# 4. Network Fundamentals

A network is a structure composed of multiple nodes, such as computers, mobile devices, servers, or any other device capable of sending and receiving information. These nodes are interconnected through communication channels, which can be physical (copper cables or fiber optics) or wireless (Bluetooth or Wi-Fi). The primary goal of any network is to share resources like files, directories, and applications, as well as facilitate electronic communication between devices and their users. Data within a network flows in the form of packets traveling from one point to another, following rules defined by protocols such as IP, TCP, UDP, and others.

## Types of Networks

Networks are mainly classified based on their size and the number of users they impact:

### LAN (Local Area Network)

These are limited-size networks usually confined to a building or a group of nearby buildings. They offer high speed and security due to their small size and ease of management.

### WAN (Wide Area Network)

These networks interconnect cities or even countries. The internet itself is an example of a WAN, connecting multiple dispersed LANs worldwide.

### MAN (Metropolitan Area Network)

Covers a broader area than a LAN but is not extensive enough to interconnect cities or countries like a WAN.

### PAN (Personal Area Network)

The smallest type of network, limited to the personal devices of a single individual that communicate with each other.

### VPN (Virtual Private Network)

Establishes an encrypted tunnel to protect network traffic when passing through a public network like the internet. It ensures data confidentiality and integrity using protocols like IPsec, OpenVPN, or WireGuard.

## Network Topologies

A topology describes how devices in a network are organized and connected, either physically (actual arrangement of cables and devices) or logically (how data flows through the network). Common topologies include:

- Bus: All devices are connected to a central cable that acts as a highway for data transmission. It's simple and cost-effective but prone to failure if the central cable is damaged.
- Star: All devices connect to a central hub or switch.
- Ring: Devices are connected in a circular fashion, and data travels in one direction, passing through each device until it reaches its destination.
- Mesh: Connects multiple devices directly to each other, allowing multiple paths for data transmission. There are two types:
  - Full Mesh: Every device connects directly to every other device, offering maximum redundancy at a high cost.
  - Partial Mesh: Only some devices are interconnected, reducing cost and complexity but also redundancy.
- Tree: A variation of the star topology where devices are organized in groups branching from a central point, combining the benefits of star and bus topologies.

## Traffic Distribution Patterns

Traffic distribution patterns describe how data is transmitted between devices on a network:

- Unicast: One-to-one communication between a sender and a receiver.
- Broadcast: Data is sent to all devices on a network or subnet simultaneously.
- Multicast: Data is sent from one device to a specific group within a network.
- Loopback: A device sends data to itself.
- Anycast: Data is sent to a group of devices, but only the nearest node in terms of routing processes the request.
- Geocast: Similar to multicast but restricted to a specific geographic area.
- Peer-to-Peer: Direct communication between two devices with a defined network path.
- Point-to-Multipoint: A single sender transmits data to multiple specific receivers over a common channel.

## What is an IP Address?

An IP address is a unique number assigned to each device connected to a network using the IP protocol. It identifies the device and its location within the network. IP addresses can be assigned statically (never changes automatically) or dynamically (changes automatically based on context). No two devices on a network can have the same IP address.

Two IP versions exist: IPv4 and IPv6. IPv6 was created because IPv4's address space is too limited to meet current demands.

## What is a Subnet Mask?

Every IP address has two parts: a network section identifying the network and a host section identifying the specific device. The subnet mask defines which portion of the IP address represents the network and which part represents the host.

## Types of IPv4 Addresses

### By Use and Distribution Pattern

- Unicast Addresses: Used for one-to-one communications, common in standard network traffic like web browsing.
- Broadcast Addresses: Send data to all devices on a specific network or subnet.
- Multicast Addresses: Deliver information to a specific group within a network (Range: 224.0.0.0 to 239.255.255.255).
- Loopback Addresses: Used by a device to send messages to itself (Range: 127.0.0.0 to 127.255.255.255).

### By Range and Scope

- Private Addresses: Reserved for internal use and not routable on the internet:
  - Class A: 10.0.0.0/8 (10.0.0.0 to 10.255.255.255)
  - Class B: 172.16.0.0/12 (172.16.0.0 to 172.31.255.255)
  - Class C: 192.168.0.0/16 (192.168.0.0 to 192.168.255.255)
- Experimental and Future Use: Reserved for future applications (Range: 240.0.0.0/4 to 255.255.255.254).
- CGNAT Addresses: Used by ISPs for shared public IPs (Range: 100.64.0.0/10 to 100.127.255.255).
- Public Addresses: Available IP addresses for internet routing:
  - 1.0.0.0 to 9.255.255.255
  - 11.0.0.0 to 172.15.255.255
  - 172.32.0.0 to 192.167.255.255
  - 192.169.0.0 to 223.255.255.255

## What is a MAC Address?

A MAC (Media Access Control) address is a unique identifier assigned to a device's network interface. Although it's hardware-bound, it can be temporarily changed via software, a practice

common in security audits.

## What is a Port?

A port is a communication endpoint allowing applications or services to exchange data over a network. Ports range from 0 to 65535 and are divided into three categories:

- **Well-Known Ports:** 0-1023
- **Registered Ports:** 1024-49151
- **Dynamic/Private Ports:** 49152-65535

## Port table

| Protocolo | Acronimo | # de puerto | Conexión | Encriptación |
|---|---|---|---|---|
| File Transfer Protocol | FTP | 20/21 | TCP | No |
| Secure Shell | SSH | 22 | TCP | Si |
| Secure File Transfer Protocol | SFTP | 22 | TCP | Si |
| Teletype Network | telnet | 23 | TCP | No |
| Simple Mail Transfer Protocol | SMTP | 25 | TCP | No |
| Domain Name System | DNS | 53 | TCP/UDP | No |
| Dynamic Host Configuration Protocol | DHCP | 67/68 | UDP | No |
| Trivial File Transfer Protocol | TFTP | 69 | UDP | No |
| Hypertext Transfer Protocol | HTTP | 80 | TCP | No |
| Post Office Protocol v3 | POP3 | 110 | TCP | No |
| Network Time Protocol | NTP | 123 | UDP | No |
| Internet Message Access Protocol | IMAP | 143 | TCP | No |
| Simple Network Managemente Protocol | SNMP | 161/162 | UDP | No |
| Lightweight Directory Access Protocol | IDAP | 389 | TCP/UDP | No |
| Hypertext Transfer Protocol Secure | HTTPS | 443 | TCP | Si |
| Server Message Block | SMB | 445 | TCP | No |
| System Logging | SYSLOG | 514 | UDP | No |
| Simple Mail Transfer Protocol over TLS | SMTPS | 587 | TCP | Si |
| LDAP over SSL | IDAPS | 636 | TCP/UDP | Si |
| POP3 over SSl | POP3S | 995 | TCP | Si |
| IMAP over SSL | IMAPS | 995 | TCP | Si |
| Structured Query Language Server | SQL | 1433 | TCP | No |
| SQLnet (Oracle Network Service) | SQLNet | 1521 | TCP | No |
| MySQL | MySQL | 3306 | TCP | No |
| Remote Desktop Protocol | RDP | 3389 | TCP/UDP | Si |
| Session Initiation Protocol | SIP | 5060/5061 | TCP/UDP | No |

## What is a Service?

A service is a function provided by a device to other devices on the same network or the internet, like file sharing, printing, email, databases, remote administration, and web access.

## What is a Protocol?

A network protocol defines the format and order of message exchange between two or more entities and the actions taken during message transmission and reception.

## OSI Model

The Open Systems Interconnection (OSI) model is a conceptual framework created by the International Organization for Standardization (ISO) to standardize communication protocols across different systems.

## Why is the OSI Model Important?

Although the modern internet doesn't strictly follow the OSI model, it remains a valuable tool for troubleshooting network issues by isolating problems to specific layers.

## OSI Model Layers

The OSI model consists of seven layers:

### 7. Application Layer

The only layer that directly interacts with user data. It supports application services like web browsers and email clients, handling protocols and data manipulation necessary for user-friendly data presentation.

### 6. Presentation Layer

Prepares data for the application layer by translating, encrypting, and compressing it. It ensures data is in a readable format for applications and can decode encrypted messages.

### 5. Session Layer

Manages the opening and closing of communication sessions between two devices. It keeps sessions open long enough to exchange all necessary data and closes them to conserve resources when the exchange is complete.

### 4. Transport Layer

Ensures end-to-end communication between devices. It breaks session layer data into segments, reassembles them on the receiving end, and manages flow control and error correction.

### 3. Network Layer

Responsible for transferring data between different networks. It divides transport layer segments into packets and finds the optimal physical path for data delivery, a process known as

routing.

### 2. Data Link Layer

Facilitates data transfer between two devices within the same network. It breaks down network layer packets into smaller units called frames and handles flow and error control.

### 1. Physical Layer

This layer includes the physical equipment involved in data transfer, such as cables and network switches. It's where data is converted into a sequence of bits.

## TCP/IP Model

The TCP/IP model is the de facto standard for computer network communication worldwide. It is a suite of network protocols that define requirements for safe and efficient data transfer.

### Key Features

- Device Compatibility: As a standard, most modern devices and operating systems are designed to be compatible with this model, facilitating cross-vendor communication.
- Interoperability: Allows different operating systems to communicate using the same set of TCP/IP protocols.
- Flexibility: Supports a wide range of applications and services, providing a solid foundation for web browsing, video streaming, and file transfer.
- Reliability and Error Control: Offers multiple mechanisms to ensure reliable data delivery, including segment numbering and tracking to guarantee complete data transmission.

## TCP/IP Model Layers

The TCP/IP model consists of four layers:

### Application Layer

Handles interaction between applications and the network. Protocols in this layer establish the rules and formats needed for effective information exchange between applications.

### Transport Layer

Manages end-to-end connections and ensures reliable data delivery.

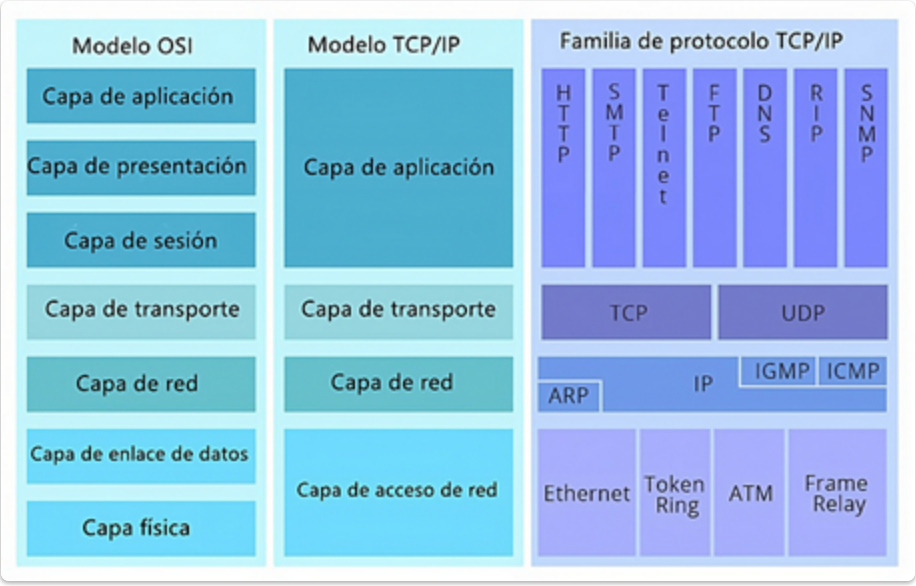
### Internet Layer

Responsible for routing data packets across the network and assembling/disassembling data for transmission.

### Network Access Layer

Handles the physical transmission of data over a network medium like Ethernet, Wi-Fi, or fiber optics.

## Distribution of protocols




## Protocol Distribution

### Application Layer Protocols

- HTTP/HTTPS: Hypertext Transfer Protocol and its secure version manage client-server communications for web content.
- SMTP: Simple Mail Transfer Protocol, used for sending and receiving email messages over the internet.
- SSH: Secure Shell, a remote administration protocol allowing users to control and modify servers over the internet.
- FTP: File Transfer Protocol, used for transferring files between networked devices.
- DNS: Domain Name System, translates human-readable domain names into machine-readable IP addresses.
- DHCP: Dynamic Host Configuration Protocol, assigns IP addresses to new devices on a network.
- RIP: Routing Information Protocol, manages router information within a contained network.
- SNMP: Simple Network Management Protocol, designed for managing information transfer in networks, especially LANs.

### Transport Layer Protocols

- TCP: Transmission Control Protocol, a reliable, connection-oriented communication standard ensuring accurate data delivery.
- UDP: User Datagram Protocol, a fast, connectionless protocol used for time-sensitive transmissions.

### Internet Layer Protocols

- IP: Internet Protocol, governs the format of data sent over the internet or local network.
- ARP: Address Resolution Protocol, dynamically converts internet addresses to unique local network hardware addresses.
- IGMP: Internet Group Management Protocol, enables multiple devices to share an IP address and receive the same data.
- ICMP: Internet Control Message Protocol, provides standardized mechanisms for network devices to communicate crucial information like connectivity and network status.

### Network Access Layer Protocols

- Ethernet: Allows devices to exchange data packets over a network.
- Frame Relay: A packet-switching technology used in WANs for efficient and reliable data transmission.

## What is TTL?

Time To Live (TTL) limits the lifespan or number of hops a packet can make in a network before being discarded. This prevents packets from circulating indefinitely and avoids routing loops.

## Connection Establishment Mechanisms

These processes and protocols initiate communication sessions between two network points. They negotiate parameters to start and secure data transmission:

- TCP Handshake: Also known as the Three-Way Handshake, this ensures a reliable connection through three steps: SYN, SYN-ACK, and ACK.
- UDP Communication: Unlike TCP, UDP does not establish a connection beforehand. Datagram packets are sent directly without ensuring delivery, order, or integrity.

## Firewalls

A firewall is a system that enforces access control policies between networks.

### Common Firewall Properties

- Withstand network attacks.

- Serve as the sole transit point between internal corporate and external networks.
- Apply access control policies.

### Firewall Advantages

- Prevent exposure of sensitive hosts, resources, and applications to untrusted users.
- Sanitize protocol flows, preventing exploitation of protocol flaws.
- Block malicious data from servers and clients.
- Simplify security administration.

### Firewall Limitations

- Misconfigured firewalls can become a single point of failure.
- Many application data types cannot be securely transmitted through firewalls.
- Users may bypass firewalls to access blocked material, exposing the network to attacks.
- Network speed can be reduced.
- Unauthorized traffic can be tunneled as legitimate traffic through the firewall.

## Types of Firewalls

### Host-Based Firewall

A security solution installed directly on an individual device, filtering incoming and outgoing network traffic based on predefined rules. Examples include Windows Defender Firewall and Linux iptables.

### Stateless Packet-Filtering Firewall

Part of router firewalls, they approve or deny traffic based on layer 3 and 4 information, using simple policy table lookups.

### Stateful Firewall

The most versatile and commonly used firewall technology. It tracks active connections and uses state tables to make filtering decisions.

### Application Gateway Firewall

Filters information on OSI layers 3, 4, 5, and 7. Most of the filtering is handled through software.

### Next-Generation Firewall (NGFW)

Advanced firewalls providing enhanced capabilities:

- **Deep Packet Inspection (DPI)**: Analyzes packet content beyond headers to detect advanced threats.
- **Intrusion Prevention System (IPS)**: Blocks malicious activities in real time.
- **Application Control**: Identifies and regulates traffic based on specific applications.
- **Cloud-Based Threat Analysis**: Uses external databases to identify emerging attack patterns.
- **User-Based Policies**: Applies security rules based on user identity, not just IP addresses.