



Computer Networks(AITC06)

CSE

V SEMESTER



Module -I

Introduction: Networks, network types, internet history, standards and administration; Network models: Protocol layering, TCP/IP protocol suite, the OSI model Transmission media: Introduction, guided media, unguided media; Switching: Introduction, circuit switched networks, packet switching.

What is Network?

- Computer Network is a collection of computers interconnect with each other and allows communication & collaboration between users.

OR

- A network is a set of devices connected by communication links.



Applications of Networks

- **Resource Sharing**
 - ✓ Hardware (computing resources, disks, printers)
 - ✓ Software (application software)
- **Access to remote database**
 - ✓ Easy accessibility from anywhere (files, databases)
 - ✓ Search Capability (WWW)
- **Better Communication**
 - ✓ Email
 - ✓ Message broadcast

Network Criteria

- **Performance**
 - ✓ Transit time
 - ✓ Response time
- **Reliability**
- **Security**

Physical Structures

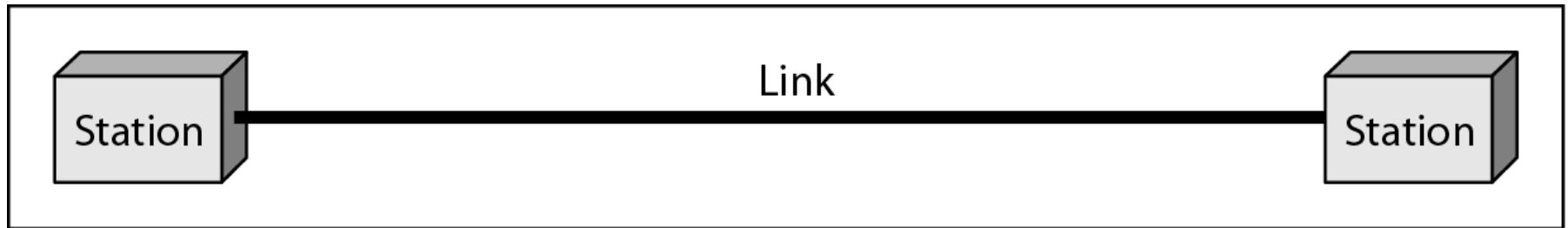
Type of connection:

✓ **Point-to-point:**

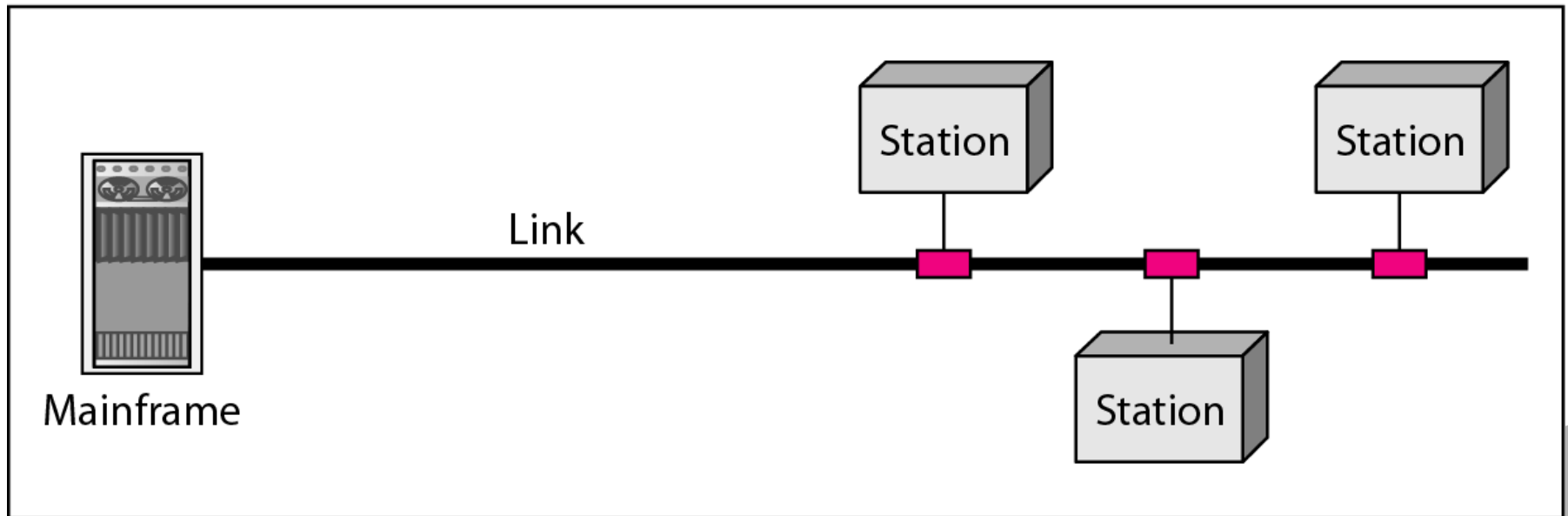
A point-to-point connection provides a dedicated link between two devices

✓ **Multipoint:**

A multipoint (also called multi-drop) connection is one in which more than two specific devices share a single link



a. Point-to-point



b. Multipoint

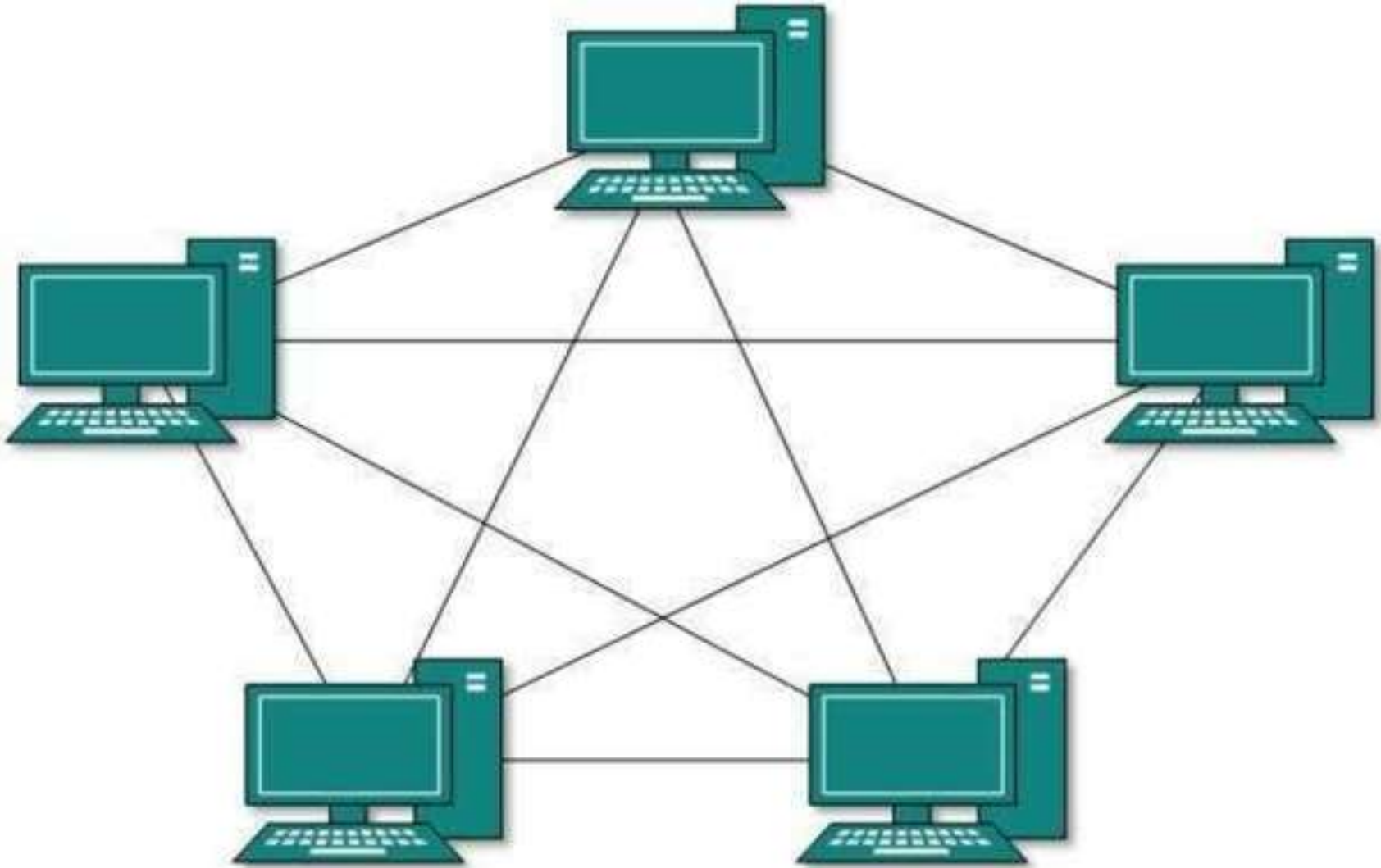
Topology

- The **topology** of a network is the geometric representation of the relationship of all the links and linking devices (usually called nodes) to one another.
- **Types of topology:**
 1. Mesh Topology
 2. Star Topology
 3. Bus Topology
 4. Ring Topology

Mesh Topology

- In a mesh topology, every device has a **dedicated point-to-point link** to every other device.
- To find the number of physical links in a fully connected mesh network with n nodes, we first consider that each node must be connected to every other node.
- We need $n(n - 1)$ **physical** links.
- we need $n(n - 1) / 2$ **duplex-mode** links.

Mesh Topology



Advantages of Mesh Topology

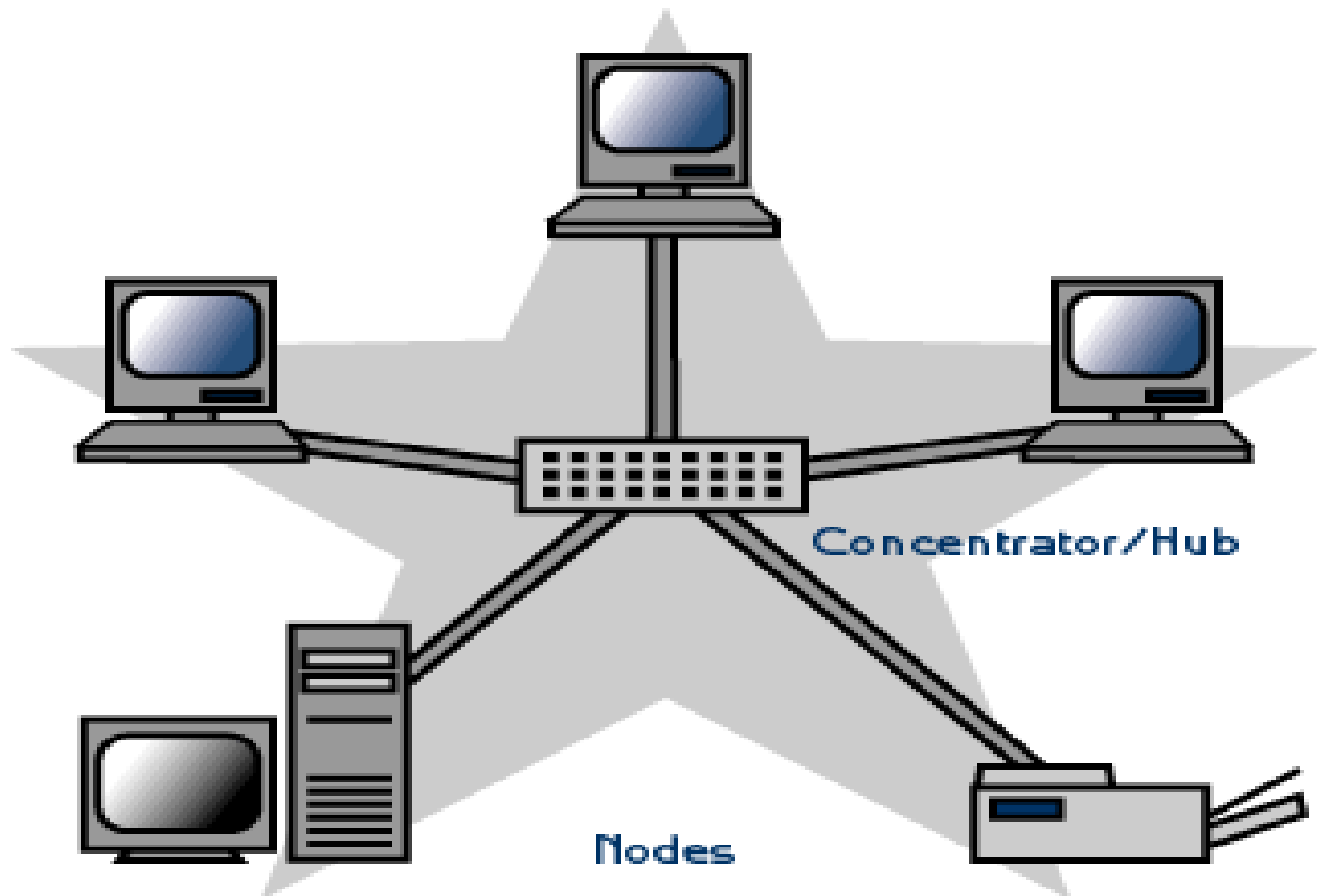
1. First, the use of dedicated links guarantees that each connection can carry its own data load, thus eliminating the traffic problems that can occur when links must be shared by multiple devices.
2. Second, a mesh topology is robust
3. Third, there is the advantage of privacy or security
4. Finally, point-to-point links make fault identification and fault isolation easy.

Disadvantages of Mesh Topology

1. Cost
2. Management
3. Efficiency
4. Hardware requirement

Star Topology

- In a star topology, each device has a dedicated point-to-point link only to a central controller, usually called a **hub**.
- Unlike a mesh topology, a star topology does not allow direct traffic between devices. 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 of Star Topology

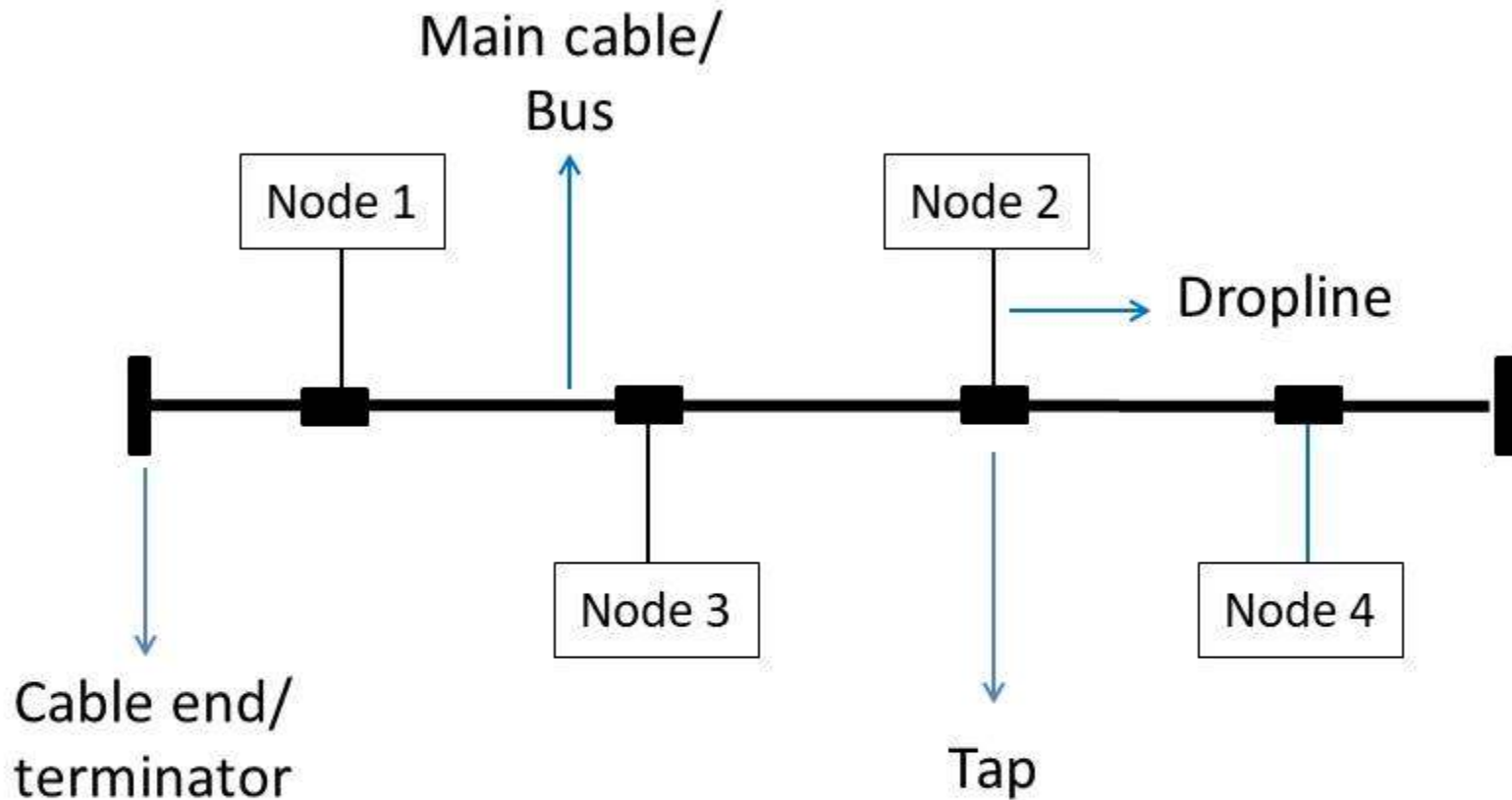
1. A star topology is less expensive than a mesh topology
2. A star topology is robust
3. As long as the hub is working, it can be used to monitor link problems and defective links.

Disadvantages of Star Topology

- One big disadvantage of a star topology is the dependency of the whole topology on one single point, the hub.
- Although a star requires far less cable than a mesh, each node must be linked to a central hub. For this reason, often more cabling is required in a star than in some other topologies

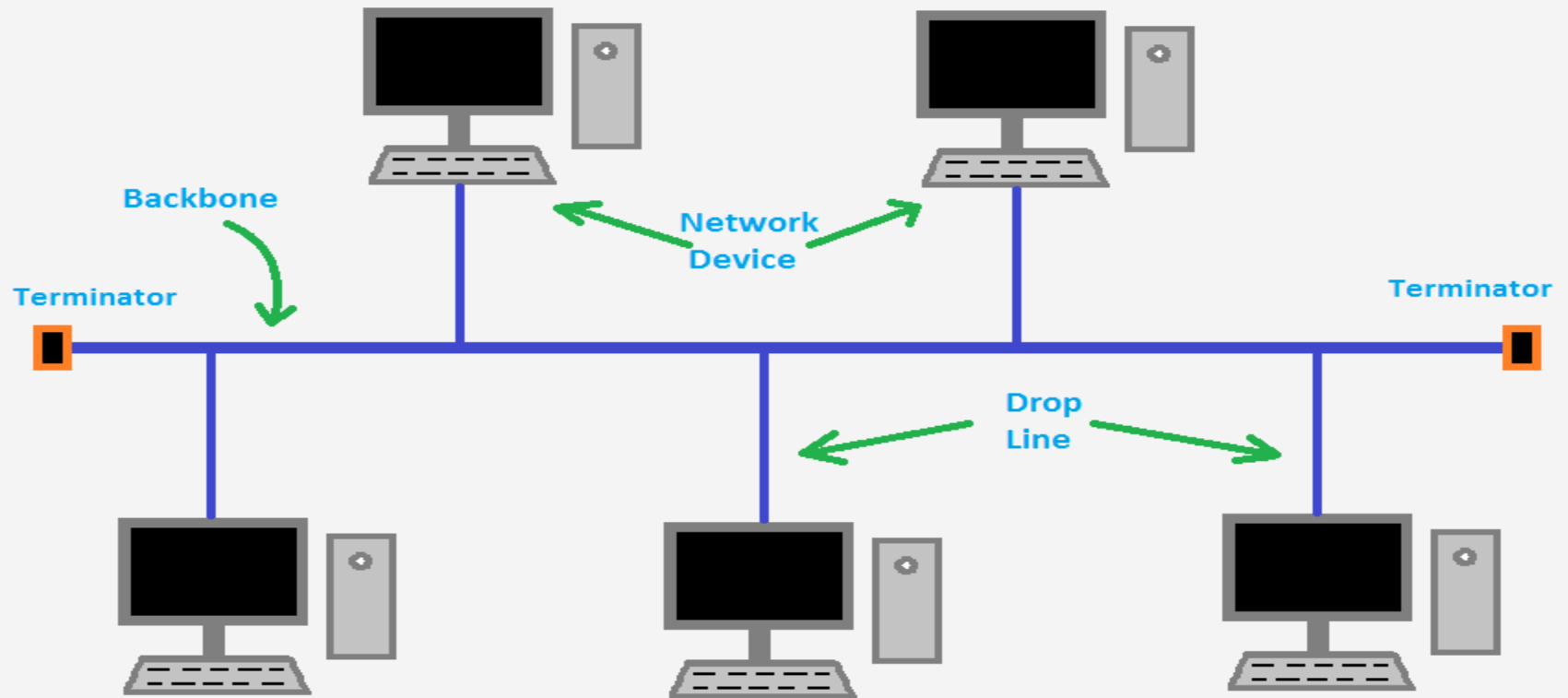
Bus Topology

- In Bus topology, every computer and network device is connected to a single cable.
- It transmits the data in single direction.
- 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.



Bus Topology

TechnoG



Bus Topology

Advantages of Bus Topology

- Advantages of a bus topology include ease of installation. Backbone cable can be laid along the most efficient path, then connected to the nodes by drop lines of various lengths.
- A bus uses less cabling than mesh or star topologies.
- In a bus, the redundancy is eliminated
- Cost of the cable is less compare to other topologies.

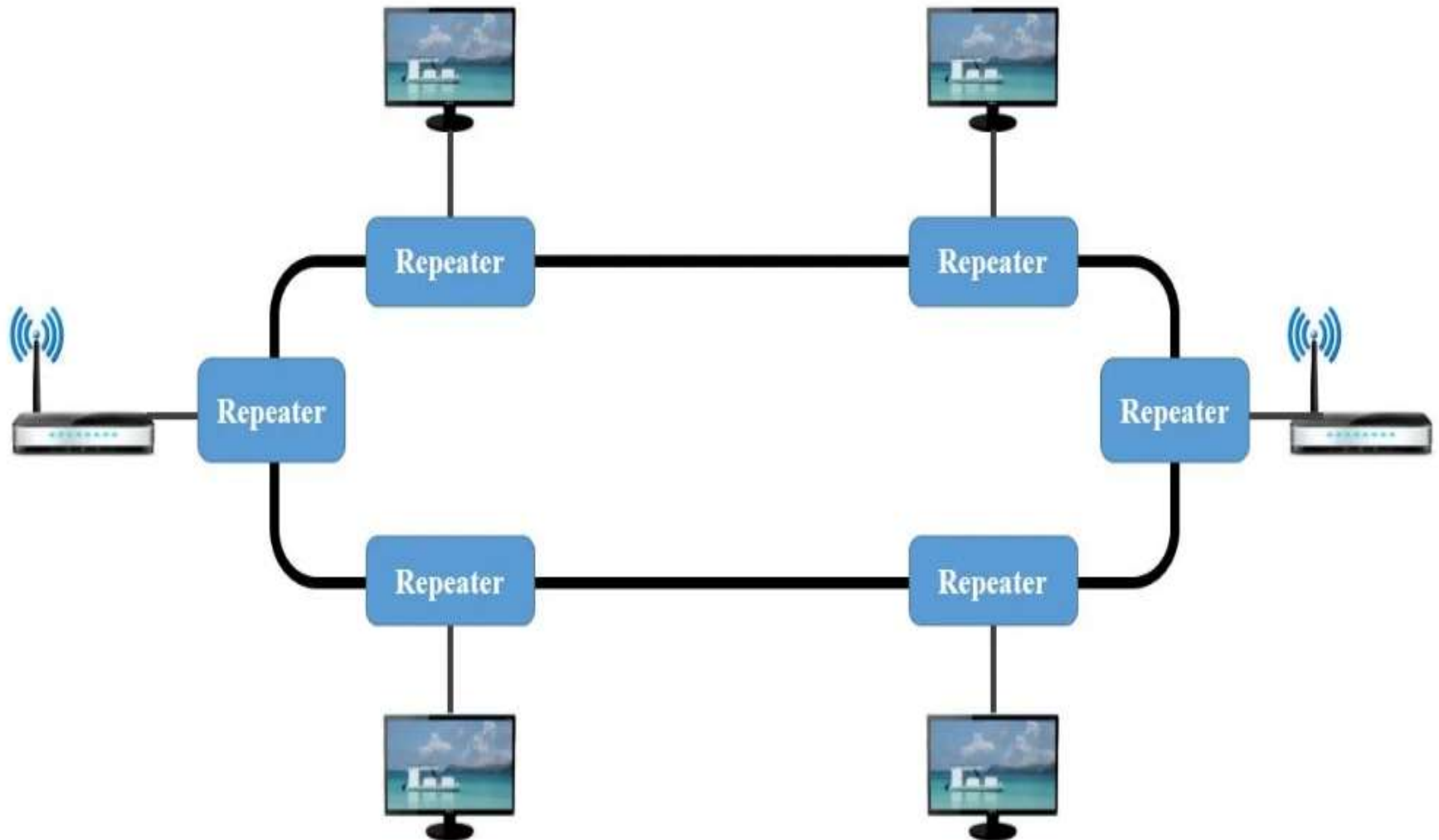
Disadvantages of Bus Topology

- A fault or break in the bus cable stops all transmission, even between devices on the same side of the problem
- If the common cable fails, then the whole system will crash down.
- If the two nodes send the messages simultaneously, then the signals of both the nodes collide with each other.
- Adding new devices to the network would slow down the network
- Security is very low .
- Builds small network.

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.
- 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

Ring Topology



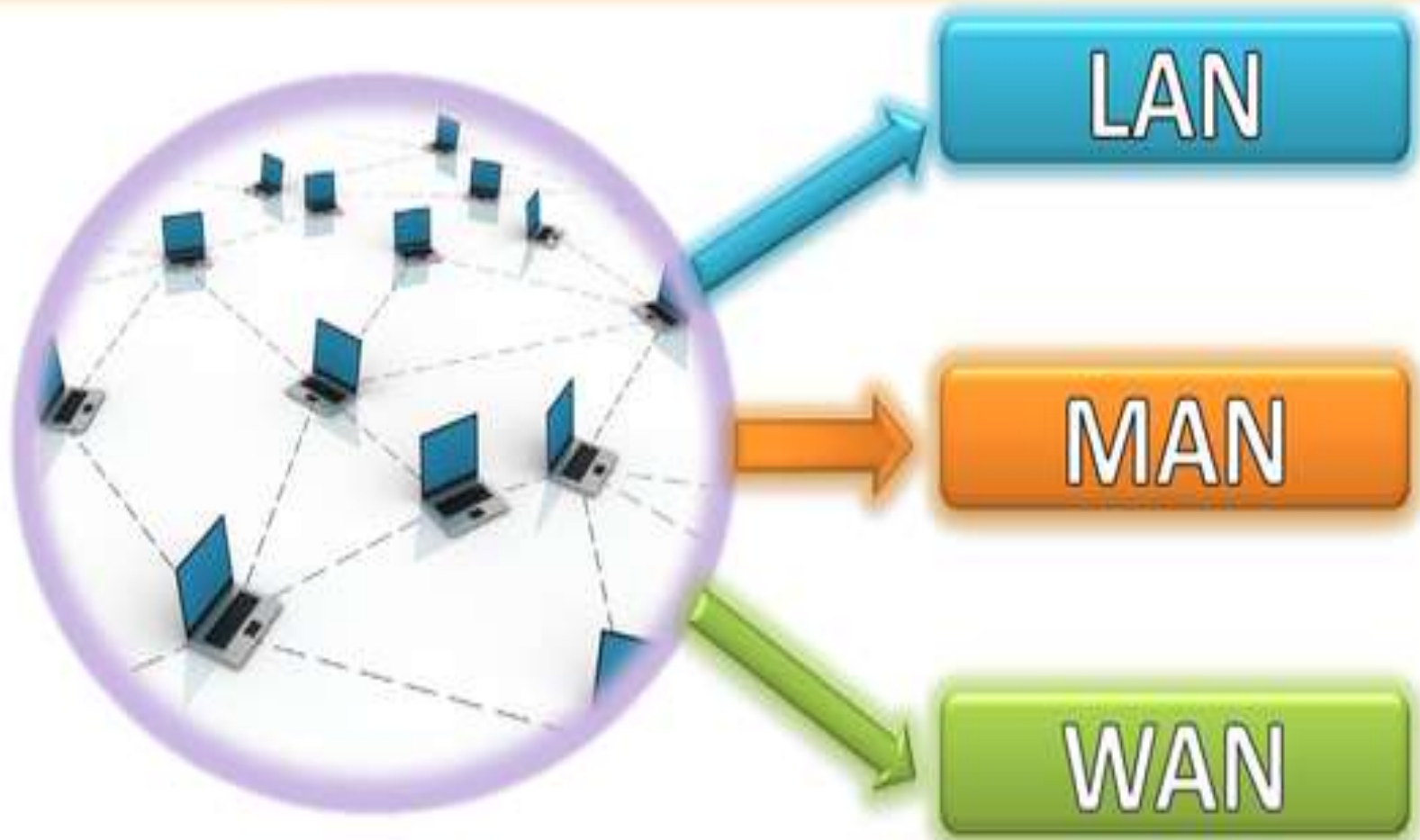
Advantages of Ring Topology

- In Ring topology, the possibility of data collision is minimal
- Network controller server is not required
- This type of network is affordable
- It is scalable
- In a Ring topology network, any two new nodes can be added without difficulty.

Disadvantages of Ring Topology

- It is much slower compared to a star topology
- Unidirectional traffic can be a disadvantage
- A break in the ring can disable the entire network
- Degradation of network performance and inefficient.

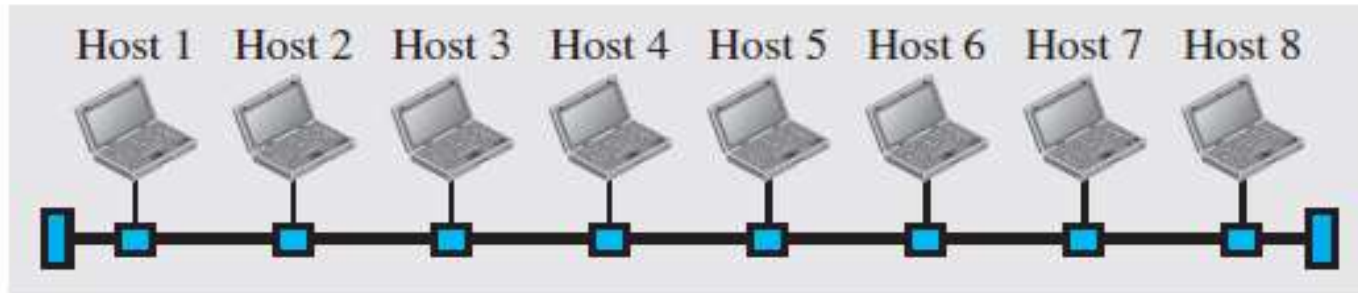
Types of Network



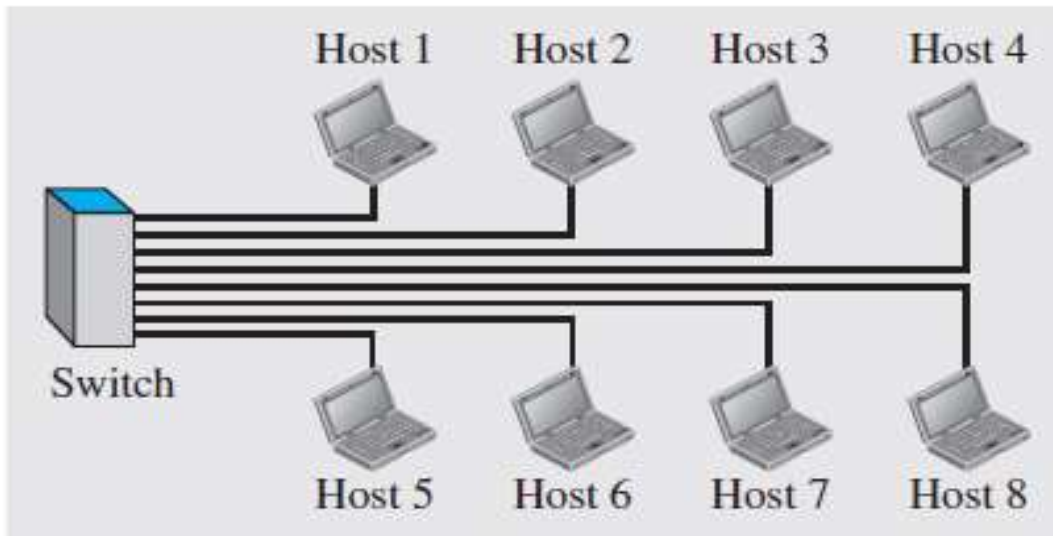
LAN(Local Area Network)

- A Local Area Network is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building.
- We can setup LAN in two ways:
 1. Wired LAN (ex: Ethernet –Hub/switch)
 2. Wireless LAN(ex: wi-fi)

LAN(Local Area Network)









a. LAN with a common cable (past)



b. LAN with a switch (today)

Legend

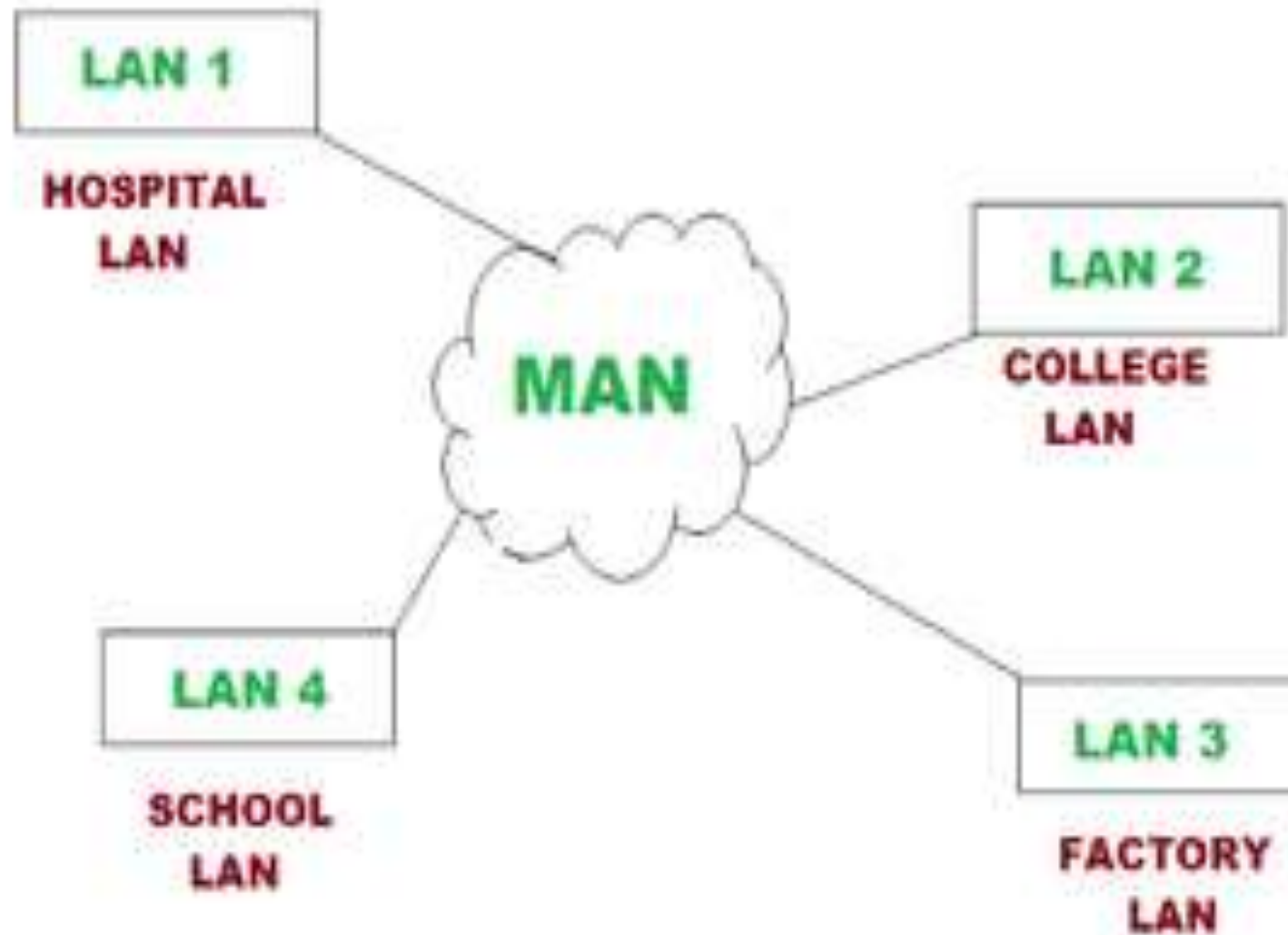
-  A host (of any type)
-  A switch
-  A cable tap
-  A cable end
-  The common cable
-  A connection

MAN(Metropolitan Area Network)



- Metropolitan Area Network is a computer network that interconnects users with computer resources in a geographic region of the size of a metropolitan area(city).
- The devices used in this MAN are:
 - Switches/Hub
 - Routers/Bridges

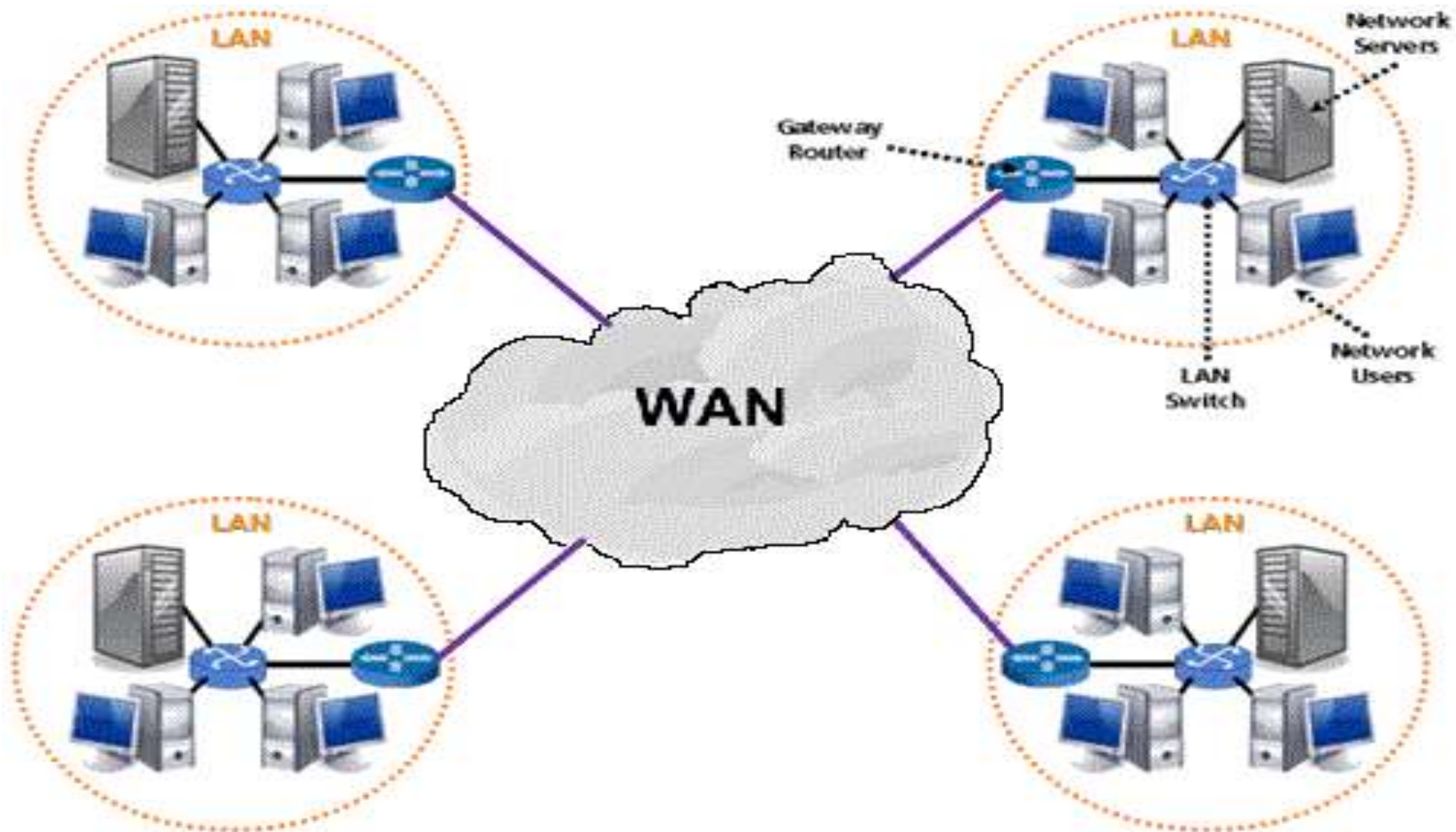
MAN(Metropolitan Area Network)



WAN(Wide Area Network)

- A WAN, also called the Wide Area Network, is defined as a telecommunication network that extends over a large area.
- The primary purpose of WAN is computer networking. The networks are linked to communicate with one another.

WAN(Wide Area Network)



WAN - Wide Area Network

Differences b/w LAN, MAN and WAN

Sr.No.	Key	LAN	MAN	WAN
1	Definition	LAN stands for Local Area Network.	MAN stands for Metropolitan Area Network.	WAN stands for Wide Area Network.
2	Ownership	LAN is often owned by private organizations.	MAN ownership can be private or public.	WAN ownership can be private or public.
3	Speed	LAN speed is quite high.	MAN speed is average.	WAN speed is lower than that of LAN.
4	Delay	Network Propagation Delay is short in LAN.	Network Propagation Delay is moderate in MAN.	Network Propagation Delay is longer in WAN.
5	Congestion	LAN has low congestion as compared to WAN.	MAN has higher congestion than LAN.	WAN has higher congestion than both MAN and LAN.
6	Fault Tolerance	Fault Tolerance of LAN is higher than WAN.	Fault Tolerance of MAN is lower than LAN.	Fault Tolerance of WAN is lower than both LAN and MAN.
7	Maintenance	Designing and maintaining LAN is easy and less costly than WAN.	Designing and maintaining WAN is complex and more costly than LAN.	Designing and maintaining WAN is complex and more costly than both LAN and MAN.

INTERNET HISTORY

- Computers from different manufacturers were unable to communicate with one another.
- The **Advanced Research Projects Agency (ARPA)** in the Department of Defense (DOD) was interested in finding a way to connect computers so that the researchers they funded could share their findings, thereby reducing costs and eliminating duplication of effort.
- The idea was that each host computer (not necessarily from the same manufacturer) would be attached to a specialized computer, called an *interface message processor (IMP)*.

INTERNET HISTORY

- In 1972, Vint Cerf and Bob Kahn, both of whom were part of the core ARPANET group, collaborated on what they called the Internetting Project.
- They wanted to link dissimilar networks so that a host on one network could communicate with a host on another

INTERNET HISTORY

- A new communications protocol was established called Transfer Control Protocol/Internetwork Protocol (TCP/IP).
- This allowed different kinds of computers on different networks to "talk" to each other.

PROTOCOL LAYERING

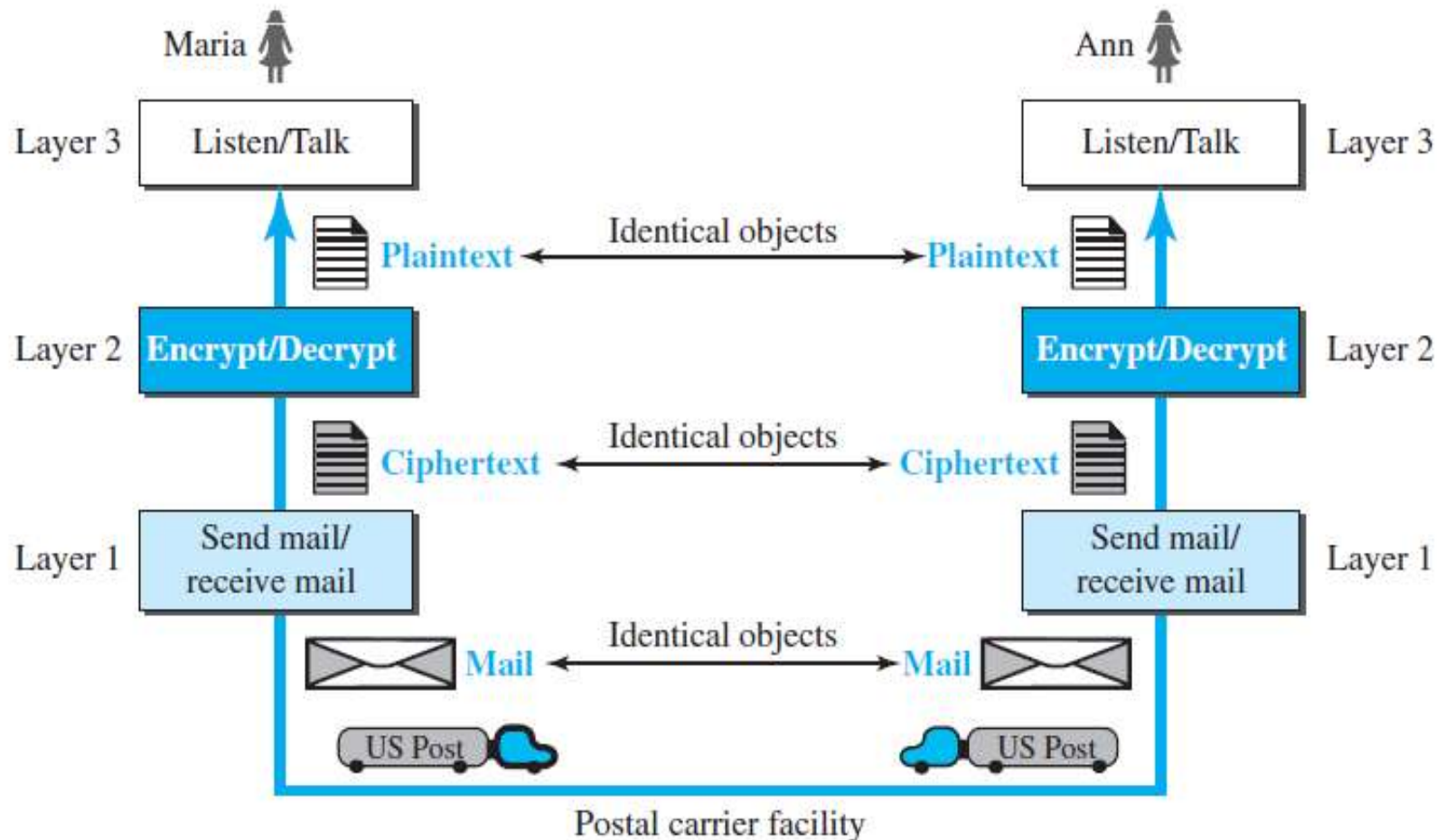
Figure 2.1 *A single-layer protocol*



PROTOCOL LAYERING

Figure 2.2 *A three-layer protocol*

PRO



Principles of Protocol Layering



- ***First Principle***
- The first principle dictates that if we want bidirectional communication, we need to make each layer so that it is able to perform two opposite tasks, one in each direction.
- For example, the third layer task is to listen (in one direction) and *talk (in the other direction)*. The second layer needs to be able to encrypt and decrypt. The first layer needs to send and receive mail.

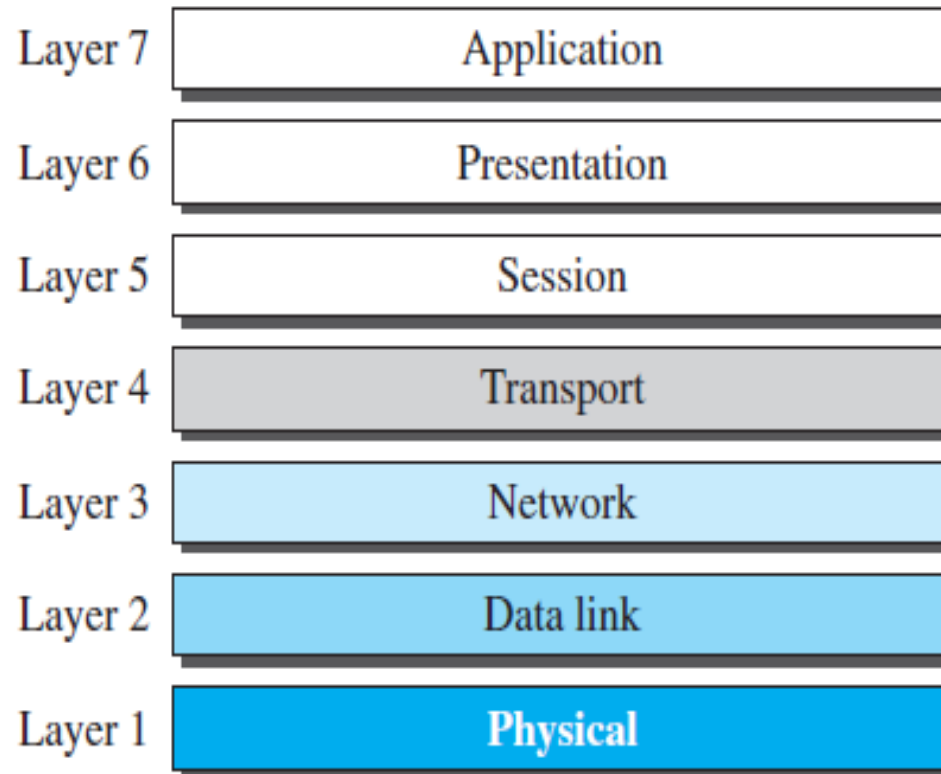
- ***Second Principle***
- The second principle that we need to follow in protocol layering is that the two objects under each layer at both sites should be identical.
- For example, the object under layer 3 at both sites should be a plaintext letter. The object under layer 2 at both sites should be a ciphertext letter. The object under layer 1 at both sites should be a piece of mail.

OSI MODEL

- **Open Systems Interconnection (OSI) model** is a standard proposed by **International Organization for Standardization (ISO)**
- An open system is a set of protocols that allows any two different systems to communicate regardless of their underlying architecture
- The OSI model is a layered framework for the design of network systems that allows communication between all types of computer systems

OSI MODEL

Figure 2.11 *The OSI model*



1. User Support Layer(Application, Presentation, Session Layer)
2. Transport Layer
3. Network Support Layer(Network, Datalink, Physical Layer)

Physical Layer

- Physical Layer is responsible for transmitting a bit stream over a physical channel.
- It also deals with mechanical properties and electrical properties of the interface and transmission medium.
- Physical Layer is responsible for:
 1. transmission rate
 2. Physical topology
 3. Bit synchronization

Data-link Layer

- This layer is responsible for sending groups of packets to the adjacent nodes without any errors.
- This is called node-to-node delivery
- Data-link Layer is responsible for:
 1. Framing
 2. Physical Addressing
 3. Flow Control
 4. Error Control
 5. Access Control

Network Layer

- The network layer is responsible for routing the packets from one network to another network.
- This is referred to as source to the destination delivery.

Transport Layer

- Responsible for end to end delivery of the entire message.
- Segmentation and reassembly

Session Layer

- The main function of Session Layer is to establish, maintain and synchronize the interactions between two connected devices.



Presentation Layer

- This layer is responsible for presenting the data in reliable format or in a suitable format.

Responsibilities:

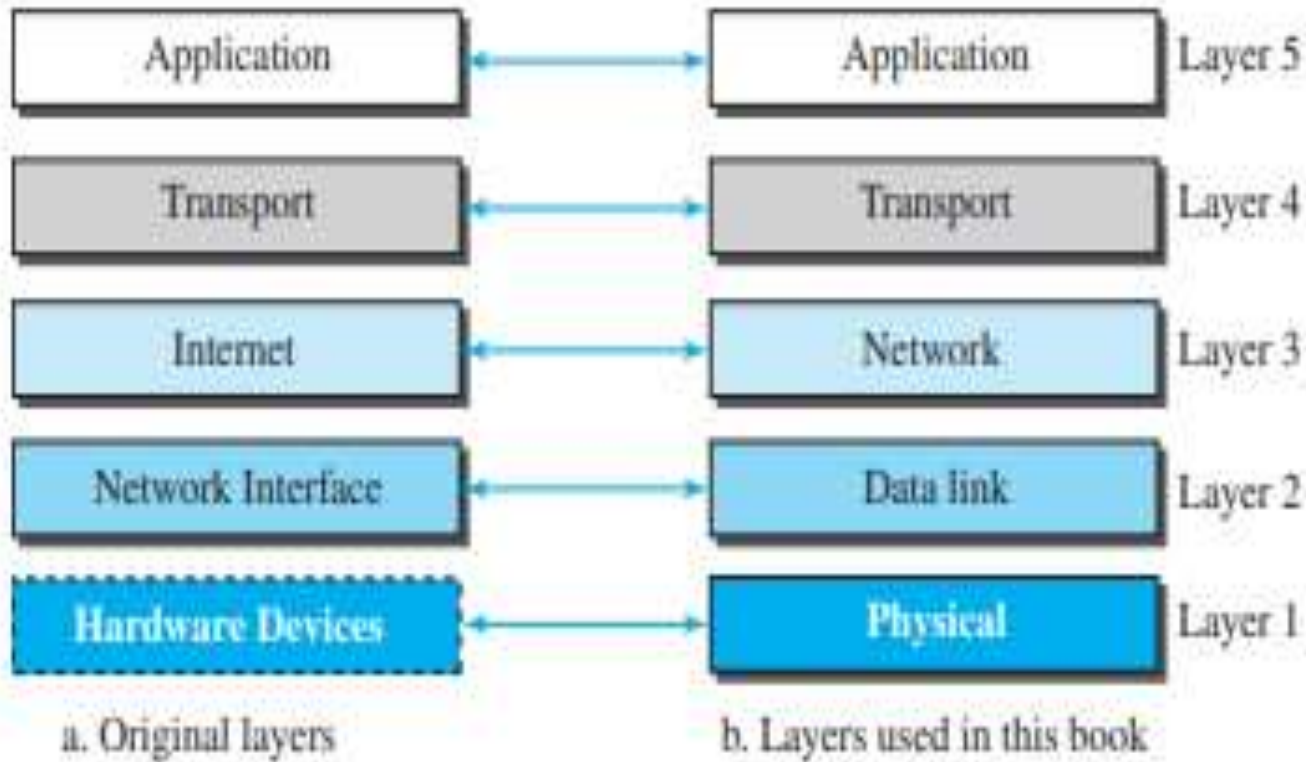
- Translation
- Encryption and Decryption
- Compression

- It enables the user to access the network
- It provides interfaces and support for services such as e-mail, ftp, distributed information services etc.

Responsibilities:

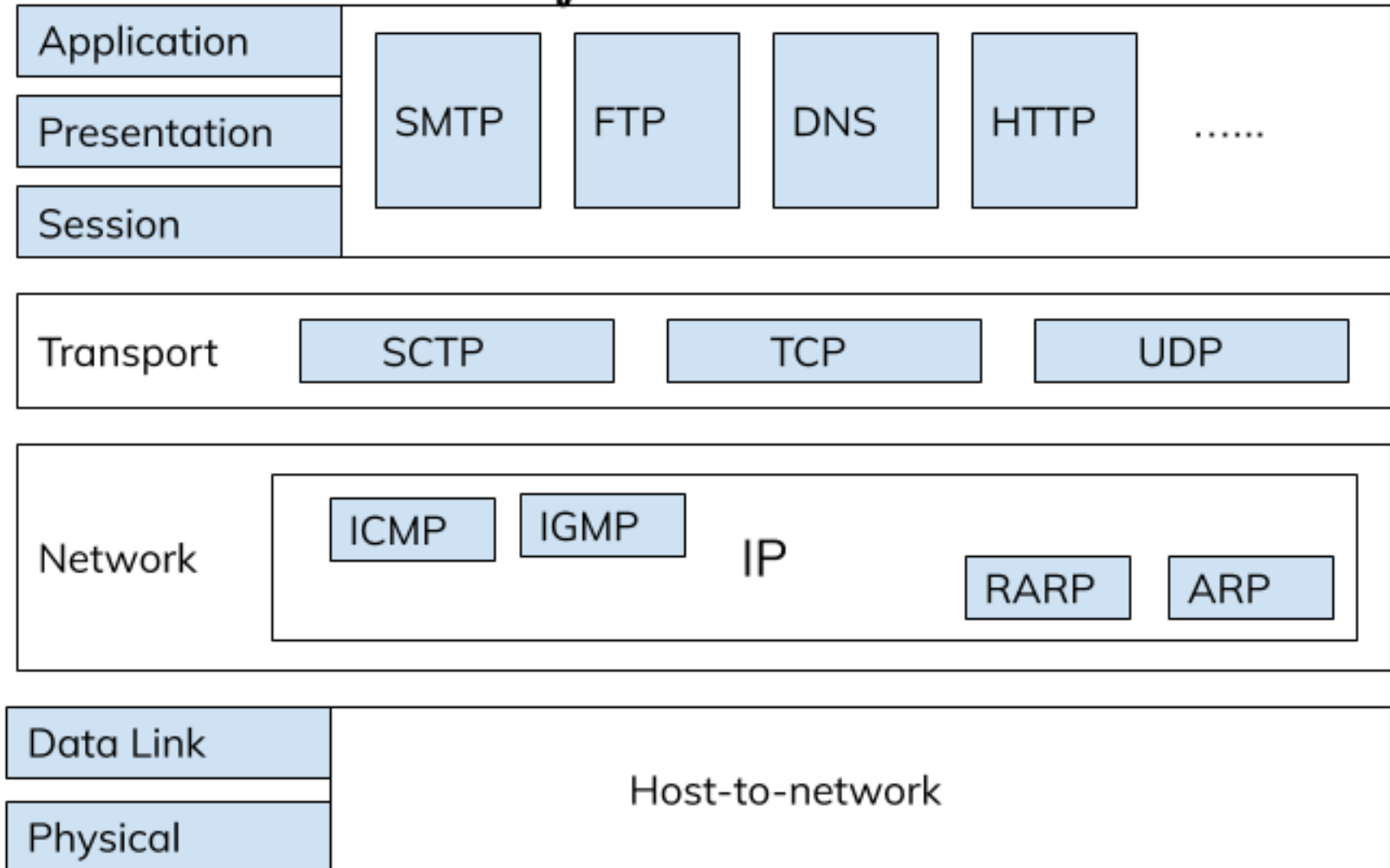
- File transfer, Access and Management
- Mail services
- Online shopping

TCP/IP PROTOCOL SUITE



TCP/IP PROTOCOL SUITE

Beginnersbook.com



1. Physical and Data Link Layer



- Physical and Data Link Layers in TCP/IP model does not define any protocols, they support all the standard protocols. They are combined known as **host-to-network layer**. A network in TCP/IP internetwork can be [LAN or WAN](#).

2. Network Layer

- In the network layer, the TCP/IP model supports internetworking protocol in short known as IP. The IP uses four protocols internally: ARP, RARP, ICMP & IGMP.
- **Address Resolution Protocol (ARP)**
- **Reverse Address Resolution Protocol (RARP)**
- **Internet Control Message Protocol (ICMP)**
- **Internet Group Message Protocol (IGMP)**

3. Transport Layer

- Transport layer in TCP/Model can be represented by three protocols: Transmission control protocol (TCP), User data gram protocol (UDP) and Stream Control Transmission Protocol (SCTP).
- **User Datagram protocol (UDP)**
- **Transmission control protocol (TCP)**
- **Stream Control Transmission Protocol (SCTP)**

4. Application Layer

- **HTTP:** HTTP stands for **H**ypertext transfer protocol
- **FTP:** FTP stands for **F**ile Transfer Protocol
- **DNS:** DNS stands for Domain Name System.
- **SMTP:** SMTP stands for Simple mail transfer protocol.

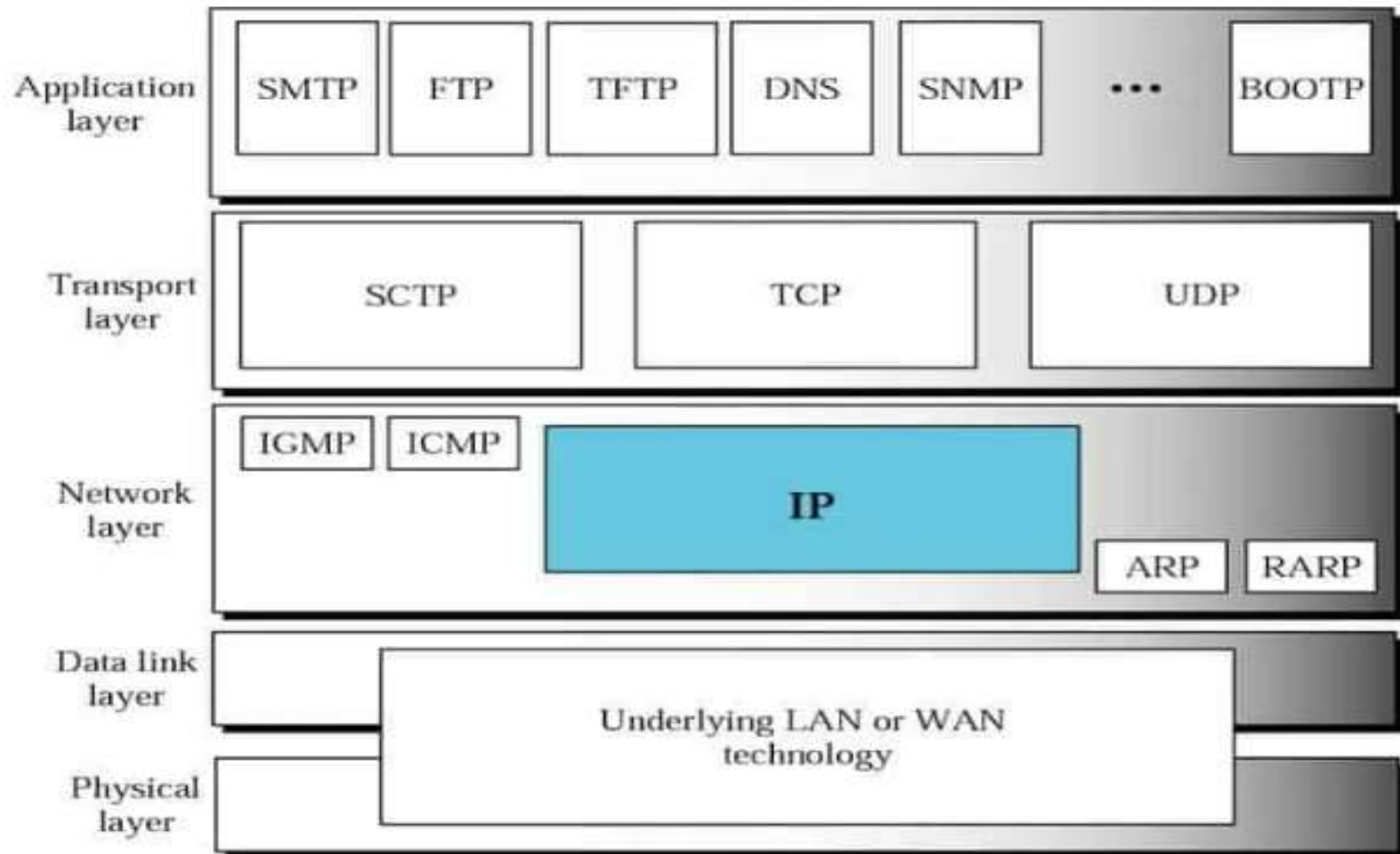
Application Layer – Data

Transport Layer – Segment

Network Layer – Packet

Data Link Layer – Frame

Physical Layer – Bits



TCP/IP PROTOCOL SUITE

Application Layer

- Hypertext Transfer Protocol (HTTP)
- Simple Mail Transfer Protocol (SMTP)
- File Transfer Protocol (FTP)

Transport Layer

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

TCP/IP PROTOCOL SUITE

Network Layer

- Internet Protocol
- Routers

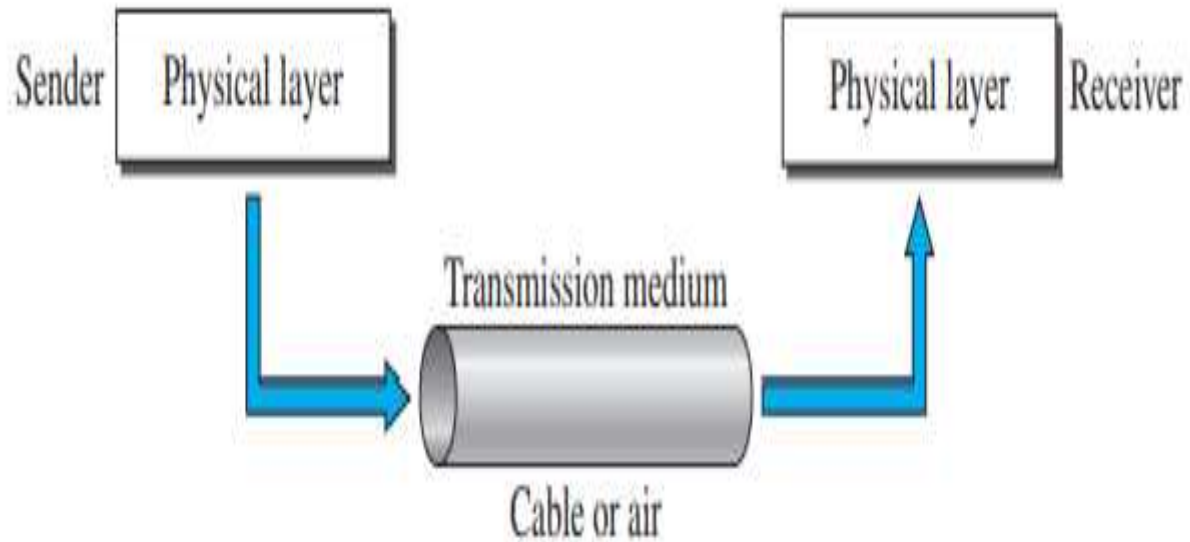
Data-link Layer

Ethernet and switches

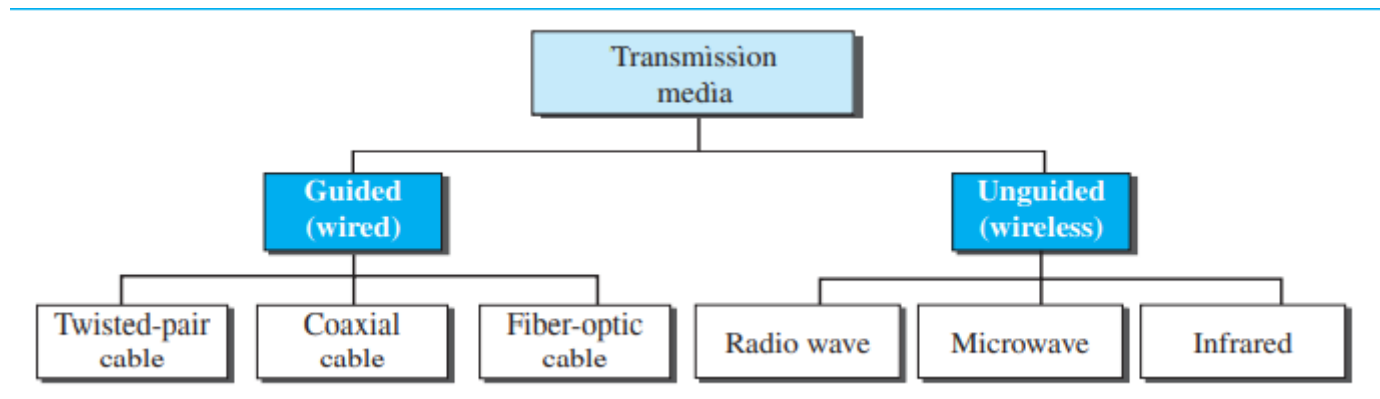
Physical Layer

Cables and NIC(Network Interface Card)

Transmission media



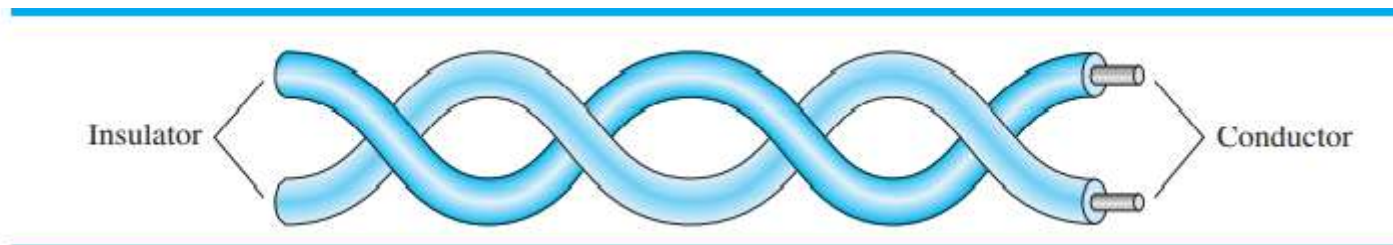
- Transmission medium can be defined as anything that can carry information from a source to a destination.
- The transmission medium is usually free space, metallic cable or fiber-optic cable.



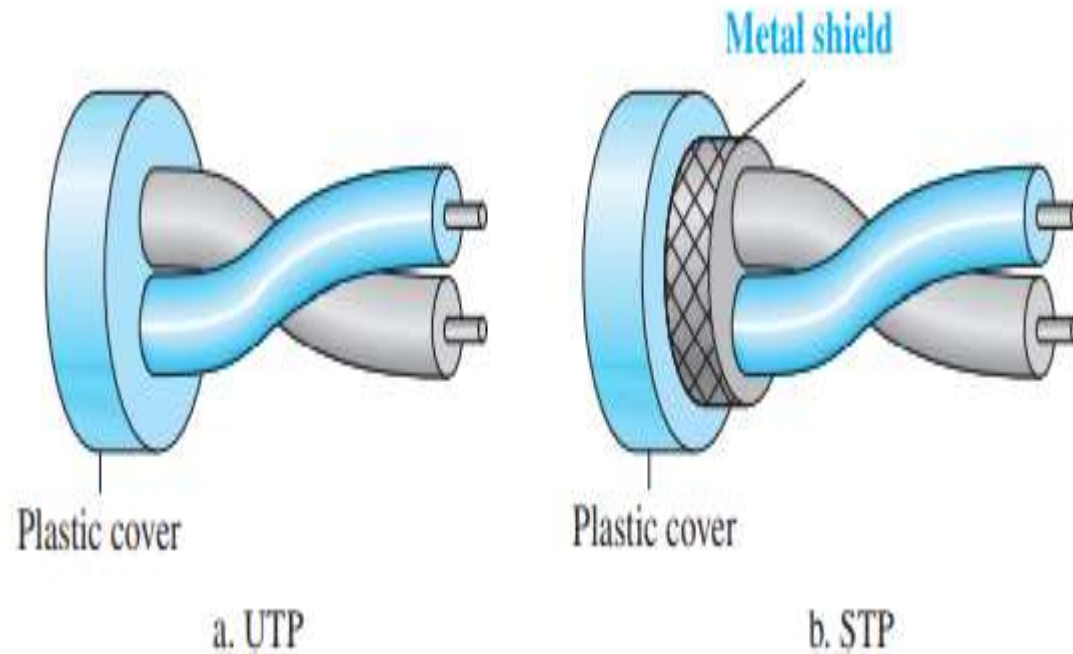
Guided media

- Guided media, which are those that provide a conduit from one device to another.
- It includes **twisted-pair cable**, **coaxial cable**, and **fiber-optic cable**.

Twisted-Pair Cable:

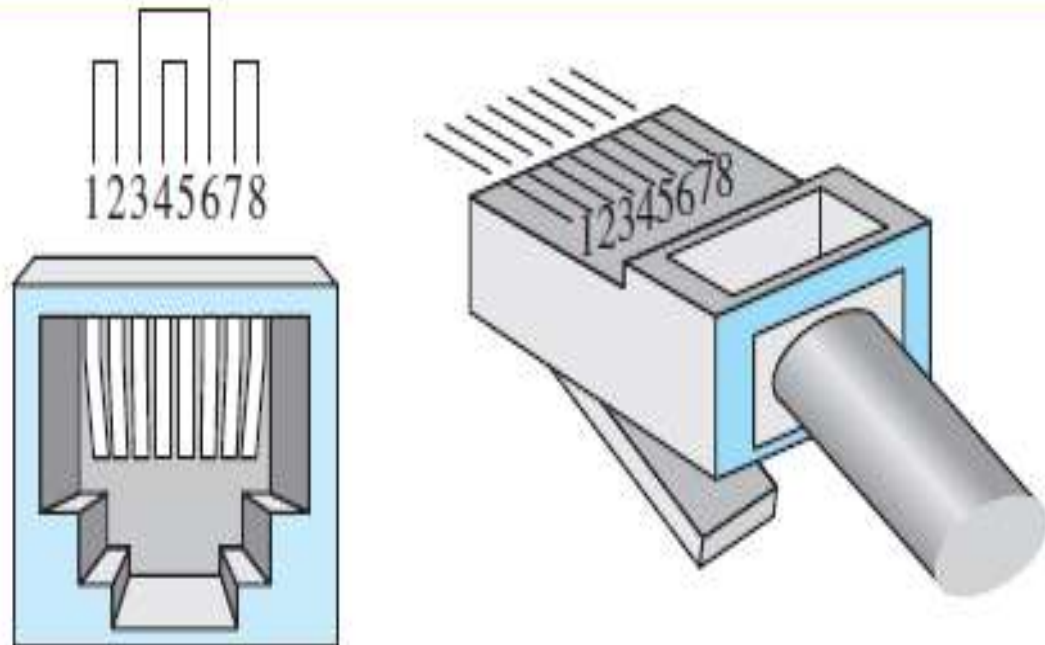


Unshielded Versus Shielded Twisted-Pair Cable



Connectors

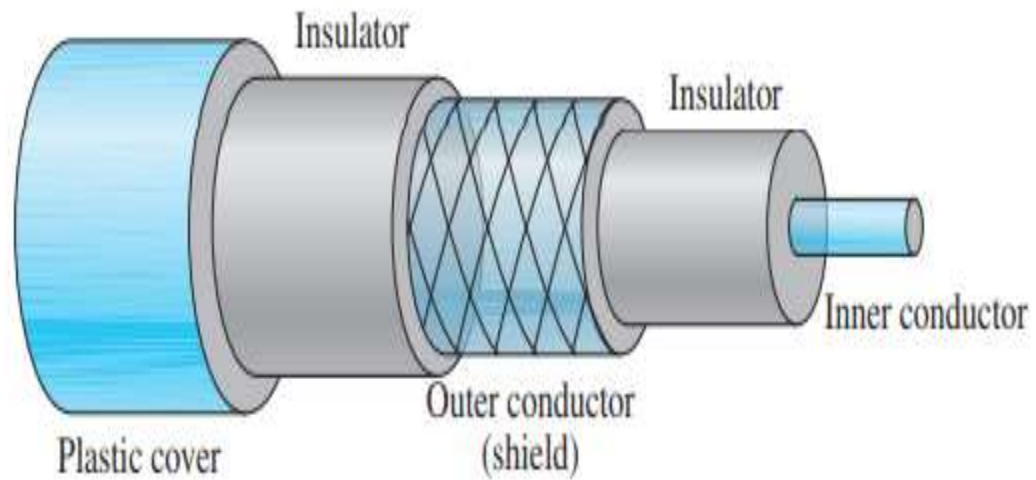
Figure 7.5 *UTP connector*



Applications

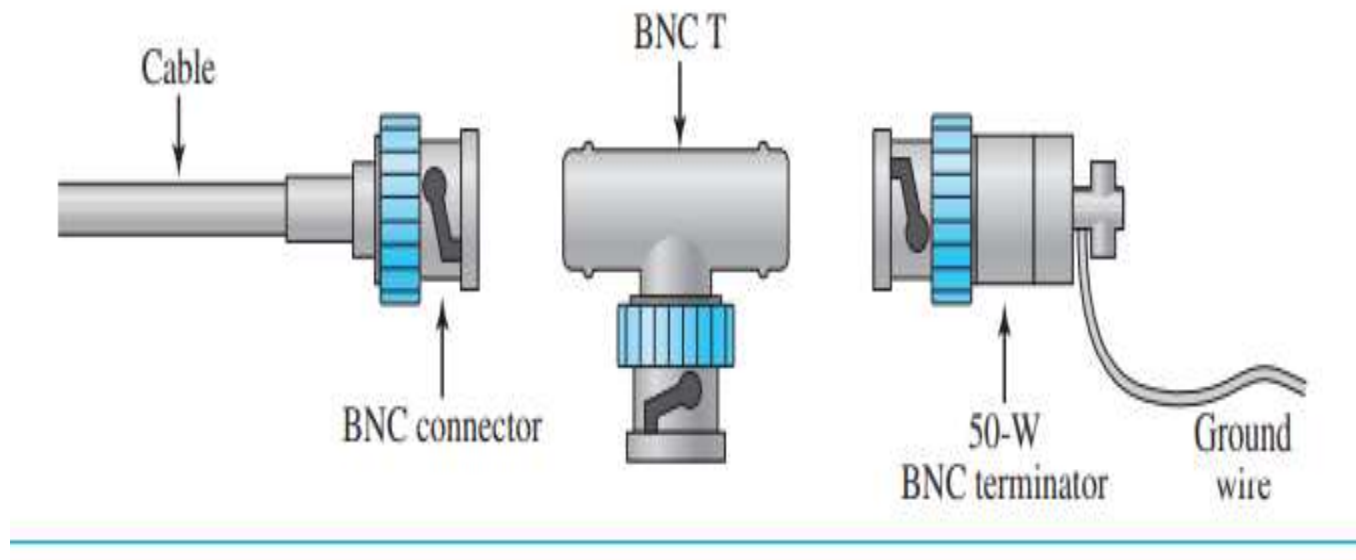
- Twisted-pair cables are used in telephone lines
- The local loop—the line that connects subscribers to the central telephone office.
- The DSL lines used by telephone companies use unshielded twisted pair cable.

Coaxial Cable



Coaxial Cable Connectors

- The most common type of connector used is the **Bayonet Neill-Concelman (BNC)** connector.

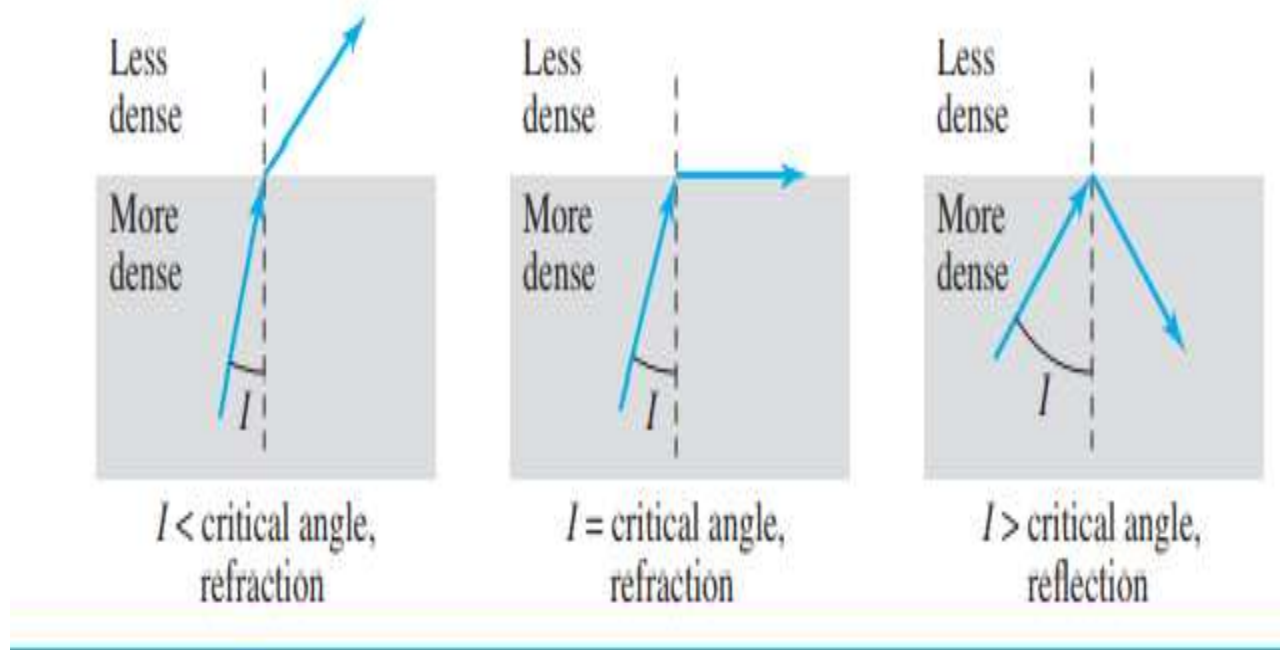


Applications

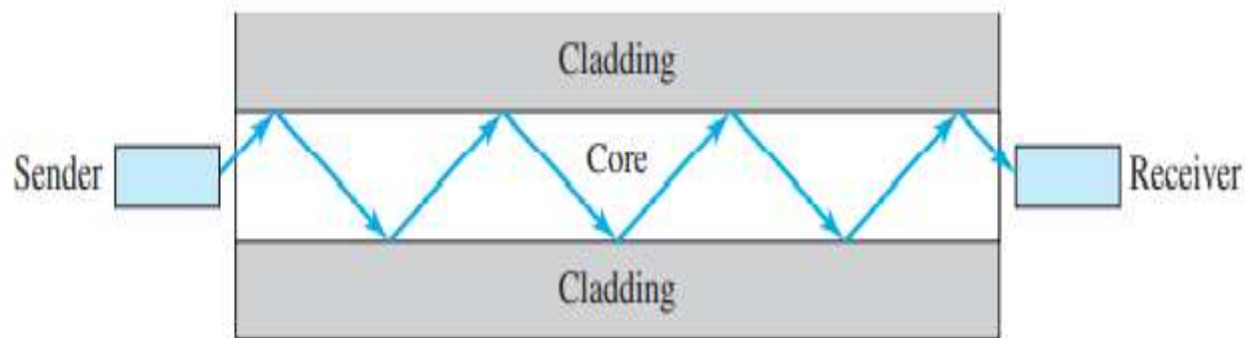
- Analog Telephone Networks-10000 voices
- Digital Telephone Networks- 600Mbps
- Cable TV networks
- Ethernet LANs

Fiber-Optic Cable

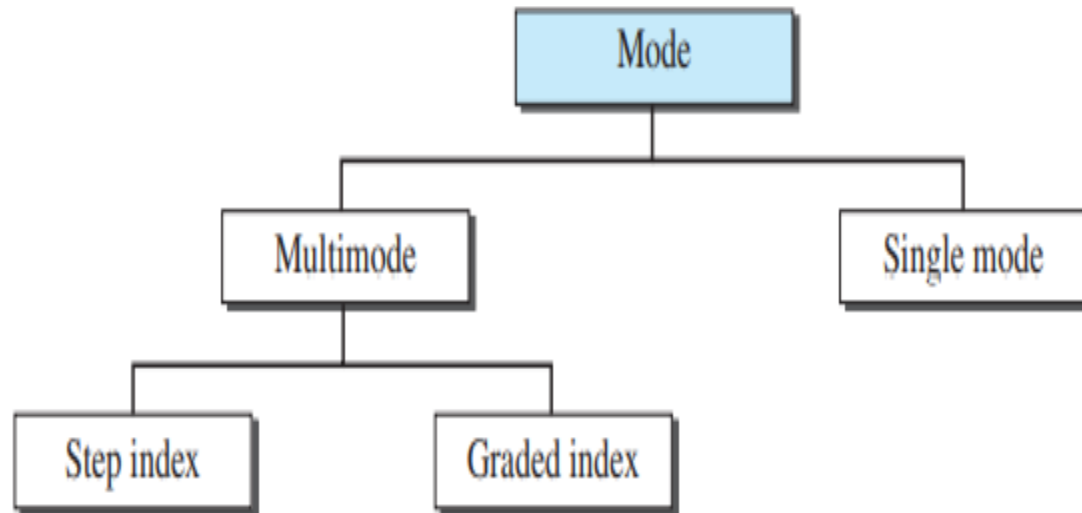
- A fiber-optic cable is made of glass or plastic and transmits signals in the form of light.



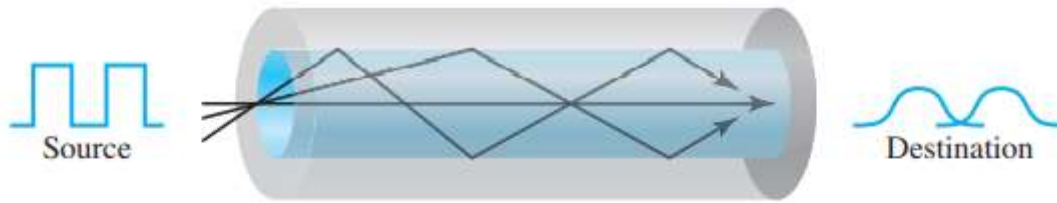
- Optical fibers use reflection to guide light through a channel.
- A glass or plastic core is surrounded by a cladding of less dense glass or plastic.
- The difference in density of the two materials must be such that a beam of light moving through the core is reflected off the cladding instead of being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



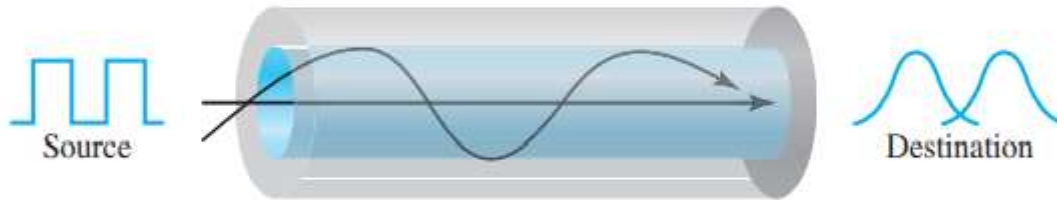
Propagation Modes



Multimode



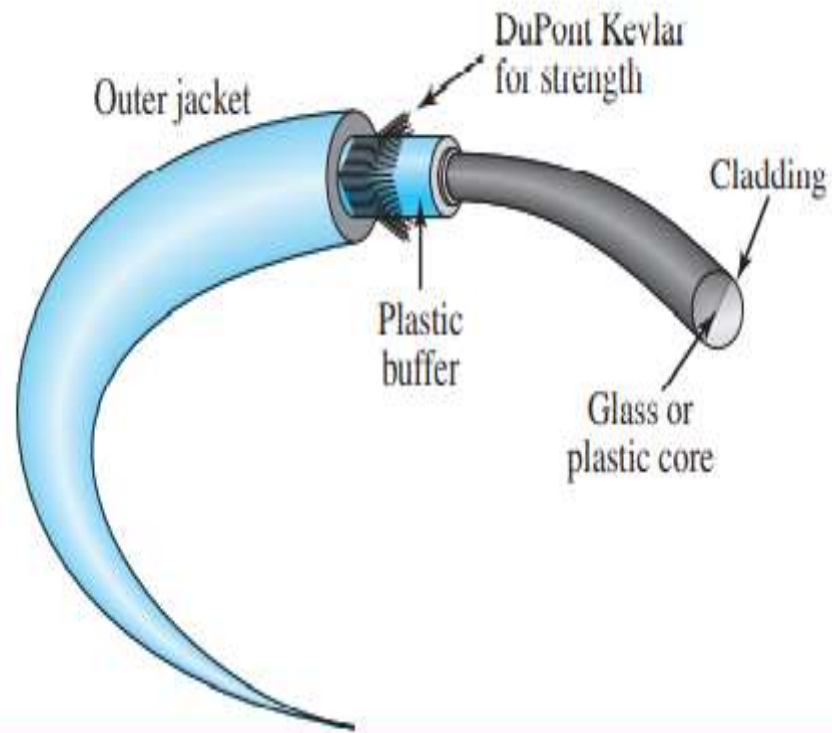
a. Multimode, step index



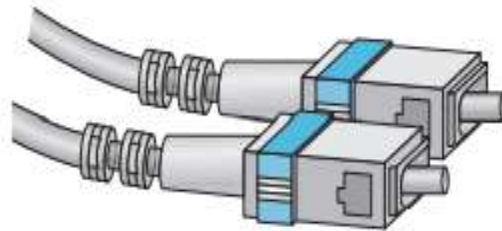
b. Multimode, graded index



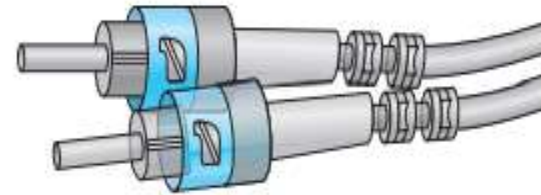
Cable Composition



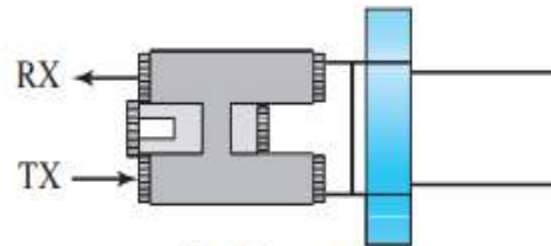
Fiber-Optic Cable Connectors



SC connector



ST connector



MT-RJ connector

- There are three types of connectors for fiber-optic cables.
- The subscriber channel (SC) connector is used for cable TV. It uses a push/pull locking system.
- The straight-tip (ST) connector is used for connecting cable to networking devices.
- MT-RJ is a connector that is the same size as RJ45.

Advantages

- Higher bandwidth
- Less signal attenuation
- Immunity to electromagnetic interference
- Resistance to corrosive materials
- Light weight

Disadvantages

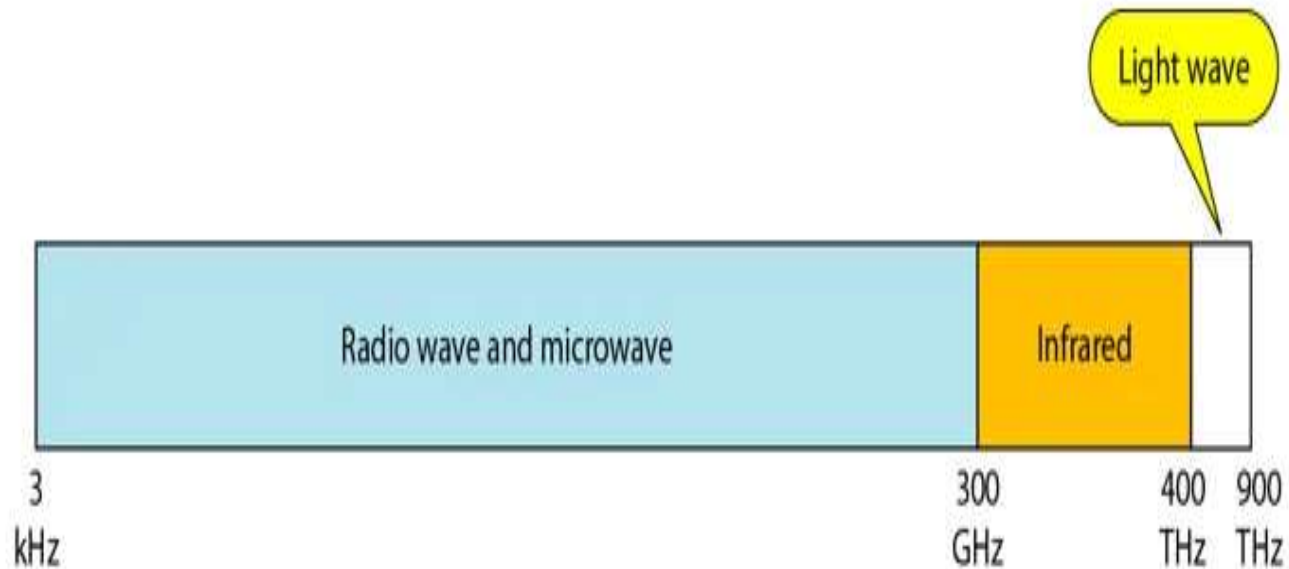
- Installation and maintenance
- Unidirectional light propagation
- Cost

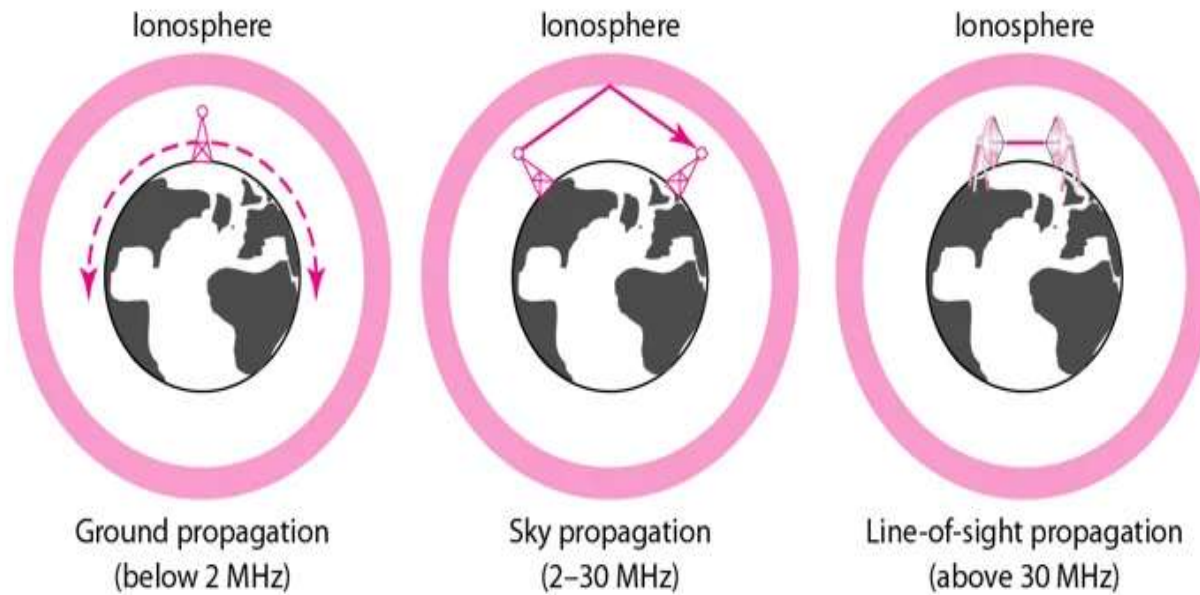
UnGuided Transmission

- An unguided transmission transmits the electromagnetic waves without using any physical medium. Therefore it is also known as **wireless transmission**.
- In unguided media, air is the media through which the electromagnetic energy can flow easily.

UnGuided Transmission

The below figure shows the part of the electromagnetic spectrum, ranging from 3 kHz to 900 THz, used for wireless communication.





Propagation Modes

Radio Waves

- Radio waves are the electromagnetic waves that are transmitted in all the directions of free space.
- Radio waves are omnidirectional, i.e., the signals are propagated in all the directions.
- The range in frequencies of radio waves is from 3Khz to 1 Ghz.
- In the case of radio waves, the sending and receiving antenna are not aligned.
- An example of the radio wave is **FM radio**.

Applications Of Radio waves



- A Radio wave is useful for multicasting when there is one sender and many receivers.
- An FM radio, television, cordless phones are examples of a radio wave.

Advantages and Disadvantages of Radio Transmission



- **Advantages :**

1. Radio waves are mainly used for Wide Area Networks (WAN) for example: Mobile networks.
2. Suitable for longer distance communications.
3. Signals can penetrate walls.
4. Higher data transmission rate compared to other transmission mediums.

- **Disadvantages :**

1. Waves are omnidirectional so faces interference from other signals of same frequency so disturbance can be there.
2. Not possible to isolate the communication inside the building.

Microwaves

- Microwaves are of two types:
 1. Terrestrial microwave
 2. Satellite microwave communication.

Terrestrial Type Microwave Transmission



1. Frequency range : 4-6Ghz to 21-23Ghz
2. Bandwidth : 1-10Mbps
3. Cost
4. Attenuation

- **Advantages of Terrestrial type microwave transmission:**

1. It is cheaper than cable transmission
2. Possible to implement in areas where cable transmission is difficult to implement such as hill areas.

- **Disadvantages of Terrestrial type microwave transmission:**

1. Not secure, susceptible to eavesdropping.
2. Weather condition can affect the transmission.
3. Limited bandwidth.

Satellite type microwave transmission



- **Advantages of Satellite type transmission:**
 1. The transmission can be done to the longer distances.
 2. Unlike terrestrial transmission where the implementation cost goes higher based on the transmission distance, the satellite communication is unaffected by the distance of the data transmission.

- **Disadvantages of Satellite type transmission:**
 1. Satellite designing and development requires more time and higher cost.
 2. The life of the satellite is about 12-15 years. Due to this reason, another launch of the satellite has to be planned before it becomes non-functional.
 3. The Satellite needs to be monitored and controlled on regular periods so that it remains in orbit.

Infrared Transmission

1. Infrared waves are highest frequency waves, frequency ranges from 300GHz to 400 THz.
2. Suitable for short distance communication.
3. Bandwidth is high so data transmit rate is high compared to other mediums.
4. These waves cannot penetrate walls, thus they are ideal for isolated communications.

- **Advantages of Infrared Transmission:**

1. Secure
2. High speed
3. High frequency signals
4. High data transfer rate

- **Disadvantages of Infrared Transmission:**

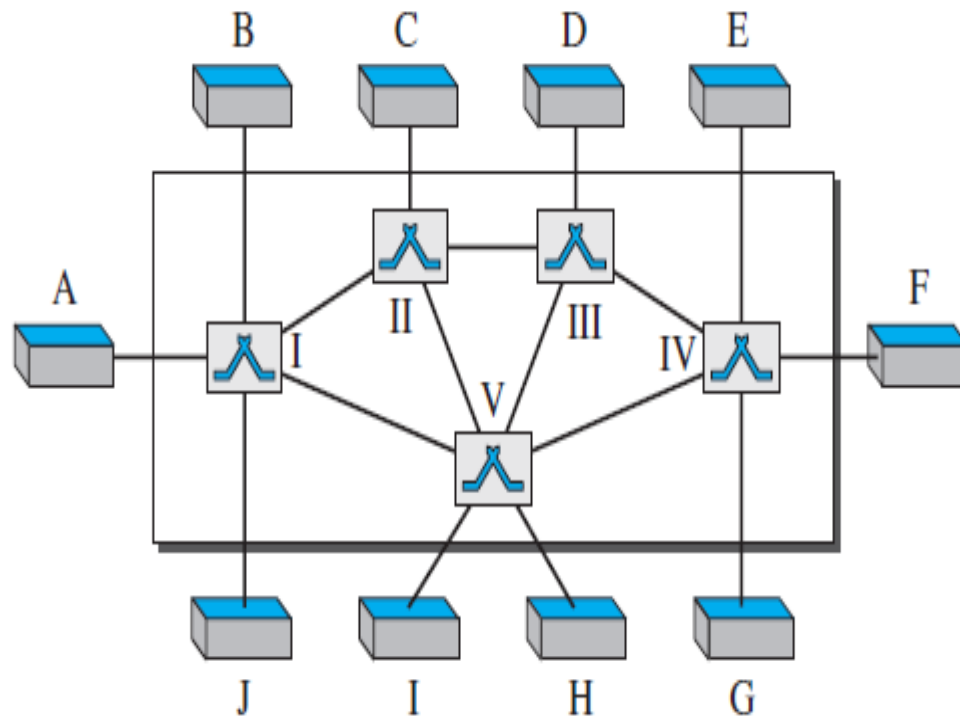
1. Sun rays interfere with the infrared rays so not ideal for outdoor communication.
2. Suitable for short distance communication only.
3. Cannot penetrate walls so difficult to establish a communication between two different rooms.

Switching

- A switched network consists of a series of interlinked nodes, called ***switches***.
- Switches are devices capable of creating temporary connections between two or more devices linked to the switch.
- In a switched network, some of these nodes are connected to the end systems (computers or telephones, for example). Others are used only for routing.

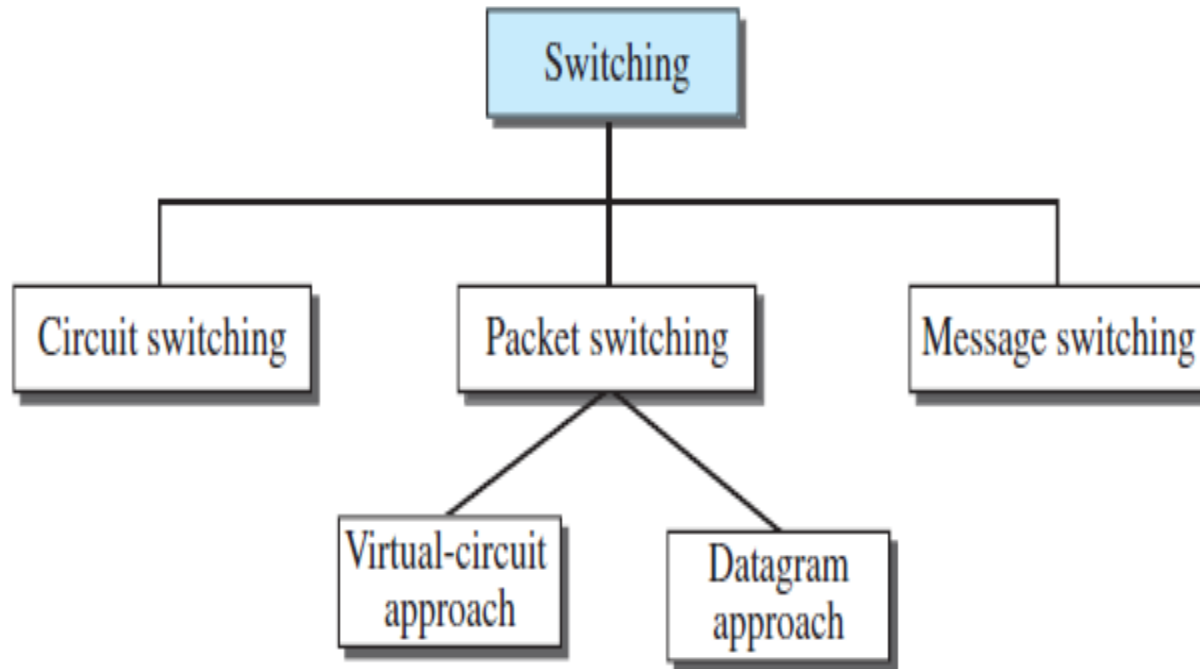
Switching

Figure 8.1 *Switched network*



Three Methods of Switching

Figure 8.2 *Taxonomy of switched networks*

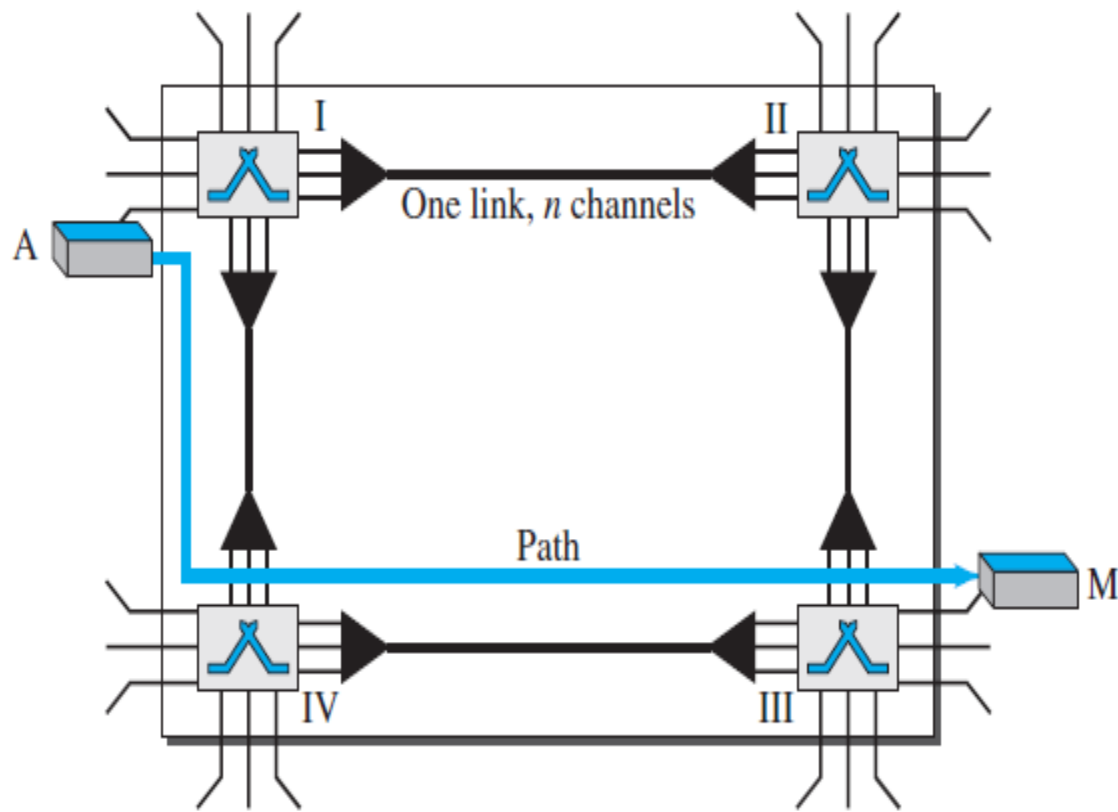


CIRCUIT-SWITCHED NETWORKS

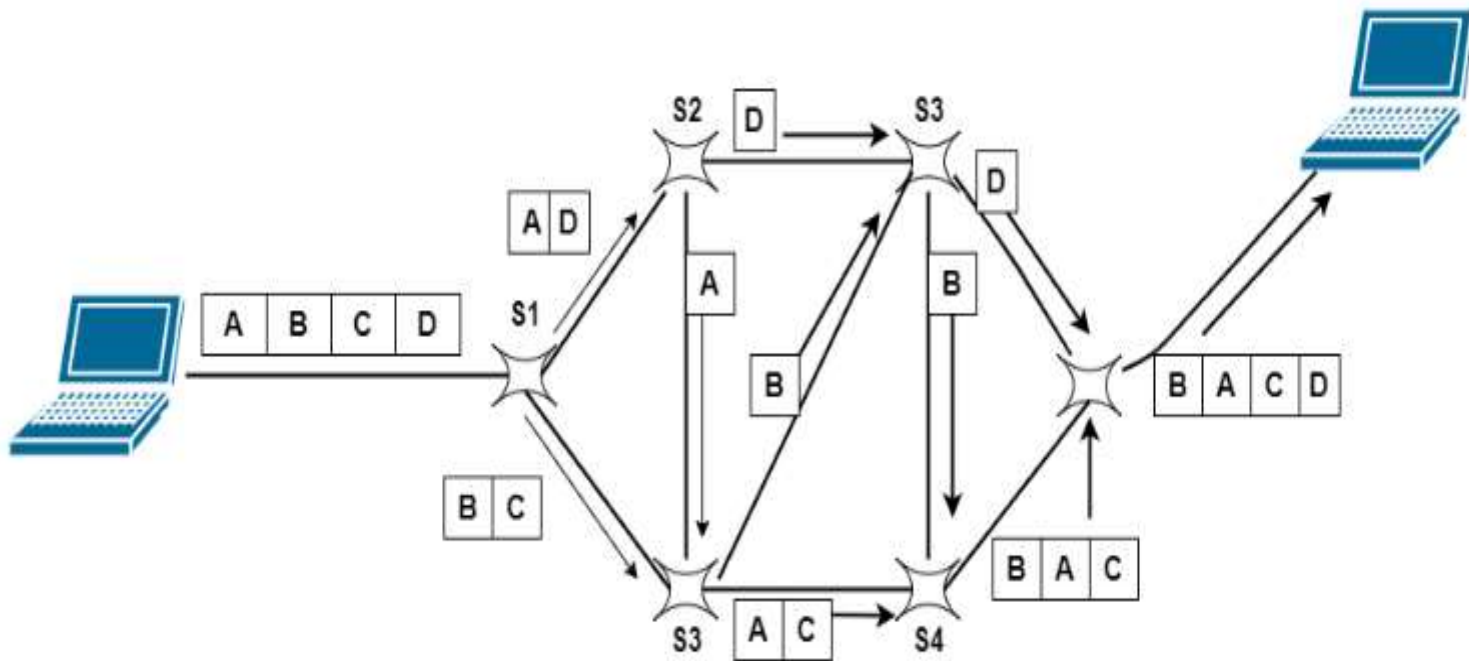
- A circuit-switched network is made of a set of switches connected by physical links, in which each link is divided into n channels.
- **Three Phases:**
 1. Setup Phase
 2. Data-Transfer Phase
 3. Teardown Phase

CIRCUIT-SWITCHED NETWORKS

Figure 8.3 *A trivial circuit-switched network*



PACKET SWITCHING



Datagram Packet Switching

- **Datagram Packet Switching:**
- In Datagram Switching, the packet is commonly known as a **datagram**.
- Datagram Packet switching is also known as Connectionless Packet Switching.
- In this technique, each packet routed individually by network devices on the basis of the destination address that is contained within each packet.

Virtual Circuit Switching

- Virtual Circuit Switching is also known as Connection-Oriented Switching.
- This switching contains the characteristics of circuit switching as well as datagram packet switching.
- In this type of packet switching the data-packets are first assembled and then sequentially numbered. Now they are ready to travel across a predefined route, sequentially.
- The information about the address is not required here, because all the data packets are sent in sequence.

Message-Switched Networks

- The Message-Switching Technique was mainly developed to act as an **alternative to circuit switching**, this was **before packet switching was introduced**. Basically, the message is a smaller unit.
- In the Message-Switching technique, the communication between end users is done by sending and receiving the message, and this message includes the **entire data to be shared**.

Message-Switched Networks

- In Message-Switching there is no dedicated path between the sender and receiver like circuit switching.
- The sender and receiver are connected by way of several intermediate nodes which helps and ensures proper data transfer between them.
- Message-Switched data networks are also known as **hop-by-hop** systems.

Characteristics of Message Switching

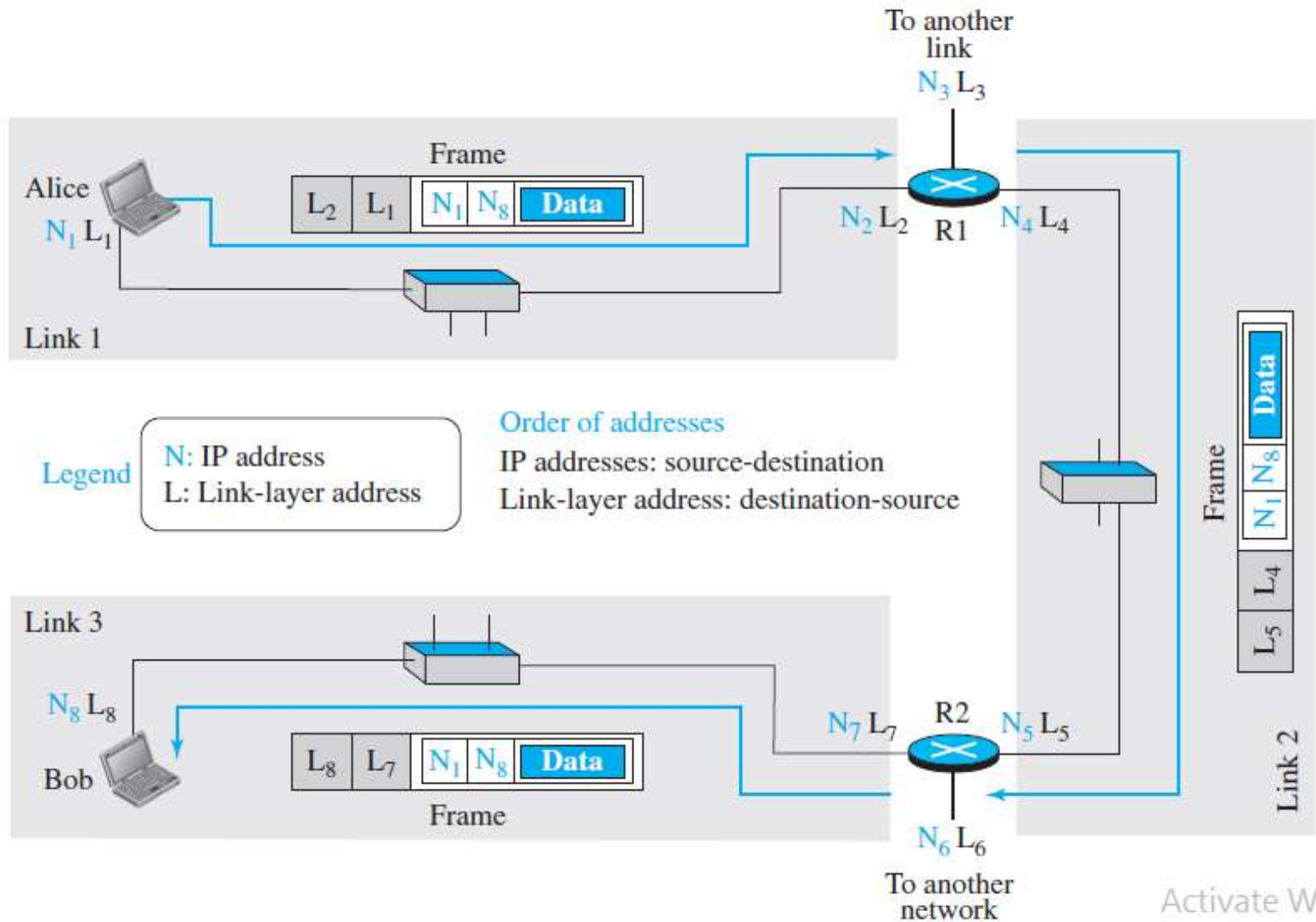


- **Store and Forward**
- **Message delivery**

Module -II: DATA LINK LAYER

Introduction: Link layer addressing; Error detection and correction: Cyclic codes, checksum, forward error correction; Data link control: DLC services, data link layer protocols, media access control: Random access, virtual LAN.

Link layer addressing



Three Types of addresses

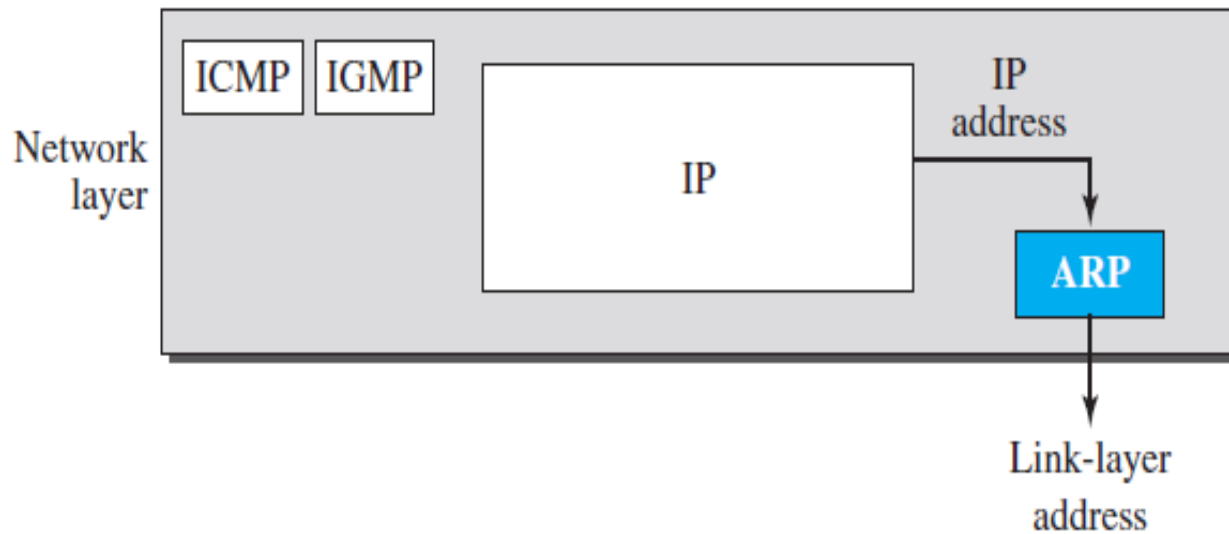
1. Unicast Address : one-to-one
2. Multicast Address : one-to-many
3. Broadcast Address : one-to-all

Examples:

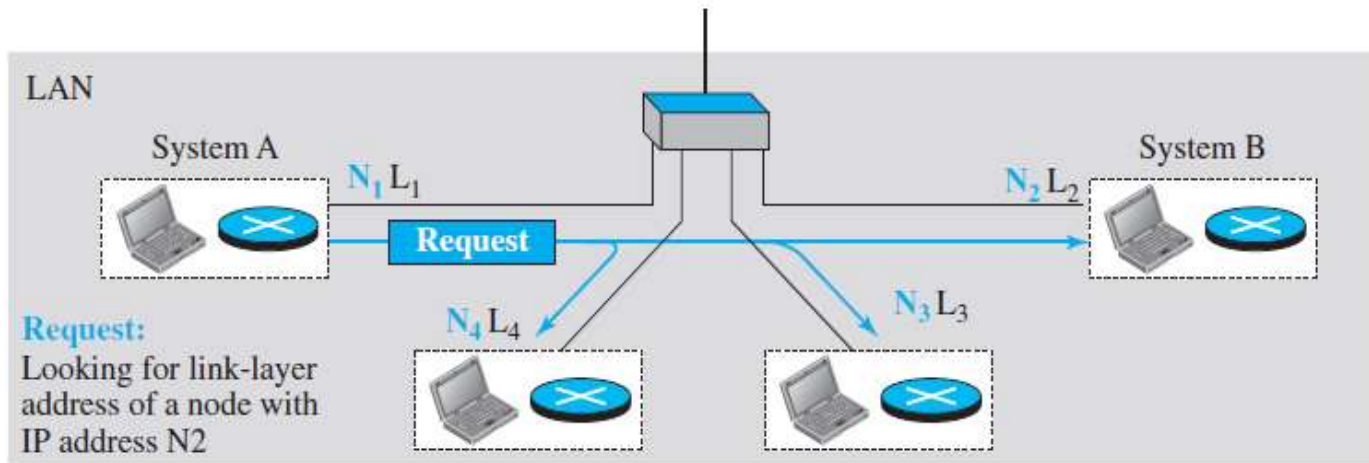
- A3:34:45:11:92:F1
- A2:34:45:11:92:F1
- FF:FF:FF:FF:FF:FF

Address Resolution Protocol (ARP)

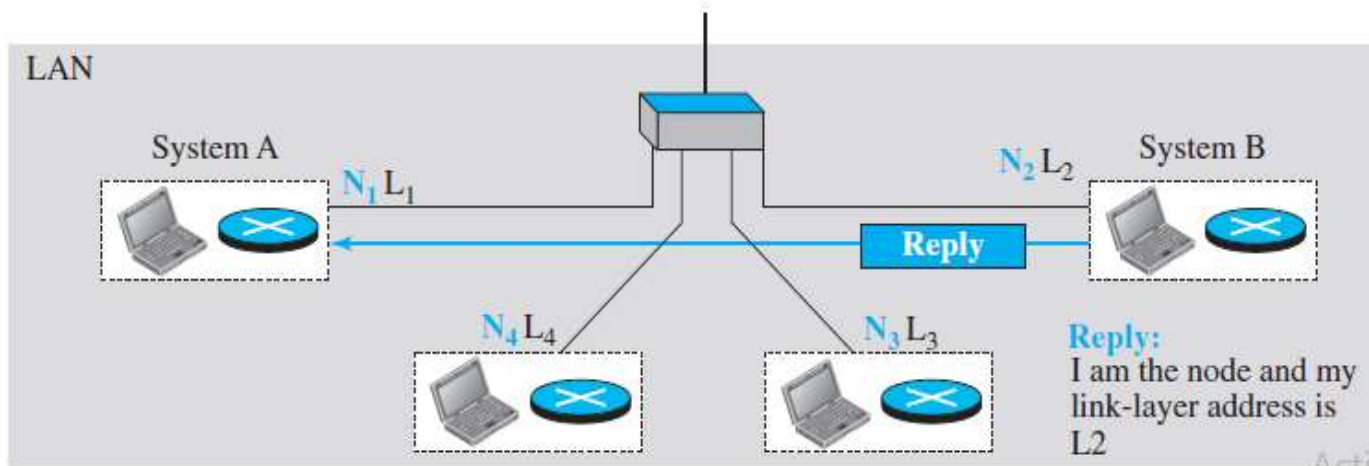
Figure 9.6 *Position of ARP in TCP/IP protocol suite*



ARP OPERATION



a. ARP request is broadcast



b. ARP reply is unicast

ARP PACKET FORMAT

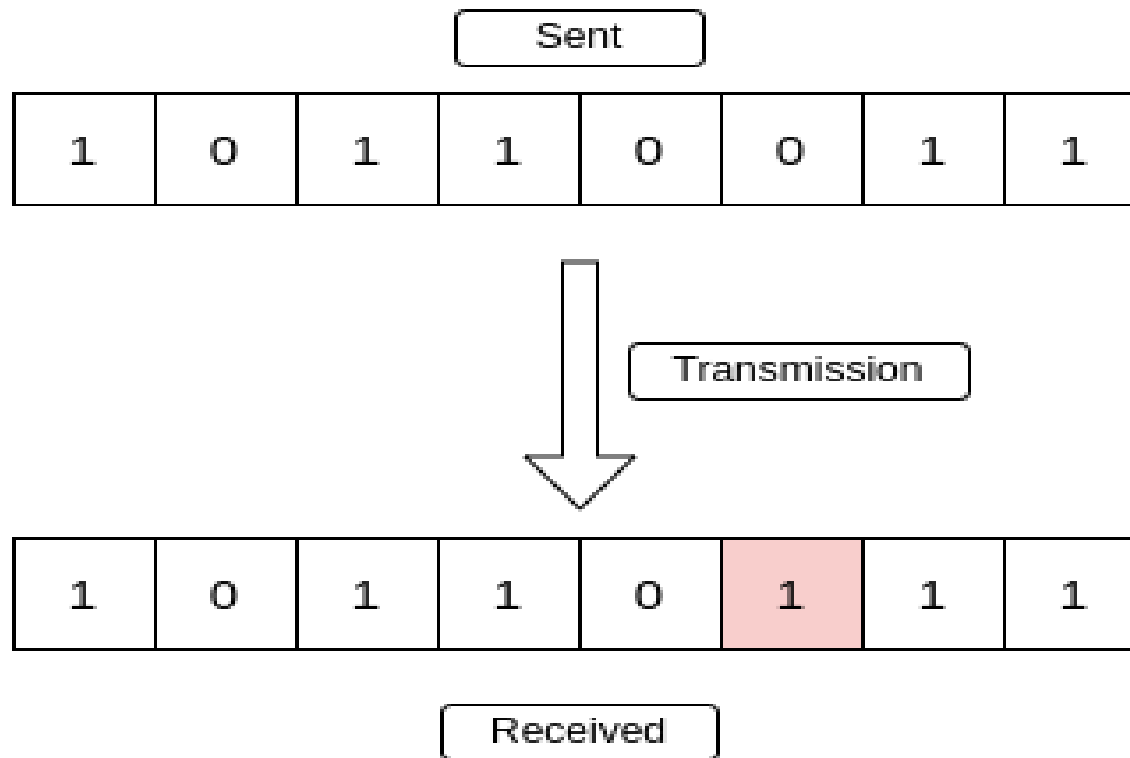
Figure 9.8 *ARP packet*

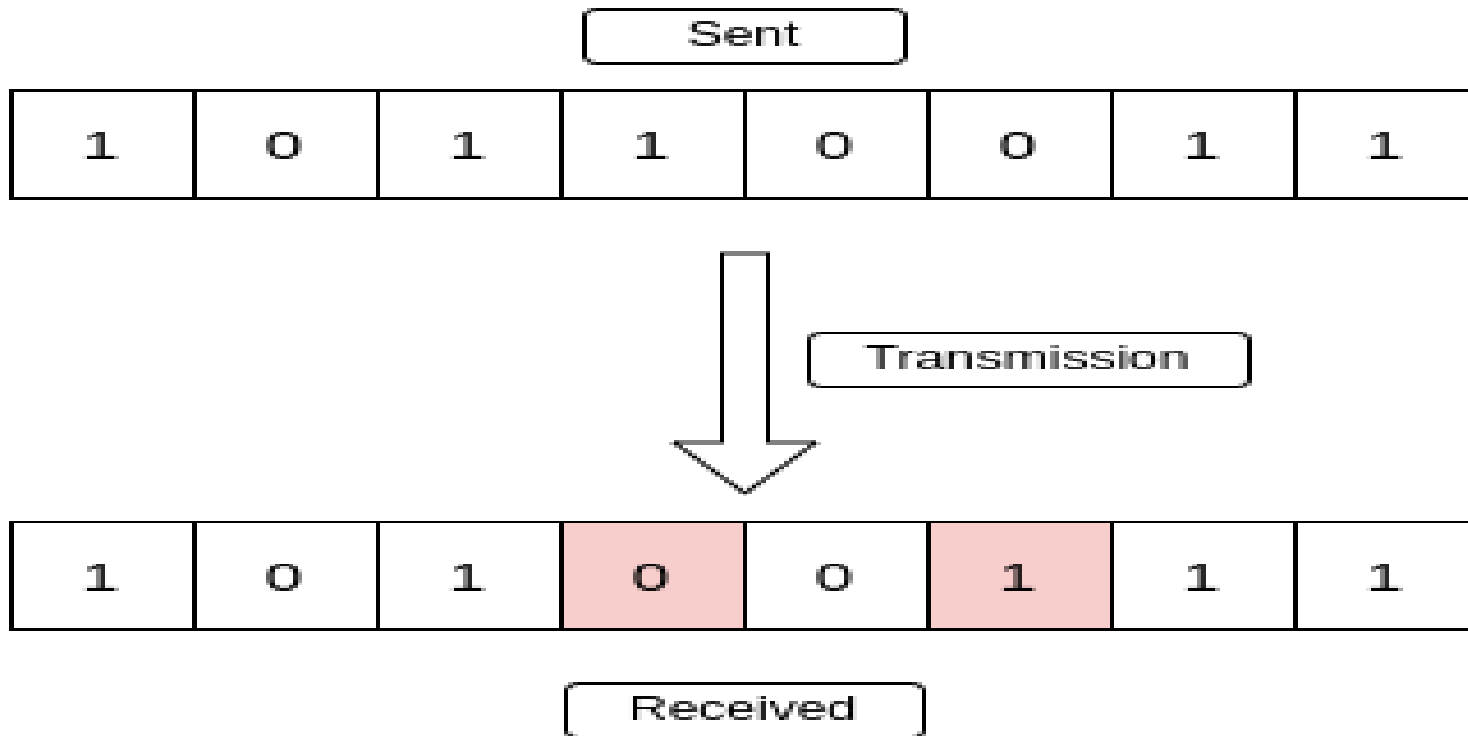
0	8	16	31
Hardware Type		Protocol Type	
Hardware length	Protocol length	Operation Request:1, Reply:2	
Source hardware address			
Source protocol address			
Destination hardware address (Empty in request)			
Destination protocol address			

Error Detection and Correction

- **Types of Errors:**

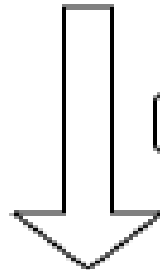
1. Single-bit error
2. Multi-bit error
3. Burst error





Sent

1	0	1	1	0	0	1	1
---	---	---	---	---	---	---	---



Transmission

1	1	0	0	0	1	1	1
---	---	---	---	---	---	---	---

Received

Error Control

- Error control can be done in two ways
 1. **Error detection**
 2. **Error correction**

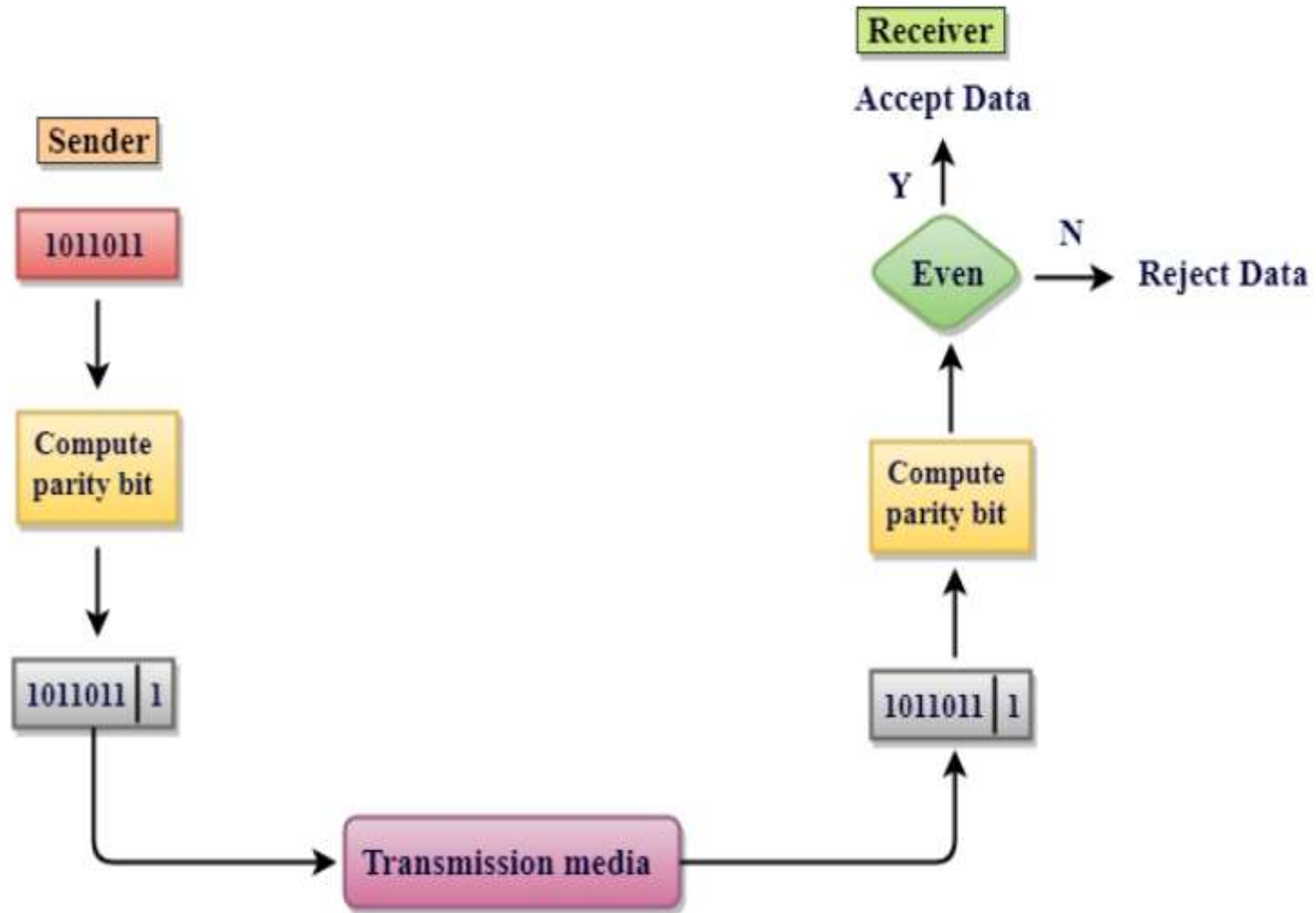
Error Detection Techniques

- Single parity check
- Two-dimensional parity check
- Checksum
- Cyclic redundancy check

Parity Check

- In case of even parity: If a number of 1s is even then parity bit value is 0. If the number of 1s is odd then parity bit value is 1.
- In case of odd parity: If a number of 1s is odd then parity bit value is 0. If a number of 1s is even then parity bit value is 1.

Single Parity Check



Drawbacks Of Single Parity Checking



- It can only detect single-bit errors which are very rare.
- If two bits are interchanged, then it cannot detect the errors.

Two-dimensional parity check

Original Data

10011001	11100010	00100100	10000100
----------	----------	----------	----------

Row parities

10011001	0
11100010	0
00100100	0
10000100	0
11011011	0

Column
parities



100110010	111000100	001001000	100001000	110110110
-----------	-----------	-----------	-----------	-----------

Data to be sent

Drawbacks Of 2D Parity Check

- If two bits in one data unit are corrupted and two bits exactly the same position in another data unit are also corrupted, then 2D Parity checker will not be able to detect the error.
- This technique cannot be used to detect the 4-bit errors or more in some cases.

Checksum

- For error detection by checksums, data is divided into fixed sized frames or segments.
- **Sender's End** – The sender adds the segments using 1's complement arithmetic to get the sum. It then complements the sum to get the checksum and sends it along with the data frames.
- **Receiver's End** – The receiver adds the incoming segments along with the checksum using 1's complement arithmetic to get the sum and then complements it.
- If the result is zero, the received frames are accepted; otherwise they are discarded.

Sender's End

Frame 1:	11001100
Frame 2:	+ 10101010
Partial Sum:	1 01110110
	+ 1
	01110111
Frame 3:	+ 11110000
Partial Sum:	1 01100111
	+ 1
	01101000
Frame 4:	+ 11000011
Partial Sum:	1 00101011
	+ 1
Sum:	00101100
Checksum:	11010011

Receiver's End

Frame 1:	11001100
Frame 2:	+ 10101010
Partial Sum:	1 01110110
	+ 1
	01110111
Frame 3:	+ 11110000
Partial Sum:	1 01100111
	+ 1
	01101000
Frame 4:	+ 11000011
Partial Sum:	1 00101011
	+ 1
Sum:	00101100
Checksum:	11010011
Sum:	11111111
Complement:	00000000

Hence accept frames.

Cyclic Redundancy Check (CRC)

- CRC Generator
 - Frame- 1010101010
 - Key-11001
- CRC Checker
 - Frame- 1010101010
 - Key-11001
 - Reminder =0000

Error Correction Techniques

- **Backward Error Correction (Retransmission)** – If the receiver detects an error in the incoming frame, it requests the sender to retransmit the frame. It is a relatively simple technique. But it can be efficiently used only where retransmitting is not expensive as in fiber optics and the time for retransmission is low relative to the requirements of the application.

- **Forward Error Correction** – If the receiver detects some error in the incoming frame, it executes error-correcting code that generates the actual frame. This saves bandwidth required for retransmission. It is inevitable in real-time systems. However, if there are too many errors, the frames need to be retransmitted.

Data Link Control(DLC)

- **DLC SERVICES:**

1. Framing
2. Flow and Error Control
3. Connectionless and Connection-Oriented

- **Frame Size:**

fixed-size framing

variable-size framing

- **Variable-size framing:**

Character-Oriented Framing

Bit-Oriented Framing

Character-Oriented Framing

Figure 11.1 *A frame in a character-oriented protocol*

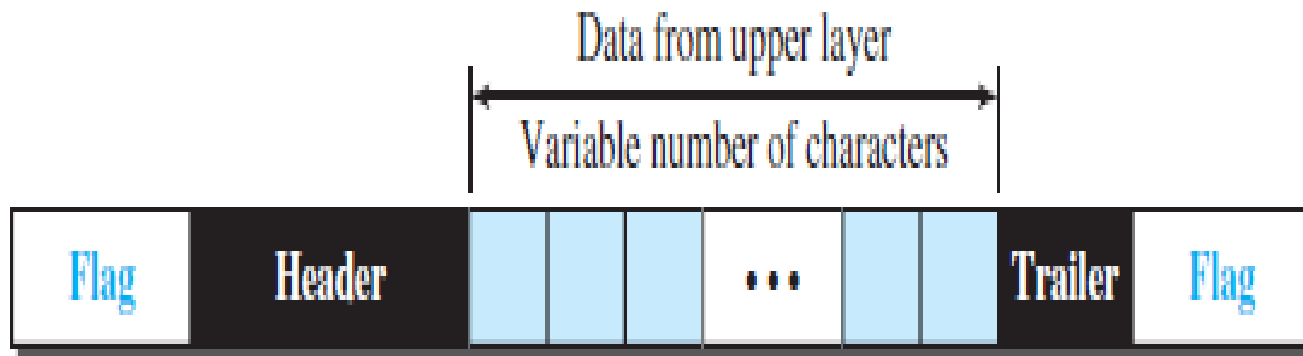
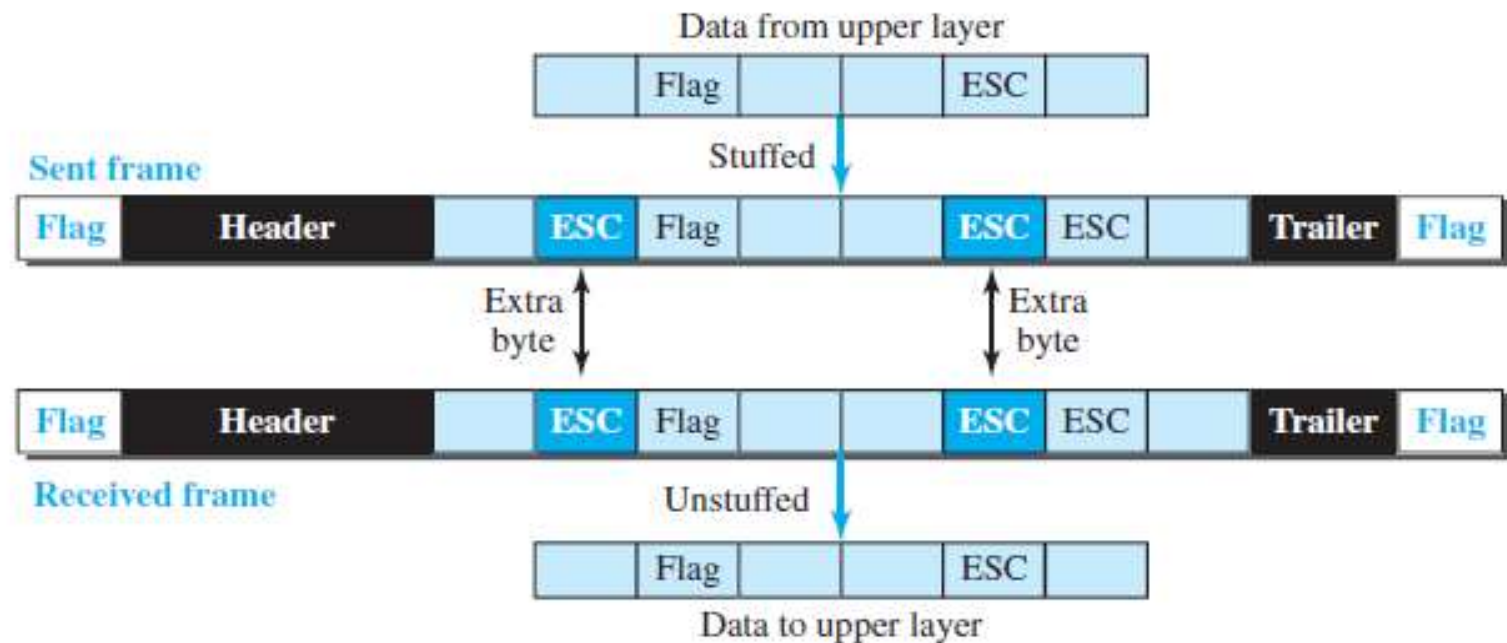


Figure 11.2 *Byte stuffing and unstuffing*



Byte stuffing is the process of adding one extra byte whenever there is a flag or escape character in the text.

Bit-Oriented Framing

Figure 11.3 *A frame in a bit-oriented protocol*

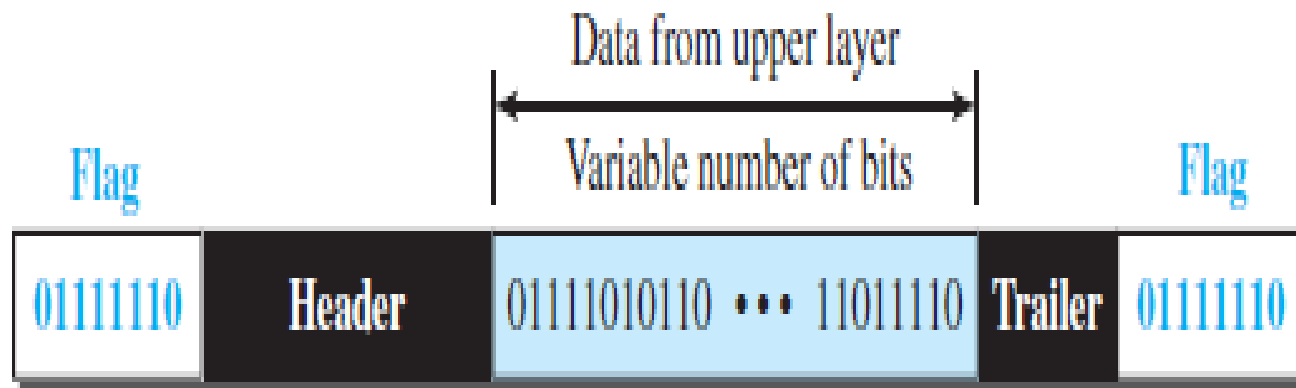
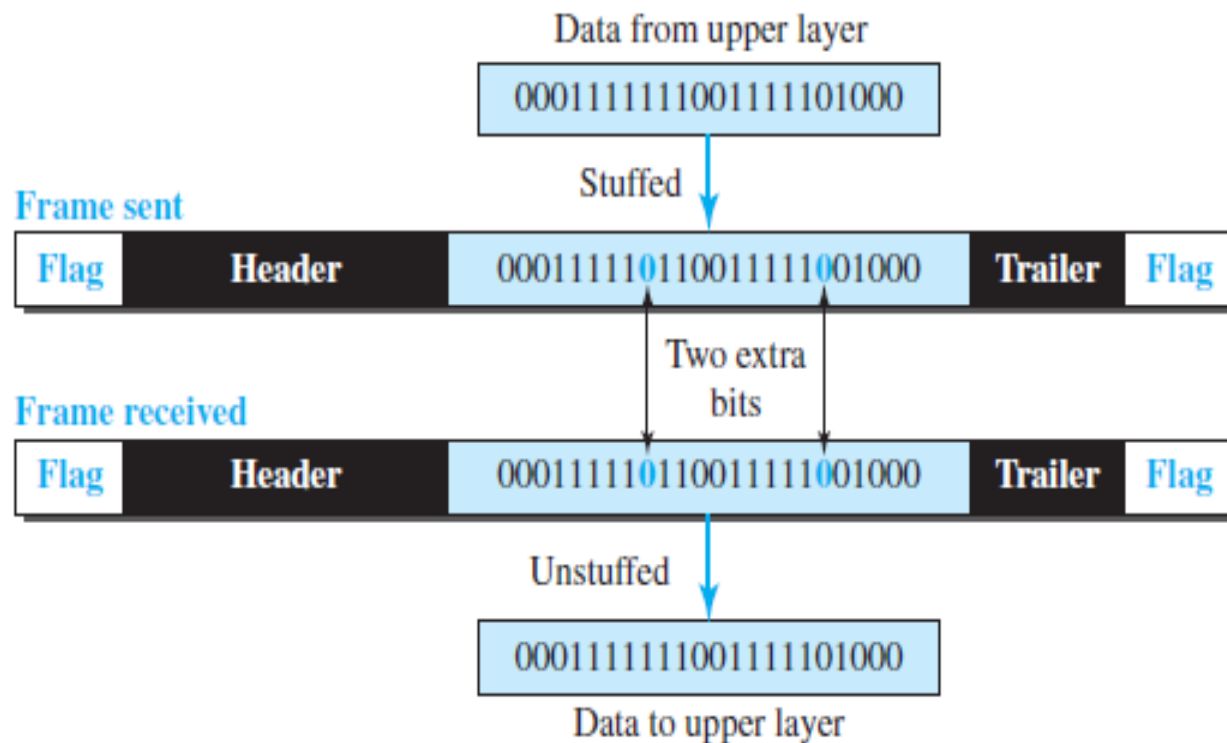


Figure 11.4 *Bit stuffing and unstuffing*

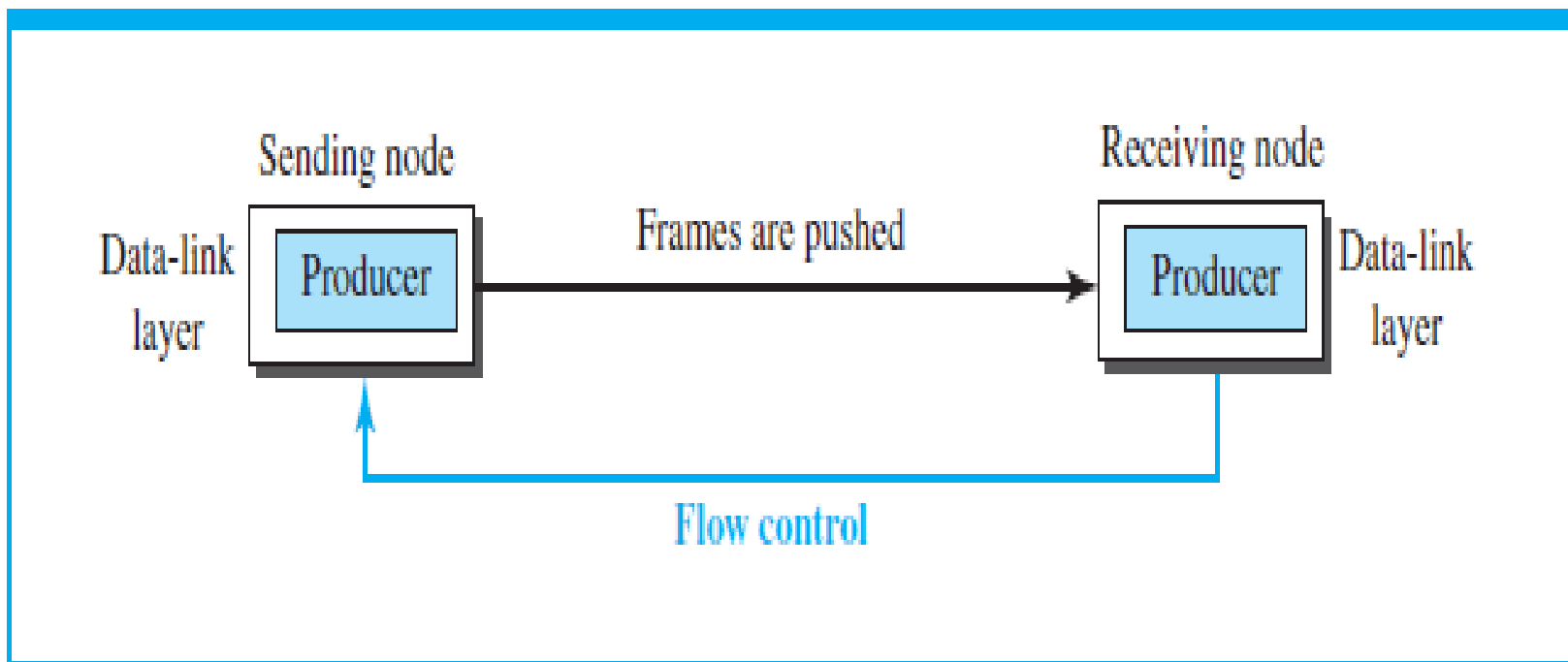


Flow and Error Control

- **Flow Control**
- **Buffers**
- **Error Control**
- **Combination of Flow and Error Control**

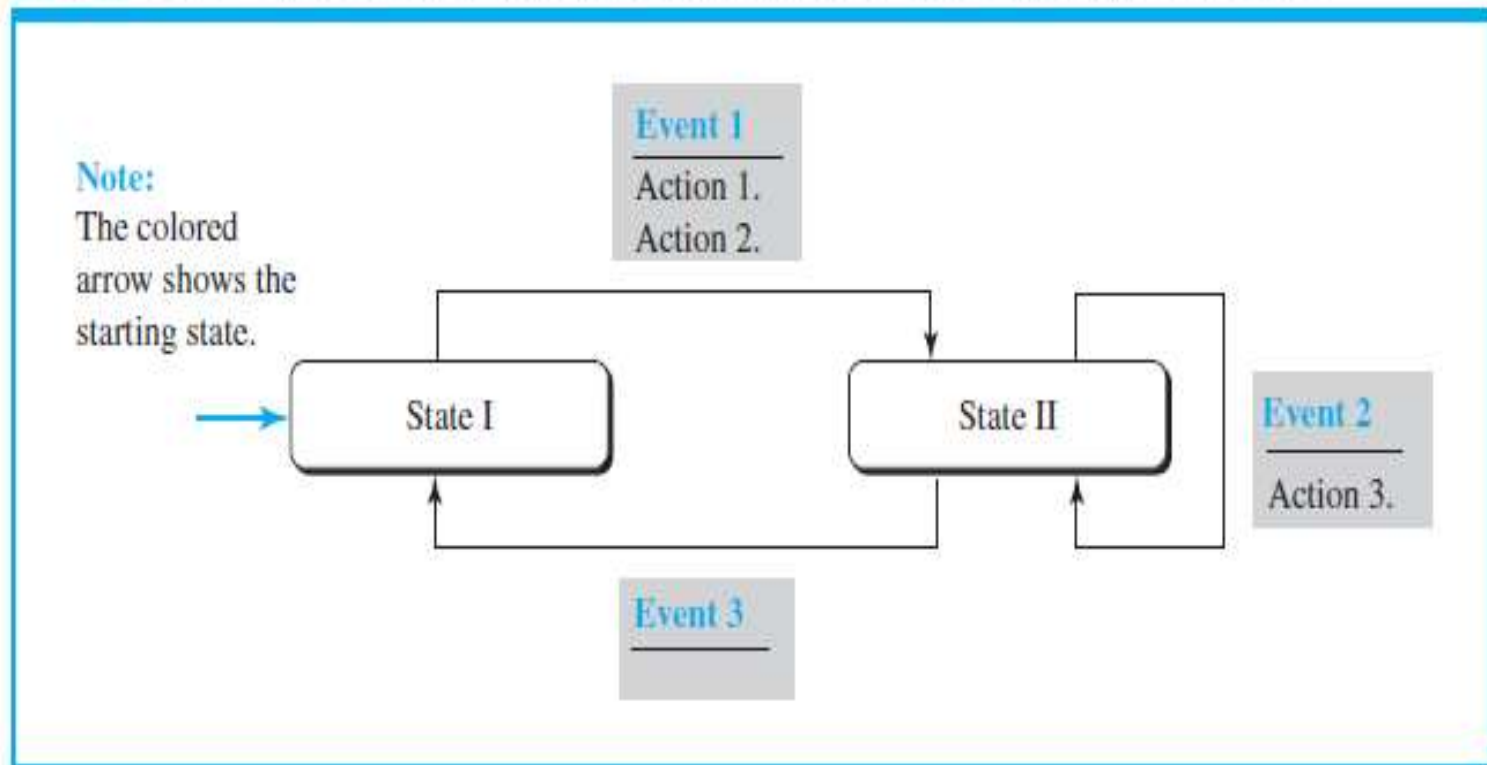
Flow Control

Figure 11.5 *Flow control at the data-link layer*



DATA-LINK LAYER PROTOCOLS

Figure 11.6 *Connectionless and connection-oriented service represented as FSMs*



Connectionless and Connection-Oriented

- **Connectionless Protocol:**
- In a connectionless protocol, frames are sent from one node to the next without any relationship between the frames
- Each frame is independent
- **Connection-Oriented Protocol**
- In a connection-oriented protocol, a logical connection should first be established between the two nodes (setup phase).
- After all frames that are somehow related to each other are transmitted (transfer phase),
- the logical connection is terminated (teardown phase).

Simple Protocol

Figure 11.7 *Simple protocol*

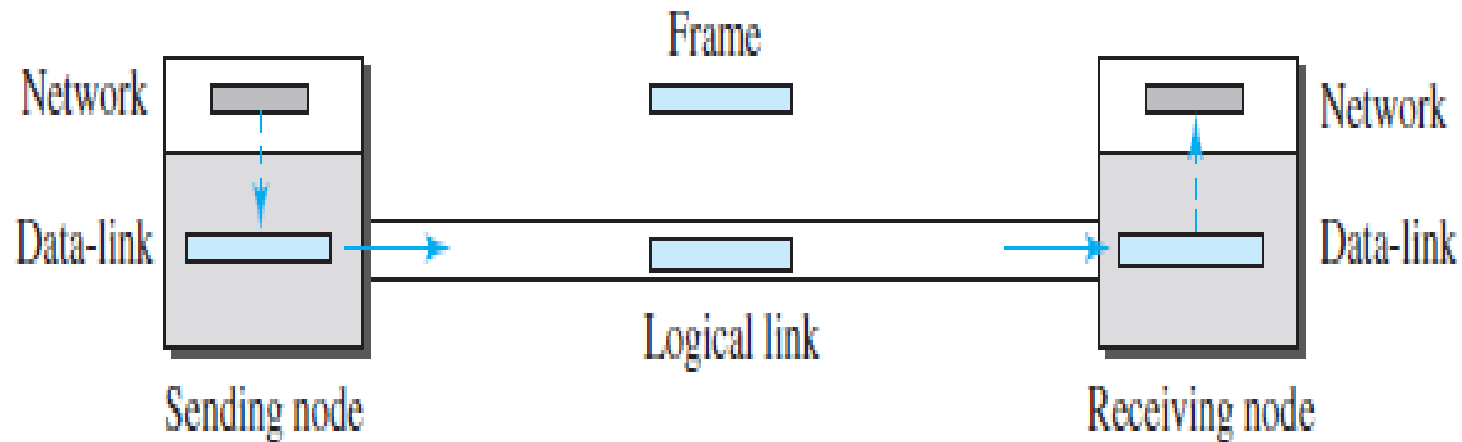


Figure 11.8 *FSMs for the simple protocol*

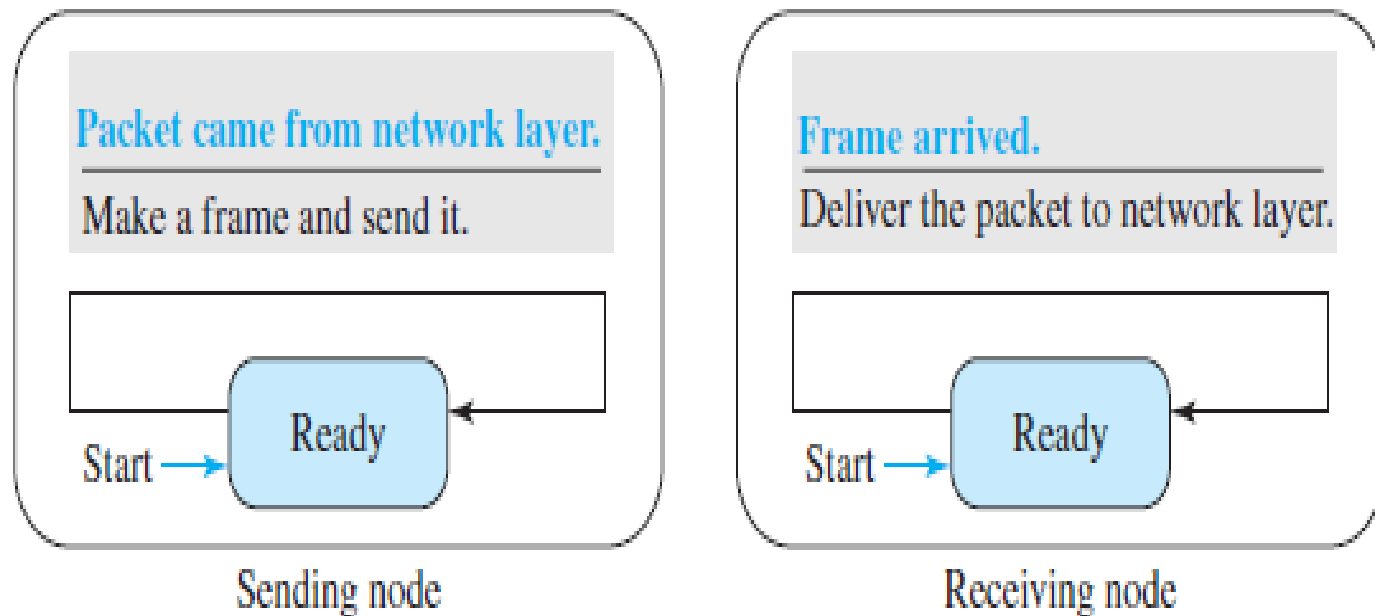
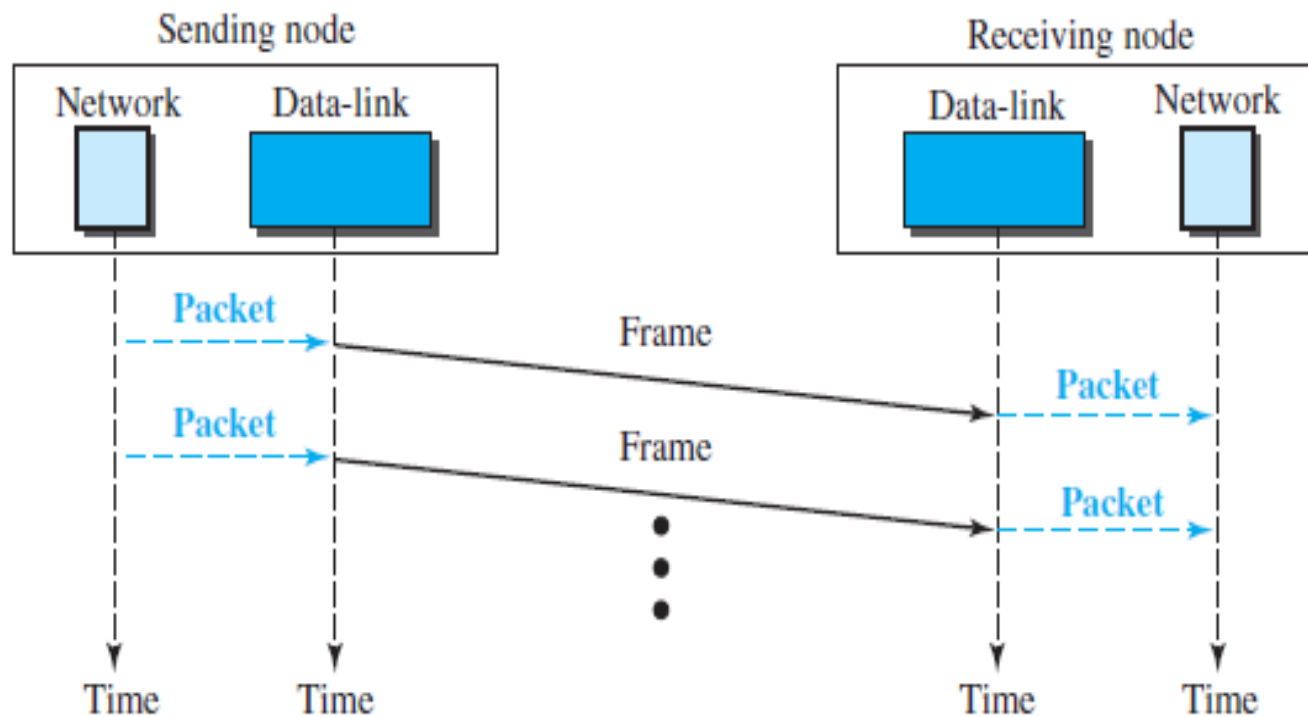


Figure 11.9 *Flow diagram for Example 11.2*



Stop-and-Wait Protocol

Figure 11.10 *Stop-and-Wait protocol*

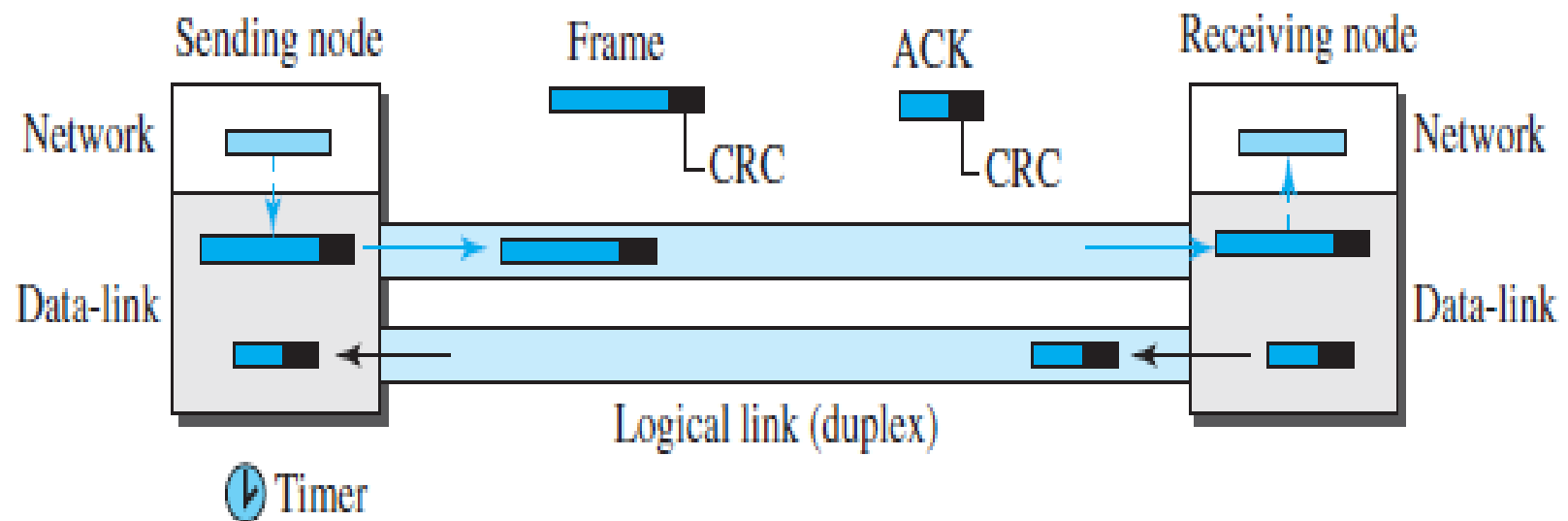


Figure 11.11 *FSM for the Stop-and-Wait protocol*

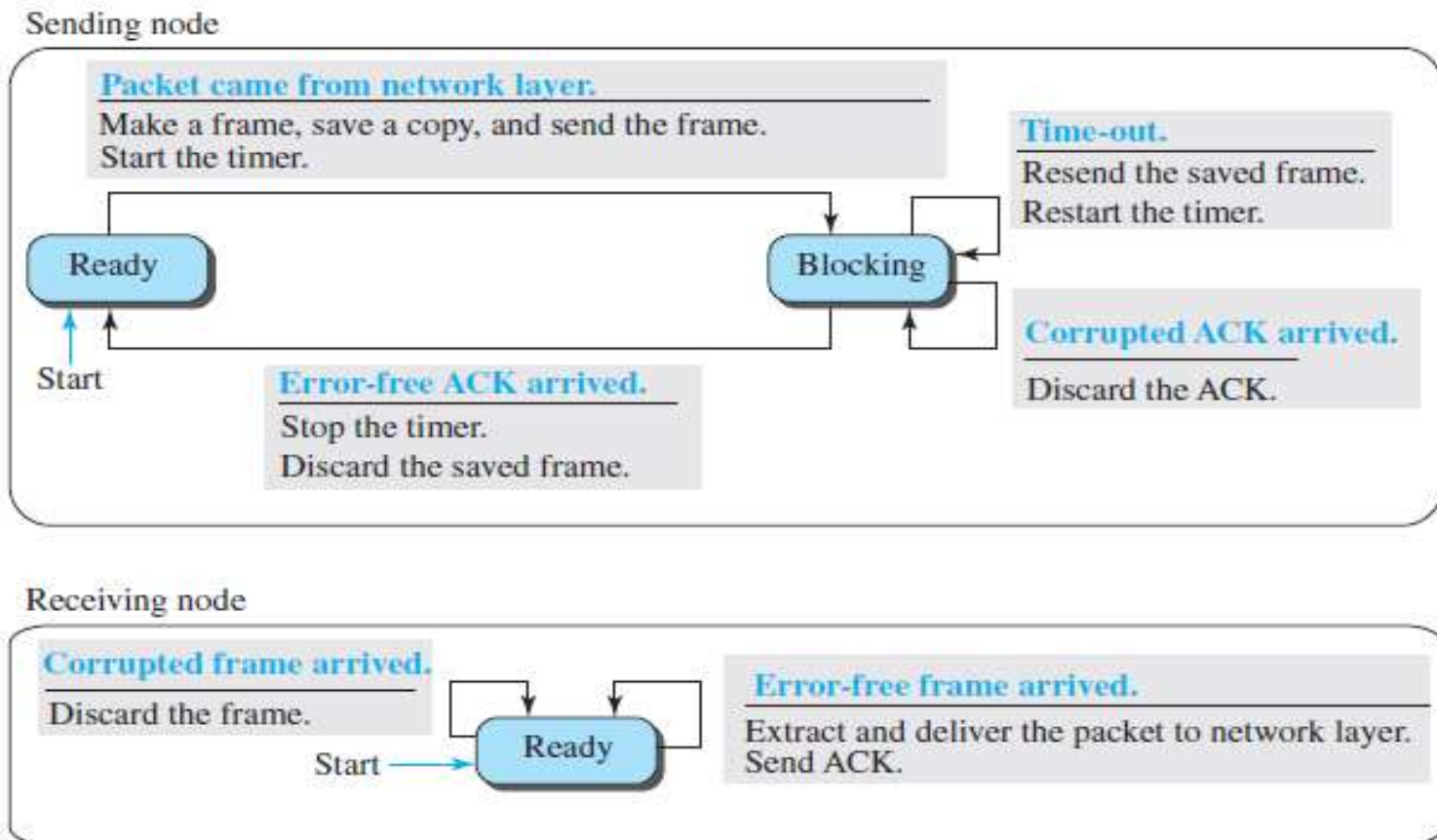


Figure 11.12 Flow diagram for Example 11.3

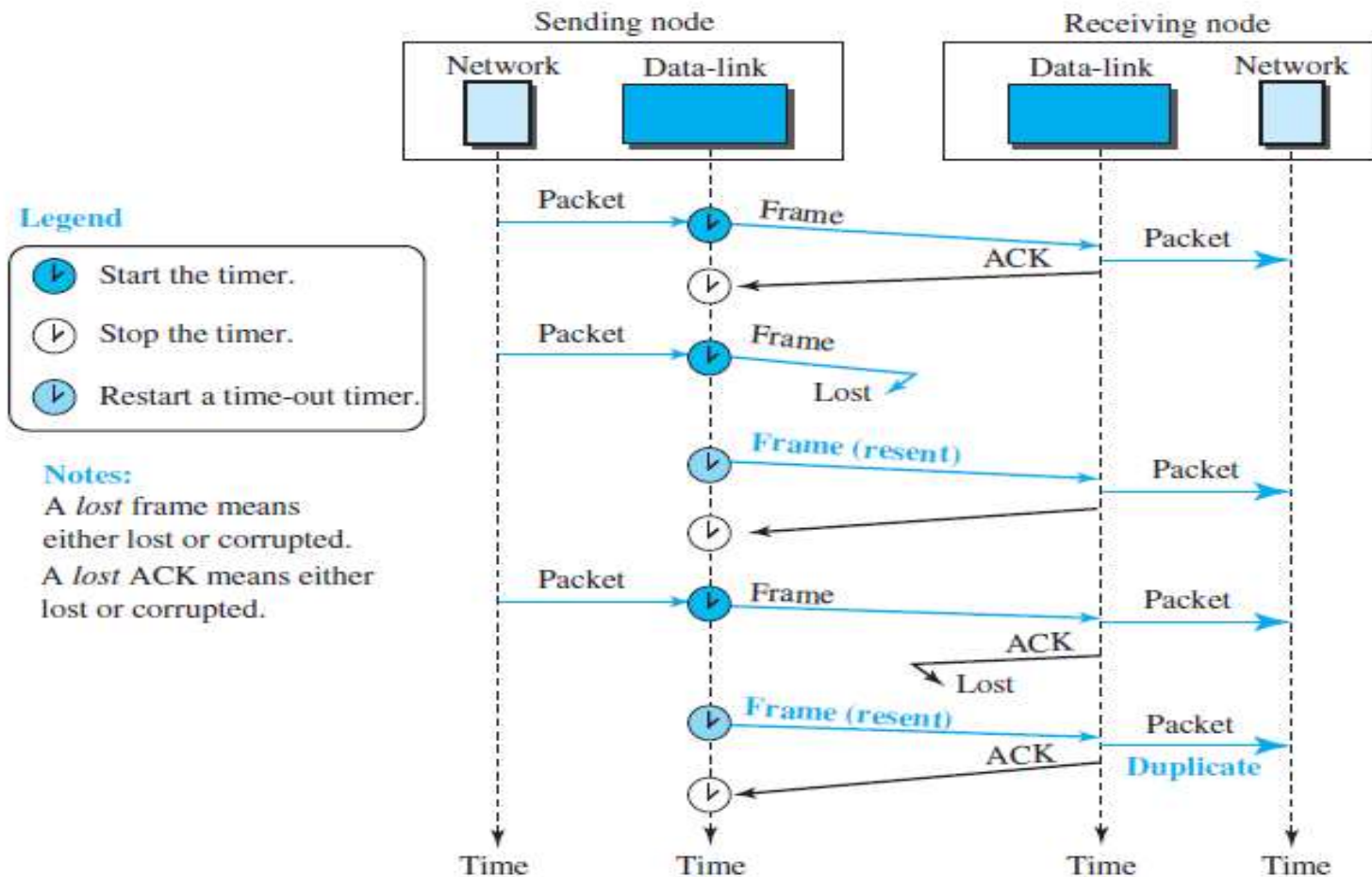
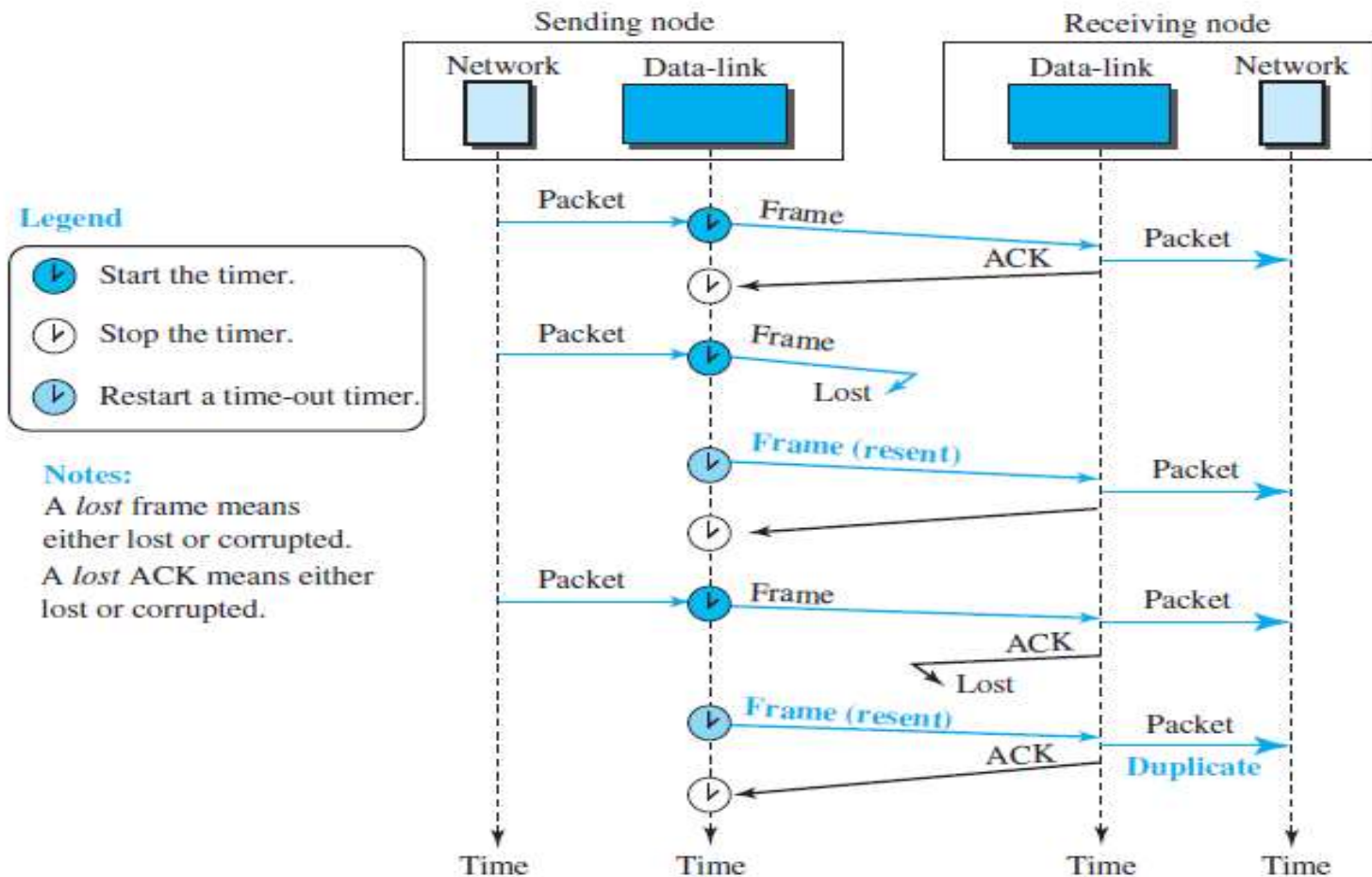


Figure 11.12 Flow diagram for Example 11.3

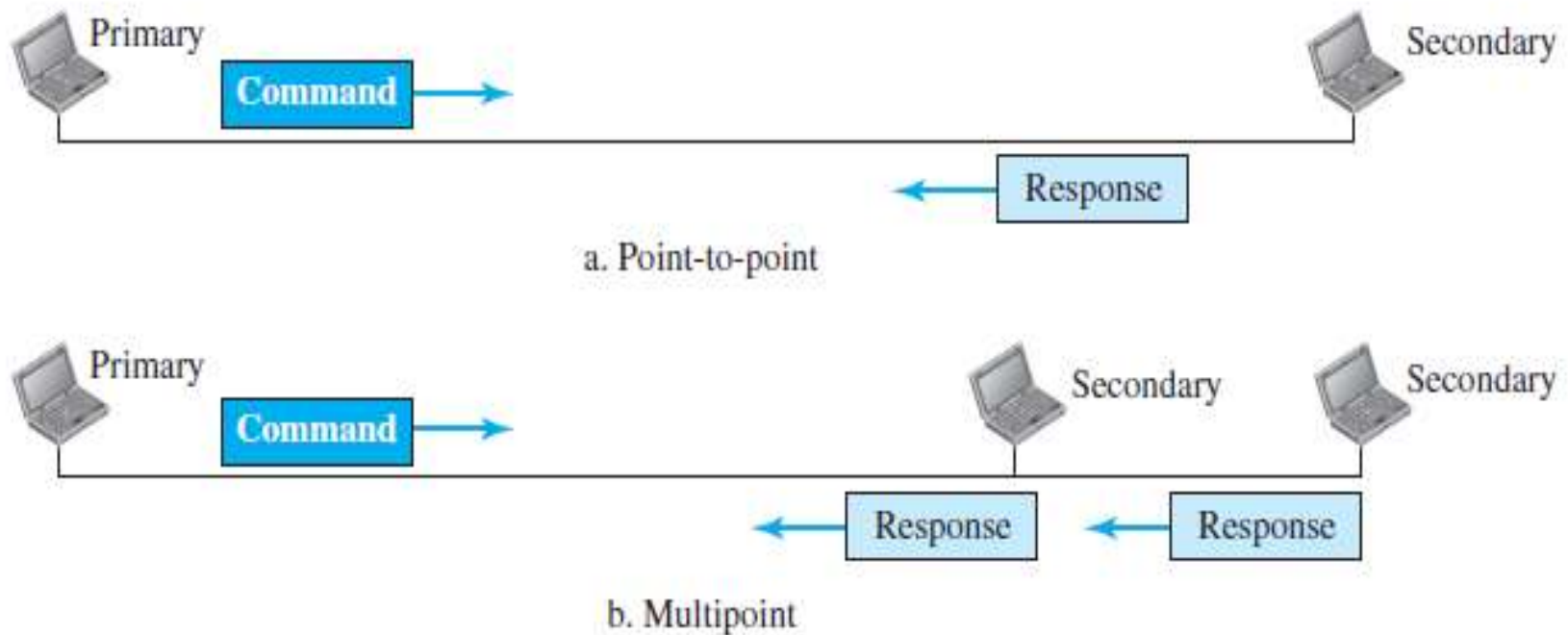


Sliding Window Protocol

- Sliding window protocol has two types:
 1. Go-Back-N ARQ
 2. Selective Repeat ARQ

HDLC

Figure 11.14 *Normal response mode*



Configurations and Transfer Modes

Figure 11.15 *Asynchronous balanced mode*

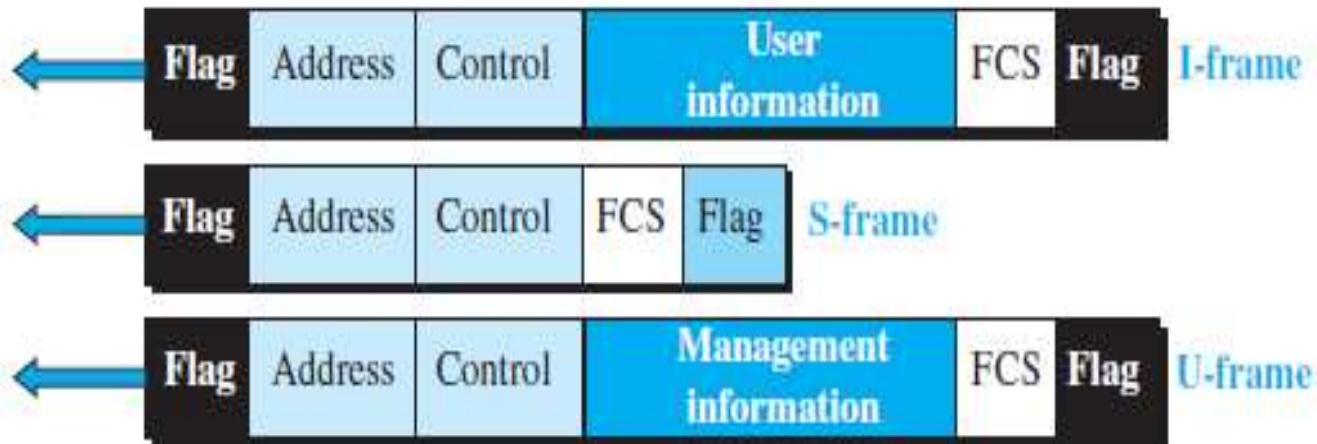


Framing

- information frames(I-frames) : control information relating to user data
- supervisory frames (S-frames) : to transport control information
- unnumbered frames (U-frames): are reserved for system management.

Framing

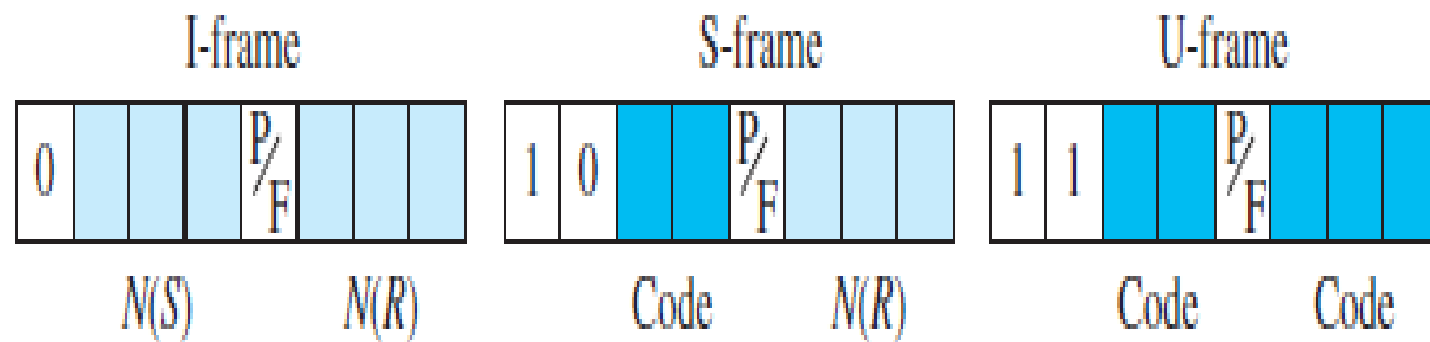
Figure 11.16 HDLC frames



Fields and their use in different frame types

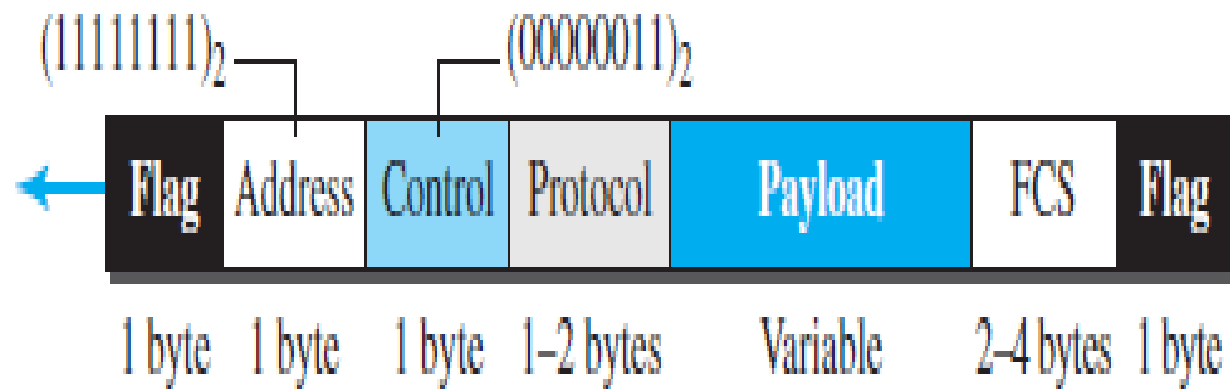
- **Flag field**
- **Address field**
- **Control field**
- **Information field**
- **FCS field**

Figure 11.17 *Control field format for the different frame types*



POINT-TO-POINT PROTOCOL (PPP)

Figure 11.20 *PPP frame format*

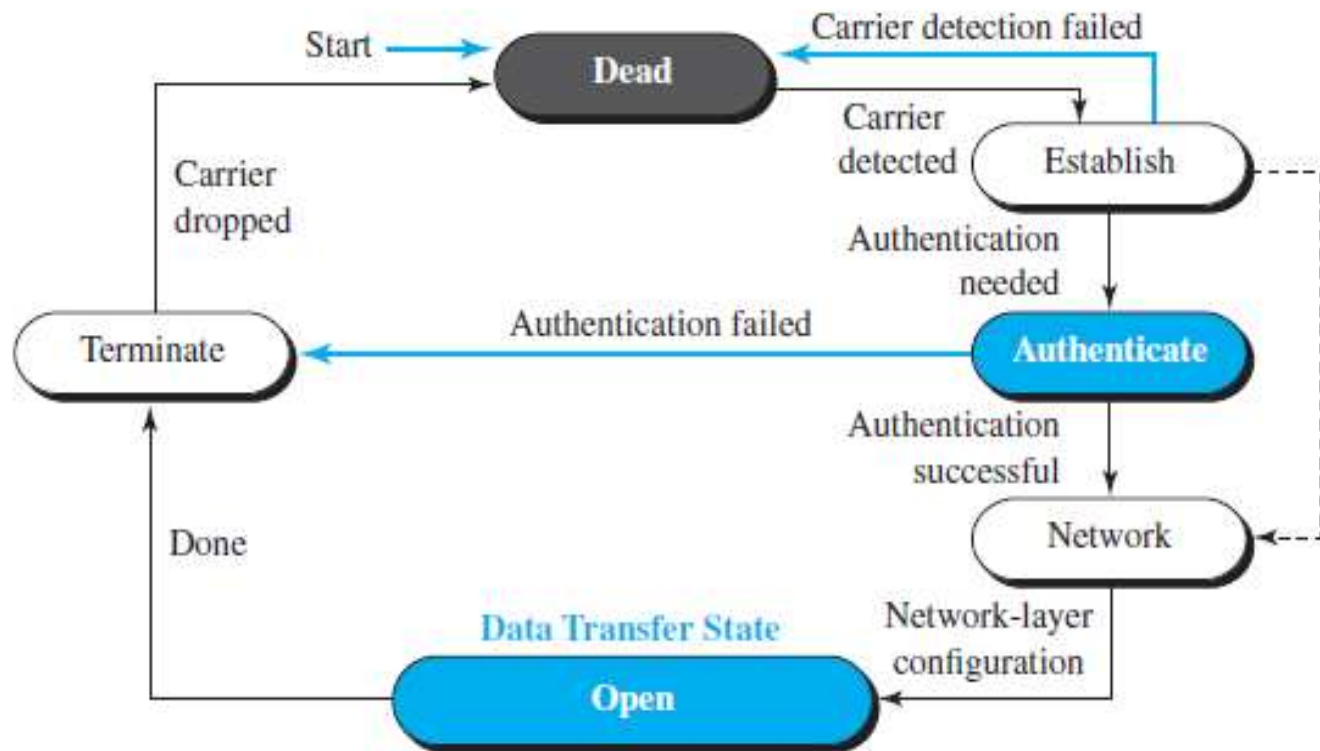


Framing

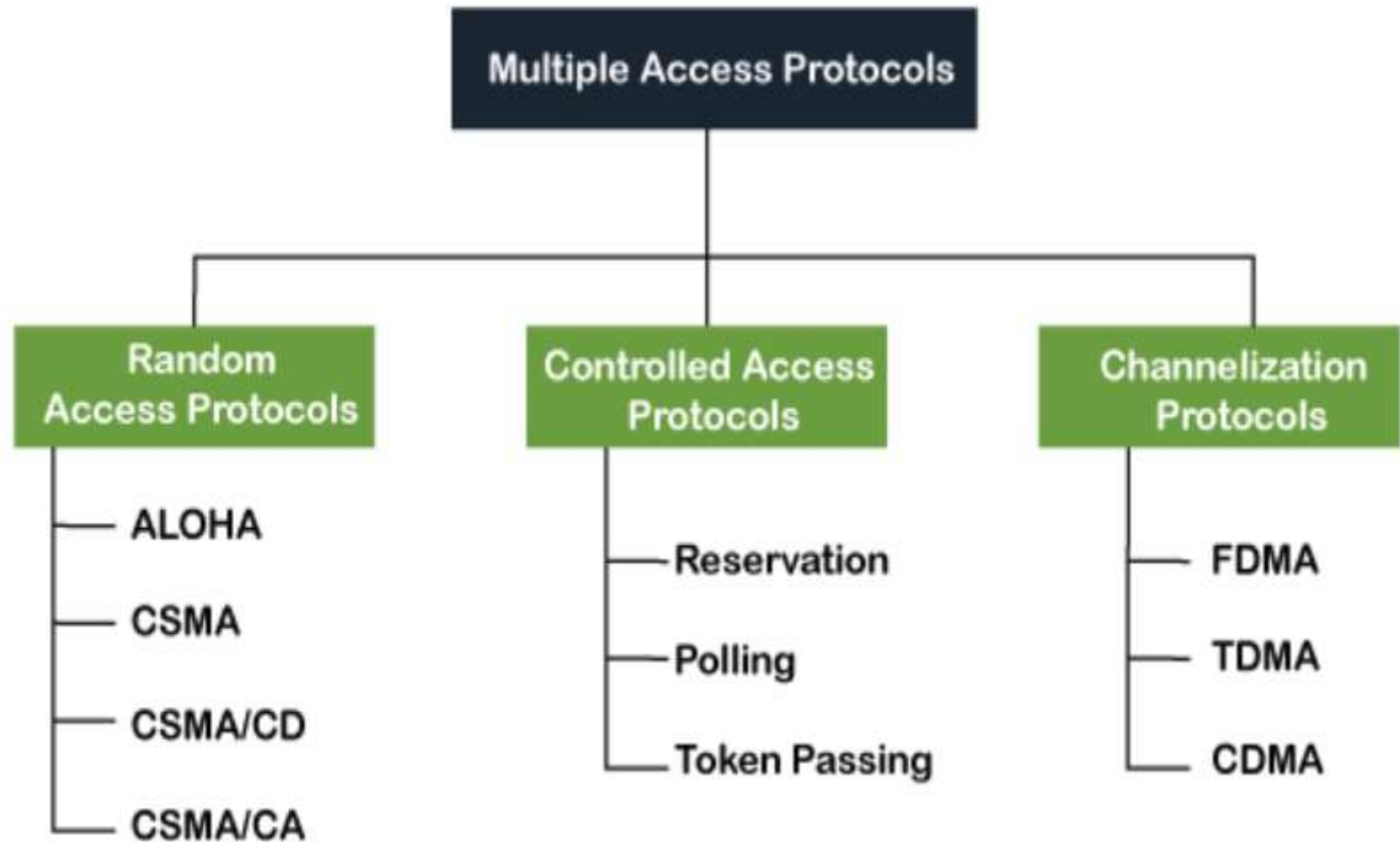
- **Flag**
- **Address**
- **Control**
- **Protocol**
- **Payload field**
- **FCS**

Transition Phases

Figure 11.21 Transition phases



Media Access Protocol



Random Access Protocol

- Aloha
- CSMA
- CSMA/CD
- CSMA/CA

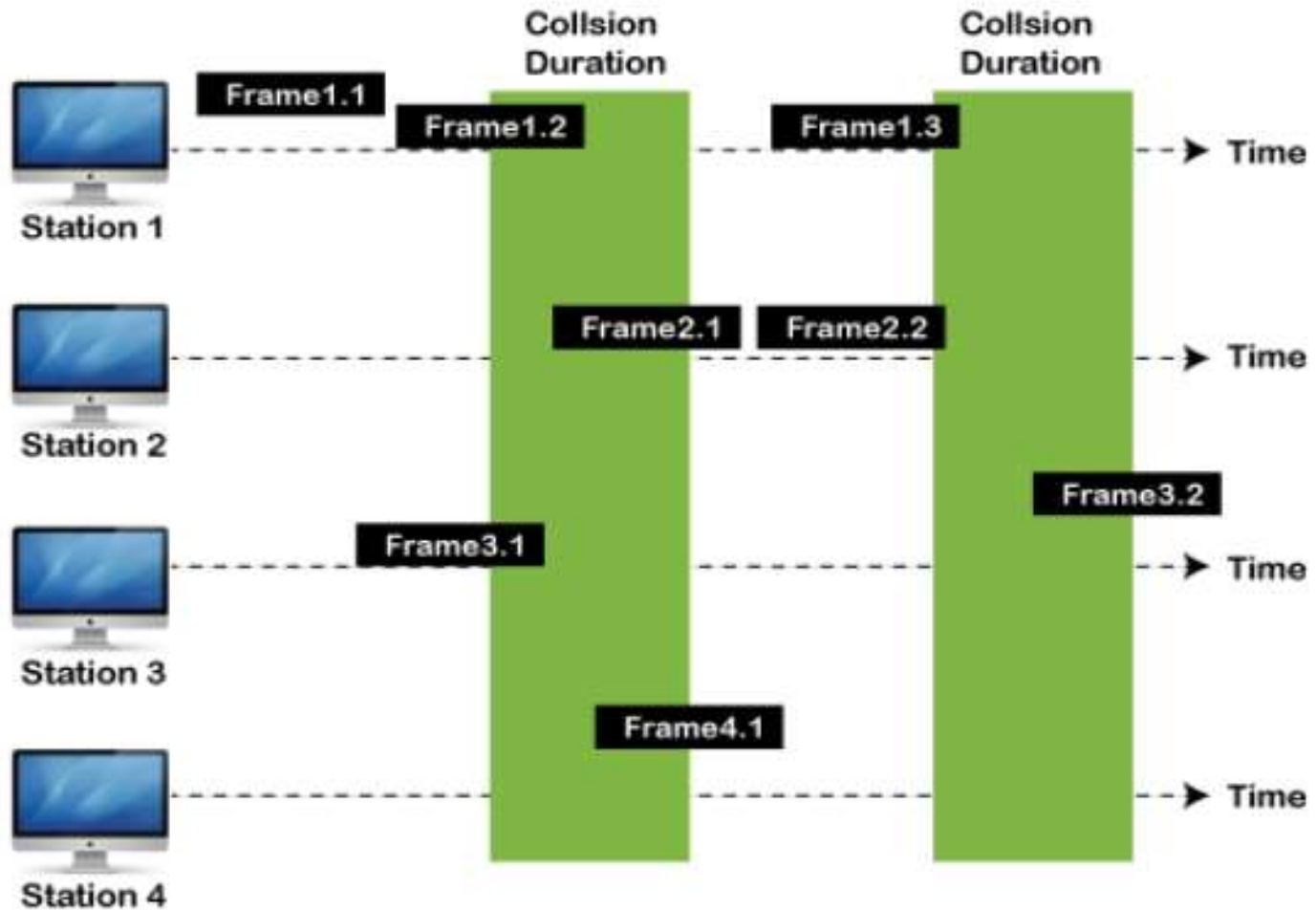
ALOHA Random Access Protocol



- **Aloha Rules**

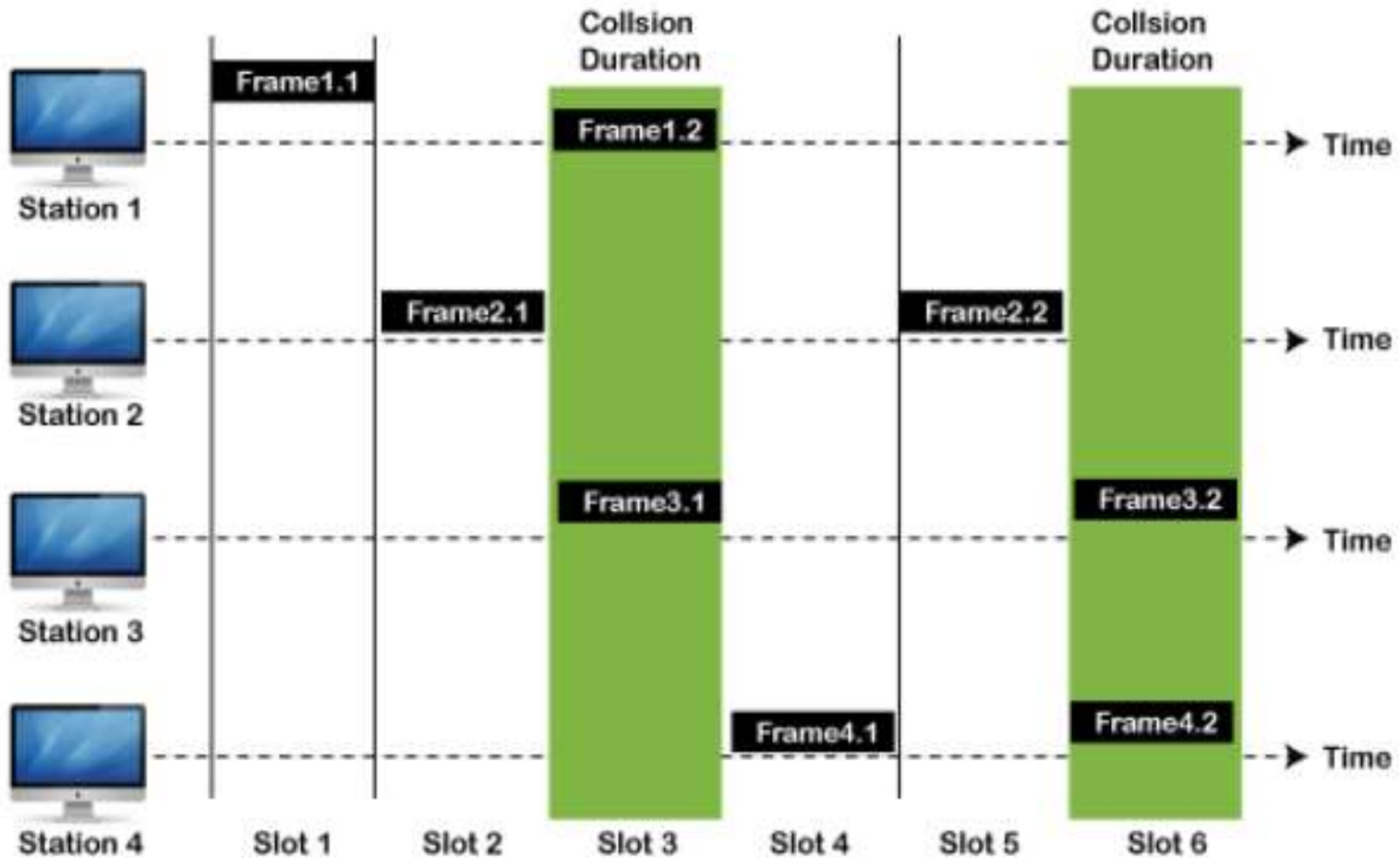
1. Any station can transmit data to a channel at any time.
2. It does not require any carrier sensing.
3. Acknowledgment of the frames exists in Aloha.
4. It requires retransmission of data after some random amount of time.

Pure Aloha



Frames in Pure ALOHA

Slotted Aloha



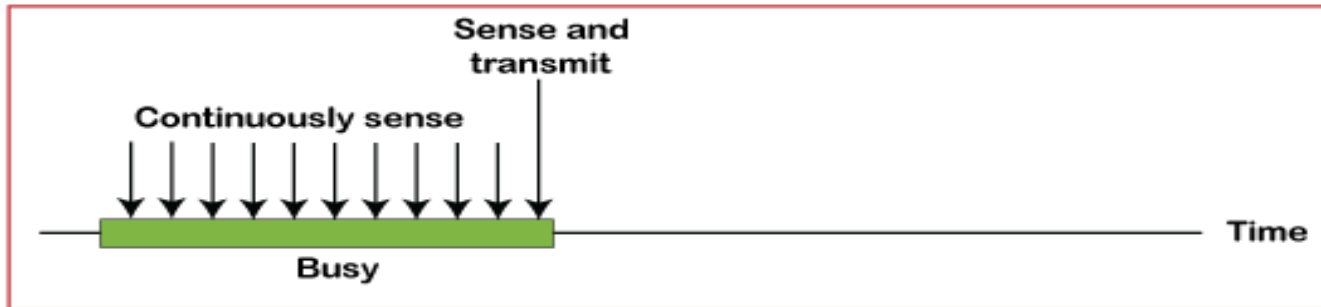
Frames in Slotted ALOHA

CSMA (Carrier Sense Multiple Access)

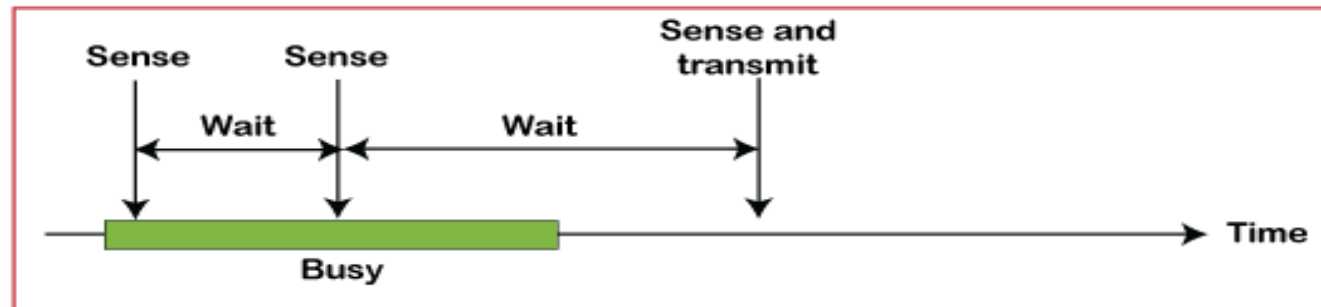


- **CSMA Access Modes:**

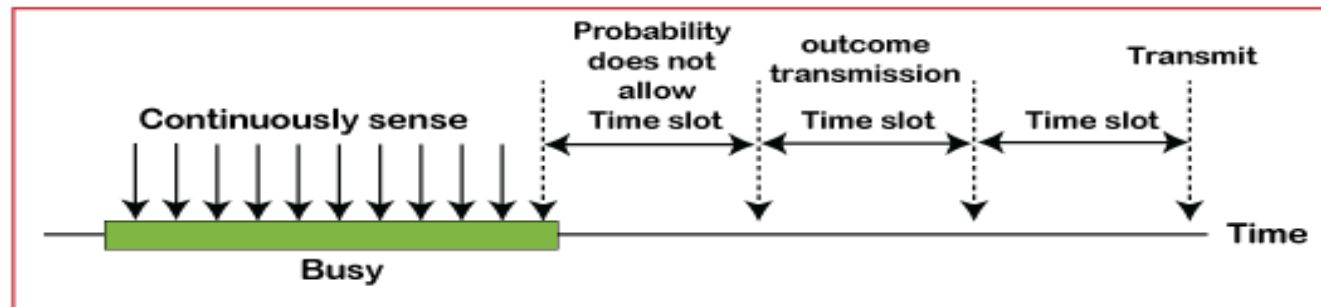
1. 1-Persistent
2. Non-Persistent
3. P-Persistent
4. O- Persistent



a. 1-persistent



b. Nonpersistent



c. p-persistent

CSMA/ CD

- It is a **carrier sense multiple access/ collision detection** network protocol to transmit data frames. The CSMA/CD protocol works with a medium access control layer.
- Therefore, it first senses the shared channel before broadcasting the frames, and if the channel is idle, it transmits a frame to check whether the transmission was successful.
- If the frame is successfully received, the station sends another frame. If any collision is detected in the CSMA/CD, the station sends a jam/ stop signal to the shared channel to terminate data transmission. After that, it waits for a random time before sending a frame to a channel.

CSMA/ CA

- It is a **carrier sense multiple access/collision avoidance** network protocol for carrier transmission of data frames. It is a protocol that works with a medium access control layer.
- When a data frame is sent to a channel, it receives an acknowledgment to check whether the channel is clear. If the station receives only a single (own) acknowledgments, that means the data frame has been successfully transmitted to the receiver.
- But if it gets two signals (its own and one more in which the collision of frames), a collision of the frame occurs in the shared channel. Detects the collision of the frame when a sender receives an acknowledgment signal.

Following are the methods used in the CSMA/ CA to avoid the collision:



- **Inter frame space:** In this method, the station waits for the channel to become idle, and if it gets the channel is idle, it does not immediately send the data. Instead of this, it waits for some time, and this time period is called the **Inter frame** space or IFS. However, the IFS time is often used to define the priority of the station.
- **Contention window:** In the Contention window, the total time is divided into different slots. When the station/ sender is ready to transmit the data frame, it chooses a random slot number of slots as **wait time**. If the channel is still busy, it does not restart the entire process, except that it restarts the timer only to send data packets when the channel is inactive.
- **Acknowledgment:** In the acknowledgment method, the sender station sends the data frame to the shared channel if the acknowledgment is not received ahead of time.

MODULE –III

Network Layer

The main functions performed by the network layer are:



1. Routing
2. Logical Addressing
3. Internetworking
4. Fragmentation and Reassembly
5. Error Handling
6. Congestion Control
7. Encapsulation and Decapsulation

Network Layer Design Issues

- Store – and – Forward Packet Switching
- Services to Transport Layer
- Providing Connection Oriented Service
- Providing Connectionless Service

Routing

- Routing is a process of selecting path along which the data can be transferred from source to the destination.
- The routing algorithms are used for routing the packets. The routing algorithm is nothing but a software responsible for deciding the optimal path through which packet can be transmitted.

Routing Metrics and Costs

- **Hop count**
- **Delay**
- **Bandwidth**
- **Load**
- **Reliability**

Static and Dynamic Routing

- Static route is the route that the network administrator manually enters into the routing table.
- Here, we don't use any routing protocol

Drawbacks of Static Routing:

- It requires 24/7 support
- It is a time consuming process

Dynamic Routing

- Dynamic Routing uses routing protocols for creating a route for the data packets.
- Here, the router automatically collect and store dynamic route in the routing table.
- It minimizes the work pressure of network administrator.
- The user no need to wait for long time

Distance vector routing

It is a dynamic routing algorithm in which each router computes a distance between itself and each possible destination i.e. its immediate neighbors.

Link state routing

- **Reliable Flooding**
- **Initial state:** Each node knows the cost of its neighbors.
- **Final state:** Each node knows the entire graph.

Congestion Control

- Too many packets present in (a part of) the network causes packet delay and loss that degrades performance. This situation is called **congestion**.
- A state occurring in network layer when the message traffic is so heavy that it slows down network response time.
- There are two congestion control algorithm which are as follows:
- **Leaky Bucket Algorithm**
- **Token bucket Algorithm**

Leaky Bucket Algorithm

Figure 30.4 *Leaky bucket*

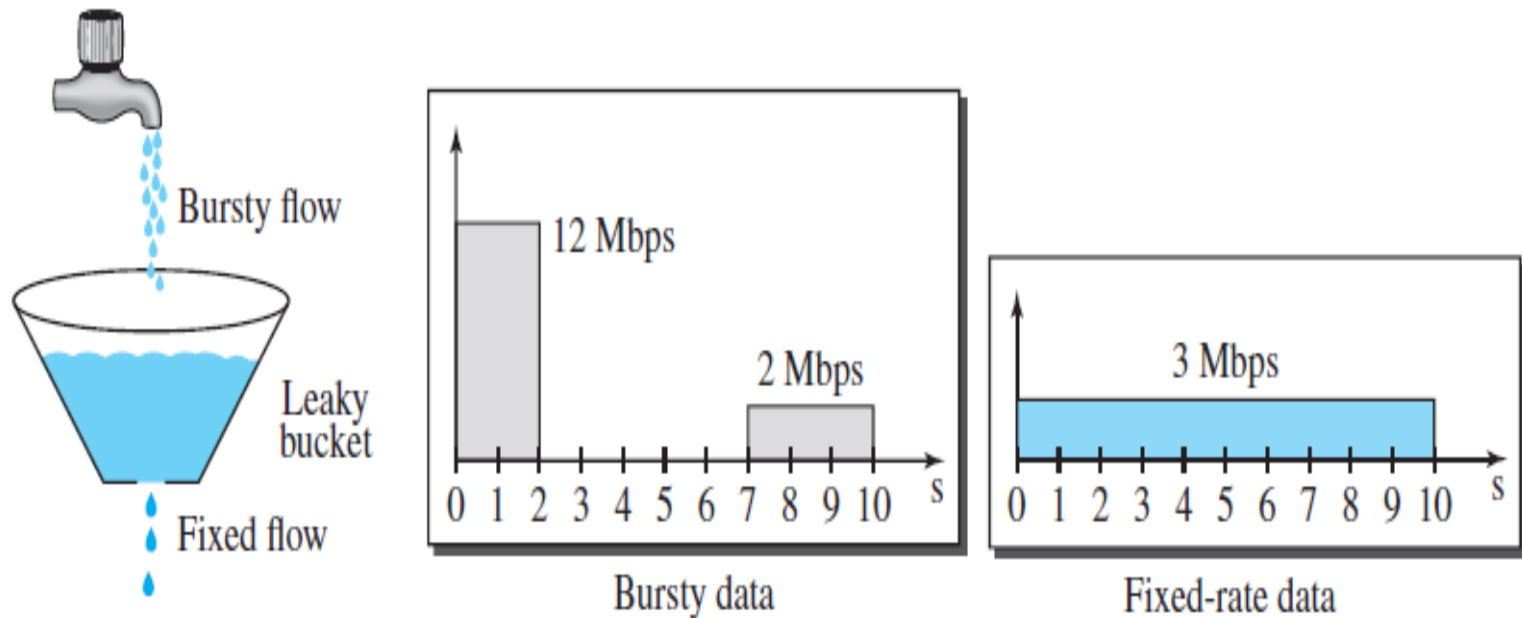
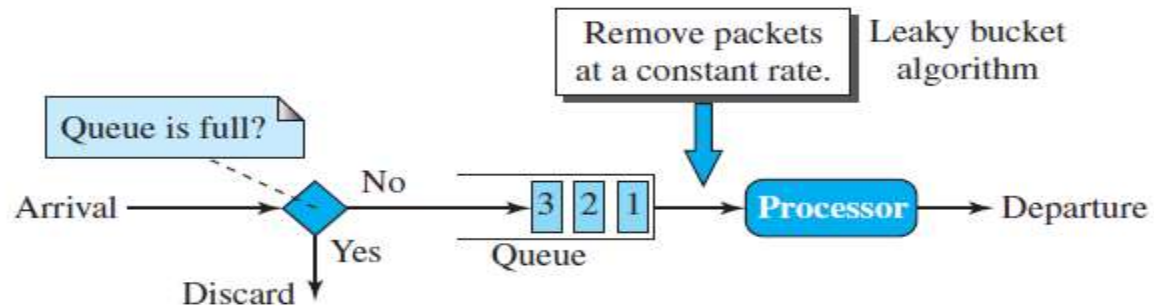


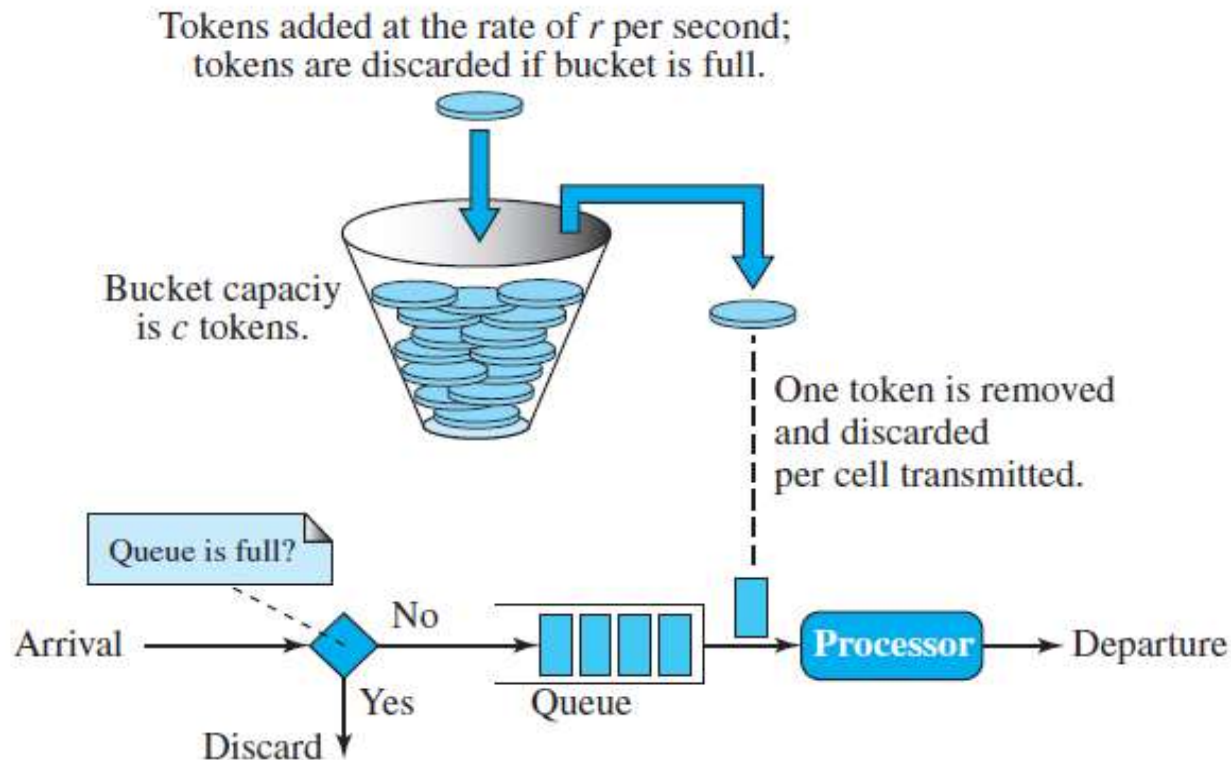
Figure 30.5 *Leaky bucket implementation*



A leaky bucket algorithm shapes bursty traffic into fixed-rate traffic by averaging the data rate. It may drop the packets if the bucket is full.

Token Bucket

Figure 30.6 *Token bucket*



The token bucket allows bursty traffic at a regulated maximum rate.

Quality of service

- **Quality of service** is an internetworking issue that can be defined as flow that is required for communication.
- **Quality of service** is an internetworking issue that refers to a set of techniques and mechanisms that guarantee the performance of the network to deliver predictable services to an application program.
- **Flow characteristics:**
 - Reliability
 - Delay
 - Jitter
 - Bandwidth

IPV4 ADDRESSES

- The identifier used in the IP layer of the TCP/IP protocol suite to identify the connection of each device to the Internet is called the Internet address or IP address
- An IPv4 address is a 32-bit address that uniquely and universally defines the connection of a host or a router to the Internet.

IPV4

0	4	8	16	19	24	31
Version	IHL	Type of service	Total length			
Identification			Flags	Fragment offset		
Time to live		Protocol	Header checksum			
Source IP address						
Destination IP address						
Options					Padding	

FIGURE 8.4 IP version 4 header.

Figure 18.16 *Three different notations in IPv4 addressing*

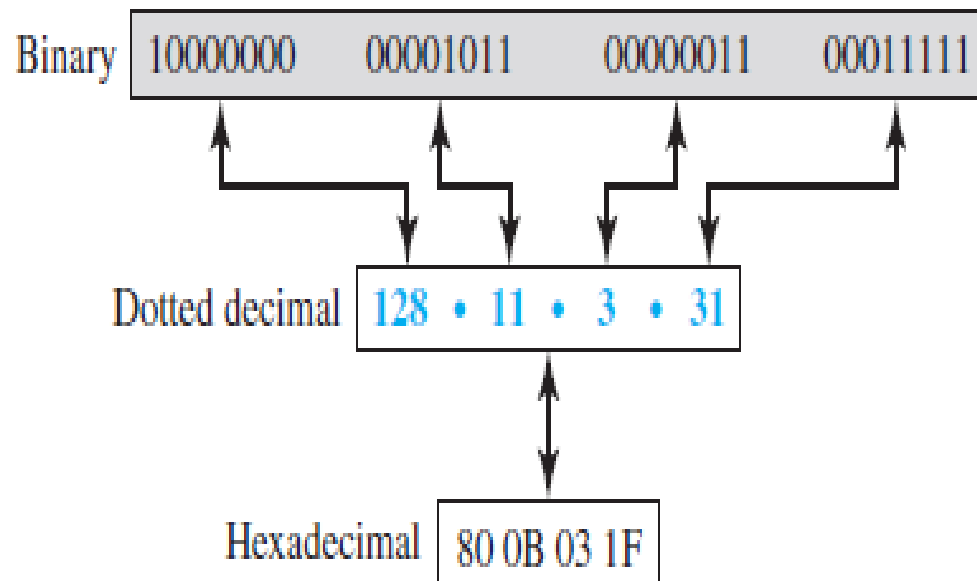


Figure 18.17 *Hierarchy in addressing*

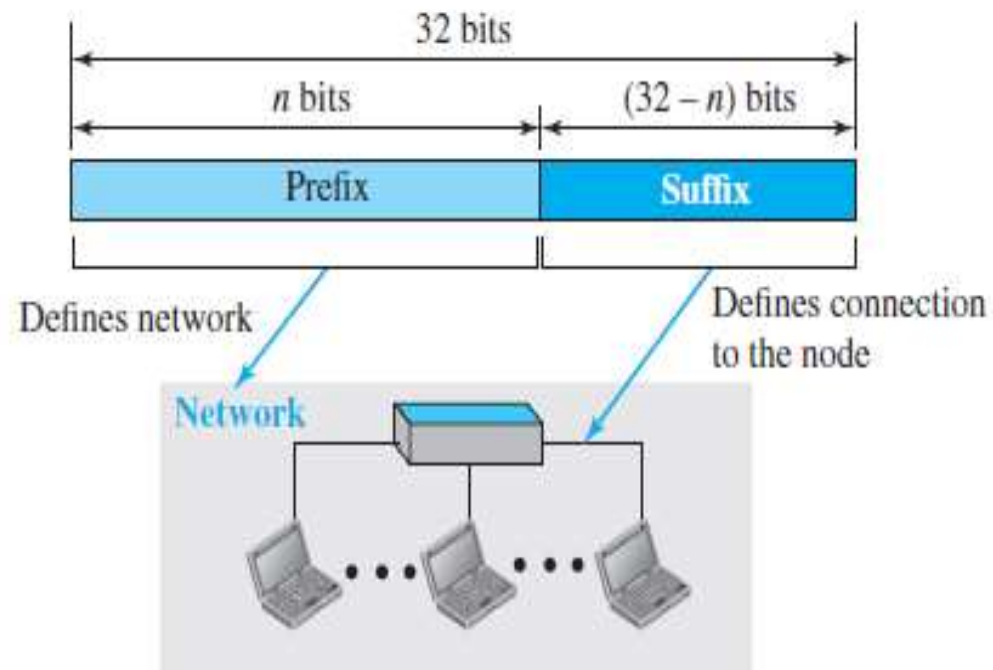
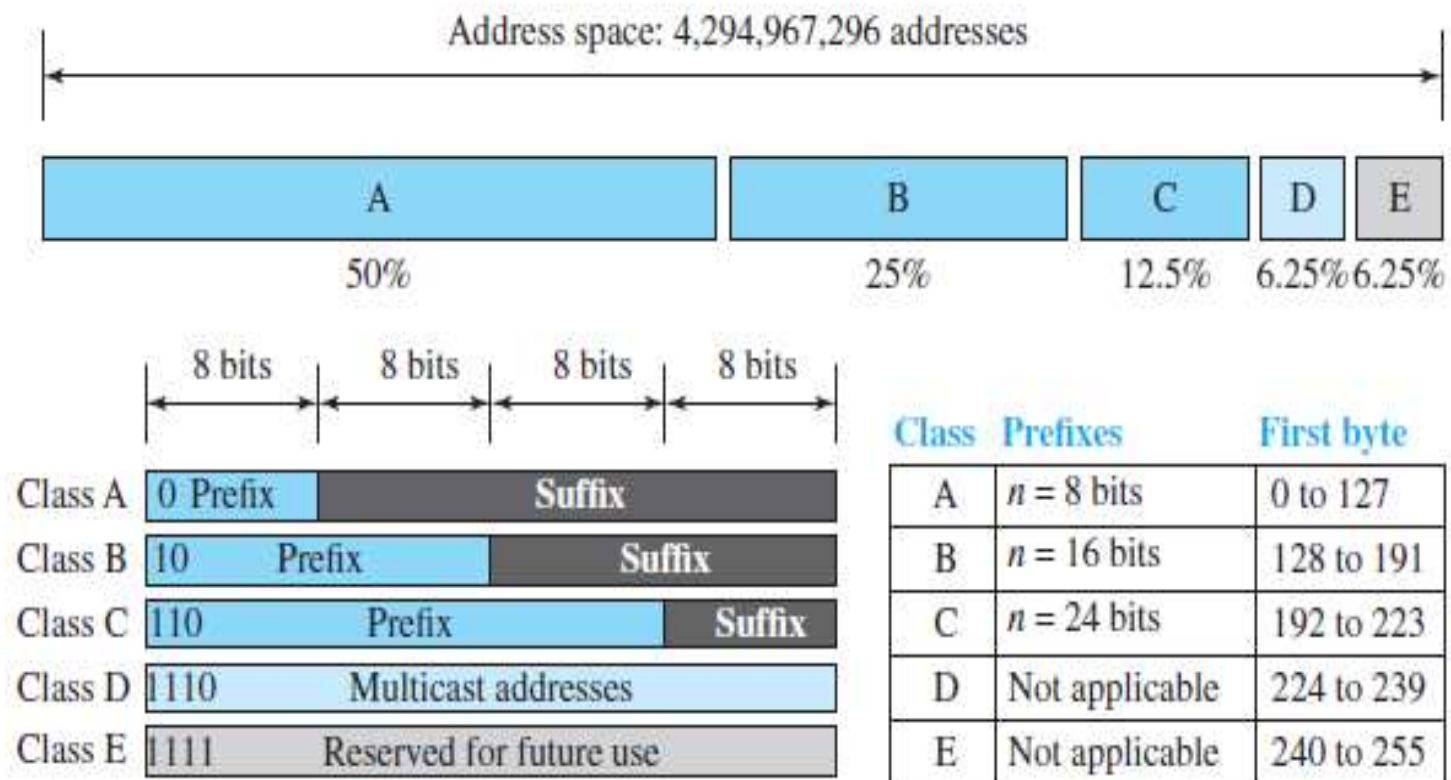


Figure 18.18 Occupation of the address space in classful addressing



IPv6 Header Format

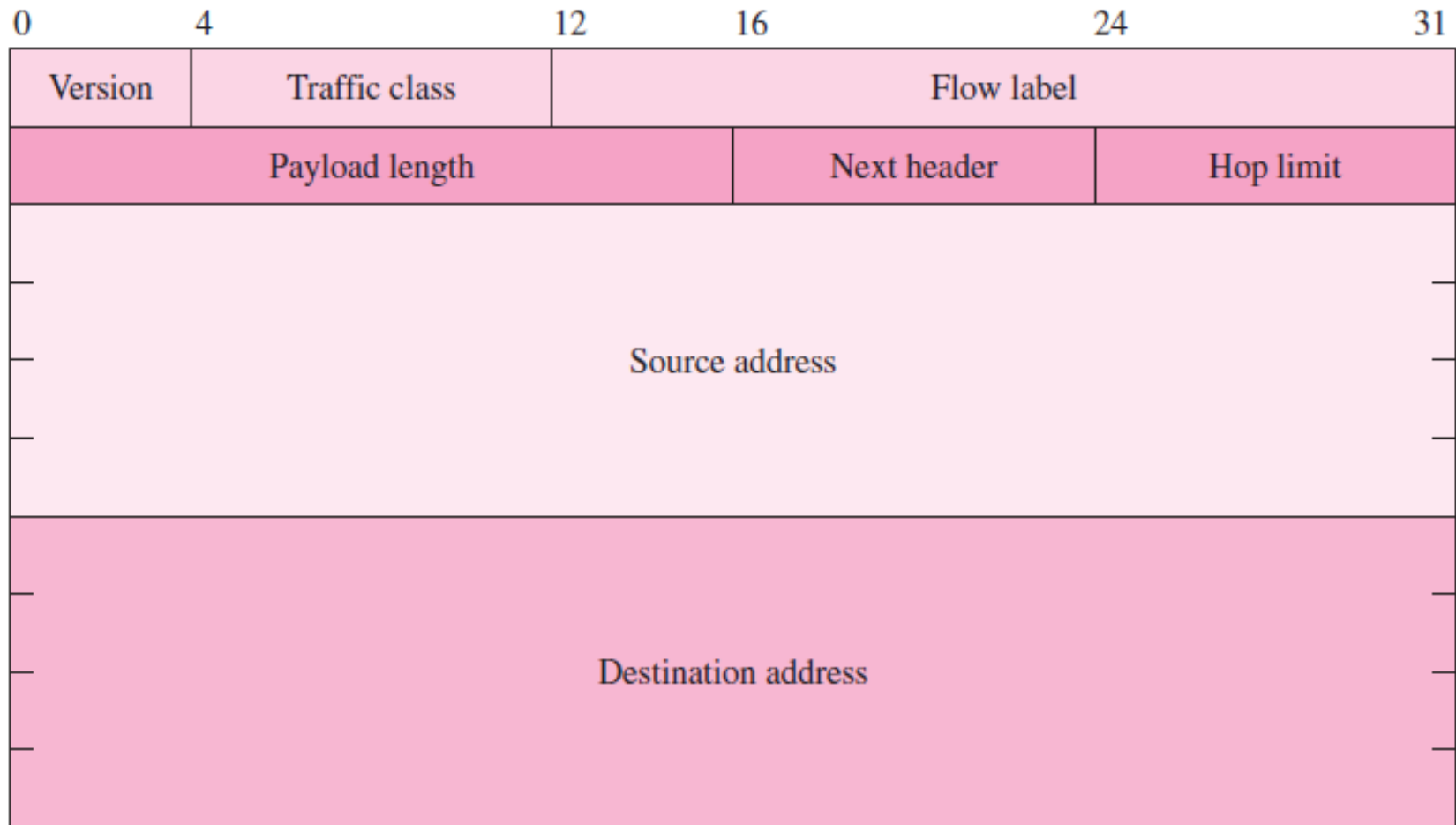


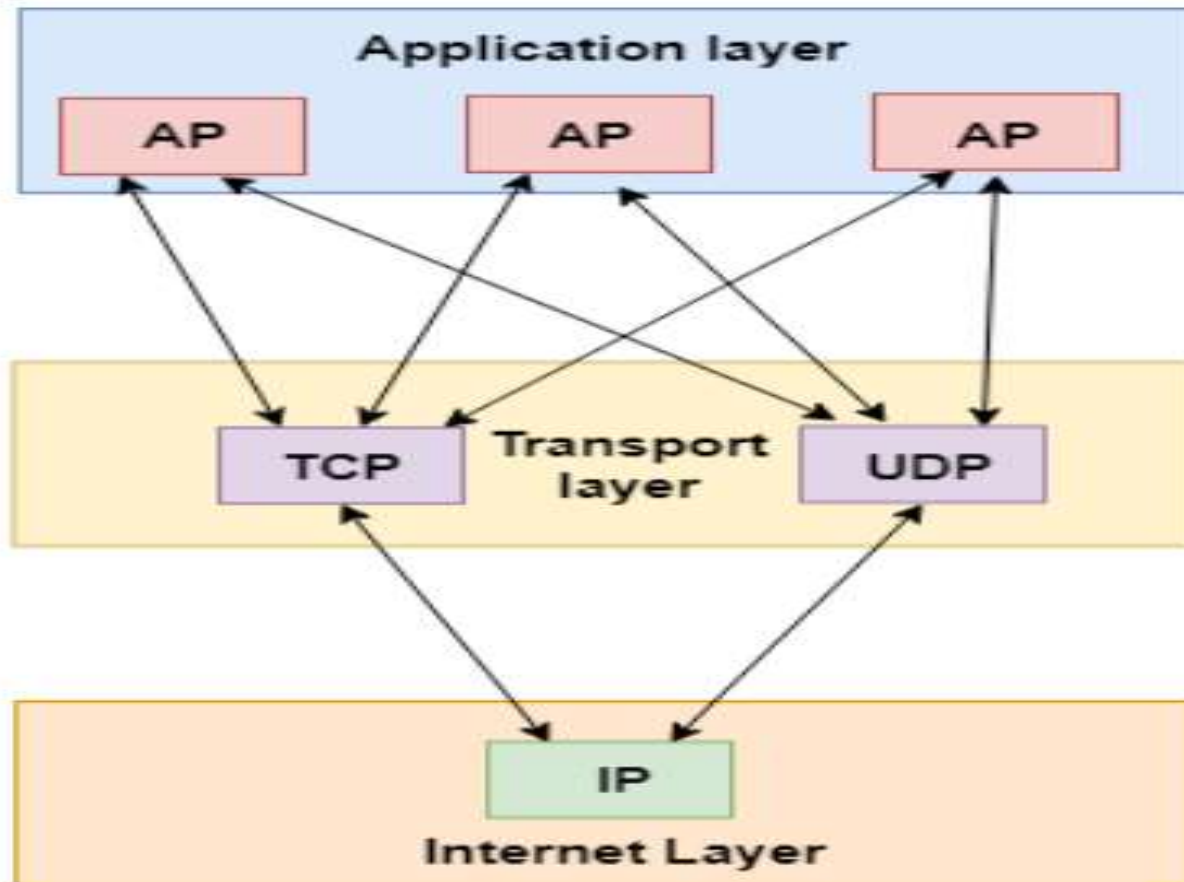
FIGURE 8.16 IPv6 basic header.

Network Addressing

- **Unicast**
- **Multicast**
- **Anycast**
- EX: 4BF5:AA12:0216:FEBC:BA5F:039A:BE9A:2176
- 4BF5:0000:0000:0000:BA5F:039A:000A:2176
- 4BF5:0:0:0:BA5F:39A:A:2176
- 4BF5::BA5F:39A:A:2176

MODULE –IV

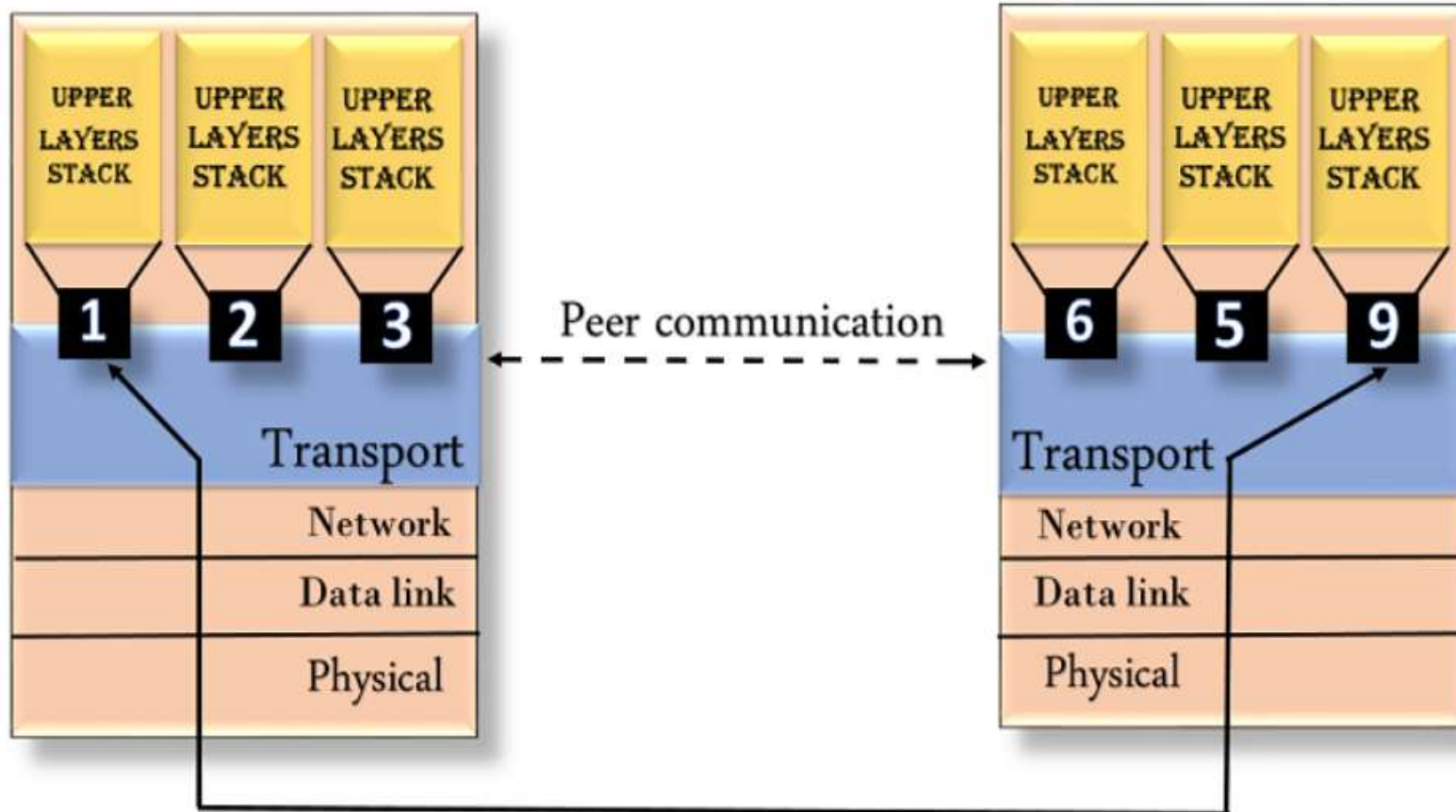
TRANSPORT LAYER



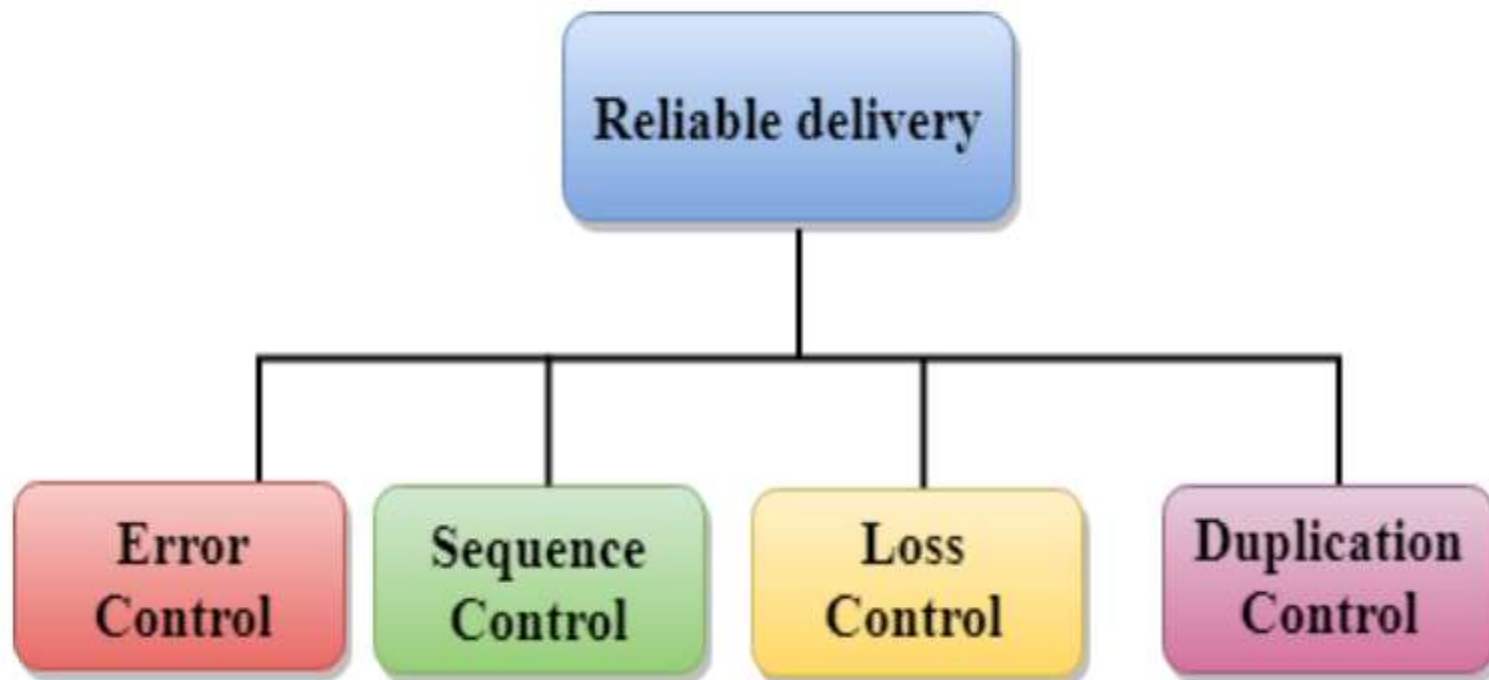
Transport Layer services

- End-to-end delivery
- Addressing
- Reliable delivery
- Flow control
- Multiplexing

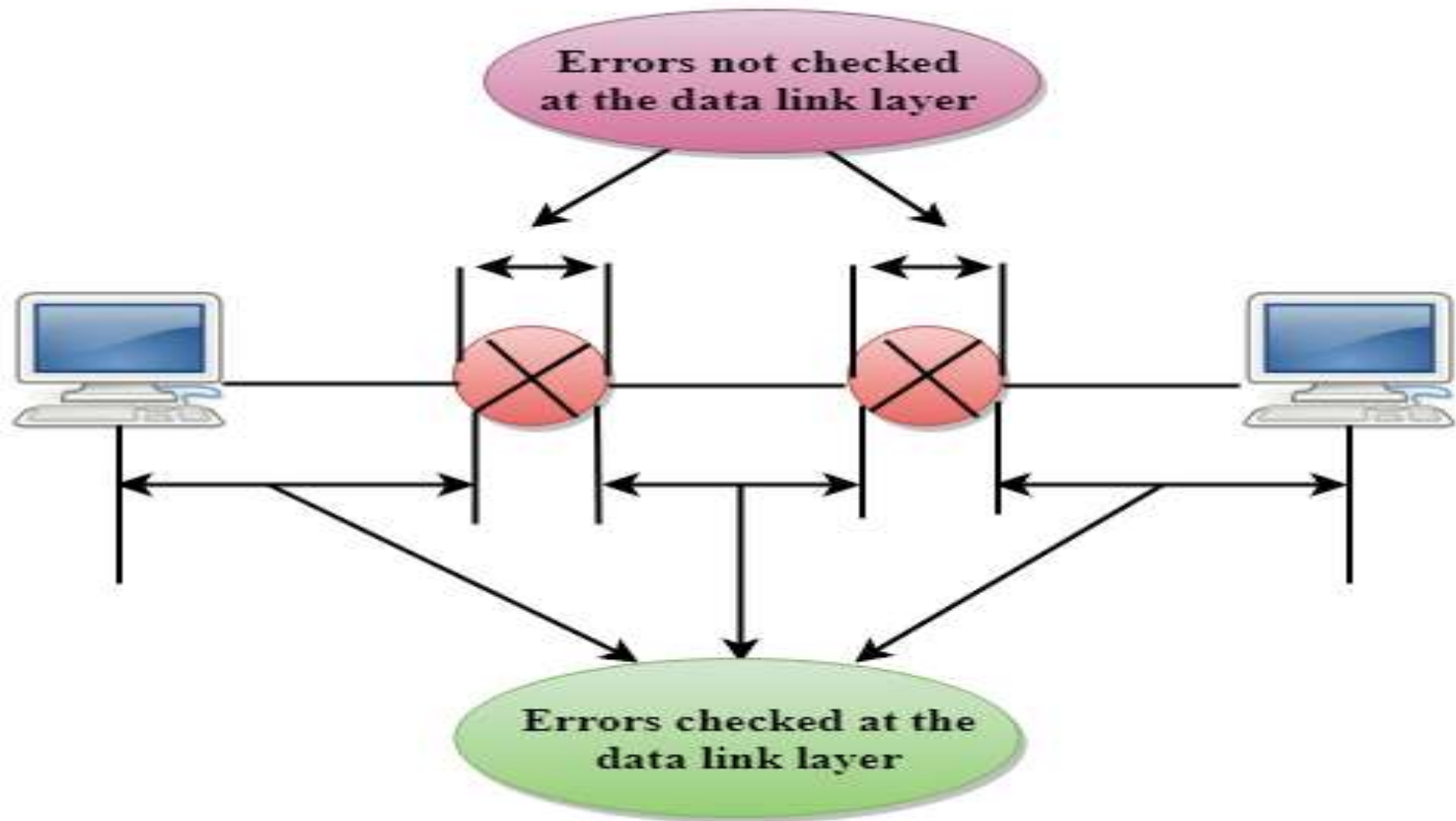
Addressing



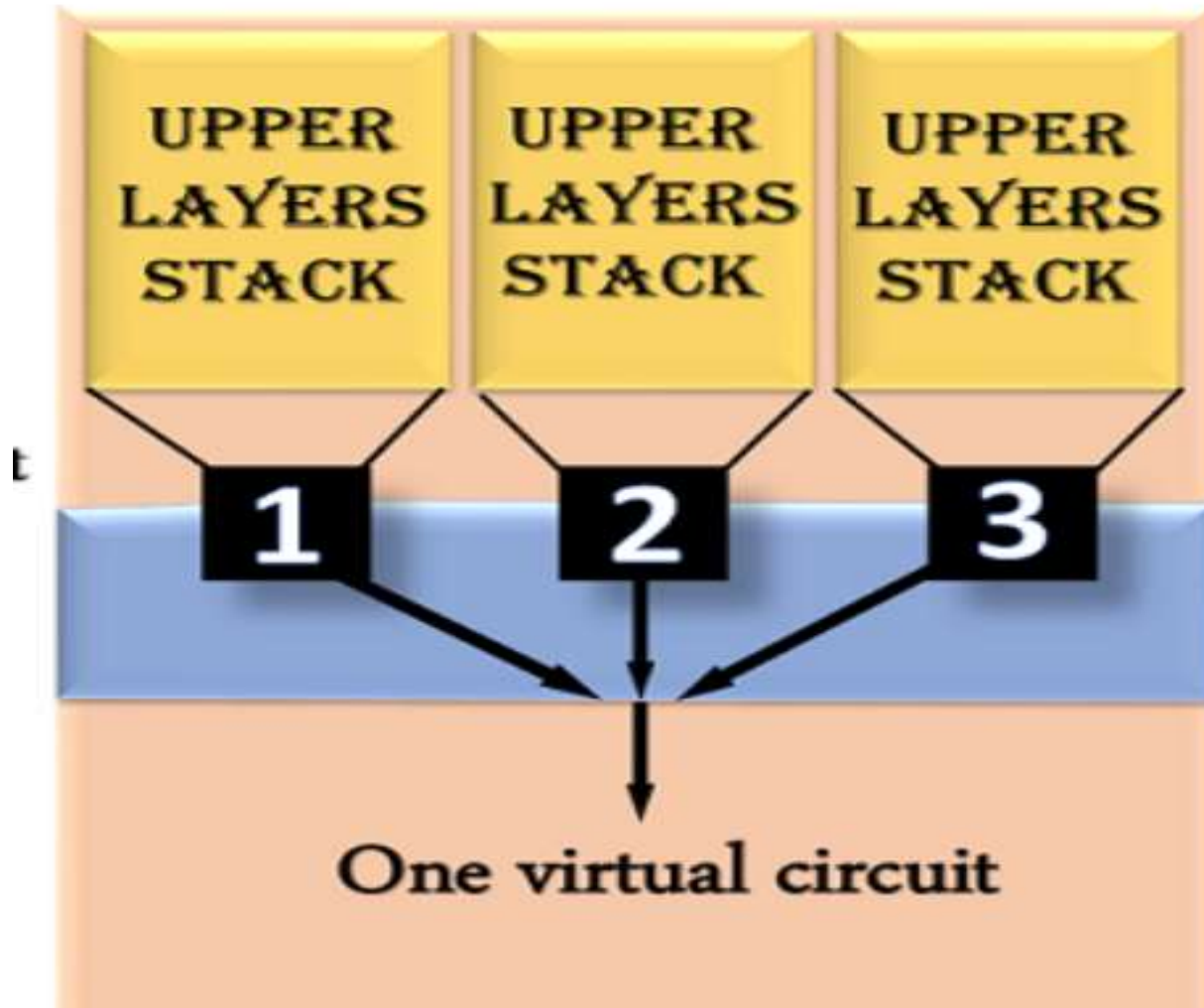
Reliable delivery



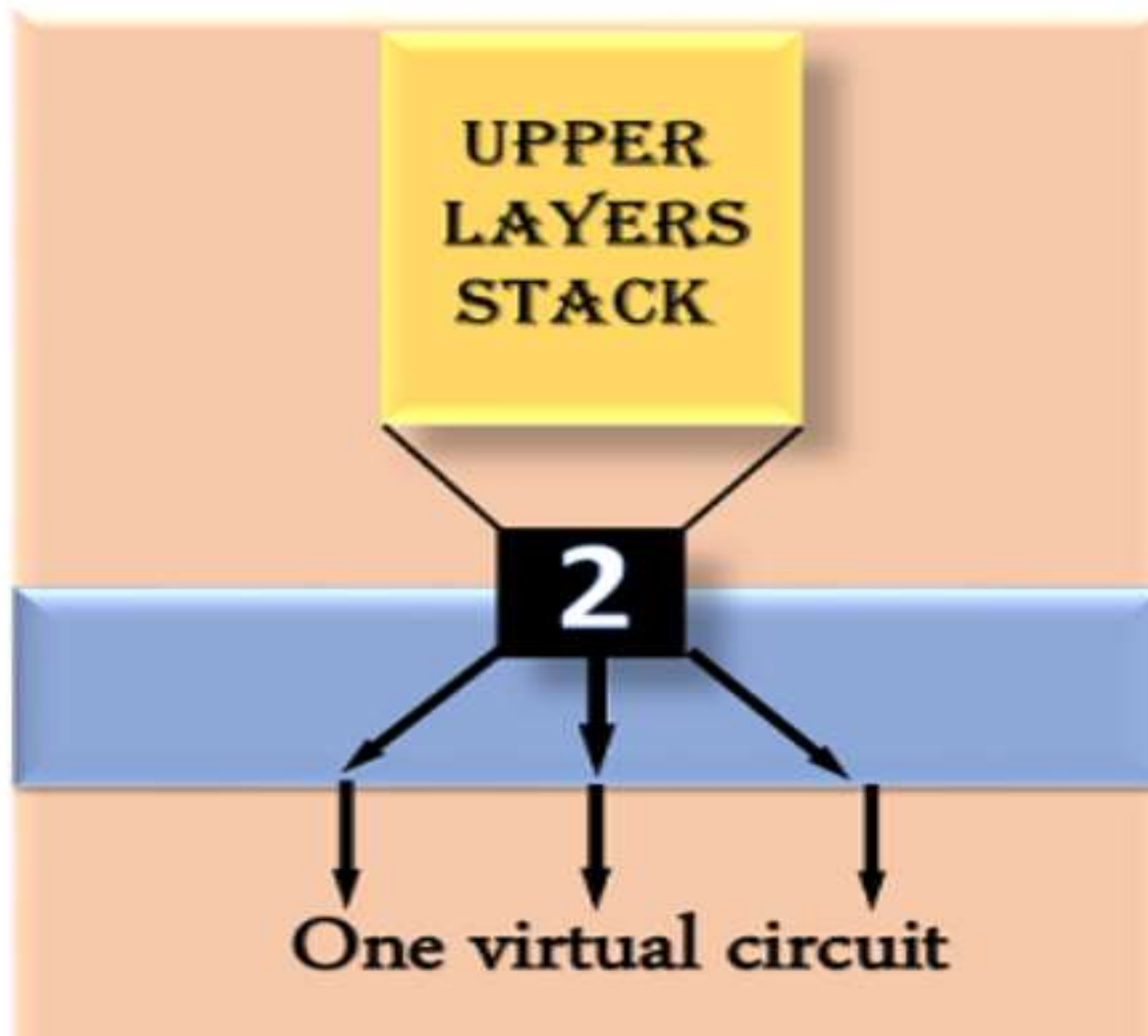
Reliable delivery



Upward multiplexing



Downward multiplexing

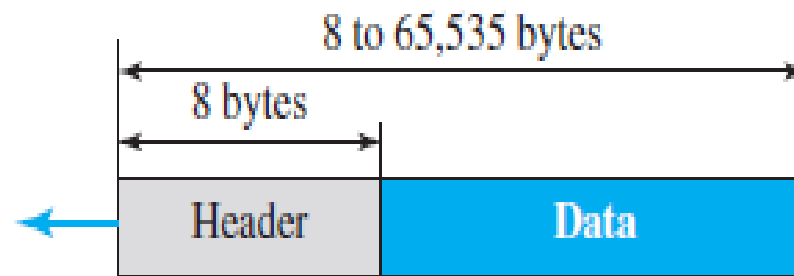


The internet transport protocols

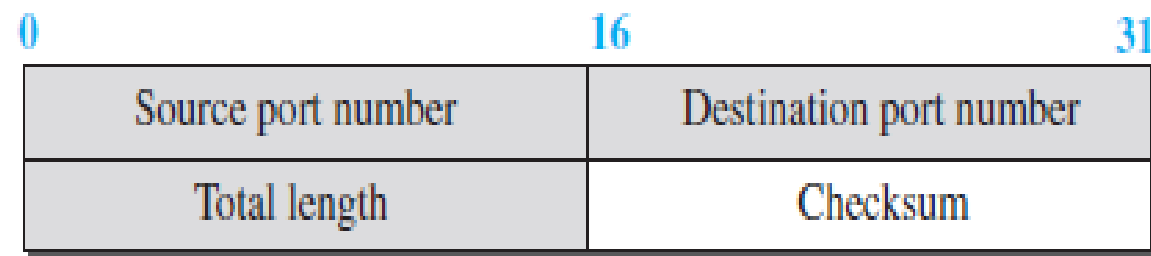


- **UDP (User Datagram Protocol)**
- UDP packets, called **user datagrams**, have a **fixed-size header of 8 bytes made of four fields, each of 2 bytes (16 bits).**

Figure 24.2 *User datagram packet format*



a. UDP user datagram

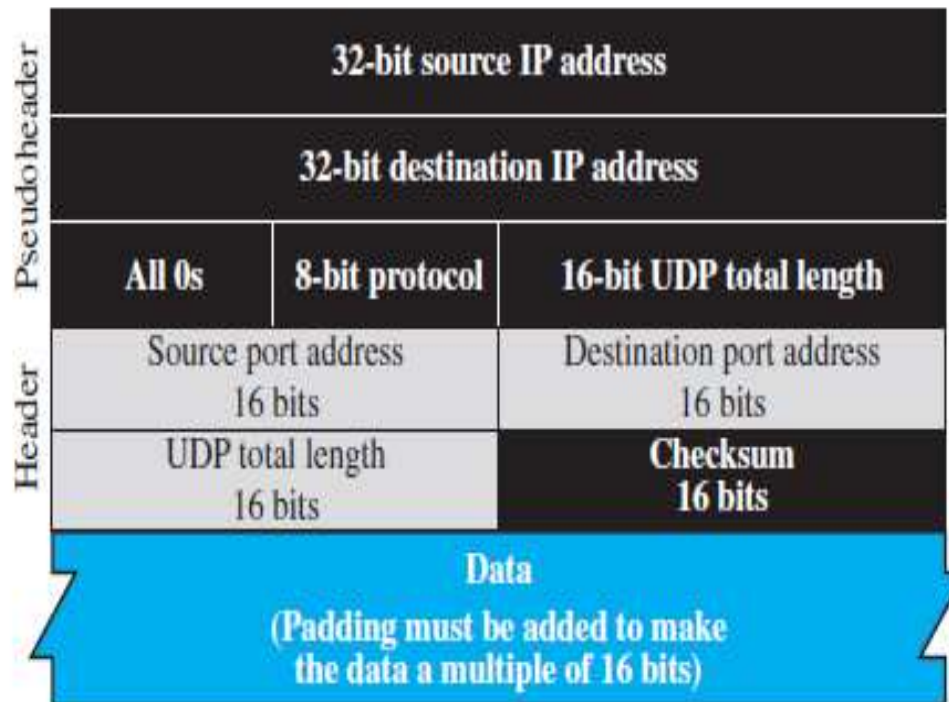


b. Header format

UDP Services

- **Process-to-Process Communication**
- **Connectionless Services**
- **Flow Control**
- **Error Control**
- **Checksum**
- **Congestion Control**
- **Encapsulation and Decapsulation**
- **Queuing**
- **Multiplexing and Demultiplexing**

Figure 24.3 *Pseudoheader for checksum calculation*



Advantages of UDP

1. With UDP, broadcast and multicast transmission is possible.
2. UDP uses the bandwidth efficiently, as there is a small packet overhead.
3. As there is no need for connection establishment, hence UDP is very fast.
4. There is no buffering and numbering of packets.
5. There is no congestion control so it is used for real-time applications.

Disadvantages of UDP

1. There is a lack of guaranteed delivery.
2. There is no flow control.
3. There is no congestion control mechanism.

- **Transmission Control Protocol (TCP) is a connection-oriented, reliable protocol.**
- TCP explicitly defines connection establishment, data transfer, and connection teardown phases to provide a connection-oriented service.

TCP Services

- Process-to-Process Communication
- Stream Delivery Service
- Full-Duplex Communication
- Multiplexing and Demultiplexing
- Connection-Oriented Service
- Reliable Service

Figure 24.4 *Stream delivery*

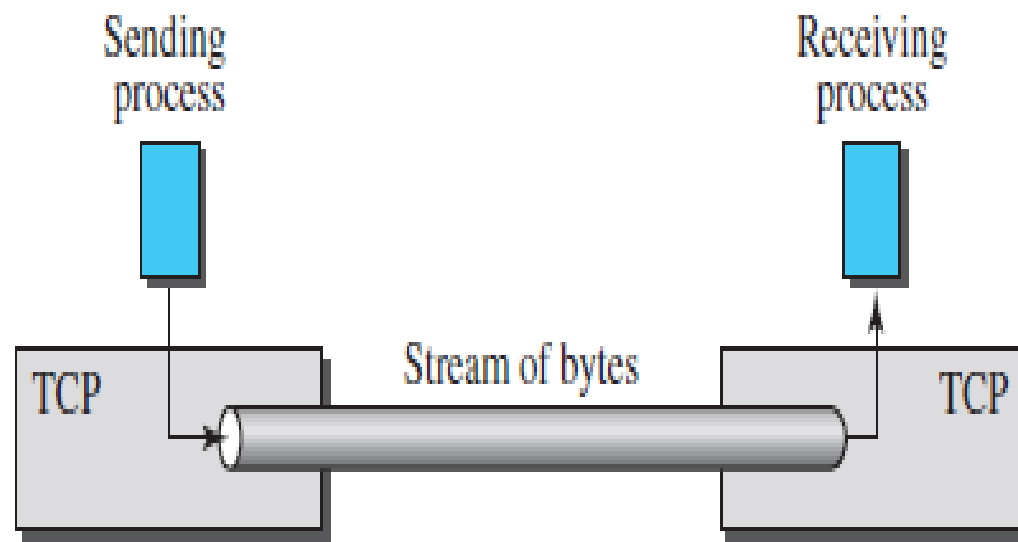
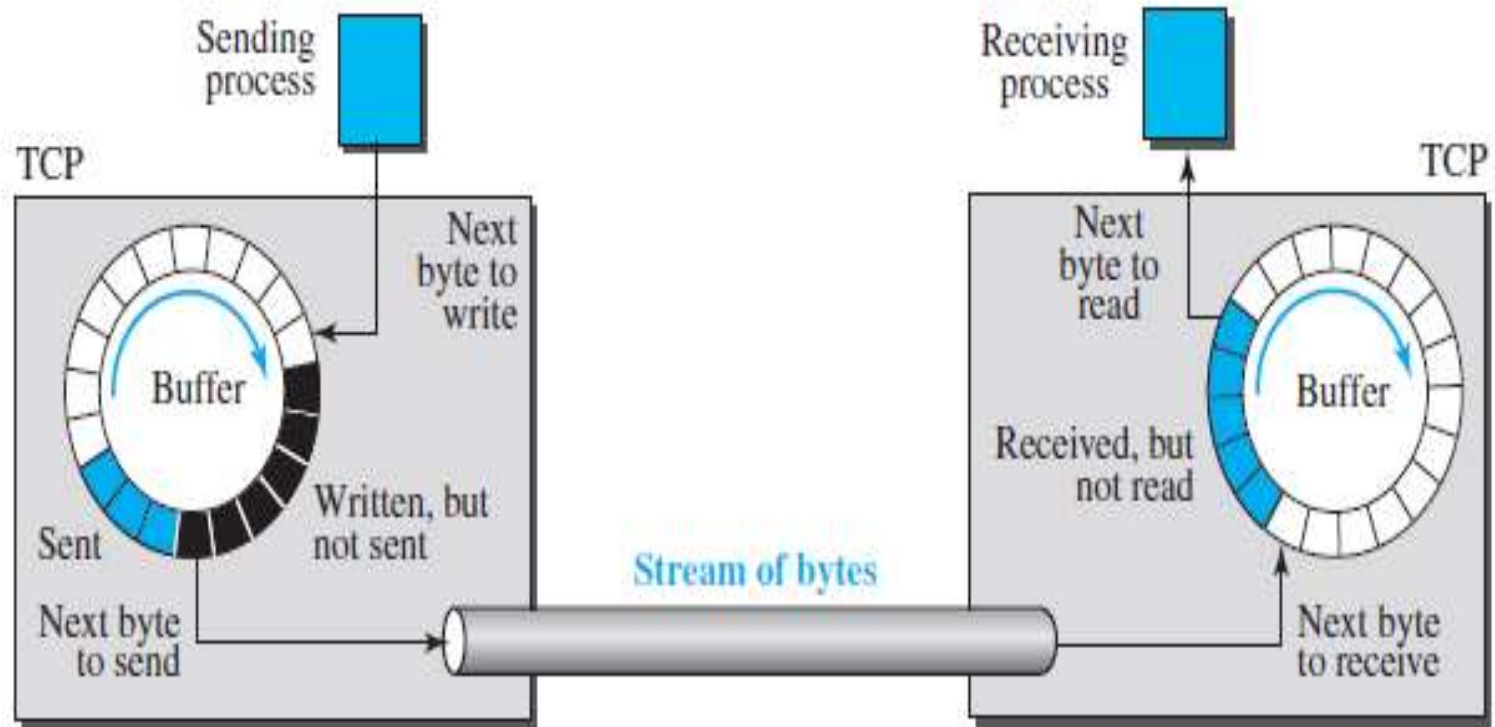


Figure 24.5 *Sending and receiving buffers*

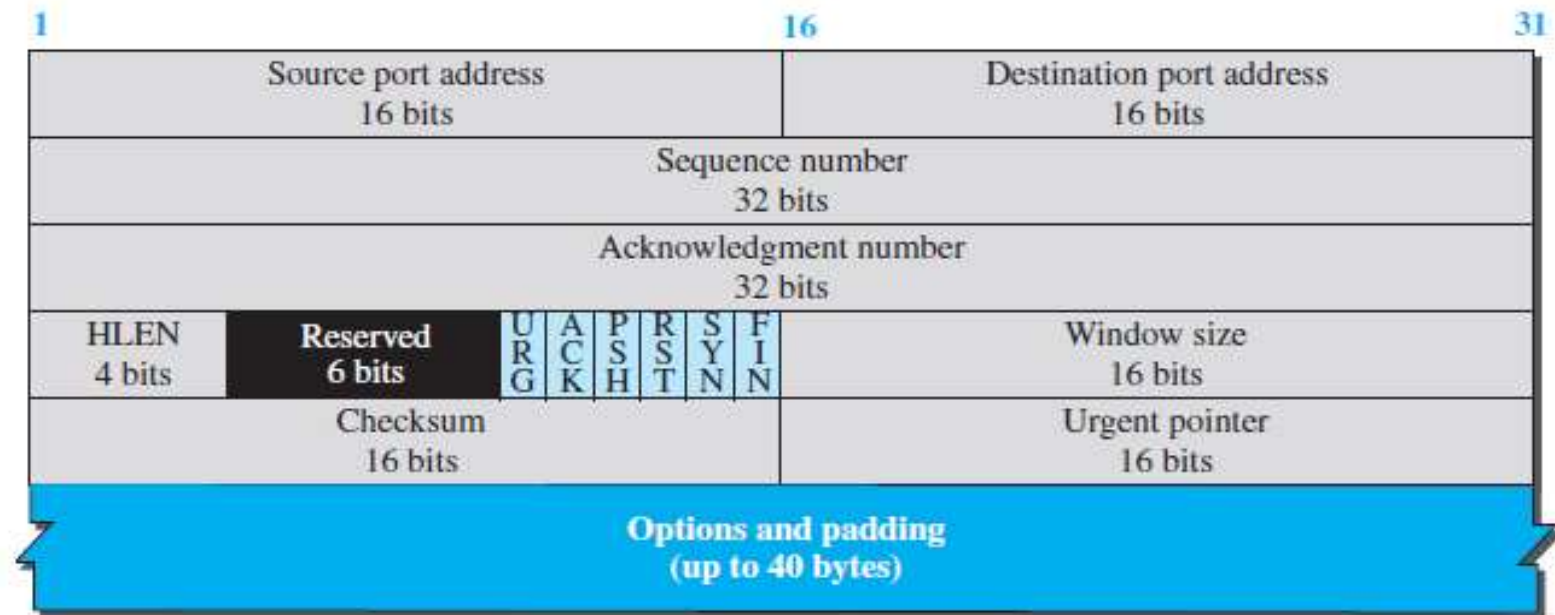


TCP segment format

Figure 24.7 TCP segment format

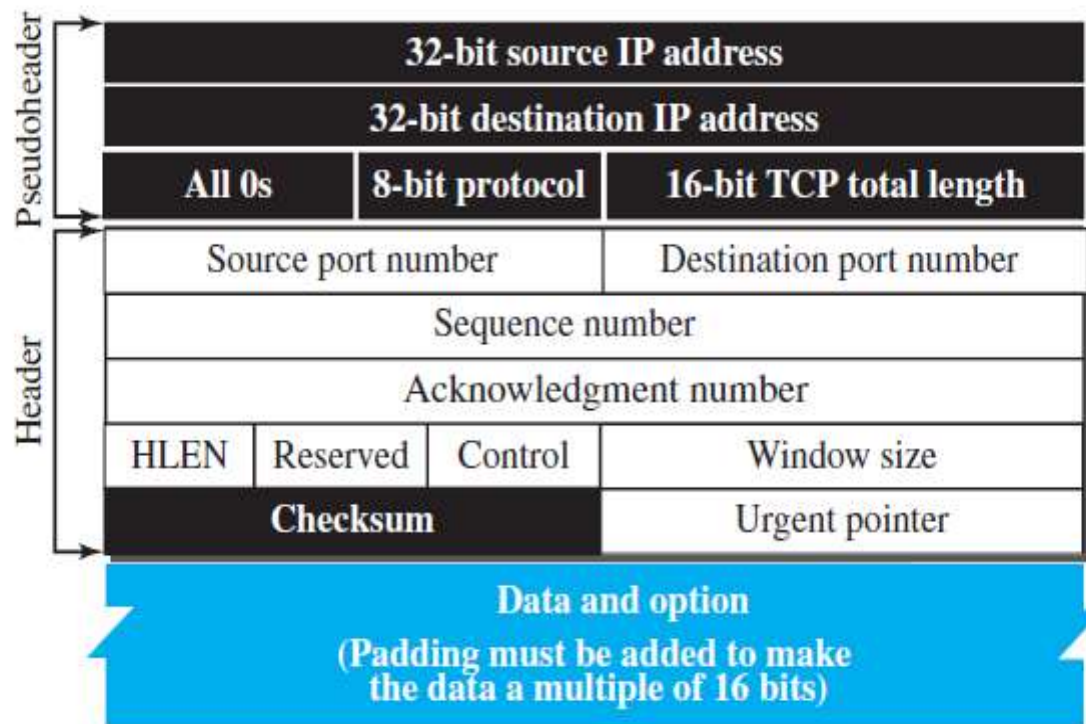


a. Segment



b. Header

Figure 24.9 *Pseudoheader added to the TCP datagram*



Three-Way Handshaking

- Handshake refers to the process to establish connection between the client and server.
- The reliable communication in TCP is termed as **PAR** (Positive Acknowledgement Re-transmission)
- A 3-way handshake is commonly known as SYN-SYN-ACK and requires both the client and server response to exchange the data.

Client

Server

sends SYN

receives
SYN+ACK

sends ACK

receives SYN

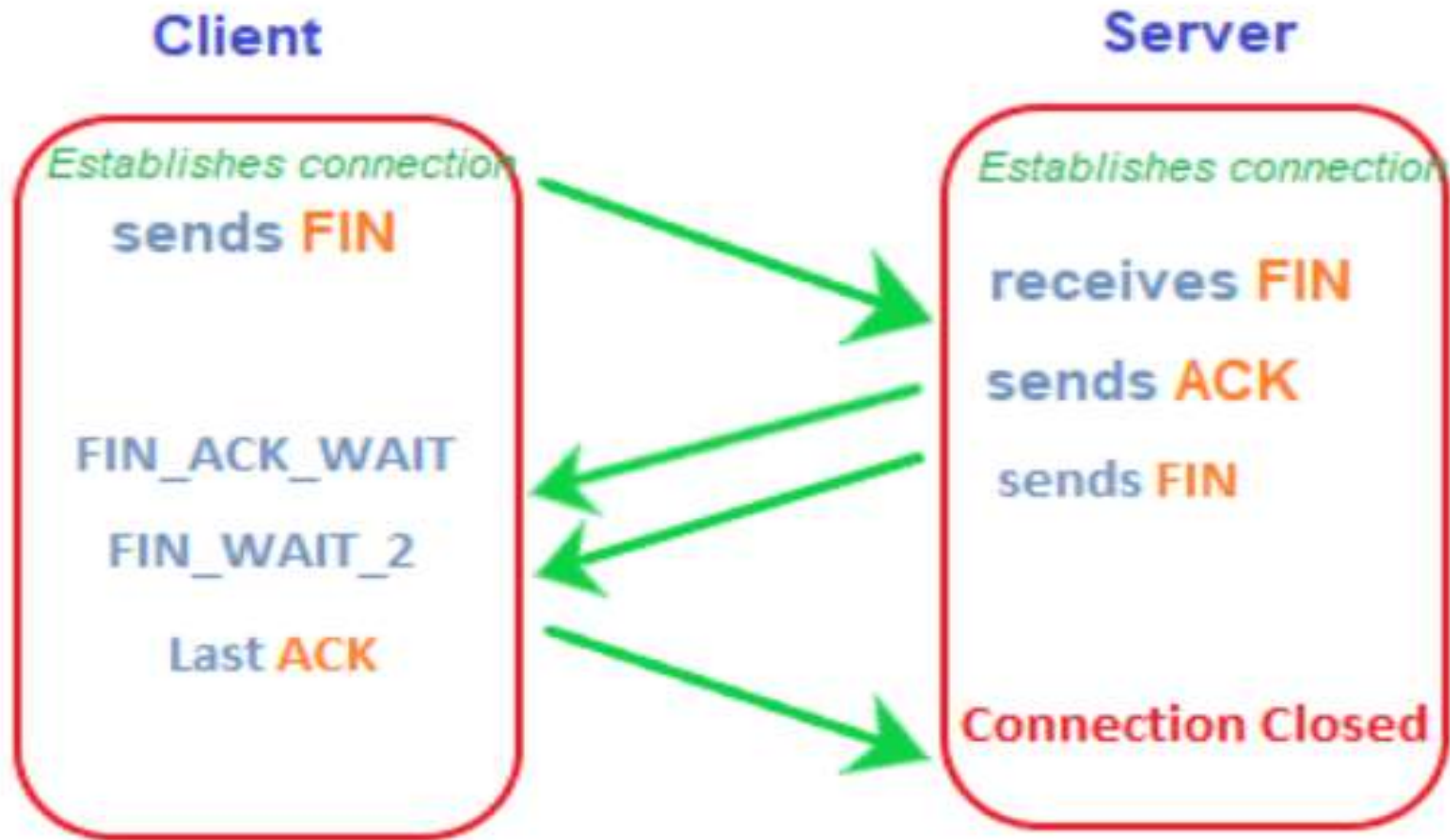
sends SYN +ACK

receives ACK



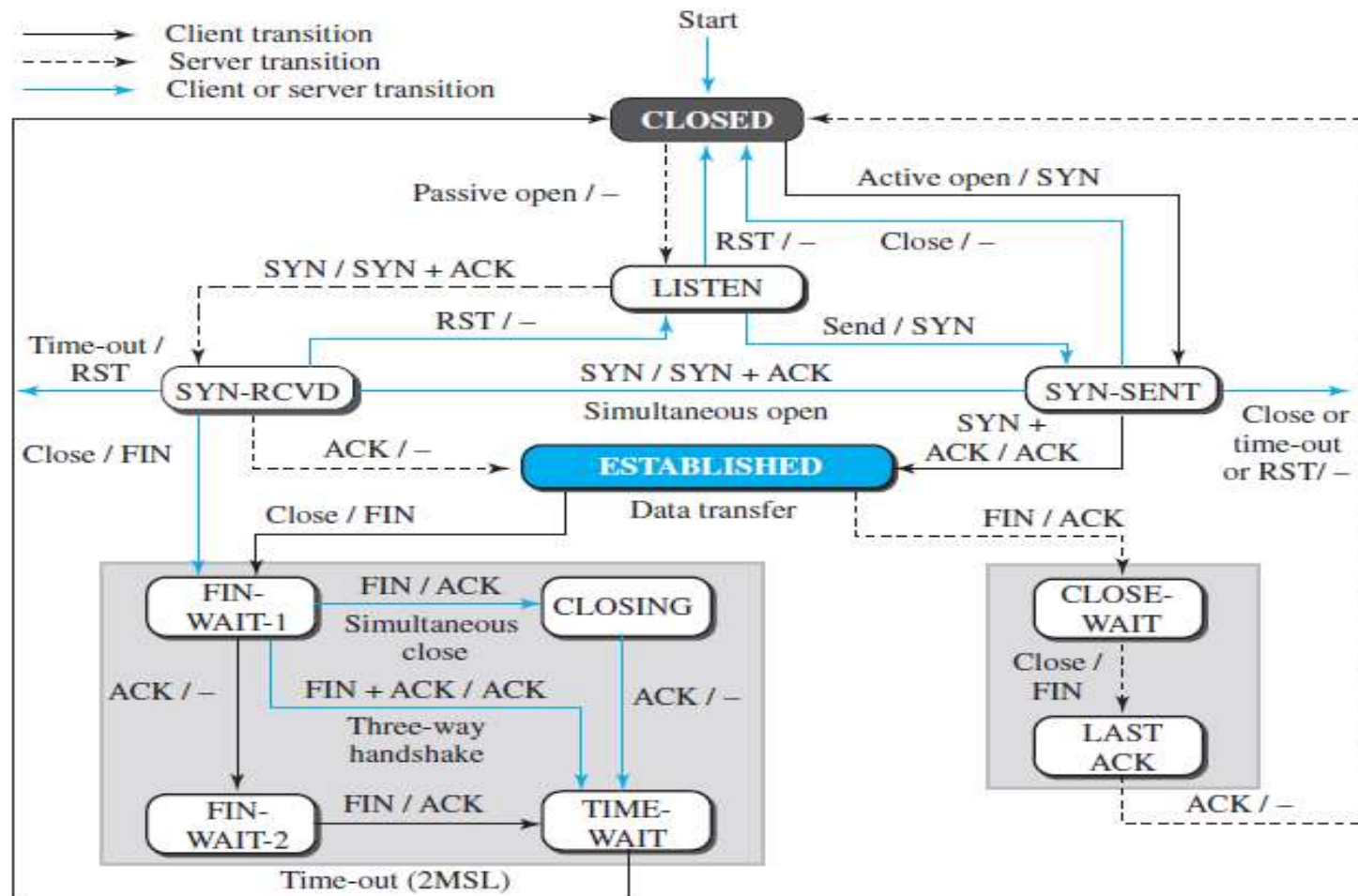
- TCP requires 3-way handshake to establish a connection between the client and server before sending the data. Similarly, to terminate or stop the data transmission, it requires a 4-way handshake.
- The segments required for TCP termination are similar to the segments to build a TCP connection (ACK and SYN) except the FIN segment

TCP Termination(4-way handshake)



State Transition Diagram

Figure 24.14 State transition diagram

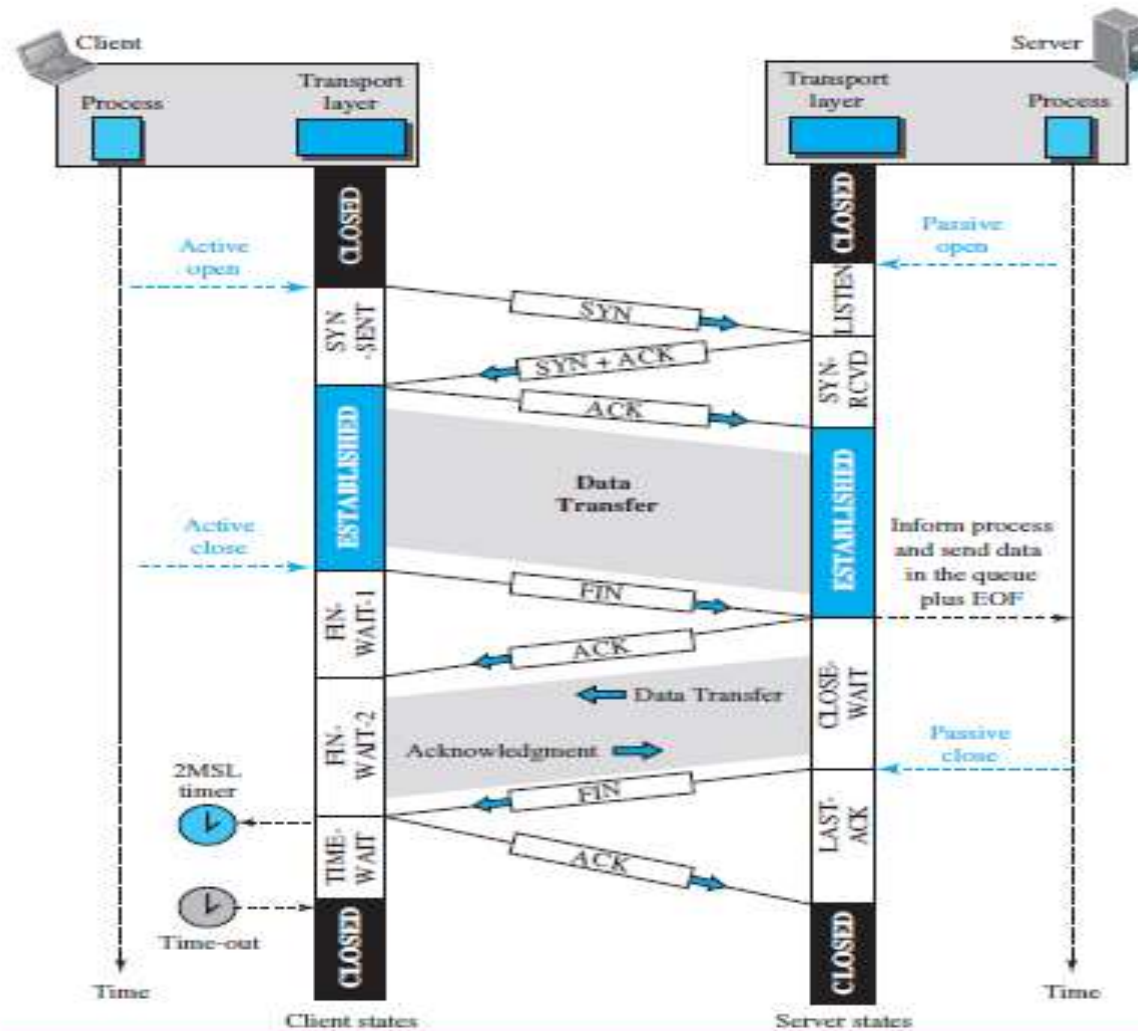


The state marked *ESTABLISHED* in the FSM is in fact two different sets of states that the client and server undergo to transfer data.

Table 24.2 *States for TCP*

<i>State</i>	<i>Description</i>
CLOSED	No connection exists
LISTEN	Passive open received; waiting for SYN
SYN-SENT	SYN sent; waiting for ACK
SYN-RCVD	SYN + ACK sent; waiting for ACK
ESTABLISHED	Connection established; data transfer in progress
FIN-WAIT-1	First FIN sent; waiting for ACK
FIN-WAIT-2	ACK to first FIN received; waiting for second FIN
CLOSE-WAIT	First FIN received, ACK sent; waiting for application to close
TIME-WAIT	Second FIN received, ACK sent; waiting for 2MSL time-out
LAST-ACK	Second FIN sent; waiting for ACK
CLOSING	Both sides decided to close simultaneously

Figure 24.16 Time-line diagram for a common scenario



MODULE –V

THE LINK LAYER and LANs

The Link Layer (Data Link Layer):

➤ **OSI Model:**

The data link layer is the second layer in the OSI model, responsible for transmitting data between adjacent network nodes.

➤ **Node-to-Node Delivery:**

Its primary function is to deliver data between network devices, ensuring error-free transmission over a local network segment.

➤ **MAC Addresses:**

It uses Media Access Control (MAC) addresses to identify devices on the local network and ensure data reaches the correct receiver.

➤ **Frame Creation:**

The link layer encapsulates data into frames, which are the units of data transmission at this layer.

➤ **Error Control:**

It implements mechanisms for detecting and potentially correcting errors that may occur during data transmission.

➤ **Flow Control:**

It regulates the flow of data to prevent slow receivers from being overwhelmed by fast senders.

➤ **Media Access Control:**

The link layer manages access to the shared communication medium, ensuring that devices can transmit data without collisions.

Local Area Networks (LANs):



Local Network:

LANs are a type of network that connects devices within a limited geographical area, such as a home, office, or school.

Shared Medium:

LANs often use shared communication media, such as Ethernet cables or wireless networks, where multiple devices share the same access point.

Link Layer Protocols:

LANs rely on link layer protocols, such as Ethernet (IEEE 802.3) and WiFi (IEEE 802.11), to establish communication between devices.

Switches and Bridges:

Switches and bridges are devices that operate at the link layer to forward data frames to the correct destination within a LAN.

DOCSIS (Data Over Cable Service Interface Specification)



DOCSIS - Data Over Cable Service Interface Specification, is a global standard that enables high-speed internet access through existing cable television (CATV) systems.

It allows cable TV companies to offer broadband internet services without the need to overhaul their entire infrastructure, making it a cost-effective solution for both providers and consumers.

How DOCSIS Works

DOCSIS operates over a Hybrid Fiber-Coaxial (HFC) network, which combines fiber-optic cables for long-distance transmission and coaxial cables for the final leg to homes and businesses.

The system comprises two main components:

Cable Modem (CM): Located at the user's premises, it modulates and demodulates data signals for internet access.

Cable Modem Termination System (CMTS): Situated at the cable provider's facility, it manages data traffic between the internet and multiple cable modems.

The communication between the CM and CMTS is facilitated by the DOCSIS protocol, which defines how data is transmitted over the cable network.

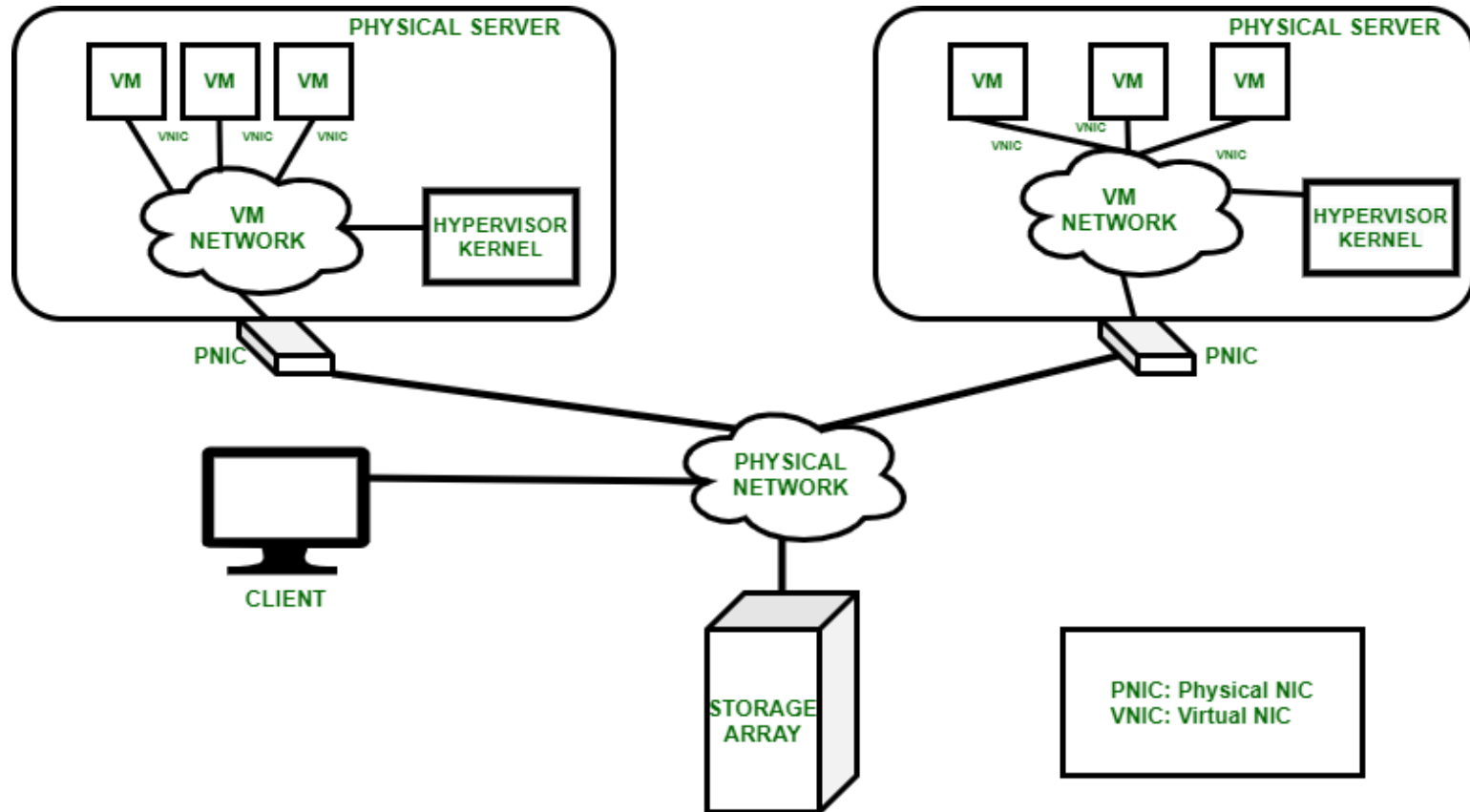
Applications of DOCSIS

- High-Speed Internet Access: Delivering fast internet to homes and businesses.
- DOCSIS allows cable companies to give internet speeds up to 10 Gbps using their existing TV cables.
- Voice over IP (VoIP) : DOCSIS supports phone services over the internet.
- It enables features like caller ID, voicemail, and call forwarding.
- DOCSIS allows reliable delivery of high-quality video streams, including HD and 4K content.
- It's used to stream services like Netflix, YouTube, or live TV over broadband.
- Businesses use DOCSIS for reliable and affordable high-speed internet.
- Especially useful for small to mid-size businesses that don't want to invest in fiber optics.
- With DOCSIS, users can attend Zoom calls, use cloud apps, and stream lectures from home without slowdowns.
- It became especially important during the COVID-19 pandemic.

Link virtualization

- Link virtualization is a network technology that allows a single physical network link to be logically divided into multiple virtual links, each with its own bandwidth and isolation. This enables multiple virtual networks or logically isolated network partitions (LINPs) to share the same physical infrastructure

Link Virtualization



Key Concepts of Link Virtualization:



- **Abstraction:**
- Link virtualization introduces a layer of abstraction between the physical network and the virtual networks that utilize it.
- **Isolation:**
- Each virtual link is isolated from others, ensuring that traffic on one virtual link does not interfere with traffic on another.
- **Programmability:**
- Virtual links can be dynamically configured and adjusted based on the needs of the virtual networks.
- **Shared Infrastructure:**
- Multiple virtual networks can share the same physical network infrastructure, such as a single cable or physical interface.
- **Bandwidth Management:**
- Link virtualization allows for the allocation of bandwidth to different virtual networks, ensuring that each virtual network has its fair share of resources.

How Link Virtualization Works:

- Link virtualization typically involves the following steps:

1. Partitioning:

- The physical network link is logically divided into multiple virtual links.

2. Identification:

- Each virtual link is assigned a unique identifier, such as a virtual network ID (VNID) or MAC address.

3. Encapsulation/Decapsulation:

- Packets destined for a specific virtual link are encapsulated with the virtual network ID, and the encapsulating/decapsulating process is handled at the link layer.

4. Routing/Forwarding:

- Packets are routed/forwarded based on the virtual network ID, ensuring that they are delivered to the correct virtual network.

5. Bandwidth Control:

- Bandwidth allocation and control mechanisms are implemented to ensure that each virtual network has its share of bandwidth.

Benefits of Link Virtualization:

- **Resource Optimization:**
- Link virtualization allows for more efficient use of network resources, as multiple virtual networks can share the same physical infrastructure.
- **Isolation:**
- Virtual networks can be isolated from each other, ensuring that traffic on one virtual network does not interfere with traffic on another.
- **Flexibility:**
- Virtual networks can be created, modified, and deleted dynamically, allowing for quick adaptation to changing network requirements.
- **Scalability:**
- Link virtualization can be scaled to support a large number of virtual networks.
- **Cost Savings:**
- By sharing resources, link virtualization can help to reduce the overall cost of network infrastructure

Applications of Link Virtualization:

- **Data Centers:**
- Link virtualization can be used to provide isolated virtual networks for different workloads within a data center.
- **Cloud Computing:**
- Link virtualization is a key technology in cloud computing, enabling multiple tenants to share the same physical infrastructure.
- **Software-Defined Networking (SDN):**
- Link virtualization is often used in SDN implementations to enable programmable and flexible network management.

Multiprotocol Label Switching (MPLS)



- Multiprotocol Label Switching (MPLS) is a networking technique that uses labels instead of IP addresses to forward data packets across a network, enabling faster and more efficient data transmission. It is particularly well-suited for applications like Virtual Private Networks (VPNs) and traffic engineering, and it's often seen in service provider networks.

How MPLS Works:

- **Labels:**
- MPLS assigns a label to each data packet, which acts as a short identifier used for routing.
- **Label Edge Routers (LERs):**
- These routers, located at the edge of the MPLS network, add labels to packets entering the network and remove them as they leave.
- **Label Switching Routers (LSRs):**
- These routers within the MPLS network use the label to forward packets along a pre-defined path, without looking at the full IP header.
- **Forwarding:**
- Instead of each router needing to perform complex IP address lookups, MPLS uses a label lookup table to quickly determine the next hop.

Benefits of MPLS:

- **Improved Speed and Efficiency:**
- By using labels and pre-defined paths, MPLS significantly reduces the time spent by routers making forwarding decisions, resulting in faster data transmission.
- **Traffic Engineering:**
- MPLS allows for flexible control over network traffic flow, making it easier to prioritize certain types of traffic or allocate bandwidth to specific applications.
- **Virtual Private Networks (VPNs):**
- MPLS provides a robust mechanism for creating private networks across a public infrastructure, offering secure and reliable connections for businesses.
- **Enhanced Quality of Service (QoS):**
- MPLS can be used to guarantee certain levels of performance for specific applications, ensuring that critical traffic receives the necessary resources.

Limitations of MPLS:

- **Complexity:**
- MPLS can be more complex to configure and manage compared to simpler routing protocols.
- **Cost:**
- MPLS networks can be more expensive to set up and maintain due to the specialized hardware and expertise required.
- **Lack of End-to-End Encryption:**
- While MPLS networks are typically secure, they do not inherently provide end-to-end encryption, which can be a concern for highly sensitive data.

Data center networking

- Data center networking is the infrastructure that interconnects the computing, storage, and network resources within a data center to enable the delivery of applications and data. It facilitates the efficient and secure transmission of data between devices within the data center and to external networks.

Key aspects of data center networking:

- **Interconnectivity:**
- Data center networks connect various resources like servers, storage systems, and networking devices to facilitate data exchange and processing.
- **Scalability and Efficiency:**
- They need to be scalable to handle the growing demands of cloud computing and efficient to ensure smooth data flow.
- **Virtualization and Software-Defined Networking:**
- Modern data center networks increasingly leverage virtualization technologies and software-defined networking (SDN) to provide flexibility and automation.
- **Security:**
- Data center networks incorporate security measures to protect data and applications from unauthorized access and threats.
- **Centralized Management:**
- They often include centralized management systems to streamline network operations and improve efficiency.

Components of a data center network:

- **Servers:** The primary computing resources within the data center.
- **Storage systems:** Used to store data and applications.
- **Network devices:** Include routers, switches, firewalls, and other networking equipment.
- **Cabling and connectivity:** Physical infrastructure that connects the various components.
- **Virtualization and containerization technologies:** Used to virtualize and manage infrastructure resources.

Benefits of data center networking



- **Enhanced performance:** Efficient data transfer and reduced latency.
- **Improved scalability:** Ability to handle growing workloads and demands.
- **Increased reliability:** Redundant power sources and cooling systems ensure uninterrupted operation.
- **Simplified management:** Centralized management platforms streamline operations.
- **Reduced costs:** Virtualization and automation can lower operational costs.

Thank you