Networks and Network Security

Outline

- Network
- Networking Architecture
- Networking Technologies
- Network Models
- Networking Devices
- LAN Technologies
- Networking Topologies
- Network Protocols – TCP/IP

Outline (Cont…)

- Physical Layer
- Data Link Layer
- Network Layer
- Network Layer Protocols
- Transport Layer
- Application Layer
- Security Vulnerabilities in TCP/IP Suite
- Security Mechanisms in Networking Layers

Outline (Cont…)

- Network Security at Network Layer with Internet Protocol Security
- Network Security at Transport Layer
- Network Security at Application Layer
- Network Security with Firewall
- Network Security with Intrusion Detection System and Intrusion Detection and Prevention System

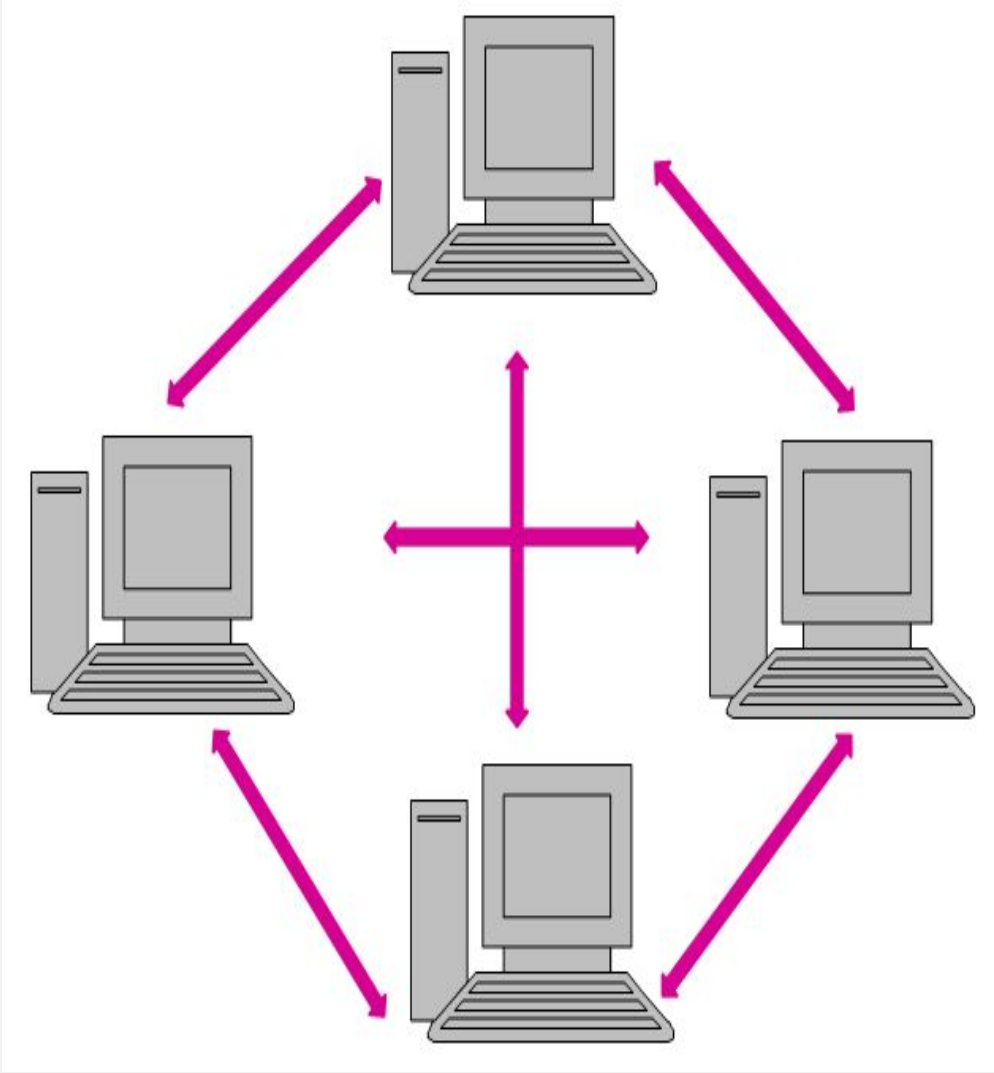
Network

- Collection of computers and devices interconnected by communication channels.

Networking Architecture

Peer-to-Peer network

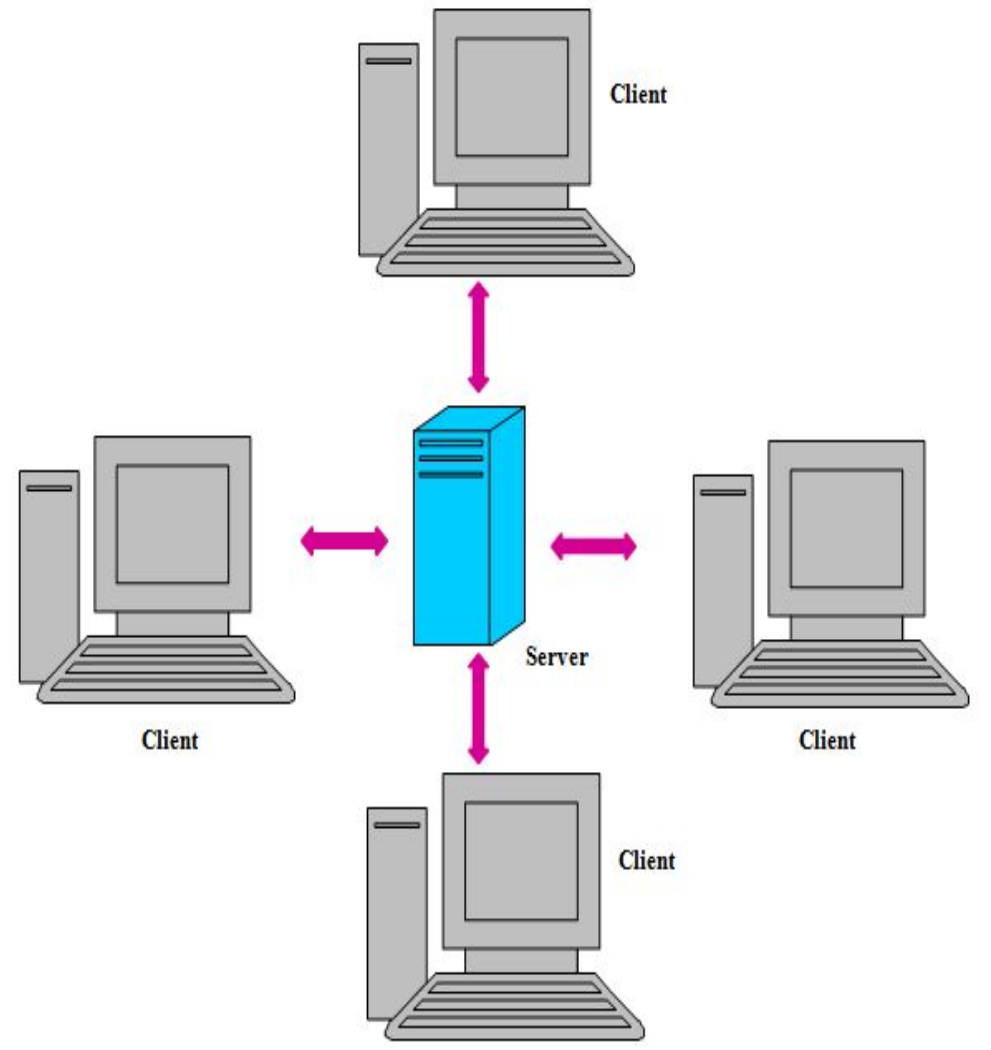
- Any computer can act as a server or a client
- No designated server.



Networking Architecture (Cont…)

Server-based network

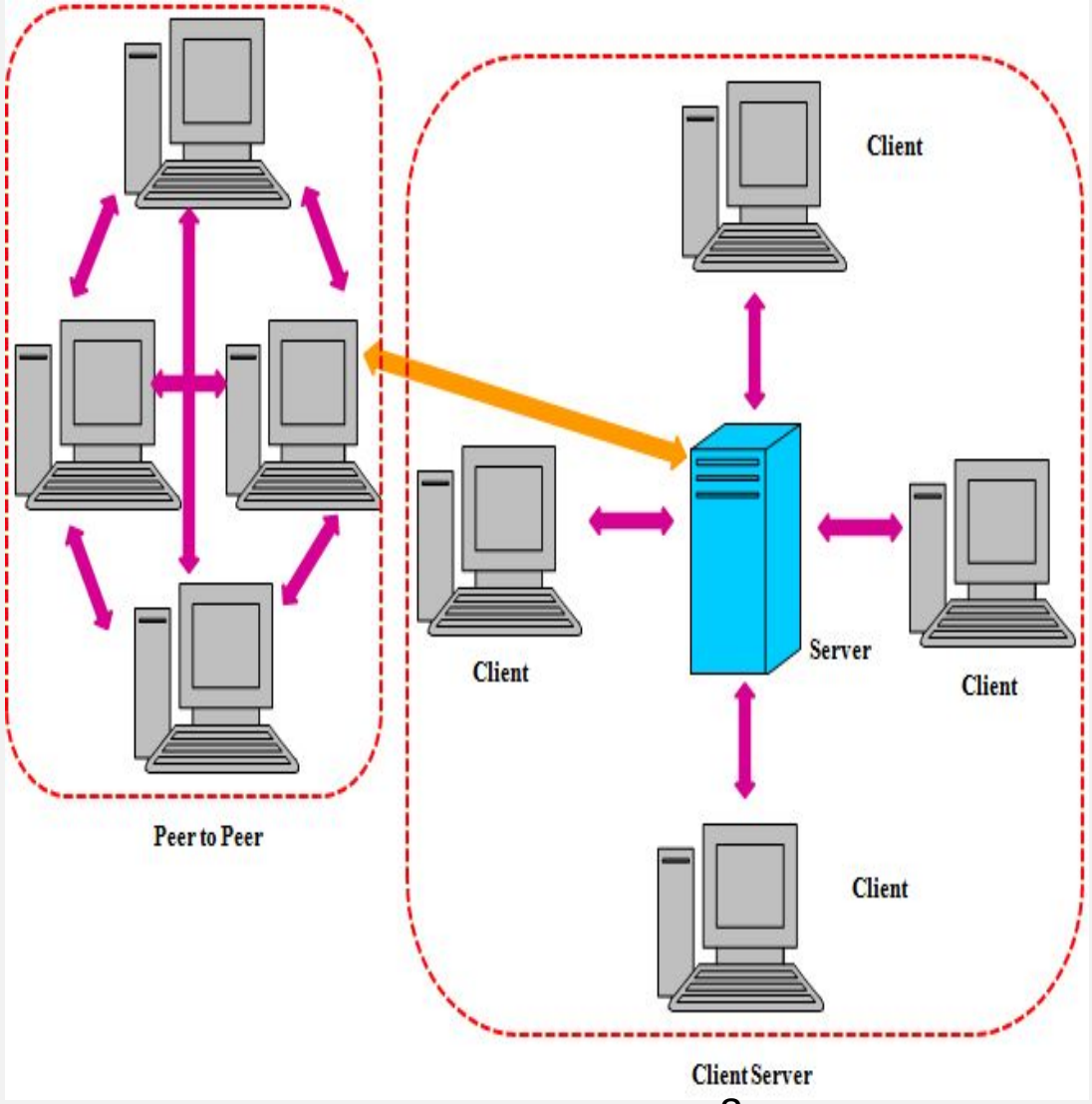
- There is a dedicated server and all the other computers are clients.



Networking Architecture (Cont…)

Hybrid network

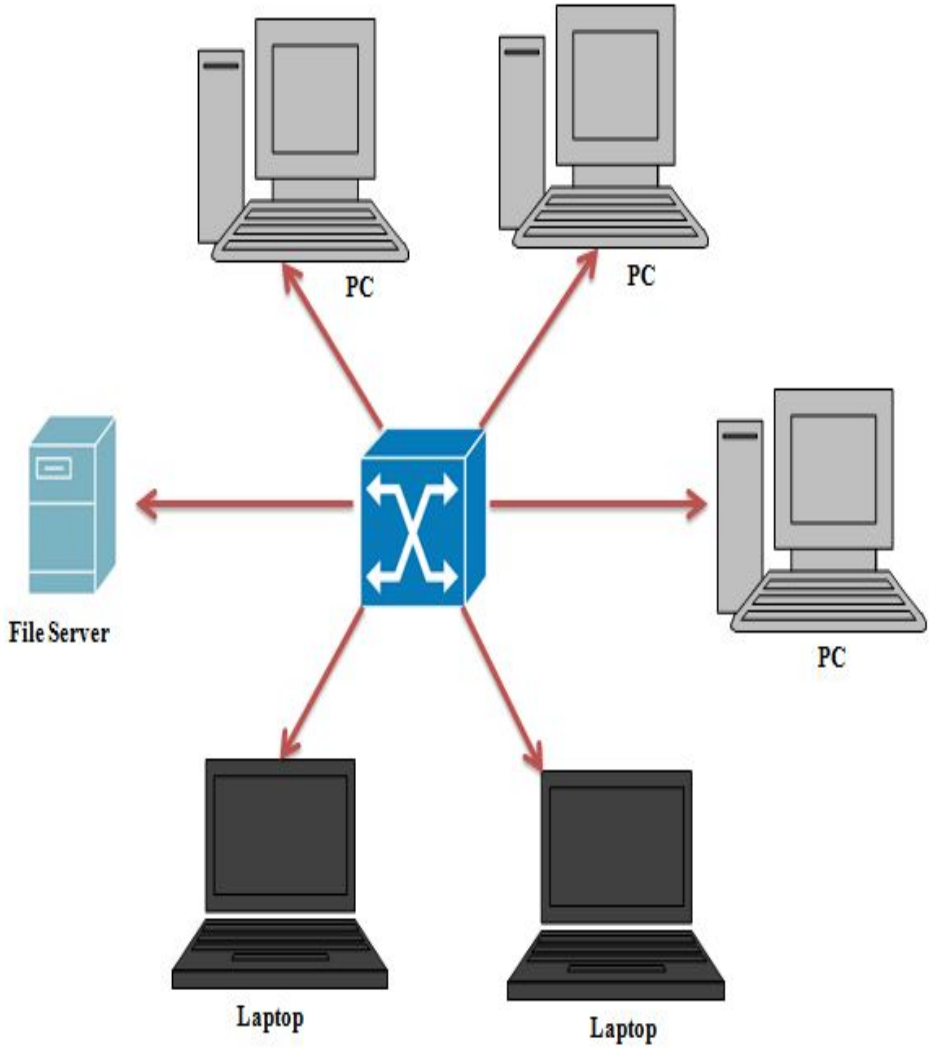
- Combination of both, peer-to-peer network and server-based network.



Networking Technologies

Local Area Network (LAN)

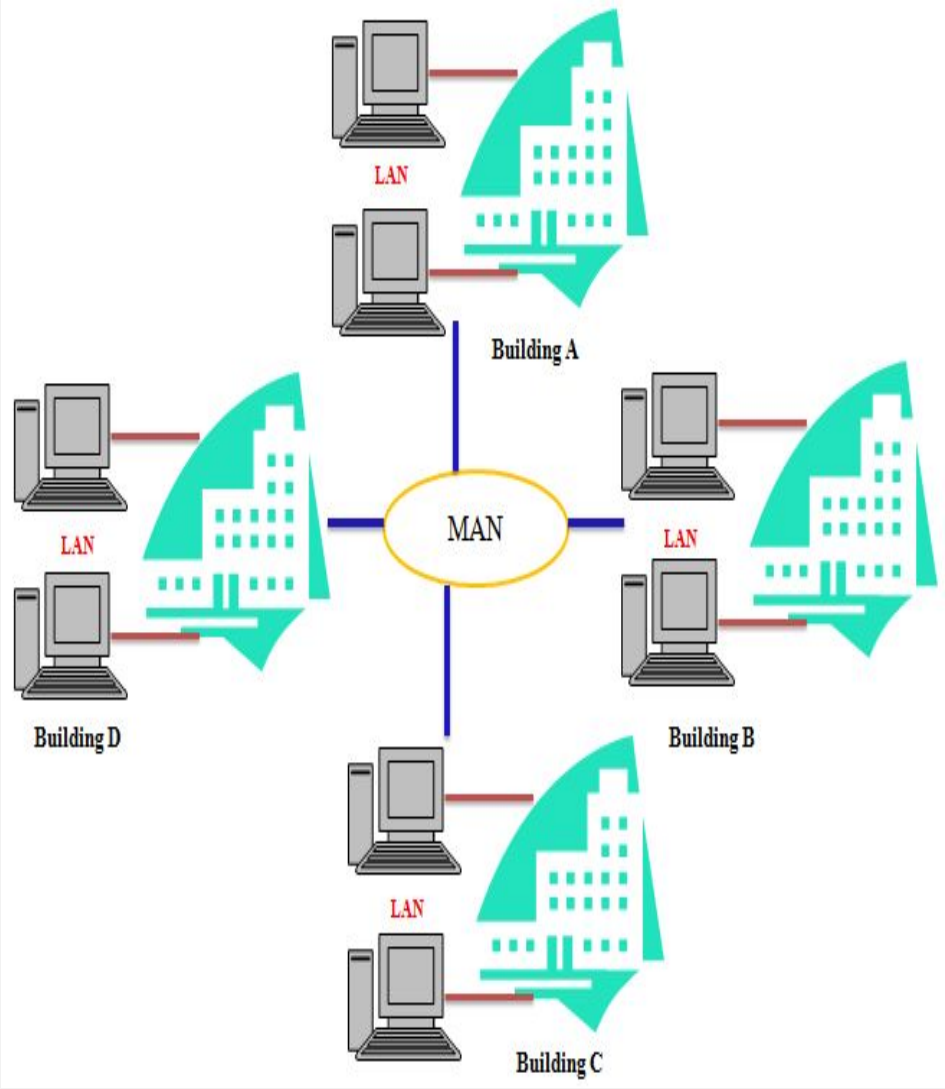
- Configured only if the distance between the computers is not much.
- Spread over a small geographical area (small organizations & home).
- Network Components: Hubs, switches, and cables (Cat-5 and Cat-5e).
- Technology: Ethernet or token ring.
- Wired, wireless or both.



Networking Technologies (Cont…)

Metropolitan Area Network (MAN)

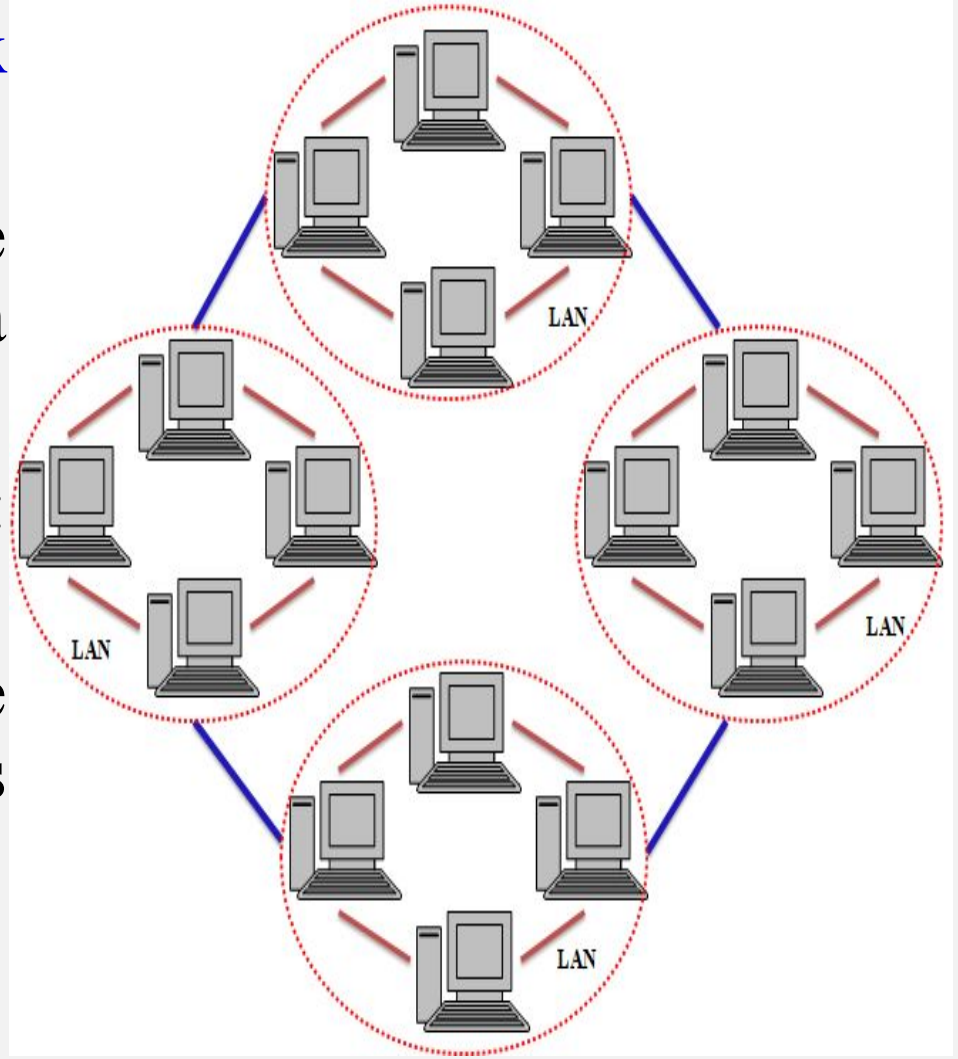
- Configured when the distance between the computers is large.
- Spanning a city or a town.
- Technology: Ethernet, token ring, asynchronous transfer mode (ATM), or fibre distributed data interface (FDDI).



Networking Technologies (Cont…)

Wide Area Network (WAN)

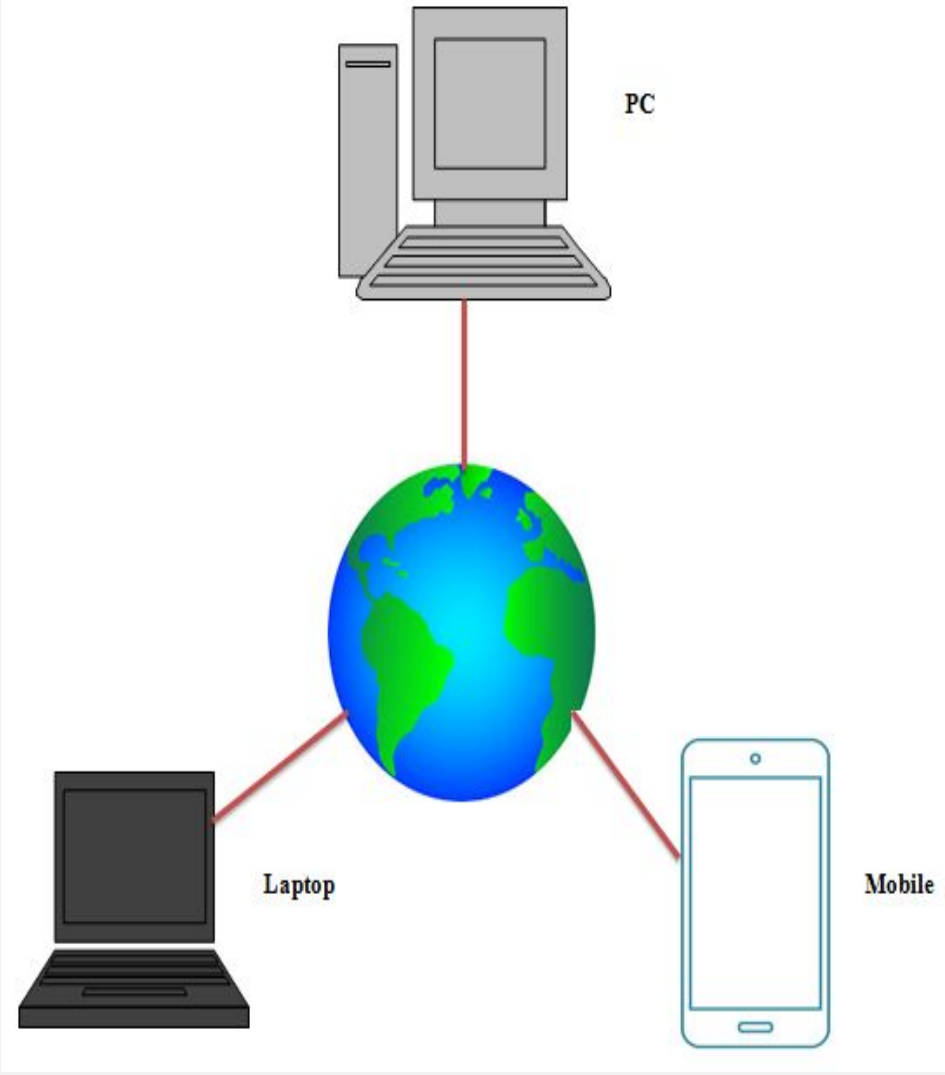
- Configured if the distance between computers spans a large geographical distance.
- Network Component: Router.
- Technology: ATM, frame relay, and synchronous optical network (SONET).



Networking Technologies (Cont…)

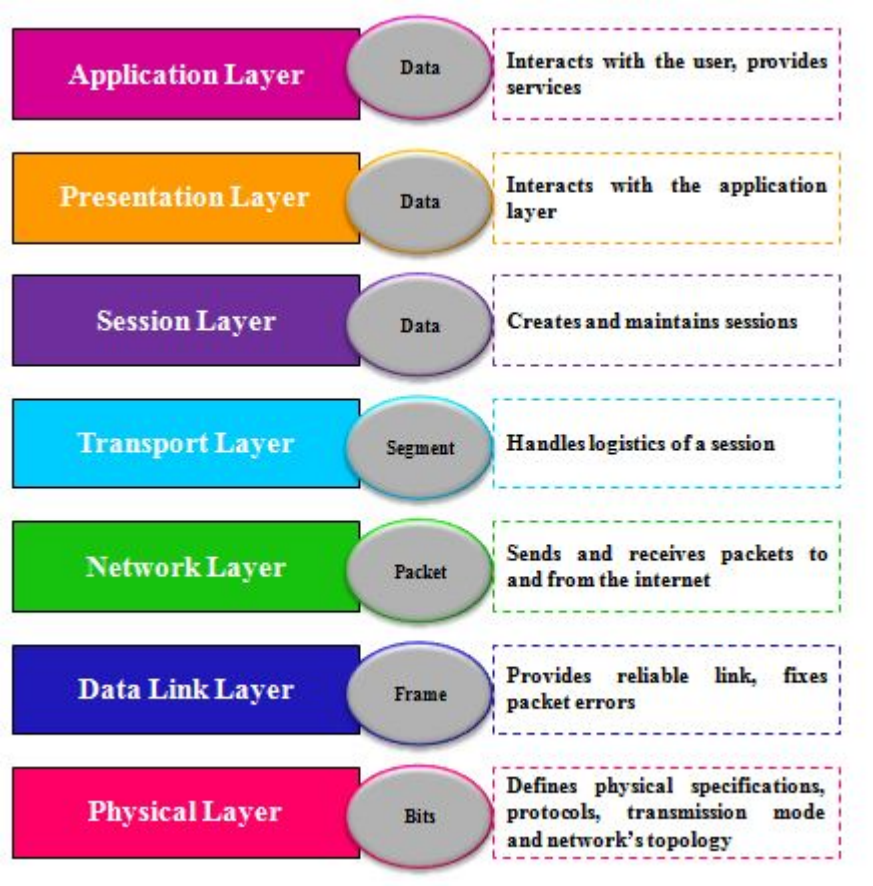
Internetwork

- Network of networks.
- Also called the Internet.
- Interconnects LAN and MAN.



Network Models

OSI Model



Network Models (Cont…)

Internet Model

- ***Layer 4—application layer:*** Enables the user to interact with the network.
- ***Layer 3—transport layer:*** Defines the data flow between hosts.
- ***Layer 2—Internet layer:*** Responsible for host addressing, recognition, and routing.
- ***Layer 1—link layer:*** Responsible for sending and receiving actual data.

Networking Devices

- Used for connecting to a network, routing the packets, strengthening the signal, communicating with others, sharing files on the network, etc.

Repeater

- Regenerate the signal before the signal becomes too weak or corrupted.

Hub

- Connect multiple network hosts.
- Also called multiport repeater.
- Carry out data transfer in terms of packets.

Networking Devices (Cont…)

- ***Passive hub***
  - Forwards the data signal from all the ports except the port on which the signal arrived.
  - No interference with the data signal.
- ***Active hub***
  - Forwards the data signal from all ports except the port on which the signal arrived.
  - Before forwarding, it improves the quality of the data signal by amplifying it.

Networking Devices (Cont…)

Bridge

- Connects two subnetworks.
- ***Local bridge:*** Connects two LAN segments directly.
- ***Remote bridge:*** Connects another bridge over the WAN link.
- ***Wireless bridge:*** ***C***onnects another bridge without any wiring.

Networking Devices (Cont…)

Switch

- A data link layer device.
- Does ‘filtering and forwarding’.

Methods of switching

- *Store and forward:*
  - Basic mode of switching.
  - Buffers the entire frame.
  - Runs FCS to check if the frame is valid or not.
- *Cut and through:*
  - Fastest method of switching.
  - Reads only the first six bytes after the preamble.
- *Fragment free:*
  - Hybrid version of the store and forward method and cut and through method.

Networking Devices (Cont…)

Routers

- Routes data packets based on their IP addresses.

Gateway

- Forward the packets which are intended for the remote network from the local network.
- Also called protocol converters.

Modem

- Stands for *modulator* + *demodulator*.
- Modulates and demodulates the signal between the digital data and the analog signal.

LAN Technologies

Ethernet

- Relies on shared media.
- Uses carrier sense multi access/collision detection (CSMA/CD) technology to detect collisions.

Fast Ethernet

- An extension of ethernet.
- Run on optical fibre and in wireless mode.

Giga Ethernet

- Offers a speed of upto 1000 Mbps.
- IEEE802.3ab defines giga ethernet over UTP.
- IEEE802.3ah defines giga ethernet over fibre.

Virtual LAN

- Enables division of a single broadcast domain into multiple broadcast domains,

Wireless Fidelity

- A wireless technology.
- Cost-effective.

Networking Topologies

- Network topology: Interconnection between computer systems and the networking devices.
- Topology
  - Define both the physical and logical aspect.
  - Defines both logical and physical topologies.
  - Could be the same or different within the same network.

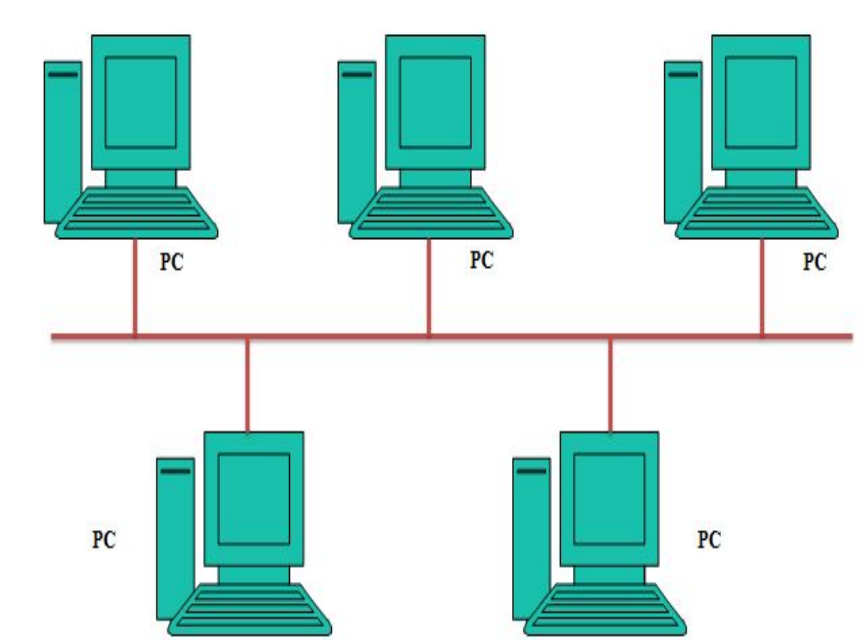
Networking Topologies (Cont…)

Point-to-Point

- Contain exactly two hosts connected back-to-back using a single piece of cable.

Bus Topology

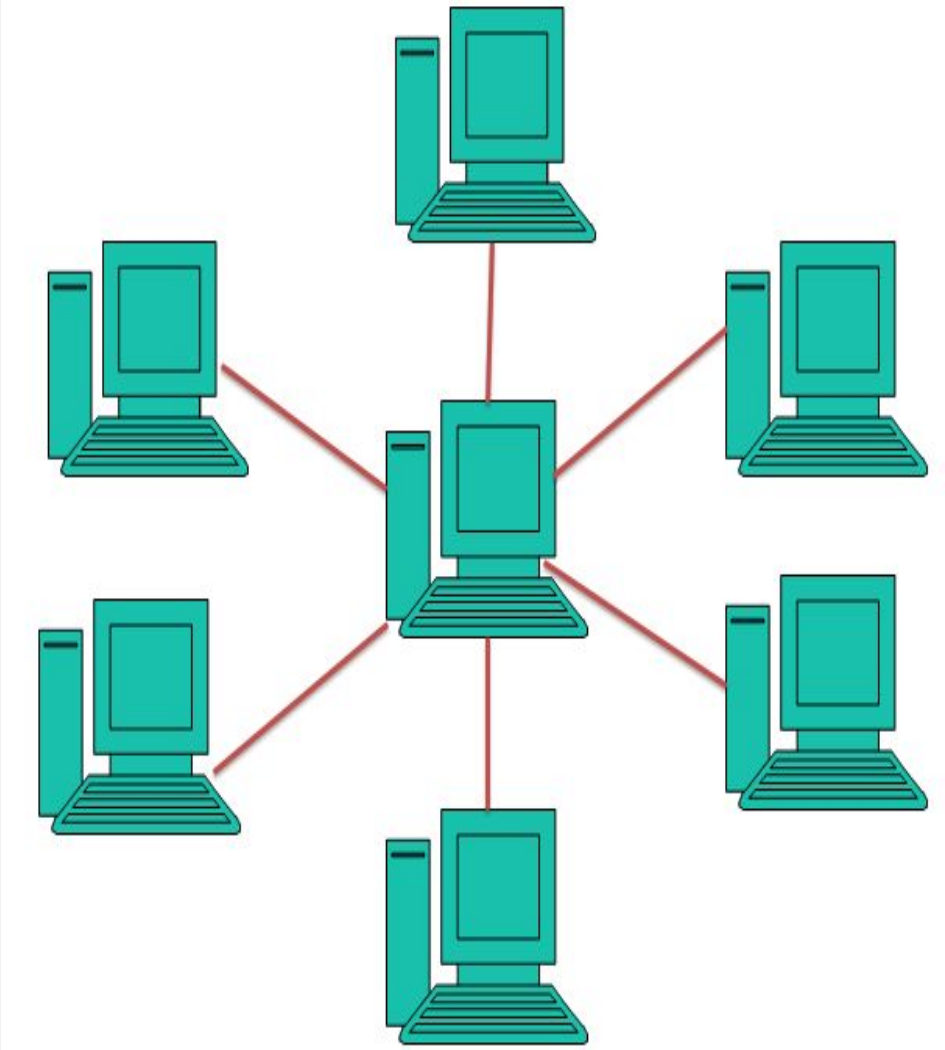
- Share a single communication line or cable.



Networking Topologies (Cont…)

Star Topology

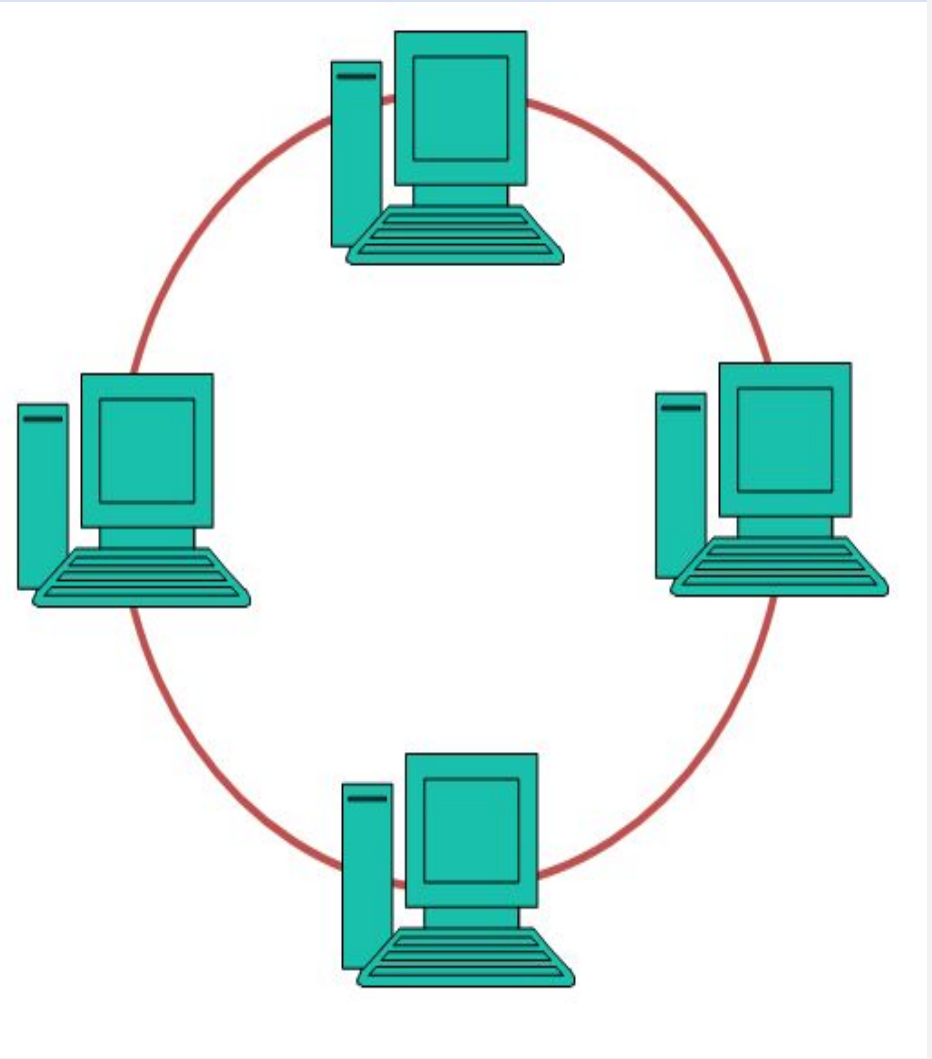
- Connected to a central device known as hub device using a point-to-point connection.
- Active hub: Regenerates and retransmits the signal.
- Passive hub: Mere connection points.



Networking Topologies (Cont…)

Ring Topology

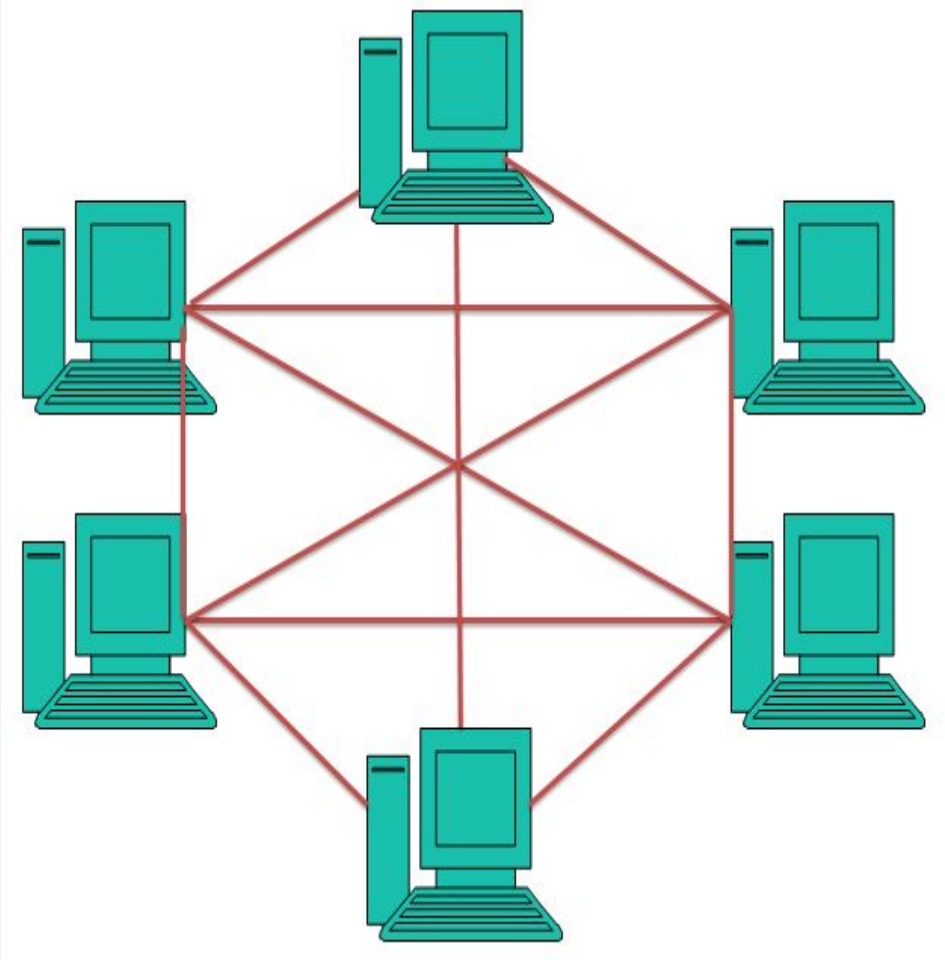
- Every host is connected to exactly two other hosts.



Networking Topologies (Cont…)

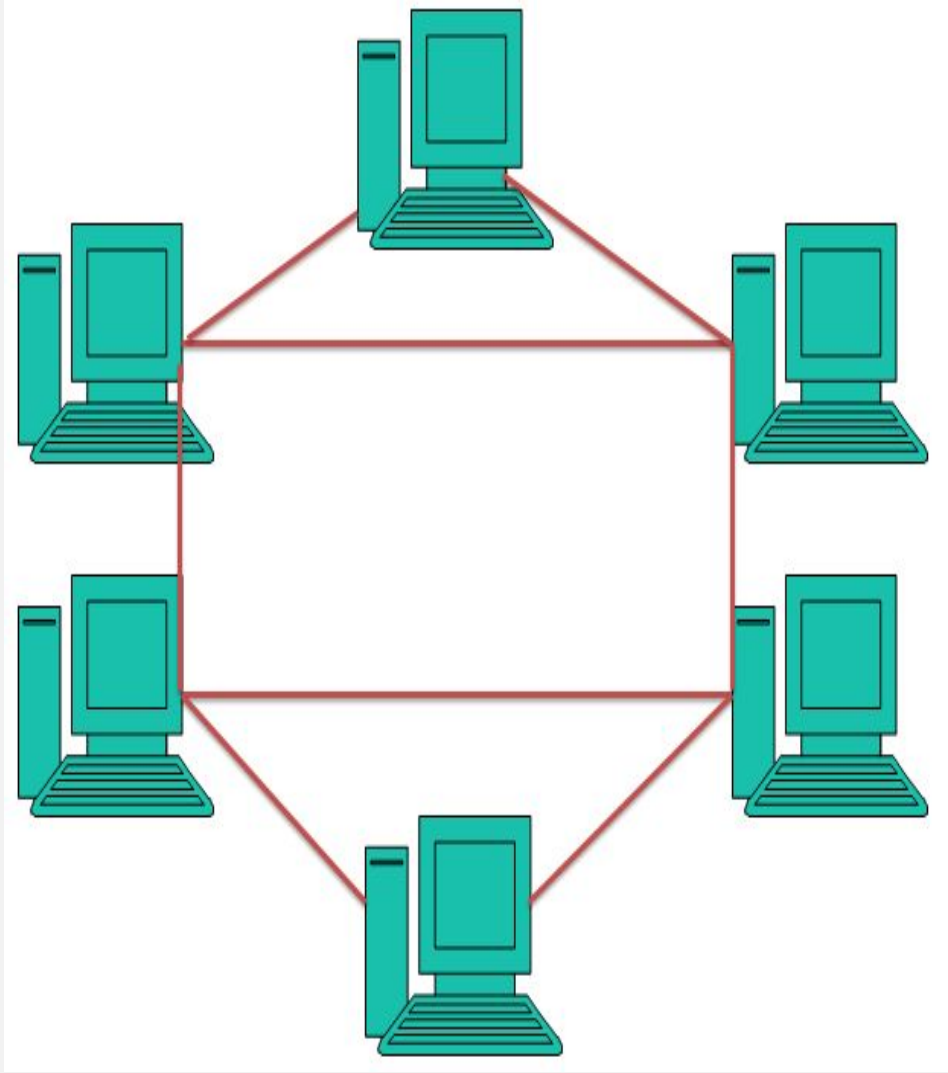
Mesh Topology

- A host is connected to one or more hosts by a point-to-point connection.
- ***Full mesh:*** All hosts have a point-to-point connection to every other host.



Networking Topologies (Cont…)

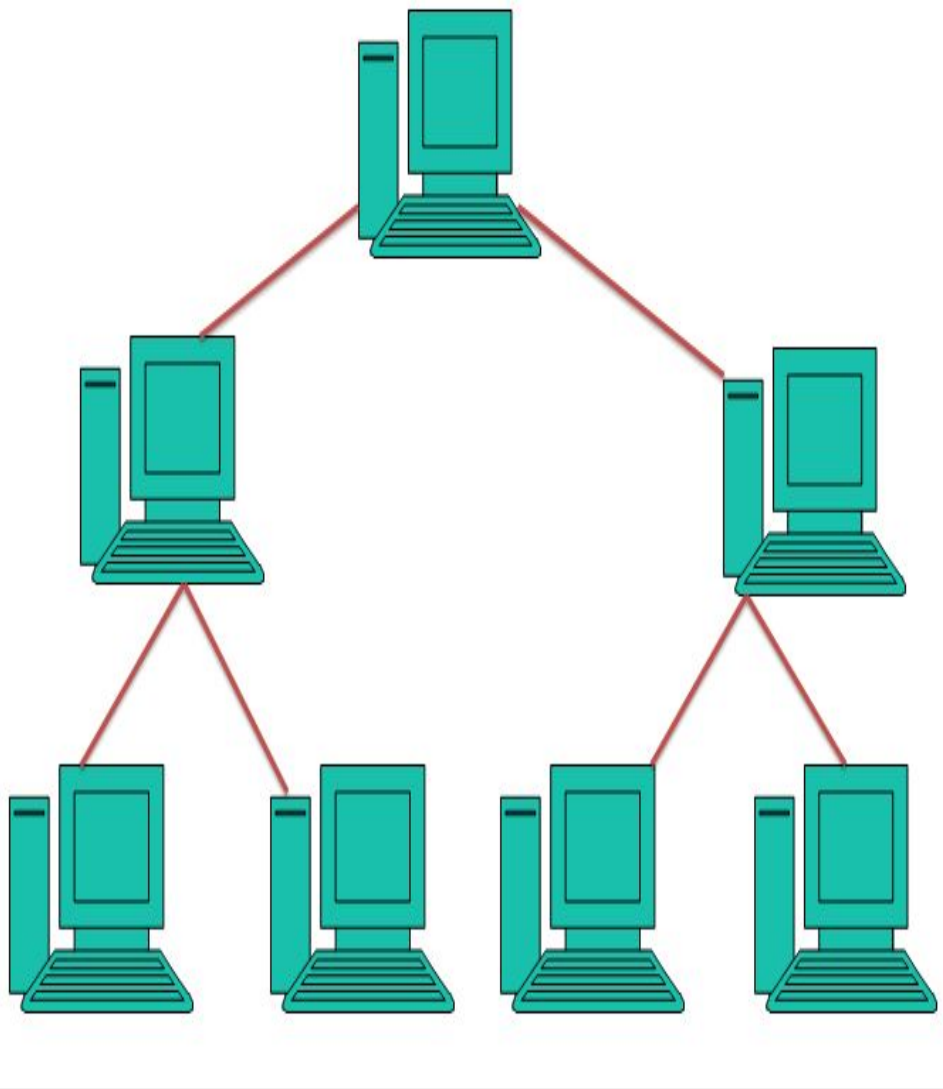
- ***Partial mesh:*** Not all hosts have a point-to-point connection; connected in arbitrary fashion.



Networking Topologies (Cont…)

Tree Topology

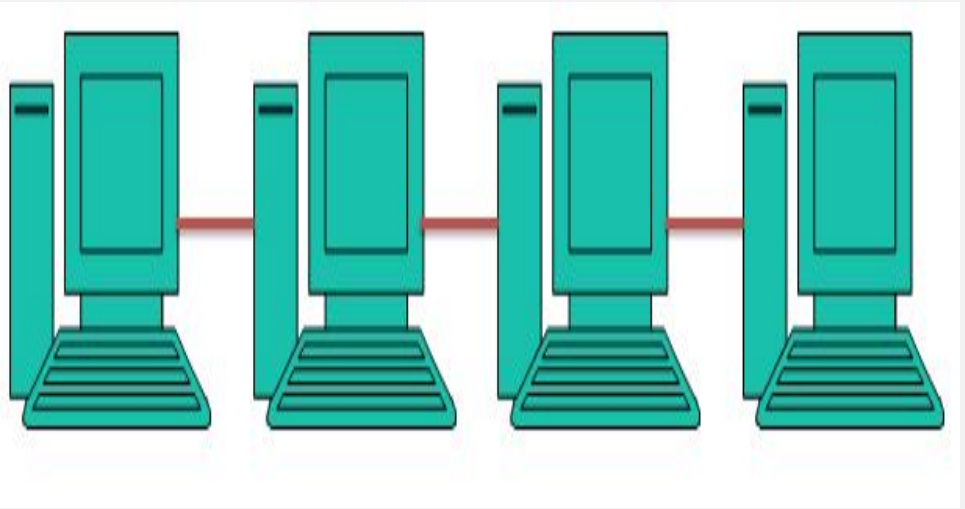
- Most common network topology.
- Presently in use.
- Also called hierarchical topology.
- Divides the network into multiple levels/layers of network.



Networking Topologies (Cont…)

Daisy Chain Topology

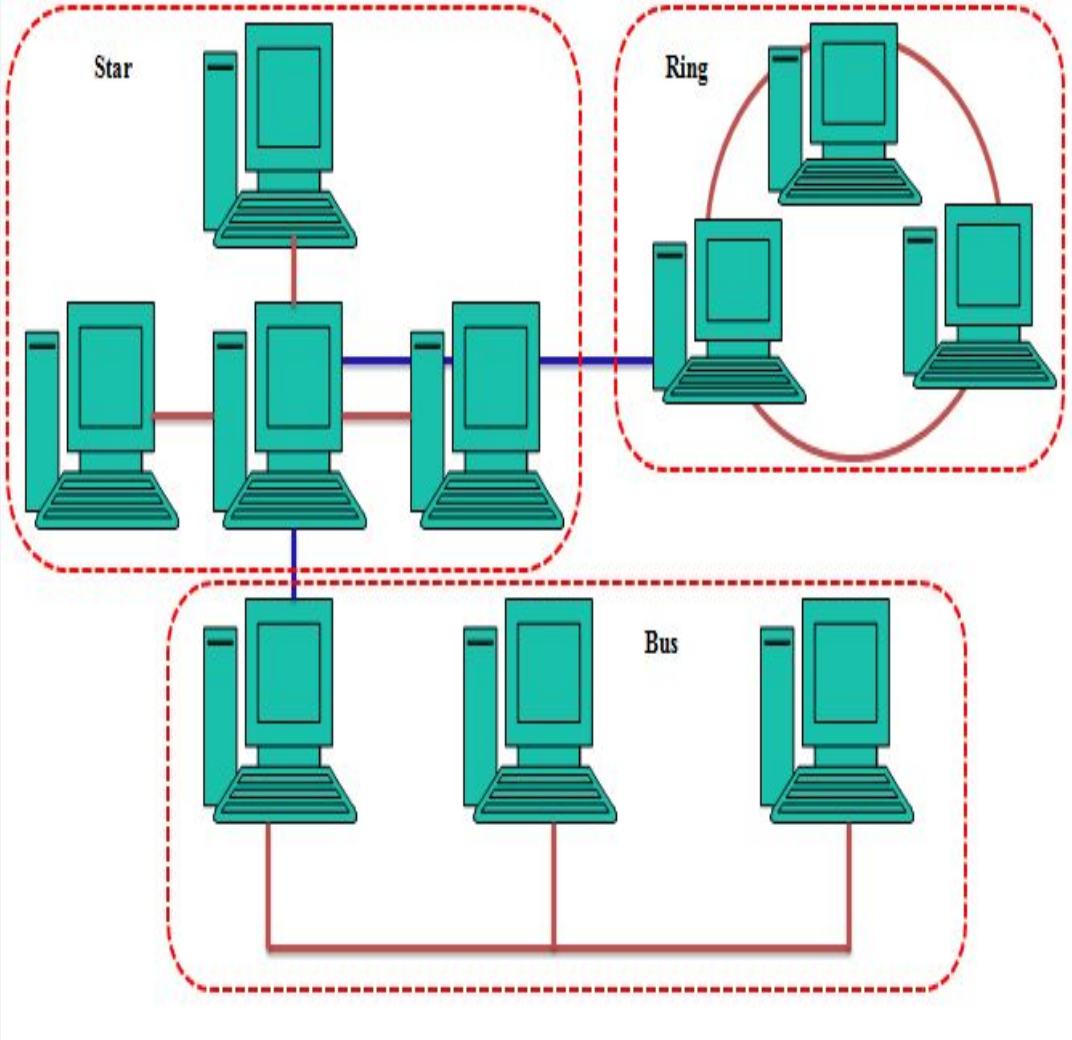
- Connected in a linear fashion.
- Similar to ring topology.
- No connection to the end hosts.



Networking Topologies (Cont…)

Hybrid Topology

- Integrates more than one topology.
- Inherits the merits and demerits of all the incorporating topologies.



Network Protocols – TCP/IP Protocol Suite

- A set of rules that govern communications between devices.

Physical Layer

- Deals with physical connectivity between any two hosts.
- Defines the hardware equipment, cabling, wiring, frequencies, and pulses used to represent binary signals, etc.

Transmission Media

- The transmission media over which data is exchanged between any two hosts.

Physical Layer (Cont…)

- ***Guided media***
  - Wires and cables
  - Information is exchanged or guided through it.
- ***Unguided media***
  - Wireless or open air space.
  - Information is exchanged over air.

Channel Capacity

- Determines the speed of transmission of information
- Depends on factors such as *bandwidth*, *error rate* and the *encoding mechanism*.

Physical Layer (Cont…)

Multiplexing

- Different analog and digital streams of transmission can be simultaneously processed over a shared link.

Switching

- Data or information is sent from the source towards destinations.
- Not directly connected,
- Uses interconnecting devices.
- ***Circuit switching***
  - Establish a dedicated communication path.
  - No other data is transferred over that path.
- ***Message switching***
  - Every switch in the transit path receives the whole message.
  - Buffers until resources are available in the next hop node.
- ***Packet switching***
  - Entire message is broken down into smaller chunks called packets.
  - Switching information is added to the header of each packet.
  - Independent transmission

Data Link Layer

- Hides the details of the underlying hardware.
- Represents to the upper layer as the medium to communicate.
- *Logical link control :* Protocols, flow-control, and error control.
- *Media access control:* Control of media.

Functions

- ***Framing:*** Receives packets from the network layer and encapsulates them into frames .
- ***Addressing:*** Deals with a Layer-2 hardware addressing mechanism.
- ***Synchronization:*** Both the sender and the receiver must be synchronized so as to guarantee correct transfer.
- ***Error control:***
  - Data during transmission is prone to errors
  - Errors may be single-bit, multiple-bit, or burst errors due to noise, crosstalk, etc., and the bits are flipped.
  - Error control attempts to detect such errors and recover actual data bits.
- ***Flow control:*** Both the sender and the receiver exchange data at the same speed.
- ***Multi-access***: Resolves collisions using CSMA/CD.

Data Link Layer (Cont…)

Error Control

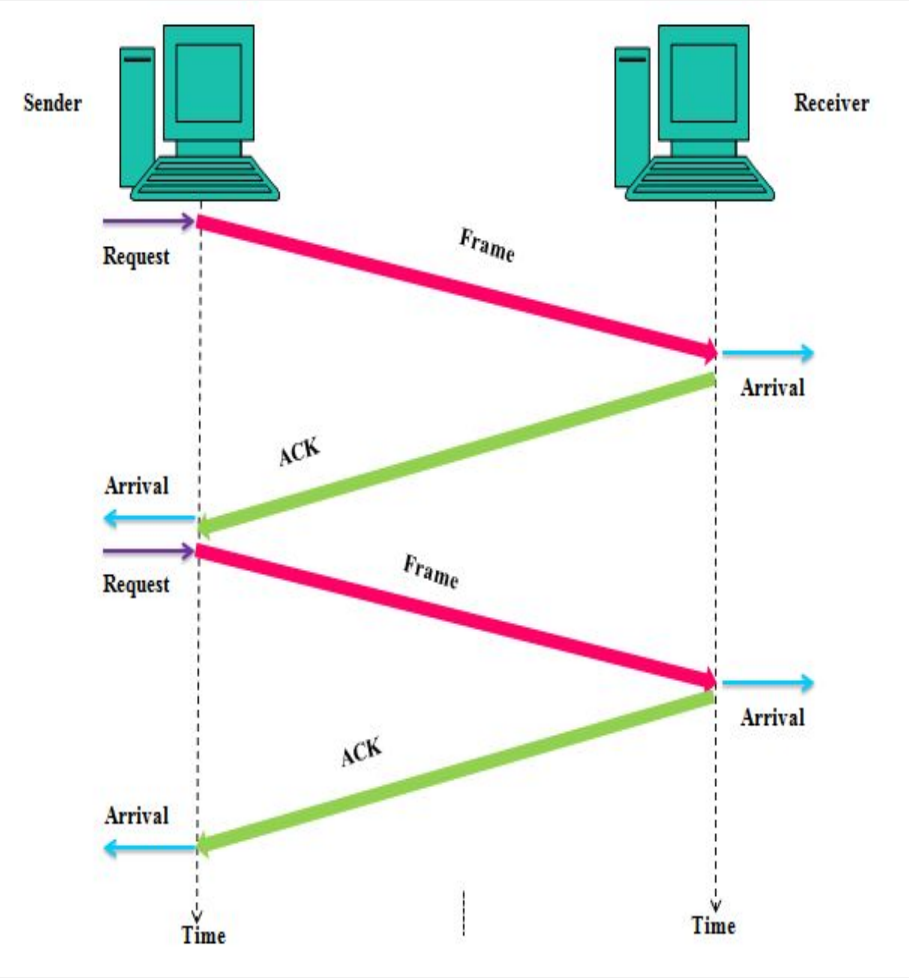
- Uses some error control mechanism to ensure that frames are transmitted with a certain level of accuracy.
- Error control involves *error detection* and *error correction.*
- Error detection: Parity check or cyclic redundancy check.
- *Parity check:* one extra bit is sent along with the original data bits to mark whether the number of 1s is even (in the case of even parity) or odd (in the case of odd parity).
- *Cyclic redundancy check* (CRC): Attempts are made to detect if the received frame contains valid data.

Data Link Layer (Cont…)

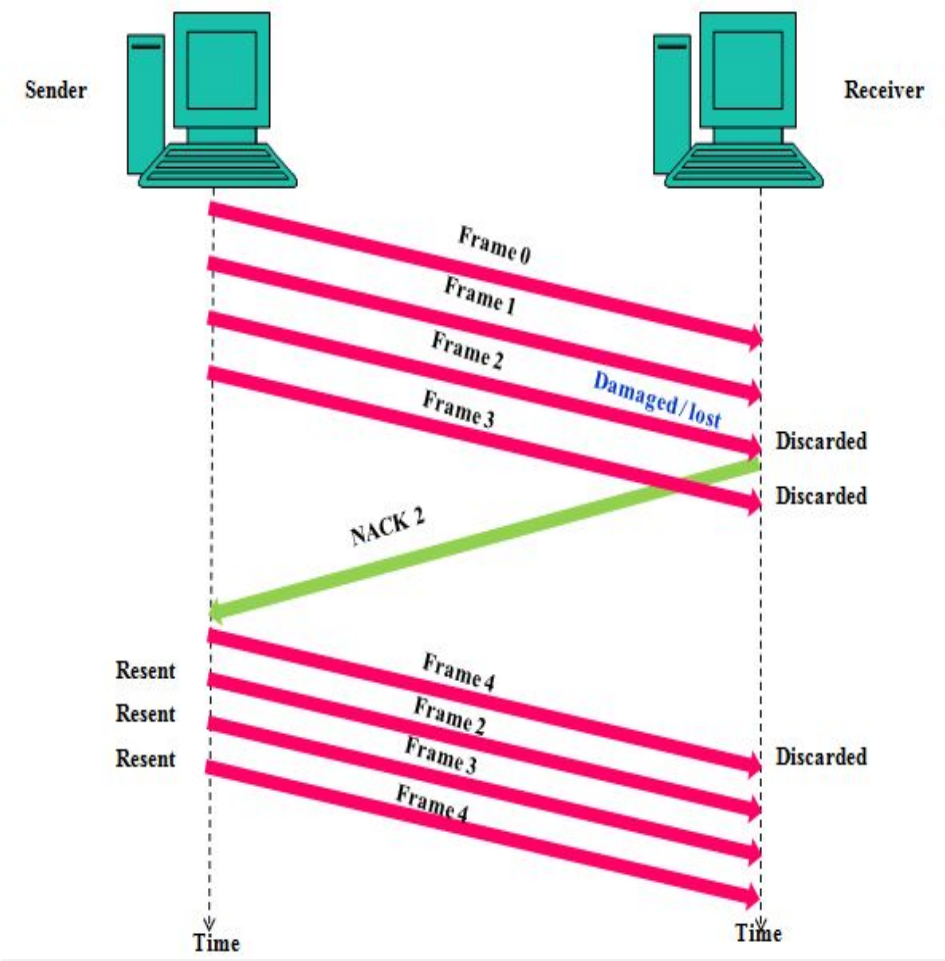
- Error correction mechanisms:
  1. Backward error correction
     - Receiver detects an error in the data received.
     - Requests the sender to retransmit the data.
  2. Forward error correction.
     - Executes error-correcting code.
     - Auto-recover from errors.
- The sender or the receiver should ascertain that there are errors during transit.
- Error control mechanisms or protocols:
  - Stop-and-wait with automatic repeat request (ARQ)
  - Go-back-N ARQ,.
  - Selective repeat ARQ.

Data Link Layer (Cont…)

Stop-and-wait ARQ

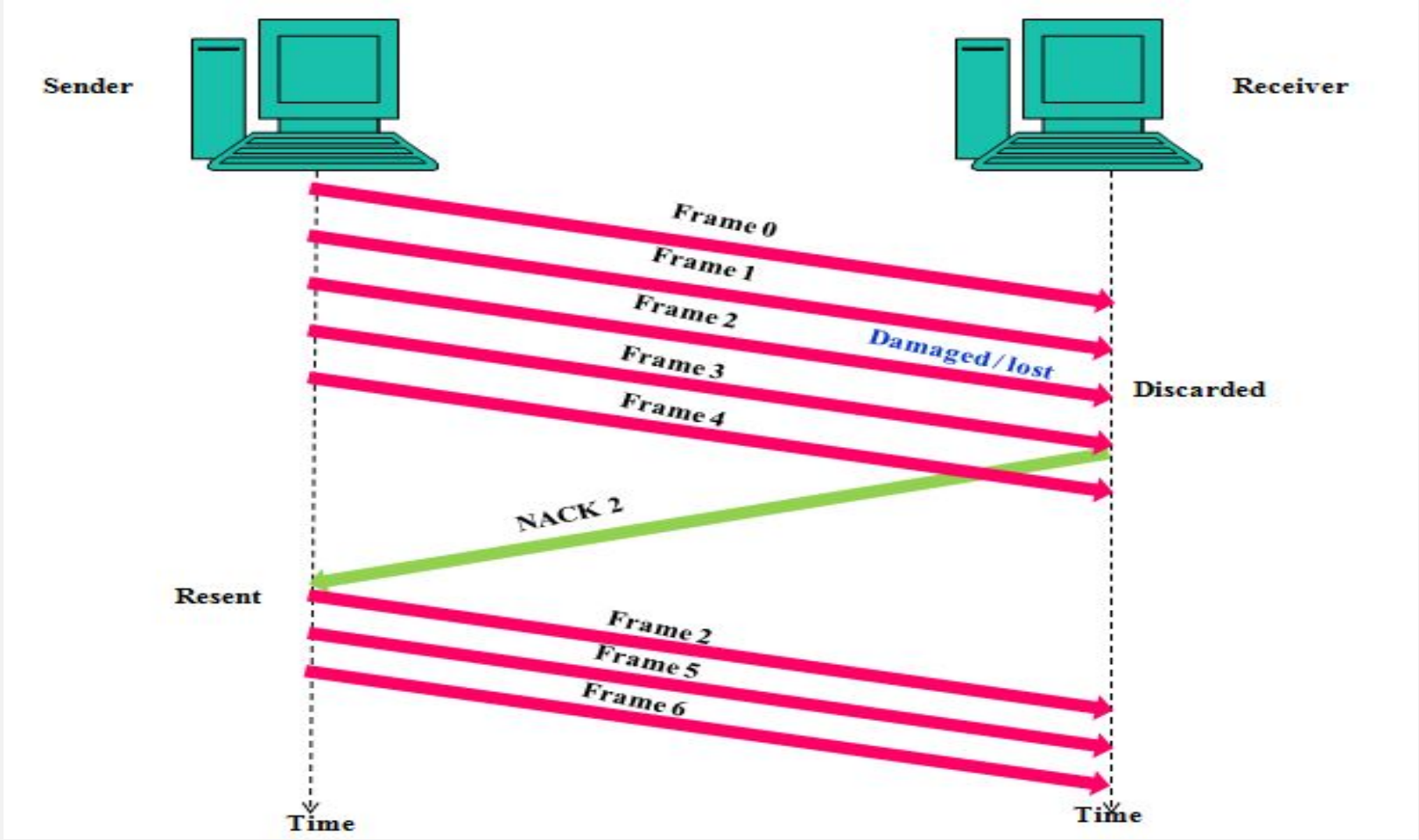


Go-Back-N-ARQ



Data Link Layer (Cont…)

Selective repeat ARQ



Data Link Layer (Cont…)

Flow Control

- Synchronize frames during sending.
- Work at the same speed.

Popular Flow Control Mechanisms

- **Stop and wait:**
  - Forces the sender to stop transmitting a data frame.
  - Waits until an acknowledgement for the previously sent data frame is received.
- **Sliding window:** Eliminates the problem of resource under utilization.

Network Layer

- Responsible for routing packets from the source to the destination.

Network Addressing

- Every node/host is uniquely identified with an IP address.
- This is the network address
- Configured on the NIC.
- This address is mapped to the MAC address for Layer-2 communication.

Network Layer (Cont…)

Routing

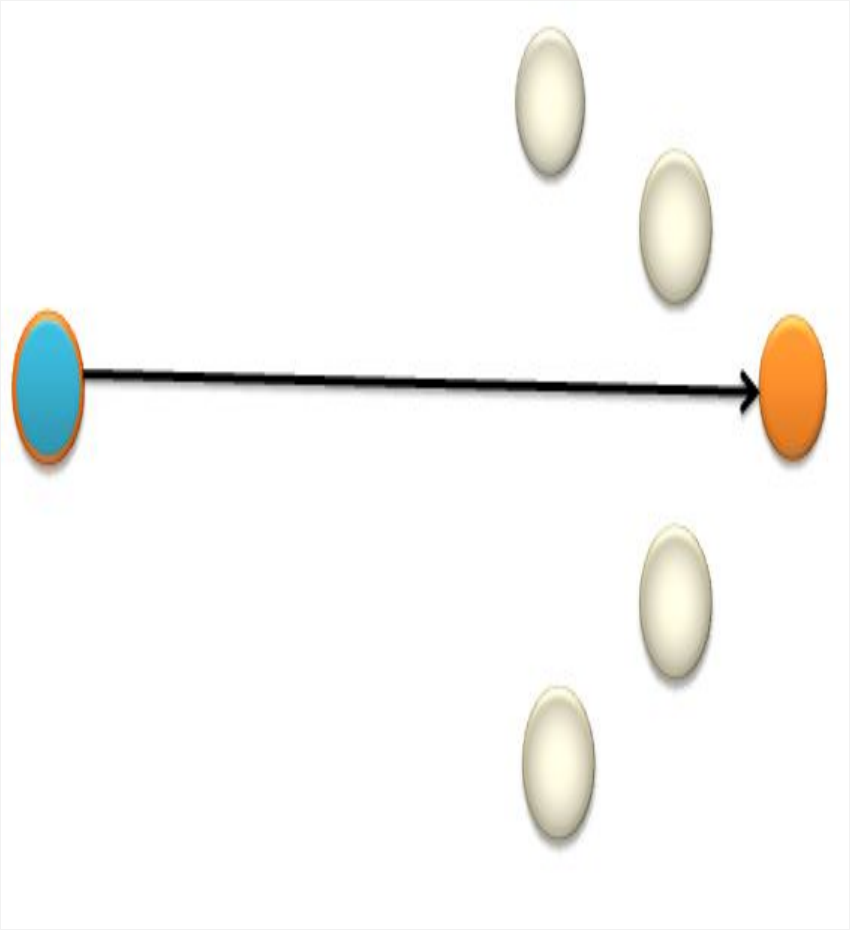
- Process of selecting one among the multiple paths to reach a destination from the routing table.
- Performed by the network device, router.

Network Layer (Cont…)

- **Unicast Routing:** Routing unicast data (from a specific known destination) over the Internet.

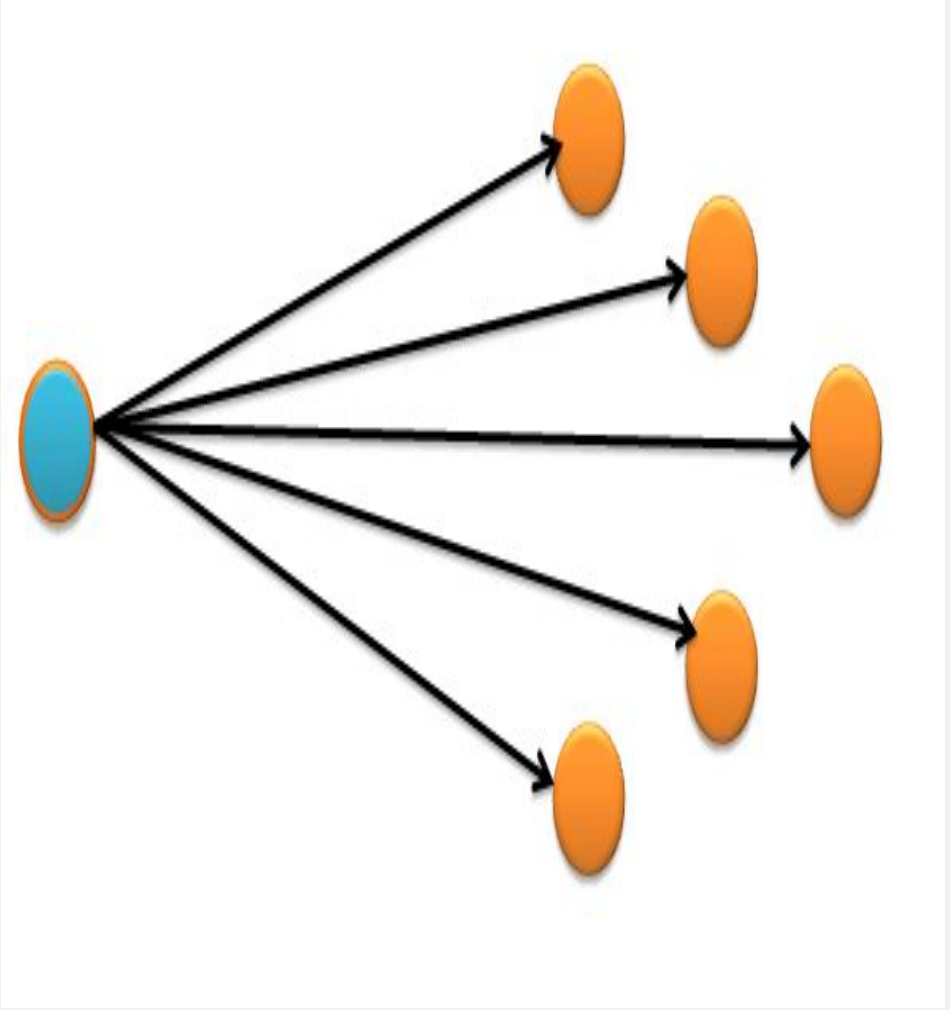
Routing Protocols for unicast

- Distance vector routing protocol
- Link state routing protocol



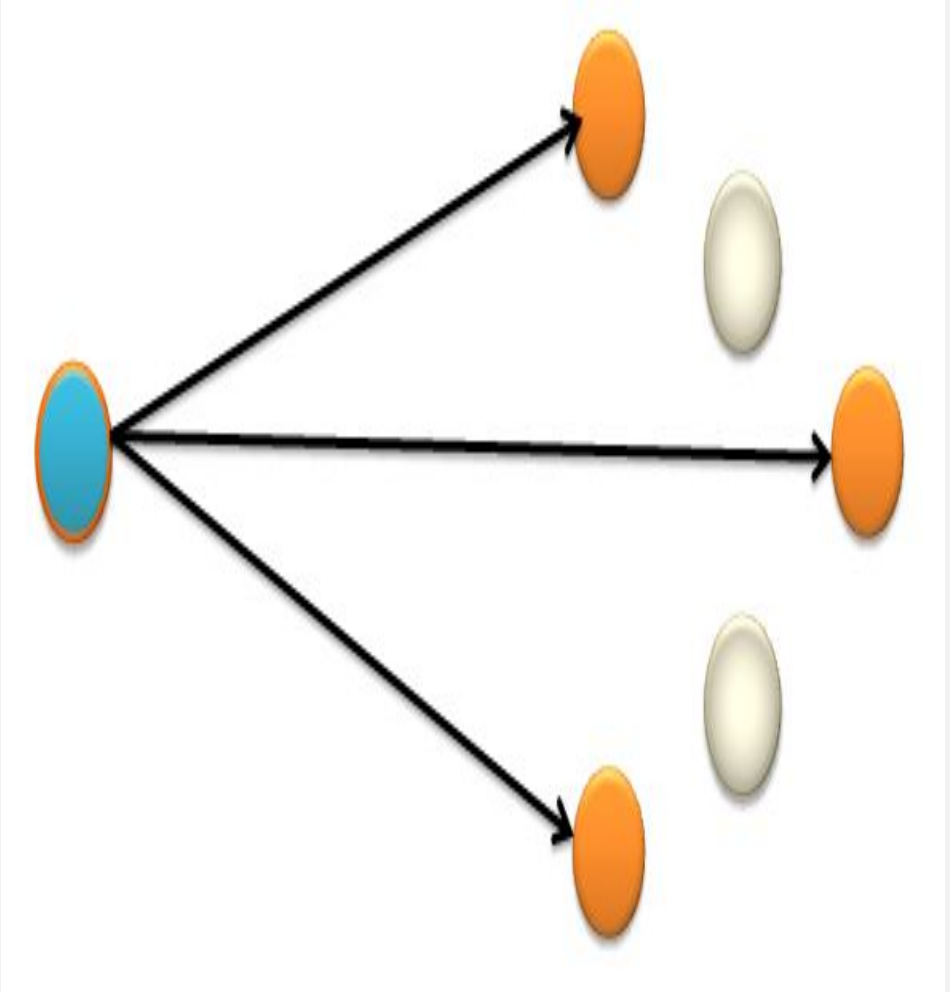
Network Layer (Cont…)

- **Broadcast Routing:** Routing packets to every host and devices in the network



Network Layer (Cont…)

- **Multicast Routing:** Special case of broadcast routing.
- Data packets are only sent to nodes which want to receive the packets.



Network Layer (Cont…)

- **Anycast Routing:** A mechanism where multiple hosts can have the same logical address.
- **Routing Algorithms:** Flooding or shortest path.
- **Flooding:** When a packet reaches a router, it is forwarded through all the interfaces except the one through which it was received.
- **Shortest path:**
  - Performs routing decisions on the basis of cost between source and destination.
  - Considers a path in the network with minimum number of hops.

Network Layer (Cont…)

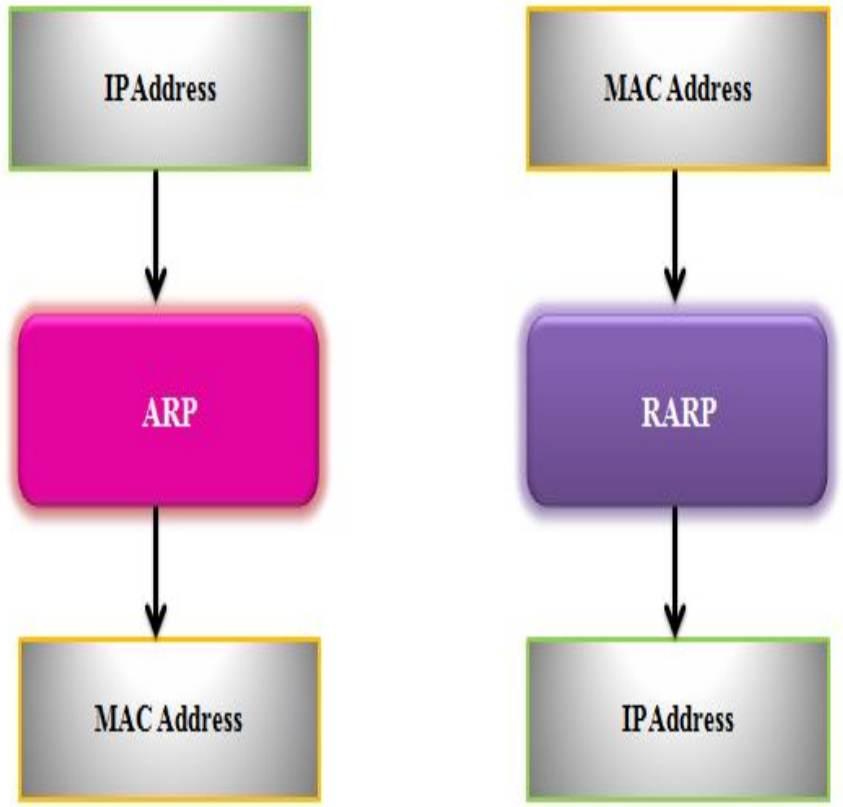
- **Internetworking:** Routing between two networks, either of the same kind or different kind, scattered geographically.
- Interior Gateway Protocols (IGP): Routing protocols used within an organization. e.g. RIP and OSPF.
- Exterior Gateway Protocol (EGP): Routing between different organizations. e. g. Border Gateway Protocol (BGP).
- *Tunneling:* Two networks communicate with each other, by passing intermediate networking complexities.
- *Fragmentation:* If the data packet size is less than or equal to the size of packet the transit network can handle, it is processed neutrally.

Network Layer Protocols

- IP address (Layer-3 address): Logical address which may change every time a computer restarts.
- Communication with the destination host requires its MAC address (Layer-2 address) as well, which is physically burnt into its NIC and never changes.

Address Resolution Protocol and Reverse Address Resolution Protocol

- To initiate a communication, the source should know the MAC address of the remote host on a broadcast domain. It sends out an address resolution protocol (ARP) broadcast message asking, 'Who has this IP address?'.
- Reverse address resolution protocol (RARP): A mechanism wherein a host that knows the MAC address of the remote host gets to know the IP address of the remote host so as to communicate.



Network Layer Protocols (Cont…)

Internet Control Message Protocol

- No inbuilt mechanism for sending error and control messages in IP.
- Internet control message protocol (ICMP), a network diagnostic and error reporting protocol.
- ICMP contains dozens of diagnostic and error reporting messages.
  - **Source quench message**
  - **Parameter problem**
  - **Time exceeded message**
  - **Destination unreachable**

Network Layer Protocols (Cont…)

Internet Protocol Version 4

- Connectionless protocol
- Used in packet-switched layer networks.
- Can be configured either manually or automatically.
- Provides a hierarchical addressing scheme.
- IP addresses are divided into many categories:
  - *Class A:* First octet for network addresses; last octet for host addressing.
  - *Class B:* First two octets for network addresses; last two octets for host addressing.
  - *Class C:* First three octets for network addresses; last one for host addressing.
  - *Class D:* Reserved for multicasting.
  - *Class E:* Reserved for future use.

Network Layer Protocols (Cont…)

Internet Protocol Version 6

- IPv6 is also called Internet protocol next generation (IPng).
- IPv6 addresses are 128-bit wide and are written in hexadecimal separated by colon.
- Has introduced anycast addressing.
- Enables devices to self-acquire an IPv6 address.
- Provides a new feature—that of IPv6 mobility.
- Mobile IPv6-equipped machines can roam around without the need for changing their IP addresses.

Transport Layer

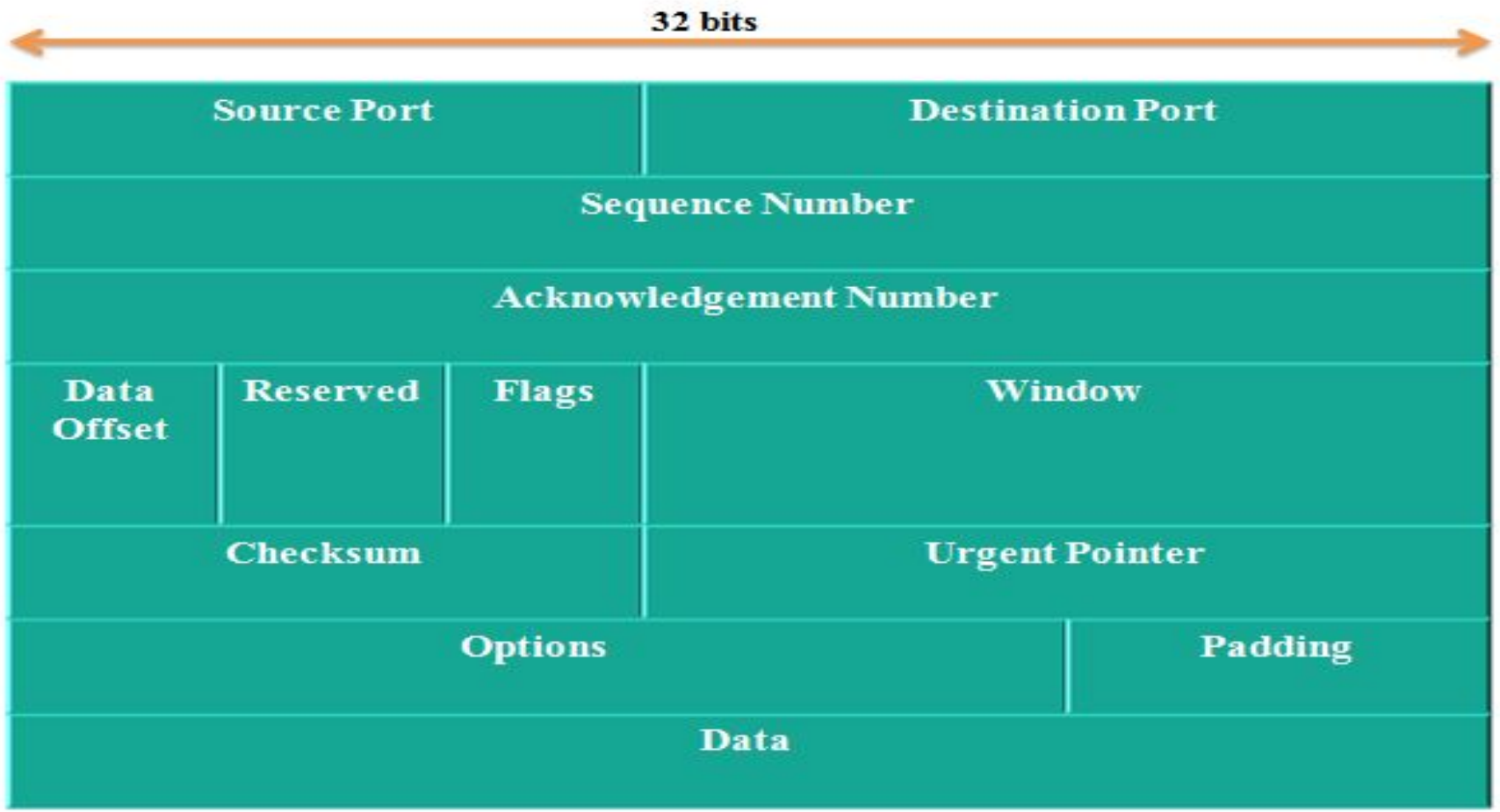
- Responsible for end-to-end connection.

Transmission Control Protocol (TCP)

- A transport layer protocol used by applications that require guaranteed delivery.
- Establishes a full duplex virtual connection.
- **Characteristics**
  - Connection-oriented protocol.
  - Reliable protocol.
  - Operates in point-to-point client/server mode.
  - Ensures the ordering of data.
  - Guarantees end-to-end communication.
  - Provides flow control, error checking, and a recovery mechanism, ensuring QoS.
  - Supports full duplex server.

Transport Layer (Cont…)

- **TCP Header**



Transport Layer (Cont…)

- **Connection Management by TCP**
  - The client initiates the connection and sends the segment with a sequence number. The server either accepts or rejects it.
  - The server acknowledges it with its own sequence number and ACK of the client's segment which is one more than the client's sequence number.
  - The client, after receiving the ACK of its segment, sends an acknowledgement of the server's response.
  - To terminate a connection, either the server or the client sends a TCP segment with FIN flag set to 1. When the receiving end responds by ACKnowledging FIN, the connection is said to have been closed and released.
- **Bandwidth Management by TCP**
  - Uses the concept of window size to manage bandwidth.
  - Window size tells the sender at the remote end, the number of data byte segments the receiver at this end can receive.
- **Error Control and Flow Control in TCP**
  - Uses port numbers to locate the application process and sequence numbers to synchronize itself with the remote host.

Transport Layer (Cont…)

- **Congestion Control in TCP**
  - Slow start, exponential increase.
  - Congestion avoidance, additive increase.
  - Congestion detection, multiplicative decrease.
- **Time Management by TCP**
  - TCP uses different types of timers to control and manage various tasks.
    - Keep-alive timer
    - Retransmission timer
    - Persist timer
    - Timed-wait
- **Crash Recovery in TCP**
  - When a TCP server crashes mid-way during communication and re-starts its process, it sends a transport protocol data unit (TPDU) broadcast to all its hosts.

User Datagram Protocol

- Simplest transport layer communication protocol.
- Involves minimum amount of communication mechanism, compared to TCP.

Transport Layer (Cont…)

- **Characteristics**
  - Stateless protocol.
  - Not connection oriented.
  - Does not guarantee ordered delivery of data.
  - Does not send any acknowledgement.
  - Suitable for data flowing in one direction, query-based communications, streaming applications like VoIP, and multimedia streaming.
  - Does not provide a congestion control mechanism.
- **UDP Header**

Application Layer

- Takes the help of transport and all the layers below it to communicate or transfer its data to the peer application layer protocol on a remote host.
- Any two processes can interact and communicate in any one of the following two ways:
  - Sockets
  - Remote Procedure Call

Application Layer Protocols

- Domain name system
- Simple mail transfer protocol
- File transfer protocol
- Post office protocol
- Hyper text transfer protocol

Security Vulnerabilities in TCP/IP Suite

- Security vulnerabilities exist in the design and implementation of the TCP/IP protocol suite.
- **Vulnerabilities**
  - In HTTP, an application layer protocol in the TCP/IP suite file transfers are made in plain text and so it is easy for an intruder to read the data packets exchanged between the server and a client.
  - A SYN-flooding attack (a kind of DoS attack) can overload the server and lead to a crash
  - IP spoofing can be launched by modification of the IP protocol header.
  - As an attack on DNS, a DNS record can be modified by the attacker to get resolved to an incorrect IP address.
  - ICMP can be exploited to discover all host IP addresses that are alive in a target network with ICMP sweep attack.

Security Mechanisms in Networking Layers

- Security in a TCP/IP protocol-based network is implemented in physical and data link layers at the user terminal and NIC, in the TCP and IP layers at the operating system, and as user process for the layers above TCP/IP.
- Goal: To ensure that the entire network is secure in terms of confidentiality, availability, and integrity.
- Confidentiality: Ensures that the data in the network is available only to intended and authorized recipients.
- Availability: Ensure that the data, network resources, and services are available to intended recipients at all times.
- Integrity: Attempts to make sure that the data in the network is reliable and not altered by unauthorized persons.

Network Security at Network Layer with Internet Protocol Security

- IPSec is a framework for ensuring security at the network layer.
- Security Functions
  - *Confidentiality*
  - *Origin verification and data integrity*
  - *Key management*
- **IPSec Operations**
  - IPSec Communication.
  - Internet Key Exchange.
- **IPSec Communication Modes**
  - Transport Mode
  - Tunnel Mode

Network Security at Network Layer with Internet Protocol Security (Cont…)

IPSec Communication

- Security policies: A rule that is programmed into the IPSec implementation telling it to process different datagrams received by the device.
- Security associations (SA): A set of security information that describes a particular kind of secured connection between one device and another.
- **IPSec Authentication Header:** AH is a protocol that provides authentication of either all or part of the contents of a datagram through the addition of a header that is calculated based on the values in the datagram.
- **IPSec Encapsulating Security Protocol:** Datagrams should be protected from intermediate devices against changes and should be protected from examining their contents. This is achieved with encapsulating security payload (ESP) protocol.

Network Security at Network Layer with Internet Protocol Security (Cont…)

- **Encapsulating Security Payload Fields:**
  - ESP header
  - ESP trailer
  - ESP authentication data

Internet Key Exchange

- Allow devices to exchange information required for secured communication.

Network Security at Transport Layer

- Transport layer security (TLS) protocol is non-interoperable with SSLv3.
- TLS modified the cryptographic algorithms for key expansion and authentication and used open crypto Diffie–Hellman (DH) and digital signature standard (DSS).

Secure Socket Layer (SSL)

- A two-layer protocol with SSL record protocol in the lower layer and an upper layer comprising SSL handshake protocol, change cipher spec protocol, and alert protocol for message exchange and an application protocol for providing information transfer service between client/server interactions.

Network Security at Transport Layer (Cont…)

- **Handshake Protocol of SSL and TLS:** Responsible for the authentication and key exchange necessary to establish or resume secure sessions.
- The handshake protocol manages the following:
  - Cipher suite negotiation.
  - Authentication of server and optionally, client.
  - Session key information exchange.

Transport Layer Security Protocol

- The architecture of the TLS protocol is similar to the SSLv3 protocol.
- It has two sub-protocols: the TLS record protocol and the TLS handshake protocol.

Network Security at Transport Layer (Cont…)

Characteristic	TLS	SSL
Protocol Version in Segment Header	Version Number 3.1	Version Number 3
Message Authentication	Keyed-Hash Message Authentication Code (H-MAC) that can operate with any hash function	MD5 or SHA
Session Key Generation	Computation of Master Secret uses HMAC Standard	Computation of Master Secret uses adhoc-MAC
Supported Cipher Suites	All suites except Fortezza	RSA, Diffie-Hellman and Fortezza cipher suites
Padding of data before encryption	Minimum to make the total data equal to a multiple of cipher's block length	Padding can be any amount up to a maximum of 255 bytes
Alert Protocol Message	Supports more error messages	Supports minimum error messages than TLS

Differences between SSL and TLS

Network Security at Transport Layer (Cont…)

HTTPS

- Provides an encrypted and authenticated connection between the client web browser and the website server thereby ensuring ‘secure’ web browsing.
- Uses one of the two popular transport layer security protocols: SSL or TLS.

Secure Shell Protocol

- Method for secure remote login from one computer to another.
- Provides strong authentication, and protects the communications’ security and integrity with strong encryption.
- SSH is organized as three sub-protocols
  - *SSH user authentication protocol*
  - *SSH connection protocol*
  - *SSH transport layer protocol.*

Network Security at Application Layer

- Email is a widely used application in the application layer, and relies on protocols such as simple mail transfer protocol (SMTP) used for forwarding e-mail messages, post office protocol (POP), and Internet message access protocol (IMAP) to retrieve the messages with the help of a mail client from the server.
- Two schemes have been developed for email security:
- Pretty Good Privacy
- S/MIME

Pretty Good Privacy

- Public key encryption program.
- Most popular standard for email encryption.
- Used to sign messages so that the receiver can verify both the identity of the sender and the integrity of the content.

Network Security at Application Layer

Secure MIME

- An Internet standard for digitally signing MIME-based email data and its public key encryption.
- A technology based on asymmetric cryptography that uses a pair of mathematically related keys to operate, namely a public key and a private key, to encrypt emails and protect it from unwanted access.

DNSSec

- A set of protocols that add a layer of security to the DNS lookup and exchange processes.
- Helps to prevent malicious activities such as cache poisoning, pharming, and man-in-the-middle attacks.

Network Security with Firewall

- A network security device that grants or rejects network access to traffic flows between an untrusted zone (e.g., the Internet) and a trusted zone (e.g., a private or corporate network).
- Firewall may be hardware, software, or a combination of both and is categorized into four types:
  - Network-level
  - Circuit-level Gateway
  - Application-level Gateway
  - Stateful Multilayer Gateways

Network Security with Intrusion Detection System and Intrusion Detection and Prevention System

- Intrusion detection system (IDS) is a device or a software application that monitors the network for any suspicious activity and notifies the network administrator (NA) or the system personnel when a suspicious activity is discovered.
- Two approaches used by IDS to detect intruders: *profile-based detection and signature-based detection.*
- IDS can be classified into three types:
  - Host based Intrusion Detection System – HDS.
  - Network based Intrusion Detection System – NIDS.
  - Hybrid Intrusion Detection System or Hybrid IDS.