



Technical Campus

योग: कर्मसु कौशलम्
IN PURSUIT OF PERFECTION



**SCHOOL OF ENGINEERING
AND TECHNOLOGY**

Computer Networks and Internet Protocol (IOT208)

By: Dr. Divya Agarwal

Course Overview:

- This course deals with fundamentals of computer networks and Internet protocols. It addresses various network models, Data link protocols, network layer protocols and implementation of computer network models and OSI layers. The course also deals with Transport layer protocols. The main emphasis of this course is on the organization and management of networks and internet protocols.

Course Objective:

- To implement a simple LAN with hubs, bridges and switches.
- To describe how computer networks are organized with the concept of layered approach.
- To demonstrate internet protocols using the modern tools of computer networks.
- To Design and implement a network for an organization.

Course Outcomes (CO):

- CO1: Understand concepts of computer networks and various Internet protocols.
- CO2: Analyse given data segments/packets/frames and protocols in various layers of computer networks.
- CO3: Design real networks using state of art components using simulation tools.
- CO4: Design and implement a network for an organization.

Syllabus Contents

• UNIT- I

❑ **Introduction to Layered Network Architecture-** What are computer networks, Layered models for networking, different types of communication models, ISO-OSI Model, TCP/IP.

• UNIT II

❑ **Data Link Protocols-** Stop and Wait protocols, Noise-free and Noisy Channels, Performance and Efficiency, Sliding Window protocols, MAC Sublayer: The Channel Allocation problem, Carrier Sense Multiple Access Protocols, Collision Free Protocols, FDDI protocol. IEEE Standard 802.3 & 802.11 for LANs and WLANs

Syllabus Contents

• UNIT- III

❑ **Network Layer protocols-** Design Issues: Virtual Circuits and Datagrams, Routing Algorithms, Optimality principle, shortest path routing Algorithms, Flooding and Broadcasting, Distance Vector Routing, Link State Routing, Flow-Based Routing, Multicast Routing; Flow and Congestion Control.

• UNIT IV

❑ **Transport Layer Protocols-** Design Issues, Quality of Services. The Internet Transport Protocols. IPV4 vs IPV6. Session Layer protocol: Dialog Management, Synchronization, Connection Establishment. Quality of service, security management, Firewalls. Application layer protocols: HTTP, SMTP, FTP, SNMP, Etc.

Unit 1

Introduction to Layered Network Architecture

DATA COMMUNICATIONS

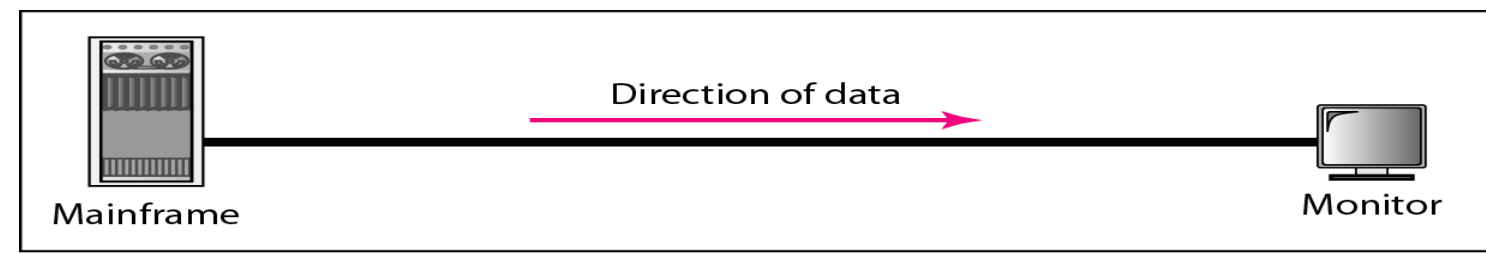
- Telecommunication means communication at a distance.
- Word data refers to information presented in whatever form is agreed upon by parties creating and using data.
- **Data communications** refers to exchange of data between two devices via some form of transmission medium such as a wire cable or wireless.
 - ❑ Delivery → Correct destination
 - ❑ Accuracy → Accurate data
 - ❑ Timelines → Real-time transmission
 - ❑ Jitter → Uneven delay

Data Representation

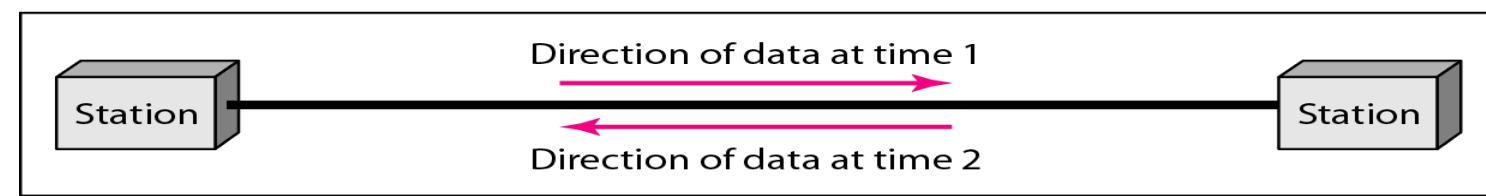
1. Text
2. Numbers
3. Images
4. Audio
5. Video

Data flow

- *Simplex*
- *Half-duplex*
- *Full-duplex*



a. Simplex



b. Half-duplex

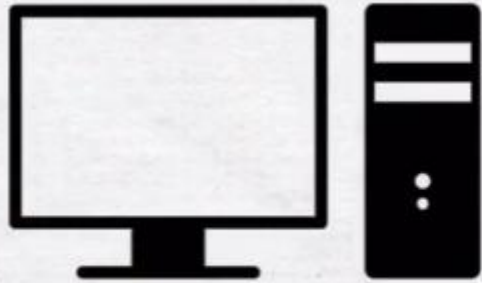


c. Full-duplex

What is Computer Network?

- **Network** - set of devices (*alias nodes*) connected by communication links.
- Node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.
- **Computer network** - collection of autonomous computers interconnected by a single technology so as to exchange information.
- Connections could be wired (optical fibre cables, coaxial cables etc.) or wireless (microwaves, infrared, and communication satellites).

What is Computer Network?



THIS IS A STANDALONE COMPUTER.

What is Computer Network?

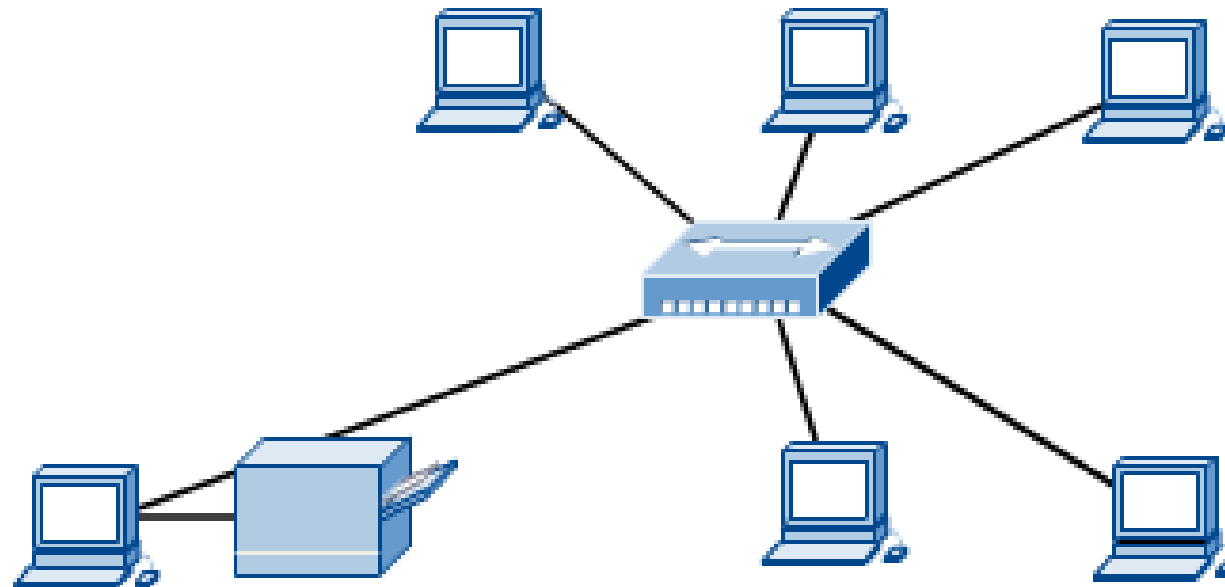
WHEN TWO OR MORE COMPUTERS ARE CONNECTED TOGETHER, IT IS CALLED...



COMPUTER NETWORK.

Computer Network

- **Computer Network** - connects two or more autonomous computers which can be geographically located anywhere.



Applications of Networks

- **Resource Sharing**

- ☐ Hardware (computing resources, disks, printers)
- ☐ Software (application software)

- **Information Sharing**

- ☐ Easy accessibility from anywhere (files, databases)
- ☐ Search Capability (WWW)

- **Communication**

- ☐ Email
- ☐ Message broadcast

- **Remote computing**

- **Distributed processing (GRID Computing)**

Benefits of Computer Networks

1. Business Applications

- To distribute information throughout company via **resource sharing** (such as printers, backup systems,
- **Client-server model**. Widely used and forms basis of much network usage.
- **Communication medium** among employees (**email**).
- Telephone calls between employees may be carried by computer network using **IP telephony** or **Voice over IP (VoIP)** when Internet is used.
- **Desktop sharing** lets remote workers see and interact
- **E-commerce (electronic commerce)** – online business

Benefits of Computer Networks

2. Home Applications

- Person-to-person communication
- Electronic commerce
- Entertainment.(Game playing,)

3. Mobile Users

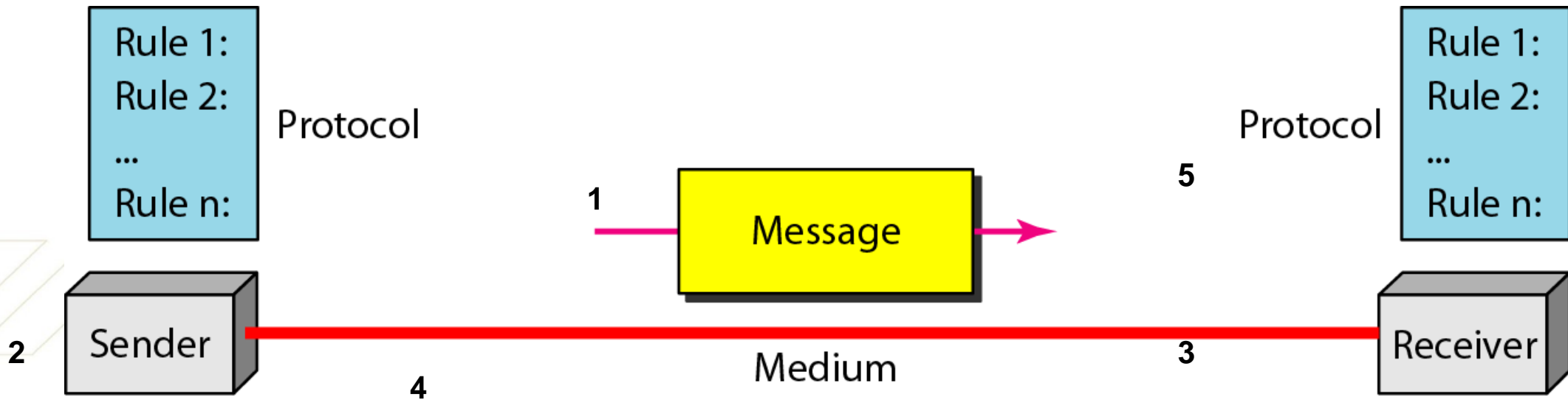
- Text messaging or texting
- Smart phones,
- GPS (Global Positioning System)
- m-commerce

Effectiveness of a computer network depends on

1. **Security.** Includes protecting data from unauthorized access, protecting data from damage and development, and implementing policies and procedures for recovery from breaches and data losses.
2. **Performance.** Performance can be measured based on **transit time** (amount of time required for a message to travel from one device to another) and **response time** (elapsed time between an inquiry and a response). Performance factors include number of users, type of transmission medium, capabilities of connected hardware, and efficiency of the software. Performance is also evaluated by two networking metrics: throughput (high) and delay (less).
3. **Reliability.** Network reliability is measured by frequency of failure, time it takes a link to recover from a failure, and network's robustness in a catastrophe.

Data Communications System Components

Figure Five components of data communication



Data Communications System Components

1. **Message.** Information (data) to be communicated (text, numbers, pictures, audio, and video).
2. **Sender.** Device that sends data message. It can be a computer, workstation, telephone handset, video camera, and so on.
3. **Receiver.** Device that receives message. It can be a computer, workstation, telephone handset, television, and so on.
4. **Transmission medium.** Physical path by which a message travels from sender to receiver. (Examples include twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves).
5. **Protocol.** Set of rules that govern data communications. Without a protocol, two devices may be connected but not communicating,

Type of Connection

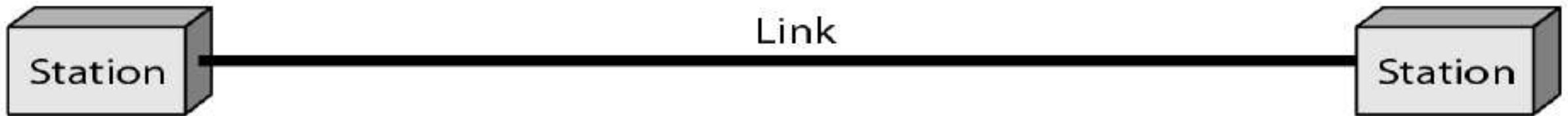
- Network is two or more devices connected through links which is communications pathway that transfers data from one device to another.

Types of connections:

1. **Point-to-Point** - provides a dedicated link between two devices.
2. **Multipoint** - more than two specific devices share a single link.

Type of Connection- Point-to-Point

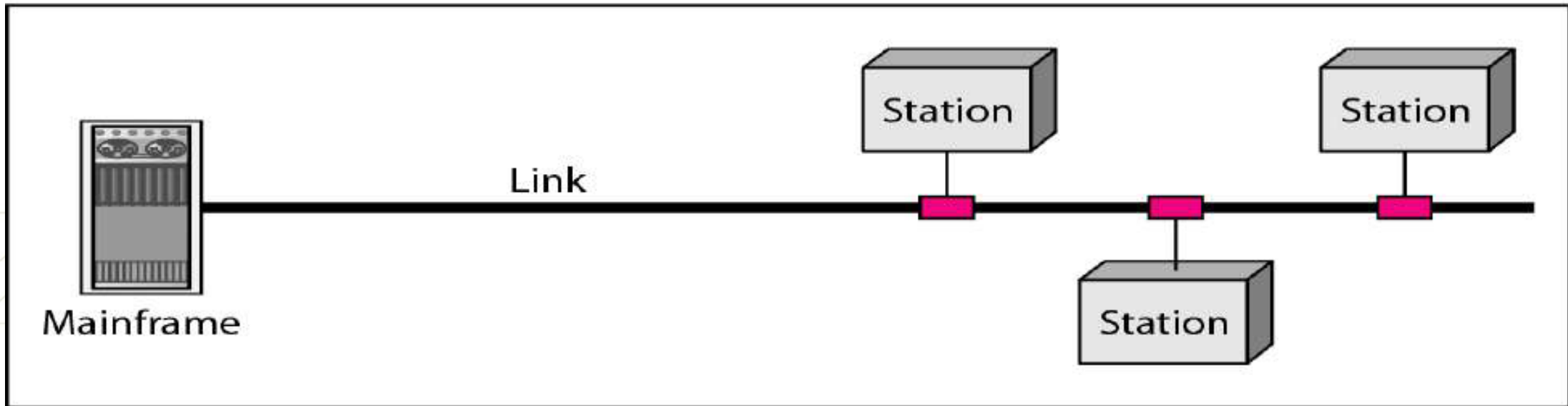
1. **Point-to-Point** - provides a dedicated link between two devices.
 - Capacity of link is reserved for transmission between those two devices.
 - Use an actual length of wire or cable to connect two ends, but other options, such as microwave or satellite links, are also possible.



a. Point-to-point

Type of Connection - Multipoint

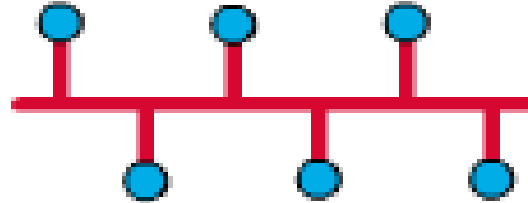
- 2. Multipoint** - more than two specific devices share a single link.
- Capacity of channel is shared, either spatially or time-shared.
 - If several devices can use the link simultaneously, it is a spatially shared connection.
 - If users must take turns, it is a timeshared connection.



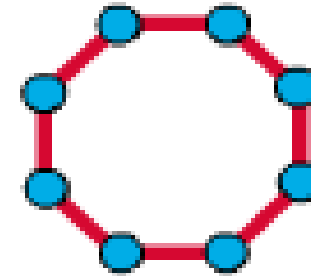
b. Multipoint

Network Topology

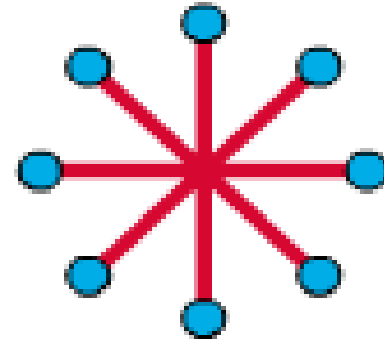
- Two or more devices connect to a link; two or more links form a topology.
- Topology of a network is geometric representation of relationship of all links and linking devices to one another.



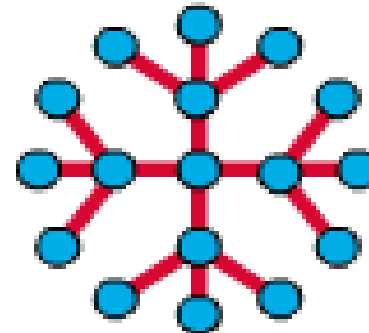
Bus Topology



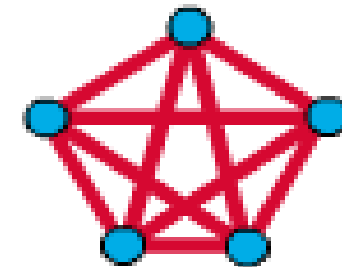
Ring Topology



Star Topology

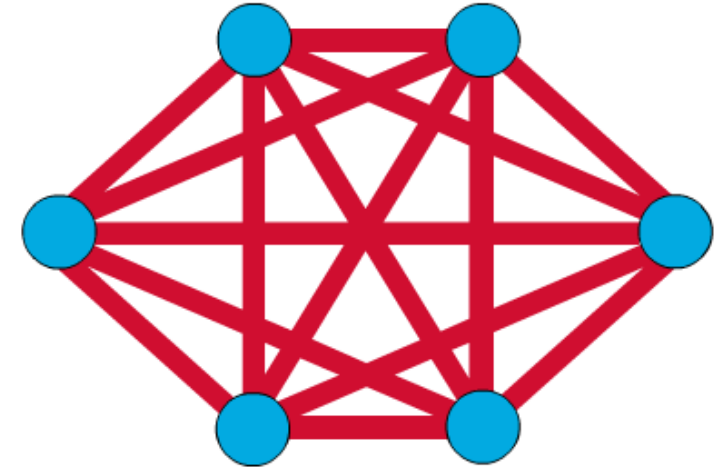


**Extended Star
Topology**



**Mesh
Topology**

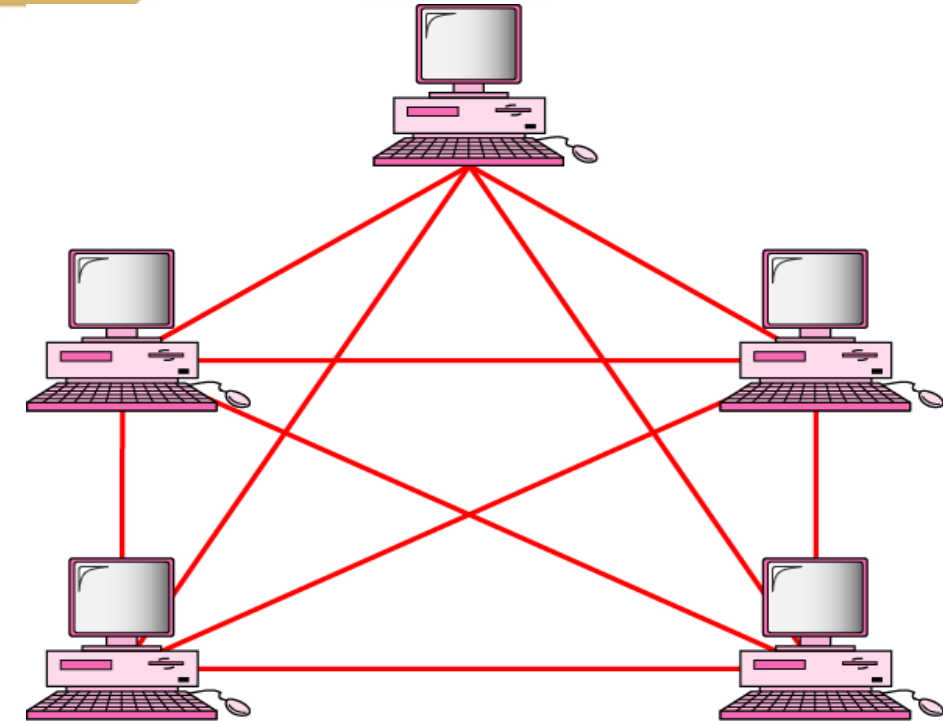
MESH Topology



- Every node is connected to every other node in network for redundancy and fault tolerance.
- Can be a **full mesh topology** (FMT) or a **partially topology** (PCMT).
- FMT - Every computer has a connection to each of other computer
Number of connections (n is number of computers in network): $\frac{n(n-1)}{2}$
- PCMT - at least two of computers in network have connections to multiple other computers in that network.
- Used in WANs to interconnect LANs and for mission critical networks like those used by banks and financial institutions.
- Implementing it is expensive and difficult.

MESH Topology

- Every device has a dedicated point-to-point link to every other devices
- **Dedicated**
 - ❑ Link carries traffic only between the two devices it connects
 - ❑ A fully connected mesh network has $n(n-1)/2$ physical channels to link n devices
 - ❑ Every device on the network must have $n-1$ input/output (I/O) ports
- **Advantage:** Less traffic, robust, secure, easy to maintain
- **Disadvantage:** Need more resource (cable and ports), expensive

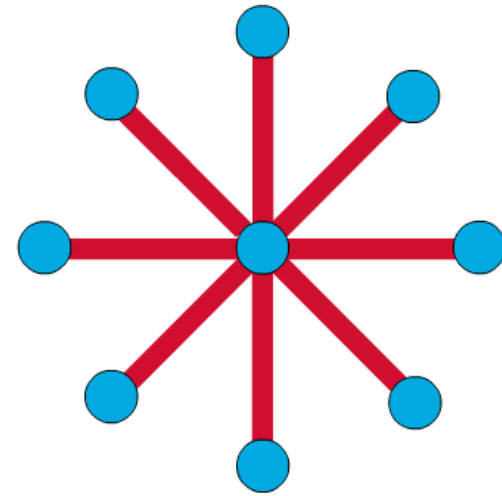


$n(n-1)/2$ physical duplex links

MESH Topology

Advantages	Disadvantages
Fault tolerant.	Issues with broadcasting messages.
Reliable.	Expensive and impractical for large networks.

Star Network, Star Topology



- Most common network setups
- Every node connects to a central network device, like a hub, switch, or computer.
- Central network device acts as a server and peripheral devices act as clients.
- Commonly used architecture in Ethernet LANs.
- When installed, it resembles spokes in a bicycle wheel.
- Larger networks use extended star topology also called tree topology.
- When used with network devices that filter frames or packets, like bridges, switches, and routers, this topology significantly reduces traffic on wires by sending packets only to wires of destination host.
- If central computer, hub, or switch fails, entire network goes down and all computers are disconnected from network

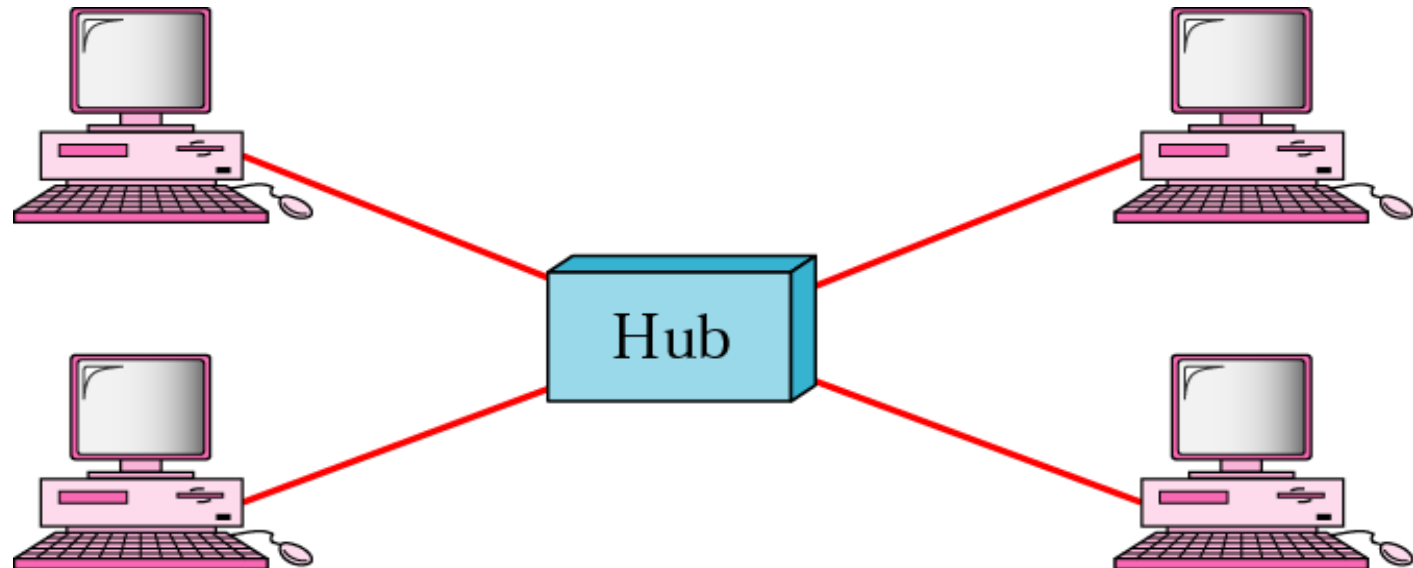
Star Network, Star Topology

- Advantages

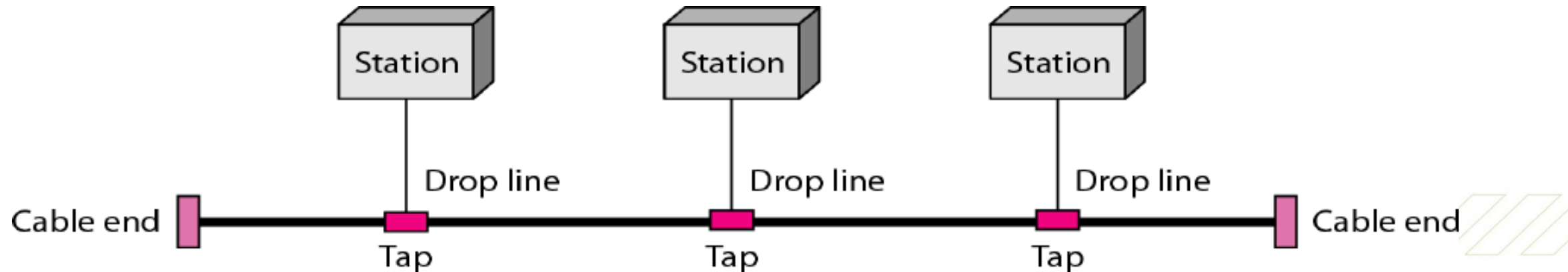
- ☐ Less expensive
- ☐ Easy to install and reconfigure
- ☐ Robustness—more scalable

- Disadvantage

- ☐ Single point of failure
- ☐ overload

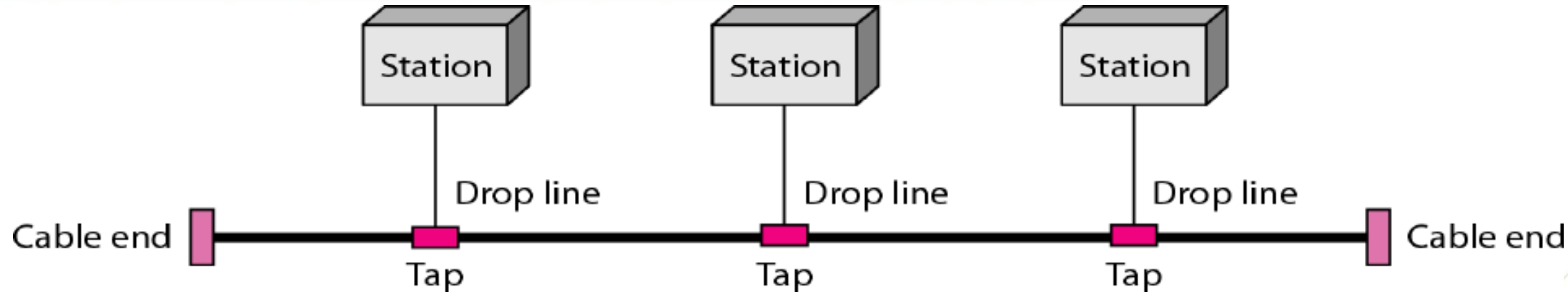


Bus Topology



- **Line topology, bus topology** is a network setup in which each computer and network device are connected to a single cable or backbone.
- Works well for small network, for connecting computers or peripherals in a linear fashion.
- Requires less cable length than a star topology.
- Can be difficult to identify problems if the whole network goes down.
- Hard to troubleshoot individual device issues specially for large networks.
- Terminators are required for both ends of main cable which slow down network.

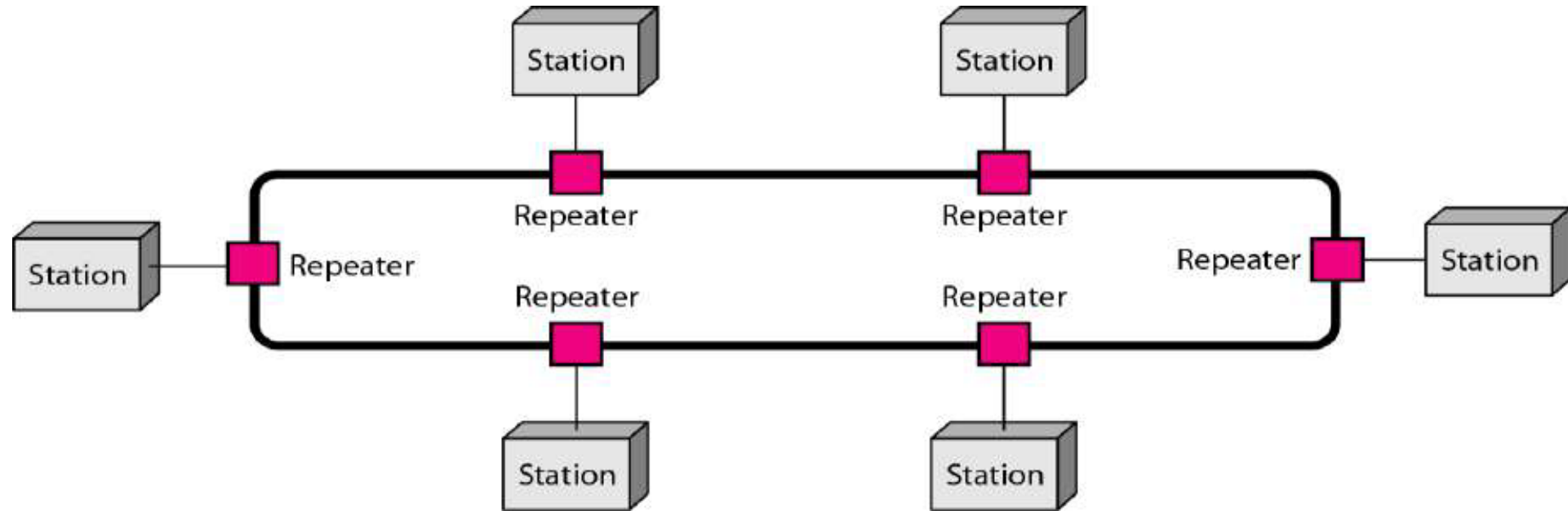
Bus Topology



- Nodes are connected to the bus cable by drop lines and taps.
 - ❑ Drop line: A connection running between the device and the main cable
 - ❑ Tap: A connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core
- **Advantage:** Ease of installation—Suited for temporary network---node failure does not effect others
- **Disadvantages:**
 - ❑ Difficult reconnection and fault isolation
 - ❑ Broken or fault of the bus cable stops all transmission
 - ❑ No security
 - ❑ Limited cable length

RING Topology

- Network configuration in which device connections create a circular data path.



- Here, packets of data travel from one device to next until they reach their destination.
- Mostly allow packets to travel only in one direction, called a **unidirectional** ring network. Others permit data to move in either direction, called **bidirectional**.
- Major disadvantage is if any individual connection in ring is broken, entire network is affected.
- Used in either local area networks (LANs) or wide area networks (WANs).

RING Topology

- Each device is dedicated point-to-point connection only with the two devices on either side of it
- A signal is passed along the ring in the direction, from device to device, until it reaches its destination
- Each device in the ring incorporates a repeater
- **Advantages:** Relatively easy to install and reconfigure, Fault isolation is simplified
- **Disadvantage:** Unidirectional traffic

Advantages	Disadvantages
Performance better than Bus topology.	Unidirectional. Single point of failure will affect the whole network.
Can cause bottleneck due to weak links.	↑ in load – ↓ in performance.
All nodes with equal access.	No security.

Tree Topology

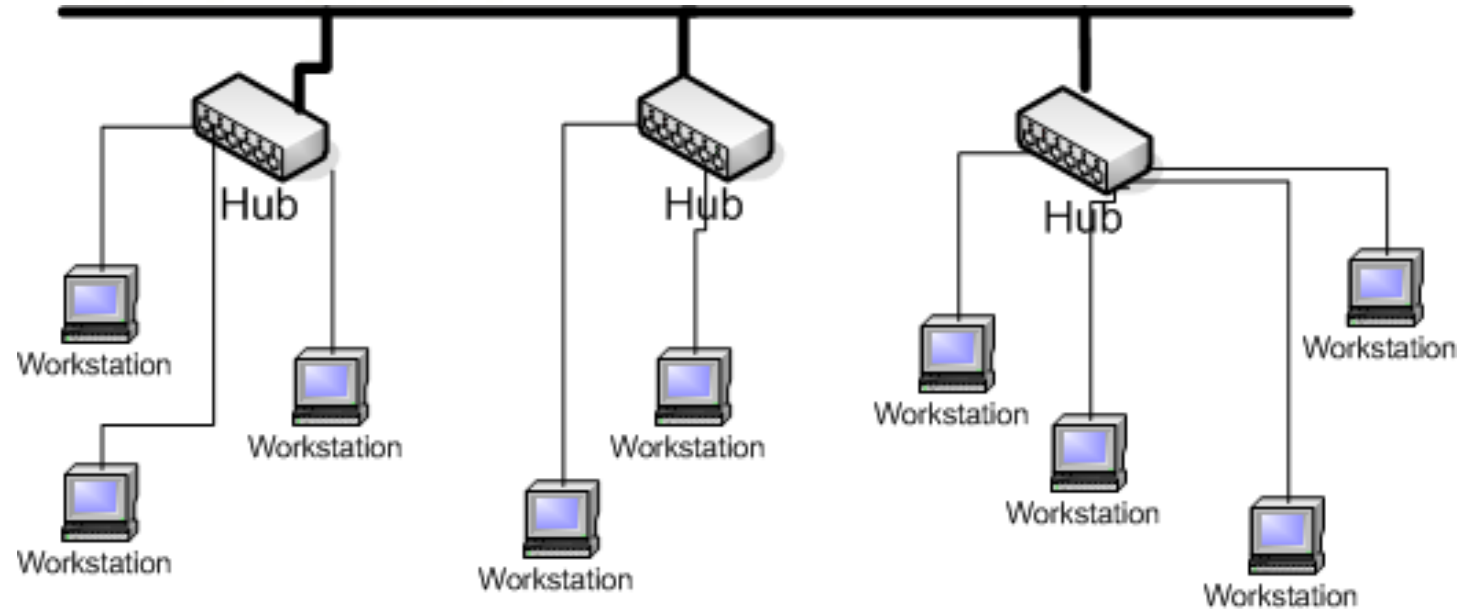
- Tree topologies integrate multiple topologies together
- **Example:** Tree topology integrates multiple star topologies together onto a bus

- **Advantages:**

- ☐ Point-to-point wiring for individual segments.
- ☐ Supported by several hardware and software vendors.

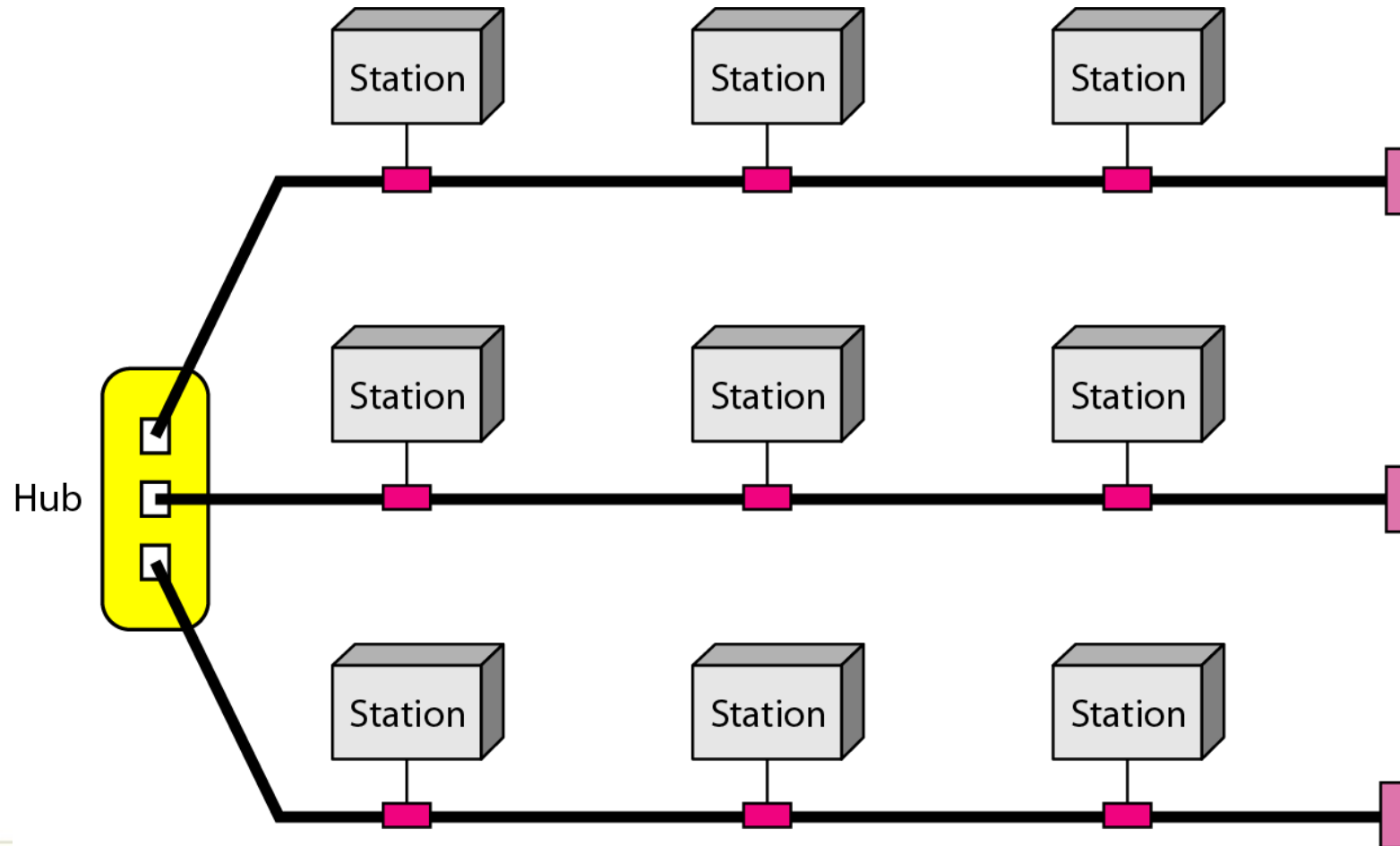
- **Disadvantages:**

- ☐ Overall length of each segment is limited by the type of cabling used.
- ☐ If the backbone line breaks, the entire segment goes down.
- ☐ More difficult to configure and wire than other topologies.



Hybrid Topology:

- Star backbone with three bus networks



Types Of Computer Network

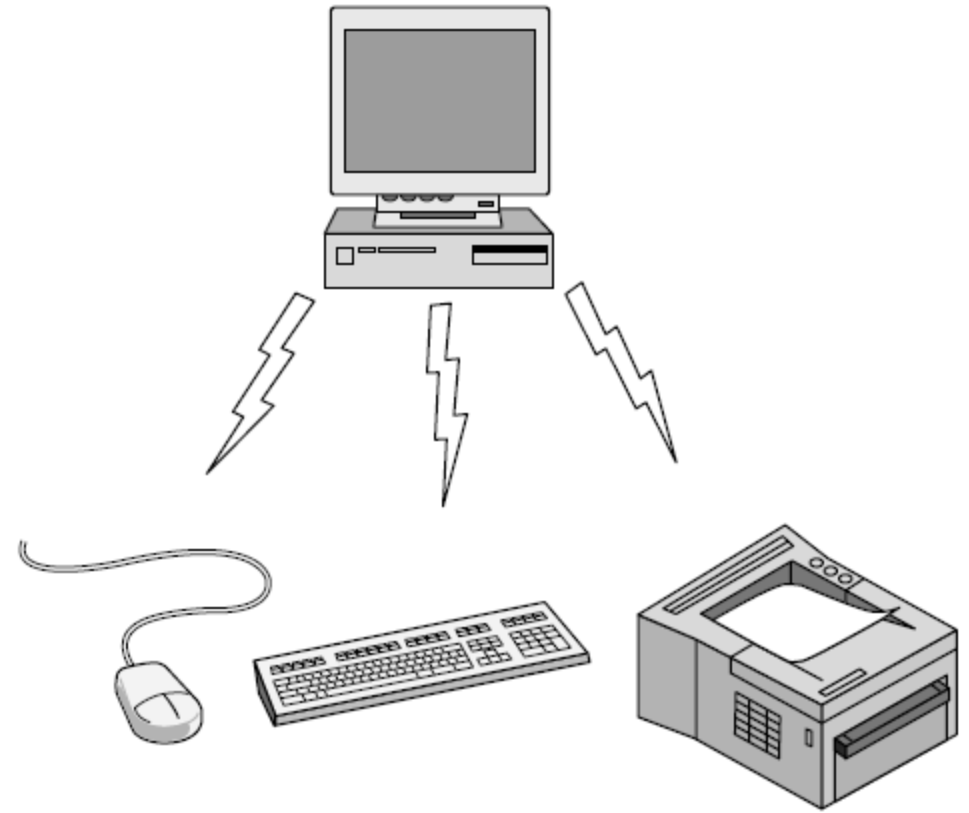
- Types of network are classified based upon
 - ❑ size,
 - ❑ area it covers and
 - ❑ its physical architecture.
- Each network differs in their characteristics such as
 - ❑ distance,
 - ❑ transmission speed,
 - ❑ cables and
 - ❑ cost.



- PERSONAL AREA NETWORK
- LOCAL AREA NETWORK
- METROPOLITAN AREA NETWORK
- WIDE AREA NETWORK

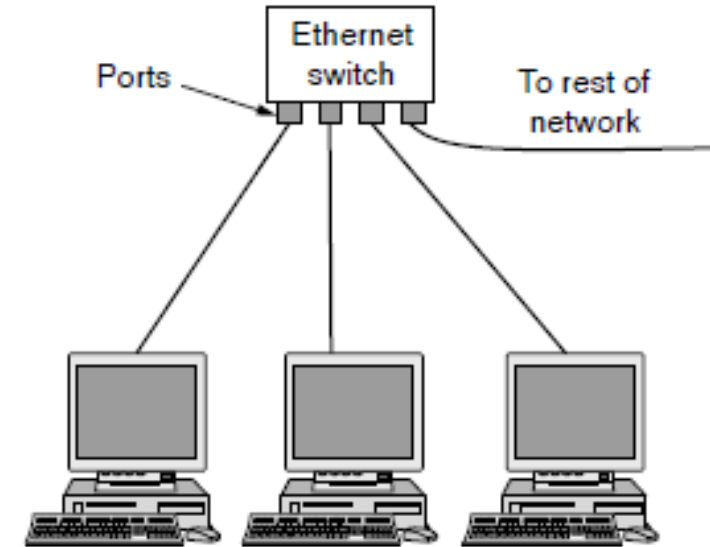
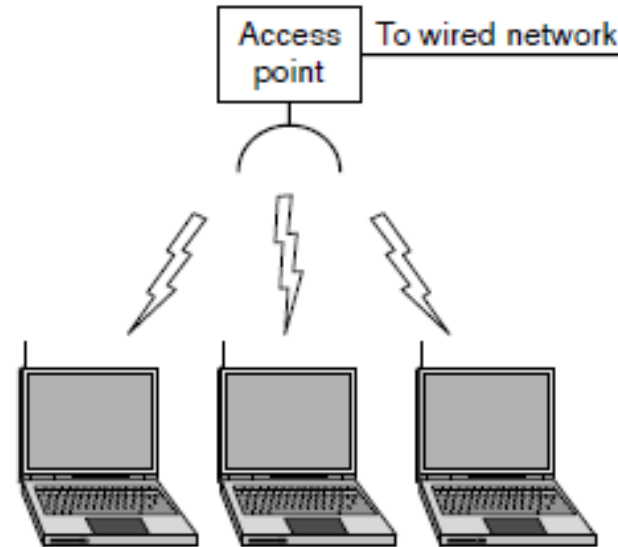
Personal Area Networks

- **PANs** let devices communicate over range of a person.
- Example - wireless network that connects a computer with its peripherals, network that connects wireless headphones and watch to smartphone.
- PANs can also be built with a variety of other technologies that communicate over short ranges.



LAN (Local Area Network)

- Group of interconnected computers within a small area. (room, building, campus)
- Two or more PC's can from a LAN to share files, folders, printers, applications and other devices.

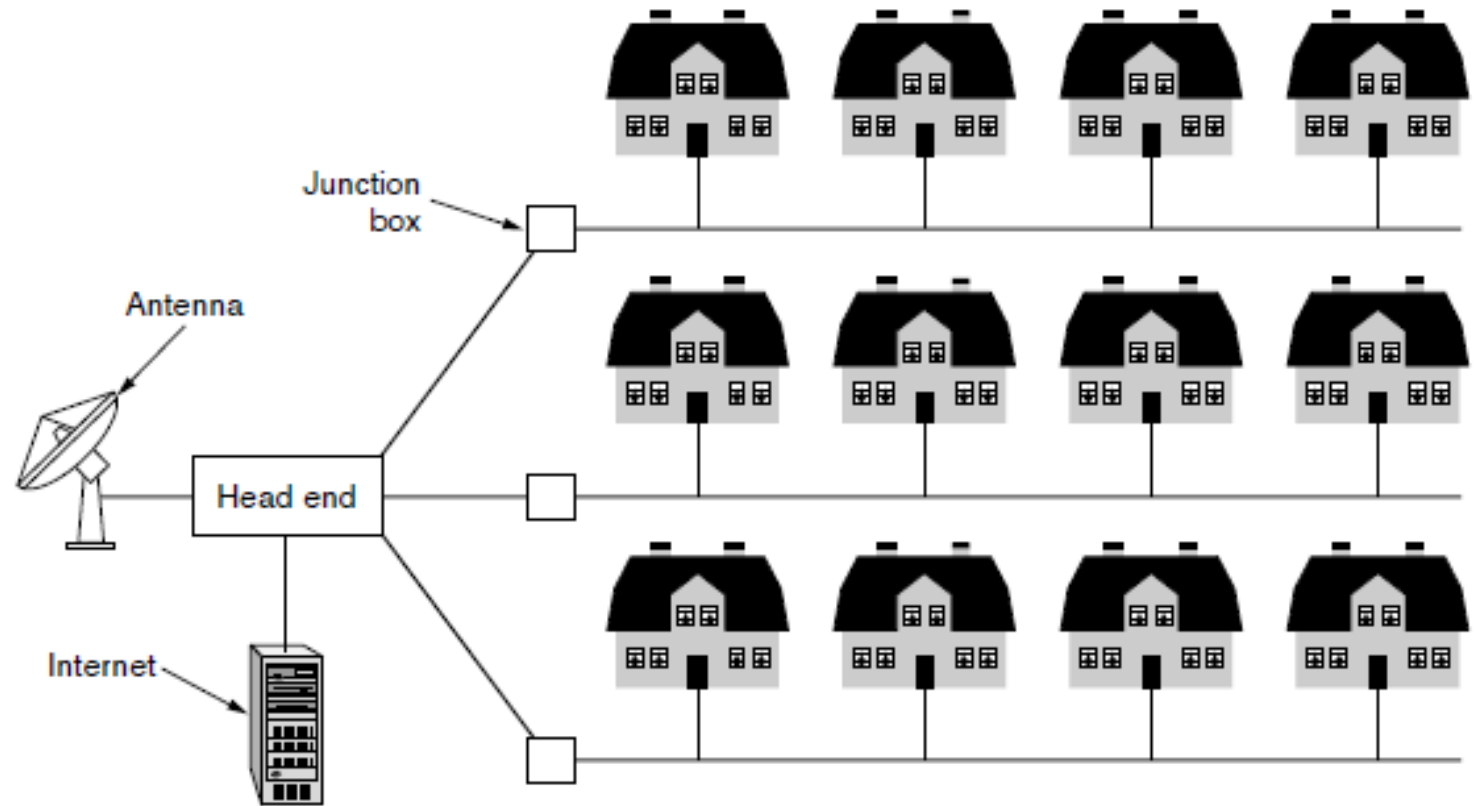


- Coaxial or CAT 5 cables are normally used for connections.
- Due to short distances, errors and noise are minimum.
- Data transfer rate is 10 to 100 mbps.
- Example: A computer lab in a college campus.

Wireless and wired LANs.
(a) 802.11.
(b) Switched Ethernet

MAN (Metropolitan Area Network)

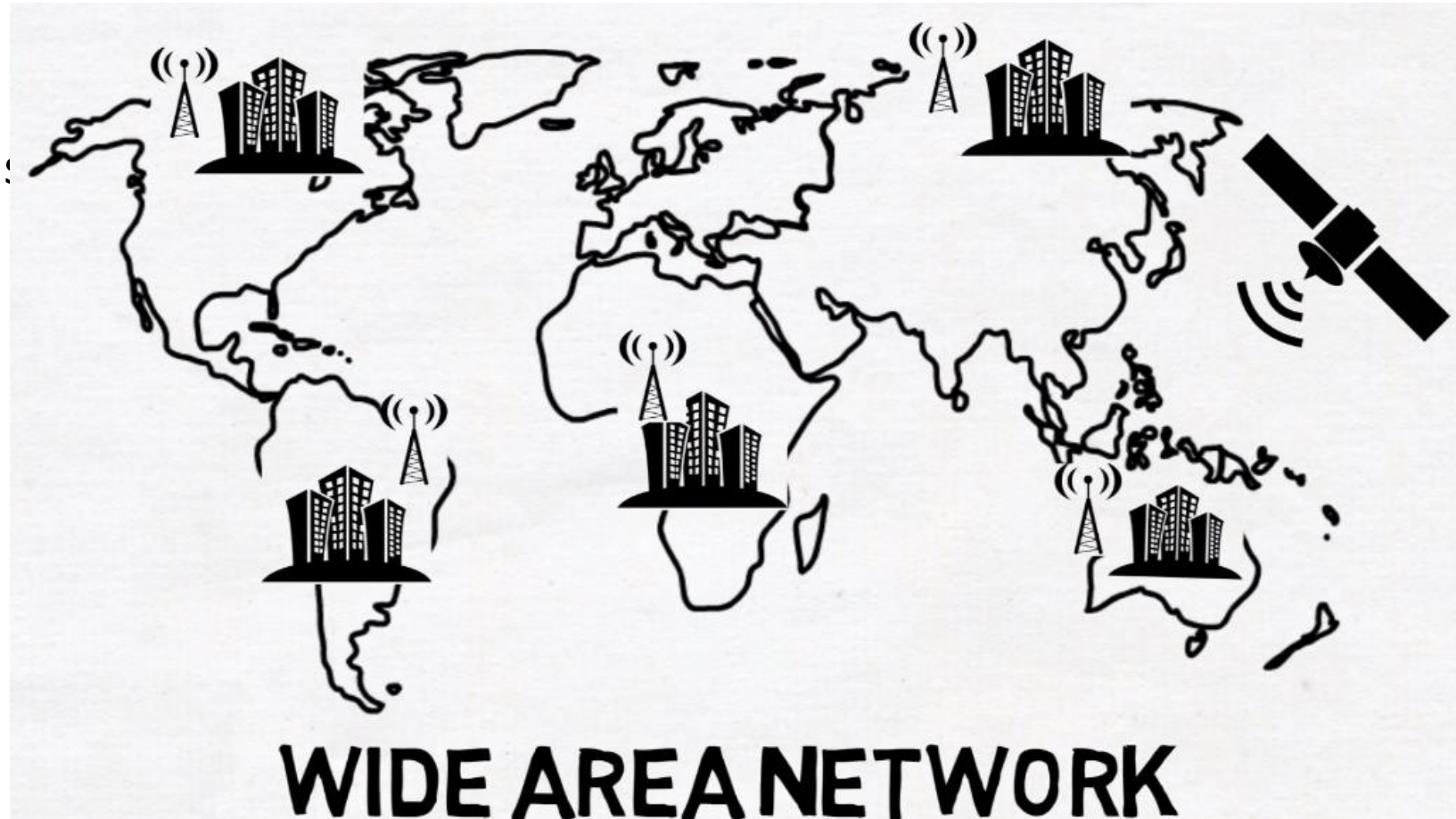
- Design to extend over a large area.
- Connecting number of LAN's to form larger network, so that resources can be shared.
- Networks can be up to 5 to 50 km.
- Owned by organization or individual.
- Data transfer rate is low compare to LAN.
- Example: Organization with different branches located in the city.



A metropolitan area network based on cable TV.

WAN (Wide Area Network)

- WAN are country and worldwide network.
- Contains multiple LAN's and MAN's.
- Distinguished in terms of geographical range.
- Uses satellites and microwave relays.
- Data transfer rate depends upon ISP provider and varies over location.
- Best example is internet.



Layered Network Architecture - Overview

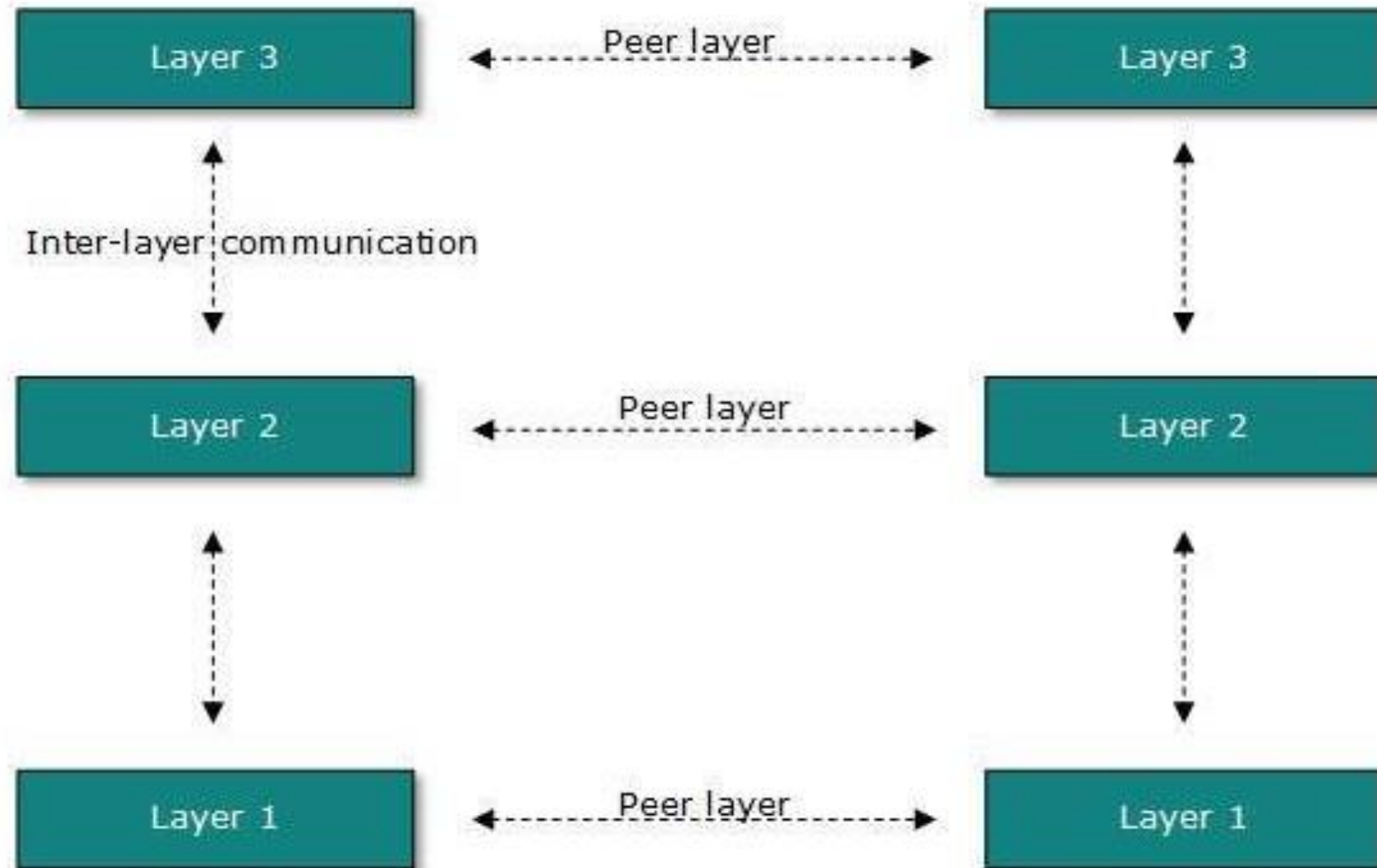
- Networking engineering is a complicated task, which involves
 - ❑ Software,
 - ❑ Firmware,
 - ❑ Chip level engineering,
 - ❑ Hardware, and
 - ❑ Electric pulses.
- To ease network engineering, whole networking concept is divided into multiple layers.
- Each layer is involved in some particular task and is independent of all other layers.
- But as a whole, almost all networking tasks depend on all of these layers.
- Layers share data and depend on each other only to take input and send output.

Layered Network Architecture - Overview

- One whole network process is divided into small tasks.
- Each small task is then assigned to a particular layer which works dedicatedly to process the task only.
- Every layer does only specific work.
- In layered communication system, one layer of a host deals with task done by or to be done by its peer layer at same level on remote host.
- Task is either initiated by layer at lowest level or at top most level.
- If task is initiated by top most layer, it is passed on to layer below it for further processing.
- Lower layer does same thing, it processes task and passes on to lower layer.
- If task is initiated by lower most layer, then reverse path is taken.

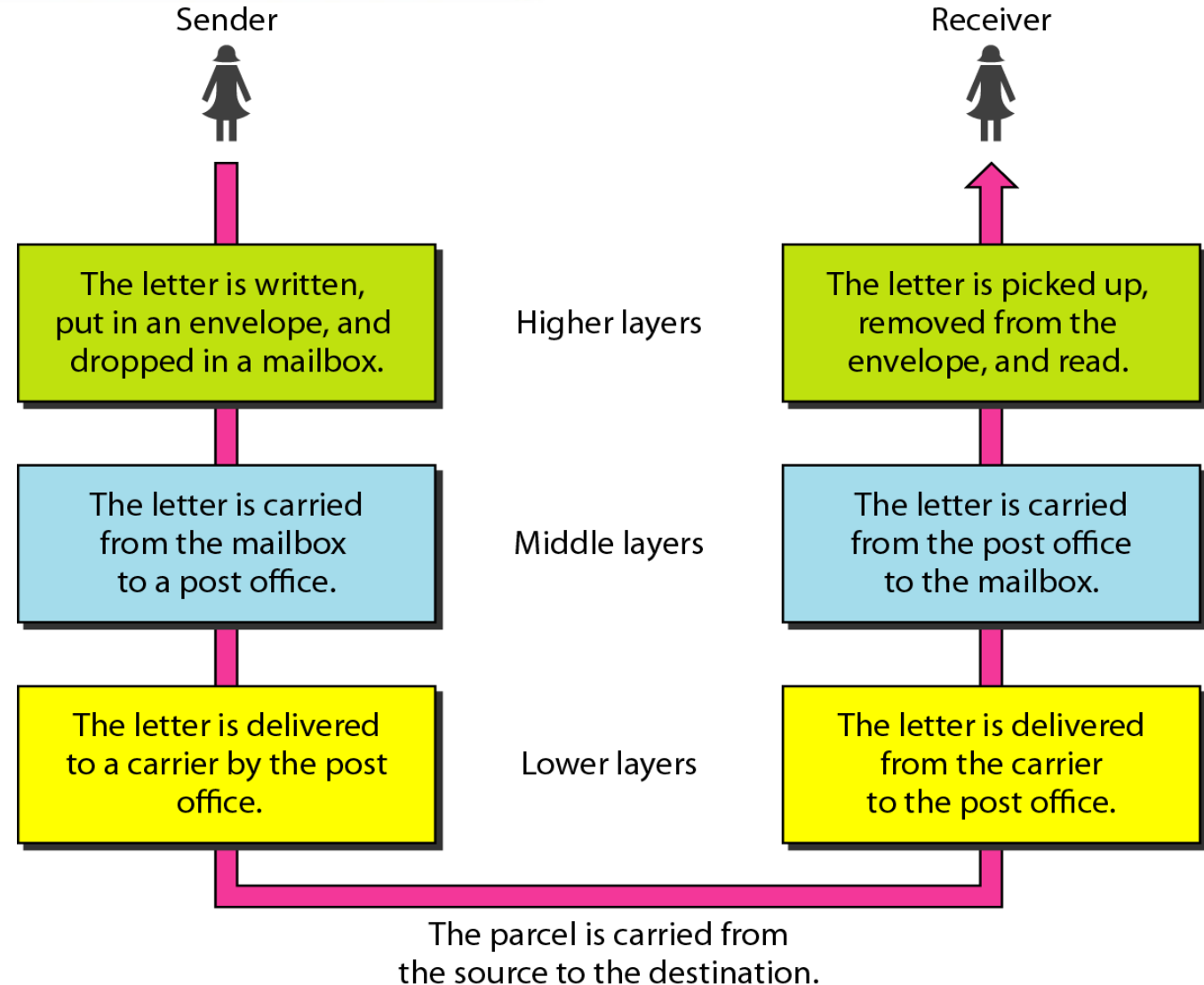
Layered Network Architecture - Overview

- Every layer clubs together all procedures, protocols, and methods which it requires to execute its piece of task.
- All layers identify their counterparts by means of encapsulation header and tail.



Layered Network Architecture - Overview

- Every layer clubs together all procedures, protocols, and methods which it requires to execute its piece of task.
- All layers identify their counterparts by means of encapsulation header and tail.



Example

Airline
Company



Example

Airline
Company



SECURITY



COMPUTER SCIENTIST



MANAGERS



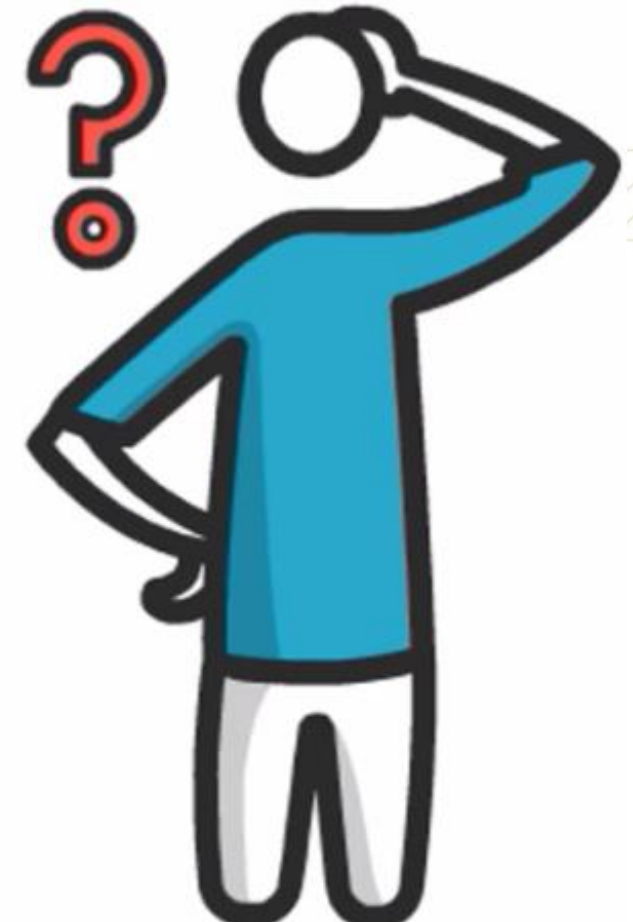
LABOUR



PILOT



AIRHOSTESS



Example



Example



CONFIRM ORDER



BAKE PIZZA



DELIVER PIZZA

Benefits Of Layered Architecture

Benefits of Layered Architecture

**Fast
Development**

Self Contained

**Easy to discuss
specific portion**

What are protocols

- In CN, communication occurs between entities in different systems which is capable of sending or receiving information.
- However, two entities cannot simply send bit streams to each other and expect to be understood.
- For communication to occur, entities must agree on a protocol.
- **A protocol is a set of rules that govern data communications.**
- Protocol defines **what** is communicated, **how** it is communicated, and **when** it is communicated.

What are protocols

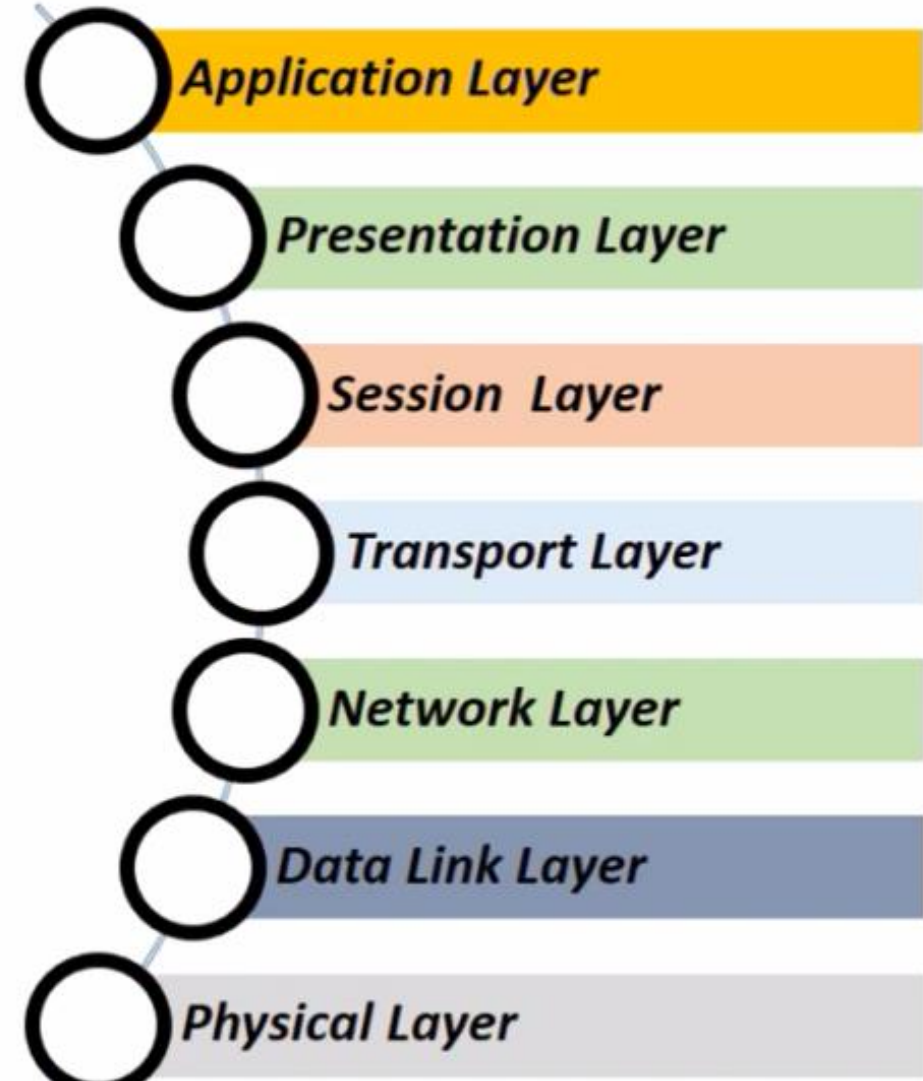
- Key elements of a protocol are **syntax, semantics, and timing**.
 - ❑ **Syntax**- Refers to structure or format of data, meaning order in which they are presented. For example, a simple protocol might expect first 8 bits of data to be sender address, second 8 bits to be receiver address, and rest bits to be message.
 - ❑ **Semantics**- Refers to meaning of each section of bits. (To interpreted a pattern and perform necessary action) For example, does an address identify route to be taken or final destination of message?
 - ❑ **Timing**- Refers to two characteristics: when data should be sent and how fast they can be sent. For example, if a sender produces data at 100 Mbps but receiver process data at only 1 Mbps, transmission will overload receiver and some data will be lost.

The OSI Model

- Established in 1984
- International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards
- ISO proposed a 7 layered architecture model named as Open Systems Interconnection model (OSI model) in 1974 to solve problem of network architecture
- OSI model is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture.
- Purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to logic of underlying hardware and software.
- **OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.**

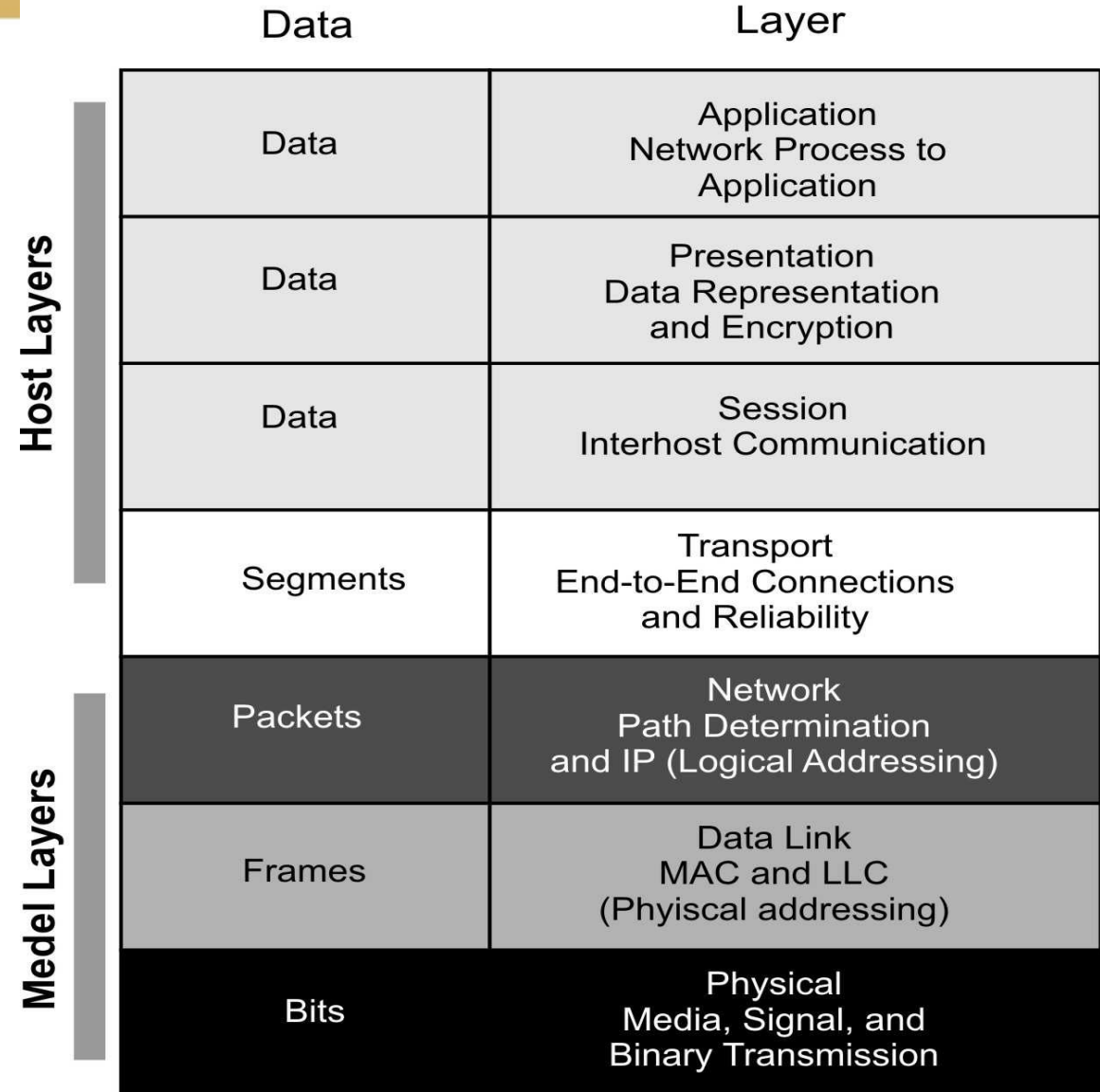
The OSI Model

- OSI model is a layered framework for design of network systems that allows communication between all types of computer systems.
- It consists of seven separate but related layers, each of which defines a part of process of moving information across a network.
- **All People Seems To Need Data Processing**
- **Please Do Not Touch Sachin's Pet Alligator**



The OSI Model

- Each layer is responsible for a particular aspect of data communication.
- For example, one layer may be responsible for establishing connections between devices, while another layer may be responsible for error checking during transfer.
- Layers in OSI model are divided into two groups: upper layers and lower layers.
- Each layer has a set of functions that are to be performed by a specific protocol(s).
- OSI reference model has a protocol suit for all of its layers.



The OSI Model

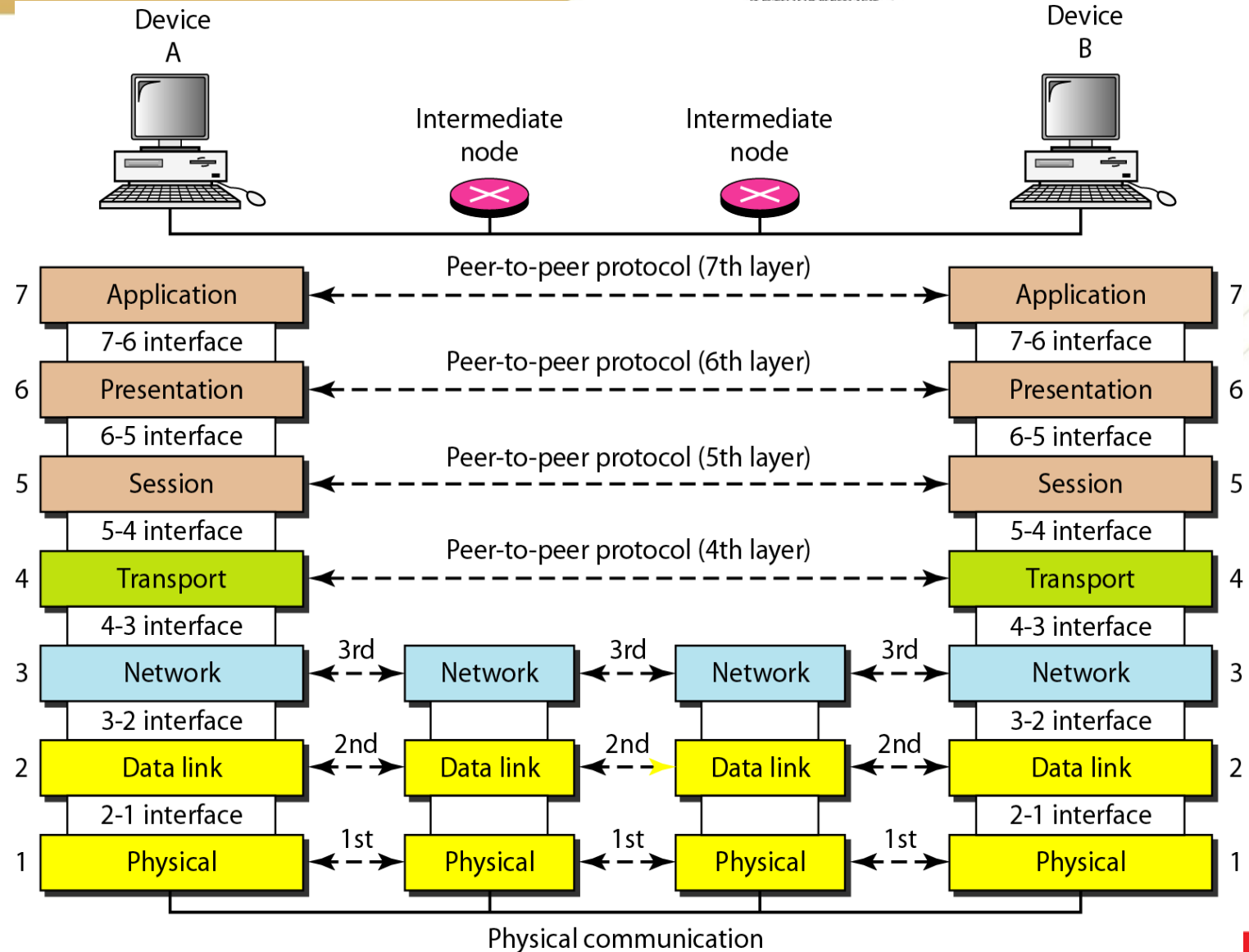
- Upper layers (Host layers) focus on user applications and how files are represented on computers prior to transport.
- Lower layers (Media Layers) concentrate on how communication across a network actually occurs.

Data Layer	
Host Layers	Data Application Network Process to Application
	Data Presentation Data Representation and Encryption
	Data Session Interhost Communication
	Segments Transport End-to-End Connections and Reliability
Media Layers	Packets Network Path Determination and IP (Logical Addressing)
	Frames Data Link MAC and LLC (Physical addressing)
	Bits Physical Media, Signal, and Binary Transmission

The OSI Model

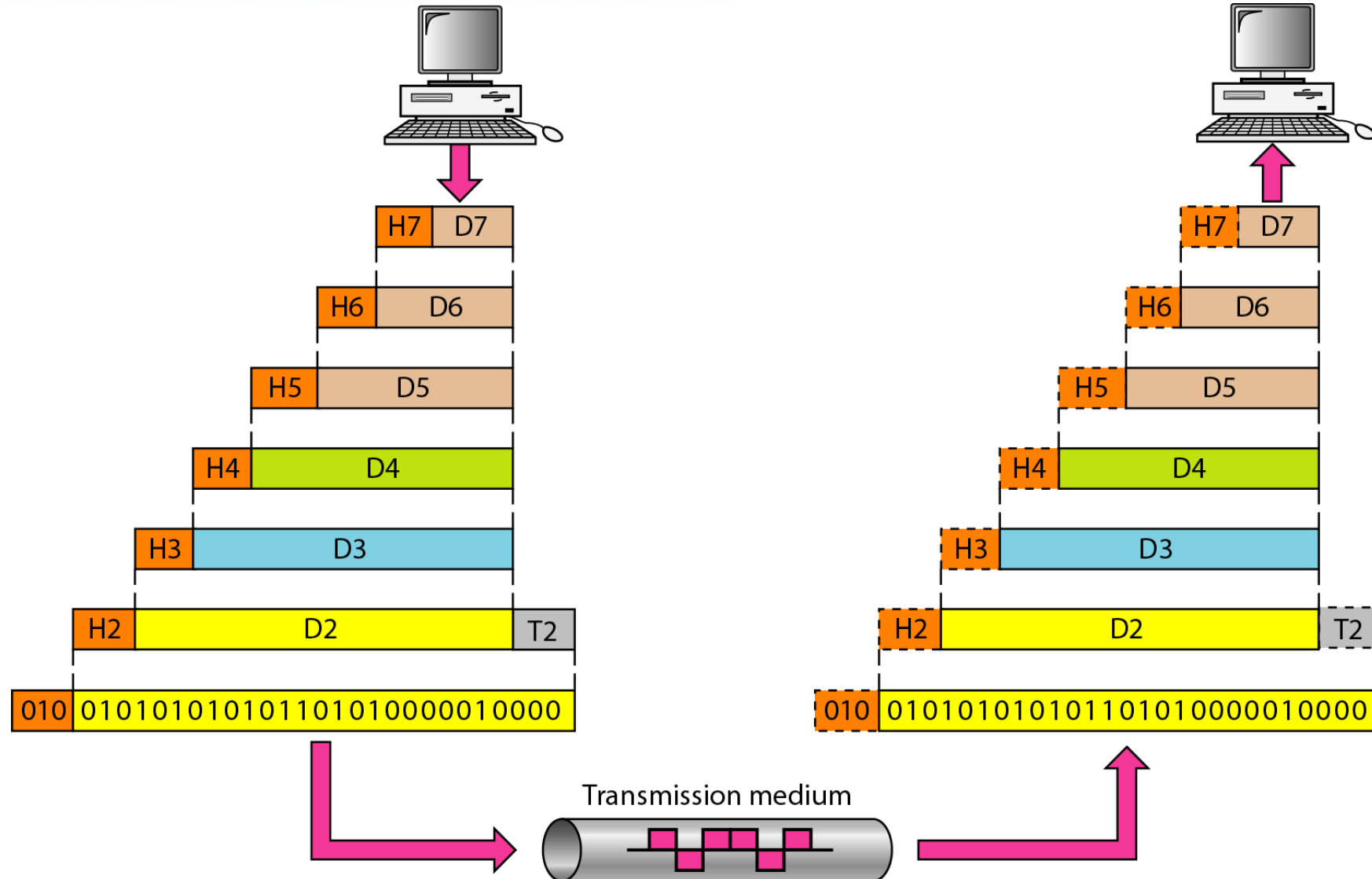
- Seven layers can be grouped into **three groups** –
Network, Transport and Application.

- Layer 1, 2 and 3 i.e. physical, data link, and network are **network support** layers.
- Layer 4, Transport layer provides end to end reliable **data transmission**.
- Layer 5, 6 and 7 i.e. Session, Presentation, and Application layer are **user support** layers.



The OSI Model

- An exchange using the OSI model



Layer 1 – Physical Layer

Bits

Physical
Media, Signal, and
Binary Transmission

- Lowest layer of OSI model, is concerned with transmission and reception of **unstructured raw bit stream over a physical medium**.
- It describes **electrical/optical, mechanical, and functional interfaces** to physical medium, and carries signals for all of higher layers.
- **Defines cables, network cards** and physical aspects.
- Responsible for actual physical connection between devices which are made by using twisted pair cable, fiber-optic, coaxial cable or wireless communication media.

Layer 1 – Physical Layer

Bits

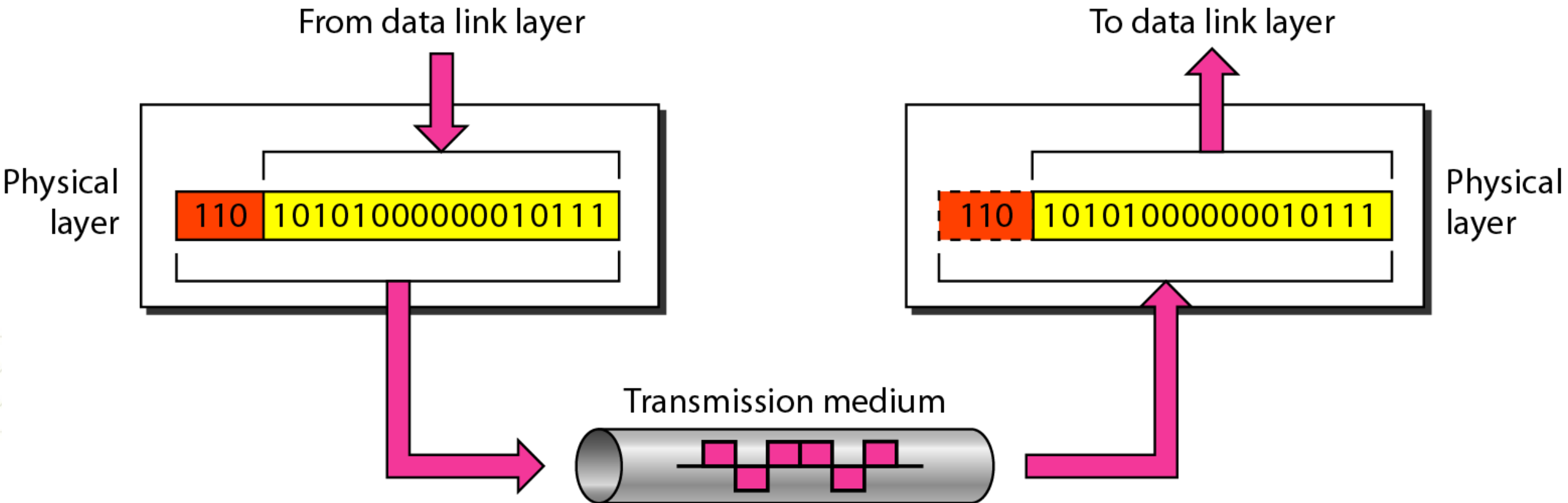
Physical
Media, Signal, and
Binary Transmission

- Receives frames sent by the Data Link layer and **converts them into signals** compatible with the transmission media.
- If a metallic cable is used, then it will convert data into **electrical signals**; if a fiber optical cable is used, then it will **convert data into luminous signals**; if a wireless network is used, then it will **convert data into electromagnetic signals**.
- When receiving data, this layer receives signal and **converts it into 0s and 1s** and send them to Data Link layer, which will put frame back together and check for its integrity
- **X.25 protocols works at physical, data link, and network layers.**

Functions of Physical Layer

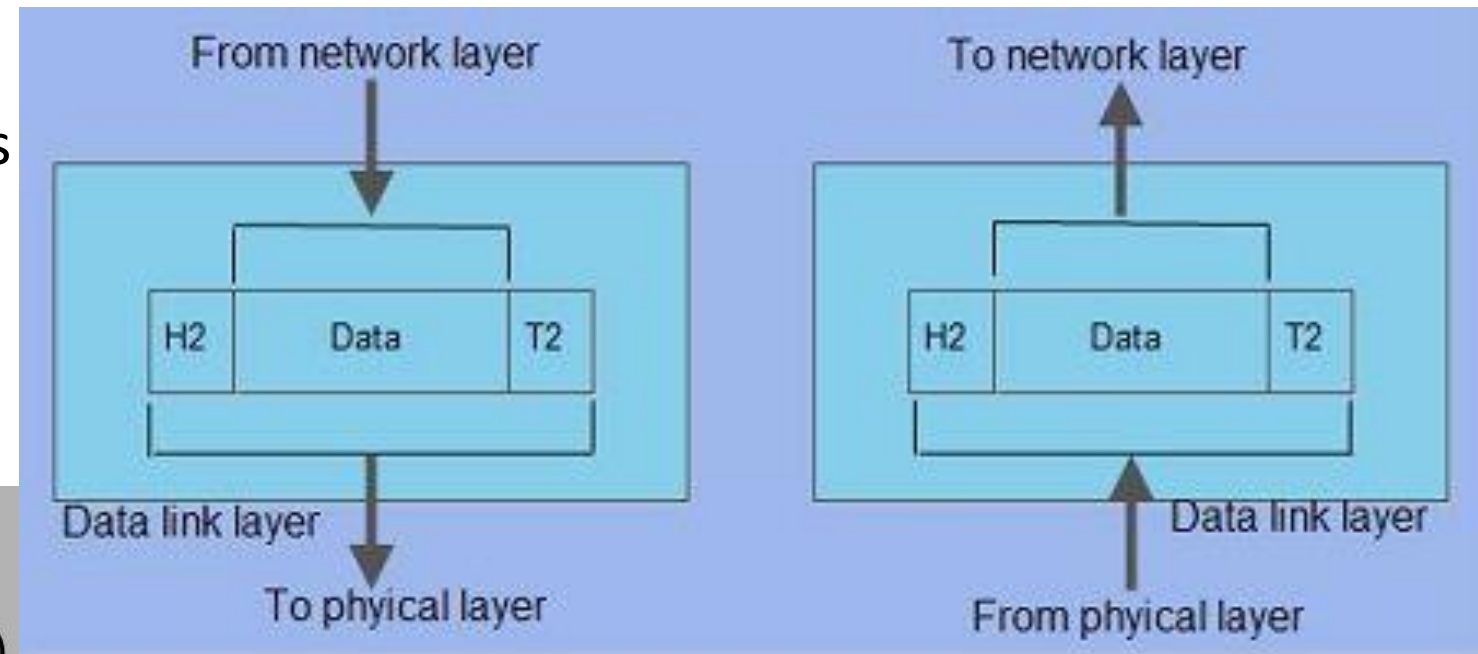
- 1. Data encoding:** modifies digital signal pattern (1s and 0s) used by PC to accommodate characteristics of physical medium, and to aid in bit and frame synchronization.
 - What signal state represents a binary 1?
 - How the receiving station knows when a “bit-time” starts
 - How the receiving station delimits a frame
- 2. Transmission technique:** determines whether encoded bits will be transmitted by baseband (digital) or broadband (analog) signaling.
- 3. Physical medium transmission:** transmits bits as electrical or optical signals appropriate for physical medium, and determines:
 - What physical medium options can be used?
 - How many volts/db should be used to represent a given signal state, using a given physical medium?

Functions of Physical Layer



Layer 2 – Data Link Layer

- Responsible for reliable node-to-node delivery of data.
- Receives data from network layer and creates frames, add physical address to these frames and pass them to physical layer
- Provides **error-free transfer** of data frames from one node to another over physical layer, allowing layers above it to assume virtually error-free transmission over link.
- Defines format of data on network.
- Network data frame, packet, includes checksum, source and destination address, and data.

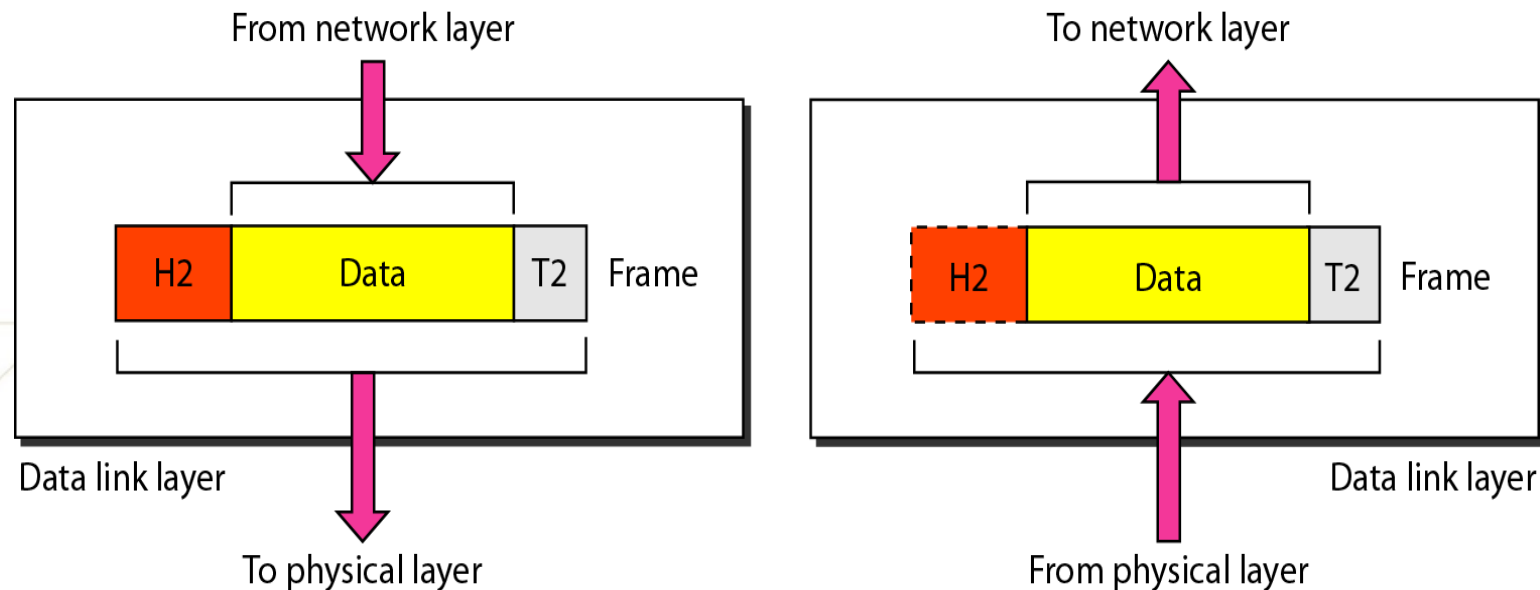


Frames

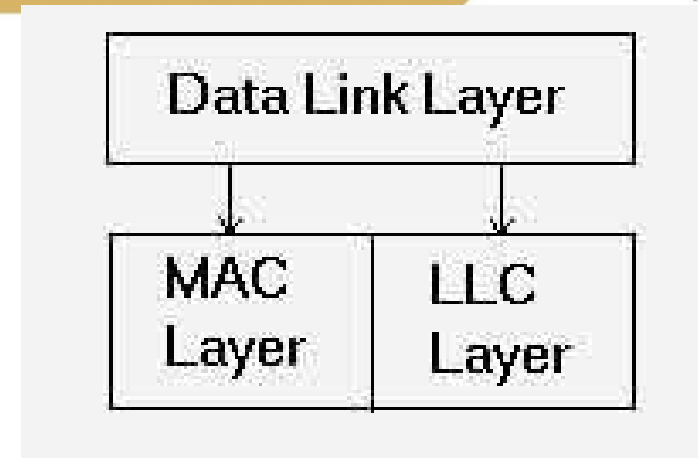
Data Link
MAC and LLC
(Physical addressing)

Layer 2 – Data Link layer

- Handles **physical and logical connections to packet's destination**, using a network interface.
- Gets data packets sent by network layer and **convert them into frames** that will be sent out to network media, **adding physical address of network card** of your computer, physical address of network card of destination, **control data and checksum data, also known as CRC**.
- **X.25 protocols works at physical, data link, and network layers.**



Sub-layers- Data Link Layer



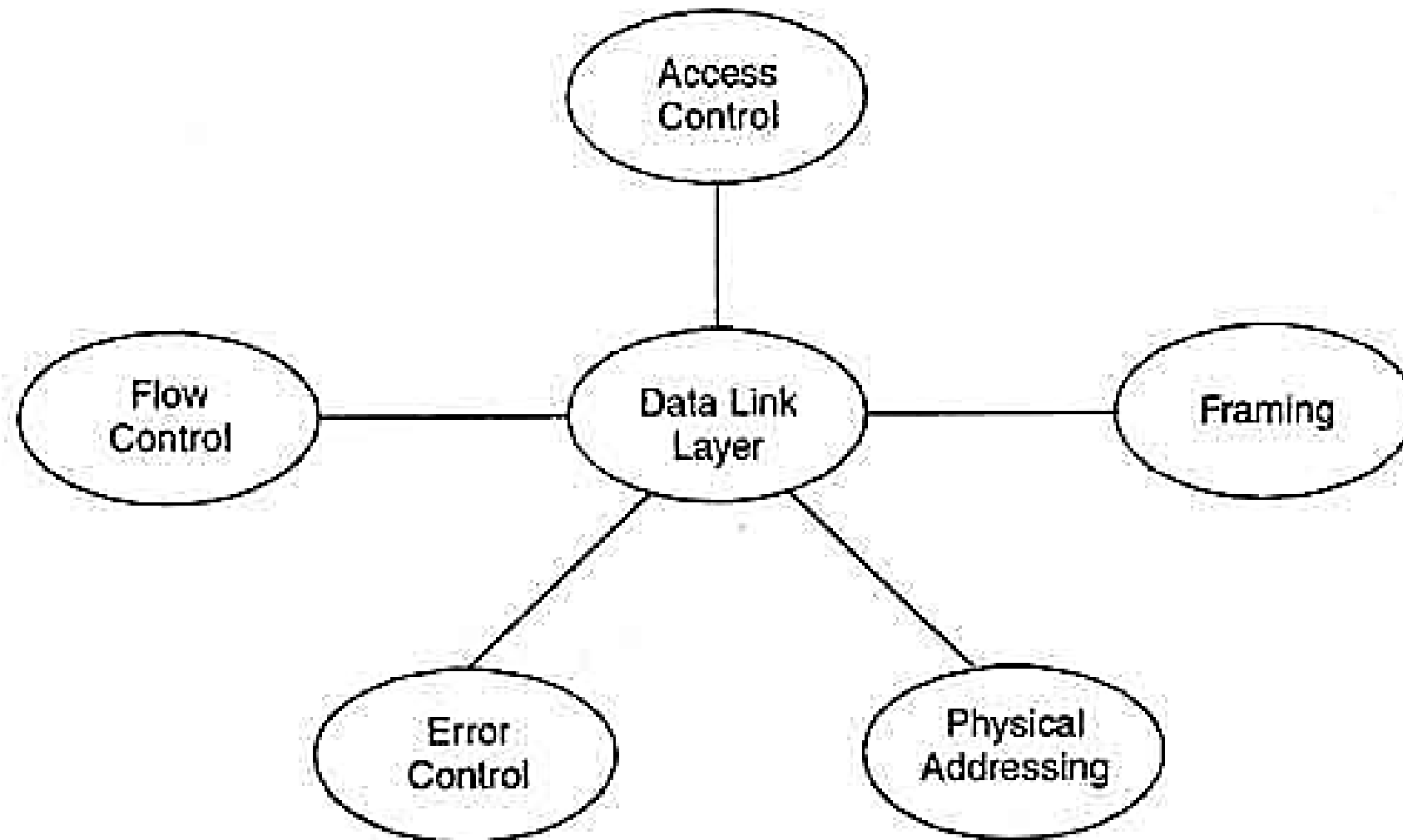
1. **Logical Link Control (LLC) sublayer**
2. **Medium Access Control (MAC) sublayer**

- **LLC sublayer** provides interface between media access methods and network layer protocols such as Internet Protocol which is a part of TCP/IP protocol suite. It determines whether communication is connectionless or connection-oriented at data link layer.
- **MAC sublayer** is responsible for connection to physical media. Here, actual physical address of device, called MAC address is added to packet. Such a packet is called a Frame that contains all addressing information necessary to travel from source device to destination device.

MAC address

- 12 digit hexadecimal number unique to every computer in this world.
- Device's MAC address is located on its Network Interface Card (NIC).
- In these 12 digits of MAC address, first six digits indicate NIC manufacturer and last six digits are unique.
- For example, 32-14-a6-42-71-0c is 12 digit hexadecimal MAC address.
- **MAC address represents physical address of a device in network.**

Functions of Data Link Layer



Functions of Data Link Layer

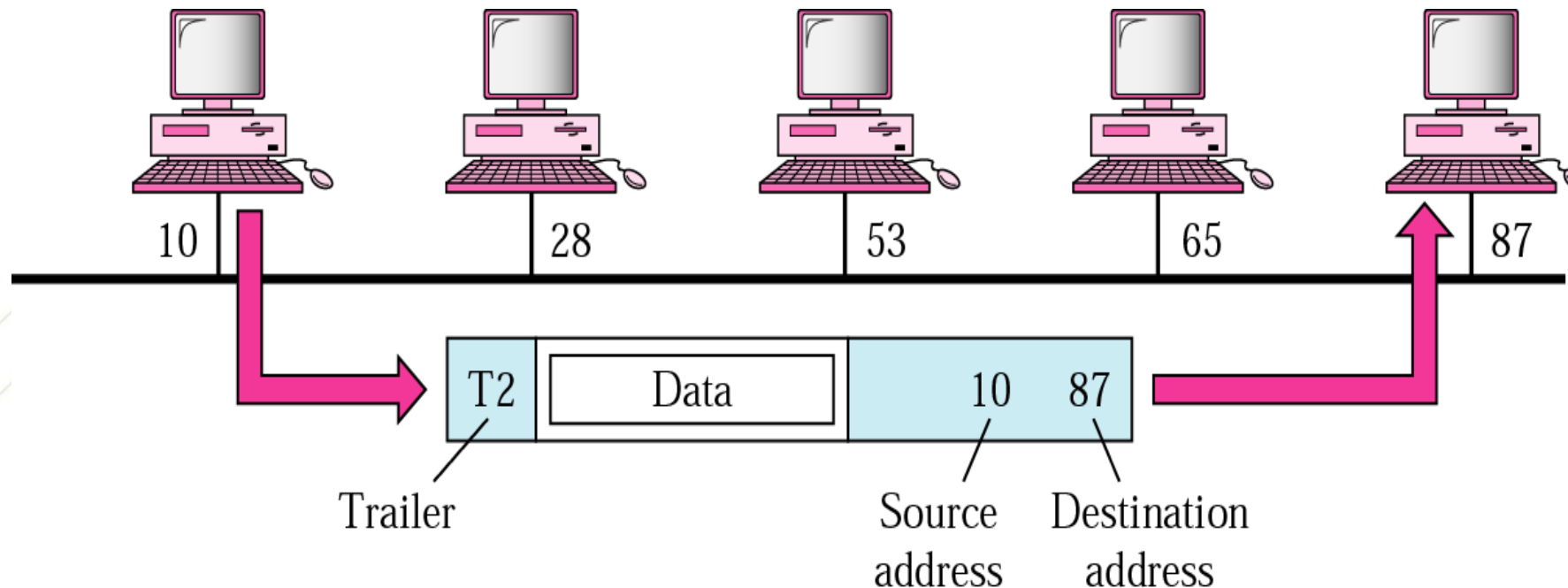
1. **Link Establishment and Termination:** Establishes and terminates logical link between two nodes.
2. **Physical addressing:** After creating frames, Data link layer adds physical addresses (MAC address) of sender and/or receiver in header of each frame.
3. **Frame Traffic Control:** Tells transmitting node to “**back-off algorithm**” when no frame buffers are available.
4. **Frame Sequencing:** Transmits/receives frames sequentially.
5. **Frame Acknowledgment:** Provides/expects frame acknowledgments. Detects and recovers from errors that occur in physical layer by **retransmitting non-acknowledged frames** and handling duplicate frame receipt.
6. **Frame Delimiting:** Creates and recognizes frame boundaries.

Functions of Data Link Layer

6. **Frame Error Checking:** Checks received frames for integrity.
7. **Media Access Management:** determines when node “has right” to use physical medium.
8. **Flow control:** Traffic regulatory mechanism implemented to prevents fast sender from drowning slow receiver. If rate at which data is absorbed by receiver is less than rate produced in sender, data link layer imposes this flow control mechanism.
9. **Error control:** To detect and retransmit damaged or lost frames. It also deals with problem of duplicate frame, thus providing reliability to physical layer.
10. **Access control:** When a single communication channel is shared by multiple devices, MAC sub-layer helps to determine which device has control over channel at a given time.
11. **Feedback:** After transmitting frames, system waits for feedback. Receiving device then sends acknowledgement frames back to source providing receipt of frames.

Example 1

- Here, a node with physical address **10** sends a frame to a node with physical address **87**. Two nodes are connected by a link. At data link level this frame contains physical addresses in header. These are only addresses needed. Rest of header contains other information needed at this level. Trailer usually contains extra bits needed for error detection



Layer 3 – Network Layer

Packets

Network
Path Determination
and IP (Logical Addressing)

- This layer is **incharge of packet addressing** , converting **logical addresses into physical addresses**.
- Responsible for source-to-destination delivery of a packet across multiple networks (links).
- Packets will use to arrive at their destination, based on factors like traffic and priorities.
- **Determines that how data transmits between network devices**
- If two systems are connected to same link, then there is no need for network layer.
- If two systems are attached to different networks with connecting devices like routers between networks, then there is need for network layer.

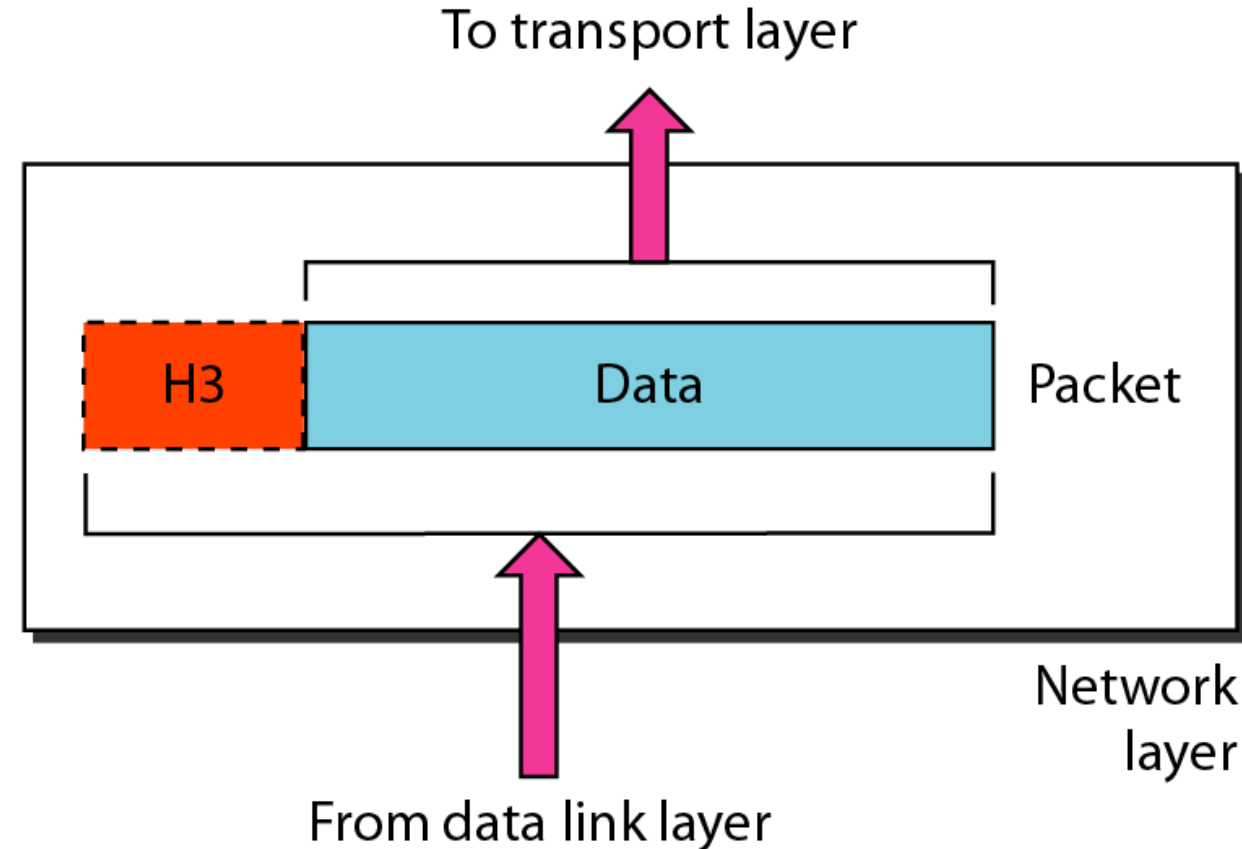
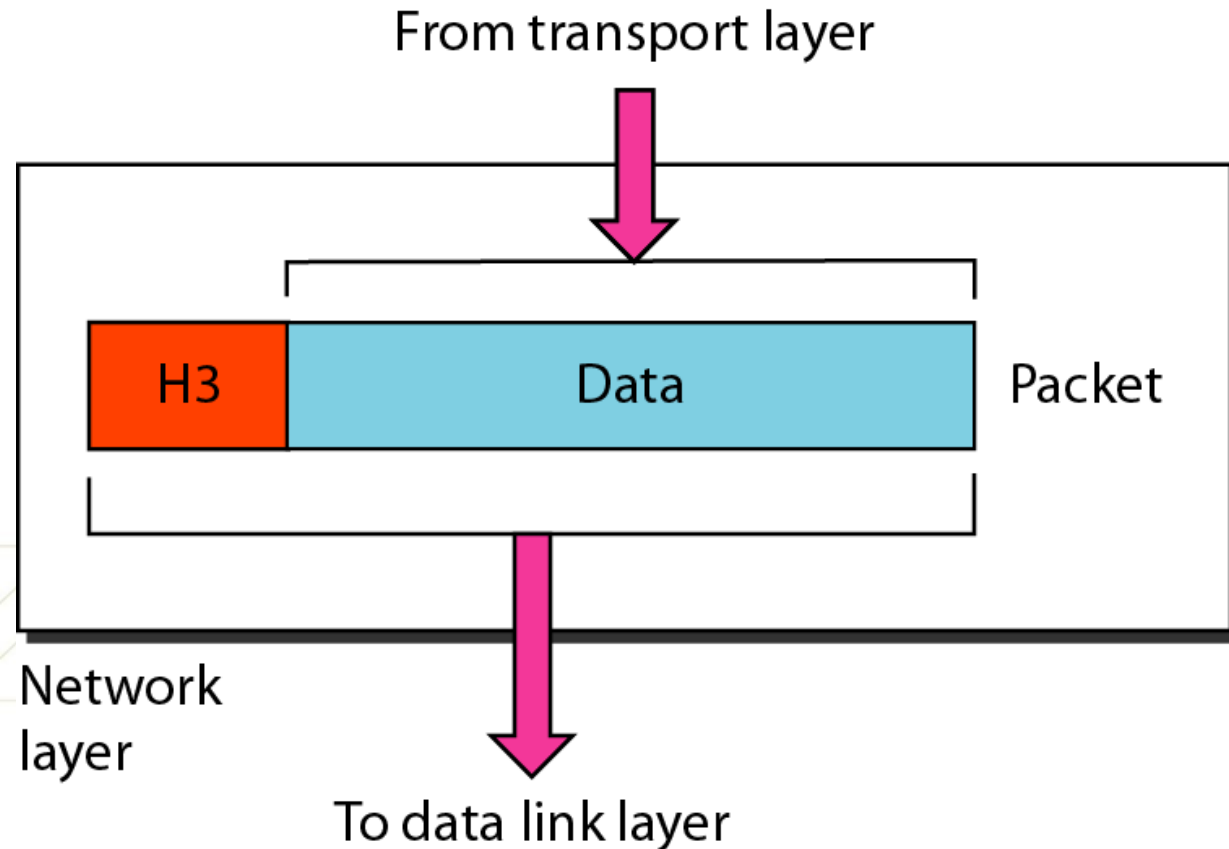
Layer 3 – Network Layer

Packets

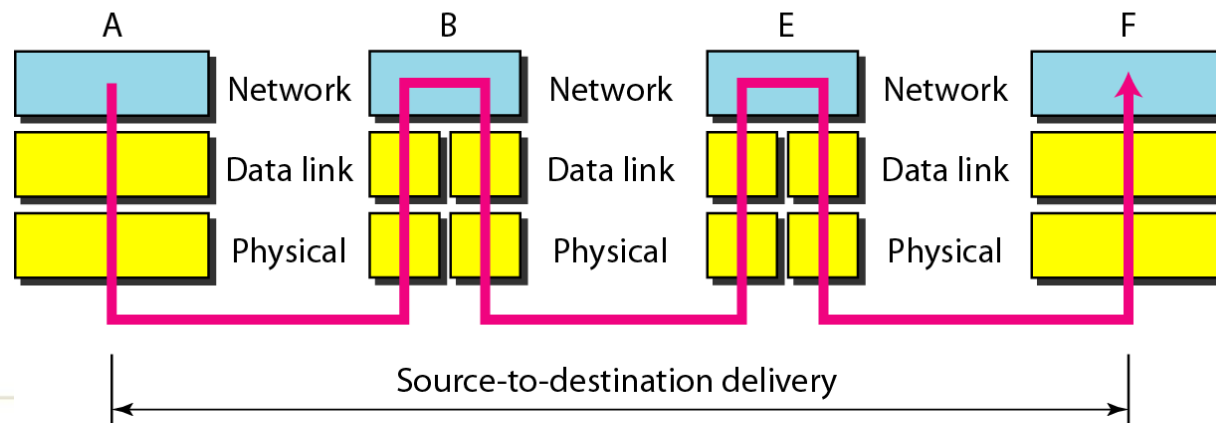
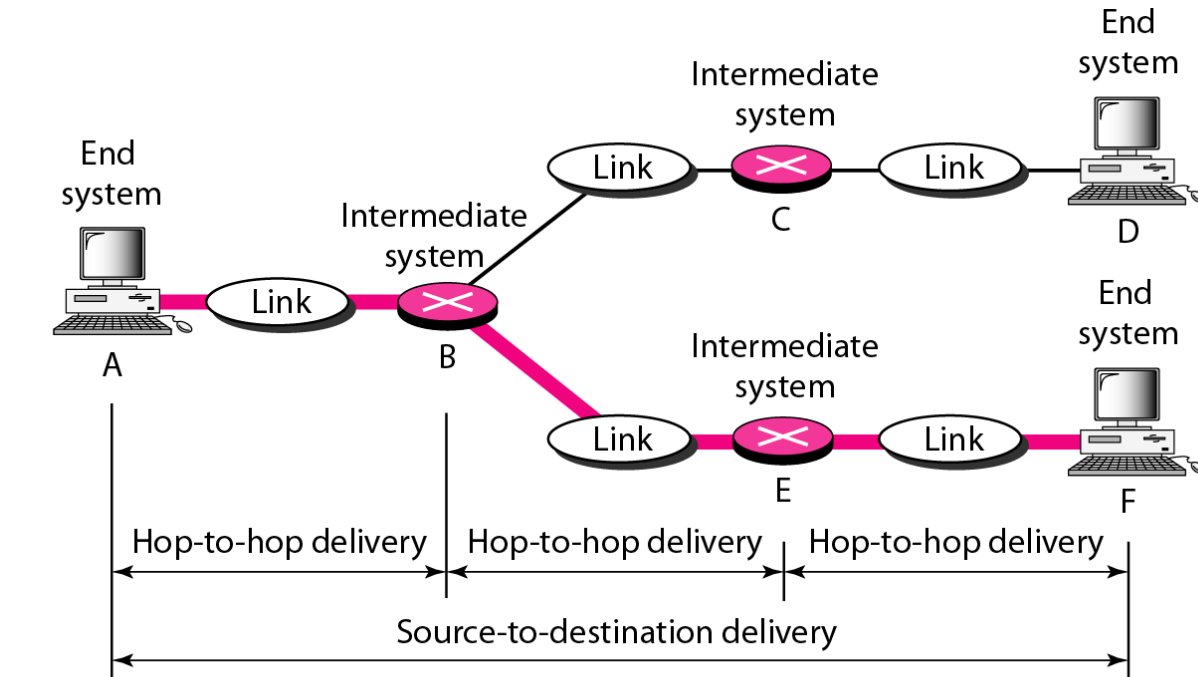
Network
Path Determination
and IP (Logical Addressing)

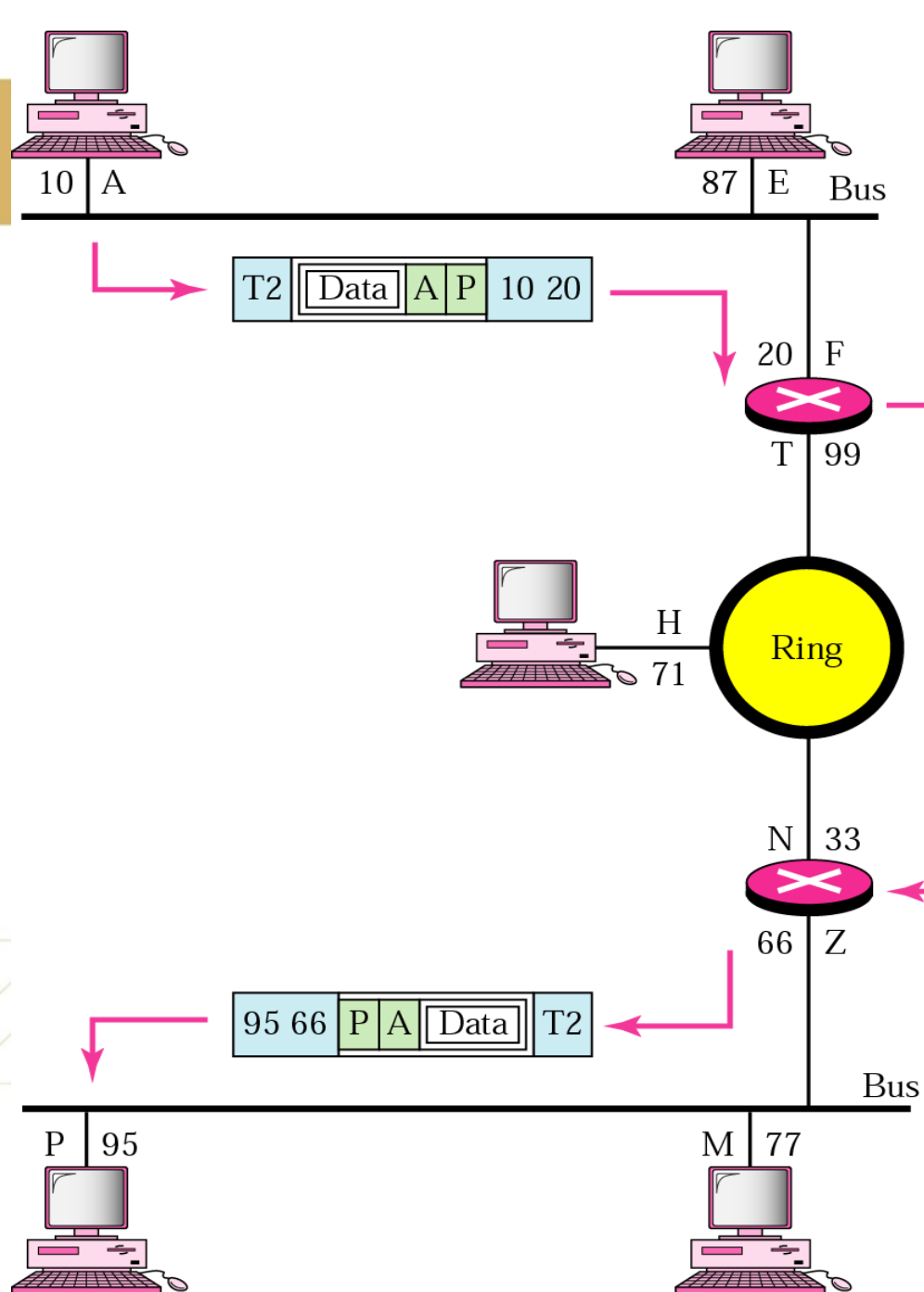
- Translates **logical address into physical address** e.g computer name into MAC address.
- Responsible for defining route, **it manages network problems and addressing**
- Controls **operation of subnet**, deciding which physical path data should take based on network conditions, priority of service, and other factors.
- **X.25 protocols works at physical, data link, and network layers.**
- Network layer lies between data link layer and transport layer. It takes services from Data link and provides services to transport layer.

Layer 3 – Network Layer



Layer 3 – Network Layer

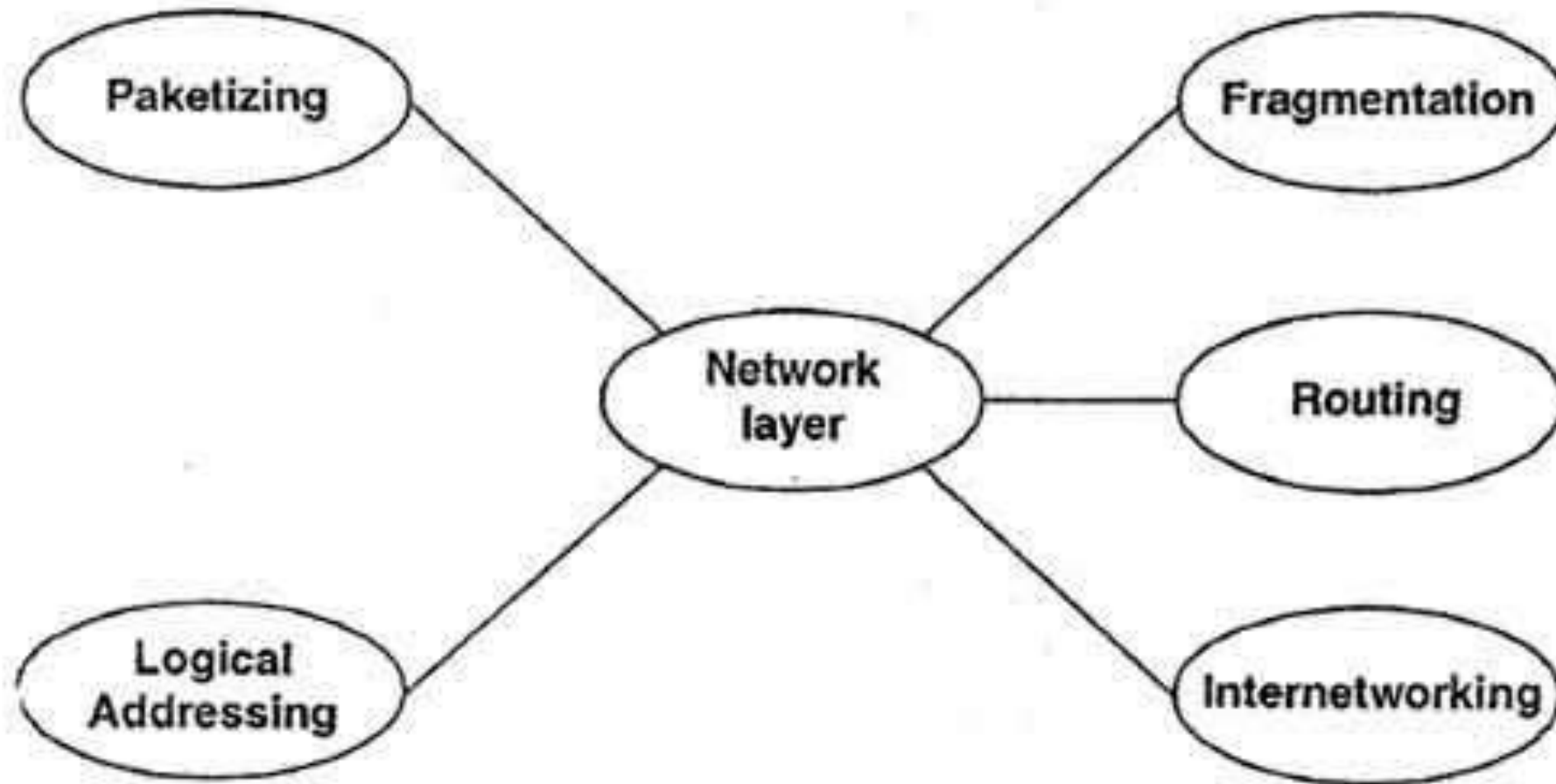




Example 2

- We want to send data from a node with network address **A** and physical address 10, located on one LAN, to a node with a network address **P** and physical address 95, located on another LAN. Because two devices are located on different networks, we cannot use physical addresses only; physical addresses only have local influence. What we need here are **universal addresses** that can pass through LAN boundaries. Network (logical) addresses have this characteristic.

Functions of Network Link Layer



Functions of Network Link Layer

1. **Subnet Traffic Control:** Routers (network layer intermediate systems) can instruct a sending station to “throttle back” its frame transmission when the router’s buffer fills up.
2. **Logical-Physical Address Mapping:** translates logical addresses, or names, into physical addresses.
3. **Subnet Usage Accounting:** has accounting functions to keep track of frames forwarded by subnet intermediate systems, to produce billing information.

In network layer and layers below, peer protocols exist between a node and its immediate neighbor, but neighbor may be a node through which data is routed, not destination station. Source and destination stations may be separated by many intermediate systems.

4. Internetworking

- To provide internetworking between different networks.
- Provides logical connection between different types of network.
- To combine various different networks to form a bigger network.

Functions of Network Link Layer

5. Logical Addressing

- Large number of different networks can be combined together to form bigger networks or internetwork.
- In order to identify each device on internetwork uniquely, network layer defines an addressing scheme.
- Such an address distinguishes each device uniquely and universally.

6. Routing

- When independent networks or links are combined together to create [internet](#) works, multiple routes are possible from source machine to destination machine.
- The network layer protocols determine which route or path is best from source to destination. This function of network layer is known as routing.
- Routes frames among networks.

Functions of Network Link Layer

7. Packetizing

- Receiving data from upper layers and creating its own packets by encapsulating these packets.
- This packetizing is done by Internet Protocol (IP) that defines its own packet format.

8. Fragmentation

- Means dividing larger packets into small fragments.
- Maximum size for a transportable packet is defined by physical layer protocol.
- Large packets are divided into fragments so that they can be easily sent on physical medium.
- If it determines that a downstream router's maximum transmission unit (MTU) size is less than frame size, a router can fragment a frame for transmission and re-assembly at destination station.

9. Protocols: Protocols working on network layer are - IP, ICMP, ARP, RIP, OSI, IPX and OSPF.

Layer 4 – Transport Layer

Segments

Transport
End-to-End Connections
and Reliability

- Transport layer (called end-to-end layer) manages end to end (source to destination) (process to process) message delivery in a network
- Ensures that all packets of a message arrive intact and in order.
- Provides acknowledgement of successful data transmission and retransmits data if found error.
- Ensures messages are delivered error-free, in sequence, and with no losses or duplications.
- Size and complexity of a transport protocol depends on type of service it can get from network layer.
- Transport layer is at core of OSI model.
- Provides services to application layer and takes services from network layer.
- Divides message received from upper layer into packets at source and reassembles these packets again into message at destination.

Layer 4 – Transport Layer



- **Transport layer provides two types of services:**

1. Connection Oriented Transmission

- a. Receiving device sends an acknowledgment to source after one or group of packet is received.
- b. Also known as reliable transport method.
- c. Slower transmission method.
- d. If data sent has problems, destination requests source for retransmission by acknowledging only packets that have been received and are recognizable.
- e. Once destination computer receives all data necessary to reassemble packet, transport layer assembles data in correct sequence and then passes it up, to session layer.

2. Connectionless Transmission

- a. Receiver does not acknowledge receipt of a packet.
- b. Sending device assumes that packet arrive just fine.
- c. Allows for much faster communication between devices.
- d. Less reliable than connection oriented.

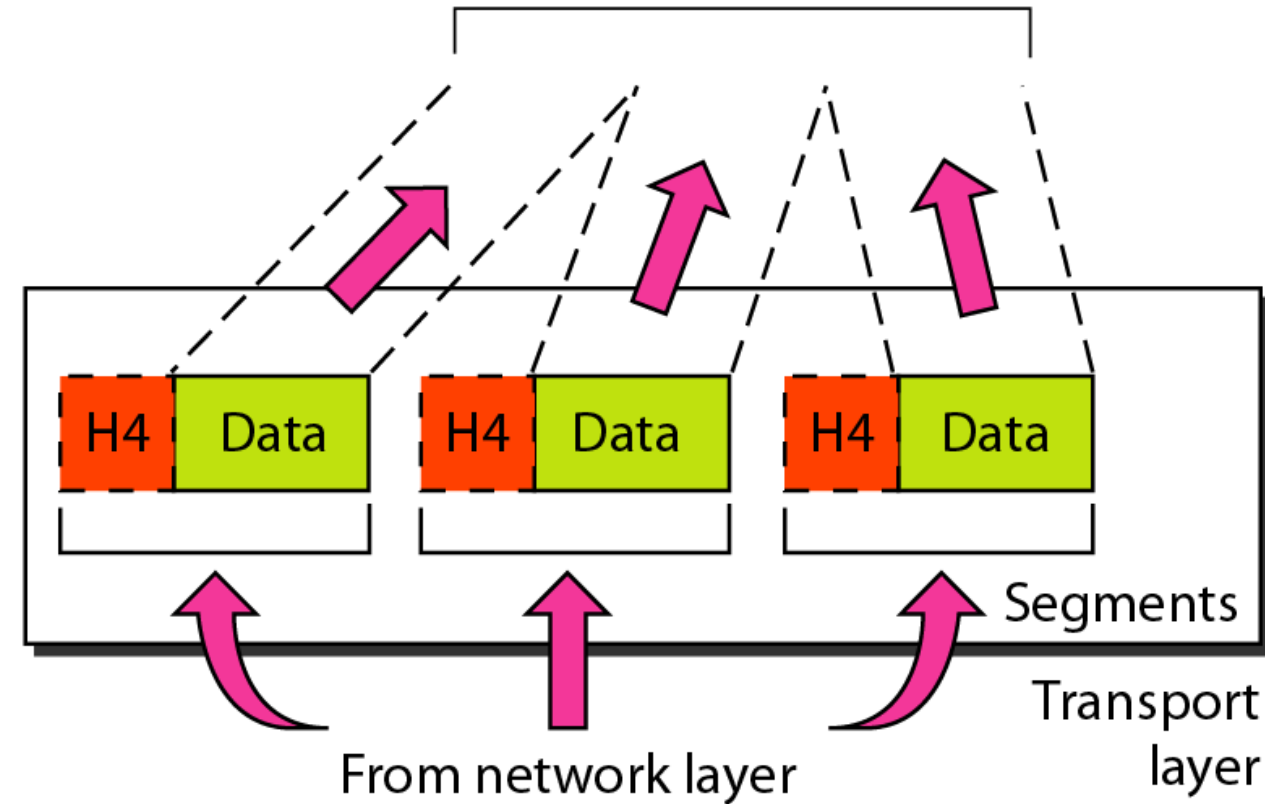
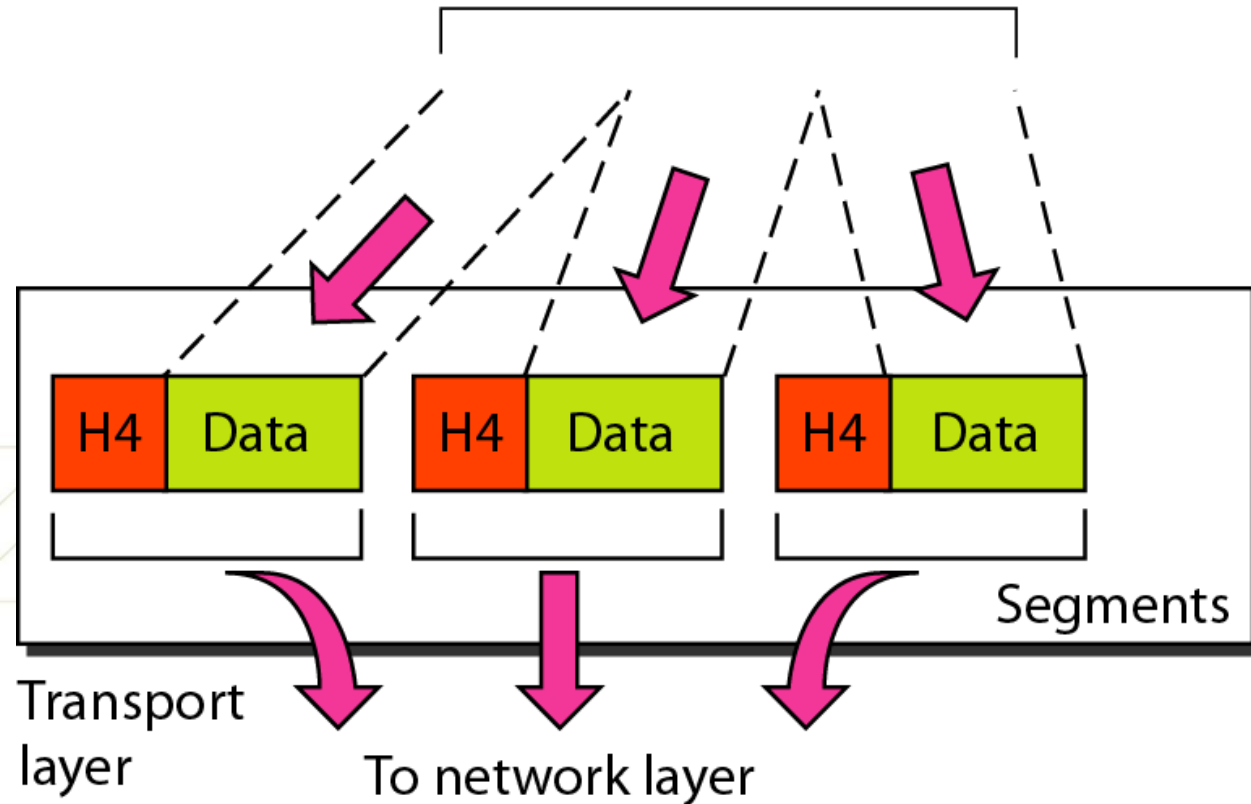
Layer 4 – Transport Layer

Segments

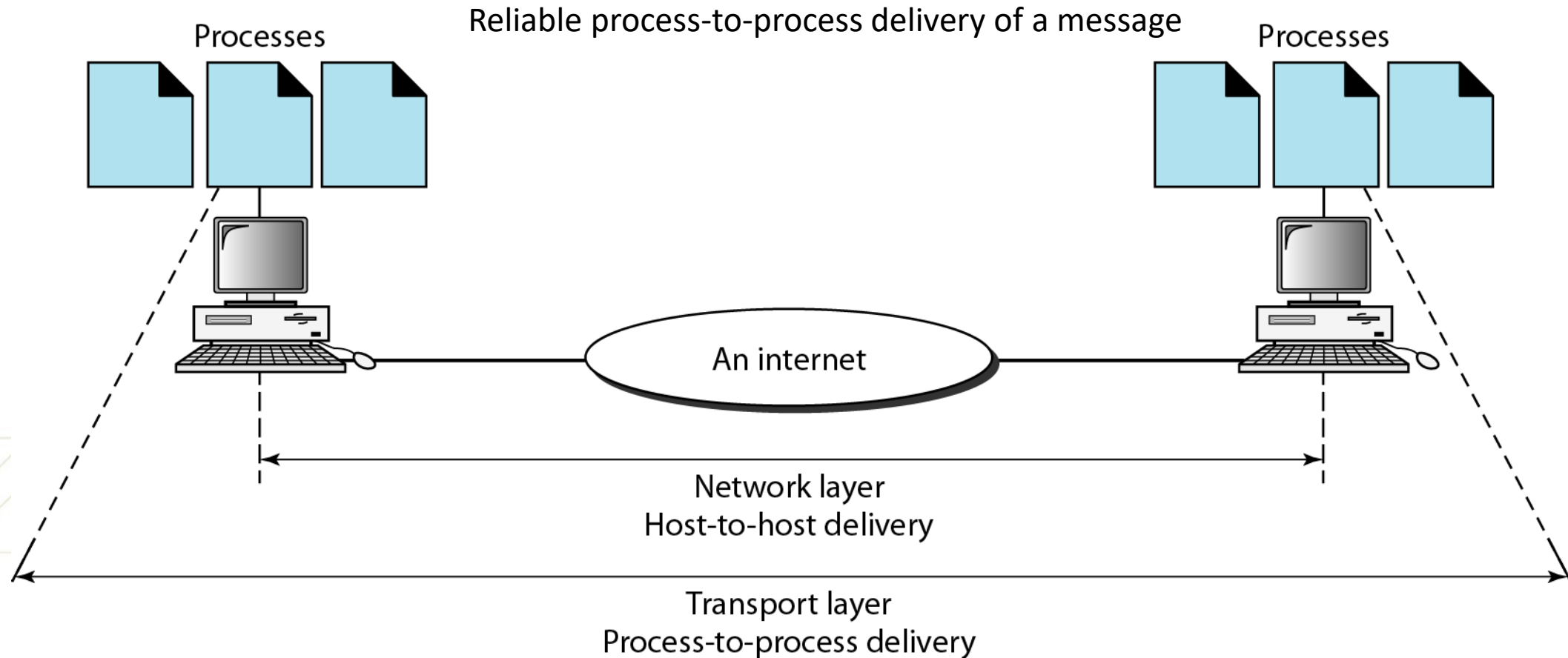
Transport
End-to-End Connections
and Reliability

From session layer

To session layer

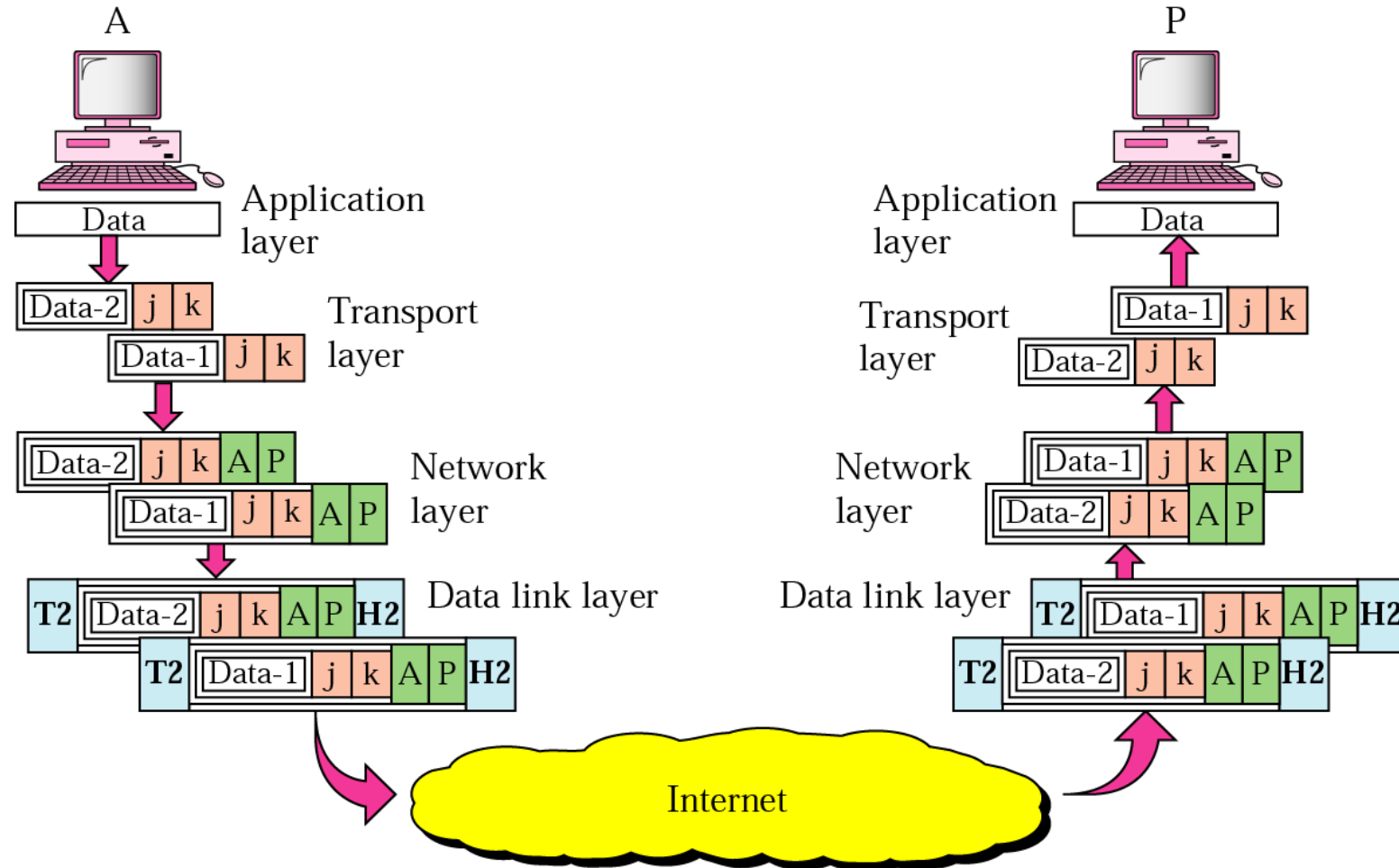


Layer 4 – Transport Layer



Example 3

- Data coming from upper layers have port addresses **j** and **k** (**j** is address of sending process, and **k** is address of receiving process). Since data size is larger than network layer can handle, data are split into two packets, each packet retaining port addresses (**j** and **k**). Then in network layer, network addresses (**A** and **P**) are added to each packet.

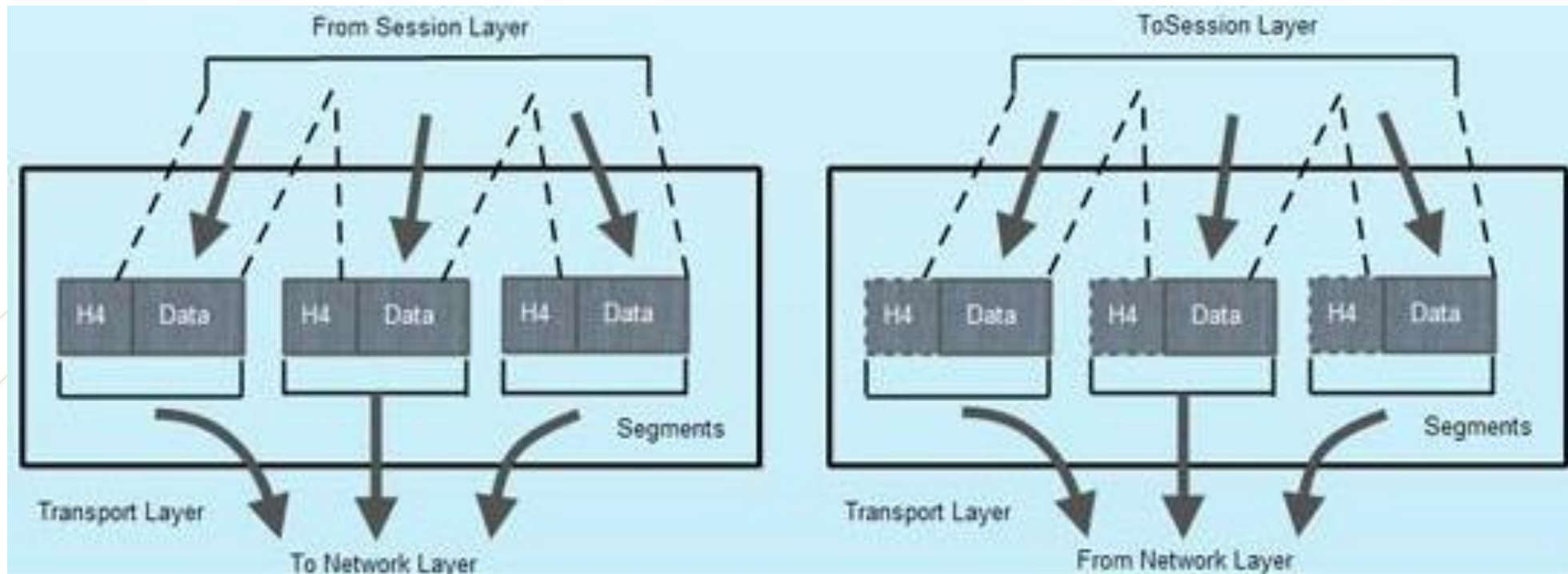


Functions of Transport Layer:

1. **Segmentation of message into packet and reassembly of packets into message:** accepts a message from (session) layer above it, splits into smaller units (if not already small enough), and passes smaller units down to network layer. Transport layer at destination station reassembles message.
2. **Message acknowledgment:** provides reliable end-to-end message delivery with acknowledgments.
3. **Message traffic control :** tells transmitting station to “back-off” when no message buffers are available.
4. **Session multiplexing :** multiplexes several message streams, or sessions onto one logical link and keeps track of which messages belong to which sessions.
5. **Service point addressing:** Purpose of transport layer is to deliver message from one process running on source machine to another process running on destination machine. It may be possible that several programs or processes are running on both machines at a time. To deliver message to correct process, transport layer header includes a type of address called **service point address or port address**. Thus by specifying this address, transport layer makes sure that message is delivered to correct process on destination machine.
6. **Protocols:** Protocols of transport layer are TCP, SPX, NETBIOS, ATP and NWLINK.

Functions of Transport Layer:

7. **Flow control:** Ensures that sender and receiver communicate at a rate they both can handle which prevents source from sending data packets faster than destination can handle. Here, flow control is performed end-to-end rather than across a link.
8. **Error control:** Here error control is performed end-to-end rather than across a single link. Sending transport layer ensures that entire message arrives at receiving transport layer without loss, error (damage, or duplication). Error correction is achieved through retransmission.



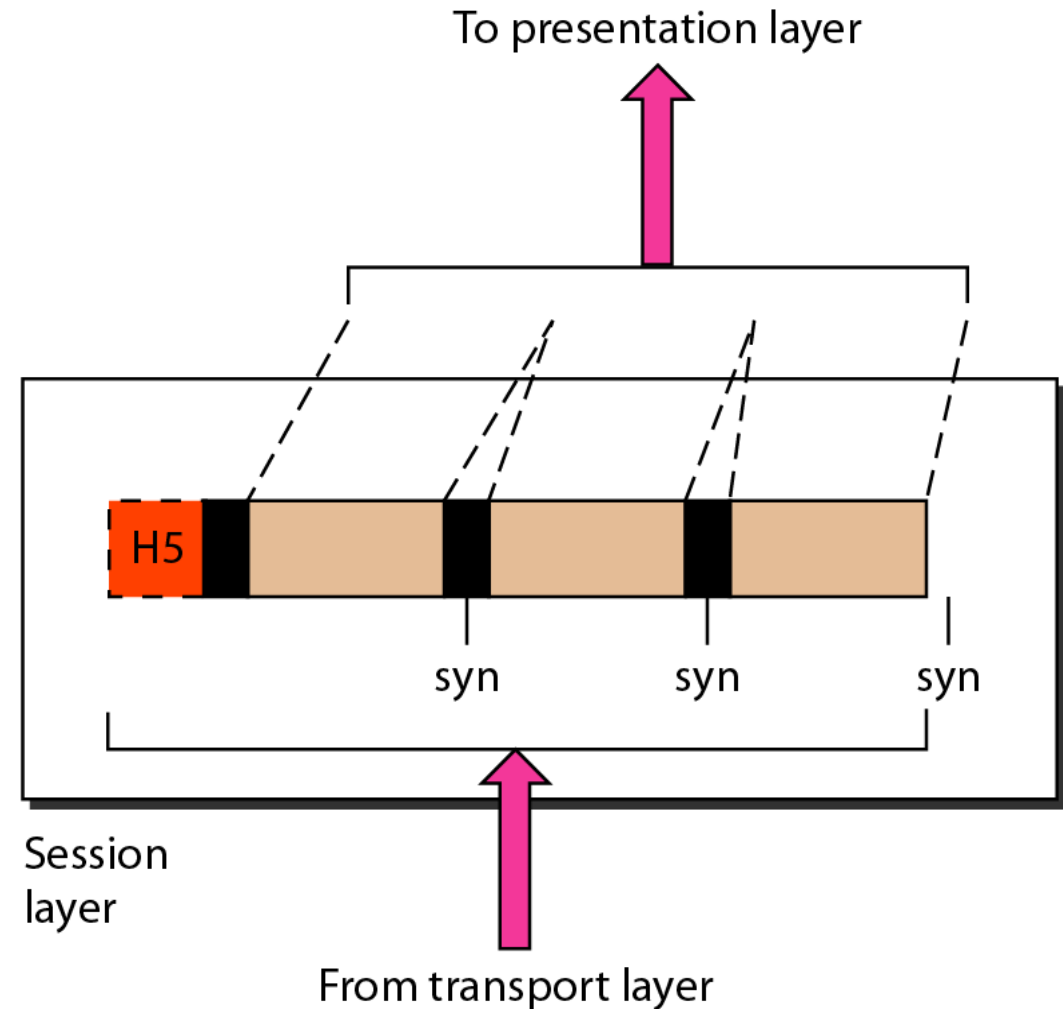
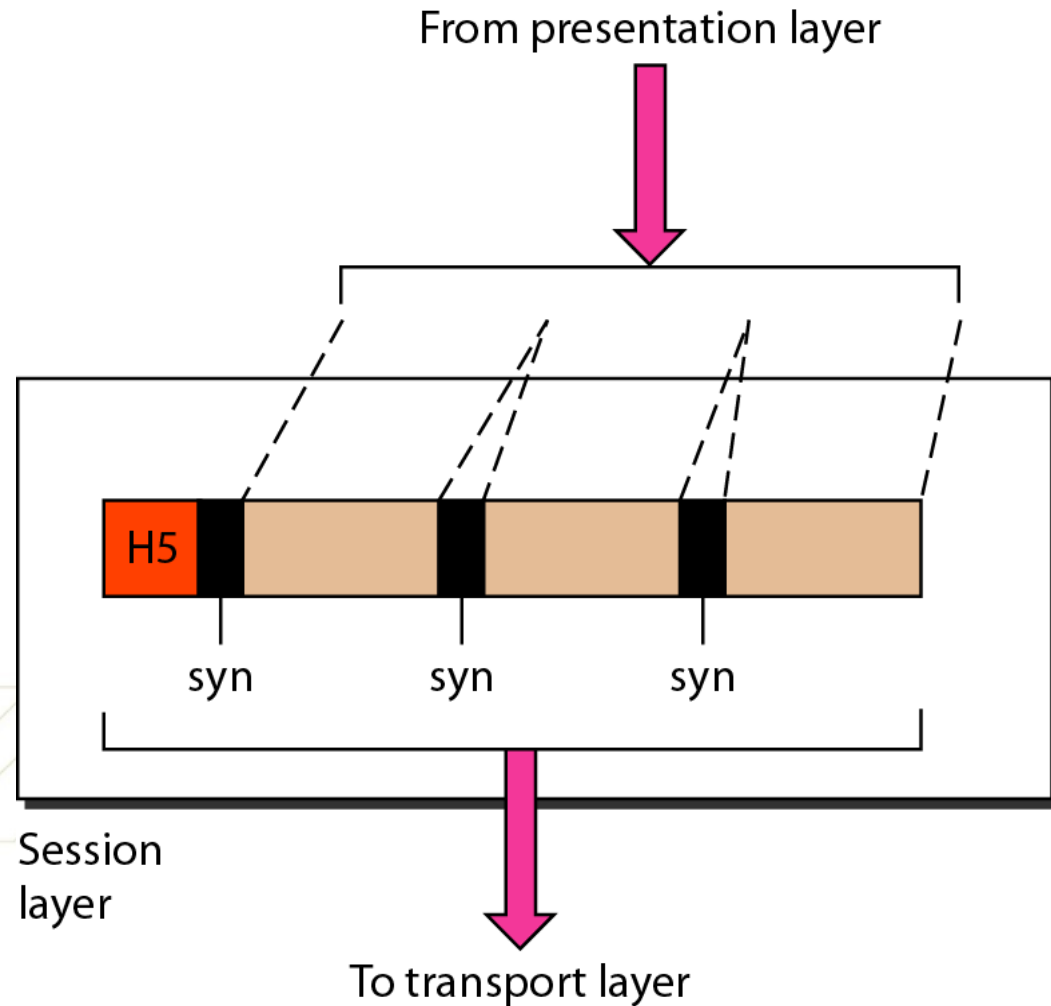
Layer 5 – Session Layer

Data

Session
Interhost Communication

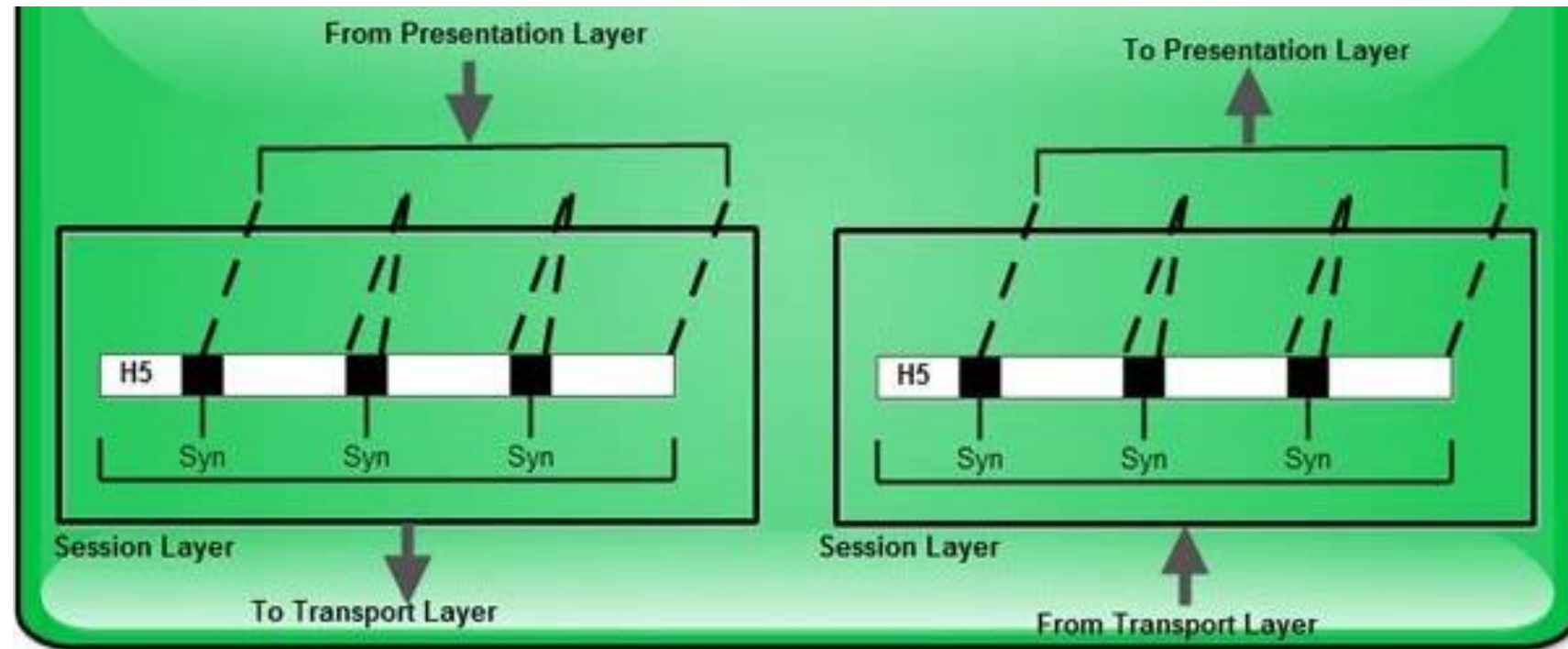
- Has primary responsibility of beginning, maintaining and ending communication between two devices, which is called Session.
- Provides for orderly communication between devices by regulating flow of data.
- Defines format of data sent over connections.
- Establishes and manages session between two users at different ends in a network.
- Manages who can transfer data in a certain amount of time and for how long.
- Reconnects session if it disconnects.
- Reports and logs and upper layer errors.
- Allows session establishment between processes running on different stations.
- **Dialogue control and token management are responsibility of session layer.**

Functions of Session Layer:



Session Layer:

- **Session establishment, maintenance and termination** : allows two application processes on different machines to establish, use and terminate a connection, called a session.
- **Session support** : performs functions that allow these processes to communicate over network, performing security, name recognition, logging and so on.
- **Dialog control**: Determines which device will communicate first and amount of data that will be sent.



Functions of Session Layer:

- **Dialog control:** Determines which device will communicate first and amount of data that will be sent.

When a device is contacted first, session layer is responsible for determining which device participating in communication will transmit at a given time as well as controlling amount of data that can be sent in a transmission. This is called dialog control.

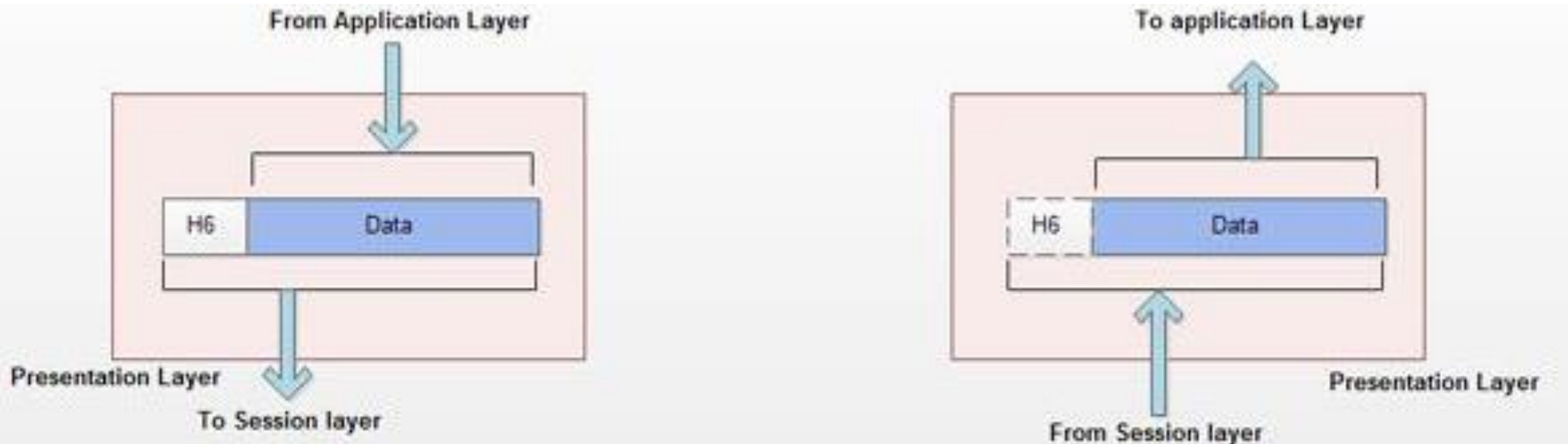
The types of dialog control that can take place include simplex, half duplex and full duplex.

- **Dialog separation or Synchronization:** Responsible for adding checkpoint or markers within message. Process of inserting markers to stream of data is known as dialog separation.
- **Protocols:** Protocols for session layer are **NetBIOS, Mail Slots, Names Pipes, and RPC.**

Layer 6 – Presentation Layer

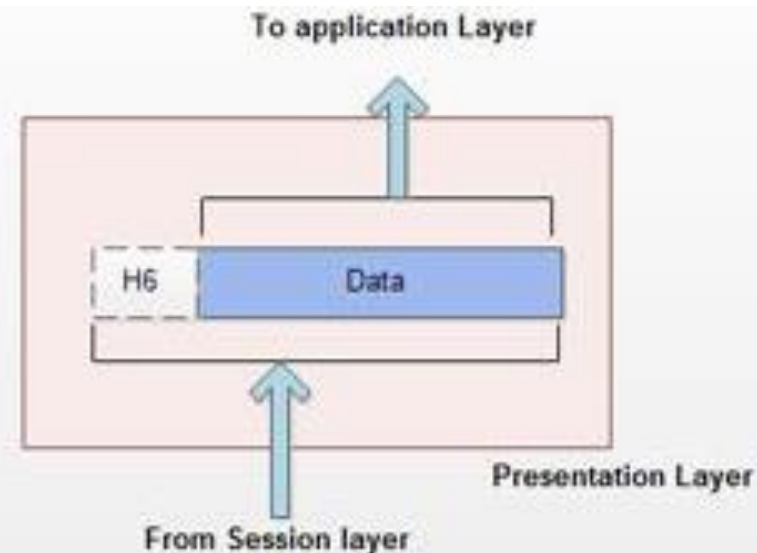
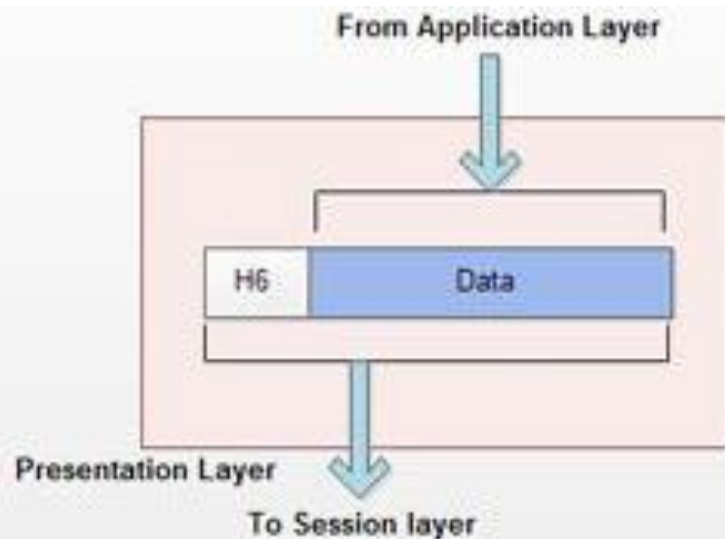
Data	Presentation Data Representation and Encryption
------	---

- Also called **Translation layer**.
- Presents data into a uniform format and masks difference of data format between two dissimilar systems.
- Presentation layer formats data to be presented to application layer.
- Can be viewed as translator for network.
- This layer may translate data from a format used by application layer into a common format at sending station, and then translate common format to a format known to application layer at receiving station.

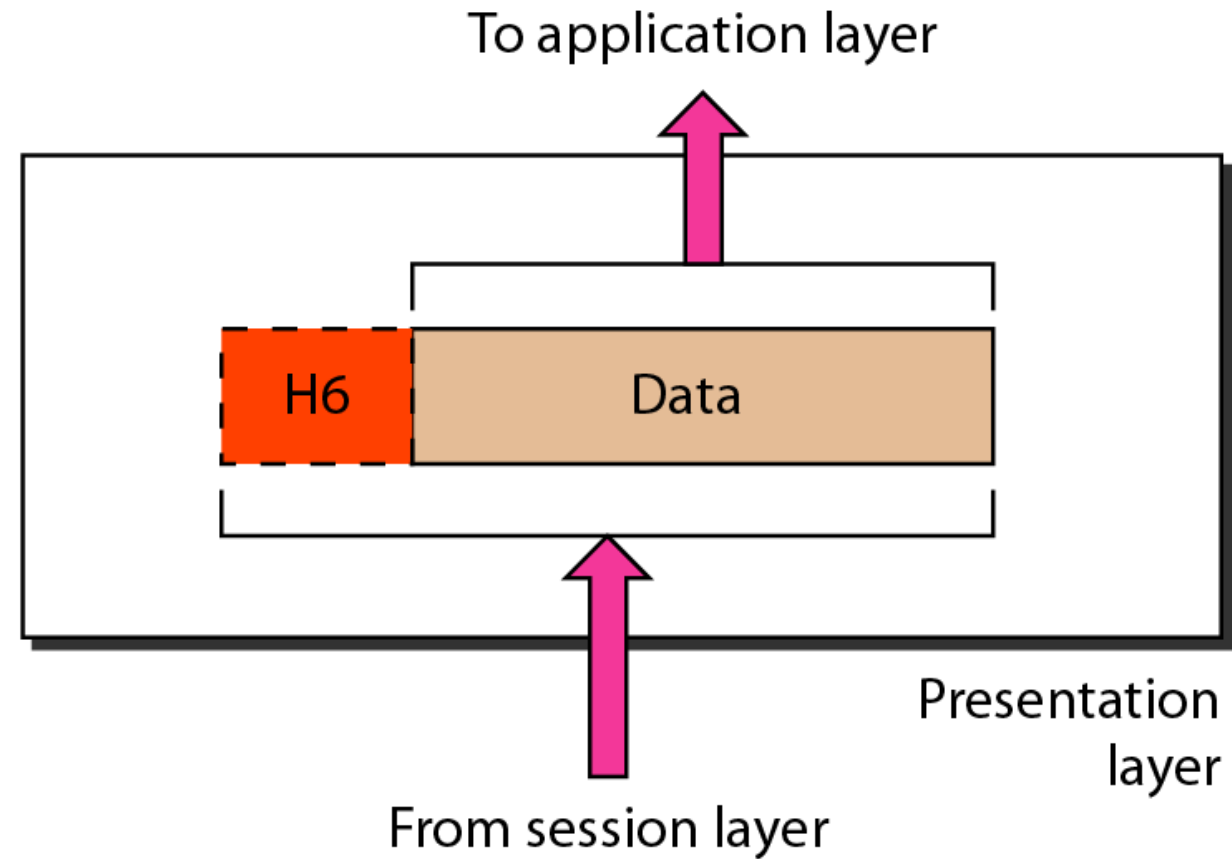
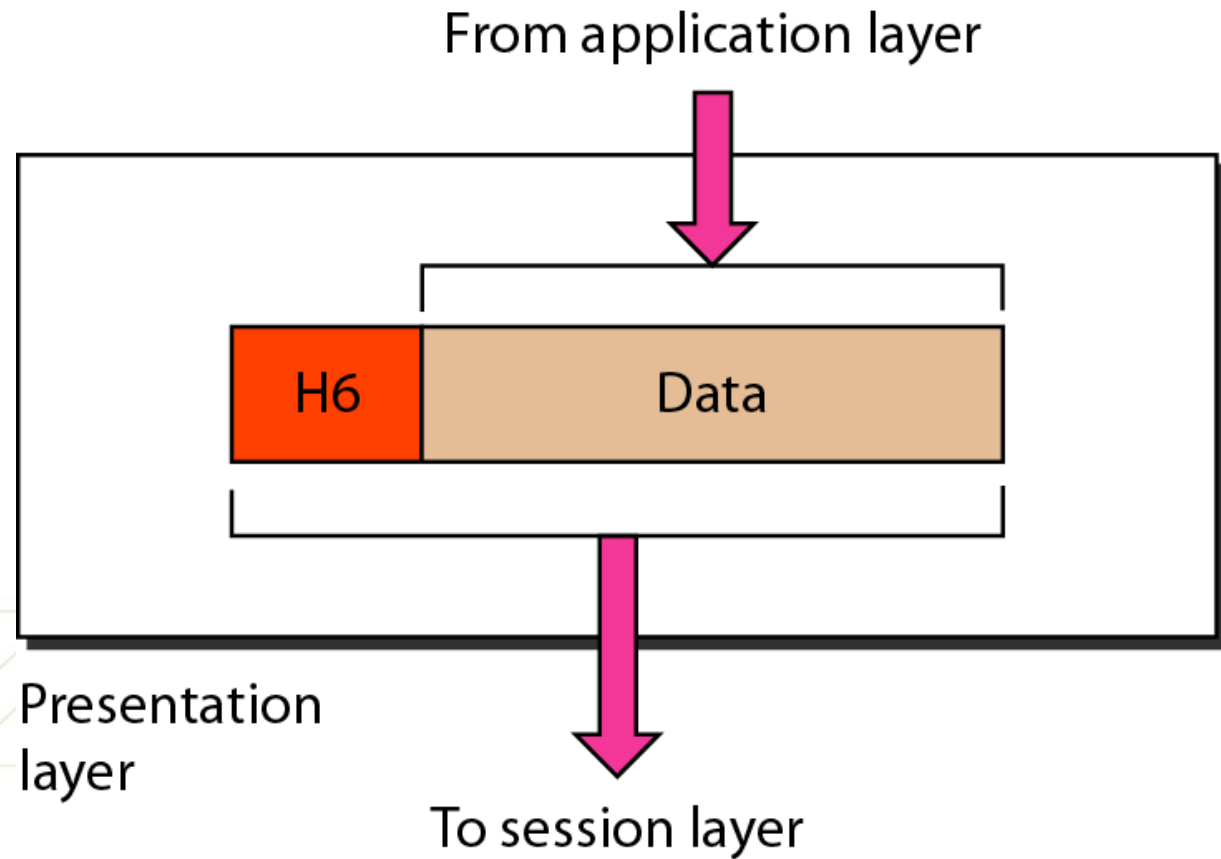


Functions of Presentation Layer:

- ❑ **Character code translation** : for example, ASCII to EBCDIC.
- ❑ **Data conversion** : bit order, CR-CR/LF, integer-floating point, and so on.
- ❑ **Data compression** : reduces number of bits that need to be transmitted on network.
- ❑ **Data encryption** : encrypt data for security purposes. For example, password encryption.



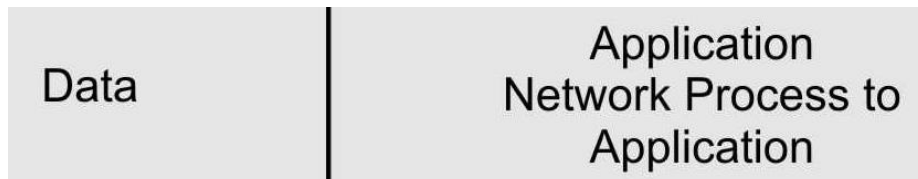
Functions of Presentation Layer:



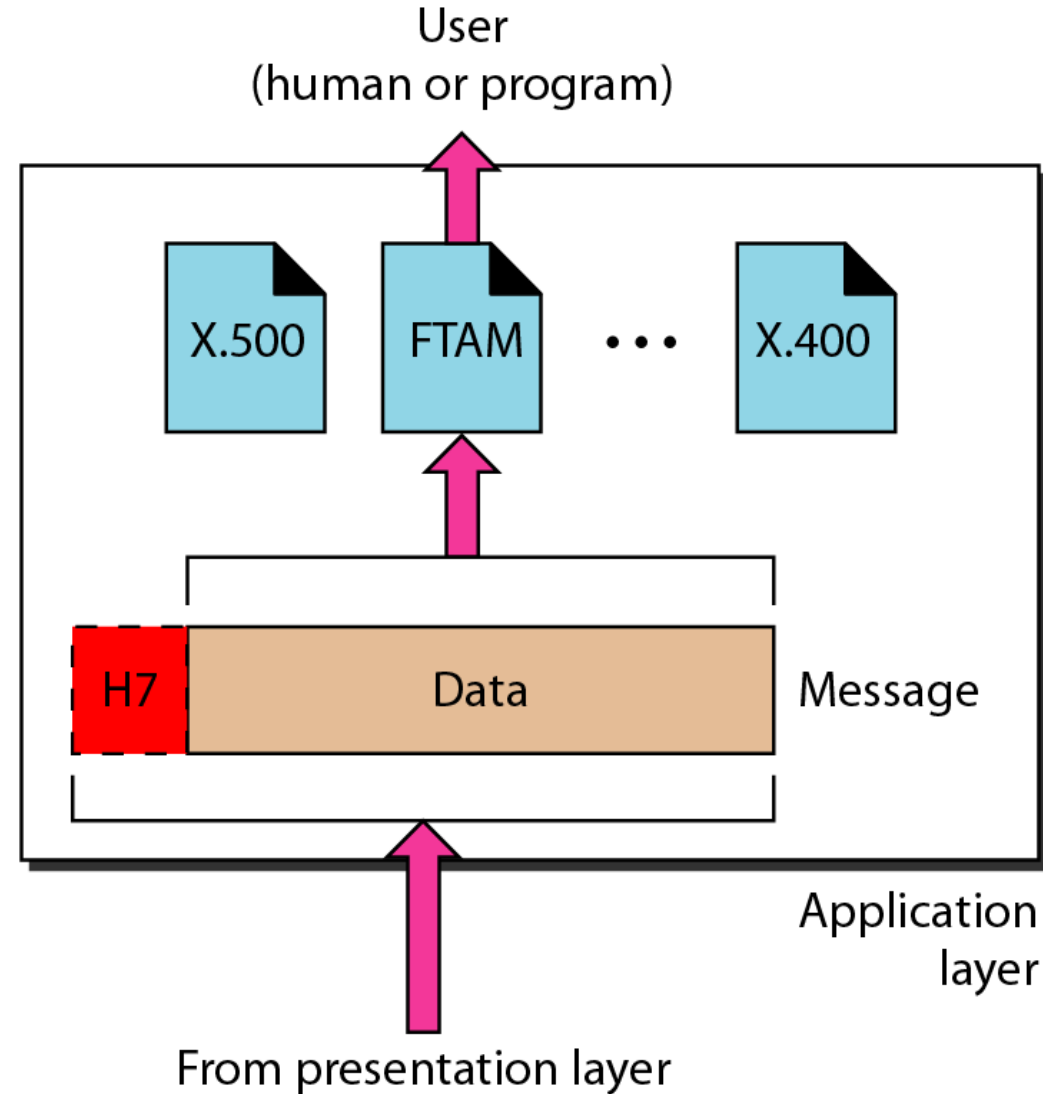
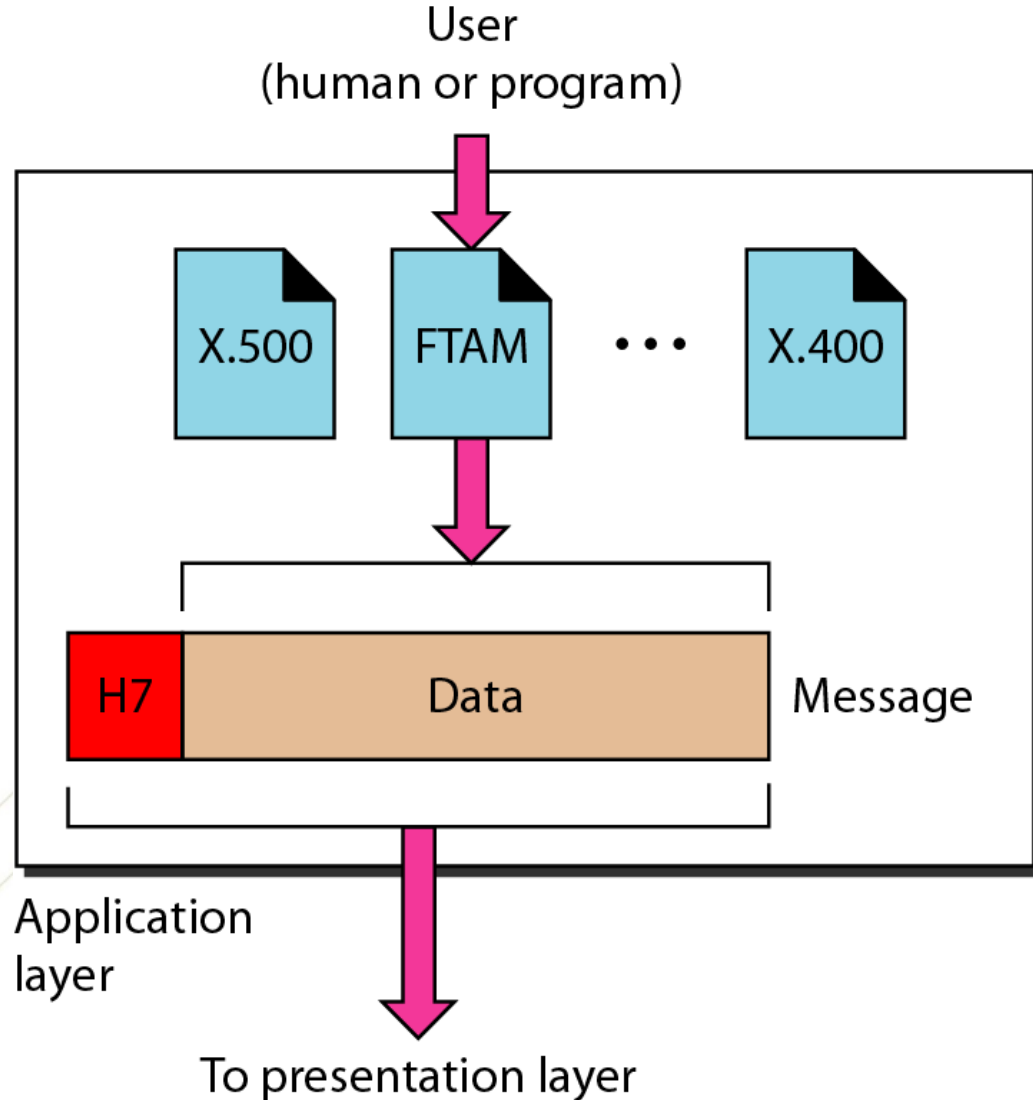
Layer 7 – Application Layer

- Serves as window for users and application processes to access network services.
- Implemented in End system.
- Makes interface between program that is sending or is receiving data and protocol stack.
- When you download or send emails, your e-mail program contacts this layer.
- This layer provides network services to end-users like Mail, ftp, telnet, DNS.

1.	FTP	File Transfer Protocol
2.	DHCP	Dynamic Host Configuration Protocol
3.	DNS	Domain Name System
4.	NFS	Network File System
5.	SMTP	Simple Mail Transfer Protocol
6.	POP3	Post Office Protocol-3
7.	SNMP	Simple Network Management Protocol
8.	HTTP	Hyper Text Transfer Protocol
9.	BGP	Border Gateway Protocol
10.	RIP	Routing Information Protocol



Layer 7 – Application Layer

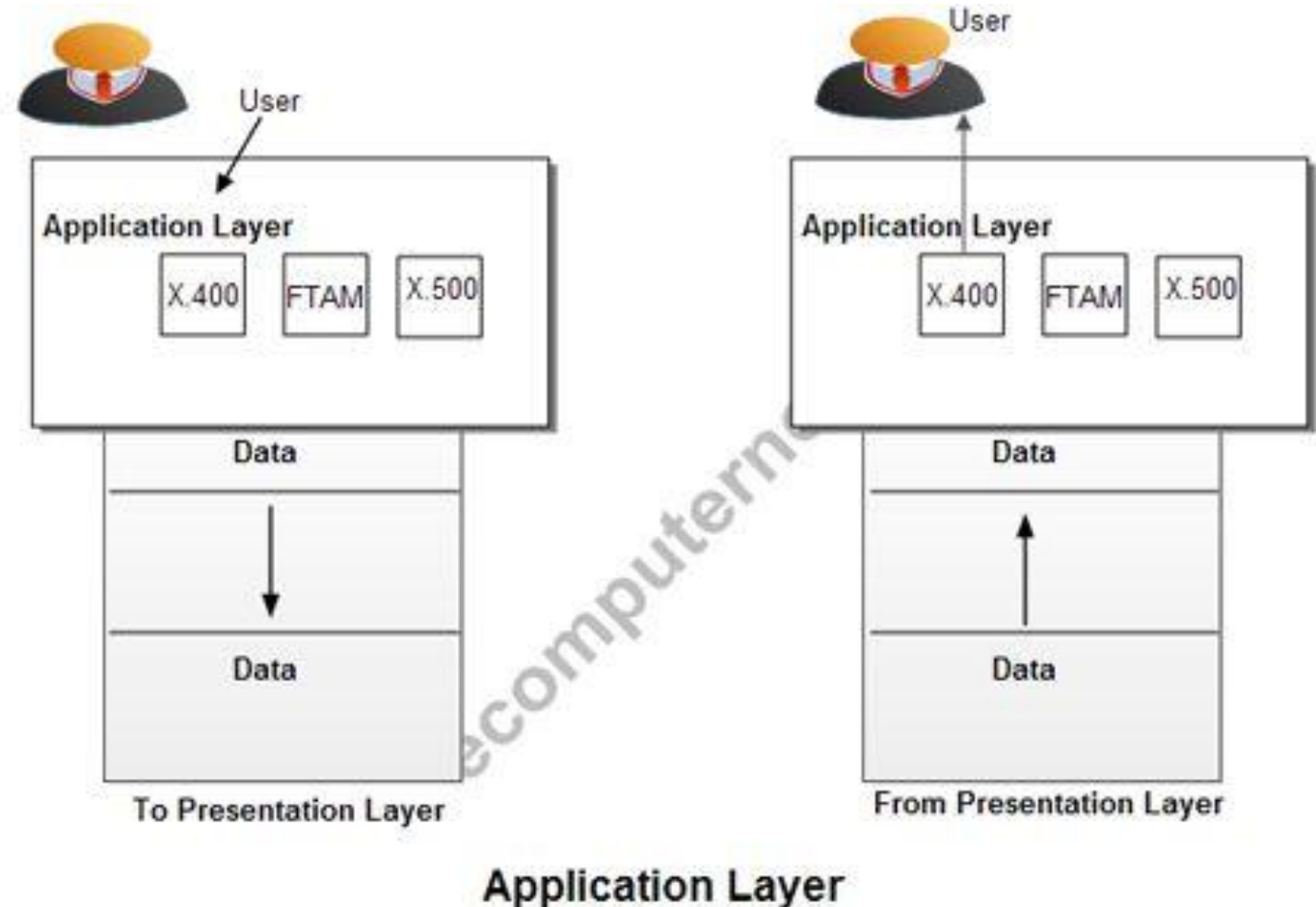


Function Of Application Layer:

- ☐ Resource sharing and device redirection.
- ☐ Remote file access.
- ☐ Remote printer access.
- ☐ Inter-process communication.
- ☐ Network management.
- ☐ Directory services.
- ☐ Electronic messaging (such as mail).

Function Of Application Layer:

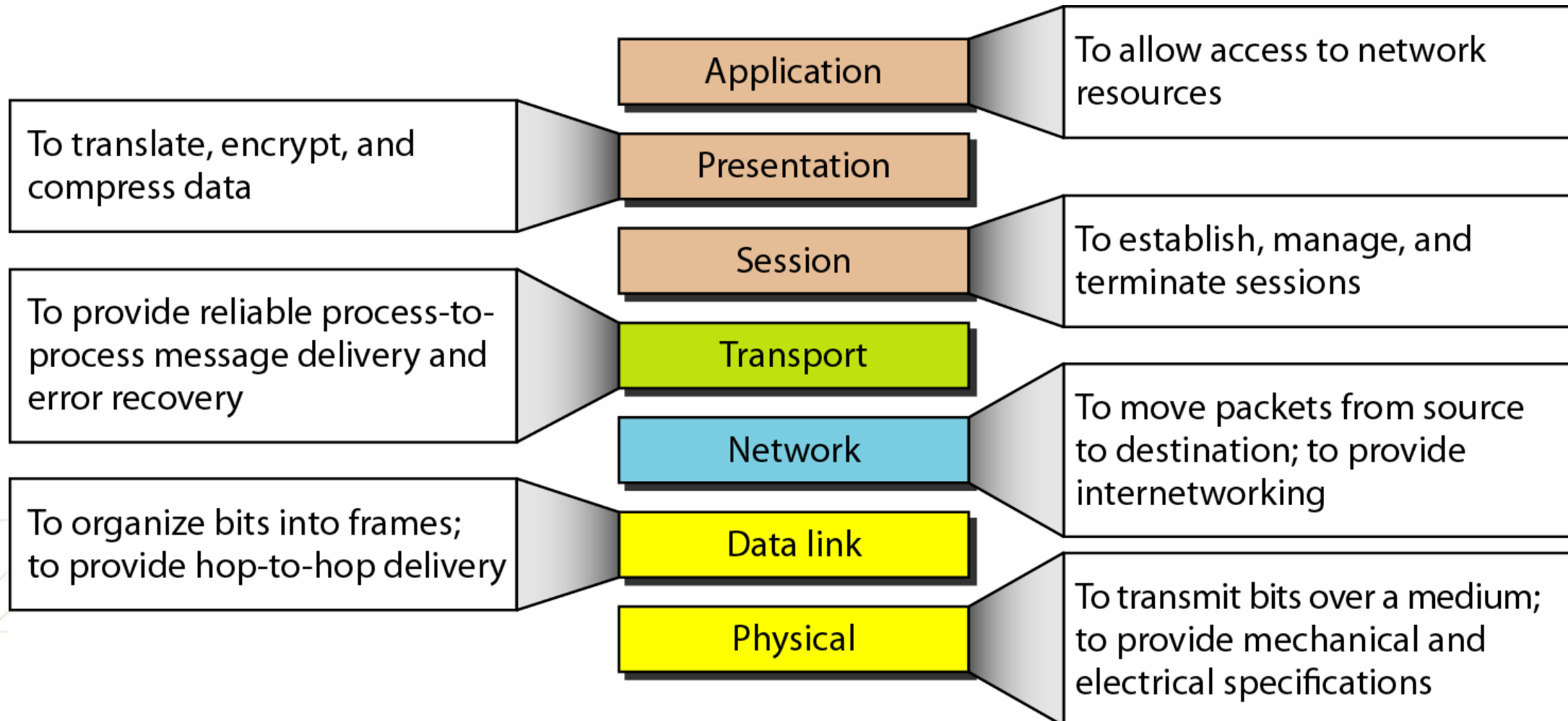
- **Network Virtual Terminal:** Software version of a physical terminal and allows a user to log on to a remote host. For this, application layer creates a software emulation of a terminal at remote host. User's computer talks to software terminal which, in turn, talks to host and vice-versa. Remote host believes it is communicating with one of its own terminals and allows user to log on.





Function of Application Layer:


- **File transfer, access and management (FTAM):** Allows a user to access a file in a remote host to make changes or to read data, to retrieve files from remote computer for use in local computer, and to manage or control files in a remote computer locally.
- **Mail services:** It provides various e-mail services such as email forwarding and storage.
- **Directory services:** This application provides distributed database sources and access for global information about various objects and services.
- **Protocols** used at application layer are FTP, DNS, SNMP, SMTP, FINGER, and TELNET.

Summary of Layers



Summary Of Layers

OSI Model			
	Data unit	Layer	Function
User support layers 	Data	7. Application	Network process to application
		6. Presentation	Data representation and encryption
		5. Session	Inter-host communication
User ↔ Network	Segment	4. Transport	End-to-end connections and reliability
Network support layers 	Packet	3. Network	Path determination and logical addressing
	Frame	2. Data Link	Physical addressing
	Bit	1. Physical	Media, signal and binary transmission


Receiver

TCP/IP Model

- Specification for computer network protocols created in 1970s by DARPA, an agency of United States Department of Defense.
- Laid foundation for ARPANET, which was world's first WAN network and a predecessor of Internet.
- **Layers in the TCP/IP Model**
 - TCP/IP is generally described as having four 'layers' or five if we include bottom physical layer.
 - Layers near top are logically closer to user application, while those near bottom are logically closer to physical transmission of data.

TCP/IP Application Layer

- Provide services to application software running on a computer.
- Identifies application running on computer through Port Numbers.
- Various Application Layer protocols are:
 - **Telnet:** Terminal Emulation is a program that runs on computer and connects PC to a server on network. Then, enter commands through Telnet program which will be executed as if entered directly on server console. **Port Number :23**
 - **FTP:** File Transfer Protocol, used for exchanging files over Internet. Most commonly used to download a file from a server using Internet or to upload a file to a server. **Port Number : 20(data port) ,21(control port)**
 - **HTTP:** Hyper Text Transfer Protocol, used by World Wide Web. Defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, Entering URL in browser, sends an HTTP command to Web server directing it to fetch and transmit requested Web page. **Port Number :80**

TCP/IP Application Layer

- Various Application Layer protocols are:
 - **NFS:** Network File System, a client/server application that allows all network users to access shared files stored on computers of different types. Users can manipulate shared files as if they were stored locally on user's own hard disk. **Port Number :2049**
 - **SMTP:** Simple Mail Transfer Protocol, used for sending e-mail messages between servers. Used to send messages from a mail client to a mail server. **Port Number :25**
 - **POP3:** Post Office Protocol, used to retrieve e-mail from a mail server. Most e-mail applications (sometimes called an e-mail client) use POP, although some can use newer IMAP (Internet Message Access Protocol) as a replacement for POP3 **Port Number :110**
 - **TFTP:** Trivial File Transfer Protocol, simple form of File Transfer Protocol (FTP). TFTP provides no security features. Used by servers to boot diskless workstations, X-terminals, and routers. **Port Number :69**

TCP/IP Application Layer

- Various Application Layer protocols are:
 - **DNS:** Domain Name System (or Service or Server), an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. For example, domain name www.example.com might translate to 198.105.232.4. **Port Number :53**
 - **DHCP:** Dynamic Host Configuration Protocol, used for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to network. Dynamic addressing simplifies network administration because software keeps track of IP addresses rather than requiring an administrator to manage task. **Port Number : 67(Server),68(Client)**
 - **BOOTP:** Bootstrap Protocol (BOOTP) is utilized by diskless workstations to gather configuration information from a network server. This enables workstation to boot without requiring a hard or floppy disk drive. **Port Number : 67(Server),68(Client)**
 - **SNMP:** Simple Network Management Protocol, used for managing complex networks. SNMP works by sending messages, called protocol data units (PDUs), to different parts of a network. **Port Number :161**

TCP/IP Transport Layer

- Host-to-host layer (Transport layer).
- Responsible for end-to-end data integrity.
- Identifies segments through Socket address (Combination of Port Number & I.P. address).
- Two most important protocols are
 - ❑ **Transmission Control Protocol (TCP):** Provides reliable, full-duplex connections and reliable service by ensuring that data is retransmitted when transmission results in an error (end-to-end error detection and correction). Enables hosts to maintain multiple, simultaneous connections.
 - ❑ **User Datagram Protocol (UDP):** When error correction is not required, UDP provides unreliable datagram service (connectionless) that enhances network throughput at host-to-host transport layer. Used primarily for broadcasting messages over a network.

TCP/IP Internet Layer

- Internet Protocol (IP), provides basic packet delivery service for all TCP/IP networks node addresses, IP implements a system of logical host addresses called IP addresses.
- IP addresses are used by internetwork and higher layers to identify devices and to perform internetwork routing.
- Used by all protocols in layers above and below it to deliver data, which means all TCP/IP data flows through IP when it is sent and received, regardless of its final destination.
- Basic protocols used at Internet Layer are:
 1. I.P. (Internet Protocol)
 2. ARP (Address Resolution Protocol)
 3. RARP(Reverse Address Resolution Protocol)
 4. I.C.M.P.(Internet Control Message Protocol):
 5. I.G.M.P. (Internet Group Management Protocol)

Internet Layer protocols are

1. I.P. (Internet Protocol): Used at internet layer of TCP/IP model by which data is encapsulated and is sent from one computer to another on Internet.
2. ARP (Address Resolution Protocol): Used to map known I.P. addresses into Physical address.
3. RARP(Reverse Address Resolution Protocol): Used to map Physical address into I.P. address
4. I.C.M.P.(Internet Control Message Protocol): Used to send error & control Messages in network
5. I.G.M.P. (Internet Group Management Protocol): Used to form multicast groups in a network to receive multicast messages.

TCP/IP Network Access Layer



- Lowest layer in TCP/IP model.
- Contains protocols that computer uses to deliver data to other computers and devices that are attached to network.
- Protocols at this layer perform three distinct functions:
 - ❑ Define how to use network to transmit a frame, which is data unit passed across physical connection.
 - ❑ Exchange data between computer and physical network.
 - ❑ Deliver data between two devices on same network using physical address.
- Includes a large number of protocols including Ethernet protocols, Point-to Point Protocol (PPP) and Frame Relay.



OSI Versus TCP/IP

OSI Model Layers

Application
Layer

Presentation
Layer

Session
Layer

Transport
Layer

Network
Layer

Data-Link
Layer

Physical
Layer

TCP/IP Protocol Architecture Layers

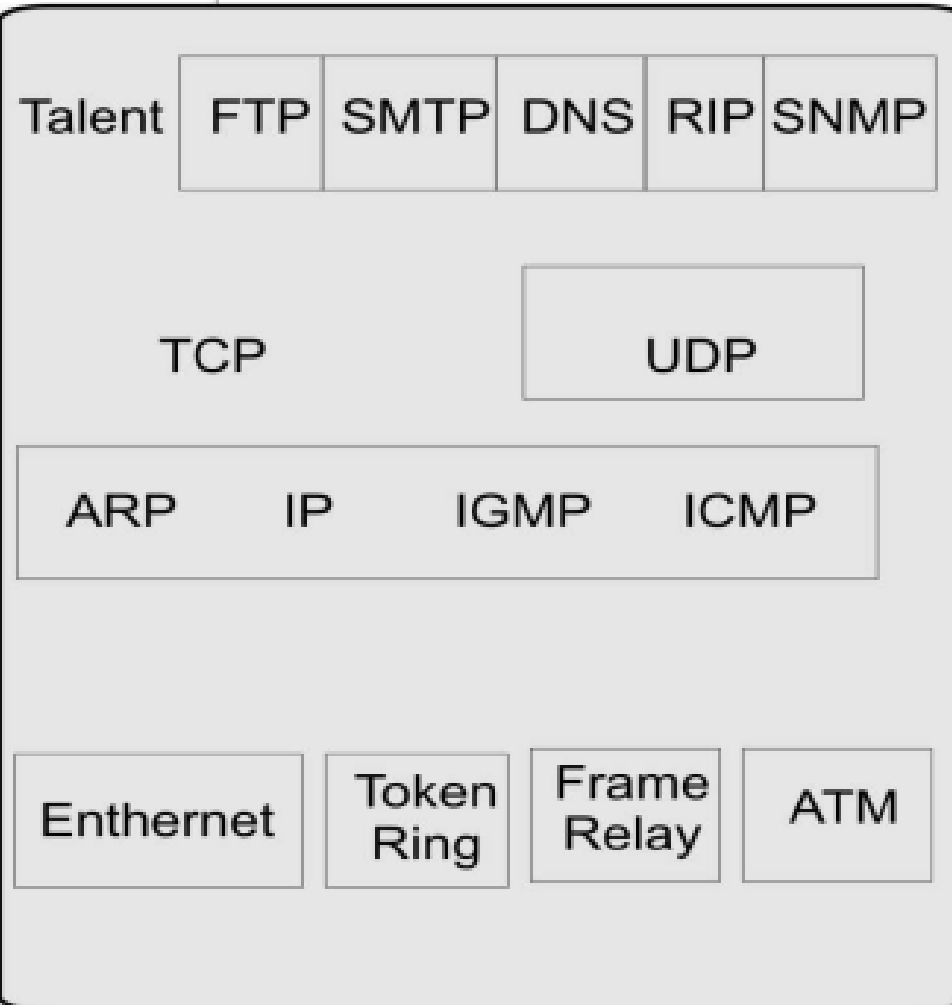
Application
Layer

Host-to-Host
Transport
Layer

Internet
Layer

Network
Interface
Layer

TCP/IP Protocol Suite



Similarities ----OSI Versus TCP/IP

- **Architecture** - Both models share a similar architecture as both are constructed with layers.
- **Application layer** - Both of models share a common "application layer". However in practice this layer includes different services depending upon each model.
- **Comparable transport and network layers**- Illustrated by fact that whatever functions are performed between presentation and network layer of OSI model similar functions are performed at Transport layer of TCP/IP model.
- **Switched packets** - Both models assume packets are switched meaning individual packets may take differing paths in order to reach same destination.

Differences ----OSI Versus TCP/IP

- TCP/IP Protocols are considered to be standards around which internet has developed while OSI model is a "generic, protocol- independent standard."
- TCP/IP combines session, presentation and application layer into its application layer.
- TCP/IP combines OSI data link and physical layers into network access layer.
- TCP/IP is a simpler model as it has fewer layers.
- TCP/IP is considered to be a more credible model due to fact because TCP/IP protocols are standards around which internet was developed therefore it mainly gains creditability due to this reason. Where as in contrast networks are not usually built around OSI model as it is merely used as a guidance tool.

Syllabus Contents

- **UNIT- I**

- ☐ **Introduction to Layered Network Architecture-** What are computer networks, Layered models for networking, different types of communication models, ISO-OSI Model, TCP/IP.

- **UNIT II**

- ☐ **Data Link Protocols-** Stop and Wait protocols, Noise-free and Noisy Channels, Performance and Efficiency, Sliding Window protocols, MAC Sublayer: The Channel Allocation problem, Carrier Sense Multiple Access Protocols, Collision Free Protocols, FDDI protocol. IEEE Standard 802.3 & 802.11 for LANs and WLANs

Unit 1- Completed

Thanks

Dr. Divya Agarwal