1. TCP (Transmission Control Protocol)

TCP is a reliable, **connection-oriented protocol** that operates at the **transport layer** of the TCP/IP model. It facilitates the accurate and ordered transmission of data between two systems over a network, ensuring error recovery and flow control.

Working

- **Three-way handshake** establishes a connection:
    - SYN → SYN-ACK → ACK.
- Data is broken into **segments**, each with a **sequence number** and **checksum** for integrity.
- Receiver acknowledges receipt of each segment; missing data is **retransmitted**.
- TCP implements **flow control** using a sliding window and **congestion control** (e.g., slow start, congestion avoidance).
- Connection termination is handled via a **four-step FIN handshake**.

Key Features

- Reliable transmission
- Ordered data delivery
- Error detection and correction
- Full-duplex communication

Advantages

- Guarantees packet delivery and order.
- Reliable for large file transfers and transactional data.

Disadvantages

- More overhead due to acknowledgments and handshakes.
- Higher latency compared to UDP.

Real-Life Use Cases

- Browsing (HTTP/HTTPS)
- Email (SMTP, IMAP, POP3)
- Remote login (SSH)
- Secure file transfers (SFTP, FTPS)

Related Protocols & Technologies

- FTP, SMTP, HTTPS, Telnet
- Operates over IP (Internet Layer)

2. UDP (User Datagram Protocol)

UDP is a **lightweight, connectionless transport layer protocol** designed for applications where speed is critical and occasional data loss is acceptable.

Working

- No session establishment , packets are sent independently.
- Each datagram includes source/destination ports and a checksum.
- No built-in mechanisms for packet sequencing, retransmission, or acknowledgment.
- Receiver processes whatever datagrams arrive , **best-effort delivery**.

Key Features

- Stateless communication
- Minimal latency
- Suitable for multicast and broadcast transmissions

Advantages

- Low overhead, faster than TCP.
- Ideal for real-time or broadcast/multicast applications.

Disadvantages

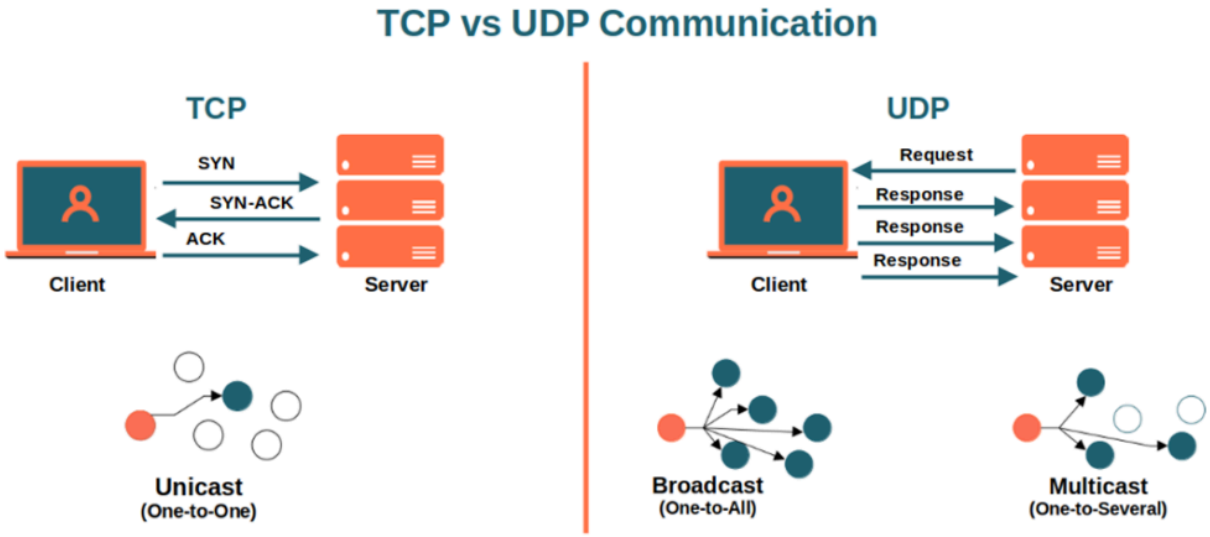
- No guarantee of delivery or order.
- Not suitable for applications needing complete reliability.

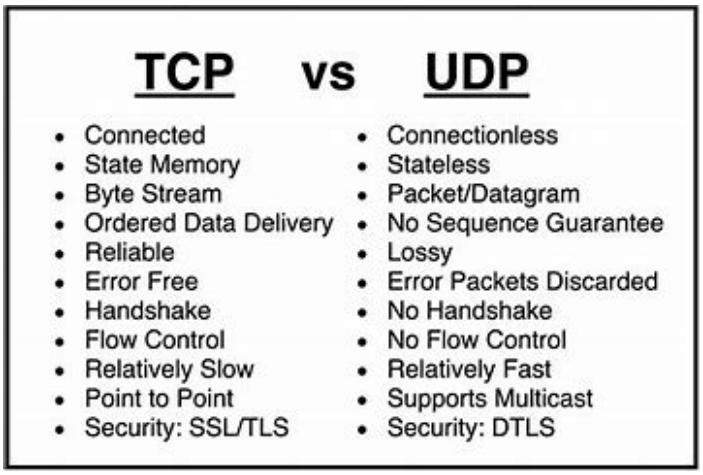
Real-Life Use Cases

- VoIP calls (Skype, Zoom)
- Video streaming (Netflix, YouTube Live)
- Online multiplayer games
- DNS queries (fast lookup)

Related Protocols & Technologies

- RTP, TFTP, SNMP, DHCP, DNS
- Often encapsulated in application protocols for streaming





3. HTTP (Hypertext Transfer Protocol)

HTTP is an **application layer protocol** that enables communication between web clients and servers. It's the foundation of data exchange on the World Wide Web, following a **stateless, request-response architecture.**

Working

- Client sends an HTTP request (GET, POST, PUT, DELETE) to the server.
- Server responds with an HTTP response, including headers, status codes, and content (HTML, JSON, etc.).
- Communication typically happens over TCP port 80.
- Each request is independent , state management is handled using cookies, sessions, or tokens.

Key Features

- Text-based and human-readable
- Supports various methods (GET, POST, etc.)
- Stateless by default

Advantages

- Simple to implement and use
- Widely supported across platforms and tools

Disadvantages

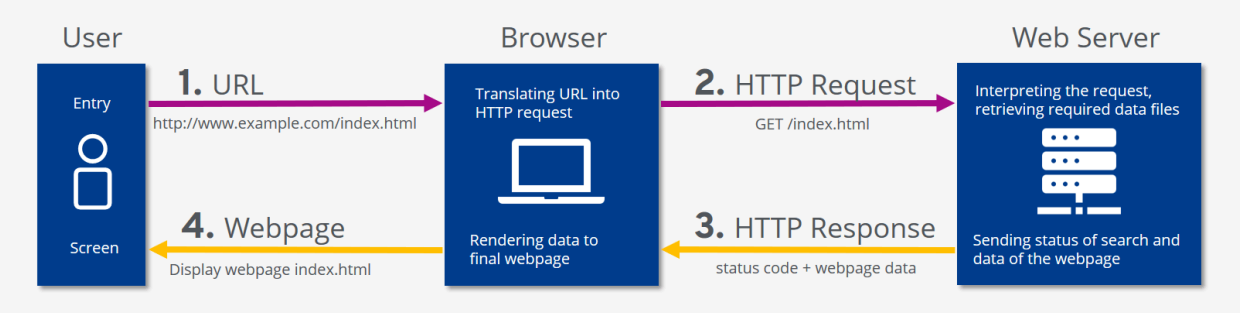
- Lacks built-in security (data sent in plaintext)
- Stateless nature can be inefficient for certain applications

Real-Life Use Cases

- Browsing websites
- REST APIs for web/mobile apps
- Non-secure online services

Related Protocols & Technologies

- HTML, CSS, JavaScript, JSON
- TCP/IP



4. HTTPS (Hypertext Transfer Protocol Secure)

HTTPS is the **secure variant of HTTP**, combining it with **SSL/TLS encryption** to ensure confidentiality, integrity, and authentication of data between web servers and clients.

Working

- Initiates a **TLS handshake**, exchanging public keys and agreeing on session encryption.
- Data is transmitted over an encrypted TCP connection.
- Server identity is verified using an X.509 certificate issued by a Certificate Authority (CA).
- Runs over TCP port 443.

Key Features

- End-to-end encryption
- Authentication via digital certificates
- Integrity verification via message authentication codes

Advantages

- Prevents man-in-the-middle (MITM) attacks and eavesdropping
- Boosts user trust and SEO rankings
- Protects login credentials, banking data, etc.

Disadvantages

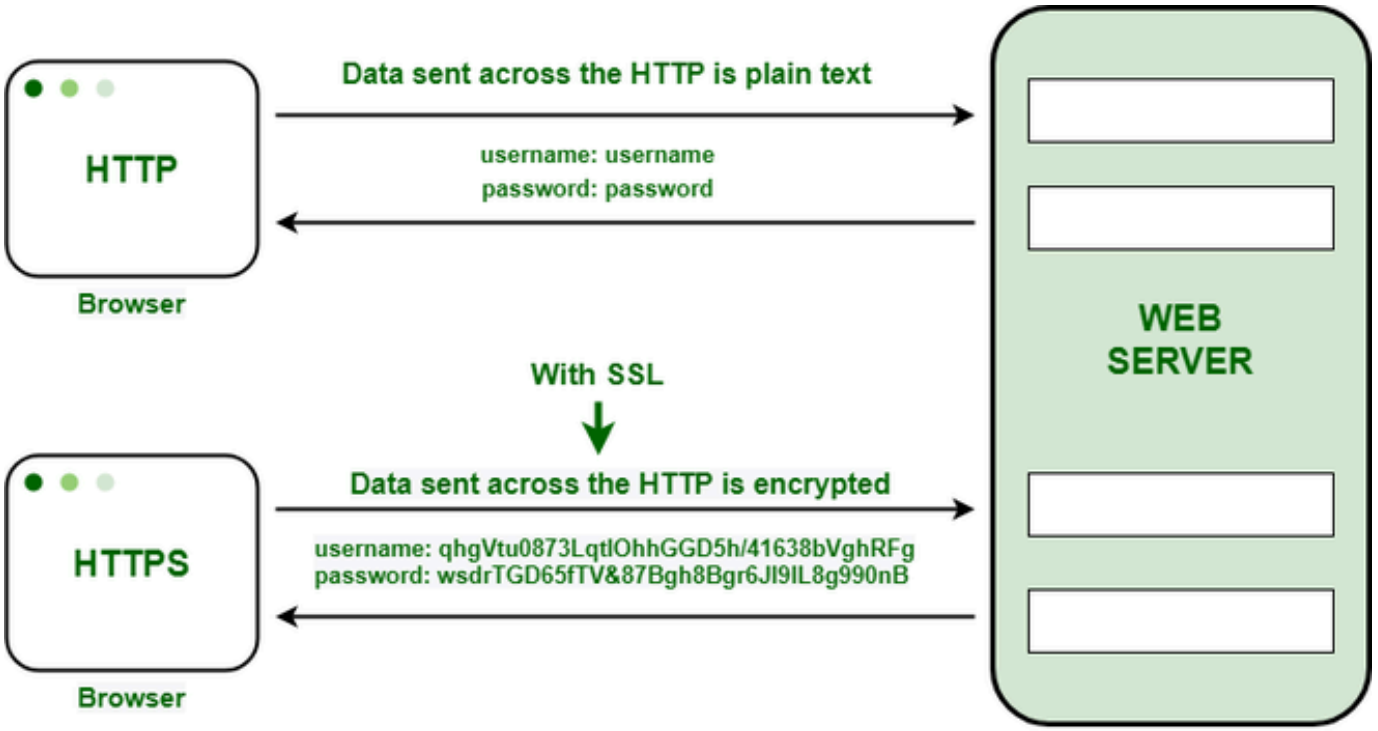
- Slight performance overhead due to encryption
- Requirs certificate management

Real-Life Use Cases

- Banking, e-commerce, secure portals
- Login and registration systems
- OAuth & federated authentication systems

Related Protocols & Technologies

- TLS 1.2/1.3, RSA, ECC, AES
- PKI, OpenSSL, Let's Encrypt



5. ICMP (Internet Control Message Protocol)

ICMP is a **supporting protocol at the Internet Layer** used for **network diagnostics**, **error reporting**, and **status checking**. It's not used for data transmission but to relay control messages.

Working

- Operates within IP, without using transport layer ports.
- Sends control messages in response to IP operations.
- Key message types:
- Echo request/reply (used by **ping**)
- Destination unreachable
- Time exceeded (used by **traceroute**)
- Helps determine path health and failure points in the network.

Key Features

- No session or state management
- Provides network feedback
- Helps monitor and manage network infrastructure

Advantages

- Useful for real-time diagnostics and troubleshooting
- No application layer dependency

Disadvantages

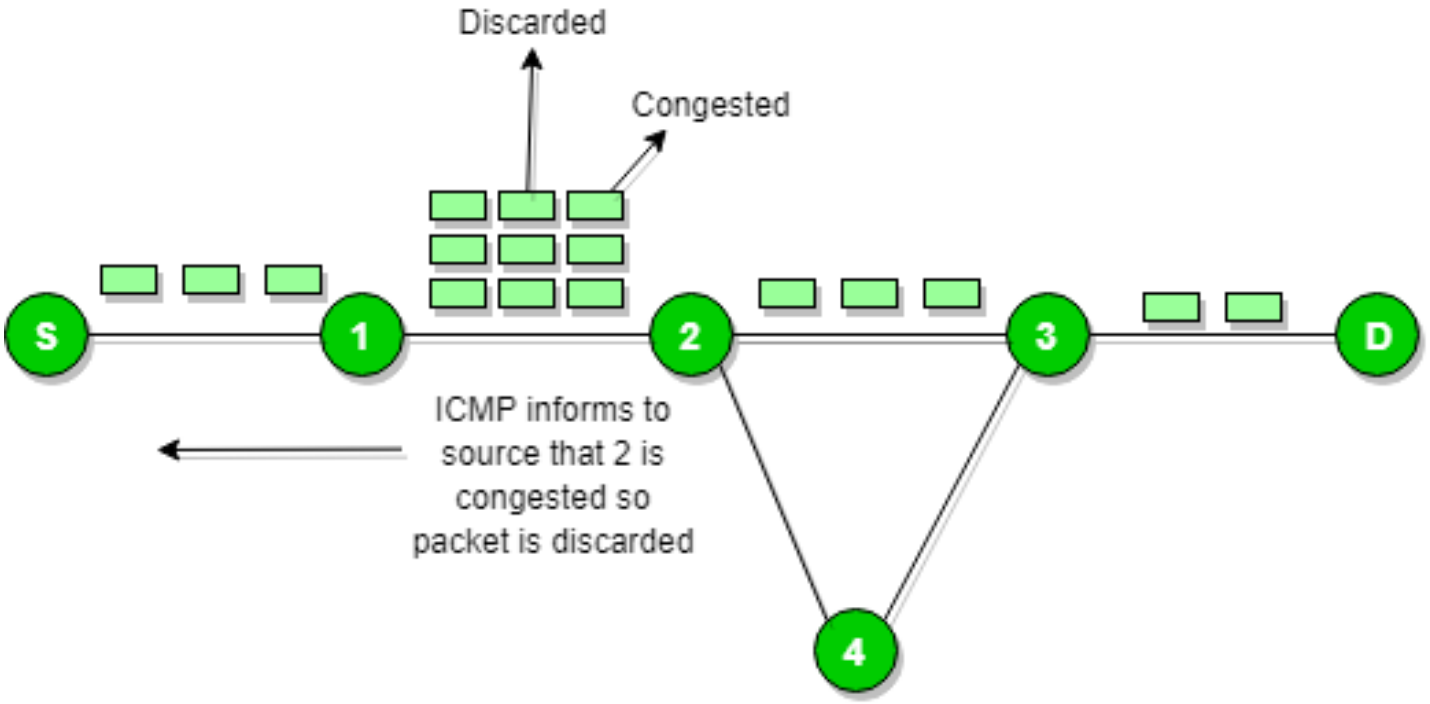
- Can be misused in DDoS attacks (e.g., ICMP flood)
- Often filtered by firewalls for security

Real-Life Use Cases

- Network troubleshooting with **ping, traceroute**
- Detecting network outages
- Identifying unreachable gateways or hosts

Related Protocols & Technologies

- IPv4, IPv6
- Ping, Traceroute tools
- NMAP and other network scanners



Comparison Table

Protocol	OSI Layer	Reliability	Security	Connection	Key Use
TCP	Transport	High	None	Connection-oriented	File transfer, Email
UDP	Transport	Low	None	Connectionless	Streaming, Gaming
HTTP	Application	Moderate	None	Stateless	Browsing, APIs
HTTPS	Application	High	Encrypted	Stateless	Secure web access
ICMP	Network	N/A	None	N/A	Diagnostics, Control