PROTOCOL

Imagine you're talking to a friend who speaks a different language. How do you communicate? You need a common language or **set of rules**—that's exactly what network **protocols** do for computers!

Protocols = Rules for communication in networks

Definition of Protocols

A **network protocol** is a well-defined set of rules and conventions that govern communication between devices over a network. These rules cover aspects such as:

- **Data formatting** – How data is structured for transmission.
- **Addressing** – Identifying the sender and receiver.
- **Error handling** – Detecting and correcting errors during transmission.
- **Data transmission speed** – Managing how fast data is sent and received.
- **Security mechanisms** – Ensuring data integrity and confidentiality.

Importance of Protocols in Networking

Protocols play a crucial role in networking by ensuring:

1. **Interoperability** – Devices from different manufacturers can communicate seamlessly using standard protocols.
2. **Reliable Communication** – Protocols like TCP ensure data is delivered accurately and in order.
3. **Data Security** – Encryption and authentication protocols (e.g., SSL/TLS, HTTPS) protect sensitive information.
4. **Efficient Data Transmission** – Protocols optimize bandwidth usage and manage network traffic effectively.
5. **Error Handling and Correction** – Network protocols detect and correct errors to maintain data integrity.
6. **Scalability** – Internet-wide protocols allow global communication across millions of devices.

TCP/IP Model: A Detailed Overview

Brief History & Purpose

The **TCP/IP model** (Transmission Control Protocol/Internet Protocol) was developed in the 1970s by the **U.S. Department of Defense (DoD)** as part of the ARPANET project. It was designed to enable **robust, scalable, and cross-platform**

communication between computers over networks, which later became the **foundation of the modern internet**.

🔷 **Why was TCP/IP created?**

- To create a **universal networking standard** for different devices.
- To ensure **data delivery across unreliable networks**.
- To support **scalability** for global internet communication.

🔷 **Key Features:**

✔️ Connection-oriented and connectionless communication (TCP & UDP).

✔️ Standardized addressing via IP.

✔️ Reliable error handling and retransmission.

✔️ Supports interoperability across different hardware and software.

Layers of the TCP/IP Model

Unlike the **OSI model**, which has 7 layers, the **TCP/IP model has only 4 layers**, combining some OSI layers for simplicity.

TCP/IP Layer	Equivalent OSI Layers	Purpose
Application	Application, Presentation, Session	Handles user-level protocols like web browsing, file transfers, and email.
Transport	Transport	Ensures end-to-end communication using TCP/UDP.
Internet	Network	Provides logical addressing and routing using IP, ICMP, and ARP.
Network Access	Data Link, Physical	Deals with physical transmission, MAC addressing, and network interfaces.

---

1. Application Layer (User Interaction Layer)

🔷 The **topmost layer**, handling application-specific protocols that interact with users.

🔷 This is where web browsers, email clients, and file transfer tools operate.

Common Protocols in the Application Layer:

Protocol	Purpose
HTTP (HyperText Transfer Protocol)	Enables web browsing & communication between web servers and browsers.
FTP (File Transfer Protocol)	Transfers files between systems over a network.
SMTP (Simple Mail Transfer Protocol)	Sends emails between mail servers.
DNS (Domain Name System)	Resolves domain names (e.g., google.com) to IP addresses.
Telnet	Allows remote login to another computer over a network.

Example: When you open a website (`https://example.com`), your browser sends an **HTTP request** to the server, which responds with a **webpage**.

---

2. Transport Layer (Reliable Data Transmission Layer)

🔷 Ensures **end-to-end communication** between devices, handling error detection, retransmissions, and flow control.

🔷 Uses two main protocols:

Protocol	Type	Purpose
TCP (Transmission Control Protocol)	Connection-oriented	Ensures reliable, ordered, and error-free data delivery (used in web browsing, email, file transfer).
UDP (User Datagram Protocol)	Connectionless	Faster, but unreliable. Used in video streaming, VoIP, and gaming where speed is more important than accuracy.

📌 **Example:**

- Watching a YouTube video? **UDP** is used (speed > reliability).
- Downloading a file? **TCP** ensures all parts arrive correctly.

---

3. Internet Layer (Routing & Addressing Layer)

🔷 Handles **logical addressing, routing, and packet forwarding** to ensure data reaches the correct destination.

🔷 Uses **IP addresses** to identify devices across networks.

Key Protocols in the Internet Layer:

Protocol	Purpose
IP (Internet Protocol)	Assigns unique addresses & routes packets.
ICMP (Internet Control Message Protocol)	Used for network diagnostics (`ping` command).
ARP (Address Resolution Protocol)	Translates IP addresses to MAC addresses for local communication.

Example:

When you **send an email**, the email's data packets travel across multiple routers. Each router uses **IP addresses** to forward the packets to the correct location.

---

4. Network Access Layer (Physical Connection Layer)

🔷 Handles **actual data transmission** over the physical network (wired or wireless).

🔷 Defines **MAC (Media Access Control) addresses** for devices within a local network.

Key Technologies in the Network Access Layer:

Technology	Purpose
Ethernet	Wired networking standard for LANs.
Wi-Fi (802.11)	Wireless network standard.
MAC (Media Access Control) Address	Unique physical address of a device's network interface.

Example:

When you **connect to a Wi-Fi network**, your device's **MAC address** is used to communicate with the router, which then assigns an **IP address** for internet access.

Comparison: TCP/IP Model vs. OSI Model (Optional)

Feature	TCP/IP Model	OSI Model
Number of Layers	4	7
Development	Based on real-world networking	Theoretical model
Usage	Used in real-world networks like the internet	Used for conceptual understanding
Application Layer	Combines Application, Presentation, and Session layers	Separate layers for each function
Reliability	Designed for scalability & flexibility	More detailed structure but less practical

Example:

TCP/IP is like **a working car** (real-world, practical), while OSI is like **a detailed blueprint** (structured but theoretical).

Wrap-Up: Why Learn TCP/IP?

✔️ **Foundation of the internet** – Everything from web browsing to video streaming uses TCP/IP.

✔️ **Universal standard** – Works across different hardware and operating systems.

✔️ **Practical & real-world** – Unlike OSI, it's actually used in modern networking.

✔️ **Scalable & flexible** – Can handle networks of any size, from small offices to the entire internet.

🛠️ **Want to see TCP/IP in action?** Try using:

- `ping` (ICMP) – To check network connectivity.
- `traceroute` – To see how packets travel through networks.
- `netstat` – To view active network connections.

What is MAC (Medium Access Control)?

MAC (**Medium Access Control**) is a **sub-layer** of the Data Link Layer in networking that controls **how devices access the network and transmit data** without interference.

Role of MAC in Networking

MAC ensures **orderly and efficient communication** by managing:

✅ **Who gets to send data** and when.

✅ **Avoiding collisions** when multiple devices want to send data at the same time.

✅ **Ensuring data reaches the correct device** using unique MAC addresses.

🔷 **Real-Life Analogy:** Imagine a roundabout with multiple cars. **Traffic lights (MAC)** control when each car (device) can enter, avoiding crashes (collisions).

CSMA/CD

CSMA/CD is a **network access method** used in Ethernet to manage how devices share a network without collisions. It allows multiple devices to transmit data efficiently **while handling collisions** when they occur.

🔷 **Real-Life Analogy:** Imagine a group of people talking on a conference call. They **listen before speaking** (Carrier Sense), but if two people talk at the same time (Collision), they **pause and retry** after a short delay.

How CSMA/CD Works?

1️⃣ **Carrier Sense (CS)**: A device **listens** to check if the network is free before transmitting.

2️⃣ **Multiple Access (MA)**: Many devices share the same network cable or wireless channel.

3️⃣ **Transmission**: If the channel is free, the device starts sending data.

4️⃣ **Collision Detection (CD)**: If two devices transmit at the same time, a **collision occurs** and corrupts the data.

5️⃣ **Jam Signal & Backoff**: The network sends a **jam signal** to notify all devices of the collision.

6️⃣ **Random Retry**: Each device waits for a **random time** (backoff period) before trying again.

🔷 **Example:** If two computers on an Ethernet network (PC A and PC B) try to send data at the same time, a **collision** happens. Both computers detect it, stop sending, wait for a random time, then **retry transmission**.

Token RING passing

Token Ring is a **networking protocol** that allows devices to communicate in a **controlled manner** using a **token-based system**. Instead of all devices trying to

send data at the same time (like in Ethernet), a **special data packet called a "token" circulates** in the network. Only the device holding the token can **transmit data**, preventing collisions.

Real-Life Analogy:

Imagine a **group discussion** where only the person **holding a microphone** can speak. Everyone else must wait for their turn until they get the microphone.

How Token Ring Works?

Token Ring networks follow a **ring topology**, where each device is connected in a **circular manner**. The data **flows in one direction** (either clockwise or counterclockwise).

🔷 Step-by-Step Working of Token Ring

1️⃣ **Token Circulation:**

- A special small data packet called a **token** keeps moving around the ring.
- The token acts like **a permission slip** for sending data.

2️⃣ **Data Transmission:**

- If a device **needs to send data**, it **grabs the token**, modifies it, and attaches its message.
- The token now carries the **destination address and data**.

3️⃣ **Message Delivery:**

- The token moves from one device to another.
- When it reaches the **destination device**, it **reads the message** and sends an acknowledgment.

4️⃣ **Token Release:**

- Once the message is delivered, the receiver **marks the token as "free"** and releases it back into the network.

Remote Login: Telnet Explained

What is Telnet?

Telnet (**Teletype Network**) is a **remote login protocol** that allows users to access and control another computer over a network. It uses **port 23** and operates in a **command-line interface (CLI)**.

🔷 **How It Works:**

1️⃣ You **connect** to a remote computer using Telnet.

2️⃣ Telnet **establishes a session** and provides a CLI to execute commands.

3️⃣ You can **control the remote machine** just like you're using it locally.

Example:

A system admin logs into a remote Linux server using Telnet to restart a service.

🛡️ Telnet vs. SSH: Security Concerns

Feature	**Telnet**	**SSH**
Encryption	❌ No encryption (Plaintext)	✅ Fully encrypted
Security	❌ Data, including passwords, is sent in clear text	✅ Secure, prevents eavesdropping
Port	23	22
Usage	❌ Not recommended for sensitive data	✅ Preferred for secure remote access

Security Risk: Telnet sends everything **in plaintext**, making it vulnerable to **man-in-the-middle attacks**. **SSH is the secure alternative**.

ISP & NSP: Understanding Internet Connectivity

When you browse the internet, stream videos, or send emails, you're relying on **ISPs (Internet Service Providers)** and **NSPs (Network Service Providers)** to deliver data between your device and the global internet. Let's break it down!

What is an ISP (Internet Service Provider)?

An **ISP (Internet Service Provider)** is a company that provides **internet access to users**. It connects homes, businesses, and organizations to the internet through various technologies like **fiber optics, DSL, cable, satellite, and mobile networks**.

Role of ISPs

✔️ Provide internet access to homes, businesses, and organizations.

✔️ Offer services like **email hosting, web hosting, and VoIP**.

✔️ Assign **IP addresses** to users.

✔️ Ensure **data reaches the correct destination** by routing traffic.

🔷 **Real-Life Analogy:**

Think of an ISP as your **local water supplier**. Just like they provide water pipelines to your home, ISPs provide **internet pipelines** to connect you to the web.

📊 Types of ISPs

🌍 Tier 1 ISPs (Global Backbone Providers)

- These are the **top-level ISPs** that form the **core of the internet**.

- They own and operate **large-scale, high-speed fiber networks**.
- Connect directly with other Tier 1 ISPs through **peering agreements**.

📌 **Examples:** AT&T, Tata Communications, CenturyLink, NTT Communications.

🔷 **Real-Life Analogy:**

Tier 1 ISPs are like **highways** that connect entire countries and continents.

🌆 Tier 2 ISPs (Regional Providers)

- Purchase internet bandwidth from **Tier 1 ISPs**.
- Provide services to **businesses and local ISPs**.
- Operate at a **national or regional level**.

📌 **Examples:** Airtel, Comcast, Vodafone.

🔷 **Real-Life Analogy:**

Tier 2 ISPs are like **state highways**, connecting smaller cities to the main highways (Tier 1 ISPs).

🏠 Tier 3 ISPs (Local Providers)

- Buy bandwidth from **Tier 2 ISPs** and **sell it to end users**.
- Provide internet to **homes, offices, and small businesses**.
- Offer **customer support and last-mile connectivity**.

📌 **Examples:** Local cable or broadband providers like JioFiber, BSNL, and Spectrum.

🔷 **Real-Life Analogy:**

Tier 3 ISPs are like **city roads** that bring internet directly to homes and offices.

📌 What is an NSP (Network Service Provider)?

An **NSP (Network Service Provider)** is a company that provides **high-speed internet backbone connections** to ISPs, large businesses, and government organizations.

🛠️ Role of NSPs

✔️ **Own and manage backbone networks** (large fiber optic cables).

✔️ **Provide high-capacity data transport** between ISPs.

✔️ Use **undersea cables and satellite links** to connect continents.

✔️ Ensure **global internet connectivity** by routing traffic efficiently.

📌 **Examples of NSPs:**

- Tata Communications
- AT&T

- NTT Communications
- Verizon

🔷 **Real-Life Analogy:**

If ISPs are roads, NSPs are **railway networks** that move large amounts of data between cities and countries.

📊 ISP vs. NSP – Key Differences

Feature	ISP (Internet Service Provider)	NSP (Network Service Provider)
Function	Provides internet to end users	Provides internet backbone to ISPs
Customer Base	Homes, businesses, local ISPs	Large ISPs, enterprises, governments
Ownership	Regional networks	Global fiber-optic networks
Examples	Jio, Airtel, Comcast, BSNL	Tata Communications, AT&T, NTT