4. Computer Networks

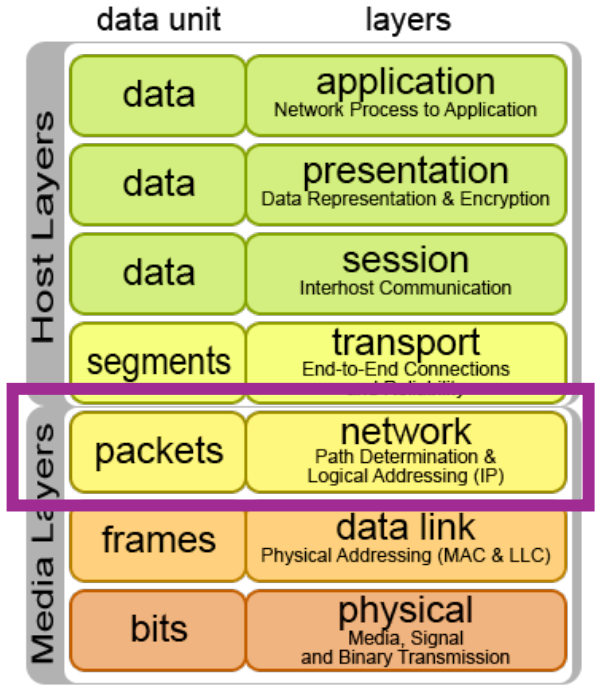
Network, Transport, Session, Presentation, Application Layers

Summary

- Network Layer
- Packet Header Structure
- Routing Process
- Logical Addressing – IP Address
- IPv4 Address Structure
- Subnet Mask Structure
- Transport Layer
- Sockets
- Segment Header Structure
- Session, Presentation, Application Layers

Network Layer

The **Network Layer** is the **third** layer in the **ISO/OSI model**. It determines how data is sent to the receiving devices across multiple networks. Specifically, it is responsible for **routing**, **forwarding**, and **addressing** data packets across different networks.



Functions of the Network Layer

- **Routing:**

Determines the optimal path for data to travel from source to destination.

- **Forwarding:**

Moves packets from the router's input to the appropriate output.

- **Logical Addressing:**

Uses IP addresses to identify devices on a network.

- **Fragmentation and Reassembly:**

Breaks down large packets into smaller fragments and reassembles them at the destination.

Packet Header Structure

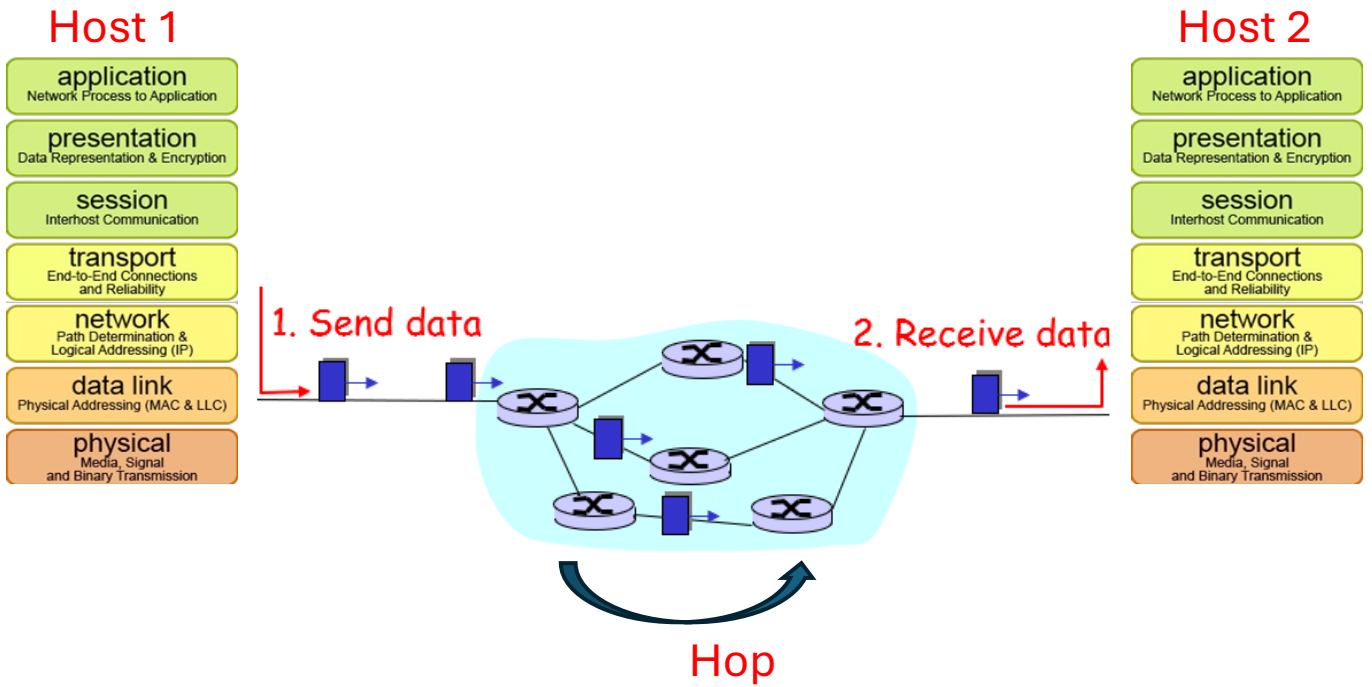
IPv4 Packet Header Structure

Field	Length (bits)	Description
Version	4	IP version (4 for IPv4)
IHL	4	Internet Header Length (in 32-bit words)
Type of Service (ToS)	8	Quality of Service indicators and priority
Total Length	16	Total length of the packet (header + data)
Identification	16	Unique identifier for fragments of the original packet
Flags	3	Control flags for fragmentation
Fragment Offset	13	Position of this fragment in the original packet
Time to Live (TTL)	8	Maximum number of hops the packet can take
Protocol	8	Protocol used in the data portion (e.g., TCP, UDP)
Header Checksum	16	Error-checking of the header
Source IP Address	32	IP address of the sender
Destination IP Address	32	IP address of the receiver
Options	Variable (0-40 bytes)	Optional fields for additional functionality (e.g., security)
Padding	Variable	Extra bytes to ensure the header is a multiple of 32 bits

Routing Process/1

The **routing process** comprises these **3 steps**:

1. **Path Determination:** Routers use routing tables and algorithms to determine the best path for data packets.
2. **Packet Switching:** Data packets are forwarded from one router to another based on the routing table.
3. **Next-Hop Forwarding:** Each router forwards the packet to the next router until it reaches the destination.



Path Determination

Path determination is the process by which routers decide the **best route** for data packets **to travel** from the source to the destination.

- **Routing Tables:** Routers maintain routing tables that contain information about **network topology** and **available routes**.
  - **Static Routing:** Routes are manually configured by network administrators.
  - **Dynamic Routing:** Routes are automatically learned and updated using routing protocols.

- **Routing Algorithms:** Algorithms such as Dijkstra's **Shortest Path First (SPF)** and **Distance Vector** are used to calculate the optimal path.
  - **Shortest Path First (SPF):** Calculates the shortest path to a destination based on cumulative cost metrics.
  - **Distance Vector:** Determines the best path based on distance metrics and updates from neighboring routers.

Packet Switching

Packet switching is the process of **moving data packets** from the **input port** of a router to the appropriate **output port**, based on routing decisions.

- **Switching Fabric:** The internal architecture of a router that connects input ports to output ports.
  - **Store-and-Forward:** Entire packet is received before it is forwarded to the next hop.
  - **Cut-Through:** Packet is forwarded as soon as the destination address is read.

- **Buffering:** Temporary storage of packets in memory if the output port is busy, preventing packet loss.

- **Forwarding Decision:** Based on the destination IP address and the routing table, the router decides the next hop for the packet.

Store-and-Forward Switching

The **entire packet** is received by the router before it is **forwarded** to the next hop.

Process:

1: The router receives the entire data packet.

2: The packet is stored temporarily in memory.

3: Error checking (such as CRC) is performed to ensure data integrity.

4: The packet is forwarded to the next hop based on the destination address.

Advantages: Ensures error-free transmission by checking the entire packet for errors before forwarding. Suitable for networks where data integrity is crucial.

Disadvantages: Higher latency due to the time taken to receive and process the entire packet. Requires more memory to store the packets.

Cut-Through Switching

The packet is **forwarded** as soon as the destination address is read, **without waiting** for the **entire packet** to be received.

Process:

1: The router begins forwarding the packet as soon as it reads the destination MAC address from the packet header.

2: The rest of the packet continues to be forwarded as it is received.

Advantages: Lower latency because forwarding begins almost immediately after the destination address is read. Faster data transfer suitable for high-performance networks.

Disadvantages: Does not check for errors in the packet, which means corrupted packets might be forwarded. Can lead to potential issues if the packet is corrupted during transmission.

Next-Hop Forwarding

Next-hop forwarding refers to the process of **sending** a data packet to the **next router** (or final destination) along the path determined by the routing algorithm.

- **Hop-by-Hop Routing**

Each router along the path makes an independent forwarding decision.

- **Next-Hop Address**

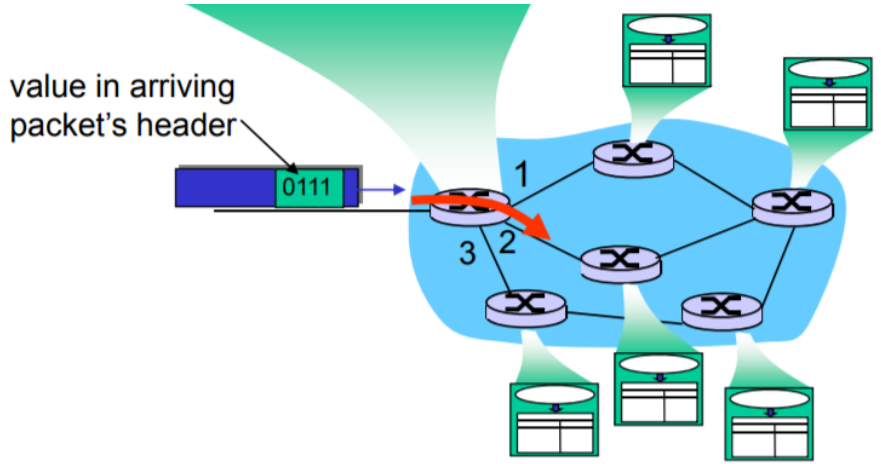
The IP address of the next router to which the packet should be sent.

- **Address Resolution Protocol (ARP)**

Translates IP addresses to MAC addresses for forwarding packets at the Data Link Layer

Routing Process/2

Destinazione IP	Maschera di Sottorete	Next Hop (Prossimo Router)	Interfaccia di Uscita
192.168.1.0	255.255.255.0	192.168.2.1	GigabitEthernet0/1
10.0.0.0	255.0.0.0	10.1.1.1	GigabitEthernet0/2
172.16.0.0	255.255.0.0	172.16.1.1	GigabitEthernet0/3
0.0.0.0	0.0.0.0	192.168.3.1	GigabitEthernet0/4 (Default Route)



Logical Addressing – IP Address

Each device on a network has a unique **IP address** used for **identification** and **communication**.

IPv4 Addresses: 32-bit addresses, e.g., 192.168.1.1

IPv6 Addresses: 128-bit addresses, e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334

IPv4 Structure

Format: Dotted decimal notation (e.g., **192.168.1.1**)

Binary Representation: 32 bits divided into four 8-bit octets.

Example: 192.168.1.1 in binary is 11000000.10101000.00000001.00000001.

Classes (to define *network size* and *purpose*):

Class A: 0.0.0.0 to 127.255.255.255

Class B: 128.0.0.0 to 191.255.255.255

Class C: 192.0.0.0 to 223.255.255.255

Class D: 224.0.0.0 to 239.255.255.255 (Multicast)

Class E: 240.0.0.0 to 255.255.255.255 (Reserved)

Subnet Mask Structure

The **Subnet Mask** is a 32-bit number that **divides** the IP address into **network** and **host** portions.

- **Function:**

Determines which part of the IP address is the network address and which part is the host address.

Format: Dotted decimal notation (e.g., 255.255.255.0).

Binary Representation: Corresponds to the IP address, using 1s for the network part and 0s for the host part.

Example: 255.255.255.0 in binary is 11111111.11111111.11111111.00000000.

Combining IP Address and Subnet Mask

Network Address: The part of the IP address identified by the subnet mask's 1s.

Host Address: The part of the IP address identified by the subnet mask's 0s.

Example:

- **IP Address:** 192.168.1.10
- **Subnet Mask:** 255.255.255.0
- **Network Address:** 192.168.1.0
- **Host Address:** 10

IPv4 Class A and Class B

Class A

Range: 0.0.0.0 to 127.255.255.255

First Octet Range: 0 to 127

Default Subnet Mask: 255.0.0.0

Number of Networks: 128 (2^7)

Hosts per Network: Over 16 million (2^{24} - 2)

Usage: Designed for very large networks with many devices, such as large corporations or ISPs.

Example: 10.0.0.1

Class B

Range: 128.0.0.0 to 191.255.255.255

First Octet Range: 128 to 191

Default Subnet Mask: 255.255.0.0

Number of Networks: 16.384 (2^{14})

Hosts per Network: Over 65k (2^{16} - 2)

Usage: Suitable for medium-sized networks, such as universities or large companies.

Example: 172.16.0.1

IPv4 Class C, Class D, and Class E

Class C

Range: 192.0.0.0 to 223.255.255.255

First Octet Range: 192 to 223

Default Subnet Mask: 255.255.255.0

Number of Networks: Over 2 million (2^{21})

Hosts per Network: 254 (2^8 - 2)

Usage: Ideal for small networks, such as small businesses or home networks.

Example: 192.168.1.1

Class D

Range: 224.0.0.0 to 239.255.255.255

First Octet Range: 224 to 239

Default Subnet Mask: 255.255.255.255

Usage: Reserved for multicast groups. Allows a single packet to be sent to multiple destinations.

Example: 224.0.0.1

Class E

Range: 240.0.0.0 to 255.255.255.255

First Octet Range: 240 to 255

Usage: Reserved for experimental purposes and future use. Not used for general networking.

Private and Public IP Addresses

Private IP Addresses

IP addresses used within a private network. Not routable on the internet.

Example:

Home Network: 192.168.1.1

Office Network: 10.0.0.1

Public IP Addresses

IP addresses that are routable on the internet. Assigned by ISPs and regulated by regional internet registries.

Example:

Website IP: 93.184.216.34

Corporate Server: 203.0.113.10

Network Address Translation (NAT)

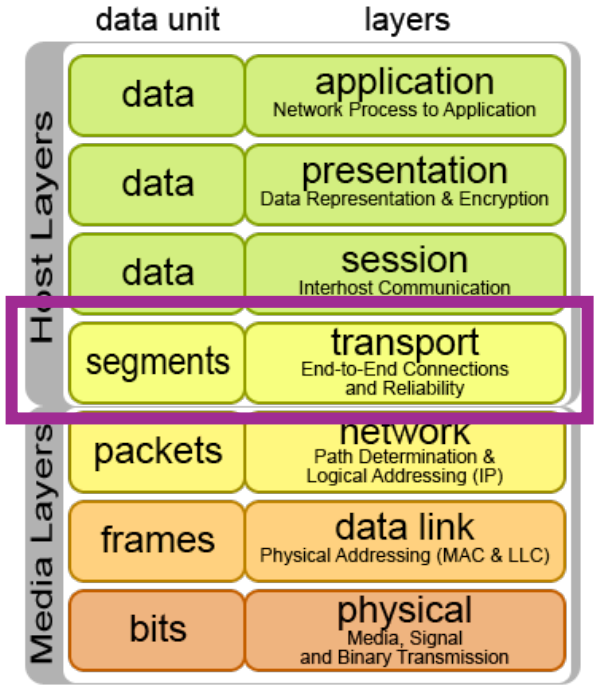
Purpose: Allows multiple private IP addresses to share a single public IP address for internet access.

Function: Translates private IP addresses to a public IP address and vice versa.

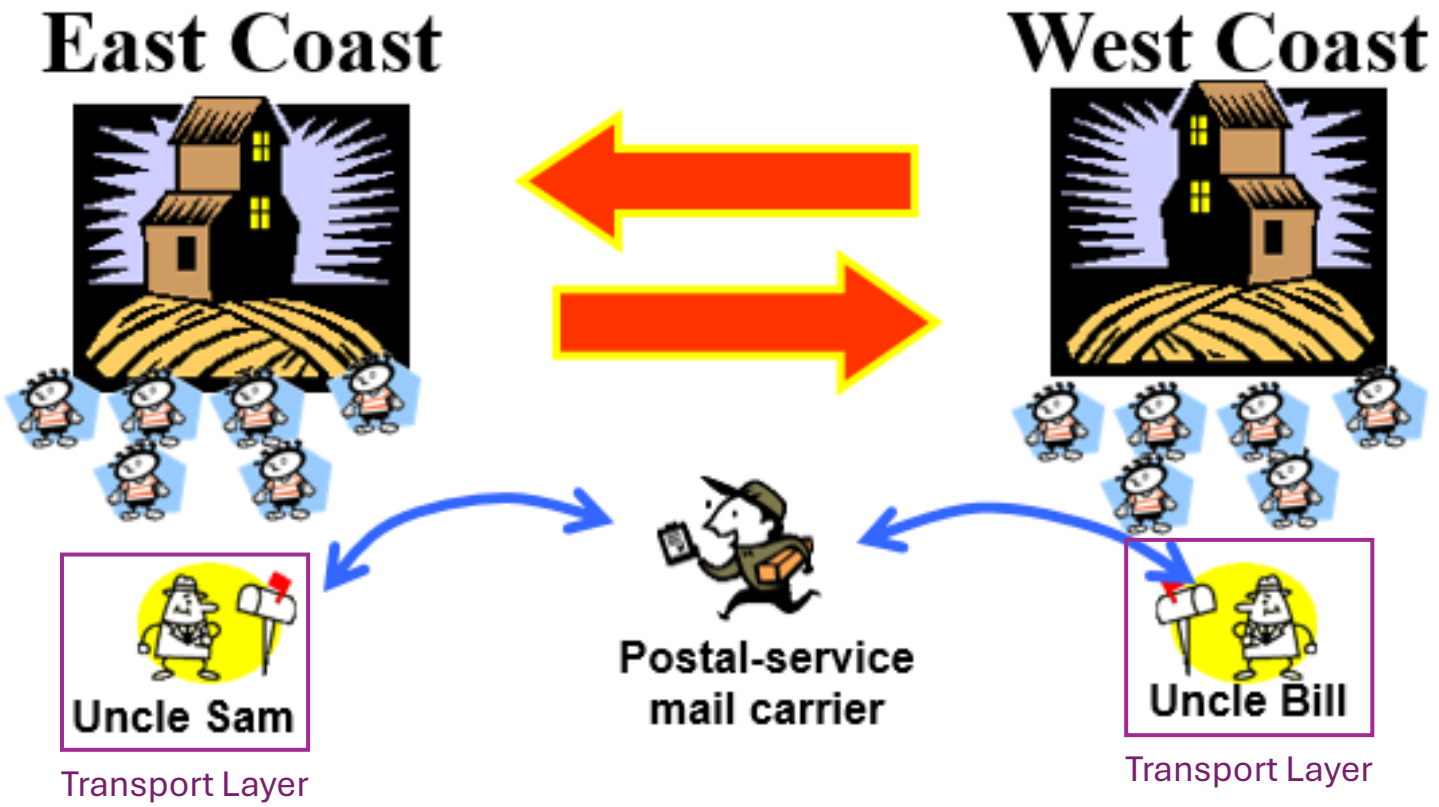
Example: A home router uses NAT to enable all devices in a home network (with private IP addresses) to access the internet using the router's public IP address.

Transport Layer

The **Transport Layer** is crucial for **end-to-end communication** between devices on a network.



Transport Layer - Analogy



Functions of the Transport Layer

- **End-to-End Communication:**

Manages data transfer between devices.

- **Segmentation and Reassembly:**

Splits large data streams into smaller segments and reassembles them at the destination.

- **Error Detection and Correction:**

Ensures data integrity and reliability.

- **Flow Control:**

Manages the rate of data transmission between devices.

Connection Management:

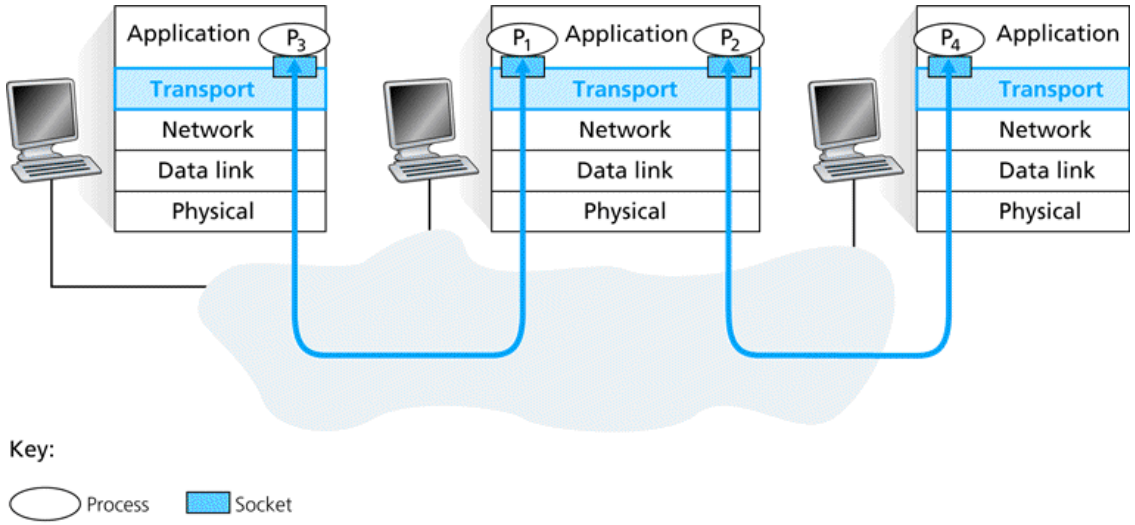
- Establishes, maintains, and terminates connections.

Sockets

Sockets are fundamental for enabling communication between devices over a network. They act as **interfaces** through which **processes (applications)** communicate across a computer network.

Combining **IP addresses** and **port numbers** uniquely identify a network connection (network, host, and applications).

Example: 192.168.1.1:80

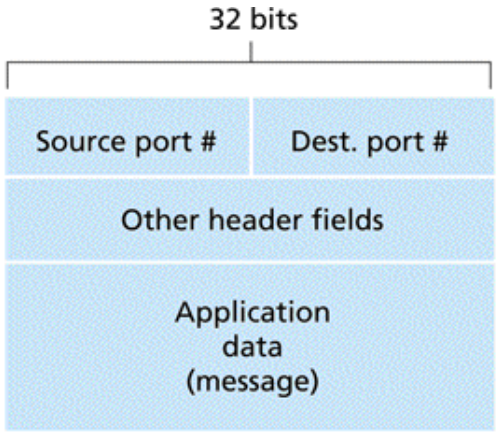


Segment Header Structure

Source Port (16 bits): Port number of the sending application

Destination Port (16 bits): Port number of the receiving application

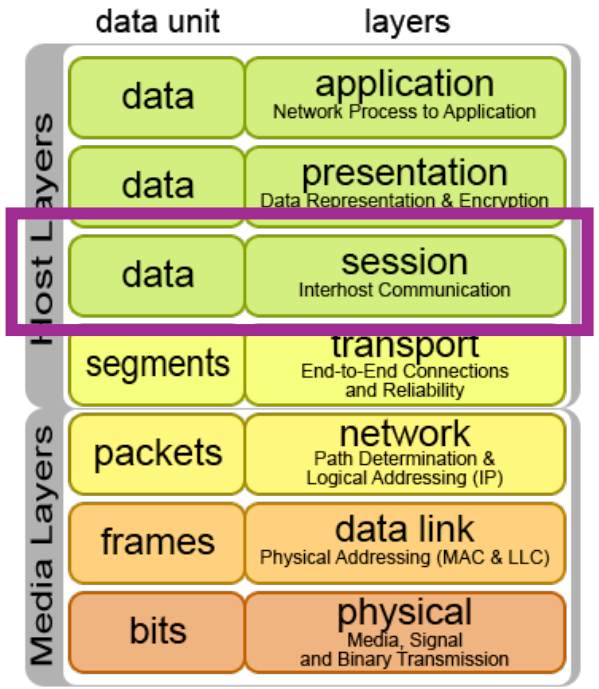
Other header fields: Fields depending on TCP or UDP protocols



Session Layer

The **Session Layer** manages and controls the connections between computers.

- Creates, maintains, and terminates **sessions** between **applications**.
- Manages dialogue (communication) between two devices, allowing them to communicate in either **half-duplex** or **full-duplex** mode.

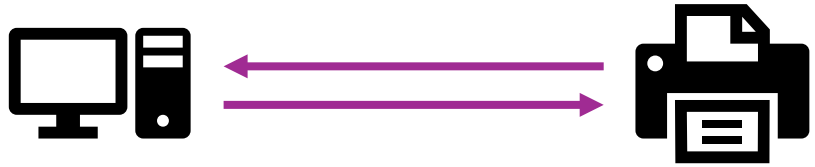


Session Layer – Dialog Control

Half-Duplex Mode:

Communication can occur in both directions, but **not simultaneously**.

Example: A network printer and a computer communicate in half-duplex mode, where the computer sends a print job, and the printer sends an acknowledgment back, but they do not send data at the same time.



Full-Duplex Mode:

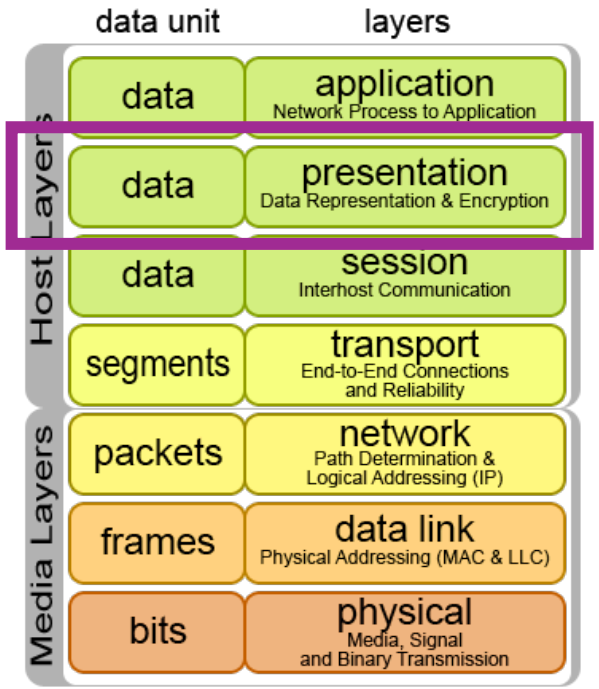
Communication can occur **simultaneously** in both directions.

Example: A video conferencing application where both participants can speak and listen at the same time, ensuring smooth two-way communication.

Presentation Layer

The **Presentation Layer** translates data between the application layer and the network.

- **Translation:** Converts data formats from application-specific formats to network formats, and vice versa.
- **Encryption/Decryption:** Ensures data security by encrypting data before transmission and decrypting it upon reception.
- **Compression:** Reduces the size of the data to be transmitted to optimize network resource usage.



Application Layer

The **Application Layer** provides network services directly to user applications.

- **Functions:** Network Services: Enables user applications to interact with the network (e.g., file transfers, email, remote login).
- **Resource Sharing:** Facilitates access to network resources.
- **User Interface:** Provides an interface for the user to interact with the network.