UNIT –III

LOCAL AREA NETWORK & UPPER LAYERS

Introduction

The networks can be divided into two categories as follows:

- Point-to-point network
- Broadcast network

- In any broadcast network, the key issue is how to determine who gets to use the channel when there is competition for it.
- Broadcast channels are sometimes referred to as **multi access channels** or **random access channels**.
- The protocols used to determine who goes next on a multi access channel belong to a sublayer of the data link layer called the **MAC** (**Medium Access Control**) sublayer.

The Channel Allocation Problem

- In a broadcast network, the single broadcast channel is to be allocated to one.
- This is called as channel allocation.
- There are two different schemes used for channel allocation as follows:
  - **Static channel allocation**
  - **Dynamic channel allocation**

Static channel allocation

- The traditional way of allocating a single channel, such as a telephone trunk, among multiple competing users is Frequency Division Multiplexing (FDM).
- If there are *N* users, the bandwidth is divided into *N* equal-sized portions , each user being assigned one portion.
- Since each user has a private frequency band, there is no interference between users.
- When there is only a small and constant number of a user, each of which has a heavy load of traffic, FDM is a simple and efficient allocation mechanism.

Dynamic channel allocation

- In this method no fixed frequency or fixed time slot is allotted to the user.
- The user can use the single channel as per his requirement.

Following assumptions are made for the implementation of this method.

1. STATION MODEL
2. SINGLE CHANNEL ASSUMPTION
3. COLLISION ASSUMPTION

4.1 CONTINUOUS TIME

4.2 SLOTTED TIME

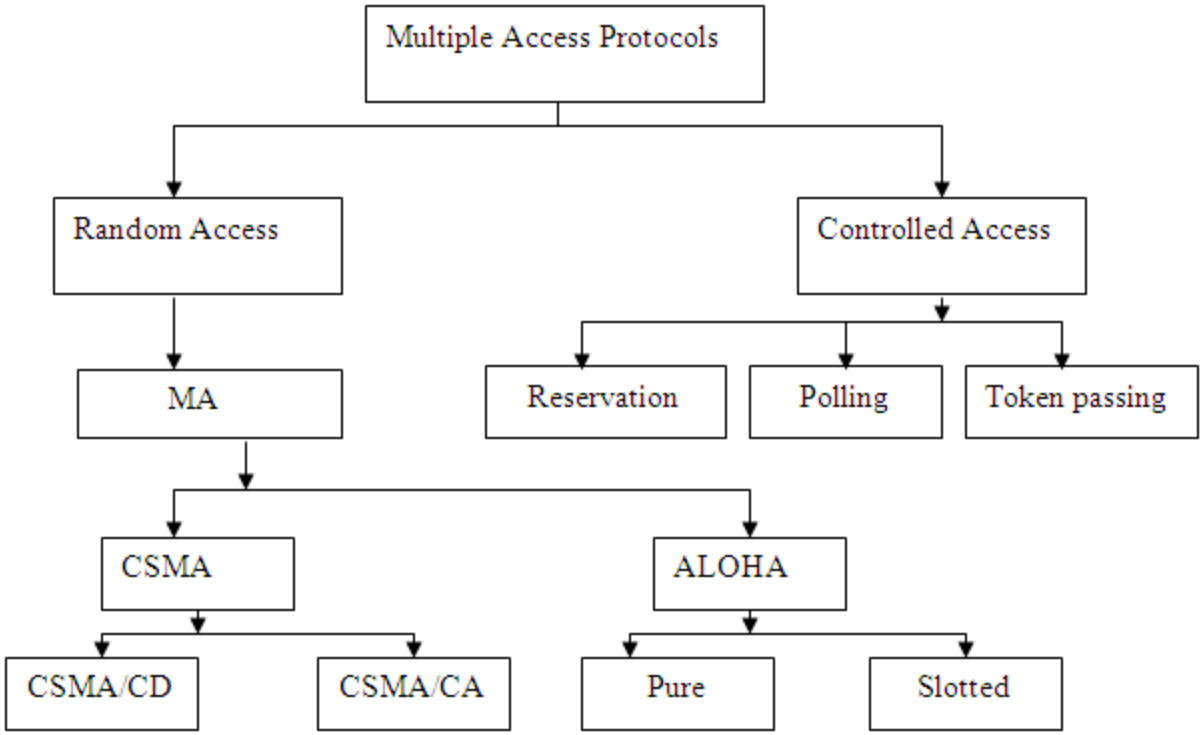
5.1 CARRIER SENSE

5.2 NO CARRIER SENSE

Multiple Access

- The techniques used to deal with the multiple access problem are as follows:
  - Random access
  - Controlled access

Multiple Access Protocol



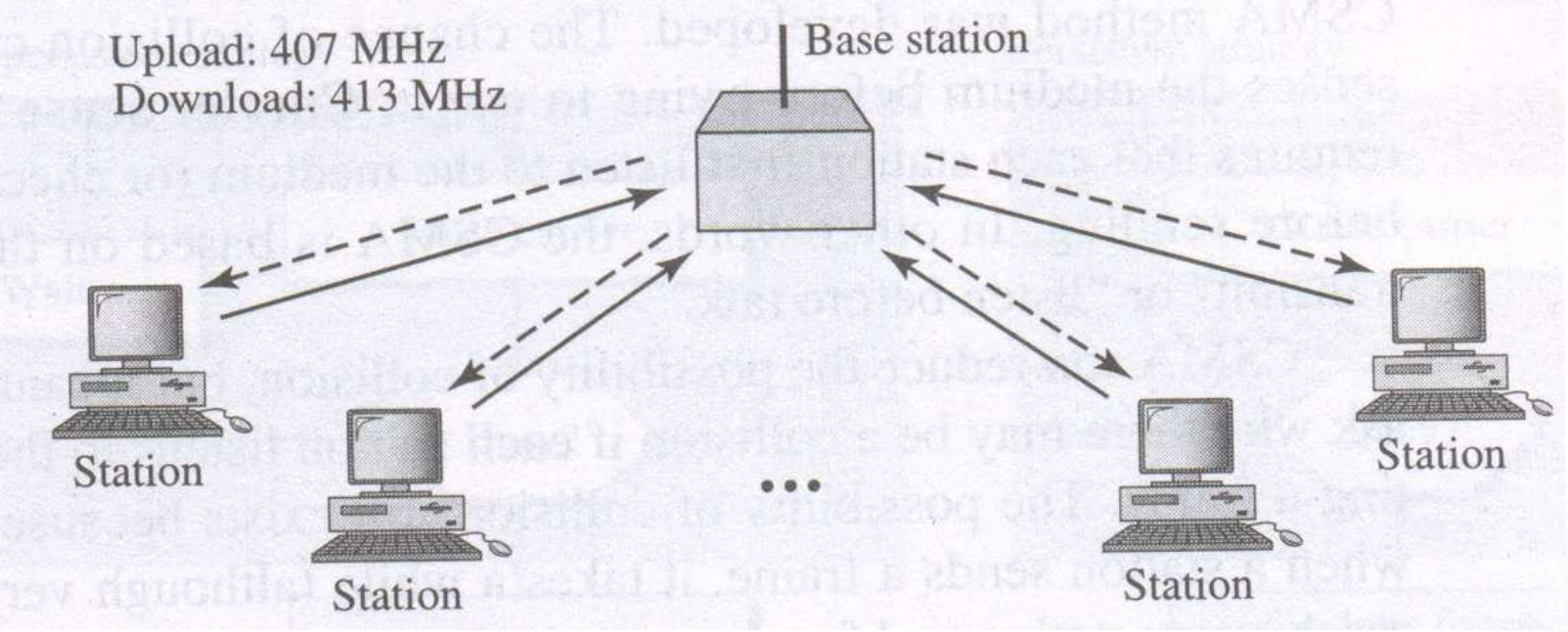
Random access

- In the random access there is no control station.
- Each station will have the right to use the common medium without any control over it.

ALOHA

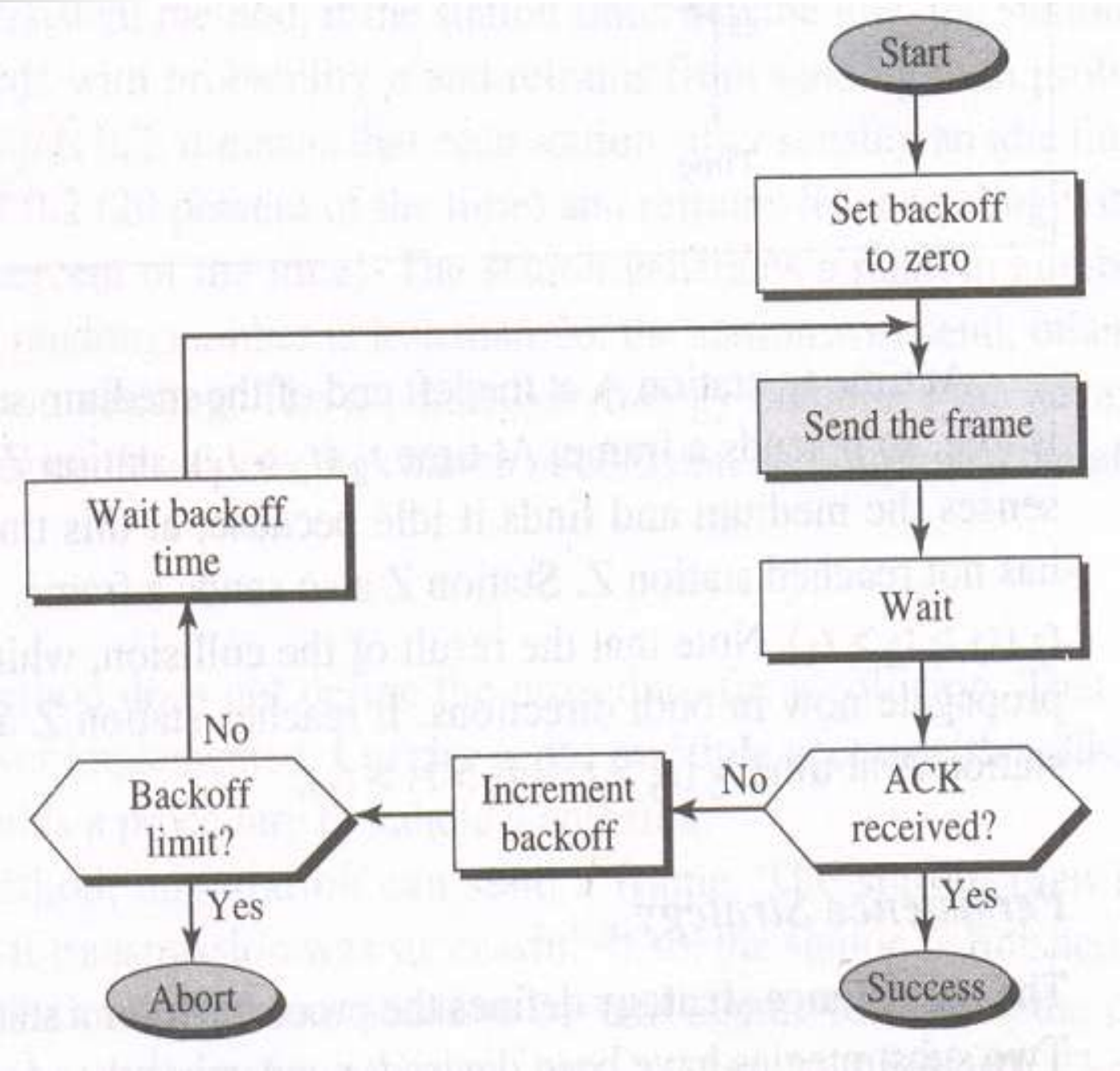
- The earliest random access method was developed at the University of Hawaii, in the early 1970's by Norman Abramson and his colleagues.
- The basic idea is applicable to any system in which uncoordinated users are competing for the use of a single shared channel.
- The ALOHA protocol is very simple. It is based on the following rules
  - **Multiple access:** any station sends a frame when it has a frame to send.
  - **Acknowledgment**: after sending the frame, the station waits for an acknowledgment.

ALOHA network



ALOHA network

- A base station is the central controller.
- Every station that needs to send a frame to another station first sends it to the base station.
- The base station receives the frame and relays it to the intended destination.
- The uploading transmission (from a station to the base station) uses modulation with a carrier frequency of 407 MHz.
- The downloading transmission (from the base station to any station) uses modulation a carrier frequency of 413 MHz.



Procedure for ALOHA protocol

Explanation

- A station which has a frame ready will send it.
- Then it waits for some time.
- If it receives the acknowledgment then the transmission is successful.
- Otherwise the station uses a backoff strategy , and sends the packet again.
- After many times if there is no acknowledgement then the station aborts the idea of transmission.

The ALOHA system has two versions:

- Pure ALOHA
- Slotted ALOHA

Pure ALOHA

- It works on a very simple principle.
- Essentially it allows for any station to broadcast at any time.
- If two signals collide, each station simply waits a random time and try again.
- Collisions are easily detected.
- When the central station receives a frame it sends an acknowledgement on a different frequency.
- If a user station receives an acknowledgement it assumes that the transmitted frame was successfully received and if it does get an acknowledgement it assumes that collision had occurred and is ready to retransmit.

Efficiency of Pure ALOHA Channel

- Let G be the average number of frames generated per slot.
- S is the throughput(is the average rate of successful frame delivery per slot) can be defined as

$$S = G\, e^{-2G}$$

$$e = 2.718$$

- The maximum throughput occurs at G = 0.5 , with S=1/(2*e) which is about 0.184 or 18.4%.

Slotted ALOHA

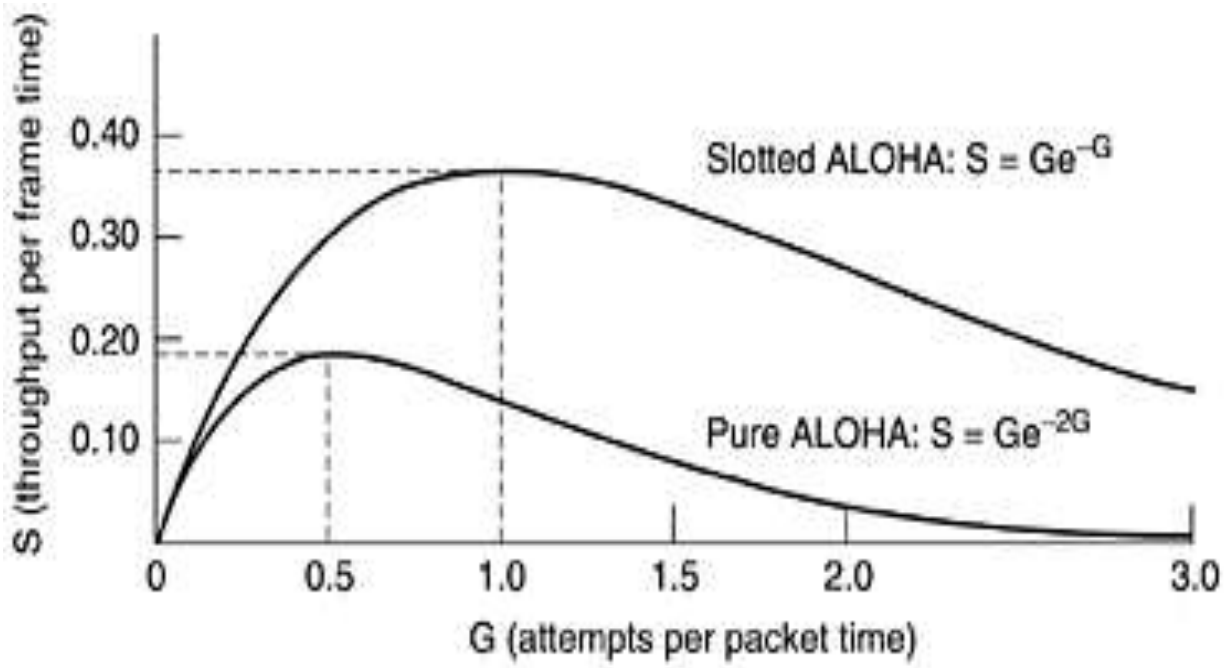
- In 1972, Roberts published a method for doubling the capacity of an ALOHA system.
- His proposal was to divide time into discrete intervals, each interval corresponding to one frame.
- This approach requires the users to agree on slot boundary.
- One way to achieve synchronization would be to name one special station emit a pip at the start of each interval, like a clock.

- Thus, the continuous pure ALOHA is turned into a discrete one.
- Throughput can be defined as

$$S=Ge^{-G}$$

- As you can see from slotted ALOHA peaks at G=1, with a throughput of S=1/e or about 0.368, twice that of pure ALOHA.

Throughput versus offered traffic for ALOHA system



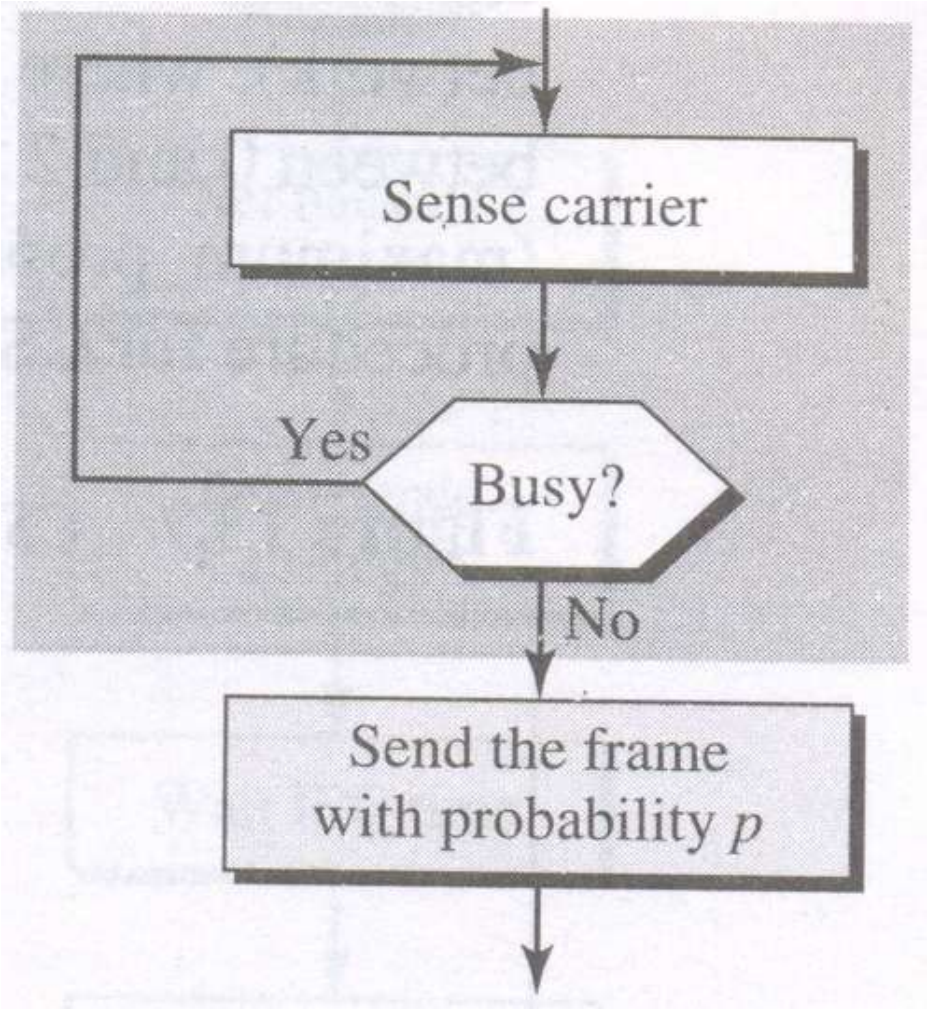
Carrier Sense Multiple Access (CSMA)

- The CSMA protocol operates on the principle of carrier sensing.
- In this protocol, a station listens to see the presence of transmission (carrier) on the cable and decides to act accordingly.

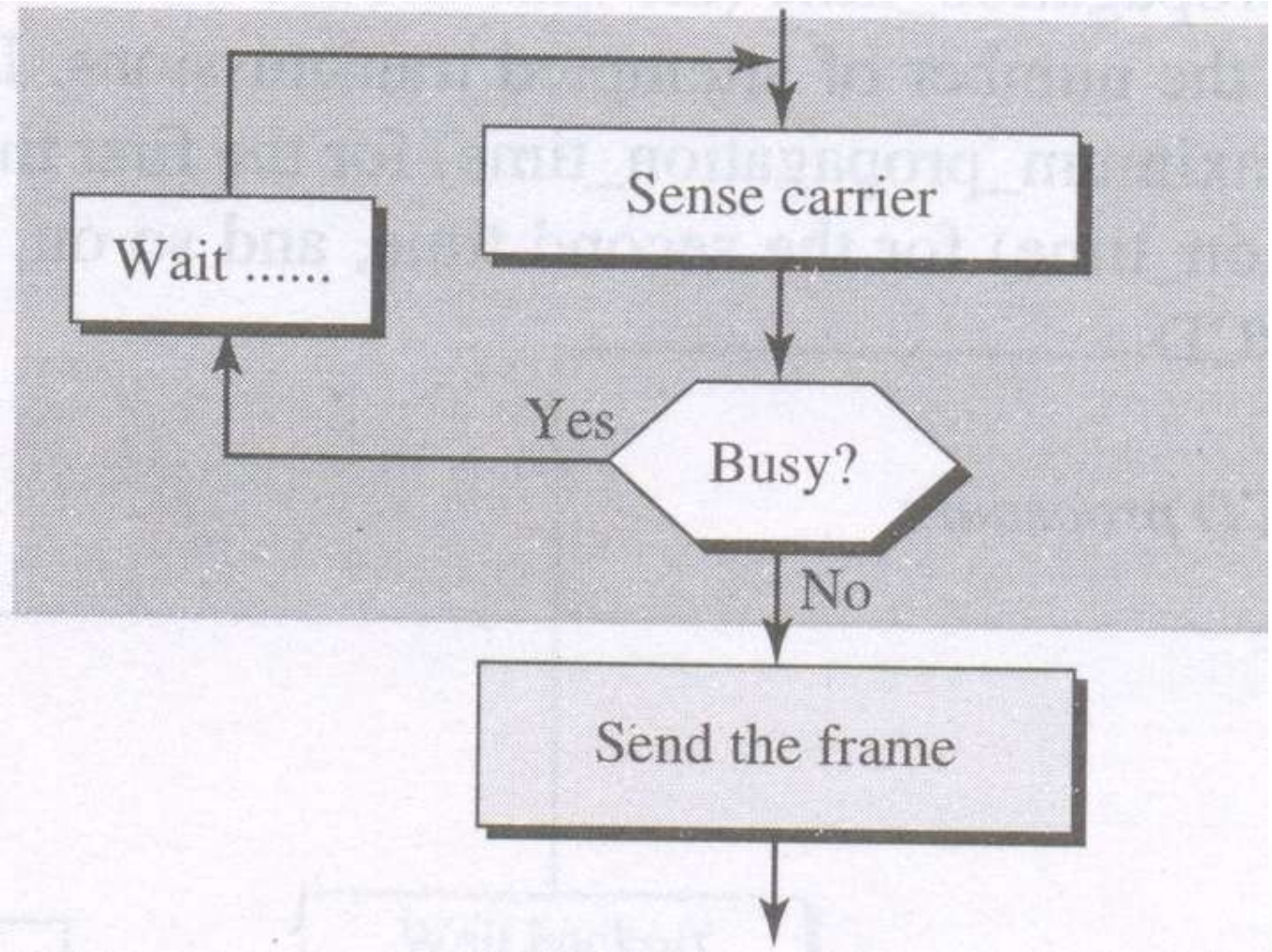
CSMA

- Persistent
- Non-persistent

Persistent



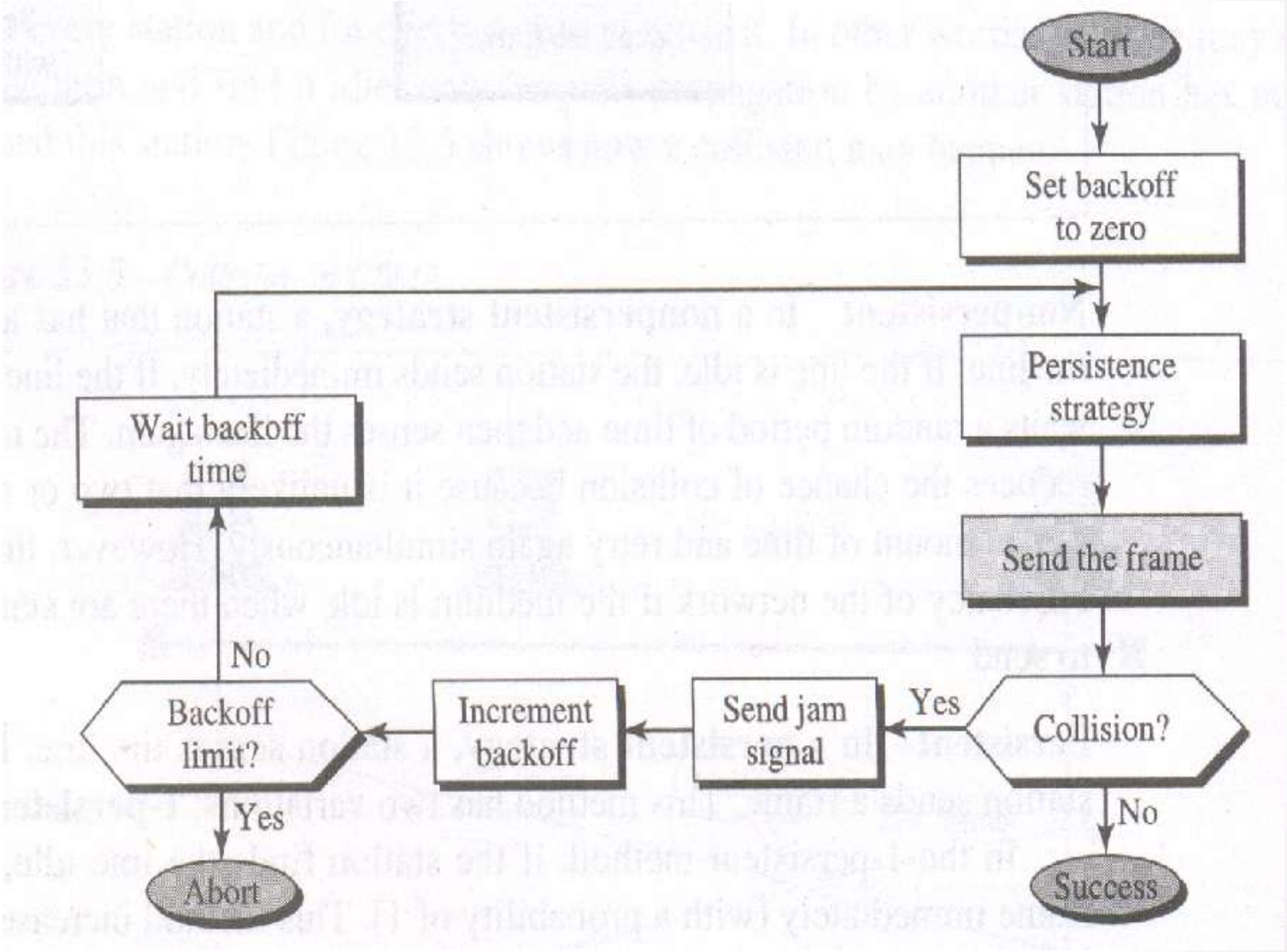
Non-persistent



CSMA with collision detection (CSMA/CD)

- If two stations sense the channel to be idle and begin transmitting simultaneously, they will both detect the collision almost immediately.
- Rather than finish transmitting their frames, they stop transmitting and release a jam signal as soon as the collision is detected.
- Quickly terminating damaged frames saves time and bandwidth. This protocol known as CSMA/CD.

CSMA/CD Procedure



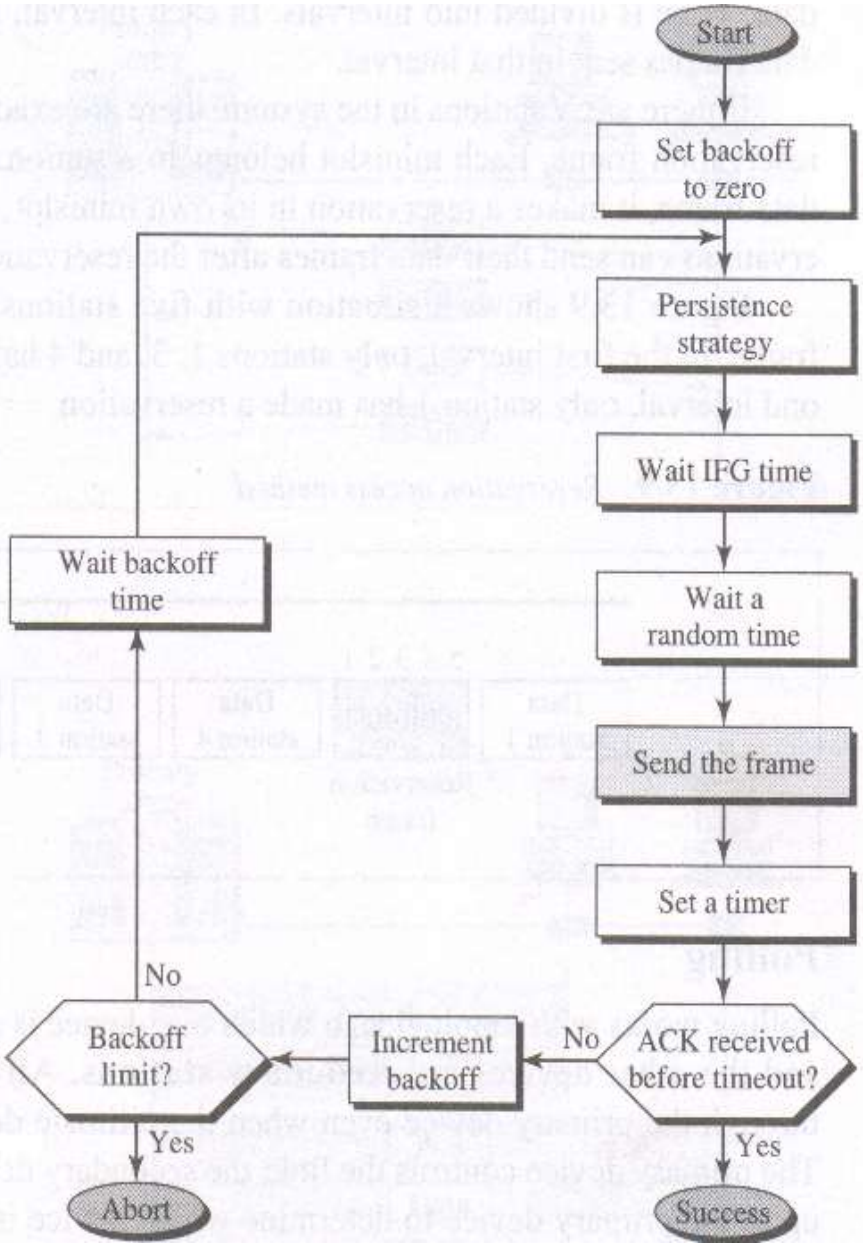
Efficiency of CSMA/CD

- A careful design can achieve efficiencies of more than 90%.

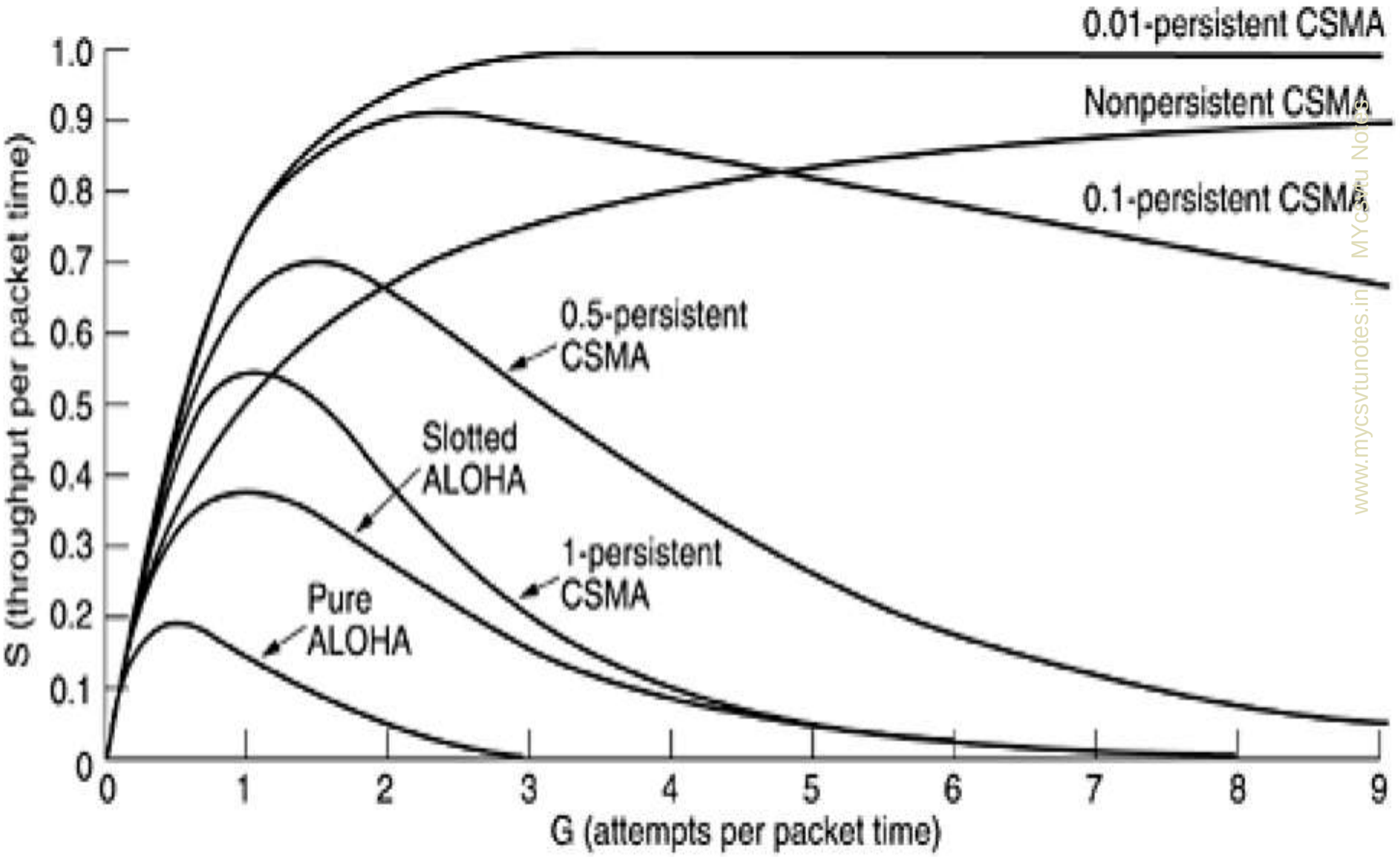
CSMA with Collision Avoidance(**CSMA/CA**)

- The station uses one of the persistence strategies.
- After it finds the line idle, the station waits an IFG (Inter-Frame-Gap) amount of time.
- It then waits another random amount of time. After that, it sends the frame and sets a timer.
- The station waits for an acknowledgement from the receiver.
- If the acknowledgement is received before expiry of the timer, then the transmission is successful.
- If the transmitting station does not receive the expected acknowledgement before the timer expiry then it increments the back off parameters, waits for the back off time and re-senses the line.

CSMA/CA Procedure



Comparison of the channel utilization versus load



IEEE 802

- Institute of Electrical and Electronics Engineers (IEEE) has produced several standards for LANs.
- These standards, collectively known as IEEE 802.
- The standards are divided into parts.

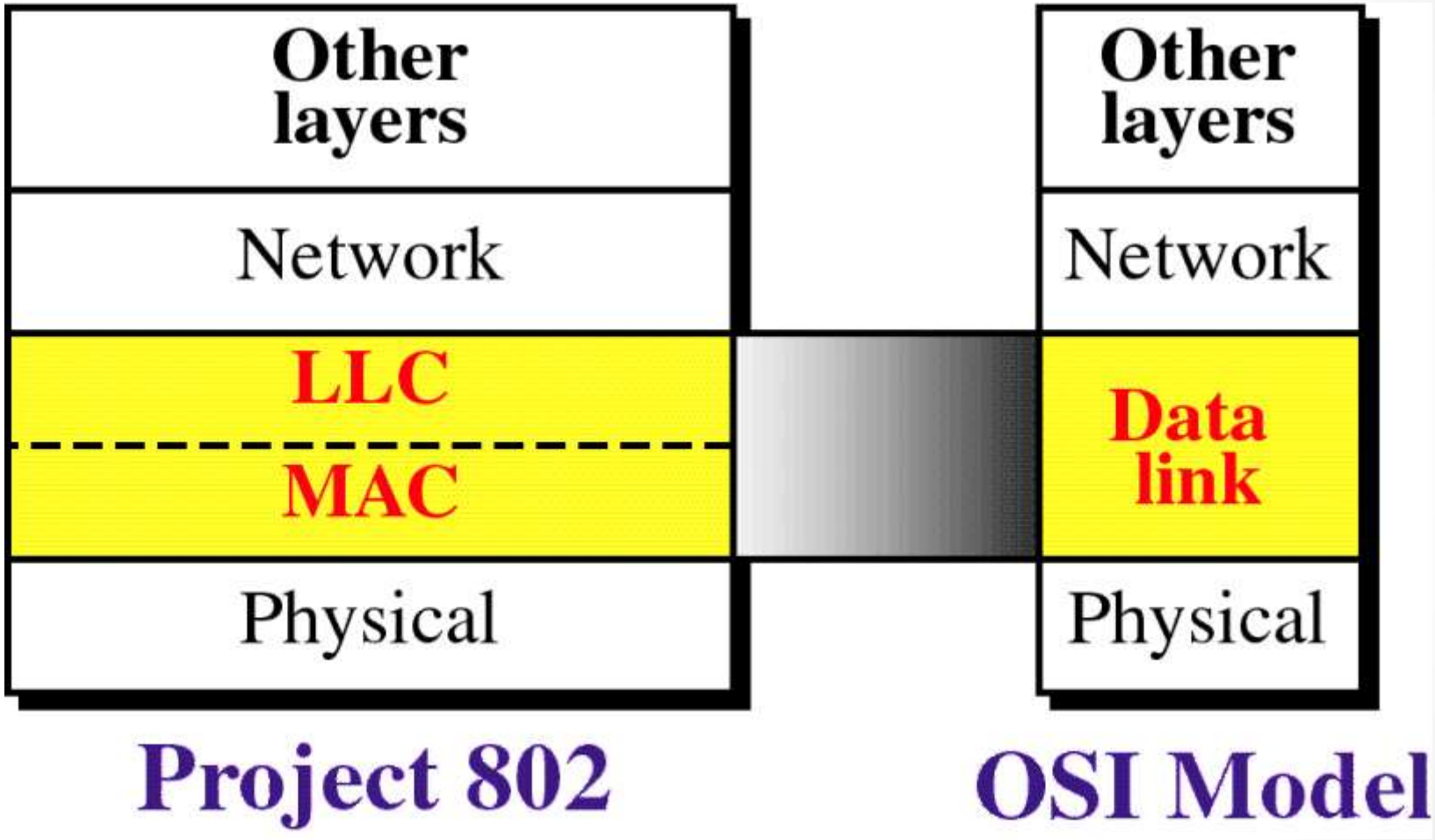
IEEE 802.x Standards

802.1	Architecture, Management,Internetworking
802.2	Logical Link Control (LLC)
802.3	CSMA/CD LAN
802.4	Token Bus LAN
802.5	Token Ring LAN
802.6	Metropolitan Area Networks (MAN)
802.7	Broadband Technical Advisory Group
802.8	Fiber-Optic Technical Advisory Group
802.9	Integrated Voice/Data Networks
802.10	Network Security
802.11	Wireless Networks
802.12	Demand Priority Access LAN, 100BaseVG-AnyLAN
802.13	Unused
802.14	Cable Modem Standards
802.15	Wireless Personal Area Networks (WPAN)
802.16	Broadband Wireless Standards

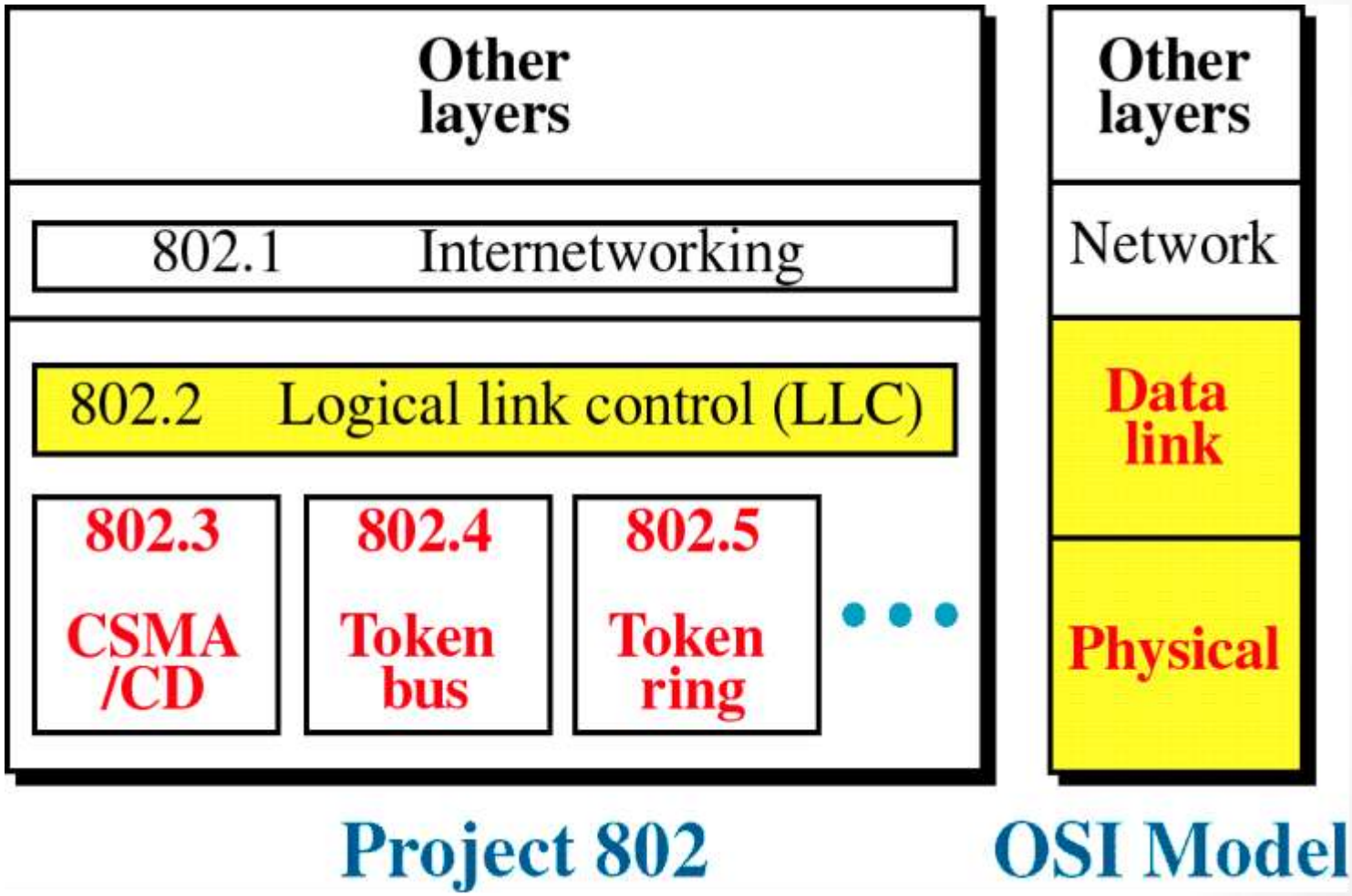
Project 802

- Project 802 has split the data link layer into two different sub layers:
  - Logical link control (LLC)
  - Media access control (MAC)
- It covers the first two layers of the OSI model and part of the third model.

OSI Model and Project 802



Project 802



IEEE 802.1

- IEEE 802.1 is an internetworking standards for LAN.
- It seeks to resolve the incompatibilities between network architecture without requiring modifications in existing addressing, access & error recovery mechanism.

LLC (Logical Link Control)

- It is the upper sublayer of the data link layer.
- It handles the logical addresses, control information and data.

MAC (Media Access Control)

- It is the lower sublayer of the data link layer.
- This layer handles or resolves certain controversies or contention for the shared media.
- This layer also handles the flow control and error control method.

PDU (Protocol Data Unit)

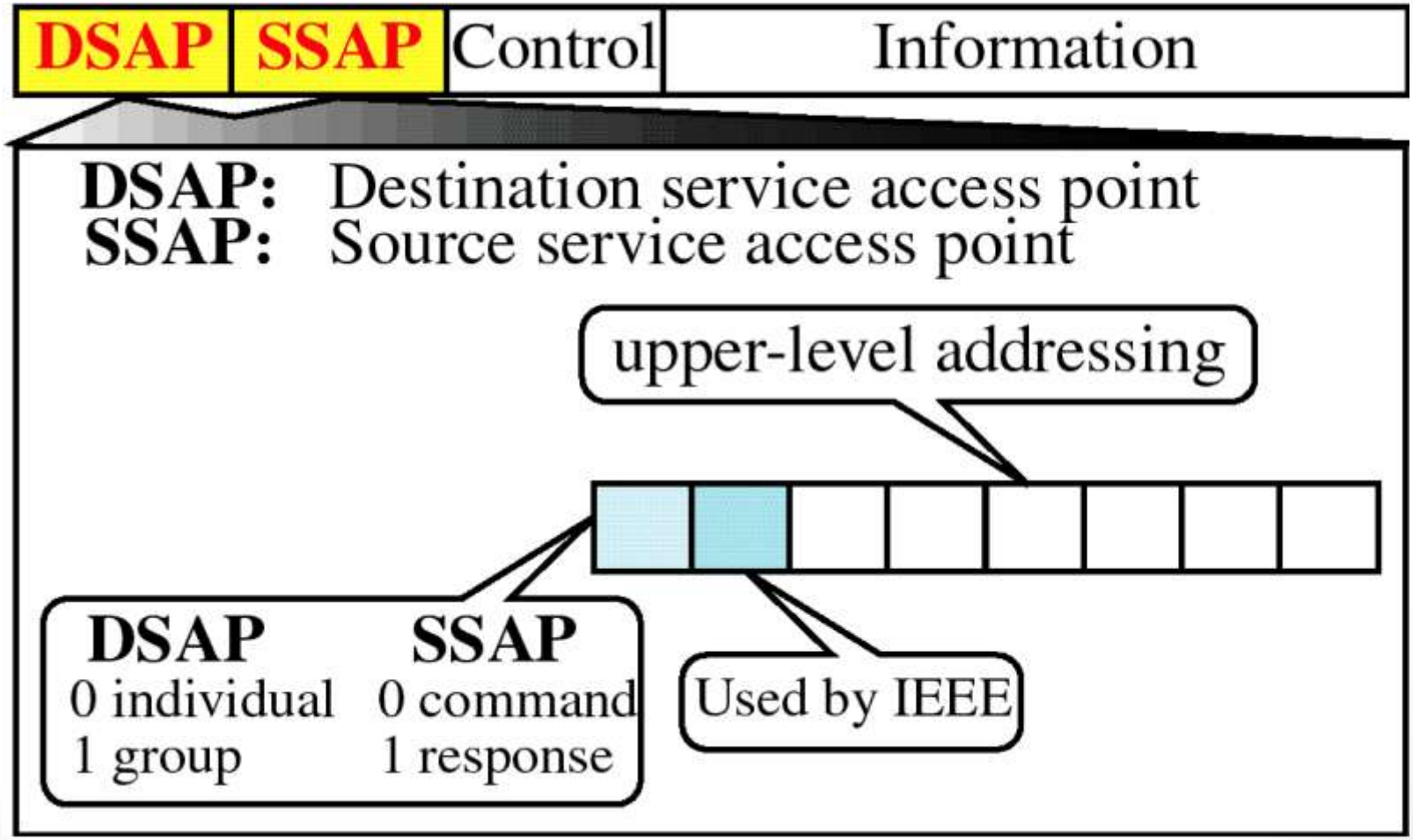
- The data unit in the LLC is called the Protocol Data Unit.

- The PDU has 4 fields:
  - DSAP(Destination Service Access Point)
  - SSAP (Source Service Access Point)
  - Control Field
  - An Information Field

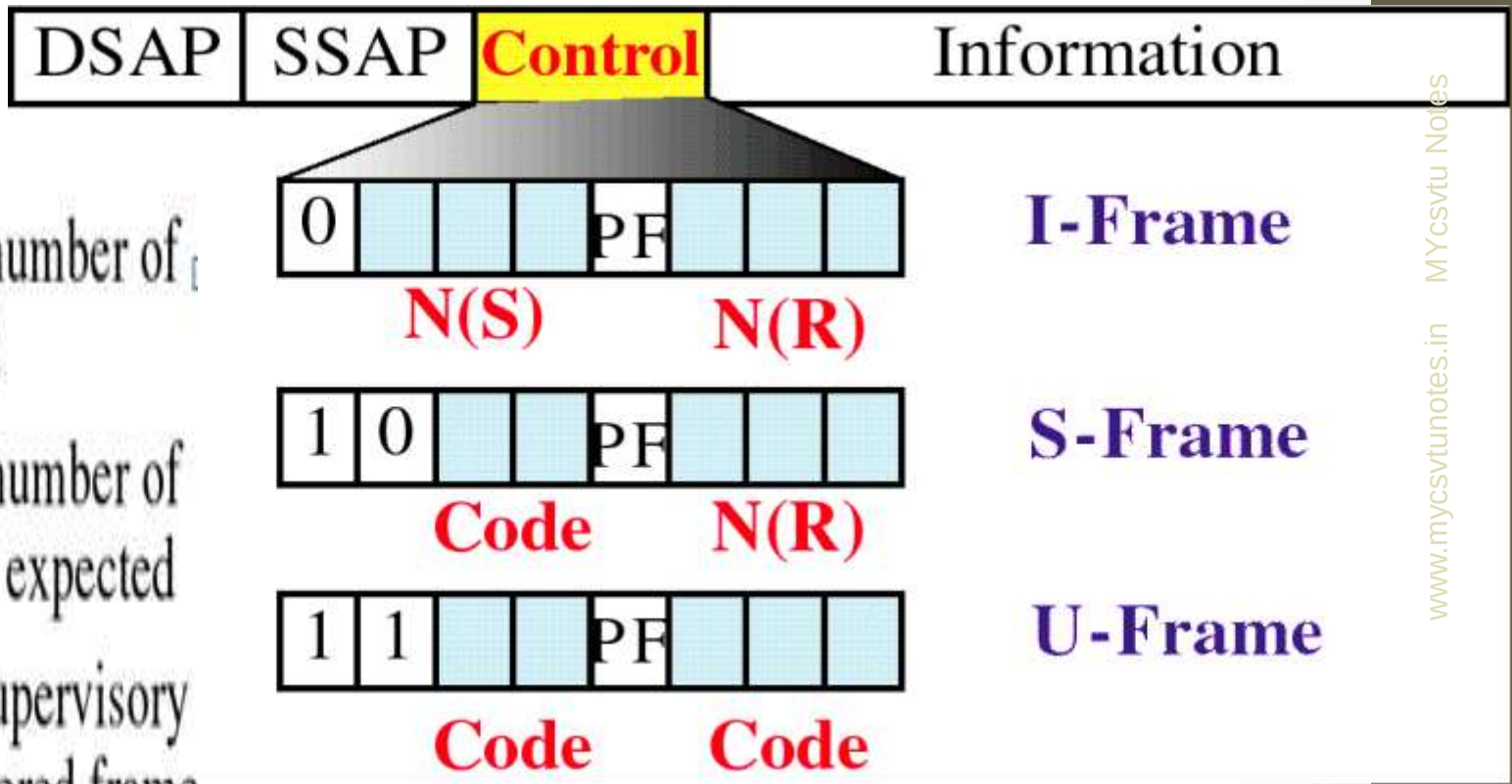
DSAP & SSAP

- The DSAP & SSAP are the addresses used by the LLC to identify the protocol stacks on the receiving and sending machines that are generating and using the data.
- The first bit of DSAP indicates whether the frame is intended for an individual or for a group.
- Similarly, the first bit of SSAP indicates whether the communications command or response.

PDU format



Control field in a PDU



N(S) Sequence number of frame sent

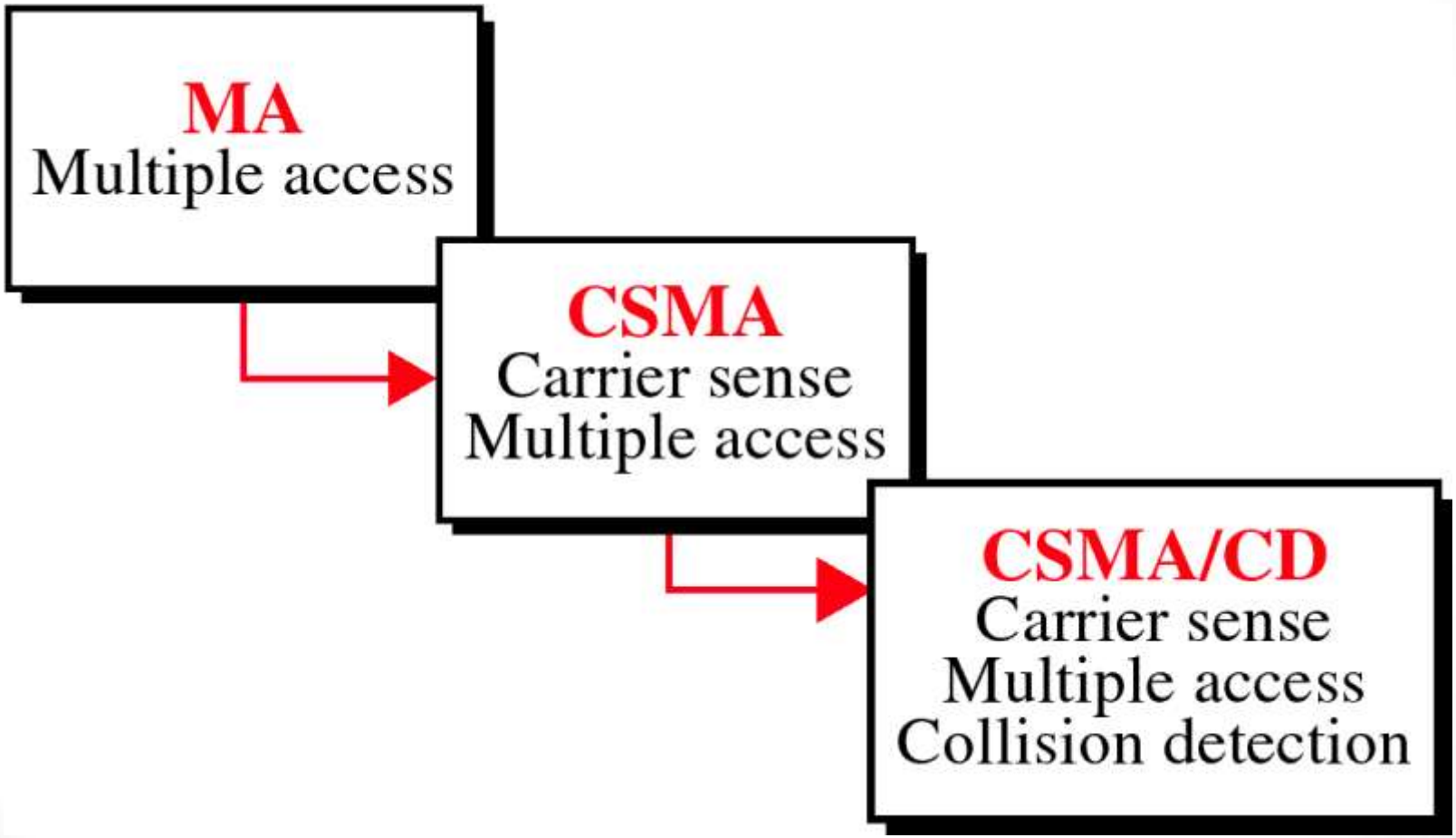
N(R) Sequence number of next frame expected

Code Code for supervisory or unnumbered frame

802.3 CSMA/CD

- The IEEE 802.3 standard is for CSMA/CD LAN.
- This system was called Ethernet after the aluminiferous ether, through which electromagnetic radiation was once thought to propagate.

Access method: (CSMA/CD)



Addressing

- Each station on an Ethernet network has its own Network interface card (NIC).
- The NIC usually fits inside the station and provides the station with a six byte physical address.
- The number on the NIC is unique.

MAC address

- The MAC address is a unique value associated with a network adapter.
- MAC addresses are also known as **hardware** addresses or **physical** addresses.
- They uniquely identify an adapter on a LAN.
- MAC addresses are 6 byte long (48 bits in length).
- By convention, MAC addresses are usually written in one of the following two formats:
  - MM:MM:MM:SS:SS:SS

MM-MM-MM-SS-SS-SS

Continued……..

- The first half of a MAC address contains the ID number of the adapter manufacturer.
- The second half of a MAC address represents the serial number assigned to the adapter by the manufacturer.
- In the example, 00:A0:C9:14:C8:29
- The prefix 00A0C9 indicates the manufacturer is Intel Corporation.

MAC vs. IP Addressing

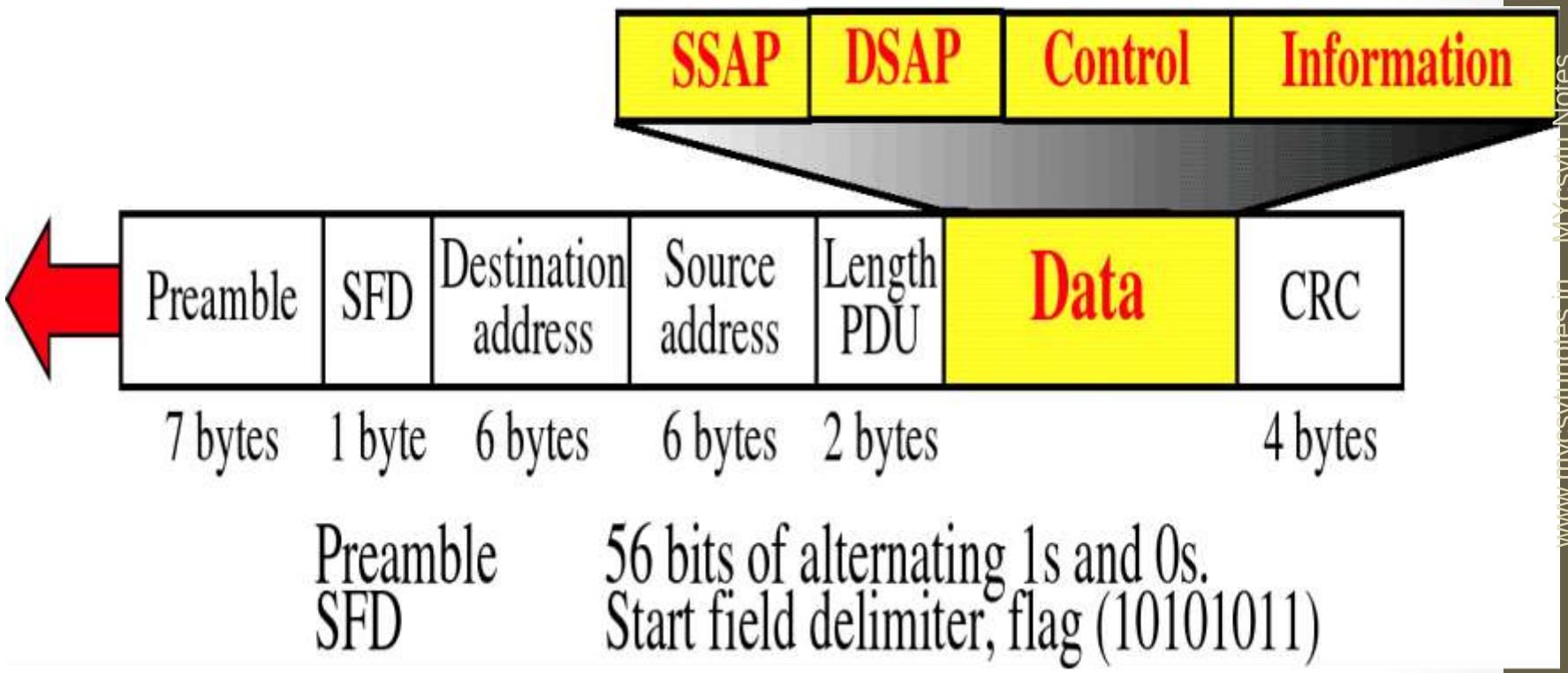
- Whereas MAC addressing works at the data link layer, IP addressing functions at the network layer (layer 3).
- It's a slight oversimplification, but one can think of IP addressing as supporting the software implementation and MAC addresses as supporting the hardware implementation of the network stack.
- The MAC address generally remains fixed and follows the network device, but the IP address changes as the network device moves from one network to another.

Ethernet system

The Ethernet system consists of three basic elements:

1. the physical medium used to carry Ethernet signals between computers,
2. a set of medium access control rules embedded in each Ethernet interface,
3. and an Ethernet frame that consists of a standardized set of bits used to carry data over the system.

Frame Format



Preamble

- It is used to alert the receiving system to the coming frame and enable it to synchronize its input timing.

SFD

- It tells the receiver that every thing that follows is data, starting with address.
- One byte: 10101011

Destination address

- Allotted 6 bytes
- Contains the physical address of the destination
- Physical address is a bit pattern encoded on its NIC

Source address

- Allotted 6 bytes
- It contains the physical address of the last device to forward the packet.
- Device can be the sending station or the most recent router to receive and forward the packet.

Length PDU

- Two bytes
- It indicates the number of bytes in the coming PDU.

Data (PDU)

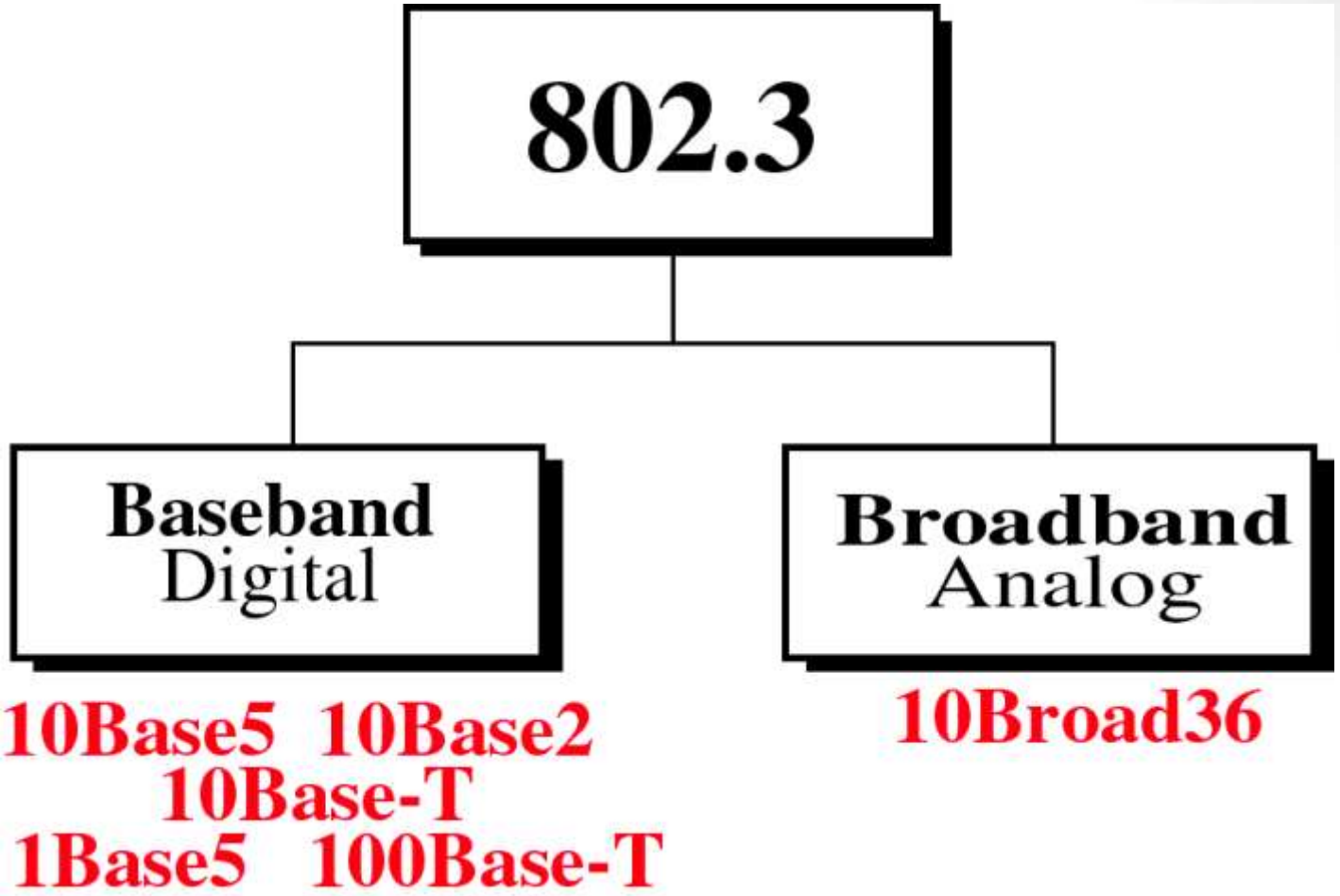
- Data up to 1500 bytes.

CRC

- Allotted 4 bytes
- It contains the error detection information.

Data rate

- Ethernet LANs can support data rates between 1 and 100 Mbps.

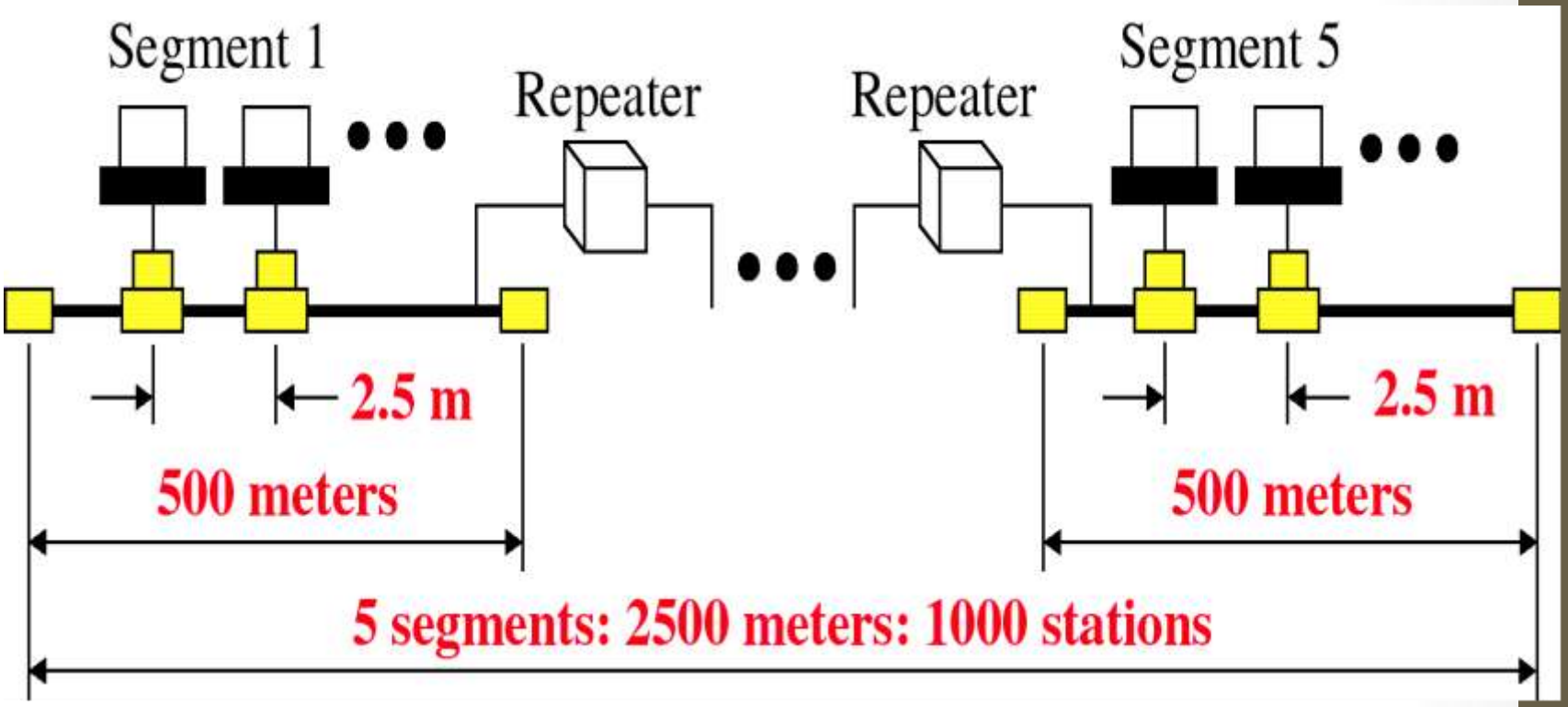


The word base specifies a digital signal.
The word broad specifies an analog signal.

Implementations of 802.3 Standard

- In this standard IEEE defines the type of cable, connections and signals that are to be used in each of 5 different Ethernet implementations.
  - 10BASE5
  - 10BASE2
  - 10BASET
  - 1BASE5

Ethernet Segments

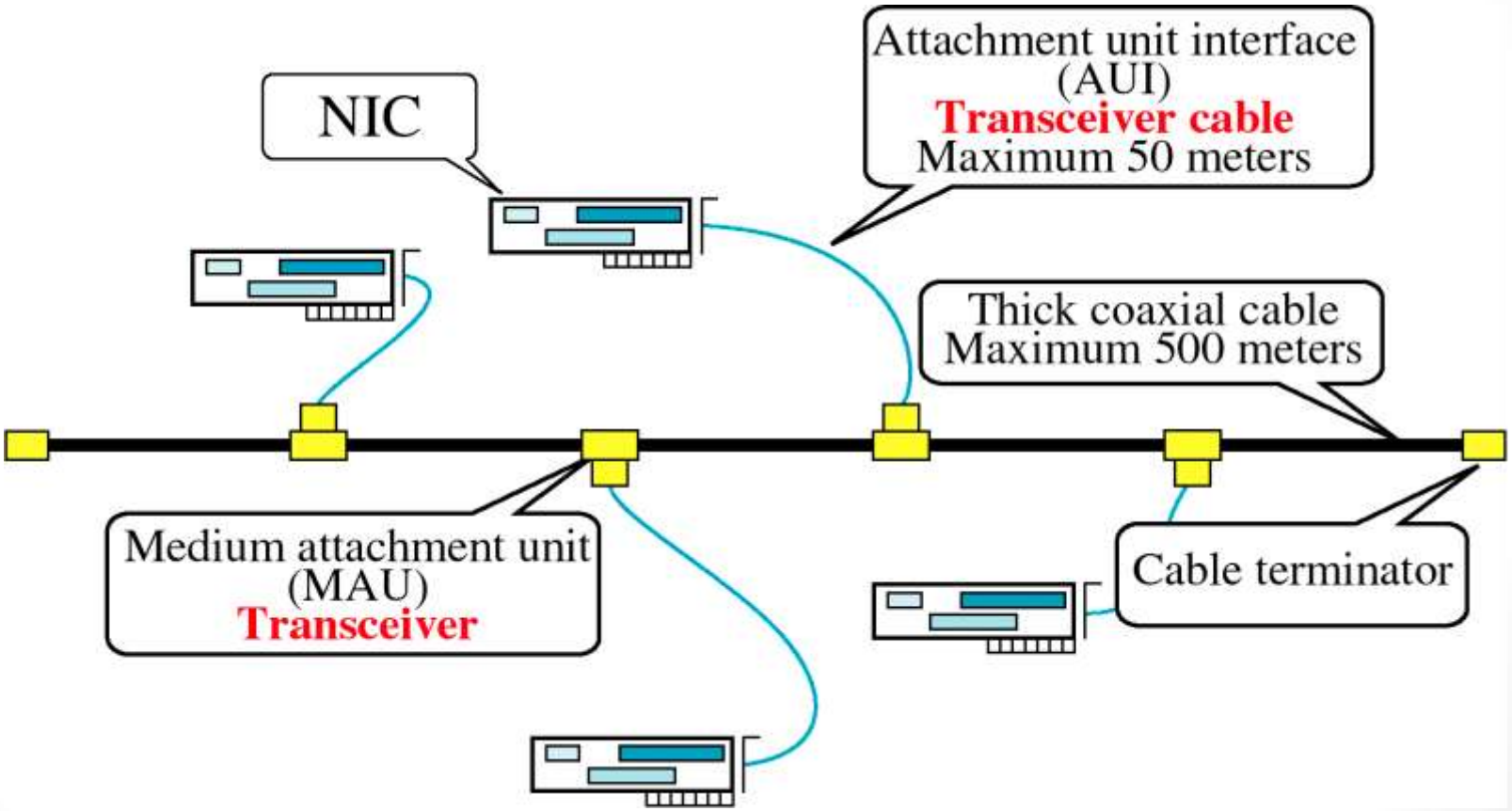


10BASE5 (Thick Ethernet / Thicknet)

Physical connectors and cables

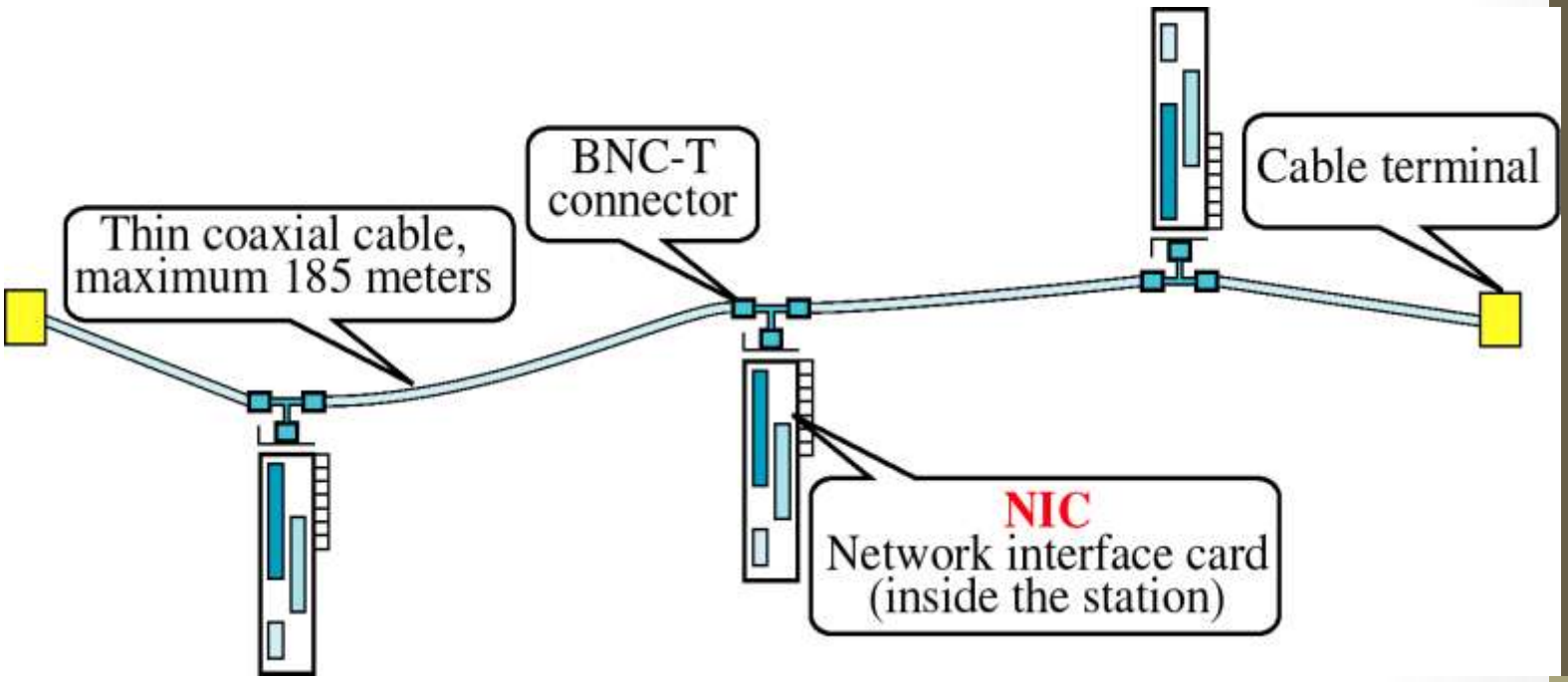
- RG-8 (Coaxial) cables
- NIC
- transceivers (short for transmitter/ receiver)
- Attachment unit interface (AUI)

Topology of 10BASE5



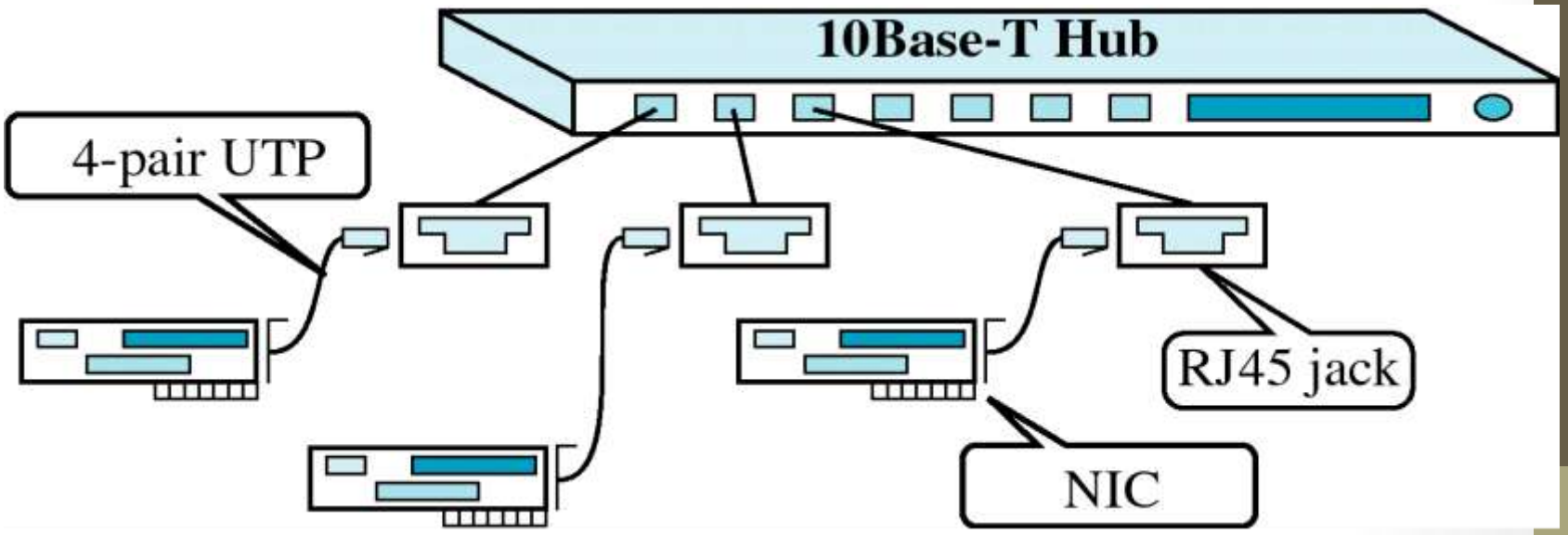
10BASE2 (Thinnet)

Topology of 10BASE2



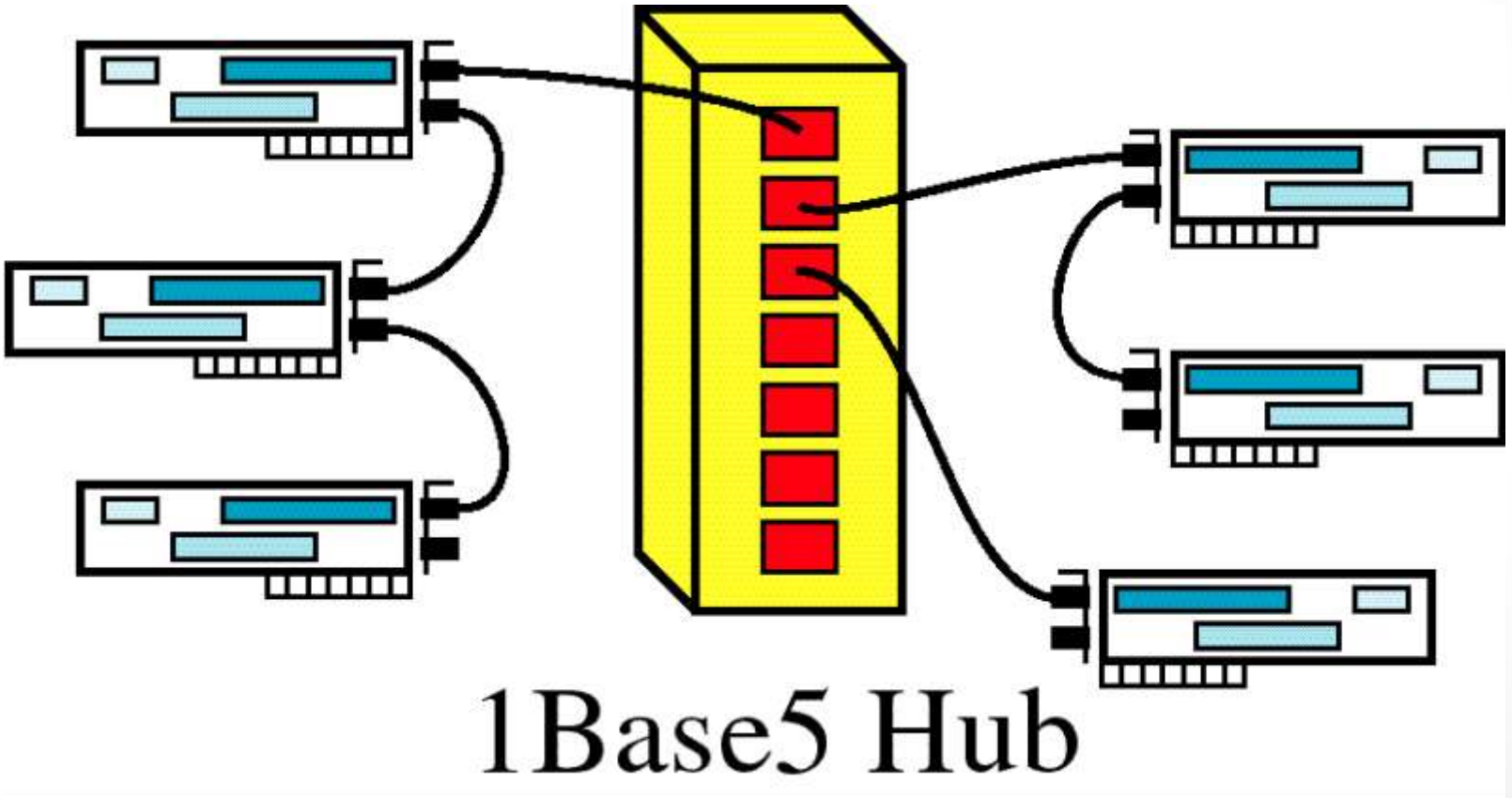
10BASET

Topology of 10BASE-T



1 Base5

Topology of 1BASE5



Disadvantage of 802.3

- In this a station might have to wait arbitrarily long to send a frame.
- Frames do not have priorities, making them unsuited for real-time systems in which important frames should not be held up waiting for unimportant frames.

Other Ethernet Networks

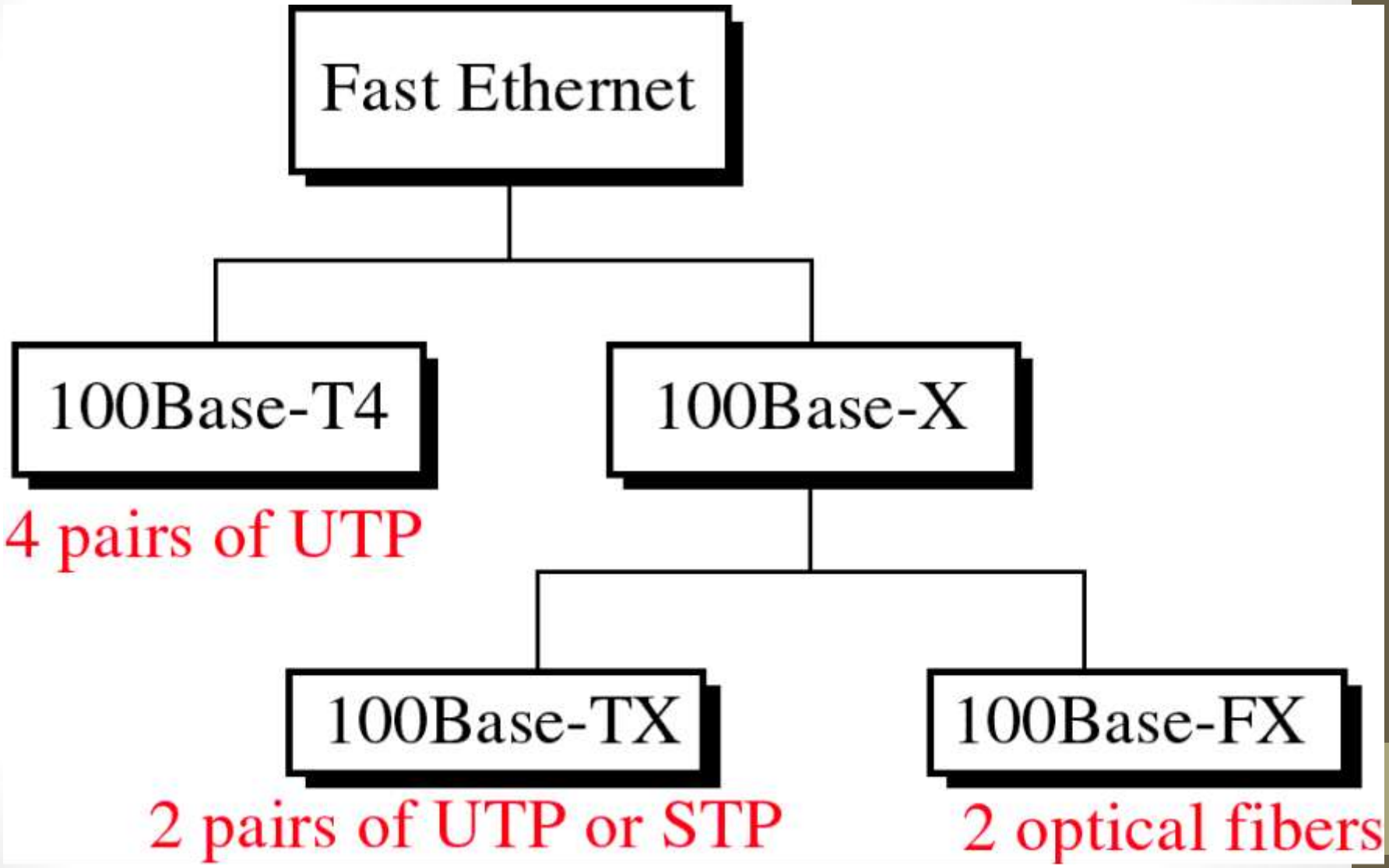
- Switched Ethernet
- Fast Ethernet
- Gigabit Ethernet

Switched Ethernet

- Switched Ethernet is an attempt to improve the performance of 10Base-T Ethernet.
- Switched Ethernet uses switch instead of hub.

Fast Ethernet

- Fast Ethernet is a version of Ethernet with a 100 Mbps data rate.



Gigabit Ethernet

- Gigabit Ethernet is a version of Ethernet with a 1000 Mbps data rate.

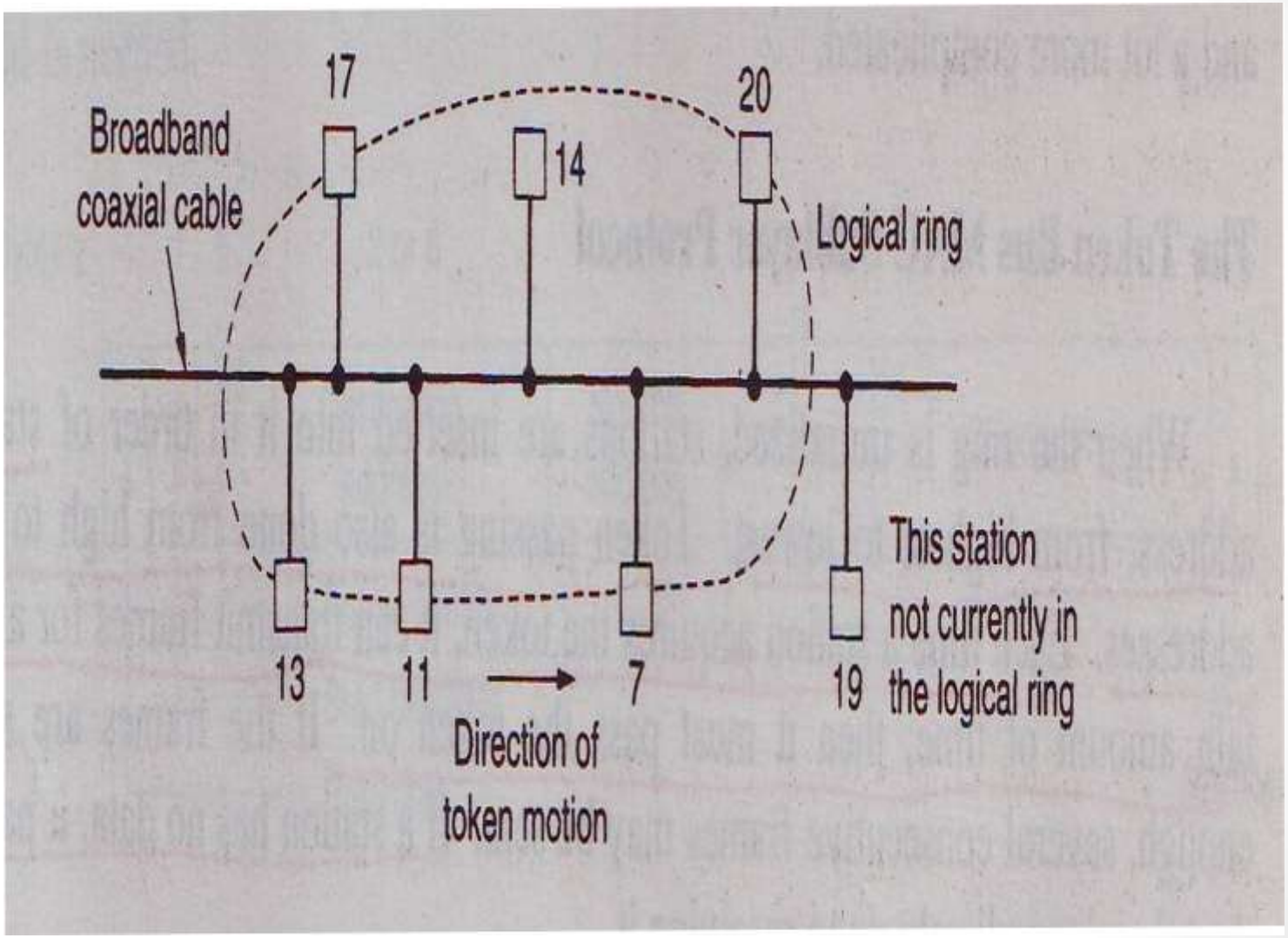
Assignment-2

- Write short notes on
  - Switched Ethernet
  - Fast Ethernet
  - Gigabit Ethernet
- Compare the data transmission rates for switched Ethernet, fast Ethernet and gigabit Ethernet.

Token Bus: IEEE 802.4

- The IEEE 802.4 standard for media access control is known as Token Bus.
- Physically, the token bus is a linear cable onto, which the stations are attached.
- Logically, the stations are organized into a ring, with each station knowing the address of the station to its “left” and “right”.

A token bus



Token

- When the logical ring is initialized, the highest numbered station may send the first frame.
- After it is done, it passes permission to its immediate neighbor by sending the neighbor a special control frame called a token.

Operation of Token Bus

- At any time, the station which holds the token only can transmit its data frames on the bus.
- Every frame contains source and destination addresses.
- All the other stations are ready to receive these data frames.
- As soon as the transmission time of a station is over, it passes the token to the next station in the logical sequence.
- The transmission is then taken over by the next station.
- When the ring is initialized, stations are inserted into it in order of station address, from highest to lowest.

Ring initialization

- Consider an idle system with all stations powered off.
- When the first station comes on-line, it notices that there is no traffic for a certain period.
- Then it sends a CLAIM_TOKEN frame.
- Not hearing any competitors contending for the token, it creates a token and sets up a ring containing only itself.

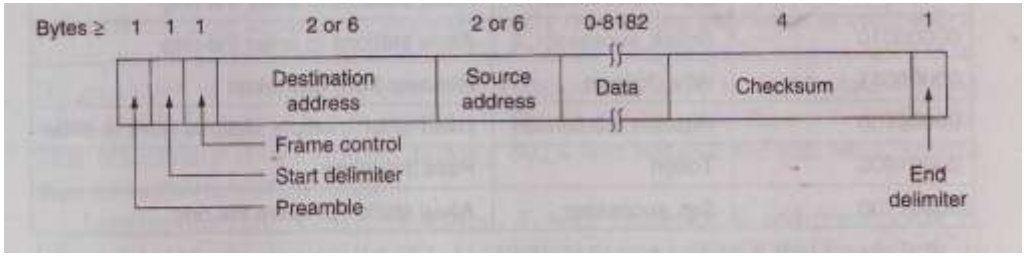
Logical Ring Maintenance

- From time to time, stations are powered on and want to join the ring. Others are turned off and want to leave.
- Once the ring has been established, each station's interface maintains the addresses of the predecessor and successor stations internally.
- Periodically, the token holder sends one of the SOLICIT_SUCCESSOR frames to solicit bids from stations that wish to join the ring.
- If no station bids to enter within a slot time, the response window is closed and the token holder continues with its normal business.
- If exactly one station bids to enter, it is inserted into the ring.
- If two or more stations bid to enter, their frames will collide and be garbled.

Leaving the ring

- It is easy.
- A station, X, with successor S, and predecessor P, leaves the ring, by sending P a SET_SUCESSOR frame telling it that henceforth its successor is S instead of X. Then X just stop transmitting.

The 802.4 frame format



Frame format

- **Preamble:** it is used to synchronize the receiver's clock. (1 byte)
- **Start Delimiter (SD):** it is a unique one byte pattern which marks the beginning of a frame.
- **Frame control (FD):** it is used to distinguish data frames from control frames.
- **Destination Address (DA):** it contains the destination address and it is 2-6 bytes long.

- **Source Address (SA):** it contains the source address and it is 2-6 bytes long.
- **Data:** it may be up to 8182 bytes long.
- **Checksum:** this field contains a CRC codes.
- **End delimiter(ED):** it marks the end of the frame.
- The total length of the frame from FC to checksum is 8192 bytes.

Physical specification

- Data rates at which a token passing operates can be 1, 5, 10 Mbps.

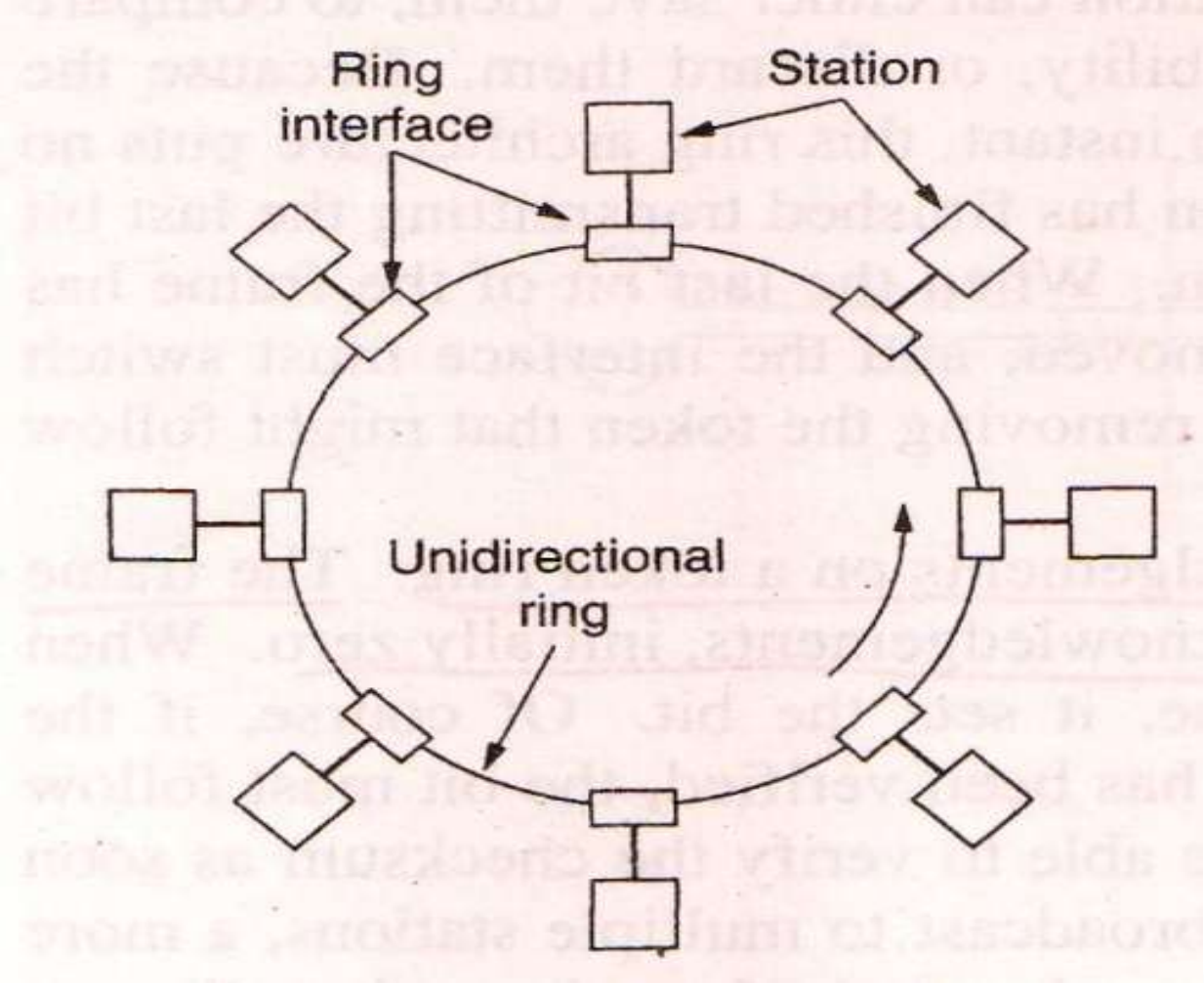
Limitations

- Any failure in the bus caused all the devices beyond the failure to be unable to communicate with the rest of the network.
- Second, adding more stations to the bus was somewhat difficult.

IEEE standard 802.5: Token Ring

- A token ring system consists of a number of stations connected to the ring through ring interface unit (RIU).
- Token Ring allows each station to send one frame per turn.
- A station may send data only when it has possession of the token.
- A token is simple placeholder frame that is passed from station to station around the ring.

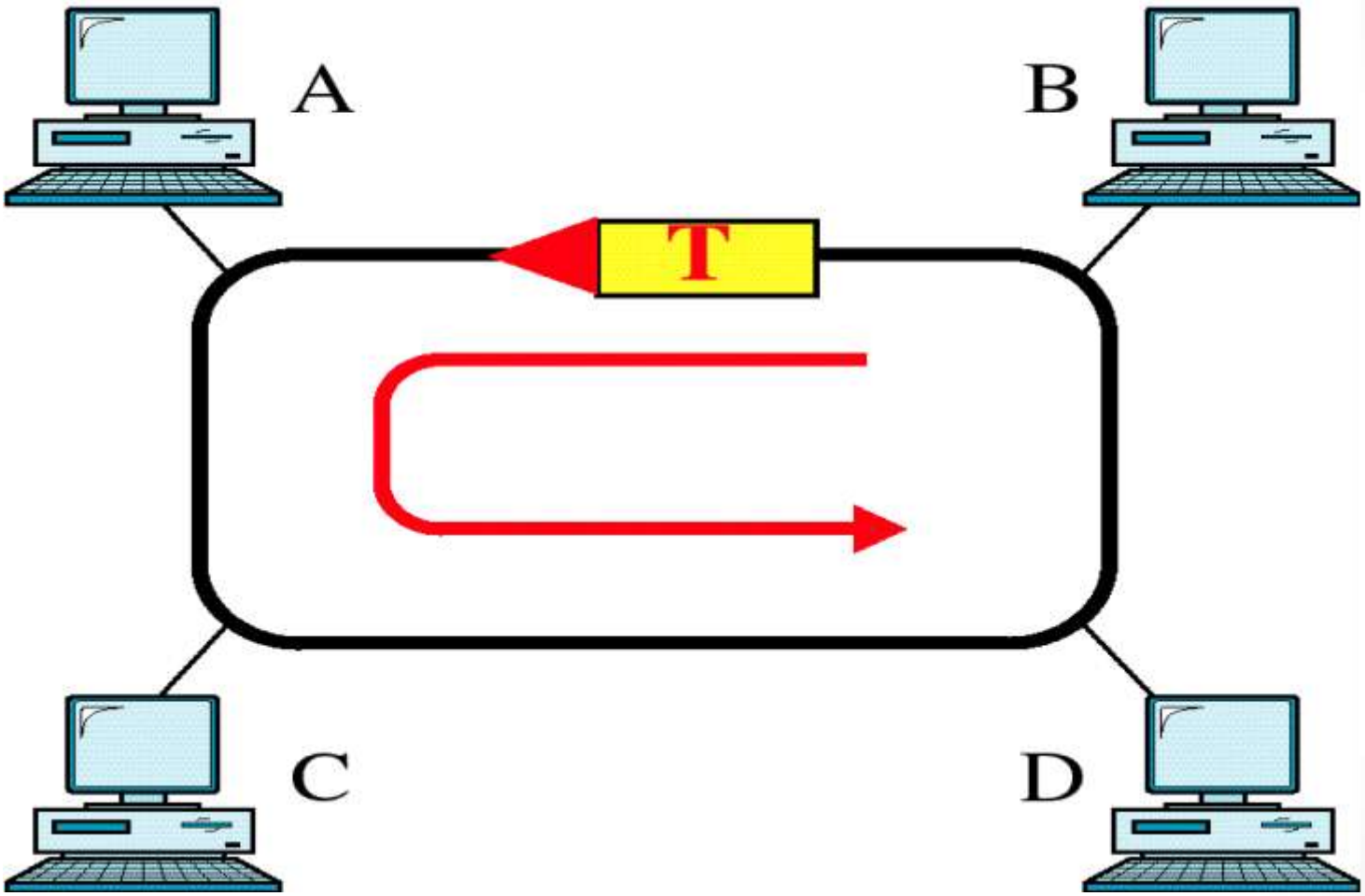
A ring network

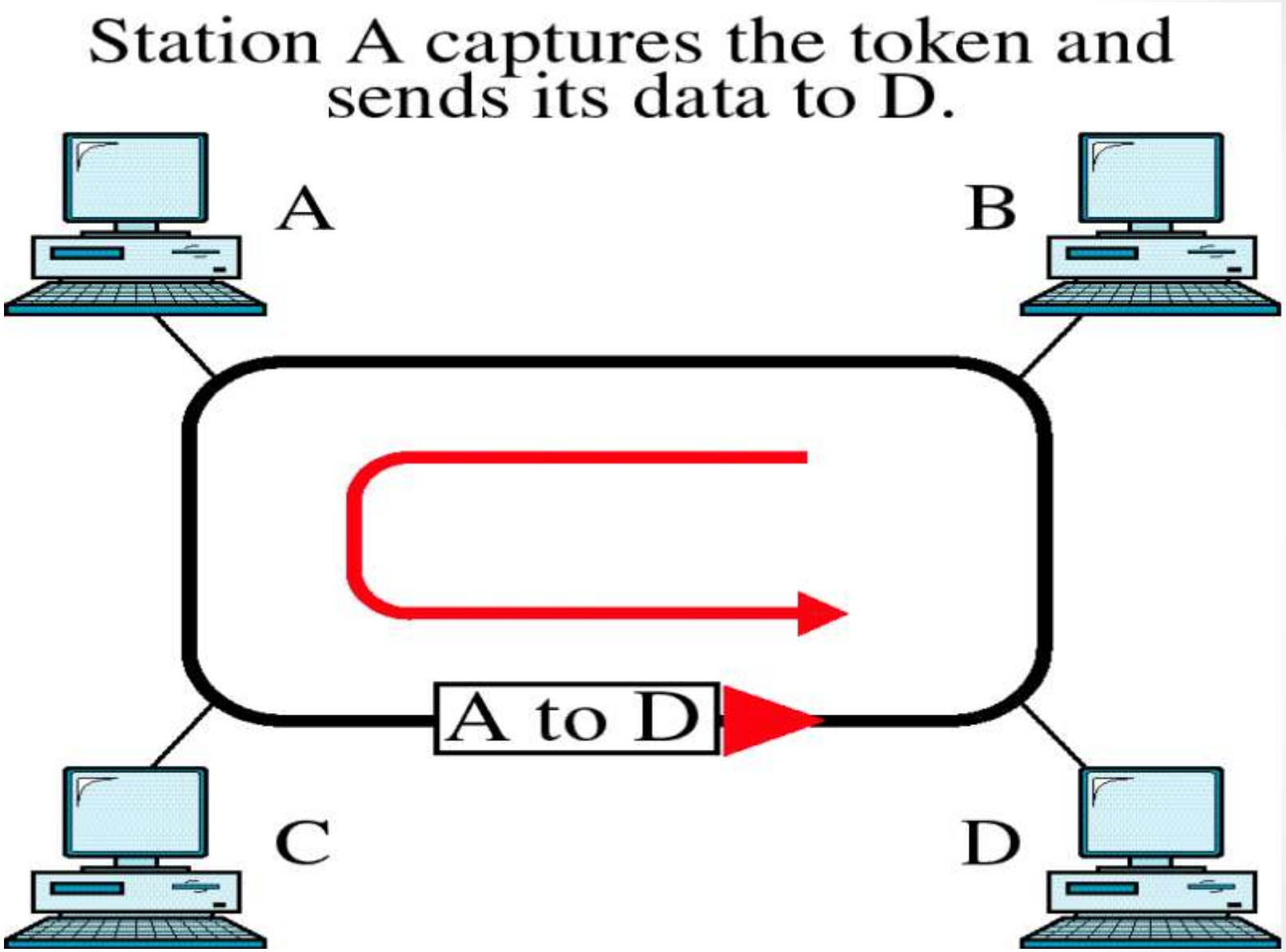


Token passing

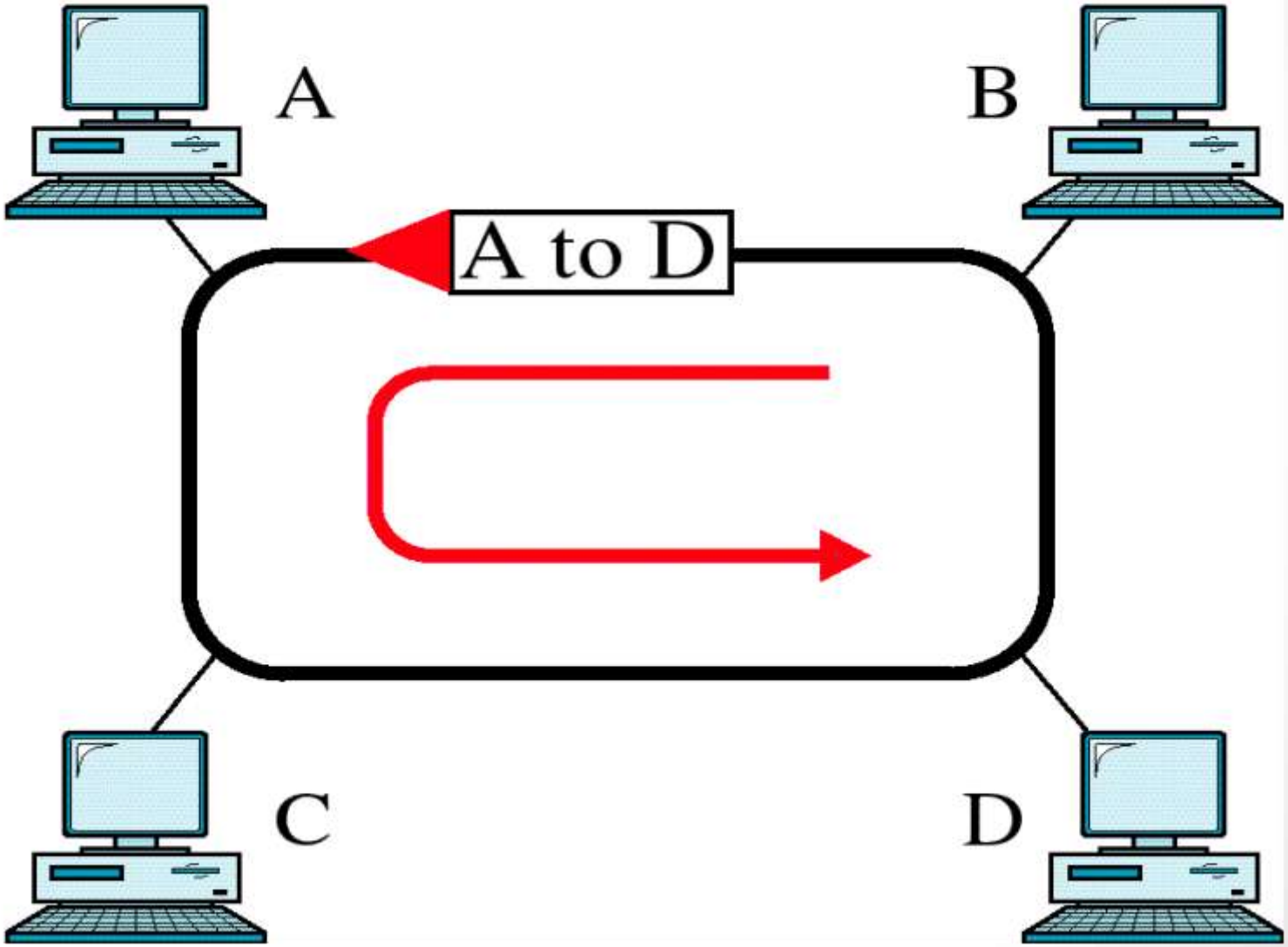
- Whenever the network is unoccupied, it circulates a simple three-byte token.
- The token is passed from station to station.
- If the token is free, the station may then send a data frame. The data frame proceeds around the ring, being regenerated by each station.
- Each station examines the destination address, finds that the frame is addressed to another station, and relays to its neighbor.
- The intended recipient recognizes its own address, copies the message, checks for errors, and changes four bits in the last byte of the frame to indicate address recognized and frame copied.
- The full packet then continues around the ring until it returns to the station that sent it. The sender receives it then discards the used data frame and release the token back to the ring.

Token is traveling along the ring.

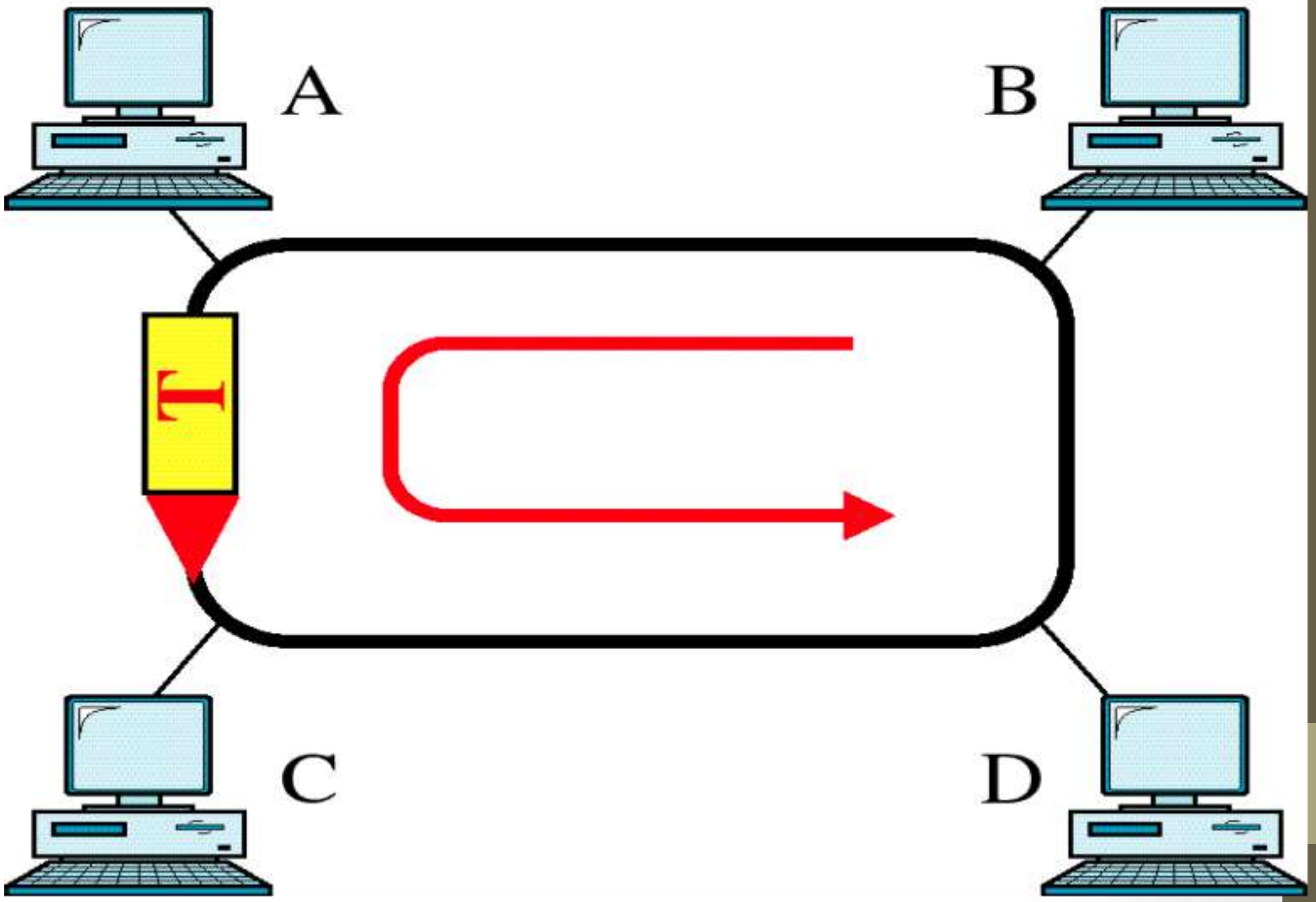




Station D copies the frame and sends the data back to the ring.



Station A receives the frame and releases the token.



Important Aspect Related to Token Ring are:

- Priority & Reservation
- Time Limits
- Monitor Station

Priority & Reservation

- Once a token has been released, the next station on the ring with data to send has the right to take charge of the ring.
- Another option is also possible.
- The busy token can be reserved by a station waiting to transmit.
- Each station has a priority code.
- As a frame passes by, a station waiting to transmit may reserve the next open token by entering its priority code in the access control field of the token or data frame.
- A station with a higher priority may remove a lower priority reservation and replace it with its own.
- Among stations of equal priority, the process is FCFS.

Time Limits

- To keep traffic moving, Token Ring imposes a time limit on any station wanting to use the ring.
- Each station expects to receive frames within regular time interval.

Monitor Station

1. Several problems may occur to disrupt the operation of a Token Ring network.

- A station may neglect to retransmit a token or a token may be destroyed by noise.
- A sending station may neglect to remove its used data frame from the ring or may not release the token once its turn has ended.

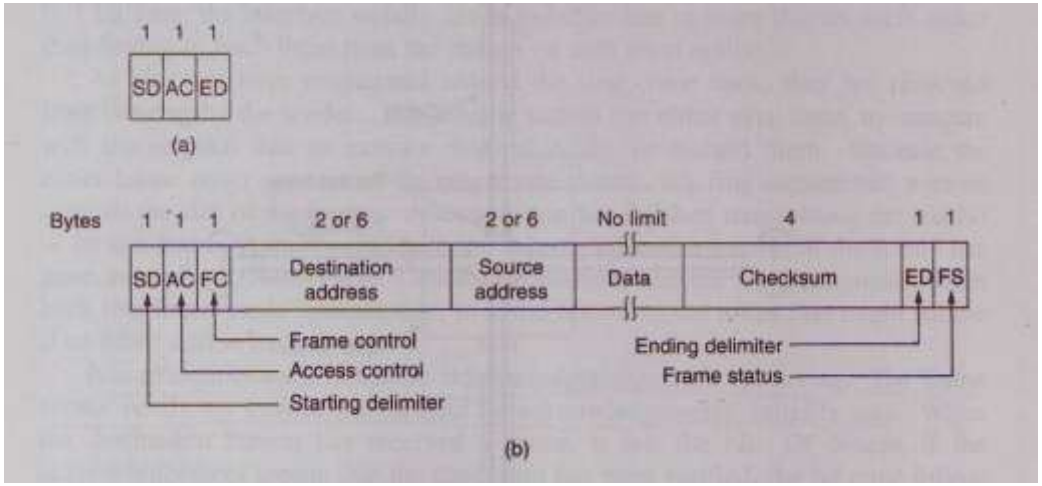
2. To handle these situations, one station on the ring is designated as a monitor station.

3. The monitor sets a timer each time the token passes.

4. If the token does not reappear in the allotted time, it is presumed to be lost and the monitor generates a new token and introduces it to the ring.

If the monitor fails, a second station, designated as back-up, takes over.

Token format



Token and data frame format

- Start Delimiter (SD):
- Access Control (AC):
- Frame Control (FC)
- Destination Address(DA)
- Source Address(SA)
- data
- Checksum
- End Delimiter (ED)
- Frame status (FS)

Start Delimiter (SD)

- It is used to alert the receiving station to the arrival of a frame as well as to allow it to synchronize its retrieval timing.

Access Control (AC)

It consists of the

- priority bits(P):
- Token bit(T): 0-token frame, 1- data frame
- Monitoring bits(M): Persistently circulating frames are detected by the monitoring bit(M).
- Reservation bits(R) :

Frame Control (FC)

Type	Special information

It consists of the
Type: (1 bit) type of information in the PDU(control or data)
Special information: (7 bits)

Frame status (FS)

A	C	X	X	A	C	X	X

It can be set by the receiver to indicate that the frame has been read, or by the monitor to indicate that the frame has already been around the ring.

It consists of the

- Two address recognized bits(A)
- Two frame copied bits(C)
- Reserved bits (X)

Physical specification

- Data rates vary between 1 and 16 Mbps.
- In practice a shielded twisted pair cable is used.

FDDI (Fiber-Distributed Data Interface)

- FDDI is a high performance fiber optic token ring LAN protocol running at 100 Mbps over distances up to 200 km with up to 1000 stations connected.

- FDDI was developed by the American National Standards Institute (ANSI) standards committee in the mid-1980s.

FDDI Transmission Media

- FDDI uses optical fiber as the primary transmission medium, but it also can run over copper cabling.
- Optical fiber has several advantages over copper media.
- In particular,
  - security,
  - reliability, and
  - higher bandwidth (throughput potential) than copper,

FDDI defines two types of optical fiber:

- A mode is a ray of light that enters the fiber at a particular angle.
- **Single-mode:** Single-mode fiber allows only one mode of light to propagate through the fiber.
- **Multi-mode:** Multi-mode fiber allows multiple modes of light to propagate through the fiber.
- Multi-mode fiber uses LED as the light-generating devices, while single-mode fiber generally uses lasers.

Types of data frame

- **Synchronous (S-frames):** Synchronous here refers to information that is real time. When a node receives a token, it is allowed to send synchronous data first.

- **Asynchronous (A-frames):** Asynchronous here refers to information that is not real time. Any remaining time may then be used to send A-frames.

Time registers

- FDDI defines three time registers to control circulation of the token
  - **Synchronous allocation(SA):** length of time allowed each station for sending data.
  - **Target Token Rotation Time (TTRT):** average time required for a token to circulate around the ring exactly once.
  - **Absolute Maximum Time (AMT):**it holds value equal to twice the TTRT.

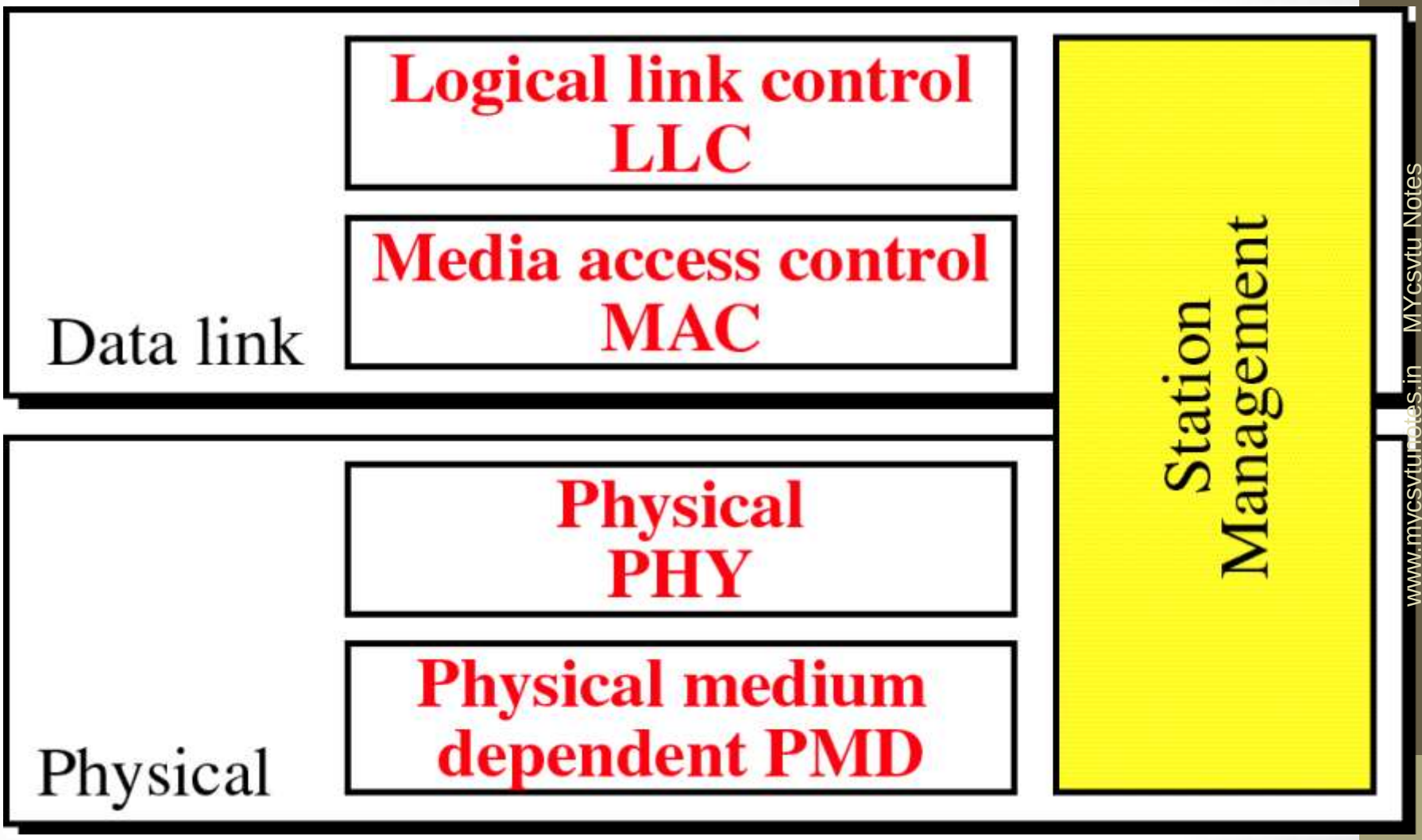
Timers

- Timers used by FDDI
  - **Token rotation timer (TRT)**: measure the actual time taken by the token to complete a cycle.
  - **Token holding timer (THT)**:the THT begins running as soon as the token is received.

Addressing

- FDDI uses a six-byte address, which is imprinted on the NIC card.

FDDI Layers



FDDI's layers

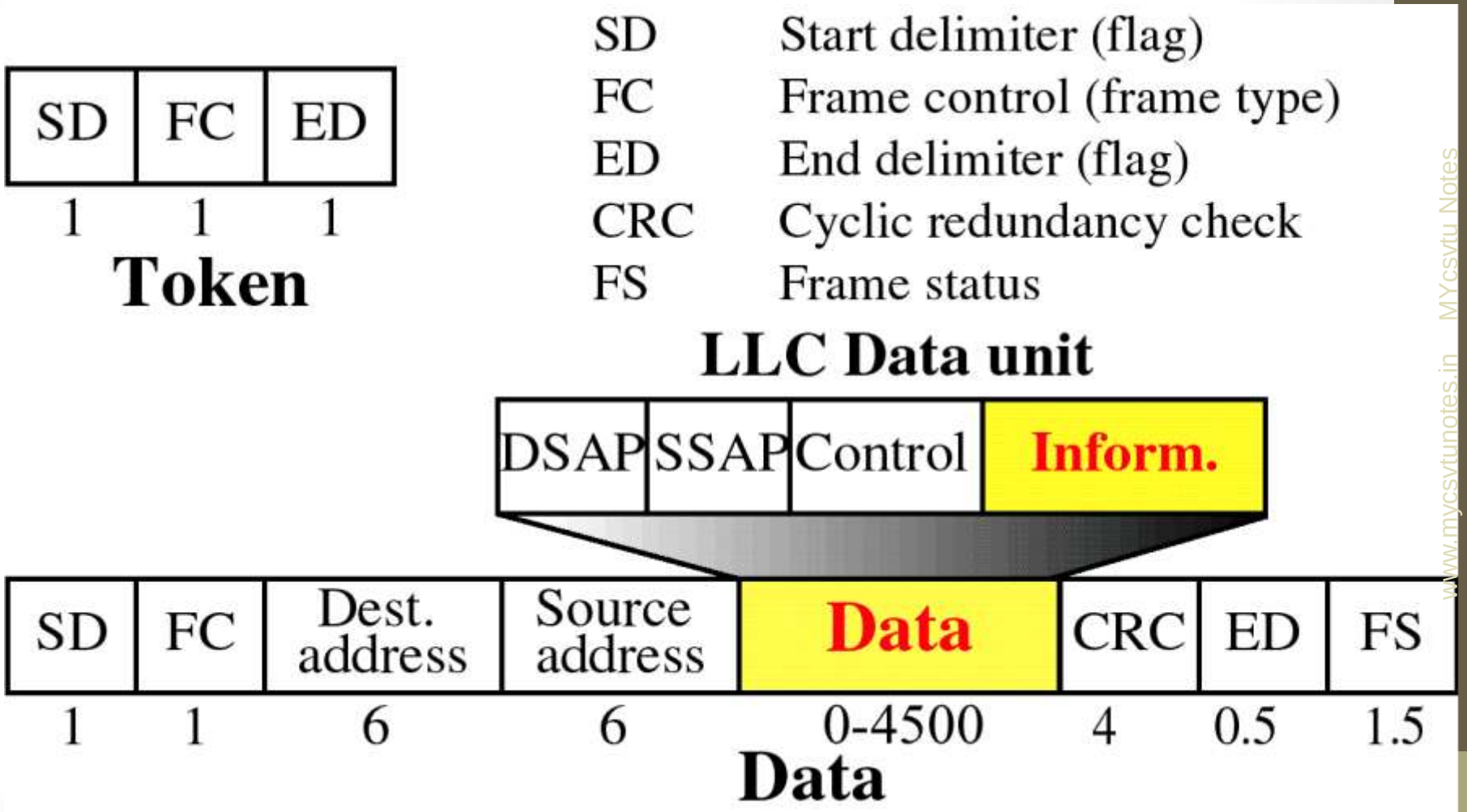
FDDI's four specifications are the

- Media Access Control (MAC),
- Physical Layer Protocol (PHY),
- Physical-Medium Dependent (PMD),
- Station Management (SMT).

FDDI's layers

- **MAC**- it defines frame format, token handling, addressing, error-recovery mechanisms.
- **PHY**- it defines data encoding/decoding procedures, clocking requirements.
- **PMD**- it defines characteristics of the transmission medium.
- **SMT-** it defines FDDI station configuration, ring configuration, and ring control features.

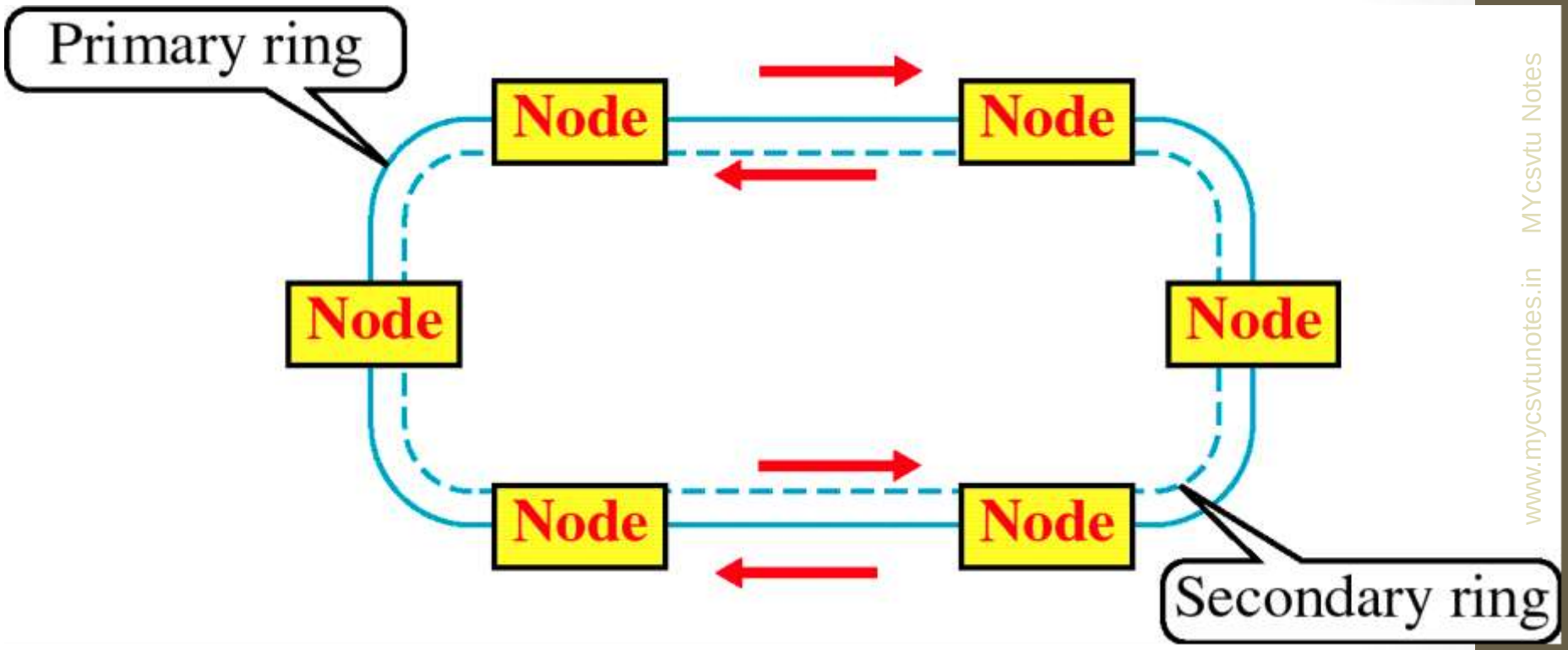
FDDI Frames



- **Start Delimiter**—Indicates the beginning of a frame by employing a signaling pattern that differentiates it from the rest of the frame.
- **Frame Control**—Indicates the size of the address fields and whether the frame contains asynchronous or synchronous data, among other control information.
- **Destination Address**—Contains a unicast (singular), multicast (group), or broadcast (every station) address. As with Ethernet and Token Ring addresses, FDDI destination addresses are 6 bytes long.
- **Source Address**—Identifies the single station that sent the frame. As with Ethernet and Token Ring addresses, FDDI source addresses are 6 bytes long.

- **Data**—Contains either information destined for an upper-layer protocol or control information.
- **Frame Check Sequence (FCS)—**Filed by the source station with a calculated cyclic redundancy check value dependent on frame contents (as with Token Ring and Ethernet). The destination address recalculates the value to determine whether the frame was damaged in transit. If so, the frame is discarded.
- **End Delimiter**—Contains unique symbols, which cannot be data symbols, that indicate the end of the frame.
- **Frame Status (FS). Contains the error detected (E), address recognized (A),**and frame copied (F) indicators.

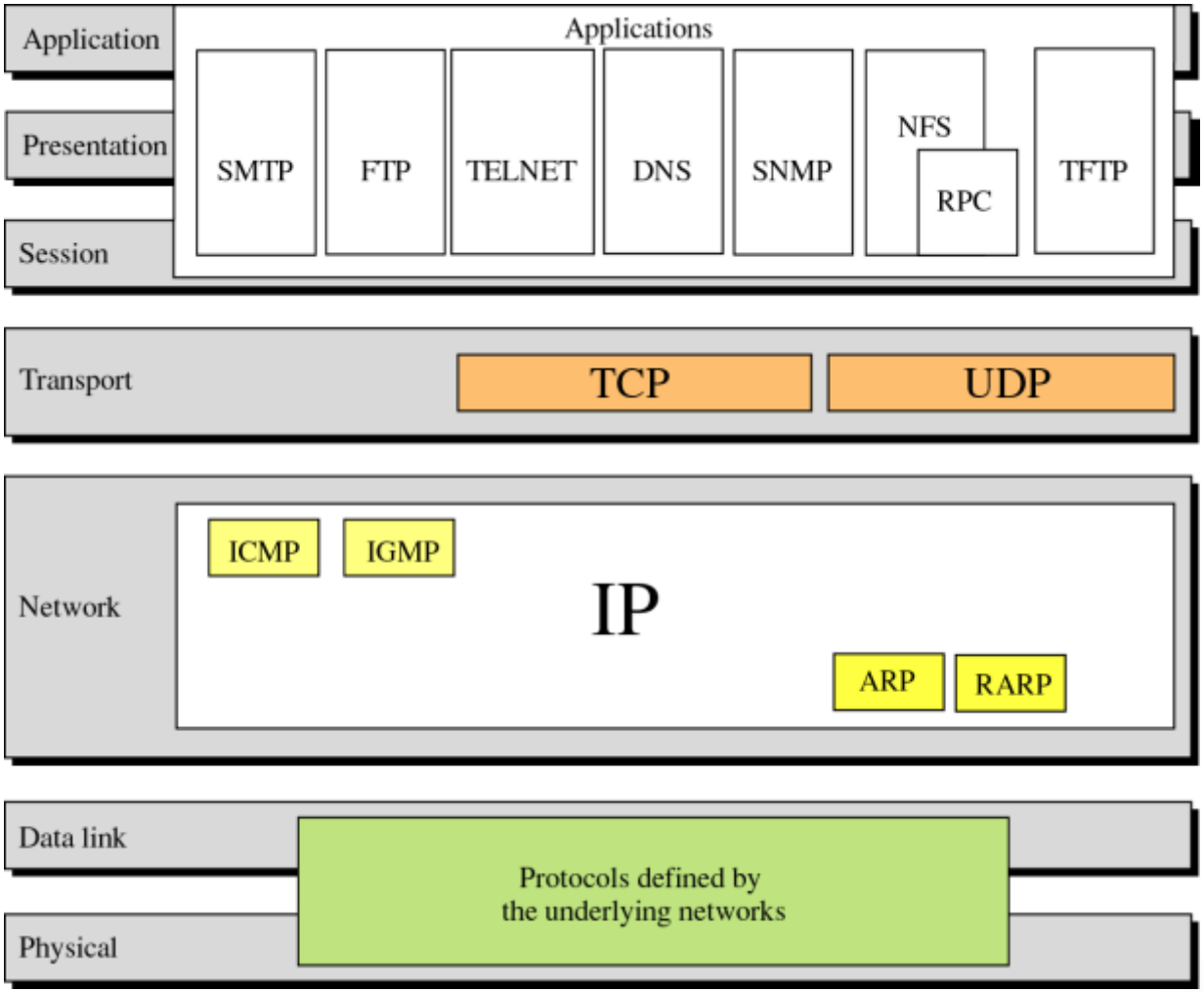
FDDI Rings



- An FDDI network contains two token rings, one for possible backup in case the primary ring fails.
- If both breaks at the same point, due to a fire or other accident in cable duct, the two rings can be joined into a single ring.
- The primary ring offers up to 100 Mbps capacity.
- If the secondary ring is not needed for backup, it can also carry data, extending capacity to 200 Mbps
- Each ring flowing in opposite directions (called counter-rotating).
- During normal operation, the primary ring is used for data transmission, and the secondary ring remains idle.
- The primary purpose of the dual rings is to provide superior reliability and robustness.

Network Layer

TCP/IP protocol suite



Network Layer

- In the internet model, or the TCP/IP suite, there are five main network layer protocols:
  - ARP
  - RARP
  - IP
  - ICMP
  - IGMP

ARP(Address Resolution Protocol)

- A packet starts from the source host, passes through many physical networks and finally reaches the destination host.
- At the network level, the hosts and routers are recognized by their IP addresses.

IP address

- An IP address is an internetwork address. It is universally unique address.
- Every protocol involved in internetworking requires IP address.

MAC address

- The packets from source to destination hosts through physical networks. At the physical level the IP address is not useful but the hosts and routers are recognized by their MAC addresses.
- A MAC address is a local address. It is unique locally but is not unique universally.
- The IP and MAC address are two different identifiers and both of them are needed.
- Similarly a packet may pass through different physical networks.
- So to **deliver a packet to a host , we require two levels of addressing namely IP addressing and MAC addressing**.
- Most importantly **we should be able to map the IP address into a corresponding MAC address**.

Mapping of IP address into a MAC address

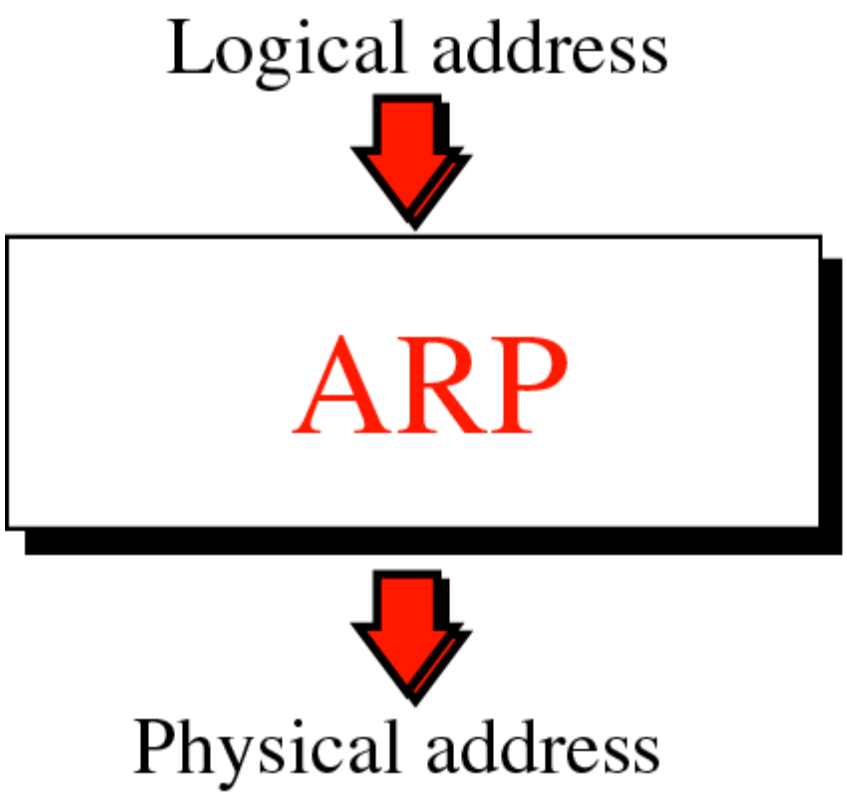
- Static mapping
- Dynamic mapping

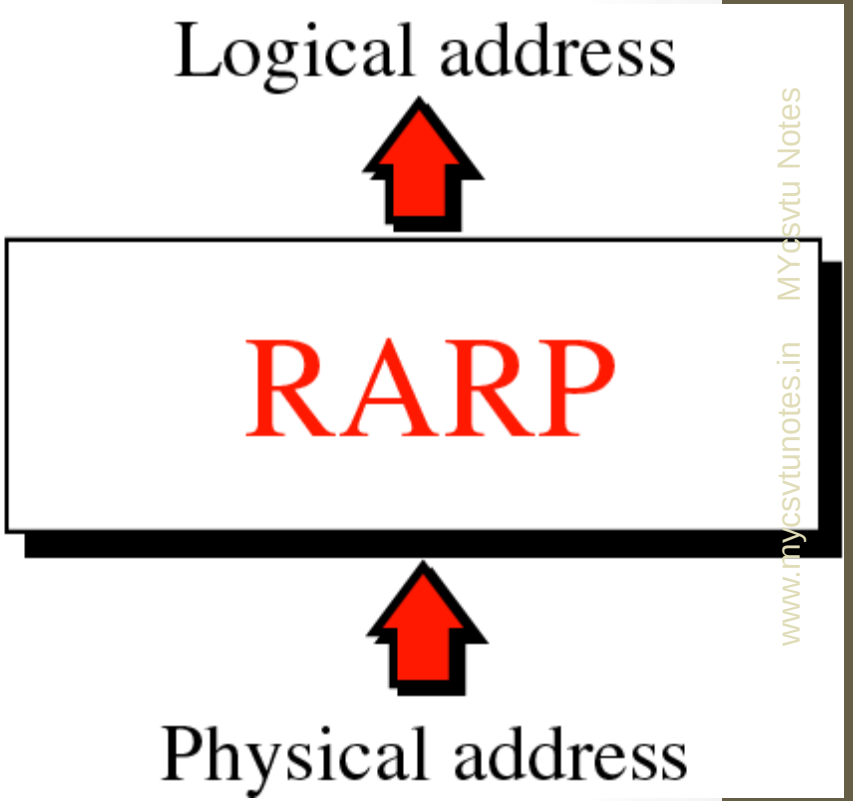
Static mapping

- In static mapping a table is created and stored in each machine.
- This table associates an IP address with a MAC address.
- If a machine knows the IP address of another machine then it can search for the corresponding MAC address in its table.
- The limitation of static mapping is that the MAC addresses can change.
- To implement static mapping, the static mapping table needs to be updated periodically.

Dynamic mapping

- In dynamic mapping technique a protocol is used for finding the other address when one type of address is known.
- There are two protocols designed to perform the dynamic mapping. They are
  - ARP
  - RARP
- The ARP maps an IP address to a MAC address whereas the RARP maps a MAC address to an IP address.





How to find the MAC address

The router or host A wants to find the MAC address of some other router

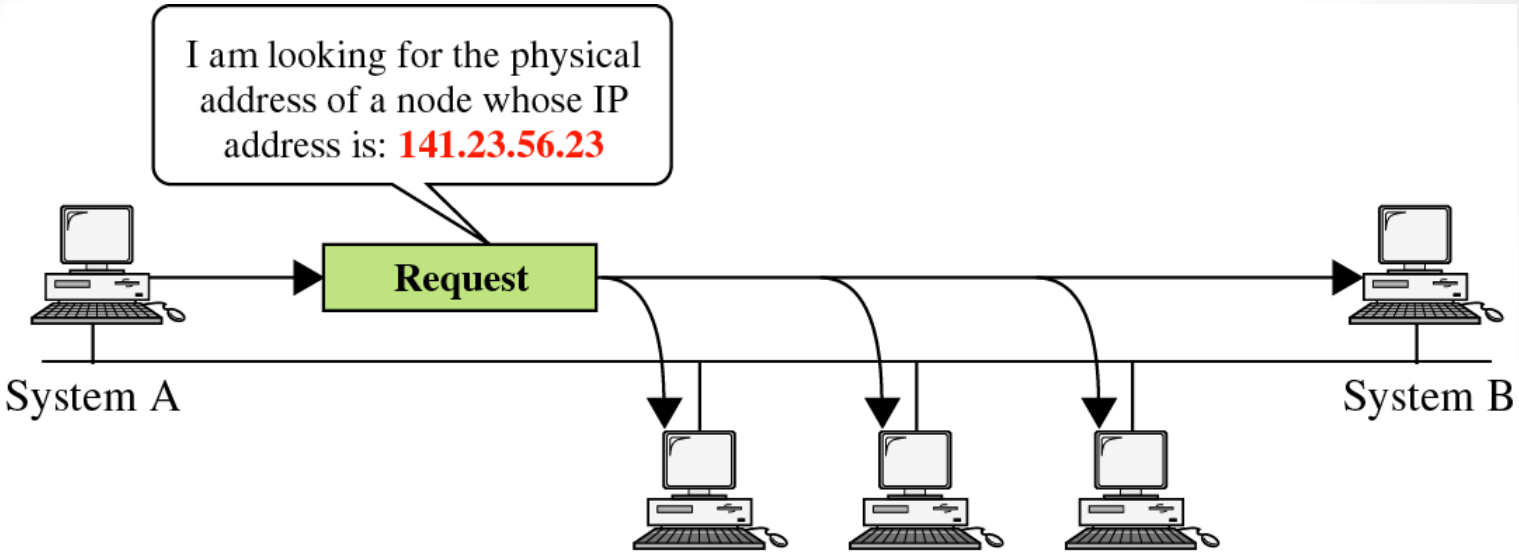
i. It sends an ARP request packet.

ii. This packet consists of IP and MAC addresses of the sender A and the IP address of the receiver(B).

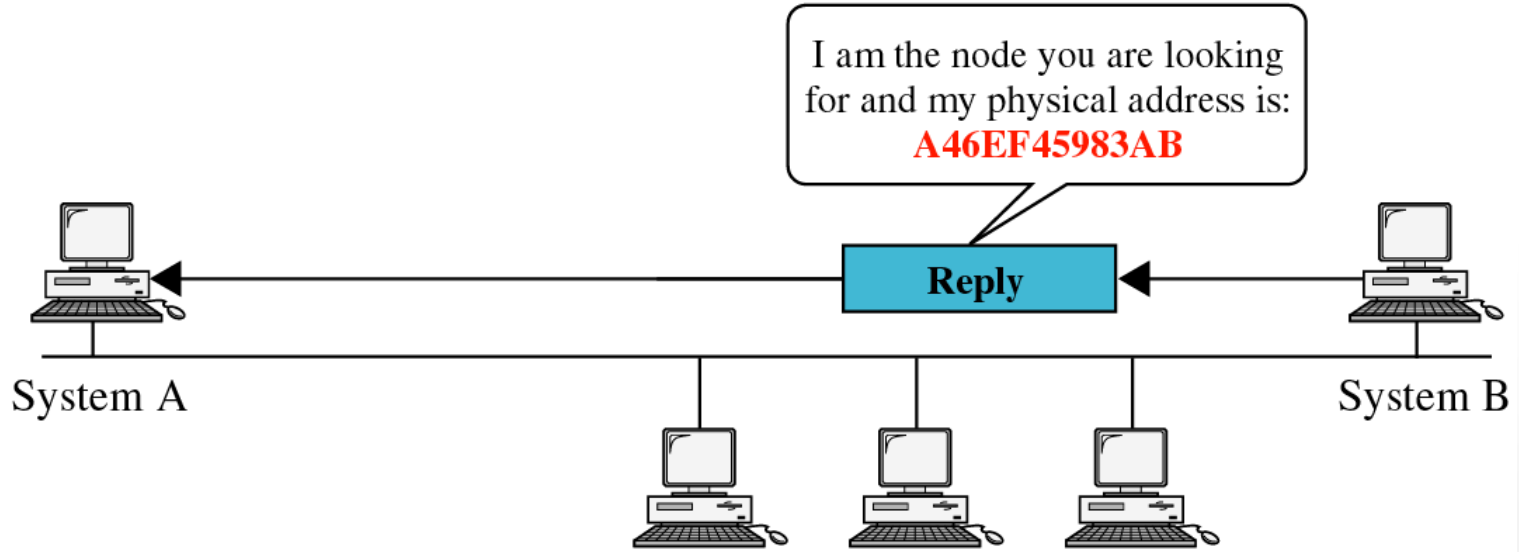
iii. The requested packet is broadcasted over the network.

iv. Every host and router on the network receives and processes the ARP request packet. But only the intended receiver (B) recognizes its IP address in the request packet and sends back an ARP response packet.

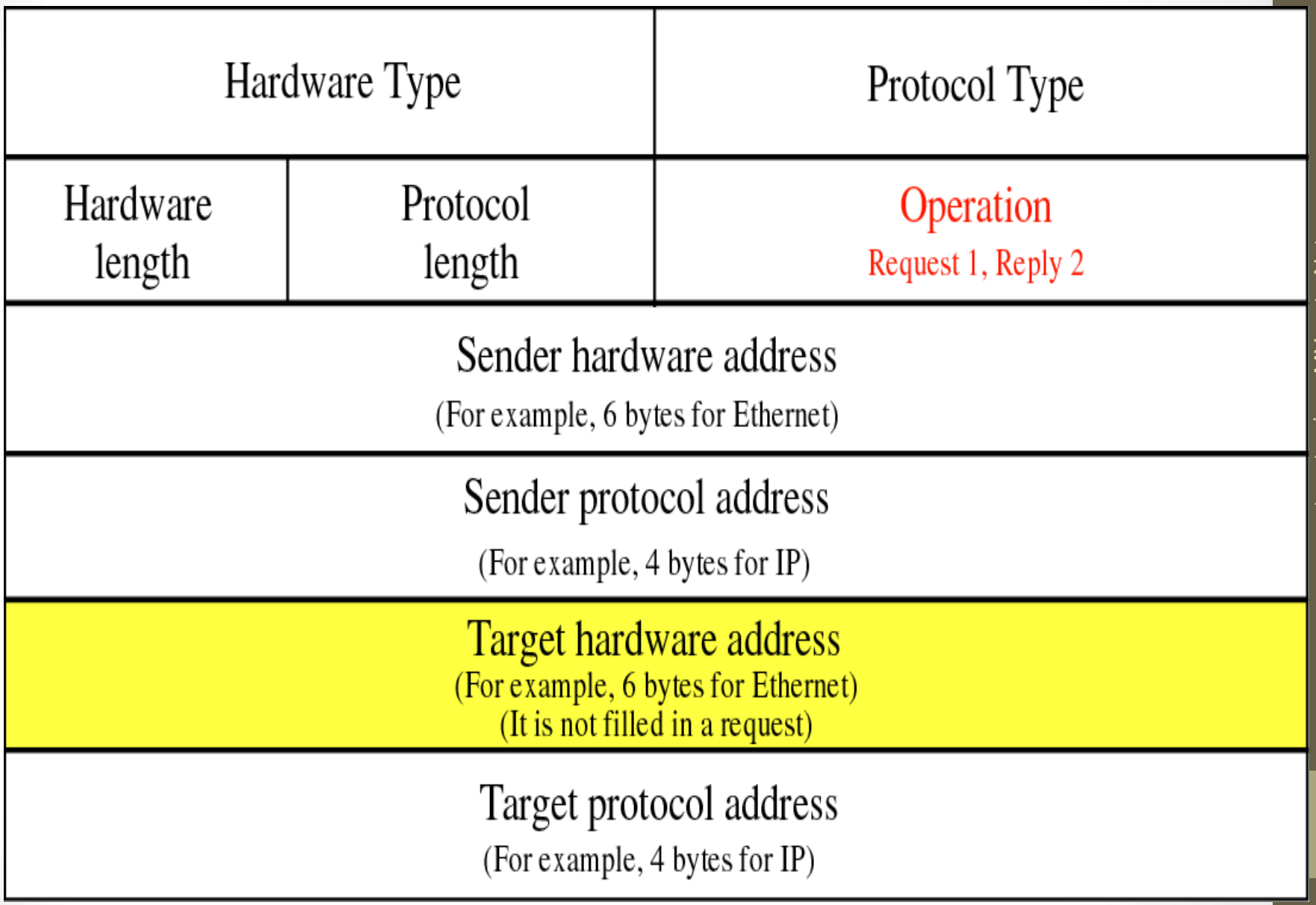
v. The ARP response packet contains the IP and physical addresses of the receiver (B). This packet is delivered only to A using A's physical address in the ARP request packet.



a. ARP request is broadcast



b. ARP reply is unicast



ARP packet format

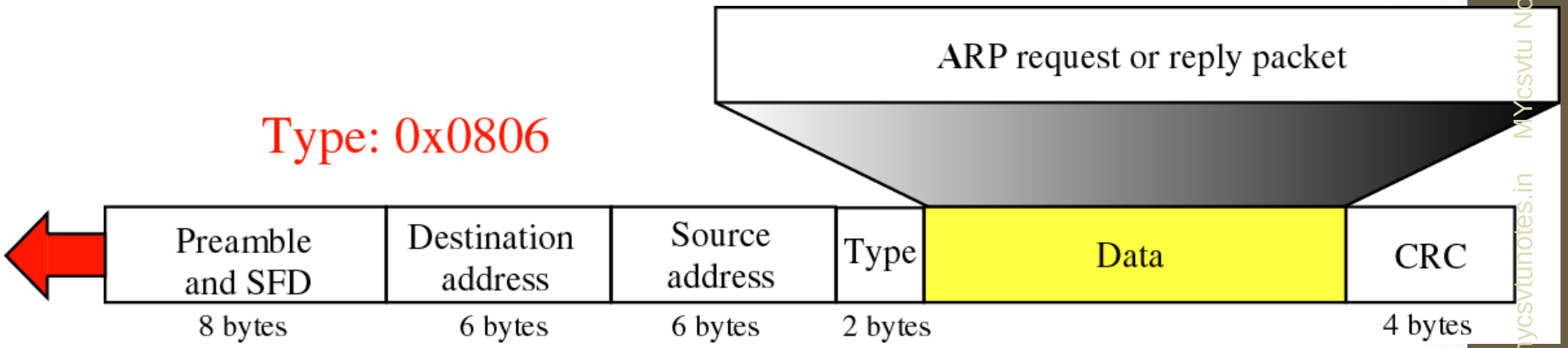
1. **HTYPE(hardware type)**: this is a 16 bit field defining the type of network on which ARP is running. Each LAN has been assigned an integer based on its type. For example, Ethernet is given type 1. ARP can be used on any physical network.
2. **PTYPE(protocol type):** this is a 16 bit field defining the protocol using ARP. For example, the value of this field for the IPv4 protocol is 0800_{16} .
3. **HLEN(hardware length):** this is an 8 bit field defining the length of the physical address in bytes. For example, for Ethernet the value is 6.
4. **PLEN(protocol length):** this is an 8-bit field defining the length of the IP address in bytes. For example, for the IPv4 protocol the value is 4.

5. **OPER(operation):** this is a 16-bit field defining the type of packet. Two packet types are defined: ARP request(1) and ARP reply(2).

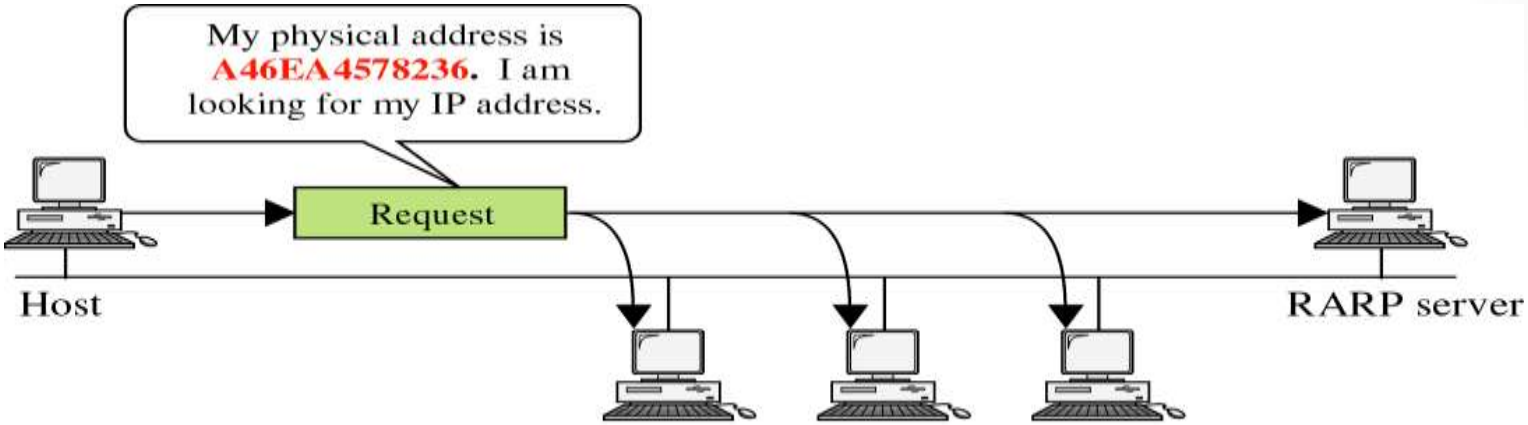
6. **SHA(sender hardware address):** this is a variable-length field defining the physical address of the sender. For example, the Ethernet this field is 6 bytes long.
7. **SPA (sender protocol address):** this is a variable-length field defining the logical address of the sender. For example, the Ethernet this field is 4 bytes long.
8. **THA(target hardware address):** this is a variable-length field defining the physical address of the target. For example, the Ethernet this field is 6 bytes long.
9. **TPA (target protocol address):** this is a variable-length field defining the logical address of the target. For example, the Ethernet this field is 4 bytes long.

Encapsulation

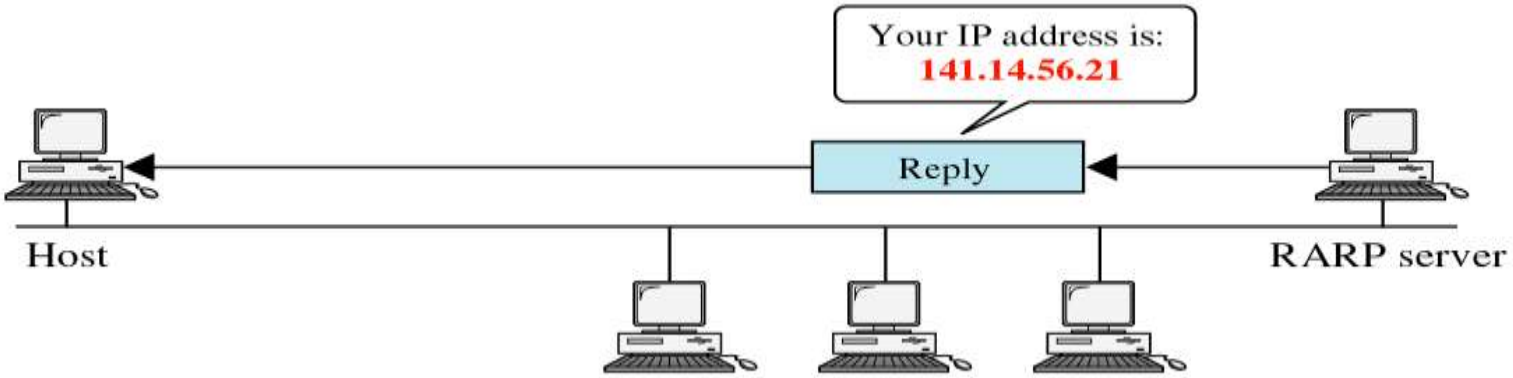
- An ARP packet is encapsulated directly into the data link frame.
- In example an ARP packet being encapsulated in an Ethernet frame.
- The type field indicates that the data carried by the frame is an ARP request or reply packet.



How to find the Physical address



a. RARP request is broadcast

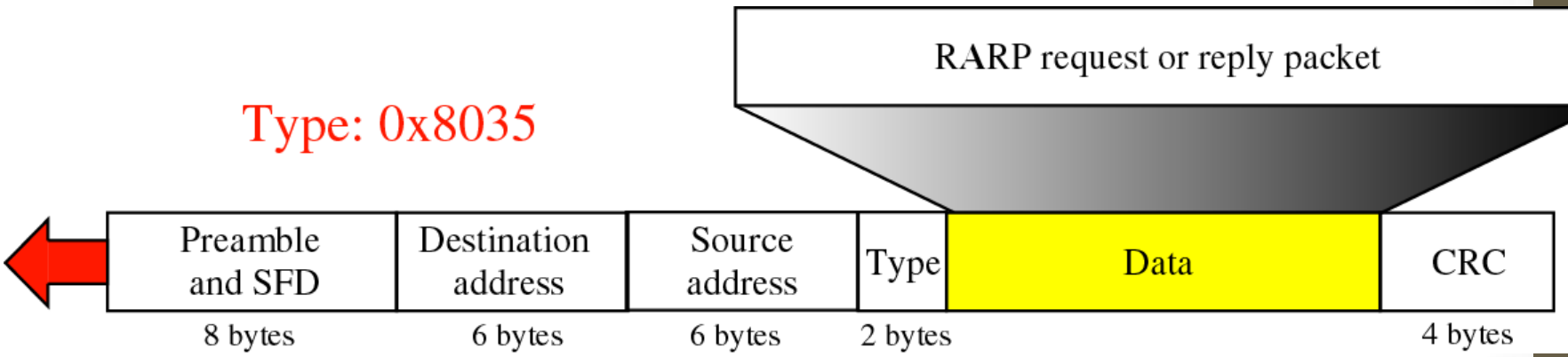


b. RARP reply is unicast

RARP packet format

Hardware type		Protocol type
Hardware length	Protocol length	Operation Request 3, Reply 4
Sender hardware address (For example, 6 bytes for Ethernet)		
Sender protocol address (For example, 4 bytes for IP) (It is not filled for request)		
Target hardware address (For example, 6 bytes for Ethernet) (It is not filled for request)		
Target protocol address (For example, 4 bytes for IP) (It is not filled for request)		

Encapsulation



Internet Protocol(IP)

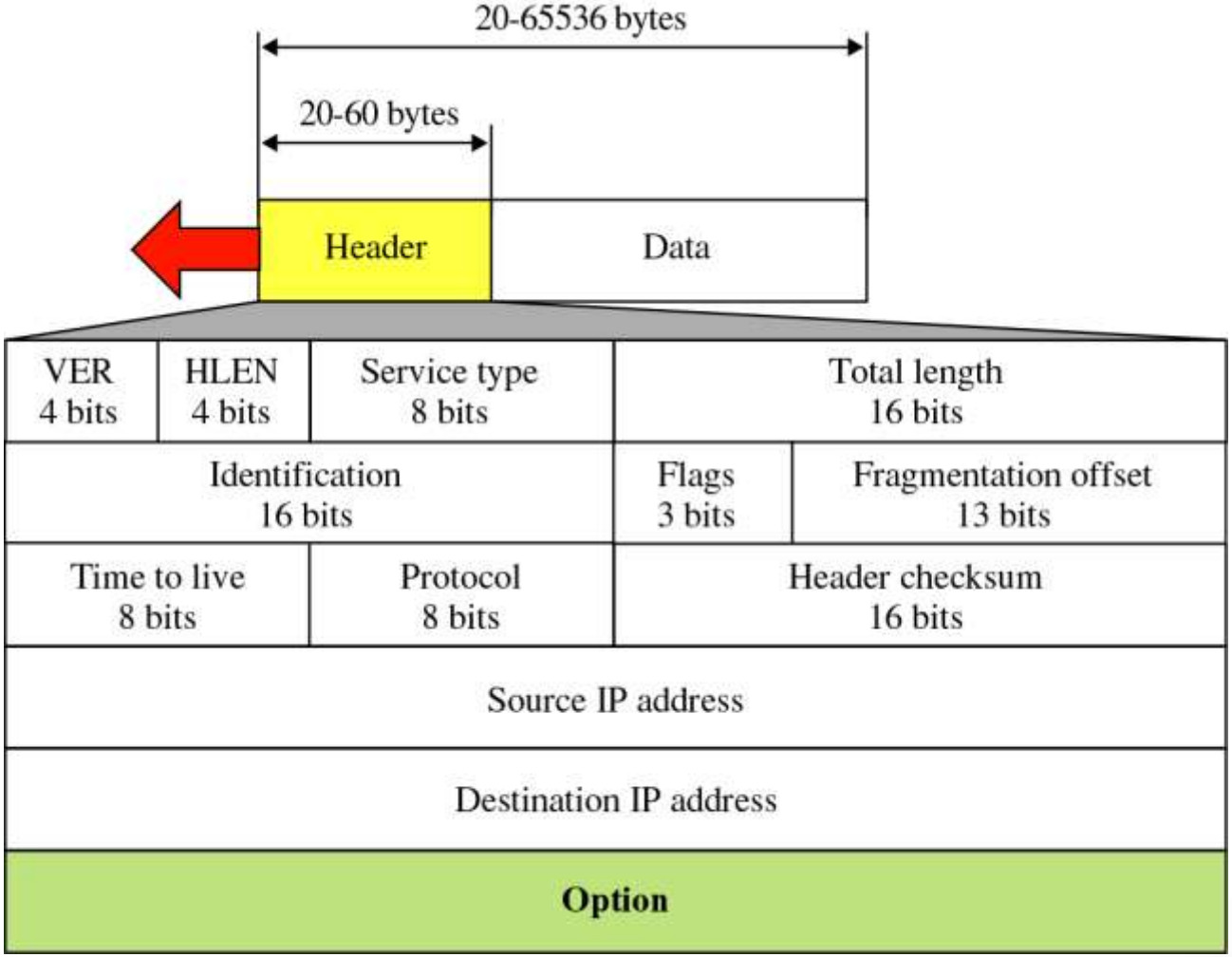
Internet Protocol(IP)

- This is the host-to-host network layer delivery protocol designed for the internet.
- IP is a connectionless datagram protocol with no guarantee of reliability.
- It is unreliable protocol because it does not provide any error control or flow control.
- IP can only detect the error and discards the packet if it is corrupted.
- If IP is to be made more reliable, then it must be paired with a reliable protocol such as TCP at the transport layer.
- Each IP datagram is handled independently and each one can follow a different route to the destination.
- So there is a possibility of receiving out of order packets at the destination. Some packets may even be lost or corrupted.
- IP relies on a higher level protocol to take care of all these problems.

Datagram

- Packets in the IP layer are called datagram.
- A datagram is a variable length packet with two parts namely the header and data.
- The header is 20 to 60 bytes in length.
- It contains the information essential for routing and delivery.
- The other part of the datagram is the data field which is of variable length.

Format of IP Datagram

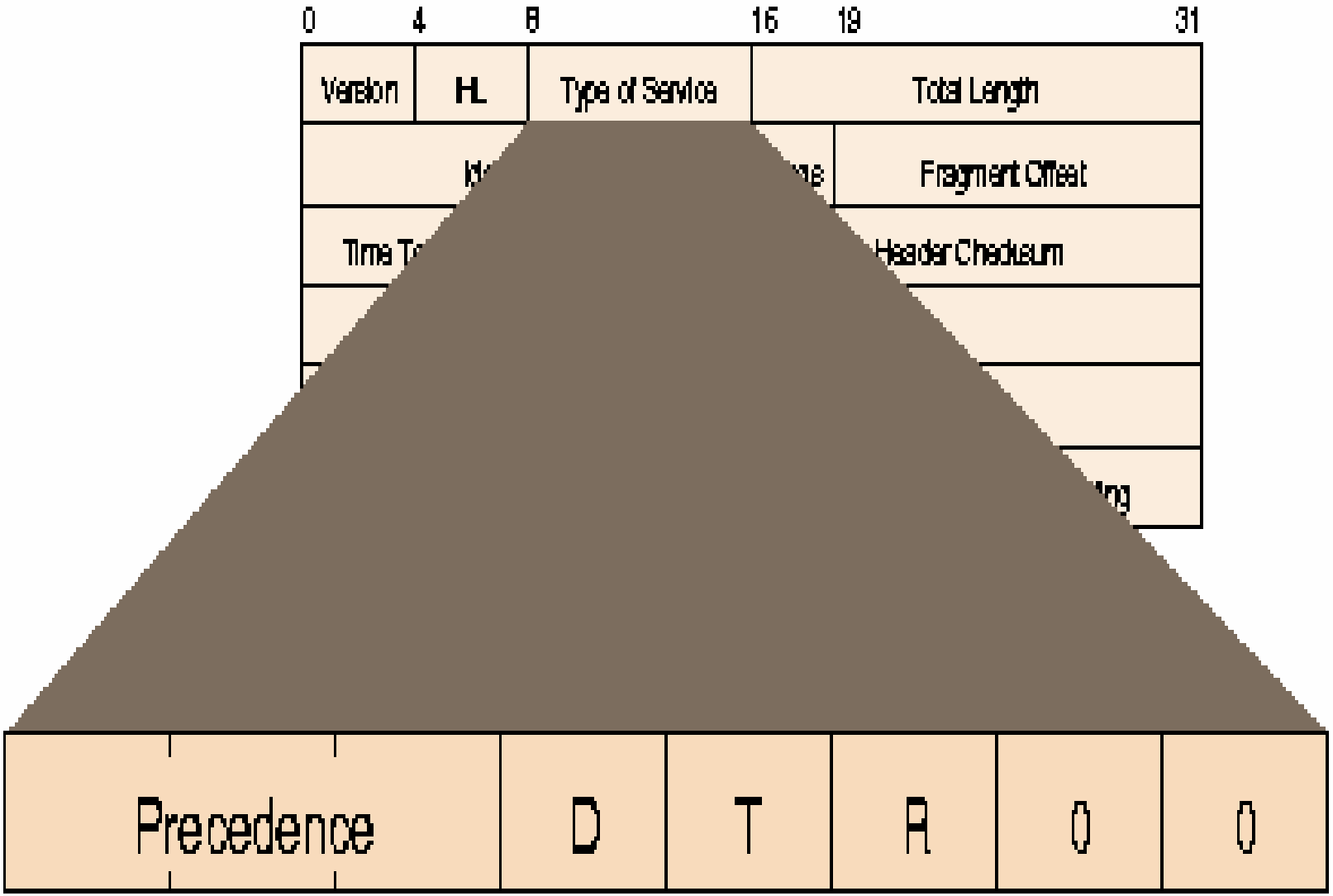


Various fields in the IP header are as follows:

VER(version): this field defines the version of IP. Current version of IP is IPv4 and the latest version of IP is IPv6.

HLEN(Header length): Length of the header is variable.

Service type: this field defines the class of the datagram for quality-of-service purposes.



Bits 0-2: Precedence.

Bit 3: 0 = Normal Delay, 1 = Low Delay.

Bit 4: 0 = Normal Throughput, 1 = High Throughput.

Bit 5: 0 = Normal Relibility, 1 = High Relibility.

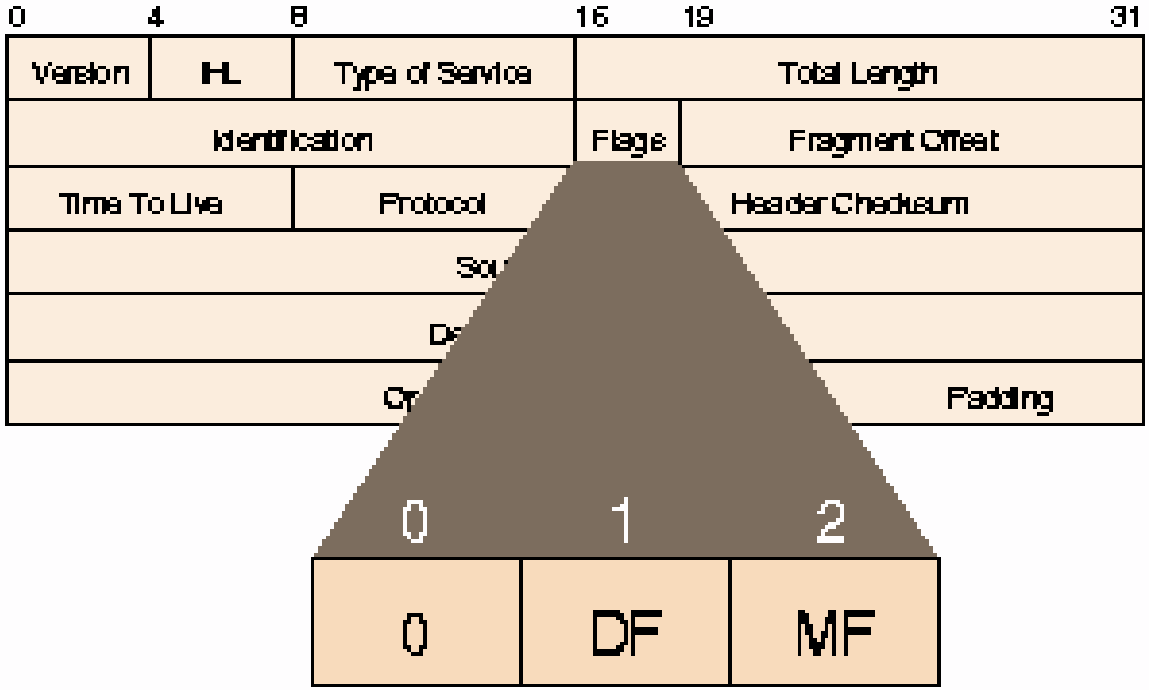
Bit 6-7: Reserved for Future Use.

Precedence

111 - Network Control	011 - Flash
110 - Internetwork Control	010 - Immediate
101 - CRITIC/ECP	001 - Priority
100 - Flash Override	000 - Routine

- **Routine: (R)** "…is used for all messages that justify transmission by electrical means unless the message delivery is of sufficient urgency to require higher precedence."
- **Priority: (P)** "…is used for all messages that require expeditious action by the addressee(s) and/or furnish essential information for the conduct of ongoing operations."
- **Immediate (O)** "…is reserved for messages relating to situations that gravely affect the security of National/Allied forces or populace."
- **Flash (Z)** "…is reserved for initial enemy contact messages or operational combat messages of extreme urgency."
- **Flash Override (X)** "… is reserved for messages relating to the outbreak of hostilities and/or detonation of nuclear devices."
- **CRITIC/ECP** "…stands for "Critical and Emergency Call Processing" and should only be used for authorized emergency communications, for example in the United States Government Emergency Telecommunications Service (GETS), the United Kingdom Government Telephone Preference Scheme (GTPS) and similar government emergency preparedness or reactionary implementations elsewhere."

- **Total length:** this field defines the total length of the IP datagram. The total length includes the length of header as well as data field.
- **Identification:** this field identifies the datagram originating from the source host.



Bit 0: reserved, must be zero

Bit 1: (DF) 0 = May Fragment, 1 = Don't Fragment.

Bit 2: (MF) 0 = Last Fragment, 1 = More Fragments.

- **Fragment offset**: this is a 13 bit field which shows the relative position of this fragment with respect to the whole datagram.
- **Time to live**: this is an 8 bit long field which controls the maximum number of routers visited by the datagram.
- **Protocol**: this field defines the higher-level protocol which uses the services of the IP layer.
- **Header checksum**: the checksum in the IP packet covers only the header, not the data.
- **Source address**: this field is used for defining the IP address of the source.
- **Destination address**: this field is used for defining the IP address of the destination.
- **Options**: they are used for network testing and debugging.

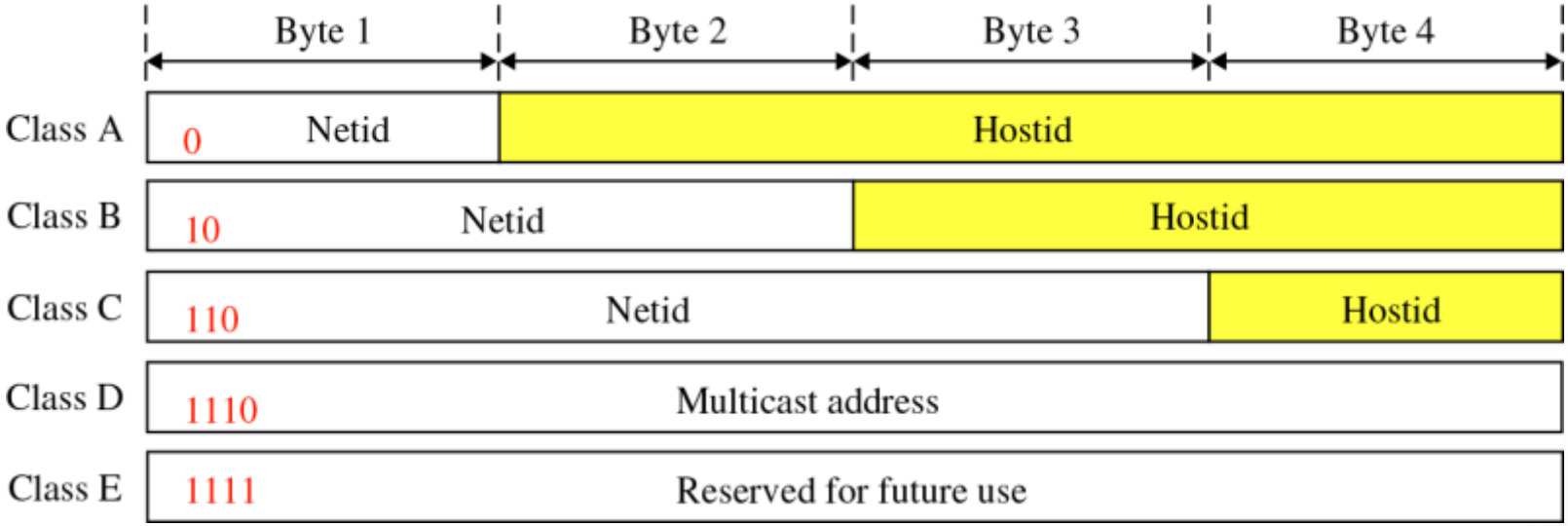
IP addresses

- Every host and router on the internet has a unique IP address.
- All the IP addresses are 32 bit long and they are used in the source address and destination fields of the IP header.
- The IP number for the hosts are assigned by the network administrator.
- For a public network on the internet, we have to obtain a network number assigned by the network information center.
- An IP address consists of two parts. The first part of the address, called the network number, identifies a network on the internet; the remainder, called the host ID, identifies an individual host on that network.

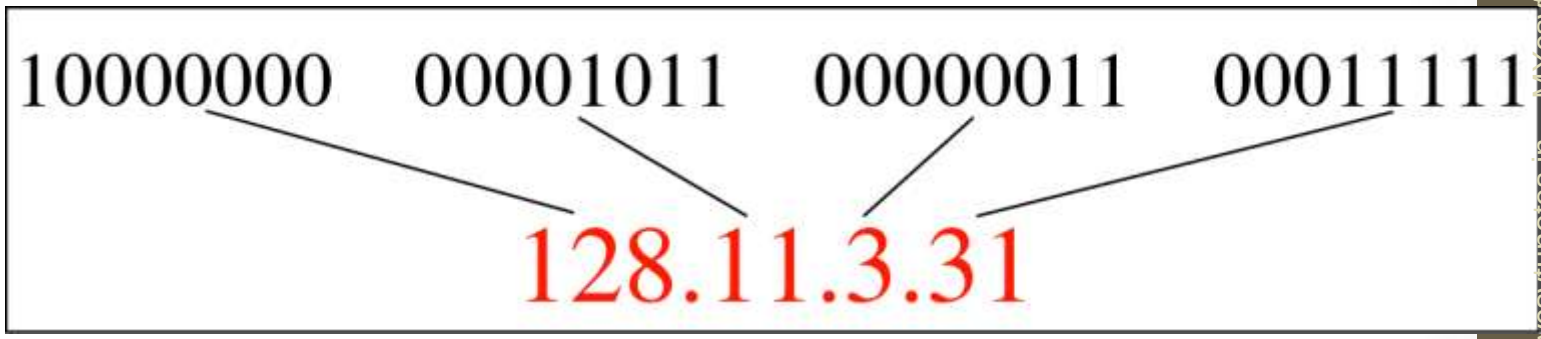
IP address

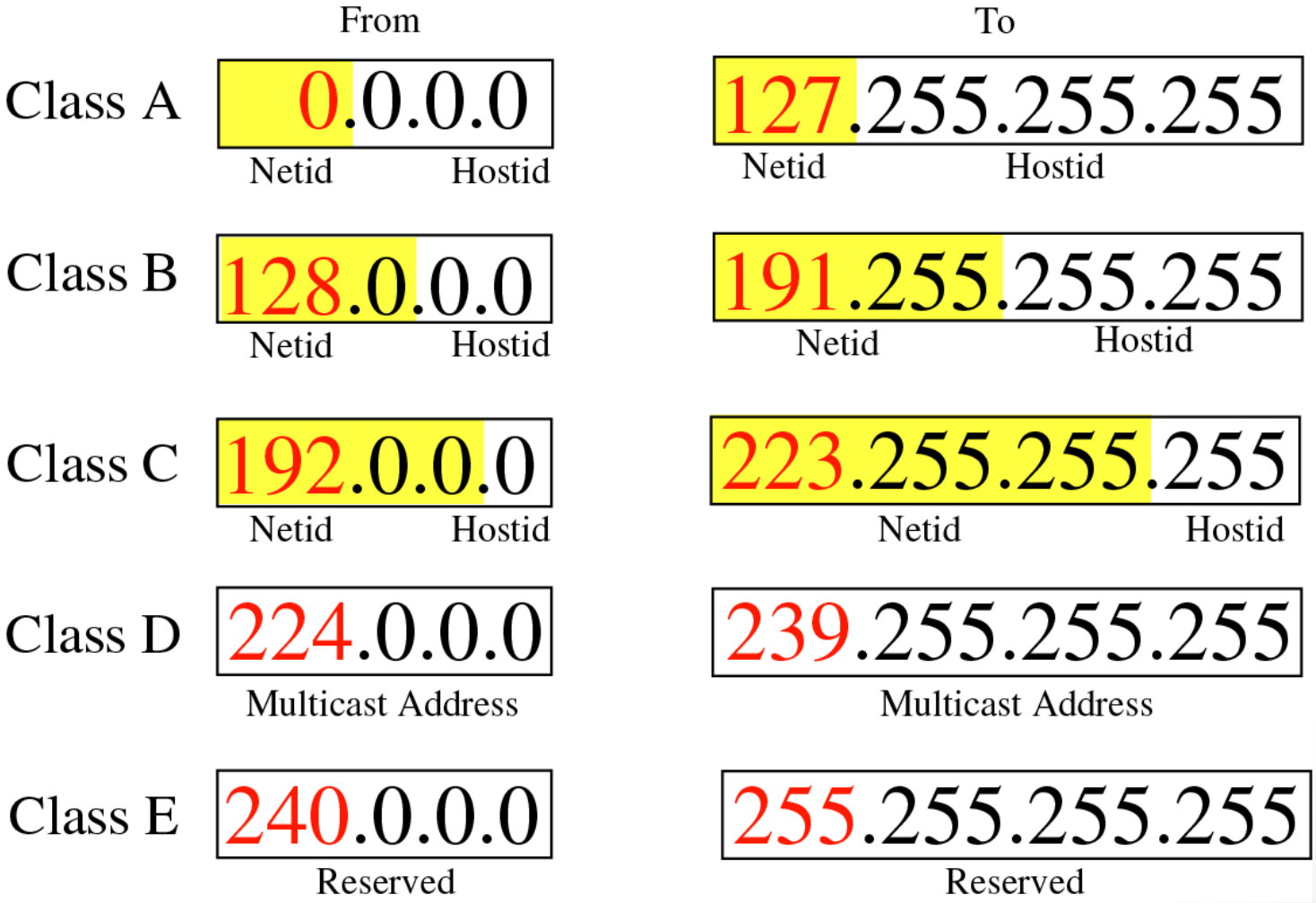
An Internet address is made of four bytes (32 bits) that define a host's connection to a network.

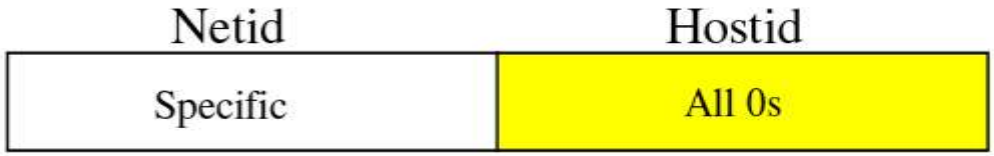
Classes

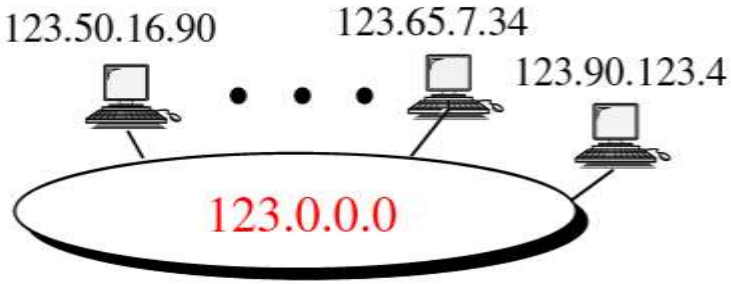


IP Address In Decimal Dotted Notation

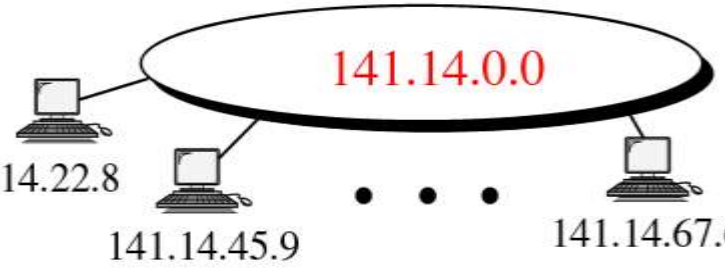




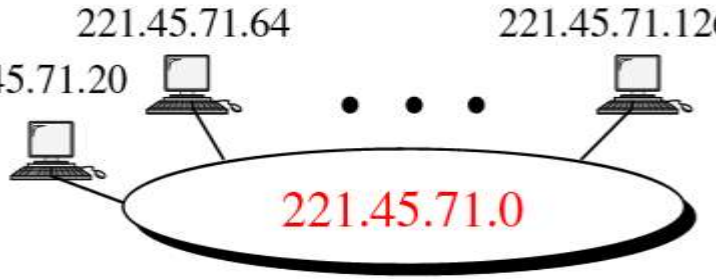




(a) Class A



(b) Class B



(c) Class C

Class	Leading Bits	Size of *Network Number* Bit field	Size of *Rest* Bit field	Number of Networks	Addresses per Network	Start address	End address
Class A	0	8	24	128 (2^7)	16,777,216 (2^{24})	0.0.0.0	127.255.255.255
Class B	10	16	16	16,384 (2^{14})	65,536 (2^{16})	128.0.0.0	191.255.255.255
Class C	110	24	8	2,097,152 (2^{21})	256 (2^8)	192.0.0.0	223.255.255.255
Class D (multicast)	1110	not defined	not defined	not defined	not defined	224.0.0.0	239.255.255.255
Class E (reserved)	1111	not defined	not defined	not defined	not defined	240.0.0.0	255.255.255.255

- The number of addresses usable for addressing specific hosts in each network is always $2^N - 2$ (where N is the number of rest field bits, and the subtraction of 2 adjusts for the use of the all-bits-zero host portion for network address and the all-bits-one host portion as a broadcast address.

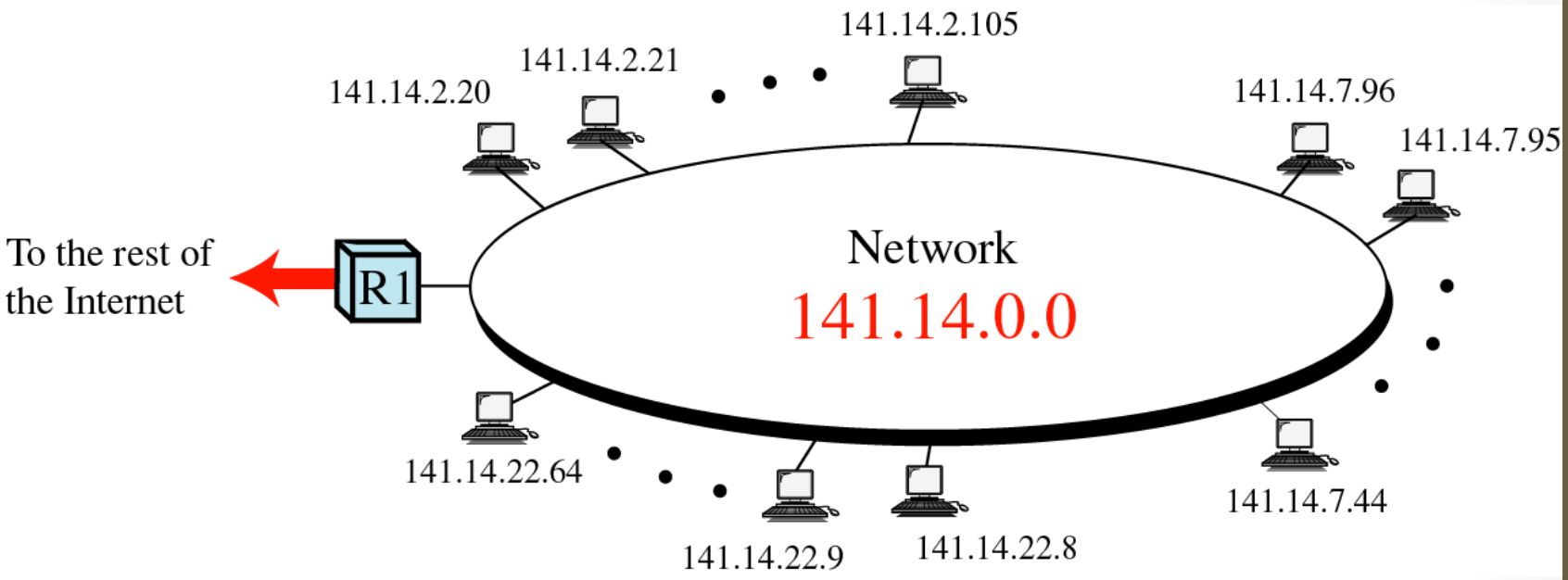
Reserved IP addresses

- It frequently happens that in a company or organization only one computer is linked to the Internet and it is through this that other computers on the network access the Internet (generally we talk of a proxy or gateway).
- In such a case, only the computer linked to the network needs to reserve an IP address with NIC.
- However, the other computers still need an IP address to be able to communicate with each other internally.
- So, NIC has reserved a handful of addresses in each class to enable an IP address to be allocated to computers on a local network linked to the Internet without the risk of creating IP address conflicts on the network of networks. These are the following addresses:
- Private class A IP addresses: 10.0.0.1 to 10.255.255.254, enabling the creation of large private networks comprising of thousands of computers.
- Private class B IP addresses: 172.16.0.1 to 172.31.255.254, making it possible to create medium sized private networks.
- Private class C IP addresses: 192.168.0.1 to 192.168.0.254, for putting in place small private networks.

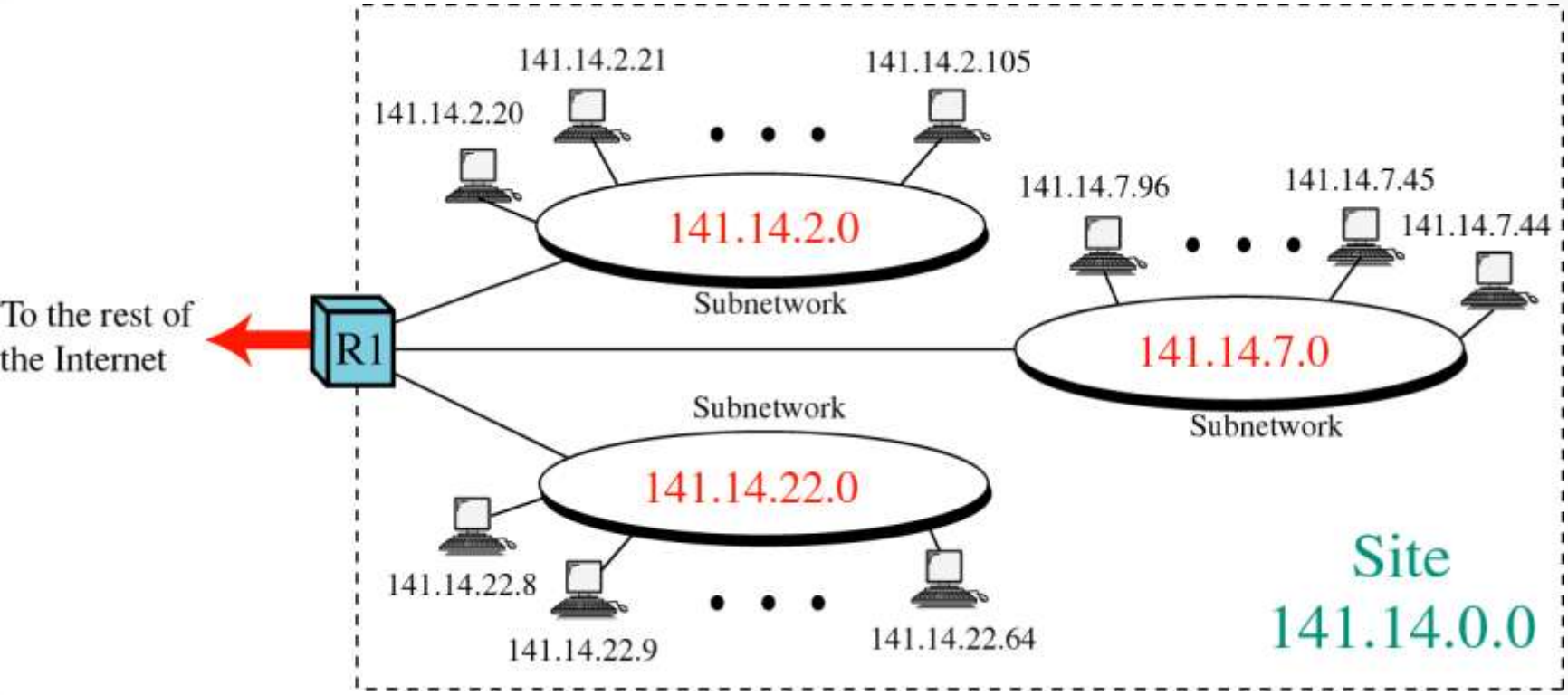
SUBNETTING

- An organization needs to assemble the hosts into groups; the network needs to be divided into several subnetworks (subnets).
- For example, a university may want to group its hosts according to department. In this case, the university has one network address, but needs several sunnetwork addresses.
- The outside world knows the organization by its network address.
- In subnetting, a network is divided into several smaller groups each subnetwork having its own subnetwork addess.

SUBNETTING Contd…….



SUBNETTING Contd…….



Internet Control Message Protocol (ICMP)

Internet Control Message Protocol (ICMP)

- The **Internet Control Message Protocol (ICMP)** is a helper protocol that supports IP with facility for
  - Error reporting
  - Simple queries
- ICMP is a mechanism used by the host and router to send notification of datagram problems back to the sender.
- If delivery of datagram is not possible, ICMP allows it to inform the original source.
- ICMP reports only to the original source.

- ICMP Only Report problem, not correct them.
- it is an integral part of IP.
- ICMP for Internet Protocol version 4 (IPv4) is also known as ICMPv4.
- IPv6 has a similar protocol, ICMPv6.
- ICMP messages are constructed at the IP layer.
- IP encapsulates the appropriate ICMP message with IP header.

ICMP HEADER FORMAT

Type (8 bits)	Code (8 bits)	Checksum (16 bits)
ADDITIONAL INFORMATION		

Each ICMP message contains three fields

1. TYPE→ field identifies the ICMP message.

2.CODE→ field provides further information about the associated TYPE field OR subtype of message.

3. CHECKSUM→ provides a method for determining the integrity of the message. similar to IP header checksum.

If there is no additional data, 4 bytes set to zero.

TYPE	Description
0	Echo Reply
1 & 2	IS RESERVED.
3	Destination Unreachable
4	Source Quench
5	Redirect Message
6	
7	RESERVED.
8	Echo Request
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request (No Longer Used)
16	Information Reply (No Longer Used)
17	Address Mask Request
18	Address Mask Reply
19	IS RESERVED FOR SECURITY.

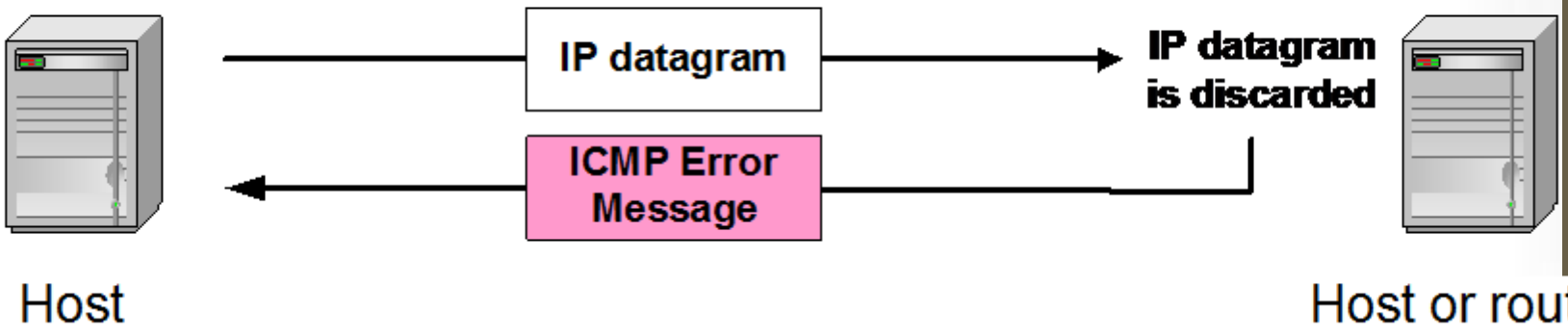
Frequent ICMP Error message

Type	Code	Description	
3	0–15	Destination unreachable	Notification that an IP datagram could not be forwarded and was dropped. The code field contains an explanation.
5	0–3	Redirect	Informs about an alternative route for the datagram and should result in a routing table update. The code field explains the reason for the route change.
11	0, 1	Time exceeded	Sent when the TTL field has reached zero (Code 0) or when there is a timeout for the reassembly of segments (Code 1)
12	0, 1	Parameter problem	Sent when the IP header is invalid (Code 0) or when an IP header option is missing (Code 1)

Some subtypes of the "Destination Unreachable"

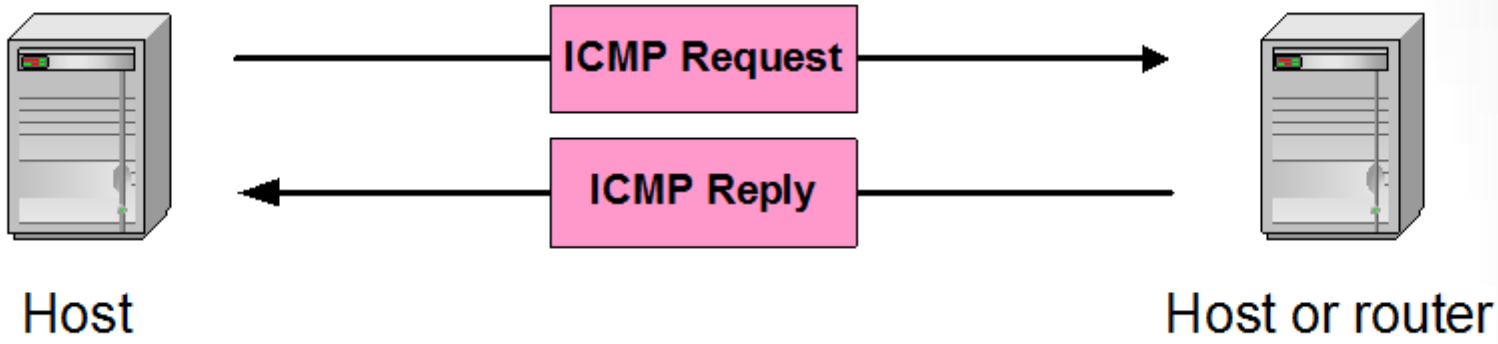
Code	Description	Reason for Sending
0	Network Unreachable	No routing table entry is available for the destination network.
1	Host Unreachable	Destination host should be directly reachable, but does not respond to ARP Requests.
2	Protocol Unreachable	The protocol in the protocol field of the IP header is not supported at the destination.
3	Port Unreachable	The transport protocol at the destination host cannot pass the datagram to an application.
4	Fragmentation Needed and DF Bit Set	IP datagram must be fragmented, but the DF bit in the IP header is set.

ICMP Error message



- **ICMP error messages report error conditions**
- **Typically sent when a datagram is discarded**
- **Error message is often passed from ICMP to the application program**

ICMP Query message



ICMP query:

- Request sent by host to a router or host
- Reply sent back to querying host

Example of ICMP Queries

Type/Code:	Description
8/0	Echo Request
0/0	Echo Reply
13/0	Timestamp Request
14/0	Timestamp Reply
10/0	Router Solicitation
9/0	Router Advertisement

Echo Request & Echo Reply

- They are designed for diagnosis purpose.
- This pair of messages determines whether two systems can communicate with each other.

Timestamp Request & Timestamp Reply

- It is used for synchronization of the clocks in two machines.

Router Solicitation & Router Advertisement

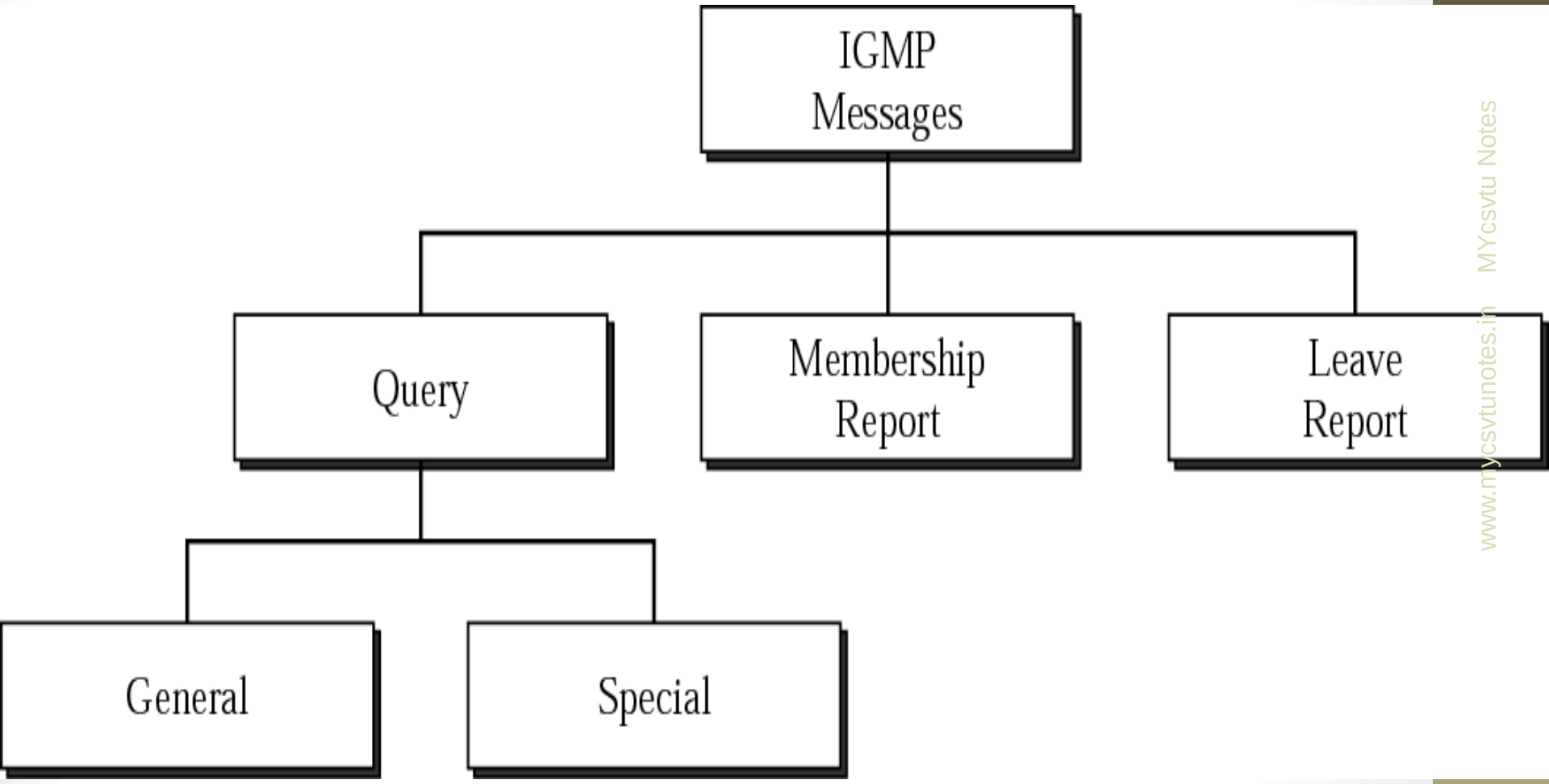
- A host that wants to send data to a host on another network must know the address of routers connected to its own network.
- In such situations this pair of query will help.
- A host can broadcast a router solicitation message.
- The routers receiving this message can broadcast their routing information using the router advertisement message.

Internet Group Management Protocol (IGMP)

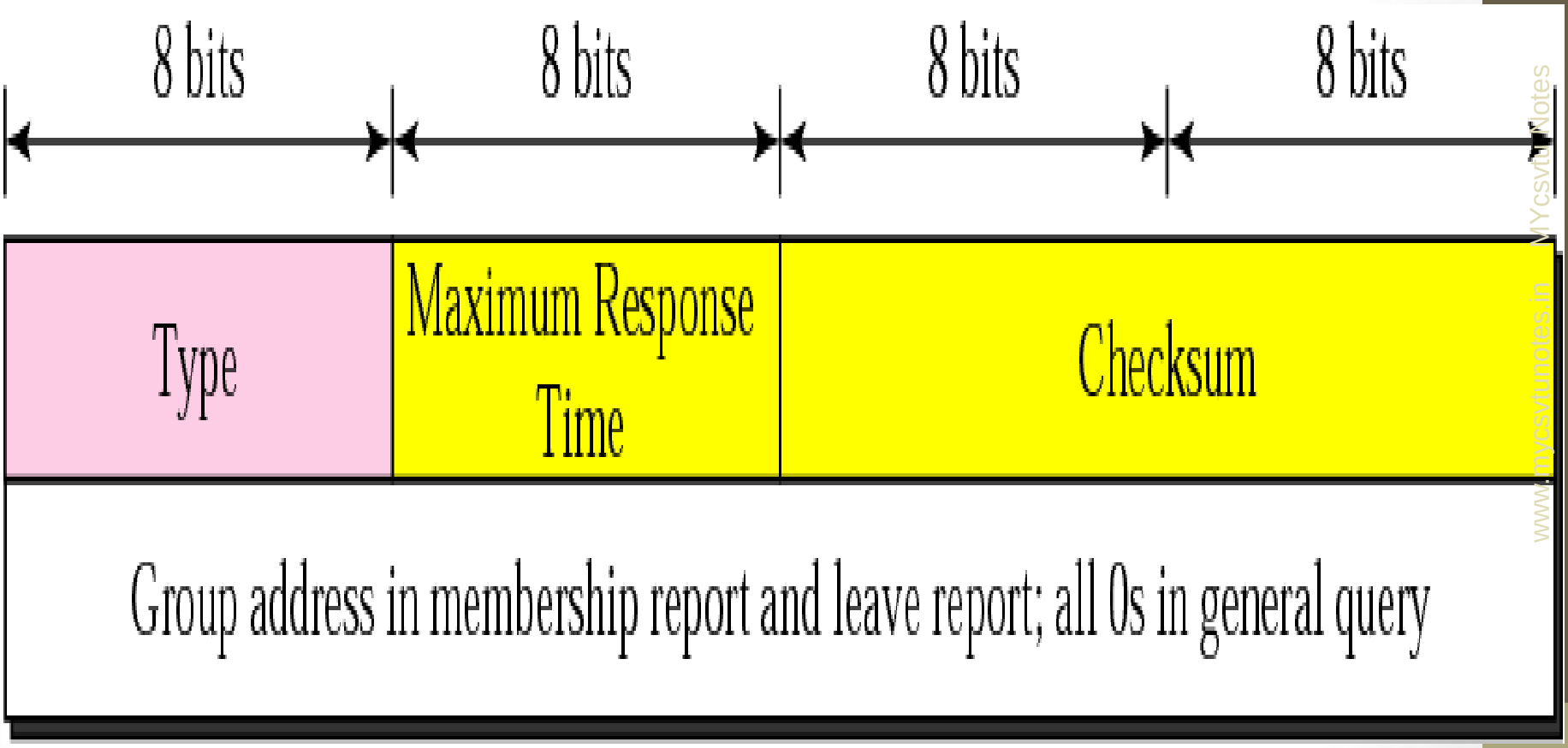
IGMP

- The Internet Group Management Protocol (IGMP) is a communication protocol used to manage the membership of Internet Protocol multicast groups.
- Multicasting allows a host to transmit an IP datagram to a set of hosts that form a multicast group.
- In multicasting there is one source and a group of destinations.
- Used in mapping of class D network.

IGMP message types



IGMP message format



IGMP type field

- It defines the type of message.

Type	value
General Or Special Query	11 OR 00010001
Membership Report	16 OR 00010110
Leave Report	17 OR 00010111

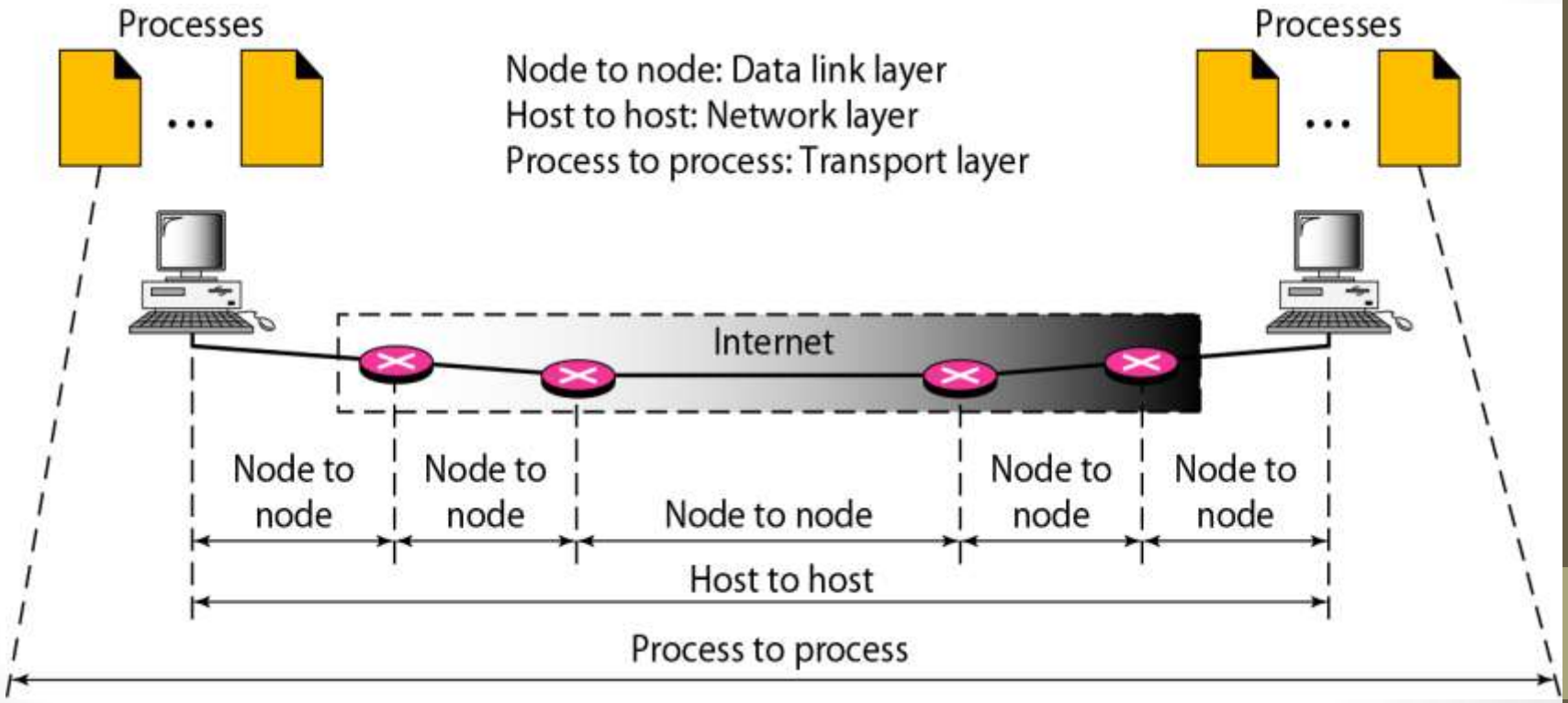
- Max Response Time → defines the amount of time in which a query should be answered. This field is used only in query messages. In all other messages, it is set to 0 by the sender and ignored by the receiver.
- Checksum →This is the 16-bit one's complement of the sum of the entire IGMP message.
- Group Address → The field is zeroed when sending a General Query. This field define the multicast address, in special query, membership report and the leave report.

Transport Layer protocols:

UDP & TCP

Types of data deliveries

- The transport layer is responsible for process-to-process delivery.

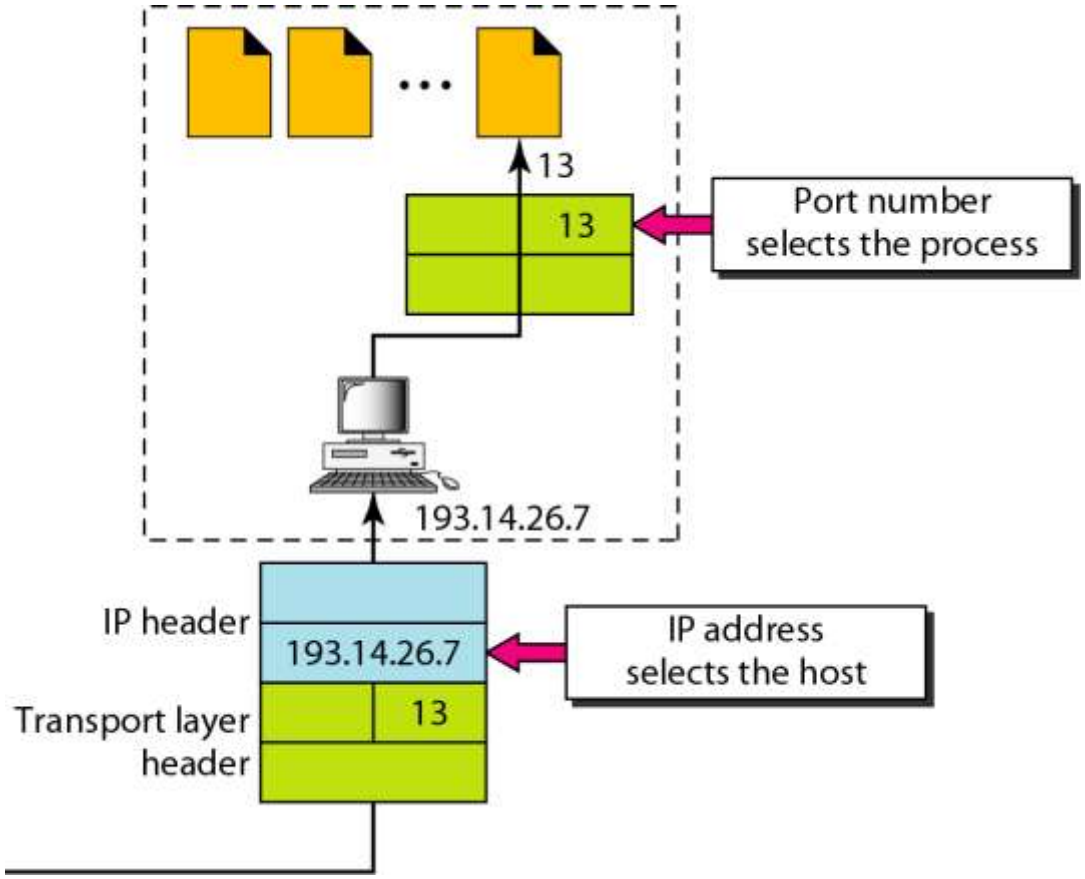


Port Addressing

- At the transport layer , we need transport layer address called a port number, the port numbers are 16 bit integers between 0 to 65535.
- A port is an endpoint to a logical connection and the way a client program specifies a specific server program on a computer in a network.
- The IANA (Internet Assigned Number Authority) has divided the port numbers into 3 ranges:
  - Well known Ports (0 to 1023)
  - Registered Ports (1024 to 49151)
  - Dynamic Ports (49152 to 65535)

Port Number	Description
1	TCP Port Service Multiplexer (TCPMUX)
5	Remote Job Entry (RJE)
7	ECHO
18	Message Send Protocol (MSP)
20	FTP -- Data
21	FTP -- Control
22	SSH Remote Login Protocol
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
29	MSG ICP
37	Time
42	Host Name Server (Nameserv)
43	WhoIs
49	Login Host Protocol (Login)
53	Domain Name System (DNS)
69	Trivial File Transfer Protocol (TFTP)
70	Gopher Services
79	Finger
80	HTTP

IP Addresses vs. Port Numbers



Connection

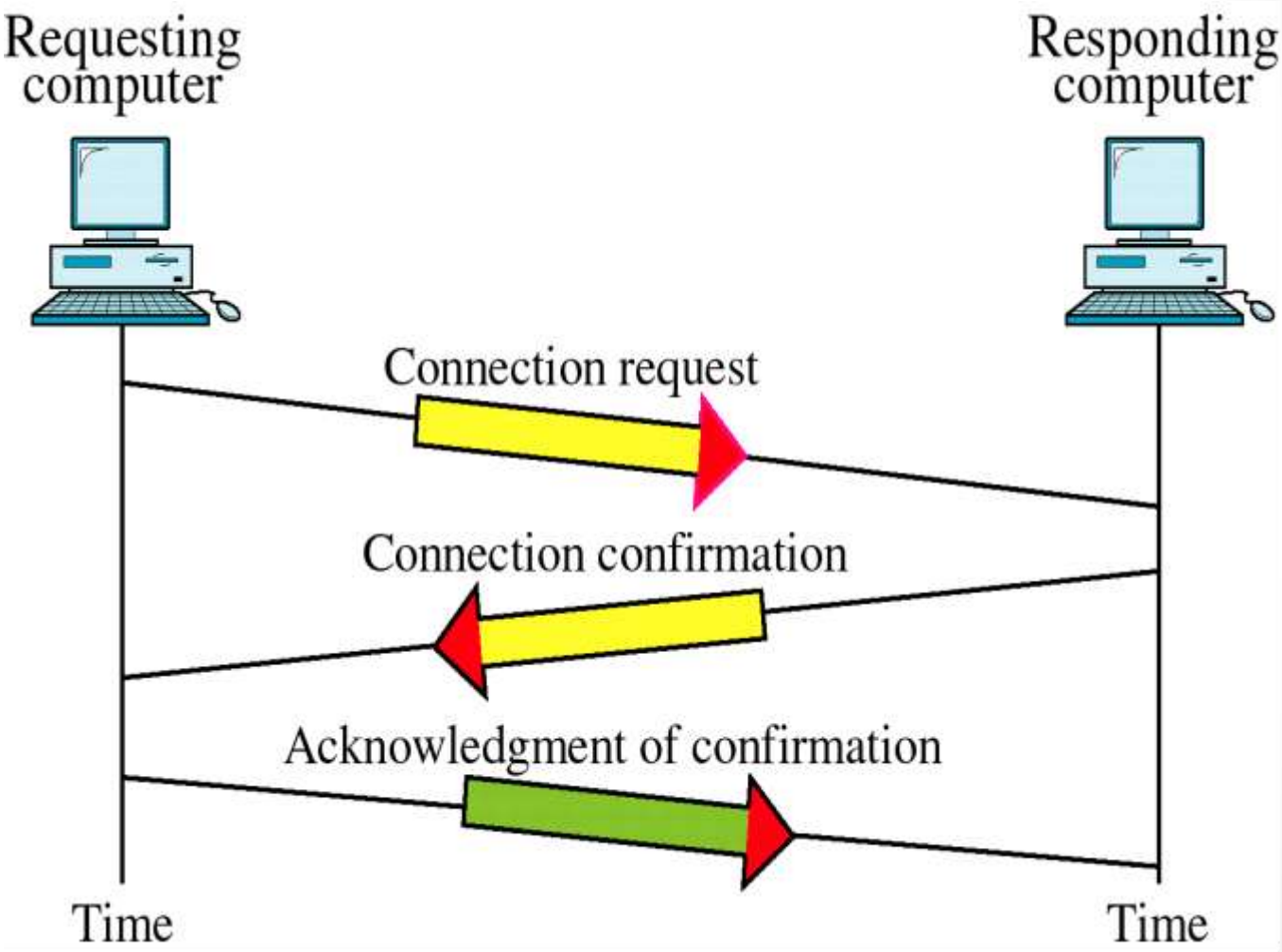
Two types

- Connection-oriented
- Connectionless

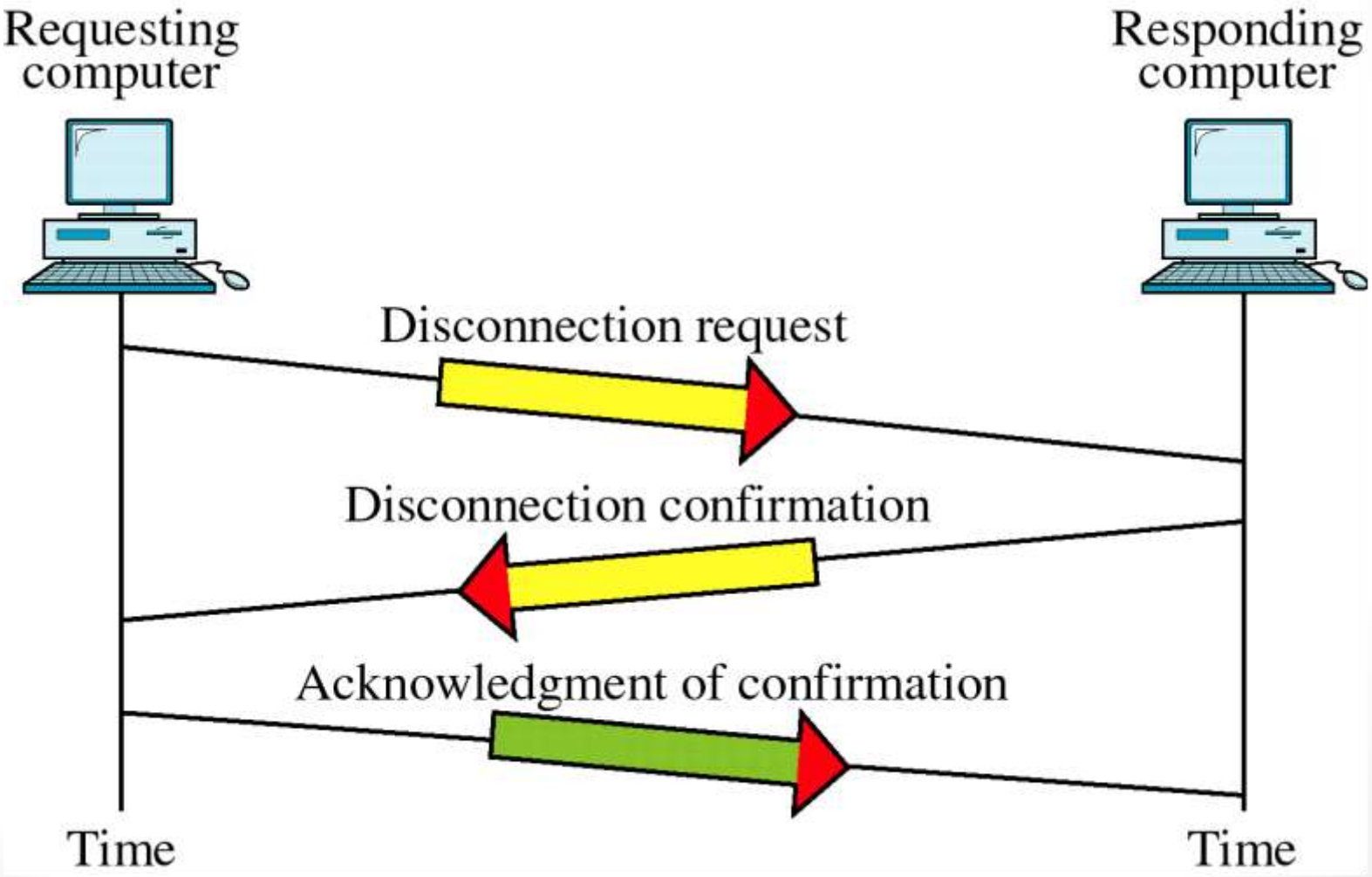
Connection-oriented

- In connection oriented service, a connection is first established between the sender and receiver and data are transferred. At the end connection is released.
  - Connection Establishment
  - Connection Termination

Connection Establishment



Connection Release



Connectionless Service

- In this service the packets are sent from one party to another without connection establishment.
- In this packets are not numbered, they may be delayed , lost or arrive out of order.
- It does not provide any acknowledgement also.

Transport layer Protocols

The Internet has two main protocols in the transport layer.

- TCP (Transmission Control Protocol) is a connection oriented protocol
- UDP (User datagram protocol) is the connectionless protocol.

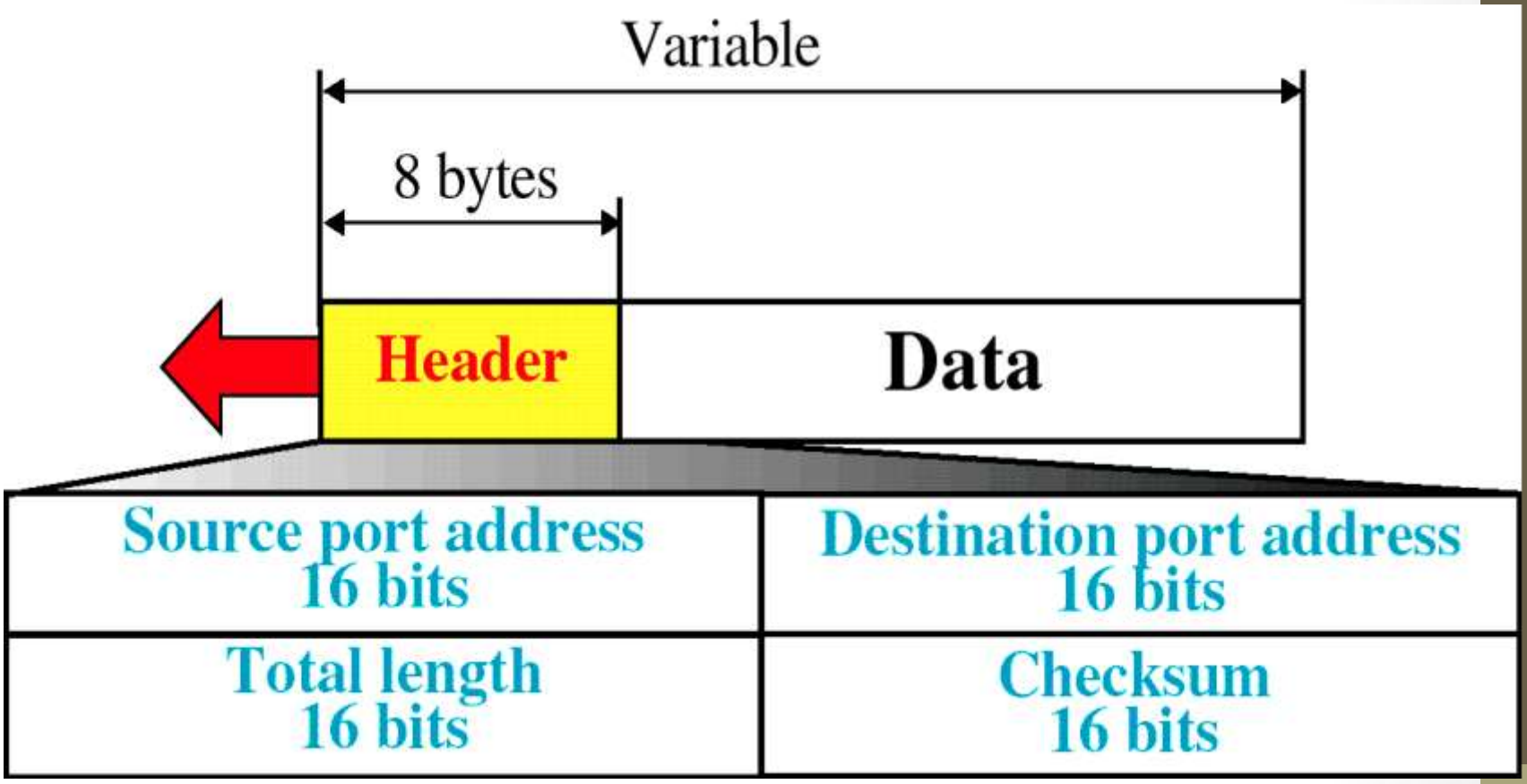
User Datagram Protocol

- UDP is connectionless, unreliable protocol that has no flow and error control.
- UDP is very simple protocol with a minimum of overhead.
- UDP is a convenient protocol for multimedia and multicasting applications.
- UDP packets are called user datagram & have a header of fixed size i.e. of 8 bytes.

Well-known Ports for 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**: this is the port number used by the process running on the source host. It is 16 byte long.
- **Destination port number**: this is the port number used by the process running on the destination host. It is 16 byte long.
- **Length**: this is a 16 bit field that defines the total length of the user datagram, header plus data.
- **Checksum**: this field is used to detect errors over the entire user datagram.

Applications

- UDP is suitable for a process that requires simple request-response communication with little concern for flow and error control.
- UDP is suitable for a process with internal flow and error control mechanism.
- UDP is suitable transport protocol for multicasting.
- UDP is suitable for some route updating protocols such as Routing Information Protocol(RIP).

Transmission control Protocol

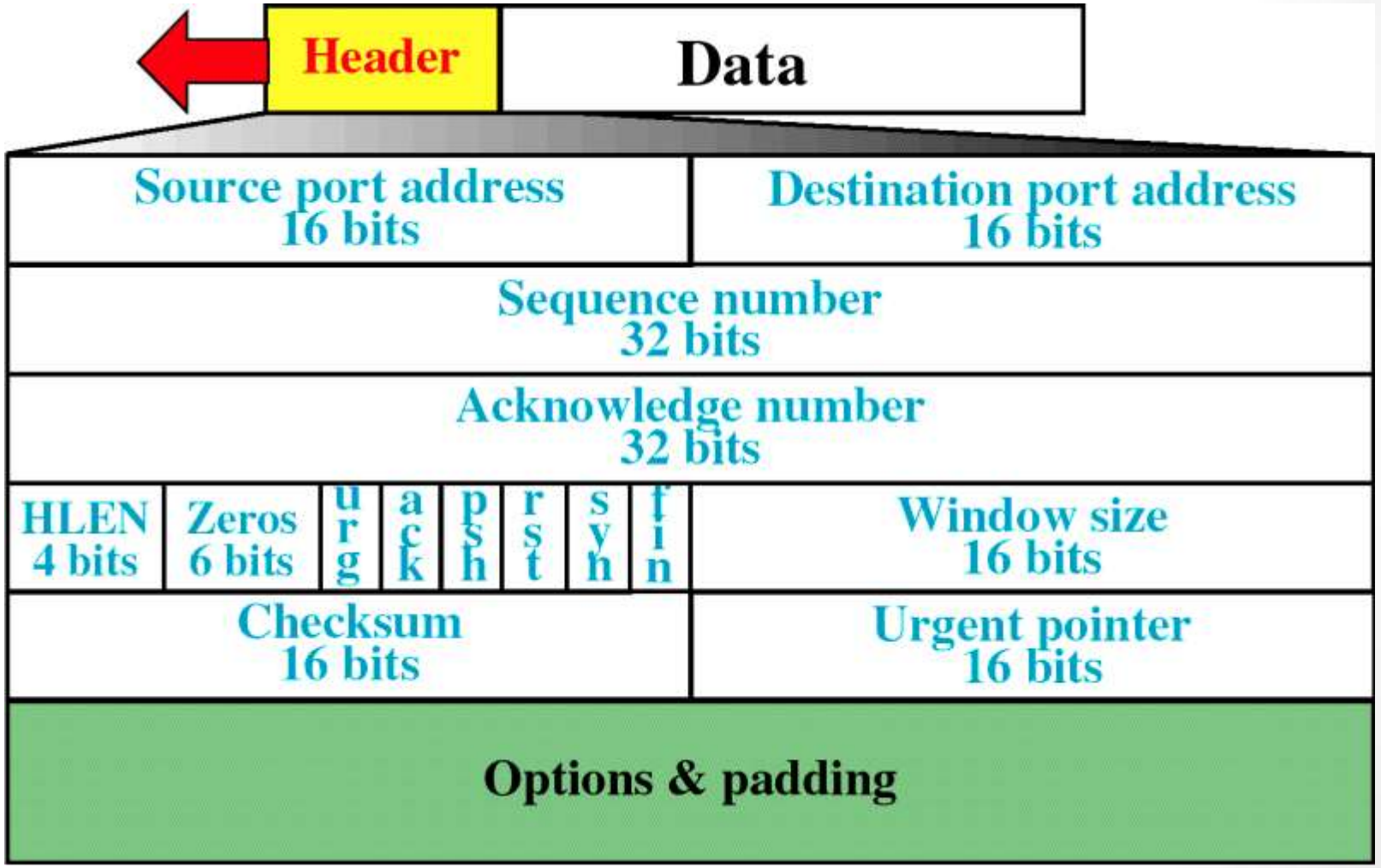
TCP (Transmission Control Protocol)

- TCP is a connection oriented and reliable protocol.
- The unit of data transfer between two devices using TCP is a segment.
- The segment consist of a 20 to 60 byte header followed by the data.
- The header is 20 bytes if there are no options and up to of 60 bytes if it contains option.

Well-known Ports for TCP

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
20	FTP, Data	File Transfer Protocol (data connection)
21	FTP, Control	File Transfer Protocol (control connection)
23	TELNET	Terminal Network
25	SMTP	Simple Mail Transfer Protocol
53	DNS	Domain Name Server
67	BOOTP	Bootstrap Protocol
79	Finger	Finger
80	HTTP	Hypertext Transfer Protocol
111	RPC	Remote Procedure Call

TCP Segment Format



Source port address: this is a 16-bit field that defines the port number of the application program in the host that is sending the segment.

Destination port address: this is a 16-bit field that defines the port number of the application program in the host that is receiving the segment.

Sequence number: this 32-bit field defines the number assigned to the first byte of data contained in this segment.

Acknowledgment number: this 32-bit field defines the byte number that the sender of the segment is expecting to receive from the other party.

Header length: this 4-bit field indicates the number of 4-byte words in the TCP header. Therefore the value of this field can be between 5(5*4=20) and 15(15*4=60)

Reserved: this is a 6-bit field reserved for future use.

Control: this field defines 6 different control bits or flags.

Window size: this field defines the size of the window in bytes, that the other party must maintain.

Checksum: this 16-bit field contains the checksum.

Urgent pointer: this 16-bit field, which is valid only if the urgent flag is set, is used when the segment contains urgent data.

Options: there can be up to 40 bytes of optional information in the TCP header.

URG: Urgent pointer is valid

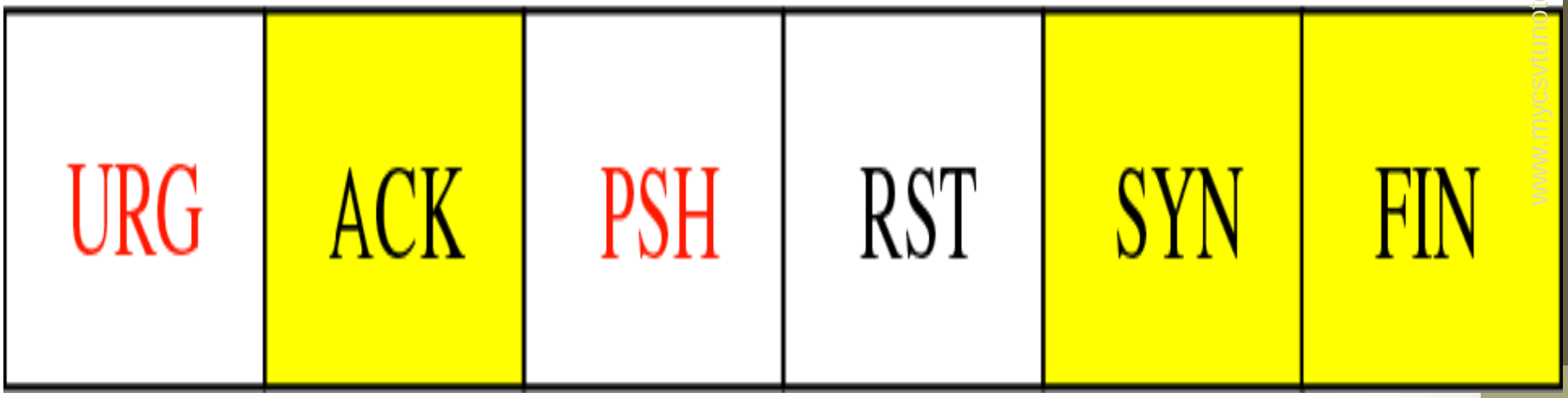
ACK: Acknowledgment is valid

PSH: Request for push

RST: Reset the connection

SYN: Synchronize sequence numbers

FIN: Terminate the connection



TCP Connection

- Connection establishment
- Data transfer
- Connection termination

Connection Establishment

- TCP transmits data in full-duplex mode.
- TCP Connection establishment called a three-way handshaking.
- The steps are:

Step 1:The client sends the first segment, a SYN segment. The segment includes the source and destination port numbers. The segment also contains the client initialization sequence number (ISN) used for numbering the bytes of data sent from the client to the server.

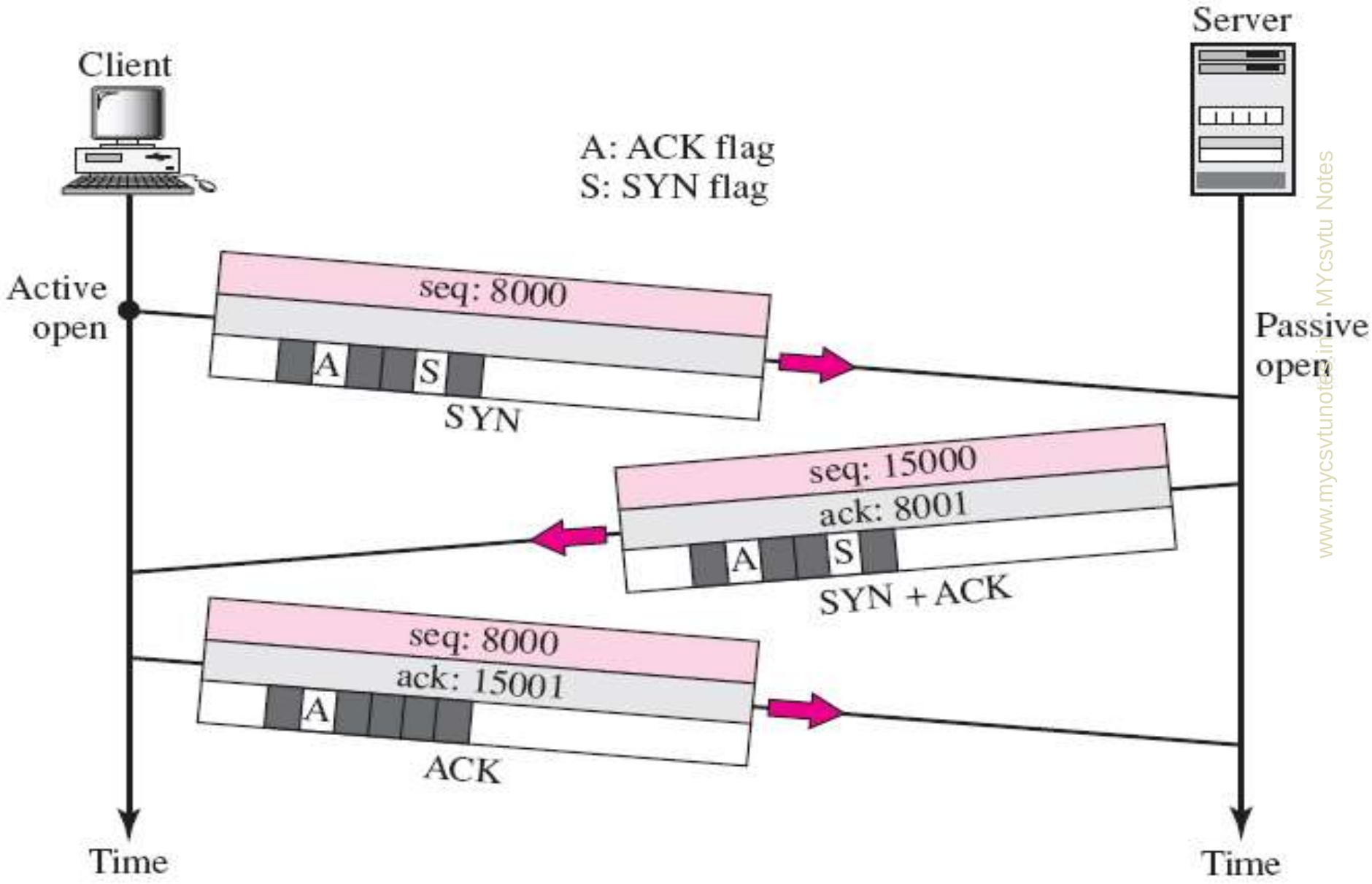
Step 2: the server sends the second segment, a SYN and an ACK segment. This segment first acknowledges the receipt of the first segment. Second, the segment is used as the initialization segment for the server.

- Step 3: the client send the third segment. it acknowledges the receipt of the second segment, using the ACK flag and acknowledgement number field.
- A SYN segment cannot carry data, but it consumes one sequence number.
- A SYN + ACK segment cannot carry data, but does consume one sequence number.
- An ACK segment, if carrying no data, consumes no sequence number.

- **Active open**: an application performs active open by indicating that it wish to establish a connection.

- **Passive open**: an application performs passive open to indicate that it is ready to accept the connection.

A TCP Connection: Establishment

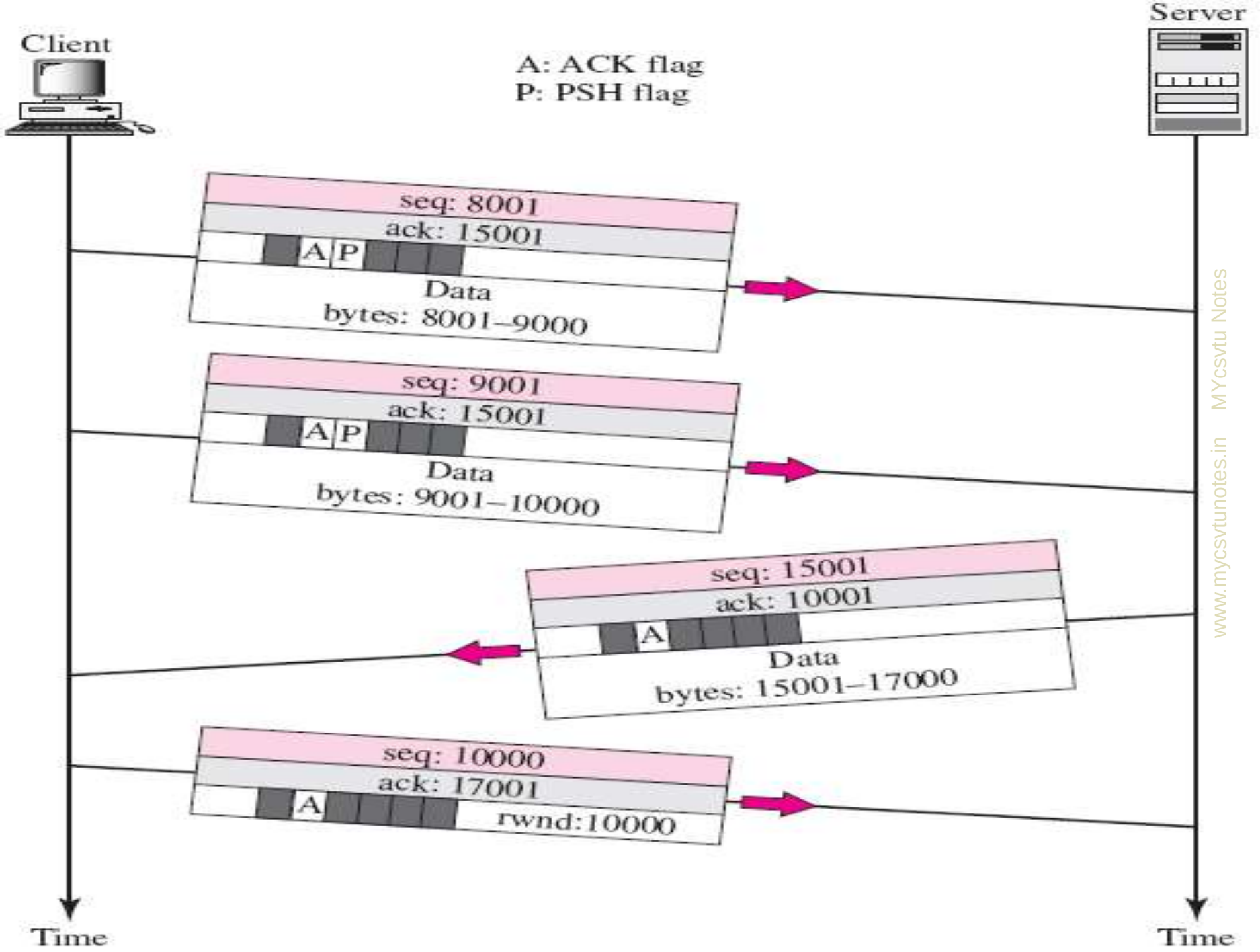


Data transfer

- After connection is established, bidirectional **data transfer can take place.**
- **The client** and server can both send data and acknowledgments.
- After connection is established, the client sends 2000 bytes of data in two segments. The server then sends 2000 bytes in one segment.
- The client sends one more segment. The first three segments carry both data and acknowledgment, but the last segment carries only an acknowledgment because there are no more data to be sent.

Data transfer continued……

- The data segments sent by the client have the PSH (push) flag set so that the server TCP knows to deliver data to the server process as soon as they are received.
- The segment from the server, on the other hand, does not set the push flag.
- Most TCP implementations have the option to set or not set this flag.



Connection Termination

- TCP Connection termination called a three-way handshaking.
- The steps are:

Step 1: the client TCP sends the first segment, a FIN segment.

Step 2: the server TCP sends these second segment, an ACK segment to confirm the receipt of the FIN segment from the client.

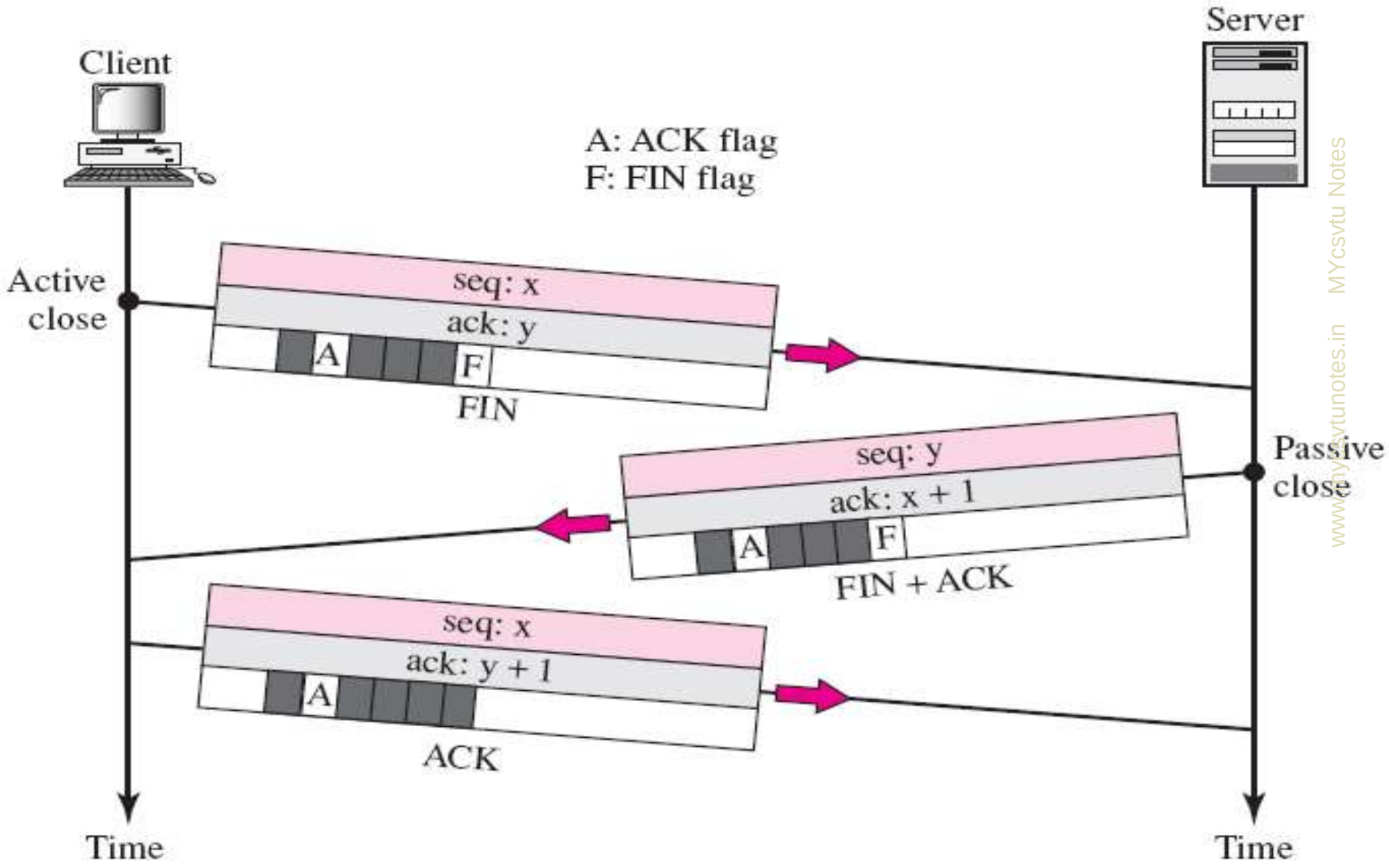
Step 3: The client TCP sends the last segment, an ACK segment, to confirm the receipt of the FIN segment from the TCP server.

- The FIN segment consumes one sequence number if it does not carry data.
- The FIN + ACK segment consumes one sequence number if it does not carry data.
- The ACK segment cannot carry data and consumes no sequence numbers.

- **Active close**: an application that performs close operation first, is said to be performing the active close application i.e the application sending FIN segment first.

- **Passive close**: an application that is receiving the FIN segment is said to be performing the passive close.

A TCP Connection: Connection Termination



Difference between TCP and UDP

1. TCP can establishes a Connection and UDP cannot.
2. TCP provides a stream of unlimited length, UDP sends small packets.
3. TCP guarantees that as long as you have a connection data sent will arrive at the destination, UDP provides not guarantee delivery.
4. TCP provides Flow and Congesion control whereas UDP does not.
5. TCP detects data duplication but UDP does not.
6. TCP is capable of multiplexing where as UDP is not.
7. TCP protocol supports full-duplex (two ways) transmission.

TCP services

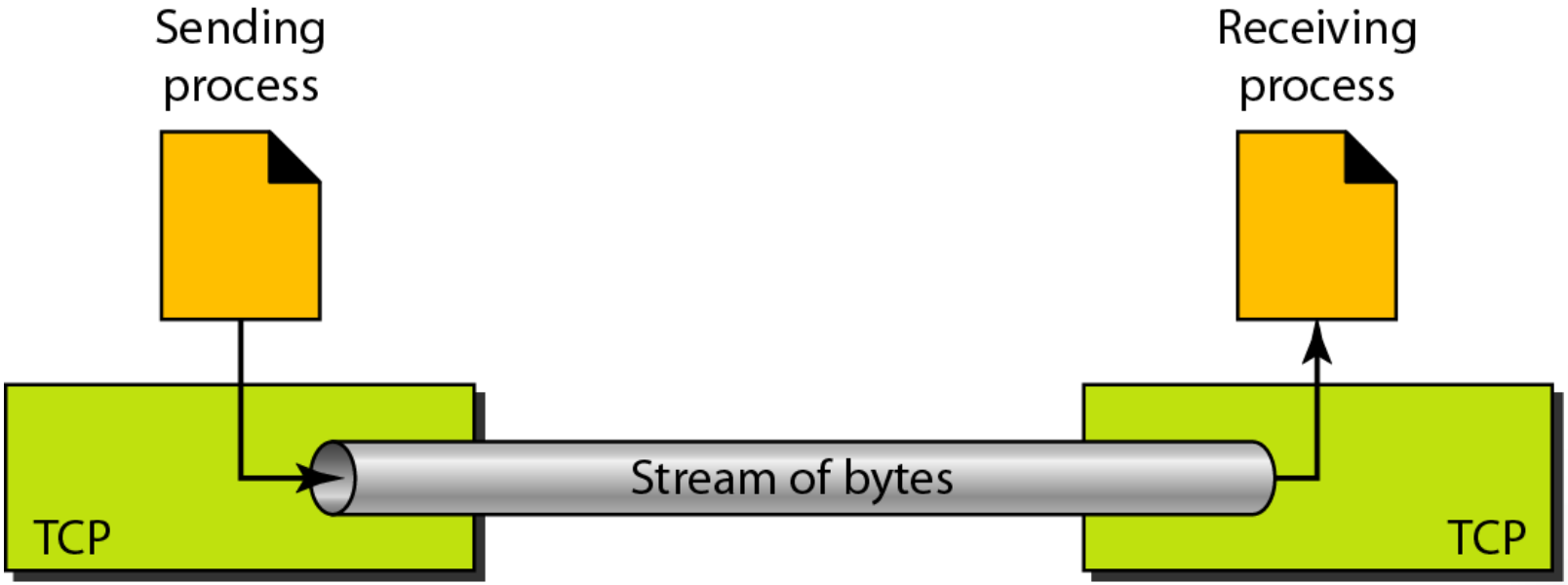
Services offered by TCP to the processes at the application layer:

- Stream delivery service
- Sending and Receiving Buffers
- Bytes and segments
- Full duplex service
- Connection-Oriented service
- Reliable service

Stream delivery service

- TCP is a stream oriented protocol.
- TCP allows the sending process to deliver data as a stream of bytes and the receiving process to obtain data as a stream of bytes.
- TCP creates an environment in which the two processes seem to be connected by an imaginary “tube” that carries their data across the Internet.

Stream deliveries



Sending and Receiving Buffers

- Because the sending and the receiving processes may not produce and consume data at the same speed, TCP needs buffers for storage.
- There are two buffers, the sending buffer and the receiving buffer, for each direction.
- One way to implement a buffer is to use a circular array of 1-byte locations.

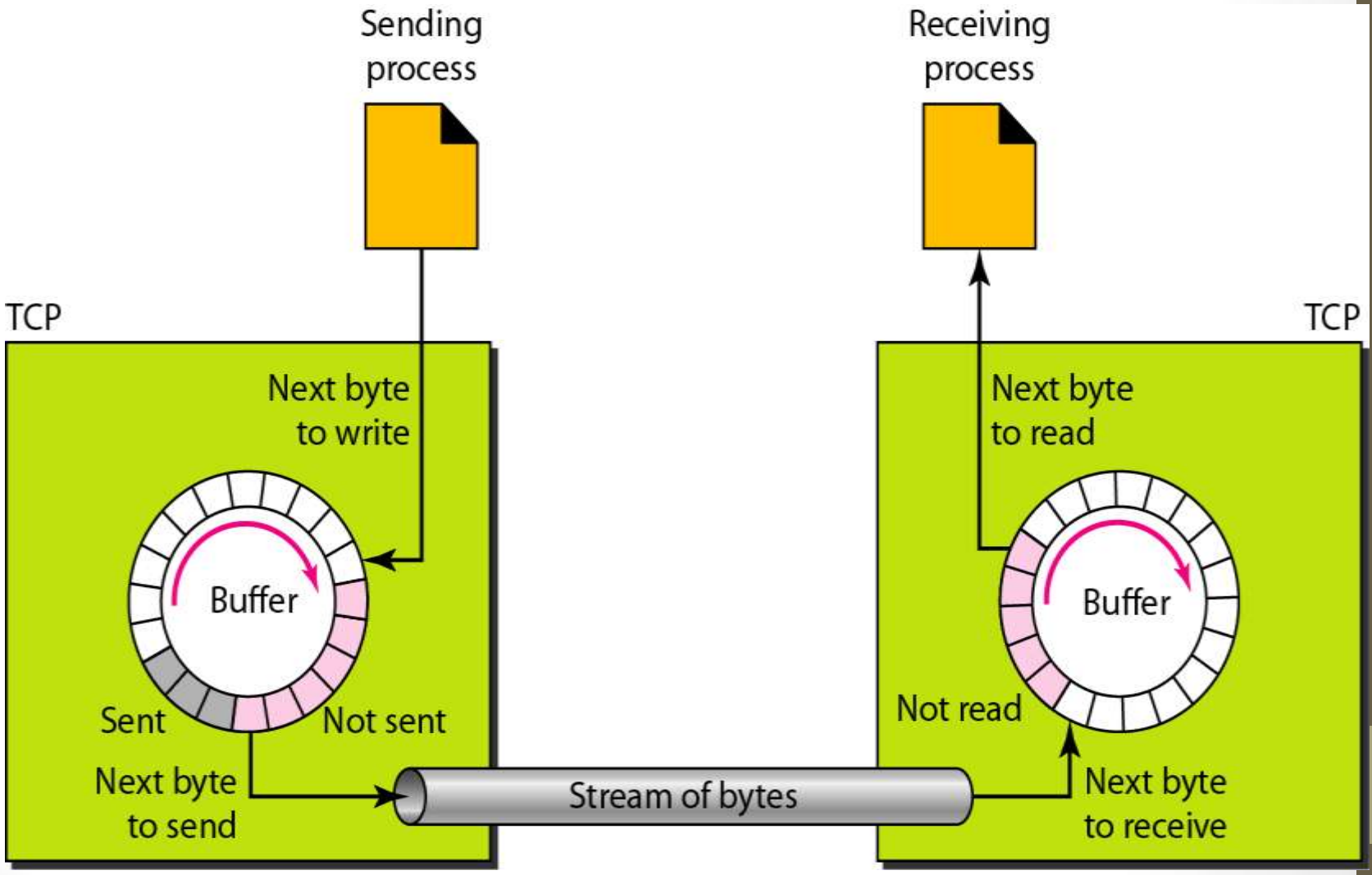
Continued……..

- The figure shows the movement of the data in one direction.
- At the sending site, the buffer has three types of locations.
- The white section contains empty locations that can be filled by the sending process.
- The grey area holds bytes that have been sent but not yet acknowledged. TCP keeps these bytes in the buffer until it receives an acknowledgment.
- The colored areas are bytes to be sent by the sending TCP.

Continued.....

- The operation at the buffer at the receiver site is simpler.
- The circular buffer is divided into two areas.
- The white area contains empty locations to be filled by bytes received from the network.
- The colored sections contain received bytes that can be consumed by the receiving process.
- When a byte is consumed by the receiving process, the location is recycled and added to the pool of empty locations.

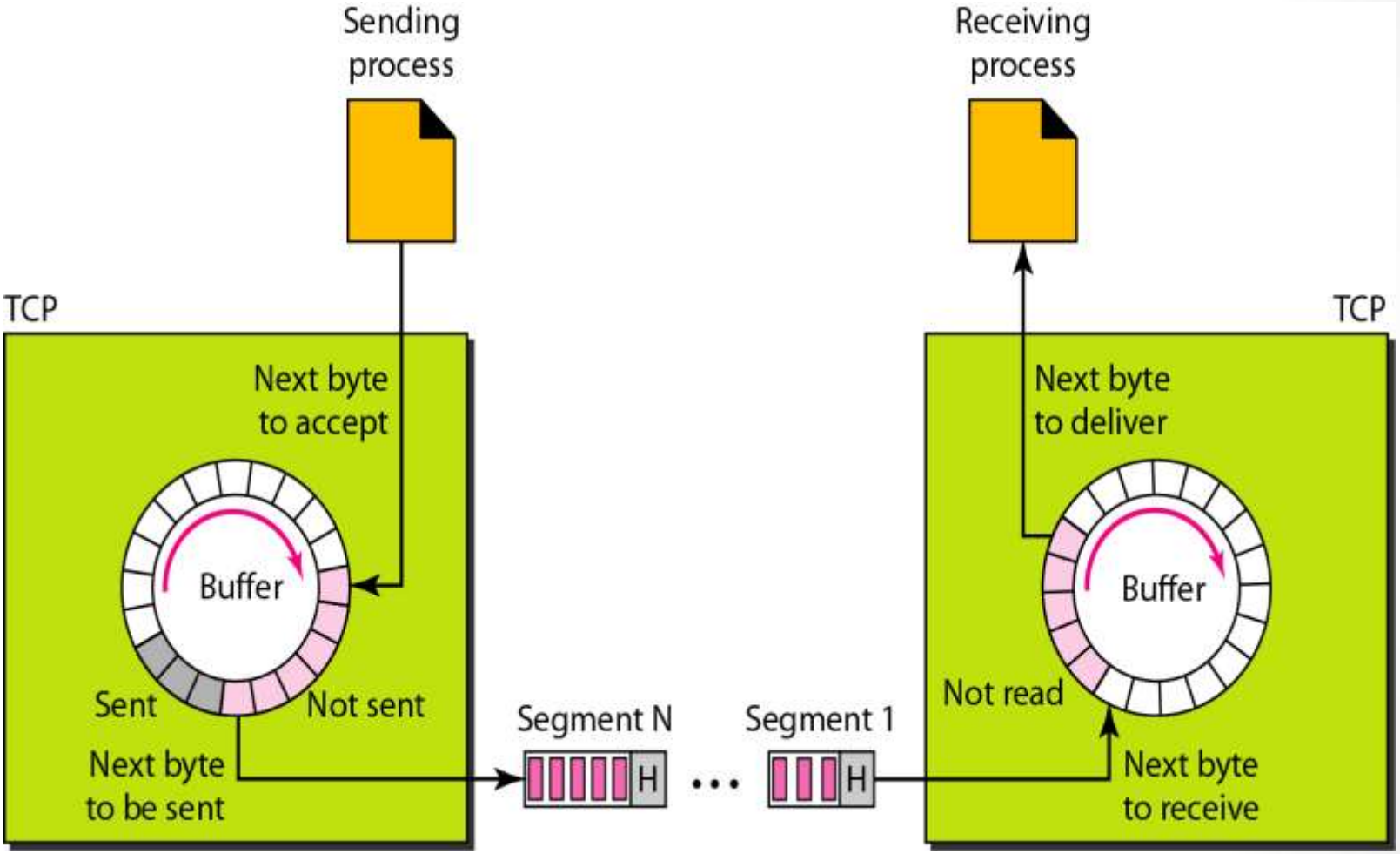
Sending and Receiving Buffers



Bytes and segments

- At the transport layer, TCP groups a number of bytes together into a packet called a segment.
- TCP adds a header to each segment and delivers the segment to the IP layer for transmission.
- In the figure, for simplicity, we show one segment carrying 3 bytes and the other carrying 5 bytes.
- In reality segments carry hundreds, if not thousands, of bytes.

TCP Segments



Full duplex service

- TCP offers full duplex service, where data can flow in both directions at the same time.
- Each TCP can then has a sending and receiving buffer, and segments are sent in both directions.

Connection-Oriented service

- TCP is a connection-oriented protocol. When a process at site A wants to send and receive data from another process at site B, the following occurs:
  - A's TCP informs B's TCP and gets approval from B's TCP.
  - A's TCP and B's TCP exchange data in both directions.
  - After both processes have no data left to send and the buffers are empty, the two TCPs destroy their buffers.

Reliable service

- TCP is a reliable transport protocol.
- It uses an acknowledgment mechanism to check the safe and sound arrival of data.

Assignment

1. Describe why application developer may choose to run an application over UDP than TCP?

   Or

1. What are the advantages of using UDP over TCP?

What are the advantages of UDP over TCP?

- The advantages of TCP over UDP are quite clear, as TCP guarantees that the sent data actually arrives, that it arrives in order and that there are no duplicates, while UDP provides none of these guarantees.
- Unlike TCP, UDP does not provide any flow and congestion control.
- On the surface, an unreliable transport protocol like UDP may not seem very worthwhile or desirable.
- But in fact, UDP can be very useful in certain situations, and it enjoys one key advantage over TCP - speed.
- The reliability features built into TCP can be expensive in terms of overhead at execution time.

Therefore, many applications find UDP well-suited for their needs, for the following reasons:

1. **No connection establishment**
2. **No connection state**
3. **Small segment header overhead**
4. **Unregulated send rate**
5. **Lower latency**
6. **Broadcast and multicast**
7. **Application flexibility**

1. No connection establishment

- While TCP uses a three-way handshake before it starts to transfer data, UDP just blasts away without any formal preliminaries.
- Thus, UDP does not introduce any delay to establish a connection.
- This feature is most useful to applications which exchange sporadic and low-volume data.

2. No connection state

- TCP maintains connection state in the end systems.
- This connection state includes receive and send buffers, congestion control parameters, and sequence and acknowledgment number parameters.
- This state information is needed to implement TCP's reliable data transfer service and to provide congestion control.
- UDP, on the other hand, does not maintain connection state and does not track any of these parameters.
- For this reason, a server devoted to a particular application can typically support many more active clients when the application runs over UDP rather than TCP.

3. Small segment header overhead

- The TCP segment has 20 bytes of header overhead in every segment, whereas UDP only has 8 bytes of overhead.
- TCP needs more header fields in order to guarantee reliability, while UDP, that gives no guarantees, does not.

4. Unregulated send rate

- TCP has a congestion control mechanism that throttles the sender when one or more links between sender and receiver becomes excessively congested.
- This throttling can have a severe impact on real-time applications, which can tolerate some packet loss but require a minimum send rate.
- On the other hand, the speed at which UDP sends data is only constrained by the rate at which the application generates data, the capabilities of the source (CPU, clock rate, etc.) and the access bandwidth to the Internet.
- We should keep in mind, however, that the receiving host does not necessarily receive all the data.
- When the network is congested, a significant fraction of the UDP-transmitted data could be lost due to router buffer overflow.
- Thus, the receive rate is limited by network congestion even if the sending rate is not constrained.

5. Lower latency

- With TCP, if a packet is lost, but the next packet makes it through, the kernel will withhold that packet until the earlier packet can be re-sent.
- This is because TCP is a guaranteed, in-order, stream protocol.
- This means that "fresh" data will sit in the kernel, becoming "stale", while waiting for the TCP timeout to be retransmitted (a minimum of 3 seconds for a lost packet).
- This is why UDP is usually better for games, voice conferencing, and other low-latency applications.

6. Broadcast and multicast

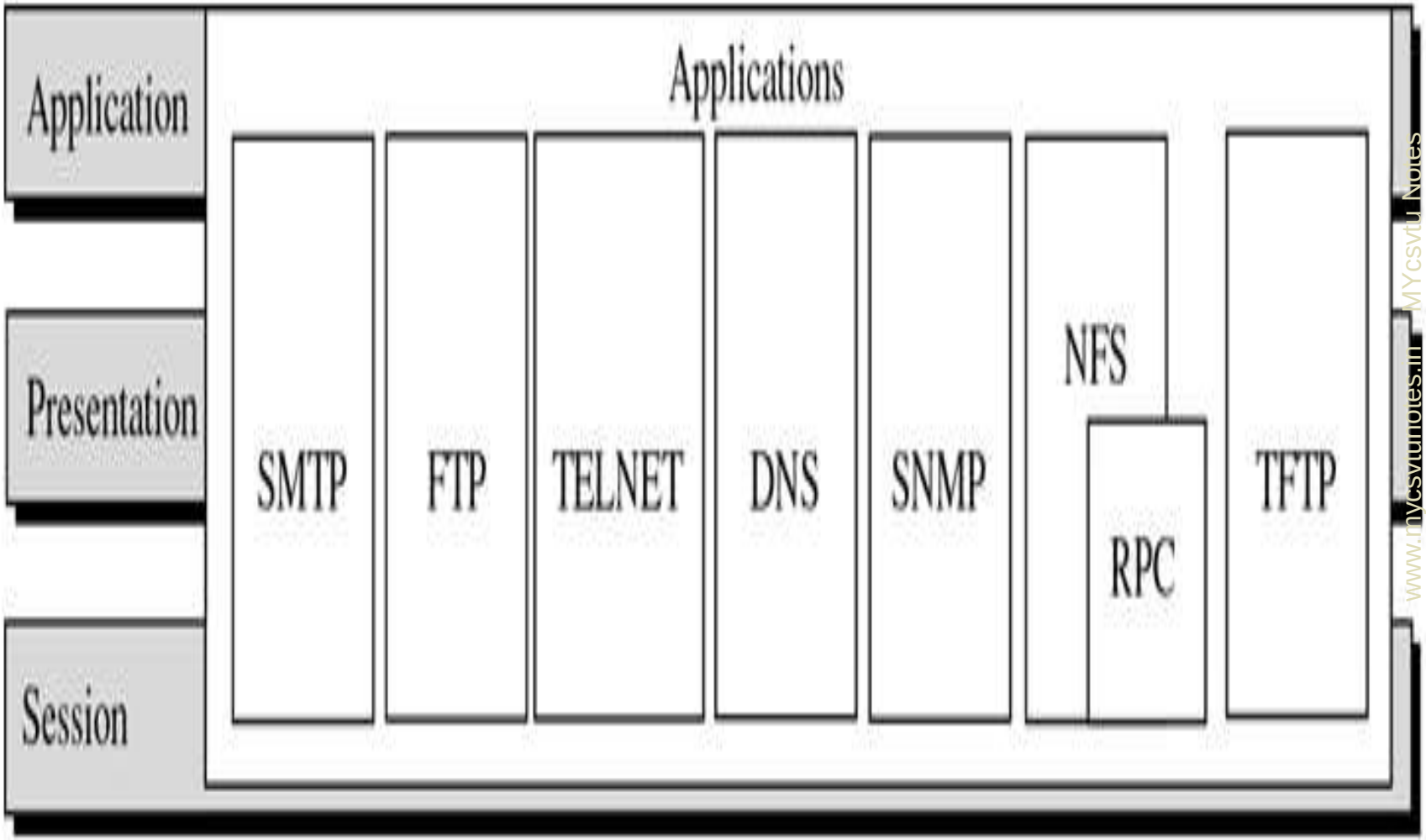
- Being a connection-oriented protocol, TCP does not support broadcast and multicast.
- Therefore, applications that require this kind of service will have to use UDP as a transport protocol.

7. Application flexibility

- The fact that UDP lacks built-in reliability mechanisms can be considered an advantage from the application designer's point of view.
- Building reliability directly into the application allows the application to "have its cake and eat it too".
- That is, application processes can communicate reliably without being constrained by the transmission rate constraints imposed by TCP's congestion control mechanism.
- Application-level reliability also allows an application to tailor its own application-specific form of error control.

- For example, an interactive real-time may occasionally choose to retransmit a lost message, provided that round trip network delays are small enough to avoid adding significant playout delays.
- In fact, many of today's proprietary streaming applications do just this: they run over UDP, but they have built acknowledgements and retransmissions into the application in order reduce packet loss.

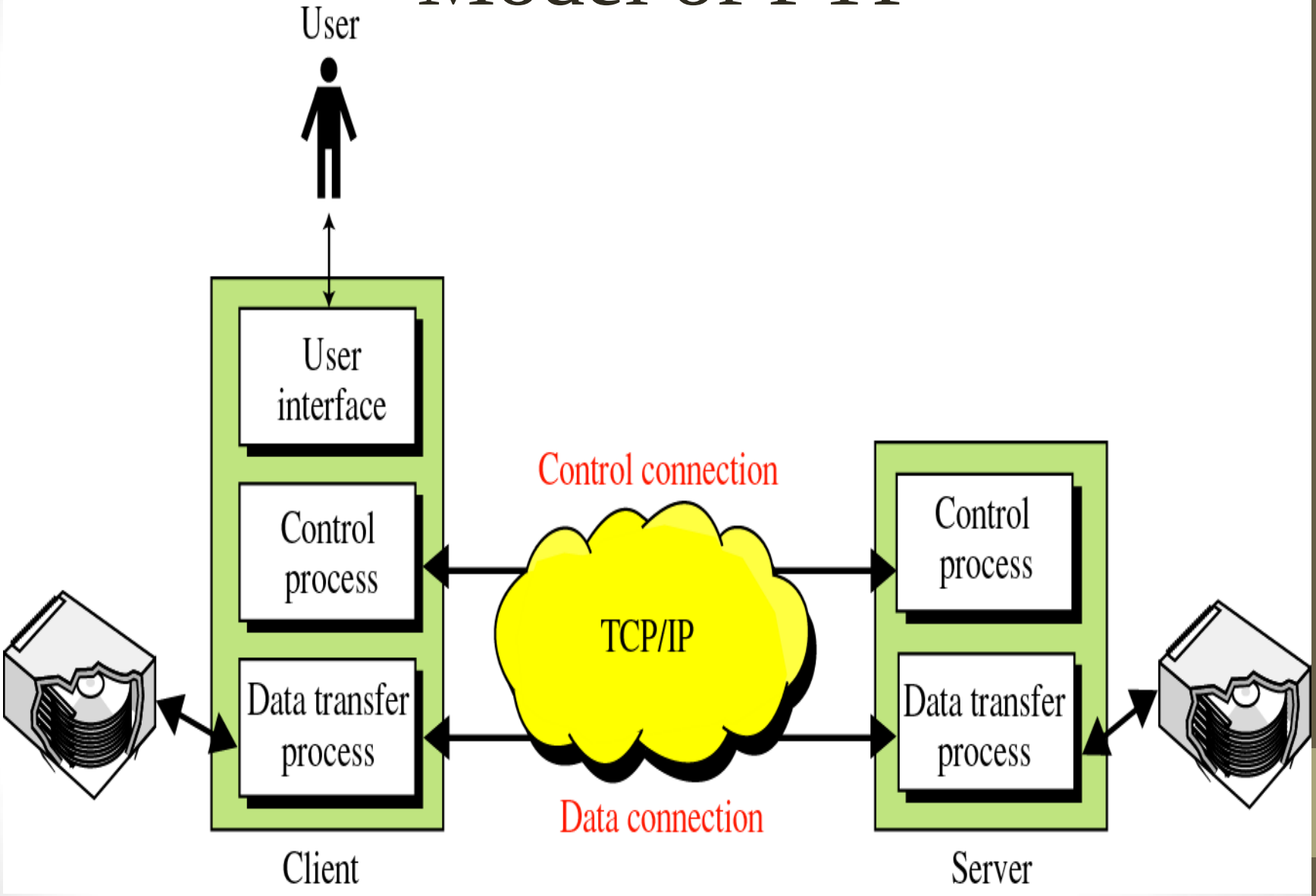
FTP, SMTP,HTTP



FTP

- It is the standard mechanism provided by the Internet for copying a file from one host to another.
- FTP establishes two connections between client and the server.
- One connection is used for data transfer, the other for control information.
- FTP uses two well-known TCP ports: Port 21 is used for the control connection, and port 20 is used for the data connection.

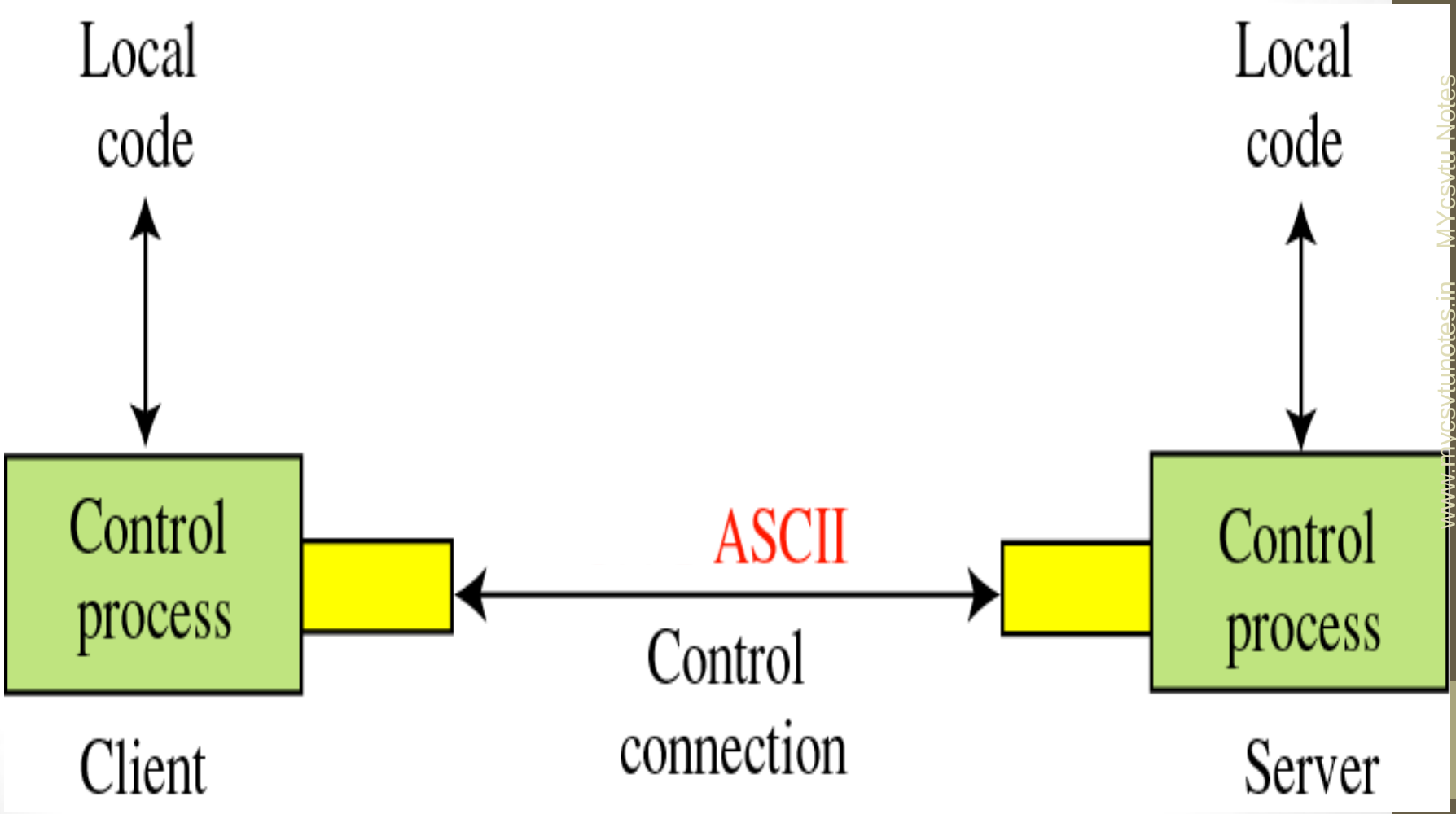
Model of FTP



- The client has three components:
  - User interface
  - Client control process
  - Client data transfer process
- The server has two components:
  - The sever control process and
  - the server data transfer process
- The control connection is made between the control processes.
- The data connection is made between the data transfer processes.
- The **TCP/IP** is the set of communications protocols used for the Internet and other similar networks. It is named from two of the most important protocols in it: the TCP and the IP which were the first two networking protocols defined in this standard.

- When a user starts an FTP session, the control connection opens.
- While the control connection is open, the data connection can be opened and closed multiple times if several files are transferred.

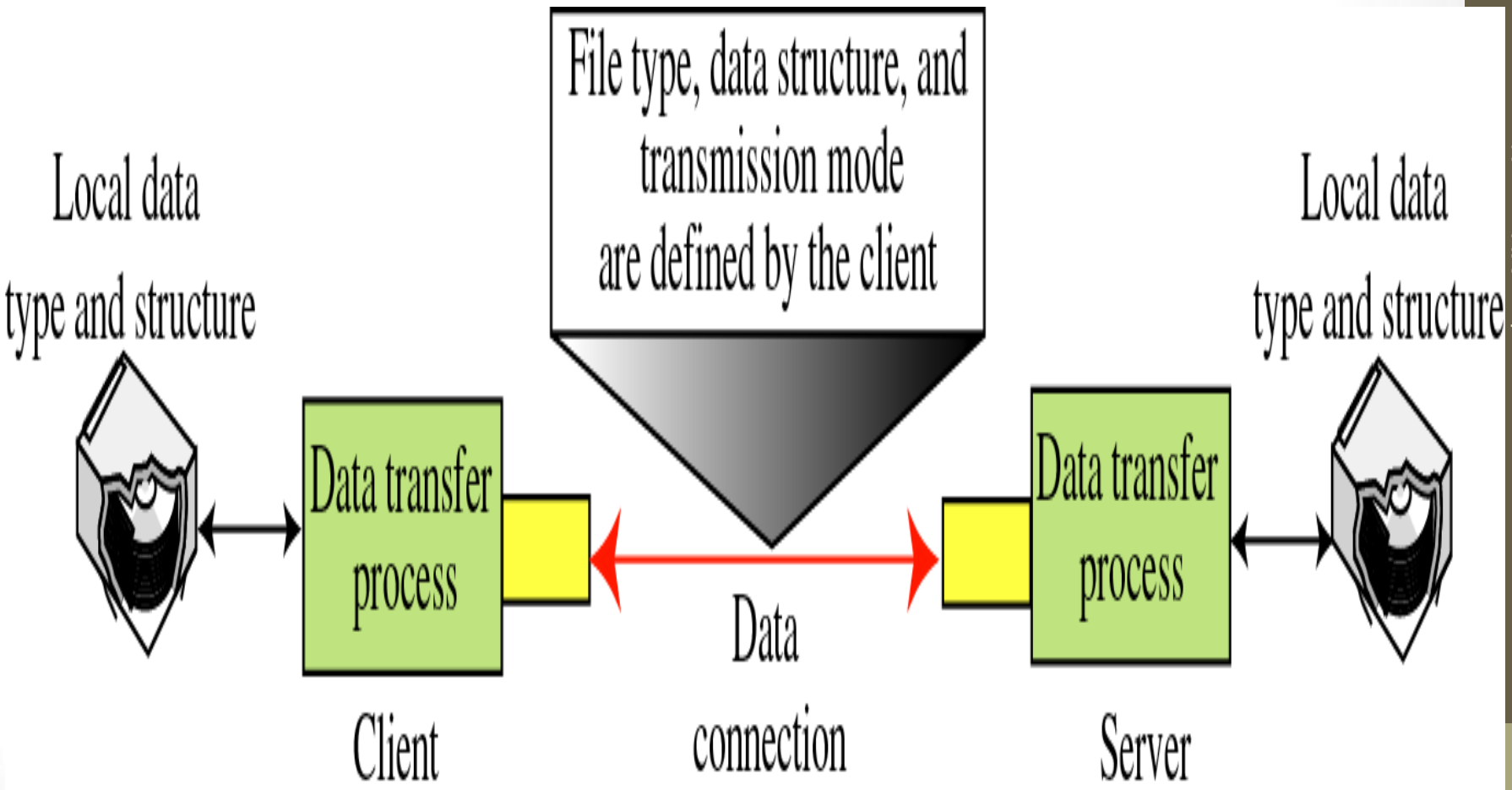
Communication over control connection



Communication over control connection

- FTP uses a set of ASCII characters to communicate across the control connection.
- Communication is achieved through commands and response.
- One command is sent at a time.
- Each command or response is only of one short line.
- Each line is terminated with a two character end of line token and line feed.

Communication over data connection



Communication over data connection

- The purpose of implementing a data connection is to transfer a file. For this the client has to define the following:
  - Type of file being transferred
  - Structure of data
  - Transmission mode

File Type

- FTP can transfer one of the following file types across the data connection:
  - ASCII File
  - EBCIDIC File
  - Image File

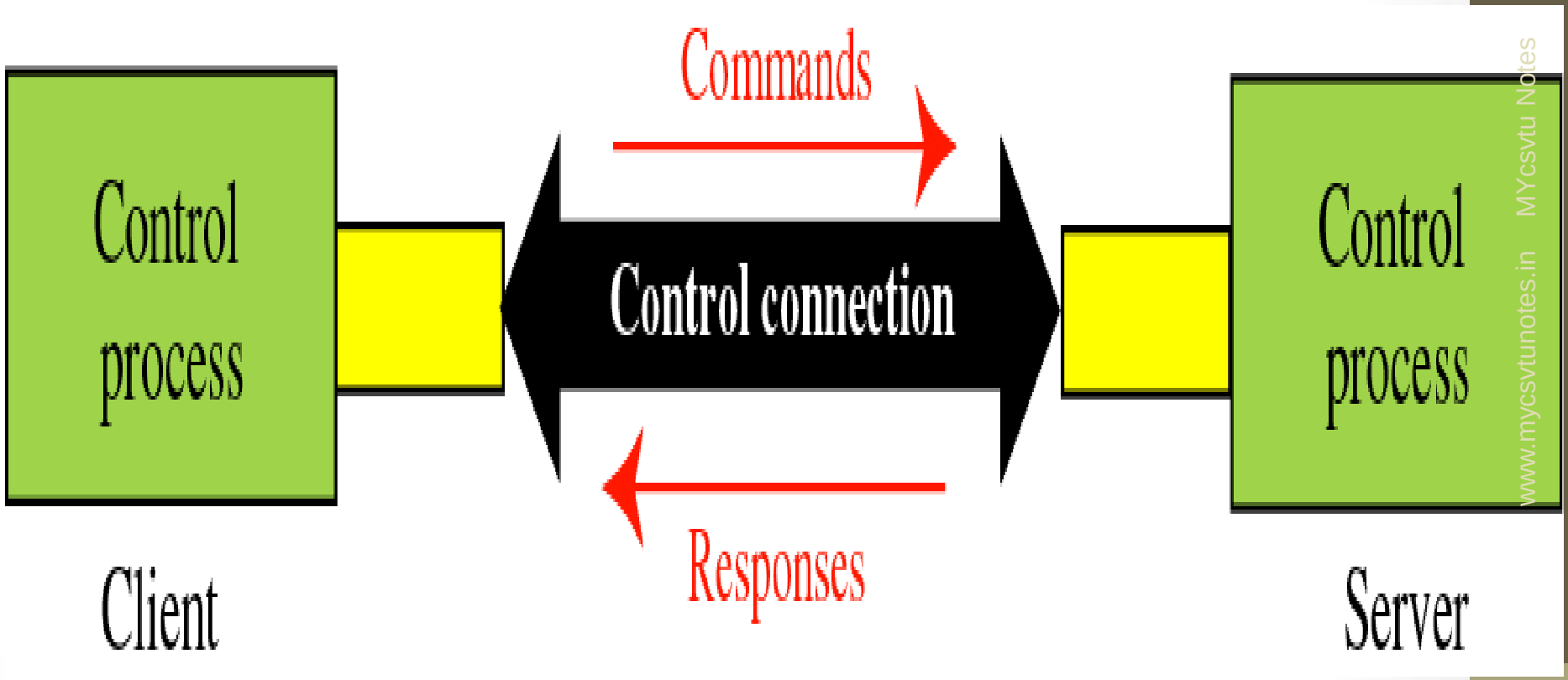
Data Structure

- **File structure**: The file has no structure. It is a continuous stream of bytes.
- **Record structure**: The file is divided into records. This is used only with the text files.
- **Page structure:** The file is divided into pages with each page having a page number and page header. These pages can be stored or accessed randomly or sequentially.

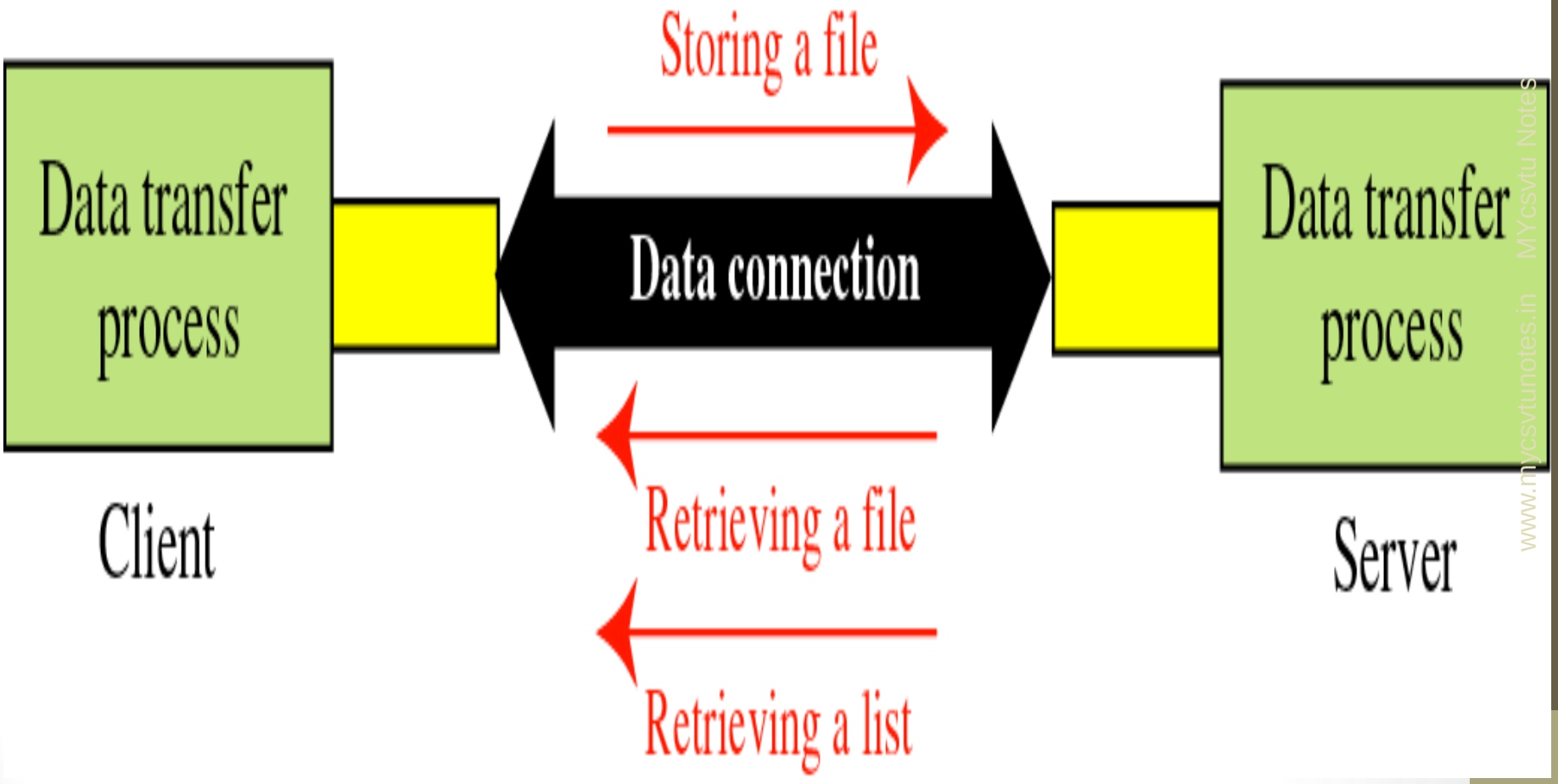
Transmission Mode

- **Stream Mode**: the data is delivered from FTP to TCP in the form of continuous stream of bytes. TCP chops this data into segments of appropriate size.
- **Block Mode**: the data is delivered from FTP to TCP in blocks. Each such block is preceded by a 3 byte header.
- **Compressed Mode**: for big files the data can be compressed.

File Transfer



File Transfer



File Transfer

- File transfer takes place over the data connection under the control of the commands sent over the control connection.
- But file transfer in FTP means one of the following
  I. Retrieving a file: a file is copied from server to client
  II. Storing a file: a file can be copied from client to the server
  III. A server sends a list of directory or file names to the client. FTP treats such a list of directory as a file.

FTP commands to connect to a remote host

Command	Explanation
Open	Select the remote host and initiate login session
User	Identify the remote user ID
Pass	Authenticate the user
Site	Send the information to the remote host

FTP commands to transfer files

Command	Explanation
Get	Copy a file from remote host to local host
M get	Copy multiple files from the remote host to local host
Put	Copy a file from local host to remote host
M put	Copy multiple files from the local host to remote host

FTP commands to terminate session

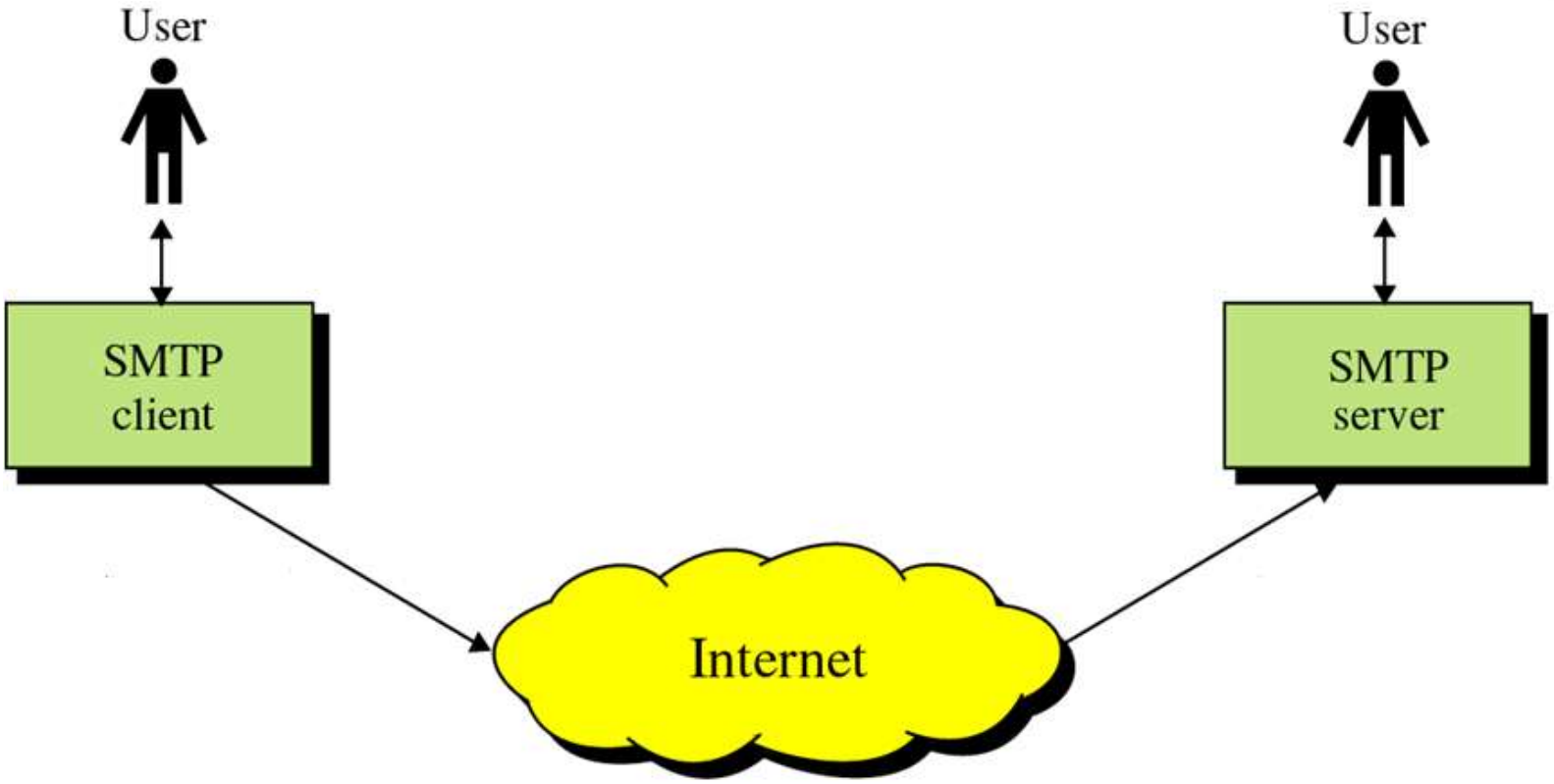
Command	Explanation
Quit	Disconnect from the remote host and terminate FTP
Close	Disconnect from the remote host but leave FTP client running

Simple Mail Transfer Protocol (SMTP)

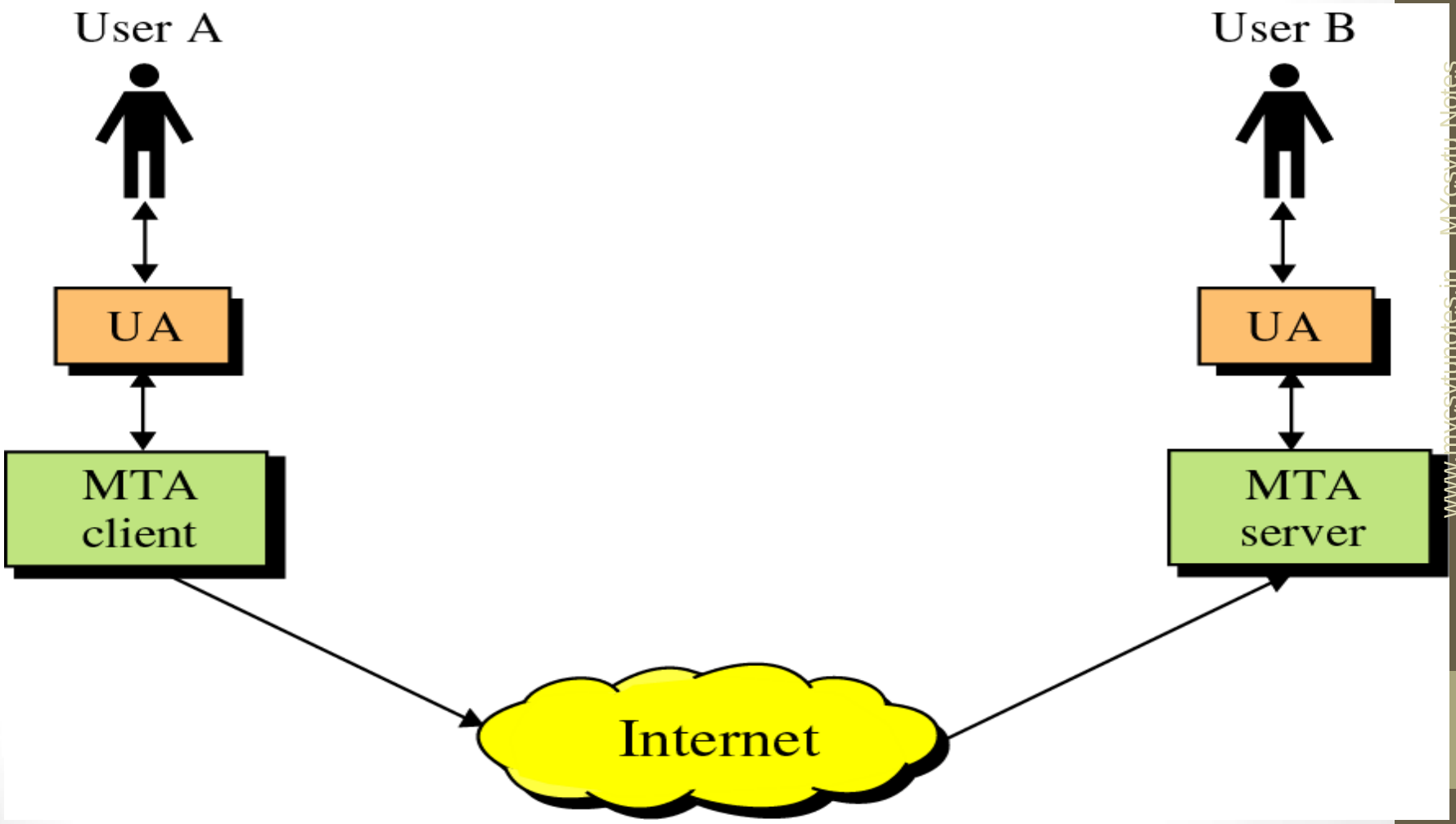
SMTP

- One of the most popular network services is electronic mail(e-mail).
- The protocol that supports e-mail on the Internet is called Simple Mail Transfer Protocol.
- It is a system for sending messages to other computer users based on email addresses.
- SMTP provides for mail exchange between users on the same or different computers and supports:
  - Sending a single message to one or more recipients.
  - Sending messages that include text, voice, video, or graphics.

SMTP concept



SMTP components: UAs and MTAs



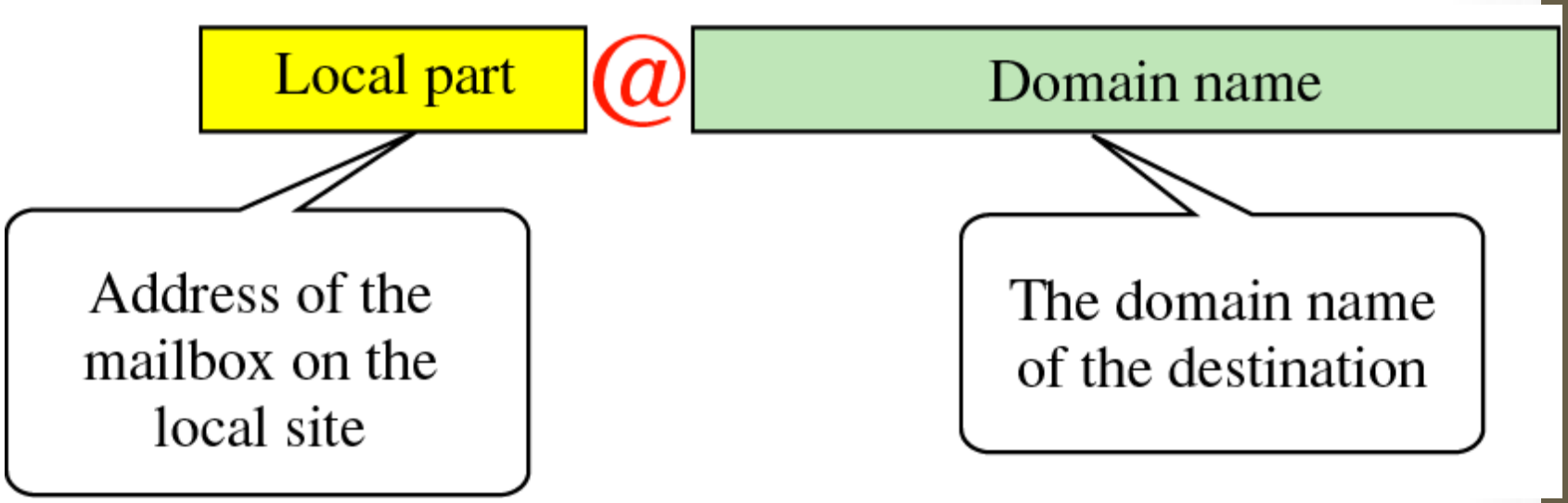
User Agent (UA)

- The UA is normally the program used to send and receive mail.
- User agent
  - Composing message
  - Reading message
  - Replying message
  - Forwarding message

Address

- To deliver mail, a mail handling system must use a unique addressing system.
- The addressing system used by SMTP consists of two parts:
- A local part: the local part defines the name of a special file, called the user mailbox, where all of the mail received for a user is stored for retrieval by the user agent.
- A domain name: an organization usually selects one or more hosts to receive and send e-mail; they are sometimes called mail exchangers.

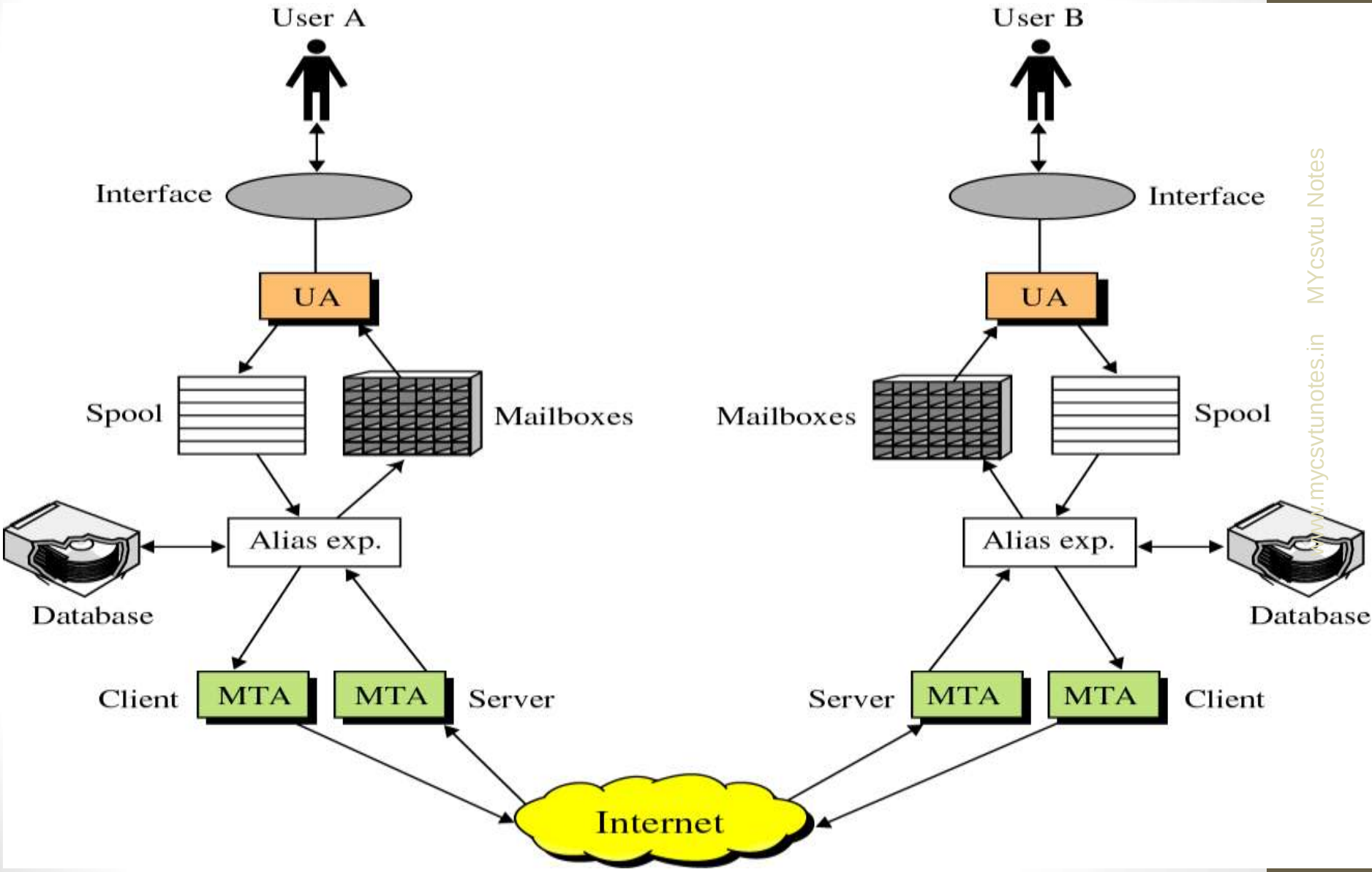
E-mail address



Mail Transfer Agent (MTA)

- The actual mail transfer is done through mail transfer agents.
- To send mail, a system must have a client MTA, and to receive mail, a system must have a server MTA.

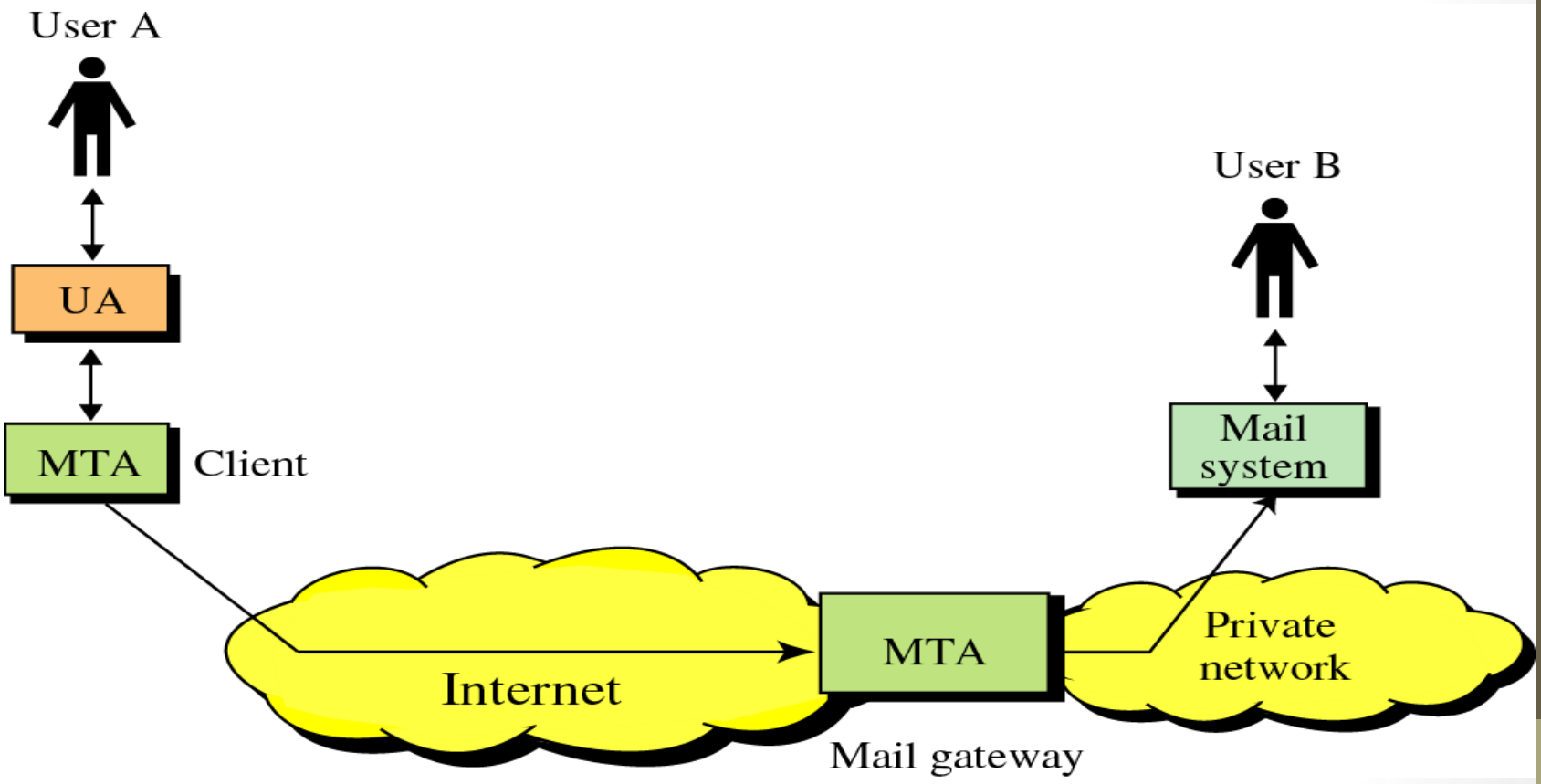
The process of sending and receiving e-mail



Mail gateway

- The system that do not use the TCP/IP protocol suite to send e-mail to users on other sites. This is accomplished through the use of a mail gateways.
- It is a MTA that can receive mail prepared by a protocol other than SMTP and transform it to SMTP format before sending it.
- It can also receive mail in SMTP format and change it to another format before sending it.

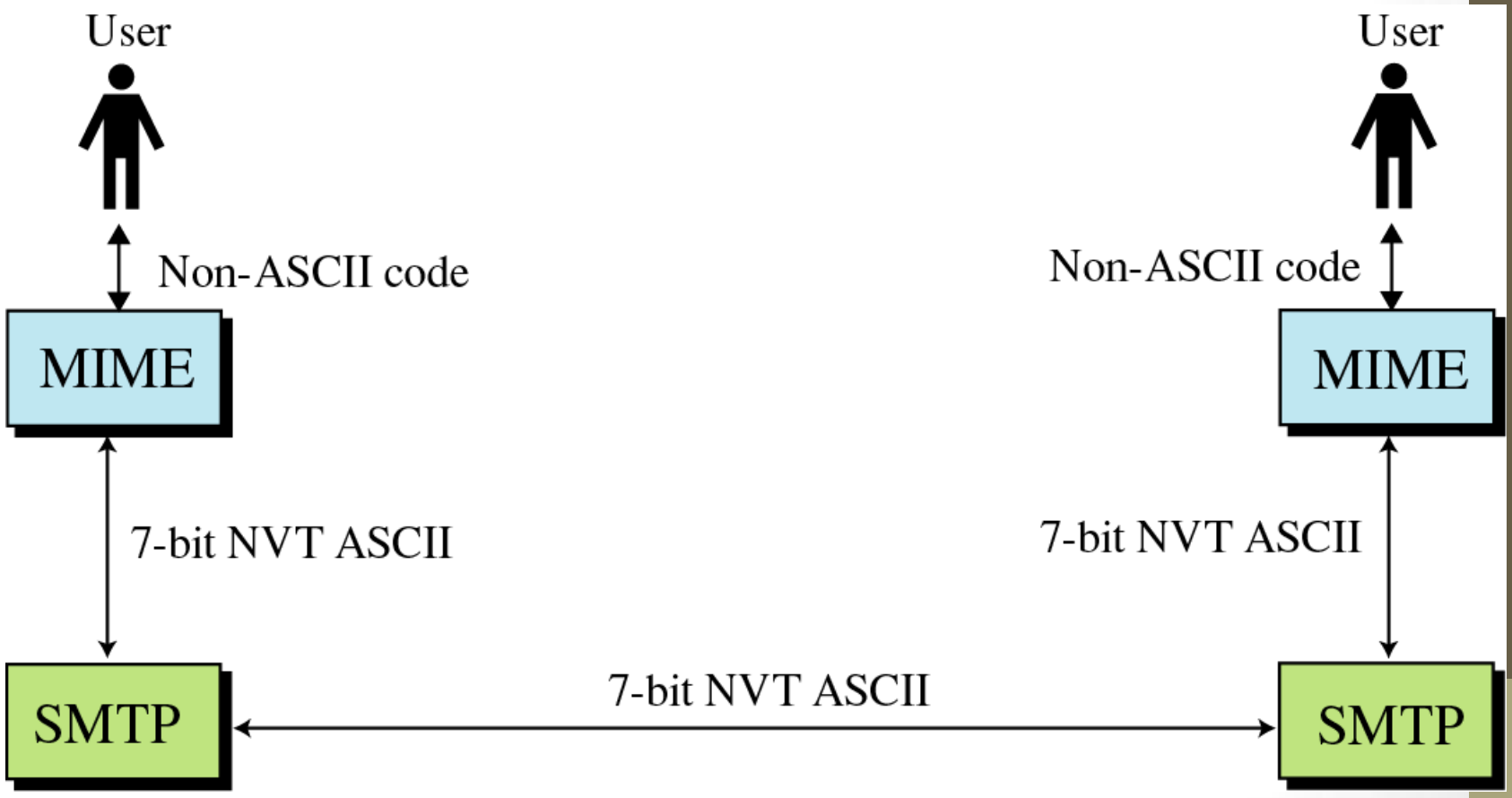
Mail gateway



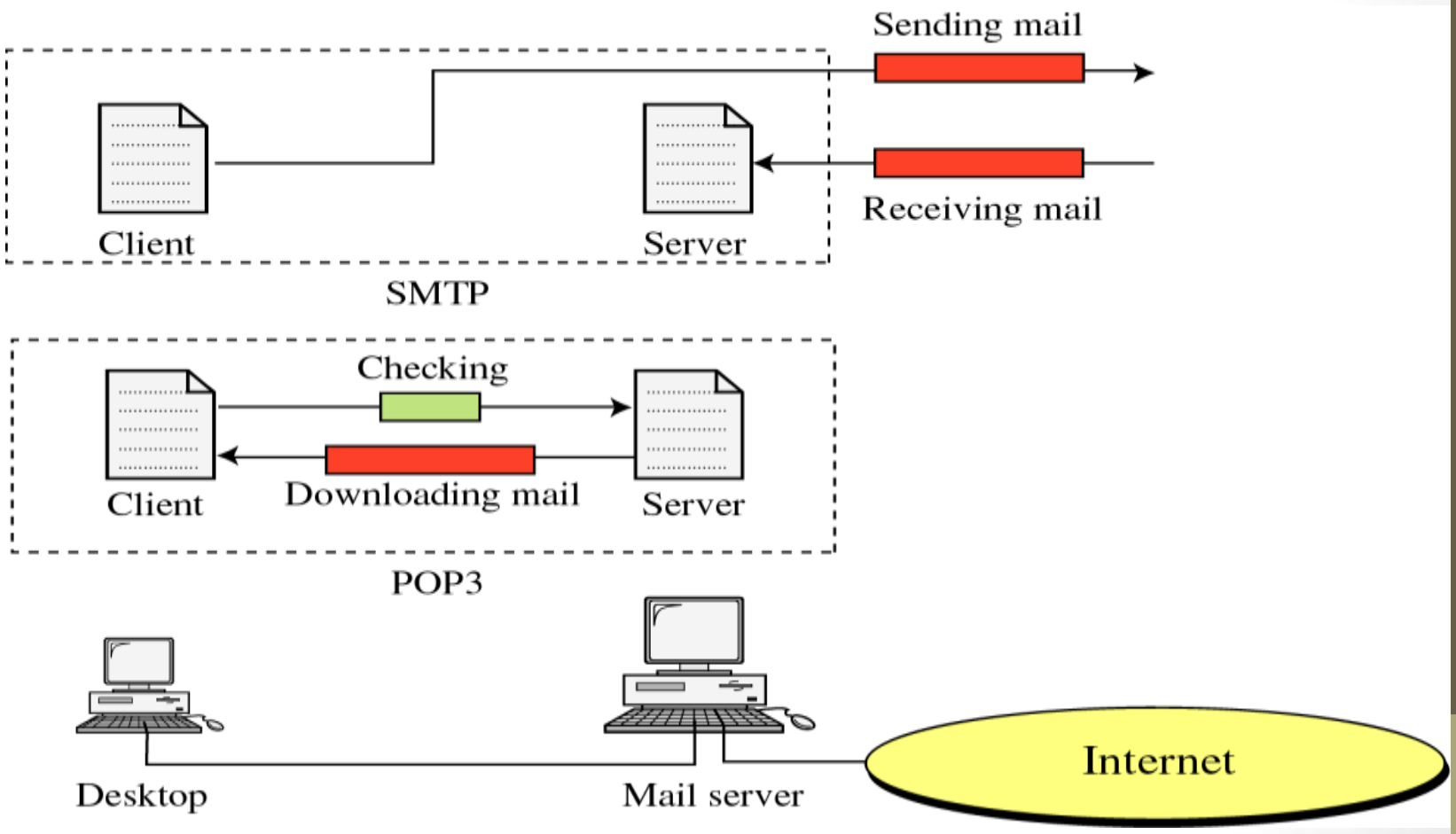
MIME

- SMTP can send messages only in NVT seven-bit ASCII format. Also, it cannot be used to send binary files or to send video or audio data.
- Multipurpose Internet Mail Extension(MIME) is a supplementary protocol that allows non-ASCII data to be sent through SMTP.
- MIME is not a mail protocol and cannot replace SMTP, it is only extension to SMTP.
- MIME transforms non-ASCII data at the sender site to NVT ASCII data and delivers it to the client SMTP to be sent through the Internet.
- The server SMTP at the receiving side receives the NVT ASCII data and delivers it to MIME to be transformed back to the original data.

MIME



POP3 and SMTP



POP3 and SMTP

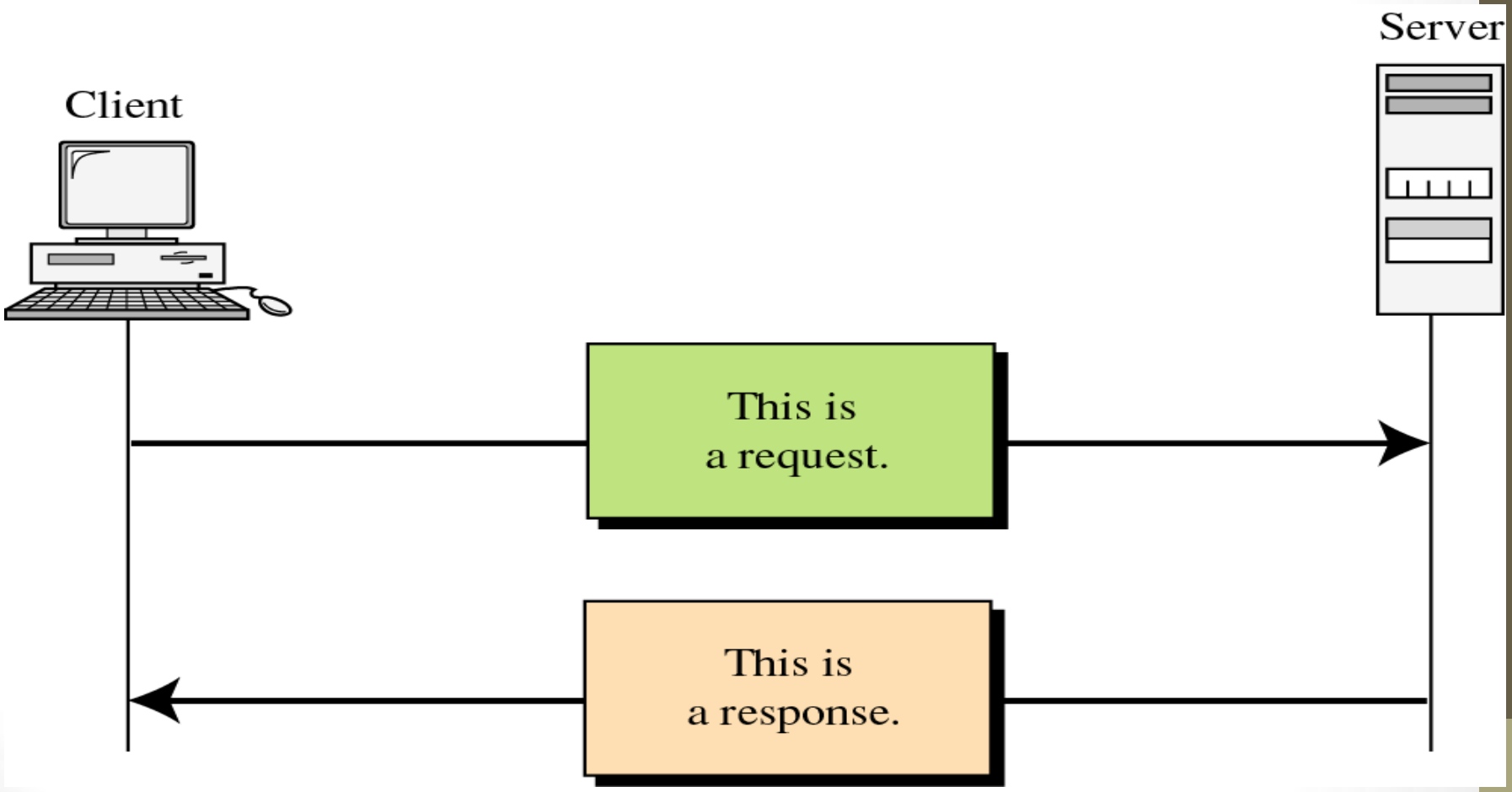
- SMTP expects the destination host, the mail server receiving the mail, to be on-line all the time; otherwise, a TCP connection cannot be established.
- For this reason, it is not practical to establish an SMTP session with a desktop computer because desktop computers are usually powered down at the end of the day.
- In many organizations, mail is received by an SMTP server that is always on-line. This SMTP server provides a mail-drop service. The server receives the mail on behalf of every host in the organization. Workstations interact with the SMTP host to retrieve messages by using a client-server protocol such as POST Office Protocol (POP3).

Hypertext Transfer Protocol (HTTP)

Introduction

- HTTP is used mainly to access data on WWW.
- This protocol transfers data in the form of plaintext, hypertext, audio, video etc.
- The function of HTTP like a combination of FTP and SMTP. It uses services of TCP.
- It uses only one TCP connection (port 80). There is no separate control connection.
- Only the data transfer takes place between the client and server.
- The data transfer in HTTP is similar to SMTP.

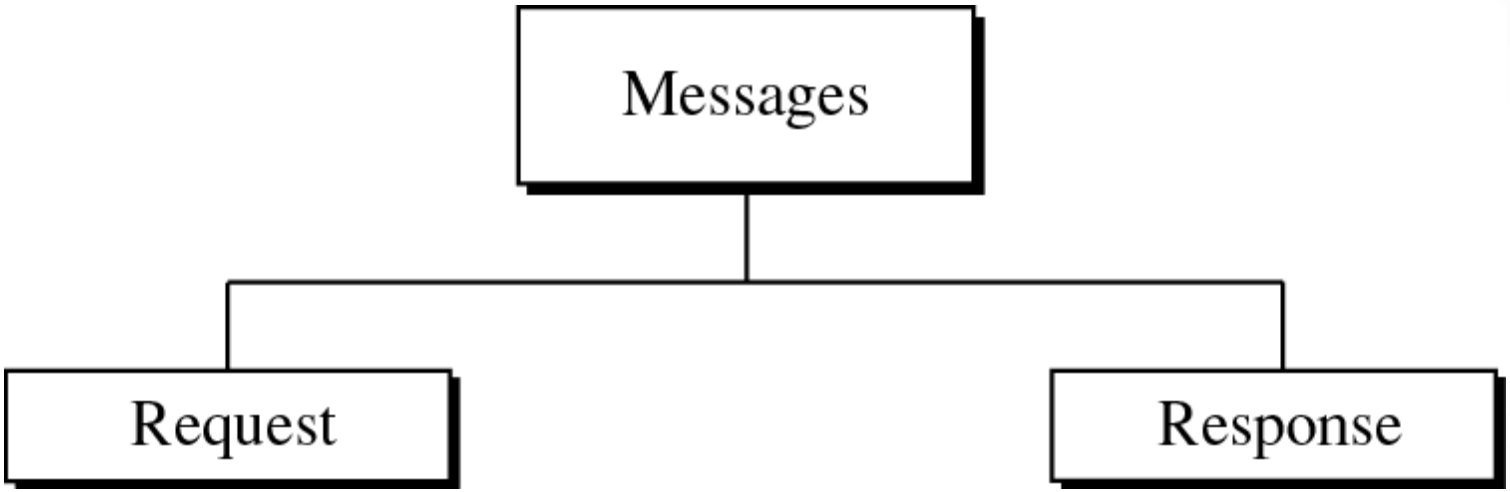
HTTP transaction



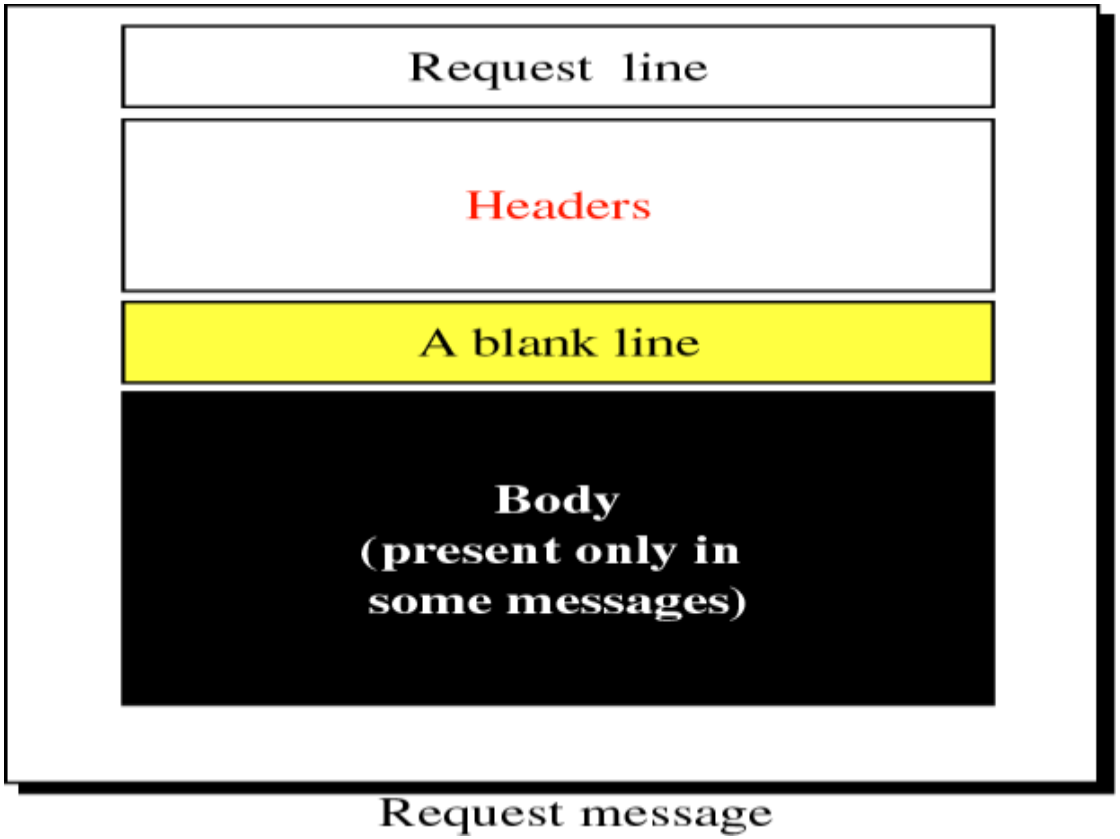
Principle of HTTP operation

- A client send a request.
- The server sends a response.
- The request and response messages carry data in the form of a letter.
- The client initializes the transaction by sending a request message and the server replies it by sending a response.

Message Types



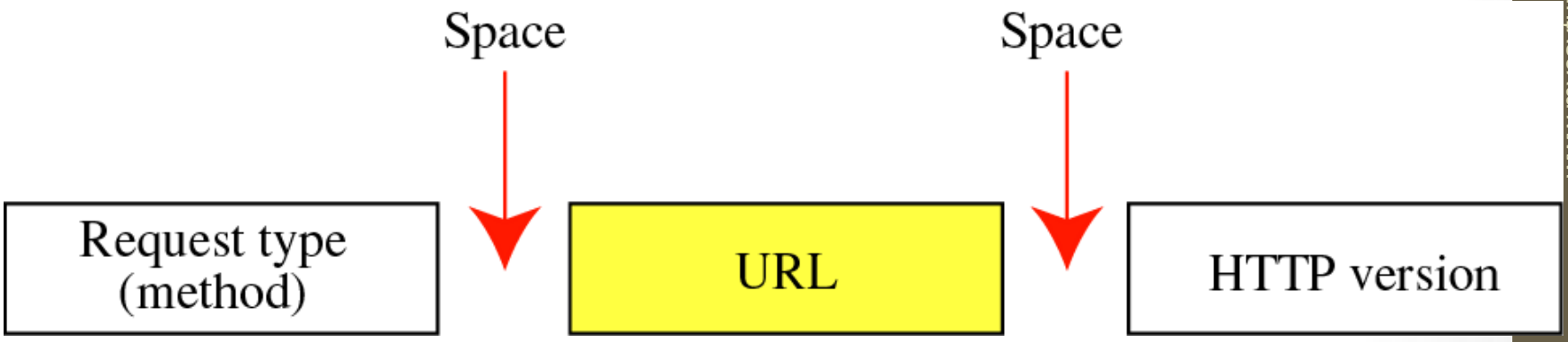
Request Message



- It consists of request line, headers and sometimes a body.

Request line format

- The request line is used for defining the request type, resource (URL) and HTTP version.



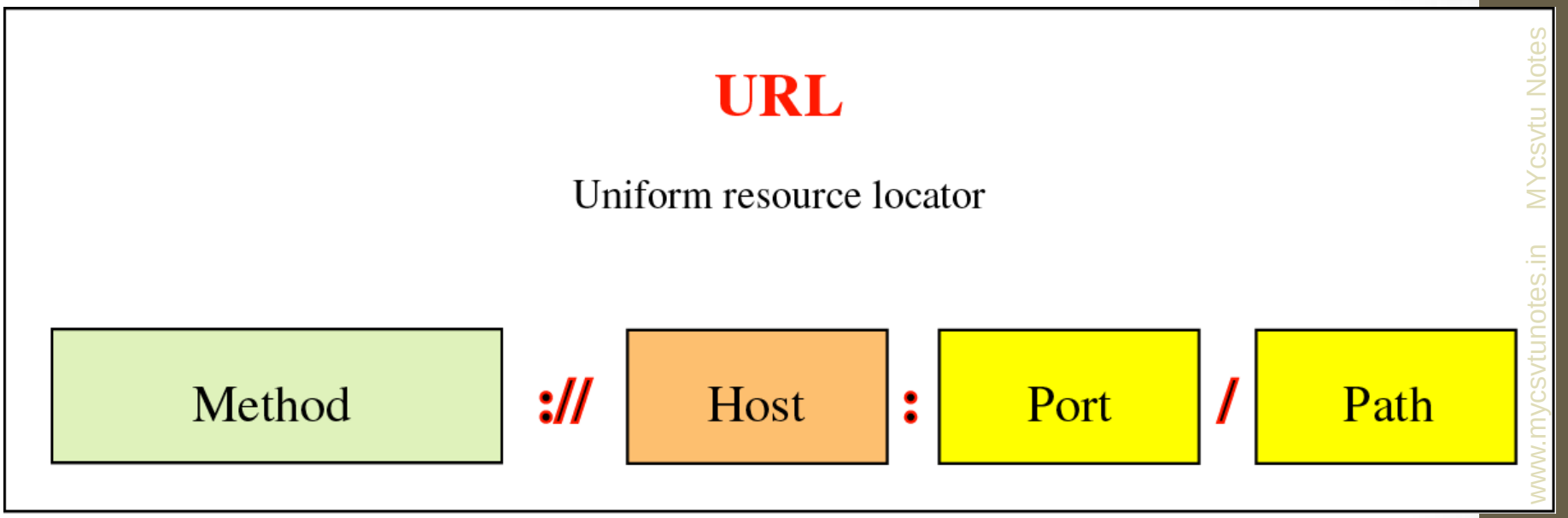
Request Type (Method)

- **GET:** this method is used when the client wants to retrieve a document from the server. The address from where this document is to be obtained is defined in the URL.
- **HEAD:** this method is used when the client wants some information about a document but not the document itself.
- **POST:** this is used by the client to provide some information to the server.
- **PUT**: this is used by the client for providing a new or replacement document to be stored on the server.
- **PATCH**: this is similar to PUT. But there is one change. The request contains a list of differences which should be implemented in the existing file.

Request Type (Method) Conti…

- **COPY**: this method is used to copy a file to another location.
- **MOVE**: this method is used for moving a file to another location.
- **DELETE**: it is used for moving a document on the sever.
- **LINK:** it is used for creating a link or a link from a document to another location. This location of the file is specified in the URL request line and the location of destination is specified in the entity header.
- **UNLINK**: it is used for deleting the links created by the LINK method.
- **OPTION**: it is used by the client to ask the server about various available options.

Uniform Resource Locator



Uniform Resource Locator

- The client accessing a web page needs an address.
- The HTTP uses the URL to facilitate the access of any document distributed over the world.
- The URL defines
  - **Method**: it is the protocol used.
  - **Host**: host is the computer where the required information is located. The name of the computer begins with WWW but this is not mandatory.
  - **Port**: URL optionally contain the server's port number. If the port is included then it should be inserted between host and path and it should be separated by a colon.
  - **Path:** it is the name of the file where the information is located.

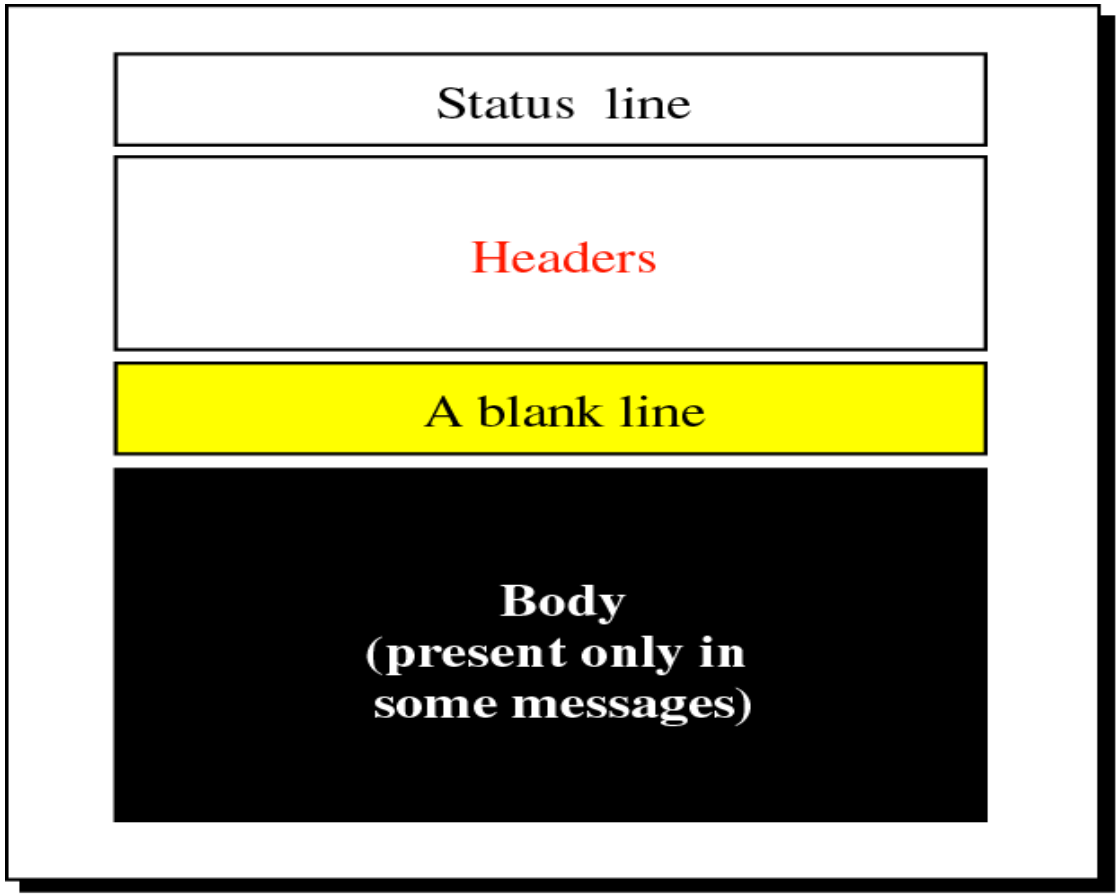
URL Example

- http: // www.w4.org/hypertext/www/project.html

HTTP version

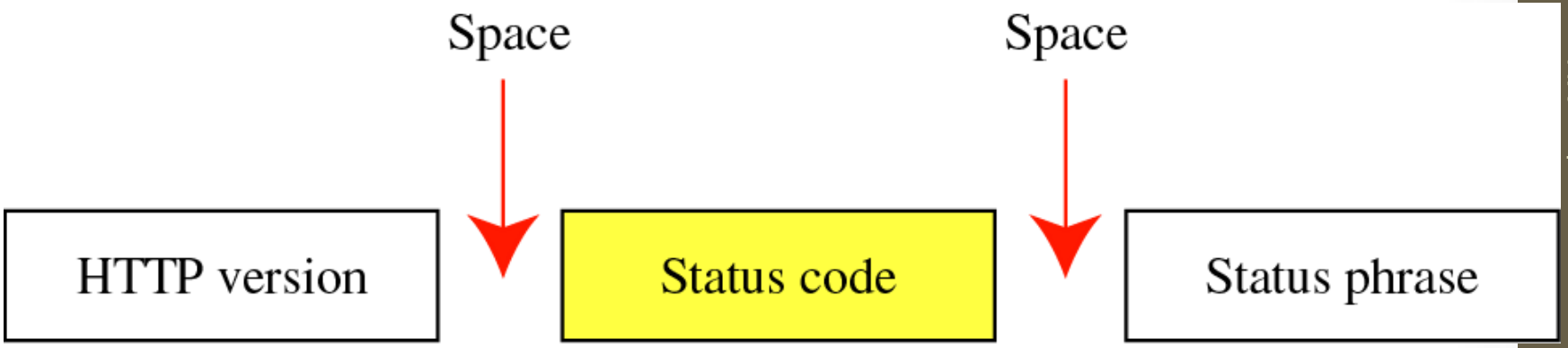
- The latest version of HTTP is 1.1 but the versions 0.9 and 1 are also used.

Response Message



Response message

Status line format

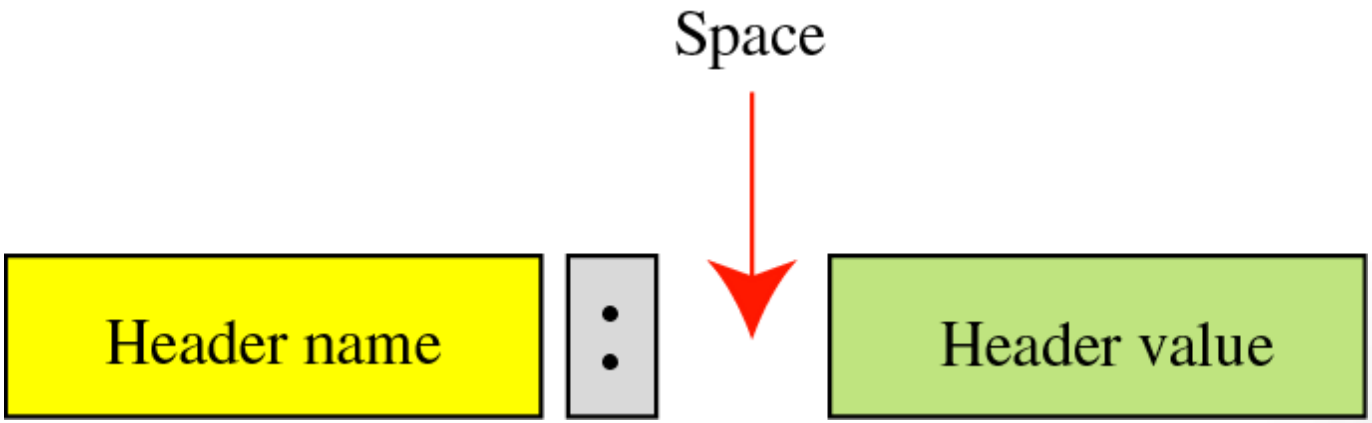


Status line

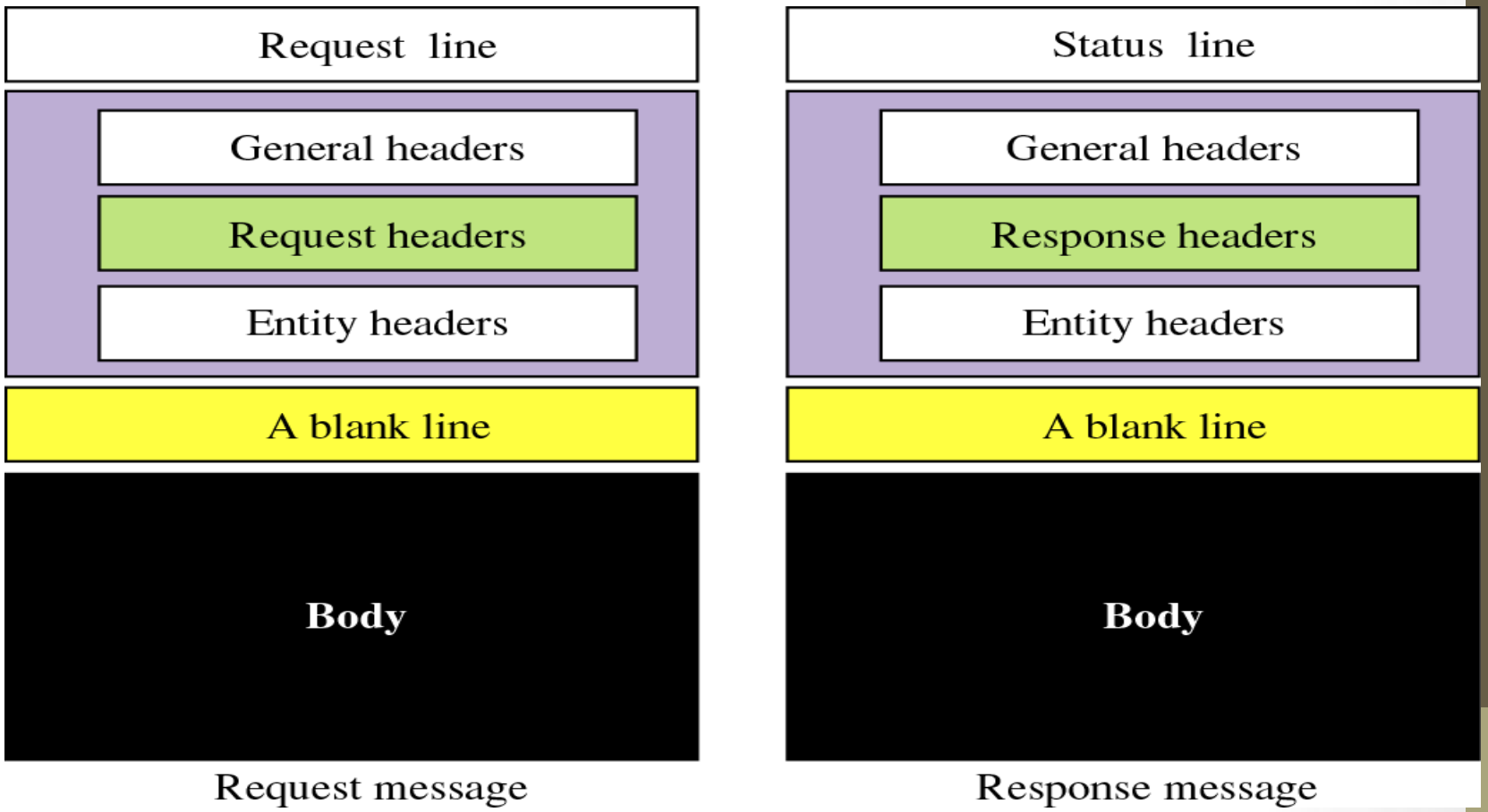
- The status line is used for defining the status of the response message.
- It consists of HTTP
  - **Version**: this field is same as the corresponding field in the request line.
  - **Status code**: this field is similar to those in FTP and SMTP protocols. It contains three digits.
  - **Status phrase**: it explains the status code in the text form.

Headers

- Headers in the response message are used for exchanging additional information between the client and server.
- The header can be one line or more lines. The header line consists of a header name, a colon, a space and a header value.



Comparison of request and response message



Domain Name System (DNS)

Introduction

- For communication to take place successfully, the sender and receiver both should have address and they should be known to each other.
- However, people prefer to use names instead of numeric addresses.
- Therefore, we need a system that can map a name to an address or an address to a name. for this an application program needs service of another entity.
- This entity is an application program called DNS. Note that DNS is not used directly by the user. It is used by another application programs for carrying out the mapping.

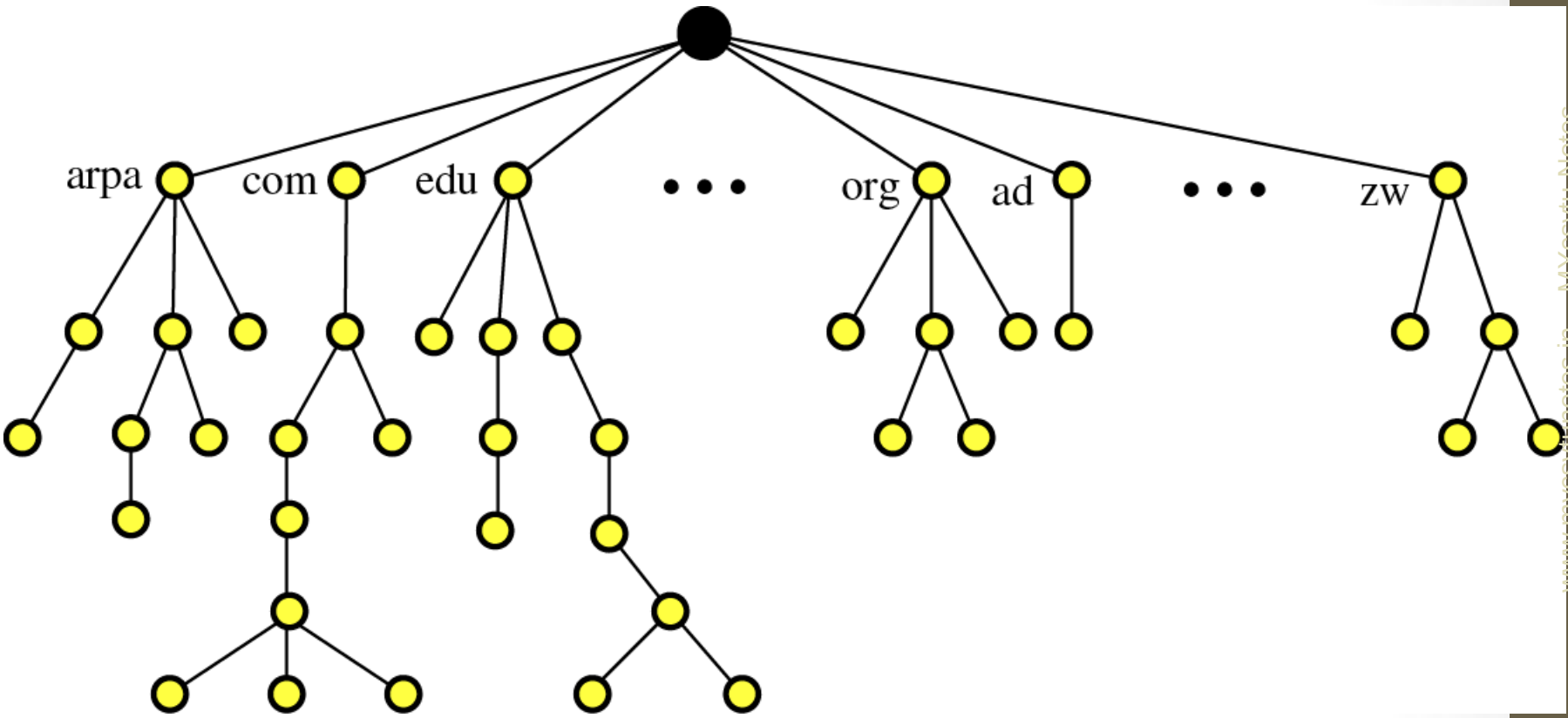
How DNS works?

- To map a name onto an IP address, an application program calls a library procedure called the resolver.
- The name is passed on to the resolver as a parameter.
- The resolver sends a UDP packet to a local DNS server which looks up the name and returns the corresponding IP address to the resolver.
- The resolver then sends this address to the caller. Then the program can establish a TCP connection with the destination or sends in the UDP packets.

The DNS Name Space

- Conceptually the Internet has been divided into hundreds of top level domains.
- Each domain covers many hosts.
- Each domain is divided into several sub-domains and they are further partitioned.
- These domains can be represented by a tree.
- The top levels domains are of two types namely generic and countries.

Domain Name Space

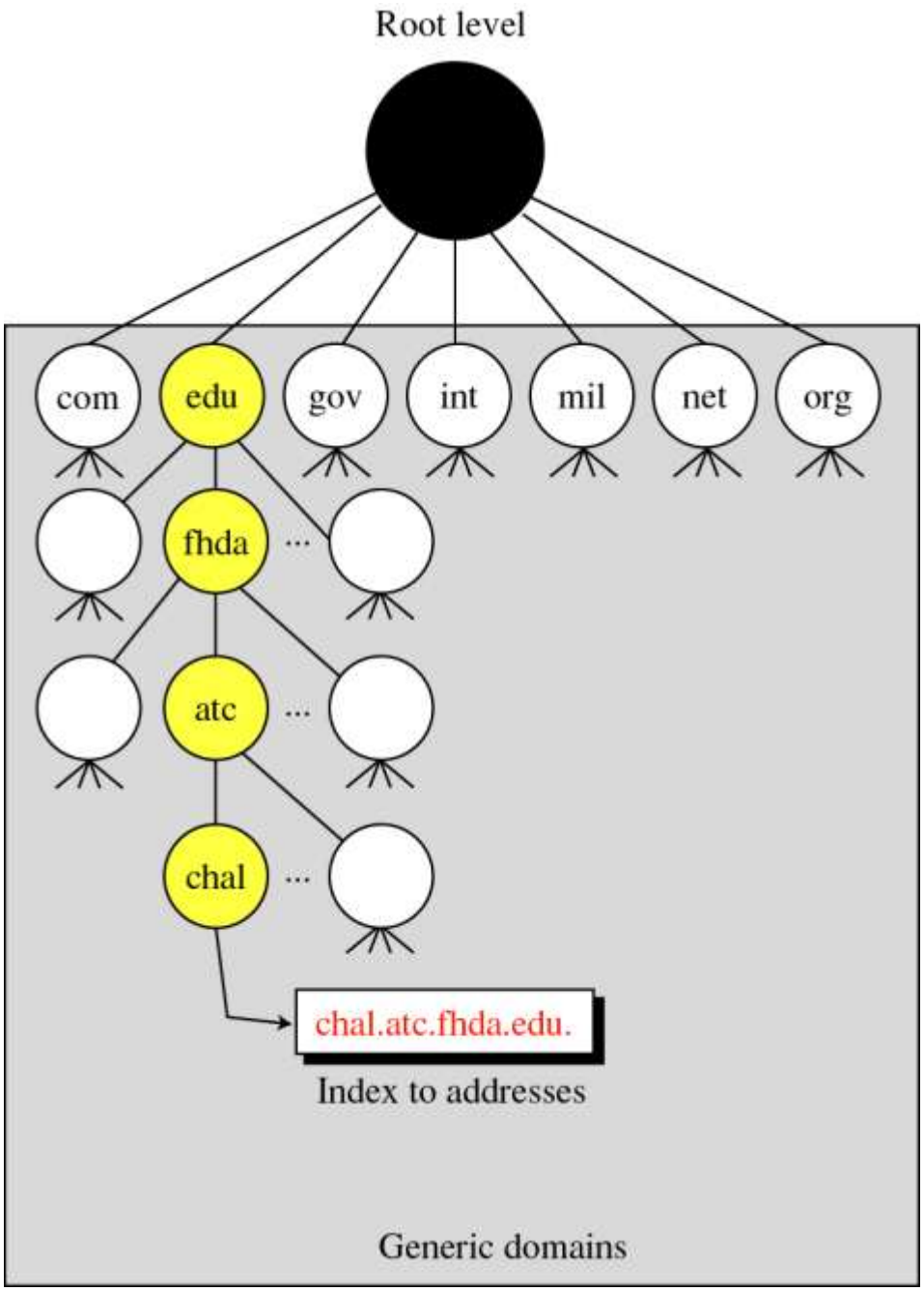


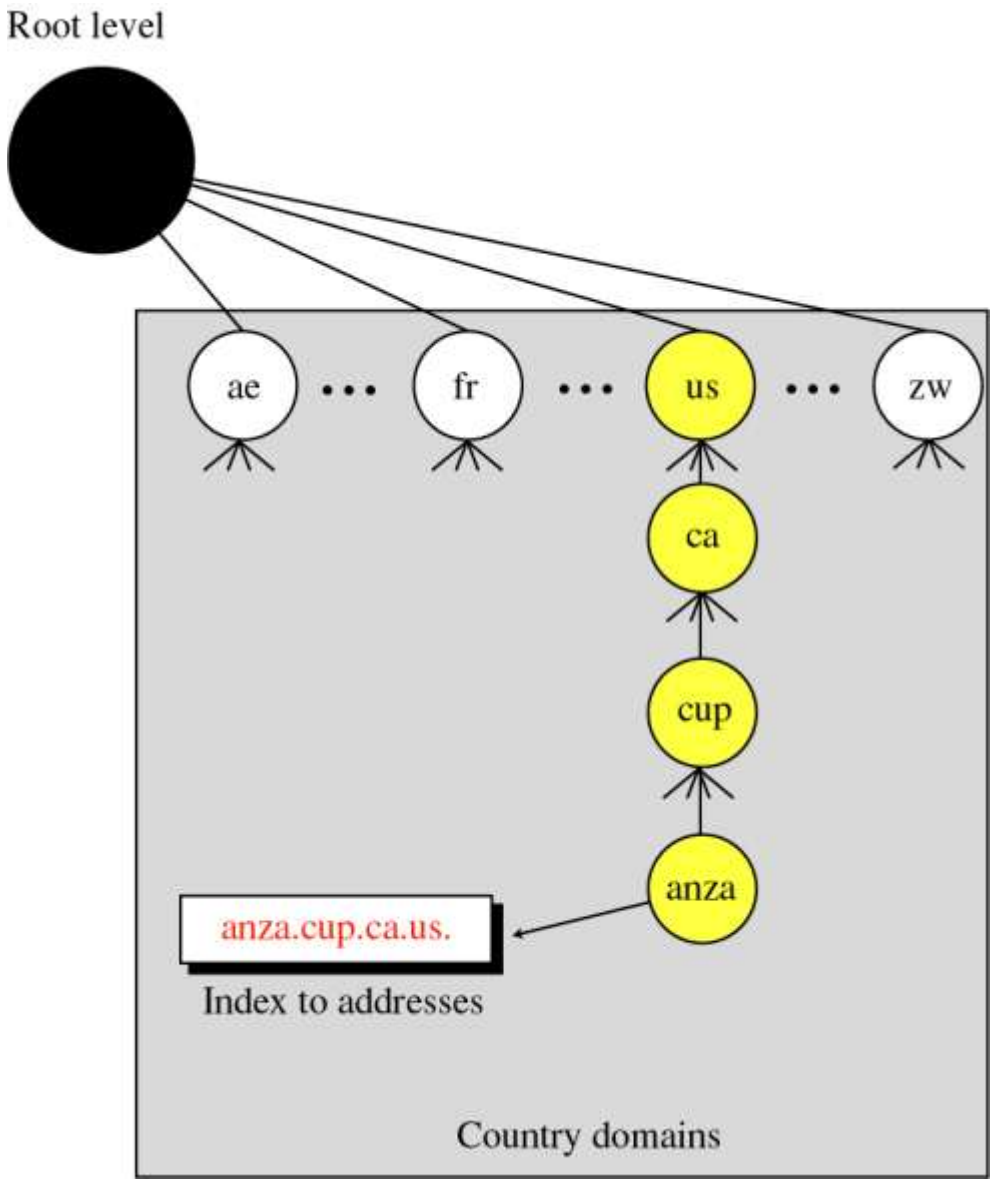
Generic domains

- The generic domains are com(commercial), edu (educational institutions), gov (government), int(some international organizations), mil (military), net(network providers) and org(nonprofit organizations).
- Each domain is named by following an upward path. The components are separated by dots. E.g. eng.sun.com. This is hierarchical naming.

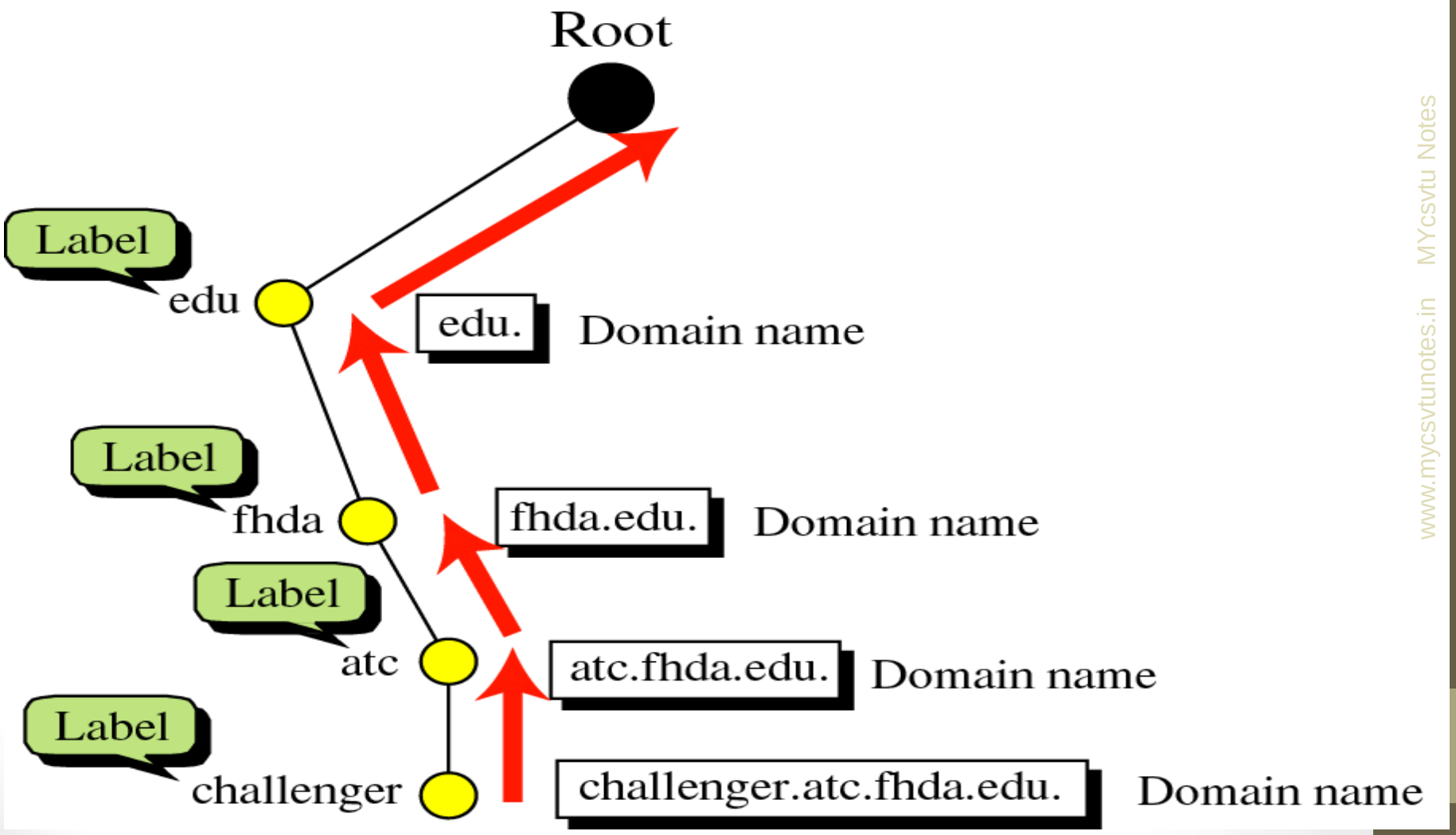
Country domain

- It includes on entry for every country.
- Each domains include one entry for every country.





Domain names and labels



Labels

- Each node in the tree has a label (or component) and it can be specified using up to 63 characters.

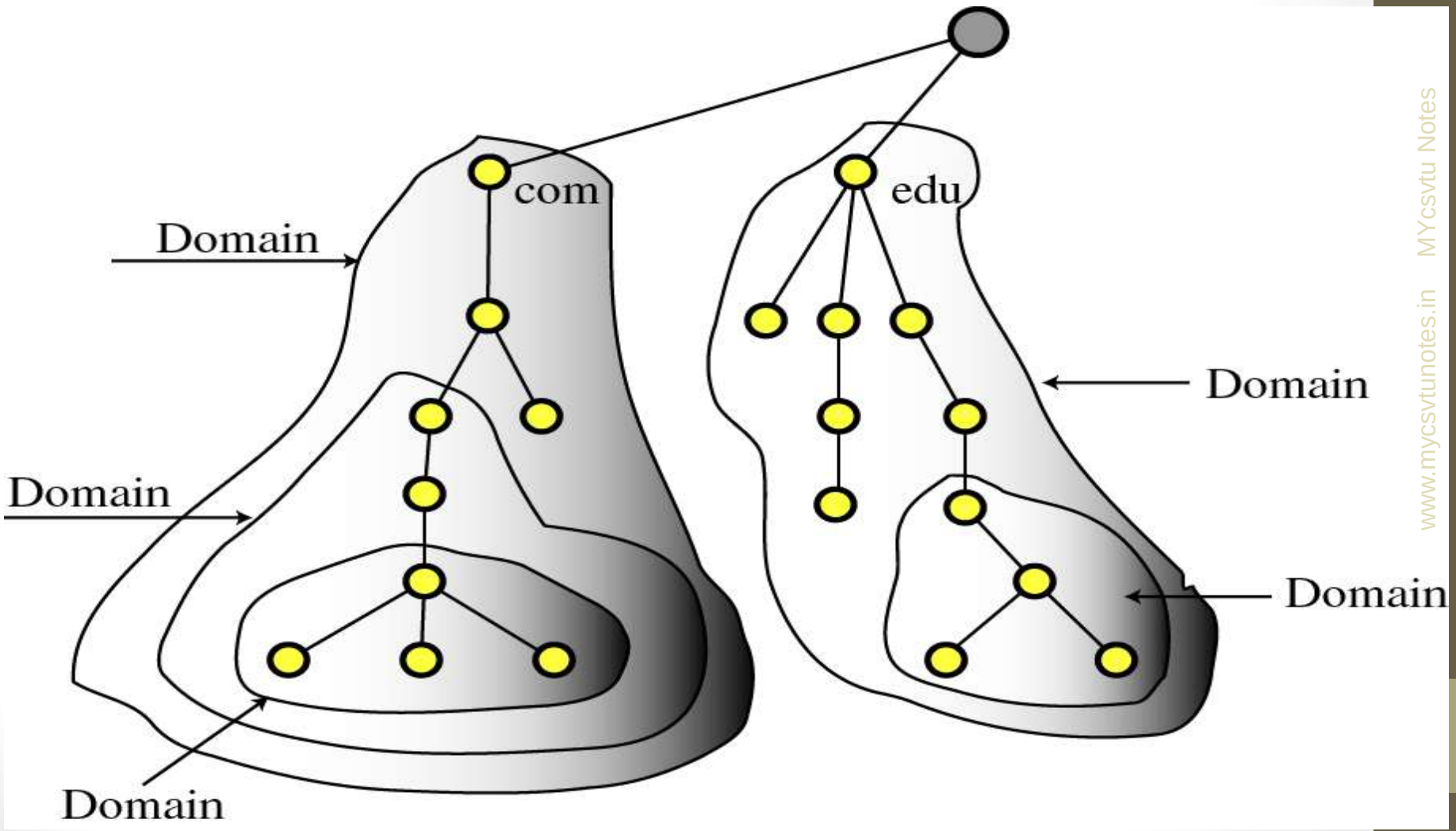
Absolute and relative domain names

- Domain names can be of two types: absolute and relative.
- An absolute domain name always ends with a dot. For example.eng.sun.com.
- But the relative domain does not end with a dot.

Domain

- A domain is a sub tree of the domain name space. The name of the domain is the domain name of the node at the top of the sub tree.

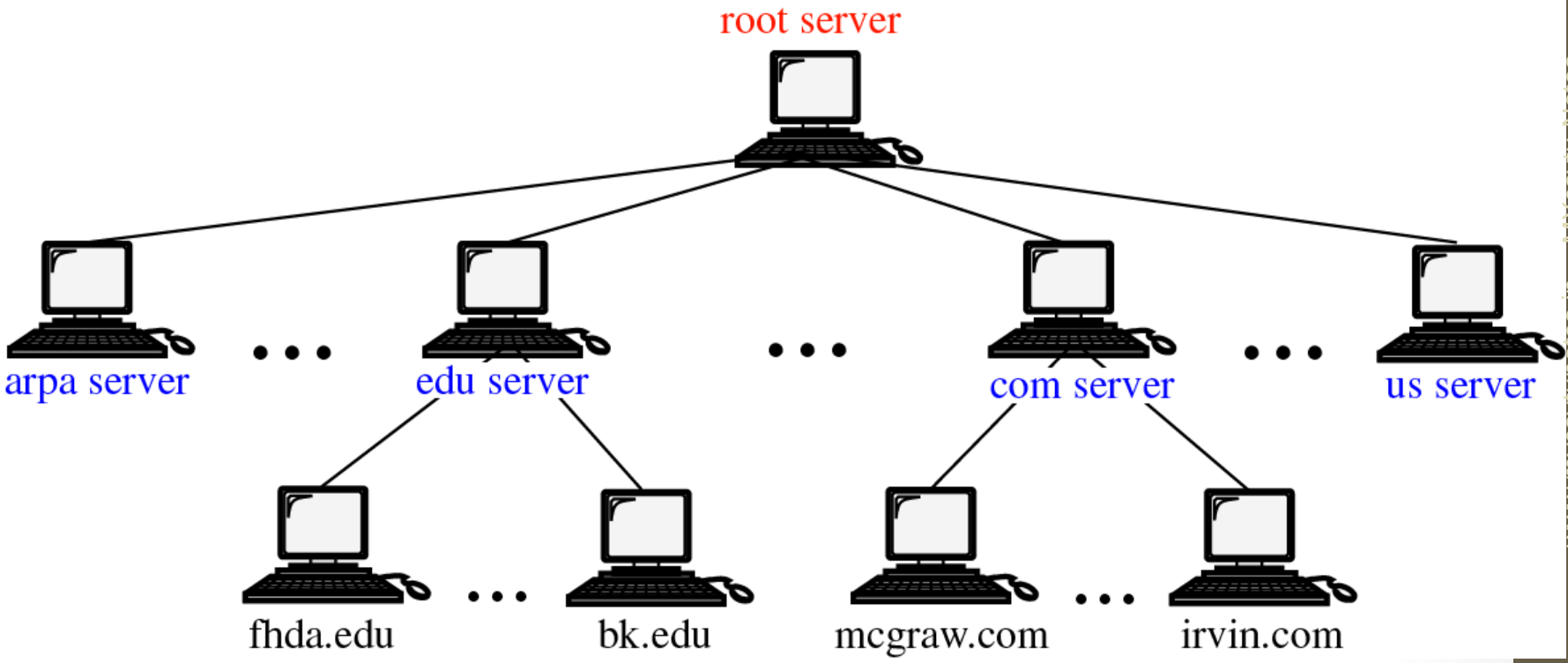
Domain



Name servers

- Name servers contains the DNS database i.e the various names and their corresponding IP addresses.
- Theoretically a single name server could contain the entire DNS database. But practically to store such a huge information at one place is inefficient and unreliable.
- Such a server will be soon overloaded and be useless and worst thing is if it ever goes down the entire Internet will go down.
- The solution to this problem is to distribute the information among many computers called DNS servers.
- First the whole space is divided into many first level domains. The root server stands alone and can create as many first level domains as required.
- The first level domains are further divided into smaller sub-domains called second level domains.

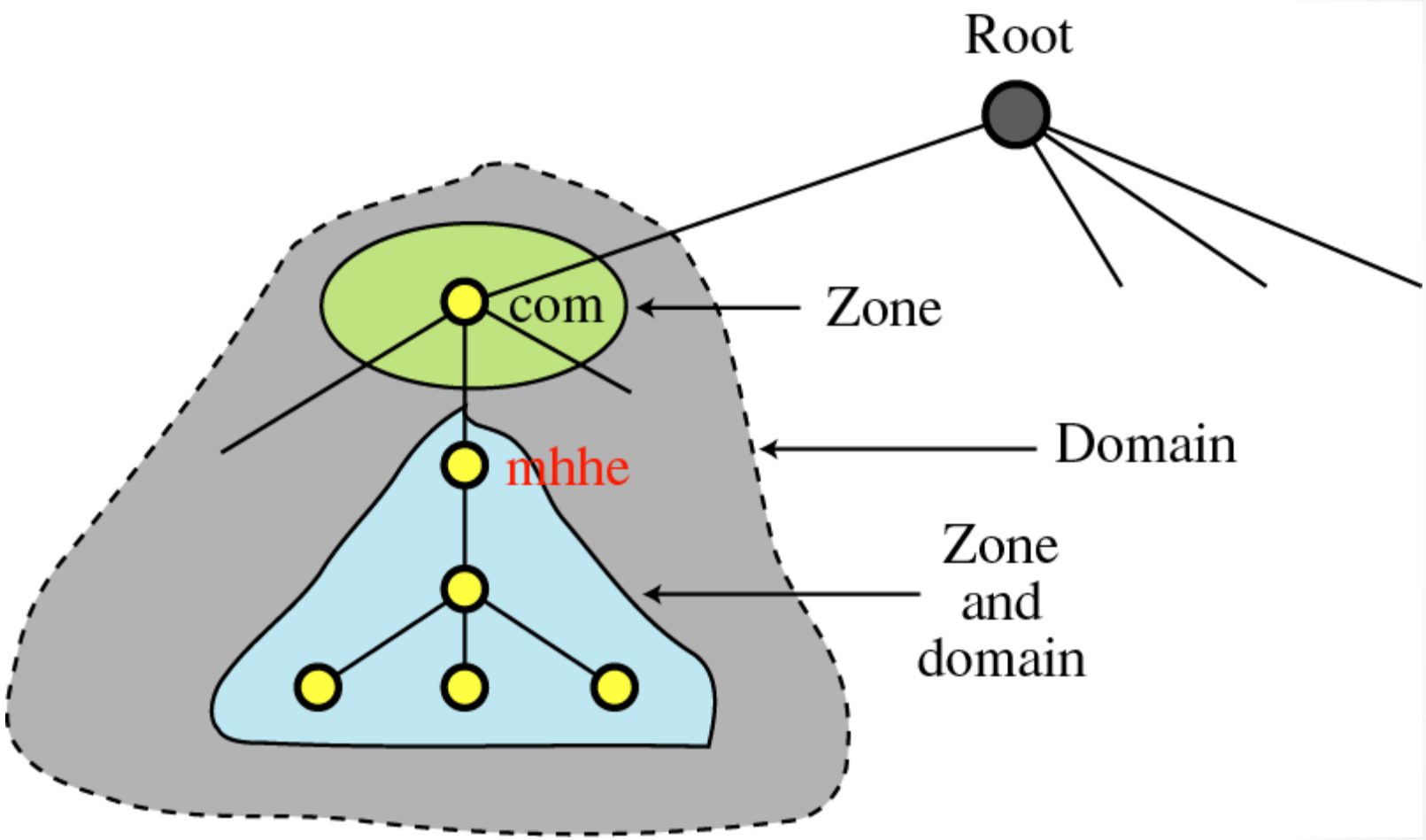
Hierarchy of name servers



Zones

- What a server is responsible for or has authority over is called as a zone.
- If a server is appointed for a domain and the domain is not further divided into sub-domains then the domain and zones will be same.
- The server makes a database called a zone file. It keeps all information about every node under that zone.
- But if a server divides its domains into sub domains and delegates a part of its authority to other servers then domain and zone will be different from each other.

Zones and domains



Root server

- A root server is a server whose zone consists of the whole DNS tree.
- It does not store any information about domains but delegates the authority to other servers. It only keeps the reference of these servers.

Resolution

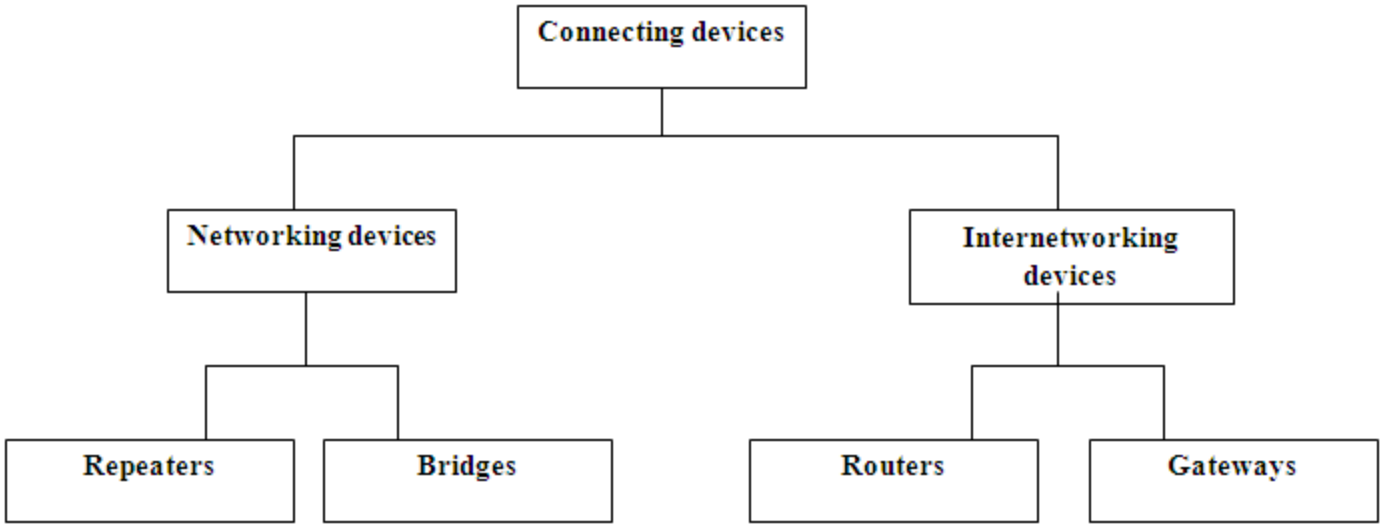
- The process of mapping a name to an address or an address to a name is called as name address resolution.

Resolver

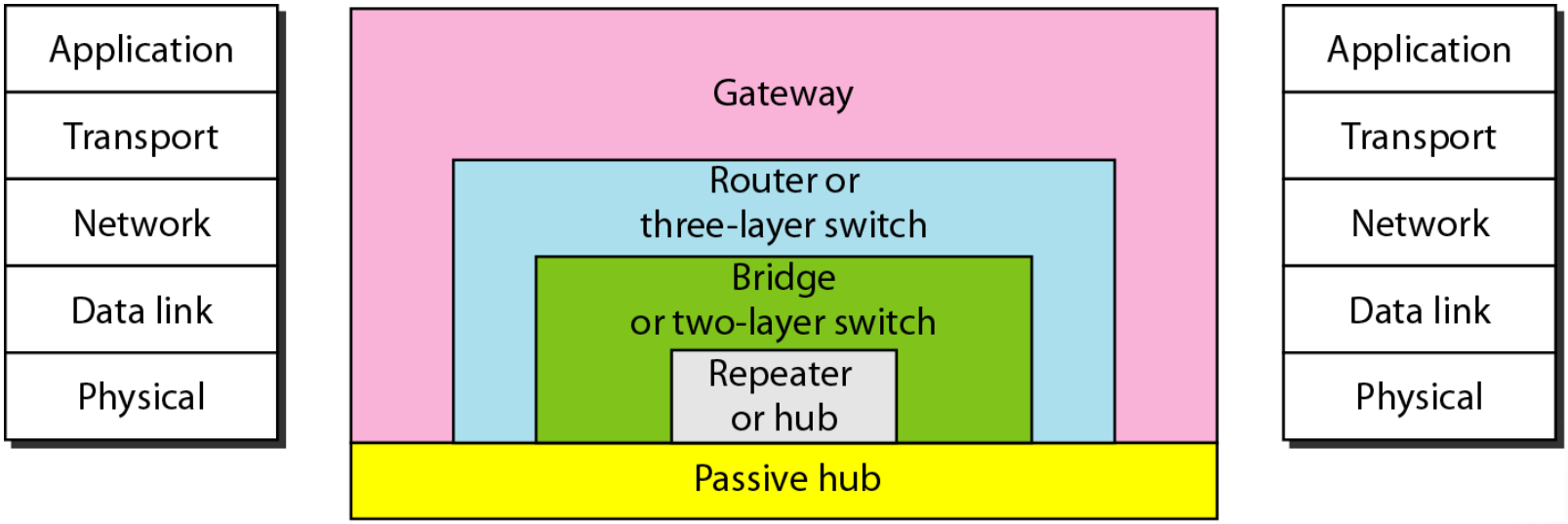
- DNS is the client server application. A host which wants to map a name to address or vice versa calls a DNS client named as resolver. The resolver then accesses the closet DNS server with a mapping request.
- If the sever has the requested information, it satisfies the resolver but if it does not have the requested information, then it refers the resolver to other servers or asks other servers to provide the information.
- The resolver receive the mapping. It then checks for errors and if found error free delivers the mapping to the requesting process.

Networking Devices

Connecting devices



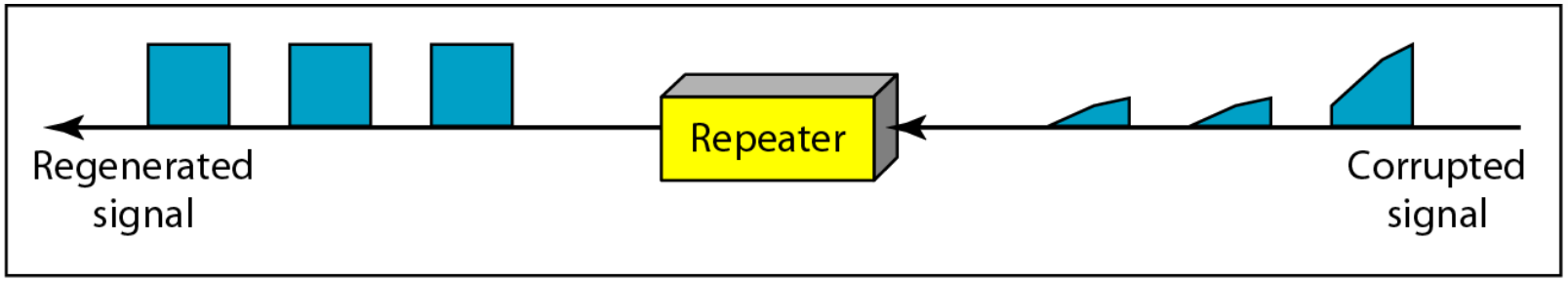
Connecting devices and the OSI model



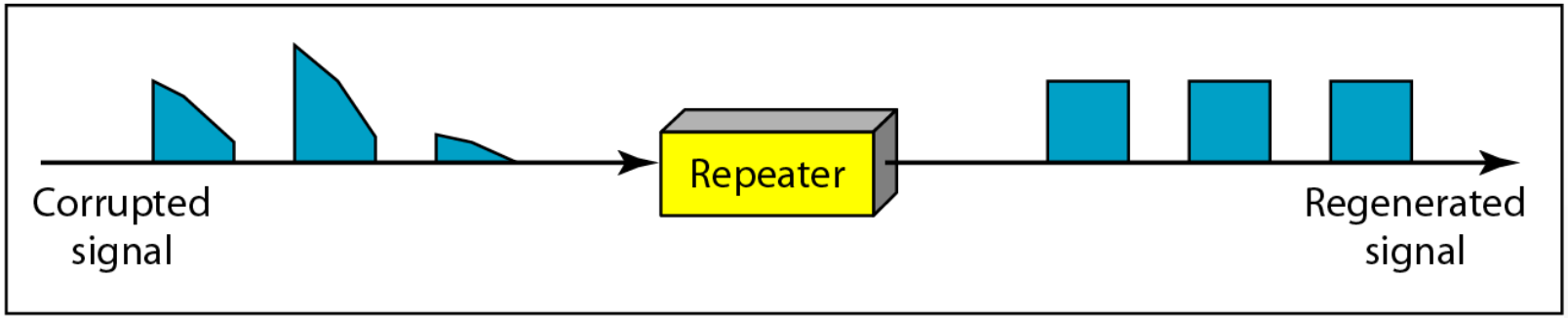
Overview of repeaters

- A repeater is an electronic device which operates only in the physical layers.
- All transmission media weaken the electromagnetic waves that travel through them.
- Attenuation of signals limits the distance any medium can carry data.
- A repeater receives a signal and before it becomes too weak or corrupted, regenerates the original bit pattern.

Function of a Repeater



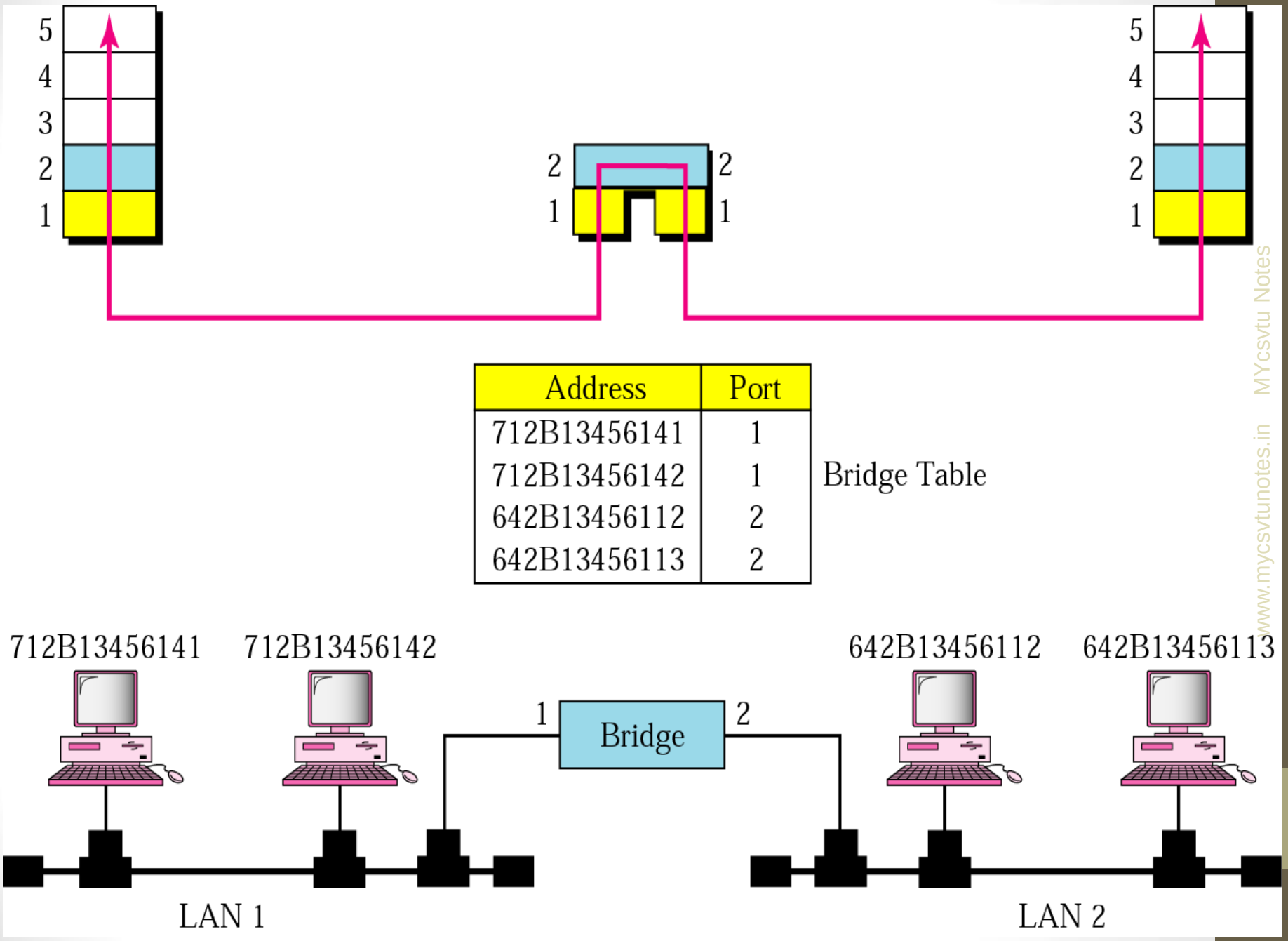
a. Right-to-left transmission.



b. Left-to-right transmission.

Bridges

- A bridge operates in both physical and data link layer.
- It can regenerate the signal that it receives and as a data link layer device, it can check the physical (MAC) addresses of source and destination contained in the frame.
- The major difference between the bridge and repeater is that the bridge has a filtering capability.
- That means it can check the destination address of a frame and decide if the frame should be forwarded or dropped.
- If the frame is to be forwarded, then the bridge should specify the port over which it should be forwarded.
- So a bridge has a table relating the addresses and ports. If a frame for 712B13456113 arrives at port 2 then the bridge goes through its table and understands that the frame is to be sent out on port 1 so it will do so.
- A bridge can check, does not change the physical (MAC) addresses in a frame.



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

Bridge Table

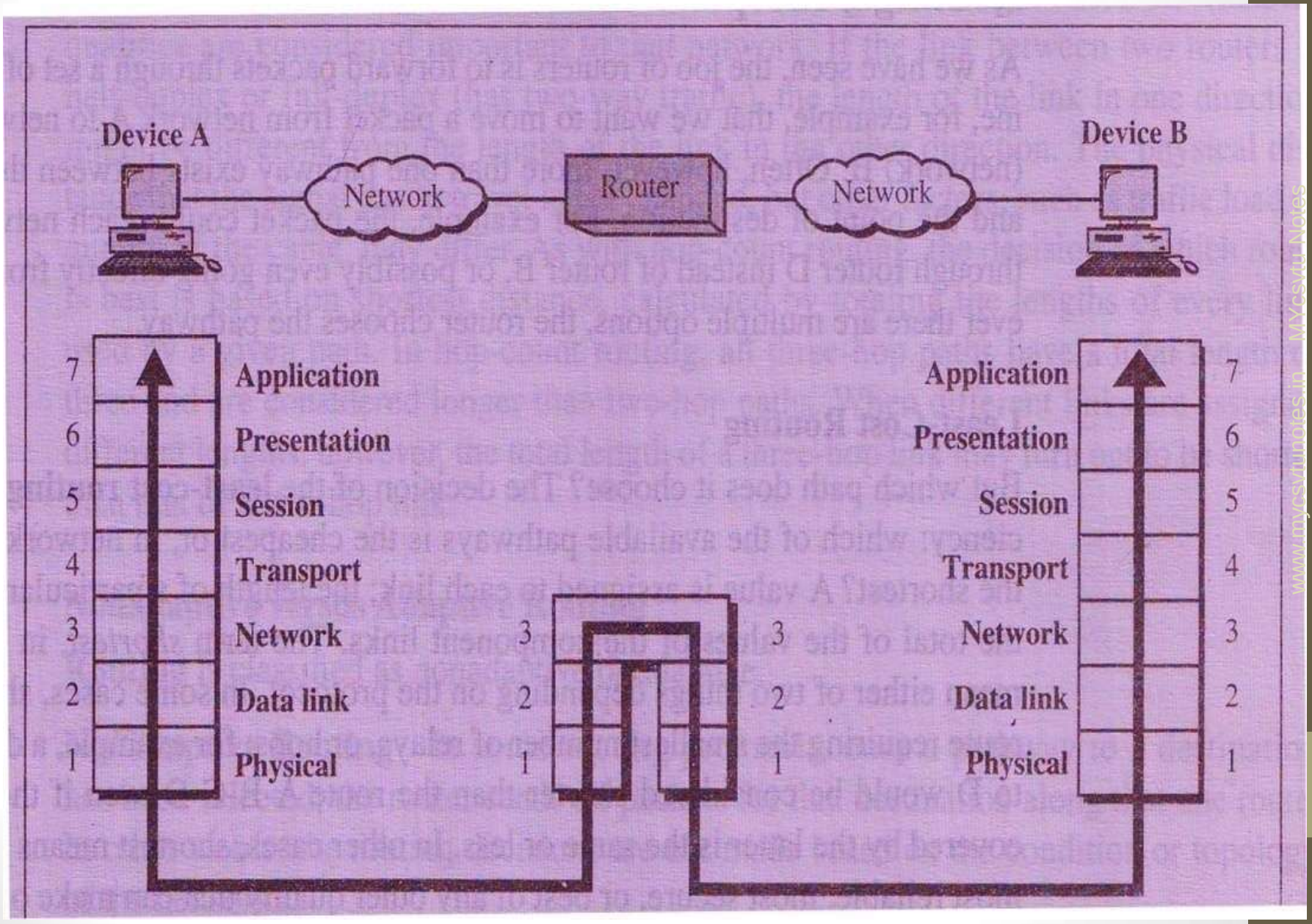
Types of Bridges

- Simple Bridge
- Multiport Bridge
- Transparent Bridge

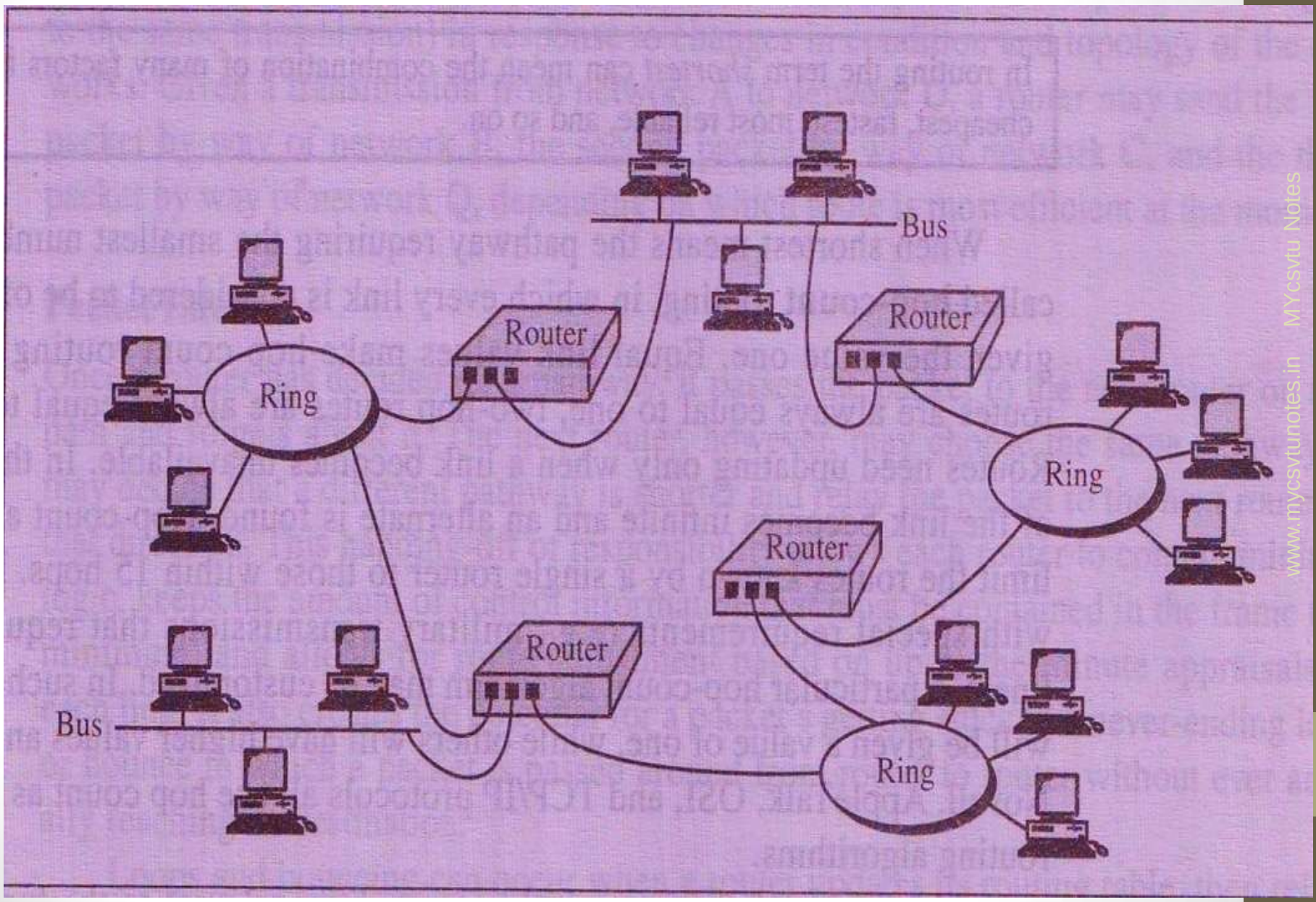
Routers

- Routers are devices that connect two or more networks.
- They consist of a combination of hardware and software.
- The hardware can be a network server, a separate computer or a special device.
- The hardware includes the physical interfaces to the various networks in the internetwork. This interface can be Token Ring, Ethernet, Frame relay, ATM or any other technology.
- The software in a router is the operating system and the routing protocol.

A router in the OSI model



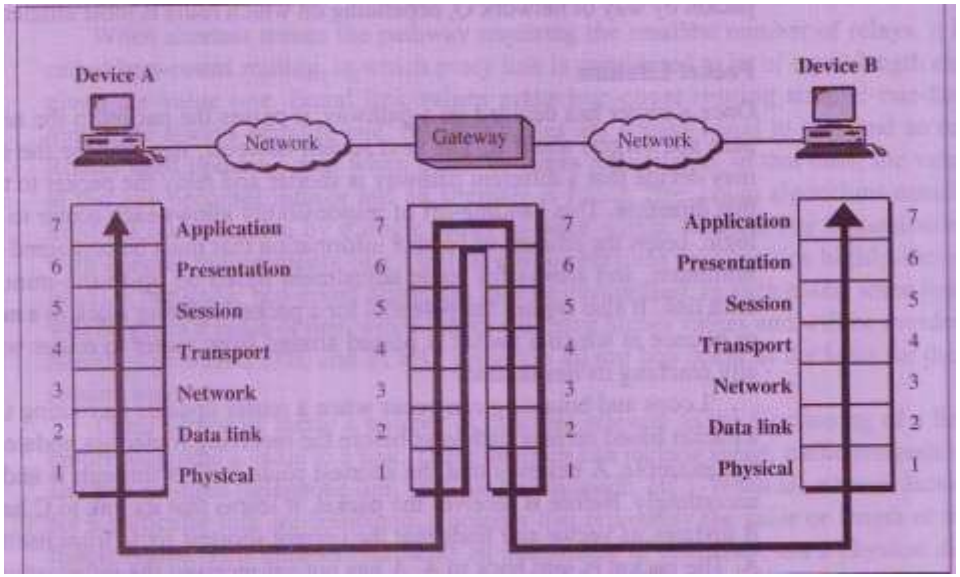
Routers in an internet



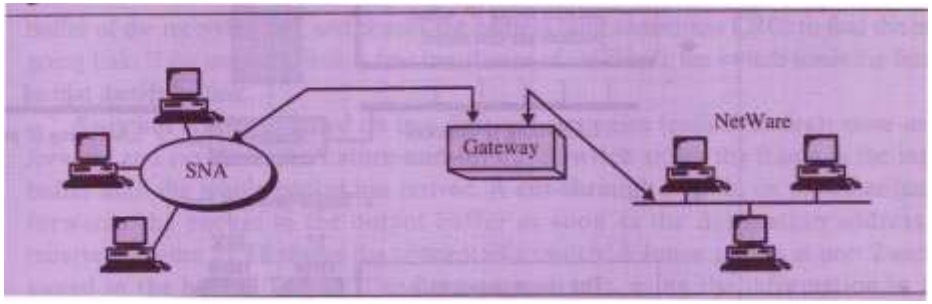
Gateways

- When the networks that must be connected are using completely different protocols from each other, a powerful and intelligent device called a gateway is used.
- A gateway is a device that can interpret and translate the different protocols that are used on two distinct networks.
- Gateways comprise of software, dedicated hardware or a combination of both.
- A gateway can receive e-mail message in one format and convert them into another format.
- Gateways can connect systems with different communication protocols, languages and architecture.

A gateway in the OSI model



A gateway



Hubs

- In general the word hub can refer to any connecting device.
- But its specific meaning is multiport repeater. It is normally used for connecting stations in a physical star topology.
- All networks require a central location to bring media segments together.
- These central locations are called hubs.
- A hub organizes the cables and relays signals to the other media segments.

There are three main types of hubs

- Passive
- Active
- Intelligent

Multiple levels of hierarchy FTP