Network hardware

Written by [Febogamedev]

Network hardware is the collection of physical devices that allow computers and other electronic devices to communicate with one another by exchanging data within a network.
It is the “tangible” part of a network: the part that helps manage the flow of information and enables data to reach the correct destination (Kurose & Ross, 2026; Tanenbaum et al., 2021)..

Network card

A network interface card (also called a network interface controller, NIC, network adapter, or physical network interface) is a digital interface implemented as an electronic circuit board. It performs the logical processing functions required to connect a device to a computer network and to transmit and receive data (Tanenbaum et al., 2021).

A network interface is the logical or physical 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 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 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 can be more complex.
A single physical network card can support or expose multiple network interfaces in order to communicate with several different networks.

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

- On one side, with internal devices such as computers, smartphones, and printers.
- On the other side, 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 (Media Access Control) address**.
A MAC address is a 48-bit identifier, expressed in hexadecimal format, assigned by the manufacturer to the network card during production (IEEE Standards Association, 2022).

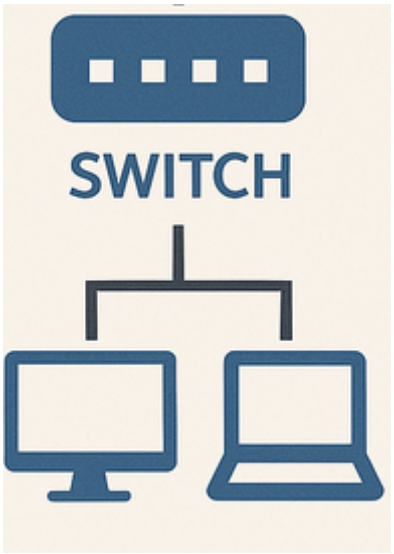
A MAC address is used to identify a network interface within a local network. When a device sends data across the same local network, it places the recipient's MAC address in the packet header so that the message can be delivered to the correct interface (IEEE Standards Association, 2022).



Network interface card showing its specific MAC address

Switch

A switch acts like a "multi-socket power strip" and allows multiple devices to be connected to one another within a local network.
A switch learns which devices can be reached through its ports. When it knows which port is associated with the destination MAC address, it forwards the data only to that port (IEEE Standards Association, 2022; Kurose & Ross, 2026)..
For example, if a packet arrives on port 1 and is addressed to a device connected to port 3, the packet is forwarded only through port 3 rather than through all the other ports.
This is because, when a packet is received, the switch checks the destination MAC address in the packet header and uses it to determine which network interface should receive the packet.



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



A 24-port switch. A device is connected to each port by cable

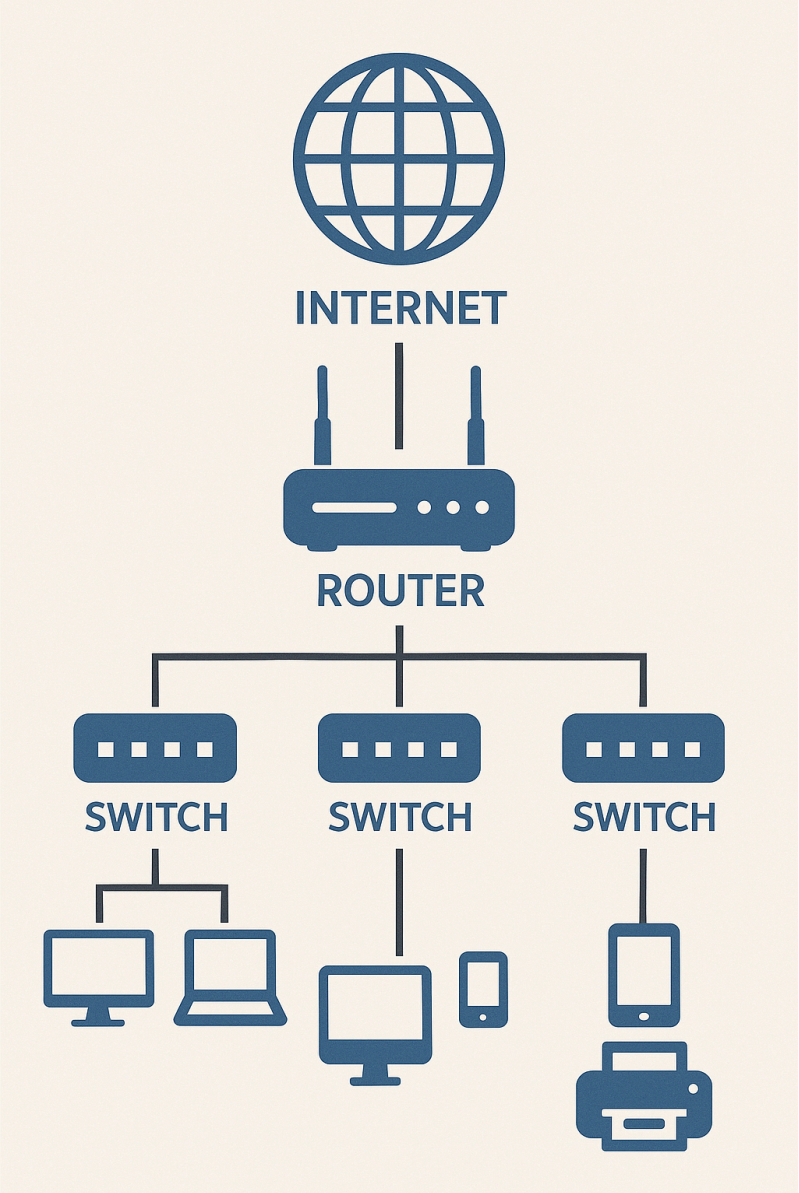
Switches are mainly used in LANs, or local area networks, where they connect nearby devices, for example within a home, school, or office.

Router

A router is a device that connects different networks and forwards packets toward their destination network (Baker, 1995).
The term router comes from the English word “route”, meaning a path or course, because a router directs packets toward 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 must connect (Baker, 1995).
For example, a router connecting three different networks must have at least three network interfaces, one for each network.



A gateway is a particular type of router.
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 (Baker, 1995).
When a device on the local network wants to communicate with a device on the 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 appropriate interface.
- When a response arrives, the gateway follows the reverse path 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 act as default gateways.

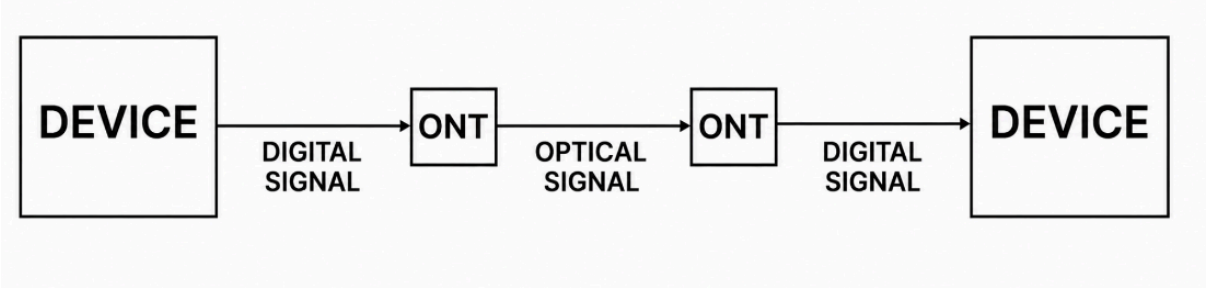
Note: not all routers are gateways.

Modem

An ADSL or fiber modem is an electronic device that connects a computer to the Internet through a twisted-pair telephone line for ADSL or through optical fiber.
The modem is usually connected to the gateway, and its task is to convert digital data into a format suitable for the network.

The term modem comes from “MOdulator-DEModulator” because, in ADSL systems, it converts a computer’s digital signals into analog signals that can travel over telephone lines, and vice versa (Tanenbaum et al., 2021).

In a fiber-optic connection, which uses light to transmit packets across the network, the device used is technically an **ONT** (Optical Network Terminal).
The ONT converts electrical signals from the local network into optical signals for the fiber and, in the opposite direction, converts optical signals from the fiber into electrical signals that network devices can use (International Telecommunication Union, 2019).



Example
Suppose we have an ADSL modem:
- When data is sent, the ADSL modem converts the digital signal into a signal suitable for transmission over the twisted-pair telephone line.
- When data is received, the modem performs the reverse operation.

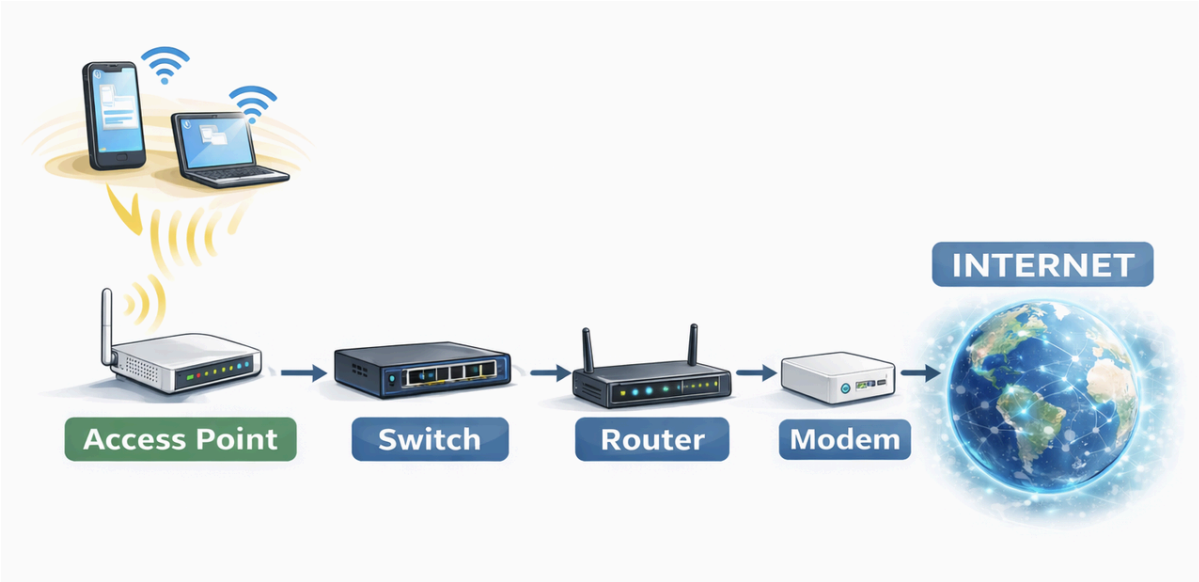
Suppose we have an ONT:
- The ONT converts the electrical/digital signal from the local network into an optical signal suitable for the fiber.
- When data is received, the ONT performs the reverse operation.



An ONT. Note that a digital signal enters through the LAN cable (the local network), while an optical signal leaves through the optical cable

Access Point

An access point, also abbreviated as AP, is a network device that provides local wireless access to an electronic communication network (IEEE Standards Association, 2025).
The access point is connected to a switch and allows users to access the Internet without a wired connection.
This means that whenever we access the Internet wirelessly, our data is sent to or received from the access point. The access point forwards it to the switch, which sends it to the router; the router can then communicate with the Internet through the modem.



A hotspot is a location where an access point is available for Internet access.
A hotspot is represented by the symbol shown below:



The term hotspot also refers to a function of a device, such as a smartphone, that shares its Internet connection.

An access point is most commonly associated with Wi-Fi, a wireless connection technology that uses radio waves (IEEE Standards Association, 2025).
A hotspot can be:

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

Firewall

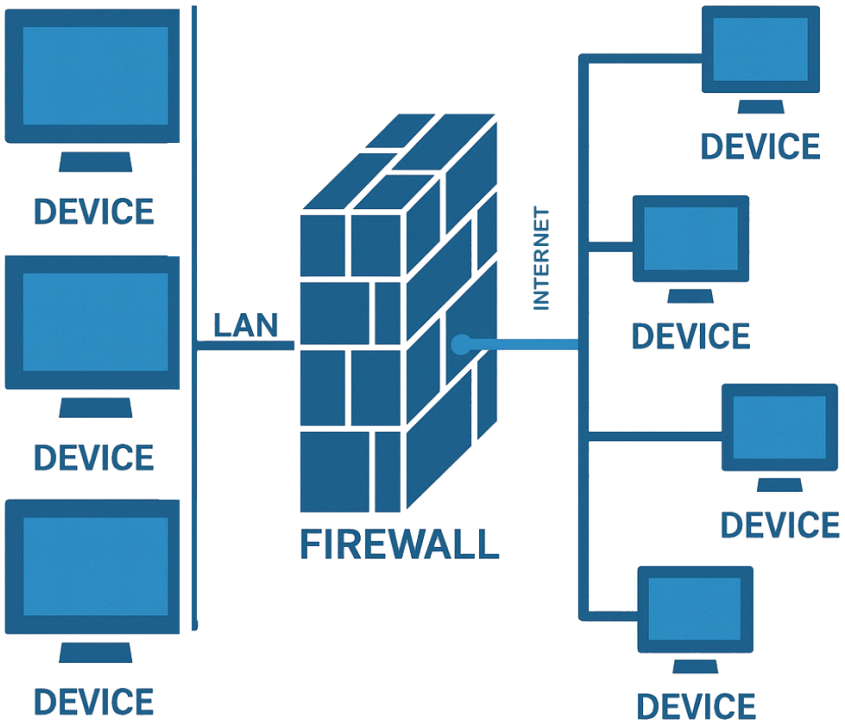
A firewall is a hardware or software network-security component that monitors incoming and outgoing traffic and applies security rules to allow or block specific communications (Scarfone & Hoffman, 2009).

In practical terms, a firewall acts as a filter that inspects data traffic and blocks dangerous or unwanted transmissions according to specific rules called ACLs (Access Control Lists). Most firewalls include standard rules to which the end user can add customized rules according to their needs.

The firewall is positioned between the external network, including the Internet, and the internal network of a company or home, or even an individual user's computer.
A firewall works this way because, in simplified terms, the internal network is considered better known and more controllable, whereas an external network such as the Internet is treated as less trustworthy and potentially dangerous.

Most firewalls use one of two general rule-application policies (Scarfone & Hoffman, 2009):

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



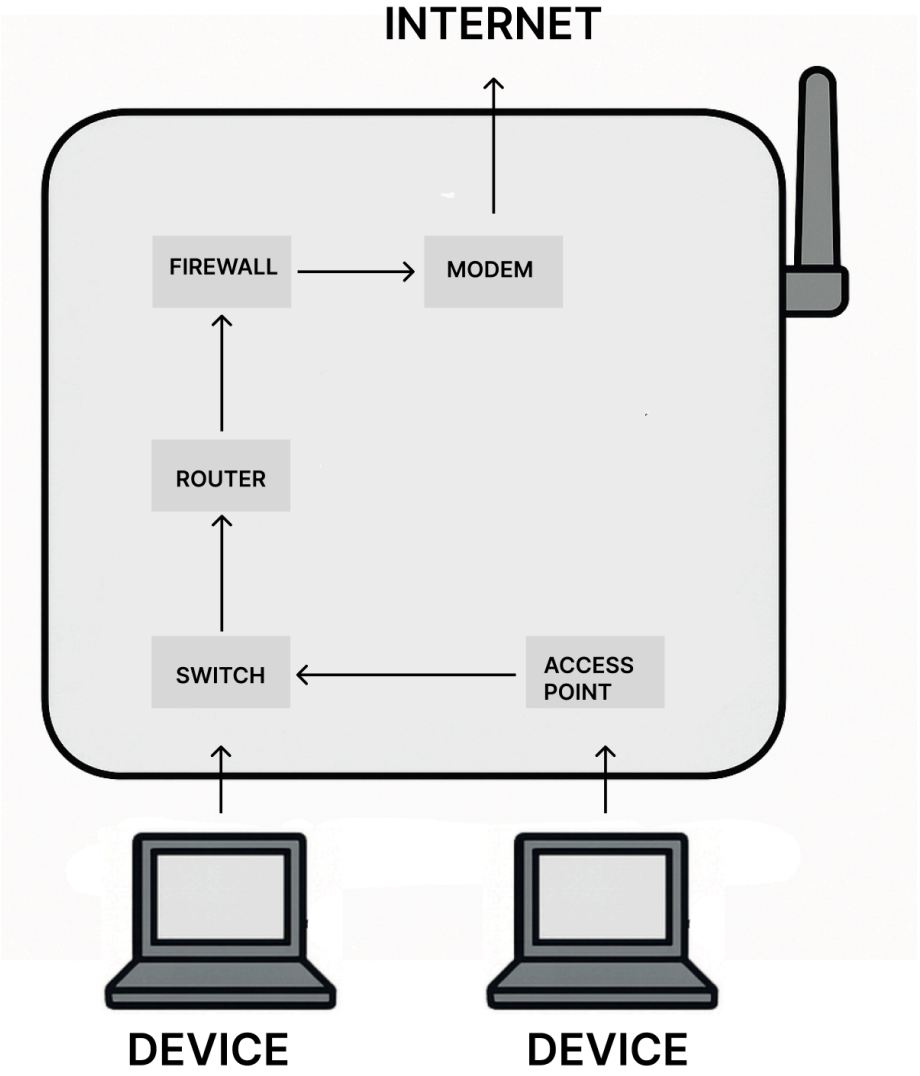
Example
In many school networks, the firewall may be configured permissively for outgoing traffic. This means that internal devices can access many Internet services except those that are explicitly blocked.
From a security perspective, a default-deny policy is generally stricter because it permits only explicitly authorized 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 (Kurose & Ross, 2026).
In practice, as well as serving as an Internet gateway, it allows all the devices in a home to communicate with one another.

For many years, people have incorrectly called the device used to connect to the Internet a “modem”, as in the case of devices such as the TIM HUB or Fast Gate.
In reality, these units combine several devices in a single box:

- An access point that handles wireless connections.
- A switch that connects the various devices on the home network.
- A gateway that enables communication with the Internet.
- A firewall that provides network security.
- A modem (or ONT) that converts signals from the home network into a format suitable for the transmission medium being used, such as a twisted-pair telephone line or optical fiber.


INTERNET
FIREWALL
MODEM
ROUTER
SWITCH
ACCESS POINT
DEVICE
DEVICE

Supplementary materials

Exercises

Network Interface Card, Network Interface, and MAC Address
A laptop can connect to a network either through an Ethernet cable or via Wi-Fi. When connected by cable, it communicates through one network interface; when using Wi-Fi, it uses another.

Answer the following questions:

- Explain the difference between a network interface card and a network interface.
- Explain why multiple network interfaces can exist on the same device.
- Describe the function of a MAC address.
- Can two network interfaces on the same device be identified by the same MAC address? Justify your answer based on what is explained in the learning material.
- A computer needs to send data to another device on the same local network. Explain which information in the header is used to identify the destination interface.
- Explain why knowing only the name assigned to the computer by the user would not be sufficient to perform the same function as a MAC address.

The Lab Switch
A school laboratory has a switch to which twenty computers are connected.

The computer connected to port 4 needs to send data to the computer connected to port 15. The switch already knows the MAC address associated with port 15.

Answer the following questions:

- Describe what the switch does when it receives the packet from port 4.
- Identify which information in the packet it uses to decide where to forward it.
- Explain why the switch does not necessarily need to send the packet to all twenty ports.
- If the destination computer is disconnected from port 15 and connected to another port, explain which information the switch will need to update.
- Explain why a switch is particularly suitable for connecting devices that belong to the same LAN.
- A student suggests using the switch to connect the school network directly to three different external networks. Explain why, based on the learning material, another type of device would be required.

Connecting Three Different Networks
A company has three separate networks:

- A network for the administrative offices.
- A network for the technical laboratory.
- A network for guests.

The company wants to allow communication between these networks.

Answer the following questions:

- Identify which device should be used to connect the three networks.
- Explain why a switch does not perform the same task.
- Indicate the minimum number of network interfaces the chosen device must have to connect the three networks directly.
- Explain why each interface must be associated with a different network.
- Describe in general terms what happens when a device on the office network needs to send a packet to a device on the laboratory network.
- Explain in what sense the chosen device must decide which “path” to use to forward the packet.

Leaving the Home Network

A home computer is connected to the local network and wants to communicate with a server on the Internet.
The network includes a device that acts as the default gateway.

Reconstruct the path followed by the data:

- Explain why the computer cannot treat the Internet as if it were simply another device on its local network.
- Identify the device to which it must send data intended for an external network.
- Describe what the gateway does when it receives this data.
- Explain what happens when the response from the Internet returns to the home network.
- Explain why a gateway must have at least one interface facing the internal network and one facing the external network.
- Evaluate the statement: “All routers are necessarily gateways.” Indicate whether it is correct according to the learning material and justify your answer.

ADSL or Fiber?

Two homes use different technologies to connect to the Internet.

- Home A: uses an ADSL connection over a telephone copper pair.
- Home B: uses a fiber-optic connection.

Answer the following questions:

- Identify which device performs the necessary conversion in Home A.
- Explain what happens to the signal when data is sent through the ADSL connection.
- Identify which device performs an equivalent function in the fiber-optic connection.
- Explain what an ONT converts when data passes from the local network to the fiber-optic link.
- Describe what happens in the reverse direction, when data arrives from the fiber-optic network and reaches the local network.
- Explain why, according to the terminology used in the learning material, simply calling the device used for a fiber connection a “modem” is not technically precise.

Designing a School Wi-Fi Network

A school already has a wired network made up of switches and routers. It also wants to allow laptops and tablets to connect wirelessly.

It must also create a Wi-Fi area that students can access in the library.

Answer the following questions:

- Identify which device must be added to provide wireless access to the network.
- Explain which other network device it should be connected to.
- Reconstruct the path that data from a tablet might follow when a student opens a web page, using the concepts access point → switch → router/gateway → modem or ONT → Internet.
- Explain the difference between an access point, Wi-Fi, and a hotspot.
- A student activates the hotspot function on their smartphone. Explain in what sense the phone is providing a function similar to the one described in the learning material.
- Explain why the library hotspot refers to a location or access service, whereas Wi-Fi refers to the technology used for the wireless connection.

Configuring the Firewall

A school wants to protect its network.
Students must be able to use the web and certain educational services, but the administrator wants to prevent communications considered undesirable.

Two strategies have been proposed:

- Strategy A: allow all traffic except what is explicitly blocked.
- Strategy B: block all traffic except what is explicitly allowed.

Analyze the two strategies:

- Associate each strategy with the concepts of default-allow and default-deny.
- Explain the function of the firewall between the internal and external networks.
- Explain what ACLs are and what role they play in firewall operation.
- Identify which of the two strategies is described in the learning material as generally more rigorous from a security perspective.
- Explain what practical problem an overly restrictive default-deny configuration could cause in a school.
- Imagine that a new online educational service is introduced. Describe what change might be required in the firewall rules so that students can use it.
- Choose which strategy you would adopt for a school network and justify your decision by considering both security and usability.

What Is Really Inside the Home “Modem”?

A family receives a single device from its Internet service provider. Four computers are connected to it by cable, smartphones connect through Wi-Fi, and the Internet line is also connected to the same device.

One family member says:
“This device is simply a modem.”

- Analyze this statement by identifying all the functions the device must perform.
- Identify which component allows devices connected by cable to communicate within the local network.
- Identify which component allows smartphones and tablets to connect wirelessly.

- Identify which component allows the home network to communicate with the external network.
- Identify which component controls traffic by applying security rules.
- Identify which component performs the conversion required to use the transmission medium provided by the ISP.
- Explain why a modern modem router can therefore integrate several logical devices or functions within the same physical unit.
- A computer connected via Wi-Fi opens a website. Reconstruct the complete path followed by the data through the different components of the device.
- Finally, imagine that the Wi-Fi function stops working while the integrated switch continues to operate. Explain which devices could continue to use the network and which could not, and justify your answer.

Bibliography

Baker, F. (1995). *Requirements for IP version 4 routers (RFC 1812)*. RFC Editor. https://doi.org/10.17487/RFC1812

IEEE Standards Association. (2022). *IEEE standard for Ethernet (IEEE Std 802.3-2022)*. https://standards.ieee.org/ieee/802.3/10422/

IEEE Standards Association. (2025). *IEEE standard for information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications (IEEE Std 802.11-2024)*. https://standards.ieee.org/ieee/802.11/10548/

International Telecommunication Union. (2019). *Gigabit-capable passive optical networks (G-PON): Physical media dependent (PMD) layer specification (Recommendation ITU-T G.984.2)*. https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=14000

Kurose, J. F., & Ross, K. W. (2026). *Computer networking: A top-down approach* (9th ed.). Pearson. https://www.pearson.com/en-us/subject-catalog/p/computer-networking-a-top-down-approach/P200000013385/9780135415603

Scarfone, K., & Hoffman, P. (2009). *Guidelines on firewalls and firewall policy (NIST Special Publication 800-41 Rev. 1)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-41r1

Tanenbaum, A. S., Feamster, N., & Wetherall, D. J. (2021). *Computer networks* (6th ed.). Pearson. https://www.pearson.com/en-us/subject-catalog/p/computer-networks/P200000003188/9780137523214

Further reading

- James F. Kurose and Keith W. Ross, Computer Networking: A Top-Down Approach, 9th ed., Pearson, 2026 — Connects the operation of network interfaces, switches,

routers, Ethernet, and wireless networks to the protocols and layered architecture that allow data to travel across local networks and the Internet.

- Andrew S. Tanenbaum, Nick Feamster, and David J. Wetherall, Computer Networks, 6th ed., Pearson, 2022 — Provides a systematic explanation of networking hardware and transmission systems, including Ethernet, switching, routing, wireless networks, network interfaces, and network security.
- Wendell Odom, CCNA 200-301 Official Cert Guide, Volume 1, 2nd ed., Cisco Press, 2024 — Offers a more practical treatment of network devices, with detailed coverage of Ethernet LANs, switches, switch interfaces, WAN connections, routers, and IP routing, making it useful for understanding how networking hardware is configured and used in real networks.
- Wendell Odom, David Hucaby, and Jason Gooley, CCNA 200-301 Official Cert Guide Library, 2nd ed., Cisco Press, 2024 — Extends the practical study of network hardware to wireless LANs, access points, IP access control lists, security services, network architecture, switches, and routers, providing a bridge between basic concepts and professional network administration.
- Douglas E. Comer, Computer Networks and Internets, 6th ed., Pearson, 2017 — Presents a broad introduction to the technologies and devices that form computer networks and the Internet, helping relate physical network infrastructure, local networks, internetworking, routing, wireless communication, and network security within a unified architecture.

Editorial notes

In producing these materials, I have used generative artificial intelligence tools to support the writing process, particularly to improve the form of the text, reorganize content, refine wording, and speed up certain editorial tasks.

As I work independently on the production of these materials, I try to automate any activities that can reasonably be automated, so that I can devote more time to research, design, and content development.

However, artificial intelligence does not determine the content of this work: the choice of topics, structure, ideas, interpretations, examples, and teaching approach are developed by me. AI is therefore used primarily as a tool to support production and formal revision, while authorship and responsibility for the design and content remain mine.

Unless otherwise indicated, this material is distributed under the Creative Commons Attribution–NonCommercial–ShareAlike 4.0 International license (CC BY-NC-SA 4.0).

You are therefore free to share, redistribute, adapt, and create derivative works based on this material, provided that appropriate credit is given, the material is not used for commercial purposes, and any modified or derivative versions are distributed under the same license.

