Data Communication and Networking

Unit-1

DEFINTION & APPLICATIONS

- **DEFINTION:**

  A computer network is defined as the interconnection of two or more computers. It is done to enable the computers to communicate and share available resources.

- **APPLICATIONS:**

  i. **Sharing of resources such as printers**
  ii. **Sharing of expensive software's and database**
  iii. **Communication from one computer to another computer**
  iv. **Exchange of data and information among users via network**
  v. **Sharing of information over geographically wide areas.**

COMPONENTS OF COMPUTER NETWORK

- Two or more computers
- Cables as links between the computers
- A network interfacing card(NIC) on each computer
- Switches
- Software called operating system(OS)

SHARING RESOURCES

- **Types of resources are:**
  1. **Hardware: A network allows users to share many hardware devices such as printers , modems, fax machines, CD ROM, players, etc.**
  2. **Software: sharing software resources reduces the cost of software installation, saves space on hard disk.**

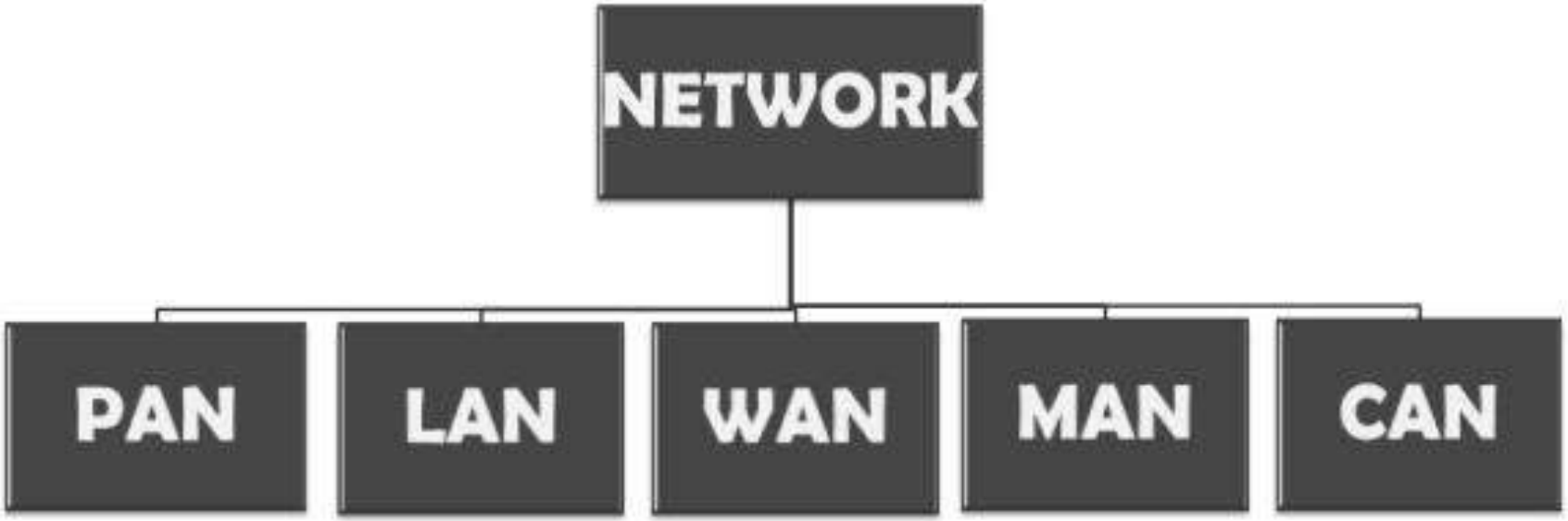
OTHER BENEFITS OF COMPUTER NETWORK

- Increased speed
- Reduced cost
- Improved security
- Centralized software managements
- Electronic mail
- Flexible access

DISDAVATAGES OF NETWORKS

- High cost of installation
- Requires time for administration
- Failure of server
- Cable faults

CLASSIFICATION OF AREA BY THEIR GEOGRAPHY



LOCAL AREA NETWORK(LAN)

- LAN is a network which is designed to operate over a small physical area such as an office, factory or a group of buildings.
- LAN's are easy to design and troubleshoot
- Exchange of information and sharing of resources becomes easy because of LAN.
- In LAN all machines are connected to a single cable.
- Different types of topologies such as star, tree, bus, ring, etc Can be used
- It is usually a privately owned network.

WIDE AREA NETWORK(WAN)

- When network spans over a large distance or when the computers to be connected to each other are at widely separated locations a local area network cannot be used. A wide area network(WAN) is installed.
- The communication between different users of WAN is established using leased telephone lines, satellite links and similar channels.
- It is cheaper and more efficient to use the phone network for the link.
- Most WAN networks are used to transfer large blocks of data between its users.

PERSONAL AREA NETWORK(PAN)

- A personal area network is a computer network organized around an individual person.
- It generally consists of a mobile computer, a cell phone or personal digital assistant. PAN enables the communication among these devices.
- It can also be used for communication among personal devices themselves for connecting to a digital level network and internet.
- The PANs can be constructed using wireless or cables.

CAMPUS AREA NETWORK(CAN)

- The campus area network is made up of an interconnection of LAN with limited geographical area.
- Network equipments such as switches, routers and the transmission media i.e. optical fibre etc are almost entirely owned by the campus owner.

METROPOLITAN AREA NETWORK(MAN)

- It is in between LAN & WAN technology that covers the entire city.
- It uses similar technology as LAN.
- It can be a single network such as cable TV network, or a measure of connecting a number of LAN's o a large network so that resources can be shared LAN to LAN as well as device to device.

Uses of Computer Network

- Simultaneous Access
- Shared Peripheral Devices
- Personal Communication
- Easier Backup

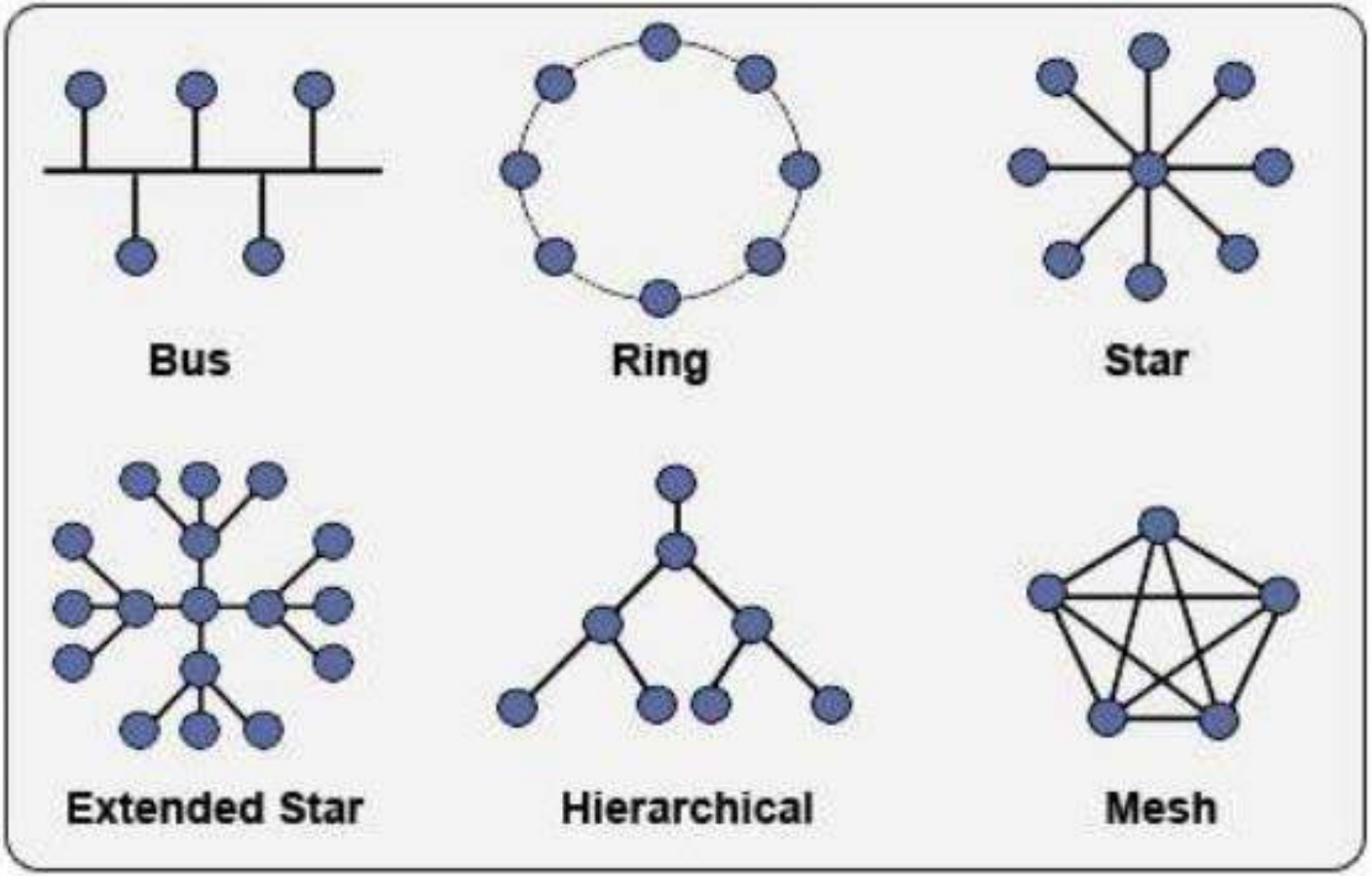
❖ What are Networking Devices ?

- Network devices are components used to connect computers or other electronic devices together so that they can share files or resources like printers or fax machines. Devices used to setup a Local Area Network (LAN) are the most common type of network devices used by the public. A LAN requires a hub, switch, router.
- Networking Devices are also called Communicating Devices.

Types of Nodes

- A typical network includes several nodes; some nodes act as server, some as client, and some as both server and client
- Server
  - a server is a node that makes its resources available to and for use by other network nodes; therefore, a server shares its resources across the network
- Client
  - a client is a node that requests and uses resources on a network which are made available and shared by a server on the network

Network Topology



The need for protocols

- Basic communication hardware can transfer bits from one place to another
- Communication software provides a convenient high level interface for application programmers
  - do not have to deal directly with hardware
  - can run over different hardware
- A set of rules for exchanging messages is a *network protocol*

Common networking issues

- Sequencing for out-of-order delivery
- Sequencing to eliminate duplicate packets
- Re-transmitting lost packets
- Avoiding replay caused by excessive delay
- Flow control to prevent data overrun
- Mechanisms to avoid network congestion

Difference between Connection Oriented and Connectionless Services

Sr no.	Connection Oriented Services	Connectionless Services
1.	It needs authentication.	It doesnot need authentication.
2.	It gurantees a delivery	It doesnot gurantee a delivery
3.	It is more reliable	It not that reliable
4.	Connection Oriented is stream based	Connectionless is message based.

Connection-oriented and connectionless services

- Connection-oriented service is modeled after the telephone system
  - To talk to someone, you pick up the phone, dial the number, talk, and then hang up
  - To use a connection-oriented network service, the service user first establishes a connection, uses the connection, and then releases the connection.
- Connectionless service is modeled after the postal system
  - Each message (letter) carries the full destination address, and each one is routed through the system independent of all the others.

Network Applications

Outline

- File Transfer Protocol
- Telnet
- Simple Mail Transfer Protocol
- Peer-to-peer applications (Napster, Gnutella)

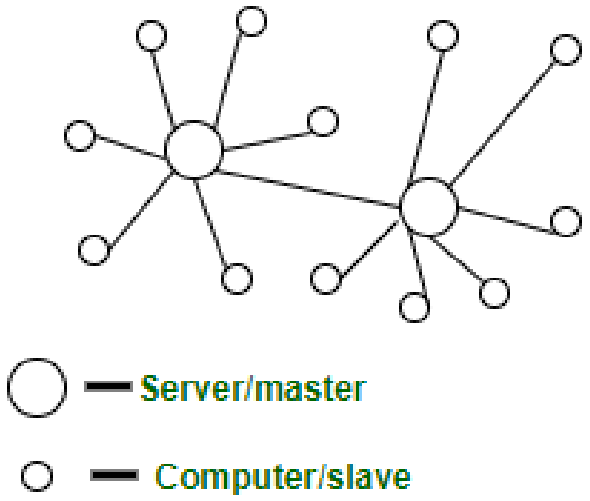
CENTRALIZED SYSTEMS:

- Centralized systems are systems that use client/server architecture where one or more client nodes are directly connected to a central server. This is the most commonly used type of system in many organizations where client sends a request to a company server and receives the response.

  Components of Centralized System are
- Node (Computer, Mobile, etc.)
- Server
- Communication link (Cables, Wi-Fi, etc.)

Decentralized systems

- In decentralized systems, every node makes its own decision. The final behavior of the system is the aggregate of the decisions of the individual nodes. Note that there is no single entity that receives and responds to the request.



1. What is a Distributed System?

Definition: A *distributed system* is one in which components located at networked computers communicate and coordinate their actions only by passing messages. This definition leads to the following characteristics of distributed systems:

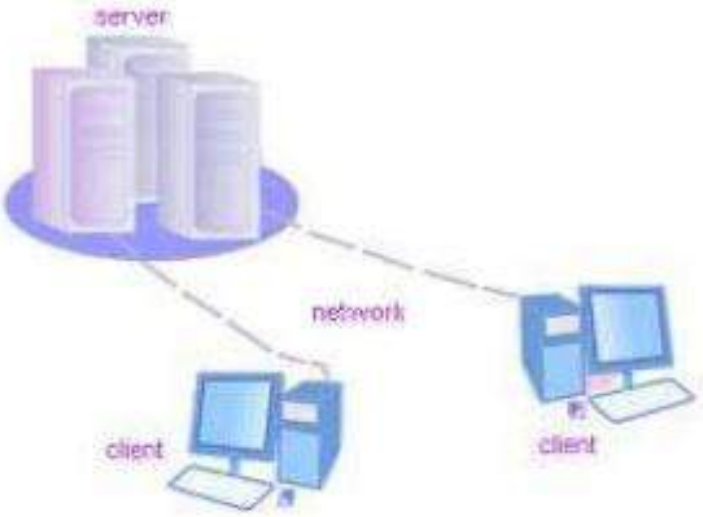
- concurrency of components
- lack of a global clock
- independent failures of components

3. Examples of Distributed Systems

- Local Area Network and Intranet
- Database Management System
- Automatic Teller Machine Network
- Internet/World-Wide Web
- Mobile and Ubiquitous Computing

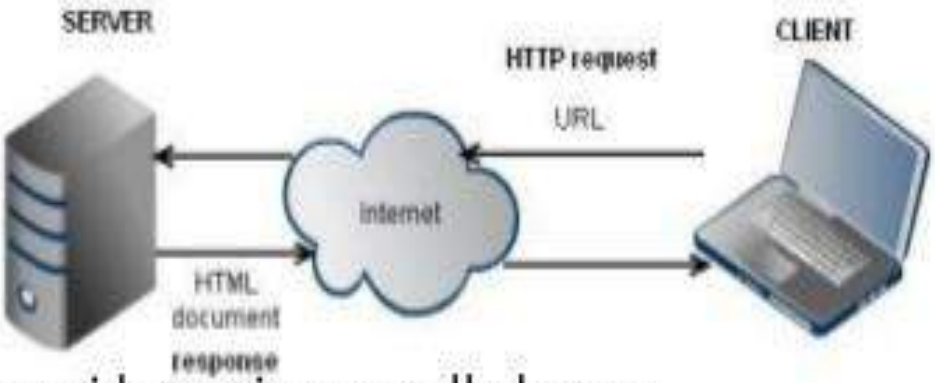
Definition

The term '**Client-Server**' refers to the Network Architecture. where one or more computers are connected a server.



That one computer *(the Client)* or more sends a service request to another computer *(the Server)*.

CLIENT SERVER MODEL

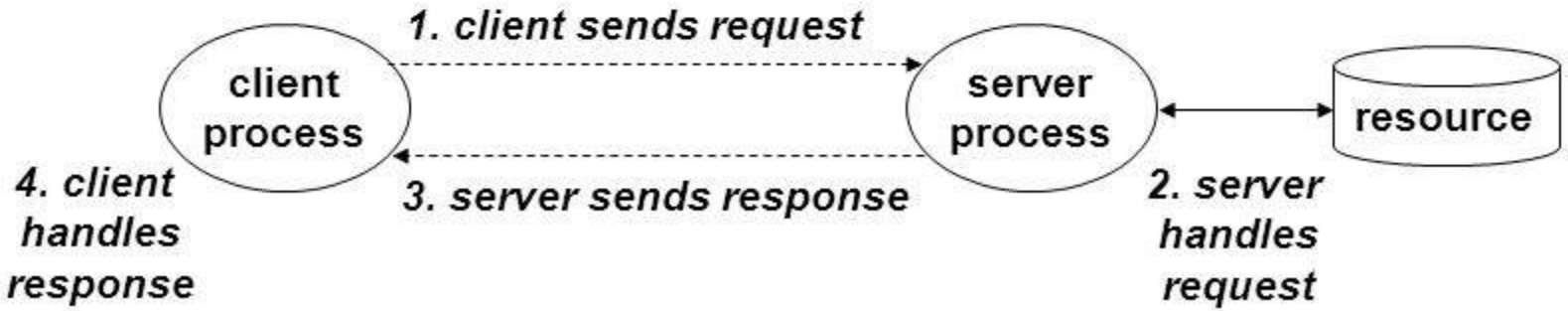


- Request service, called clients and provide service are called sever
- Server is often designed to be a centralized system that serves many clients.
- Clients and servers communicate over a computer network on separate hardware
- Clients and servers exchange messages in a request response messaging pattern
- To prevent abuse and maximize uptime, the server's software limits how a client can use the server's resources.
- A denial of service attack exploits a server's obligation to process requests by bombarding it with requests incessantly

Client-server model

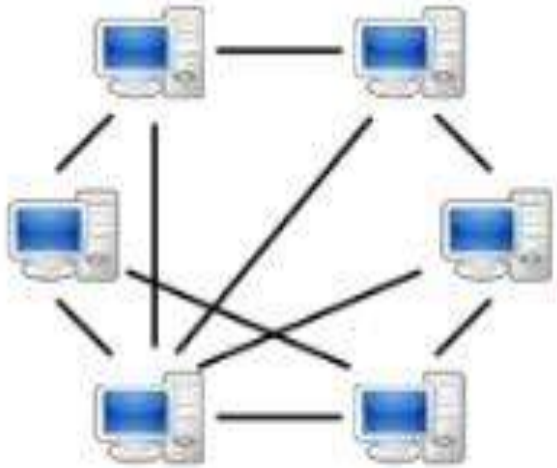
Every network application is based on the client-server model:

- Application is a *server* process and one or more *client* processes
- Server manages some *resource*, and provides *service* by manipulating resource for *clients*.
- Client makes a request for a service
  - request may involve a conversation according to some server protocol
- Server provides service by manipulating the resource on behalf of client and then returning a response



Architecture

- A peer-to-peer network is designed around the notion of equal *peer* nodes simultaneously functioning as both "clients" and "servers" to the other nodes on the network.
- This model of network arrangement differs from the client-server model where communication is usually to and from a central server.



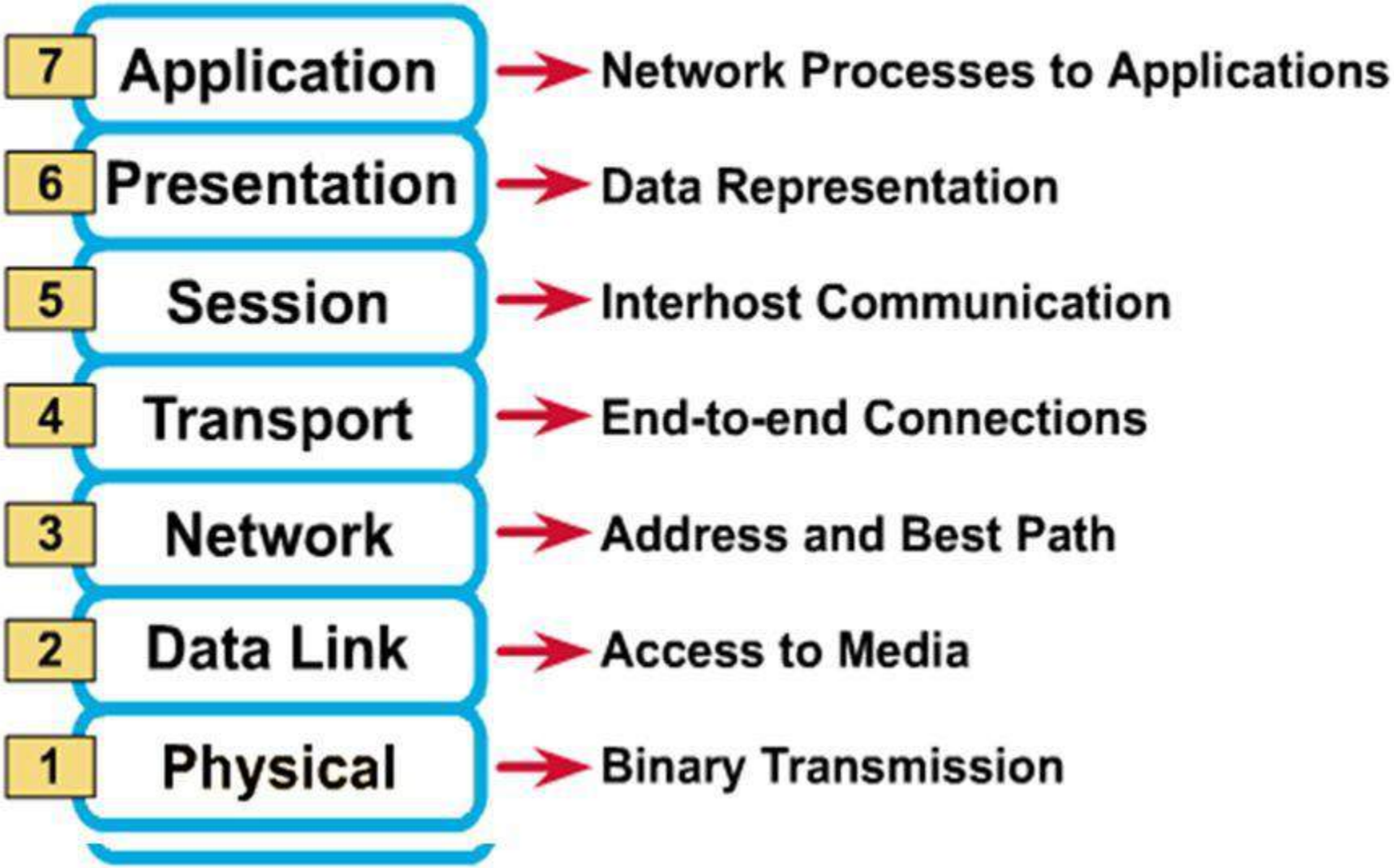
Introduction

- A Peer-to-Peer network has no dedicated Servers.
- In Peer-to-Peer network, a number of workstations (or clients) are connected together for the purpose of sharing devices, information or data. All the workstations are considered as equal.
- Any one computer can act as client or server at any instance.

The OSI Reference Model

- The OSI layer was introduced by the International Organization for Standardization (ISO) in 1984 in order to provide a reference model to make sure products of different vendors would interoperate in networks.
- OSI is short for Open Systems Interconnection.
- The OSI layer shows WHAT needs to be done to send data from an application on one computer, trough a network, to an application on another computer, not HOW it should be done.
- A layer in the OSI model communicates with three other layers: the layer above it, the layer below it, and the same layer at its communication partner.
- Data transmitted between software programs passes all 7 OSI layers.
- The Application, Presentation and Session layers are also known as the Upper Layers.
- The Data Link and Physical layers are often implemented together to define LAN and WAN specifications.

7 Layers of OSI Model



Data, Protocol & Activities

OSI Layers	TCP/IP Suit	Activities
Application	**Application** Telnet, FTP, SMTP, HTTP, DNS, SNMP, *Specific address* etc…	To allow access to network resources
Presentation	**Presentation**	To Translate, encrypt, and compress data
Session	**Session**	To establish, manage, and terminate session
Transport	**Transport** SCTP, TCP, UDP, Sockets and *Ports address*	To Provide reliable process-to-process Message delivery and error recovery
Network	**Network** IP, ARP/RARP, ICMP, IGMP, *Logical address*	To move packets from source to destination; to provide internetworking
Data Link	**Data Link** IEEE 802 Standards, TR, FDDI, PPP, *Physical address*	To organize bits into frames; to provide Hop-to-hop delivery
Physical	**Physical** Medium, Coax, Fiber, 10base, Wireless	To Transmit bits over a medium; to provide Mechanical and electrical specifications

The TCP/IP Reference Model

- TCP is Transmission Control Protocol.
- IP is Internet Protocol.
- Only 4 layers:

1	Application Layer
2	Transport Layer
3	Internet Layer
4	Link Layer (network)

OSI and TCP/IP Reference Models

	OSI	TCP/IP
7	Application	Application
6	Presentation	
5	Session	
4	Transport	Transport
3	Network	Internet
2	Link	Link/Network
1	Physical	

Comparison between OSI and TCP/IP Reference Models

OSI

1)It has 7 layers

2)Transport layer guarantees delivery of packets

3)Separate presentation layer

4)Separate session layer

5)Network layer provides both connectionless and connection oriented services

6)It defines the services, interfaces and protocols very clearly and makes a clear distinction between them

7)It has a problem of protocol filtering into a model

TCP/IP

1)Has 4 layers

2)Transport layer does not guarantees delivery of packets

3)No presentation layer, characteristics are provided by application layer

4)No session layer, characteristics are provided by transport layer

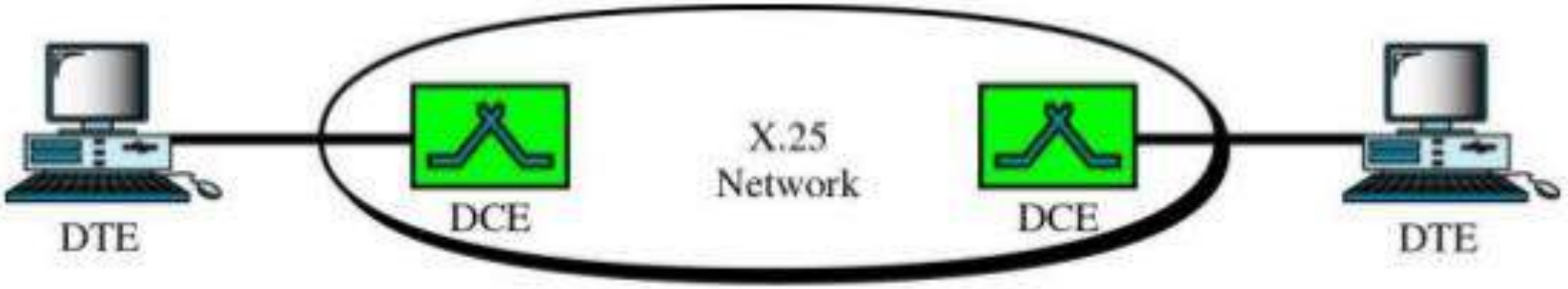
5)Network layer provides only connection less services

6)It does not clearly distinguishes between service interface and protocols

7)The model does not fit any protocol stack.

X.25 Protocol:

- X.25 defines how a node terminal could be interfaced to the network for communication in Packet Mode.
- Key terms used here are: **DTE** and **DCE** node
- It defines how DTE's communicates with network and how packets are sent over that network using DCEs.
- It is also known as SUBSCRIBER NETWORK INTERFACE(SNI) PROTOCOL.



X.25 Protocol

- X.25 is a ***reliable protocol***, meaning it performs error control and retransmits bad packets.
- Although widely used in Europe, X.25 is not in widespread use in North America. The primary reason is the low transmission speed, now 2.048 Mbps (up from 64 Kbps)

Introduction

- Frame Relay (FR) is a high-performance WAN protocol that operates at the physical and data link layers of the OSI reference model.
- FR originally was designed for use across Integrated Service Digital Network (ISDN) interfaces.
- Today, it is used over a variety of other network interfaces as well.
- FR is an example of a packet-switched technology.

Asynchronous Transfer Mode

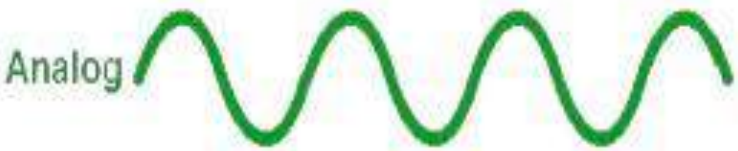
Asynchronous Transfer Mode (ATM) is a switching technique for telecommunication networks. It uses asynchronous time-division multiplexing,[1][2] and it encodes data into small, fixed-sized *cells*.

ATM differs from networks such as the Internet or Ethernet LANs that use variable sized *packets* or *frames*. ATM provides data link layer services that run over OSI Layer 1 physical links. ATM has functional similarity with both circuit switched networking and small packet switched networking.

This makes it a good choice for a network that must handle both traditional high-speed data traffic (e.g., file transfers), and real-time, low-latency content such as voice and video.

Unit-2

Two type of Electromagnetic Signals



An analog signal is a continuous wave denoted by a sine wave and may vary in signal strength (amplitude) or frequency (time).

A digital signal is described as using binary (0s and 1s), and therefore, cannot take on any fractional values. This kind of signal denoted by digits that's why it is called Digital Signal.

"Analog" and "Digital" both are electro magnetic signal. Now a days both signals are used as a ***Full duplex*** *communication mainly in* ***Libraries*** *and in* ***Information systems.***

3-2 PERIODIC ANALOG SIGNALS

*Periodic analog signals can be classified as **simple** or **composite**. A simple periodic analog signal, a **sine wave**, cannot be decomposed into simpler signals. A composite periodic analog signal is composed of multiple sine waves.*

Topics discussed in this section:

Sine Wave
Wavelength
Time and Frequency Domain
Composite Signals
Bandwidth

3-5 DATA RATE LIMITS

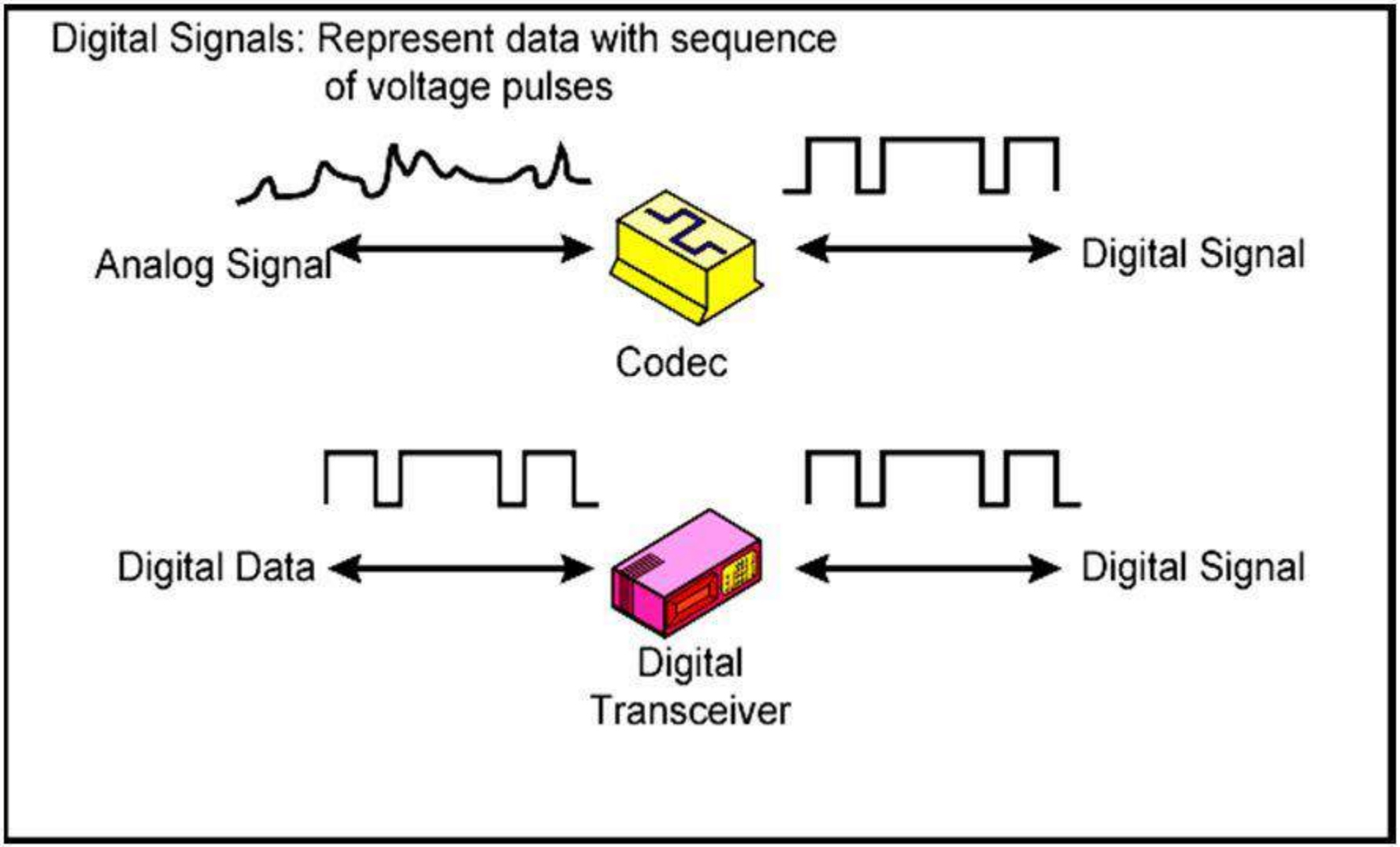
A very important consideration in data communications is how fast we can send data, in bits per second, over a channel. Data rate depends on three factors:

1. *The bandwidth available*
2. *The level of the signals we use*
3. *The quality of the channel (the level of noise)*

Topics discussed in this section:

- **Noiseless Channel: Nyquist Bit Rate**
- **Noisy Channel: Shannon Capacity**
- **Using Both Limits**

Digital Signals



Data Rate and Bandwidth

- Effective bandwidth is the band within which most of the signal energy is concentrated. Here, "most" is somewhat arbitrary.

- Although a given waveform may contain frequencies over a very broad range, as a practical matter, any transmission system will be able to accommodate only a limited band of frequencies.
  - —because of the limitation of **transmitter** & **medium** & **receiver**
  - —This limits the data rate that can be carried on the transmission system.

Bit Rate, Baud Rate and Minimum BW

- Two basic aspects of digital-to-analog modulation; bit and baud rate.
- **Bit rate** - number of bits per second (rate at which bit changes, bps).
  - Computer Efficiency - how long it takes to process each piece of information (time to send)
- **Baud rate** - number of signal units per second (rate at which signal element changes). Also called modulation rate or symbol rate.
  - Data Transmission Efficiency - how efficient we can move those data from place to place.
- Analogy - In transportation, baud ≈ car and bit ≈ passenger

- A car can carry one or more passengers. If 1000 cars go from one point to another, carrying only 1 passenger (i.e the driver), then 1000 passengers are transported.
- However, if each car carries four passengers (carpooling), then 4000 passengers are transported.
- Note that the number of cars not the number of passengers, determine the traffic, and therefore, the need for wider highways.
- Similarly, the number of bauds determines the required bandwidth, not the number of bits.

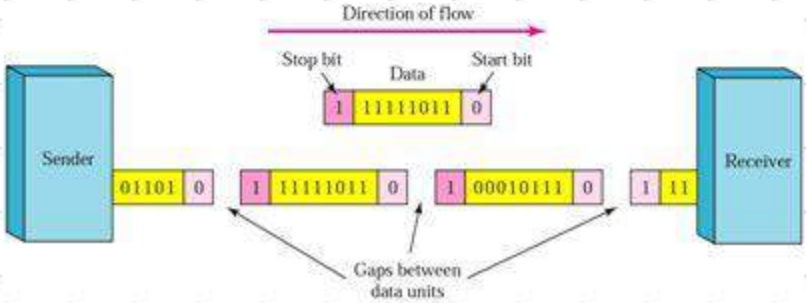
Synchronous	Asynchronous
• Fast transmission • Needs a common clock signal, or some way of sharing it • May have to wait briefly until data can be sent	• Slower transmission, due to the extra bits and the gaps • Cheap and easy to implement = no clock sharing • Can transmit when ready

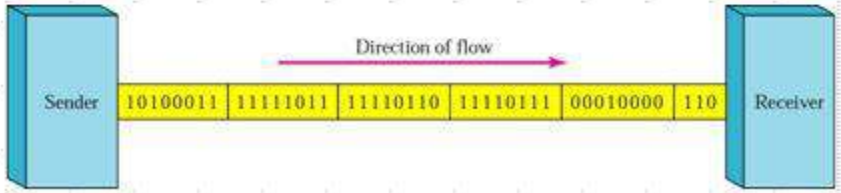
- Almost all parallel transmission is synchronous
- Asynchronous transmission is used when data is sent sporadically, e.g. via a mouse or keyboard

2. Asynchronous and Synchronous Transmissions

- Transfer of data with start and stop bits and a variable time interval between data units
- Timing is unimportant
- Start bit alerts receiver that new group of data is arriving
- Stop bit alerts receiver that byte is finished
- Synchronization achieved through start/stop bits with each byte received
- Requires additional overhead (start/stop bits)
- Slower but Cheap and effective
- Ideal for low-speed communication when gaps may occur during transmission (ex: keyboard)

- Requires constant timing relationship
- Bit stream is combined into longer frames, possibly containing multiple bytes
- Any gaps between bursts are filled in with a special sequence of 0s and 1s indicating idle
- Advantage: speed, no gaps or extra bits
- Byte synchronization accomplished by data link layer





Encoding Techniques

1. Digital data as digital signal
2. Digital data as analog signal: Converter (Modem)
3. Analog data as digital signal: Converter (Codec)
4. Analog data as analog signal

- In general:
  - When the outcome is a digital signal we use an Encoding process
  - When the outcome is an analog signal we use a Modulation process
    - But we call the modulation of analog signal by digital data shift-keying

Types of Encoding

- Digital Data , Analog signals

  Basis for analog signaling is a continuous, constant-frequency signal known as the carrier frequency.

  By modulating(Amplitude , Frequency , Phase)

- Analog Data ,Digital signals

  Analog-to-digital conversion is an electronic process in which a continuously variable analog signal is changed, without altering its essential content, into a multi-level digital signal.

- Digital Data , Digital signals

  Digital signal –is a sequence of discrete, discontinuous voltage pulses.

  Bit duration :: the time it takes for the transmitter to emit the bit.

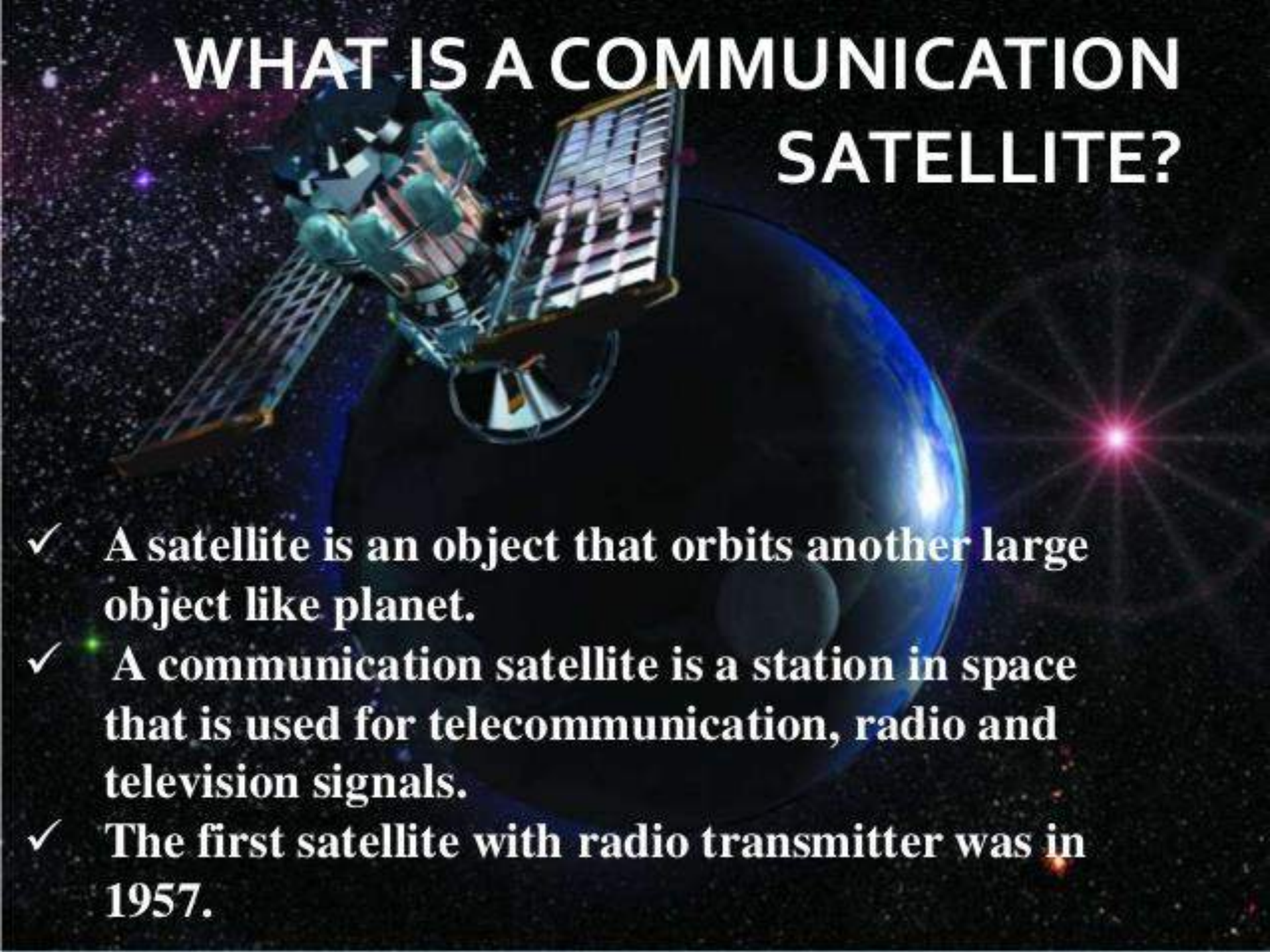
Modulation Techniques

- Modulation can be done by varying the
  - Amplitude
  - Phase, or
  - Frequency

  of a high frequency carrier in accordance with the amplitude of the message signal.
- **Demodulation** is the inverse operation: *extracting the baseband message from the carrier* so that it may be processed at the receiver.

Basis	Guided/ Bounded Media	UnGuided/ UnBounded Media
Transmission	Guided is wired transmission, in which data signals are guided along a physical path i.e. within a wire	Unguided/ Unbounded communication is wireless transmission. To exchange bits of data for laptop, notebook, smart watch, without wires, you need wireless communication.
Also, called?	Guided transmission is also known as Bounded Transmission Media.	UnGuided transmission is also known as UnBounded Transmission Media.
Media Types	Some well-known Guided Transmission media includes Twisted Pair Cable, Coaxial cable, fiber optic cable, etc.	UnGuided Transmission media includes Microwave Transmission, Satellite Communication, etc.
Media	The media can be seen and touched i.e. tangible.	The media is wireless and cannot be seen and touched i.e. intangible.
Distance	Used for shorter distance.	Used for larger distance.
Penetration	Guided Media cannot penetrate through the buildings	UnGuided Media can penetrate through the buildings.

WHAT IS A COMMUNICATION SATELLITE?



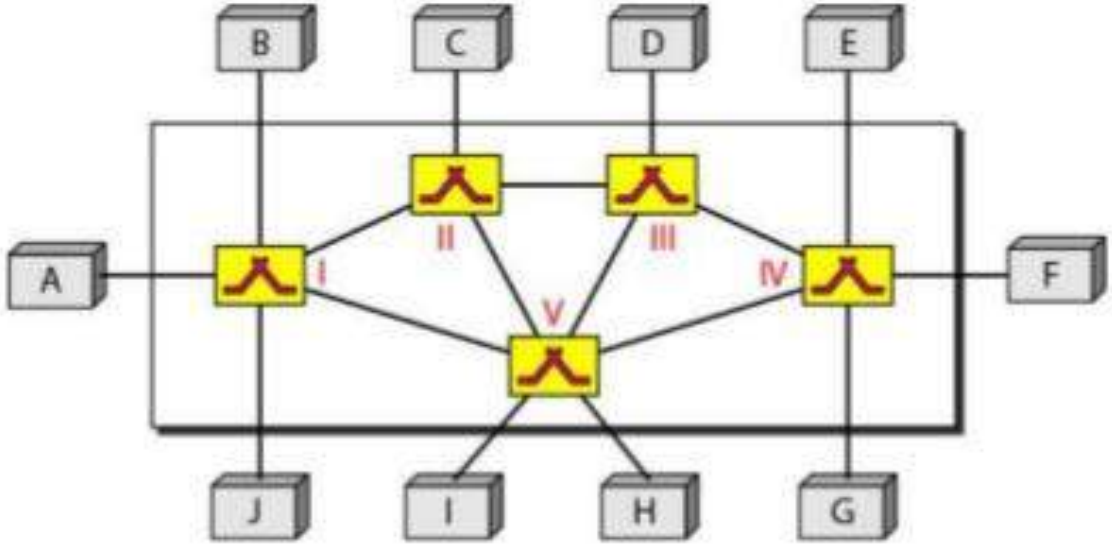
- ✓ A satellite is an object that orbits another large object like planet.
- ✓ A communication satellite is a station in space that is used for telecommunication, radio and television signals.
- ✓ The first satellite with radio transmitter was in 1957.

Communication Satellite

- They are used for mobile applications such as communication to ships, vehicles, planes, hand-held terminals and for TV and radio broadcasting.
- A satellite works most efficiently when the transmissions are focused with a desired area.
- The earth station should be in a position to control the satellite if it drifts from its orbit it is subjected to any kind of drag from the external forces.
- Transmission cost is independent of distance.
- The power and bandwidth of these satellites depend upon the preferred size of the footprint, complexity of the traffic control protocol schemes and the cost of ground stations.

Switched network

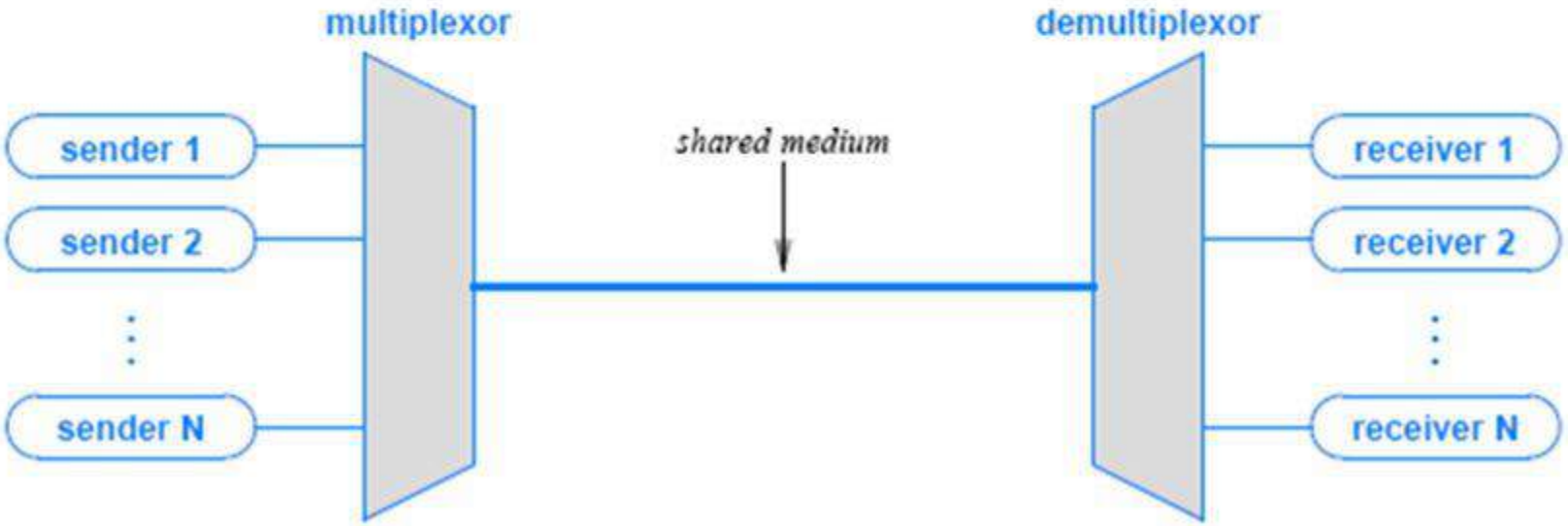
- **Switched network:** Series of interlinked nodes, called switches.



- **Switches:** Devices capable of creating temporary connections between two or more devices linked to the switches . Some of these switches are connected to the end systems (computers or telephones) . Others used only for routing

Multiplexing and Demultiplexing

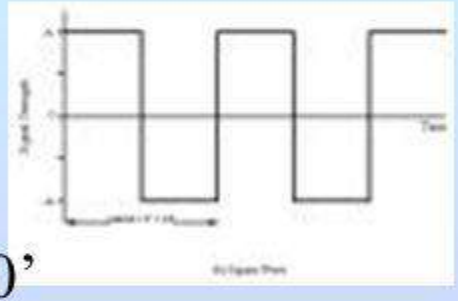
- Multiplexing: A network word for sharing
  - Combining information streams from multiple sources for transmission over a shared medium
  - Multiplexor: a method/device to implement this.
  - Demultiplexing: Separating a combined stream back into individual streams



Dial-up connections (2)

A device called a 'Modem' was developed to allow Digital data to be carried over the analogue telephone system.

'1'

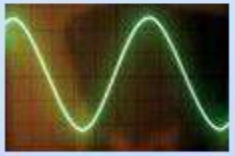


'0'

Digital signal

MODEM

One Tone represents Binary '1'



A different Tone represents Binary '0'

Telephone line

This is why dial modems can be heard to 'whistle' as they communicate. You are hearing the tones that represent digital information

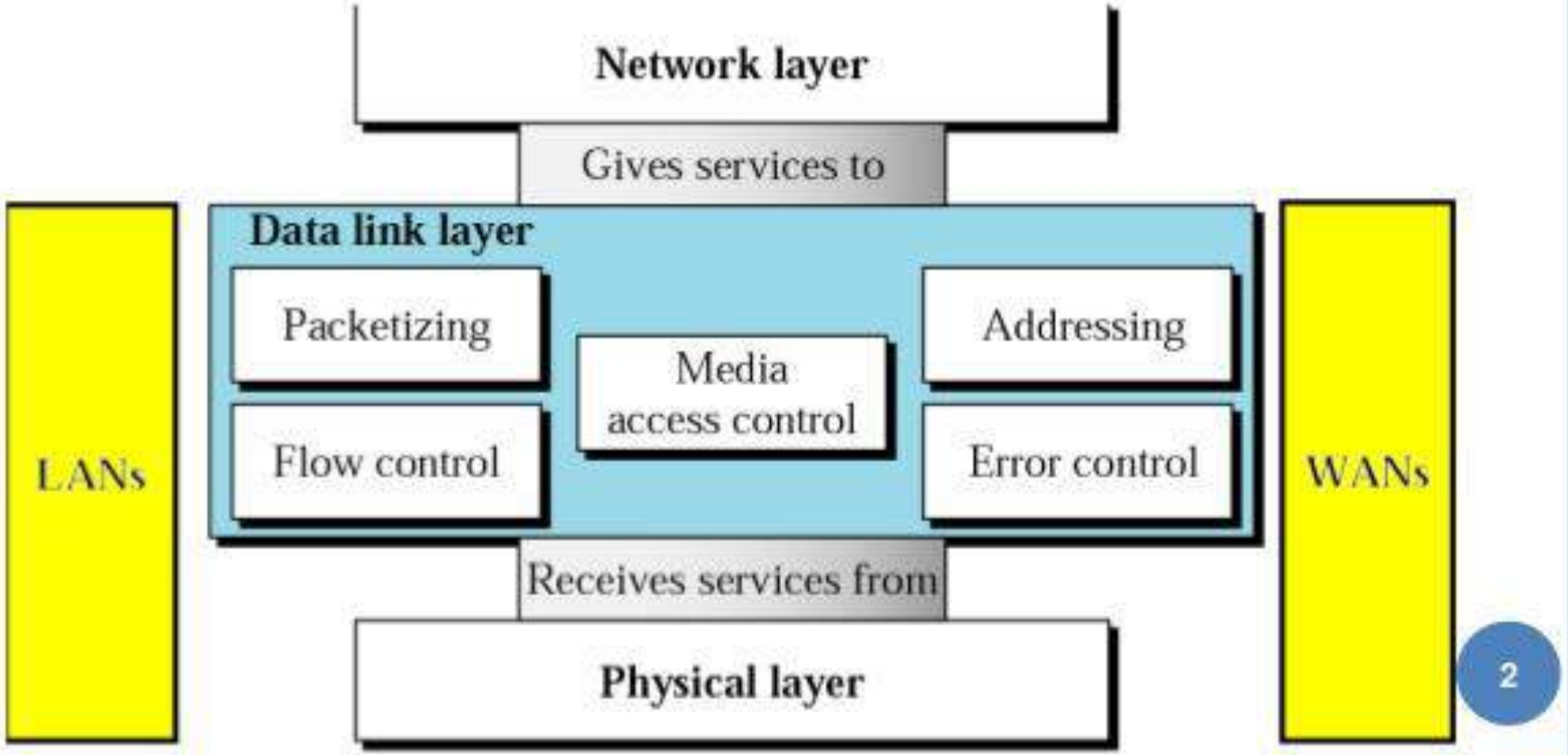
What is DSL?

- Digital Subscriber Line
  - A technology which uses the existing transmission medium (telephone wire) to provide high-speed transfer of information across the internet.
  - DSL simply uses more of the bandwidth.
- DSL
- allows simultaneous voice and high-speed data services such as super fast Internet access
- over a single pair of copper telephone wires.

Unit-3

OVERVIEW OF DLL

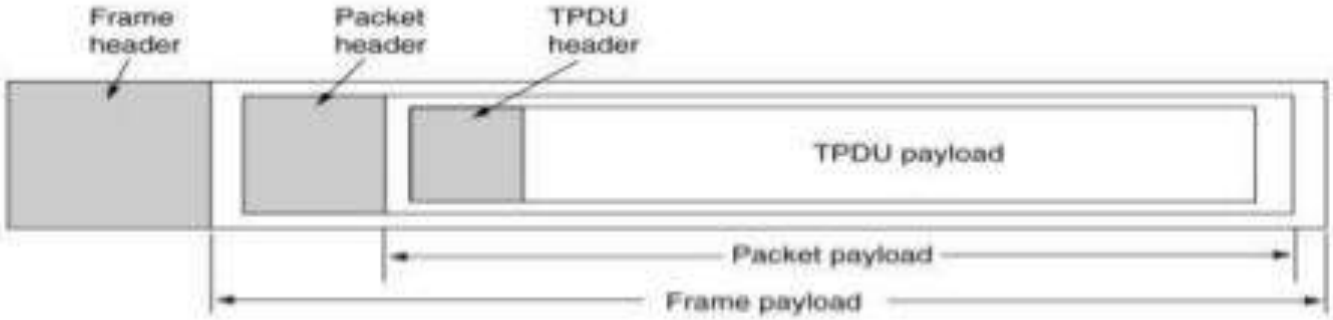
The data link layer transforms the physical layer, a raw transmission facility, to a link responsible for node-to-node (hop-to-hop) communication. Specific responsibilities of the data link layer include *framing, addressing, flow control, error control, and media access control.*



FRAMING

- DLL translates the physical layer's raw bit stream into discrete units (messages) called frames.

- How can frame be transmitted so the receiver can detect frame boundaries? That is, how can the receiver recognize the start and end of a frame?
  1. Character Count
  2. Flag byte with Byte Stuffing
  3. Starting and ending flag with bite stuffing
  4. Encoding Violations

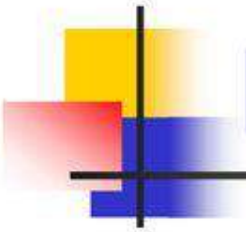


FLOW CONTROL

- *Flow control* deals with throttling the speed of the sender to match that of the receiver.

- Two Approaches:
  - **feedback-based flow control**, the receiver sends back information to the sender giving it permission to send more data or at least telling the sender how the receiver is doing
  - **rate-based flow control**, the protocol has a built-in mechanism that limits the rate at which senders may transmit data, without using feedback from the receiver.

- Various Flow Control schemes uses a common protocol that contains well-defined rules about when a sender may transmit the next frame. These rules often prohibit frames from being sent until the receiver has granted permission, either implicitly or explicitly.



Flow Control

- Flow Control is a technique for speed-matching of transmitter and receiver. Flow control ensures that a transmitting station does not overflow a receiving station with data
- We will discuss two protocols for flow control:
  - Stop-and-Wait
  - Sliding Window
- For the time being, we assume that we have a perfect channel (**no errors)**

Error Control

Note:

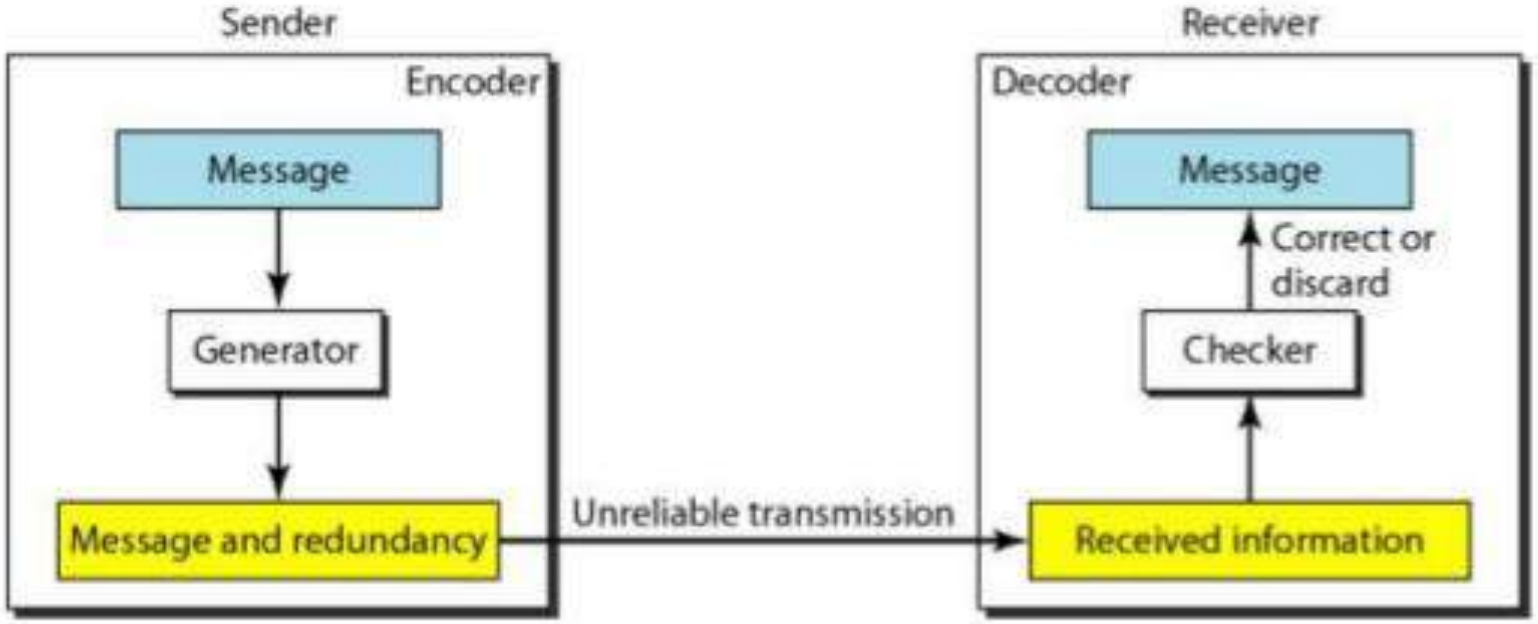
Error control in the data link layer is based on automatic repeat request, which is the retransmission of data.

Error Correction and Detection

- It is physically impossible for any data recording or transmission medium to be 100% perfect 100% of the time over its entire expected useful life.
  - In data communication, line noise is a fact of life (e.g., signal attenuation, natural phenomenon such as lightning, and the telephone repairman).
- As more bits are packed onto a square centimeter of disk storage, as communications transmission speeds increase, the likelihood of error increases-- sometimes geometrically.
- Thus, error detection and correction is critical to accurate data transmission, storage and retrieval.
- Detecting and correcting errors requires *redundancy* -- sending additional information along with the data.

Error Detection Vs Error Correction

- There are two types of attacks against errors:
- **Error Detecting Codes:** Include enough redundancy bits to *detect* errors and use ACKs and retransmissions to recover from the errors.
- **Error Correcting Codes:** Include enough redundancy to detect *and* correct errors. The use of error-correcting codes is often referred to as forward error correction.



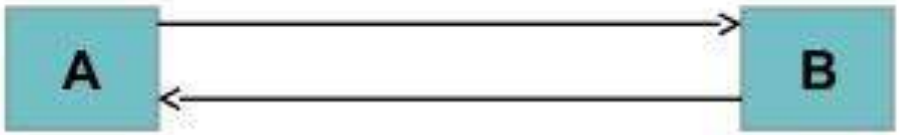
Sliding Window Protocol

- Sliding window algorithms are a method of flow control for network data transfers.

- Data Link Layer uses a sliding window algorithm, which allows a sender to have more than one unacknowledged packet "in flight" at a time, which improves network throughput.

Key concepts of the Sliding Window

- Both the sender and receiver maintain a finite size buffer to hold outgoing and incoming packets from the other side.
- Every packet sent by the **sender**, must be acknowledged by the receiver. The sender maintains a timer for every packet sent, and any packet unacknowledged in a certain time, is **resent**.
- The sender may send a whole window of packets before receiving an acknowledgement for the first packet in the window. This results in higher transfer rates, as the sender may send multiple packets without waiting for each packet's acknowledgement.
- The Receiver advertises a window size that tells the sender how much data it can receive, in order for the sender not to fill up the receivers buffers.
- Efficiency can also be improved by making use of the full-duplex line



RANDOM ACCESS PROTOCOL

When node has packet to send

Sense the channel.

If it is busy, wait for **random** amount of time and then retry.

no ***a prior*** coordination among nodes.

All nodes use the same time, frequency and code.

Two or more transmitting nodes ➜ "collision"

Random access MAC protocol specifies how to recover from collisions -> Exponential backoff.

Examples of random access MAC protocols:

CSMA, CSMA/CA, CSMA/CD

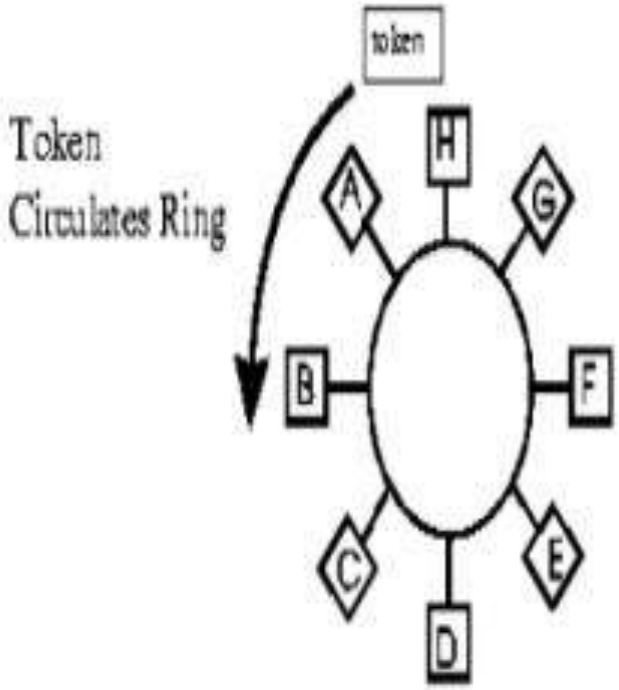
Token Passing Protocols Overview

- The order each station gets to send a frame is predetermined
- Similar to a relay race: each runner (station) must wait for the baton (token) to be passed to complete his leg of race
- Devices in a network are arranged in a ring topology
- The token circulates across the network
- Each station must wait for the token to arrive at its location before it can send data on the network

TOKEN RING

- **Token ring** local area network (LAN) technology is a protocol which resides at the data link layer (DLL) of the OSI model.
- It uses a special three-byte frame called a token that travels around the ring.
- Token
  - Data packet that could carry data
  - Circulates around the ring
  - Offers an opportunity for each workstation and server to transmit data.

IEEE 802.5 TOKEN RING



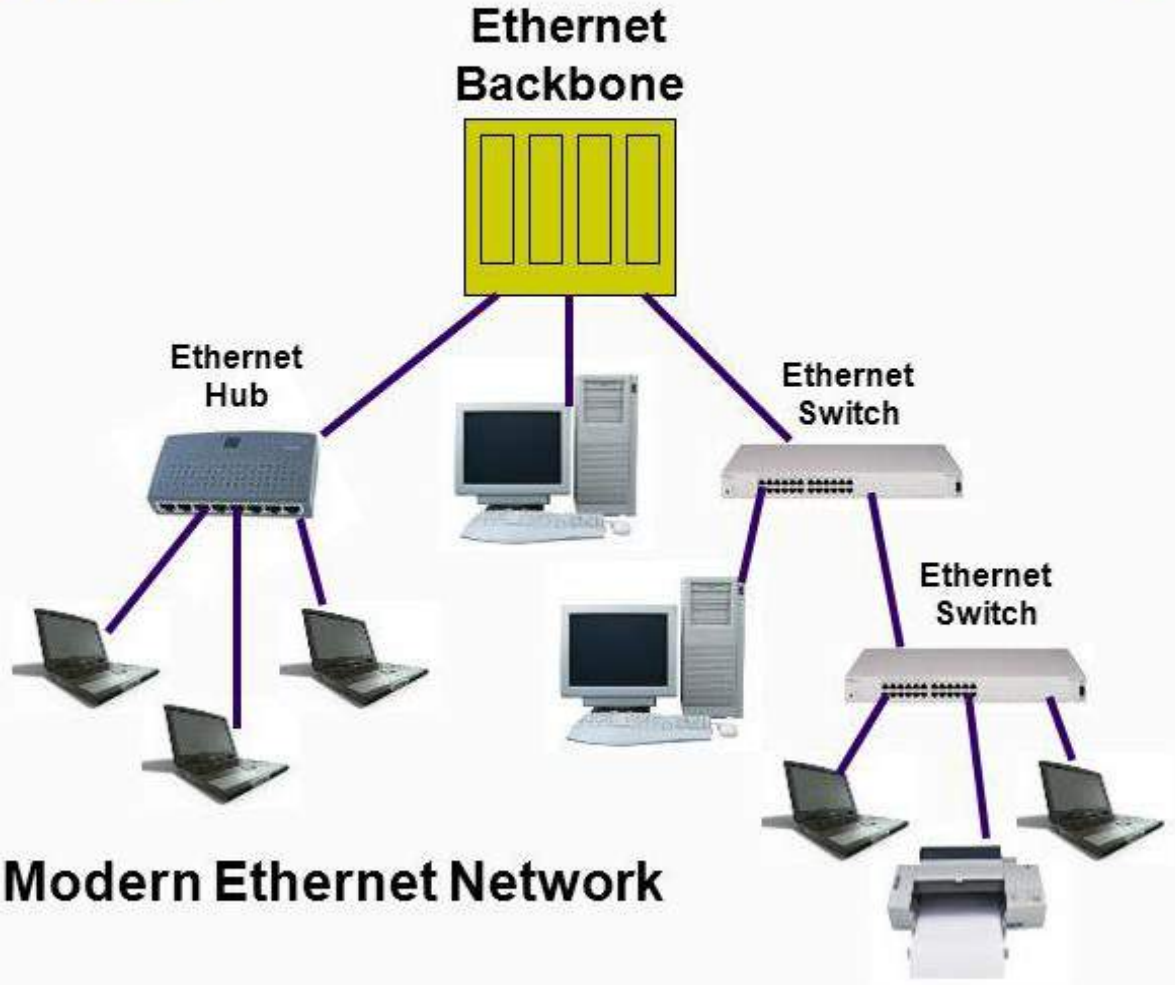
- There is a point to point link between stations that form a ring.
- Physical Layer Topology: *Ring*
  - Stations connected in a loop
  - Signals go in only one direction, station-to-station
- In a token ring a special bit format called a token circulated around all the stations.

What is Ethernet?

Ethernet is a family of computer networking technologies for local area networks (LANs) and metropolitan area networks (MANs). It was commercially introduced in 1980 and first standardized in 1983 as IEEE 802.3,[1] and has since been refined to support higher bit rates and longer link distances.

Over time, Ethernet has largely replaced competing wired LAN technologies such as token ring, FDDI, and ARCNET

Ethernet

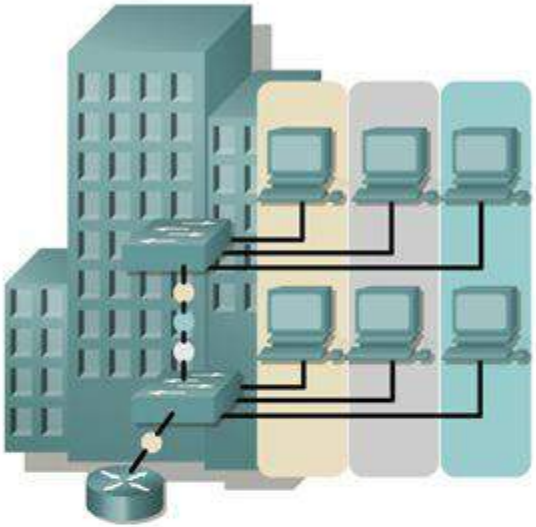


The Modern Ethernet Network

What is VLAN?

- It stands for Virtual Local Area Network.
- It is defined as a broadcast domain within a switch network.
- A switch can be configured to support a single or multiple VLANs.
- Each VLAN Becomes its own broadcast domain.
- Virtual LAN is a solution to divide a single Broadcast domain into multiple Broadcast domains.
- Host in one VLAN cannot speak to a host in another.
- By default, all hosts are placed into the same VLAN.

VLAN introduction



- A group of ports or users in same broadcast domain
- Can be based on port ID, MAC address, protocol, or application
- LAN switches and network management software provide a mechanism to create VLANs
- Frame tagged with VLAN ID

- **VLANs are created to provide segmentation services traditionally provided by physical routers in LAN configurations.**
- VLANs address scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, and traffic flow management.
- Switches may not bridge any traffic between VLANs, as this would violate the integrity of the VLAN broadcast domain.
- Traffic should only be routed between VLANs.

FAST ETHERNET

It was designed to compete with LAN protocols such as FDDI or Fiber channel . IEEE created Fast Ethernet under the name 802.3u.Fast Ethernet is backward-compatible with standard Ethernet , but it can transmit data 10 times faster at rate of100Mbps.

GOALS OF FAST ETHERNET:

- Upgrade the data rate to 100Mbps.
- Make it compatible with standard Ethernet.
- Keep the same 48 bit-address.
- Keep the same frame format.
- Keep the same minimum and maximum frame lengths.

Summary

- Gigabit Ethernet supports data rate of 1000Mbps.

- CSMA/CD protocol are same as that of Ethernet and Fast Ethernet. It helps in reducing the collision.

- Carrier extension is extended with special symbols so that the block is 512 bytes. Frame bursting is used to achieve higher throughput.

- GMII is an interface between MAC and Physical layer, supports half and full duplex modes of operation and also connects various media.

- Auto negotiation selects the duplex modes, transfers 16 bit of information data at a time.

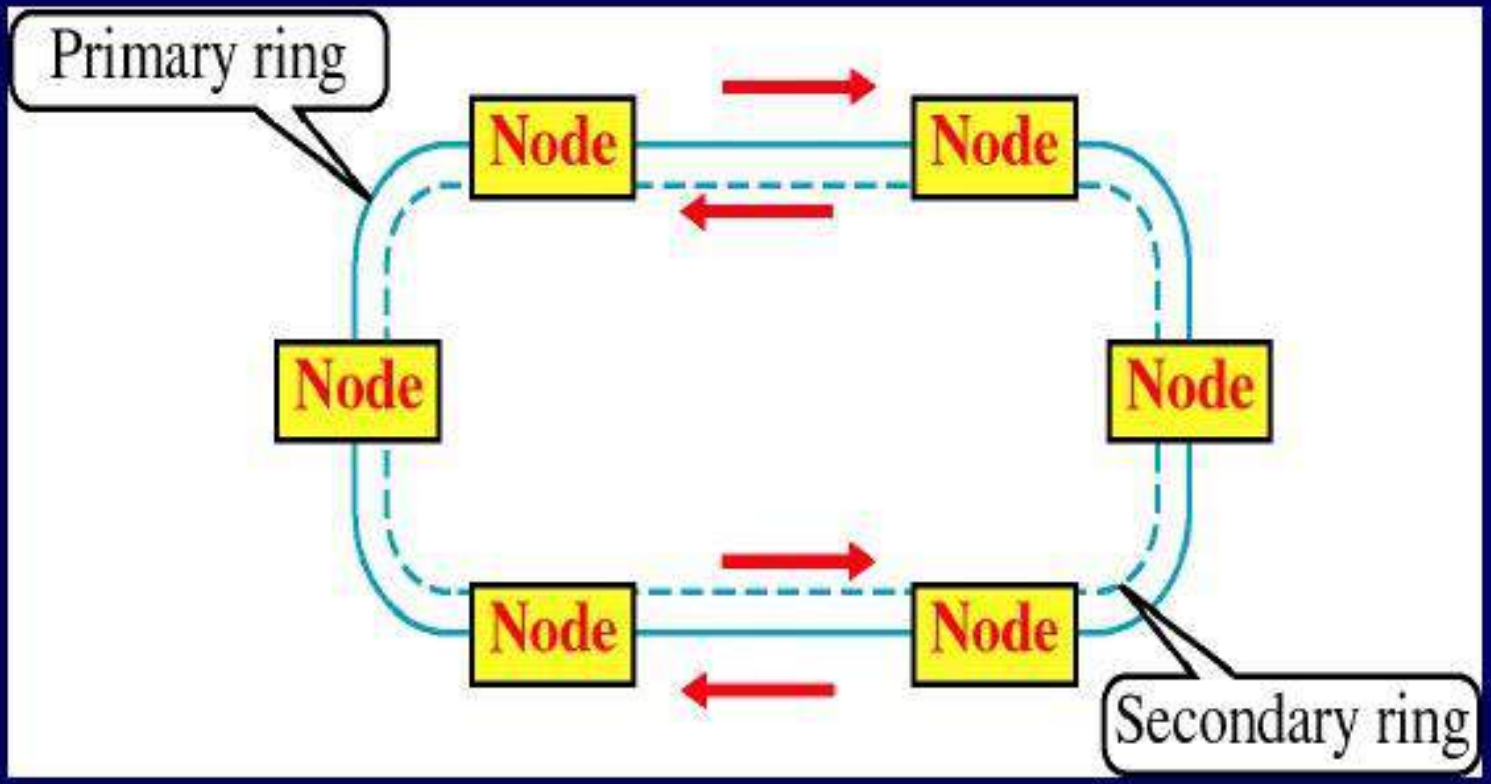
- Gigabit Ethernet uses higher bandwidth and provides higher performance.

- It is still not in use. And it only works with network traffics.

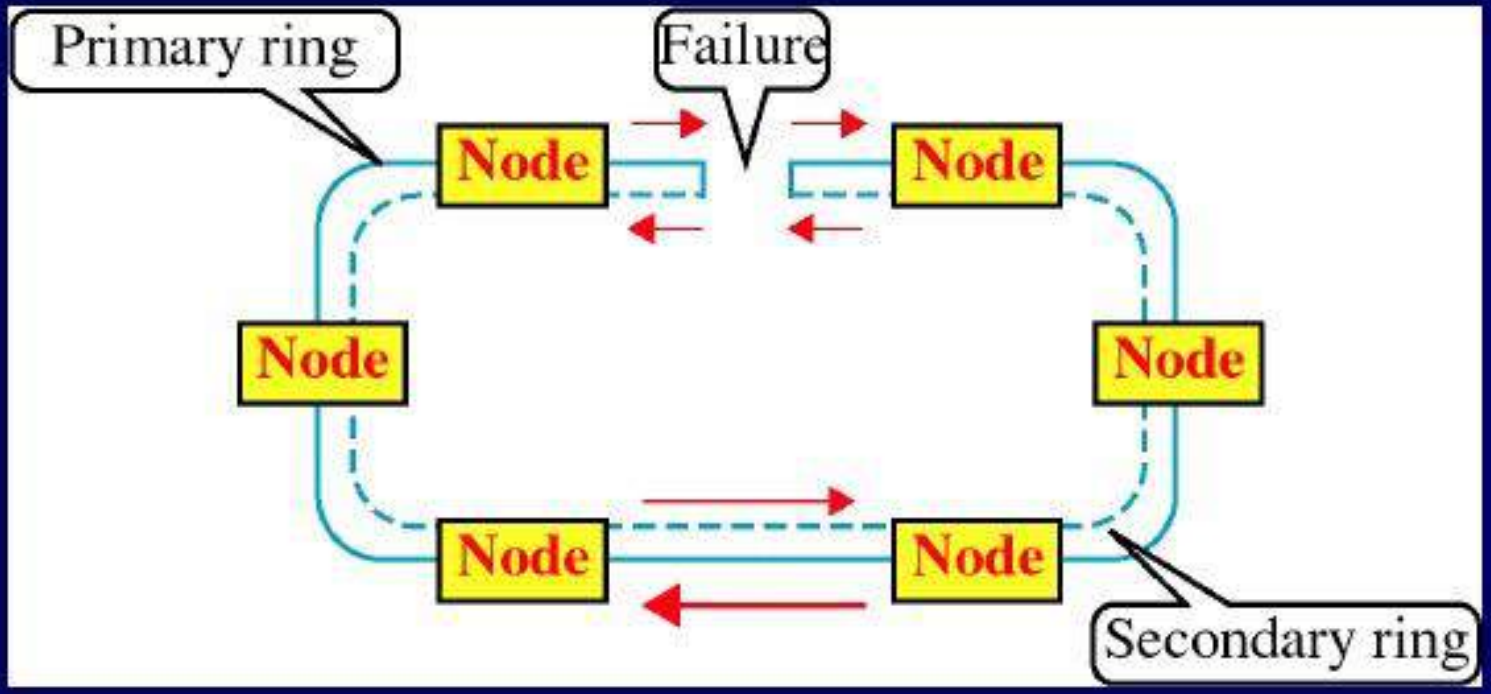
What is FDDI?

- Fiber Distributed Data Interface
- 100-Mbps token passing
- Dual-ring LAN
- A high-speed backbone technology
- High bandwidth
- Optical fiber transmission
- Allows up to 1000 stations

FDDI Architecture



Ring Wrapping



When a single station fails, devices on either side of the failed (or powered-down) station wrap, forming a single ring. Network operation continues for the remaining stations on the ring.

Definition of Bluetooth

Bluetooth is a short-range wireless communication technology.Bluetooth technology allows you to share voice, data, music, photos, videos and other information wirelessly between paired devices.

Connectors

RJ45 – This connector is used to connect the twisted pair cables with the networking devices.

BNC- it is commonly used in base 10 Ethernet network, it is used to end the magnetic signal within the cable which carries info.

TRANSCEIVER

a transceiver of this kind, it is impossible to receive signals while transmitting.

- This mode is called half duplex.
- Transmission and reception often, but not always, are done on the same frequency. Some transceivers are designed to allow reception of signals during transmission periods.

❑ Repeater

- Network **repeaters** regenerate incoming electrical, wireless or optical signals. With physical media like Ethernet or Wi-Fi, data transmissions can only span a limited distance before the quality of the signal degrades. Repeaters attempt to preserve signal integrity and extend the distance over which data can safely travel.
- Repeaters remove the unwanted noise in an incoming signal.
- It can't filter the signal traffic.
- it works in physical layer of OSI Model.

Hub

- A hub is a common connection point for devices in a network.
- works at physical layer and hence connect networking devices physically together.
- contains multiple ports.
- When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets.

Compiled by Mr. Benjamin Muganzi

1. Network Interface Card (NIC)

- Any computer that is to be connected to a network, needs to have a network interface card (NIC).
- Modern computers have inbuilt NICs. However you can also add an expansion NIC card.
- Most laptops have two inbuilt NICs; one for the wireless network, and another for the wired network.

What is a Bridge?

- A hardware device used to create a connection between two separate computer networks or to divide one network into two.

- Filters data traffic at a network boundary and reduces the amount of traffic on a LAN dividing it into two segmen

- 1-4E to Ethernet (10/100M) Network Bridge. [online image]. Network Bridge. Available at www.freewfc.com. July 12, 2013.

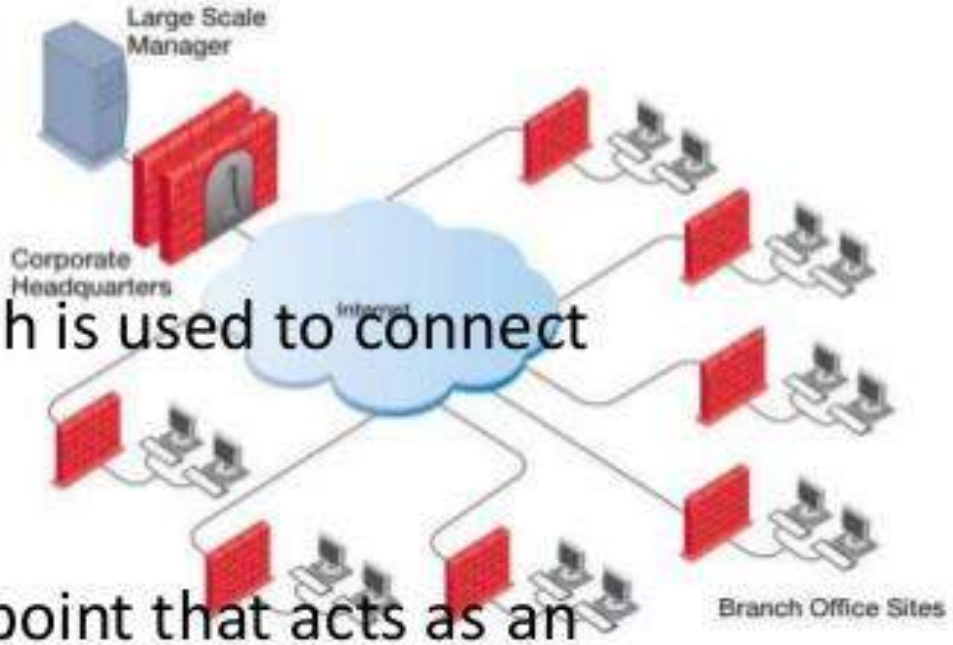
Switches

- A switch is an intelligent device that works in the data link layer.
- It is linkage points of an Ethernet network.
- The term intelligent refers to the decision making capacity of the Switch.
- **Hub** works by sending the data to all the ports on the device whereas a **switch** transfers it only to that port which is connected to the destination device.

Router

- Router is a device which connects different networks-frequently over a large distances.
- A router is a device that forwards data packets between computer networks, creating an overlay internetwork.

Gateways



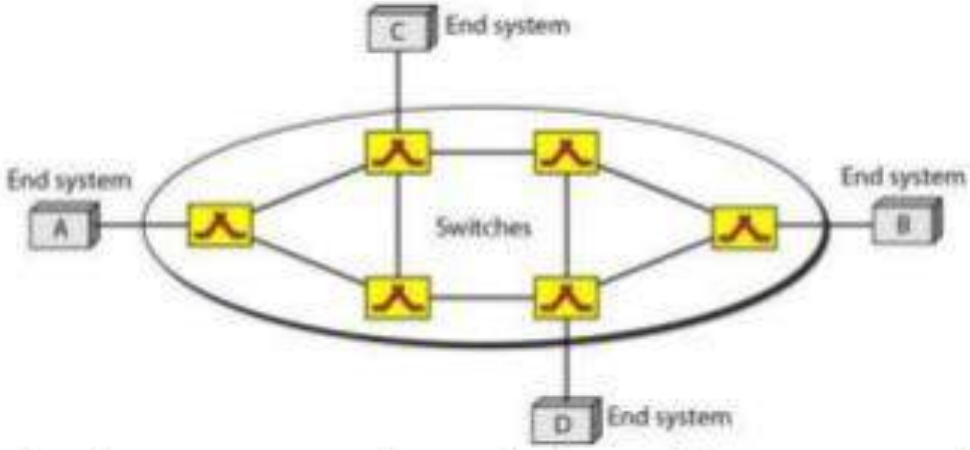
- Gateway is a device which is used to connect multiple networks.

- A **gateway** is a **network** point that acts as an entrance to another **network.**
- It allows the computer programs, either on the same computer or on different computers to share information across the network through protocols.
- A router is also a gateway, since it interprets data from one network protocol to another.

Unit-4

2.2 VIRTUAL-CIRCUIT NETWORKS

- It's a cross between circuit switched network and datagram network, and has some characteristics of both.



- Characteristics:
  - **Packets** from a single message travel **along the same path**.
  - Three phases to transfer data (set up, data transfer and tear down)
  - Resources can be allocated during setup phase
  - Data are packetized and each packet carries an address in the header
  - **Implemented** in **data link layer**

Flooding Routing

Advantages:

- Reliable.
- All routes are tried, so at least one packet goes to shortest route.
- All nodes direct or indirectly visited.

Problems:

- Generate large number copies are generate which make congestion.
- Suitable if use damping mechanism so that larges number of packets are not make.

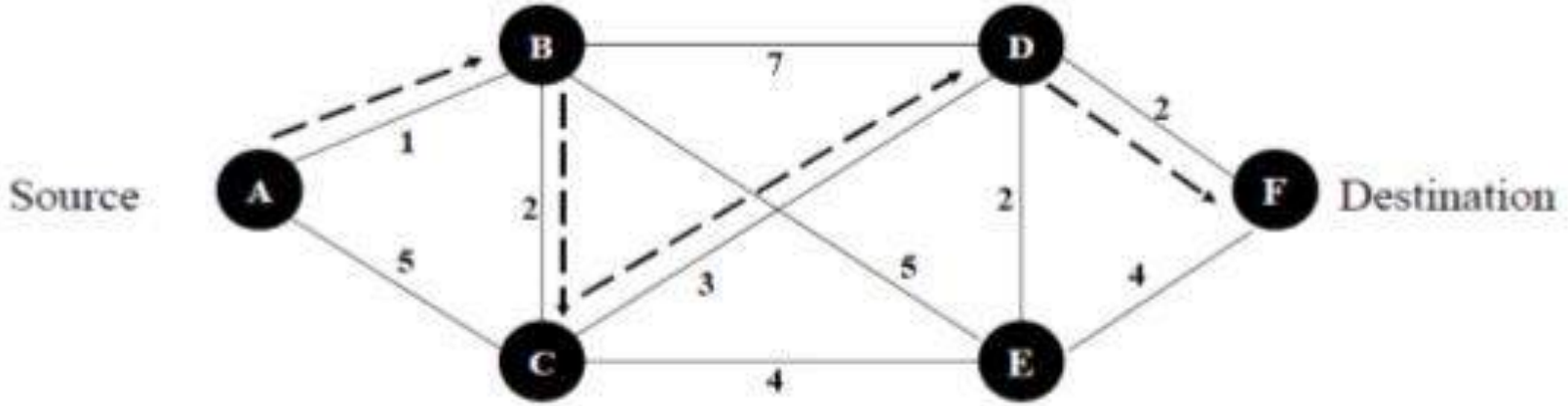
Technique To Use

- **Hop-Count**: a hop counter is contain in header of packet and it decrease each one time when pass through the node and discard when it reach to zero.
- **Sequence Number**: Keep track of packets which are responsible for flooding using a sequence number .Avoid sending them out second time.

Shortest-Path Routing

- Routing algorithms generally use a shortest path algorithm to calculate the route with the least cost.
  Three components
- Measurement Component: Nodes (routers) measure the current characteristics such as delay, throughput, and "cost"
- Protocol: Nodes disseminate the measured information to other nodes
- Calculation: Nodes run a least-cost routing algorithm to recalculate their routes

Shortest Path Routing.



- The shortest path in the n/w is (A-B-C-D-F).
- The path is calculated by adding up the labels.
- The total is 8 for the shortest path.
- For other paths it's greater than 8.

Shortest Path Routing

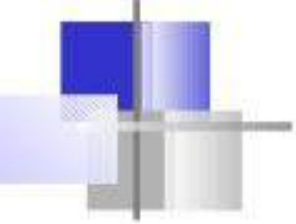
1. Bellman-Ford Algorithm [Distance Vector]
2. Dijkstra's Algorithm [Link State]

What does it mean to be the shortest (or optimal) route?

a. Minize the number of hops along the path.

b. Minimize mean packet delay.

c. Maximize the network throughput.



Distance Vector Routing

a) The least-cost route between any two nodes is the route with minimum distance.

b) Each node maintains a vector(table) of minimum distances to every node.

c) The table at each node also guides the packets to the desired node by showing the showing the next hop routing.

Example:

Assume each node as the cities.

Lines as the roads connecting them.

Distance Vector Routing (DVR)

a) 3 keys to understand how this algorithm works:

- **Sharing knowledge about the entire AS**. Each router shares its knowledge about the entire AS with neighbours. It sends whatever it has.
- **Sharing only with immediate neighbours**. Each router sends whatever knowledge it has thru **all** its interface.
- **Sharing at regular intervals**. sends at fixed intervals, e.g. every 30 sec.

a) Problems: Tedious comparing/updating process, slow response to infinite loop problem, huge list to be maintained!!

Advantages of DVR

- Distance Vector is a relatively simple approach and easy to use, implement and maintain and does not require High-level knowledge to deploy.
- It does not demand high bandwidth level to send their periodic updates as the size of the packets are relatively small.
- distance vector protocols do not require a large amount of CPU resources or memory to store the routing data.

Link-State Routing Process

- *How does a link-state routing protocol work?*
- 5 Step Process:
  1. Each router learns about its own directly connected networks.
  2. Each router is responsible for contacting its neighbors on directly connected networks.
  3. Each router builds a link-state packet (LSP) containing the state of each directly connected link.
  4. Each router floods the LSP to all neighbors, who then store all LSPs received in a database.
  5. Each router uses the LSPs to construct a database that is a complete map of the topology and computes the best path to each destination network.

Link State Routing

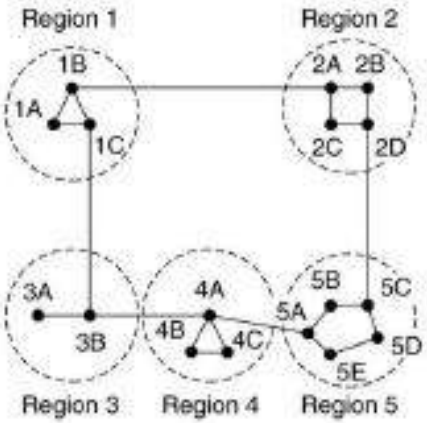
- Each node holds a routing table with the link state of all nodes in the network
  - Periodically or on link change: flood "link state" – list of neighbors (neighbor = 1 hop)
  - Re-broadcasts link state information received from neighbors
  - Use timestamp to distinguish new from stale updates
- Routing
  - The destination is stored in the message header
  - Each forwarding node finds the shortest path to the destination according to its routing table
- On each update of the topology map – each node must calculate the shortest path to all other nodes again.

Hierarchical Routing

- As a network becomes larger, the amount of information that must be propagated increases, and the routing calculation becomes increasingly expensive.
- (Increase the memory amount and calculation)
- Hierarchical routing:
  - Divide the network into regions, with a router only knowing the details of how to route to other routers in its region.
  - Hides information from far-away nodes, reducing the amount of information a given router needs to perform routing
    - Router don't know about the internal topology of other regions.
    - Gateway is a router that knows about other regions

Hierarchical Routing

- Reduce routing table - Scalability
- Enforce administrative autonomy
  - internet = network of networks
  - each network admin may want to control routing in its own network
- Divide into regions (Autonomous Systems)
  - Optimal # of levels ln N, requiring e ln N entries per router
- May cause non-optimal routing
  - E.g. 1A to 5C



Full table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

(b)

Hierarchical table for 1A

Dest.	Line	Hops
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

4+2

(c)

Congestion Control Algorithms

- When too many packets are present is (a part of) the subnet, performance degrades. This situation is called **congestion**.
- When the number of packets dumped into the subnet by the hosts is within its carrying capacity, the number delivered is proportional to the number sent. However, as traffic increases too far, the routers are no longer able to cope, and they begin losing packets.

Internetworking

- What is internetworking?
  - Connect multiple networks of one or more organizations into a large, uniform communication system.
  - The resulting system is called an internetwork or internet.

- What is Internet?
  - The Internet is the specific global internetwork that grew out of ARPA-NET for communication of between computer located anywhere in the world

Security Threats

- According to ITSecurity.com the following are ten of the biggest network threats:
- “1.Viruses and Worms”,
- “2.Trojan Horses”,
- ”3.SPAM”,
- “4.Phishing”,
- “5.Packet Sniffers”,
- ”6. Maliciously Coded Websites”,
- ”7. Password Attacks”,
- “8.Hardware Loss and Residual Data Fragments”,
- “9. Shared Computers”,
- “10.Zombie Computers and Botnets” (ITSecurity [2], 2007)

What is Encryption?

- Encryption is the process of encoding messages or information in such a way that only authorized parties can read it
- A process that converts original information, also called plain text into a difficult-to-interpret form called ciphertext
- Encryption does not of itself prevent interception, but denies the message content to the interceptor
- Done by using an encryption algorithm, a formula used to turn plain text into ciphertext.

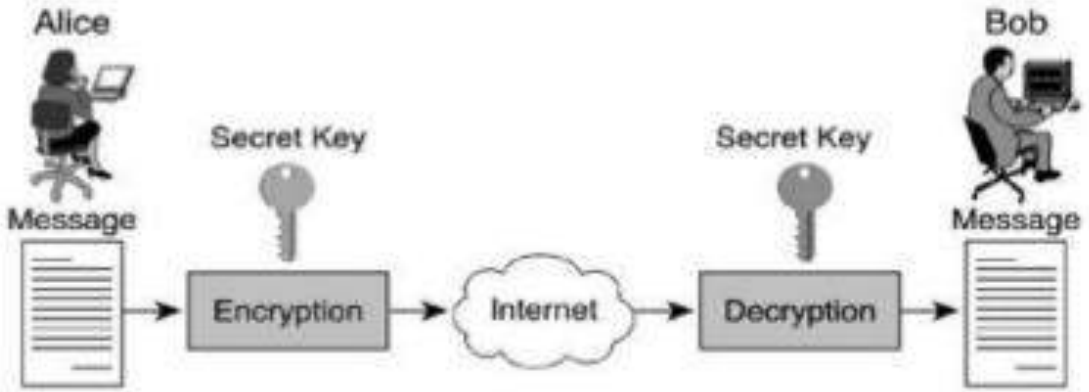
Encryption methods

- **Hashing Encryption**

  Since a hash is unique to a specific message, even minor changes to that message result in a dramatically different hash, thereby alerting a user to potential tampering. Some common hashing algorithms are Message Digest 5 (MD5) and Secure Hashing Algorithm (SHA).

SECRET-KEY ALGORITHMS

* The implementation of a simple cryptography using single key is done by the secret-key algorithms.
* This can be done by p-box, s-box and product cipher.

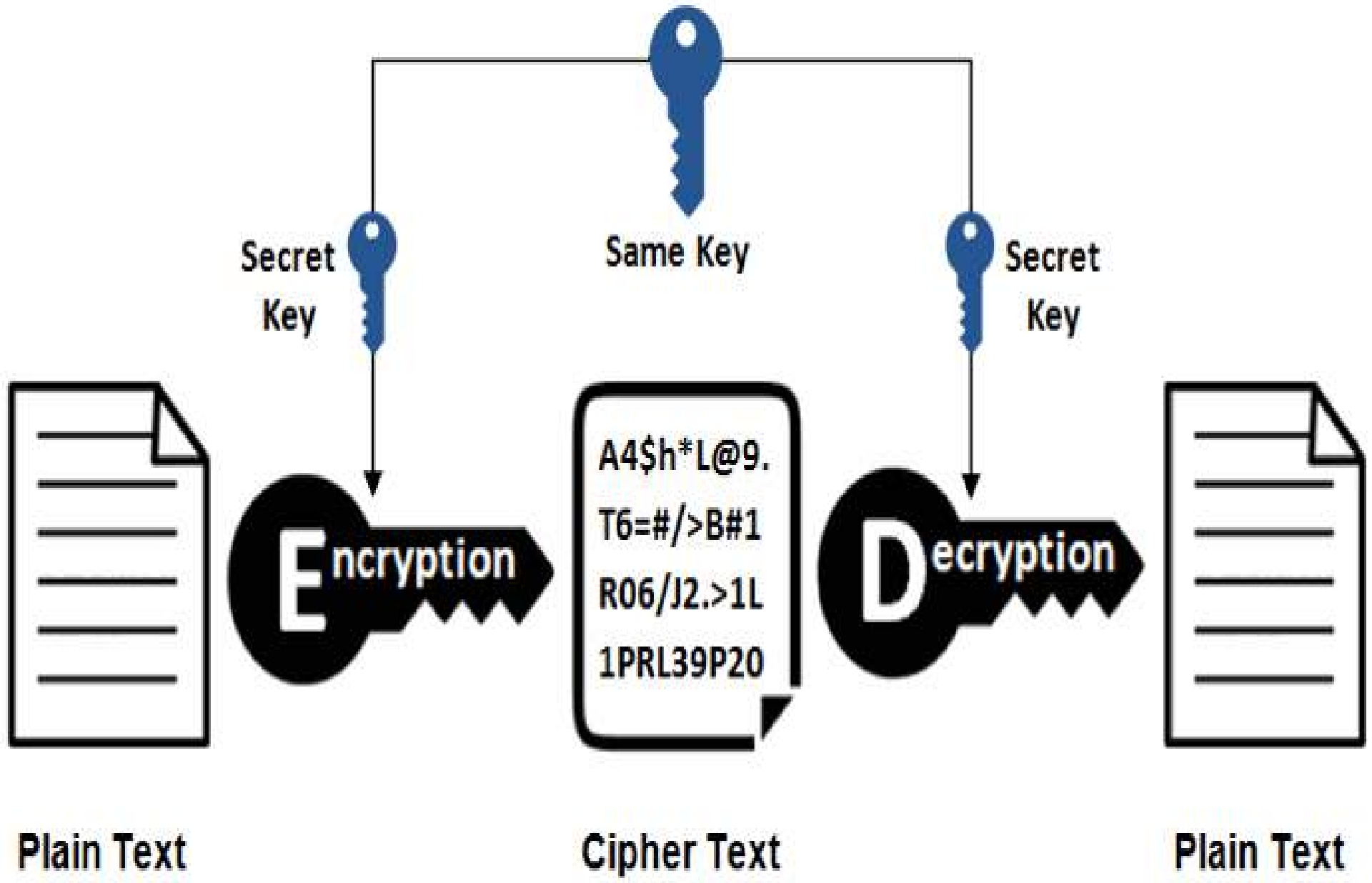


SYMMETRIC ENCRYPTION

TRIAD
SQUARE INFOSEC PVT.LTD

- An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message.
- In other terms, Data is encrypted and decrypted using the same key.
- Symmetric-key cryptography is sometimes called *secret-key cryptography*.

Symmetric Encryption



PUBLIC KEY CRYPTOGRAPHY

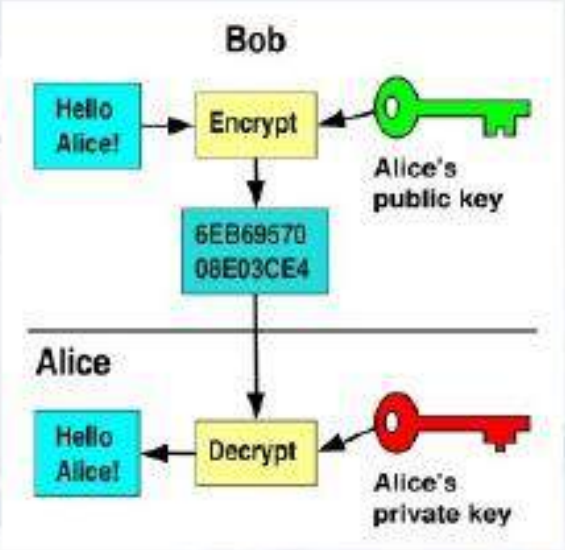
- A form of cryptography in which the key used to encrypt a message differs from the key used to decrypt it.
- In public key cryptography, a user has a pair of cryptographic keys—a public key and a private key. The private key is kept secret, while the public key may be widely distributed.
- The two main branches of public key cryptography are:

1. **Public key encryption**
2. **Digital signatures**

PUBLIC KEY ENCRYPTION

- **A message encrypted with a recipient's public key cannot be decrypted by anyone except the recipient possessing the corresponding private key.**

Actual algorithms - two linked keys:



Contd.

Public Key Encryption

- A good public key algorithm:
  - Infeasible to derive one key from the other
  - Keys are interchangeable
- Simplifies (but does not solve) key distribution problem
- Public key is slower than secret key algorithms
  - RSA is about 1000-5000 times slower than DES
  - Public key encryption is sometimes used to encrypt a secret key algorithm's session key