DATA COMMUNICATION & NETWORKING

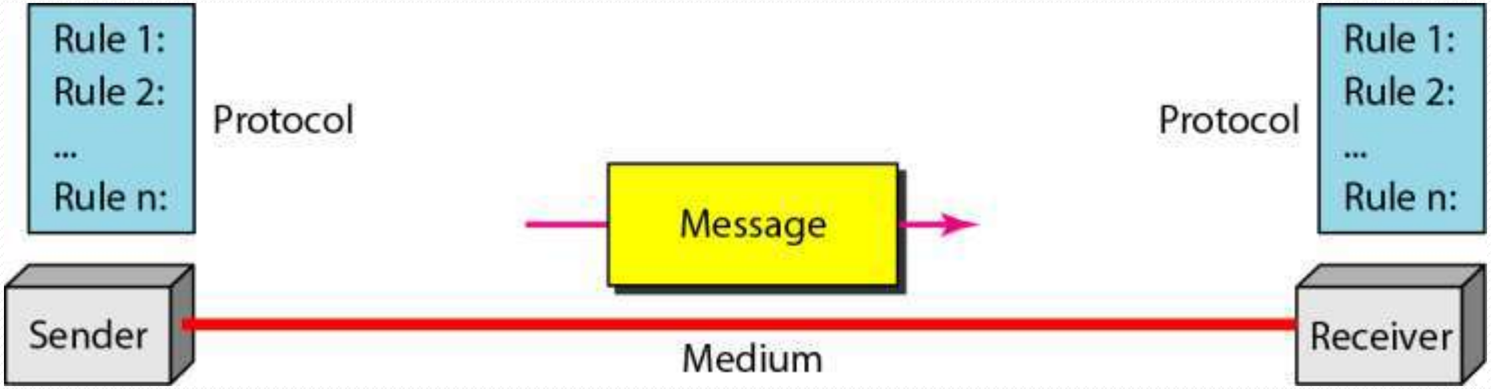
PREPARED BY

Mrs. V.SATHIYAVANI,M.E(Ph. D),
ASST.PROFESSOR,ECE DEPT,
KUPPAM ENGINEERING COLLEGE.

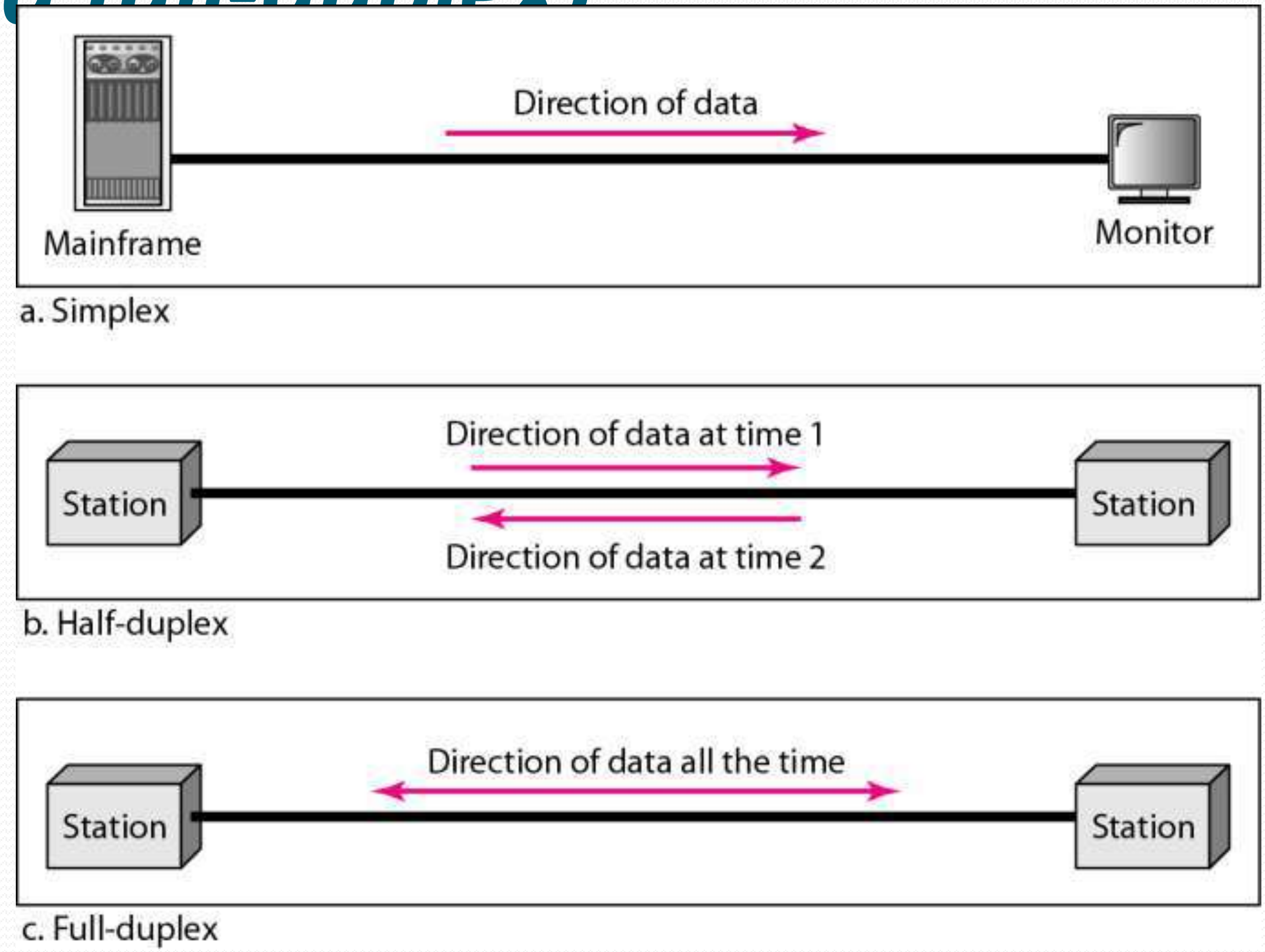
Data Communication

- The term telecommunication means communication at a distance.
- The word data refers to information presented in whatever form is agreed upon by the parties creating and using the data.
- Data communications are the exchange of data between two devices via some form of transmission medium such as a wire cable.

Components of a data communication system



Data flow (simplex, half-duplex, and full-duplex)


Direction of data
Mainframe
Monitor
Direction of data at time 1
Station
Station
Direction of data at time 2
Direction of data all the time
Station
Station

a. Simplex

b. Half-duplex

c. Full-duplex

NETWORKS

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

Network Criteria Performance

- Performance
  - Depends on Network Elements
  - Measured in terms of Delay and Throughput
- Reliability
  - Failure rate of network components
  - Measured in terms of availability/robustness
- Security
  - Errors
  - Malicious users

Categories of Networks

- Local Area Networks (LANs)

  Short distances

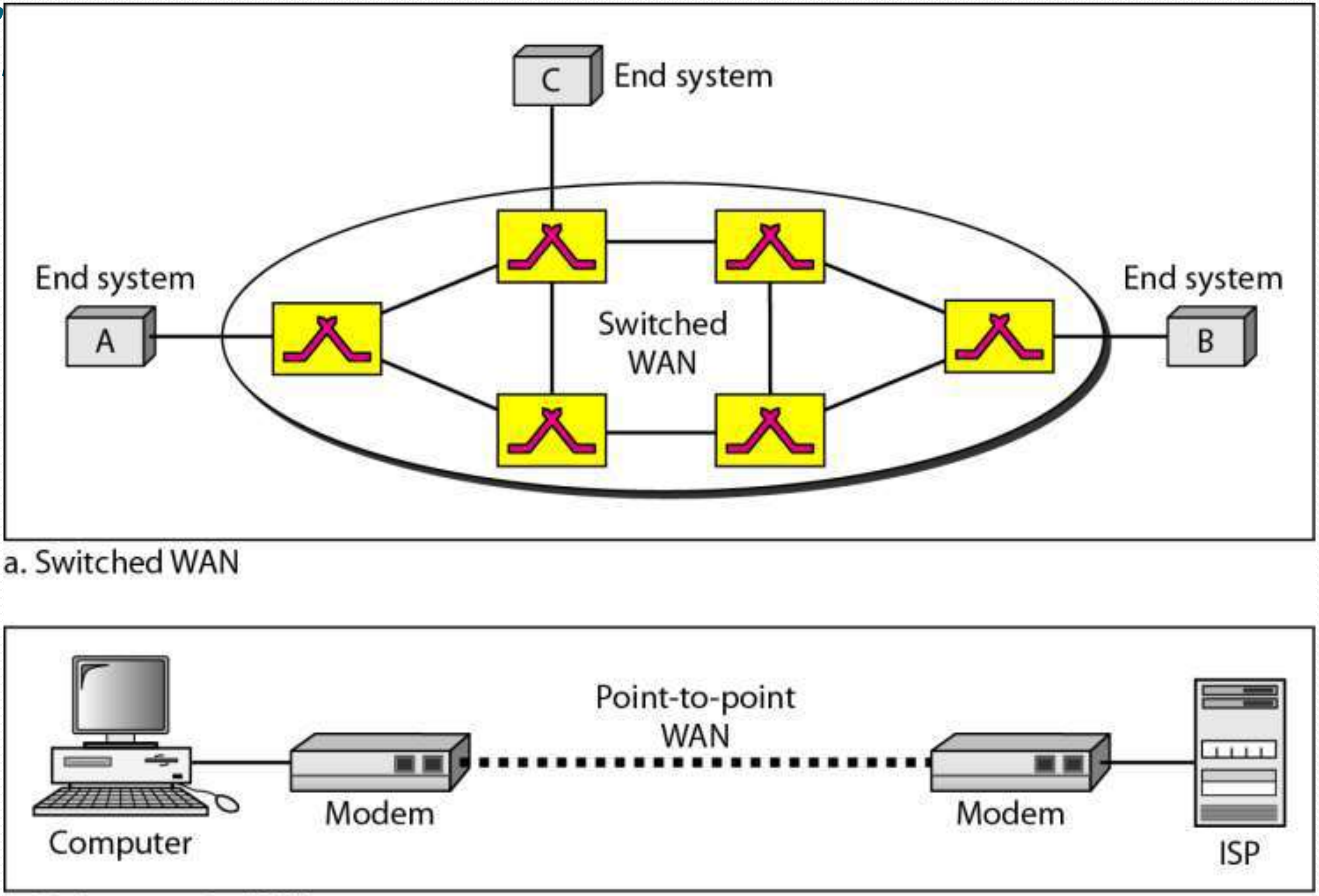
  Designed to provide local interconnectivity
- Wide Area Networks (WANs)

  Long distances

  Provide connectivity over large areas
- Metropolitan Area Networks (MANs)

  Provide connectivity over areas such as a city, a campus

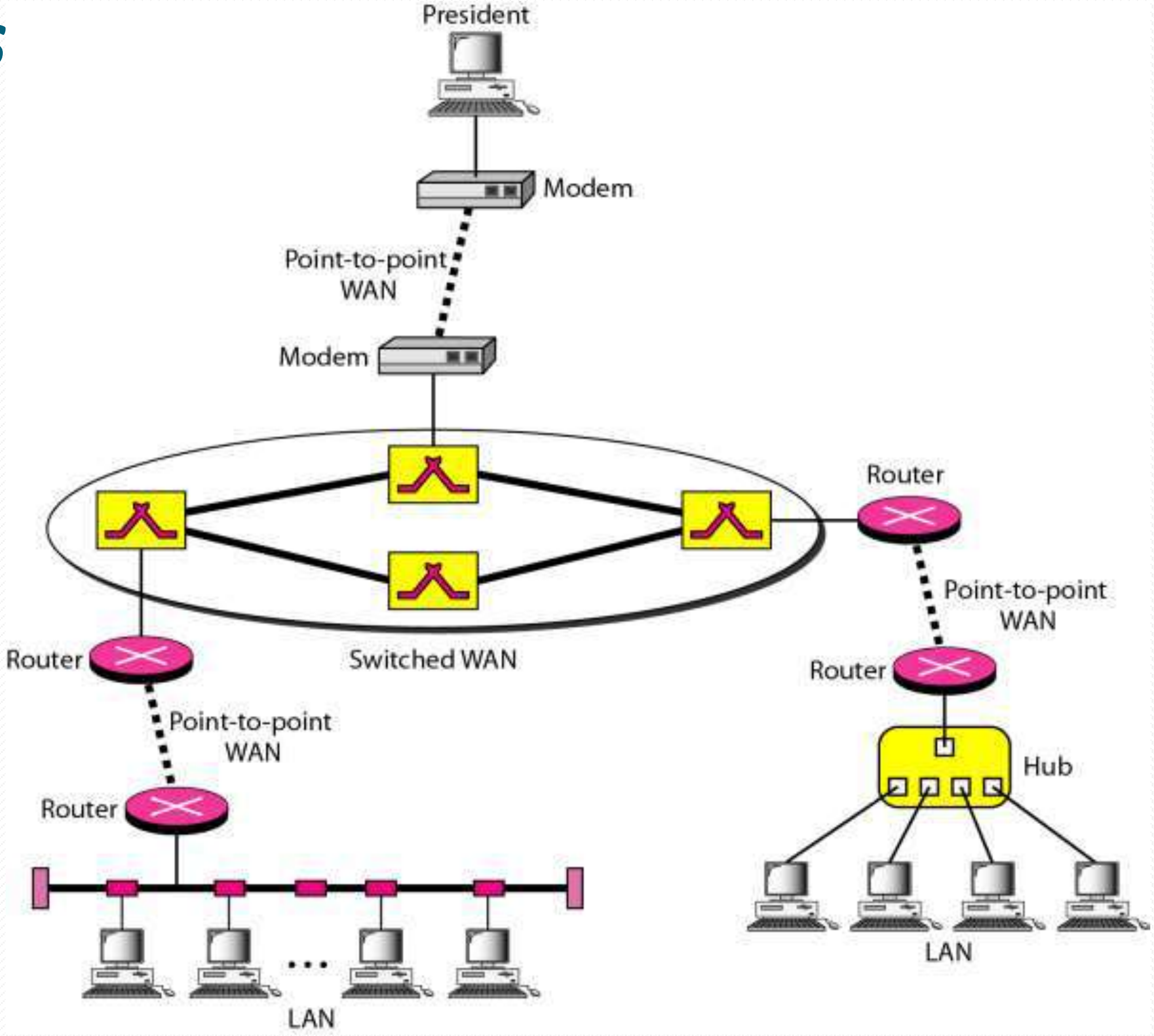
WANs: a switched WAN and a poi



a. Switched WAN

b. Point-to-point WAN

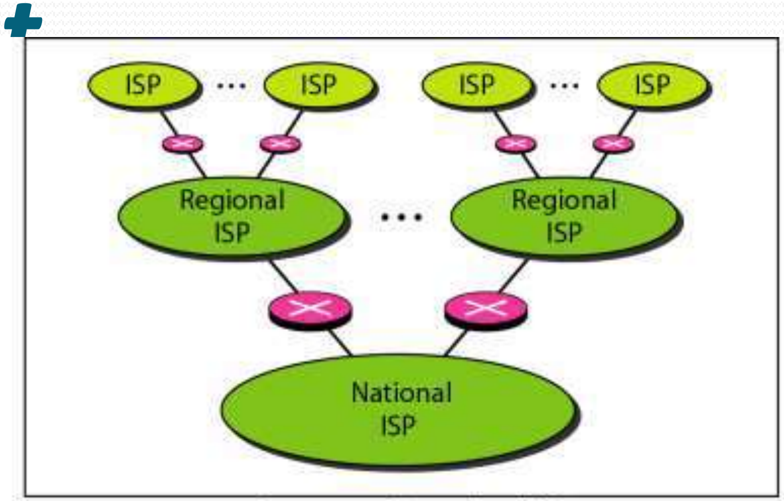
A heterogeneous network made of four WANs



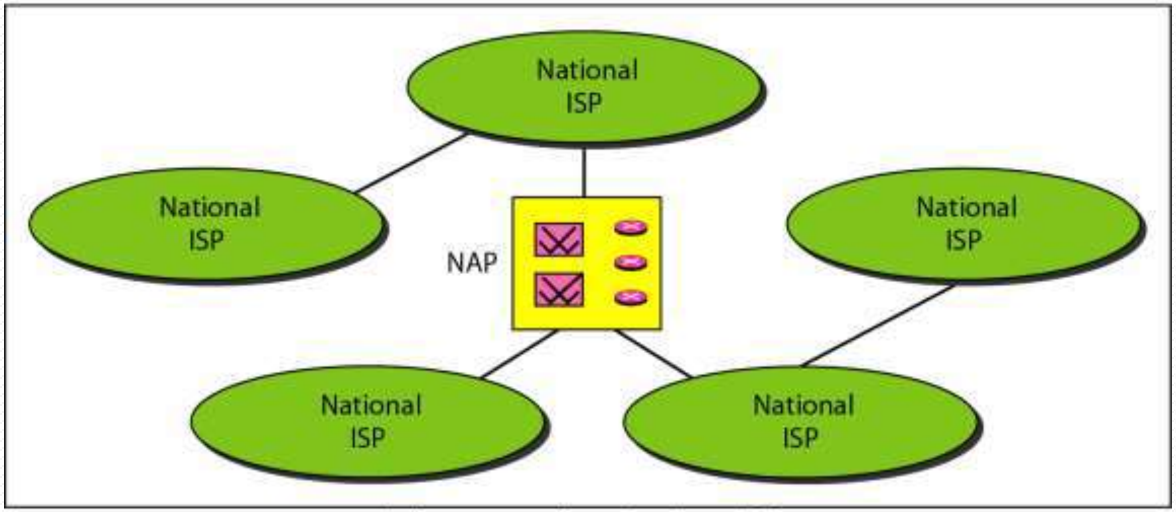
THE INTERNET

- The Internet has revolutionized many aspects of our daily lives. It has affected the way we do business as well as the way we spend our leisure time.
- The Internet is a communication system that has brought a wealth of information to our finger tips and organized it for our use.

Hierarchical organization of the Internet



a. Structure of a national ISP



b. Interconnection of national ISPs

Hierarchical organization

- **International Internet Service Providers**: At the top of the hierarchy are the international service providers that connect nations together.
- **National Internet Service Providers**: The national Internet service providers are backbone networks created and maintained by specialized companies.
- **Regional Internet Service Providers**: Regional internet service providers or regional ISPs are smaller ISPs that are connected to one or more national ISPs.
- **Local Internet Service Providers**: Local Internet service providers provide direct service to the end users.

PROTOCOLS & STANDARDS

- A protocol is synonymous with rule. It consists of a set of rules that govern data communications.
- It determines what is communicated, how it is communicated and when it is communicated.
- The key elements

  Syntax

  Semantics

  Timing

Elements of a Protocol

- Syntax

  Structure or format of the data

  Indicates how to read the bits -field delineation

- Semantics

  Interprets the meaning of the bits

  Knows which fields define what action

- Timing

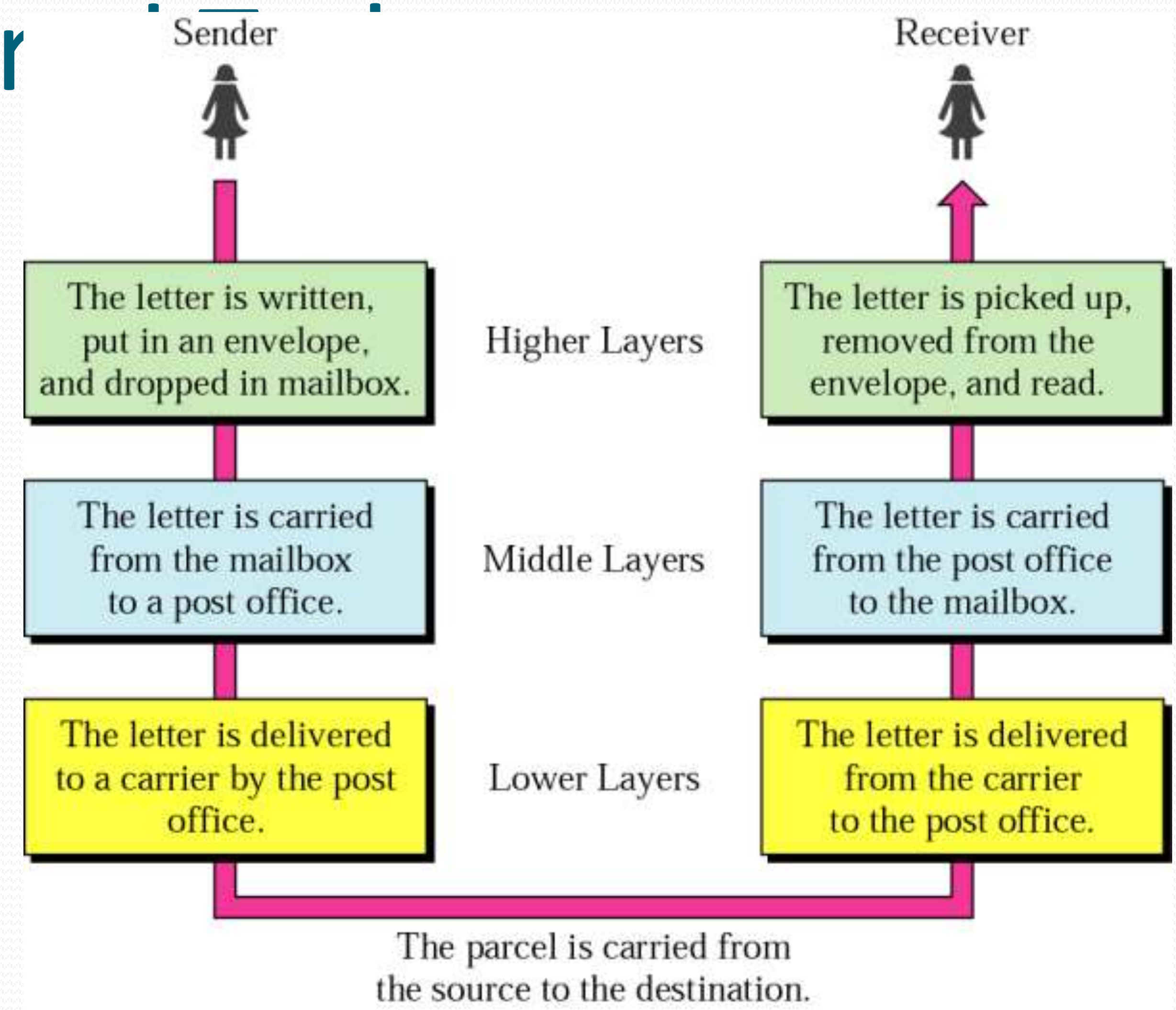
  When data should be sent and what

  Speed at which data should be sent or speed at which it is being

STANDARDS

- International Organization for Standardization (ISO)
- International Telecommunication Union-Telecommunication Standards Sector (ITU-T)
- American National Standards Institute (ANSI)
- Institute of Electrical and Electronics Engineers (IEEE)
- Electronic Industries Association (EIA)

Layer



Sender

Receiver

The letter is written, put in an envelope, and dropped in mailbox.

Higher Layers

The letter is picked up, removed from the envelope, and read.

The letter is carried from the mailbox to a post office.

Middle Layers

The letter is carried from the post office to the mailbox.

The letter is delivered to a carrier by the post office.

Lower Layers

The letter is delivered from the carrier to the post office.

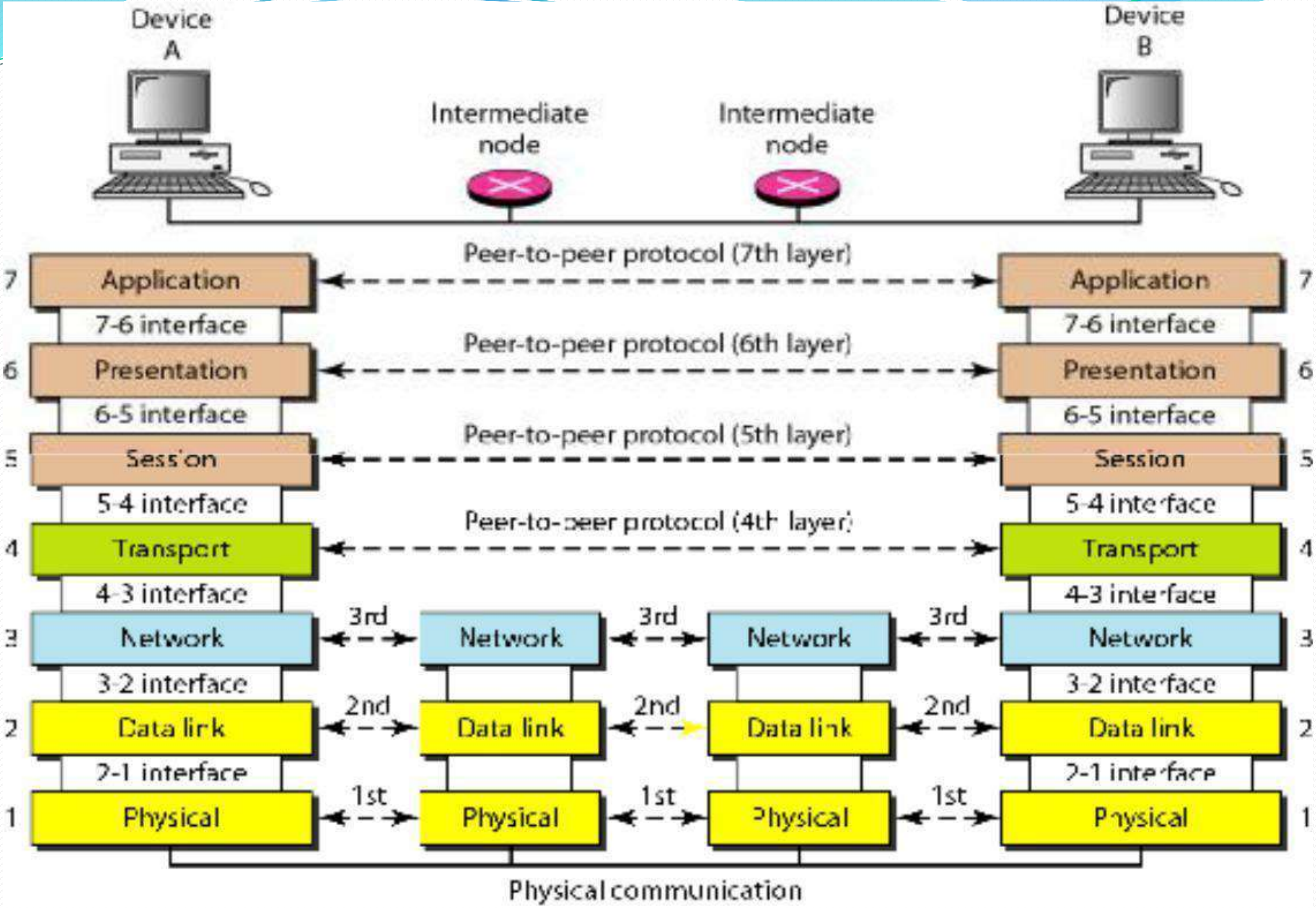
The parcel is carried from the source to the destination.

Why layered communication?

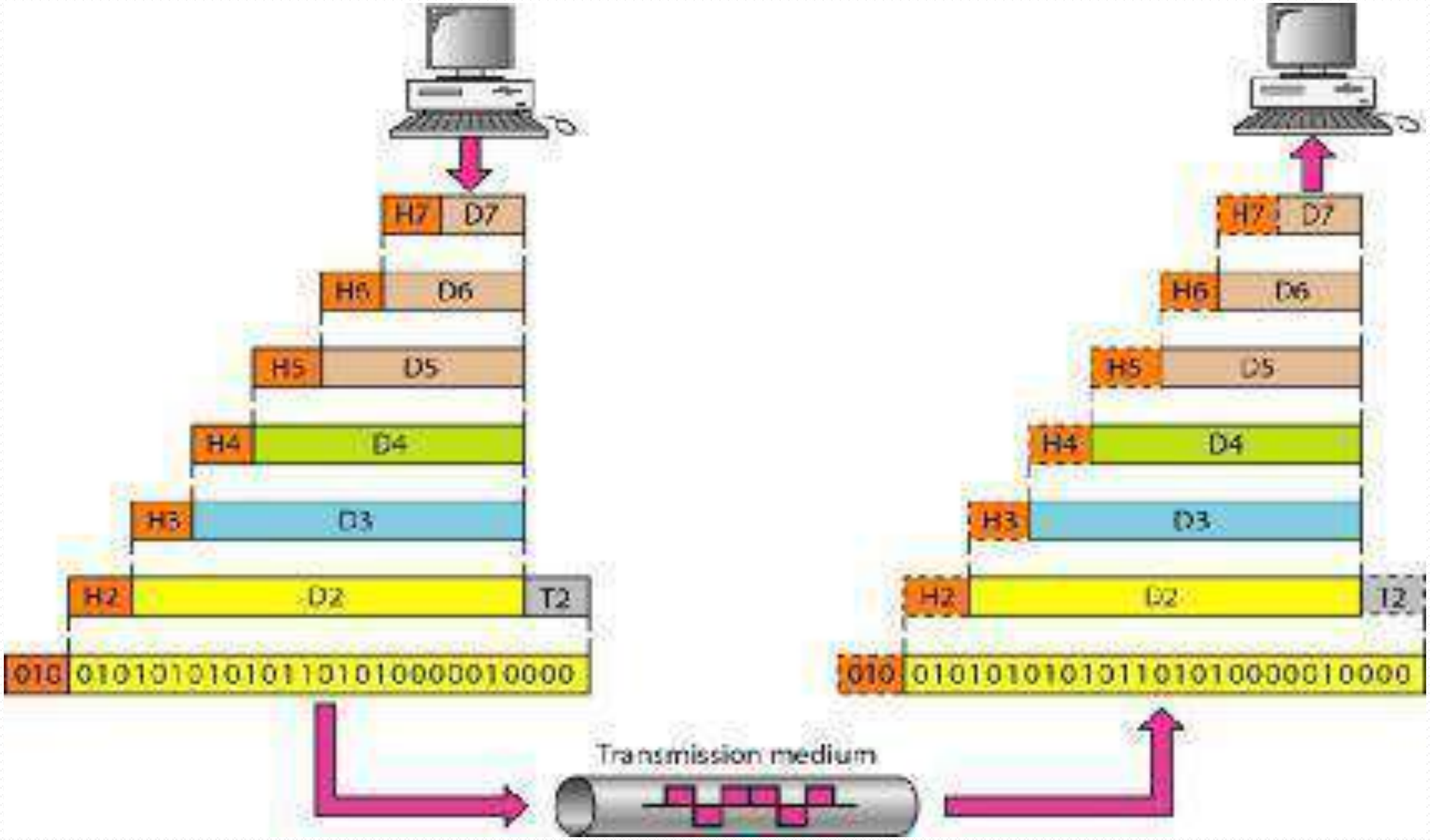
- To reduce complexity of communication task by splitting it into several layered small tasks
- Functionality of the layers can be changed as long as the service provided to the layer above stays unchanged
- Makes easier maintenance & updating
- Each layer has its own task
- Each layer has its own protocol
- There are two layered Models namely OSI Model and TCP/IP Model

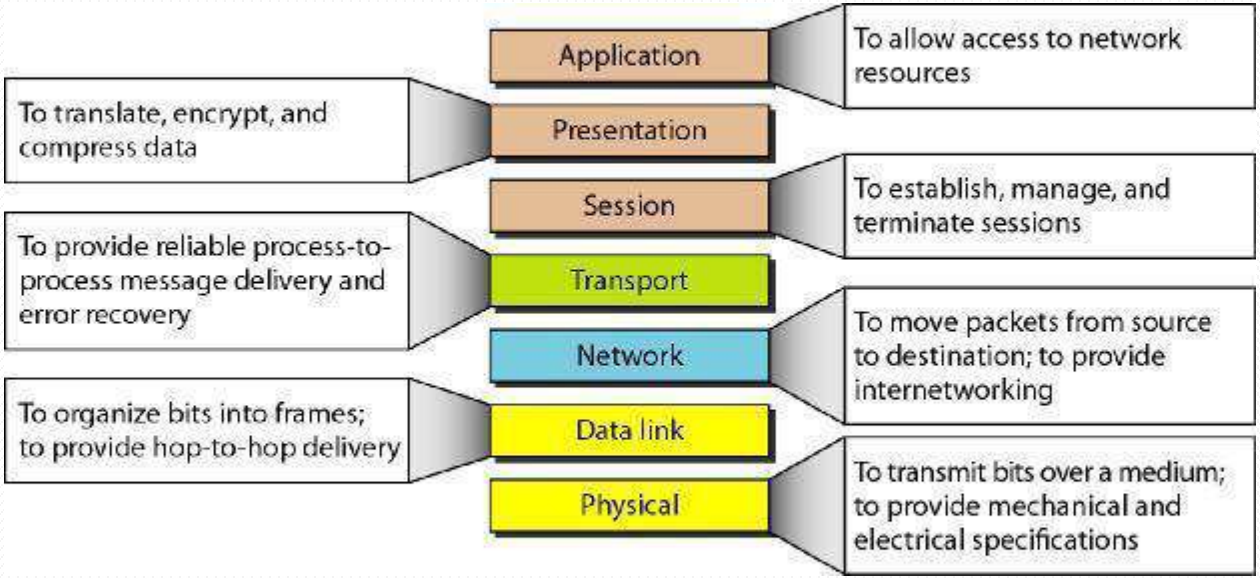
OSI Reference model

- Open System Interconnection
- The Open Systems Interconnection (OSI) reference model was approved as an international standard for communications architecture.
- The purpose of OSI Model is to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.
- The OSI reference model divides the problem of moving information between computers over a network medium into SEVEN smaller and more manageable problems.


Device A
Device B
Intermediate node
Intermediate node
Peer-to-peer protocol (7th layer)
7
Application
Application
7
7-6 interface
7-6 interface
Peer-to-peer protocol (6th layer)
6
Presentation
Presentation
6
6-5 interface
6-5 interface
Peer-to-peer protocol (5th layer)
5
Session
Session
5
5-4 interface
5-4 interface
Peer-to-peer protocol (4th layer)
4
Transport
Transport
4
4-3 interface
4-3 interface
3
Network
3rd
Network
3rd
Network
3rd
Network
3
3-2 interface
3-2 interface
2
Data link
2nd
Data link
2nd
Data link
2nd
Data link
2
2-1 interface
2-1 interface
1
Physical
1st
Physical
1st
Physical
1st
Physical
1
Physical communication

- Message descends from top layer to bottom layer
- Each layer interact and exchange data with same layer in other side
- As the message descends, each successive OSI model layer adds a header to it.





Application

To allow access to network resources

Presentation

To translate, encrypt, and compress data

Session

To establish, manage, and terminate sessions

Transport

To provide reliable process-to-process message delivery and error recovery

Network

To move packets from source to destination; to provide internetworking

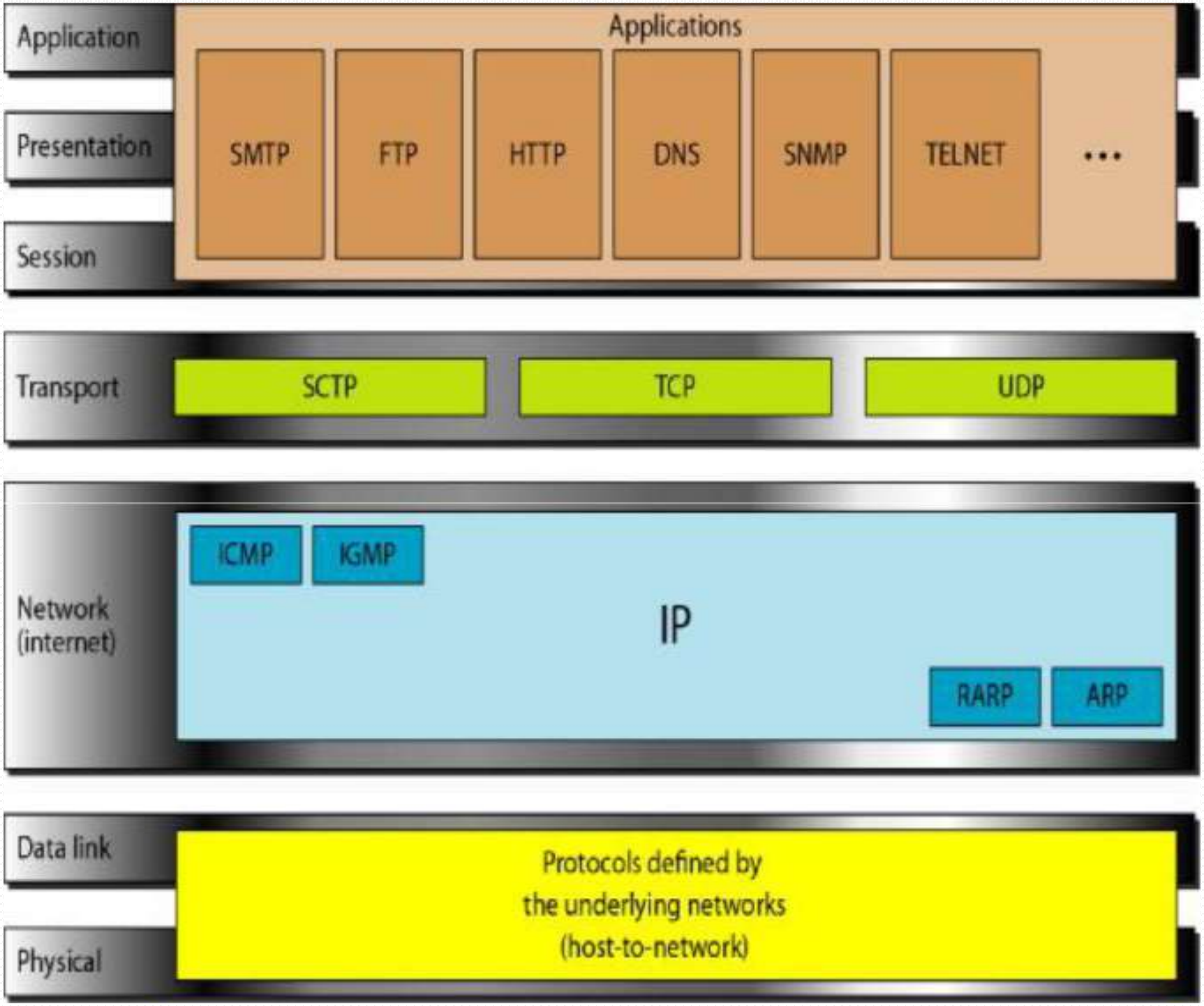
Data link

To organize bits into frames; to provide hop-to-hop delivery

Physical

To transmit bits over a medium; to provide mechanical and electrical specifications

- TCP/IP protocol suite is made of five layers: physical, data link, network, transport, and application.



TCP/IP MODEL

APPLICATION LAYER

- Application layer protocols define the rules when implementing specific network applications. It relies on the underlying layers to provide accurate and efficient data delivery. Typical protocols are
- FTP – File Transfer Protocol: For file transfer
- Telnet – Remote terminal protocol: For remote login on any other computer on the network
- SMTP – Simple Mail Transfer Protocol: For mail transfer
- HTTP – Hypertext Transfer Protocol: For Web browsing

TRANSPORT LAYER

- Transport Layer protocols define the rules of dividing a chunk of data into segments and then reassemble segments into the original chunk . Typical protocols are:
- TCP – Transmission Control Protocol: Provide functions such as reordering and data resend.
- UDP – User Datagram Service: Use when the message to be sent fit exactly into a datagram and Use also when a more simplified data format is required.
- SCTP - Stream Control Transmission Protocol

  provides support for newer applications such as voice over the Internet

NETWORK LAYER

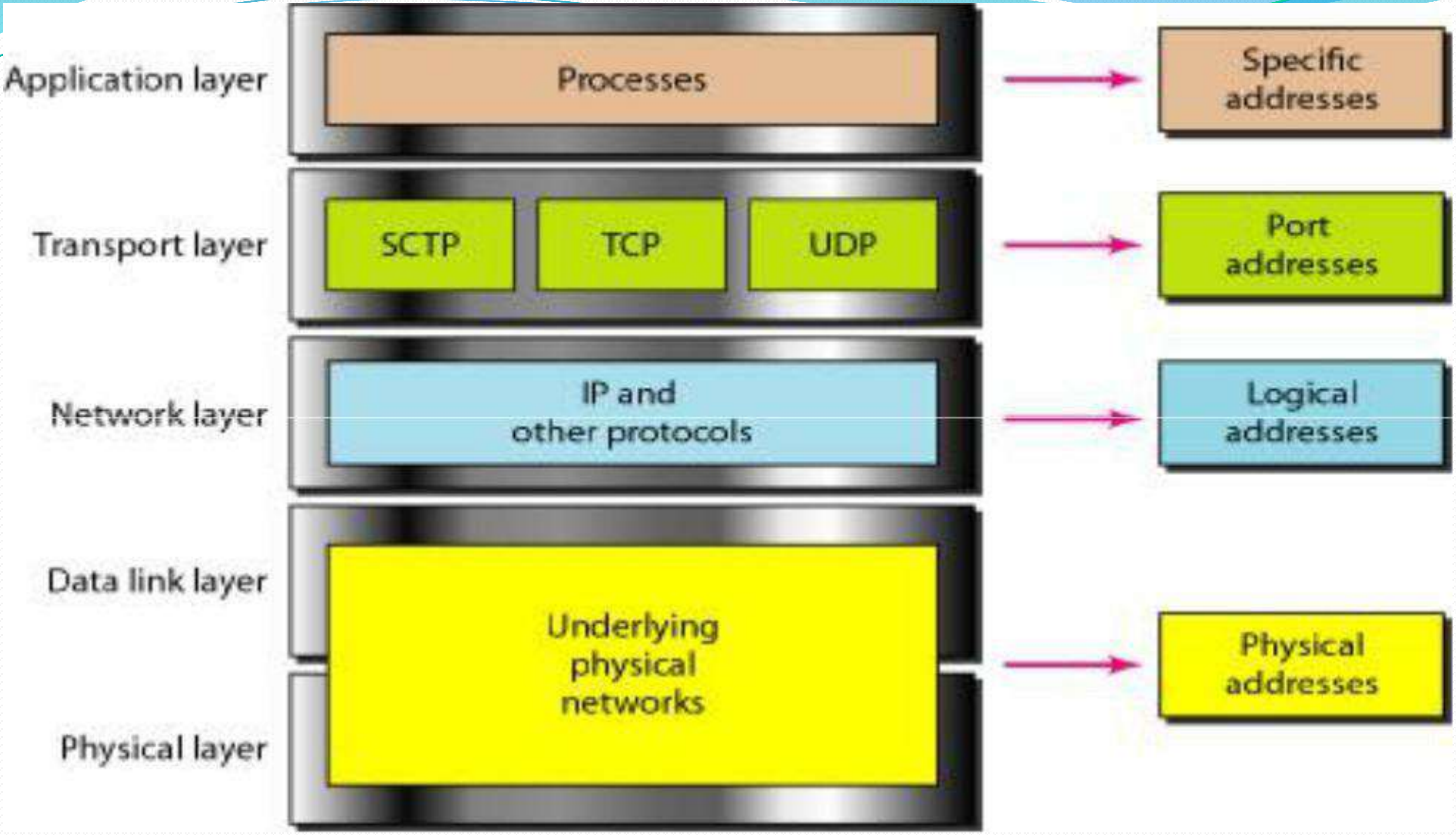
- Network layer protocols define the rules of how to find the routes for a packet to the destination(Packets can be delayed, corrupted, lost, duplicated, out-of-order) it gives best delivery.
- IP – Internet Protocol
- ARP
- RARP – Reverse Address Resolution Protocol
- ICMP – Internet Control Message Protocol
- IGMP – Internet Group Message Protocol

PHYSICAL AND DATA LINK LAYER

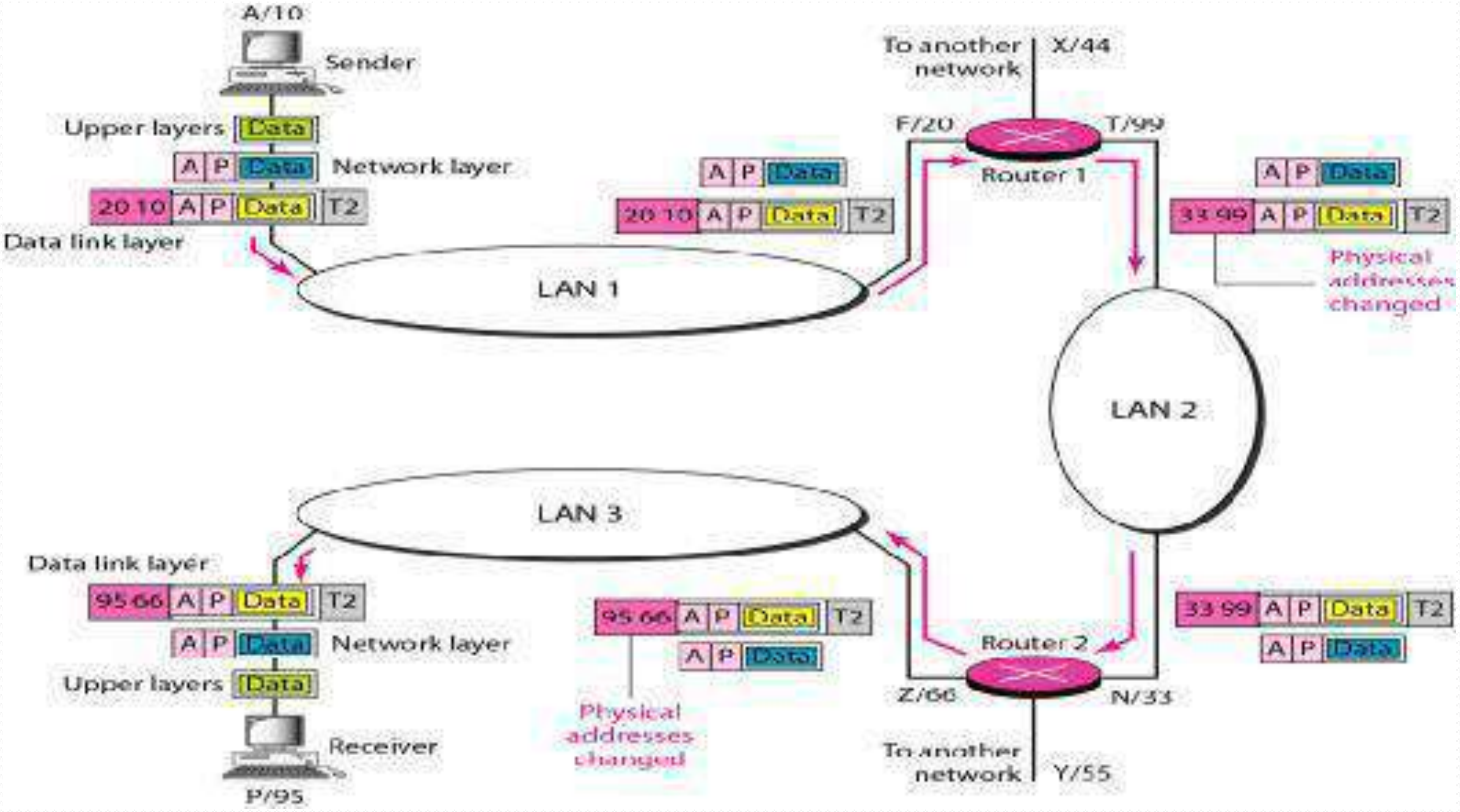
- TCP-IP does not define any specific protocol. Rather, it supports all the standard protocols

ADDRESSING

- There are four levels of addresses are used in an internet employing the TCP/IP protocols: physical, logical, port, and specific.
- **PHYSICAL ADDRESSING:** also known as the **link address**, it is the address of a node as defined by its LAN or WAN
- It is included in the frame used by the data link layer
- It is the lowest-level address.
- The size and format of these addresses vary depending on the network.

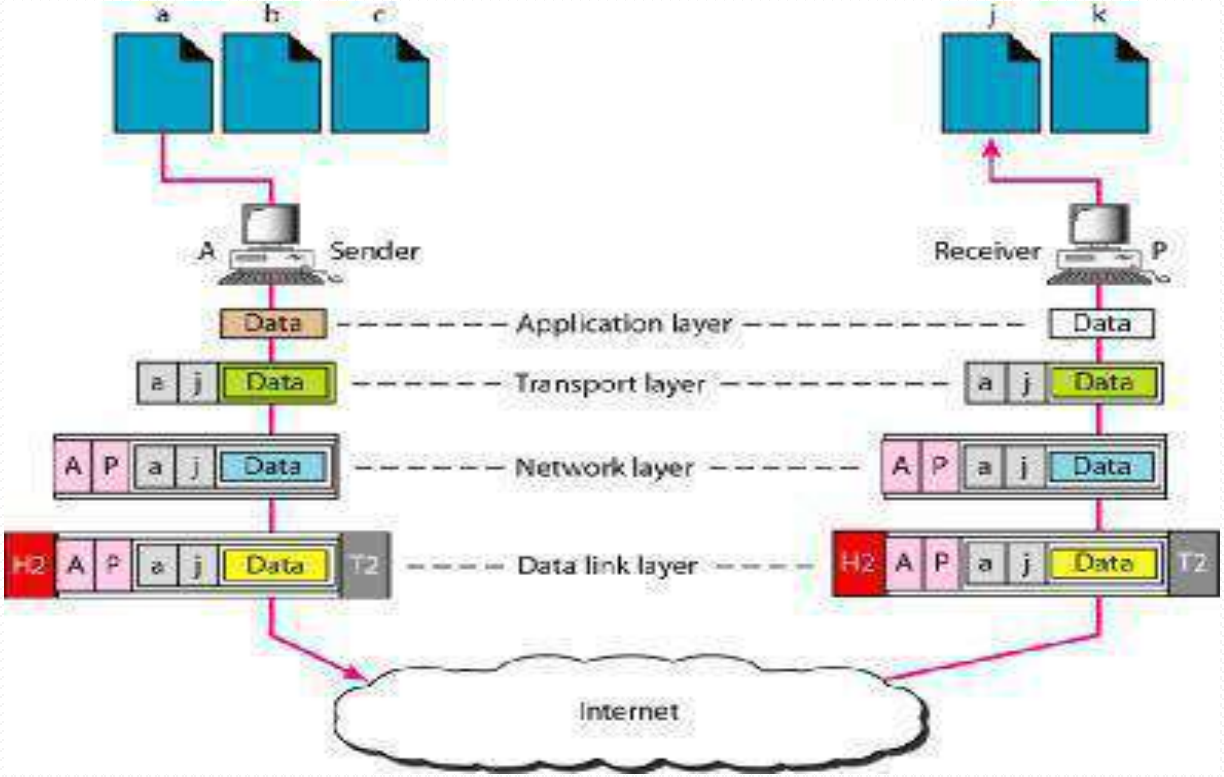

Application layer
Processes
Specific addresses
Transport layer
SCTP
TCP
UDP
Port addresses
Network layer
IP and other protocols
Logical addresses
Data link layer
Underlying physical networks
Physical addresses
Physical layer

- **LOGICAL ADDRESSING:** Logical addresses are necessary for universal communications that are independent of underlying physical networks.



PORT ADDRESSING

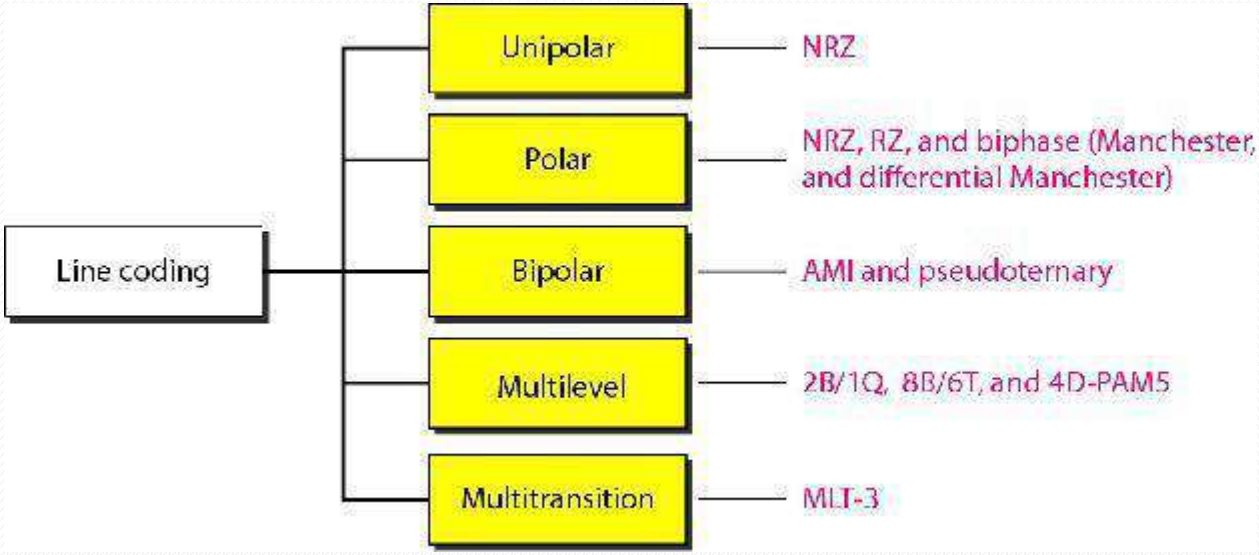
- The IP address and the physical address are necessary for a quantity of data to travel from a source to the destination host



LINE CODING

- Line coding is the process of converting digital data to digital signals.
- Data, in the form of text, numbers, graphical images, audio, or video, are stored in computer memory as sequences of bits.

Contd



Line coding

Unipolar — NRZ

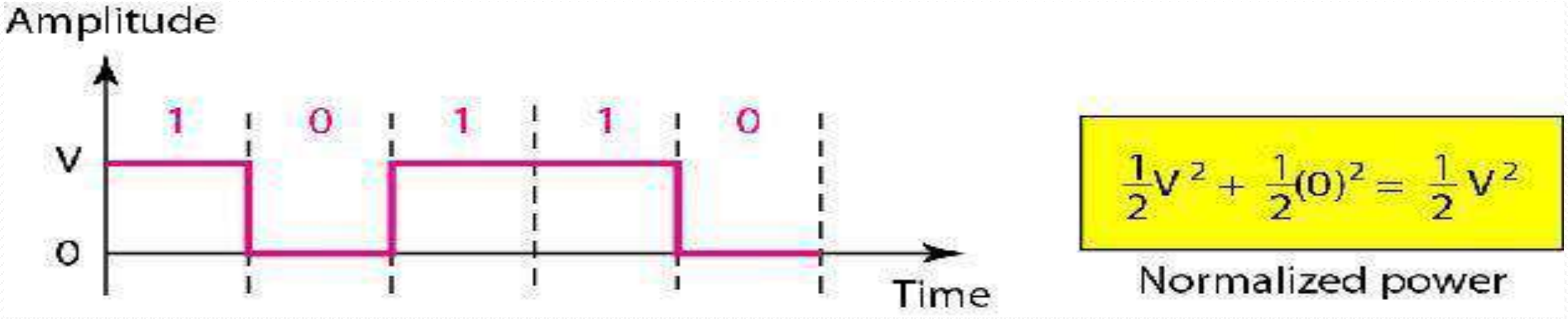
Polar — NRZ, RZ, and biphase (Manchester, and differential Manchester)

Bipolar — AMI and pseudoternary

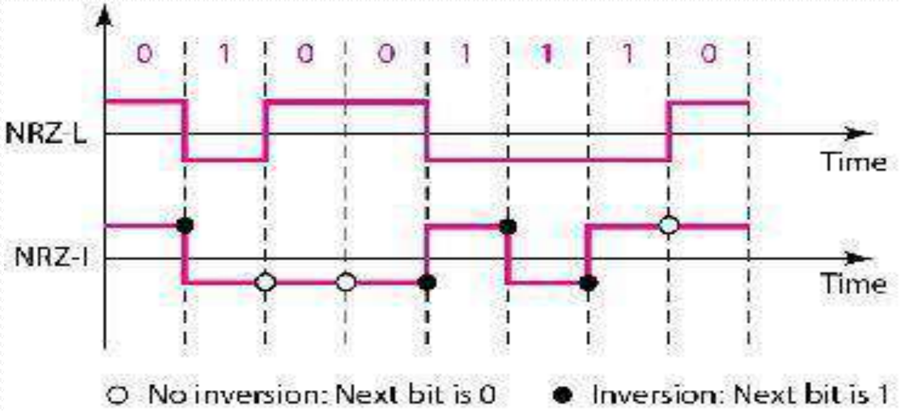
Multilevel — 2B/1Q, 8B/6T, and 4D-PAM5

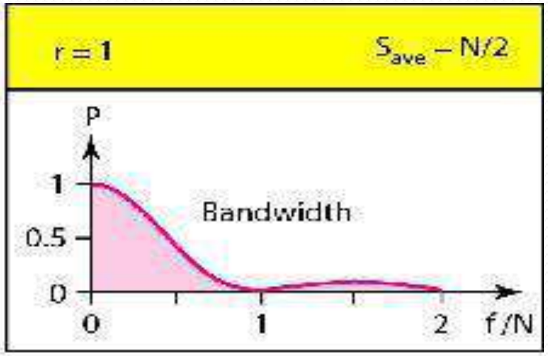
Multitransition — MLT-3

- Unipolar Scheme: In a unipolar scheme, all the signal levels are on one side of the time axis, either above or below.

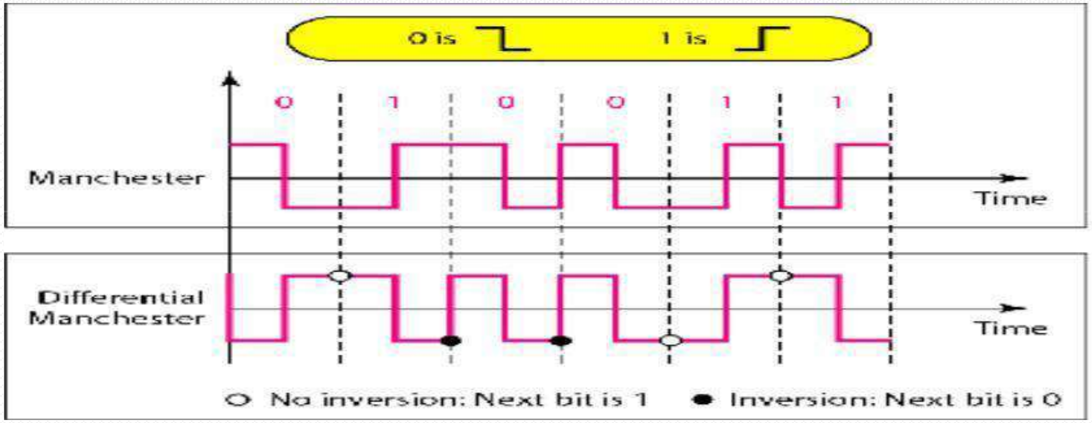


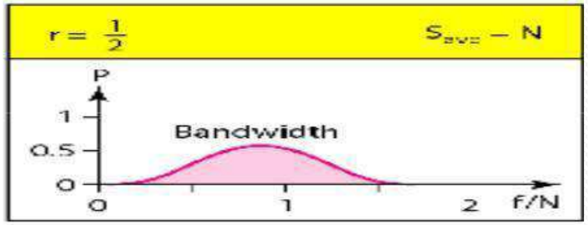
- Polar Schemes: In polar schemes, the voltages are on the both sides of the time axis





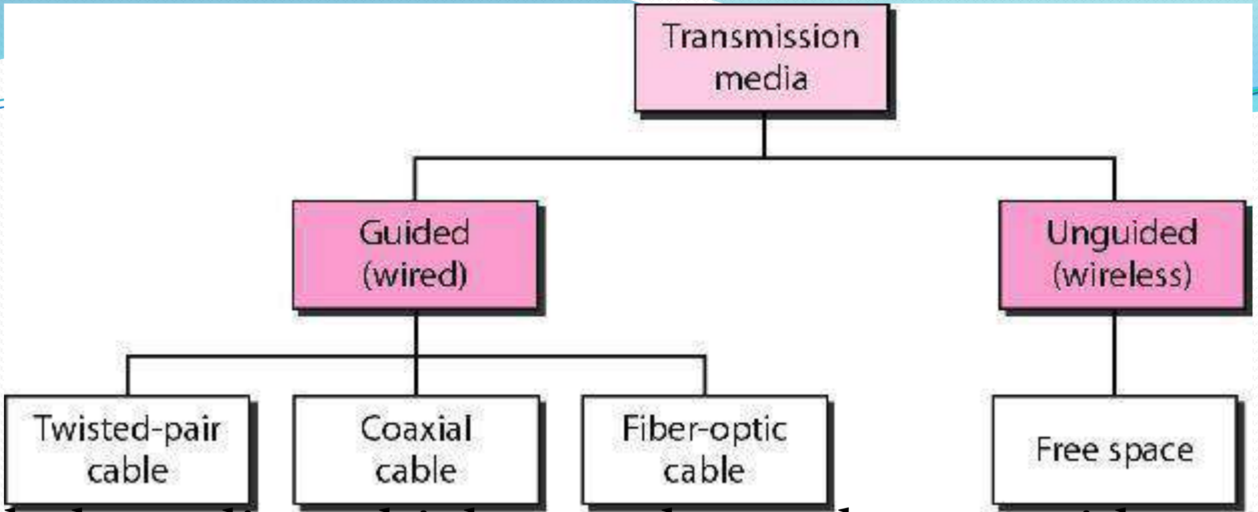
- Manchester and Differential Manchester: In Manchester encoding, the duration of the bit is divided into two halves.



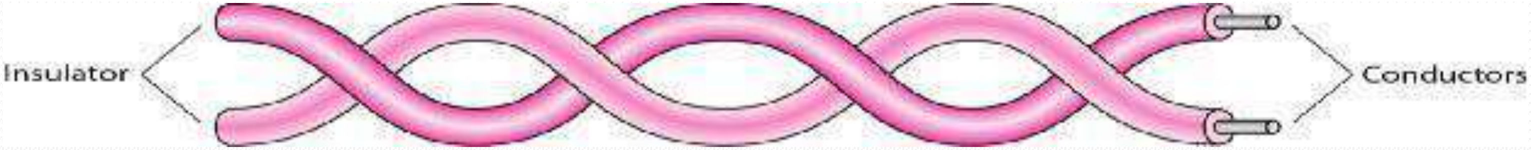


TRANSMISSION MEDIA

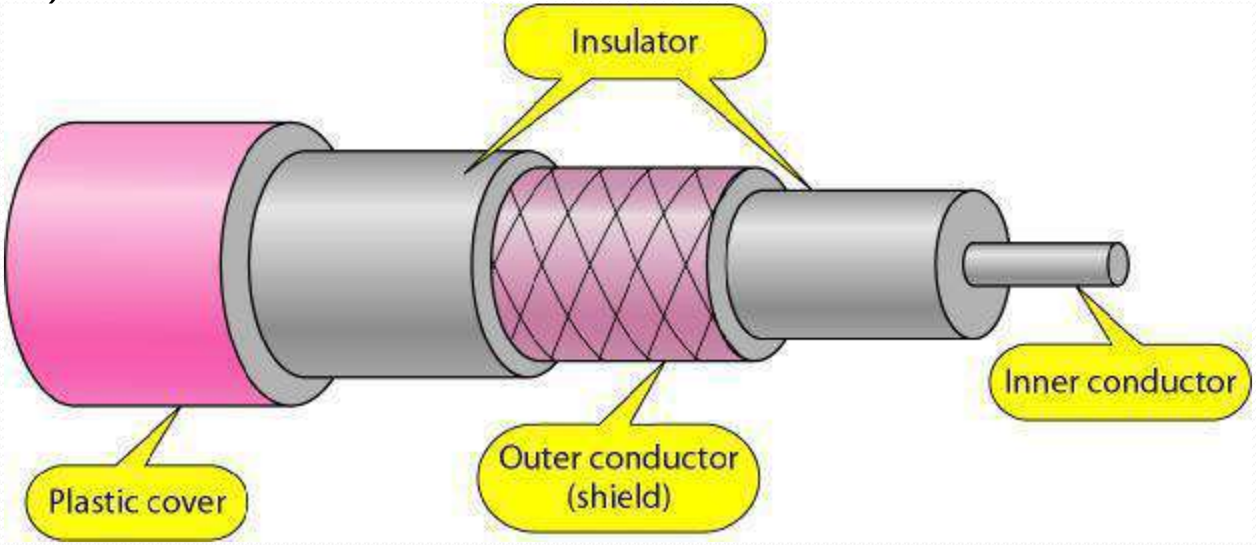
- A transmission medium can be broadly defined as anything that can carry information from a source to a destination.
- In data communications the definition of the information and the transmission medium is more specific.
- The transmission medium is usually free space, metallic cable, or fiber-optic cable.



- Guided media, which are those that provide a conduit from one device to another, include twisted-pair cable, coaxial cable, and fiber-optic cable.
- Twisted Pair Cable: A twisted pair consists of two conductors (normally copper), each with its own plastic insulation, twisted together
- Twisted-pair cables are used in telephone lines to provide voice and data channels

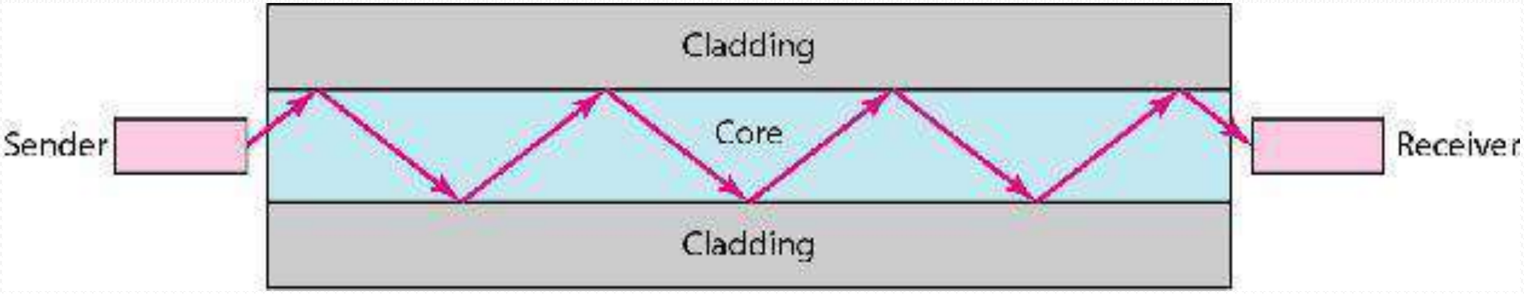


- Coaxial Cable: Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable,

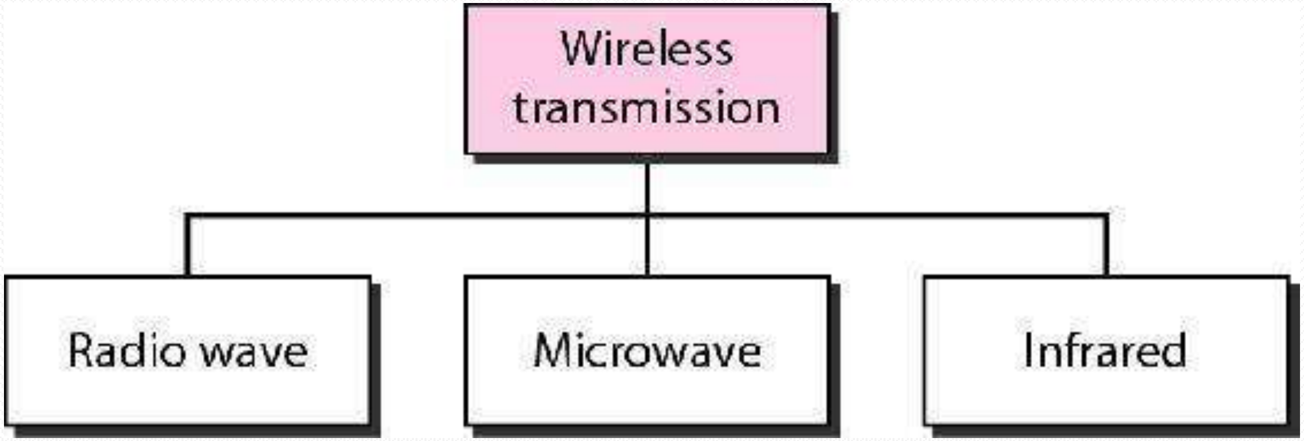


a single coaxial network could carry **10,000** voice signals

- Fiber Optic Cable: fiber-optic cable is made of glass or plastic and transmits signals in the form of light
- To understand optical fiber, we first need to explore several aspects of the nature of light.
- Light travels in a straight line as long as it is moving through a single uniform substance.



- Unguided media transport electromagnetic waves without using a physical conductor This type of communication is often referred to as wireless communication



Wireless transmission

Radio wave

Microwave

Infrared

Wireless (Unguided Media) Transmission

- transmission and reception are achieved by means of antenna
- Directional

    Transmitting antenna puts out focused beam

    Transmitter and receiver must be aligned

- Omni directional

    signal spreads out in all directions

    can be received by many antennas

Wireless Examples

- Terrestrial microwave
- Satellite microwave
- Broadcast radio
- infrared

- **Terrestrial Microwave**
  used for long-distance telephone service
  uses radio frequency spectrum, from 2 to 40 Ghz
  Parabolic dish transmitter, mounted high
  used by common carriers as well as private networks
  requires unobstructed line of sight between source and receiver
  curvature of the earth requires stations (repeaters) ~30 miles apart
- **Applications**
  Television distribution
  Long-distance telephone transmission
  Private business networks

- Microwave Transmission Disadvantages

  line of sight requirement

  expensive towers and repeaters

  subject to interference such as passing airplanes and rain

- Satellite Microwave Transmission

  a microwave relay station in space

  can relay signals over long distances

  geostationary satellites

  remain above the equator at a height of 22,300 miles (geosynchronous orbit)

  travel around the earth in exactly the time the earth takes to rotate

- Applications

  television distribution

  a network provides programming from a central location

  direct broadcast satellite (DBS)

  long-distance telephone transmission

  high-usage international trunks

  private business networks

- Principal Satellite Transmission Bands

  C band: 4(downlink) -6(uplink) GHz

  the first to be designated

  Ku band: 12(downlink) -14(uplink) GHz

  rain interference is the major problem

  Ka band: **19(downlink) -29(uplink) GHz**

  equipment needed to use the band is still very expensive

Radio

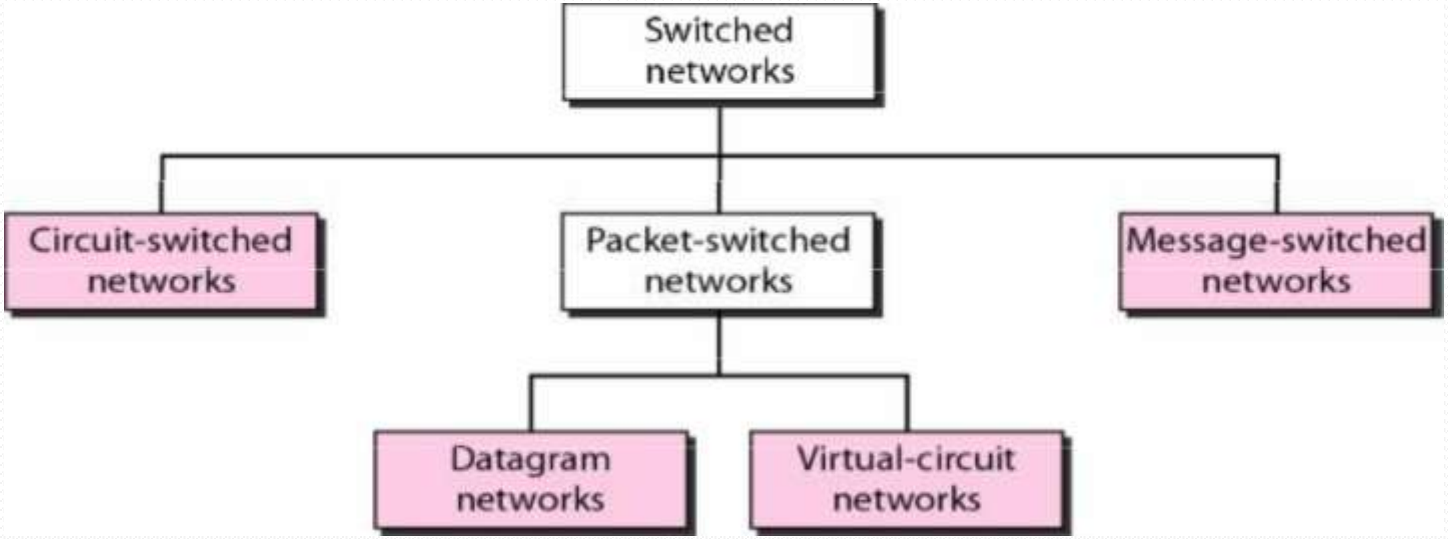
- Radio is Omni directional and microwave is directional
- Radio is a general term often used to encompass frequencies in the range 3 kHz to 300 GHz.
- Mobile telephony occupies several frequency bands just under 1 GHz.

Infrared

- Uses transmitters/receivers (transceivers) that modulate non coherent infrared light.
- Transceivers must be within line of sight of each other (directly or via reflection).
- Unlike microwaves, infrared does not penetrate walls.

SWITCHING

Switching is process to forward packets coming in from one port to a port leading towards the destination.



Switched networks

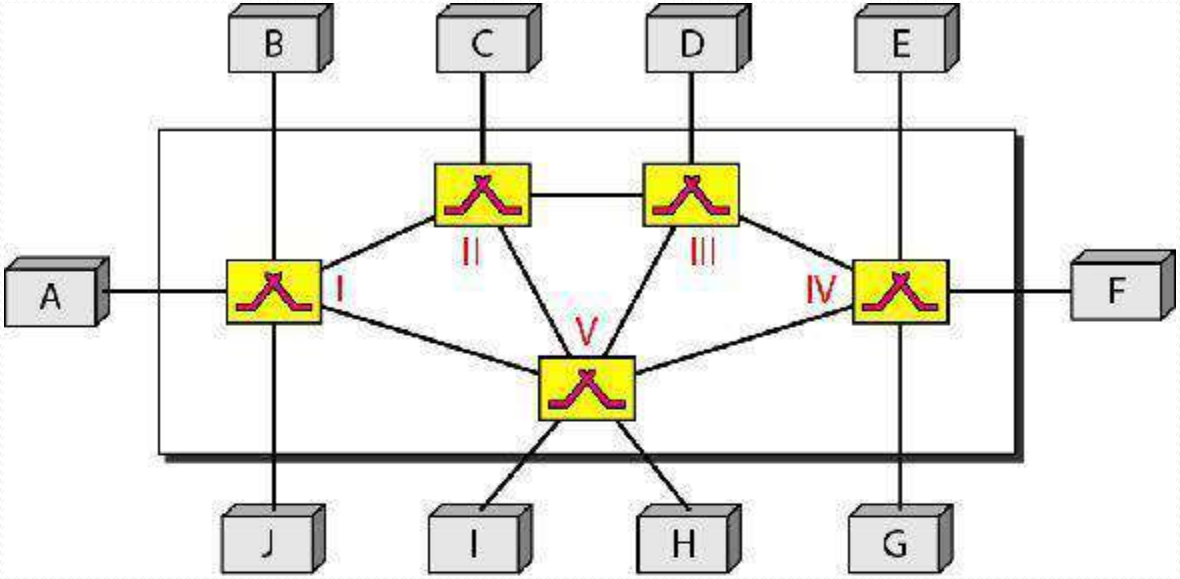
Circuit-switched networks

Packet-switched networks

Message-switched networks

Datagram networks

Virtual-circuit networks

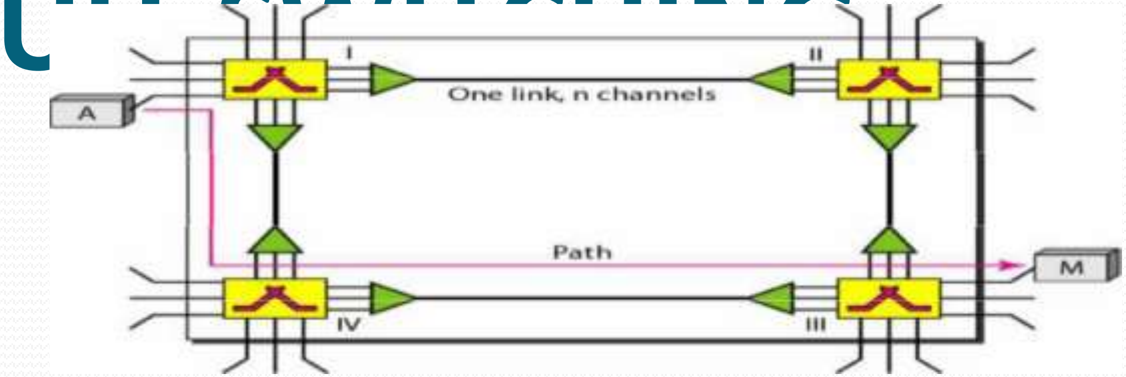


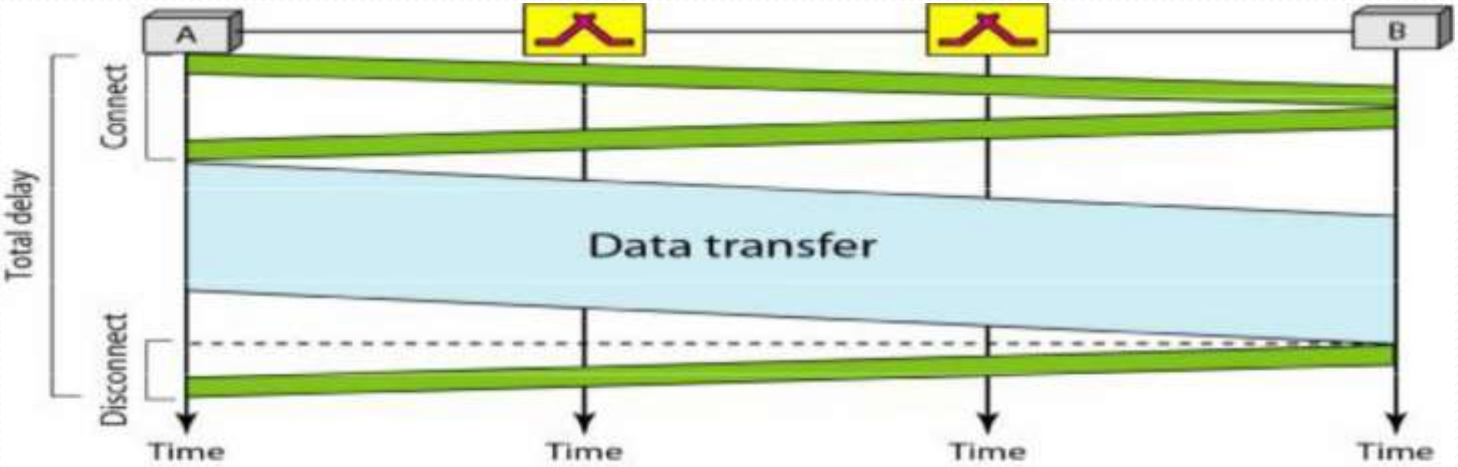
- At broad level, switching can be divided into two major categories:
- Connectionless: The data is forwarded on behalf of forwarding tables. No previous handshaking is required and acknowledgements are optional.
- Connection Oriented: Before switching data to be forwarded to destination, there is a need to pre-establish circuit along the path between both end points. Data is then forwarded on that circuit. After the transfer is completed, circuits can be kept for future use or can be turned down immediately.

CIRCUIT SWITCHING

- A circuit-switched network consists of a set of switches connected by physical links.
- A connection between two stations is a dedicated path made of one or more links.
- Each connection uses only one dedicated channel on each link
- Each link is normally divided into n channels by using FDM or TDM

CIRCUIT SWITCHING

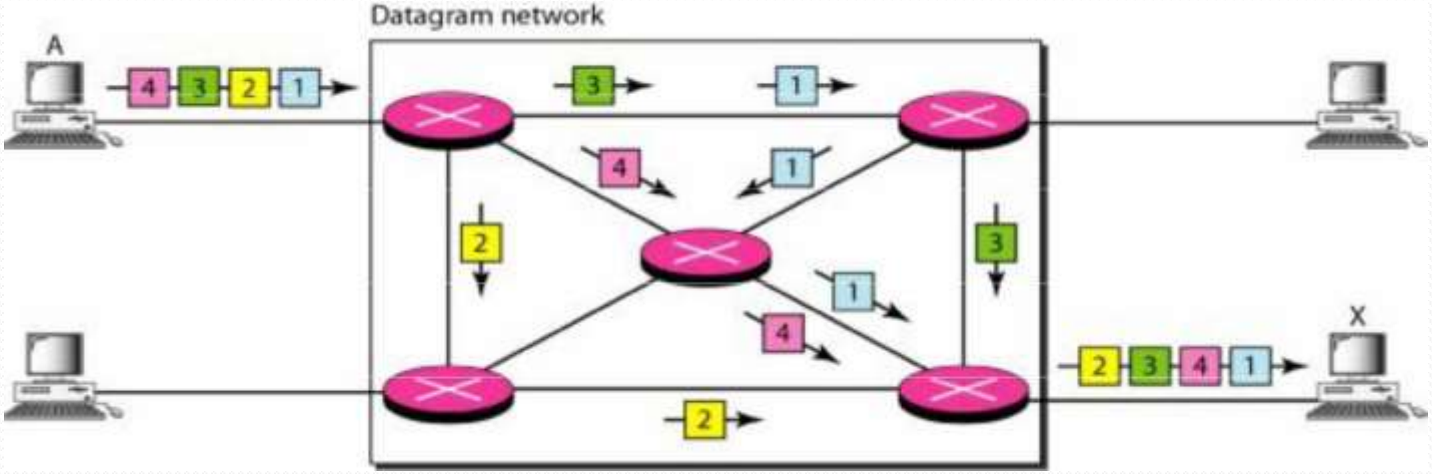


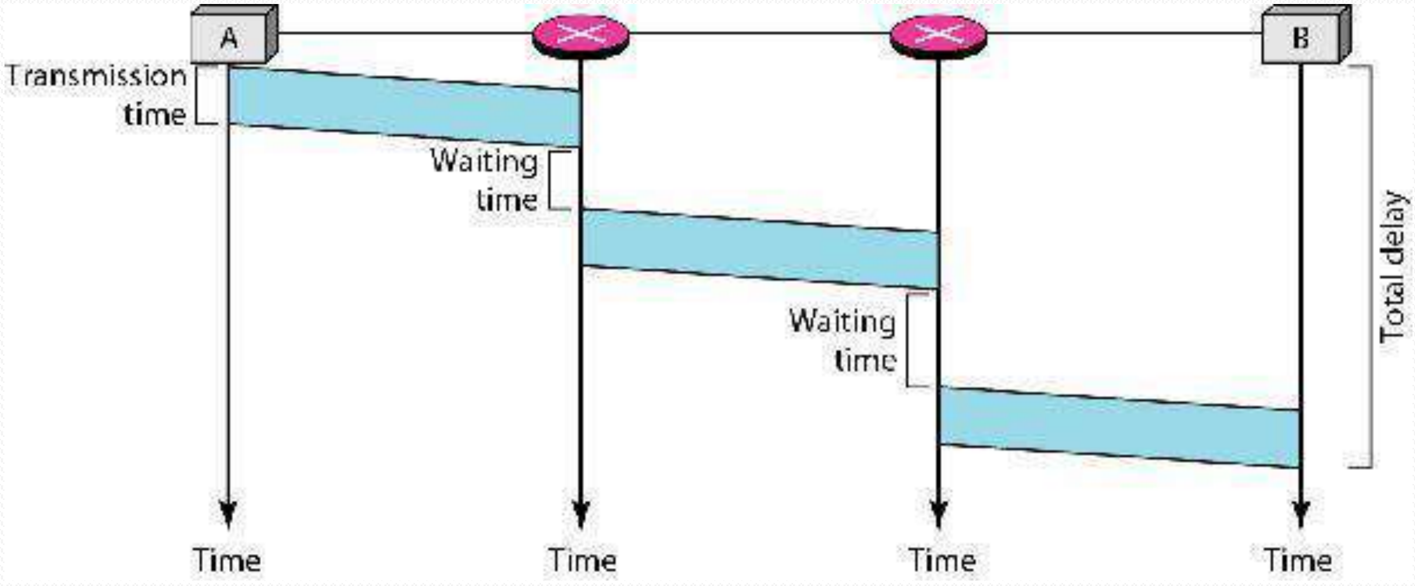


PACKET SWITCHING

- In packet Switching, flow of data is not continuous rather it flows in the form of packets
- The size of the packet is determined by the network and the governing protocol
- This type of switching further classify into datagram networks and virtual circuit networks

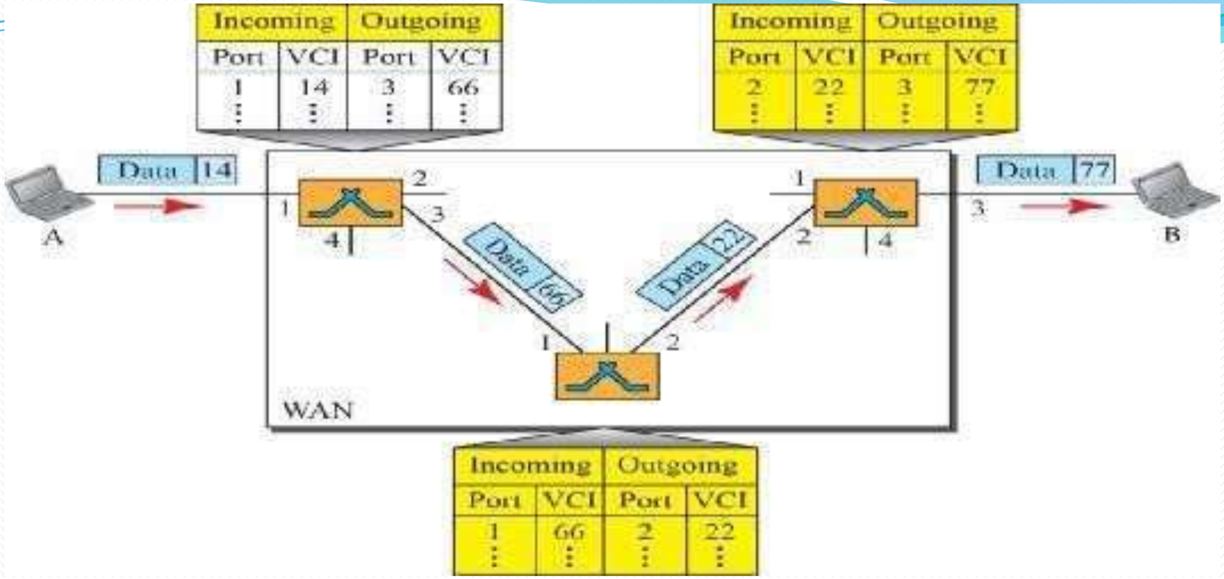
Dat


Datagram network
A
4
3
2
1
3
1
4
1
2
3
1
4
2
X
2
3
4
1


A
B
Transmission time
Waiting time
Waiting time
Total delay
Time
Time
Time
Time

Virtual Circuit Networks

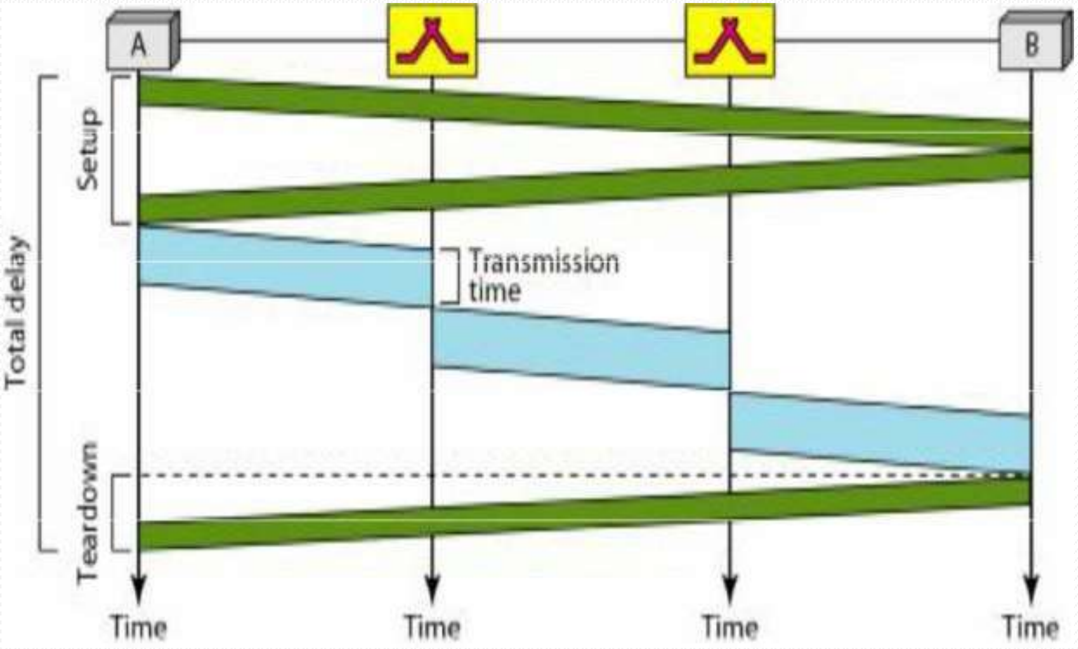
- A virtual-circuit network is a cross between a circuit-switched network and a datagram network.
- The virtual-circuit shares characteristics of both. Packets form a single message travel along the same path.
- Three phases to transfer data
- Resources can be allocated during setup phase
- Data are packetized and each packet carries an address in the header
- All packets follow the same path



Incoming		Outgoing	
Port	VCI	Port	VCI
1	14	3	66
⋮	⋮	⋮	⋮

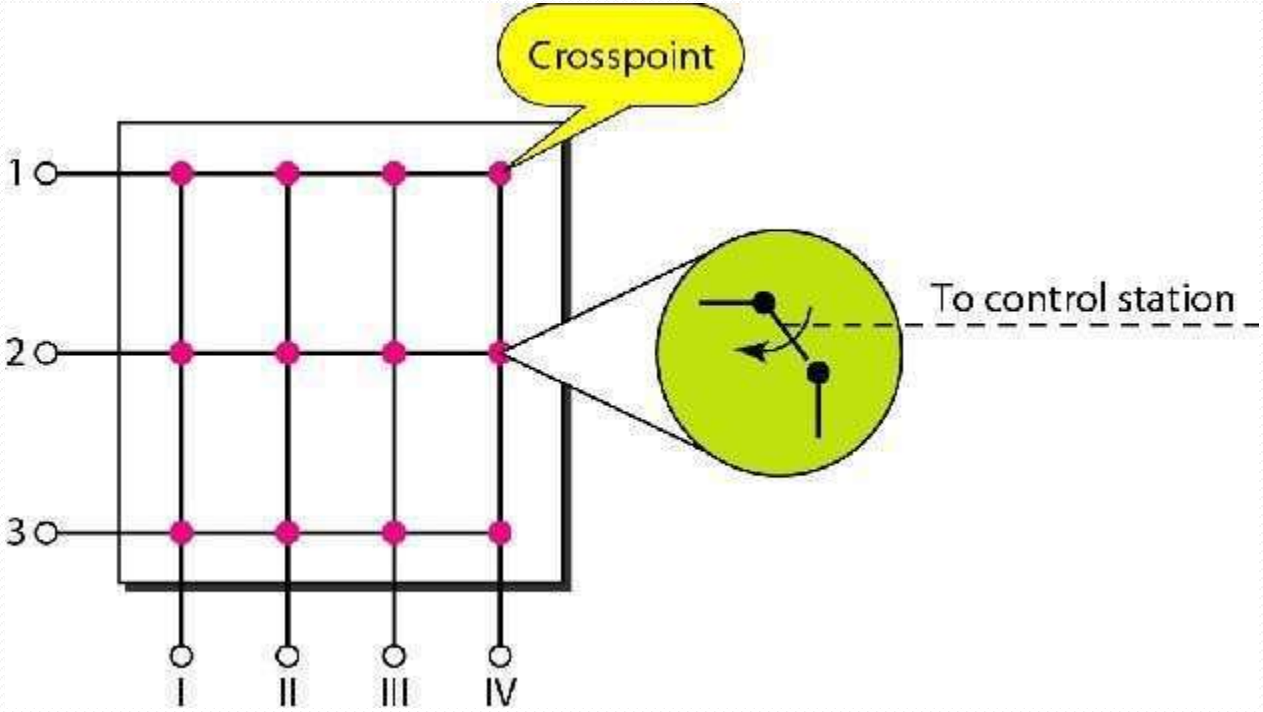
Incoming		Outgoing	
Port	VCI	Port	VCI
2	22	3	77
⋮	⋮	⋮	⋮

Incoming		Outgoing	
Port	VCI	Port	VCI
1	66	2	22
⋮	⋮	⋮	⋮

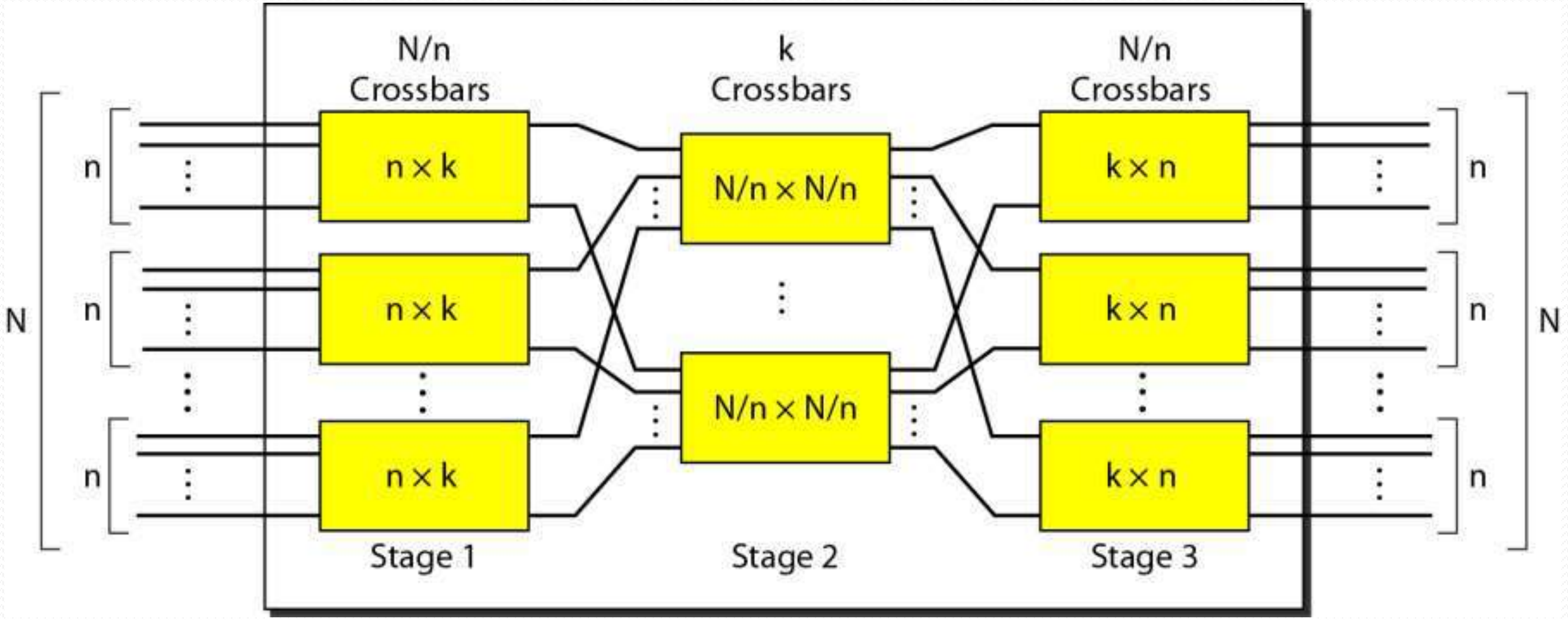


Structure of a Switch

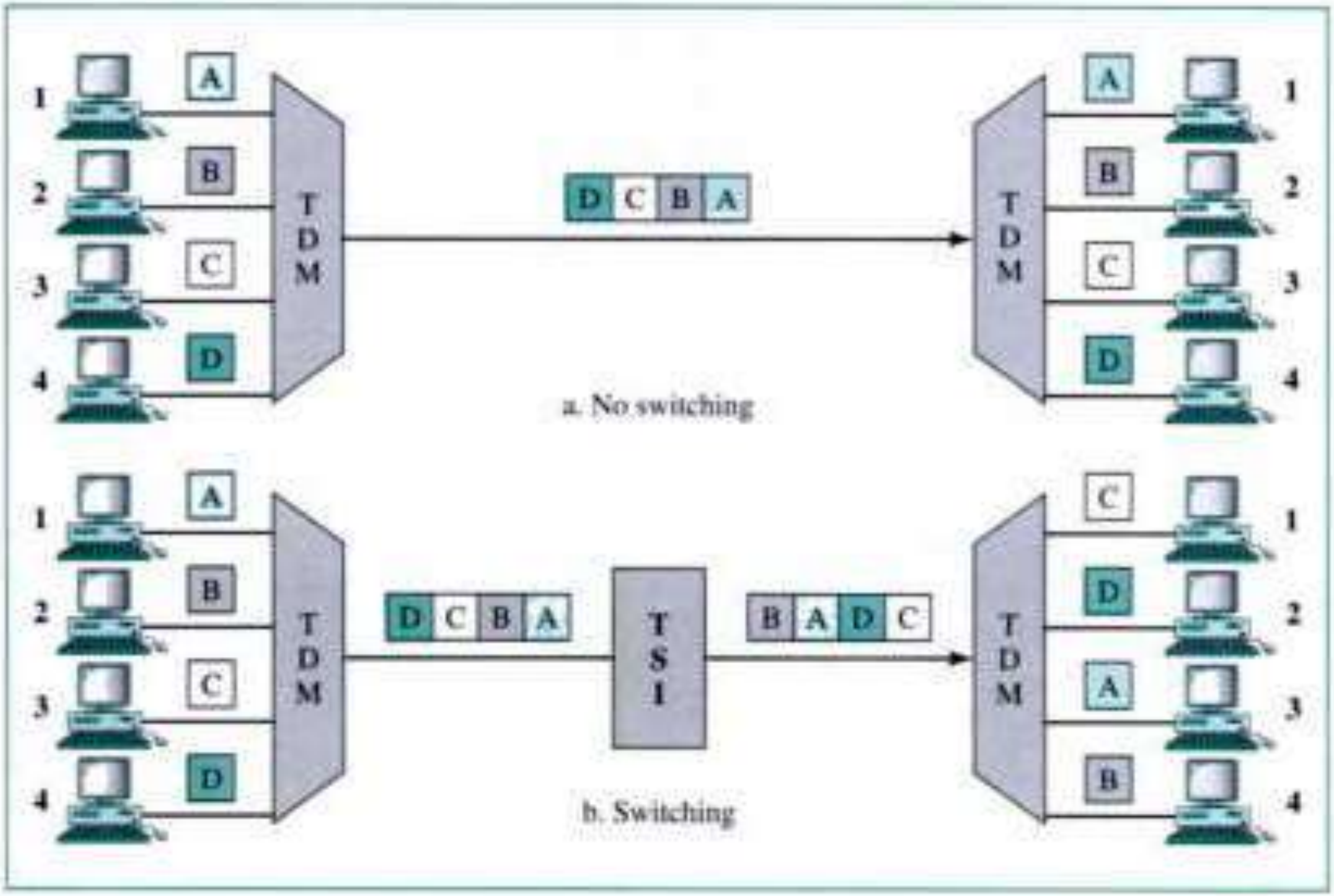
- We use switches in circuit-switched and packet-switched networks. There are two structures of a switch named as space division switch and time division switch.



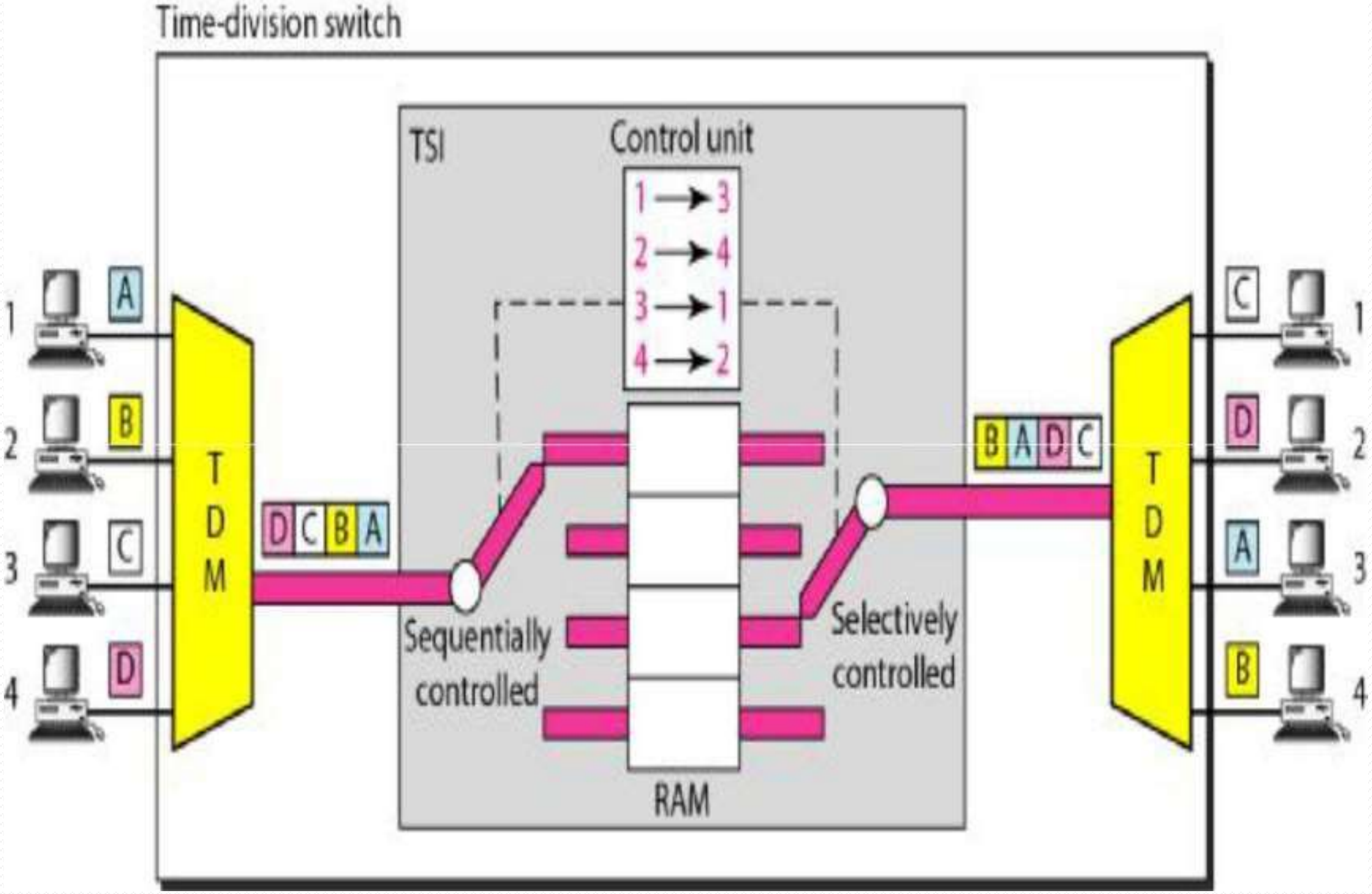
Multistage switch



Time-division switch

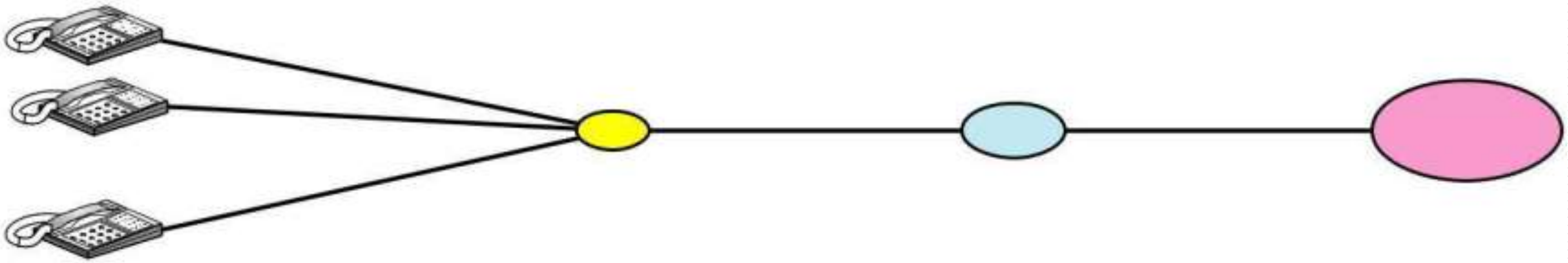


Time-division switch



Telephone networks

- Telephone networks use circuit switching. The telephone network had its beginnings in the late 1800s. The entire network, which is referred to as the plain old telephone system(POTS), was originally an analog system using analog signals to transmit voice. There are three major components of telephone system namely
- local loops,
- Trunks
- Switching offices



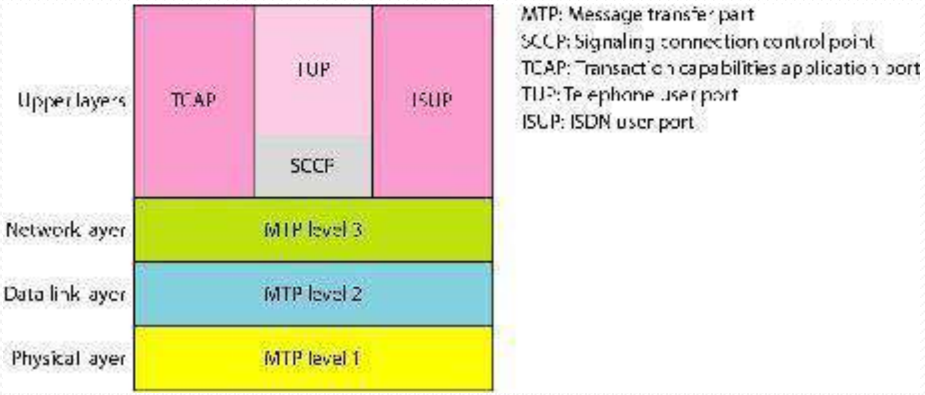
Local Loops: One component of the telephone network is the local loop, a twisted-pair cable that connects the subscriber telephone to the nearest end office or local central office.

Trunks: Trunks are transmission media that handle the communication between offices. A trunk normally handles hundreds or thousands of connections through multiplexing.

Switching Offices: To avoid having a permanent physical link between any two subscribers,

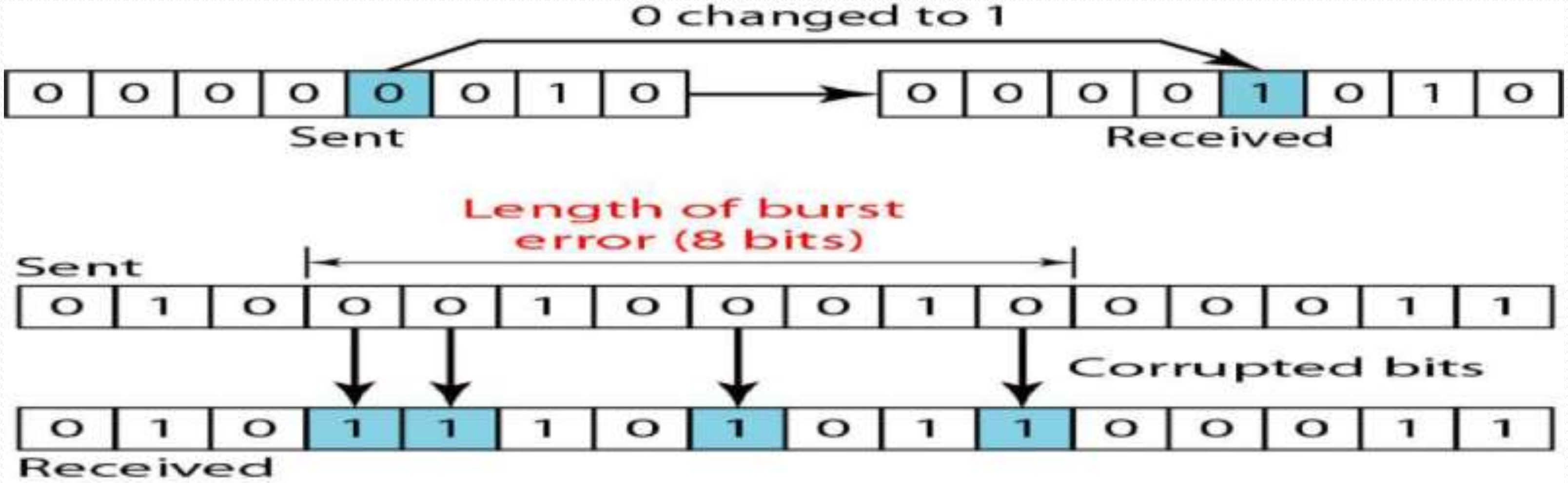
Signaling

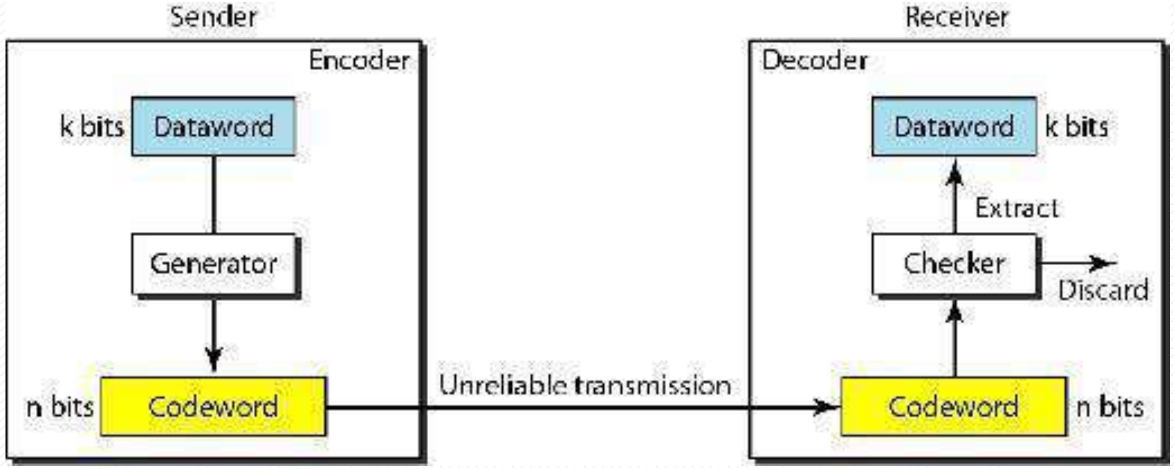
Signaling can be defined as the information exchange concerning the establishment and control of a telecommunication circuit and the management of the network. There are two types: In-Band and Out-Band.

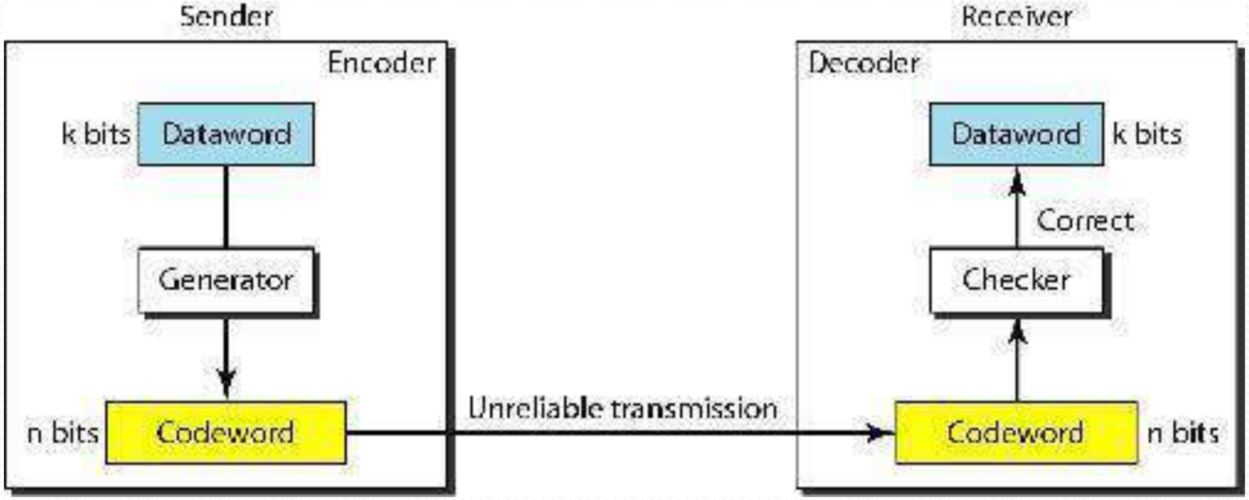


DATA LINK LAYER

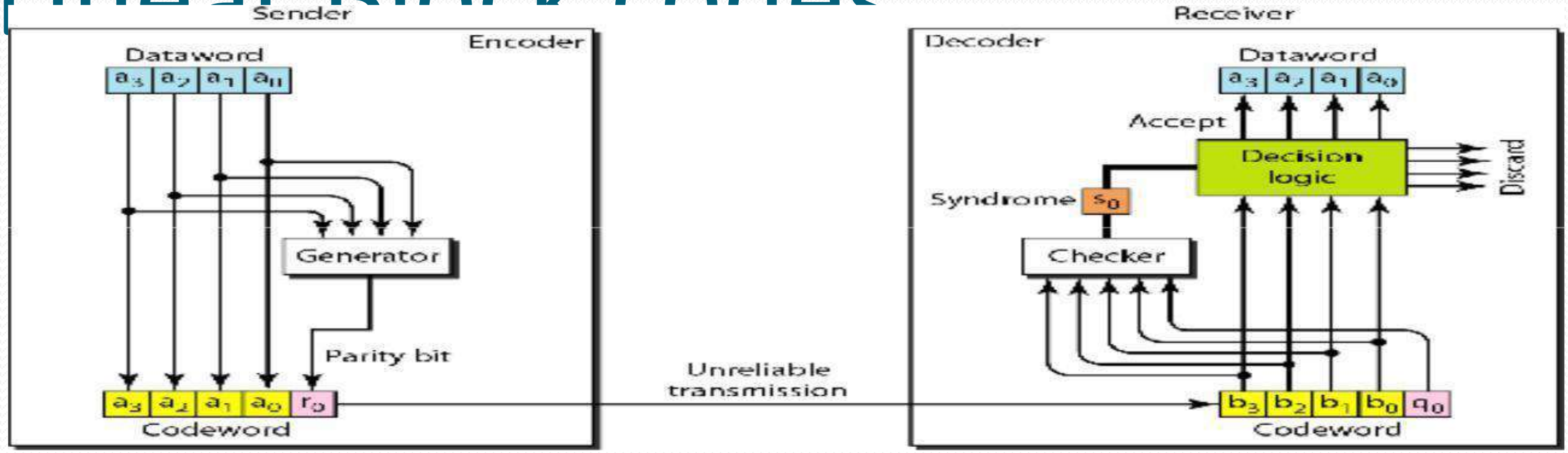
- Data can be corrupted during transmission. Some applications require that errors be detected and corrected.
- There are two types error: single-bit error and burst error




Sender
Encoder
k bits
Dataword
Generator
n bits
Codeword
Unreliable transmission
Receiver
Decoder
Dataword
k bits
Extract
Checker
Discard
Codeword
n bits

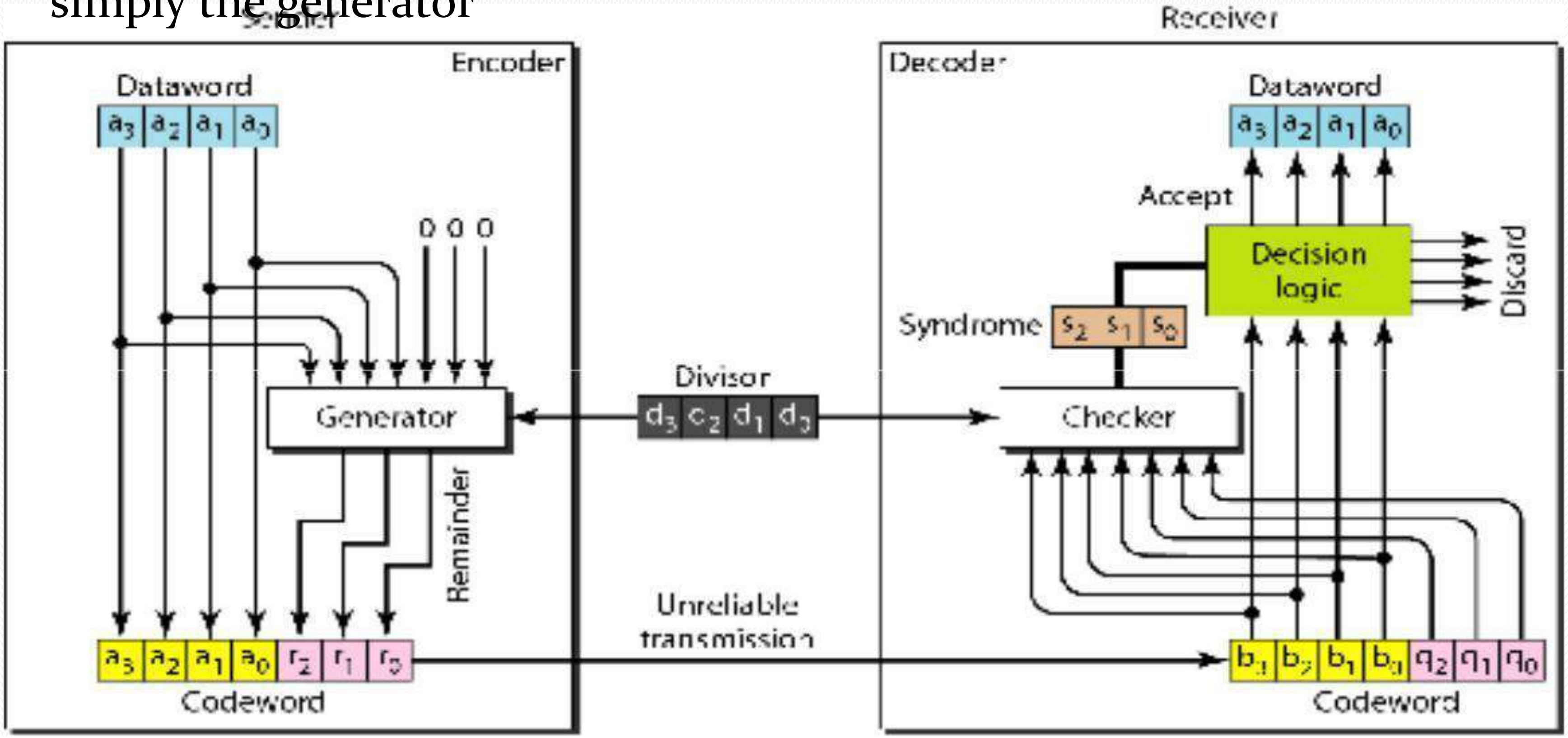

Sender
Encoder
k bits
Dataword
Generator
n bits
Codeword
Unreliable transmission
Receiver
Decoder
Dataword
k bits
Correct
Checker
Codeword
n bits

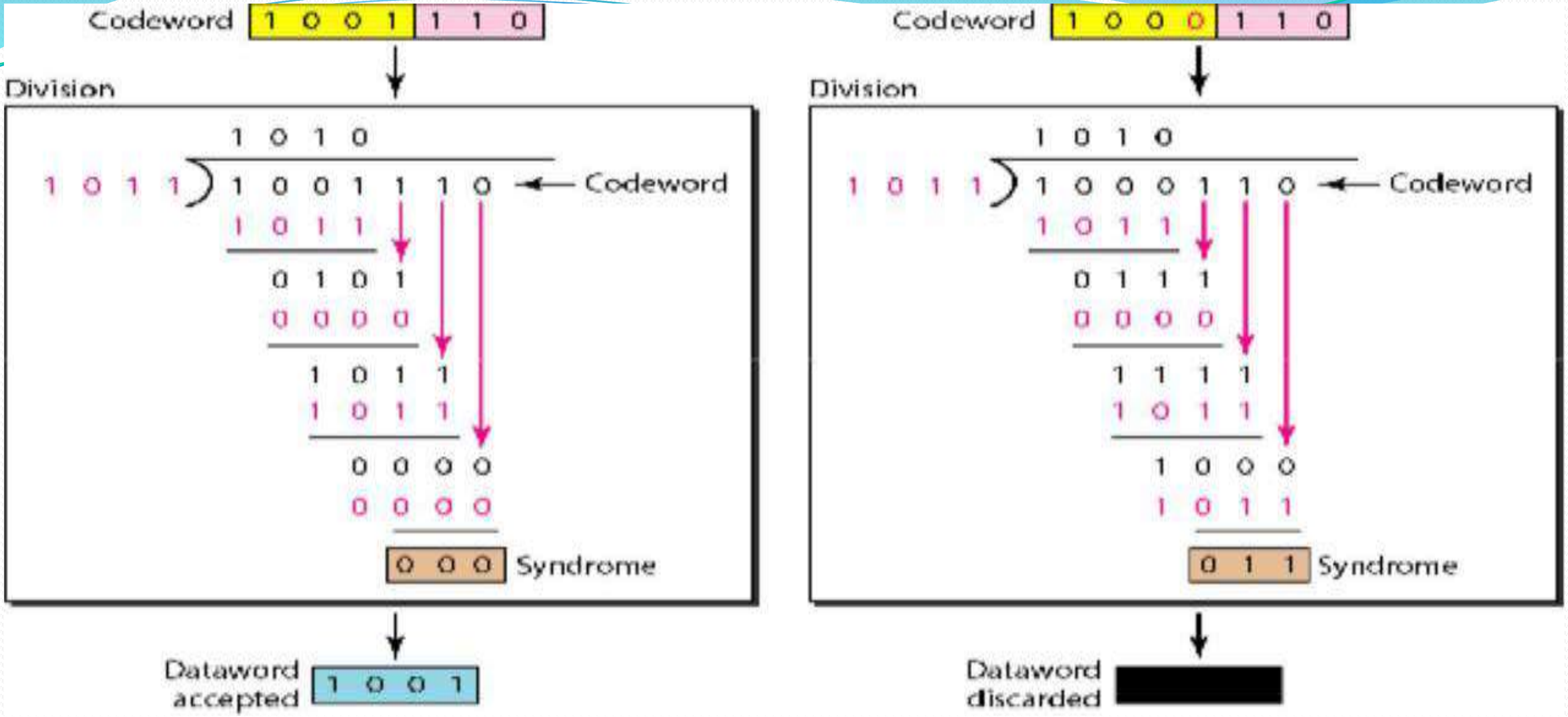
Linear Block codes



Cyclic Codes: Cyclic codes are special linear block codes with one extra property

In cyclic code, concept of long division has been used. The divisor in a cyclic code is normally called the generator polynomial or simply the generator





In a cyclic code, following cases exist:

If syndrome s(x) ≠ 0, **one or more bits is corrupted.**

If syndrome s(x) = 0, either

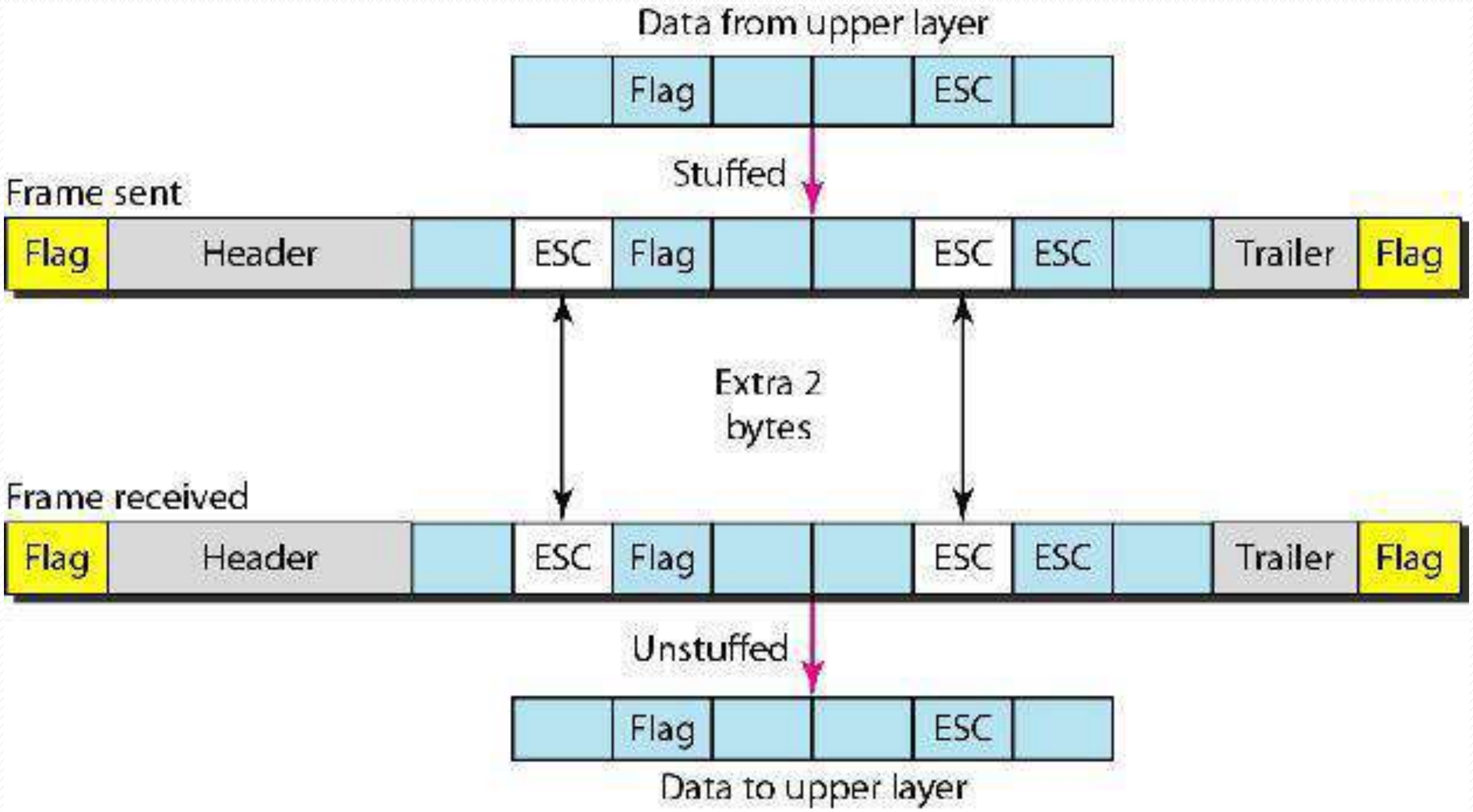
No bit is corrupted

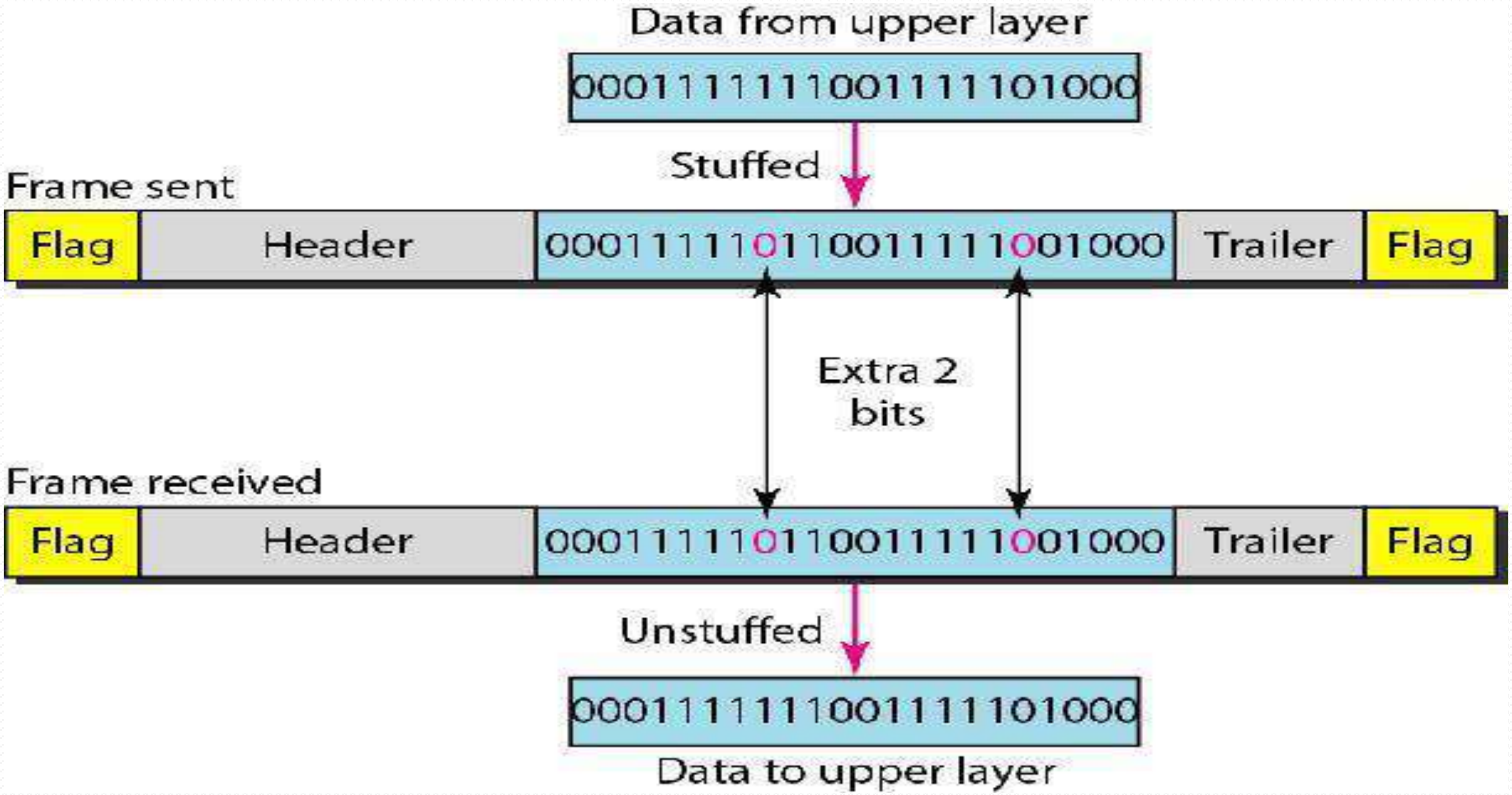
Some bits are corrupted, but the decoder failed to detect them.

Framing

The data link layer needs to pack bits into frames, so that each frame is distinguishable from another frame.

There are two types of framing namely fixed size framing and variable size framing.





Data from upper layer

0001111111001111101000

Stuffed

Frame sent

Flag | Header | 000111110110011111001000 | Trailer | Flag

Extra 2 bits

Frame received

Flag | Header | 000111110110011111001000 | Trailer | Flag

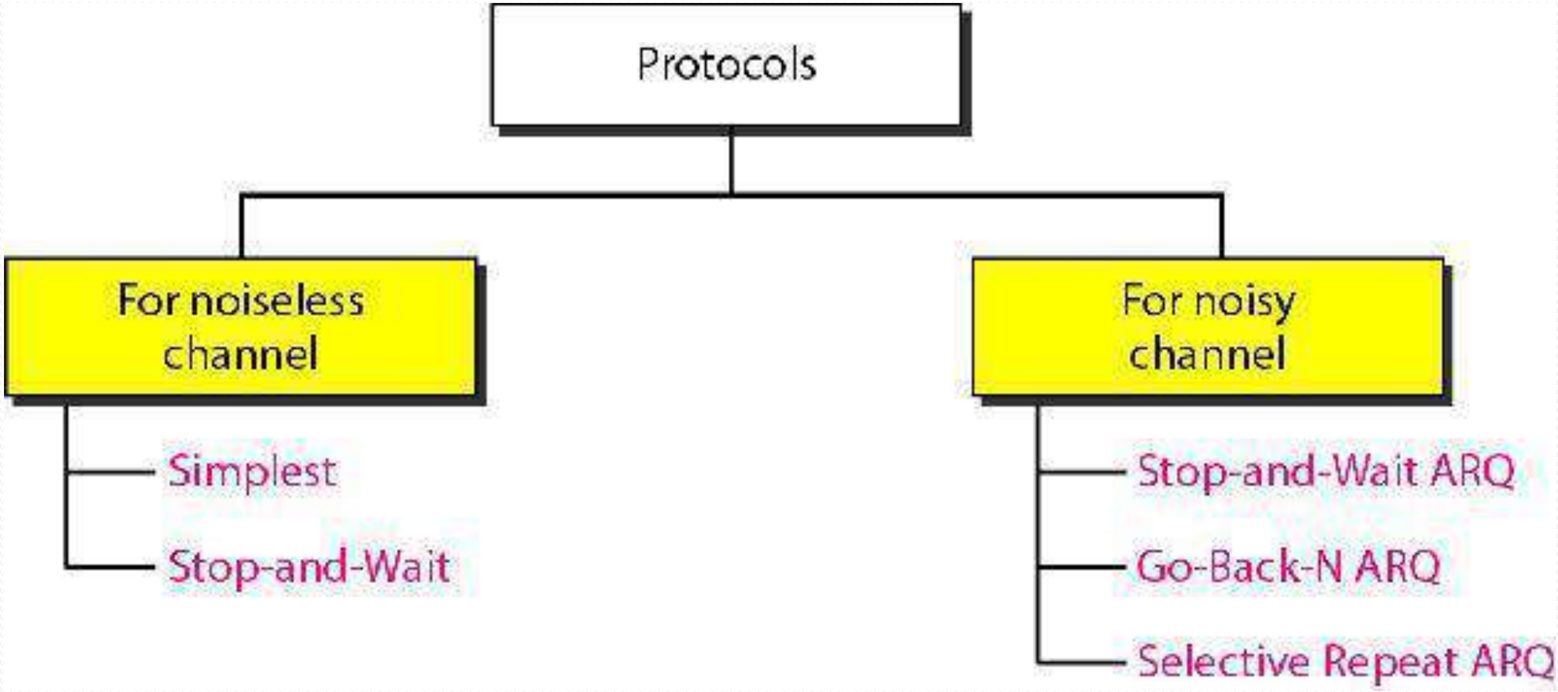
Unstuffed

0001111111001111101000

Data to upper layer

NOISELESS CHANNEL & NOISY CONTROL PROTOCOL

- Noiseless protocols takes channel as an ideal one in which no frames are lost, duplicated, or corrupted. There are two types of protocols used for noiseless channels namely simple stand stop & wait protocol.
- The first is a protocol that does not use flow control; second is the one that does of course, neither has error control because we have assumed that the channel is a perfect noise less channel.



Protocols

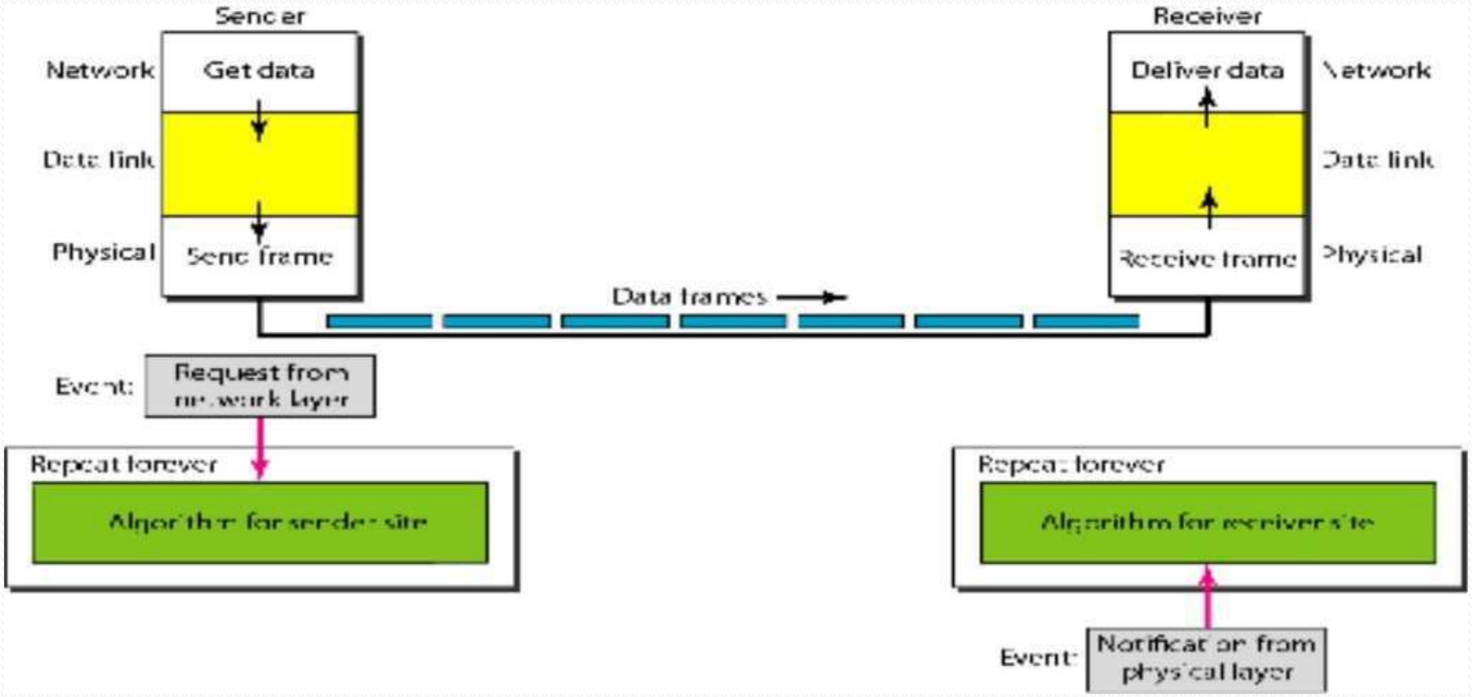
For noiseless channel

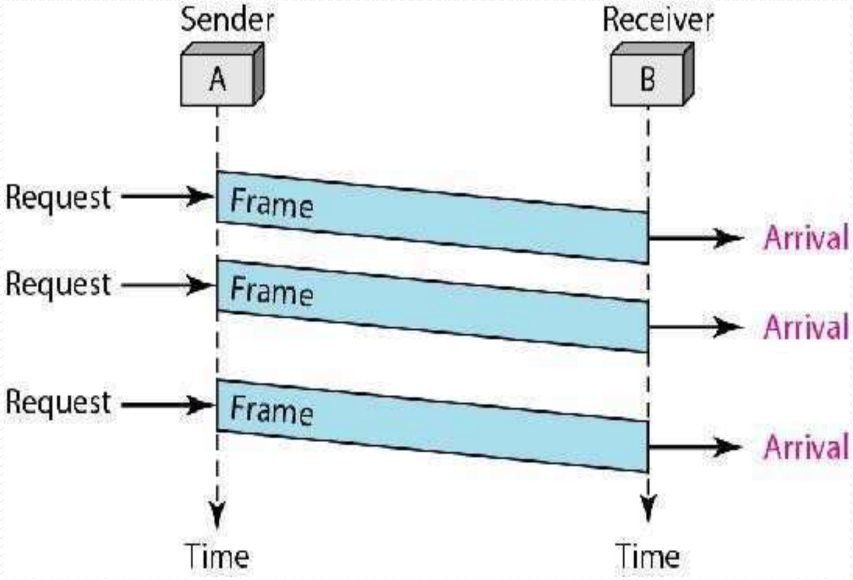
- Simplest
- Stop-and-Wait

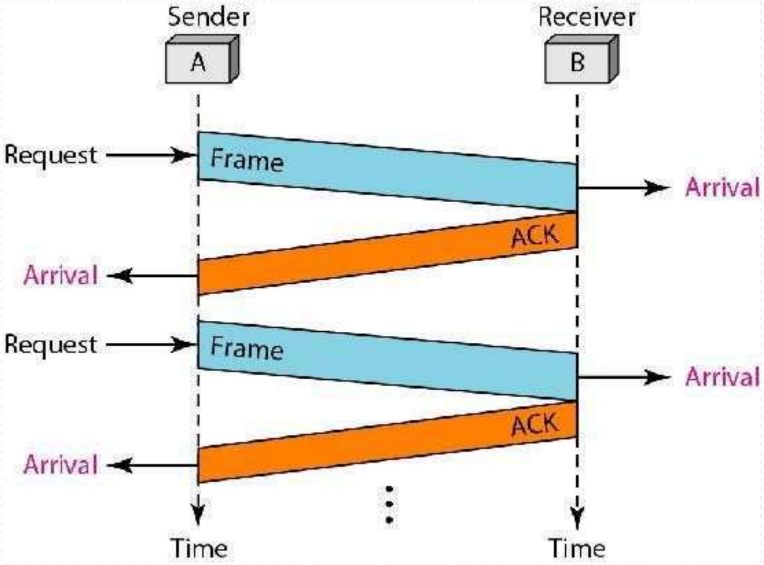
For noisy channel

- Stop-and-Wait ARQ
- Go-Back-N ARQ
- Selective Repeat ARQ

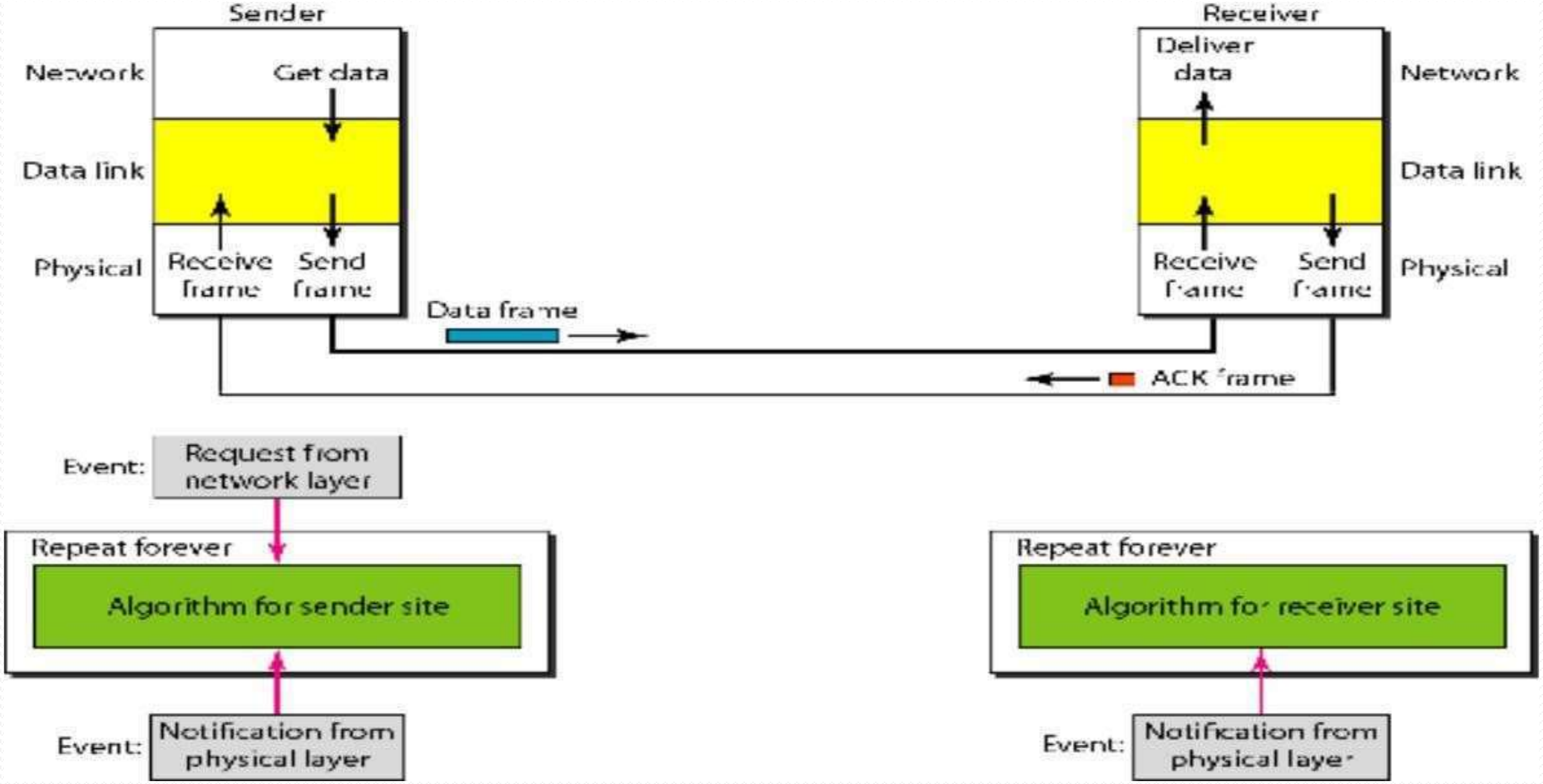
Simplest protocol



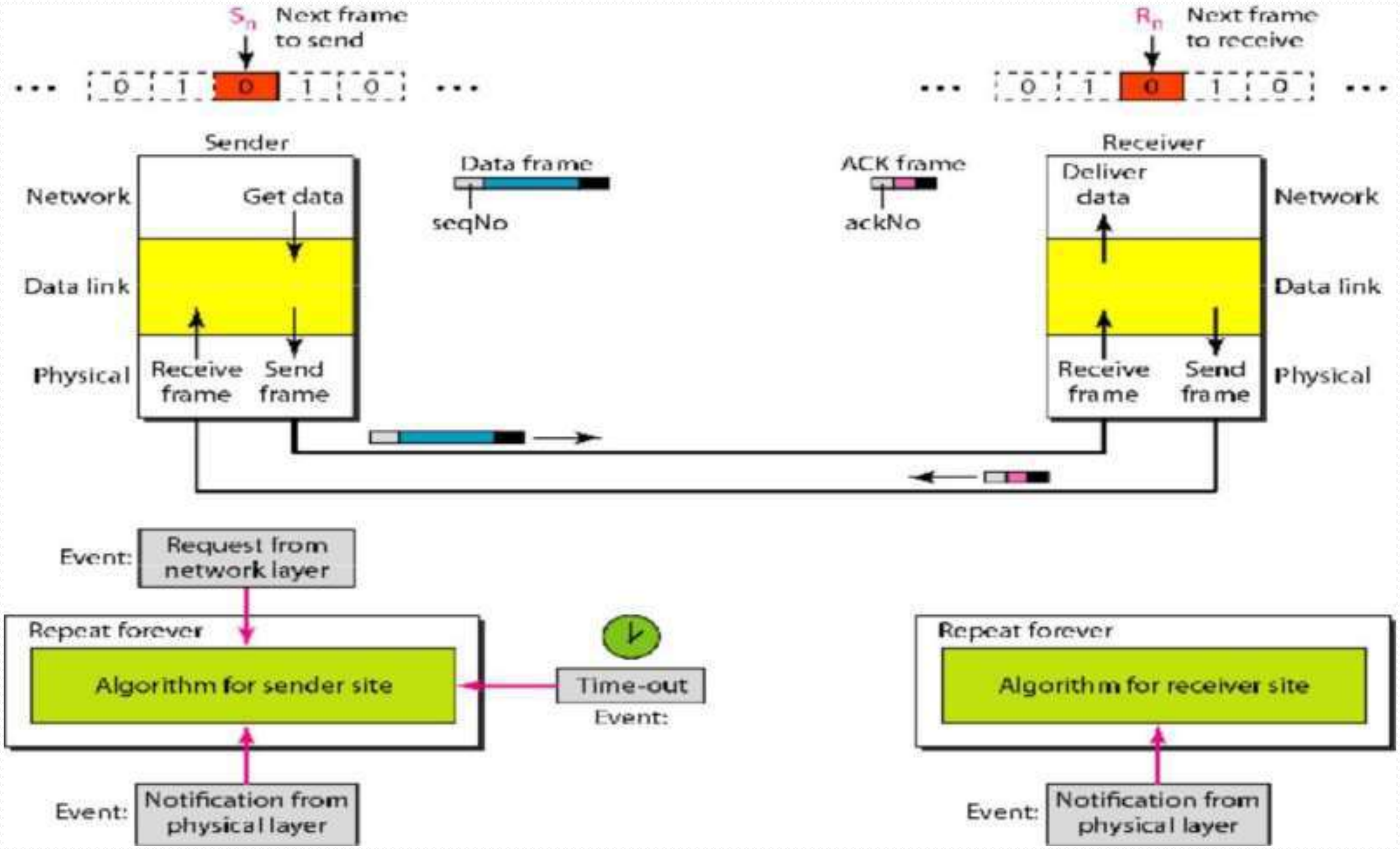

Sender
Receiver
A
B
Request
Frame
Arrival
Request
Frame
Arrival
Request
Frame
Arrival
Time
Time


Sender
Receiver
A
B
Request
Frame
Arrival
ACK
Arrival
Request
Frame
Arrival
ACK
Arrival
Time
Time

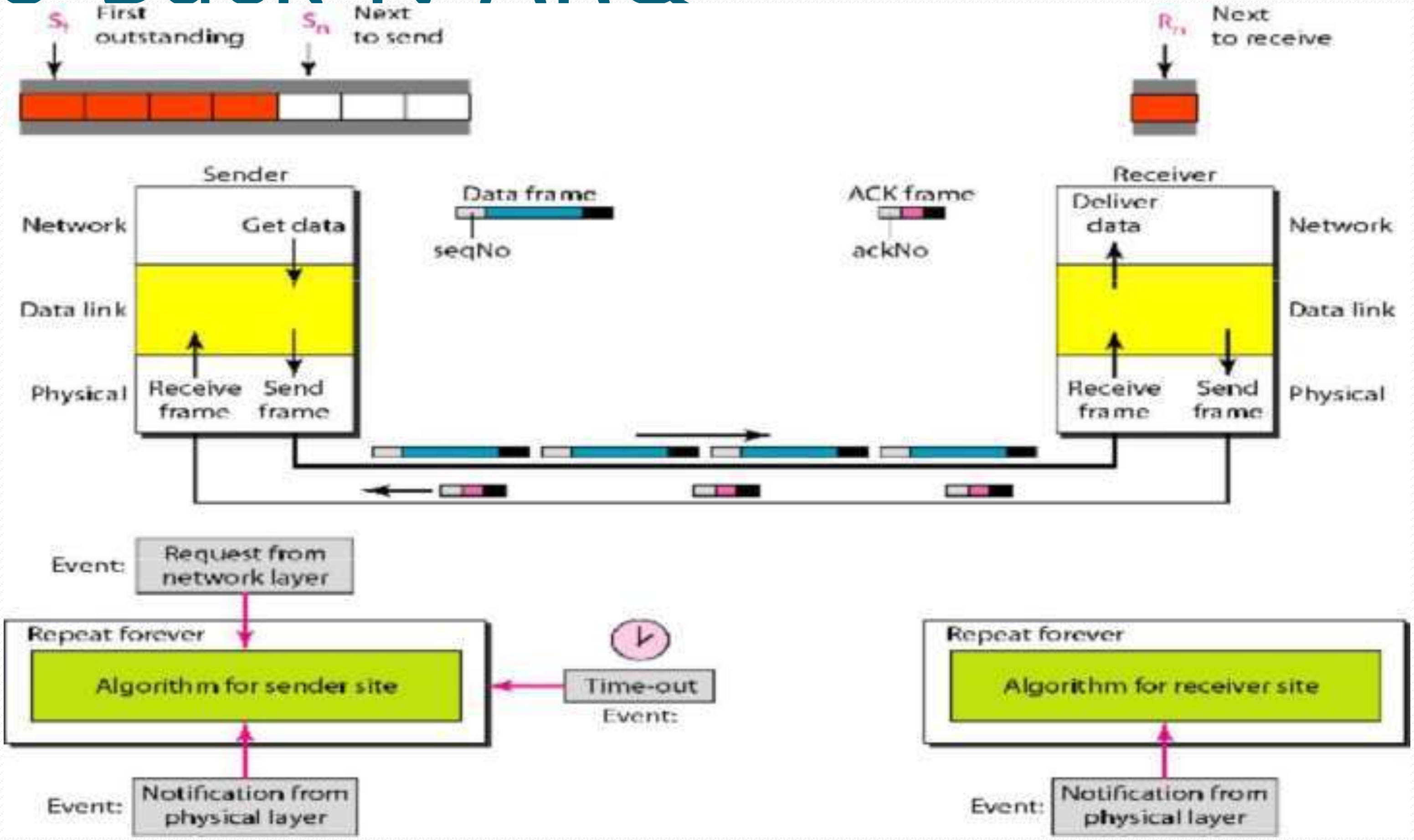
Stop-and-Wait Protocol



Stop & Wait ARQ

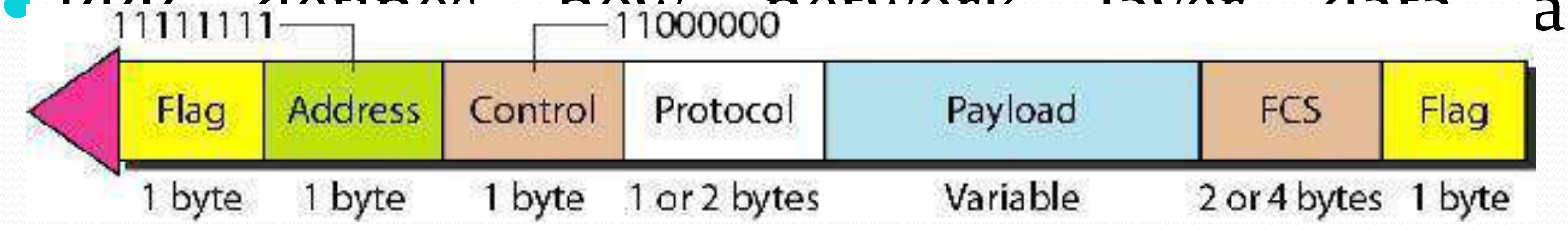


Go-Back-N-ARQ


S_f
First outstanding
S_n
Next to send
R_n
Next to receive
Sender
Receiver
Data frame
seqNo
ACK frame
ackNo
Network
Data link
Physical
Get data
Receive frame
Send frame
Deliver data
Network
Data link
Physical
Receive frame
Send frame
Event:
Request from network layer
Repeat forever
Algorithm for sender site
Time-out
Event:
Event:
Notification from physical layer
Repeat forever
Algorithm for receiver site
Event:
Notification from physical layer

POINT-TO-POINT PROTOCOL

- PPP defines the format of the frame to be exchanged between devices.
- PPP defines how two devices can negotiate the establishment of the link and the exchange of data.
- PPP defines how network layer data are



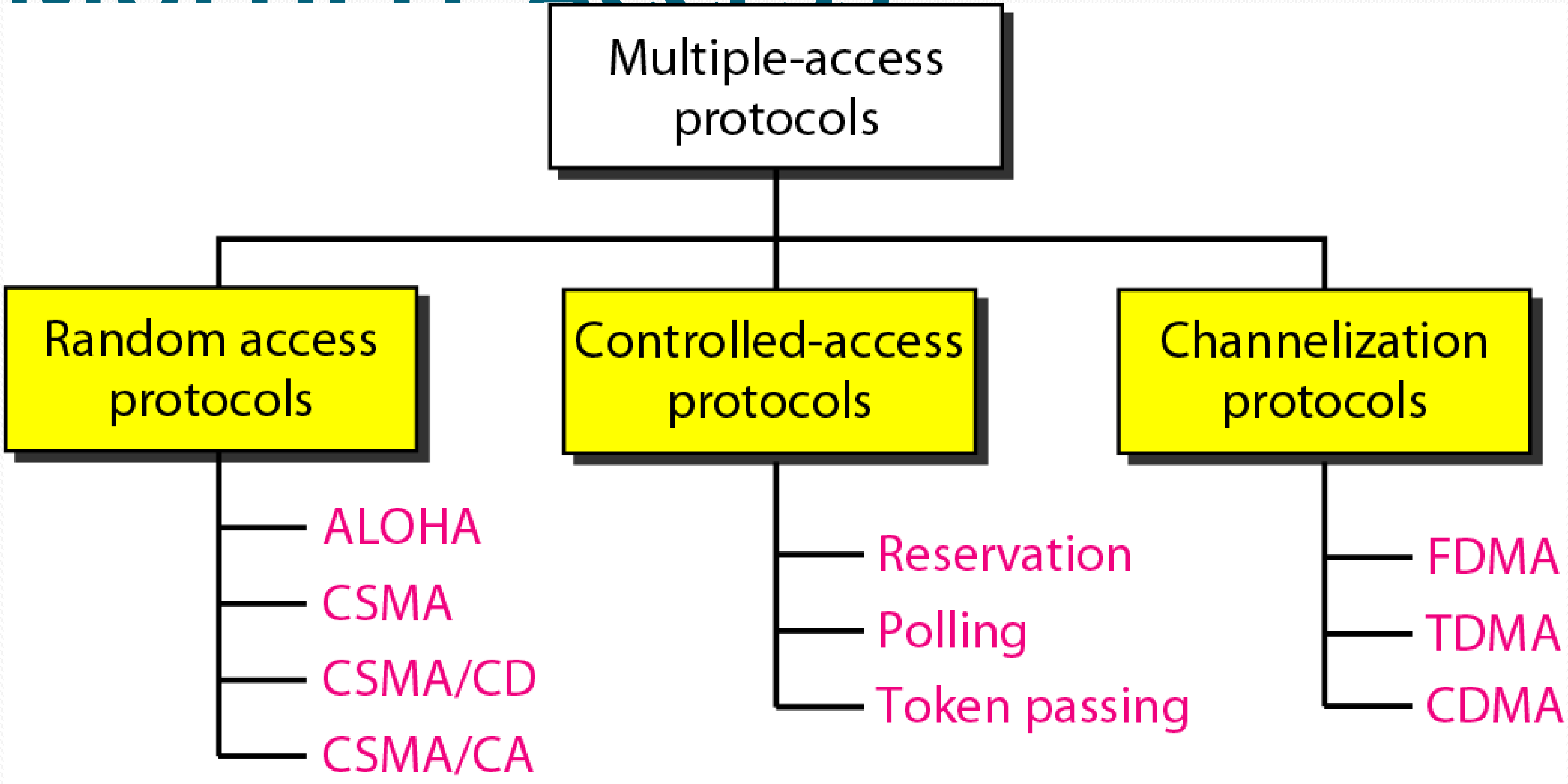
POINT-TO-POINTPROTOCOL

- PPP provides multiple network layer services supporting a variety of network layer protocols.
- PPP provides connections over multiple links.
- PPP provides network address configuration. This is particularly useful when a home user needs a temporary network address to connect to the Internet.

contd..

- On the other hand, to keep PPP simple, several services are missing :
- PPP does not provide flow control.
- PPP has a very simple mechanism for error control.
- PPP does not provide a sophisticated addressing mechanism.

MULTIPLE ACCESS



Multiple-access protocols

Random access protocols
- ALOHA
- CSMA
- CSMA/CD
- CSMA/CA

Controlled-access protocols
- Reservation
- Polling
- Token passing

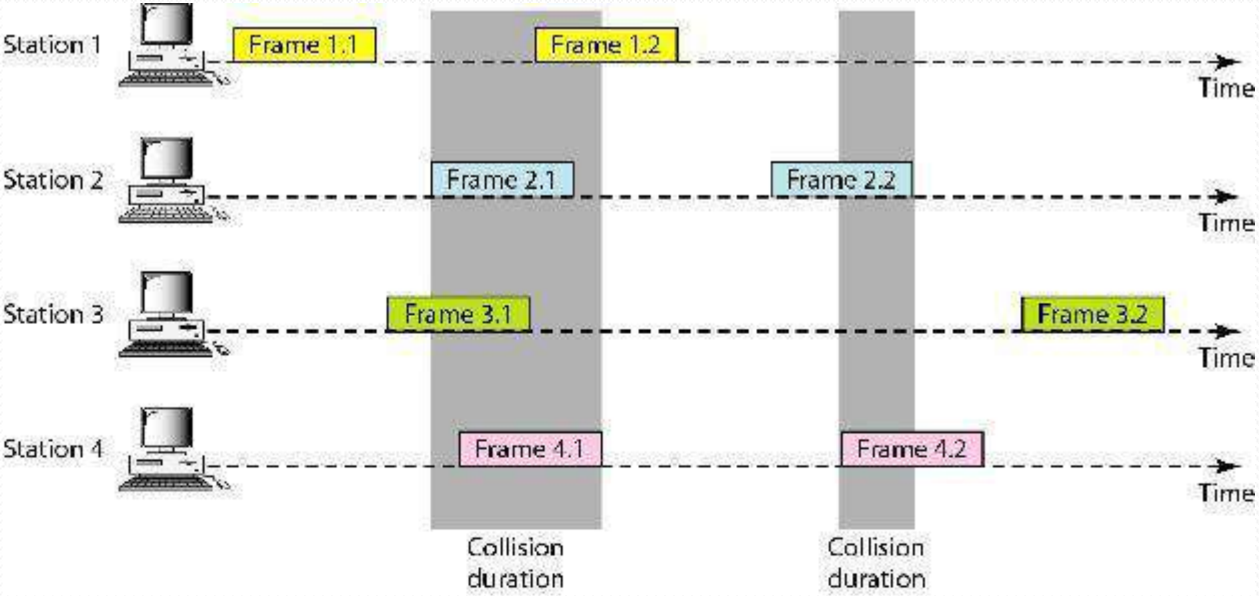
Channelization protocols
- FDMA
- TDMA
- CDMA

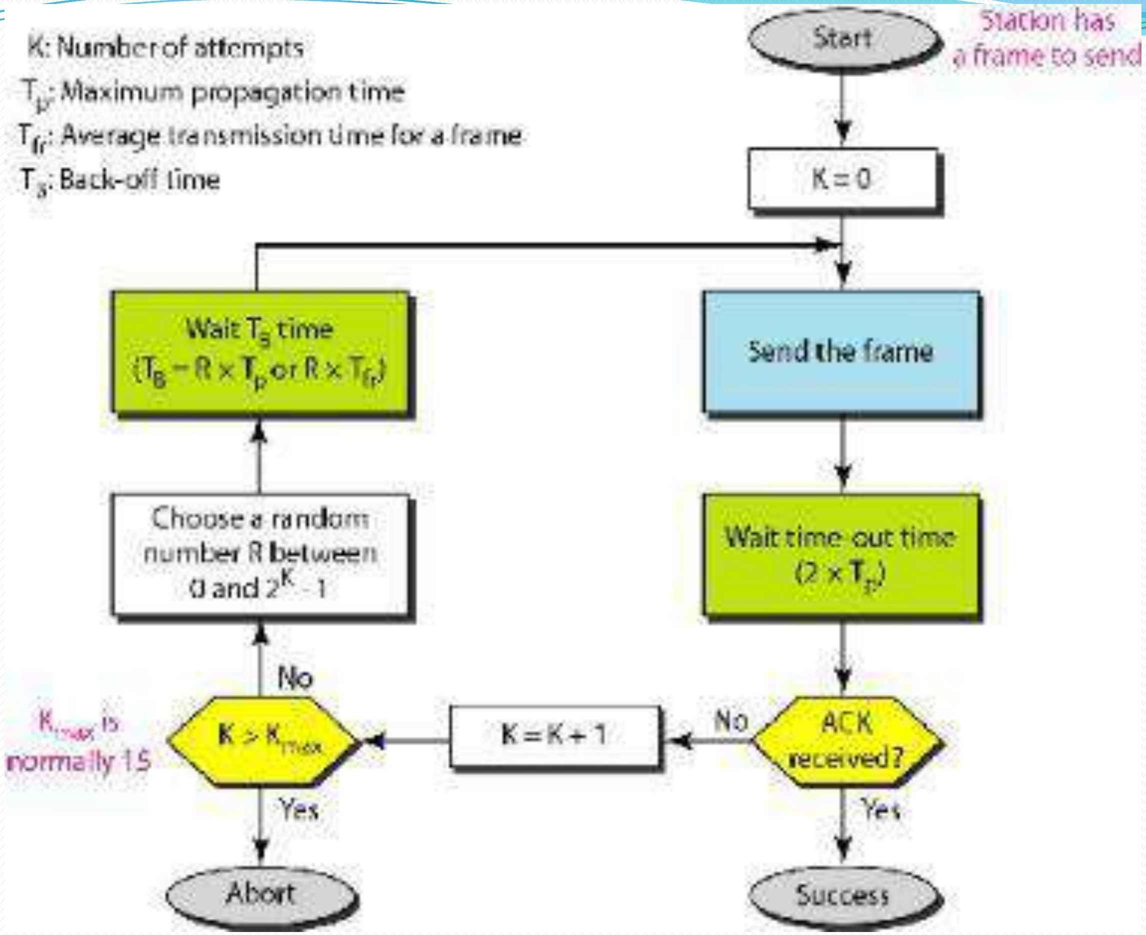
- **Random Access (or contention) Protocols:**
  - No station is superior to another station and none is assigned the control over another.
  - A station with a frame to be transmitted can use the link directly based on a procedure defined by the protocol to make a decision on whether or not to send.
- **ALOHA Protocols :**

  Was designed for **wireless LAN and can be used for any shared medium**
- **Pure ALOHA Protocol:**
  - All frames from any station are of fixed length (**L bits**)
  - Stations transmit at equal **transmission time** (***all stations produce frames with equal frame lengths***).

Pure ALOHA

The original ALOHA protocol is called pure ALOHA. This is a simple, but elegant protocol. The idea is that each station sends a frame whenever it has a frame to send.



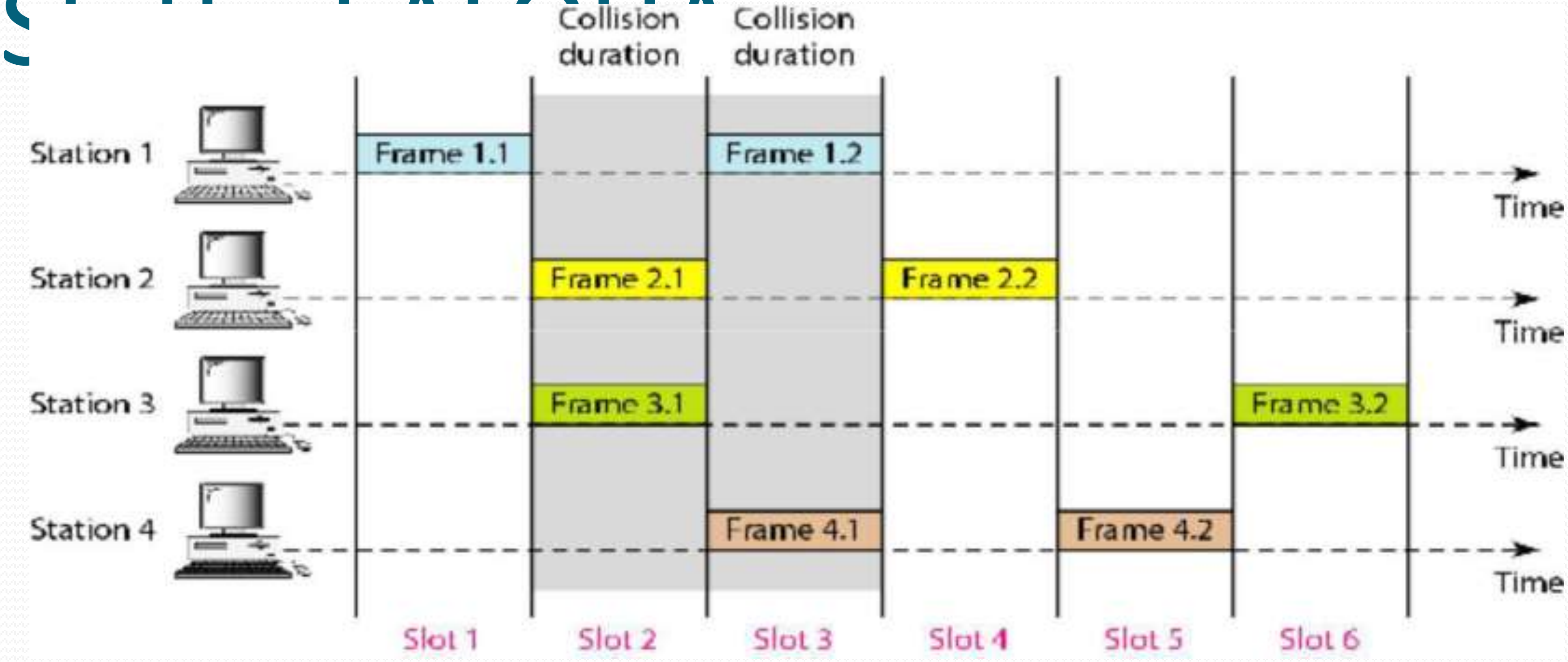

K: Number of attempts
T_p: Maximum propagation time
T_{fr}: Average transmission time for a frame
T_B: Back-off time
Start
Station has a frame to send
K = 0
Send the frame
Wait time-out time ($2 \times T_p$)
ACK received?
Yes
Success
No
K = K + 1
$K > K_{max}$
K_{max} is normally 15
Yes
Abort
No
Choose a random number R between 0 and $2^K - 1$
Wait T_B time ($T_B = R \times T_p$ or $R \times T_{fr}$)

Pure ALOHA vulnerable time = 2 x Tfr

The throughput for pure ALOHA is S =G x e-2G.

The maximum throughput Smax =0.184 when G =(1/2)

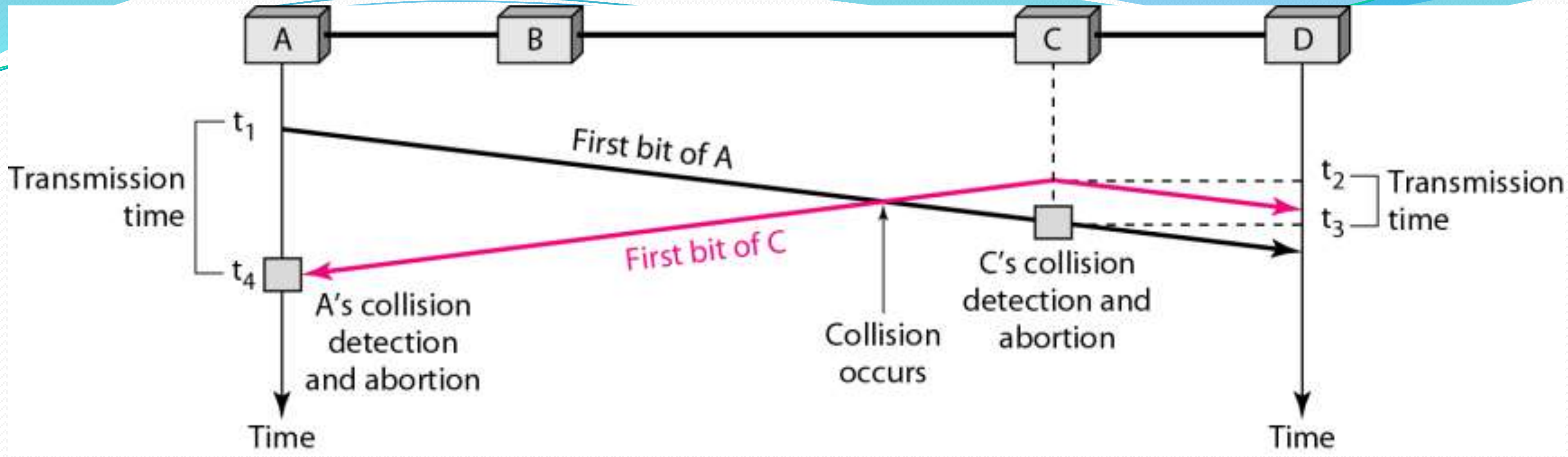
Slotted ALOHA

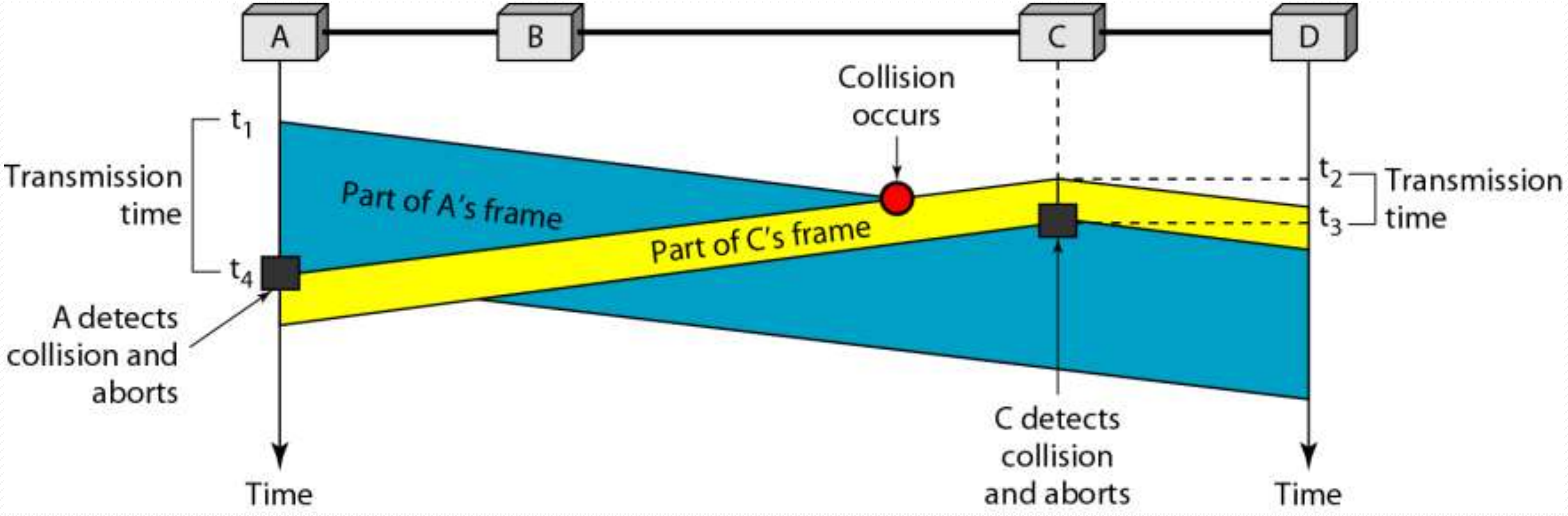


Slotted ALOHA vulnerable time = Tfr
The throughput for slotted ALOHA is *S =: G x e-G.*
The maximum throughput *Smax == 0.368 when G=1*

CSMA

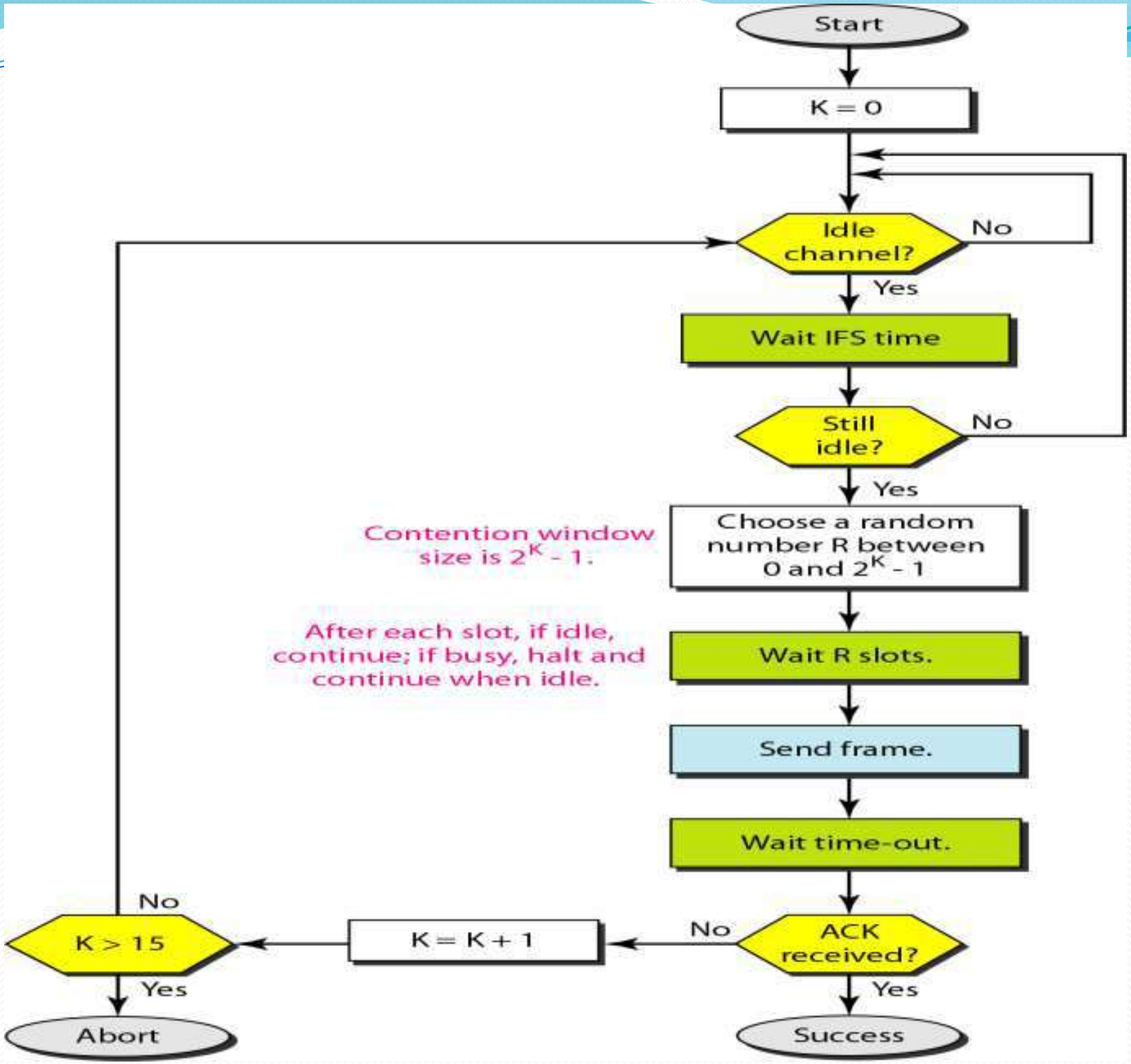
- Carrier Sense Multiple Access : CSMA requires that each station first listen to the medium before sending.
- CSMA is based on the principle “sense before transmit” or “listen before talk”.
- CSMA can reduce the possibility of collision, but it cannot eliminate it.


A
B
C
D
t1
Transmission time
t4
First bit of A
First bit of C
t2
t3
Transmission time
A's collision detection and abortion
Collision occurs
C's collision detection and abortion
Time
Time


A
B
C
D
Collision occurs
t1
Transmission time
t4
Part of A's frame
Part of C's frame
t2
t3
Transmission time
A detects collision and aborts
C detects collision and aborts
Time
Time

CSMA/CA

- CSMA was invented for wireless networks.
  - Collisions are through the use of CSMA/CA's three strategies:
  - the inter frame space,
  - the contention window, and
  - acknowledgement.

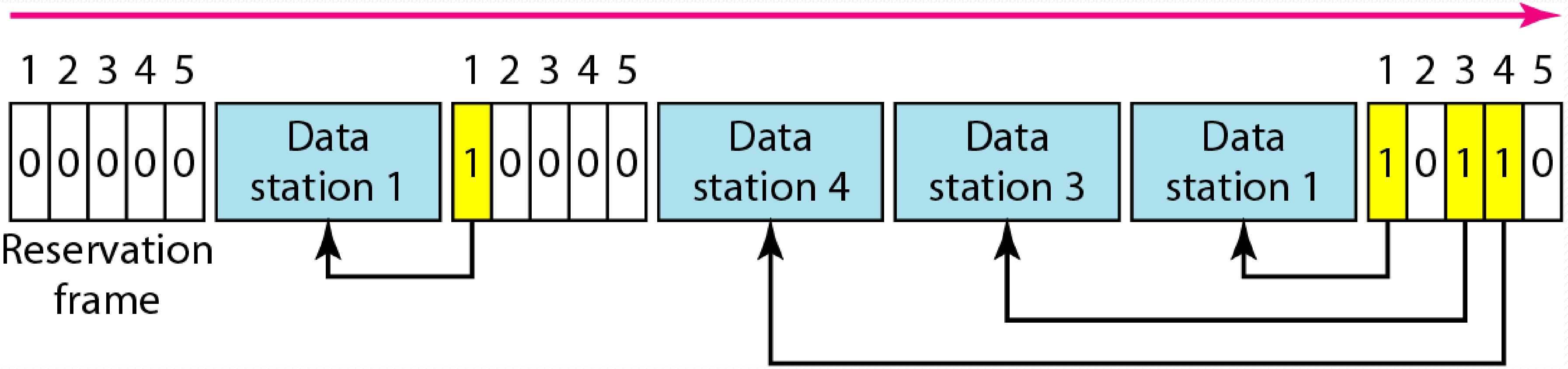

Start
K = 0
Idle channel?
No
Yes
Wait IFS time
Still idle?
No
Yes
Contention window size is $2^K - 1$.
Choose a random number R between 0 and $2^K - 1$
After each slot, if idle, continue; if busy, halt and continue when idle.
Wait R slots.
Send frame.
Wait time-out.
No
K > 15
K = K + 1
No
ACK received?
Yes
Yes
Abort
Success

Controlled Access

- In controlled access, the stations consult one another to find which station has the right to send.
- A station cannot send unless it has been authorized by other stations.
- Provides **in order access to shared medium so that every station has chance to transfer (fair protocol)**
- ***Eliminates collision completely***
- **Three methods for controlled access:**
  - Reservation
  - Polling
  - Token Passing

Reservation

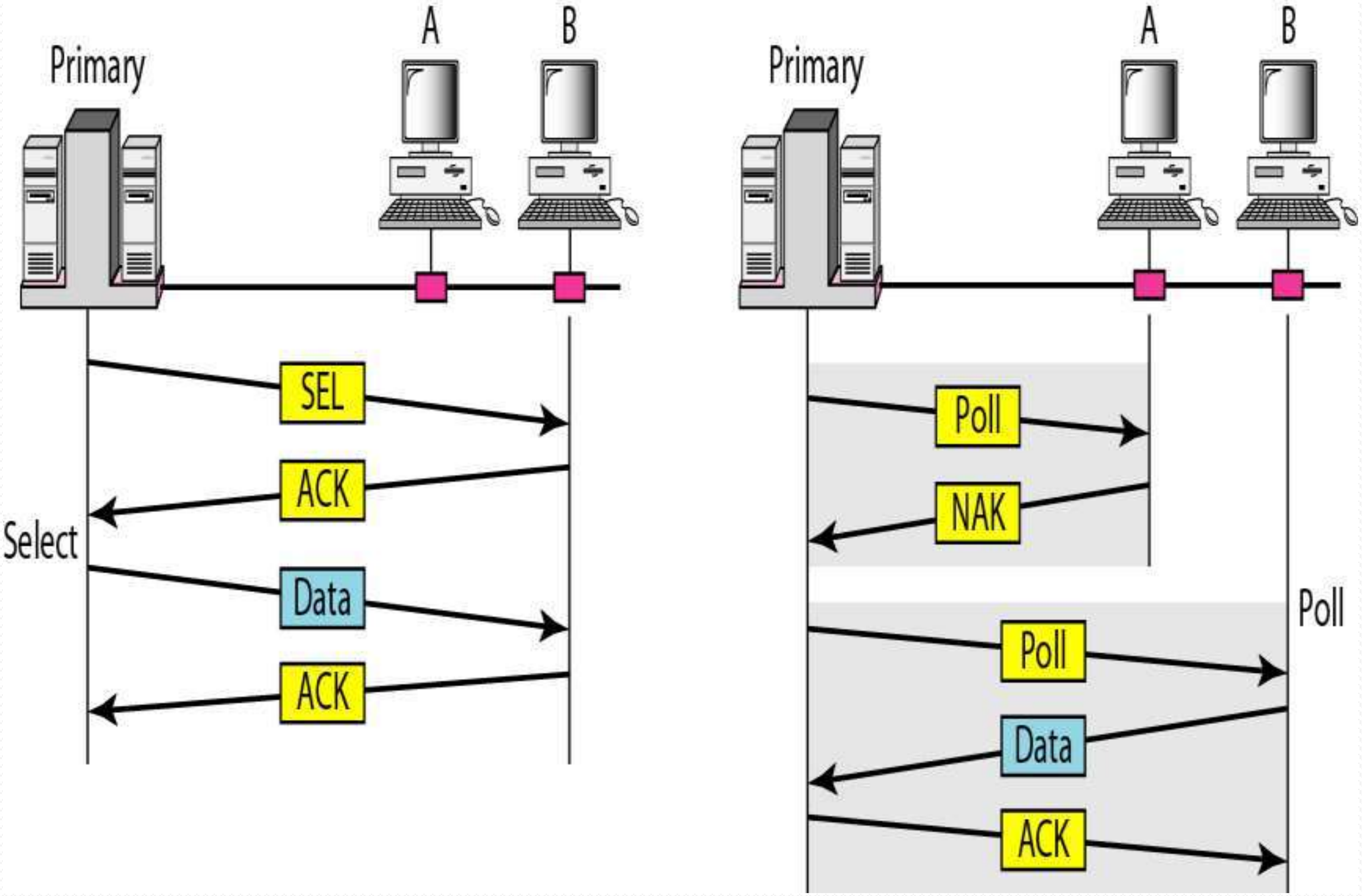
- Transmissions are organized into variable length cycles
- Each cycle begins with a reservation interval that consists of (N) mini slots. One mini slot for each of the N stations
- When a station needs to send a data frame, it makes a **reservation in its own mini slot.**
- By listening to the reservation interval, every station knows which stations will transfer frames, and in which order.
- The stations that made reservations can send their data frames after the reservation frame.



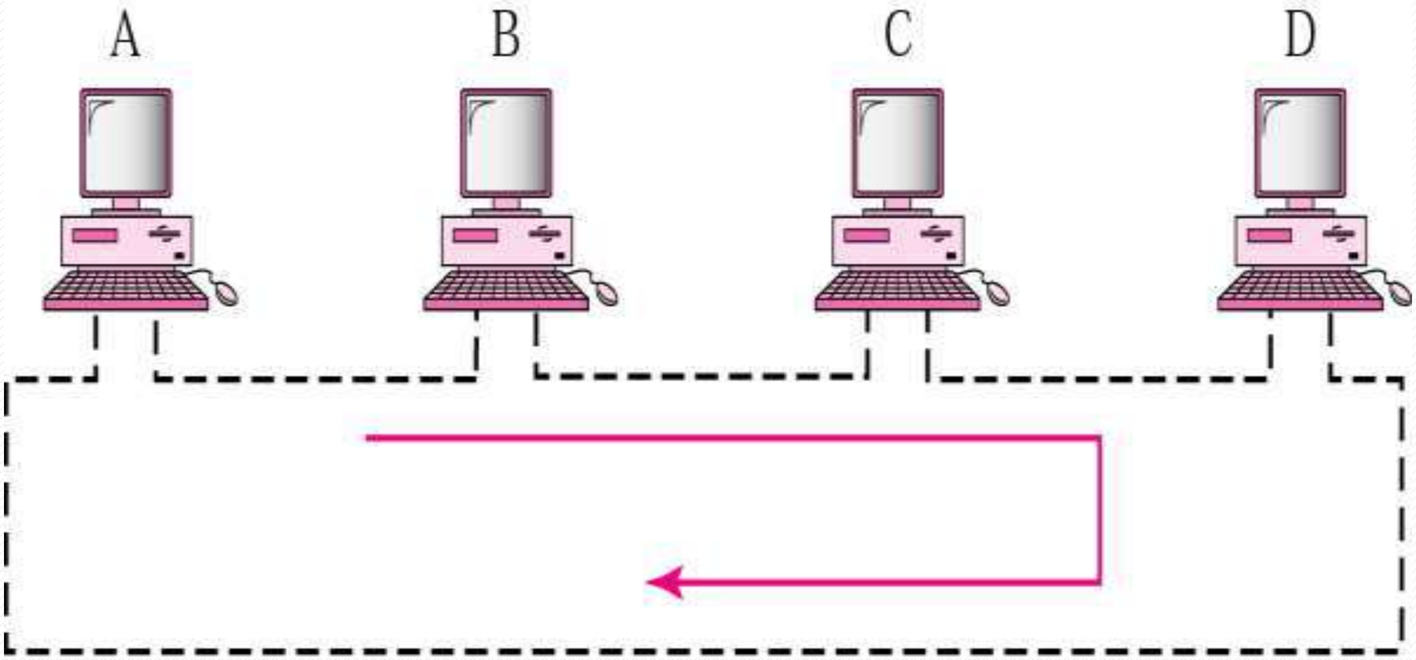
Polling

- Stations take turns accessing the medium
- Two models: **Centralized and distributed polling**
- **Centralized polling**
  - One device is assigned as **primary station and the others as secondary stations**
  - All data exchanges are done through the **primary**
  - When **the primary has a frame to send it sends a select frame that includes the address of the intended secondary**
  - When **the primary is ready to receive data it send a Poll frame for each device to ask if it has data to send or not. If yes, data will be transmitted otherwise NAK is sent.**
  - Polling can be done in order(Round-Robin) or based on predetermined order

- **Distributed polling**
  - No primary and secondary
  - Stations have a known polling order list which is made based on some protocol
  - station with the highest priority will have the access right first, then it passes the access right to the next station (it will send a pulling message to the next station in the pulling list), which will passes the access right to the following next station, …


Primary
A
B
SEL
ACK
Select
Data
ACK
Primary
A
B
Poll
NAK
Poll
Poll
Data
ACK

- **Token Passing**: It Implements Distributed Polling System
  - In the token-passing method, the stations in a network are organized in a logical ring. In other words, for each station, there is a *predecessor and a successor.*



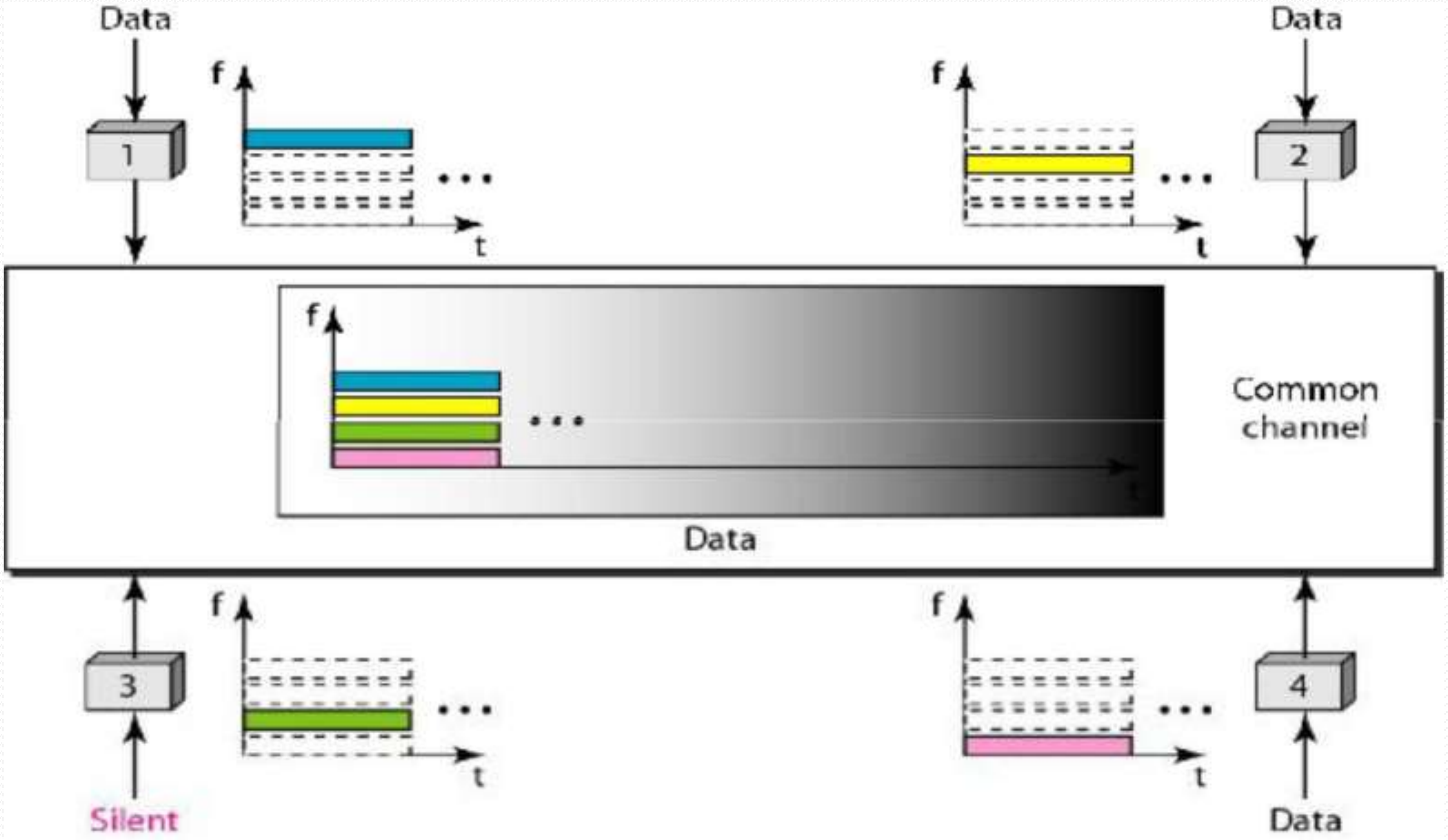
Channelization

- Channelization is a multiple-access method in which the available bandwidth of a link is shared in time, frequency, or through code, between different stations.
- There are three channelization protocols:
  - ***FDMA,***
  - ***TDMA and***
  - ***CDMA.***

FDMA

  - In **frequency-division multiple access (FDMA),the available bandwidth is divided into frequency bands.**
  - Each station is allocated a band to send its data. In other words, each band is reserved for specific station
- FDMA specifies a predetermined frequency band for the entire period of communication.
- FDM is a physical layer technique that combines the loads from low bandwidth channels and transmits them by using a high-bandwidth channel.
- **FDMA, on the other hand, is an access method in the data-link layer.**
- The data link layer in each station tells its physical layer to make a band pass signal from the data passed to it.

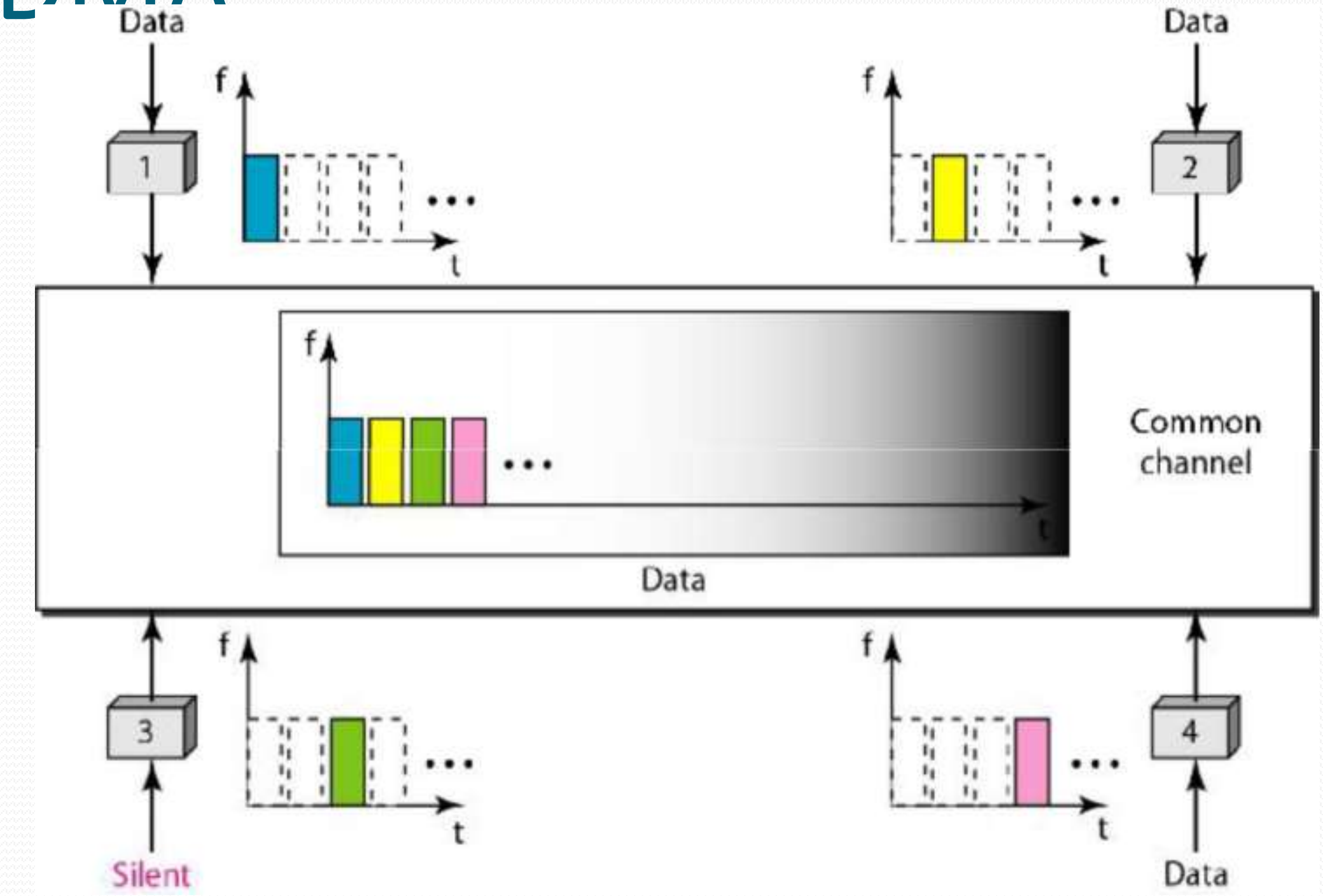
FDMA



TDMA

- In **time-division multiple access (TDMA),the stations share the bandwidth of the channel in time.**
- Each station is allocated a time slot during which it can send data. Each station transmits its data in its assigned time slot.
- The main problem with TDMA lies in achieving synchronization between the different stations.
- Each station needs to know the beginning of its slot and the location of its slot.
- This may be difficult because of propagation delays introduced in the system if the stations are spread over a large area.
- To compensate for the delays, we can insert *guard times.*
- Synchronization is normally accomplished by having some synchronization bits (normally referred to as *preamble bits) at the beginning of each slot.*

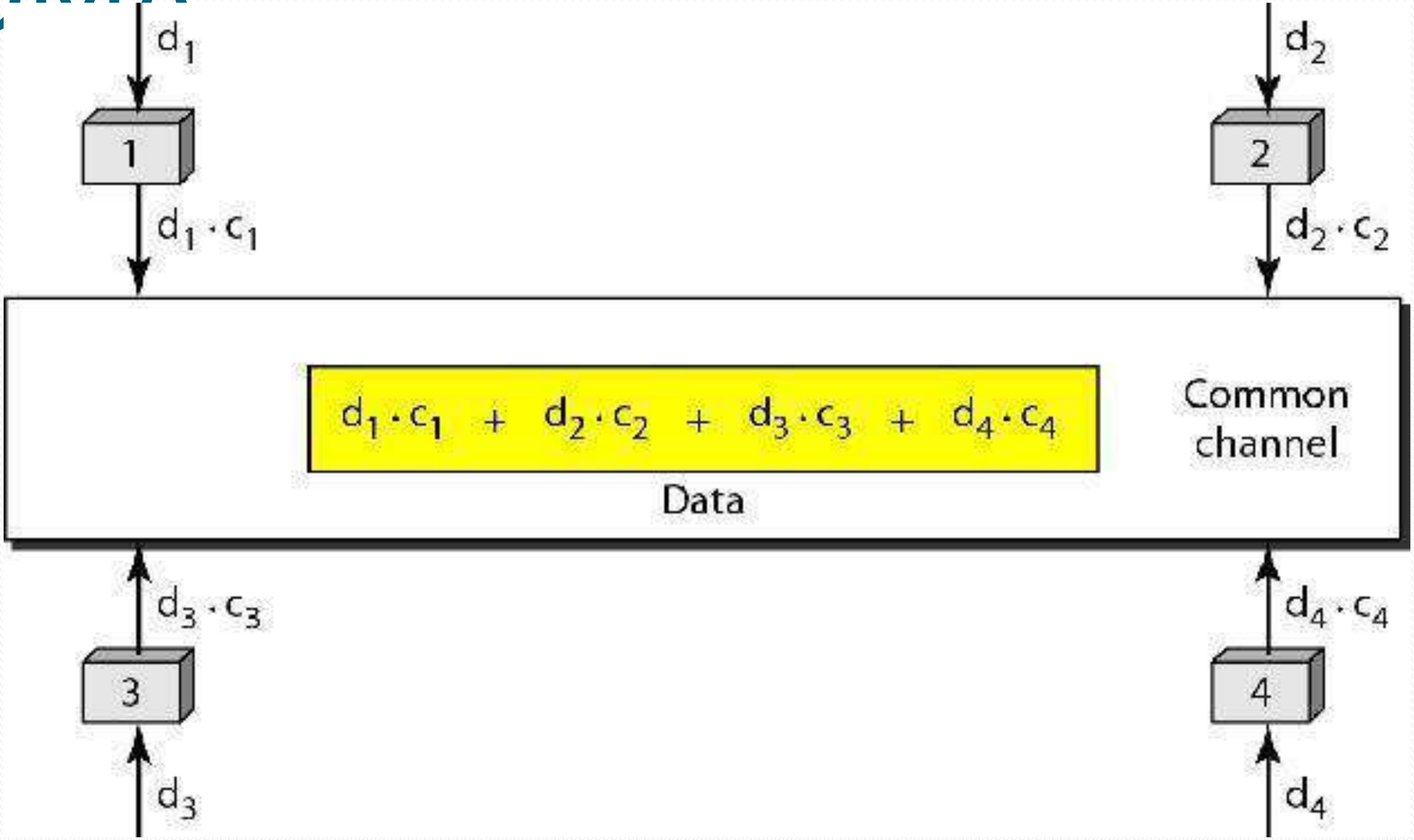
TDMA



CDMA

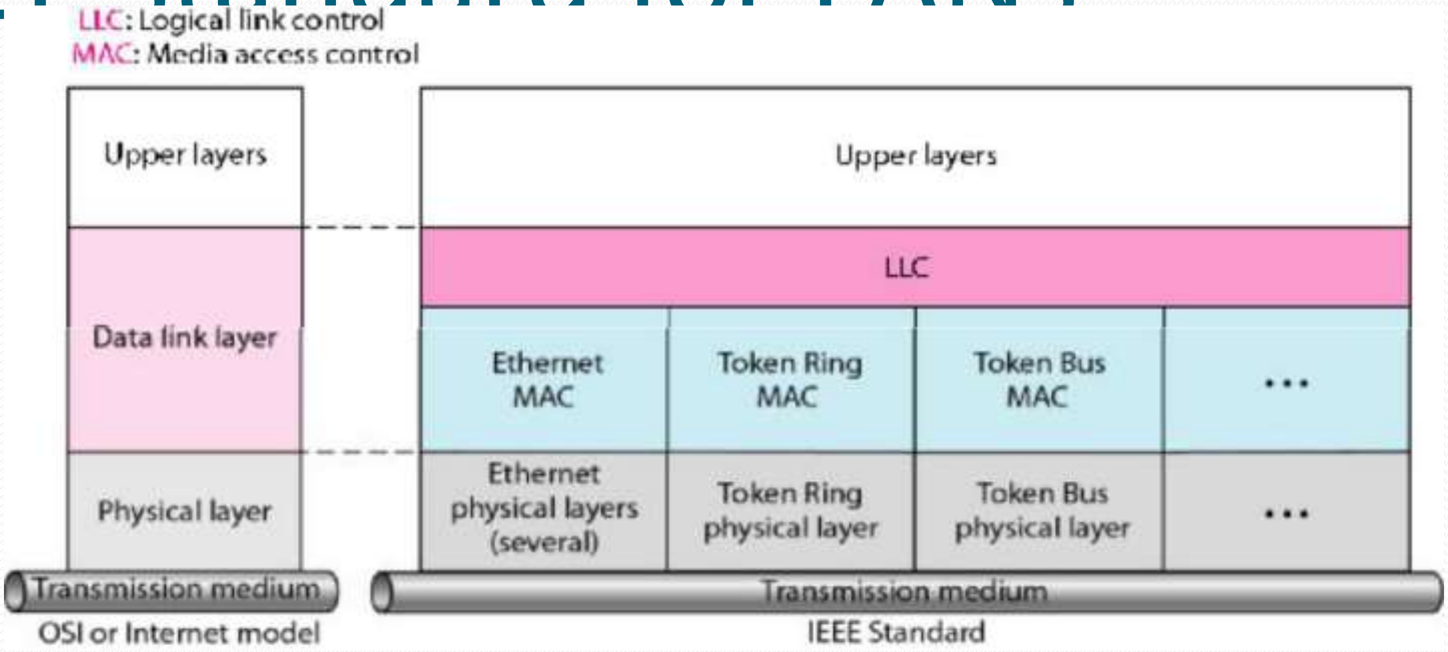
- **Code-division multiple access (CDMA) was visualized *several decades ago.***
- Recent advances in electronic technology have finally made its implementation possible.
- CDMA differs from FDMA in that only one channel occupies the entire bandwidth of the link.
- It differs from TDMA in that all stations can send data simultaneously; there is no timesharing.
- In CDMA, one channel carries all transmissions simultaneously.
- We assume that the assigned codes have two properties.
  - **If we multiply each code by another, we get 0.**
  - **If we multiply each code by itself, we get 4**

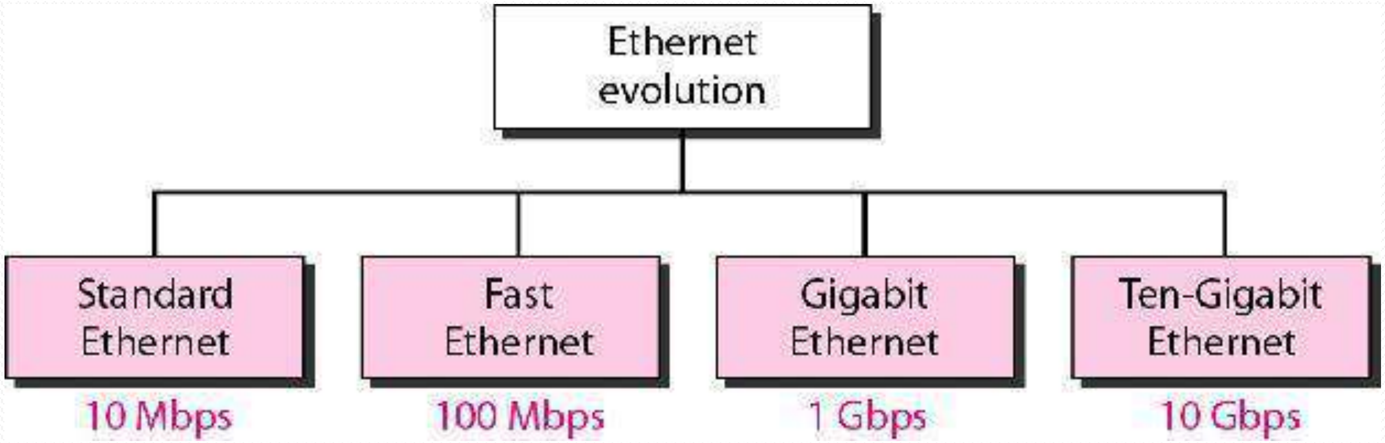
CDMA



d_1
1
$d_1 \cdot c_1$
d_2
2
$d_2 \cdot c_2$
$d_1 \cdot c_1 + d_2 \cdot c_2 + d_3 \cdot c_3 + d_4 \cdot c_4$
Data
Common channel
$d_3 \cdot c_3$
3
d_3
$d_4 \cdot c_4$
4
d_4

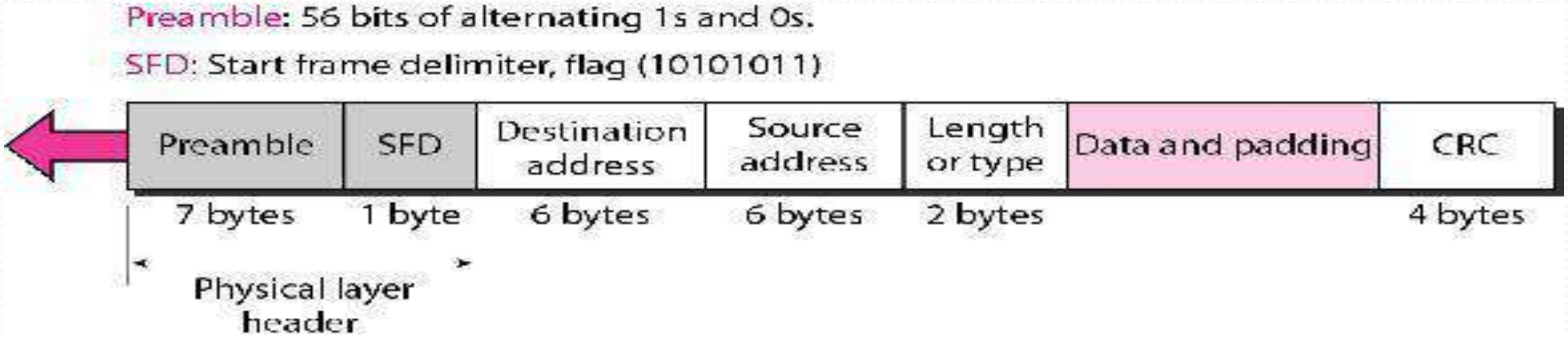
IEEE standard for LANs





Standard Ethernet

- Ethernet is most widely used LAN Technology, which is defined under IEEE standards 802.3.
- The reason behind its wide usability is Ethernet is easy to understand, implement, maintain and allows low-cost network implementation.
- Also, Ethernet offers flexibility in terms of topologies which are allowed.
- Ethernet operates in two layers of the OSI model, Physical Layer, and Data Link Layer.
- For Ethernet, the protocol data unit is Frame since we mainly deal with DLL.
- In order to handle collision, the Access control mechanism used in Ethernet is CSMA/CD.



- Physical Media :-
  - 10 Base5 -Thick Co-axial Cable with Bus Topology
  - 10 Base2 -Thin Co-axial Cable with Bus Topology
  - 10 Base T -UTP Cat 3/5 with Tree Topology
  - 10 Base FL -Multimode/Single mode Fiber with Tree Topology

Fast Ethernet:

- The Fast Ethernet standard (IEEE 802.3u) has been established for Ethernet networks that need higher transmission speeds.
- This standard raises the Ethernet speed limit from 10 Mbps to 100 Mbps with only minimal changes to the existing cable structure.

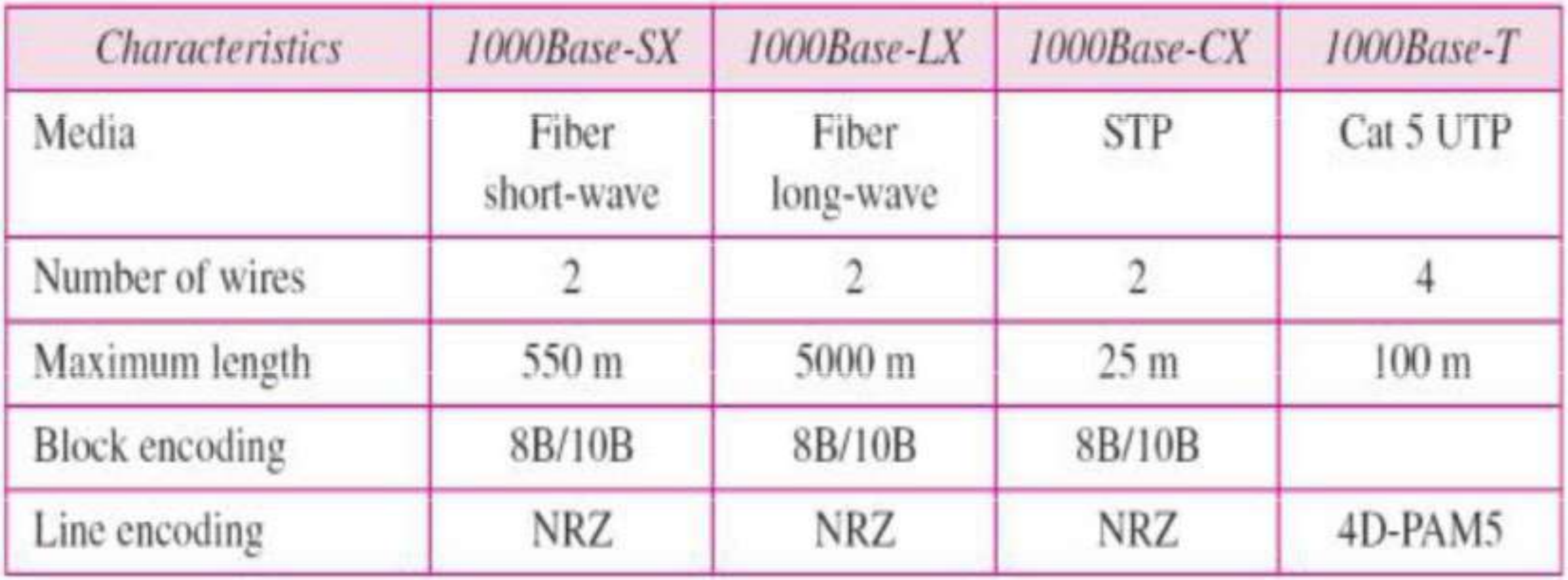
- Fast Ethernet provides faster throughput for video, multimedia, graphics, Internet surfing and stronger error detection and correction.
- **There are three types of Fast Ethernet: 100BASE-TX for use with level 5 UTP cable;**
- 100BASE-FX for use with fiber-optic cable; and 100BASE-T4 which utilizes an extra two wires for use with level 3 UTP cable.
- The 100BASE-TX standard has become the most popular due to its close compatibility with the 10BASE-T Ethernet standard.
- Network managers who want to incorporate Fast Ethernet into an existing with existing 10BASE-T segments.

Gigabit Ethernet

- Gigabit Ethernet was developed to meet the need for faster communication networks with applications such as multimedia and Voice over IP (VoIP).
- Also known as “gigabit-Ethernet-over-copper” or 1000Base-T, GigEis a version of Ethernet that runs at speeds 10 times faster than 100Base-T.
- It is defined in the IEEE 802.3 standard and is currently used as an enterprise backbone.
- Existing Ethernet LANs with 10 and 100 Mbps cards can feed into a Gigabit Ethernet backbone to interconnect high performance switches, routers and servers.
- The most important differences between Gigabit Ethernet and Fast Ethernet include the additional support of full duplex operation in the MAC layer and the data rates.

10 Gigabit Ethernet

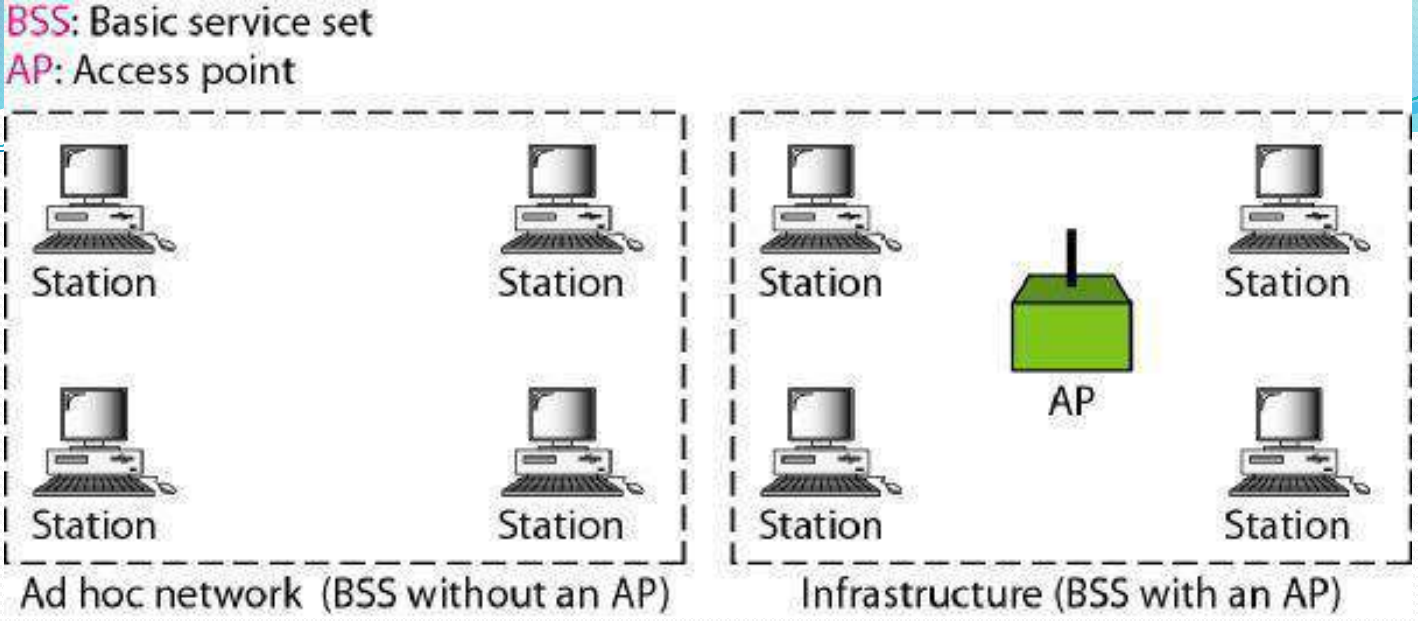
- 10 Gigabit Ethernet is the fastest and most recent of the Ethernet standards.
- IEEE 802.3ae defines a version of Ethernet with a nominal rate of 10Gbits/s that makes it 10 times faster than Gigabit Ethernet.
- Unlike other Ethernet systems, 10 Gigabit Ethernet is based entirely on the use of optical fiber connections.
- This developing standard is moving away from a LAN design that broadcasts to all nodes, toward a system which includes some elements of wide area routing.



Characteristics	*1000Base-SX*	*1000Base-LX*	*1000Base-CX*	*1000Base-T*
Media	Fiber short-wave	Fiber long-wave	STP	Cat 5 UTP
Number of wires	2	2	2	4
Maximum length	550 m	5000 m	25 m	100 m
Block encoding	8B/10B	8B/10B	8B/10B	
Line encoding	NRZ	NRZ	NRZ	4D-PAM5

WIRELESS LAN

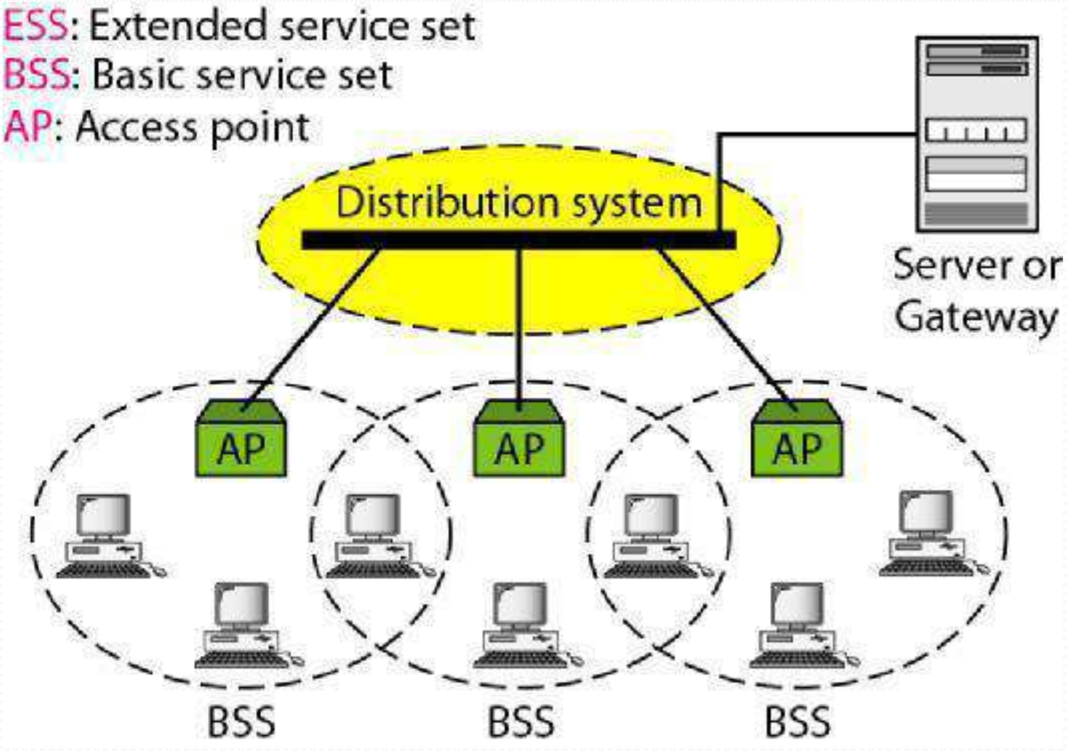
- IEEE has defined the specifications for a wireless LAN, called **IEEE 802.11**, which covers the physical and data link lay
- The standard defines two kinds of services: the basic service set (BSS) and the extended service set (ESS).



BSS: Basic service set
AP: Access point

Ad hoc network (BSS without an AP)

Infrastructure (BSS with an AP)

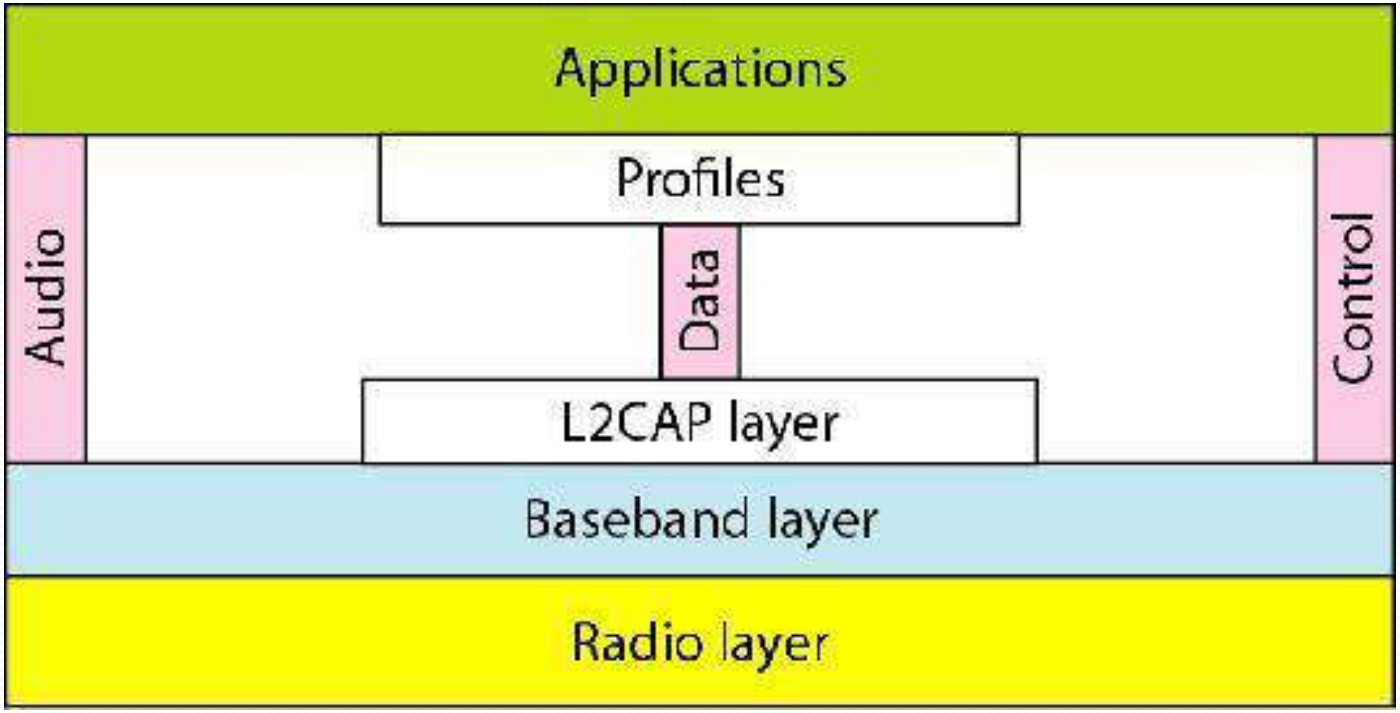


ESS: Extended service set
BSS: Basic service set
AP: Access point

Bluetooth

- Bluetooth radio typically hops faster and uses shorter packets as compared to other systems operating in the same frequency band.
- Use of FEC (Forward Error Correction) limits the impact of random noise.
- As the interference increases, the performance decreases.
- Bluetooth devices can interact with other Bluetooth devices.
- One of the devices acts as a master and others as slaves.
- This network is called "Piconet".
- A single channel is shared among all devices in Piconet.
- There can be up to seven active slaves in the Piconet.
- Each of the active slaves has an assigned 3 bit Active Member address.

Bluetooth


Applications
Audio
Profiles
Data
Control
L2CAP layer
Baseband layer
Radio layer

Network Layer DESIGN ISSUES

- Four Issues:
- **1.Interface between the host and the network** (the network layer is typically the boundary between the host and subnet)
- **2.Routing**
- **3.Congestion and deadlock**

- When more packets enter an area than can be processed, delays increase and performance decreases. If the situation continues, the subnet may have no alternative but to discard packets.
- If the delay increases, the sender may (incorrectly) retransmit, making a bad situation even worse.
- Overall, performance degrades because the network is using (wasting) resources processing packets that eventually get discarded.
- **4.Internetworking** (A path may traverse different network technologies(e.g., Ethernet, point-to-point links, etc.) packets may travel through many different networks each network may have a different frame format some networks may be connectionless, other connection oriented

ROUTING ALGORITHMS

A) NON-HIERARCHICAL ROUTING

- In this type of routing, interconnected networks are viewed as a single network, where bridges, routers and gateways are just additional nodes.
  - Every node keeps information about every other node in the network
  - In case of adaptive routing, the routing calculations are done and updated for all the nodes.

B) HIERARCHICAL ROUTING

- This is essentially a 'Divide and conquer' strategy. The network is divided into different regions and a router for a particular region knows only about its own domain and other routers. Thus, the network is viewed at two levels:
- The **Sub-network level**, where each node in a region has information about its peers in the same region and about the region's interface with other regions.
- The **Network Level**, where each region is considered as a single node connected to its interface nodes. The routing algorithms at this level handle the routing of packets between two interface nodes, and is isolated from intra-regional transfer.

- Advantages of Hierarchical Routing:
  - Smaller sizes of routing tables.
  - Substantially lesser calculations and updates of routing tables.
- Disadvantage:
  - Once the hierarchy is imposed on the network, it is followed and possibility of direct paths is ignored. This may lead to sub optimal routing.

- **SOURCE ROUTING**
  - Source routing is similar in concept to virtual circuit routing. It is implemented as under:
  - Initially, a path between nodes wishing to communicate is found out, either by flooding or by any other suitable method.
- This route is then specified in the header of each packet routed between these two nodes. A route may also be specified partially, or in terms of some intermediate hops.
- Advantages:
  - Bridges do not need to look up their routing tables since the path is already specified in the packet itself.

- The throughput of the bridges is higher, and this may lead to better utilization of bandwidth, once a route is established.
- Disadvantages:
  - Establishing the route at first needs an expensive search method like flooding.
  - To cope up with dynamic relocation of nodes in a network, frequent updates of tables are required; else all packets would be sent in wrong direction.

- **SHORTEST PATH ROUTING**
  - Here, the central question dealt with is 'How to determine the optimal path for routing?' Various algorithms are used to determine the optimal routes with respect to some predetermined criteria. Some of the important ways of determining the cost are:
- **Minimum number of hops:** If each link is given a unit cost, the shortest path is the one with minimum number of hops. Such a route is easily obtained by a breadth first search method. This is easy to implement but ignores load, link capacity etc.
- **Transmission and Propagation Delays:** If the cost is fixed as a function of transmission and propagation delays, it will reflect the link capacities and the geographical distances. However these costs are essentially static and do not consider the varying load conditions.
- **Queuing Delays:** If the cost of a link is determined through its queuing delays, it takes care of the varying load conditions, but not of the propagation delays.

- **a) Bellman-Ford Algorithm**
  - This algorithm iterates on the number of edges in a path to obtain the shortest path. Since the number of hops possible is limited (cycles are implicitly not allowed), the algorithm terminates giving the shortest path.
- Notation:

d i,j= Length of path between nodes iand j, indicating the cost of the link.

h= Number of hops

- D[i,h] = Shortest path length from node ito node 1, with upto'h' hops.

D[1,h] = 0

for all h .

b) Dijkstra's Algorithm

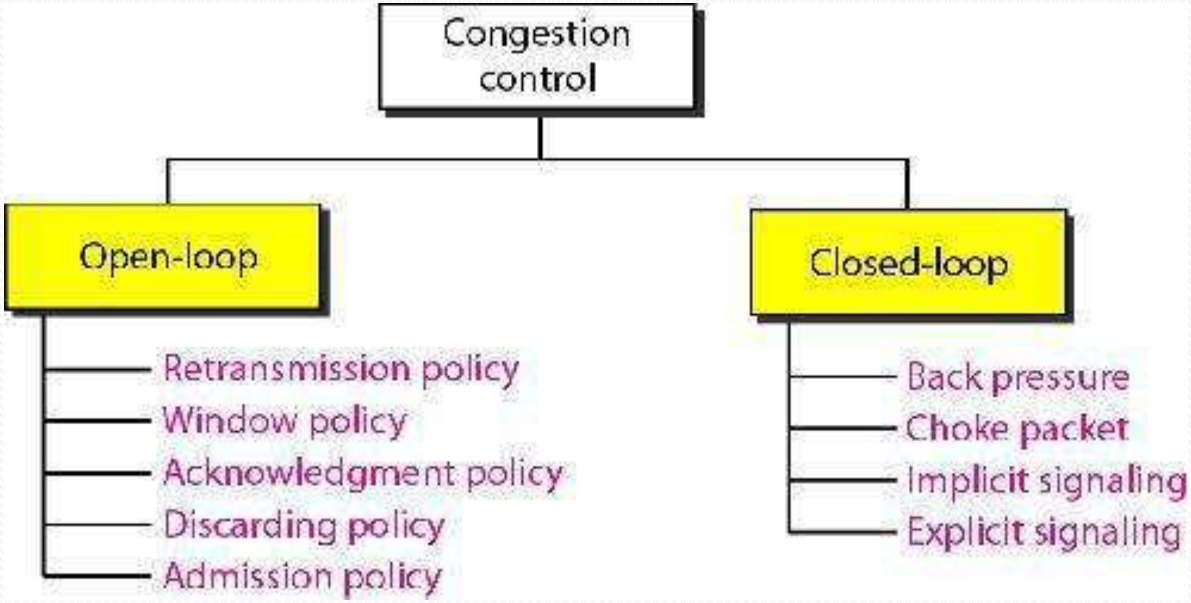
- Notation:
- Di =Length of shortest path from node 'i' to node 1.

  di,j =Length of path between nodes i and j
- **Dj= min [Dj , Di + dj,i]**
- Finally, after N-1 iterations, the shortest paths for all nodes are known, and the algorithm terminates.

CONGESTION CONTROL ALGORITHMS

- An important issue in a packet-switched network is **congestion.**
- **Congestion in a network may occur if the load on the network-the number of packets sent to the network-is greater than the *capacity of the network the number of packets a network can handle.***
- ***Congestion control refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.***
- Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. In general, we can divide congestion

- In general, we can divide congestion control mechanisms into two broad categories: open-loop congestion control (prevention) and closed-loop congestion control (removal) as shown



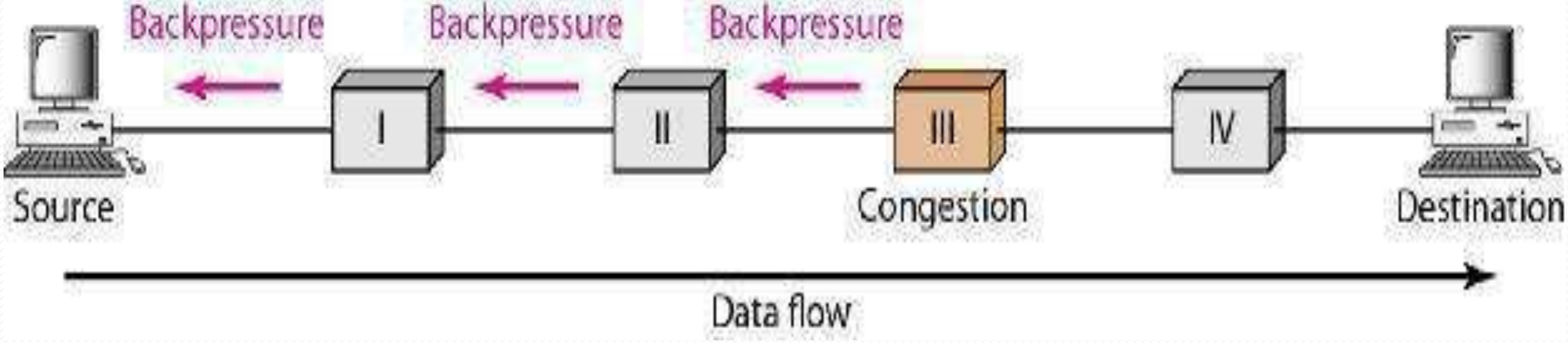
A) OPEN-LOOP CONGESTION CONTROL

- In open-loop congestion control, policies are applied to prevent congestion before it happens. In these mechanisms, congestion control is handled by either the source or the destination. We give a brief list of policies that can prevent congestion.
- a) **Retransmission Policy**: Retransmission is sometimes unavoidable. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted.

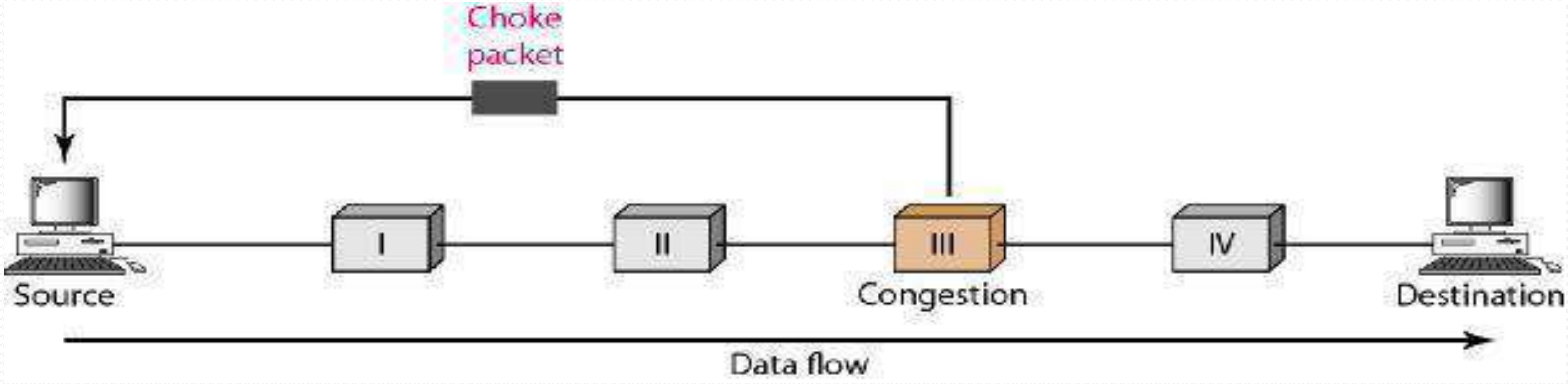
- b) **Window Policy**: The type of window at the sender may also affect congestion. The Selective Repeat window is better than the Go-Back-N window for congestion control.

- c) **Acknowledgment Policy**: The acknowledgment policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion.
- d) **Discarding Policy**: A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transmission.
- e) **Admission Policy**: An admission policy, which is a quality-of-service mechanism, can also prevent congestion in virtual-circuit networks..

- Node III in the figure has more input data than it can handle. It drops some packets in its input buffer and informs node II to slow down. Node II, in turn, may be congested because it is slowing down the output flow of data. If node II is congested, it informs node I to slow down, which in turn may create congestion.



- b) **Choke Packet**: A choke packet is a packet sent by a node to the source to inform it of congestion. Note the difference between the backpressure and choke packet methods. In backpressure, the warning is from one node to its upstream node, although the warning may eventually reach the source station

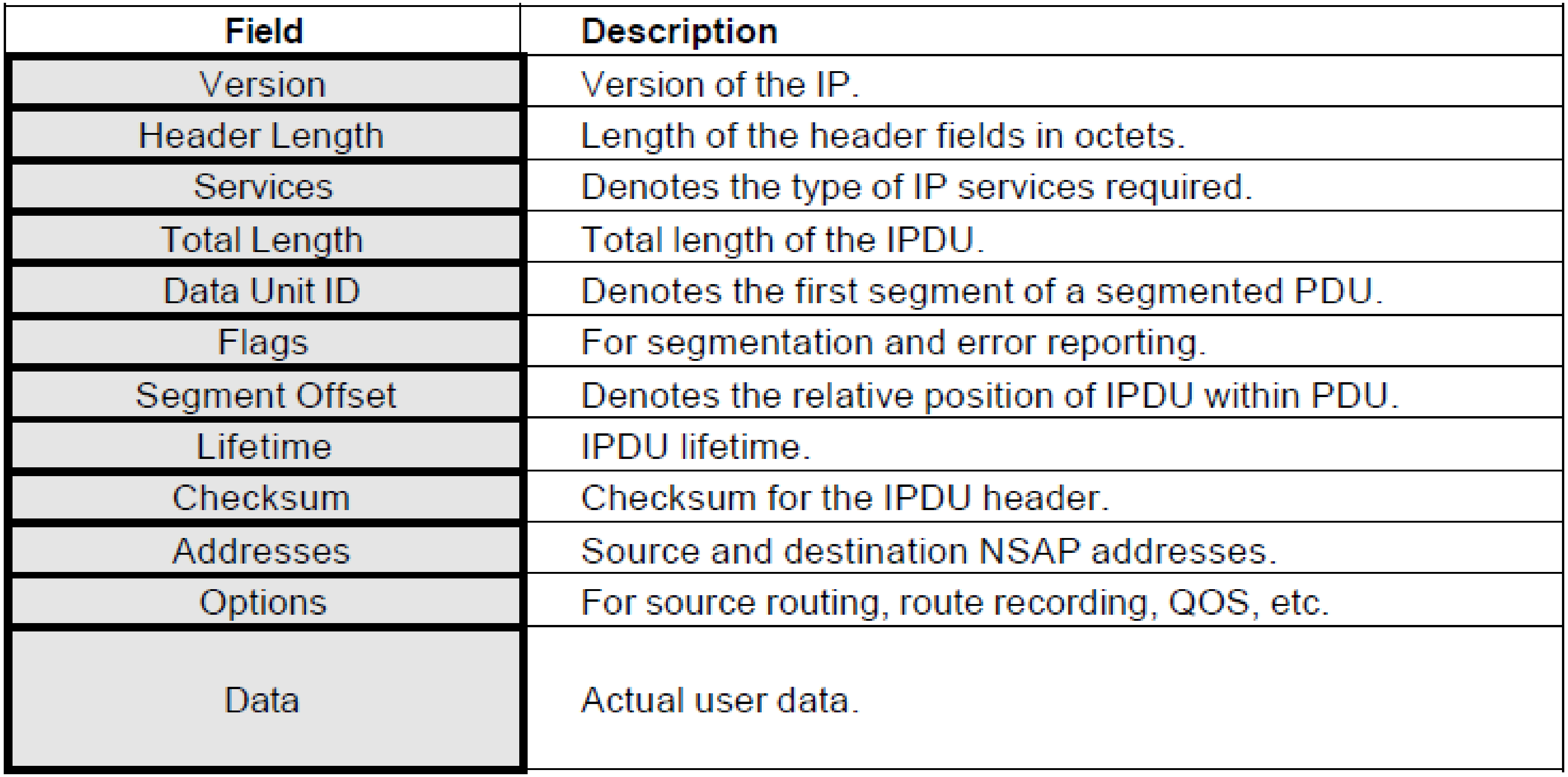


- c) **Implicit Signaling**: In implicit signaling, there is no communication between the congested node or nodes and the source. The source guesses that there is congestion somewhere in the network from other symptoms.
- d) **Explicit Signaling**: The node that experiences congestion can explicitly send a signal to the source or destination. The explicit signaling method, however, is different from the choke

IP

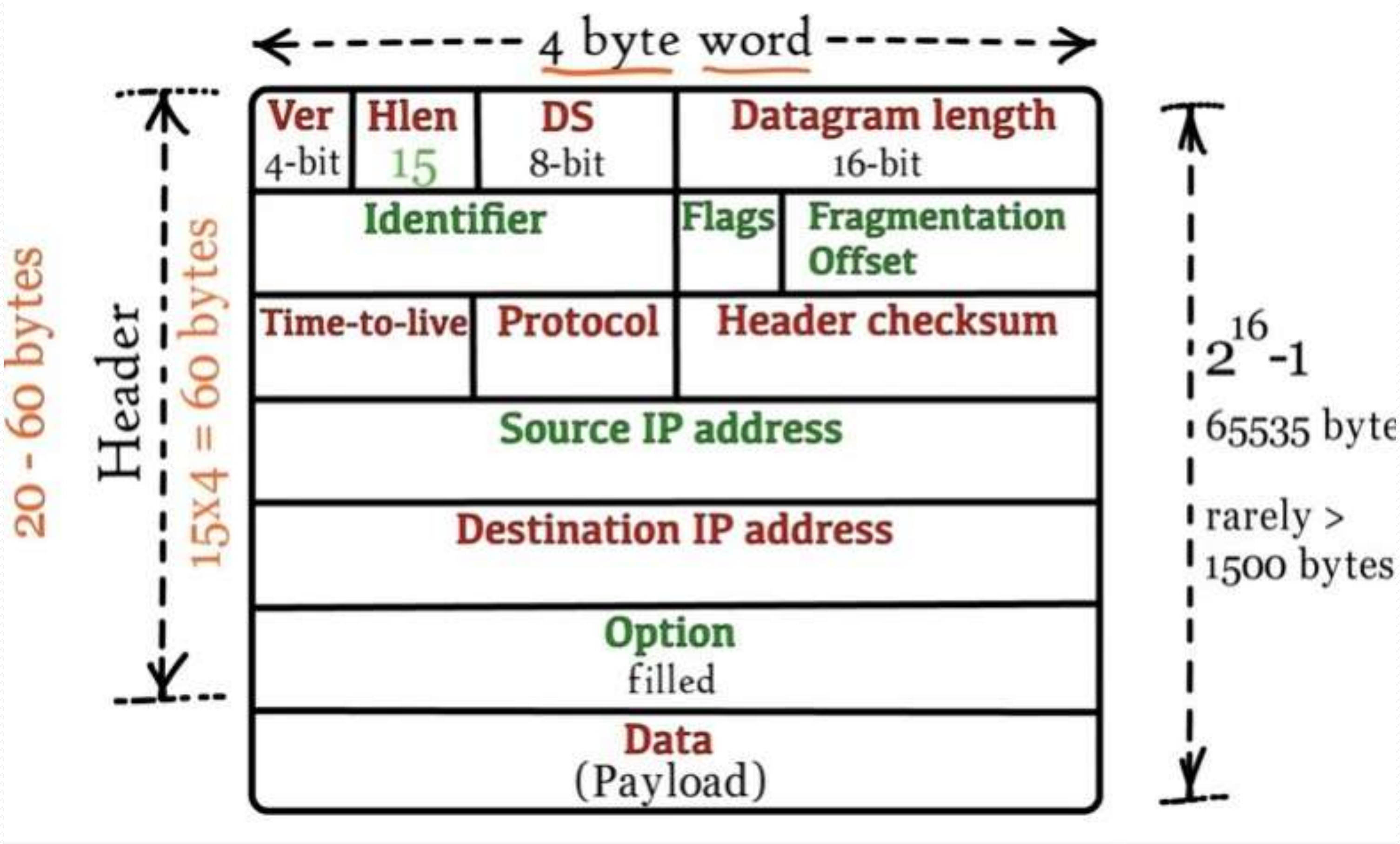
- IP”, the “Internet Protocol”, is the network layer protocol associated with the popular “TCP/IP” network software.
- The Internet Protocol (IP) is a connectionless datagram protocol developed by the US Department of Defense Advanced Research Projects Agency.
- An IP network consists of a set of **subnets** and a set of **intermediate stations** which act as gateways.

- IP data grams are referred to as **Internet Protocol Data Units, or IPDUs**

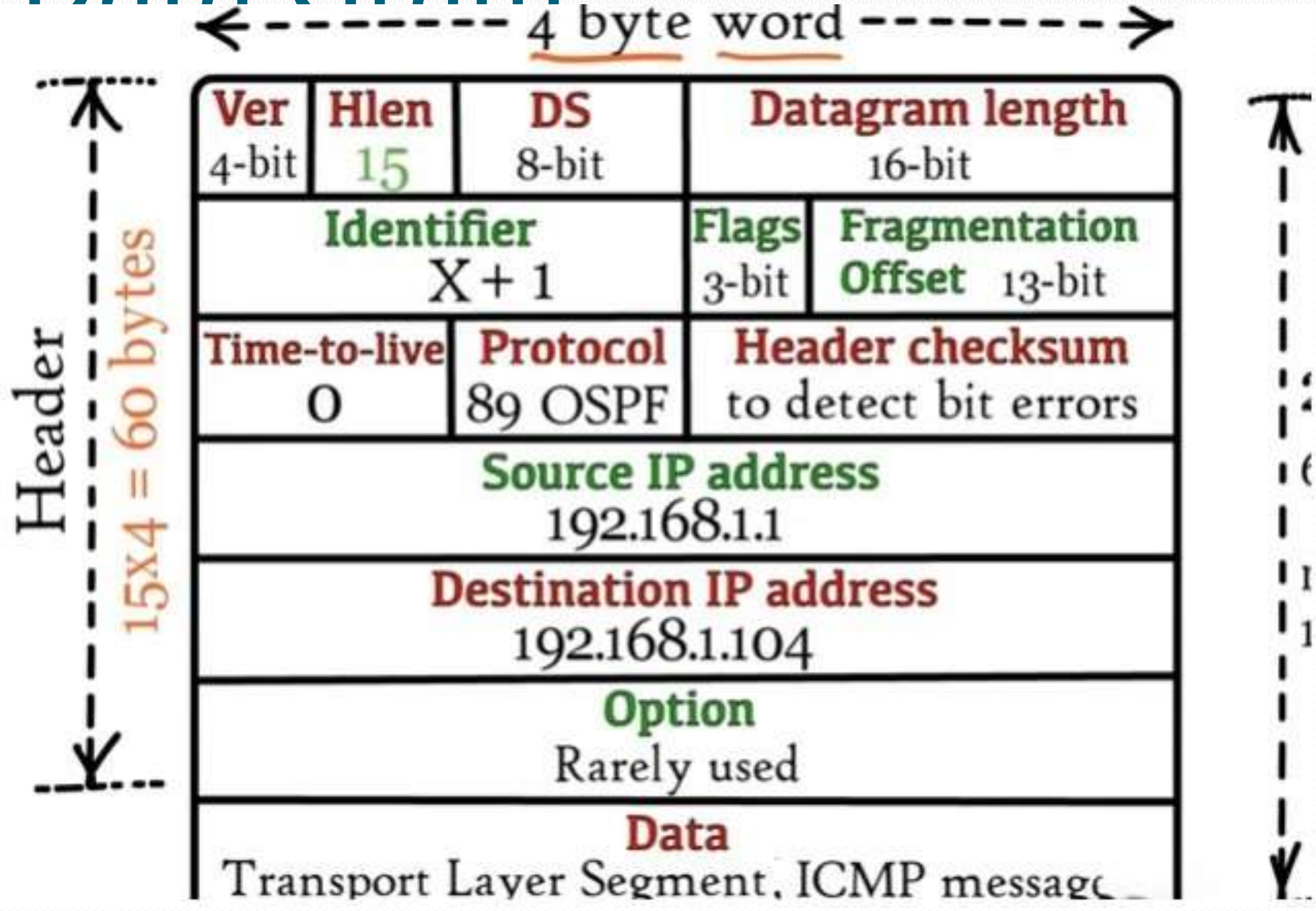


Field	Description
Version	Version of the IP.
Header Length	Length of the header fields in octets.
Services	Denotes the type of IP services required.
Total Length	Total length of the IPDU.
Data Unit ID	Denotes the first segment of a segmented PDU.
Flags	For segmentation and error reporting.
Segment Offset	Denotes the relative position of IPDU within PDU.
Lifetime	IPDU lifetime.
Checksum	Checksum for the IPDU header.
Addresses	Source and destination NSAP addresses.
Options	For source routing, route recording, QOS, etc.
Data	Actual user data.

- The interface for IP service users is quite simple, and consists of two primitives: ***send*** *and* ***deliver*****.** (An IP service user transmits data by issuing a *send command* which contains various IPDU fields as parameters.)
- When the IPDU is delivered to its final destination, (the receiving station is issued with a *deliver command which* contains the original data.)


4 byte word
Ver
4-bit
Hlen
15
DS
8-bit
Datagram length
16-bit
Identifier
Flags
Fragmentation Offset
Time-to-live
Protocol
Header checksum
Source IP address
Destination IP address
Option
filled
Data
(Payload)
20 - 60 bytes
Header
15X4 = 60 bytes
2^16 -1
65535 byte
rarely >
1500 bytes

IP Data Gram



Ver 4-bit
Hlen 15
DS 8-bit
Datagram length 16-bit

Identifier X + 1
Flags 3-bit
Fragmentation Offset 13-bit

Time-to-live 0
Protocol 89 OSPF
Header checksum to detect bit errors

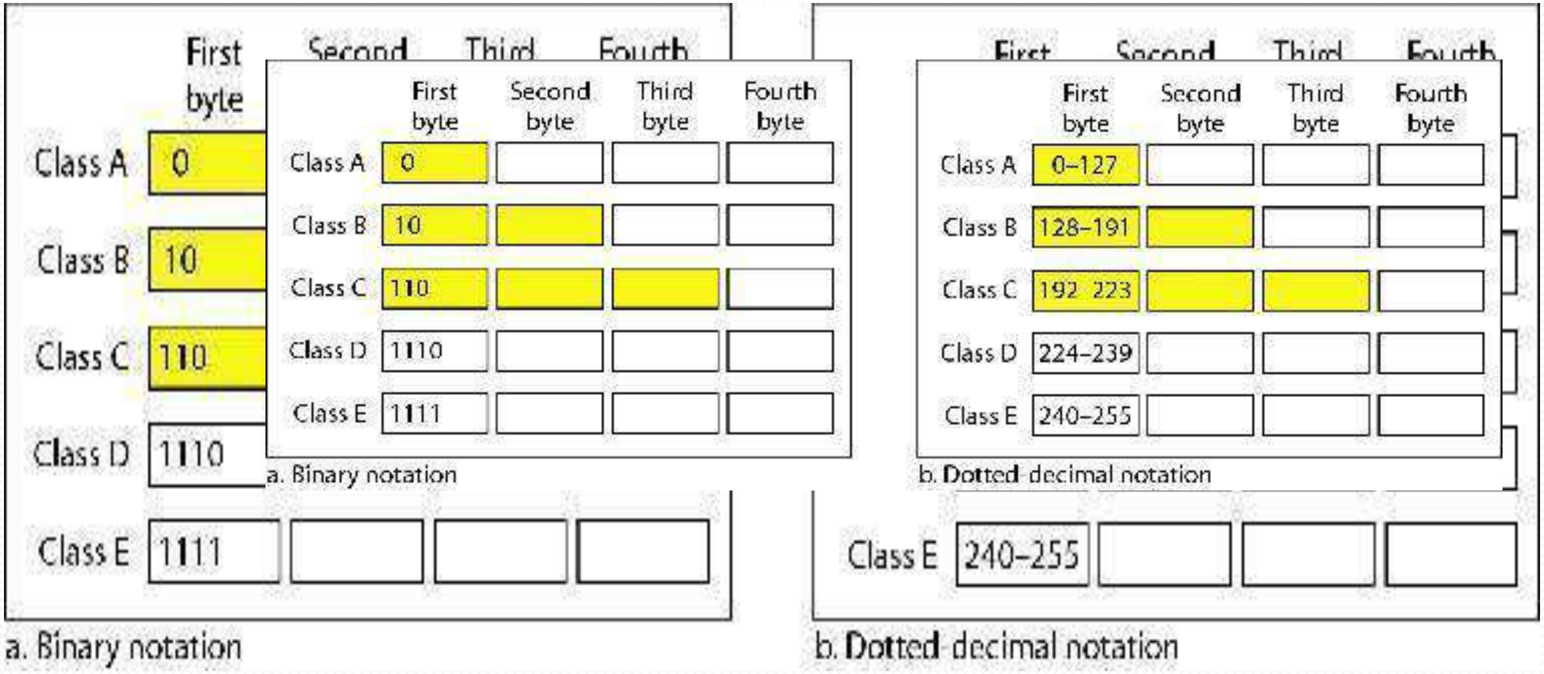
Source IP address 192.168.1.1

Destination IP address 192.168.1.104

Option Rarely used

Data Transport Layer Segment, ICMP message

Class full addressing



	First byte	Second byte	Third byte	Fourth byte
Class A	0			
Class B	10	🟨		
Class C	110	🟨	🟨	
Class D	1110			
Class E	1111			

a. Binary notation

	First byte	Second byte	Third byte	Fourth byte
Class A	0–127			
Class B	128–191	🟨		
Class C	192–223	🟨	🟨	
Class D	224–239			
Class E	240–255			

b. Dotted-decimal notation

a. Binary notation

b. Dotted-decimal notation

Hardware address vs IP address

- Hardware address is also called MAC address or Physical address
- Every node in the LAN is identified with the help of MAC address
- Unique
- Cannot be changed
- Assigned by the manufacturer
- Represented in hexadecimal
- Example 70-20-84-00-ED-FC
- Separator: hyphen(-), period(.), and colon(:)

Hardware address vs IP address

MAC Address	IP Address
Needed for communication	Needed for communication
48 bits	32 bits
Represented in hexadecimal	Represented in Decimal
Switch needs MAC address to forward data	Router needs IP address to forward data
Example: 70-00-20-80-ED-FC	Example:10.10.20.56

CONNECTING DEVICES

- The communication media used to link devices to form a computer network include electrical cable (Home PNA, power line communication), optical fiber (fiber-optic communication), and radio waves (wireless networking).
- Various devices are used to connect network of a computer The most common devices are:
- Routers
- Gateways
- Repeaters
- Bridges
- Hub
- Modem

- **A) ROUTER**

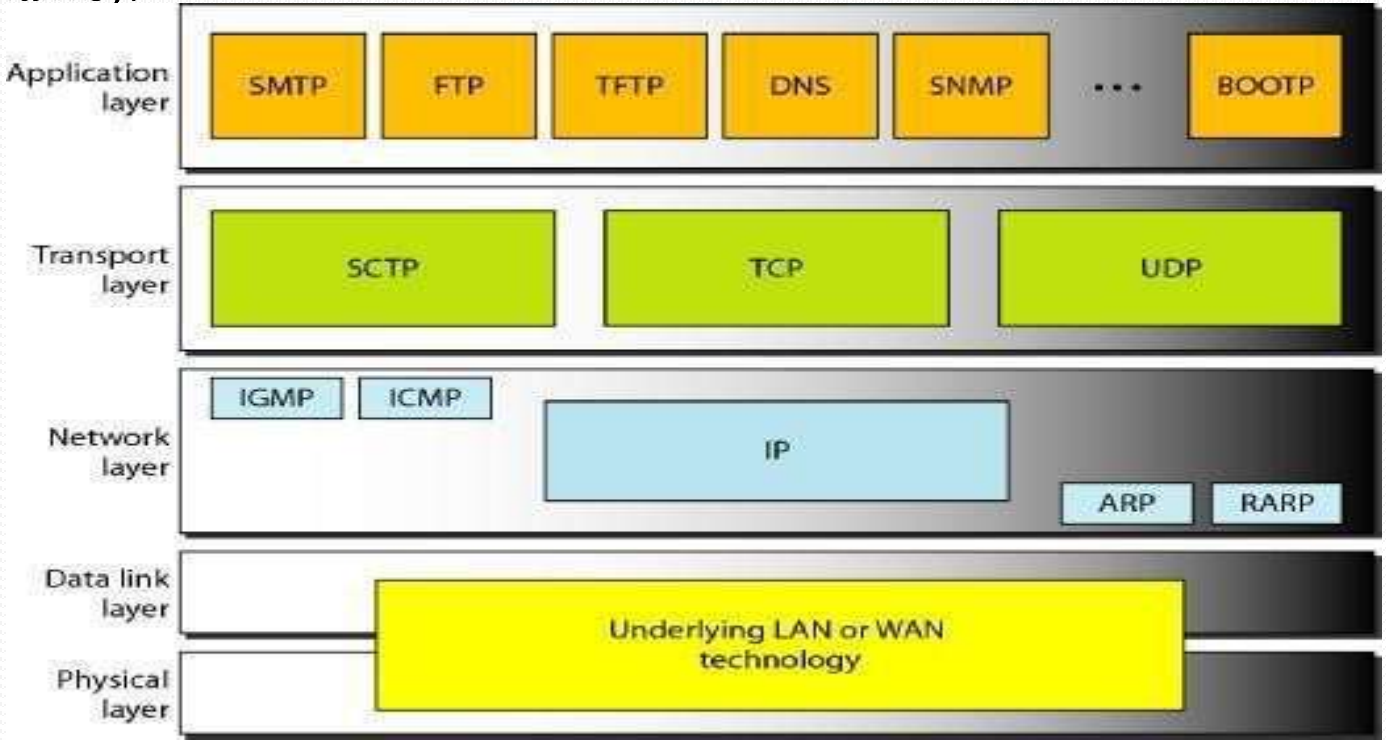
  Routers are devices which connect two are more networks that use similar protocol. A router consists of hard ware and software. Hard ware can be a computer is specific device. Software consists of special management program that controls flow of data between networks. Routers operate at a network layer of O.S.I model.

- **B) GATEWAYS**

  Gateways are devices which connect two are more networks that use different protocols. They are similar in function to routes but they are more powerful and intelligent devices. A gateway can actually convert data so that network with an application on a computers

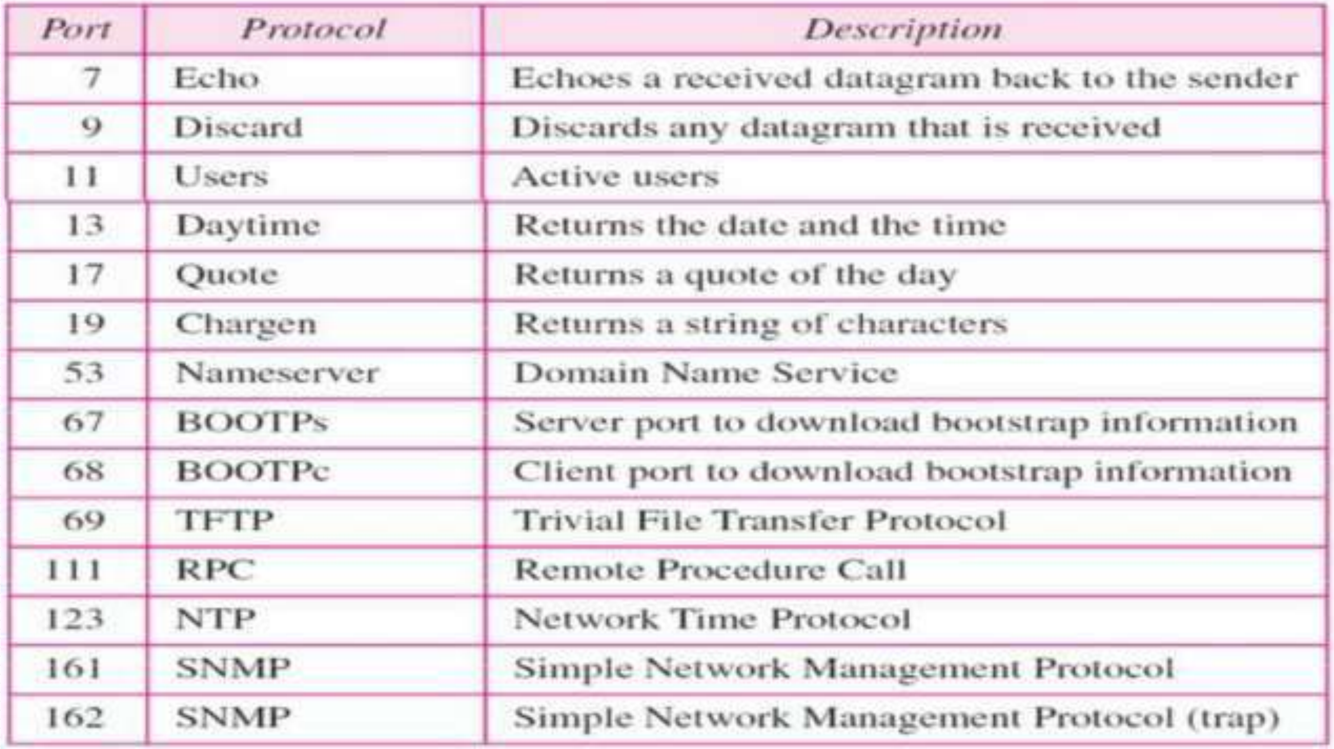
TRANSPORT LAYER PROTOCOL

- The data link layer is responsible for delivery of frames between two neighboring nodes over a link. This is called *node-to-node delivery.*
- The network layer is responsible for delivery of datagrams between two hosts. This is called *host-to-host delivery.*
- Communication on the Internet is not defined as the exchange of data between two nodes or between two hosts.
- **Real communication takes place between two processes (application programs).**



USER DATAGRAM PROTOCOL (UDP)

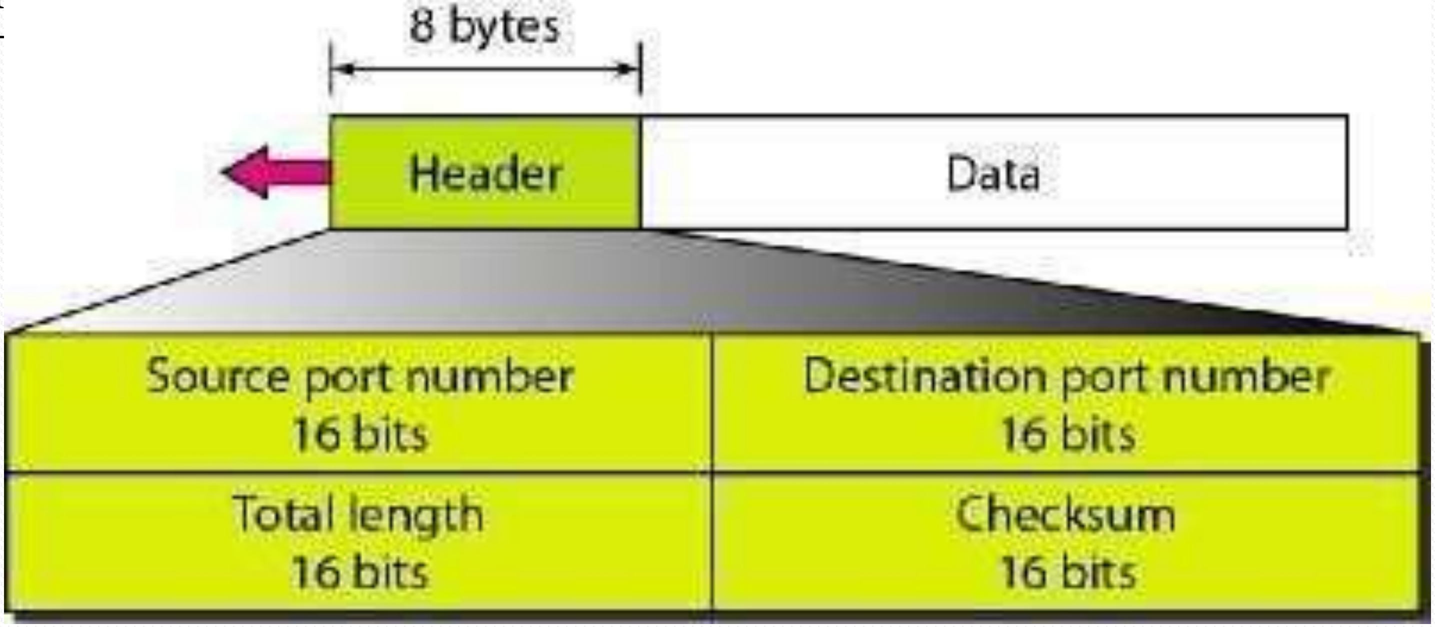
- The User Datagram Protocol (UDP) is called a connectionless, unreliable transport protocol. It does not add anything to the services of IP except to provide process-to process communication instead of host -to-host communication. Also, it performs very limited error checking.



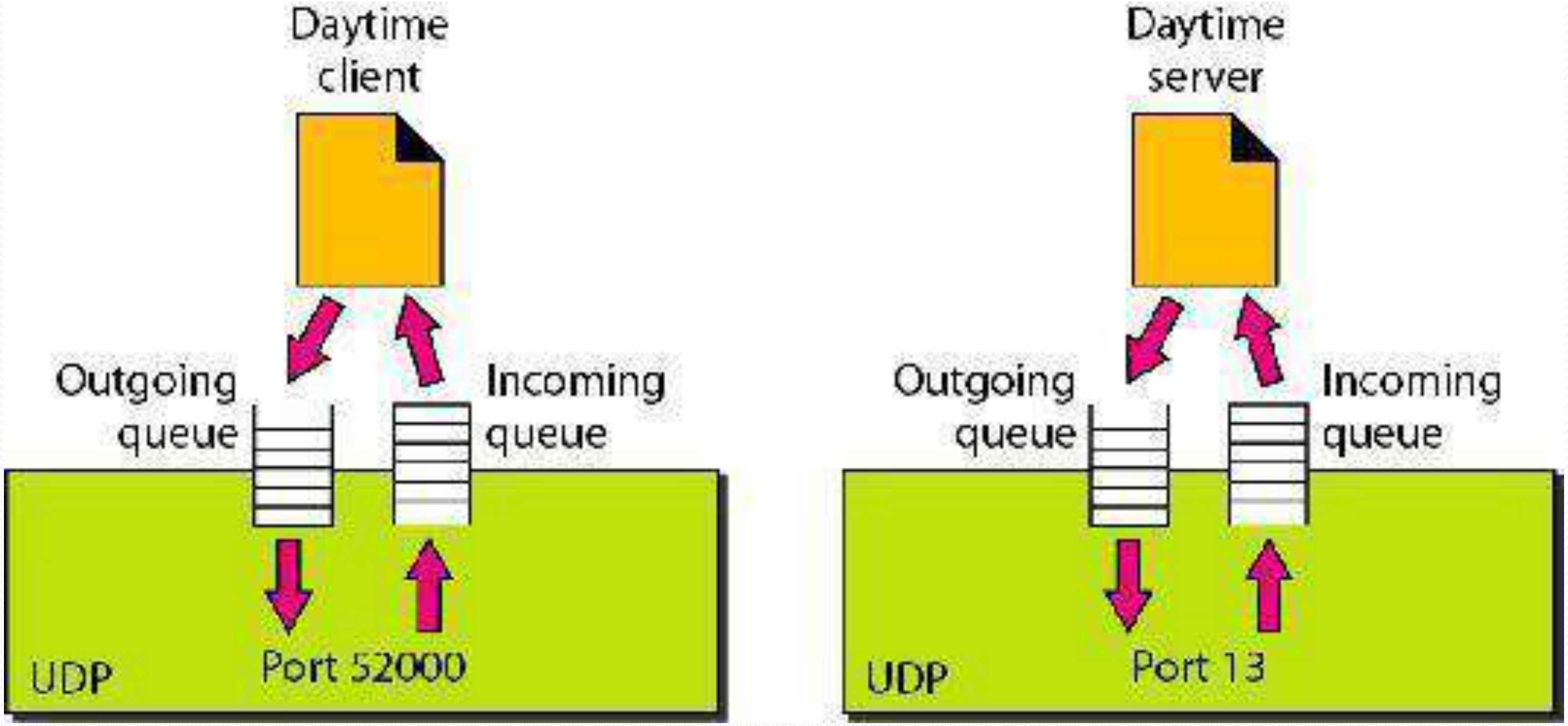
Port	*Protocol*	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
53	Nameserver	Domain Name Service
67	BOOTPs	Server port to download bootstrap information
68	BOOTPc	Client port to download bootstrap information
69	TFTP	Trivial File Transfer Protocol
111	RPC	Remote Procedure Call
123	NTP	Network Time Protocol
161	SNMP	Simple Network Management Protocol
162	SNMP	Simple Network Management Protocol (trap)

USER DATAGRAM

- UDP packets, called user datagrams, have a fixed-size header of 8 bytes.
- UDP is a very simple protocol using a minimum of overhead. If a process wants to send a small message and does not care much about reliability, it can use UDP. Sending a small message by using UDP takes much less interaction between the sender and receiver than using TCP or SC



UDP Operation


Daytime client
Outgoing queue
Incoming queue
UDP
Port 52000
Daytime server
Outgoing queue
Incoming queue
UDP
Port 13