

Network Hardware

Network hardware is the collection of physical devices that allow computers and other electronic devices to communicate with one another and exchange data within a network.

It is the “tangible” part of a network: the part that helps manage the flow of information and allows data to reach the correct destination.

Network Interface Card

A **network interface card**—also known as a **network interface controller**, **NIC**, **network adapter**, or **physical network interface**—is a digital interface consisting of an electronic component that performs all the logical processing functions required to connect a device to a computer network and consequently transmit and receive data.

A **network interface** is the physical or logical connection point between a device, such as a computer, server, or smartphone, and a specific computer network.

It converts data into signals that can be transmitted and has identifiers that are used for communication.

In everyday language, the terms *network interface card* and *network interface* are often used as synonyms, but it is technically useful to distinguish between them:

- The **network interface card** is the hardware component.
- The **network interface** is the physical or logical point through which the system communicates with the network.

In a simple case, the relationship may be:

1 physical network interface card → 1 network interface

In this case, the situation is fairly intuitive: one physical card corresponds to one network interface.

However, in modern networks, the situation may be more complex.

A single physical network interface card may support or expose multiple network interfaces in order to communicate with several specific networks.

For example, the device that connects a home network to the Internet must communicate with two different networks:

- On one side, it communicates with internal devices such as computers, smartphones, and printers.
- On the other side, it communicates with the external network, namely the Internet.

For this reason, it has multiple network interfaces, each dedicated to a different type of communication.

Each network interface has a unique identifier called a **MAC address (Media Access Control address)**.

A MAC address is a 48-bit identifier, expressed in hexadecimal format, assigned by the manufacturer to the network interface card during production.

The MAC address is used to identify a network interface within a local network. When a device sends data within the same local network, it includes the recipient's MAC address in the data header so that the message can be delivered to the correct interface.



Network interface card showing its specific MAC address

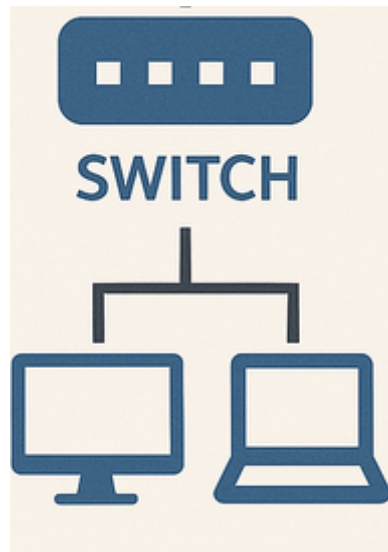
Switch

A **switch** acts like a “power strip” for a network and allows multiple devices to be connected to one another within a local network.

A switch learns which devices can be reached through each of its ports. When it knows which port is associated with the destination MAC address, it forwards the data only through that port.

For example, when a packet arrives through port 1 and is addressed to a device connected to port 3, the packet is forwarded only through port 3 and not through all the other ports.

This happens because, when data is received, the switch checks the destination MAC address in the header and uses it to determine which network interface should receive the data.



Switches are commonly used in business networks, home networks, and many other situations in which network traffic between connected devices must be managed and directed.



A 24-port switch. Each port connects to a device through a cable

Switches are mainly used in **LANs**, or local area networks, where they connect devices that are physically close to one another, for example within a home, school, or office.

Router

A **router** is a device that connects different networks and forwards packets towards their destination network.

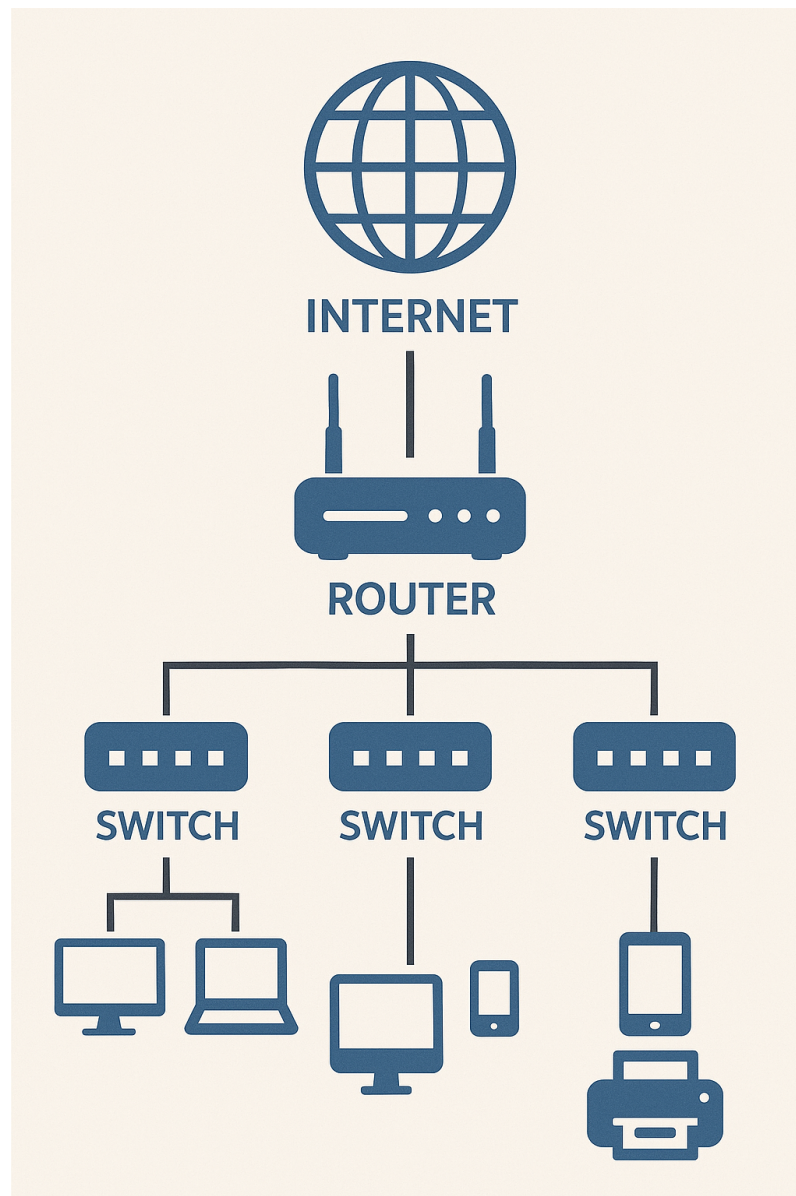
The term *router* comes from the English word *route*, meaning a road or path, because the router's purpose is to route packets towards different devices.

From a logical point of view, a router is not very different from a switch.

It also connects different network devices, but with one important difference: a router can route packets between different networks.

Routers have multiple network interfaces, one for each network they need to connect.

For example, a router connecting three different networks must have at least three network interfaces, one for each network.



A particular type of router is the **gateway**.

A gateway acts as an access point between a local network and an external network. An external network is a network that connects several local networks.

When a device on the local network wants to communicate with a device on an external network, several steps take place:

- The device sends the data to the gateway.
- The gateway checks the destination and forwards the data to the external network through the correct interface.
- When a response arrives, the gateway performs the reverse process and forwards the data to the device on the local network.
- When the external network is the Internet, the gateway is often called the **default gateway**. Home routers usually act as default gateways.

Note: not all routers are gateways.

Modem

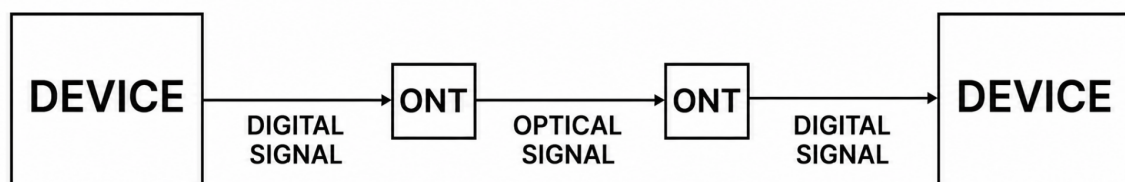
An **ADSL or fibre modem** is an electronic device that connects a computer to the Internet through a telephone line, in the case of ADSL, or through optical fibre.

The modem is usually connected to the gateway, and its task is to convert digital data into a format suitable for transmission over the network.

The term *modem* comes from **modulator-demodulator** because, in ADSL systems, it converts the computer's digital signals into analogue signals that can travel over telephone lines and performs the reverse conversion when receiving data.

In the case of optical fibre, which uses light to transmit data through the network, the device used is technically called an **ONT**, or **Optical Network Terminal**.

The ONT converts the electrical signals from the local network into optical signals for transmission through the fibre. It also converts optical signals arriving through the fibre into electrical signals that can be used by network devices.



Example

Imagine that we have an ADSL modem:

- When data is sent, the ADSL modem converts the digital signal into a signal suitable for travelling through the telephone line.
- When data is received, the modem performs the reverse operation.

Now imagine that we have an ONT:

- The ONT converts the electrical or digital signal coming from the local network into an optical signal suitable for transmission through optical fibre.
- When data is received, the ONT performs the reverse operation.



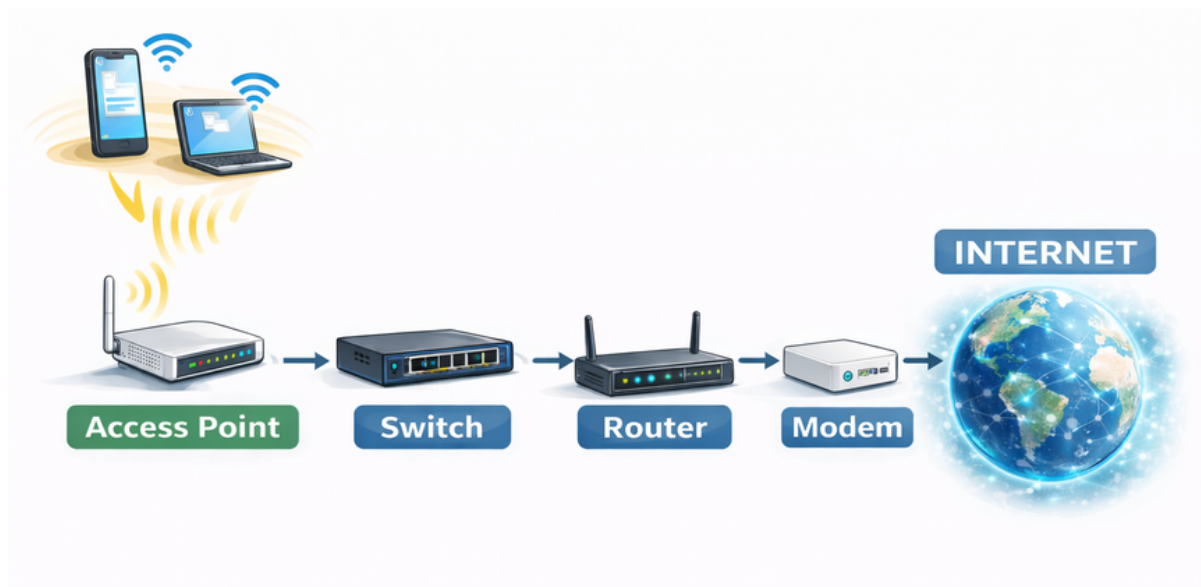
An ONT. Notice that a digital signal enters through the LAN cable—the local network—and an optical signal exits through the optical cable.

Access Point

An **access point**, also known as an **AP**, is a network device that provides devices with wireless access to an electronic communication network within a local area.

The access point is connected to a switch and allows users to access the Internet without using cables.

This means that whenever we use the Internet wirelessly, our data is sent to or received from the access point. The access point then forwards the data to the switch, which sends it to the router. Through the modem, the router can communicate with the Internet.



hotspot is a location where an access point is available for connecting to the Internet.

A hotspot is represented by the symbol shown below.



The term *hotspot* can also refer to a function provided by a device, such as a smartphone, that shares its Internet connection.

An access point is commonly associated with **Wi-Fi**, a wireless communication technology that primarily uses radio waves.

A hotspot may be:

- **Public hotspot:** a hotspot found in places such as cafés, airports, and hotels. It is connected to a fixed Internet connection and is available to multiple users, sometimes through a password.
- **Private or mobile hotspot:** a hotspot created by a device, such as a smartphone, that shares its mobile data connection with other devices.
- **Home hotspot:** a hotspot created when a home Wi-Fi router provides Internet access to nearby devices.

Firewall

A **firewall** is a hardware or software network-security component that monitors incoming and outgoing traffic and applies security rules to allow or block specific communications.

In practical terms, a firewall acts as a filter that checks data traffic and blocks dangerous or unwanted transmissions according to a set of specific rules called an **ACL**, or **Access Control List**.

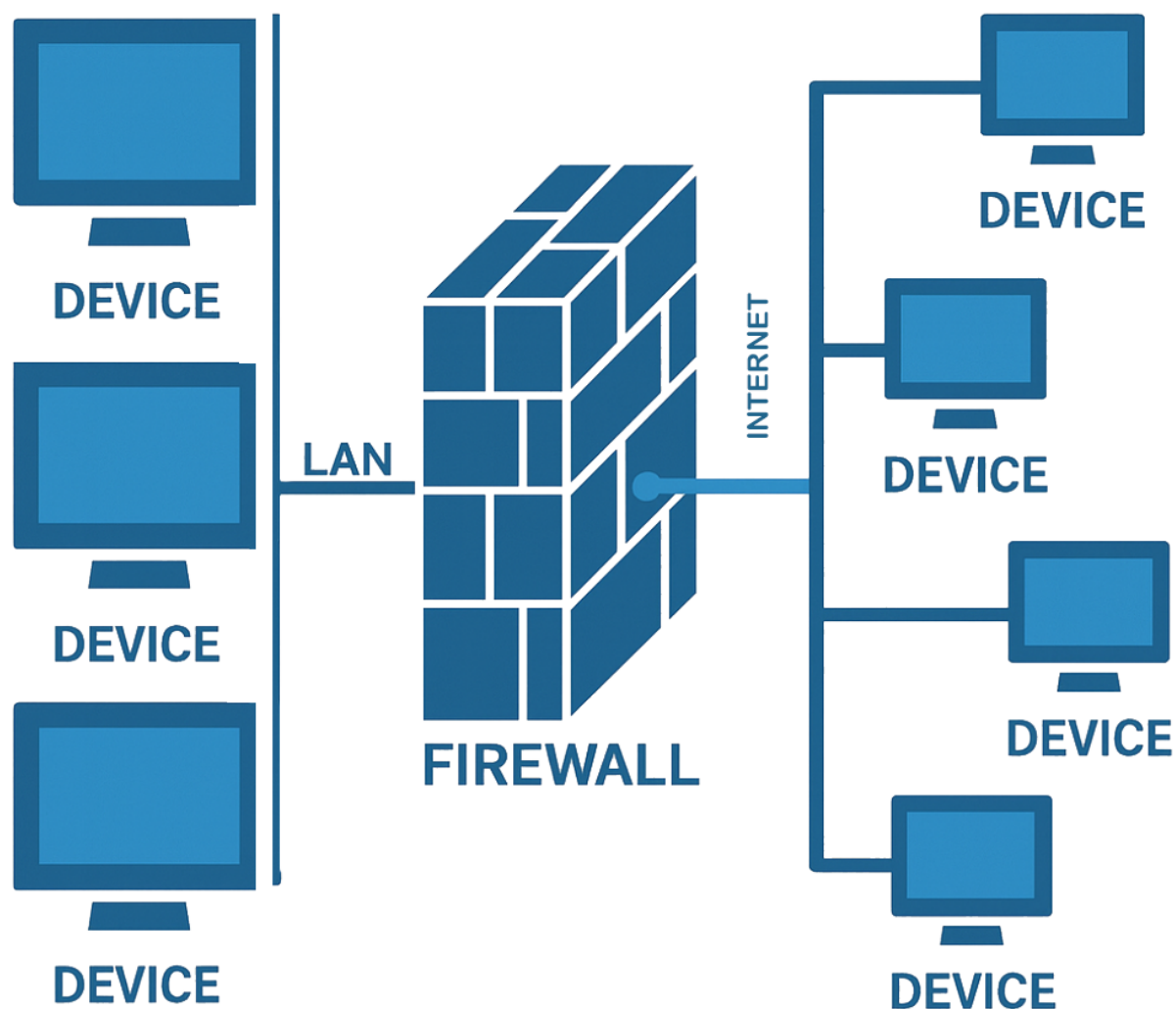
Most firewalls include standard rules to which the user can add customised rules according to their needs.

The firewall is positioned between the external network, which includes the Internet, and the internal network of a company, home, or individual user's computer.

A firewall works in this way because, in simplified terms, the internal network is considered more familiar and controllable, while the external network, such as the Internet, is treated as less trustworthy and potentially dangerous.

Most firewalls use one of two general approaches when applying their rules:

- **Default-deny:** by default, only explicitly authorised traffic is allowed, while everything else is blocked.
- **Default-allow:** by default, only explicitly prohibited traffic is blocked, while everything else is allowed.



Esempio

In many school networks, the firewall may be configured permissively for outgoing traffic. This means that internal devices can access many Internet services except those that have been explicitly blocked.

From a security perspective, a **default-deny** approach is generally stricter because it allows only explicitly authorised traffic.

However, it requires more careful configuration to avoid blocking services that are useful for teaching and learning.

Modem Router

A **modem router** is a device that performs the functions of both a modem and a router.

In practice, as well as acting as a gateway to the Internet, it allows all the devices in a home to communicate with one another.

For many years, we have commonly—but incorrectly—used the word *modem* to refer to the device used to connect to the Internet, such as a TIM HUB or Fast Gate.

In reality, devices of this kind combine several different network devices within a single unit:

- An **access point** that manages wireless connections.
- A **switch** that allows different devices on the home network to communicate with one another.
- A **gateway** that allows the home network to communicate with the Internet.
- A **firewall** that manages network security.
- A **modem**, or an **ONT**, that converts signals from the home network into a format suitable for the transmission medium being used, such as a telephone line or optical fibre.

