
Introduction
Module 1

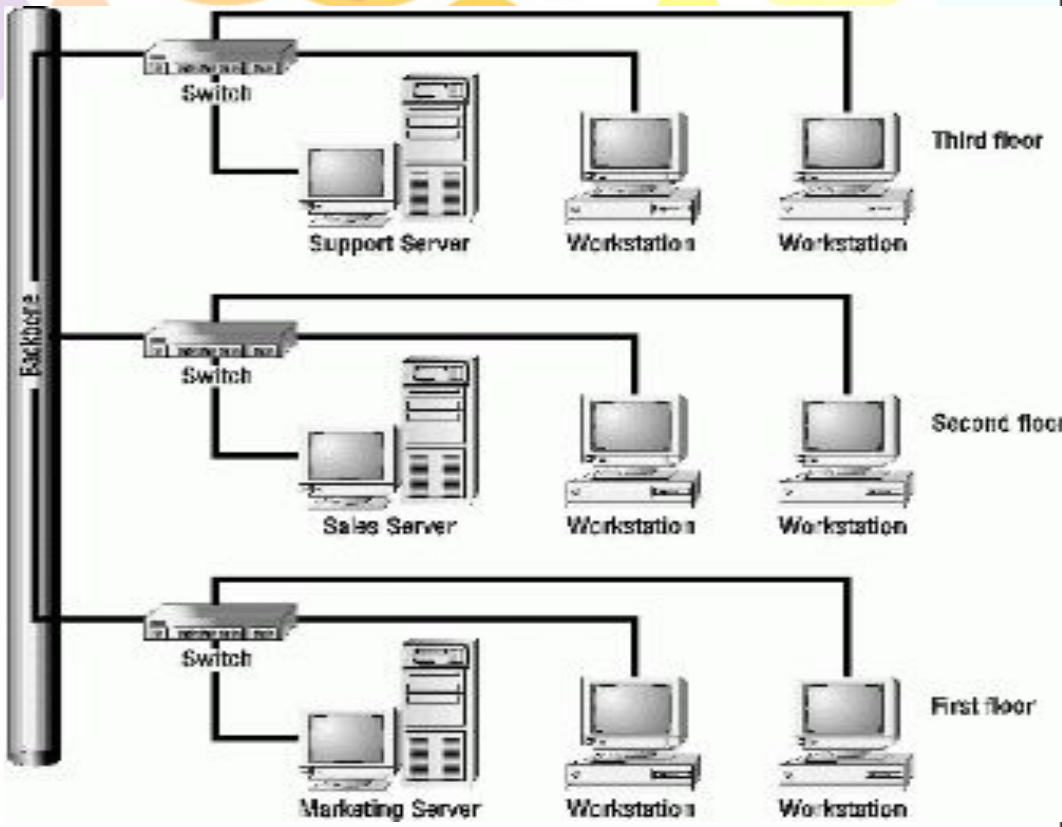
Definition:

Computer Network is a series of **points, or nodes**, **interconnected** by communication paths for the purpose of transmitting, receiving and exchanging data, voice and video traffic.

- Nodes/Endpoints can include servers, personal computers, phones and many types of network devices.

- Network devices including switches and routers use a variety of protocols and algorithms to exchange information and to transport data to its intended endpoint.

- Every endpoint (sometimes called a host) in a network has a unique identifier, often an **IP address** or a **Media Access Control address**
- Networks may also be divided into subnetworks, also called subnets.
- **Types of networks**
  - Networks may also be categorized by the scope of their domains.
  - Storage area networks interconnect storage devices and resources.
  - **Size/ Geographical area**
    - Local area networks interconnect endpoints in a single domain.
    - Wide area networks interconnect multiple LANs, Metropolitan area networks interconnect computer resources in a geographic area.



LAN

- Privately owned
- Connect hosts in single office, building or campus
- Connects host

WAN

- Wider geographical span – town, state country
- Connects switches, routers
- Types: Point to Point WAN and switched WAN

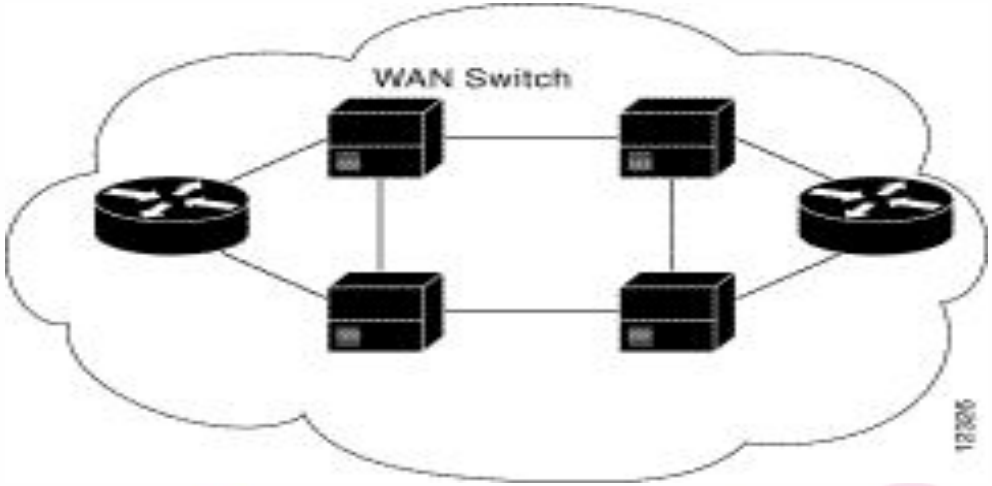
MAN

- long-distance communication systems.
-

How are nodes connected?

- Point to Point WAN

- Switched WAN



- An ***internetwork*** is a collection of individual networks connected by networking devices and that function as a single large network.

- Networks may use a mix of **wired** (optical fiber, coaxial cable or copper wires)and **wireless** technologies (broadcast radio, cellular radio, microwave and satellite).

- Internet is a switched network

Need for Computer Networks

- File Sharing
- Resource Sharing
- Data Protection and Redundancy
- Distributed Computing
- Ease of Administration
- Internal Communications

Switching

Circuit switching

- **Dedicated physical path** established between source and destination in 3 phases
  i) Connection Establishment.
  ii) Data Transfer.
  iii) Connection Released.
- In circuit switching, each data unit know the entire path address which is provided by the source, through the **switch**
- In Circuit switching, data is processed at source system only

Packet switching

- In Packet switching directly data transfer takes place, in available path. **No Dedicated physical path**
- In Packet switching, each data unit just know the final destination address intermediate path is decided by the **routers**
- In Packet switching, data is processed at all intermediate node including source system.

Circuit switching

- Delay between data units in circuit switching is uniform.
- Resource reservation is the feature of circuit switching because path is fixed for data transmission.
- Circuit switching is more reliable.
- Wastage of resources are more in Circuit Switching

Packet switching

- Delay between data units in packet switching is not uniform.
- There is no resource reservation because bandwidth is shared among users.
- Packet switching is less reliable.In Packet switching, data is processed at all intermediate node including source system.
- Less wastage of resources as compared to Circuit Switching.

Network Criteria

- Performance
  - rate of transferring **error free data**.
  - measured by the **Response Time**.
  - Factors that affect Response Time are:
  - **Number of Users**: More users on a network - slower the network will run
  - **Transmission Speed**: speed that data will be transmitted measured in bits per second (bps)
  - **Media Type**: Type of physical connection used to connect nodes together
  - **Hardware Type**: Slow computers such as XT or fast such as Pentiums
  - **Software Program**: How well is the network operating system (NOS) written

Other metric used to measure performance

- **Bandwidth :** number of bits per second that a channel, a link, or even a network can transmit.
- **Throughput :** throughput is a measure of how fast we can actually send data through a network
- **Latency:** how long it takes for an entire message to completely arrive at the destination from the time the first bit is sent out from the source.

Latency =propagation time +transmission time +queuing time + processing delay

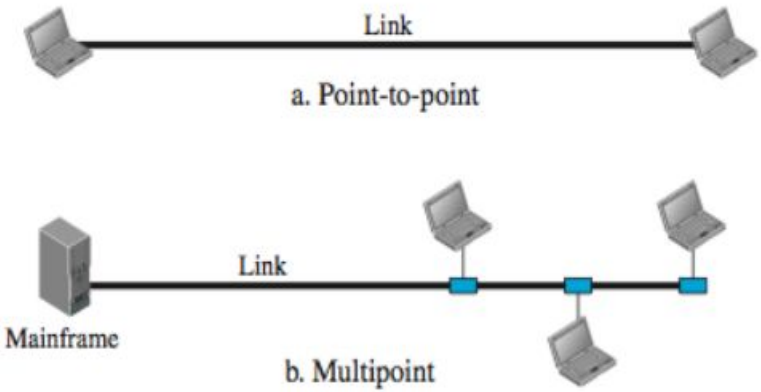
- **Jitter:** problem if different packets of data encounter different delays and the application using the data at the receiver site is time

- Consistency
  - predictability of **response time** and a**ccuracy** of data
- Reliability
  - measure of how often a **network is useable**.
  - MTBF (**Mean Time Between Failures**) is a measure of the average time a component is expected to operate between failures.
  - A network failure can be: hardware, data carrying medium and Network Operating System.
- Recovery
  - Network's ability to return to a prescribed level of operation after a network failure.
  - is based on having Back-up Files.

- Security
  - protection of Hardware, Software and Data from unauthorized access.
  - Restricted physical access to computers, password protection, limiting user privileges and data encryption are common security methods.
  - Anti-Virus monitoring programs to defend against computer viruses are a security measure

Physical Structures

- Here we'll discuss the physical connections for Networks.
- Two possible connection types :
- Point-to-point or Multipoint



Point-to-point connections

- provides a dedicated link or between two devices.
- The entire capacity of the link is reserved for transmission between those two devices. (actual length of wire or cable to connect)

Multipoint connections

- more than two devices are sharing a link
- The entire capacity of the link is either shared spatially or temporally.

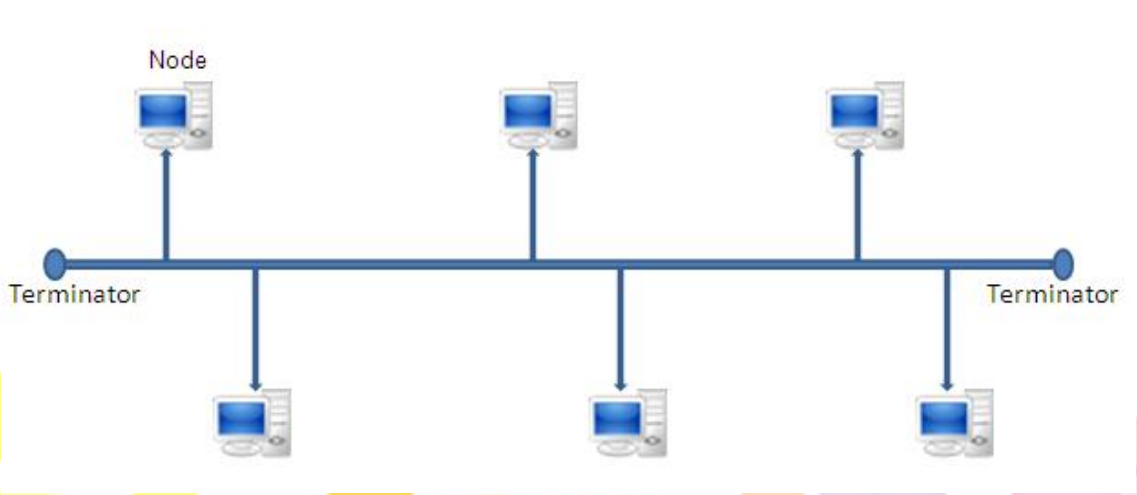
Network Topology

Network Topology – the way a network is laid out physically

- **Types**

BUS Topology

- only one computer can send data on the bus at any one time.
- Every device is connected to a single cable



Advantages of Bus Topology

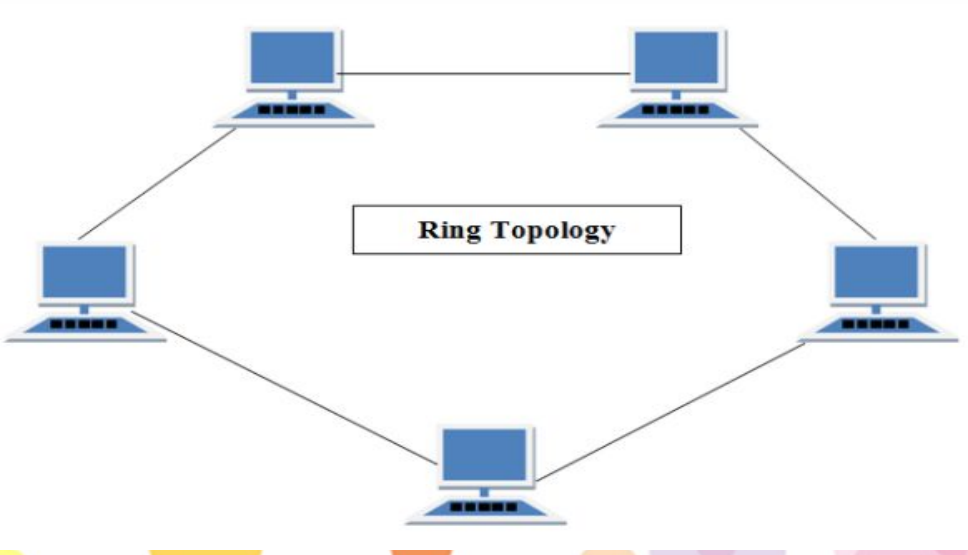
- It is **cost effective**.
- **Cable required is least** compared to other network topology.
- Used in small networks.
- It is **easy** to understand.
- Easy to expand joining two cables together.

Disadvantages of Bus Topology

- Cables fails then whole network fails.
- If network traffic is heavy or nodes are more the performance of the network decreases.
- Cable has a limited length.
- It is slower than the ring topology.

RING Topology

- It is called ring topology because it forms a ring as each computer is connected to another computer, with the last one connected to the first.
- A number of repeaters are used
- The transmission is unidirectional /bidirectional (Dual Ring)



Advantages of Ring Topology

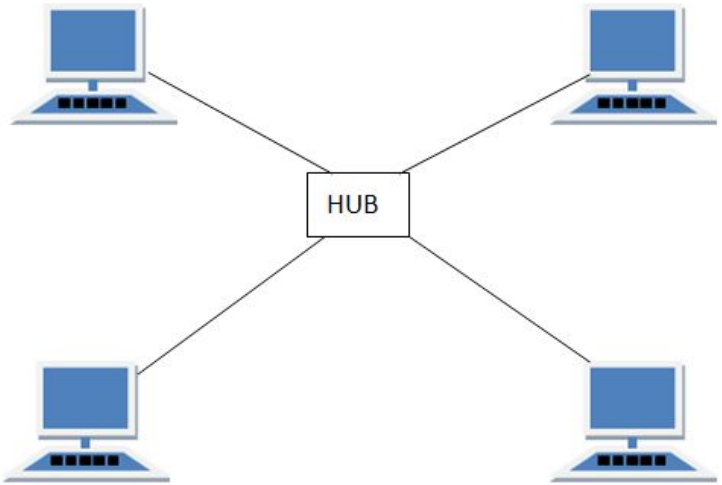
- Transmitting network is **not affected by high traffic** or by adding more nodes, as only the nodes having tokens can transmit data.
- **Cost effective** to install and expand

Disadvantages of Ring Topology

- **Troubleshooting is difficult** in ring topology.
- Adding or deleting the computers disturbs the network activity.
- **Failure of one** computer disturbs the whole network.

STAR Topology

- In this type of topology **all the computers are connected to a single hub** through a cable. This hub is the central node and all others nodes are connected to the central node.
- Every node has its **own dedicated connection to the hub**.
- Hub acts as a **repeater** for data flow.
- Can be used with twisted pair, Optical Fibre or coaxial cable.



Advantages of Star Topology

- Fast performance with few nodes and low network traffic.
- Hub can be **upgraded easily**.
- Easy to **troubleshoot.**
- Easy to **setup and modify**.
- Only that node is affected which has **failed**, rest of the nodes can work smoothly.

Disadvantages of Star Topology

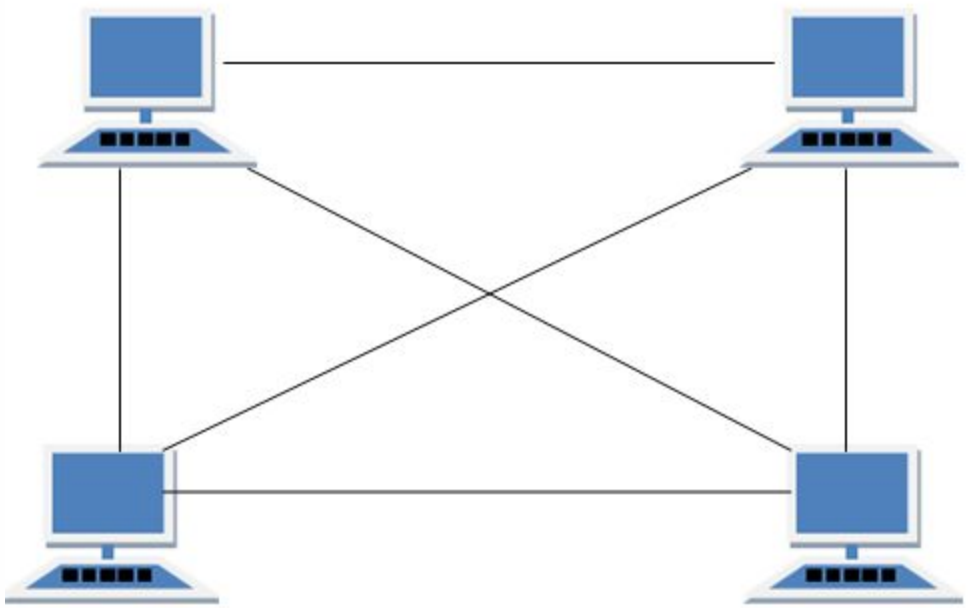
- Cost of installation is **high**. (cable and extra device)
- If the **hub fails** then the whole network is stopped because all the nodes depend on the hub.
- **Performance** is based on the hub that is it depends on its capacity

MESH Topology

•It is **a point-to-point** connection to other nodes or devices.

•All the network nodes are connected to each other.

•Mesh has **n(n-1)/2** physical channels to link **n** devices.



There **are two techniques** to transmit data over the Mesh topology, they are :

1.Routing

2.Flooding

Routing

•In routing, the nodes have a routing logic as per the network requirements - shortest distance, information about the broken links

Flooding

•In flooding, the same data is transmitted to all the network nodes,

•The network is robust, and the its very unlikely to lose the data. But it leads to unwanted load over the network.

Types of Mesh Topology

•**Partial Mesh Topology :** In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two or three devices.

•**Full Mesh Topology :** Each and every nodes or devices are connected to each other.

Advantages of Mesh Topology

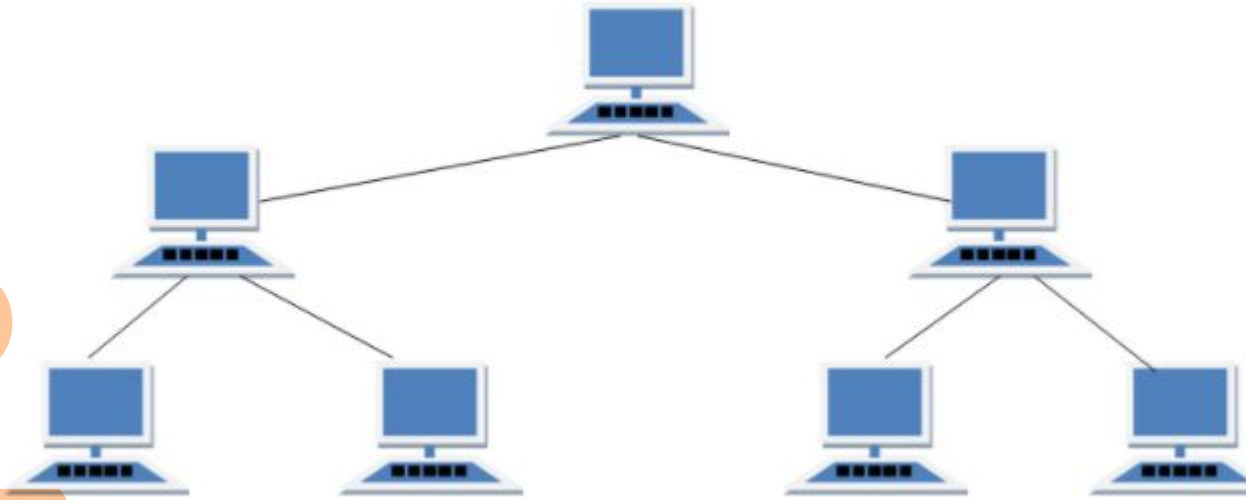
- Each connection can carry its own data load.
- It is robust.
- Fault is diagnosed easily.
- Provides security and privacy.

Disadvantages of Mesh Topology

- Installation and configuration is difficult.
- Cabling cost is more.
- Bulk wiring is required.

TREE Topology

- It has a root node and all other nodes are connected to it forming **hierarchy**.
- It is also called **hierarchical topology**
- It should at least have three levels to the hierarchy
- Ideal if **workstations** are located in groups.
- Used in **Wide Area Network**.



Advantages of Tree Topology

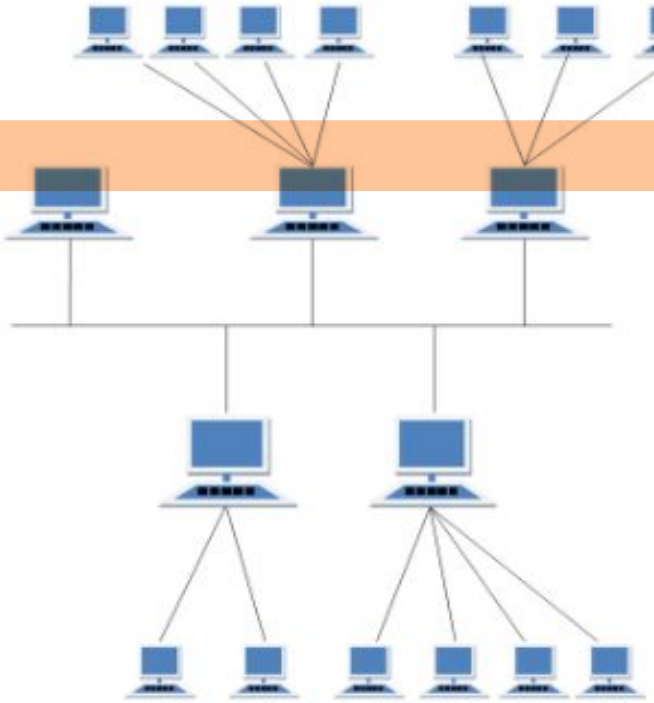
- **Extension** of bus and star topologies.
- **Expansion** of nodes is possible and easy.
- Easily **managed and maintained**.
- Error detection is easily done.

Disadvantages of Tree Topology

- Heavily cabled.
- Costly.
- If more nodes are added maintenance is difficult.
- Central hub fails, network fails.

HYBRID Topology

- It is two different types of topologies which is a mixture of two or more topologies.
- It is a combination of two or tc
- Inherits the advantages and d included



Advantages of Hybrid Topology

- Reliable as Error detecting and troubleshooting is easy.
- Effective.
- Scalable as size can be increased easily.
- Flexible.

Disadvantages of Hybrid Topology

- Complex in design.
- Costly.

OSI Reference Model

- **OSI stands for Open Systems Interconnection** model (**OSI** model)
- developed by ISO – '**International Organization of Standardization**', in 1974
- It is a 7 layer architecture with each layer having specific functionality to perform
- conceptual framework that describes functions of the networking or telecommunication system independently from the underlying technology infrastructure.
-

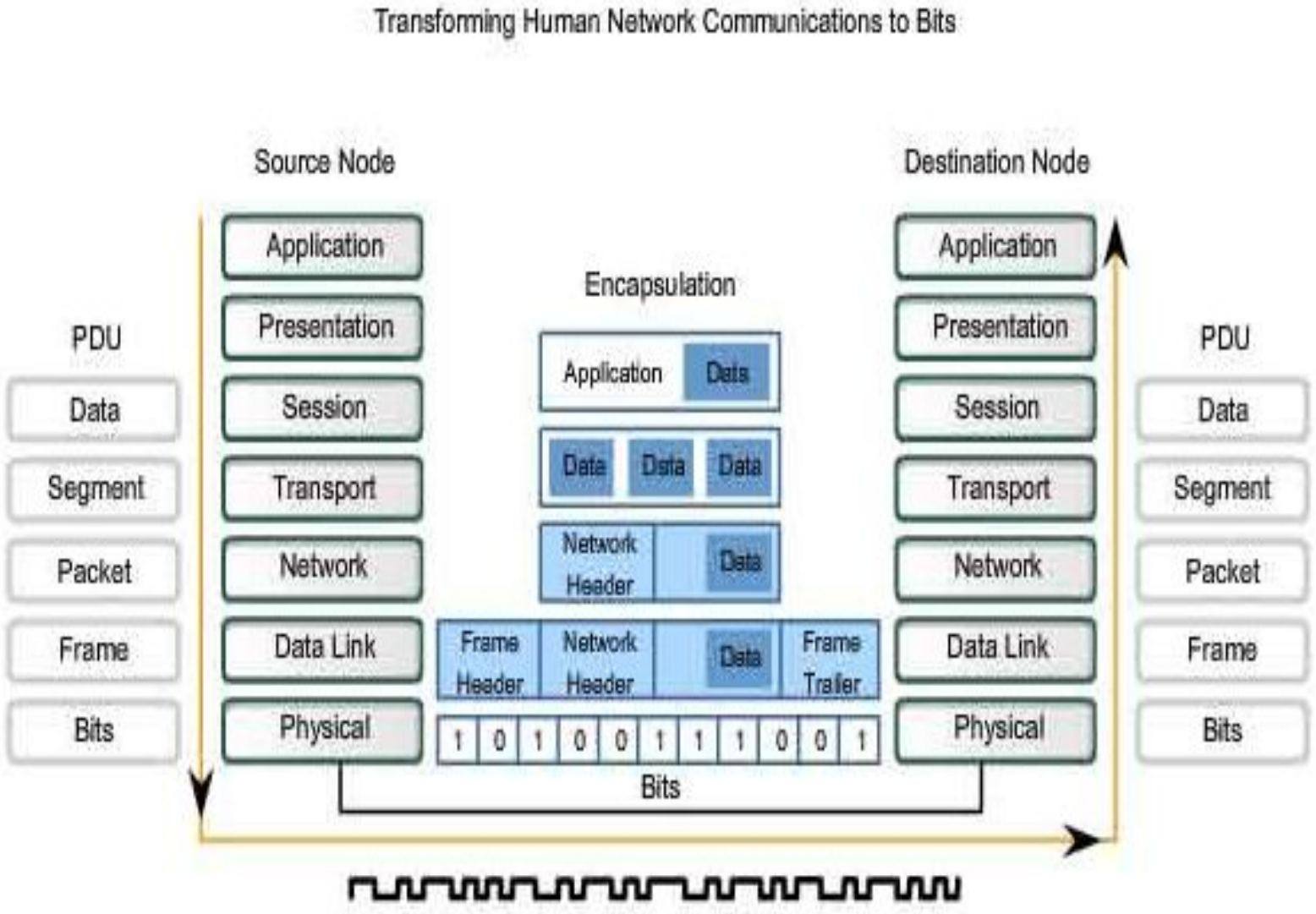
Why layering?

Dealing with complex systems:

- explicit structure allows identification, relationship of **complex system's p**ieces
- modularization e**ases maintenance, updating of system**
  - change of implementation of layer's service transparent to rest of system
    - e.g. change in gate procedure doesn't affect rest of system
- was originally developed to facilitate **interoperability between vendors** and to define clear standards for network communication.

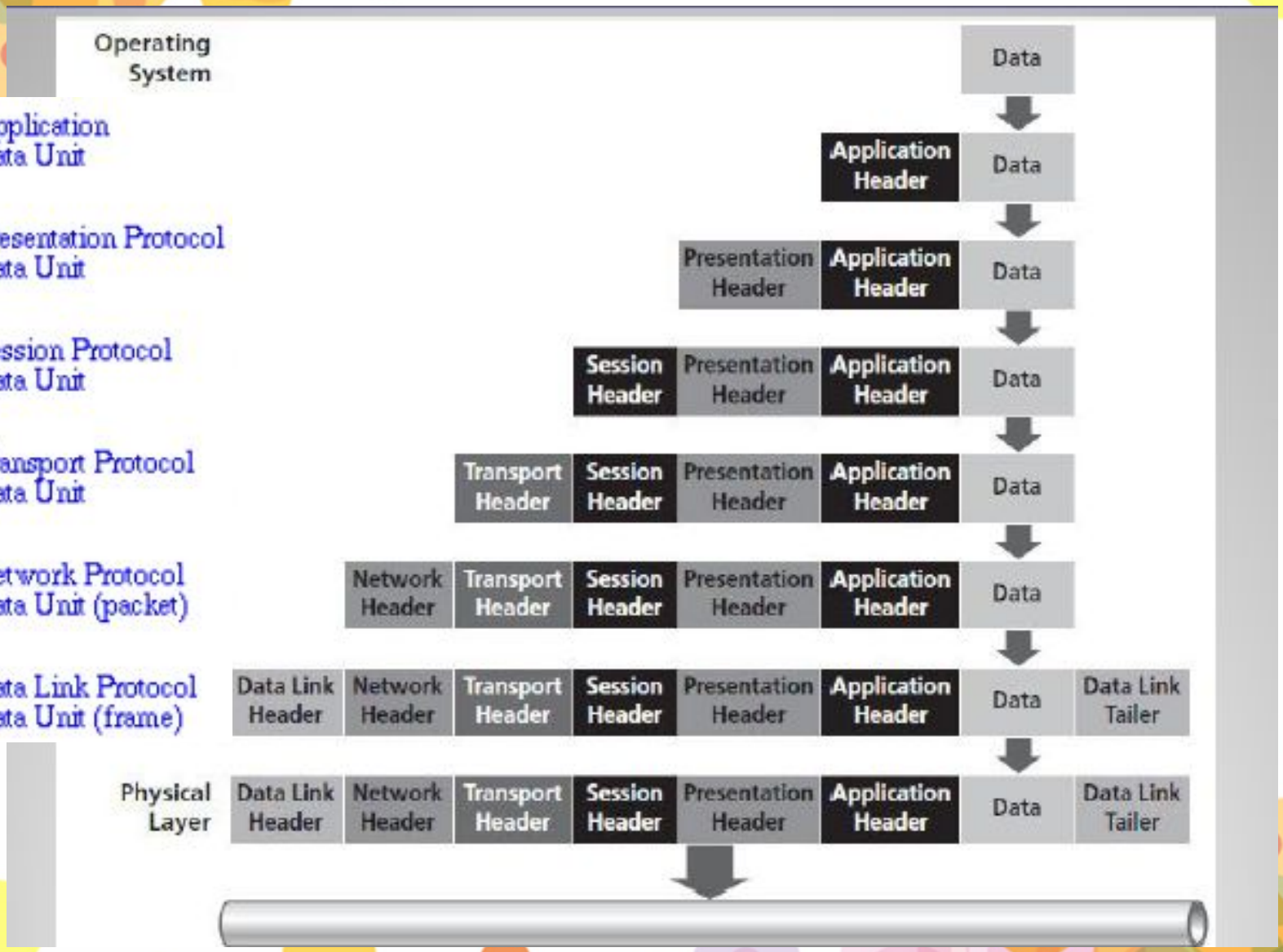
- OSI is not a physical model; rather it is a set of guidelines that application developer can use to create application that run on network.
- It provides framework for creating and implementing networking standards, devices, internetworking scheme.
- O.S.I Has 7 Layer, divided into 2 groups.
  - The Layer 4-3-2-1 layer defines how data is transmitted end-to-end.
  - The Layer 7-6-5 defines how the application within one station will communicate with each other. Responsible for application communication between hosts.

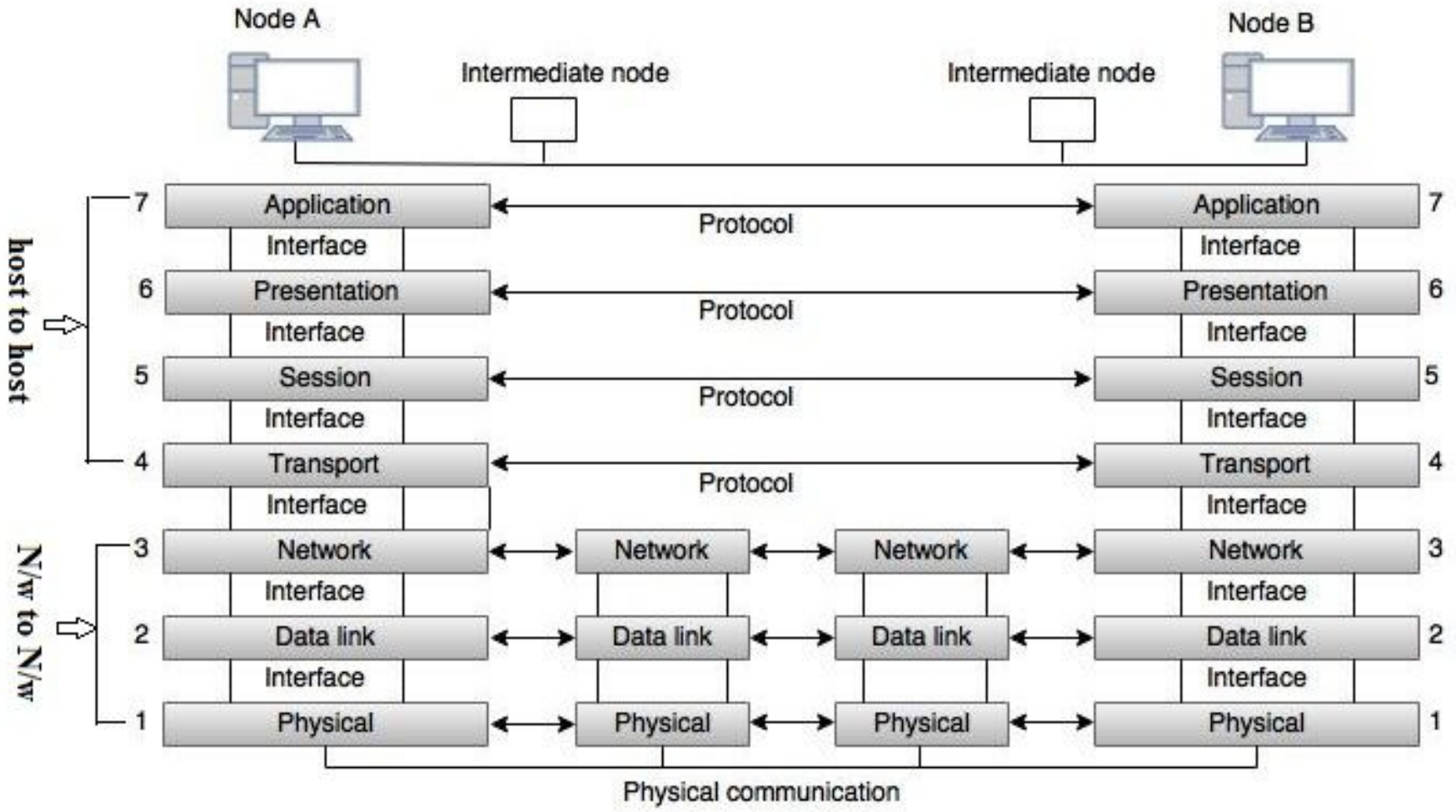
- Layers are as under:
  - A layer should be created where a different level of abstraction is needed.
  - Each layer should perform a well defined function.
  - The function of each layer should be chosen with an eye towards defining internationally standardized protocols.
  - The layer boundaries should be chosen to minimize the information flow across the interfaces.
  - The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity.



- protocol data unit (**PDU**) is a single unit of information transmitted among peer entities of a computer network.

Packet Data Unit (PDU)




Node A
Intermediate node
Intermediate node
Node B
7
Application
Interface
6
Presentation
Interface
5
Session
Interface
4
Transport
Interface
3
Network
Interface
2
Data link
Interface
1
Physical
Protocol
Protocol
Protocol
Protocol
Application
Interface
Presentation
Interface
Session
Interface
Transport
Interface
Network
Interface
Data link
Interface
Physical
7
6
5
4
3
2
1
Network
Data link
Physical
Network
Data link
Physical
host to host
N/w to N/w
Physical communication

7. Application

Network process to application

DNS, WWW/HTTP, P2P, EMAIL/POP, SMTP, Telnet, FTP

6. Presentation

Data representation and encryption

Recognizing data: HTML, DOC, JPEG, MP3, AVI, Sockets

5. Session

Interhost communication

Session establishment in TCP, SIP, RTP, RPC-Named pipes

4. Transport

End-to-end connections and reliability

TCP, UDP, SCTP, SSL, TLS

3. Network

Path determination and logical addressing

IP, ARP, IPsec, ICMP, IGMP, OSPF

2. Data Link

Physical addressing

Ethernet, 802.11, MAC/LLC, VLAN , ATM, HDP, Fibre Channel,
Frame Relay, HDLC, PPP, Q.921, Token Ring

1. Physical

Media, signal, and binary transmission

RS-232, RJ45, V.34, 100BASE-TX, SDH, DSL, 802.11

Application Layer:

- This layer provides the operational system with direct **access to the network services** and is responsible to **generate Data** (user info/ system commands)
- It also provides an **interface** so that Application (Web Browser) that are running on the local machine can access the network services. So It **enables user or software to access the network**.
- It provides user interfaces and support for services such as **electronic mail, remote file access** and **transfer,** shared database management, and other types of distributed information services.

Presentation Layer:

- This layer is concern with the **syntax and semantics** of the information exchanged between 2 systems.
- The presentation layer is concerned with translating, interpreting, and converting the data from various formats.
- Data is compressed for transmission and uncompressed on receipt in this layer.
- Encryption techniques are also implemented at the presentation layer.
- Function: Present Data, Handles Processing Such as Encryption, Compression and Translation Services

- Translation: Information should be changed to bit streams before being transmitted. Because different computers us e different encoding system, the presentation layer is responsible for interoperability between these different encoding methods.
- Encryption: To carry sensitive information, a system must be able to assure privacy. Transformation is carried out at this layer.
- Compression: Data compression reduces the number of bits to be transmitted. It is highly required when transmitting data of text, audio and video.

Session Layer:

- The session layer is responsible for **establishing**, **managing**, and **terminating** a connection called session.
- A session is an exchange of messages between computers.
- Logon, name recognition and security functions occur while establishing a session.
  - Managing the session involves **synchronization of user tasks and messages.**
  - Synchronization involves the use of **checkpoints in the data stream.** In the event of a failure, only the data from the last checkpoint has to be resent.

- Function: **Keeps different application data separate, Dialog control**, **Synchronization**
  - Dialog control: The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place either in half-duplex or full duplex.
  - Synchronization: This layer allows a process to add checkpoints into a stream of data.

Transport Layer:

- The transport layer is responsible for the **control of flow** and **ensuring that messages are delivered error free** source -to-destination (end-to-end).
- On the originating side, messages are packaged for efficient transmission and assigned a tracking number.
- On the receiving side, the p**ackets are reassembled, checked for errors, and acknowledged**.
- The transport layer performs error handling by ensuring that all data is received in the **proper sequence** without errors. If there are errors the data is retransmitted.

- This layer ensures that the **whole message arrives intact and in order,** overseeing both **error control** and **flow control** at the source-to-destination level.
- For security purpose, this layer may create a connection between the two end ports, a **logical path** between source and destination.
- **Function: End-to-End Connection, Perform error correction before retransmit**
  - **Service -point addressing:** Computer runs several programs at the same time. So this layer is responsible for delivering data to specific process (port) of computer.

- **It** contains service-point address (**port address**) and therefore, network layer gets each packet to the correct computer on correct network.
- **Segmentation and Reassembly:** A message is divided into **transmittable segments**, each segment containing sequence number, which enables layer to reassembling the message correctly upon arriving at the destination and can identify those packets which are lost during the transmission.

- **Connection control:** The transport layer can be either connection or connection oriented.
  - A connection-less transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine.
  - Whereas connection oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packet.

- **Error control:** This layer is more concern with end -to-end control rather than single link control of data link layer. The receiving transport layer makes sure that the **entire message arrives without error**. Error correction is usually achieved through retransmission.

Network Layer:

- The network layer is primarily concerned with addressing and routing.
- **Logical addresses** or IP addresses are translated into physical addresses or machine addresses for transmission at the network layer.
  - On the receiving side, the translation process is reversed.
  - The network layer also determines the route from the source to the destination computer to deliver packets.

- **Routes are determined based on packet addresses and network conditions**. Traffic control measures are also implemented at the network layer.
  - If 2 systems are connected in the same network, there is no need for the network layer.
- **Function: Routing, Provides Logical addressing which router used for path determination**
  - Logical Addressing: The physical addressing implemented by the data link layer handles the

- addressing problem locally. If packet passes the network boundary, it needs another addressing system to help distinguish the source and destination system.
- Routing: When independent networks or links are connected together to create internetwork, the connecting device (router or gateway) route the packets to their final destination. This is one more mechanism provided by this layer.

Data Link Layer:

- The data link layer defines how the signal will be placed.
- In this layer, the **data frames are broken down into individual bits** that can be translated into electronic signals and sent over network. On the receiving end the bits are reassembled into frames for processing by upper levels.
- If an acknowledgement is expected and not received, the frame will be resent.
- Error and corrupt data detection and correction is also performed at the data link layer

- The data link layer transforms the physical layer, a raw transmission facility, to a reliable link and is responsible for **node-to-node** delivery.
- **Function: Framing, Combine Packets into Bytes And bytes into Frame**
  - **Framing:** the data link layer divides the stream of bits received from the network layer into manageable data units called frames.
  - **Physical Addressing:** If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the physical address of the sender and receiver of the frame.

- **Flow control:** If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender, the data link layer imposes the flow control mechanism to prevent overwhelming the receiver.
- **Error control:** The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It uses the mechanism to prevent duplication of frames. Error control is normally achieved through a trailer added to the end of the frame.

- **Access control:** When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.

Physical Layer:

- The physical layer of the OSI model establishes the **physical characteristics** of the network such as the **type of cable, connectors, and the length of the cable**.
- This layer also defines the electrical characteristics of the signals used to transmit the data.
- The physical layer transmits the binary data (bits) as electrical or optical signals depending on medium.

- This layer is concern with the following:
  - **Physical characteristics of interface and medium:** This layer defines the characteristics of the interface between the devices and the transmission medium.
  - **Representation of bits:** Data of this layer consists of a stream of bits without any interpretation. They must be encoded into signals (electronics or optical), which is defined by the physical medium.
  - **Data rates:** The number of bits sent each second, is also defined b the physical layer.

- **Line configuration:** They physical layer is concerned with the connection of device to the medium. It can be Point-to-Point or Multipoint Configuration.
- **Transmission Mode:** The physical layer also defined the direction of transmission between two devices (Simplex, Half-Duplex or Full-Duplex).

Summary of OSI

Physical Layer: To transmit bits over a medium.

Data Link Layer: To organize bits into frames; to provide node-to-node delivery.

Network Layer: To move packets from source to destination.

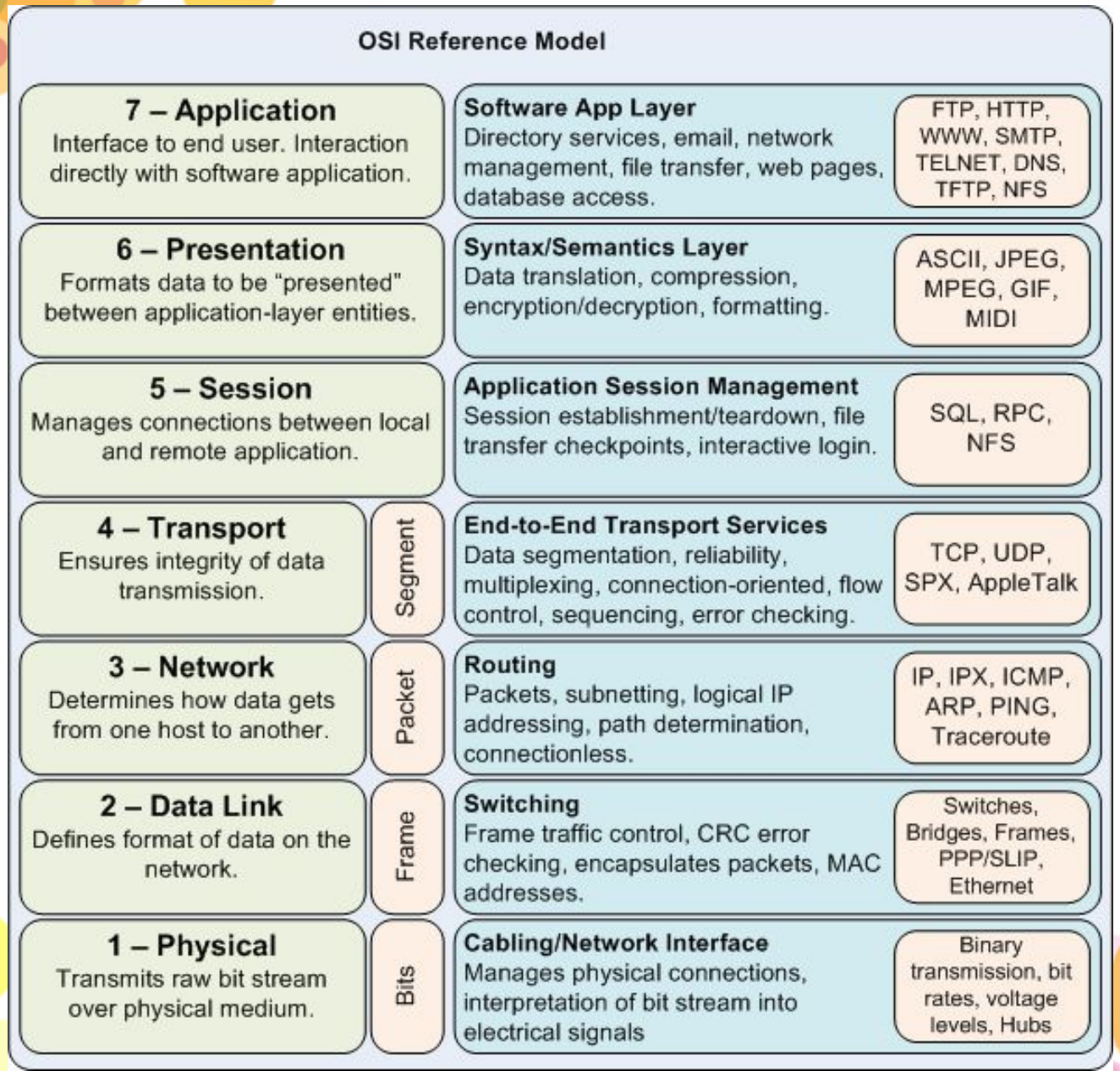
Transport Layer: To provide reliable end-to-end message delivery and error recovery.

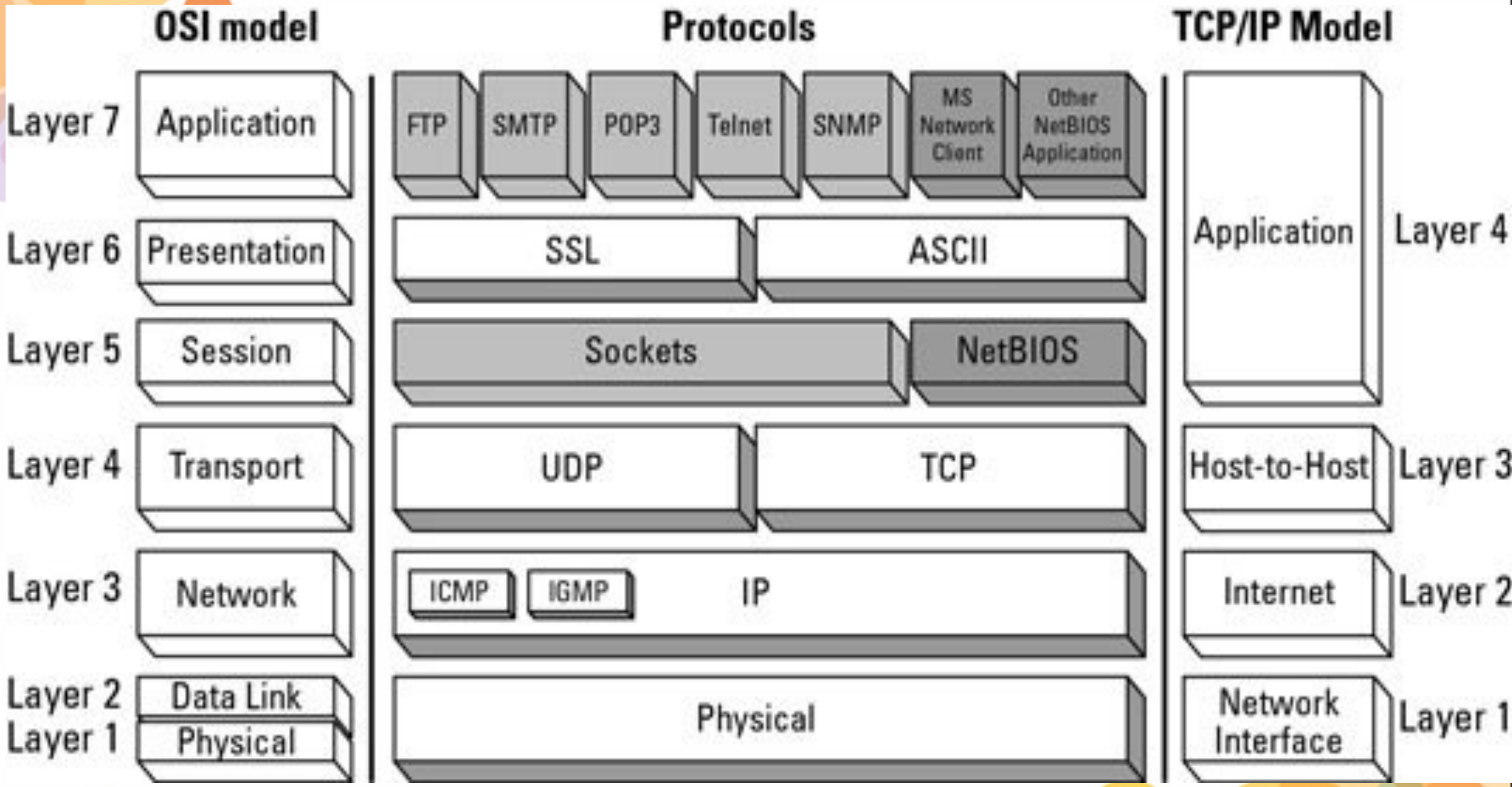
Session Layer: To establish, manage and terminate sessions.

Presentation Layer: To translate, encrypt, and compress data.

Application Layer: To generate data and allow access to network resources.

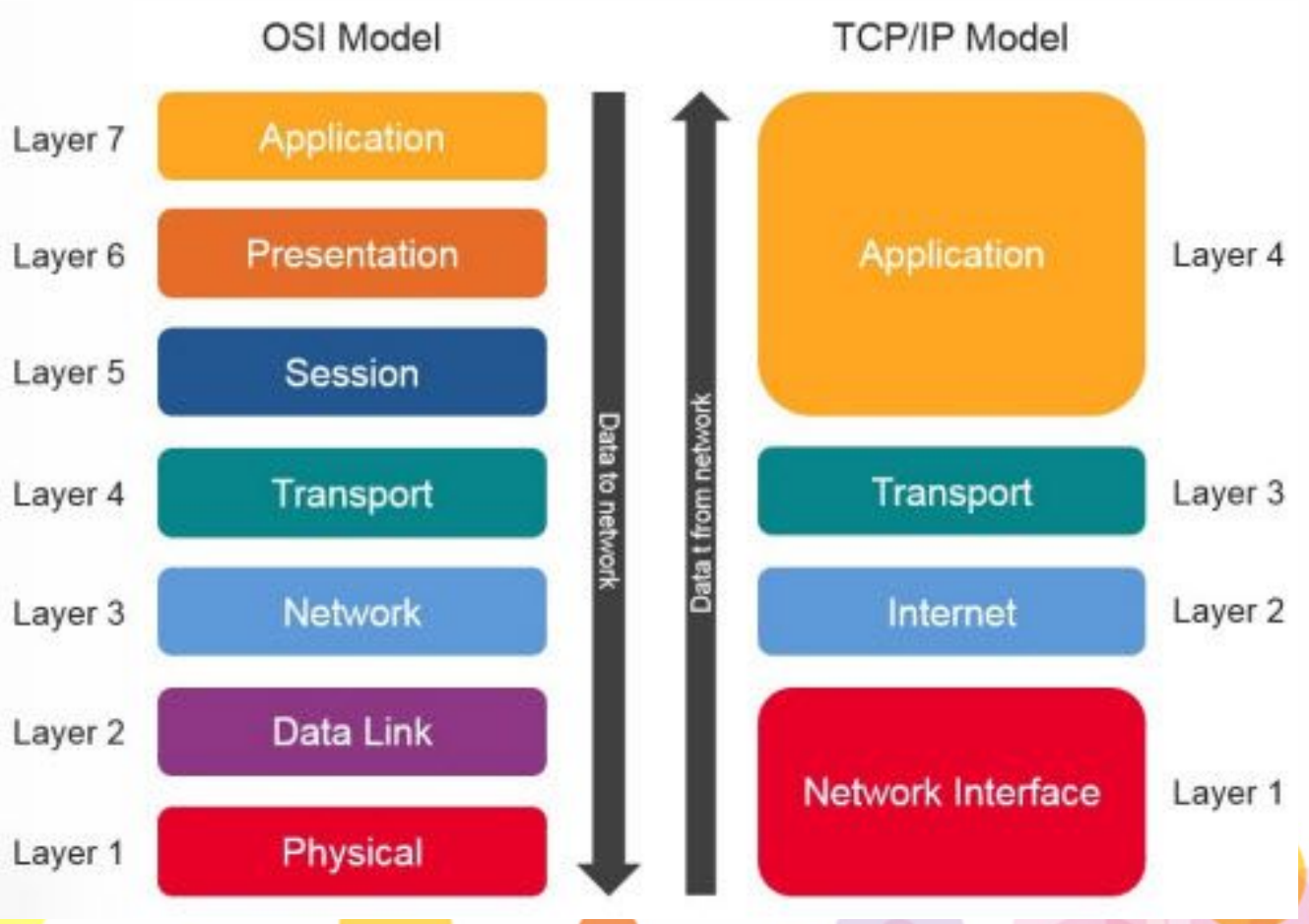
Protocols, Functions of OSI Model



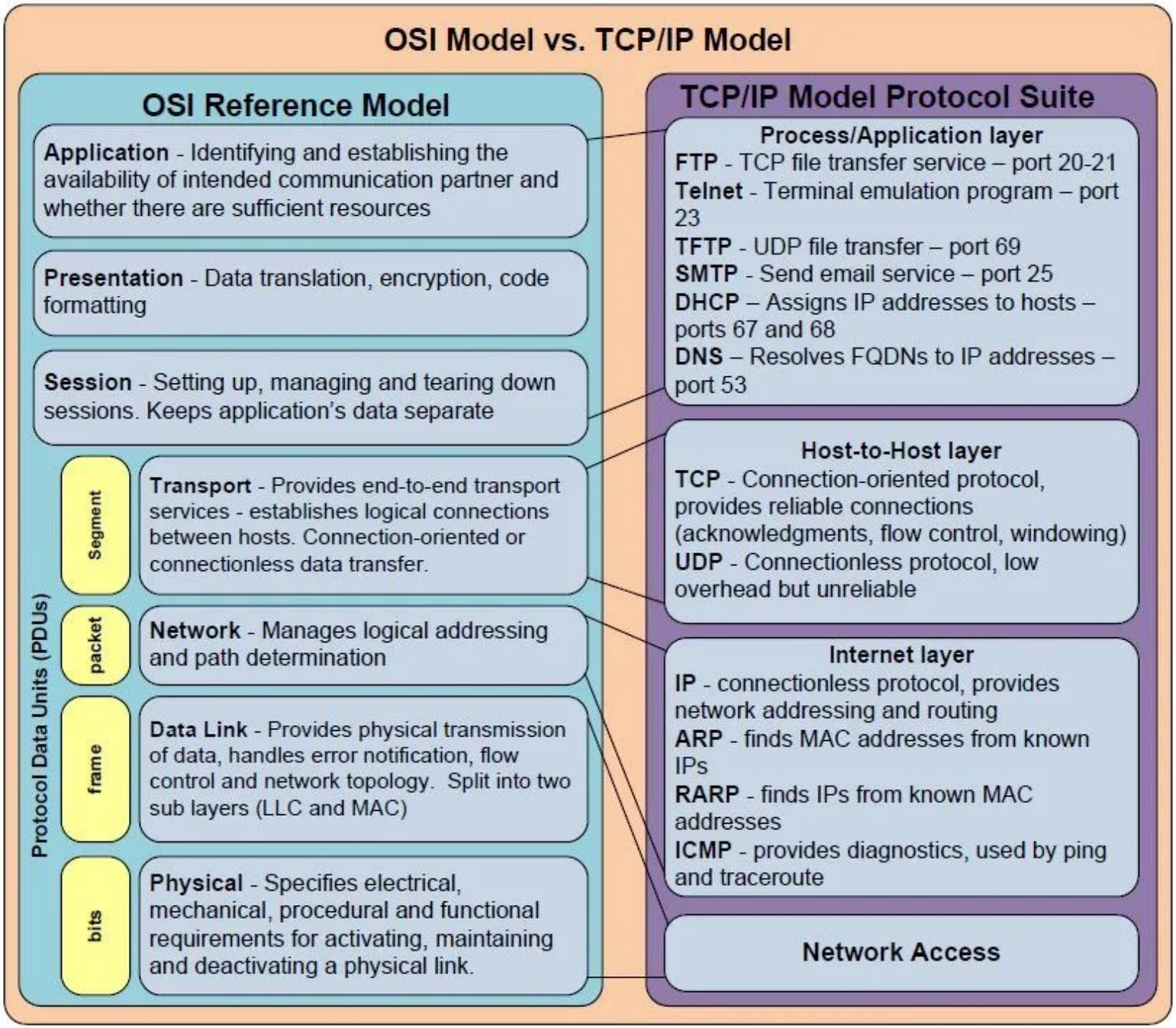

OSI model
Protocols
TCP/IP Model
Layer 7
Application
FTP
SMTP
POP3
Telnet
SNMP
MS Network Client
Other NetBIOS Application
Application
Layer 4
Layer 6
Presentation
SSL
ASCII
Layer 5
Session
Sockets
NetBIOS
Layer 4
Transport
UDP
TCP
Host-to-Host
Layer 3
Layer 3
Network
ICMP
IGMP
IP
Internet
Layer 2
Layer 2
Data Link
Layer 1
Physical
Physical
Network Interface
Layer 1

Comparison between OSI Reference Model and TCP/IP Reference Model

- TCP refers to Transmission Control Protocol.
  OSI refers to Open Systems Interconnection.



OSI Model vs. TCP/IP Model



Similarities between OSI Reference and TCP/IP Reference Model

- Both are layered architecture.
- Layers provide similar functionalities.
- Both are protocol stack.
- Both are reference models

Comparison of OSI Reference Model and TCP/IP Reference Model

- OSI has **seven** layers
- OSI emphasis on providing a **reliable data transfer service, Each layer** of the OSI model detects and handles errors, all data transmitted includes checksums.
- Is a general model. The OSI model was devised before the protocols were invented. It can be made to work in diverse he. terogeneous networks.

- TCP/IP has **four** layers
- TCP/IP treats reliability as an end to end Problem. The **transport layer handles all error detection and recovery**, it was checksums, acknowledgments, and timeouts to control transmissions and provides end-to-end verification.
- Cannot be used in other applications

Comparison of OSI Reference Model and TCP/IP Reference Model (contd)

- OSI model supports both connectionless and connection oriented communication in the network layer, but only connection oriented communication in the transport layer, where it counts.
- OSI makes the distinction between services, interfaces, and protocol.
- The OSI model supports both connectionless and connection-oriented communication in the network layer, but only connection-oriented communication in the transport layer.
- The TCP/IP model has only one mode in the network layer (connectionless) but supports both modes in the transport layer, giving the user choice.
- TCP/IP does not originally clearly distinguish between services, interface, and protocol.
- TCP/IP model was just a description of the existing protocols. The model and the protocol fit perfectly.

Network devices

Repeater

- A repeater operates at the **physical** layer.
- 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.
- It regenerate it to the original strength.
- It is a **2 port** device.

Hub

- **multiport repeater**.
- A hub connects multiple wires like in star topology which connects different stations.
- Does not find out best path for data packets which leads to inefficiencies and wastage.

Bridge

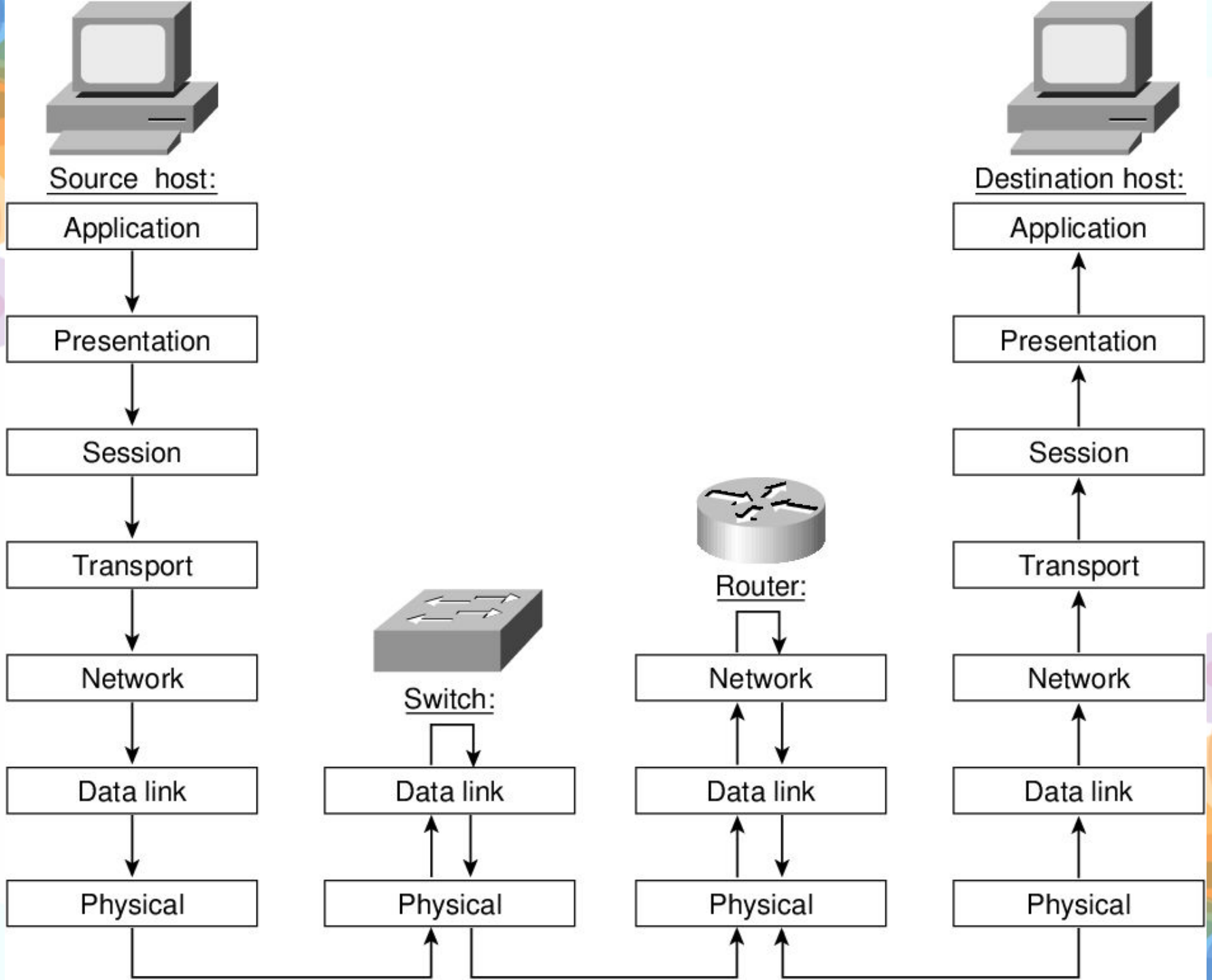
- A bridge operates at data link layer.
- A bridge is a repeater, with add on functionality of filtering content by reading the MAC addresses of source and destination.
- used for interconnecting two LANs working on the same protocol.
- It has a single input and single output port, it is a 2 port device.

Switch

- A switch is a multi port bridge with a buffer and a design that can boost its efficiency(large number of ports imply less traffic) and performance.
- Switch is data link layer device.
- Switch can perform error checking before forwarding data, that makes it very efficient as it does not forward packets that have errors and forward good packets selectively to correct port only.

Routers

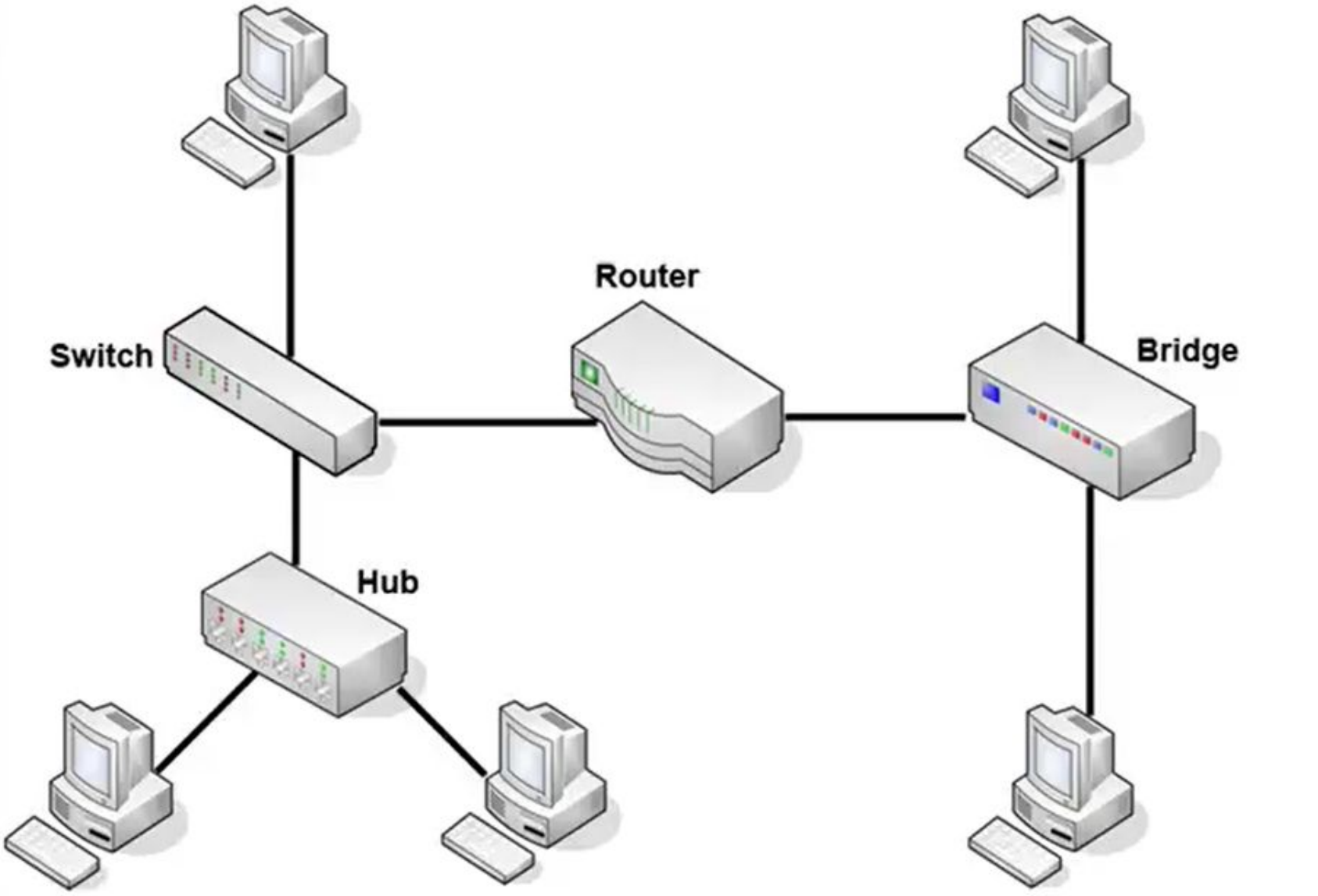
- Switchs the routes data packets based on their IP addresses.
- Is a Network Layer device.
- connect LANs and WANs together
- dynamically updating routing table based on which they make decisions on routing the data packets.
- Router divide broadcast domains of hosts connected through it

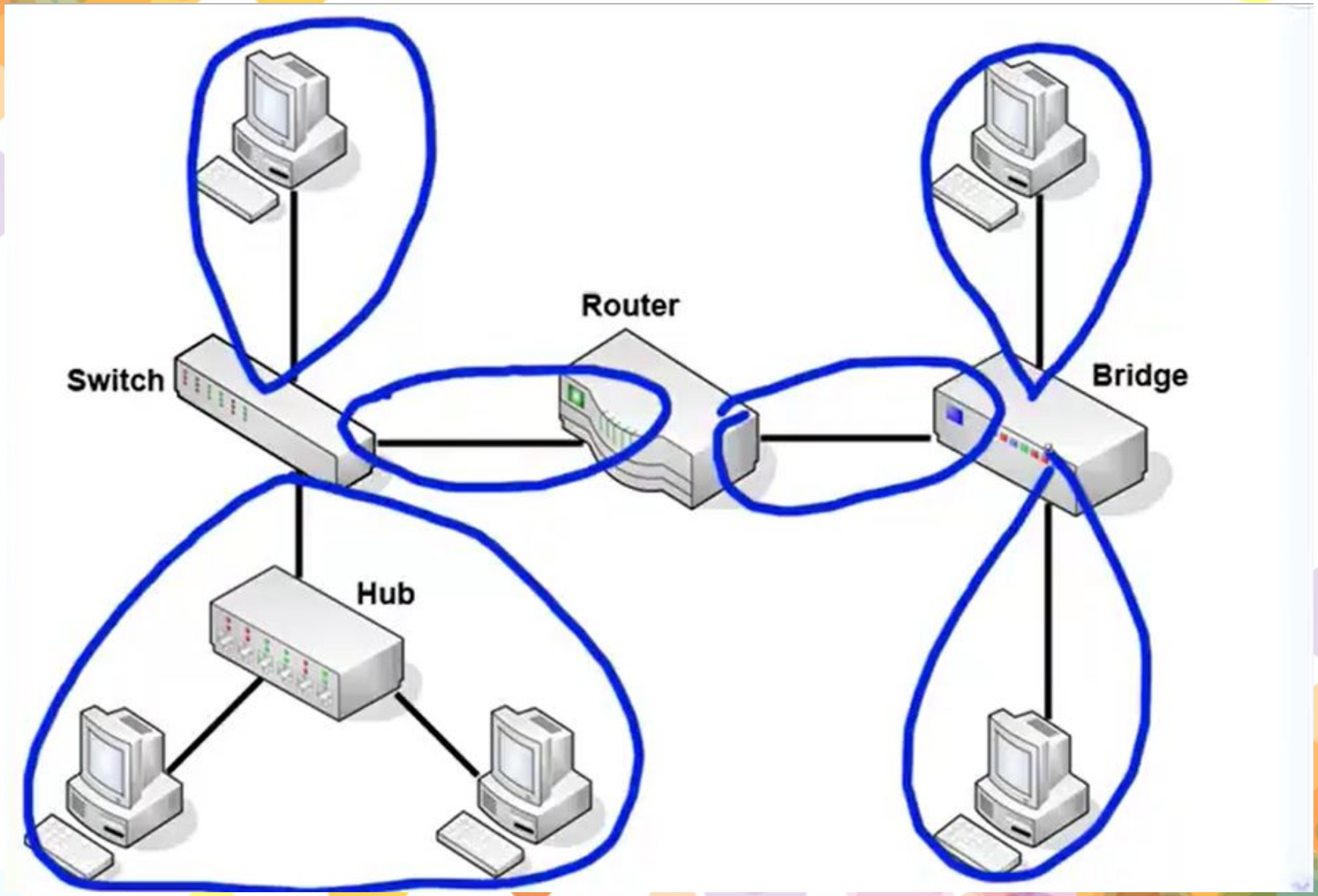

Source host:
Application
Presentation
Session
Transport
Network
Data link
Physical
Switch:
Data link
Physical
Router:
Network
Data link
Physical
Destination host:
Application
Presentation
Session
Transport
Network
Data link
Physical

Gateway

- connects two networks together that may work upon different networking models.
- They basically works as the messenger agents that take data from one system, interpret it, and transfer it to another system.
- Operates at network layer.
- are generally more complex than switch or router.

Collision domain




Router
Switch
Bridge
Hub