MIT Art Design and Technology University

MIT School of Computing, Pune

23BTCS2011 -Computer Network

Class - S.Y. (SEM-II), Div -14

Prof. Suruchi Deshmukh

AY 2024-2025 SEM-II

Course Outcomes

- **After completion of the course students are able to:**
- Apply the fundamentals of data communication & networking in real life applications
- Demonstrate various design issues of data link layer.
- Analyze different routing protocols in network layer and transport layer
- Explore various Application Layer protocols

Unit I - Syllabus

- **Unit I – Introduction to Data Communication 09 hours**

- **Main Topic 1 :** Introduction to data communication, Networks: Network Hardware, Network Software
- **Main Topic 2 :** Internet: Internet history standards and administration,
- Protocols & Standards, RFCs,
- **Main Topic 3 :** OSI Model, TCP/IP Protocol Suite, Comparison of the OSI and TCP/IP reference model, Analog & Digital Signals, Transmission Impairments.

Course Outcome

- After completion of the course students are able to:

CO1: Apply the fundamentals of data communication & networking in real life applications

Computer Network

- Computer network refers to collection of autonomous **interconnected computing devices that can exchange data and share resources with each other**.
- These networked devices use a system of rules, called communications protocols, to transmit information over physical or wireless technologies

Uses of Computer Network

- Business Application
- Home Application
- Mobile Users
- Social issues

Business Application

- Resource Sharing : VPN
- client server model : web application
- communication medium : email , IP telephony or VoIP
- Desktop Sharing
- E-Commerce

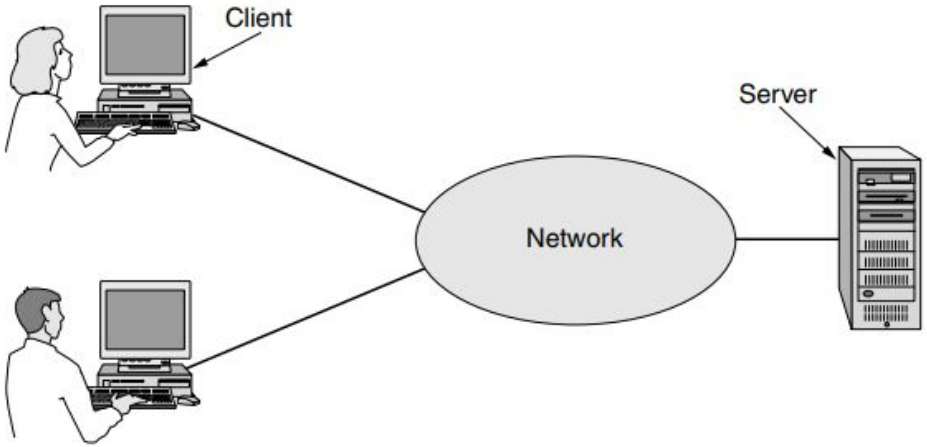


Figure 1-1. A network with two clients and one server.

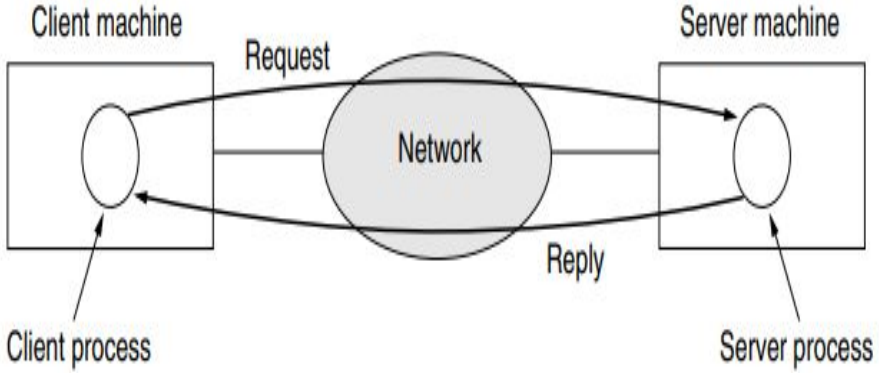


Figure 1-2. The client-server model involves requests and replies.

Home Applications

- In 1977, Ken Olsen ,the Digital Equipment Corporation company
- Initially for Word processing and games.
- Internet : connectivity to remote computers. eg :E –commerce
- Surfing WWW
- Peer-to peer system: no central database , access information from social network applications ,
- IP TV , Ubiquitous Computing

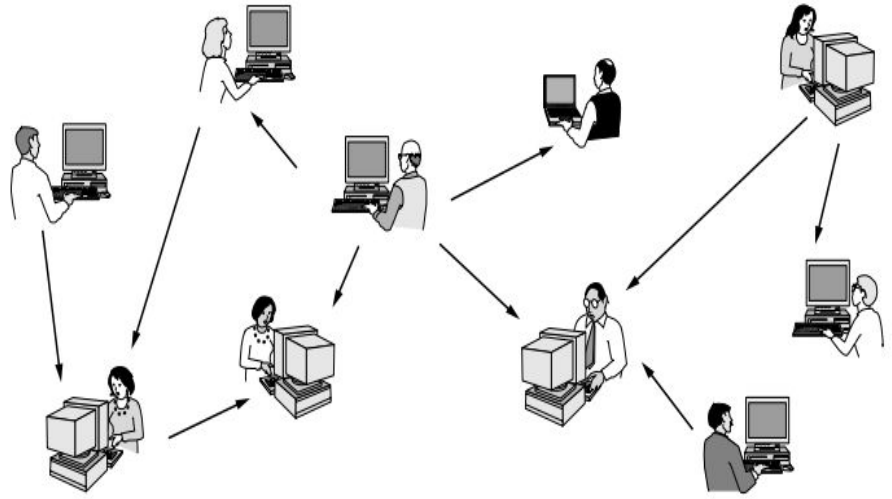


Figure 1-3. In a peer-to-peer system there are no fixed clients and servers.

Tag	Full name	Example
B2C	Business-to-consumer	Ordering books online
B2B	Business-to-business	Car manufacturer ordering tires from supplier
G2C	Government-to-consumer	Government distributing tax forms electronically
C2C	Consumer-to-consumer	Auctioning second-hand products online
P2P	Peer-to-peer	Music sharing

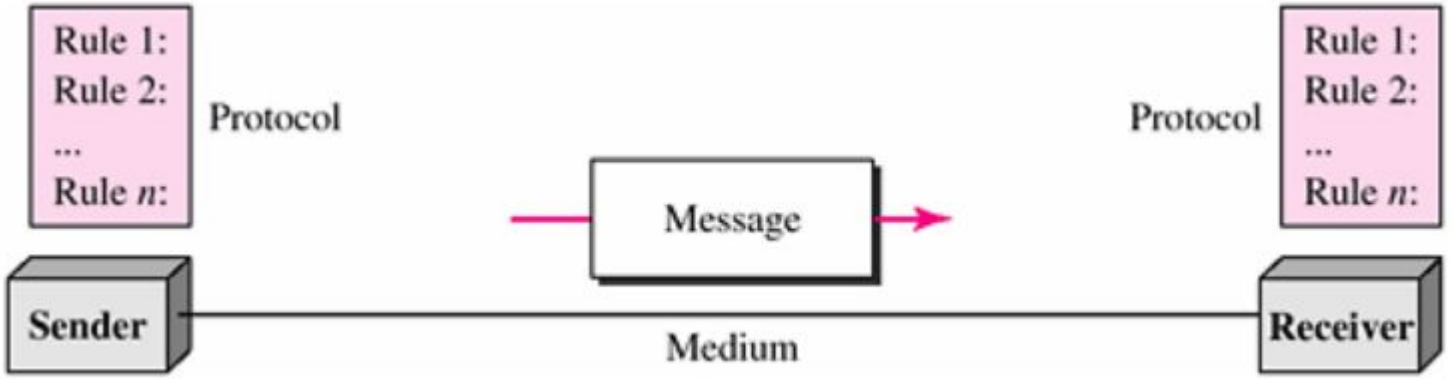
Figure 1-4. Some forms of e-commerce.

Mobile Users

- Mobile computers, such as laptop and handheld computers
- Text messaging or texting
- Smart phones,
- GPS (Global Positioning System)
- m-commerce

Topic: Introduction to data communication

- Data and data communication
- **Fundamental characteristic of Data communication**
  - Delivery
  - Accuracy
  - Jitter
  - Timeliness
- **Components of data communication**



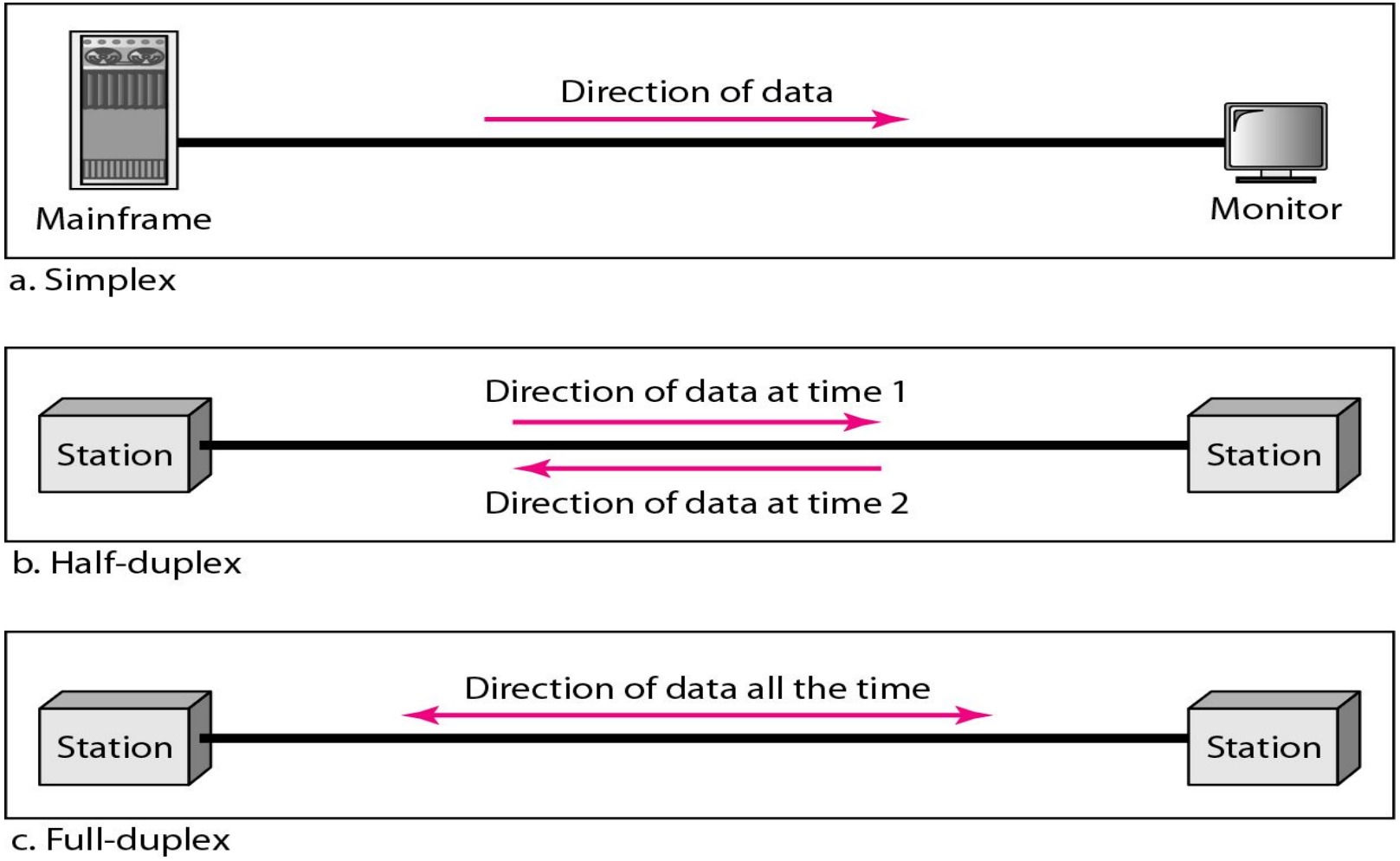
Topic: Introduction to data communication

Data Representation:

- TEXT: represented in specific bit pattern. Unicode format -ASCII
- Numbers : represented in specific bit pattern
- Images : Pixel, bit pattern. B & W -1 bit pattern, colour image –RGB,YCM
- Audio : recording or broadcasting of sound or music . continuous
- Video : recording or broadcasting of a picture or movie

Introduction to data communication : Data Flow

Data flow



Networks: Network Hardware/Network Software

- A network is a set of devices (often referred to as nodes) connected by communication links.
- A node can be a computer, printer, or any other device capable of sending and/or receiving data generated by other nodes on the network.
- Networks come in many sizes, shapes and forms.

Network Hardware

Network hardware depends on **transmission technology** and **scale**.

Transmission Technology

- **Broadcast network**
  Broadcast networks have a single communication channel that is shared by all the machines on the network
- **Point-to-point network**.
  point-to-point networks consist of many connections between individual pairs of machines

Network Hardware

Scale

- An alternative criterion for classifying networks is their scale. Multiple processor systems can be arranged by their physical size.

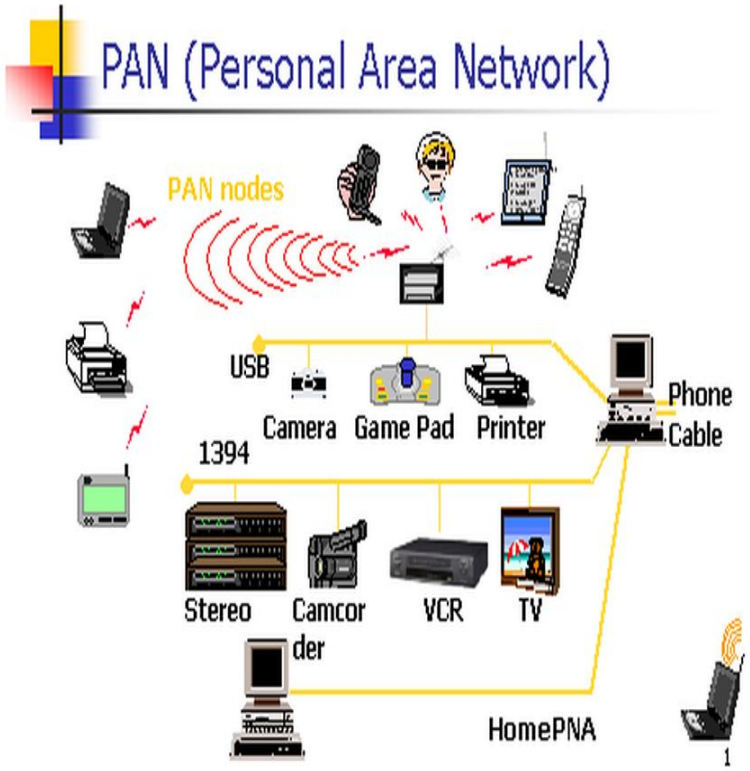
Inter processor Distances	Processors located in same	Examples
1 m	Square meter	Personal Area Network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan Area Netwo
100 km	Country	Wide Area Network
1000 km	Continent	
10000 km	Planet	The Internet

Classification of interconnected processors by scale.

- **Scale**
  - Personal Area Networks
  - Local Area Networks
  - Metropolitan Area Networks
  - Wide Area Networks
  - Internetworks

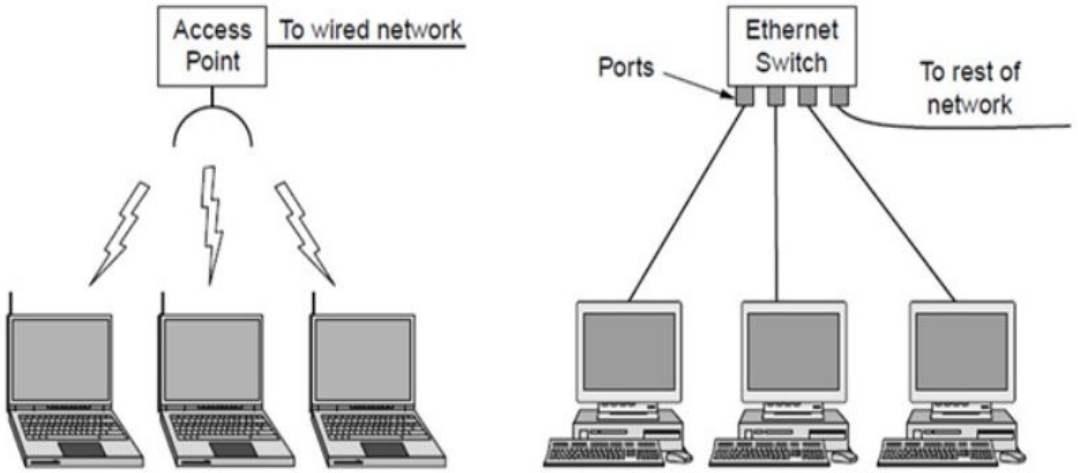
1. Personal Area Network

1. Personal Area Network (PAN) is a computer network used for data transmission amongst devices such as computers, telephones, tablets and personal digital assistants.
2. **Also Known as HAN (Home Area Network)**
3. PANs can be used for communication amongst the personal devices themselves (interpersonal communication), or for connecting to a higher level network and the Internet (an uplink) where one "master" device takes up the role as internet router.



2. Local Area Network

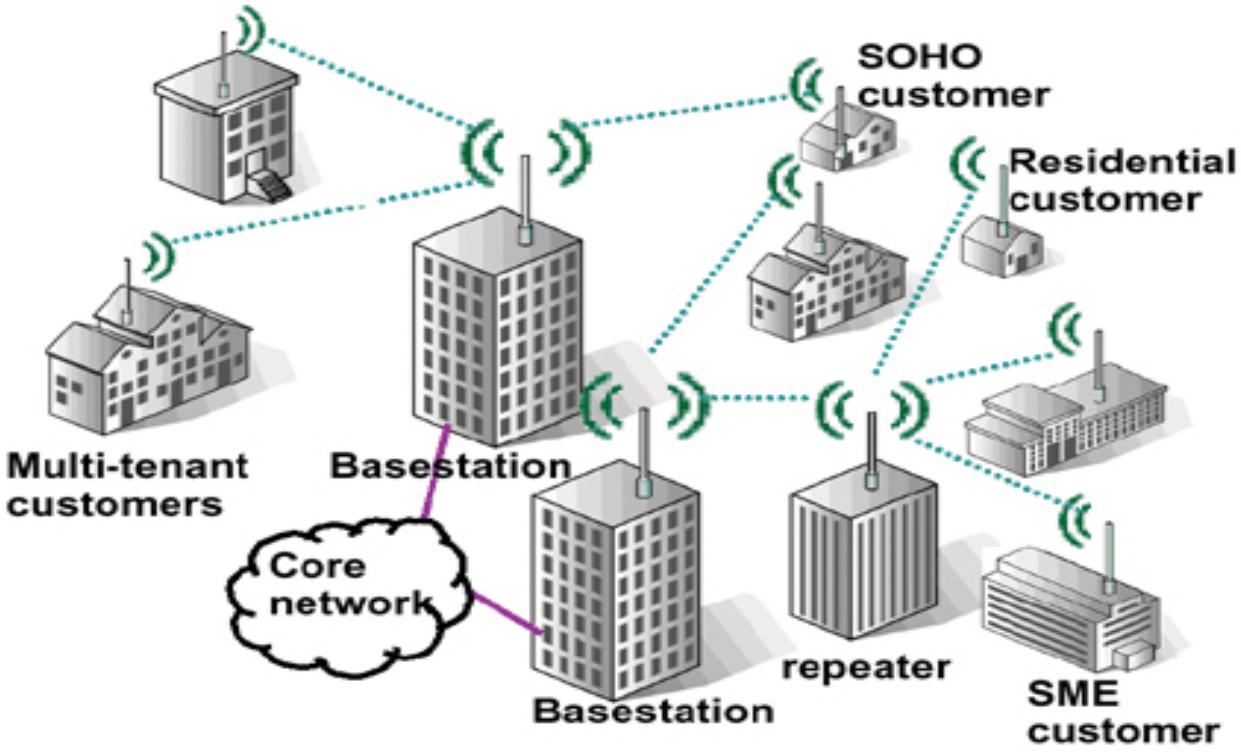
- Ethernet has evolved and has seen significant improvements in regard to speed and efficiency.
- An upside of a LAN is fast data transfer with data speed that can reach up to 10Gbps.
- classic Ethernet
- wireless and wired broadcast networks can be divided into static and dynamic designs(centralized and decentralized) , depending on how the channel is allocated.



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

3. Metropolitan Area Network

1. A MAN is larger than a LAN but smaller than or equal in size to a WAN.
2. The size range anywhere from 5 to 50km in diameter.
3. MANs are typically owned and managed by a single entity.
4. This could be an ISP or telecommunications company that sells its services to end-users in that metropolitan area.
5. For all intents and purposes, a MAN has the same characteristics as a WAN with distance constraints



Metropolitan Area Network - www.certiology.com

4. Wide Area Network

- A Wide Area Network exist over a large area
- Data travels through telephone or cable lines
- Usually requires a Modem
- The world's largest Wide Area Network in the Internet

Network Devices

- **What is a network device?**

Components used to connect computers as well as other electrical devices together in order to share resources such as printers and fax machines.

- Hubs
- Switches
- Routers
- Network bridges
- Gateways
- Firewalls
- Wireless AP (Access Points)

HUB

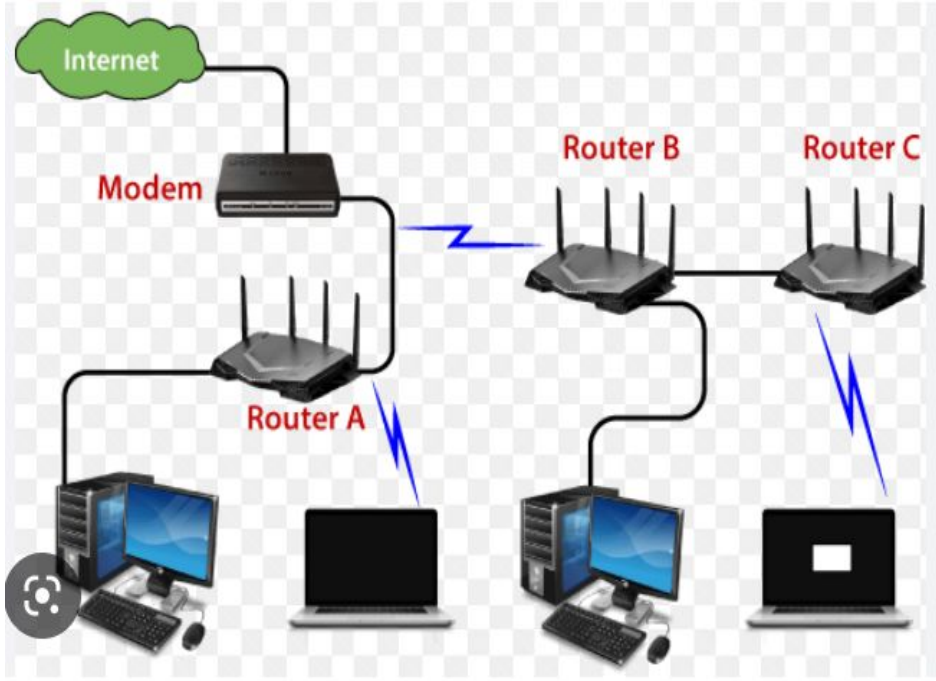
- A small rectangular box that joins computers together through ports on the back of the hub
- hub receives data packets and passes on all the Information it receives to all the other computers connected to the hub.
- Information is also sent to the computer that sent the information!
- Example: if computer 1 wants to communicate with computer 3, the data will be sent to all the computers on the network since hubs do not know the destination of the information it receives.
- Hubs can be used for a smaller network such as a home network or a small office network

Switch

- Switches look similar to hubs in that they are rectangular in shape
- Unlike hubs, switches can identify the destination of a packet.
- Switches send information only to the computer that is suppose to receive the information.
- Switches can also send and retrieve information at the same time which makes sending information faster to retrieve than hubs.
- Switches are a better option than hubs for larger networks or home networks with 4 or more connected computers.

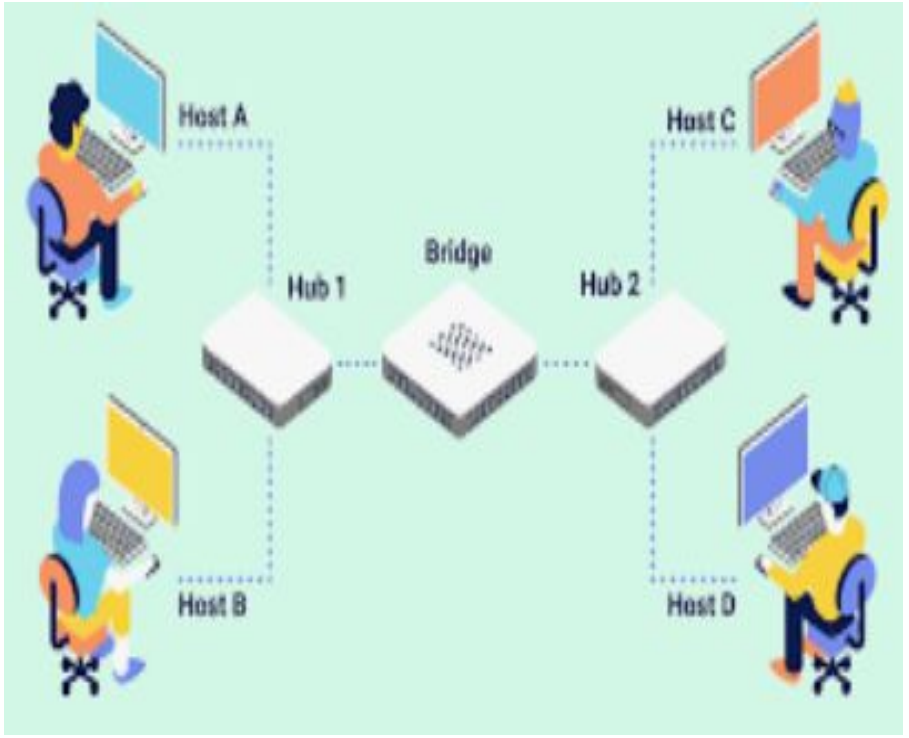
Router

- A specialized computer programmed to interface between different networks
- A router receives data from the user.
- Looks for the remote address of the other computer making routing decisions along the way
- Forwards the user data out to a different interface that is closer to the remote computer
- Routers make sure data sent over the Internet goes where it needs to go and not where it is not needed.
- Acts like a traffic controller, working to cut down congestion throughout the network and keeps everything flowing smoothly along the best path.



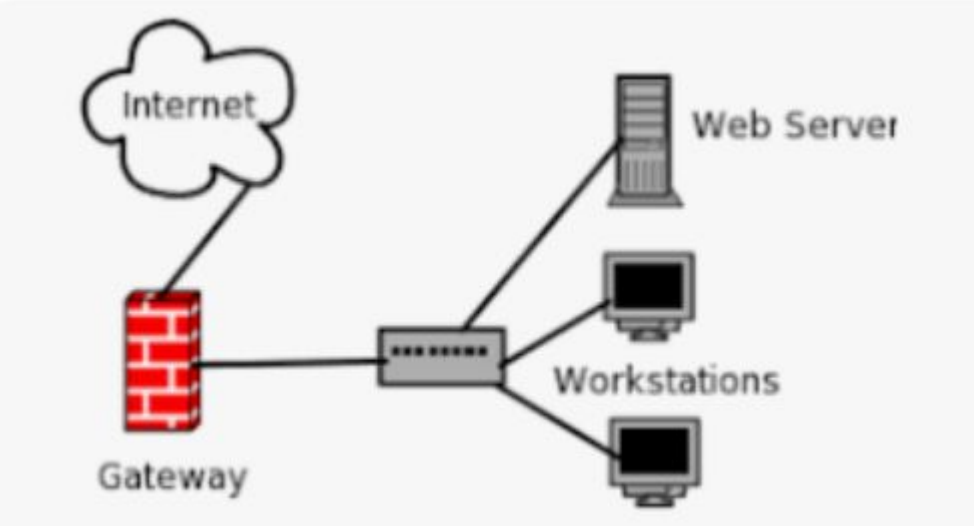
Bridge

- A hardware device used to create a connection between two separate computer networks or to divide one network into two.
- Filters data traffic at a network boundary and reduces the amount of traffic on a LAN dividing it into two segments.
- Each bridge consist of a MAC address and operates at layer 2 of the OSI model
- When a packet is received on the bridge ports the forwarding table including the MAC address is automatically updated to map the source MAC address to the network port from which the packet originated
- The gateway then process the received packet according to the packet's type.



Gateway

- A communication device that provides a remote network with connectivity to the host network
- The gateway node acts like a proxy server and firewall.
- The gateway uses forwarding tables to determine where packet are to be sent.
- On the Internet a node or stopping point can be a gateway.
- The computers controlling traffic within a network are gateway nodes.
- A gateway is also associated with a router.



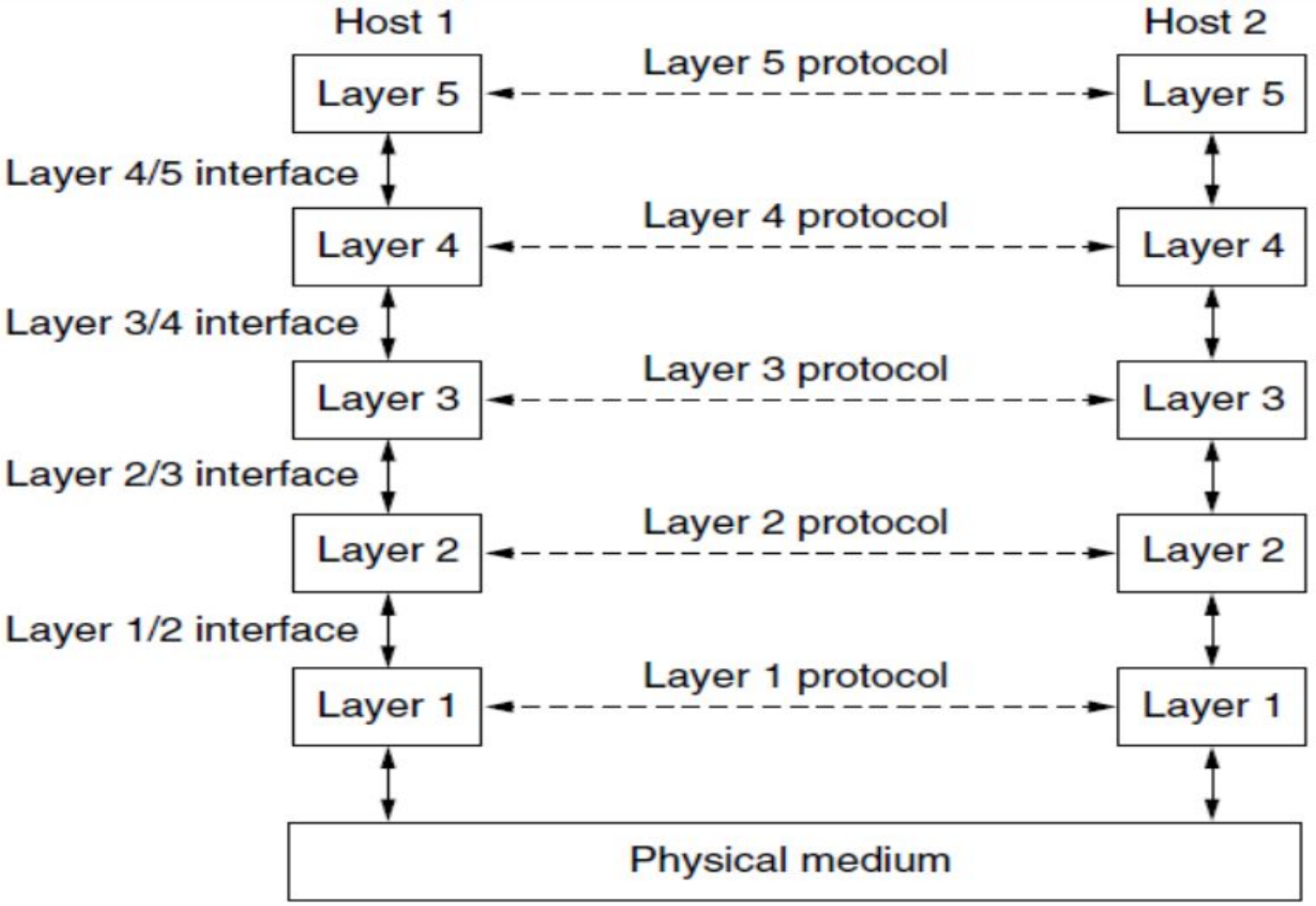
Network Software

- Communication Protocol Hierarchies
- Connection-Oriented and Connectionless Services
- Service Primitives
- The Relationship of Services to Protocols

Network Software: Protocol Hierarchies

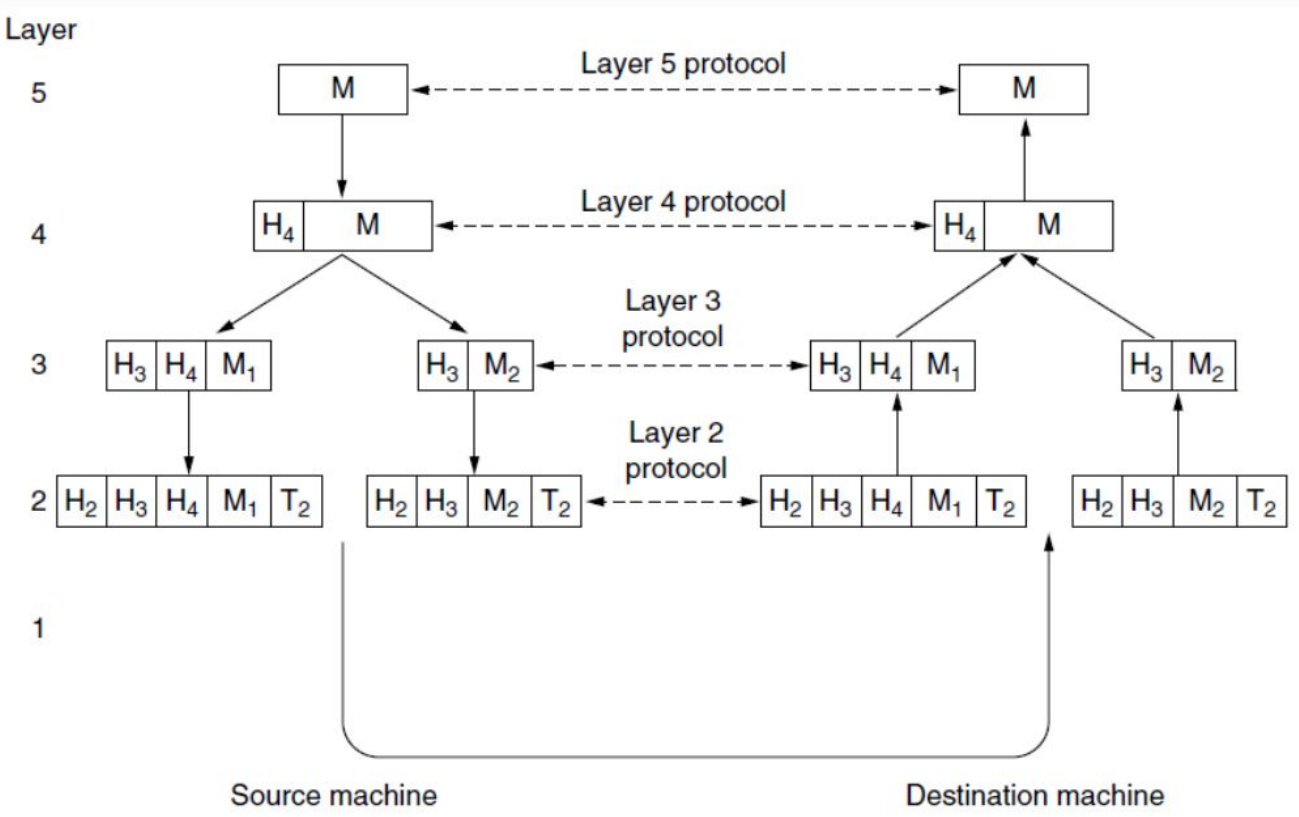
- **Layers, protocols, and interfaces**
- Conversation between layer n on one machine with layer n on another machine: the rules and conventions used in this conversation are collectively known as the

  layer n protocol.
- Between each pair of adjacent layers is an interface.
- The **interface** defines which primitive operations and services the lower layer makes available to the upper one
- A set of layers and protocols is called a **network architecture**
- A list of the protocols used by a certain system, one protocol per layer, is called a **protocol stack**


Host 1
Host 2
Layer 5
Layer 5 protocol
Layer 5
Layer 4/5 interface
Layer 4
Layer 4 protocol
Layer 4
Layer 3/4 interface
Layer 3
Layer 3 protocol
Layer 3
Layer 2/3 interface
Layer 2
Layer 2 protocol
Layer 2
Layer 1/2 interface
Layer 1
Layer 1 protocol
Layer 1
Physical medium

Network Software: Protocol Hierarchies

- Communication Flow
- Definition 1: A protocol is an agreement between the communicating parties on how communication is to proceed
- Definition 2: A protocol is a set of communication "rules" between two processes



Design Issues for the Layers

A number of design issues exist for the layer to layer approach of computer networks

- Reliability : operate correctly.
  - Error detection
  - Error correction
  - routing
- Addressing
- Resource Allocation : Flow Control & congestion
- Security
- Scalability

Network Software: Connection-Oriented

- Connection is established, the sender, receiver, and subnet conduct a negotiation about the parameters to be used, such as
  - Maximum message size
  - Quality of service required, and other issues
- Typically, one side makes a proposal and the other side can accept it, reject it, or make a counter proposal.
- A circuit is another name for a connection with associated resources (after the **telephone model** …)
- Reliability: do not lose data – e.g., the receiver acknowledge the receipt of each message
- so the sender is sure that it arrived
- TCP – Transmission Control Protocol is connection oriented
- **Text documents, email, image attachments**

Network Software: Connectionless Services

- In contrast to connection-oriented service, connectionless service is modeled after the **postal system**
- Each message (letter/package) carries the full destination address and each one is routed through the intermediate nodes inside the system independent of all the subsequent messages
- UDP – User Datagram Protocol – unreliable
- Unreliable (meaning not acknowledged) connectionless service is often called **datagram service**, in analogy with **telegram** (service, which also does not return an acknowledgement to the sender)
- Video streaming, Video conference, VOIP, Digital TV transmission

Connection-Oriented and Connectionless Services

	Service	Example
Connection-oriented	Reliable message stream	Sequence of pages
	Reliable byte stream	Remote login
	Unreliable connection	Digitized voice
Connection-less	Unreliable datagram	Electronic junk mail
	Acknowledged datagram	Registered mail
	Request-reply	Database query

Connection-oriented Service Primitives

- Minimal example of service primitives that provide a reliable byte stream
- A service is formally specified by a set of primitives (operations) available to user processes to access the service
- These primitives tell the service to perform some action or report on an action taken by a peer entity (usually as operating system calls)
- Modeled after the Berkeley socket interface

Primitive	Meaning
LISTEN	Block waiting for an incoming connection
CONNECT	Establish a connection with a waiting peer
RECEIVE	Block waiting for an incoming message
SEND	Send a message to the peer
DISCONNECT	Terminate a connection

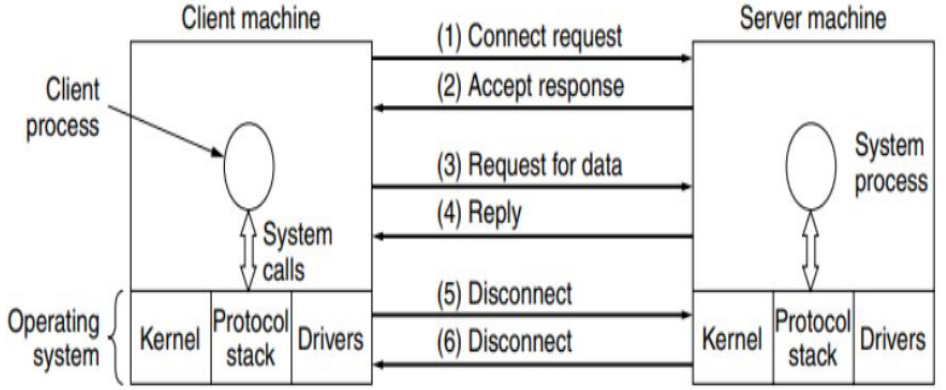


Figure 9. A simple client-server interaction using acknowledged datagrams.

Difference between Connection-Oriented Connectionless Services

S.NO	Connection-oriented Service	Connection-less Service
1	Connection-oriented service is related to the telephone system.	Connection-less service is related to the postal system.
2.	Connection-oriented service is preferred by long and steady communication.	Connection-less Service is preferred by bursty communication.
3.	In connection-oriented Service, Congestion is not possible.	In connection-less Service, Congestion is possible.
4.	Connection-oriented Service gives the guarantee of reliability.	Connection-less Service does not give a guarantee of reliability.
5.	In connection-oriented Service, Packets follow the same route.	In connection-less Service, Packets do not follow the same route.
6.	Connection-oriented services require a bandwidth of a high range.	Connection-less Service requires a bandwidth of low range.
7.	Ex: TCP (Transmission Control Protocol)	Ex: UDP (User Datagram Protocol)
8.	Connection-oriented requires authentication.	Connection-less Service does not require authentication.

The Relationship of Services to Protocols

- A service is a set of primitives (operations) that a layer provides to the layer above it.
- The service defines what operations the layer is prepared to perform or behalf of its users, but it says nothing at all about how these operations are implemented.
- A service relates to an interface between two layers, with the lower layer being the service provider and the upper layer being the service user.
- A service is like an abstract data type or an object in an object-oriented language.
- It defines operations that can be performed on an object but does not specify how these operations are implemented.

The Relationship of Services to Protocols

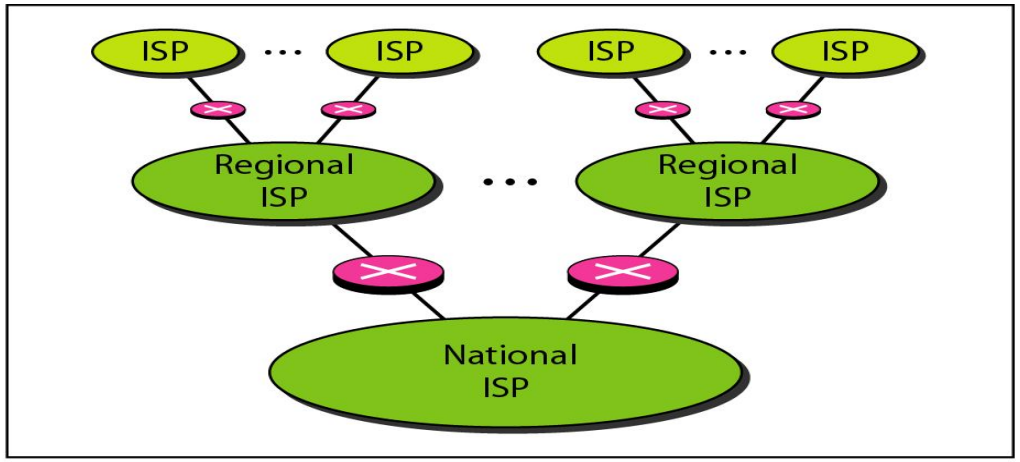
- A protocol, in contrast, is a set of rules governing the format and meaning of the frames, packets, or messages that are exchanged by the peer entities within a layer.
- Entities use protocols in order to implement their service definitions.
- They are free to change their protocols at will, provided they do not change the service visible to their users.
- In this way, the service and the protocol are completely decoupled
- A protocol relates to the implementation of the service and as such is not visible to the user of the service

Internet: Internet history

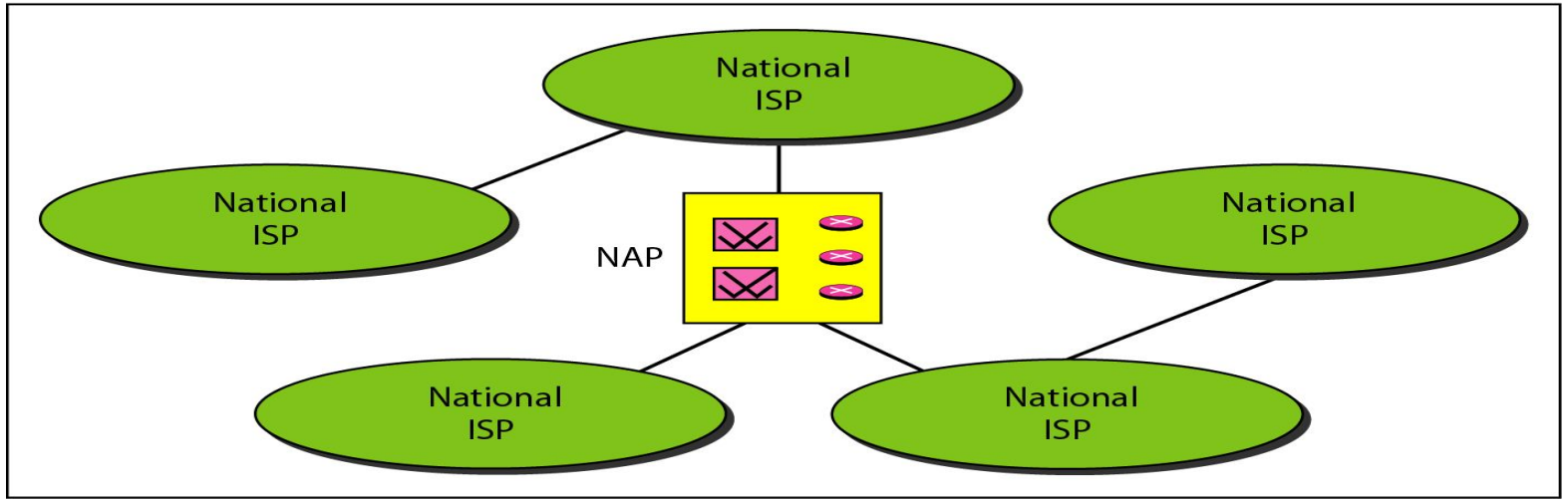
Internet :

- Started as DARPNET – scientist and researchers used to communicate and share file.
- 1965 –MIT developed packet switching network
- 1967: Larry Roberts, a program manager at ARPA –remote access –networking : packet switched network –using router
- 1969 – ARPANET started node to node communication
- 1970 – Robert E Khann and Vinton Cerf invented TCP and IP
- 1980 – Scientist and researcher used network to share files between different universities and labs. Late 80's DNS in existence
- 1991 –Tim- Berners Lee introduced the WWW : an Internet. He created the first browser and the Internet
- 1992 – a group of student and researcher developed a browser called Mosaic. Which was later called Netscape

Hierarchical Organization of Internet



a. Structure of a national ISP



b. Interconnection of national ISPs

Protocols and Standards

Protocols are rules and regulations.

- It defines what is communicated, how it is communicated, and when it is communicated.
- Key elements of protocol are,
  - Syntax: Format of data
  - Semantics: Meaning of each section of bits
  - Timing: When data should sent and how fast?

Standards are agreed rules.

- Essential for creating and maintaining an open and competitive market for equipment manufactures.
- For national and international interoperability.
- De facto standards: Not been approved by an organized body but have been adopted as standards through widespread use.

Protocols and Standards

- **Standard Organizations**
  - Standard Creation Committees
    - ISO (International Standard Organization)
    - International Telecommunication Union-Telecommunication Standards Sector (ITU-T)
    - American National Standards Institute (ANSI)
    - Institute of Electrical and Electronics Engineers (IEEE)
    - Electronic Industries Association (EIA)
  - Forums
  - Regulatory Agencies: FCC (Federal Communications Commissions)
- **Internet Standards**
  - Internet draft: Lifetime of only 6 month
  - RFC (Request for Comment): After recommendation from internet authorities, draft will be converted to RFC.

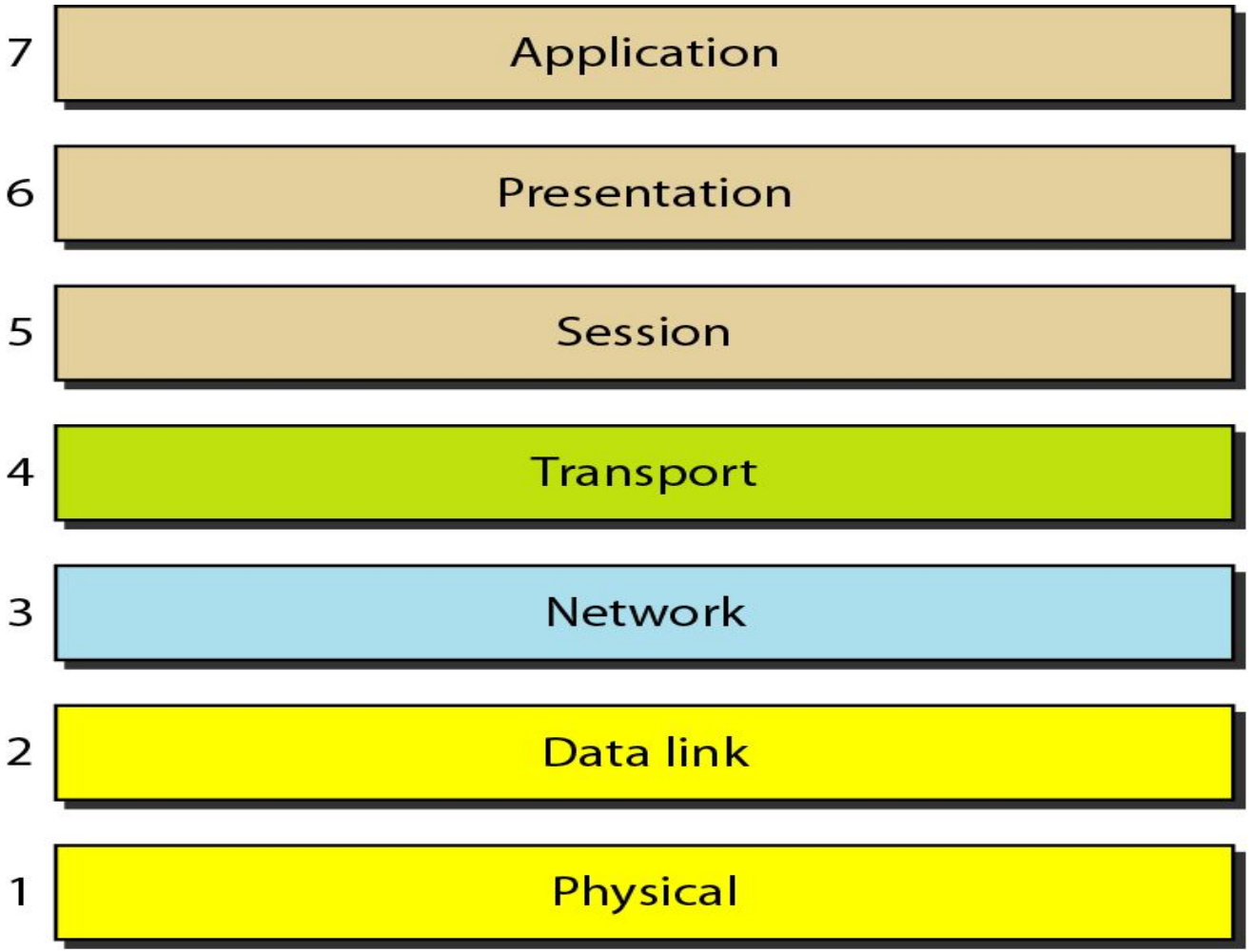
RFCs

- A Request for Comments (RFC) is a formal document from the **Internet Engineering Task Force (IETF)** that contains **specifications and organizational notes** about topics related to the **internet and computer networking**, such as **routing, addressing and transport technologies**
- An IETF RFC begins with an initial draft, referred to as the Internet-Draft (I-D). This draft is typically created by an individual or small group. The I-D is then adopted by a working group that reviews, improves and revises the document's content.
- RFCs are produced primarily by the Internet Architecture Board (IAB), Internet Research Task Force (IRTF) and IETF
- After an RFC has gone through the review and revision process, it receives a final review for errors, as well as for style and editorial issues. Once a satisfactory document is produced, the **RFC Production Center (RPC)** assigns a unique number to the RFC and publishes it through the RFC Editor.
- Eg : DHCP RFC 2131, DNS RFC 1034,1035

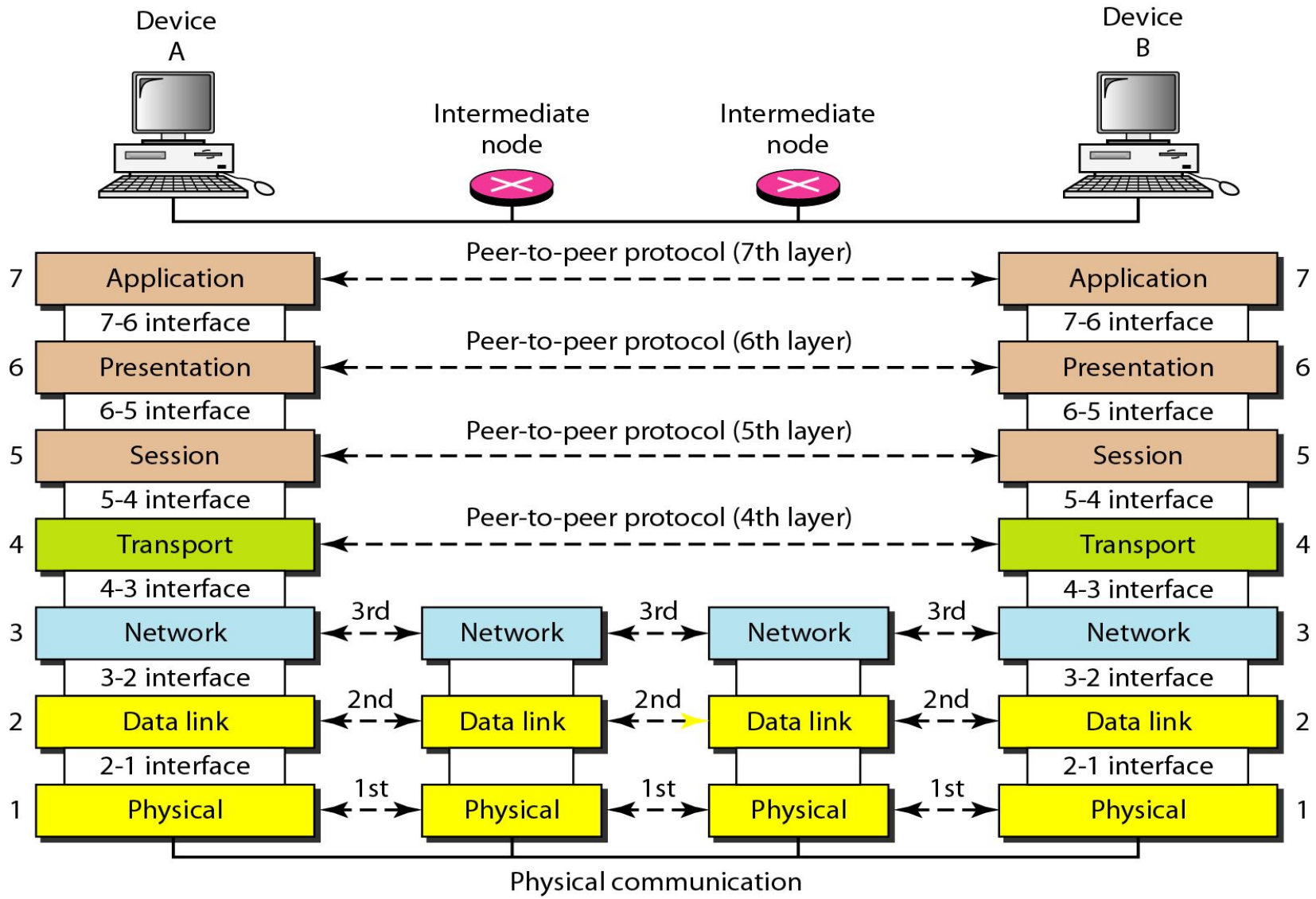
OSI Model

- Established in 1947, the International Standards Organization (ISO) is a multinational body dedicated to worldwide agreement on international standards.
- An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model. It was first introduced in the late 1970s.
- ISO is the organization. OSI is the model.
- The principles that were applied to arrive at the seven layers can be briefly summarized as follows:
  1. A layer should be created where a different abstraction is needed.
  2. Each layer should perform a well-defined function.
  3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols

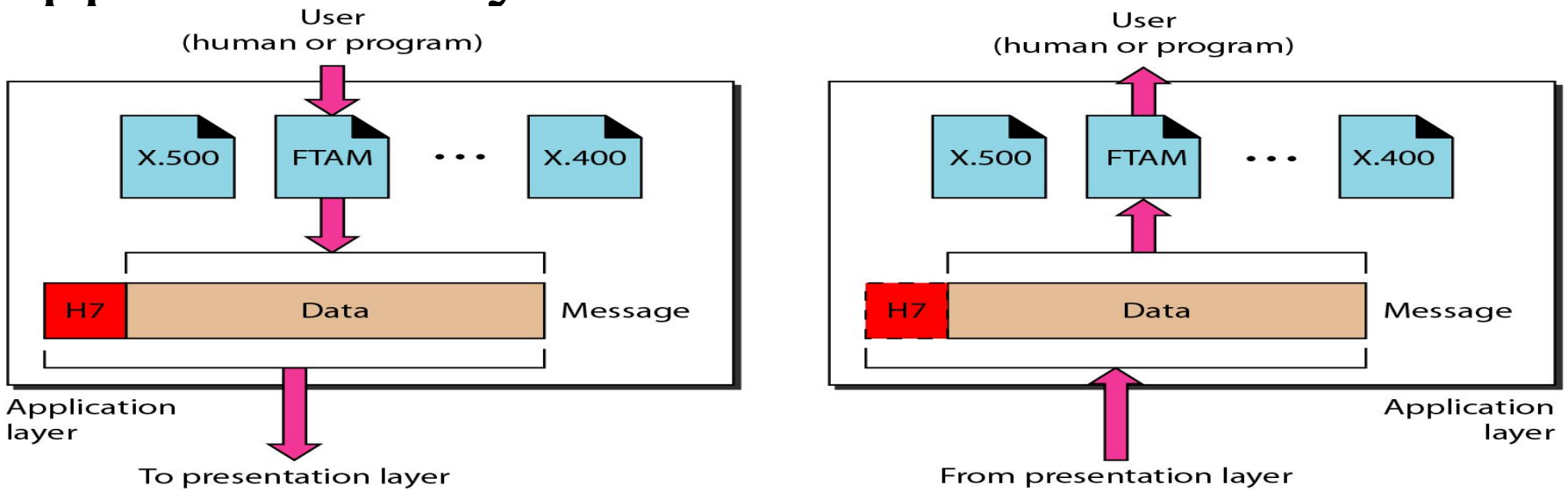
Seven Layers of OSI



Interaction between Layers

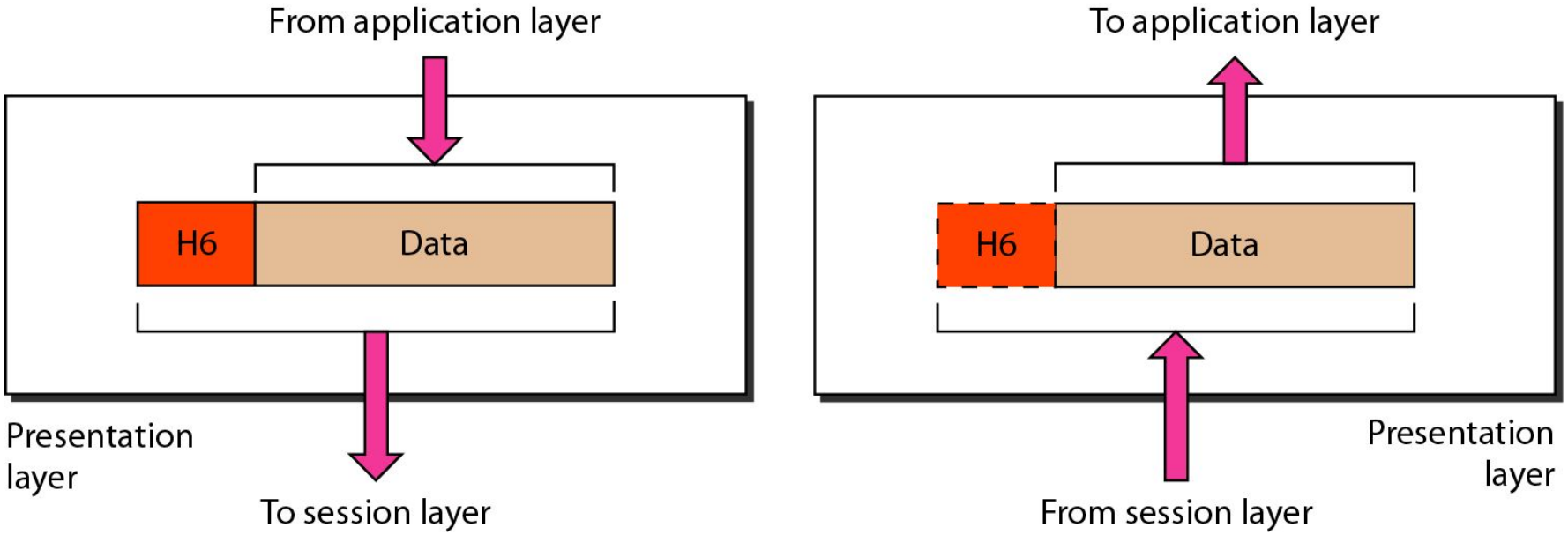


Application Layer



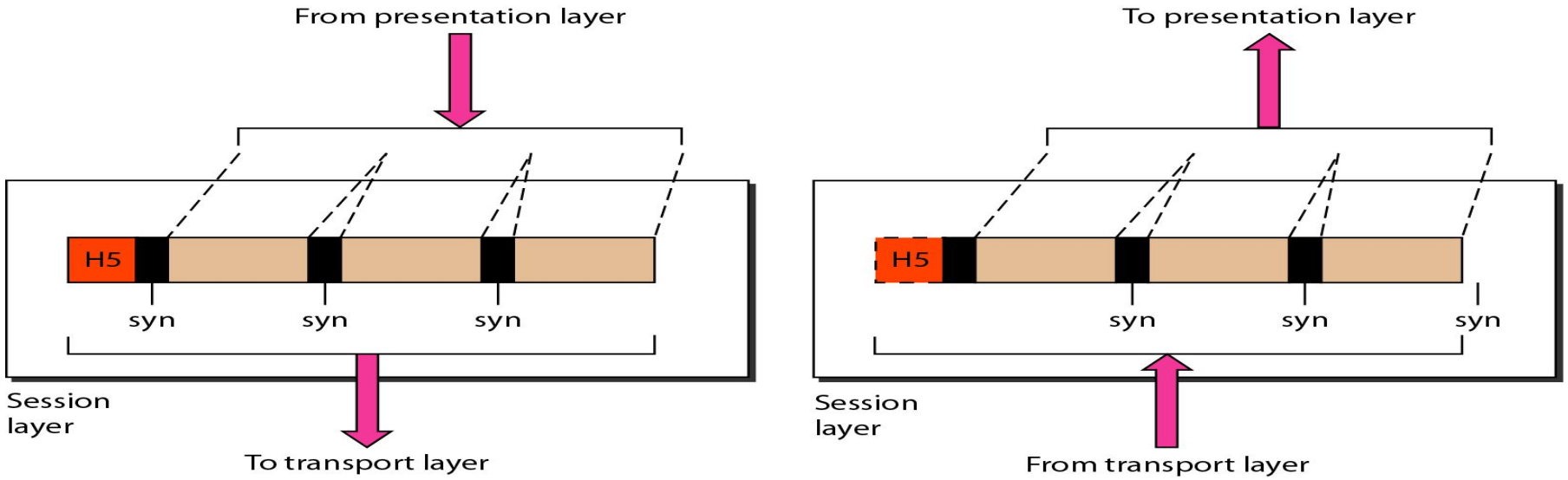
- Functionality:
  - File transfer, access and management
  - Mail services
  - Directory services

Presentation Layer



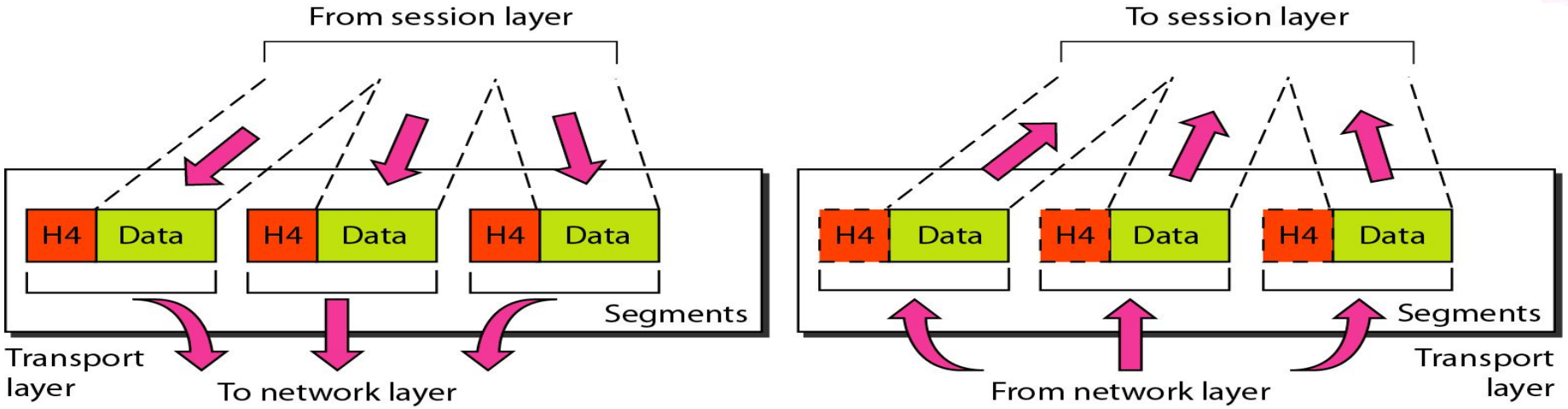
- Functionality: Syntax and Semantics
  - Translation
  - Compression
  - Encryption.

Session Layer



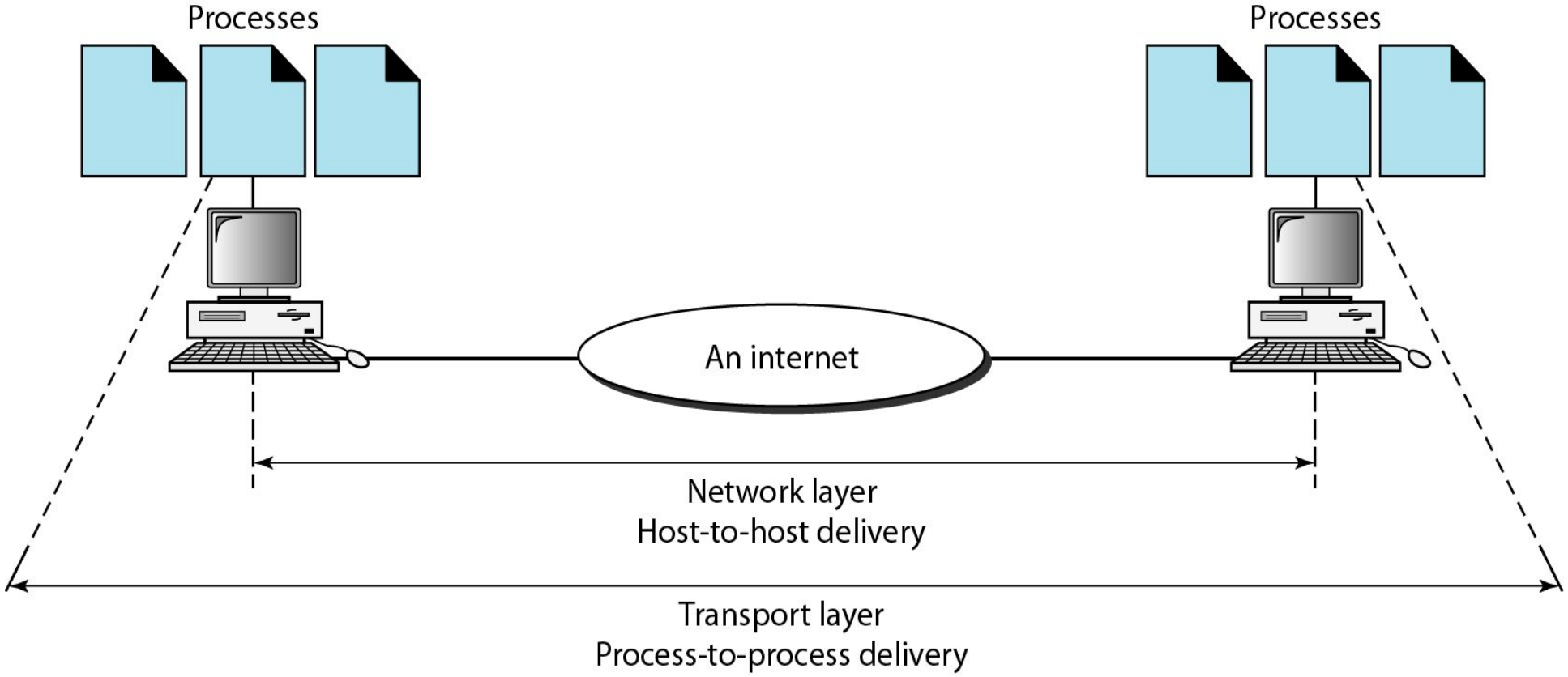
- Functionality:
  - Dialog control
  - Synchronization and Check-pointing
  - This layer is network dialog controller – establishes, maintains, synchronizes the interaction among computer

Transport Layer

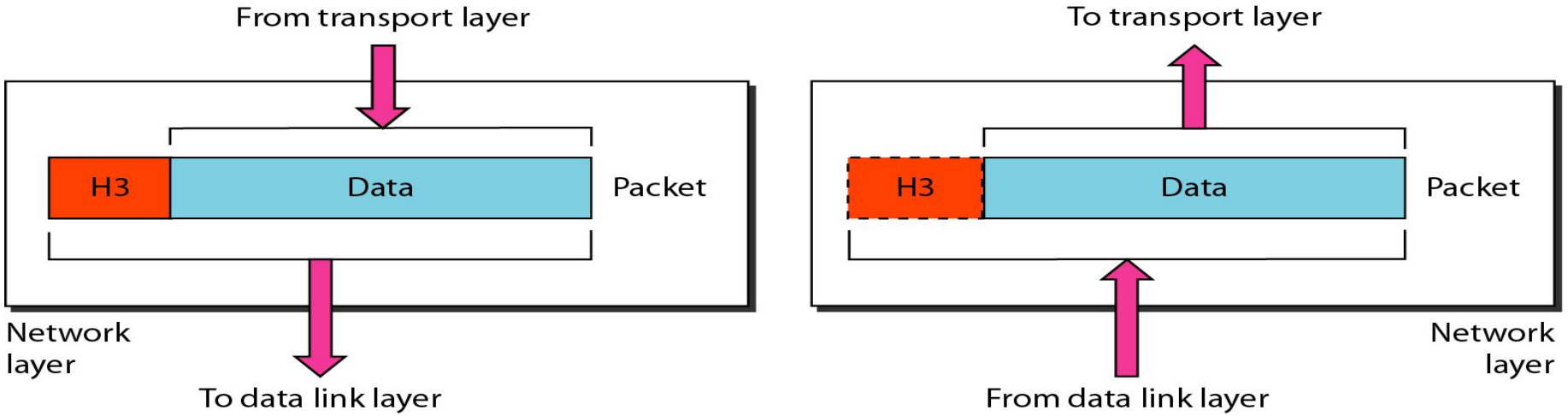


- The transport layer is responsible for the delivery of a message from one process to another.
- Functionality:
  - Service point addressing (port addressing)-provides proper service point address.
  - Segmentation and reassembly-divides message into transmittable segments with a sequence number.
  - Connection control-Connectionless or connection oriented
  - Flow control-process to process rather than across single link.
  - Error control-process to process rather than across single link.
  - Process-to-process delivery

Process to Process Delivery

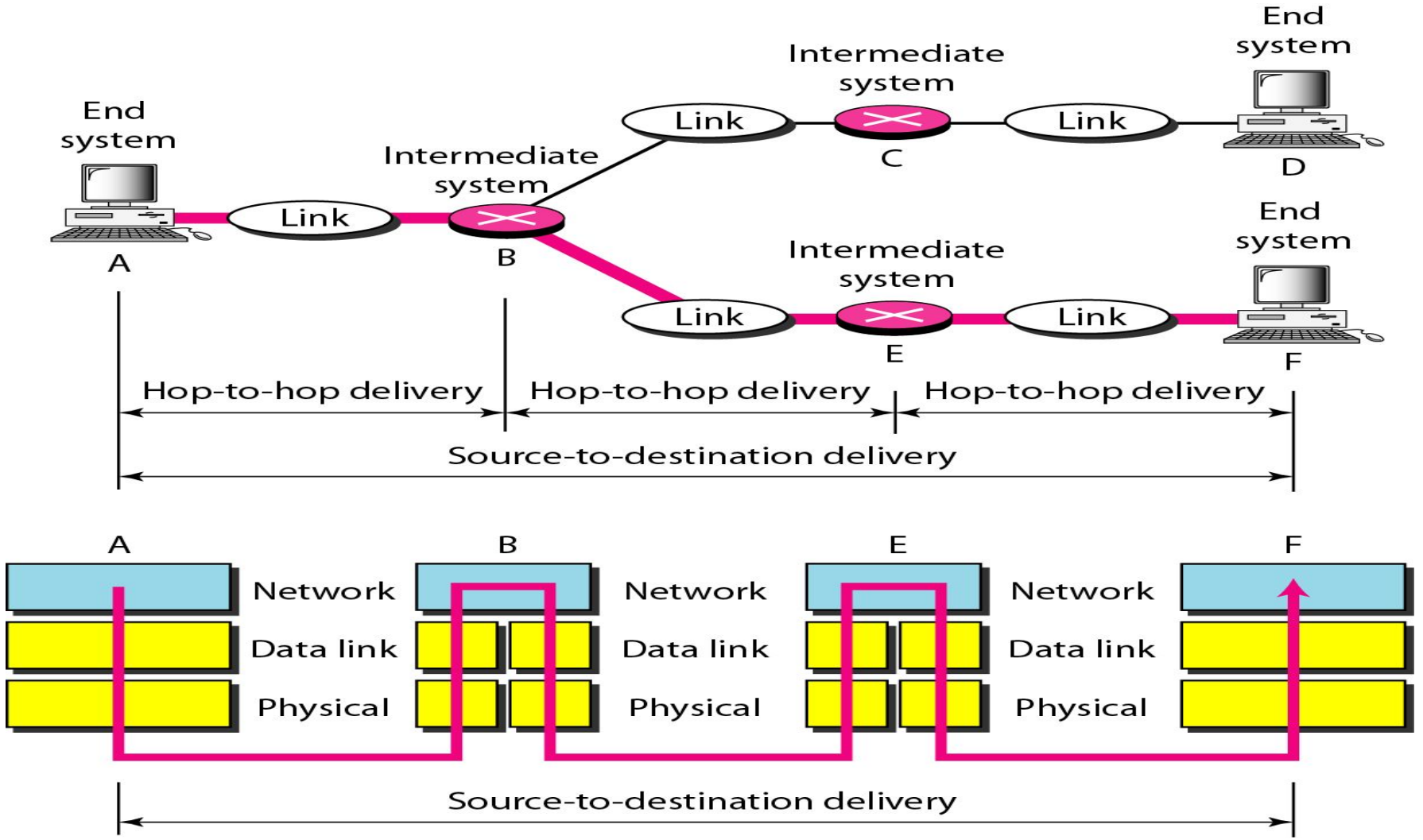


Network Layer

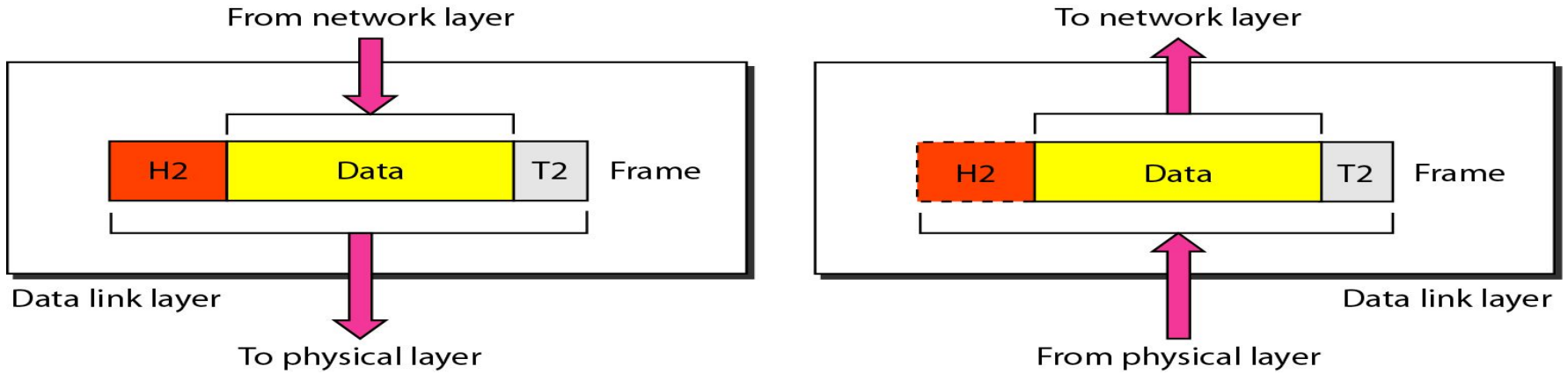


- The network layer is responsible for the delivery of individual packets from the source host to the destination host.
- Functionality :
  - Logical addressing
  - Routing
  - Source-to-destination delivery

Source to Destination Delivery

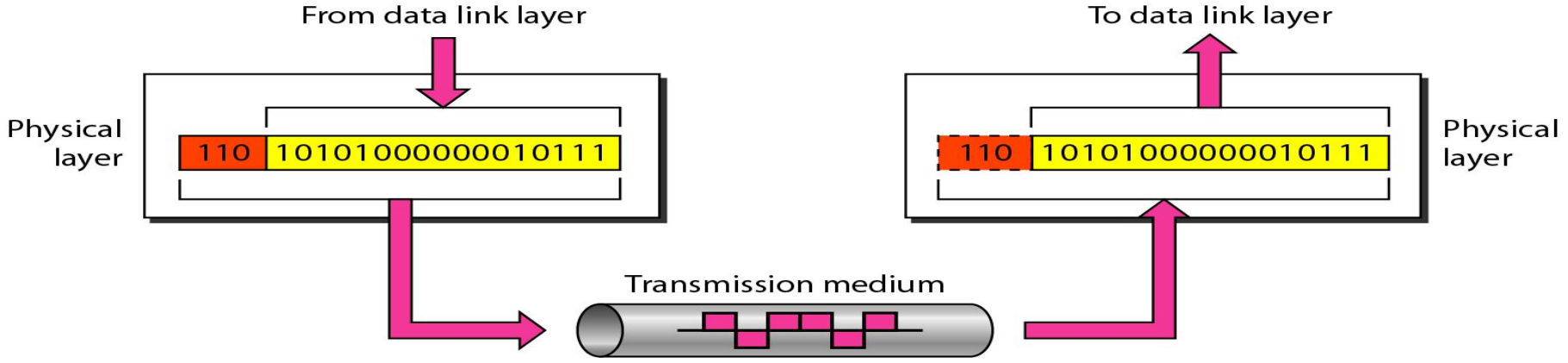


Data Link Layer



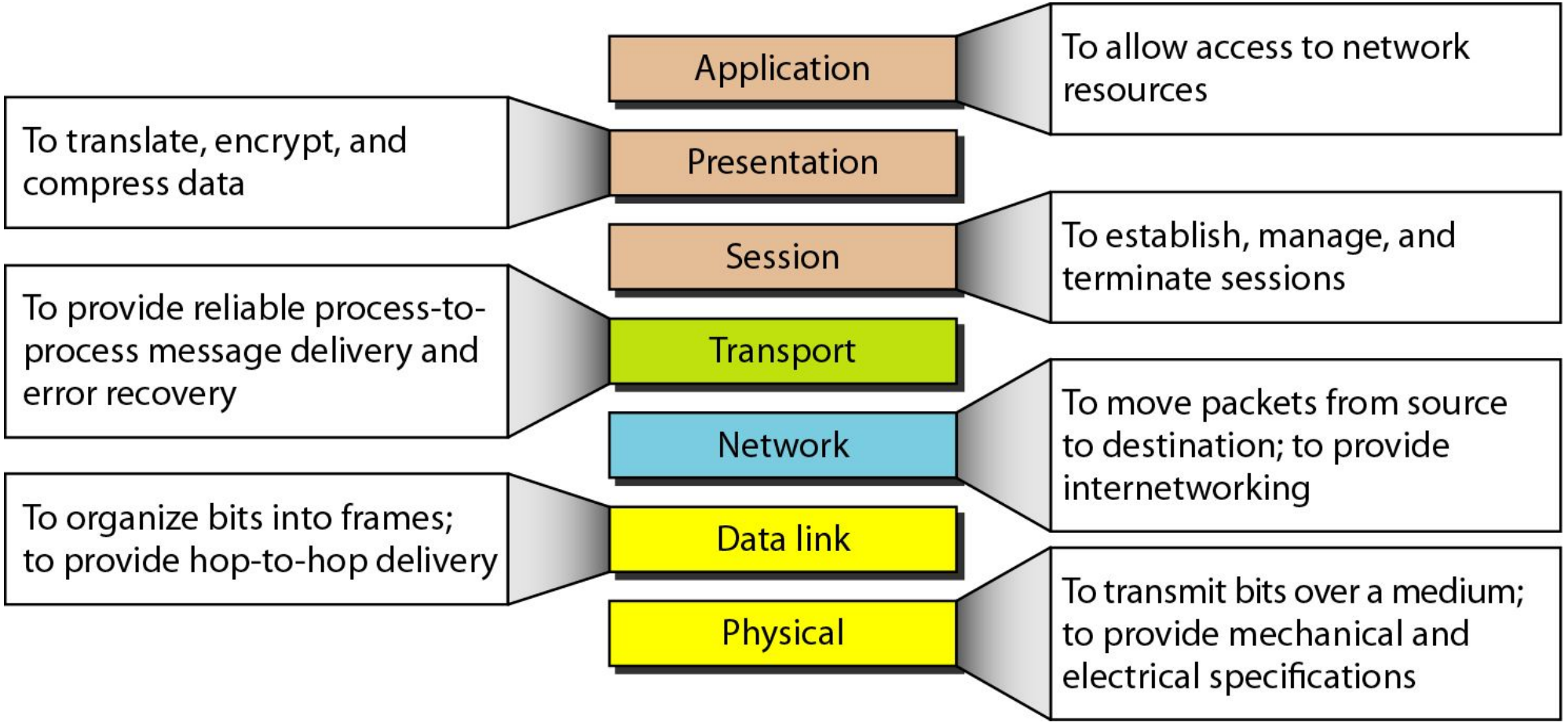
- The data link layer is responsible for moving frames from one hop (node) to the next
- Functionality:
  - Framing
  - Physical addressing
  - Flow control-controlling of flow of data
  - Error control-detection & retransmission of damaged or lost frames.
  - Hop-to-hop delivery or node-to-node delivery

Physical Layer



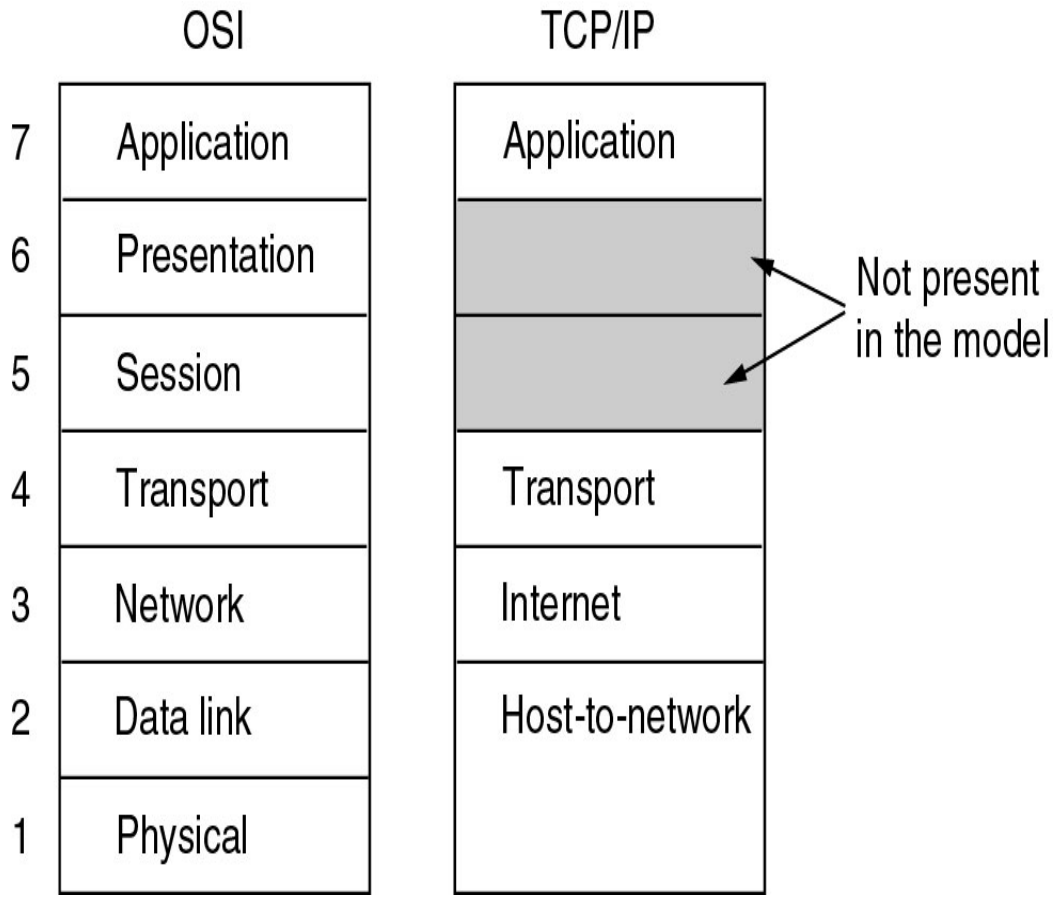
- The physical layer is responsible for movements of individual bits from one hop (node) to the next.
- Functionality of Physical Layer
  - Physical characteristics : interface and medium like guided cables
  - Representation of bits (electrical or optical)
  - Synchronization of bits
  - Line configuration: Point to point, Multipoint
  - Physical topology: Bus, Star, Ring, Hybrid
  - Transmission modes: simplex, half-duplex, full-duplex

Summary of OSI Model

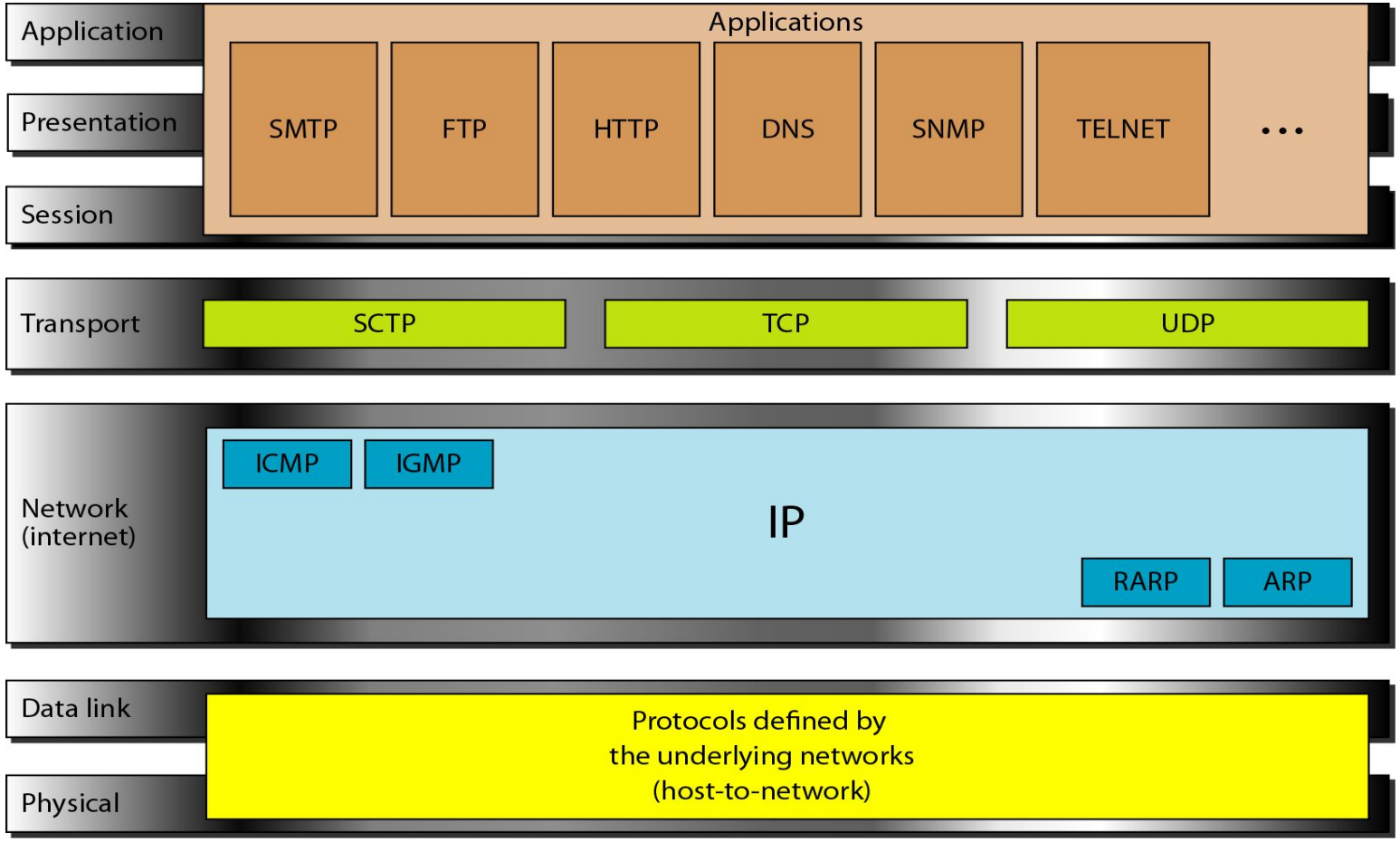


TCP/IP Protocol Suite

- The layers in the TCP/IP protocol suite do not exactly match those in the OSI model.
- The original TCP/IP protocol suite was defined as having four layers: host-to-network, internet, transport, and application.
- However, when TCP/IP is compared to OSI, the TCP/IP protocol suite is made of five layers:
- Host to network, Internet, transport, and application.



TCP/IP Protocol Suite



Application Layer

- Application layer protocols define the rules when implementing specific network applications
- Rely on the underlying layers to provide accurate and efficient data delivery
- Typical protocols:
  1) FTP – File Transfer Protocol : For file transfer
  2) Telnet – Remote terminal protocol : For remote login on any other computer on the network
  3) SMTP – Simple Mail Transfer Protocol : For mail transfer
  4) HTTP – Hypertext Transfer Protocol : For Web browsing
- Encompasses same functions as these OSI Model layers Application Presentation Session

Transport Layer

- **TCP &UDP**
- **TCP is a connection-oriented protocol**
  - Does not mean it has a physical connection between sender and receiver
  - TCP provides the function to allow a connection virtually exists – also called virtual circuit
- **UDP provides the functions:**
  - Dividing a chunk of data into segments
  - Reassembly segments into the original chunk
  - Provide further the functions such as reordering and data resend
- Offering a reliable byte-stream delivery service
- Functions the same as the Transport layer in OSI
- Synchronize source and destination computers to set up the session between the respective computers

Internet Layer & Host-to-network layer

- The **network layer**, also called the internet layer, deals with packets and connects independent networks to transport the packets across network boundaries. The network layer protocols are the IP and the Internet Control Message Protocol (ICMP), which is used for error reporting.

- The **Host-to-network layer** is the lowest layer of the TCP/IP reference model. It combines the link layer and the physical layer of the ISO/OSI model. At this layer, data is transferred between adjacent network nodes in a WAN or between nodes on the same LAN.

Comparison of OSI and TCP/IP reference model

Sr. No	OSI reference Model	TCP/IP reference model
1	OSI represents **Open System Interconnection**	TCP/IP model represents the Transmission Control Protocol / Internet Protocol.
2	It contains 7 layers	It contains 4 layers
3	Protocol independent standard	Protocol dependent standard
4	The OSI model was developed first, and then protocols were created to fit the network architecture's needs	The protocols were created first and then built the TCP/IP mode
5	It distinguishes between Service, Interface and Protocol	Does not clearly distinguishes between Service, Interface and Protocol
6	It provides quality services	It does not provide quality services.
7	The smallest size of the OSI header is 5 bytes.	The smallest size of the TCP/IP header is 20 bytes.

Comparison of OSI and TCP/IP reference model

Sr. No	OSI reference Model	TCP/IP reference model
8	It follows vertical approach	It follows horizontal approach
9	Has separate session and presentation layer	Combines session and presentation layer in the application layer
10	Supports both connectionless and connection-oriented communication in the Network Layer , but only connection-oriented communication in Transport layer	Supports only connection-oriented communication in the Network Layer , but both connectionless and connection-oriented communication in Transport layer
11		
12		

Data and Signals :Analog and Digital Data

Data

It is defined as the entities that convey meaning or information.

Data can be of two types:

1) Analog Data

Analog data is the type of data that varies continuously with respect to time.

Analog data take on continuous values.

E.g. an Analog clock which is having hour, minute, and second hands that gives information in a continuous form, voice and video

2) Digital Data:

Digital data refers to information that has discrete states.

Digital data take on discrete values.

E.g.Digital clock, The data stored in the computer memory in the form of 0's and 1's.

Data and Signals :Analog and Digital Signal

Signal

An electrical or electromagnetic quantity (current, voltage, radio wave, micro wave, etc.) that carries data or information from one system (or network) to another is called a **signal**.

Two basic types of signals are used for carrying data, viz. **analog signal** and **digital signal**

1) **Analog Signals**

Have Infinitely many levels of intensity over a period of time.

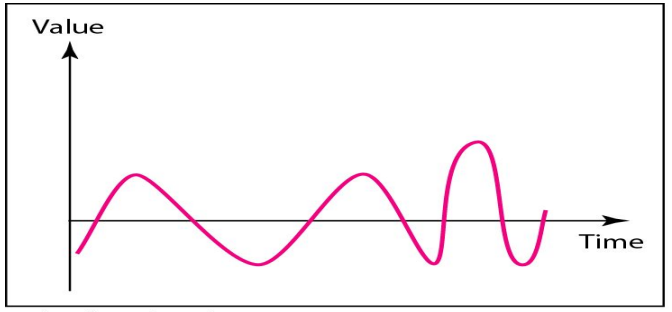
As the wave moves from value A to value B, it passes through and includes an infinite number of values along its path.

Have infinite number of values in a range.

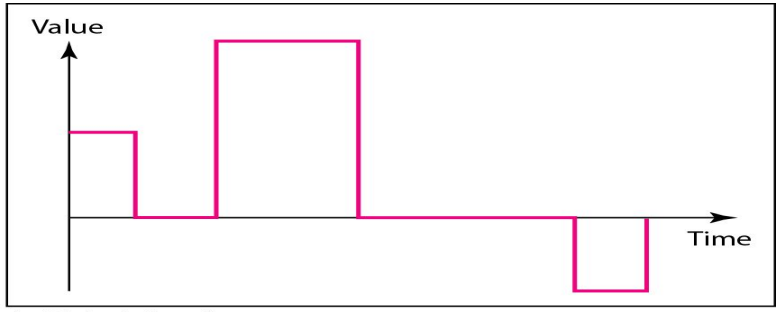
E.g. sine and cosine waves.

2)Digital Signals

Digital signals can have only a limited number of defined values.



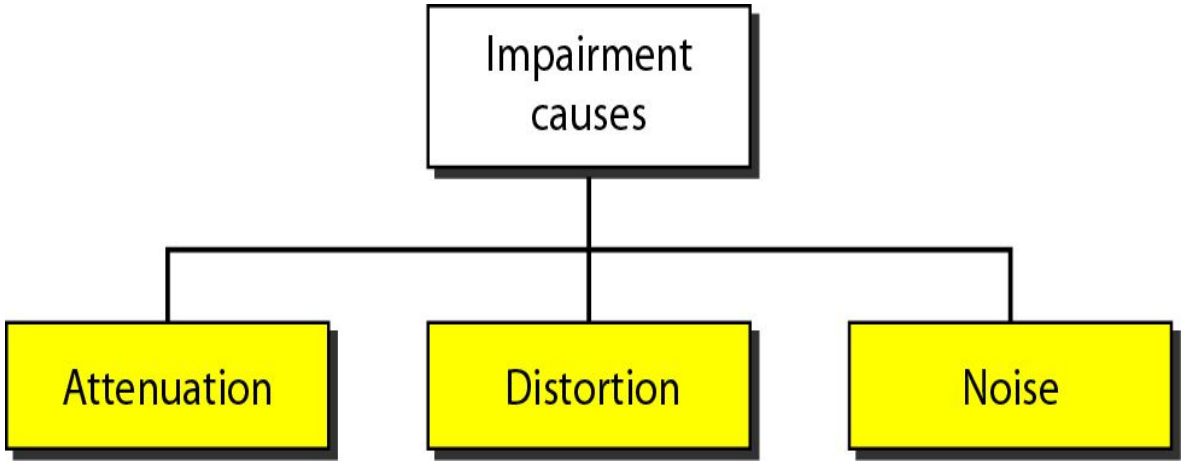
a. Analog signal



b. Digital signal

Transmission Impairment

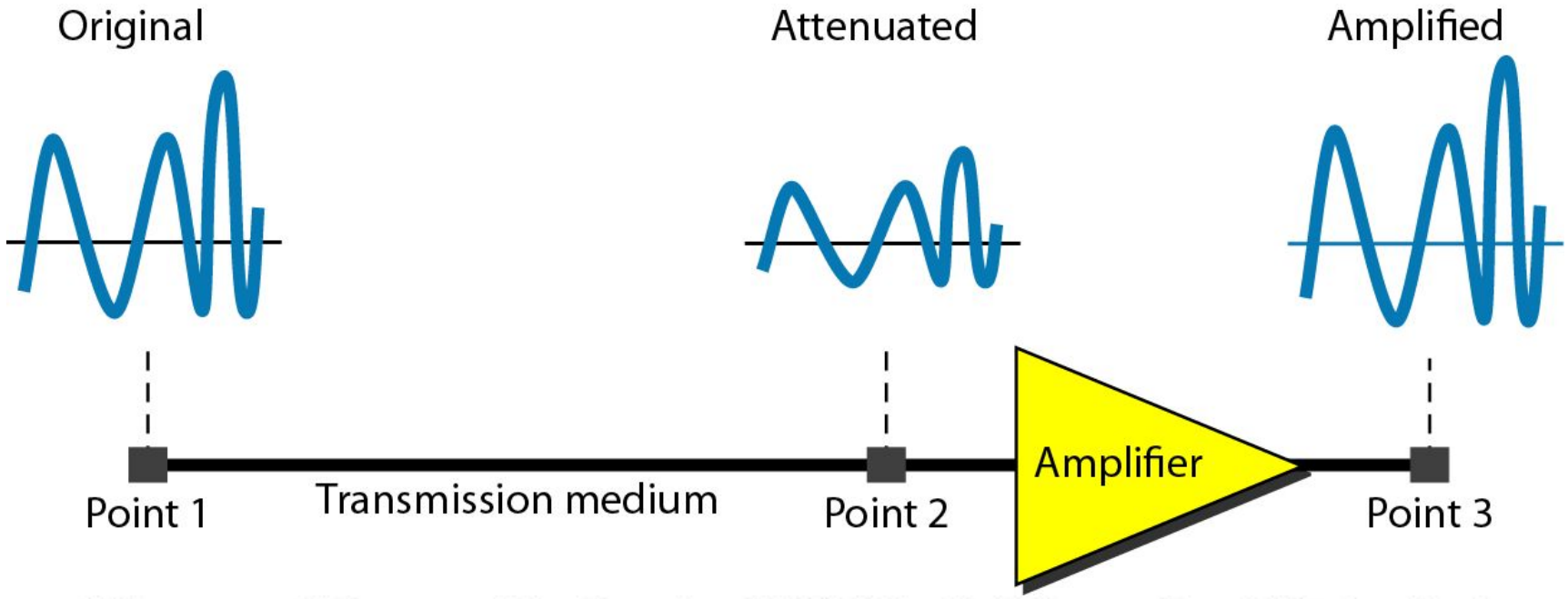
- Signals travel through transmission media, which are not perfect. The imperfection causes signal impairment.
- This means that the signal at the beginning of the medium is not the same as the signal at the end of the medium. What is sent is not what is received.
- Three causes of impairment are attenuation, distortion, and noise.



Attenuation

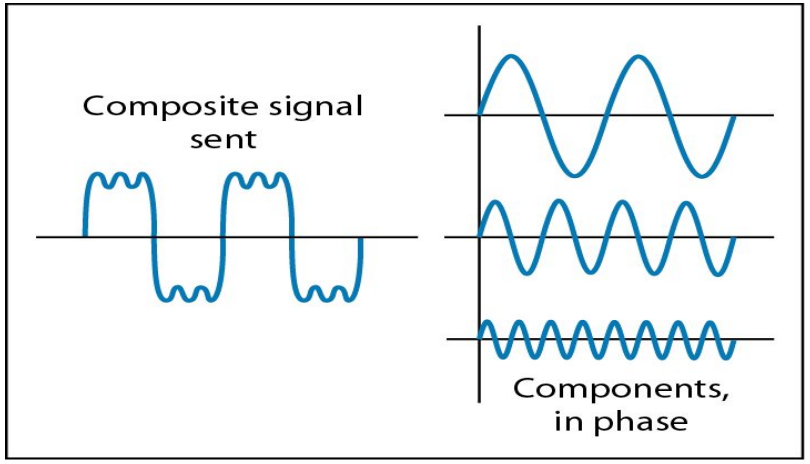
Attenuation means a **loss of energy**. When a signal, simple or composite, travels through a medium, it loses some of its energy in overcoming the resistance of the medium.

That is why a wire carrying electric signals gets warm, if not hot, after a while. Some of the electrical energy in the signal is converted to heat.

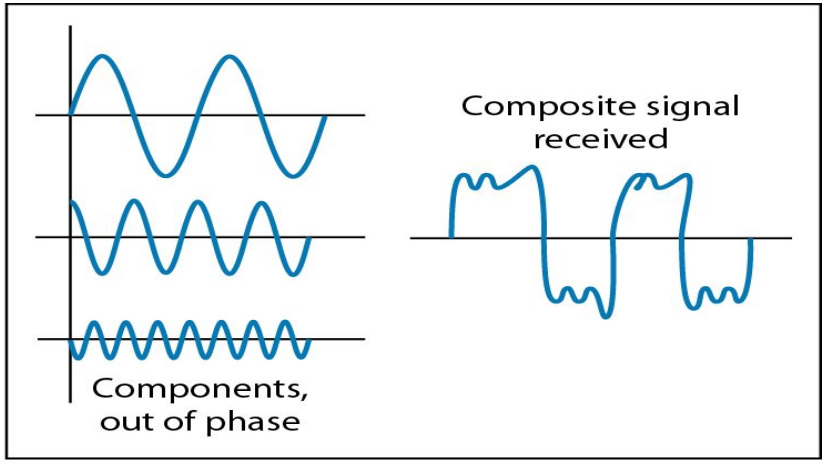


Distortion

Distortion means that the signal changes its form or shape.
Distortion can occur in a **composite signal** made of **different frequencies**.
Each signal component has its own propagation speed through a medium and, therefore, its own delay in arriving at the final destination.
Differences in delay may create a difference in phase if the delay is not exactly the same as the period duration.



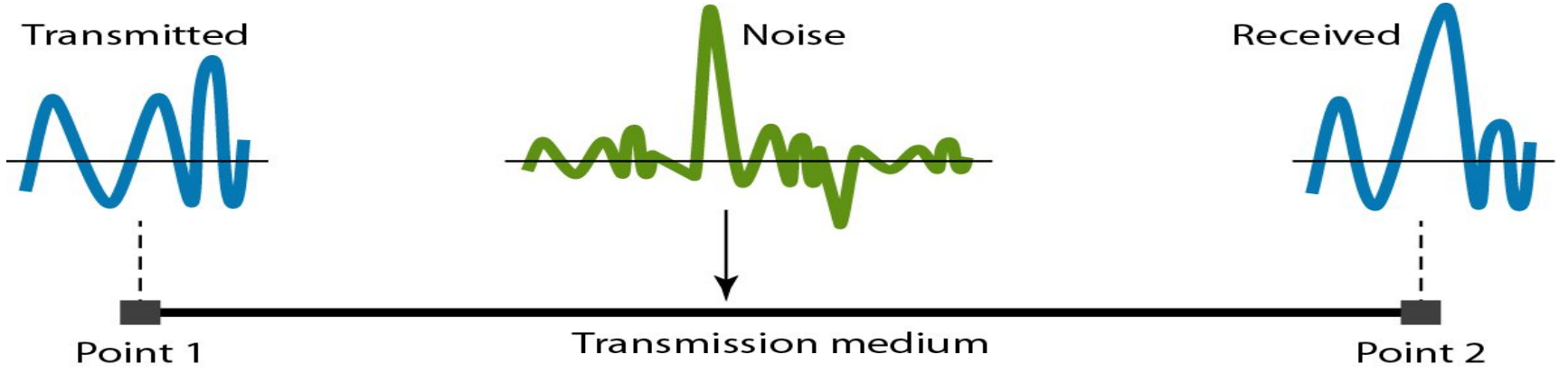
At the sender



At the receiver

Noise

- Thermal noise, induced noise, crosstalk, and impulse noise
- **Thermal noise** is the random motion of electrons in a wire which creates an extra signal not originally sent by the transmitter
- **Induced noise** comes from sources such as motors and appliances
- **Crosstalk** is the effect of one wire on the other. One wire acts as a sending antenna and the other as the receiving antenna
- **Impulse noise** is a spike (a signal with high energy in a very short time) that comes from power lines, lightning, and so on



Q. No.	Question	CO
1	Define Computer Network? Explain the uses of computer networks.	CO1
2	Explain characteristic and components of data communication	CO1
3	How network hardware and network software are classified based upon transmission technology and scale? explain in detail	CO1
4	Enlist & Explain different network devices used at different layers of OSI model	CO1
5	Enlist and explain the design issues for the layers.	CO1
6	Enlist and explain connection-oriented service primitives	CO1
7	Differentiate between connection oriented and connection less services	CO1
8	Explain OSI reference model with neat diagram	CO1
9	Explain TCP/IP reference model with neat diagram	CO1
10	Differentiate between OSI reference model and TCP/IP reference model	CO1
11	Categorize the following to one or more layers of OSI reference model along with justification 1. Transmission of bit stream across physical medium 2. Error control ad retransmission 3. Reliable process to process message delivery 4. Define frames 5. Route selection 6. Provides user services such as Email and file transfer	CO1
12	Explain the relationship of services to protocols	CO1
13	What is data communication? Explain various types of signals	CO1
14	What do you mean by transmission Impairments? explain causes of it	CO1
15	Enlist & Explain different network connecting devices	CO1

References

- Client Server Programming - Slide Figures/quotes from Andrew Tanenbaum Computer Networks book