Syllabus

- **UNIT-1 : Introduction Concepts:** Goals and Applications of Networks, Network structure and architecture, The OSI reference model, services, Network Topology Design - Delay Analysis, Back Bone Design, Local Access Network Design, Physical Layer Transmission Media, Switching methods, ISDN, Terminal Handling.

- **UNIT-2 : Medium Access sub layer:** Medium Access sub layer - Channel Allocations, LANprotocols - ALOHA protocols - Overview of IEEE standards - FDDI. Data Link Layer - Elementary Data Link Protocols, Sliding Window protocols, Error Handling.

- **UNIT-3 : Network Layer:** Network Layer - Point - to Pont Networks, routing, Congestion control Internetworking TCP / IP, IP packet, IP address, IPv6.

- **UNIT-4 : Transport Layer:** Transport Layer - Design issues, connection management, session Layer-Design issues, remote procedure call. Presentation Layer-Design issues, Data compression techniques, cryptography - TCP - Window Management.

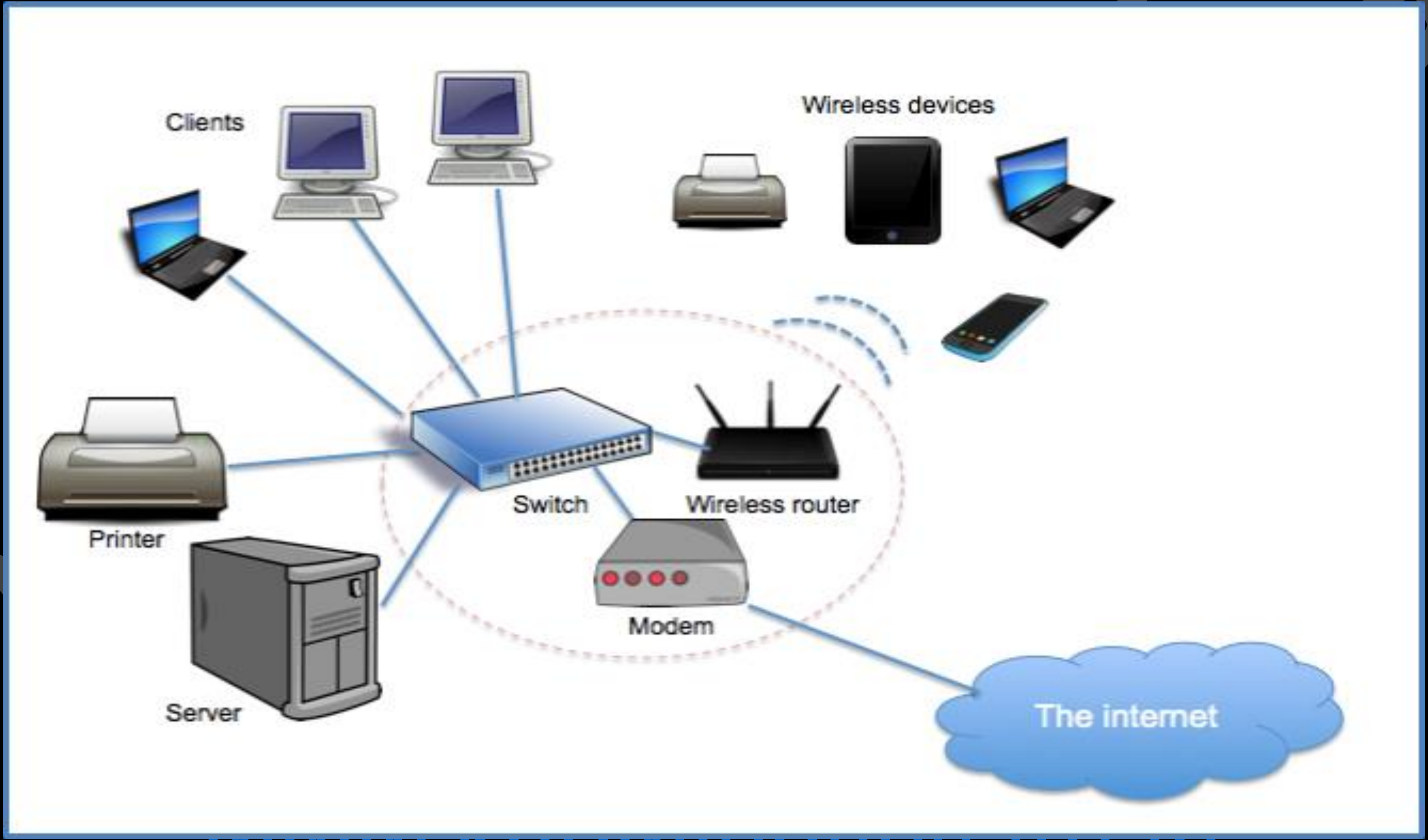
- **UNIT-5 : Application Layer:** Application Layer: File Transfer, Access and Management, Electronic mail, Virtual Terminals, Other application. Example Networks - Internet and Public Networks.

Video chapters

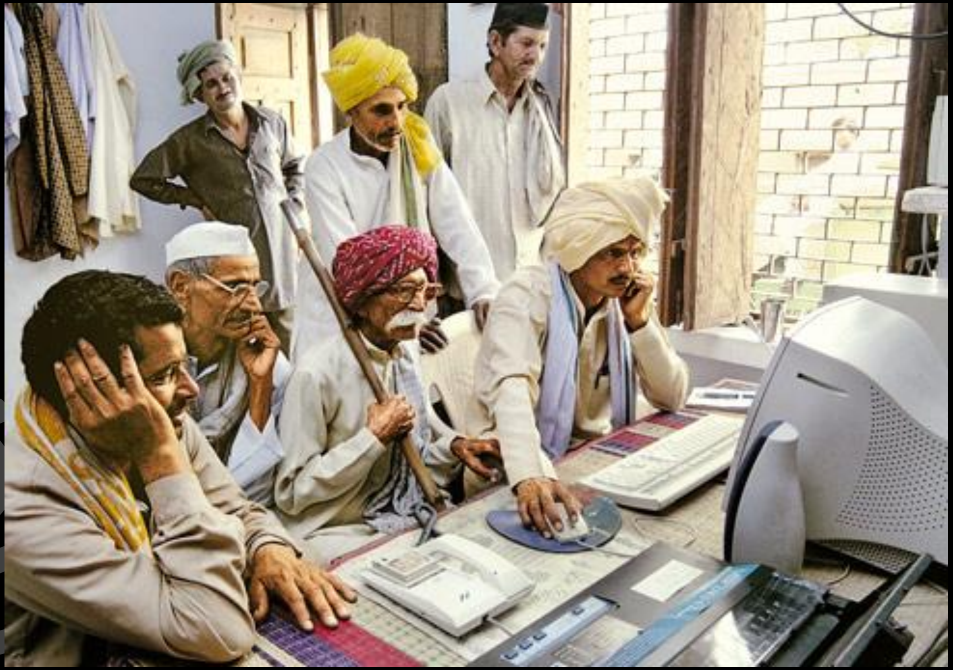
- **Chapter-1 (Basics):** What is Computer Networks, Goals, Application, Data Communication, Transmission Mode, Network Criteria, Connection Type, Topology, LAN, WAN, MAN, OSI Model, All Layer Duties, Transmission Media, Switching, ISDN.
- **Chapter-2 (Data Link Layer):** Random Access, ALOHA, Slotted ALOHA, CSMA, (CSMA/CD), (CSMA/CA), Sliding Window Protocol, Stop-and-Wait, Go-Back-N, Selective Repeat ARQ, Error Handling, Parity Check, Hamming Codes, CheckSum, CRC, Ethernet, Token Bus, Token Ring, FDDI, Manchester Encoding.
- **Chapter-3 (Network Layer):** Basics, IPv4 Header, IPv6 Header, ARP, RARP, ICMP, IGMP, IPv4 Addressing, Notations, Classful Addressing, Class A, Class B, Class C, Class D, Class E, Casting, Subnetting, Classless Addressing, Routing, Flooding, Intra-Domain Vs Inter-Domain, Distance Vector Routing, Two-Node Instability, Split Horizon, Link State Routing.
- **Chapter-4 (Transport Layer):** Basics, Port Number, Socket Addressing, TCP-Header, Three-way-Handshake, User Datagram Protocol, Data Compression, Cryptography, Symmetric Key, DES, Asymmetric Key, RSA Algorithm, Block-Transposition Cipher.
- **Chapter-5 (Application Layer):** E-Mail, SMTP, POP3/IMAP4, MIME, Web-Based Mail, FTP, WWW, Cookies, HTTP, DNS, Name Space, Telnet, ARPANET, X.25, SNMP, Voice over IP, RPC, Firewall, Repeater, Hub, Bridge, Switch, Router, Gateway.

What is Computer Networks

- A **computer network** is a telecommunications network, which allows autonomous digital devices(nodes) to exchange data between each other using either wired or wireless connections to share resources (h/w or s/w) interconnected by a single technology e.g. internet.



Internet means empowerment



Internet Of Things

Any Device

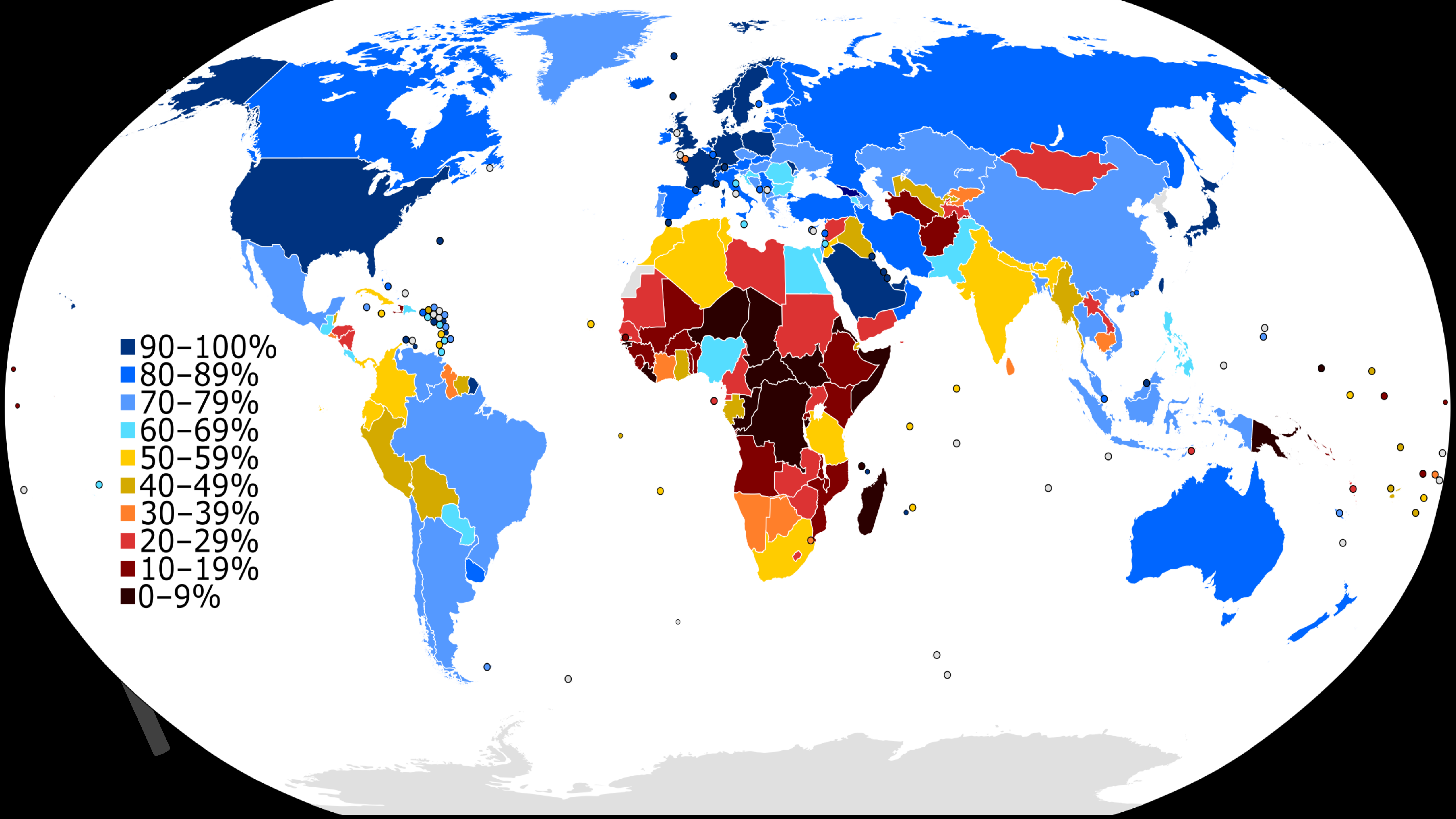
Anybody

Anywhere

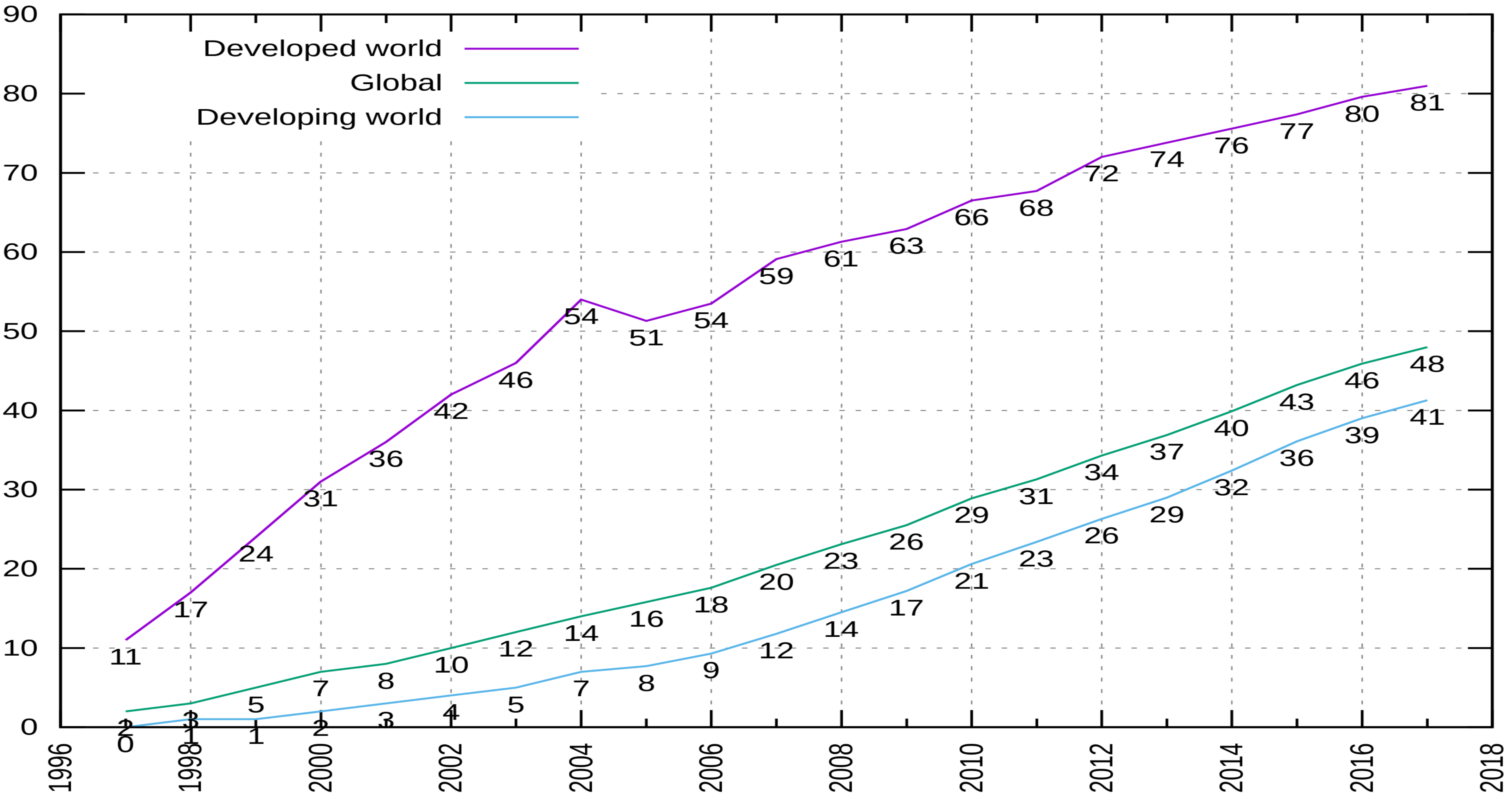
Any Business

Any Network

Anytime



90–100%
80–89%
70–79%
60–69%
50–59%
40–49%
30–39%
20–29%
10–19%
0–9%

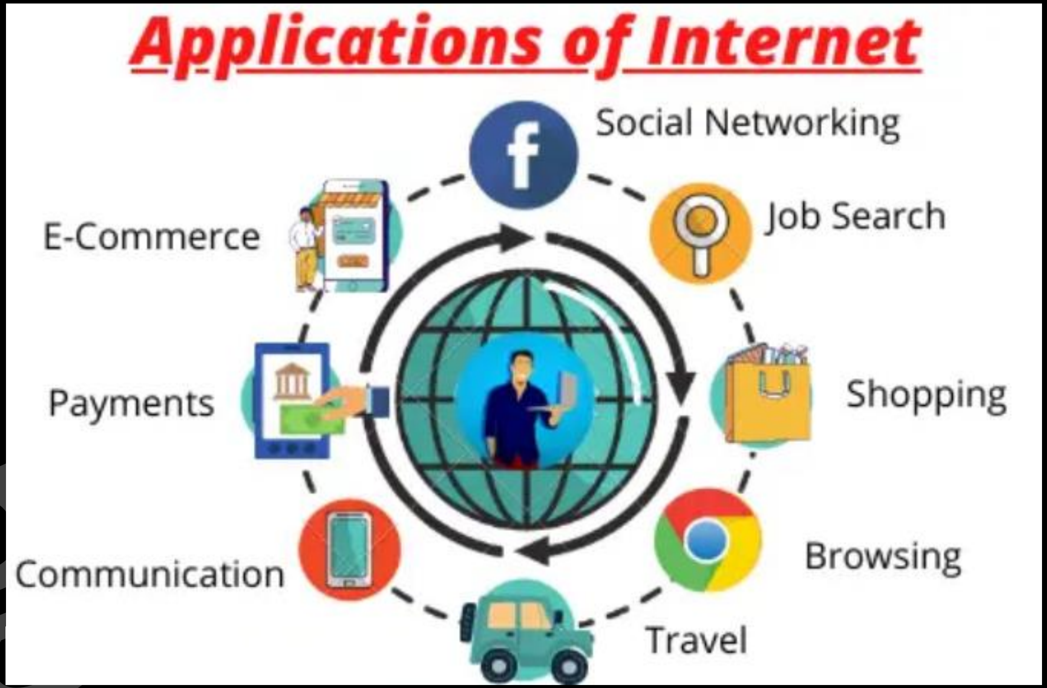

Internet Users Per 100 Inhabitants

Goals of Computer Networks

- **Facilitating Communication**:
  - Enabling swift and efficient communication between individuals and organizations.
  - Supports video conferencing, emails, instant messaging, etc.
- **Resource Sharing**:
  - Allows users to share hardware and software resources.
  - Enables printer sharing, file sharing, etc.
- **Data Storage and Access**:
  - Centralized storage systems that allow data access from any connected device.
  - Helps in easy data backup and recovery.
- **Cost Efficiency**:
  - Reduces costs by sharing resources and avoiding duplication of hardware and software.
- **Reliability and Redundancy**:
  - Enhances reliability through alternate paths and redundant systems in case of failures.

Applications of Computer Networks

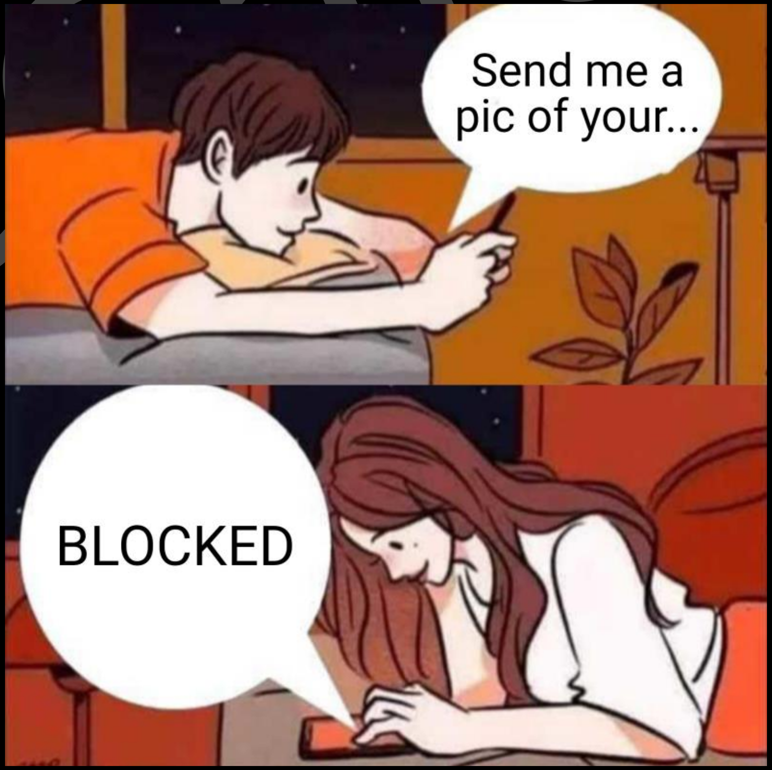
- **Business and Commerce**:
  - E-commerce, online banking, stock trading, etc.
  - Facilitates remote working and global collaboration.
- **Education**:
  - E-learning platforms, virtual classrooms, online exams, etc.
  - Facilitates research and knowledge sharing.



- **Healthcare**:
  - Telemedicine, electronic health records, remote patient monitoring, etc.
- **Government Services**:
  - E-governance, online public services, secure communication between government agencies, etc.
- **Entertainment**:
  - Online gaming, streaming services, social media platforms, etc.
- **Scientific Research**:
  - Facilitates data sharing and collaboration on research projects between institutions worldwide.
- **Travel and Hospitality**:
  - Online ticket booking, hotel reservations, GPS and navigation services, etc.

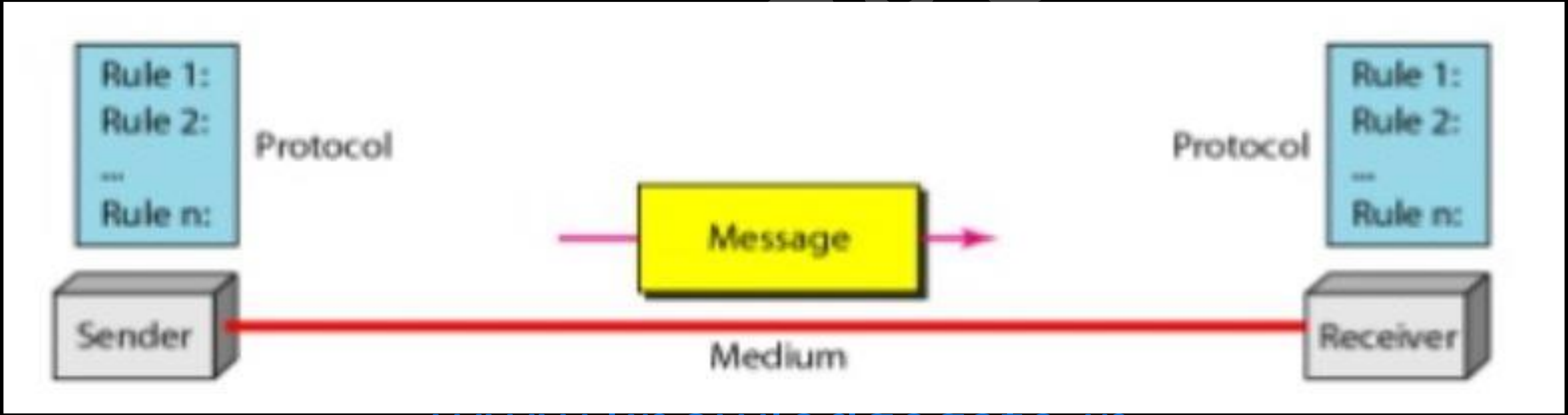
Data communication

- Data communications are the exchange of data between to two devices via some transmission medium.



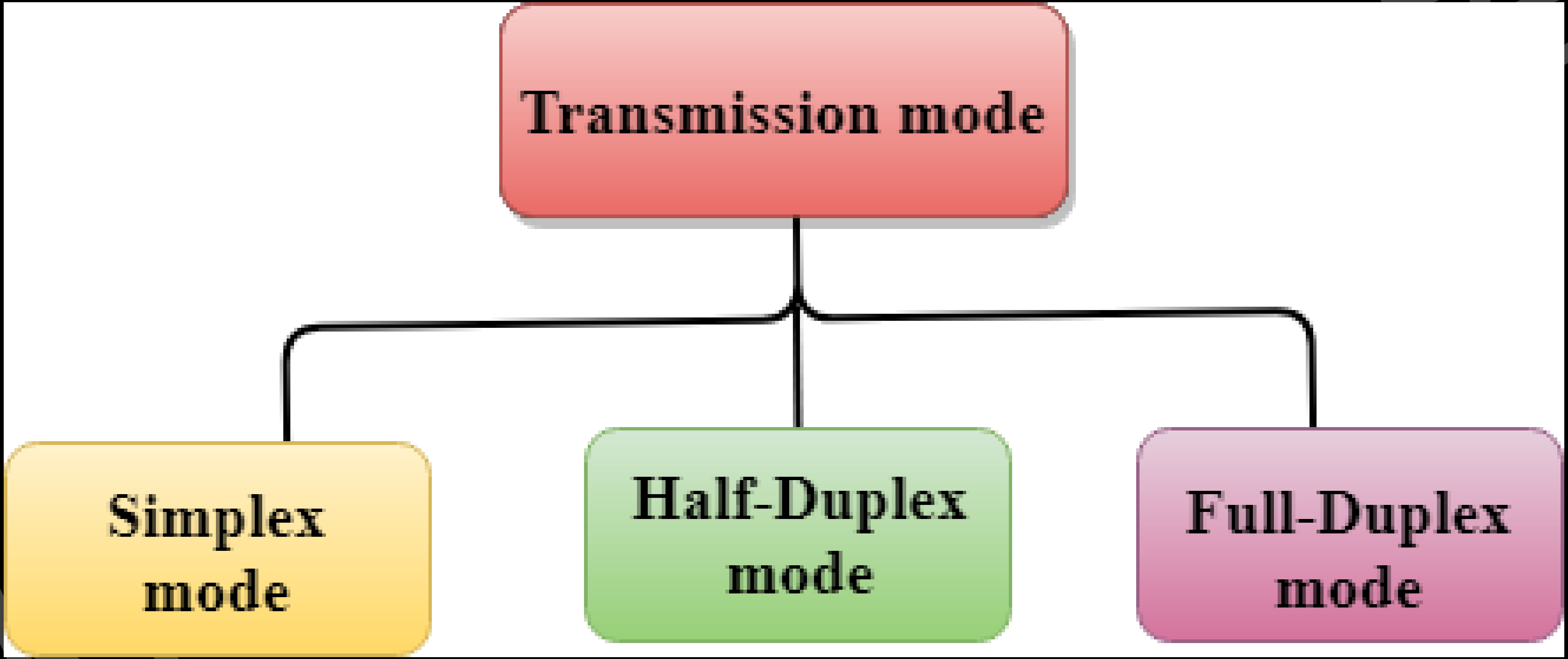
Data communication system has five components

1. **Message**- information (data) to be communicated e.g. text, audio, video.
2. **Sender**- device how sends the message (computer, phone, camera etc.)
3. **Receiver**- device how receives the message (computer, phone, television etc.)
4. **Transmission medium** – is the physical path by which a message travels from sender to receiver.
5. **Protocol** – Which includes Syntax, Semantics, Timing, De facto, De jure.



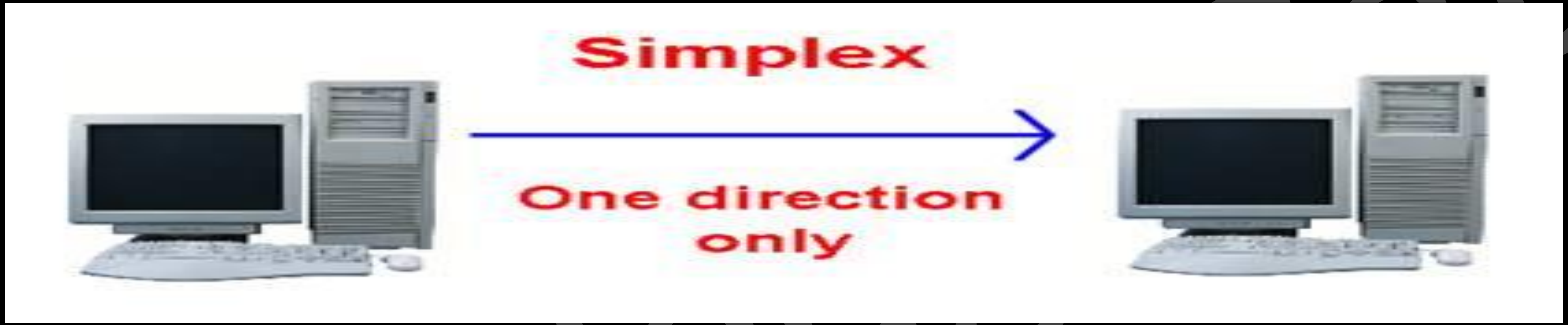
Transmission Mode

- Data flow between two systems can be categorised into three types –



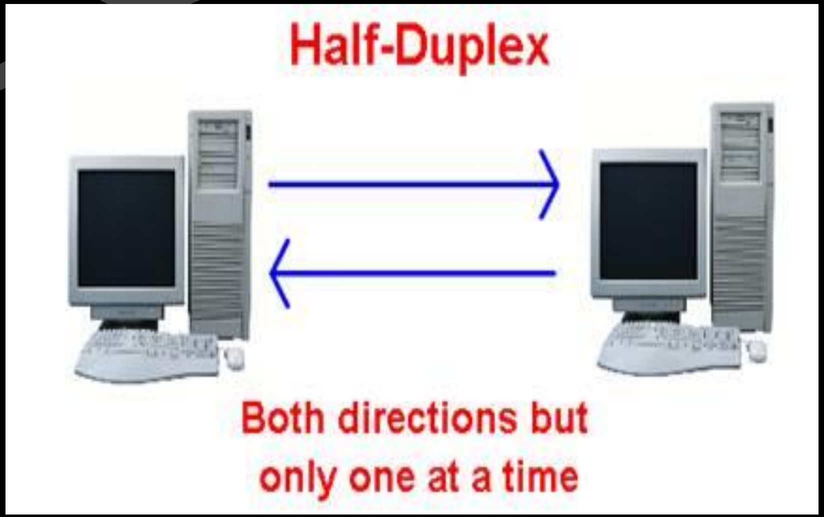
Simplex

- The communication is unidirectional as a one-way street, one device always, other can always receive. E.g. radio, mouse. The simplex mode can use the entire capacity of the channel to send data in one direction.



Half duplex

- Each station can both transmit and receive, but not at the same time. E.g. like a one lane road, walkie-talkie etc.
  - When one device is sending, the other can only receive, and vice versa.
  - In a half-duplex transmission, the entire capacity of a channel is taken over by whichever of the two devices is transmitting at the time.
  - Walkie-talkies are both half-duplex systems.

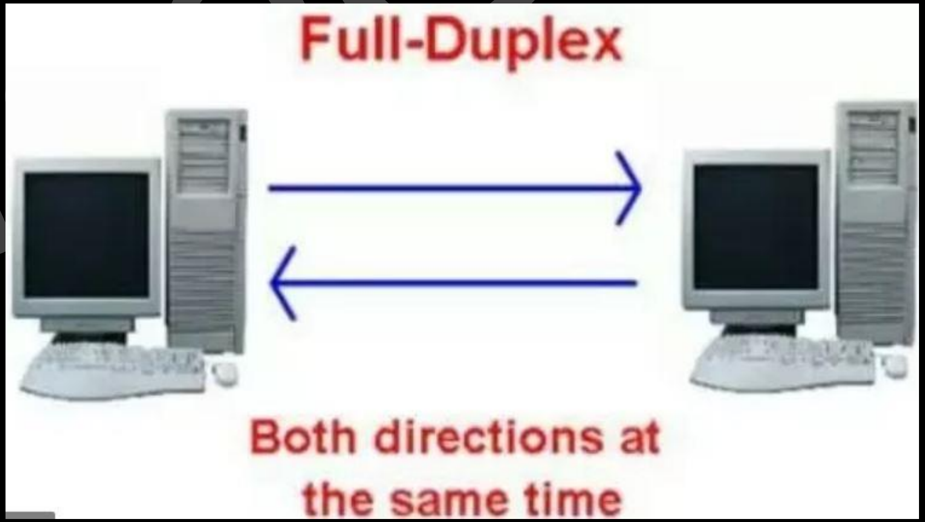


Walkie-talkies

www.knowledgegate.in

Full duplex

- Both stations can transmit and receive at the same time. Actually, it is two half duplex connections.
- Telephone network is an example of full-duplex mode, when two people are communicating by a telephone line, both can talk and listen at the same time.
- The capacity of the channel, must be divided between the two directions.



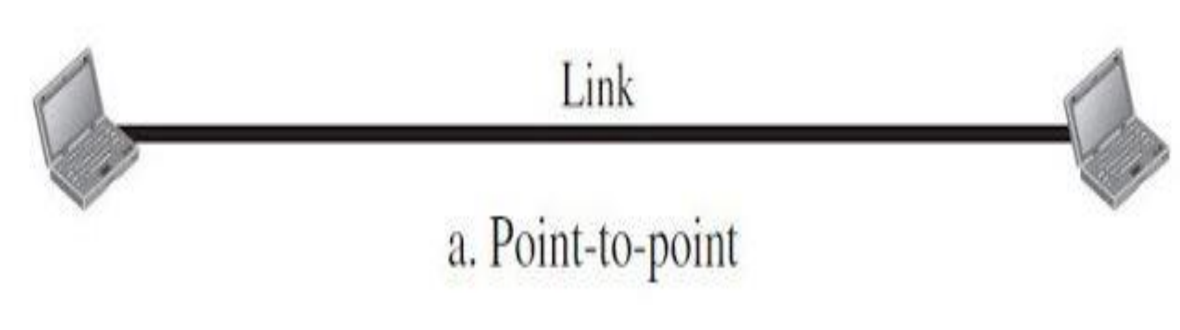
Network criteria

- A network must be able to meet a certain number of criteria. The most important of these are.
  1. **Delivery & Accuracy**- Must deliver the data to correct destination without any error.
  2. **Performance** – Can be measured in many ways including transit time, response time, number of users, type of transmission medium, capabilities of connected hardware's and efficiency of software.
  3. **Reliability** – Is a measure of frequency of failure and the time taken to resolve from the failure.
  4. **Security** – Includes protecting data from unauthorised access, protecting data from damage and development.

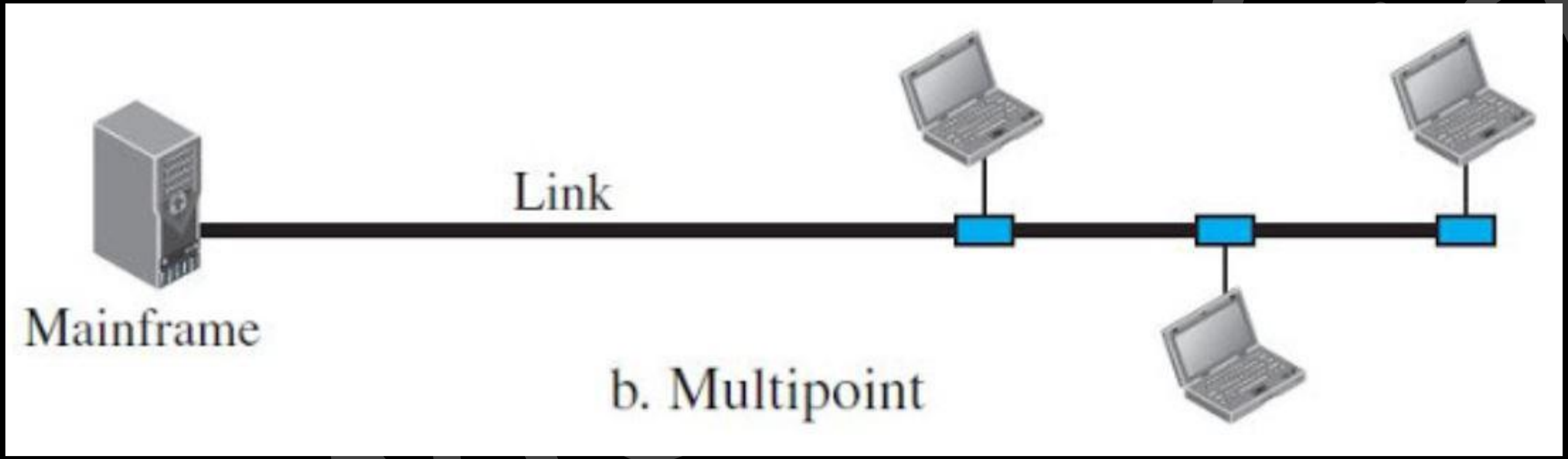
Sender
Medium
Receiver

Types of connection

- **Point to point -** A point-to-point connection provides a dedicated link between two devices.
- Most point-to-point connections use an actual length of wire or cable to connect the two ends, but other options, such as microwave or satellite links, are also possible.

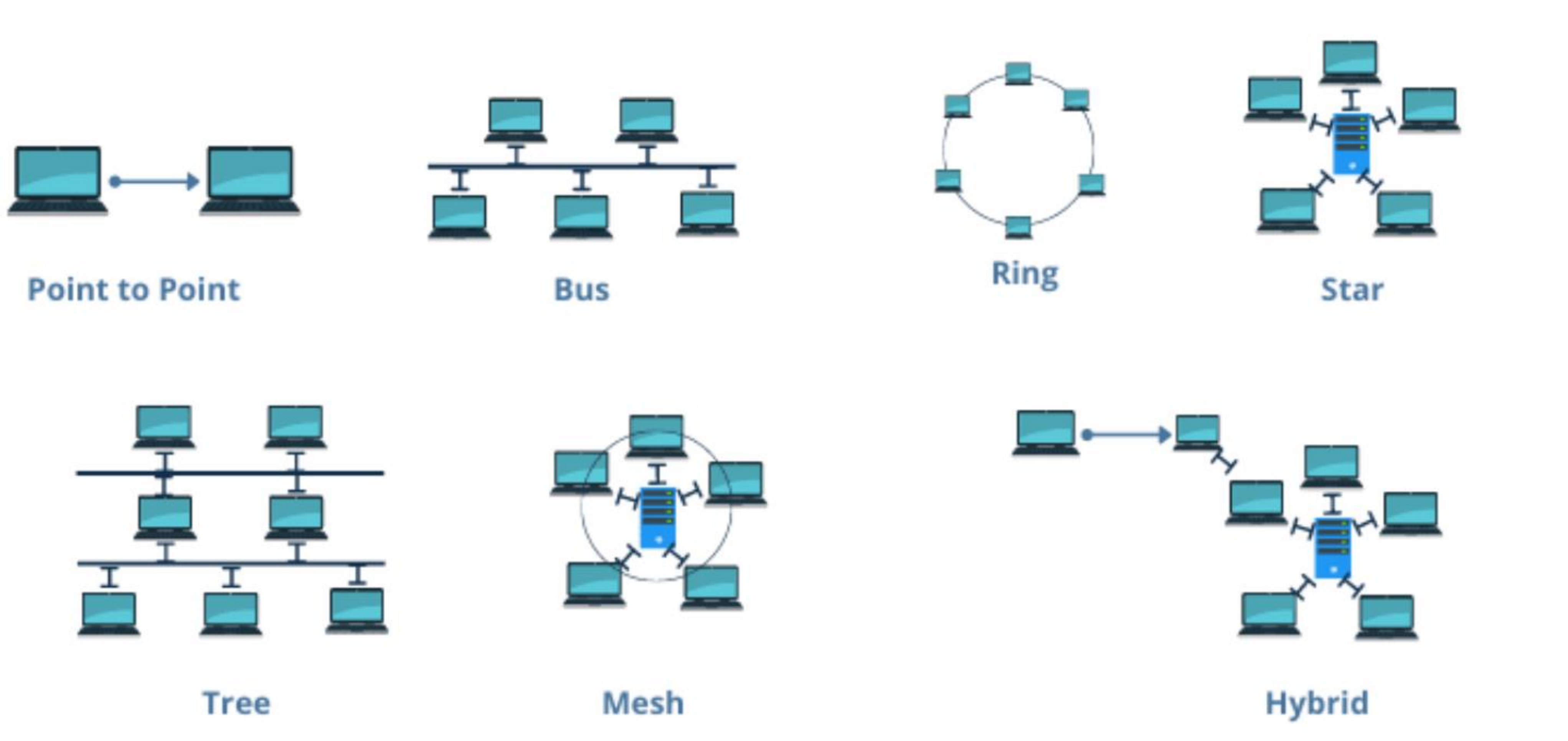


- **Multipoint** - A multipoint (also called multidrop) connection is one in which more than two specific devices share a single link.



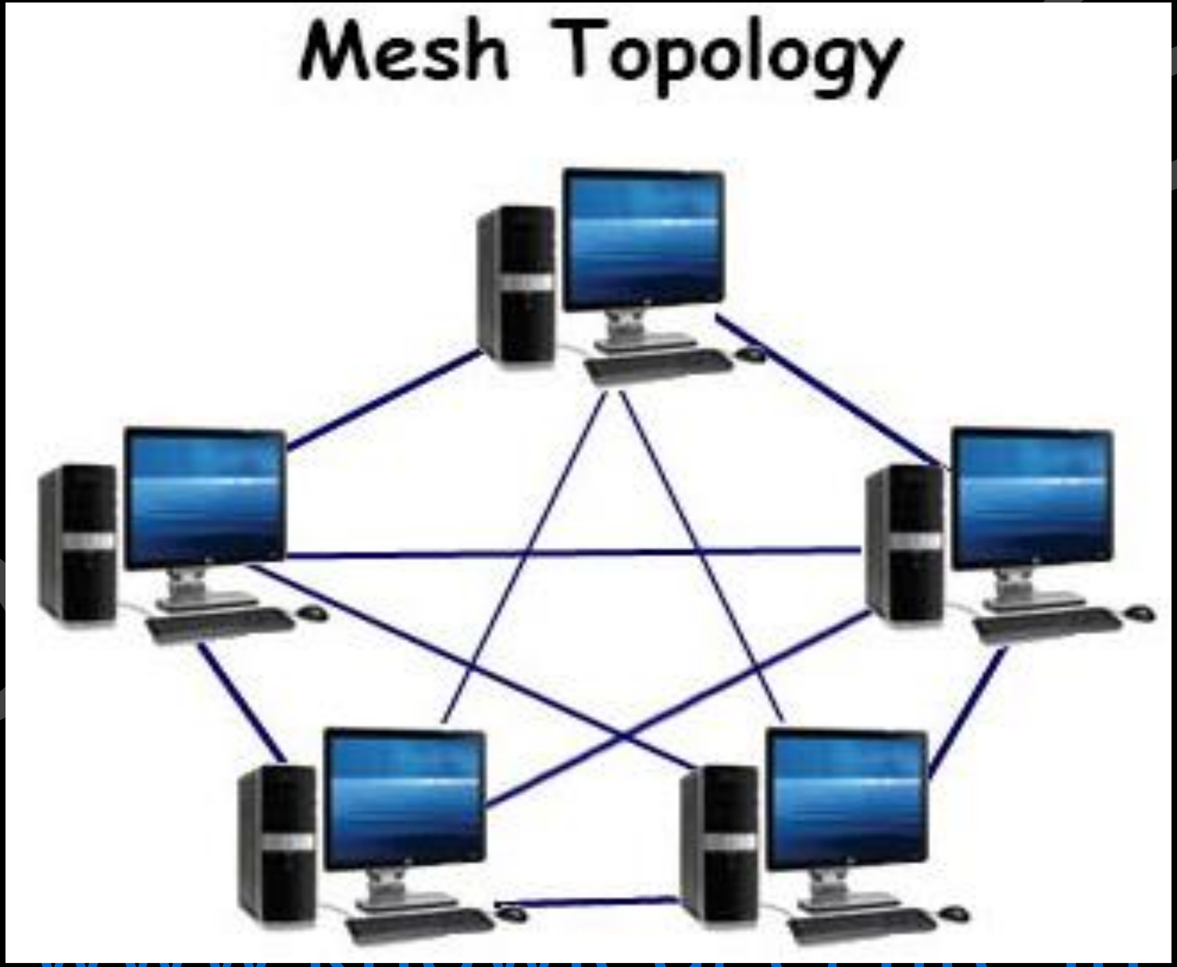
Physical topology

- Refers to the way in which a network is laid out physically. Topology of a network is the geometric representation of the relationship of all the links and linking devices to one another.

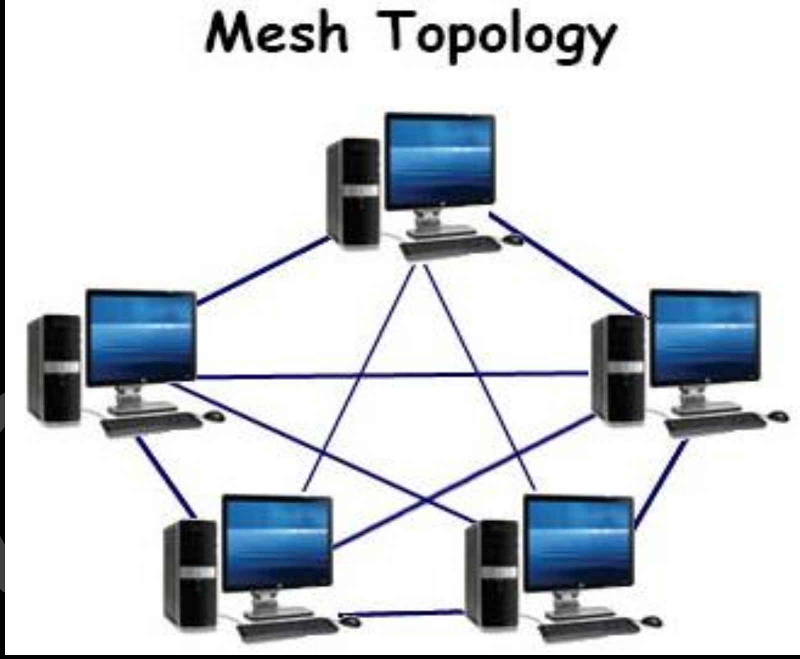


Mesh Topology

- In a mesh topology, every device has a dedicated point-to-point link to every other device. We need, **n (n -1) /2,** duplex-mode links, where n is number of nodes.



- **Advantages**
  1. No **traffic problems**
  2. **Robust**
  3. **Privacy or security**
  4. **Fault identification and fault isolation easy.**

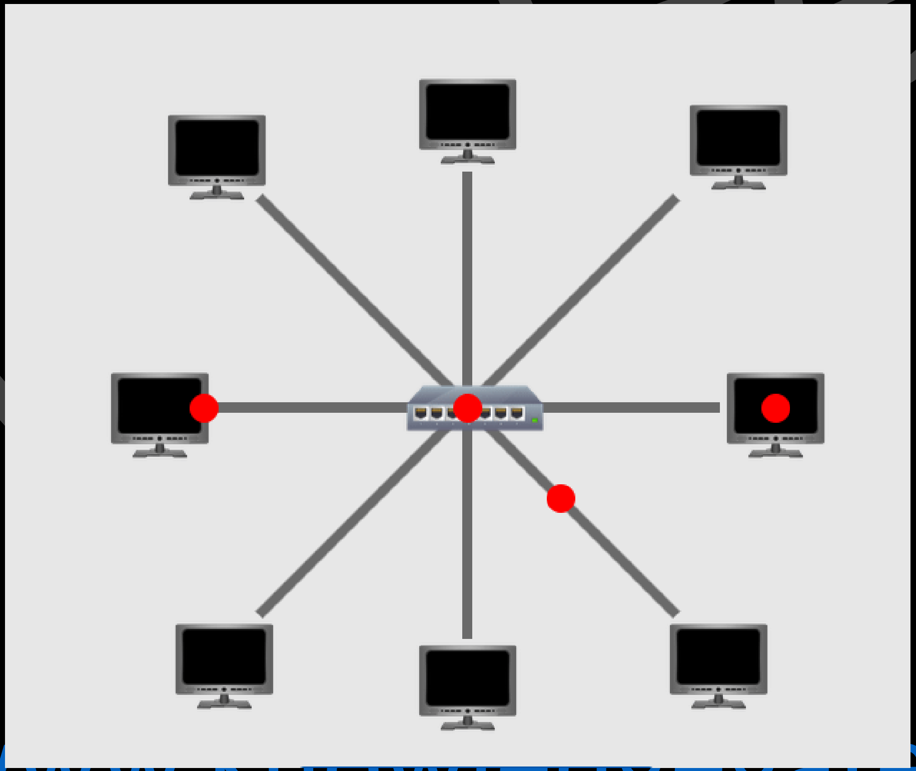


- **Disadvantage**
  1. **Installation and reconnection are difficult.**
  2. The **sheer bulk** of the wiring.
  3. **Expensive.**

Star Topology

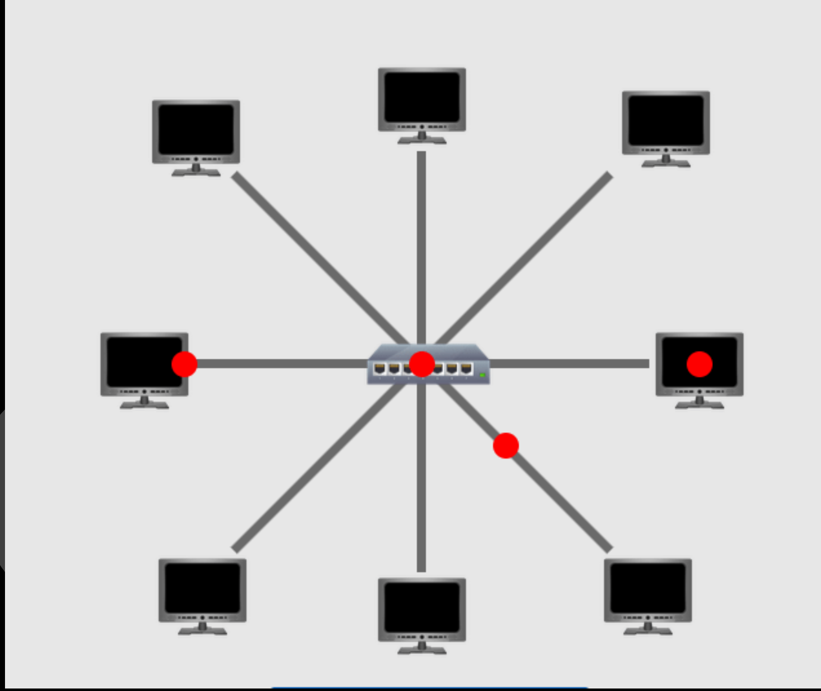
- In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a hub. The devices are not directly linked to one another.

- The controller acts as an exchange: If one device wants to send data to another, it sends the data to the controller, which then relays the data to the other connected device.



Advantages

1. Less expensive than a mesh topology.
2. Easy to install and reconfigure and less costly.
3. It is robust. If one link fails, only that link is affected.
4. Easy fault identification and fault isolation.

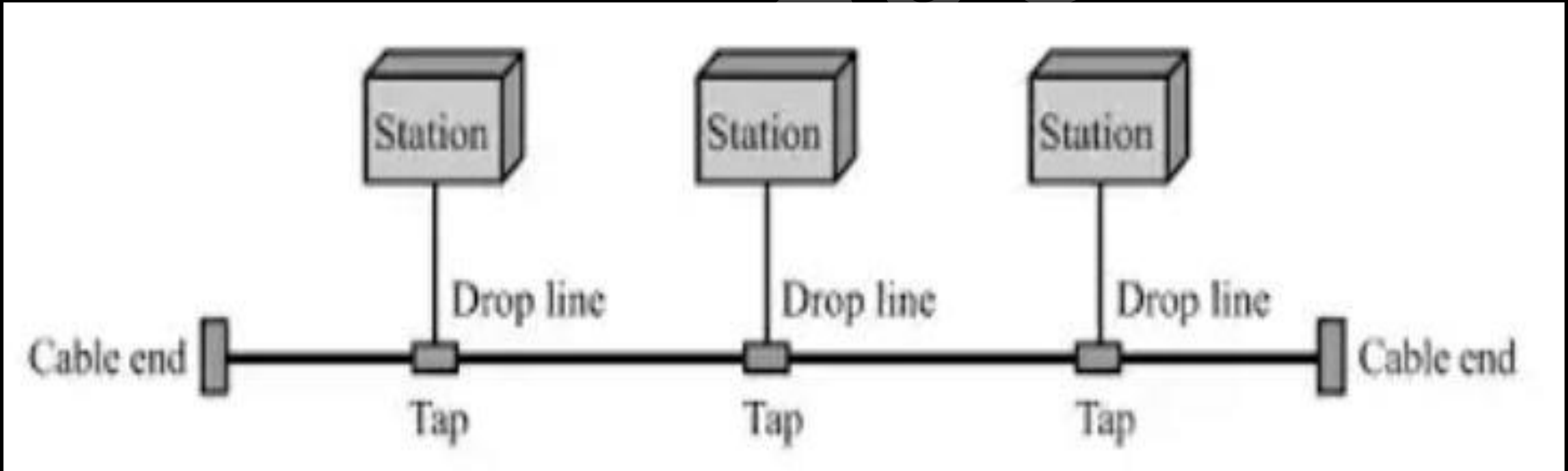


Disadvantage

1. Dependency of the whole topology on one single point, the hub.
2. Often more cabling is required in a star than in some other topologies.

Bus Topology

- A bus topology, is multipoint. One long cable acts as a backbone to link all the devices in a network.
- Nodes are connected to the bus cable by drop lines and taps.
- A drop line is a connection running between the device and the main cable.
- A tap is a connector that either splices into the main cable or punctures the sheathing of a cable to create a contact with the metallic core.

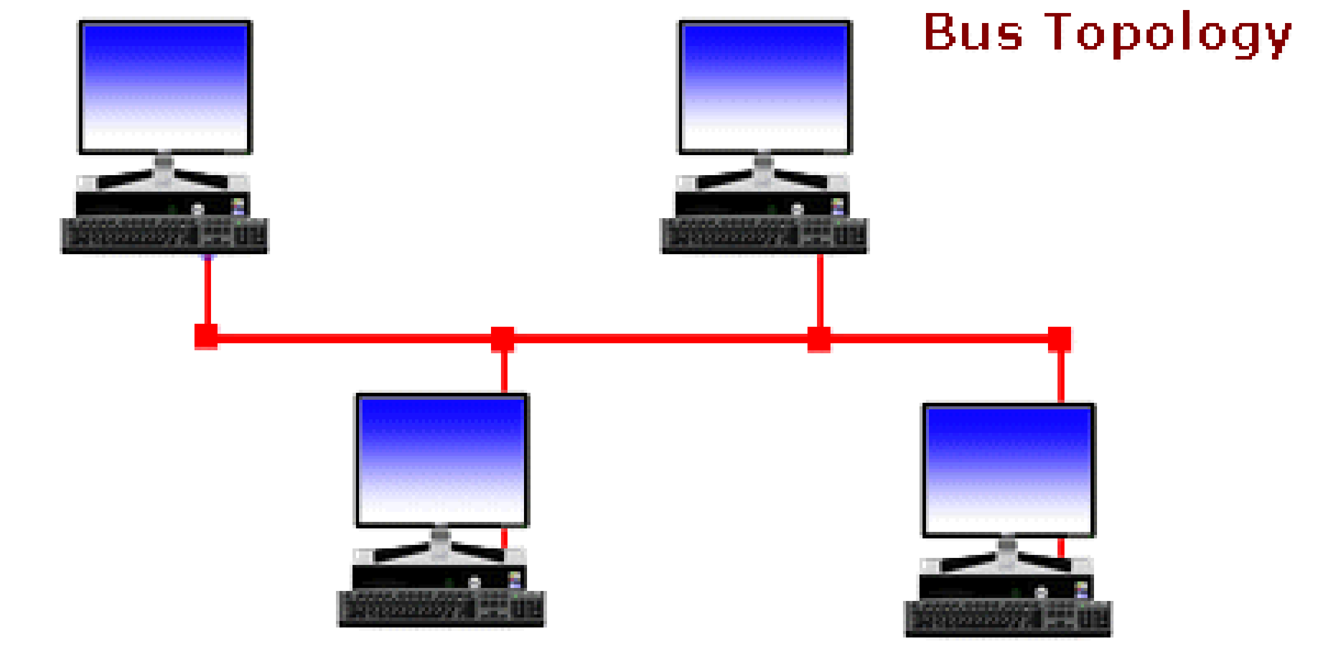


Advantages

1. Ease of installation.
2. Uses less cabling than mesh or star topologies.

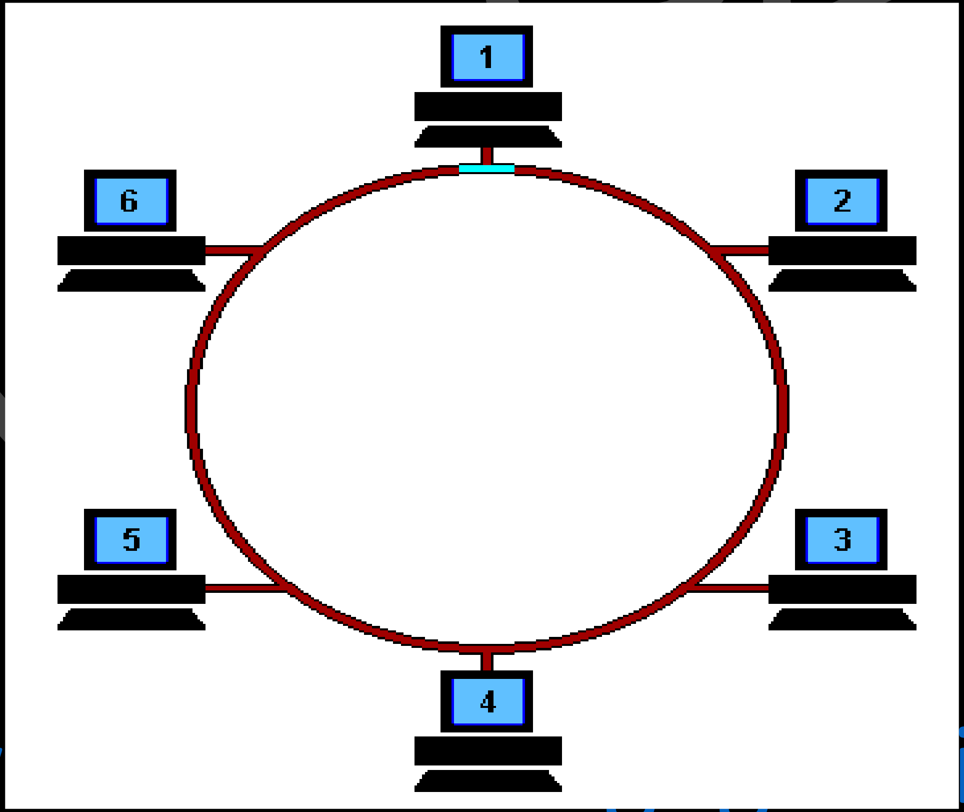
Disadvantage

1. Difficult reconnection and fault isolation.
2. Difficult to add new devices to network.
3. A fault or break in the bus cable stops all transmission.



Ring Topology

- In a ring topology, each device has a dedicated point-to-point connection with only the two devices on either side of it.
- A signal is passed along the ring in one direction, from device to device, until it reaches its destination. Each device in the ring incorporates a repeater.
- When a device receives a signal intended for another device, its repeater regenerates the bits and passes them along.

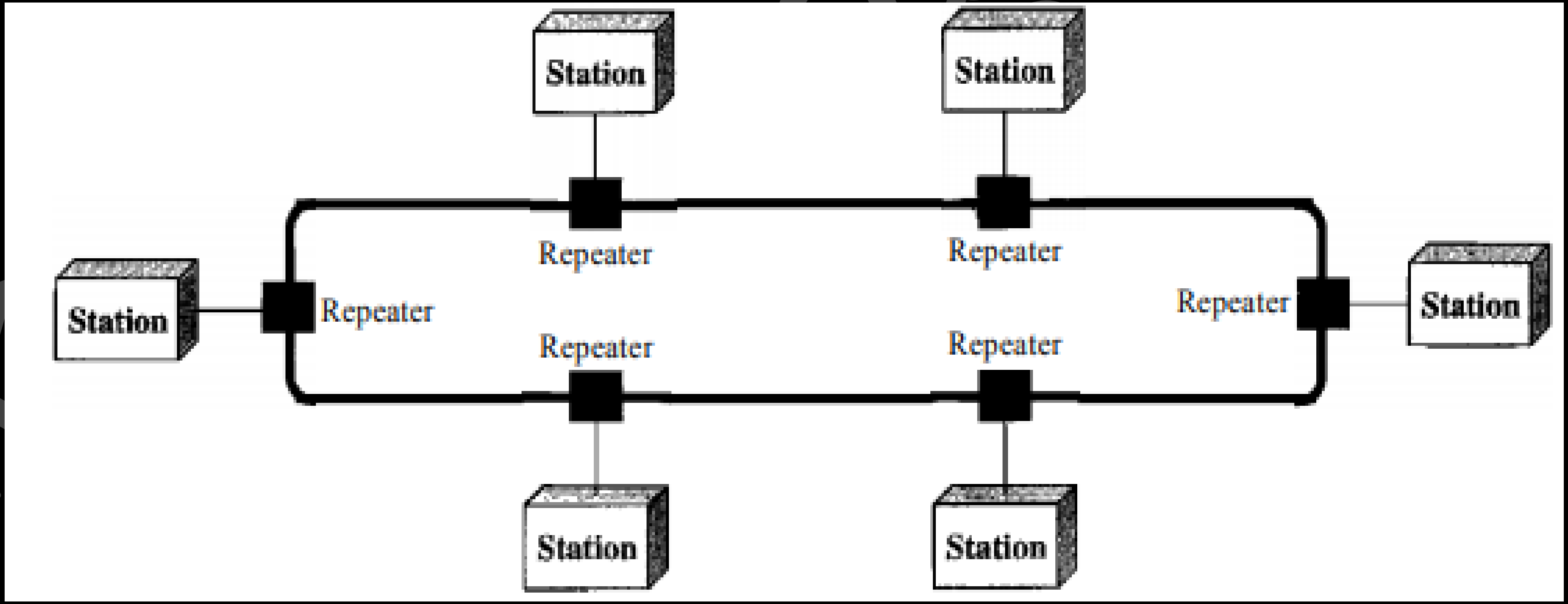


Advantages

1. A ring is relatively easy to install and reconfigure.
2. Fault isolation is simplified.

Disadvantages

1. A break in the ring (such as a disabled station) can disable the entire network.



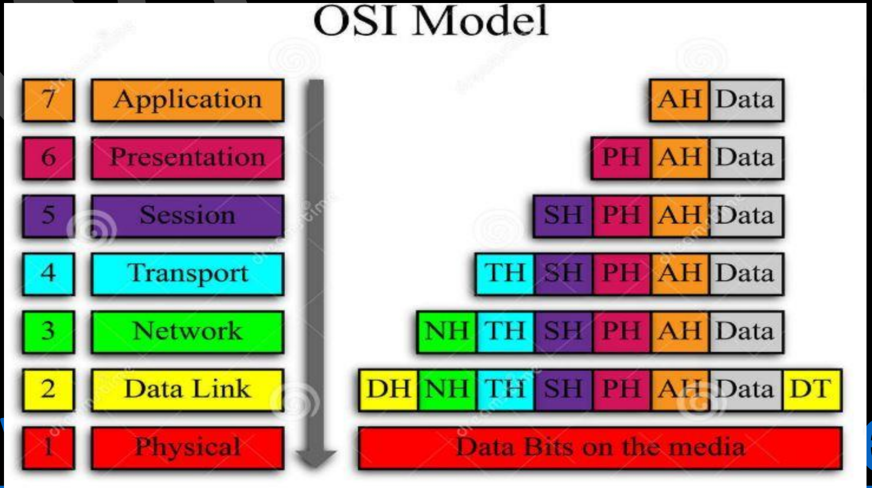
- **Local Area Network** (LAN) :
  - LAN is usually limited to a few kilometers of area.
  - It may be privately owned and could be a network inside an office on one of the floor of a building or a LAN could be a network consisting of the computers in an entire building.

- **Wide Area Network** (WAN) :
  - WAN is made of all the networks in a (geographically) large area.
  - The network in the entire state of UP could be a WAN.

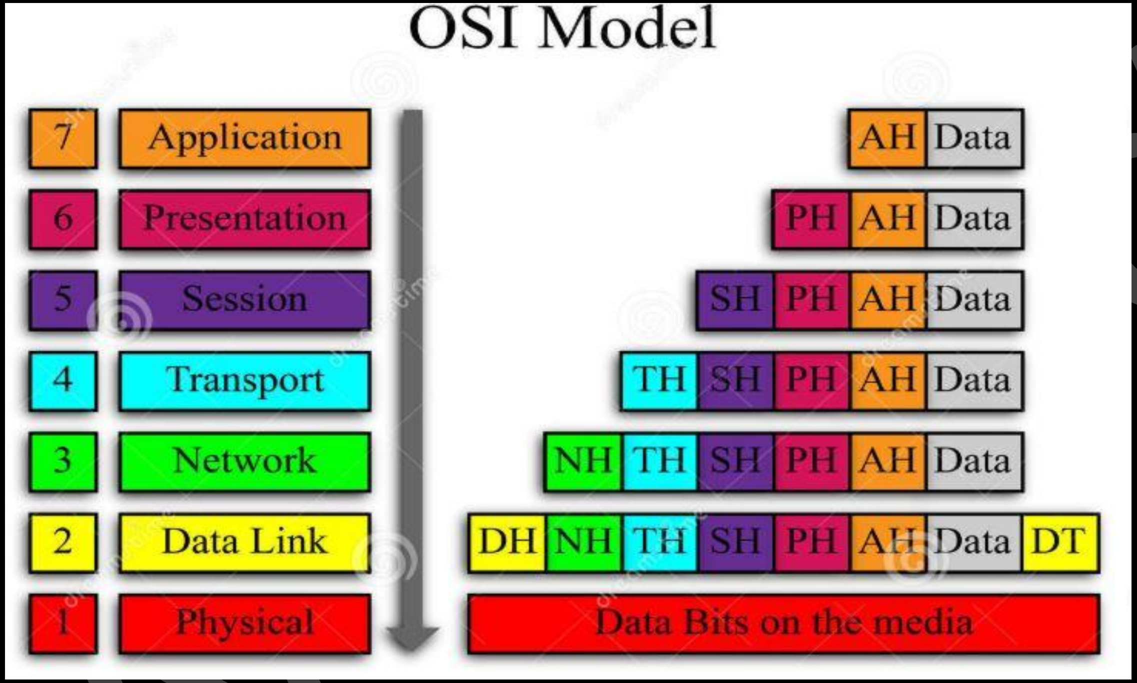
- **Metropolitan Area Network** (MAN) :
  - MAN is of size between LAN and WAN.
  - It is larger than LAN but smaller than WAN.
  - It may comprise the entire network in a city like Mumbai.

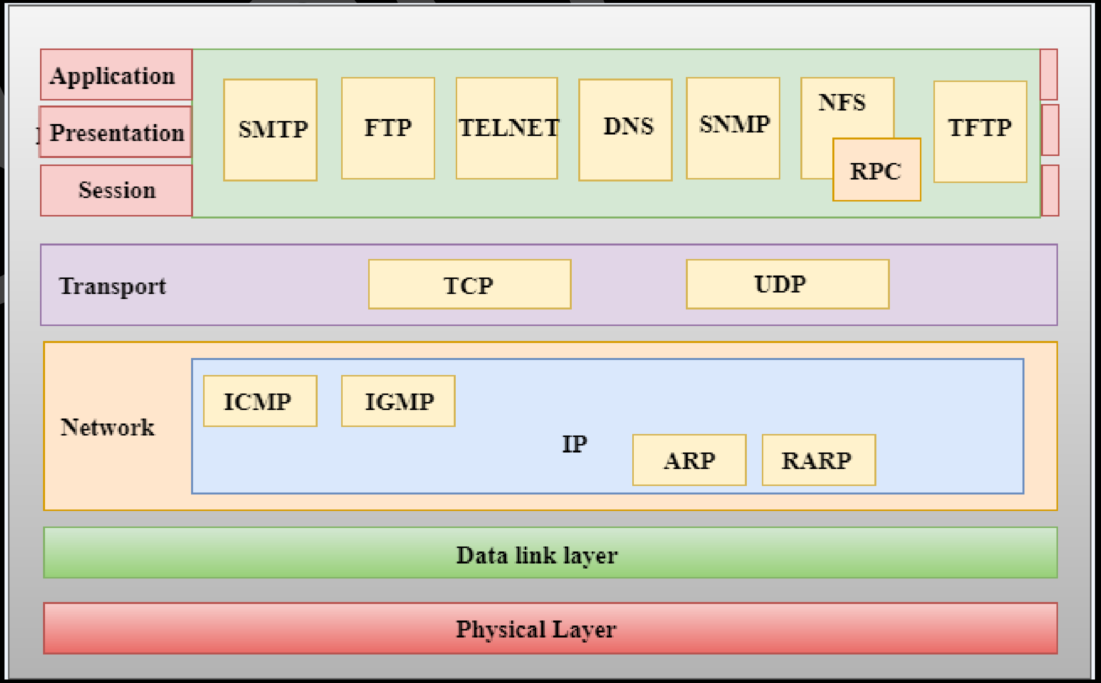
Network Models

- International standard organization (ISO)- proposed an open system interconnection (OSI) model that allows two system to communicate regardless of their architecture.



- The purpose of the OSI model is to show how to facilitate communication between different systems without requiring changes to the logic of the underlying hardware and software.
- The OSI model is not a protocol; it is a model for understanding and designing a network architecture that is flexible, robust, and interoperable. It consists of seven separate but related layers, each of which defines a part of the process of moving information across a network.





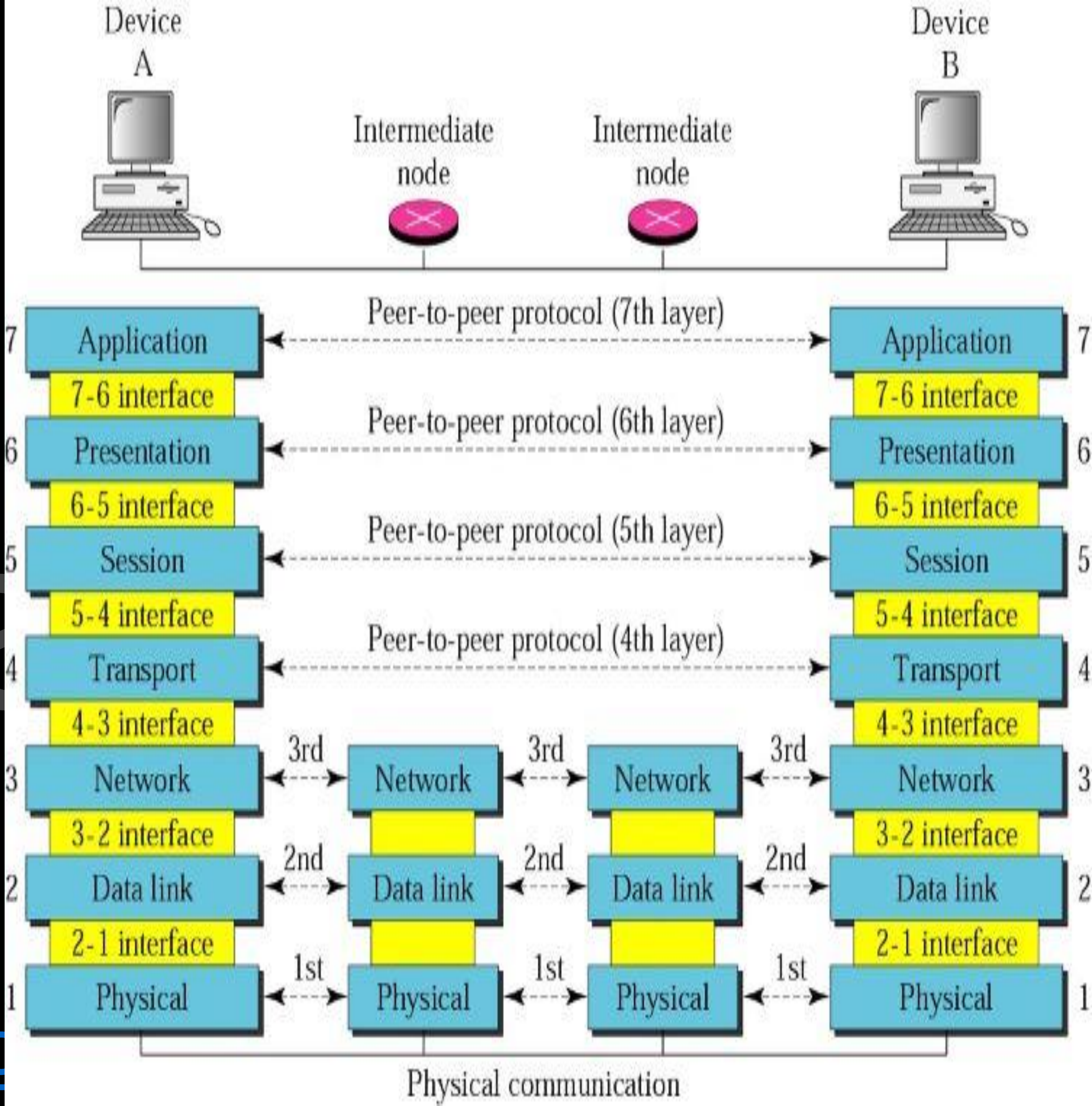
Directive Principles Constitution

Layered Architecture

1. The OSI model is composed of seven ordered layers, within a single machine, each layer calls upon the services of the layer just below it and provide services to the layer above it.

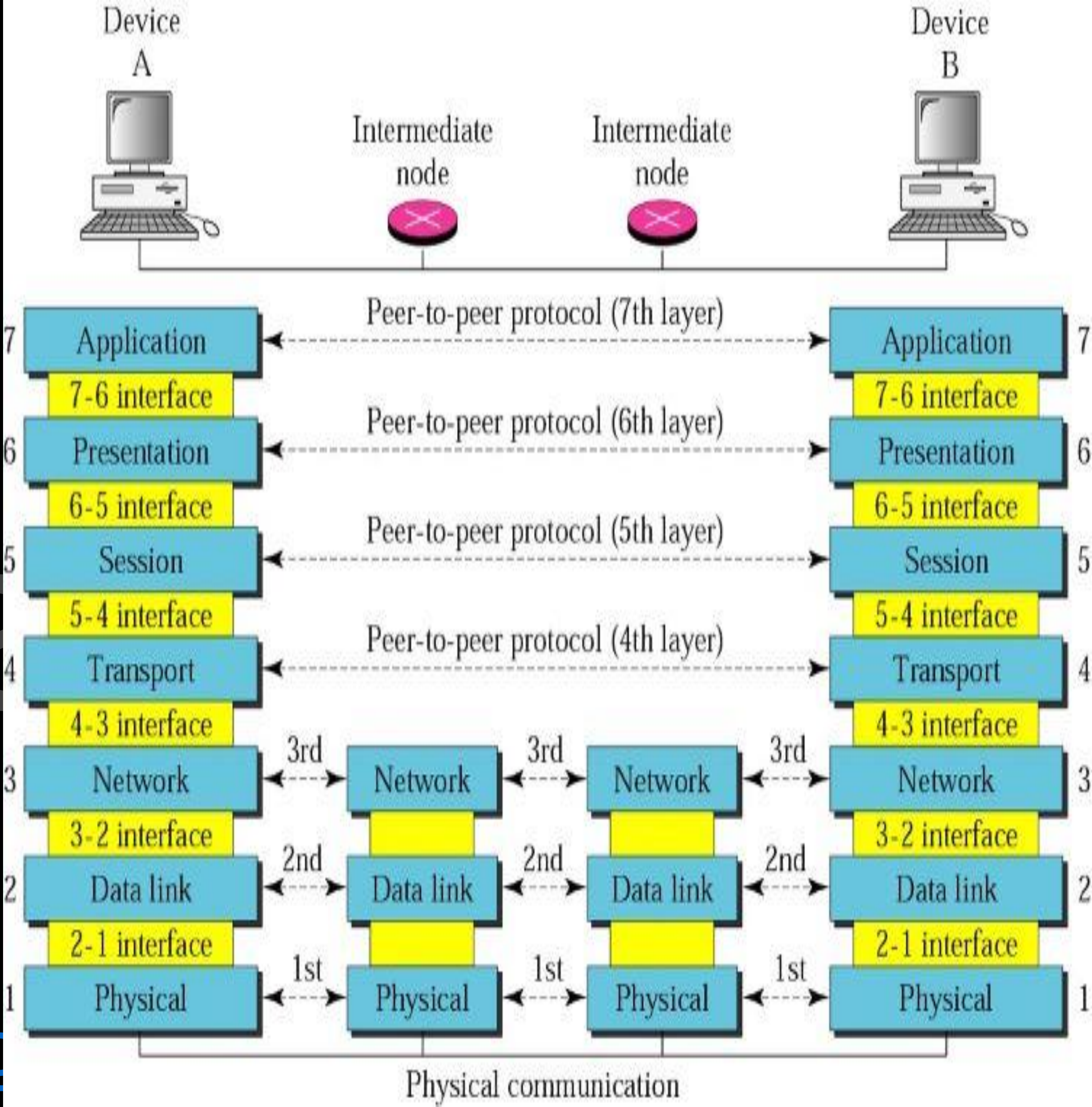
2. Between machines, layer x on one machine communicates with layer x on another machine. This communication is governed by an agreed-upon series of rules and conventions called protocols.

3. The processes on each machine that communicate at a given layer are called peer-to-peer processes.



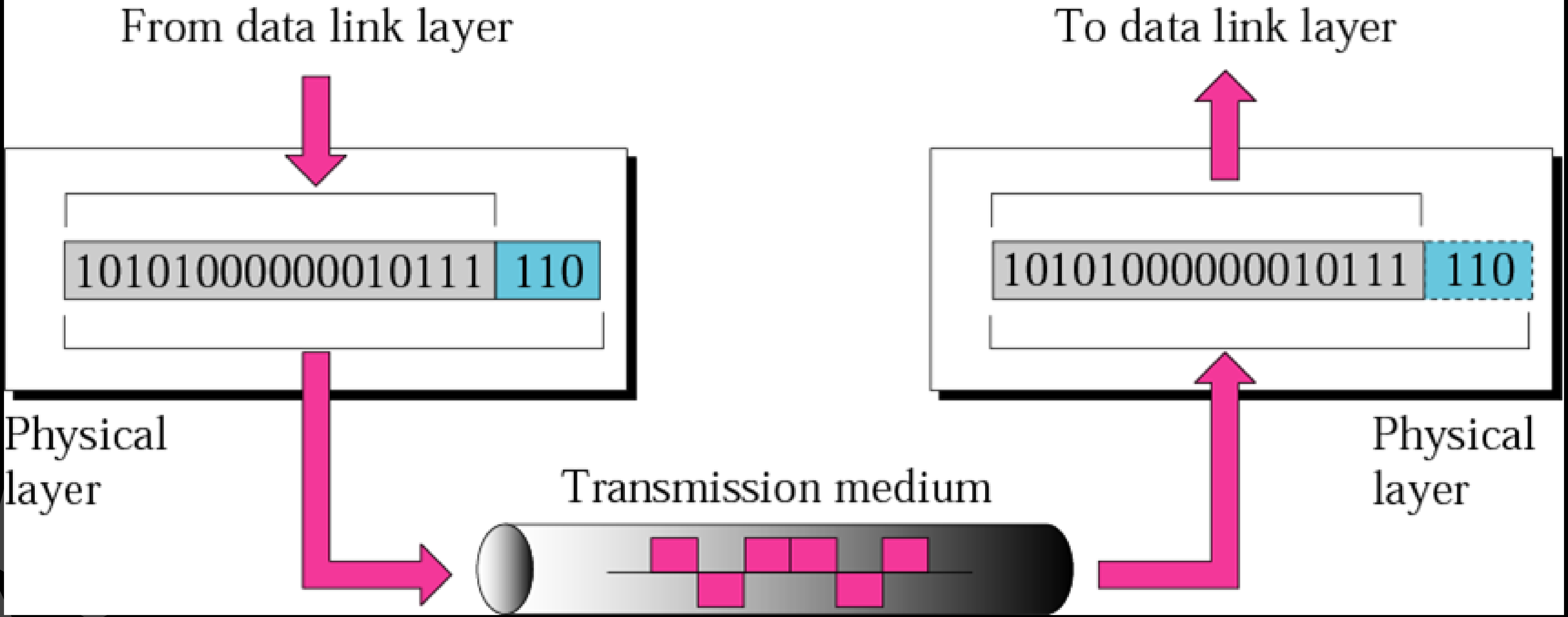
Peer-to-Peer Processes

- At the physical layer, communication is direct: device A sends a stream of bits to device B (through intermediate nodes).
- At the higher layers, communication must move down through the layers on device A, over to device B, and then back up through the layers.
- Each layer in the sending device adds its own information to the message it receives from the layer just above it and passes the whole package to the layer just below it.
- At layer 1 the entire package is converted to a form that can be transmitted to the receiving device.
- At the receiving machine, the message is unwrapped layer by layer, with each process receiving and removing the data meant for it.

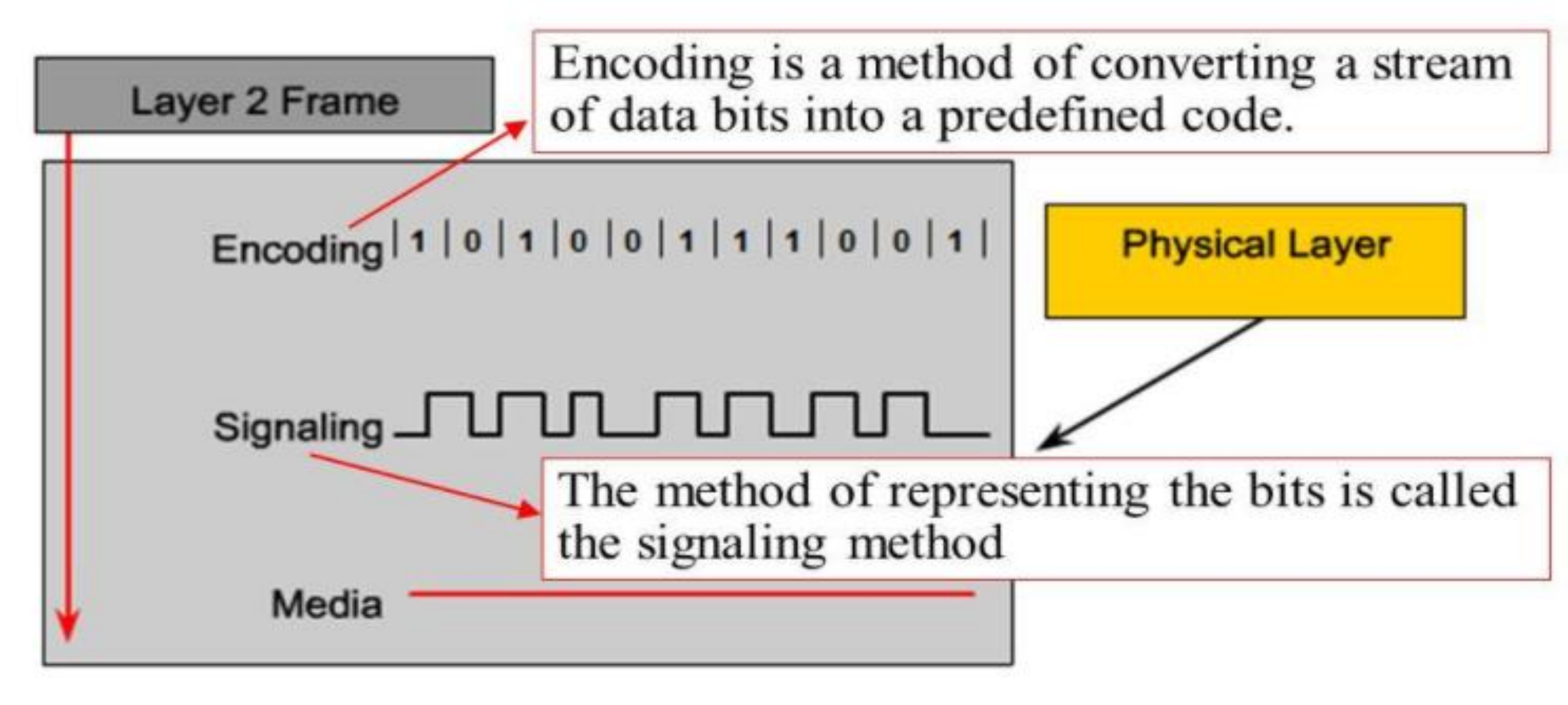


Physical layer

- The physical layer defines the **characteristics of the interface** between the devices and the transmission medium.



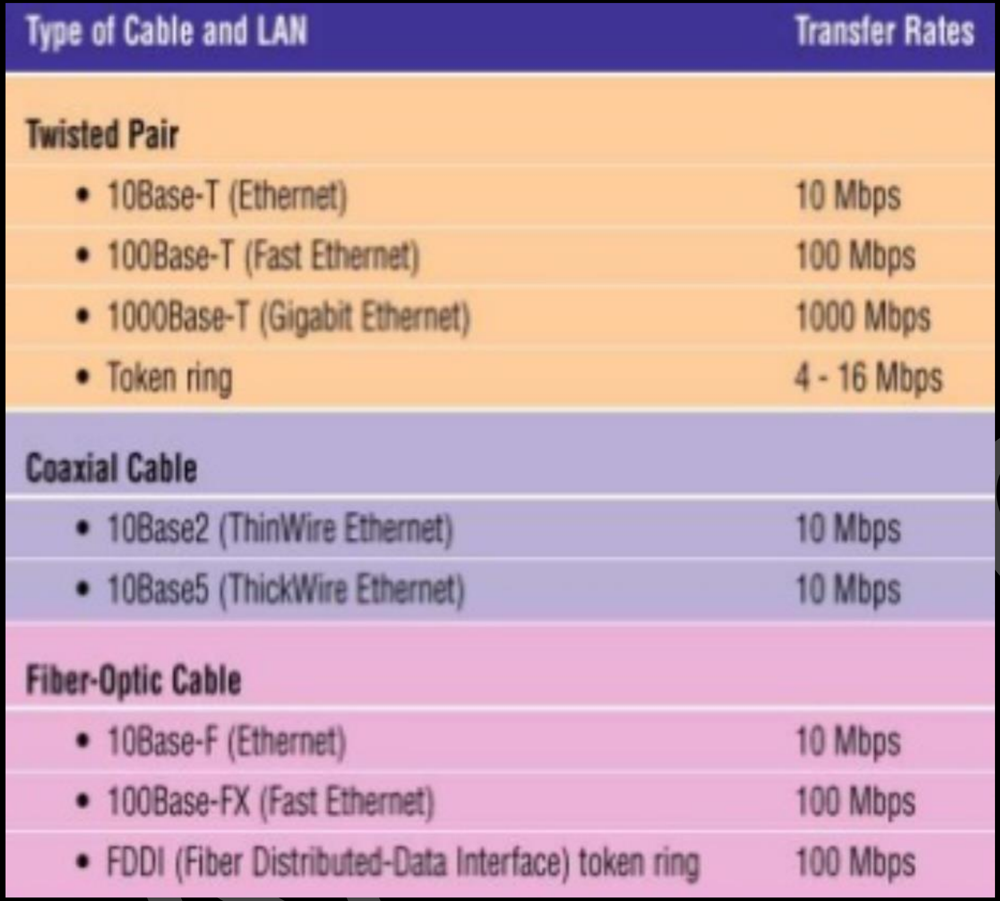
1. Representation of bits: The physical layer data consists of a stream of bits (sequence of 0s or 1s) with no interpretation. To be transmitted, bits must be encoded into signals- electrical or optical.



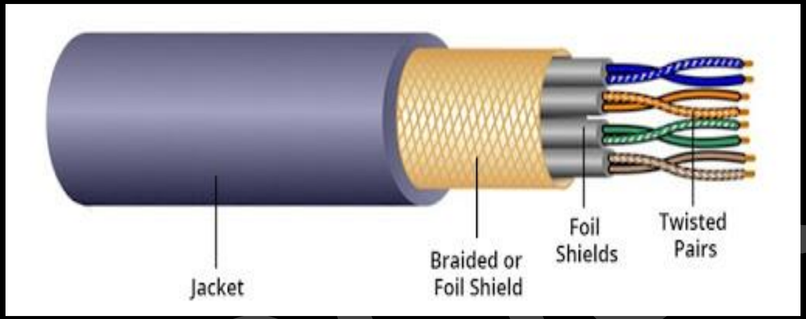
Encoding is a method of converting a stream of data bits into a predefined code.

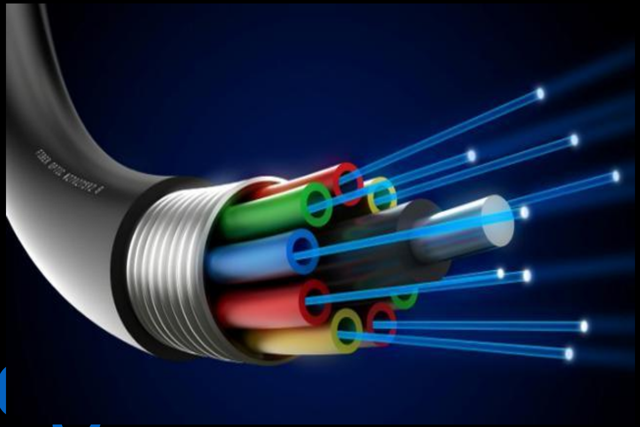
The method of representing the bits is called the signaling method

2. Data rate: The transmission rate-the number of bits sent each second-is also defined by the physical layer.

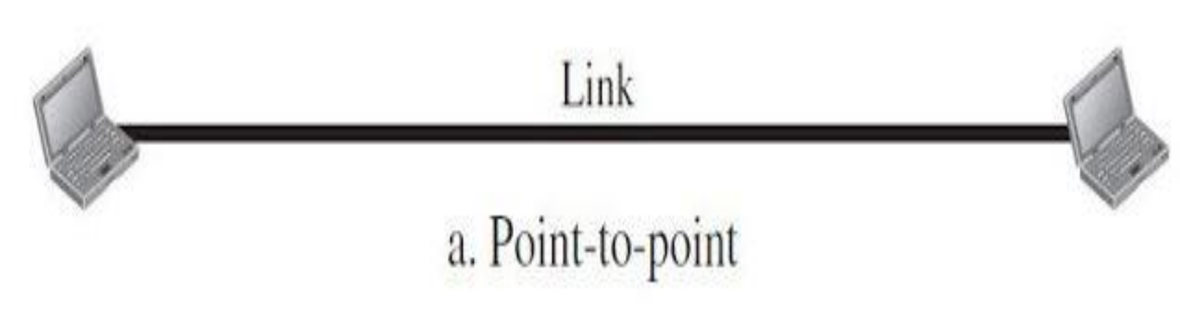


Type of Cable and LAN	Transfer Rates
Twisted Pair	
• 10Base-T (Ethernet)	10 Mbps
• 100Base-T (Fast Ethernet)	100 Mbps
• 1000Base-T (Gigabit Ethernet)	1000 Mbps
• Token ring	4 - 16 Mbps
Coaxial Cable	
• 10Base2 (ThinWire Ethernet)	10 Mbps
• 10Base5 (ThickWire Ethernet)	10 Mbps
Fiber-Optic Cable	
• 10Base-F (Ethernet)	10 Mbps
• 100Base-FX (Fast Ethernet)	100 Mbps
• FDDI (Fiber Distributed-Data Interface) token ring	100 Mbps

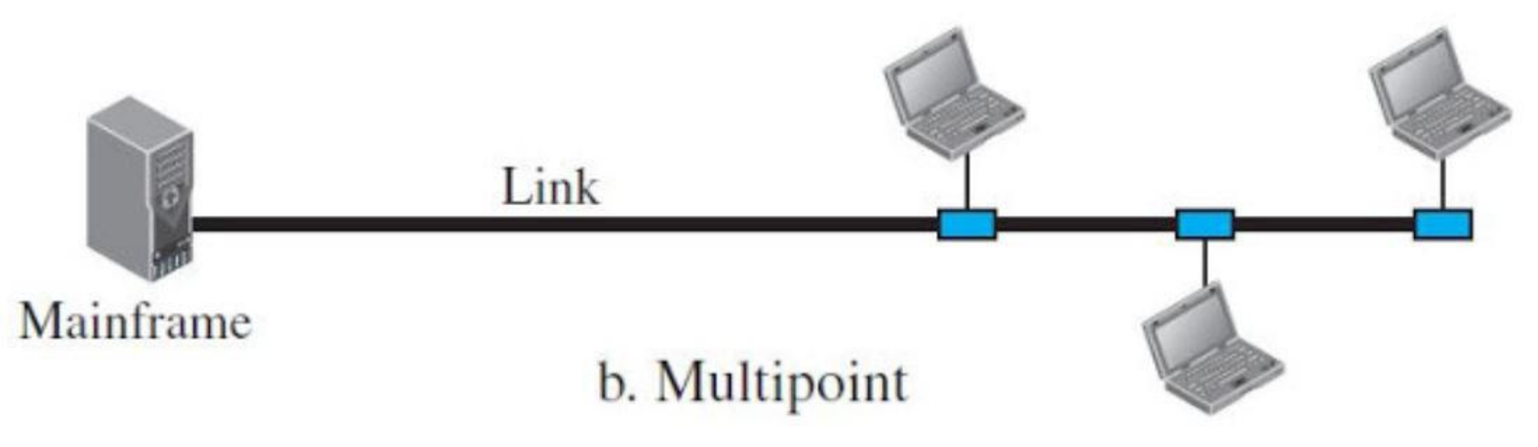




3. Line configuration: The physical layer is concerned with the connection of devices to the media.

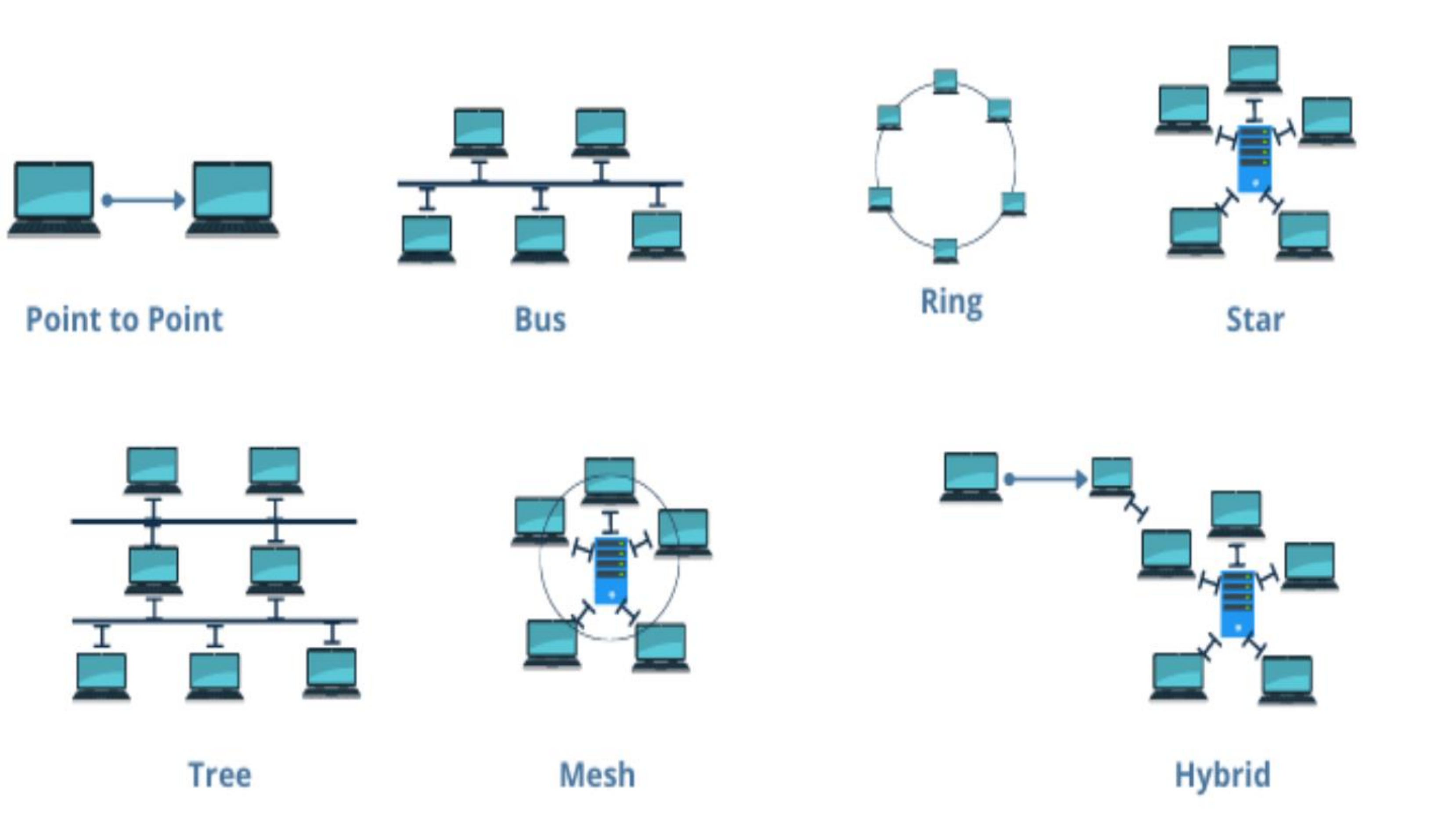


a. Point-to-point

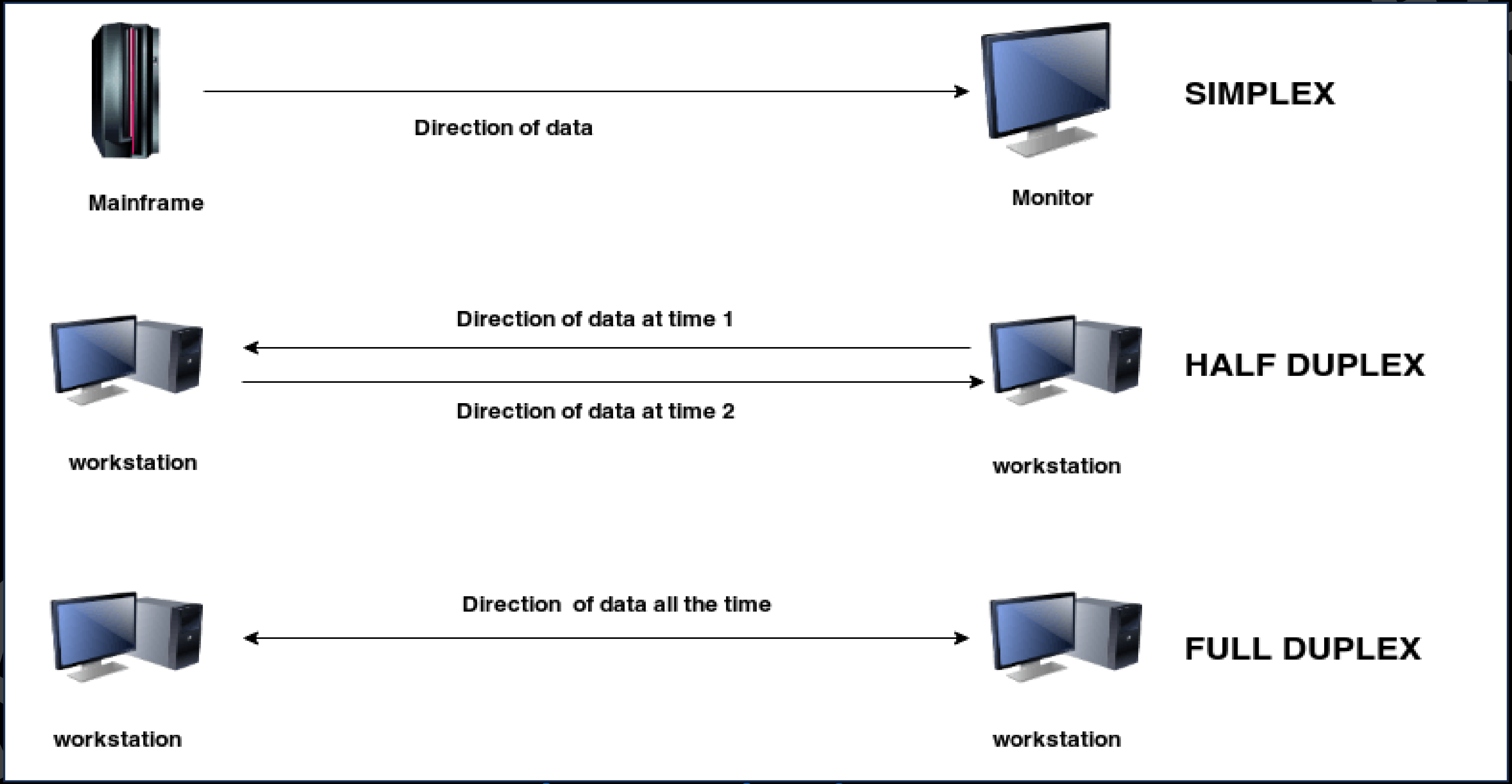


b. Multipoint

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

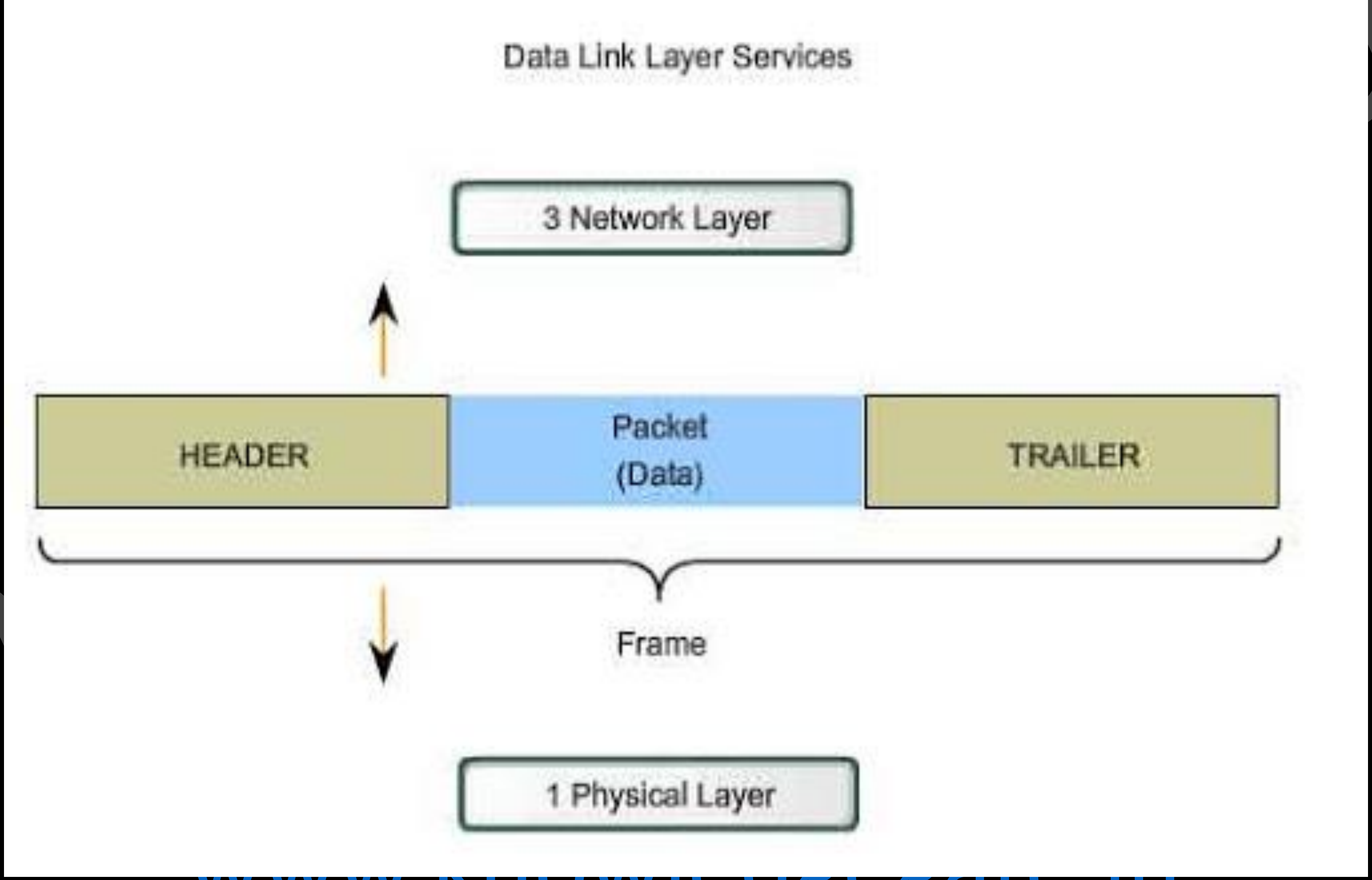


5. Transmission mode: The physical layer also defines the direction of transmission between two devices: simplex, half-duplex, or full-duplex.



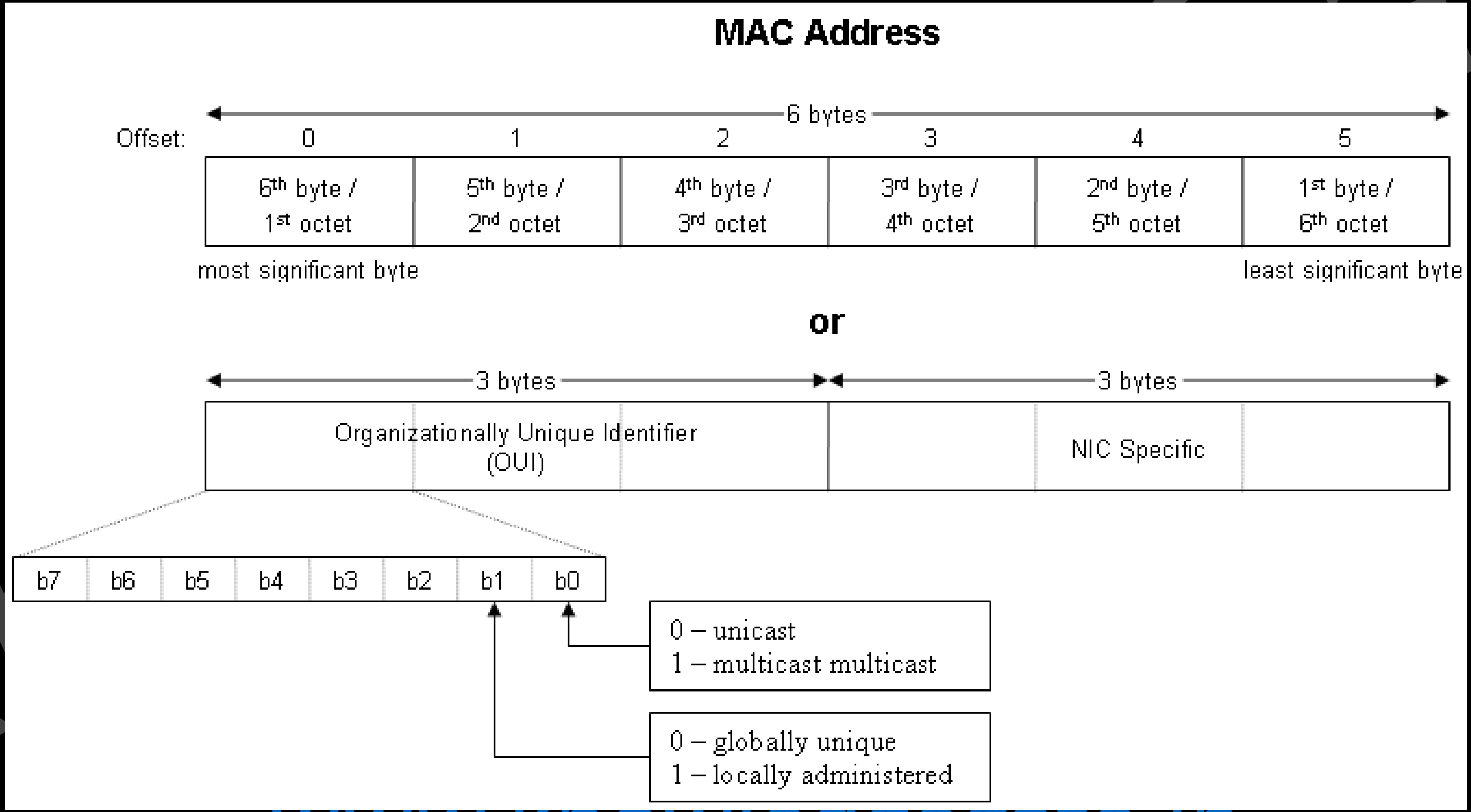
Data link layer

1. Framing: The data link layer divides the stream of bits received from the network layer into manageable data units called frames.



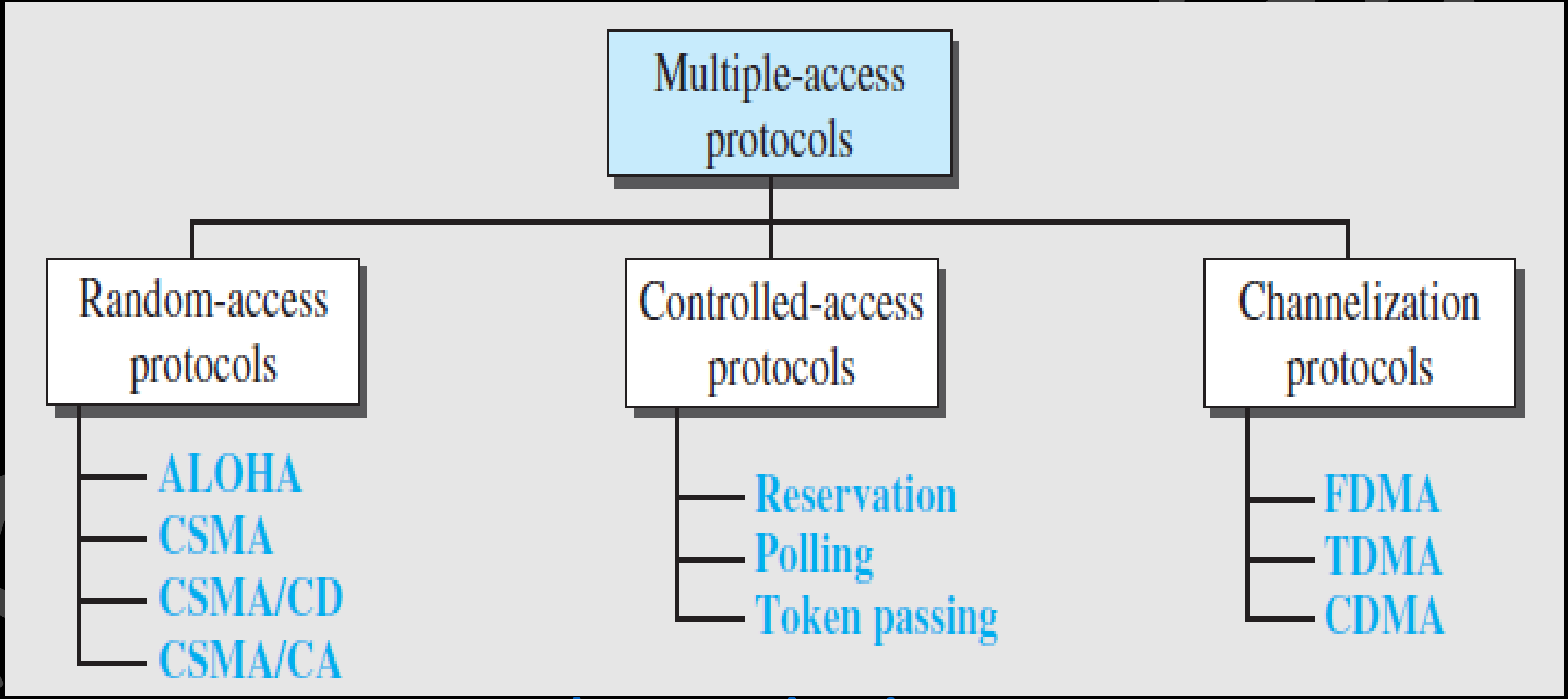
Data link layer

2. Physical addressing: If frames are to be distributed to different systems on the network, the data link layer adds a header to the frame to define the sender and/or receiver of the frame.



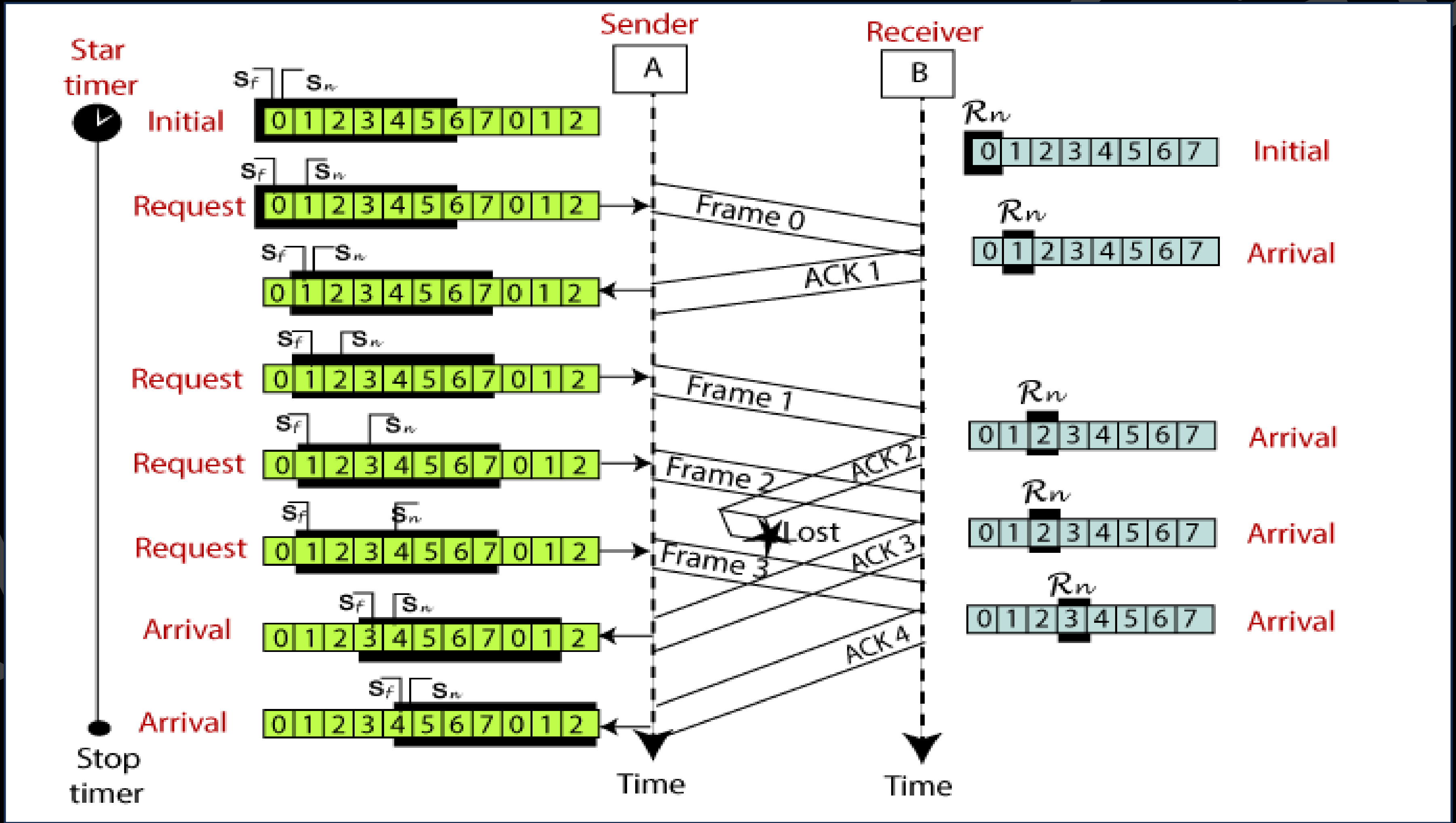
Data link layer

3. Access control: When two or more devices are connected to the same link, data link layer protocols are necessary to determine which device has control over the link at any given time.



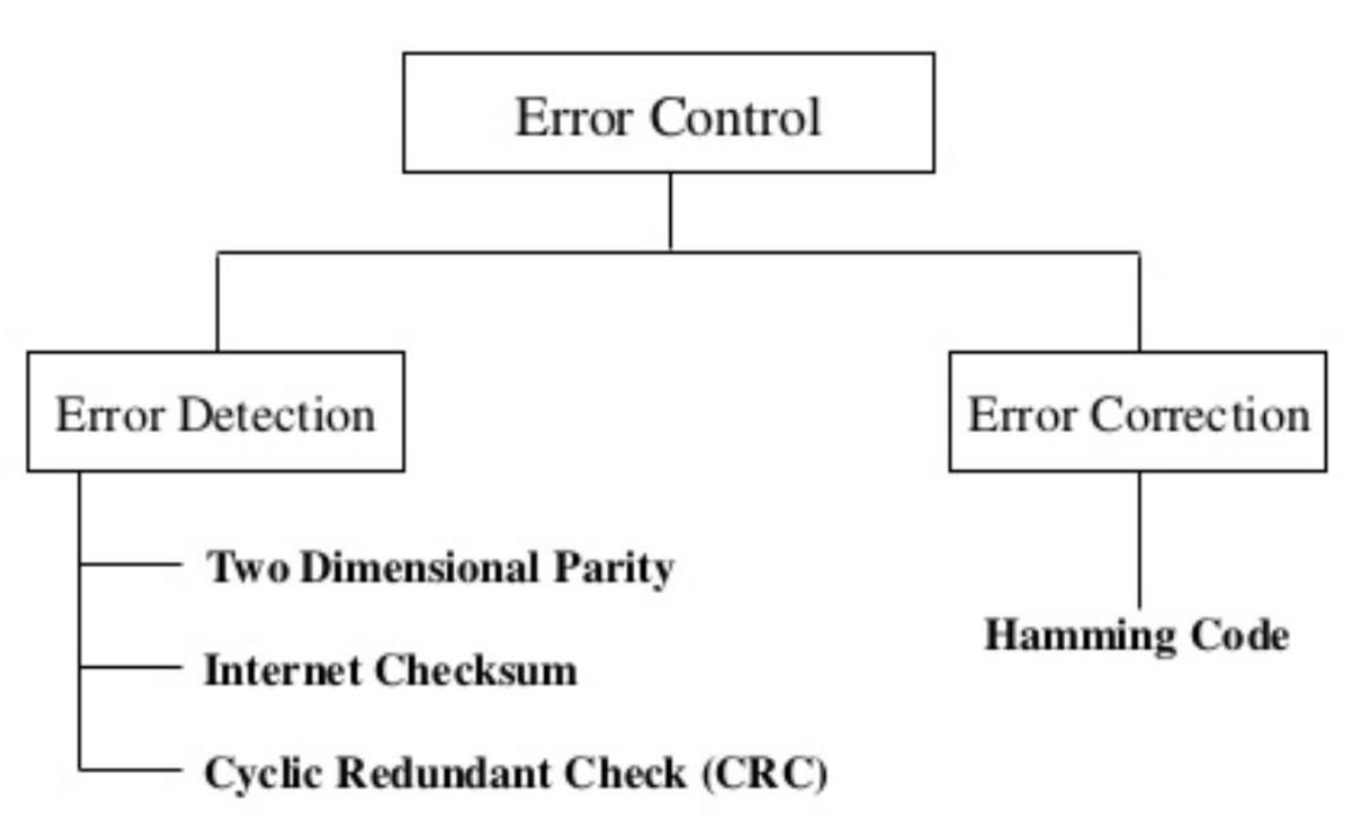
Data link layer

4. Flow control: If the rate at which the data are absorbed by the receiver is less than the rate at which data are produced in the sender, the data link layer imposes a flow control mechanism to avoid overwhelming the receiver.



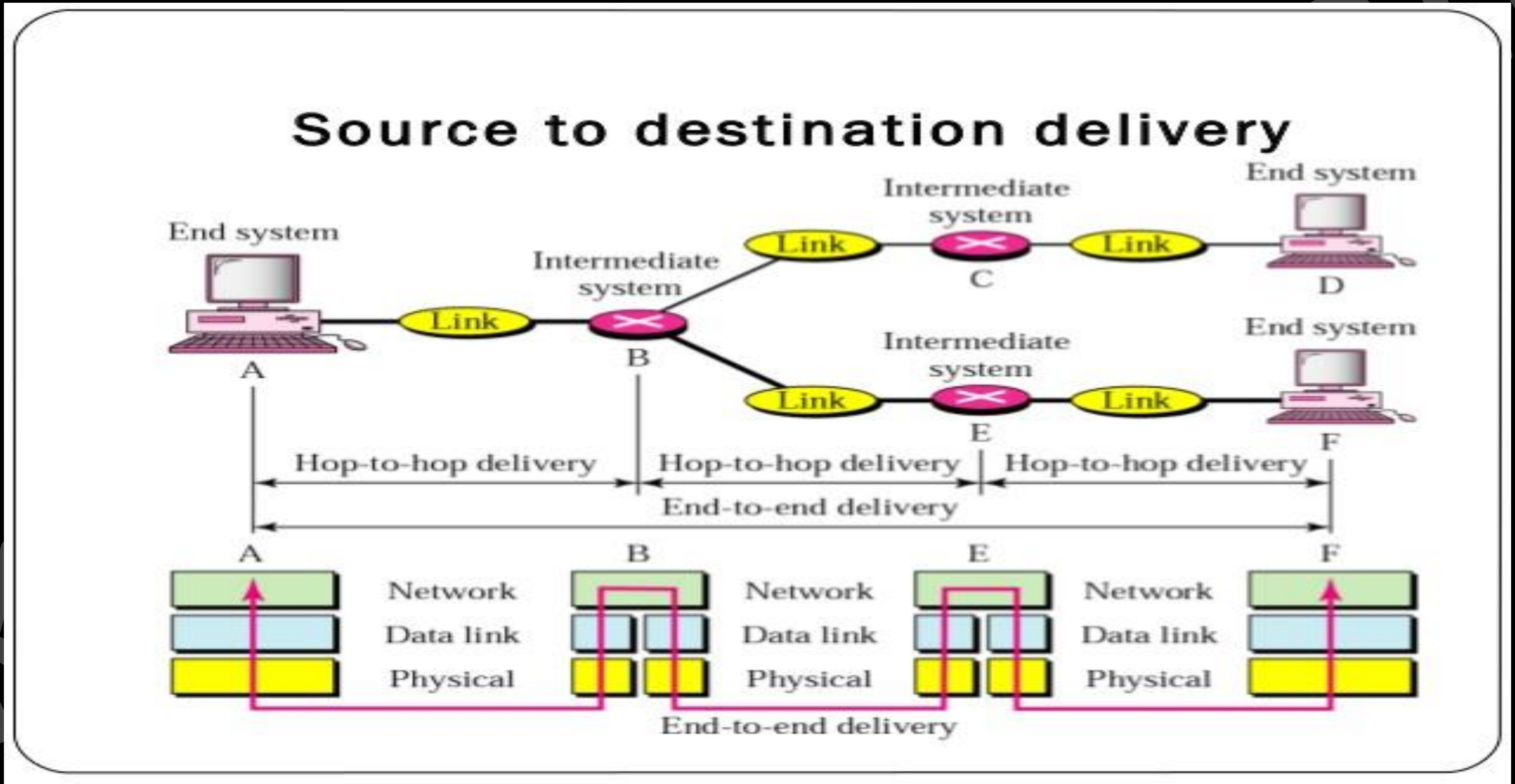
Data link layer

5. Error control: The data link layer adds reliability to the physical layer by adding mechanisms to detect and retransmit damaged or lost frames. It also uses a mechanism to recognize duplicate frames. Error control is normally achieved through a trailer added to the end of the frame.



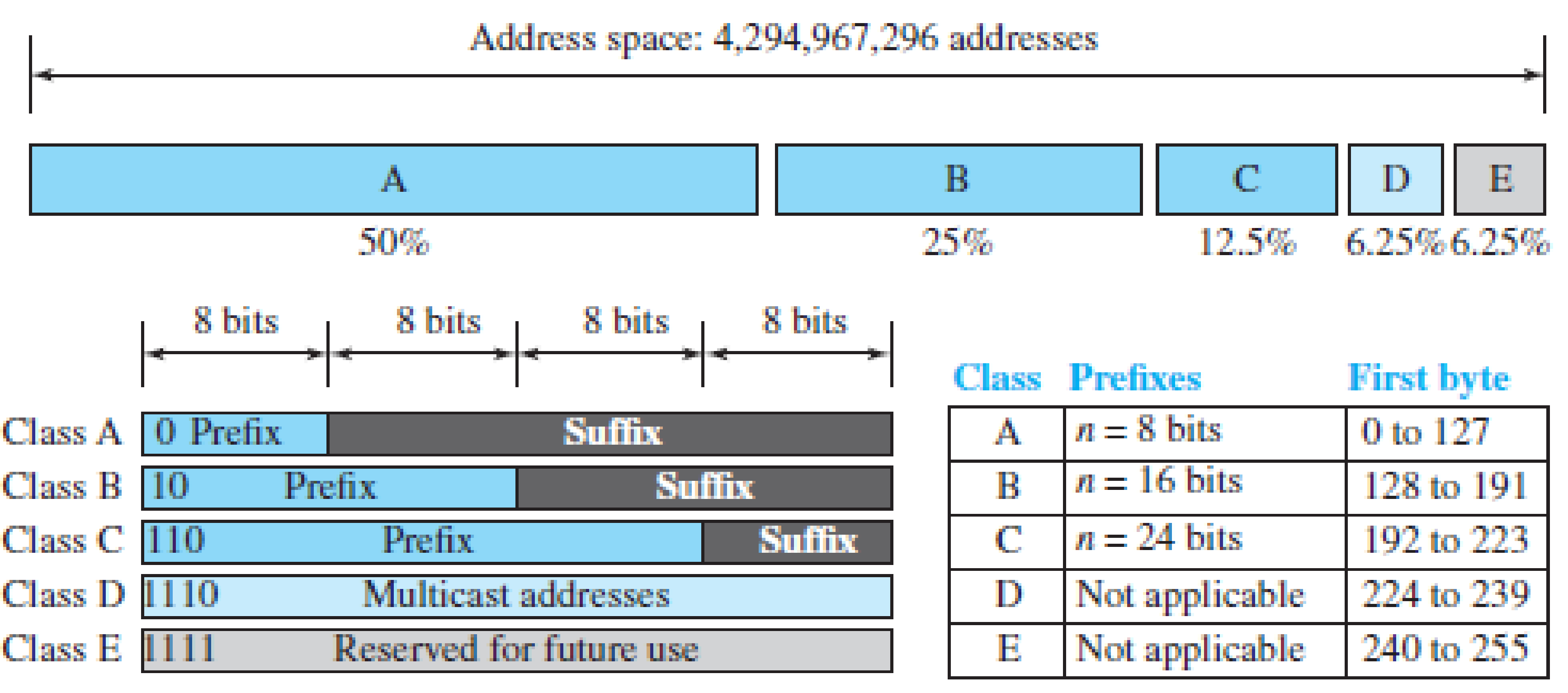
Network layer

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



Network layer

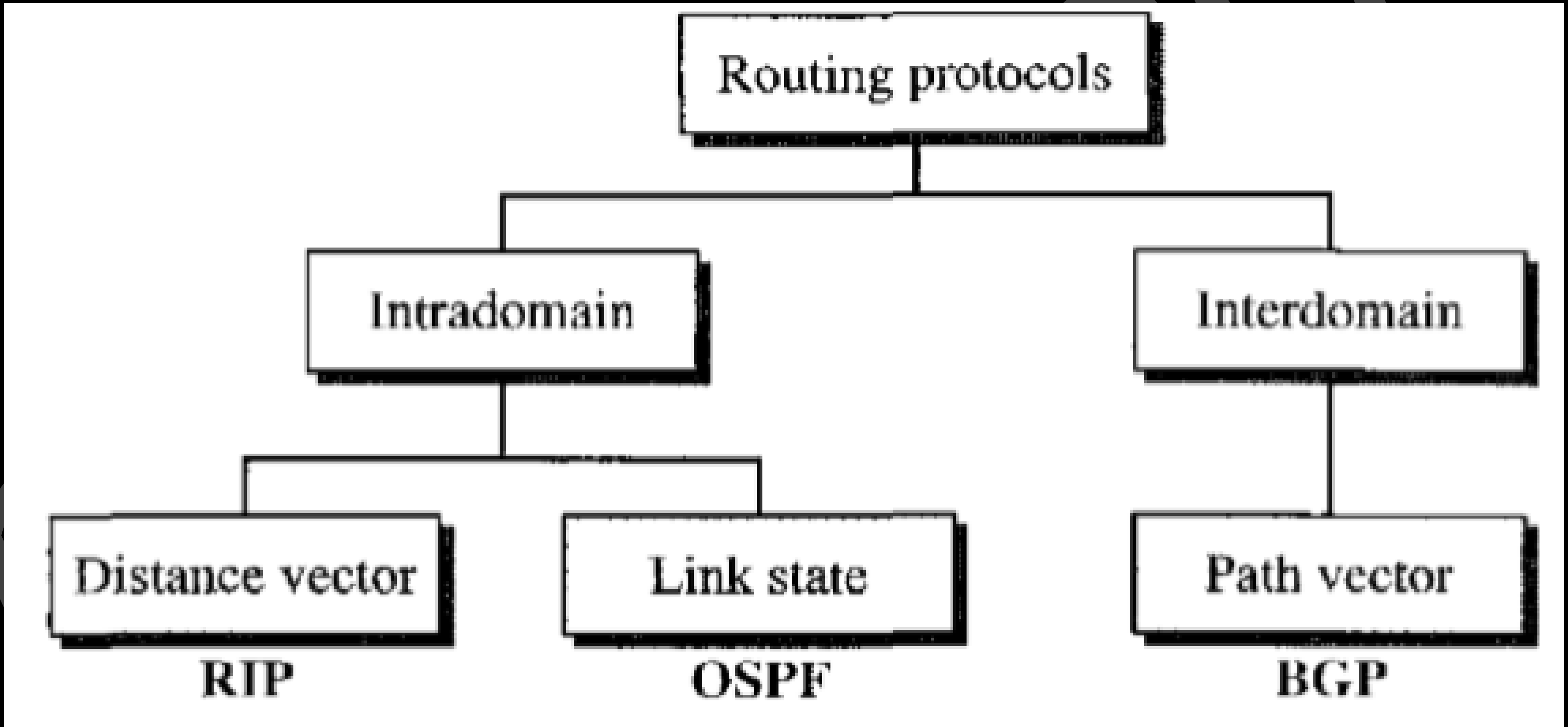
1. Logical addressing: If a packet passes the network boundary, we need another addressing system to help distinguish the source and destination systems. The network layer adds a header to the packet coming from the upper layer that, among other things, includes the logical addresses of the sender and receiver.



Class	Prefixes	First byte
A	$n = 8$ bits	0 to 127
B	$n = 16$ bits	128 to 191
C	$n = 24$ bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

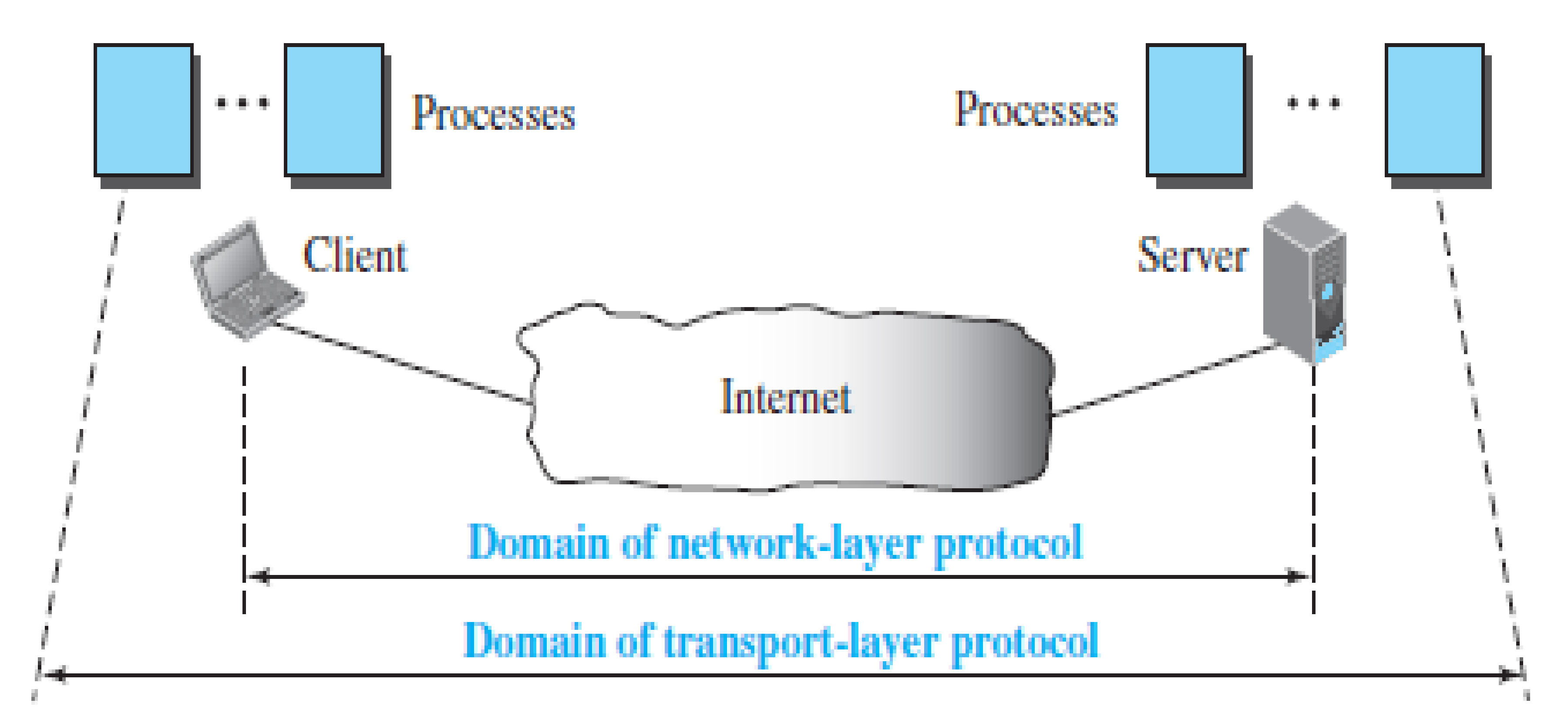
Network layer

2. Routing: When independent networks or links are connected to create internetworks (network of networks) or a large network, the connecting devices (called routers or switches) route or switch the packets to their final destination. One of the functions of the network layer is to provide this mechanism.



Transport layer

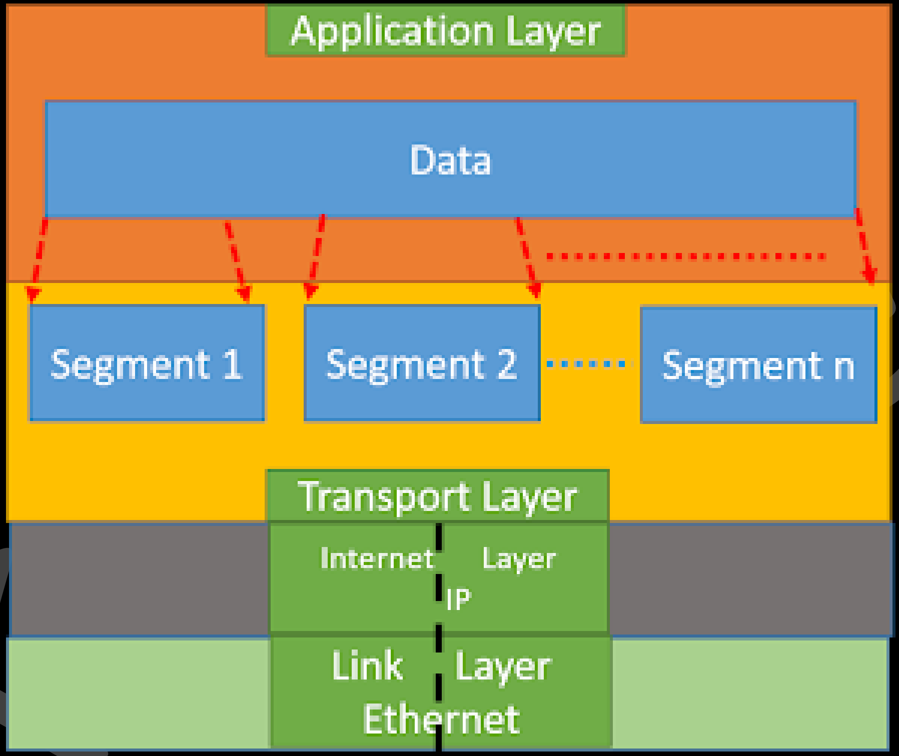
1. Service-point addressing: The transport layer header must include a type of address called a service-point address (or port address). The network layer gets each packet to the correct computer; the transport layer gets the entire message to the correct process on that computer. The transport layer is responsible for process-to-process delivery of the entire message.

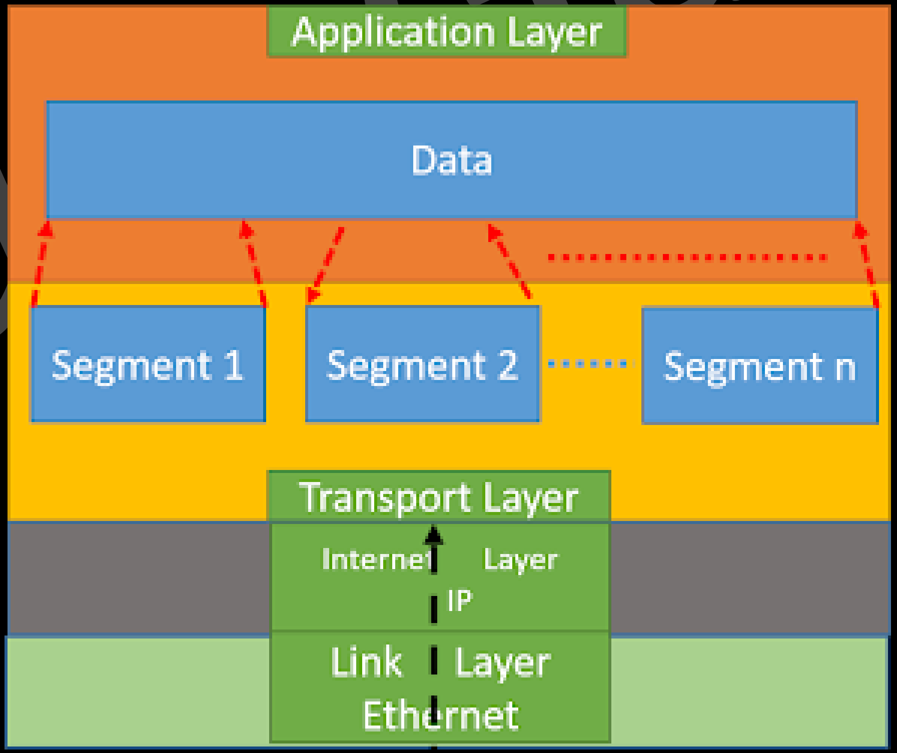


Processes
Processes
Client
Server
Internet
Domain of network-layer protocol
Domain of transport-layer protocol

Transport layer

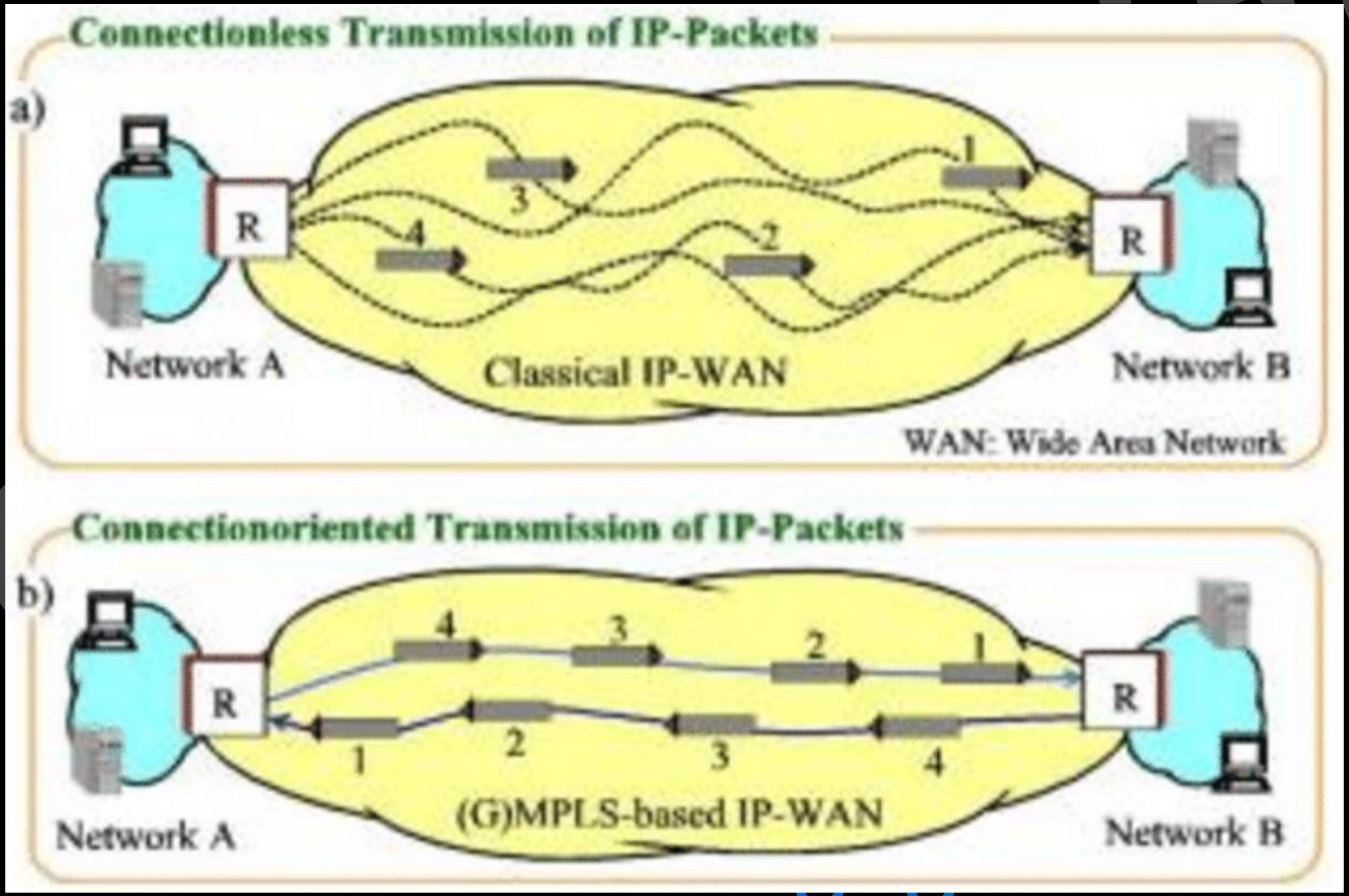
2. Segmentation and reassembly: A message is divided into transmittable segments, with each segment containing a sequence number. These numbers enable the transport layer to reassemble the message correctly upon arriving at the destination and to identify and replace packets that were lost in transmission.





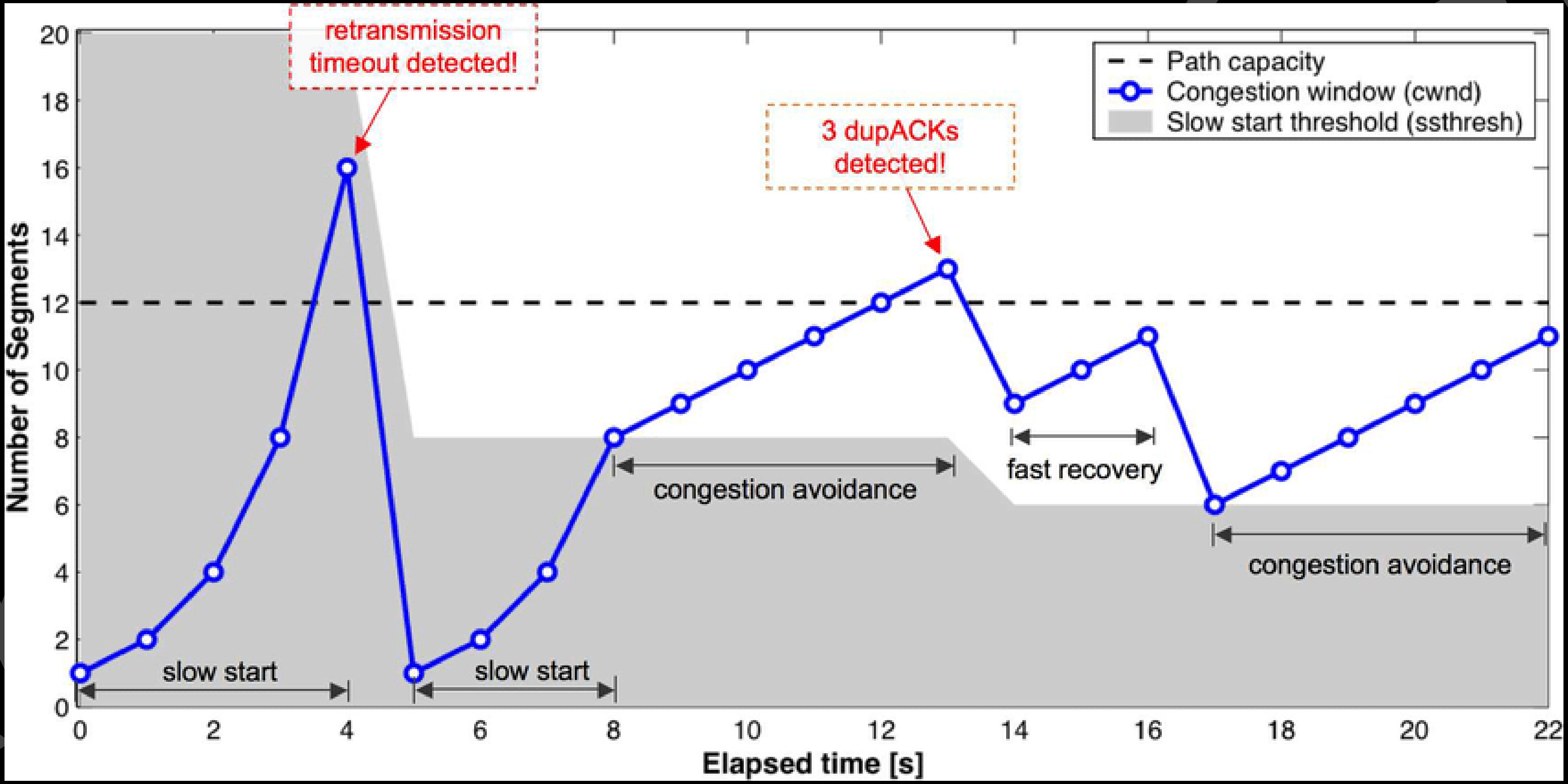
Transport layer

3. Connection control: The transport layer can be either connectionless or connection oriented. A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine. A connection-oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data are transferred, the connection is terminated.



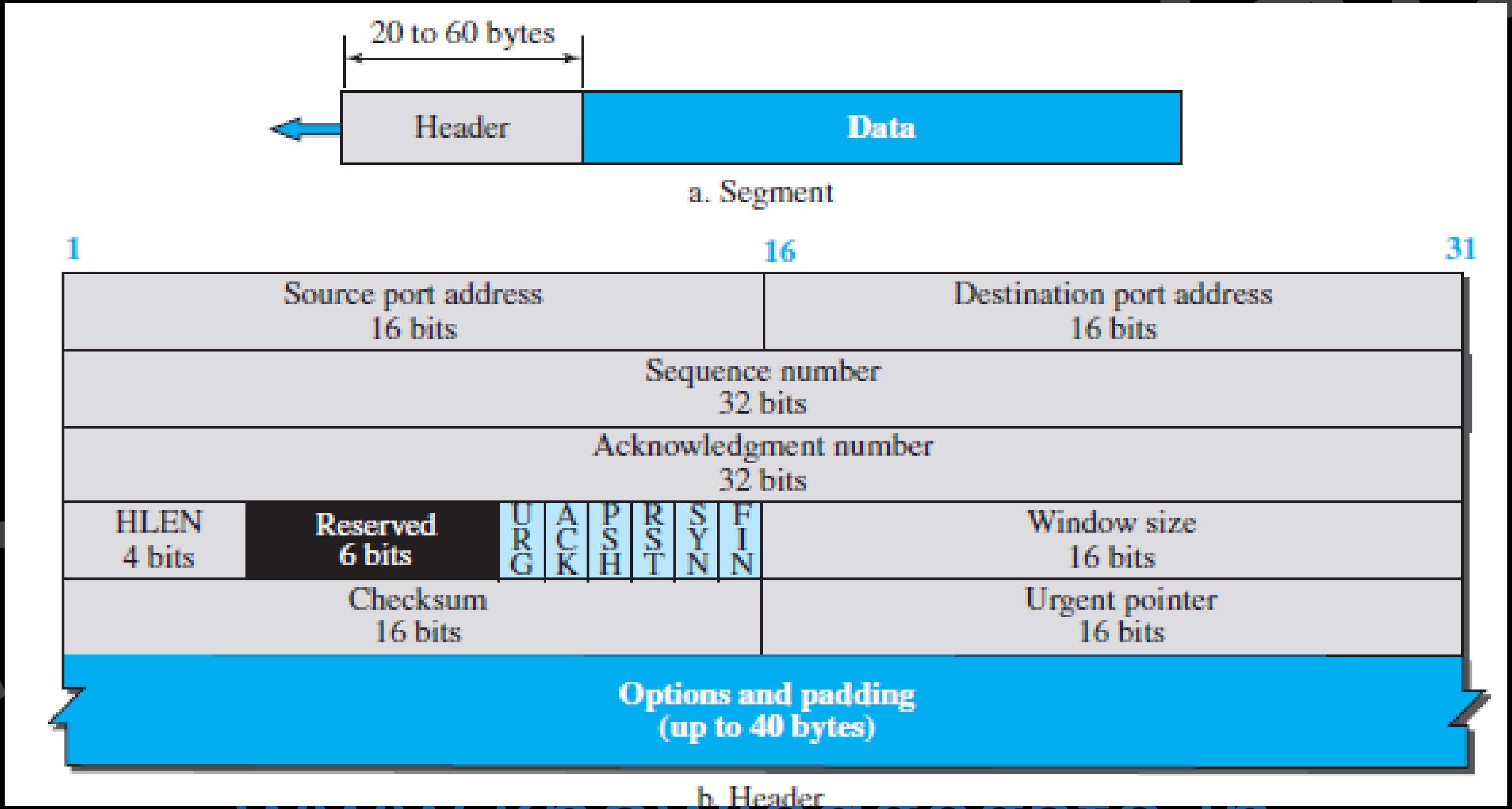
Transport layer

4. Flow control: Like the data link layer, the transport layer is responsible for flow control. However, flow control at this layer is performed end to end rather than across a single link.



Transport layer

5. Error control: Like the data link layer, the transport layer is responsible for error control. However, error control at this layer is performed process-to process rather than across a single link. The sending transport layer makes sure that the entire message arrives at the receiving transport layer without error (damage, loss, or duplication). Error correction is usually achieved through retransmission.



a. Segment

b. Header

Session layer

- The session layer is the **network dialog controller**. It establishes, maintains, and synchronizes the interaction among communicating systems.

1. The session layer is responsible for **dialog control and synchronization**.

2. Dialog control: The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either half duplex (one way at a time) or full-duplex (two ways at a time) mode.

3. Synchronization: The session layer allows a process to add checkpoints, or synchronization points, to a stream of data.

Presentation layer

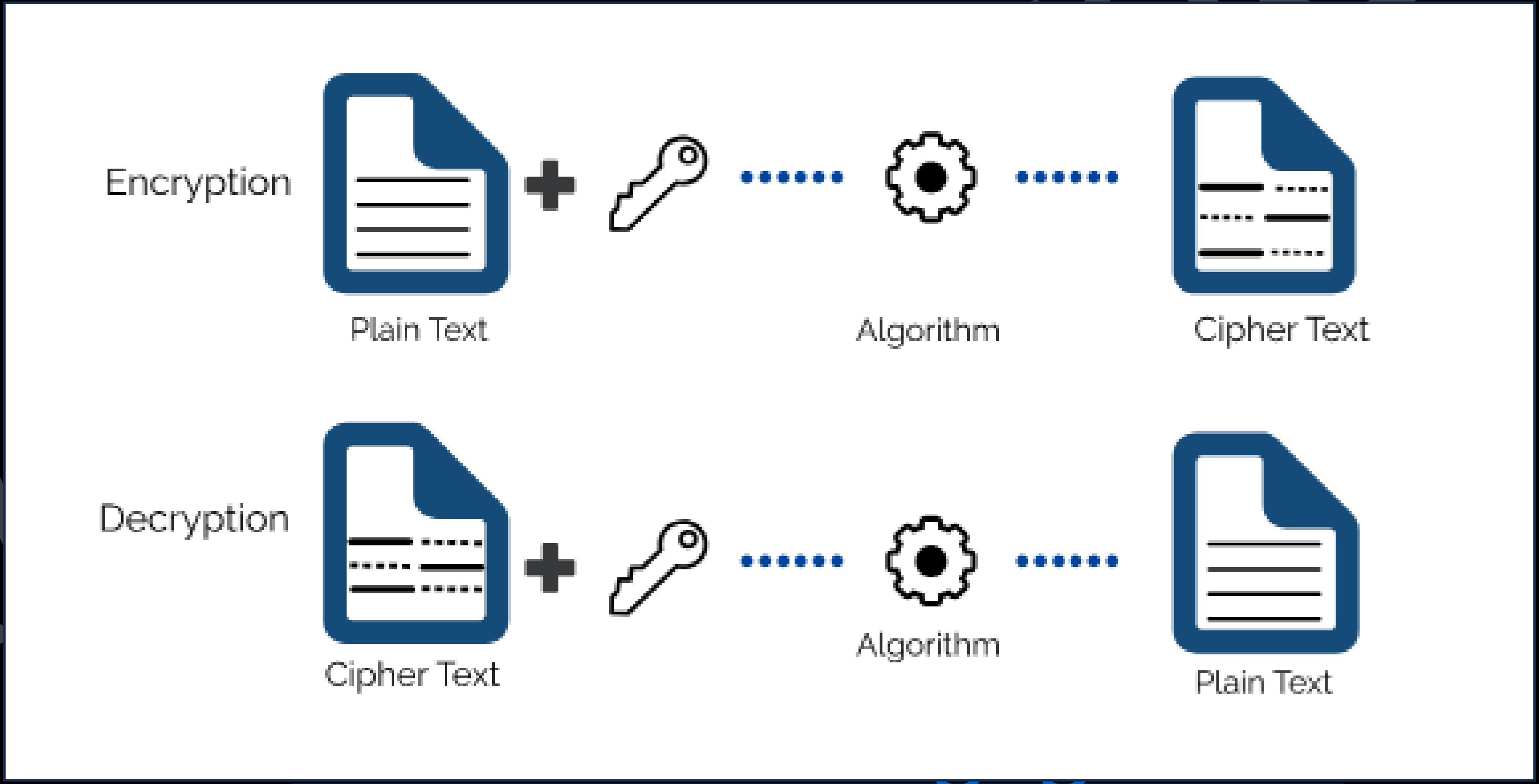
1. **Translation**: The processes (running programs) in two systems are usually exchanging information in the form of character strings, numbers, and so on.

- The information must be changed to bit streams before being transmitted. Because different computers use different encoding systems, the presentation layer is responsible for interoperability between these different encoding methods.
- The presentation layer at the sender changes the information from its sender-dependent format into a common format. The presentation layer at the receiving machine changes the common format into its receiver-dependent format.

Presentation layer

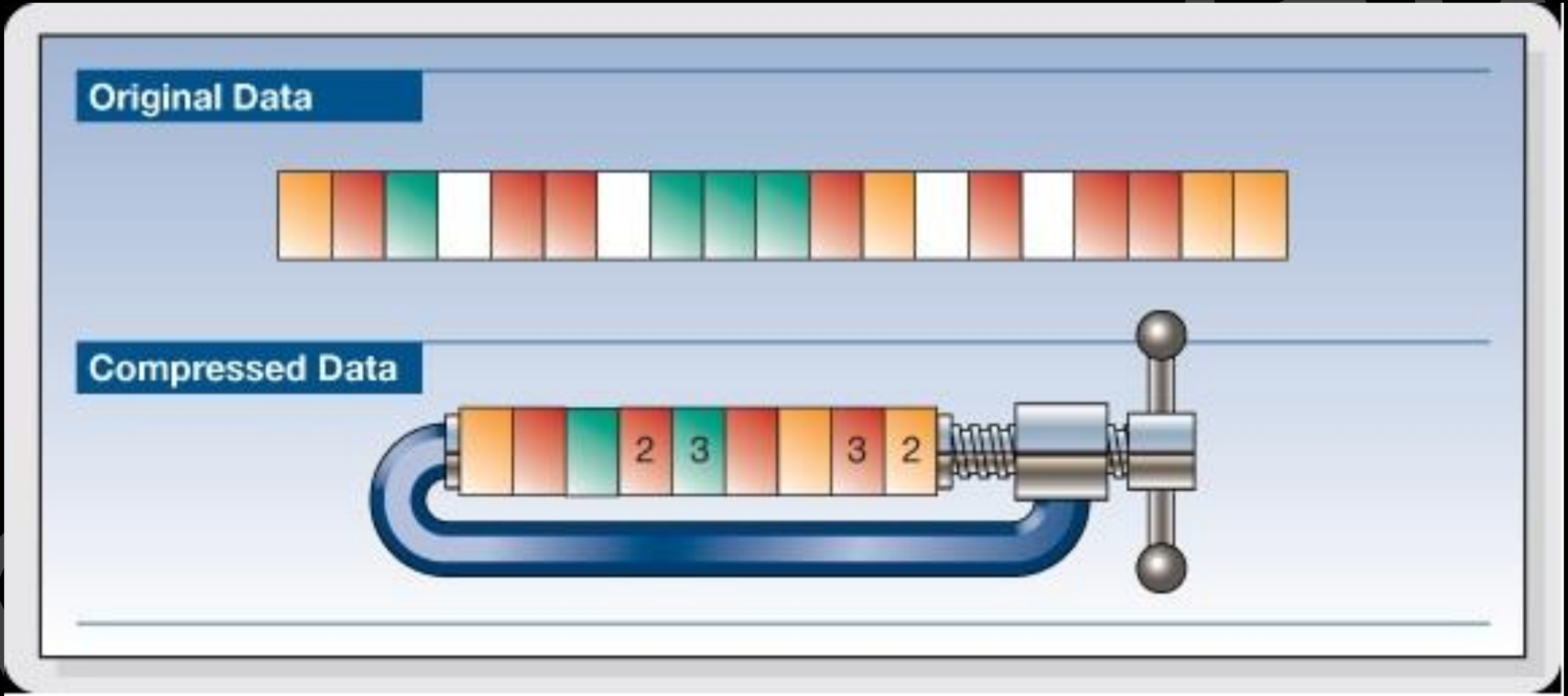
2. Encryption: To carry sensitive information, a system must be able to ensure privacy. Encryption means that the sender transforms the original information to another form and sends the resulting message out over the network.

- Decryption reverses the original process to transform the message back to its original form.



Presentation layer

3. Compression: Data compression reduces the number of bits contained in the information. Data compression becomes particularly important in the transmission of multimedia such as text, audio, and video.



Application layer

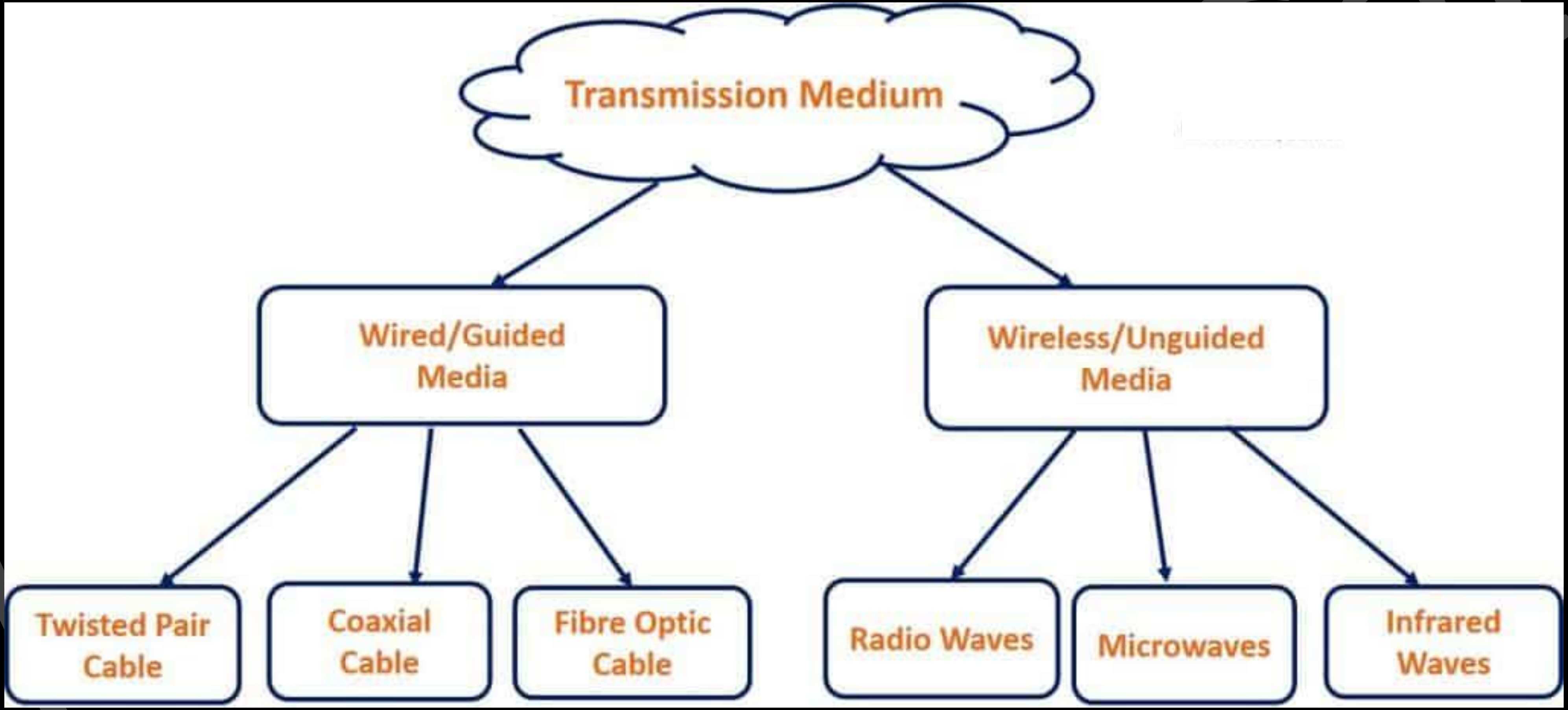
- The application layer enables the user, whether human or software, to access the network.
- It provides user interfaces and support for services such as electronic mail, remote file access and transfer, shared database management, and other types of distributed information services.

Services

1. **Network virtual terminal**: A network virtual terminal is a software version of a physical terminal, and it allows a user to log on to a remote host. To do so, the application creates a software emulation of a terminal at the remote host. The user's computer talks to the software terminal which, in turn, talks to the host, and vice versa. The remote host believes it is communicating with one of its own terminals and allows the user to log on.
2. **File transfer, access, and management**: This application allows a user to access files in a remote host (to make changes or read data), to retrieve files from a remote computer for use in the local computer, and to manage or control files in a remote computer locally.
3. **Mail services**: This application provides the basis for e-mail forwarding and storage.
4. **Directory services**: This application provides distributed database sources and access for global information about various objects and services.

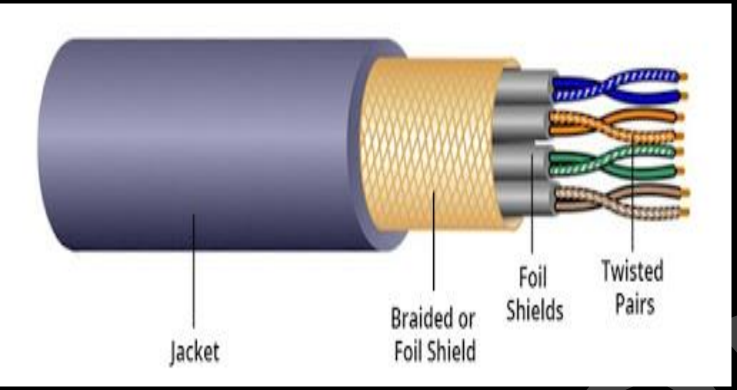
Transmission media

- (layer-0) can broadly be defined anything that can carry information from source to destination.

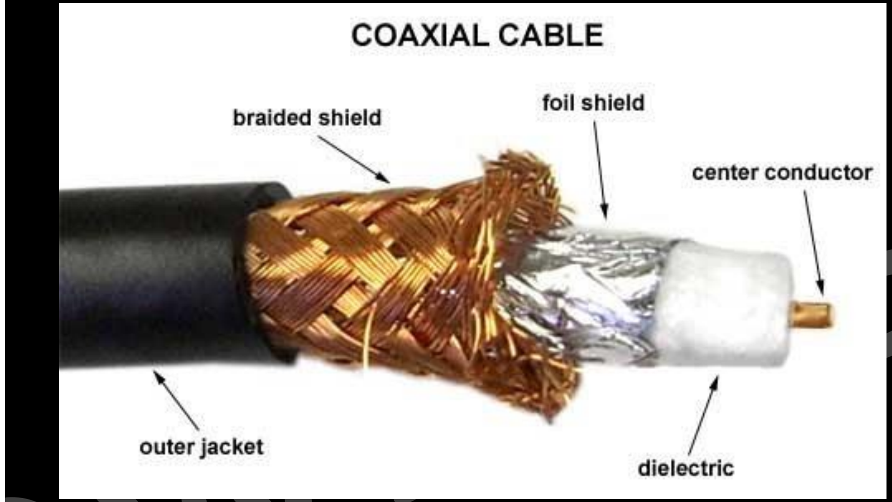


Guided media

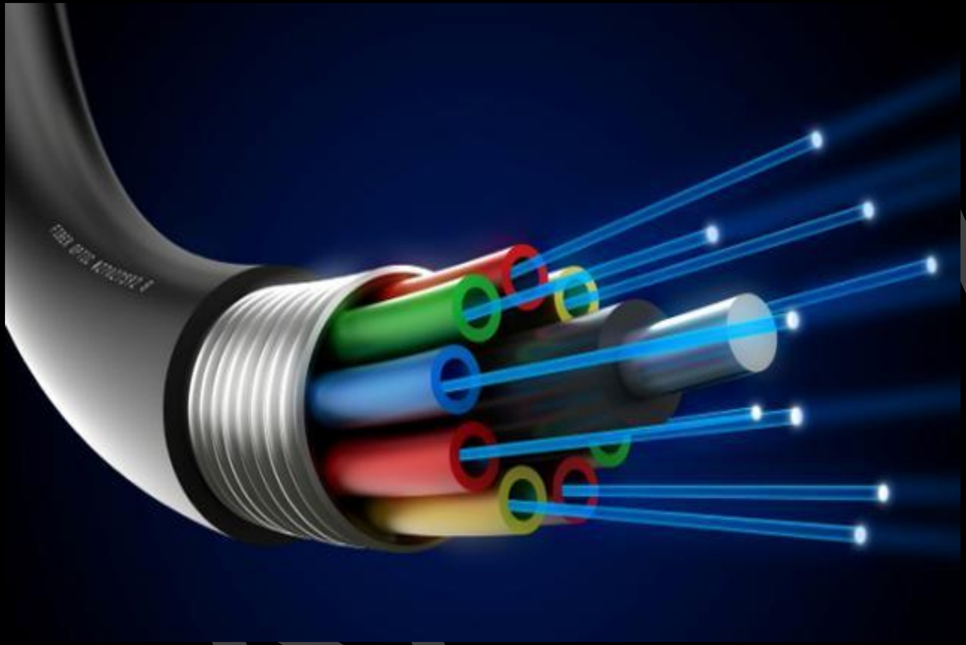
- Are those which provide a connection from one device to another.
- **Twisted pair cable** - Consists of two conductors (copper), each with it’s own plastic insulation, twisted together. (shielded and unshielded twisted pair of cables)(telephone line)

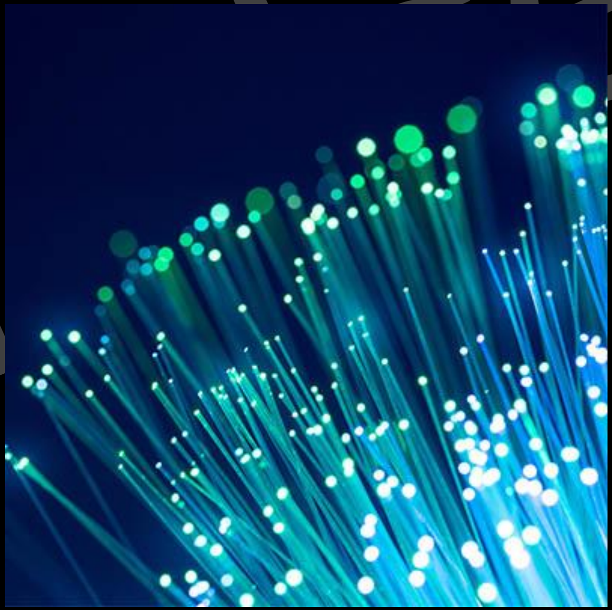


- **Coaxial Cable** – Has a central core conductor of solid wire enclosed in an insulating sheath, which in turn, encased in an outer conductor of metal foil, braid or a combination of two. (Cable tv)



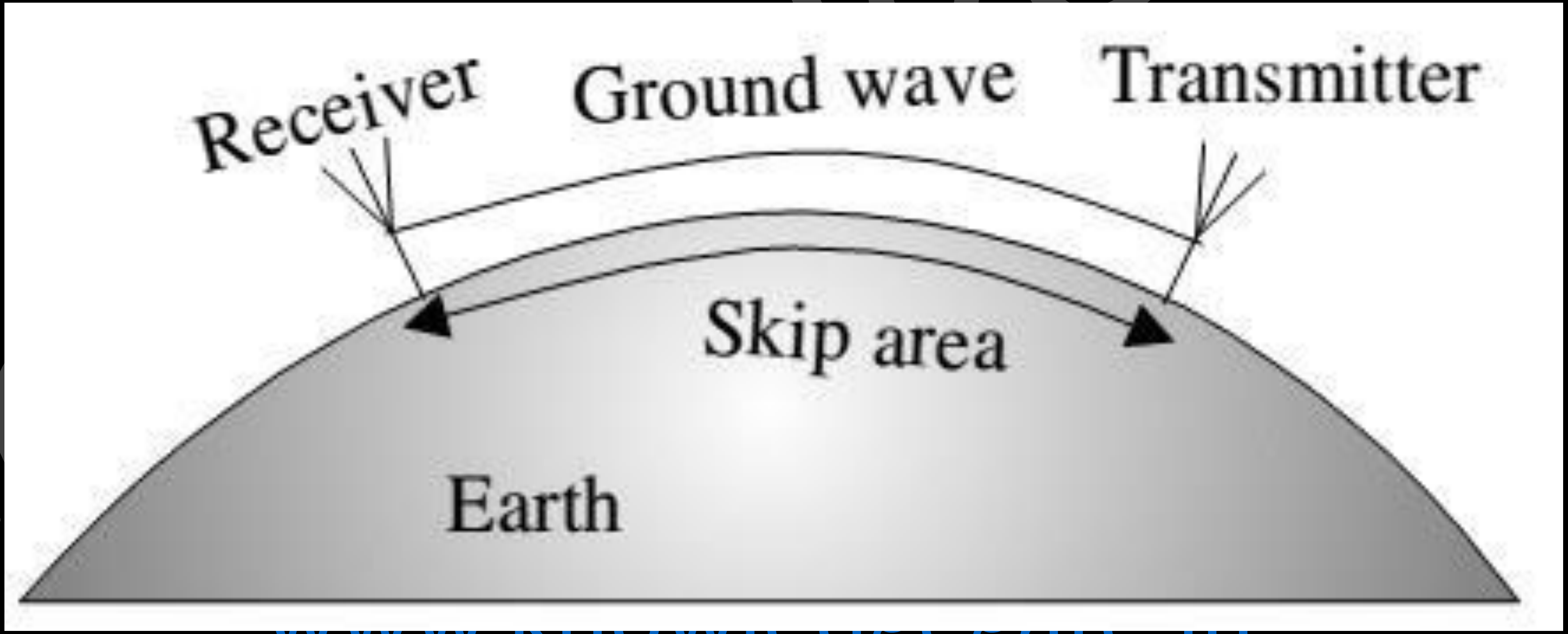
- **Fibre optic** - Made of glass or plastic and transmit signal in the form of light, using the principle of total internal reflection, a glass or plastic core is surrounded by a cladding of less dense glass or plastic.
- Backbone network cost effective can go up to 1600 Gbps (higher bandwidth, less signal attenuation, no noise problem, no corrosion, light weight, greater immunity to tapping) (installation and maintenance, unidirectional light propagation, cost)





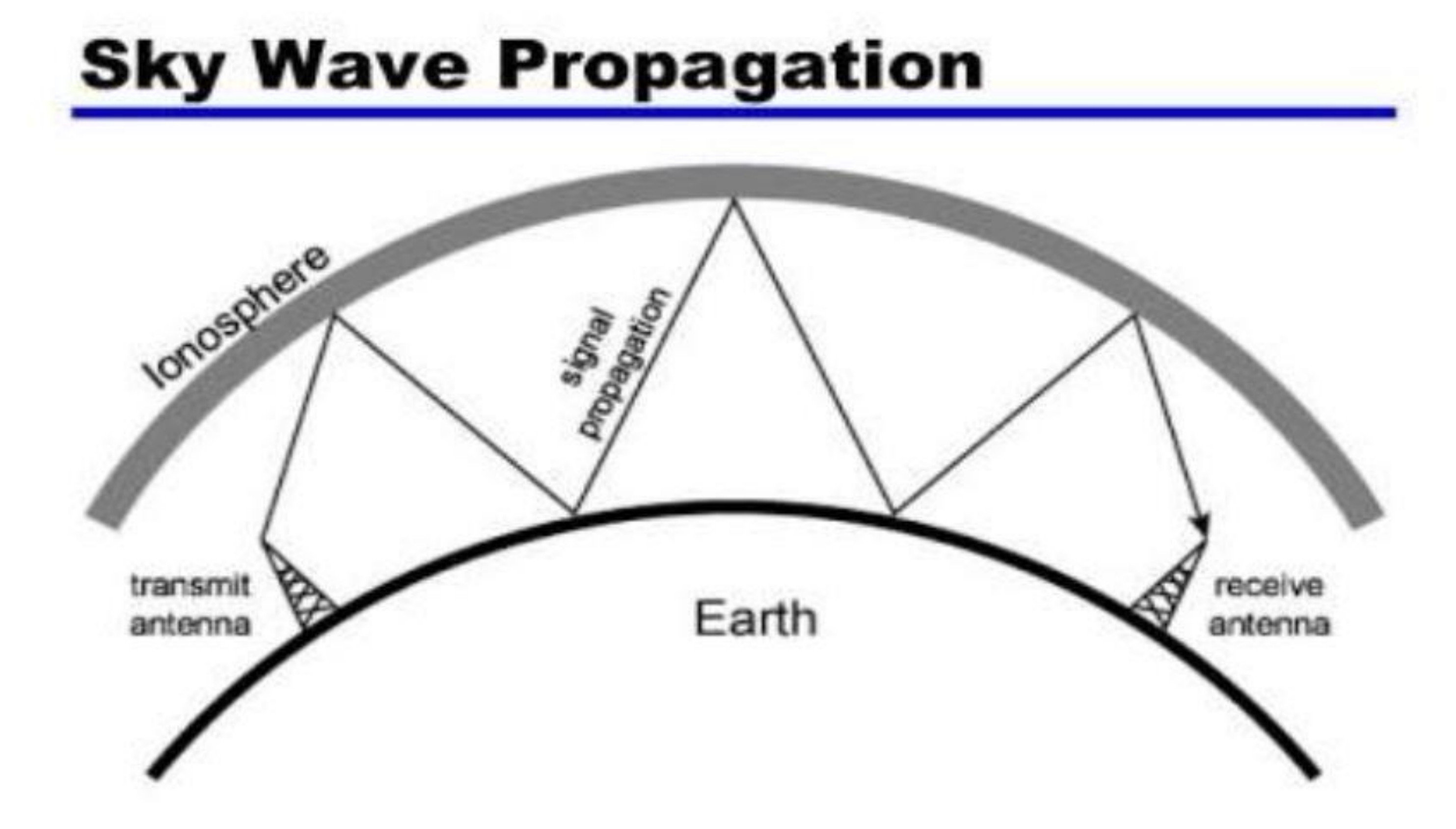
Unguided Media: Wireless

- **Ground propagation** – Waves travel through lower portion of the atmosphere hugging the earth, they are omni directional, distance depends on the amount of power.
- Will having low frequency and large wave length (Khz - Mhz)
- Bend round the obstructions, because large of Wave Length(e.g. light and sound)
- Attenuate in short range.



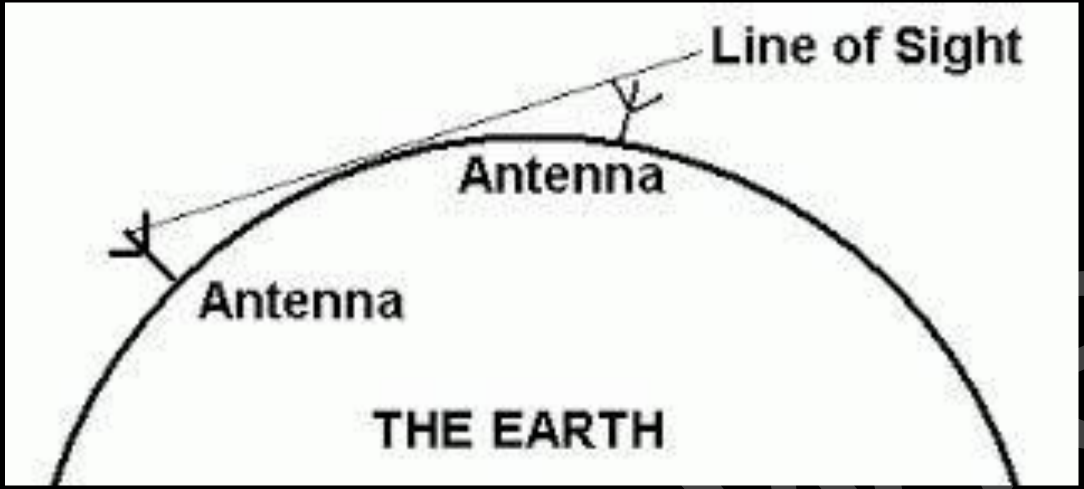
Unguided Media: Wireless

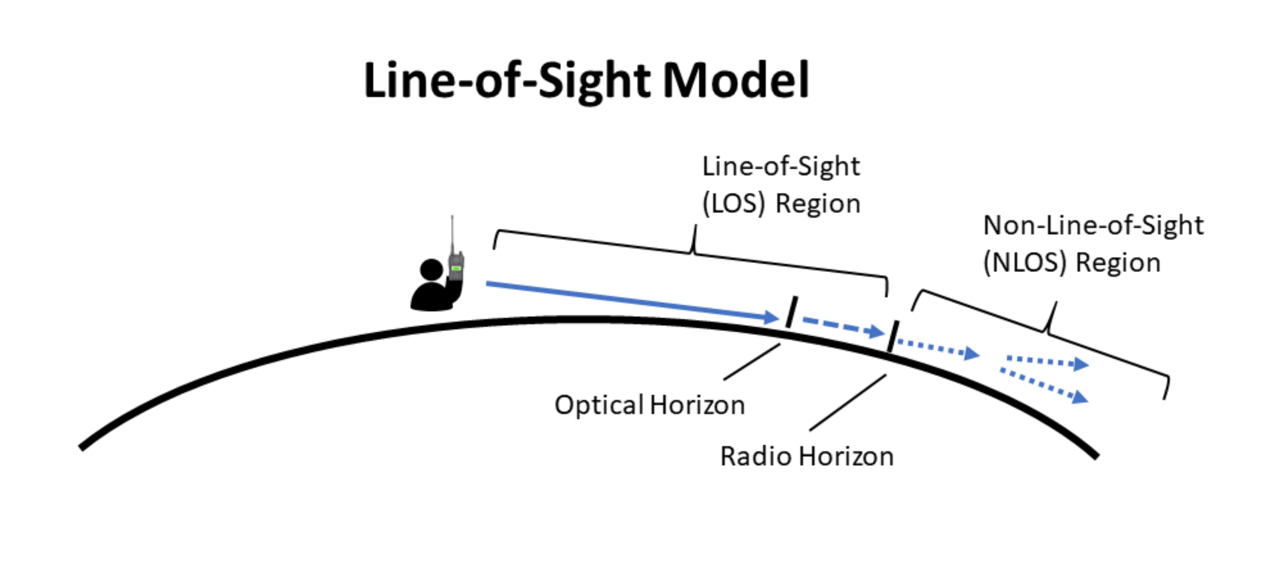
- **Sky propagation** – high frequency radio waves, radiated upward into the ionosphere where they are reflected back to earth. greater distance with lower output.
- 3 Mhz to 32 Mhz
- Range go up to 5000 km

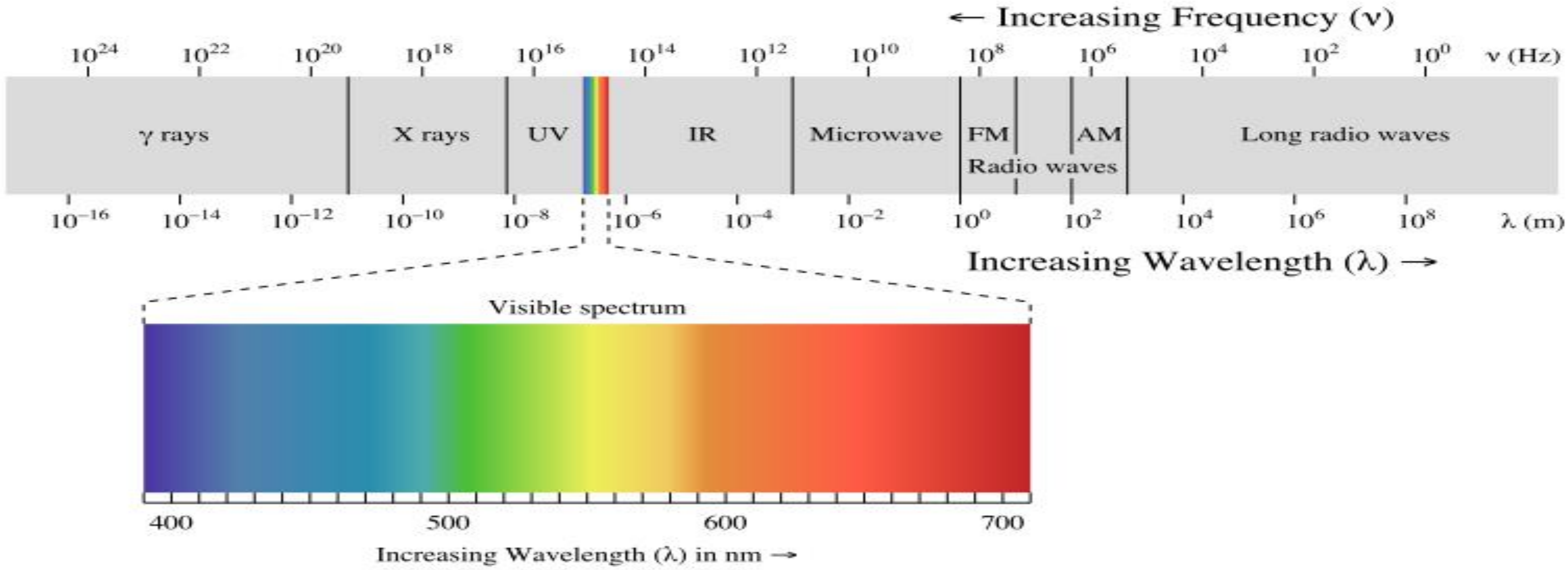


Unguided Media: Wireless

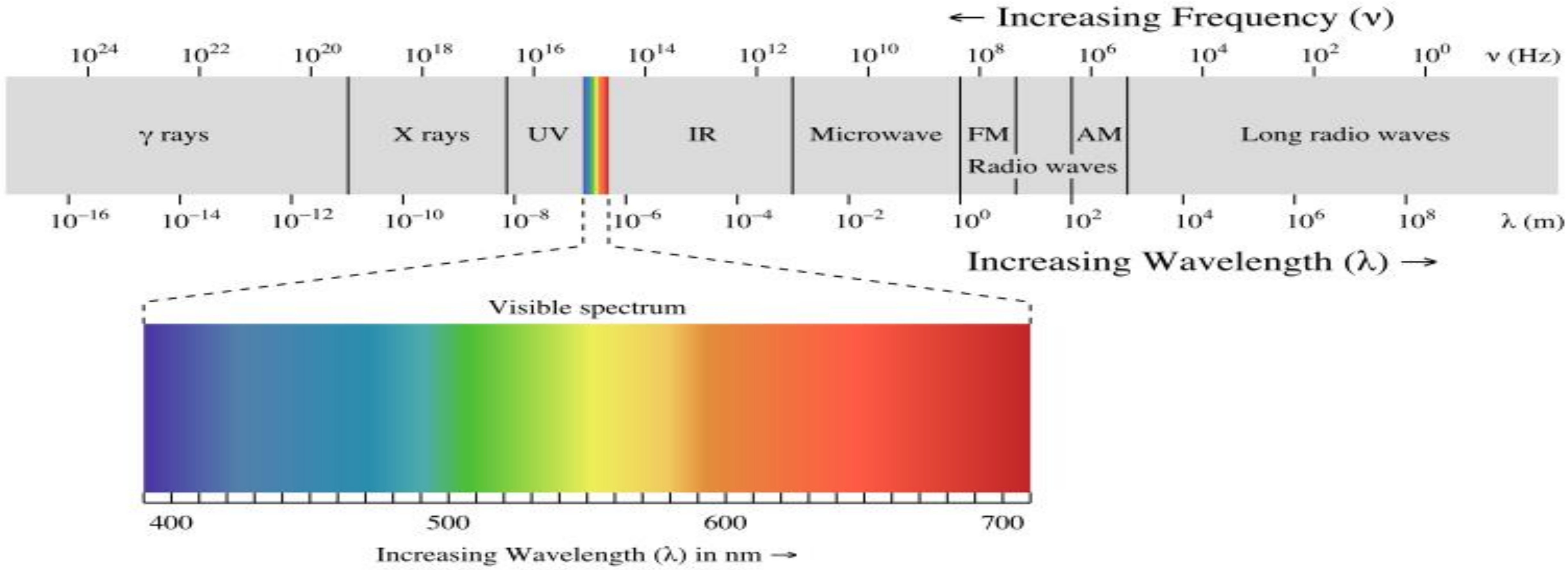
- **Line of sight propagation** – Very high frequency signals transmitted in straight lines directly from antenna to antenna.



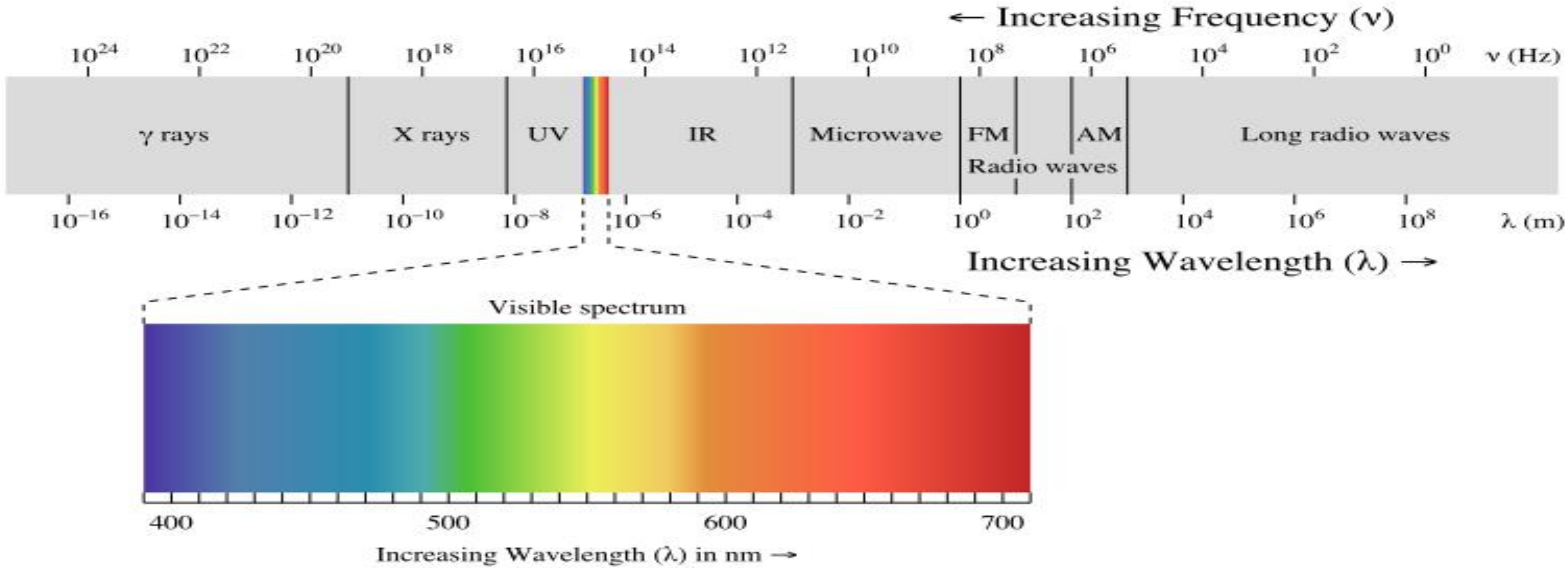




- **Radio Waves** – (3KHz- 1GHz) (omnidirectional) (interference problem because of omnidirectional) (sky mode) (long distance) (AM radio) (can penetrate through wall) (managed by government)


← Increasing Frequency (ν)
10^{24} 10^{22} 10^{20} 10^{18} 10^{16} 10^{14} 10^{12} 10^{10} 10^{8} 10^{6} 10^{4} 10^{2} 10^{0} ν (Hz)
γ rays
X rays
UV
IR
Microwave
FM
AM
Radio waves
Long radio waves
10^{-16} 10^{-14} 10^{-12} 10^{-10} 10^{-8} 10^{-6} 10^{-4} 10^{-2} 10^{0} 10^{2} 10^{4} 10^{6} 10^{8} λ (m)
Increasing Wavelength (λ) →
Visible spectrum
400
500
600
700
Increasing Wavelength (λ) in nm →

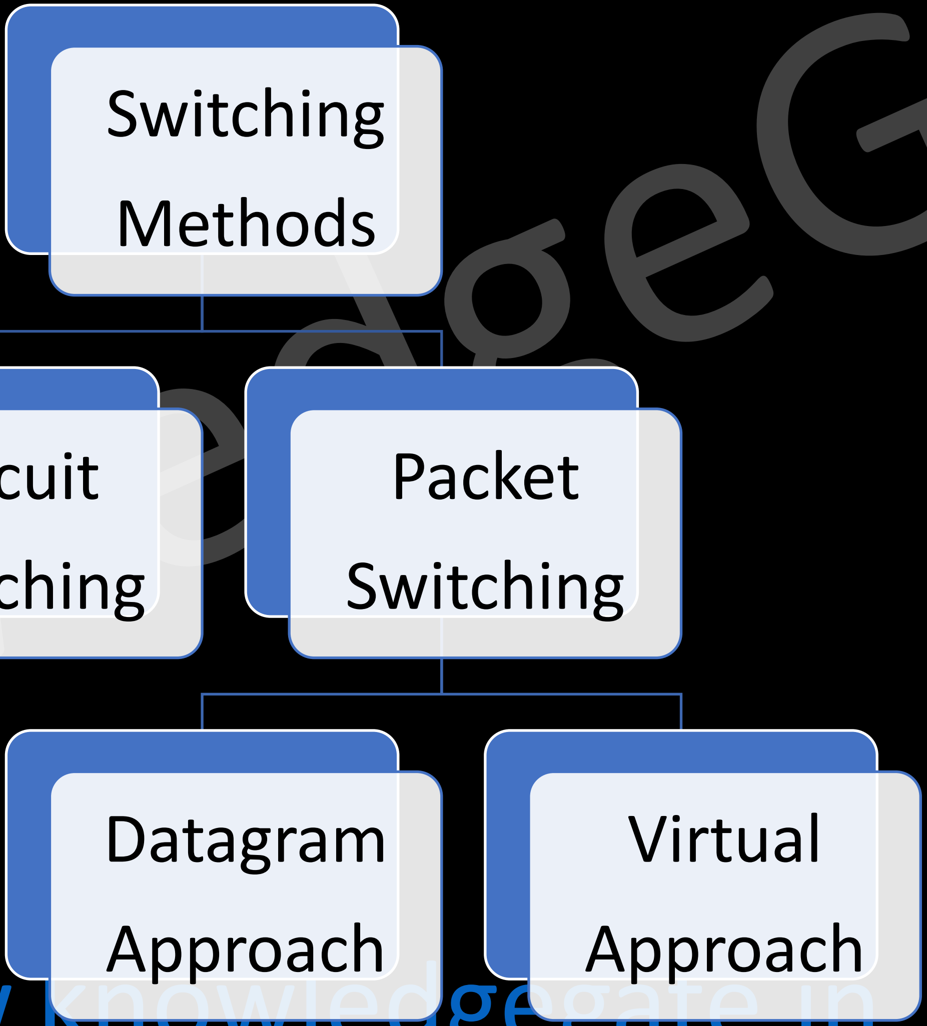
- **Microwaves** – (1GHZ- 300GHz) (unidirectional) (can be focused narrowly) (sending and receiving antenna needed to be aligned) (cannot penetrate wall) (wide band so high data rates are possible) (managed by government)



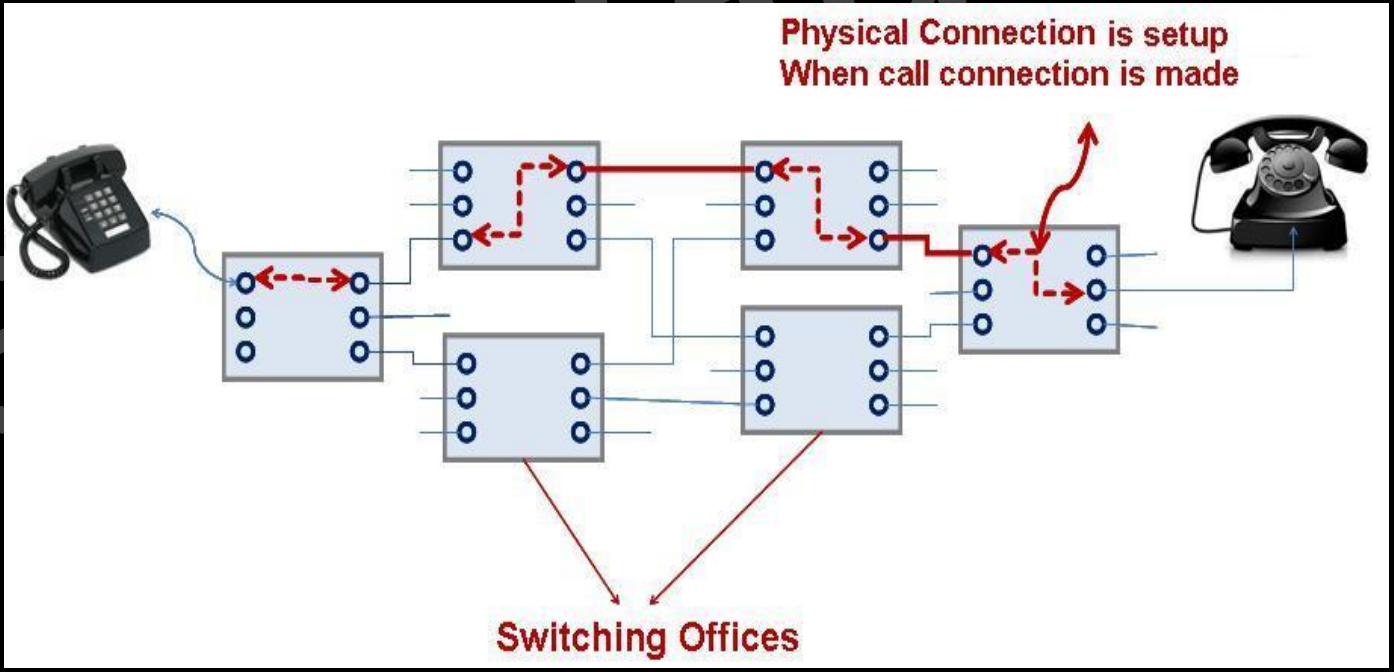
- **Infrared** – (300GHz- 400THz) (short range communication) (home appliances)

Switching

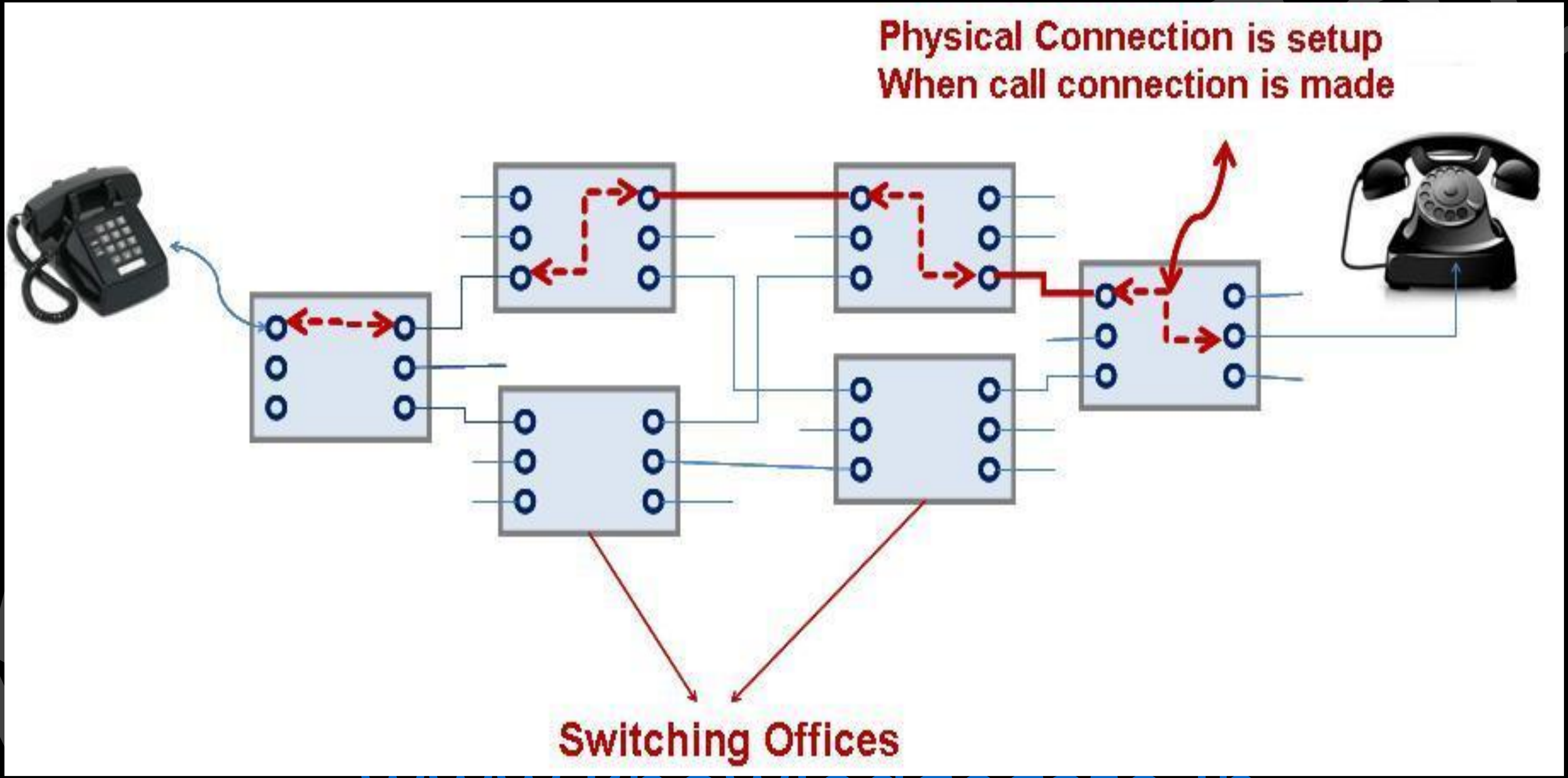
- Switching is the technique by which nodes control or switch data to transmit it between specific points on a network.



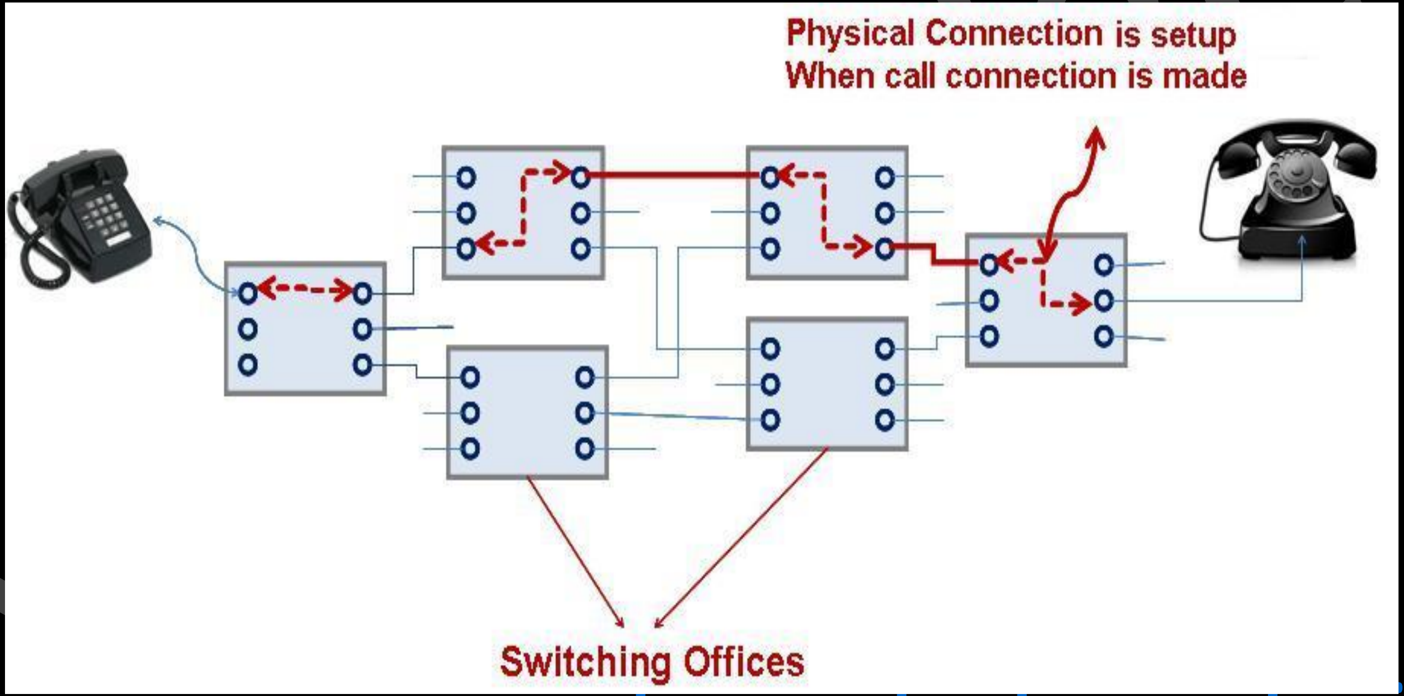
- In circuit switching network resources (bandwidth) is divided into pieces and bit delay is constant during a connection.
- The dedicated path/circuit established between sender and receiver provides a guaranteed data rate. Data can be transmitted without any delays once the circuit is established. Telephone system network is the one of example of Circuit switching.



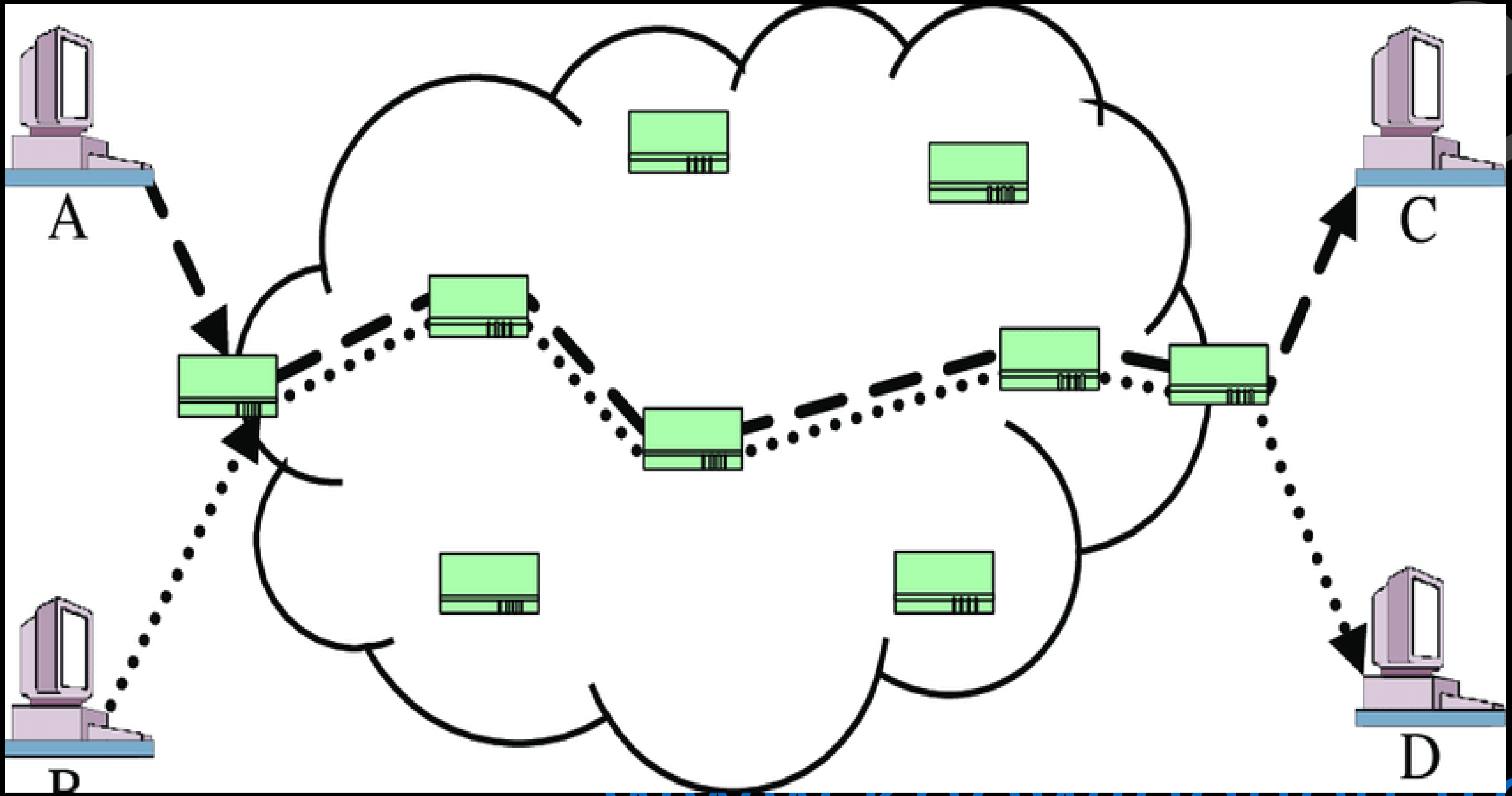
- Telephone system network is the one of example of Circuit switching.
    - **TDM (Time Division Multiplexing)**
    - **FDM (Frequency Division Multiplexing)**
- are two methods of multiplexing multiple signals into a single carrier.



- **Time Division Multiplexing :** *Divides into frames*
  - Time-division multiplexing (TDM) is a method of transmitting and receiving independent signals over a common signal path by means of synchronized switches at each end of the transmission line.
  - TDM is used for long-distance communication links and bears heavy data traffic loads from end user.
  - Time division multiplexing (TDM) is also known as a digital circuit switched.



- **Frequency Division Multiplexing :** *Divides into multiple bands*
  - Frequency Division Multiplexing or FDM is used when multiple data signals are combined for simultaneous transmission via a shared communication medium.
  - It is a technique by which the total bandwidth is divided into a series of non-overlapping frequency sub-bands, where each sub-band carry different signal. Practical use in radio spectrum & optical fiber to share multiple independent signals.

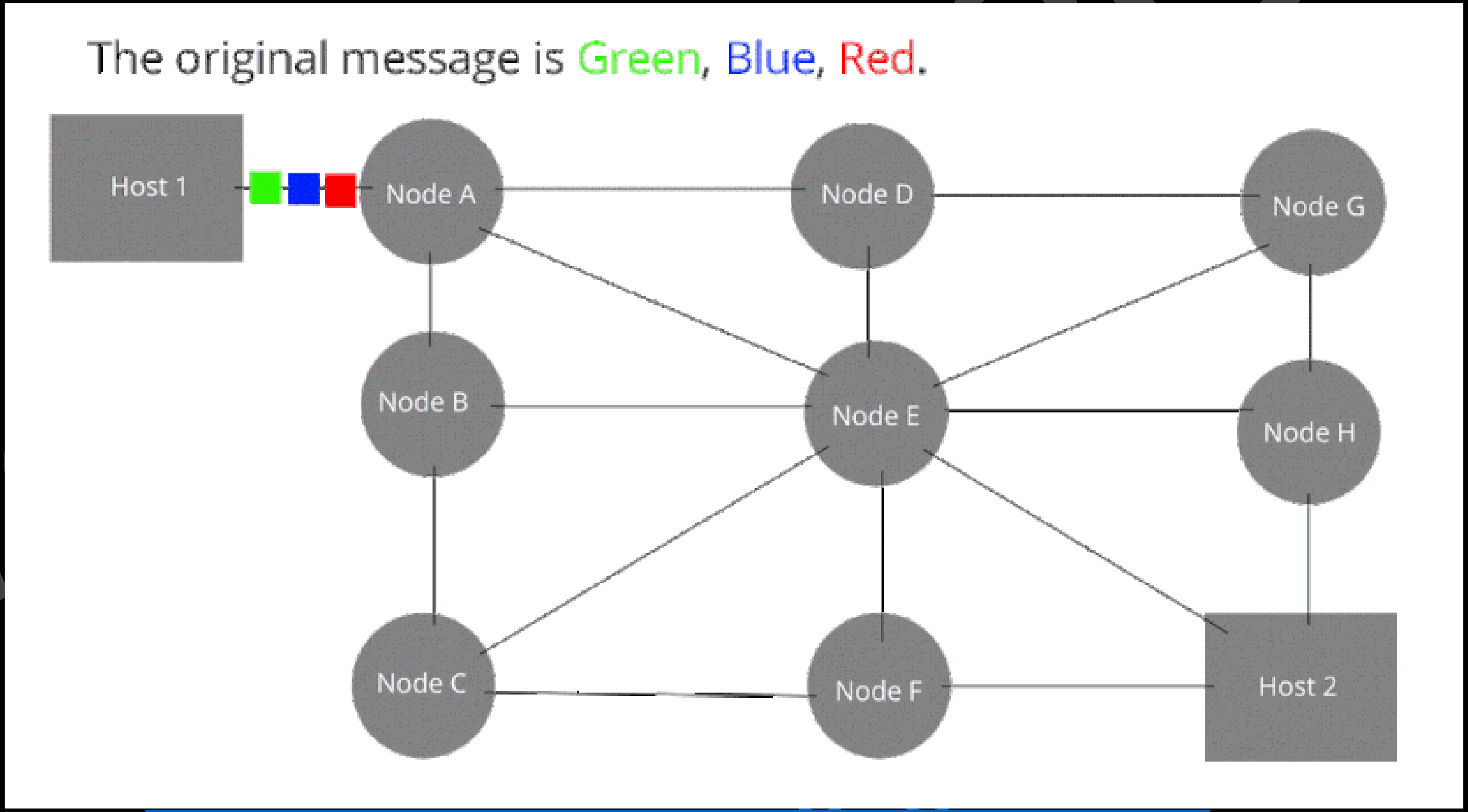


- **Advantages of Circuit Switching:** It has the following advantages :
  - The main advantage of circuit switching is that a committed transmission channel is established between the computers which gives a guaranteed data ratee.
  - In circuit switching there is no delay in data flow because of the dedicated transmission path.
  - No Header is required
  - Reordering of data cannot happen.

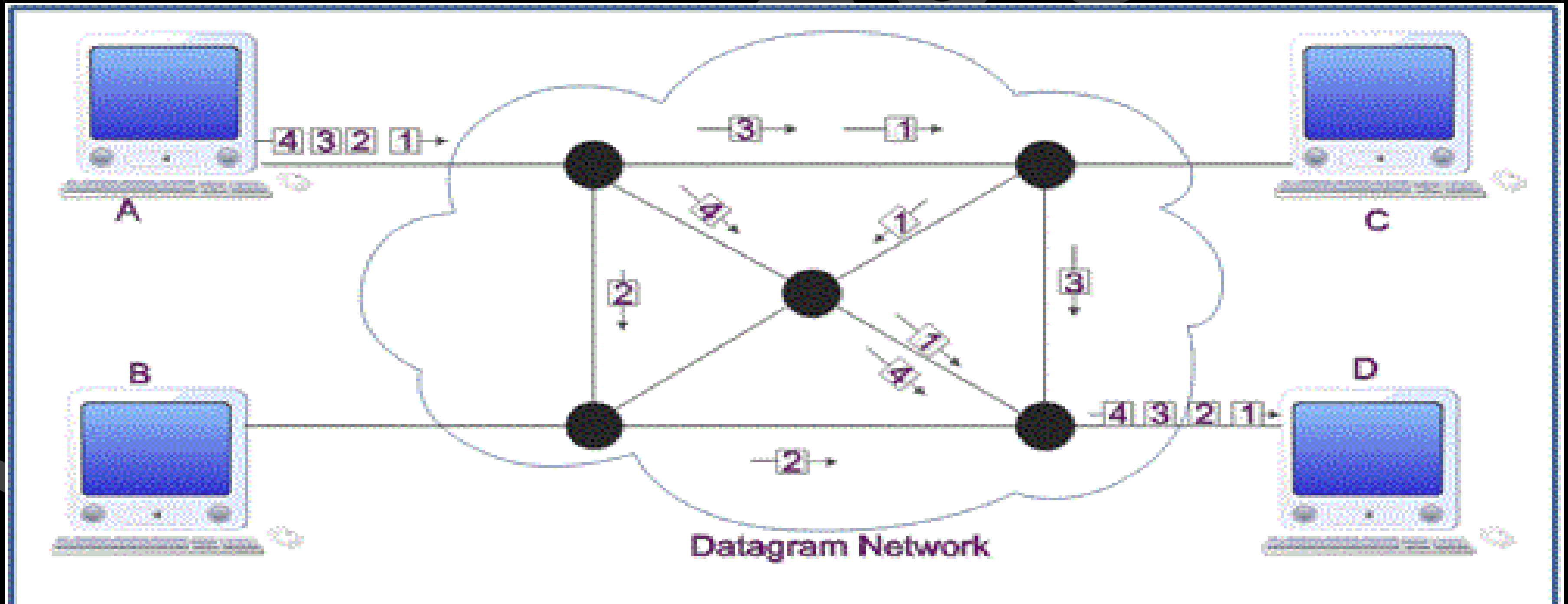
- **Disadvantages of Circuit Switching:** It has the following disadvantages :
  - It takes long time to establish connection.
  - More bandwidth is required in setting up of dedicated channels.
  - It cannot be used to transmit any other data even if the channel is free as the connection is dedicated in circuit switching.
  - Outdated, not used now a days

Packet Switching

- **Datagram network** - If the message is going to pass through a packet-switched network, it needs to be divided into packets of fixed or variable size. The size of the packet is determined by the network and the governing protocol.
- In packet switching, there is no resource allocation for a packet. This means that there is no reserved bandwidth on the links, and there is no scheduled processing time for each packet. Resources are allocated on demand. The allocation is done on a first come, first-served basis.

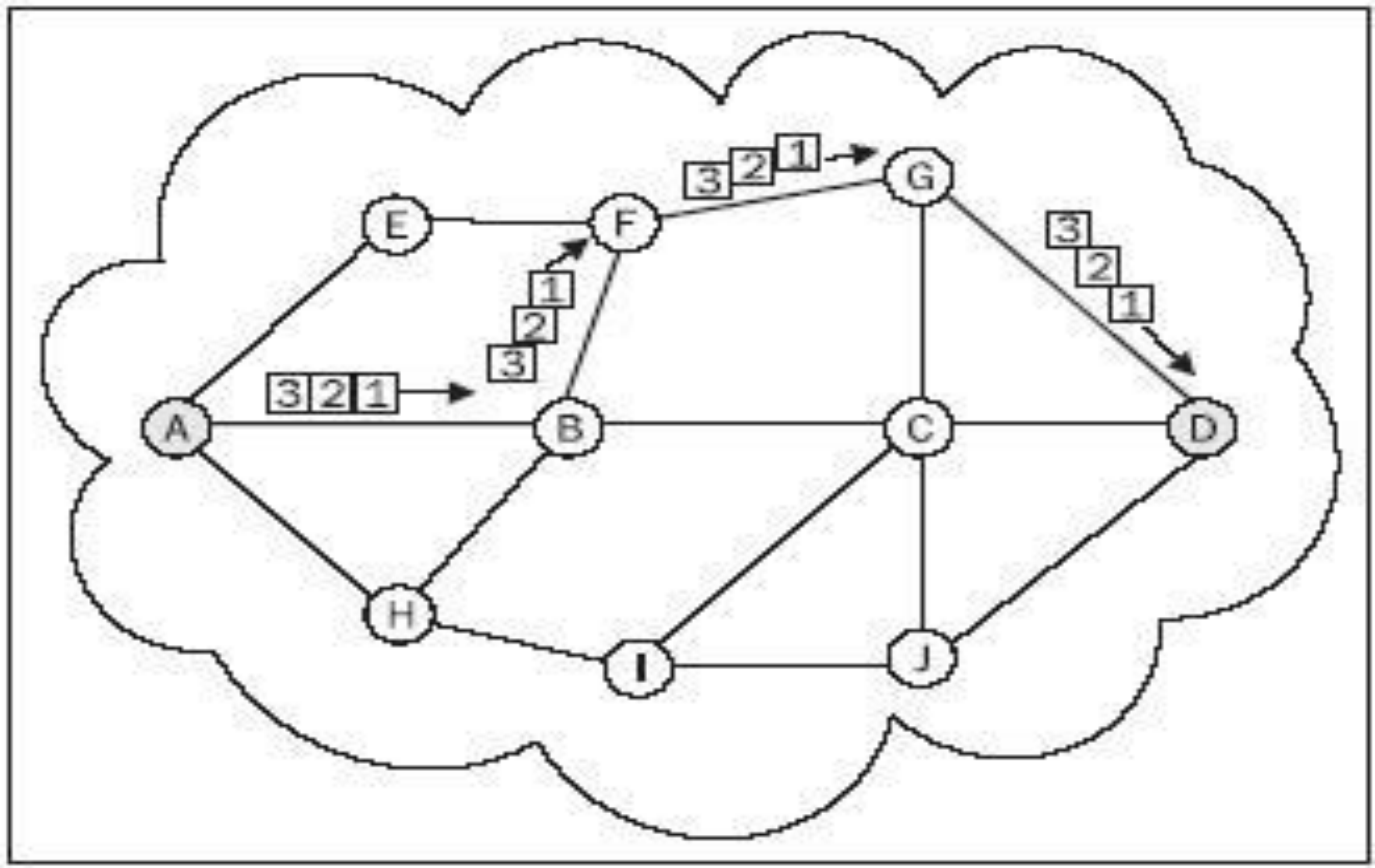


- When a switch receives a packet, no matter what is the source or destination, the packet must wait if there are other packets being processed. As with other systems in our daily life, this lack of reservation may create delay.
- Even if a packet is part of a multipacket transmission, the network treats it as though it existed alone. Packets in this approach are referred to as datagrams. Packets may also be lost or dropped because of a lack of resources.
- In most protocols, it is the responsibility of an upper-layer protocol to reorder the datagrams or ask for lost datagrams before passing them on to the application.



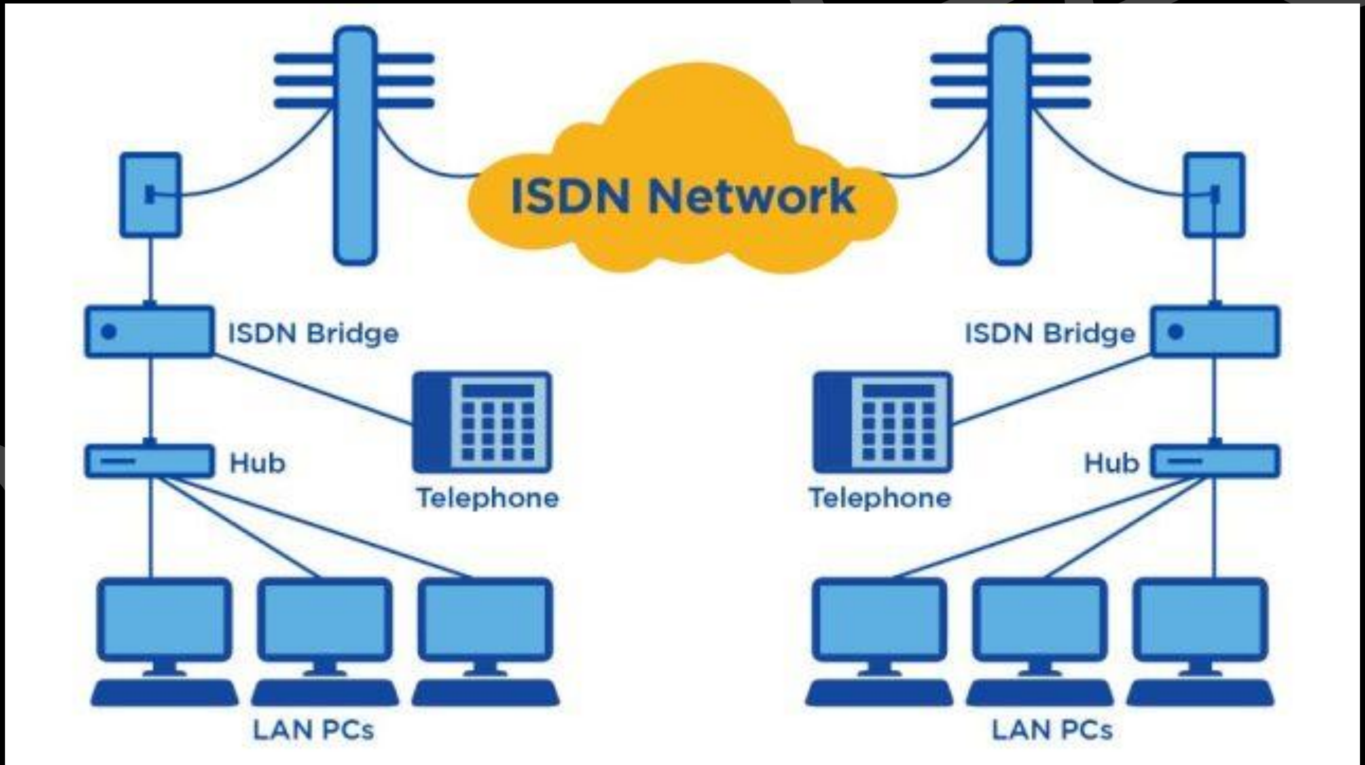
Datagram Packet switching

- **Virtual network** - A virtual-circuit network is a cross between a circuit-switched network and a datagram network. It has some characteristics of both. Used now-a-days in telephone networks



ISDN (Integrated Services Digital Network)

1. **Definition**: Integrated Services Digital Network - a set of protocols for establishing and breaking circuit-switched connections, and for advanced call features for the user.
2. **Development Period**: Developed during the late 1980s and early 1990s.
3. **Digital Transmission**: Unlike traditional telephone services which use analog signals, ISDN uses digital signals for transmission.
4. **Channels**: ISDN provides channels known as B-channels (for data) and D-channels (for control and signaling).

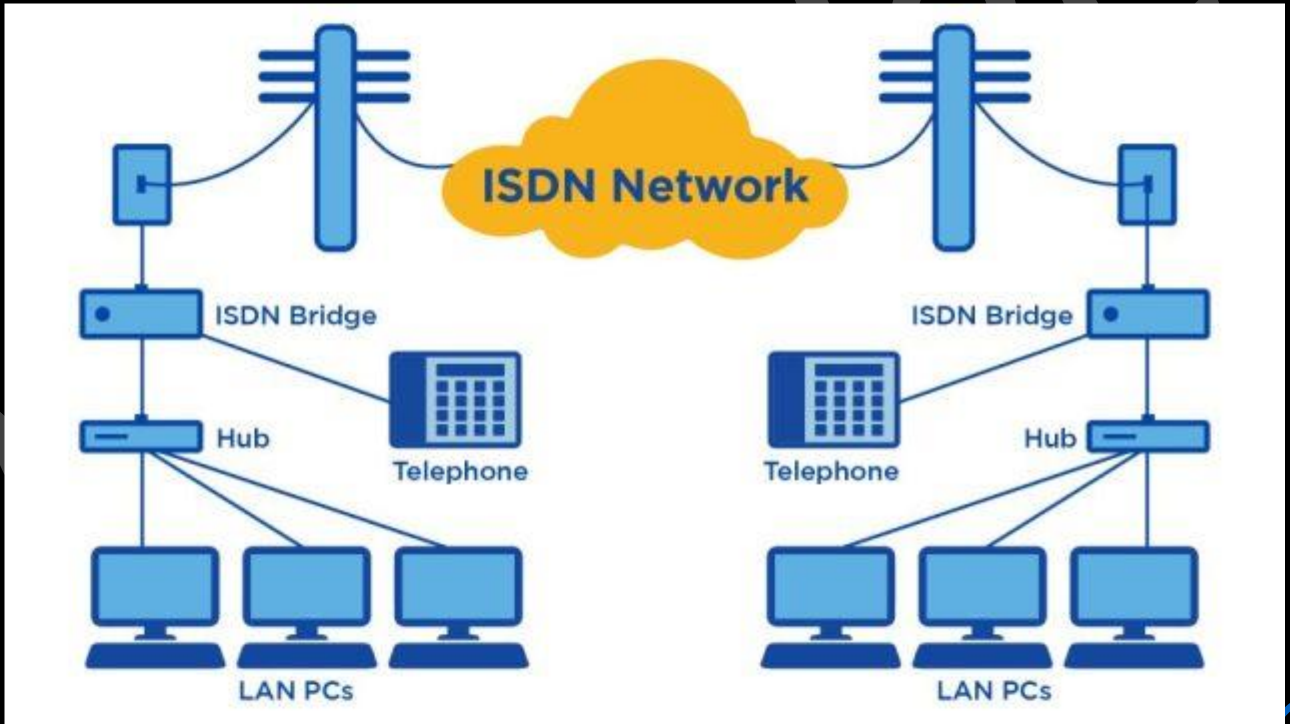


5. **BRI and PRI**: There are two types of ISDN interfaces - Basic Rate Interface (BRI) and Primary Rate Interface (PRI). BRI is suitable for home and small enterprise, while PRI is used for larger installations.

6. **Speed**: ISDN provides data rates up to 128 kbps in the case of BRI, and up to 1.544 Mbps for PRI in North America and 2.048 Mbps in Europe.

7. **Usage**: Initially popular for internet access before the widespread availability of broadband.

8. **Decline**: Its popularity has declined with the advent of faster, more reliable broadband internet services.



Unit-2

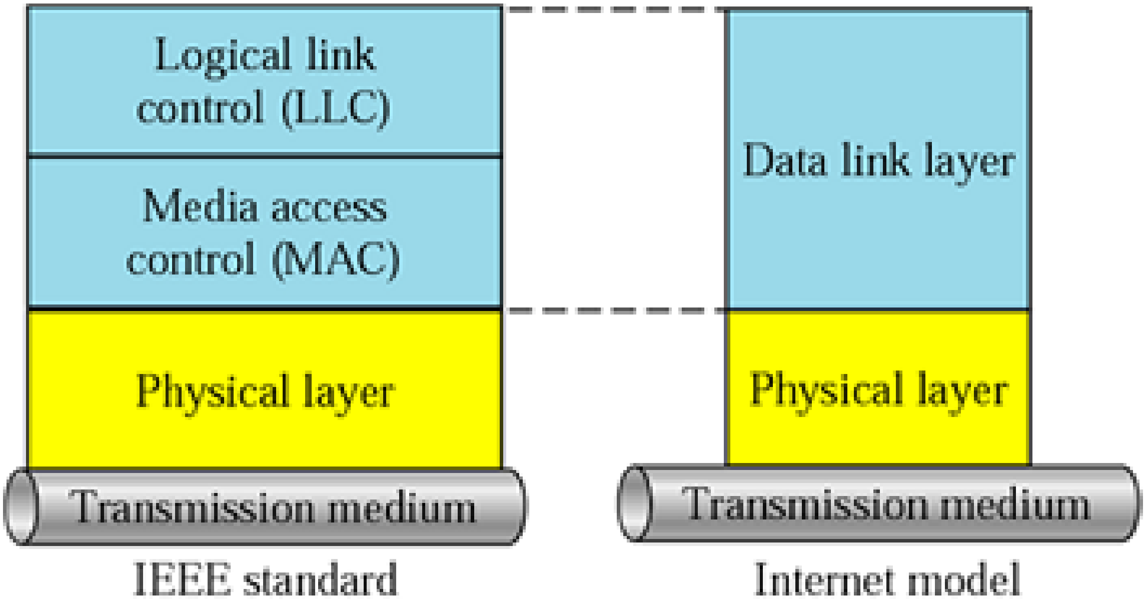
Two Sublayers

1. The IEEE has subdivided the data-link layer into two sublayers: **logical link control (LLC)** (TOP) **and media access control (MAC)** (BOTTOM)**.**

2. ***Media Access Control (MAC):*** It defines the specific access method for each LAN, Ethernet and Take care of Addressing at the level (Lan technology).

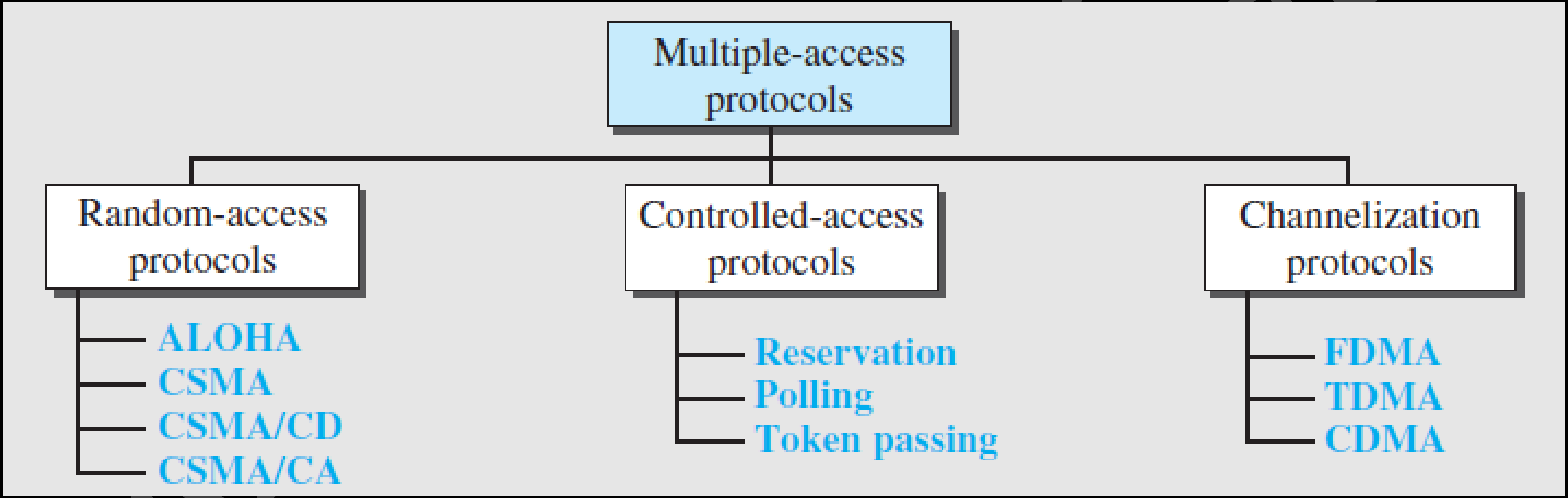
3. Flow control, error control, and part of the framing duties are collected into one sublayer called the *logical link control* (LLC).

4. Framing is handled in both the LLC sublayer and the MAC sublayer.

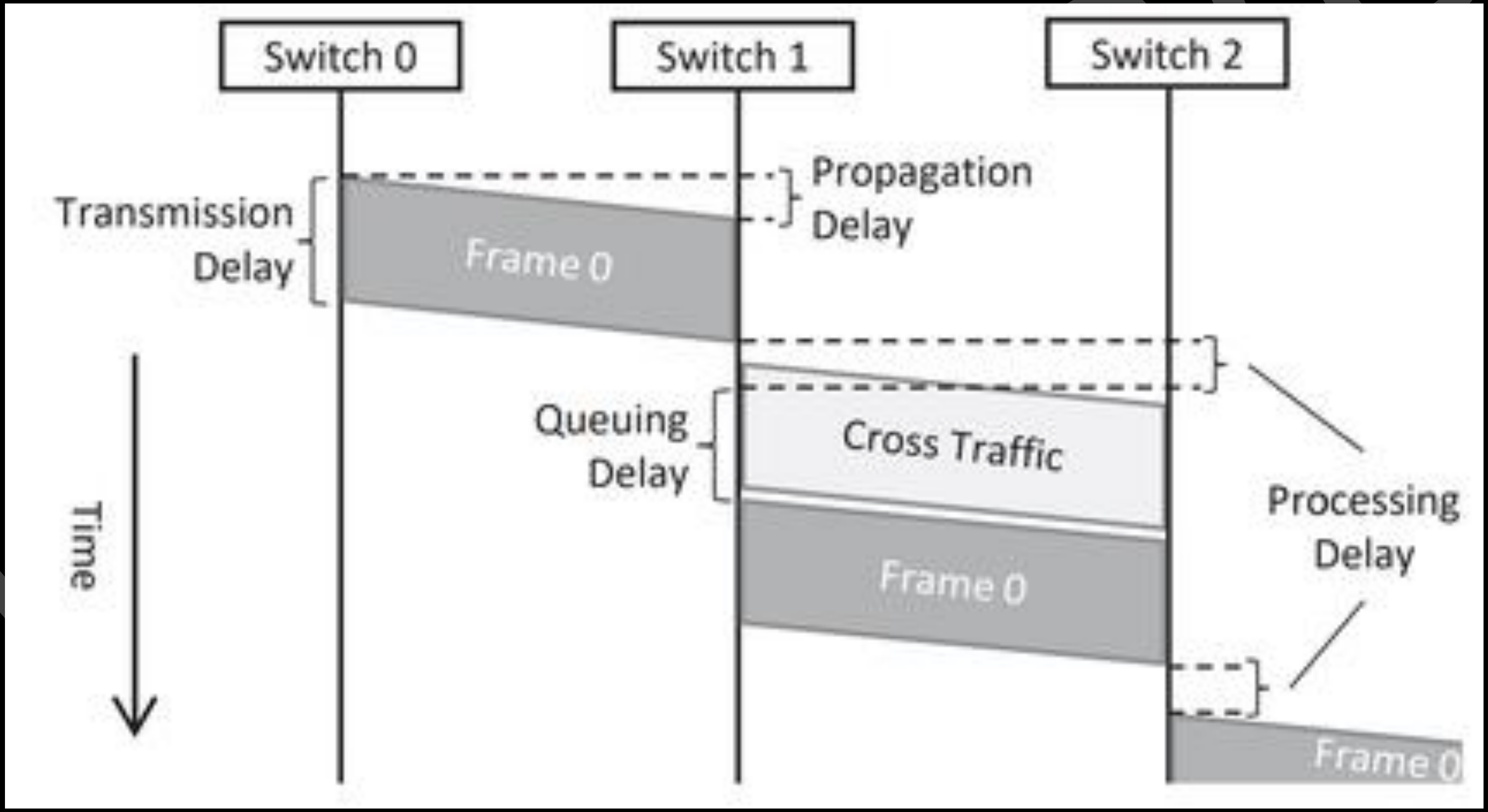


Media Access Control

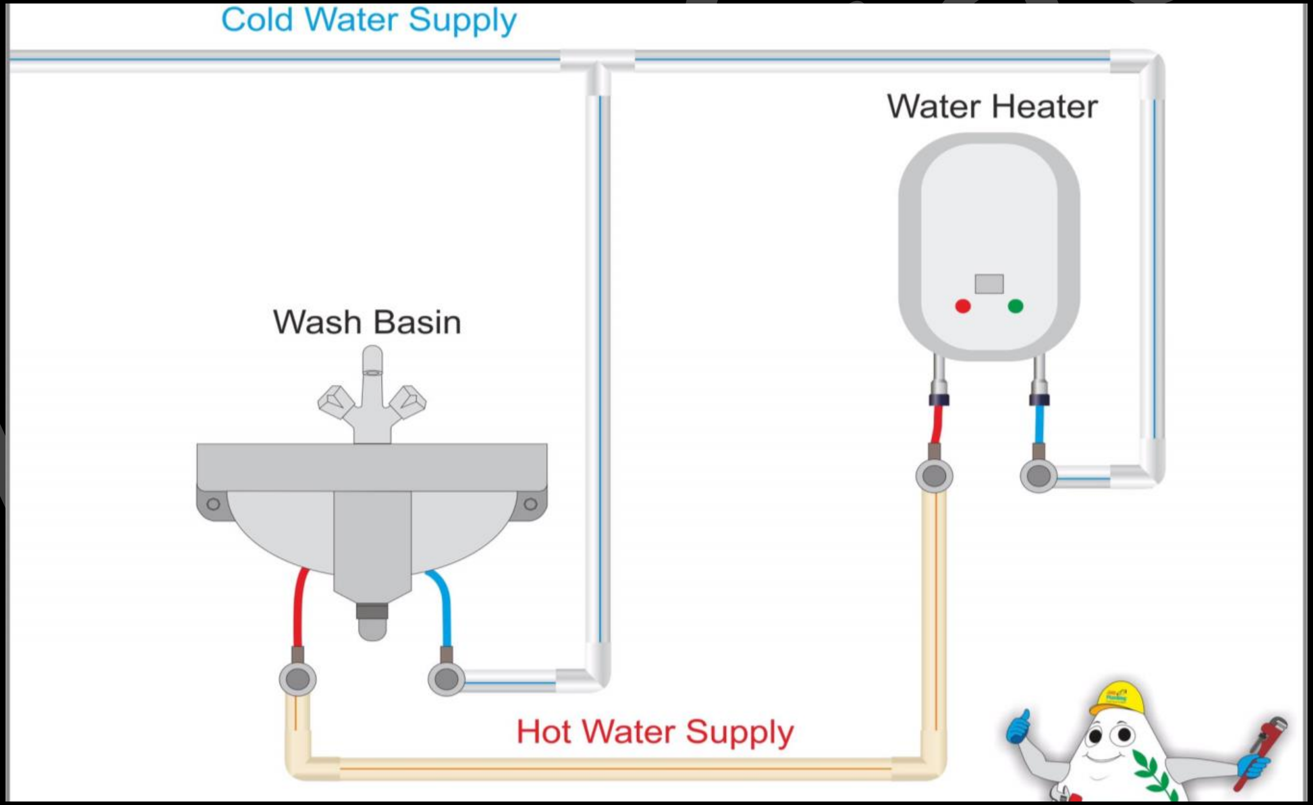
- When nodes or stations are connected and use a common link, we need a multiple-access protocol to coordinate access to the link. Many protocols have been devised to handle access to a shared link.



- **Propagation Delay**: Propagation delay is the time it takes for a bit to travel from point A to point B in the transmission media.
  T_P = (Distance) / (Propagation speed)



- **Transmission Delay (TT) :** A sender needs to put the bits in a packet on the line one by one. If the first bit of the packet is put on the line at time t_1 and the last bit is put on the line at time t_2, transmission delay of the packet is $(t_2 - t_1)$.
T_t = (Packet length (L)) / (Transmission rate or Bandwidth (B)) = L / B



www.knowledgegate.in

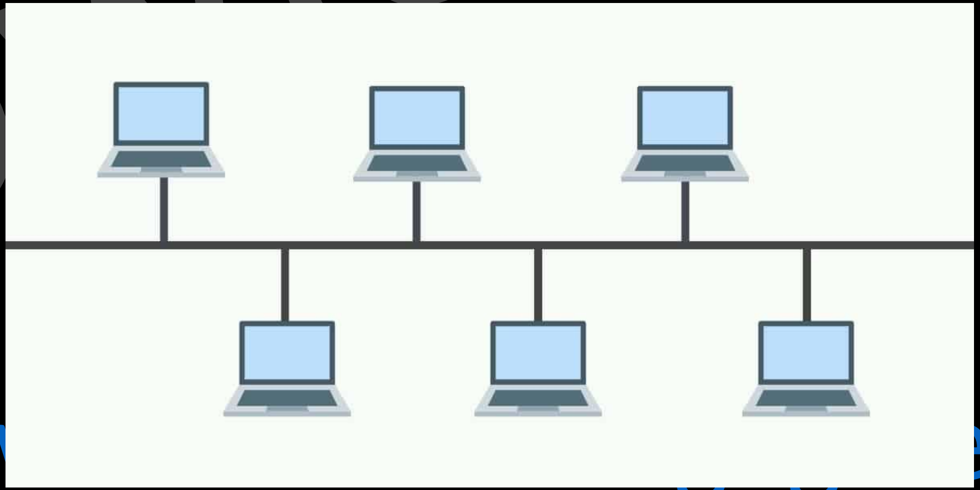
RANDOM ACCESS

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

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

3. Two features give this method its name.
   - First, there is no scheduled time for a station to transmit. Transmission is random among the stations. That is why these methods are called random access.
   - Second, no rules specify which station should send next. Stations compete with one another to access the medium. That is why these methods are also called contention methods.

4. However, if more than one station tries to send, there is an access conflict-collision-and the frames will be either destroyed or modified.



- All the protocols in Random access approach will answer the following questions
    1. When can the station access the medium?
    2. What can the station do if the medium is busy?
    3. How can the station determine the success or failure of the transmission?
    4. What can the station do if there is an access conflict?

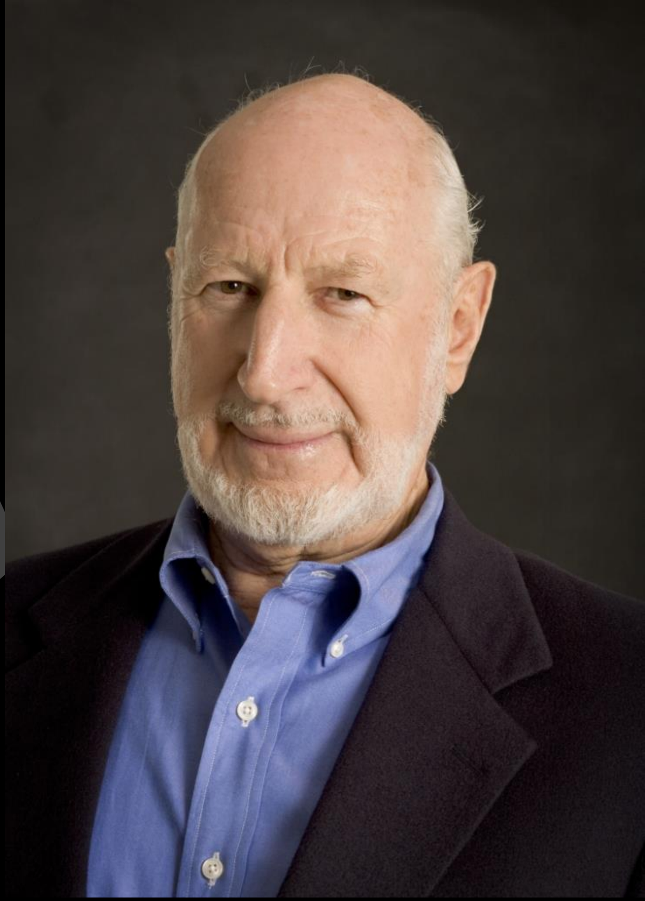
Aloha

- Earliest random-access method, was developed at the University of Hawaii around 1970.

- It was designed for a radio (wireless) LAN, but it can be used on any shared medium.

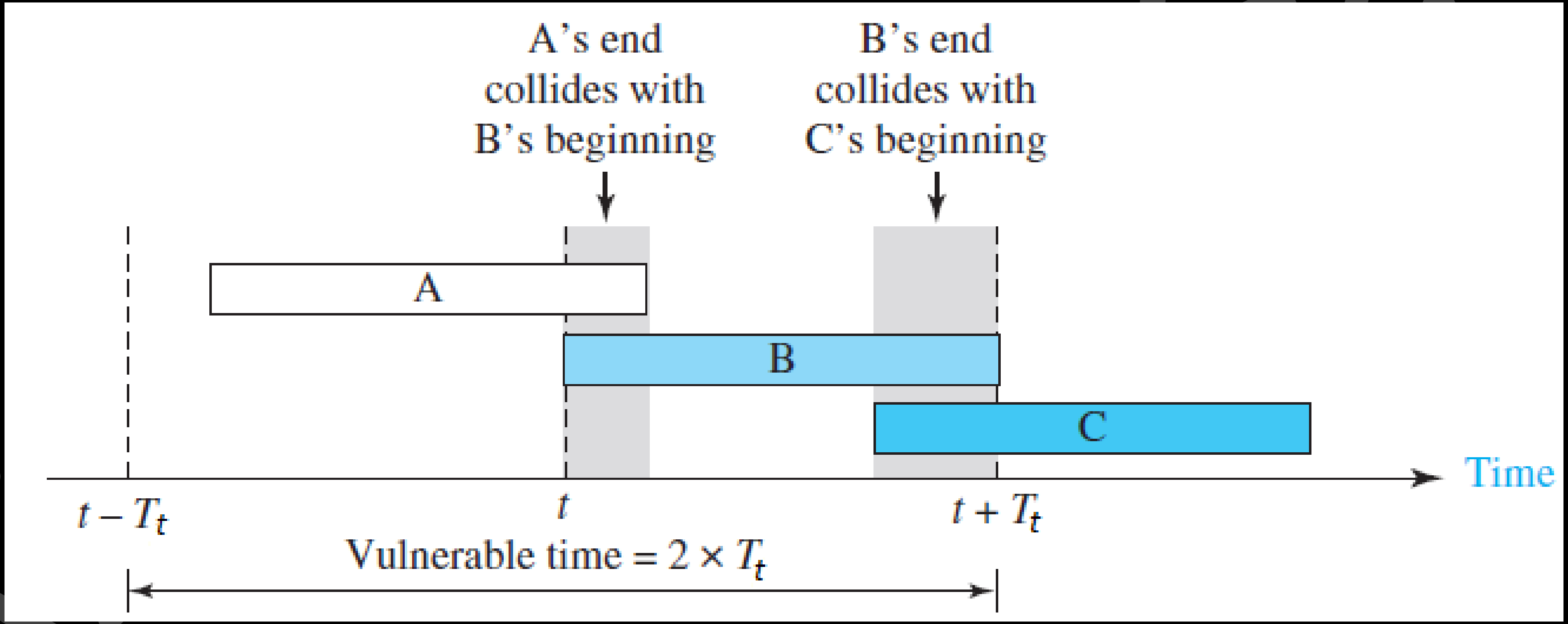
- The original ALOHA protocol is called pure ALOHA. This is a simple, but elegant protocol.

- The idea is that each station sends a frame whenever it has a frame to send. However, there is the possibility of collision between frames from different stations.



Norman Manuel Abramson

- We assume that the stations send fixed-length frames with each frame taking T_{fr} to send.
- Vulnerable time in which there is a possibility of collision, we see that the time during which a collision may occur in pure ALOHA, is 2 times the frame transmission time. Pure ALOHA vulnerable time= 2 x T_{fr}


A's end collides with B's beginning
B's end collides with C's beginning
A
B
C
Time
$t - T_t$
t
$t + T_t$
Vulnerable time = $2 \times T_t$

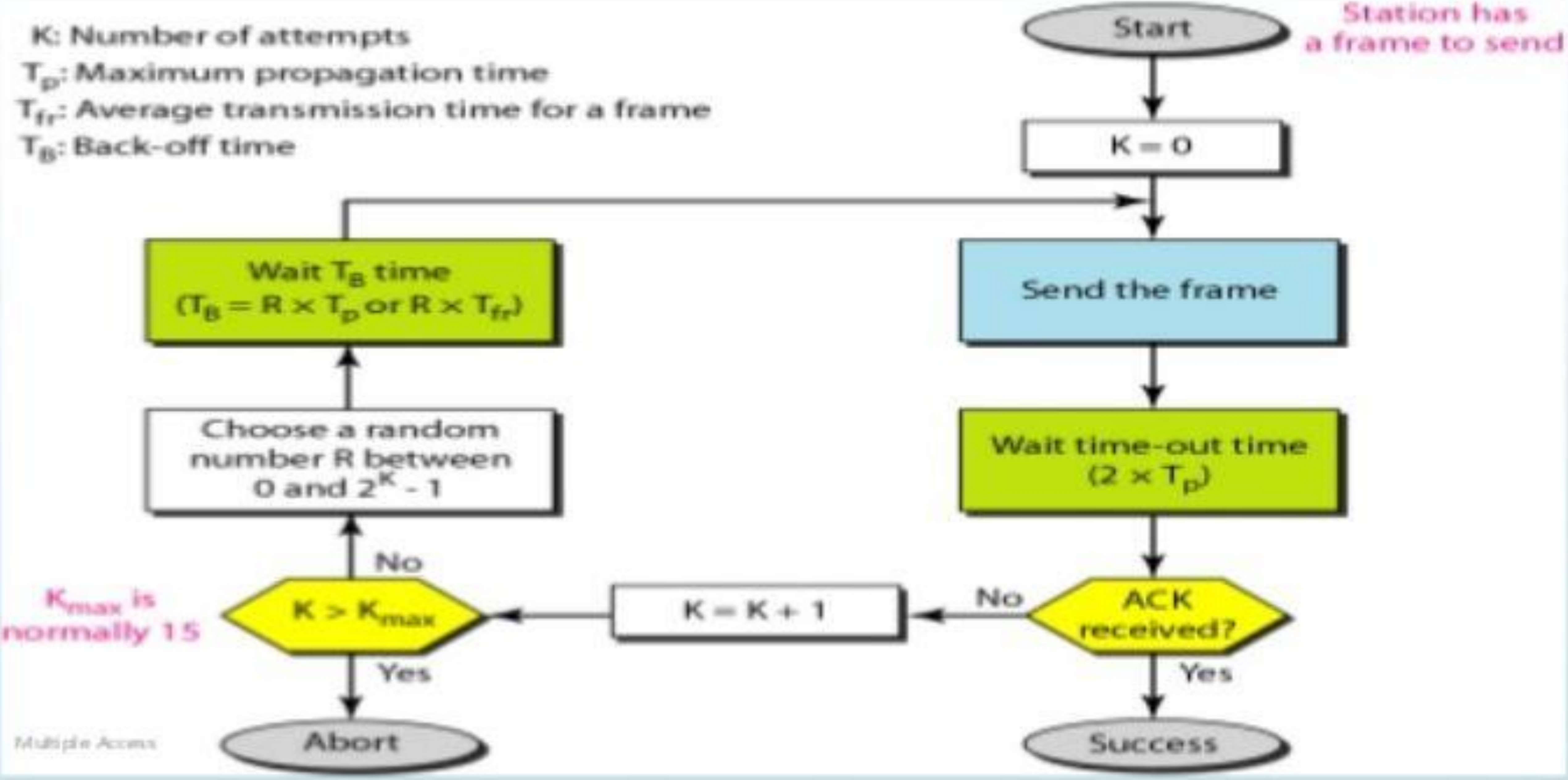
Procedure for Pure ALOHA protocol

K: Number of attempts

T_p: Maximum propagation time

T_{fr}: Average transmission time for a frame

T_B: Back-off time


Start
Station has a frame to send
K = 0
Send the frame
Wait time-out time ($2 \times T_p$)
ACK received?
Yes
Success
No
K = K + 1
$K > K_{max}$
K_{max} is normally 15
Yes
Abort
No
Choose a random number R between 0 and $2^K - 1$
Wait T_B time ($T_B = R \times T_p$ or $R \times T_{fr}$)
Multiple Access

- If all these stations try to resend their frames after the time-out, the frames will collide again.
- Pure ALOHA dictates that when the time-out period passes, each station waits a random amount of time before resending its frame. The randomness will help avoid more collisions. We call this time the back-off time T_B.
- Pure ALOHA has a second method to prevent congesting the channel with retransmitted frames. After a maximum number of retransmissions attempts K_{max} a station must give up and try later.

Example 12.2

A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the requirement to make this frame collision-free?

Solution

Average frame transmission time T_{fr} is 200 bits/200 kbps or 1 ms. The vulnerable time is 2×1 ms $=$ 2 ms. This means no station should send later than 1 ms before this station starts transmission and no station should start sending during the period (1 ms) that this station is sending.

Throughput

Let us call G the average number of frames generated by the system during one frame transmission time. Then it can be proven that the average number of successfully transmitted frames for pure ALOHA is $S = G \times e^{-2G}$. The maximum throughput S_{max} is 0.184, for $G = 1/2$. (We can find it by setting the derivative of S with respect to G to 0; see Exercises.) In other words, if one-half a frame is generated during one frame transmission time (one frame during two frame transmission times), then 18.4 percent of these frames reach their destination successfully. We expect $G = 1/2$ to produce the maximum throughput because the vulnerable time is 2 times the frame transmission time. Therefore, if a station generates only one frame in this vulnerable time (and no other stations generate a frame during this time), the frame will reach its destination successfully.

The throughput for pure ALOHA is $S = G \times e^{-2G}$.
The maximum throughput $S_{max} = 1/(2e) = 0.184$ when $G = (1/2)$.

Example 12.3

A pure ALOHA network transmits 200-bit frames on a shared channel of 200 kbps. What is the throughput if the system (all stations together) produces

a. 1000 frames per second?

b. 500 frames per second?

c. 250 frames per second?

Solution

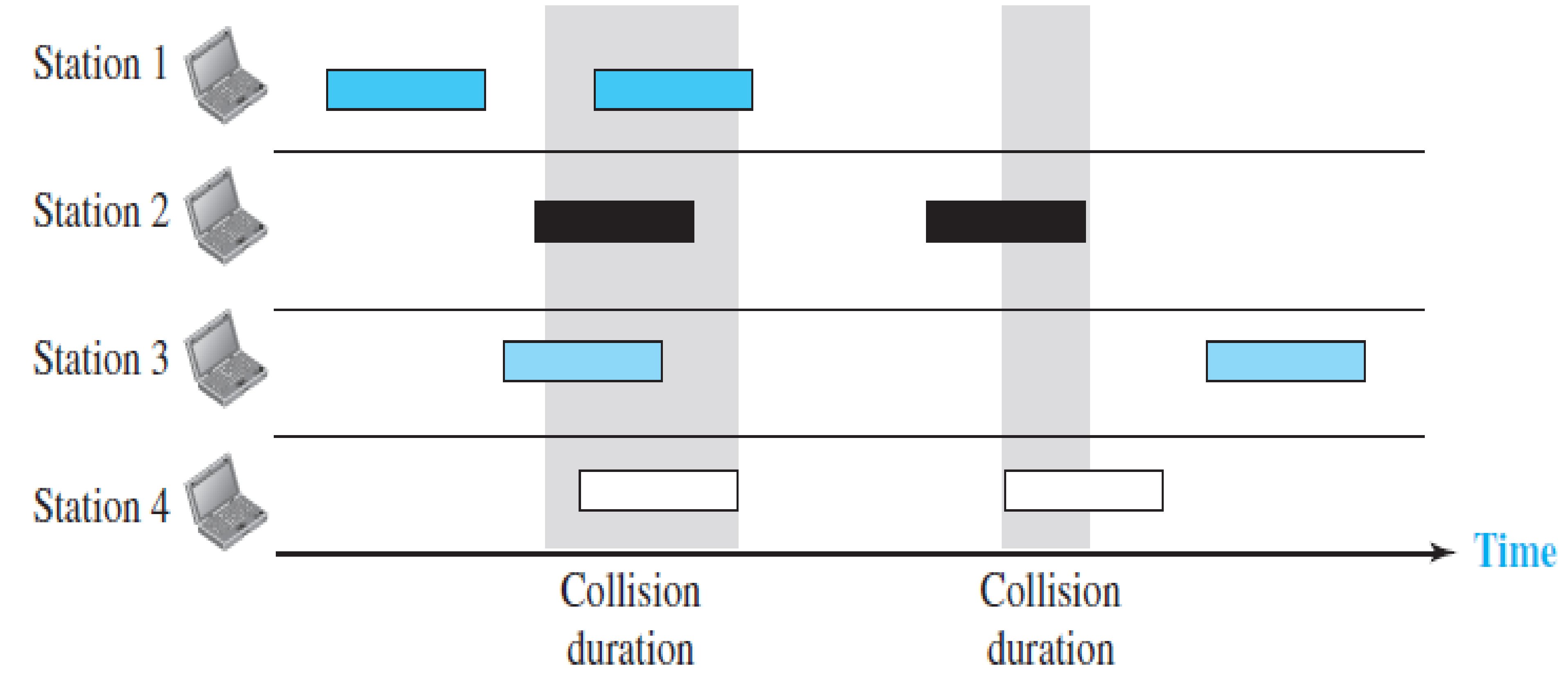
The frame transmission time is 200/200 kbps or 1 ms.

a. If the system creates 1000 frames per second, or 1 frame per millisecond, then $G = 1$. In this case $S = G \times e^{-2G} = 0.135$ (13.5 percent). This means that the throughput is $1000 \times 0.135 = 135$ frames. Only 135 frames out of 1000 will probably survive.

b. If the system creates 500 frames per second, or 1/2 frames per millisecond, then $G = 1/2$. In this case $S = G \times e^{-2G} = 0.184$ (18.4 percent). This means that the throughput is $500 \times 0.184 = 92$ and that only 92 frames out of 500 will probably survive. Note that this is the *maximum* throughput case, percentagewise.

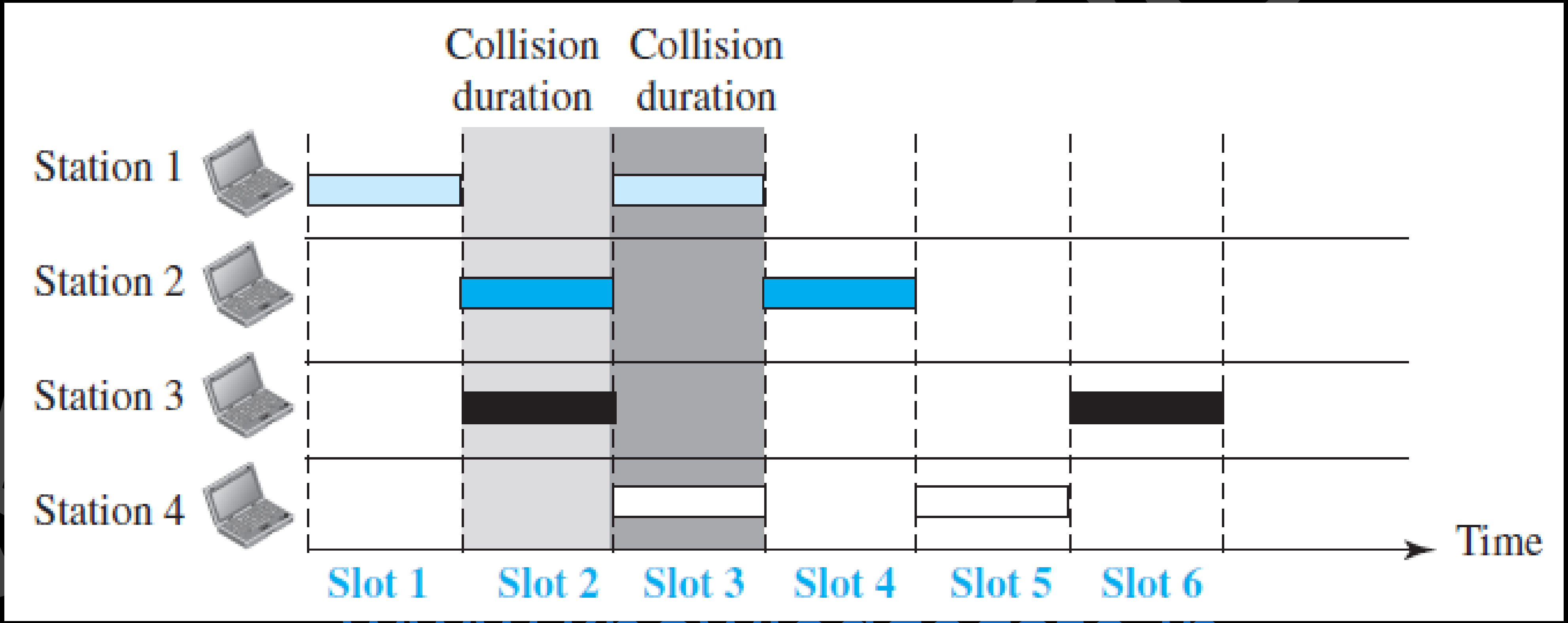
c. If the system creates 250 frames per second, or 1/4 frames per millisecond, then $G = 1/4$. In this case $S = G \times e^{-2G} = 0.152$ (15.2 percent). This means that the throughput is $250 \times 0.152 = 38$. Only 38 frames out of 250 will probably survive.

ALOHA

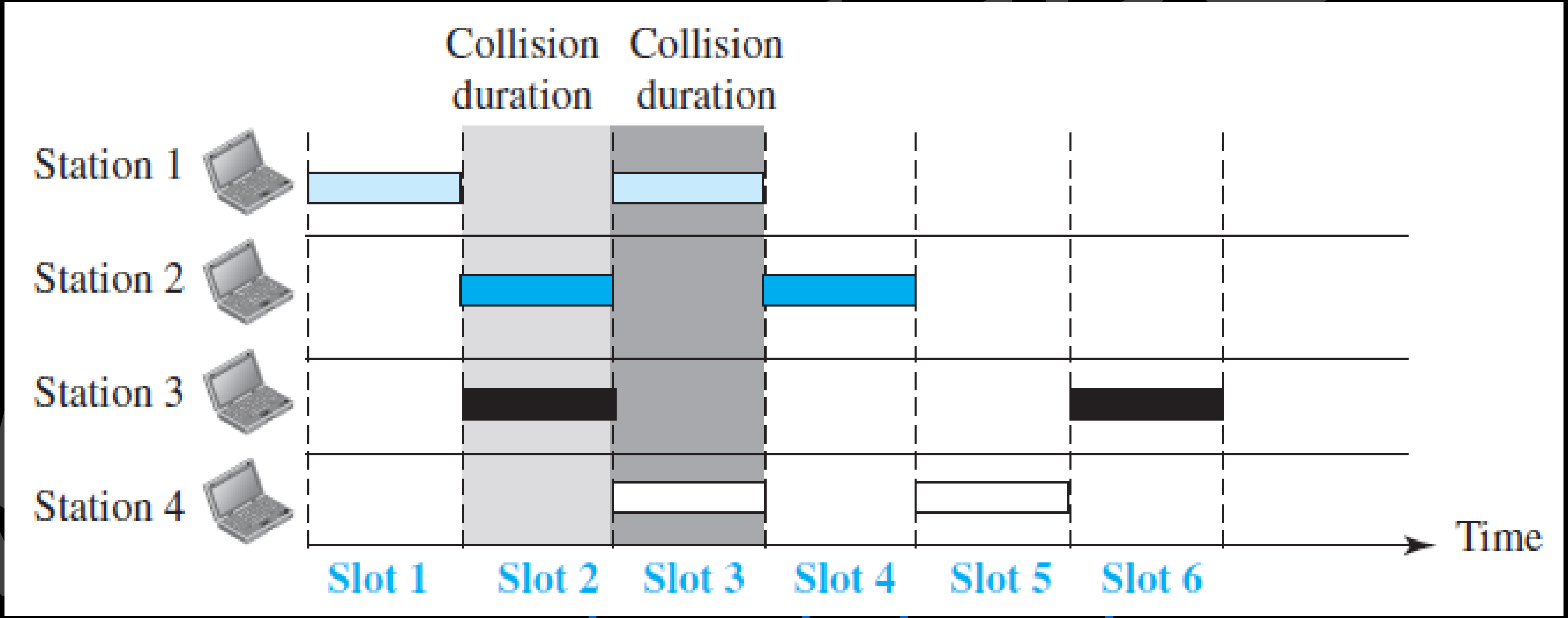

Station 1
Station 2
Station 3
Station 4
Time
Collision duration
Collision duration

Slotted ALOHA

- Pure ALOHA has a vulnerable time of 2 x T_{fr}. This is so because there is no rule that defines when the station can send. A station may send soon after another station has started or soon before another station has finished.
- Slotted ALOHA was invented to improve the efficiency of pure ALOHA. In slotted ALOHA we divide the time into slots of T_{fr} s and force the station to send only at the beginning of the time slot.



- Because a station is allowed to send only at the beginning of the synchronized time slot, if a station misses this moment, it must wait until the beginning of the next time slot. This means that the station which started at the beginning of this slot has already finished sending its frame.
- Off course, there is still the possibility of collision if two stations try to send at the beginning of the same time slot. However, the vulnerable time is now reduced to one-half, equal to T_{fr}

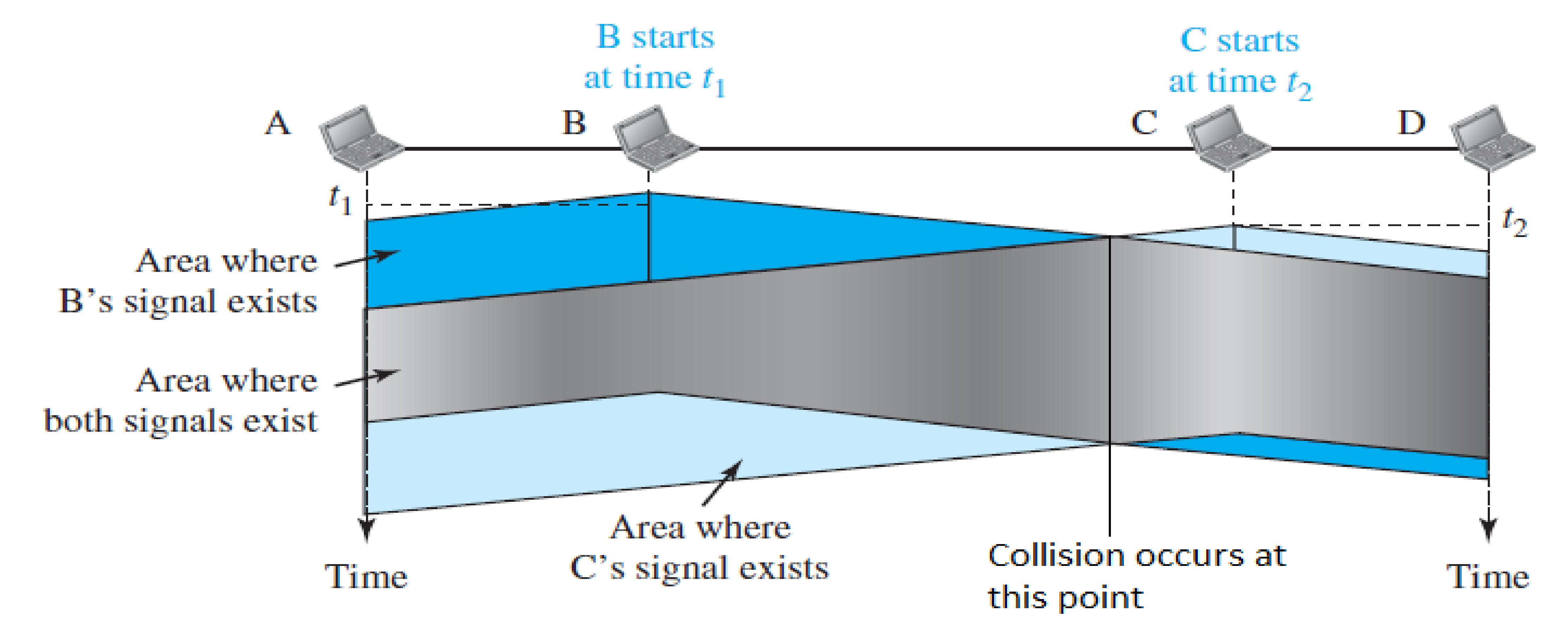


Aspect	Pure ALOHA	Slotted ALOHA
Time Structure	No specific time structure; data can be sent at any time.	Operates on time slots; data is sent at the beginning of a time slot.
Efficiency	Lower efficiency (~18.4%) due to higher probability of collisions.	Higher efficiency (~37%) as it reduces the chance of collisions.
Collision Handling	If a collision occurs, the message is resent after a random time interval.	Messages are sent in synchronized time slots, reducing the chance of collision but if a collision occurs, it is handled similarly to Pure ALOHA.
Complexity	Less complex as it doesn't require synchronization.	More complex due to the need for time synchronization.
Implementation	Easier to implement due to lack of synchronization requirements.	Implementation is moderately complex because of the synchronization of time slots.

Carrier Sense Multiple Access (CSMA)

- To minimize the chance of collision and, therefore, increase the performance, the CSMA method was developed. The chance of collision can be reduced if a station senses the medium before trying to use it.
- Carrier sense multiple access (CSMA) requires that each station first listen to the medium (or check the state of the medium) before sending, so "sense before transmit" or" listen before talk." CSMA can reduce the possibility of collision, but it cannot eliminate it.

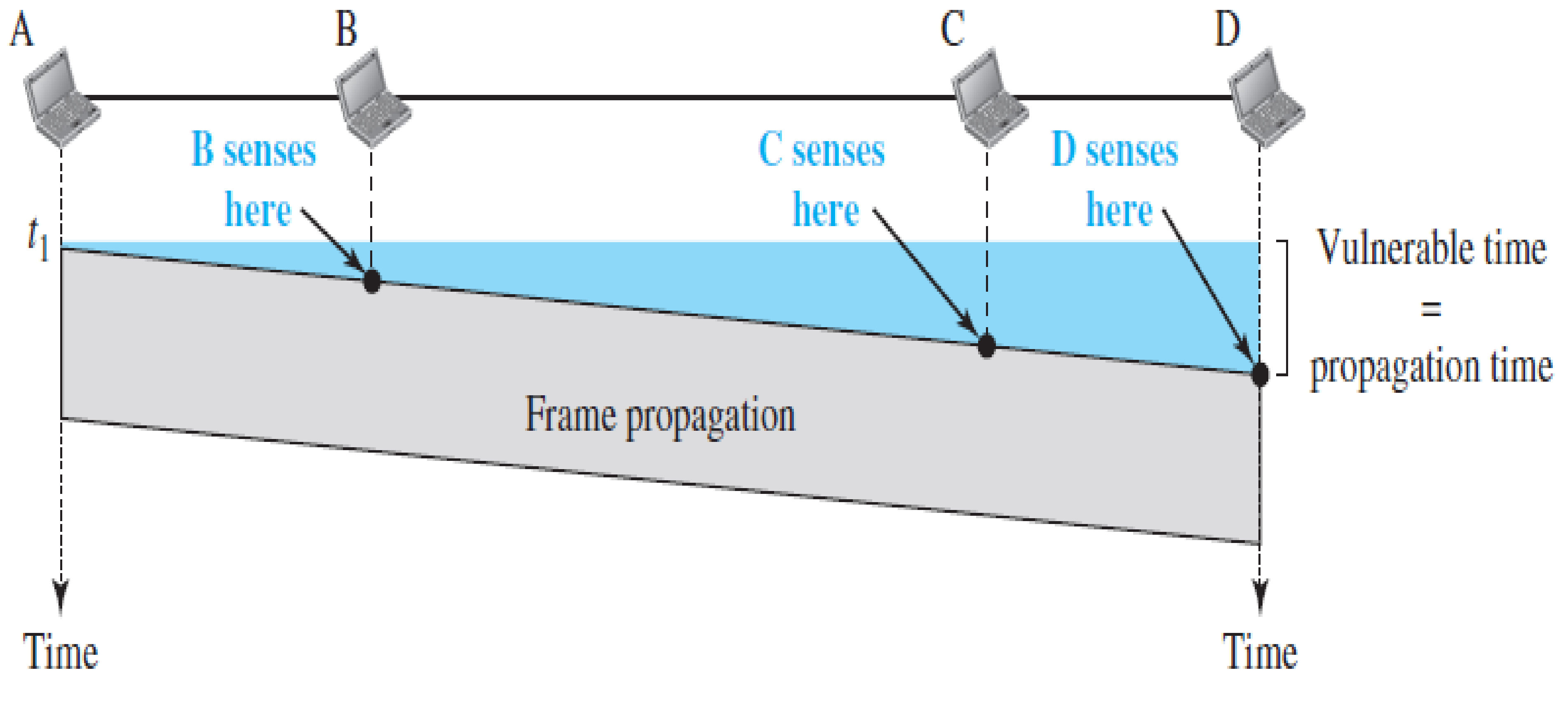
- The possibility of collision still exists because of propagation delay; when a station sends a frame, it still takes time (although very short) for the first bit to reach every station and for every station to sense it. In other words, a station may sense the medium and find it idle, only because the first bit sent by another station has not yet been received.



B starts at time t_1
C starts at time t_2
A
B
C
D
t_1
t_2
Area where B's signal exists
Area where both signals exist
Area where C's signal exists
Time
Collision occurs at this point
Time

Vulnerable Time

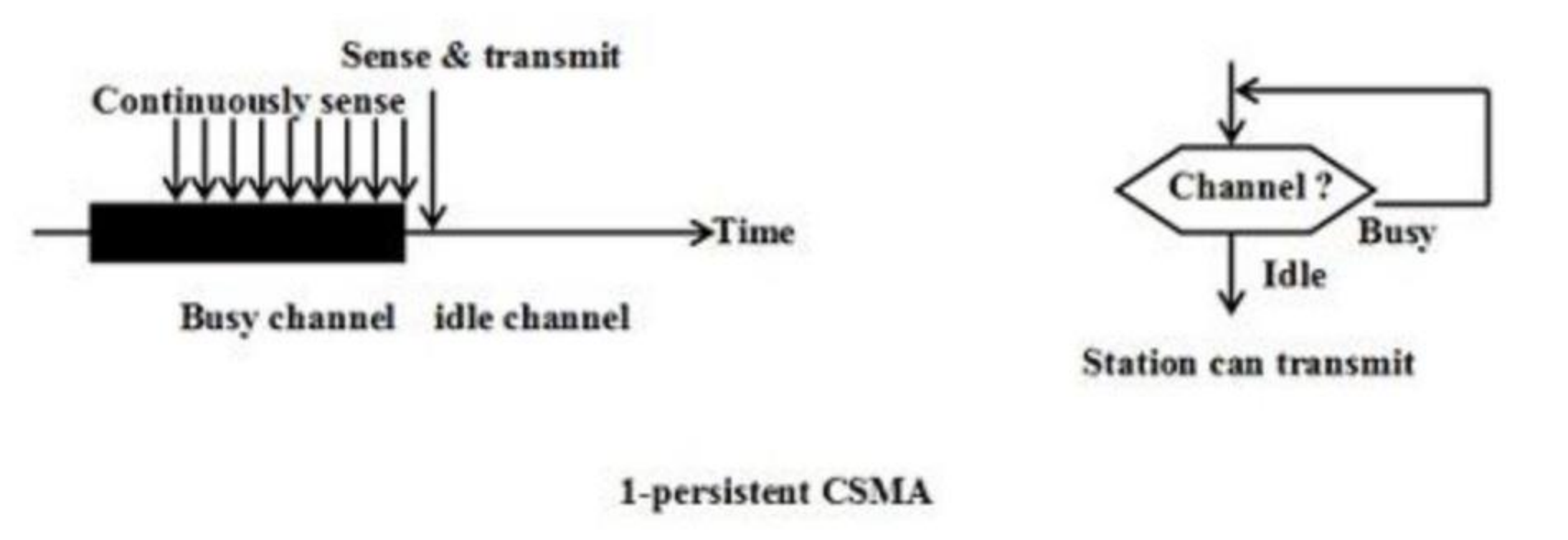
- The vulnerable time for CSMA is the ***propagation time*** *Tp*. When a station sends a frame and any other station tries to send a frame during this time, a collision will result.
- But if the first bit of the frame reaches the end of the medium, every station will already have heard the bit and will refrain from sending.



Persistence Methods

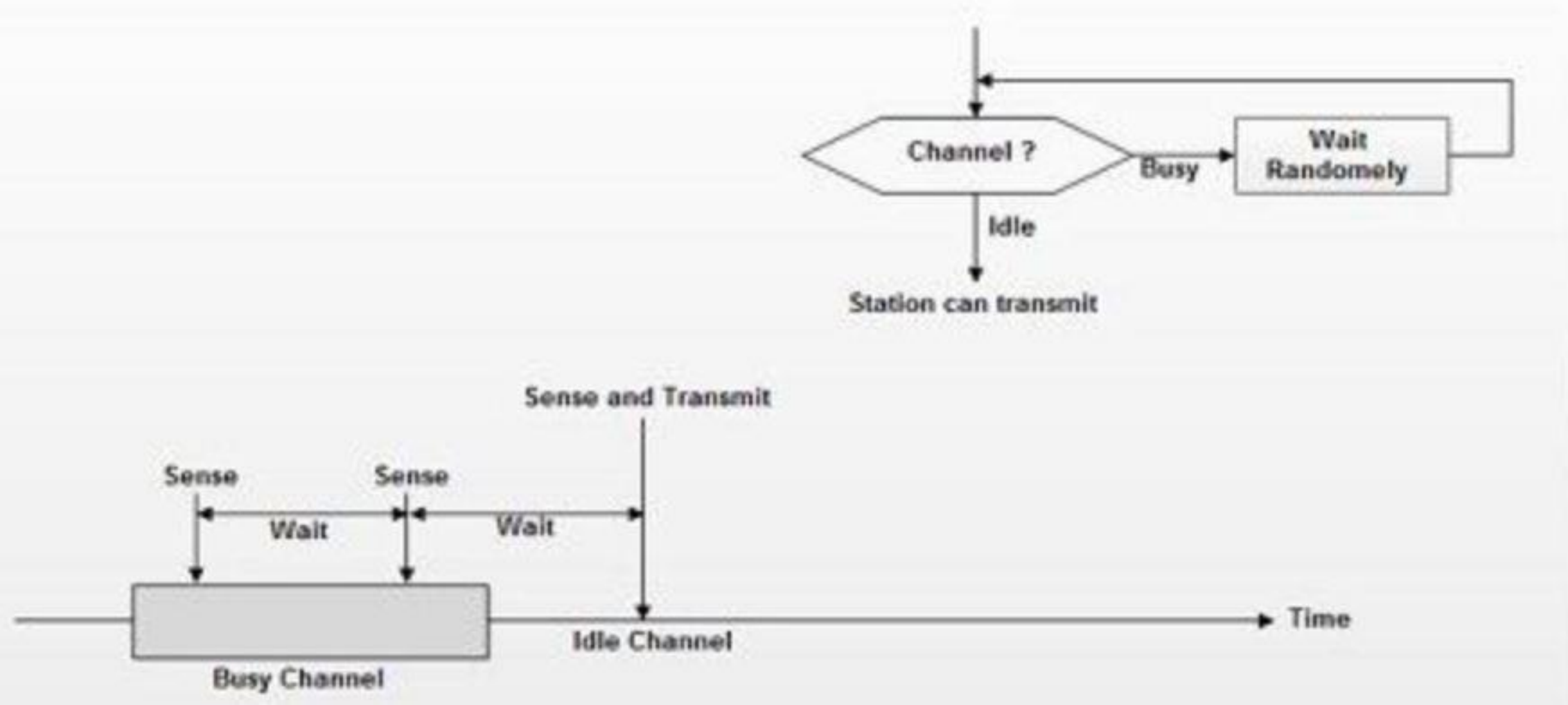
- What should a station do if the channel is busy? What should a station do if the channel is idle?
- Three methods have been devised to answer these questions:
  - 1-persistent method
  - Non-persistent method
  - P-persistent method.

- **1-Persistent**
  - The 1-persistent method is simple and straightforward. In this method, after the station finds the line idle, it sends its frame immediately (with probability 1). This method has the highest chance of collision because two or more stations may find the line idle and send their frames immediately.

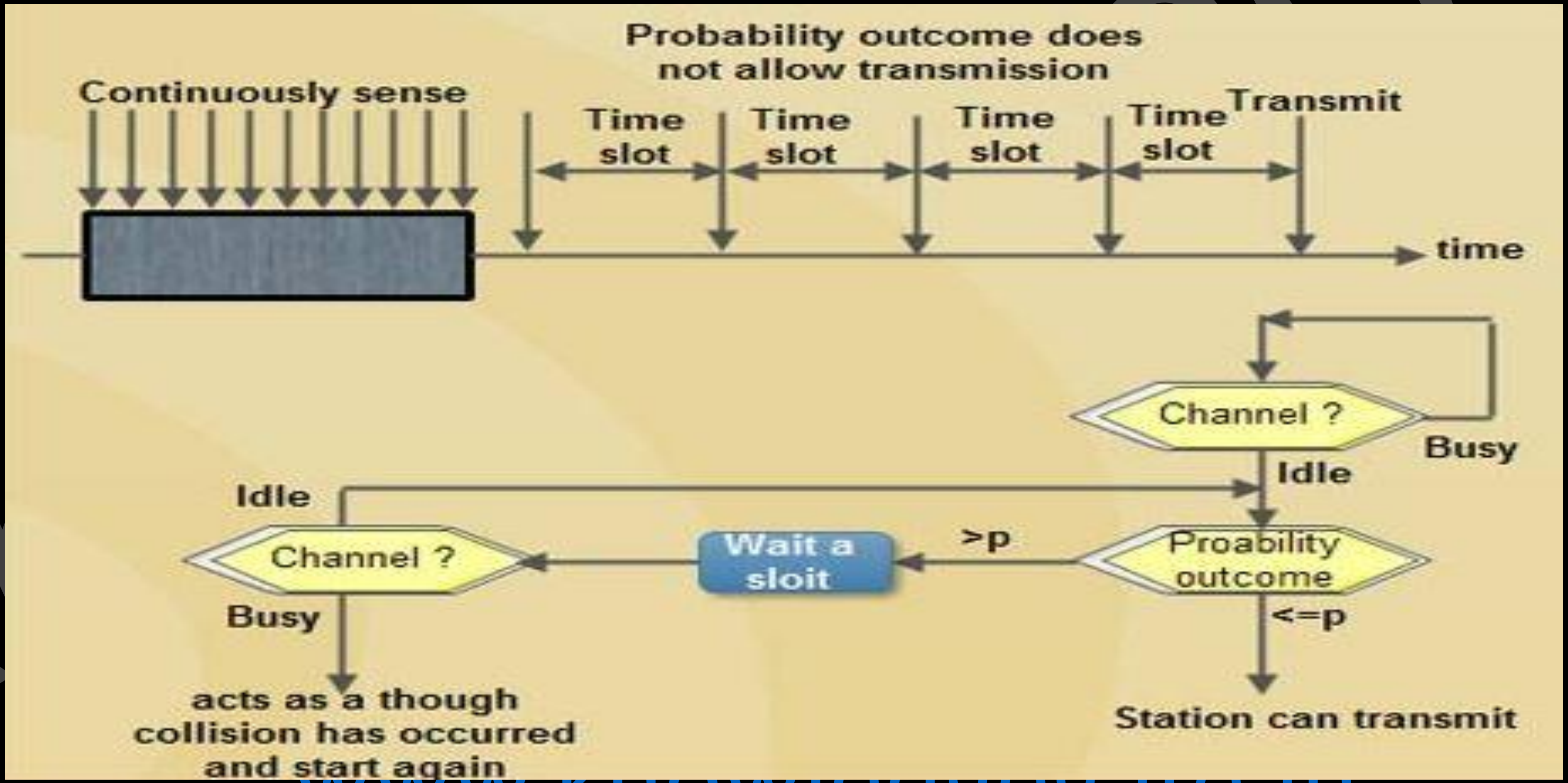


1-persistent CSMA

- **Nonpersistent**
  - In the nonpersistent method, a station that has a frame to send senses the line. If the line is idle, it sends immediately. If the line is not idle, it waits a random amount of time and then senses the line again.
  - The nonpersistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously. However, this method reduces the efficiency of the network because the medium remains idle when there may be stations with frames to send.

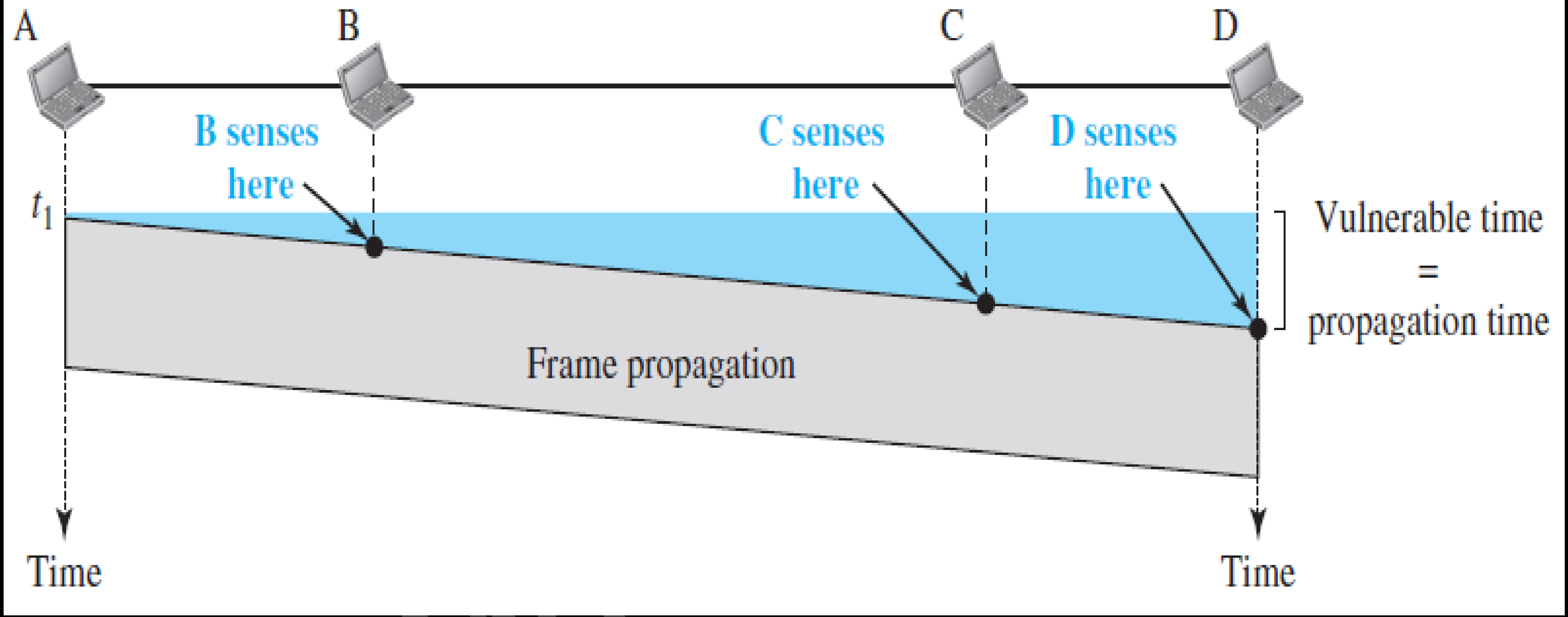


- **P-Persistent**
  - The p-persistent approach combines the advantages of the other two strategies. It reduces the chance of collision and improves efficiency. In this method, after the station finds the line idle it follows these steps:
  - With probability p, the station sends its frame.
  - With probability q = 1 - p, the station waits for the beginning of the next time slot and checks the line again.
    - a. If the line is idle, it goes to step 1.
    - b. If the line is busy, it acts as though a collision has occurred and uses the backoff procedure.

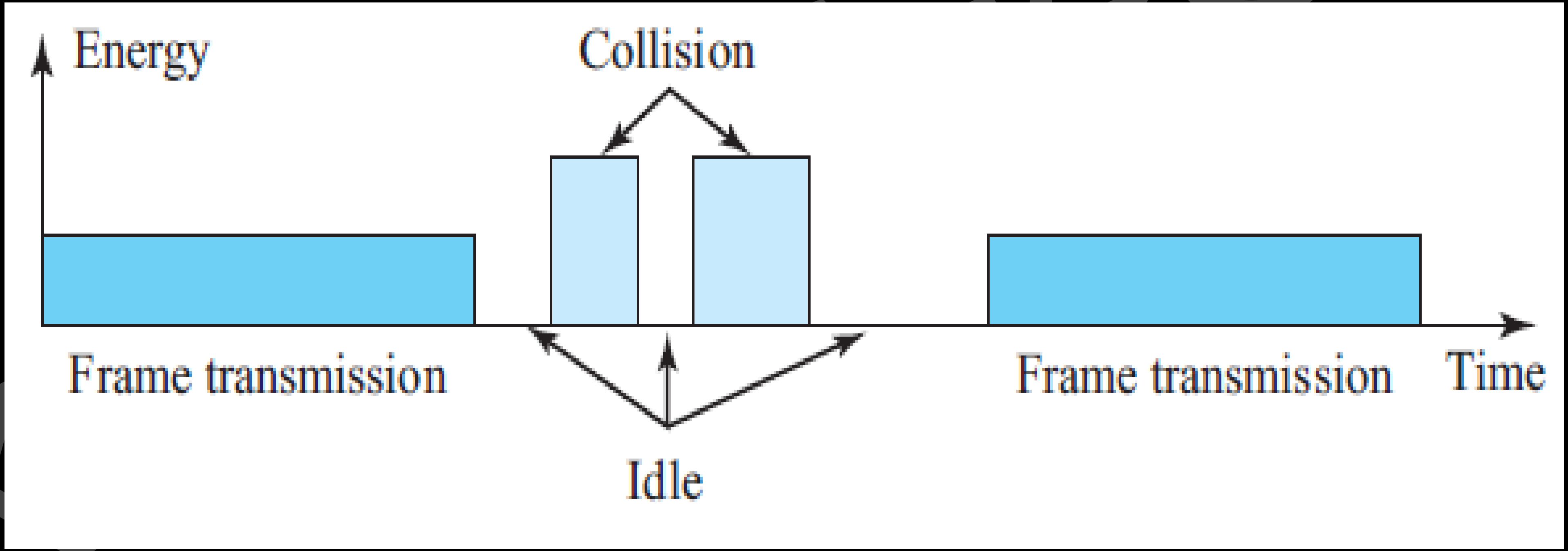


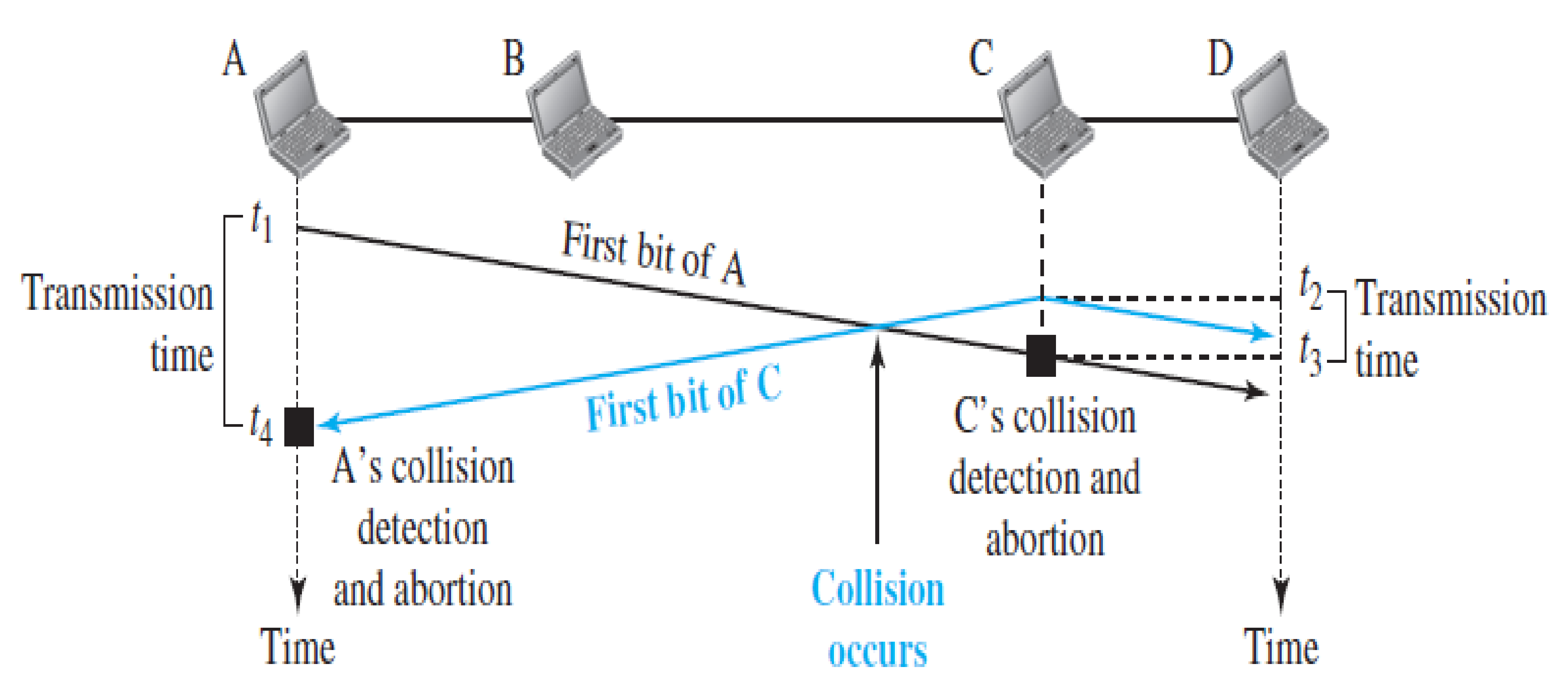
Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

- In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If so, the station is finished. If, however, there is a collision, the frame is sent again.
- Minimum Frame Size - For CSMA / CD to work, we need a restriction on the minimum frame size. Before sending the last bit of the frame, the sending station must detect a collision, if any, and abort the transmission.
- This is so because the station, once the entire frame is sent, does not monitor the line for collision detection. Therefore, the frame transmission time T_{fr} must be at least two times the maximum propagation time Tp.
- To understand the reason, let us think about the worst-case scenario. If the two stations involved in a collision are the maximum distance apart, the signal from the first takes time T_p to reach the second, and the effect of the collision takes another time T_p to reach the first. So the requirement is that the first station must still be transmitting after $2T_p$.


A
B
C
D
B senses here
C senses here
D senses here
t_1
Vulnerable time = propagation time
Frame propagation
Time
Time

- **Energy Level**
  - We can say that the level of energy in a channel can have three values: zero, normal, and abnormal. At the zero level, the channel is idle. At the normal level, a station has successfully captured the channel and is sending its frame.
  - At the abnormal level, there is a collision and the level of the energy is twice the normal level. A station that has a frame to send or is sending a frame needs to monitor the energy level to determine if the channel is idle, busy, or in collision mode.



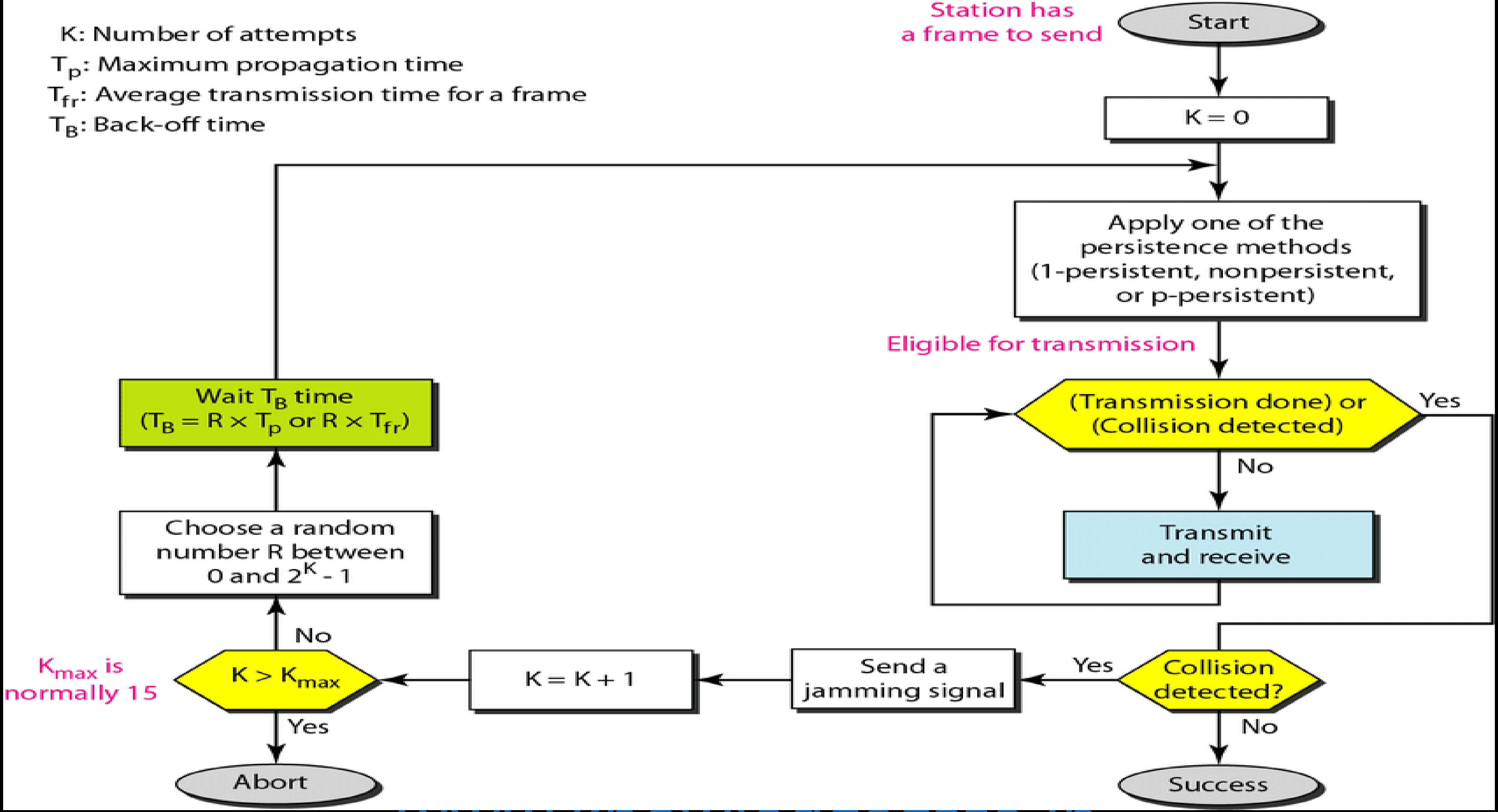

A
B
C
D
t_1
Transmission time
t_4
First bit of A
First bit of C
t_2
t_3
Transmission time
A's collision detection and abortion
Collision occurs
C's collision detection and abortion
Time
Time

K: Number of attempts

T_p: Maximum propagation time

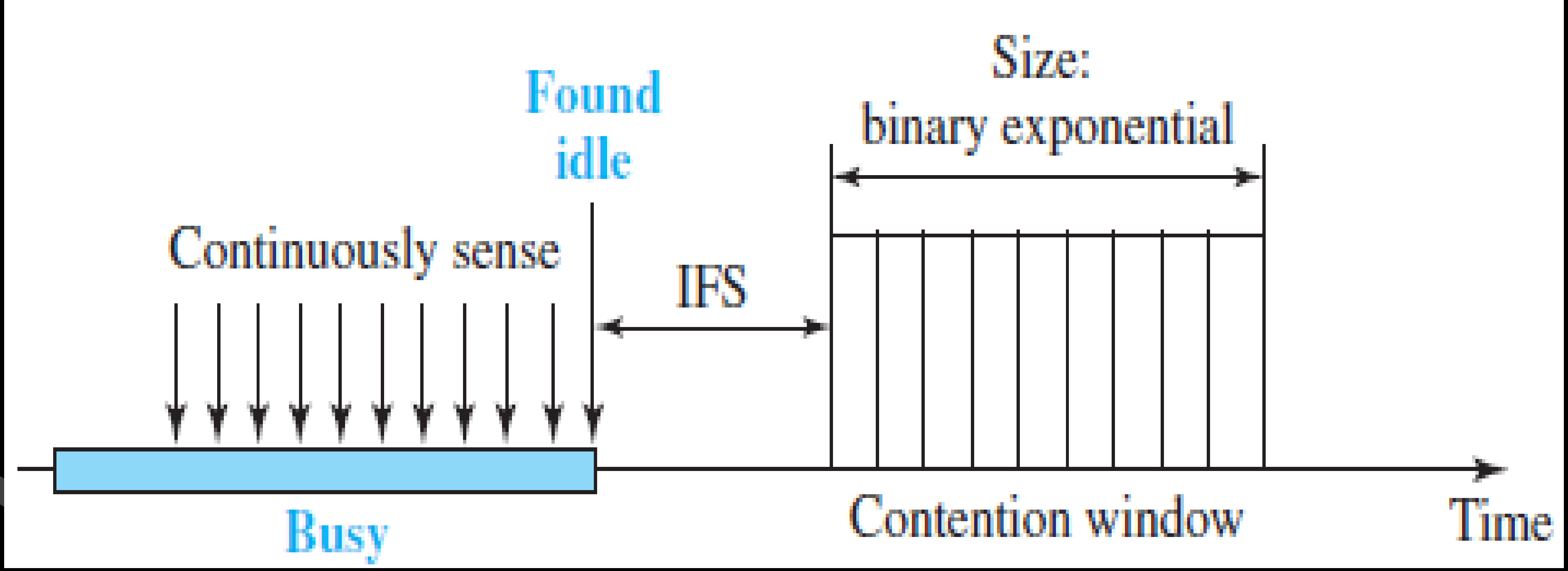
T_{fr}: Average transmission time for a frame

T_B: Back-off time

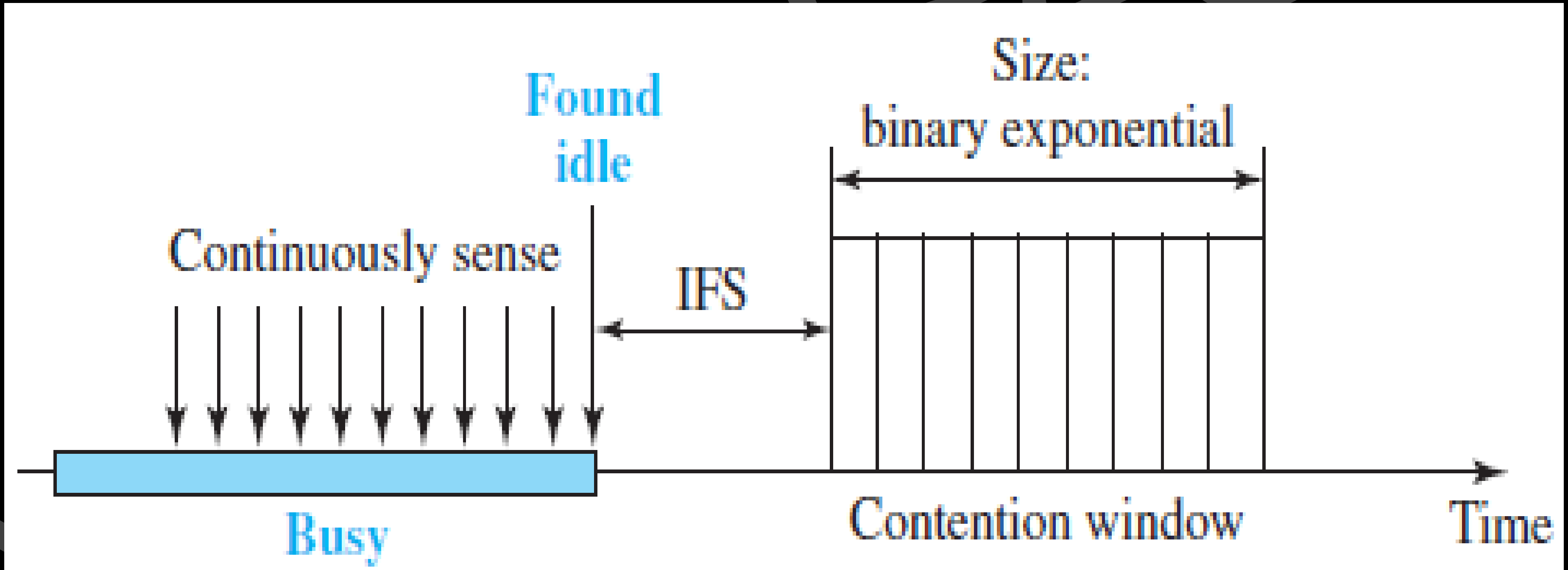

Station has a frame to send
Start
K = 0
Apply one of the persistence methods (1-persistent, nonpersistent, or p-persistent)
Eligible for transmission
(Transmission done) or (Collision detected)
Yes
No
Transmit and receive
Collision detected?
Yes
No
Success
Send a jamming signal
K = K + 1
$K > K_{max}$
K_{max} is normally 15
Yes
Abort
No
Choose a random number R between 0 and 2^K - 1
Wait T_B time
($T_B = R \times T_p$ or $R \times T_{fr}$)

Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

- In a wireless network, much of the sent energy is lost in transmission. The received signal has very little energy. Therefore, a collision may add only 5 to 10 percent additional energy. This is not useful for effective collision detection.
- We need to avoid collisions on wireless networks because they cannot be detected. Carrier sense multiple access with collision avoidance (CSMA / CA) was invented for this network. Collisions are avoided through the use of CSMA / CA
- three strategies: the interframe space, the contention window, and acknowledgment



- **Interframe Space (IFS)**
  - First, collisions are avoided by deferring transmission even if the channel is found idle. When an idle channel is found, the station does not send immediately. It waits for a period of time called the interframe space or IFS.
  - The IFS time allows the front of the transmitted signal by the distant station to reach this station. If after the IFS time the channel is still idle, the station can send, but it still needs to wait a time equal to the contention time. The IFS variable can also be used to prioritize stations or frame types.



Contention Window

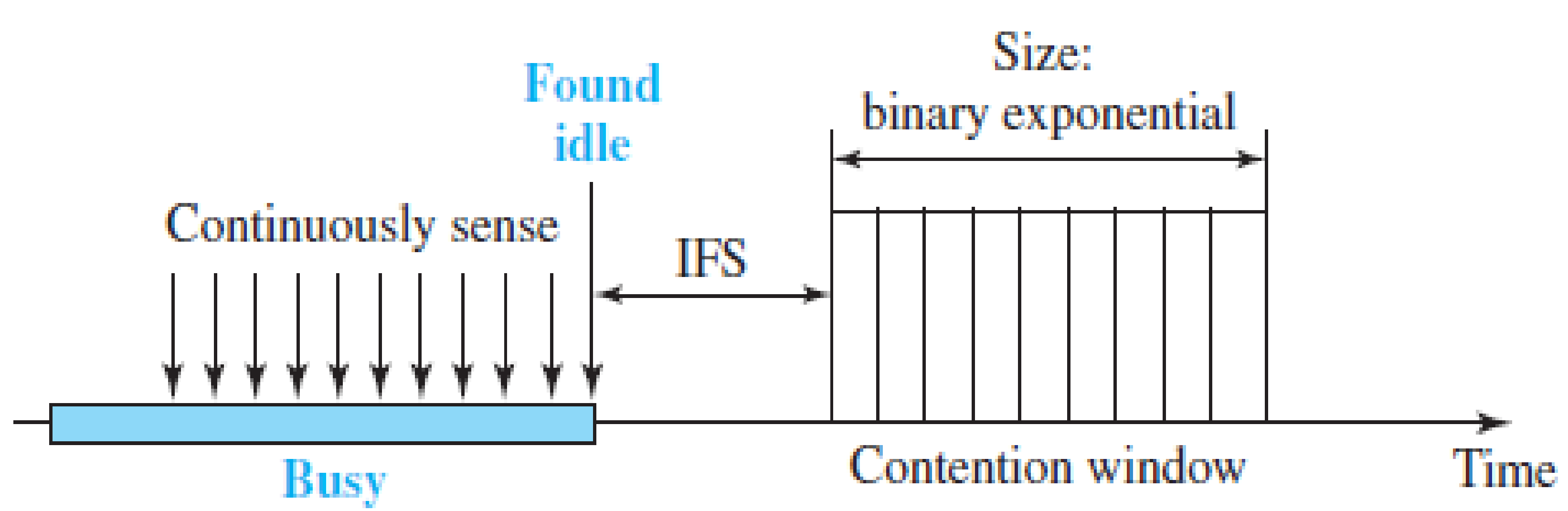
- The contention window is an amount of time divided into slots. A station that is ready to send chooses a random number of slots as its wait time.

- The number of slots in the window changes according to the binary exponential back-off strategy.

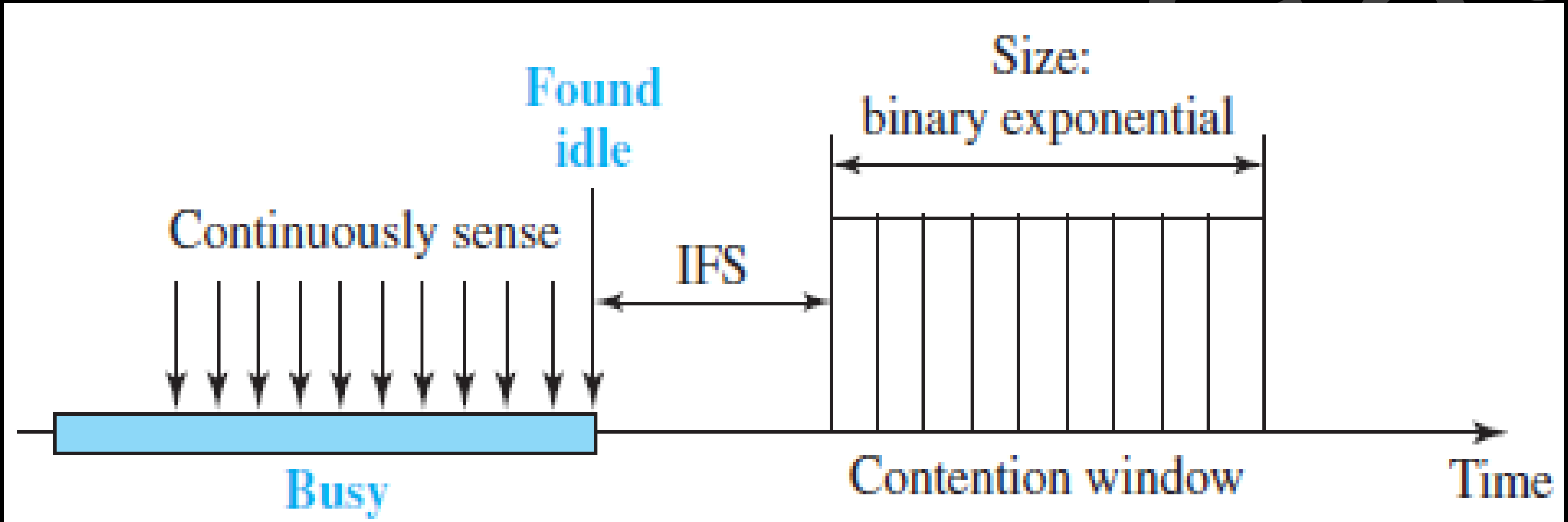
- This means that it is set to one slot the first time and then doubles each time.

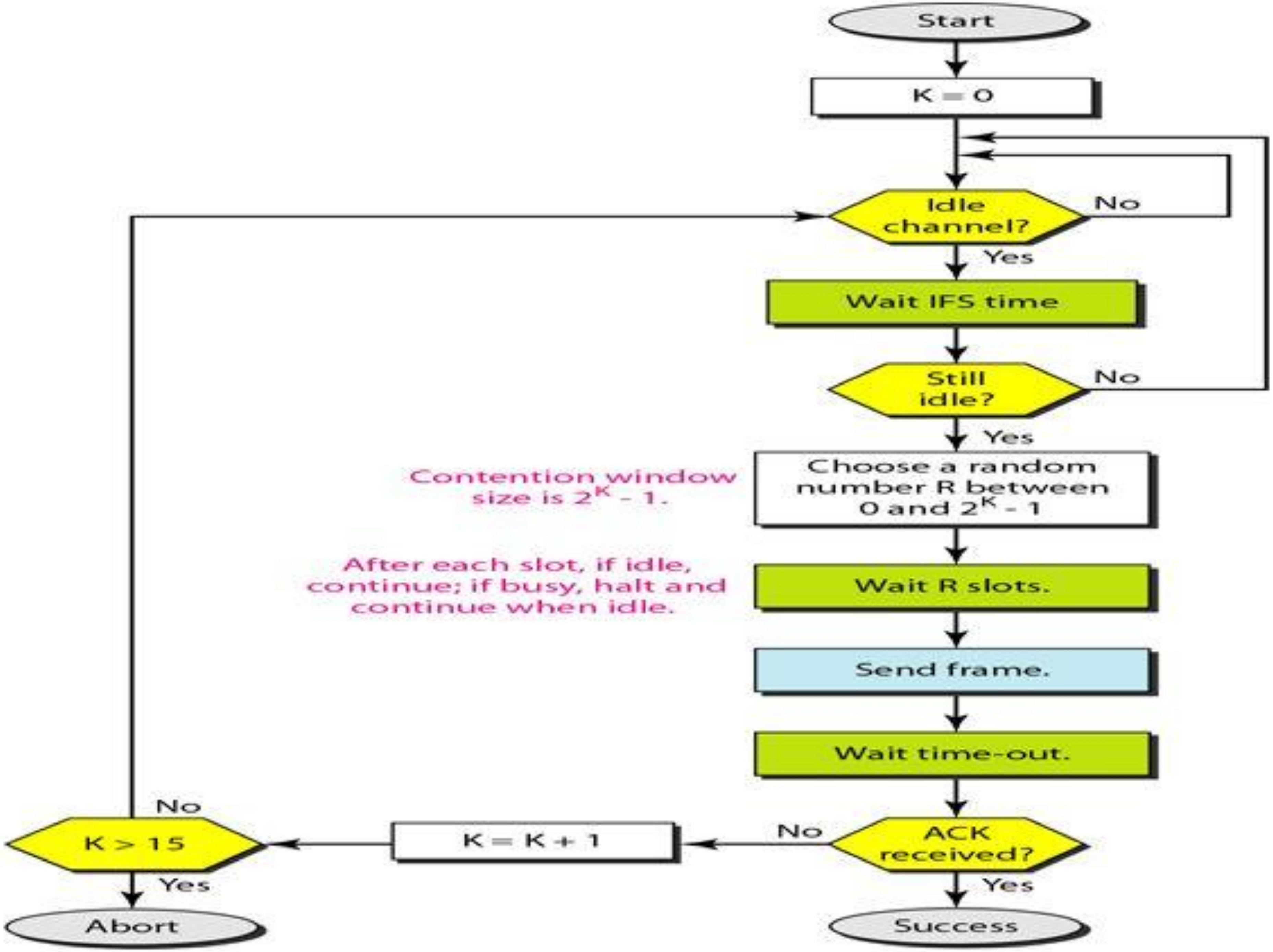
- One interesting point about the contention window is that the station needs to sense the channel after each time slot.

- However, if the station finds the channel busy, it does not restart the process; it just stops the timer and restarts it when the channel is sensed as idle. This gives priority to the station with the longest waiting time.



- **Acknowledgment**
  - With all these precautions, there still may be a collision resulting in destroyed data. In addition, the data may be corrupted during the transmission. The positive acknowledgment and the time-out timer can help guarantee that the receiver has received the frame.





Start

K = 0

Idle channel?

No

Yes

Wait IFS time

Still idle?

No

Yes

Choose a random number R between 0 and $2^K - 1$

Contention window size is $2^K - 1$.

Wait R slots.

After each slot, if idle, continue; if busy, halt and continue when idle.

Send frame.

Wait time-out.

ACK received?

No

Yes

Success

K = K + 1

K > 15

No

Yes

Abort

FLOW CONTROL

- To prevent data overflow, the receiving device has a buffer memory where incoming data are temporarily stored until processed; the data processing speed often lags behind the transmission rate.
- If the buffer is nearing its capacity, the receiver somehow must communicates with the sender to reduce the number of frames sent or pause transmission temporarily, ensuring smooth data flow and preventing system overload.

ERROR CONTROL

- **(lost, out of order, corrupt) (detection and retransmission)**
- Error control, encompassing error detection and correction, enables the receiver to notify the sender about lost or damaged frames during transmission, facilitating the coordination for their retransmission.
- In the data link layer, error control is commonly implemented through the Automatic Repeat Request (ARQ) process, where detected errors trigger the retransmission of specific frames to maintain data integrity.

Sliding Window Protocol

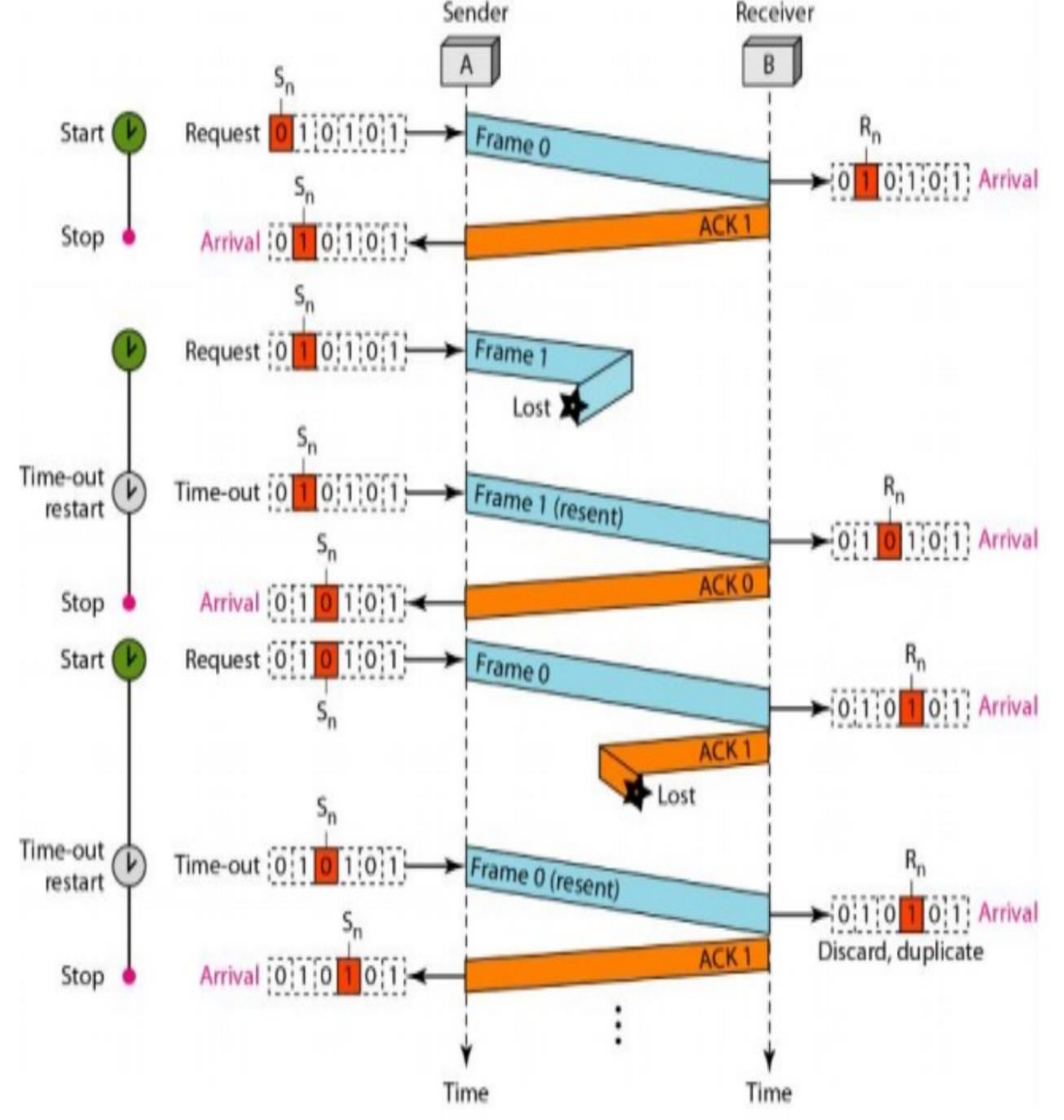
1. Stop-and-Wait Automatic Repeat Request
2. Go-Back-N Automatic Repeat Request
3. Selective Repeat Automatic Repeat Request

Stop-and-Wait Automatic Repeat Request

- When the frame arrives at the receiver site, it is checked and if it is corrupted, it is silently discarded. The detection of errors in this protocol is manifested by the silence of the receiver and no ack in send to sender.

- The sender keeps a copy of the sent frame. At the same time, it starts a timer. If the timer expires and there is no ACK for the sent frame, the frame is resent, the copy is held, and the timer is restarted.

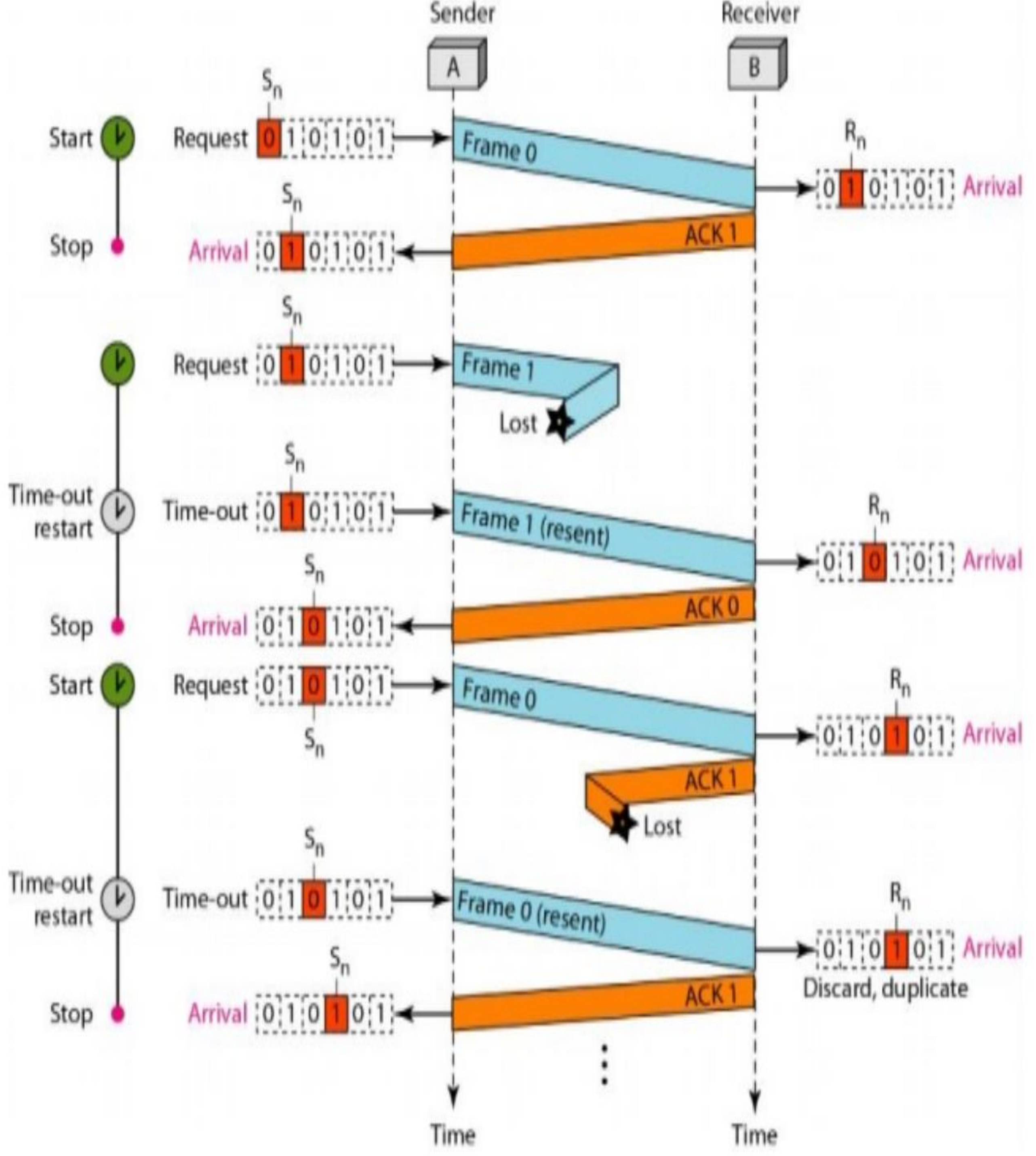
- Lost frames are more difficult to handle than corrupted ones. The solution is to number the frames. When the receiver receives a data frame that is out of order, this means that frames were either lost or duplicated.



Sequence Numbers

- Frames are numbered using sequence numbers, added in a field within the data frame, to facilitate unambiguous communication with minimized frame size; the numbering can wrap around in a defined range.

- Sequence numbers only need to alternate between 0 and 1, enabling the receiver to differentiate between new frames and retransmitted frames without confusion, thereby optimizing the communication process.

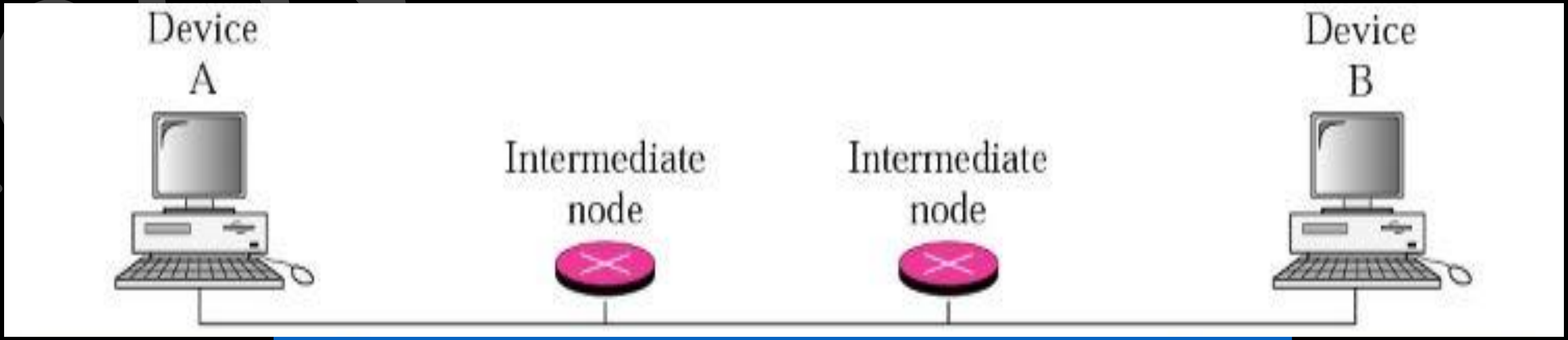


- **Propagation Delay:** Propagation delay is the time it takes for a bit to travel from point A to point B in the transmission media.
  T_P = (Distance) / (Propagation speed)

- **Transmission Delay (TT):** A sender needs to put the bits in a packet on the line one by one. If the first bit of the packet is put on the line at time t_1 and the last bit is put on the line at time t_2, transmission delay of the packet is $(t_2 - t_1)$.
  T_t = (Packet length (L)) / (Transmission rate or Bandwidth (B)) = L / B

- ***Queuing Delay*** **-** It is measured as the time a packet waits in the input queue and output queue of a router.
  - Delay_{qu} = The time a packet waits in input and output queues in a router

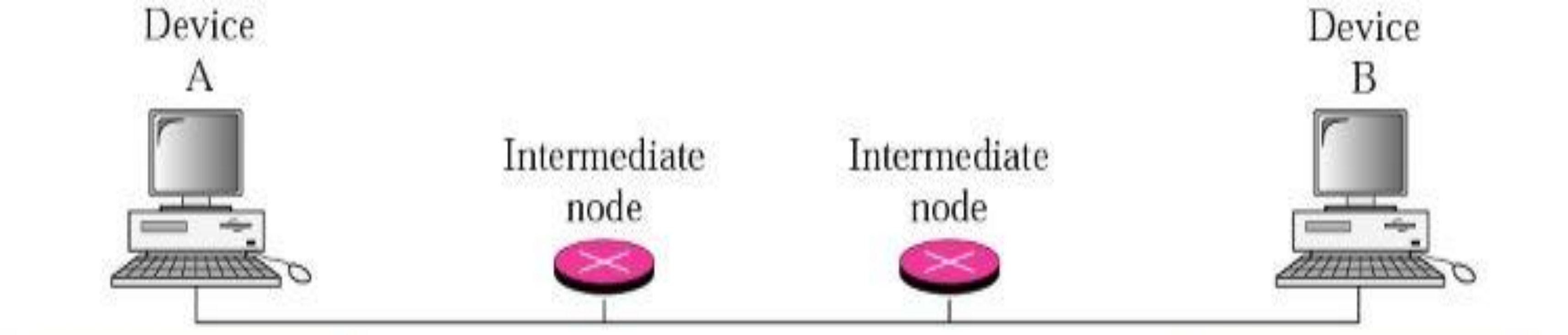
- ***Processing Delay*** **-** It is the time required for a destination host to receive a packet from its input port, remove the header, perform an error detection procedure, and deliver the packet to the output port or deliver the packet to the upper-layer protocol (in the case of the destination host).
  - Delay_{pr} = Time required to process a packet in a destination host



Measuring Performance for Stop and Wait

1. Total time = $T_{t\ (data)} + T_{p\ (data)}$ + $Dealy_{que}$ + $Delay_{pro}$ + $T_{t\ (ack)} + T_{p\ (ack)}$ + $Dealy_{que}$ + $Delay_{pro}$
2. Queuing delay and processing delays are generally kept 0.
   - Total Time = $T_{t\ (data)} + T_{p\ (data)} + T_{t\ (ack)} + T_{p\ (ack)}$
3. In general we have taken $T_{t\ (ack)}$ as negligible as the ack size is generally very less
   - Total Time = $T_{t\ (data)} + T_{p\ (data)} + T_{p\ (ack)}$
4. The T_p for data and ack are going to be same
   - Total Time = $T_{t\ (data)} + 2*T_p$

- Note:- Some times *$2 * T_p$ time is also called Round Trip Time (RTT)*



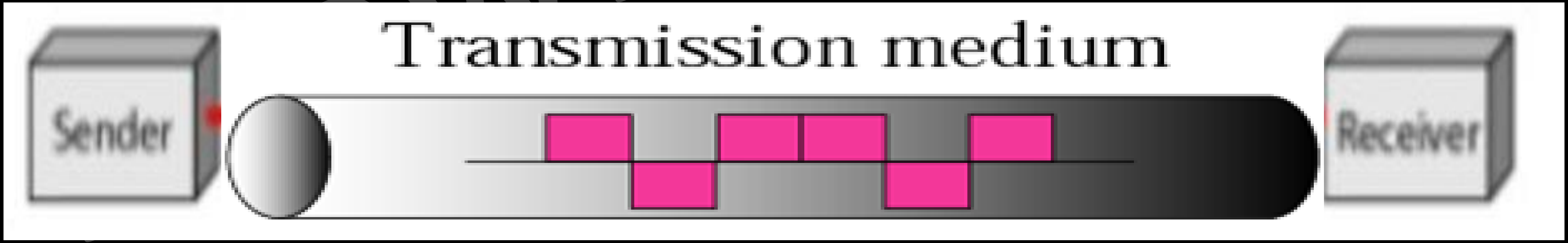
- **Efficiency(η)**:-
  - Useful Time / Total Cycle time = T_t / T_t + 2 * T_p
  - Here, Useful time in the entire cycle time is T_t and for the rest 2 * T_p time we are waiting for the processing, whereas instead of waiting we could have sent more packets.
  - Dividing numerator and denominator with T_t, we get: η = 1 / 1 + (2 * T_p/T_t)
  - So, η = 1 / 1 + 2a, (where a = T_p / T_t)

- Effective Bandwidth / Throughput / Bandwidth Utilization is calculated as:
- Throughput = η * B (efficiency * bandwidth)

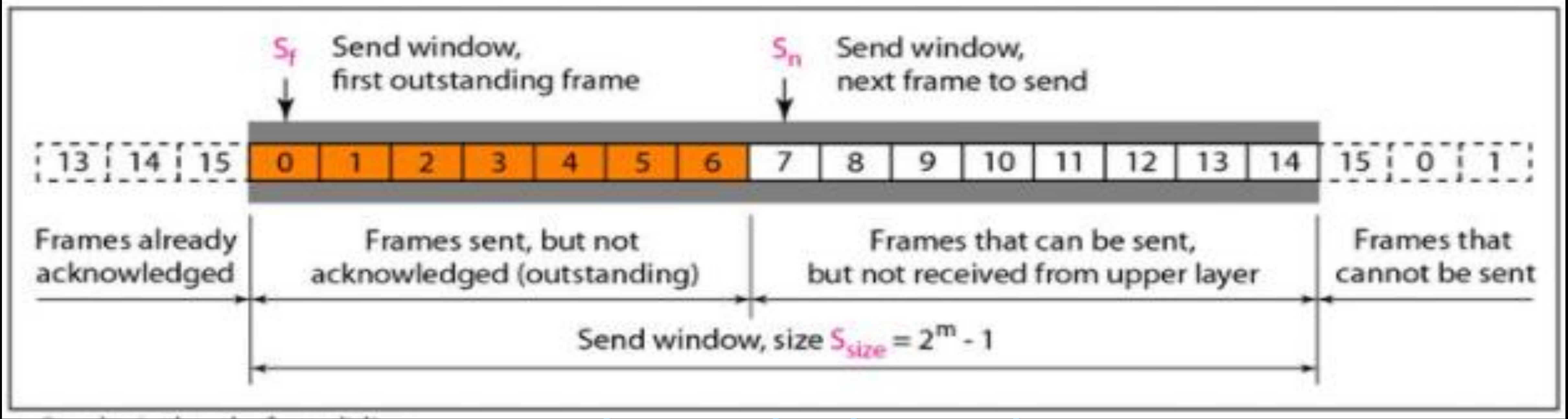
Go-Back-N Automatic Repeat Request

- The Stop-and-Wait ARQ method can be inefficient for channels with high bandwidth, resulting in underutilization of the available data pipeline. Solution is Go-Back-N.

- To enhance transmission efficiency, the Go-Back-N ARQ protocol allows multiple frames to be transmitted before acknowledgments are received, utilizing a "sliding window" concept.

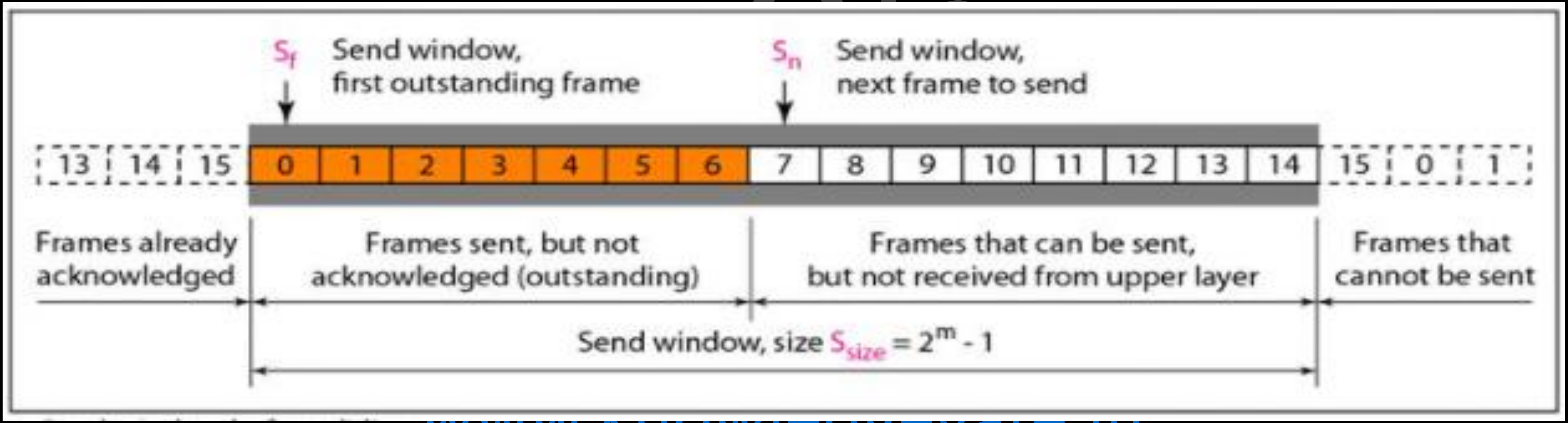


- The send window, an imaginary concept, covers the sequence numbers of frames that can be in transit, having a maximum size of $2^m - 1$.
- Sequence numbers are divided into four regions: the first represents acknowledged frames (no copies kept), the second represents frames sent but with unknown status (outstanding frames), the third denotes frames ready to be sent pending data packets from the network layer, and the fourth signifies sequence numbers inaccessible until the window slides further.



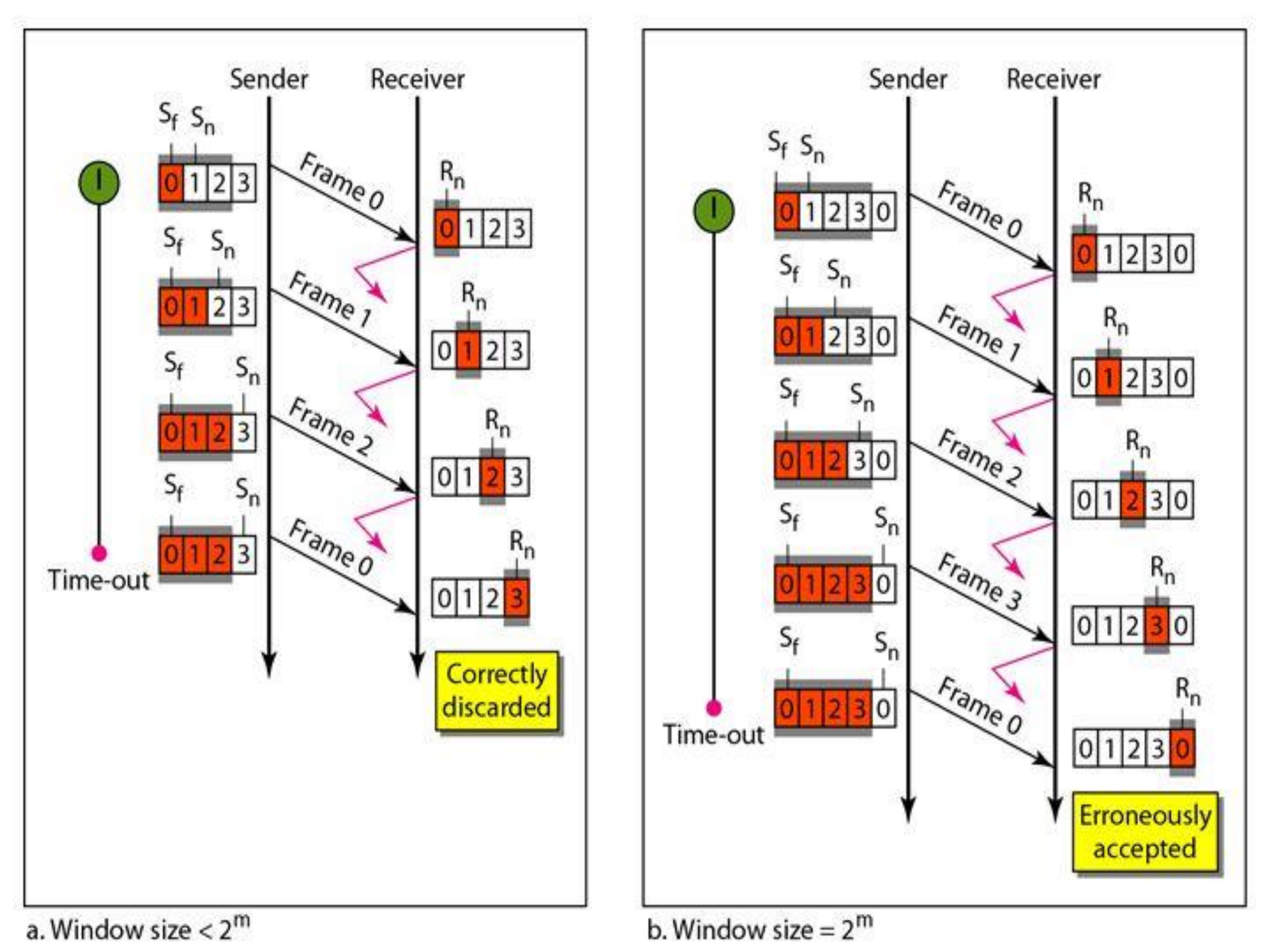
S_f Send window, first outstanding frame
S_n Send window, next frame to send
13 14 15 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 0 1
Frames already acknowledged
Frames sent, but not acknowledged (outstanding)
Frames that can be sent, but not received from upper layer
Frames that cannot be sent
Send window, size $S_{size} = 2^m - 1$

- The send window is characterized by three variables:
    - S_f (marks the first outstanding frame)
    - S_n (indicates the next frame to be dispatched)
    - S_{size} (represents the fixed window size).
- Conversely, the receive window, with a constant size of one, ensures the receipt of correct data frames and the issuance of appropriate acknowledgments, discarding and necessitating the resending of any out-of-order frames.


S_f
Send window, first outstanding frame
S_n
Send window, next frame to send
13
14
15
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
0
1
Frames already acknowledged
Frames sent, but not acknowledged (outstanding)
Frames that can be sent, but not received from upper layer
Frames that cannot be sent
Send window, size $S_{size} = 2^m - 1$

Timers

- Although there can be a timer for each frame that is sent, in our protocol we use only one. The reason is that the timer for the first outstanding frame always expires first; we send all outstanding frames when this timer expires.

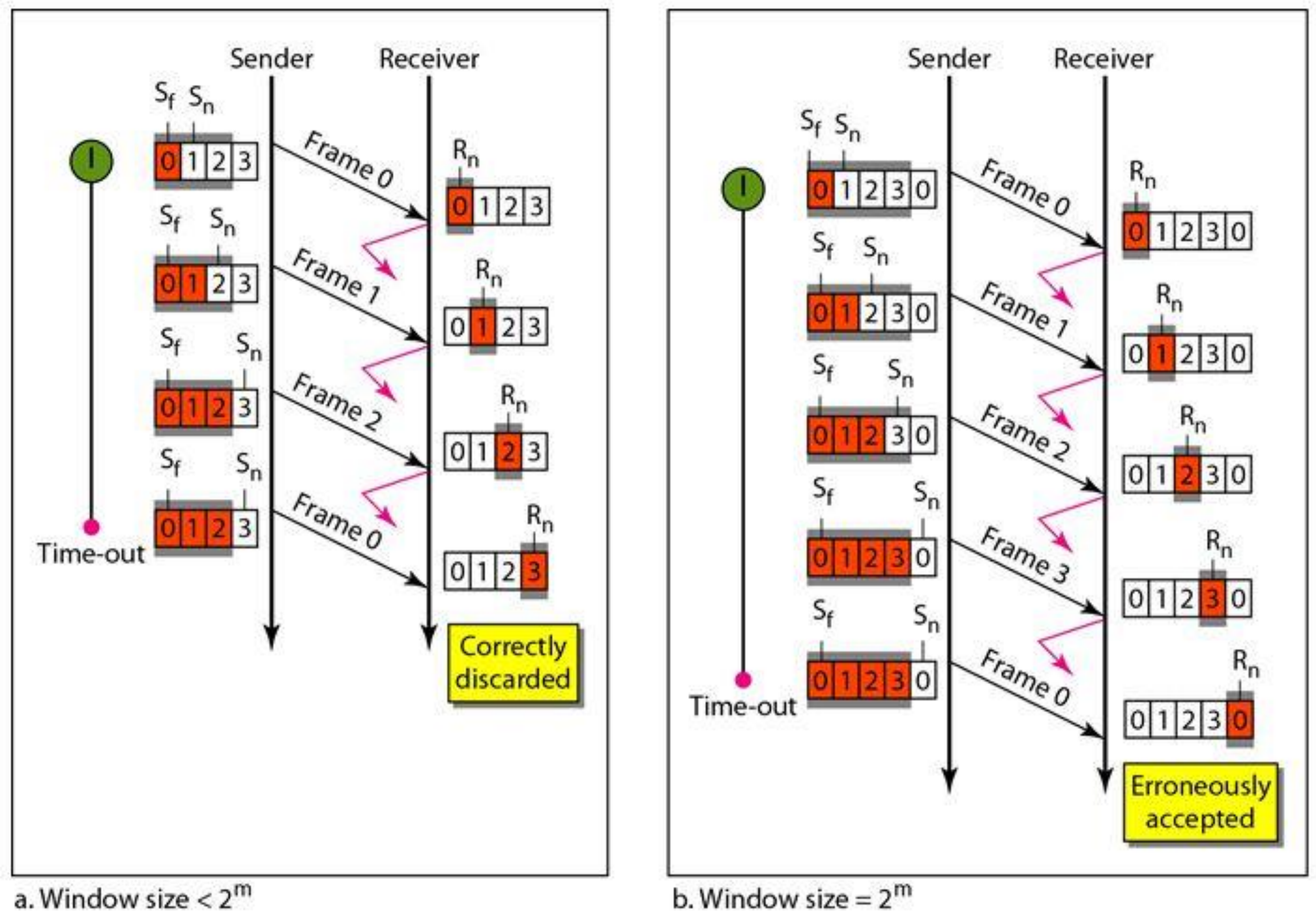


a. Window size < 2^m

b. Window size = 2^m

Acknowledgment

- The receiver sends a positive acknowledgment for frames that arrive intact and in the correct order, whereas it remains silent and discards frames that are damaged or received out of sequence, maintaining a focus on the expected frame's arrival.
- The receiver's silence triggers the timer of the unacknowledged frame at the sender site to expire, prompting the sender to resend all frames from the one with the expired timer
- The receiver can issue a cumulative acknowledgment for multiple frames, enhancing efficiency.



Sequence and Acknowledgement Numbers

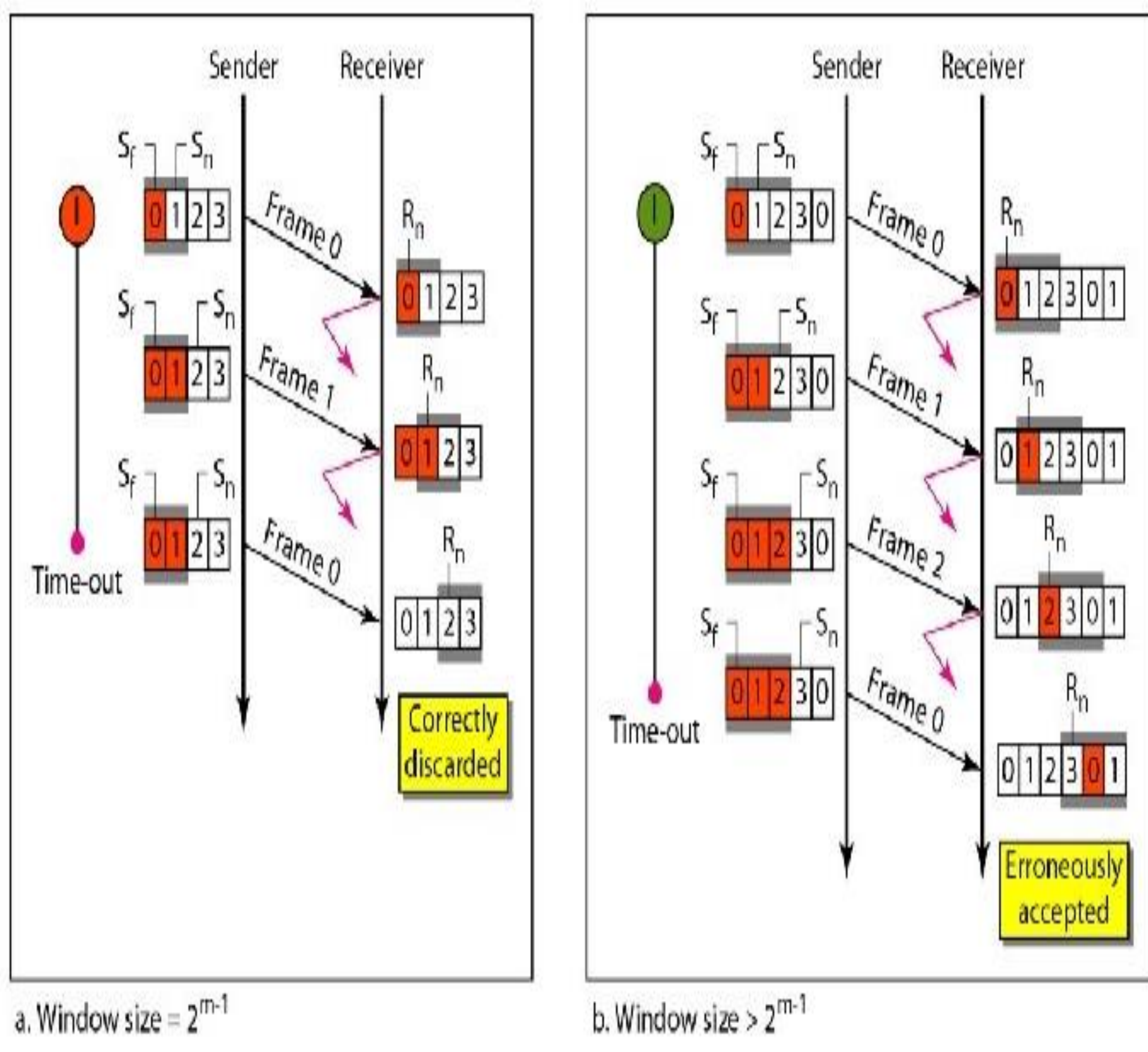
- To improve the efficiency of transmission (to fill the pipe), multiple packets must be in transition while the sender is waiting for acknowledgment

- In order to maximize the efficiency, the window size (W_s) = (1+ 2a)

- Number of bits required for sequence numbers = ceil ($\log_2$ (1 + 2a))

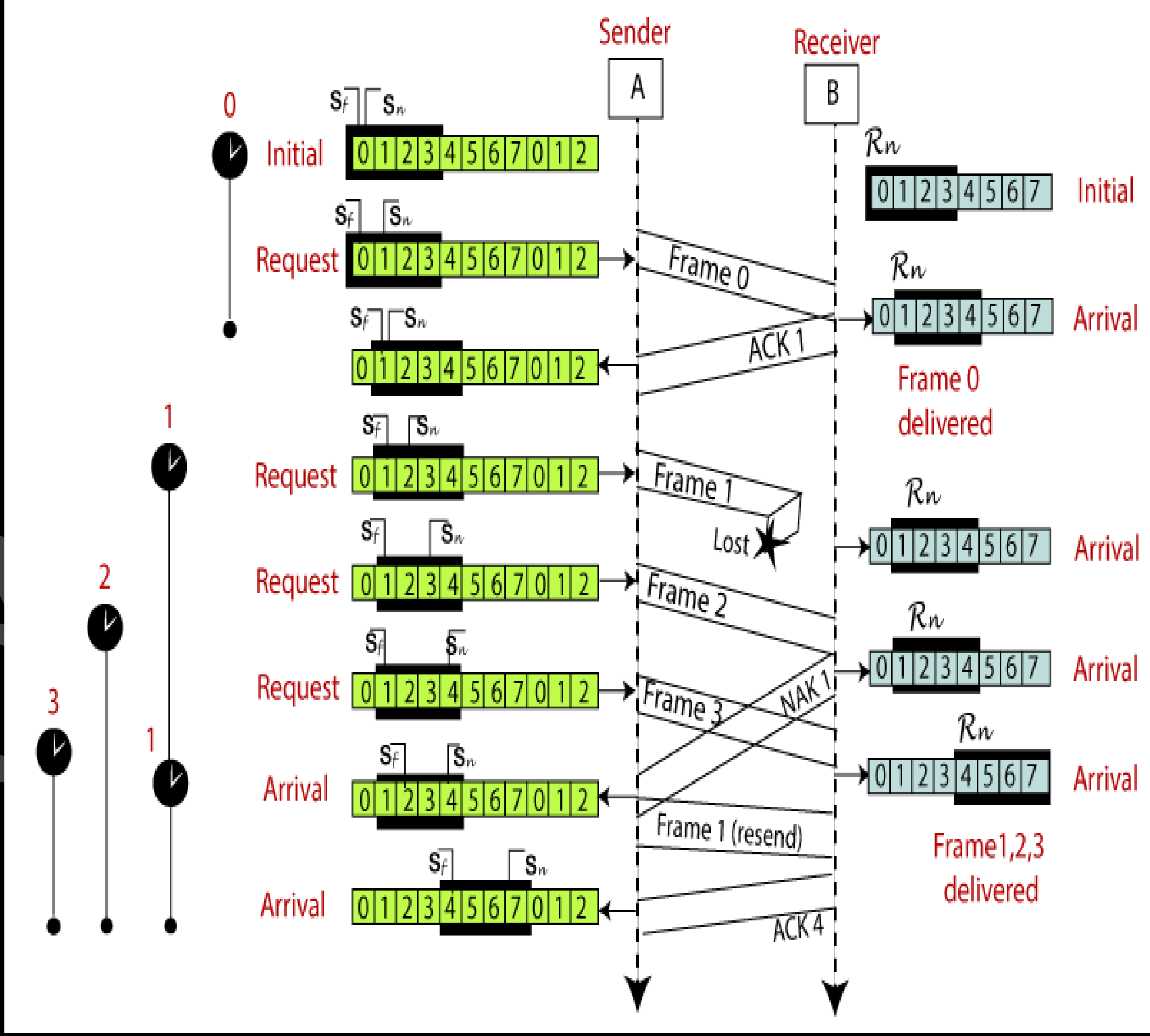
Selective Repeat Automatic Repeat Request

- Go-Back-N ARQ makes it easier for the receiver by only keeping track of one thing and ignoring frames that arrive in the wrong order. However, if the connection is not great, it can waste time and data by having to resend a bunch of frames often.
- If the connection is not stable, the Selective Repeat ARQ is better as it only resends the frames that didn't arrive correctly, saving time and data. But, it makes the receiver's job a bit tougher.
- The Selective Repeat ARQ also lets the receiver gather frames even if they come in the wrong order and keeps them until they can be arranged correctly and passed on, using equal room for storing and sending frames to work more efficiently.



- In Selective Repeat ARQ, the data windows for sending and receiving are kept fairly small to manage data better 2^{m-1}; each frame sent has its own countdown timer, making the tracking of requests quite similar to earlier methods but more detailed when data arrives.

- When a clear NAK message arrives, we simply send the frame again; if a clear ACK message comes, we clear old data, stop the related countdown, and move the window's starting point. If a timeout happens, only the late frame is sent again.



Piggybacking

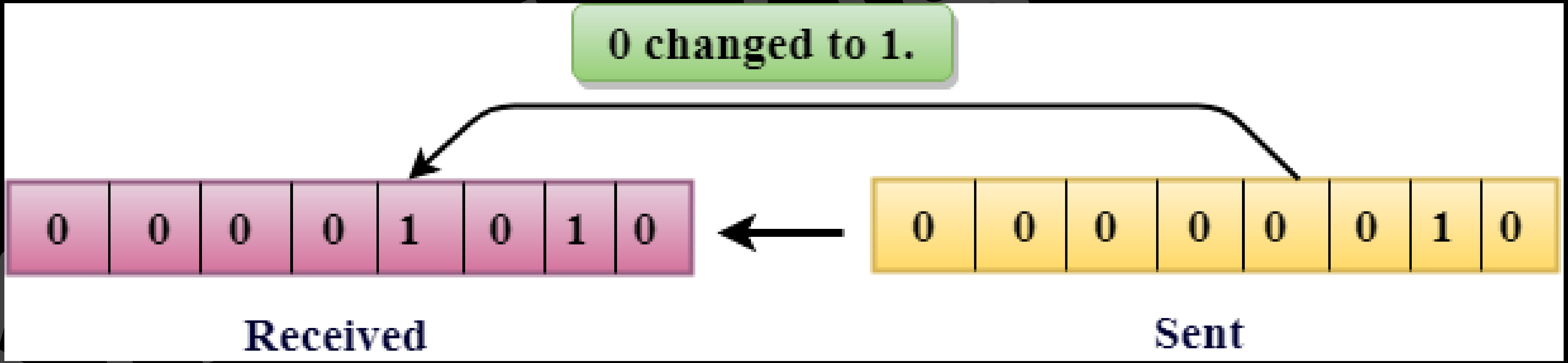
- The discussed protocols are unidirectional, primarily allowing data frames to move in one direction, although control signals like ACK and NAK can go both ways. In practice, data frames flow bidirectionally, requiring a method called piggybacking to enhance bidirectional protocol efficiency.

- Piggybacking enables a data frame moving from A to B to also convey control information regarding B's frames and vice versa, streamlining the communication process. Every node maintains two operational windows: a send and a receive window, along with a timer overseeing three events: request, arrival, and time-out.

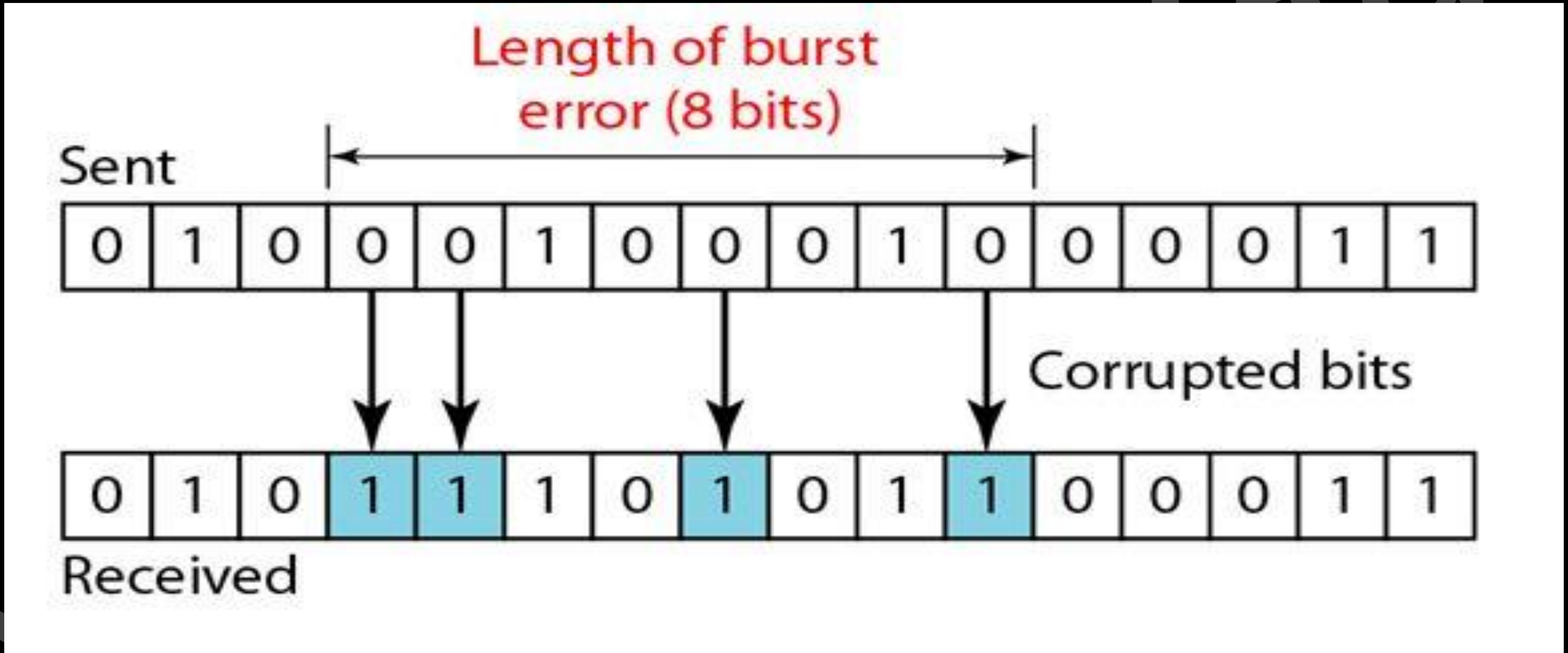
- This strategy complicates the arrival event, necessitating the simultaneous handling of control information and the actual data frame within a singular event, employing both windows at the respective site. A uniform algorithm, albeit complex, must be employed by both sites to effectively manage the unified arrival events.

Types of Errors

- Data transmitted between nodes can sometimes be altered or corrupted during transmission. This corruption can manifest as either a single-bit error or a burst error.
- A single-bit error refers to a scenario where only one bit in a data unit (like a byte or packet) is changed, either from 1 to 0 or vice versa. This type of error is less common.



- Burst error, on the other hand, involves the alteration of two or more bits within a data unit. These changes might not be in successive bits. It's a more common error type as noise typically affects a set of bits, the extent of which is influenced by the data rate and noise duration.



Sent: 0 1 0 0 0 1 0 0 0 1 0 0 0 0 1 1

Received: 0 1 0 1 1 1 0 1 0 1 1 0 0 0 1 1

Hamming Distance

- Hamming distance, represented as d(x, y), is a measure of the difference between two words of equal size, calculated by counting the number of dissimilar bits at the corresponding positions in the two words.

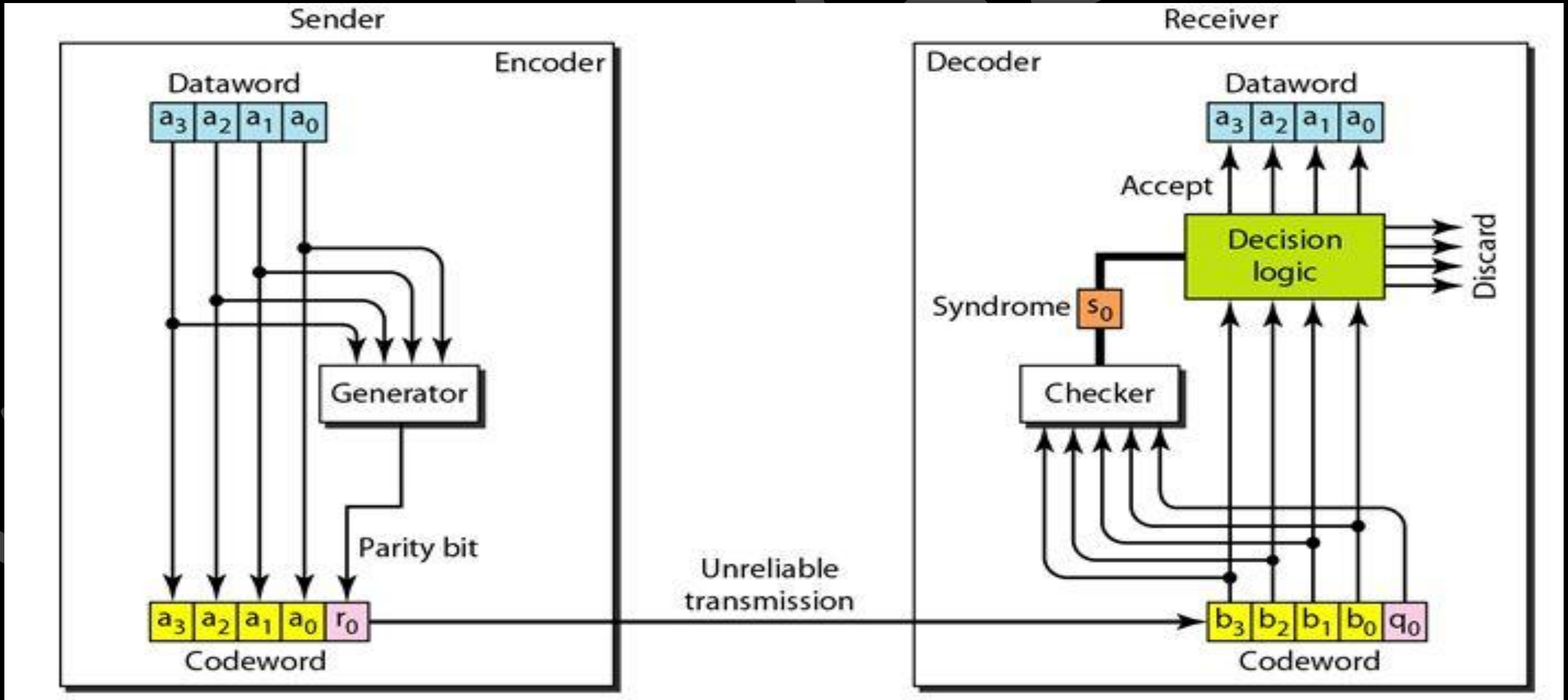
- To find the Hamming distance, perform an XOR operation on the two words and count the number of 1s in the outcome.

- For instance, the Hamming distance d(000, 011) equals 2, illustrated through the XOR operation: 000 XOR 011 equals 011, which has two 1s.

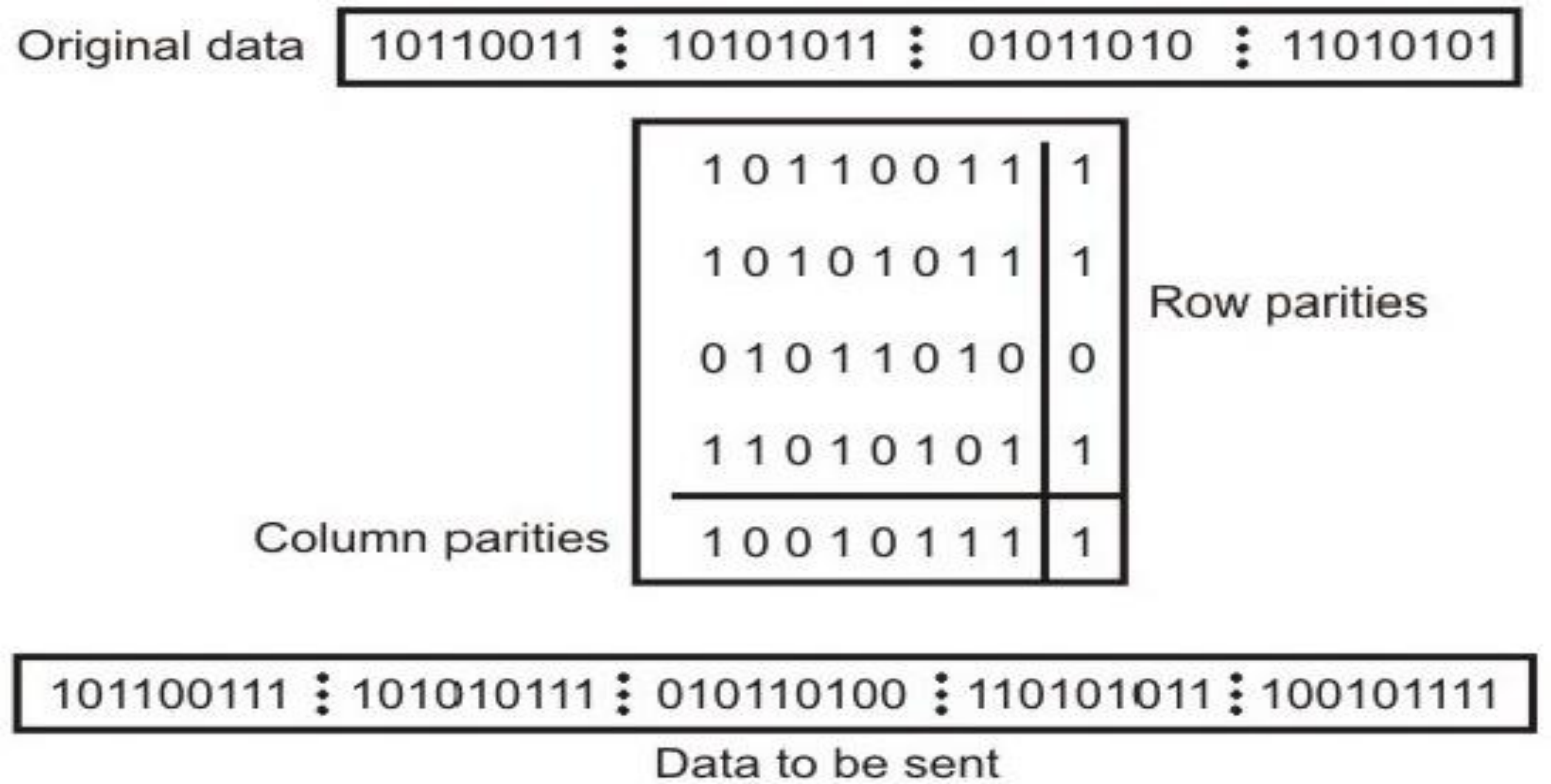
- The Hamming distance d(10101, 11110) is __________ ?

Simple Parity-Check Code

- The simple parity-check code expands a k-bit dataword to an n-bit codeword (n = k + 1), with the additional bit serving as a parity bit to ensure an even total count of 1s in the codeword, though some variations aim for an odd count instead.
- This code acts as a single-bit error-detecting mechanism, characterized by n = k + 1 and a minimum Hamming distance (d_{min}) of 2.
- It is designed to identify an odd number of errors within the data transmitted.



- In the two-dimensional parity check, data words are arranged in a table with rows and columns. A special bit called a parity-check bit is added to each row and column to help identify errors in the data.
- After the table is sent, the receiver checks the parity bits for each row and column to find "syndromes", which are indicators of where errors might have occurred.
- This method can identify up to three errors in the table, but might miss errors if four or more bits are affected.



Original data 10110011 ⋮ 10101011 ⋮ 01011010 ⋮ 11010101

	1 0 1 1 0 0 1 1	1
	1 0 1 0 1 0 1 1	1
	0 1 0 1 1 0 1 0	0
	1 1 0 1 0 1 0 1	1
Column parities	1 0 0 1 0 1 1 1	1

Row parities

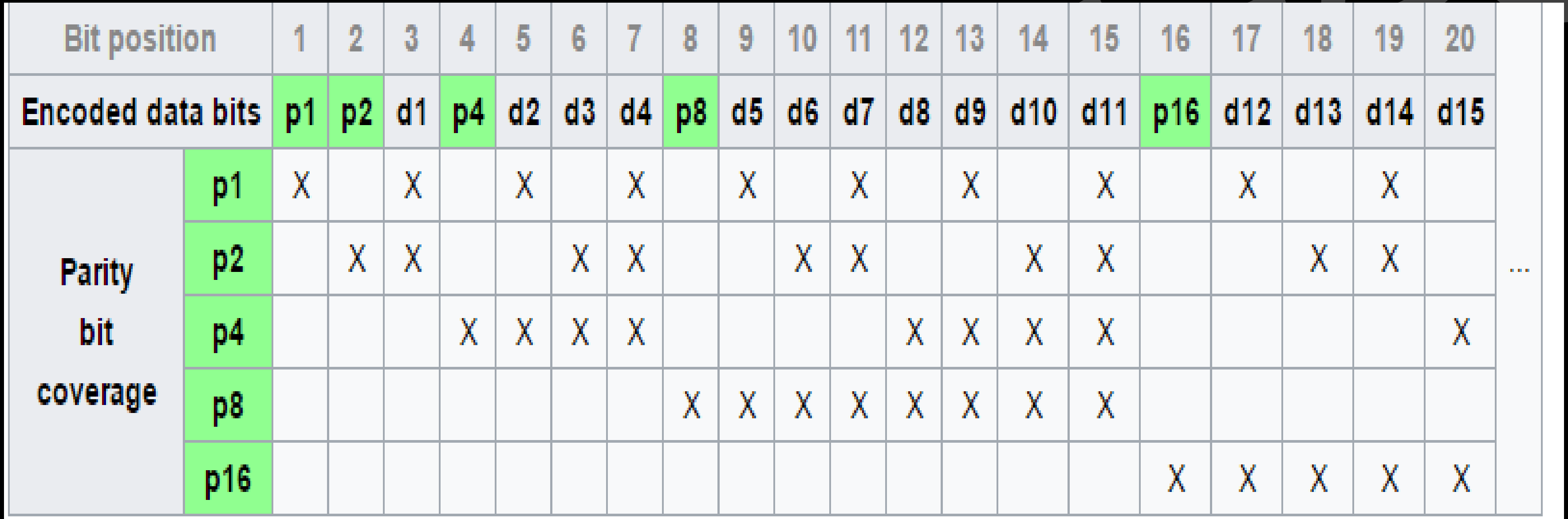
101100111 ⋮ 101010111 ⋮ 010110100 ⋮ 110101011 ⋮ 100101111

Data to be sent

Hamming Codes

- Now let us discuss a category of error-correcting codes called Hamming codes. These codes were originally designed to detect up to two errors or correct one single error.

- First let us find the relationship between n and k in a Hamming code. The values of n and k are then calculated from r as $k = 2^r - r - 1$.



Bit position		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
Encoded data bits		p1	p2	d1	p4	d2	d3	d4	p8	d5	d6	d7	d8	d9	d10	d11	p16	d12	d13	d14	d15	
Parity bit coverage	p1	X		X		X		X		X		X		X		X		X		X		
	p2		X	X			X	X			X	X			X	X			X	X		...
	p4				X	X	X	X					X	X	X	X					X	
	p8								X	X	X	X	X	X	X	X						
	p16																X	X	X	X	X	

Richard Hamming

- For example, if m = 3, then n = 7 and k = 4. This is a Hamming code C(7, 4) with dmin =3. shows the datawords and codewords for this code.

- Position of parity bits $2^0, 2^1, 2^2, \ldots, 2^n$

- If we use even parity then
  - For parity bit P_1 we check position 1, 3, 5, 7 (take 1, leave 1)(which have 1 at 2^0)
  - For parity bit P_2 we check position 2, 3, 6, 7 (take 2, leave 2)(which have 1 at 2^1)
  - For parity bit P_4 we check position 4, 5, 6, 7 (take 4, leave 4)(which have 1 at 2^2)

7	6	5	4	3	2	1
111	110	101	100	011	010	001
D_4	D_3	D_2	P_4	D_1	P_2	P_1

CHECKSUM

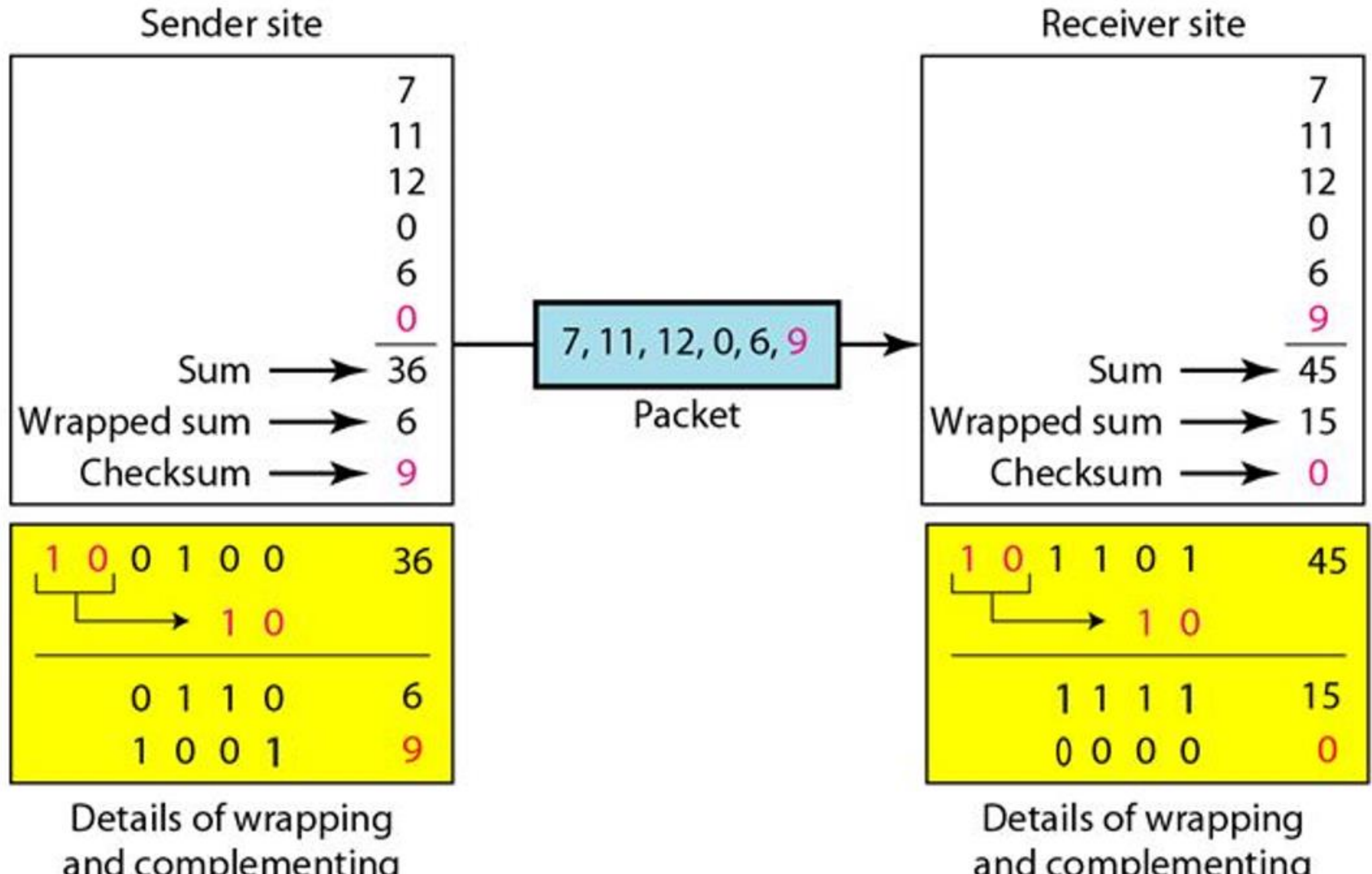
- The checksum method is a way to check for errors when sending a list of numbers over the internet. In this method, we add up all the numbers we want to send and send this total sum, along with the original numbers.

- At the receiving end, the numbers are added up again and compared with the received sum. If everything adds up correctly, it means that no errors occurred during transmission. Otherwise, it indicates that there was an error and the data is not accepted.For example, if the set of numbers is (7, 11, 12, 0, 6), we send (7, 11, 12, 0, 6, 36), where 36 is the sum of the original numbers. The receiver adds the five numbers and compares the result with the sum.

- We can make the job of the receiver easier if we send the negative (complement) of the sum, called the checksum. In this case, we send (7, 11, 12, 0, 6, -36). The receiver can add all the numbers received (including the checksum). If the result is 0, it assumes no error; otherwise, there is an error.

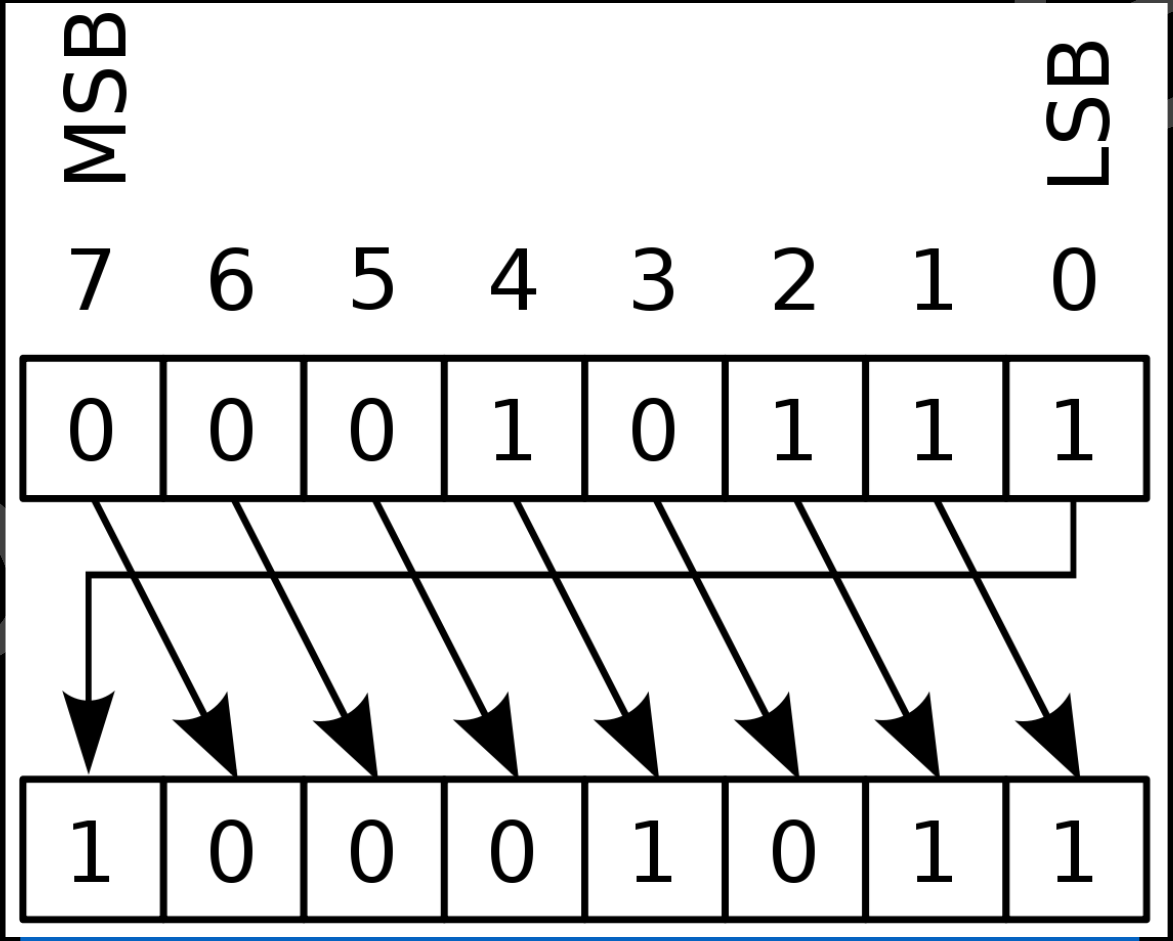
One's Complement

- The previous example has one major drawback. All of our data can be written as a 4-bit word (they are less than 15) except for the checksum.
- One solution is to use one's complement arithmetic. In one's complement arithmetic, a negative number can be represented by inverting all bits (changing a 0 to a 1 and a 1 to a 0). This is the same as subtracting the number from $2^n - 1$. If the number has more than n bits, the extra leftmost bits need to be added to the n rightmost bits (wrapping).



CYCLIC CODES

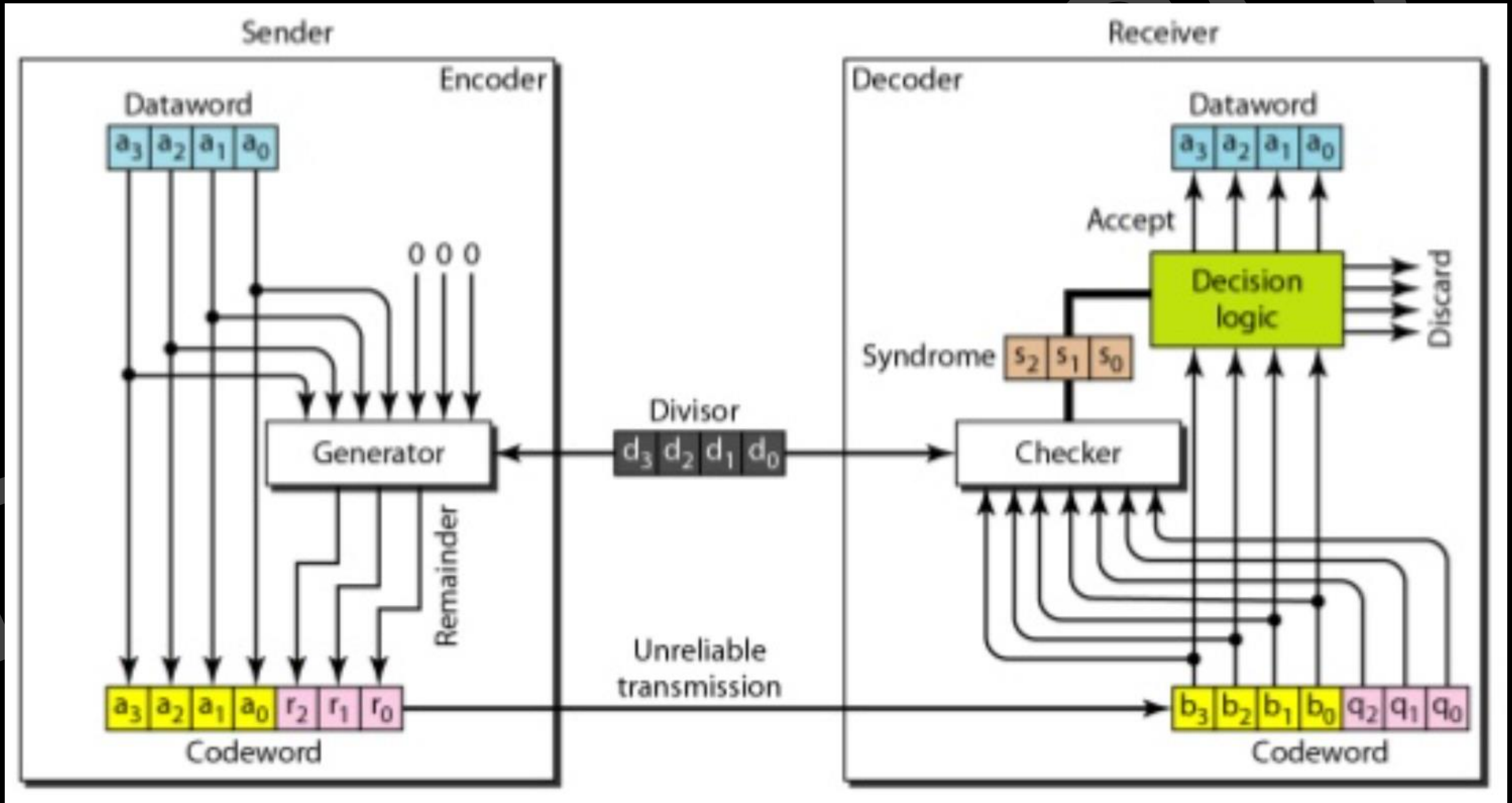
- Cyclic codes are special linear block codes with one extra property. In a cyclic code, if a codeword is cyclically shifted (rotated), the result is another codeword.



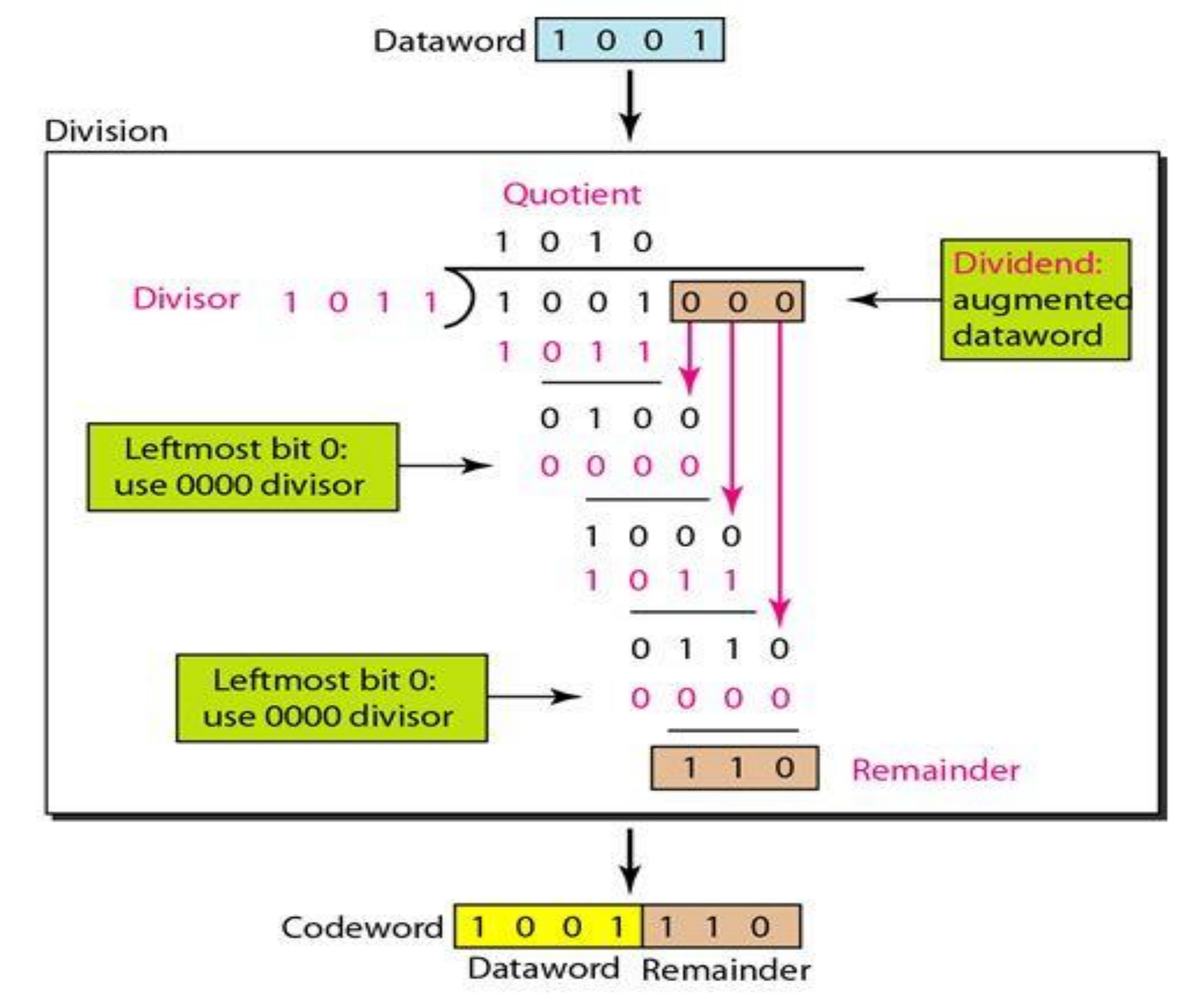
7	6	5	4	3	2	1	0
0	0	0	1	0	1	1	1
1	0	0	0	1	0	1	1

Cyclic Redundancy Check

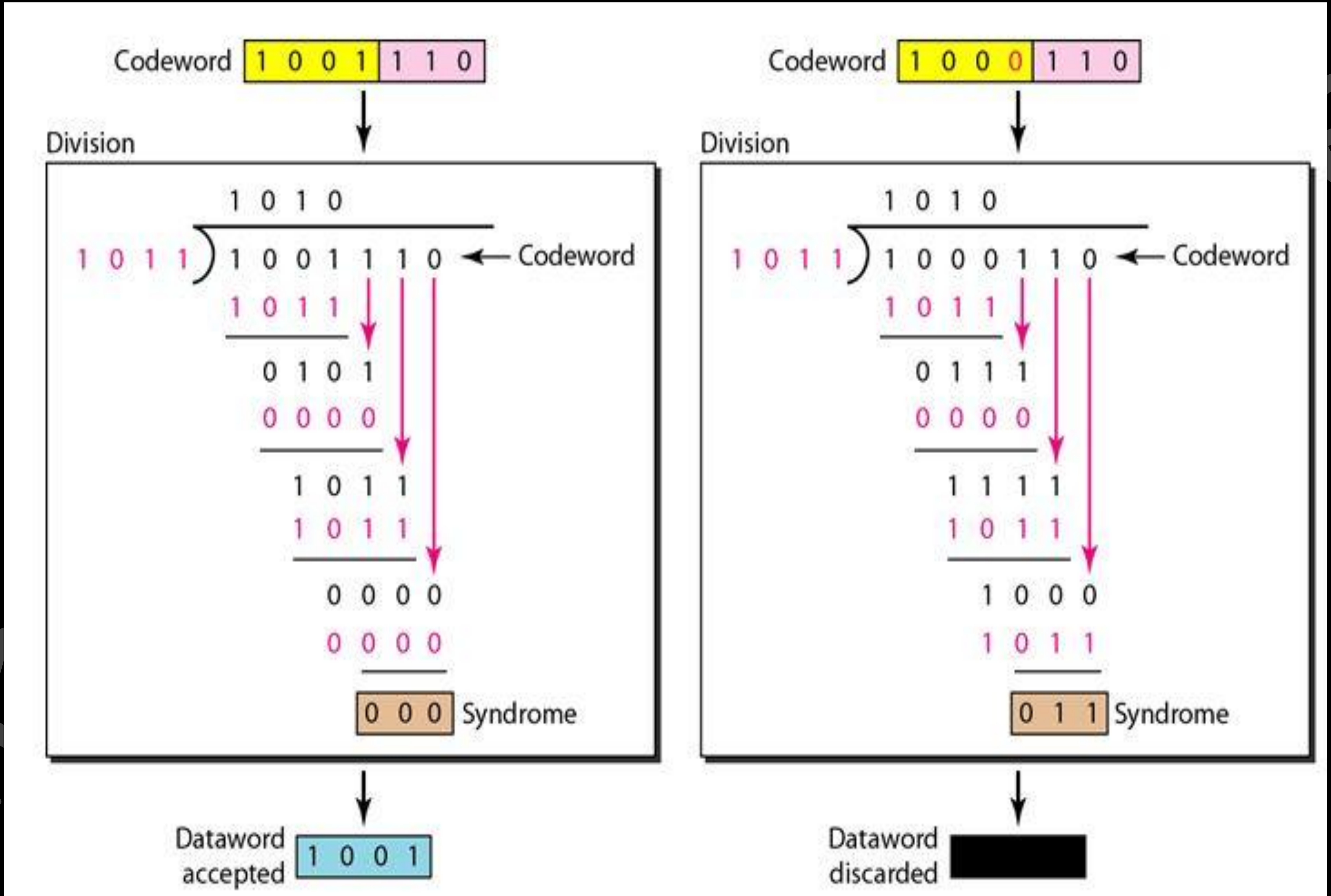
- We can create cyclic codes to correct errors. In the encoder, the dataword has k bits (4 here); the codeword has n bits (7 here). The size of the dataword is augmented by adding n - k (3 here) 0^s to the right-hand side of the word.
- The n-bit result is fed into the generator. The generator uses a divisor of size n - k + 1 (4 here), predefined and agreed upon. The generator divides the augmented dataword by the divisor (modulo-2 division). The quotient of the division is discarded; the remainder (r_2 r_1 r_0) is appended to the dataword to create the codeword.



Encoder

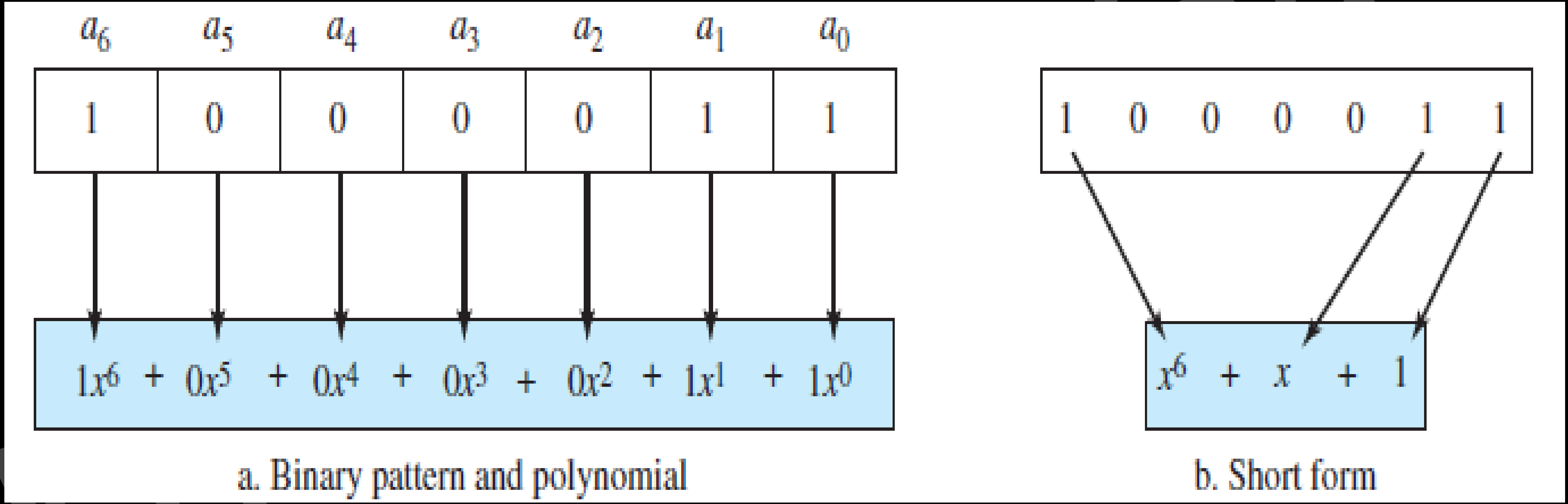

Dataword 1 0 0 1
Division
Quotient
1 0 1 0
Divisor 1 0 1 1
1 0 0 1 0 0 0
Dividend: augmented dataword
1 0 1 1
0 1 0 0
Leftmost bit 0: use 0000 divisor
0 0 0 0
1 0 0 0
1 0 1 1
0 1 1 0
Leftmost bit 0: use 0000 divisor
0 0 0 0
1 1 0
Remainder
Codeword 1 0 0 1 1 1 0
Dataword
Remainder

Decoder


Codeword 1 0 0 1 1 1 0
Division
1 0 1 0
1 0 1 1
1 0 0 1 1 1 0
Codeword
1 0 1 1
0 1 0 1
0 0 0 0
1 0 1 1
1 0 1 1
0 0 0 0
0 0 0 0
0 0 0 Syndrome
Dataword accepted 1 0 0 1
Codeword 1 0 0 0 1 1 0
Division
1 0 1 0
1 0 1 1
1 0 0 0 1 1 0
Codeword
1 0 1 1
0 1 1 1
0 0 0 0
1 1 1 1
1 0 1 1
1 0 0 0
1 0 1 1
0 1 1 Syndrome
Dataword discarded

Polynomials

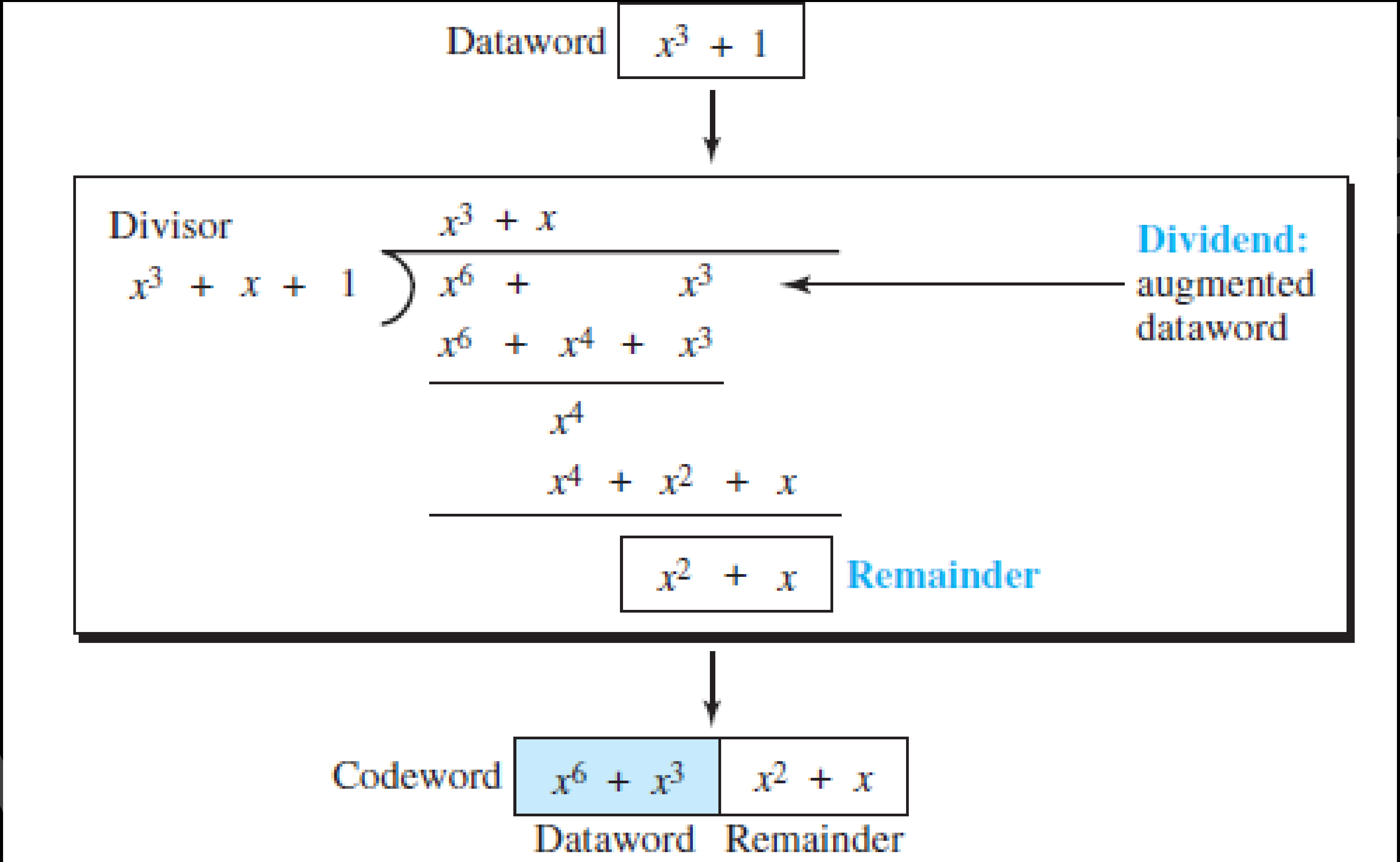
- A pattern of 0^s and 1^s can be represented as a **polynomial** with coefficients of 0 and 1. The power of each term shows the position of the bit; the coefficient shows the value of the bit. An advantage is that a large binary pattern can be represented by short terms.



a_6 a_5 a_4 a_3 a_2 a_1 a_0
1 0 0 0 0 1 1
$1x^6 + 0x^5 + 0x^4 + 0x^3 + 0x^2 + 1x^1 + 1x^0$
1 0 0 0 0 1 1
$x^6 + x + 1$

a. Binary pattern and polynomial

b. Short form



Dataword $x^3 + 1$

Divisor $x^3 + x + 1$

$$\begin{array}{r}
x^3 + x \\
x^3 + x + 1 \overline{)\, x^6 + x^3} \\
x^6 + x^4 + x^3 \\
\hline
x^4 \\
x^4 + x^2 + x \\
\hline
\boxed{x^2 + x}
\end{array}$$

Dividend: augmented dataword

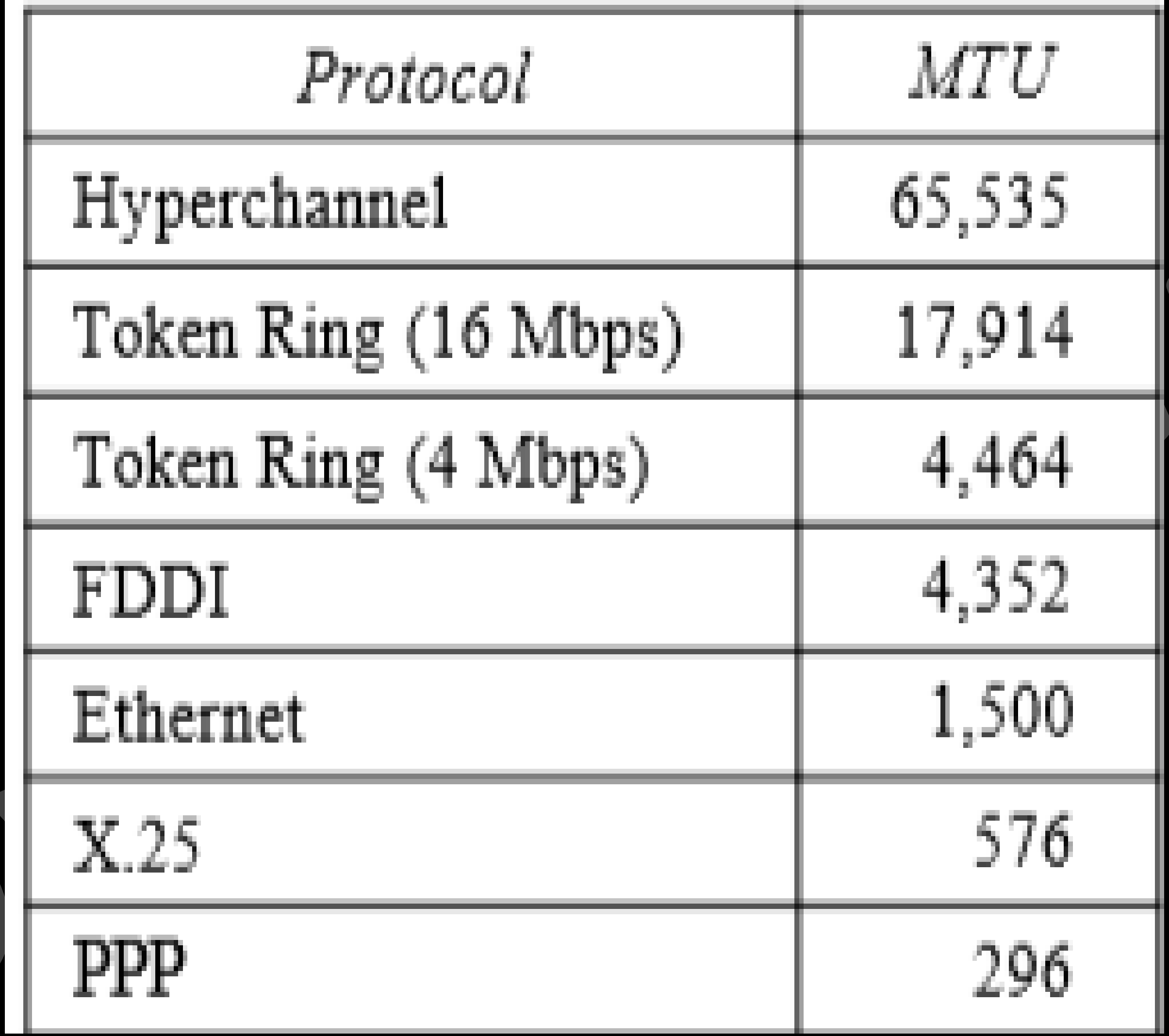
Remainder

Codeword $x^6 + x^3$ | $x^2 + x$

Dataword Remainder

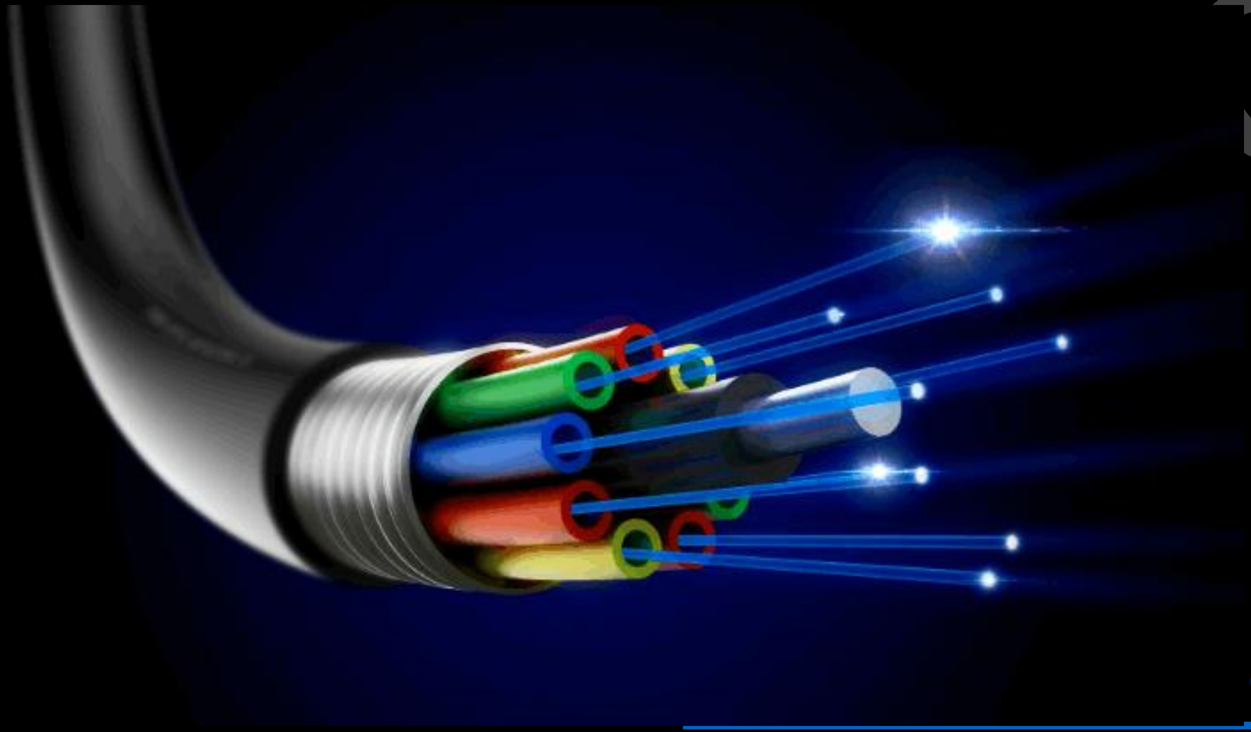
Ethernet

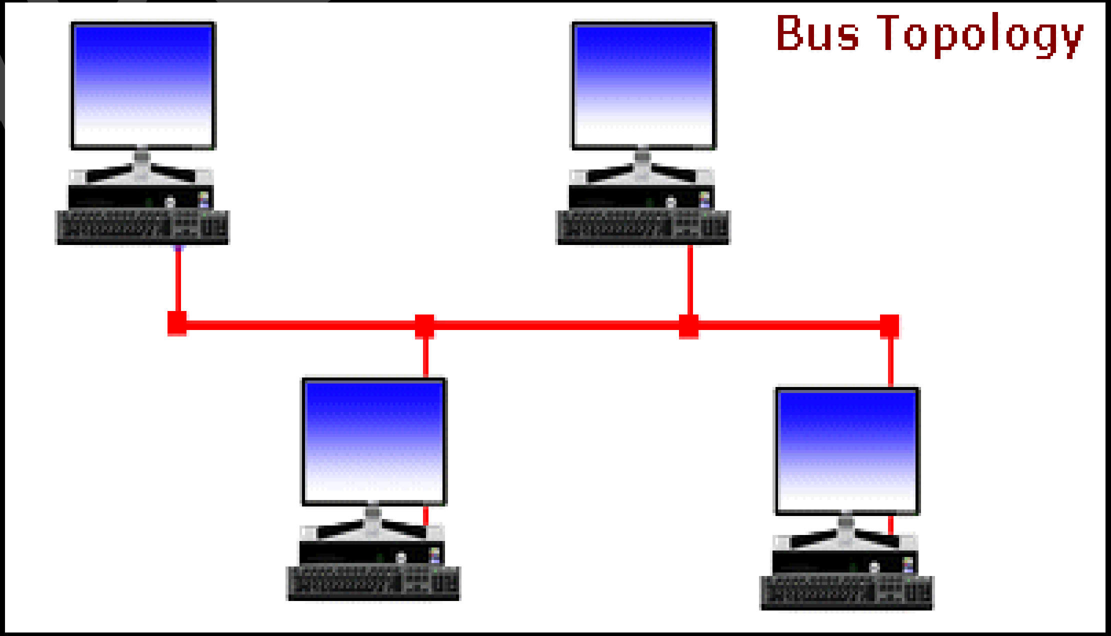
- Introduced commercially in 1980 and first standardized as IEEE 802.3 in 1983, Ethernet has undergone numerous refinements to support higher bit rates and extended link distances, replacing other LAN technologies like token ring, FDDI, and ARCNET.
- Initially utilizing coaxial cables as a shared medium, modern Ethernet variations have adopted twisted pair and fiber optic links, coupled with hubs or switches, to facilitate communication and data transfer within LANs and MANs.
- Over its evolution, Ethernet has boosted data transfer rates from an initial 2.94 Mbit/s to a remarkable 100 Gbit/s, offering several wirings and signaling options as part of the OSI physical layer in sync with Ethernet standards.



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

- Data is segmented into "frames" that carry source and destination addresses along with error-checking data, facilitating the detection and discarding of damaged frames, and enabling higher-layer protocols to trigger the retransmission of lost frames.
- Wi-Fi, a wireless protocol standardized as IEEE 802.11, serves as a prominent alternative to Ethernet in contemporary Local Area Networks (LANs).
- Operates using a Bus topology, connecting all devices to a common communication line; acknowledgments are not inherently used, but can be incorporated as data packets if necessary; utilizes Manchester encoding techniques for data transmission.





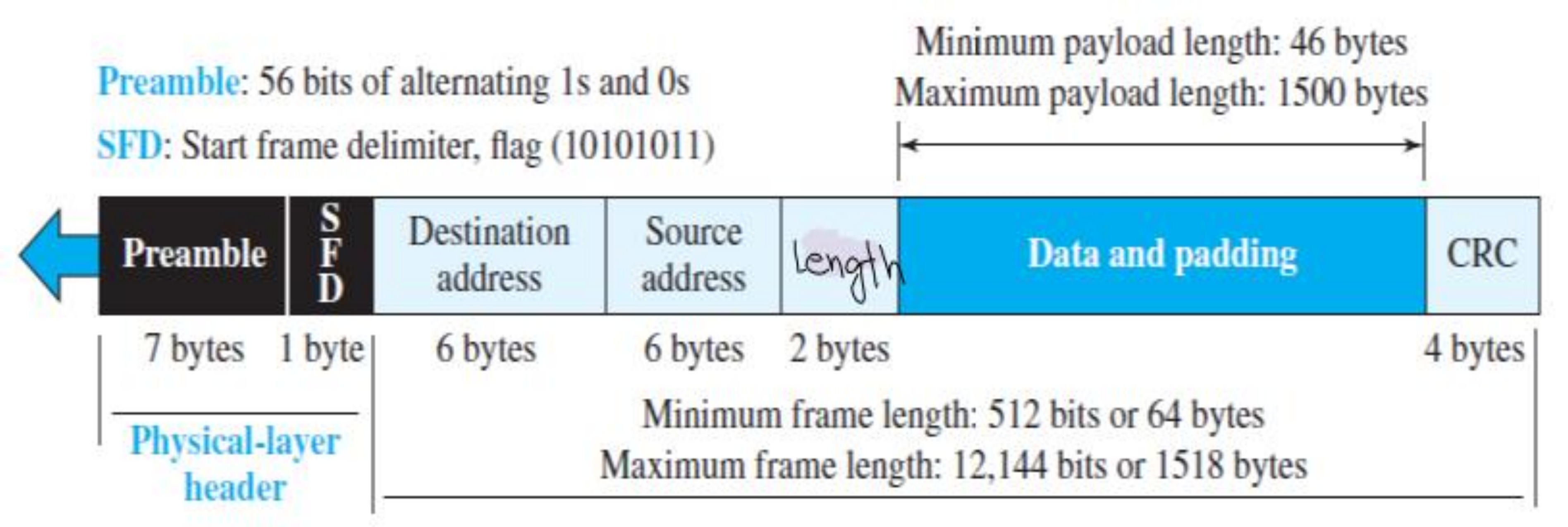
edgegate.in

STANDARD ETHERNET

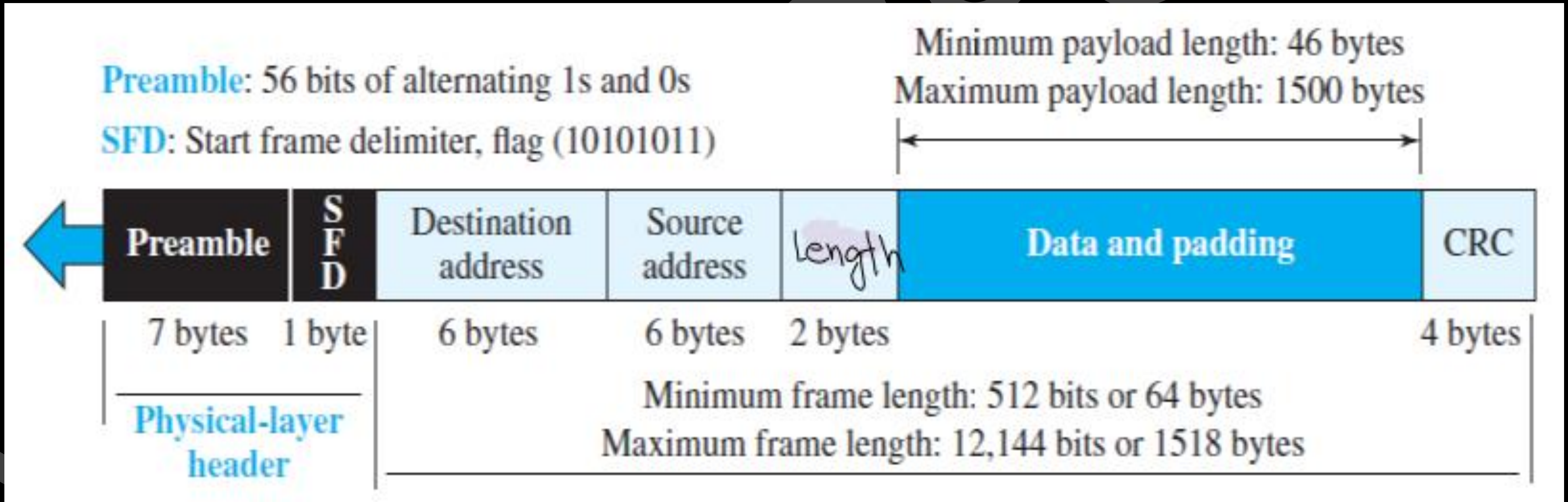
Connectionless and Unreliable Service:

- Each frame sent is independent of the previous or next frame. Ethernet has no connection establishment or connection termination phases.
- Ethernet is also unreliable, if a frame is corrupted during transmission and the receiver finds out about the corruption, the receiver drops the frame silently.
- In case of requirement ack can be sent separately at data packets.

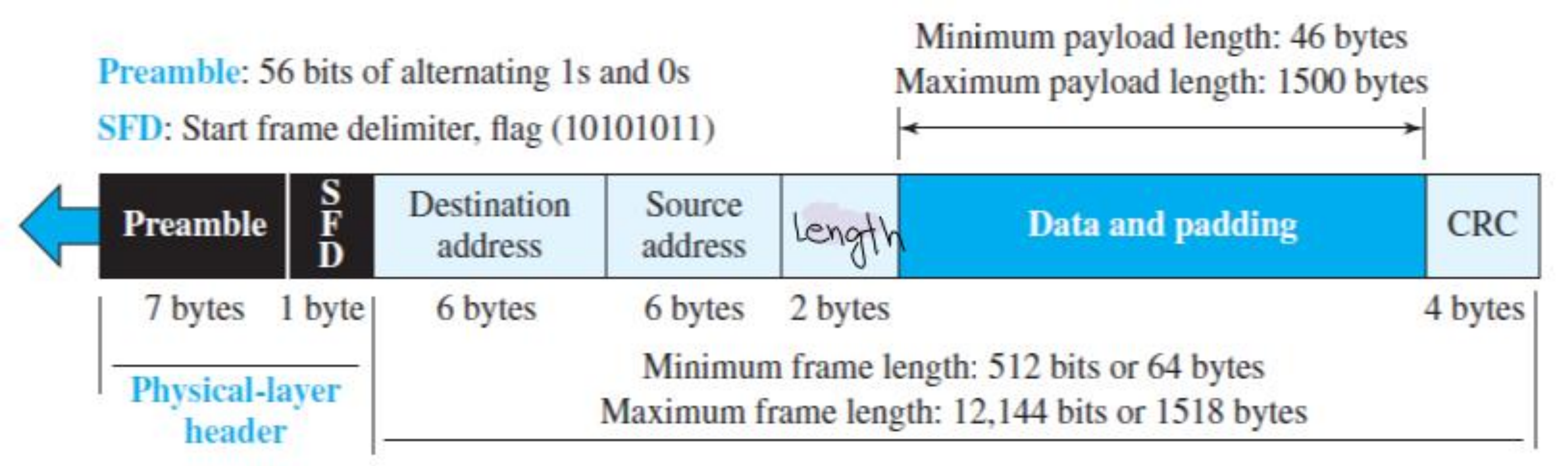
- **Preamble**
    - It is a 7-byte field that contains a pattern of alternating 0's and 1's.
    - It alerts the stations that a frame is going to start.
    - It also enables the sender and receiver to establish bit synchronization.
    - The Preamble field is added at the physical layer.


Preamble: 56 bits of alternating 1s and 0s
SFD: Start frame delimiter, flag (10101011)
Minimum payload length: 46 bytes
Maximum payload length: 1500 bytes
Preamble
S F D
Destination address
Source address
length
Data and padding
CRC
7 bytes
1 byte
6 bytes
6 bytes
2 bytes
4 bytes
Physical-layer header
Minimum frame length: 512 bits or 64 bytes
Maximum frame length: 12,144 bits or 1518 bytes

- **Start Frame Delimiter (SFD)**
  - It is a 1-byte field which is always set to 10101011.
  - The last two bits "11" indicate the end of Start Frame Delimiter and marks the beginning of the frame.
  - The SFD field is also added at the physical layer.
  - Initial only SFD was there Preamble was added later

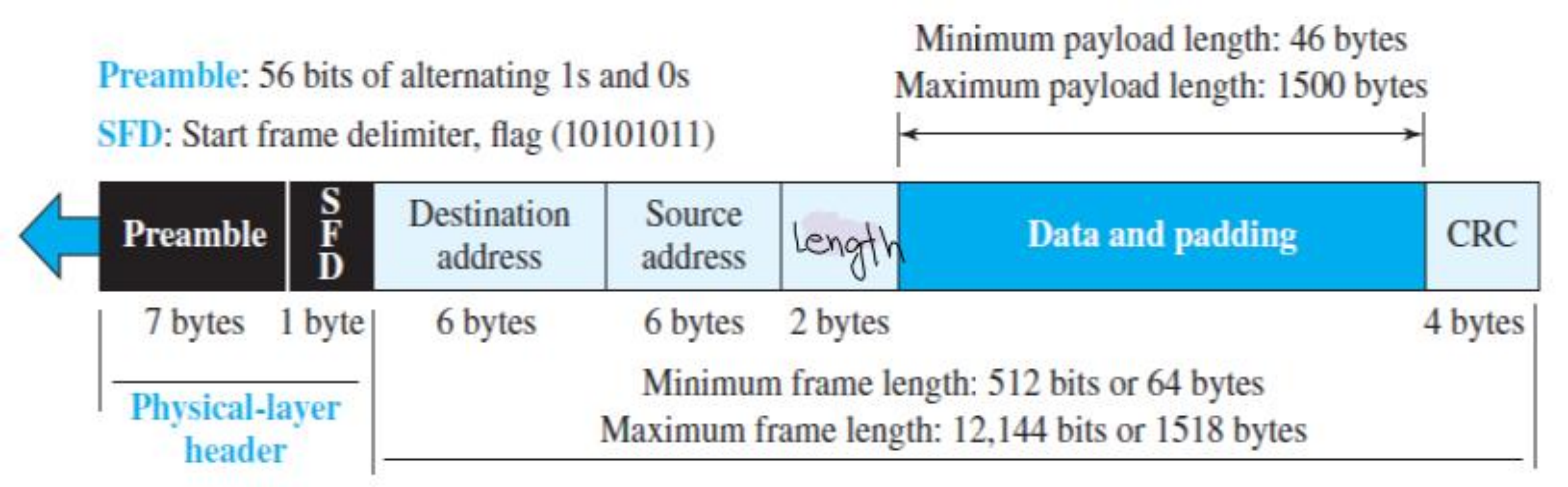

Preamble: 56 bits of alternating 1s and 0s
SFD: Start frame delimiter, flag (10101011)
Minimum payload length: 46 bytes
Maximum payload length: 1500 bytes
Preamble
S F D
Destination address
Source address
length
Data and padding
CRC
7 bytes
1 byte
6 bytes
6 bytes
2 bytes
4 bytes
Physical-layer header
Minimum frame length: 512 bits or 64 bytes
Maximum frame length: 12,144 bits or 1518 bytes

- **Destination Address**
  - It is a 6-byte field that contains the MAC address of the destination for which the data is destined. e.g. 2D : 8A : 7B : C5
  - MAC address is present on NIC card.
  - MAC address can be of three types
    - Unicast-LSB of the first byte is 0 (Source address will always be unicast)
    - Multicast- LSB of the first byte is 1, if we want to send, repeated messages to a group of station on the network then we can group these stations together and can assign a Multicast address to the group.
    - Broadcast-all bit are assigned 1's



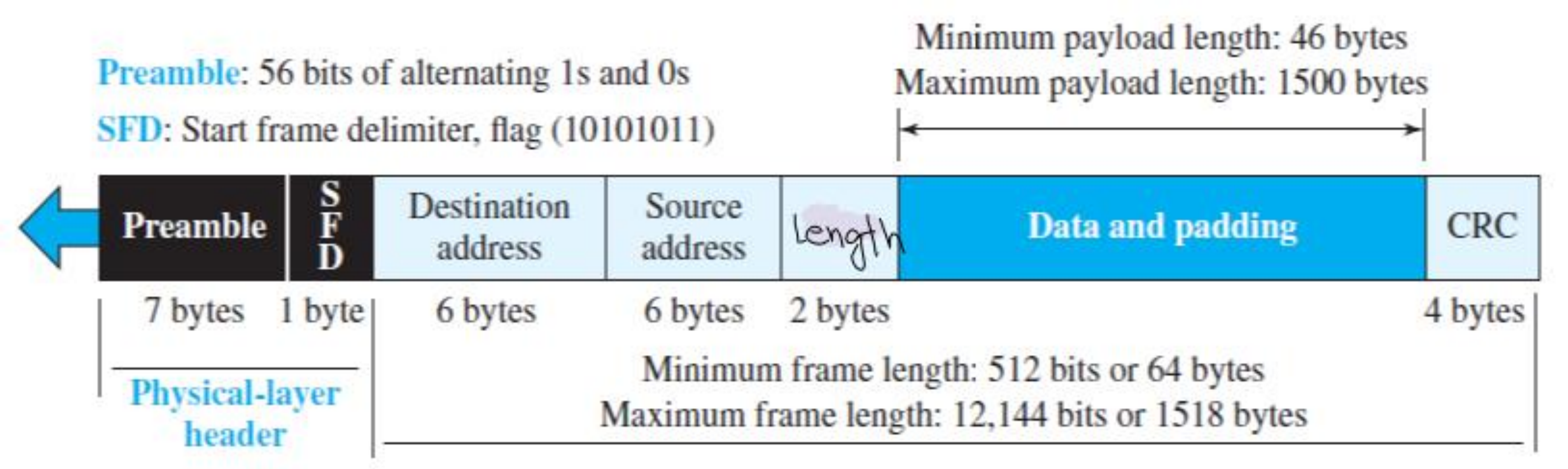
Preamble: 56 bits of alternating 1s and 0s
SFD: Start frame delimiter, flag (10101011)
Minimum payload length: 46 bytes
Maximum payload length: 1500 bytes
Preamble
SFD
Destination address
Source address
length
Data and padding
CRC
7 bytes
1 byte
6 bytes
6 bytes
2 bytes
4 bytes
Physical-layer header
Minimum frame length: 512 bits or 64 bytes
Maximum frame length: 12,144 bits or 1518 bytes

- **Source Address**
  - It is a 6-byte field that contains the MAC address of the source which is sending the data.
  - Using some protocol, we can broadcast a request message asking MAC address of every other station in the network.

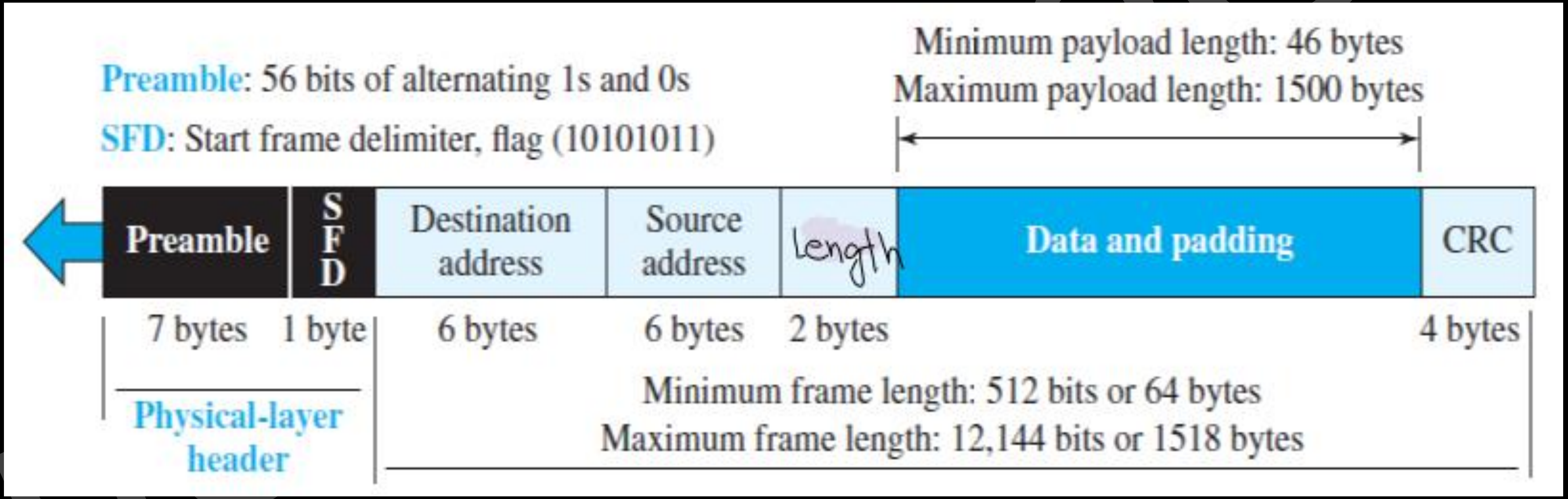


Preamble: 56 bits of alternating 1s and 0s
SFD: Start frame delimiter, flag (10101011)
Minimum payload length: 46 bytes
Maximum payload length: 1500 bytes
Preamble
S F D
Destination address
Source address
length
Data and padding
CRC
7 bytes
1 byte
6 bytes
6 bytes
2 bytes
4 bytes
Physical-layer header
Minimum frame length: 512 bits or 64 bytes
Maximum frame length: 12,144 bits or 1518 bytes

- **Length**
  - As ethernet use variable size frames therefore we need Length field
  - It is a 16-bit field.

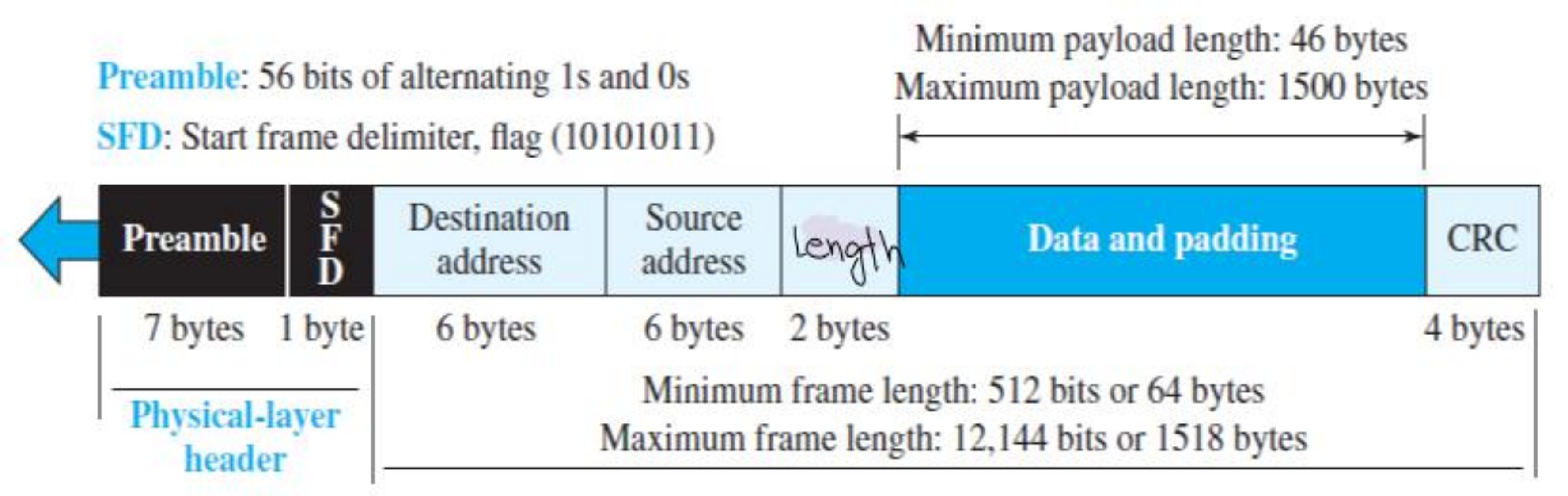

Preamble: 56 bits of alternating 1s and 0s
SFD: Start frame delimiter, flag (10101011)
Minimum payload length: 46 bytes
Maximum payload length: 1500 bytes
Preamble
S F D
Destination address
Source address
length
Data and padding
CRC
7 bytes
1 byte
6 bytes
6 bytes
2 bytes
4 bytes
Physical-layer header
Minimum frame length: 512 bits or 64 bytes
Maximum frame length: 12,144 bits or 1518 bytes

- **Data**
  - It is a variable length field which contains the actual data, also called as a payload field.
  - The length of this field lies in the range [46 bytes, 1500 bytes], i.e. in an Ethernet frame, minimum data has to be 46 bytes and maximum data can be 1500 bytes.
  - If it is less than 46 bytes, it needs to be padded with extra 0s.
  - If more than 1500 bytes, it should be fragmented and encapsulated in more than one frame.

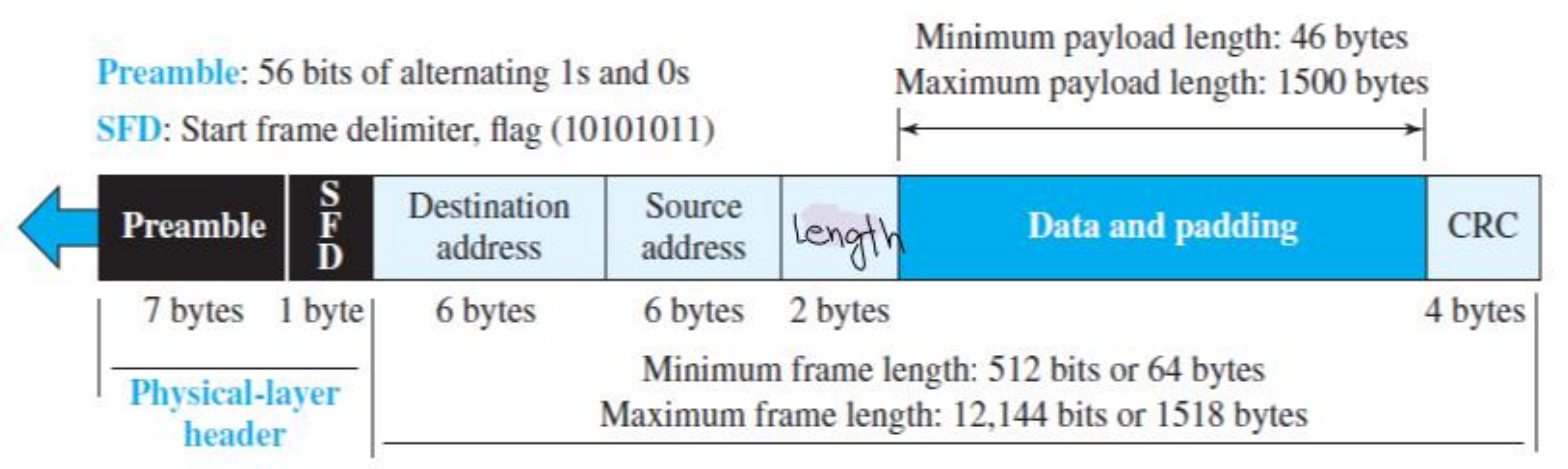


Preamble: 56 bits of alternating 1s and 0s
SFD: Start frame delimiter, flag (10101011)
Minimum payload length: 46 bytes
Maximum payload length: 1500 bytes
Preamble
SFD
Destination address
Source address
length
Data and padding
CRC
7 bytes
1 byte
6 bytes
6 bytes
2 bytes
4 bytes
Physical-layer header
Minimum frame length: 512 bits or 64 bytes
Maximum frame length: 12,144 bits or 1518 bytes

- **Data**
  - The minimum length restriction is required for the correct operation of CSMA/CD, value in general come to be 64B, 64-6-6-2-4 = 46B.
  - The maximum length restriction has two historical reasons:
    - Memory was very expensive when Ethernet was designed; a maximum length restriction helped to reduce the size of the buffer.
    - The maximum length restriction prevents one station from monopolizing the shared medium, blocking other stations that have data to send.


Preamble: 56 bits of alternating 1s and 0s
SFD: Start frame delimiter, flag (10101011)
Minimum payload length: 46 bytes
Maximum payload length: 1500 bytes
Preamble
S F D
Destination address
Source address
length
Data and padding
CRC
7 bytes
1 byte
6 bytes
6 bytes
2 bytes
4 bytes
Physical-layer header
Minimum frame length: 512 bits or 64 bytes
Maximum frame length: 12,144 bits or 1518 bytes

- **CRC**
  - The last field contains error detection information.
  - At the time of transmission CRC is calculated so it is in the last.
  - It is a 4-Byte field



Preamble: 56 bits of alternating 1s and 0s
SFD: Start frame delimiter, flag (10101011)
Minimum payload length: 46 bytes
Maximum payload length: 1500 bytes
Preamble
S F D
Destination address
Source address
length
Data and padding
CRC
7 bytes
1 byte
6 bytes
6 bytes
2 bytes
4 bytes
Physical-layer header
Minimum frame length: 512 bits or 64 bytes
Maximum frame length: 12,144 bits or 1518 bytes

Point to Note

- Ethernet is very simple easy to install and reconfigure.
- Should not be used with real time applications, because of collision possibility.
- if amount of data is very less then also should not be used.
- No idea of priority (Server suffer).

Token Bus (IEEE 802.4)

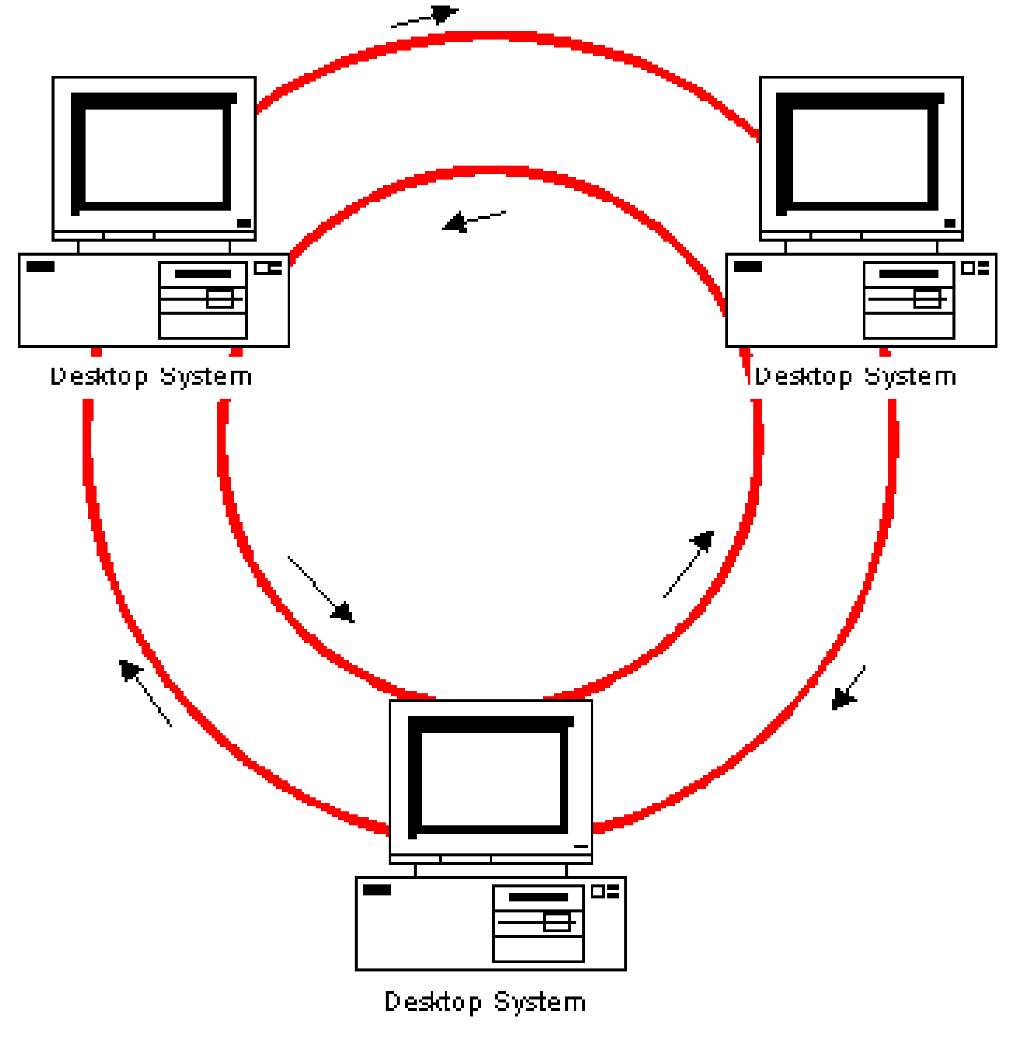
- IEEE 802.4 refers to the Token Bus network standard, another member of the IEEE 802 series of networking standards. Token Bus is designed to work over a bus topology but shares the token-passing access method for controlling the network traffic. Here are some key points about IEEE 802.4 Token Bus:
- **Topology**: As the name suggests, it operates over a bus topology, where all devices are connected to a central backbone.
- **Token Access**: Similar to Token Ring, it uses a token-passing mechanism to manage network access and prevent data collisions.
- **Data Rate**: Originally designed to operate at speeds up to 10 Mbps, although this may vary based on specific implementations.
- **Industries**: Often found in industrial applications and settings that require deterministic network behaviour, such as manufacturing or automation systems.
- **Deterministic**: Provides more predictable network timing compared to Ethernet, making it useful for real-time applications.
- **Obsolescence**: Like Token Ring, Token Bus has been largely superseded by Ethernet networks due to their higher speeds and easier configuration and maintenance.
- Token Bus was less common than both Ethernet and Token Ring but had specific use-cases where its deterministic behaviour was valuable.

Token Ring (IEEE 802.5)

- 802.5 refers to the IEEE standard for Token Ring networks. Token Ring networks were initially developed by IBM and later standardized by IEEE as 802.5. Here are a few points about it:
- Operates over a star or ring topology, where data packets are circulated in one direction from one device to the next until they reach their destination.
- Utilizes a "token" for managing network access; a device can only send data if it seizes the token, which helps to prevent collisions.
- Typically offers data transfer rates ranging from 4 Mbps to 16 Mbps, although later developments increased speeds up to 100 Mbps.
- Over the years, it has been largely replaced by Ethernet networks due to their greater speeds and simpler configuration and maintenance.

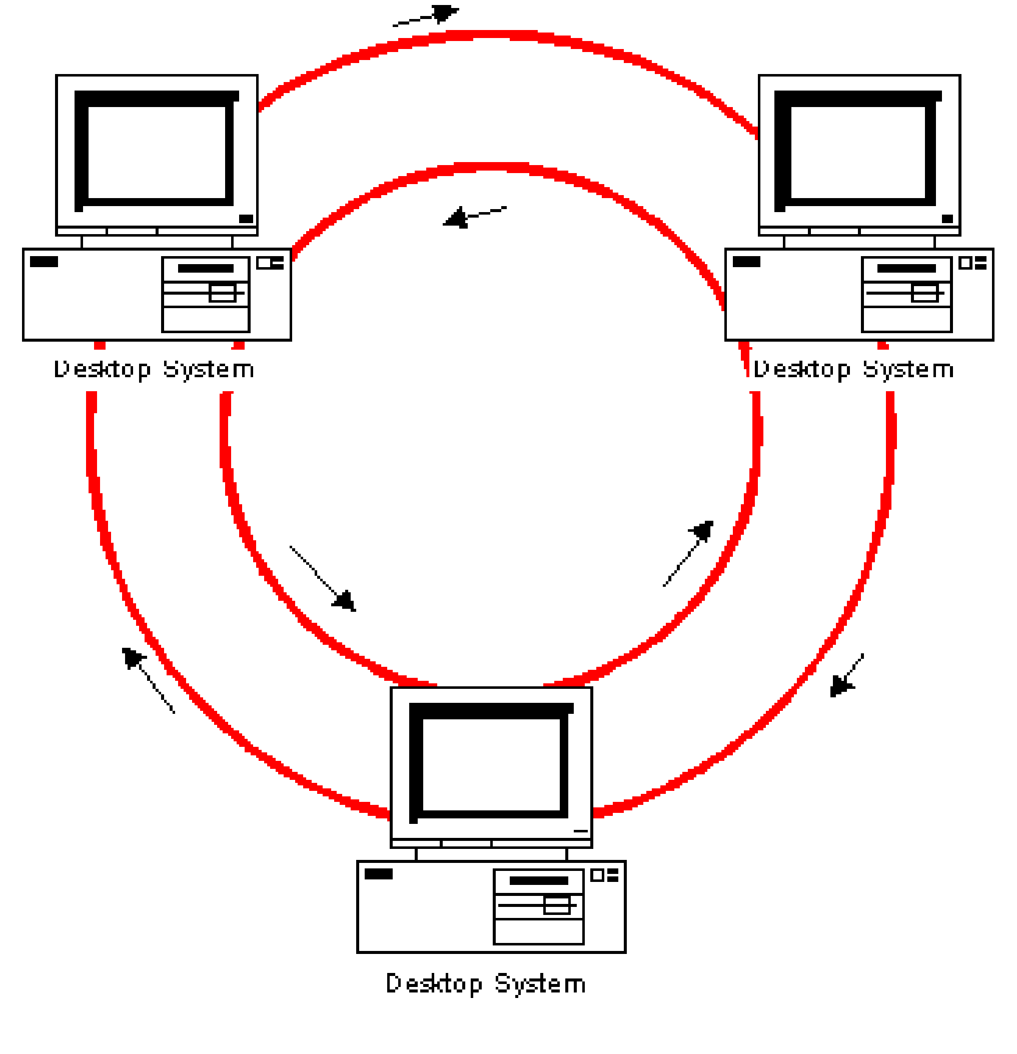
Fiber Distributed Data Interface (FDDI)

- Fiber Distributed Data Interface (FDDI) is a standard for data transmission in a local area network (LAN) that can extend in range up to 200 kilometers (124 miles). It uses optical fiber as its standard underlying physical medium, although it was later adapted for copper wiring as well (CDDI or Copper Distributed Data Interface). Here are some key points about FDDI:
- **Dual Ring**: FDDI uses a dual-ring architecture. In the event of a failure on one ring, data can be automatically sent over the second ring, providing fault tolerance.
- **High Speed**: Operates at a data rate of 100 Mbps, which was quite high when FDDI was first introduced in the late 1980s.
- **Token Passing**: Similar to Token Ring and Token Bus, FDDI also uses token-passing as the access method to prevent data collisions.



FDDI - all stations functioning

- **Deterministic**: Offers predictable latency, making it suitable for real-time applications and time-sensitive data.
- **Scalability**: Due to its fiber-optic nature, FDDI networks can be quite large, spanning distances that are impractical for copper-based Ethernet networks.
- **Industry Use**: Initially used for mission-critical, high-availability environments like banking, telecoms, and air traffic control systems.
- **Obsolescence**: With advancements in Ethernet technology, including Gigabit and 10-Gigabit Ethernet, FDDI has largely been phased out in favor of Ethernet solutions that offer higher speeds and are easier to manage.
- FDDI was an important step in the development of robust, high-speed networking but has largely been replaced by newer technologies.



FDDI - all stations functioning

be sent first.

Frame format :

SD	FC	ED
1	1	1

Token

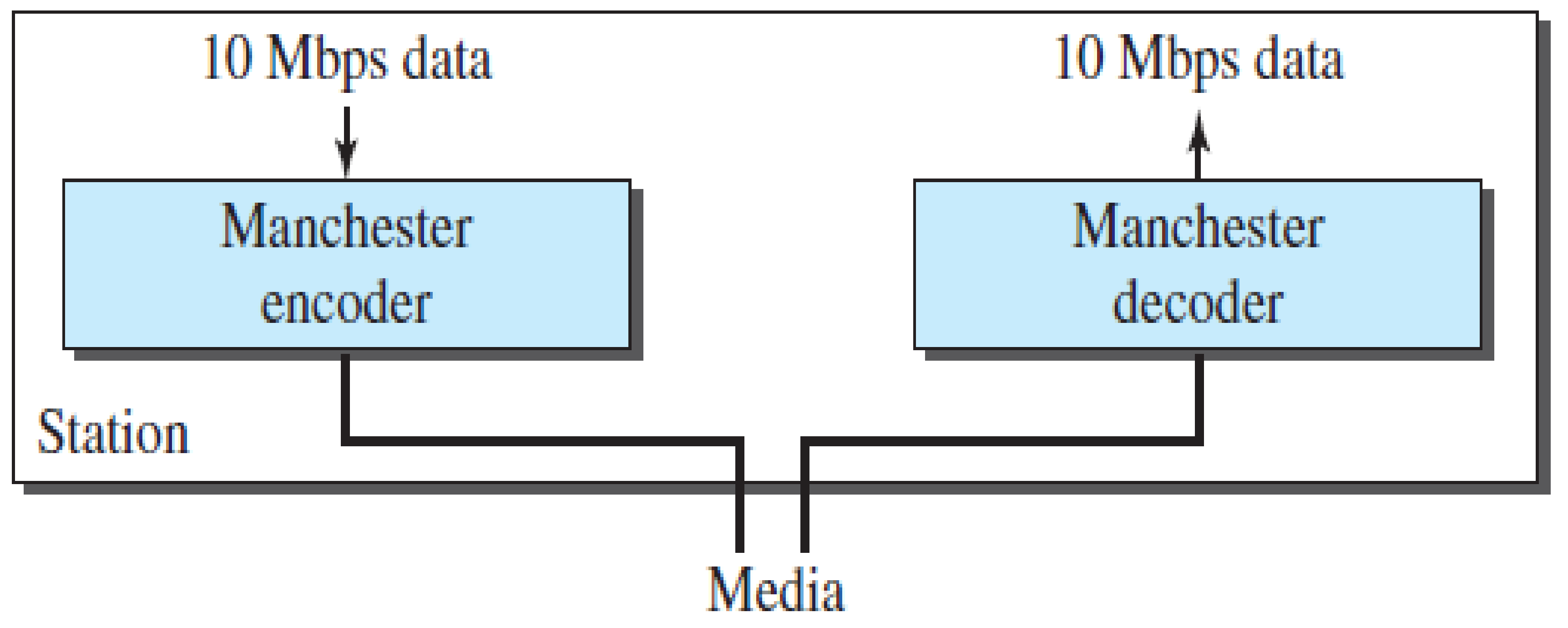
LLC data unit

DSAP	SSAP	Control	Information

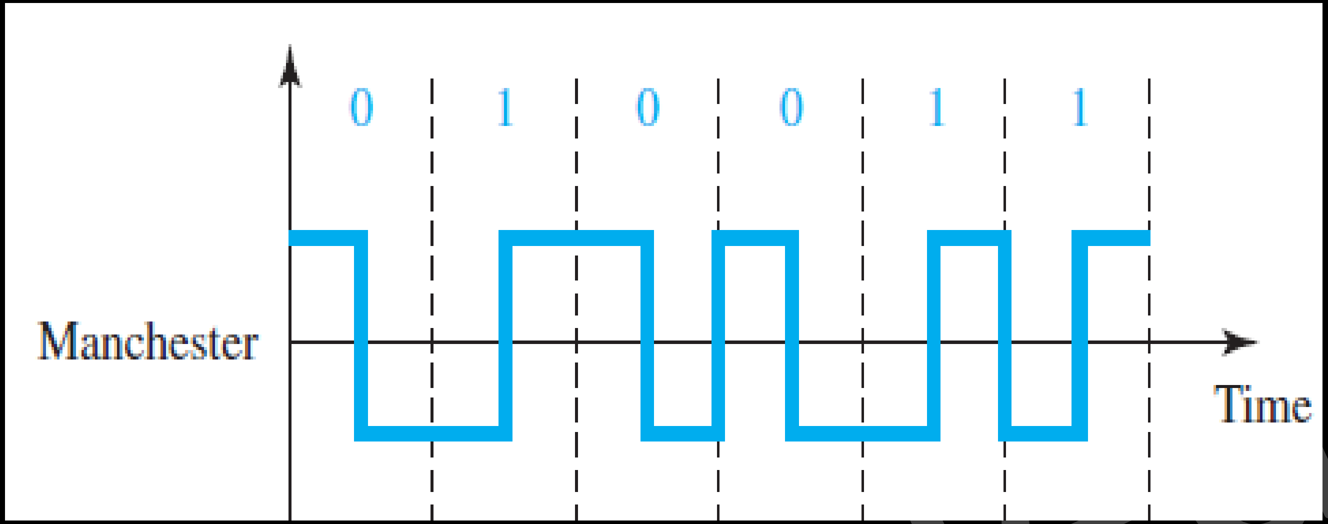
SD	FC	Destination address	Source address	**Data/command**	CRC	ED	FS
1 byte	1 byte	2-6 bytes	2-6 bytes	0-4500 bytes	4 bytes	0.5 bytes	1.5 bytes

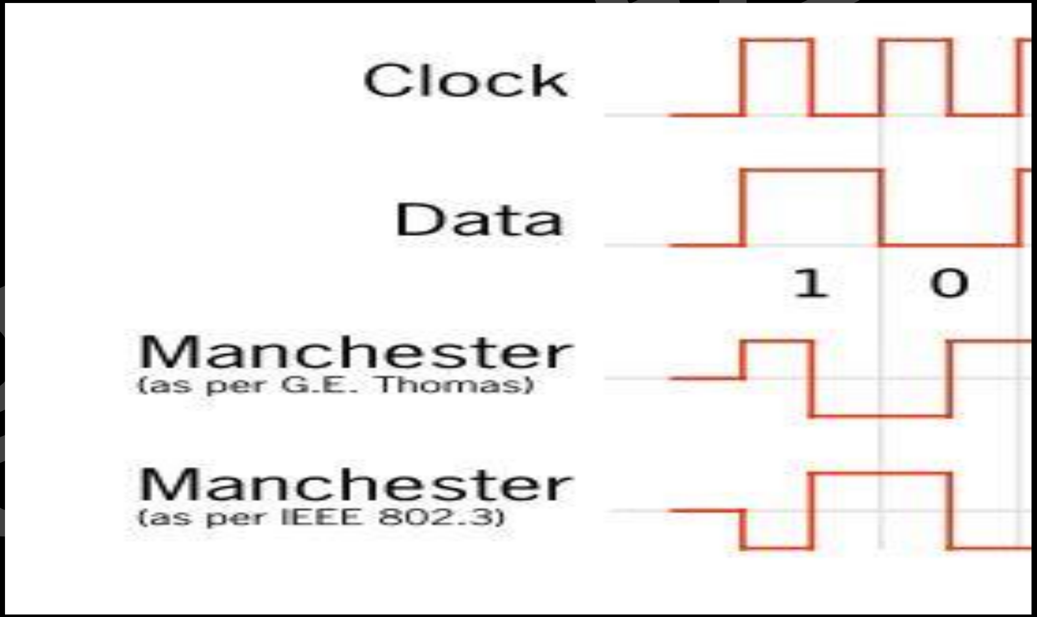
Implementation

- At the sender, data are converted to a digital signal using the Manchester scheme; at the receiver, the received signal is interpreted as Manchester and decoded into data.



- In Manchester encoding, the duration of the bit is divided into two halves. The voltage remains at one level during the first half and moves to the other level in the second half. The transition at the middle of the bit provides synchronization

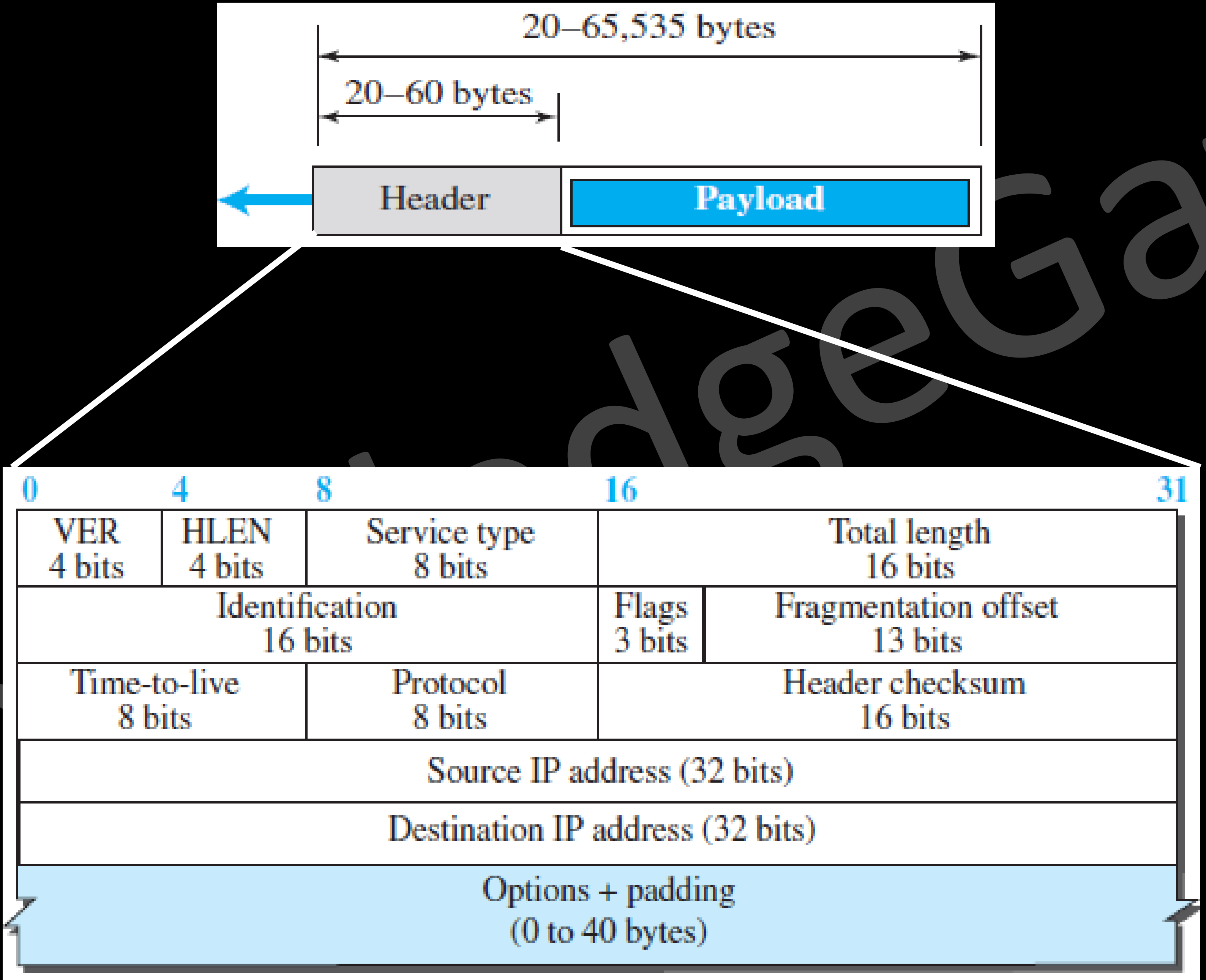




Network layer

- **Source to Destination Delivery**: Delivers packets from source to destination, possibly over multiple networks.
- **Logical Addressing**: Uses logical addresses to identify the sender and receiver.
- **Routing**: Responsible for finding the best route to send packets using routing protocols.
- **Packetizing**: Involves encapsulating payload at the source, adding a header with essential details, and preserving payload integrity during transit, barring fragmentation cases.
- **Error and Flow Control**: Encompasses adding a checksum in the datagram header for detecting corruption (not covering the entire datagram), with limited direct involvement in flow control, and using ICMP for some error control activities.
- **Congestion Control**: Manages network congestion, handling situations when too many datagrams crowd a network segment and addressing capacity exceedance issues in networks or routers.

IPv4



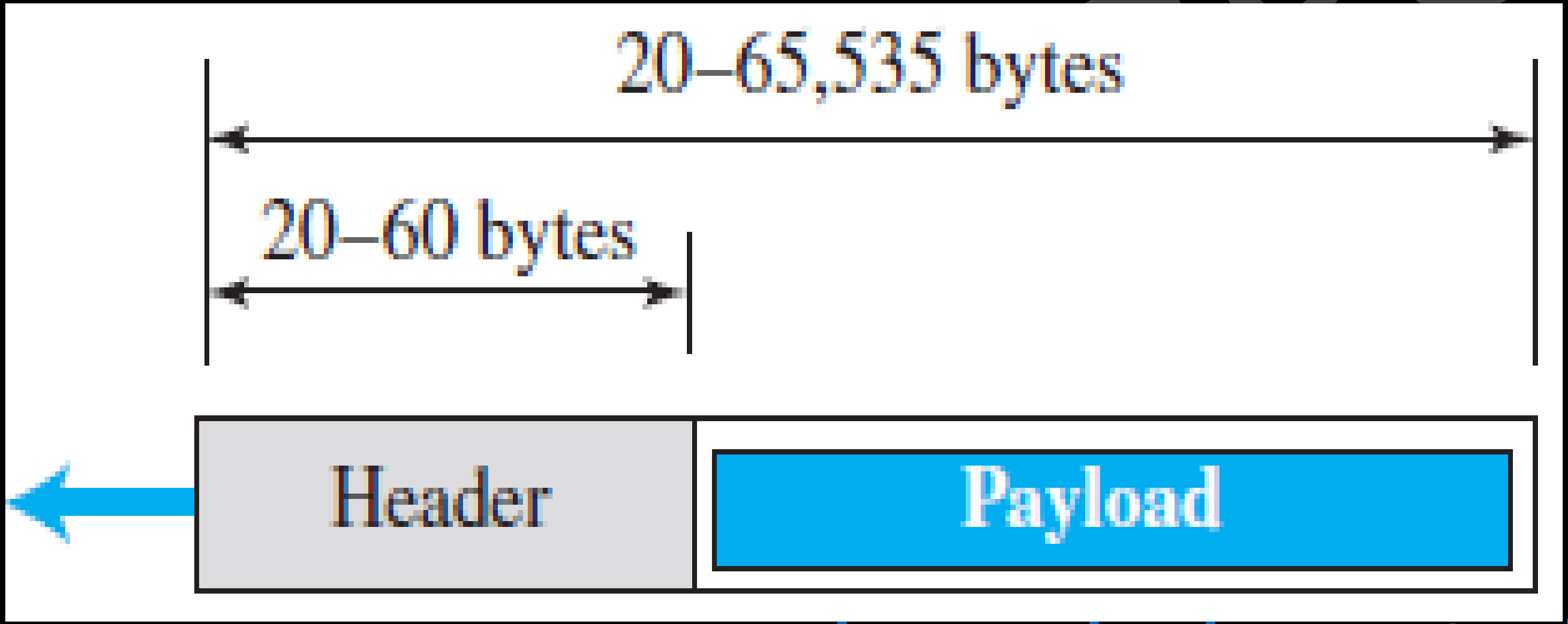
0	4	8	16	31
VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits	
Identification 16 bits			Flags 3 bits	Fragmentation offset 13 bits
Time-to-live 8 bits		Protocol 8 bits	Header checksum 16 bits	
Source IP address (32 bits)				
Destination IP address (32 bits)				
Options + padding (0 to 40 bytes)				

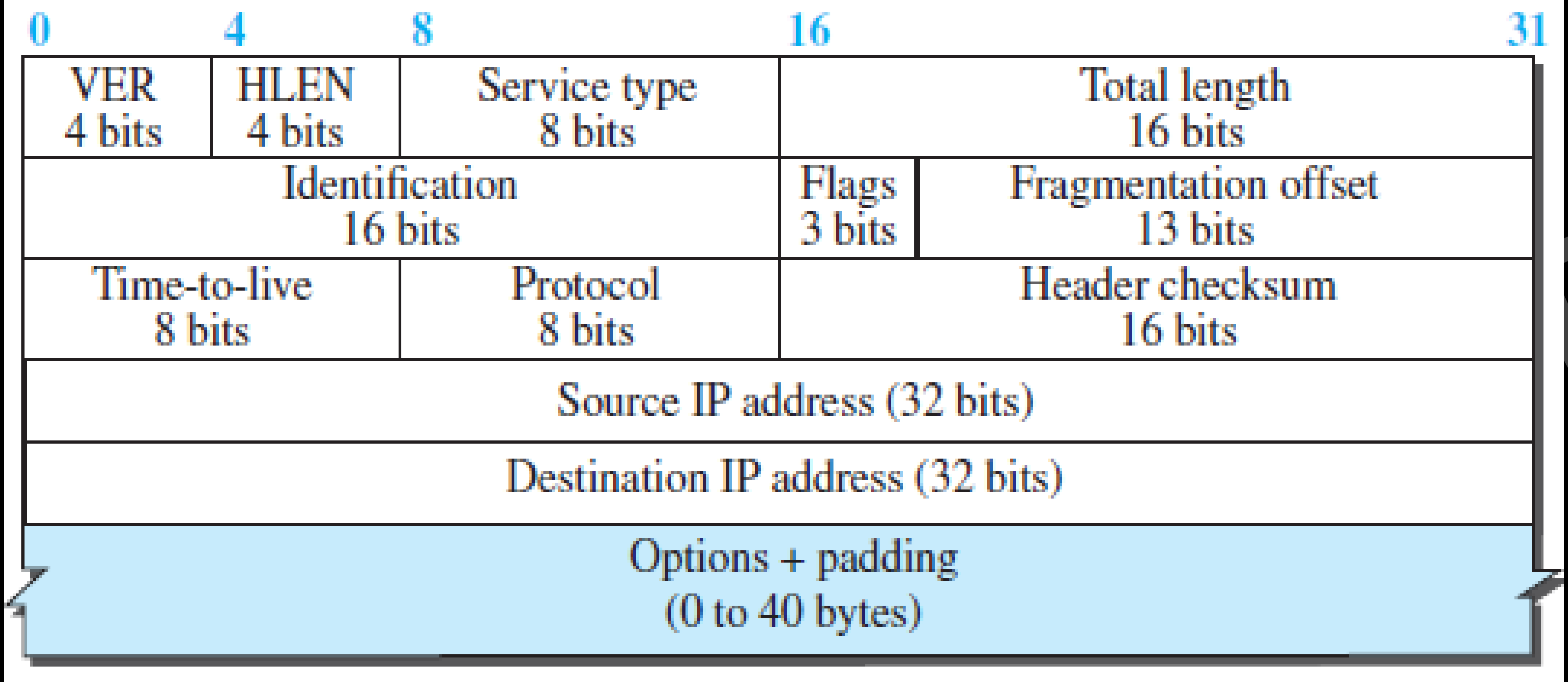
IPv4

- IPv4 operates as an unreliable connectionless datagram protocol, offering a best-effort delivery service which doesn't guarantee packet safety or order.
- The "best-effort" notion implies that IPv4 packets might experience corruption, loss, delays, or out-of-order arrival, potentially causing network congestion.
- Employing a datagram approach, IPv4 treats each datagram independently, allowing them to traverse different routes to their destination.
- To enhance reliability, IPv4 should be coupled with a reliable protocol like TCP, forming the TCP/IP protocol stack for secured data delivery.

Datagram Format

- Packets used by the IP are called ***datagrams*****.**
- A datagram is a variable-length packet consisting of two parts: header and payload (data).
- The header is 20 to 60 bytes in length and contains information essential to routing and delivery.



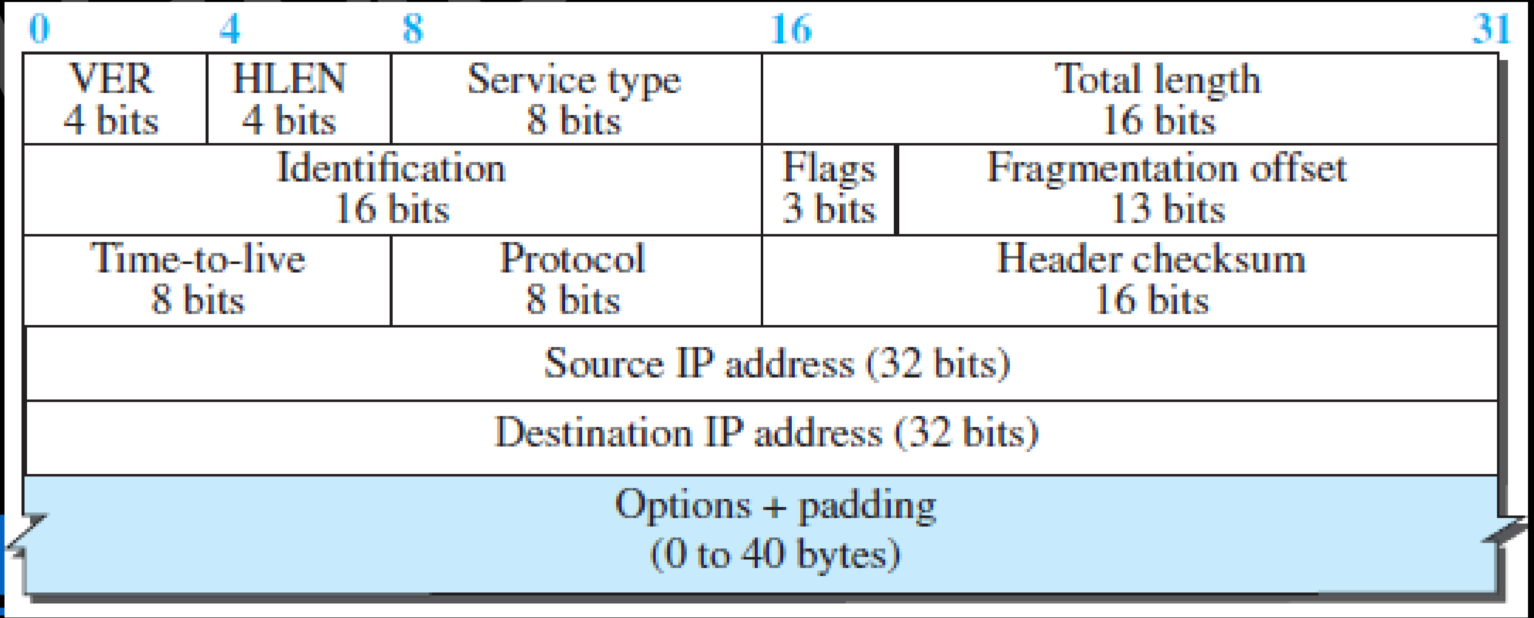


0	4	8	16	31
VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits	
Identification 16 bits			Flags 3 bits	Fragmentation offset 13 bits
Time-to-live 8 bits		Protocol 8 bits	Header checksum 16 bits	
Source IP address (32 bits)				
Destination IP address (32 bits)				
Options + padding (0 to 40 bytes)				

- **Version Number*:*** The 4-bit version number (VER) field defines the version of the IPv4 protocol, which, has the value of 4.

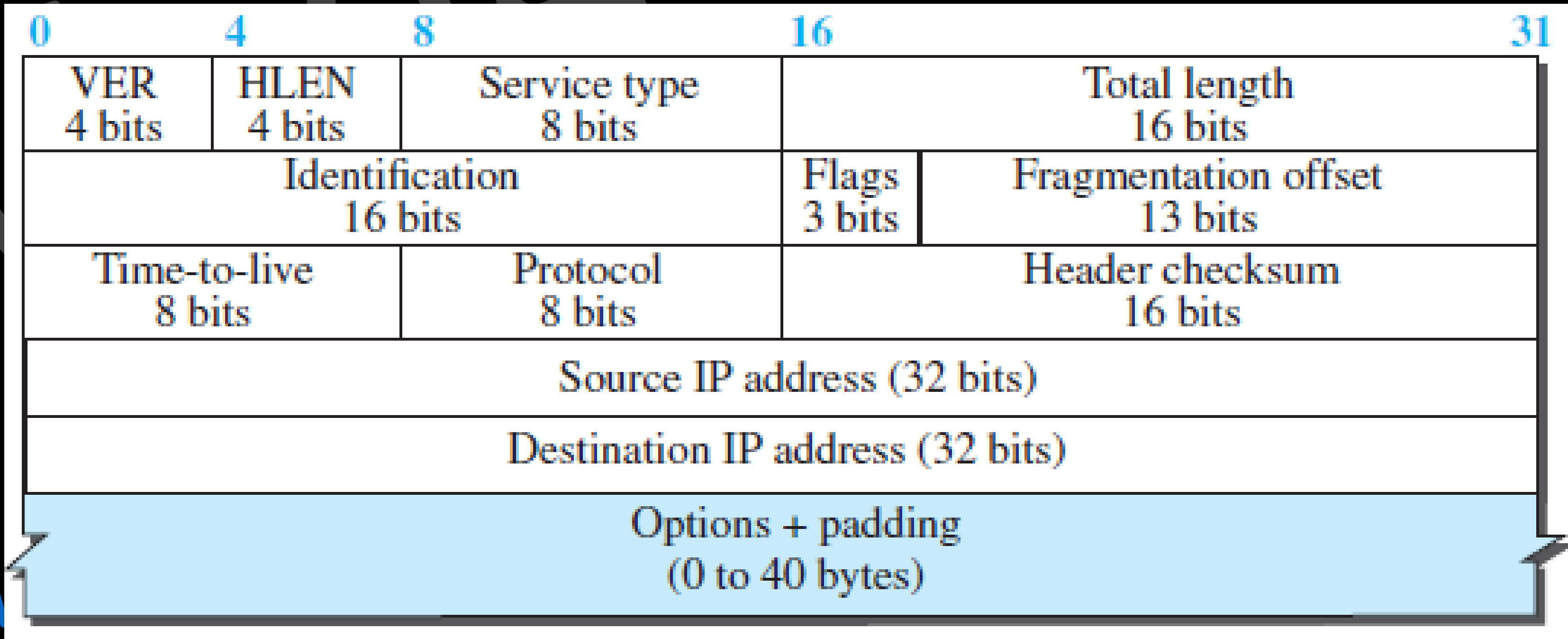
- **Header Length:** The 4-bit header length (HLEN) field defines the total length of the datagram header in 4-byte words. The IPv4 datagram has a variable-length header.

- **Scaling Factor:**
  - To make the value of the header length (number of bytes) fit in a 4-bit header length, the total length of the header is calculated as 4-byte words.
  - The total length is divided by 4 and the value is inserted in the field.
  - The receiver needs to multiply the value of this field by 4 to find the total length.
  - Example: If header length field contains decimal value 5 (represented as 0101), then Header length = 5 x 4 = 20 bytes



0	4	8	16		31
VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits		
Identification 16 bits			Flags 3 bits	Fragmentation offset 13 bits	
Time-to-live 8 bits		Protocol 8 bits	Header checksum 16 bits		
Source IP address (32 bits)					
Destination IP address (32 bits)					
Options + padding (0 to 40 bytes)					

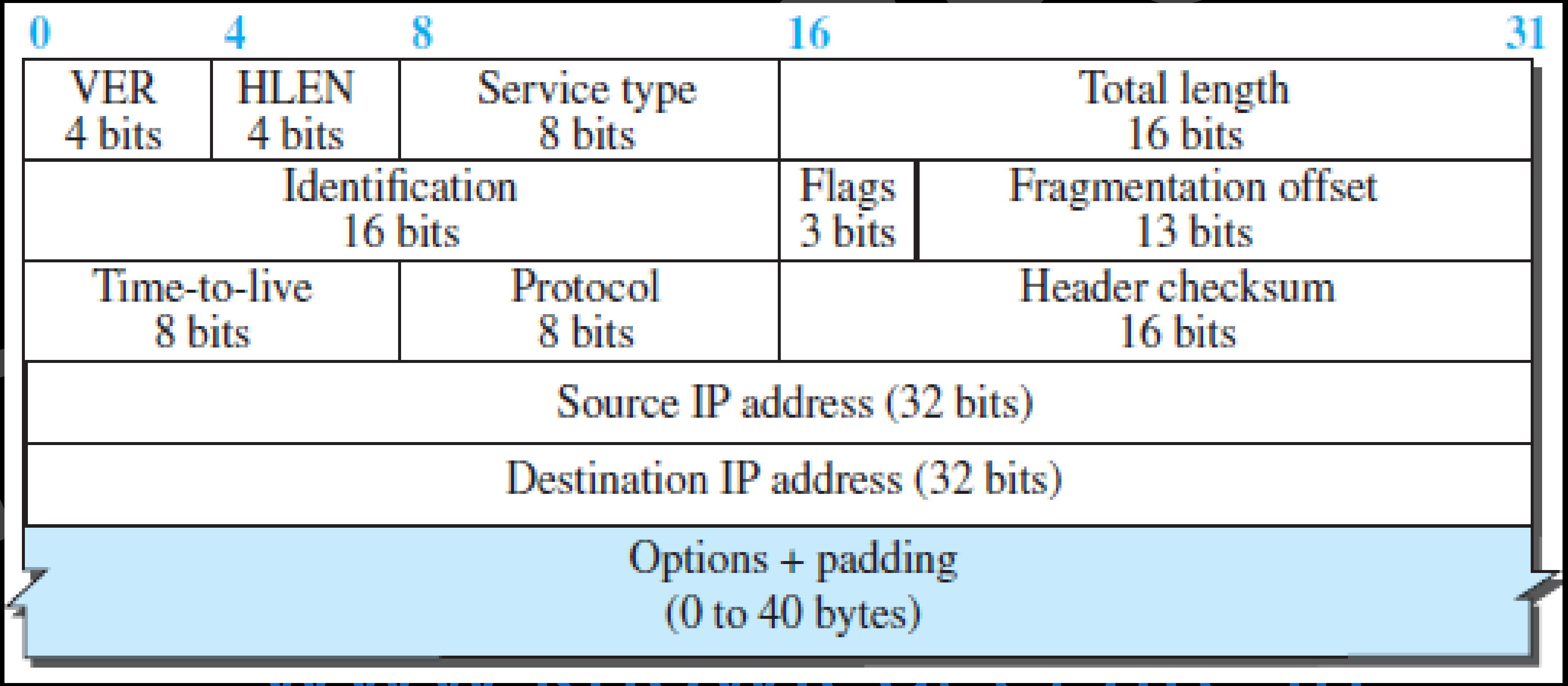
- **Point to Note**
  - The length of IP header always lies in the range of [20 bytes, 60 bytes]
  - The initial 5 rows of the IP header are always used. So, ***minimum length of IP header*** = 5 x 4 bytes = 20 bytes.
  - The size of Options field can go up to 40 bytes. So, ***maximum length of IP header*** = 20 bytes + 40 bytes = 60 bytes.
  - The range of header length field value is always [5, 15] as [20/4 = 5, 60/4 = 15]
  - The range of header length is always [20, 60].



<table>
<tr><th>0</th><th>4</th><th>8</th><th>16</th><th>31</th></tr>
<tr><td>VER
4 bits</td><td>HLEN
4 bits</td><td>Service type
8 bits</td><td colspan="2">Total length
16 bits</td></tr>
<tr><td colspan="3">Identification
16 bits</td><td>Flags
3 bits</td><td>Fragmentation offset
13 bits</td></tr>
<tr><td colspan="2">Time-to-live
8 bits</td><td>Protocol
8 bits</td><td colspan="2">Header checksum
16 bits</td></tr>
<tr><td colspan="5">Source IP address (32 bits)</td></tr>
<tr><td colspan="5">Destination IP address (32 bits)</td></tr>
<tr><td colspan="5">Options + padding
(0 to 40 bytes)</td></tr>
</table>

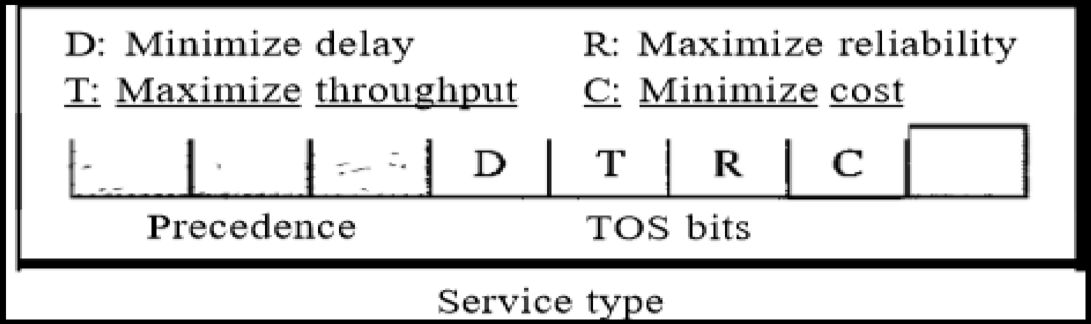
- **Services:** - IETF has changed the interpretation and name of this 8-bit field. This field, previously called service type, is now called differentiated services.

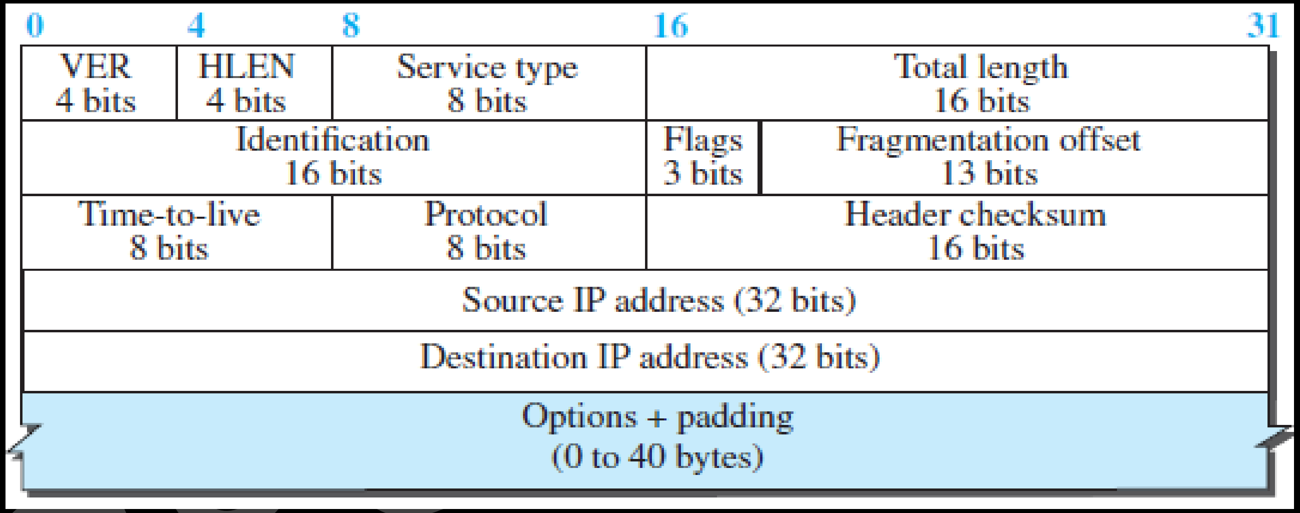
- Precedence is a 3-bit subfield ranging from 0 (000 in binary) to 7 (111 in binary). The precedence defines the priority of the datagram in issues such as congestion. If a router is congested and needs to discard some datagrams, those datagrams with lowest precedence are discarded first.



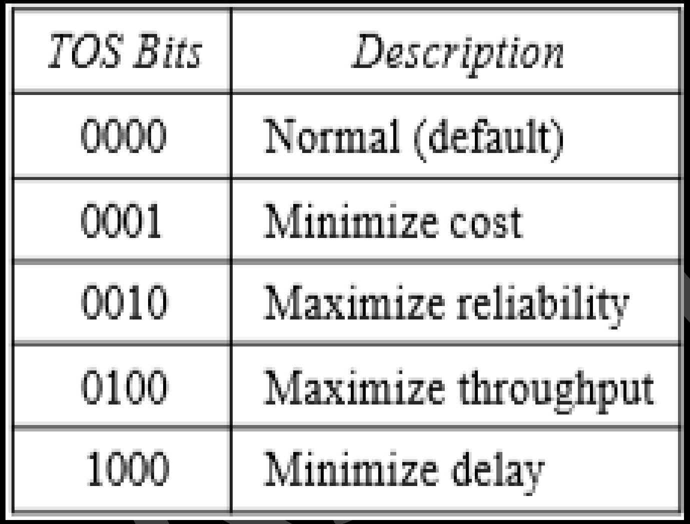
0	4	8	16	31
VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits	
Identification 16 bits			Flags 3 bits	Fragmentation offset 13 bits
Time-to-live 8 bits		Protocol 8 bits	Header checksum 16 bits	
Source IP address (32 bits)				
Destination IP address (32 bits)				
Options + padding (0 to 40 bytes)				

- **Service Type***:* It defines how the datagram should be handled. Service type is an 8-bit field that is used for Quality of Service (QoS).


D: Minimize delay
T: Maximize throughput
R: Maximize reliability
C: Minimize cost

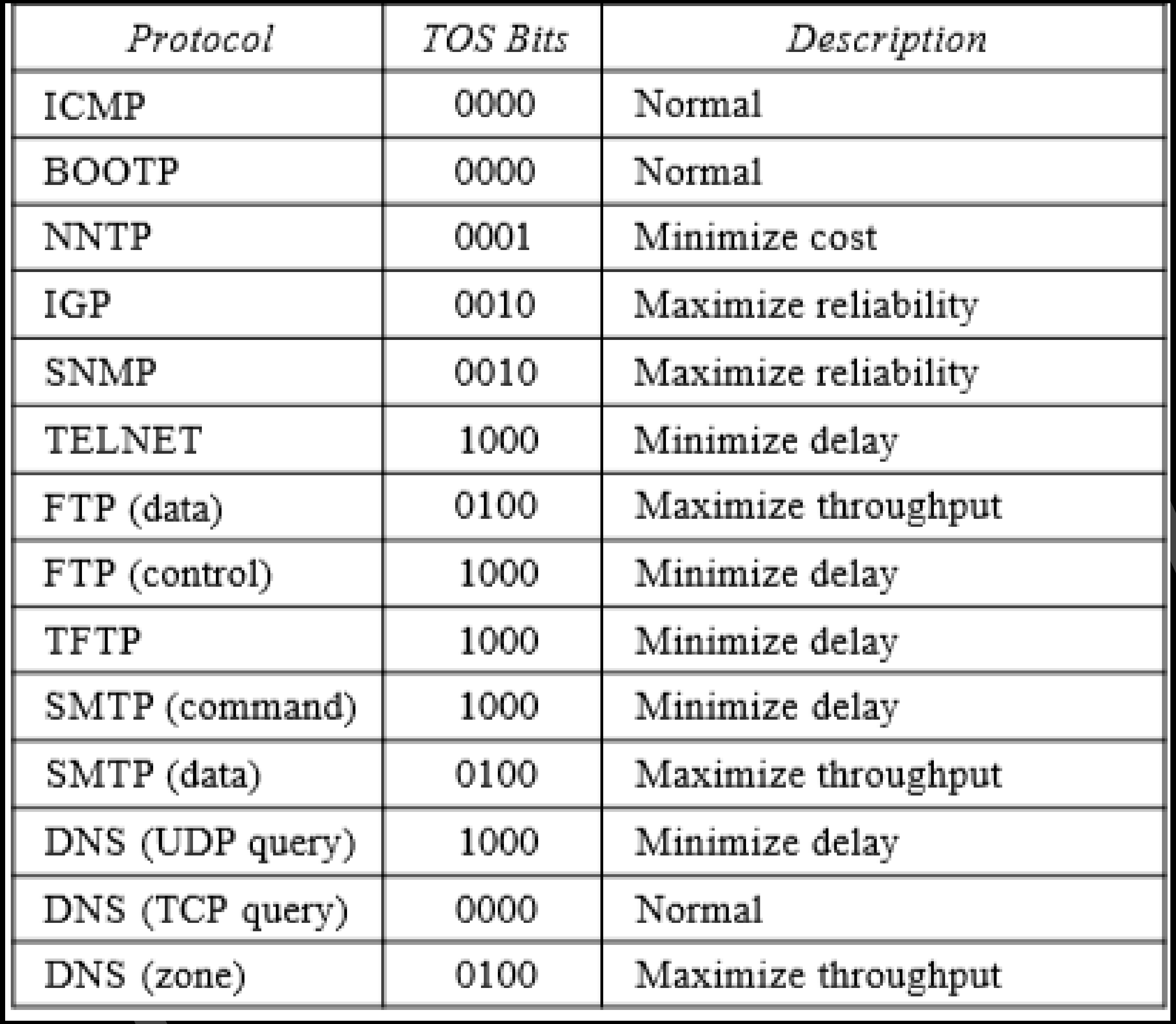


0	4	8	16	31
VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits	
Identification 16 bits			Flags 3 bits	Fragmentation offset 13 bits
Time-to-live 8 bits		Protocol 8 bits	Header checksum 16 bits	
Source IP address (32 bits)				
Destination IP address (32 bits)				
Options + padding (0 to 40 bytes)				



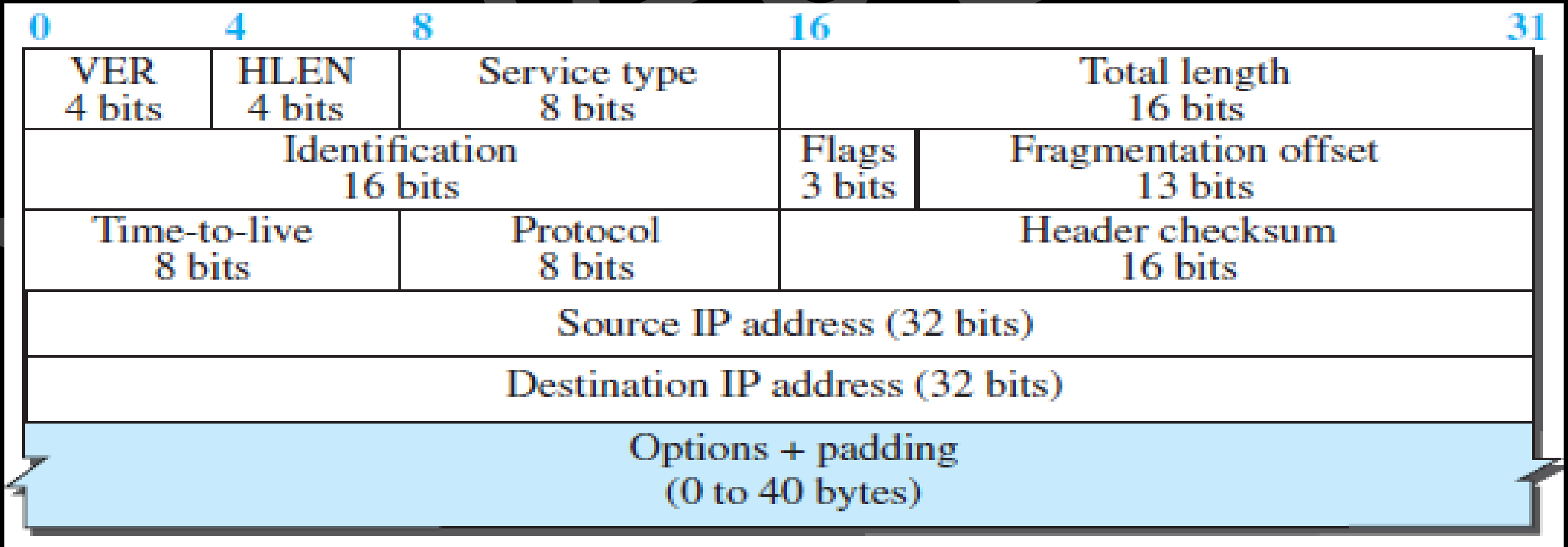
TOS Bits	*Description*
0000	Normal (default)
0001	Minimize cost
0010	Maximize reliability
0100	Maximize throughput
1000	Minimize delay

- TOS bits is a 4-bit subfield with each bit having a special meaning. Although a bit can be either 0 or 1, one and only one of the bits can have the value of 1 in each datagram



Protocol	*TOS Bits*	*Description*
ICMP	0000	Normal
BOOTP	0000	Normal
NNTP	0001	Minimize cost
IGP	0010	Maximize reliability
SNMP	0010	Maximize reliability
TELNET	1000	Minimize delay
FTP (data)	0100	Maximize throughput
FTP (control)	1000	Minimize delay
TFTP	1000	Minimize delay
SMTP (command)	1000	Minimize delay
SMTP (data)	0100	Maximize throughput
DNS (UDP query)	1000	Minimize delay
DNS (TCP query)	0000	Normal
DNS (zone)	0100	Maximize throughput

- **Total Length:** It defines the total length (header plus data) of the IP datagram in bytes. This field helps the receiving device to know when the packet has completely arrived.
- **Minimum total length of datagram** = 20 bytes (20 bytes header + 0 bytes data)
- **Maximum total length of datagram** = Maximum value of 16-bit word = 65535 bytes
- To find the length of the data coming from the upper layer, subtract the header length from the total length.
- **Length of data = total length – (HLEN) × 4**



0 4 8 16 31

VER 4 bits | HLEN 4 bits | Service type 8 bits | Total length 16 bits

Identification 16 bits | Flags 3 bits | Fragmentation offset 13 bits

Time-to-live 8 bits | Protocol 8 bits | Header checksum 16 bits

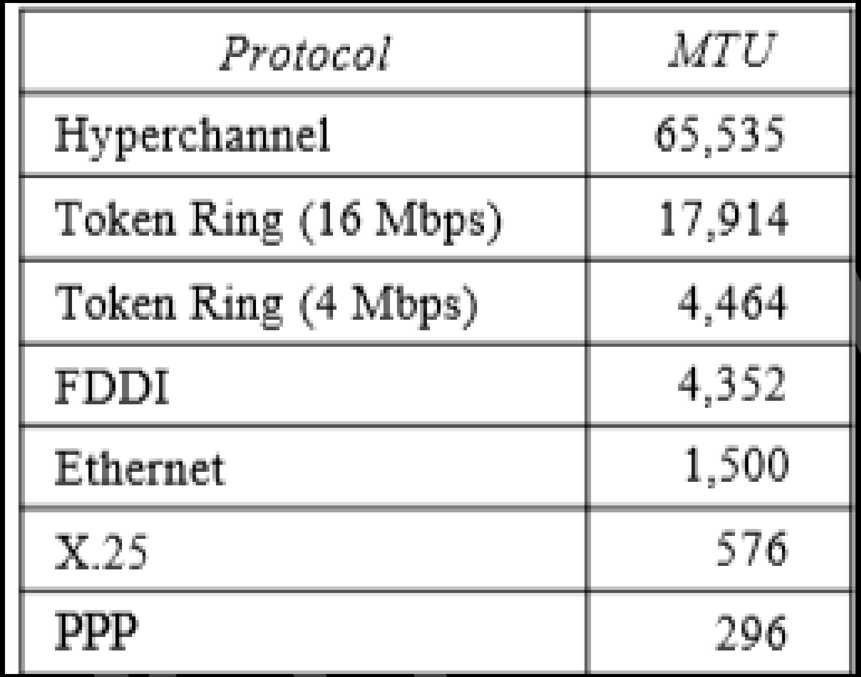
Source IP address (32 bits)

Destination IP address (32 bits)

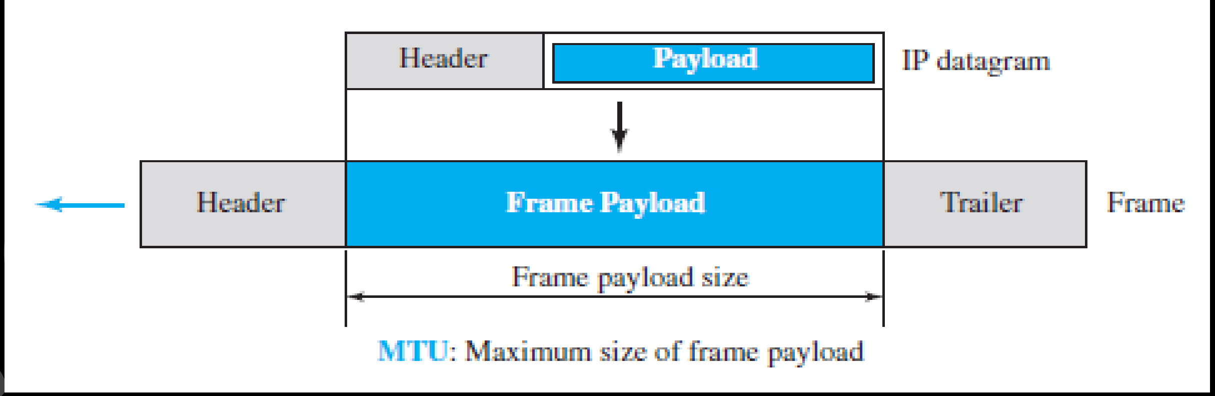
Options + padding (0 to 40 bytes)

Maximum Transfer Unit (MTU)

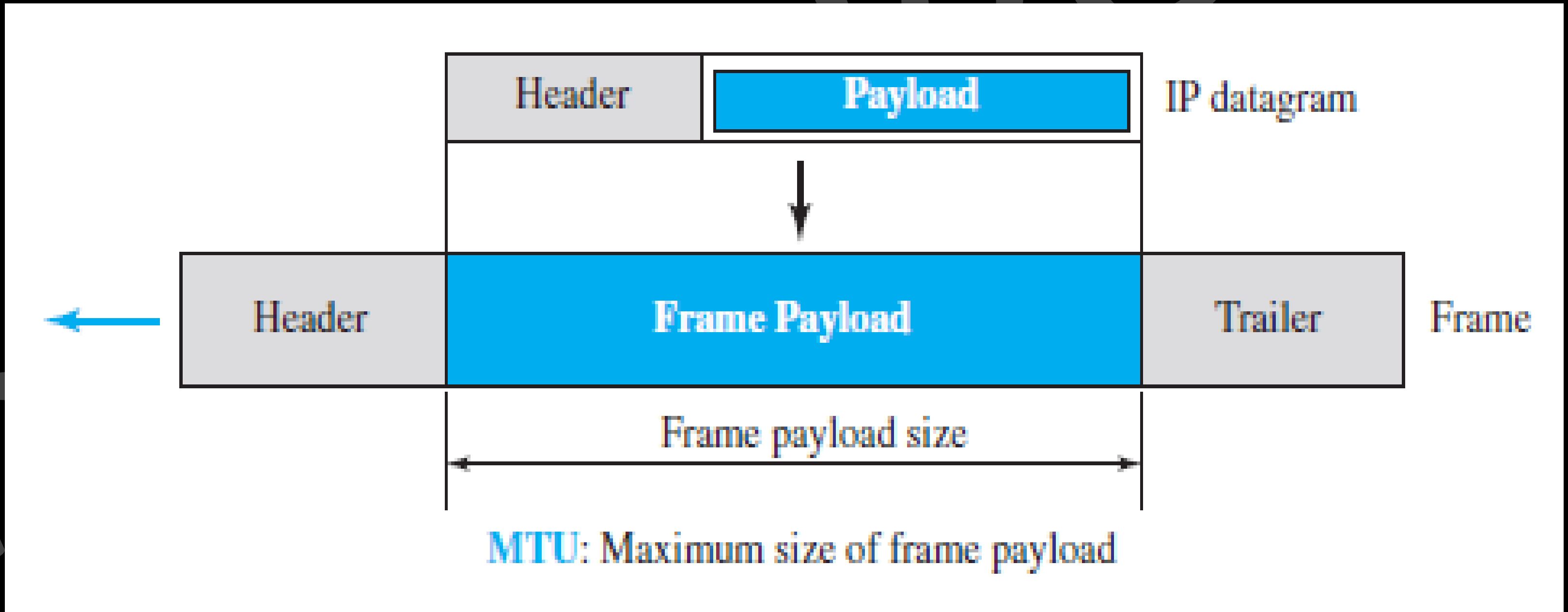
- Each link-layer protocol has its own frame format. One of the features of each format is the maximum size of the payload that can be encapsulated. In other words, when a datagram is encapsulated in a frame, the total size of the datagram must be less than this maximum size.



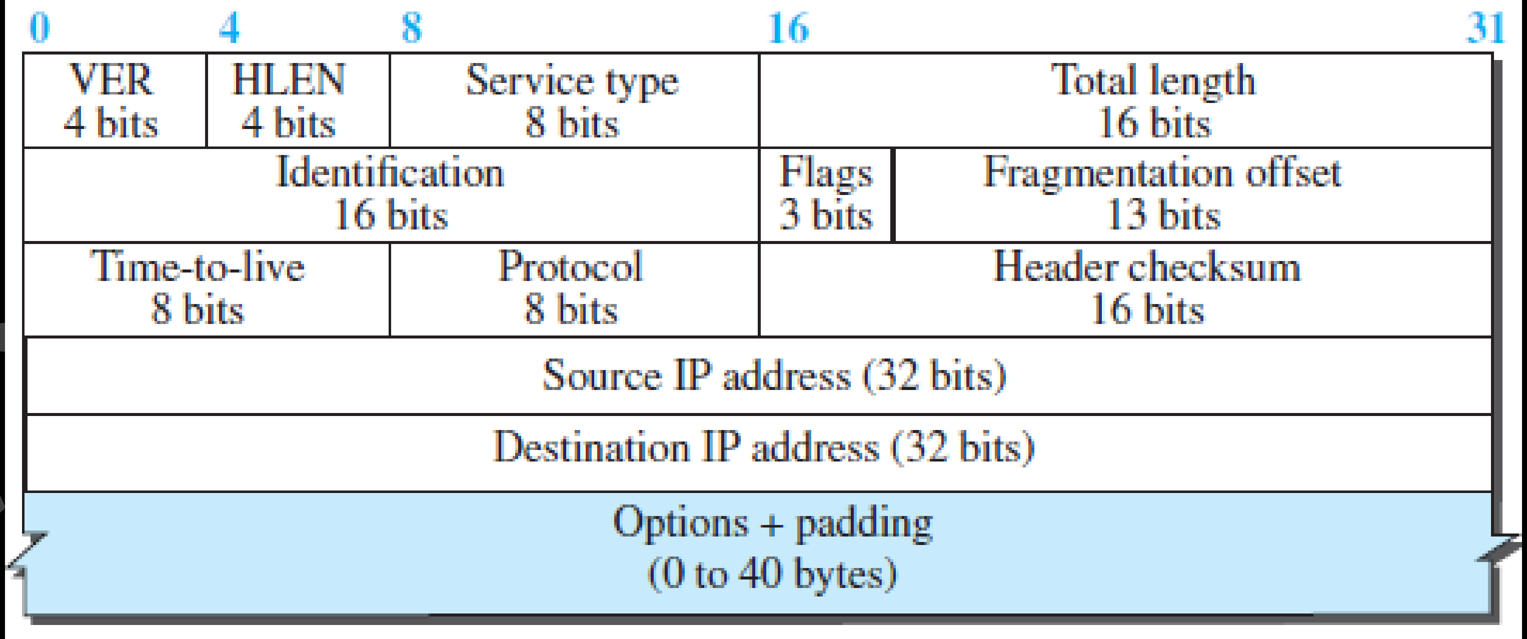
Protocol	*MTU*
Hyperchannel	65,535
Token Ring (16 Mbps)	17,914
Token Ring (4 Mbps)	4,464
FDDI	4,352
Ethernet	1,500
X.25	576
PPP	296



- ***The value of the MTU differs from one physical network protocol to another.*** For example, the value for a LAN is normally 1500 bytes, but for a WAN it can be larger or smaller.
- When a datagram is fragmented it means that the payload of the IP datagram is fragmented and each fragment has its own header with most of the fields repeated, but some have been changed such as flags, fragmentation offset, and total length and checksum is recalculated at each point.
- A fragmented datagram may itself be fragmented if it encounters a network with an even smaller MTU. Thus, ***datagram may be fragmented several times before it reaches the final destination.***



- **Identification**: 16-bit *identification field* identifies a datagram originating from the source host. To guarantee uniqueness, IP protocol uses a counter to label the datagrams.
- The counter is initialized to a positive number. When the IP protocol sends a datagram, it copies the current value of the counter to the identification field and increments the counter by one.
- When a datagram is fragmented, the value in the identification field is copied into all fragments, used for the identification of the fragments of an original IP datagram. The identification number helps the destination in reassembling the datagram.

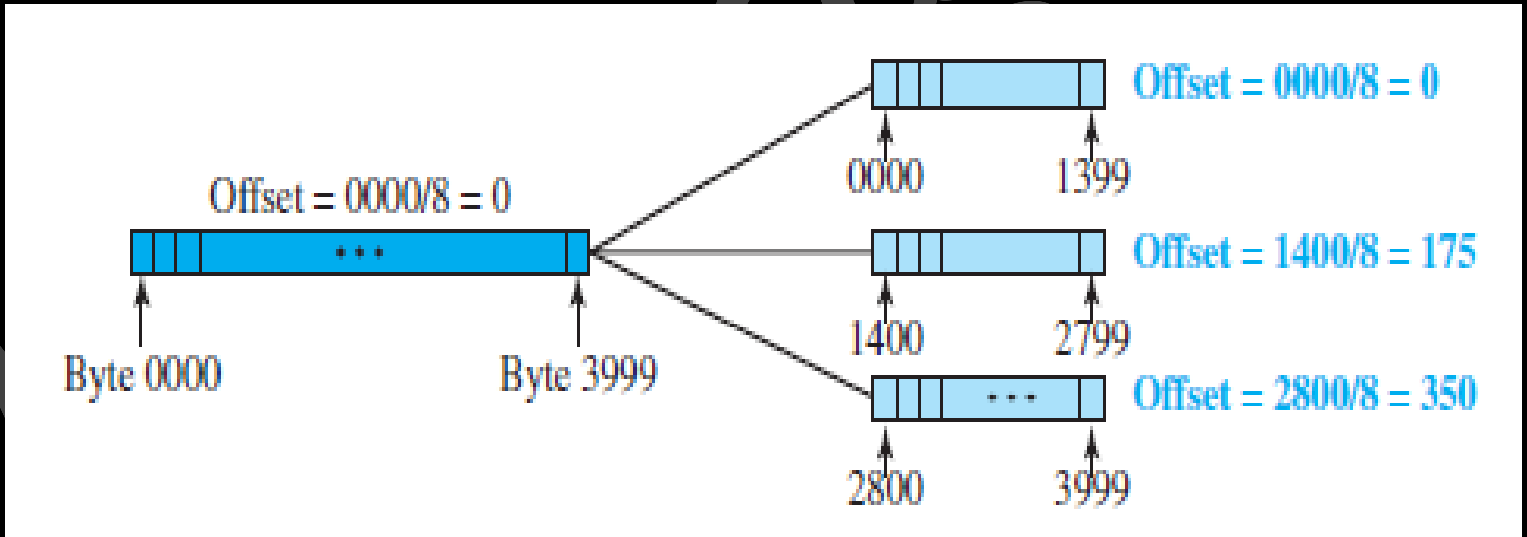


0 4 8 16 31

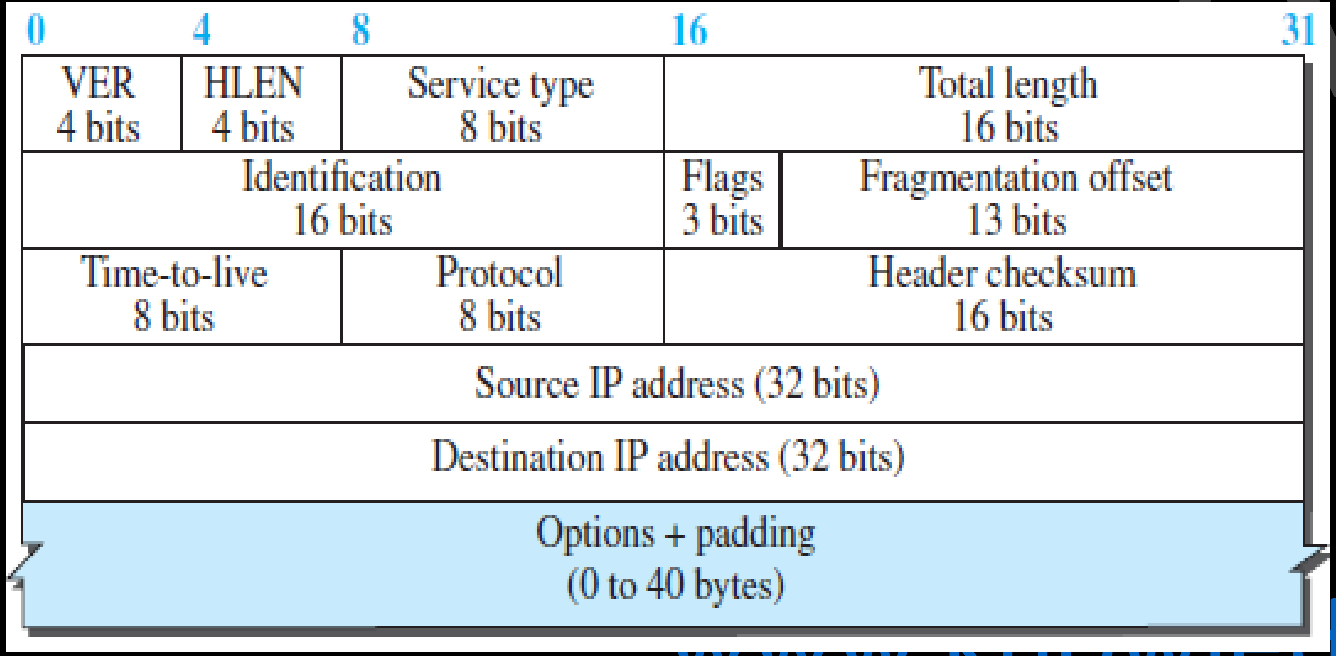
VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits	
Identification 16 bits			Flags 3 bits	Fragmentation offset 13 bits
Time-to-live 8 bits		Protocol 8 bits	Header checksum 16 bits	
Source IP address (32 bits)				
Destination IP address (32 bits)				
Options + padding (0 to 40 bytes)				

Fragmentation

- Fragmentation is a process of dividing the datagram into fragments during its transmission.
- Datagram can be fragmented by the source host or any router in the path.
- The reassembly of the datagram, is done only by the destination host, because each fragment becomes an independent datagram.
- The fragmented datagram can travel through different routes.



- **Flag Field:** The 3-bit *flags field* defines three flags.
  - The leftmost bit is reserved (not used).
  - The second bit (D bit) is called the *do not fragment* bit.
    - If its value is 1, the machine must not fragment the datagram.
    - If its value is 0, the datagram can be fragmented if necessary.
  - The third bit (M bit) is called the *more fragment bit*.
    - If its value is 1, it means the datagram is not the last fragment; there are more fragments after this one.
    - If its value is 0, it means this is the last or only fragment.



VER 4 bits | HLEN 4 bits | Service type 8 bits | Total length 16 bits

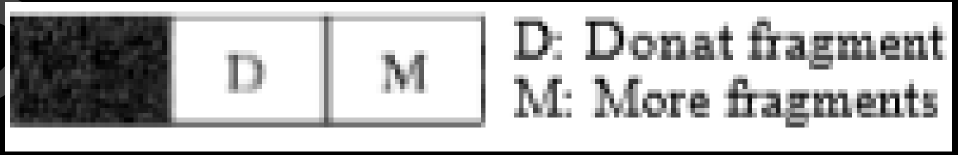
Identification 16 bits | Flags 3 bits | Fragmentation offset 13 bits

Time-to-live 8 bits | Protocol 8 bits | Header checksum 16 bits

Source IP address (32 bits)

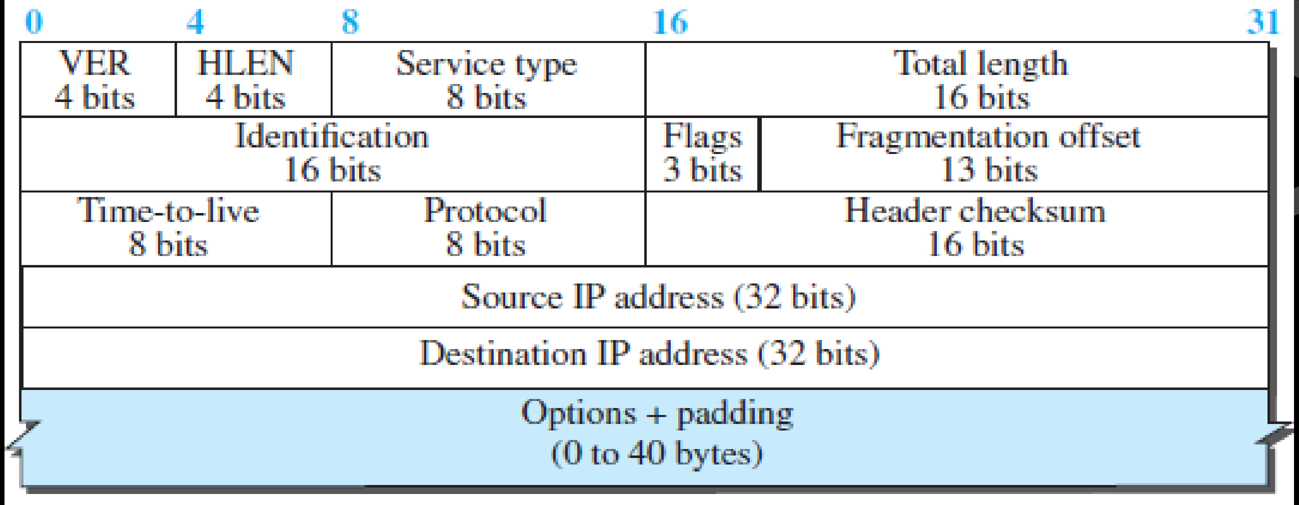
Destination IP address (32 bits)

Options + padding (0 to 40 bytes)

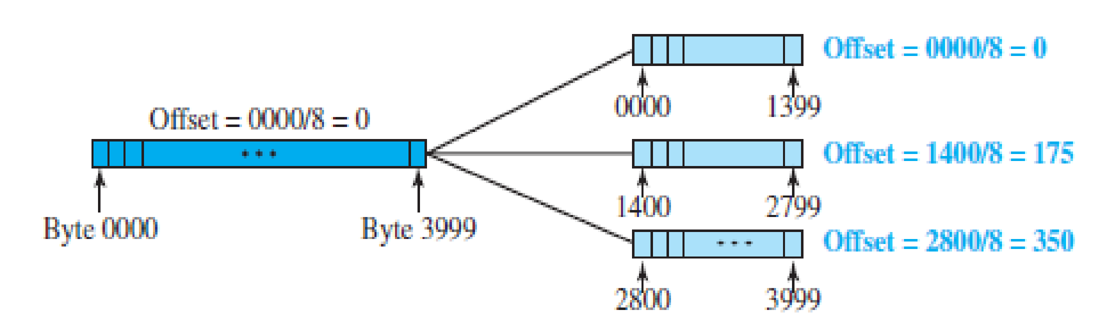


D: Donat fragment
M: More fragments

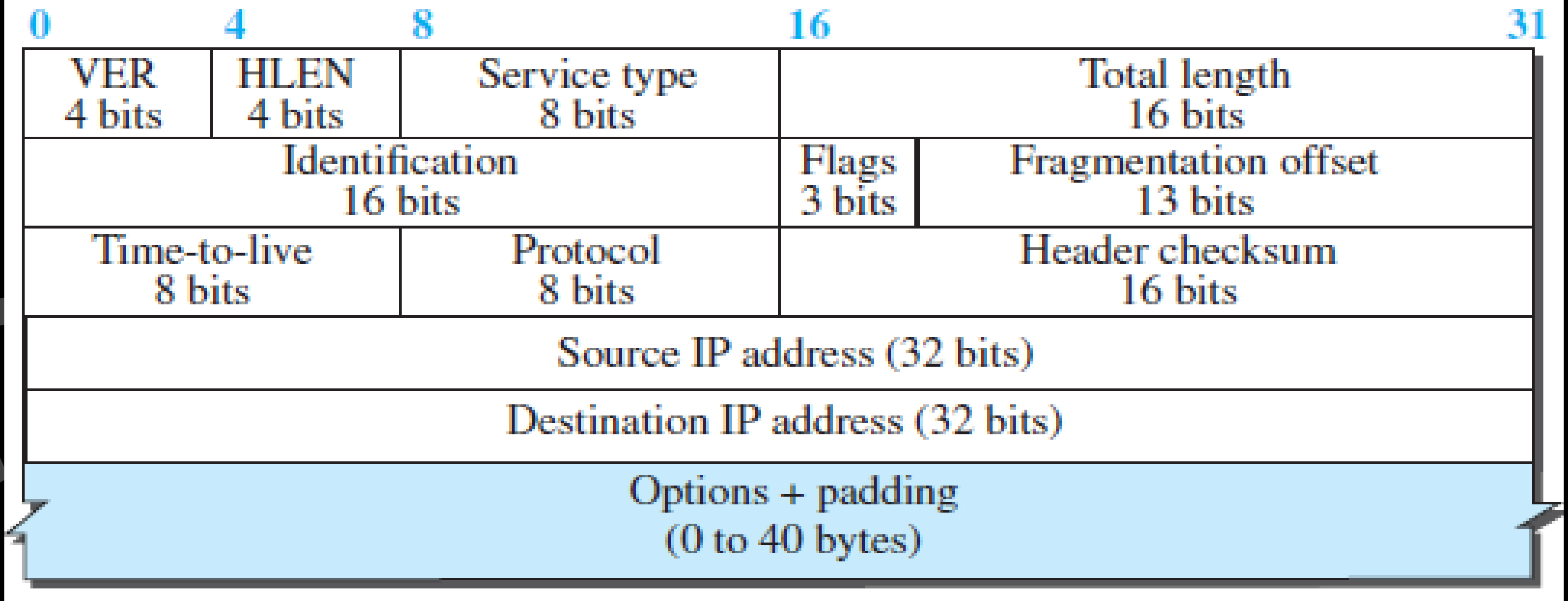
- **Fragmentation Offset**: The 13-bit *fragmentation offset field* shows the relative position of this fragment with respect to the whole datagram.
- It is the offset of the data in the original datagram measured in units of 8 bytes.
- The bytes in the original datagram are numbered 0 to 3999.
- The first fragment carries bytes 0 to 1399. The offset value => 0/8 = 0.
- The second fragment carries bytes 1400 to 2799; the offset value => 1400/8 = 175.
- The third fragment carries bytes 2800 to 3999. The offset value => 2800/8 = 350.



VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits	
Identification 16 bits			Flags 3 bits	Fragmentation offset 13 bits
Time-to-live 8 bits		Protocol 8 bits	Header checksum 16 bits	
Source IP address (32 bits)				
Destination IP address (32 bits)				
Options + padding (0 to 40 bytes)				

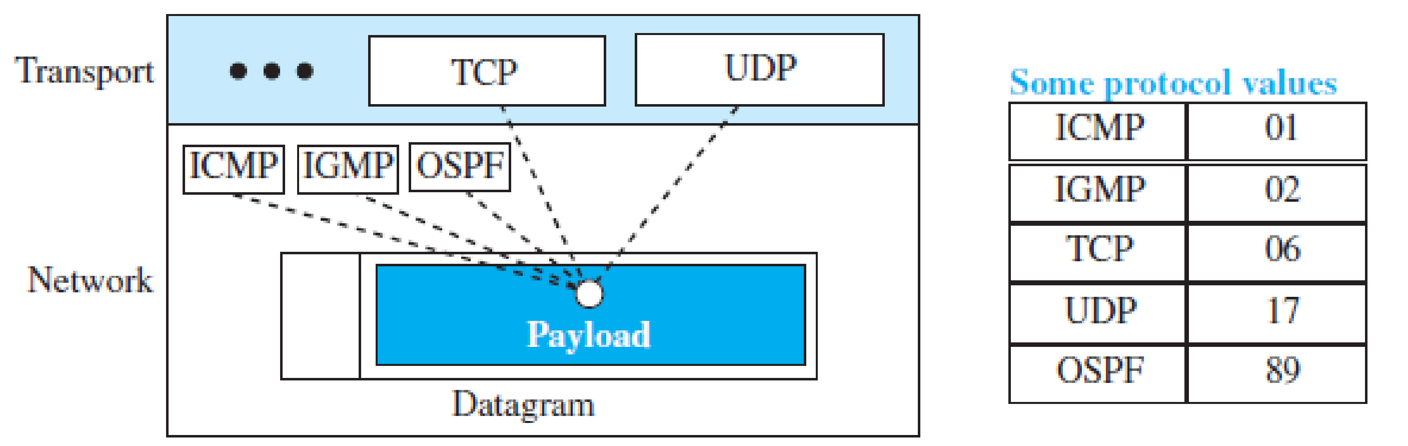


- **Time-to-Live** (TTL): field in a datagram dictates the maximum number of hops (via routers) it can take, generally set to twice the highest number of routers between any two hosts.
- Every router the datagram passes through decreases the TTL value by one; the datagram is discarded if the TTL reaches zero, preventing it from circulating indefinitely due to potential routing table errors.
- Besides limiting a datagram's lifespan, the TTL field can be used to restrict a packet's journey deliberately, like confining it to a local network by setting the TTL value to 1, causing its discard at the first router.



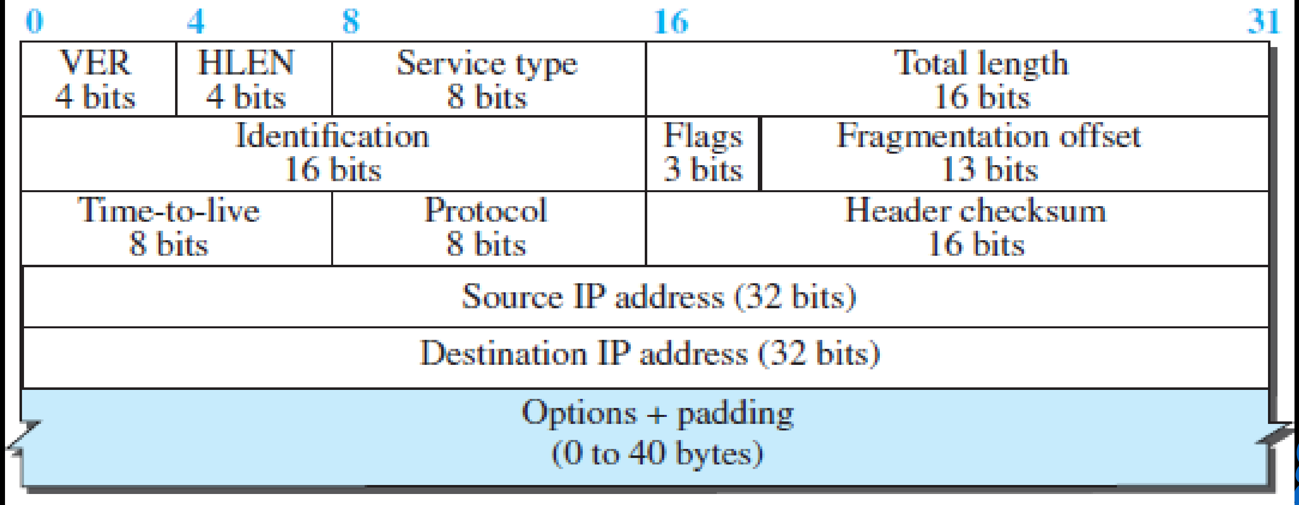
<table>
<tr><th>0</th><th>4</th><th>8</th><th>16</th><th>31</th></tr>
<tr><td>VER
4 bits</td><td>HLEN
4 bits</td><td>Service type
8 bits</td><td colspan="2">Total length
16 bits</td></tr>
<tr><td colspan="3">Identification
16 bits</td><td>Flags
3 bits</td><td>Fragmentation offset
13 bits</td></tr>
<tr><td colspan="2">Time-to-live
8 bits</td><td>Protocol
8 bits</td><td colspan="2">Header checksum
16 bits</td></tr>
<tr><td colspan="5">Source IP address (32 bits)</td></tr>
<tr><td colspan="5">Destination IP address (32 bits)</td></tr>
<tr><td colspan="5">Options + padding
(0 to 40 bytes)</td></tr>
</table>

- **Protocol:** In TCP/IP, the data section of a packet, called the payload, carries the whole packet from another protocol. A datagram, for example, can carry a packet belonging to any transport-layer protocol such as UDP or TCP.
- When the datagram arrives at the destination, the value of this field helps to define to which protocol the payload should be delivered.



Some protocol values

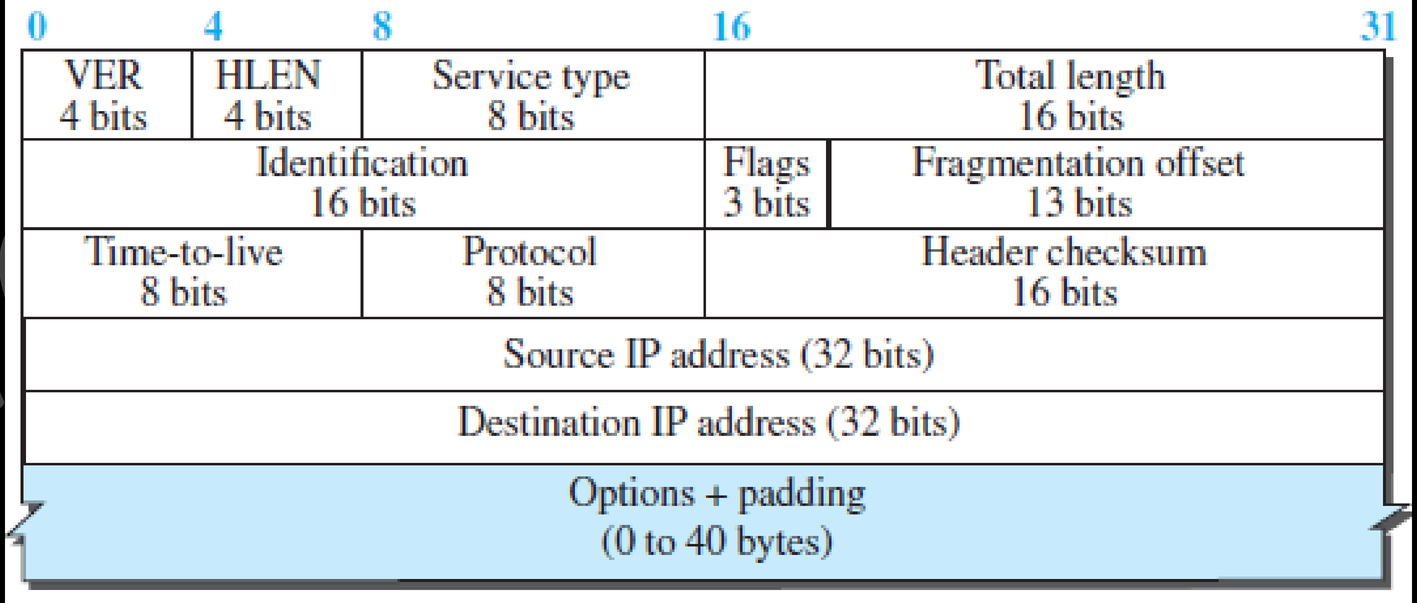
ICMP	01
IGMP	02
TCP	06
UDP	17
OSPF	89



<table>
<tr><td>0</td><td>4</td><td>8</td><td>16</td><td>31</td></tr>
<tr><td>VER
4 bits</td><td>HLEN
4 bits</td><td>Service type
8 bits</td><td colspan="2">Total length
16 bits</td></tr>
<tr><td colspan="3">Identification
16 bits</td><td>Flags
3 bits</td><td>Fragmentation offset
13 bits</td></tr>
<tr><td colspan="2">Time-to-live
8 bits</td><td>Protocol
8 bits</td><td colspan="2">Header checksum
16 bits</td></tr>
<tr><td colspan="5">Source IP address (32 bits)</td></tr>
<tr><td colspan="5">Destination IP address (32 bits)</td></tr>
<tr><td colspan="5">Options + padding
(0 to 40 bytes)</td></tr>
</table>

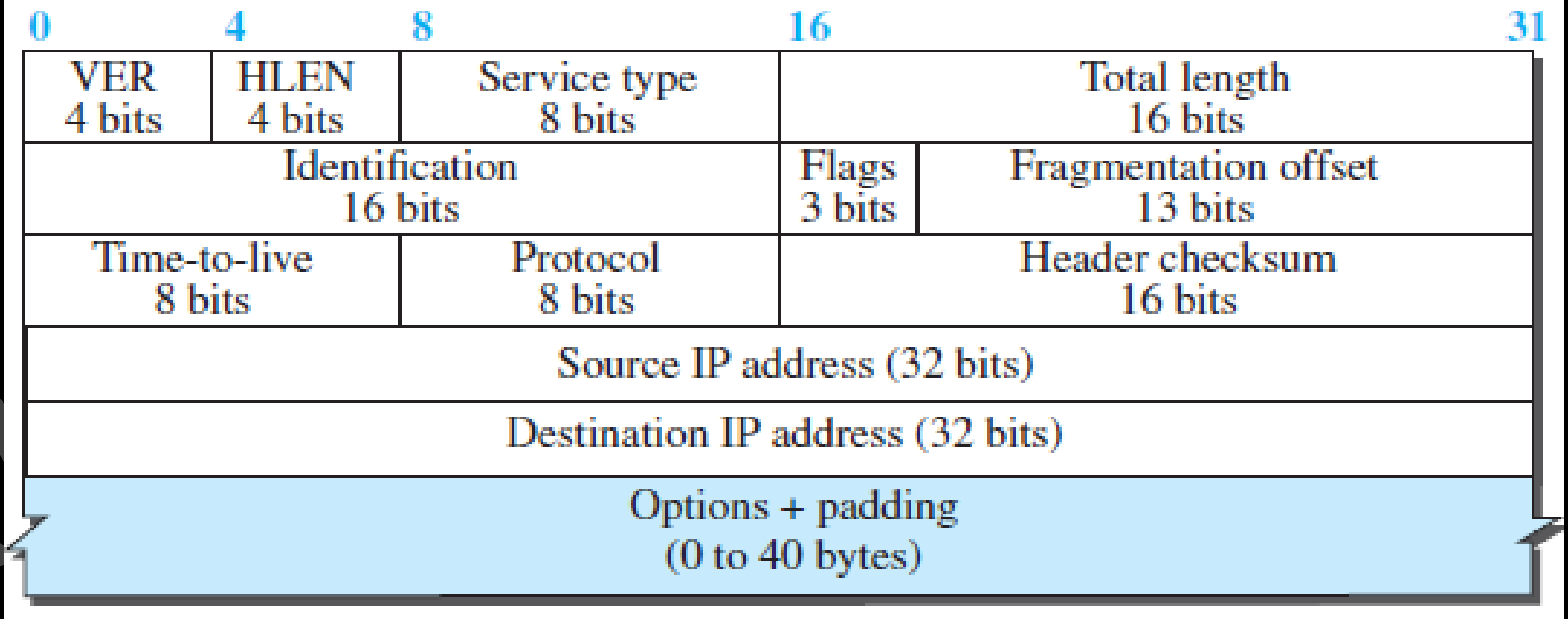
Header checksum: The IP header checksum field only verifies the header, not the payload, indicating that IP is not entirely reliable as it doesn't affirm the payload remains unaltered during transmission.

- Due to alterations in fields such as TTL at every router, the checksum needs frequent recalculations.
- Upper-level protocols encapsulating data in the IPv4 datagram maintain separate checksums that cover the complete packet, thus the IPv4 datagram checksum doesn't validate the contained data.
- The IPv4 packet's header, which changes at each visited router (but not the data), is the only section included in the checksum, preventing unnecessary increases in processing time from recalculating the entire packet's checksum at every router.



0	4	8	16	31
VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits	
Identification 16 bits			Flags 3 bits	Fragmentation offset 13 bits
Time-to-live 8 bits		Protocol 8 bits	Header checksum 16 bits	
Source IP address (32 bits)				
Destination IP address (32 bits)				
Options + padding (0 to 40 bytes)				

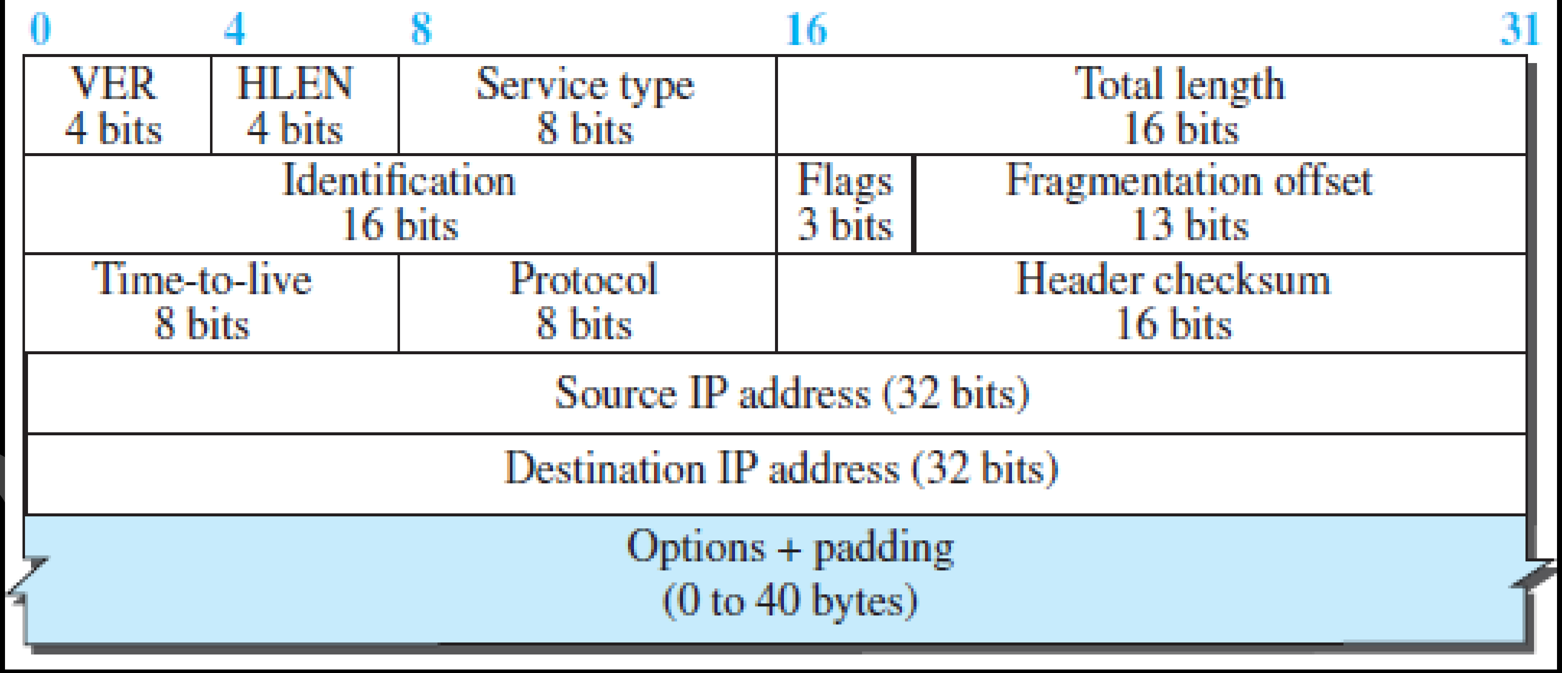
- **Source and Destination Addresses:** These 32-bit source and destination address fields define the IP address of the source and destination respectively.



0	4	8	16	31
VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits	
Identification 16 bits			Flags 3 bits	Fragmentation offset 13 bits
Time-to-live 8 bits		Protocol 8 bits	Header checksum 16 bits	
Source IP address (32 bits)				
Destination IP address (32 bits)				
Options + padding (0 to 40 bytes)				

Variable part

- The variable part comprises the options that can be a maximum of 40 bytes. Options, as the name implies, are not required for a datagram. They can be used for network testing and debugging.



0	4	8	16	31
VER 4 bits	HLEN 4 bits	Service type 8 bits	Total length 16 bits	
Identification 16 bits			Flags 3 bits	Fragmentation offset 13 bits
Time-to-live 8 bits		Protocol 8 bits	Header checksum 16 bits	
Source IP address (32 bits)				
Destination IP address (32 bits)				
Options + padding (0 to 40 bytes)				

- **End of Option**
  - An end-of-option option is a 1-byte option used for padding at the end of the option field. It, however, can only be used as the last option.

- **Record Route**
  - A record route option is used to record the Internet routers that handle the datagram. It can list up to nine router addresses. It can be used for debugging and management purposes.

- **Strict Source Route**
  - A strict source route option is used by the source to predetermine a route for the datagram as it travels through the Internet. Dictation of a route by the source can be useful for several purposes.
  - The sender can choose a route with a specific type of service, such as minimum delay or maximum throughput.
  - Alternatively, it may choose a route that is safer or more reliable for the sender's purpose. For example, a sender can choose a route so that its datagram does not travel through a competitor's network.
  - If a datagram specifies a strict source route, all the routers defined in the option must be visited by the datagram. A router must not be visited if its IPv4 address is not listed in the datagram. If the datagram visits a router that is not on the list, the datagram is discarded and an error message is issued.
  - If the datagram arrives at the destination and some of the entries were not visited, it will also be discarded and an error message issued.

- **Loose Source Route**
  - A loose source route option is similar to the strict source route, but it is less rigid. Each router in the list must be visited, but the datagram can visit other routers as well.

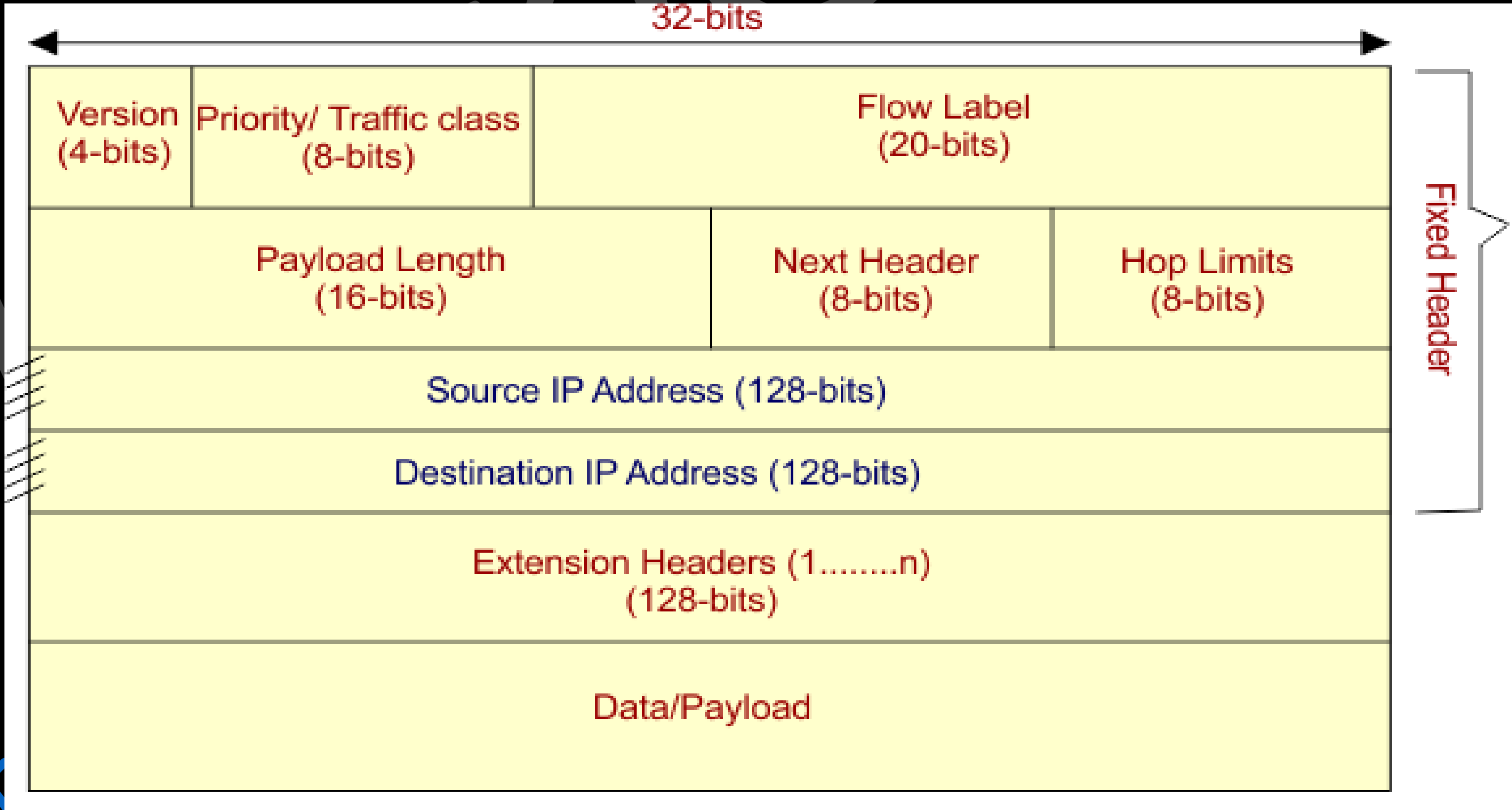
- **Timestamp**
  - A timestamp option is used to record the time of datagram processing by a router. The time is expressed in milliseconds from midnight, Universal time or Greenwich mean time.
  - Knowing the time, a datagram is processed can help users and managers track the behaviour of the routers in the Internet. We can estimate the time it takes for a datagram to go from one router to another. We say estimate because, although all routers may use Universal time, their local clocks may not be synchronized.

IPv6

- Each packet can be divided into two parts :
  - Base header
  - Payload

- The payload is made up of two parts :
  - An optional extension header
  - The upper layer data

- Base header has eight fields



32-bits
Version (4-bits)
Priority/ Traffic class (8-bits)
Flow Label (20-bits)
Payload Length (16-bits)
Next Header (8-bits)
Hop Limits (8-bits)
Source IP Address (128-bits)
Destination IP Address (128-bits)
Extension Headers (1........n) (128-bits)
Data/Payload
Fixed Header

IPV6 Header

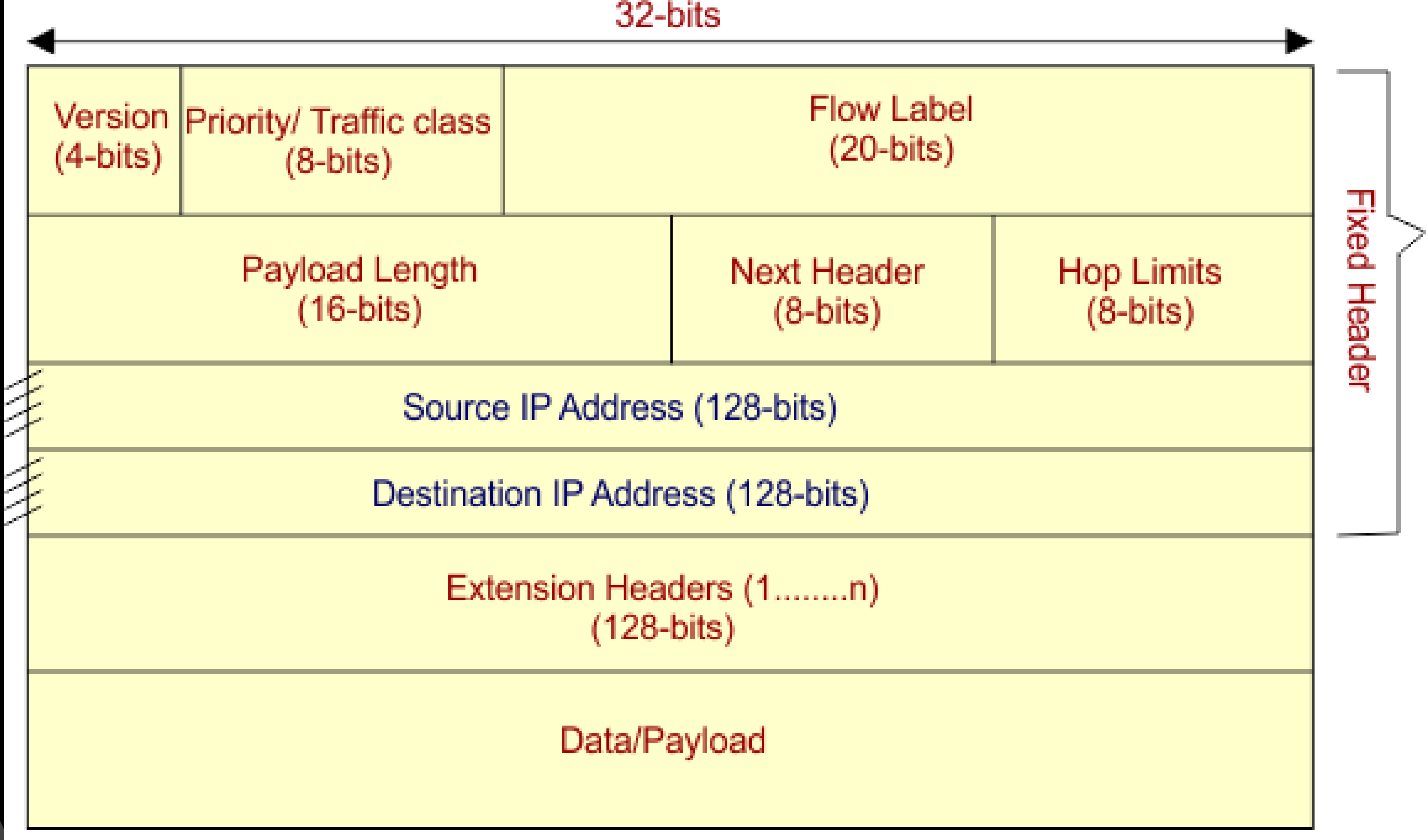
i. Version: This is 4-bit field which defines the version number of IP. For IPv6, the value is 6.

ii. Priority: The 4-bit priority field defines the priority of the packet with respect to traffic congestion.

iii. Flow label: The flow label is a 3-byte field that is designed to provide special handling for a particular flow of data.

iv. Payload length: The 2-byte payload length field defines the total length of IP datagram excluding the base header.

v. Next header: The next header is an 8-bit field defines the header that follows the base header in the datagram.


32-bits
Version (4-bits)
Priority/ Traffic class (8-bits)
Flow Label (20-bits)
Payload Length (16-bits)
Next Header (8-bits)
Hop Limits (8-bits)
Source IP Address (128-bits)
Destination IP Address (128-bits)
Extension Headers (1........n) (128-bits)
Data/Payload
Fixed Header

IPV6 Header

vi. Hop limit: This 8-bit hop limit field serves the same purpose as TTL field in IPv4.

vii. Source address: The source address field is a 16-bytes internet address that identifies the original source of datagram.

viii. Destination address: The destination address field is a 16-byte internet address that usually identifies the final destination of the datagram.

ix. Extension header: Extension header field help in processing of data packets by appending different extension header. Each extension header has a length equal to multiple of 64-bits.

1. Address Length
    1. IPv4: 32-bit (4 bytes)
    2. IPv6: 128-bit (16 bytes)
2. Address Notation
    1. IPv4: Decimal (e.g., 192.168.1.1)
    2. IPv6: Hexadecimal (e.g., 2001:0db8:85a3:0000)
3. Number of Addresses
    1. IPv4: Approximately 4.3 billion
    2. IPv6: Approximately 340 undecillion
4. Configuration
    1. IPv4: Manual or DHCP
    2. IPv6: Stateless address autoconfiguration (SLAAC) or DHCPv6
5. Security
    1. IPv4: Initially lacked, added later as extensions
    2. IPv6: Inbuilt support for IPsec, providing network security at the IP layer

Advancements in IPv6:

- **Larger Address Space**: Can accommodate a virtually unlimited number of unique addresses, facilitating the growth of the internet.
- **Simplified Header**: IPv6 has a simpler header structure, which improves the speed of routing by allowing routers to process packets more efficiently.
- **Improved Multicast**: IPv6 utilizes multicast addressing to send data packets to multiple destinations in a single transmission, which conserves bandwidth compared to IPv4.
- **No NAT Required**: IPv6 was designed to eliminate the need for NAT, making end-to-end connection more straightforward and reducing latency and complexity.
- **Mobility and Security**: IPv6 was built considering modern requirements, offering better support for mobile devices and higher levels of security.

Need of Additional protocols

- IP packets, however, need to be encapsulated in a frame, which needs physical addresses (node-to-node). We will see that a protocol called ARP, the **Address Resolution Protocol**.

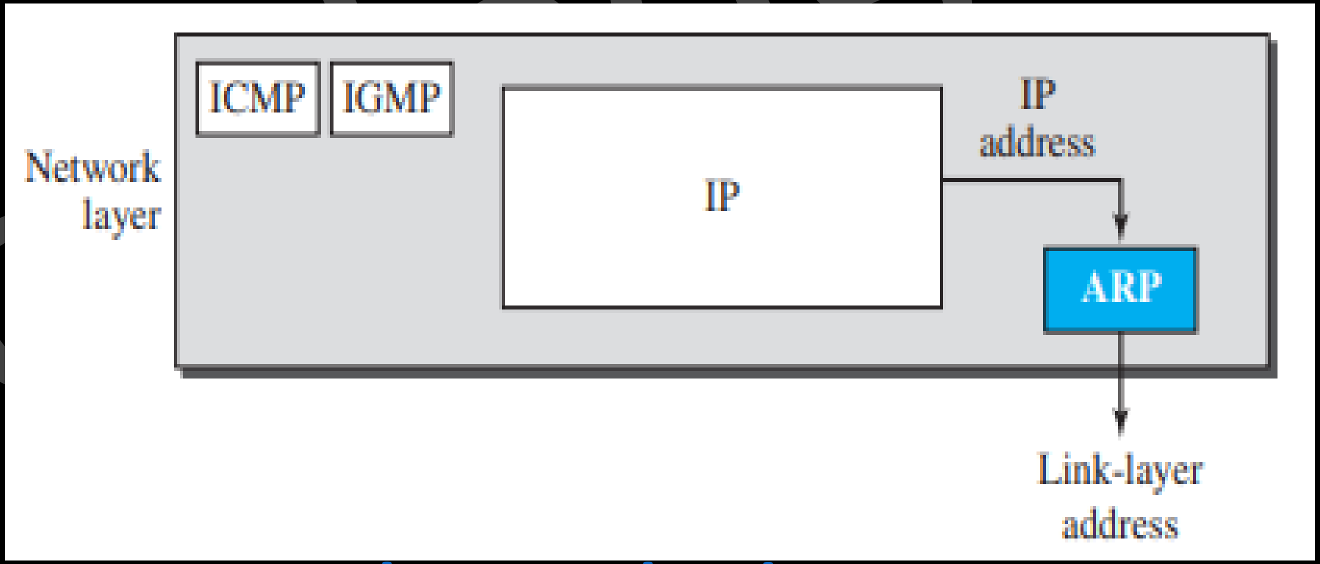
- We sometimes need reverse mapping-mapping a physical address to a logical address. For example, when booting a diskless network or leasing an IP address to a host, **RARP** is used.

- Lack of flow and error control in the Internet Protocol has resulted in another protocol, **ICMP**, that provides alerts. It reports congestion and some types of errors in the network or destination host

- IP was originally designed for unicast delivery, one source to one destination. As the Internet has evolved, the need for multicast delivery, one source to many destinations, has increased tremendously. **IGMP** gives IP a multicast capability.

Address Resolution Protocol (ARP)

- The IP address of the next node alone is not helpful in moving a frame through a link; we need the link-layer address of the next node.
- ARP maps an IP address to a logical-link address. ARP accepts an IP address from the IP protocol, maps the address to the corresponding link-layer address, and passes it to the data-link layer.
- The ARP protocol is one of the auxiliary protocols defined in the **network layer.**

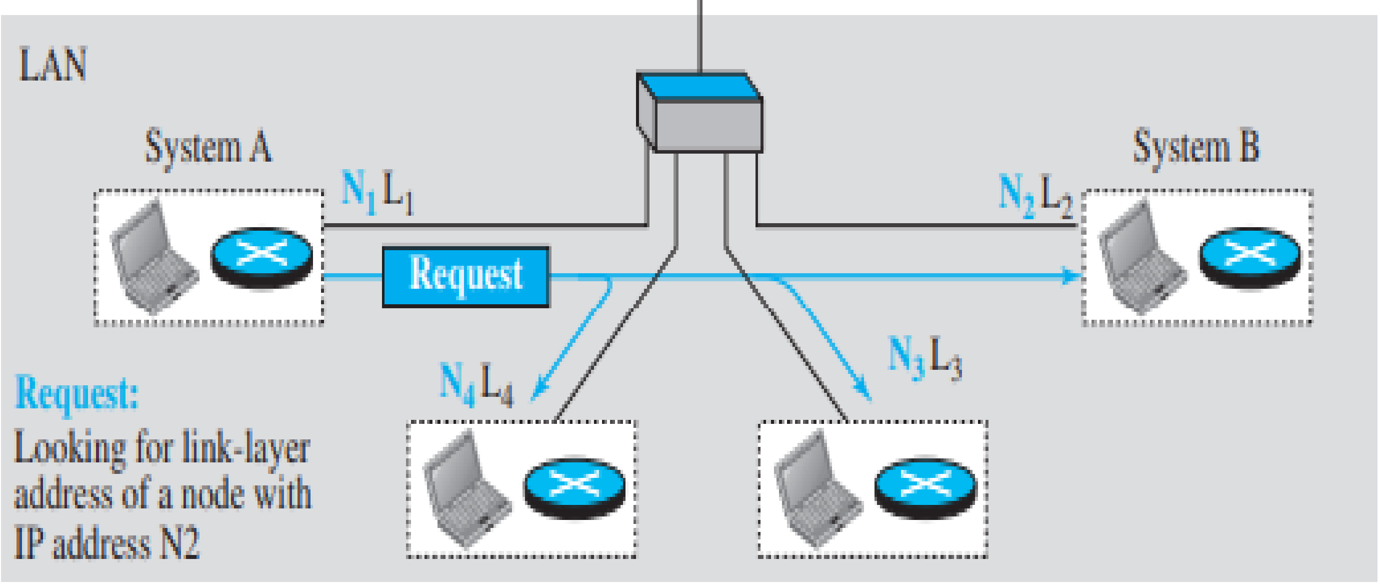


1. Anytime a host or a router needs to find the link-layer address of another host or router in its network, it sends an ARP request packet. The packet includes the ***link-layer and IP addresses of the sender and the IP address of the receiver.***

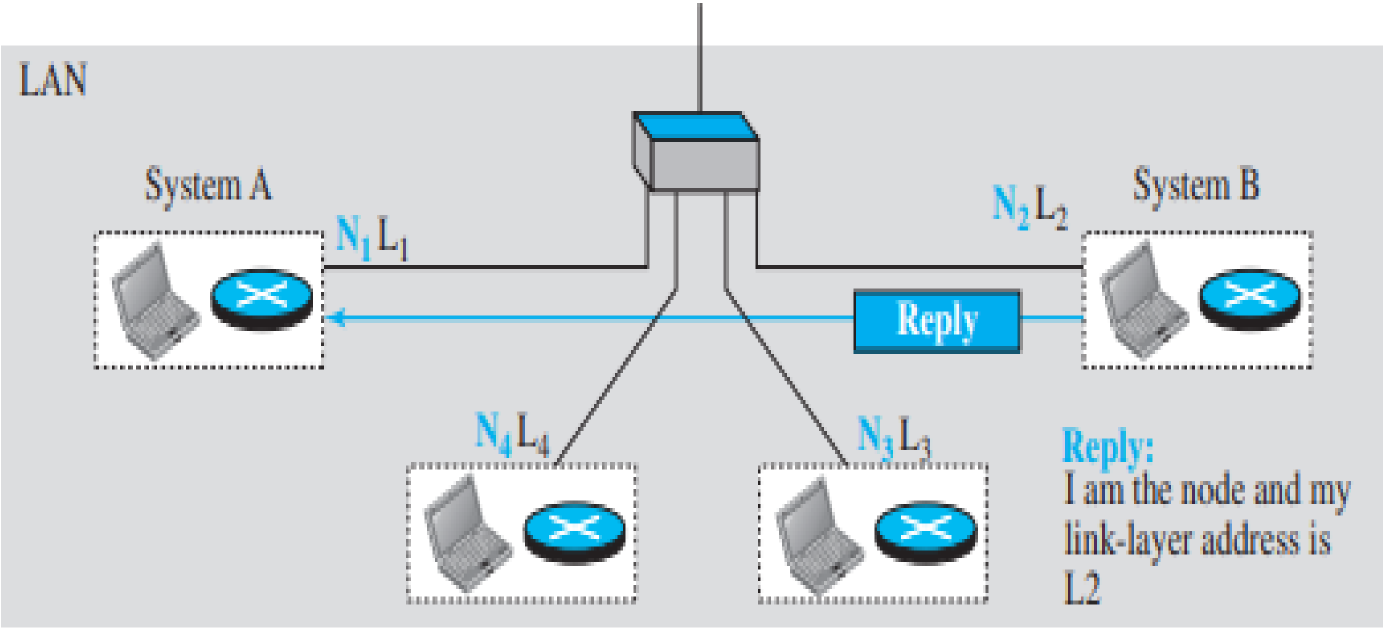
2. Because the sender does not know the link-layer address of the receiver, the query is broadcast over the link.

3. Every host or router on the network receives and processes the ARP request packet, but only the intended recipient recognizes its IP address and sends back an ARP response packet.

4. The response packet contains the recipient's IP and link-layer addresses. ***The packet is unicast directly to the node that sent the request packet.***



a. ARP request is broadcast



b. ARP reply is unicast

RARP

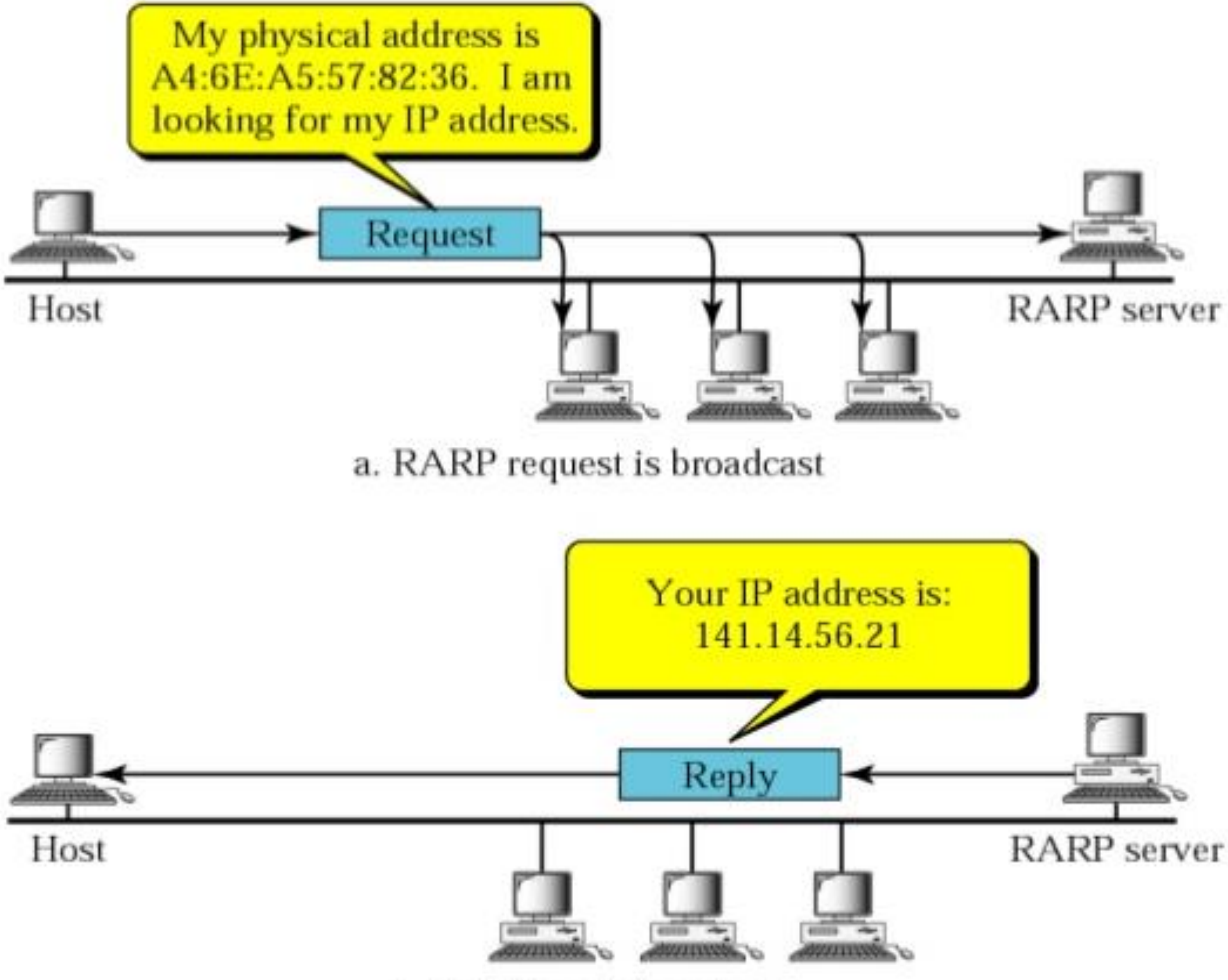
- Reverse Address Resolution Protocol (RARP) finds the logical address for a machine that knows only its physical address. Each host or router is assigned one or more logical (IP) addresses, which are unique and independent of the physical (hardware) address of the machine. To create an IP datagram, a host or a router needs to know its own IP address.

- The IP address of a machine is usually read from its configuration file stored on a disk file. However, a diskless machine is usually booted from ROM, which has minimum booting information. The ROM is installed by the manufacturer. It cannot include the IP address because the IP addresses on a network are assigned by the network administrator.

- The machine can get its physical address (by reading its NIC, for example), which is unique locally. It can then use the physical address to get the logical address by using the RARP protocol.

- A RARP request is created and broadcast on the local network. Another machine on the local network that knows all the IP addresses will respond with a RARP reply.

- The requesting machine must be running a RARP client program; the responding machine must be running a RARP server program.


My physical address is A4:6E:A5:57:82:36. I am looking for my IP address.
Request
Host
RARP server
Your IP address is: 141.14.56.21
Reply
Host
RARP server

a. RARP request is broadcast

b. RARP reply is unicast

ICMP

- IP has two deficiencies: lack of error control and lack of assistance mechanisms. The IP protocol has no error-reporting or error-correcting mechanism.
    - What happens if something goes wrong?
    - What happens if a router must discard a datagram because it cannot find a router to the final destination,
    - or because the time-to-live field has a zero value?
    - What happens if the final destination host must discard all fragments of a datagram because it has not received all fragments within a predetermined time limit?

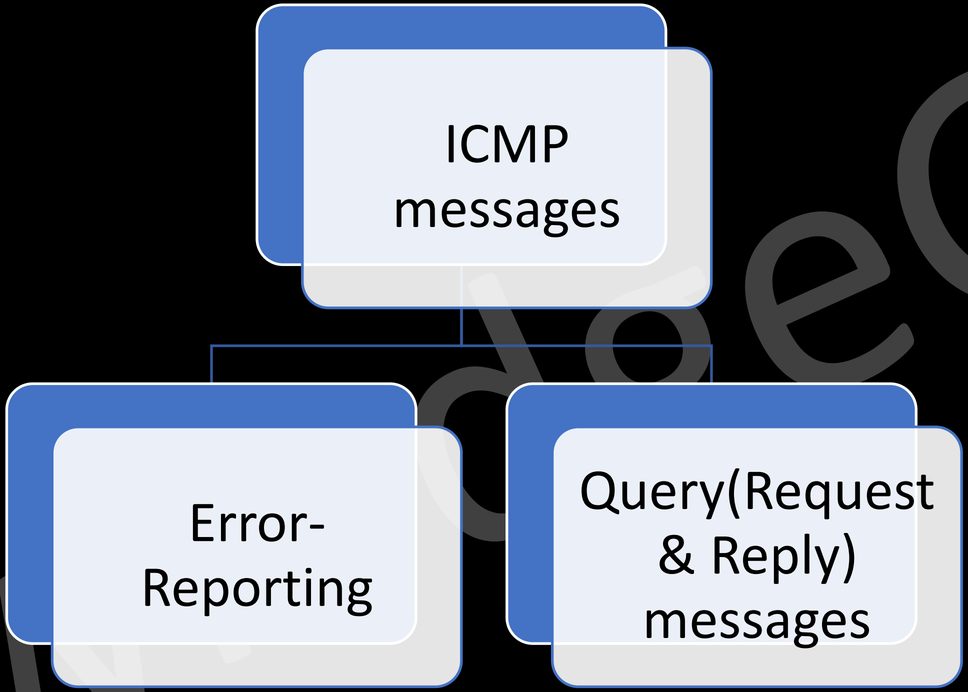
- These are examples of situations where an error has occurred and the IP protocol has no built-in mechanism to notify the original host. The IP protocol also lacks a mechanism for host and management queries. A host sometimes needs to determine if a router or another host is alive. And sometimes a network administrator needs information from another host or router.

- The Internet Control Message Protocol (ICMP) has been designed to compensate for the above two deficiencies. It is a companion to the IP protocol.

Types of Messages

- ICMP messages are divided into two broad categories: Error-Reporting messages and query(request & reply) messages.

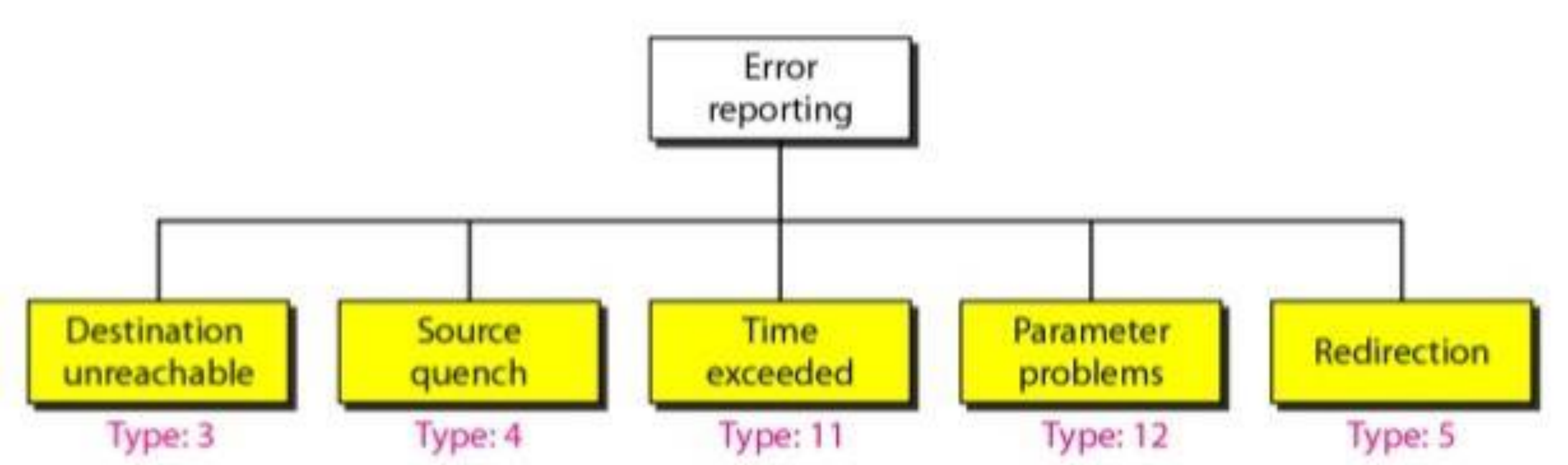
The error-reporting messages report problems that a router or a host (destination) may encounter when it processes an IP packet.



The query messages, which occur in pairs, help a host or a network manager get specific information from a router or another host.

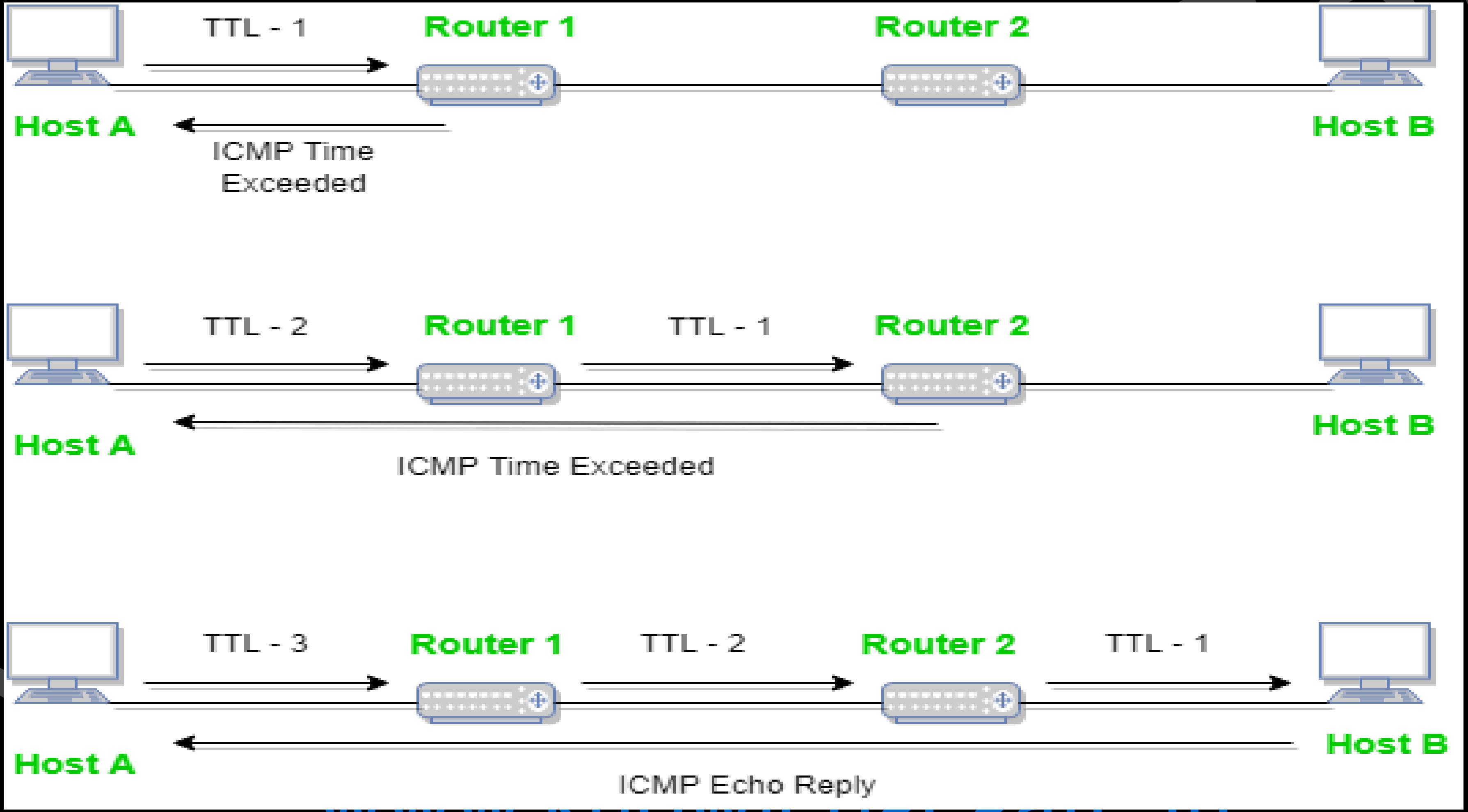
Error Reporting

- ICMP does not correct errors-it simply reports them. Error correction is left to the higher-level protocols. Error messages are always sent to the original source because the only information available in the datagram about the route is the source and destination IP addresses. ICMP uses the source IP address to send the error message to the source (originator) of the datagram.



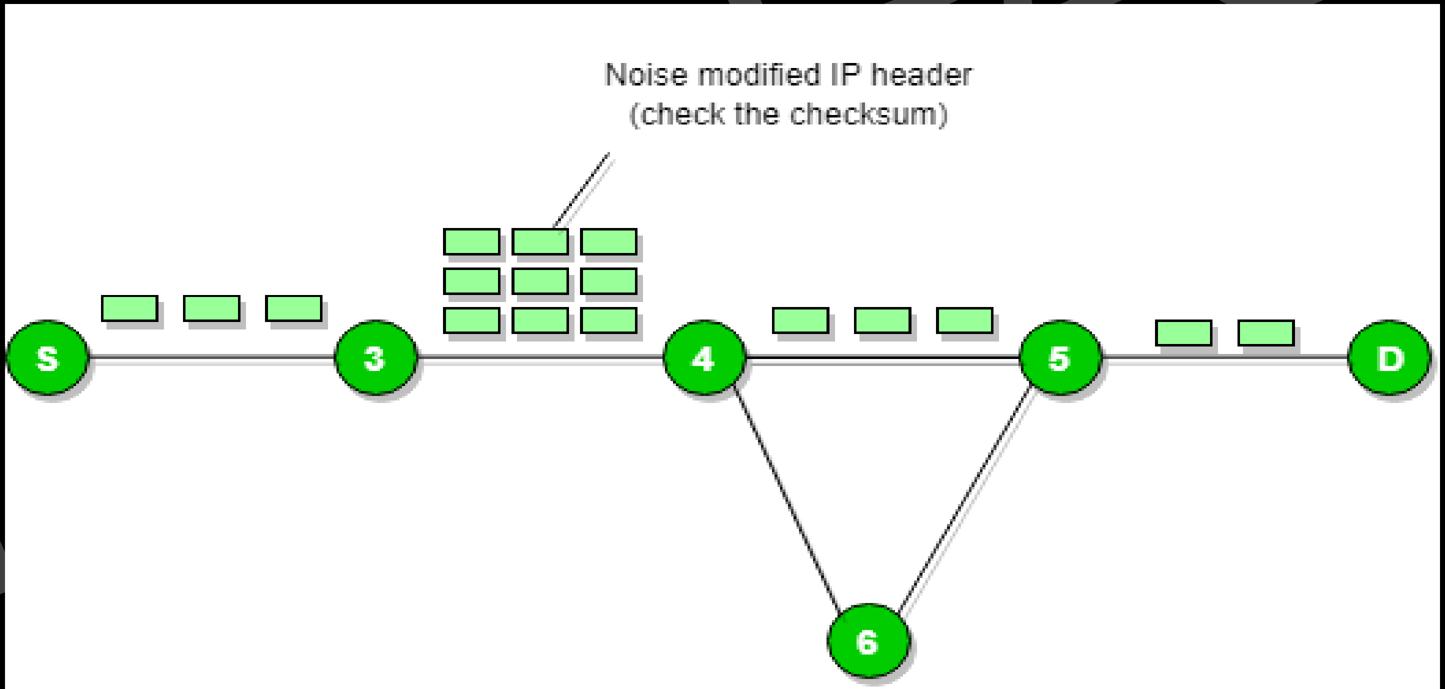
Time exceeded message

- ICMP will take source IP from discarded packet and informs to the source, of discarded datagram due to time to live field reaches to zero, by sending time exceeded message.



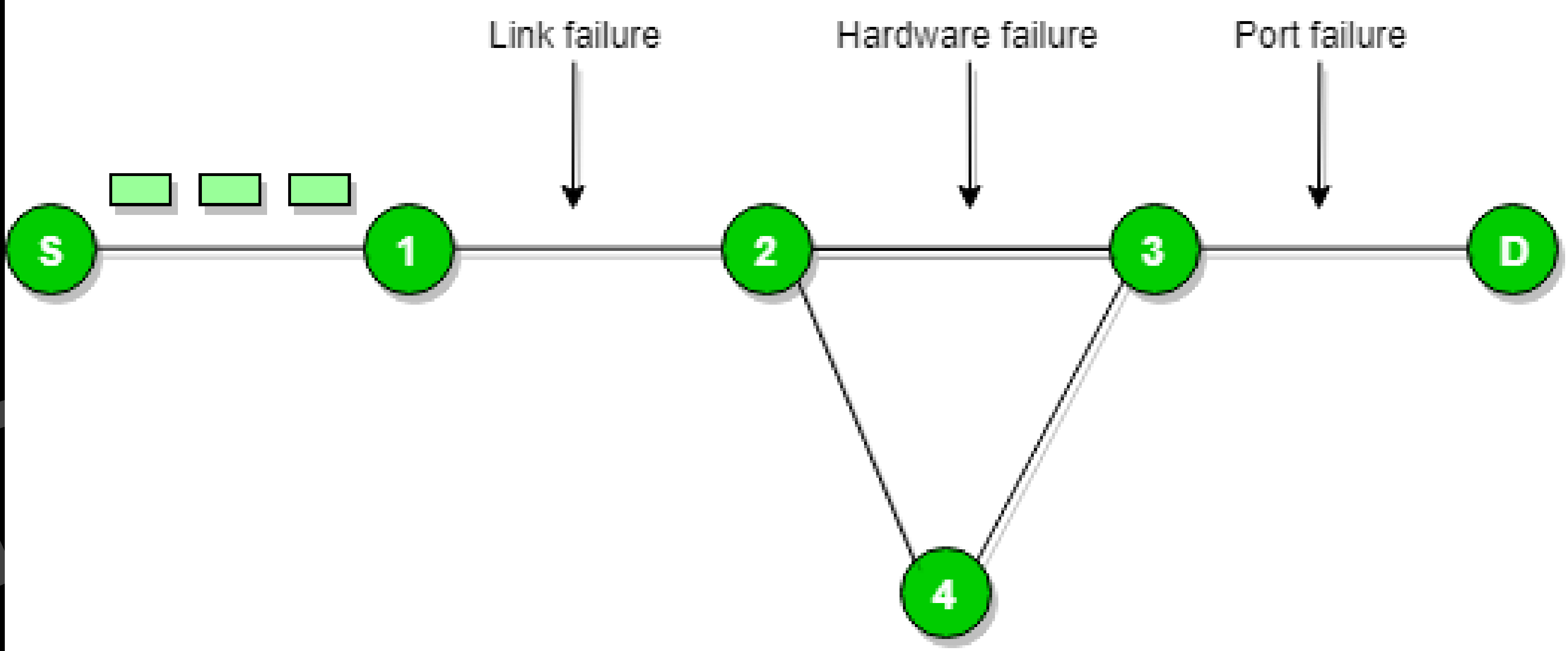
Parameter problem

- Whenever packets come to the router then calculated header checksum should be equal to received header checksum then only packet is accepted by the router.
- If there is mismatch packet will be dropped by the router. ICMP will take the source IP from the discarded packet and informs to source by sending parameter problem message.



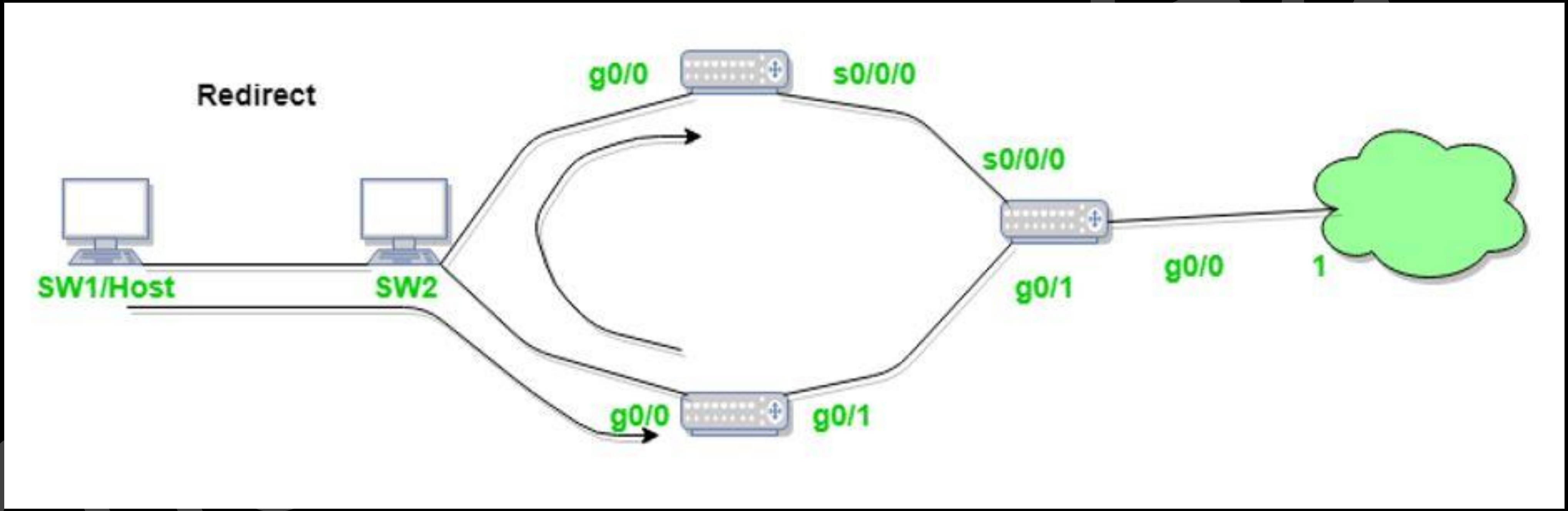
Destination Un-reachable

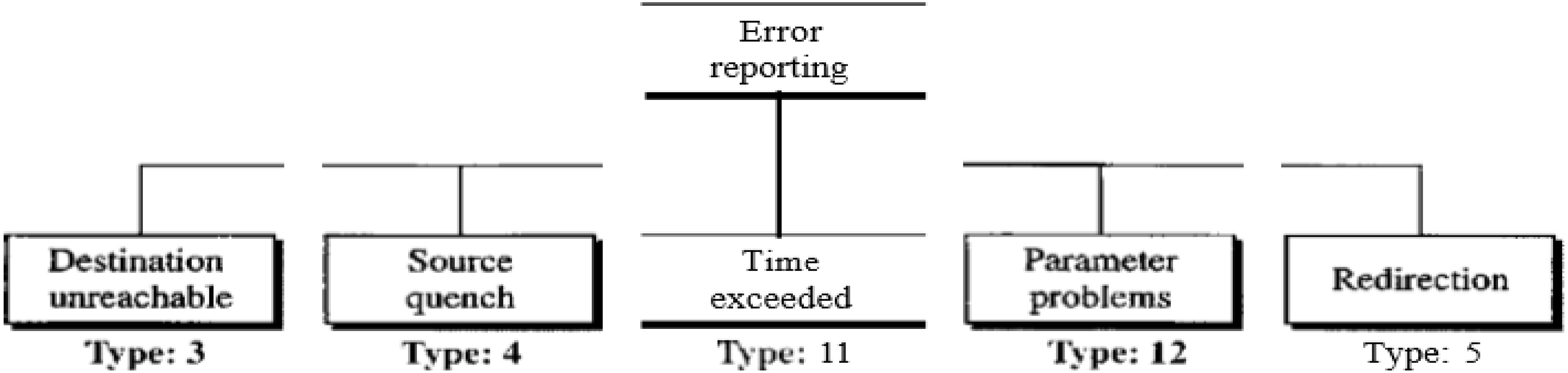
- Destination unreachable is generated by the host or its inbound gateway to inform the client that the destination is unreachable for some reason.
- There is no necessary condition that only router give the ICMP error message some time destination host send ICMP error message when any type of failure (link failure, hardware failure, port failure etc.) happen in the network.



Redirection message

- Redirect requests data packets be sent on an alternate route. The message informs to a host to update its routing information (to send packets on an alternate route).





The following are important points about ICMP error messages:

O No ICMP error message will be generated in response to a datagram carrying an ICMP error message.

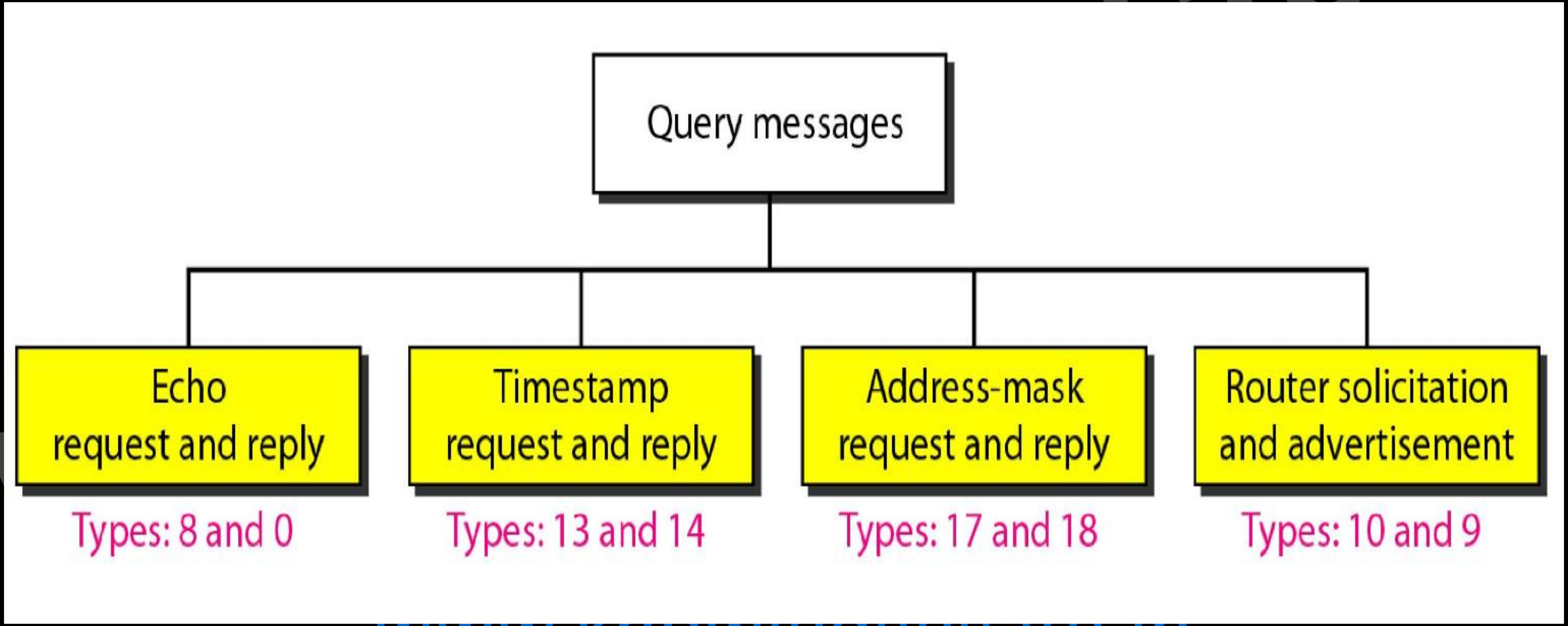
D No ICMP error message will be generated for a fragmented datagram that is not the first fragment.

D No IeMP error message will be generated for a datagram having a multicast address.

D No ICMP error message will be generated for a datagram having a special address such as 127.0.0.0 or 0.0.0.0.

Query

- In addition to error reporting, ICMP can diagnose some network problems. This is accomplished through the query messages, a group of four different pairs of messages.
- In this type of ICMP message, a node sends a message that is answered in a specific format by the destination node. A query message is encapsulated in an IP packet, which in turn is encapsulated in a data link layer frame.



Echo Request and Reply

- Echo-request and echo-reply messages, encapsulated within IP datagrams, are essential diagnostic tools enabling network managers and users to pinpoint network issues and confirm that IP protocols in sender and receiver systems are in sync.
- Modern systems offer an advanced version of the ping command, capable of generating a series of these messages, facilitating comprehensive network analysis through the collection of vital statistical data.

Router Solicitation and Advertisement

- As we discussed in the redirection message section, a host that wants to send data to a host on another network needs to know the address of routers connected to its own network. Also, the host must know if the routers are alive and functioning. The router-solicitation and router-advertisement messages can help in this situation.
- A host can broadcast (or multicast) a router-solicitation message. The router or routers that receive the solicitation message broadcast their routing information using the router-advertisement message.
- A router can also periodically send router-advertisement messages even if no host has solicited. Note that when a router sends out an advertisement, it announces not only its own presence but also the presence of all routers on the network of which it is aware.

Address-Mask Request and Reply

- A host may know its IP address, but it may not know the corresponding mask. For example, a host may know its IP address as 159.31.17.24, but it may not know that the corresponding mask is /24.
- To obtain its mask, a host sends an address-mask-request message to a router on the LAN. If the host knows the address of the router, it sends the request directly to the router. If it does not know, it broadcasts the message.
- The router receiving the address-mask-request message responds with an address-mask-reply message, providing the necessary mask for the host. This can be applied to its full IP address to get its subnet address.

Timestamp Request and Reply

- Two machines (hosts or routers) can use the timestamp request and timestamp reply messages to determine the round-trip time needed for an IP datagram to travel between them. It can also be used to synchronize the clocks in two machines.

IGMP

- The IP protocol can be involved in two types of communication: unicasting and multicasting. Unicasting is the communication between one sender and one receiver. It is a one-to-one communication.

- However, some processes sometimes need to send the same message to a large number of receivers simultaneously. This is called multicasting, which is a one-to-many communication.

- Multicasting has many applications. For example, multiple stockbrokers can simultaneously be informed of changes in a stock price, or travel agents can be informed of a plane cancellation.

Video-on-Demand

Distance Learning

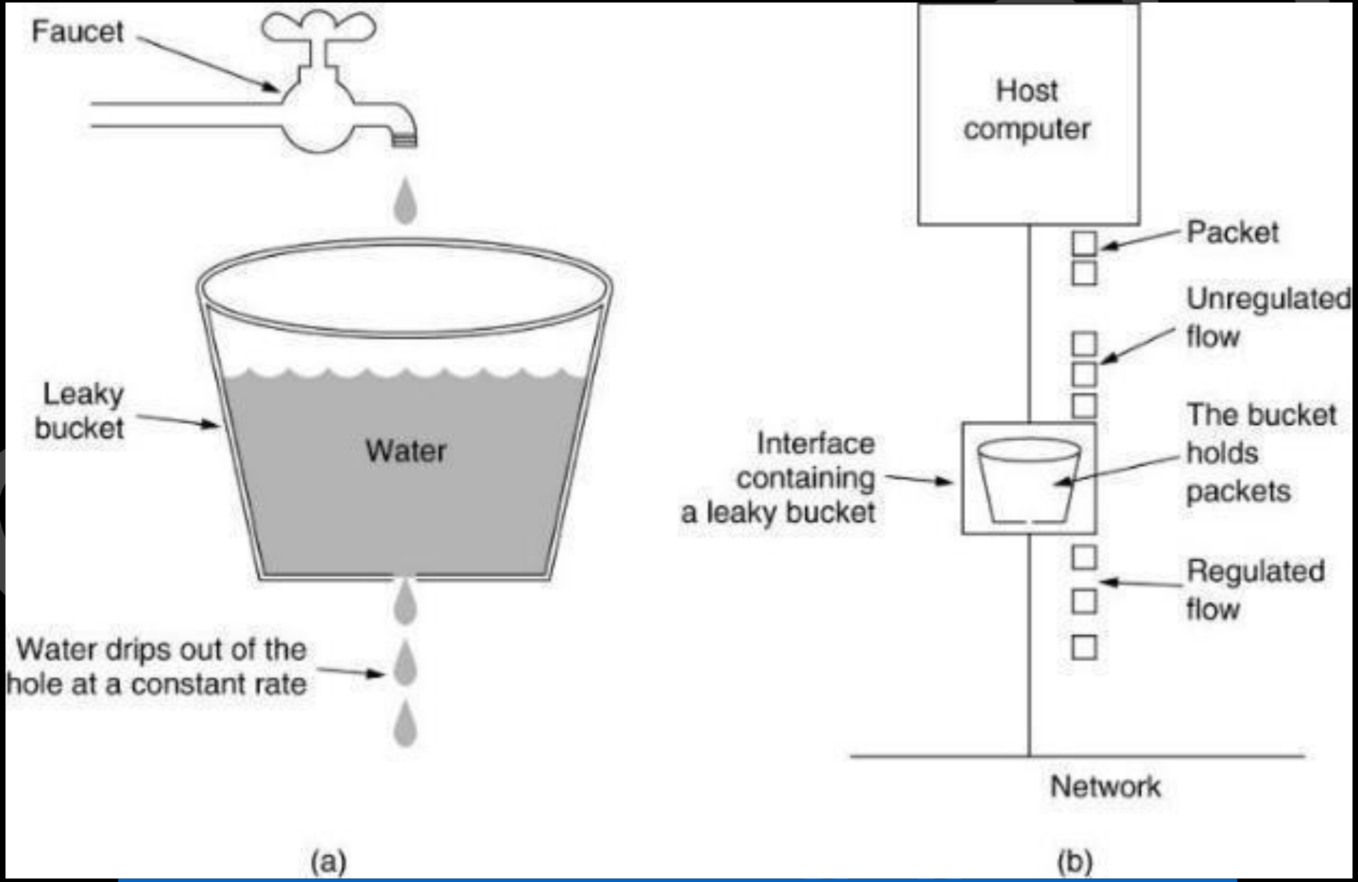
Congestion

- Congestion is a situation which may occur if users send data into the network at a rate greater than that allowed by network resources.
- **Congestion control** : Congestion control refers to techniques and mechanisms that can either prevent congestion, before it happens, or remove congestion, after it has happened. Techniques to prevent congestion :
- **Open-loop congestion control** : In open-loop congestion control, policies are applied to prevent congestion before it happens. In these mechanisms, congestion control is handled by either the source or the destination. Following are the policies that can prevent congestion :
  - i. **Retransmission policy** : The retransmission policy is designed to optimize efficiency and at the same time prevent congestion.
  - ii. **Window policy** : The type of window at the sender may also affect congestion. The selective repeat window is better than the Go-Back-N window for congestion control.
  - iii. **Acknowledgement policy** : The acknowledgement policy imposed by the receiver may also affect congestion. If the receiver does not acknowledge every packet it receives, it may slow down the sender and help to prevent congestion.

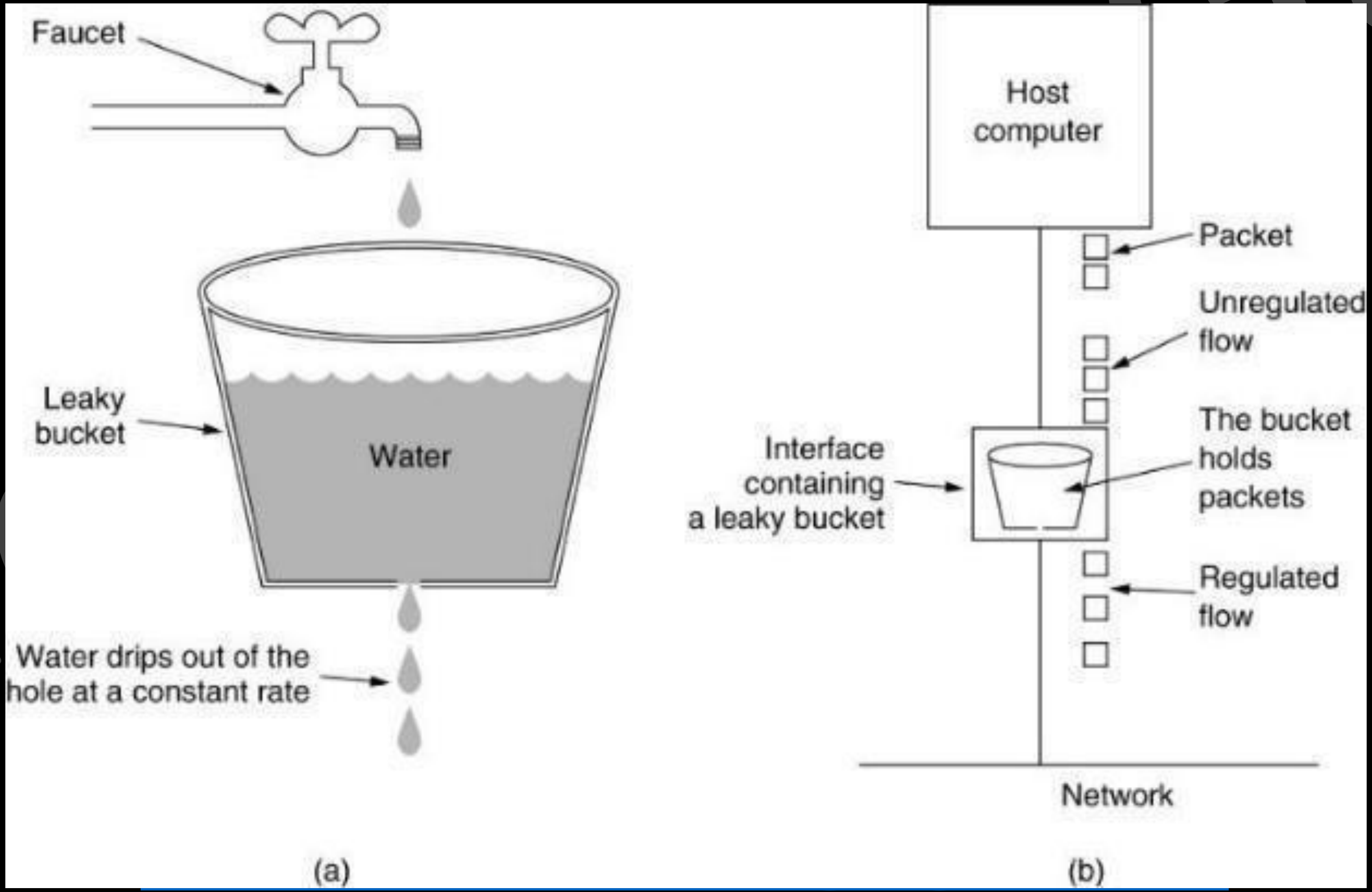
- Closed-loop congestion control : Closed-loop congestion control mechanisms try to reduce congestion after it happens. Several mechanisms have been used by different protocols which are as follows :
  - i. **Backpressure** : The technique of backpressure refers to mechanism in which a congested node stops congestion control m)receiving data from the immediate upstream node or nodes.
  - ii. **Choke packet** : A choke packet is a packet sent by a node to the source to inform about congestion. In the choke packet method ,the warning is from the router, which has encountered congestion to the source station directly.
  - iii. **Implicit signaling** : In implicit signaling, there is no communication between the congested node or nodes and the source.
  - iv. **Explicit signaling** : The node that experiences congestion can explicitly send a signal to the source or destination.

Leaky bucket algorithm

- If a bucket has a small hole at the bottom, the water leaks from the bucket at a constant rate as long as there is water in the bucket. The rate at which the water leaks does not depend on the rate at which the water is input to the bucket unless the bucket is empty. The input rate can vary, but the output rate remains constant.
- Similarly, in networking, a technique called leaky bucket which can smooth out bursty traffic. A simple leaky bucket implementation a FIFO queue holds the packets. If the traffic consists of fixed size packets the process removes a fixed number of packets from the queue at each tick of the clock. If the traffic consists of variable length packets, the fixed output rate must be based on the number of bytes or bits.



- The following is an algorithm for variable length packets:
  - Initialize a counter to n at the tick of the clock.
  - If n is greater then the size of the packet, send the packet and decrement the counter by the packet size. Repeat this step until n is smaller than the packet size.
  - Reset the counter and go to step(i).



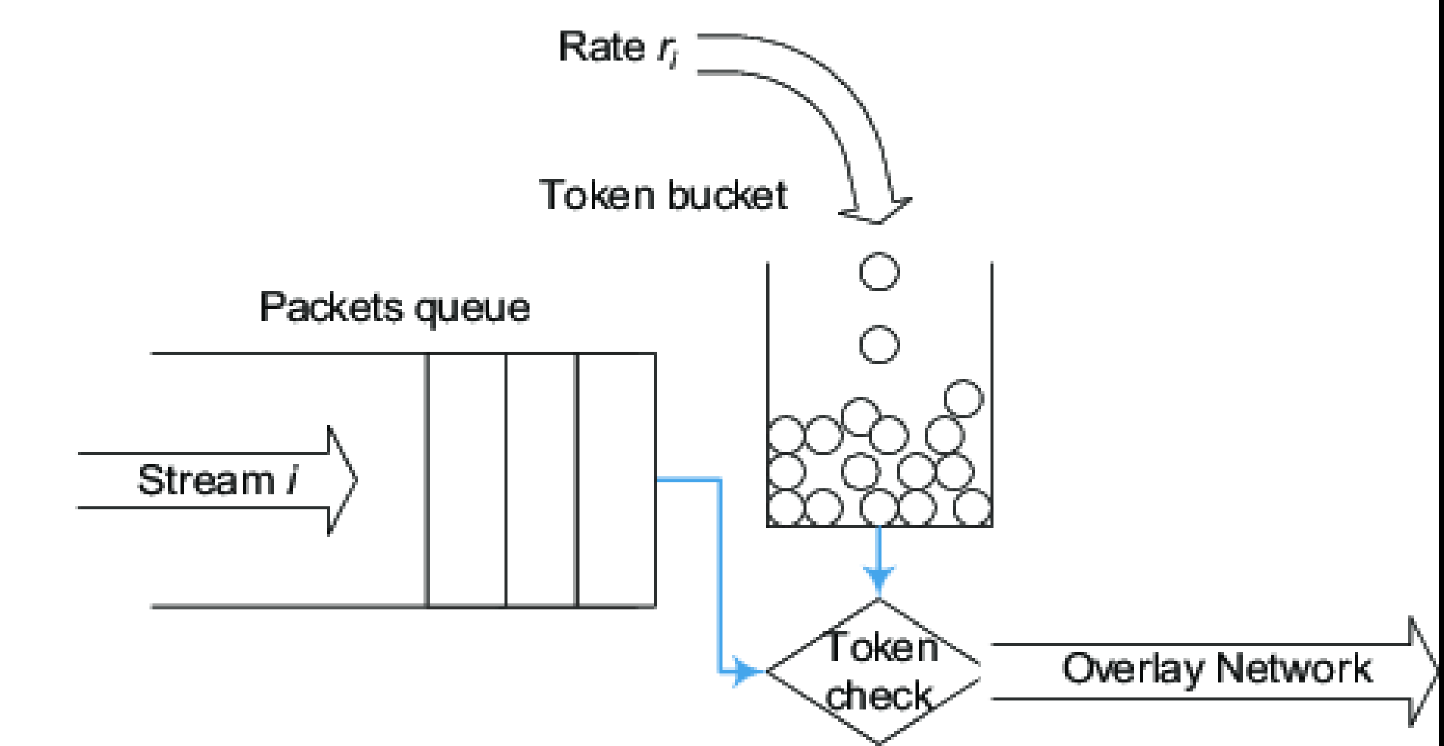
Token Bucket Algorithm:

1. **Concept**: It is another algorithm used to control data rate in networks.
2. **Working**: Tokens are added to the bucket at a fixed rate. Data packets can be transmitted if sufficient tokens are available.
3. **Solution**: It allows data to be sent at varying speeds, permitting bursts of data until the bucket is empty of tokens.

Advantage: Offers more flexibility than the leaky bucket as it accommodates bursts of high-speed data without data loss.

How Token Bucket Solves the Problem of Leaky Bucket:

1. **Flexibility**: It allows for bursts of data, adapting better to varying network speeds.
2. **Prevents Data Loss**: Data is not discarded suddenly as in the leaky bucket algorithm, reducing the chances of data loss.
3. **Better Utilization of Bandwidth**: By allowing data bursts, it utilizes available bandwidth more efficiently.



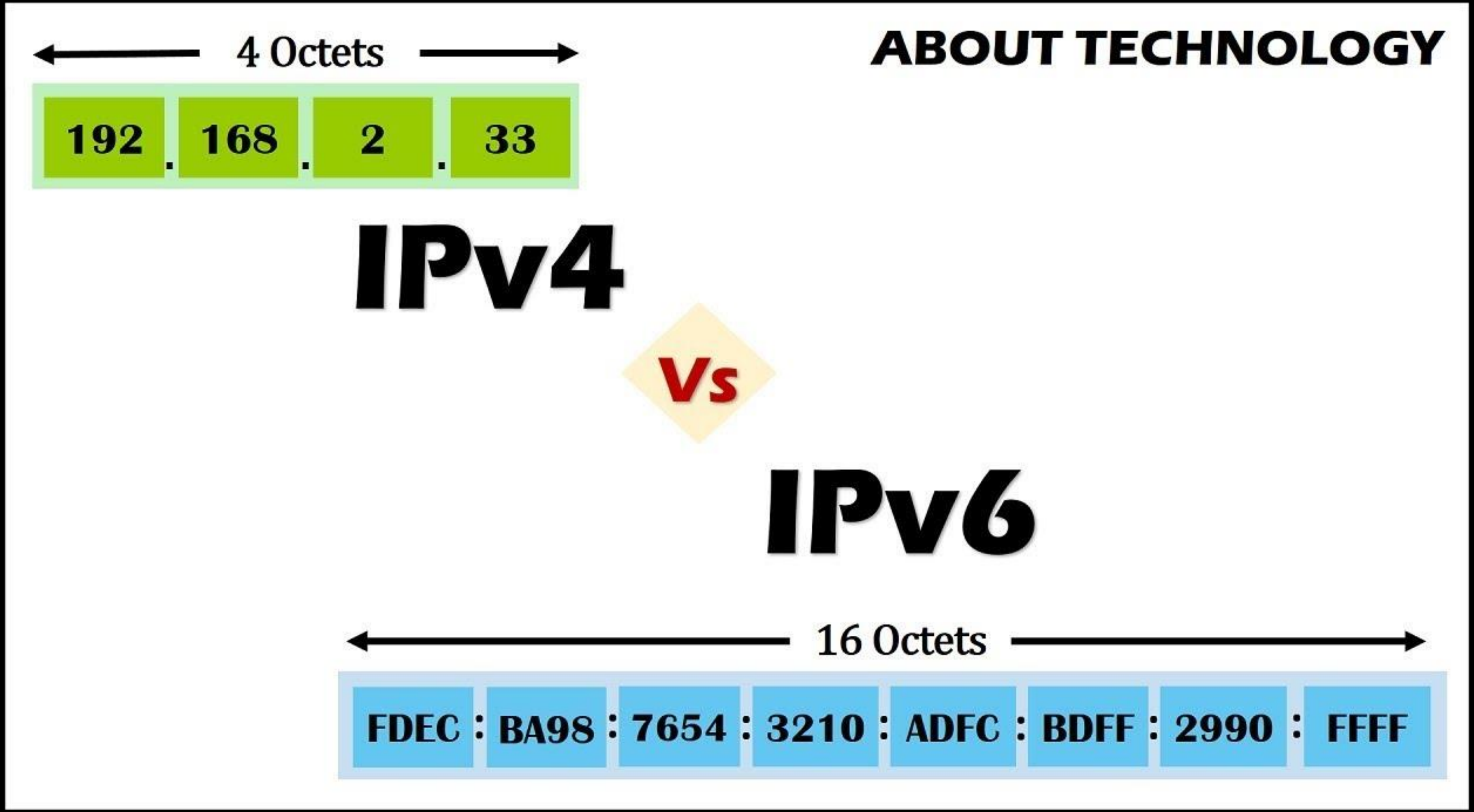
IPV4 ADDRESSES

- The Internet Protocol addresses are 32 bits in length; this gives us a maximum of 2^{32} addresses. These addresses are referred to as IPv4.

- This means that, theoretically, if there were no restrictions, more than 4 billion (4,29,49,67,296) devices could be connected to the Internet. The actual number is much less because of the restrictions imposed on the addresses.

- **World population** is often used to refer to the total number of humans currently living, and was estimated to have exceeded 8.0 billion as of Sept 2023

- The need for more addresses, in addition to other concerns about the IP layer, motivated a new design of the IP layer called the new generation of IP or IPv6 (IP version 6). In this version, the Internet uses 128-bit addresses that give much greater flexibility in address allocation (3.4 $*10^{38}$). These addresses are referred to as IPv6 (IP version 6) addresses.



Unique and Universal

- An IP address is uniquely and universally defining the connection of a host or a router to the Internet.

- They are unique in the sense that each address defines one, and only one, connection to the Internet. Two devices on the Internet can never have the same address at the same time.

- The IPv4 addresses are universal in the sense that the addressing system must be accepted by any host that wants to be connected to the Internet.

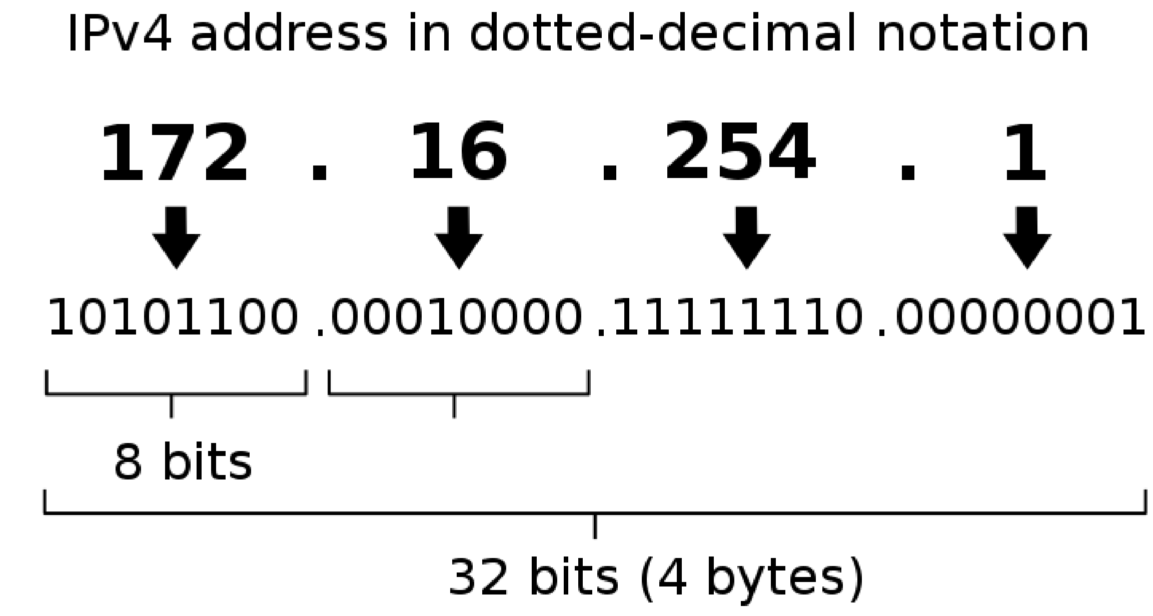
- The IP address is the address of the connection, not the host or the router, because if the device is moved to another network, the IP address may be changed.

Notations

- There are two prevalent notations to show an IPv4 address: binary notation and dotted decimal notation.

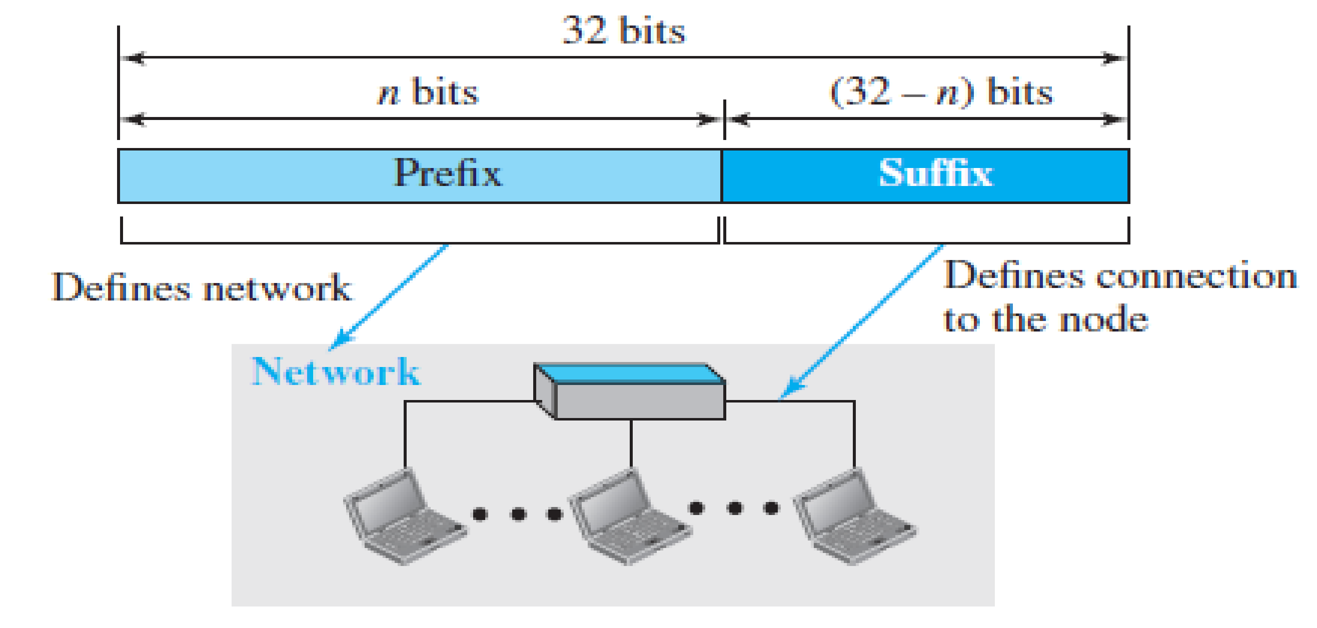
- **Binary Notation** - In binary notation, the IPv4 address is displayed as 32 bits. Each octet is often referred to as a byte. So, it is common to hear an IPv4 address referred to as a 32-bit address or a 4-byte address. An example of an IPv4 address in binary notation: **01110101 10010101 00011101 00000010**

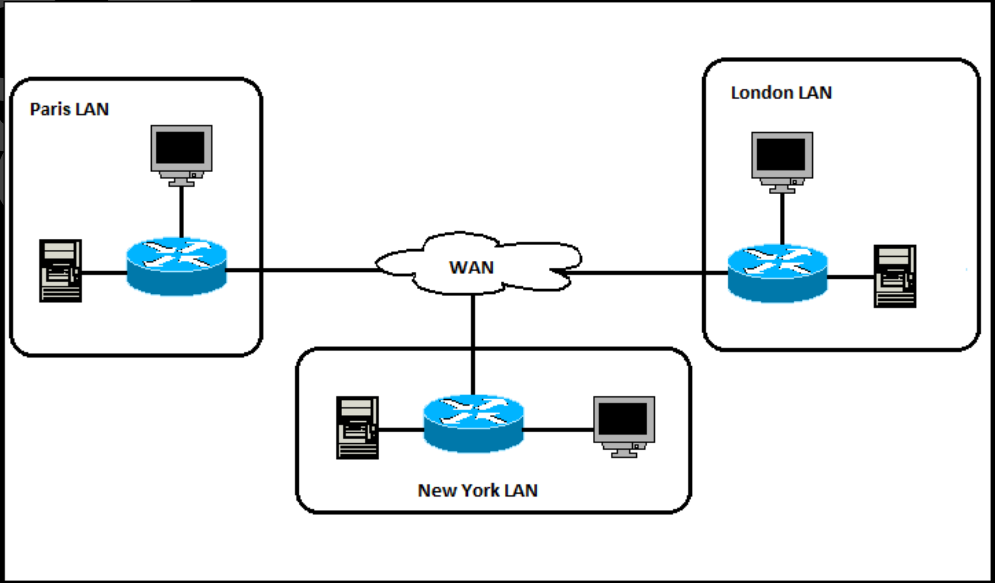
- **Dotted-Decimal Notation** - To make the IPv4 address more compact and easier to read, Internet addresses are usually written in decimal form with a decimal point (dot) separating the bytes. The following is the dotted decimal notation of the above address: **117.149.29.2**



Classful Addressing

- IPv4 addressing, at its inception, used the concept of classes. This architecture is called classful addressing.
- A 32-bit IPv4 address is hierarchical and divided only into two parts:
- The first part of the address, called the *prefix*, defines the network (NetworkID).
- The second part of the address, called the *suffix*, defines the node (connection of a device to the Internet (HostID)).





- IPv4 was first designed as a fixed-length prefix and is referred to as classful addressing
- In classful addressing, the address space is divided into five classes: A, B, C, D, and E. Each class occupies some part of the address space.
- To accommodate both small and large networks, three fixed-length prefixes were designed (*n* = 8, *n* = 16, and *n* = 24).

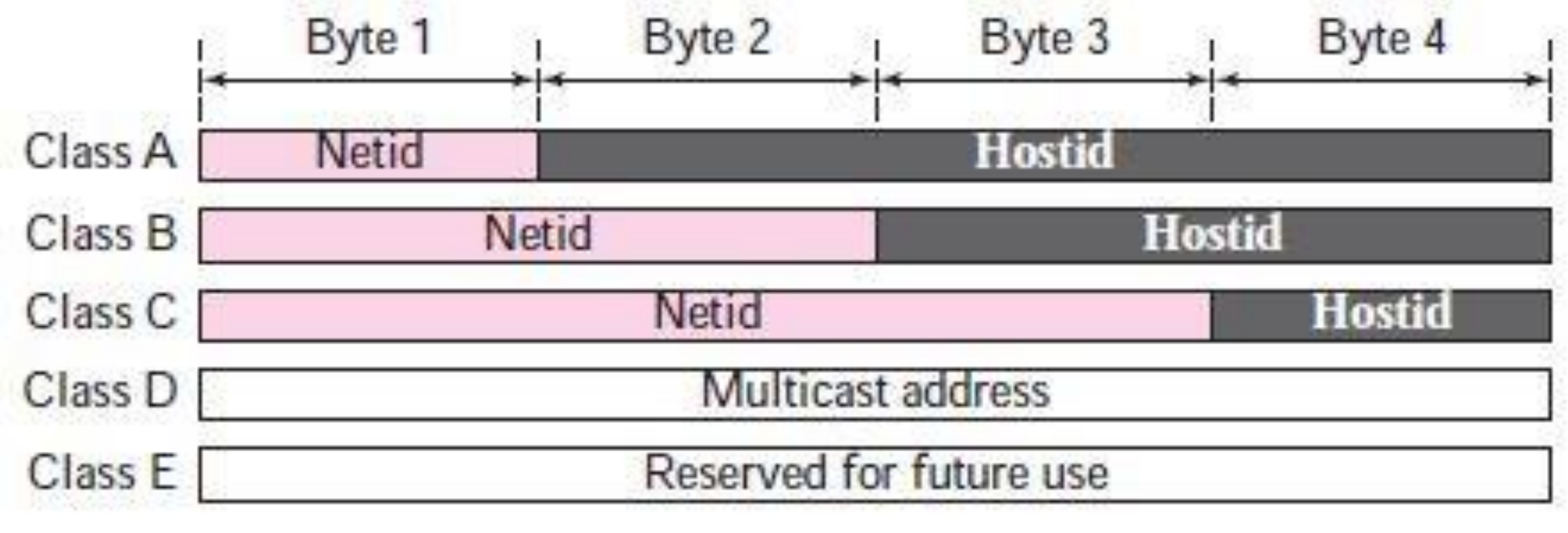
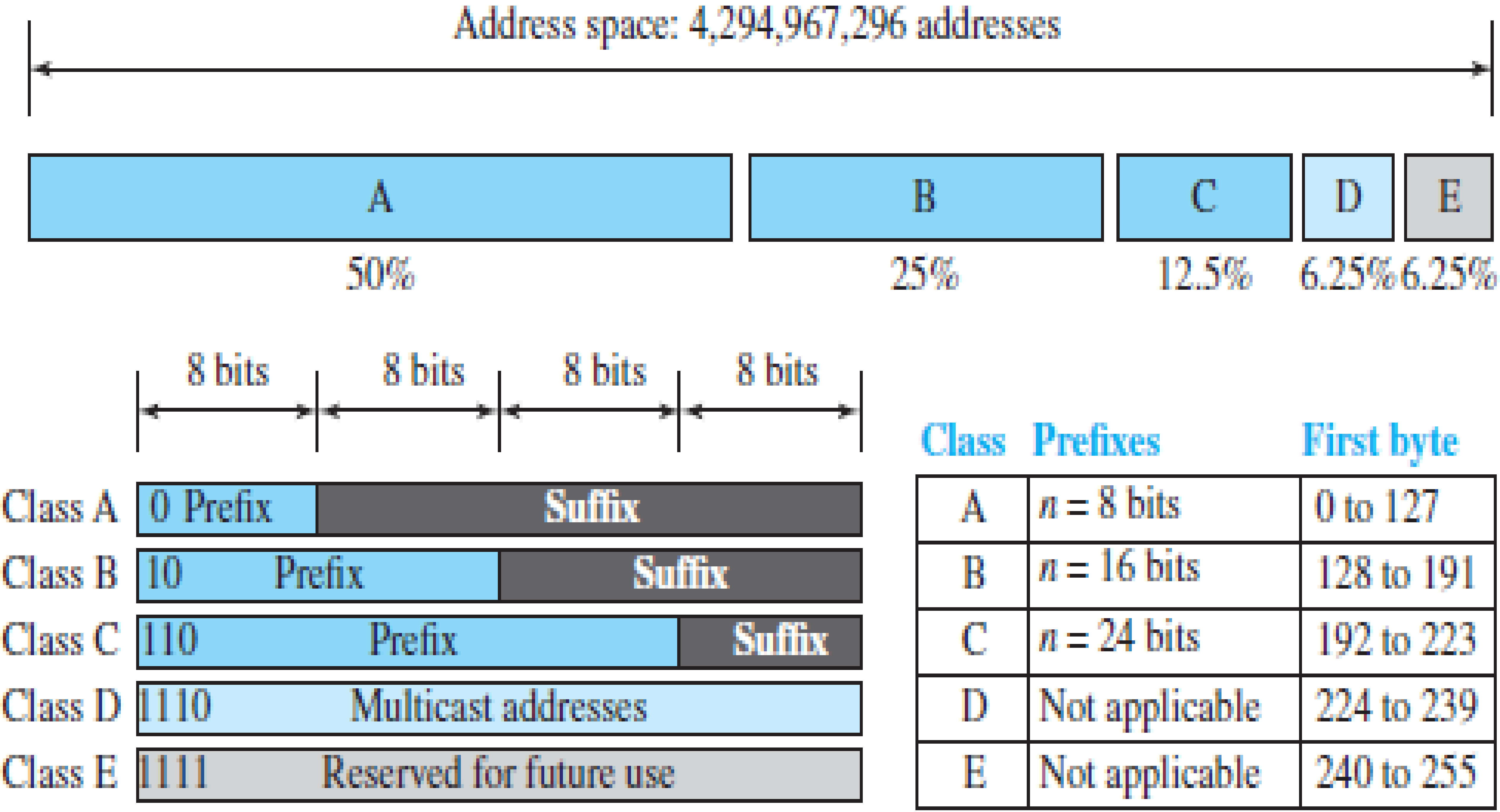


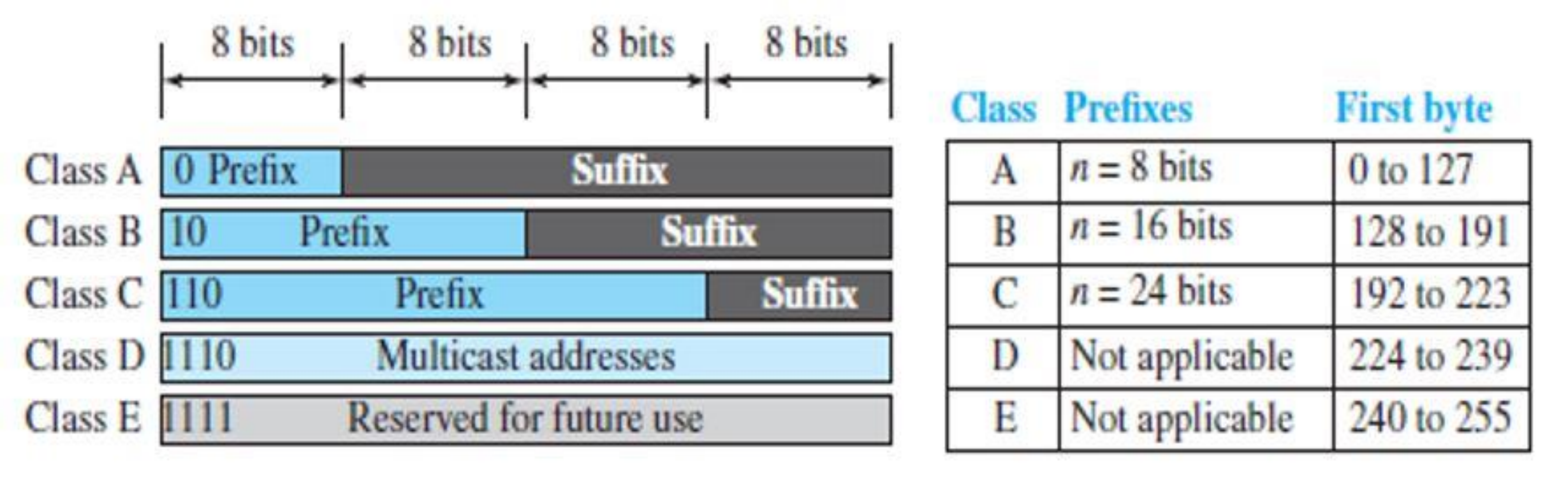
Fig1: Netid and hostid



Class	Prefixes	First byte
A	n = 8 bits	0 to 127
B	n = 16 bits	128 to 191
C	n = 24 bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

Class A

- In Class A NetID = 8 bits and HostID = 24.
- How to identify class A address
  - First bit is reserved to 0 in binary notation
  - Range of 1st octet is [0, 127] in dotted decimal notation



Class	Prefixes	First byte
A	n = 8 bits	0 to 127
B	n = 16 bits	128 to 191
C	n = 24 bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

- Total number of connections in class A is 2^{31} (2,14,74,83,648)

- There are 2^7 -2 = 126 networks in Class A network.
  - In Class A, total network available are 2 less, because:
  - IP Address 0.0.0.0 is reserved for broadcasting requirements
  - IP Address 127.0.0.1 is reserved for loopback address / self-connectivity.

- The range of 1st octet is [0, 127] but since two addresses are reserved it is: [1, 126].

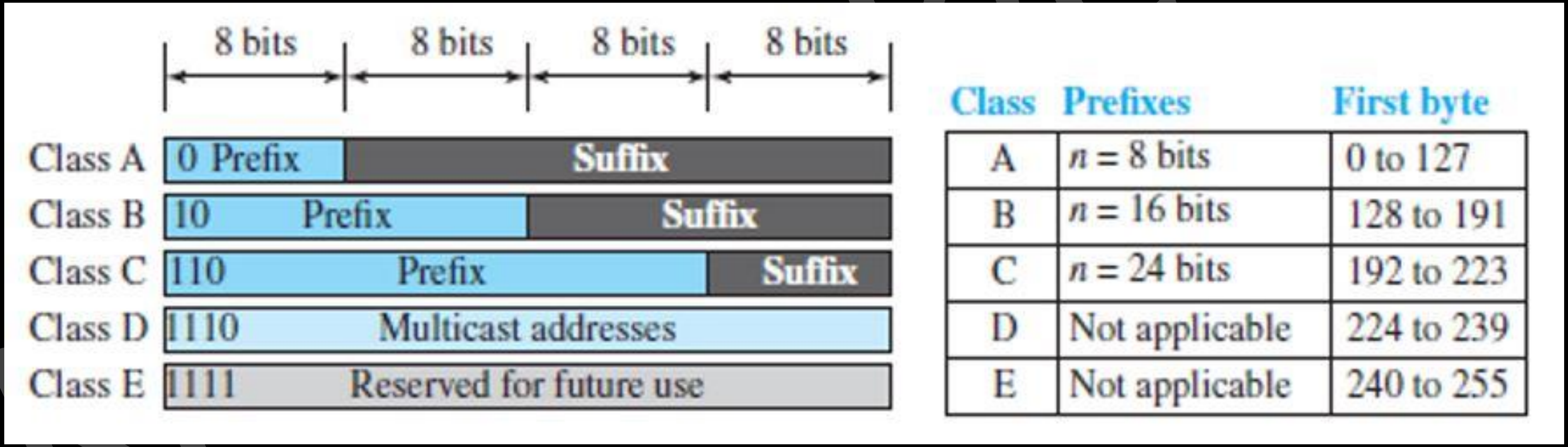
- There are $2^{24} – 2$ (1,67,77,214) HostID in Class A.

  - In all the classes, total number of hosts that can be configured are 2 less because:
  - This is to account for the two reserved IP addresses in which all the bits for host ID are either zero or one.
  - When all Host ID bits are 0, it represents the Network ID for the network.
  - When all Host ID bits are 1, it represents the Broadcast Address.

- Class A is used by organizations requiring very large size networks like Indian Railways.

Class B

- In Class B NetID = 16 bits and HostID = 16.
- How to identify class B address
  - First two bits are reserved to 10 in binary notation
  - Range of 1st octet is [128, 191] in dotted decimal notation

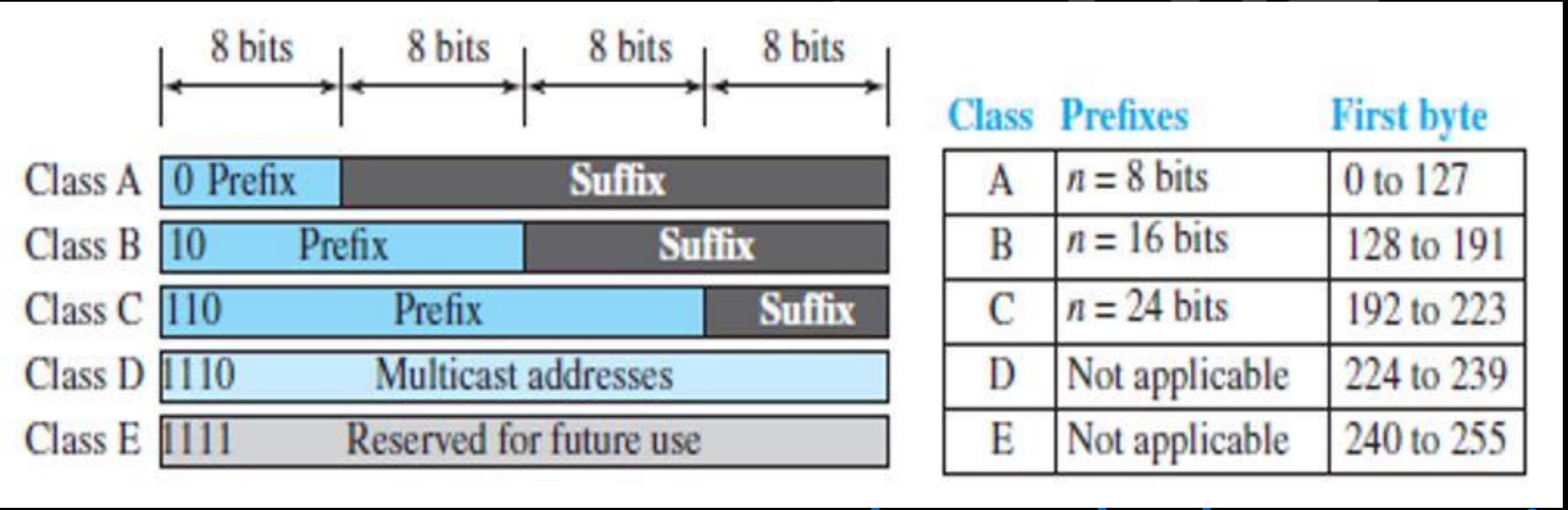


Class	Prefixes	First byte
A	n = 8 bits	0 to 127
B	n = 16 bits	128 to 191
C	n = 24 bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

- Total number of connections in class B is 2^{30} (1,07,37,41,824)
- Total number of networks available in class B is 2^{14} (16,384)
- Total number of hosts that can be configured in every network in class B is $2^{16} – 2$ (65,534)
- Class B is used by organizations requiring medium size networks

Class C

- In Class C NetID = 24 bits and HostID = 8.
- How to identify class C address
  - First three bits are reserved to 110 in binary notation
  - Range of 1st octet is [192, 223] in dotted decimal notation

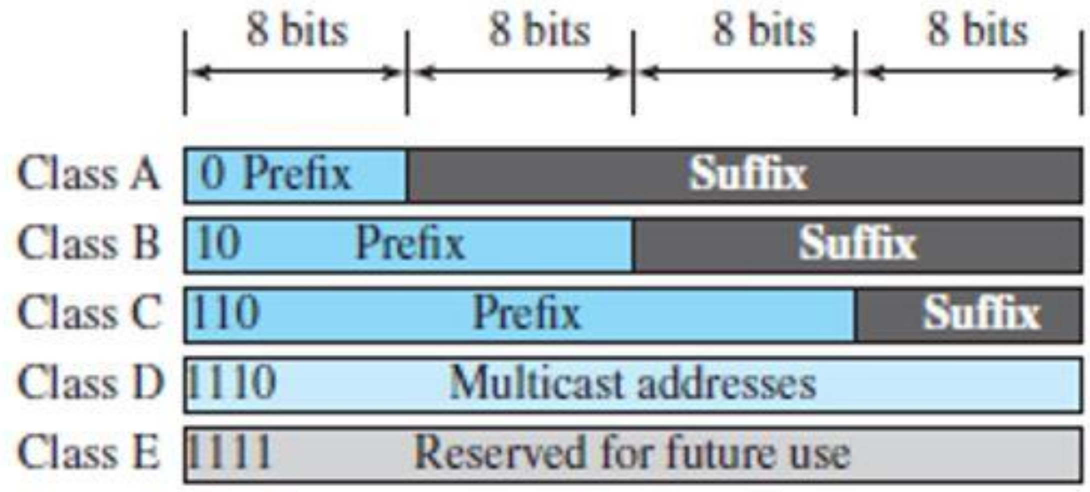


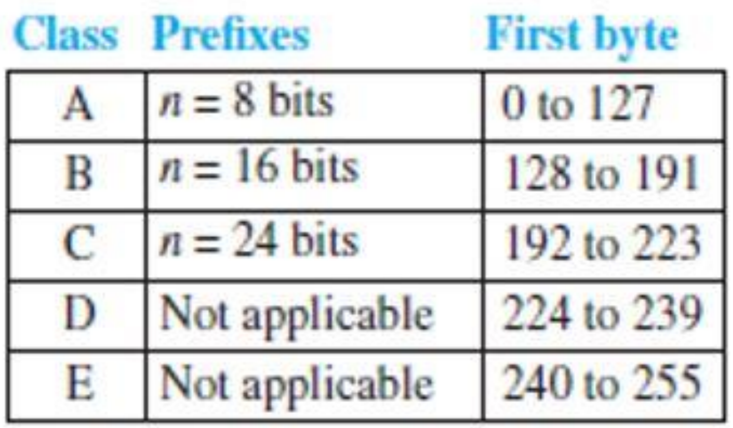
Class	Prefixes	First byte
A	$n = 8$ bits	0 to 127
B	$n = 16$ bits	128 to 191
C	$n = 24$ bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

- Total number of connections in class C is 2^{29} (53,68,70,912)
- Total number of networks available in class C is 2^{21} (20,97,152)
- Total number of hosts that can be configured in every network in class C is $2^{8} – 2$ (254)
- Class C is used by organizations requiring small to medium size networks.

Class D

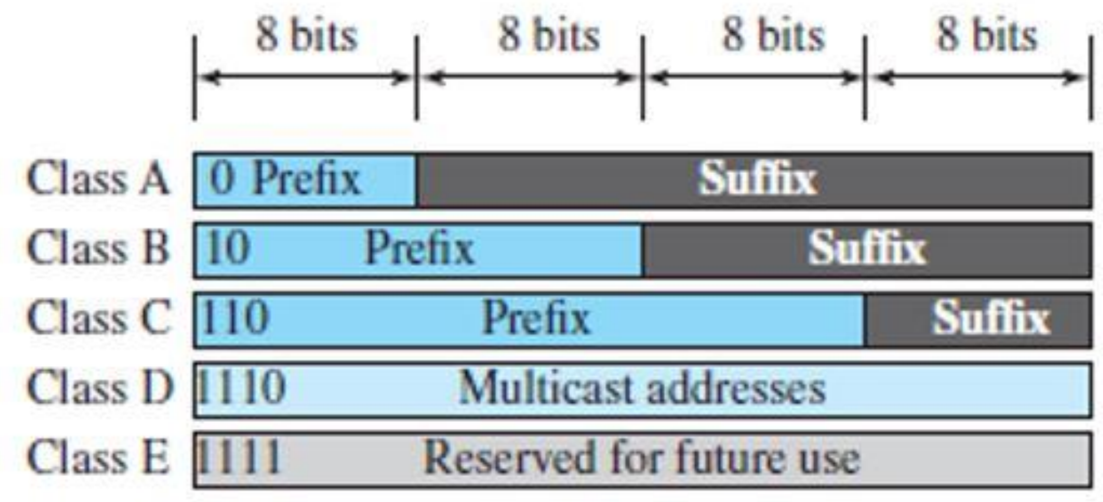
- Class D is not divided into Network ID and Host ID.
- How to identify class D address
  - First four bits are reserved to 1110 in binary notation
  - Range of 1st octet is [224, 239] in dotted decimal notation





Class	Prefixes	First byte
A	$n = 8$ bits	0 to 127
B	$n = 16$ bits	128 to 191
C	$n = 24$ bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

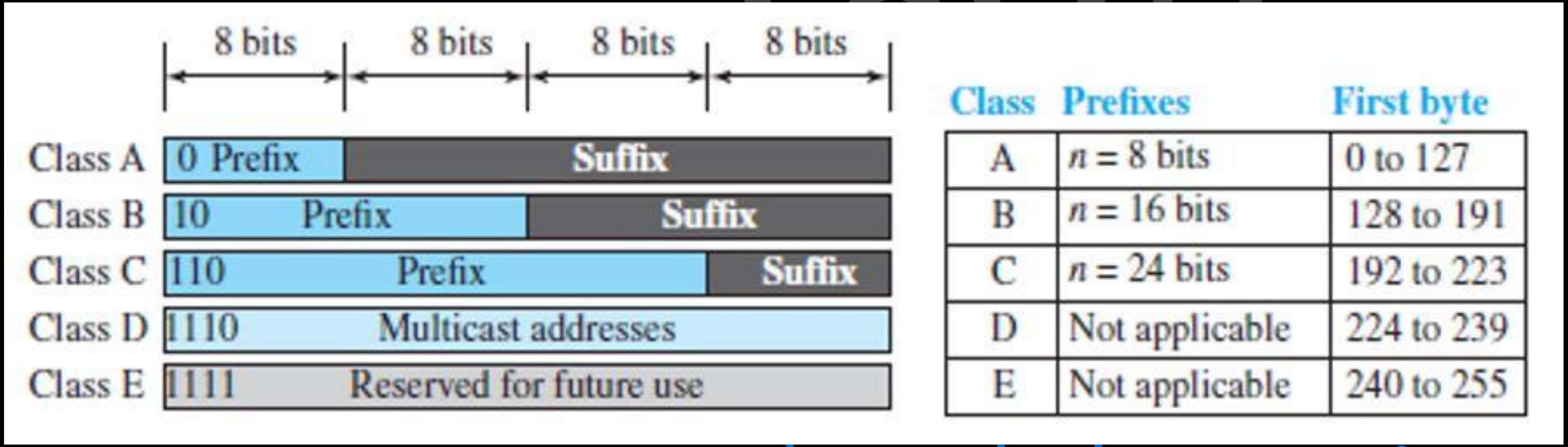
- Total number of IP Addresses available in class D = 2^{28} (26,84,35,456)
- Class D is reserved for multicasting, in multicasting, there is no need to extract host address from the IP Address, this is because data is not destined for a particular host.



Class	Prefixes	First byte
A	$n = 8$ bits	0 to 127
B	$n = 16$ bits	128 to 191
C	$n = 24$ bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

Class E

- Class E is not divided into Network ID and Host ID.
- How to identify class E address
  - First four bits are reserved to 1111 in binary notation
  - Range of 1st octet is [240, 255] in dotted decimal notation



Class	Prefixes	First byte
A	$n = 8$ bits	0 to 127
B	$n = 16$ bits	128 to 191
C	$n = 24$ bits	192 to 223
D	Not applicable	224 to 239
E	Not applicable	240 to 255

- Total number of IP Addresses available in class E = 2^{28} (26,84,35,456)
- Class E is reserved for future or experimental purposes.

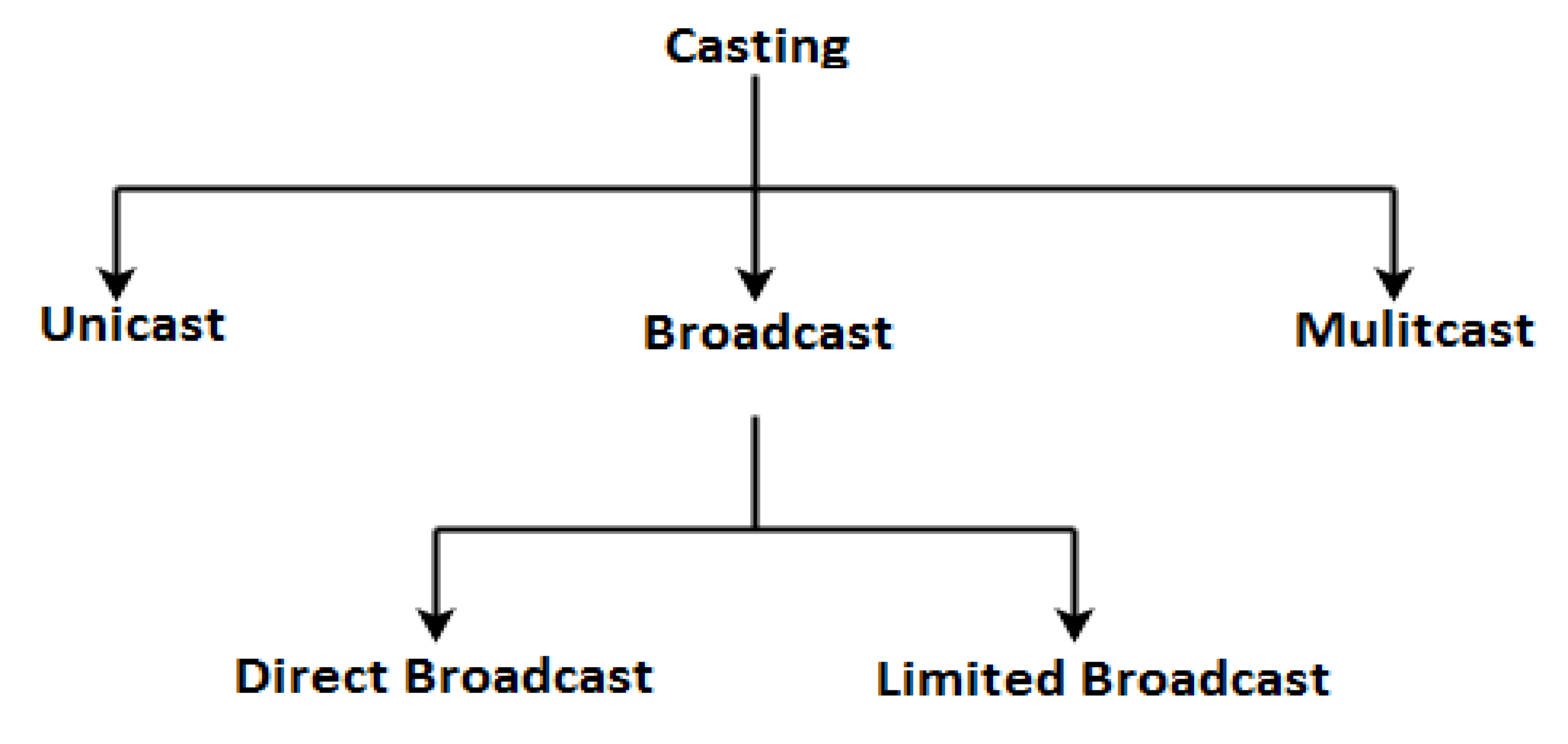
Points to note

- All the hosts in a single network always have the same network ID but different Host ID.
- Two hosts in two different networks can have the same host ID.
- Only those devices which have the network layer will have IP Address, switches, hubs and repeaters does not have any IP Address.

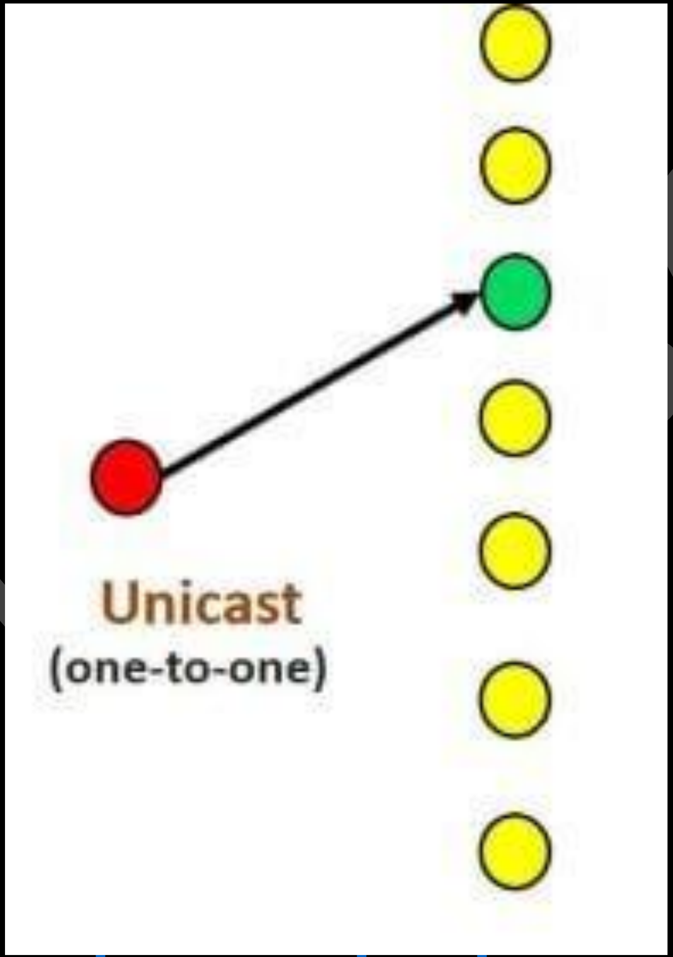
Casting in Networks

Types of Casting

- Casting in a network is basically of three type: Unicast, Multicast and Broadcast.

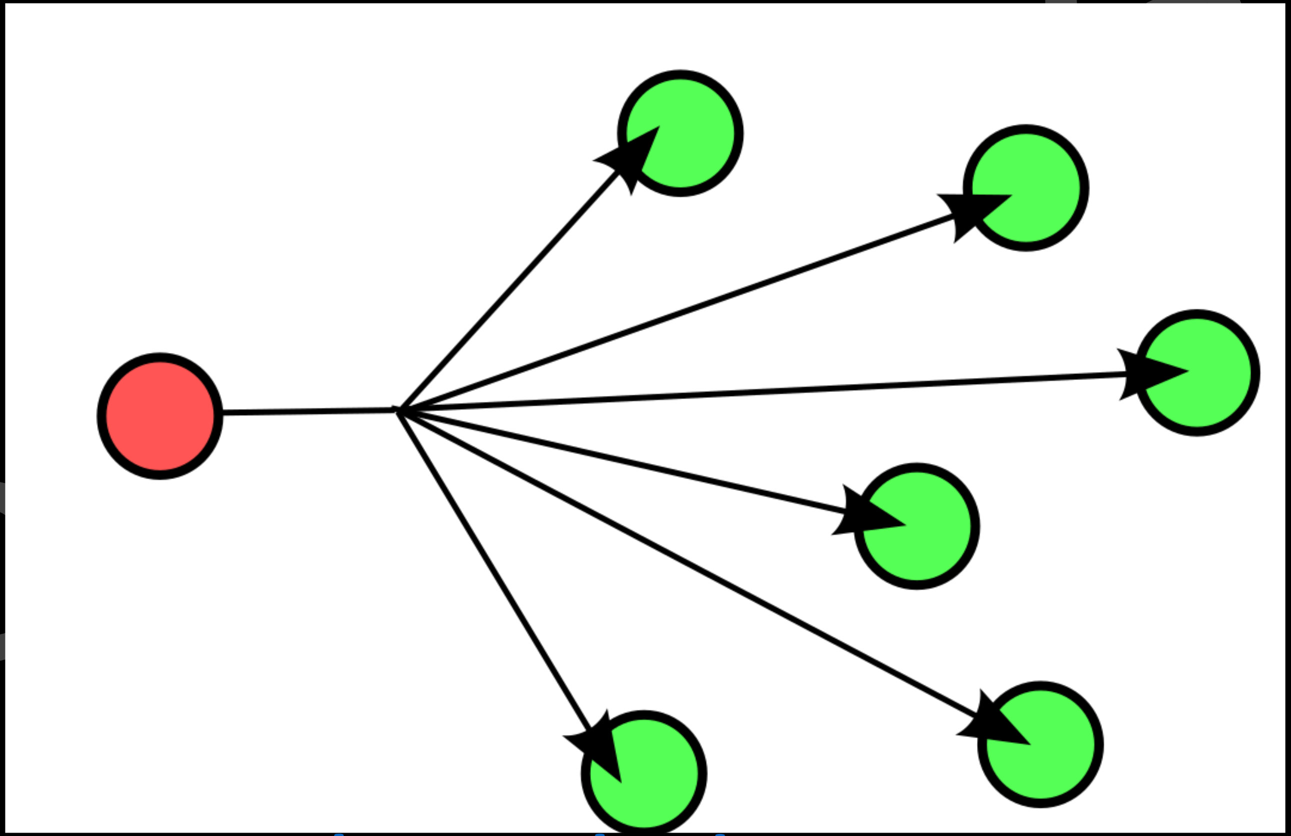


- **Unicast**: Transmitting data from one source host to one destination host is called as **unicast**. It is a one to one transmission.

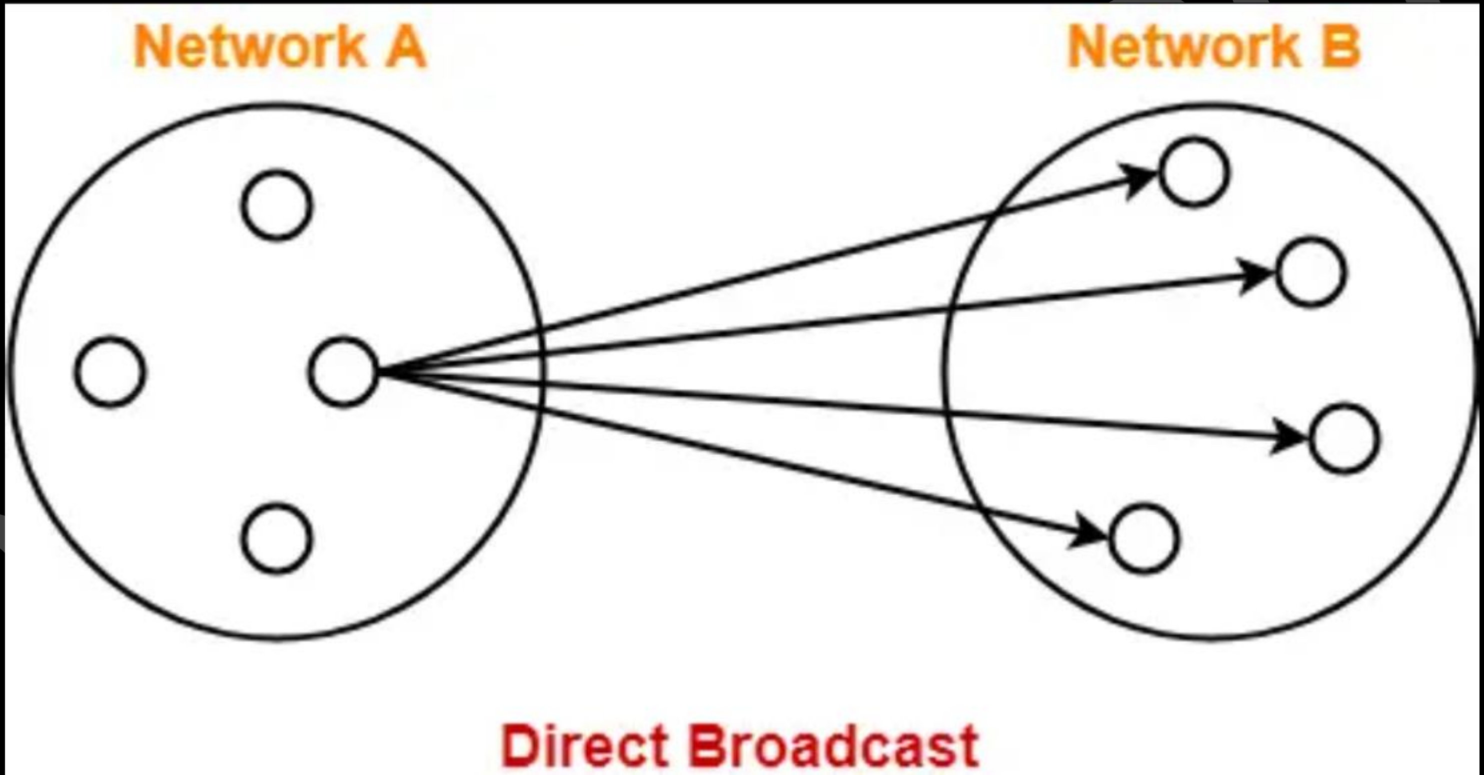


- **Broadcast:** Transmitting data from one source host to all other hosts residing in a network either same or other network is called as **broadcast**. It is a one to all transmission.
  - **Limited Broadcast**:
  - **Direct Broadcast**:

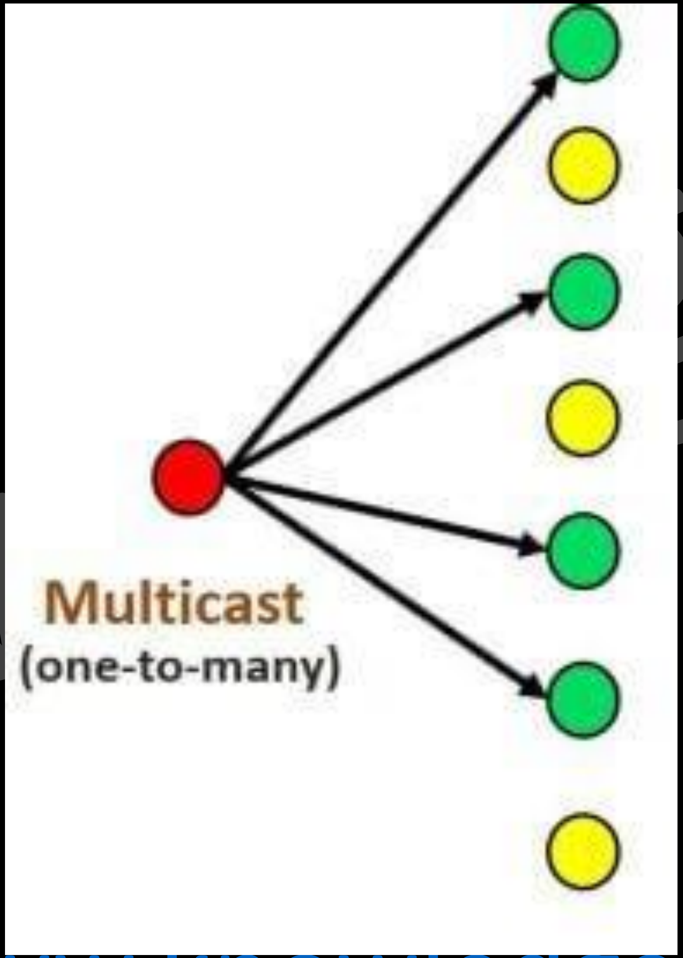
- **Limited Broadcast**: Transmitting data from one source host to all other hosts residing in the same network is called as limited broadcast. Limited Broadcast Address for any network is All 32 bits set to 1 = 11111111.11111111.11111111.11111111 = 255.255.255.255



- **Direct Broadcast**: Transmitting data from one source host to all other hosts residing in some other network is called as direct broadcast.
  - Direct Broadcast Address for any network is the IP Address where, Network ID is the IP Address of the network where all the destination hosts are present and Host ID bits are all set to 1.



- **Multicast**: Transmitting data from one source host to a particular group of hosts having interest in receiving the data is called as multicast. It is a one to many transmissions.



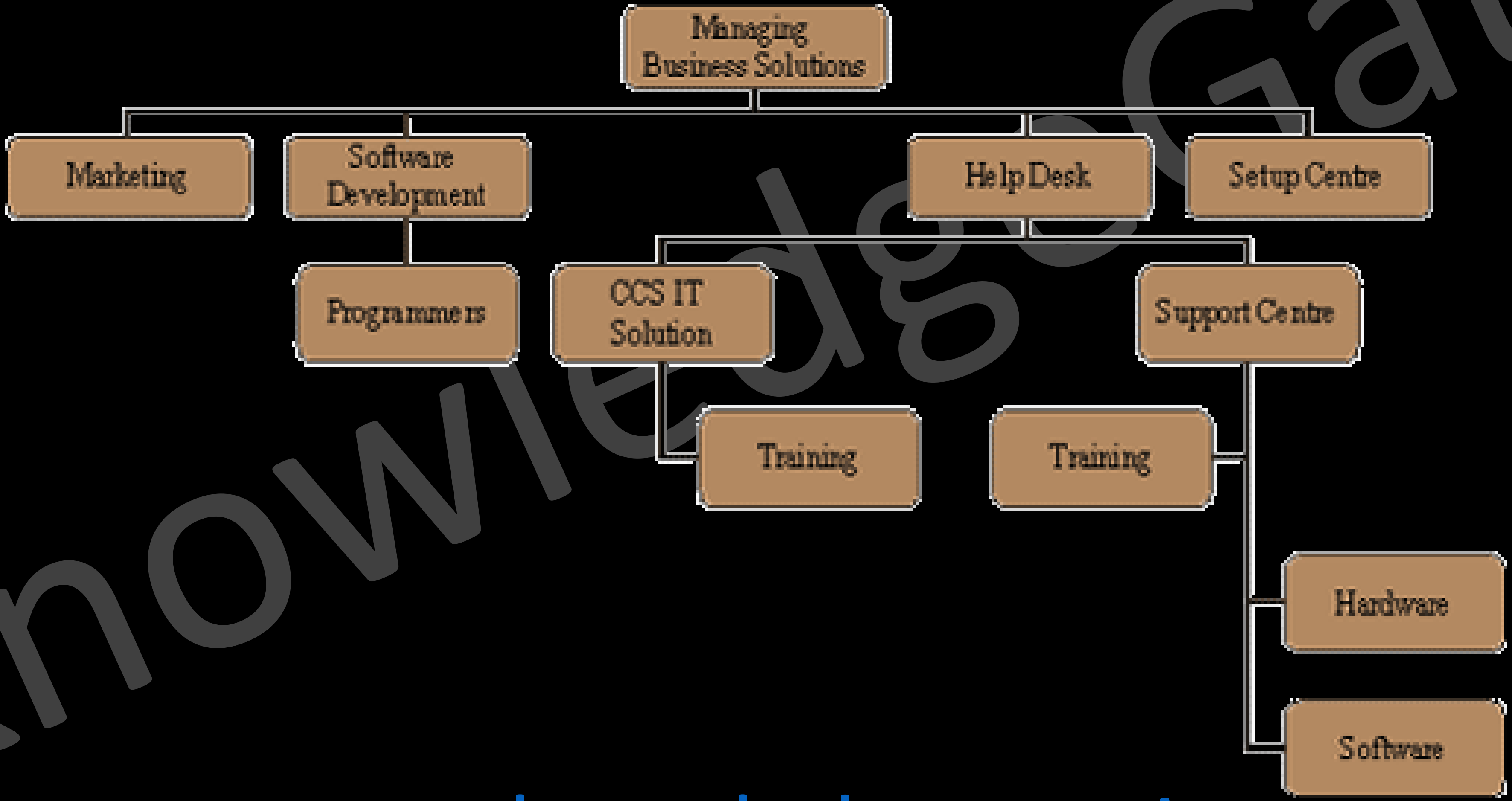
Reason For Subnetting

- Maintenance of a very big network like class A and class B is very difficult for network administrator.

www.knowledgegate.in

Reason For Subnetting

- Having all the computer from different departments in a company on the same networks is less secure from company prospective.

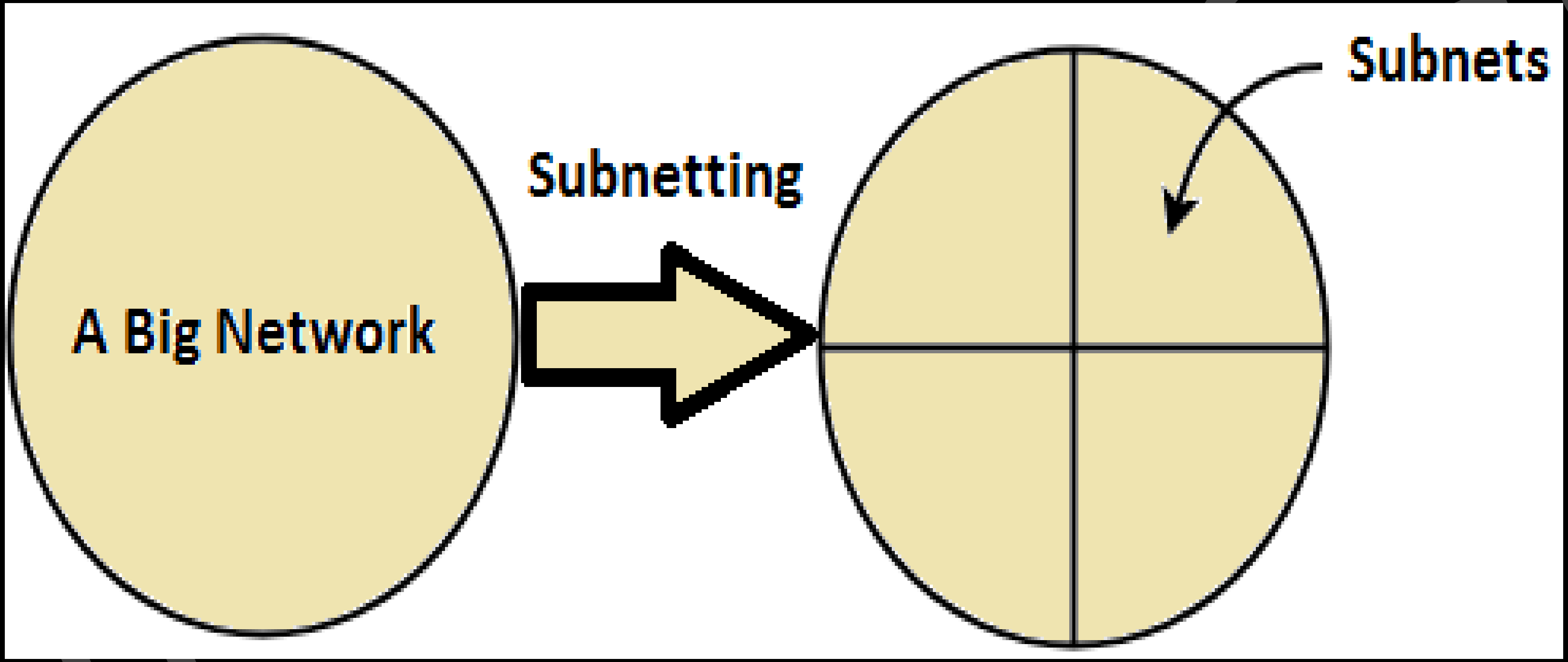


www.knowledgegate.in

Reason For Subnetting

- So, if an organization was granted a large block in class A or B, it could divide the addresses into several contiguous groups and assign each group to smaller networks (called subnets) or, in rare cases, share part of the addresses with neighbours.

- **Conclusion:** An organization (or an ISP) that is granted a range of addresses may divide the range into several subranges and assign each subrange to a subnetwork (or subnet). A subnetwork can be divided into several sub-subnetworks. A sub-subnetwork can be divided into several sub-sub-subnetworks, and so on.



Advantages

- It improves the security.
- The maintenance and administration of subnets is easy.

Disadvantages

- Identification of a station is difficult
- Not possible to directed broadcast from outside network.

Types of Subnetting

Subnets can be of two types:

1. Fixed Length Subnetting
2. Variable Length Subnetting

Fixed Length Subnetting

- Fixed length subnetting (classful subnetting) divides the network into subnets such that:
  - All the subnets are of same size.
  - All the subnets have equal number of hosts.
  - All the subnets have same subnet mask.

Q Consider the network having IP Address 200.1.2.0. Divide this network into two subnets.

Q Consider the network having IP Address 200.1.2.0. Divide this network into two subnets.

1st Subnet

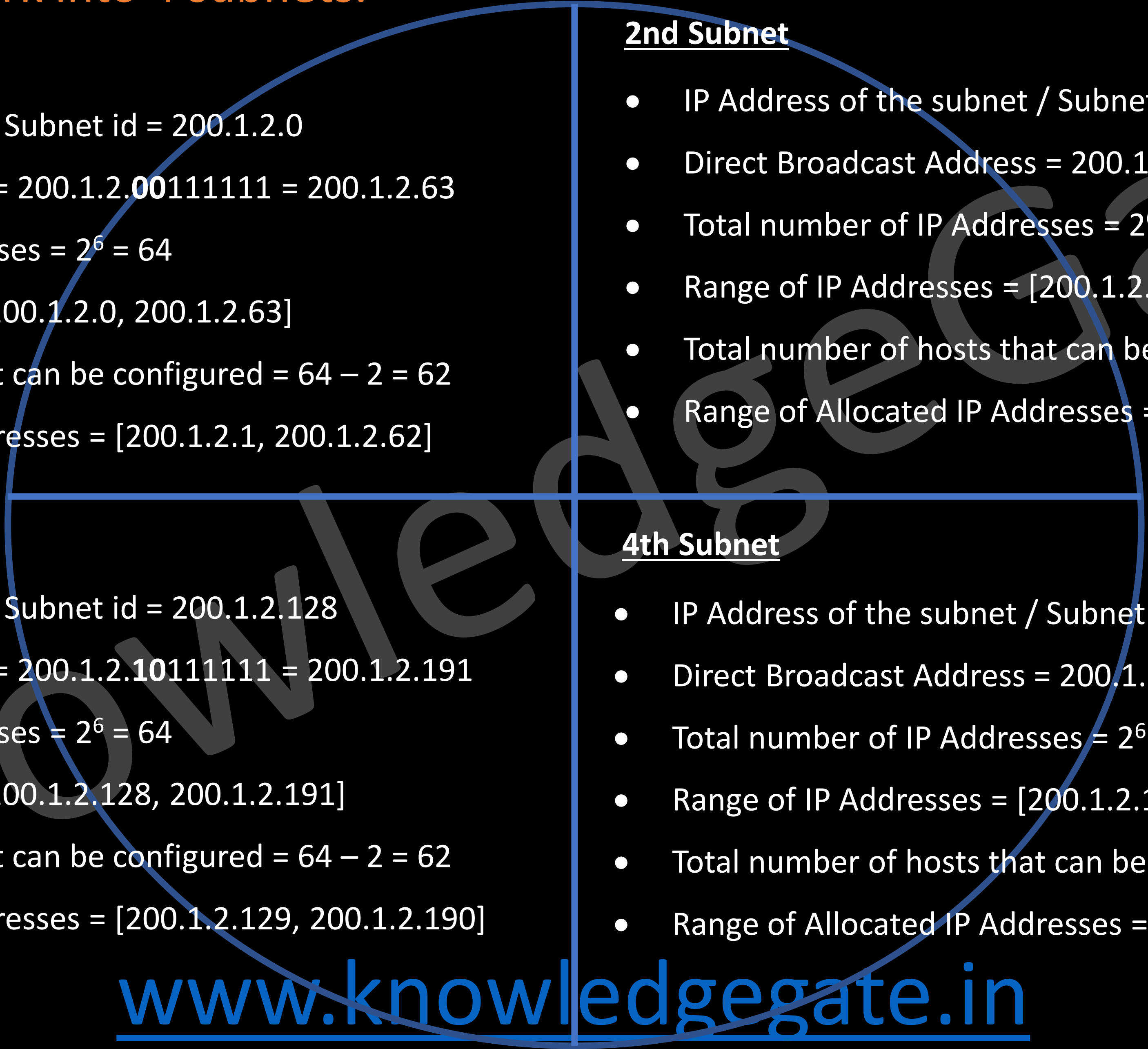
- IP Address of the subnet / Subnet id = 200.1.2.0
- Direct Broadcast Address = 200.1.2.01111111 = 200.1.2.127
- Total number of IP Addresses = 2^7 = 128
- Range of IP Addresses = [200.1.2.0, 200.1.2.127]
- Total number of hosts that can be configured = 128 – 2 = 126
- Range of Allocated IP Addresses = [200.1.2.1, 200.1.2.126]

2nd Subnet

- IP Address of the subnet / Subnet id = 200.1.2.128
- Direct Broadcast Address = 200.1.2.11111111 = 200.1.2.255
- Total number of IP Addresses = 2^7 = 128
- Range of IP Addresses = [200.1.2.128, 200.1.2.255]
- Total number of hosts that can be configured = 128 – 2 = 126
- Range of Allocated IP Addresses = [200.1.2.129, 200.1.2.254]

Q Consider we have a big single network having IP Address 200.1.2.0. We want to do subnetting and divide this network into 4 subnets.

Q Consider we have a big single network having IP Address 200.1.2.0. We want to do subnetting and divide this network into 4 subnets.



1st Subnet

- IP Address of the subnet / Subnet id = 200.1.2.0
- Direct Broadcast Address = 200.1.2.**00**111111 = 200.1.2.63
- Total number of IP Addresses = 2^6 = 64
- Range of IP Addresses = [200.1.2.0, 200.1.2.63]
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of Allocated IP Addresses = [200.1.2.1, 200.1.2.62]

2nd Subnet

- IP Address of the subnet / Subnet id = 200.1.2.64
- Direct Broadcast Address = 200.1.2.**01**111111 = 200.1.2.127
- Total number of IP Addresses = 2^6 = 64
- Range of IP Addresses = [200.1.2.64, 200.1.2.127]
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of Allocated IP Addresses = [200.1.2.65, 200.1.2.126]

3rd Subnet

- IP Address of the subnet / Subnet id = 200.1.2.128
- Direct Broadcast Address = 200.1.2.**10**111111 = 200.1.2.191
- Total number of IP Addresses = 2^6 = 64
- Range of IP Addresses = [200.1.2.128, 200.1.2.191]
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of Allocated IP Addresses = [200.1.2.129, 200.1.2.190]

4th Subnet

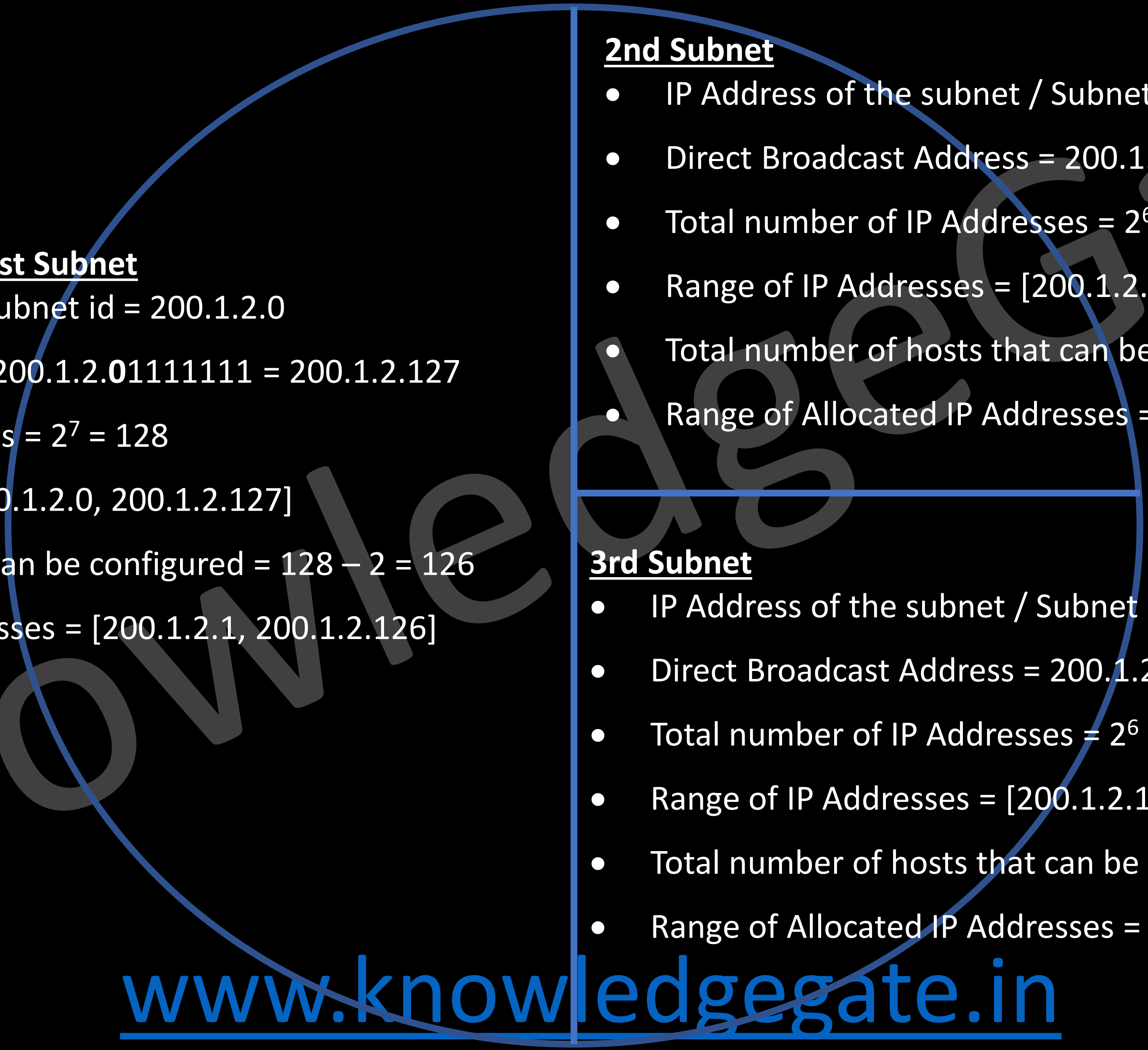
- IP Address of the subnet / Subnet id = 200.1.2.192
- Direct Broadcast Address = 200.1.2.**11**111111 = 200.1.2.255
- Total number of IP Addresses = 2^6 = 64
- Range of IP Addresses = [200.1.2.192, 200.1.2.255]
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of Allocated IP Addresses = [200.1.2.193, 200.1.2.254]

Variable Length Subnetting

- Variable length subnetting (classless subnetting) divides the network into subnets such that:
    - All the subnets are not of same size.
    - All the subnets do not have equal number of hosts.
    - All the subnets do not have same subnet mask.

Q Consider we have a big single network having IP Address 200.1.2.0. We want to do subnetting and divide this network into 3 subnets, such that first contains 126 hosts, and other two contains 62 hosts each?

Q Consider we have a big single network having IP Address 200.1.2.0. We want to do subnetting and divide this network into 3 subnets, such that first contains 126 hosts, and other two contains 62 hosts each?



1st Subnet

- IP Address of the subnet / Subnet id = 200.1.2.0
- Direct Broadcast Address = 200.1.2.**0**1111111 = 200.1.2.127
- Total number of IP Addresses = 2^7 = 128
- Range of IP Addresses = [200.1.2.0, 200.1.2.127]
- Total number of hosts that can be configured = 128 – 2 = 126
- Range of Allocated IP Addresses = [200.1.2.1, 200.1.2.126]

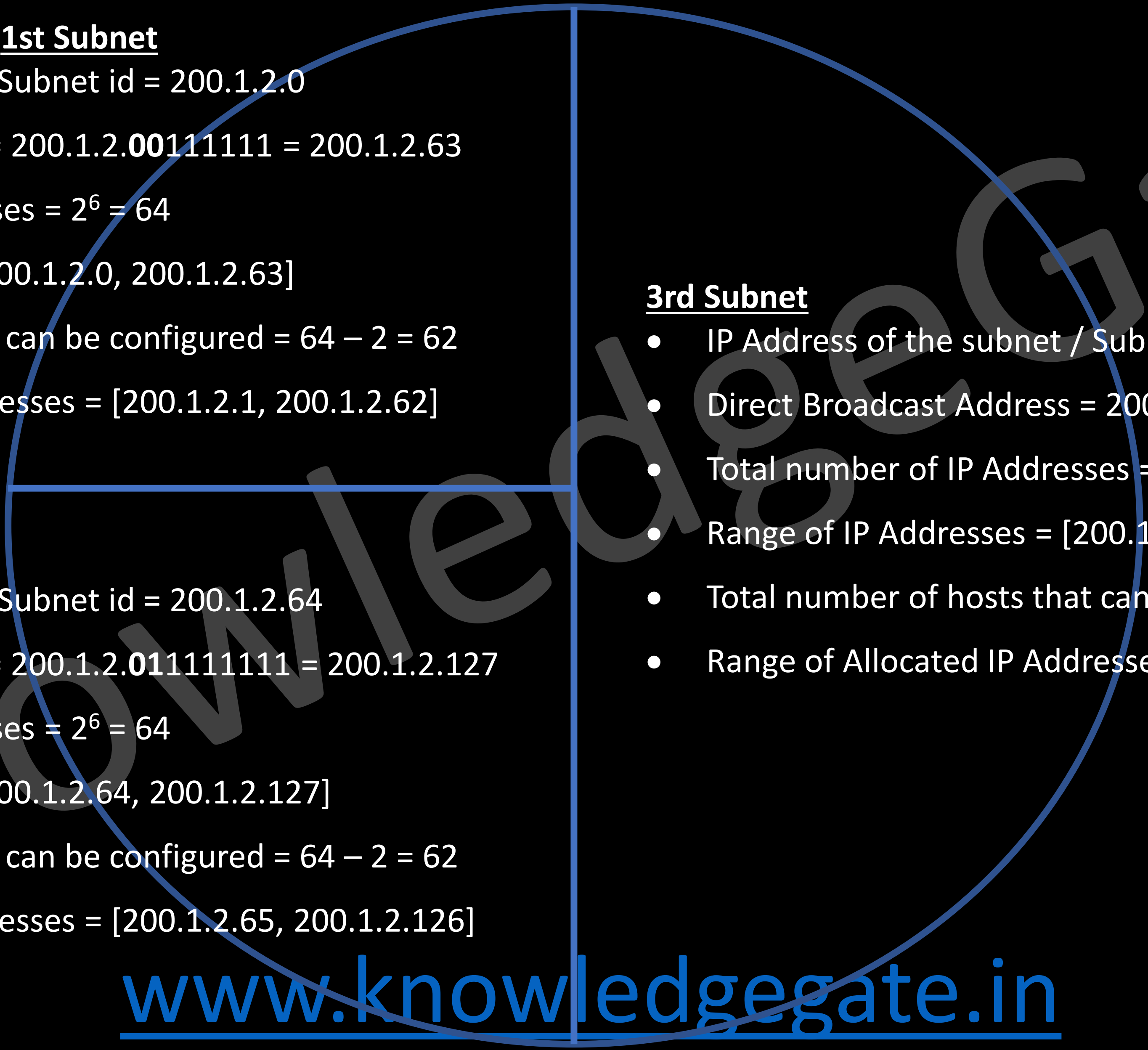
2nd Subnet

- IP Address of the subnet / Subnet id = 200.1.2.128
- Direct Broadcast Address = 200.1.2.**10**111111 = 200.1.2.191
- Total number of IP Addresses = 2^6 = 64
- Range of IP Addresses = [200.1.2.128, 200.1.2.191]
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of Allocated IP Addresses = [200.1.2.129, 200.1.2.190]

3rd Subnet

- IP Address of the subnet / Subnet id = 200.1.2.192
- Direct Broadcast Address = 200.1.2.**11**111111 = 200.1.2.255
- Total number of IP Addresses = 2^6 = 64
- Range of IP Addresses = [200.1.2.192, 200.1.2.255]
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of Allocated IP Addresses = [200.1.2.193, 200.1.2.254]

Q Consider we have a big single network having IP Address 200.1.2.0. We want to do subnetting and divide this network into 3 subnets, such that first contains 126 hosts, and other two contains 62 hosts each?



1st Subnet

- IP Address of the subnet / Subnet id = 200.1.2.0
- Direct Broadcast Address = 200.1.2.**00**111111 = 200.1.2.63
- Total number of IP Addresses = 2^6 = 64
- Range of IP Addresses = [200.1.2.0, 200.1.2.63]
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of Allocated IP Addresses = [200.1.2.1, 200.1.2.62]

2nd Subnet

- IP Address of the subnet / Subnet id = 200.1.2.64
- Direct Broadcast Address = 200.1.2.**01**111111 = 200.1.2.127
- Total number of IP Addresses = 2^6 = 64
- Range of IP Addresses = [200.1.2.64, 200.1.2.127]
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of Allocated IP Addresses = [200.1.2.65, 200.1.2.126]

3rd Subnet

- IP Address of the subnet / Subnet id = 200.1.2.128
- Direct Broadcast Address = 200.1.2.**1**1111111 = 200.1.2.255
- Total number of IP Addresses = 2^7 = 128
- Range of IP Addresses = [200.1.2.128, 200.1.2.255]
- Total number of hosts that can be configured = 128 – 2 = 126
- Range of Allocated IP Addresses = [200.1.2.129, 200.1.2.254]

Point to Note:

- Subnetting increases the number of 1’s in the mask

Subnet Masks

- In case of subnetting the problem is how to identify to which subnet the incoming packet from outside the network must be delivered. To solve this problem, we use the idea of subnet mask.

- Subnet mask is a 32-bit number which is a sequence of 1’s followed by a sequence of 0’s where:
  - o 1’s represents the Network ID part along with the subnet ID.
  - o 0’s represents the host ID part.

- Default mask for different classes of IP Address are:
  - o Default subnet mask of Class A = 255.0.0.0
  - o Default subnet mask for Class B = 255.255.0.0
  - o Default subnet mask for Class C = 255.255.255.0

o Networks of same size always have the same subnet mask.

Address Depletion

- The addresses were not distributed properly as class A and B are usually very large for any organization and class C is usually very small

- Flexibility is not there is classful addressing, we cannot have the exact allocation as we want for e.g. if some company wants 150 IP address then must go for 256, resulting into address depletion.

- Wastage of addresses, for example: Class E addresses were almost never used, wasting the whole class.

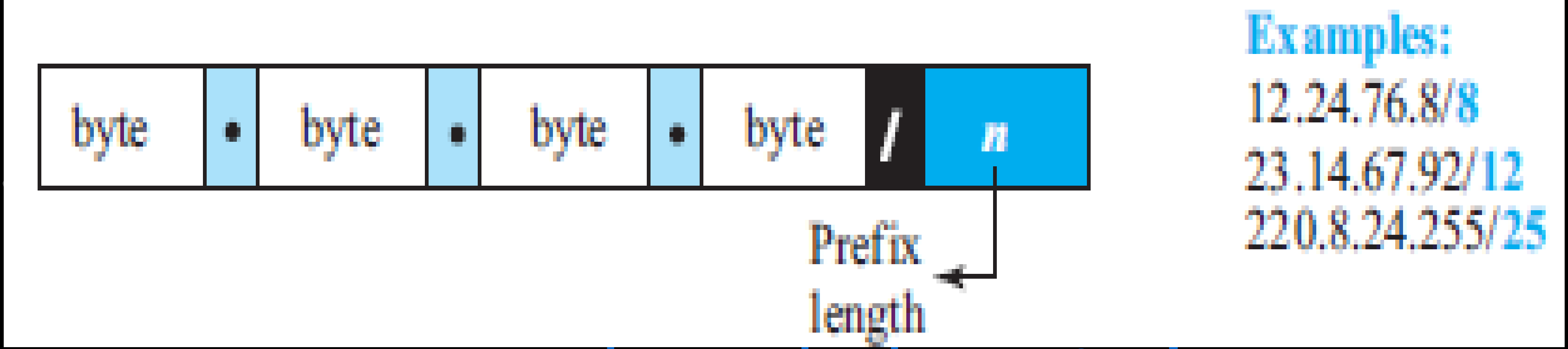
- **Conclusion:** The Internet was faced with the problem of the addresses being rapidly used up, resulting in no more addresses available for organizations and individuals that needed to be connected to the Internet.

Classless Addressing (Blocks/Network)

- Classless Addressing is an improved IP Addressing system.
- The class privilege is removed from the distribution to compensate for the address depletion, so no class.
- Here we can ask exact set of IP address which are required and a Variable-length blocks are assigned which satisfy the request.

CIDR Notation

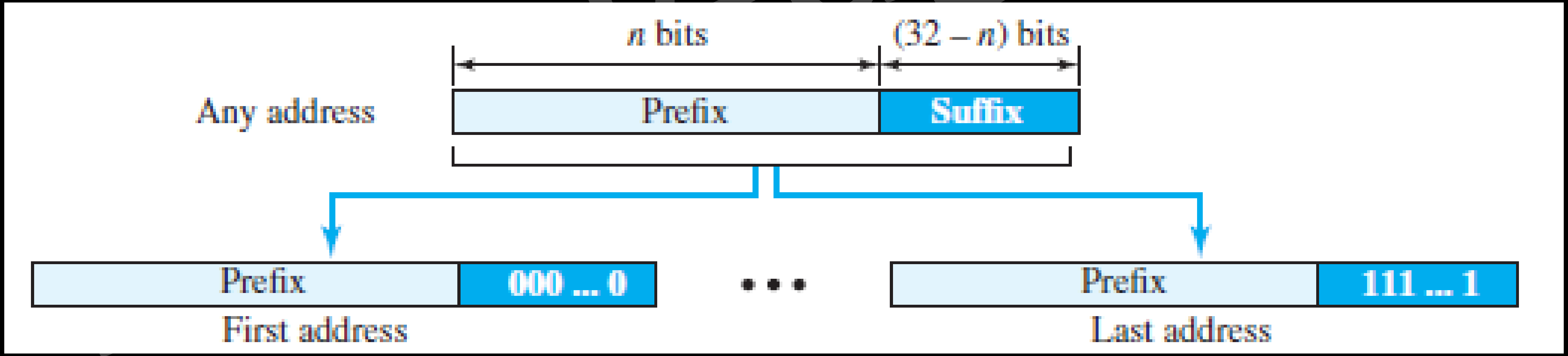
- The question is as there are no classes, how to identify block id and host id, as address in classless addressing does not define the block or network to which the address belongs.
- To solve this problem now we have a new CIDR notation, this notation is informally referred to as *slash notation* and formally as ***classless interdomain routing*** or ***CIDR.***
- To find the prefix(net_id), *n* is added to the address, separated by a slash.
- n represent number of bits in net_id



Examples:
12.24.76.8/8
23.14.67.92/12
220.8.24.255/25

Extracting Information from an Address

- The number of addresses in the block is found as $N = 2^{32-n}$.
- To find the first address, we keep the n leftmost bits and set the $(32 - n)$ rightmost bits all to 0s.
- To find the last address, we keep the n leftmost bits and set the $(32 - n)$ rightmost bits all to 1s.



Q Find the Number of addresses, first and last address of the CIDR block to which Following Address belongs to 167.199.170.82/**27** (10100111 11000111 10101010 01010010)

167.199.170.82/**27** (10100111 11000111 10101010 01010010)

10100111 11000111 10101010 010_ _ _ _ _

No of Address = 2^5

167.199.170.82/**27** (10100111 11000111 10101010 01010010)

64

10100111 11000111 10101010 010$\underline{0}$ $\underline{0}$ $\underline{0}$ $\underline{0}$ $\underline{0}$

10100111 11000111 10101010 010$\underline{1}$ $\underline{1}$ $\underline{1}$ $\underline{1}$ $\underline{1}$

95

Address Mask

- The address mask is a 32-bit number in which the *n* leftmost bits are set to 1s and the rest of the bits (32 − *n*) are set to 0s.
- It is another way to find the first and last addresses in the block.
- Using the three bit-wise operations NOT, AND, and OR a computer can find:

  1. The number of addresses in the block N = **NOT** (mask) + 1.
  2. The first address in the block = (Any address in the block) **AND** (mask).
  3. The last address in the block = (Any address in the block) **OR** [(**NOT** (mask)].

Rules for Creating CIDR Block (Network)

- All the IP Addresses in the CIDR block must be contiguous.
- The size of the block (total number of IP Addresses contained in the block) must be presentable as power of 2, size of any CIDR block will always be in the form 2^1, 2^2, 2^3, 2^4, 2^5 and so on. (calculation can be easy)
- First IP Address of the block must be divisible by the size of the block. (so that we get the host id from all 0 to all 1)

Subnetting in CIDR

Q Consider the network having IP Address 40.30.20.10/25 Divide this network into two subnets.

Q Consider the network having IP Address 40.30.20.10/25 Divide this network into two subnets.

40.30.20.00001010

1st Subnet

- 40.30.20.00001010
- Total number of IP Addresses = 2^6 = 64
- First Address of the Subnet = 40.30.20.00000000
- Last Address of the Subnet = 40.30.20.00111111
- Range of IP Addresses = [40.30.20.0, 40.30.20.63]
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of Allocated IP Addresses = [40.30.20.1, 40.30.20.62]
- CIRD Representation 40.30.20. __/26

0,1,2,3,4,5,---,63

2st Subnet

- 40.30.20.01001010
- Total number of IP Addresses = 2^6 = 64
- First Address of the Subnet = 40.30.20.01000000
- Last Address of the Subnet = 40.30.20.01111111
- Range of IP Addresses = [40.30.20.64, 40.30.20.127]
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of Allocated IP Addresses = [40.30.20.65, 40.30.20.126]
- CIRD Representation 40.30.20. __/26

64,65,66,67,---,127

Q Consider we have a big single network having IP Address 200.1.2.0/24 We want to do subnetting and divide this network into 4 subnets.

Q Consider we have a big single network having IP Address 200.1.2.0/24. We want to do subnetting and divide this network into 4 subnets.

1st Subnet

- IP Address of the subnet / Subnet id = 200.1.2.0
- Direct Broadcast Address = 200.1.2.**00**111111 = 200.1.2.63
- Total number of IP Addresses = 2^6 = 64
- Range of IP Addresses = [200.1.2.0, 200.1.2.63]
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of Allocated IP Addresses = [200.1.2.1, 200.1.2.62]

2nd Subnet

- IP Address of the subnet / Subnet id = 200.1.2.64
- Direct Broadcast Address = 200.1.2.**01**111111 = 200.1.2.127
- Total number of IP Addresses = 2^6 = 64
- Range of IP Addresses = [200.1.2.64, 200.1.2.127]
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of Allocated IP Addresses = [200.1.2.65, 200.1.2.126]

3rd Subnet

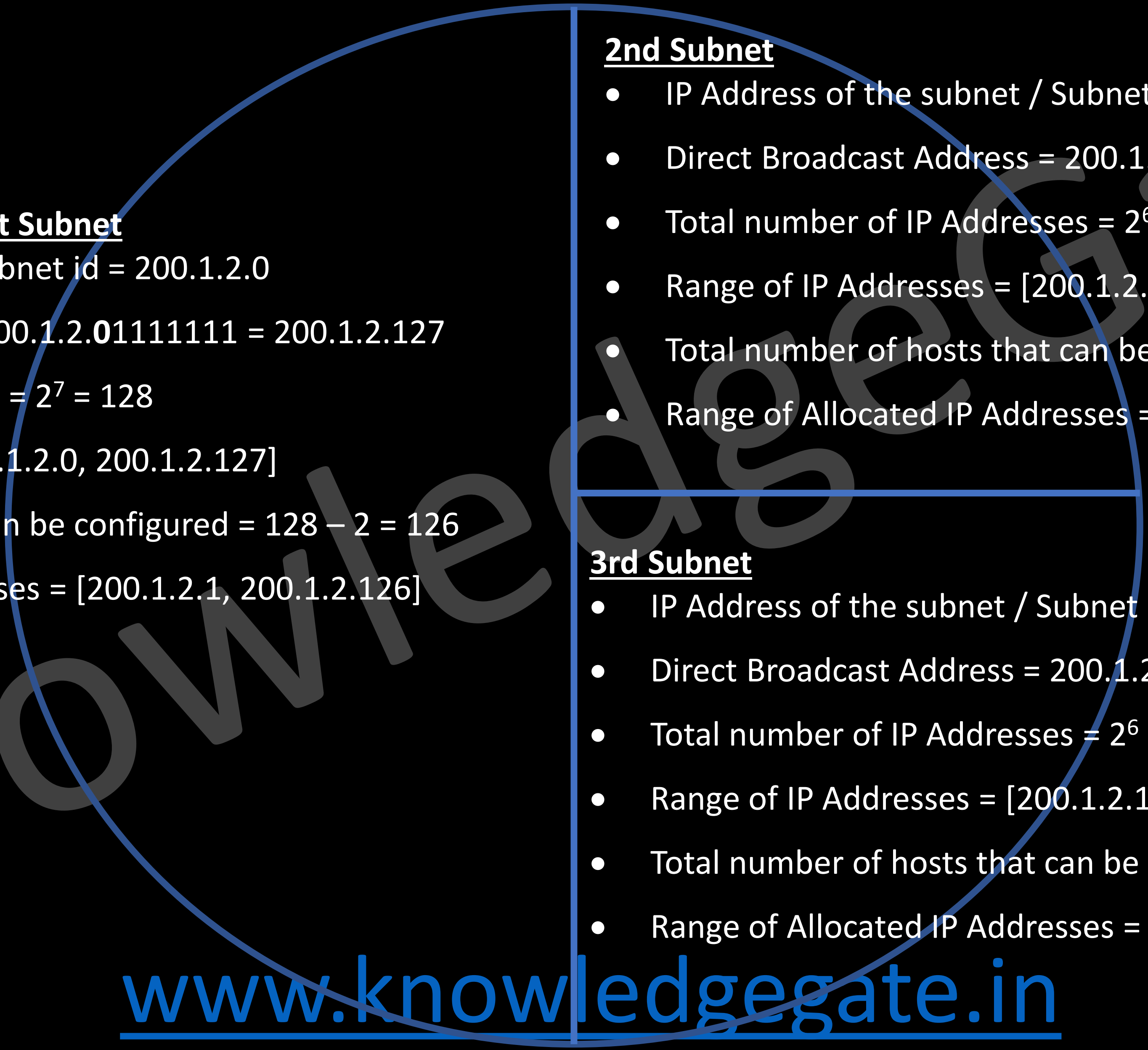
- IP Address of the subnet / Subnet id = 200.1.2.128
- Direct Broadcast Address = 200.1.2.**10**111111 = 200.1.2.191
- Total number of IP Addresses = 2^6 = 64
- Range of IP Addresses = [200.1.2.128, 200.1.2.191]
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of Allocated IP Addresses = [200.1.2.129, 200.1.2.190]

4th Subnet

- IP Address of the subnet / Subnet id = 200.1.2.192
- Direct Broadcast Address = 200.1.2.**11**111111 = 200.1.2.255
- Total number of IP Addresses = 2^6 = 64
- Range of IP Addresses = [200.1.2.192, 200.1.2.255]
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of Allocated IP Addresses = [200.1.2.193, 200.1.2.254]

Q Consider we have a big single network having IP Address 200.1.2.0/24. We want to do subnetting and divide this network into 3 subnets, such that first contains 126 hosts, and other two contains 62 hosts each?

Q Consider we have a big single network having IP Address 200.1.2.0/24. We want to do subnetting and divide this network into 3 subnets, such that first contains 126 hosts, and other two contains 62 hosts each?



1st Subnet

- IP Address of the subnet / Subnet id = 200.1.2.0
- Direct Broadcast Address = 200.1.2.**0**1111111 = 200.1.2.127
- Total number of IP Addresses = 2^7 = 128
- Range of IP Addresses = [200.1.2.0, 200.1.2.127]
- Total number of hosts that can be configured = 128 – 2 = 126
- Range of Allocated IP Addresses = [200.1.2.1, 200.1.2.126]

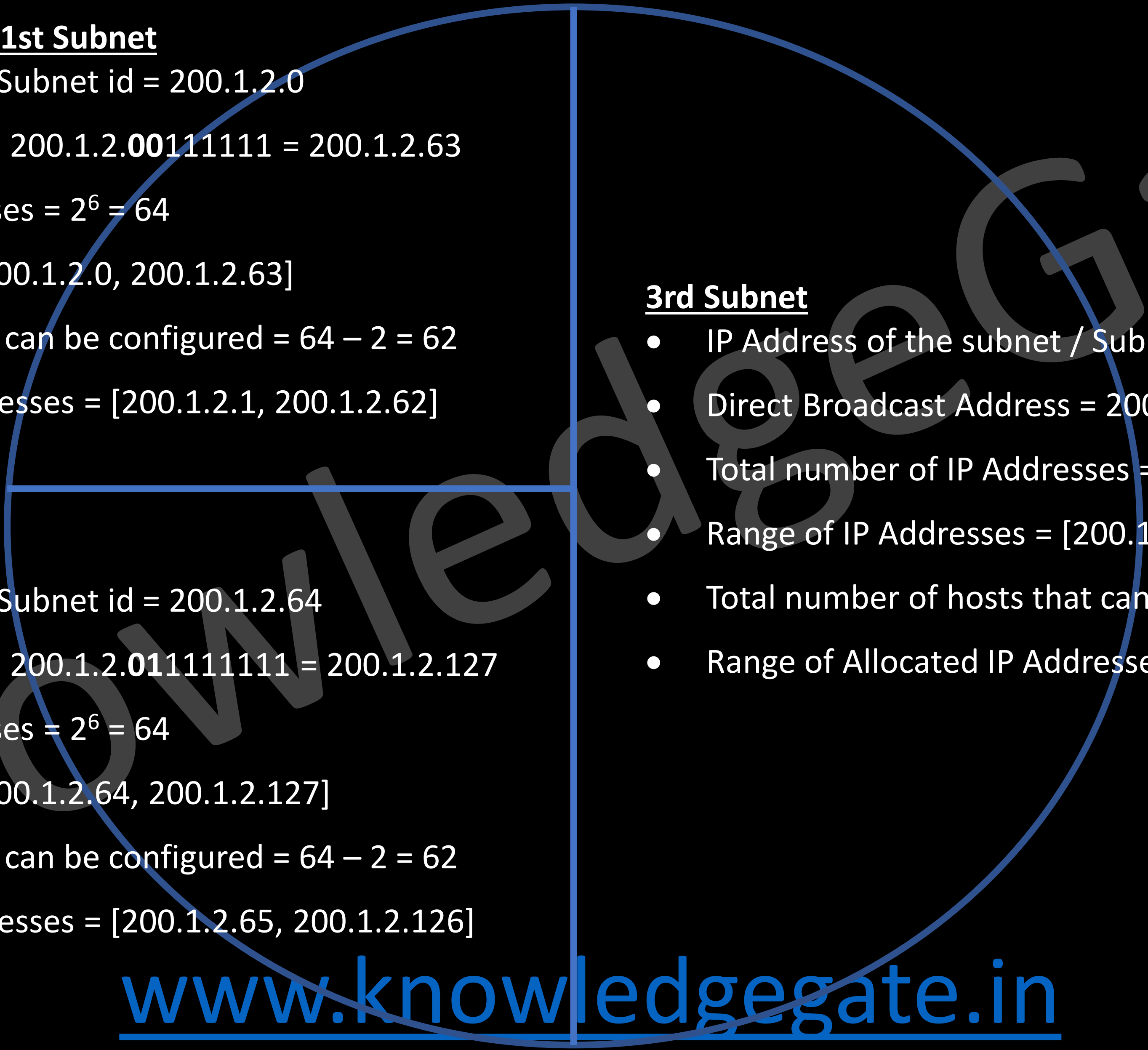
2nd Subnet

- IP Address of the subnet / Subnet id = 200.1.2.128
- Direct Broadcast Address = 200.1.2.**10**111111 = 200.1.2.191
- Total number of IP Addresses = 2^6 = 64
- Range of IP Addresses = [200.1.2.128, 200.1.2.191]
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of Allocated IP Addresses = [200.1.2.129, 200.1.2.190]

3rd Subnet

- IP Address of the subnet / Subnet id = 200.1.2.192
- Direct Broadcast Address = 200.1.2.**11**111111 = 200.1.2.255
- Total number of IP Addresses = 2^6 = 64
- Range of IP Addresses = [200.1.2.192, 200.1.2.255]
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of Allocated IP Addresses = [200.1.2.193, 200.1.2.254]

Q Consider we have a big single network having IP Address 200.1.2.0/24. We want to do subnetting and divide this network into 3 subnets, such that first contains 126 hosts, and other two contains 62 hosts each?



1st Subnet

- IP Address of the subnet / Subnet id = 200.1.2.0
- Direct Broadcast Address = 200.1.2.**00**111111 = 200.1.2.63
- Total number of IP Addresses = 2^6 = 64
- Range of IP Addresses = [200.1.2.0, 200.1.2.63]
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of Allocated IP Addresses = [200.1.2.1, 200.1.2.62]

2nd Subnet

- IP Address of the subnet / Subnet id = 200.1.2.64
- Direct Broadcast Address = 200.1.2.**01**1111111 = 200.1.2.127
- Total number of IP Addresses = 2^6 = 64
- Range of IP Addresses = [200.1.2.64, 200.1.2.127]
- Total number of hosts that can be configured = 64 – 2 = 62
- Range of Allocated IP Addresses = [200.1.2.65, 200.1.2.126]

3rd Subnet

- IP Address of the subnet / Subnet id = 200.1.2.128
- Direct Broadcast Address = 200.1.2.**1**11111111 = 200.1.2.255
- Total number of IP Addresses = 2^7 = 128
- Range of IP Addresses = [200.1.2.128, 200.1.2.255]
- Total number of hosts that can be configured = 128 – 2 = 126
- Range of Allocated IP Addresses = [200.1.2.129, 200.1.2.254]

Designing subnets for CIDR Notations

- Assume:
    - The total number of addresses granted to the organization is **N**
    - The prefix length is ***n***
    - The assigned number of addresses to each sub-network is **N_{sub}**
    - The prefix length for each sub-network is ***n_{sub}***.
- Then, The number of addresses in each sub-network should be a power of 2.

- The prefix length for each sub-network should be found using the following formula: **$n_{sub} = 32 - \log_2 N_{sub}$**

- The starting address in each sub-network should be divisible by the number of addresses in that sub-network. This can be achieved if we first assign addresses to larger sub-networks.

Super Netting in Classful addressing

- In super netting, an organization can combine several blocks to create a larger range of addresses. In other words, several networks are combined to create a super network or a supernet.

- An organization can apply for a set of class C blocks instead of just one. For example, an organization that needs 1000 addresses can be granted four contiguous class C blocks. The organization can then use these addresses to create one super network.

- Super netting decreases the number of 1's in the mask.

Super Netting / Aggregation with CIDR

- Rules for Super netting in CIDR
  - All network should be contiguous
  - first net id should be divisible by size of the block

Q Perform CIDR aggregation on the following IP Addresses-

128.56.24.0/24

128.56.25.0/24

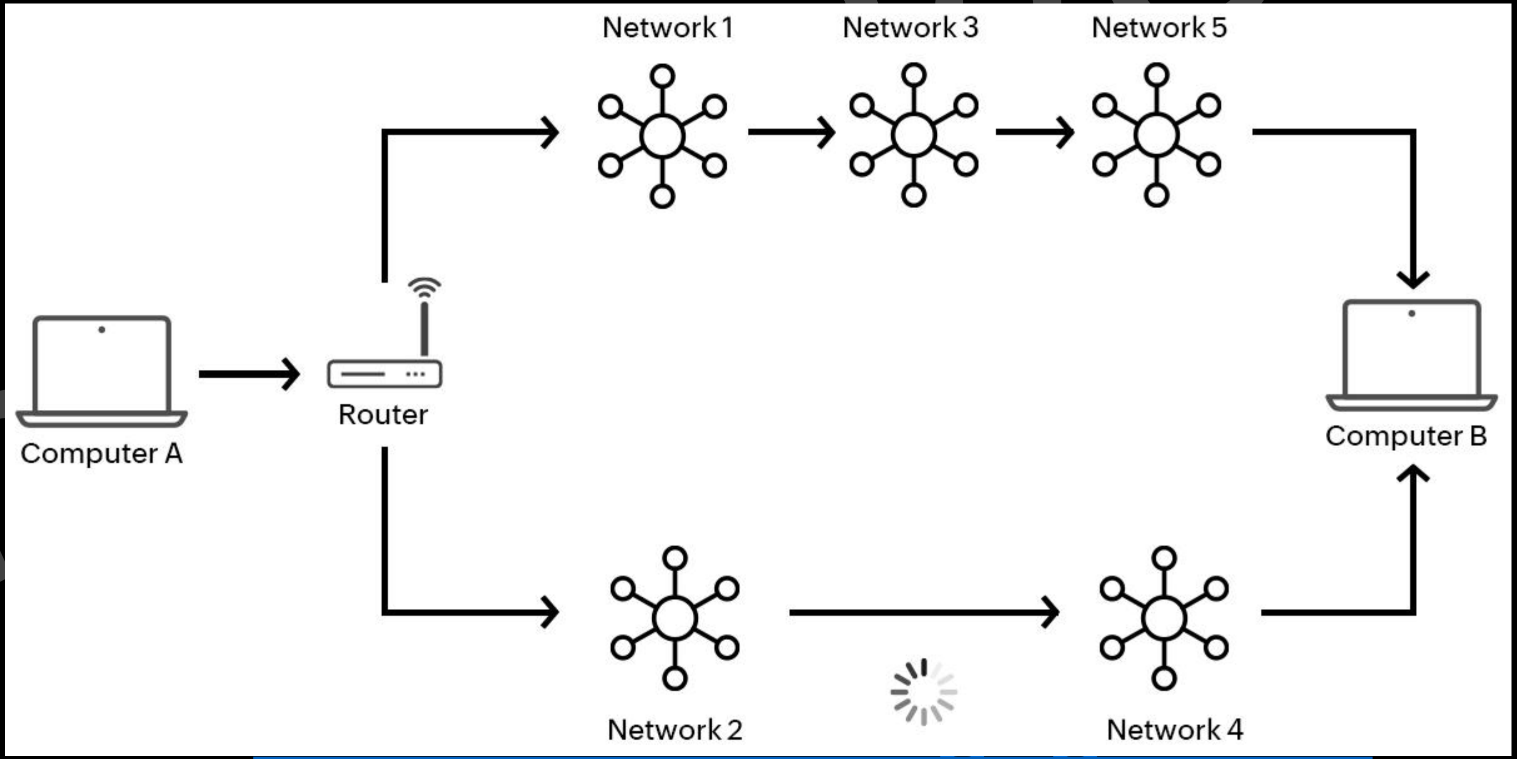
128.56.26.0/24

128.56.27.0/24

- Rules for Super netting in CIDR
  - All network should be contiguous
  - first net id should be divisible by size of the block

Routing

- When a router receives an IP packet with destination address then how can it decide to which interface the packet must be send. This decision at the router, is taken with the help of a routing table.
- Actually the process of designing a routing table is called routing. Taking a packet and sending it to some path is actually switching.



Flooding

- One question, is it possible that a packet reaches its destination without routing table, actually yes, the process is called flooding. That is instead of trying to identify the shortest path, we can send it to all possible way and then we can be sure that at least one packet will reach the destination.
- Flooding Advantage
  - No Routing Algorithm is required
  - Shortest Path is guaranteed
  - Highly Reliable
- Flooding Disadvantage
  - Duplicate packets will arrive at destination and intermediate router
  - Traffic is high.

ROUTING

- A routing table contains information about the network, and it helps deciding to which interface the incoming packet should be sent inorder to reach destination. Routing table can be either static or dynamic.

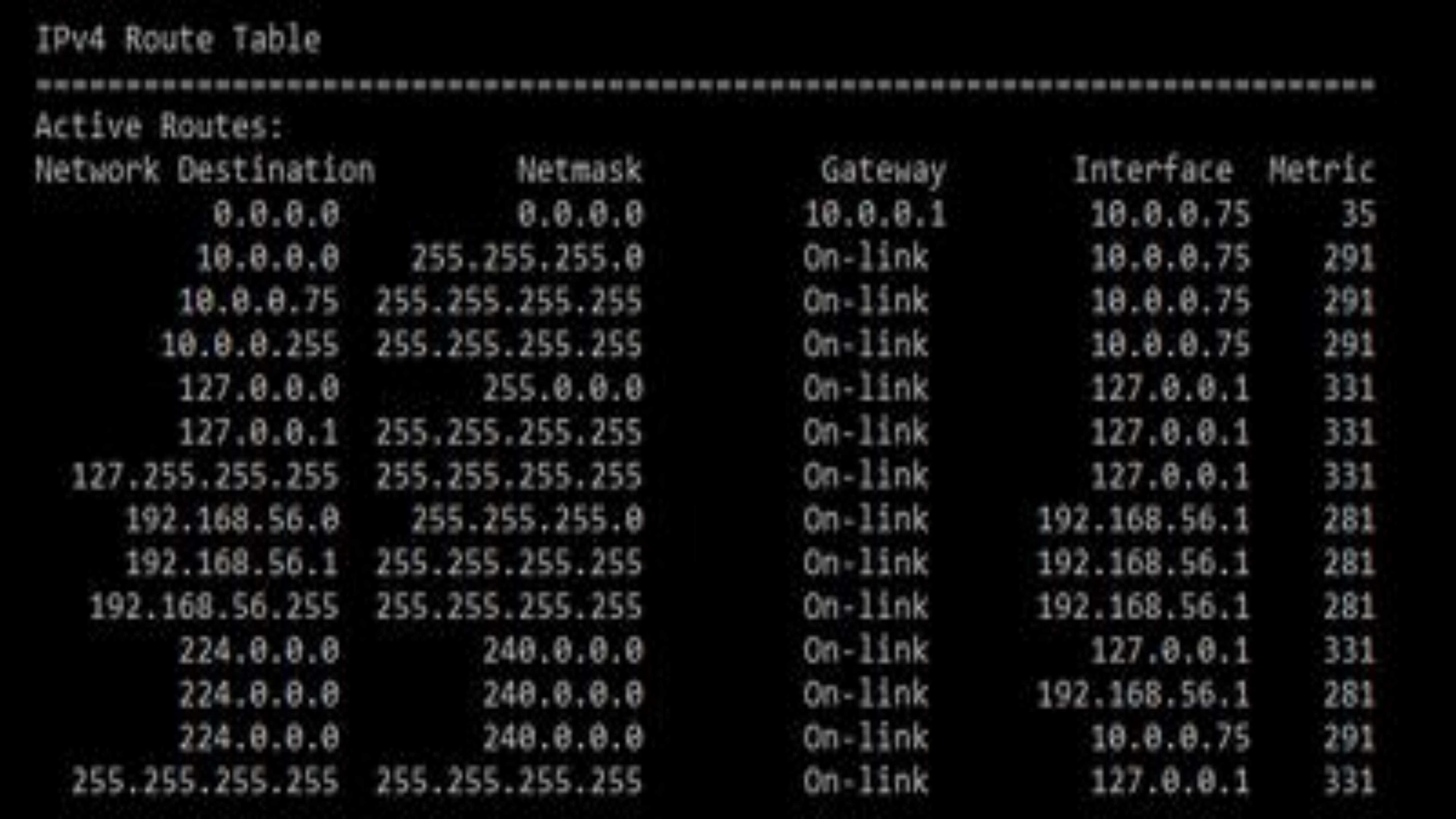
- A static table is one with manual entries, i.e. if someone has information about all the routers in the network and can compute the shortest distance from one router to another and can upload the routing information in a table for each router then it is called Static Routing.
  - Now-a days as we know the internet is so complex that no one can have complete information about the entire internet
  - Internet keeps on changing some new routers come and some old routers may go down, means topology and traffic keeps on changing. Conclusion Static routing is not possible.

- A dynamic table, on the other hand, is one that is updated automatically, without human intervention, when there is a change somewhere in the internet either in topology or traffic.

UNICAST ROUTING PROTOCOLS

- Routing protocols have been created in response to the demand for dynamic routing tables. A routing protocol is a combination of rules and procedures that lets routers in the internet inform each other of changes.

- It allows routers to share whatever they know about the internet or their neighbourhood. The sharing of information allows a router in Delhi to know about the failure of a network in Singapore. The routing protocols also include procedures for combining information received from other routers. Router to have several routing tables based on the required type of service.

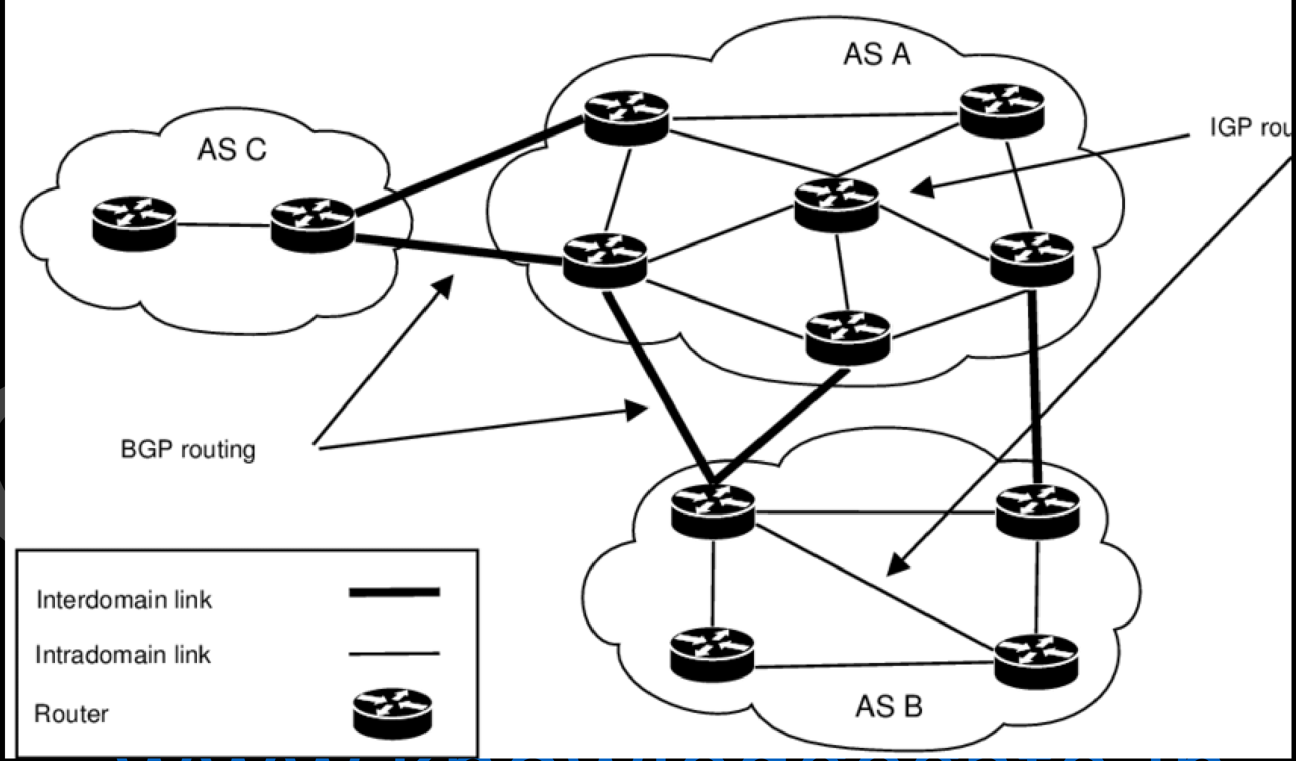


```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0         10.0.0.1       10.0.0.75     35
         10.0.0.0    255.255.255.0         On-link        10.0.0.75    291
        10.0.0.75  255.255.255.255         On-link        10.0.0.75    291
       10.0.0.255  255.255.255.255         On-link        10.0.0.75    291
        127.0.0.0        255.0.0.0         On-link        127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link        127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link        127.0.0.1    331
     192.168.56.0    255.255.255.0         On-link     192.168.56.1    281
     192.168.56.1  255.255.255.255         On-link     192.168.56.1    281
   192.168.56.255  255.255.255.255         On-link     192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link        127.0.0.1    331
        224.0.0.0        240.0.0.0         On-link     192.168.56.1    281
        224.0.0.0        240.0.0.0         On-link        10.0.0.75    291
  255.255.255.255  255.255.255.255         On-link        127.0.0.1    331
```

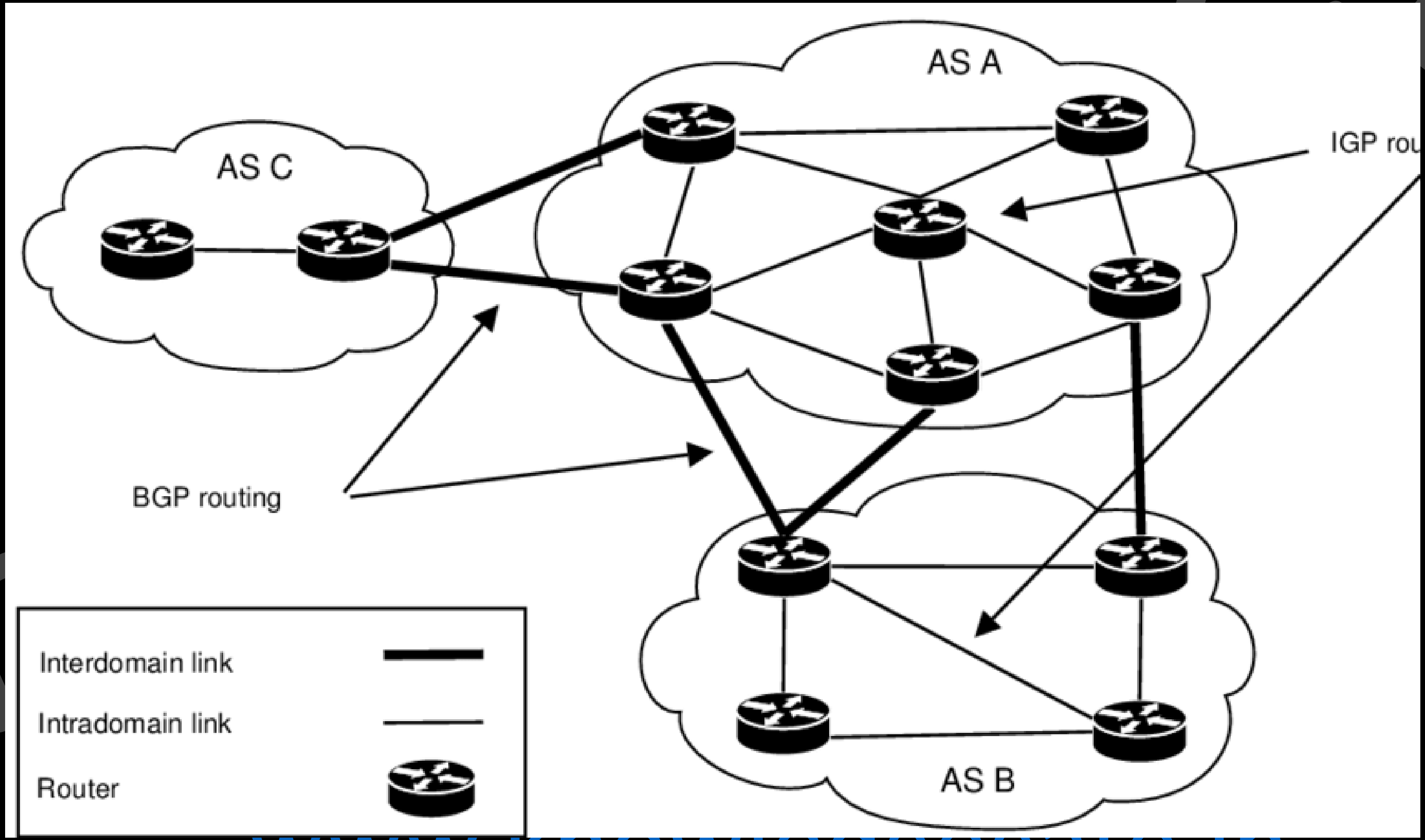
Intra-domain and Interdomain Routing

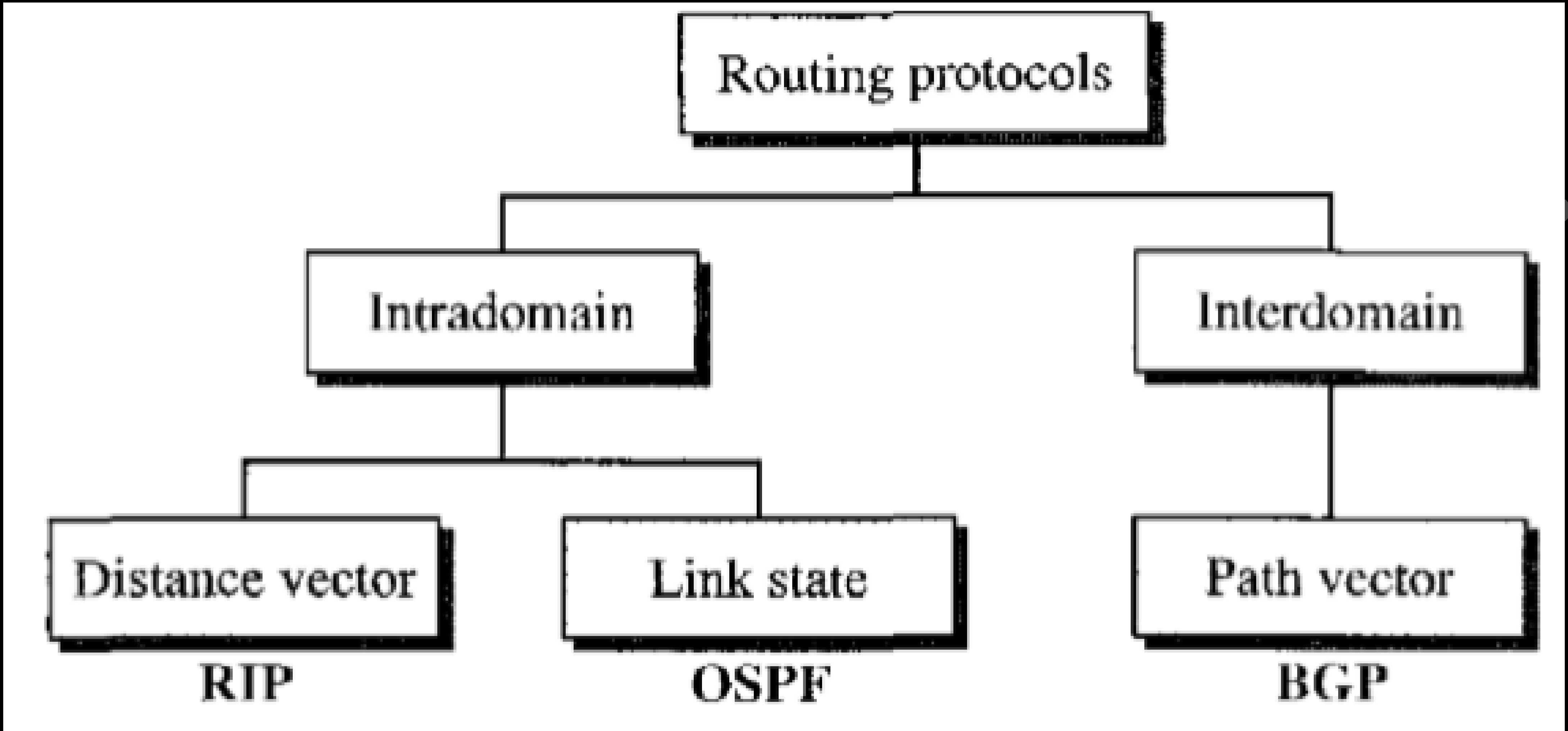
- Today, an internet can be so large that one routing protocol cannot handle the task of updating the routing tables of all routers. For this reason, an internet is divided into autonomous systems.

- An autonomous system (AS) is a group of networks and routers under the authority of a single administration. Routing inside an autonomous system is referred to as intradomain routing.



- Routing between autonomous systems is referred to as interdomain routing.
- Each autonomous system can choose one or more intradomain routing protocols to handle routing inside the autonomous system. However, only one interdomain routing protocol handles routing between autonomous systems.




Routing protocols
Intradomain
Interdomain
Distance vector
Link state
Path vector
RIP
OSPF
BGP

- Which of the available pathways is the optimum pathway? What is the definition of the term optimum? And What is the definition of the term cost

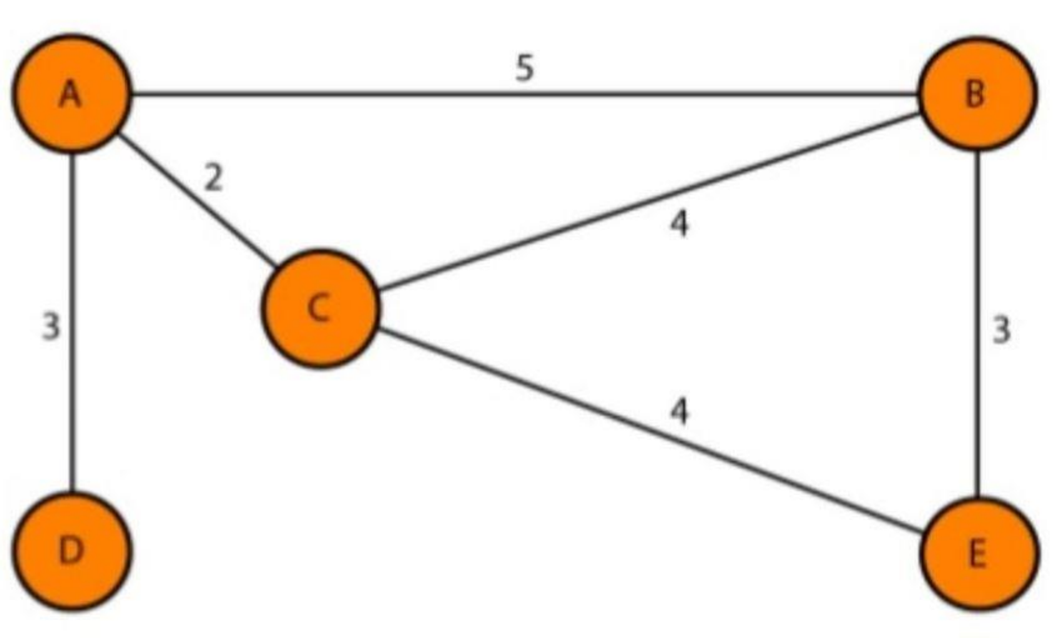
- However, the metric assigned to each network depends on the type of protocol. Some simple protocols, such as the Routing Information Protocol (RIP), treat all networks as equals. The cost of passing through a network is the same; it is one hop count. So if a packet passes through 10 networks to reach the destination, the total cost is 10 hop counts.

- Other protocols, such as Open Shortest Path First (OSPF), allow the administrator to assign a cost for passing through a network based on the type of service required. A route through a network can have different costs (metrics).

Distance Vector Routing

- In distance vector routing, the least-cost route between any two nodes is the route with minimum distance.
- In this protocol, as the name implies, each node maintains a vector (table) of minimum distances to every node. The table at each node also guides the packets to the desired node by showing the next stop in the route (next-hop routing).

To	Cost	Next
A		
B		
C		
D		
E		



To	Cost	Next
A		
B		
C		
D		
E		

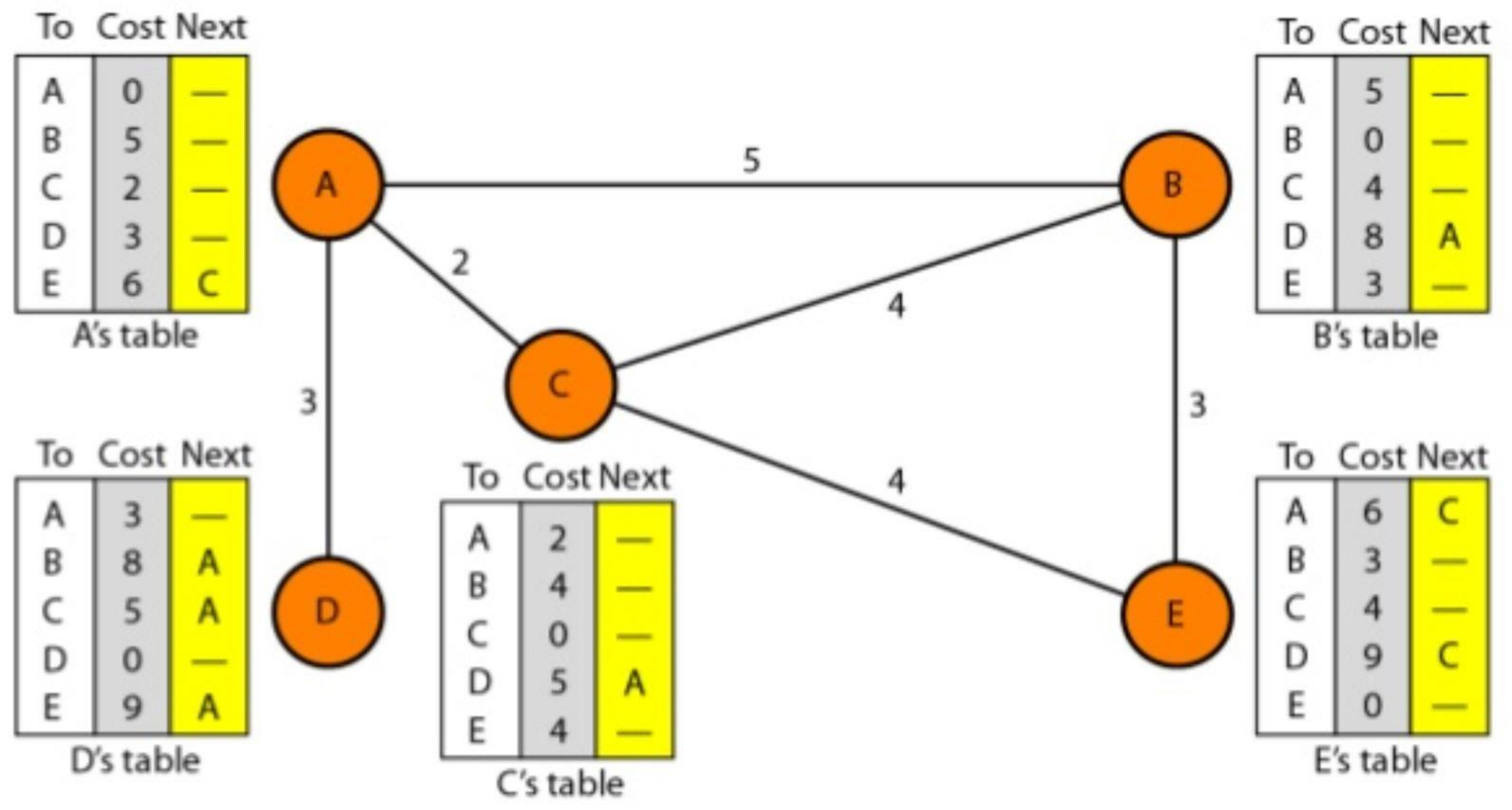
To	Cost	Next
A		
B		
C		
D		
E		

C		
D		
E		

To	Cost	Next
A		
B		
C		
D		
E		

- The whole idea of distance vector routing is the sharing of information between neighbours. Although node A does not know about node E, node C does. So, if node C shares its routing table with A, node A can also know how to reach node E.

- On the other hand, node C does not know how to reach node D, but node A does. If node A shares its routing table with node C, node C also knows how to reach node D. In other words, nodes A and C, as immediate neighbours, can improve their routing tables if they help each other.



To	Cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E	6	C

A's table

To	Cost	Next
A	5	—
B	0	—
C	4	—
D	8	A
E	3	—

B's table

To	Cost	Next
A	3	—
B	8	A
C	5	A
D	0	—
E	9	A

D's table

To	Cost	Next
A	2	—
B	4	—
C	0	—
D	5	A
E	4	—

C's table

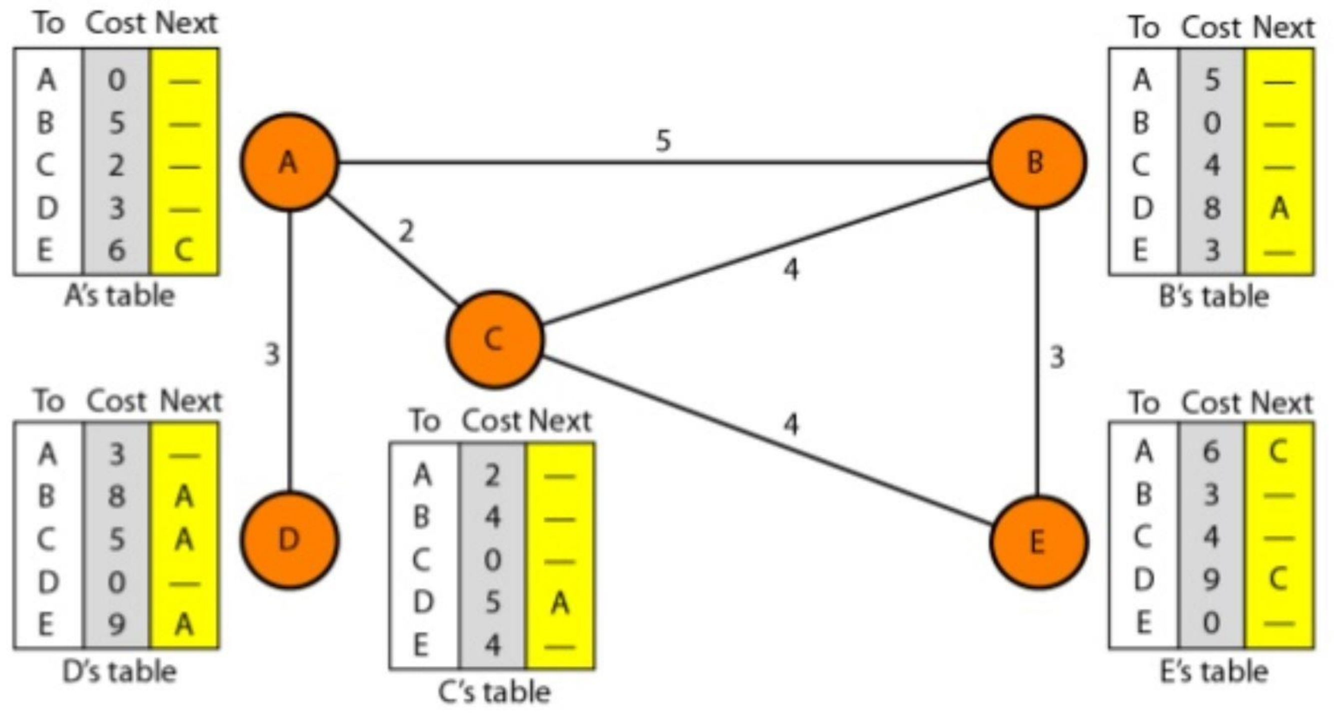
To	Cost	Next
A	6	C
B	3	—
C	4	—
D	9	C
E	0	—

E's table

- There is only one problem. How much of the table must be shared with each neighbour? A node is not aware of a neighbour’s table. The best solution for each node is to send its entire table to the neighbour and let the neighbour decide what part to use and what part to discard.

- However, the third column of a table (next stop) is not useful for the neighbour. When the neighbour receives a table, this column needs to be replaced with the sender's name. If any of the rows can be used, the next node is the sender of the table.

- A node therefore can send only the first two columns of its table to any neighbour. In other words, sharing here means sharing only the first two columns.



To	Cost	Next
A	0	—
B	5	—
C	2	—
D	3	—
E	6	C

A's table

To	Cost	Next
A	5	—
B	0	—
C	4	—
D	8	A
E	3	—

B's table

To	Cost	Next
A	3	—
B	8	A
C	5	A
D	0	—
E	9	A

D's table

To	Cost	Next
A	2	—
B	4	—
C	0	—
D	5	A
E	4	—

C's table

To	Cost	Next
A	6	C
B	3	—
C	4	—
D	9	C
E	0	—

E's table

- The question now is, when does a node send its partial routing table (only two columns) to all its immediate neighbours? The table is sent both periodically and when there is a change in the table.

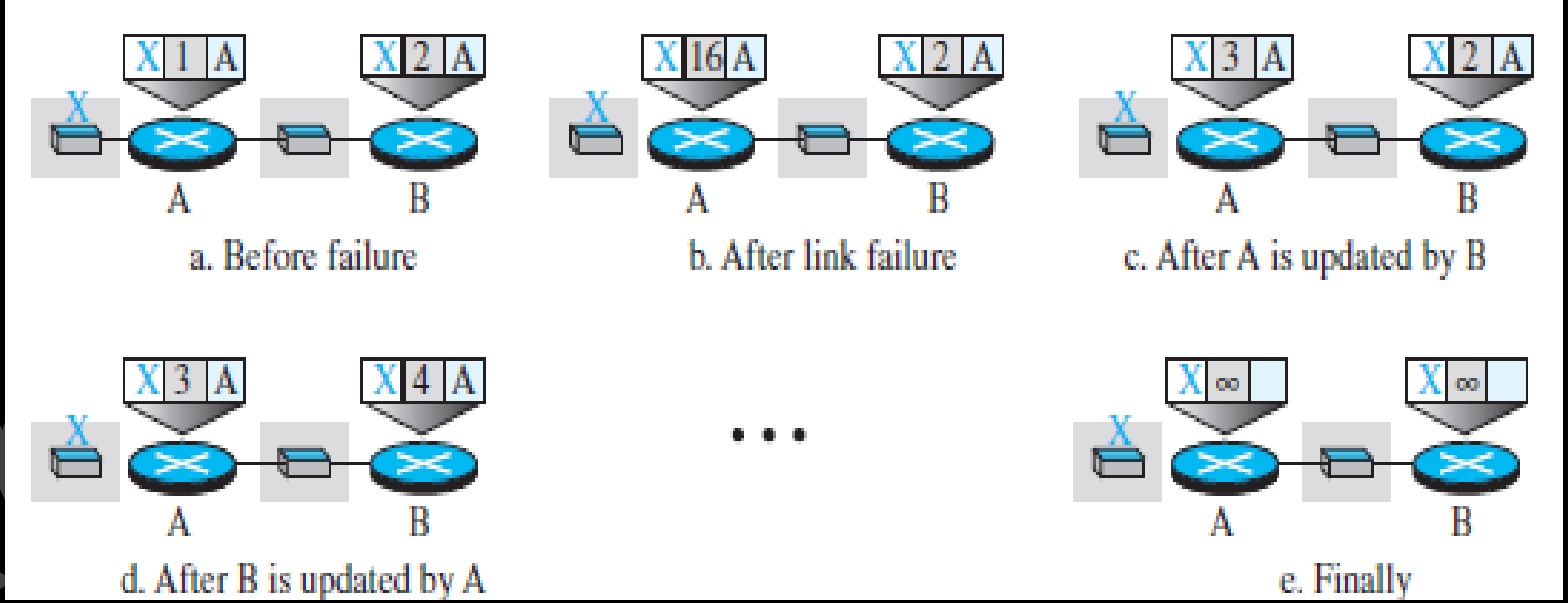
- **Periodic Update** A node sends its routing table, normally every 30 s, in a periodic update. The period depends on the protocol that is using distance vector routing.

- **Triggered Updat**e A node sends its two-column routing table to its neighbours anytime there is a change in its routing table. This is called a triggered update. The change can result from the following.
    - A node receives a table from a neighbour, resulting in changes in its own table after updating.
    - A node detects some failure in the neighbouring links which results in a distance change to infinity.

Two-Node Loop Instability

- If a link is broken (cost becomes infinity), every other router should be aware of it immediately, but in distance-vector routing, this takes some time as the algorithms is designed in such a way that it reports the minimum first.

- The problem is referred to as *count to infinity*. It sometimes takes several updates before the cost for a broken link is recorded as infinity by all routers.



a. Before failure

b. After link failure

c. After A is updated by B

d. After B is updated by A

e. Finally

Split Horizon

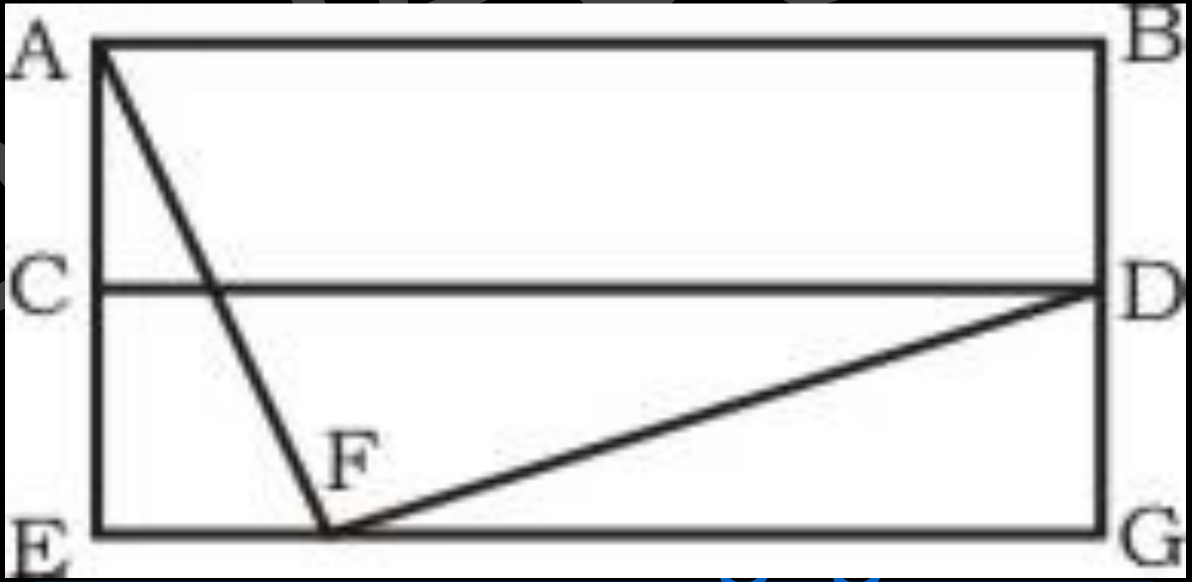
- In this strategy, instead of flooding the table through each interface, each node sends only part of its table through each interface.
- If, according to its table, node B thinks that the optimum route to reach X is via A, it does not need to advertise this piece of information to A; the information has come from A (A already knows).
- Taking information from node A, modifying it, and sending it back to node A creates the confusion. In our scenario, node B eliminates the last line of its routing table before it sends it to A.
- In this case, node A keeps the value of infinity as the distance to X. Later when node A sends its routing table to B, node B also corrects its routing table. The system becomes stable after the first update: both node A and B know that X is not reachable

Link State Routing

- Link state routing has a different philosophy from that of distance vector routing. In link state routing, if each node in the domain has the entire topology of the domain the list of nodes and links, how they are connected including the type, cost (metric), and condition of the links (up or down)-the node can use Dijkstra's algorithm to build a routing table.

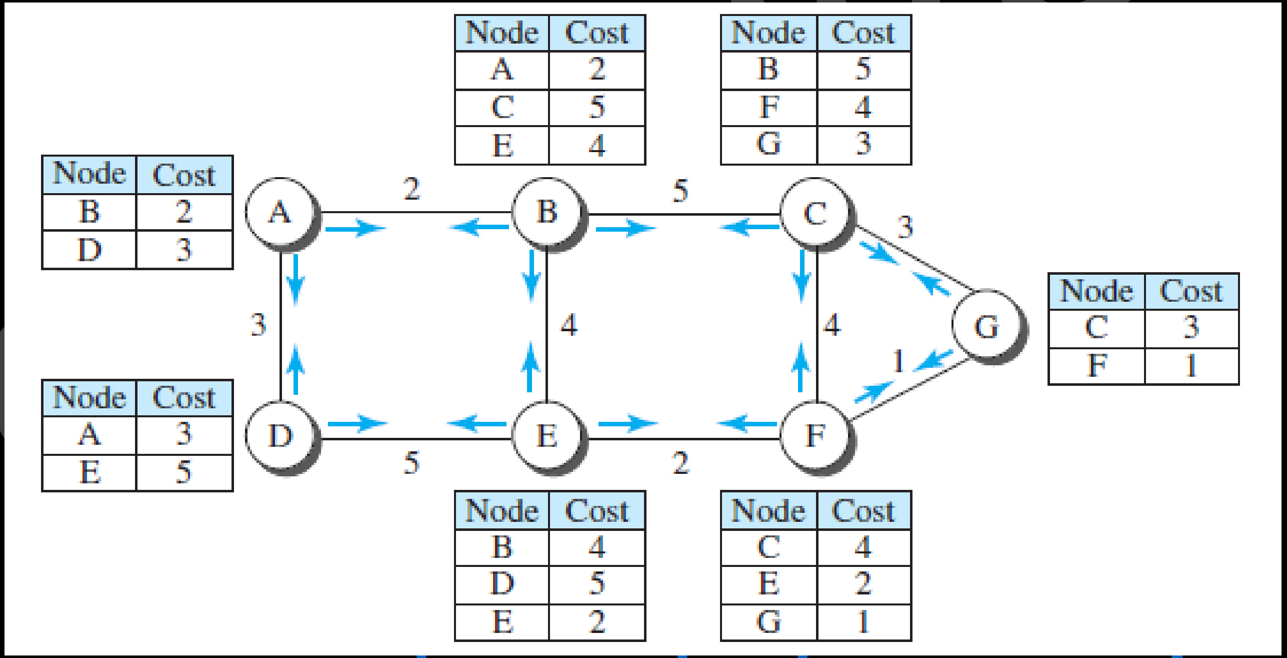
- Each node uses the same topology to create a routing table, but the routing table for each node is unique because the calculations are based on different interpretations of the topology.

- The topology must be dynamic, representing the latest state of each node and each link. If there are changes in any point in the network (a link is down, for example), the topology must be updated for each node.



Building Routing Tables

- In link state routing, four sets of actions are required to ensure that each node has the routing table showing the least-cost node to every other node.
  1. Creation of the states of the links by each node, called the link state packet (LSP).
  2. Dissemination of LSPs to every other router, called flooding, in an efficient and reliable way.
  3. Formation of a shortest path tree for each node.
  4. Calculation of a routing table based on the shortest path tree



Node	Cost
B	2
D	3

Node	Cost
A	2
C	5
E	4

Node	Cost
B	5
F	4
G	3

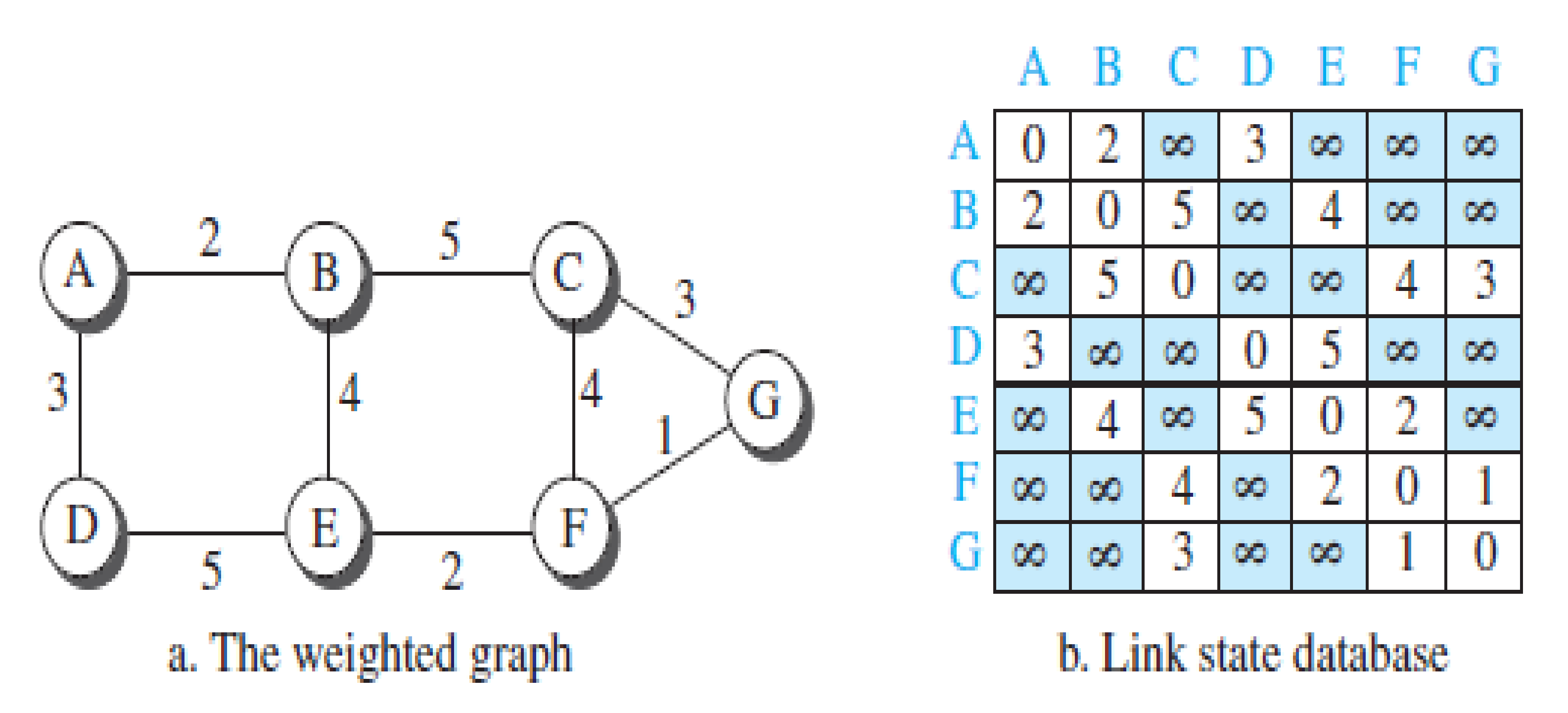
Node	Cost
C	3
F	1

Node	Cost
A	3
E	5

Node	Cost
B	4
D	5
E	2

Node	Cost
C	4
E	2
G	1

- The collection of state for all links is called the ***link-state database (LSDB).***
- There is only one LSDB for the whole internet; each node needs to have a duplicate of it to be able to create the least-cost tree.
- The LSDB can be represented as a two-dimensional array (matrix) in which the value of each cell defines the cost of the corresponding link.



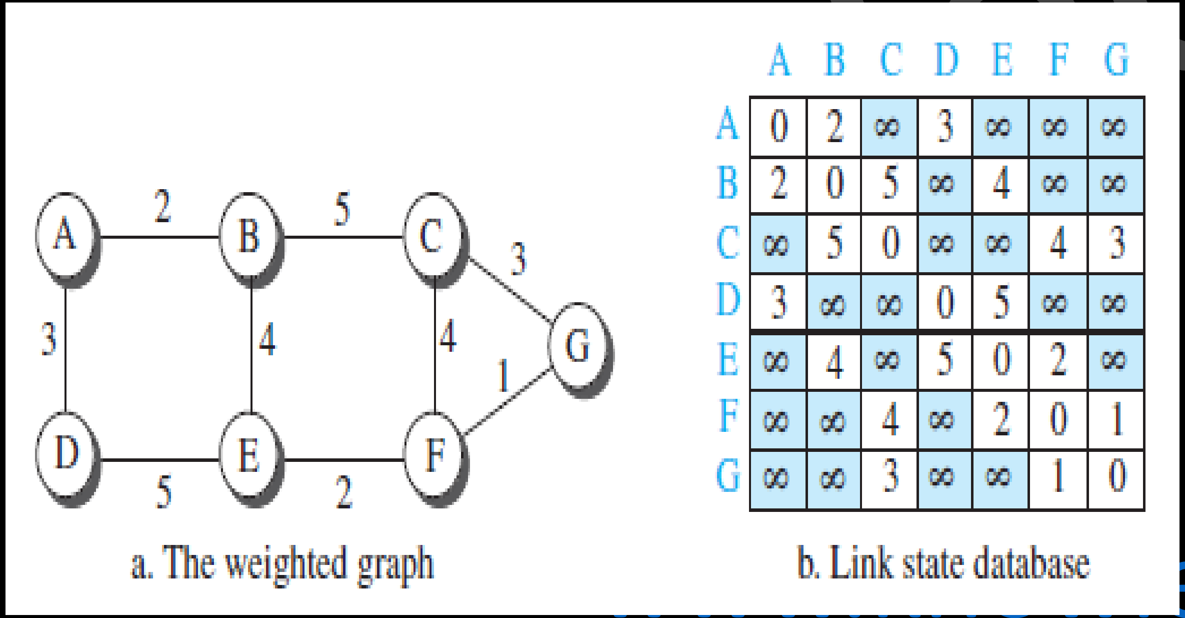
a. The weighted graph

	A	B	C	D	E	F	G
A	0	2	∞	3	∞	∞	∞
B	2	0	5	∞	4	∞	∞
C	∞	5	0	∞	∞	4	3
D	3	∞	∞	0	5	∞	∞
E	∞	4	∞	5	0	2	∞
F	∞	∞	4	∞	2	0	1
G	∞	∞	3	∞	∞	1	0

b. Link state database

- When a node receives an LSP from one of its interfaces, it compares the LSP with the copy it may already have.
  - If the newly arrived LSP is older than the one it has (found by checking the sequence number), it discards the LSP.
  - If it is newer or the first one received, the node discards the old LSP (if there is one) and keeps the received one.
  - It then sends a copy of it out of each interface except the one from which the packet arrived.

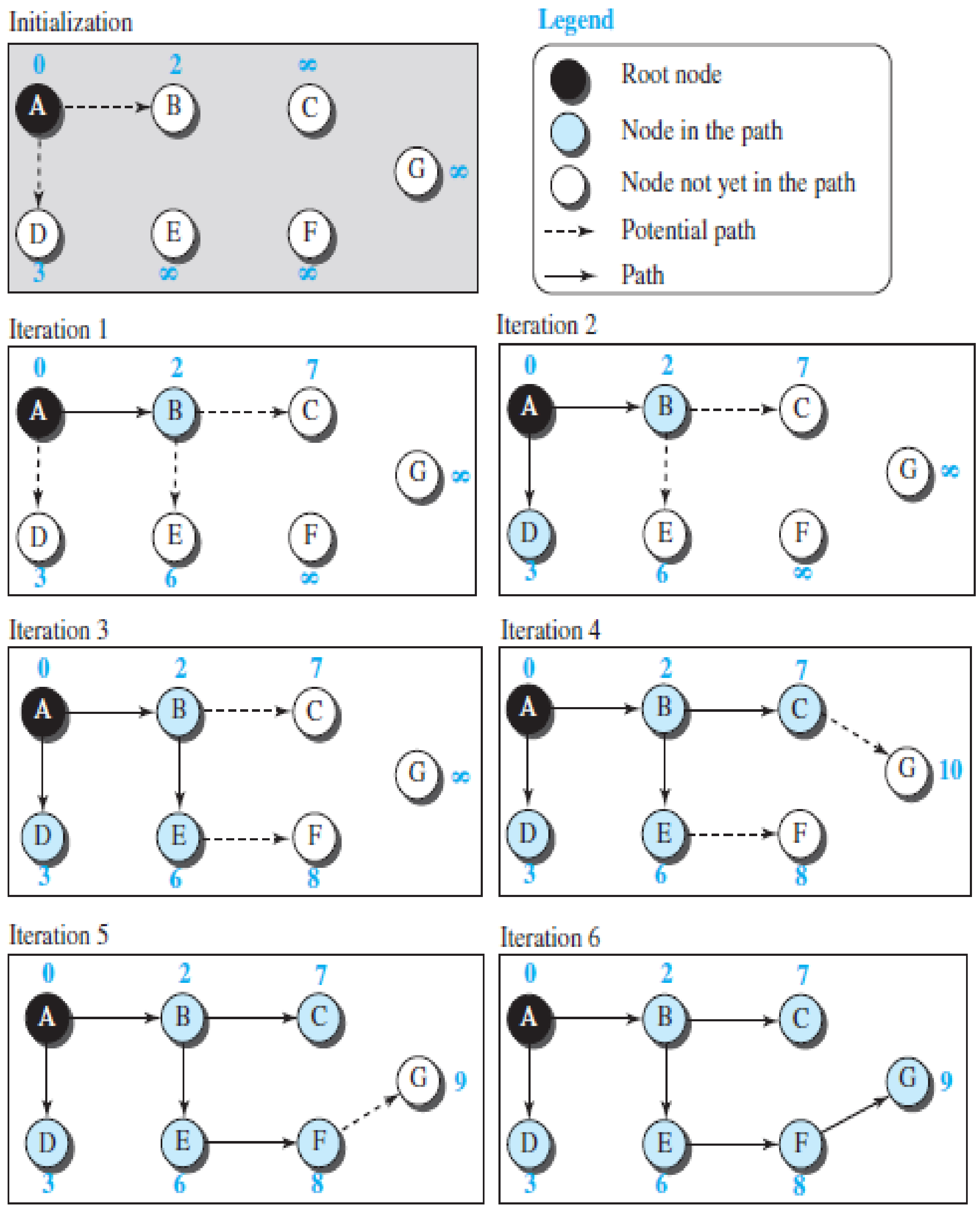
- The Dijkstra algorithm creates a shortest path tree from a graph. The algorithm divides the nodes into two sets: tentative and permanent. It finds the neighbours of a current node, makes them tentative, examines them, and if they pass the criteria, makes them permanent.
- To find the shortest path in each step, we need the cumulative cost from the root to each node, which is shown next to the node. Nodes and lists with the cumulative costs.



a. The weighted graph

	A	B	C	D	E	F	G
A	0	2	∞	3	∞	∞	∞
B	2	0	5	∞	4	∞	∞
C	∞	5	0	∞	∞	4	3
D	3	∞	∞	0	5	∞	∞
E	∞	4	∞	5	0	2	∞
F	∞	∞	4	∞	2	0	1
G	∞	∞	3	∞	∞	1	0

b. Link state database

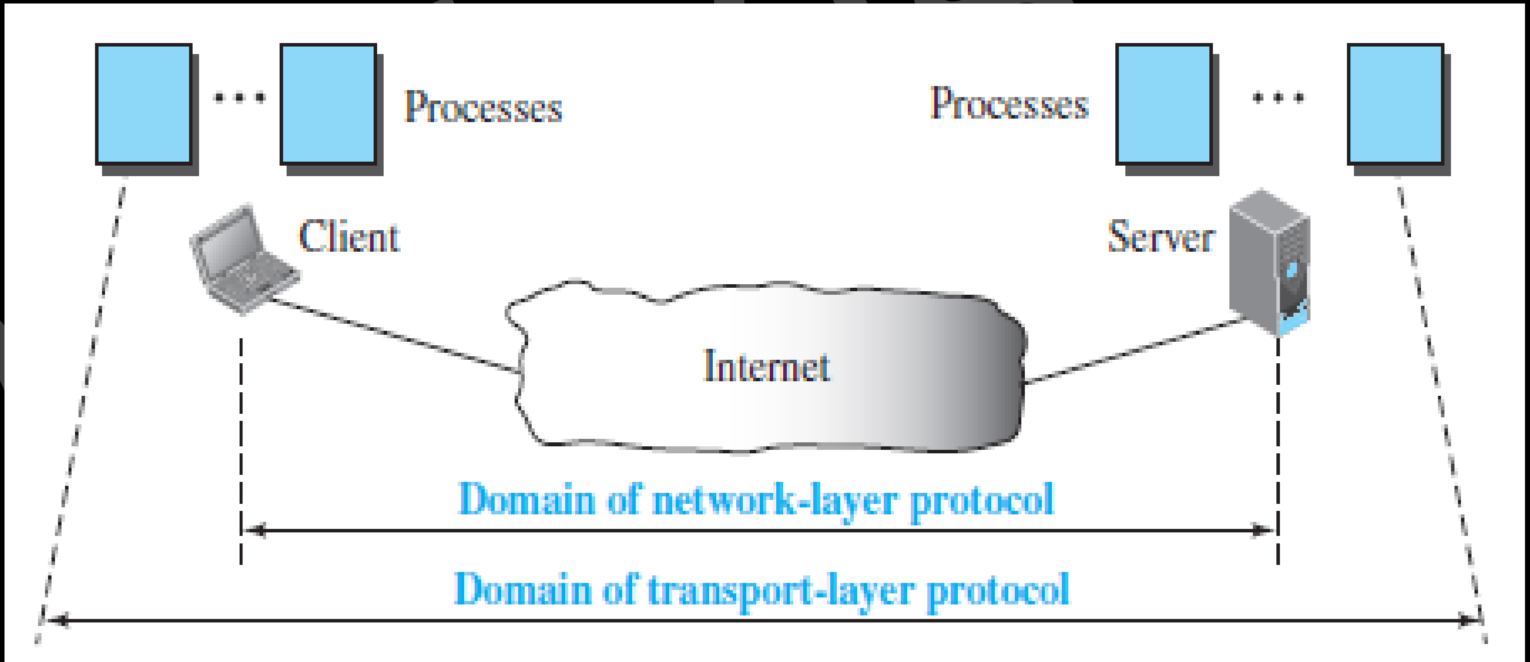


Difference between DVR and LSR

• In the distance-vector routing algorithm, each router tells its neighbours what it knows about the whole internet.	• In the link-state routing algorithm, each router tells the whole internet what it knows about its neighbours.
• Was most popularly used around 1980’s	• Was most popularly used around 1990’s
• Based on the idea of Local Knowledge	• Based on the idea of Global Knowledge
• Bandwidth requirement is Less	• Bandwidth requirement is high
• Roughly based on the idea of Bellman-Ford Algo	• Directly based on the idea of Dijkstra’s
• Traffic is usually less	• Traffic is Usually high
• Converge slowly	• Converge faster
• Counts to Infinity	• No Counts to infinity
• RIP	• OSPF

Transport-Layer Services

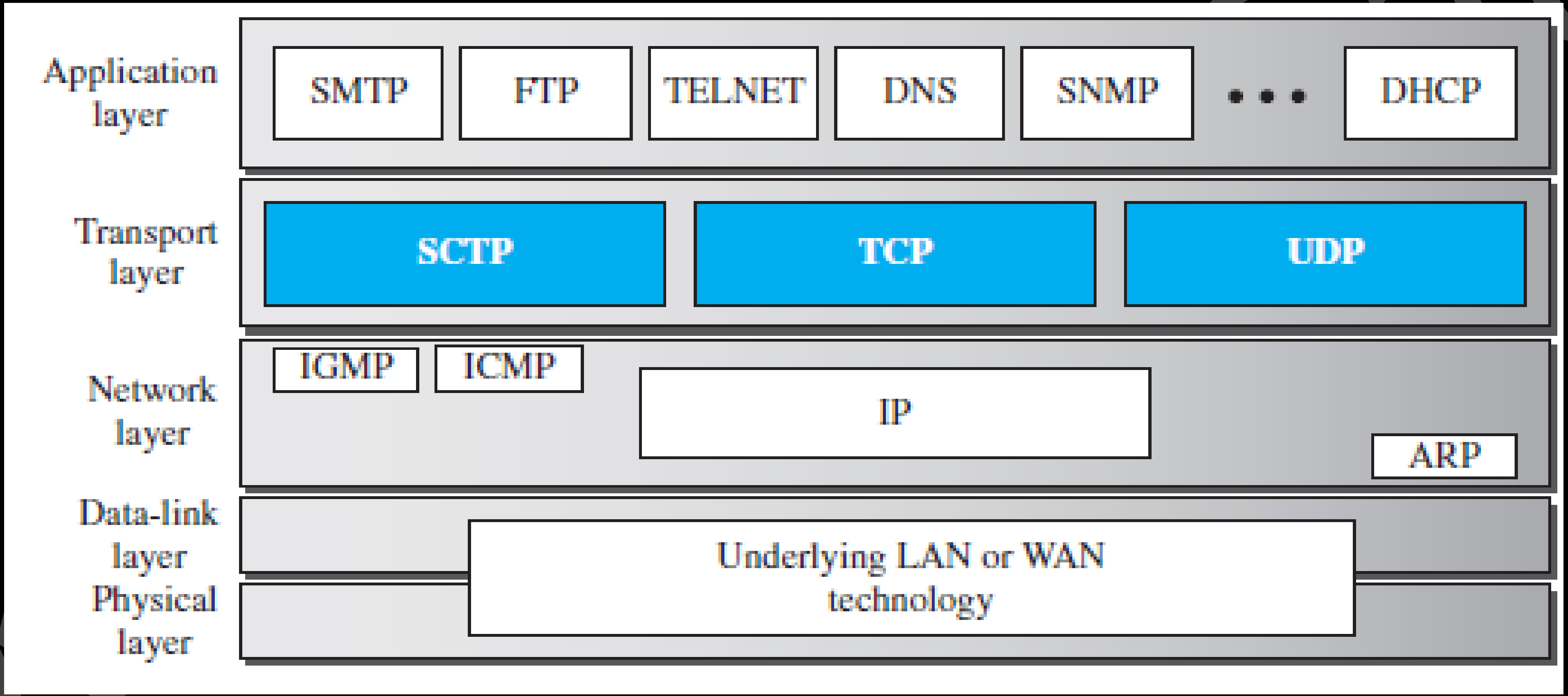
- The network layer is responsible for communication at the computer level (host-to-host communication). A network-layer protocol can deliver the message only to the destination computer.
- However, this is an incomplete delivery, as the message still needs to be handed to the correct process. A transport-layer protocol is responsible for delivery of the message to the appropriate process. TL provides end to end or process to process communication.


Processes
Processes
Client
Server
Internet
Domain of network-layer protocol
Domain of transport-layer protocol

- A transport layer protocol can be either connectionless or connection-oriented.
  - A connectionless transport layer treats each segment as an independent packet and delivers it to the transport layer at the destination machine.
  - A connection-oriented transport layer makes a connection with the transport layer at the destination machine first before delivering the packets. After all the data is transferred, the connection is terminated.

- Reliable Versus Unreliable
  - If the application layer program needs reliability, we use a reliable transport layer protocol by implementing flow and error control at the transport layer. This means a slower and more complex service.
  - On the other hand, if the application program does not need reliability because it uses its own flow and error control mechanism or it needs fast service or the nature of the service does not demand flow and error control (real-time applications), then an unreliable protocol can be used.

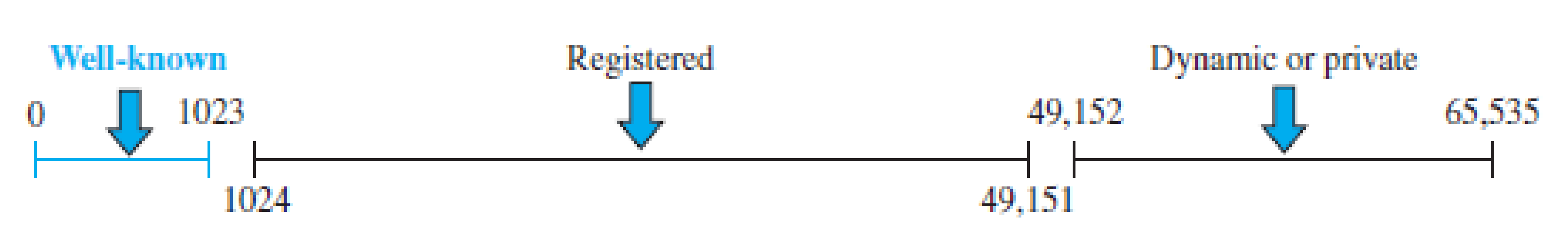
- There are three common different transport layer protocols.
  - UDP is connectionless and unreliable;
  - TCP and SCTP are connection oriented and reliable. These three can respond to the demands of the application layer programs.



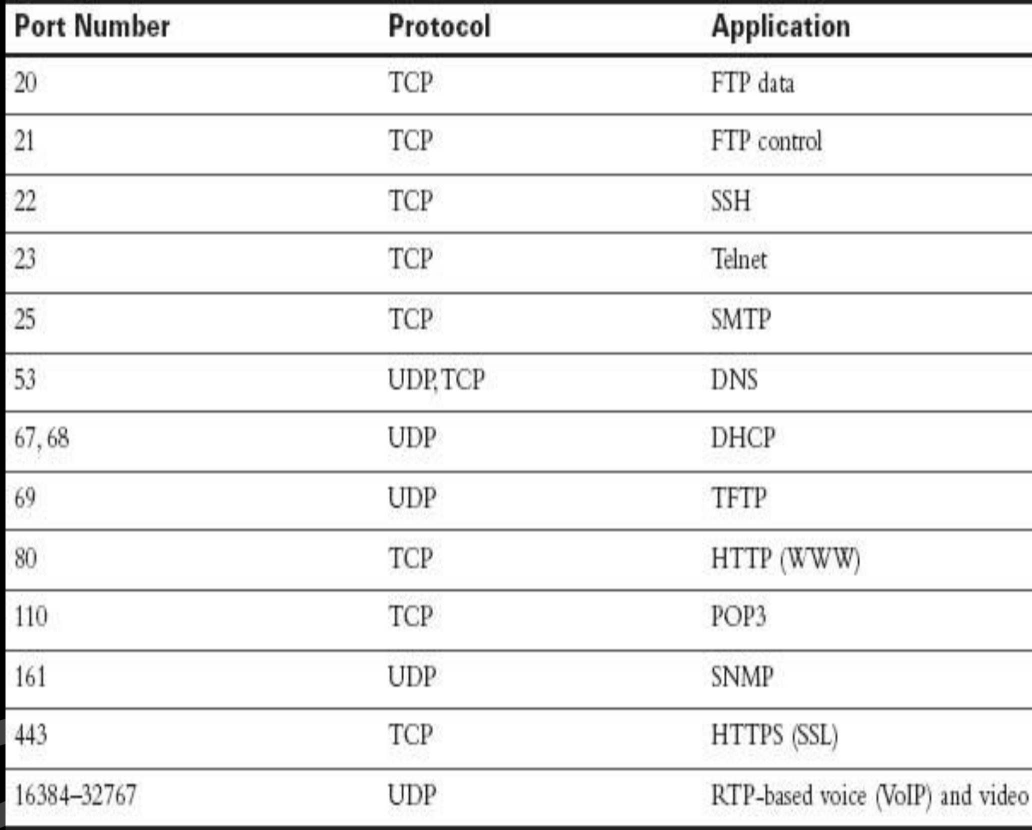
Addressing: Port Numbers

- For communication, we must define the local host, local process, remote host, and remote process. Local and Remote host are defined by IP Addresses. To define the processes inside a host, we need second identifiers, called port numbers, they are 16-bits integers ranging from (0 to $2^{16} – 1$) or (0 to 65535).

- The IANA (Internet Assigned Number Authority) has divided the port numbers into three ranges: well known, registered, and dynamic (or private).



- **Well-known ports:**
  - The ports ranging from 0 to 1023 are assigned and controlled by IANA. The server process must also define itself with a port number. This port number, however, cannot be chosen randomly as the client has to request the data from server.
- **Registered ports:**
  - The ports ranging from 1024 to 49,151 are not assigned or controlled by IANA. They can only be registered with IANA to prevent duplication.
- **Dynamic/Ephemeral ports:**
  - The ports ranging from 49,152 to 65,535 are neither controlled nor registered. They can be used by any process.
  - The client program defines itself with a port number, chosen randomly by the transport layer software running on the client host.
  - Ephemeral means “short-lived” and is used because the life of a client is normally short.

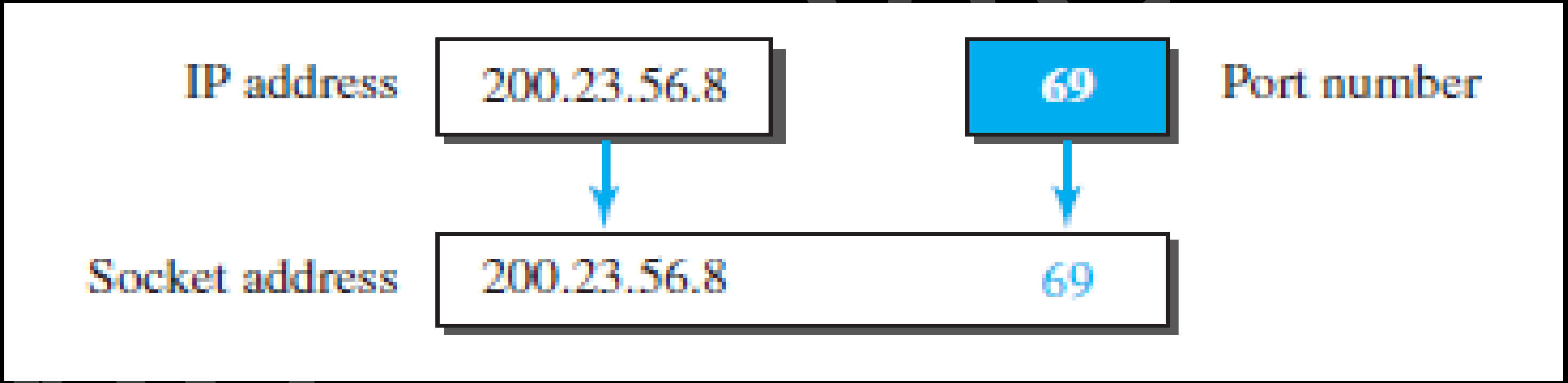


Port Number	Protocol	Application
20	TCP	FTP data
21	TCP	FTP control
22	TCP	SSH
23	TCP	Telnet
25	TCP	SMTP
53	UDP, TCP	DNS
67, 68	UDP	DHCP
69	UDP	TFTP
80	TCP	HTTP (WWW)
110	TCP	POP3
161	UDP	SNMP
443	TCP	HTTPS (SSL)
16384–32767	UDP	RTP-based voice (VoIP) and video

Socket Addresses

- A transport-layer protocol in the TCP suite needs both the IP address and the port number, at each end, to make a connection. To use the services of the transport layer in the Internet, we need a pair of socket addresses: the client socket address and the server socket address.

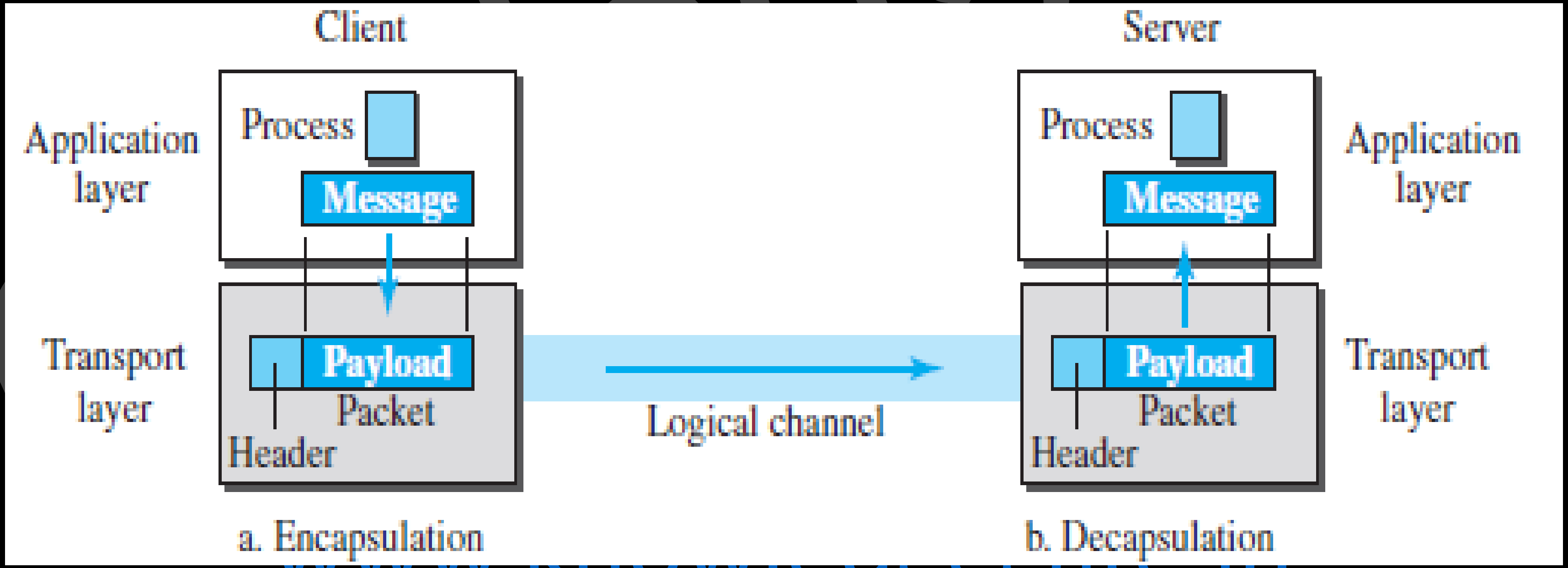
- The combination of an IP address and a port number is called a ***socket address.***



Encapsulation and Decapsulation

- Encapsulation happens at the sender site. When a process has a message to send, it passes the message to the transport layer along with a pair of socket addresses. The transport layer receives the data and adds the transport-layer header. The packets at the transport layer in the Internet are called ***segments.***

- Decapsulation happens at the receiver site. When the message arrives at the destination transport layer, the header is dropped and the transport layer delivers the message to the process running at the application layer.

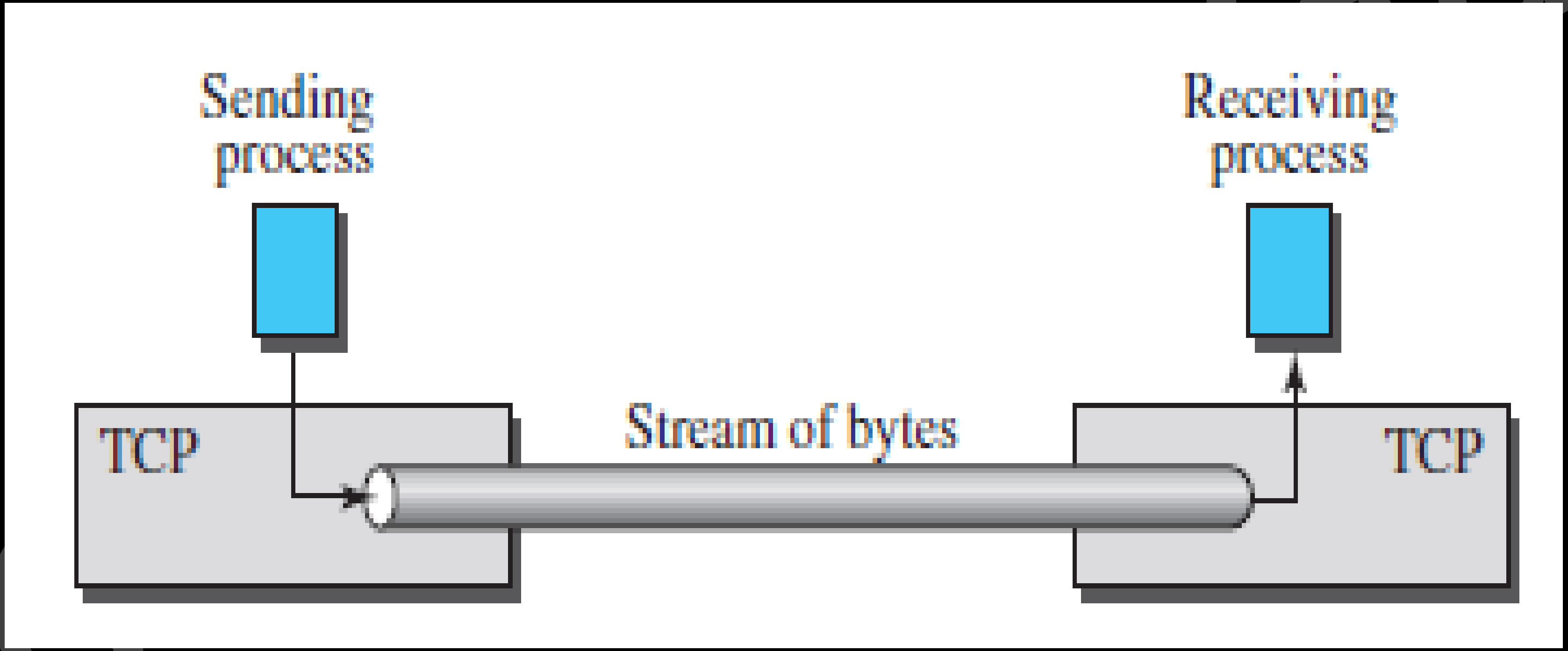


a. Encapsulation

b. Decapsulation

TCP (Transmission Control Protocol)

- TCP creates a virtual connection between two TCPs to send data. TCP allows the sending process to deliver data as a stream of bytes and allows 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.



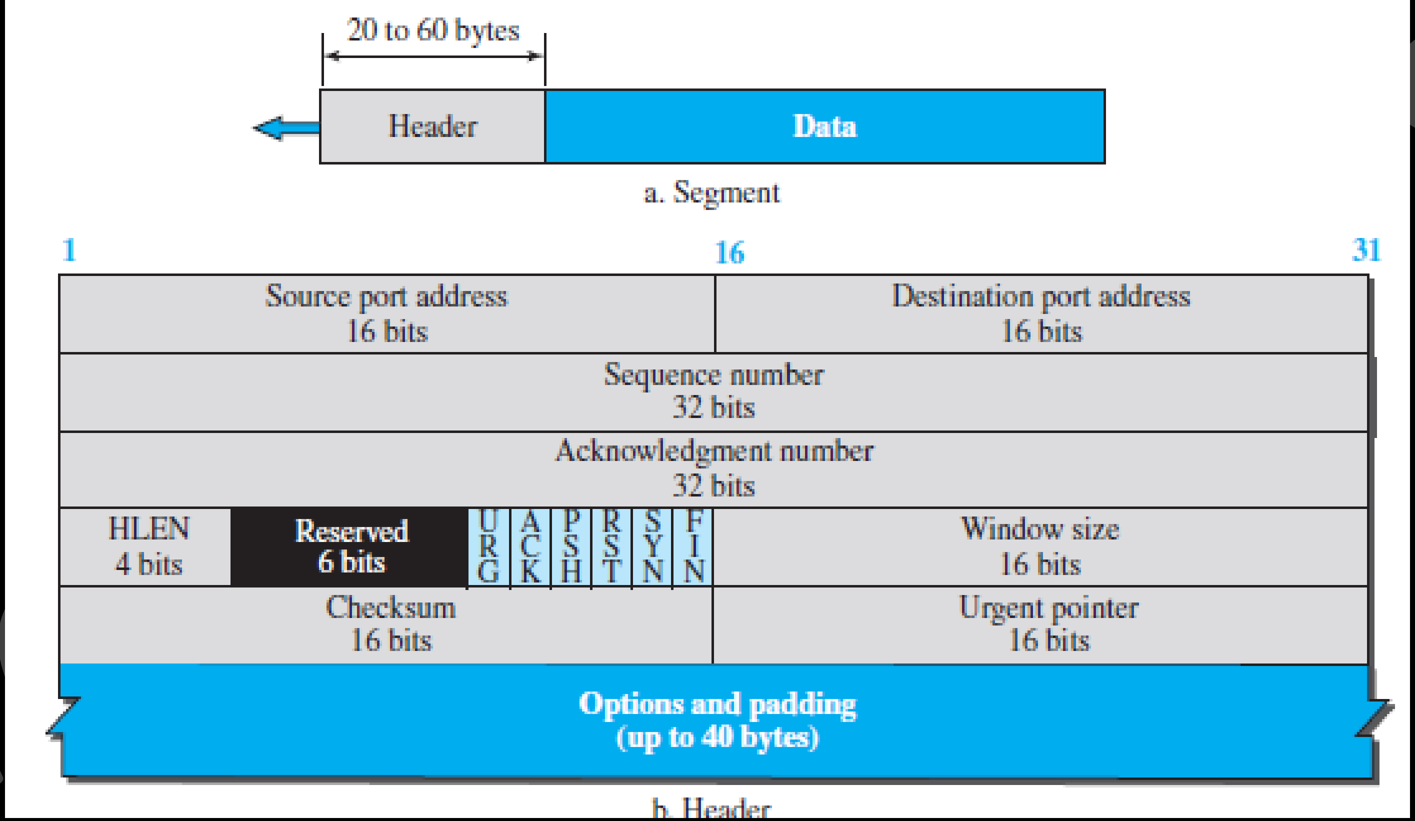
- **Flow Control**
  - The receiver of the data controls the amount of data that are to be sent by the sender. This is done to prevent the receiver from being overwhelmed with data. The numbering system allows TCP to use a byte-oriented flow control.

- **Error Control**
  - To provide reliable service, TCP implements an error control mechanism. Although error control considers a segment as the unit of data for error detection (loss or corrupted segments), error control is byte-oriented.

- **Congestion Control**
  - TCP, unlike UDP, takes into account congestion in the network. The amount of data sent by a sender is not only controlled by the receiver (flow control), but is also determined by the level of congestion in the network.

TCP Header

- The segment consists of a 20- to 60-byte header, followed by data from the application program. The header is 20 bytes if there are no options and up to 60 bytes if it contains options.



a. Segment

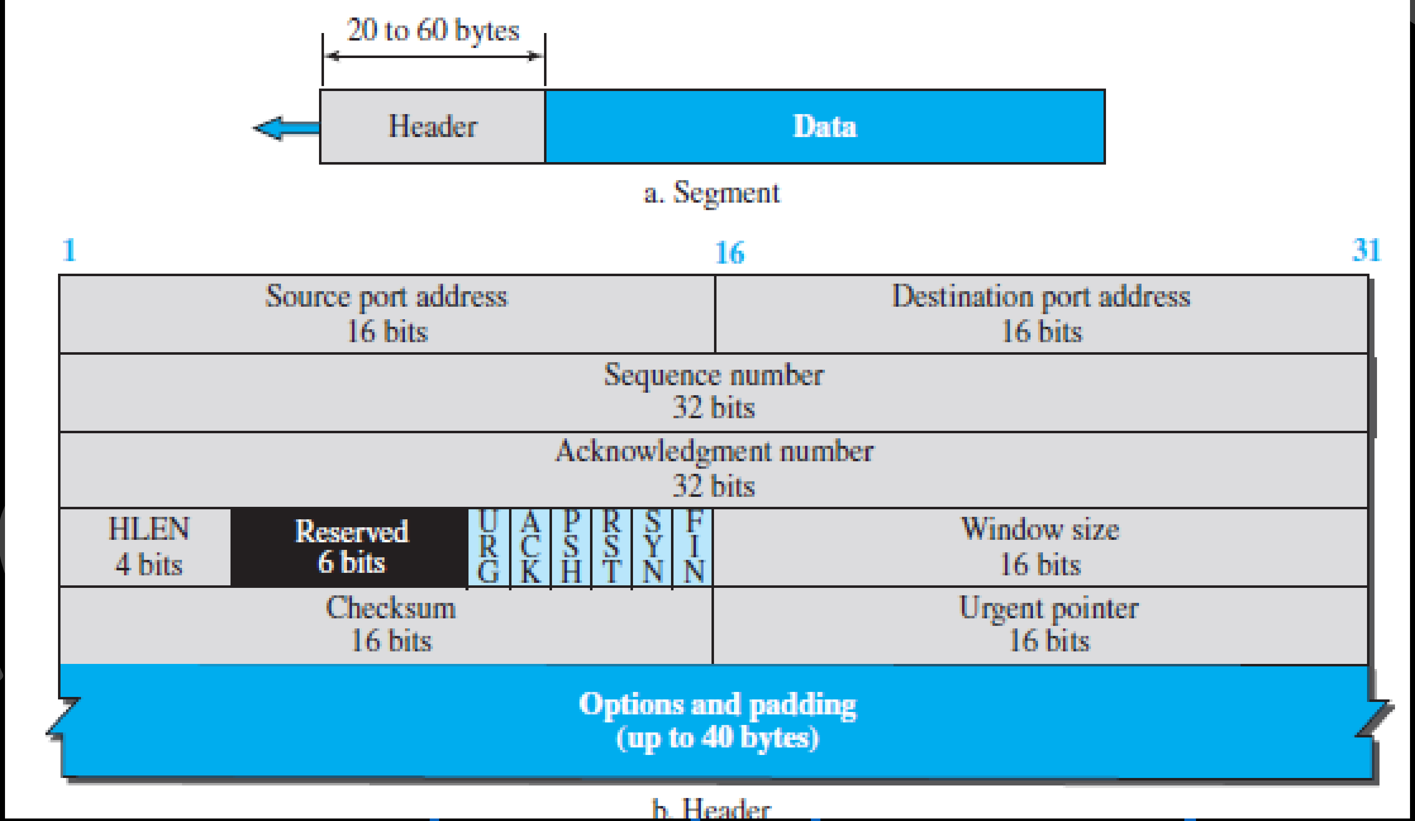
Source port address 16 bits
Destination port address 16 bits
Sequence number 32 bits
Acknowledgment number 32 bits
HLEN 4 bits
Reserved 6 bits
URG
ACK
PSH
RST
SYN
FIN
Window size 16 bits
Checksum 16 bits
Urgent pointer 16 bits
Options and padding (up to 40 bytes)

b. Header

Source & Destination port address

- **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.



a. Segment

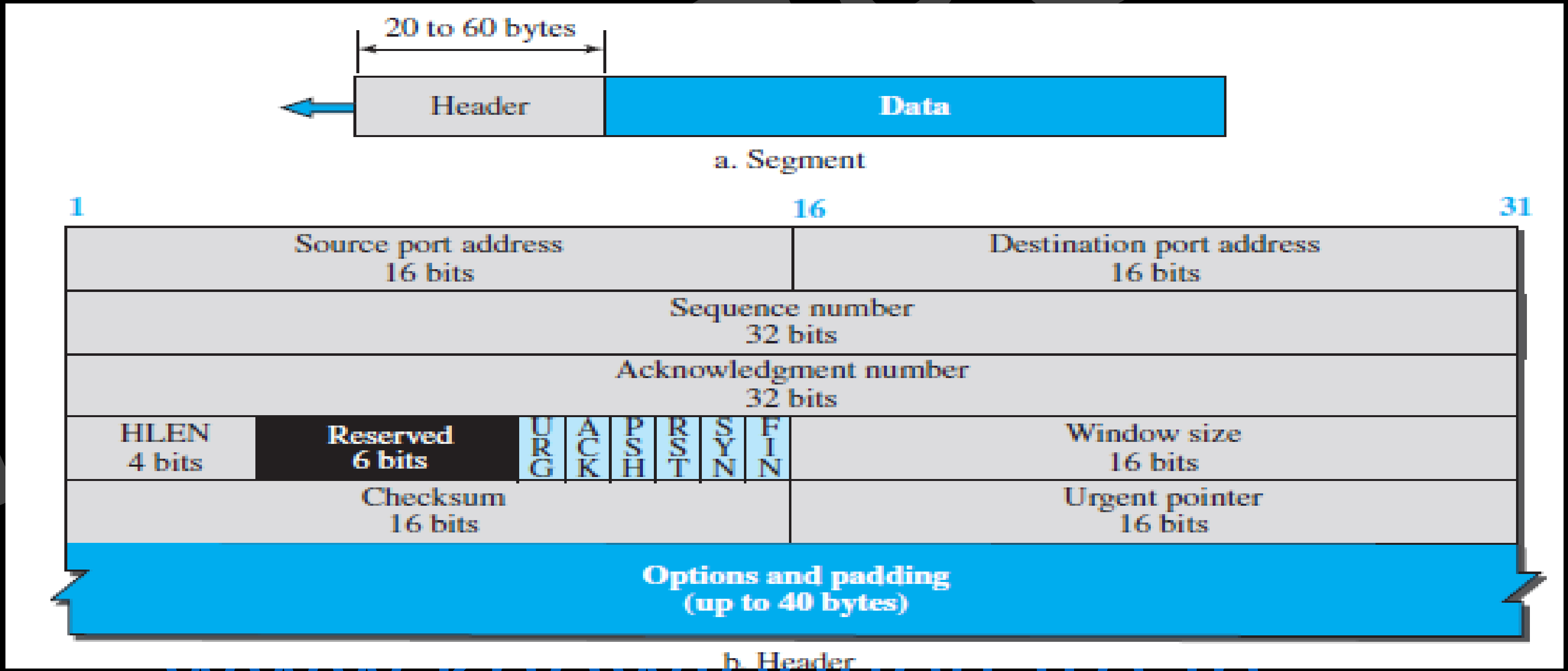
Source port address 16 bits			Destination port address 16 bits
Sequence number 32 bits			
Acknowledgment number 32 bits			
HLEN 4 bits	Reserved 6 bits	URG ACK PSH RST SYN FIN	Window size 16 bits
Checksum 16 bits			Urgent pointer 16 bits
Options and padding (up to 40 bytes)			

b. Header

Sequence number

- TCP is a stream transport protocol. To ensure connectivity, each byte to be transmitted is numbered. Sequence number is 32-bit field defines the number assigned to the first byte of data contained in this segment. So, maximum number of possible sequence numbers = 2^{32}. These sequence numbers lie in the range [0, $2^{32} – 1$].

- During connection establishment, each party uses a random number generator to create an initial sequence number (ISN), which is usually different in each direction. Sequence number should be started at random, to remove duplication problem. The sequence number of any other segment is the sequence number of the previous segment plus the number of bytes (real or imaginary) carried by the previous segment.



a. Segment

Source port address 16 bits | Destination port address 16 bits

Sequence number 32 bits

Acknowledgment number 32 bits

HLEN 4 bits | Reserved 6 bits | URG | ACK | PSH | RST | SYN | FIN | Window size 16 bits

Checksum 16 bits | Urgent pointer 16 bits

Options and padding (up to 40 bytes)

b. Header

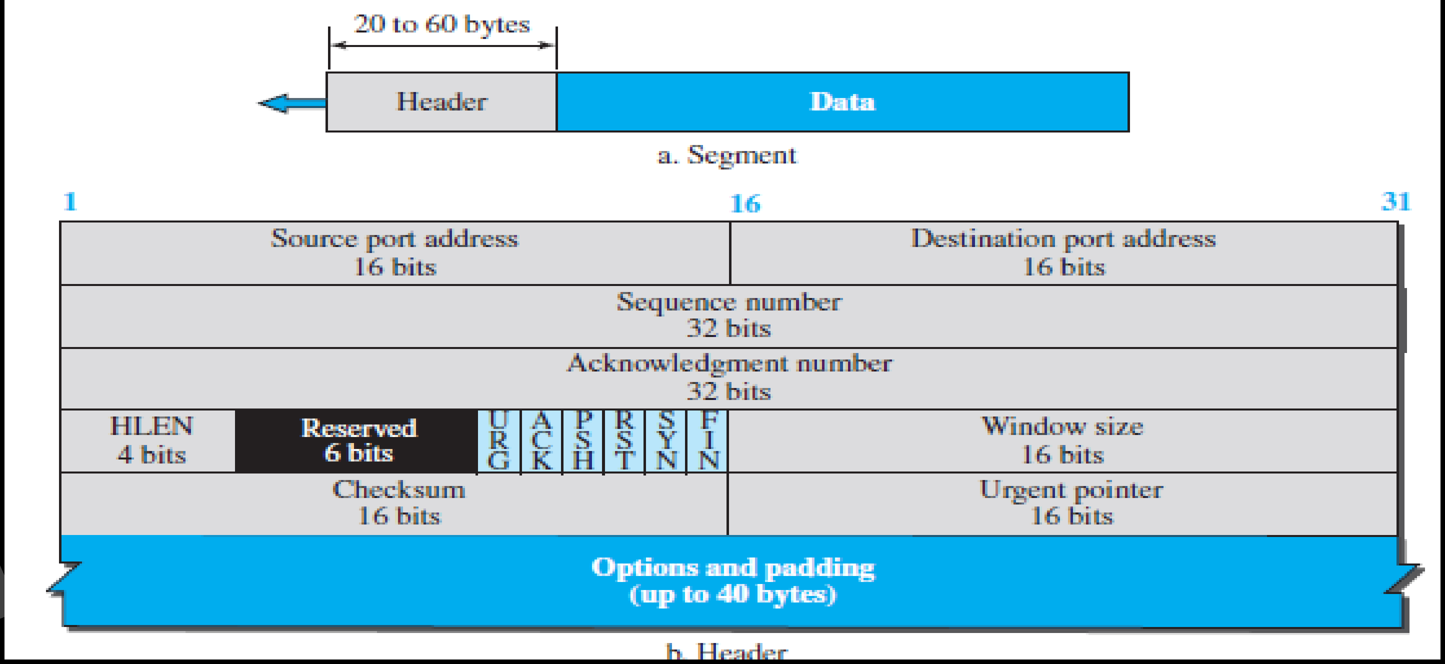
- This does not imply that only 2^{32} bytes = 4 GB data can be sent using TCP. The concept of wrap around allows to send unlimited data using TCP.

- After all the 2^{32} sequence numbers are used up and more data is to be sent, the sequence numbers can be wrapped around and used again from the starting.

Acknowledgment Number

- If the receiver of the segment has successfully received byte number x from the other party, it defines x + 1 as the acknowledgment number. Acknowledgment and data can be piggybacked together.

- The acknowledgment number is cumulative, which means that the party takes the number of the last byte that it has received, safe and sound, adds 1 to it, and announces this sum as the acknowledgment number.

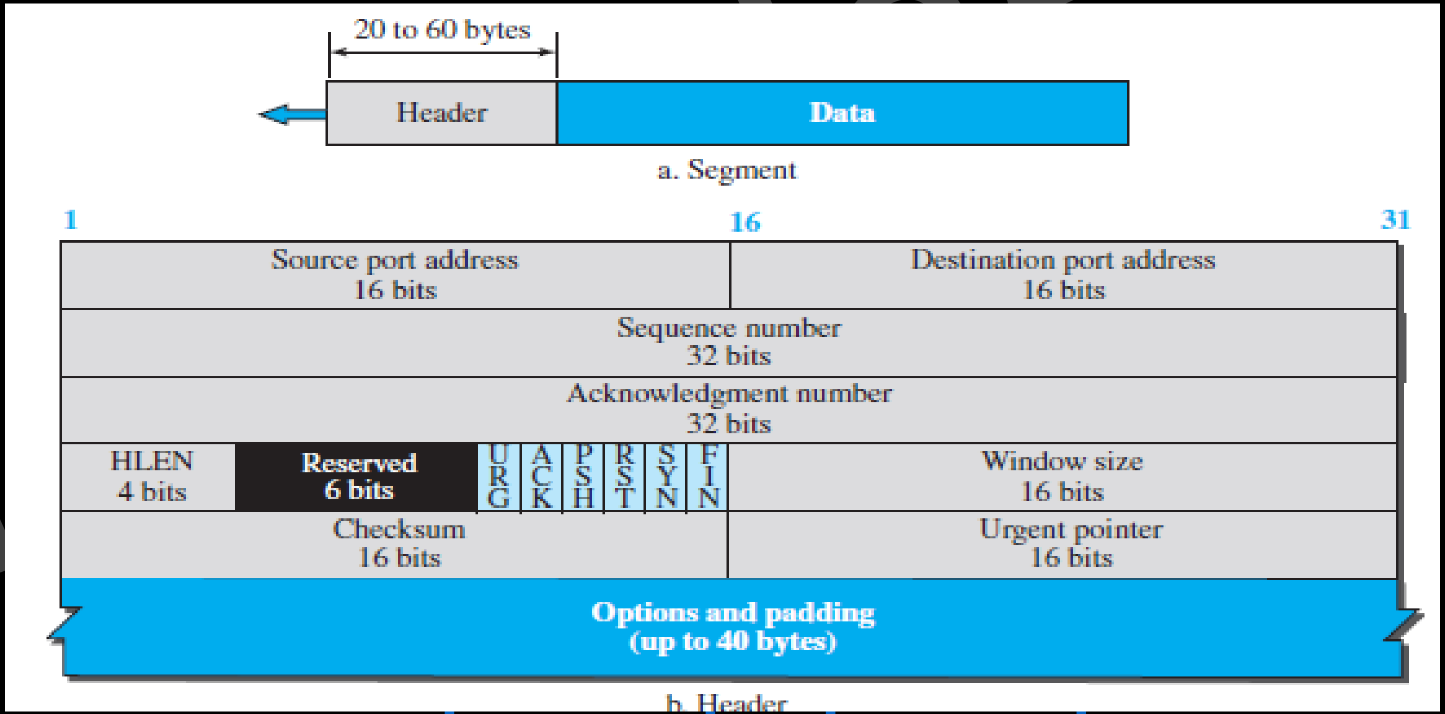


Header length

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

- Concept of Scaling Factor
  - *Header length = Header length field value x 4 bytes*

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



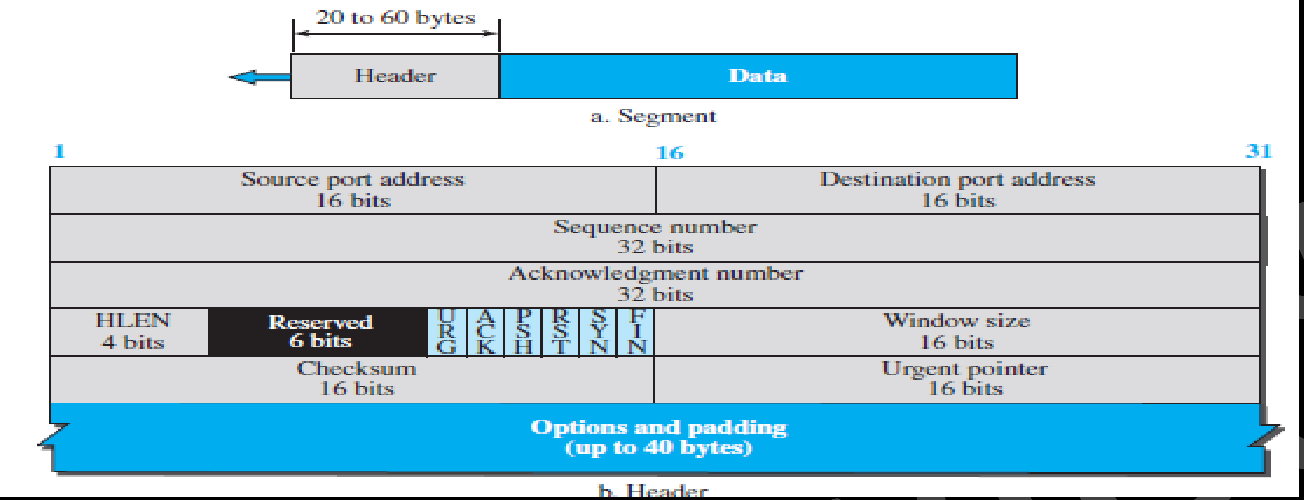
a. Segment

Source port address 16 bits								Destination port address 16 bits
Sequence number 32 bits								
Acknowledgment number 32 bits								
HLEN 4 bits	Reserved 6 bits	URG	ACK	PSH	RST	SYN	FIN	Window size 16 bits
Checksum 16 bits								Urgent pointer 16 bits
Options and padding (up to 40 bytes)								

b. Header

Checksum

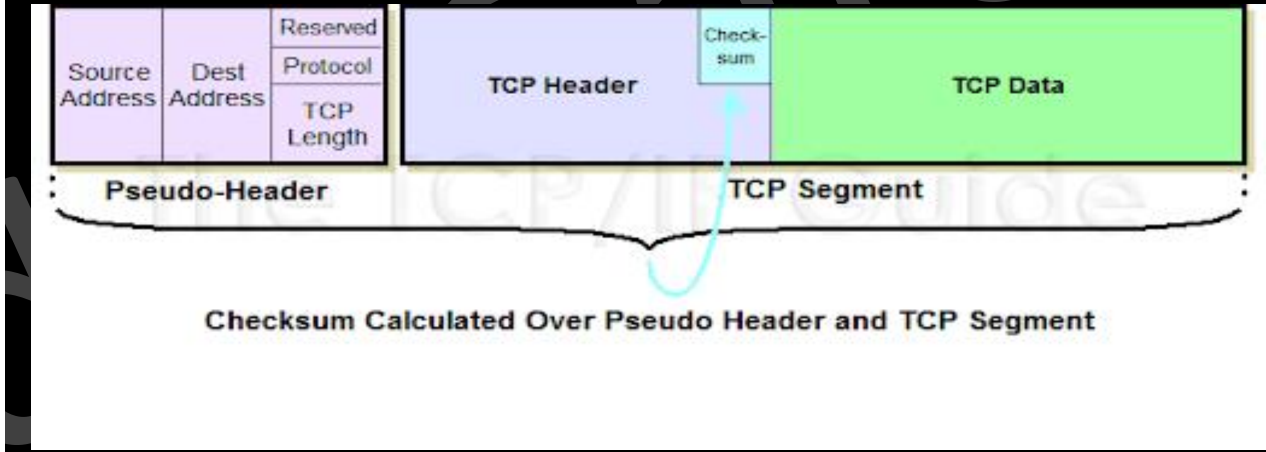
- **Checksum:** This 16-bit field contains the checksum.
- While calculation of the checksum for TCP, Entire TCP segment and pseudo header (IP) is considered.
- For the TCP pseudo header, the value for the protocol field is 6.



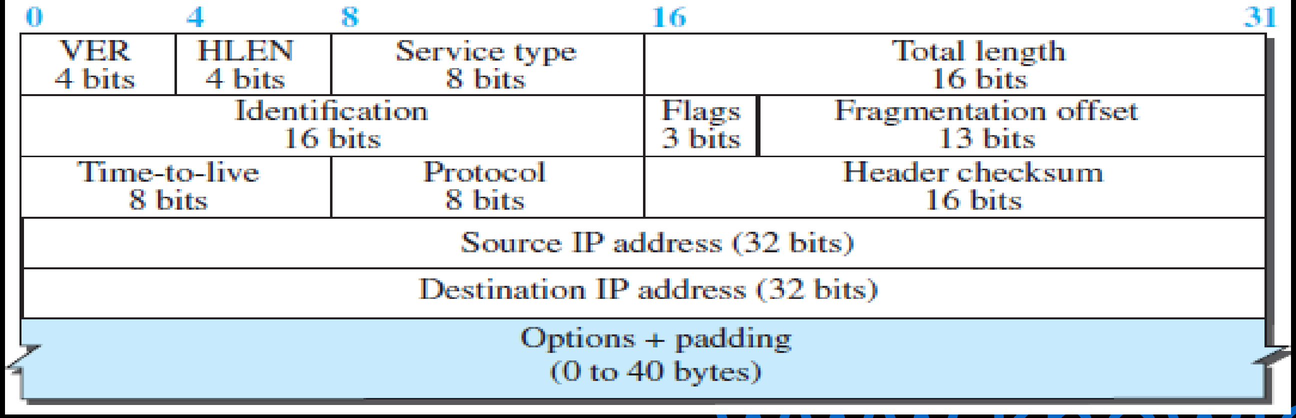
a. Segment

<table>
<tr><td colspan="8">1 … 16</td><td>31</td></tr>
<tr><td colspan="8">Source port address
16 bits</td><td>Destination port address
16 bits</td></tr>
<tr><td colspan="9">Sequence number
32 bits</td></tr>
<tr><td colspan="9">Acknowledgment number
32 bits</td></tr>
<tr><td>HLEN
4 bits</td><td>Reserved
6 bits</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td>Window size
16 bits</td></tr>
<tr><td colspan="8">Checksum
16 bits</td><td>Urgent pointer
16 bits</td></tr>
<tr><td colspan="9">Options and padding
(up to 40 bytes)</td></tr>
</table>

b. Header



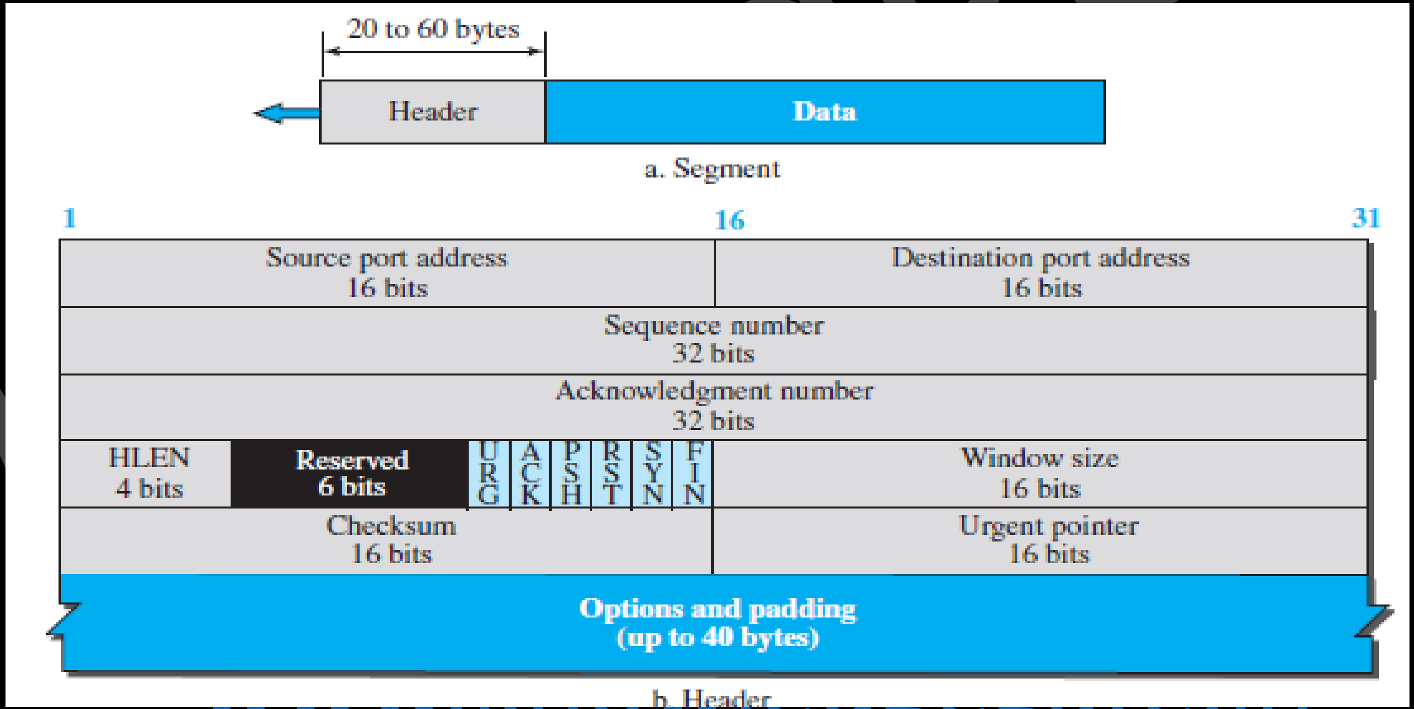
Checksum Calculated Over Pseudo Header and TCP Segment



<table>
<tr><td>0</td><td>4</td><td>8</td><td>16</td><td>31</td></tr>
<tr><td>VER
4 bits</td><td>HLEN
4 bits</td><td>Service type
8 bits</td><td colspan="2">Total length
16 bits</td></tr>
<tr><td colspan="3">Identification
16 bits</td><td>Flags
3 bits</td><td>Fragmentation offset
13 bits</td></tr>
<tr><td colspan="2">Time-to-live
8 bits</td><td>Protocol
8 bits</td><td colspan="2">Header checksum
16 bits</td></tr>
<tr><td colspan="5">Source IP address (32 bits)</td></tr>
<tr><td colspan="5">Destination IP address (32 bits)</td></tr>
<tr><td colspan="5">Options + padding
(0 to 40 bytes)</td></tr>
</table>

Window Size/Advertisement window(Flow control)

- Basics idea is a sender should never send what a receiver can not receive. Window size: This field defines the size of the window, in bytes, that the receiver have reserved for the incoming data from sender.
- Note that the length of this field is 16 bits, which means that the maximum size of the window is 65,535 bytes. This value is normally referred to as the receiving window and is determined by the receiver. The sender must obey the dictation of the receiver in this case.
- One problem with this idea is window size is only 16 bits long, so very small amount of data can be advertise in todays world context.A solution is additional 14 bits can be taken from options so total size become 30 bits or 1GB.



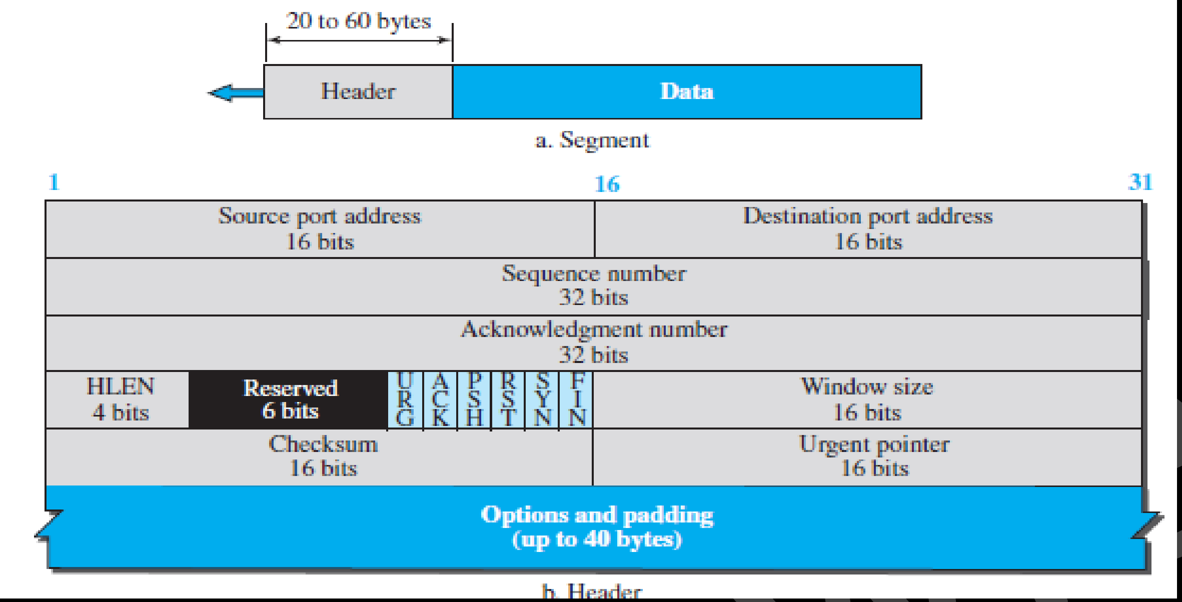
a. Segment

b. Header

Control Flag

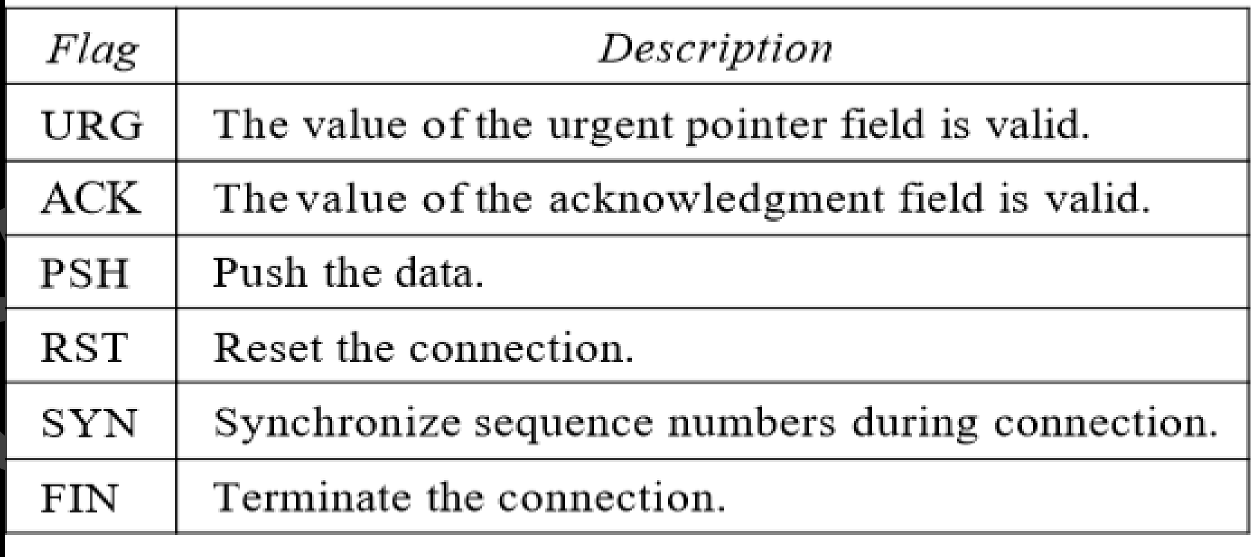
- **Control Flag:** This field defines 6 different control bits or flags. One or more of these bits can be set at a time.

- These bits enable flow control, connection establishment and termination, connection abortion, and the mode of data transfer in TCP.



a. Segment

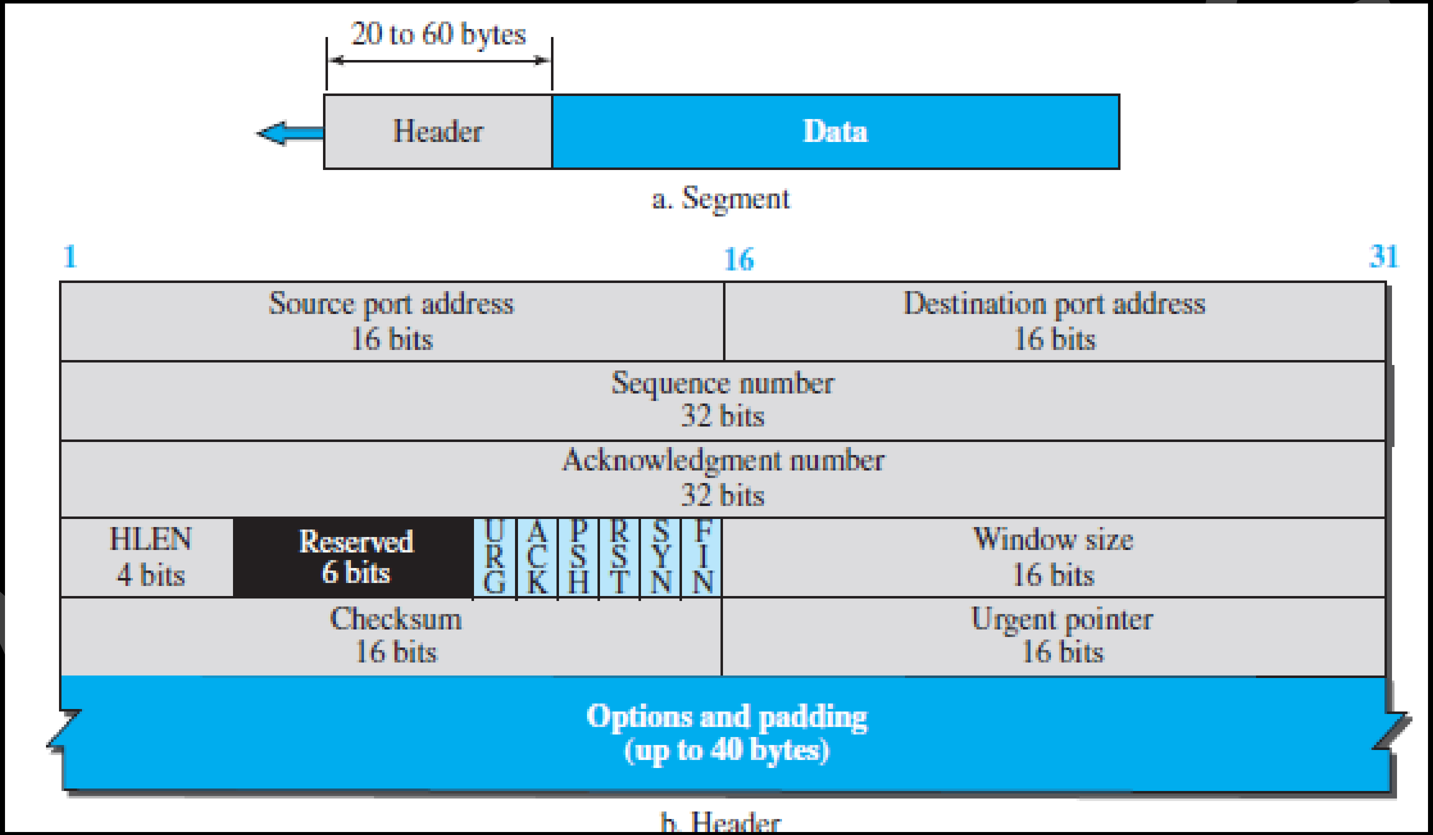
b. Header



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

Urgent pointer

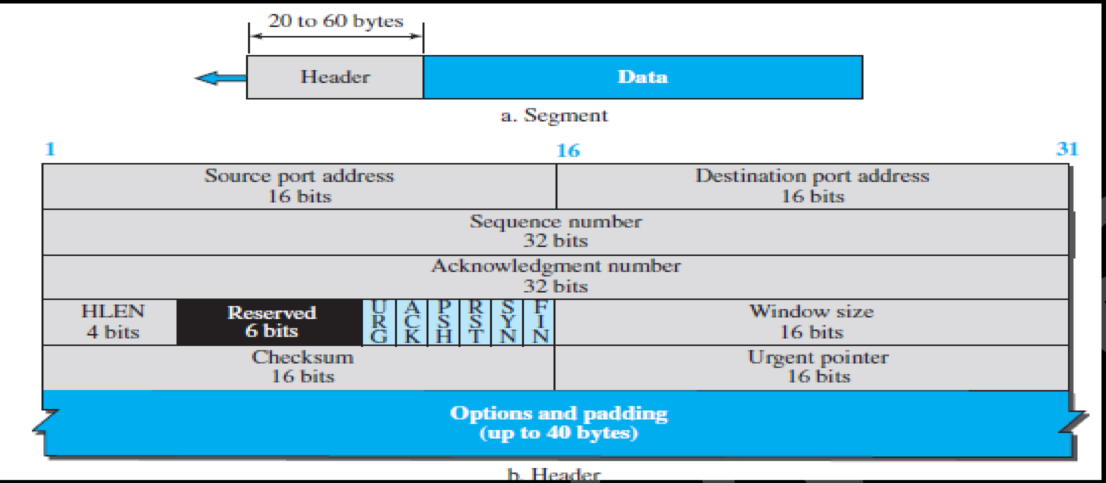
- **Urgent pointer:** This 16-bit field, which is valid only if the urgent flag is set, is used when the segment contains urgent data. It defines the number that must be added to the sequence number to obtain the number of the last urgent byte in the data section of the segment.

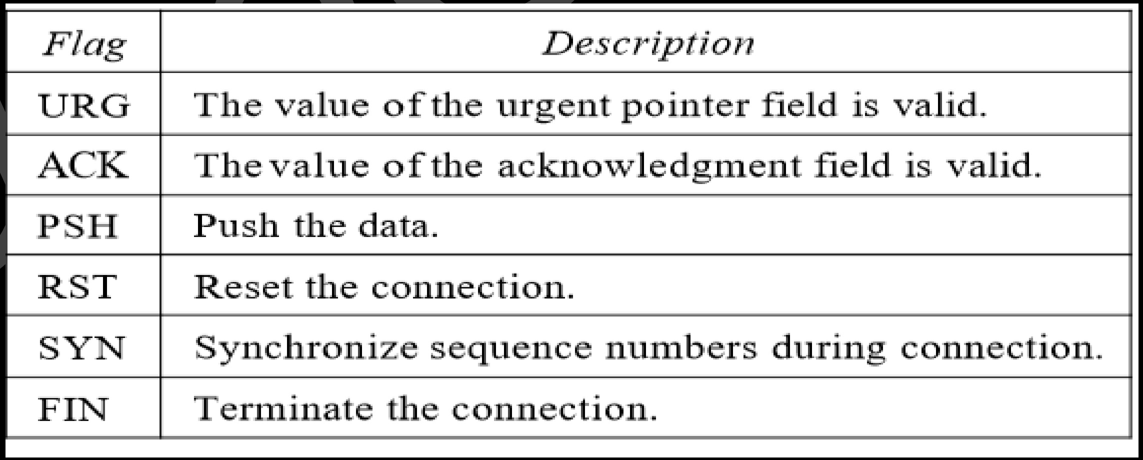


b. Header

PUSH Flag

- **Push (PSH) –** Transport layer by default waits for some time for application layer to send enough data equal to maximum segment size so that the number of packets transmitted on network minimizes which is not desirable by some application like interactive applications(chatting).
- This problem is solved by using PSH. Transport layer sets PSH = 1 and immediately sends the segment to network layer as soon as it receives signal from application layer. Receiver transport layer, on seeing PSH = 1 immediately forwards the data to application layer. In general, it tells the receiver to process these packets as they are received instead of buffering them.



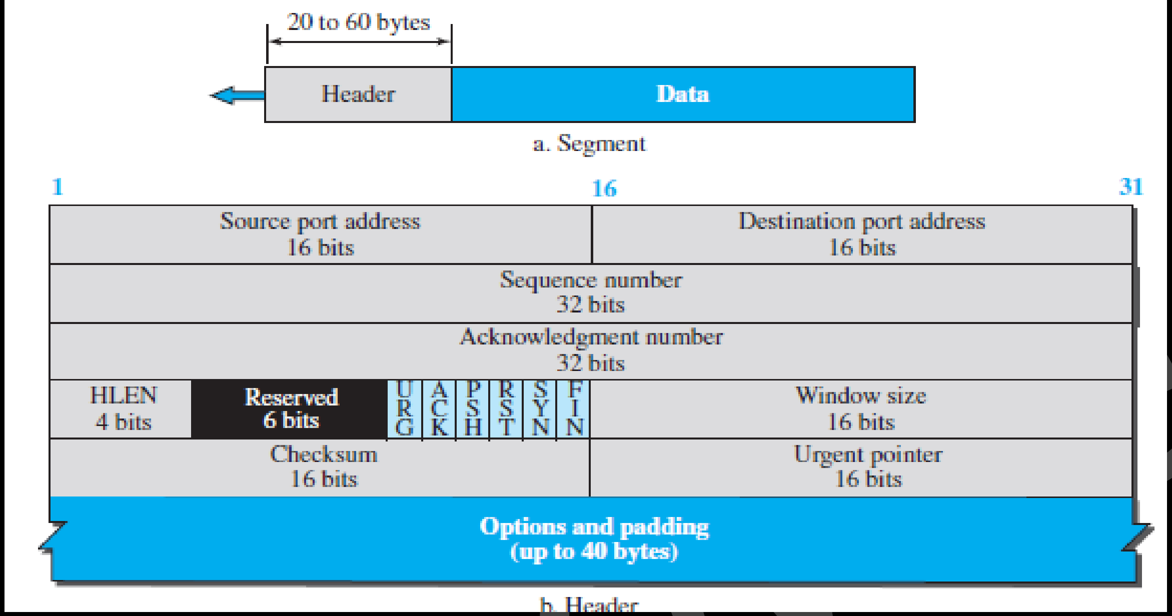


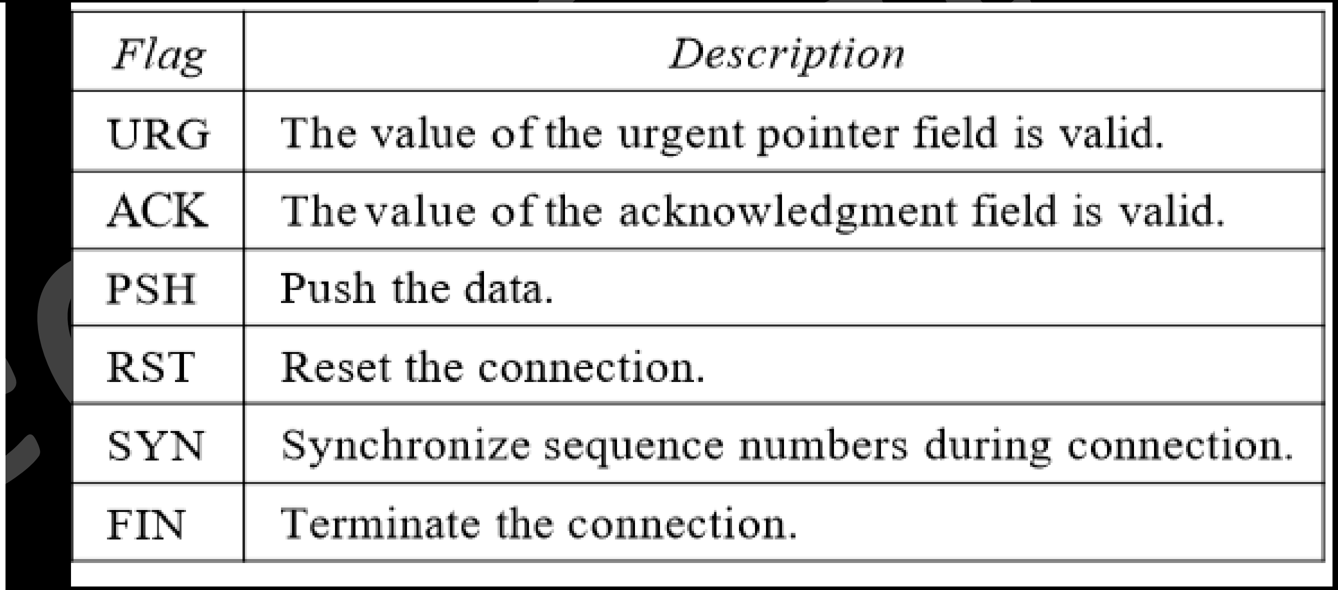
Flag	*Description*
URG	The value of the urgent pointer field is valid.
ACK	The value of the acknowledgment field is valid.
PSH	Push the data.
RST	Reset the connection.
SYN	Synchronize sequence numbers during connection.
FIN	Terminate the connection.

RST Flag

- **Reset (RST) –** It is used to terminate the connection if the sender or receiver feels something is wrong with the TCP connection or that the conversation should not exist.

- It can get send from receiver side when packet is send to particular host that was not expecting it.

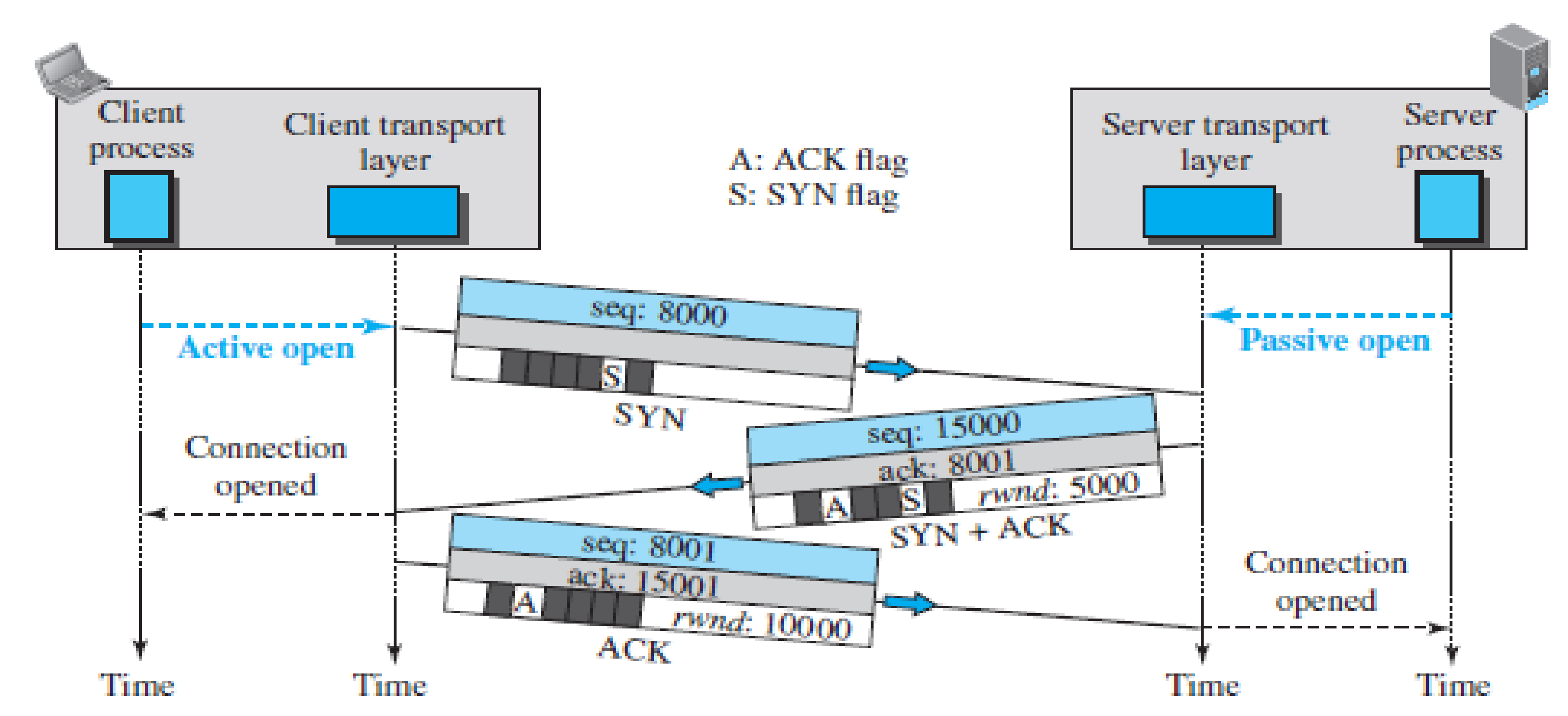




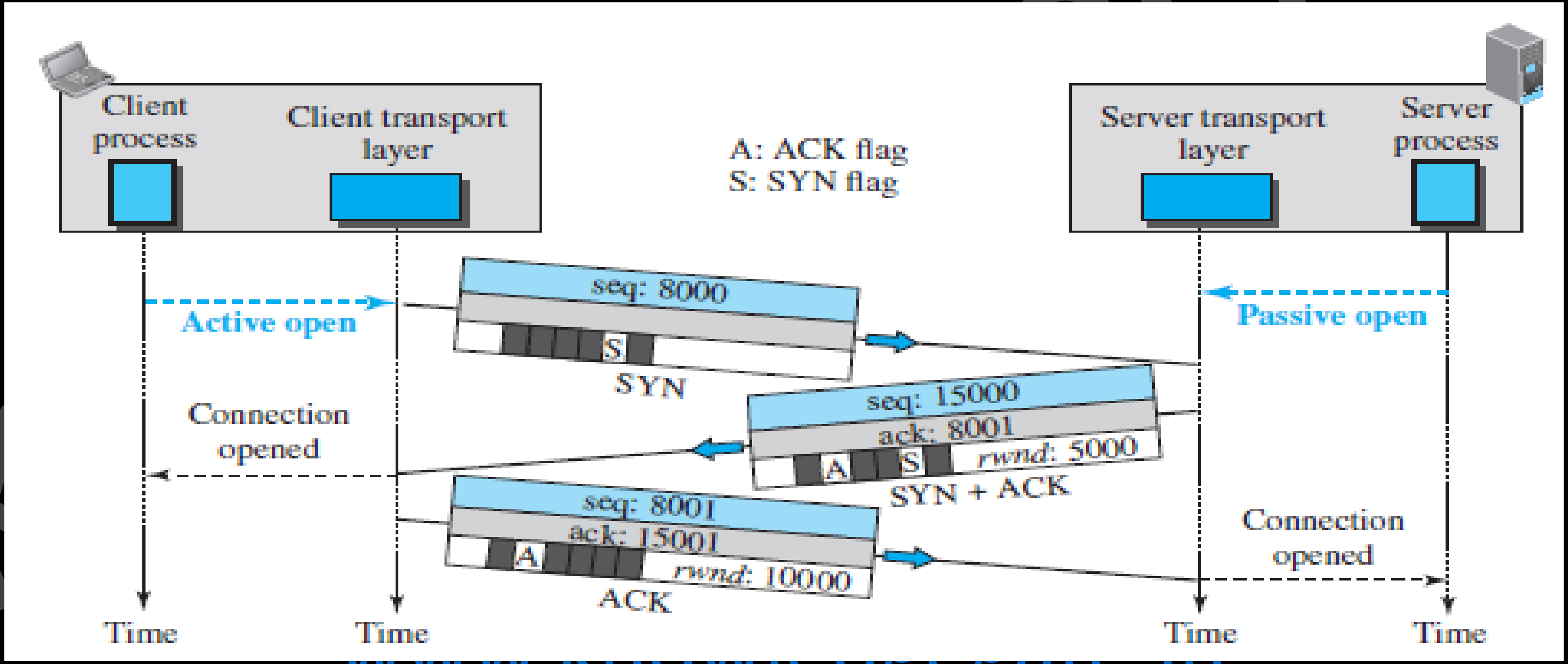
Flag	*Description*
URG	The value of the urgent pointer field is valid.
ACK	The value of the acknowledgment field is valid.
PSH	Push the data.
RST	Reset the connection.
SYN	Synchronize sequence numbers during connection.
FIN	Terminate the connection.

A TCP Connection

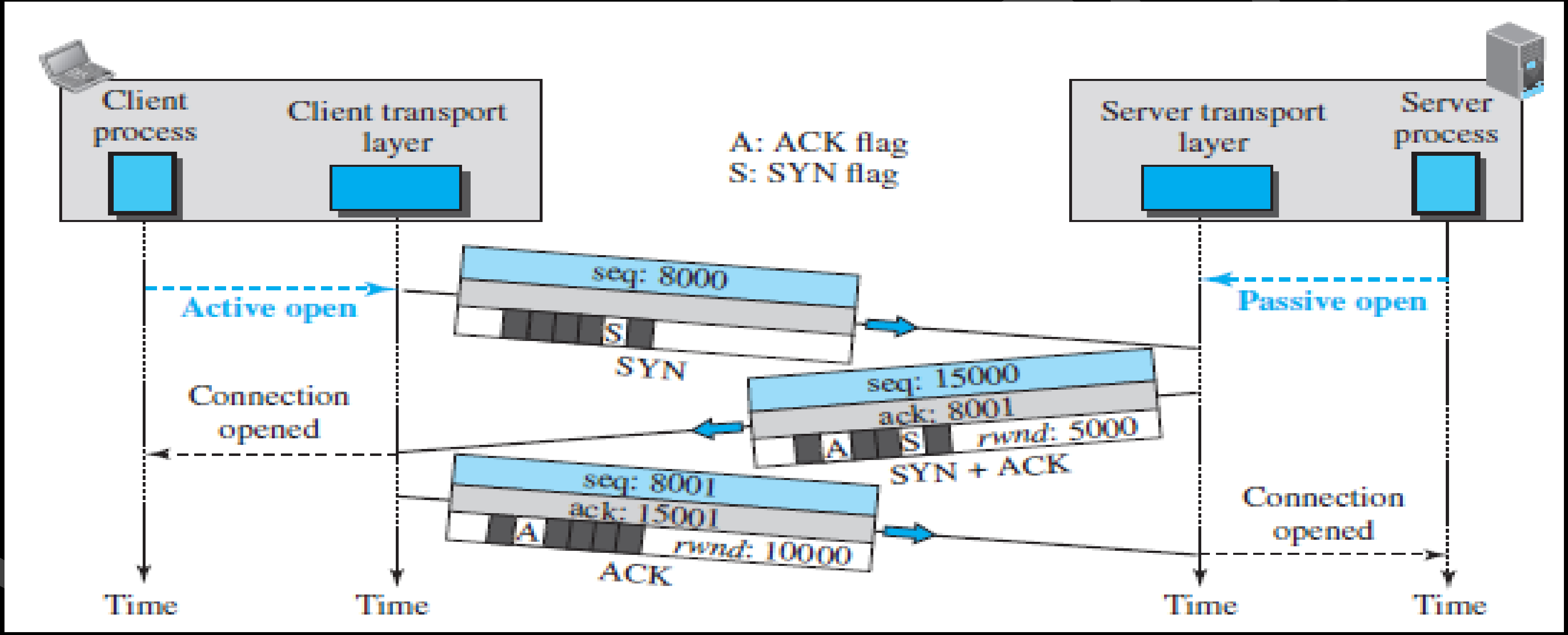
- The connection establishment in TCP is called ***three-way handshaking.***
- The client program issues a request for an *active open*. A client that wishes to connect to an open server tells its TCP to connect to a particular server. TCP can now start the three-way handshaking process.



- The server sends the second segment, a SYN + ACK segment with two flag bits set as: SYN and ACK.
  - It is a SYN segment for communication in the other direction.
  - The server uses this segment to initialize a sequence number for numbering the bytes sent from the server to the client.
  - The server also acknowledges the receipt of the SYN segment from the client by setting the ACK flag and displaying the next sequence number it expects to receive from the client.
  - A SYN + ACK segment cannot carry data, but it does consume one sequence number.



- The client sends the third segment.
  - This is just an ACK segment.
  - It acknowledges the receipt of the second segment with the ACK flag and acknowledgment number field.
- ACK segment does not consume any sequence numbers if it does not carry data.
- After connection is established, bidirectional data transfer can take place.



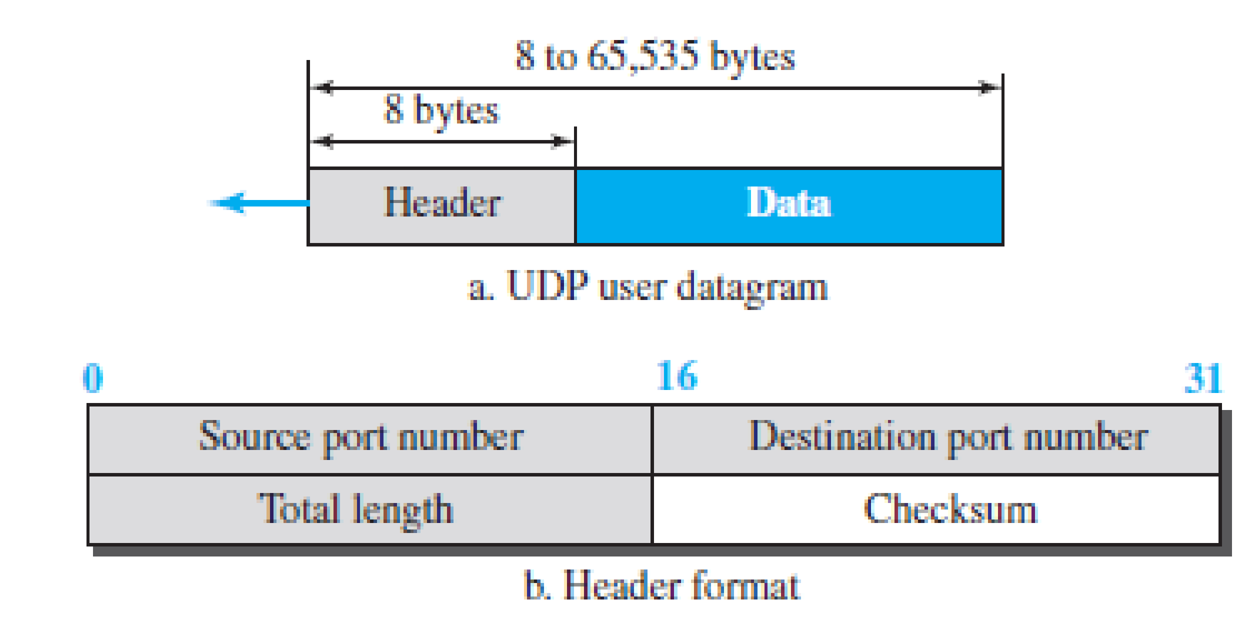
USER DATAGRAM PROTOCOL (UDP)

- The **User Datagram Protocol (UDP)** is a connectionless, unreliable transport protocol.
- It does not add anything to the services of IP except for providing process-to-process communication instead of host-to-host communication.

- **Why to use UDP**
  - UDP is a very simple protocol using a minimum of overhead.
  - If a process wants to send a small message and does not care much about reliability, it can use UDP.
  - Sending a small message using UDP takes much less interaction between the sender and receiver than using TCP.

User Datagram

- UDP packets, called ***user datagrams,*** have a fixed-size header of 8 bytes made of four fields, each of 2 bytes (16 bits).
- The first two fields define the source and destination port numbers.
- The third field defines the total length of the user datagram, header plus data.
- The 16 bits can define a total length of 0 to 65,535 bytes. However, the total length needs to be less because a UDP user datagram is stored in an IP datagram with the total length of 65,535 bytes.
- The last field can carry the optional checksum



a. UDP user datagram

Source port number	Destination port number
Total length	Checksum

b. Header format

UDP Services

- ***Process-to-Process Communication***
  - UDP provides process-to-process communication using **socket addresses,** a combination of IP addresses and port numbers.
- ***Connectionless Services***
  - Each user datagram sent by UDP is an independent datagram. There is no relationship between the different user datagrams. The user datagrams are not numbered. There is no connection establishment and no connection termination unlike TCP.
- ***Flow Control***
  - There is no *flow control,* and hence no window mechanism.
- ***Error Control***
  - There is no *error control* mechanism in UDP except for the checksum.
- ***Congestion Control***
  - It does not provide congestion control.

UDP Applications

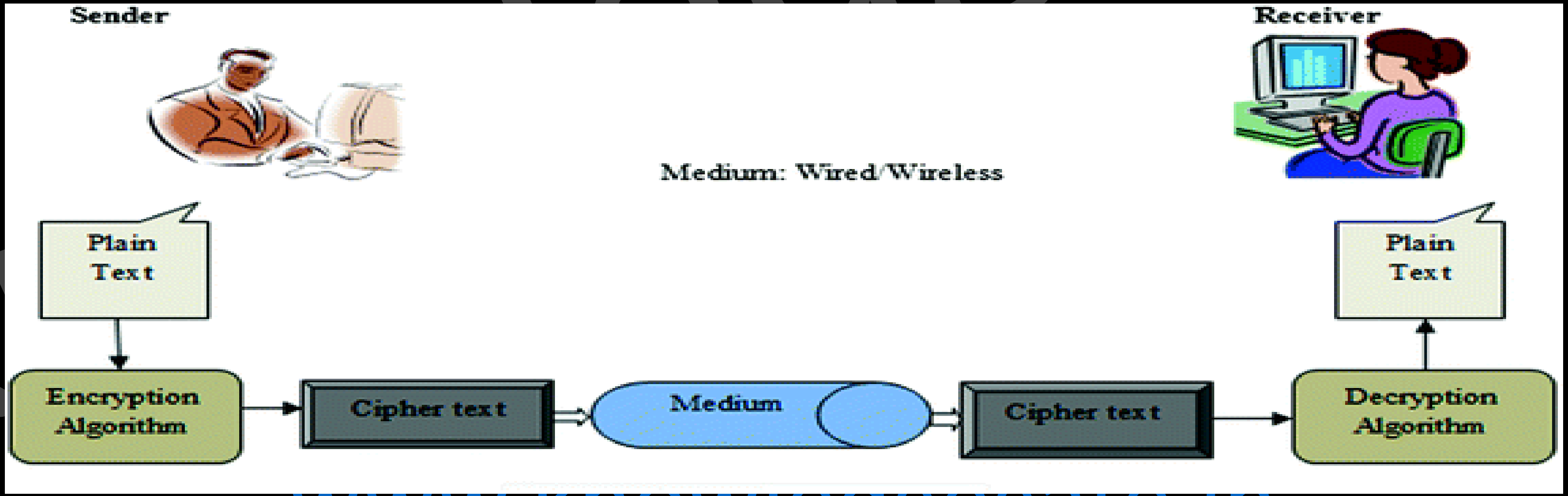
- UDP is suitable for a process with internal flow- and error-control mechanisms. For example, the ***Trivial File Transfer Protocol (TFTP)*** process includes flow and error control. It can easily use UDP.
- UDP is a suitable transport protocol for multicasting. Multicasting capability is embedded in the UDP software but not in the TCP software.
- UDP is used for management processes such as SNMP
- UDP is used for some route updating protocols such as Routing Information Protocol (RIP)
- UDP is normally used for interactive real-time applications that cannot tolerate uneven delay between sections of a received message.
- DNS,

S.No.	TCP	RTP
1	TCP stands for transmission control protocol.	RTP stand for Real Time Transport Protocol.
2	It is a lossless protocol.	RTP is a stateless protocol.
3	It is a slow process.	It is a faster than TCP.
4	It cannot tolerate packet loss.	It can tolerate packet loss.
5	TCP is not generally used for ‘real-time’ streaming.	RTP is used for ‘real-time’ streaming.

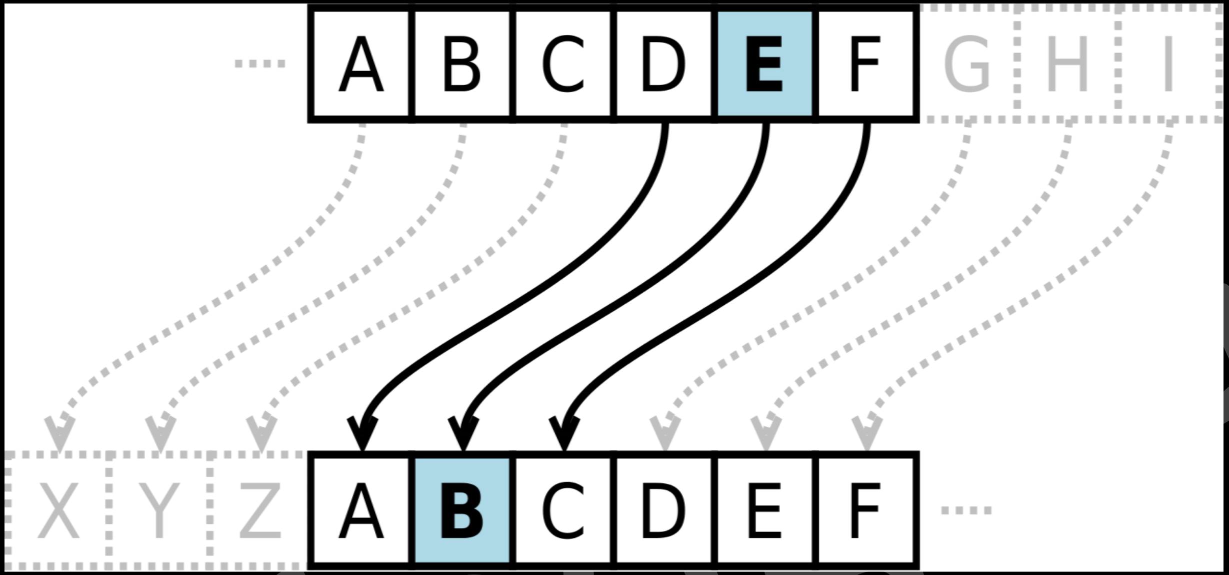
- Data compression :
  - Data compression is the way of downloading the compressed form of text, audio and video data using the computer.
  - Data compression is essential for efficient storage and transmission of different type of data.
  - A data compression system consists of an encoder and a decoder.
  - The encoder performs compression of the incoming data and decoder is used for decompression and reconstruction.
- Types of compression :
  - Lossless compression (or data compaction) :
    - In lossless compression, the redundant information contained in the data is removed.
    - In lossless compression, there is no loss of information.
    - Lossless compression has lower compression ratio.
  - Lossy compression :
    - In lossy compression, there is a loss of information in a controlled manner.
    - The lossy compression is not completely reversible.
    - The lossy compression has higher compression ratio.

Cryptography

- **Cryptography** is the practice and study of techniques for secure communication in the presence of third parties called adversaries.
- More generally, cryptography is about constructing and analysing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography.
- Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications.

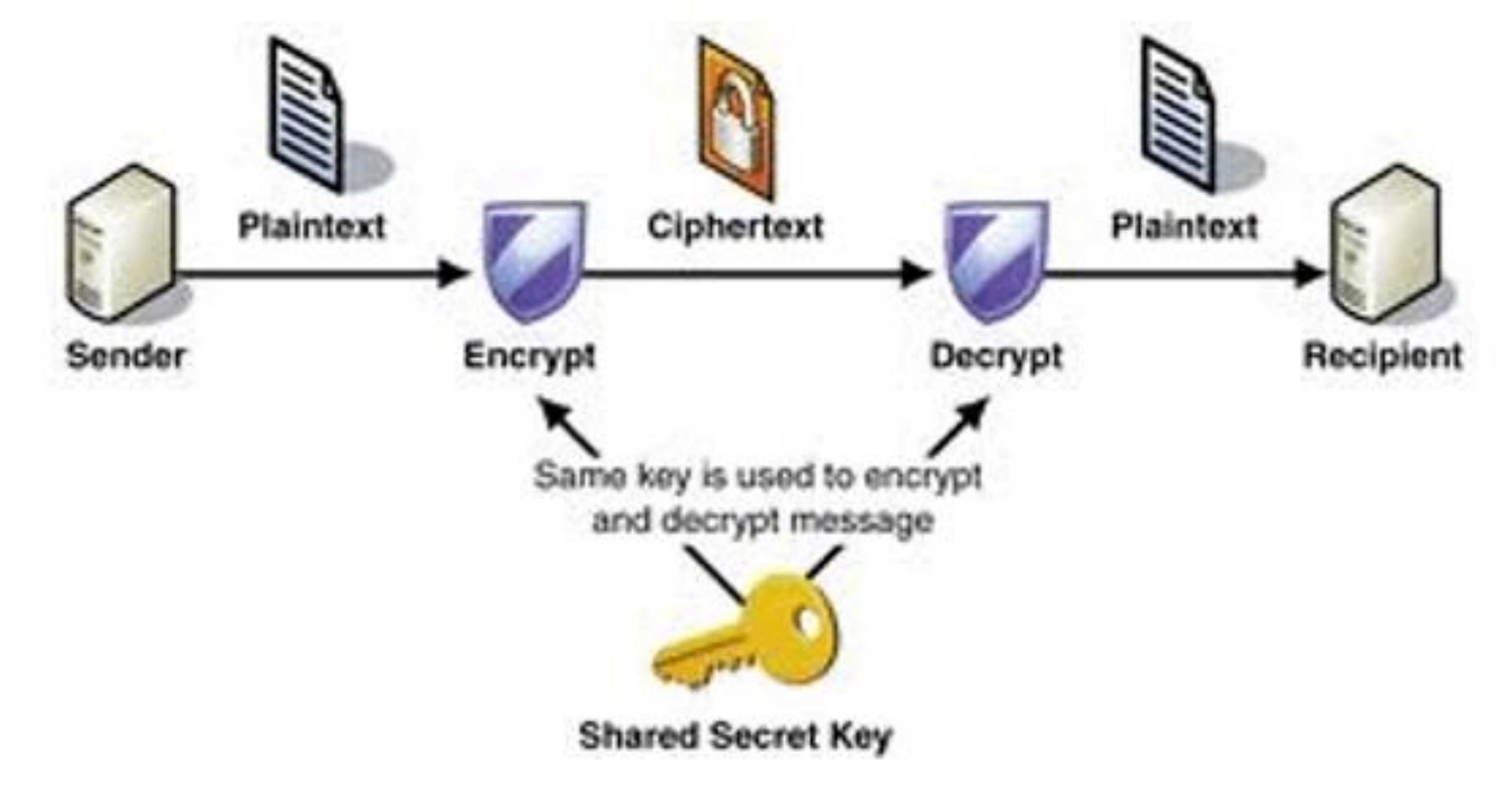


- Alphabet shift ciphers are believed to have been used by Julius Caesar over 2,000 years ago.

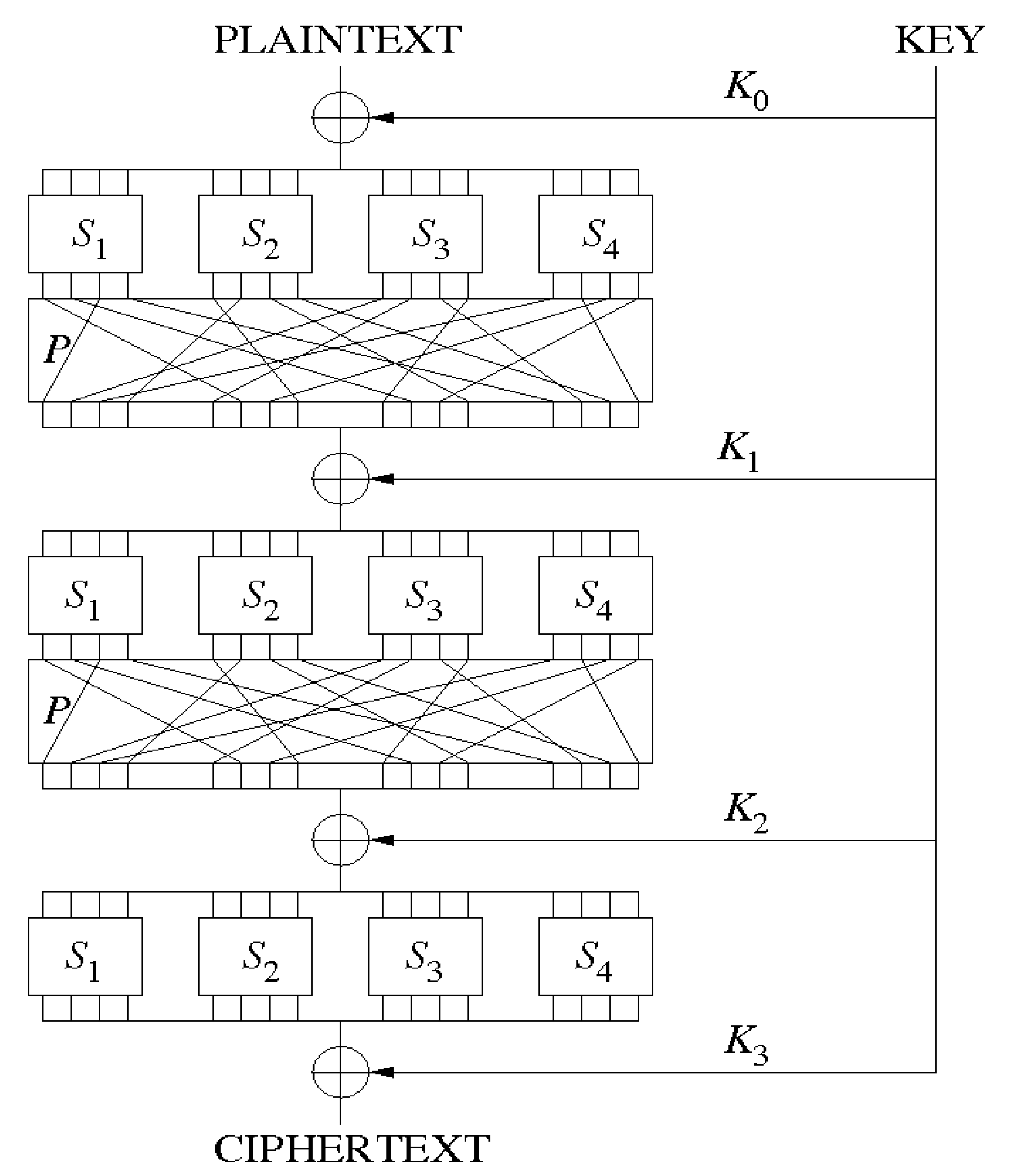


Symmetric key

- Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). This was the only kind of encryption publicly known until June 1976.



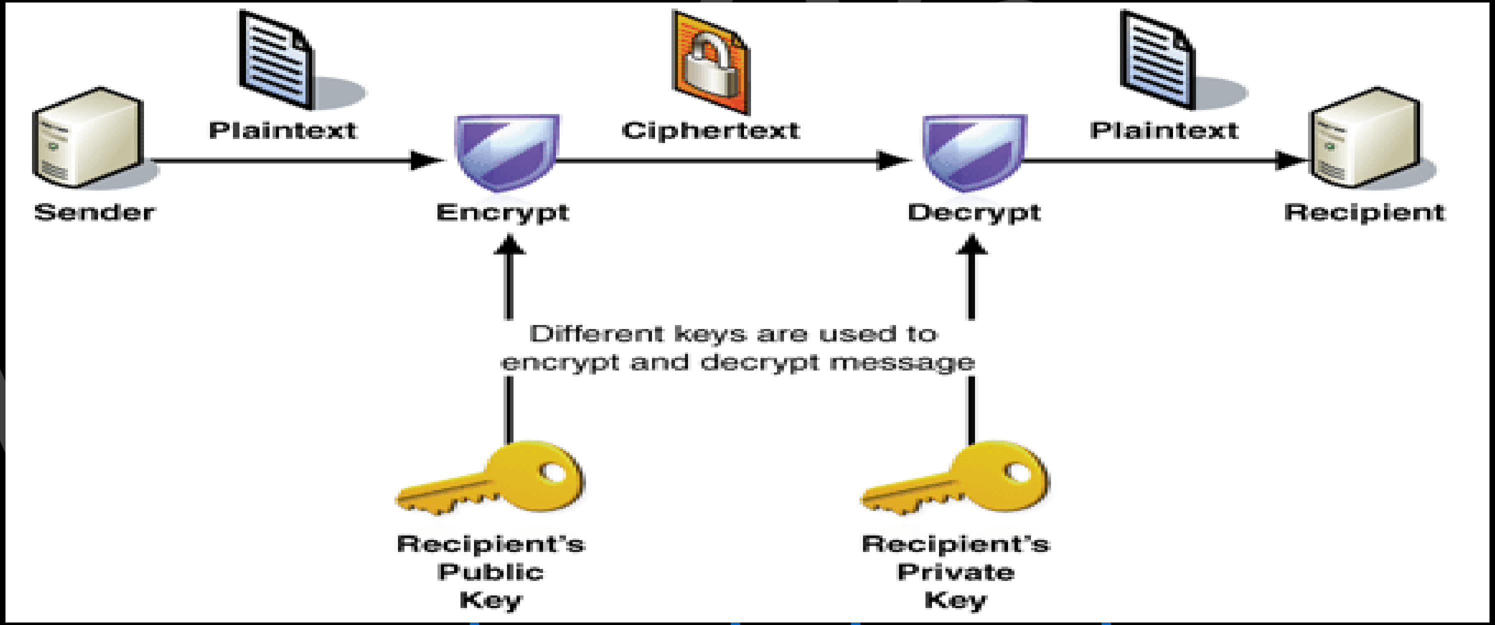
- The Data Encryption Standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs that have been designated cryptography standards by the US government (though DES's designation was finally withdrawn after the AES was adopted).
- Despite its deprecation as an official standard, DES (especially its still-approved and much more secure triple-DES variant) remains quite popular; it is used across a wide range of applications, from ATM encryption to e-mail privacy and secure remote access.



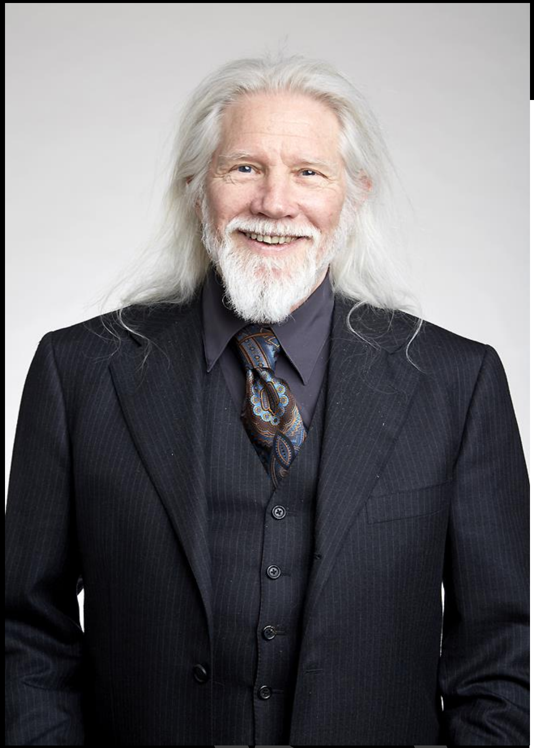
- The data encryption standard(DES) is a block cipher that used shared secret encryption.
- DES is based on a symmetric key algorithm that uses a 56-bit key.
- DES is basically a mono-alphabetic substitution cipher using a 64-bit character.
- Whenever the same 64-bit plaintext block goes in, the same 64-bit ciphertext block comes out.
- Working of DES involves the following stages:
    - The first stage is a key independent transposition on the 64-bit plaintext.
    - The last stage is the exact inverse, before that is an exchange of the leftmost with the rightmost 32 bits.
    - The remaining 16 stages are functionally identical but are parameterized by different functions of the key.
    - The left output of an iteration stage is simply a copy of the right input. The right output is the exclusive OR of the left input and a function of the right input and the key for this iteration. All the complexity lies in this functions which consists of four sequential steps.

Asymmetric key (Public-key cryptography)

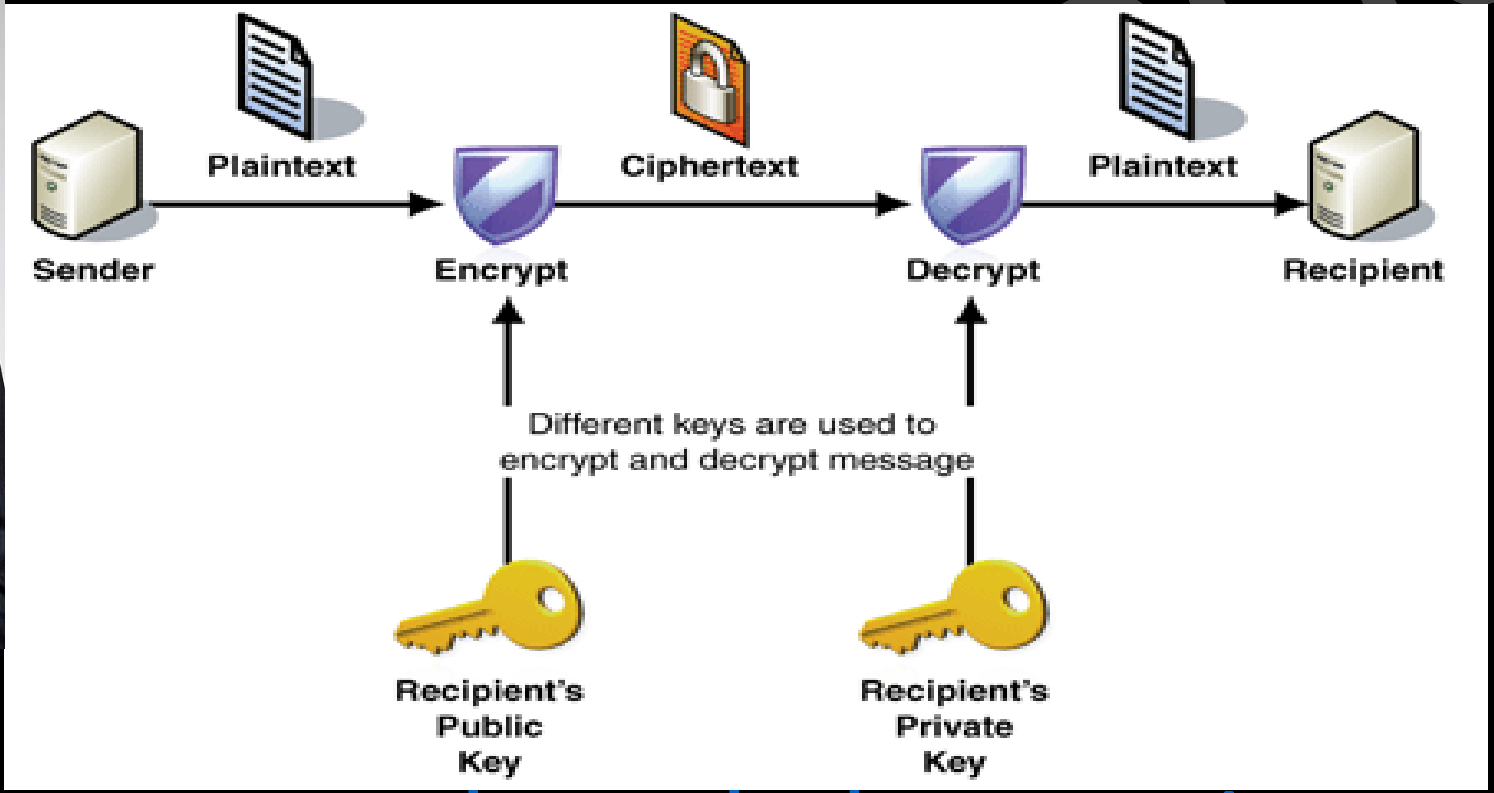
- Symmetric-key cryptosystems use the same key for encryption and decryption of a message, although a message or group of messages can have a different key than others.
- A significant disadvantage of symmetric ciphers is the key management necessary to use them securely. Each distinct pair of communicating parties must, ideally, share a different key, and perhaps for each ciphertext exchanged as well.
- The number of keys required increases as the square of the number of network members, which very quickly requires complex key management schemes to keep them all consistent and secret.



- In a ground breaking 1976 paper, Whitfield Diffie and Martin Hellman proposed the notion of *public-key* (also, more generally, called *asymmetric key*) cryptography in which two different but mathematically related keys are used—a *public* key and a *private* key.
- A public key system is so constructed that calculation of one key (the 'private key') is computationally infeasible from the other (the 'public key'), even though they are necessarily related. Instead, both keys are generated secretly, as an interrelated pair.

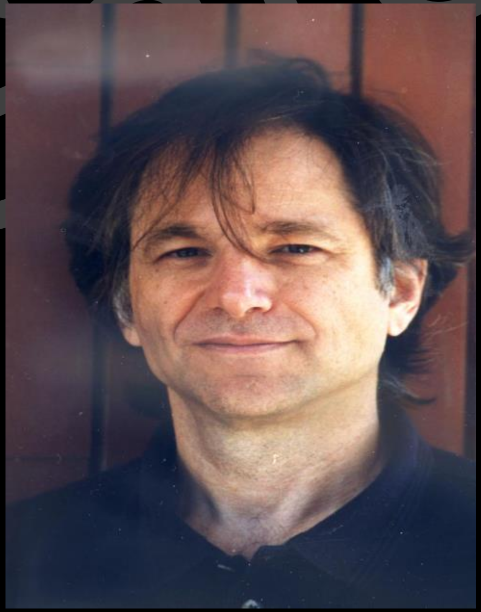


Whitfield Diffie

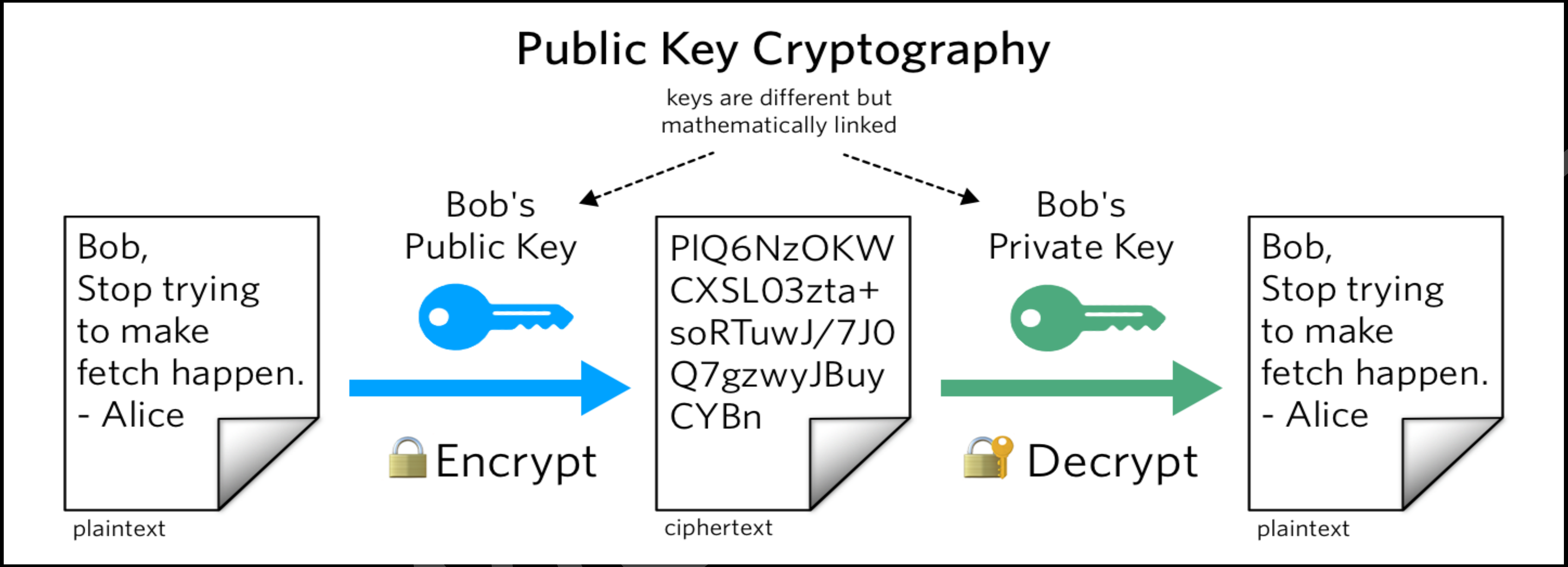


Martin Hellman

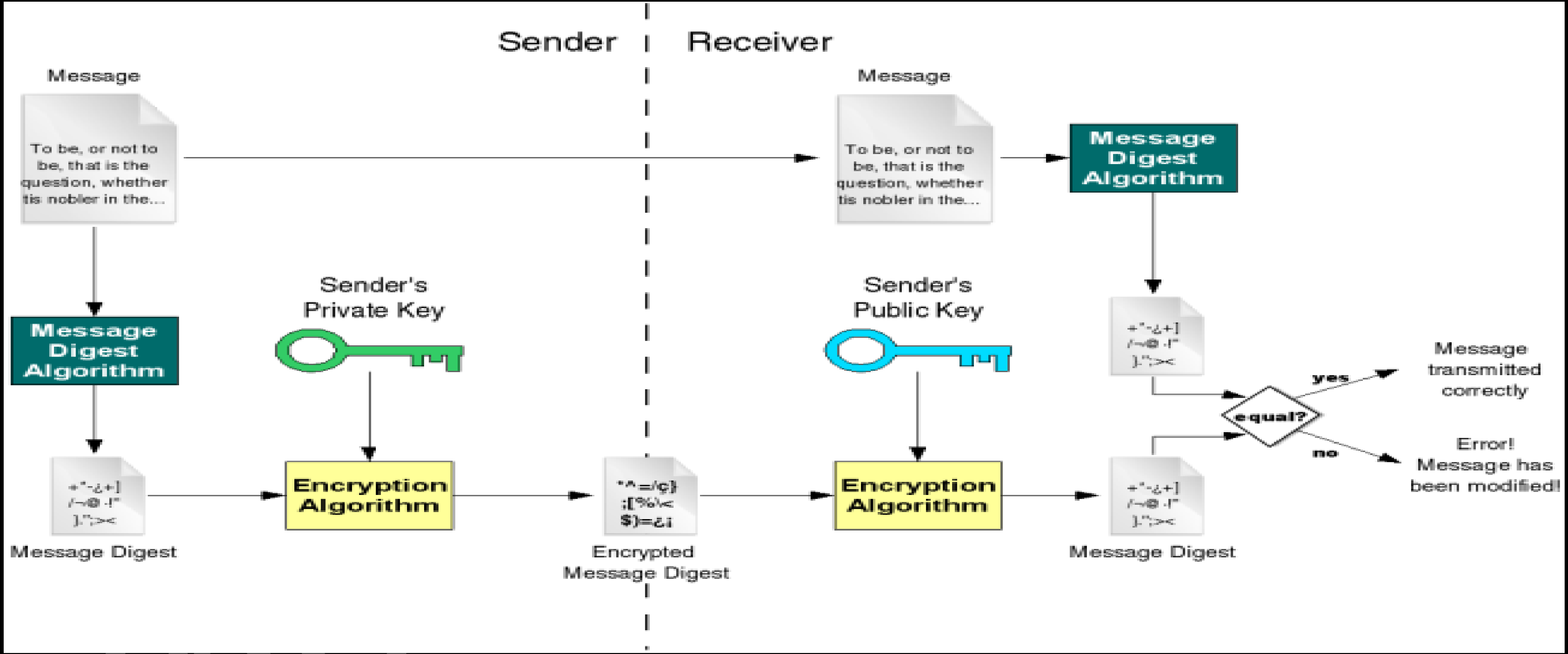
- Diffie and Hellman's publication sparked widespread academic efforts in finding a practical public-key encryption system. This race was finally won in 1978 by Ronald Rivest, Adi Shamir, and Len Adleman, whose solution has since become known as the RSA algorithm.



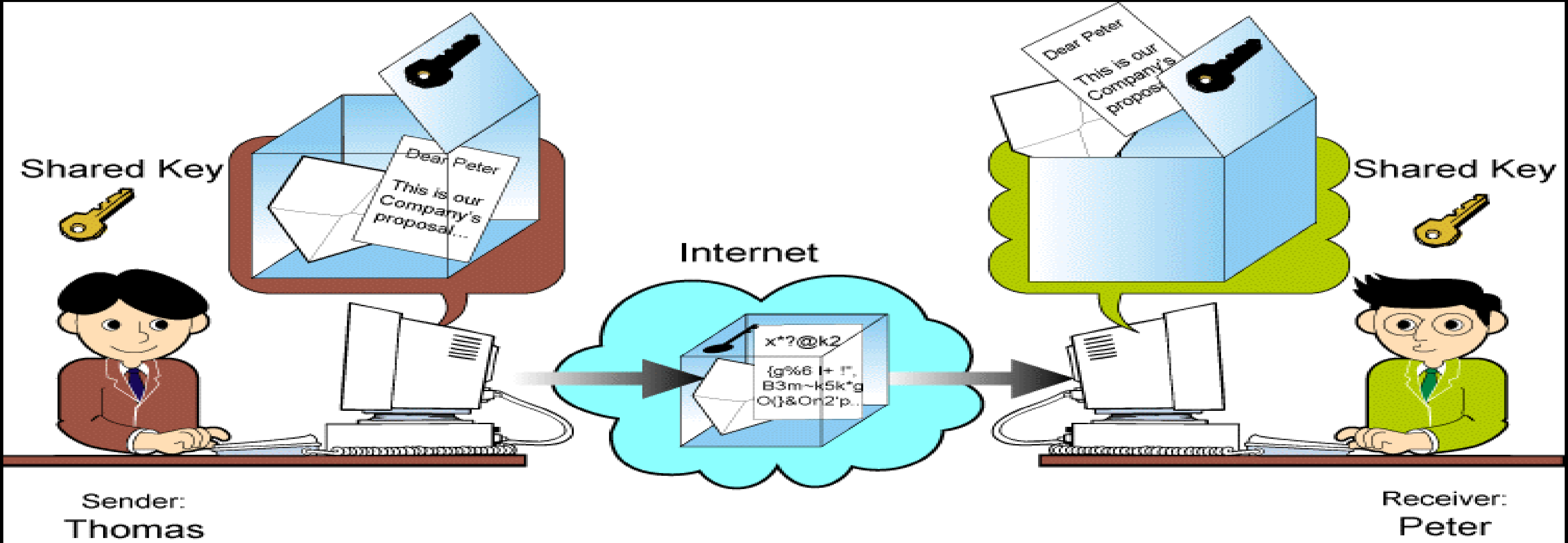
Confidentiality



Authentication

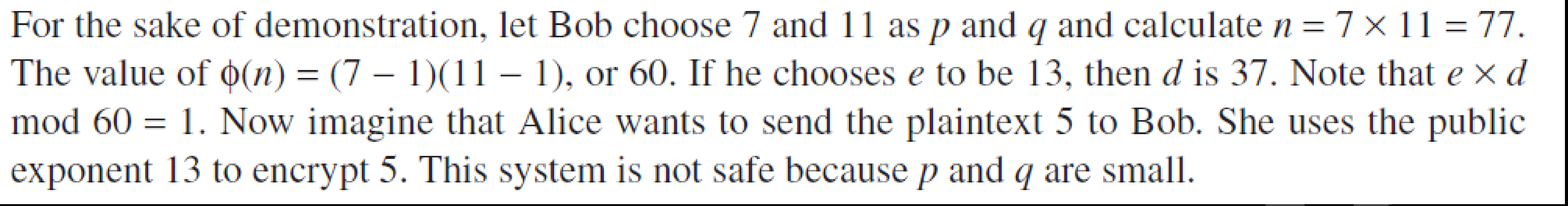


Authentication Confidentiality

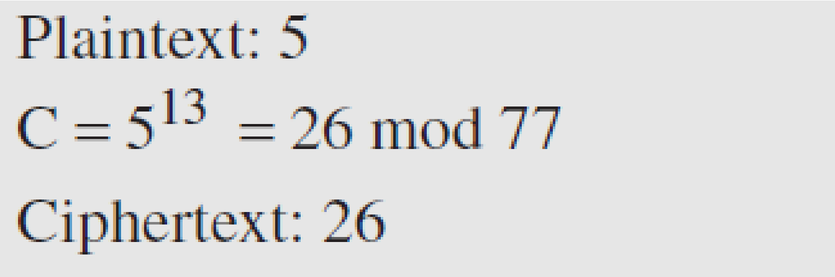


RSA Algorithm

1. Bob chooses two large numbers, p and q, and calculates $n = p \times q$ and $0 = (p - 1) \times (g - 1)$.
2. Bob then selects e and d such that $(e \text{ x } d) \bmod 0 = 1$.
3. Bob advertises e and n to the community as the public key; Bob keeps d as the private key.
4. Anyone, including Alice, can encrypt a message and send the ciphertext to Bob, using $C = (P^e) \bmod n$; only Bob can decrypt the message, using $P = (C^d) \bmod n$.
5. An intruder such as Eve cannot decrypt the message if p and q are very large numbers (she does not know d).



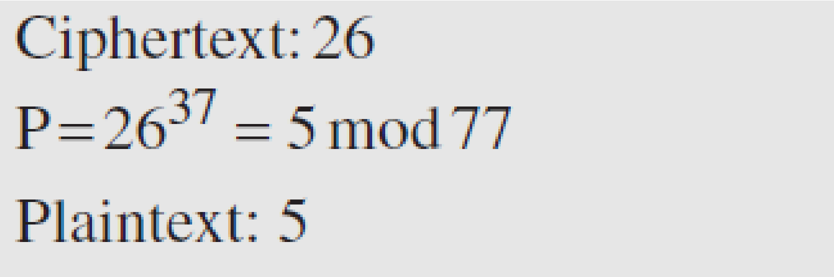
For the sake of demonstration, let Bob choose 7 and 11 as p and q and calculate $n = 7 \times 11 = 77$. The value of $\phi(n) = (7 - 1)(11 - 1)$, or 60. If he chooses e to be 13, then d is 37. Note that $e \times d$ mod $60 = 1$. Now imagine that Alice wants to send the plaintext 5 to Bob. She uses the public exponent 13 to encrypt 5. This system is not safe because p and q are small.



Plaintext: 5

$C = 5^{13} = 26 \bmod 77$

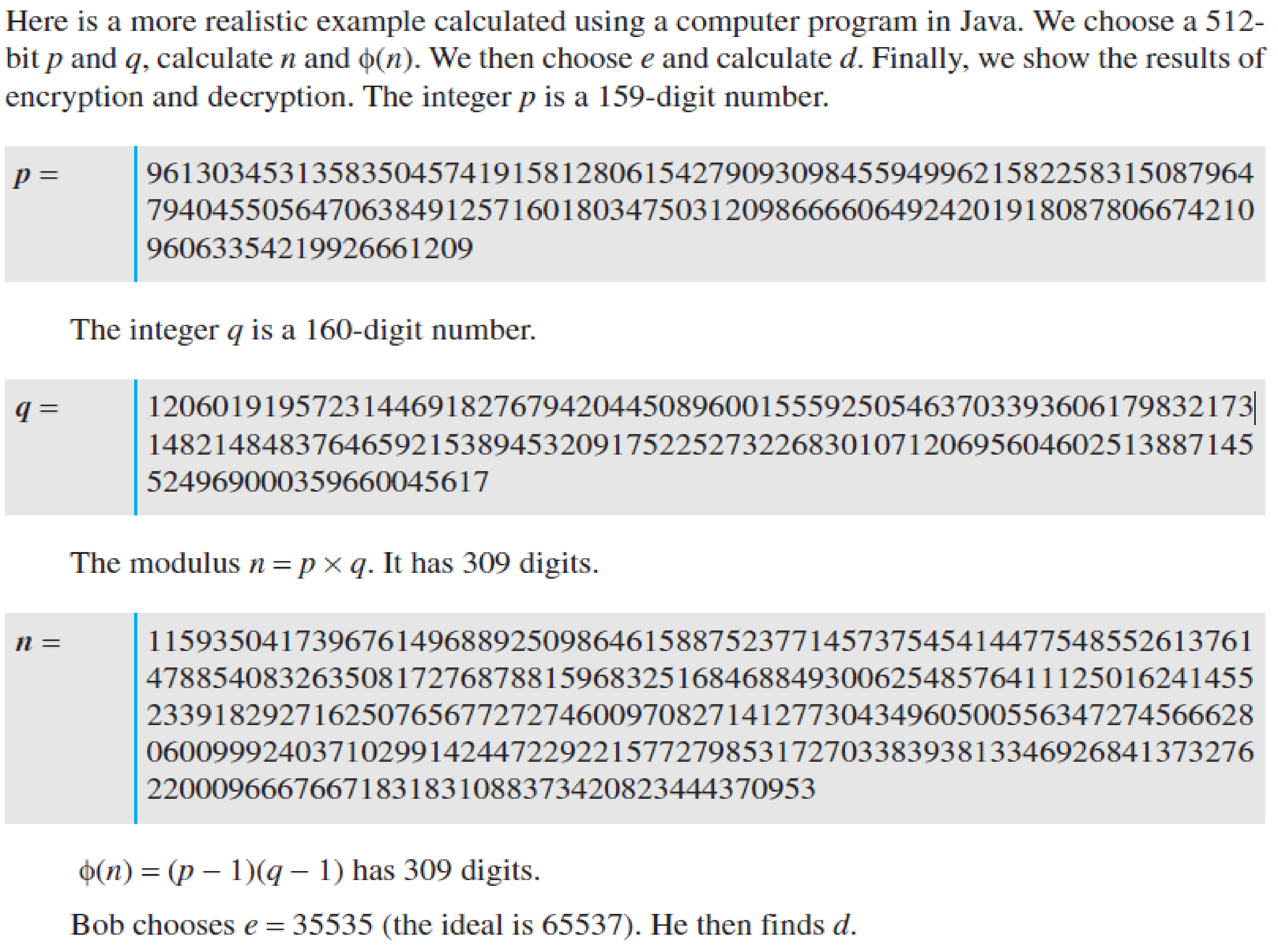
Ciphertext: 26



Ciphertext: 26

$P = 26^{37} = 5 \bmod 77$

Plaintext: 5



Here is a more realistic example calculated using a computer program in Java. We choose a 512-bit p and q, calculate n and $\phi(n)$. We then choose e and calculate d. Finally, we show the results of encryption and decryption. The integer p is a 159-digit number.

$p =$	96130345313583504574191581280615427909309845594996215822583150879647940455056470638491257160180347503120986666064924201918087806674210960633542199266612090

$p =$	9613034531358350457419158128061542790930984559499621582258315087964 7940455056470638491257160180347503120986666064924201918087806674210 96063354219926661209

The integer q is a 160-digit number.

$q =$	1206019195723144691827679420445089600155592505463703393606179832173 1482148483764659215389453209175225273226830107120695604602513887145 524969000359660045617

The modulus $n = p \times q$. It has 309 digits.

$n =$	1159350417396761496889250986461588752377145737545414477548552613761
	4788540832635081727687881596832516846884930062548576411125016241455
	2339182927162507656772727460097082714127730434960500556347274566628
	0600999240371029914244722922157727985317270338393813346926841373276
	220009666766718318310883734208234443709 53

$\phi(n) = (p - 1)(q - 1)$ has 309 digits.

Bob chooses $e = 35535$ (the ideal is 65537). He then finds d.

$\phi(n) =$	115935041739676149688925098646158875237714573754541447754855261376147885408326350817276878815968325168468849300625485764111250162414552339182927162507656751054233608492916752034482627988117554787657013923444405716989581728196098226361075467211864612171359107358640614008885170265377277264467341066243857664128

$e =$	35535
$d =$	580083028600377639360936612896779175946690620896509621804228661113805938528223587317062869100300217108590443384021707298690876006115306202524959884448047568240966247081485817130463240644077704833134010850947385295645071936774061197326557424237217617674620776371642076003370853332885321447088595513667029483 1

Alice wants to send the message "THIS IS A TEST", which can be changed to a numeric value using the 00–26 encoding scheme (26 is the *space* character).

The ciphertext calculated by Alice is $C = P^e$, which is shown below.

P =	1907081826081826002619041819

C =	4753091236462268272063655506105451809423717960704917165232392430544529606131993285666178434183591141511974112520056829797945717360361012782188478927415660904800235071907152771859149751884658886321011483541033616578984679683867637337657774656250792805211481418440481418443081277305900469287424855916646210865 6

Bob can recover the plaintext from the ciphertext using $P = C^d$, which is shown below.

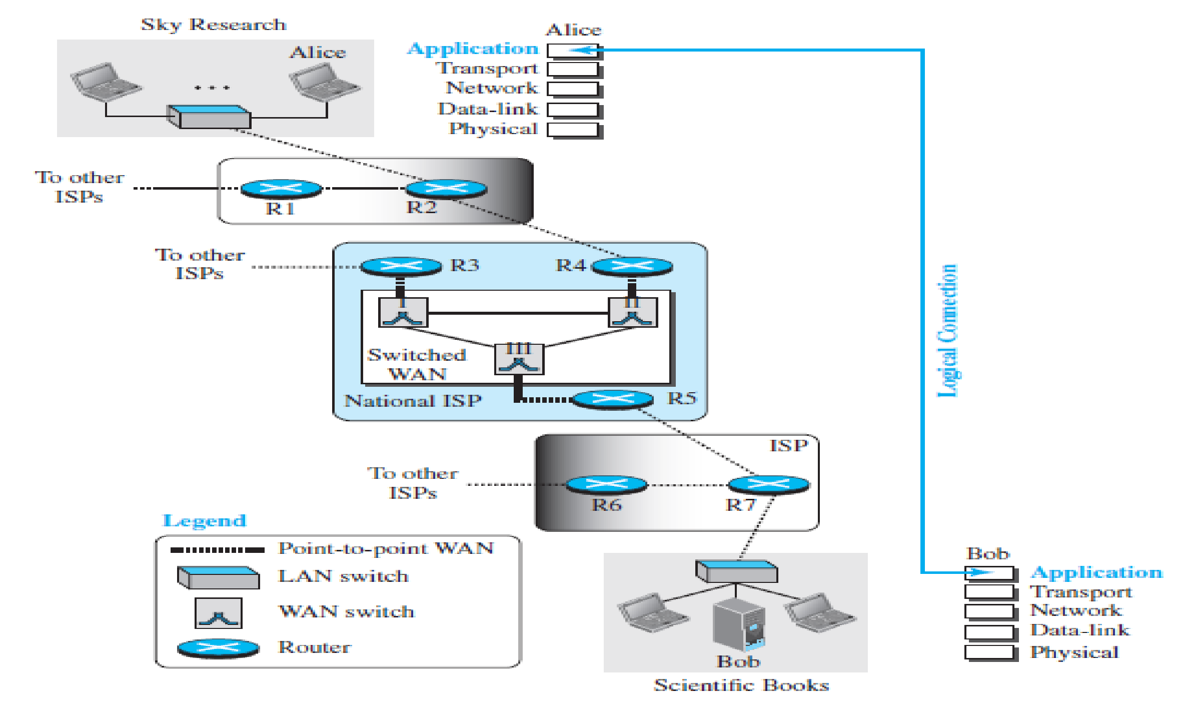
P =	1907081826081826002619041819

The recovered plaintext is "THIS IS A TEST" after decoding.

S.No.	Block Cipher	Transposition Cipher
1	Block cipher A block cipher is one in which a block of plaintext is treated as a whole and used to produce a ciphertext block of equal length.	Transposition cipher Transposition cipher is the cipher in which the plaintext is written -down as a sequence of diagonals and then read off as a sequence of rows.
2	Errors in transmitting one block generally do not affect other blocks.	Error in one letter will affect the whole ciphertext.
3	Encryption process is slow.	Encryption process is fast.
4	Security of block cipher depends on the design of encryption function.	Transposition cipher can be made more secure by performing more than one transposition.
5	Algorithm breaks the plaintext into blocks and operates on each block independently.	Algorithm breaks the plaintext into letters and operates on each letter independently.

Application Layer

- The application layer enables the user, whether human or software, to access the network. It provides user interfaces and responsible for providing services to the user such as
  - Electronic mail
  - File access and transfer
  - Access to system resources
  - Surfing the world wide web
  - Network management.



- Communication between two application layers happens over a logical connection. This means both layers act like they're directly connected for message exchange. To use the Internet, you need two application programs: one on one computer and another on a different computer. Both interact to send and receive data.

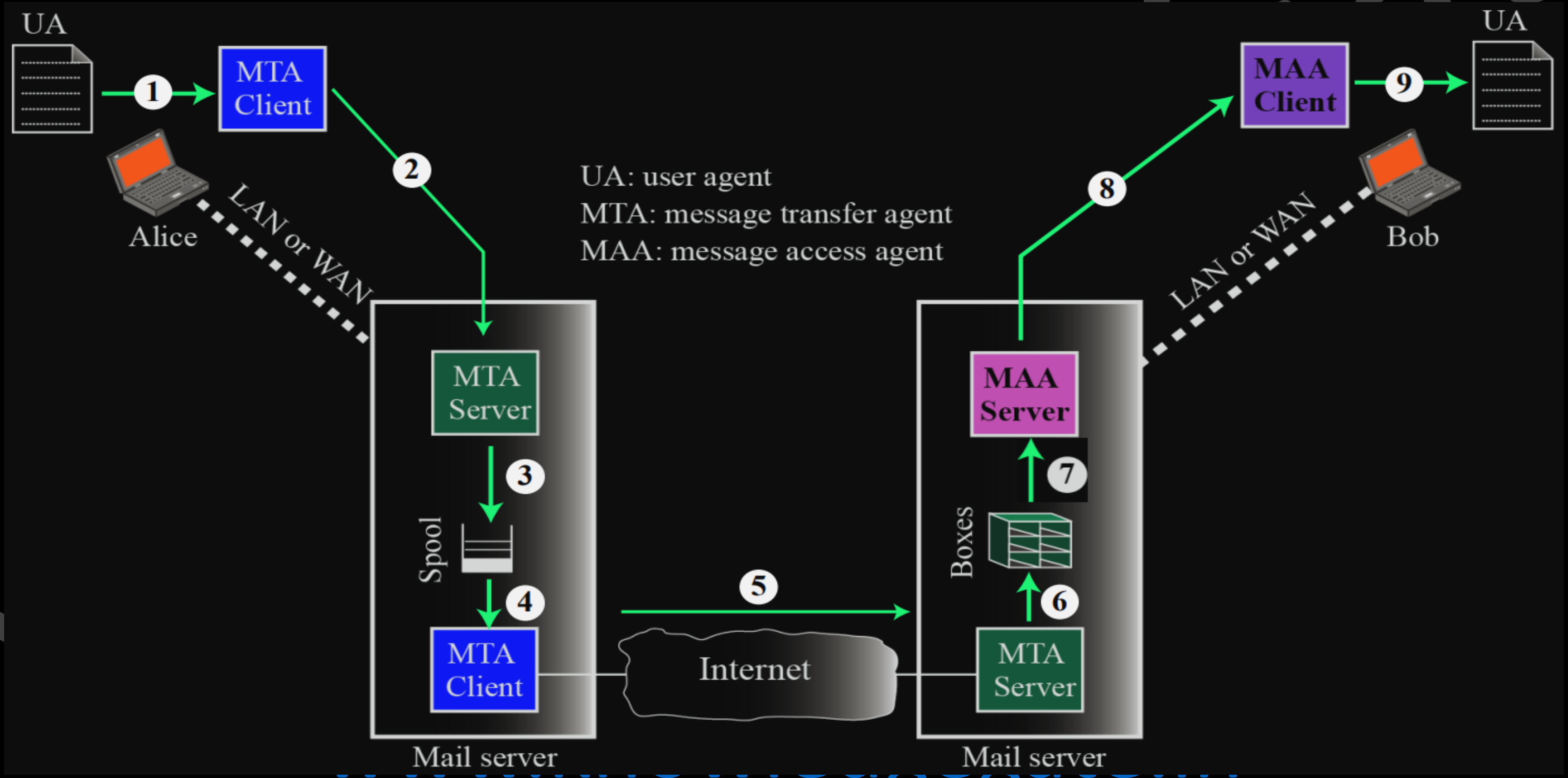
ELECTRONIC MAIL

- E-mail has evolved significantly since the early days of the Internet. Originally designed for simple text-based communication, it was essentially a way to send digital memos between users. The creators of this system likely couldn't have foreseen just how versatile and popular e-mail would become.
  - **Multimedia**: Modern e-mails can include not just text, but also images, audio, and video attachments.
  - **Multiple Recipients**: E-mails can be sent to multiple recipients at once, with features like CC (carbon copy) and BCC (blind carbon copy) for added flexibility.
  - **Hyperlinks and HTML**: E-mails now often include hyperlinks and even HTML content, allowing for richly formatted messages.
  - **Encryption and Security**: Advanced security protocols like SSL/TLS are often used to encrypt e-mails for secure transmission.
  - **Filters and Folders**: Advanced organizational tools let you filter and sort e-mails into various folders, helping manage the influx of messages.
  - **Integration**: E-mails are now often integrated with other services such as calendars, task management tools, and even AI-based assistants to help manage appointments and reminders.

Message Transfer Agent: SMTP

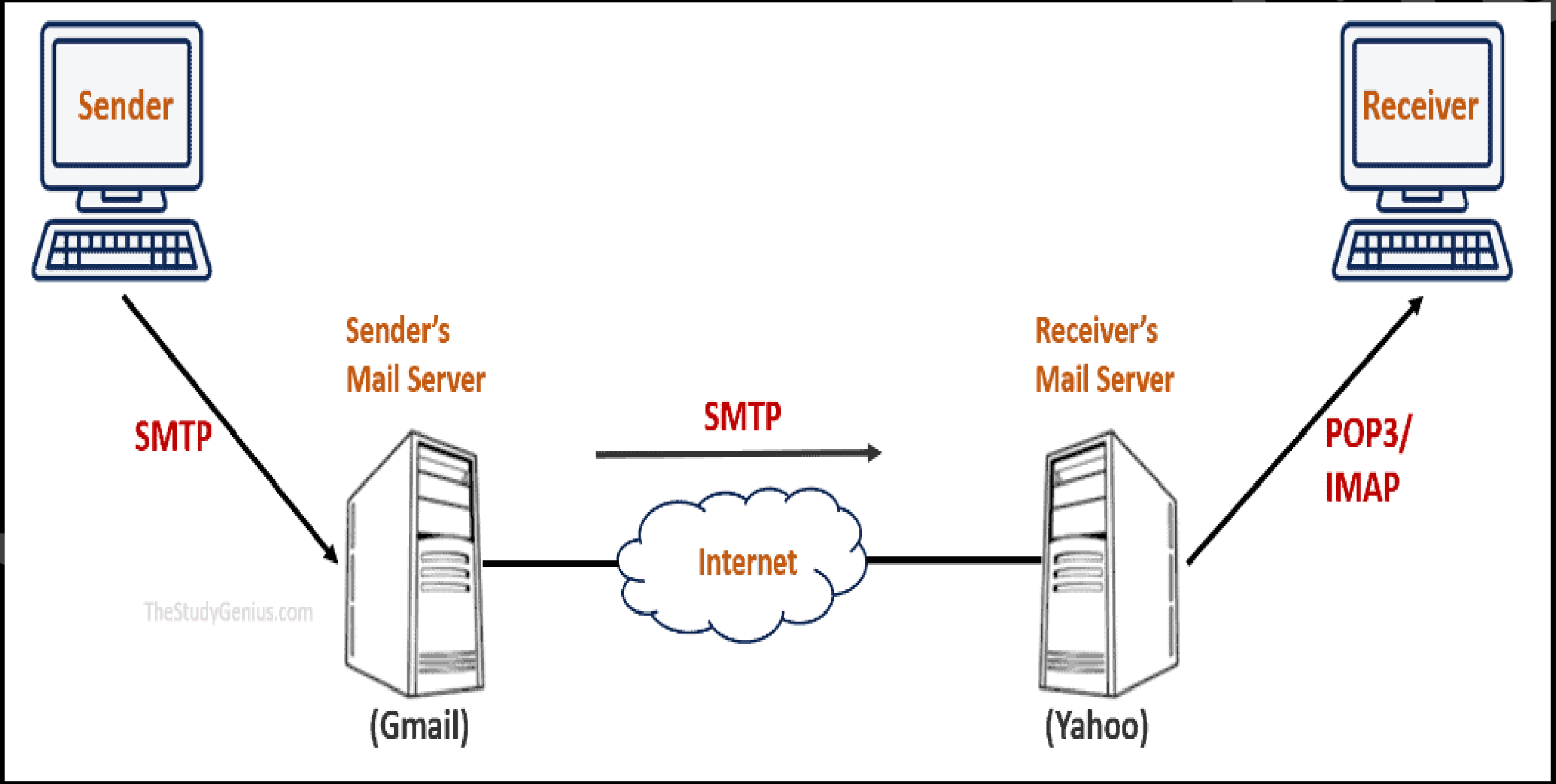
- The actual mail transfer is done through message transfer agents. To send mail, a system must have the client MTA, and to receive mail, a system must have a server MTA.

- The formal protocol that defines the MTA client and server in the Internet is called the Simple Mail Transfer Protocol (SMTP).



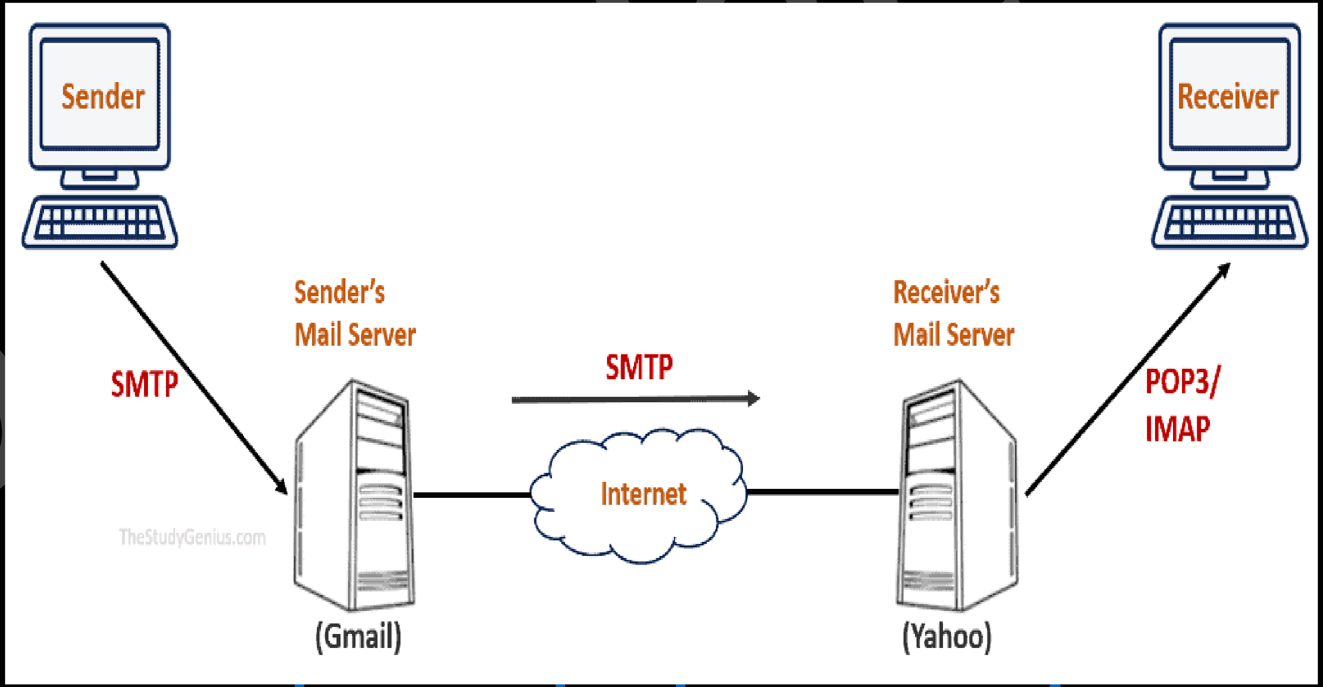
- SMTP is used two times, between the sender and the sender's mail server and between the two mail servers

- SMTP simply defines how commands and responses must be sent back and forth.



Message Access Agent: POP and IMAP

- The first and the second stages of mail delivery use SMTP. However, SMTP is not involved in the third stage because SMTP is a push protocol; it pushes the message from the client to the server.
- On the other hand, the third stage needs a pull protocol; the client must pull messages from the server.
- The third stage uses a message access agent. Currently two message access protocols are available: Post Office Protocol, version 3 (POP_3) and Internet Mail Access Protocol, version 4 ($IMAP_4$).



POP3

- Post Office Protocol, version 3 (POP3) is simple and limited in functionality. The client POP3 software is installed on the recipient computer; the server POP3 software is installed on the mail server.

- Mail access starts with the client when the user needs to download e-mail from the mailbox on the mail server. The client opens a connection to the server on TCP port 110. It then sends its user name and password to access the mailbox.

- The user can then list and retrieve the mail messages, one by one. POP3 has two modes: the delete mode and the keep mode. In the delete mode, the mail is deleted from the mailbox after each retrieval. In the keep mode, the mail remains in the mailbox after retrieval.

- The delete mode is normally used when the user is working at her permanent computer and can save and organize the received mail after reading or replying.

- The keep mode is normally used when the user accesses her mail away from her primary computer (e.g., a laptop). The mail is read but kept in the system for later retrieval and organizing.

IMAP4

- Another mail access protocol is Internet Mail Access Protocol, version 4 (IMAP4). IMAP4 is similar to POP3, but it has more features; IMAP4 is more powerful and more complex.

- POP3 is deficient in several ways. It does not allow the user to organize her mail on the server; the user cannot have different folders on the server. (Of course, the user can create folders on her own computer.)

- In addition, POP3 does not allow the user to partially check the contents of the mail before downloading. IMAP4 provides the following extra functions:

  - A user can check the e-mail header prior to downloading.
  - A user can search the contents of the e-mail for a specific string of characters prior to downloading.
  - A user can partially download e-mail. This is especially useful if bandwidth is limited and the e-mail contains multimedia with high bandwidth requirements.
  - A user can create, delete, or rename mailboxes on the mail server.
  - A user can create a hierarchy of mail boxes in a folder for e-mail storage.

MIME

- Electronic mail has a simple structure. Its simplicity, however, comes at a price. It can send messages only in NVT 7-bit ASCII format. In other words, it has some limitations. For example, it cannot be used for languages that are not supported by 7-bit ASCII characters (such as Hindi, French, German, Hebrew, Russian, Chinese, and Japanese).
- Also, it cannot be used to send binary files or video or audio data.
- Multipurpose Internet Mail Extensions (MIME) is a supplementary protocol that allows non-ASCII data to be sent through e-mail.
- MIME transforms non-ASCII data at the sender site to NVT ASCII data and delivers them to the client MTA to be sent through the Internet. The message at the receiving side is transformed back to the original data.

Web-Based Mail

- E-mail is such a common application that some websites today provide this service to anyone who accesses the site. Two common sites are Hotmail and Yahoo.

- The idea is very simple. Mail transfer from Alice's browser to her mail server is done through HTTP.

- The transfer of the message from the sending mail server to the receiving mail server is still through SMTP.

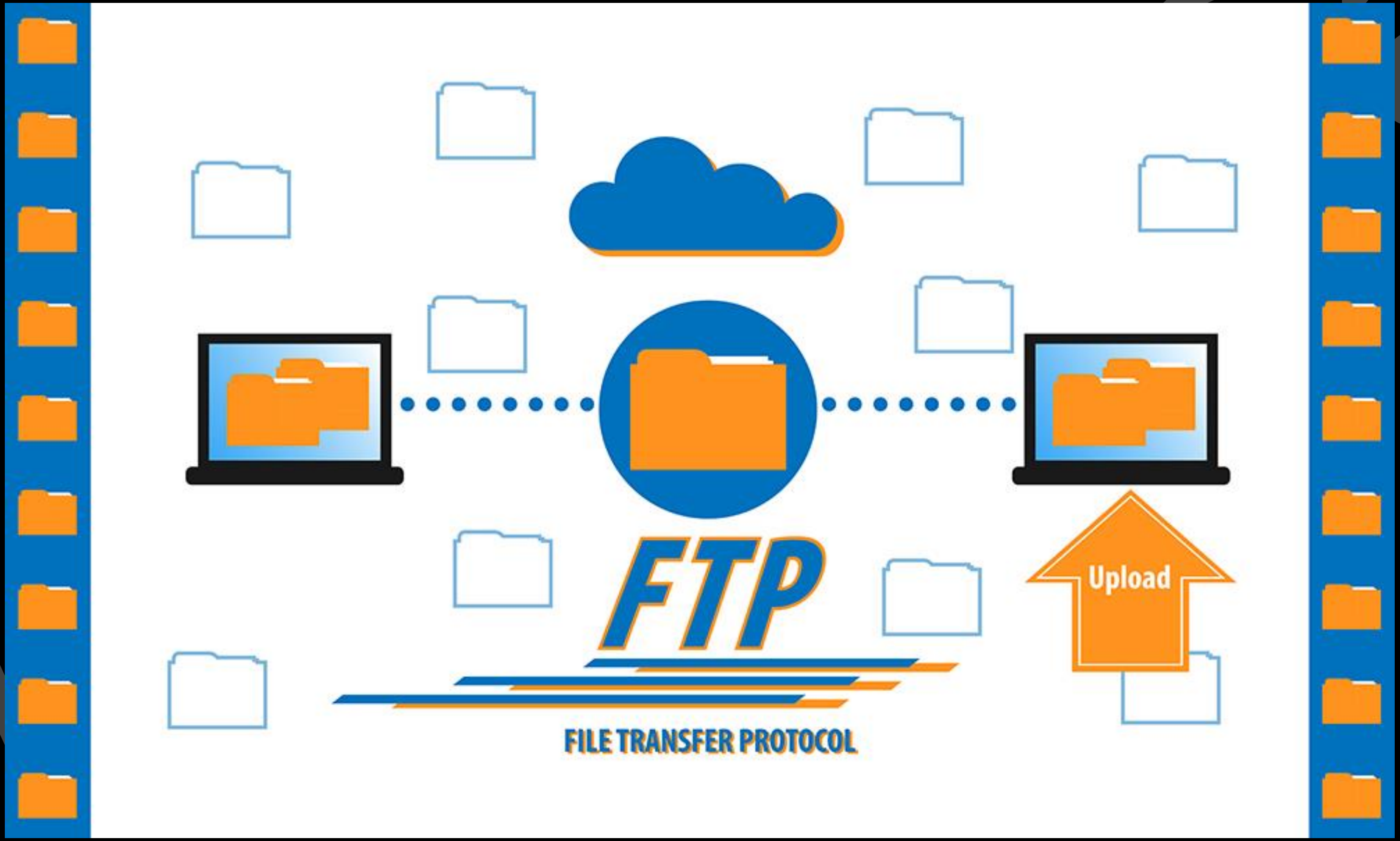
- Finally, the message from the receiving server (the Web server) to Bob's browser is done through HTTP.

- The last phase is very interesting. Instead of POP3 or IMAP4, HTTP is normally used. When Bob needs to retrieve his e-mails, he sends a message to the website (Hotmail, for example).

- The website sends a form to be filled in by Bob, which includes the log-in name and the password. If the log-in name and password match, the e-mail is transferred from the Web server to Bob's browser in HTML format.

FILE TRANSFER

- Transferring files from one computer to another is one of the most common tasks expected from a networking or internetworking environment. As a matter of fact, the greatest volume of data exchange in the Internet today is due to file transfer.



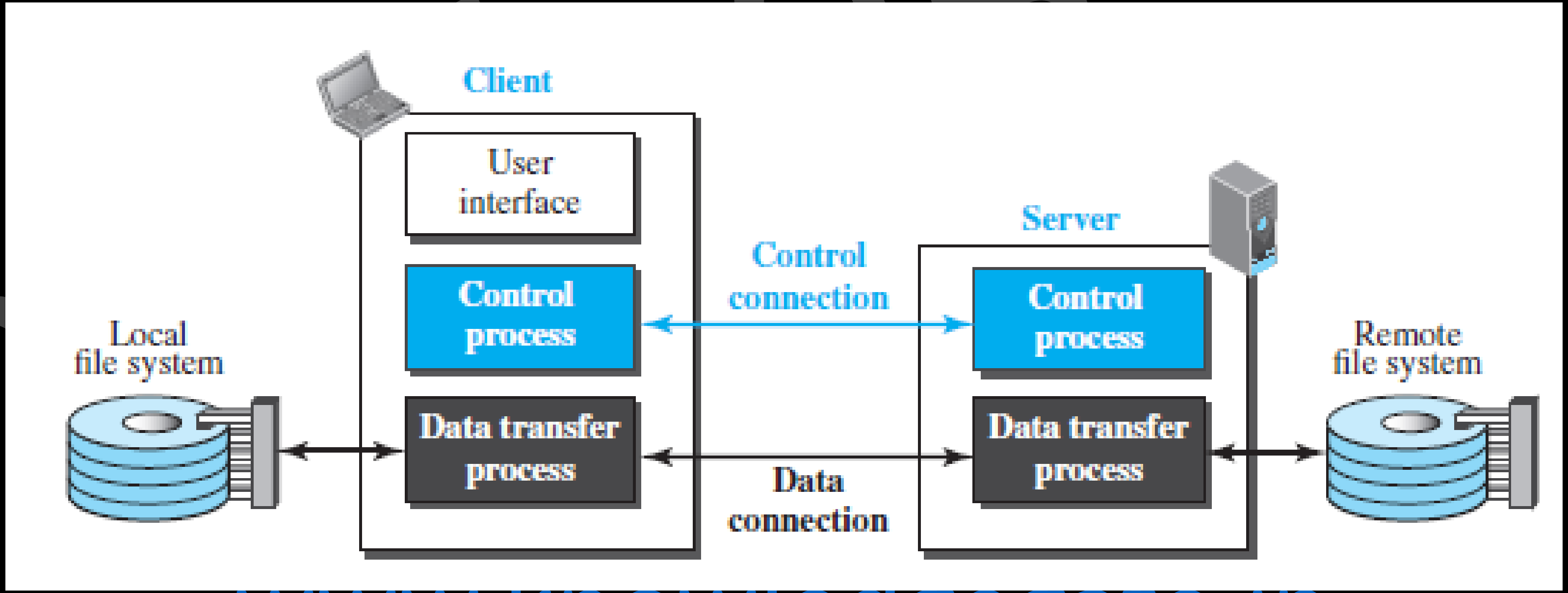
File Transfer Protocol (FTP)

- It is used for exchanging files over the internet and enables the users to upload and download the files from the internet.

- File Transfer Protocol (FTP) is the standard mechanism provided by TCP/IP for copying a file from one host to another. Although transferring files from one system to another seems simple and straightforward, some problems must be dealt with first. For example, two systems may use different file name conventions.

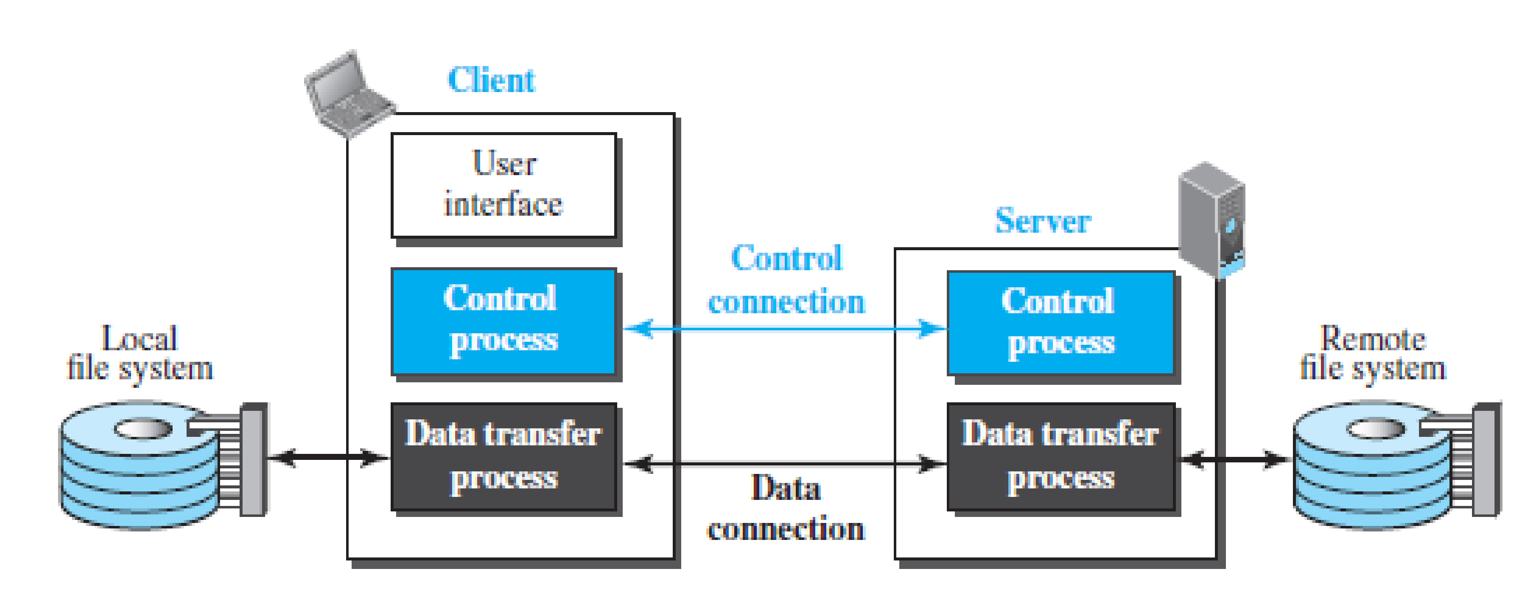
- Two systems may have different ways to represent text and data. Two systems may have different directory structures.

- All these problems have been solved by FTP in a very simple and elegant approach. FTP differs from other client/server applications in that it establishes two connections between the hosts.



- One connection is used for data transfer, the other for control information (commands and responses). Separation of commands and data transfer makes FTP more efficient. The control connection uses very simple rules of communication. We need to transfer only a line of command or a line of response at a time. The data connection, on the other hand, needs more complex rules due to the variety of data types transferred.

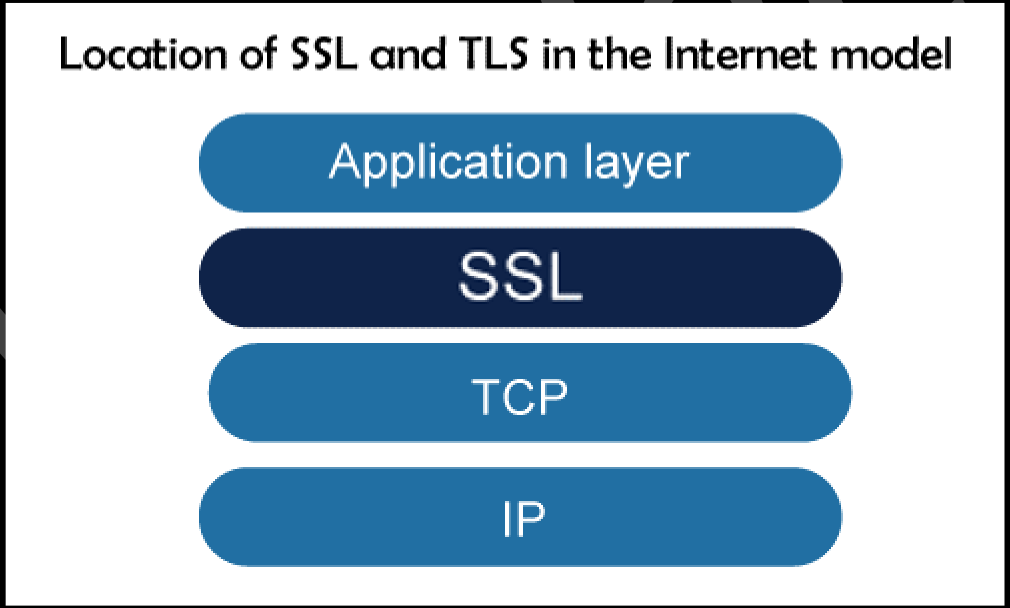
- However, the difference in complexity is at the FTP level, not TCP. For TCP, both connections are treated the same. FTP uses two well-known TCP ports: Port 21 is used for the control connection, and port 20 is used for the data connection. The control connection remains connected during the entire interactive FTP session. The data connection is opened and then closed for each file transfer activity.



Security for FTP

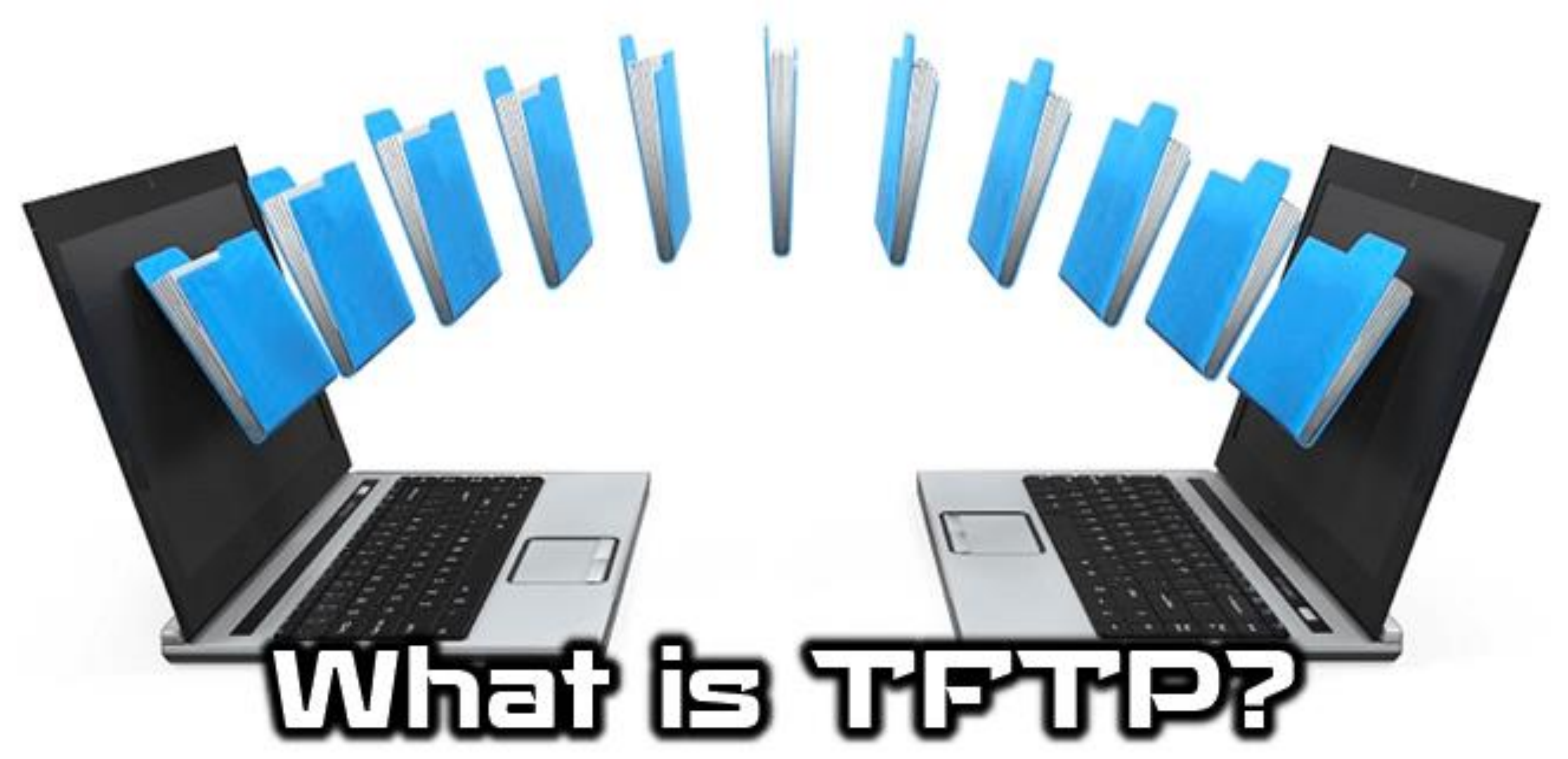
- The FTP protocol was designed when security was not a big issue. Although FTP requires a password, the password is sent in plaintext (unencrypted), which means it can be intercepted and used by an attacker. The data transfer connection also transfers data in plaintext, which is insecure.

- To be secure, one can add a Secure Socket Layer between the FTP application layer and the TCP layer. In this case FTP is called SSL-FTP.


Location of SSL and TLS in the Internet model

Trivial File Transfer Protocol (TFTP)

- TFTP is a simple, UDP-based file transfer protocol that supports only basic read and write operations, typically using port 69, and is often used for booting systems or initial configurations.
- Due to its lack of authentication and encryption, as well as minimal error handling, TFTP is not suitable for secure or reliable long-distance file transfers.
- Although largely replaced by more secure and feature-rich protocols like FTPS and SFTP, TFTP's simplicity and minimal resource requirements make it useful for specific, local network applications.



WWW

- The idea of the Web was first proposed by Tim Berners-Lee in 1989 CERN (European Laboratory for Particle Physics) to create a system to handle distributed resources necessary for scientific research.

- The World Wide Web (WWW) is a repository of information linked together from points all over the world. It a unique combination of flexibility, portability, and user-friendly features that distinguish it from other services provided by the Internet.

- **ARCHITECTURE**
  - The WWW today is a distributed client server service, in which a client using a browser can access a service using a server. However, the service provided is distributed over many locations called sites.
  - Each site holds one or more documents, referred to as Web pages. Each Web page can contain a link to other pages in the same site or at other sites. The pages can be retrieved and viewed by using browsers.

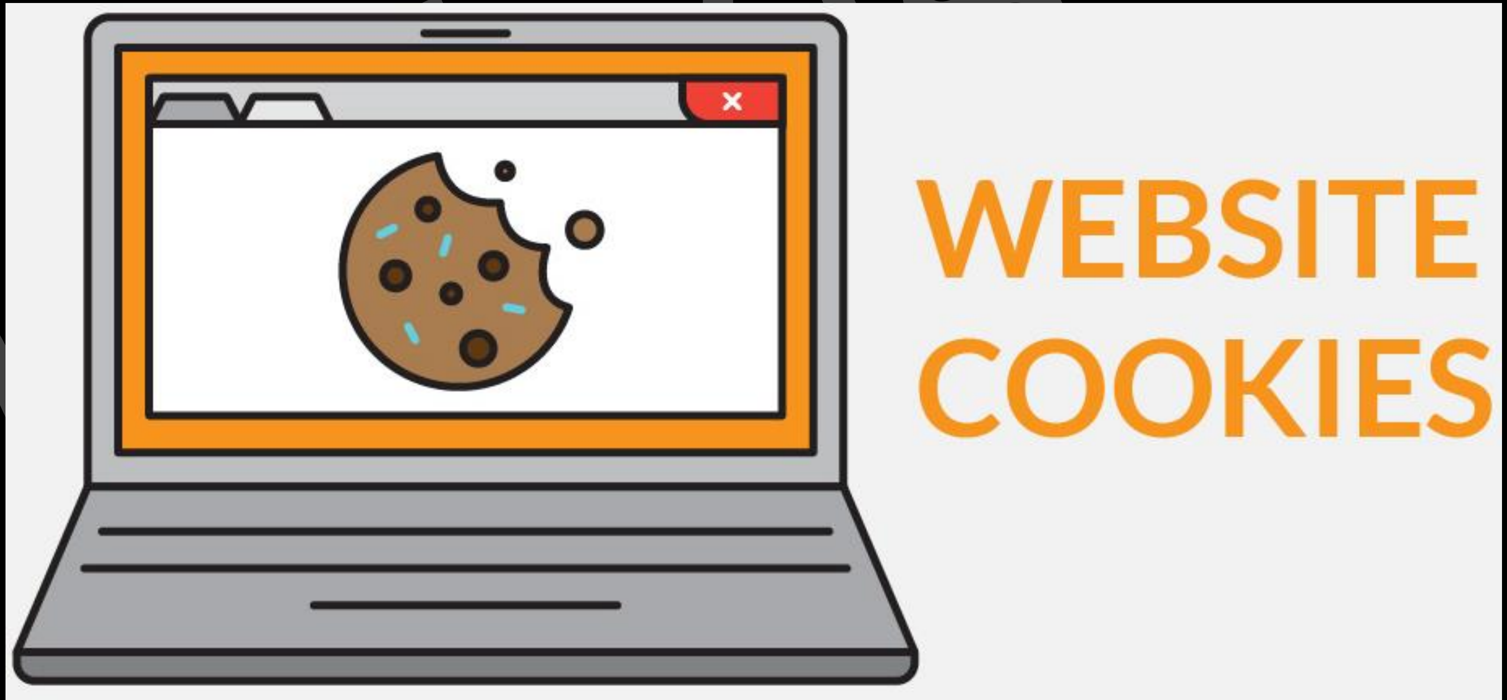
- **Client (Browser)**
  - A variety of vendors offer commercial browsers that interpret and display a Web document, and all use nearly the same architecture.
  - Each browser usually consists of three parts: a controller, client protocol, and interpreters.
  - The controller receives input from the keyboard or the mouse and uses the client programs to access the document. After the document has been accessed, the controller uses one of the interpreters to display the document on the screen.

- **Server**
  - The Web page is stored at the server. Each time a client request arrives, the corresponding document is sent to the client.
  - To improve efficiency, servers normally store requested files in a cache in memory; memory is faster to access than disk.
  - A server can also become more efficient through multithreading or multiprocessing. In this case, a server can answer more than one request at a time.
  - A client that wants to access a Web page needs the address. To facilitate the access of documents distributed throughout the world, HTTP uses locators.

- **Uniform Resource Locator (URL)**
  - A web page, as a file, needs to have a unique identifier to distinguish it from other web pages.
  - To define a web page, we need four identifiers in general: ***Protocol***, ***host, port, and path.***
  - ***Protocol*****.** Which client-server application we are using is called protocol. Although most of the time the protocol is HTTP (Hyper Text Transfer Protocol), we can also use other protocols such as FTP (File Transfer Protocol).
  - ***Host.*** The host identifier can be the IP address of the server or the unique name to the server.
  - ***Port*****.** The port, a 16-bit integer, is normally predefined for the client-server application.

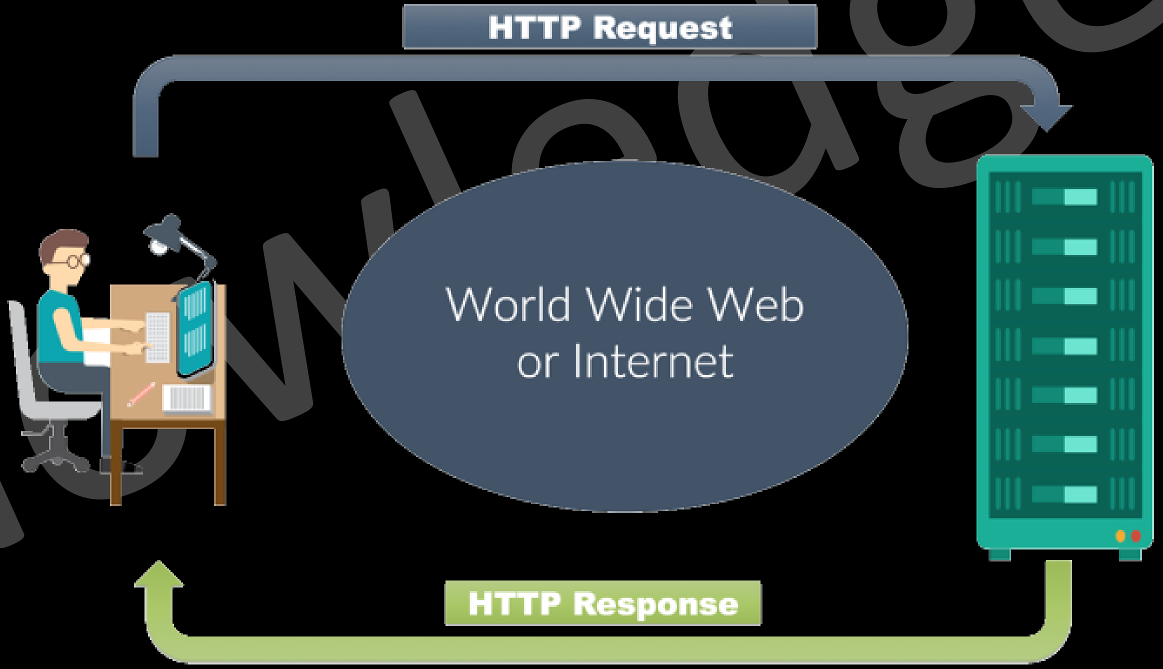
Cookies

- Cookies enable stateful interactions on the World Wide Web, allowing websites to remember users and their activities, such as login status or items in a shopping cart.
- Upon a client's request, the server creates a cookie containing user information and sends it back to the client; the client's browser stores this cookie.
- During subsequent interactions, the client's browser sends the stored cookie back to the server, allowing the server to recognize returning clients and provide a more personalized experience.



HTTP

- The Hypertext Transfer Protocol (HTTP) is a protocol used mainly to access data on the World Wide Web. The **Hyper Text Transfer Protocol (HTTP)** is used to define how the client-server programs can be written to retrieve web pages from the Web.
- HTTP uses the services of TCP on well-known port 80, the client uses a temporary port number.
- It is a connection-oriented and reliable protocol.
- HTTP functions as a combination of FTP and SMTP.



- It is similar to FTP because it transfers files and uses the services of TCP. However, it is much simpler than FTP because it uses only one TCP connection. There is no separate control connection; only data are transferred between the client and the server.

- HTTP is like SMTP because the data transferred between the client and the server look like SMTP messages. Unlike SMTP, the HTTP messages are not destined to be read by humans; they are read and interpreted by the HTTP server and HTTP client (browser).

- SMTP messages are stored and forwarded, but HTTP messages are delivered immediately. The commands from the client to the server are embedded in a request message. The contents of the requested file or other information are embedded in a response message.

Nonpersistent versus Persistent Connections

- ***Nonpersistent Connections***: - In a **nonpersistent connection**, one TCP connection is made for each request/response. The following lists the steps in this strategy:
  - The client opens a TCP connection and sends a request.
  - The server sends the response and closes the connection.
  - The client reads the data until it encounters an end-of-file marker; it then closes the connection.
  - **For example:** If a file contains links to N different pictures in different files (all located on the same server), the connection must be opened and closed N + 1 times.

- **Disadvantage** The nonpersistent strategy imposes high overhead on the server because the server needs N + 1 different buffer each time a connection is opened.

Persistent Connections

- HTTP version 1.1 specifies a **persistent connection** by default.
- In a persistent connection, the server leaves the connection open for more requests after sending a response.
- The server can close the connection at the request of a client or if a time-out has been reached.

- **Advantages**
  - Time and resources are saved using persistent connections.
  - Only one set of buffers and variables needs to be set for the connection at each site.
  - The round-trip time for connection establishment and connection termination is saved.

- ***It is important to know that HTTP is a stateless protocol as:***
  - HTTP server does not maintain any state. It forgets about the client after sending the response.
  - It treats every new request independently.

- ***HTTP Security***
  - HTTP per se does not provide security.
  - HTTP can be run over the Secure Socket Layer (SSL). In this case, HTTP is referred to as HTTPS.
  - HTTPS provides confidentiality, client and server authentication, and data integrity.

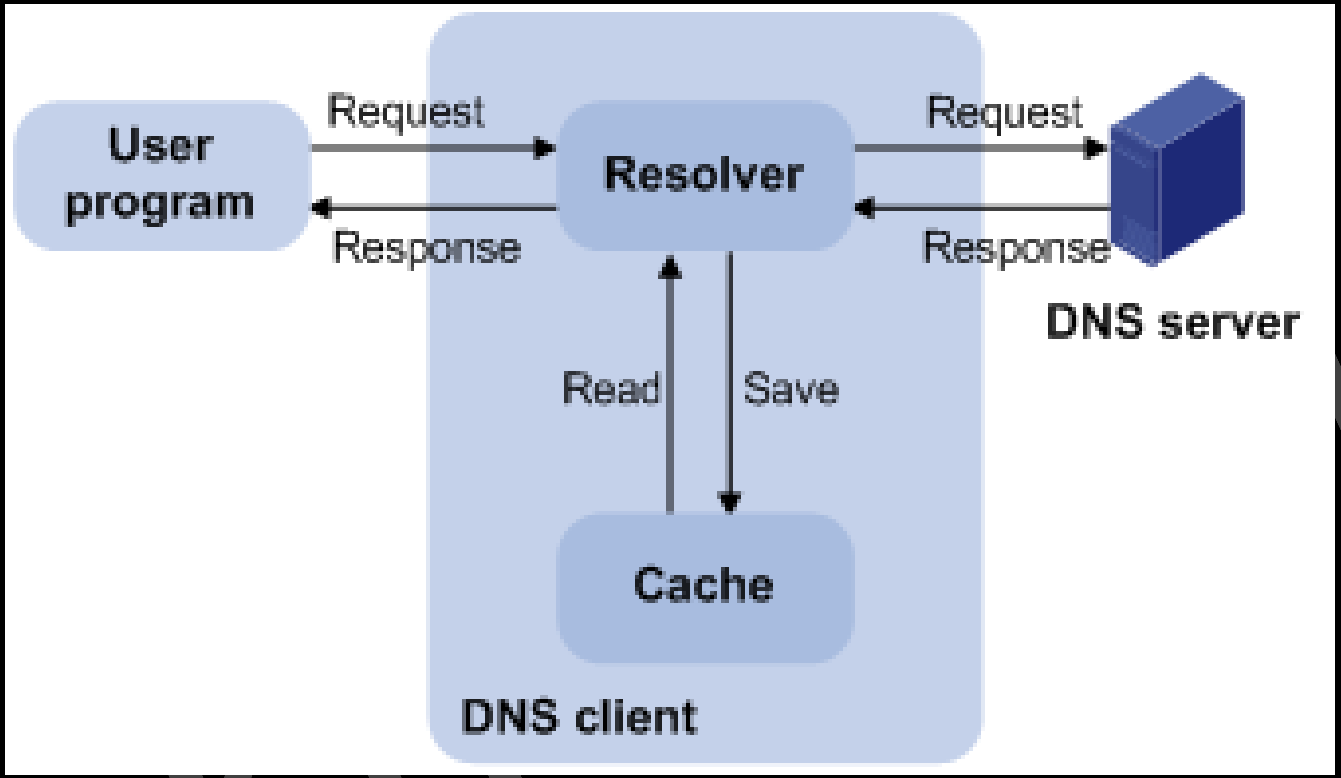
DNS

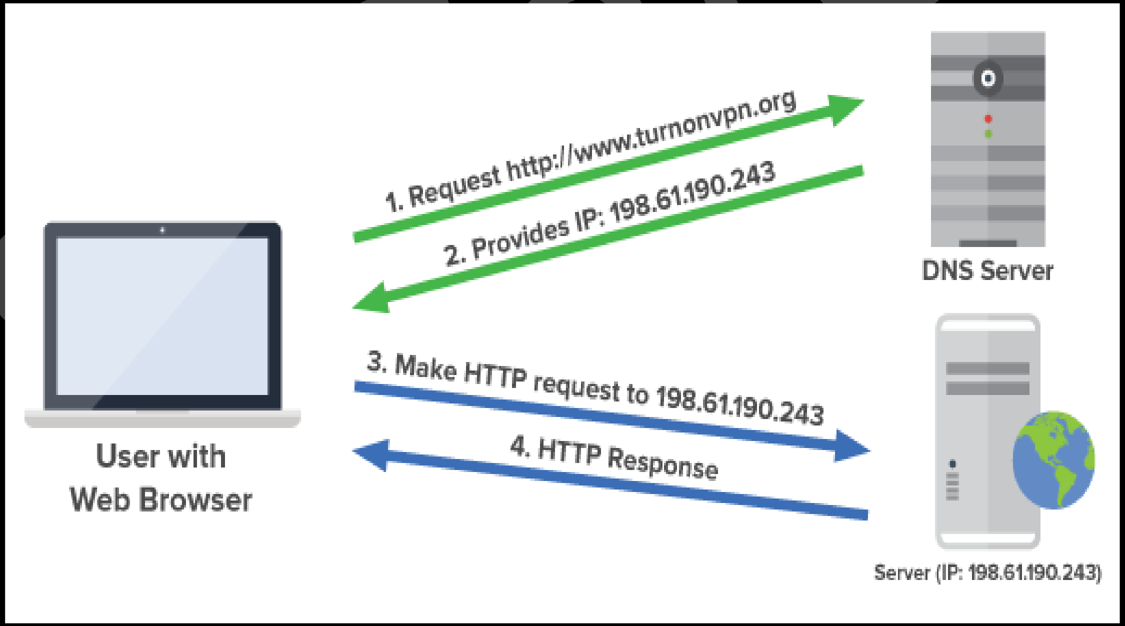
- As we know human beings are not comfortable in remembering numbers so to remember IP address of a website or mail account in internet is difficult. Secondly IP addresses of mail or websites keeps on changing, so we have to come up with one more level of addressing which is easy to remember and do not change with time.

- Solution is Name addressing, i.e. we give some names to websites and mail account like we do to humans in real world. But then if someone write a name of the website in the browser we need some mechanism to convert it back into IP address.

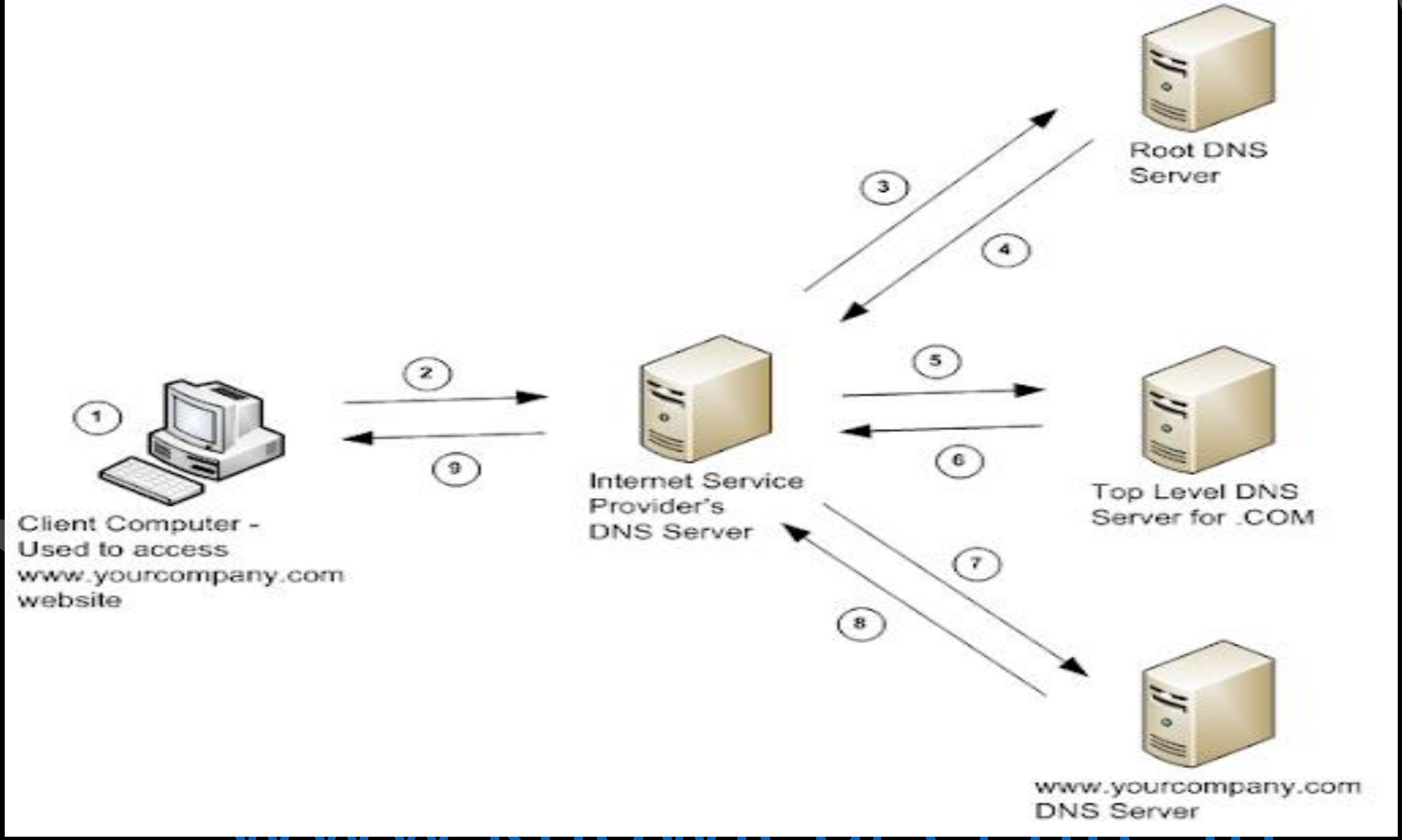
- Domain Name System solve this problem.

- This diagram perfectly represent how DNS works, A user of a website may know the name of the website; however, the IP protocol needs the IP address.
- The DNS client program sends a request to a DNS server to map the Web-site address to the corresponding IP address.

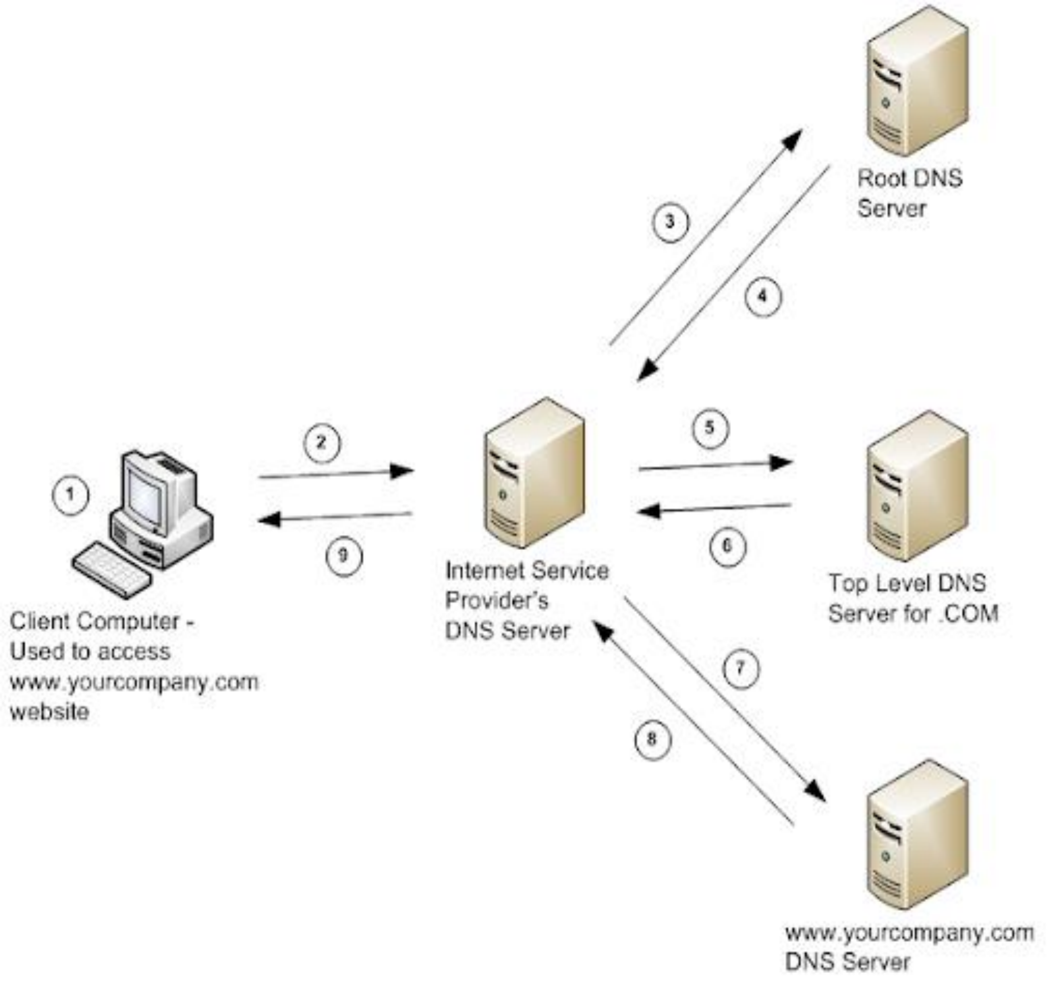



1. Request http://www.turnonvpn.org
2. Provides IP: 198.61.190.243
DNS Server
User with Web Browser
3. Make HTTP request to 198.61.190.243
4. HTTP Response
Server (IP: 198.61.190.243)

- Today we divide this huge amount of information into smaller parts and store each part on a different computer. In this method, the host that needs mapping can contact the closest computer holding the needed information.
- It is Very difficult to find out the ip address associated to a website because there are millions of websites and with all those websites, we should be able to generate the ip address immediately, there should not be a lot of delay for that to happen organization of database is very important.


Root DNS Server
3
4
1
2
9
Internet Service Provider's DNS Server
5
6
Top Level DNS Server for .COM
Client Computer - Used to access www.yourcompany.com website
7
8
www.yourcompany.com DNS Server

- **Hierarchy of Name Servers**
    - **Root name servers** – It is contacted by name servers that cannot resolve the name. It contacts authoritative name server if name mapping is not known. It then gets the mapping and return the IP address to the host.
    - **Top level server** – It is responsible for com, org, edu etc and all top-level country domains like uk, fr, ca, in etc. They have info about authoritative domain servers and know names and IP addresses of each authoritative name server for the second level domains.
    - **Authoritative name servers** This is organization's DNS server, providing authoritative hostName to IP mapping for organization servers. It can be maintained by organization or service provider. In order to reach cse.dtu.in we have to ask the root DNS server, then it will point out to the top-level domain server and then to authoritative domain name server which actually contains the IP address. So, the authoritative domain server will return the associative ip address.



Root DNS Server
3
4
1
2
9
5
6
Client Computer - Used to access www.yourcompany.com website
Internet Service Provider's DNS Server
Top Level DNS Server for .COM
7
8
www.yourcompany.com DNS Server

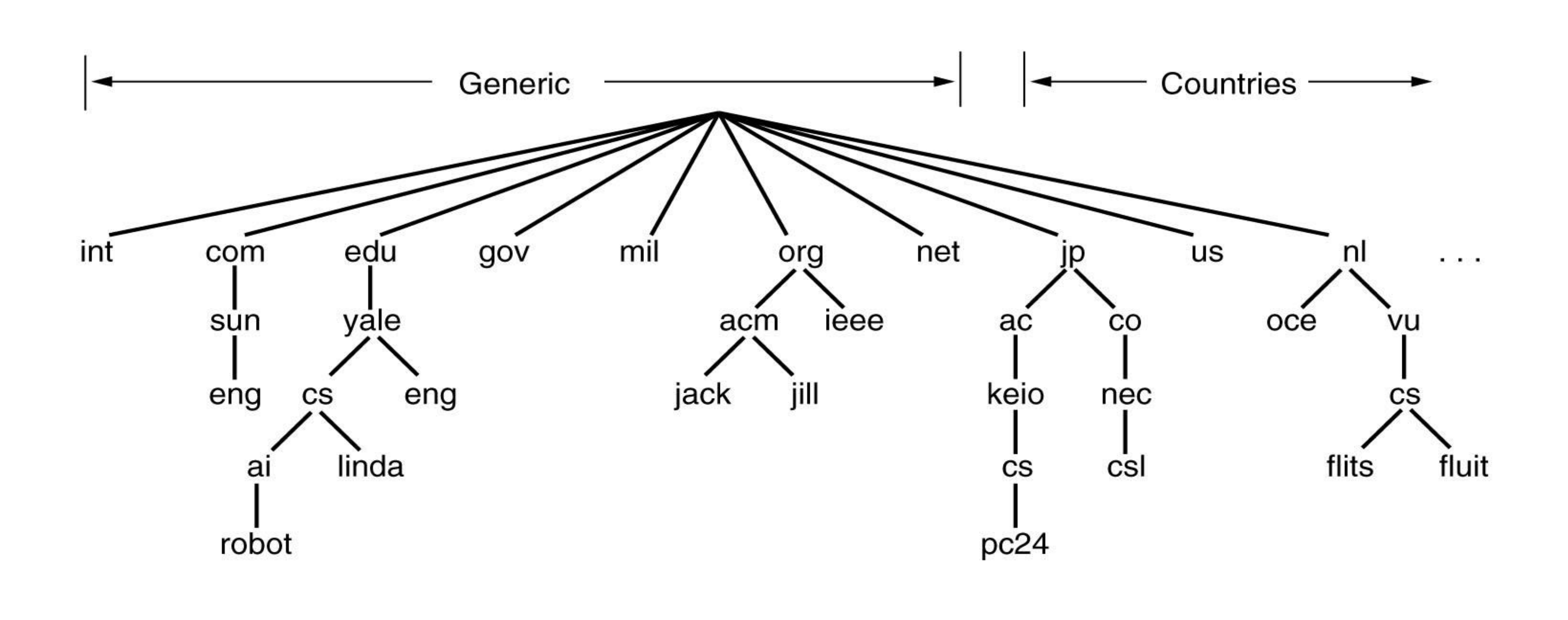
NAME SPACE

- To be unambiguous, the names must be unique because the addresses are unique. A name space that maps each address to a unique name can be organized in two ways: flat or hierarchical.

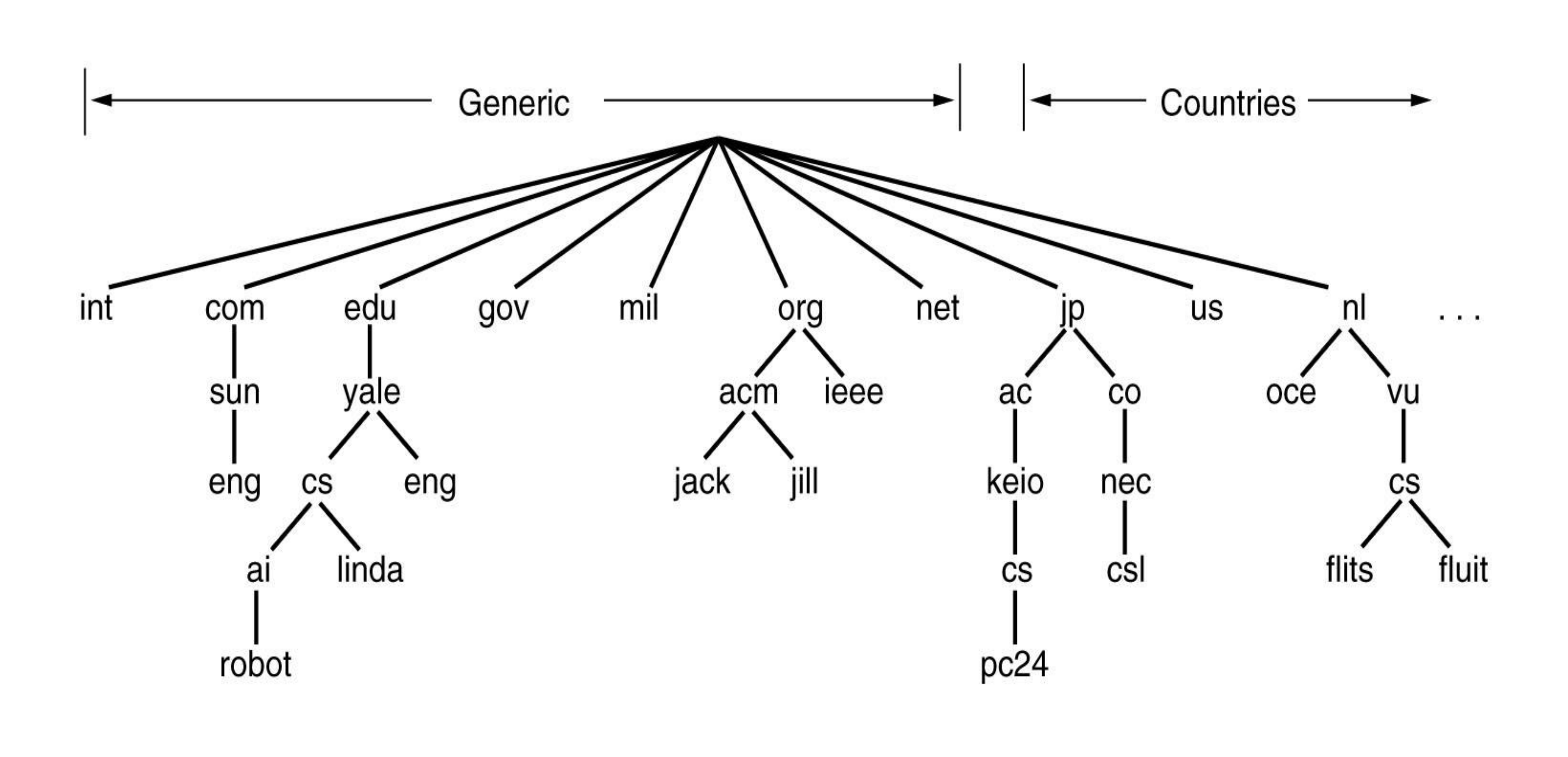
- **Flat Name Space**
  - In a flat name space, a name is assigned to an address. A name in this space is a sequence of characters without structure.
  - The main disadvantage of a flat name space is that it cannot be used in a large system such as the Internet because it must be centrally controlled to avoid ambiguity and duplication.
  - So, Solution is Hierarchical Name Space

Hierarchical Name Space

- In a hierarchical name space, each name is made of several parts. The first part can define the nature of the organization
- the second part can define the name of an organization, the third part can define departments in the organization, and so on.
- In this case, the authority to assign and control the name spaces can be decentralized. A central authority can assign the part of the name that defines the nature of the organization and the name of the organization.
- The responsibility of the rest of the name can be given to the organization itself.
- The management of the organization need not worry that the prefix chosen for a host is taken by another organization because, even if part of an address is the same, the whole address is different

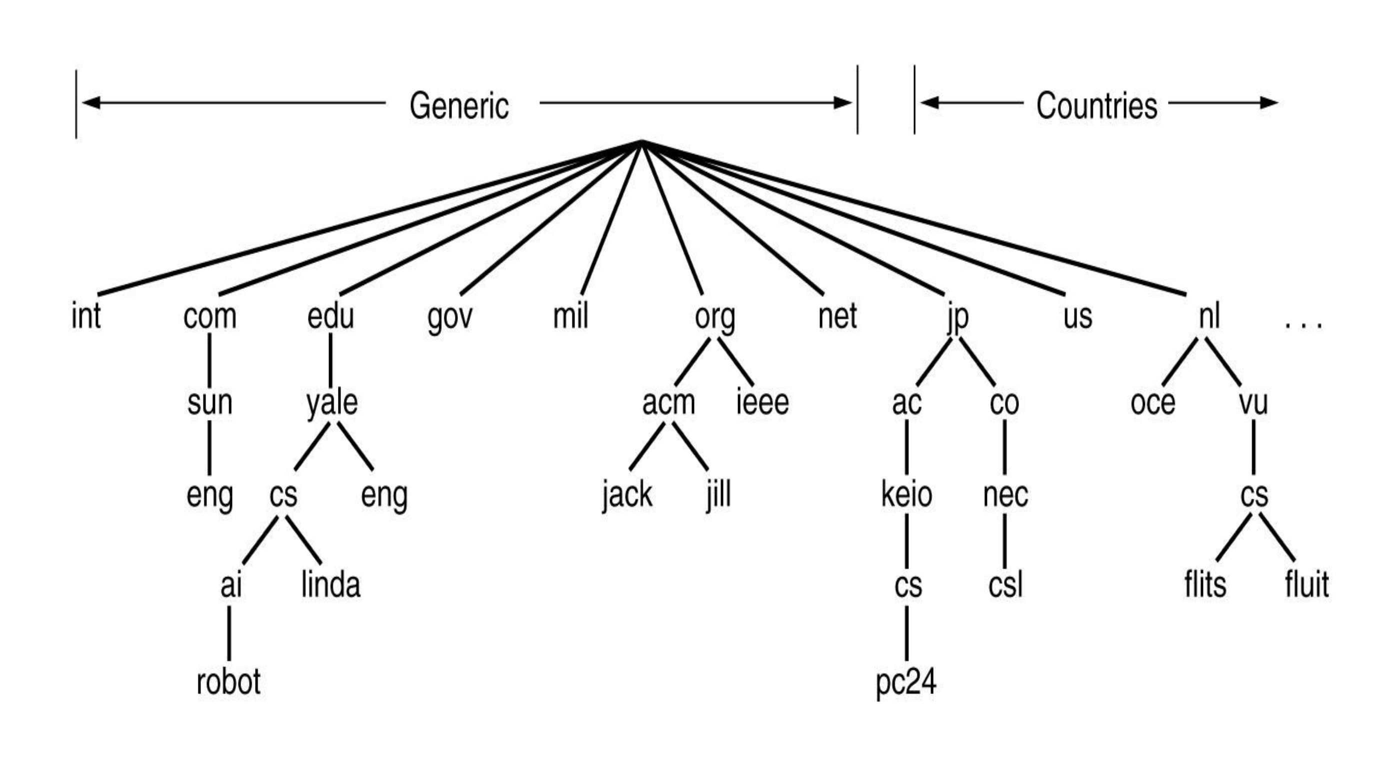


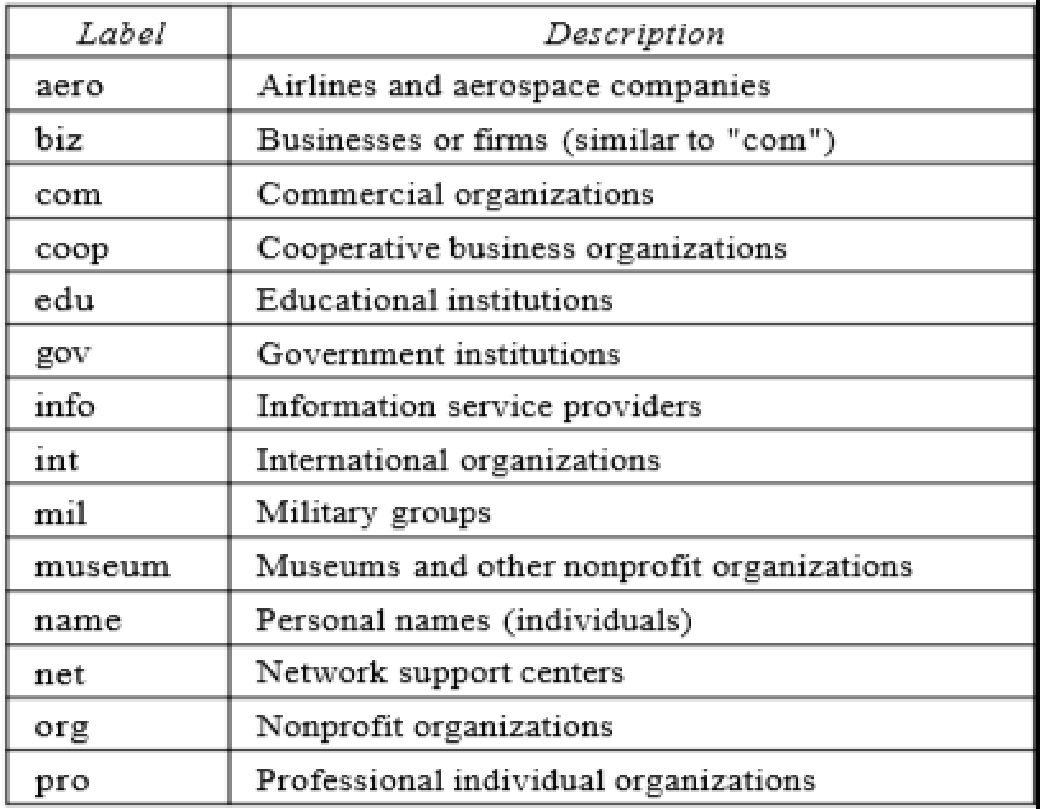
- Generic domain: .com(commercial) .edu(educational) .mil(military) .org (non-profit organization) .net (similar to commercial) all these are generic domain.
- Country domain .in (india) .us .uk
- Inverse domain if we want to know what is the domain name of the website. Ip to domain name mapping. So, DNS can provide both the mapping for example to find the ip addresses of www.unacademy.com then we have to type nslookup www.unacademy.com



DOMAIN NAME SPACE

- To have a hierarchical name space, a domain name space was designed. In this design the names are defined in an inverted-tree structure with the root at the top. The tree can have only 128 levels: level 0 (root) to level 127

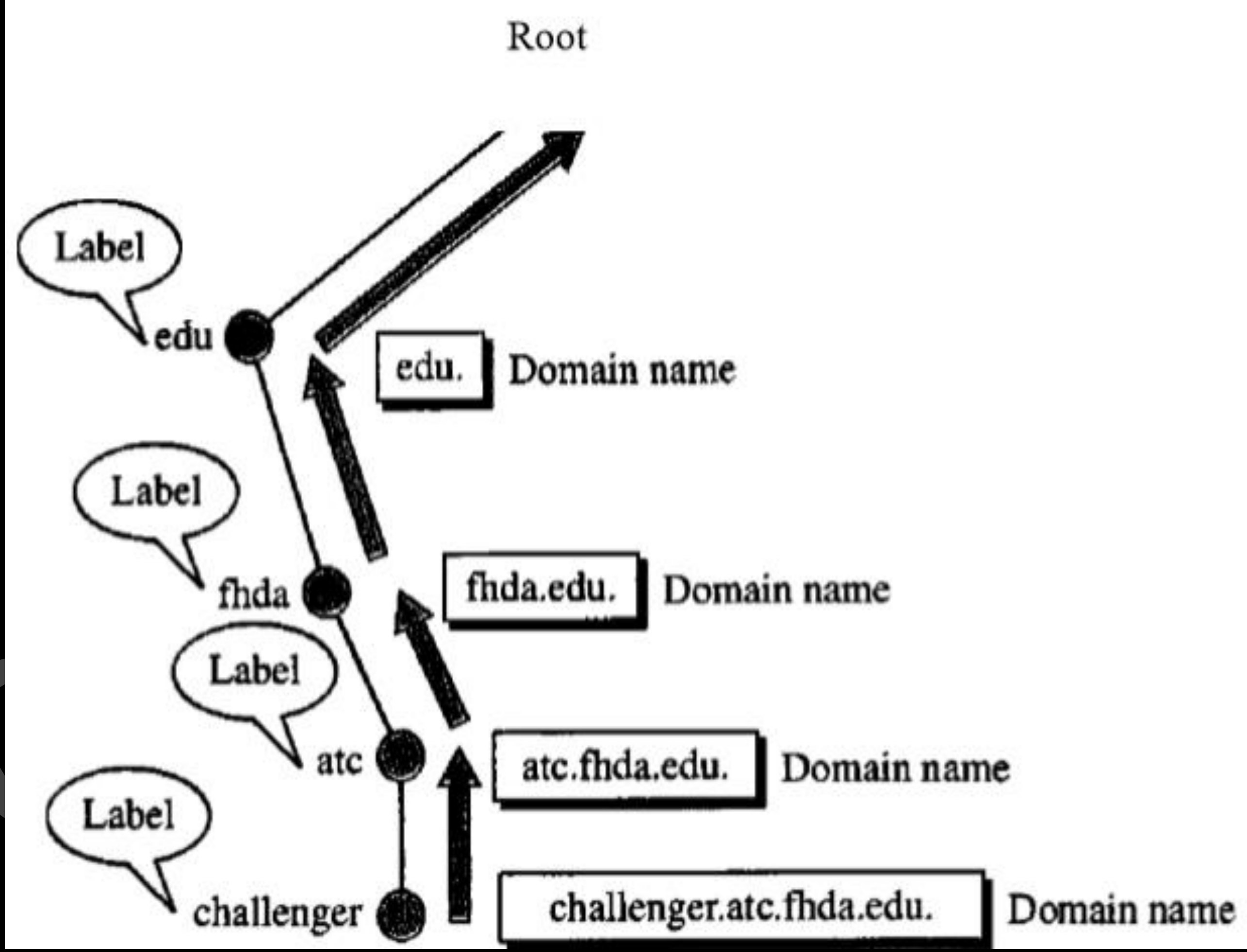




Label	*Description*
aero	Airlines and aerospace companies
biz	Businesses or firms (similar to "com")
com	Commercial organizations
coop	Cooperative business organizations
edu	Educational institutions
gov	Government institutions
info	Information service providers
int	International organizations
mil	Military groups
museum	Museums and other nonprofit organizations
name	Personal names (individuals)
net	Network support centers
org	Nonprofit organizations
pro	Professional individual organizations

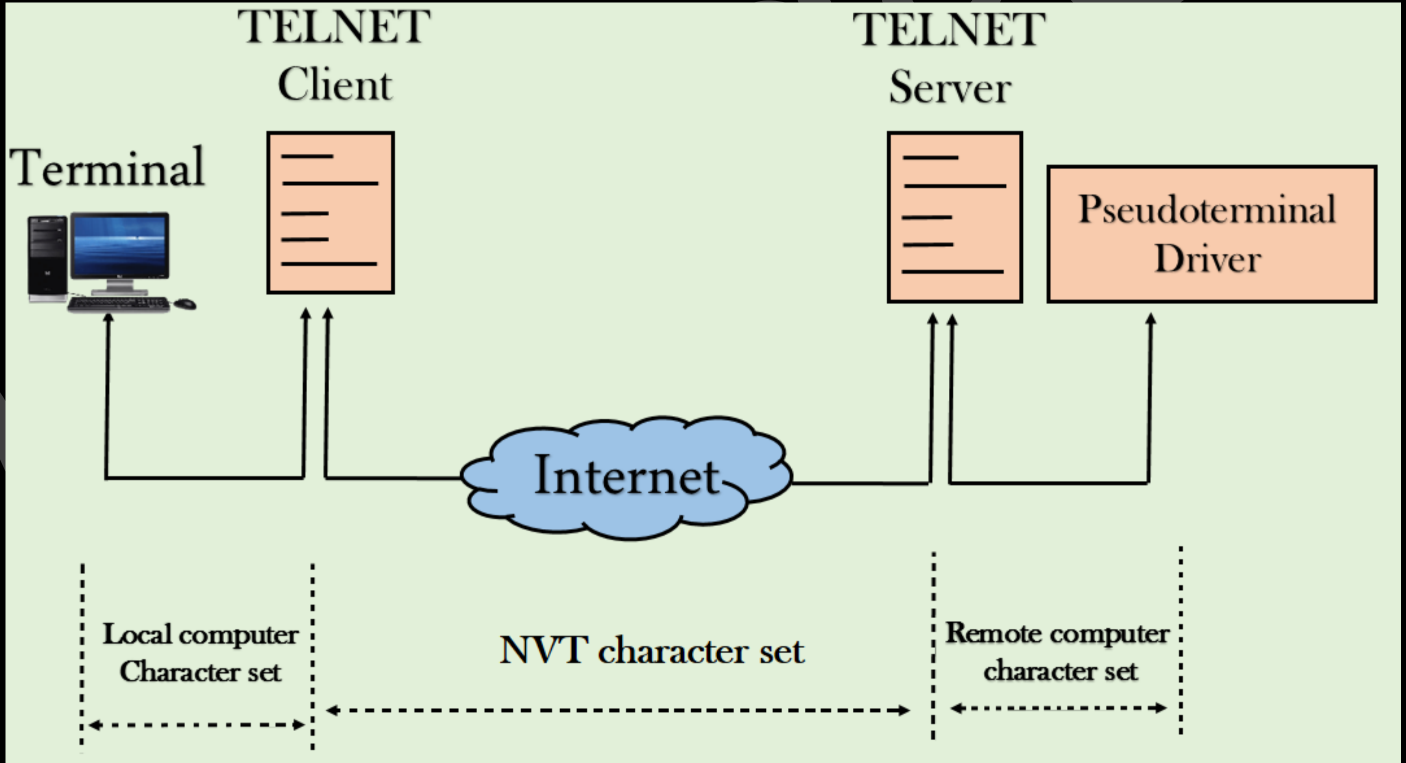
- **Label**
  - Each node in the tree has a label, which is a string with a maximum of 63 characters.
  - The root label is a null string (empty string).
  - DNS requires that children of a node (nodes that branch from the same node) have different labels, which guarantees the uniqueness of the domain names.

- **Domain Name**
  - Each node in the tree has a domain name. A full domain name is a sequence of labels separated by dots (.).
  - The domain names are always read from the node up to the root. The last label is the label of the root (null). This means that a full domain name always ends in a null label, which means the last character is a dot because the null string is nothing.



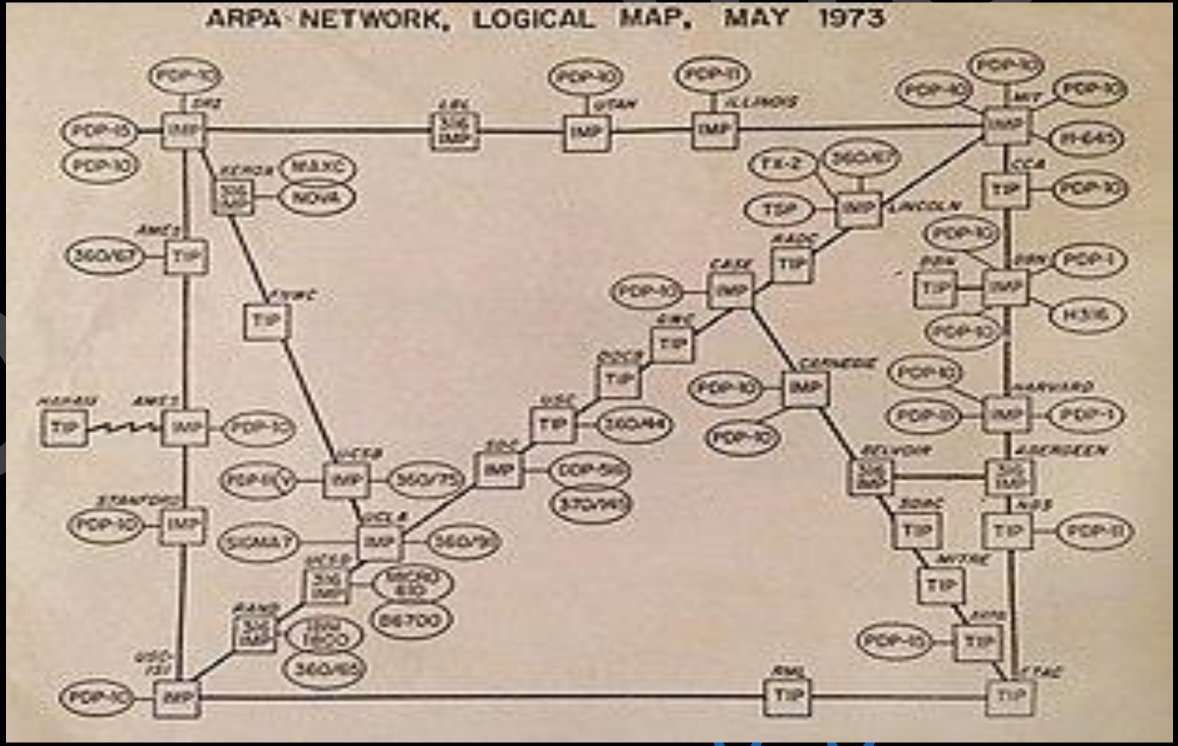
Telnet (Telecommunication Network)

- Telnet is a text-based protocol used for remote access to servers, operating on TCP port 23 and following a client-server model, but lacks data encryption.
- Although useful for debugging and interactive sessions, its lack of security measures makes it susceptible to eavesdropping and unsuitable for transmitting sensitive information.
- Largely replaced by more secure alternatives like SSH, Telnet still finds use in legacy systems and specialized applications where high security is not crucial.



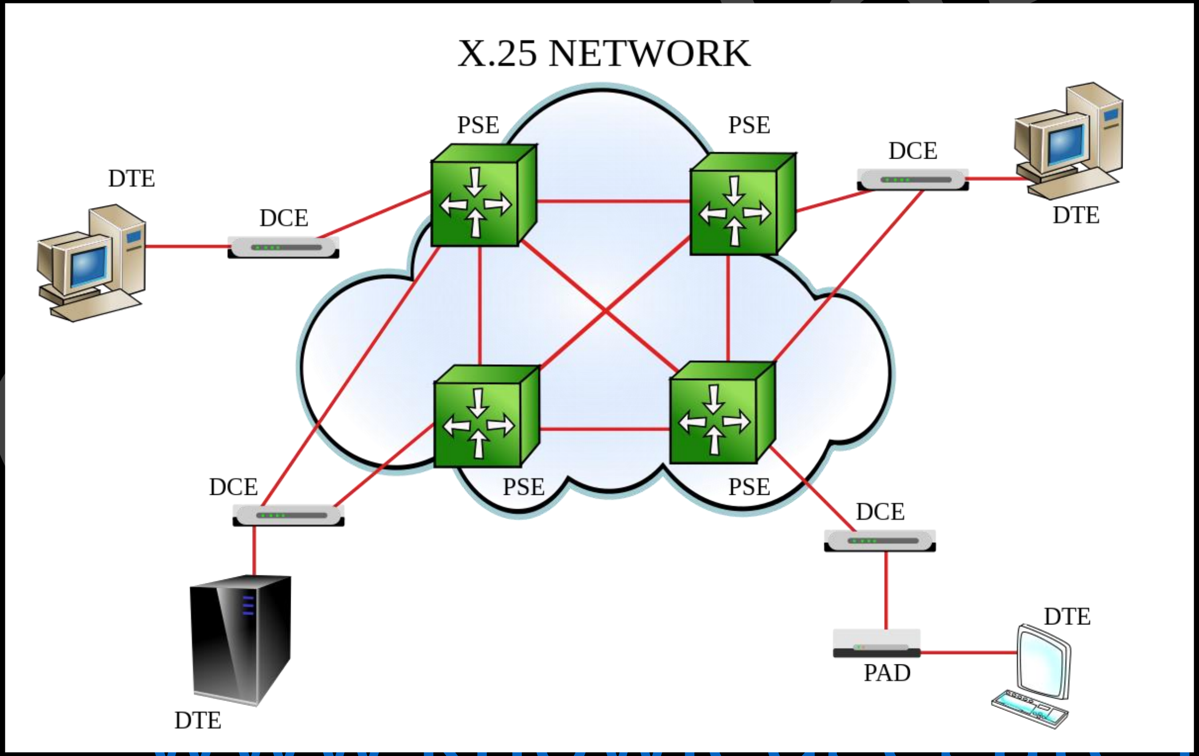
ARPANET (Advanced Research Projects Agency Network)

- ARPANET was the first wide-area network using packet switching, created in the late 1960s by the U.S. Department of Defense, and it laid the groundwork for today's internet.
- It introduced early networking protocols like NCP, gave rise to applications like email, and was designed for research and resource sharing, expanding to connect hundreds of institutions over time.
- Though decommissioned in 1990, its technologies and concepts had a lasting impact, inspiring subsequent networks and internet protocols, but initially lacked strong security measures.



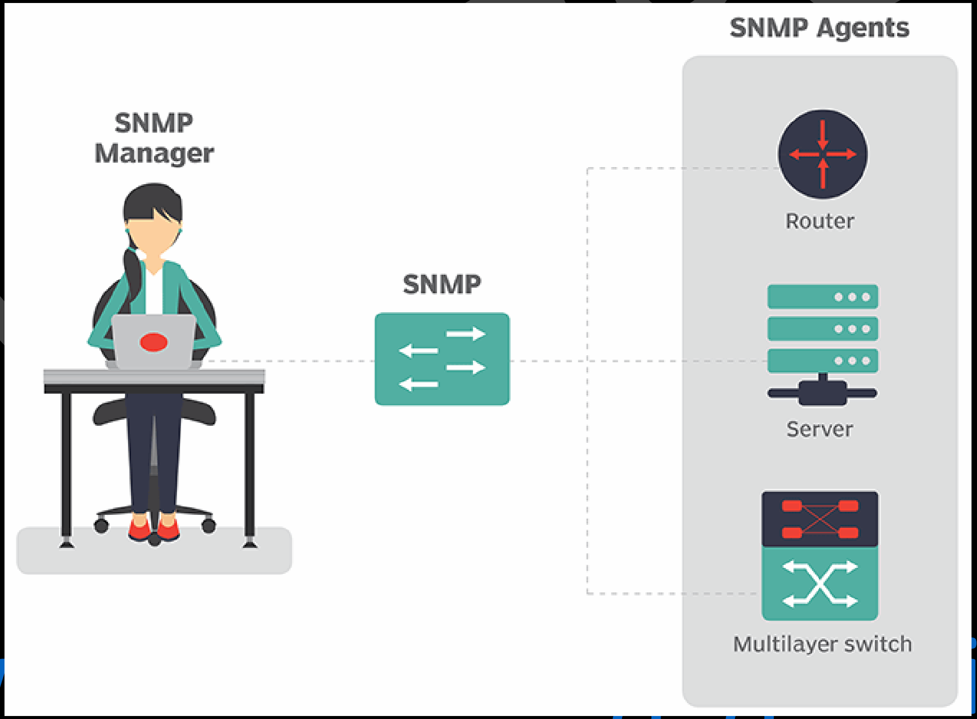
X.25

- X.25 is an old protocol for wide area networks that includes features for error checking, virtual circuit setup, and usage-based billing, operating across three layers of the OSI model.
- It was widely used in the past for applications like credit card processing and ATMs, supporting slower data rates initially but evolving over time.
- Although its usage has declined due to faster protocols like IP, it inspired newer technologies like Frame Relay and ATM and was a backbone for international data services before the Internet.



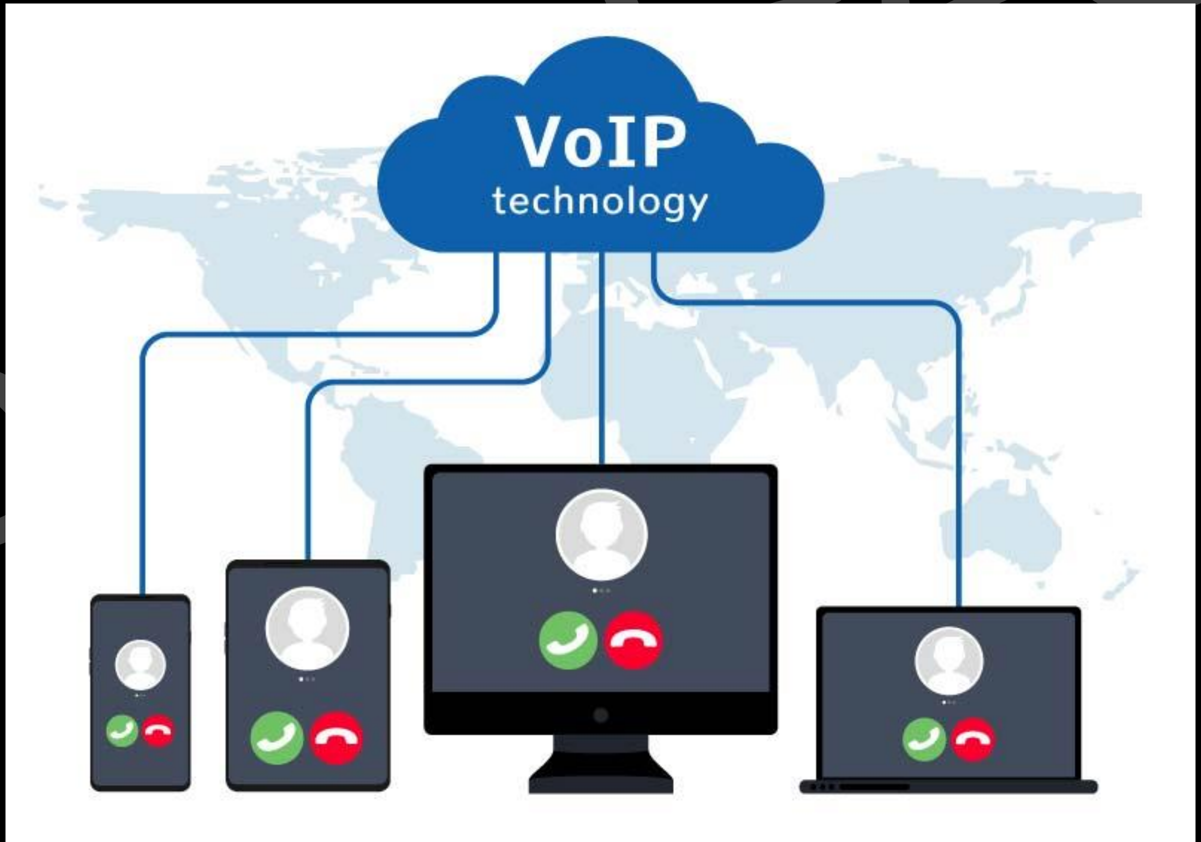
Simple Network Management Protocol (SNMP)

- SNMP is a common tool for managing and monitoring network devices; it operates over UDP and interacts with databases known as MIBs to control device properties.
- It works on a client-server model with an SNMP manager and agents, supports various operations like GET, SET, and TRAP, and comes in different versions with varying security features.
- It's scalable and used for real-time monitoring, collecting data either by polling from the manager to the agent or trapping where the agent notifies the manager about specific events.



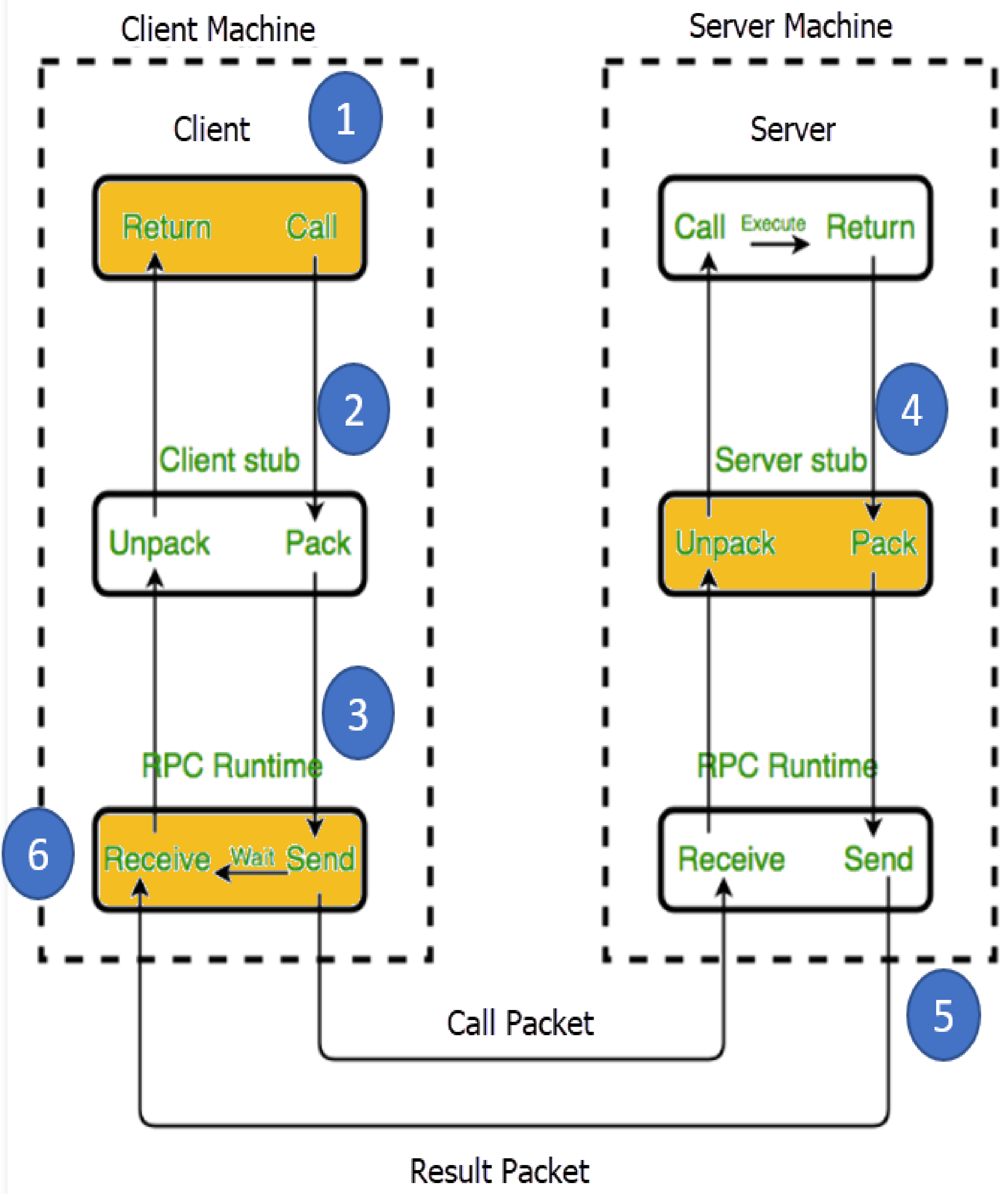
Voice over IP

- VoIP allows for versatile communication, including voice calls and multimedia, over IP networks, offering cost savings and network efficiency.
- Relies on a stable internet connection and computer hardware; any disruption can affect the telephone service.
- Susceptible to delays, security risks, and challenges in routing emergency calls due to the nature of IP networks.



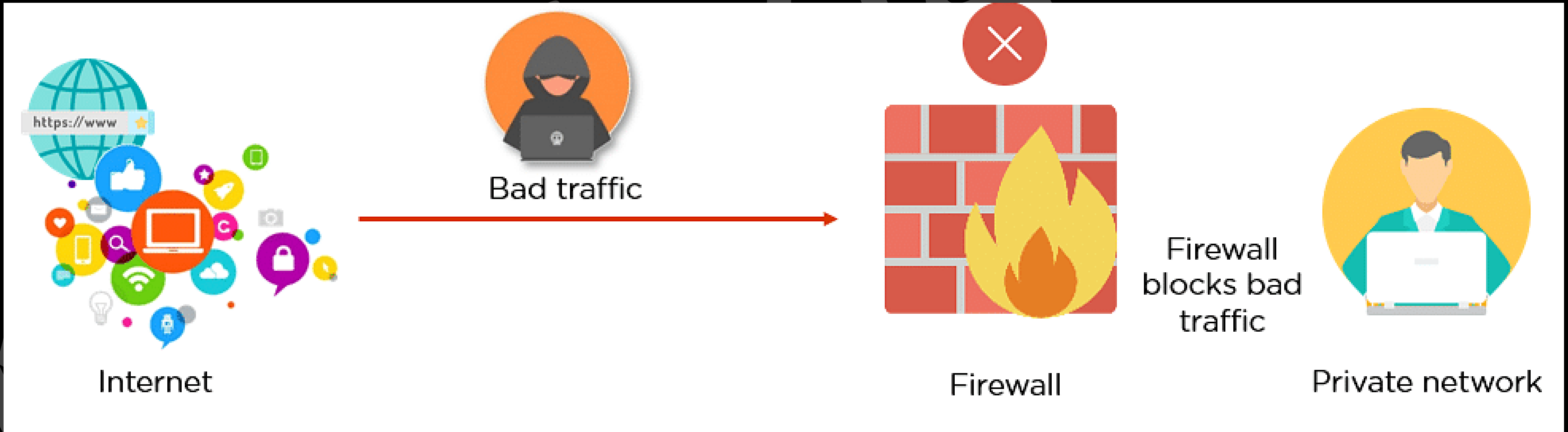
Remote Procedure Call

- Remote Procedure Call (RPC) allows programs to execute procedures (functions) on a remote server, as if they were local, facilitating distributed computing.
- Operates over various transport protocols such as TCP or HTTP and may include authentication and encryption features for secure communication.
- Often used in client-server architectures and distributed systems, but can introduce complexities like network latency and failure handling.



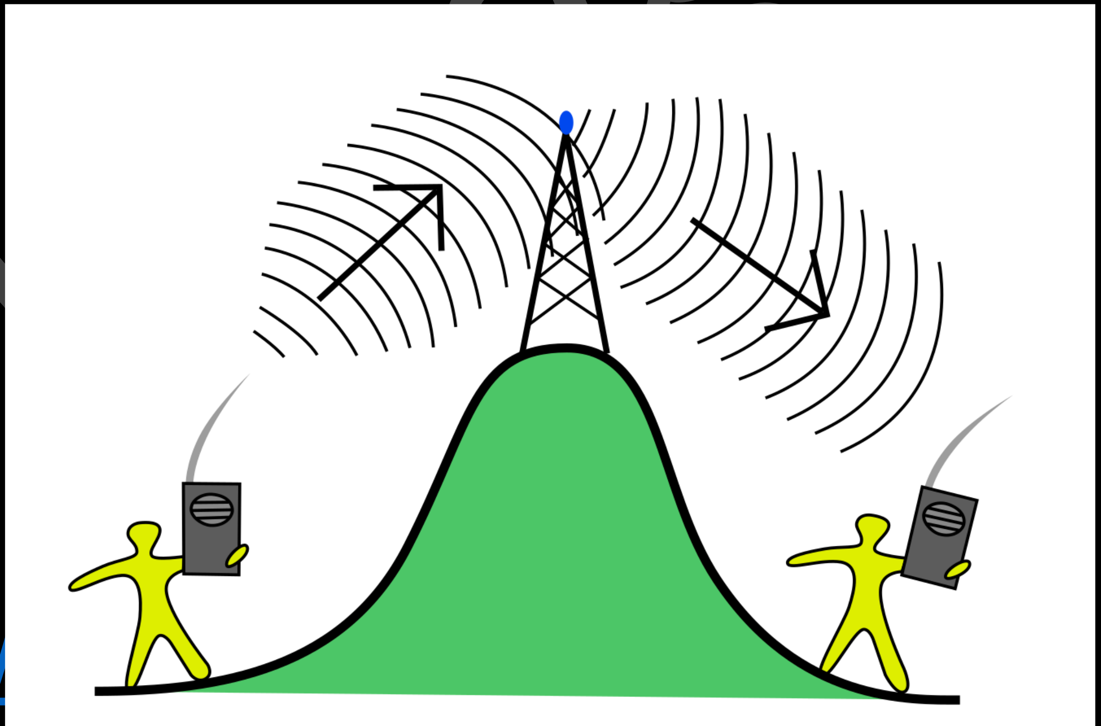
firewall

- Firewalls act as security guards for network traffic, checking data packets and allowing or blocking them based on set rules like IP addresses and port numbers.
- They offer different features like Stateful Inspection, Proxy Services, and VPN Support to enhance security measures, some even include intrusion detection systems.
- Types of firewalls range from hardware versions that are separate devices to software ones installed on individual computers, and they often come with logging and reporting features for network monitoring.



Repeater

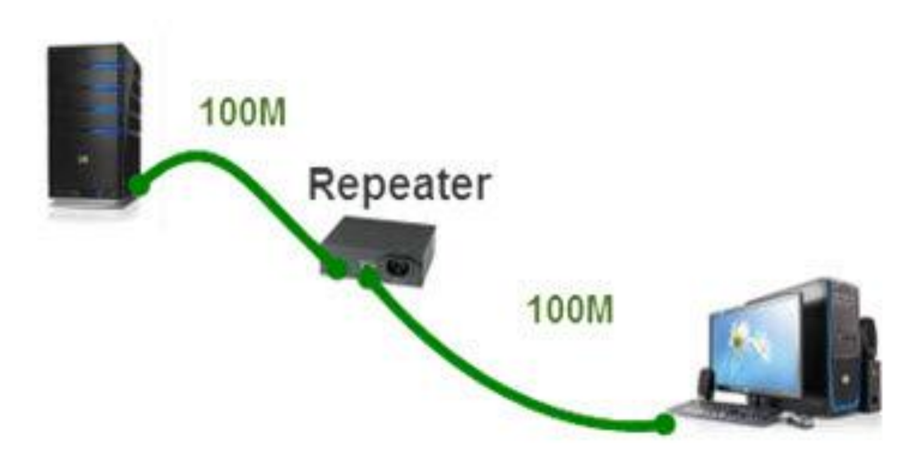
- Repeaters boost the strength of a signal as it travels through a communication channel, like a telephone line or a radio frequency, to help it cover longer distances.
- In situations where signals lose power due to resistance or distance, a repeater amplifies the signal before sending it further.
- In computer networking, repeaters operate on the physical layer of the OSI model, as they only work with the actual signal and don't interpret data.



W

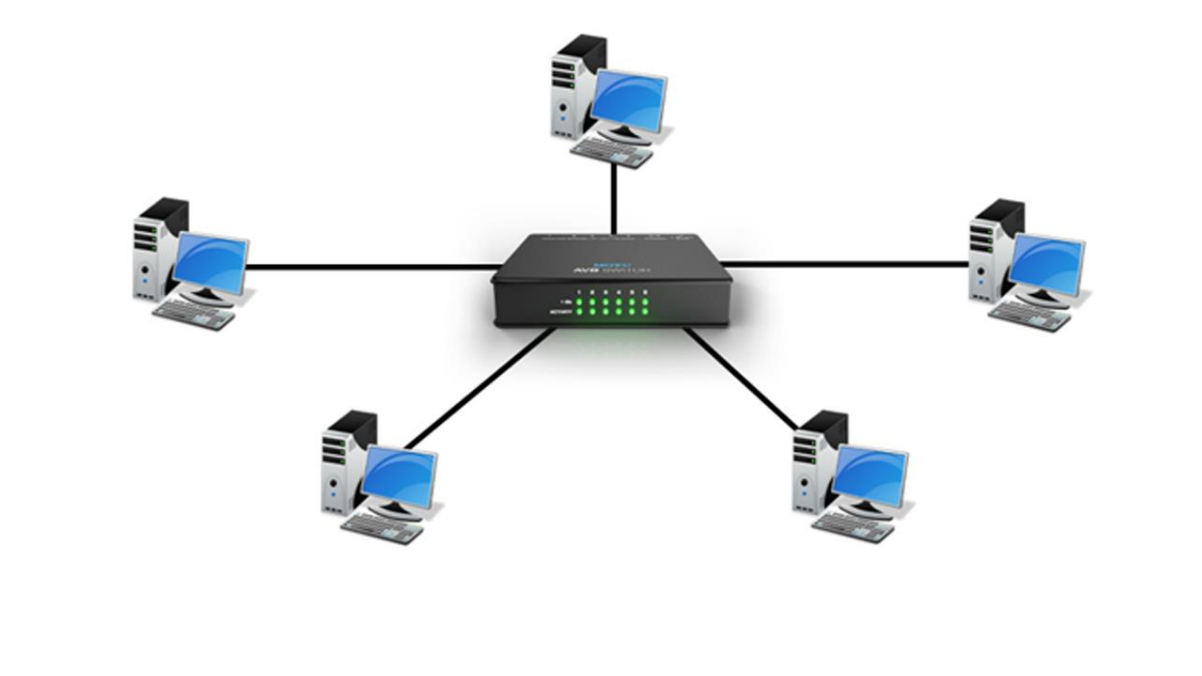
- Repeaters are used to extend transmissions so that the signal can cover longer distances or be received on the other side of an obstruction.

- In computer networking, because repeaters work with the actual physical signal, and do not attempt to interpret the data being transmitted, they operate on the physical layer, the first layer of the OSI model.



Hub

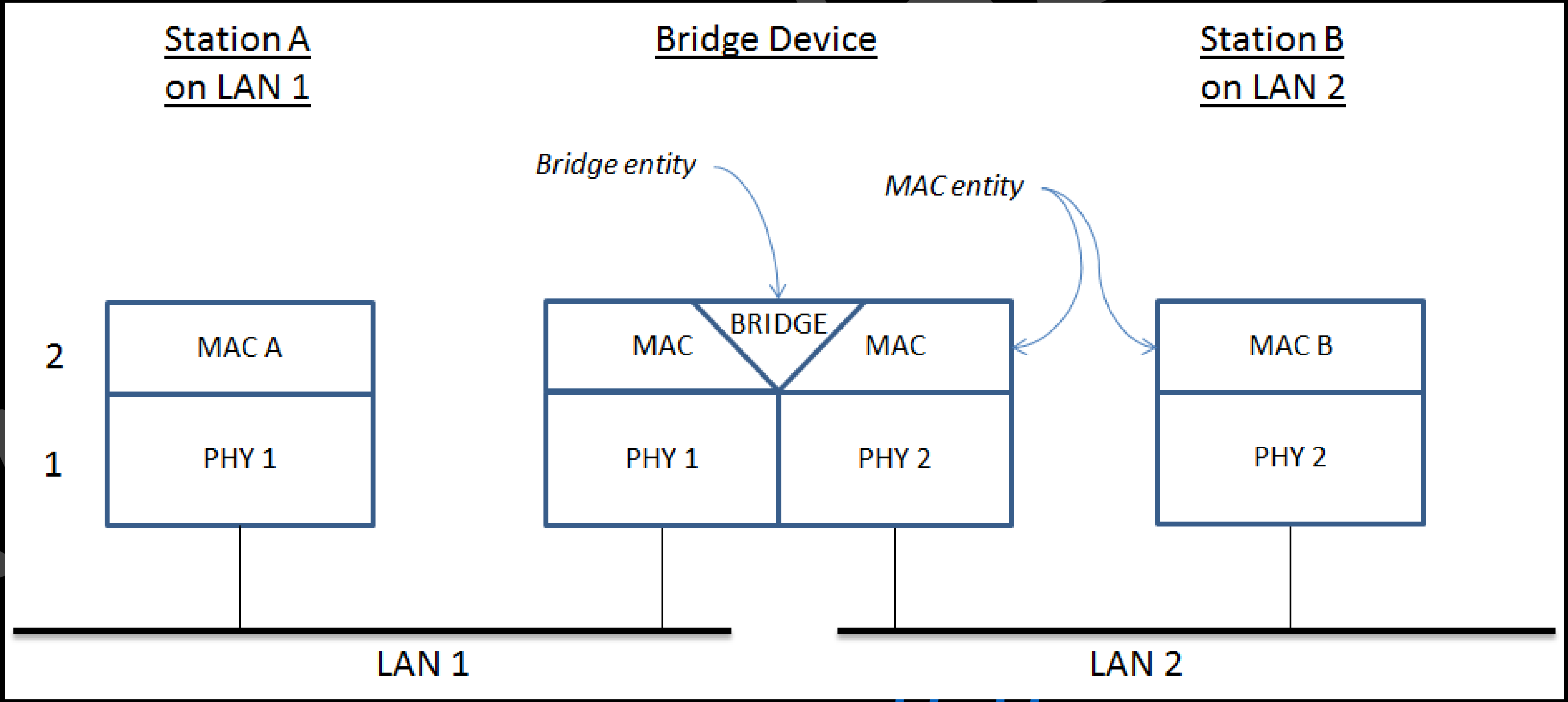
- Hubs are multiport repeater. An **Ethernet hub**, **active hub**, **network hub**, **repeater hub**, **multiport repeater**, or simply **hub** is a network hardware device for connecting multiple Ethernet devices together and making them act as a single network segment.
- It has multiple input/output (I/O) ports, in which a signal introduced at the input of any port appears at the output of every port except the original incoming. A hub works at the physical layer (layer 1) of the OSI model. Hubs are now largely obsolete, having been replaced by network switches except in very old installations



Bridge

- Bridge is used to connect two different lan. A **network bridge** is a computer networking device that creates a single, aggregate network from multiple communication networks or network segments. Bridging connects two separate networks as if they were a single network.

- In the OSI model, bridging is performed in the data link layer (layer 2).



Switch

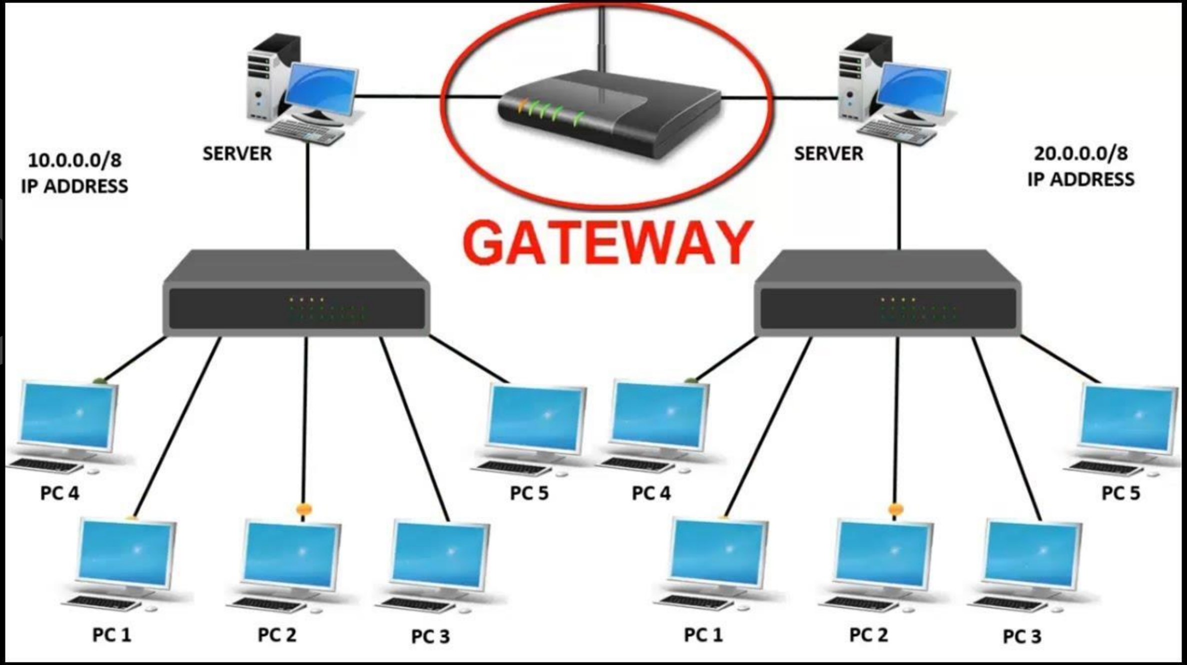
- A network switch connects multiple devices on a network and uses MAC addresses to send data directly to the right device.
- Unlike simpler devices like repeater hubs that send data to all ports, a switch is smarter and only sends data to the specific device it's meant for.
- The most common type of switch is for Ethernet networks, and the first one was made by Kalpana in 1990.

Router

- A router moves data between different computer networks, directing it based on destination information.
- It checks a data packet's header to know where to send it next, using its own set of rules or a "routing table."
- Simple routers are used in homes, while more advanced ones are for big businesses and internet service providers.

Gateway

- A **gateway** is a piece of networking hardware or software used in telecommunications for telecommunications networks that allows data to flow from one discrete network to another.
- Gateways are distinct from routers or switches in that they communicate using more than one protocol to connect multiple networks and can operate at any of the seven layers of the open systems interconnection model (OSI).
- The term gateway can also loosely refer to a computer or computer program configured to perform the tasks of a gateway, such as a default gateway or router.


10.0.0.0/8
IP ADDRESS
SERVER
GATEWAY
SERVER
20.0.0.0/8
IP ADDRESS
PC 4
PC 5
PC 4
PC 5
PC 1
PC 2
PC 3
PC 1
PC 2
PC 3