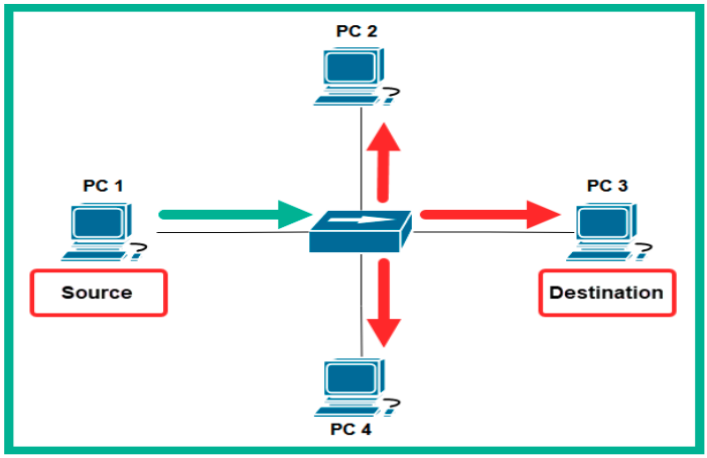
Networking Devices

Networking devices are tools that connect different parts of a network and help users share information and resources.

HUB

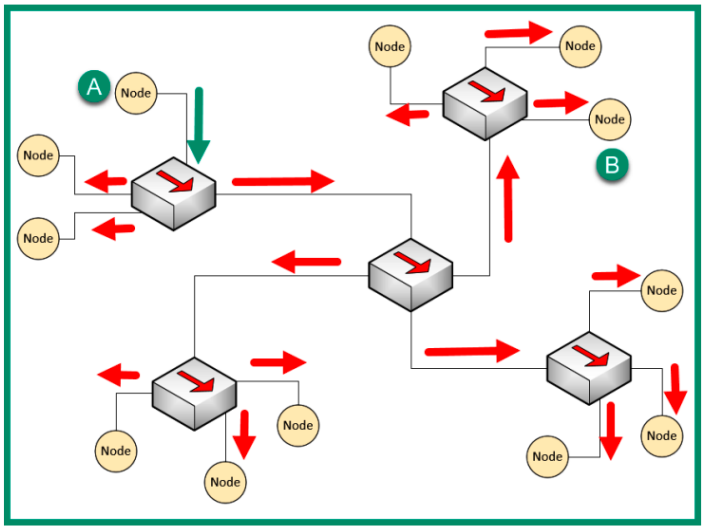
A network hub **is an old networking device that works at** OSI Layer 1**.**
It acts like a repeater**, meaning it takes an incoming electrical signal and sends it out to** all other ports**, not just the intended device.**

The following diagram shows how a hub forwards a message:



+

All devices connected to a hub share one collision domain**.**
A collision domain **is a part of the network where two or more devices can send data at the same time and cause a** collision**.**
When a collision happens, the data is lost, and the sender has to send it again**.**



hub sends every message to all ports without checking any MAC or IP address.
So if two devices try to send data at the same time, problems can happen.

To avoid this, devices use **CSMA/CD**, which means:

- Before sending data, a device **listens** to the network.
- If it hears another signal, it knows the network is busy.
- The device **waits** until the network is clear.
- When no signal is detected, it finally sends the message.

Because of this limitation, **hubs do not scale well** for larger networks.

Layer 2

Layer 2 Switch (L2 Switch)

- Operates at the **Data Link Layer (Layer 2)** of the OSI model.
- Forwards **Ethernet frames** based on **destination MAC addresses**.
- Used to connect end devices such as computers, printers, and servers.
- Creates **separate collision domains** for each port.
- Does not perform IP routing.

Need for VLANs

Large organizations divide their networks into **VLANs (Virtual LANs)** to:

- Logically segment a physical network
- Separate departments (HR, Sales, IT, etc.)
- Reduce broadcast traffic by creating **smaller broadcast domains**

- Improve security and performance

📌 **Broadcasts stay inside the same VLAN** and do not reach other VLANs.

Why Inter-VLAN Routing Is Needed

- Devices in **different VLANs cannot communicate** because VLANs are isolated at Layer 2.
- To enable communication between VLANs, **Layer 3 routing** is required.

Example:
Sales VLAN ↔ IT VLAN
→ Need a Layer 3 device to route traffic.

Layer 3 Switch (L3 Switch)

•Network Switches

- Traditional switches operate at **Layer 2 (Data Link Layer)** of the OSI model.
- They forward data frames using **MAC addresses**.
- Modern networks also use **Layer 3 switches**, which can perform routing functions.

VLANs (Virtual LANs)

- VLANs divide a single physical network into **multiple logical networks**.
- Commonly used in large organizations to separate departments (HR, Sales, IT, etc.).
- Each VLAN is a **separate broadcast domain**, so broadcasts do not cross VLAN boundaries.

Inter-VLAN Communication

- Devices in different VLANs **cannot communicate directly**.
- A **Layer 3 device** is required to route traffic between VLANs.
- This process is known as **inter-VLAN routing**.

Router vs. Layer 3 Switch

Feature	Router	Layer 3 Switch
OSI Layer	Layer 3 only	Layer 2 + Layer 3
Purpose	Connect different networks (WAN/LAN)	Internal LAN routing (Inter-VLAN)
Features	Advanced security, NAT, VPN, voice	Basic routing, high-speed switching
Speed	Slower (software-based)	Very fast (hardware-based)

Difference Between Layer 2 Switch and Layer 3 Switch

Feature	Layer 2 Switch	Layer 3 Switch
OSI Layer	Data Link Layer (Layer 2)	Network Layer (Layer 3)
Primary Function	Forwarding frames based on **MAC addresses**	Forwarding packets based on **IP addresses**
Routing Capability	Cannot perform routing between VLANs	Can perform **inter-VLAN routing** and route between subnets
Traffic Handling	Works mainly within a single **VLAN**	Works across multiple VLANs and networks
Address Table	Uses **MAC address table (CAM table)**	Uses **routing table + MAC table**
Example Use Case	Office network connecting PCs, printers	Enterprise networks requiring VLAN routing and inter-subnet communication
Performance	High-speed switching within VLAN	Slightly more processing due to routing, but optimized for Layer 3 switching

Bridge

A **network bridge** is a device that works at **Layer 2** of the OSI model. It helps split a network into **smaller collision domains** to improve performance.

In older networks, **hubs** were used to connect devices. But hubs created **one big collision domain**, meaning:

- Any message sent by one computer was **broadcast to every device**.
- If two or more computers sent data at the same time, **collisions** happened.

A **bridge** solves this problem by controlling traffic and reducing collisions.

Bridge vs Hub

Feature	Hub	Bridge
OSI Layer	Layer 1	Layer 2
Collision Domains	One large domain	Divides into multiple smaller domains
Data Forwarding	Broadcasts to all ports	Filters using MAC addresses
Intelligence	Not intelligent	Intelligent (learns MAC addresses)
Performance	More collisions, slower	Fewer collisions, better performance

Difference Between Layer 2 Switch and Bridge

Feature	Bridge	Layer 2 Switch
OSI Layer	Layer 2	Layer 2
Ports	2–4 ports	Many ports (12, 24, 48…)
Forwarding Method	Software-based	Hardware-based (ASIC)
Speed	Slower	Very fast
Collision Domains	Few	Each port is a separate collision domain
Broadcast Domain	One	One (unless VLANs are used)
MAC Address Table	Small	Large (CAM table)
Duplex Mode	Mostly half-duplex	Full-duplex supported
Use Case	Older, small networks	Modern, high-performance networks

(ASIC = a special hardware chip in switches that performs switching tasks at high speed.)

Routers (Layer 3 Devices)

1. Function of a Router

- A router operates at **Layer 3 (Network Layer)** of the OSI model.
- It connects **two or more different networks** together.
- It acts as the **default gateway** for hosts.
- It forwards packets from one network to another (e.g., LAN to internet or VLAN to VLAN).

2. How a Router Processes an Inbound Packet

Step 1: Layer 2 Check (MAC Address)

- When a frame enters the router, it examines the **destination MAC address**.
- If the MAC address matches the router's interface MAC, the router accepts it.
- The frame is then **de-encapsulated** (Layer 2 header removed).

Step 2: Layer 3 Check (IP Address)

- The router now inspects the **destination IP address** in the packet.
- It uses this IP to decide where the packet should go next.

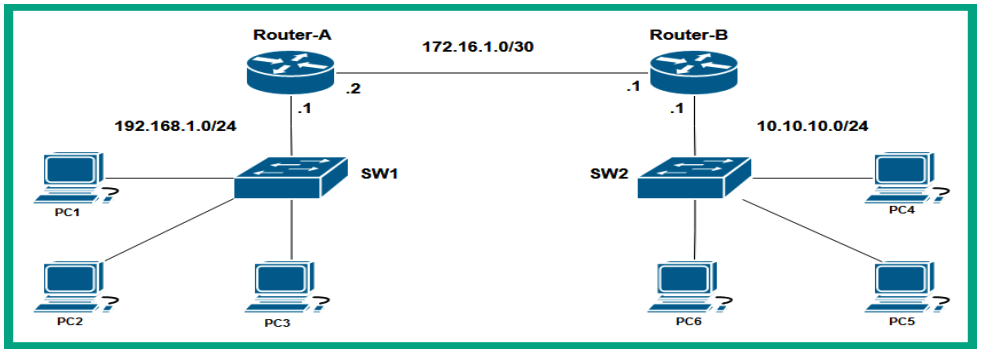
3. Routing Table Lookup

- Every router has a **routing table** containing routes to:
  - Local networks
  - Remote networks

    - Internet routes
- The router searches the routing table **from top to bottom**.
- When it finds a matching route:
    - It stops searching
    - Uses that route to forward the packet
    - Determines the **next-hop IP** and outbound interface

4. Forwarding

- After selecting the route, the router:
    - Re-encapsulates the packet with a new Layer 2 header
    - Sends it out the correct **outbound interface**



Network summary (from the diagram)

- **Left LAN:** `192.168.1.0/24` (PC1, PC2, PC3). Default gateway → **Router-A** (e.g. `192.168.1.1`).
- **Right LAN:** `10.10.10.0/24` (PC4, PC5, PC6). Default gateway → **Router-B** (e.g. `10.10.10.1`).
- **Router inter-link:** `172.16.1.0/30` between Router-A and Router-B (two usable IPs only — a typical /30 point-to-point network).

Switches (SW1, SW2) connect the PCs to their local routers and operate at Layer-2 (MAC & CAM tables).

Example flow: PC1 (192.168.1.10) → PC4 (10.10.10.20)

1. **PC1 wants to send to PC4's IP** (different subnet), so it sends the packet to its **default gateway** (Router-A).
    - PC1 looks up Router-A's MAC in its **ARP cache**. If unknown, PC1 broadcasts an **ARP request**; Router-A replies with its interface MAC.
    - SW1 learns PC1's MAC → Port mapping in its **CAM table** while forwarding the ARP request/reply.
2. **PC1 sends the Ethernet frame** with:
    - Dest MAC = Router-A's LAN MAC
    - Src MAC = PC1's MAC

    - IP src = 192.168.1.10, IP dst = 10.10.10.20
3. **Router-A receives the frame**, checks the destination MAC — it matches its interface MAC, so it **de-encapsulates** and inspects the IP packet.
    - Router-A checks its **routing table** and sees that `10.10.10.0/24` is reachable via the directly connected interface toward Router-B (over the `172.16.1.0/30` link) or via a static/ learned route to Router-B.
4. **Router-A forwards the packet** toward Router-B:
    - Router-A re-encapsulates the packet in a new frame addressed to the next hop (Router-B's link MAC) and sends it out on the `172.16.1.0/30` interface.
    - If Router-A does not already know Router-B's link MAC, it ARPs for it on the /30 link first.
5. **Router-B receives, decapsulates, and routes**:
    - Router-B sees IP dst = `10.10.10.20`, knows it is on its directly connected `10.10.10.0/24` network, so it re-encapsulates the packet with dest MAC = PC4's MAC (using ARP on its LAN if required) and sends it via SW2 to PC4.
6. **PC4 receives the packet** and replies. The return follows the reverse path: PC4 → Router-B → Router-A → PC1. Each hop uses ARP, CAM updates and routing table lookups as needed.

Access Point (AP)

An **access point (AP)** is a device that lets Wi-Fi devices connect to a **wired network**. It provides wireless access so users can connect without using cables.

Organizations mainly use wired networks, but APs add **mobility and convenience**. By connecting an AP to a switch, you can easily extend the wired network to wireless.

The AP works at **Layer 2** and sends wireless signals on **2.4 GHz and 5 GHz** using the **IEEE 802.11** Wi-Fi standards.

An AP converts a wired network into a wireless network so Wi-Fi devices can connect and communicate just like wired devices.

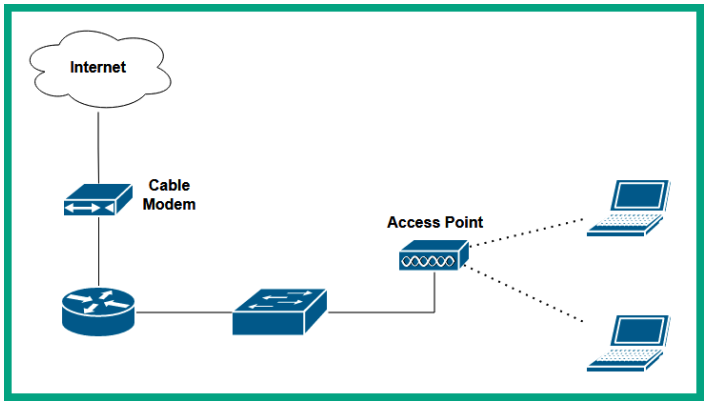


Figure: Wireless network

The following steps are written in layman's terms to provide clarity on how a wireless client proceeds to send a message on a wireless network:

1. **Client-A wants to send a message** to another wireless client on the same Access Point (AP).
2. **Client-A checks if the network is free** by sending a **Request to Send (RTS)** to the AP.

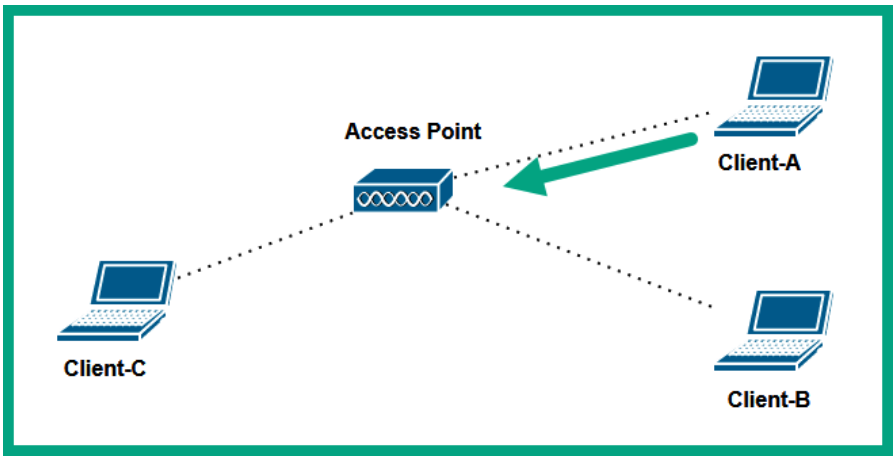


Figure: Requesting status from the AP

3. **AP responds with Clear to Send (CTS)** if no one else is transmitting.

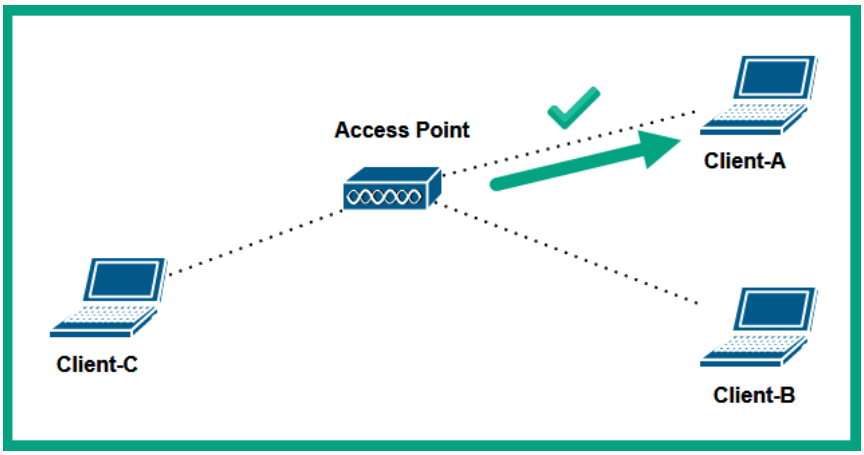


Figure: AP providing a response

4. **Client-A sends the message** to the AP.
5. **AP forwards the message** to the destination client (or rebroadcasts to all clients, like a hub).

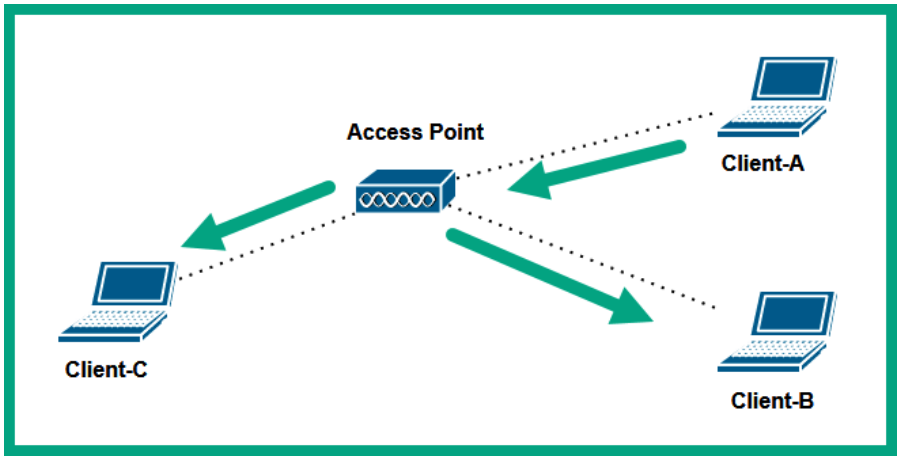


Figure: AP forwarding message

Wireless Router

- A wireless router is an all-in-one device that acts as a router, switch, and access point (AP).
- It creates a Wi-Fi network on 2.4 GHz and 5 GHz frequencies, lets devices connect wired or wirelessly, and allows communication between connected devices.
- It also routes traffic between the wired and wireless networks, giving each network a separate IP subnet.
- So, a smartphone on Wi-Fi gets a different IP from devices on the wired LAN.

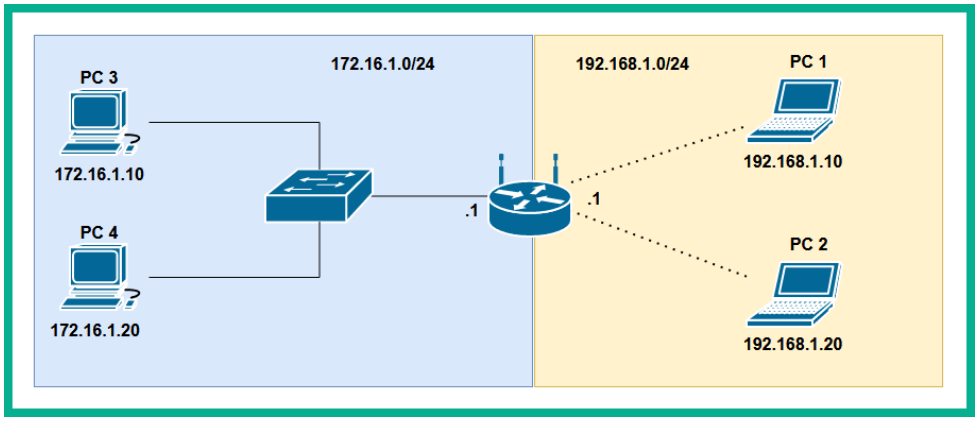


Figure: Wireless router

- PC 1 has an IP address in the 192.168.1.0/24 network and connects to a wireless router.
- The router connects to a wired LAN on the 172.16.1.0/24 network through a switch.
- The router's job is to route traffic between the wireless and wired networks, and between these two different IP networks.

Wireless LAN Controller (WLC)

- A WLC is a device that centrally manages all wireless access points (WAPs) in an organization.
- **Purpose:** Simplifies configuration, firmware upgrades, and troubleshooting across multiple WAPs.
- **Scalability:** As wireless devices increase, additional WAPs are added to ensure coverage, eliminate dead zones, and provide sufficient bandwidth.
- **Central Management:**
  - Configure all WAPs from a single web interface.
  - Automatically push configuration changes to all WAPs.
  - Monitor performance and identify issues in real time.
- **Benefits:**
  - Reduces manual configuration and human error.
  - Enables scheduling and monitoring of firmware updates.
  - Ensures wireless network operates optimally, even if some WAPs fail.

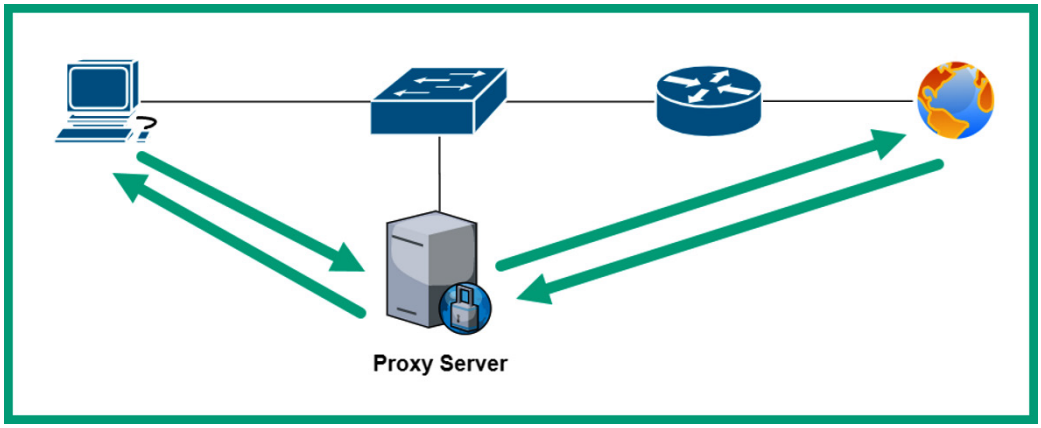
Proxy server

A **proxy server** is a network device or server that acts as an intermediary between a client (like a computer) and other servers on the internet or a network. It receives requests from clients, checks or filters them, and then forwards them to the destination server. When the server responds, the proxy sends the response back to the client.

Key points:

- Enhances **security** by hiding internal network details.
- Can **filter websites** (allowing or blocking access).
- Can **cache data** to improve performance.
- Helps **monitor and control** network traffic.

In simple terms, it's like a **middleman** that manages and protects the communication between your device and the internet.



Example:

If a company doesn't want employees visiting social media during work hours, a proxy can block access while still allowing them to browse work-related sites. At the same time, it can cache frequently visited sites like internal portals for faster access.

Common Types of proxy servers:

• **Forward proxy** – This is a common type of proxy that intercepts a client's request message and forwards it to the destination on the internet
• **Reverse proxy** – This type of proxy server intercepts and forwards the request message from devices that are on the internet to the servers on the internal network of the organization.

Cable Modem (CM)

- **A** cable modem **is a device provided by an ISP that connects a customer's network to the ISP's cable modem termination system (CMTS) n**etwork **over coaxial cables.**
- **It acts as a** router, switch, and wireless access point**, allowing devices at home or office to access the internet through the SP's infrastructure**.
- A **Digital subscriber line (DSL)** DSL modem is another type of modem provided by ISPs that delivers internet over regular telephone lines, also known as public switched telephone network (PSTN) lines PSTN, sometimes called the plain old telephone service (POTS) lines.

Repeater

- A **repeater (Wi-Fi extender)** is a **Layer 1 device** that receives a weak wireless signal and **rebroadcasts it with stronger power**.
- Used in buildings or large areas to **extend Wi-Fi coverage**.
- Wireless signals become weaker with distance and due to obstacles like **concrete or steel walls**.
- Repeaters are placed in **strategic locations** to capture signals from an AP and **regenerate the same signal**.
- Helps eliminate **dead zones** and ensures better wireless coverage for all users.