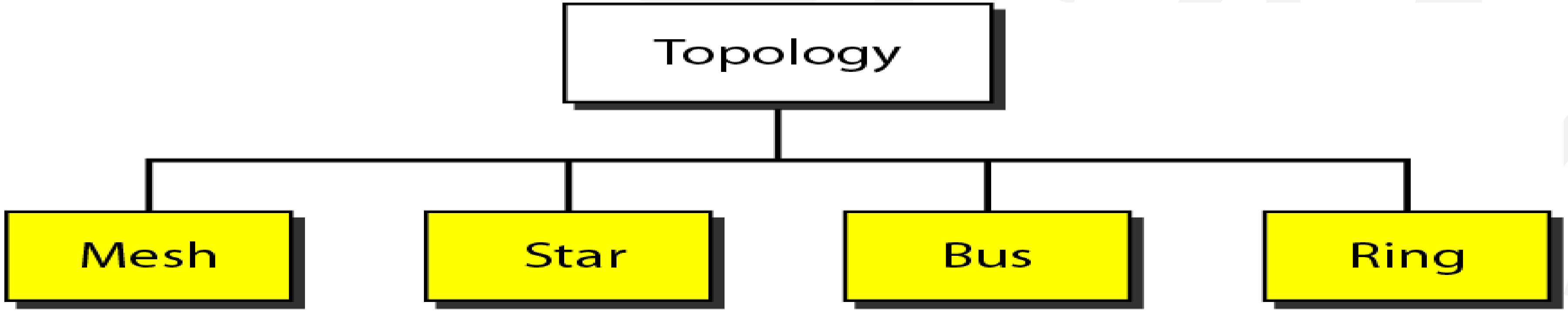
Data Communication & Network

Trainer : Sujata Mohite
Email: sujata.mohite@sunbeaminfo.com

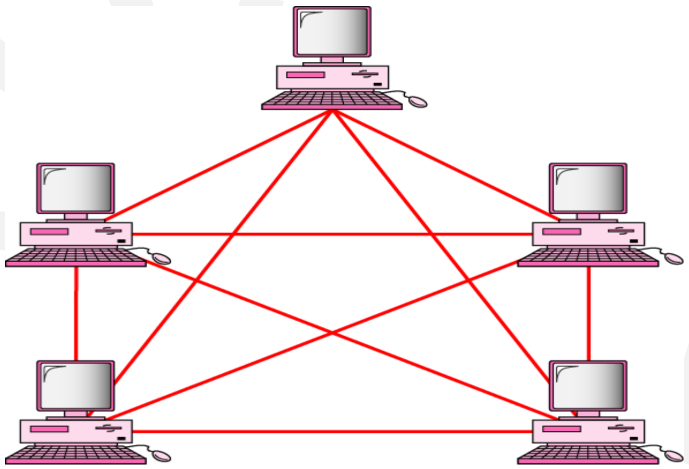
Network Physical Structure

Physical Topology

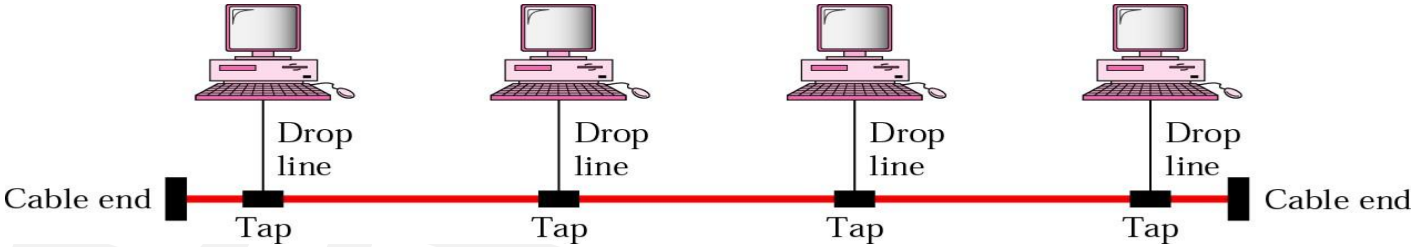
- Topology defines the way hosts are connected to the network
- The network topology defines the way in which computers, printers, and other devices are connected.
- A network topology describes the layout of the wire and devices as well as the paths used by data transmissions.
- Physical topology is the geometric representation of all the nodes in a network.



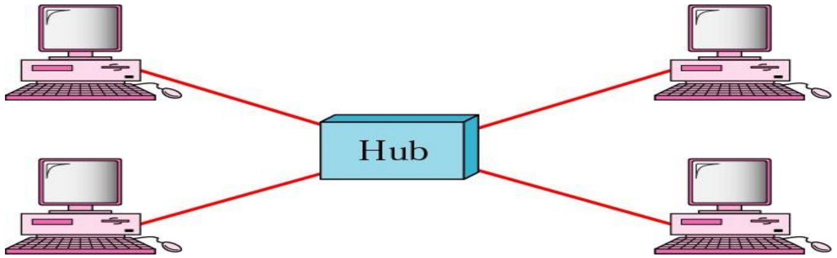
Network Topology



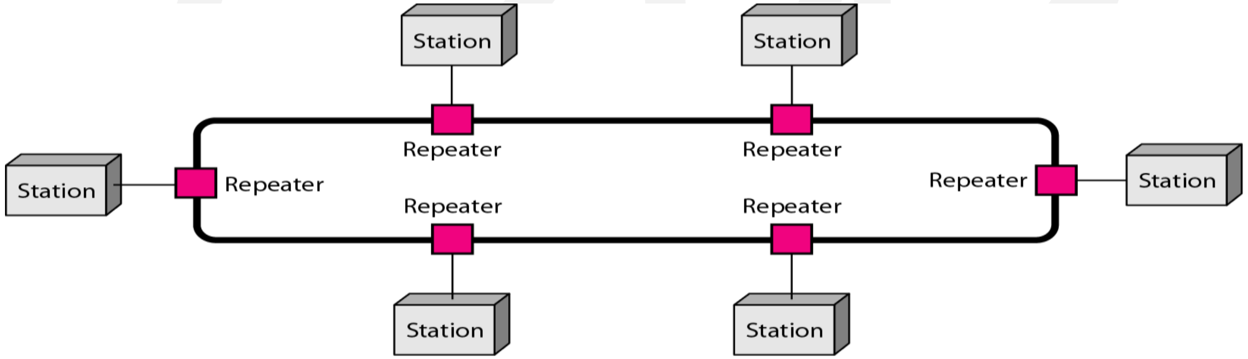
mesh



bus



star



ring

Mesh

- Mesh topology is a type of networking in which all the computers are inter-connected to each other.
- In Mesh Topology, the connections between devices take place randomly.
- The connected nodes can be computers, switches, hubs, or any other devices.
- In this topology, even if one of the connections goes down, it allows other nodes to be distributed.
- This type of topology is very costly.
- It is used for wireless networks, and its connections can be wired or wireless.
- There is a **point-to-point** connection between all nodes in the mesh topology setup.
- we have n devices in the network then each device must be connected with (n-1) devices of the network.
- Number of links in a mesh topology of n devices would be n(n-1)/2.
- It is highly reliable and robust, often used in **critical communication systems**.
- Eg: internet backbone, various internet service providers are connected to each other via dedicated channels. Also used in military communication systems and aircraft navigation systems.

Star

- Star topology, sometimes known as a star network, is a network topology in which each device is connected to a central hub.
- In this network arrangement, all devices linked to a central network device are displayed as a star.
- In star topology, all connected devices are completely dependent on the central device; the communication through the whole Computer Network fails if the central device gets any problem.
- Each node in this diagram has a direct **point-to-point** link to the central device, yet no single node can communicate directly with the others. Therefore, before reaching the destination, each message has to pass through this central device only.
- Point-to-point connection between hosts and hub.
- Coaxial cables or RJ-45 cables are used to connect the computers.
- Eg: A local area network (LAN) in an office where all computers are connected to a central hub. Also used in wireless networks where all devices are connected to a wireless access point.
- Banking system every bank is connected to the RBI.

Bus

- The bus topology is designed in such a way that all the stations are connected through a single cable known as a **backbone cable**.
- Each node is either connected to the backbone cable by drop cable or directly connected to the backbone cable.
- The configuration of a bus topology is quite simpler as compared to other topologies.
- The backbone cable is considered as a **"single lane"** through which the message is broadcast to all the stations.
- In this topology, even if one of the connections goes down, it does not affect whole network but if backbone cable is affected then whole network is affected.
- There is a **multipoint connection** between all nodes.
- The most common access method of the bus topologies is **CSMA** (Carrier Sense Multiple Access).
- This method is used to prevent the collision of data as two or more devices can send the data to main cable at the same time.
- Eg: Ethernet LAN, where all devices are connected to a single coaxial cable or twisted pair cable. Also used in cable television networks.

Ring

- Ring topology is like a bus topology, but with connected ends.
- The node that receives the message from the previous computer will retransmit to the next node.
- The data flows in one direction, i.e., it is **unidirectional**.
- The data flows in a single loop continuously known as an endless loop.
- It has no terminated ends, i.e., each node is connected to other node and having no termination point.
- The data in a ring topology flow in a **clockwise direction**.
- There is a **multipoint connection** between all nodes.
- But each system is connect in point-to-point fashion and if one system goes down then entire network will go down.
- Access method used in ring topology is **token passing method.** The word token describes segment of data send through the network. There are multiple tokens available on the network, the device that successfully acquires the token attaches the data to the token. The device that successfully decodes the token, receives the data.
- Eg: industrial control systems, telecommunications, and some security and transportation networks.

Topology

- Small home or small to medium office LANs: **Star**

- Large corporate network: **Hybrid**

- Critical systems (data centers, military), Military and Aerospace networks
  Disaster recovery and emergency systems: **Mesh**

- Simple or temporary networks, Networks with few devices and low traffic : **Bus**

- Circular flow systems, Certain industrial and telecom networks , IBM Token Ring networks: **Ring** (uncommon today)

Network Devices / Internetworking Devices

Internetworking Devices

- Internetworking devices are products used to connect networks.

- As computer networks grow in size and complexity, so the internetworking devices used to connect them.
  - Hubs
  - Repeaters
  - Bridges
  - Switches
  - Routers
  - Gateways

Hubs

- Hub is used to build a LAN.
- Common connection point for devices in a network.
- It is non intelligent device.
- It does not understand the addressing.
- Hub is Multiport repeater containing multiple ports to interconnect multiple devices
- Hubs regenerate and retime network signals (increases traffic and collision)
- They cannot filter network traffic and they cannot determine best path
- The hub contains multiple ports.
- When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.
  - does not concern about the address
  - concerns with only electrical signals
  - increases the traffic, as they broadcast data to all
  - increases the collision

Hubs

- A hub is a Layer 1 (Physical Layer) device in the OSI model that connects multiple devices in a network and broadcasts data it receives to all connected devices, regardless of the destination. especially in older or small-scale local area networks (LANs).
- When a device sends data to a hub:

1. The hub does not read the destination.
2. It sends the data to every device connected to it.
3. Only the intended recipient accepts the data; others discard it.

- Used in small home or office LANs.
- Now, replaced by switches due to better performance, security, and intelligence.

Repeaters

- A repeater is a network device used to regenerate and amplify signals in a network to extend the transmission distance.
- Works at OSI Layer 1 (Physical Layer) .
- Regenerates weak or distorted signals
- Does not filter or interpret data—just repeats it
- Repeaters are used in **Ethernet**, **Wi-Fi**, and **fiber optic** networks.
- They do **not filter traffic**, **do not understand frames**, and **cannot reduce congestion**.

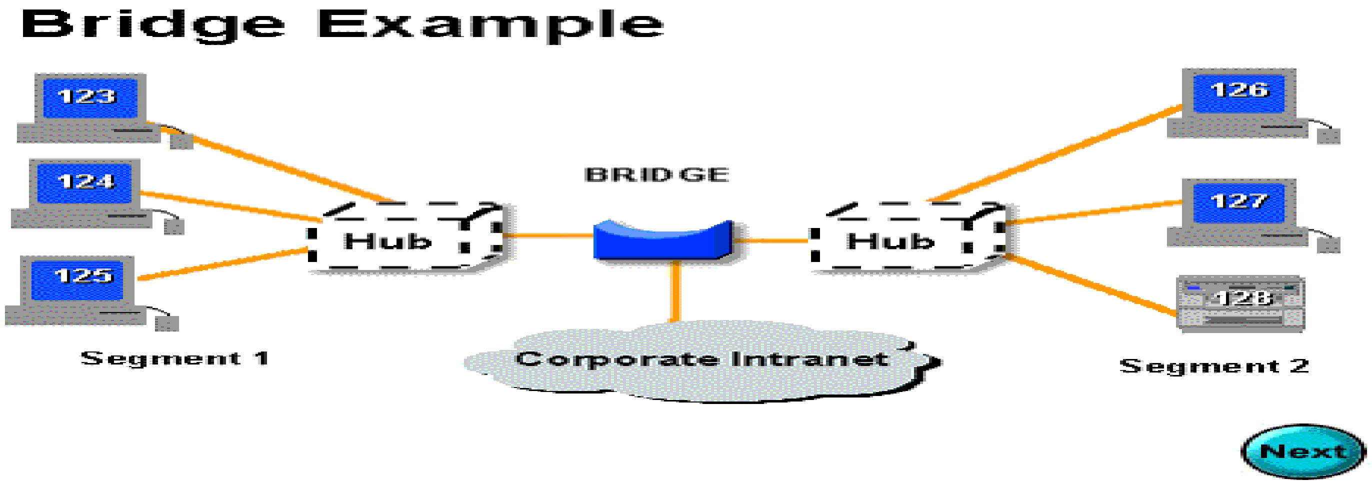
Repeaters

- **Repeaters or hubs work at the OSI physical layer to regenerate the network's signal and resend them to other segments.**
- Its job is to regenerate the signal over the same network before the signal becomes too weak or corrupted so as to extend the length to which the signal can be transmitted over the same network.
- The longer the cable length, the weaker and more deteriorated the signals become as they pass along the networking media.
- Repeaters can be installed along the way to ensure that data packets reach destination.

One way to solve the problems of too much traffic on a network and too many collisions is to use an internetworking device **called a bridge.**

Bridges : Operates at Data Link Layer

- A bridge eliminates unnecessary traffic and minimizes the chances of collisions occurring on a network by dividing it into segments .
- Device that connects and passes packets between two network segments.
- More intelligent than hub- As they analyze incoming packets and forwards (or drops) based on addressing information.(Routing Table is Build to record segment number of address)
- **Bridges work best where traffic from one segment of a network to other segments is not too great.**



However, when traffic between network segments becomes too heavy, the bridge can become a bottleneck and actually slow down communication.

Bridge

- Works at **OSI Layer 2**.
- Connects **two LAN segments**.
- Uses **MAC addresses** to filter traffic.
- Reduces collisions by dividing the network into segments.
- Similar to a switch but with **fewer ports**.
- 1. Receives a frame on one interface.
- 2. Reads the destination MAC address.
- 3. Looks up its MAC table.
- 4. Forwards, filters, or drops the frame depending on destination.

Switches (Multiport Bridges)

- **Switches operate at the Data Link layer (layer 2) of the OSI model**
- A switch is a device that is used to segment networks into sub networks called subnets. (Used to build LAN)
- **Can interpret address information**
- Uses Addressing Scheme knows as MAC Addressing.
- Switches are capable of inspecting data packets as they are received, determining the source and destination device of that packet, and forwarding it appropriately
- Switch conserves network bandwidth and offers generally better performance than a hub.
- **Switch may Broadcase , unicast or Multicast .**

Learning the MAC Addresses and forwarding to the respective machine is switching.

- Switches have
  - ASIC (Application Specific IC)
  - OS is hardcoded in microprocessor
  - So switches are hardware based.
  - Ports are unlimited

- Bridges have
  - OS is separated
  - So bridges are not used
  - Bridges are software based.
  - Limited Ports (16)

Switches

- Works at OSI Layer 2 (Data Link Layer).
- Uses MAC addresses to forward frames.
- Creates separate collision domains, reducing collisions.
- Supports **full-duplex communication.**
- Learns MAC addresses using a MAC address table.
- Faster and more efficient than hubs
- 1. Device A sends a frame to Device B through the switch.
- 2. Switch reads the source MAC address and stores it in the MAC table.
- 3. It then checks the destination MAC address in its table.
- 4. If known, it forwards the frame to the correct port.
- 5. If unknown, it floods the frame to all ports (except source), then updates its table once the destination responds.

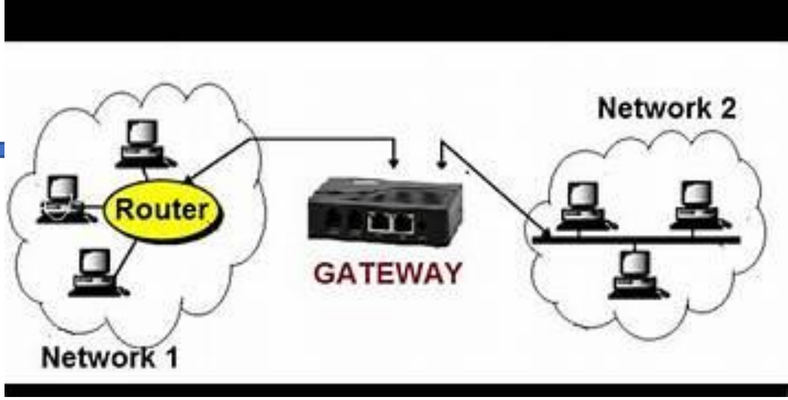
Routers

- Used to build WAN
- Router connect multiple networks and route the packets.
- Uses IP Address to identify every machine uniquely.
- Routers are used to connect two or more networks. For routing to be successful, each network must have a unique network number
- Routers have the ability to make intelligent decisions as to the best path for delivery of data on the network.
- **They use the "logical address" of packets and routing tables to determine the best path for data delivery**
- To determine the **best path**, routers communicate with each other through **routing protocols**
- The four most common routing protocols:
  - RIP (Routing Information Protocol) for IP
  - OSPF (Open Shortest Path First) for IP
  - EIGRP (Enhanced Interior Gateway Routing Protocol) for IP, IPX, and AppleTalk
  - BGP (Border Gateway Protocol) for IP

Router

- Works at OSI Layer 3 (Network Layer).
- Uses IP addresses to route packets across networks.
- Connects different networks (LAN to WAN, LAN to LAN).
- Chooses best path using routing protocols (e.g., RIP, OSPF).
- Supports NAT, firewall functions, and packet filtering.
- 1. Receives packet from a connected network (e.g., from a LAN device)
- 2. Reads destination IP address
- 3. Looks up routing table to find the best route
- 4. Forwards the packet to the next hop (another router or the destination network)
- Connects home networks to the internet ,Links multiple office networks, Routes traffic between different subnets in large organizations, Powers internet backbone infrastructure

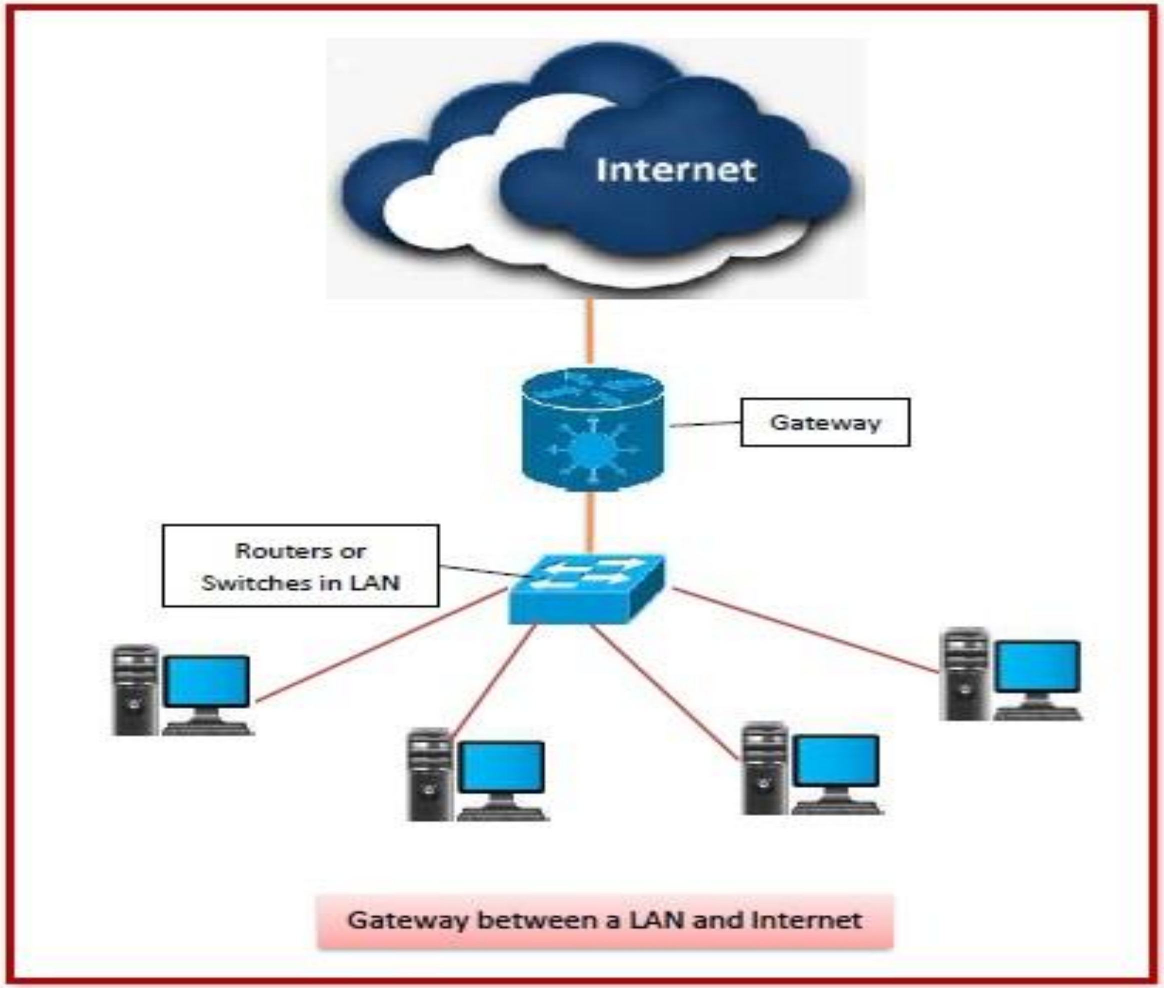
Gateways



- Device that connects dissimilar networks.
- Operates at the highest level of abstraction.
- Expands the functionality of routers by performing data translation and protocol conversion.
- Establishes an intelligent connection between a local network and external networks with completely different structures.
- Gateways serve as an entry and exit point for a network as all data must pass through or communicate with the gateway prior to being routed.
- If a network wants to communicate with devices, nodes or networks outside of that boundary, they require the functionality of a gateway.
- A gateway is often characterized as being the combination of a router and a modem.

Gateways

- A gateway is a network node that forms a passage between two networks operating with different transmission protocols.
- **It operates at all layers of the OSI model but is most commonly associated with the Network Layer (Layer 3).**
- However, depending upon the functionality, a gateway can operate at any of the seven layers of OSI model.
- It **acts as the entry – exit point** for a network since all traffic that flows across the networks should pass through the gateway..



Gateways

- Protocol Conversion Converts data between different communication protocols (e.g., IPv4 ↔ IPv6, TCP/IP ↔ AppleTalk).
- Network Translation Bridges networks using different architectures or formats.
- Application Gateway Security Control Translates data between different application protocols (e.g., email, VoIP). Acts as a security checkpoint, often integrating firewalls or proxies.
- Routing/Forwarding Forwards packets between networks (like a router, but with added conversion).
- Home Network to Internet Example Your home router functions as a gateway between your LAN and the Internet.
- Email Communication VoIP and PSTN Integration A mail gateway translates between different email systems.

Address Resolution Protocol (ARP)

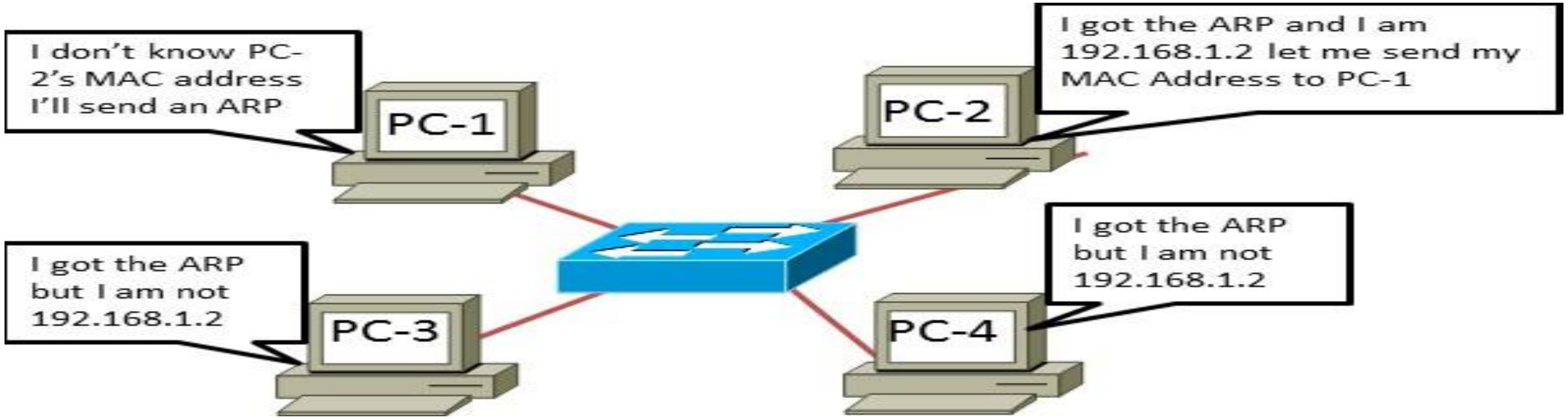
ARP

- Address resolution refers to the process of finding an address of a computer in a network.
- The address is "resolved" using a protocol in which a piece of information is sent by a client process executing on the local computer to a server process executing on a remote computer.
- The address resolution procedure is completed when the client receives a response from the server containing the required address.
- The job of the ARP is essentially to translate 32-bit addresses to 48-bit addresses and vice-versa.
- This protocol works between layer 2 and layer 3 of the OSI model.
- The MAC address resides at layer 2, which is also known as the data link layer and IP address resides at layer 3, this layer is also known as the network layer.

ARP

- Step1 : ARP Broadcast
  - Note: Broadcast is received by everyone and processed by everyone.
- Step 2: ARP Reply
- Step 3 : Actual Data Transfer

- Router creates an ARP Request message to be sent to all hosts on the subnet.
- Address resolution protocol message asks “Who has specified IP address ?”
- Passes ARP request to data link layer process for delivery


I don’t know PC-2’s MAC address I’ll send an ARP
PC-1
I got the ARP and I am 192.168.1.2 let me send my MAC Address to PC-1
PC-2
I got the ARP but I am not 192.168.1.2
PC-3
I got the ARP but I am not 192.168.1.2
PC-4

ARP

- **ARP stands for Address Resolution Protocol.**
- Works at **OSI Layer 2 & Layer 3 boundary**.
- Used to **map an IP address (Layer 3) to a MAC address (Layer 2)**.
- Essential for communication inside a **local network (LAN)**.
- When a device wants to send data to an IP address, it must know the **MAC address** → ARP is used
- Device checks its **ARP cache** for the MAC address.
- If not found, it sends an **ARP Request** (broadcast).
- The device with that IP sends an **ARP Reply** (unicast).
- Sender stores the info in its **ARP table/cache**.

Protocol

Protocol and Standards

- ***Protocols define the format and order of messages sent and received among network entities, and actions taken on message transmission and receipt.***

□ A protocol defines what, how, when it communicated.

□ **The key elements of a protocol :**

  □ **syntax :** structure and format of the information data(what can be communicated)

  □ **Semantics:** meaning of each section of bits. an route identify the route to be taken or the final destination of the message(how it can be communicated)

  □ **Timing(synchronization):** when data should be sent and how fast it should be sent(when and at what speed it can be communicated)

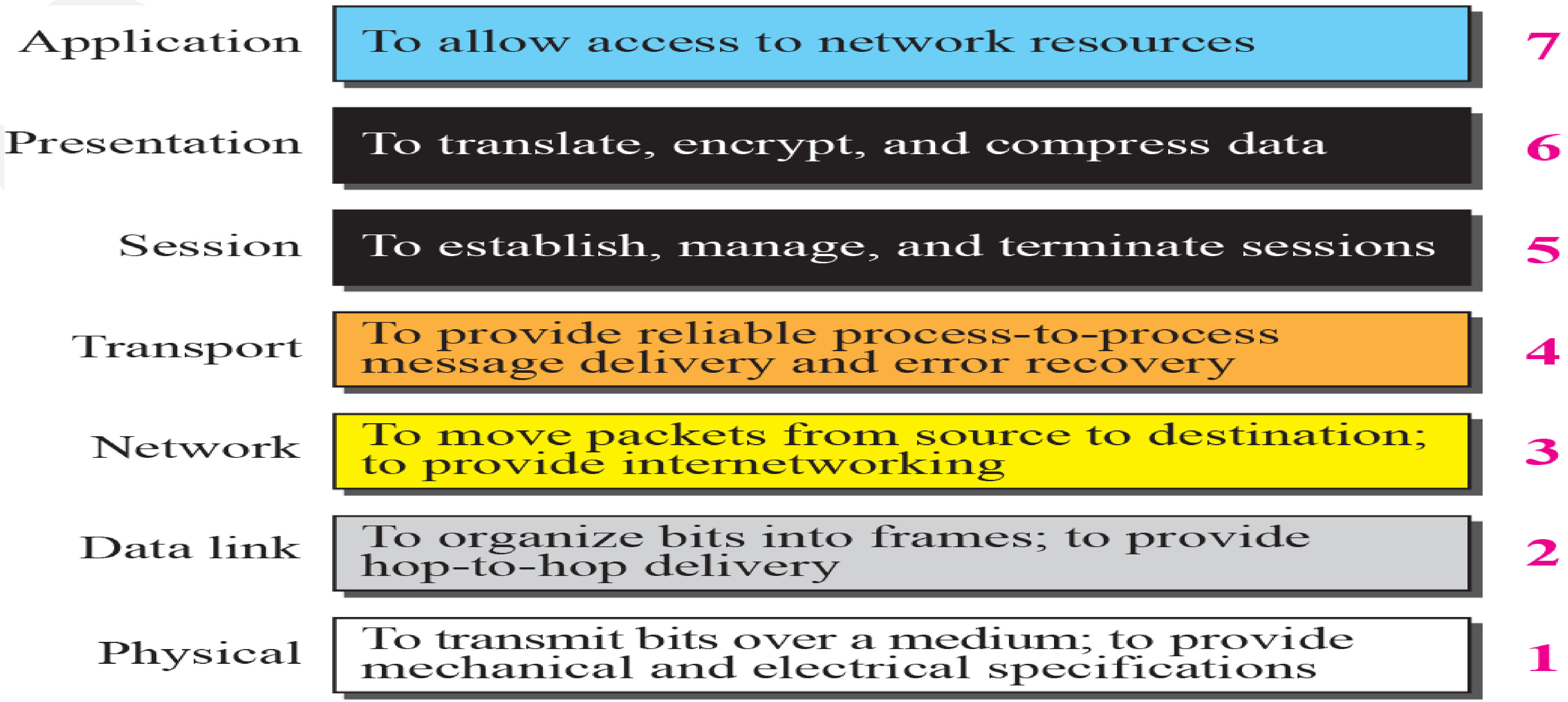
Standards

- Standards are developed by cooperation among standards creation committees, forums, and government regulatory agencies.
- Standards Creation Committees
  1. International Organization for Standardization (ISO)
  2. International Telecommunications Union (ITU)
  3. American National Standards Institute (ANSI)
  4. Institute of Electrical and Electronics Engineers (IEEE)

OSI Model & Layers

- Established in 1947, **International Organization for Standardization (ISO)** is a multinational body dedicated to worldwide agreement on international standards.
- We cannot see standard but we can represent them.
- An ISO standard that covers all aspects of network communications is the **Open Systems Interconnection (OSI)** model.
- OSI model is now considered the primary Architectural model for inter-computer communications.
- **Term "open" denotes the ability to connect any two systems which conform to the reference model and associated standards.**

OSI Layers



Application	To allow access to network resources	7
Presentation	To translate, encrypt, and compress data	6
Session	To establish, manage, and terminate sessions	5
Transport	To provide reliable process-to-process message delivery and error recovery	4
Network	To move packets from source to destination; to provide internetworking	3
Data link	To organize bits into frames; to provide hop-to-hop delivery	2
Physical	To transmit bits over a medium; to provide mechanical and electrical specifications	1

OSI Layers

Q. UDP packets have a fixed-size header of ___ bytes.
A. 16
B. 8
C. 40
D. 20
Ans: B

Q. The IPv4 header size _______
A. is 20 to 60 bytes long
B. is always 20 bytes long
C. is always 60 bytes long
D. depends on the MTU
Ans: A

Application Layer

- Interacts with application programs and is the highest level of OSI model.
- contains management functions to support distributed applications.
- enables the user, whether human or software, to access the network
- Examples : browser , applications such as file transfer, electronic mail, remote login etc.
- Protocols
    - http [80]: hyper text transfer protocol
    - https [443]: secure hyper text transfer protocol
    - ftp [20/21]: file transfer protocol
    - Smtp (25) : simple mail transfer protocol
    - Pop3 (110) : post office protocol
    - telnet(23) : used to connect to the remote machine
    - ssh [22]: secure shell
    - dns (53) : domain name service (used to get the IP address from the domain name)

Presentation Layer

Translation

- On sender side : translates from ASCII to EBDIC (Extended Binary Coded Decimal Interchange Code)
- On receiver side: translates from EBDIC to ASCII

Encryption/Decryption

- Plain Text to Cipher Text
- Algorithms : RSA, SHA

Compression / Decompression

- Sender Side : Compression
- Receiver Side : Decompression

Data Representation [Content-type] (Used to Decide Common File Formats)

- For text (plain: text/plain , html: text/html , json: application/json , xml: text/xml)
- For image (bmp: image/bmp , png: image/png, jpg: image/jpg , jpeg: image/jpeg)
- For audio & Video (wave: audio/wav, mp3: audio/mp3, mp4: video/mp4, fllv: video/flv

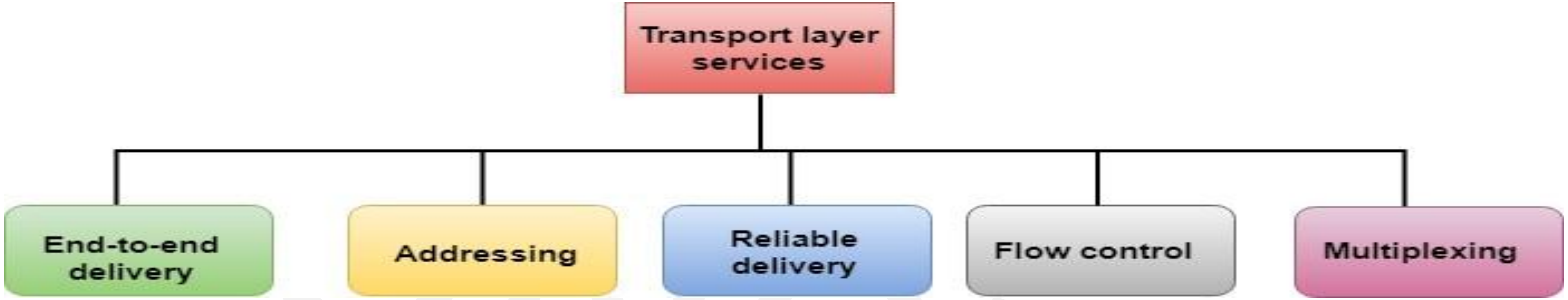
Session Layer

- **To start/manage/terminate the session.**
  - how to start, control and end conversations (called sessions) between applications.
  - log-on or password validation is also handled by this layer.
- **The session layer is the network *dialog controller.***
  - mechanism for controlling the dialogue between the two end systems and synchronization.
  - Allows the communication between two processes to take place in either half duplex (one way at a time) or full-duplex (two ways at a time) mode.
- **Synchronization**
  - Session layer can also provide check-pointing mechanism such that if a failure of some sort occurs between checkpoints, all data can be retransmitted from the last checkpoint.
  - It establishes, maintains, and synchronizes the interaction among communicating systems.
- **Protocols**
  - SIP: session initiation protocol
  - NetBIOS : Network Basic Input Output Service
  - RPC: Remote Procedure Call

Transport Layer

- Most Important Layer of OSI
- Responsible **for process-to-process/ End to End delivery** of the entire message.
- Provide a reliable mechanism for the **exchange of data between two processes** in different computers.
- Segment
  - smaller part of session PDU
  - every segment contains sequence number
  - every segment contains checksum for error checking
  - Segment contains:
    - **data** (from the session layer PDU)
    - **sequence number** : used for re-assembling the segments on the receiver machine
    - **checksum :** used to check if the data is not damaged

Responsibilities of Transport Layer



Transport layer services

End-to-end delivery

Addressing

Reliable delivery

Flow control

Multiplexing

End –to-End delivery

- The transport layer transmits the entire message to the destination

Addressing

- The transport layer provides the user address which is specified as a station or port.

Reliable delivery

- provides reliability services by retransmitting the lost and damaged packets
- Error control, sequence control, loss control, duplicate control.

Error Control

- performs the checking for the errors end-to-end to ensure that the packet has arrived correctly.

Flow Control

- Flow control is used to prevent the sender from overwhelming the receiver.
- If the receiver is overloaded with too much data, then the receiver discards the packets & ask for retransmission of packets.

Multiplexing

- uses the multiplexing to improve transmission efficiency.

Transport Layer Protocol

TCP

- Transmission Control Protocol (Reliable)
- connection oriented protocol
  - connection will be kept alive till the data transfer in progress
- flow control, error checking and sequencing
- slower than UDP
- E.g. Email (no data loss)

UDP

- User Datagram Protocol (Unreliable)
- Connection Less Protocol
- does not provide error checking/ flow control
- Faster than TCP because no ACK only sending of data packets
- E.g: Online Games, Streaming

User DatagramProtocol(UDP)

UDP (User Datagram Protocol) is a lightweight, **connectionless transport layer protocol** in the TCP/IP model used to send messages (called datagrams) without establishing a connection.

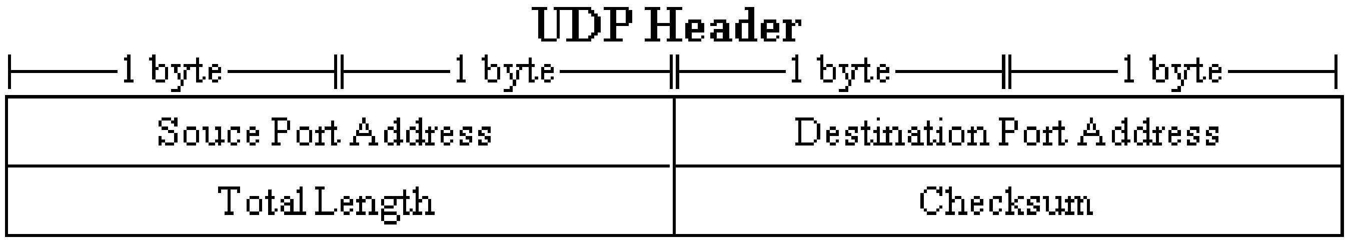
UDP is used in applications where **speed is more important than reliability**:
Eg: Online Gaming, Streaming (live video/audio), Broadcast/Multicast(Can send to many recipients at once)

Feature	**Description**
Connectionless	No need to establish a connection before sending data.
No Acknowledgments	Sender doesn't wait for the receiver to confirm receipt.
Faster than TCP	Minimal overhead makes it ideal for time-sensitive data.
No Error Correction	If data is lost or corrupted, it’s not retransmitted.
Supports Broadcasting	Can send to multiple devices at once.

UDP Header Format(8 Bytes)

Field	**Size (bits)**	**Description**
Source Port	16	Port of sending application
Destination Port	16	Port of receiving application
Length	16	Total length of UDP header + data
Checksum	16	Optional integrity check

UDP = Fast, simple, and connectionless
Best for **real-time apps** where **speed matters more than reliability**.



UDP Header

1 byte | 1 byte | 1 byte | 1 byte

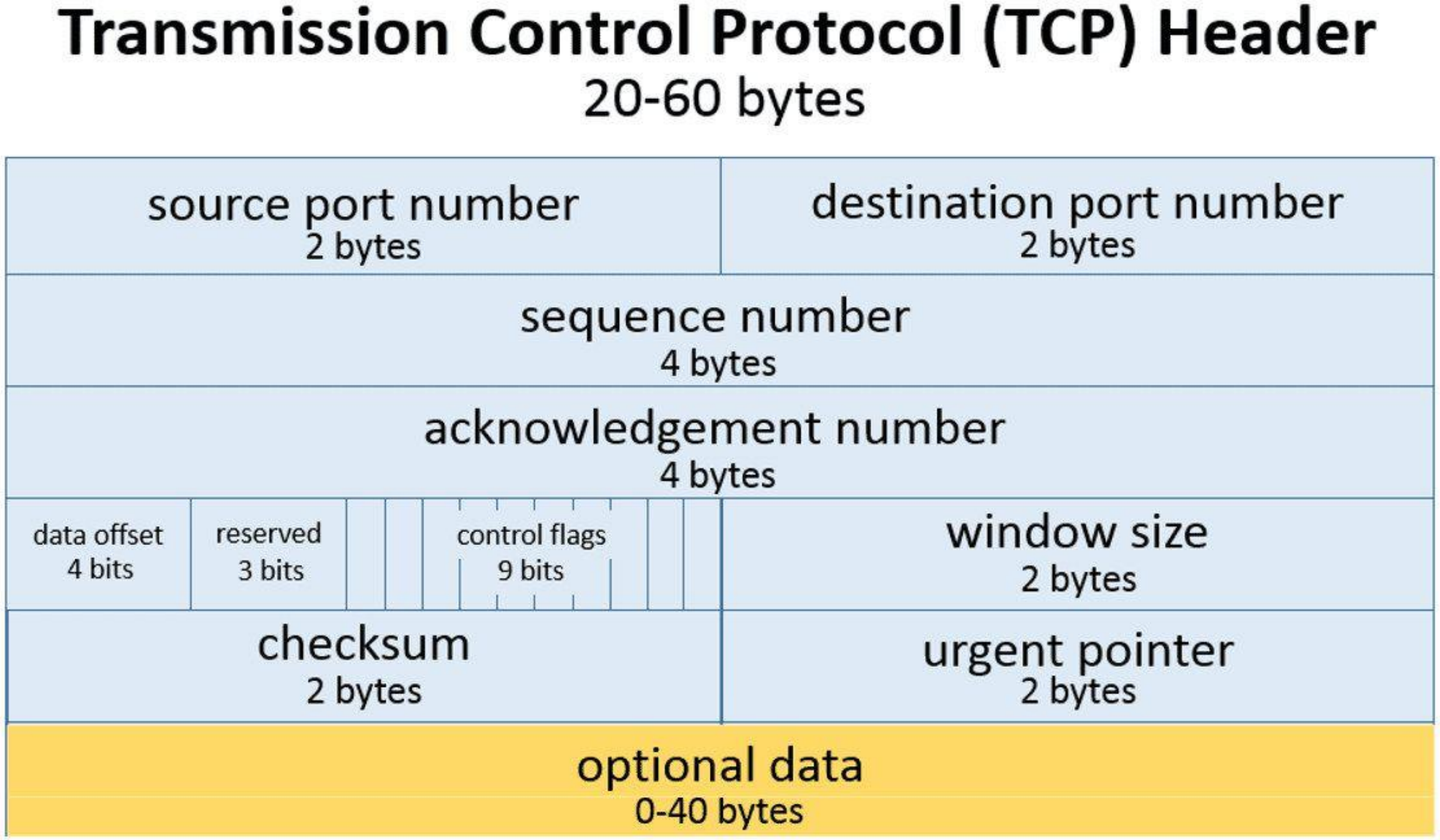
Souce Port Address	Destination Port Address
Total Length	Checksum

Transmission Control Protocol (TCP):

- TCP is a reliable **connection-oriented protocol** that can be used in any application where reliability is important.
- TCP explicitly defines to provide a connection establishment, data transfer, and connection teardown phases to provide a connection-oriented service.
- TCP connections are **full-duplex**
- TCP uses GBN and SR protocols to attain reliability. Therefore it has selective acknowledgment.
- It provides end-to-end communication due to the port number of source and destination.
- TCP connections are **byte streams.**

- TCP includes a checksum field in its header.
- It checks both the header and data for errors.
- It's one of the reasons why TCP is considered reliable
- Connection-Oriented, Reliable Data Transfer**,** Error Checking, Flow Control, Congestion Control,
- Byte-Oriented Protocol

TCP Header Format (20–60 bytes)



Transmission Control Protocol (TCP) Header

20-60 bytes

source port number
2 bytes

destination port number
2 bytes

sequence number
4 bytes

acknowledgement number
4 bytes

data offset
4 bits

reserved
3 bits

control flags
9 bits

window size
2 bytes

checksum
2 bytes

urgent pointer
2 bytes

optional data
0-40 bytes

TCP Header Format (20–60 bytes)

Field	Size (bits)	Description
Source Port	16	Port number of the sender.
Destination Port	16	Port number of the receiver.
Sequence Number	32	Number assigned to the first byte of data in this segment. Used for data ordering.
Acknowledgment Number	32	If the ACK flag is set, this field indicates the next expected byte.
Data Offset (Header Length)	4	Specifies the size of the TCP header (in 32-bit words).
Reserved	3	Reserved for future use.
Flags (Control Bits)	9	Includes control bits like SYN, ACK, FIN, RST, PSH, URG, etc.
Window Size	16	Size of the receive window (flow control).
Checksum	16	Error-checking for header + data.
Urgent Pointer	16	Indicates if urgent data is present (used with URG flag).
Options	Variable (0–40 bytes)	Used for things like window scaling, timestamps, etc.
Data	Variable	The actual payload being transmitted.

TCP Header Format (20–60 bytes)

Flag	Meaning
SYN	Start of a connection
ACK	Acknowledgment
FIN	Graceful connection termination
RST	Reset the connection
PSH	Push data to the application immediately
URG	Urgent pointer field is valid

Transmission Control Protocol (TCP):

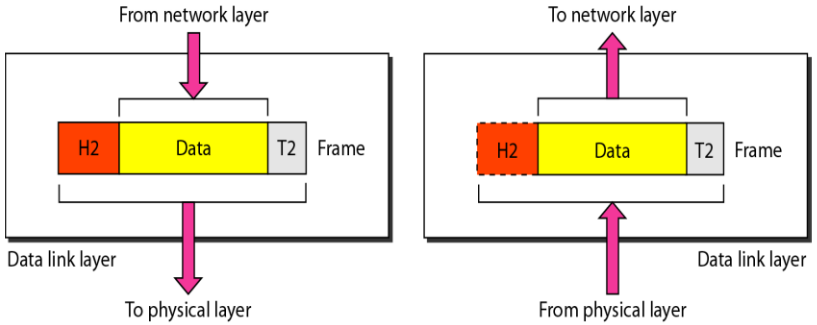
- **Web browsing**: HTTP/HTTPS
- **Email**: SMTP, POP3, IMAP(Reading mail from server)
- **File transfer**: FTP, SFTP
- **Remote access**: SSH, Telnet

Network Layer

- The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links).
- It determines the route from the source to the destination and also manages the traffic problems such as switching, routing and controls the congestion of data packets.
- Segment Contains :
  - data
  - source IP address
  - destination IP address
- **Network Layer Responsibilities:**
  - Logical Addressing : The network layer translates the logical addresses into physical addresses
  - Routing : sending the data across the network
  - Internetworking : provides the logical connection between different types of networks
  - Fragmentation : breaking the packets into the smallest individual data units that travel through different networks.
- **Protocols :**
  - IP : internet protocol
  - IPx : internetwork packet exchange
  - ICMP : Internet Control Messaging Protocol
  - NAT : Network Address Translation
  - ARP : Address Resolution Protocol
  - PPP: Point to Point Protocol
- **Device** : Router

Data Link Layer

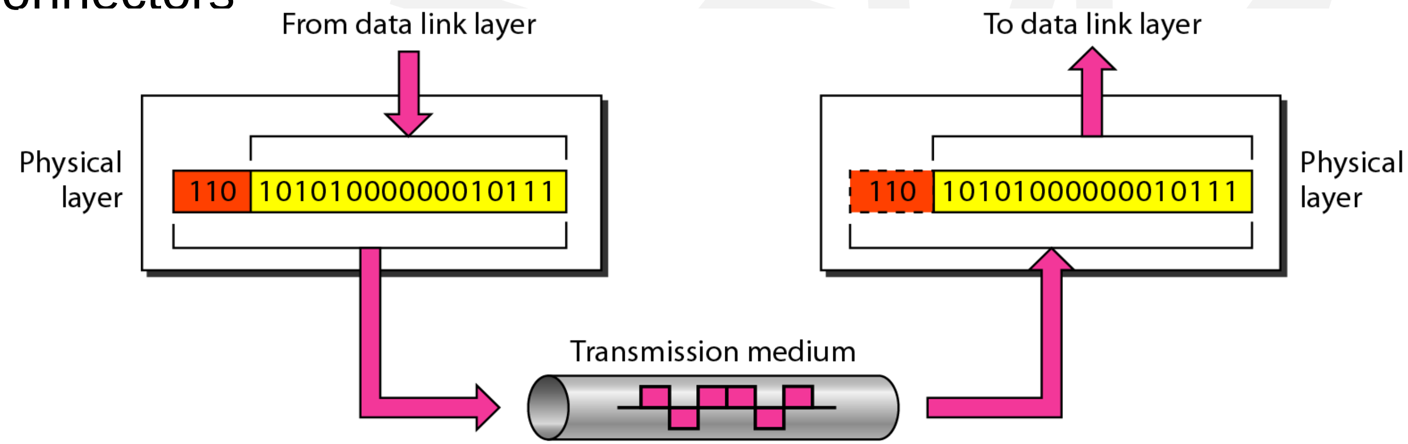
- Data link layer attempts to provide reliable communication over the physical layer interface.
- **DATA LINK Layer Responsibilities :**
  - **Framing:**
    - Breaks the outgoing data into frames and reassemble the received frames.
    - every frame contains (Source MAC address and Destination MAC address)
  - **Physical Addressing:**
    - uses MAC address to identify every NIC uniquely
  - **Flow Control:**
    - A flow control mechanism to avoid a fast transmitter from running a slow receiver by buffering the extra bit is provided by flow control. This prevents traffic jam at the receiver side.
  - **Error Control:**
    - Error control is achieved by adding a trailer at the end of the frame. Duplication of frames are also prevented by using this mechanism. Data Link Layers adds mechanism to prevent duplication of frames.
  - **Access Control:**
    - Protocols of this layer determine which of the devices has control over the link at any given time, when two or more devices are connected to the same link.



- **Protocols**
  - ARP(Address Resolution Protocol) : getting physical address from logical address
  - RARP: Reverse Address Resolution Protocol
- **Device :** Switch

Physical Layer

- Provides physical interface for transmission of information.
- Covers all - mechanical,electrical,functional and procedural - aspects for physical communication. Characteristics like voltage levels, timing of voltage changes, physical data rates, etc.
- send data in the form of 1’s and 0’s.
- senders and receivers clock must be synchronized.
- **Transmission mode:**
  - Defines direction of transmission simplex, half duplex and full duplex
- **Devices:**
  - NIC , Cables , hubs , repeaters , connectors



7 Layers of OSI Model

A **PDU (Protocol Data Unit)** is the **formatted block of data** that is exchanged between devices at **each layer** of the OSI or TCP/IP networking model.

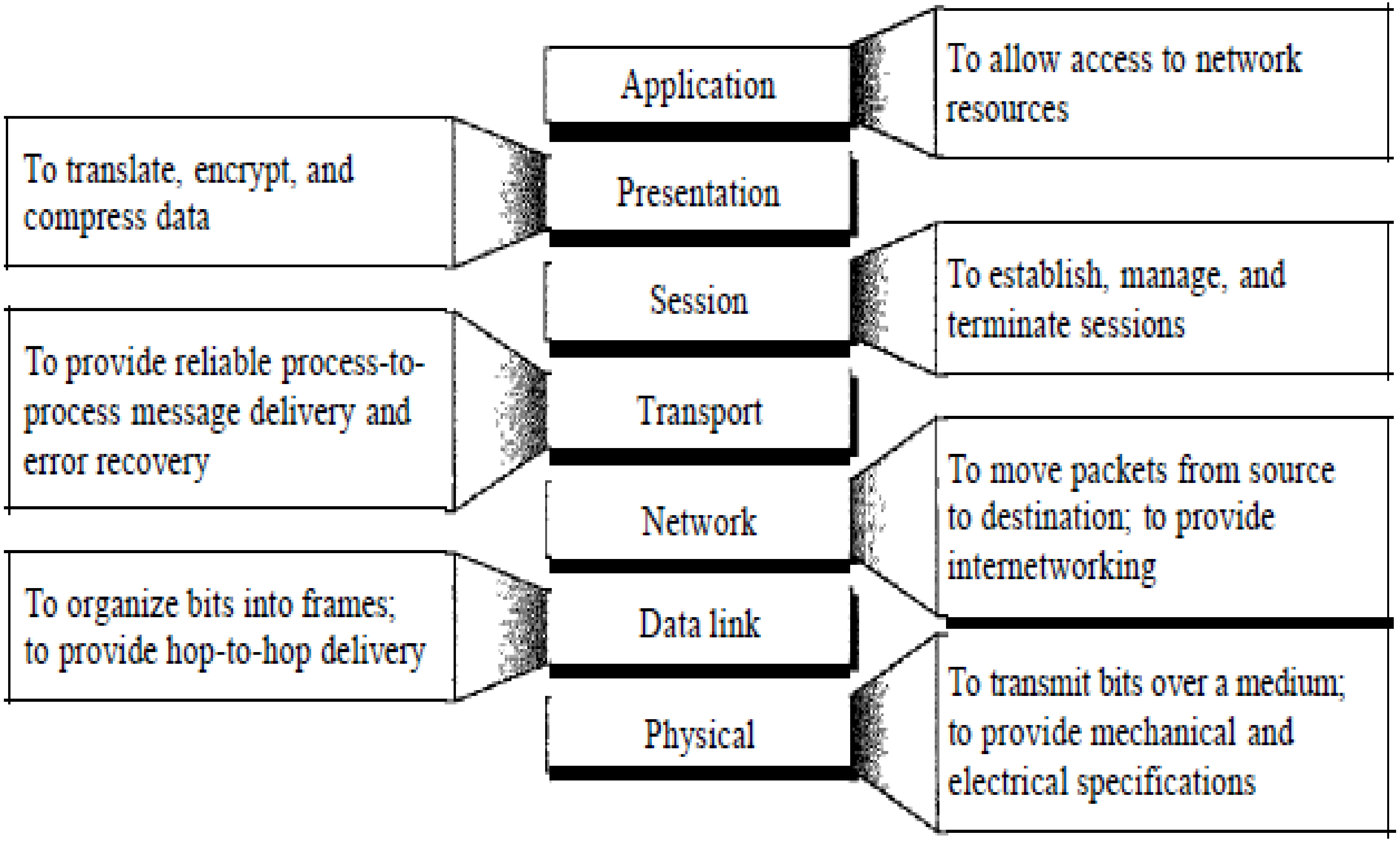
It helps define **how data is packaged** at each layer
Essential for understanding **encapsulation** and **data flow**
Helps network professionals troubleshoot which layer a problem occurs in

Example: Sending a Message via TCP/IP
Let's say you're sending a message through a web browser:
Application Layer: Message is created → **Data**
Transport Layer: Adds TCP header → **Segment**
Network Layer: Adds IP header → **Packet**
Data Link Layer: Adds MAC header → **Frame**
Physical Layer: Frame becomes electrical signals → **Bits**
Each new PDU **encapsulates** the one before it.

7 Layers of OSI Model

Application **(PDU : Data)**	• End user Layer • HTTP, FTP, IRC, SSH, DNS
Presentation **(PDU : Data)**	• Syntax Layer • SSL, SSH, IMAP, FTP, MPEG, JPEG
Session **(PDU : Data)**	• Synch and Send to port • API's, Sockets
Transport **(PDU : Segment)**	• End to end Connections • TCP , UDP
Network **(PDU : Packet)**	• Packets • IP, ICMP, IPSec, IGMP
Data Link **(PDU : Frame)**	• Frames • Ethernet, PPP. Switch, Bridge
Physical **(PDU : Bits)**	• Physical Structure • Coax, Fiber, Wireless, Hubs, Repeaters

Summary of layers



Application
To allow access to network resources
Presentation
To translate, encrypt, and compress data
Session
To establish, manage, and terminate sessions
Transport
To provide reliable process-to-process message delivery and error recovery
Network
To move packets from source to destination; to provide internetworking
Data link
To organize bits into frames; to provide hop-to-hop delivery
Physical
To transmit bits over a medium; to provide mechanical and electrical specifications

TCP/IP Model

- The **TCP/IP model** (also called the **Internet Protocol Suite**) is a conceptual framework used to describe how data is transmitted over networks, including the internet.
- It is the foundation of internet communication.

- The TCP/IP model defines how data travels from one device to another over a network.
- It's practical and closely reflects real-world protocols used today.
- TCP/IP is the backbone of the internet and most modern networks.
- **DNS** is like the **phonebook of the internet** — it translates **human-friendly domain names** (like www.google.com) into **IP addresses** (like 142.250.72.68) that computers use to identify each other on the network.

Protocol	Purpose	Direction
SMTP (Simple Mail Transfer Protocol)	Sends email	Outgoing
IMAP (Internet Message Access Protocol)	Reads/stores email on server	Incoming
POP3 (Post Office Protocol version 3)	Downloads email to device	Incoming

TCP/IP Model

Layer	Protocol Examples	Description
4. Application Layer	HTTP, FTP, DNS, SMTP	Provides services directly to user applications.
3. Transport Layer	TCP, UDP	Ensures reliable or fast delivery of data between devices.
2. Internet Layer	IP, ICMP, ARP	Handles addressing and routing of data across networks.
1. Network Access Layer	Ethernet, Wi-Fi	Deals with physical transmission of data over hardware.

TCP/IP Model

When data is sent using TCP/IP,

[IP Header] [TCP Header] [Data Payload]

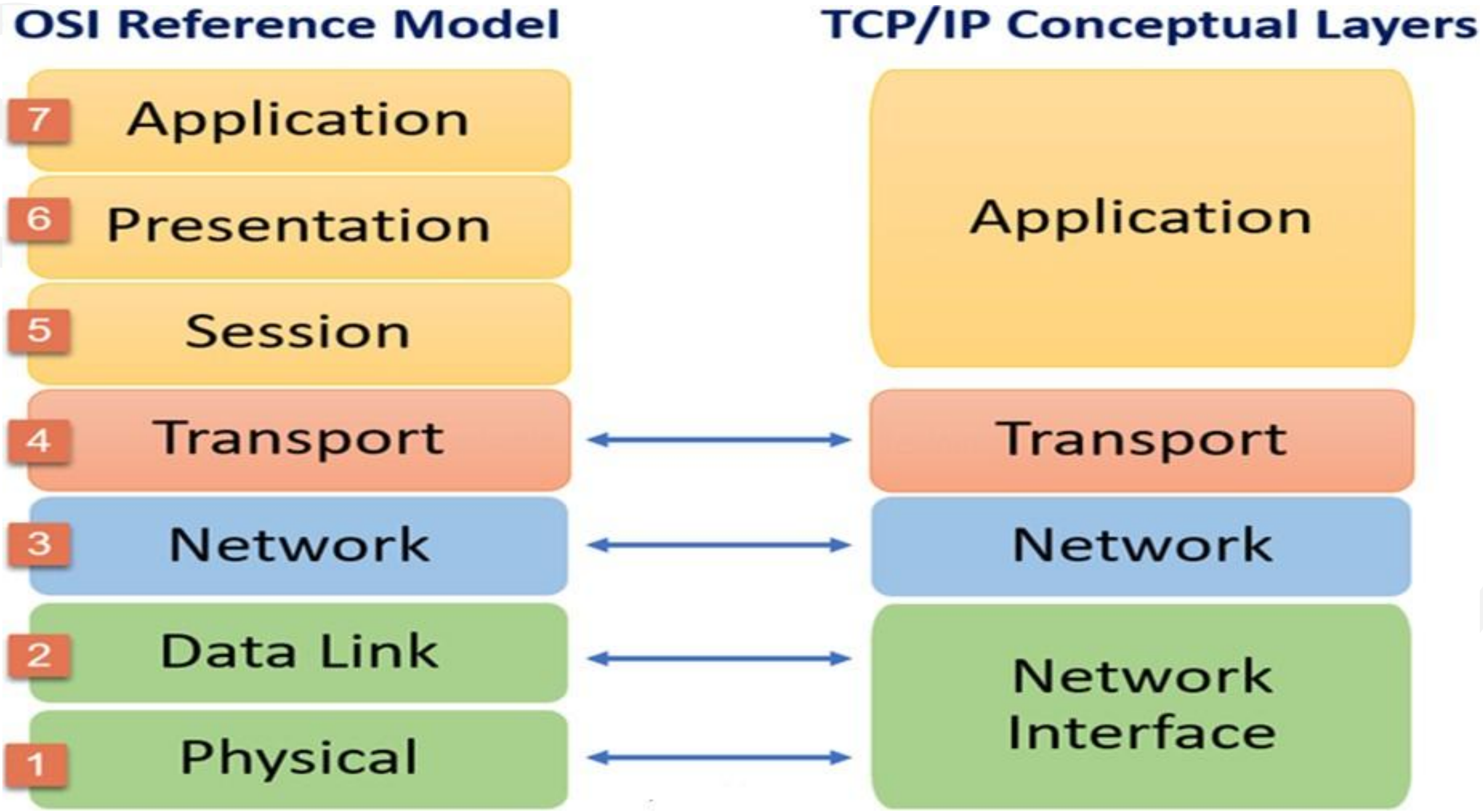
- The IP header handles addressing and routing.
- The TCP header handles connection, reliability, and sequencing.
- The Payload is your actual data (e.g., a webpage or file).

Feature	DNS	DHCP
Stands for	Domain Name System	Dynamic Host Configuration Protocol
Function	Resolves domain names to IPs	Assigns IPs to devices
Client uses	To find servers	To get network config

OSI and TCP/IP Model

- OSI model is a generic model that is based upon functionalities of each layer. TCP/IP model is a protocol-oriented standard.
- OSI model distinguishes the three concepts, namely, services, interfaces, and protocols. TCP/IP does not have a clear distinction between these three.
- OSI model gives guidelines on how communication needs to be done, while TCP/IP protocols layout standards on which the Internet was developed. So, TCP/IP is a more practical model.
- In OSI, the model was developed first and then the protocols in each layer were developed. In the TCP/IP suite, the protocols were developed first and then the model was developed.
- The OSI has seven layers while the TCP/IP has four layers.

OSI and TCP/IP Model



OSI and TCP/IP Model

Q. A _____ is a connecting device that operates in all five layers of the internet model or seven layers of OSI model.
a. Repeater
B. Bridge
C. Router
D. Gateway
Ans: D

Q. A ________ regenerates a signal, connects segments of a LAN, and has no filtering capability.
A. Repeater
B. Bridge
C. Router
D. Gateway
Ans: A

Q. Which topology requires a central controller or hub?
A. Mesh
B. Star
C. Bus
D. Ring
Ans: B

Protocols

	Protocol	Full Form	Description
1	SSH	Secure Shell	Secure remote login and command execution
2	FTP	File Transfer Protocol	Transfers files with authentication; supports control and data channels
3	TFTP	Trivial File Transfer Protocol	Simple, no-auth file transfer (often used in booting)
4	SNMP	Simple Network Management Protocol	Manages and monitors network devices
5	HTTP	Hypertext Transfer Protocol	Used for accessing websites (non-secure)
6	HTTPS	HTTP Secure	Secure version of HTTP using TLS/SSL
7	NTP	Network Time Protocol	Syncs clocks across networks
8	DNS	Domain Name System	Translates domain names to IP addresses
9	DHCP/BOOTP	Dynamic Host Configuration Protocol / Bootstrap Protocol	Automatically assigns IP addresses and configs to devices
10	APIPA	Automatic Private IP Addressing	Assigns IP when DHCP fails (range: 169.254.x.x)

Thank You!!