INSTITUTE OF AERONAUTICAL ENGINEERING

(Autonomous)

Dundigal, Hyderabad - 500 043

Course Title	**COMPUTER NETWORKS**			
Course Code	**A70515**			
Regulation	**R15 – JNTUH**			
Course Structure	Lectures	Tutorials	Practical	Credits
	4	-	-	4
Course Coordinator	Mr. P Ravinder, Assistant Professor, CSE			
Team of Instructors	Mr. P. Ravinder, Associate Professor, CSE. Mr. C. Raghavendra, Associate Professor, CSE. Ms. M. Geetha Yadav, Assistant Professor, CSE. Ms. B. Geethavani, Assistant Professor, CSE.			
Branch	IV B. Tech I Sem, ECE			

UNIT -I

Physical Layer, Data Link Layer and Overview of the Internet

PROTOCOLS AND STANDARDS

Protocol

A protocol is a set of rules that govern data communications. A protocol defines what is communicated, how it is communicated, and when it is communicated. The key elements of a protocol are syntax, semantics, and timing

Syntax

The term syntax refers to the structure or format of the data, meaning the order in which they are presented

For example, a simple protocol might expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

Semantics

The word semantics refers to the meaning of each section of bits.

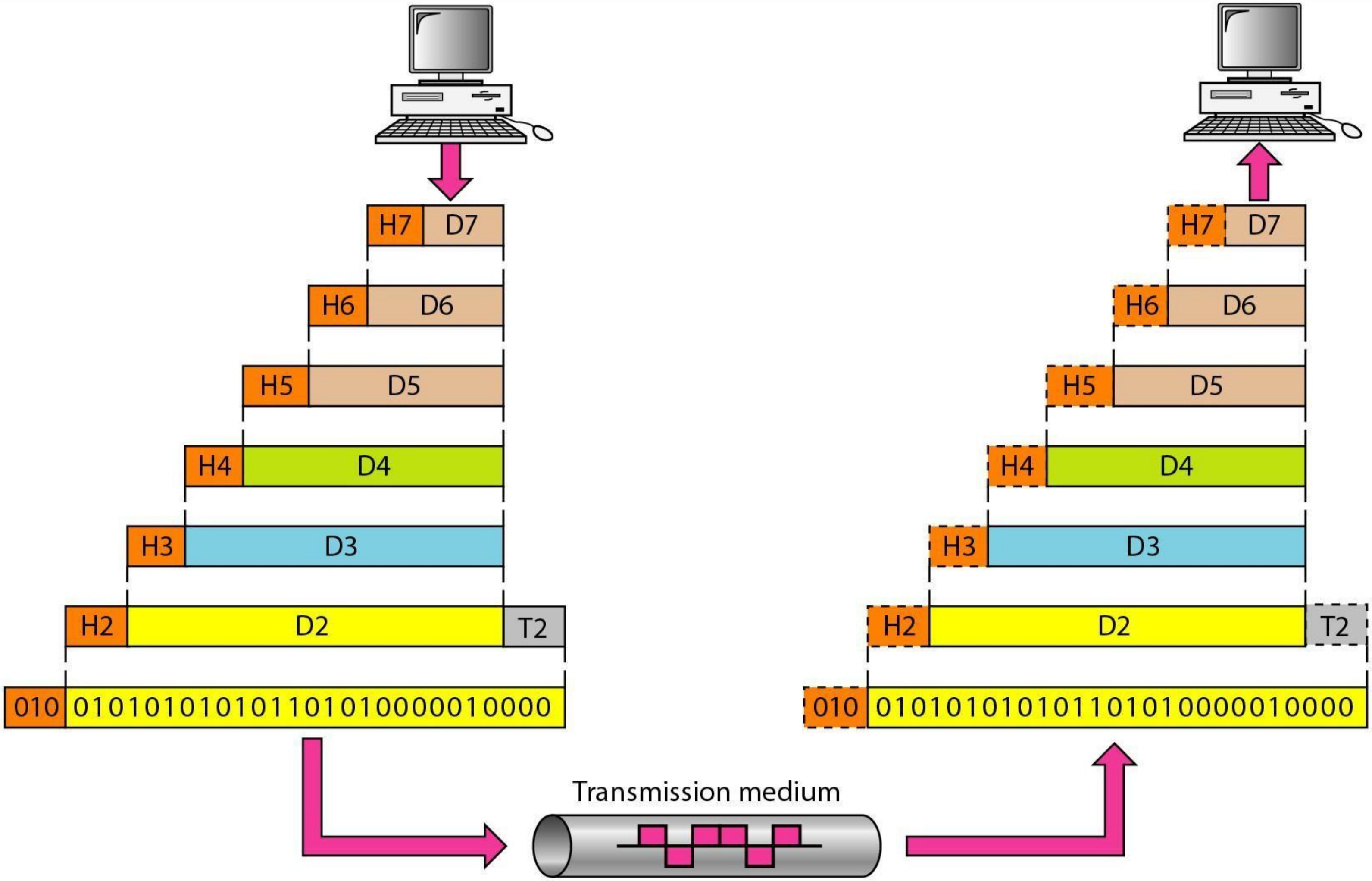
For example, does an address identify the route to be taken or the final destination of the message?

Timing

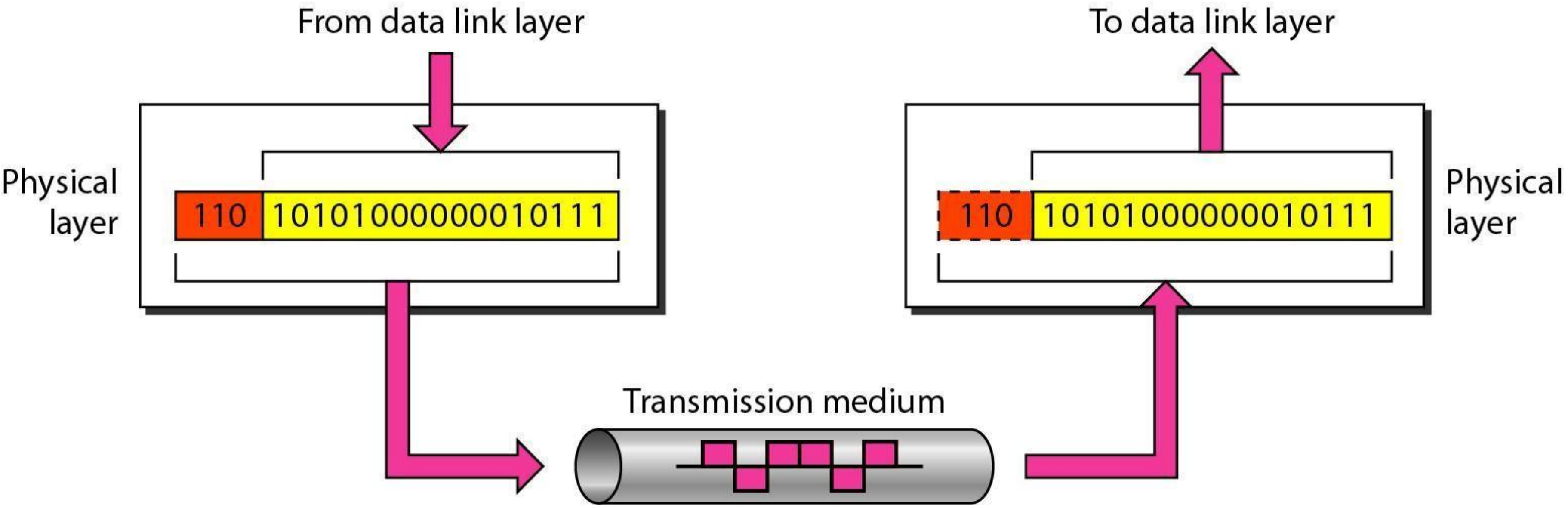
The term timing refers to two characteristics: when data should be sent and how fast they can be sent.

For example, if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and some data will be lost.

AN EXCHANGE USING THE OSI MODEL



LAYERS IN THE OSI MODEL



PHYSICAL LAYER

The physical layer coordinates the functions required to **carry a bit stream over a physical medium**. It deals with the **mechanical and electrical specifications** of the interface and transmission medium.

It also defines the procedures and functions that physical devices and interfaces have to perform for transmission to Occur

The physical layer is also concerned with the following:

1. **Physical characteristics of interfaces and medium**

The physical layer defines the characteristics of the **interface** between the devices and the **transmission medium**. It also defines the type of transmission medium.

- **Physical topology**

The physical topology defines how devices are connected to make a network.

Devices can be connected by using a **mesh** topology, **star** topology, **bus** topology, **ring** topology or **hybrid** topology

- **Transmission mode**

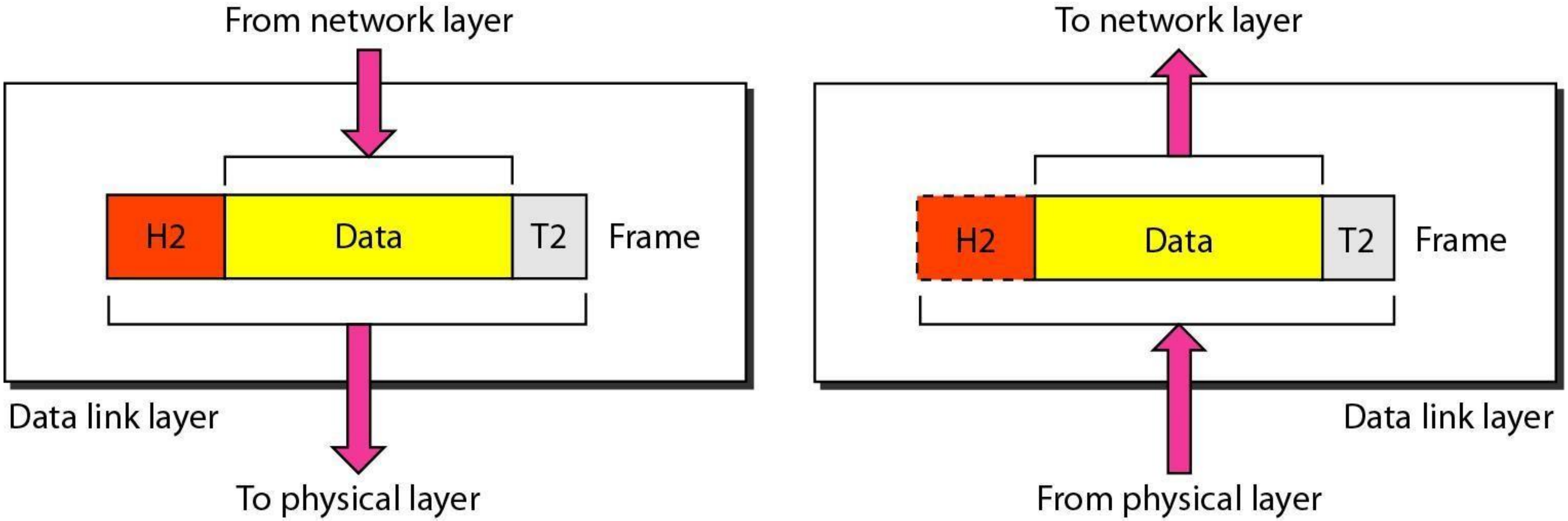
Physical layer defines direction of transmission between to systems

Simplex mode : only one device can send and other can only receive. It is one way communication.

Half duplex mode: Two devices can send and receive but not at the same time

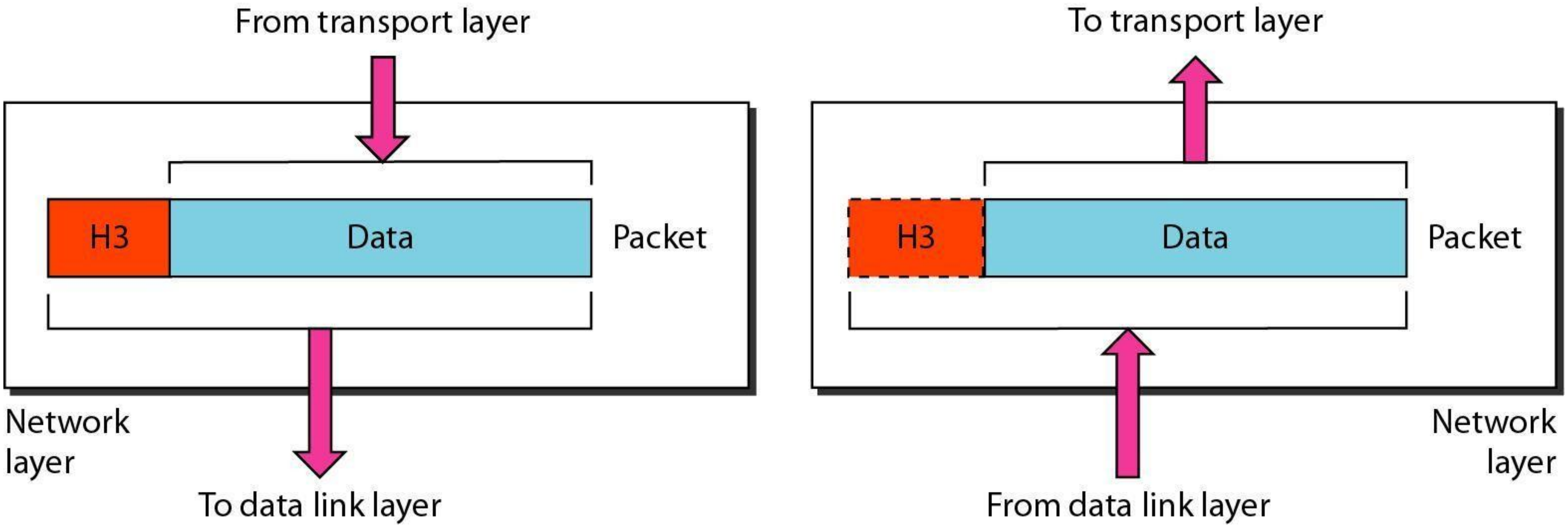
Full duplex mode: Two devices can send and receive at the same time

2. DATA LINK LAYER



The data link layer is responsible for moving frames from one hop (node) to thenext.

3.NETWORK LAYER



The network layer is responsible for the delivery of individual packets from the source host to the destination host.

Network Layer

The network layer is responsible for the source-to-destination delivery of a packet, possibly across multiple networks (links).

Whereas the data link layer oversees the delivery of the packet between two systems on the same network (links), the network layer ensures that each packet gets from its point of origin to its final destination.

If the two systems are attached to different networks (links) with connecting devices between the networks (links), there is often a need for the network layer to accomplish source-to-destination delivery

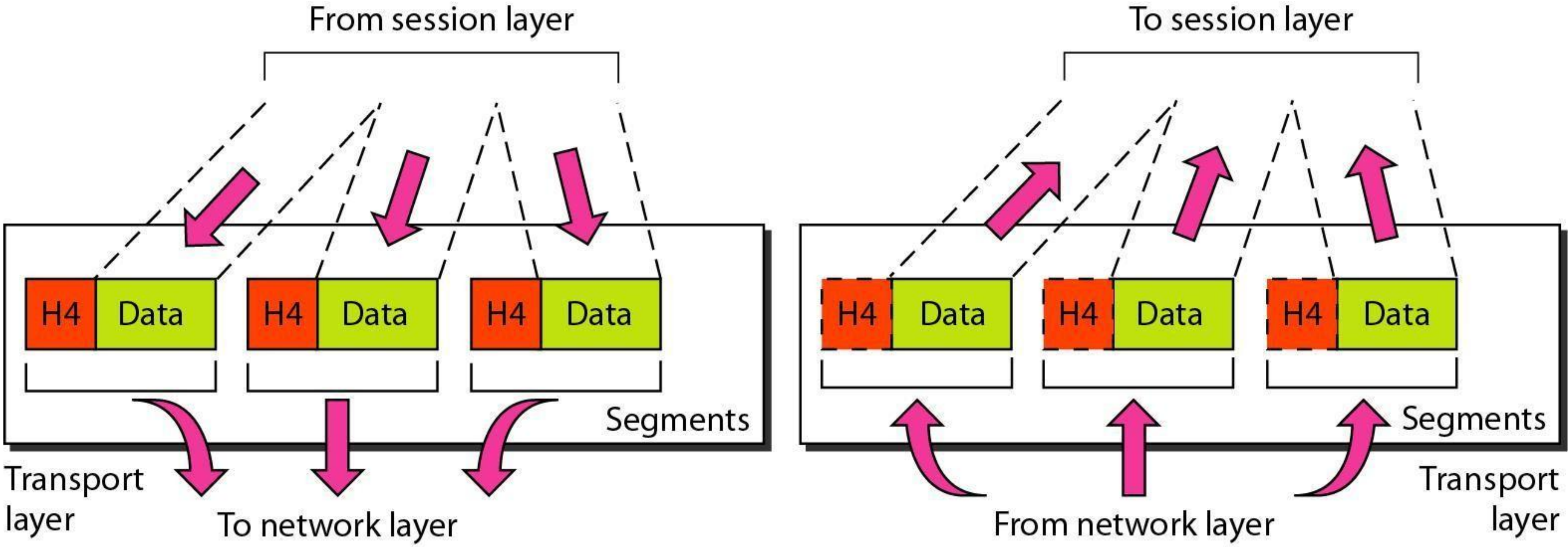
Logical addressing.

The **physical addressing** implemented by the data link layer handles the addressing problem **locally**.

If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems.

The network layer **adds a header** to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.

4 .TRANSPORT LAYER



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

TRANSPORT LAYER

A process is an application program running on a host

The transport layer, on the other hand, ensures that the whole message arrives intact and in order, overseeing both error control and flow control at the source-to-destination level.

Service-point addressing

Computers often run several programs at the same time. For this reason, source to destination delivery means delivery not only from one computer to the next but also from a **specific process** **(**running program) **on one computer to a specific process** (running program) **on the other**

The transport layer header must therefore include a type of address called a service-point address (or port address).

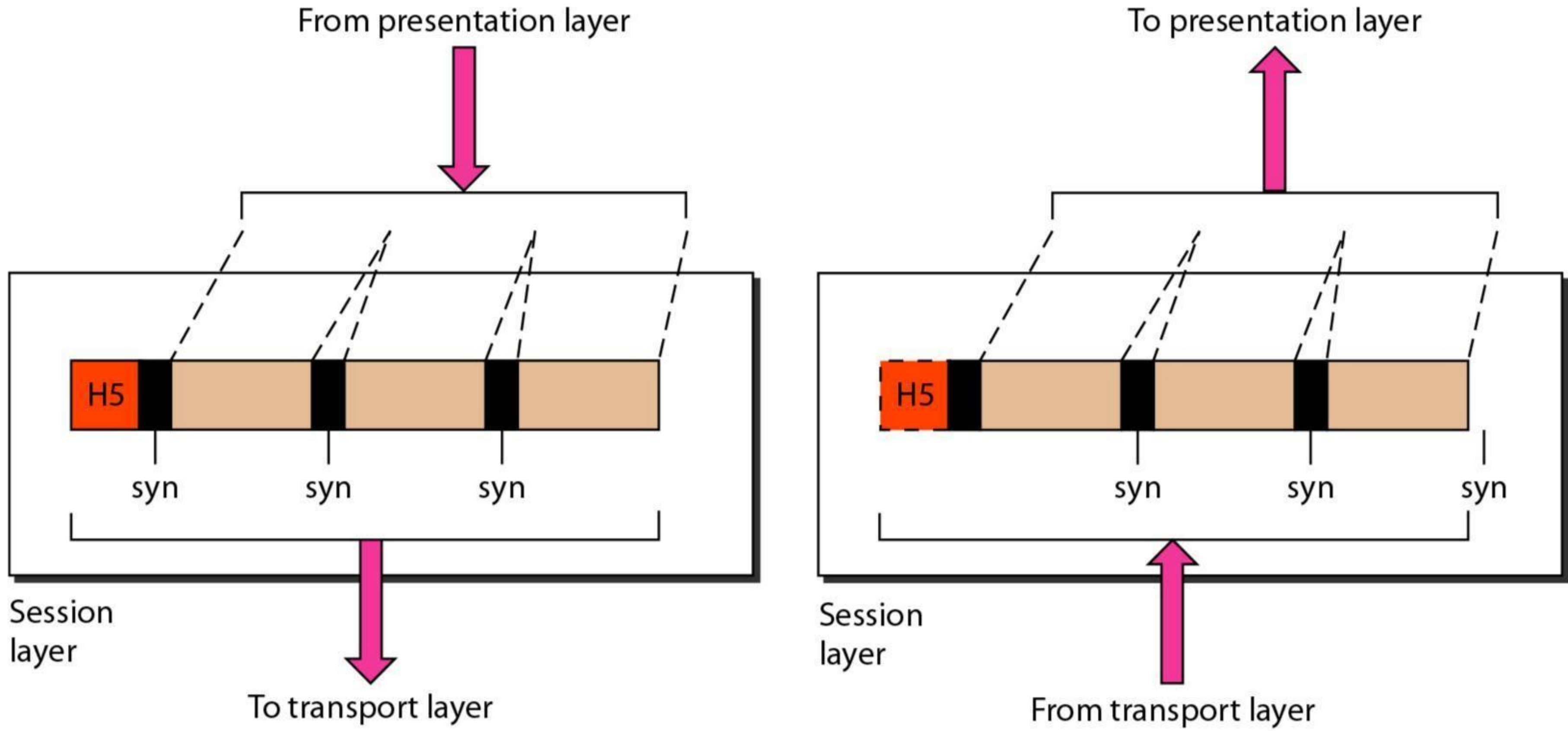
The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer.

Segmentation and reassembly

A message is divided into transmittable **segments**, with each segment containing a **sequence number**

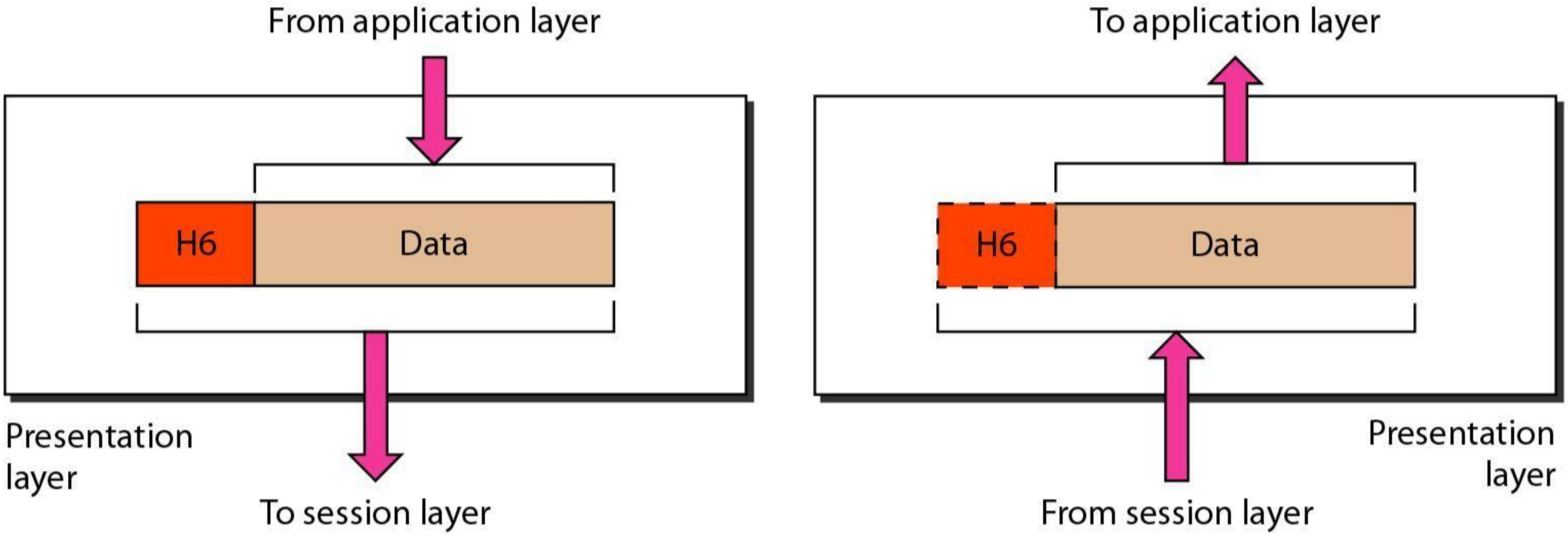
These numbers enable the transport layer to **reassemble** the message correctly upon arriving at the destination and to identify and replace packets that were **lost** in transmission

5. SESSION LAYER



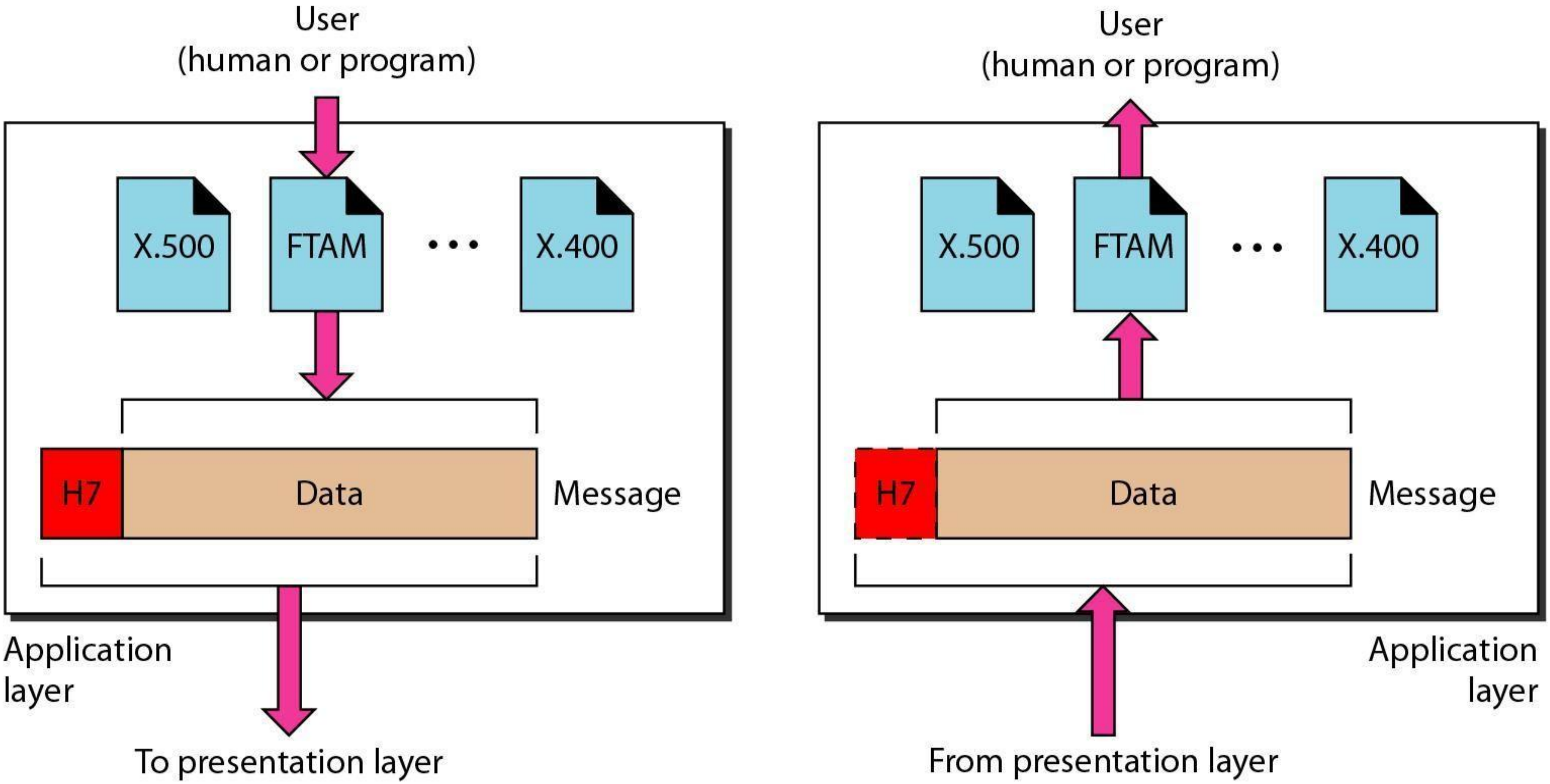
The session layer is responsible for dialog control and synchronization.

6.PRESEANTATION LAYER



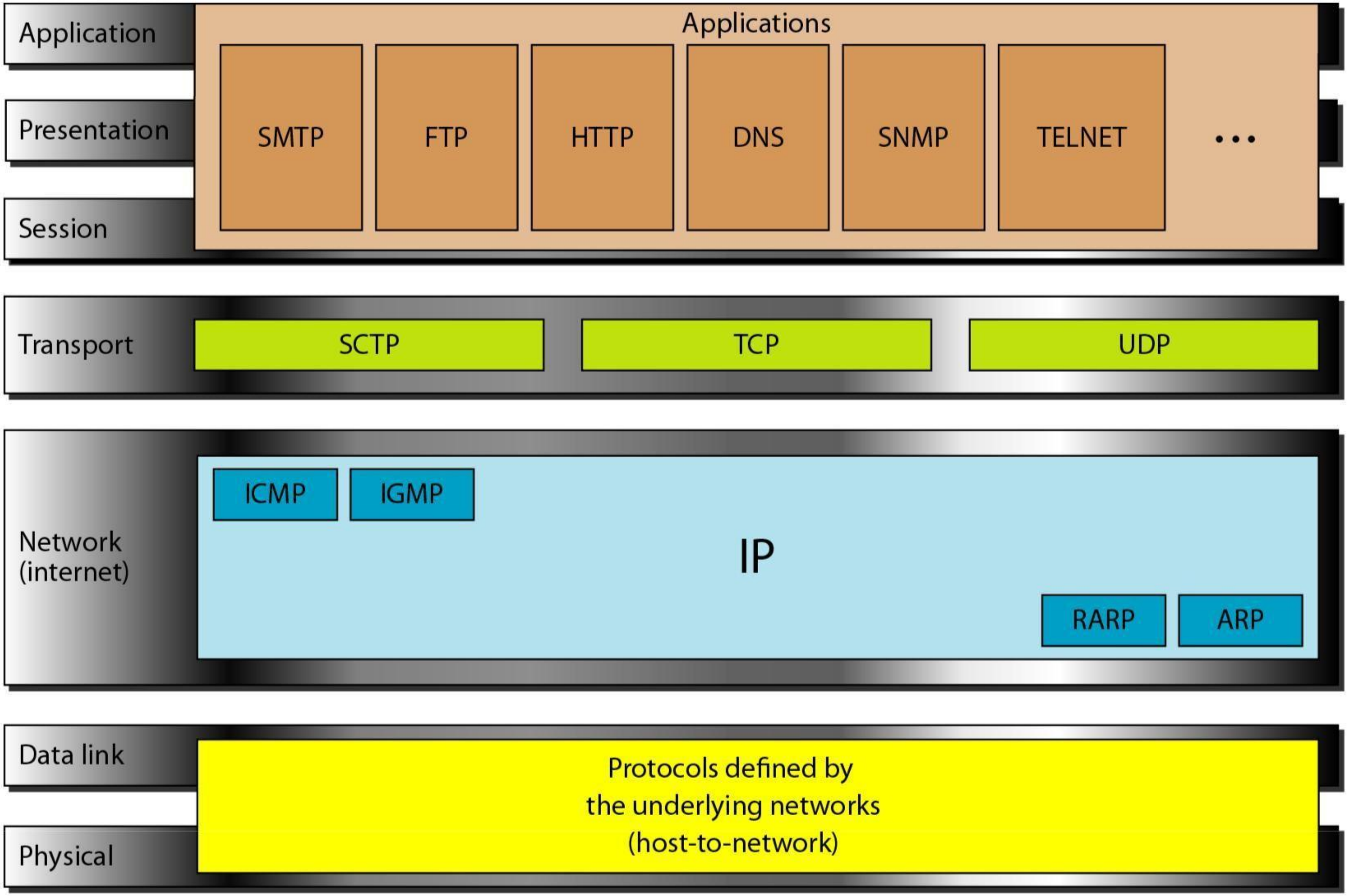
The presentation layer is responsible fortranslation, compression, and encryption.

7.APPLICATION LAYER



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

TCP/IP MODEL


Application
Presentation
Session
Applications
SMTP
FTP
HTTP
DNS
SNMP
TELNET
• • •
Transport
SCTP
TCP
UDP
Network
(internet)
ICMP
IGMP
IP
RARP
ARP
Data link
Physical
Protocols defined by
the underlying networks
(host-to-network)

TCP/IP PROTOCOLSUITE

The original TCP/IP protocol suite was defined as having four layers:

1 Host-to-Network Layer
2 Internet Layer
3 Transport Layer
4 Application Layer

TCPIIP protocol suite is made of five layers:
physical, data link, network, transport, and application.

The first four layers provide physical standards, network interfaces, internetworking, and transport functions that correspond to the first four layers of the OSI model.

Transport Layer

Traditionally the transport layer was represented in TCP/IP by two protocols: TCP and UDP

IP is a host-to-host protocol, meaning that it can deliver a packet from one physical device to another.

UDP and TCP are transport level protocols responsible for delivery of a message from a process (running program) to another process.

A new transport layer protocol, SCTP, has been devised to meet the needs of some newer applications.

User Datagram Protocol(UDP)

The User Datagram Protocol (UDP) is the simpler of the two standard TCP/IP transport protocols.

It is a process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer

Transmission Control Protocol(TCP)

The Transmission Control Protocol (TCP) provides full transport-layer services to applications TCP is a reliable stream transport protocol. A connection must be established between both ends of a transmission before either can transmit data.

At the sending end of each transmission, TCP divides a stream of data into smaller units called segments. Each segment includes a sequence number for reordering after receipt, together with an acknowledgment number for the segments received.

THE INTERNET

A Brief History

1. A network is a group of connected communicating devices such as computersand printers.
2. In the mid-1960s, mainframe computers in research organizations were standalone devices.

3. The Advanced Research Projects Agency (ARPA) in the Department of Defense (DoD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort
4. In 1967, at an Association for Computing Machinery (ACM) meeting, ARPA presented its ideas for ARPANET, a small network of connected computers.

5. In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the Internetting Project. Cerf and Kahn's landmark1973 paper outlined the protocols to achieve end-to-end delivery of packets. This paper on Transmission Control Protocol (TCP) included concepts such as encapsulation, the datagram, and the functions of a gateway.

1. Shortly thereafter, authorities made a decision to split TCP into two protocols: Transmission Control Protocol (TCP) and Internetworking Protocol (lP).. The internetworking protocol became known as TCP/IP

The Internet Today

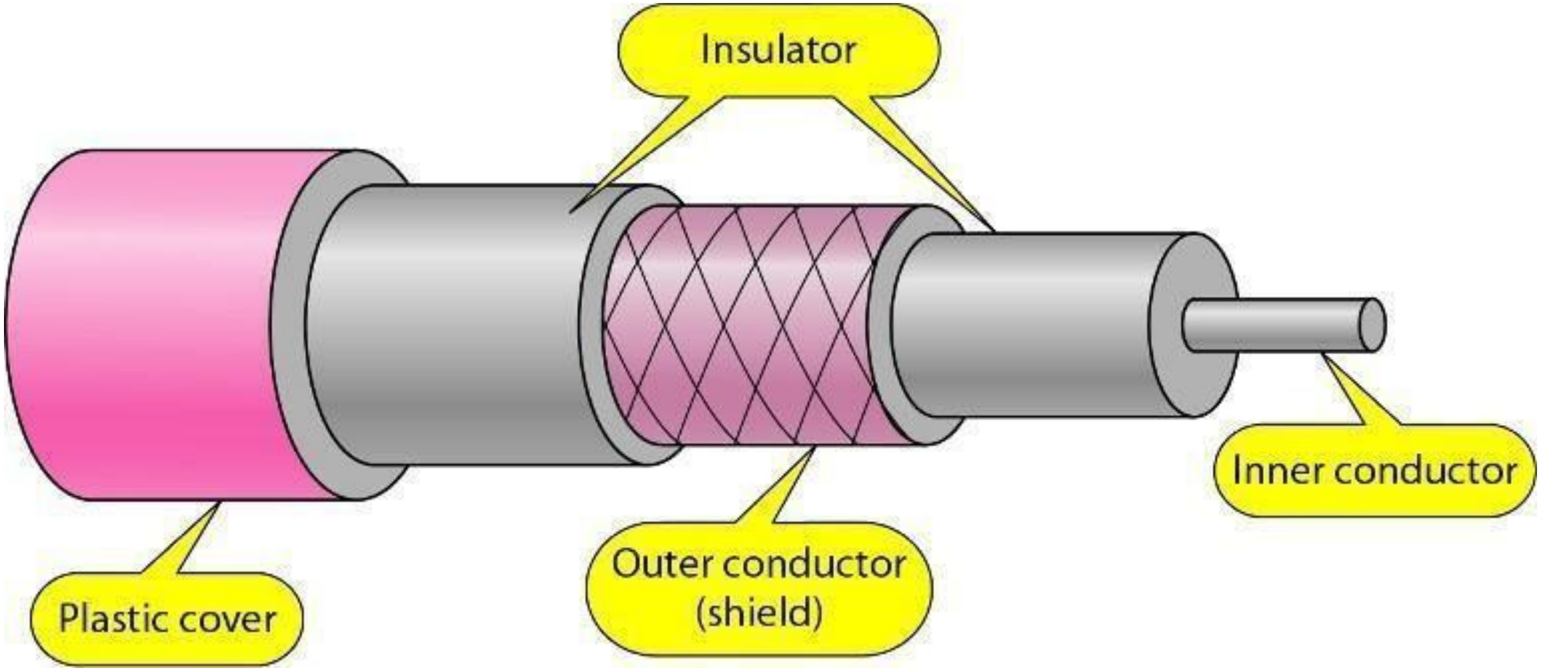
The Internet has come a long way since the 1960s. The Internet today is not a simple hierarchical structure. It is made up of many wide- and local-area networks joined by connecting devices and switching stations.

Today most end users who want Internet connection use the services of Internet service providers (lSPs).
There are

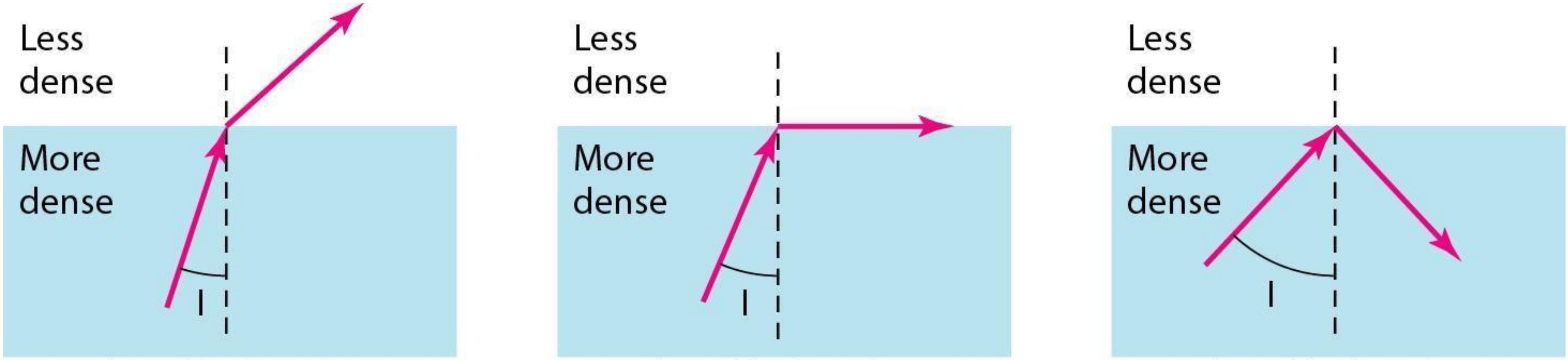
1. international service providers,
2. national service providers,
3. regional service providers
4. local service providers.

.

COAXIAL CABLE



FIBER OPTICS: BENDING OF LIGHT RAY



I < critical angle, refraction

I = critical angle, refraction

I > critical angle, reflection

FIBER-OPTIC CABLE

1. A fiber-optic cable is made of **glass or plastic** andtransmits signals in the form of **light**

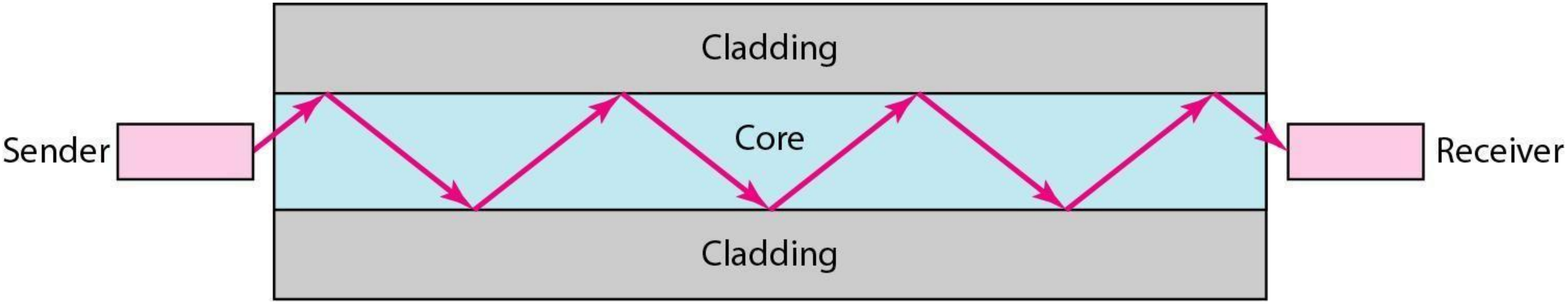
2. Light travels in a straight line as long as it is moving through a single uniform substance

3. if the angle of incidence *I* is **less than** the critical angle, the ray **refracts** and moves **closer to the surface**

4. If the angle of incidence is **equal to** the critical angle, the light **bends along the interface**

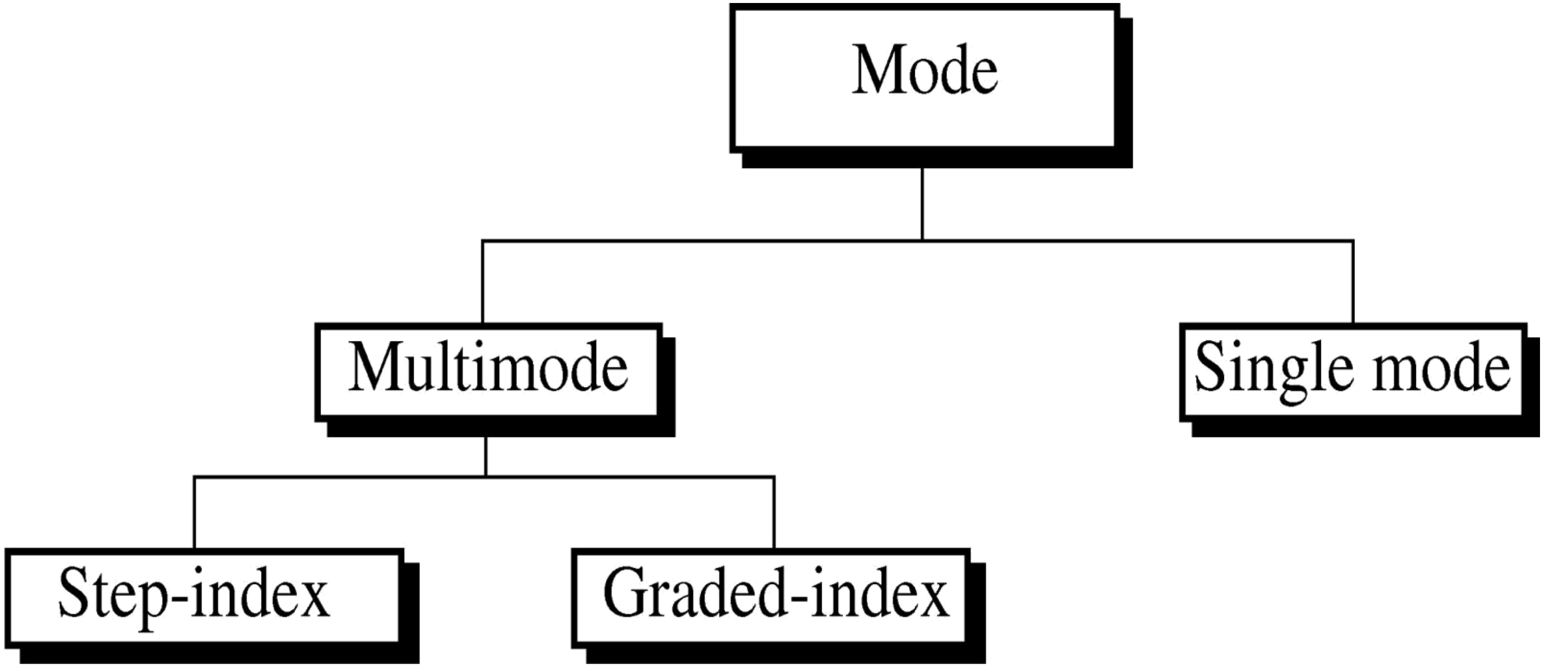
5. If the angle is **greater than the critical angle**, the ray reflects and travels again in the **denser substance**.

OPTICAL FIBER



OPTICAL FIBER

1. Optical fibers use reflection to guide light through a channel
2. . A glass or plastic core is surrounded by a cladding of less dense glass or plastic.
3. The difference in density of the two materials must be such that
4. a beam of light moving through the core is reflected off the cladding instead of being refracted into it



Mode

Multimode

Single mode

Step-index

Graded-index

MULTIMODE

- Multimode is so named because multiple beams from a light source move through the core in different paths

- In multimode step-index fiber, the density of the core remains constant from the center to the edges.

- A beam of light moves through this constant density in a straight line until it reaches the interface of the core and the cladding

- step index refers to the suddenness of this change, which contributes to the distortion of the signal as it passes through the fiber.

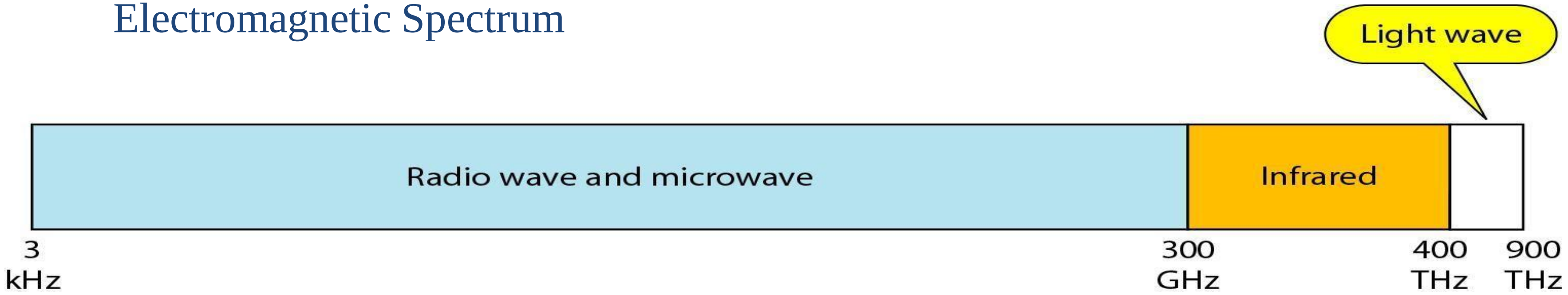
UNGUIDED MEDIA: WIRELESS

1. Unguided media transport electromagnetic waves without using a physical conductor

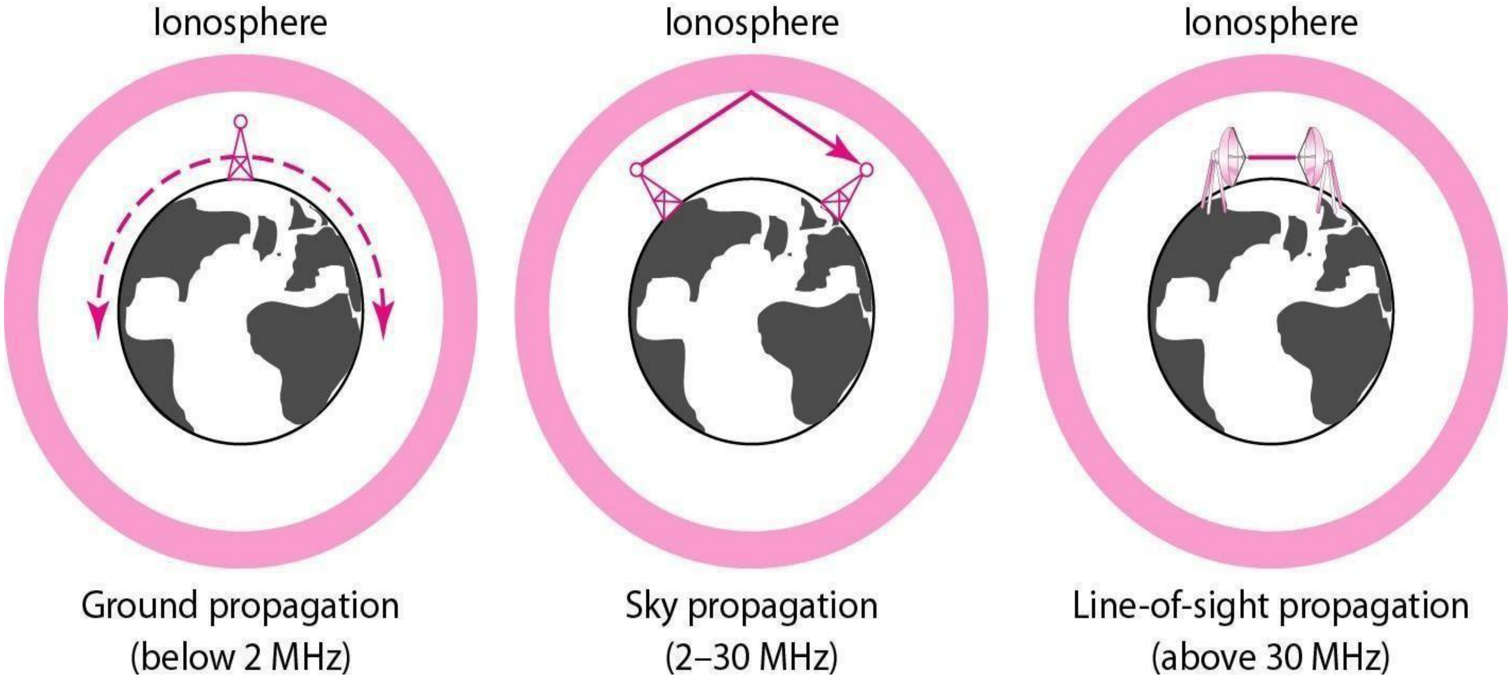
2. This type of communication is often referred to as wireless communication

3. Signals are normally broadcast through free space

Electromagnetic Spectrum

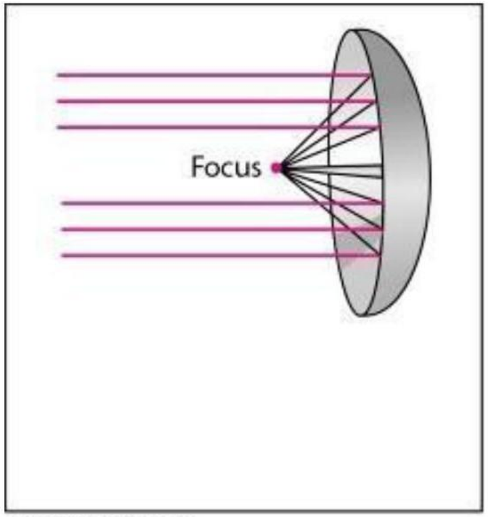


PROPAGATION METHODS

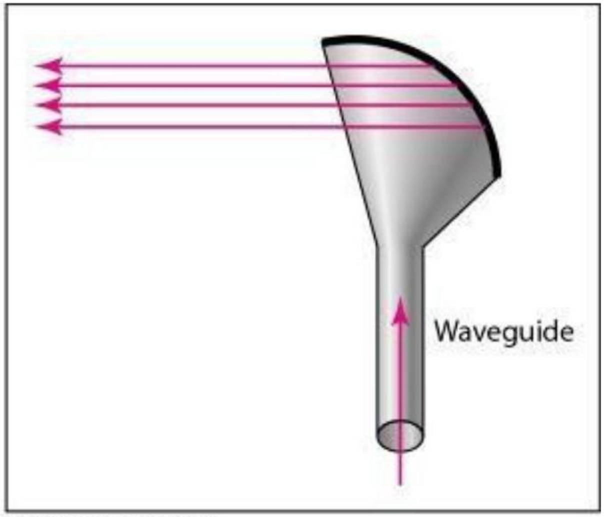


Unguided signals can travel from the source to destination in several ways: ground propagation, sky propagation, and line-of-sight propagation

ANTENNAS



a. Dish antenna

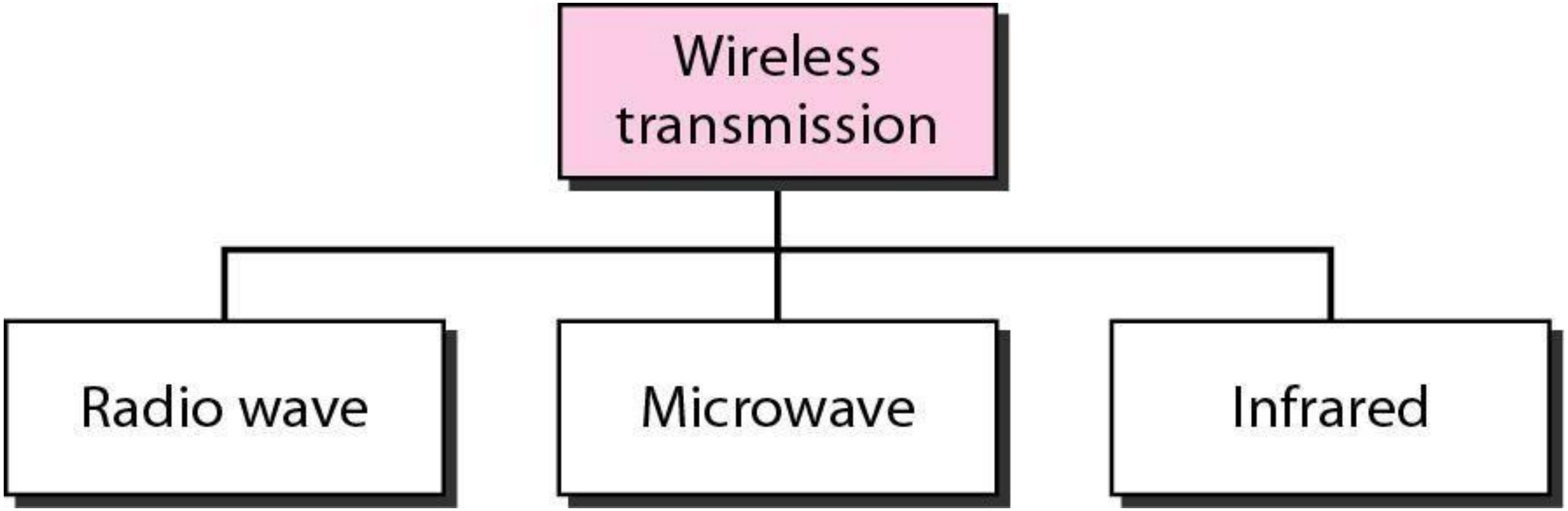


b. Horn antenna

Omni-directional Antenna

Unidirectional Antennas

WIRELESS TRANSMISSION WAVES



used for multicast/broadcast communications, such as radio and television

used for unicast communication such as cellular telephones, satellite networks,
and wireless LANs

used for short-range communication in a closed area using line-of- sight propagation

RADIO WAVES

1. Electromagnetic waves ranging in frequencies between 3 kHz and 1 GHz are called radio waves.

2. Radio waves, for the most part, are omni directional.

3. When an antenna transmits radio waves, they are propagated in all directions

4. The radio waves transmitted by one antenna are susceptible to interference by another antenna that may send signals using the same frequency

5. Radio waves, particularly those of low and medium frequencies, can penetrate walls.

MICROWAVES

1. Electromagnetic waves having frequencies between I and 300 GHz are called microwaves

2. Microwaves are unidirectional.

3. Sending and receiving antennas need to be aligned

4. Microwave propagation is line-of-sight.

5. Very high-frequency microwaves cannot penetrate walls.

INFRARED

1. Infrared waves, with frequencies from 300 GHz to 400 THz can be used for short-range communication

2. Infrared waves, having high frequencies, cannot penetrate walls

Applications

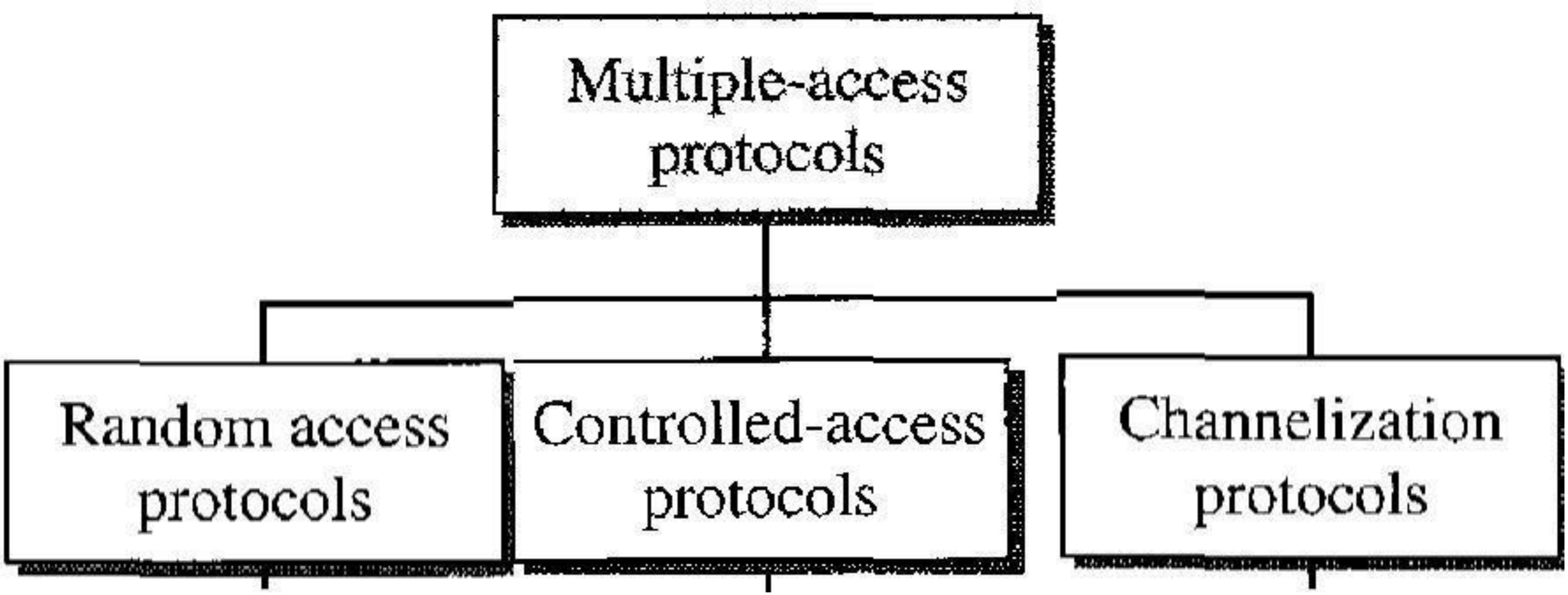
1. Infrared signals can be used for short-range communication in a closed area using line-of-sight propagation.

2. A wireless keyboard to communicate with a PC

UNIT -II

Multiple Access Protocols

TAXONOMY OF MULTIPLE-ACCESS PROTOCOLS



ALOHA
CSMA
CSMA/CD

Reservation
Polling
Token passing

FDMA
TDMA
CDMA

MULTIPLE ACCESS

1. When nodes or stations are connected and use a common link, called a multipoint or broadcast link,we need a multiple-access protocol to coordinate access to the link.

2. The problem of controlling the access to the medium is similar to the rules of speaking in an assembly.

3. The procedures guarantee that the right to speak is upheld and ensure that :
   1. Two people do not speak at the same time
   2. do not interrupt each other
   3. do not monopolize the discussion, and so on.

RANDOM ACCESS

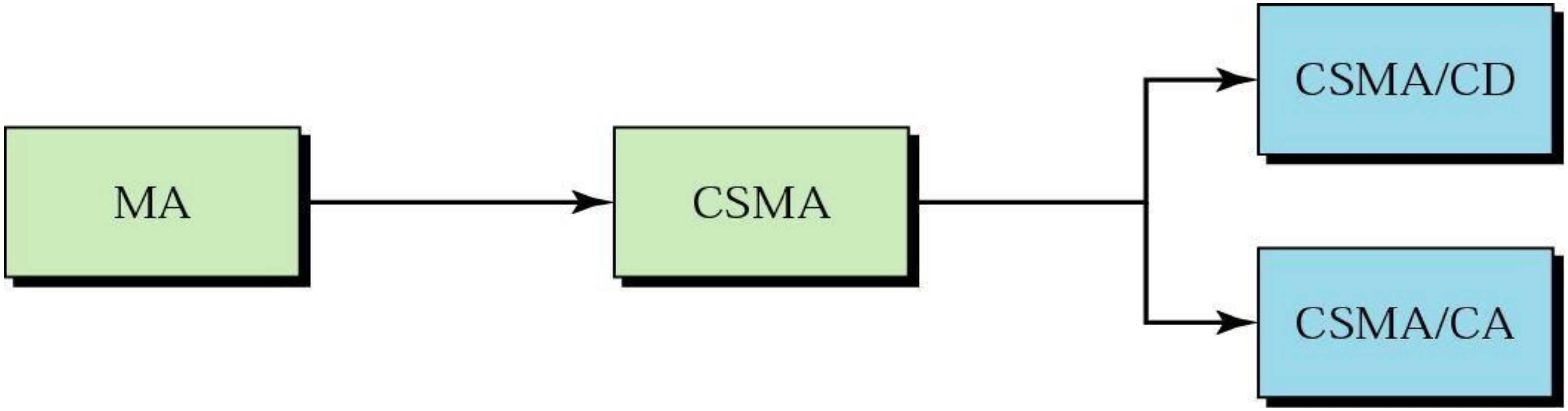
1. In random accessor contention methods, no station is superior to another station and none is assigned the control over another.

2. No station permits, or does not permit, another station to send.

3. At each instance, a station that has data to send uses a procedure defined by the protocol to make a decision on whether or not to send.

4. This decision depends on the state of the medium (idle or busy)

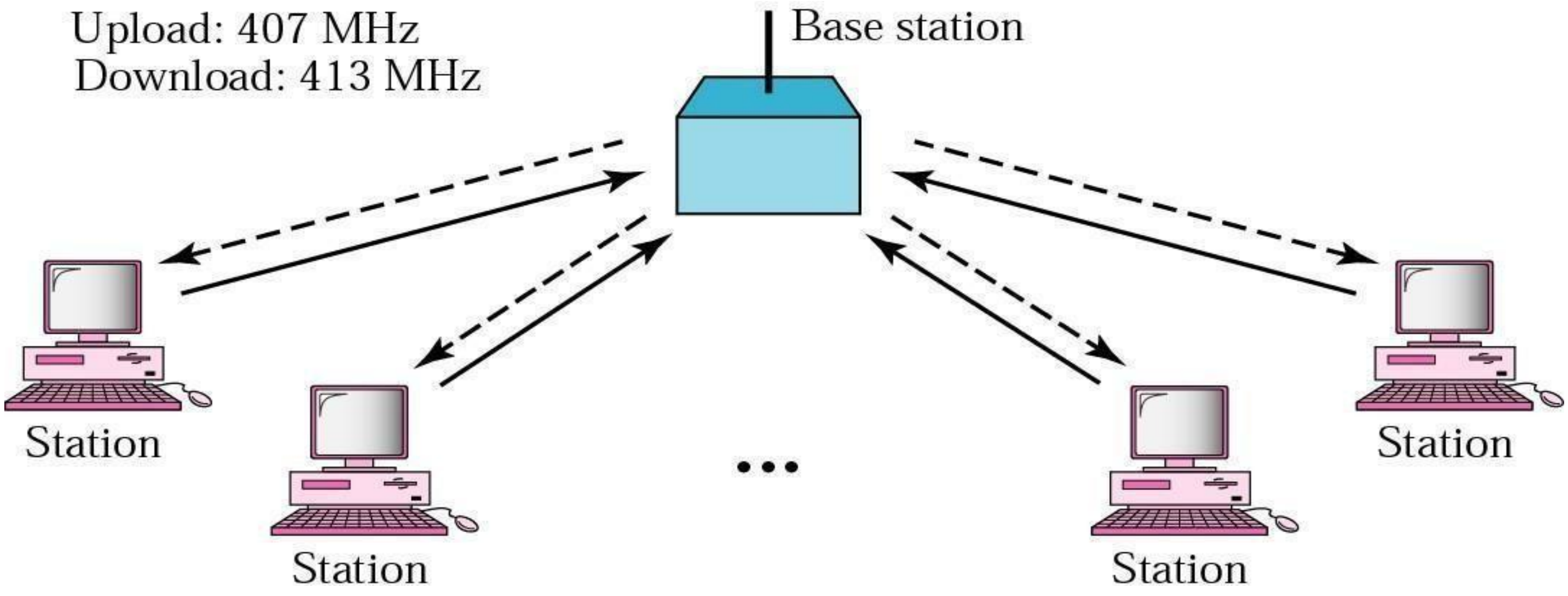
EVOLUTION OF RANDOM-ACCESS METHODS



PURE ALOHA

1. ALOHA was developed in 1970.it was designed for a radio LAN,but it cannot b used on any sharedmedium.
2. Pure aloha: original aloha
3. Idea is that each stn sends frame when ever it has frame to send.
4. Only one channel to share there is possibility of collision btw frames from different stations.
5. Pure aloha relies on ack from receiver.if ack does not arrive aftertime out period stn resends the frame.
6. If all stns try to resend their frames after time out,frames collide again.pure aloha dictates that when timeout period passes ,each stn waits for random amount of time bfore resending the frame.this time is called back off time .

ALOHA NETWORK



PROCEDURE FOR ALOHA PROTOCOL

K: Number of attempts

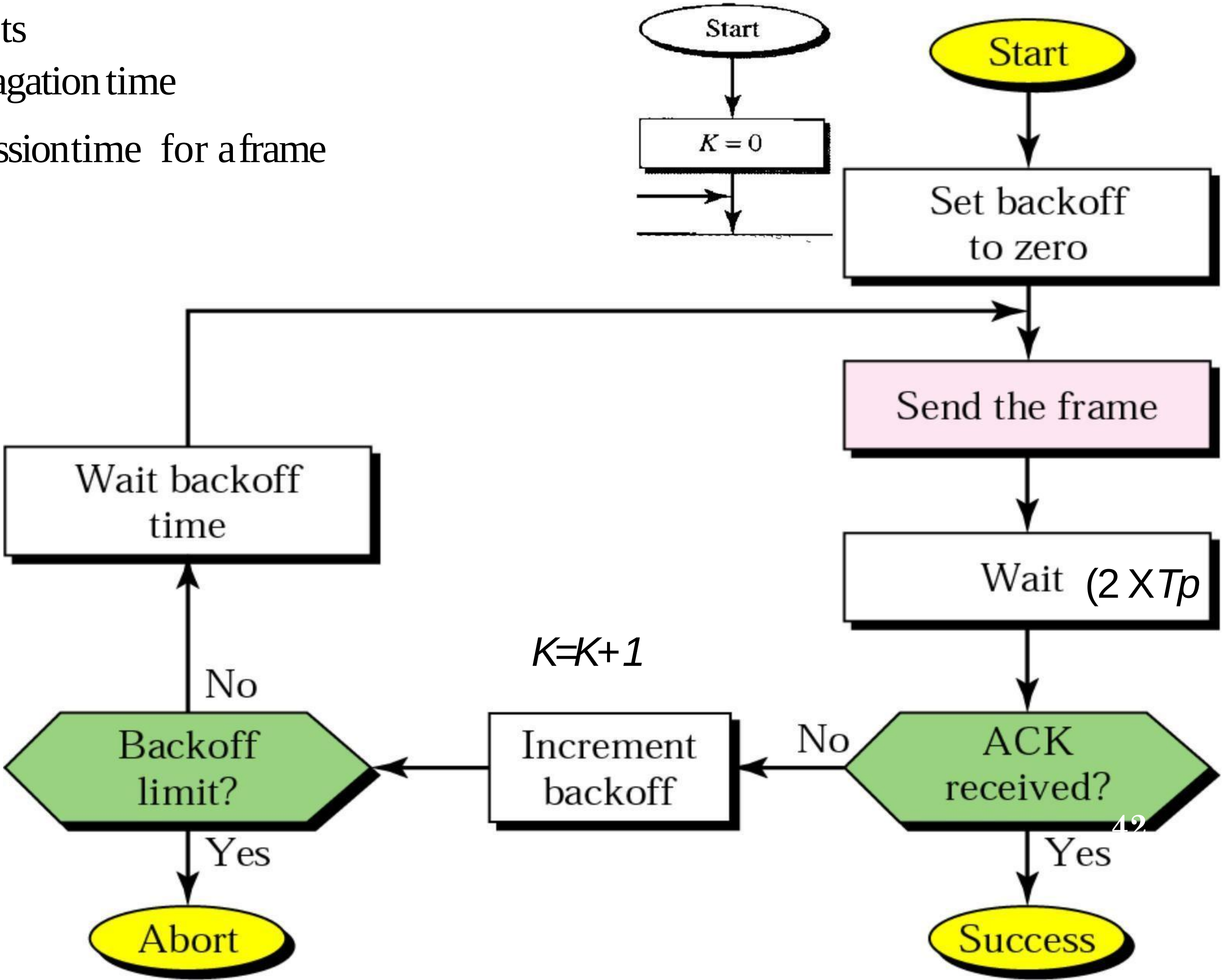
Tp: Maximum propagation time

Tfr : Average transmission time for a frame

TB: Back-off time

(Ta=R x Tp or R x Tfr

Kma, is normally 15

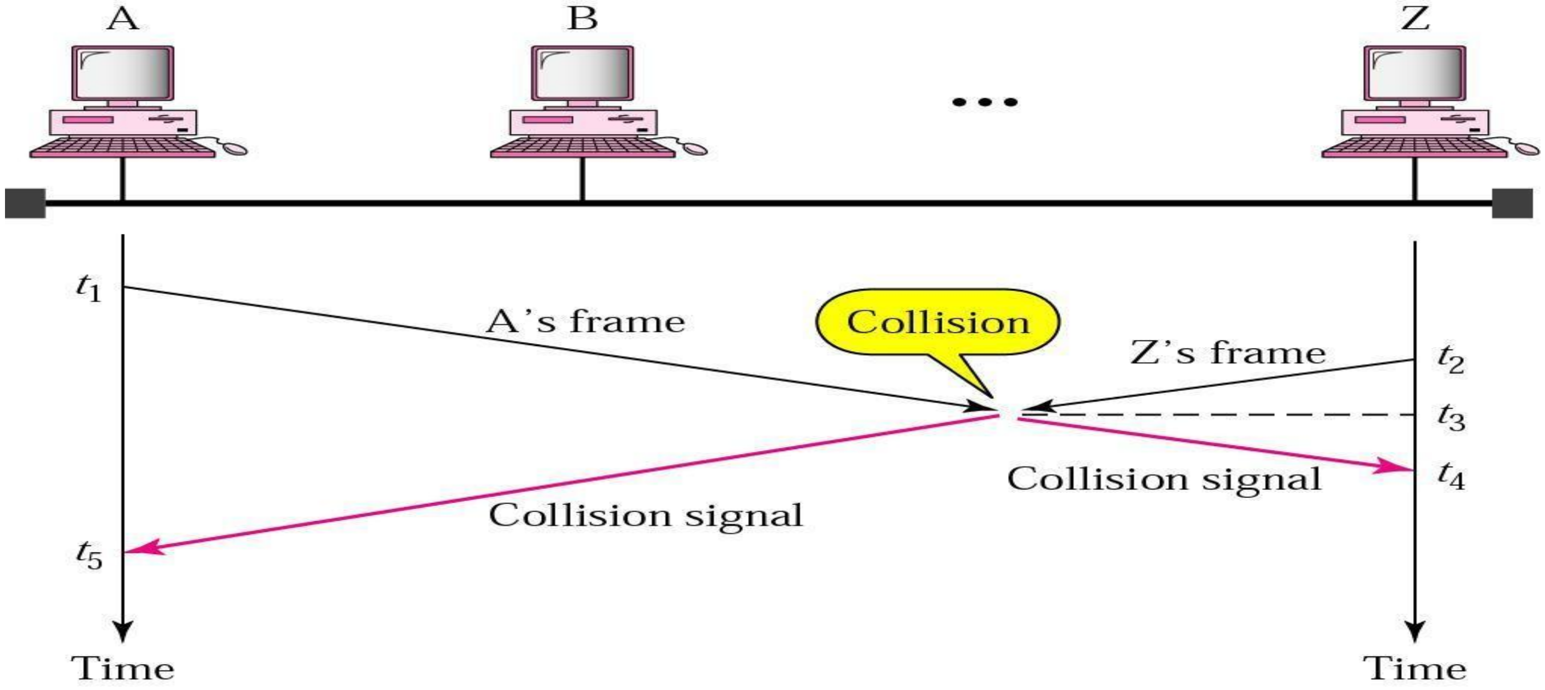


SLOTTED ALOHA

1. Slotted aloha : was invented to improve the efficiency of pure aloha.
2. here we divide the time into slots t_{fr} s and force the station to send only at the beginning of time slot.
3. Here if station misses to send at beginning of time slot it has to wait till next time slot.
4. But 2 or more stations try to send at same time slot, collision occurs.

CSMA(CARRIER SENSE MULTIPLE ACCESS)

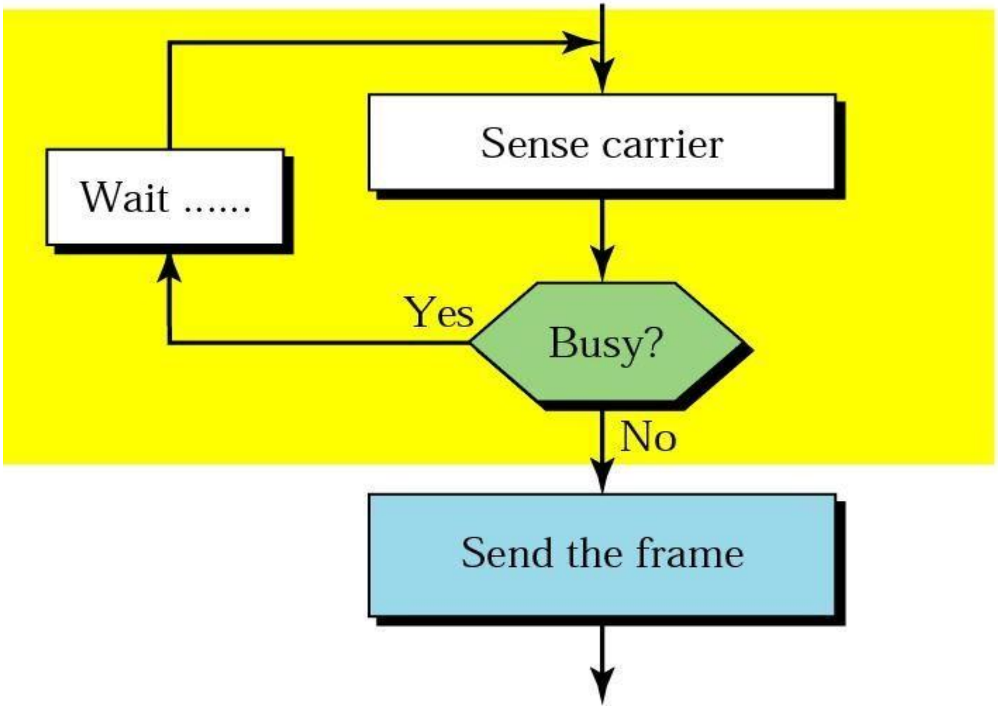
1. In CSMA every station must first listen to the medium before sending.
2. **principle:** sense before transmit or listen before talk.
3. It can reduce the possibility of collision but cannot avoid it because of propagation delay.
4. To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed.



Collision in CSMA

PERSISTENCE STRATEGIES

Nonpersistent strategy



Sense carrier

Wait ......

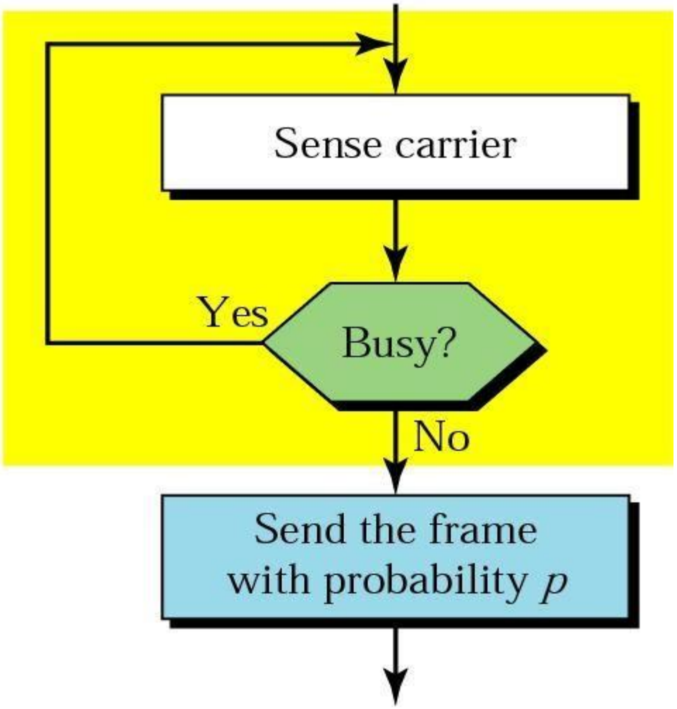
Busy?

Yes

No

Send the frame

Persistent strategy



Sense carrier

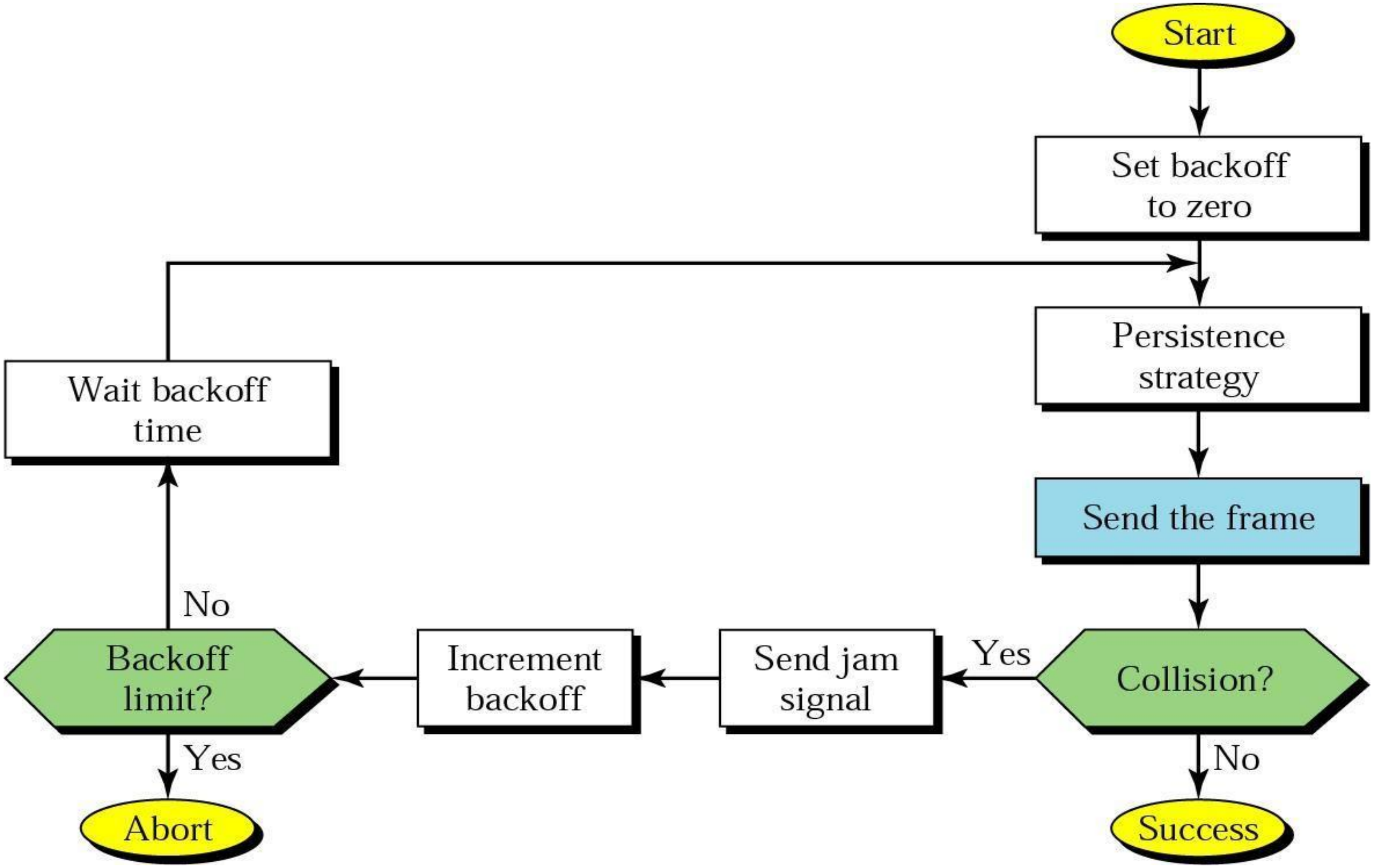
Busy?

Yes

No

Send the frame with probability *p*

CSMA/CD PROCEDURE

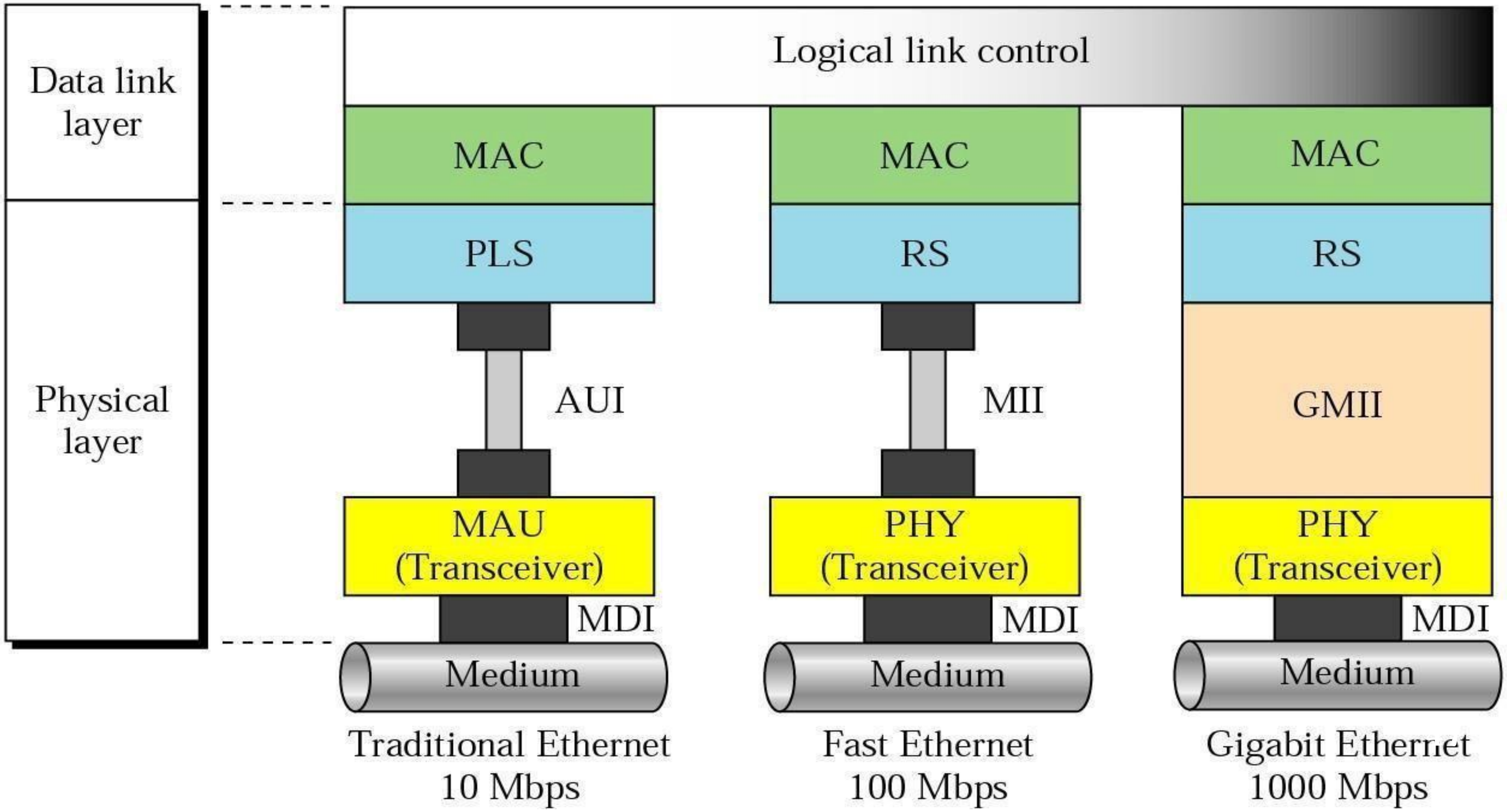


THREE GENERATIONS OF ETHERNET

AUI: Attachment Unit Interface
MAC: Media Access Control
MAU: Medium Attachment Unit

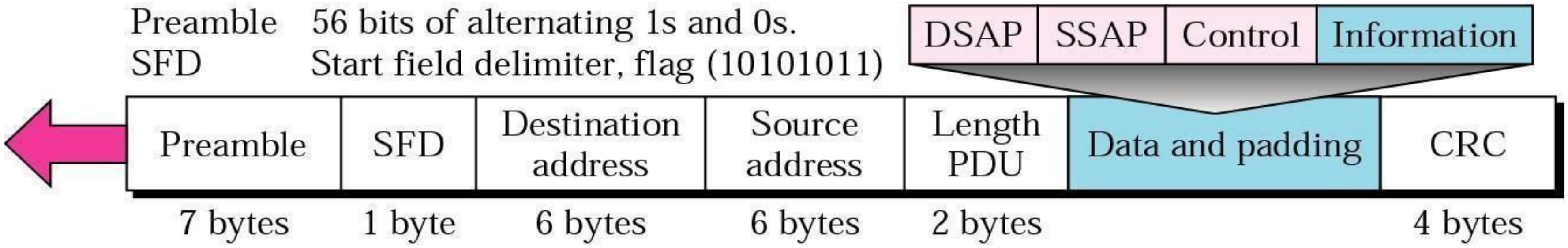
MDI: Medium-Dependent Interface
MII: Medium-Independent Interface
GMII: Gigabit Medium-Independent Interface

PHY: Physical Layer Entity
PLS: Physical Layer Signaling
RS: Reconciliation Signaling



802.3 MAC FRAME

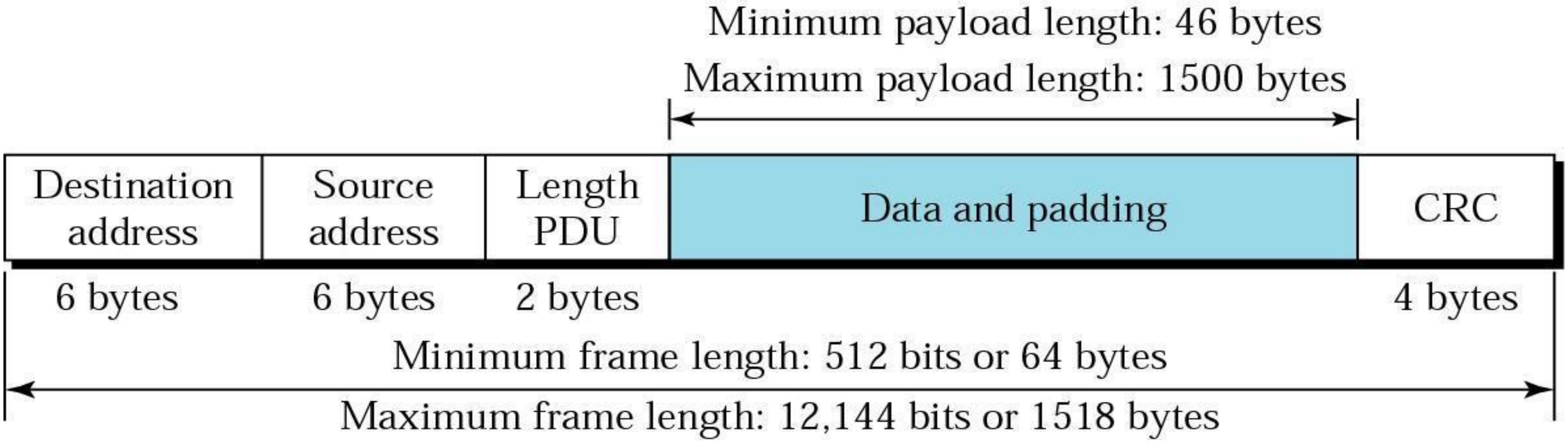
1. Preamble:it alerts the receiver to coming frame and enables synchronization.it is added at physical layer
2. Sfd:signals beginning of frame.sfd warns stns that this is last chance for sync.the last bits 11 alerts the recvr that next field is destination address.



1. Data:minimum 46 and maximum 1500bytes
2. Crc: crc-32 is used
3. Dsap:destination service access point.

MINIMUM AND MAXIMUM LENGTH

1. Min length restriction is req for correct opn of csma/cd.of 64 bytes,header and trailer length is 18 bytes.so data 46bytes
2. Max length is 1518,of which header and trailer length is 18 bytes.so data 1500 bytes



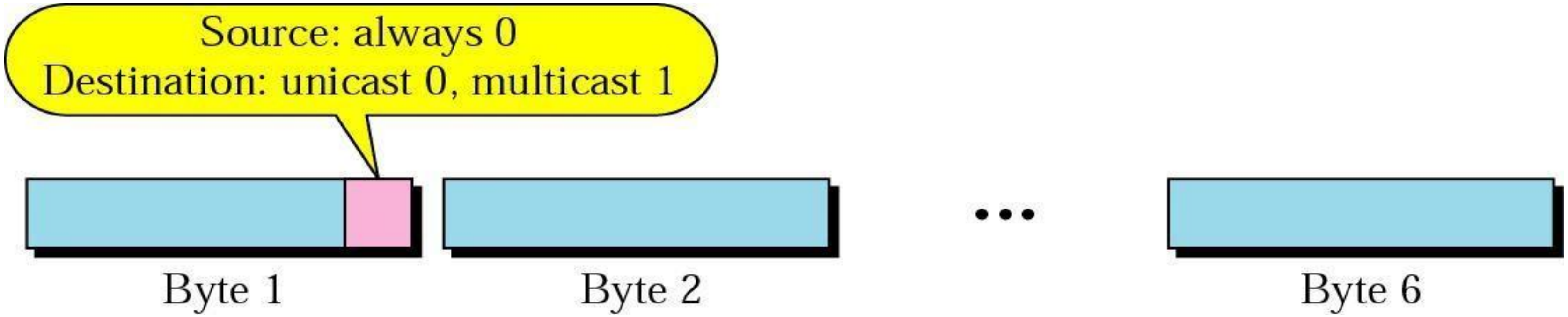
Minimum payload length: 46 bytes
Maximum payload length: 1500 bytes
Destination address
Source address
Length PDU
Data and padding
CRC
6 bytes
6 bytes
2 bytes
4 bytes
Minimum frame length: 512 bits or 64 bytes
Maximum frame length: 12,144 bits or 1518 bytes

1. Max restriction bcoz memory was expensive and it prevents 1 stn from monopolizing shared medium,blocking other stns that have datatosend.

ETHERNET ADDRESSES IN HEXADECIMAL NOTATION

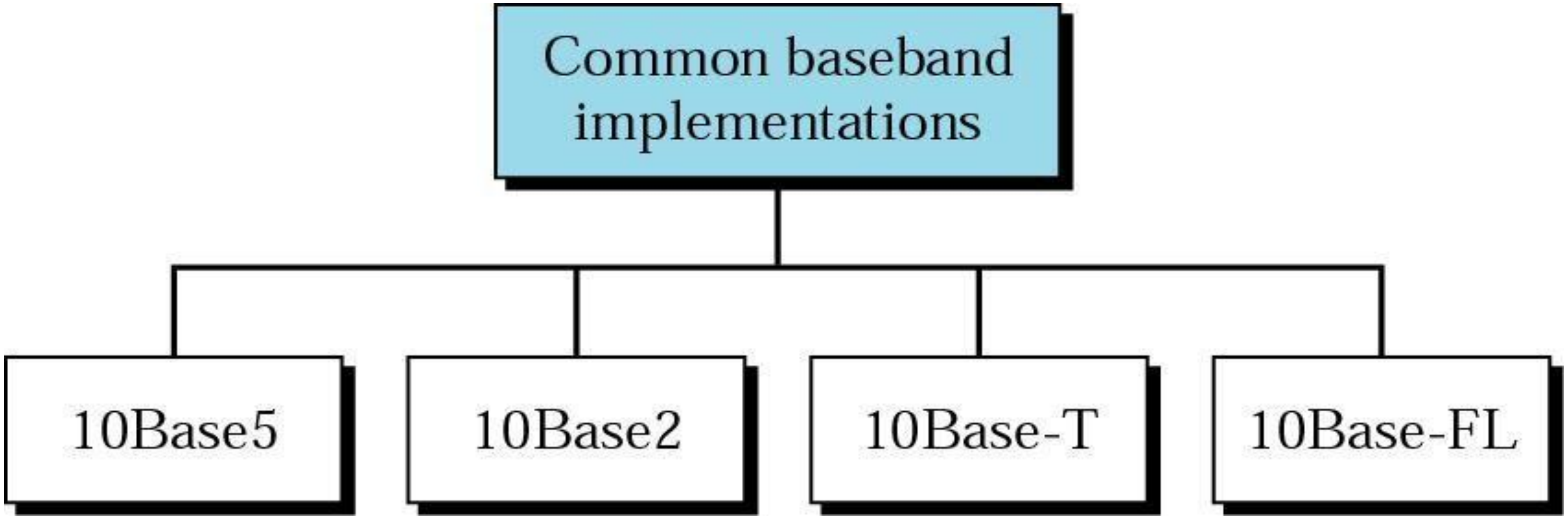
1. Each stn on ehternet n/w has n/w interface card.(NIC).nic fits inside the stn and provides the stn with 6 byte physical address.
2. In unicast dest address defines only 1 recepient,multicast defines group of adresses,broadcast are all stns on lan.its address is481s.

06-01-02-01-2C-4B



CATEGORIES OF TRADITIONAL ETHERNET

1. All standard implementations use digital signaling at 10 mbps.at sender data are converted to digital signal using manchesterscheme

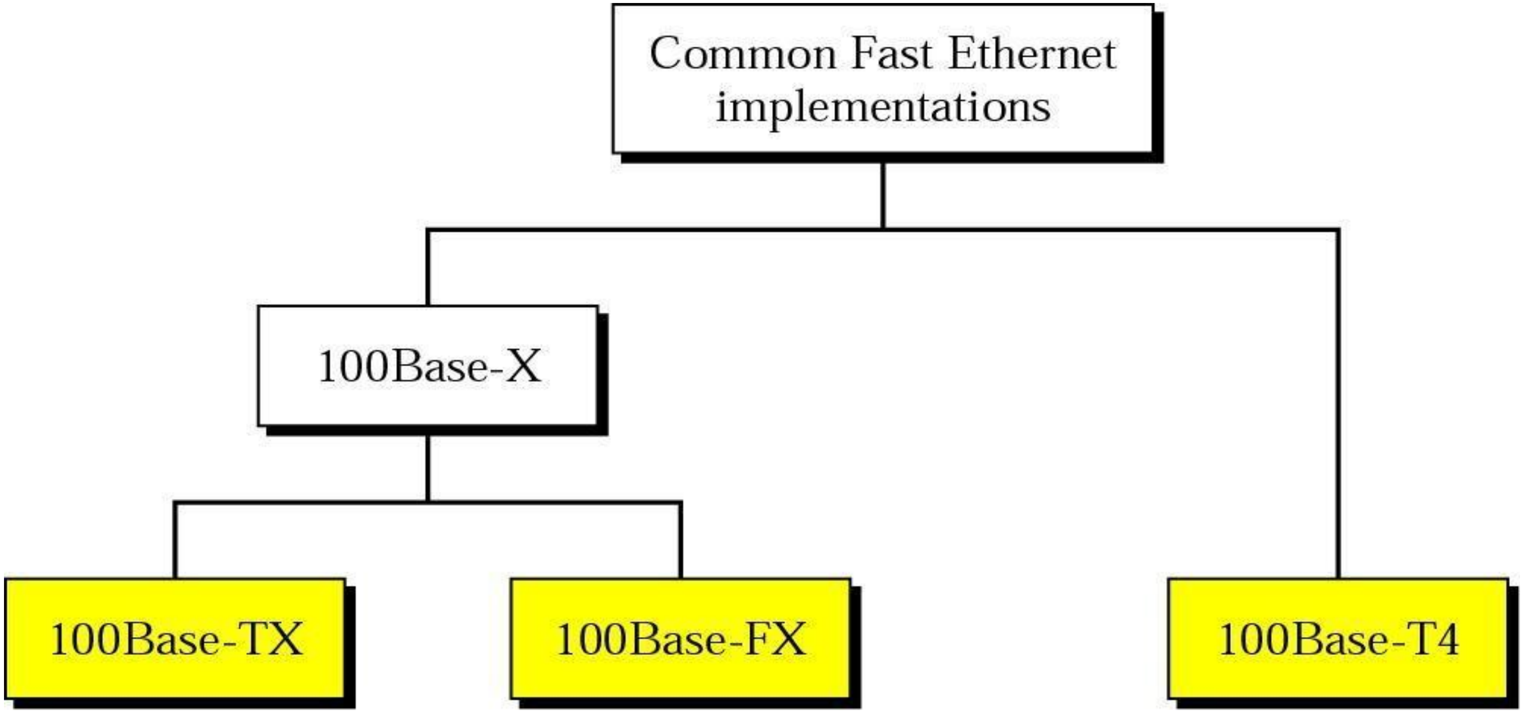


1. Bus,thick coaxial bus,thin coaxial star,utp star,fiber

FAST ETHERNET PHYSICAL LAYER

1. It is designed to compete with lan protocols such as fddi or fiber channel.it is backward compatible with stndEthernet T
2. **<u>Goals:</u>** 1)upgrade the datarate to 100mbps
3. 2) compatible with stnd Ethernet.
4. 3)keep same 48 bit address.
5. 4)keep same frame format.
6. 5)keep same min and max lengths.
7. **<u>Mac sublayer</u>**
8. Keep mac layer untouched,but drop bus topology and consider star topology-half & full duplex.in half duplex,stns r connected via hub and acess mthd is csma/cd.in full duplex,connection is made via switch with buffers at each port no need of acess mthd as csma/cd.
9. <u>Autonegotiation:</u> it allows a stn or a hub a range of capabilities.it allows 2 devices to negotiate the mode r data rate of opn.

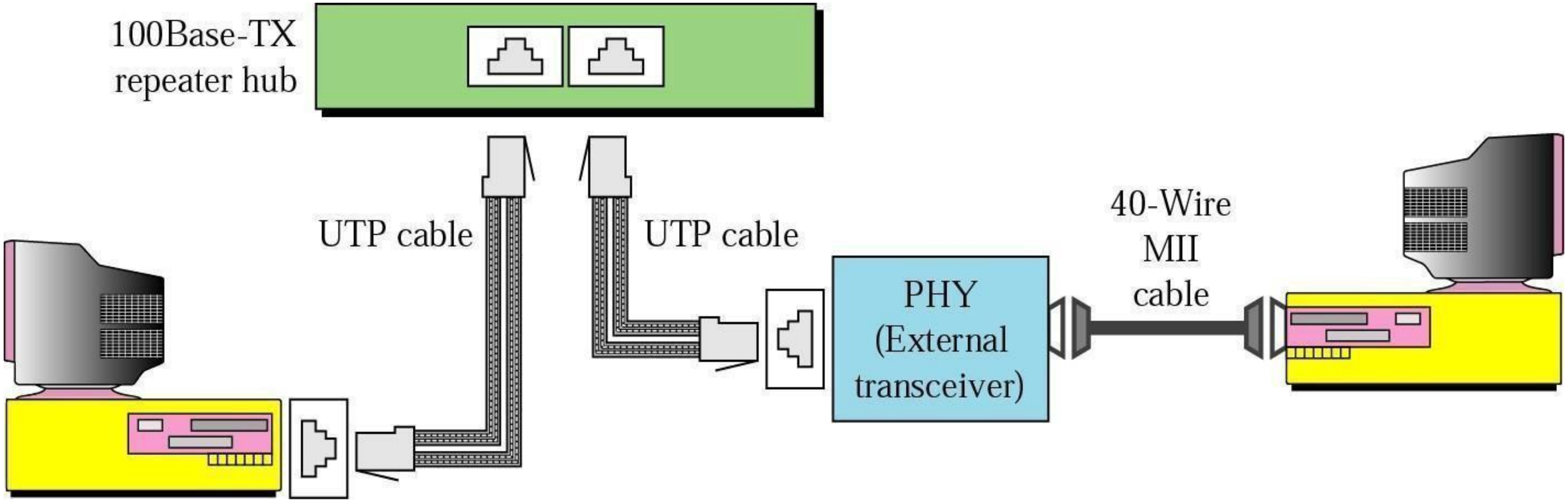
FAST ETHERNET IMPLEMENTATIONS



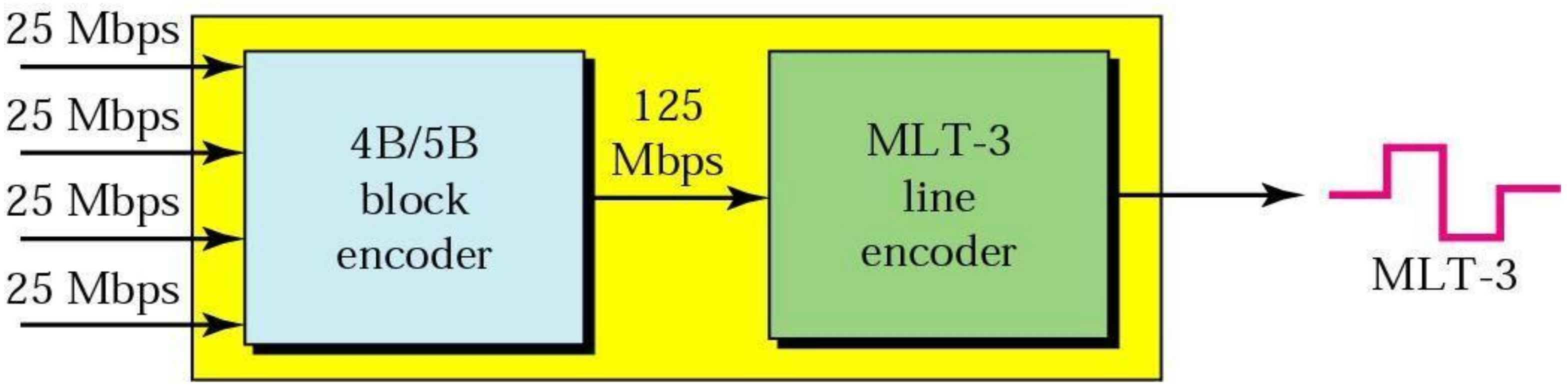
- 2 wires category 5 UTP 2 wires,fiber 4 wires category 3 UTP

100BASE-TX IMPLEMENTATION

1. It uses 2 pairs oftwisted pair cables.
2. It uses mlt3 scheme since it has good performance.since mlt3 is not self synchronous,4B/5B encoding is uesd for bit synchronization by prventing long sequence of 0’s and 1’s.this crates a datarate of 125 mbps,which is fed into mlt3 forencoding

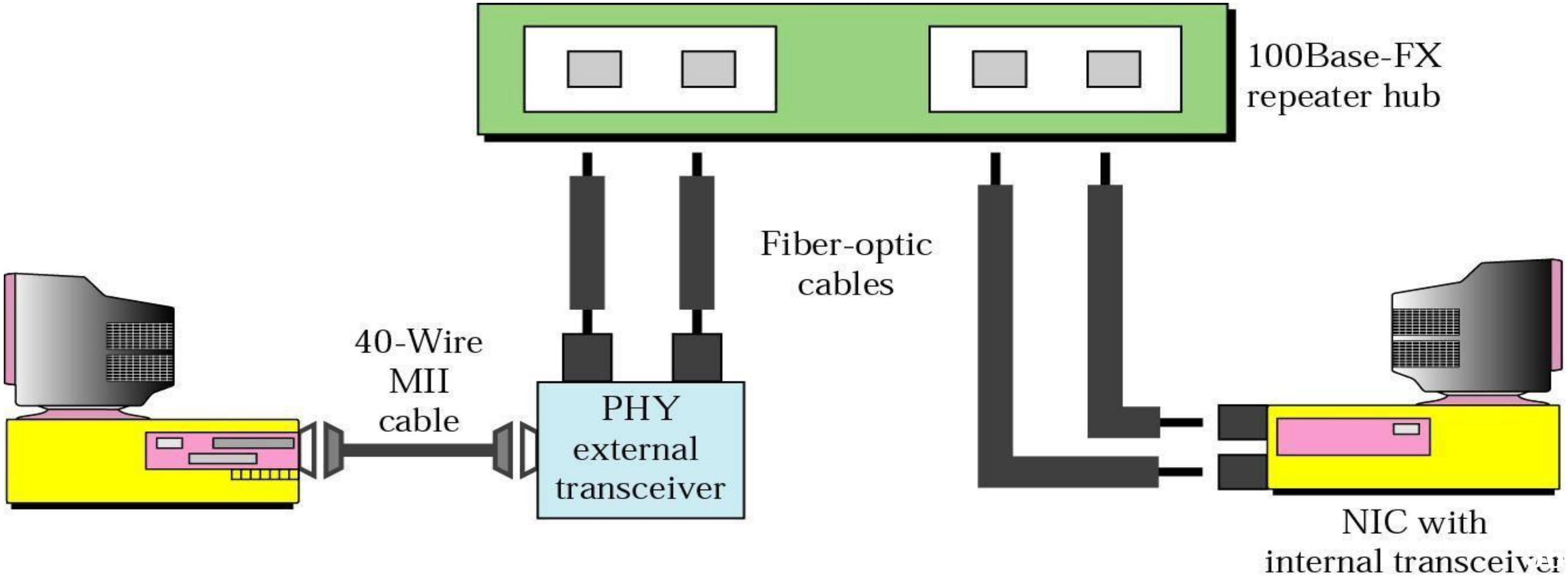


ENCODING AND DECODING IN 100BASE-TX

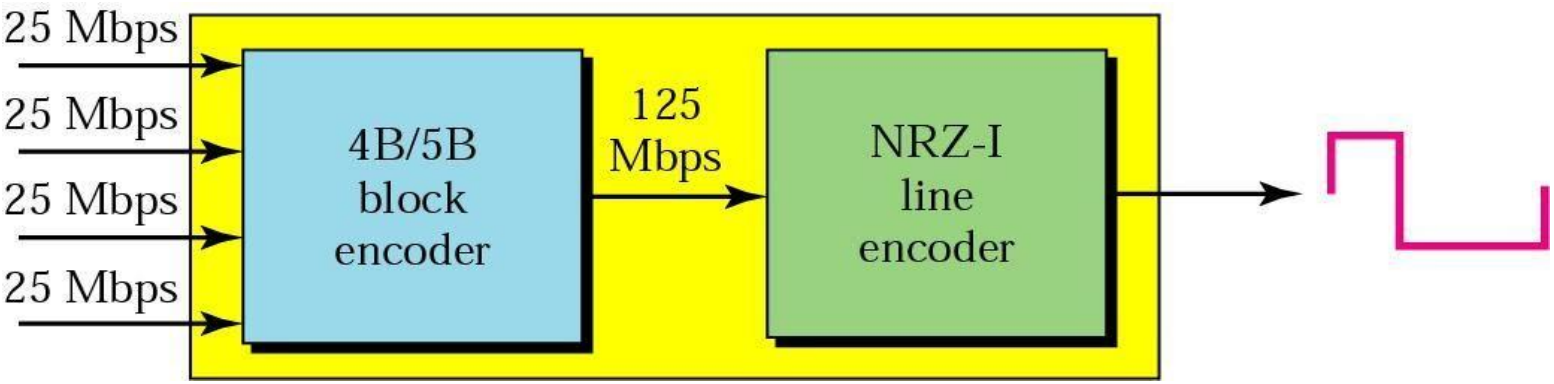


100BASE-FX IMPLEMENTATION

1. It uses 2 pairs of fiber optic cables. fiber optic cables can easily handle high bandwidth requirements by usingencodingschemes.
2. Nrz-I has bit synchronization prblm for long seq of 0’s.designers use 4b/5b block encoding.

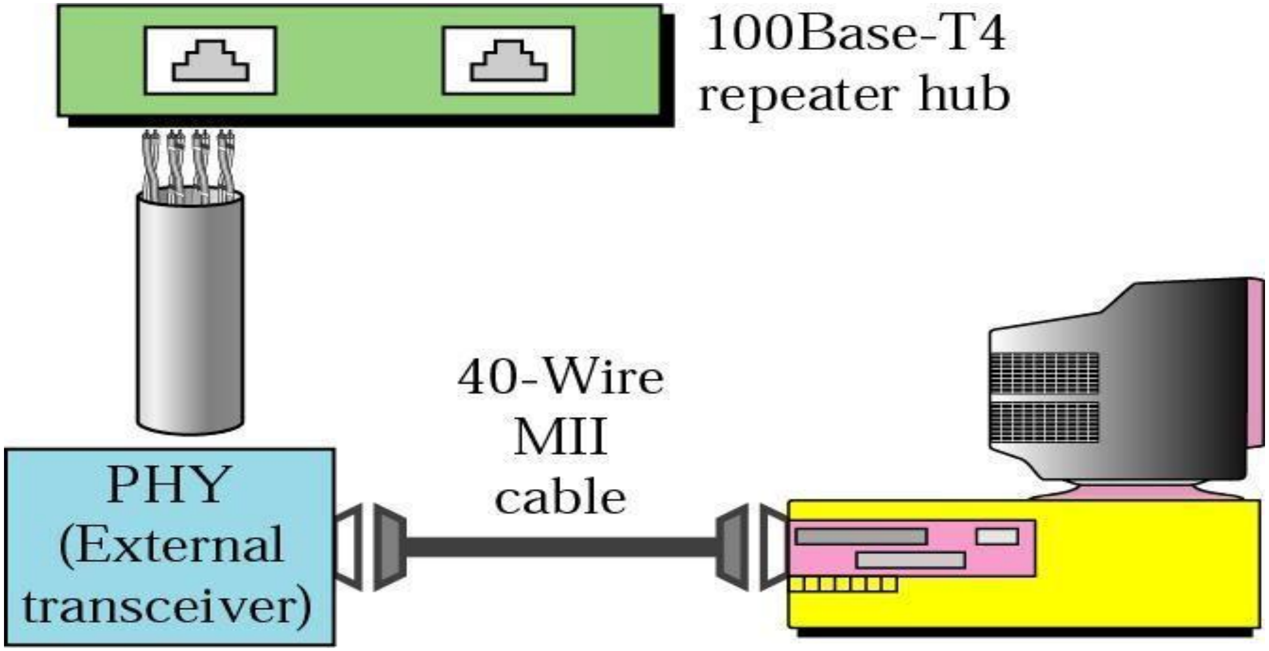


ENCODING AND DECODING IN 100BASE-FX

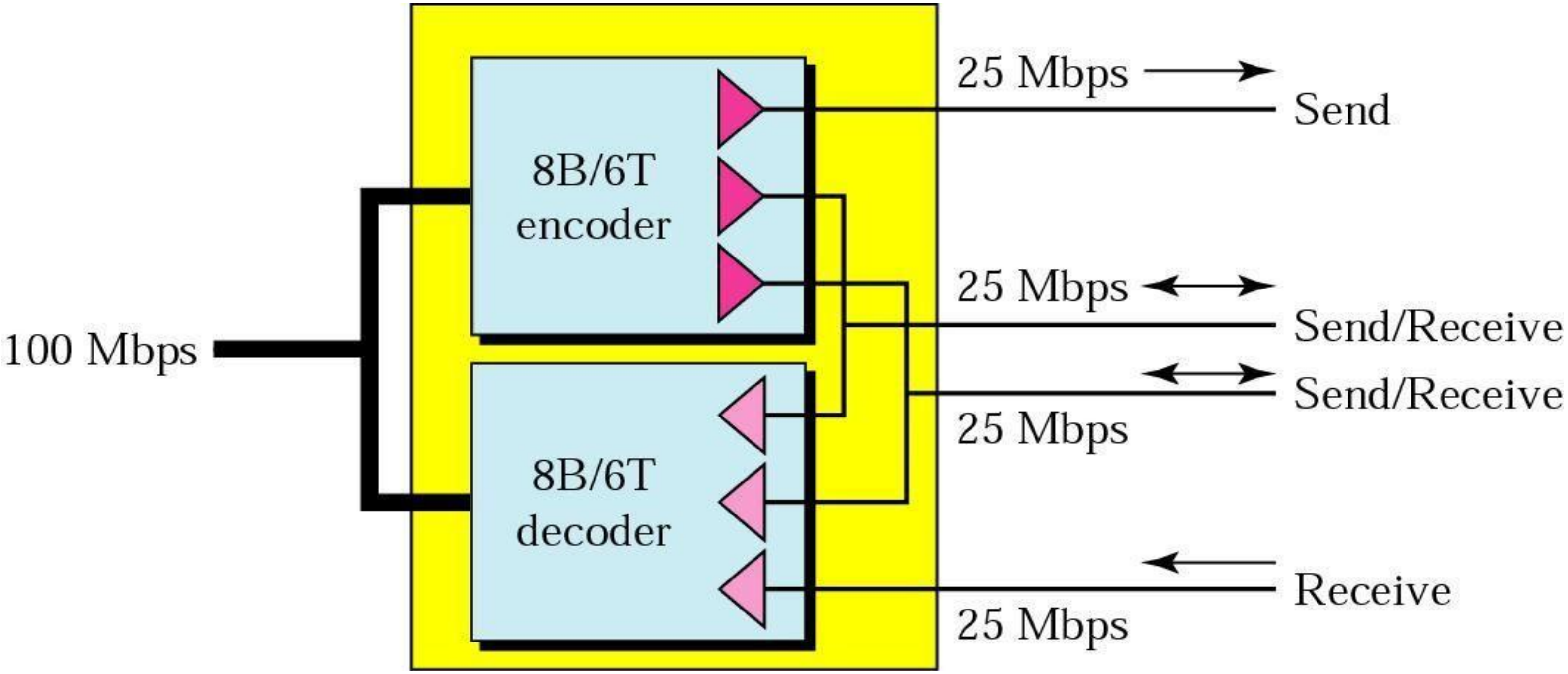


100BASE-T4 IMPLEMENTATION

1. Uses category 3 r higher utp.encoding and decoding is complicated.uses 4 pairs of utp for transmitting.



USING FOUR WIRES IN 100BASE-T4

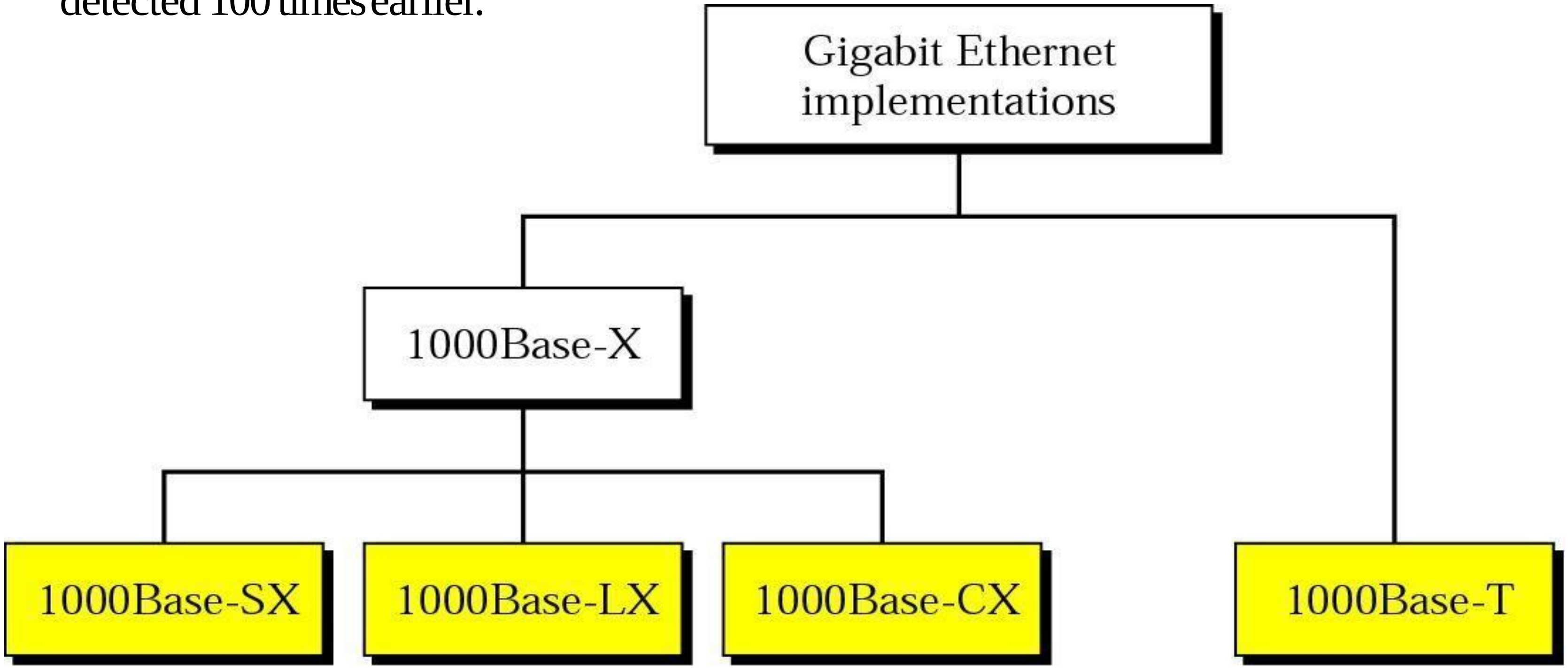


PHYSICAL LAYER IN GIGABIT ETHERNET

1. Need for even higher data rate resulted in design of gigabit ethernet(1000mbps)
2. **Goals:** 1)upgrade the date rate to 1gbps.
    1. compatible with stnd ethernet.
    2. keep same 48 bit address.
    3. keep same frame format.
    4. keep same min and max lengths.
    5. To support autonegotiation.
3. **Mac sublayer:** it is untouched.uses half & full duplex.
4. In full duplex there is central switch connected to all computers.each switch has buffers for each input port in which data r stored until they r transmitted.no collision in this mode.csma/cd not used.
5. In half duplex,a switch is replaced by hub,which acts as a common cable in which collision might occur.uses csma/cd.

GIGABIT ETHERNET IMPLEMENTATIONS

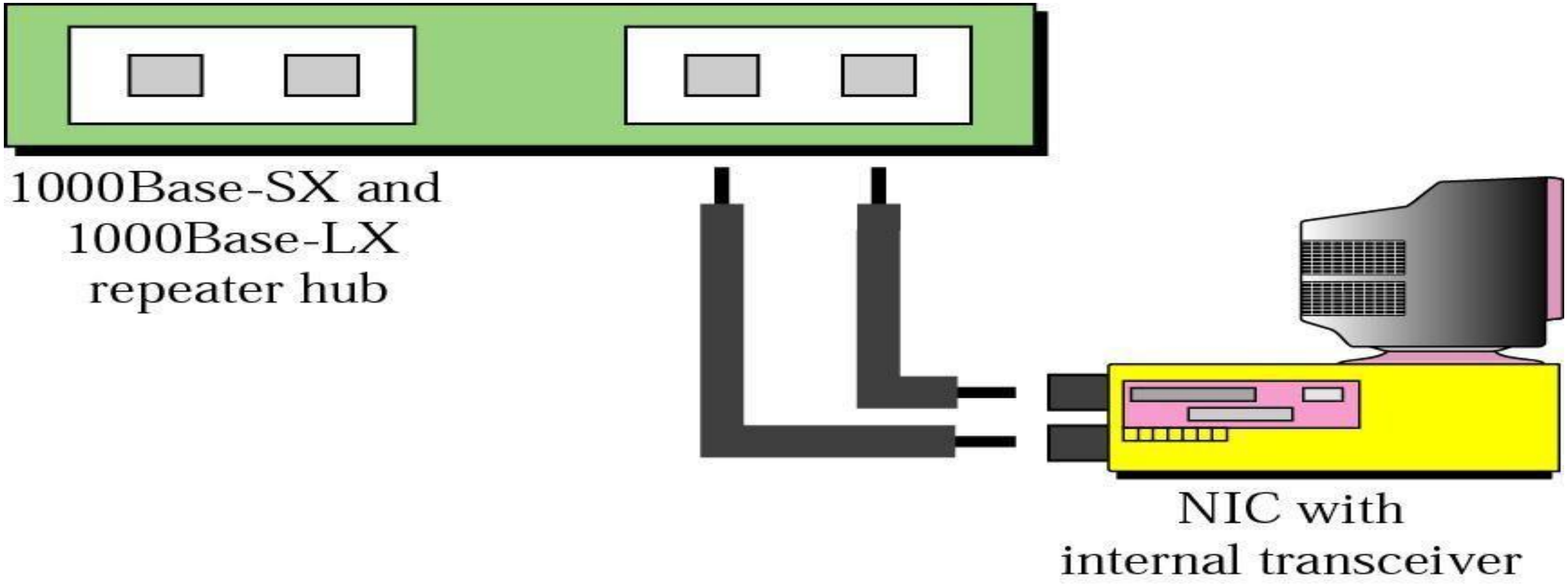
1. In traditional approach we keep minimum leghth of frame as 512 bits.so slot time in gigabit ethernet is 512 bitsX1/1000micro secs.reduced slot time means collision is detected 100 times earlier.



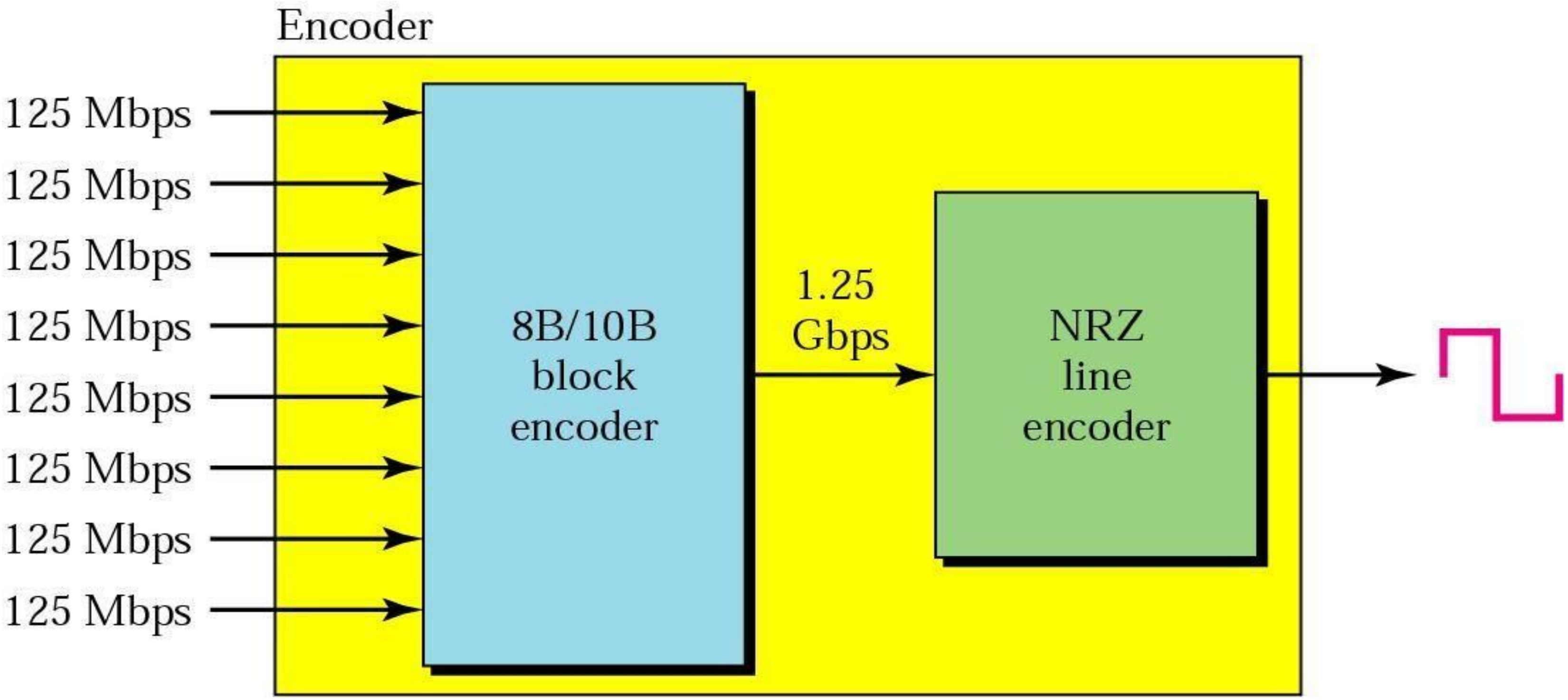
1. 2 wire 2 wire,long wave fiber 2 wire,copper(stp) 4 wire utp short wave fiber

1000BASE-X IMPLEMENTATION

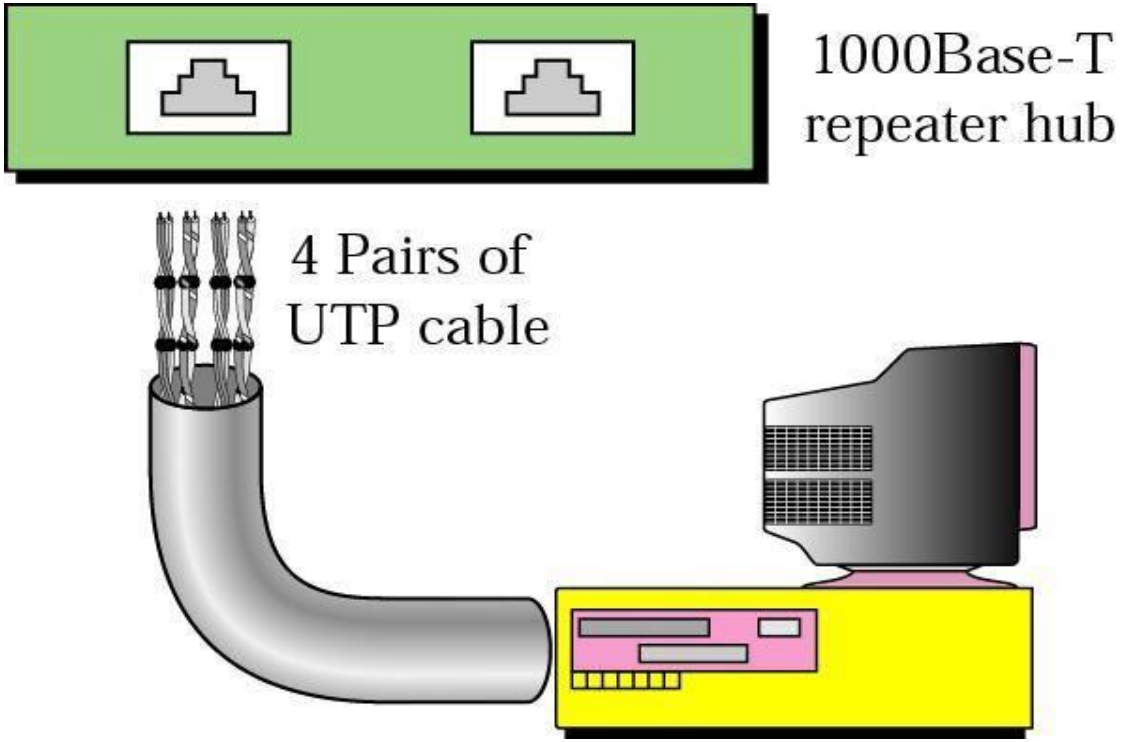
1. 1000 base-T was designed in response to those users who had already installed this wiring for other pursposes such as fastethernet.
2. Gigabit thernet cannot use manchestor encoding scheme bcoz it involves very high bandwidth.8b/10b block encoding is used.



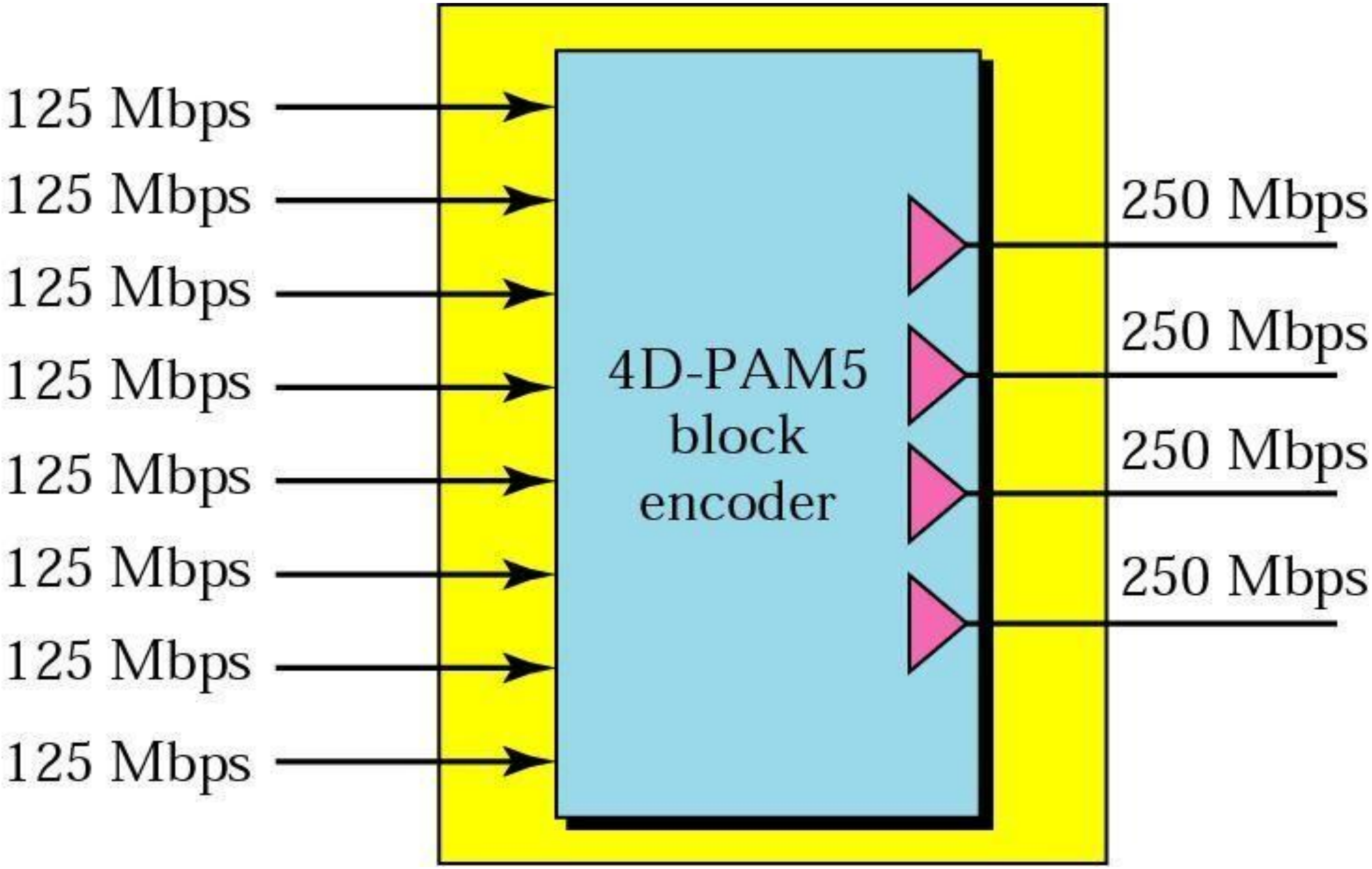
ENCODING IN 1000BASE-X



1000BASE-T IMPLEMENTATION



ENCODING IN 1000BASE-T



THE FIVE CATEGORIES

1. Those which operate below the physical layer such as a passive hub.

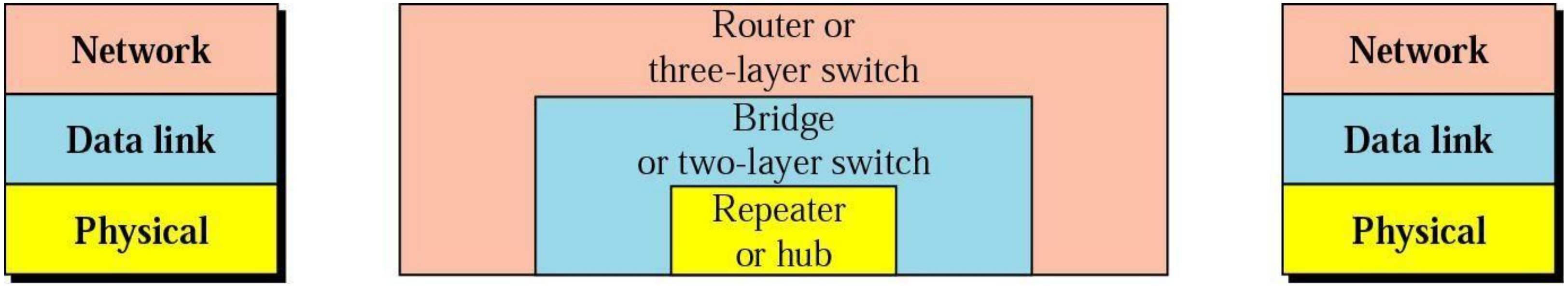
2. Those which operate at the physical layer(a repeater or an active hub).

3. Those which operate at the physical and data link layers (a bridge or a two-layer switch).

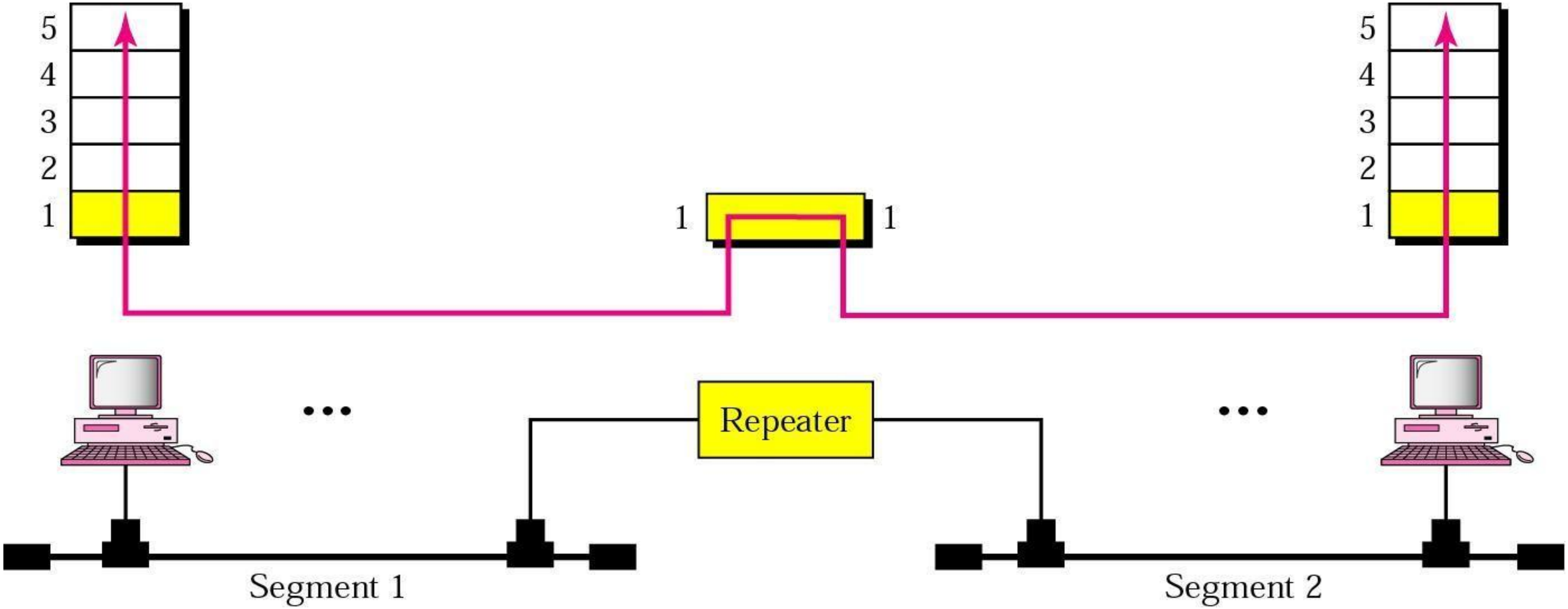
4. 4Those which operate at the physical, datalink, and network layers (a router or a
three-layer switch).

1. Those which can operate at all five layers (a gateway).

CONNECTING DEVICES

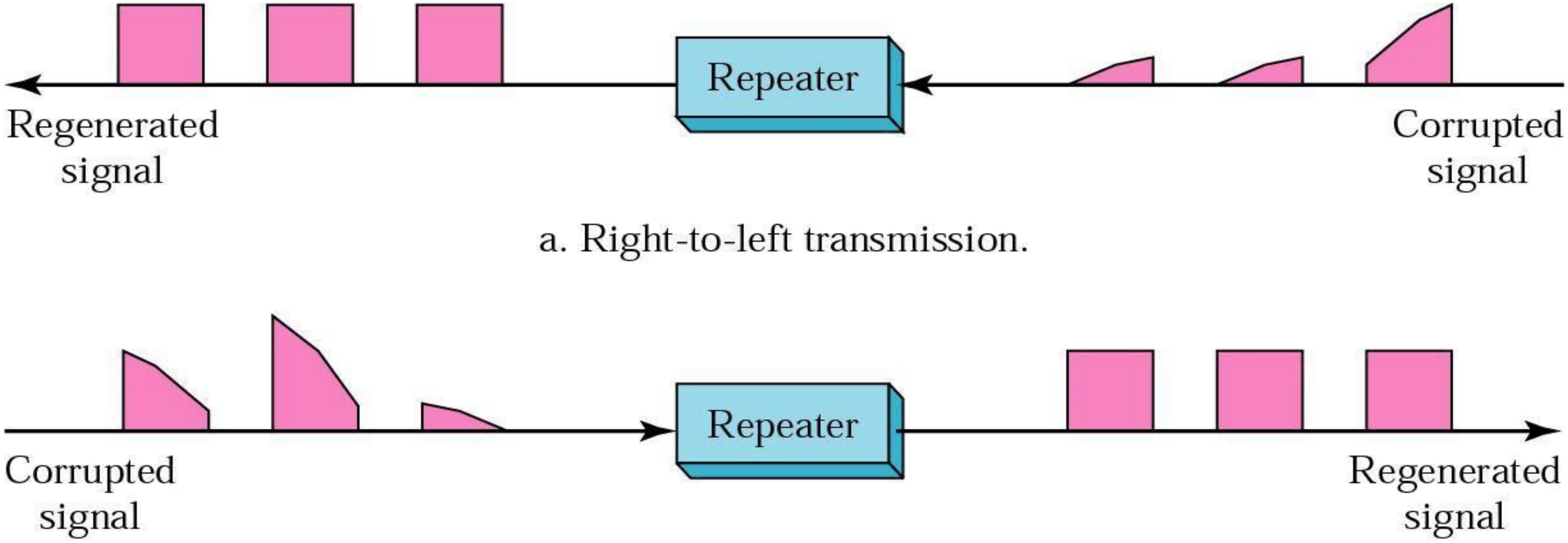


REPEATER



FUNCTION OF A REPEATER

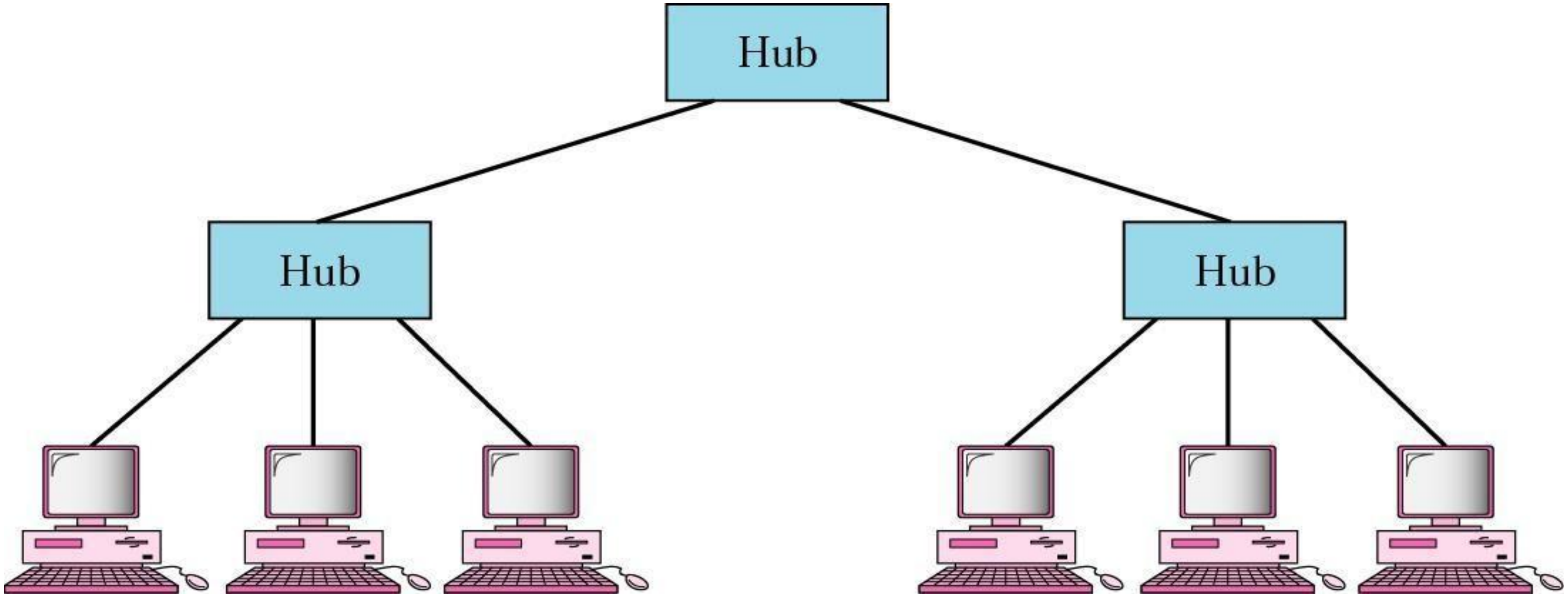
1. Location of repeater on a link is vital.
2. A repeater must be placed so that a signal reaches it before any noise changes meaning of bit.



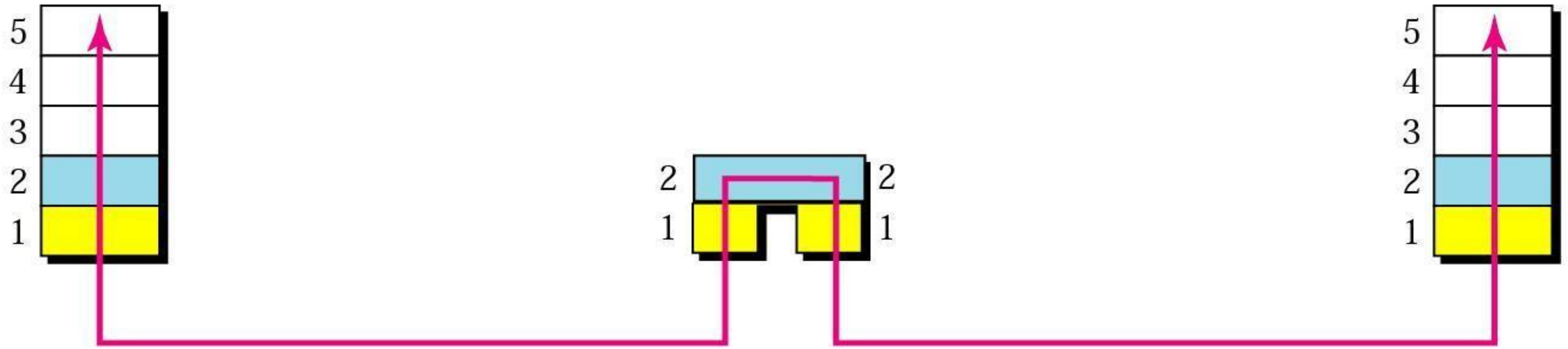
a. Right-to-left transmission.

b. Left-to-right transmission.

ACTIVE HUBS

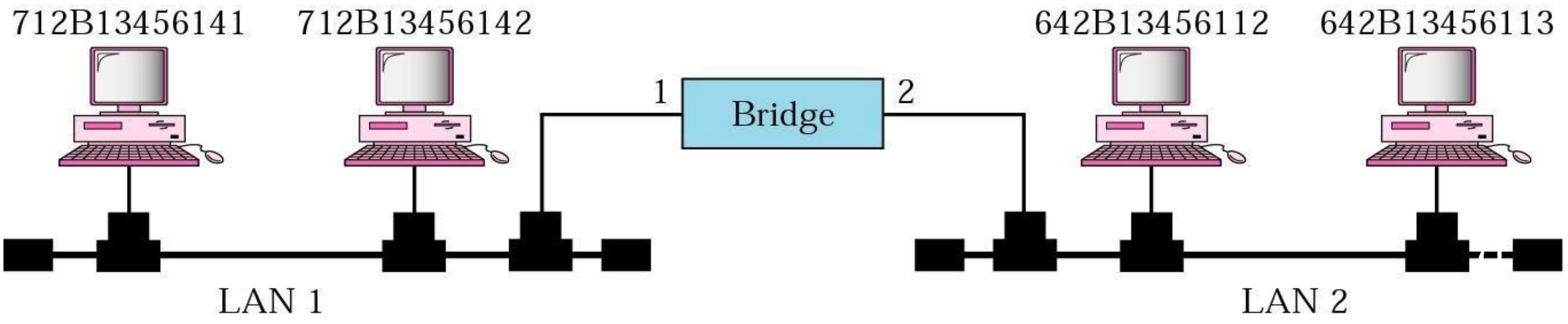


BRIDGE

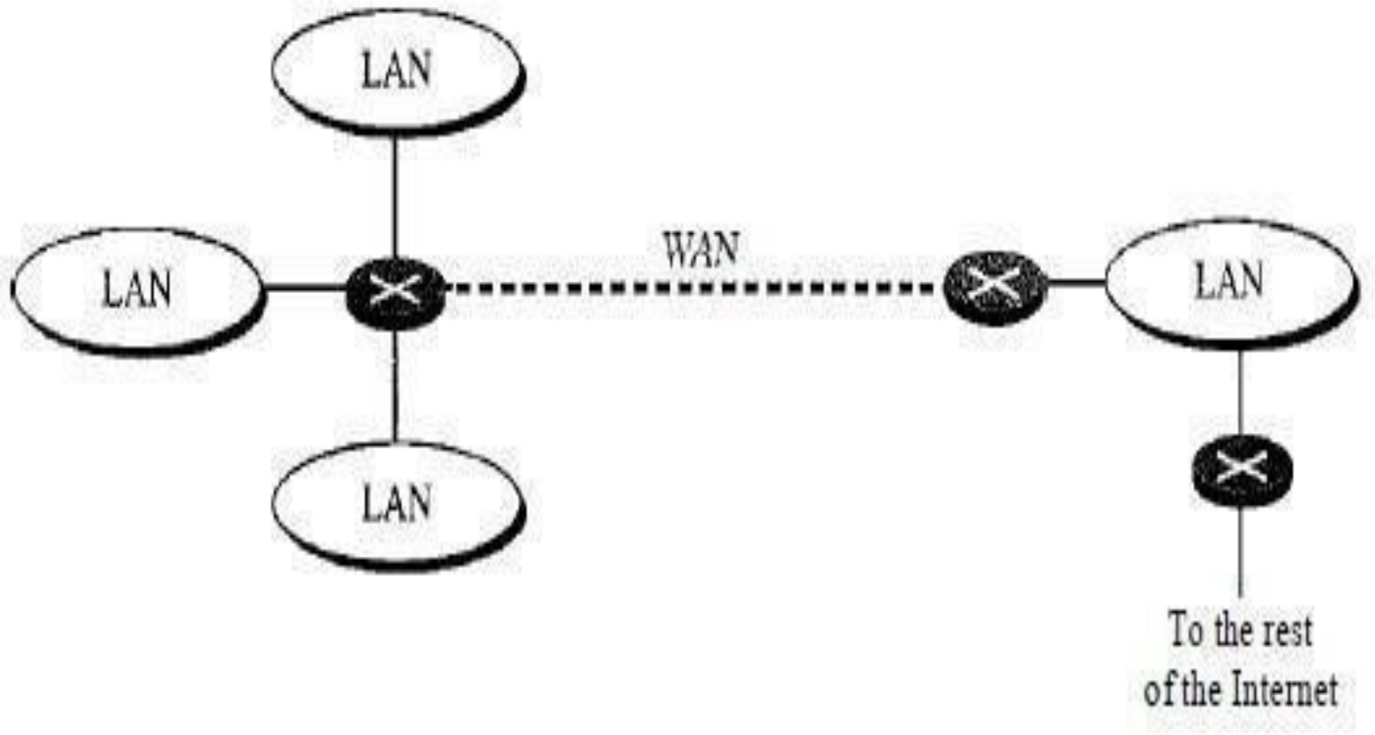


Address	Port
712B13456141	1
712B13456142	1
642B13456112	2
642B13456113	2

Bridge Table



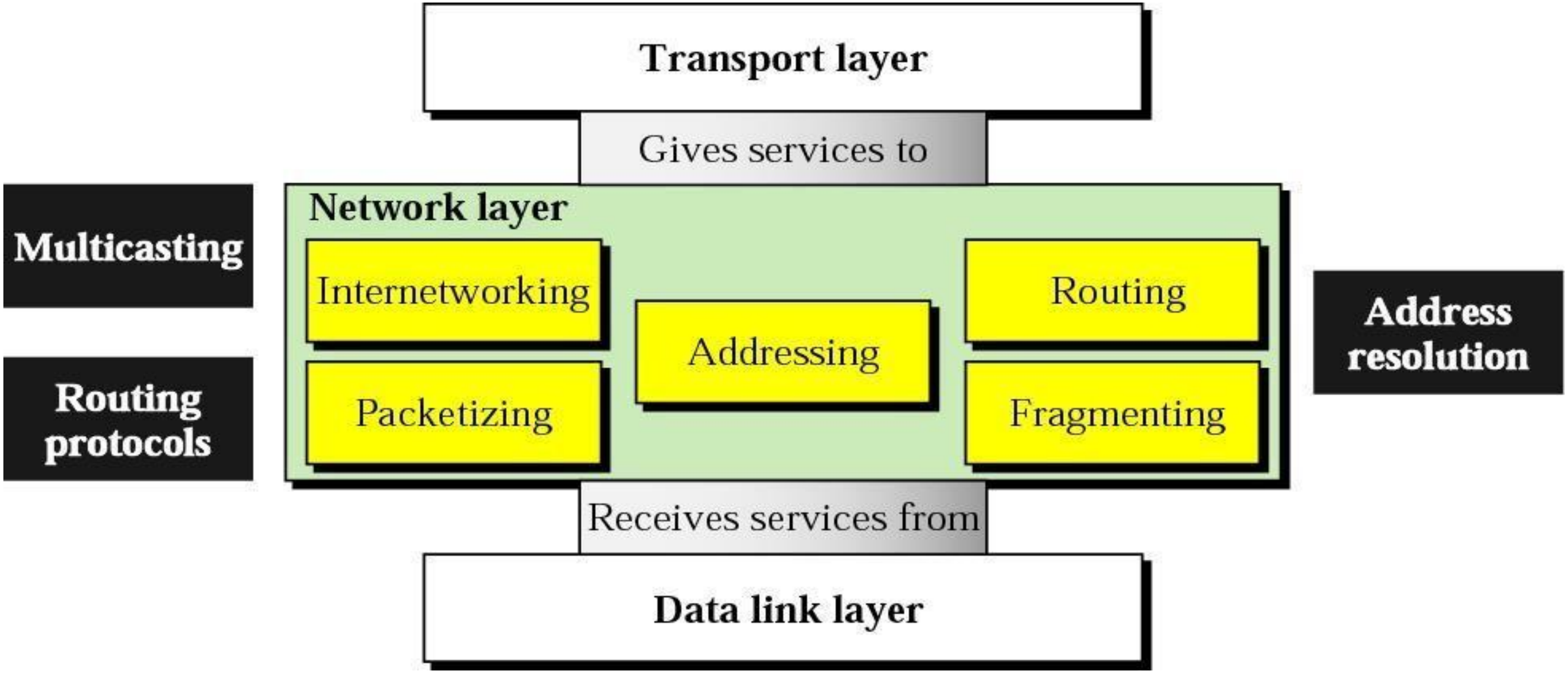
ROUTERS



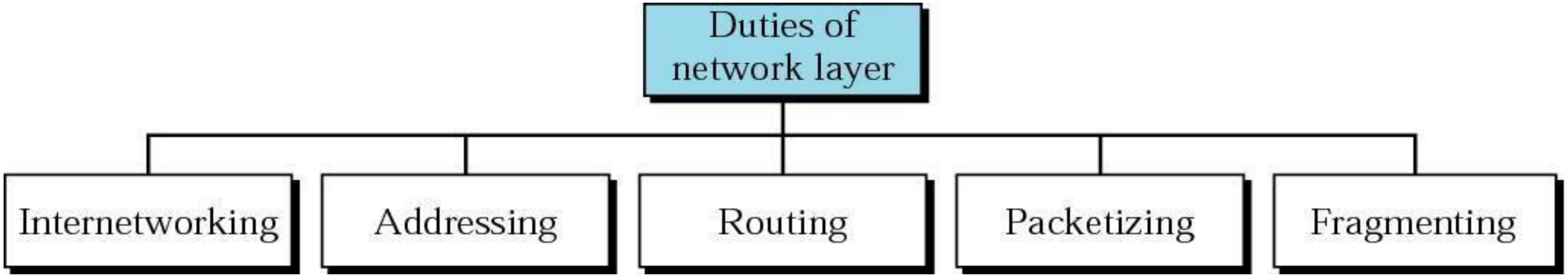
UNIT -III

Network Layer

POSITION OF NETWORKLAYER



NETWORK LAYER DUTIES



ROUTING INFORMATION PROTOCOL

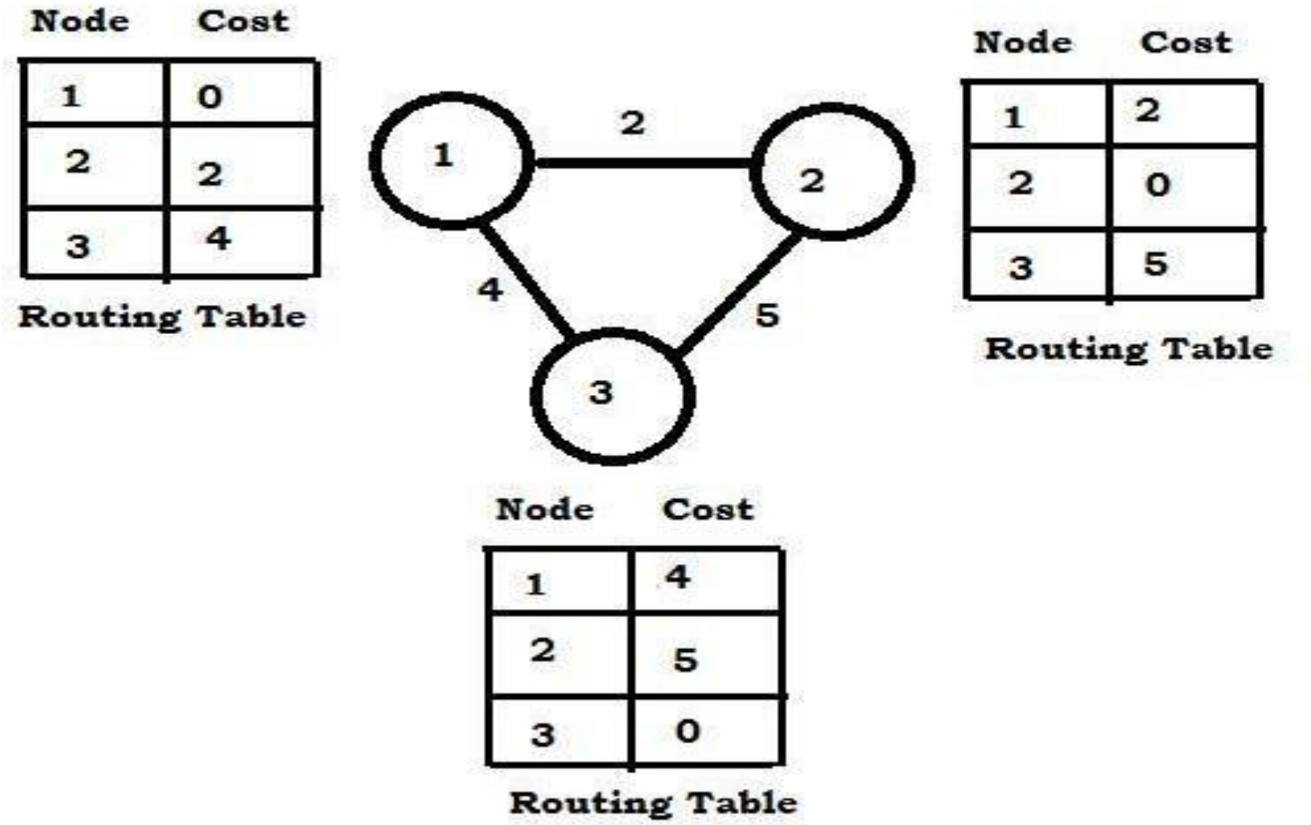
1. The routing information protocol (RIP) is an interior routing protocol used inside an autonomous system.

2. It is a very simple protocol based on distance vector routing which uses the Bellman-Ford alg for calculating the routingtables.

DISTANCE VECTOR ROUTING

1. In distance vector routing each router periodically shares its knowledge about the entire internet with its neighbors.
2. In distance vector routing, the least-cost routebetweenany two nodes is the route with minimum distance.
3. In this protocol, as the name implies, each nodemaintains
   4. a vector (table) of minimum distances toeverynode.
5. The table at each node also guides the packets to the desired node by showing the next stop in the route (next-hop routing).
6. We can think of nodes as the cities in an area andthe lines as the roads connecting them.
7. Atable can show a tourist the minimum distancebetween cities.

DISTANCE VECTOR ROUTING ALG



Node	Cost
1	0
2	2
3	4

Routing Table

Node	Cost
1	2
2	0
3	5

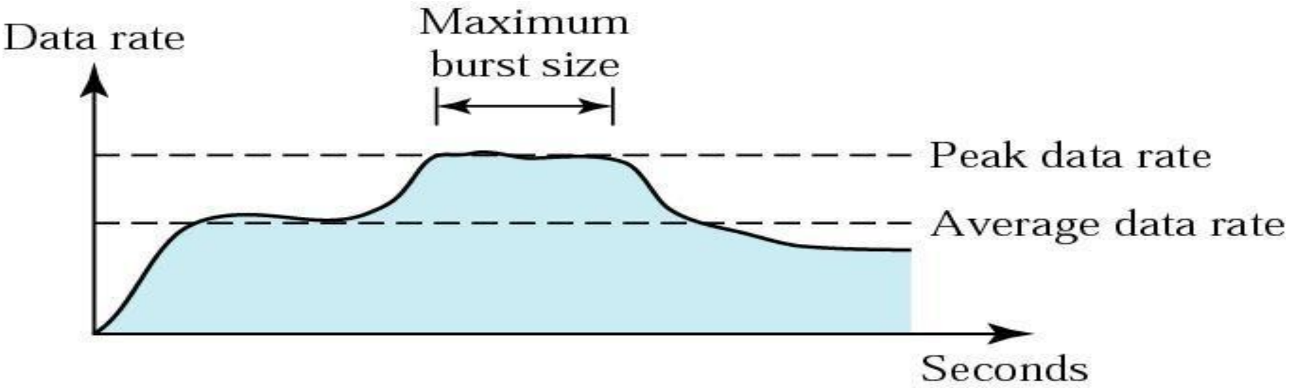
Routing Table

Node	Cost
1	4
2	5
3	0

Routing Table

TRAFFIC DESCRIPTORS

1. In **cc**control we try to avoid traffic congestion.in **qos**wetry to create an appropriate envt fortraffic.
2. **Traffic descriptor**r qualitative values that representdata flow.
3. **Avg bit rate** is no. of bits sent during period of time divided by no. of secs.
4. **Peak data rate** defines max data rate of traffic.
5. Max length of time traffic is generated at peak rate is **ax burst size**.



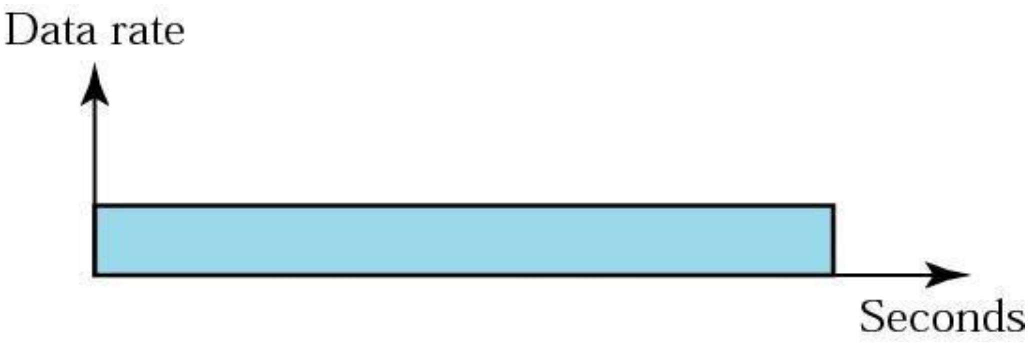
TRAFFIC PROFILES

1. A data flow can have one of the following traffic profiles:
   - constant bit rate,
   - variable bit rate,
   - or bursty

CONSTANT-BIT-RATE TRAFFIC

A constant-bit-rate (CBR), or a fixed-rate, traffic model has a data rate that does not change.

In this type of flow, the average data rate and the peak data rate are the same.

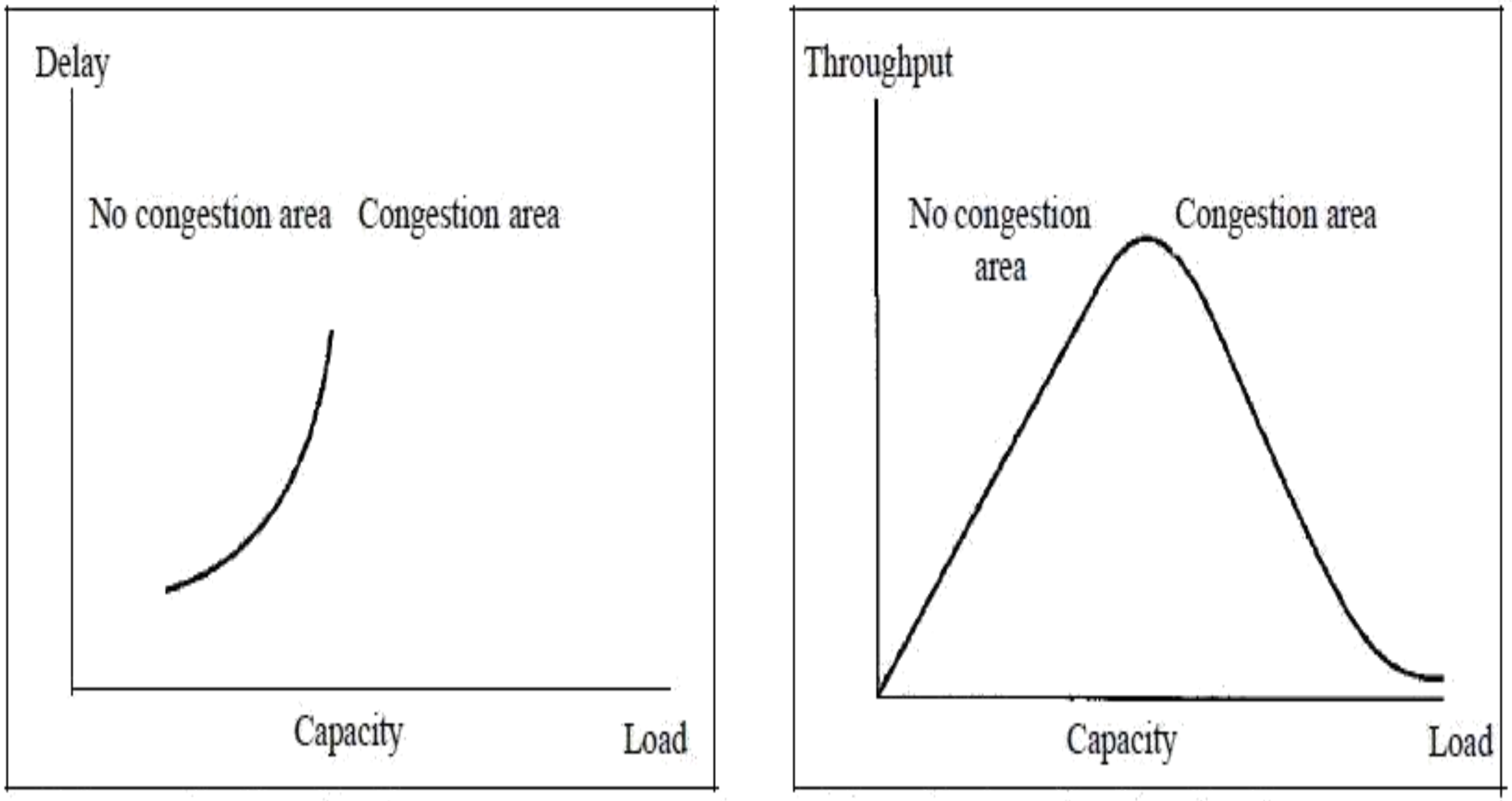


VARIABLE-BIT-RATE (VBR)

1. In the variable-bit-rate (VBR) category, the rate of the data flow changes in time, with the changes smooth instead of sudden and sharp.

2. In this type of flow, the average data rate and the peak data rate are different.

3. The maximum burst size is usually a small value.



a. Delay as a function ofload

b. Throughput as a function of load

1. Congestion in anetwork may occur if the

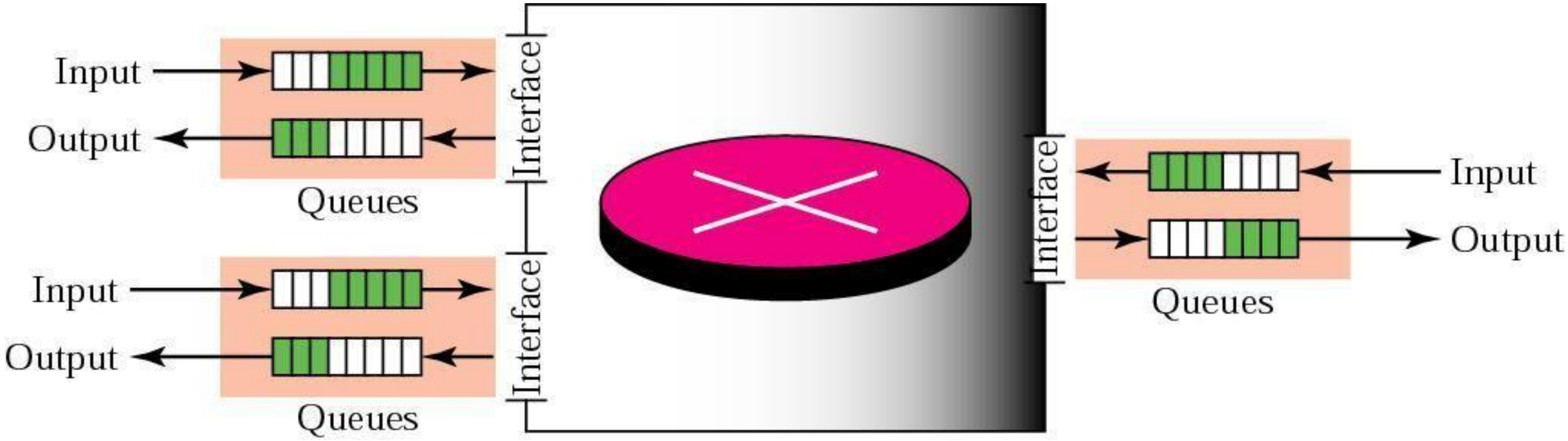
   load on the network

   - The number of packets sent to the network- is greater than the capacity of the network.
   - **capacity** : The number of packets a network can handle.

1. **Congestion control** refers to the mechanisms and techniques to control the congestion and keep the load below the capacity.

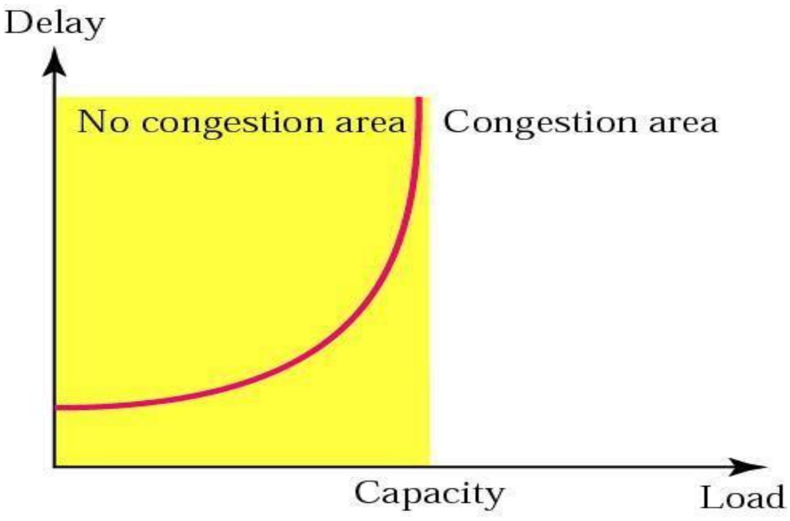
3 STEPS

1. 1. The packet is put at the end of the input queue while waiting to be checked.
2. 2. The processing module of the router removes the packet from the input queue once it reaches the front of the queue and uses its routing table and the destination address to find theroute.
3. 3. The packet is put in the appropriate output queue and waits its turn to be sent.



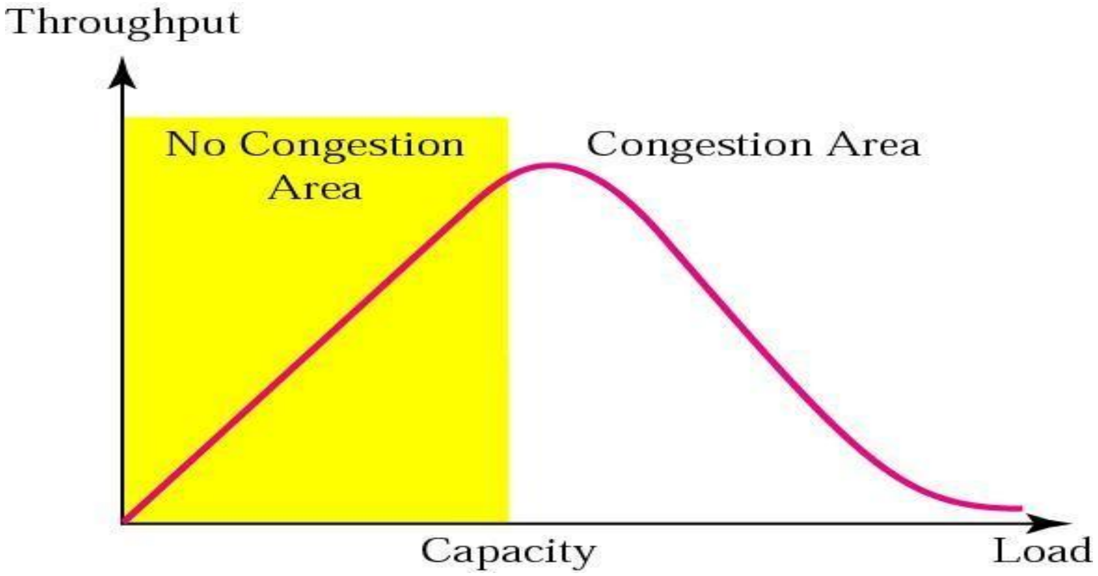
PACKET DELAY AND NETWORK LOAD

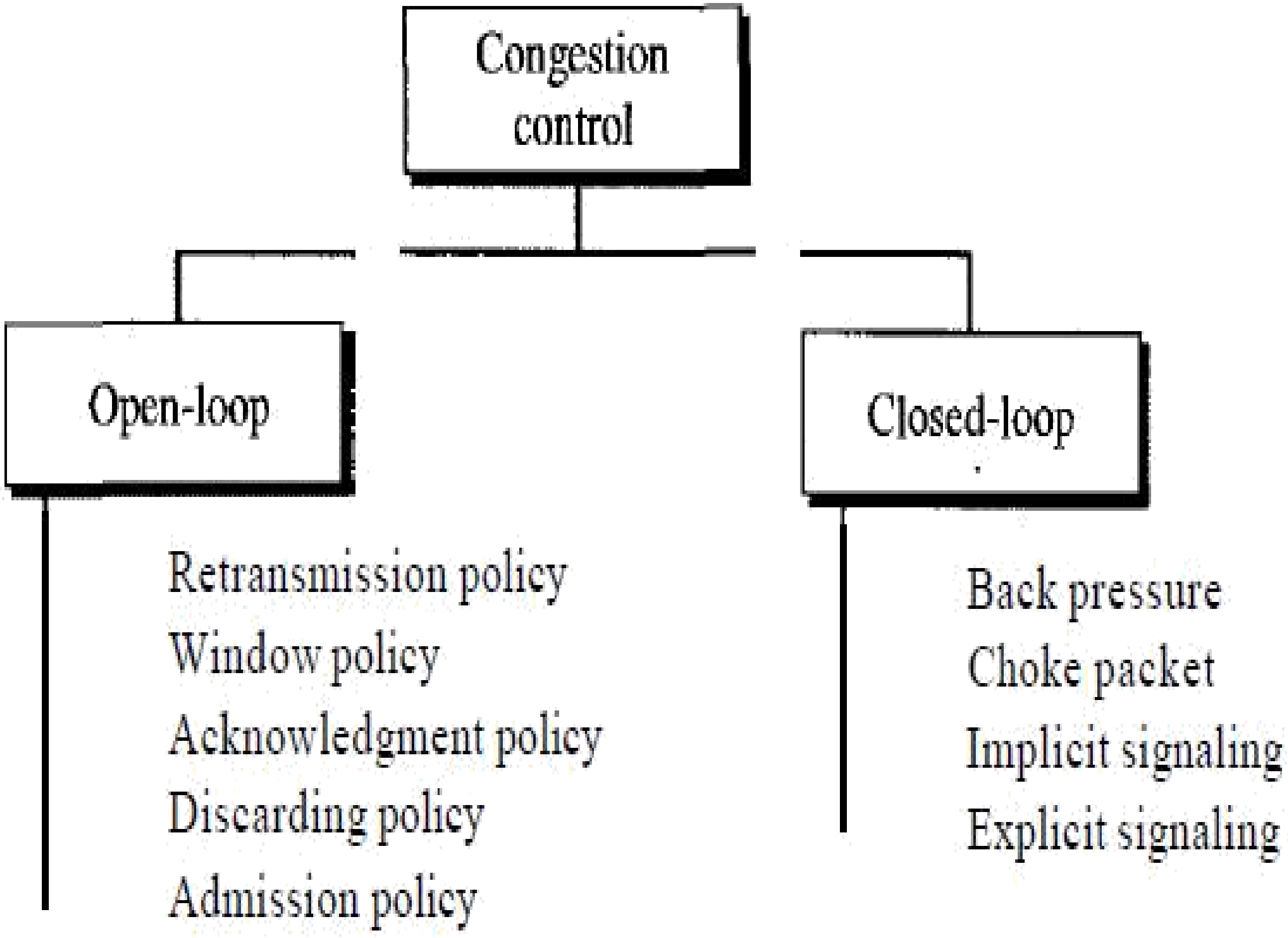
1 Involves 2 factors that measure the performance of n/w -delay & throughput.



THROUGHPUT VERSUS NETWORK LOAD

1. Throughput is no. of packets passing through n/w in unit of time.





Congestion control
Open-loop
Closed-loop
Retransmission policy
Window policy
Acknowledgment policy
Discarding policy
Admission policy
Back pressure
Choke packet
Implicit signaling
Explicit signaling

OPEN-LOOP CONGESTION CONTROL

1. In open-loop congestion control, policies are applied to prevent congestion before it happens.
2. In these mechanisms, congestion control is handled by either the source or the destination.

RETRANSMISSION POLICY

1. If the sender feels that a sent packet is lost or corrupted, the packet needs to be retransmitted.

2. Retransmission in general may increase congestion in the network.

WINDOW POLICY

1. Thetype of window at thesendermay also affect congestion.

2. The Selective Repeat window is better than the Go-Back-N window for congestion control.

3. In the *Go-Back-N* window, when the timer for a packet times out, several packets may be resent

4. The Selective Repeat window, on the other hand, tries to send the specific packets that have been lost or corrupted.

ACKNOWLEDGMENT POLICY

1. The acknowledgment policy imposed by the receiver may also affect congestion.
2. If the receiver does not acknowledge every packet it receives, it may slow down the sender and help prevent congestion.

Discarding Policy

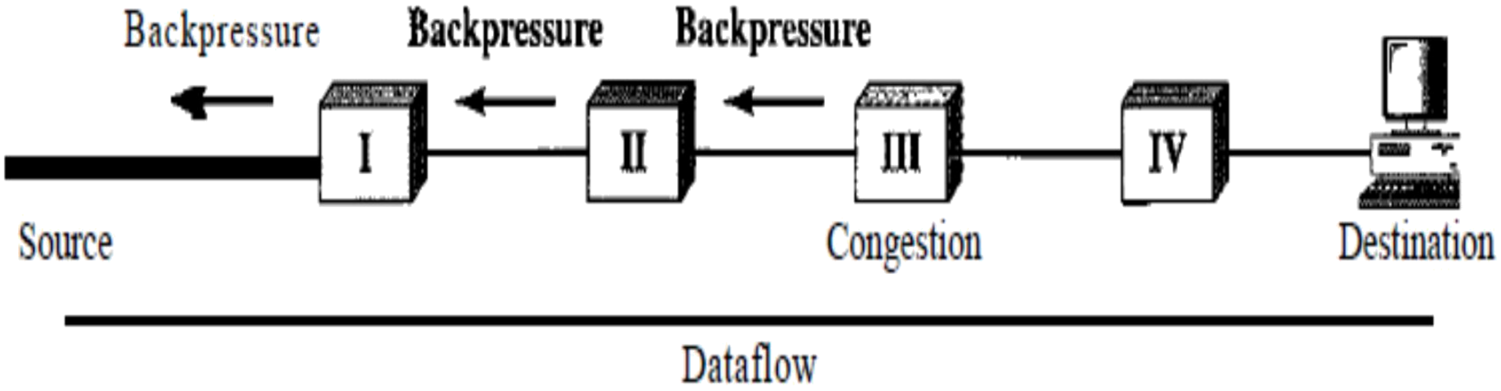
1. A good discarding policy by the routers may prevent congestion and at the same time may not harm the integrity of the transmission.

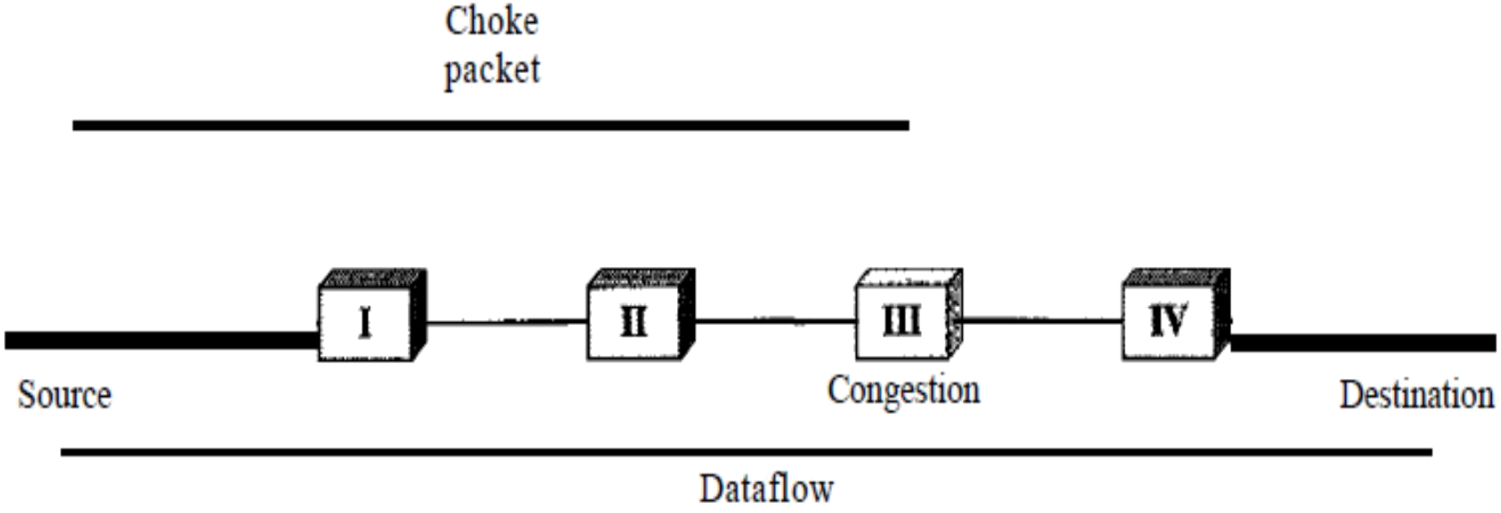
ADMISSION POLICY

1. An admission policy, which is a quality-of- service mechanism, can also prevent congestion in virtual-circuit networks.
2. Switches in a flow first check the resource requirement of a flow before admitting it to the network.
3. A router can deny establishing a virtual circuit connection if there is congestion in the network or if there is a possibility of future congestion.

CLOSED LOOP

1. Closed-loop congestion control mechanisms try to alleviate congestion after it happens.
2. backpressure->in which congested node stops recvng data frm immediate upstream
3. Choke packet:is a packet sent by a node to source to inform it of congestion.
4. Implicit signaling:no communication btw source and congested nodes.source guesses that there is congestion somewhere in n/w.
5. Explicit signaling:source that experiences congestion can explicitly send a signal to source r destn.


Backpressure
Backpressure
Backpressure
I
II
III
IV
Source
Congestion
Destination
Dataflow


Choke
packet
I
II
III
IV
Source
Congestion
Destination
Dataflow

CONGESTION WINDOW

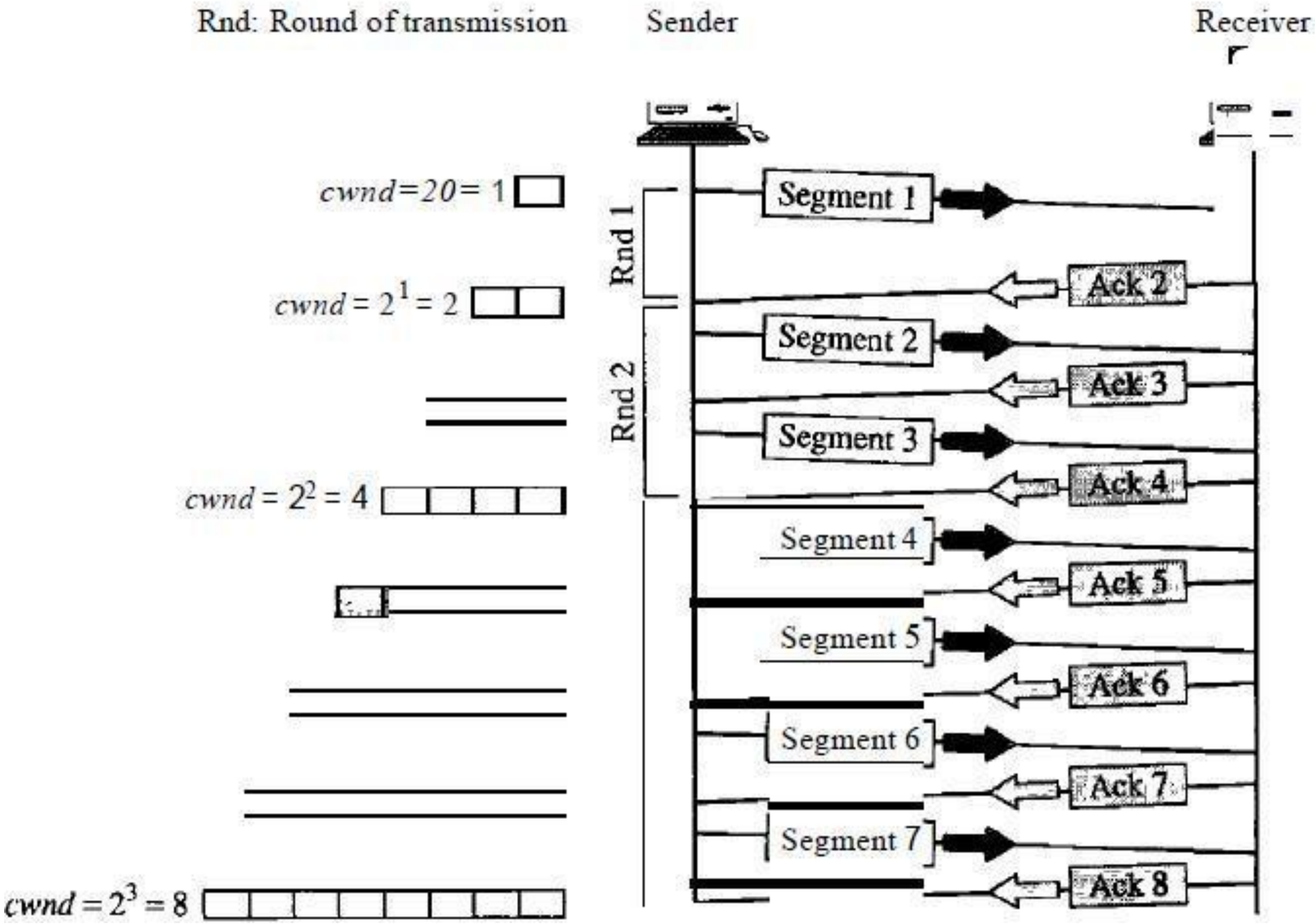
1. The sender's window size is determined not only by the receiver but also by congestion in the network.
2. The sender has two pieces of information:
   - The receiver-advertised window size and
   - The congestion window size.
3. The actual size of the window is the minimum of these two.
4. Actual window size = minimum (rwnd, cwnd)

CONGESTION AVOIDANCE

1. **In tcp it uses2policies**
   - slow start and additive increase
   - multiplicative decrease

2. **1)slow start:exponential increase:** alg is based on idea that size of congestion window starts with 1 max segment size(MSS).
3. MSSis determined during connectionestablishment.
4. size of window increases 1 MSSeach time ack is sent.
5. window starts slowly and grows exponentially.
6. **additive increase**:to avoid congestion bfore it happens,one must slow down itsexponential growth.
7. when size of congestion window reaches slow start threshold,slow start phase stops and additive phase begins.
8. In this algorithm, each time the whole window of segments is acknowledged (one round), the size of the congestion window is increased by 1
9. **2)multiplicative decrease**:if congestion occurs,congestion window size must b decreased.size of threshold must be dropped to one half.

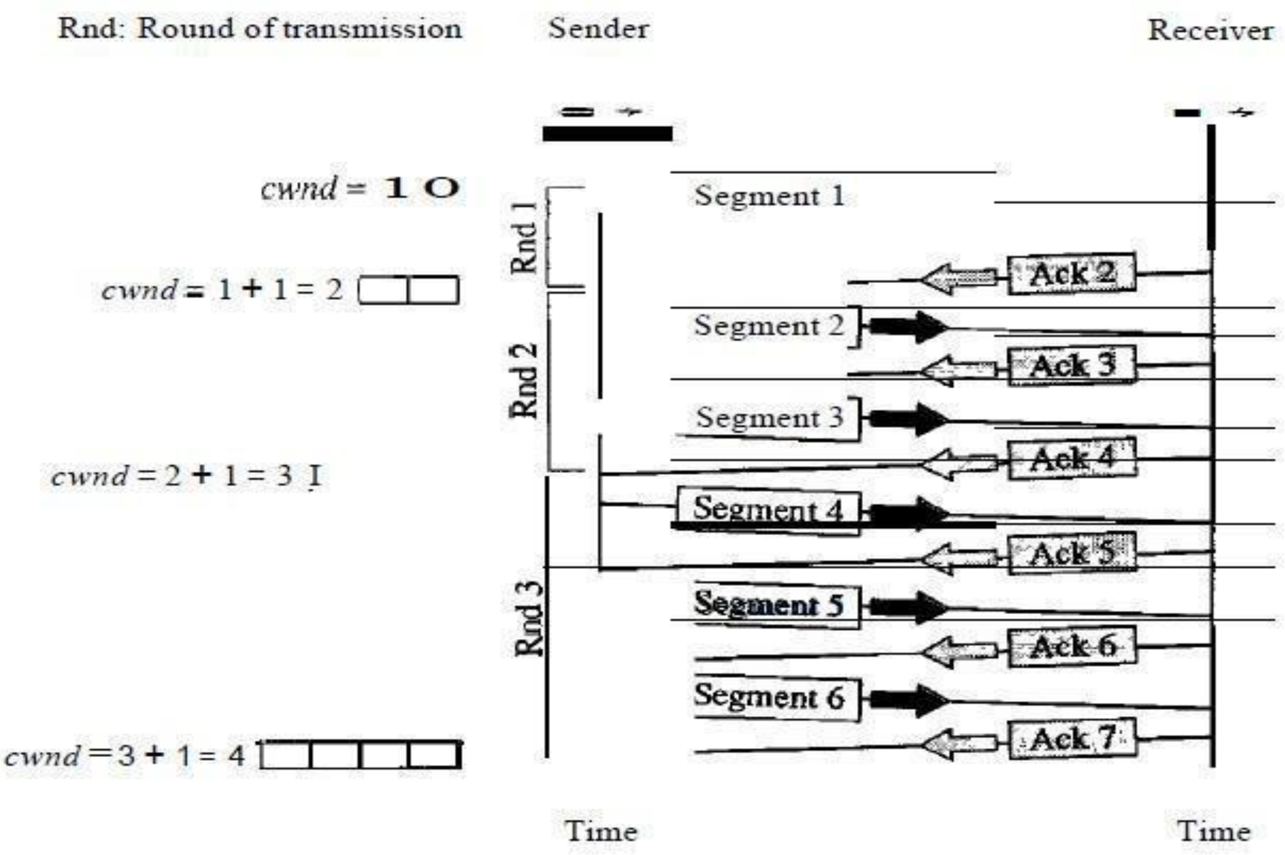
SLOWSTART, EXPONENTIALINCREASE



If we look at the size of cwnd in terms of rounds we find that therate is exponential as shown below:

1. Start ..... cwnd=l
2. After round 1 ..... cwnd=21=2
3. After round 2 ..... cwnd=22=4
4. After round 3 ..... cwnd=23=8

CONGESTIONAVOIDANCE, ADDITIVE INCREASE



this case, after the sender has received acknowledgments for a complete windov

IF WE LOOK AT THE SIZE OF CWND IN TERMS OF ROUNDS, WE FIND THAT THE RATE IS ADDITIVE AS SHOWN BELOW:

1. Start
2. After round1
3. After round2
4. After round3

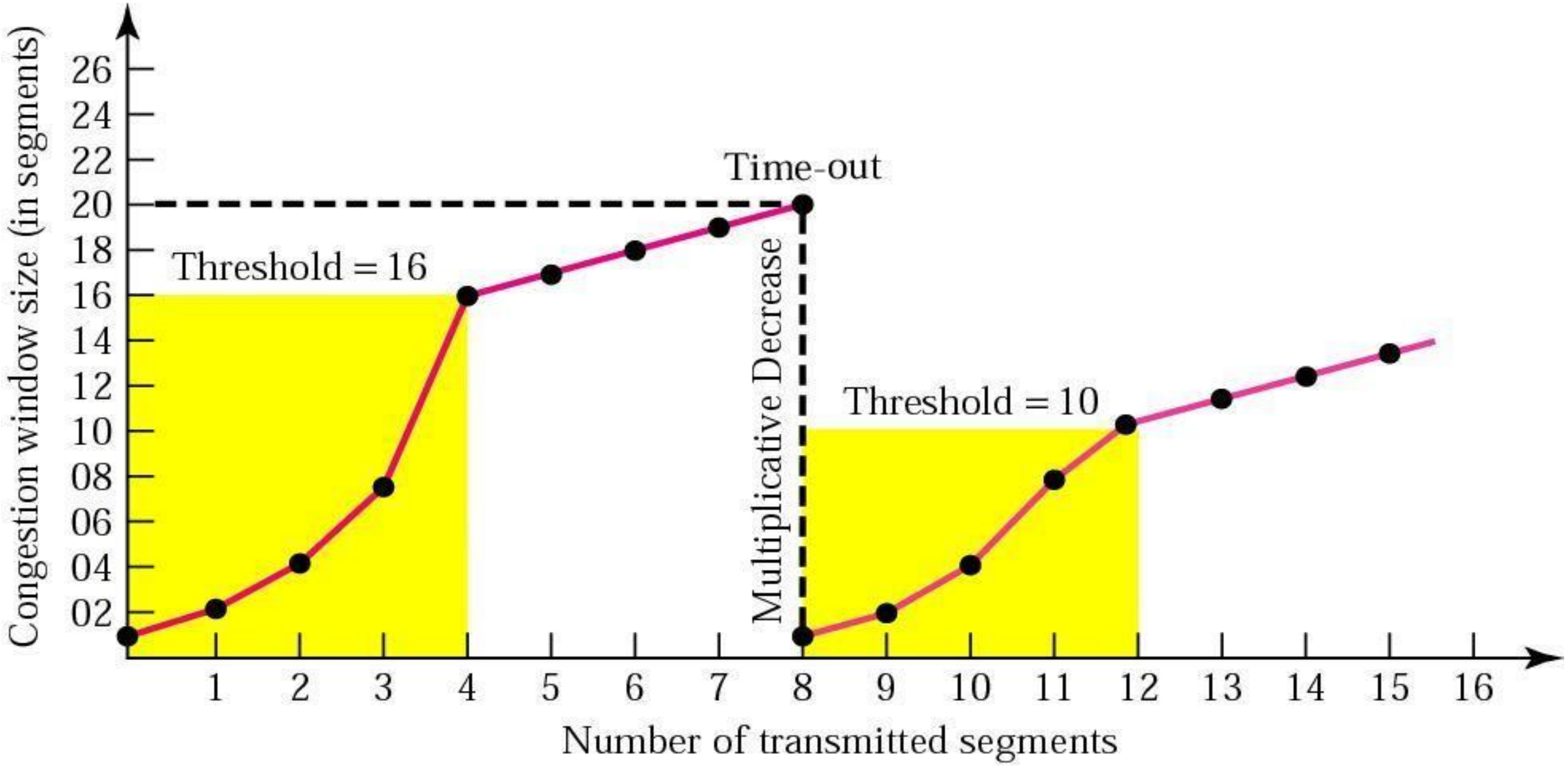
- ....

1. cwnd=l
2. cwnd= 1+1 =2
3. cwnd=2+1 =3
4. cwnd=3+1 =4

MULTIPLICATIVE DECREASE

1. If congestion occurs, the congestion window size must be decreased.
2. The only way the sender can guess that congestion has occurred is by the need to retransmit a segment.
3. The strategy says if a time-out occurs, the threshold must be set to one-half of the last congestion window size, and the congestion window size from 1 again.

MULTIPLICATIVE DECREASE



CONGESTION CONTROL IN FRAME RELAY

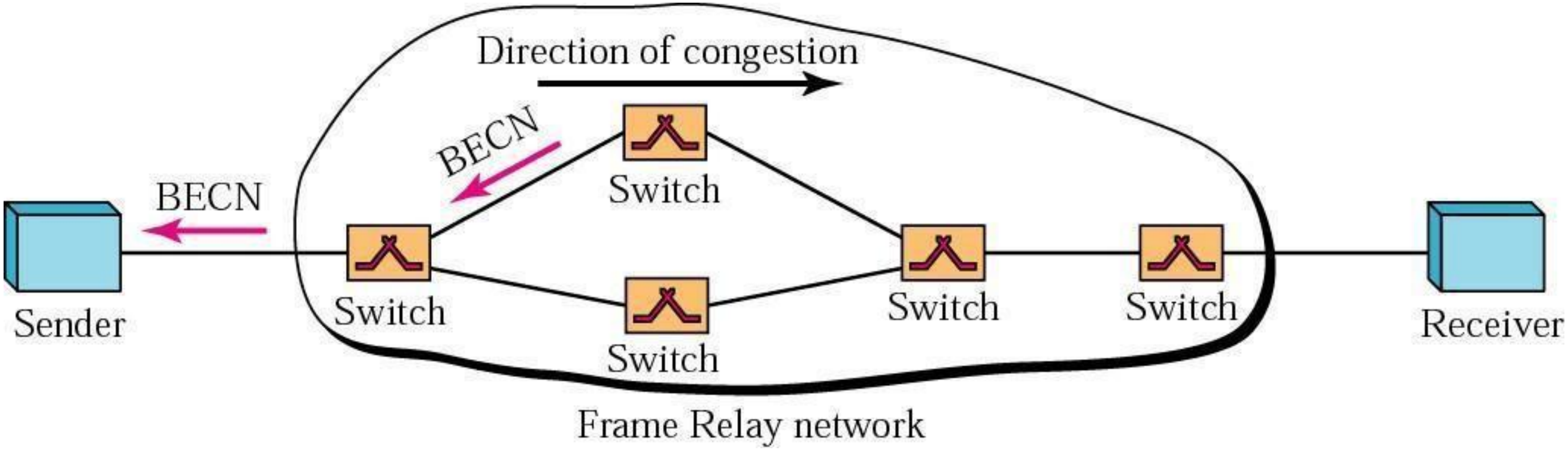
1. Congestion in a Frame Relay network decreases throughput and increases delay.
2. A high throughput and low delay are the main goals of the Frame Relay protocol.
3. Frame Relay does not have flow control.

Congestion Avoidance

- For congestion avoidance, the Frame Relay protocol uses 2 bits in the frame to explicitly warn the source and the destination of the presence of congestion.
- BECN
- FECN

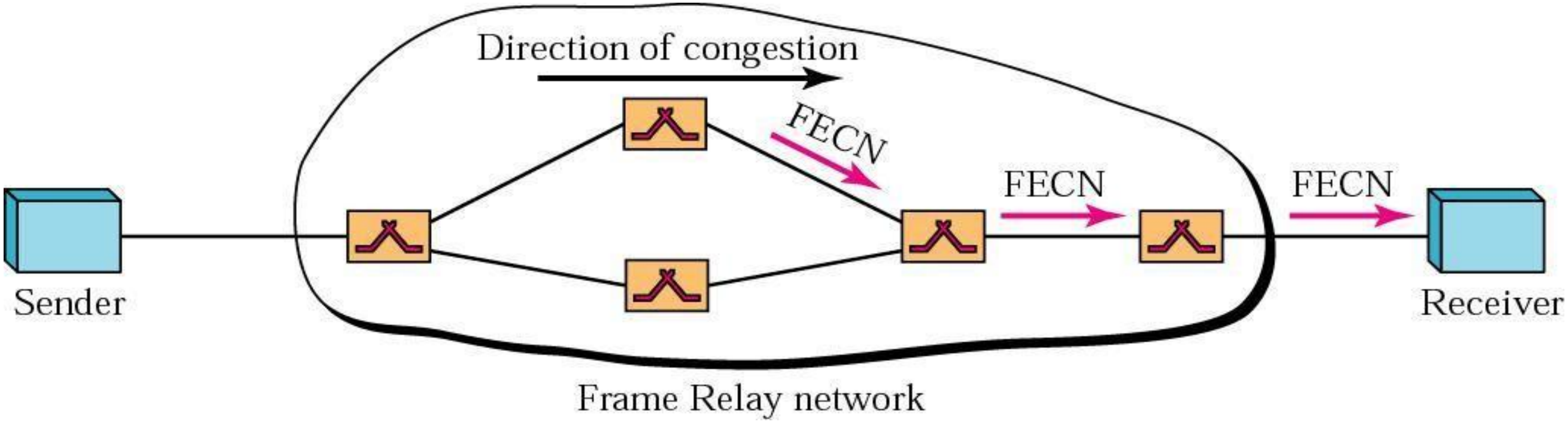
BACKWARD EXPLICIT CONGESTION NOTIFICATION(BECN):

1. Abit warns sender of congestion inn/w.
2. switch uses response frames from receiver or switch can use predefined connection(DLCI) to send special frames for this specificpurpose.
3. Thesender canrespond to this warningby simply reducing the datarate.

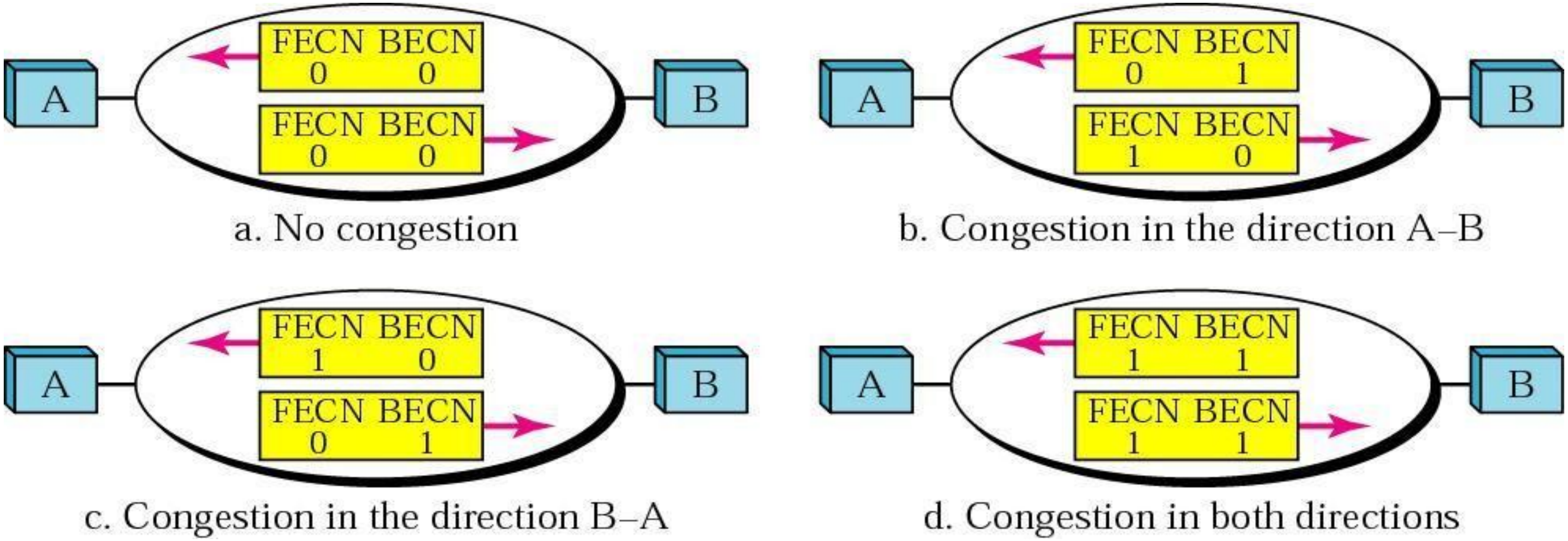


FORWARD EXPLICIT CONGESTION NOTIFICATION(FECN)

1. ABit is used to warns receiver of congestion inn/w.
2. The receiver can respond to this warning by simply can delay the acknowledge thus forcing the sender to slow downrate.



FOUR CASES OF CONGESTION



a. No congestion

b. Congestion in the direction A–B

c. Congestion in the direction B–A

d. Congestion in both directions

QUALITY OF SERVICE

1. four types of characteristics are attributed to a flow:
   - Reliability
   - delay,
   - Jitter
   - bandwidth

RELIABILITY

1. Reliability is a characteristic that a flow needs.

2. Lack of reliability means losing a packet or acknowledgment, which entails retransmission.

3. However, the sensitivity of application programs to reliability is not the

   same.

4. For example, it is more important that electronic mail, file transfer, and Internet access have reliable transmissions than telephony or audio conferencing

DELAY

1. Source-to-destination delay is another flow characteristic.

2. Again applications can tolerate delay in different degrees.

3. In this case, telephony, audio conferencing, video conferencing, and remote log-in need minimum delay, while delay in file transfer or e-mail is less important

JITTER

1. Jitter is the variation in delay for packets belonging to the sameflow.

2. For example, if four packets depart at times 0, 1, 2, 3 and arrive at 20, 21, 22, 23, all have the same

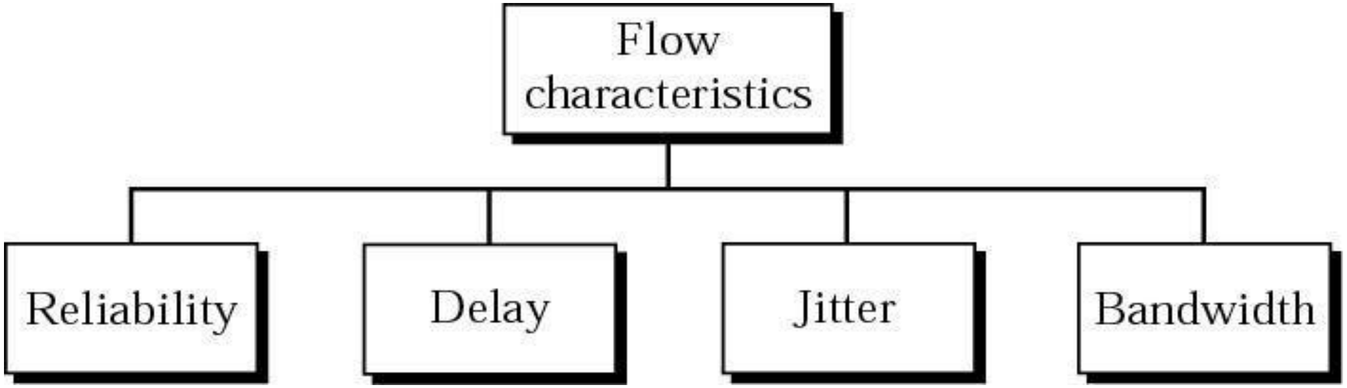
   delay, 20 units of time.

3. On the other hand, if the above four packets arrive at 21, 23, 21, and 28, they will have different delays: 21,22, 19, and24.

BANDWIDTH

1. Different applications need different bandwidths.
2. For In video conferencing need more bandwidth
3. in an e-mail it may need less bandwidth

FLOW CHARACTERISTICS



1. reliability Lackof reliability means losing apacket or acknowledgment, which entails retransmission.
2. delay Applications can tolerate delay in different degrees.
3. In this case, telephony, audio conferencing, video conferencing, and remote log-in need minimum delay.
4. while delay in file transfer or e-mail is less important.

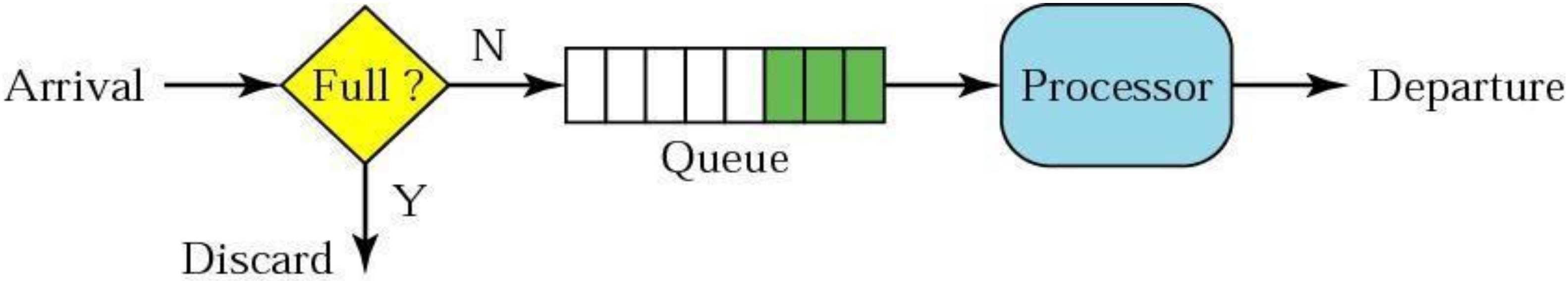
TECHNIQUES TO IMPROVE QOS

1. four common methods to improve QoS
   - scheduling,
   - traffic shaping,
   - admission control,
   - resource reservation.

FIFO QUEUE

1. Several scheduling techniques are designed to improve QoS.

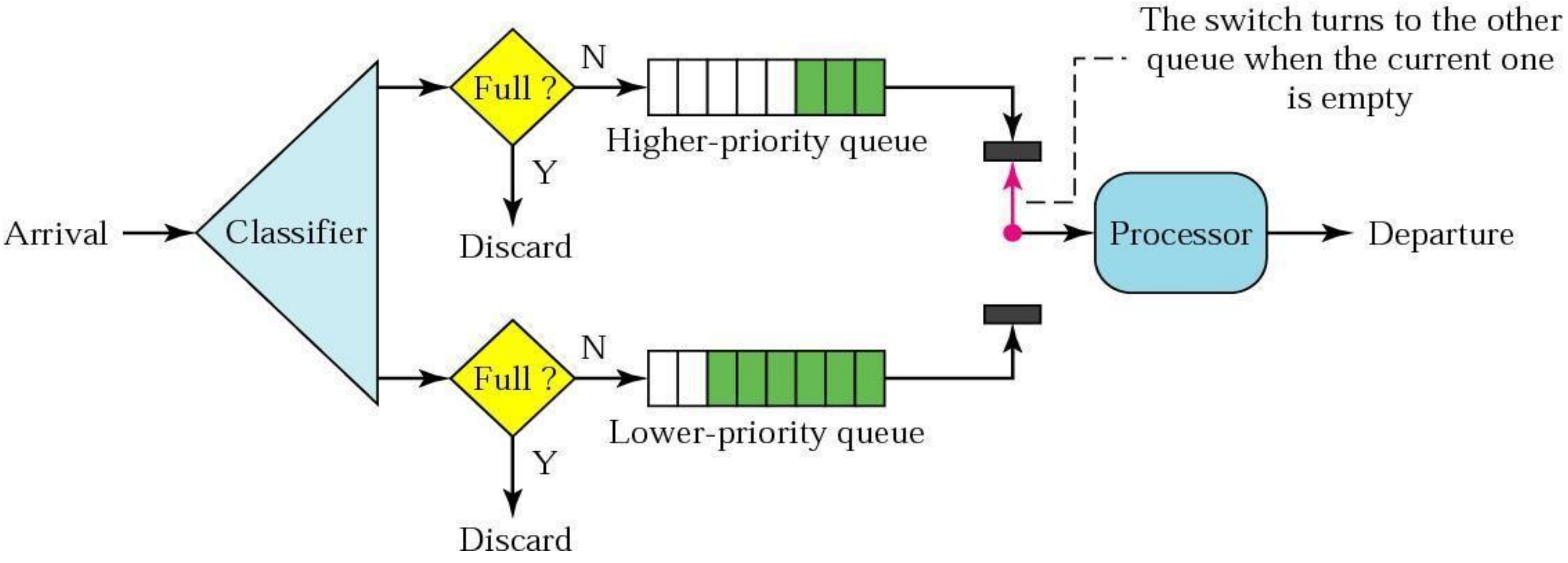
1. FIFO queing:in FIFO queue,packets wait in a buffer until node is ready to process them



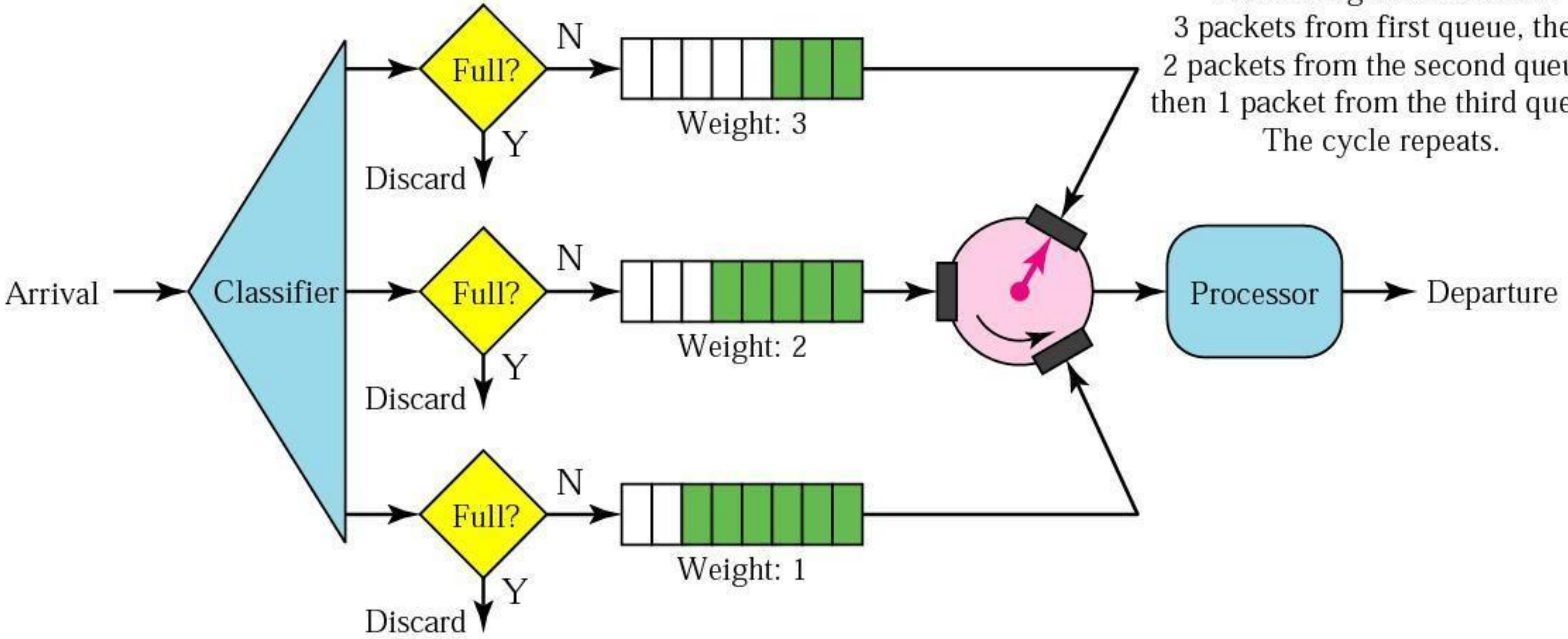
PRIORITY QUEUING

1. In priority queuing, packets are first assigned to a priority class.
2. Each priority class has its own queue.
3. The packets in the highest-priority queue are processed first.
4. Packets in the lowest-priority queue are processed last.

PRIORITY QUEUING



WEIGHTED FAIR QUEUING

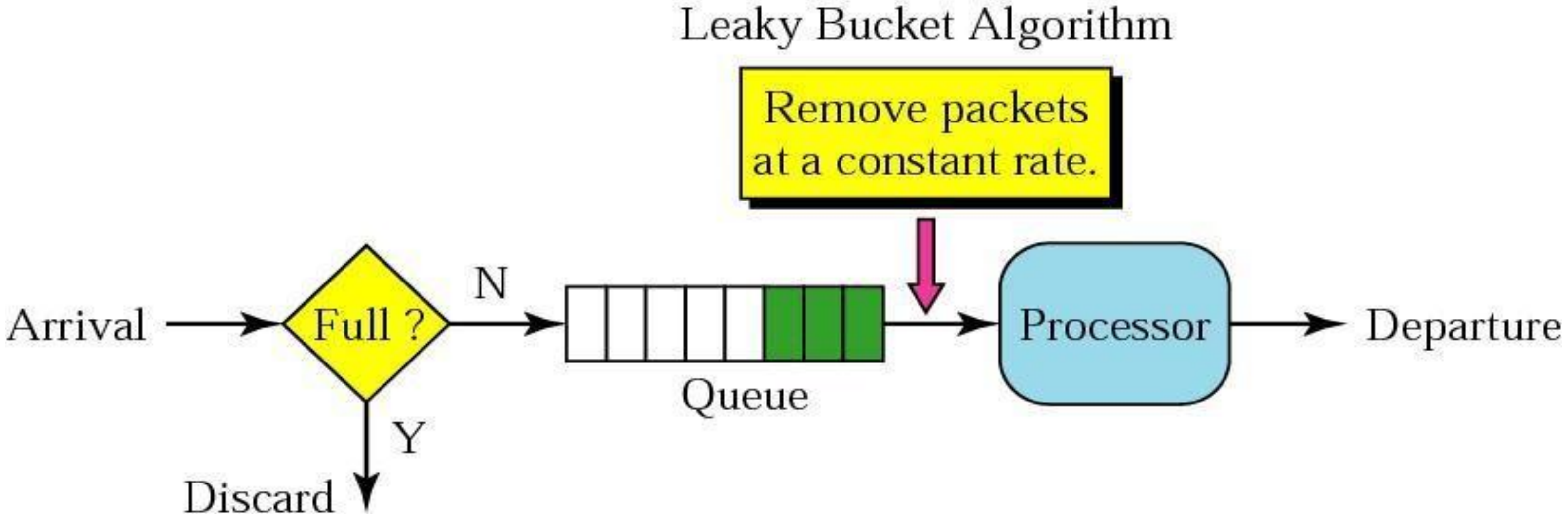


The turning switch selects
3 packets from first queue, then
2 packets from the second queue,
then 1 packet from the third queue,
The cycle repeats.

TRAFFIC SHAPING

1. Traffic shaping is a mechanism to control the amount and the rate of the traffic sent to the network.
2. Two techniques can shape traffic:
   - leaky bucket and
   - token bucket.

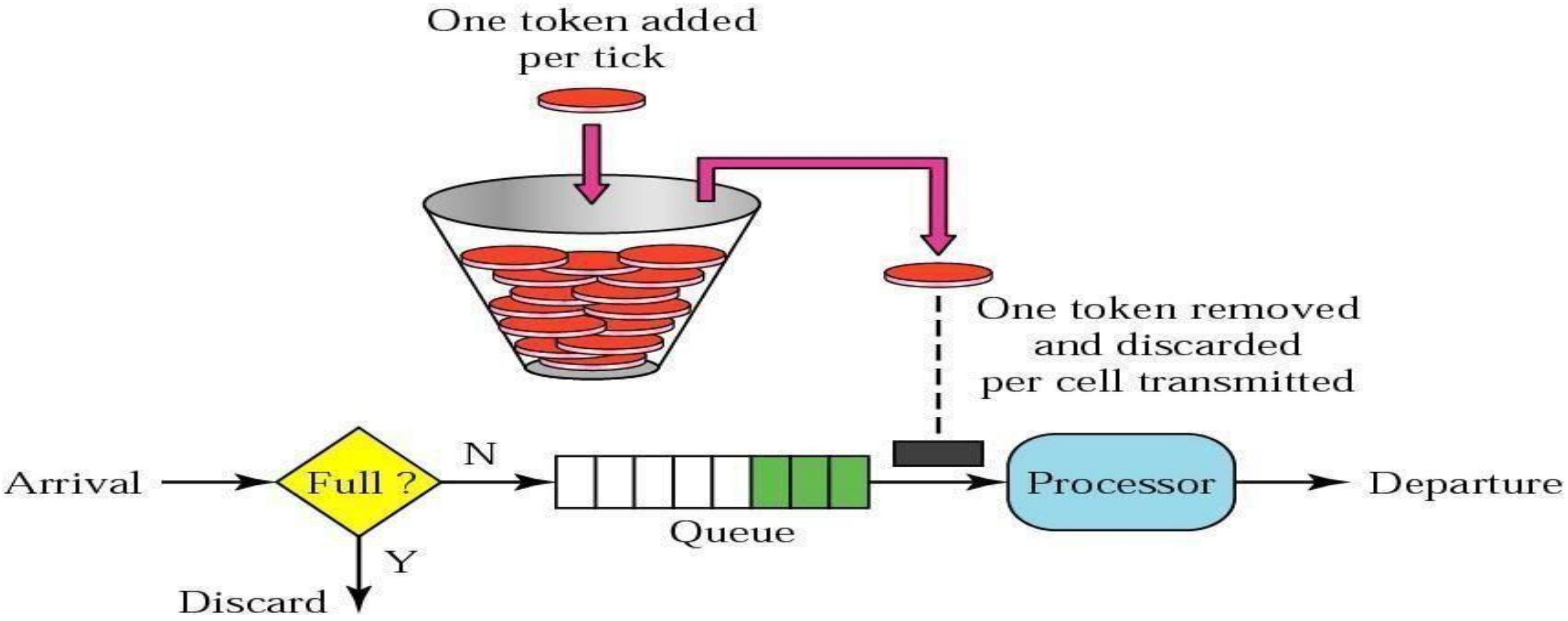
LEAKY BUCKET IMPLEMENTATION



TOKEN BUCKET

1. Leakybucket is very restrictive.
2. Doesn't credit idlehost.
3. token bucket alg allows idle hosts toaccumulate credit for future in the form of tokens.
4. For each tick of clock, system sends n tokens tobucket.
5. System removes 1 token for every cell ofdata sent.
6. **Implemented** by using counter-initialized to 0 & incremented by 1 each time tokenadded
7. Eachtime aunit of data is sent, thecounter is decremented by 1.
8. When the counter is zero, the hostcannot send data.

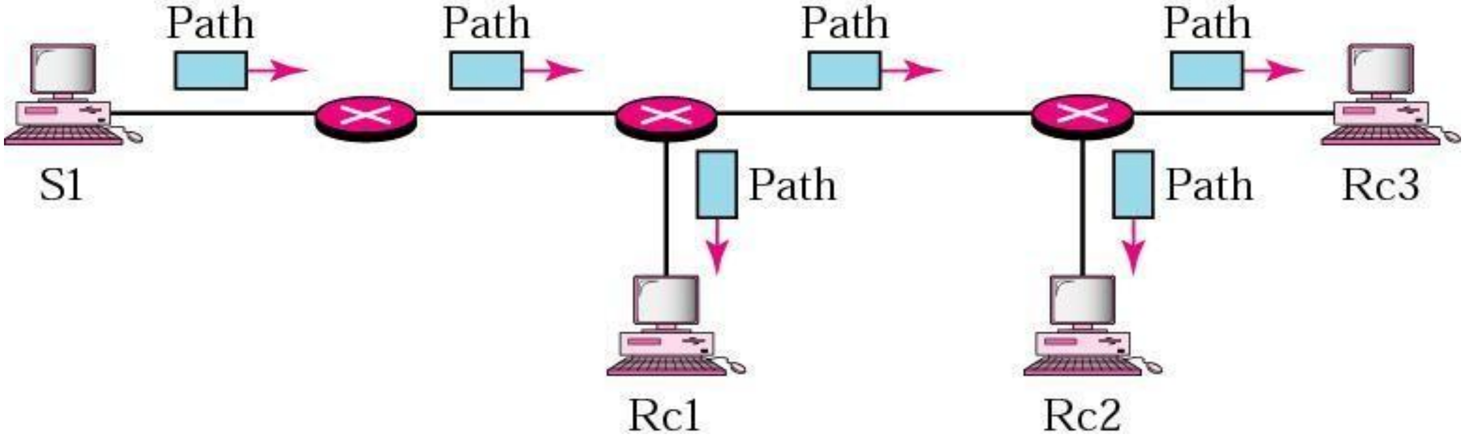
TOKEN BUCKET



1. How can we implement a flow based model over connectionless protocol?
2. Solution is signaling protocol to run over IP that provides signaling
   3. mechanism for making reservation.
4. This protocol resource reservation protocol.
5. **Flow specification** has 2 parts-
   - rspec(resorce specification) → buffer, bandwidth
   - tspec(traffic specification) → traffic characterization

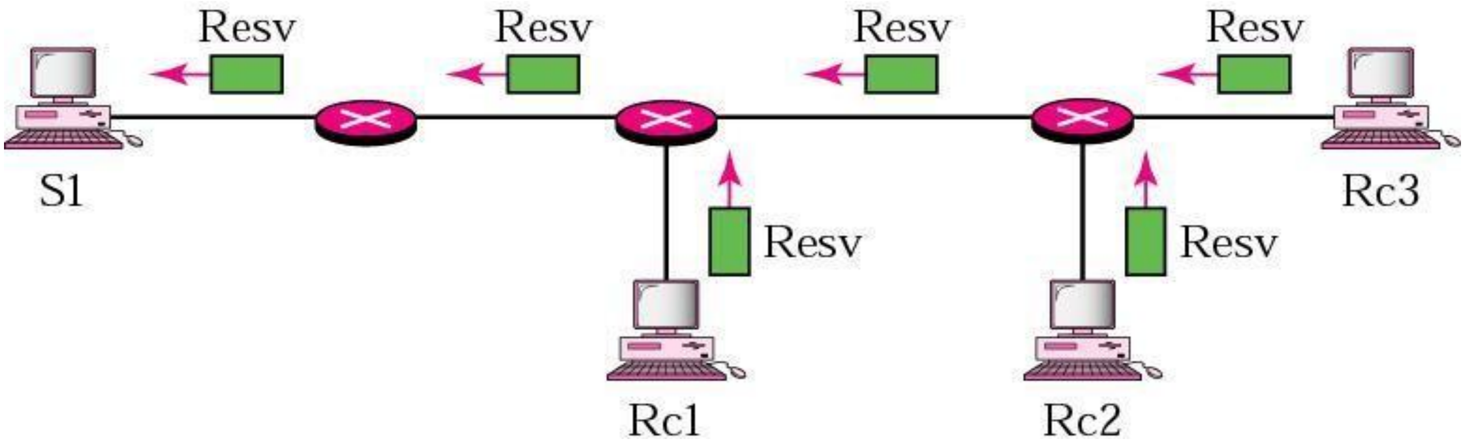
1. Admission: After router rcvs flow specn frm appn it decidesto admit or deny service.
2. Service classes : guaranteed service is designed for realtime traffic that needs minimum end to end delay
3. Controlled load service access: designed for appns that can accept some delays,but they are sensitive to overloaded n/w.ex:file transfer,email,internet access.

RSVP



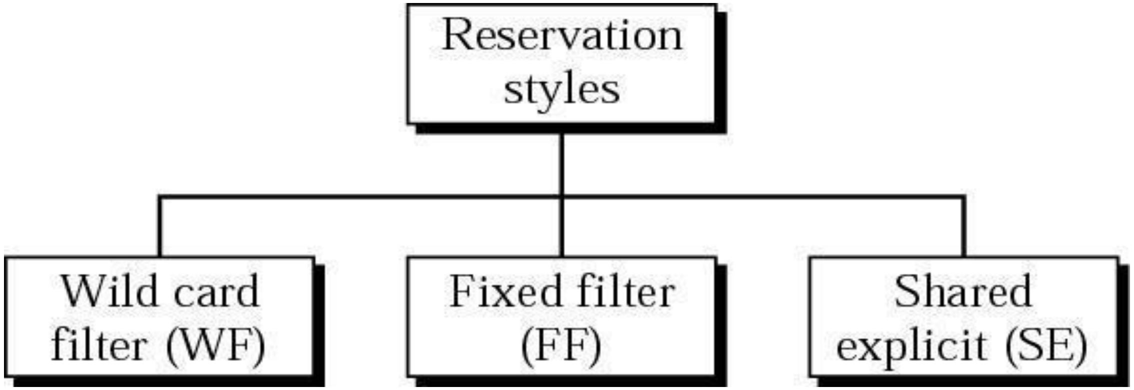
RESV MESSAGES

1. When rcvr rceives path msg,it sendsrecv msgwhich trvels toward sender andmakes rr on the routers that supportrsvp.



RESERVATION STYLES

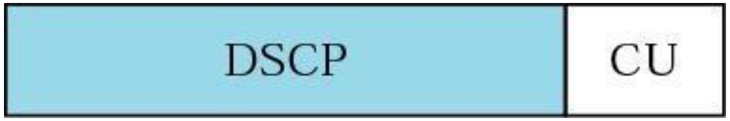
When there is more than one flow the router needs to make reservation to accommodate all of them



1. In wf,router creates single reservation for all senders. reservation is basedon largerrequest.
2. In ff, router creates distinctreservation forflow.
3. In se, router creates single reservation which canbeshared by set of flows.

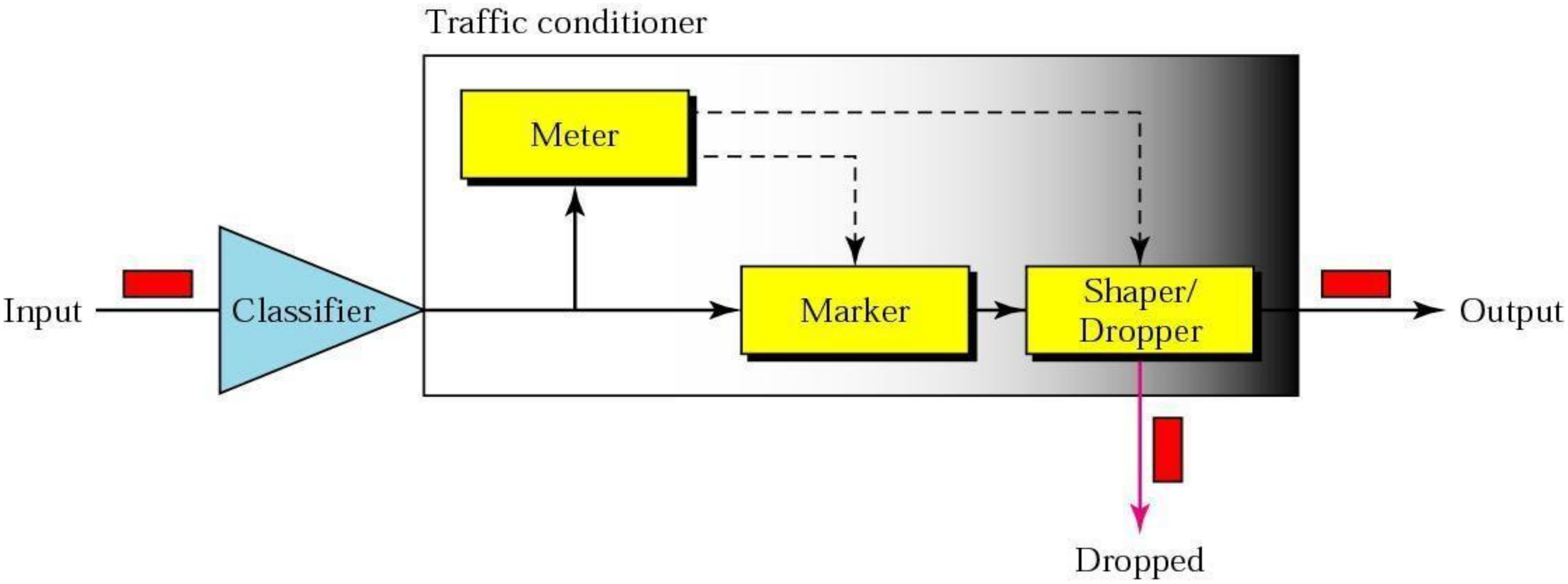
DS FIELD

1. In diffserv each packet contains DS field whose value is set at the boundary of n/w by host or first router designated as boundary router.



1. Differentiated services core point (DSCP) defines per hop behviour.
2. cu-currently unused.
3. To implement diffserv DS node uses traffic conditioners such as
   - Meters
   - Markers
   - shapers.
4. Meters check to see if incmg flow matches negotiated traffic profile
5. Marker can mark a packet that is using best effort delivery.
6. Shaper uses infn recvd from meter to reshape the traffic
7. Dropper works as a shaper with no buffer ,discards the packets.

TRAFFIC CONDITIONER

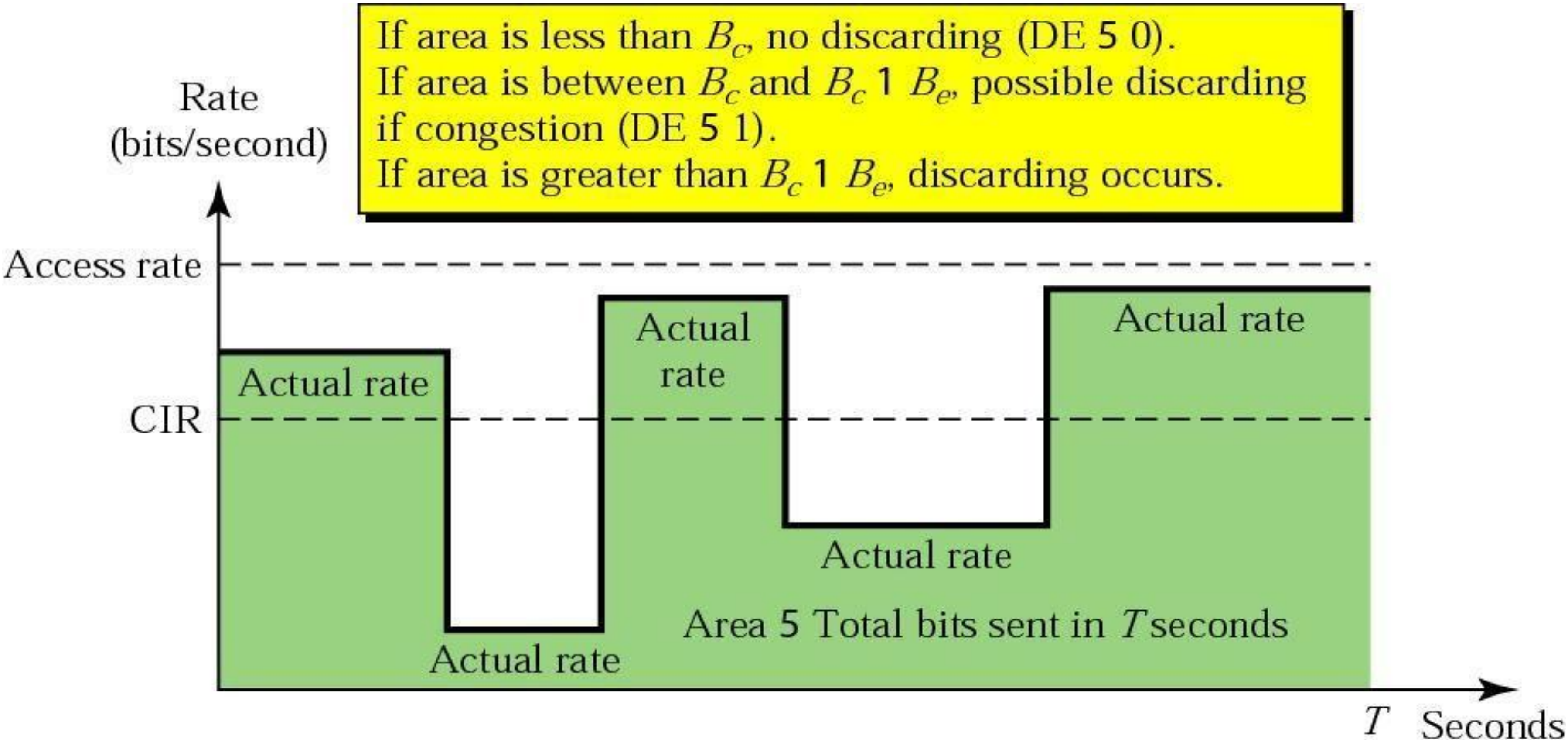


QoS IN SWITCHED NETWORKS

QoSin FrameRelay

1. Four different attributes to control traffic have been devised in Frame Relay:
   - access rate,
   - committed burst size Be'
   - committed information rate (CIR),
   - excess burst size Be'
2. For every connection access rate which depends on the bw of channel is defined.
3. Committed burst size Bc: maximum no. of bits in predefined time that n/w is committed to transfer without discarding any frame r setting de bit.
4. Committed info rate(CIR) defines avg rate inbits per sec.
   - CIR=Bc/T
5. Excess burst size Be: max no. of bits in excess of bc that a usercan send during a predefined time.

USER RATE IN RELATION TO BC AND BC + BE



If area is less than B_c, no discarding (DE 5 0).
If area is between B_c and B_c 1 B_e, possible discarding if congestion (DE 5 1).
If area is greater than B_c 1 B_e, discarding occurs.

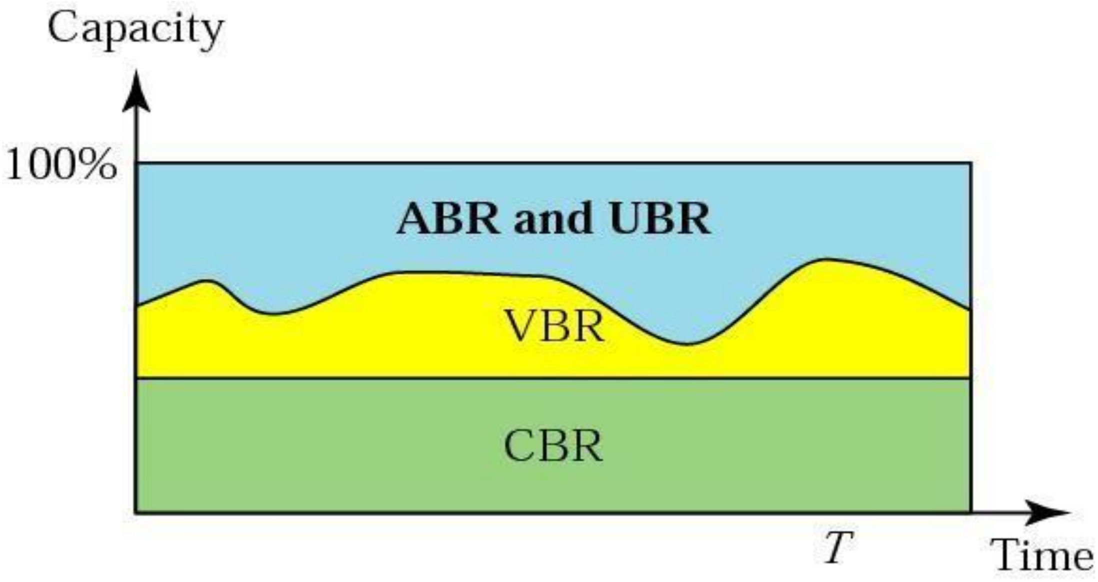
QoS IN ATM

1. The QoS in ATM is based on the
   - class,
   - user-related attributes,
   - and network-related attributes

ATM:SERVICE CLASSES

1. CBRdesigned for custmers who need realtime audio,video services.
2. VBRclass is divided into two subclasses:real-time
3. (VBR-RT)and non-real-time (VBR-NRT).
4. VBR-RTis designed for those users who need real-time services
5. VBR-NRTis designed for those users who do not needreal- time services
6. Abr (avilable bit rate)delivers cells atminimum rate.
7. Unspecified bit rate(UBR) is abest effort delivery servicethat does not guarantee anything

RELATIONSHIP OF SERVICE CLASSES TO THE TOTAL CAPACITY

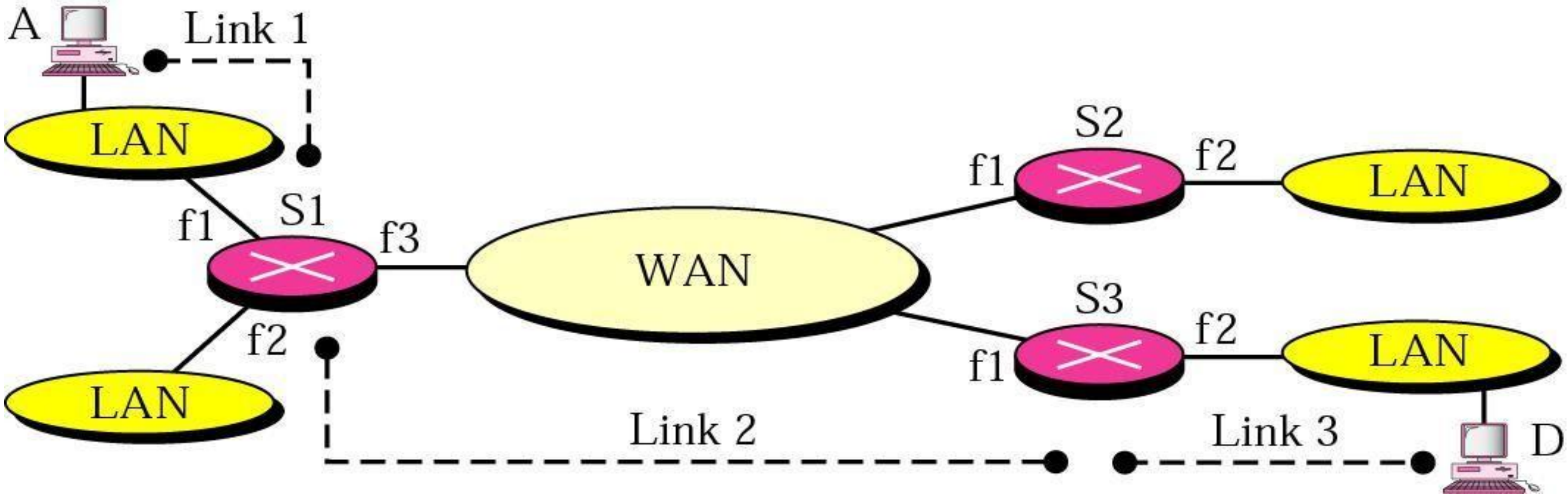


UNIT -IV

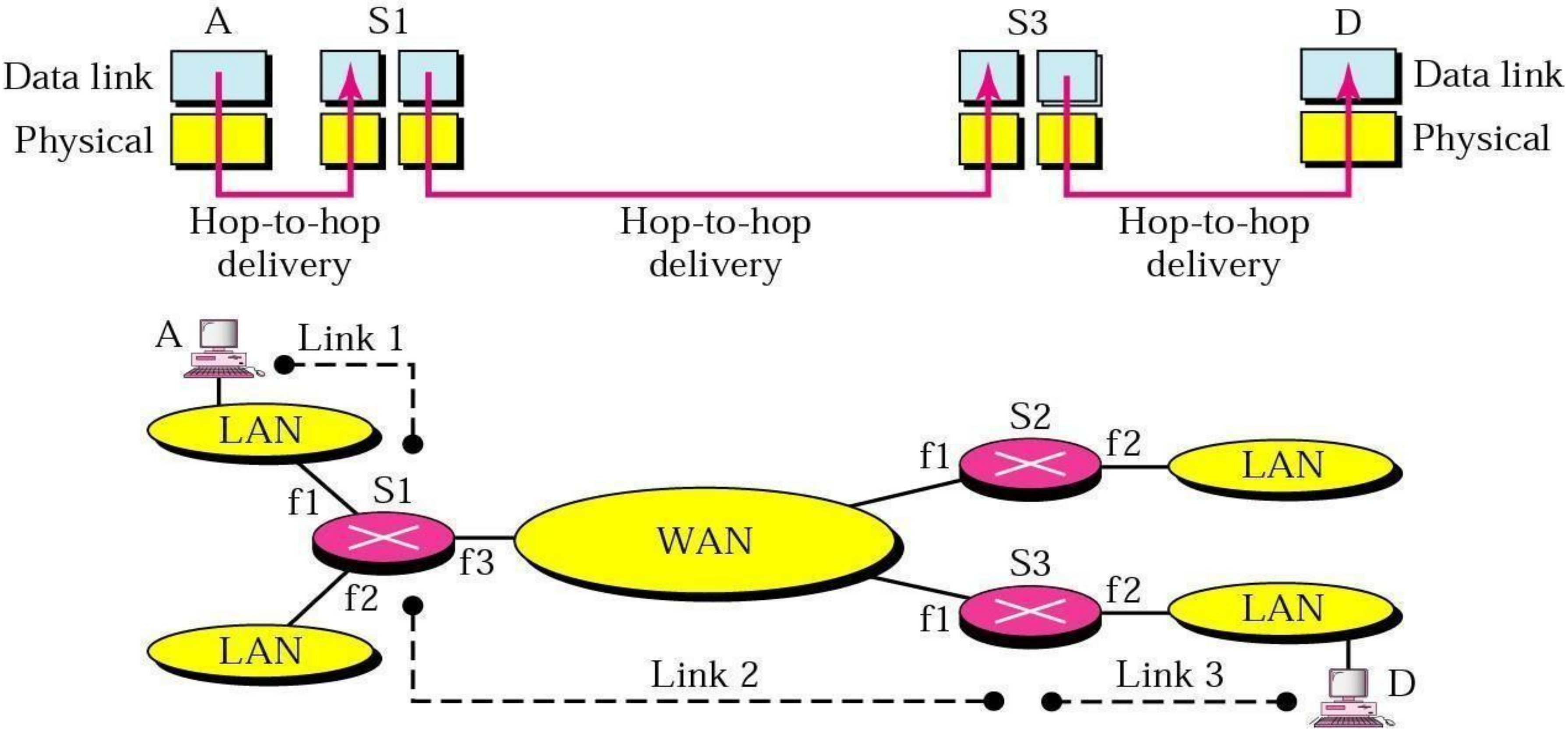
Internetworking, Transport Layer

INTERNETWORK

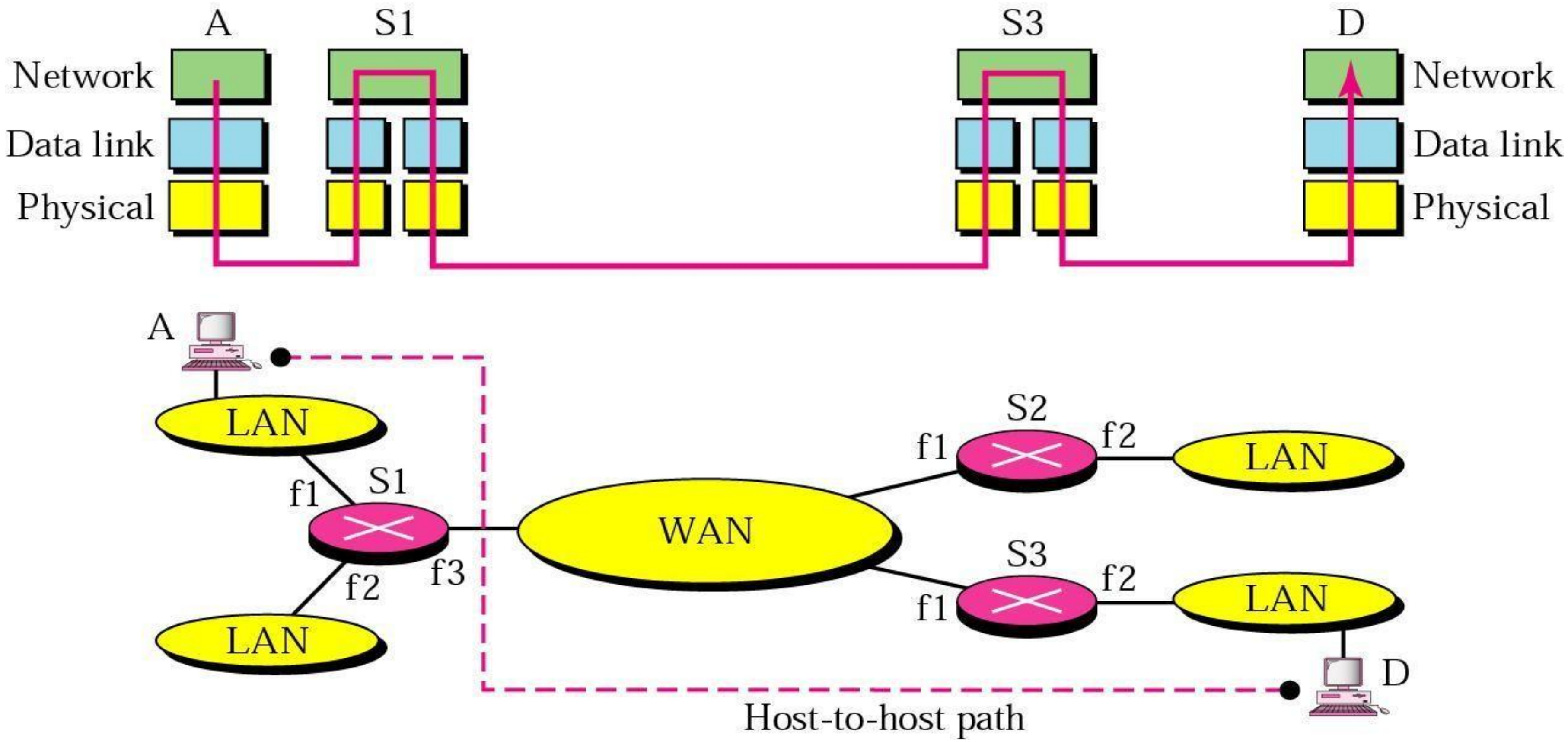
1. Here Intern/w is made up of 4 lans and 1 wan.to solve prblm of delivery through several links,n/w layer was designed for host to host delivery and routing packets.



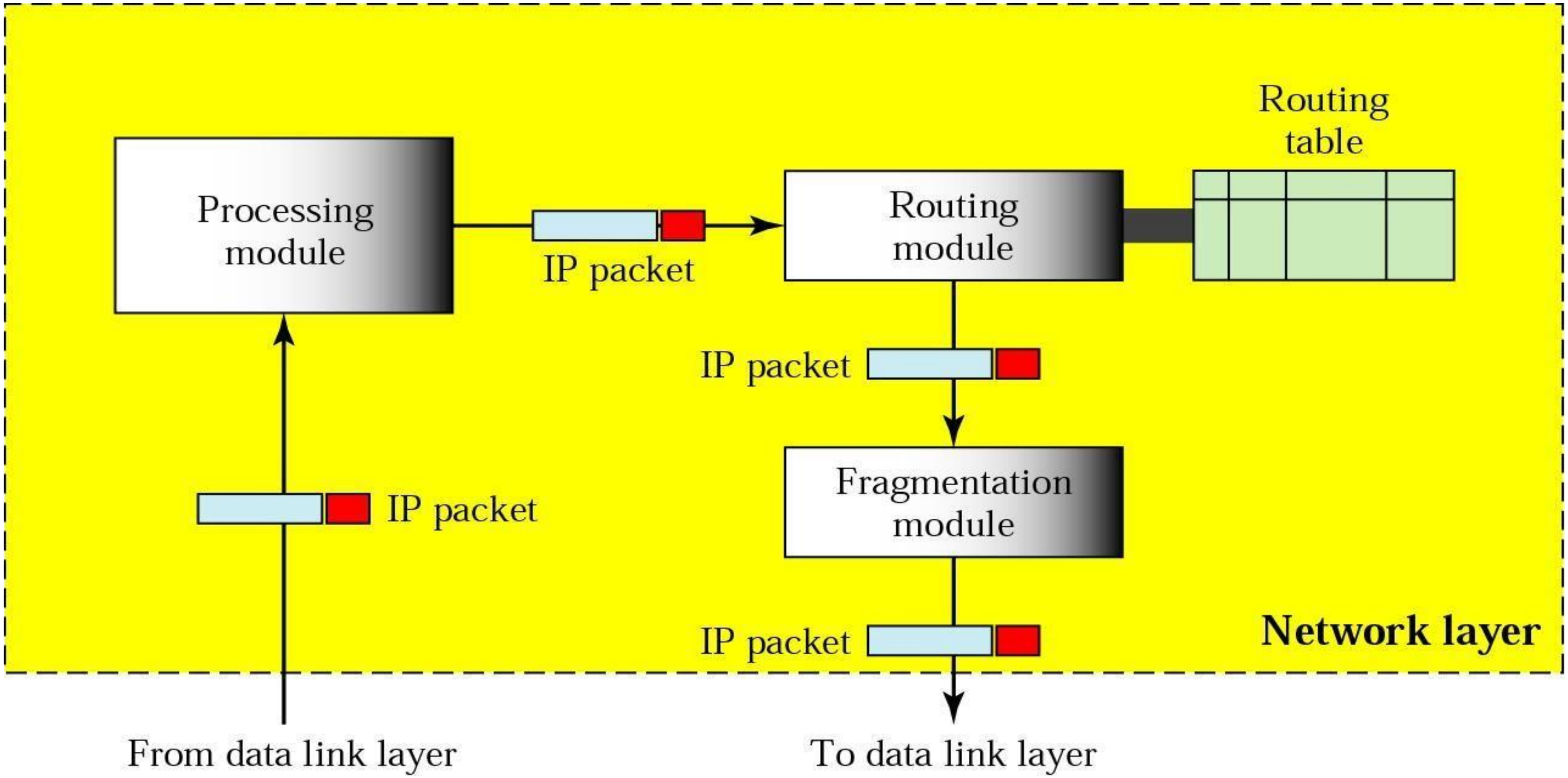
LINKS IN AN INTERNETWORK



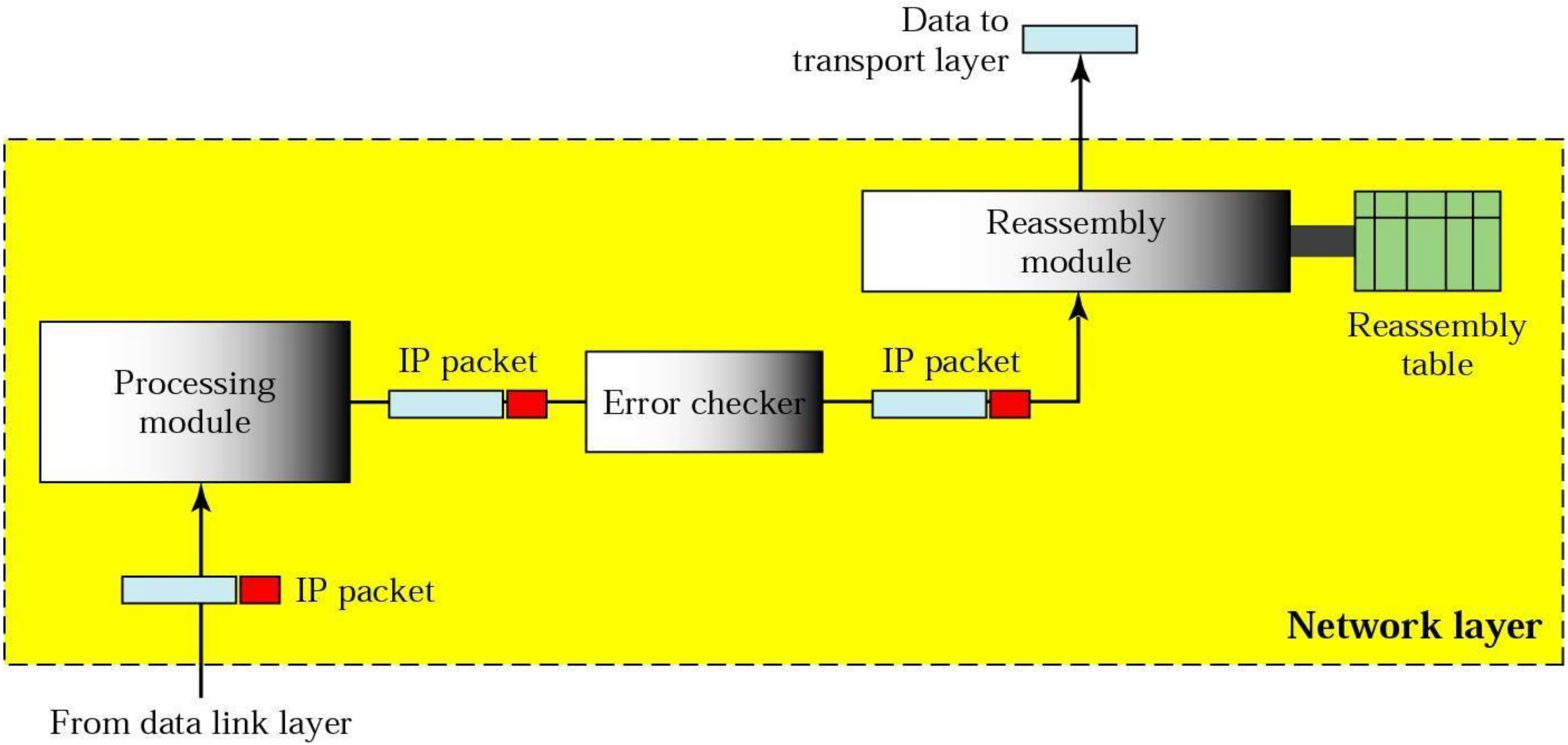
NETWORK LAYER IN ANINTERNETWORK



NETWORK LAYER AT A ROUTER



NETWORK LAYER AT THE DESTINATION



IPV4

1. The Internet Protocol version 4 (IPv4) is the delivery mechanism used by the TCP/IP protocols.
2. IPv4 is an unreliable and connectionless datagram protocol-a best-effort delivery service.
3. The term best-effort means that IPv4 provides no error control or flow control (except for error detection on the header).
4. IPv4 assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with noguarantees.

   If reliability is important, IPv4 must be paired with a reliable protocol suchasTCP.

DATAGRAM

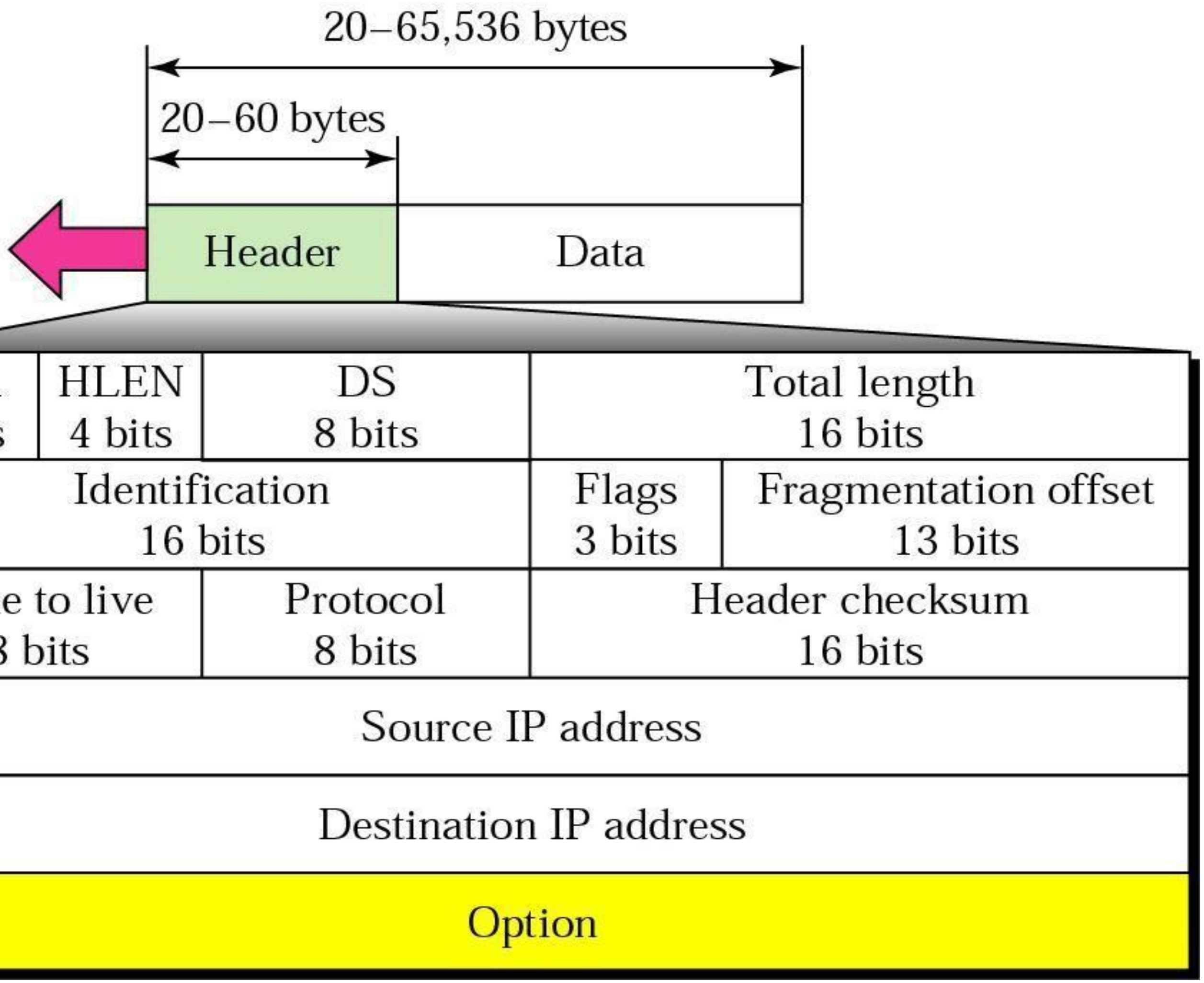
1. Packets in the IPv4 layer are called datagram's.

2. A datagram is a variable-length packet consisting of two parts: header and data.

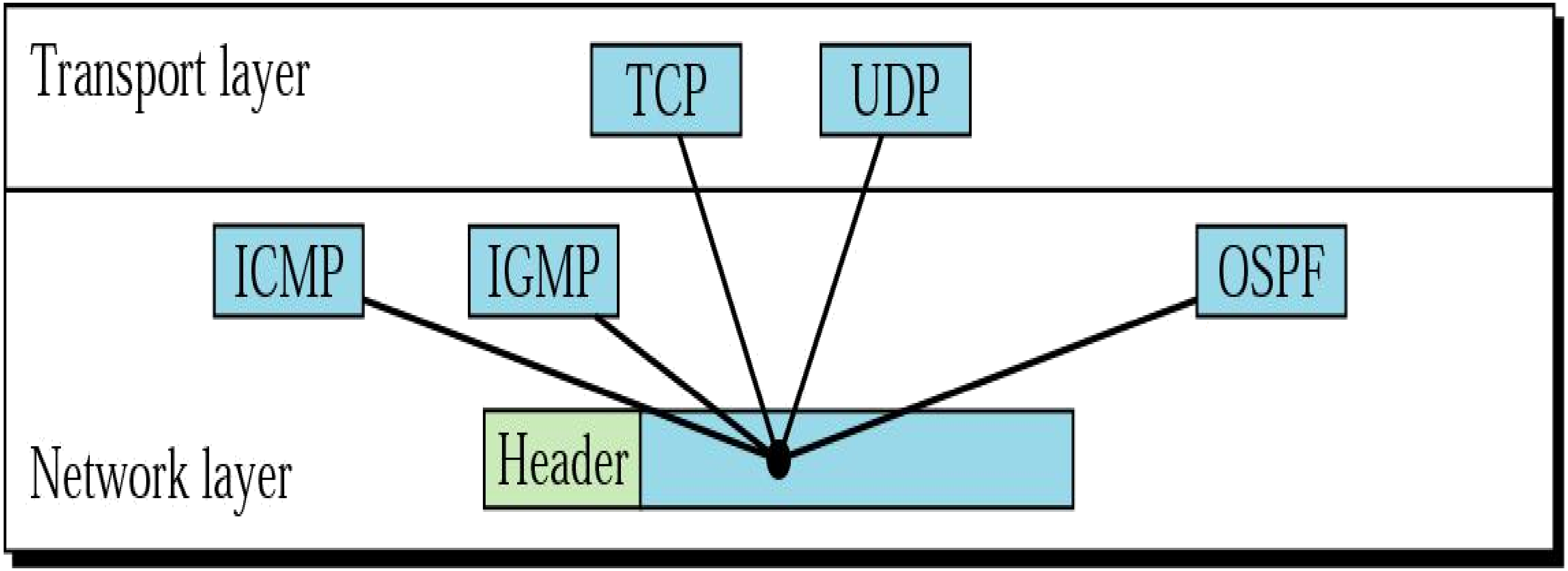
3. The header is 20 to 60 bytes in length and contains information essential to routing and delivery.

4. It is customary in TCP/IP to show the header in 4-byte sections.

IP DATAGRAM



<table>
<tr><td>VER
4 bits</td><td>HLEN
4 bits</td><td>DS
8 bits</td><td colspan="2">Total length
16 bits</td></tr>
<tr><td colspan="3">Identification
16 bits</td><td>Flags
3 bits</td><td>Fragmentation offset
13 bits</td></tr>
<tr><td colspan="2">Time to live
8 bits</td><td>Protocol
8 bits</td><td colspan="2">Header checksum
16 bits</td></tr>
<tr><td colspan="5">Source IP address</td></tr>
<tr><td colspan="5">Destination IP address</td></tr>
<tr><td colspan="5">Option</td></tr>
</table>


Transport layer
TCP
UDP
ICMP
IGMP
OSPF
Network layer
Header

FRAGMENTATION

1. A datagram can travel through different networks. Each router de-capsulates the IPv4 datagram from the frame it receives, processes it, and then encapsulates it in another frame.
2. The format and size of the received frame depend on the protocol used by the physical network through which the frame has just traveled.
3. The format and size of the sent frame depend on the protocol used by the physical network through which the frame is going to travel.
4. For example, if a router connects a LAN to a WAN, it receives a frame in the LAN format and sends a frame in the WAN format.

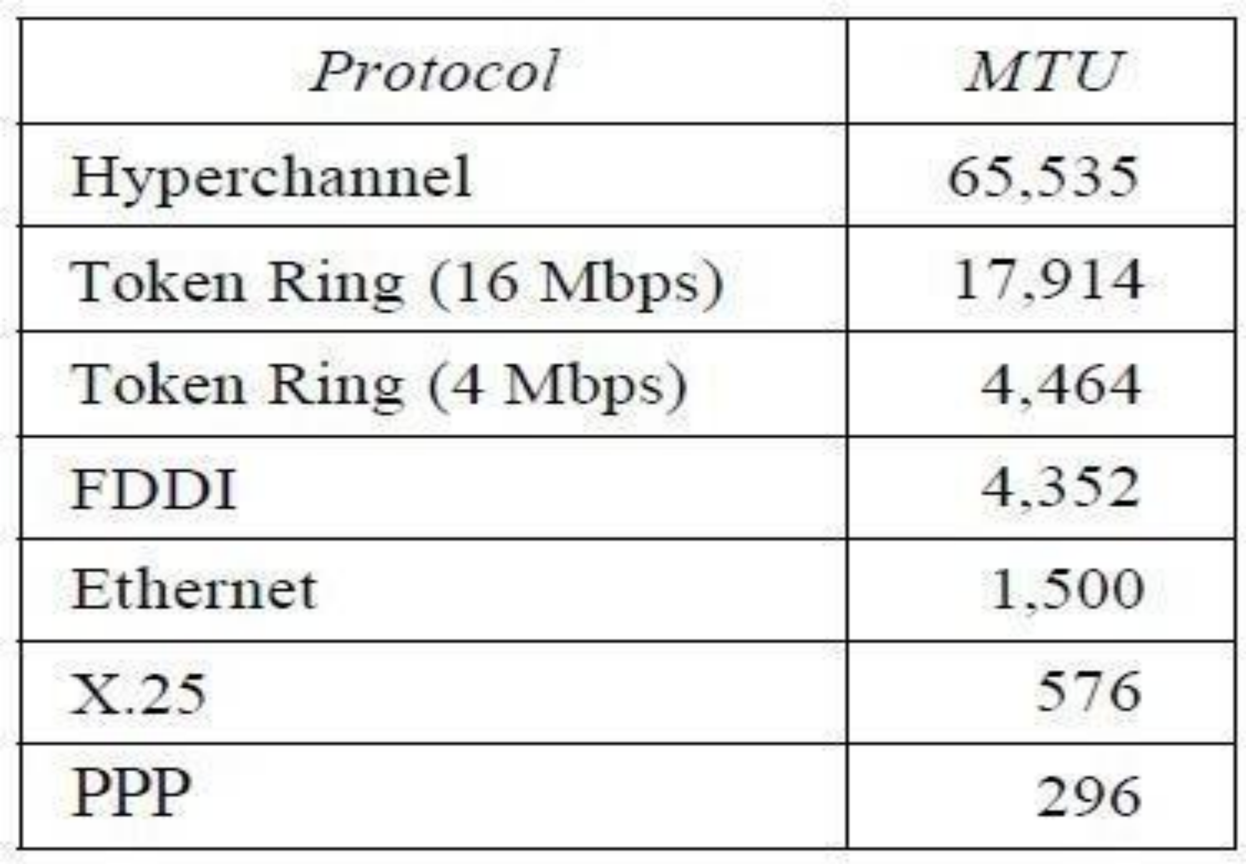
MAXIMUM TRANSFER UNIT (MTU)

1. Each data link layer protocol has its own frame format in most protocols.

2. One of the fields defined in the format is the maximum size of the data field.

3. In other words, when a datagram is encapsulated in a frame, the total size of the datagram must be less than this maximum size

THEVALUE OF THE MTU DEPENDS ONTHE PHYSICAL NETWORK PROTOCOL.



Protocol	*MTU*
Hyperchannel	65,535
Token Ring (16 Mbps)	17,914
Token Ring (4 Mbps)	4,464
FDDI	4,352
Ethernet	1,500
X.25	576
PPP	296

1. To make the IPv4 protocol independent of the physical network, the designers decided to make the maximum length of the IPv4 datagram equal to **65,535 bytes.**

2. When a datagram is fragmented, each fragment has its own header with most of the fields repeated, but with some changed.

3. A fragmented datagram may itself be fragmented if it encounters a network with an even smaller MTU In IPv4, a datagram can be fragmented by the source host or any router in the path

4. The reassembly of the datagram, however, is done only by the destination host because each fragment becomes an independent datagram.

1. **Identification**. This 16-bit field identifies a datagram originating from the source host.
   - The combination of the identification and source IPv4 address must uniquely define a datagram as it leaves the source host.

1. **Flags.** This is a 3-bit field.
   - The first bit is reserved.
   - The second bit is called the **do not fragment bit.** If its value is 1, the machine must not fragment the datagram.
   - If it cannot pass the datagram through any available physical network, it discards the datagram and sends an ICMP error message to the source host.

     If its value is 0, the datagram can be fragmented if necessary.

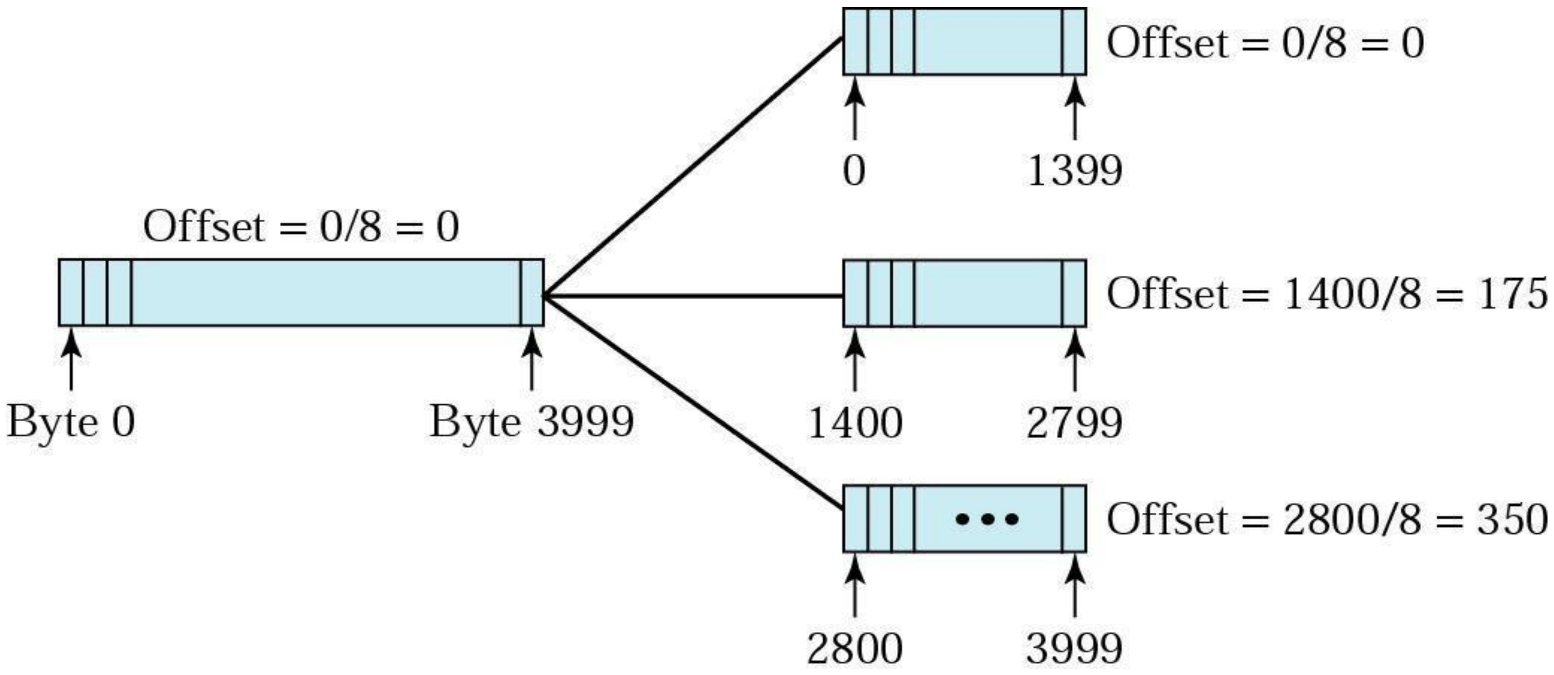
- The third bit is called the more fragment bit. If its value is 1, it means the datagram is not the last fragment;
  - there are more fragments after this one.
  - If its value is 0, it means this is the last or only fragment

1. Figure shows a datagram with a data size of 4000 bytes fragmented into three fragments.
2. The bytes in the original datagram are numbered 0 to 3999.
3. The first fragment carries bytes 0 to 1399.
4. The offset for this datagram is 0/8 =O.

5. The second fragment carries bytes 1400 to 2799; the offset value for this fragment is 1400/8 =175.

1. Finally, the third fragment carries bytes 2800 to 3999. The offset
   2. value for this fragment is 2800/8=350.
3. Remember that the value of the offset is measured in units of 8 bytes.
4. This is done because the length of the offset field is only 13 bits and cannot represent a sequence of bytes greater than 8191.
5. This forces hosts or routers that fragment datagram's to choose a fragment size so that the first bytenumber is divisible by 8.

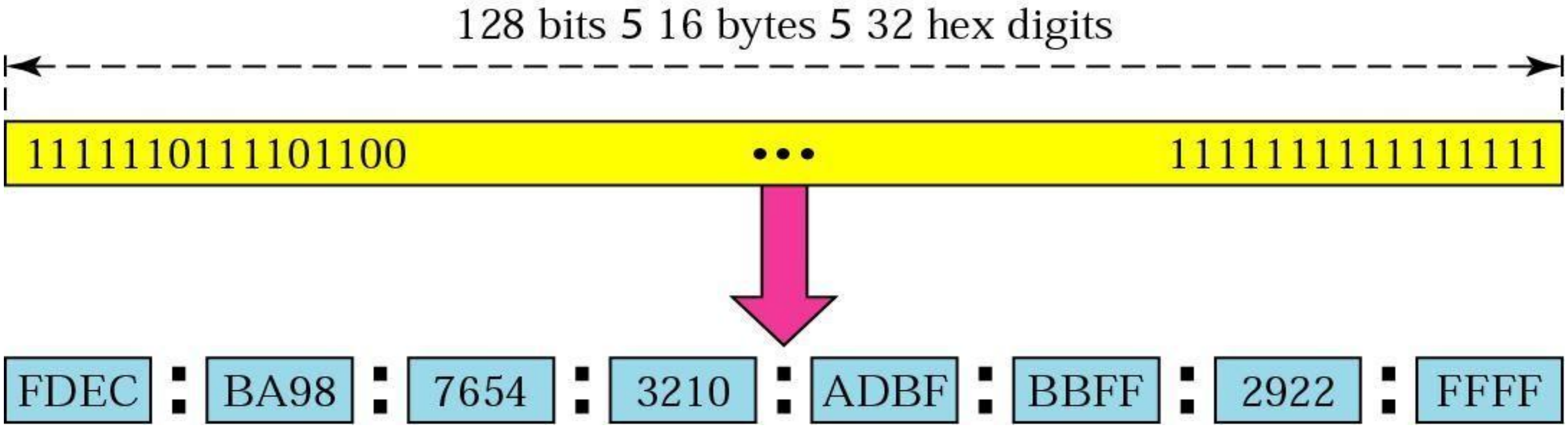
FRAGMENTATION EXAMPLE



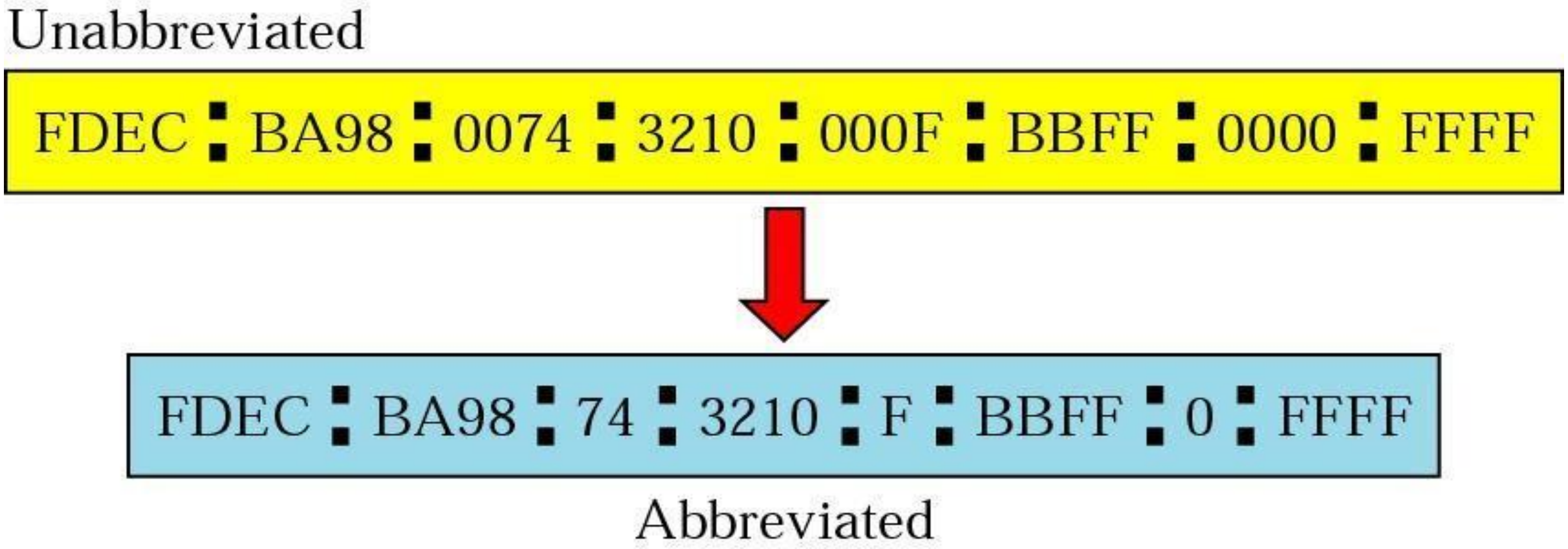
IPV4 DEFICIENCIES:

1. IPV4has a two-level address structure categorized into five classes. The use of address space is inefficient.
2. The internet must accommodate real-time audio and video transmission. This type of transmission requires minimum delay strategies and reservation of resources not provided in the ipv4design.
3. The internet must accommodate encryption and authentication of data for some application. No security mechanism was provided by IPv4

IPV6 ADDRESS



ABBREVIATED ADDRESS



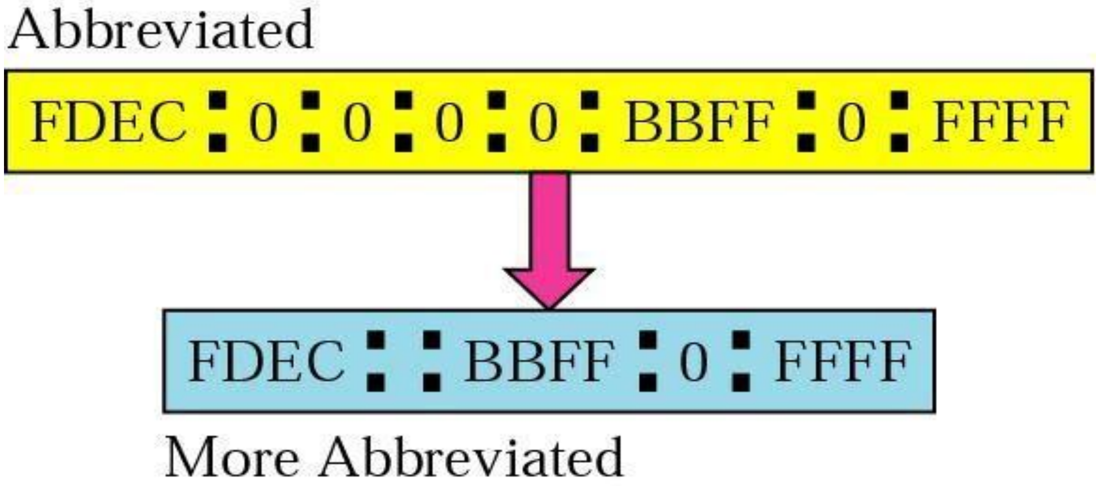
Unabbreviated

FDEC : BA98 : 0074 : 3210 : 000F : BBFF : 0000 : FFFF

FDEC : BA98 : 74 : 3210 : F : BBFF : 0 : FFFF

Abbreviated

ABBREVIATED ADDRESS WITH CONSECUTIVE ZEROS



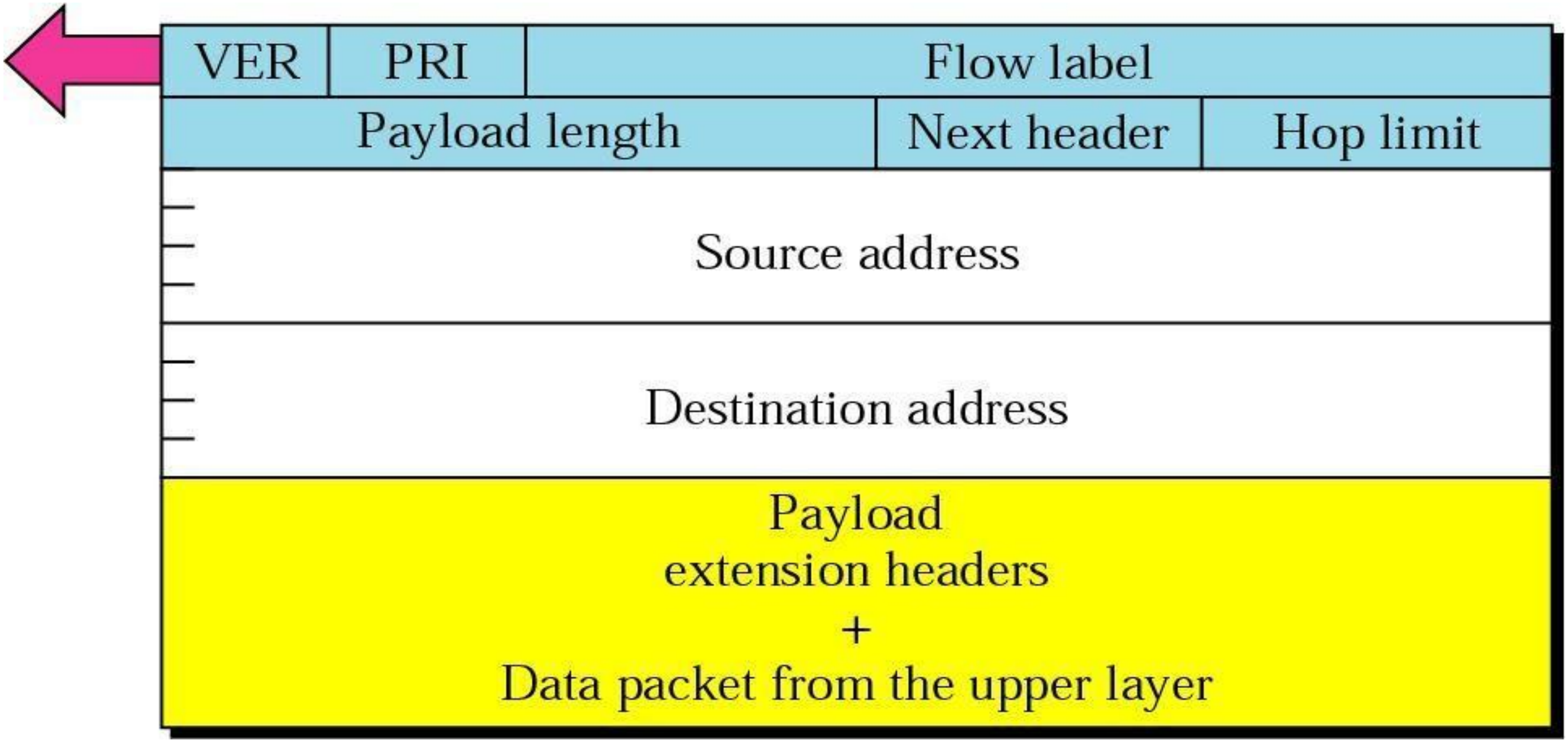
Abbreviated

FDEC : 0 : 0 : 0 : 0 : BBFF : 0 : FFFF

FDEC : : BBFF : 0 : FFFF

More Abbreviated

FORMAT OF AN IPV6 DATAGRAM



VER

PRI

Flow label

Payload length

Next header

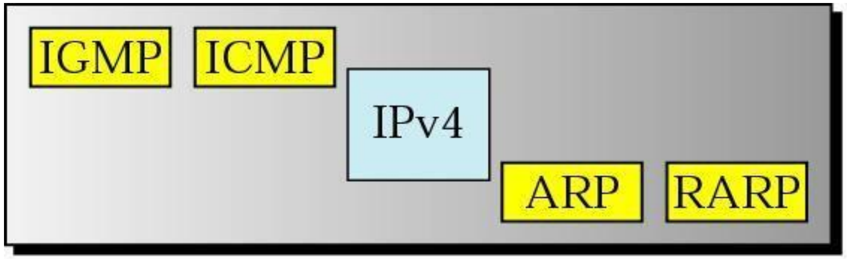
Hop limit

Source address

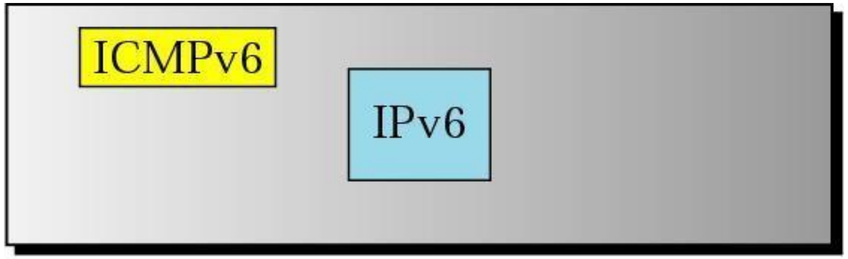
Destination address

Payload
extension headers
+
Data packet from the upper layer

COMPARISON OF NETWORK LAYERS IN VERSION 4 AND VERSION 6

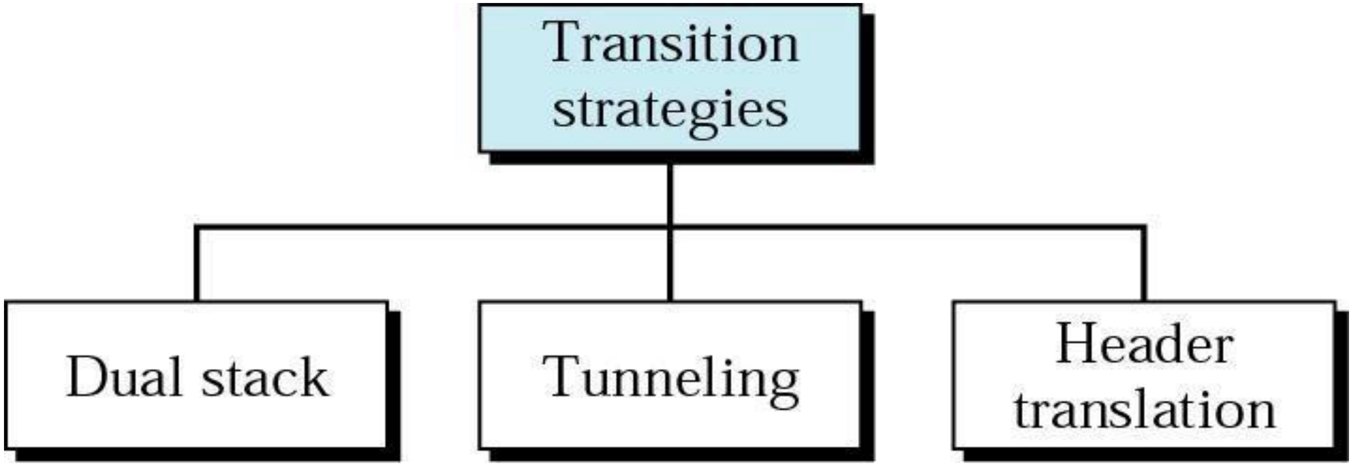


Network layer in version 4

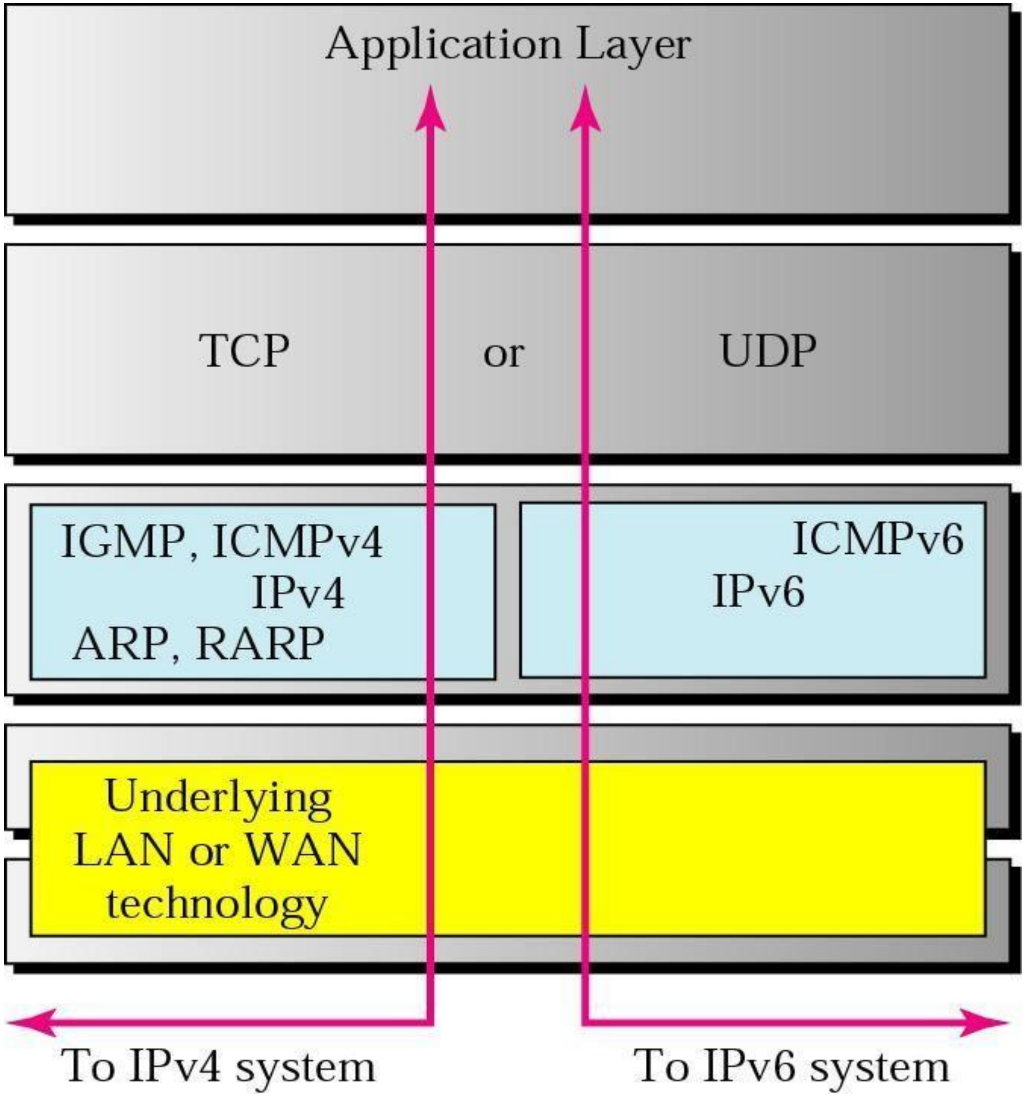


Network layer in version 6

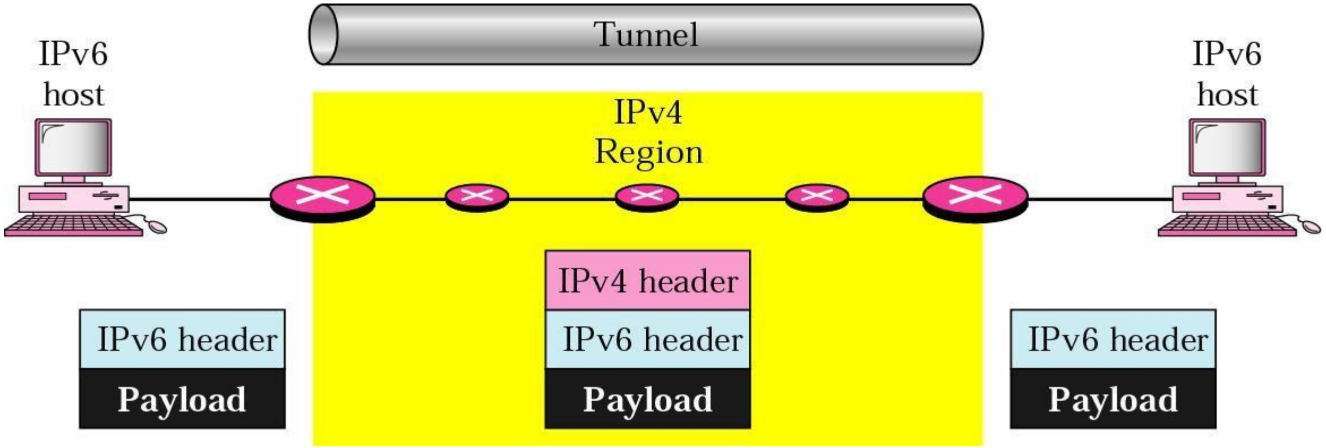
THREE TRANSITION STRATEGIES



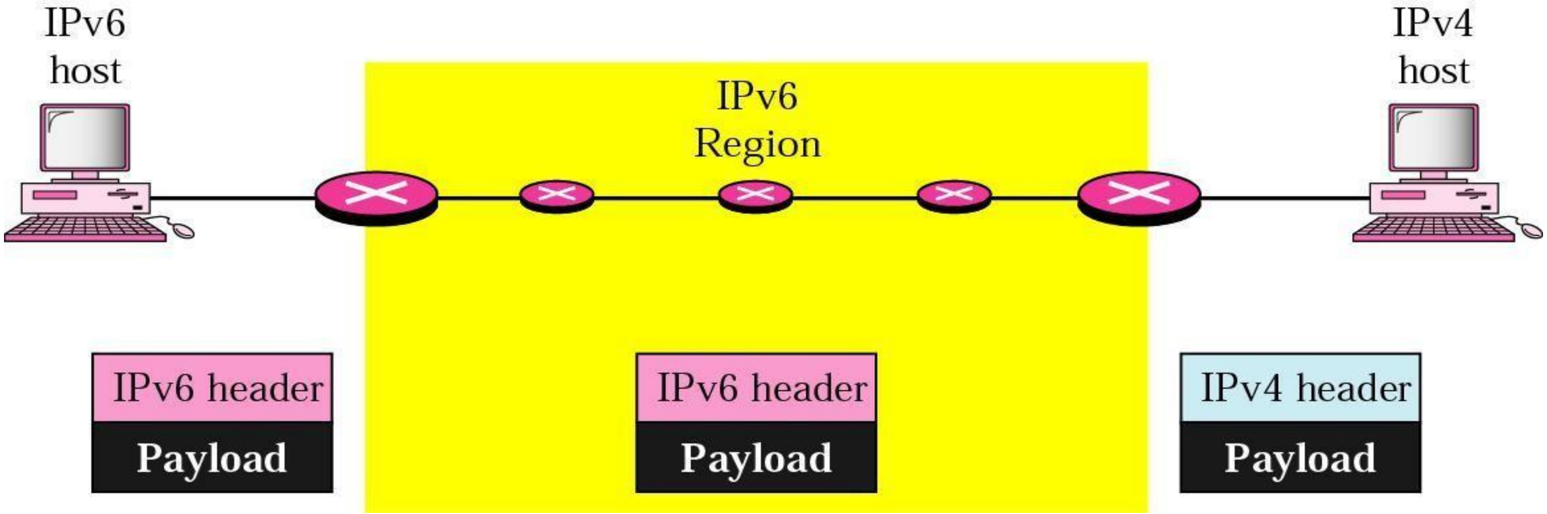
THREE TRANSITION STRATEGIES



TUNNELING


Tunnel
IPv6
host
IPv4
Region
IPv6
host
IPv6 header
Payload
IPv4 header
IPv6 header
Payload
IPv6 header
Payload

HEADER TRANSLATION



ARP INTRODUCTION

1. An internet is made of a combination of physical networks connected by internetworking devices such as routers.
2. A packet starting from a source host may pass through several different physical networks before finally reaching the destination host.
3. The hosts and routers are recognized at the network level by their logical (IP) addresses.
4. A physical address is a local address. It must be unique locally, but is not necessarily unique universally.
5. It is called a physical address because it is usually (but not always) implemented in hardware.
6. An example of a physical address is the 48-bit MAC address in the Ethernet protocol, which is imprinted on the NIC installed in the host or router

MAPPING

1. We need to be able to map a logical address to its corresponding physical address and vice versa.
2. To implement these changes, a static mapping table must be updated periodically. This overhead could affect network performance.
3. These can be done by using either
    1. static or
    2. dynamic mapping.

STATIC MAPPING

1. Static mapping involves in the creation of a table that associates a logical address with a physical address.
2. This table is stored in each machine on the network. Each
3. machine that knows, the IP address of another machine but not its physical address
4. This has some limitations because physical addresses may change in the following ways:
   - 1. A machine could change its NIC, resulting in a new physical address.
   - 2. In some LANs, such as LocalTalk, the physical address changes every
   - time the computer is turned on.
   - 3. A mobile computer can move from one physical network to another, resulting in a change in its physical address
5. To implement these changes, a static mapping table must be updated periodically. This overhead could affect network performance.

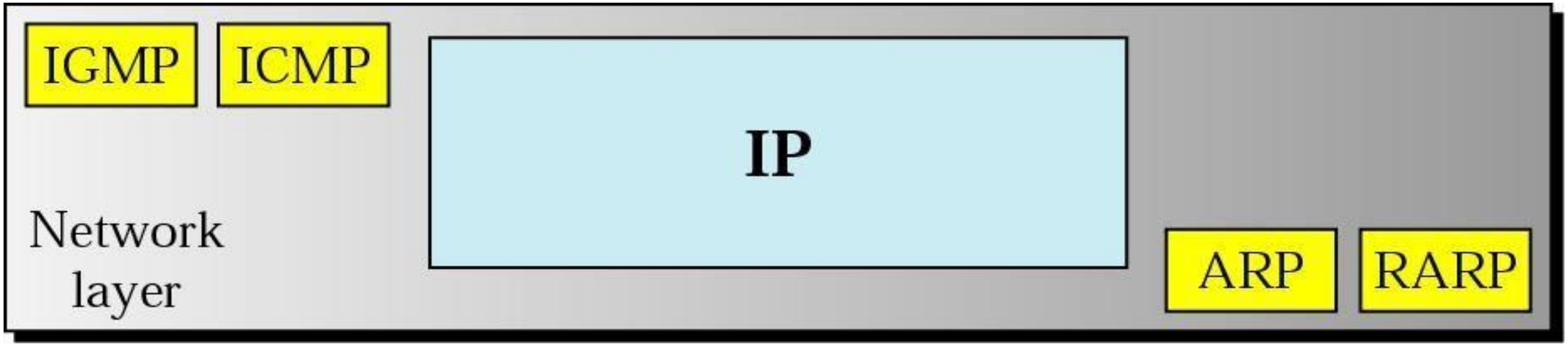
MAPPING LOGICAL TO PHYSICAL ADDRESS: ARP

1. In dynamic mapping each time a machine knows one of the two addresses (logical or physical), it can use a protocol to find the other one.

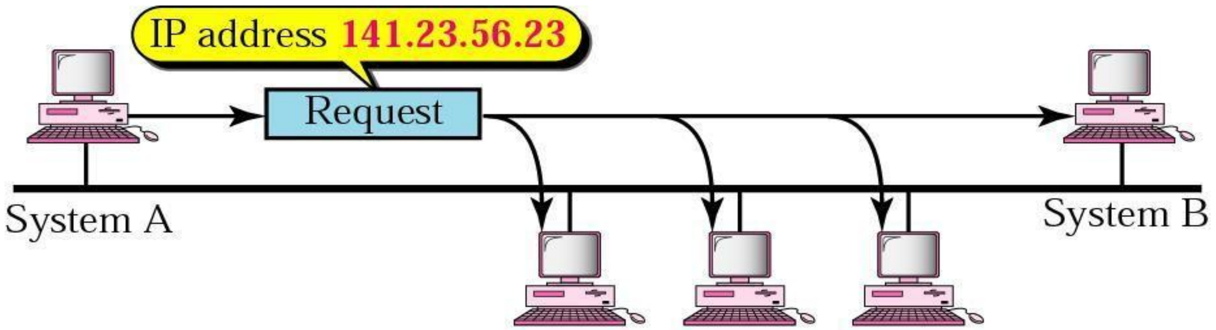
2. Two protocols have been designed to perform dynamic mapping:

   - Address Resolution Protocol(ARP)
   - Reverse Address Resolution(RARP)

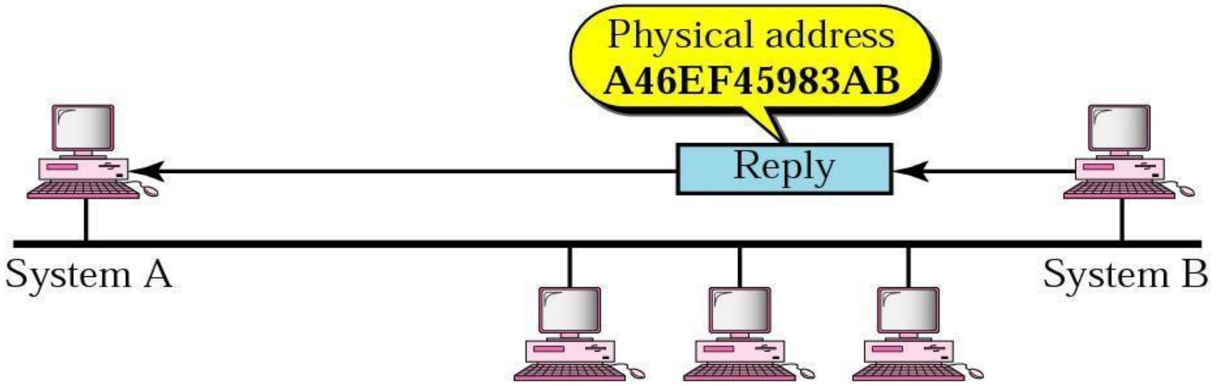
PROTOCOLS AT NETWORK LAYER



ARP OPERATION



a. ARP request is broadcast



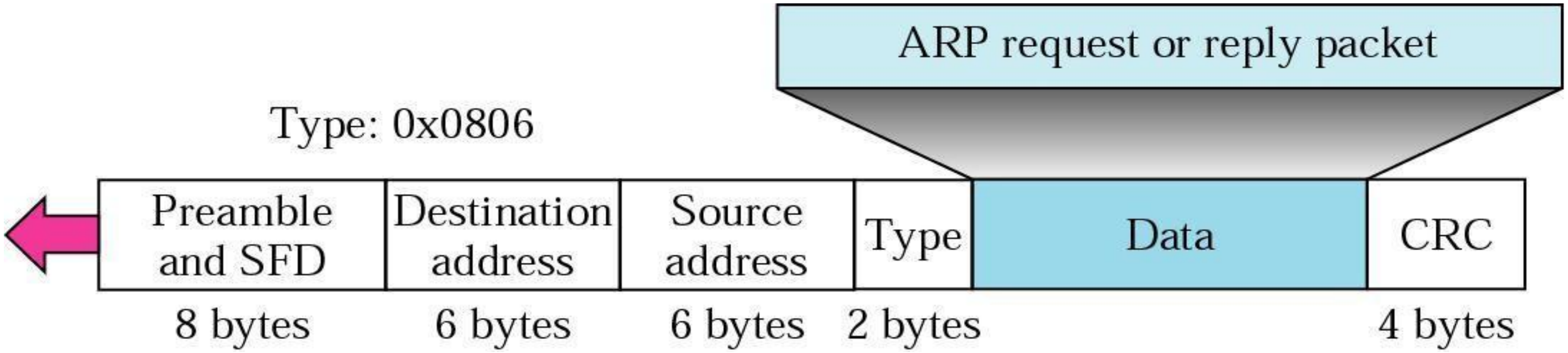
b. ARP reply is unicast

ARP PACKET

<table>
<tr><td colspan="2">Hardware Type</td><td>Protocol Type</td></tr>
<tr><td>Hardware length</td><td>Protocol length</td><td>Operation
Request 1, Reply 2</td></tr>
<tr><td colspan="3">Sender hardware address
(For example, 6 bytes for Ethernet)</td></tr>
<tr><td colspan="3">Sender protocol address
(For example, 4 bytes for IP)</td></tr>
<tr><td colspan="3">Target hardware address
(For example, 6 bytes for Ethernet)
(It is not filled in a request)</td></tr>
<tr><td colspan="3">Target protocol address
(For example, 4 bytes for IP)</td></tr>
</table>

ENCAPSULATION OF ARP PACKET

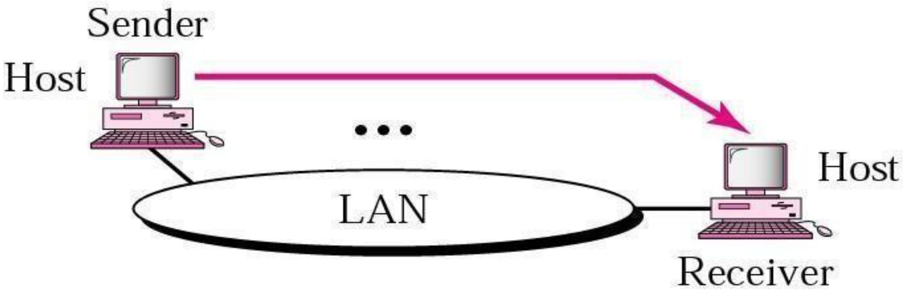
AN ARP PACKET IS ENCAPSULATED DIRECTLY INTO A DATALINK FRAME.



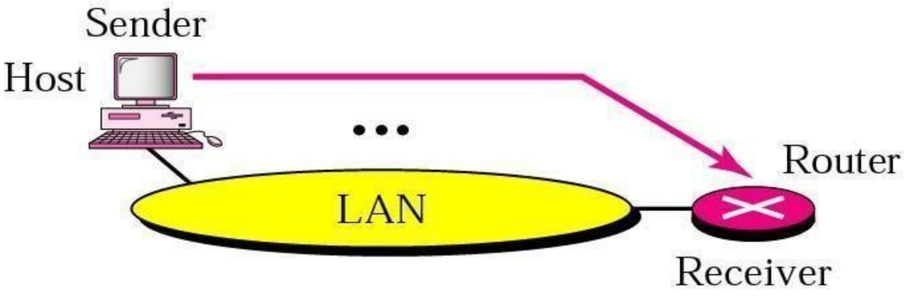
OPERATION

1. sndr knows ipaddress of target.
2. ip asks ARP to create ARP request msg,filling sndr physical addr,sender IP addr,target IP add.
3. msg is passed to dll where it is encapsulated in a frame by using physical address of sndr at source address and physical broadcast address at dest address.
4. every host or router receives the frame.bcoz frame contains broadcast dest address,all stns remove msg and pass it to arp.all machines except one targeted drop the packet.target machine recgnizes ip address.
5. target machine replies with ARP reply msg that contains its physical address.msg is unicast.
6. sndr rcvs reply msg.it now kows physical address of target machine.
7. IP addr which carries data for target machine is now encapsulated in a frame and is unicast to dest.

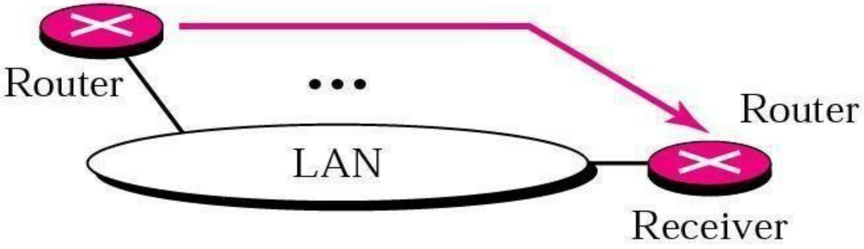
FOUR CASES USING ARP



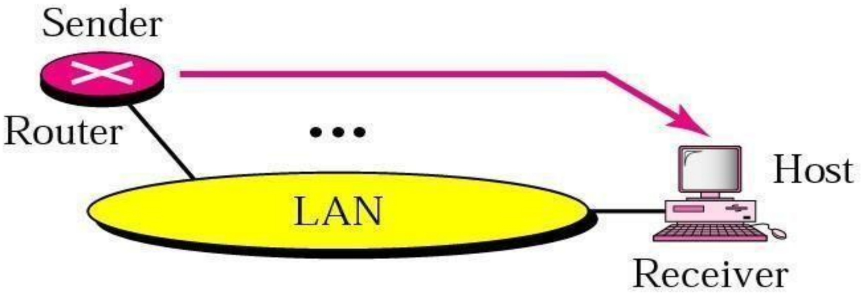
Case 1. A host has a packet to send to another host on the same network.



Case 2. A host wants to send a packet to another host on another network.
It must first be delivered to the appropriate router.



Case 3. A router receives a packet to be sent to a host on another network.
It must first be delivered to the appropriate router.

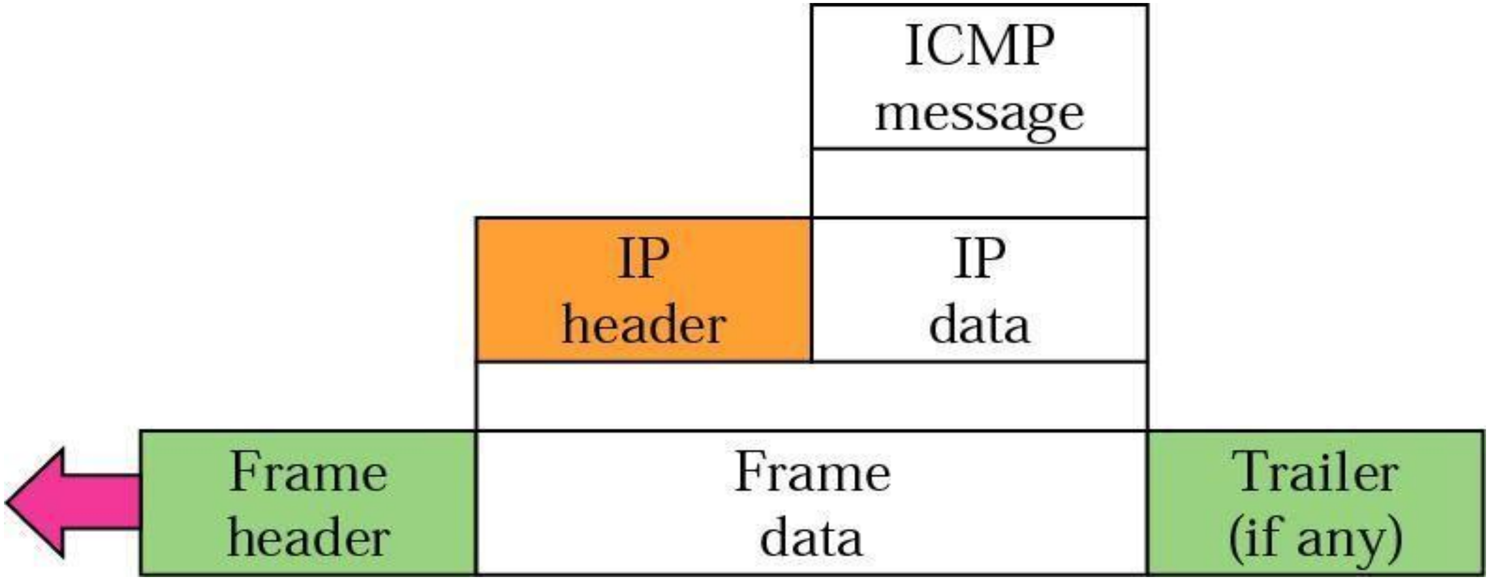


Case 4. A router receives a packet to be sent to a host on the same network.

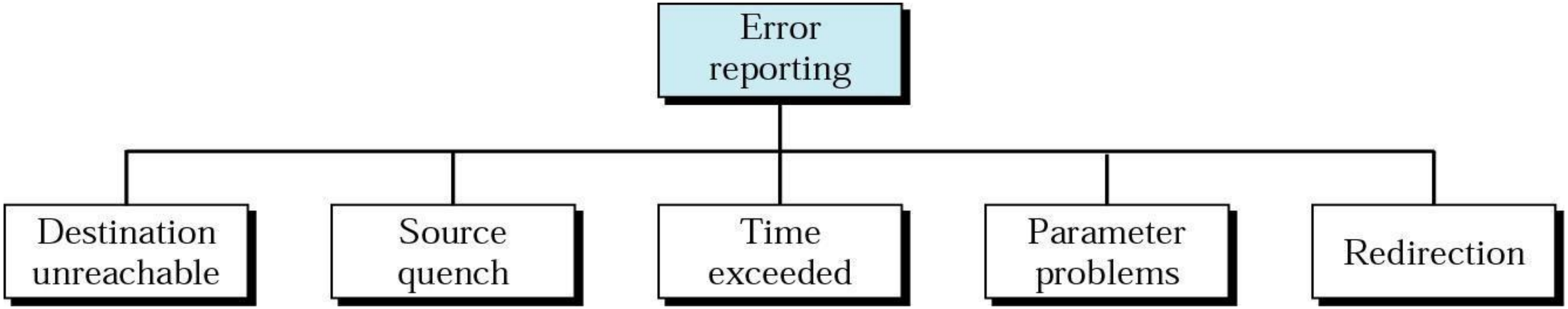
ICMP

1. The IP protocol also lacks a mechanism for host and management queries.
2. A host sometimes needs to determine if a router or another host is alive.
3. And sometimes a network administrator needs information from another host or router.
4. The Internet Control Message Protocol (ICMP) has been designed to compensate for the above two deficiencies.
5. It is a companion to the IP protocol
6. The value of the protocol field in the IP datagram is 1 to indicate that the IP data are an ICMP message.

ICMP ENCAPSULATION



ERROR-REPORTING MESSAGES



DESTINATION UNREACHABLE

1. When a router cannot route a datagram or a host cannot deliver a datagram, the datagram is discarded and the router or the host sends a destination-unreachable message back to the source host that initiated the datagram.

2. Note that destination-unreachable messages can be created by either a router or the destination host.

SOURCE-QUENCH

1. When a router or host discards a datagram due to congestion, it sends a source-quench message to the sender of the datagram.
2. This message has two purposes.
3. First, it informs the source that the datagram has been discarded.
4. Second, it warns the source that there is congestion somewhere in the path and that the source should slow down (quench) the sending process.

TIME EXCEEDED

1. When the time-to-live value reaches 0, after decrementing, the router discards the datagram.

2. **First:** when the datagram is discarded, a time-exceeded message must be sent by the router to the original source.

3. **Second,** a time-exceeded message is also generated when not all fragments that make up a message arrive at the destination host within a certain time limit.

PARAMETER PROBLEM

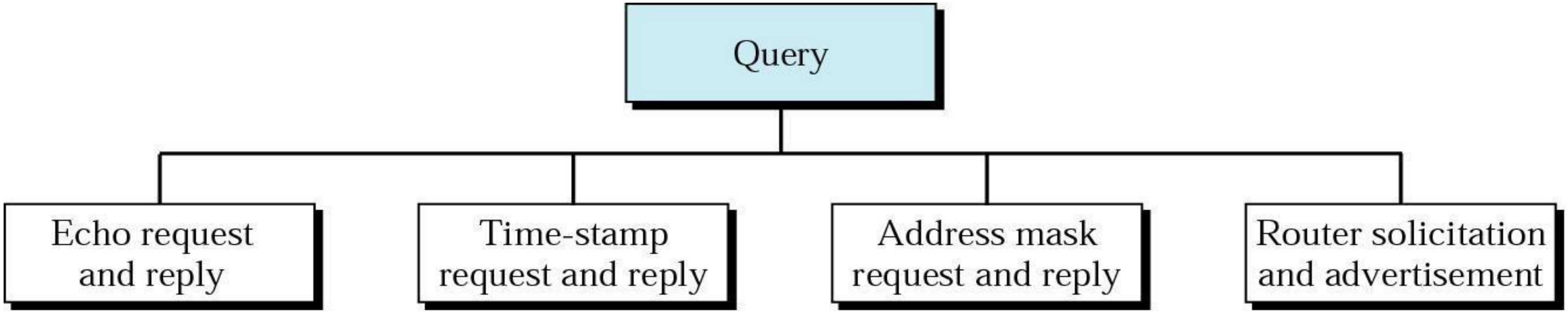
1. Any ambiguity in the header part of a datagram can Create serious problems as the datagram travels through the Internet.

2. If a router or the destination host discover an ambiguous or missing value in any field of the datagram, it discards the datagram and sends a parameter-problem message back to the source

REDIRECTION MESSAGE

1. If Any host may send a datagram, which is destined for another network, to the wrong router.
2. In this case, the router that receives the datagram will forward the datagram to the correct router.
3. However, to update the routing table of the host, it sends a redirection message to the host

QUERY MESSAGES


Query
Echo request and reply
Time-stamp request and reply
Address mask request and reply
Router solicitation and advertisement

ECHO REQUEST AND REPLY

1. The echo-request and echo-reply messages are designed for diagnostic purposes.

2. Network managers and users utilize this pair of messages to identify network problems.

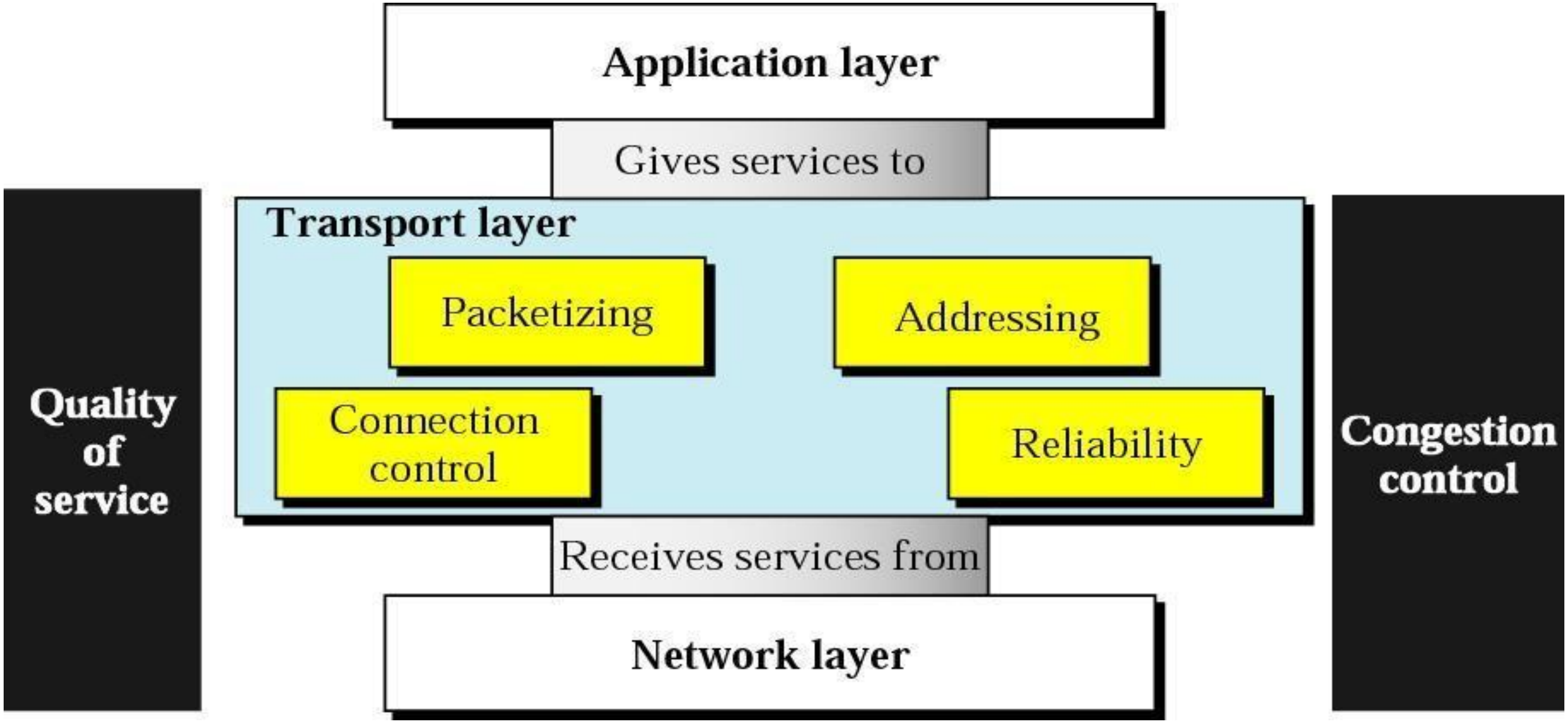
3. The combination of echo-request and echo- reply messages determine whether two systems (hosts or routers) can communicate with each other.

TIMESTAMP REQUEST AND REPLY

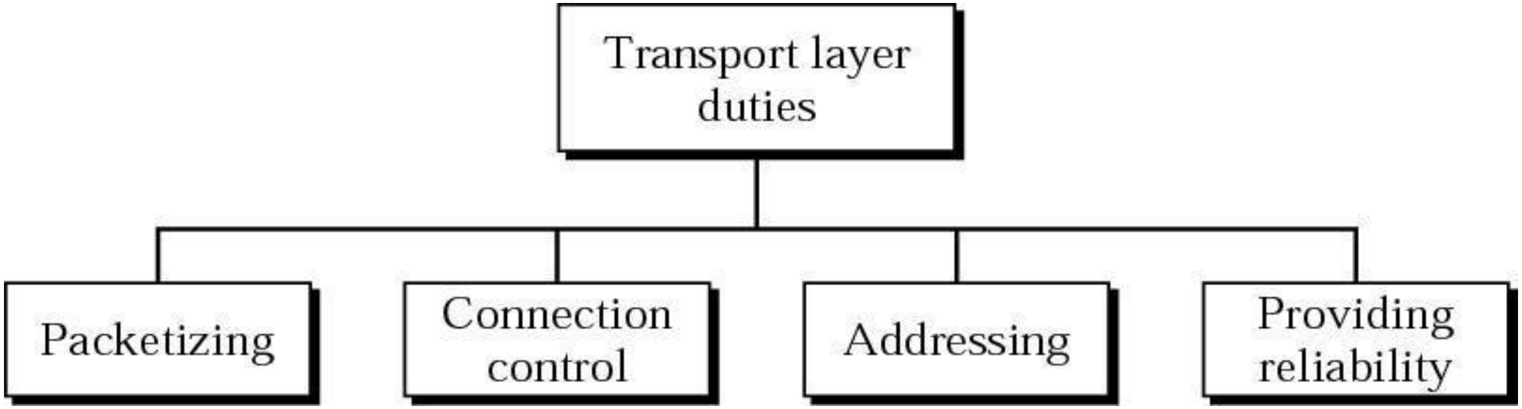
1. Two machines (hosts or routers) can use the timestamp request and timestamp reply messages to determine the round-trip time needed for an IP datagram to travel between them.

2. It can also be used to synchronize the clocks in two machines.

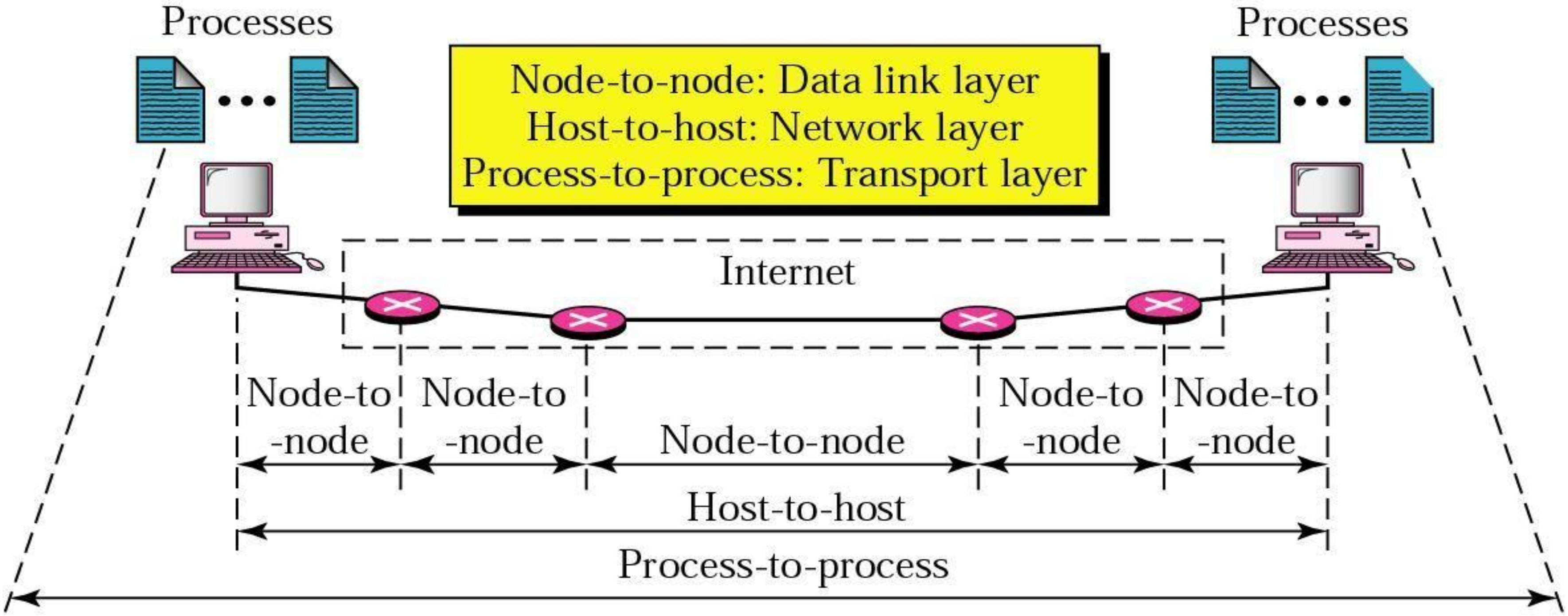
POSITION OF TRANSPORT LAYER



TRANSPORT LAYER DUTIES



TYPES OF DATA DELIVERIES



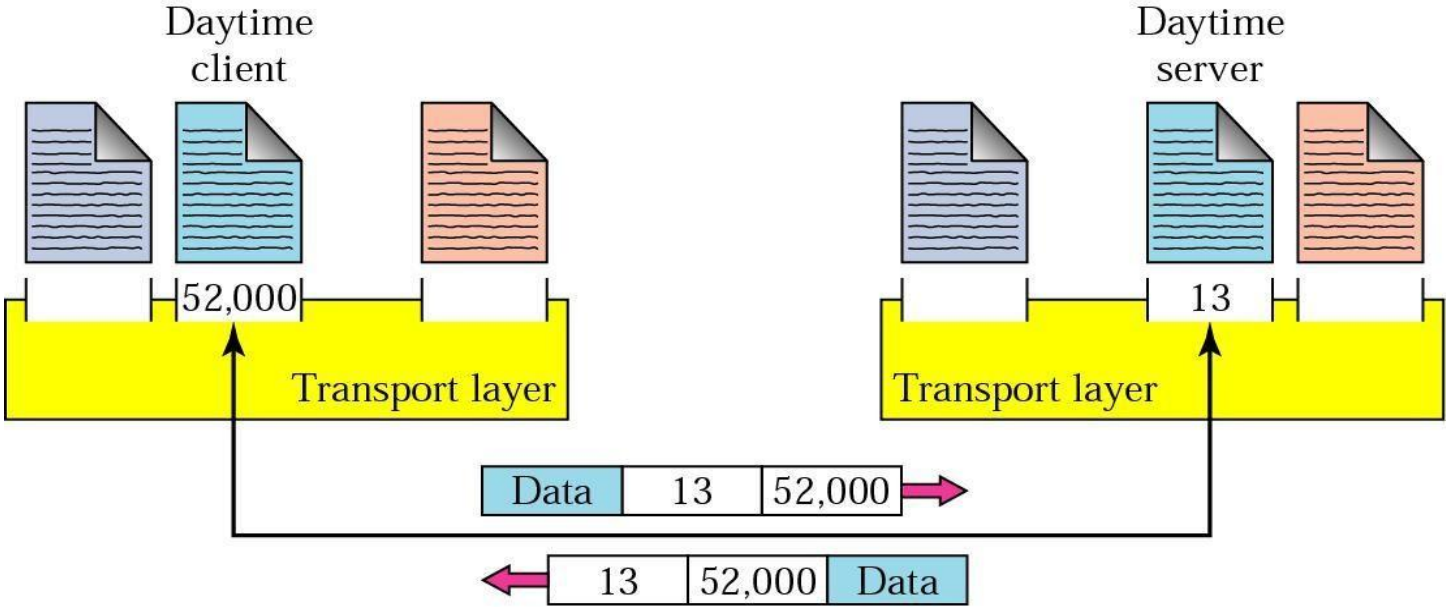
CLIENT/SERVER PARADIGM

1. A process on the local host, called a client, needs services from a process usually on the remote host, called a server.

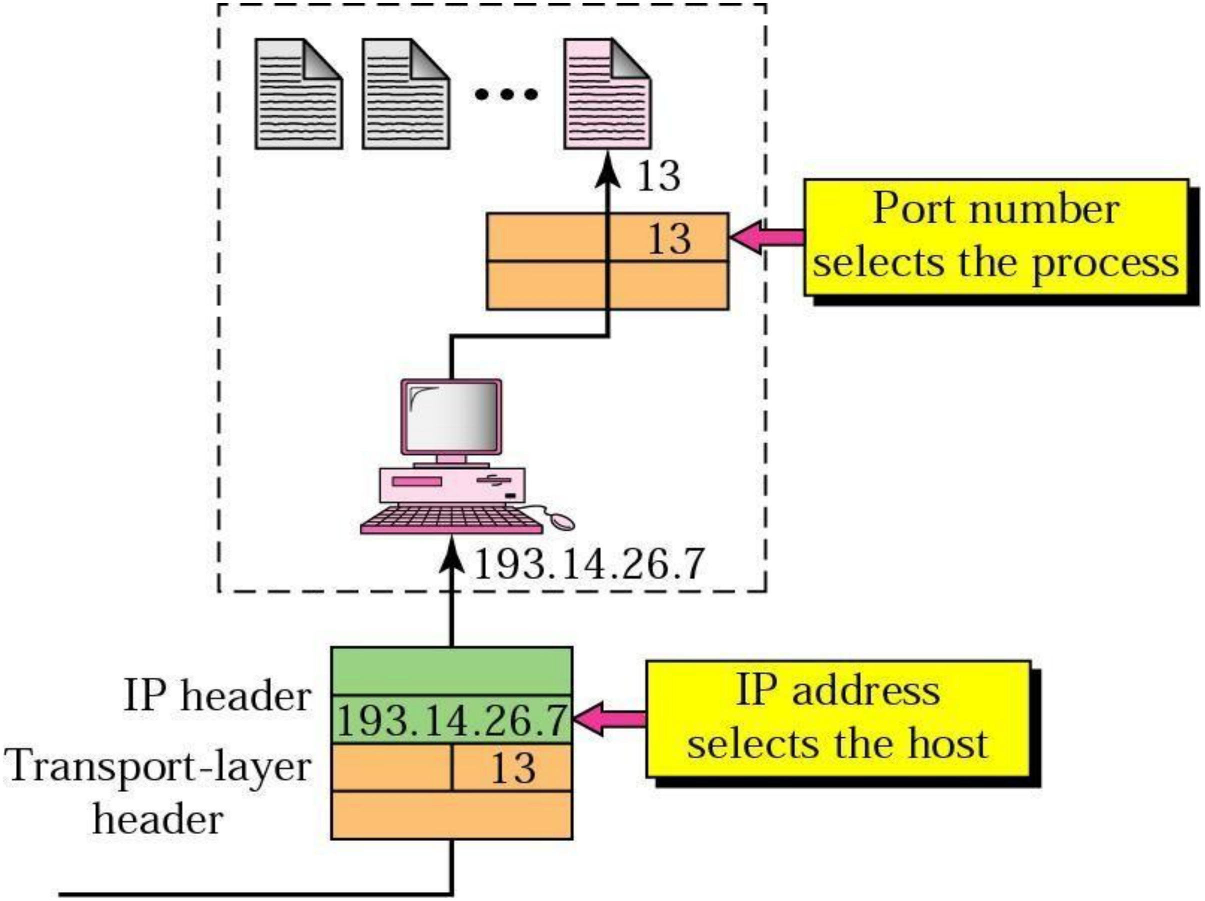
2. Both processes (client and server) have the same name.

3. For example, to get the day and time from a remote machine, we need a Daytime client process running on the local host and a Daytime server process running on a remote machine.

PORT NUMBERS



IP ADDRESSES VERSUS PORT NUMBERS



LANARANGES

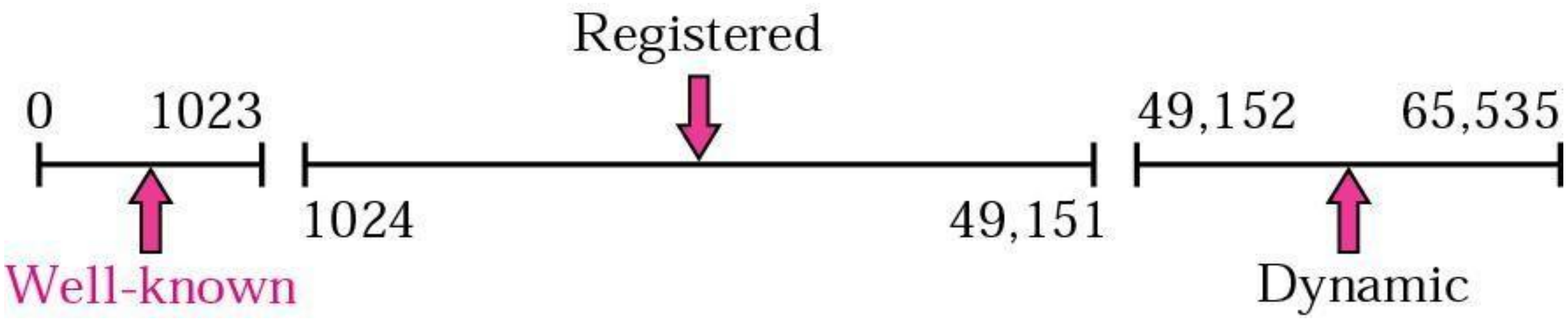
1. The lANA (Internet Assigned Number Authority) has divided

   the port numbers into threeranges:

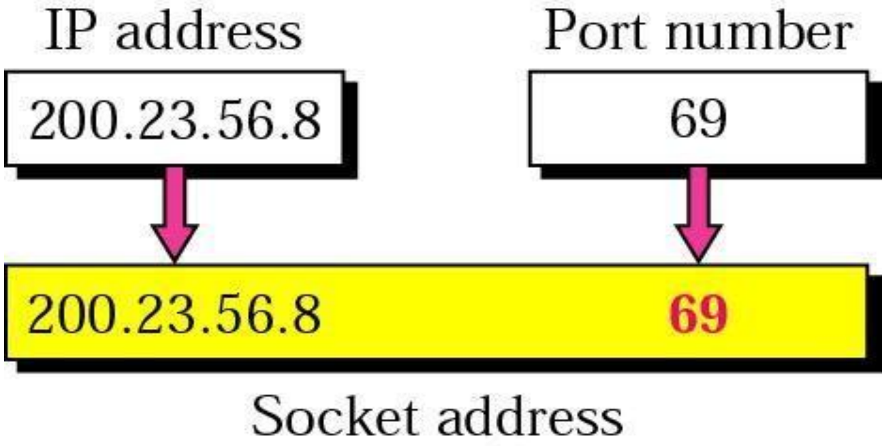
   - well known,
   - registered,
   - dynamic (or private)

1. Well-known ports. The ports ranging from 0 to 1023 are assigned and controlled by lANA. These are the **well- known ports**.
2. Registered ports. The ports ranging from 1024 to 49,151 are not assigned or controlled by lANA. They can only be registered with lANA to preventduplication.
3. Dynamic ports. The ports ranging from 49,152 to 65,535 are neither controlled nor registered. They can be usedby any process. These are the **ephemeral ports.**

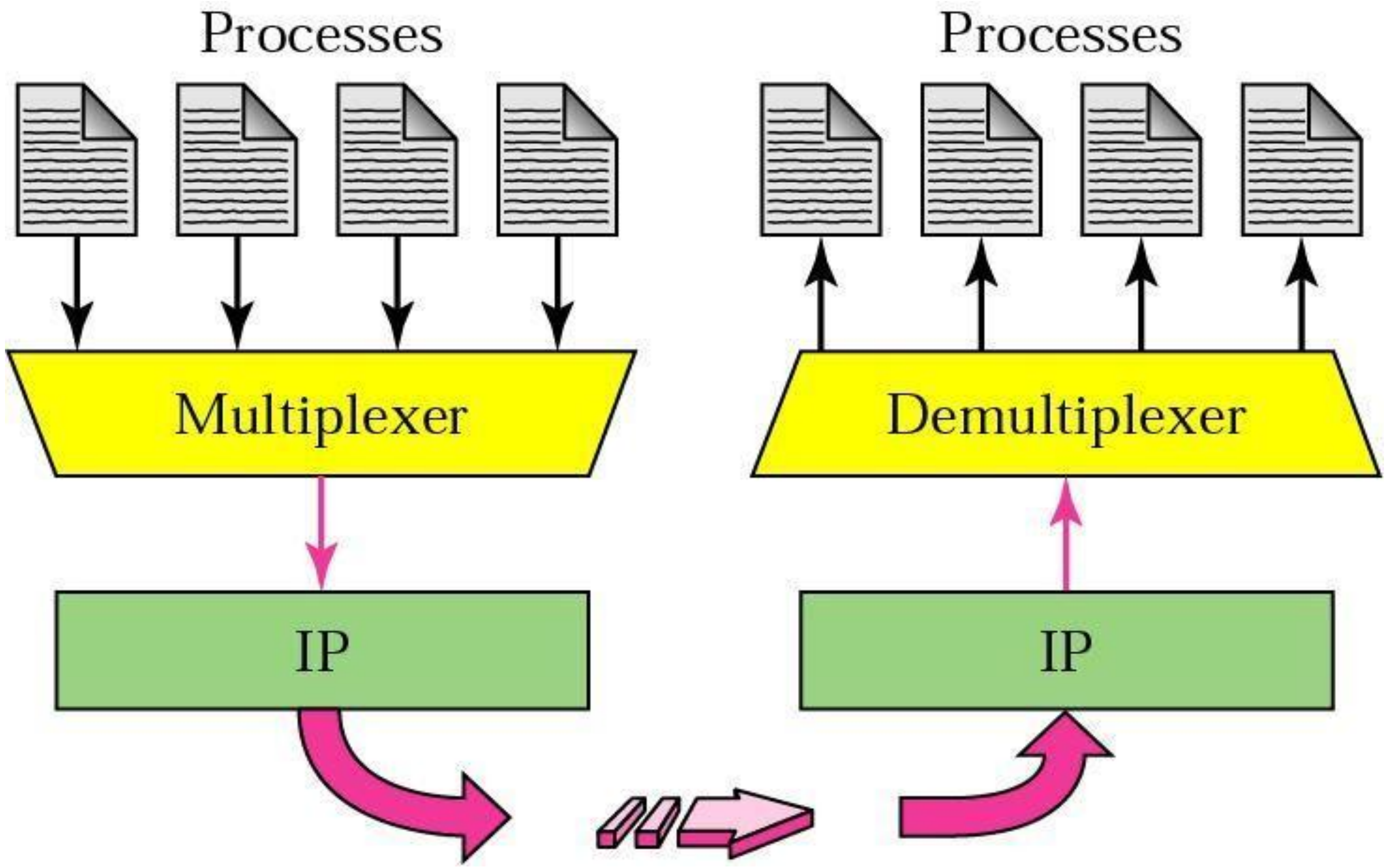
IANA RANGES


Registered
0
1023
49,152
65,535
1024
49,151
Well-known
Dynamic

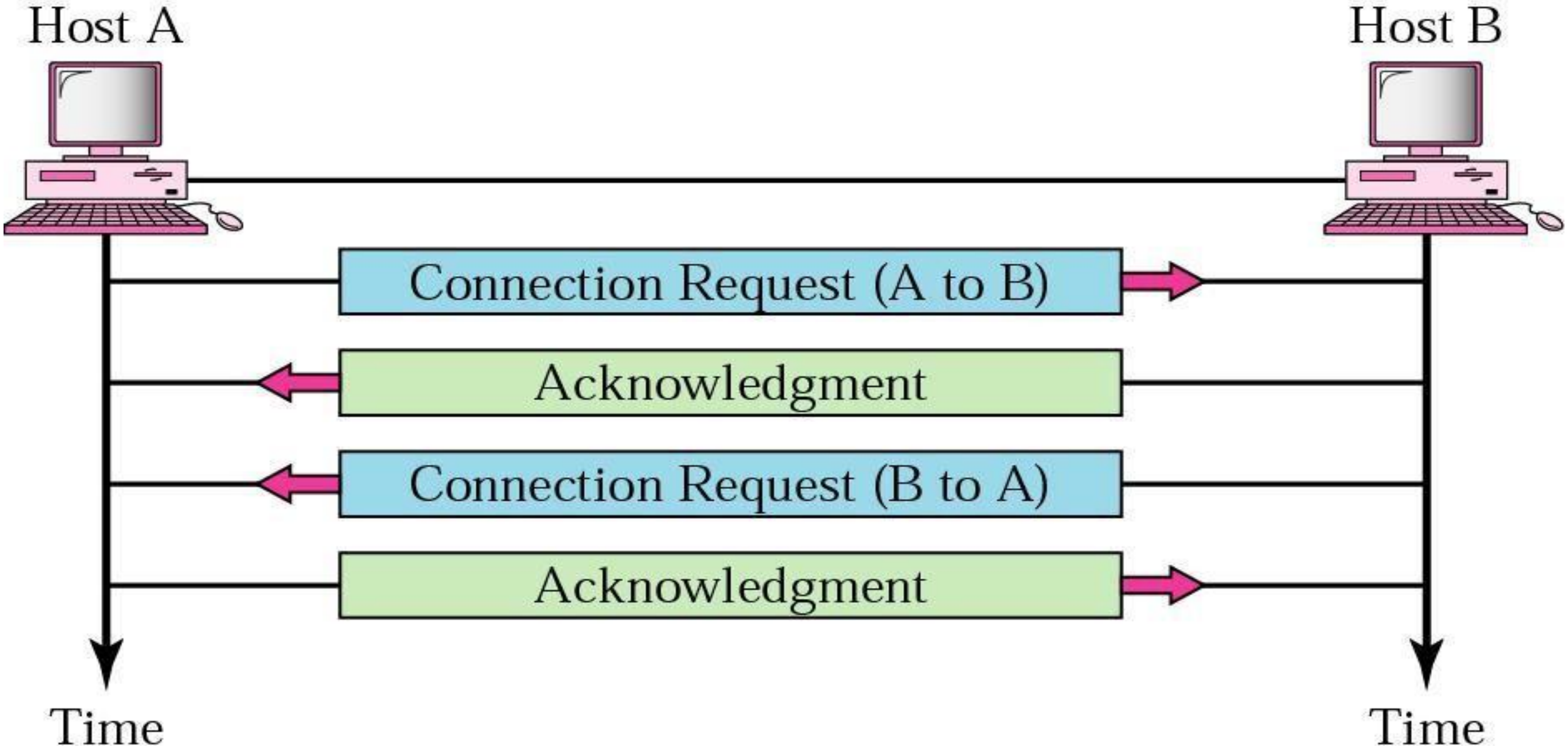
SOCKET ADDRESS



MULTIPLEXING AND DEMULTIPLEXING



CONNECTION ESTABLISHMENT



Host A

Host B

Connection Request (A to B)

Acknowledgment

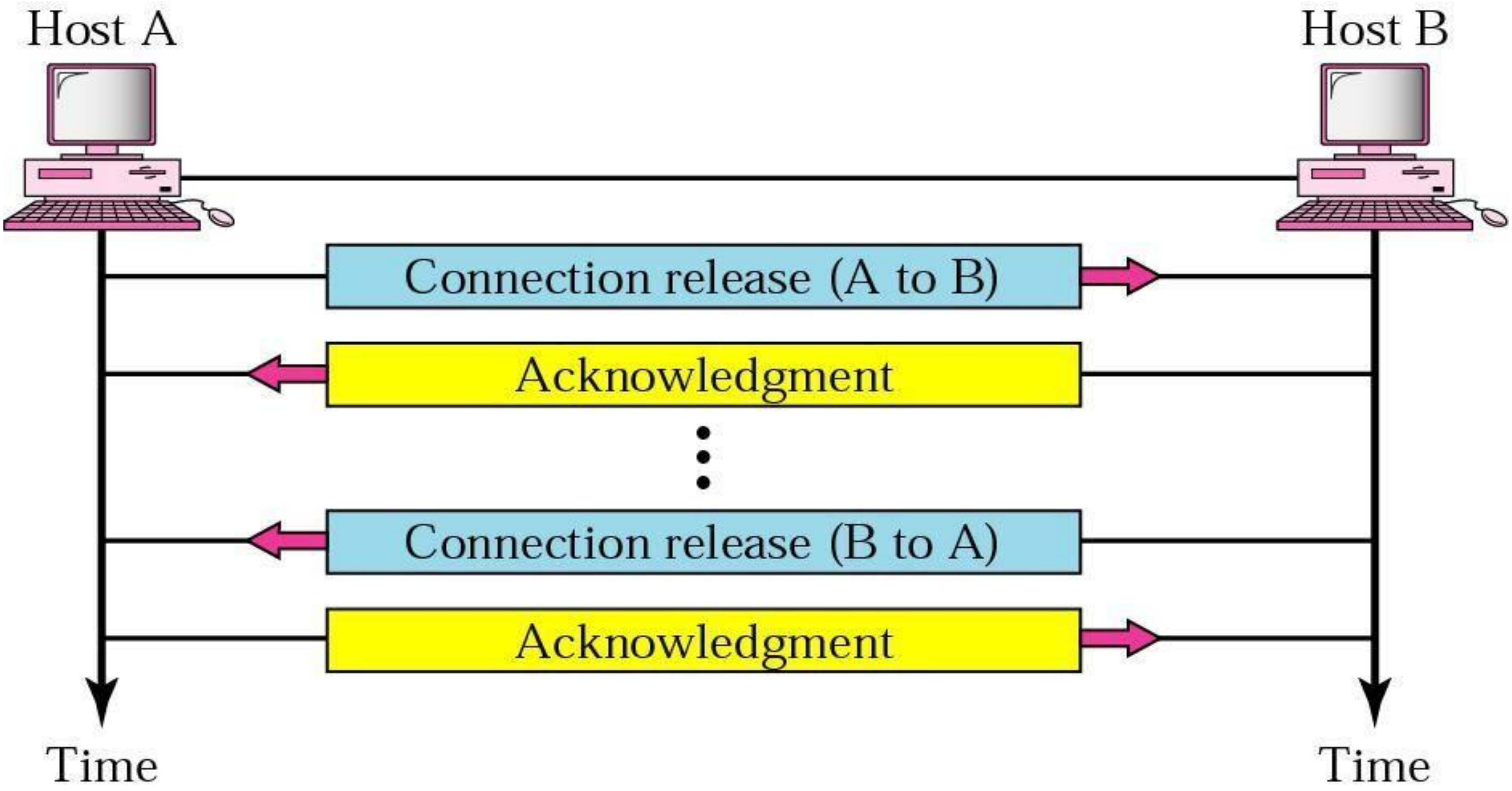
Connection Request (B to A)

Acknowledgment

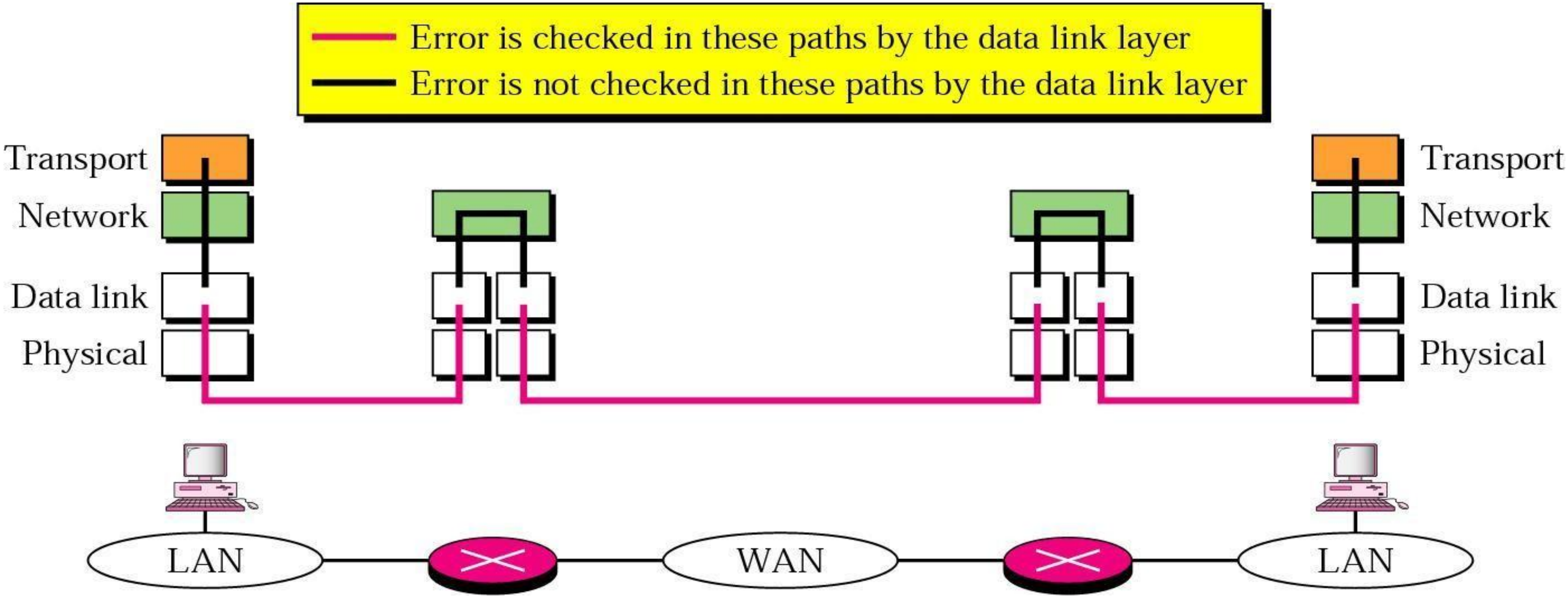
Time

Time

CONNECTION TERMINATION



ERROR CONTROL


Error is checked in these paths by the data link layer
Error is not checked in these paths by the data link layer
Transport
Network
Data link
Physical
Transport
Network
Data link
Physical
LAN
WAN
LAN

UNIT -V

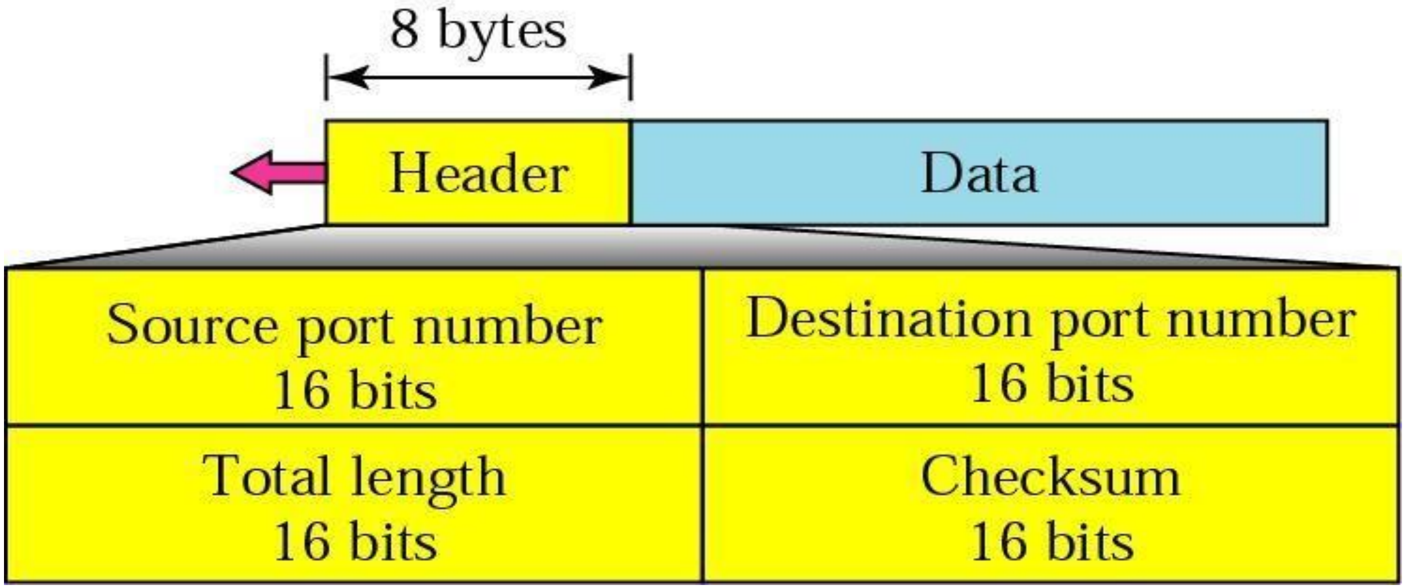
The Internet Transport Protocols,

The Internet Transport Protocols, Application Layer

WELL-KNOWN PORTS USED BY UDP

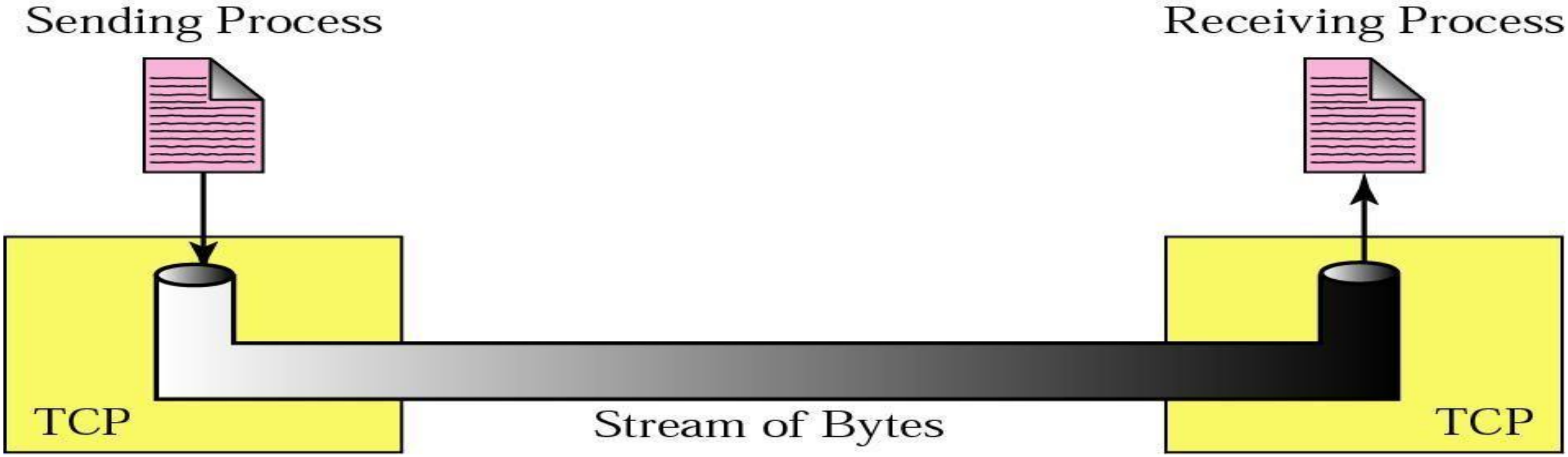
Port	*Protocol*	*Description*
7	Echo	Echoes a received datagram back to the sender
9	Discard	Discards any datagram that is received
11	Users	Active users
13	Daytime	Returns the date and the time
17	Quote	Returns a quote of the day
19	Chargen	Returns a string of characters
53	Nameserver	Domain Name Service
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 FORMAT



Source port number 16 bits	Destination port number 16 bits
Total length 16 bits	Checksum 16 bits

STREAM DELIVERY

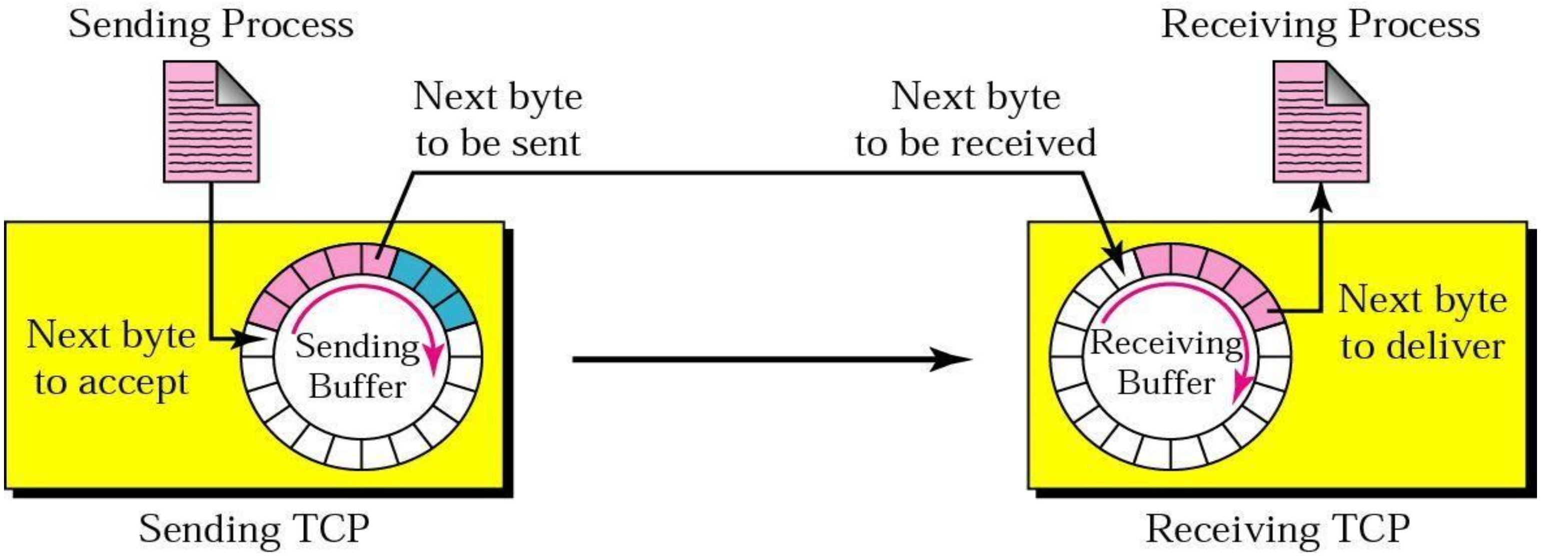


- In udp process sndsmsgs with predifined boundaries to udp

  for delivery,but tcp allows sndng process to deliver data as a stream of bytes and allows revng process to obtain data as stream of bytes.

SENDING AND RECEIVING BUFFERS

1. Bcozsnding & rcvng process may not writer read data at same speed ,tcp needs buffers for storage.

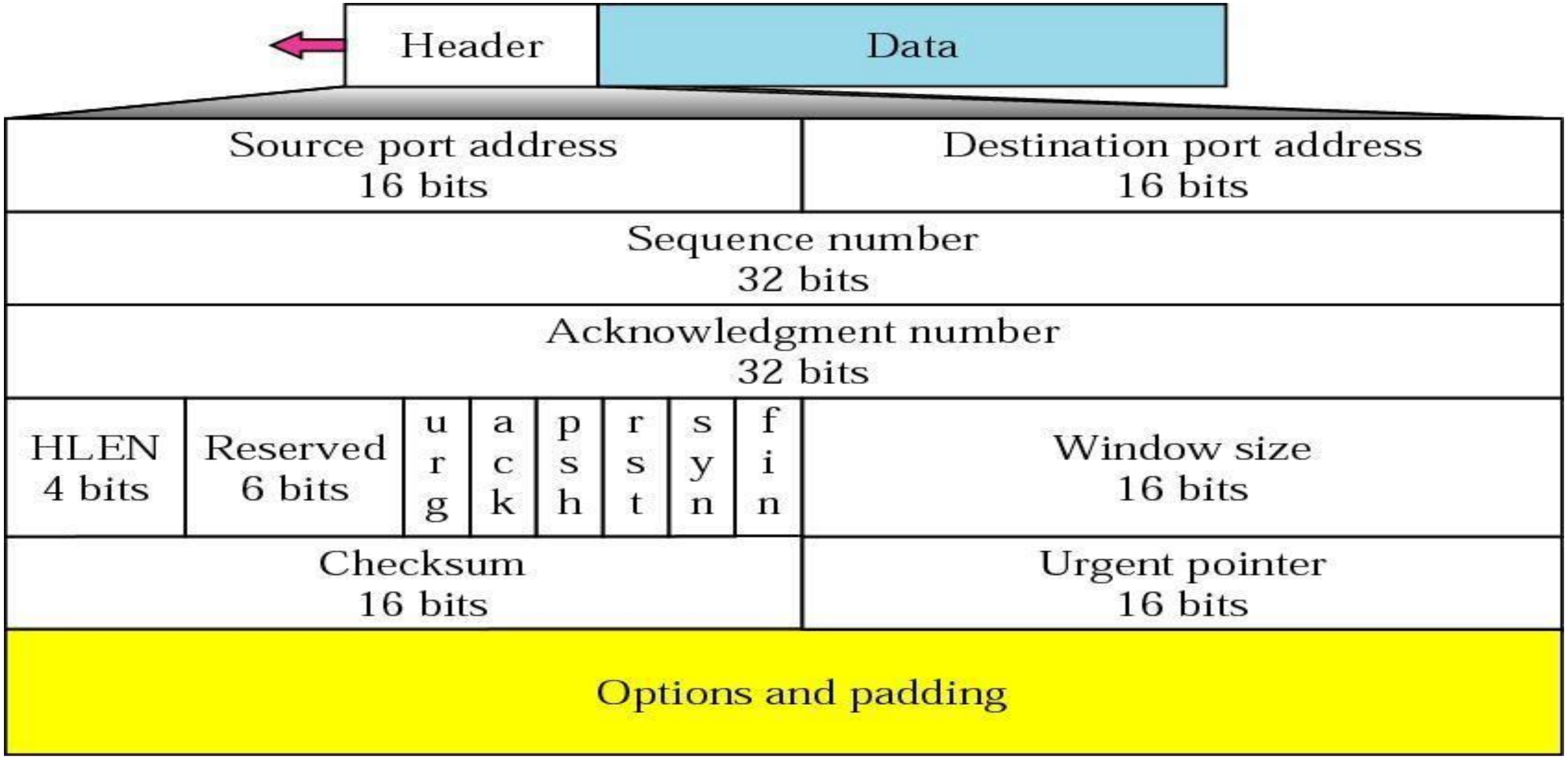


TCP SEGMENTS

- At TL,TCP groups no. of bytes together into packet cald segment.tcp adds header to each segment and delivers segment to ip layer for transmission.segments r encapsulated in ip datagram.
- Tcp supports full duplex,connection oriented,reliable service.

TCP SEGMENT FORMAT

1. Segment consists of 20-60 byte header followed bydata frm appnprgm.



Header

Data

Source port address
16 bits

Destination port address
16 bits

Sequence number
32 bits

Acknowledgment number
32 bits

HLEN
4 bits

Reserved
6 bits

urg

ack

psh

rst

syn

fin

Window size
16 bits

Checksum
16 bits

Urgent pointer
16 bits

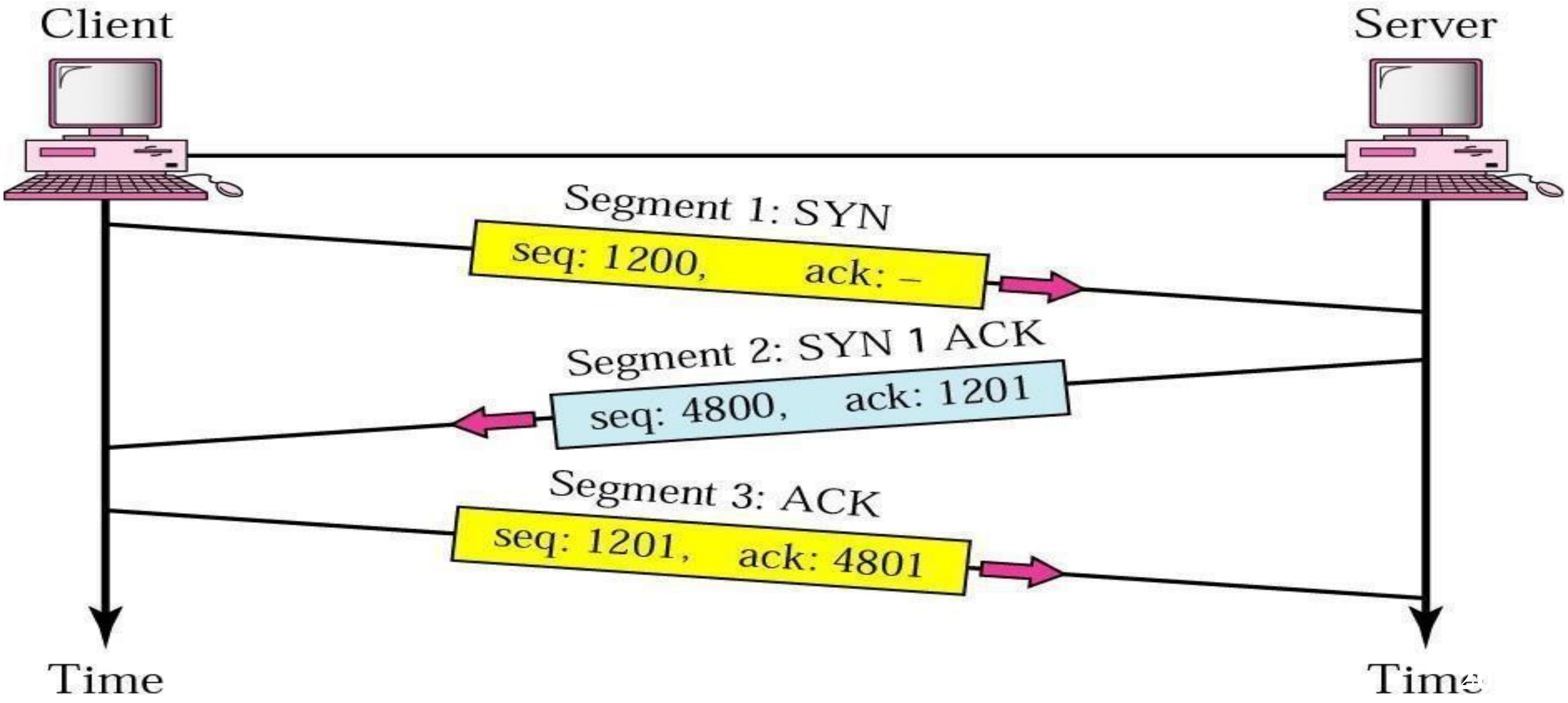
Options and padding

CONTROL FIELD

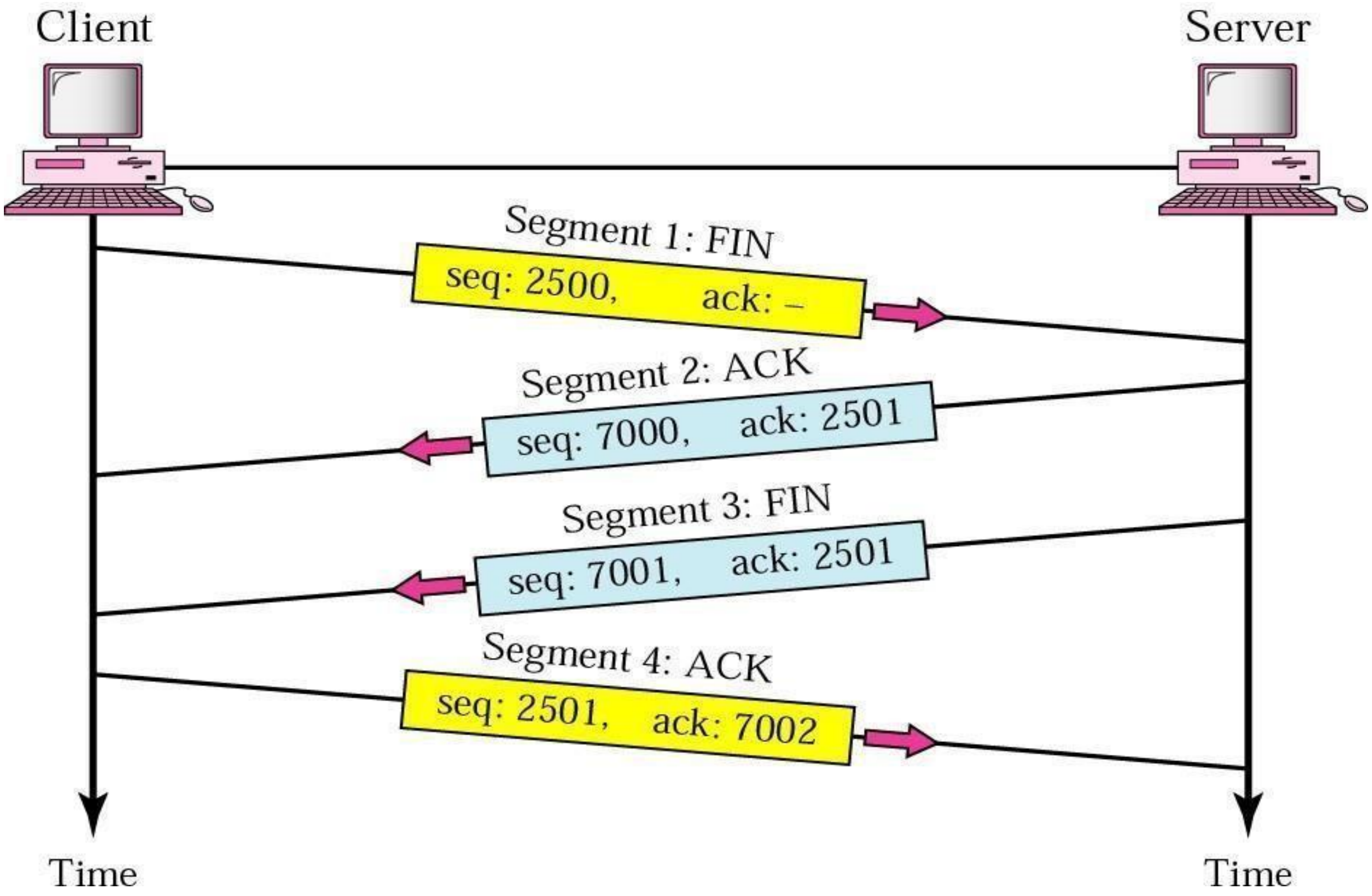
Flag	Description
URG	The value of the urgent pointer field is valid.
ACK	The value of the acknowledgment field is valid.
PSH	Push the data.
RST	The connection must be reset.
SYN	Synchronize sequence numbers during connection.
FIN	Terminate the connection.

THREE-STEP CONNECTION ESTABLISHMENT

1. In tcp connected oriented transmission requires3 phases-connection establishment,data transfer,connection termination.



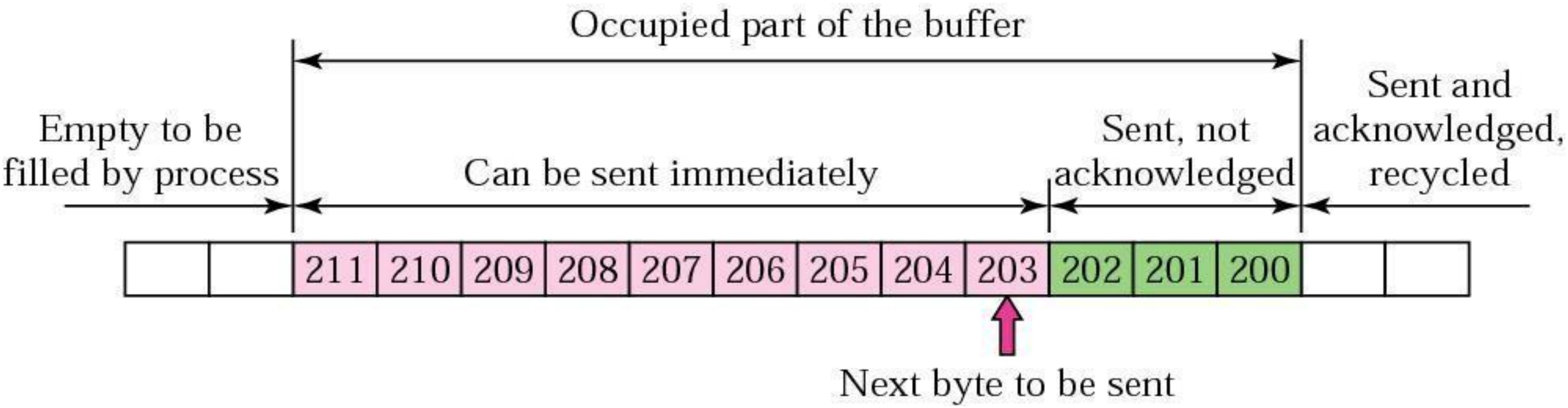
FOUR-STEP CONNECTION TERMINATION



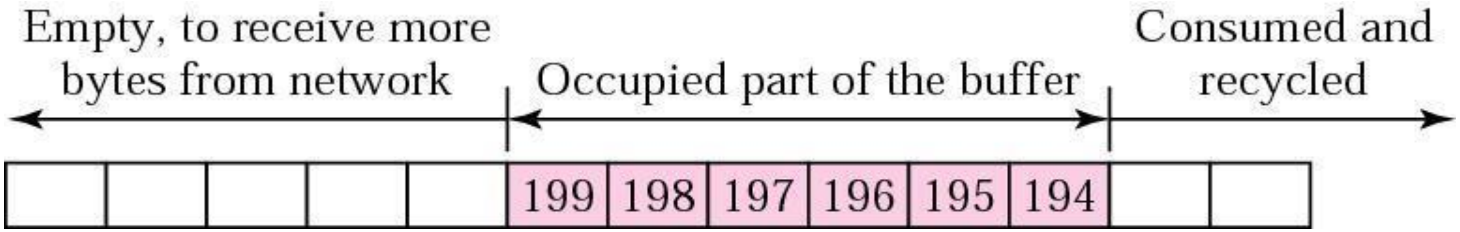
STATES FOR TCP

State	Description
CLOSED	There is no connection.
LISTEN	The server is waiting for calls from the client.
SYN-SENT	A connection request is sent; waiting foracknowledgment.
SYN-RCVD	A connection request is received.
ESTABLISHED	Connection is established.
FIN-WAIT-1	The application has requested the closing of the connection.
FIN-WAIT-2	The other side has accepted the closing of the connection.
TIME-WAIT	Waiting for retransmitted segments to die.
CLOSE-WAIT	The server is waiting for the application to close.
LAST-ACK	The server is waiting for the lastacknowledgment.

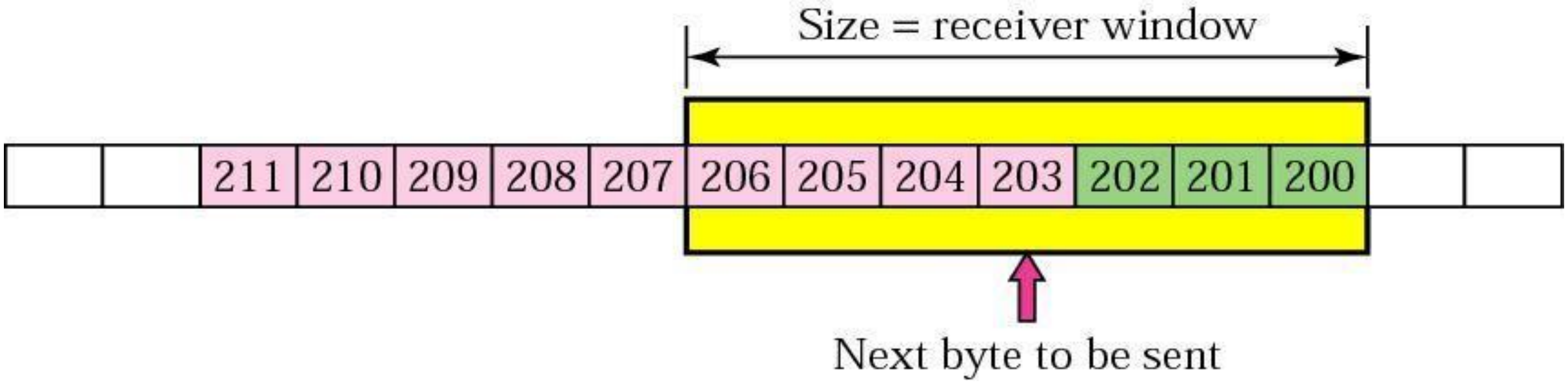
SENDER BUFFER



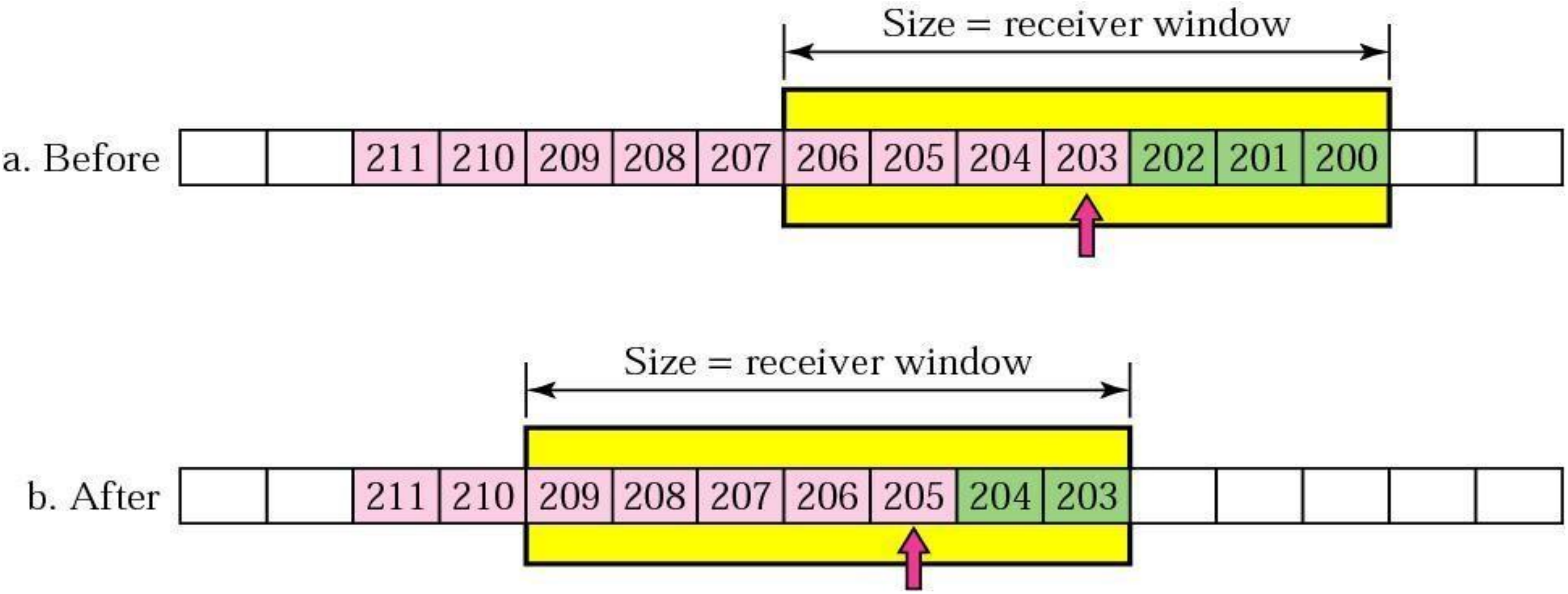
RECEIVER WINDOW


Empty, to receive more bytes from network
Occupied part of the buffer
Consumed and recycled
199
198
197
196
195
194

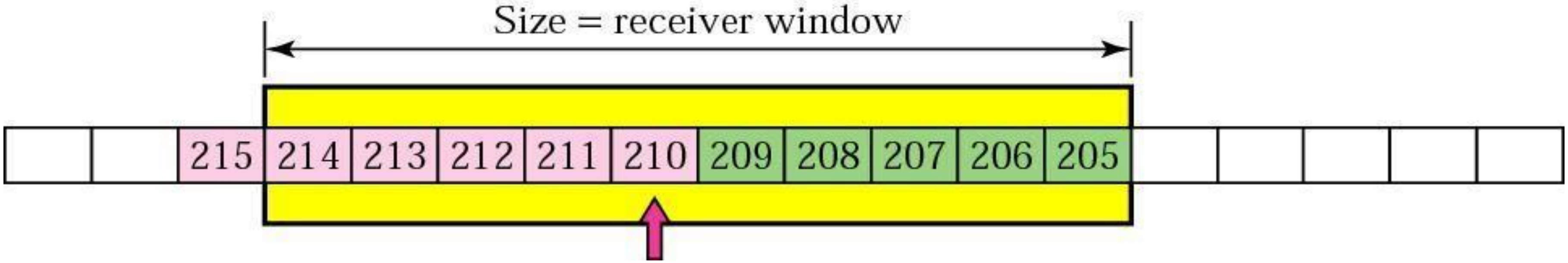
SENDER BUFFER AND SENDER WINDOW



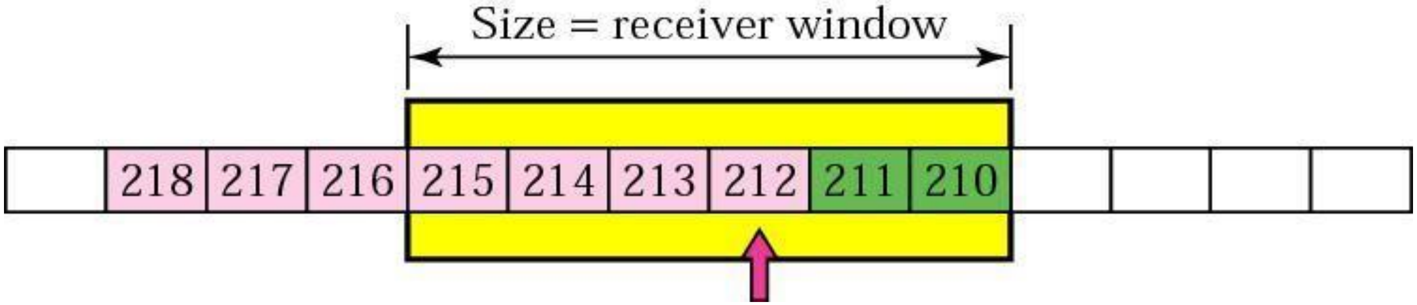
SLIDING THE SENDER WINDOW



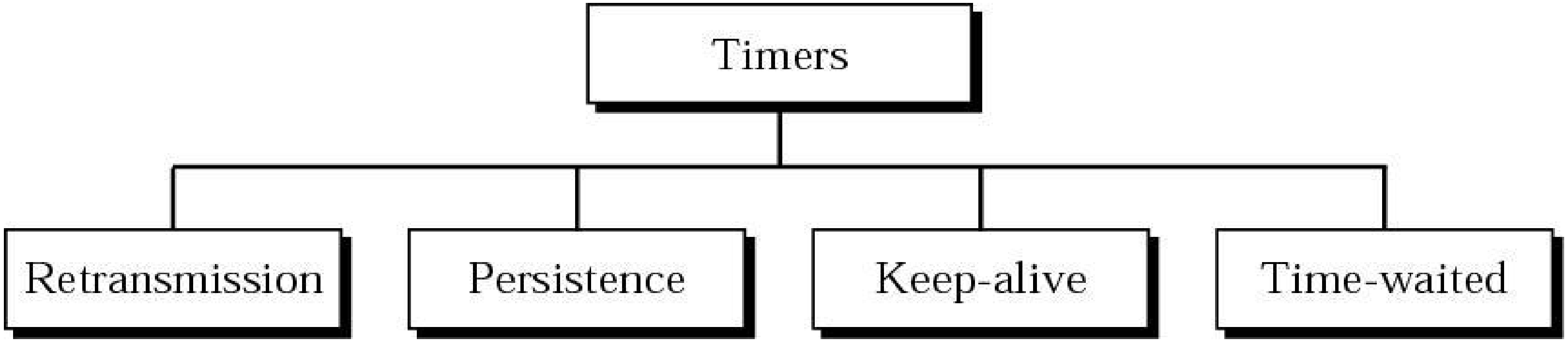
EXPANDING THE SENDER WINDOW



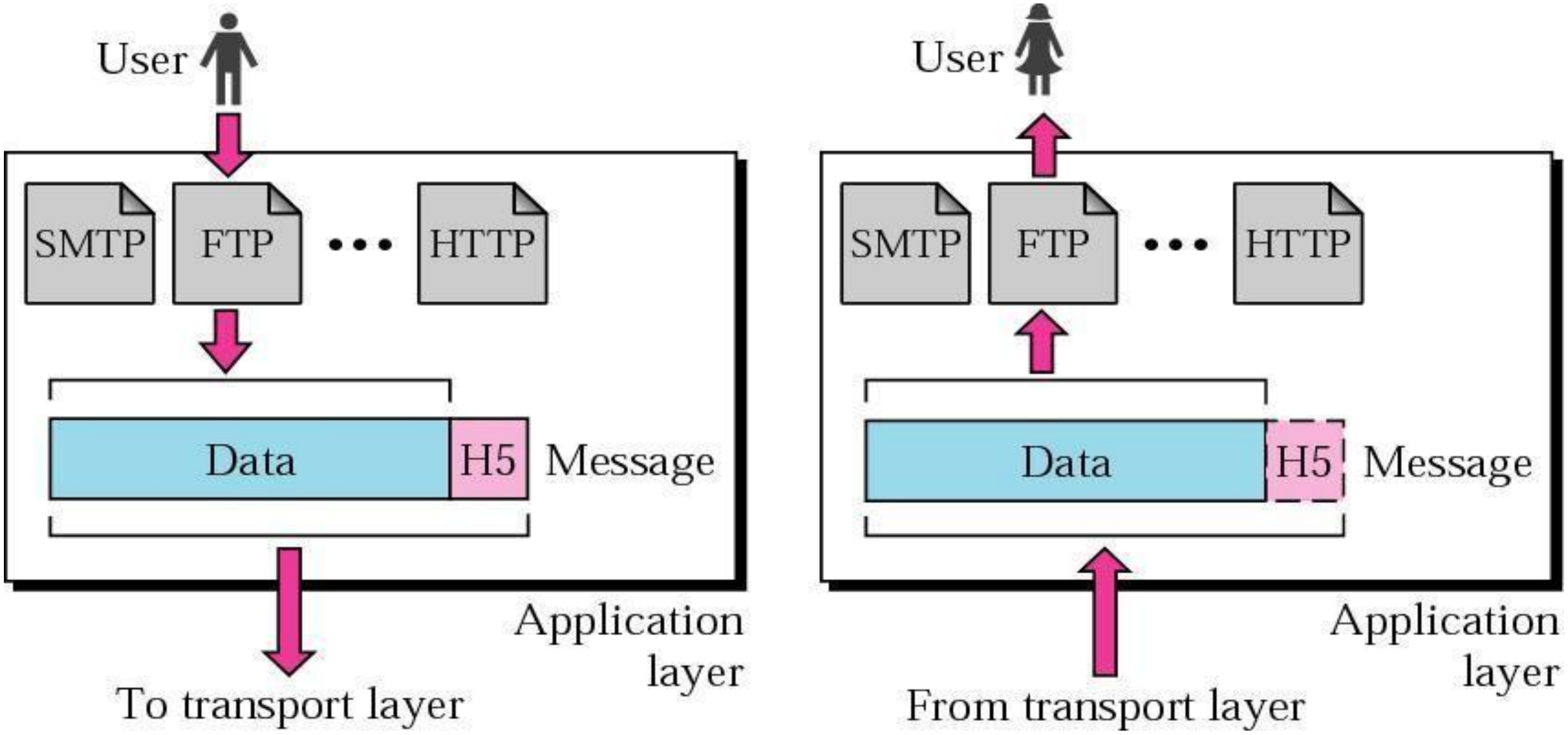
SHRINKING THE SENDER WINDOW



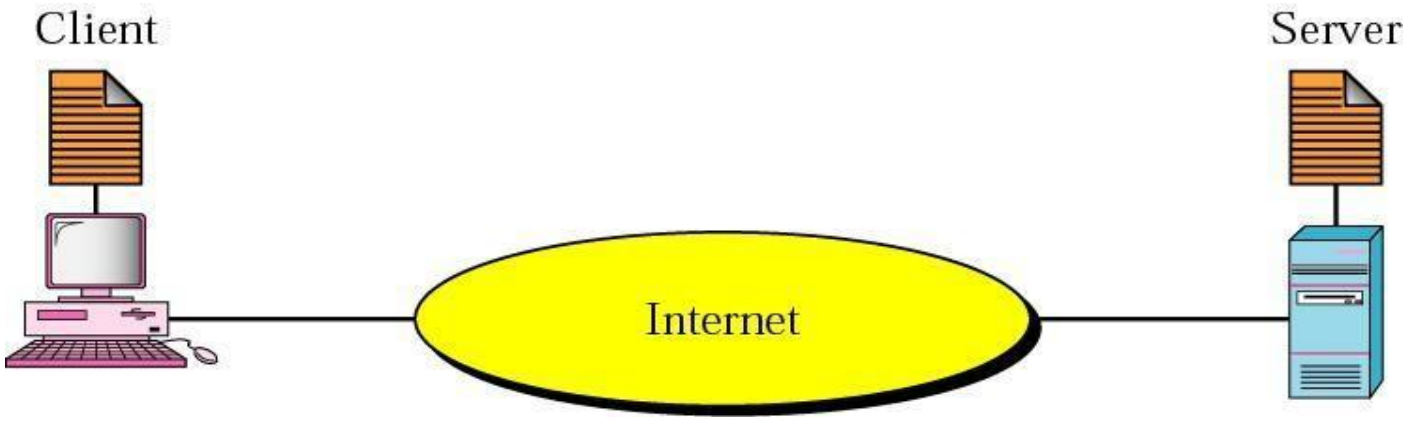
TCP TIMERS


Timers
Retransmission
Persistence
Keep-alive
Time-waited

NETWORK LAYER DUTIES



CLIENT-SERVER MODEL

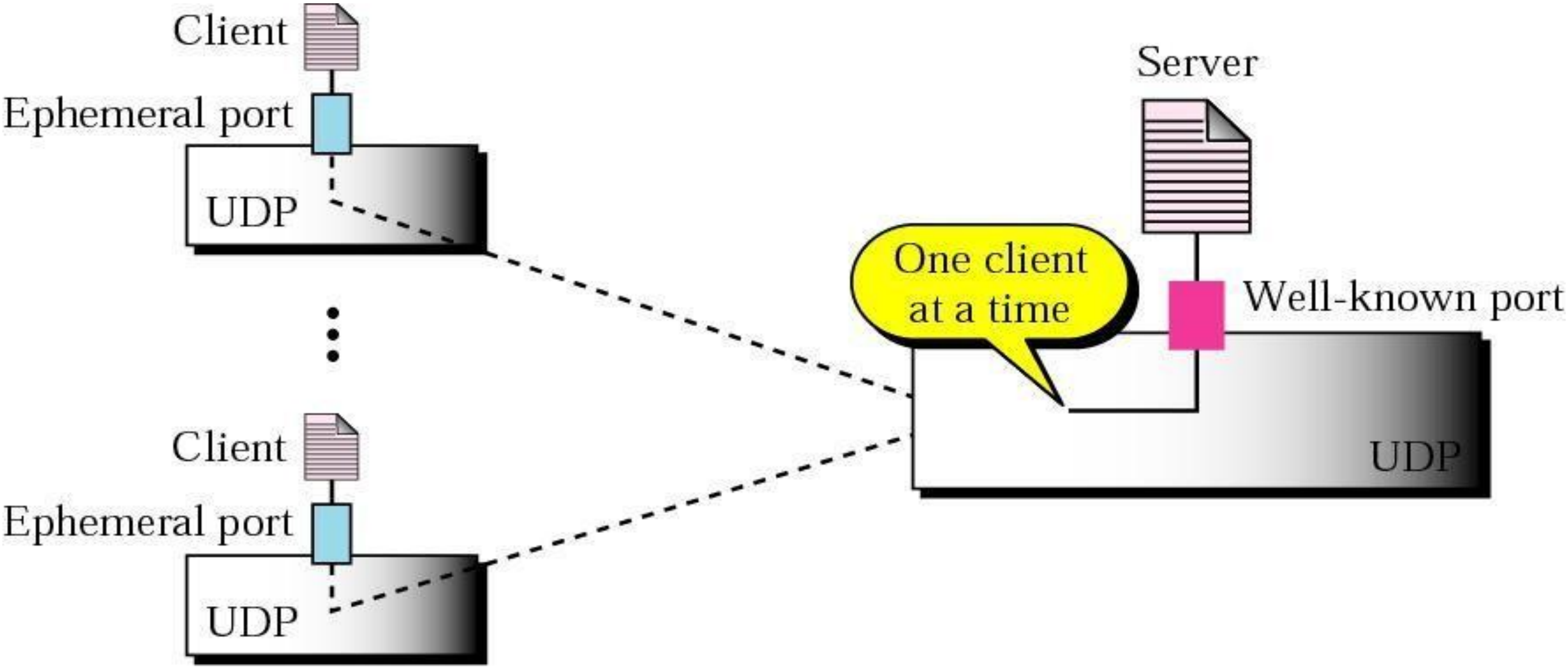


CLIENT-SERVER MODEL

1. Client application program running on the local machine requests a service from another application program – server – running on the remote machine.
2. Commonly server provides service to any client, not a particular

   client
3. Generally, a client application program that requests a service should run only when it is needed.
4. A server program providing service should run all the time, as it does not know when its services will be needed.

CONNECTIONLESS ITERATIVE SERVER



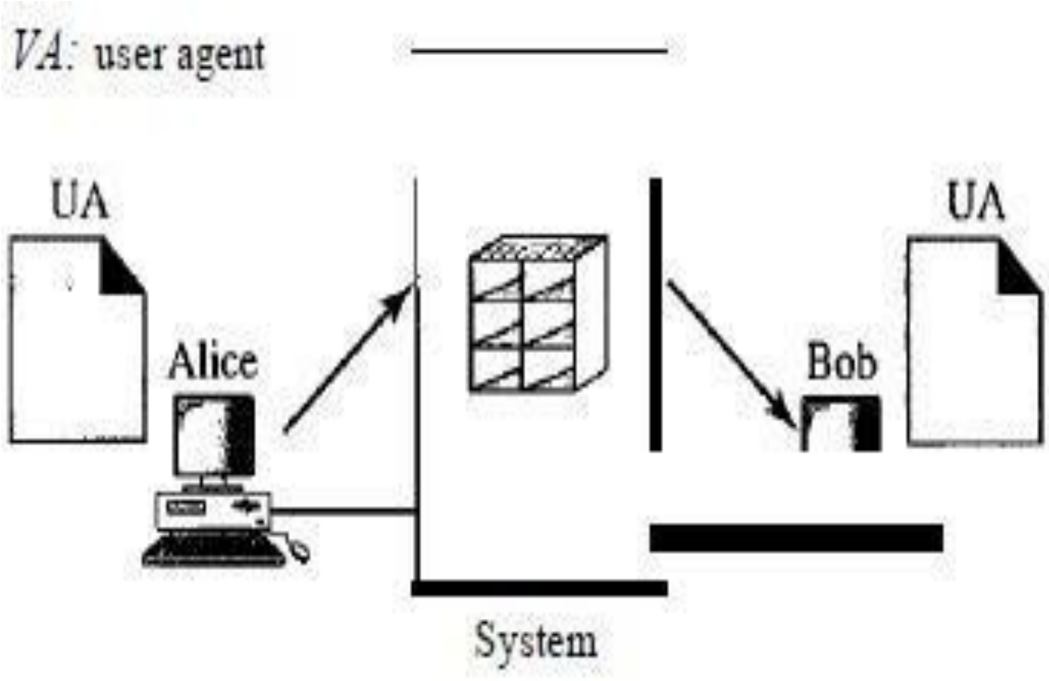
ELECTRONIC MAIL

1. There are two popular applications for exchanging information.
    1. Electronic mail exchanges information between people.
    2. File transfer exchanges files between computers.

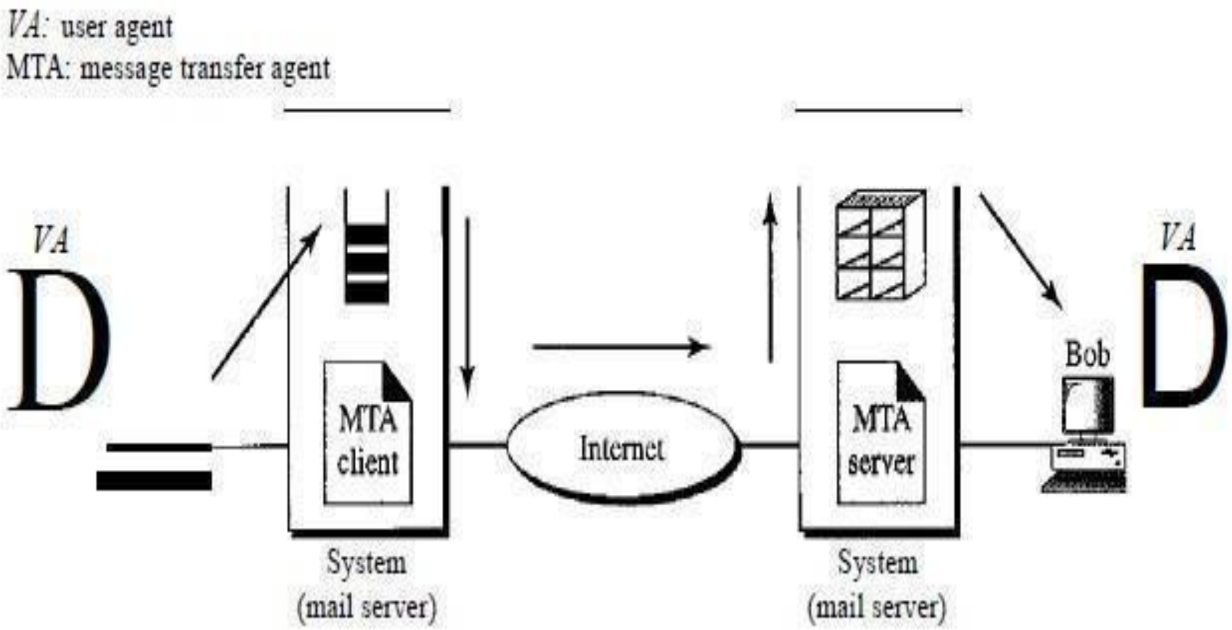
ARCHITECTURE

1. To explain the architecture of e-mail, we give four scenarios
2. First Scenario
   - In the first scenario, the sender and the receiver of the e-mail are users (or application programs) on the same system;
   - they are directly connected to a shared system.
   - When Alice, a user, needs to send a message to Bob, another user, Alice runs a user agent (UA) program to prepare the message and store it in Bob's mailbox.
   - Bob can retrieve and read the contents of his mailbox at his convenience, using a user agent.

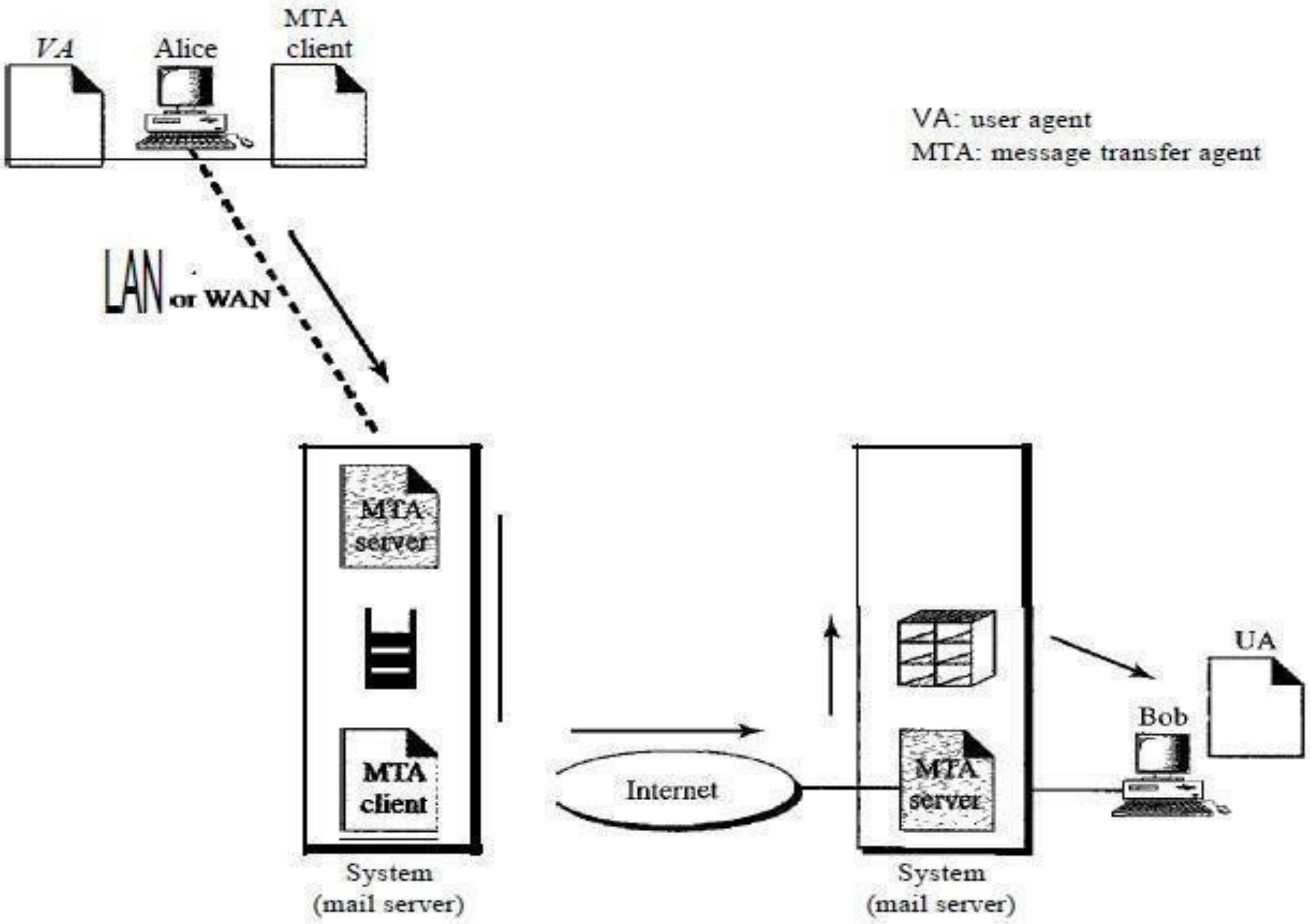
FIRST SCENARIO



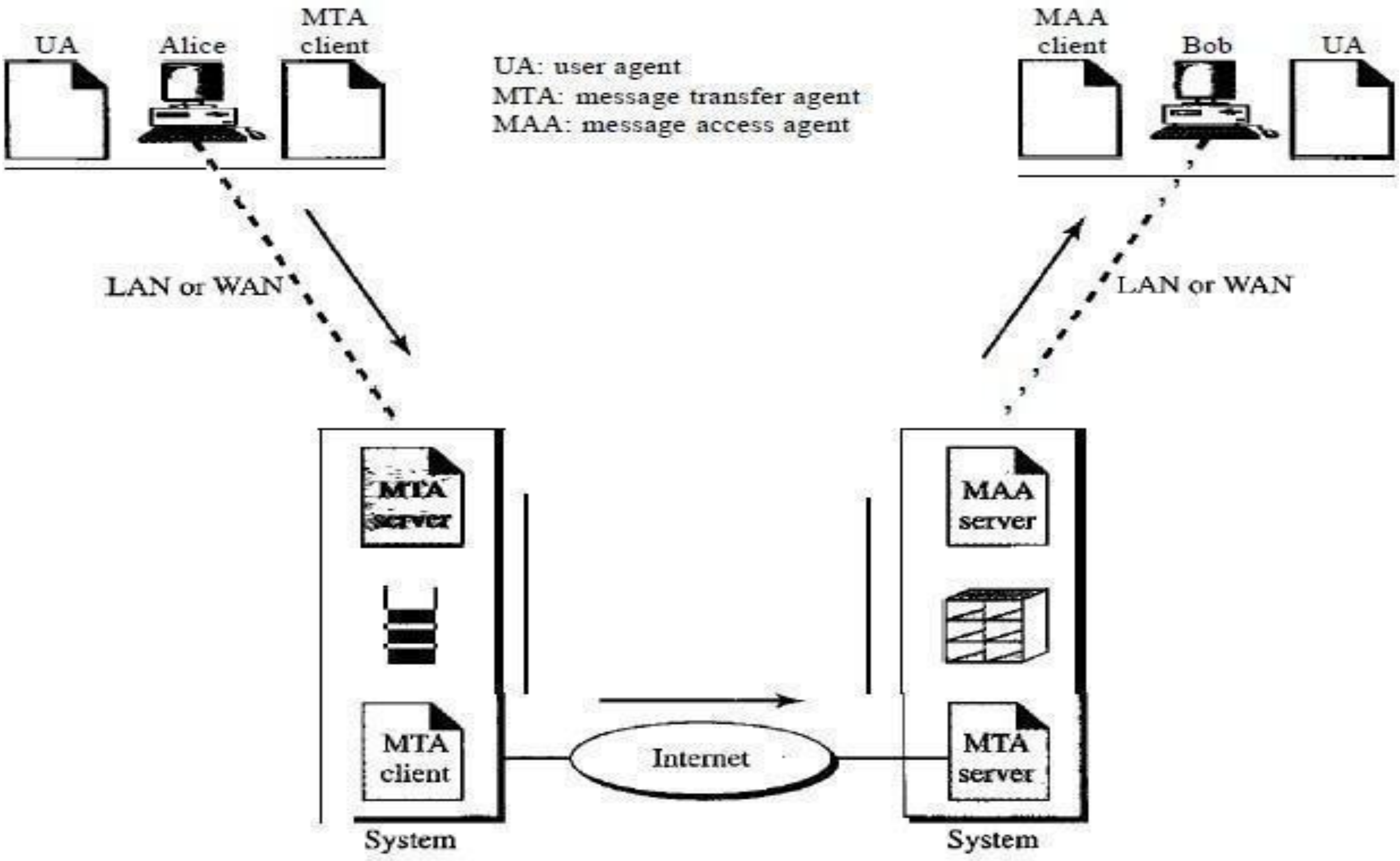
SECOND SCENARIO



THIRD SCENARIO



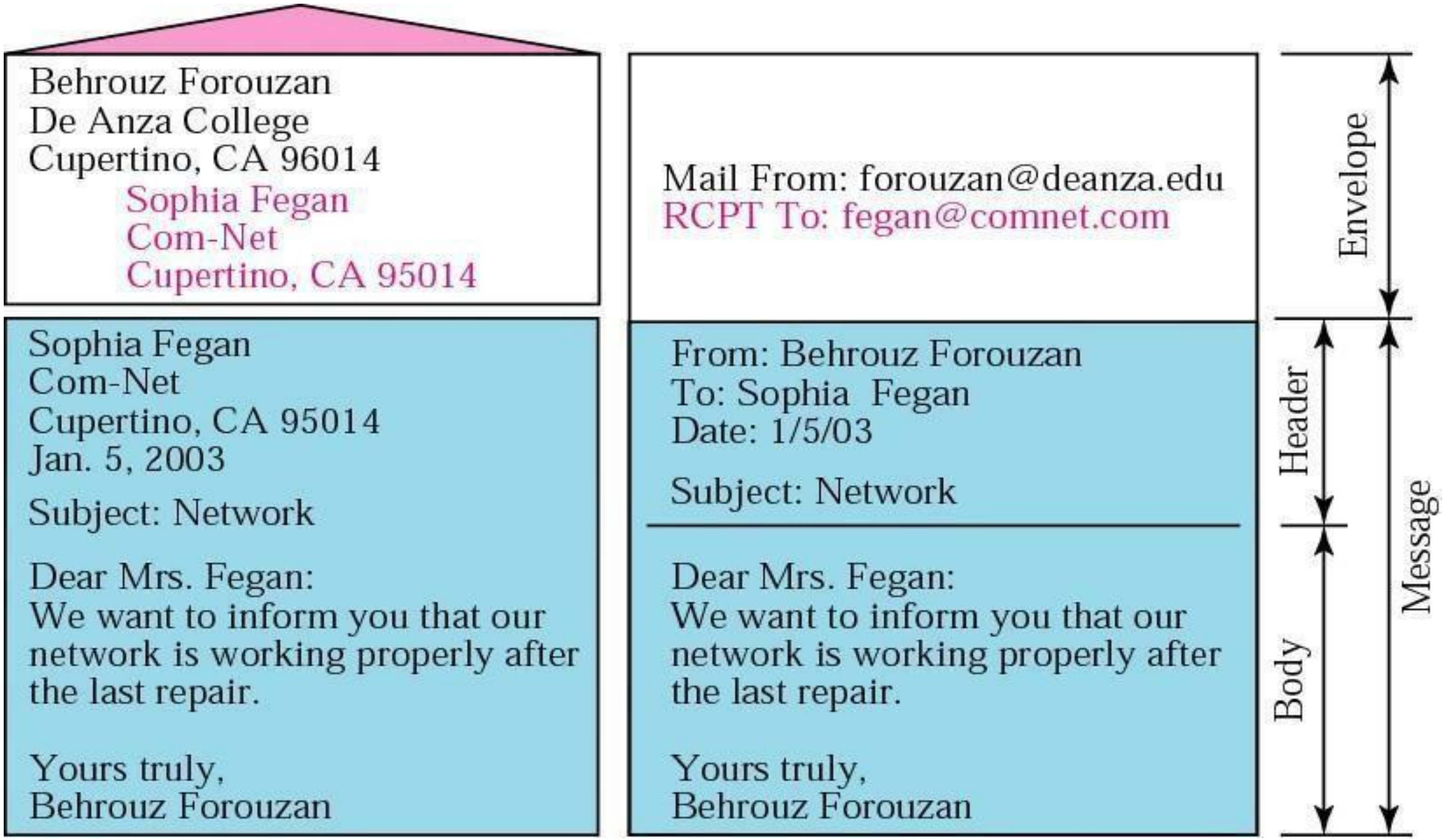
FOURTH SCENARIO



SENDING MAIL

1. To send mail the user creates mail that looks very similar to postal mail
2. It has envelope and a message.
3. **Enelope:**
   - the envelope usually contains the sender address, the receiver address and other information
4. **Message:**
   - Contains header and body.
   - The header of the message define the sender, the receiver, the subject of the message
   - The body of the message contains actual information to be read by the recipient.

FORMAT OF AN EMAIL



Behrouz Forouzan
De Anza College
Cupertino, CA 96014

Sophia Fegan
Com-Net
Cupertino, CA 95014

Sophia Fegan
Com-Net
Cupertino, CA 95014
Jan. 5, 2003

Subject: Network

Dear Mrs. Fegan:
We want to inform you that our network is working properly after the last repair.

Yours truly,
Behrouz Forouzan

Mail From: forouzan@deanza.edu
RCPT To: fegan@comnet.com

From: Behrouz Forouzan
To: Sophia Fegan
Date: 1/5/03

Subject: Network

Dear Mrs. Fegan:
We want to inform you that our network is working properly after the last repair.

Yours truly,
Behrouz Forouzan

Envelope

Header

Body

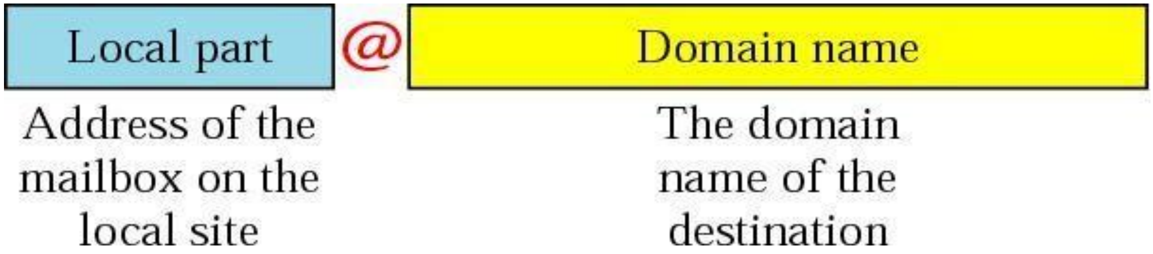
Message

RECEIVING MAIL

1. The receiving system periodically checks mailboxes.
2. If a user has mail, it informs the user with a notice.
3. If the user is ready to read the mail, a list is displayed in which each line contains a summary of the information about a particular message in the mailbox
4. The summary usually includes the sender mail address, the subject and the time the mail was sent or received.
5. The user can select any of the messages and display its contents on the screen.

EMAIL ADDRESS

1. To deliver mail, a mail handling system must user an addressing system with unique address.

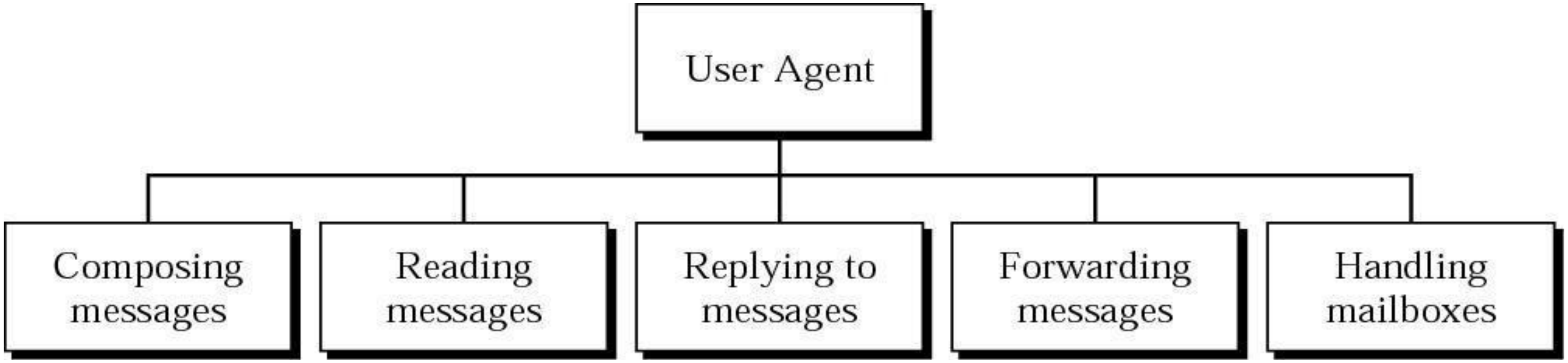

Local part
@
Domain name
Address of the mailbox on the local site
The domain name of the destination

1. Local part: defines the name of a special file, called the user mailbox, where all the mail received are stored for retrieval by the useragent.

USER AGENT

1. The first component of an electronic mail system is the user agent (UA).
2. It provides service to the user to make the process of sending and receiving a message easier.
3. A user agent is a software package (program) that
   - composes,
   - reads,
   - replies to,
   - and forwards messages
4. It also handles mailboxes

USER AGENT

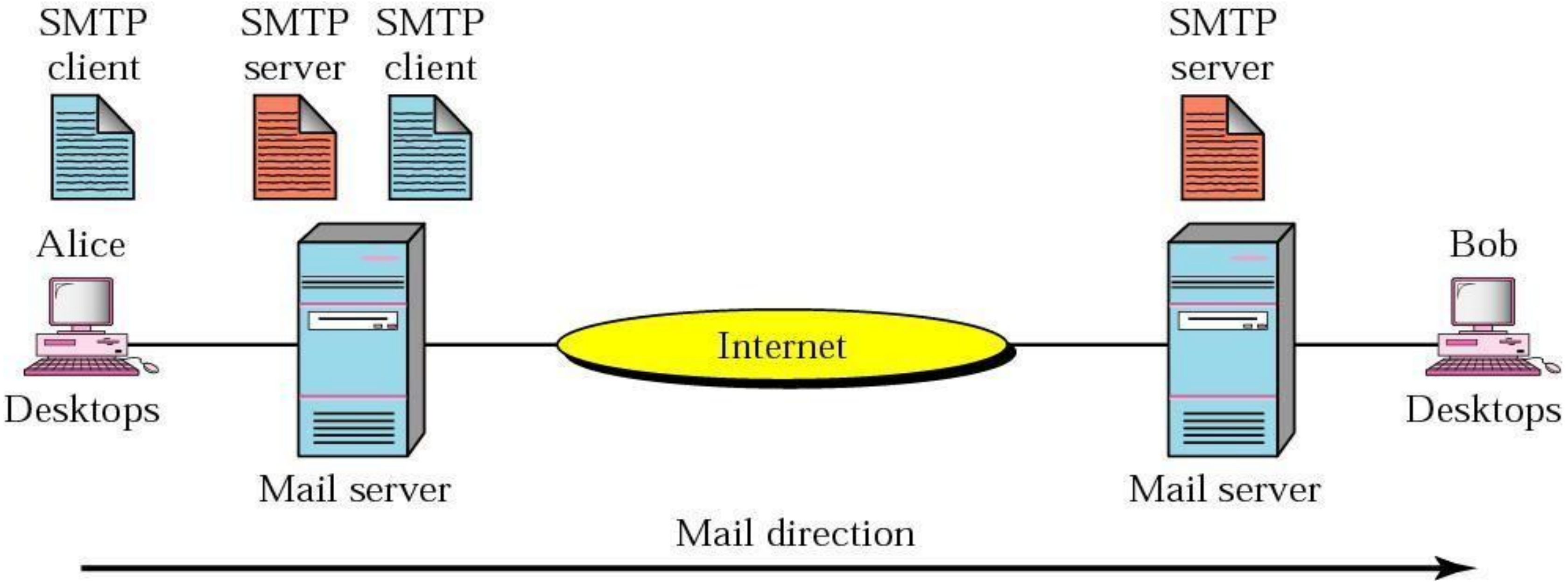

User Agent
Composing messages
Reading messages
Replying to messages
Forwarding messages
Handling mailboxes

MIME

1. MIME defines five headers that can be added to the original e-mail header section to define the transformation parameters:
   - 1. MIME-Version
   - 2. Content-Type
   - 3. Content-Transfer-Encoding
   - 4. Content-Id
   - 5. Content-Description

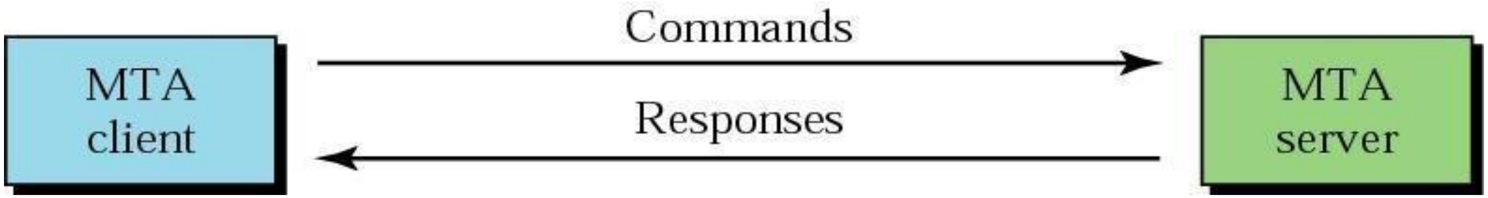
MTA CLIENT AND SERVER

1. Actual mail transfer is done through message transfer agents.
2. To send a mail, a sys must have client MTA and to rcv mail,a sys must have a server MTA.



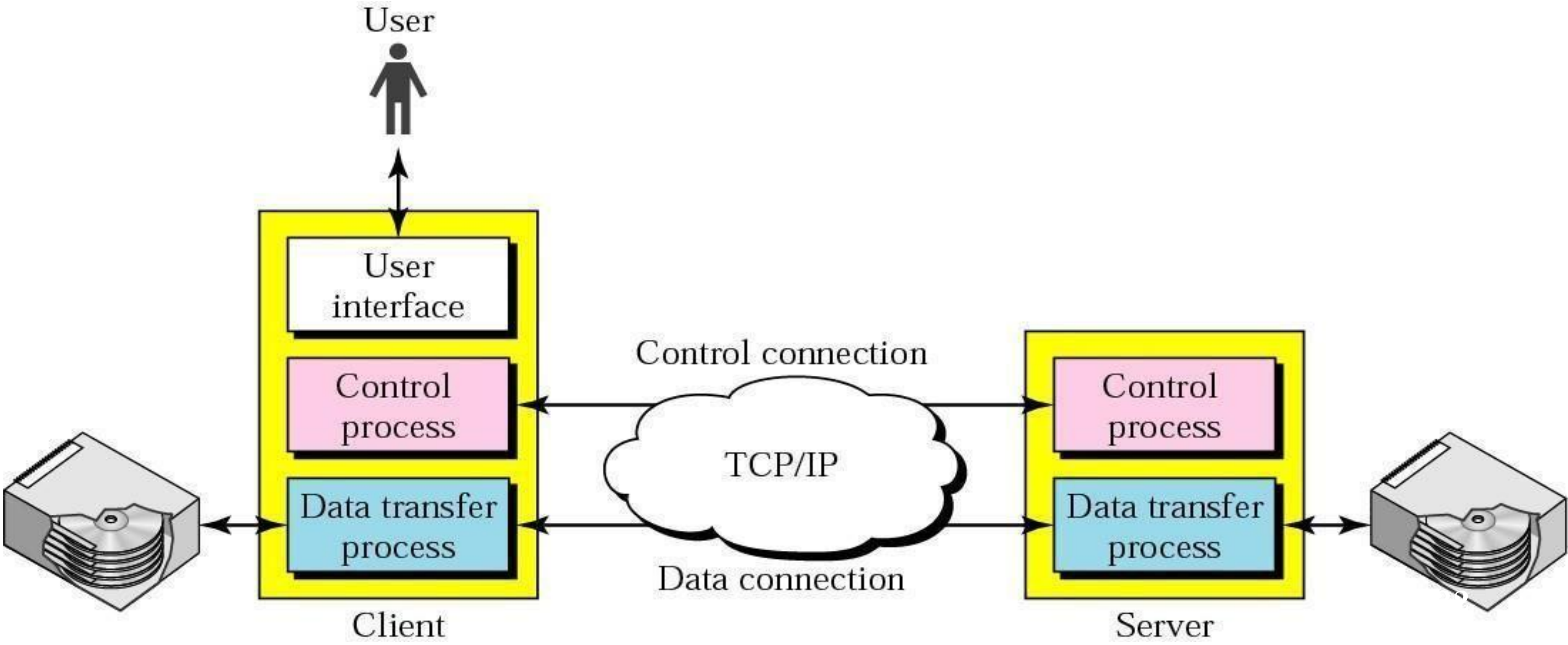
COMMANDS AND RESPONSES

1. SMTP simply defines how cmds and responses must be sent back and forth btw MTA client and MTA server.

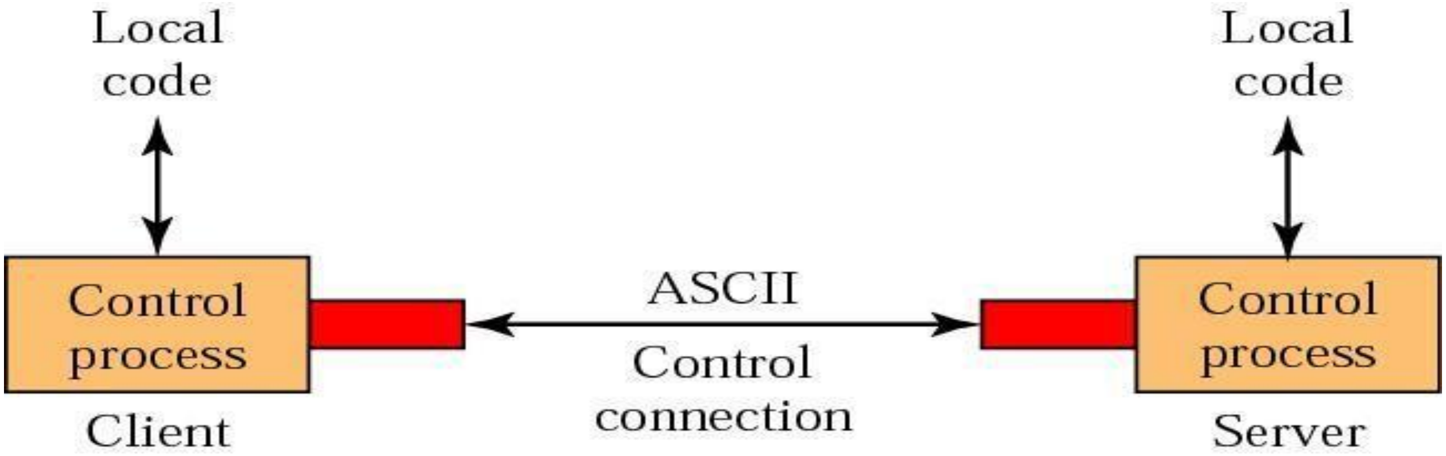


FTP CONNECTIONS

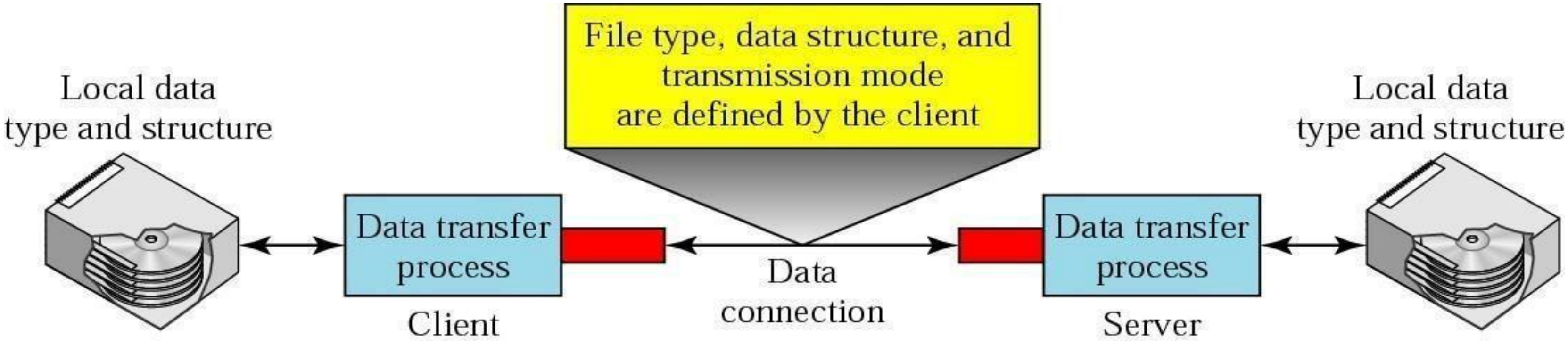
1. **Control connection** remains connected during entire interactive ftp session.
2. **data connection** is opened and then closed for each file transferred.when a user starts ftp session,cc opens,while cc opens,data connection is opened and closed multiple times.



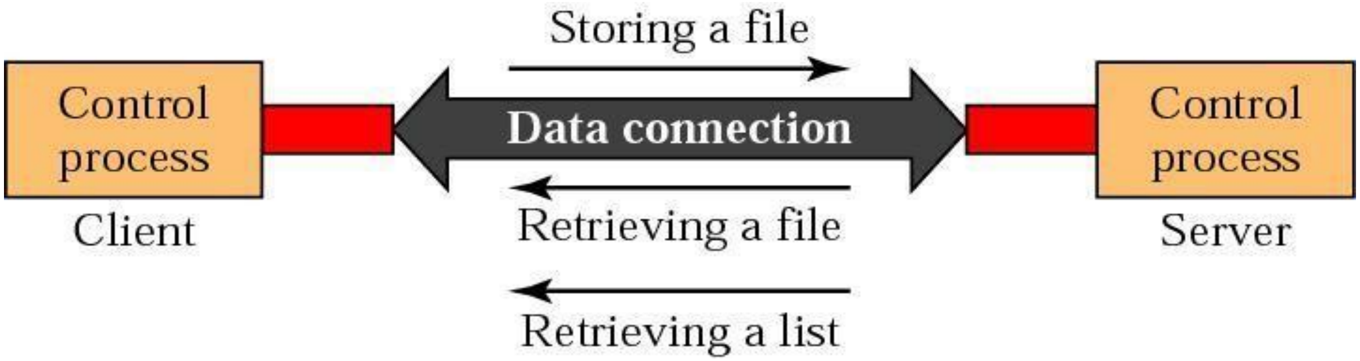
COMMUNICATION OVER CONTROL CONNECTION



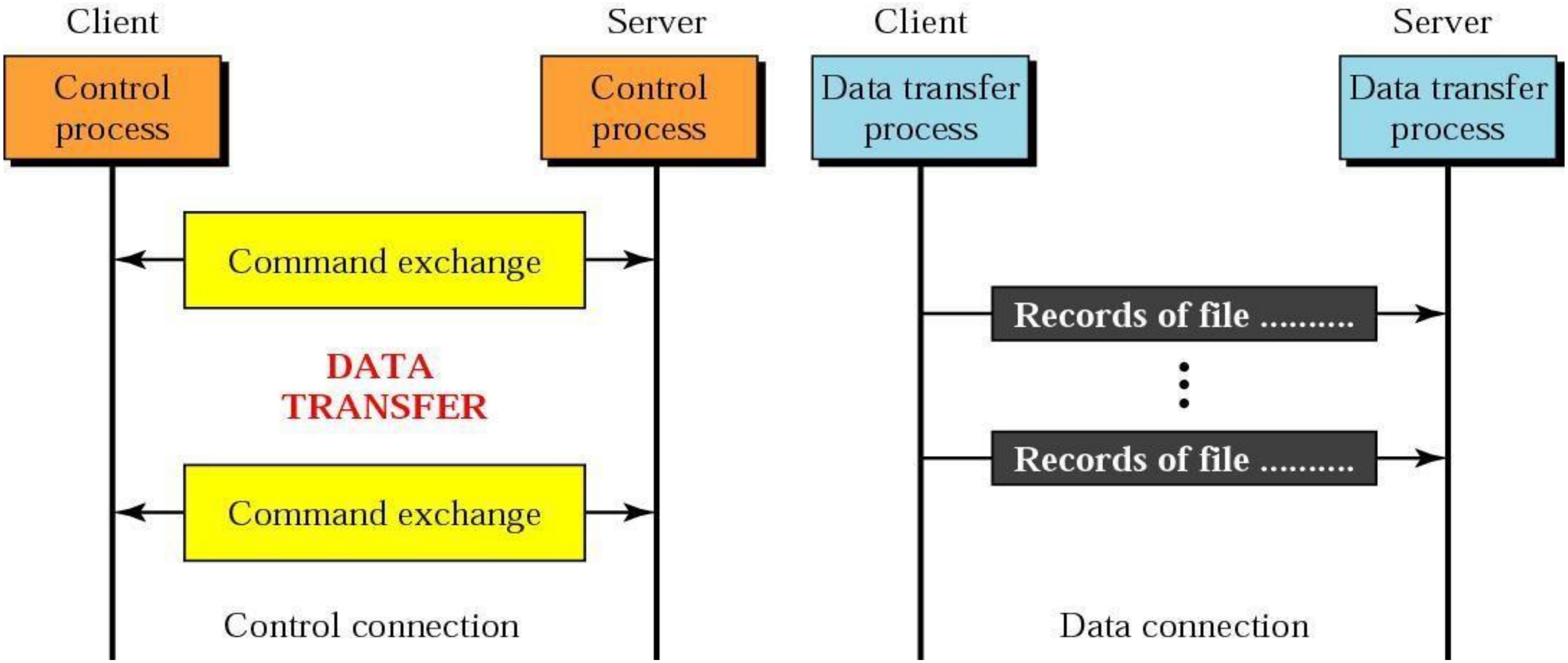
USING THE DATA CONNECTION


File type, data structure, and transmission mode are defined by the client
Local data type and structure
Data transfer process
Client
Data connection
Data transfer process
Server
Local data type and structure

FILE TRANSFER



EXAMPLE 1


Client
Server
Control process
Control process
Command exchange
DATA TRANSFER
Command exchange
Control connection
Client
Server
Data transfer process
Data transfer process
Records of file ....
Records of file ....
Data connection

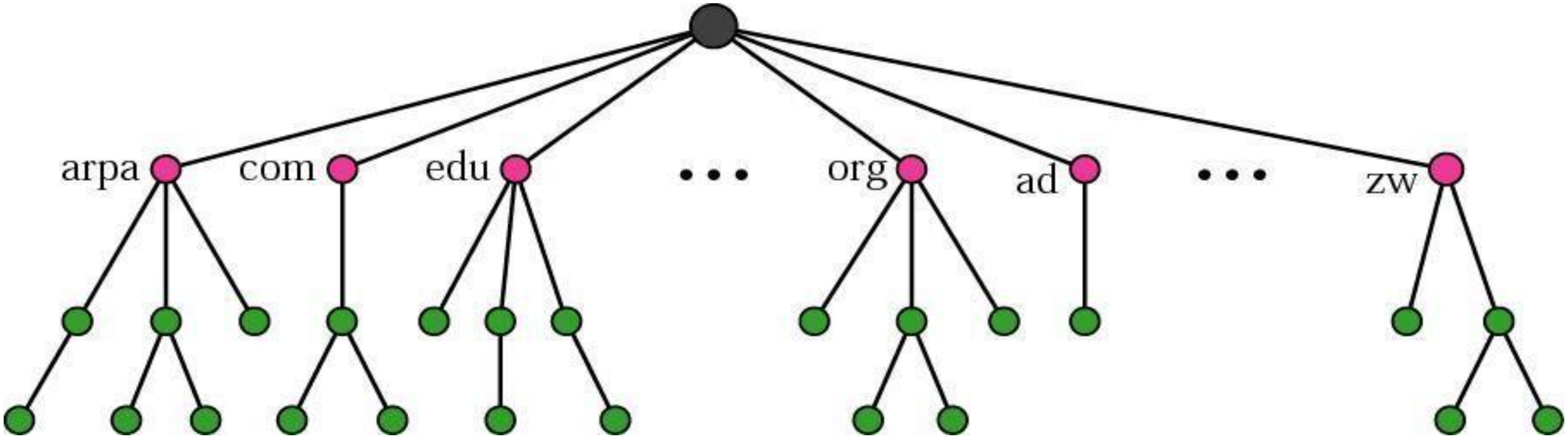
NAMESPACE

1. DNS is supporting program that is used by other programs such as email.
2. To be unambiguous, the names assigned to machine must be carefully selected from a name space.
3. Flat Name Space:a name is assigned to an address.
4. a name in this space is sequence of chars without structure.
5. main disadv it cannot b usd in large sys such as internet.
6. **Hierarchical Name Space:**
7. Each name is made of several names first part can
8. define nature of orgn ,second part can define depts in orgn

   here authority to assign and control name spaces can b decentralized.

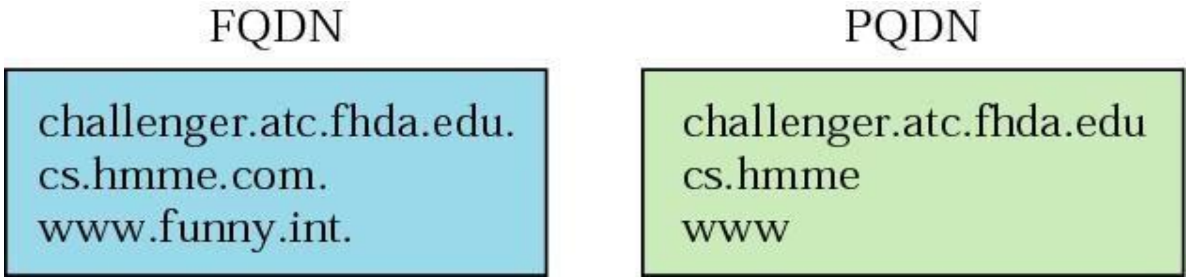
DOMAIN NAME SPACE

1. To have a hierarchical name space a domain name space was designed.
2. Names r defined using inverted tree structure with root at top.
3. Tree can have from 0 to 127levels.
4. Each node in tree has label which is string with max of63 chars.
5. Each node in tree has domain name .



FQDN AND PQDN

1. If domain name is terminated by null string, itis called fully qualified domain name.
2. If domain name is not terminated by null string, it is called partially qualified domain name



FQDN

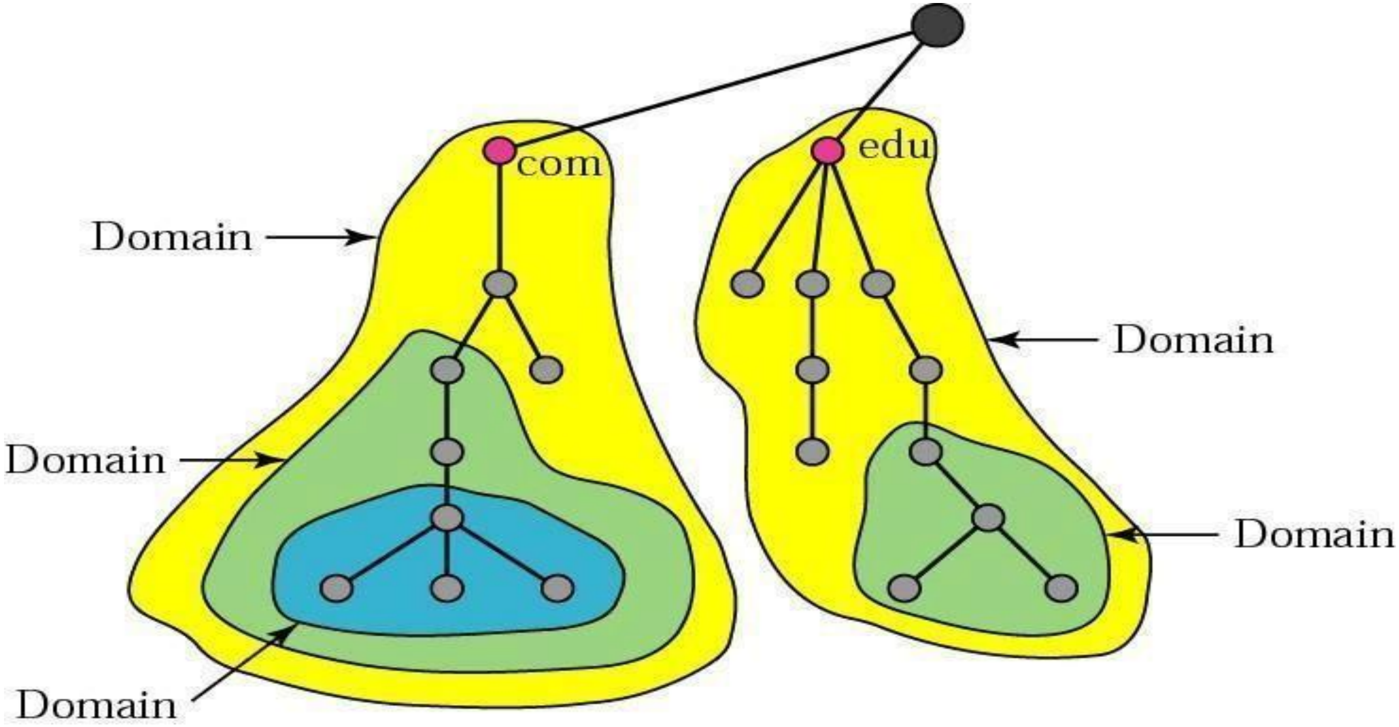
challenger.atc.fhda.edu.
cs.hmme.com.
www.funny.int.

PQDN

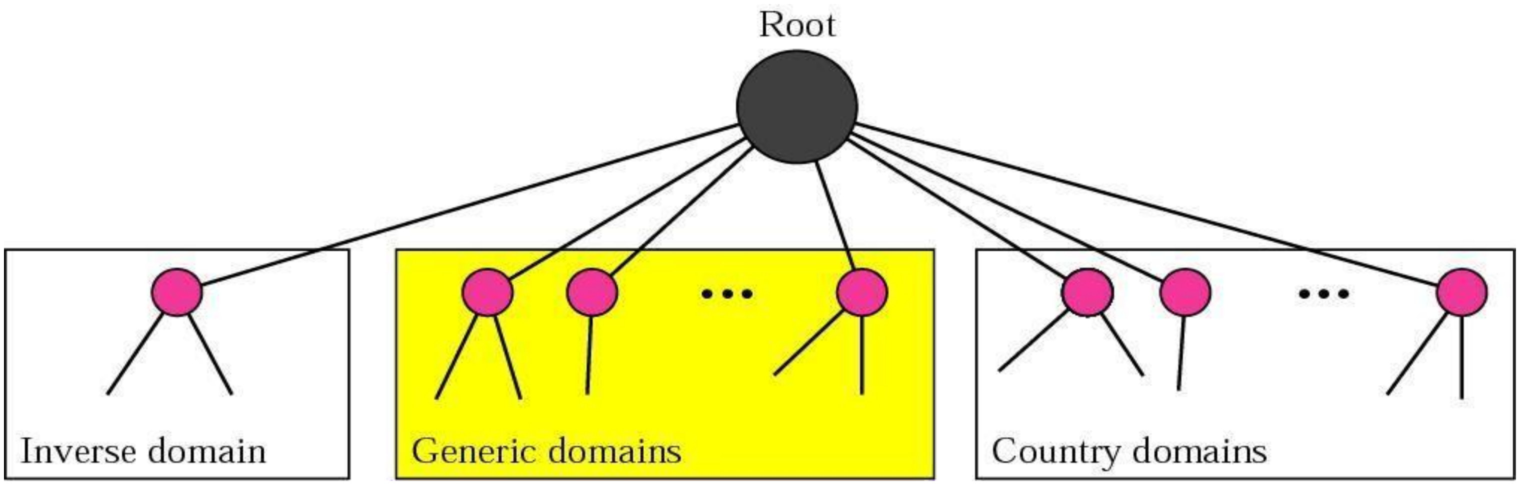
challenger.atc.fhda.edu
cs.hmme
www

DOMAINS

1. Adomain is asub tree of domain name space.
2. The name of the domain is the domain name of the node at the top of the sub tree.



DNS IN THE INTERNET



GENERIC DOMAINS

1. The generic domains define registered hosts according to their generic behavior.

2. Each node in the tree defines a domain, which is an index to the domain name space database

COUNTRY DOMAINS

1. The country domains section uses two- character country abbreviations (e.g., us for
2. United States).
3. Second labels can be organizational, or they can be more specific, national designations.
4. The United States, for example, uses state abbreviations as a subdivision of us (e.g., ca.us.).
5. The address *anza.cup.ca.us can* be translated to De Anza College in Cupertino, California, in the United States.

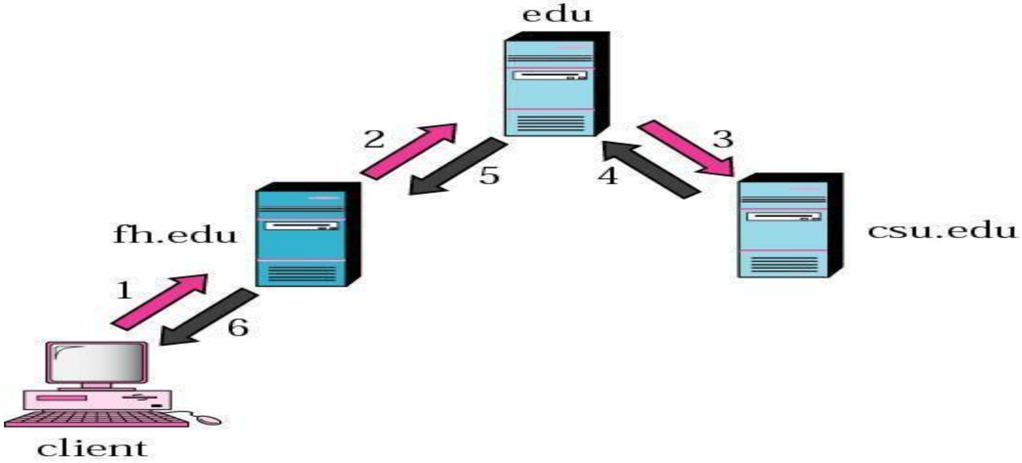
INVERSE DOMAIN

1. The inverse domain is used to map an address to a name.

2. This may happen, for example, when a server has received a request from a client to do a task.

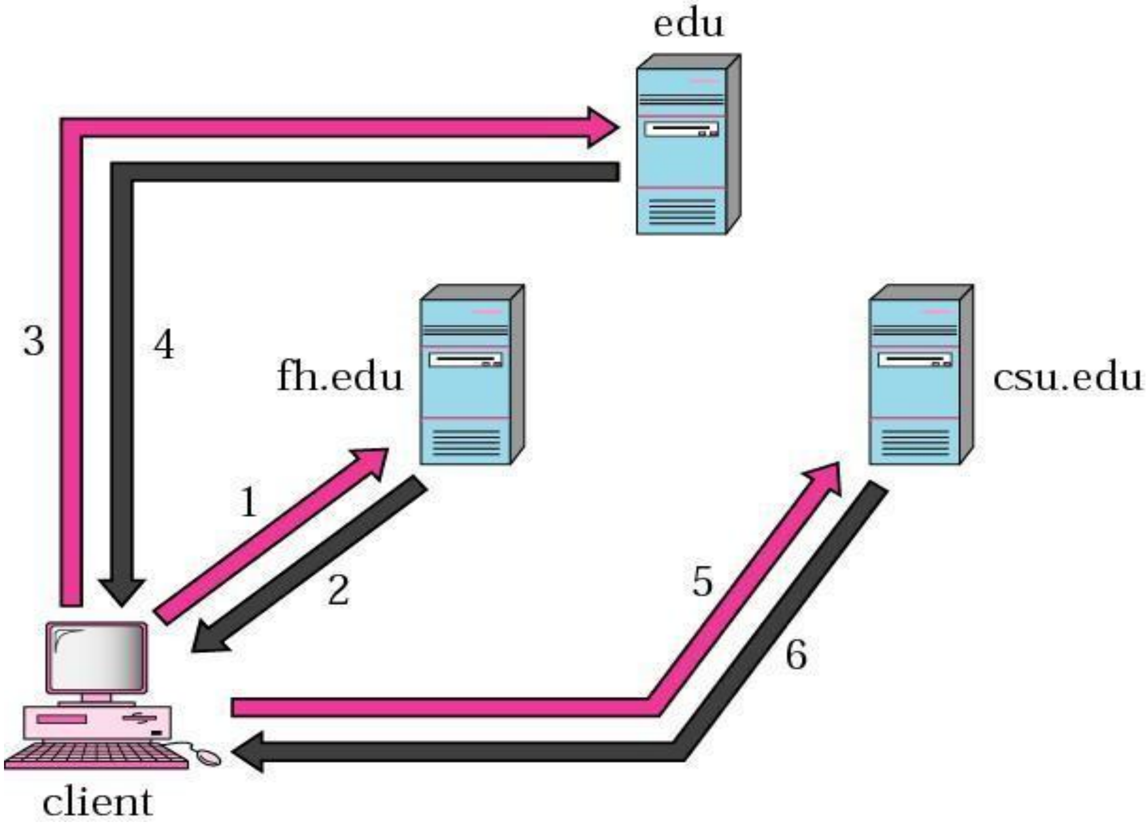
RECURSIVE RESOLUTION

1. Dns is designed as a client server appn.a host that needs to map an address to a name or a name to an address calls a dns client called a resolver.resolver accesses the closest dns server with a mapping req.if the server has infn ,it satisfies resolver otherwise it asks resolver to refer other server r to give infn frm other servers.
2. Mapping names to addresses
3. Mapping addresses to names.
4. <u>Recursive resolution</u>:resolver expects server to supply final answer.



ITERATIVE RESOLUTION

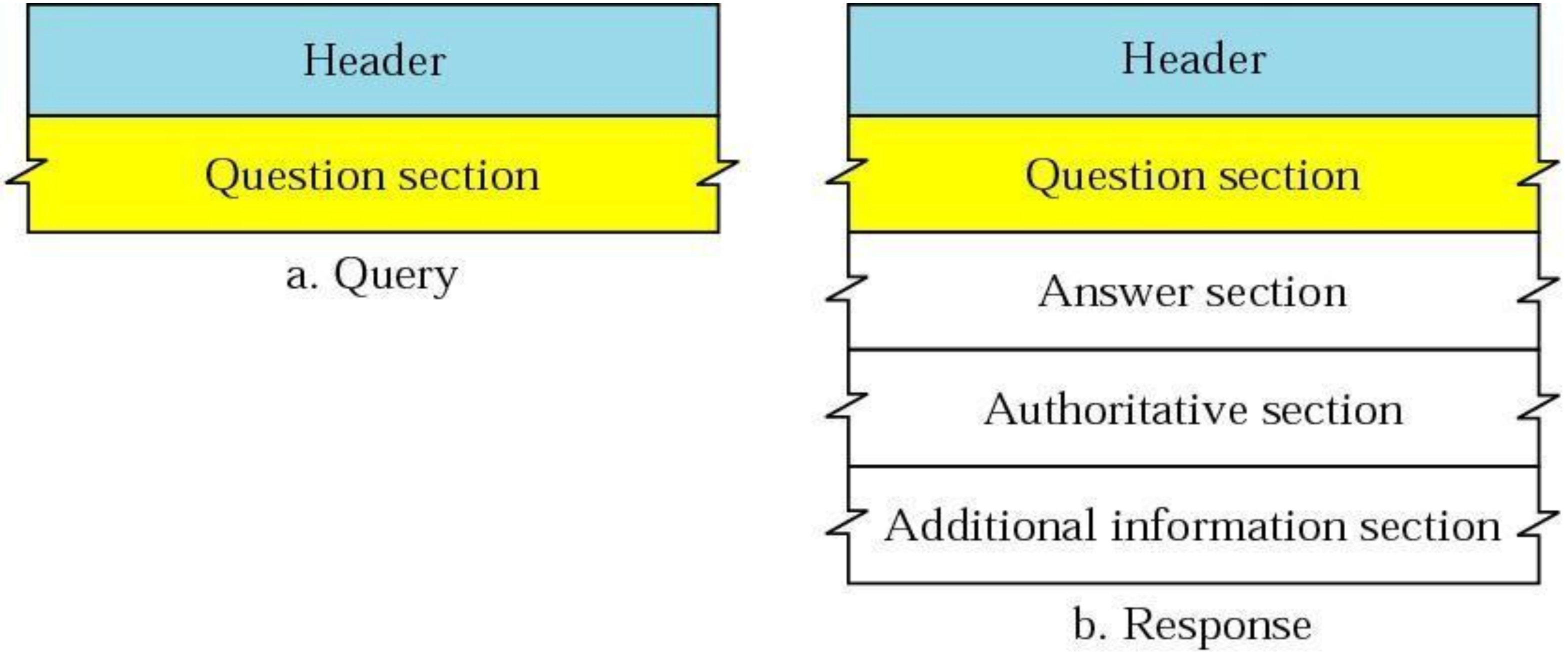
1. Client repeats same query to multiple servers.



QUERY AND RESPONSE MESSAGES

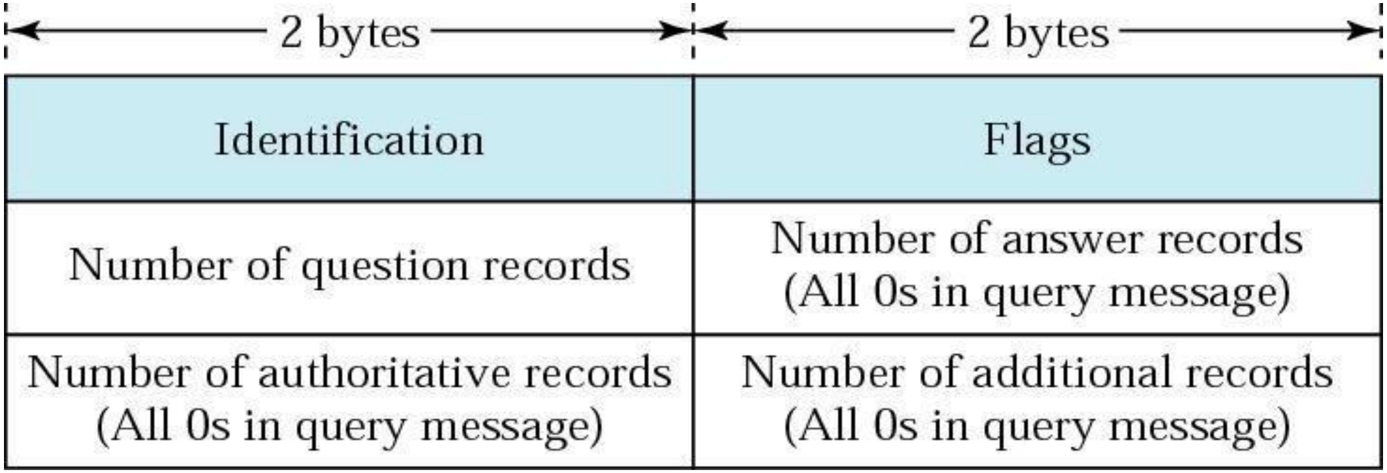
DNS MESSAGES

1. Identification subfield is used by client to match response with query.



HEADER FORMAT

1. Id field is usd by client to match response with query.flags field define type of msg, type of answer requested, type of desired resolution.no.of question records contains no. of queries in question section of msg.



2 bytes	2 bytes
Identification	Flags
Number of question records	Number of answer records (All 0s in query message)
Number of authoritative records (All 0s in query message)	Number of additional records (All 0s in query message)