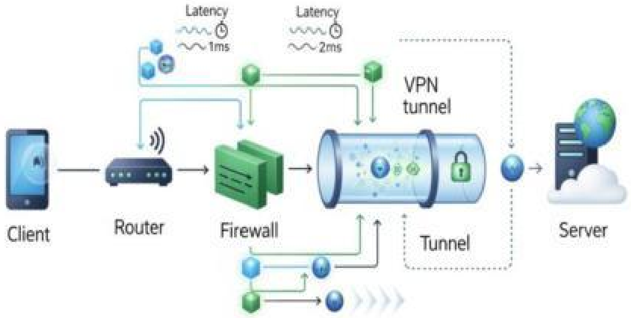
How Networks Keep Us Connected

Modern communication depends on networks. Whether you send an email, stream a video, or connect to Wi-Fi in a café, you are using a combination of hardware, software, and protocols that keep data flowing securely and efficiently.

A Network is a group of connected computers and devices that share data and resources. Inside a school or company, these connections form a LAN (Local Area Network). A Switch connects multiple devices within the LAN, while a Router directs the Data Packets to the correct destinations, either inside the local network or out to the WAN (Wide Area Network) — the Internet. Each device has a unique IP Address, which helps the router identify where the information should go.

When a user opens a website, the DNS (Domain Name System) translates the site's name into its numerical IP address, allowing the browser to locate the correct Server. The Server is a powerful computer that stores information and provides services to multiple Clients — devices such as laptops or phones that request access.

Wireless devices connect to the network through an Access Point, which converts wired signals into Wi-Fi. The speed of this connection depends on Bandwidth and Latency. High bandwidth means more data can be transferred at once, while high latency causes delays and slower response times.



To connect a local network to the Internet, a Modem is used. It converts digital signals from the computer into analog signals that can travel through telephone or cable lines. However, as soon as data travels outside a secure LAN, Security Protocols become crucial. A Firewall filters and controls incoming and outgoing traffic, preventing unauthorized access. Additionally, Encryption ensures that even if data is intercepted, it cannot be read.

In recent years, the concept of Zero Trust has transformed network security. Instead of assuming that devices inside the network are safe, Zero Trust requires strict verification for every user and device — no matter their location. For remote workers, a VPN (Virtual Private Network) provides an extra layer of protection by creating a secure, encrypted tunnel between their device and the company's internal systems.

Finally, every network has a Topology, the structure that defines how devices are physically or logically connected. Choosing the right topology and security measures helps organizations maintain fast, reliable, and safe communication — the backbone of the digital world.

Exercise 1

Decide whether the statements are True (T) or False (F).

1. A LAN connects computers that are located far away from each other.
2. A Firewall helps control and filter the flow of network traffic.
3. High latency improves the speed of a network.
4. Zero Trust assumes that every internal device can be trusted.

Exercise 2

Match each concept (A–D) with its correct description (1–4).

1. Translates web names into IP addresses.	A. Router
2. Connects several devices within a LAN.	B. DNS
3. Creates a secure tunnel for private online connections.	C. VPN
4. Directs data packets between networks.	D. Switch

Exercise 3

Complete each sentence with a suitable word from the text

1. The device that connects computers to the Internet through telephone or cable lines is called a ________.
2. Each device has a unique __________ that helps the router identify where the information should go.
3. __________ ensures that even if data is intercepted, it cannot be read.
4. Every network has a __________ that defines how devices are physically or logically connected.

Exercise 4

Rewrite the following active sentences in the Passive Voice, omitting the agent when unnecessary.

1. The router directs data packets to their destination. → __________________________

2. Firewalls protect networks from unauthorized access. → __________________________

4. The administrator must configure the firewall policy every month. → __________________________

Exercise 5 - Discussion Topics

- How important is a good Internet connection in your school or workplace? What problems appear when the network, bandwidth, or access point doesn't work properly?
- What basic rules should everyone follow to stay safe online? Mention habits like using a firewall, VPN, or strong passwords, but explain them in your own words.
- Think of a time when your Internet connection failed or was very slow. How did it affect your communication or daily tasks? What could have caused the latency or the problem?