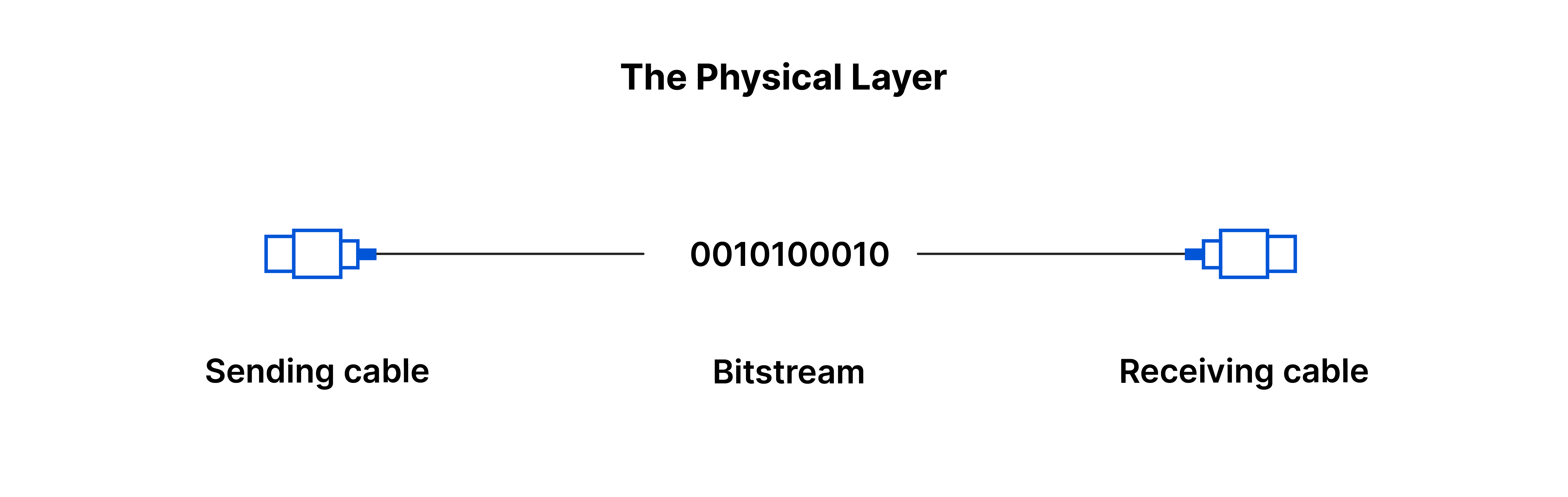
**Packet Traveling(imp)**

[](https://www.practicalnetworking.net/wp-content/uploads/2016/01/packtrav-encap-decap.gif)

**1. The physical layer**



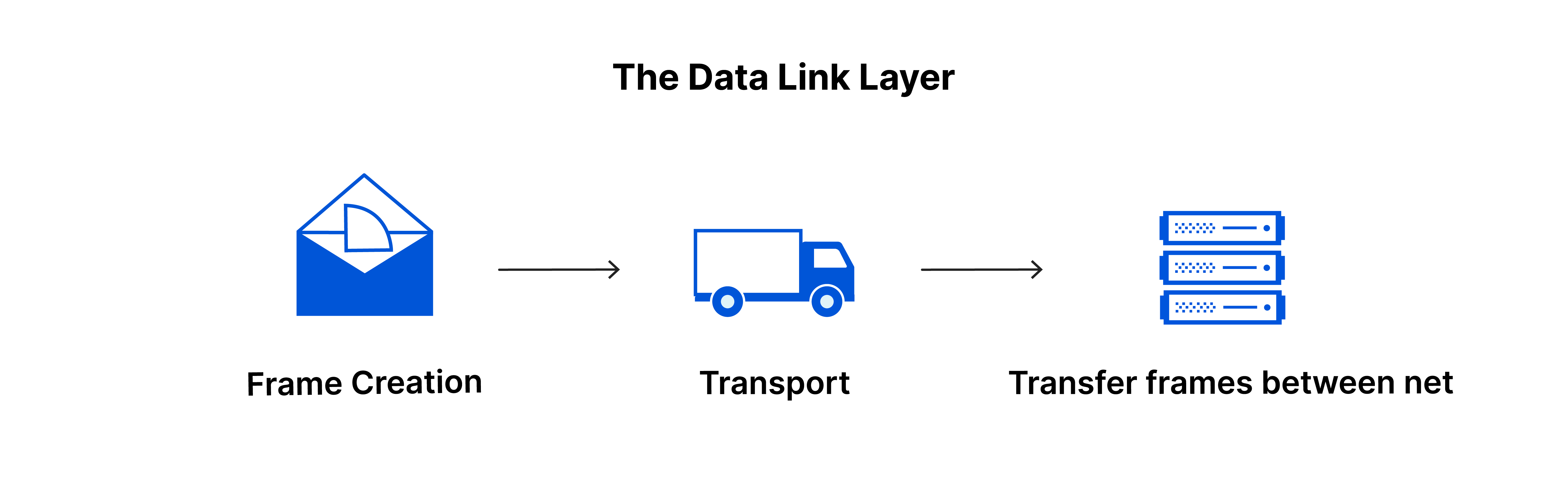
The lowest OSI layer, responsible for transmitting raw bit streams over physical media such as cables (twisted-pair, fiber-optic) or wireless connections, using electrical, optical, or mechanical signals.

**Function**: This is the lowest layer of the OSI model, responsible for the physical connection between devices.

**Responsibilities**: It deals with raw data transmission over physical mediums like cables, fiber optics, or wireless signals.

**Examples**: Ethernet cables, USB, Wi-Fi, voltage levels, physical connectors.

**2. The data link layer**



Layer 2 will then group together those 1’s and 0’s into chunks known as Frames.

It uses MAC addresses and is responsible for packet delivery from hop to hop.

The MAC address is replaced at each hop, with the source MAC set to the current device (e.g., router's interface) and the destination MAC set to the next hop's MAC address

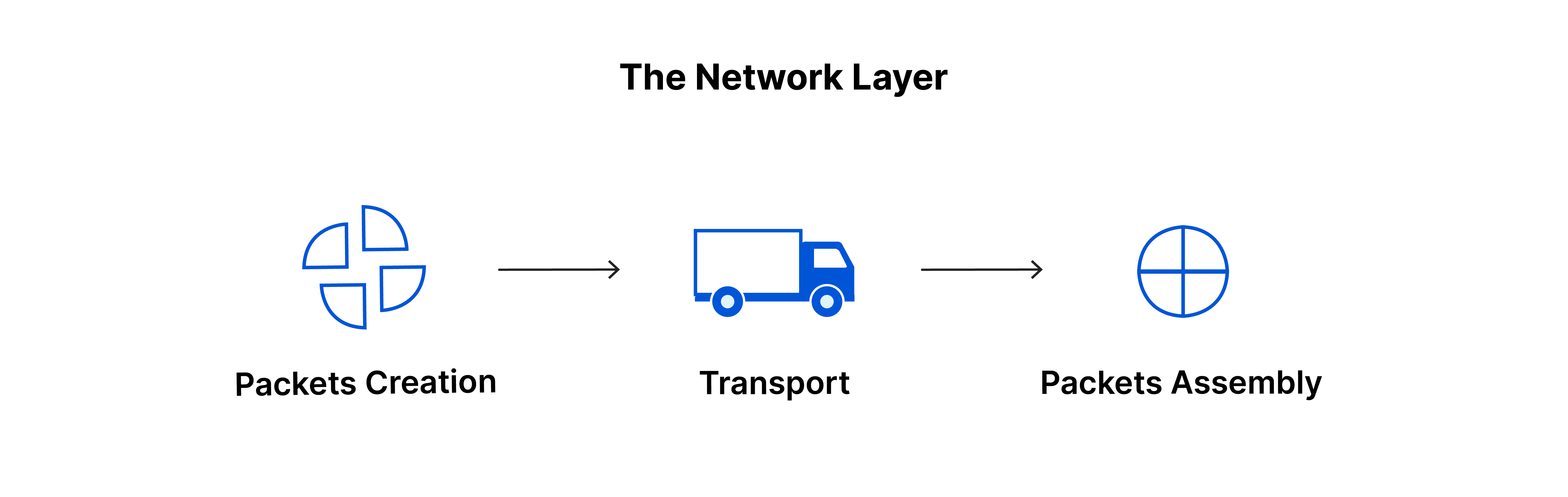
It handles frame synchronization, flow control, error detection/correction, and link management.

**Function**: Fragmentation, hop to hop delivery, physical addressing.

**Responsibilities**: This layer manages node-to-node data transfer and handles error detection and correction from the physical layer.

**Examples**: Ethernet, Wi-Fi (IEEE 802.11), MAC (Media Access Control), and ARP (Address Resolution Protocol).

**3. The network layer**



The Network layer of the OSI model is responsible for packet delivery from end to end.

The network layer converts logical addresses to physical addresses and determines the best route for packets (routing). Its key functions are:

**Routing, Logical addressing, Packet forwarding, Fragmentation and reassembly**

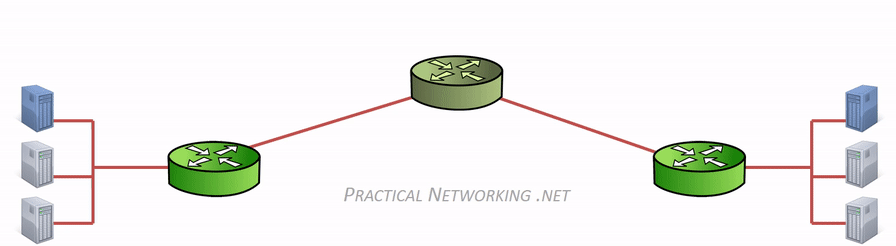
**Logical Addressing**: Assigns IP addresses to devices for identification across networks.

**Routing**: Determines the best path for data to travel between the source and destination, often through multiple networks.

**Packet Forwarding**: Moves data packets through intermediate devices (e.g., routers) to reach the target network.

**Fragmentation**: Breaks large packets into smaller ones to accommodate different network capacities and reassembles them at the destination.

Protocols like **IP**, **ICMP**, and **routing protocols** (OSPF, RIP, BGP) operate at this layer, making global network communication possible.

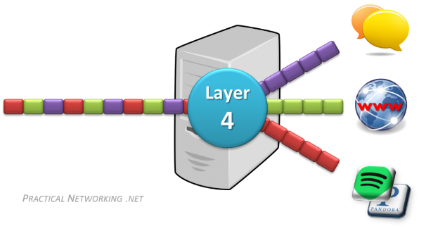
[](https://www.practicalnetworking.net/wp-content/uploads/2016/01/packtrav-l2-vs-l3.gif)

**4. The transport layer**

Layer 4 is responsible for *service to service* delivery.

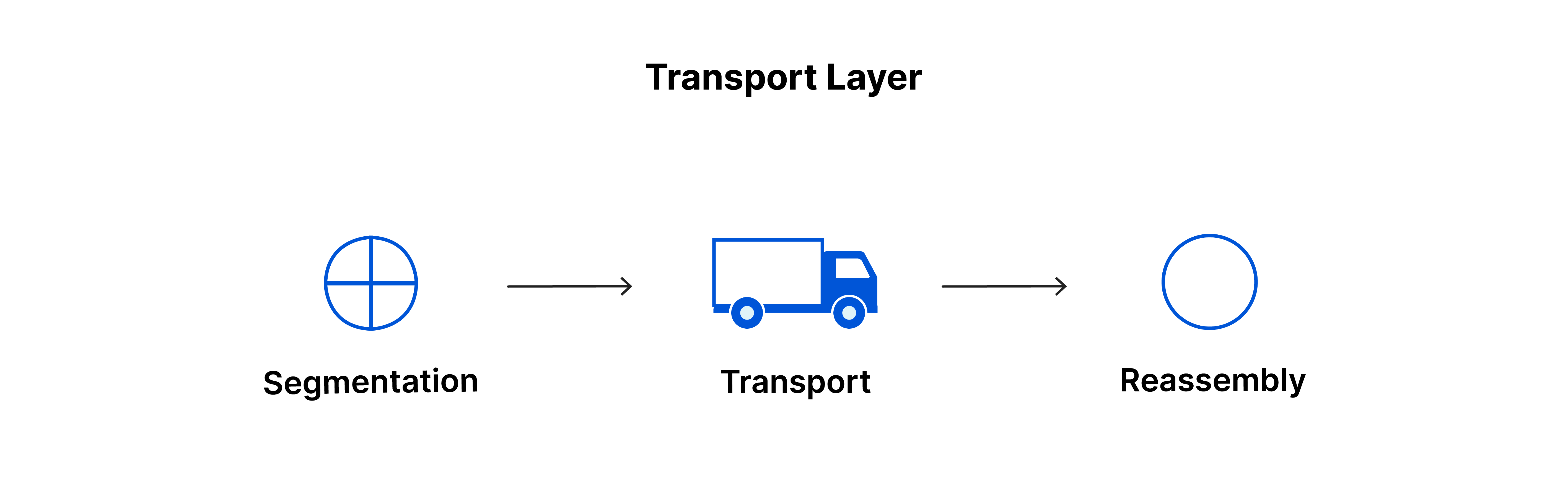
At any given time on a user’s computer there might be an Internet browser open, while music is being streamed, while a messenger or chat app is running. Each of these applications are sending and receiving data from the Internet, and all that data is arriving in the form of 1’s and 0’s on to that computer’s NIC.

Something has to exist in order to distinguish which 1’s and 0’s belong to the messenger or the browser or the streaming music. That “something” is Layer 4:



Layer 4 accomplishes this by using an addressing scheme known as Port Numbers.

Specifically, two methods of distinguishing network streams exist. They are known as the Transmission Control Protocol (TCP), or the User Datagram Protocol (UDP).



This includes taking data from the session layer and breaking it up into chunks called segments before sending it to layer 3.

Transport layer protocols include the [Transmission Control Protocol (TCP)](https://www.cloudflare.com/learning/ddos/glossary/tcp-ip/) and the [User Datagram Protocol (UDP)](https://www.cloudflare.com/learning/ddos/glossary/user-datagram-protocol-udp/).

**Service-point Addressing**:  
The transport layer adds a service-point (port) address to direct data to the correct process, while the network layer handles computer-to-computer communication.

**Segmentation and Reassembly**:  
The transport layer breaks data into segments with sequence numbers and reassembles it at the destination.

**Connection Control**:  
The transport layer offers both connectionless (independent packets) and connection-oriented (consistent path for packets) services.

**Flow Control**:  
It manages data flow end-to-end to prevent the sender from overwhelming the receiver.

**Error Control**:  
Ensures error-free data delivery end-to-end, not just on a single link.

**5. The session layer**

Manages, maintains, and terminates communication sessions between devices, and handles errors from upper layers.

**Function**: Manages sessions or connections between two systems.

**Responsibilities**: Establishes, maintains, and terminates connections (sessions) between applications on different devices.

**Examples**: NetBIOS, PPTP (Point-to-Point Tunneling Protocol).

**6. The presentation layer**

Translates data formats between application-specific and common formats, handles character code translation, data conversion, compression, and encryption.

**Function**: Transforms data into a format understandable by the application layer.

**Responsibilities**: Handles data translation, encryption, and compression to ensure data from the sender is readable by the receiver.

**Examples**: JPEG, PNG, ASCII, EBCDIC (character encoding standards), SSL/TLS (for encryption).

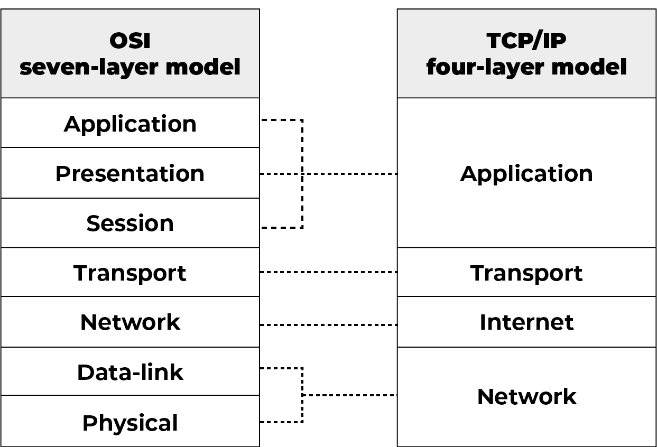
**7. The application layer**

Provides user access to network services using protocols like HTTP, FTP, SMTP, and DNS. It facilitates web requests and other application-level interactions.

**Function**: Provides services and network applications directly to the end user.

**Responsibilities**: Interfaces directly with software applications, enabling network services like email, file transfer, and web browsing.

**Examples**: HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), DNS (Domain Name System).



**TCP/IP** (Transmission Control Protocol/Internet Protocol) is a suite of communication protocols used for the Internet and similar networks. It specifies how data is packaged, addressed, transmitted, routed, and received across networks. The TCP/IP model is generally divided into four layers:

* **Application Layer**: This layer is responsible for providing network services to end-user applications. Protocols such as HTTP, FTP, SMTP, and DNS operate at this layer.
* **Transport Layer**: This layer manages end-to-end communication and data integrity. It includes protocols like TCP (Transmission Control Protocol) and UDP (User Datagram Protocol).
* **Internet Layer**: Responsible for logical addressing and routing of packets. The most important protocol at this layer is the Internet Protocol (IP), which routes packets across networks.
* **Link Layer**: This layer defines how data is physically transmitted over the network medium (e.g., Ethernet, Wi-Fi). It manages hardware addressing and the protocols required to transmit data on the local network.

**Bandwidth**: Bandwidth measures the maximum data transfer rate over a network connection. It refers to the amount of data that can be transmitted in a given time.

An **IP address** (Internet Protocol address) is a unique identifier assigned to each device connected to a computer network that uses the Internet Protocol for communication. It serves two primary functions:

**Identification: An IP address uniquely identifies a device on a network, ensuring that data is sent to the correct recipient.**

**Location Addressing: It provides the device's location in the network, enabling proper routing of data between devices.**

**Dynamic IP Addresses:** Assigned by a DHCP (Dynamic Host Configuration Protocol) server, these addresses can change over time.

**Static IP Addresses:** Permanently assigned to a device and do not change.

**Ipconfig**: Command in Windows to view and configure network interfaces.

The reliability of a network can be measured by: Downtime, Failure Frequency, Catastrophe.

NIC (Network Interface Card) is a peripheral card that connects a PC to a network, has a unique MAC address for identification, and provides a wireless connection, primarily used in desktop computers.

**POP3**: Protocol for accessing mail on a client, with Delete and Keep modes.

**Private IP Address**: Reserved IP ranges for internal use, requiring a proxy or NAT to access the internet.

**Public IP Address**: ISP-assigned address for internet communication.

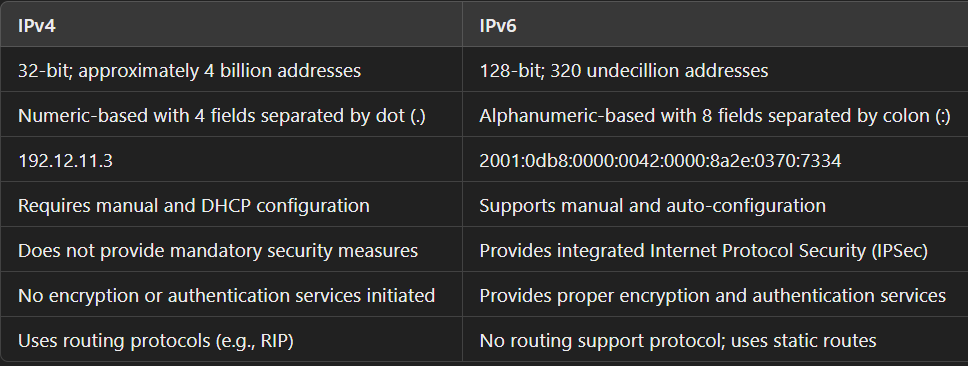
**RAID**: Fault tolerance method using multiple hard drives.

**Unicasting**: Message to a single node.

**Anycasting**: Message to any available node.

**Multicasting**: Message to multiple specific nodes.

**Broadcasting**: Message to all network nodes.



A **subnet** is a segmented part of a larger network that improves organization, performance, and security by allowing efficient IP address management and communication through routers.

**Subnetting** is the practice of dividing a larger IP network into smaller, more manageable subnetworks (subnets). It helps improve network performance and security by reducing broadcast domains and efficiently allocating IP addresses.

A subnet mask is a 32-bit number that divides an IP address into network and host parts, used for subnetting.

**Network Topology**:

* **Bus**: Single central cable.
* **Star**: Devices connected to a central hub.
* **Ring**: Devices in a circular layout.
* **Mesh**: Devices interconnect with many-to-many links.

**Node**: Any device in a network.  
**Link**: A communication pathway between two nodes.

A **gateway** is a network device that connects and translates communication between different networks using different protocols.

A **router** is a network device that forwards data packets between networks, directing traffic based on IP addresses.

A **router** directs data between similar networks (usually within the same protocol), whereas a **gateway** connects and translates data between different networks that may use different protocols.

A **hub** is a networking device that connects multiple Ethernet devices, making them act as a single network segment by transmitting data to all connected devices.

A **switch** is a networking device that connects devices on a local area network (LAN) and forwards data only to the specific device or devices that need it, improving network efficiency and security.

The **ping** command checks the connectivity between two devices by sending ICMP echo requests and measuring the time it takes for a response, helping to diagnose network issues.

ping google.com

ICMP is the Internet Control Message Protocol. It is a network layer protocol used for error handling. It is mainly used by network devices like routers for diagnosing the network connection issues and crucial for error reporting.

ARP is Address Resolution Protocol. It is a network-level protocol used to convert the logical address i.e. IP address to the device's physical address i.e. MAC address.

DNS (Domain Name System) translates human-readable domain names into IP addresses to locate and access resources on the internet.

**google.com** , IP address **142.250.190.14**

**DNS Forwarder**: Sends unresolved DNS queries to external servers for faster resolution.

MAC addresses are unique 48-bit hardware identifiers embedded in a network interface card (NIC) during manufacturing, often referred to as the physical address of a network device

A protocol is a set of rules governing information communication, with main elements including:

* **Syntax**: Structure and format of data presentation.
* **Semantics**: Meaning of each section of bits.
* **Timing**: Specifies when and how fast data is sent.

**DHCP**: Assigns IP addresses and network configurations to devices automatically, enabling communication over IP networks (Port 67).

**FTP**: Transfers files between hosts reliably and efficiently (Port 27).

**ICMP**: Handles error reporting and network diagnostics (Port 7).

**ARP**: Converts IP addresses to MAC addresses for local network communication.

**RIP**: Helps routers find the best route for data using hop count in small/medium networks.

In a **Class C network**, the default subnet mask is 255.255.255.0, meaning the first 24 bits are used for the network portion and the last 8 bits for host addresses.

CIDR: 192.168.1.0/24:

**IP address**: 192.168.1.0

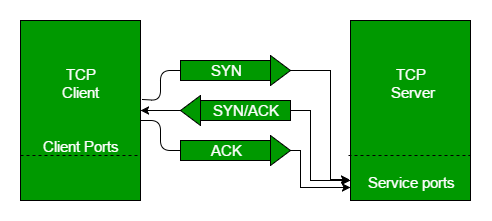
**Prefix length**: /24 means the first 24 bits are used for the network, leaving 8 bits for host addresses.

**Subnet Mask**: 255.255.255.0

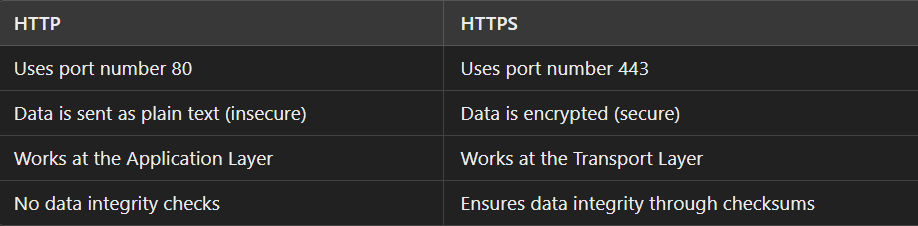
A **firewall** is a security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules to protect networks from unauthorized access and threats.

The TCP 3-way handshake is a method for establishing a reliable connection between a client and server in the TCP/IP model. It involves three steps:

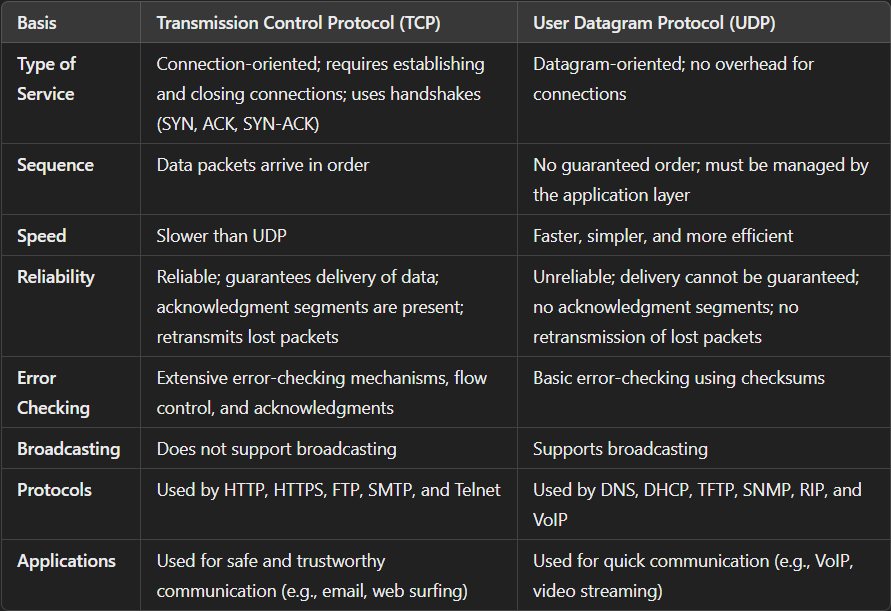
1. **SYN**: The client sends a SYN segment to initiate communication.
2. **SYN-ACK**: The server responds with a SYN-ACK segment, acknowledging the request and indicating its own sequence number.
3. **ACK**: The client sends an ACK segment, confirming the server's response, establishing a reliable connection for data transfer.



A server-side load balancer distributes incoming network traffic across multiple servers to improve availability, reliability, and performance.



SMTP (Simple Mail Transfer Protocol) is a protocol used for sending and receiving email messages over the internet.



what happens when you type "google.com" in your browser?

1. **DNS Resolution**: The browser checks its cache for the IP address of "google.com." If not found, it queries a DNS server to get the IP address.
2. **Establishing Connection**: The browser establishes a TCP connection with the server at the obtained IP address, using a 3-way handshake.
3. **Sending Request**: The browser sends an HTTP/HTTPS request to the server for the webpage.
4. **Load Balancer**: The request is routed through a load balancer that distributes it to one of Google’s many servers.
5. **Server Response**: The server processes the request and sends back HTML, CSS, and JavaScript files.
6. **Rendering the Page**: The browser renders the received data, displaying the Google homepage for you to interact with.

A VPN creates a secure, encrypted connection over Internet, hiding your IP address and enhancing online privacy.

1. **Secure Connections:** Encrypts data for protection against cyber threats.
2. **IP Address Masking:** Hides your IP address for enhanced privacy.
3. **Slower Speeds:** May reduce internet connection speed.
4. **Connection Drops:** Can occasionally lose connection, risking data exposure.

**Proxy**: An intermediary server that forwards client requests to the destination server, typically used to hide the client's IP address and improve security or caching. Eg: An employee uses a proxy server to access websites while hiding their actual IP address.

**Reverse Proxy**: A server that sits between clients and backend servers, forwarding client requests to the appropriate backend server, often used for load balancing, security, and caching. Eg: A website uses a reverse proxy to handle requests and distribute them across multiple backend servers, improving performance and security.