# 5. Computer Networks

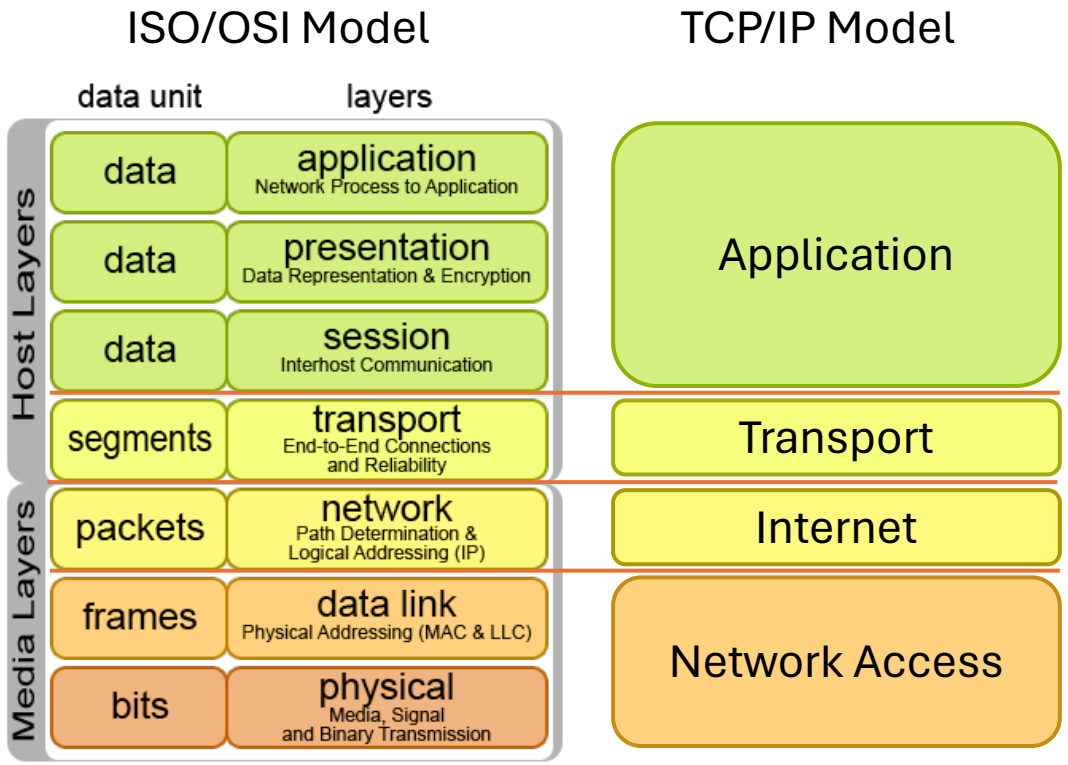
TCP/IP Model

# Summary

- ISO/OSI Model vs TCP/IP Model
- Application Layer
- DNS - HTTP - FTP – SMTP/POP3/IMAP - DHCP
- Transport Layer
- TCP - UDP
- Internet Layer
- ICMP - ARP
- Network Access Layer

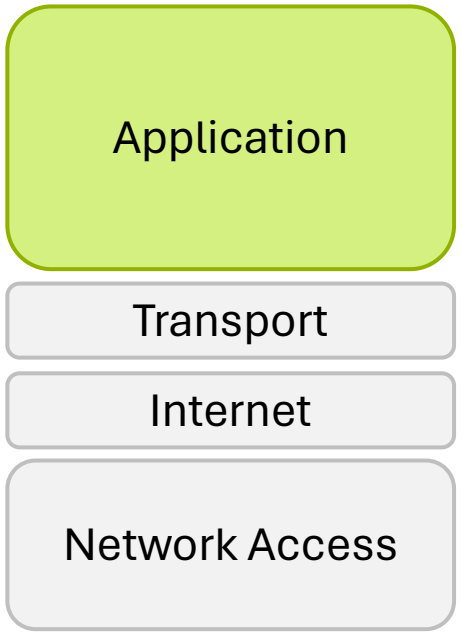
# ISO/OSI Model vs TCP/IP Model

The **TCP/IP model** is a concise framework used to standardize and ensure reliable data communication across diverse interconnected networks, including the **internet**. It consists of **four layers**, each responsible for specific functions in the process of data transmission. The TCP/IP model is the **standard de facto** for internet and network communication, widely adopted due to its robustness and flexibility.




ICTAcademy
INFORMATION AND COMMUNICATIONS TECHNOLOGY

# Application Layer




**Functions:**

Provides network services directly to user applications.

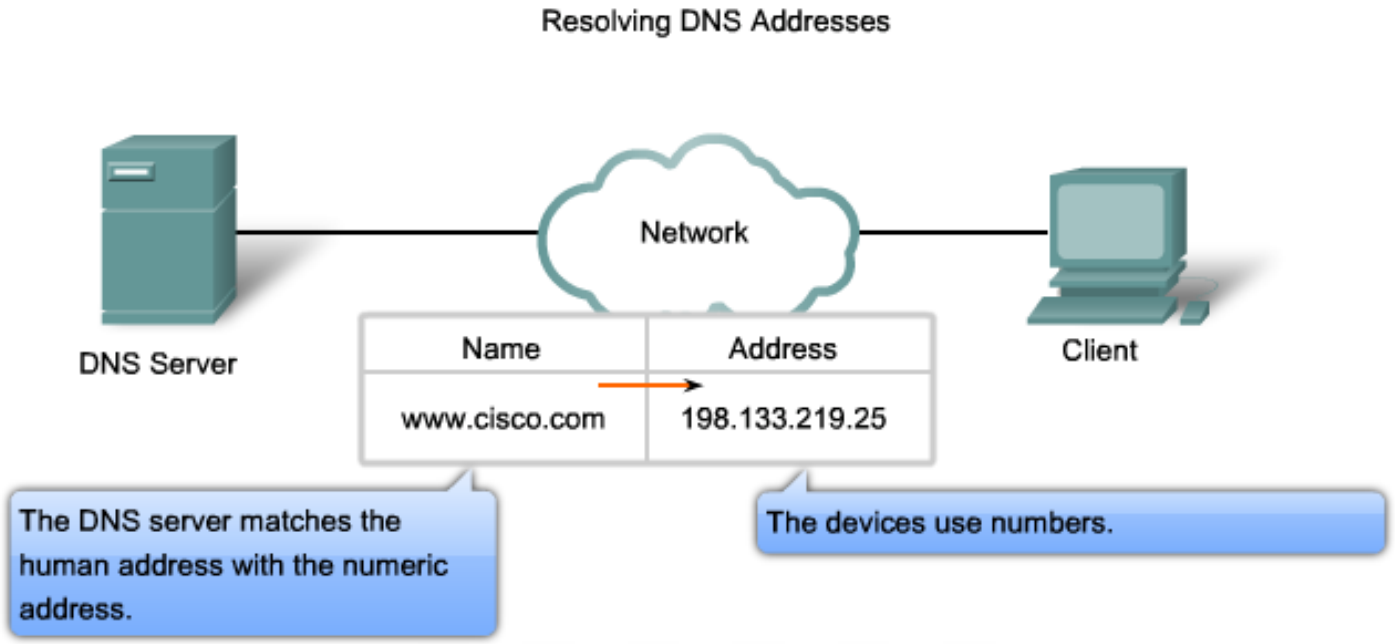
Manages application-level protocols.

**Protocols:**

- **DNS:** Domain name resolution
- **HTTP/HTTPS:** Web browsing
- **FTP:** File transfer
- **SMTP/POP3/IMAP:** Email
- **DHCP:** Management of IP addresses allocation

# Domain Name System (DNS)

The **Domain Name System** (**DNS**) is a hierarchical and decentralized naming system used to **resolve** human-readable **domain names** (like www.cisco.com) into machine-readable **IP addresses** (like 198.133.219.25).



# Domain Name System (DNS) – How it works

DNS is a critical component of the internet, enabling the translation of human-readable domain names into IP addresses.

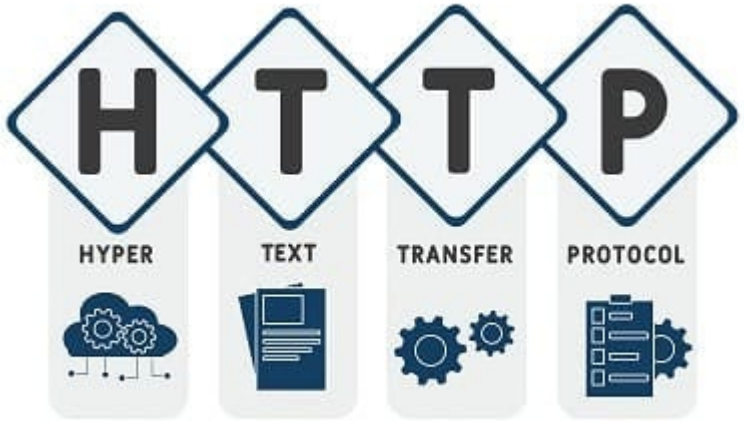
1. **DNS Query:** The process begins when a user types a domain name into a web browser.
2. **Recursive Resolver:** The query is sent to a DNS resolver, which starts the resolution process.
3. **Root Server:** The resolver queries a root server to find the top-level domain (TLD) server (e.g., .com, .org).
4. **TLD Server:** The resolver then queries the TLD server to find the authoritative DNS server for the specific domain.
5. **Authoritative DNS Server:** The authoritative server provides the IP address associated with the domain name.
6. **Response:** The resolver returns the IP address to the user's browser, which then connects to the web server.

# HyperText Transfer Protocol (HTTP)

The **HyperText Transfer Protocol** (**HTTP**) facilitates the **transfer** of **hypertext documents**, such as HTML pages, between a **web server** and a **client** (browser).

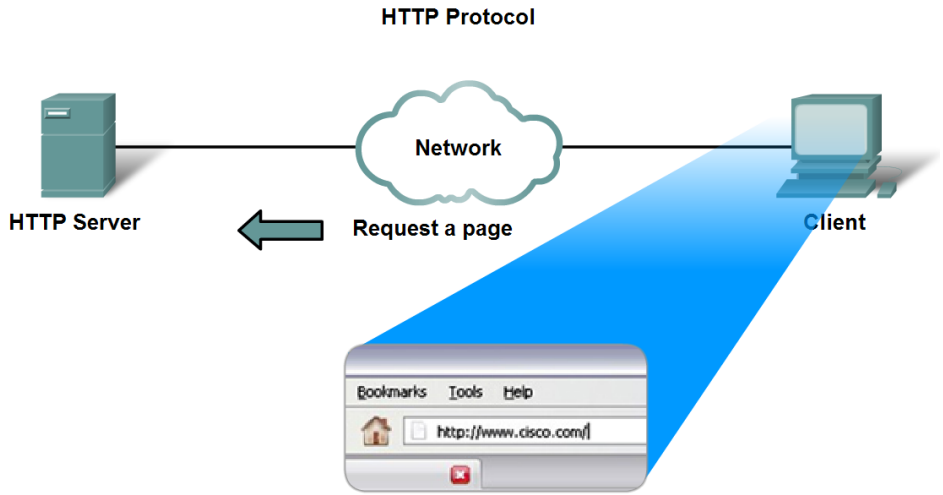
## What is HTTPS?

**HyperText Transfer Protocol Secure** (**HTTPS**) is an extension of HTTP with added **security features**. It provides secure communication over a computer network by **encrypting** the data exchanged between the client and server.




# HTTP – Web Browsing Process

1. **Entering the URL:** The user types a URL into the browser's address bar.
2. **DNS Resolution:** The browser queries a DNS server to resolve the URL to an IP address.
3. **Server Connection:** The browser establishes a connection to the identified server.
4. **Sending a Request:** Using HTTP or HTTPS, the browser sends a GET request to the server, typically requesting the default document (e.g., index.html).
5. **Receiving the Response:** The server responds by sending the HTML content of the requested webpage to the browser.
6. **Rendering the Page:** The browser interprets the HTML code and displays the formatted webpage in the browser window.



# File Transfer Protocol (FTP)

The **File Transfer Protocol** (**FTP**) is a standard network protocol used for **transferring files** from one host to another over a TCP-based network, such as the internet. It facilitates the transfer of files between a **client** and a **server**.

1. **Connection Establishment:**

*Control Connection:* Client establishes a control connection to the server for sending commands.

*Data Connection:* A separate data connection is established for transferring files, which can use various ports.

2. **Authentication:**

*Username and Password:* The client provides specific credentials to authenticate with the server when accessing protected files. For publicly available files, the default username is 'anonymous' and the password is typically set to 'guest'.

3. **File Transfer:**

*Commands:* Client sends commands (e.g., RETR, STOR) over the control connection.

*Data Transfer:* Files are transferred over the data connection.

# SMTP/POP3/IMAP – Email

## What is SMTP?

The **Simple Mail Transfer Protocol** (**SMTP**) is a protocol used for **sending emails** from a client to a server or between servers.

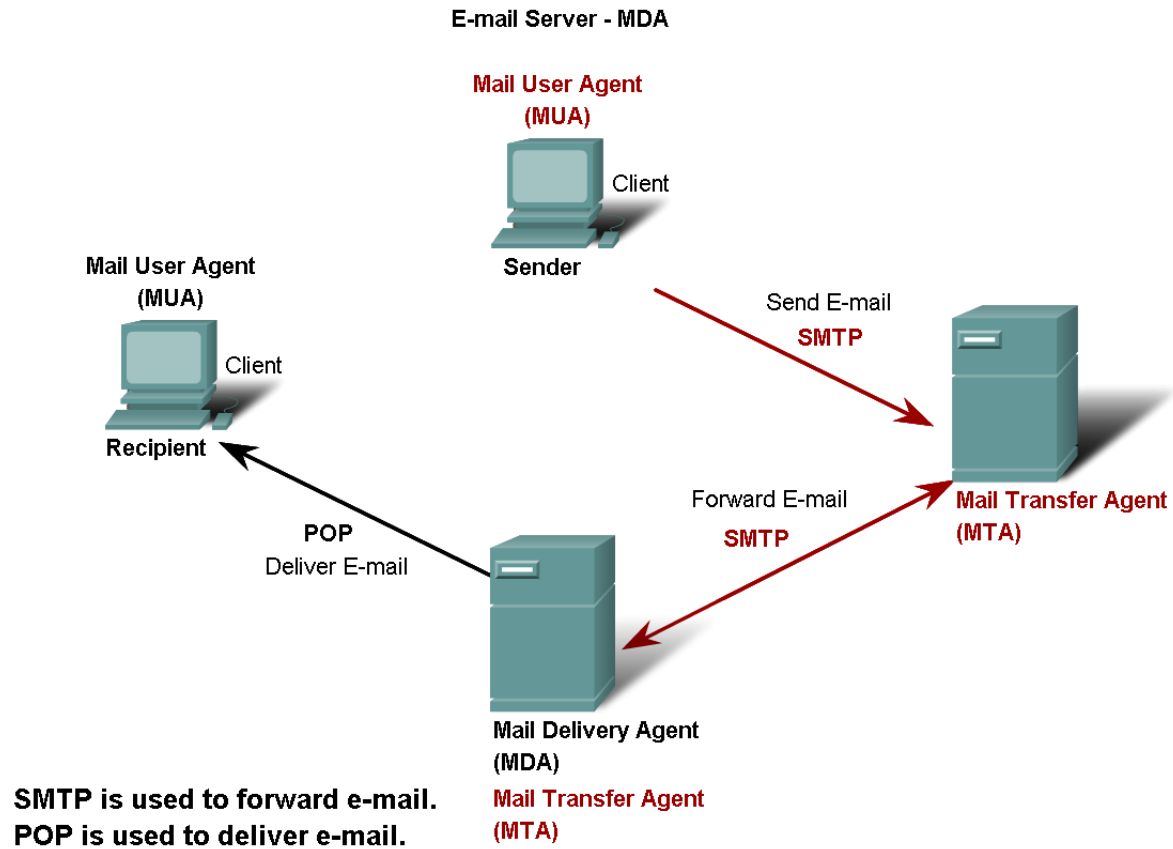
## What is POP3?

The **Post Office Protocol version 3** (**POP3**) is a protocol used for **retrieving emails** from a mail server to a client. It **downloads** emails from the server to the client and emails are typically **deleted** from the server after download.

## What is IMAP?

The **Internet Message Access Protocol** (**IMAP**) is a standard email protocol used to **access** and **manage** email messages on a **mail server**. Allows users to **view** and **manipulate** their email messages as if they were stored locally on their device, while keeping them on the **server**. Allows **multiple devices** to access the same mailbox, maintaining synchronization across devices.

# SMTP/POP3 Example



# Dynamic Host Configuration Protocol (DHCP)

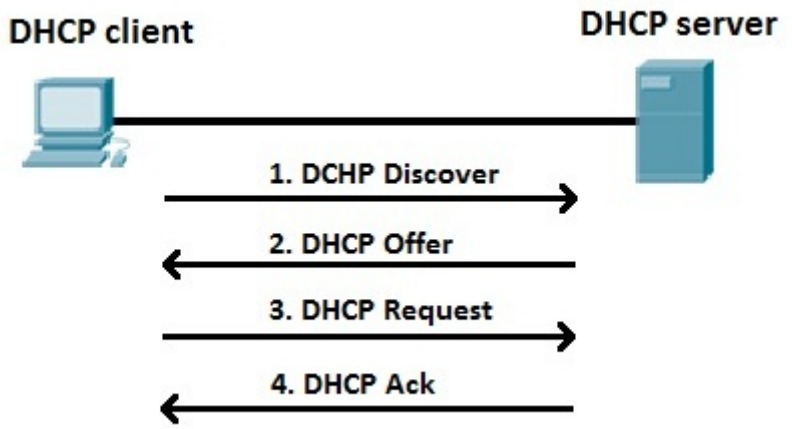
**Dynamic Host Configuration Protocol** (**DHCP**) is a network **management protocol** used to automatically assign **IP addresses** and other **network configuration parameters** to devices on a network. It reduces the need for manual configuration of IP addresses and ensures unique IP assignment.

1. **DHCP Discovery:** The client sends a DHCPDISCOVER broadcast message to find available DHCP servers.

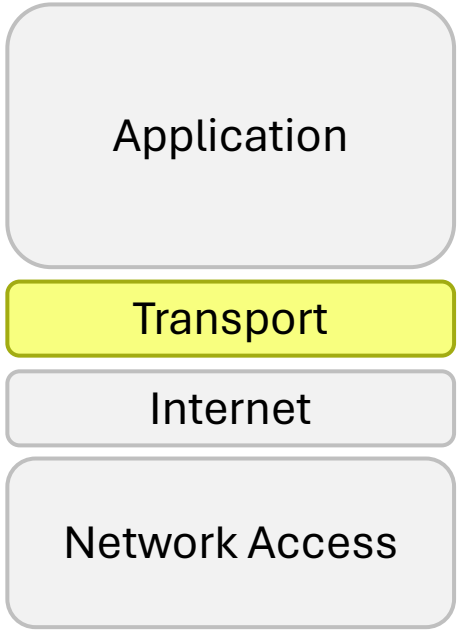
2. **DHCP Offer:** A DHCP server responds with a DHCPOFFER message, offering an IP address and other network configuration settings.

3. **DHCP Request:** The client replies with a DHCPREQUEST message, indicating acceptance of the offer.

4. **DHCP Acknowledgment:** The DHCP server confirms the lease with a DHCPACK message, finalizing the IP address assignment and configuration.



# Transport Layer




**Functions:**

Provides either reliable or unreliable data transmission between hosts.

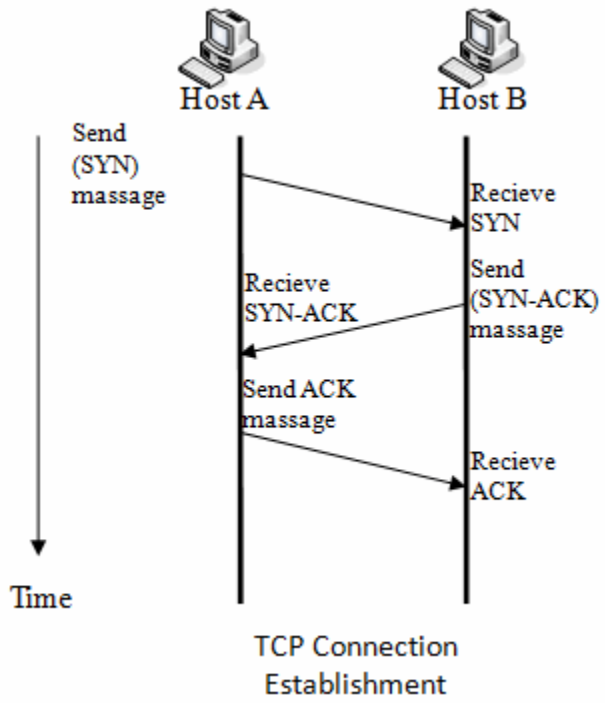
Includes mechanisms to ensure reliable data transmission.

**Protocols:**

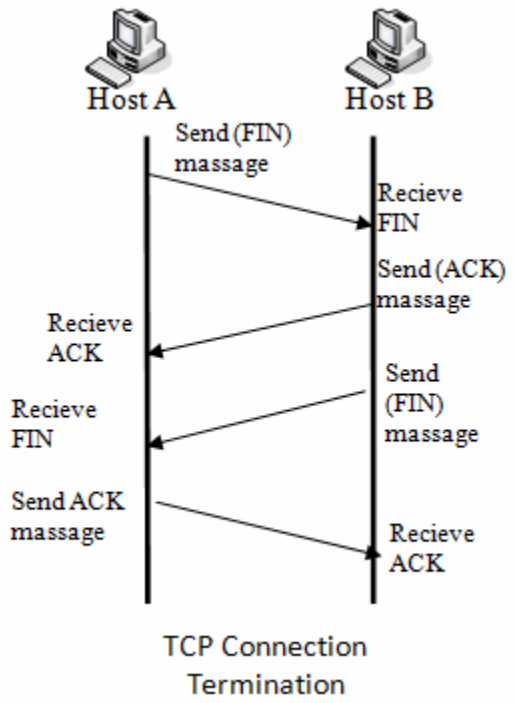
- **TCP:** Reliable, connection-oriented communication.
- **UDP:** Unreliable, connectionless communication.

# Transmission Control Protocol (TCP)

The **Transmission Control Protocol** (**TCP**) is a **connection-oriented** protocol that ensures **reliable** data transmission. It provides **error checking**, **flow control**, and **acknowledgment** of data packets, ensuring that data is delivered in the **correct order** without loss or duplication.



TCP Connection Establishment



TCP Connection Termination

# TCP Header Structure

| Field | Length (bits) | Description |
|---|---|---|
| Source Port | 16 | Port number of the sending application |
| Destination Port | 16 | Port number of the receiving application |
| Sequence Number | 32 | Position of the first byte of data in the segment |
| Acknowledgment Number | 32 | Next expected byte from the sender |
| Data Offset | 4 | Size of the TCP header in 32-bit words |
| Reserved | 3 | Reserved for future use, must be zero |
| Flags | 9 | Control flags (e.g., SYN, ACK, FIN) |
| Window Size | 16 | Size of the sender's receive window |
| Checksum | 16 | Error-checking of the header and data |
| Urgent Pointer | 16 | Points to urgent data (if URG flag is set) |
| Options | Variable | Optional fields for additional control |
| Padding | Variable | Ensures header length is a multiple of 32 bits |

**KEY FIELD**

**Source and Destination Port:**
Identifies the sending and receiving applications.

**Sequence Number:**
Tracks the position of data in the segment.

**Acknowledgment Number:**
Confirms receipt of data.

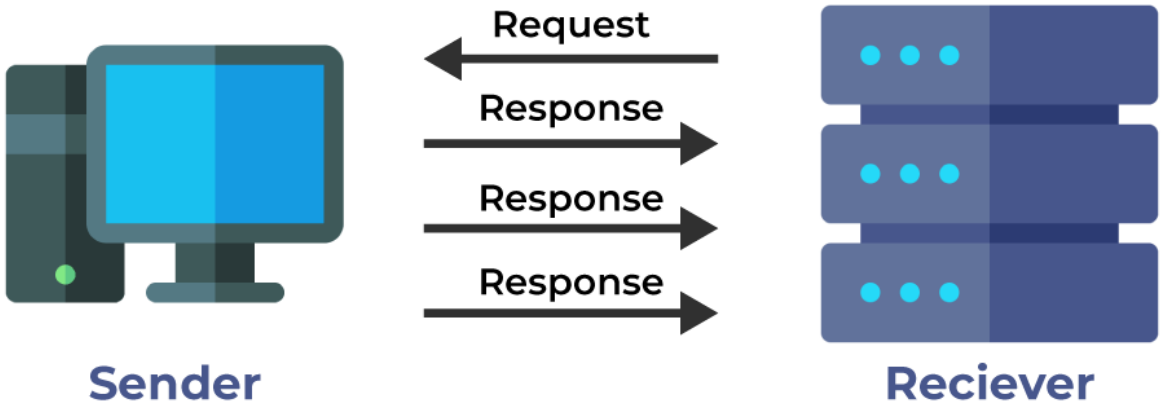
**Checksum:**
For error-checking of header and data

**Flags:**

- SYN: Synchronize sequence numbers (connection setup).
- ACK: Acknowledgment field significant.
- FIN: No more data from sender (connection teardown).

# User Datagram Protocol (UDP)

The **User Datagram Protocol** (**UDP**) is a **connectionless** protocol that provides **unreliable** data transmission. It does **not guarantee delivery**, **order**, or **error-correction** of the packets. It is used in scenarios where speed is more critical than reliability, such as streaming audio or video.



# UDP Header Structure

| Field | Length (bits) | Description |
|---|---|---|
| Source Port | 16 | Port number of the sending application |
| Destination Port | 16 | Port number of the receiving application |
| Length | 16 | Length of the UDP header and data |
| Checksum | 16 | Error-checking of the header and data |

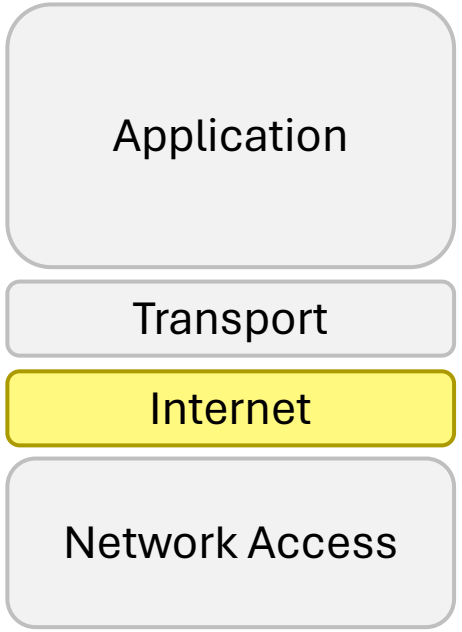
**KEY FIELD**

**Source and Destination Port:**
Identifies the sending and receiving applications.

**Length:**
Specifies the total length of the UDP header and data.

**Checksum:**
For error-checking of header and data

# Internet Layer




**Functions:**

Manages logical addressing and routing of data packets.

Ensures data reaches the correct destination across multiple networks.

**Protocols:**

- **IP:** Primary protocol for routing (IPv4 and IPv6).
- **ICMP:** Error messages and operational information.
- **ARP:** Maps IP addresses to MAC addresses.

# Internet Control Message Protocol (ICMP)

**Internet Control Message Protocol** (**ICMP**) is an Internet layer protocol used for sending **error** messages and **operational** information. It helps diagnose **network communication issues** and **report errors** back to the source IP address.

- **Diagnostic Tools:** Used in network utilities like *ping* and *traceroute* to test connectivity and trace paths.
- **Error Reporting:** Communicates network issues such as unreachable hosts, network congestion, and routing problems.

## Common ICMP Message Types:

**Echo Request (Type 8):** Sent by the ping command to request a response from a host.

**Echo Reply (Type 0):** Sent in response to an echo request, indicating the host is reachable.

**Destination Unreachable (Type 3):** Indicates that a destination is unreachable for various reasons (e.g., network unreachable, host unreachable).

**Time Exceeded (Type 11):** Indicates that a packet has expired in transit (used by traceroute).

**Redirect (Type 5):** Instructs a host to use a different route for packets.

# Address Resolution Protocol (ARP)

The **Address Resolution Protocol** (**ARP**) is an Internet layer protocol used to map an **IP address** to a **MAC address**. It facilitates communication within a local network by **linking** layer 2 IP addresses to layer 1 MAC addresses.

### How it works:

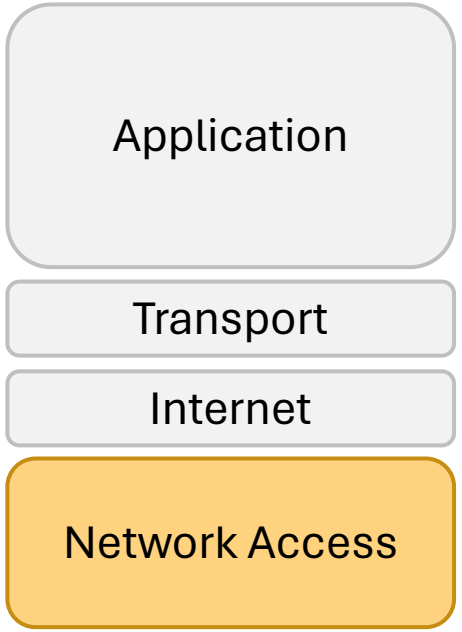
**ARP Request:** A device sends a broadcast ARP request to all devices on the local network, asking for the MAC address corresponding to a specific IP address.

**ARP Reply:** The device with the requested IP address responds with an ARP reply, providing its MAC address.

- **ARP Cache:**

A table stored in a device's memory that maintains a record of IP-to-MAC address mappings. It have a limited lifetime and are periodically refreshed.

# Network Access Layer




**Functions:**

Manages data framing, physical addressing, and error detection at the data link level.

Controls hardware and software communication on the physical network.

**Protocols:**

- **Ethernet:** LAN technology.
- **Wi-Fi:** Wireless networking technology.