BCSE308L - Computer Networks

Dr.S.Thamizharasan
Assistant Professor Gr.2
Department of IoT, SCOPE
Vellore Institute of Technology
thamizharasan.s@vit.ac.in

Overview I

Course Information

BCSE308L	Computer Networks	L	T	P	C
		3	0	0	3
Pre-requisite	NIL	Syllabus version			
		1.0			

Course Objective

Course Objectives
1. To build an understanding among students about the fundamental concepts of computer networking, protocols, architectures, and applications.
2. To help students to acquire knowledge in design, implement and analyze performance of OSI and TCP-IP based Architectures.
3. To identify the suitable application layer protocols for specific applications and its respective security mechanisms.

Course Outcomes

Course Outcomes
On completion of this course, student should be able to: 1. Interpret the different building blocks of Communication network and its architecture. 2. Contrast different types of switching networks and analyze the performance of network 3. Identify and analyze error and flow control mechanisms in data link layer. 4. Design sub-netting and analyze the performance of network layer with various routing protocols. 5. Compare various congestion control mechanisms and identify appropriate transport layer protocol for real time applications with appropriate security mechanism.

Module 1

Module:1	Networking Principles and Layered Architecture	6 hours
Data Communications and Networking: A Communications Model – Data Communications - Evolution of network, Requirements , Applications, Network Topology (Line configuration, Data Flow), Protocols and Standards, Network Models (OSI, TCP/IP)		

Module 2

Module:2	Circuit and Packet Switching	7 hours
Switched Communications Networks – Circuit Switching – Packet Switching – Comparison of Circuit Switching and Packet Switching – Implementing Network Software, Networking Parameters(Transmission Impairment, Data Rate and Performance)		

Module 3

Module:3	Data Link Layer	8 hours
Error Detection and Correction – Hamming Code , CRC, Checksum- Flow control mechanism – Sliding Window Protocol - GoBack - N - Selective Repeat - Multiple access Aloha - Slotted Aloha - CSMA, CSMA/CD – IEEE Standards(IEEE802.3 (Ethernet), IEEE802.11(WLAN))- RFID- Bluetooth Standards		

Module 4

Module:4	Network Layer	8 hours
IPV4 Address Space – Notations – Classful Addressing – Classless Addressing – Network Address Translation – IPv6 Address Structure – IPv4 and IPv6 header format		

Module 5

Module:5	Routing Protocols	6 hours
Routing-Link State and Distance Vector Routing Protocols- Implementation-Performance Analysis- Packet Tracer		

Module 6

Module:6	Transport Layer	5 hours
TCP and UDP-Congestion Control-Effects of Congestion-Traffic Management-TCP Congestion Control-Congestion Avoidance Mechanisms-Queuing Mechanisms-QoS Parameters		

Module 7

Module:7	**Application layer**	**3 hours**
Application layer-Domain Name System-Case Study : FTP-HTTP-SMTP-SNMP		
Module:8	**Contemporary Issues**	**2 hours**

Text and Reference Books

Text Book	
1.	Behrouz A. Forouzan, Data communication and Networking, 5th Edition, 2017

Reference Books	
1.	James F. Kurose and Keith W.Ross, Computer Networking: A Top-Down Approach, 6th Edition, 2017, Pearson Education.
2.	William Stallings, "Data and Computer Communication", 10th Edition, 2017, Pearson, United Kingdom.

Module 1
Networking Principles and Layered Architecture

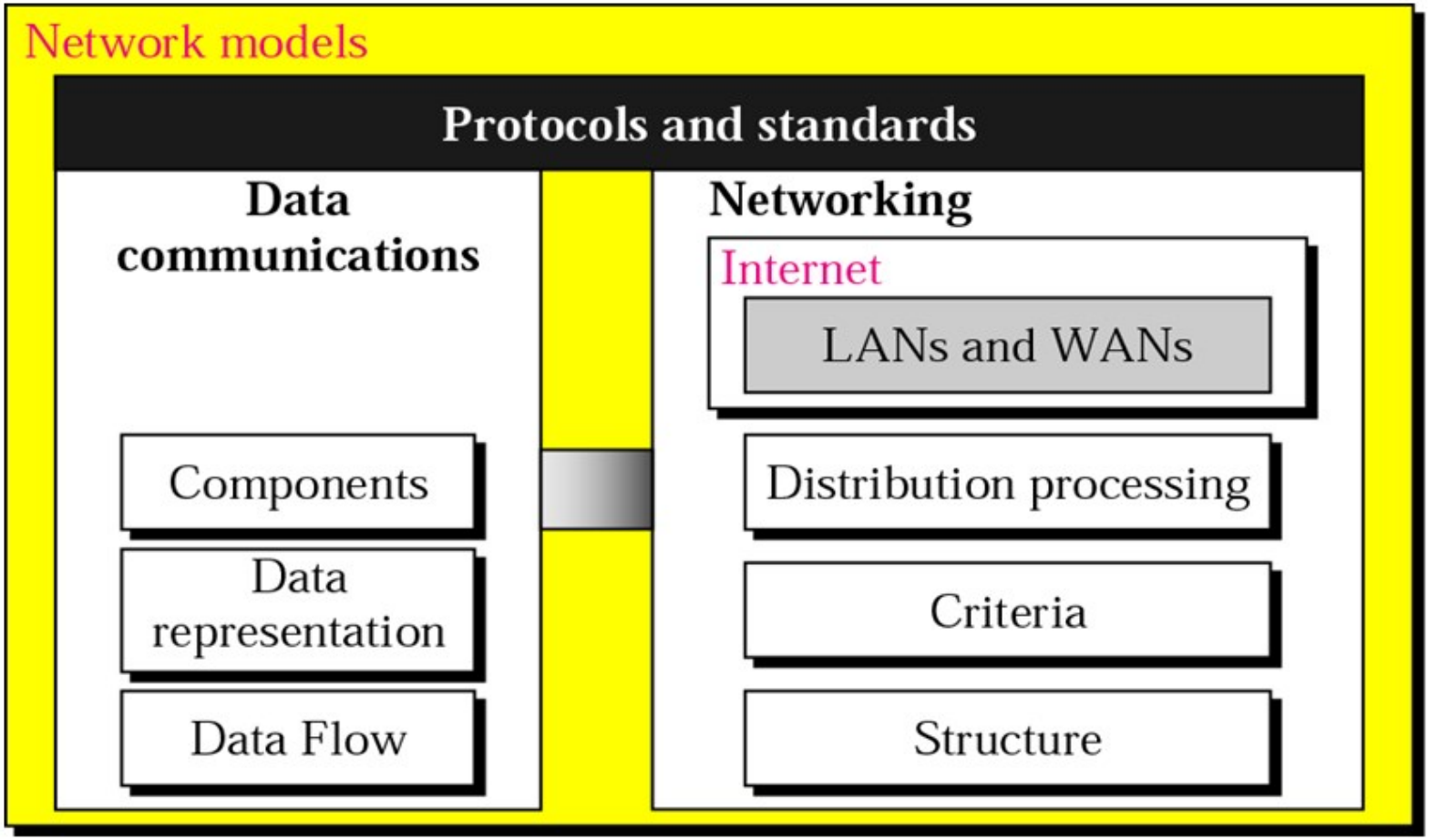
Data Communications and Networking

- Definition: Data communication is the exchange of data between two devices via some form of transmission medium such as a wired or wireless medium.

Data Communications and Networking

- Definition: Data communication is the exchange of data between two devices via some form of transmission medium such as a wired or wireless medium.
- For data communications to occur;
  The communicating devices must be part of a communication system made up of a combination of hardware (physical equipment) and software (programs).

Data Communications and Networking



Data Communications and Networking

- Data Communication:
  Effectiveness of data communication system depends on four fundamental characteristics:

Data Communications and Networking

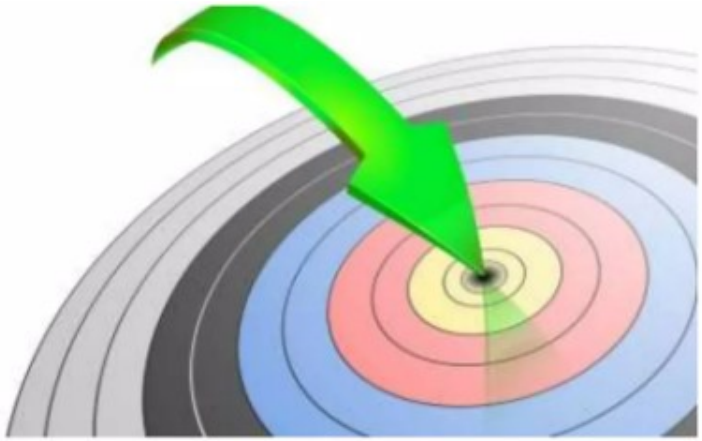
- Data Communication:
  Effectiveness of data communication system depends on four fundamental characteristics:
  - Delivery
  - Accuracy
  - Timeliness
  - Jitter

Data Communications and Networking

- Delivery:
  - System must deliver data to the correct destination.
  - Data must be received only by the intended device or user.

Data Communications and Networking

- Accuracy:
  - System must deliver the data accurately.
  - Data that have been altered in transmission and left uncorrected are unusable.



Accuracy

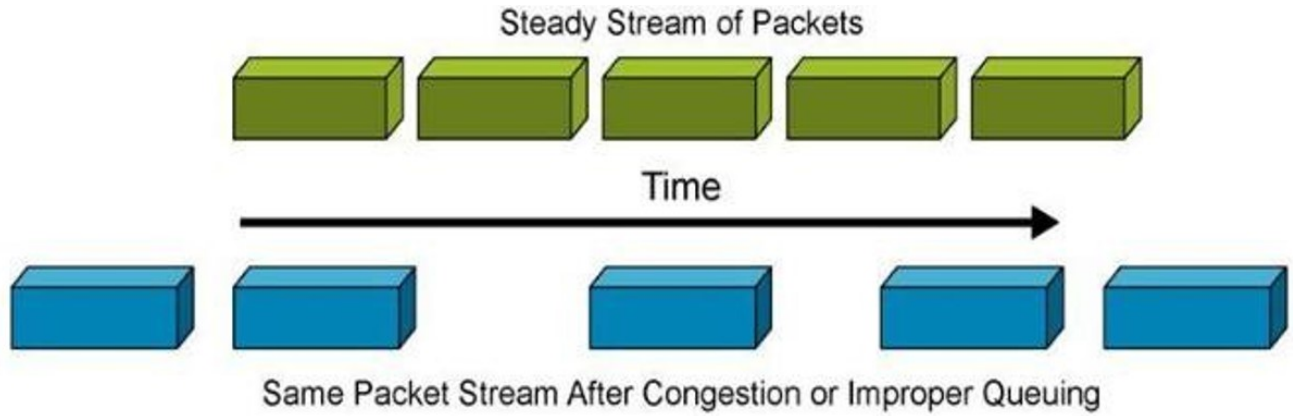
Data Communications and Networking

- Timeliness:
  - System must deliver data in a timely manner.
  - Data delivered late are useless.
  - For example, Real-time transmission.
    video and audio - deliver it in the same order that they are produced, and without significant delay.

Timeliness

Data Communications and Networking

- Jitter: variation in the packet arrival time
  - It is the uneven delay in the delivery of audio or video packets.
  - Caused by network congestion and packet loss.



Components of Data Communication System

- Message:
  - Information (data) to be communicated.
  - Example: text, numbers, pictures, audio, and video.

Components of Data Communication System

- Message:
  - Information (data) to be communicated.
  - Example: text, numbers, pictures, audio, and video.
- Sender:
  - Device that sends the data message.
  - Example: computer, workstation, telephone handset, video camera, and so on.

Components of Data Communication System

- Message:
  - Information (data) to be communicated.
  - Example: text, numbers, pictures, audio, and video.
- Sender:
  - Device that sends the data message.
  - Example: computer, workstation, telephone handset, video camera, and so on.
- Receiver:
  - Device that receives the message.
  - Example: computer, workstation, telephone handset, television, and so on.

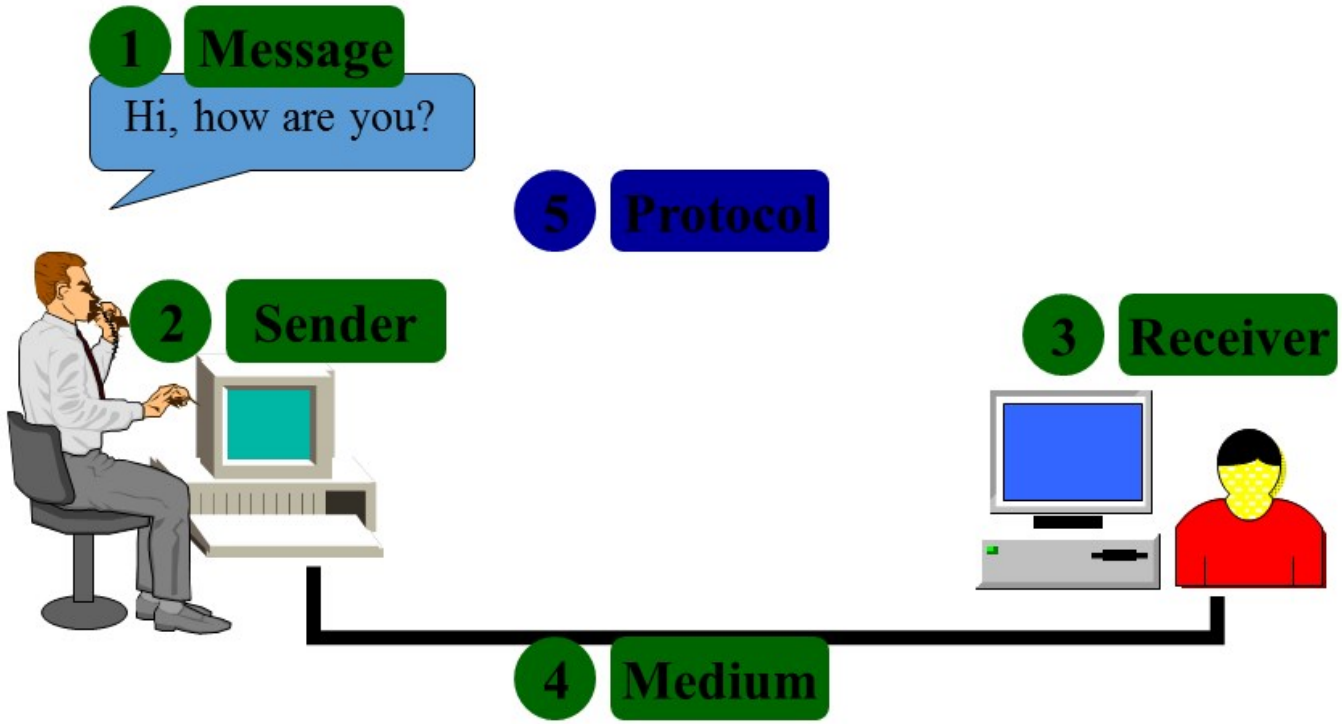
Components of Data Communication System

- Message:
  - Information (data) to be communicated.
  - Example: text, numbers, pictures, audio, and video.
- Sender:
  - Device that sends the data message.
  - Example: computer, workstation, telephone handset, video camera, and so on.
- Receiver:
  - Device that receives the message.
  - Example: computer, workstation, telephone handset, television, and so on.
- Transmission medium:
  - physical path by which a message travels from sender to receiver.
  - Examples: twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.

Components of Data Communication System

- Message:
  - Information (data) to be communicated.
  - Example: text, numbers, pictures, audio, and video.
- Sender:
  - Device that sends the data message.
  - Example: computer, workstation, telephone handset, video camera, and so on.
- Receiver:
  - Device that receives the message.
  - Example: computer, workstation, telephone handset, television, and so on.
- Transmission medium:
  - physical path by which a message travels from sender to receiver.
  - Examples: twisted-pair wire, coaxial cable, fiber-optic cable, and radio waves.
- Protocol:
  - a set of rules that govern data communications.
  - It represents an agreement between the communicating devices.
  - Example: a person speaking French cannot be understood by a person who speaks only Japanese

Components of Data Communication System



Data Representation

- Data Representation: Information comes in different forms such as text, numbers, images, audio and video.

Data Representation

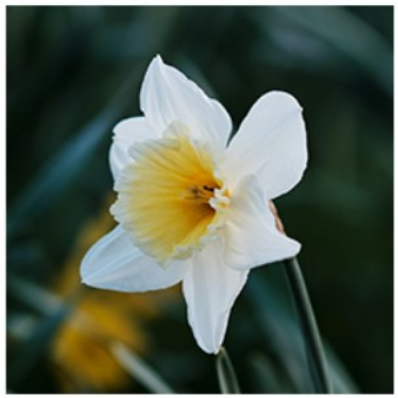
- Data Representation: Information comes in different forms such as text, numbers, images, audio and video.
- Text:
  - Represented as a bit pattern, a sequence of bits (0s or 1s).
  - Different sets of bit patterns have been designed to represent text symbols.
  - Each set is called a code.
  - Process of representing symbols is called coding.
  - ASCII (American Standard Code for Information Interchange) - 8 bits to represent a symbol or character used in any language in the world.

Data Representation

- Data Representation: Information comes in different forms such as text, numbers, images, audio and video.
- Text:
  - Represented as a bit pattern, a sequence of bits (0s or 1s).
  - Different sets of bit patterns have been designed to represent text symbols.
  - Each set is called a code.
  - Process of representing symbols is called coding.
  - ASCII (American Standard Code for Information Interchange) - 8 bits to represent a symbol or character used in any language in the world.
- Numbers:
  - Represented by bit patterns.
  - ASCII is not used to represent numbers.
  - The number is directly converted to a binary number to simplify mathematical operations.

Data Representation

- Images:
  - Represented by bit patterns.
  - Composed of a matrix of pixels.
  - Each pixel is a small dot and each pixel assigned a bit pattern.
  - Resolution depends on size of the pixel.
  - The number of bits used to represent each pixel in an image is termed as bit depth.
  - More memory is needed for better resolution.
    That is, image can be divided into 1000 pixels or 10,000 pixels.



Data Representation

- Audio:
  - Refers to recording or broadcasting of sound or music.
  - It is continuous, not discrete.

Data Representation

- Video:
  - Refers to recording or broadcasting of a picture or movie.
  - Video can either be produced as a continuous entity or it can be a combination of images, each a discrete entity, arranged to convey the idea of motion.

Data Flow

- Communication between two devices can be:
  (1) Simplex
  (2) Half-Duplex
  (3) Full-Duplex

Data Flow

- Communication between two devices can be:
  (1) Simplex
  (2) Half-Duplex
  (3) Full-Duplex

- Simplex: In simplex mode, the communication is unidirectional.
  - Communication between sender and receiver occurs in only one direction.
  - Only sender can send the data and receiver can receive the data.
  - Receiver cannot reply to the sender.
  - Use the entire capacity of the channel to send data
  - Example: Keyboards and monitors are examples of simplex devices. Here, the keyboard can only give input; the monitor can only accept output.

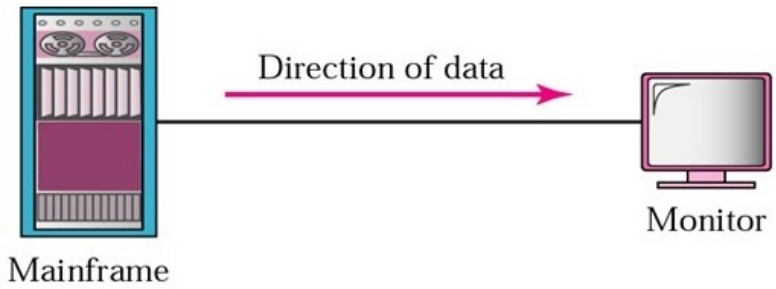


Figure 1 : Simplex communication

Data Flow

- Half-Duplex: In half-duplex mode, each station can both transmit and receive, but not at the same time.
  - When one device is sending, the other can only receive, and vice versa.
  - The half-duplex mode is used in cases where there is no need for communication in both directions at the same time.
  - Entire capacity of a channel is taken over by the transmitting device.
  - Example: Walkie-talkie

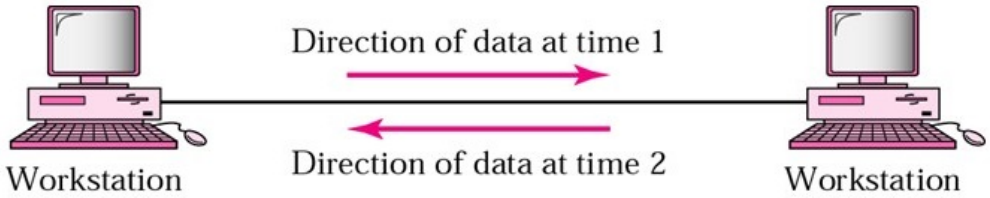


Figure 2 : Half-Duplex communication

Data Flow

- Full-Duplex: In full-duplex, both stations can transmit and receive simultaneously.
  - Signals going in either direction sharing the capacity of the link.
  - Sharing can occur in two ways;
    (1) Link has two physically separate transmission paths, one for sending and other for receiving.
    (2) Capacity of the channel is divided between signals travelling in both directions.
  - Example: telephone network.

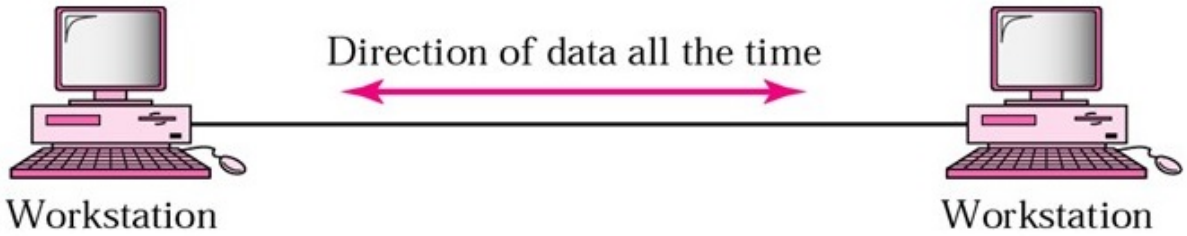


Figure 3 : Full-Duplex communication

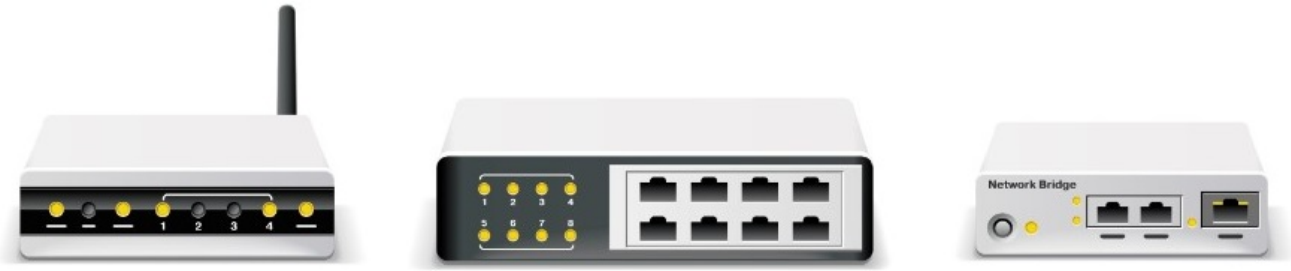
Computer Networks

Networks

- A Network is a set of devices(nodes) connected by communication links.
- A node can be a computer, printer or any other device capable of sending or receiving data generated by other nodes on the network.
- A link can be a cable, air, optical fiber, or any medium which can transport a signal carrying information.

Networks

- Device can also be a connecting device;
  - Router, which connects the network to other networks
  - Switch, which connects devices together
  - Modem (modulator-demodulator), which changes the form of data.



Networks

- Network Criteria: A network must be able to meet a certain number of criteria;
  - Performance
  - Reliability
  - Security

Networks

- Performance: Measured in many ways, including transit and response time.
  - Transit time: Amount of time required for a message to travel from one device to another.
  - Response time: Elapsed time between an inquiry and beginning of a response

Networks

- Performance: It is also evaluated by
  - Throughput (high)
  - Delay (low)
- Contradictory: If we try to send more data to the network, we may increase throughput but we increase the delay because of traffic congestion in the network.

Networks

- Performance of a network also depends on a number of factors
  - Number of users
  - Type of transmission medium
  - Capabilities of the connected hardware
  - Efficiency of the software.

Networks

- Reliability: It is measured by
  - Frequency of failure
  - Time it takes a link to recover from a failure
  - Network robustness

Networks

- Security: Network security issues include
  - Protecting data from unauthorized access
  - Protecting data from damage
  - Implementing policies and procedures for recovery from breaches and data losses.

Network Elements

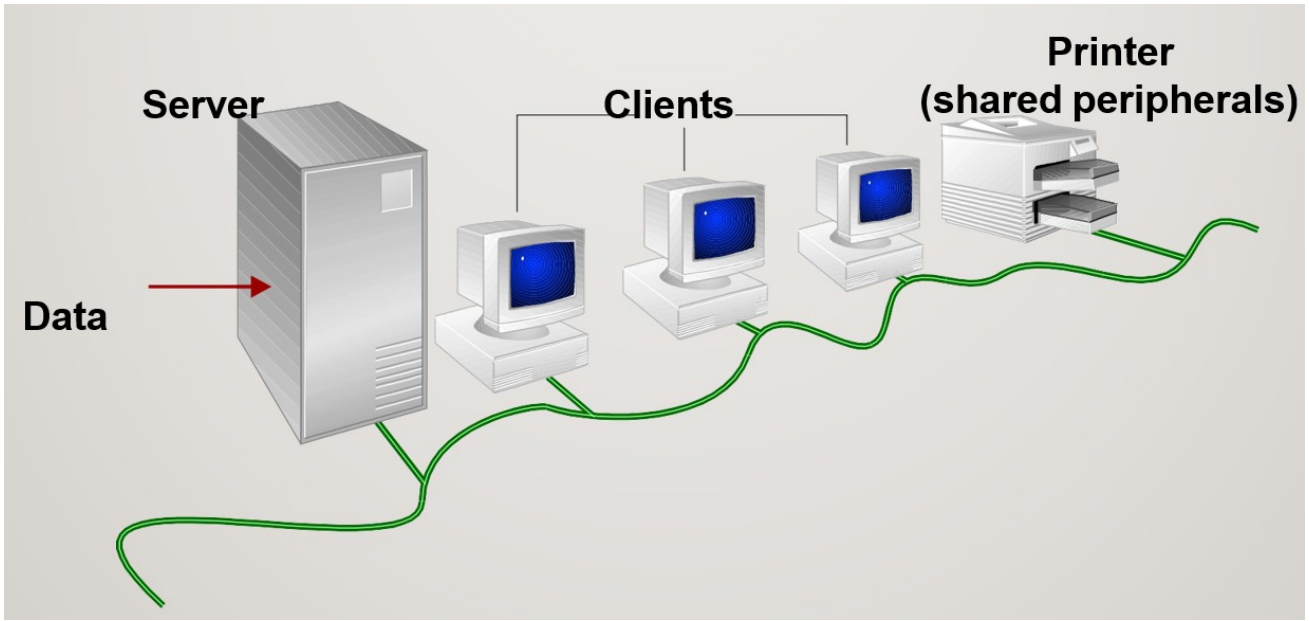
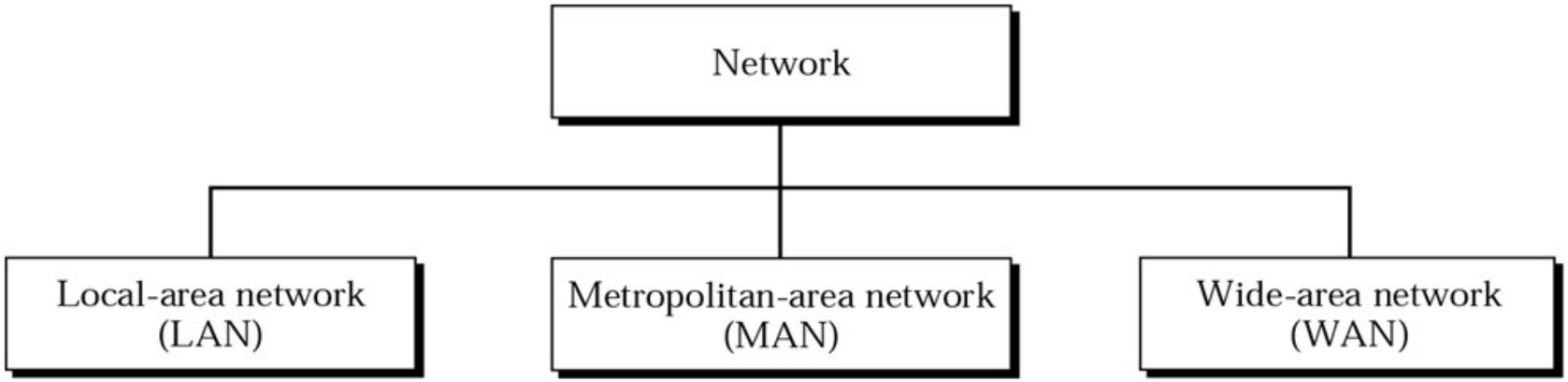


Figure 4 : Common Network Elements

Networks


Network
Local-area network (LAN)
Metropolitan-area network (MAN)
Wide-area network (WAN)

- Application of Networks
  - Financial Services, ex: online Banking

- Application of Networks
  - Financial Services, ex: online Banking
  - Electronic Messaging, ex: E-mail

- Application of Networks
  - Financial Services, ex: online Banking
  - Electronic Messaging, ex: E-mail
  - Directory Services, ex: Centralized database

- Application of Networks
  - Financial Services, ex: online Banking
  - Electronic Messaging, ex: E-mail
  - Directory Services, ex: Centralized database
  - Information Services, ex: Bulletin boards

- Application of Networks
  - Financial Services, ex: online Banking
  - Electronic Messaging, ex: E-mail
  - Directory Services, ex: Centralized database
  - Information Services, ex: Bulletin boards
  - Teleconference, ex: Voice conferencing

- Application of Networks
  - Financial Services, ex: online Banking
  - Electronic Messaging, ex: E-mail
  - Directory Services, ex: Centralized database
  - Information Services, ex: Bulletin boards
  - Teleconference, ex: Voice conferencing
  - Cellular Telephone, ex: Mobile phone communication

- Application of Networks
  - Financial Services, ex: online Banking
  - Electronic Messaging, ex: E-mail
  - Directory Services, ex: Centralized database
  - Information Services, ex: Bulletin boards
  - Teleconference, ex: Voice conferencing
  - Cellular Telephone, ex: Mobile phone communication
  - Cable Television, ex: Video on Request.

- Application of Networks
  - Financial Services, ex: online Banking
  - Electronic Messaging, ex: E-mail
  - Directory Services, ex: Centralized database
  - Information Services, ex: Bulletin boards
  - Teleconference, ex: Voice conferencing
  - Cellular Telephone, ex: Mobile phone communication
  - Cable Television, ex: Video on Request.
  - Marketing and sales, ex: online reservation of Hotels

Physical Structures

- Type of Connection:
  Point to Point - single transmitter and receiver
  Multipoint - multiple recipients of single transmission
- Physical Topology:
  Connection of devices
  Type of transmission - unicast, mulitcast, broadcast

Types of Connection

- Point to Point: A dedicated link is provided between two devices.

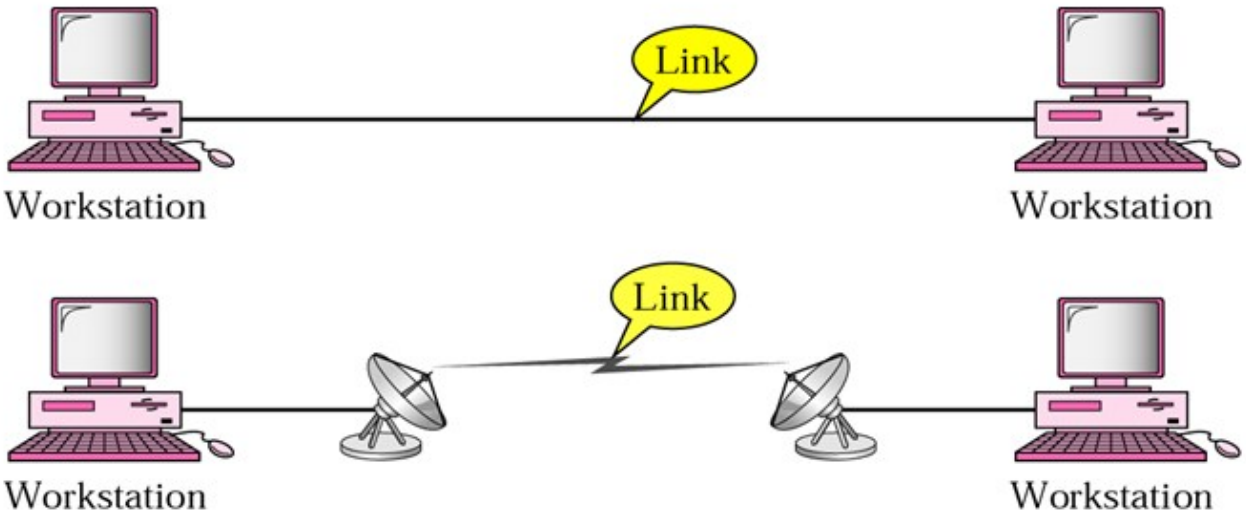


Figure 5 : Point to Point connection

Types of Connection

- Multipoint: More than two specific devices share a single link.

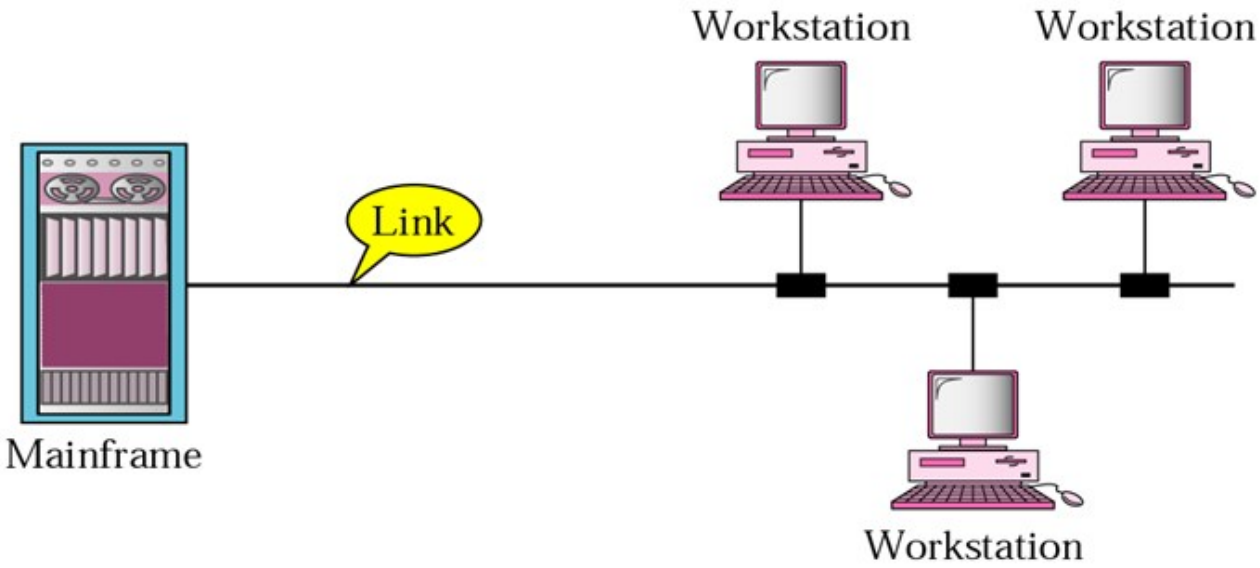


Figure 6 : Multipoint connection

Categories of Topology

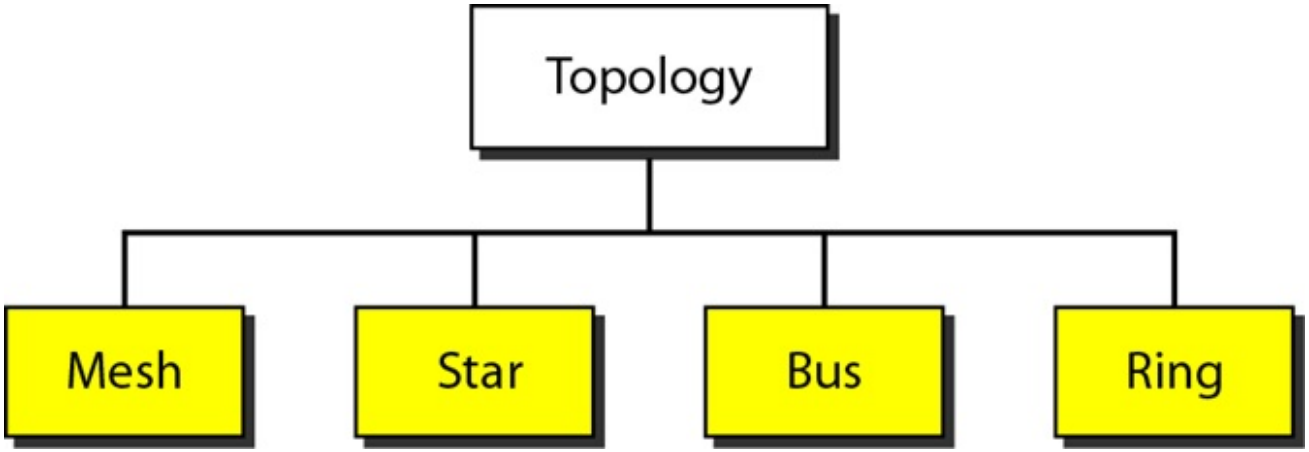


Figure 7 : Categories of Topology

Categories of Topology

- Mesh Topology: Every link is dedicated point-to-point link.
- The dedicated link carries traffic only between the two devices it connects.

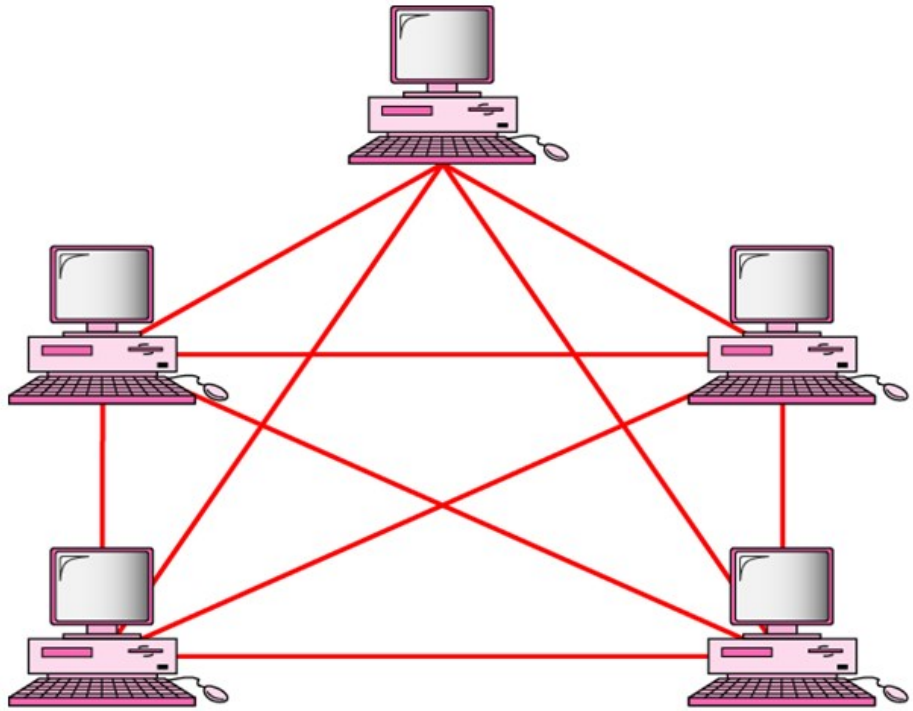


Figure 8 : Mesh Topology

Categories of Topology

- Mesh Topology:
  - To connect n number of nodes, each node must be connected to $n-1$ nodes. That is, we need $\frac{n(n-1)}{2}$ duplex mode links.
  - To accommodate that many links, every device must have $n-1$ input/output (I/O) ports to be connected to the other $n-1$ stations.
- For example, if 8 devices in mesh, then
  Number of links $= \frac{8(8-1)}{2} = 28$
  Number of ports per device = 8 - 1 = 7

Categories of Topology

- Examples:
  - Connection of telephone regional offices
    In which each regional office needs to be connected to every other regional office.

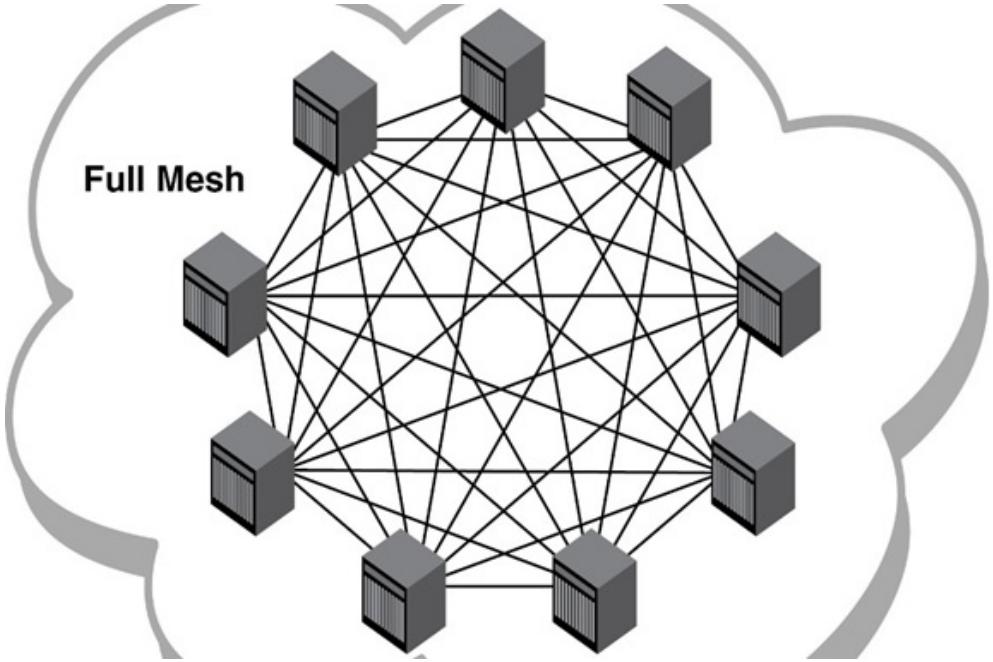


Figure 9 : Mesh Topology

Categories of Topology

- Advantages of Mesh Topology:
  - Eliminate the traffic problems.
    Each connection can carry its own data load
  - It is robust.
    If one link becomes failure, it does not weaken the entire system.
  - There is privacy
    Only the intended recipient sees the message. Prevent other users from gaining access to messages.
  - Traffic can be routed to avoid links with suspected problems.
  - Network manager discover the exact location of fault and helps in finding its cause and solution

Categories of Topology

- Disdvantages of Mesh Topology:
  - Requires more amount of cabling and number of I/O ports.
  - Installation and reconnection are difficult
  - Hardware (I/O ports and cable) can be expensive.
  - For these reasons it is implemented in a limited fashion.

Categories of Topology

- Star Topology:
  - Each device has a dedicated point-to-point link only to a central controller (hub).
  - No direct link between the devices.
  - It does not allow direct traffic between devices.
  - Controller acts as an exchange.
    If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.

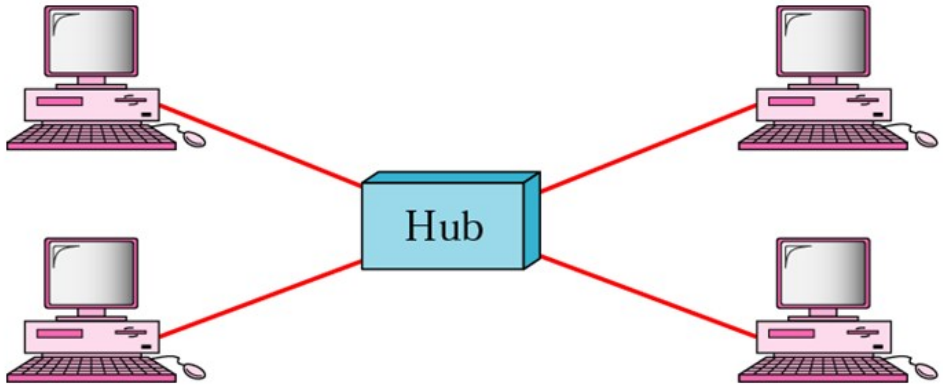


Figure 10 : Star Topology

Categories of Topology

- Advantages of Star Topology:
  - It is less expensive than a mesh topology.
  - Each device needs only one link and one I/O port.
  - It is easy to install and reconfigure.
  - Less cabling needs to be housed.
  - Easy to setup and modify
    Additions and deletions required one connection between that device and the hub
  - It is robust
    If one link fails, only that link is affected. All other links remain active.
  - Easy fault identification and fault isolation.
  - Hub can be used to monitor link problems and bypass defective links.

Categories of Topology

- Disadvantages of Star Topology:
  - If the hub goes down, the whole system is dead.
  - More cabling is required than ring or bus topologies
- Examples:
  - Used in High-speed LANs.
  - n devices are connected using n links.

Categories of Topology

- Bus Topology:
  - Multipoint configuration.
  - One long cable acts as a backbone to link all devices in a network.
  - Nodes are connected to the bus cable by drop lines and taps.
  - As a signal travels along the backbone, some of its energy is transformed into heat.
    Therefore, it becomes weaker and weaker as it travels farther and farther.
  - For this reason there is a limit on the number of taps and on the distance between those taps.

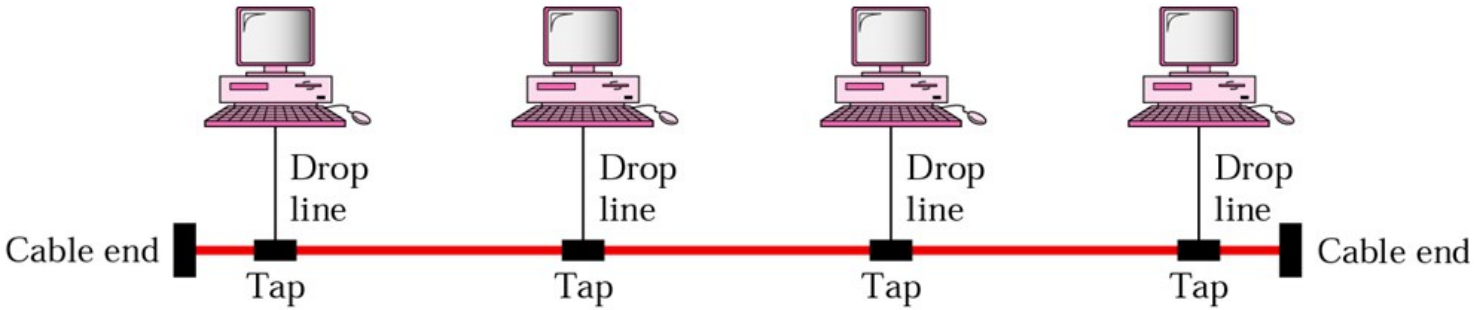


Figure 11 : Bus Topology

Categories of Topology

- Advantages of Bus Topology:
  - It is very simple to install
  - It uses less cable than other topologies.
  - It is relatively inexpensive.
  - Used in small networks.

Categories of Topology

- Advantages of Bus Topology:
  - It is very simple to install
  - It uses less cable than other topologies.
  - It is relatively inexpensive.
  - Used in small networks.

  Disadvantages of Bus Topology:
  - It is very difficult to troubleshoot.
  - It provides slow data transfer speed.
  - A single fault can bring the entire network down.

Categories of Topology

- Ring Topology:
  - Each device has a dedicated point-to-point configuration to neighbors.
  - Signal is passed from device to device until it reaches destination.
  - Signal is passed in one direction only.
  - Each device in the ring incorporates a repeater.
  - Repeater regenerates the bits and pass.

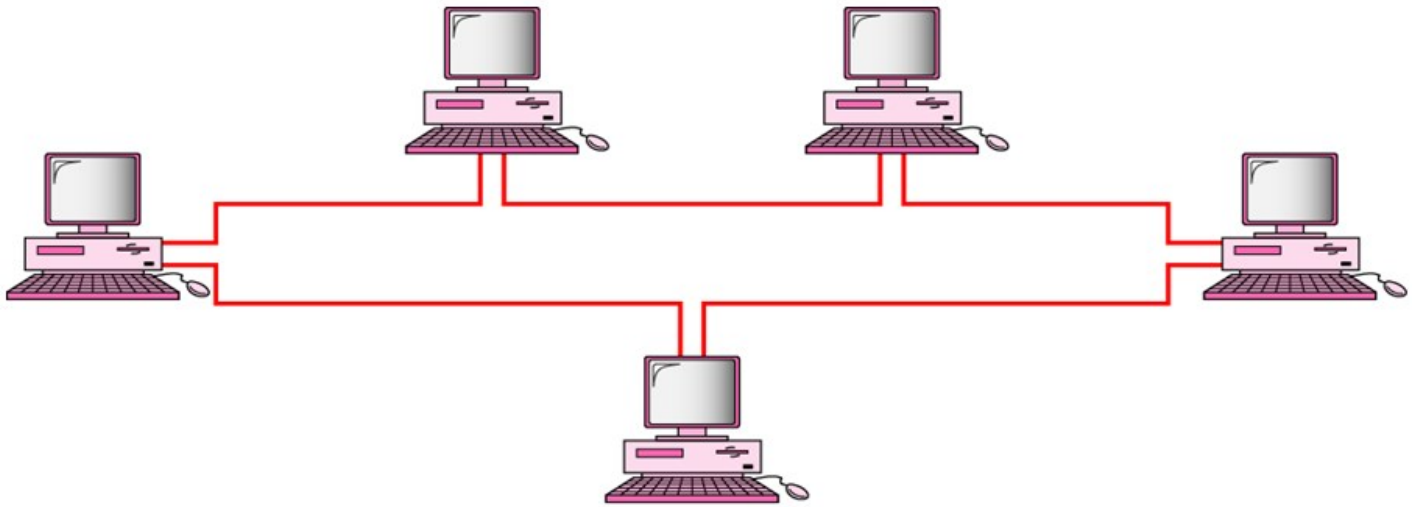


Figure 12 : Ring Topology

Categories of Topology

- Advantages of Ring Topology:
  - Easy of install and reconfigure
  - Each device is linked to only its immediate neighbors.
  - To add or delete a device, change only two connections.
  - Fault isolation is simple.
    A signal is circulating at all times. If one device does not receive a signal within a specified period, it can issue an alarm.
  - Alarm alerts the network operator to the problem and its location.

Categories of Topology

- Disadvantages of Ring Topology:
  - Unidirectional traffic.
    A break in the ring can disable the entire network.
  - This weakness can be solved by using a dual ring or a switch capable of closing off the break.
    It is used as a backup in case the primary ring fails.

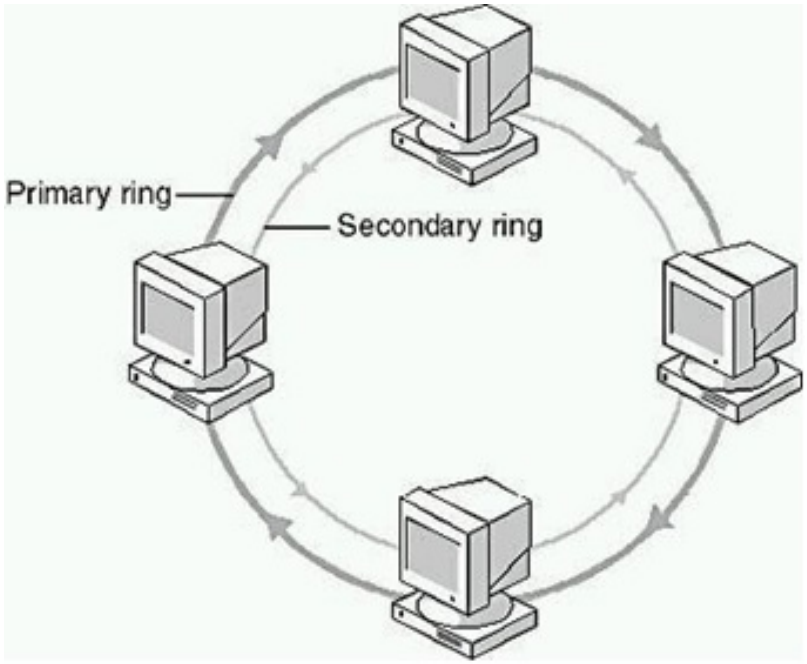


Figure 13 : Ring Topology

OSI Layers

OSI Layers

- The OSI Model: An ISO standard that covers all aspects of network communications is the Open Systems Interconnection (OSI) model.
- The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.
- The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable.

OSI Layers

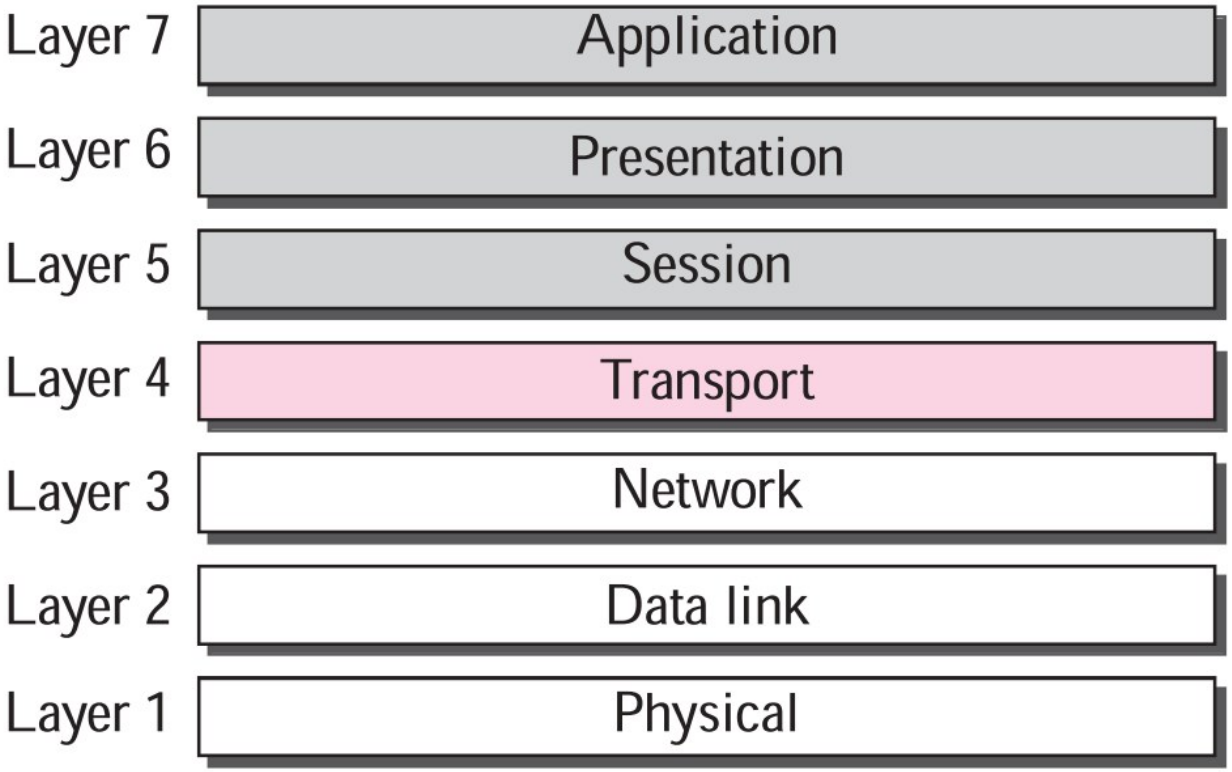
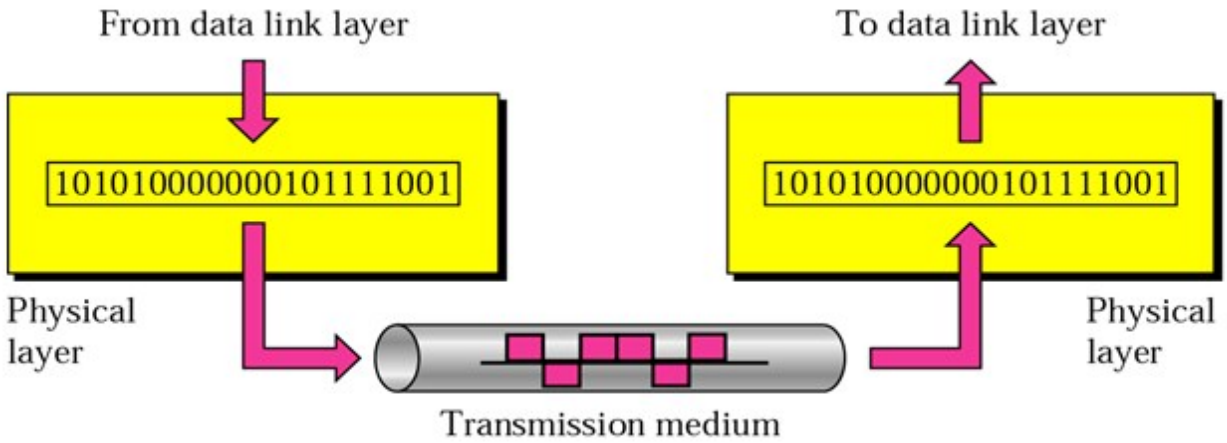


Figure 14 : The OSI model

Physical Layer

- The physical layer is the lowest layer of the Open Systems Interconnection (OSI) model of computer networking.
- It consists of the basic hardware transmission technology to move bits of data on a network.



Physical Layer

- Physical characteristics of interfaces and media: The physical layer defines the characteristics of the interface between the devices and the transmission media. It also defines the type of transmission media.

Physical Layer

- Physical characteristics of interfaces and media: The physical layer defines the characteristics of the interface between the devices and the transmission media. It also defines the type of transmission media.
- Representation of bits: The physical layer data consists of a stream of bits (sequence of 0s or 1s) with no interpretation.
  To be transmitted, bits must be encoded into signals(electrical or optical). The physical layer defines the type of encoding (how 0s and 1s are changed to signals).

Physical Layer

- Physical characteristics of interfaces and media: The physical layer defines the characteristics of the interface between the devices and the transmission media. It also defines the type of transmission media.
- Representation of bits: The physical layer data consists of a stream of bits (sequence of 0s or 1s) with no interpretation.
  To be transmitted, bits must be encoded into signals(electrical or optical). The physical layer defines the type of encoding (how 0s and 1s are changed to signals).
- Date rate: The number of bits sent each second(transmission rate).
  In other words, the physical layer defines the duration of a bit.

Physical Layer

- Synchronization of bits: The sender and receiver not only use the same bit rate but also must be synchronized at the bit level.
  In other words, the sender and the receiver clocks must be synchronized.

Physical Layer

- Synchronization of bits: The sender and receiver not only use the same bit rate but also must be synchronized at the bit level.
  In other words, the sender and the receiver clocks must be synchronized.
- Line configuration: The physical layer is concerned with the connection of devices to the media.
  In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.

Physical Layer

- Synchronization of bits: The sender and receiver not only use the same bit rate but also must be synchronized at the bit level.
  In other words, the sender and the receiver clocks must be synchronized.
- Line configuration: The physical layer is concerned with the connection of devices to the media.
  In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.
- Physical topology: The physical topology defines how devices are connected to make a network.
  Devices can be connected either by using a mesh topology, star topology, ring topology, bus topology or hybrid topology.

Physical Layer

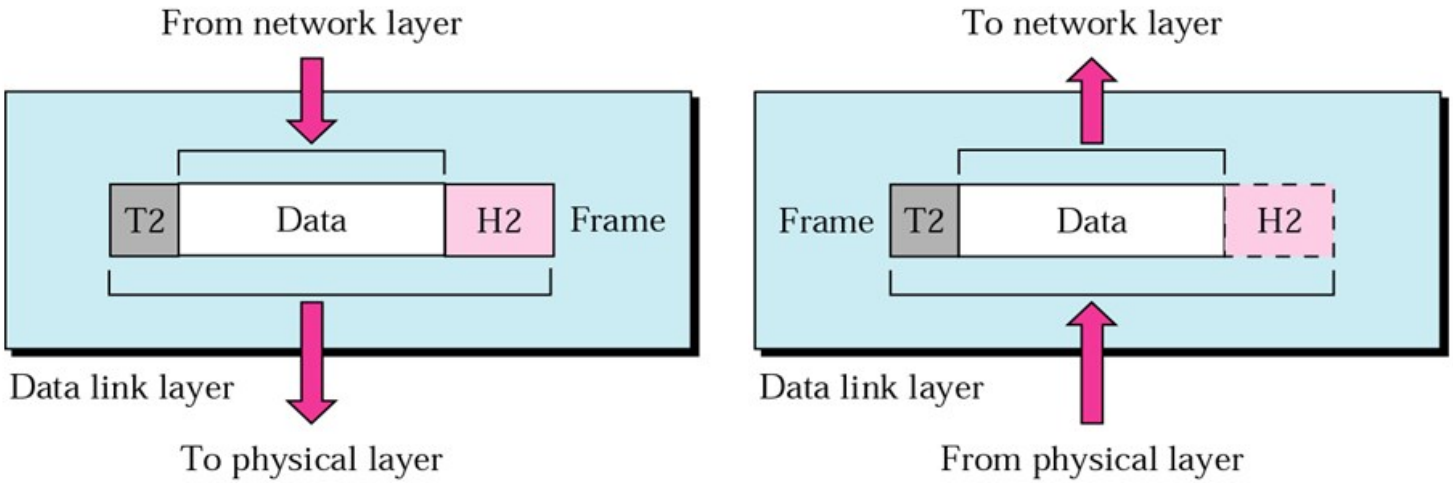
- Synchronization of bits: The sender and receiver not only use the same bit rate but also must be synchronized at the bit level.
  In other words, the sender and the receiver clocks must be synchronized.
- Line configuration: The physical layer is concerned with the connection of devices to the media.
  In a point-to-point configuration, two devices are connected through a dedicated link. In a multipoint configuration, a link is shared among several devices.
- Physical topology: The physical topology defines how devices are connected to make a network.
  Devices can be connected either by using a mesh topology, star topology, ring topology, bus topology or hybrid topology.
- Transmission mode: The physical layer also defines the direction of transmission between two devices, (i.e) simplex, half-duplex, or full-duplex.

Physical Layer

The physical layer is responsible for transmitting individual bits from one node to the next.

Data Link Layer

- The data link layer is the second lowest layer of the OSI model.
- The data link layer transforms the physical layer, to a reliable link. It makes the physical layer appear error-free to the upper layer(network layer).



Data Link Layer

- Framing: The data link layer divides the stream of bits into manageable data units called frames.

Data Link Layer

- Framing: The data link layer divides the stream of bits 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 sender and receiver of the frame.

Data Link Layer

- Framing: The data link layer divides the stream of bits 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 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 at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.

Data Link Layer

- Framing: The data link layer divides the stream of bits 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 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 at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid 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.
  Error control is normally achieved through a trailer added to the end of the frame.

Data Link Layer

- Framing: The data link layer divides the stream of bits 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 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 at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid 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.
  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.

Data Link Layer

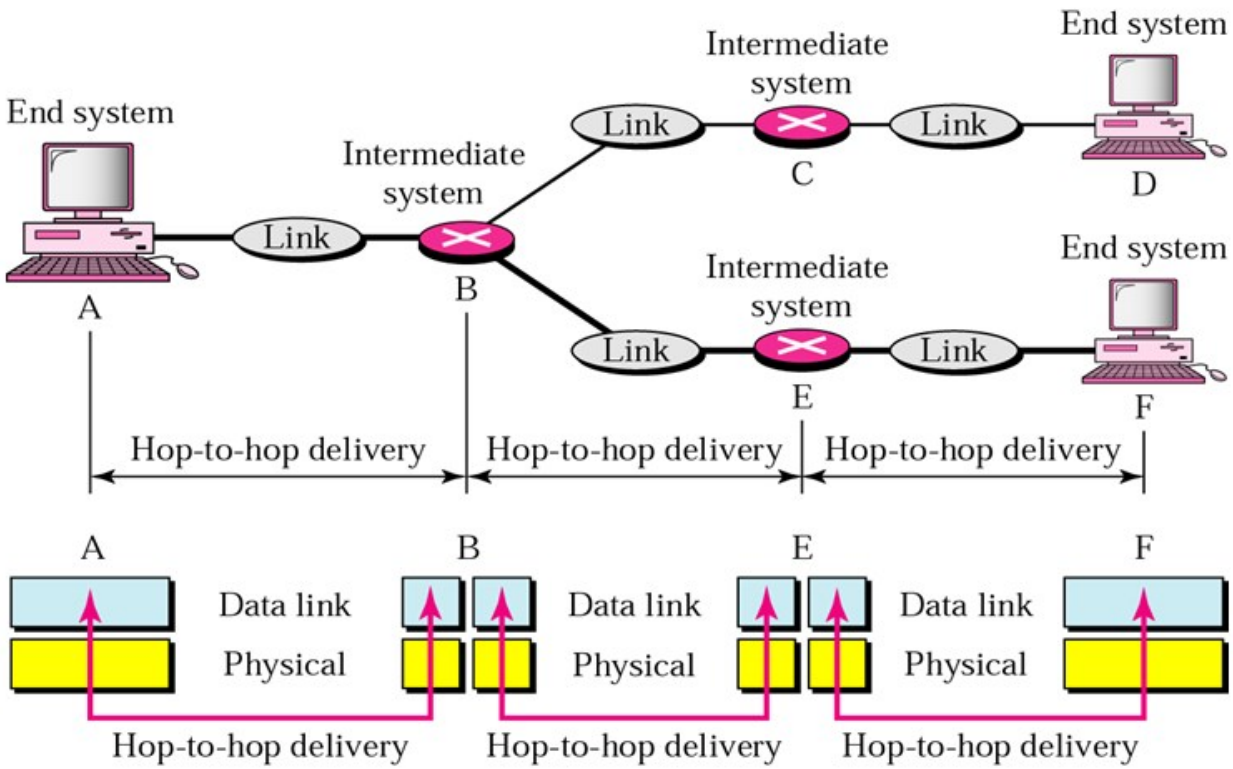


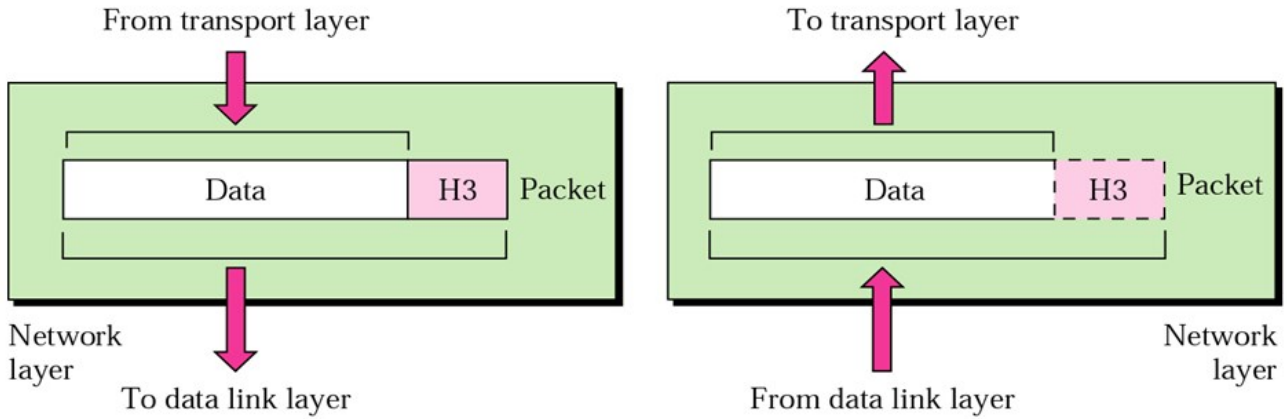
Figure 15 : Node to node delivery

Data Link Layer

The data link layer is responsible for transmitting frames from one node to the next.

Network Layer

- The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links).
  Whereas the data link layer oversees the delivery of the frames between two systems on the same network (links).
- The network layer ensures that each packet gets from its point of origin to its final destination.



Network Layer

- Packets: It is a protocol data unit utilized in the network layer.
  The source and destination MAC addresses are included in the framing.
  In contrast, the source and destination IP addresses are included in the packetization process.

Network Layer

- Packets: It is a protocol data unit utilized in the network layer.
  The source and destination MAC addresses are included in the framing.
  In contrast, the source and destination IP addresses are included in the packetization process.
- Source to destination delivery of packets: If two systems are connected to the same link, there is usually no need for a network layer. However, if the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery.

Network Layer

- Logical addressing: If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, includes the logical addresses of the sender and receiver.

Network Layer

- Logical addressing: If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, includes the logical addresses of the sender and receiver.
- Routing: When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination.

Network Layer

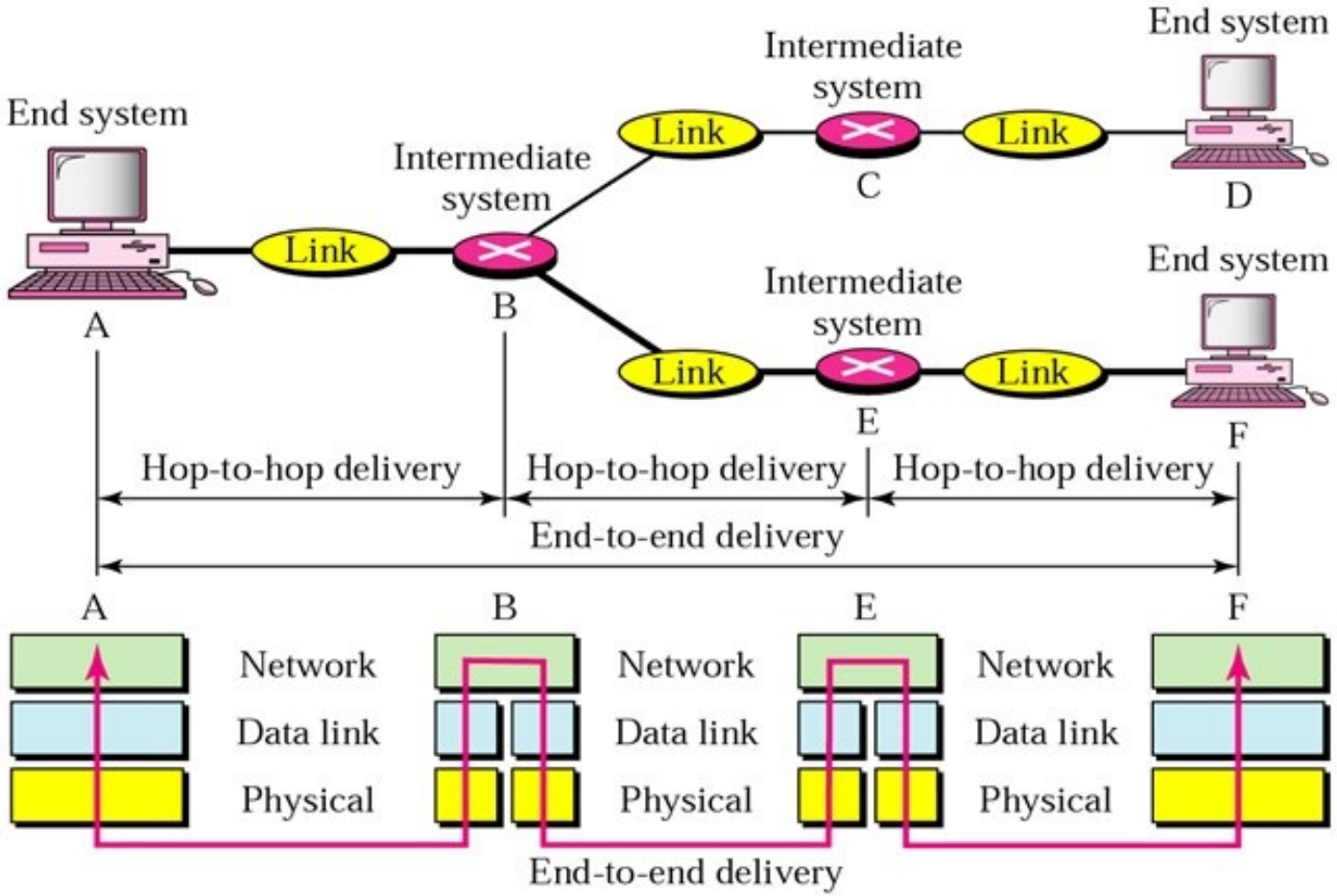


Figure 16 : Source to destination delivery

Network Layer

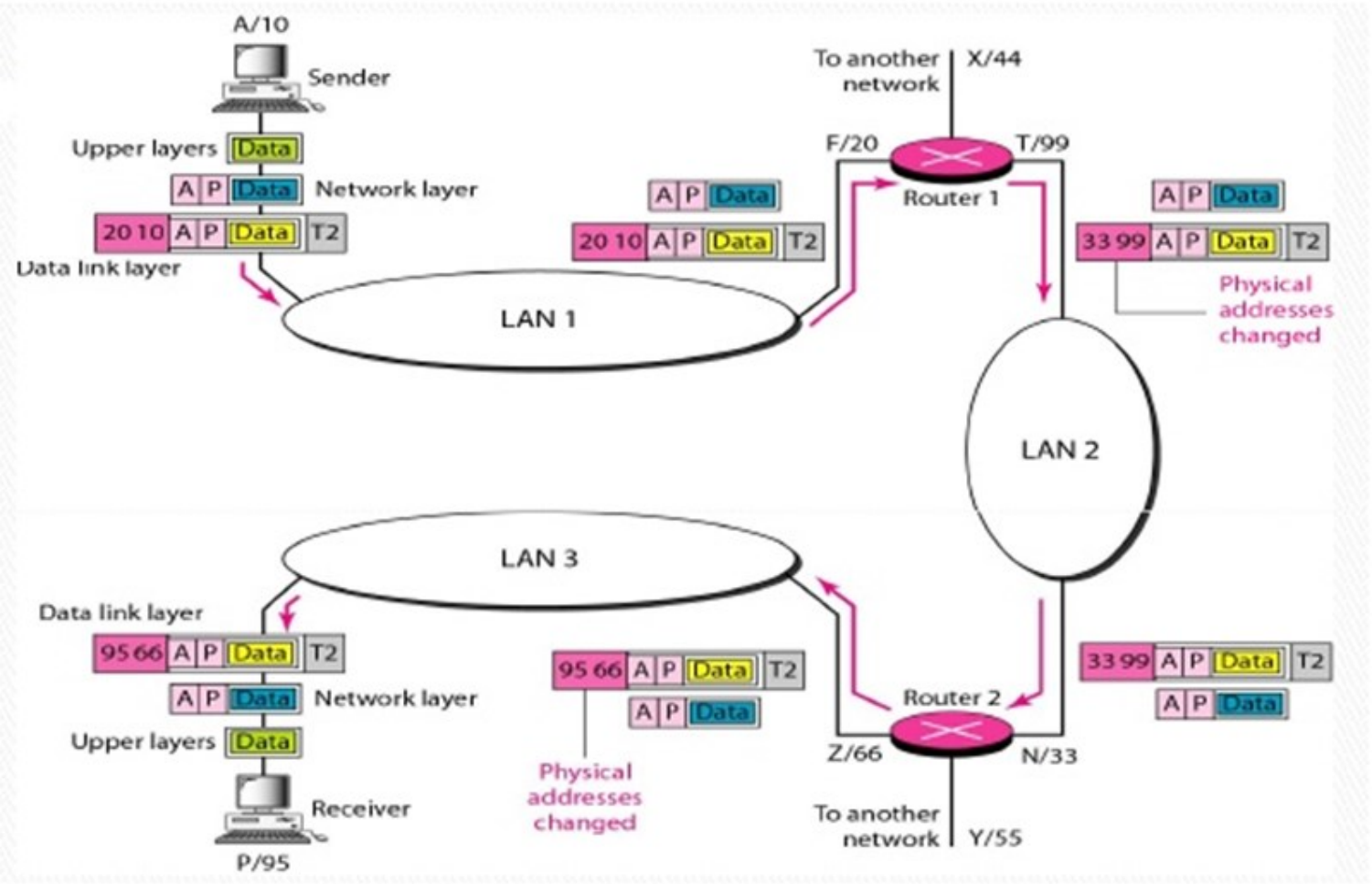


Figure 17 : Logical addressing

Network Layer

The network layer is responsible for the delivery of packets from the original source to the final destination.

Transport layer

- The transport Layer is responsible for process-to-process delivery of the entire message.
  A process is an application program running on a host.
- Whereas the network layer oversees source-to-destination delivery of individual packets, it does not recognize any relationship between those packets. It treats each one independently, as though each piece belonged to a separate message, whether or not it does.
- The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.

Transport layer

- Service-point addressing: Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a service-point address (or port address).
  The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

Transport layer

- Service-point addressing: Computers often run several programs at the same time. For this reason, source-to-destination delivery means delivery not only from one computer to the next but also from a specific process (running program) on one computer to a specific process (running program) on the other. The transport layer header must therefore include a type of address called a service-point address (or port address).
  The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.
- Segmentation and reassembly: A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.

Transport layer

- Connection control: The transport layer can be either connectionless or connection oriented.
  A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine.
  A connection-oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.

Transport layer

- Connection control: The transport layer can be either connectionless or connection oriented.
  A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine.
  A connection-oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.
- Flow control (perform end to end): Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.

Transport layer

- Connection control: The transport layer can be either connectionless or connection oriented.
  A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine.
  A connection-oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.
- Flow control (perform end to end): Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.
- Error control (perform end to end): Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to-process rather than across a single link.
  The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error(damage, loss, or duplication).

Transport layer

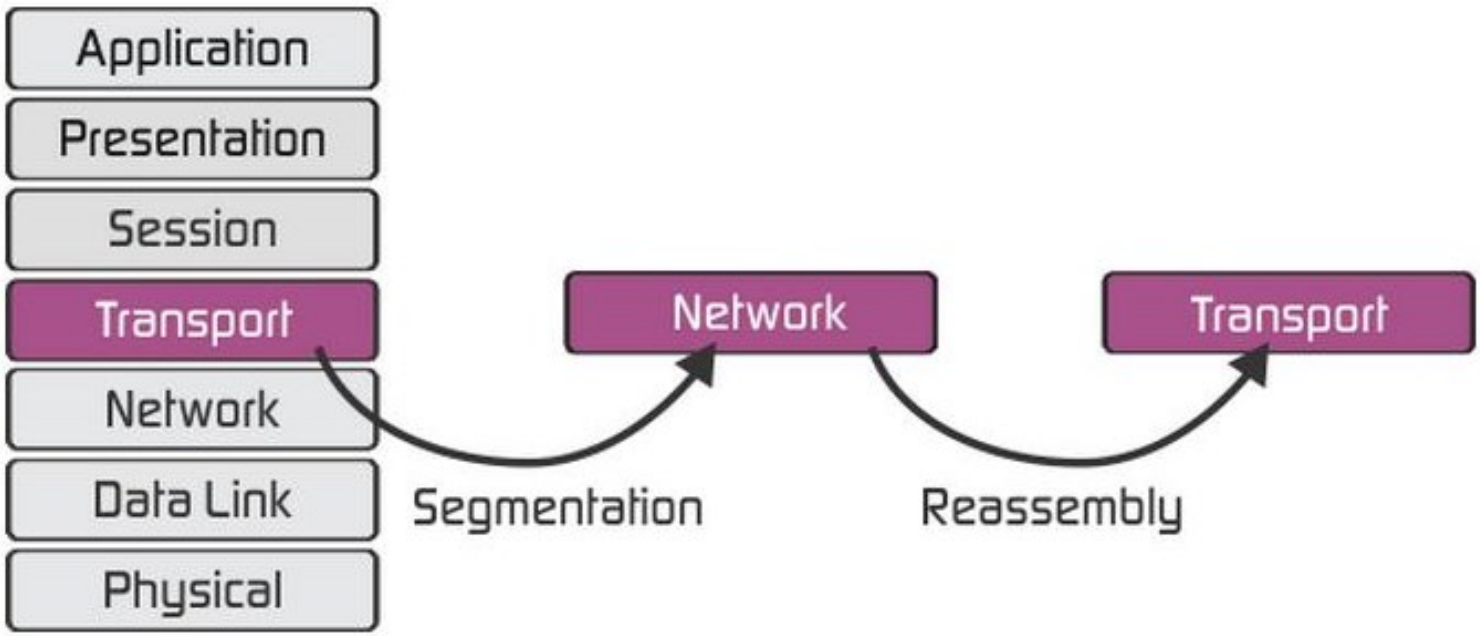


Figure 18 : Segmentation and Reassembly

Transport layer

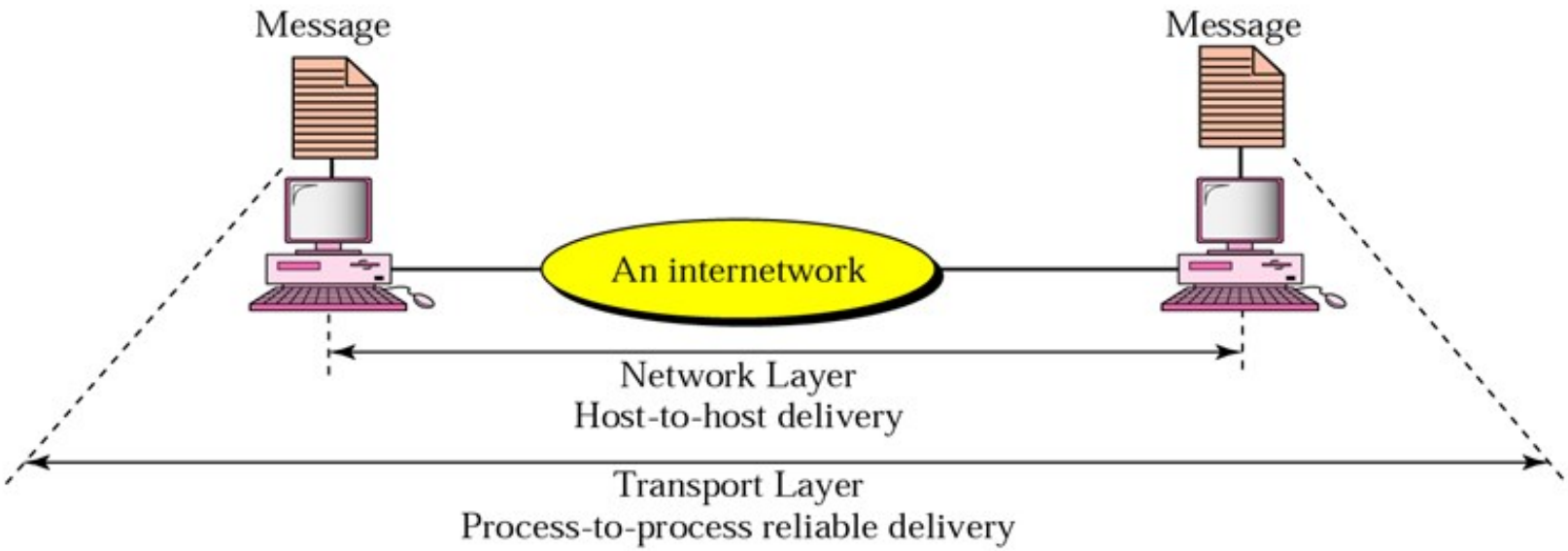


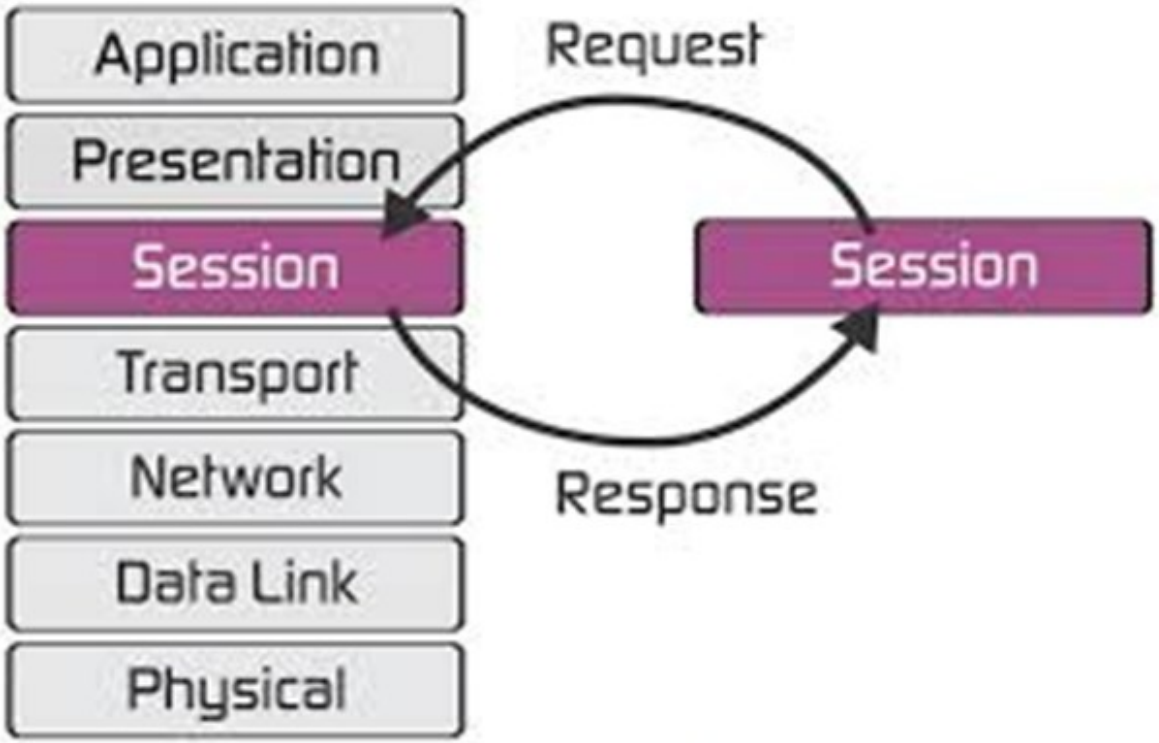
Figure 19 : Process to process delivery

Transport layer

The transport layer is responsible for delivery of a message from one process to another.

Session Layer

- The session layer is the network dialog controller.
  It establishes, maintains, and synchronizes the interaction among communicating systems.



Session Layer

- Dialog control:The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half-duplex (one way at a time) or full-duplex (two ways at a time) mode.

Session Layer

- Dialog control:The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half-duplex (one way at a time) or full-duplex (two ways at a time) mode.
- Synchronization: The session layer allows a process to add checkpoints, or synchronization points, to a stream of data.
  For example, if a system is sending a file of 2000 pages, it is advisable to insert checkpoints after every 100 pages to ensure that each 100-page unit is received and acknowledged independently. In this case, if a crash happens during the transmission of page 523, the only pages that need to be resent after system recovery are pages 501 to 523. Pages previous to 501 need not be resent.

Presentation Layer

- The presentation layer is responsible for translation, compression, and encryption.
- Translation: The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on. The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods.
  The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

Presentation Layer

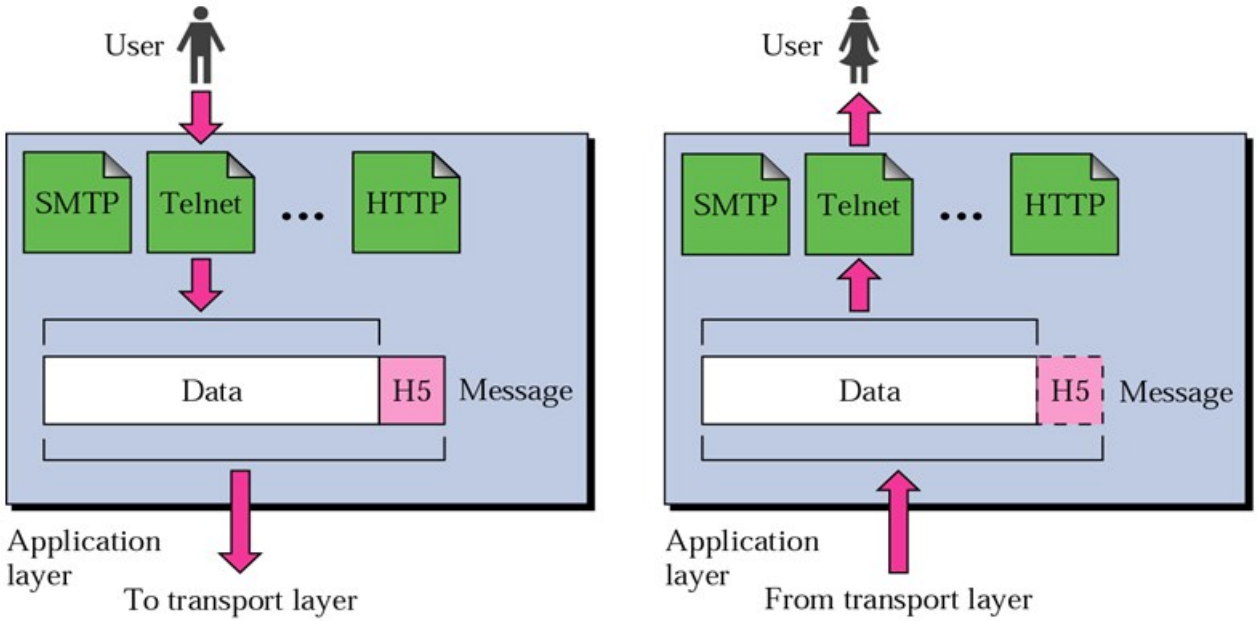
- Encryption: To carry sensitive information, a system must be able to ensure privacy.
  Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.

Presentation Layer

- Encryption: To carry sensitive information, a system must be able to ensure privacy.
  Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network. Decryption reverses the original process to transform the message back to its original form.
- Compression: Data compression reduces the number of bits contained in the information.
  Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.

Application Layer

- The Application layer is responsible for providing services to the user.
- It provides protocols that allow software to send and receive information and present meaningful data to users.



Application Layer

- Network virtual terminal: A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.

Application Layer

- Network virtual terminal: A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.
- File transfer, access, and management (FTAM): This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.

Application Layer

- Network virtual terminal: A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.
- File transfer, access, and management (FTAM): This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
- Mail services: This application provides the basis for e-mail forwarding and storage.

Application Layer

- Network virtual terminal: A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host.
- File transfer, access, and management (FTAM): This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
- Mail services: This application provides the basis for e-mail forwarding and storage.
- Directory services: This application provides distributed database sources and access for global information about various objects and services.

OSI Layers

The application layer is responsible for providing services to the user.

OSI Layers

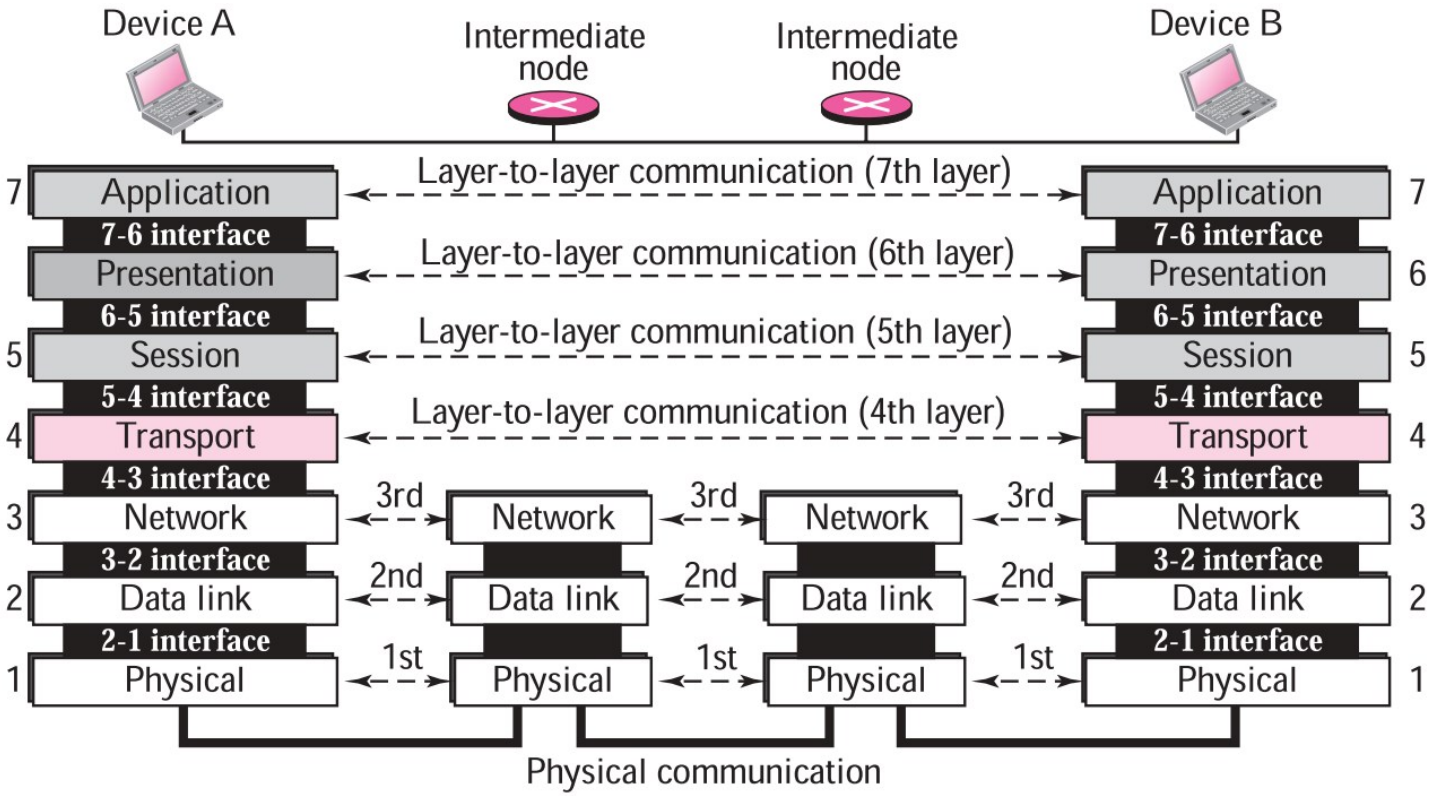


Figure 20 : OSI Layers: Peer to peer process

OSI Layers

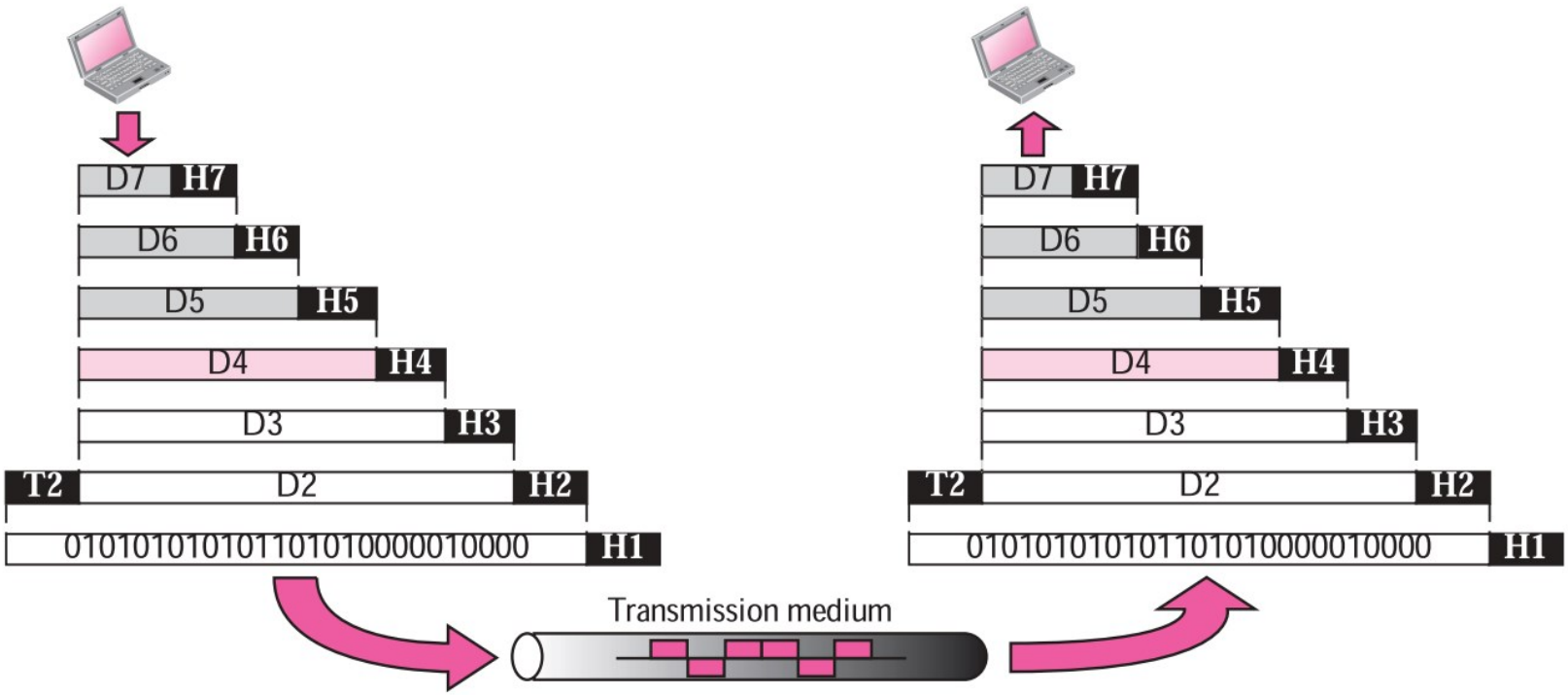


Figure 21 : Exchange using OSI model

OSI Layers

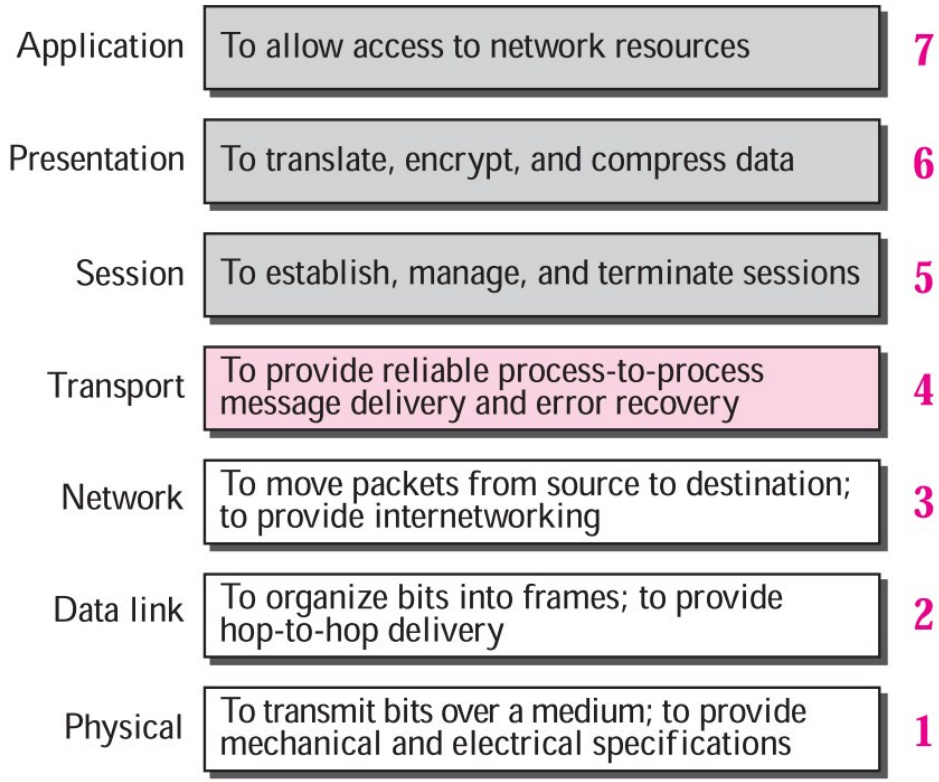


Figure 22 : Comparison

TCP/IP Protocol Suite

TCP/IP Protocol Suite

- The layers in the TCP/IP protocol suite is a five layer model and do not exactly match those layers in the OSI model.
- When TCP/IP is compared to OSI, we can say that the TCP/IP protocol suite is made of five layers:
  (1) physical
  (2) data link
  (3) network
  (4) transport
  (5) application
- This model is used in internet today.

TCP/IP Protocol Suite

- In figure23, small internet made up of three LANs (links), each with a link-layer switch.
- Links are connected by one router.
- Five communicating devices in this communication:
  - Source host (computer A)
  - Link-layer switch in link 1
  - Router
  - Link-layer switch in link 2
  - Destination host (computer B).

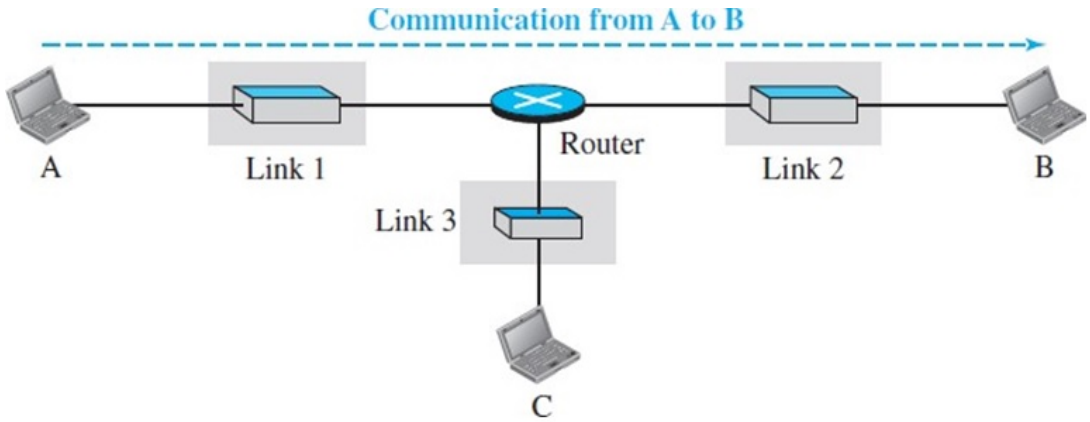


Figure 23 : Small internet model

TCP/IP Protocol Suite

- Each device is involved with a set of layers depending on the role of the device in the internet.
- Two hosts are involved in all five layers.
- Router is involved in only three layers.
- A link-layer switch is involved only in two layers, data-link and physical.

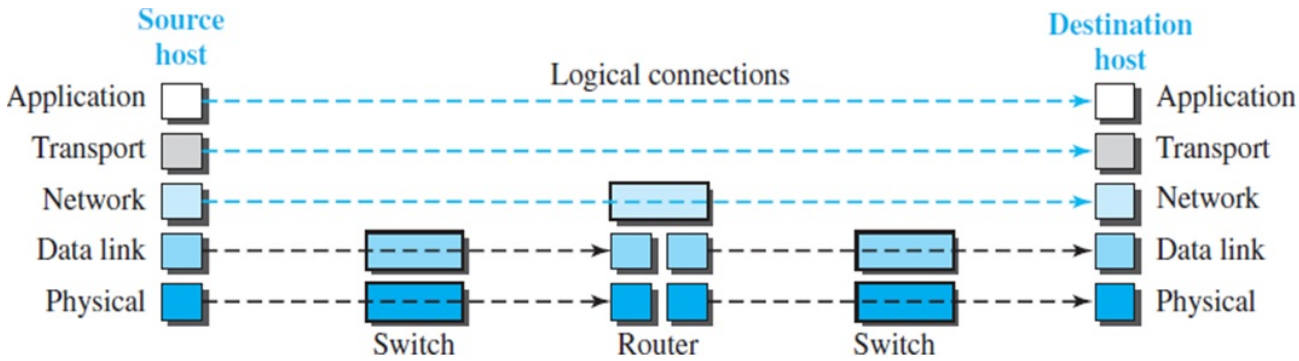


Figure 24 : Logical connections between layers

TCP/IP Protocol Suite

- Top three layers - application, transport, and network
  - Duty is end-to-end.
  - Domain of duty is the internet.
  - Data unit (packets) should not be changed by any router or link-layer switch

TCP/IP Protocol Suite

- Top three layers - application, transport, and network
  - Duty is end-to-end.
  - Domain of duty is the internet.
  - Data unit (packets) should not be changed by any router or link-layer switch
- Bottom two layers - data-link and physical
  - Duty is hop-to-hop, in which a hop is a host or router.
  - Domain of duty is the link.
  - Packet created by the host is changed only by routers, not by link-layer switches.

TCP/IP Protocol Suite

- Physical Layer
  - Responsible for carrying individual bits in a frame across the link.

TCP/IP Protocol Suite

- Physical Layer
  - Responsible for carrying individual bits in a frame across the link.
  - Two devices are connected by a transmission medium (cable or air).

TCP/IP Protocol Suite

- Physical Layer
  - Responsible for carrying individual bits in a frame across the link.
  - Two devices are connected by a transmission medium (cable or air).
  - Medium carries electrical or optical signals.

TCP/IP Protocol Suite

- Physical Layer
  - Responsible for carrying individual bits in a frame across the link.
  - Two devices are connected by a transmission medium (cable or air).
  - Medium carries electrical or optical signals.
  - Bits received in a frame from DLL are transformed and sent through transmission media.

TCP/IP Protocol Suite

- Physical Layer
  - Responsible for carrying individual bits in a frame across the link.
  - Two devices are connected by a transmission medium (cable or air).
  - Medium carries electrical or optical signals.
  - Bits received in a frame from DLL are transformed and sent through transmission media.
  - Several protocols that transform a bit to a signal.

TCP/IP Protocol Suite

- Data Link Layer
  - It takes a datagram and encapsulates it in a packet called a frame.

TCP/IP Protocol Suite

- Data Link Layer
  - It takes a datagram and encapsulates it in a packet called a frame.
  - When next link to travel is determined by router, DLL is responsible for taking datagram and moving it across link.

TCP/IP Protocol Suite

- Data Link Layer
  - It takes a datagram and encapsulates it in a packet called a frame.
  - When next link to travel is determined by router, DLL is responsible for taking datagram and moving it across link.
  - Link can be a
    - Wired LAN with a link-layer switch
    - Wireless LAN
    - Wired WAN
    - Wireless WAN

TCP/IP Protocol Suite

- Data Link Layer
  - It takes a datagram and encapsulates it in a packet called a frame.
  - When next link to travel is determined by router, DLL is responsible for taking datagram and moving it across link.
  - Link can be a
    - Wired LAN with a link-layer switch
    - Wireless LAN
    - Wired WAN
    - Wireless WAN
  - Different protocols used with any link type.

TCP/IP Protocol Suite

- Network Layer
  - Responsible for creating a connection between source and destination.

TCP/IP Protocol Suite

- Network Layer
  - Responsible for creating a connection between source and destination.
  - Responsible for host-to-host communication.

TCP/IP Protocol Suite

- Network Layer
  - Responsible for creating a connection between source and destination.
  - Responsible for host-to-host communication.
  - Routers are responsible for choosing best route for each packet.

TCP/IP Protocol Suite

- Network Layer
  - Responsible for creating a connection between source and destination.
  - Responsible for host-to-host communication.
  - Routers are responsible for choosing best route for each packet.
  - In the Internet, network layer includes the main protocol, IP.

TCP/IP Protocol Suite

- Network Layer
  - Responsible for creating a connection between source and destination.
  - Responsible for host-to-host communication.
  - Routers are responsible for choosing best route for each packet.
  - In the Internet, network layer includes the main protocol, IP.
  - Defines - format of the packet, called a datagram.

TCP/IP Protocol Suite

- Network Layer
  - Responsible for creating a connection between source and destination.
  - Responsible for host-to-host communication.
  - Routers are responsible for choosing best route for each packet.
  - In the Internet, network layer includes the main protocol, IP.
  - Defines - format of the packet, called a datagram.
  - Defines - format and structure of addresses used in this layer.

TCP/IP Protocol Suite

- Network Layer
  - Responsible for creating a connection between source and destination.
  - Responsible for host-to-host communication.
  - Routers are responsible for choosing best route for each packet.
  - In the Internet, network layer includes the main protocol, IP.
  - Defines - format of the packet, called a datagram.
  - Defines - format and structure of addresses used in this layer.
  - Responsible for routing a packet from source to destination.

TCP/IP Protocol Suite

- Network Layer
  - Responsible for creating a connection between source and destination.
  - Responsible for host-to-host communication.
  - Routers are responsible for choosing best route for each packet.
  - In the Internet, network layer includes the main protocol, IP.
  - Defines - format of the packet, called a datagram.
  - Defines - format and structure of addresses used in this layer.
  - Responsible for routing a packet from source to destination.
  - Each router forwarding the datagram to next router in its path.

TCP/IP Protocol Suite

- Network Layer
  - Responsible for creating a connection between source and destination.
  - Responsible for host-to-host communication.
  - Routers are responsible for choosing best route for each packet.
  - In the Internet, network layer includes the main protocol, IP.
  - Defines - format of the packet, called a datagram.
  - Defines - format and structure of addresses used in this layer.
  - Responsible for routing a packet from source to destination.
  - Each router forwarding the datagram to next router in its path.
  - Connectionless protocol.

TCP/IP Protocol Suite

- Network Layer: Routing Protocol
  - Layer includes;
    - Unicast (one-to-one) routing protocol
    - Multicast (one-to-many) routing protocol
  - It does not take part in routing (it is the responsibility of IP).
  - It creates forwarding tables for routers to help them in the routing process.

TCP/IP Protocol Suite

- Network Layer: Routing Protocol
  Help Internet Protocol(IP) in its delivery and routing tasks.

TCP/IP Protocol Suite

- Network Layer: Routing Protocol
  Help Internet Protocol(IP) in its delivery and routing tasks.
  - Internet Control Message Protocol (ICMP)
    Report some problems when routing a packet.

TCP/IP Protocol Suite

- Network Layer: Routing Protocol
  Help Internet Protocol(IP) in its delivery and routing tasks.
  - Internet Control Message Protocol (ICMP)
    Report some problems when routing a packet.
  - Internet Group Management Protocol (IGMP)
    Multitasking.

TCP/IP Protocol Suite

- Network Layer: Routing Protocol
  Help Internet Protocol(IP) in its delivery and routing tasks.
  - Internet Control Message Protocol (ICMP)
    Report some problems when routing a packet.
  - Internet Group Management Protocol (IGMP)
    Multitasking.
  - Dynamic Host Configuration Protocol (DHCP)
    Get network-layer address for a host.

TCP/IP Protocol Suite

- Network Layer: Routing Protocol
  Help Internet Protocol(IP) in its delivery and routing tasks.
  - Internet Control Message Protocol (ICMP)
    Report some problems when routing a packet.
  - Internet Group Management Protocol (IGMP)
    Multitasking.
  - Dynamic Host Configuration Protocol (DHCP)
    Get network-layer address for a host.
  - Address Resolution Protocol (ARP)
    Find link-layer address of a host or a router when its network-layer address is known.

TCP/IP Protocol Suite

- Transport Layer
  - Logical connection is end-to-end.

TCP/IP Protocol Suite

- Transport Layer
  - Logical connection is end-to-end.
  - At source, it gets message from application layer, encapsulates it in a transport layer packet (called a segment or a user datagram in different protocols) and sends it, through logical connection, to transport layer at destination.

TCP/IP Protocol Suite

- Transport Layer
  - Logical connection is end-to-end.
  - At source, it gets message from application layer, encapsulates it in a transport layer packet (called a segment or a user datagram in different protocols) and sends it, through logical connection, to transport layer at destination.
  - It is responsible for giving services to application layer.
    Get a message from an application program running on source and deliver it to corresponding application program on destination.

TCP/IP Protocol Suite

- Transport Layer
  - Logical connection is end-to-end.
  - At source, it gets message from application layer, encapsulates it in a transport layer packet (called a segment or a user datagram in different protocols) and sends it, through logical connection, to transport layer at destination.
  - It is responsible for giving services to application layer.
    Get a message from an application program running on source and deliver it to corresponding application program on destination.
  - There are a few transport-layer protocols in the Internet.
    Each designed for some specific task.

TCP/IP Protocol Suite

- Transport Layer: TCP protocol
  - Connection-oriented protocol.
  - It first establishes a logical connection between transport layers at two hosts before transferring data.
  - It creates a logical pipe between two TCPs for transferring a stream of bytes.
  - Flow control: Match sending data rate of source with receiving data rate of destination to prevent overwhelming the destination.
  - Error control: Guarantee that segments arrive at destination without error and resending corrupted ones.
  - Congestion control: Reduce loss of segments due to congestion in network.

TCP/IP Protocol Suite

- Transport Layer: UDP protocol
  - Connectionless protocol.
  - It transmits user datagrams first without creating a logical connection.
  - Each user datagram is an independent entity.
  - Simple protocol that does not provide flow, error, or congestion control.
  - It is attractive to an application program that needs to send short messages and cannot afford retransmission.
  - Stream Control Transmission Protocol (SCTP)
    a new protocol and it is designed to respond to new applications that are emerging in multimedia

TCP/IP Protocol Suite

- Application Layer
  - Logical connection between two application layers is end-to-end.
  - Duty is process-to-process communication.
    Communication is between two processes (two programs running at this layer).
  - In Internet, it includes many predefined protocols.

TCP/IP Protocol Suite

- Application Layer: Protocols
  - Hypertext Transfer Protocol (HTTP): for access World Wide Web (WWW).

TCP/IP Protocol Suite

- Application Layer: Protocols
  - Hypertext Transfer Protocol (HTTP): for access World Wide Web (WWW).
  - Simple Mail Transfer Protocol (SMTP): Main protocol used in electronic mail (e-mail) service.

TCP/IP Protocol Suite

- Application Layer: Protocols
  - Hypertext Transfer Protocol (HTTP): for access World Wide Web (WWW).
  - Simple Mail Transfer Protocol (SMTP): Main protocol used in electronic mail (e-mail) service.
  - File Transfer Protocol (FTP): Used for transferring files from one host to another.

TCP/IP Protocol Suite

- Application Layer: Protocols
  - Hypertext Transfer Protocol (HTTP): for access World Wide Web (WWW).
  - Simple Mail Transfer Protocol (SMTP): Main protocol used in electronic mail (e-mail) service.
  - File Transfer Protocol (FTP): Used for transferring files from one host to another.
  - Terminal Network (TELNET) and Secure Shell (SSH): Used for accessing a site remotely.

TCP/IP Protocol Suite

- Application Layer: Protocols
  - Hypertext Transfer Protocol (HTTP): for access World Wide Web (WWW).
  - Simple Mail Transfer Protocol (SMTP): Main protocol used in electronic mail (e-mail) service.
  - File Transfer Protocol (FTP): Used for transferring files from one host to another.
  - Terminal Network (TELNET) and Secure Shell (SSH): Used for accessing a site remotely.
  - Simple Network Management Protocol (SNMP): Used by an administrator to manage Internet at global and local levels.

TCP/IP Protocol Suite

- Application Layer: Protocols
  - Hypertext Transfer Protocol (HTTP): for access World Wide Web (WWW).
  - Simple Mail Transfer Protocol (SMTP): Main protocol used in electronic mail (e-mail) service.
  - File Transfer Protocol (FTP): Used for transferring files from one host to another.
  - Terminal Network (TELNET) and Secure Shell (SSH): Used for accessing a site remotely.
  - Simple Network Management Protocol (SNMP): Used by an administrator to manage Internet at global and local levels.
  - Domain Name System (DNS): Used by other protocols to find the network-layer address of a computer.

TCP/IP Protocol Suite

- Application Layer: Protocols
  - Hypertext Transfer Protocol (HTTP): for access World Wide Web (WWW).
  - Simple Mail Transfer Protocol (SMTP): Main protocol used in electronic mail (e-mail) service.
  - File Transfer Protocol (FTP): Used for transferring files from one host to another.
  - Terminal Network (TELNET) and Secure Shell (SSH): Used for accessing a site remotely.
  - Simple Network Management Protocol (SNMP): Used by an administrator to manage Internet at global and local levels.
  - Domain Name System (DNS): Used by other protocols to find the network-layer address of a computer.
  - Internet Group Management Protocol (IGMP): Used to collect membership in a group.

TCP/IP Protocol Suite

- Encapsulation and Decapsulation
  - Encapsulation in source, decapsulation in destination.
  - encapsulation and decapsulation in router.
  - No encapsulation/ decapsulation occurs link-layer switches.

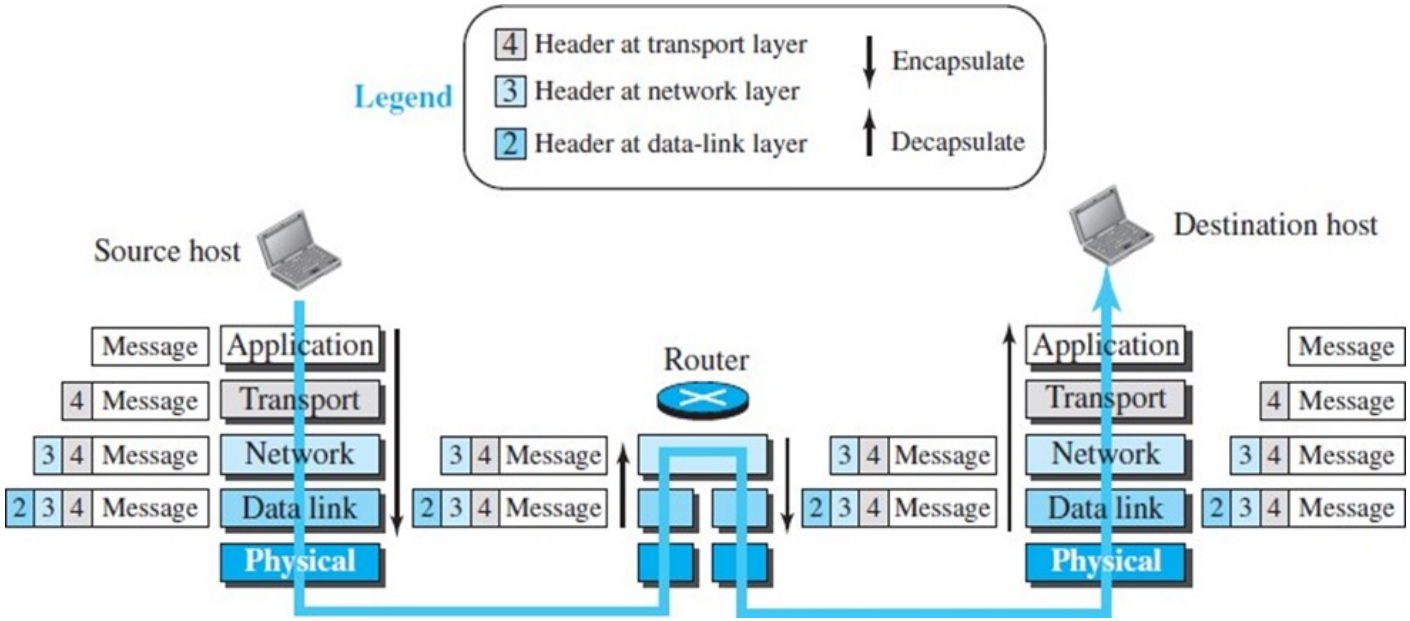


Figure 25 : Encapsulation and Decapsulation

TCP/IP Protocol Suite

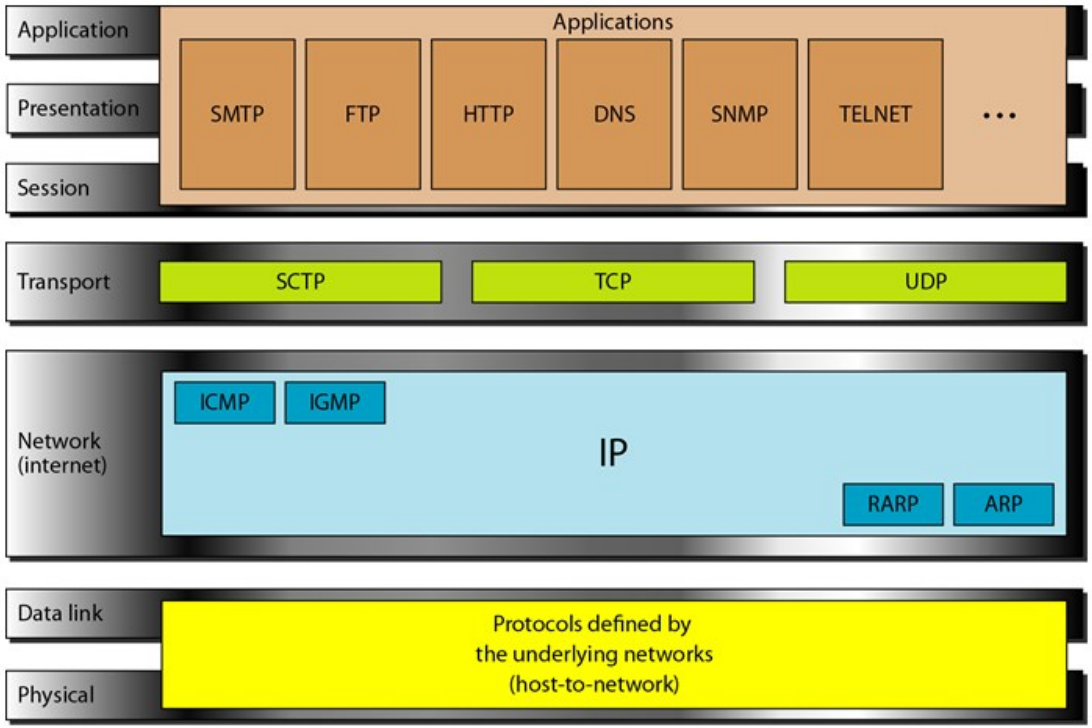


Figure 26 : TCP/IP Protocol suite

TCP/IP Protocol Suite

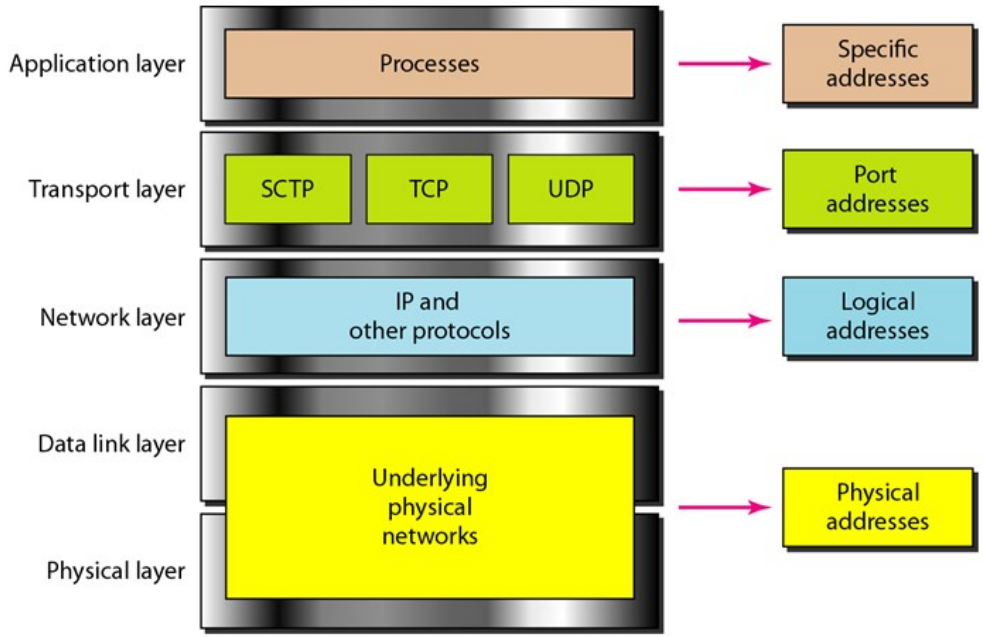


Figure 27 : Relationship of layers and addresses in TCP/IP

TCP/IP Protocol Suite

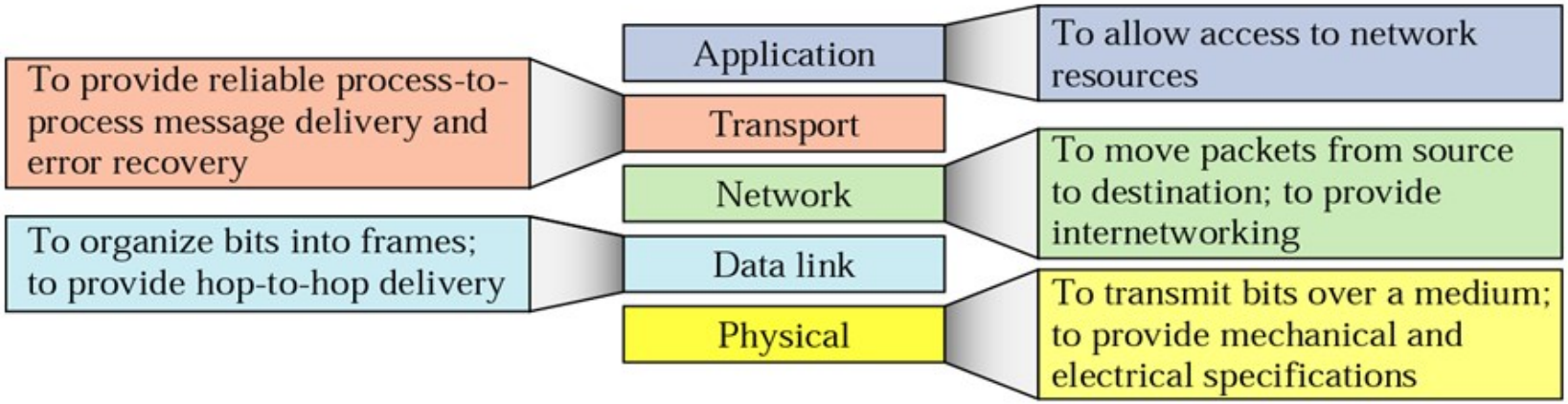


Figure 28 : Comparison

Thank you

&

Queries