Mod_1
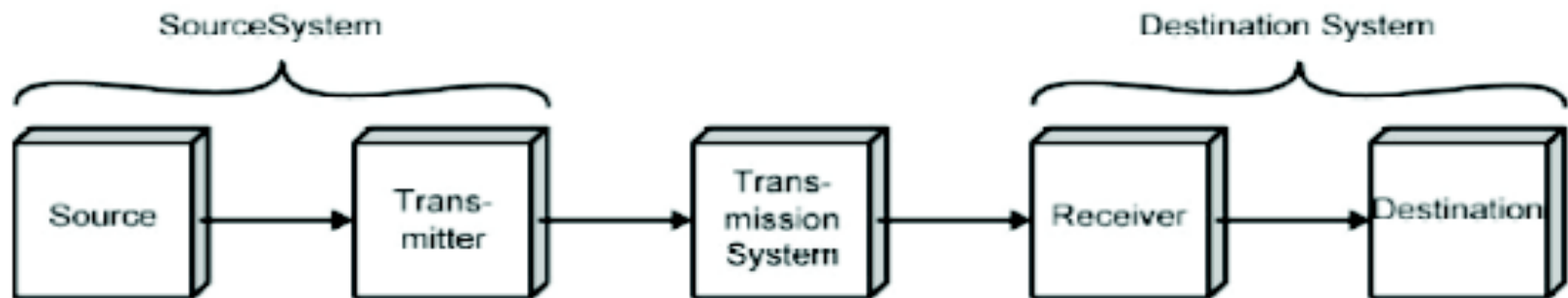
Data Communication

Process of transmitting data from one point to another

Simplified Communications Model - Diagram

SourceSystem

Destination System

| Source | → | Trans-mitter | → | Trans-mission System | → | Receiver | → | Destination |

(a) General block diagram

Workstation — Modem — Public Telephone Network — Modem — Server

(b) Example

Key elements in the model

- **Source**: Device which generates the data to be transmitted
- **Transmitter**: Device which transforms and encodes the information that needs to be transmitted
- **Transmission medium**: provides the path for data communication
- **Receiver**: Device which accepts the signal from the transmission media and converts in to a form that can be handled by the destination device
- **Destination**: Takes the incoming data from the receiver

Computer Network

- A collection of transmission hardware and facilities, terminal equipment, and protocols

- Provides communication that is
  - Reliable
  - Fair
  - Efficient
  - From one application to another
- Automatically detects and corrects
  - Data corruption
  - Data loss
  - Duplication
  - Out-of-order delivery
- Automatically finds optimal path from source to destination

Network Hardware

- Transmission technology (2 types)
  - Broadcast links: A single communication link for all systems in network
  - Point-to-point links: Individual connections between pairs of machines

  - ❏Media
    - ◎ Wired
    - ◎ Wireless

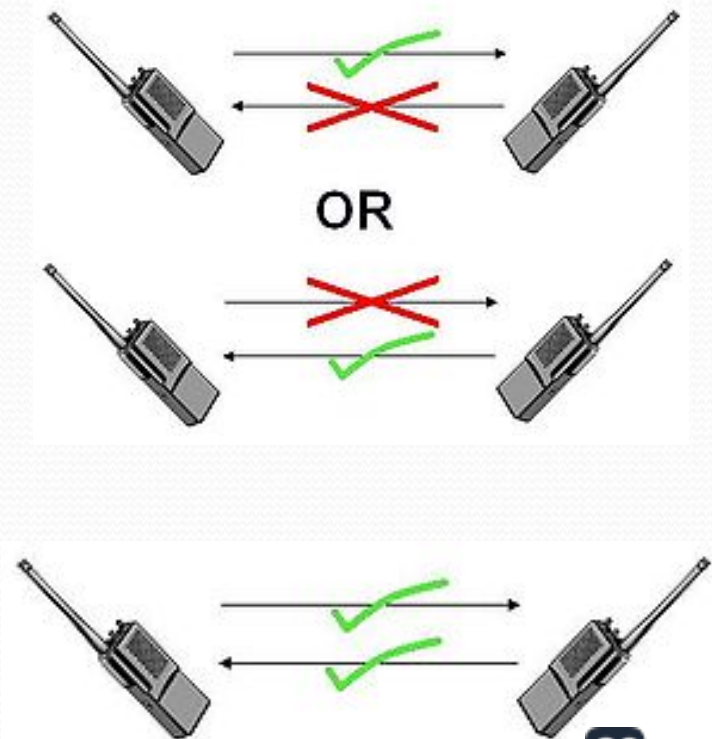# Classification by scale

Interprocessor distance	Processors located in same	Example
1 m	Square meter	Personal area network
10 m	Room	Local area network
100 m	Building	
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

Transmission Modes

- Simplex
  - One direction
    - e.g. Television

- Half duplex
  - Either direction, but only one way at a time
    - e.g. police radio

- Full duplex
  - Both directions at the same time
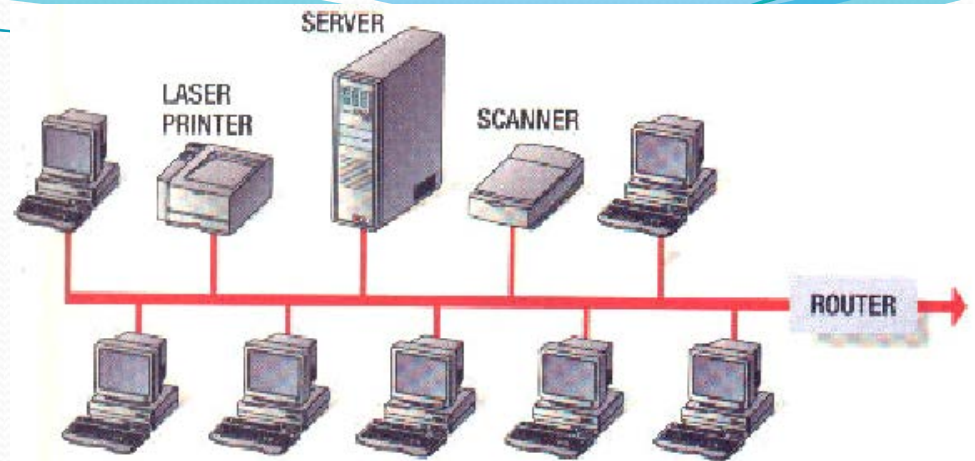   - e.g. telephone

Network Classification: Topology

- The physical topology of a network refers to the configuration of cables, computers, and other peripherals

- categorized into the following basic types
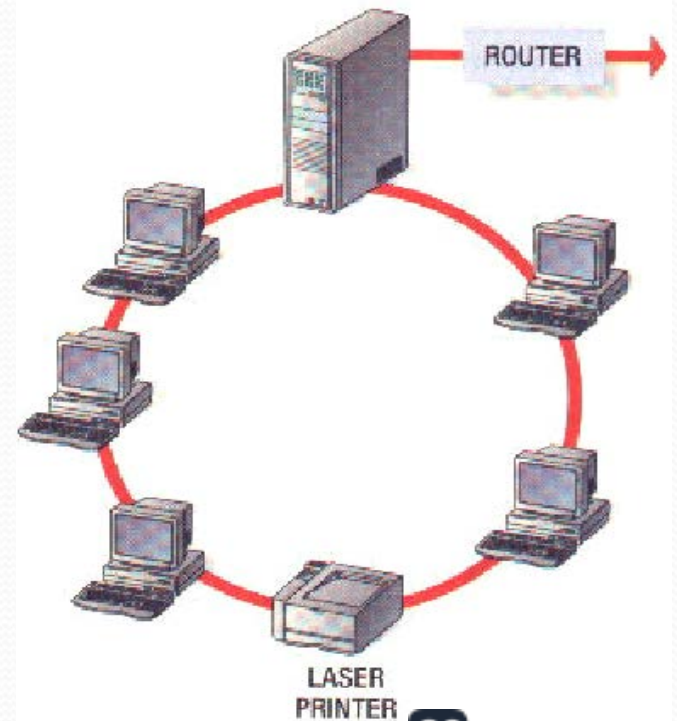
- bus

- ring

- star

- tree

- mesh

Bus Topology
- All nodes connected to single line (bus)
- Terminator ends the wires

Ring Topology

- Links all nodes in a circular chain

- Data messages travel around ring in a single direction

- If one node fails, ring is broken and network fails

Star Topology

- A star topology is designed with each node (file server, workstations, and peripherals) connected directly to a central network hub, switch, or concentrator

- Data on a star network passes through the hub, switch, or concentrator before continuing to its destination.

- The hub, switch, or concentrator manages and controls all functions of the network.

- It also acts as a repeater for the data flow. This configuration is common with twisted pair cable; however, it can also be used with coaxial cable or fiber optic cable.

HUB

ROUTER

LASER PRINTER
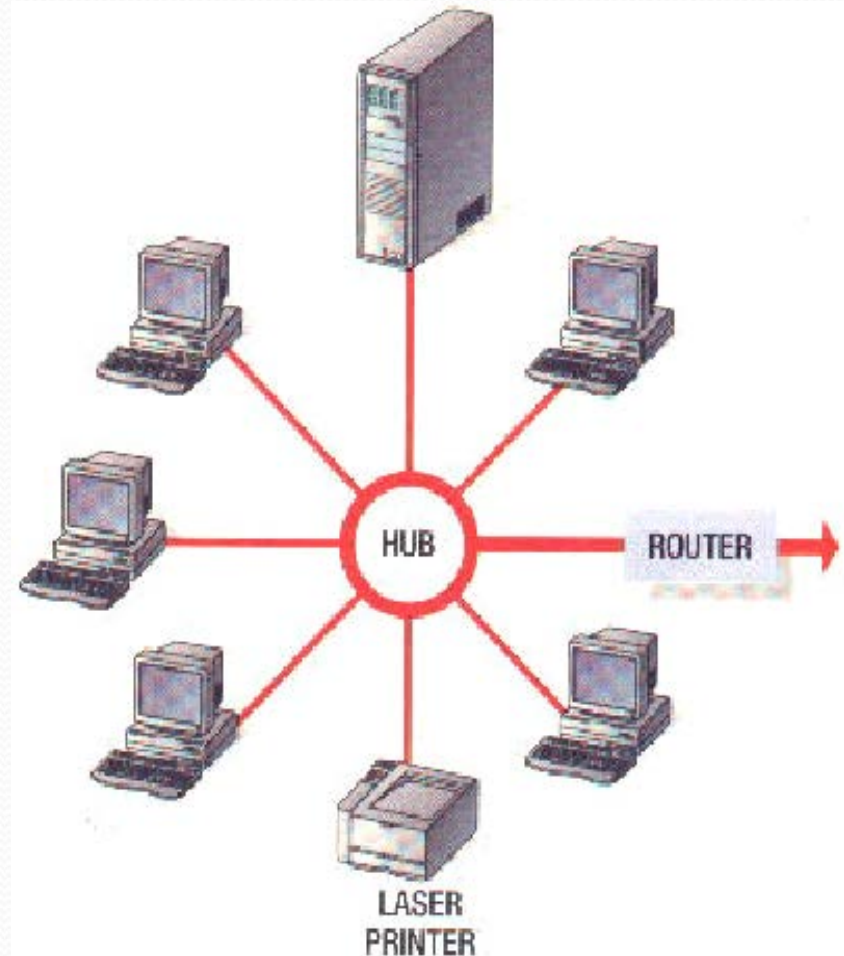
Mesh Topology

Has direct connection between every pair of devices in the n/w
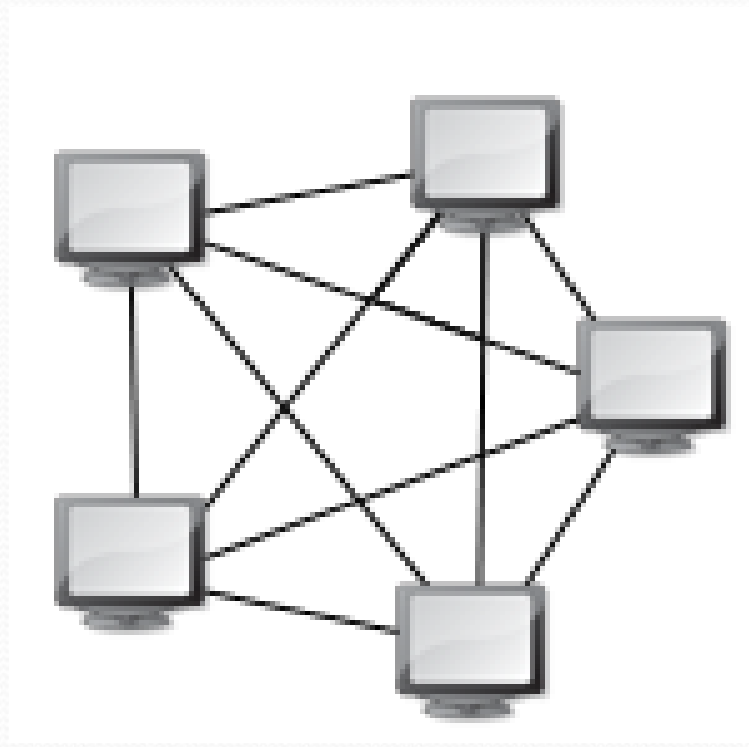
Types of nodes important to networks.

Hub   :A device that repeats or broadcasts the network stream of information to individual nodes (usually personal computers)

Switch: A device that receives packets from its input link, and then sorts them and transmits them over the proper link that connects to the node addressed.

Bridge: A link between two networks that have identical rules of communication.

Gateway: A link between two different networks that have different rules of communication.

Router: A node that sends network packets in one of many possible directions to get them to their destination.

- Network Classification: By size or scale

- <u>LAN-Local Area Network</u>
- connects network devices over a relatively short distance operates in a limited space, LANs are also typically owned, controlled, and managed by a single person or organization.

- two different operating modes can be defined:
- In a "<u>peer-to-peer</u>" network, in which communication is carried out from one computer to another, without a central computer, and where each computer has the same role.
- in a "<u>client/server</u>" environment, in which a central computer provides network services to users.

- **Metropolitan Area Network**
- a network spanning a physical area larger than a LAN but smaller than a WAN, such as a city.
- typically owned an operated by a single entity such as a government body or large corporation.
- Can support both data and voice
- Eg: Cable television network.
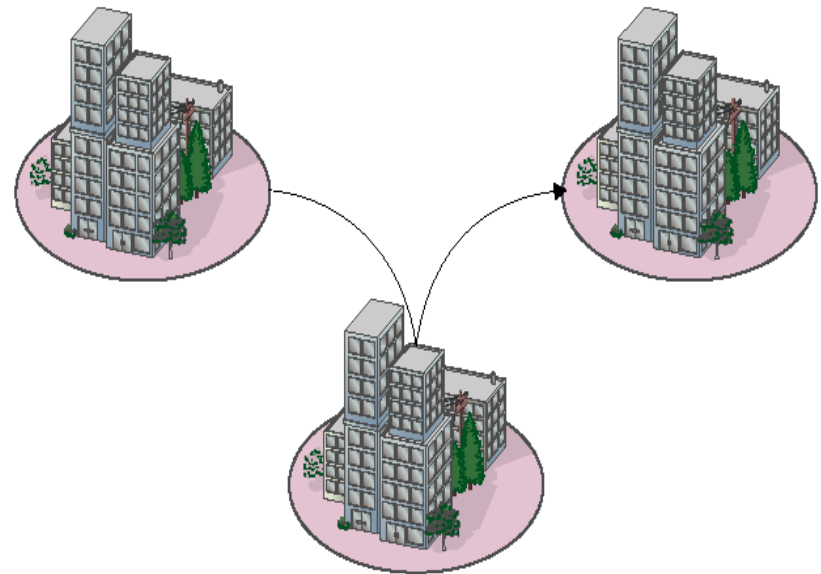
WAN - Wide Area Network

- network that spans a large geographical area
- the most common example being the Internet the largest known WAN today
- Contains a collection of machines (hosts) intended for running user programs.
- Host connected by communication subnet.

Wide Area Network (WAN)
Typical Schematic
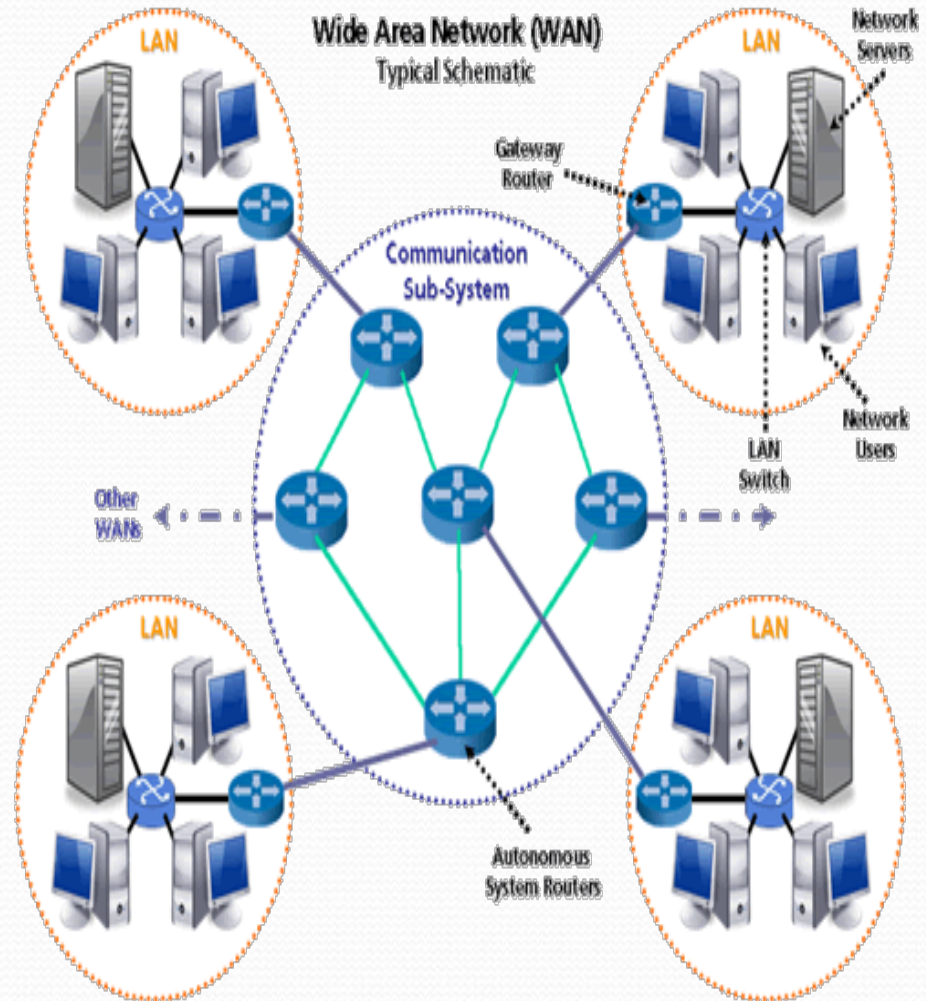
Relation between hosts on LAN's and the subnet
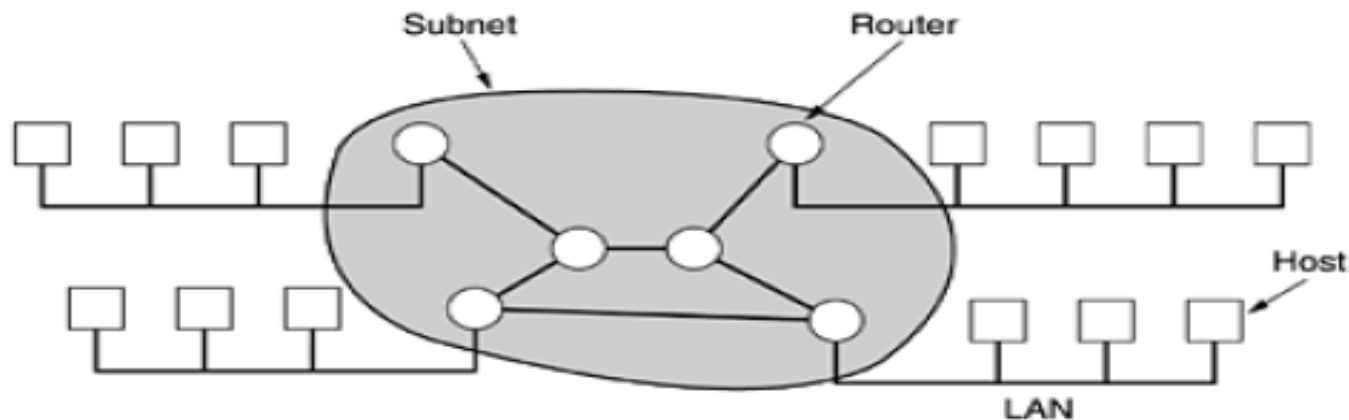
Subnet consists of transmission lines and switching elements (routers).

Store and forward or packet switched network..

Packets small and of same size are called cells.

- WIRELESS NETWORKS :
- any type of computer network that is wireless, and is commonly associated with a telecommunications network whose interconnections between nodes is implemented without the use of wires.

- implemented with some type of remote information transmission system that uses electromagnetic waves, such as radio waves, for the carrier

Internetwork

- An Internetwork is the connection of two or more distinct computer networks or network segments via a common routing technology.

- Any interconnection among or between public, private, commercial, industrial, or governmental networks may also be defined as an internetwork.

Internetwork

- **Intranet**
  - An intranet is a set of networks, using the Internet Protocol and IP-based tools such as web browsers and file transfer applications, that is under the control of a single administrative entity.
  - Most commonly, an intranet is the internal network of an organization

- **Extranet**
  - An extranet is a network or internetwork that is limited in scope to a single organization or entity but which also has limited connections to the networks of one or more other usually, but not necessarily, trusted organizations or entities
  - by definition, an extranet cannot consist of a single LAN; it must have at least one connection with an external network.

- **Internet**
  - The Internet consists of a worldwide interconnection of governmental, academic, public, and private networks based upon the networking technologies of the Internet Protocol Suite.

Protocol Layers and their service models

- Layered Architecture
- A layered architecture allows us to discuss a well-defined, specific part of a large and complex system.
- This simplification provides modularity, making it much easier to change the implementation of the service
- provided by the layer.
- As long as the layer provides the same service to the layer above it, and uses the same services from the layer below it, the remainder of the system remains unchanged when a layer's implementation is changed.
- For large and complex systems that are constantly being updated, the ability to change the implementation of a service without affecting other components of the system is another important advantage of layering.

Protocol Layering

- A **protocol defines the format and the order of messages exchanged between** two or more communicating entities, as well as the actions taken on the transmission and/or receipt of a message or other event.
- The Internet, and computer networks in general, make extensive use of protocols. Different protocols are used to accomplish different communication tasks.
- To provide structure to the design of network protocols, network designers organize protocols—and the network hardware and software that implement the protocols—
- in **layers.**
- **Each protocol belongs to one of the layers**

- Each layer provides its service by
- (1) performing certain actions within that layer and by
- (2) using the services of the layer directly below it.
- For example, the services provided by layer *n may* include reliable delivery of messages from one edge of the network to the other.
- A protocol layer can be implemented in software, in hardware, or in a combination of the two.
- Protocol layering has conceptual and structural advantages.
- Layering provides a structured way to discuss system components.
- Modularity makes it easier to update system components.
- Divide complex task into several smaller and simpler tasks.
- Separate services from implementation .

- One potential drawback of layering is that one layer may duplicate lower-layer functionality.
- For example, many protocol stacks provide error recovery on both a per-link basis and an end-to-end basis.
- A second potential drawback is that functionality at one layer may need information (for example, a timestamp value) that is present only in another layer; this violates the goal of separation of layers.

- When taken together, the protocols of the various layers are called the **protocol stack.**
- **The Internet protocol stack consists of five layers: the physical**, **link**, **network**, transport, and application layers

Layer Architecture

- Layer architecture simplifies the network design.

- It is easy to debug network applications in a layered architecture network.

- The network management is easier due to the layered architecture.

- Network layers follow a set of rules, called protocol.

- The protocol defines the format of the data being exchanged, and the control and timing for the handshake between layers.

Each layer communicate with each other by exchanging layer-n messages. These messages are called layer-n protocol data units, or more commonly **n-PDUs**.

The contents and format of an *n-PDU*, as well as the manner in which the *n-PDUs* are exchanged among the network elements, are defined by a layer-n protocol. When taken together, the protocols of the various layers are called the **protocol stack**.

In a computer network, each layer may perform one or more of the following generic set of tasks:

Error control, which makes the logical channel between the layers in two peer network elements more reliable.

Flow control, which avoids overwhelming a slower peer with PDUs.

Segmentation and Reassembly, which at the transmitting side divides large data chunks into smaller pieces; and at the receiving side reassembles the smaller pieces into the original large chunk.

Multiplexing, which allows several higher-level sessions to share a single lower-level connection.

Connection setup, which provides the handshaking with a peer.

Open Systems Interconnection (OSI) Model

- International standard organization (ISO) established a committee in 1977 to develop an architecture for computer communication.

- Open Systems Interconnection (OSI) reference model is the result of this effort.

- In 1984, the Open Systems Interconnection (OSI) reference model was approved as an international standard for communications architecture.

- Term "open" denotes the ability to connect any two systems which conform to the reference model and associated standards.

OSI Reference Model

- The OSI model is now considered the primary Architectural model for inter-computer communications.

- The OSI model describes how information or data makes its way from application programmes (such as spreadsheets) through a network medium (such as wire) to another application programme located on another network.

- The OSI reference model divides the problem of moving information between computers over a network medium into SEVEN smaller and more manageable problems .

- This separation into smaller more manageable functions is known as layering.

OSI Reference Model: 7 Layers
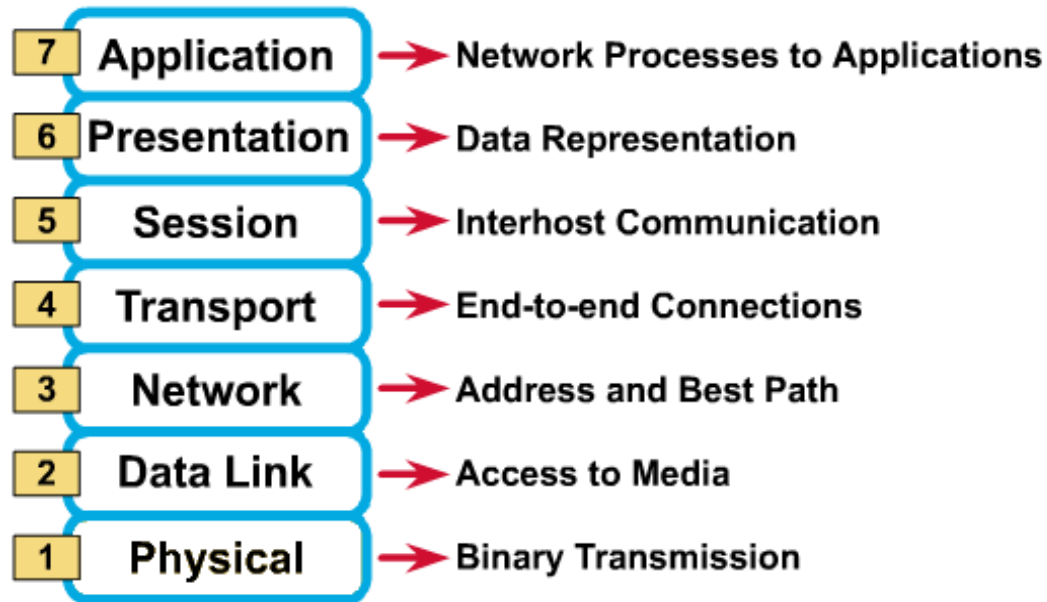
OSI: A Layered Network Model

- The process of breaking up the functions or tasks of networking into layers reduces complexity.

- Each layer provides a service to the layer above it in the protocol specification.

- Each layer communicates with the same layer's software or hardware on other computers.

- The lower 4 layers (transport, network, data link and physical — Layers 4, 3, 2, and 1) are concerned with the flow of data from end to end through the network.

- The upper three layers of the OSI model (application, presentation and session—Layers 7, 6 and 5) are orientated more toward services to the applications.

- Data is Encapsulated with the necessary protocol information as it moves down the layers before network transit.

Physical Layer

- Provides physical interface for transmission of information.

- Defines rules by which bits are passed from one system to another on a physical communication medium.

- Covers all - mechanical, electrical, functional and procedural - aspects for physical communication.

- Such characteristics as voltage levels, timing of voltage changes, physical data rates, maximum transmission distances, physical connectors, and other similar attributes are defined by physical layer specifications.

FUNCTIONS OF PHYSICAL LAYER:

1. **Representation of Bits:** Data in this layer consists of stream of bits. The bits must be encoded into signals for transmission. It defines the type of encoding i.e. how 0's and 1's are changed to signal.

2. **Data Rate:** This layer defines the rate of transmission which is the number of bits per second.

3. **Synchronization:** It deals with the synchronization of the transmitter and receiver. The sender and receiver are synchronized at bit level.

4. **Interface:** The physical layer defines the transmission interface between devices and transmission medium.

5. **Line Configuration:** This layer connects devices with the medium: Point to Point configuration and Multipoint configuration.

6. **Topologies:** Devices must be connected using the following topologies: Mesh, Star, Ring and Bus.

7. **Transmission Modes:** Physical Layer defines the direction of transmission between two devices: Simplex, Half Duplex, Full Duplex.

8. Deals with baseband and broadband transmission.

Data Link Layer

- Data link layer attempts to provide reliable communication over the physical layer interface.

- Breaks the outgoing data into frames and reassemble the received frames.

- Create and detect frame boundaries.

- Handle errors by implementing an acknowledgement and retransmission scheme.

- Implement flow control.

- Supports points-to-point as well as broadcast communication.

- Supports simplex, half-duplex or full-duplex communication.

Network Layer

- Implements routing of frames (packets) through the network.

- Defines the most optimum path the packet should take from the source to the destination

- Defines logical addressing so that any endpoint can be identified.

- Handles congestion in the network.

- Facilitates interconnection between heterogeneous networks (Internetworking).

- The network layer also defines how to fragment a packet into smaller packets to accommodate different media.

Transport Layer

- Purpose of this layer is to provide a reliable mechanism for the exchange of data between two processes in different computers.

- Ensures that the data units are delivered error free.

- Ensures that data units are delivered in sequence.

- Ensures that there is no loss or duplication of data units.

- Provides connectionless or connection oriented service.

- Provides for the connection management.

- Multiplex multiple connection over a single channel.

Session Layer

- Session layer provides mechanism for controlling the dialogue between the two end systems. It defines how to start, control and end conversations (called sessions) between applications.

- This layer requests for a logical connection to be established on an end-user's request.

- Any necessary log-on or password validation is also handled by this layer.

- Session layer is also responsible for terminating the connection.

- This layer provides services like dialogue discipline which can be full duplex or half duplex.

- Session layer can also provide check-pointing mechanism such that if a failure of some sort occurs between checkpoints, all data can be retransmitted from the last checkpoint.

Presentation Layer

- **Presentation layer defines the format in which the data is to be exchanged between the two communicating entities.**

- **Also handles data compression and data encryption (cryptography).**

Application Layer

- Application layer interacts with application programs and is the highest level of OSI model.

- Application layer contains management functions to support distributed applications.

- Examples of application layer are applications such as file transfer, electronic mail, remote login etc.

OSI in Action

A message begins at the top application layer and moves down the OSI layers to the bottom physical layer.

As the message descends, each successive OSI model layer adds a header to it.

A header is layer-specific information that basically explains what functions the layer carried out.

Conversely, at the receiving end, headers are striped from the message as it travels up the corresponding layers.
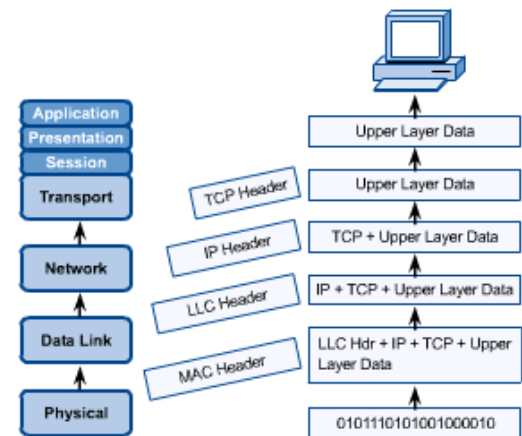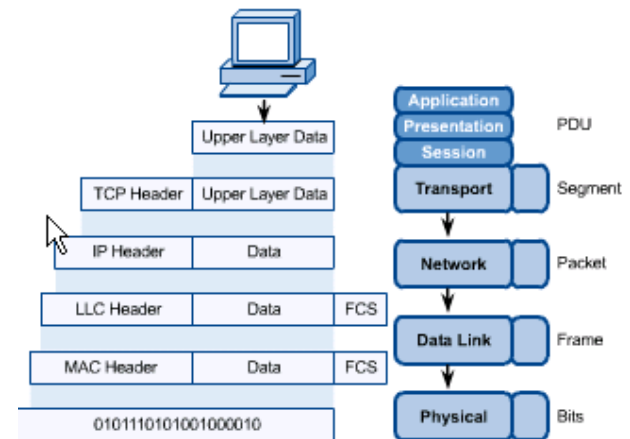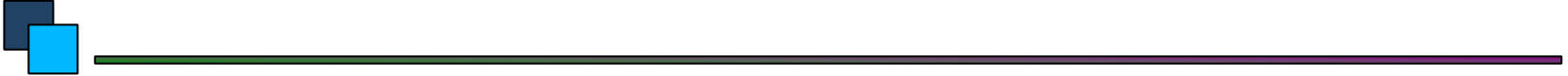
TCP/IP MODEL

OSI & TCP/IP Models

OSI Model

OSI Model	
7 Application	Application Layers
6 Presentation	
5 Session	
4 Transport	Data Flow Layers
3 Network	
2 Data Link	
1 Physical	

OSI Reference Model
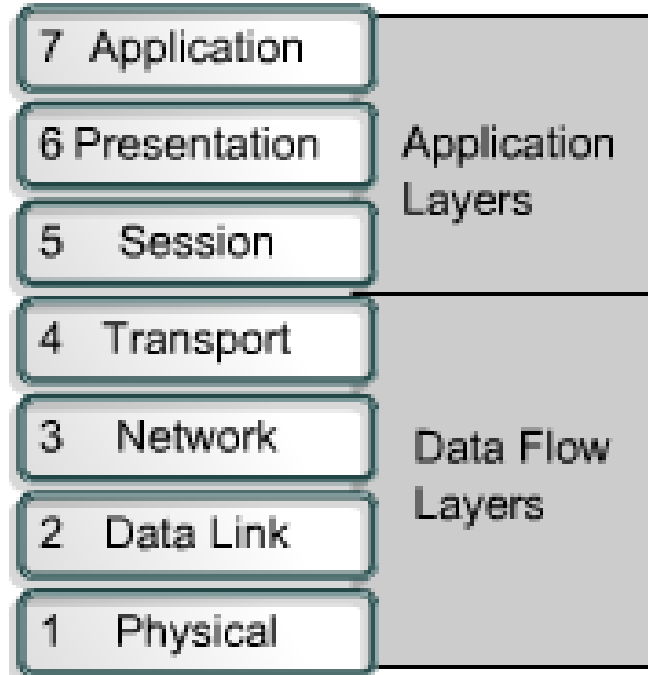
	OSI Reference Model		TCP/IP Conceptual Layers
7	Application		Application
6	Presentation		
5	Session		
4	Transport	↔	Transport
3	Network	↔	Network
2	Data Link	↔	Network Interface
1	Physical	↔	
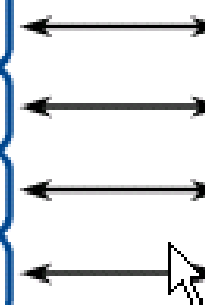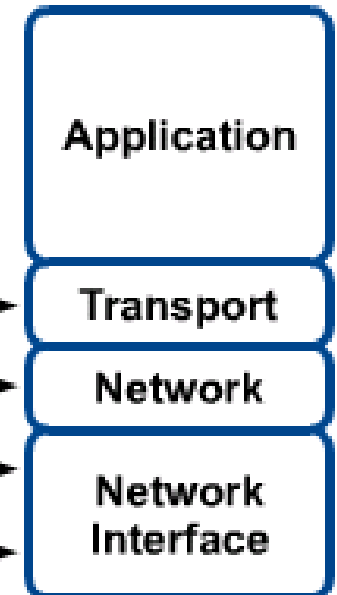
TCP/IP Model

Application Layer
Application programs using the network

Transport Layer (TCP/UDP)
Management of end-to-end message transmission, error detection and error correction

Network Layer (IP)
Handling of datagrams : routing and congestion

Data Link Layer
Management of cost effective and reliable data delivery, access to physical networks

Physical Layer
Physical Media

Transport Layer

- **TCP (Transmission Control Protocol):** provides a reliable connection oriented protocol that delivers a byte stream from one node to another. Guarantees delivery and provides flow control.

- **UDP (User Datagram Protocol)** provides an unreliable connection-less protocol for applications that provide their own.
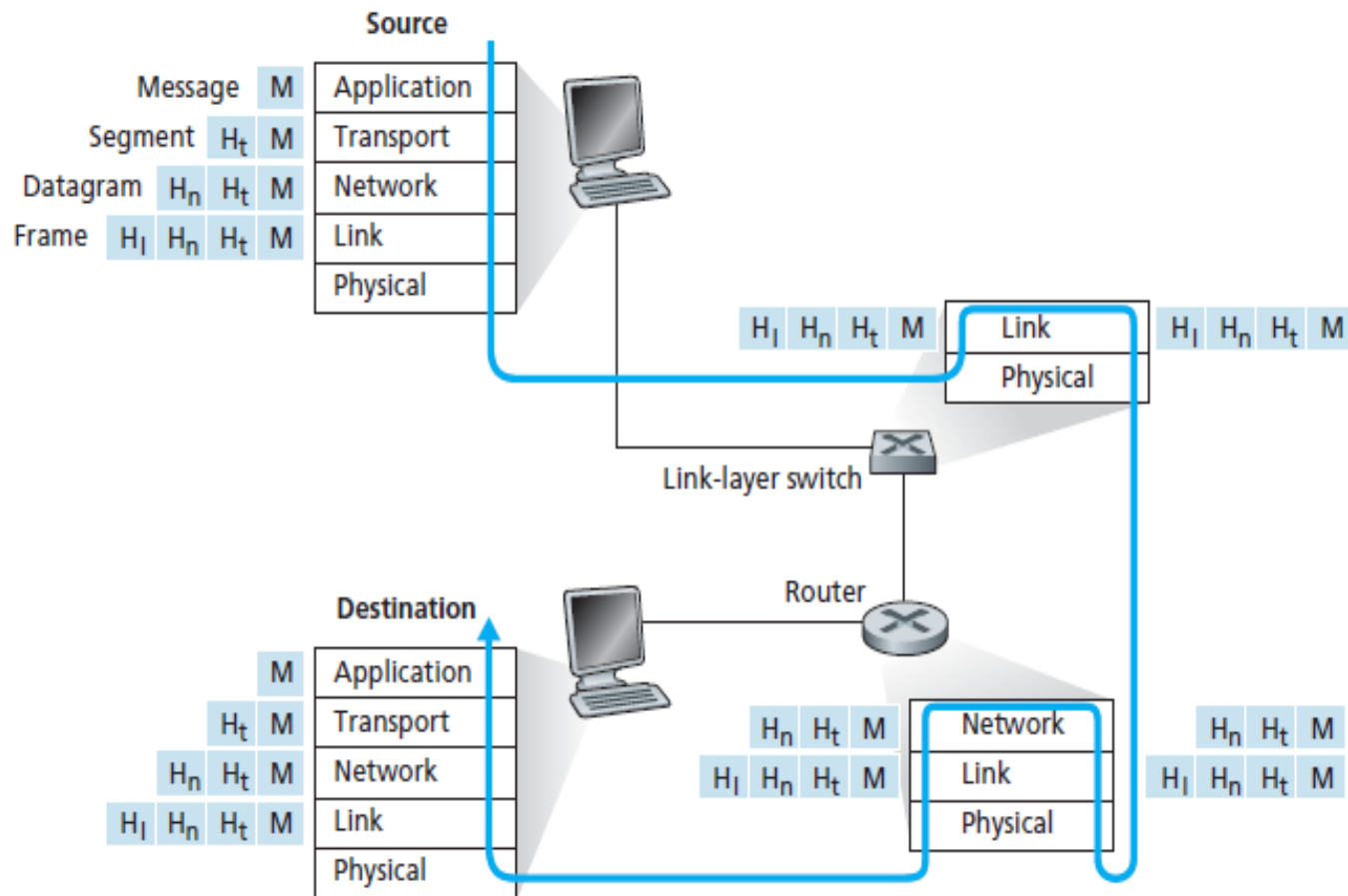
Figure 1.24 ♦ Hosts, routers, and link-layer switches; each contains a different set of layers, reflecting their differences in functionality

Physical path that data takes down a sending end systems protocol stack, up and down the protocol stacks of an intervening link layer switch and router and then up the protocol stack at the receiving end system.

- At the sending host, an **application-layer message (M) is passed to the** transport layer.

- The transport layer takes the message and appends additional information (transport-layer header information, Ht) that will be used by the receiver-side transport layer.

- The application-layer message and the transport-layer header information together constitute the **transport-layer segment.**

- **The transport-layer segment thus encapsulates the** application-layer message.

- The added information might include information allowing the receiver-side transport layer to deliver the message up to the appropriate application, and error-detection bits that allow the receiver to determine whether bits in the message have been changed in route.

- The transport layer then passes the segment to the network layer, which adds network-layer header information (Hn) *such as source and destination end system addresses,* creating a **network-layer datagram.**

- **The datagram is then passed to the link** layer, which will add its own link-layer header information and create a **link-layer frame.**

- **Thus, we see that at each layer, a packet has two types of** fields: header fields and a **payload field. The payload is typically a packet from** the layer above.

Security in the internet

- The **Internet** is the global system of interconnected [computer networks](#) that use the [Internet protocol suite](#) (TCP/IP) to link devices worldwide

- The Internet has become mission critical for many institutions today, including large and small companies, universities, and government agencies. Many individuals also rely on the Internet for many of their professional, social, and personal activities.

- There is a dark side, a side where "bad guys" attempt to wreak havoc in our daily lives by damaging our Internet-connected computers, violating our privacy, and rendering inoperable the Internet services on which we depend.

- **The bad guys can put malware into your host via the Internet.**
- **malware—malicious stuff that can enter and infect our devices which can** delete our files; install spyware that collects our private information, such as social security numbers, passwords.
- The malware is **self-replicating: once it infects one** host, from that host it seeks entry into other hosts over the Internet, and from the newly infected hosts, it seeks entry into yet more hosts. In this manner, self replicating malware can spread exponentially fast.
- Malware can spread in the form of a virus or a worm.
- **Viruses are malware that require some form of user** interaction to infect the user's device.
- Eg: an e-mail attachment containing malicious executable code. If a user receives and opens such an attachment ,the user inadvertently runs the malware on the device. Typically, such email viruses are self-replicating: once executed, the virus may send an identical message with an identical malicious attachment to, for example, every recipient in
- the user's address book.
- **Worms are malware that can enter a device without any** explicit user interaction.

- **The bad guys can attack servers and network infrastructure**
- **denial-of-service (DoS) attacks.**
- **DoS attack renders a network, host, or other piece** of infrastructure unusable by legitimate users. Web servers, e-mail servers, DNS servers, and institutional networks can all be subject to DoS attacks.
- DoS attacks fall into one of three categories:
- • *Vulnerability attack :sending a few well-crafted messages to a vulnerable* application or operating system running on a targeted host. If the right
- sequence of packets is sent to a vulnerable application or operating system, the service can stop or, worse, the host can crash.
- • *Bandwidth flooding: The attacker sends a deluge of packets to the targeted* host—so many packets that the target's access link becomes clogged, preventing legitimate packets from reaching the server.
- • *Connection flooding. The attacker establishes a large number of half-open or* fully open TCP connections at the target host. The host can become so bogged down with these bogus connections that it stops accepting legitimate connections.

- **The bad guys can sniff packets**
- Placing a passive receiver in the vicinity of the wireless transmitter, that receiver can obtain a copy of every packet that is transmitted.
- These packets can contain all kinds of sensitive information, including passwords, social security numbers, trade secrets, and private personal messages.
- A passive receiver that records a copy of every packet that flies by is called a **packet sniffer.**

- **The bad guys can masquerade as someone you trust**

- A packet created with an arbitrary source address, packet content, and destination address and then transmit ted into the Internet, which will dutifully forward the packet to its destination.

- Unsuspecting receiver (say an Internet router) who receives such a packet, takes the (false) source address as being truthful, and then performs some command embedded in the packet's contents (say modifies its forwarding table).

- The ability to inject packets into the Internet with a false source address is known as **IP spoofing.**

- To solve this problem, need *end-point authentication, that is, a mechanism* that will allow us to determine with certainty if a message originated from valid source.

- **The bad guys can delete or modify messages.**
- Man – in –the –middle attack
- The bad guy not only has the ability to sniff all packets that pass between communicating devices, but can also inject, modify or delete packets.