JAIN DEEMED-TO-BE UNIVERSITY
SCHOOL OF COMPUTER SCIENCE AND IT

Master of Computer Applications

23MCAC102 – Advanced Computer Networks

Module-2

Data Link Layer

Module-2 Syllabus

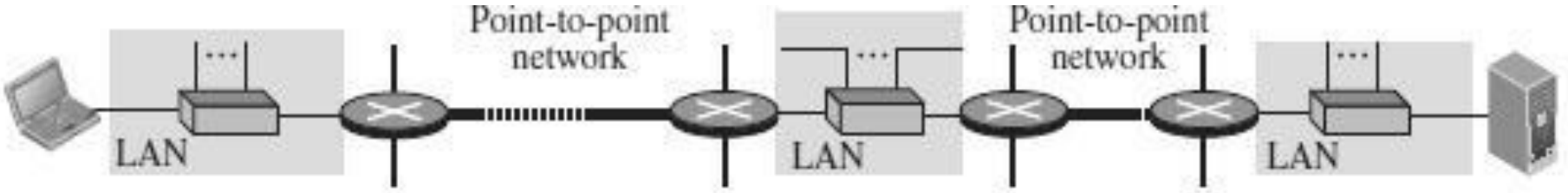
DATA-LINK LAYER & MEDIA ACCESS

- Introduction
- Link-Layer Addressing
- Media Access Control
- Wired LANs: Ethernet
- Wireless LANs : IEEE 802.11
- Bluetooth
- Connecting Devices.

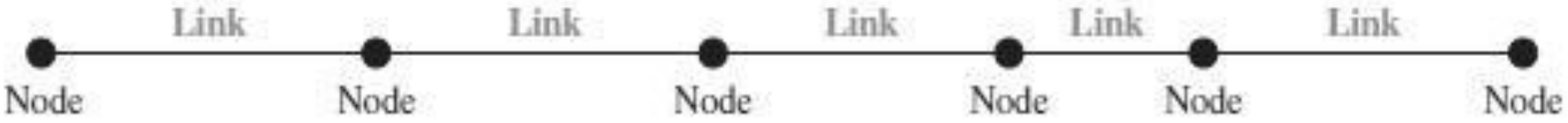
- It is responsible for **transmitting frames from one node to next node**.
- The main responsibility of the Data Link Layer is **to transfer the datagram across an individual link.**
- The other **responsibilities of this layer** are
  - **Framing -** Divides the stream of bits received into data units called frames.
  - **Physical addressing** – I**f frames are to be distributed to different systems on the same network**, **data link layer adds a header to the frame** to define the sender and receiver.
  - **Flow control**- If the rate at which the data are absorbed by the receiver is less than the rate produced in the sender, the Data link layer imposes a flow control mechanism.
  - **Error control**- Used for **detecting and retransmitting damaged or lost frames and to prevent duplication of frames**. This is achieved through a trailer added at the end of the frame.
  - **Medium Access control** - Used **to determine which device has control over the link** at any given time.

Nodes and Links

- Communication at the data-link layer is **node-to-node.**
- In order to move the datagram from source to the destination, the **datagram must be moved across an individual link.**
- LANs and WANs are **connected by routers.**



a. A small part of the Internet



b. Nodes and links

Two Categories of Links

Point- to-Point link and Broadcast link.

- In a point-to-point link, the link is dedicated to the two devices
- In a broadcast link, the link is shared between several pairs of devices.

Data Link Layer Services

- The datalink layer **provides services to the network layer**; it **receives services from the physical layer.**
- When a packet is travelling, the **data-link layer of a node (host or router)** is **responsible for delivering a datagram to the next node** in the path.
- The **datagram received by the data-link layer** of the source host is **encapsulated in a frame.**
- The frame is logically transported from the source host to the router.
- The frame is **decapsulated at the data-link layer of the router** and encapsulated at another frame.
- The new **frame is logically transported from the router to the destination host**.

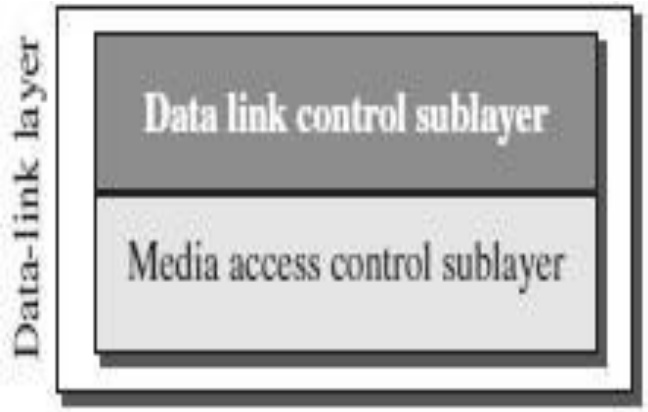
Sublayers in Data Link layer

- We can divide the data-link layer into **two sublayers:**

  (i) Data Link Control (DLC) and

  (ii) Media Access Control (MAC).

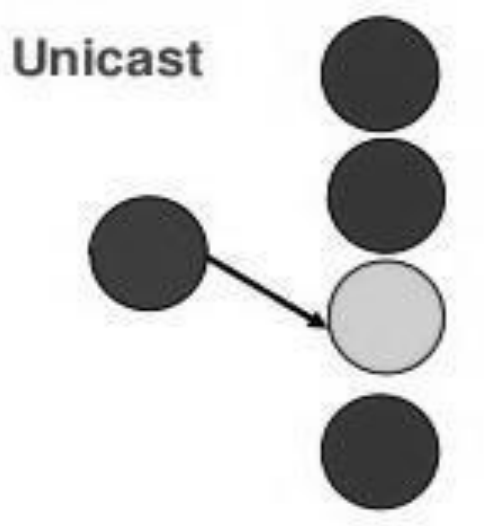
- The DLC sublayer deals with all issues common to both point- to-point and broadcast links
- The MAC sublayer deals only with issues specific to broadcast links

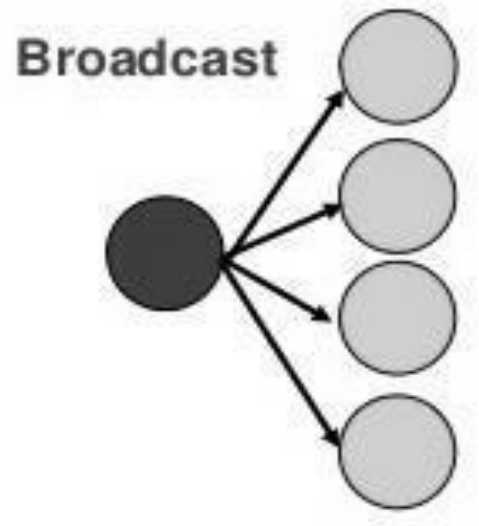


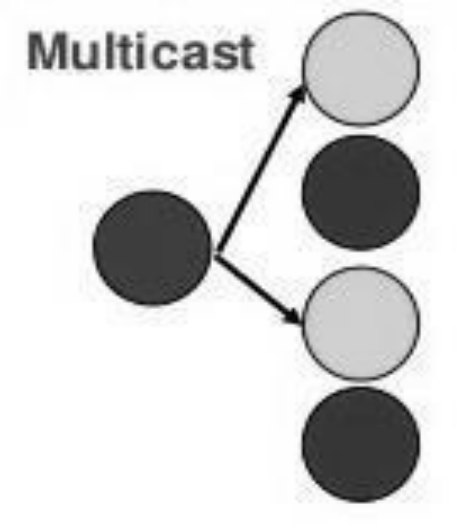
- A link-layer address is sometimes called a link address, sometimes a **physical address, and sometimes a MAC address**.
- Since a link is controlled at the data-link layer, the addresses need to belong to the data-link layer.
- When a datagram passes from the network layer to the data-link layer, the datagram will be encapsulated in a frame and **two data-link addresses are added to the frame header.**
- **These two addresses are changed every time the frame moves from one link to another**

THREE TYPES OF ADDRESSES

- The link-layer protocols define three types of addresses:
  (i) Unicast (ii) Multicast (iii) Broadcast.







Unicast Address:

- Each host or each interface of a router is assigned a unicast address. Unicasting means one-to-one communication. A frame with a unicast address destination is destined only for one entity in the link.

Multicast Address:

- Link-layer protocols define multicast addresses. Multicasting means one-to-many Communication but not all.

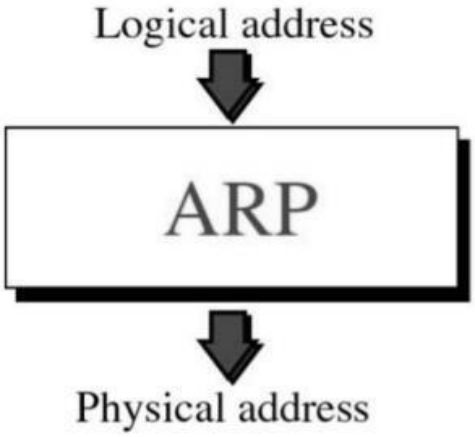
Broadcast Address:

- Link-layer protocols define a broadcast address. Broadcasting means one- to-all communication. A frame with a destination broadcast address is sent to all entities in the link.

ADDRESS RESOLUTION PROTOCOL (ARP)

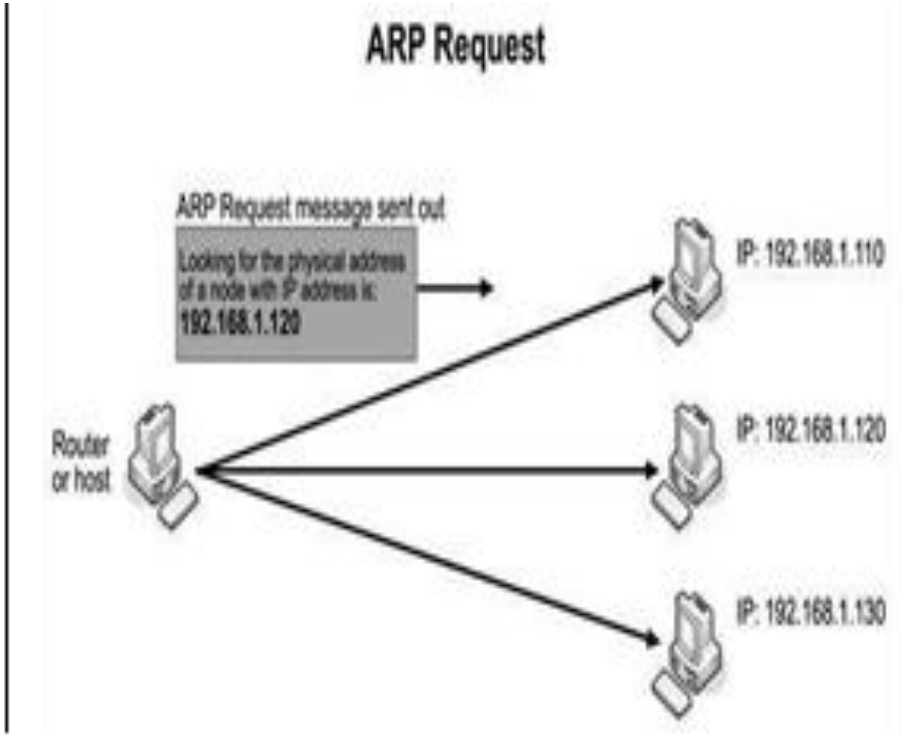
ADDRESS RESOLUTION PROTOCOL (ARP)

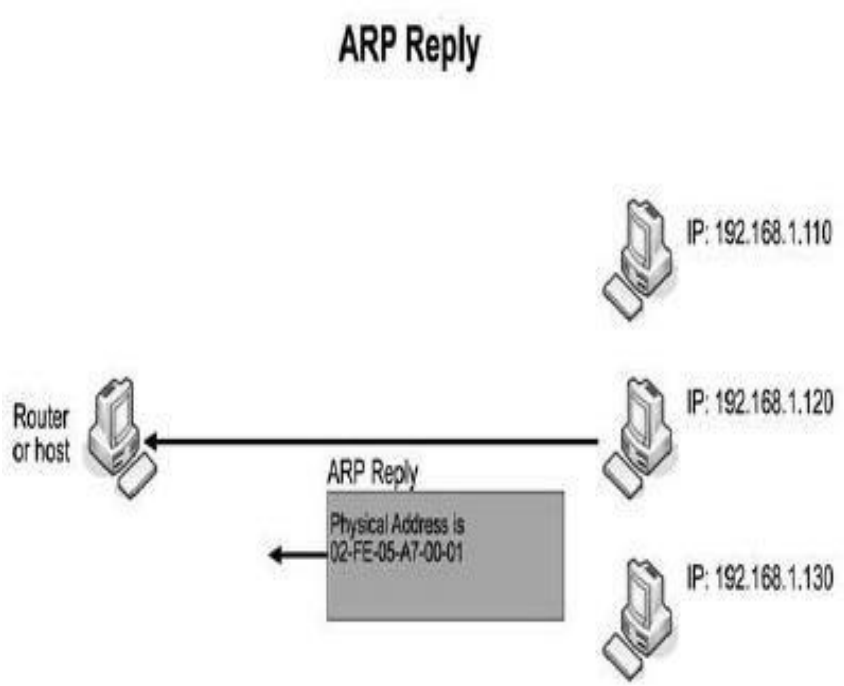
- The ARP is a communication protocol **used for discovering the link layer address, such as a MAC address, associated with a given IP Address,** typically an IPv4 address
- The computer applications use logical address to send/receive messages, however the actual communication happens over the physical address.
- **To send a datagram over a network**, we need both the logical and physical address.
- **IP addresses** are made up of **32 bits** whereas **MAC addresses** are made up of **48 bits**.
- **ARP enables each host to build a table of IP address and corresponding physical address.**
- ARP relies on broadcast support from physical networks.
- **The ARP Protocol is a request and response protocol.**
- The types of ARP messages are:
  - **ARP request**
  - **ARP reply**



ARP Operation

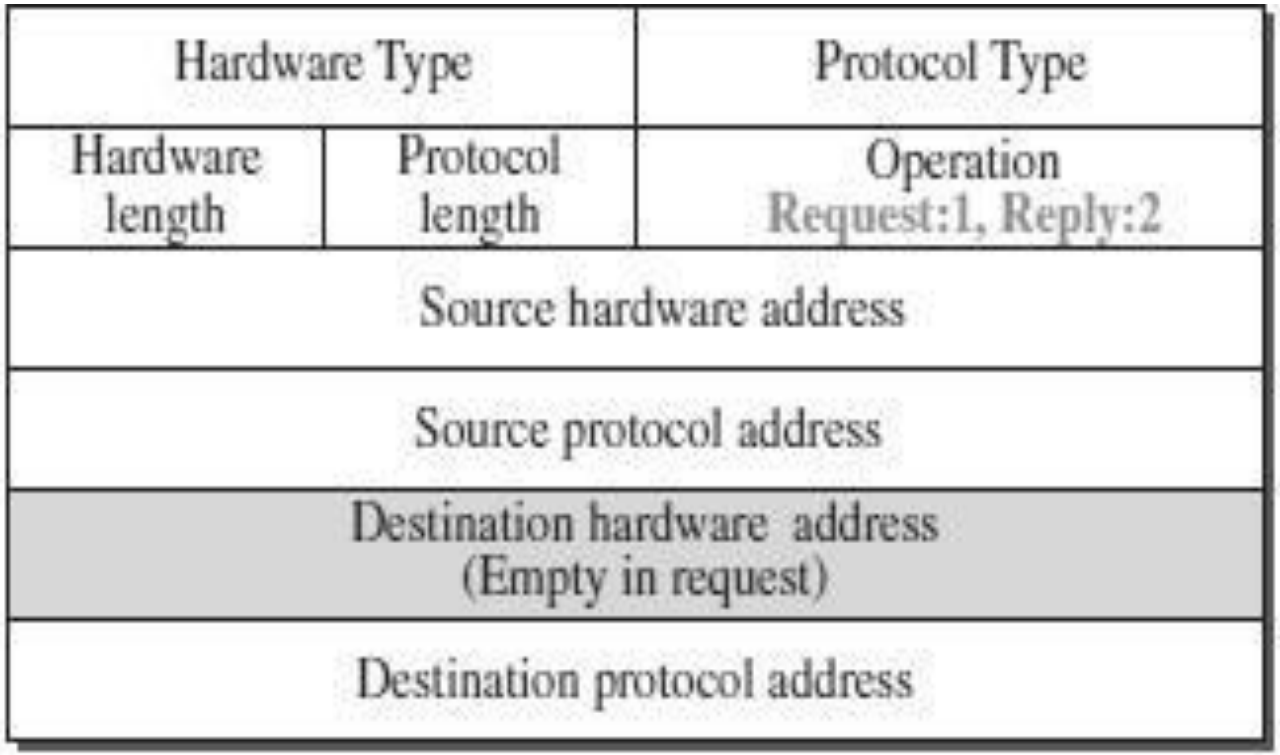
- ARP maintains a **cache table in which MAC addresses are mapped to IP addresses.**
- **If a host wants to send an IP datagram to a host**, it **first checks for a mapping in the cache table.**
- **If no mapping is found, it needs to invoke the ARP over the network.**
- It does this **by broadcasting an ARP query onto the network**.
- This query contains the target IP address.
- **Each host receives the query** and **checks to see if it matches its IP address**.
- **If it does match**, the **host sends a response message** that contains its link- layer address (MAC Address) back to the originator of the query.
- The **originator adds** the information contained in this **response to its ARP table.**
- **For example:** To determine system B's physical (MAC) address, system A broadcasts an ARP request containing B's IP address to all machines on its network.





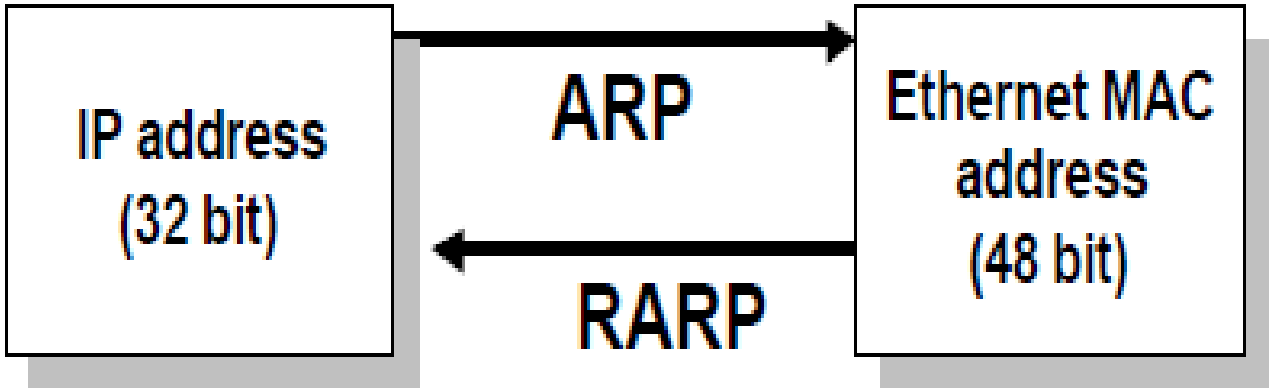
- **All nodes except the destination discard the packet but update their ARP table.**
- Destination host (System B)constructs an ARP Response packet. ARP Response is unicast and sent back to the source host (System A).
- Source stores target Logical & Physical address pair in its ARP table from ARP Response.
- **If target node does not exist on same network, ARP request is sent to default router.**

ARP Packet


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

RARP – Reverse ARP

- RARP is used to request its Internet Protocol (IPv4) address from a computer network, when all it has available is its link layer or hardware address, such as a MAC address.



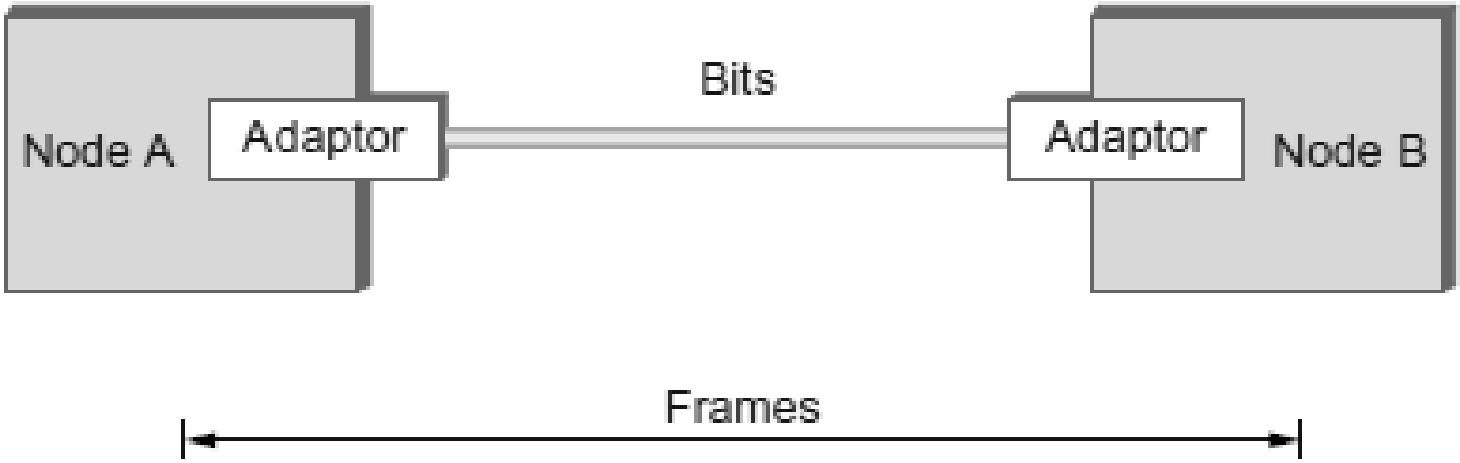
DLC Services

DLC Services

- The data link control (DLC) **deals with procedures for communication between two adjacent nodes**—node-to-node communication—no matter whether the link is dedicated or broadcast.
- DLC services include
  - **(1) Framing**
  - **(2) Flow Control**
  - **(3) Error Control**

i) FRAMING

- The data-link layer packs the bits of a message into frames, so that each frame is distinguishable from another.
- One reason is that a **frame can be very large**, **making flow and error control very inefficient.**
- When a message is carried in **one very large frame, even a single-bit error would require the retransmission** of the whole frame.
- When **a message is divided into smaller frames**, a **single-bit error affects only that small frame.**
- Framing in the data-link layer separates a message from one source to a destination by **adding a sender address and a destination address.**



Frame Size

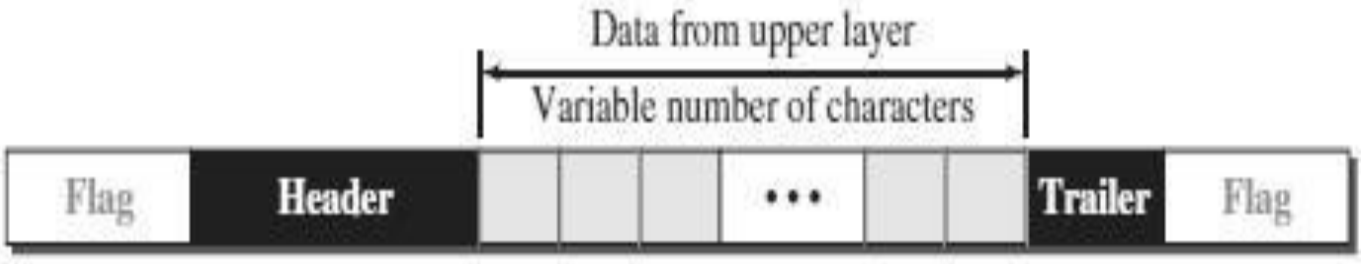
- Frames can be of **fixed or variable size.** Frames of fixed size are called cells.
- **In fixed-size framing,** there is **no need for defining the boundaries of the frames**; the size itself can be used as a delimiter.
- **In variable-size framing**, we need a way to **define the end of one frame and the beginning of the next.**
- **Two approaches were used for this purpose**:

  (a) Character-oriented approach and

  (b) Bit-oriented approach.

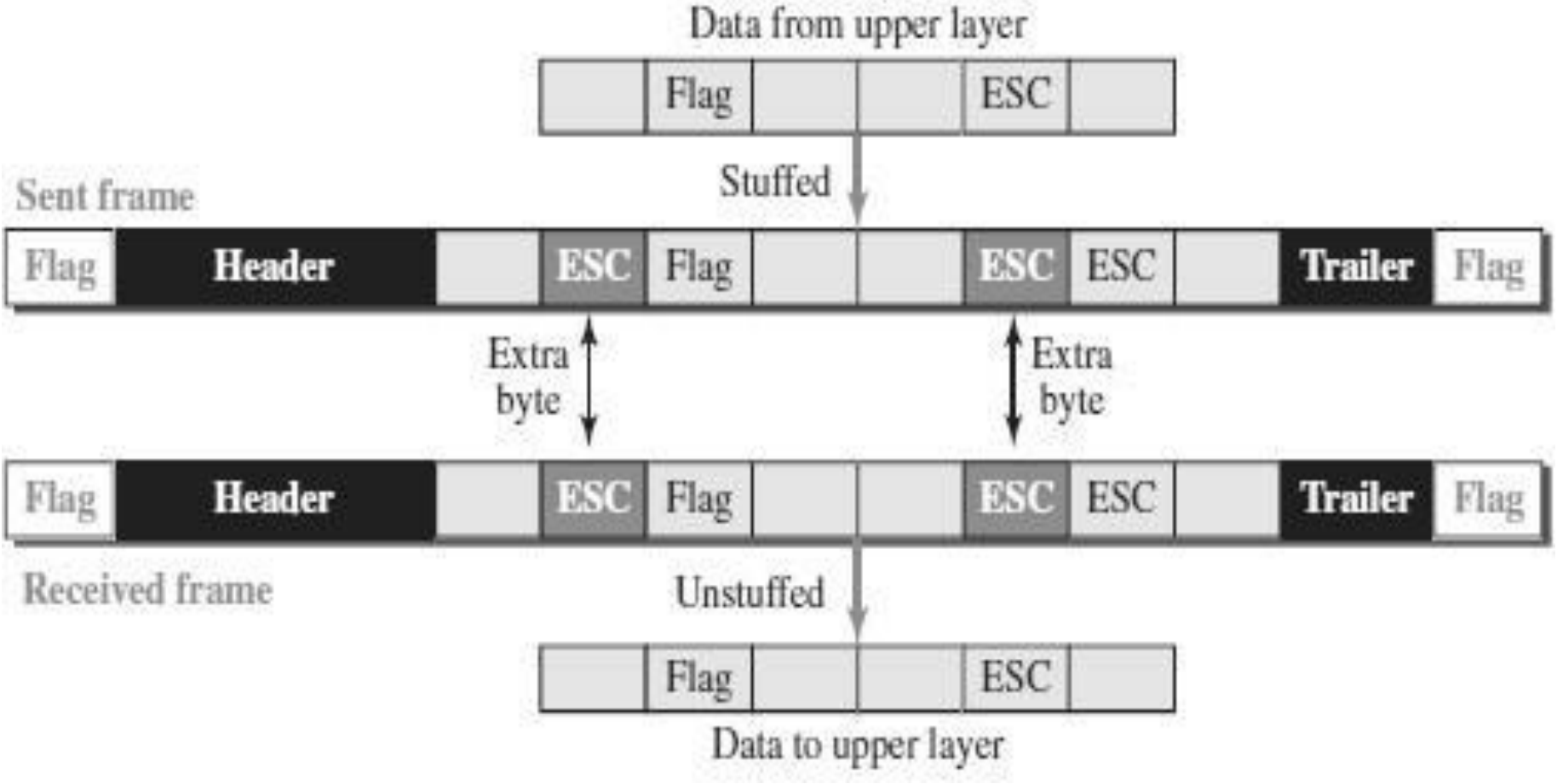
a) Character-Oriented Framing

- In character-oriented (or byte-oriented) framing, **data to be carried are 8-bit characters.**
- **To separate one frame from the next,** an **8-bit (1-byte) flag is added at the beginning and the end of a frame.**
- The **flag**, composed of protocol-dependent special characters, **signals the start or end of a frame.**
- Any **character used for the flag could also be part of the information**.
- If this happens, **when it encounters this pattern in the middle of the data, the receiver thinks it has reached the end of the frame.**
- To fix this problem, a **byte-stuffing** strategy was added to character-oriented framing.



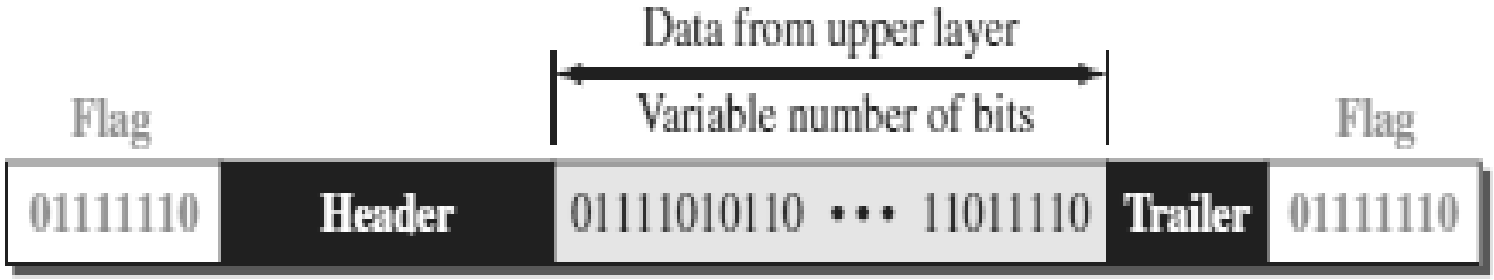
Byte Stuffing (or) Character Stuffing

- **Byte stuffing is the process of adding one extra byte whenever there is a flag or escape character in the text.**
- In byte stuffing, a **special byte is added to the data section** of the frame when there is a character with the same pattern as the flag.
- The data section is stuffed with an extra byte. **This byte is usually called the escape character (ESC)** and has a predefined bit pattern.
- **Whenever the receiver encounters the ESC character**, it removes it from the data section and treats the next character as data, not as a delimiting flag.


Data from upper layer
Flag
ESC
Stuffed
Sent frame
Flag
Header
ESC
Flag
ESC
ESC
Trailer
Flag
Extra byte
Extra byte
Flag
Header
ESC
Flag
ESC
ESC
Trailer
Flag
Received frame
Unstuffed
Flag
ESC
Data to upper layer

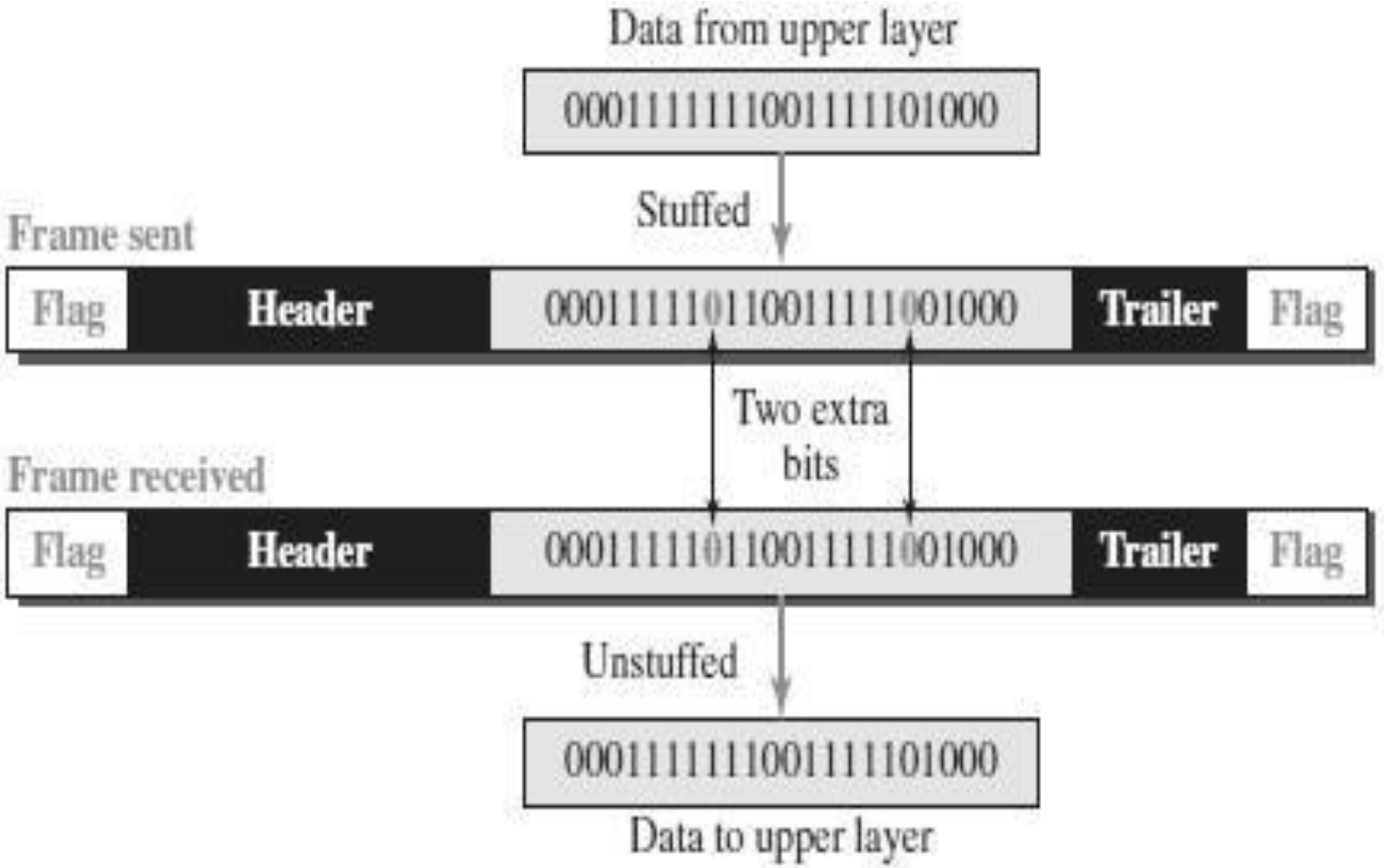
b) Bit-Oriented Framing

- In bit-oriented framing, the **data section of a frame is a sequence of bits** to be **interpreted by the upper layer as text, graphic, audio, video,** and so on.
- In addition to headers and trailers, we still **need a delimiter to separate one frame from the other**.
- Most protocols use a **special 8-bit pattern flag, 01111110,** as the delimiter **to define the beginning and the end of the frame**
- **If the flag pattern appears in the data,** the **receiver must be informed** that this is **not the end of the frame**.
- This is **done by stuffing 1 single bit** (instead of 1 byte) to prevent the pattern from looking like a flag. The **strategy is called bit stuffing.**



Bit Stuffing

- **Bit stuffing is the process of adding one extra 0 whenever five consecutive 1s follow a 0 in the data, so that the receiver does not mistake the pattern 0111110 for a flag.**
- In bit stuffing, if a 0 and five consecutive 1 bits are encountered, **an extra 0 is added.**
- This extra **stuffed bit is eventually removed from the data** by the receiver.
- The extra **bit is added after one 0 followed by five 1's regardless of the value of the next bit.**
- This guarantees that the flag field sequence does not inadvertently appear in the frame.


Data from upper layer
000111111100111101000
Stuffed
Frame sent
Flag
Header
0001111101100111101000
Trailer
Flag
Two extra bits
Frame received
Flag
Header
0001111101100111101000
Trailer
Flag
Unstuffed
000111111100111101000
Data to upper layer

FLOW CONTROL

FLOW CONTROL

Flow control refers to a set of procedures used to restrict the amount of data that the sender can send before waiting for acknowledgment.

- The receiving device has **limited speed and limited memory** to store the data.
- Therefore, the receiving device must be able to inform the sending device to stop the transmission temporarily before the limits are reached.
- It requires a buffer, a block of memory for storing the information until they are processed.

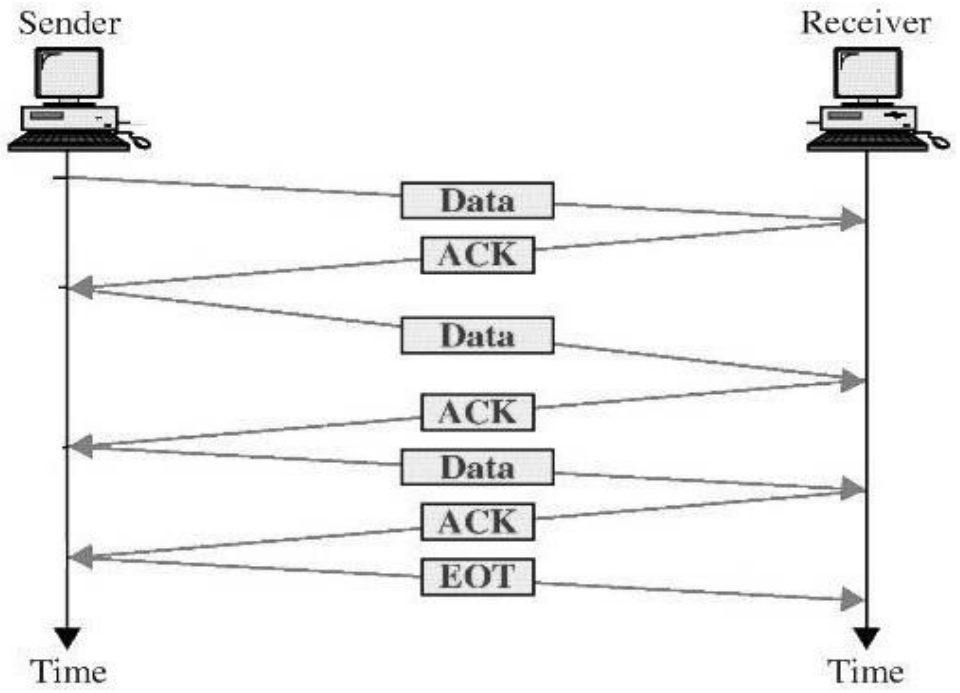
Two methods have been developed to control the flow of data:

i) Stop-and-Wait

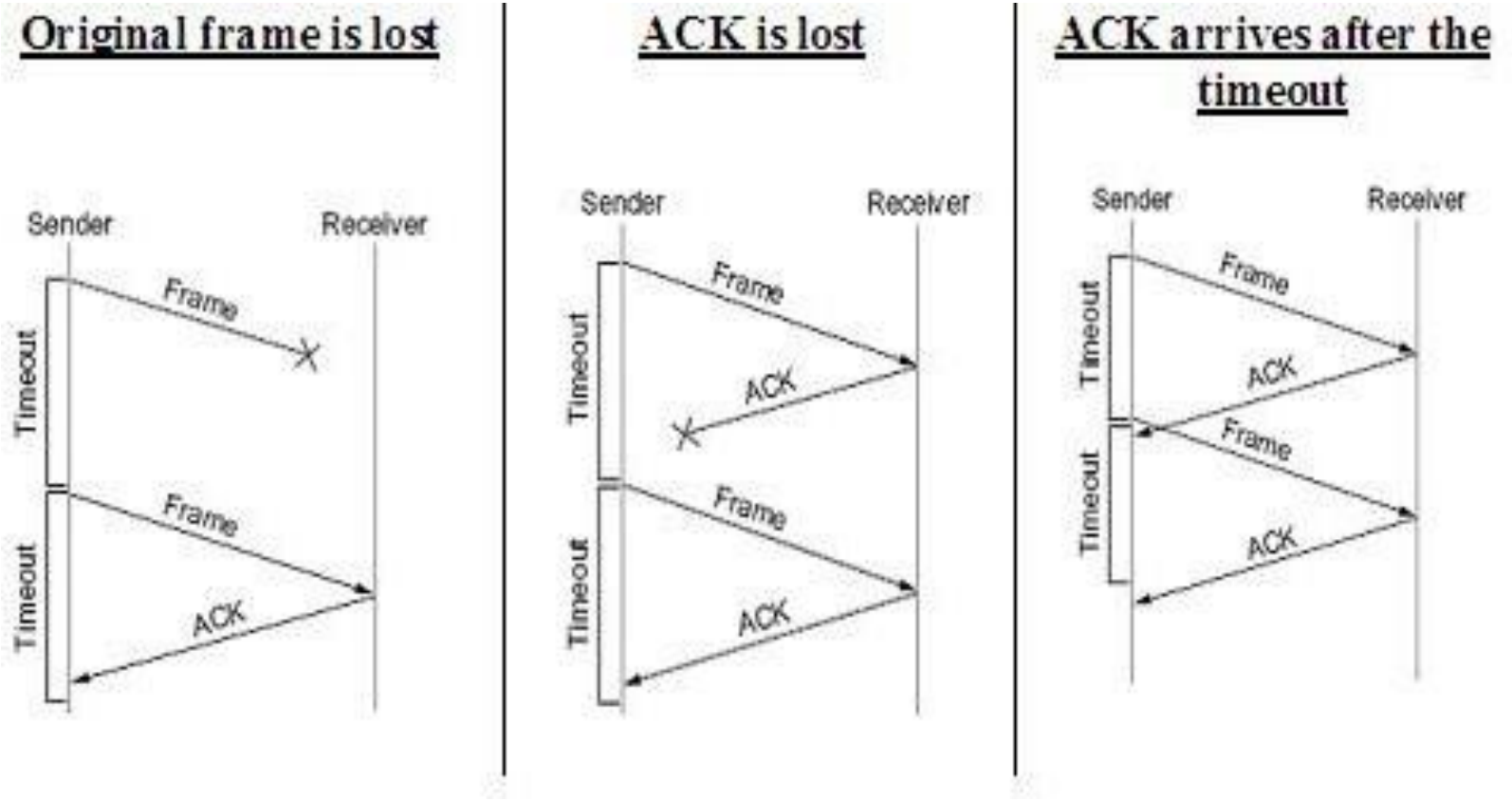
ii) Sliding Window

i) STOP-AND-WAIT

- In Stop-and-wait method, the **sender waits for an acknowledgement after every frame it sends.**
- **When acknowledgement is received**, **then only next frame is sent.**
- The **process** of alternately sending and waiting of a frame **continues until the sender transmits the EOT** (End of transmission) frame.
- If the **acknowledgement is not received within the allotted time**, **then the sender assumes that the frame is lost** during the transmission, **so it will retransmit the frame.**



- **The acknowledgement may not arrive because of the following three scenarios:**
  - Original frame is lost
  - ACK is lost
  - ACK arrives after the timeout



Advantage of Stop-and-wait

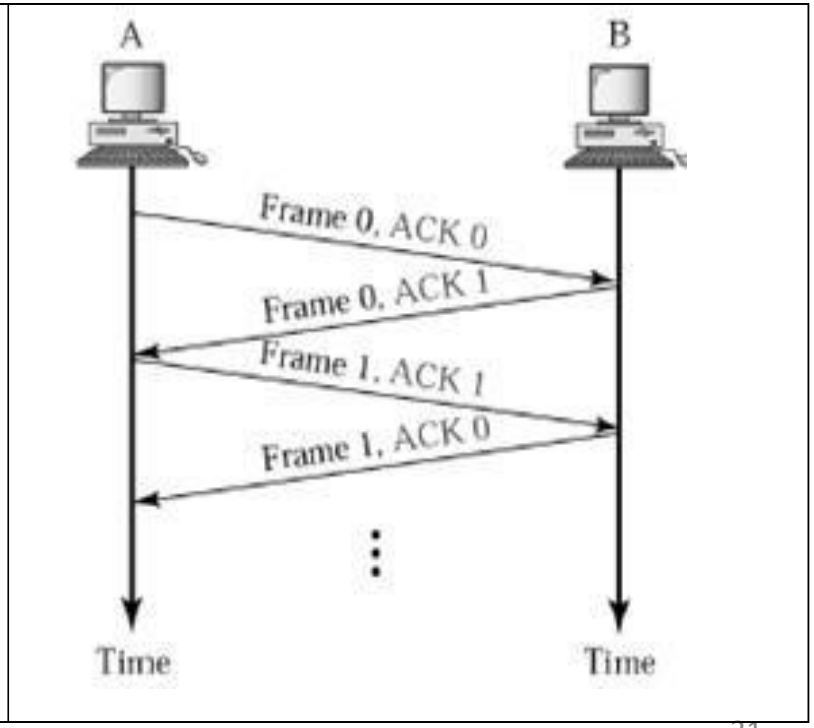
- The Stop-and-wait method is **simple** as each frame is **checked and acknowledged** before the next frame is sent.

Disadvantages of Stop-And-Wait

- In stop-and-wait, at any point in time, there is **only one frame that is sent and waiting to be acknowledged.**
- This is **not a good use of transmission medium.**
- **To improve efficiency, multiple frames should be in transition while waiting for ACK.**

Piggybacking

- A method to **combine a data frame with ACK.**
- **Piggybacking saves bandwidth**
- **Station A and B both have data to send.**
- Instead of sending separately, station A sends a data frame that includes an ACK.
- Station B does the same thing

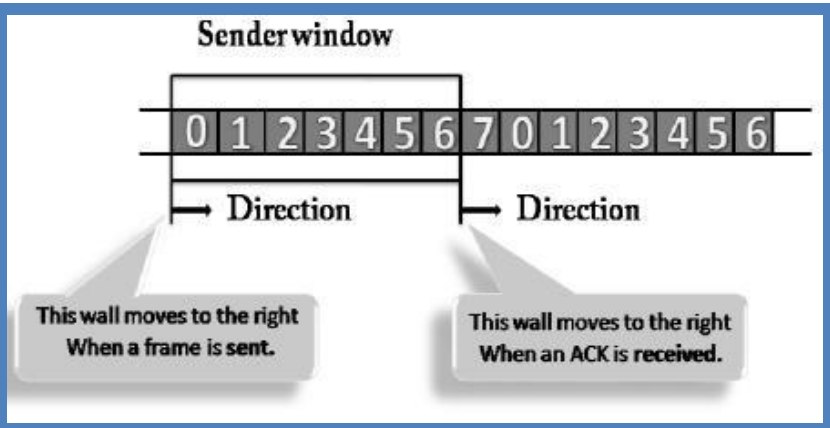


ii) SLIDING WINDOW

- The Sliding Window is a method of flow control in which **a sender can transmit several frames before getting an acknowledgement.**
- In Sliding Window Control, multiple frames can be sent one after the another due to which **capacity of the communication channel can be utilized efficiently.**
- A **single ACK** acknowledge multiple frames.
- Sliding Window refers to imaginary boxes at both the sender and receiver end.
- The window can hold the frames at either end, and **it provides the upper limit on the number of frames** that can be transmitted before the acknowledgement.
- Frames can be acknowledged even when the window is not completely filled.

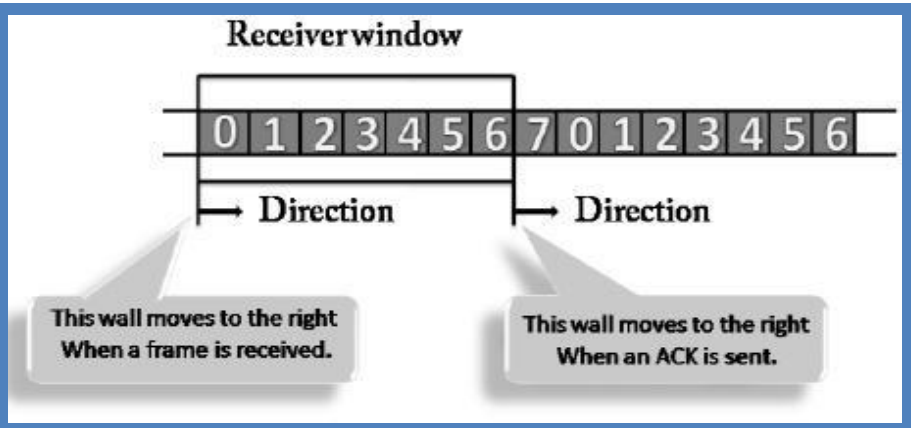
- The **window has a specific size** in which they are numbered as modulo-n means that they are **numbered from 0 to n-1.**
- For example, **if n = 8**, the frames are numbered from **0,1,2,3,4,5,6,7,0,1,2,3,4,5,6,7,0,1.....**
- **The size of the window is represented as n-1**. Therefore, maximum n-1 frames can be sent before acknowledgement.
- **When the receiver sends the ACK**, **it includes the number of the next frame that it wants to receive**.
- **For example, to acknowledge the string of frames ending with frame number 4, the receiver will send the ACK containing the number 5.**
- When the sender sees the ACK with the number 5, it got to know that the frames from 0 through 4 have been received.

Sender Window



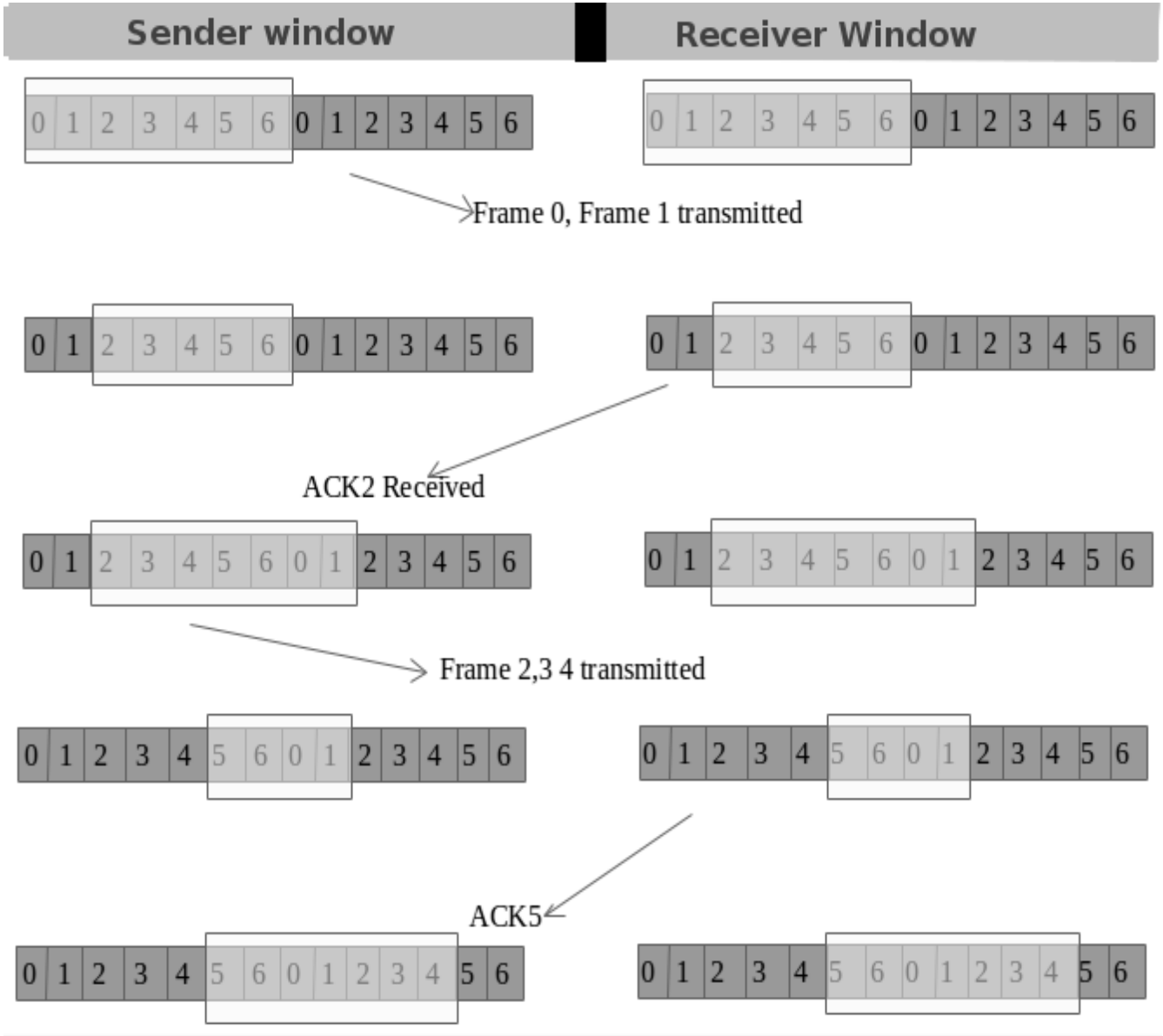
- At the beginning of a transmission, the sender window contains n-1 frames.
- When a frame is sent, the size of the window shrinks.
- For example, if the size of the window is 'w' and if three frames are sent out, then the number of frames left out in the sender window is w-3.
- Once the ACK has arrived, then the sender window expands to the number which will be equal to the number of frames acknowledged by ACK.

Receiver Window



- At the beginning of transmission, the receiver window does not contain n frames, but it contains n-1 spaces for frames.
- When the new frame arrives, the size of the window shrinks.
- For example, the size of the window is w and if three frames are received then the number of spaces available in the window is (w-3).
- Once the acknowledgement is sent, the receiver window expands by the number equal to the number of frames acknowledged.

Example of Sliding Window



Error Control

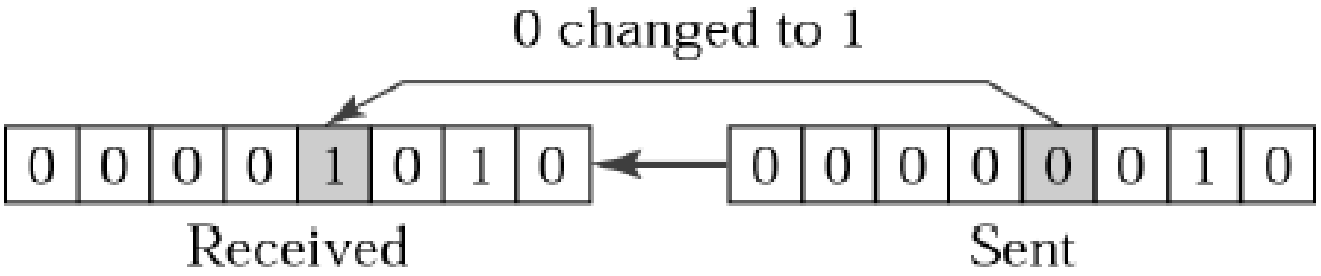
Error Control

- Data can be corrupted during transmission. For reliable communication, errors must be detected and corrected. **Error Control is a technique of error detection and retransmission.**

TYPES OF ERRORS: i) SINGLE-BIT ERROR ii) BURST ERROR

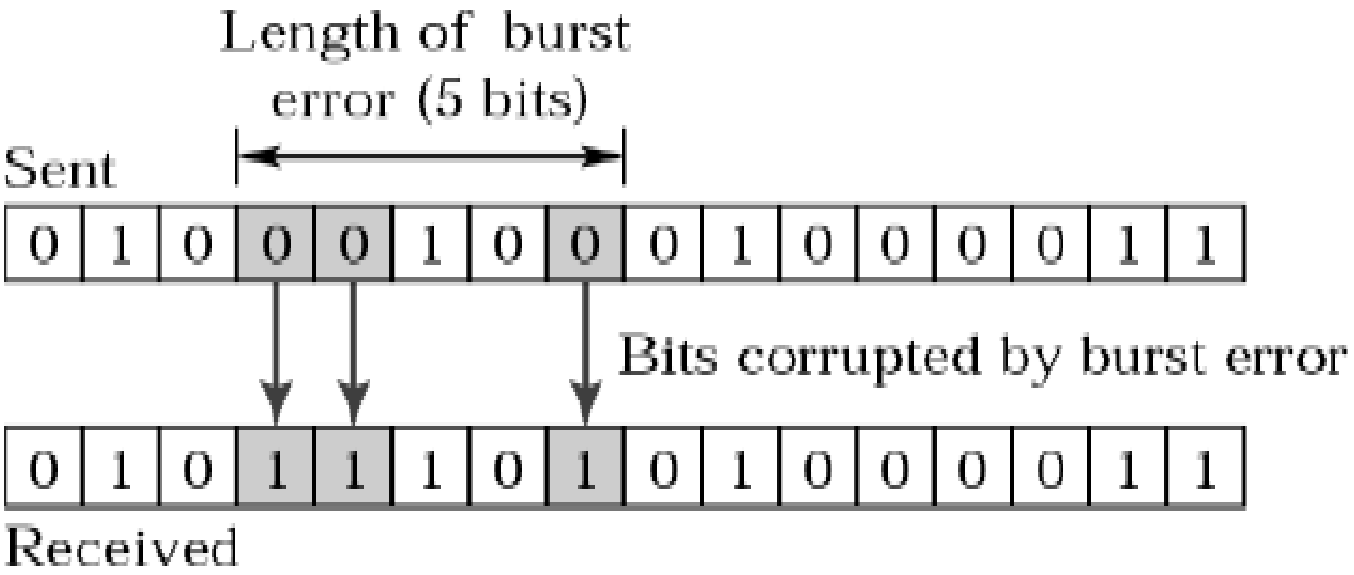
i. Single-Bit Error

- The term Single-bit error means that **only one bit of a given data unit** (such as byte, character, data unit or packet) **is changed from 1 to 0 or from 0 to 1.**



BURST ERROR

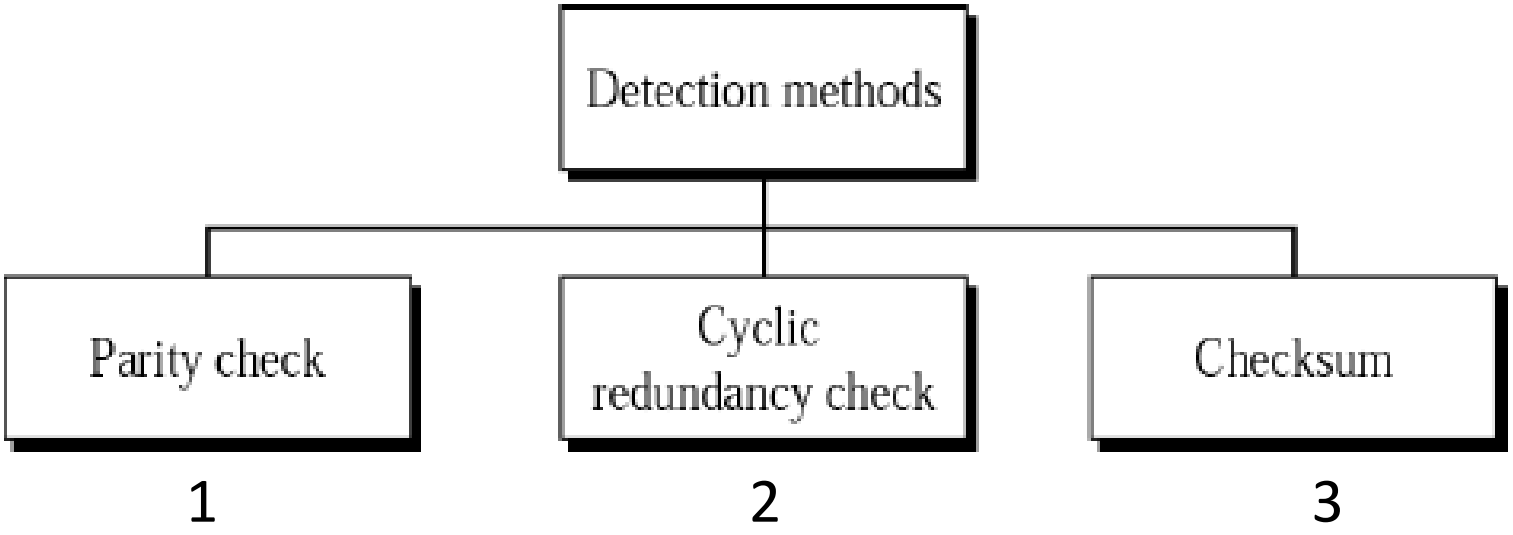
- The term Burst Error means that **two or more bits in the data unit have changed from 1 to 0 or from 0 to 1**.



ERROR DETECTION TECHNIQUES / METHODS

ERROR DETECTION TECHNIQUES / METHODS

- The basic **idea behind any error detection scheme is to add additional information to a frame** that can be used to determine if errors have been introduced.



1) PARITY CHECK

- One bit, called parity bit is added to every data unit so that the **total number of 1's in the data unit becomes even (or) odd.**
- The source then transmits this data via a link, and bits are checked and verified at the destination.
- **Data is considered accurate if the number of bits (even or odd)** matches the number transmitted from the source.
- This techniques is the most common and least complex method.

Even parity – Maintain even number of 1s

E.g., 1011 → 1011 **1**

Odd parity – Maintain odd number of 1s

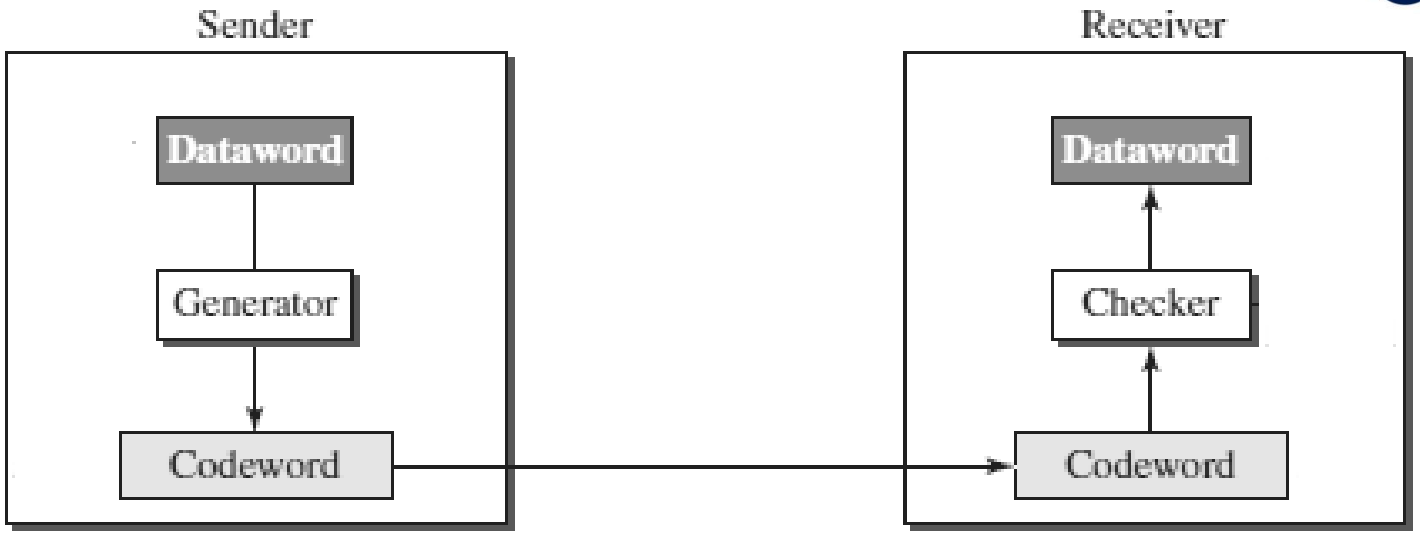
E.g., 1011 → 1011 **0**

2) CYCLIC REDUNDANCY CHECK

- Cyclic codes refers to encoding messages by adding a fixed-length check value.
- CRCs are popular because they are simple to implement, easy to analyze mathematically and particularly good at detecting common errors caused in transmission channels.

Steps Involved :

- Consider the original **message (dataword) as M(x)** consisting of 'k' bits and the **divisor as C(x) consists of 'n+1' bits**.
- The original message **M(x) is appended by 'n' bits of zero's.**
- Let us call this **zero-extended message as T(x)**.
- **Divide T(x) by C(x)** and **find the remainder.**
- The **division operation is performed using XOR operation.**
- The resultant **remainder is appended to the original message M(x) as CRC and sent by the sender (codeword).**



Example 1:

Consider the Dataword / Message **M(x) = 1001**

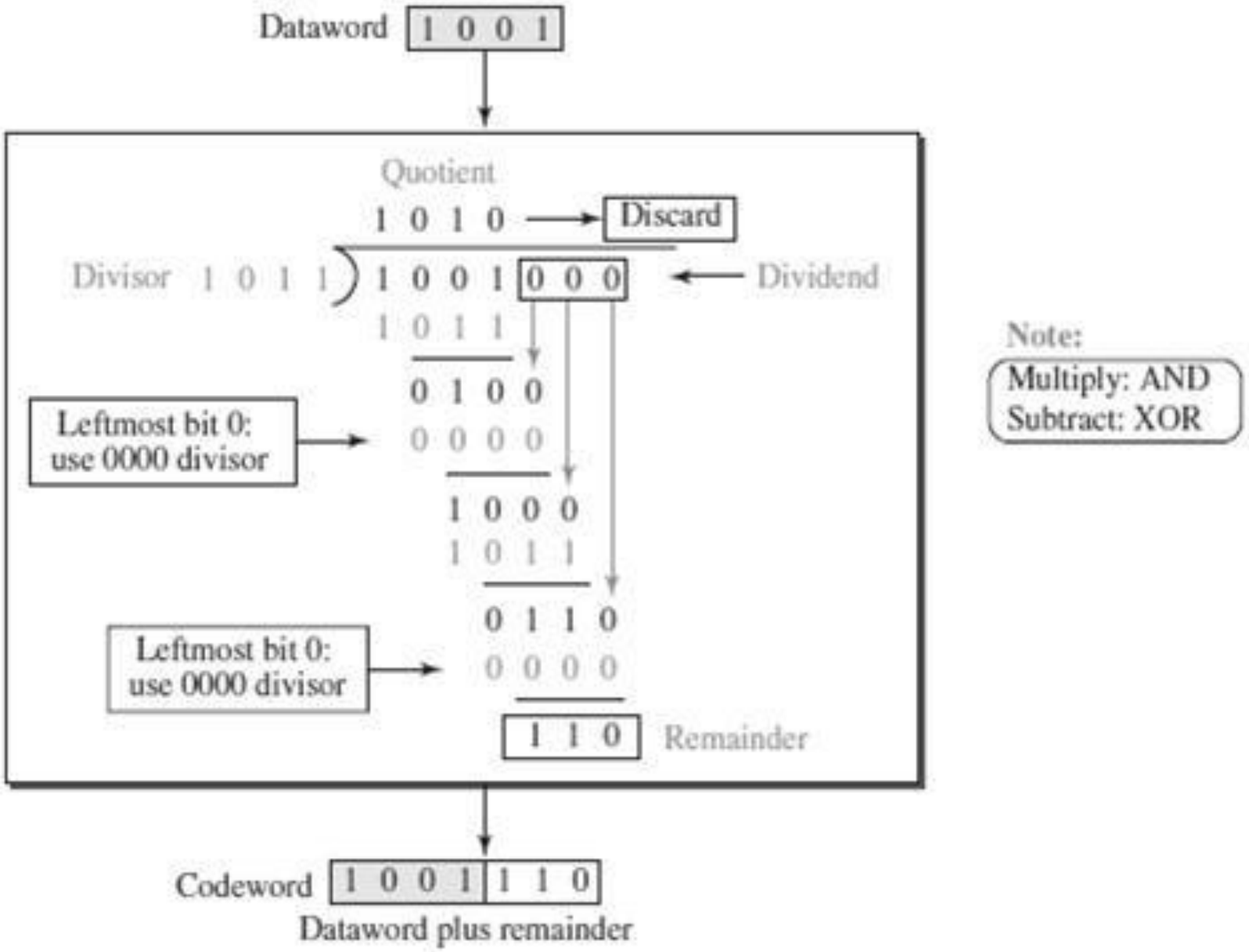
Divisor **C(x) = 1011 (n+1=4)**

Appending 'n' zeros to the original Message M(x).

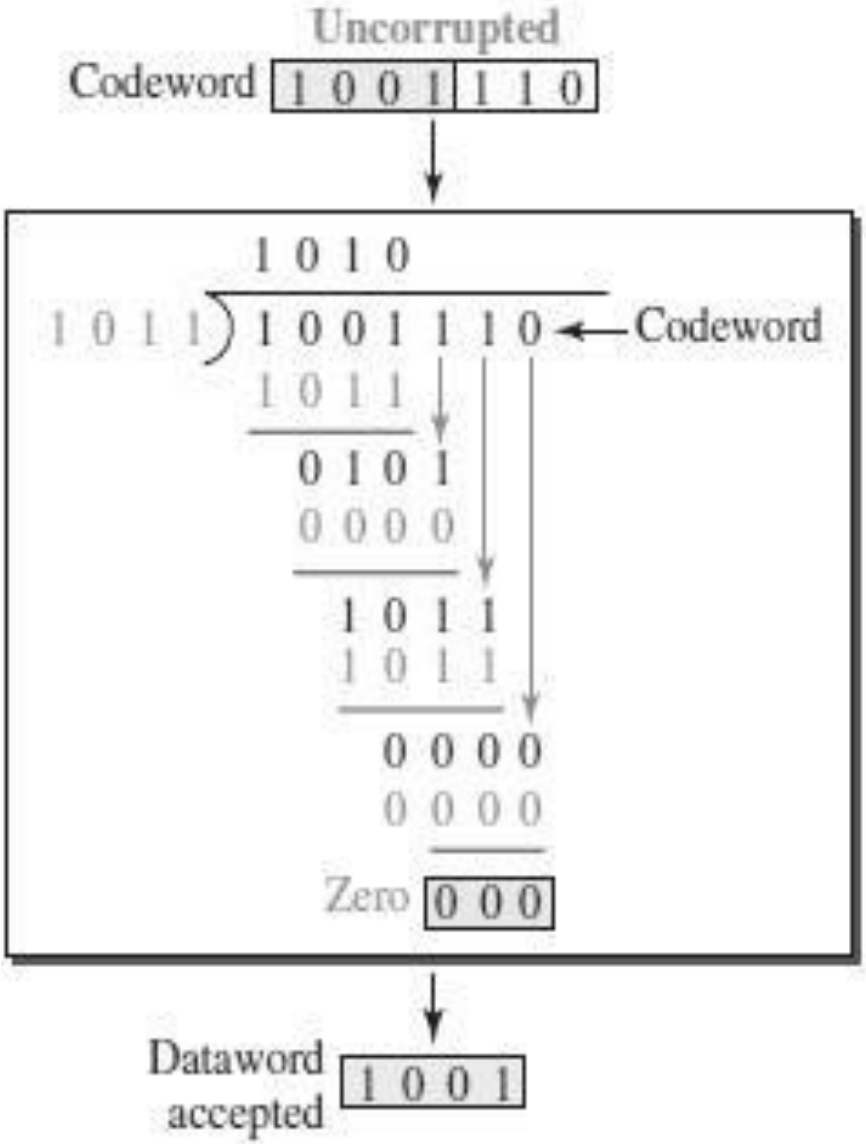
The resultant messages is called **T(x) = 1001 000.** (here n=3)

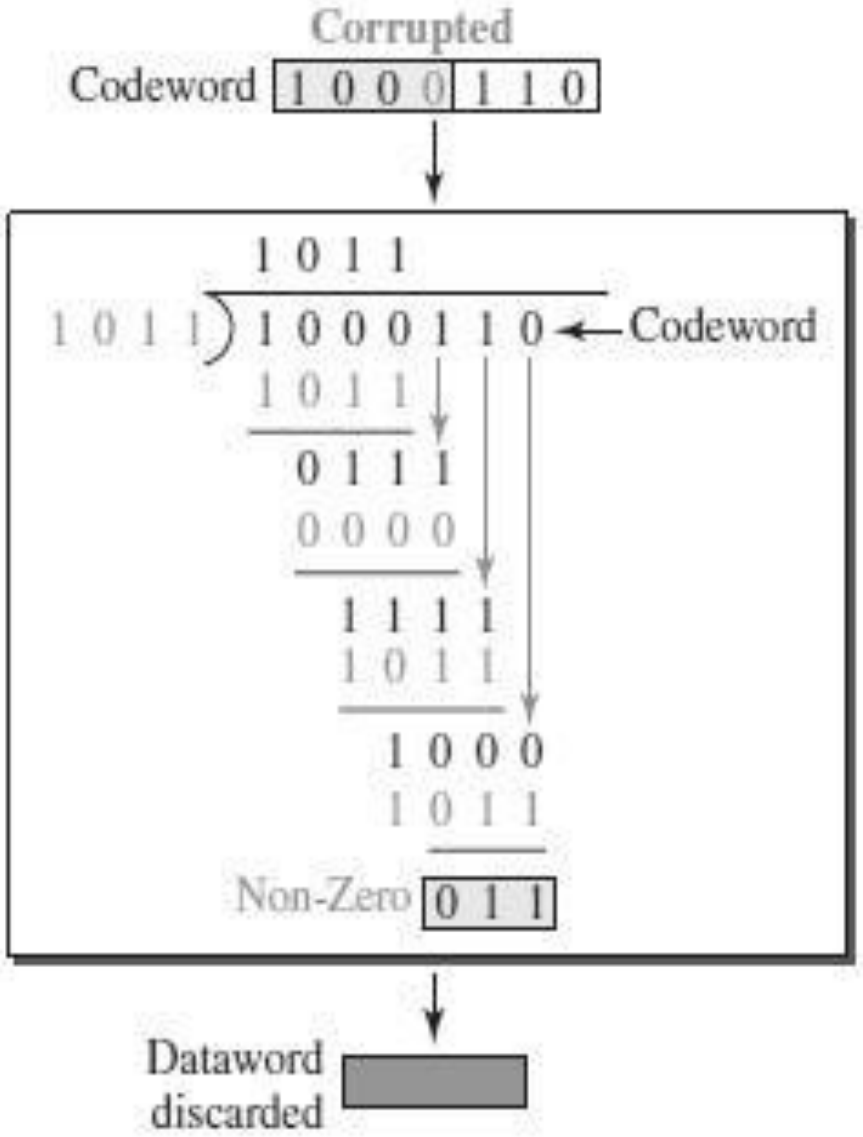
Divide T(x) by the divisor C(x) using XOR operation.

Sender Side


Dataword
1 0 0 1
Quotient
1 0 1 0
Discard
Divisor 1 0 1 1
1 0 0 1 0 0 0
Dividend
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 plus remainder
Note:
Multiply: AND
Subtract: XOR

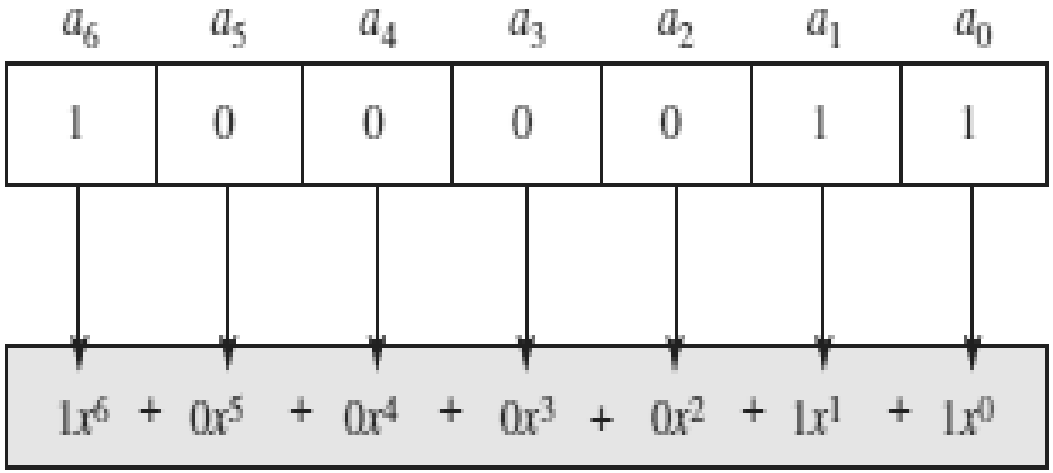
Receiver Side



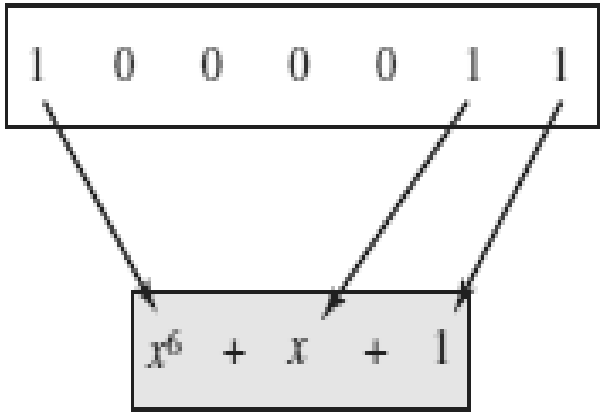


Polynomials

- A pattern of 0s and 1s 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.



a. Binary pattern and polynomial



b. Short form

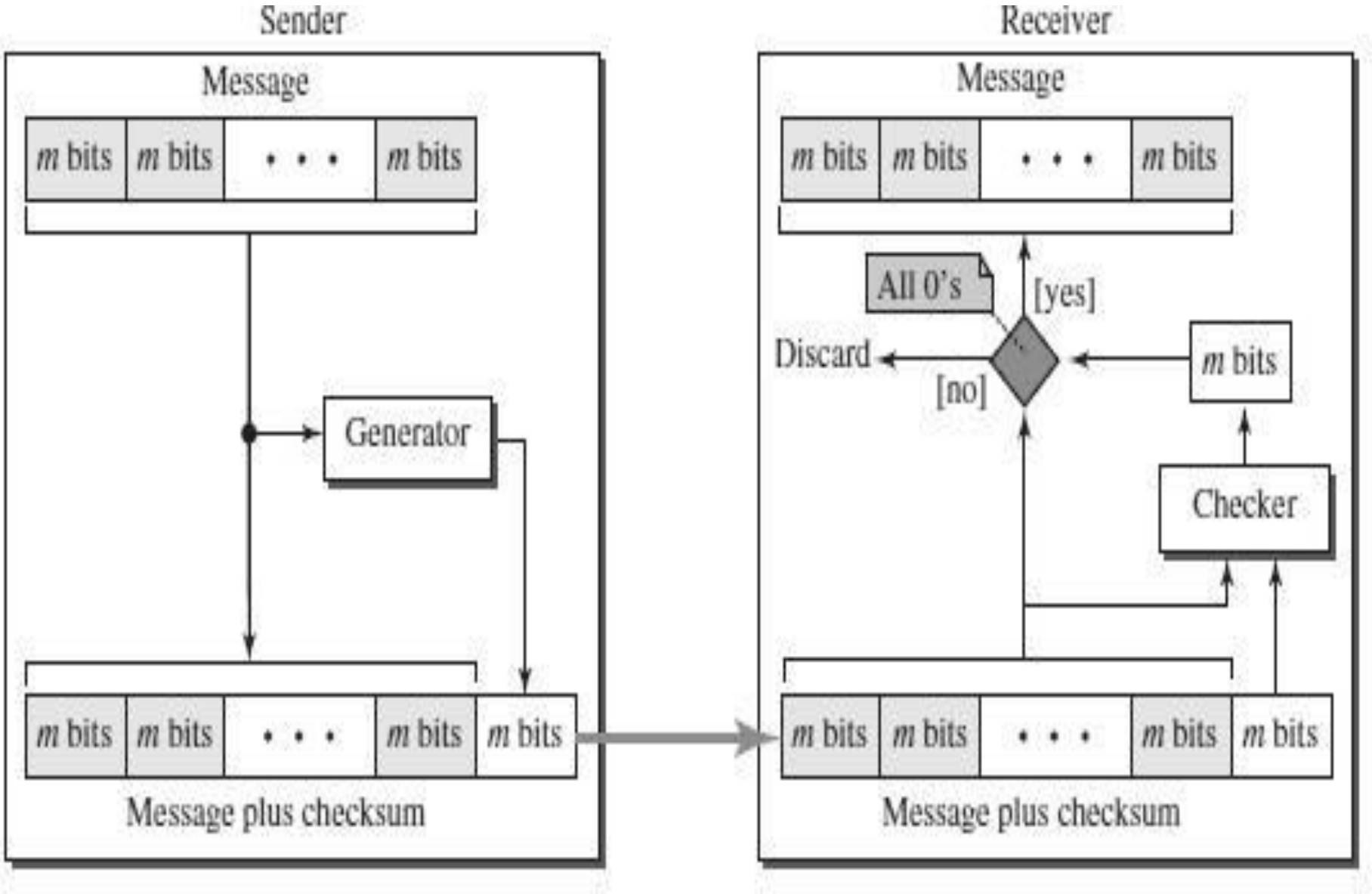
3) Checksum

INTERNET CHECKSUM

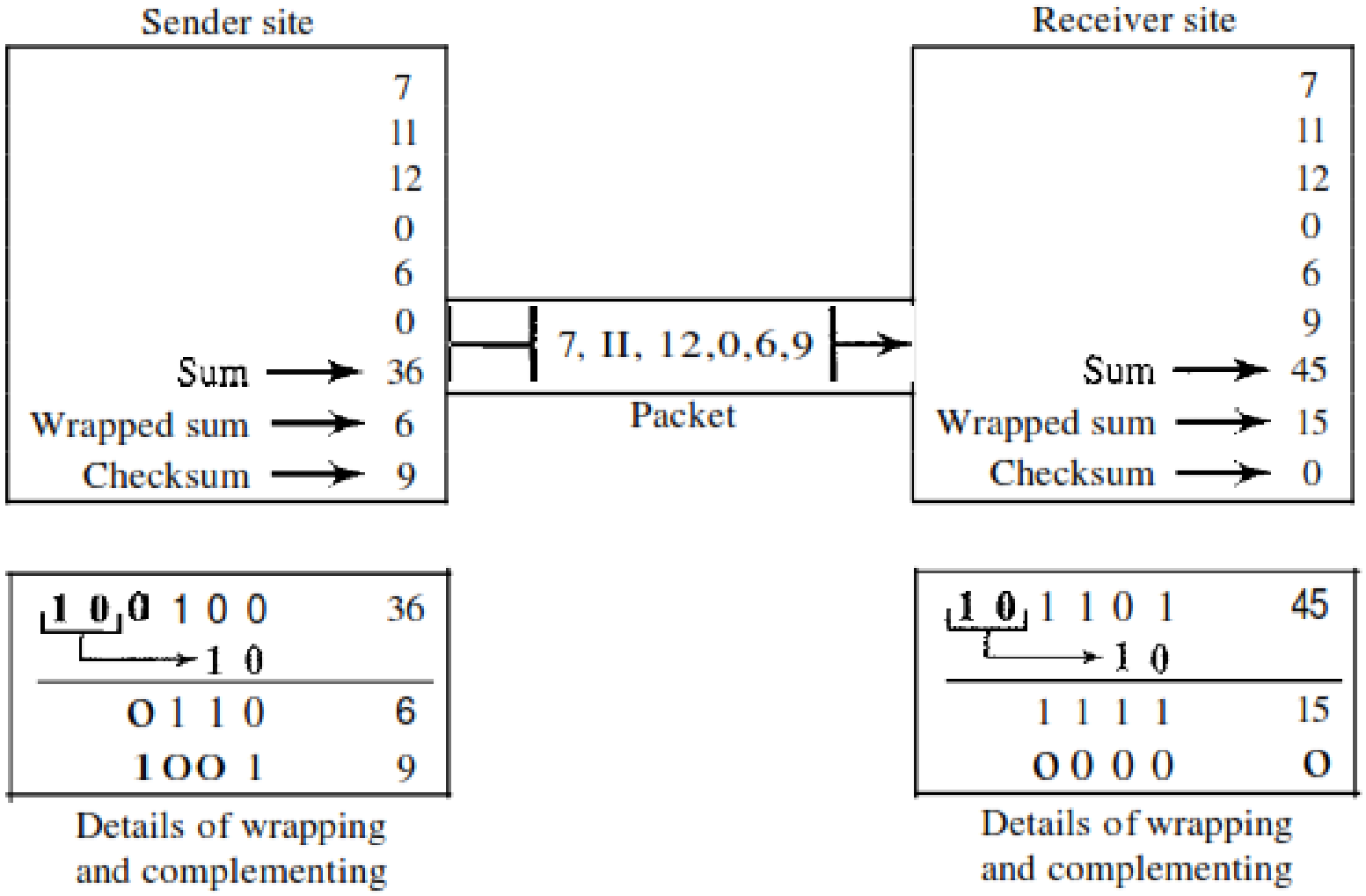
- Checksum is a calculated value that is used to determine the integrity of data.

Procedure to calculate the traditional checksum

Sender	*Receiver*
1. The message is divided into 16-bit words.	1. The message and the checksum are received.
2. The value of the checksum word is initially set to zero.	2. The message is divided into 16-bit words.
3. All words including the checksum are added using one's complement addition.	3. All words are added using one's complement addition.
4. The sum is complemented and becomes the checksum.	4. The sum is complemented and becomes the new checksum.
5. The checksum is sent with the data.	5. If the value of the checksum is 0, the message is accepted; otherwise, it is rejected.


Sender
Message
m bits
m bits
• • •
m bits
Generator
m bits
m bits
• • •
m bits
m bits
Message plus checksum
Receiver
Message
m bits
m bits
• • •
m bits
All 0's
[yes]
Discard
[no]
m bits
Checker
m bits
m bits
• • •
m bits
m bits
Message plus checksum

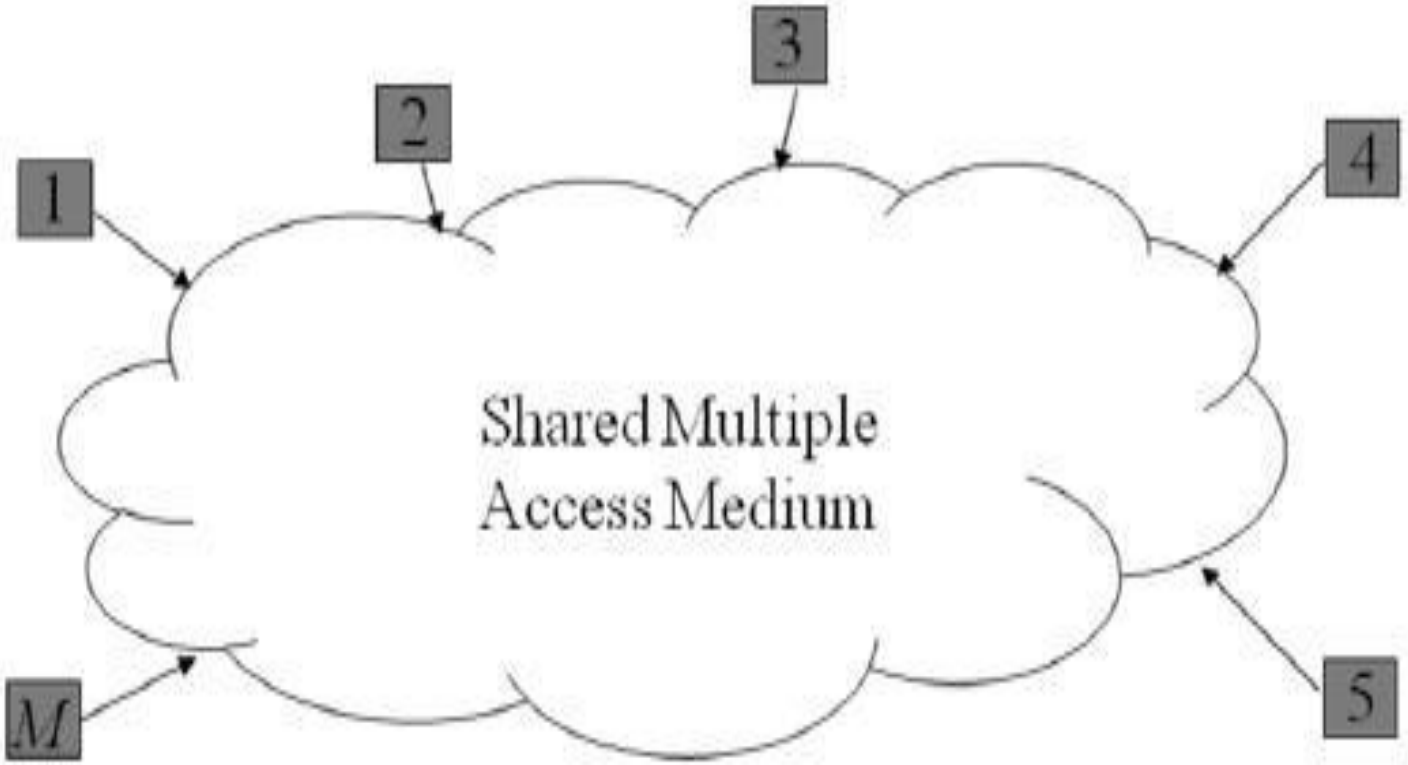
Example : Let the message to be transmitted be 7,11,12,0,6



MEDIA ACCESS CONTROL (MAC)

MEDIA ACCESS CONTROL (MAC)

- When **two or more nodes transmit data at the same time**, their **frames will collide and the link bandwidth is wasted** during collision.
- To coordinate the access of multiple sending / receiving nodes to the shared link, we **need a protocol to coordinate the transmission.**
- These protocols are called **Medium or Multiple Access Control (MAC) Protocols**. MAC belongs to the data link layer of OSI model
- MAC defines **rules for orderly access to the shared medium.**
- It tries to **ensure that no two nodes are interfering with each other's transmissions**, and deals with the situation when they do.


1
2
3
4
5
M
Shared Multiple
Access Medium

Issues involved in MAC

- The key issues involved are:
  - ***Where*** the control is exercised - refers to whether the control is exercised in a centralized or distributed manner
  - ***How*** the control is exercised - refers to in what manner the control is exercised

Goals of MAC

- Fairness in sharing
- Efficient sharing of bandwidth
- Need to avoid packet collisions at the receiver due to interference

MAC Management

- Medium allocation (collision avoidance)
- Contention resolution (collision handling)

MAC Types

- **Round-Robin:** – Each station is given opportunity to transmit in turns. Either a central controller polls a station to permit to go, or stations can coordinate among themselves.
- **Reservation: -** Station wishing to transmit makes reservations for time slots in advance. (Centralized or distributed).
- **Contention (Random Access)** : - No control on who tries; If collision occurs, retransmission takes place.

MECHANISMS USED

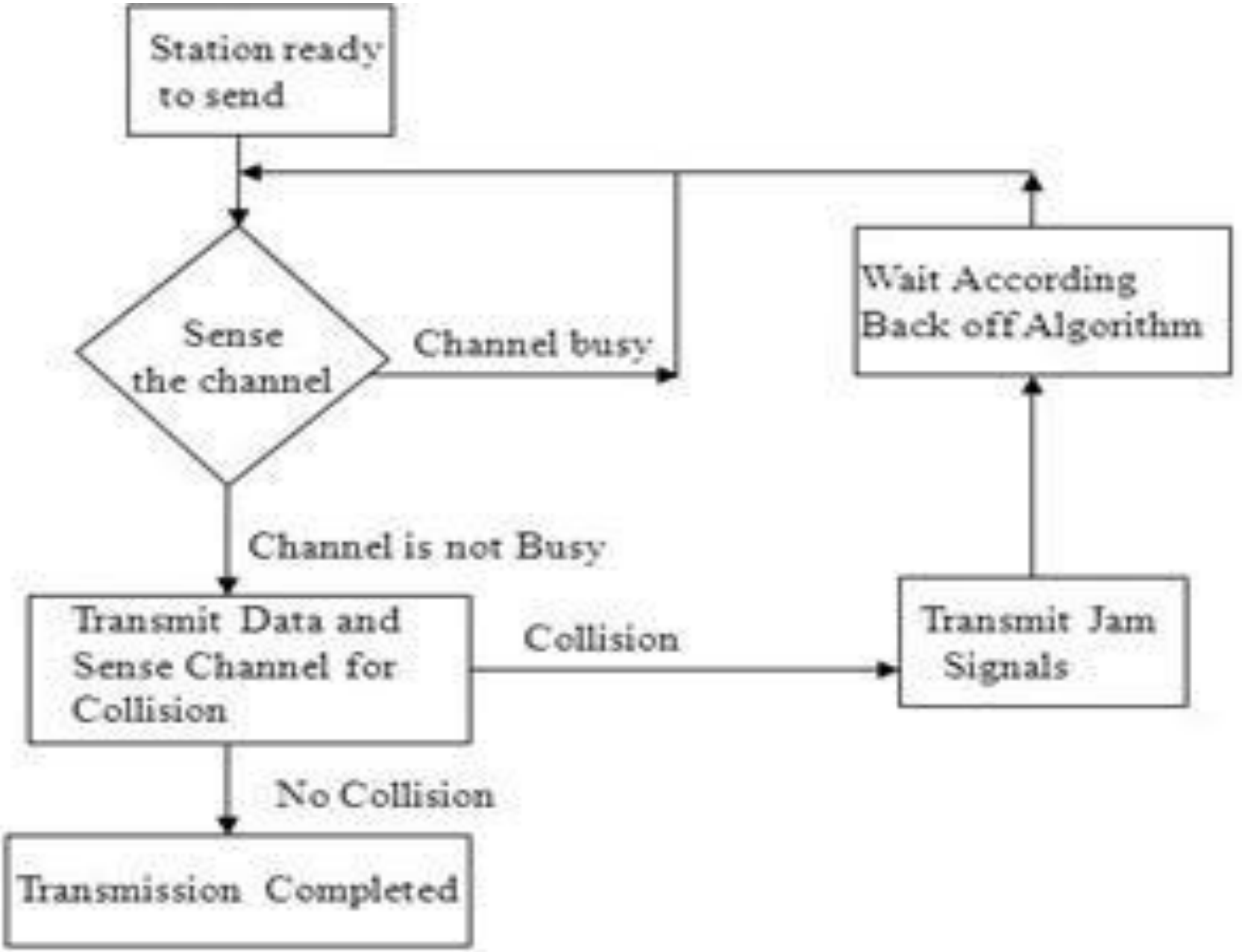
- **Wired Networks:**
  - **CSMA / CD** – Carrier Sense Multiple Access / Collision Detection
- **Wireless Networks:**
  - **CSMA / CA** – Carrier Sense Multiple Access / Collision Avoidance

CARRIER SENSE MULTIPLE ACCESS / COLLISION DETECTION (CSMA / CD)

- **Carrier Sense** in CSMA/CD means that all the nodes sense the medium to check whether it is idle or busy.
  - **If the carrier sensed is idle, then the node transmits the entire frame.**
  - **If the carrier sensed is busy, the transmission is postponed.**

- **Collision Detect** means that a node listens as it transmits and can therefore detect when a frame it is transmitting has collided with a frame transmitted by another node.

Flowchart of CSMA/CD Operation



Transmitter Algorithm in CSMA / CD

- Transmitter Algorithm defines the procedures for a node that senses a busy medium.

Three types of Transmitter Algorithm exist**.** They are:

i) Non-Persistent Strategy

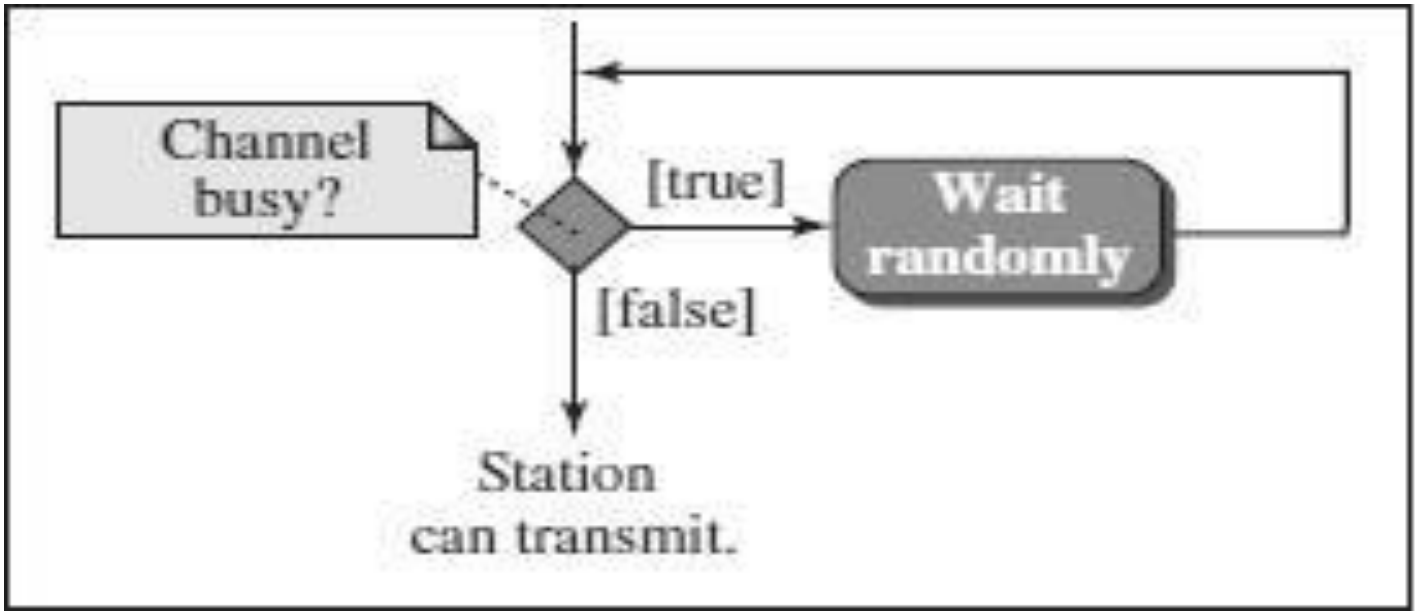
ii) Persistent Strategy :

a) 1-Persistent

b) P-Persistent

i) Non-Persistent Strategy

- In the non-persistent 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.



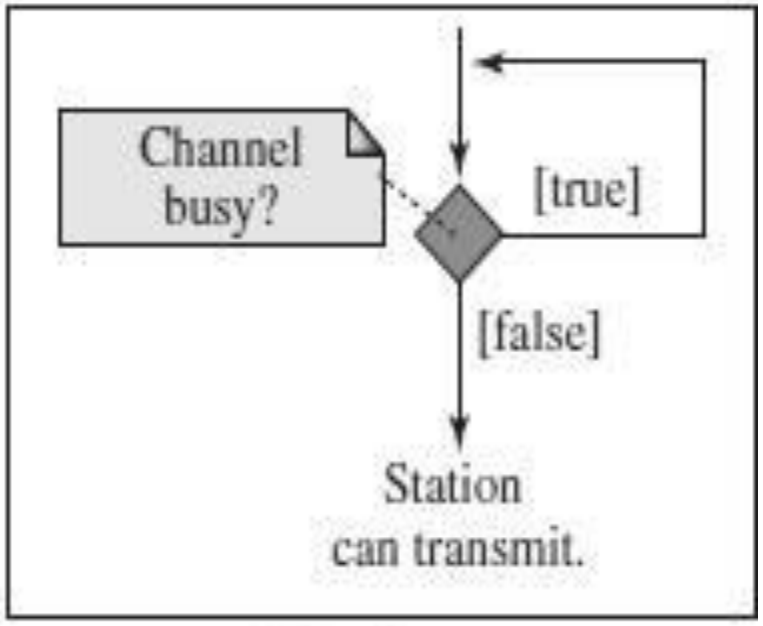
- The **non-persistent approach reduces the chance of collision because it is unlikely that two or more stations will wait the same amount of time and retry to send simultaneously.**

- However**, this method reduces the efficiency of the network** because **the medium remains idle when there may be stations with frames to send.**

ii) Persistent Strategy

a) 1-Persistent:

- 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.



b) P-Persistent

In this method, **after the station finds the line idle it follows these steps:**

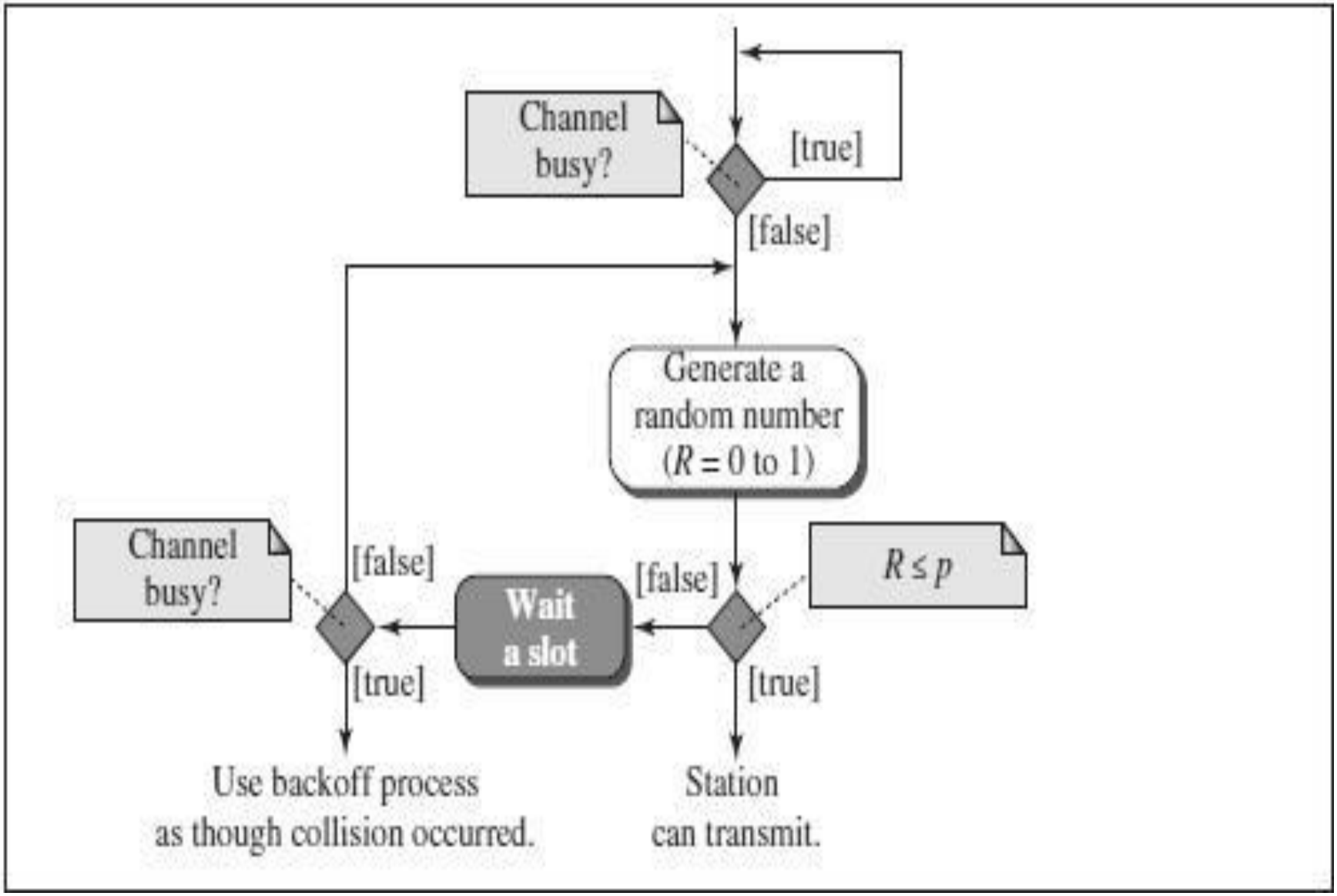
→ **With probability *p*,** the **station sends its frame.**

→ **With probability *q* = 1 – *p*,** the **station waits for the beginning of the next time slot** and **checks the line again.**

→ The **p-persistent method is used if the channel has time slots with a slot duration equal to or greater than the maximum propagation time.**

→The **p-persistent approach combines the advantages of the other two strategies.**

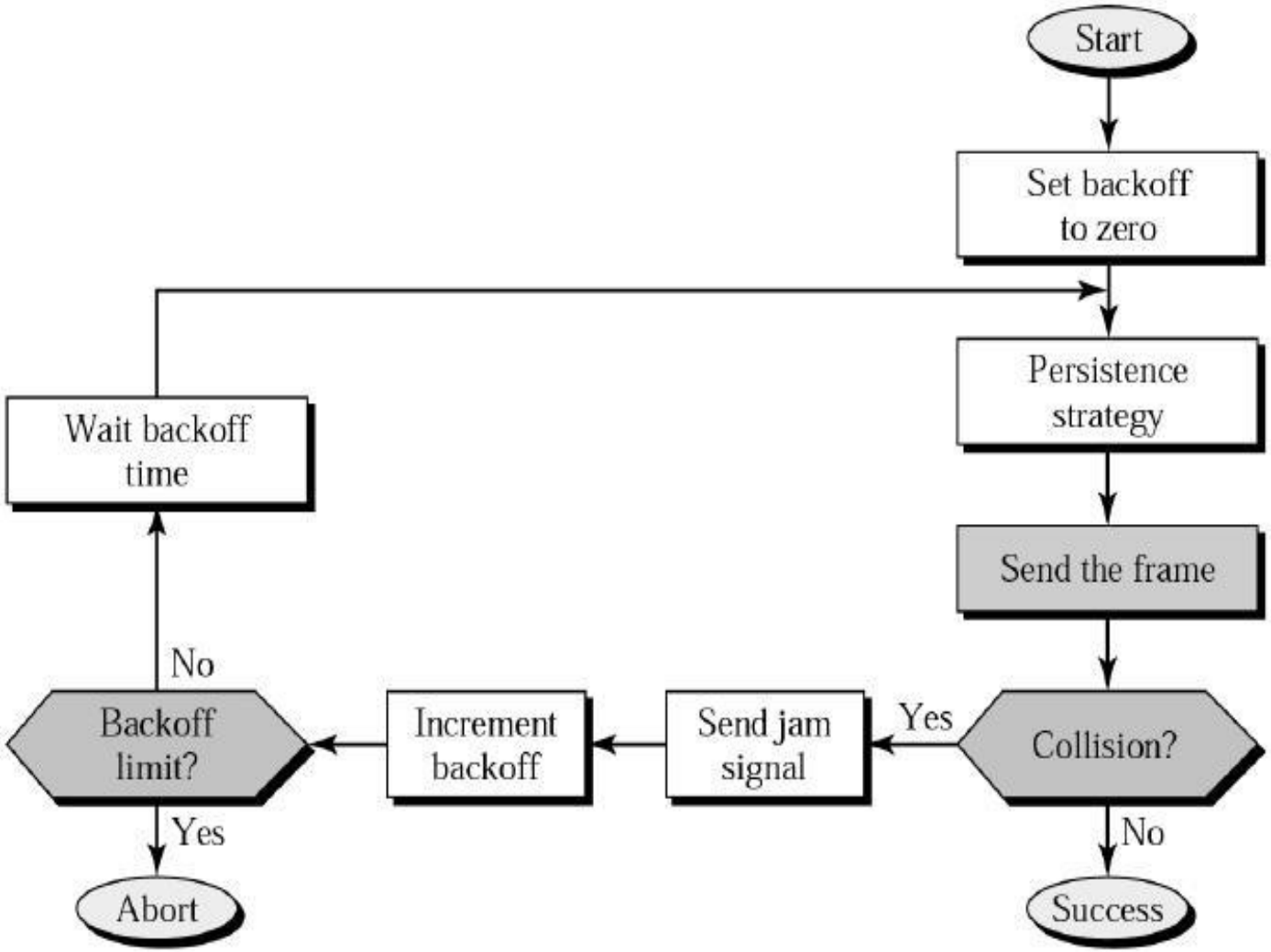
- **It reduces the chance of collision and improves efficiency**.


Channel busy?
[true]
[false]
Generate a random number (R = 0 to 1)
Channel busy?
[false]
Wait a slot
[false]
R ≤ p
[true]
[true]
Use backoff process as though collision occurred.
Station can transmit.

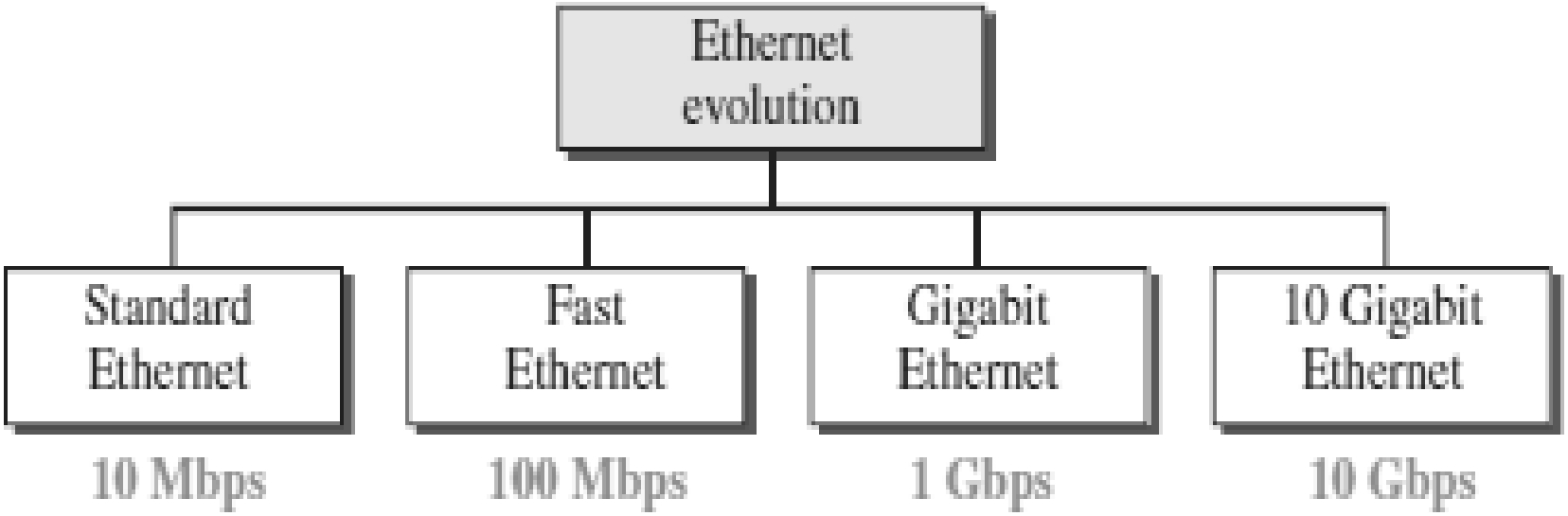
- **EXPONENTIAL BACK-OFF**
  - Once an adaptor has detected a collision and stopped its transmission,

    ➔ it waits a certain amount of time and tries again.
  - Each time it tries to transmit but fails,

    ➔ the **adaptor doubles the amount of time** it waits before trying again.
  - This strategy of **doubling the delay interval between each retransmission attempt** is a general technique known as **exponential back-off.**


Start
Set backoff to zero
Persistence strategy
Send the frame
Collision?
Yes
Send jam signal
Increment backoff
Backoff limit?
No
Wait backoff time
Yes
Abort
No
Success

EVOLUTION OF ETHERNET



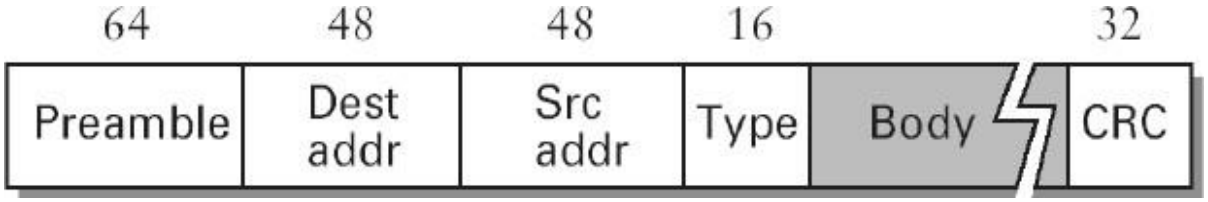
- **ACCESS METHOD/ PROTOCOL OF ETHERNET**

  ➔ The access method of Ethernet is CSMA/CD.

- **COLLISION DETECTION IN ETHERNET**
  - As the Ethernet supports collision detection, senders are able to determine a collision.
  - At the moment an adaptor detects that its frame is colliding with another, it first makes sure to transmit a **32-bit jamming sequence** along with the **64- bit preamble** (totally 96 bits) and then stops the transmission.
  - These **96 bits** are sometimes called **Runt Frame.**

FRAME FORMAT OF ETHERNET

The Ethernet frame is defined by the format



- The 64-bit ***preamble*** allows the receiver to synchronize with the signal; it is a sequence of alternating 0's and 1's.
- Both the ***source and destination*** hosts are identified with **a 48-bit *address.***
- The packet ***type*** field serves as the demultiplexing key.
- Each frame contains up to 1500 bytes of ***data(Body).***
- ***CRC*** is used for Error detection

Ethernet Addresses

- Every Ethernet **host has a unique Ethernet address** (48 bits – 6 bytes).
- Each number corresponds to 1 byte of the 6 byte address and is given by pair of hexadecimal digits.
- **Eg: 8:0:2b:e4:b1:2** is the representation of 00001000 00000000 00101011 11100100 10110001 00000010
- Each frame transmitted on an Ethernet is received by every adaptor connected to the Ethernet.
- In addition to ***unicast*** addresses an Ethernet address consisting of ***all 1s*** is treated as ***broadcast*** address.
- Similarly the address that has the ***first bit set to 1*** but it is not the broadcast address is called ***multicast*** address.

ADVANTAGES OF ETHERNET

Ethernets are successful because

- It is extremely ***easy to administer and maintain.***
- There are **no switches** that can fail,

→ **no routing or configuration tables** that have to be kept up-to-date, and

→ it is **easy to add a new host to the network**.

- It is ***inexpensive:*** Cable is cheap, and the only other cost is the network adaptor on each host.

Wireless LAN

WIRELESS LAN (IEEE 802.11)

- Wireless communication is one of the fastest-growing technologies.
- The demand for connecting devices without the use of cables is increasing everywhere.
- Wireless LANs can be found on college campuses, in office buildings, and in many public areas.

ADVANTAGES OF WLAN / 802.11

- **Flexibility:** **Within radio coverage**, nodes can access each other as radio waves can penetrate even partition walls.
- **Planning :** **No prior planning is required** for connectivity as long as devices follow standard convention
- **Design :** Allows to design and develop **mobile devices.**
- **Robustness :** **Wireless network can survive disaster**. If the devices survive, communication can still be established.

DISADVANTAGES OF WLAN / IEEE 802.11

- **Quality of Service :** Low bandwidth (1 – 20 Mbps), higher error rates due to interference, delay due to error correction and detection.
- **Cost :** Wireless LAN adapters are costly compared to wired adapters.
- **Proprietary Solution :** Due to slow standardization process, many solution are proprietary that limit the homogeneity of operation.
- **Restriction :** Individual countries have their own radio spectral policies. This restricts the development of the technology
- **Safety and Security :** Wireless Radio waves may interfere with other devices. Eg; In a hospital, radio waves may interfere with high-tech equipment.

TECHNOLOGY USED IN WLAN / IEEE 802.11

- WLAN's uses **Spread Spectrum (SS) technology.**
- The idea behind Spread spectrum technique is **to spread the signal over a wider frequency band than normal**, so as to minimize the impact of interference from other devices.
- There are **two types of Spread Spectrum**:
  - Frequency Hopping Spread Spectrum (FHSS)
  - Direct **S**equence Spread Spectrum (DSSS)

TOPOLOGY IN WLAN / 802.11

- WLANs can be built with either of the following **two topologies** /architecture:

i) Infra-Structure Network Topology

➔ **AP based Topology**

ii) Ad Hoc Network Topology

ARCHITECURE OF WLAN (IEEE 802.11)

ARCHITECURE OF WLAN (IEEE 802.11)

- The standard defines two kinds of services:

  i) Basic Service Set (BSS)

  ii) Extended Service Set (ESS)

Basic Service Set (BSS)

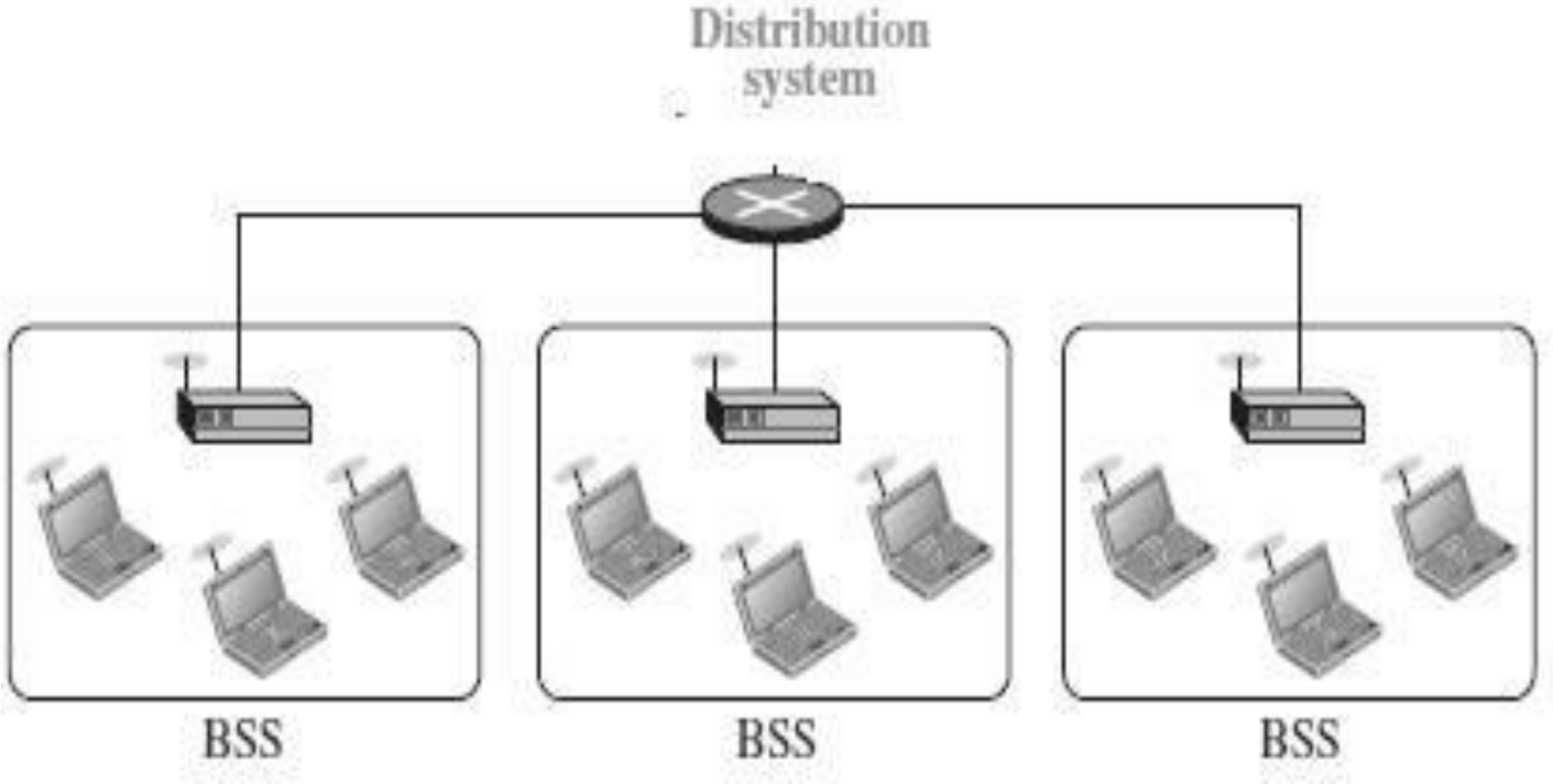
- IEEE 802.11 defines the **Basic Service Set (BSS)** as the building blocks of a wireless LAN.
- A BSS is made of stationary or mobile wireless stations and an **optional central base station**, known as the ***access point (AP)***.

Extended Service Set (ESS)

An extended service set (ESS) is made up of two or more BSSs with APs.

- In this case, the **BSSs are connected through a *distribution system***, which is a wired or a wireless network.
- The **distribution system connects the APs in the BSSs**.
- The ESS uses two types of stations: **mobile and stationary.**
- The mobile stations are normal stations inside a BSS.
- The **stationary stations are AP stations** that are part of a wired LAN.

Extended Service Set (ESS)



Station Types

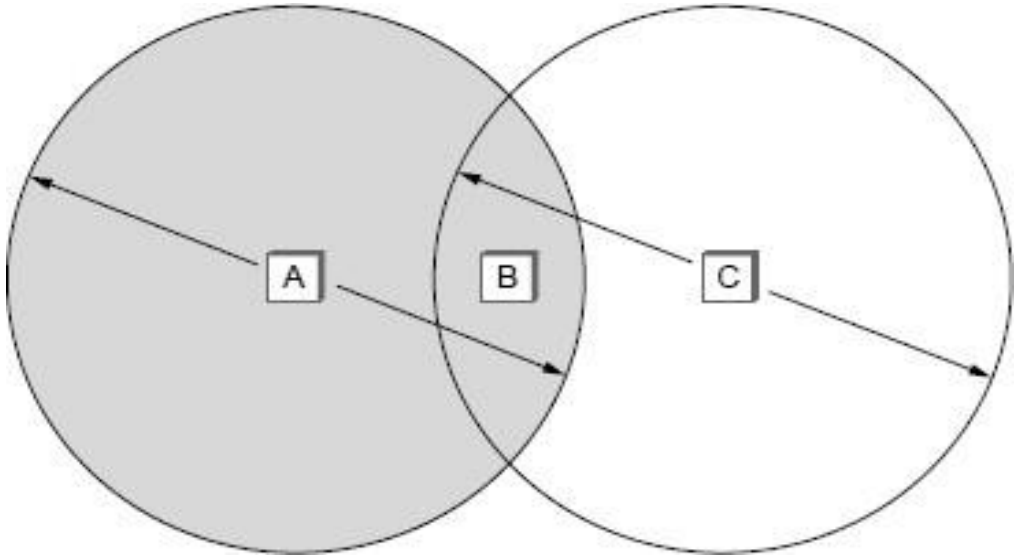
IEEE 802.11 defines **three types of stations** based on their mobility in a wireless LAN:

- ***No-transition*** - A station with **no-transition mobility is either stationary (not moving)** or **moving only inside a BSS.**
- ***BSS-transition*** - A station with **BSS-transition mobility can move from one BSS to another**, but the movement is confined inside one ESS
- ***ESS-transition*** - A station with ESS-transition mobility can **move from one ESS to another**.

COLLISION AVOIDANCE IN WLAN / 802.11

- Wireless protocol would follow exactly the same algorithm as the Ethernet—**Wait until the link becomes idle** before transmitting and **back off** should a collision occur.

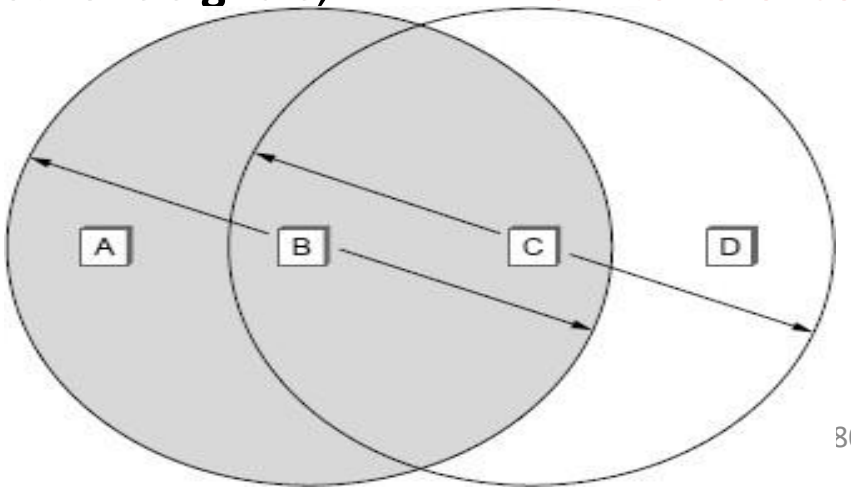
Hidden Node Problem



- Consider the situation shown in the Figure.
- Here A and C are both within range of B but not with each other.
- Suppose both A and C want to communicate with B and so they each send a frame to B.
- A and C are unaware of each other since their signals do not carry that far.
- These two **frames collide with each other at B, but neither A nor C is aware of this collision**.
- **A and C are said to be *hidden nodes* with respect to each other.**

Exposed Node Problem

- Each of the four nodes is able to send and receive signals that reach just the nodes to its immediate left and right.
- For example, **B can exchange frames with A and C but it cannot reach D,** while **C can reach B and D but not A.**
- Suppose **B is sending to A. Node C is aware of this communication because it hears B's transmission.**
- **If at the same time**, **C wants to transmit to node D.**
- It would be a mistake, however, for **C to conclude that it cannot transmit to anyone** just **because it can hear B's transmission.**
- This is **not a problem since C's transmission to D will not interfere with A's ability to receive from B**. This is called exposed problem.
- Although **B and C are exposed to each other's signals**, there is **no interference if B transmits to A while C transmits to D.**



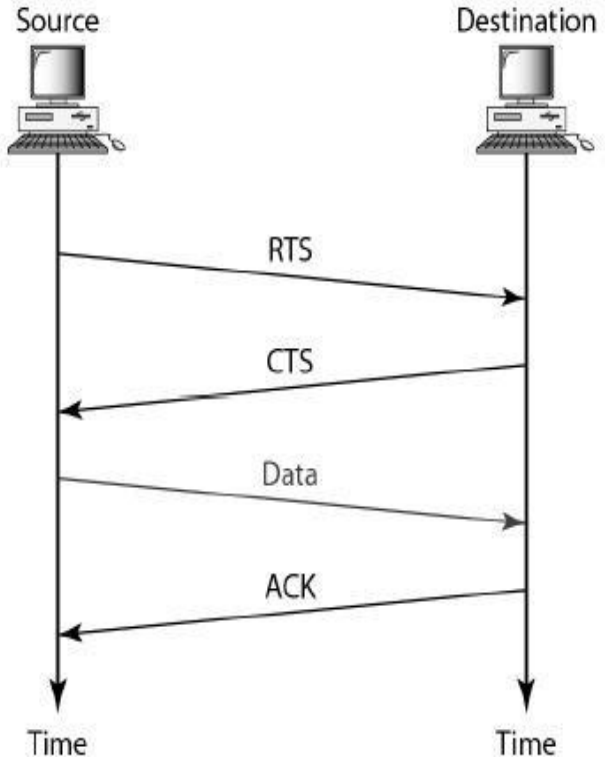
MULTIPLE ACCESS WITH COLLISION AVOIDANCE (MACA)

- **MACA is used to avoid collisions caused by the** hidden terminal problem **and** exposed terminal problem.
- MACA uses short **signaling packets** called **Request-To-Send (RTS)** and **Clear-To-Send (CTS)** for collision avoidance.
- The RTS and CTS signals helps us **to determine who else is in the transmission range** or **who is busy.**
- When a sender wants to transmit, it **sends a signal called RTS.**
- If the receiver allows the transmission, it **replies to the sender a signal called CTS.**

MULTIPLE ACCESS WITH COLLISION AVOIDANCE (MACA)

- Any **node that sees the CTS frame knows that it is close to the receiver**, and therefore **cannot transmit for the period of time**.
- Any **node that sees the RTS frame but not the CTS frame is not close enough to the receiver** to interfere with it, and so is **free to transmit**.
- The Signaling packets RTS and CTS contains information such as
  - **sender address**
  - **receiver address**
  - **length of the data to be sent/received**

- The **receiver sends an ACK to the sender** after successfully receiving a frame.
- All **nodes must wait for this ACK before trying to transmit.**
- When two or more nodes detect an idle link and **try to transmit an RTS frame at the same time, their RTS frames will collide** with each other.
- ***802.11 do not support collision detection,*** but instead, the **senders realize the collision has happened when they do not receive the CTS frame after a period of time**.
- **Each node waits for a random amount of time before trying again**.
- The amount of time a given node delays is defined by **exponential back-off algorithm.**



FRAME FORMAT OF WLAN / 802.11

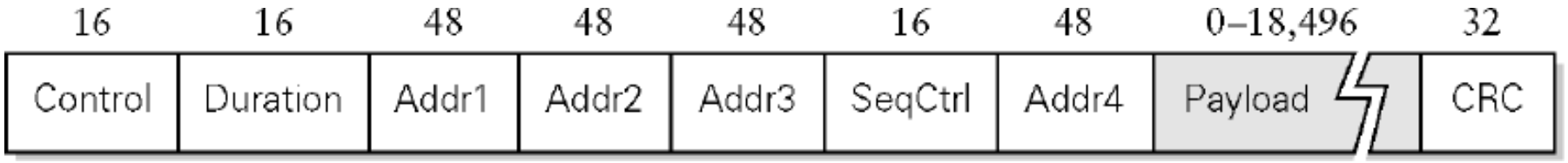
- ***Control field*** - contains three subfields :

  → ***Type field*** - Indicates whether the **frame carries Data, RTS or CTS**

  → ***To DS*** - Data frame sent to DS (Distribution System)

  → ***From DS –*** ACK sent from DS

- When **both the DS bits are set to 0,** it indicates that one **node is sending directly to another.**
- **Addr l** identifies the target node and **Addr2** identifies the source node.
- When **both the DS bits are set to 1**, it indicates that **one node is sending the message to another indirectly using the DS.**
- ***Duration*** **-** contains the duration of time the medium is occupied by the nodes.



***Addr* l** - identifies the final original destination

Addr 2 - identifies the immediate sender (the one that forwarded the frame from the distribution system to the ultimate destination)

Addr 3 - identifies the intermediate destination (the one that accepted the frame from a wireless node and forwarded it across the distribution system)

Addr 4 **-** identifies the original source

Sequence Control - to avoid duplication of frames sequence number is assigned to each frame

Payload **-** Data from sender to receiver

CRC **-** used for Error detection of the frame.

BLUETOOTH (IEEE 802.15)

BLUETOOTH (IEEE 802.15)

- A **Bluetooth is an ad hoc network**, which means that the network is formed spontaneously.
- Bluetooth is a wireless LAN technology designed **to connect devices of different functions such as telephones, notebooks, computers (desktop and laptop), cameras, printers**, when they are at a short distance from each other.
- Bluetooth technology is the implementation of a protocol defined by the IEEE 802.15 standard.
- The standard defines a **Wireless Personal-Area Network (WPAN)**
- Bluetooth operates in the 2.4 GHz Unlicensed ISM band.
- The range for Bluetooth communication is **0 to 30 feet (10 meters).**

BLUETOOTH (IEEE 802.15)

- This **distance can be increased to 100 meters by amplifying the power**.
- Bluetooth links have **typical bandwidths around 1 to 3 Mbps.**
- Upto **eight devices can be connected** through Bluetooth.
- One device will function as a **Master and the other seven devices will function as slaves**.
- Bluetooth uses **Frequency Hopping Spread Spectrum (FHSS) to avoid any interference.**

Bluetooth supports two kinds of links:

i) **Asynchronous Connectionless** (ACL) links - for data

ii) **Synchronous Connection oriented** (SCO) links - for audio/voice

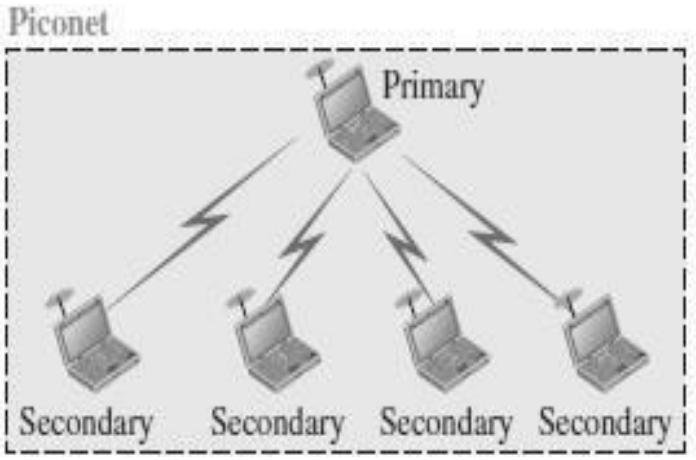
BLUETOOTH ARCHITECTURE

- Bluetooth defines two types of networks: **Piconet** and **Scatternet.**

PICONET

- The basic Bluetooth network configuration is called a **Piconet**
- A Piconet is a **collection of eight bluetooth devices** which are synchronized.
- One device in the piconet can act as **Primary (M*aster*)**, all other devices connected to the master act as **Secondary (Slaves).**
- All the **secondary stations synchronize their clocks and hopping sequence with the primary.**
- Any communication is between the primary/master and a secondary/slave.
- The **communication** between the primary and secondary stations **can be one-to-one or one-to-many**.
- The **slaves do not communicate directly with each other.**

• The devices in a piconet can be in any one of the **three types / states**. They are



i) Active Device / State

→ **Connected to the piconet and participates** in the communication.

→ Can be a **Master or a Slave** device.

→ All active devices are **assigned a 3-bit address** (**AMA-Active Member Address**).

ii) Parked Device / State

→ **Connected to the piconet**, but does **not actively participate** in the communication.

→ More than **200 devices can be parked**.

→ All parked devices use an **8-bit parked member address (PMA).**

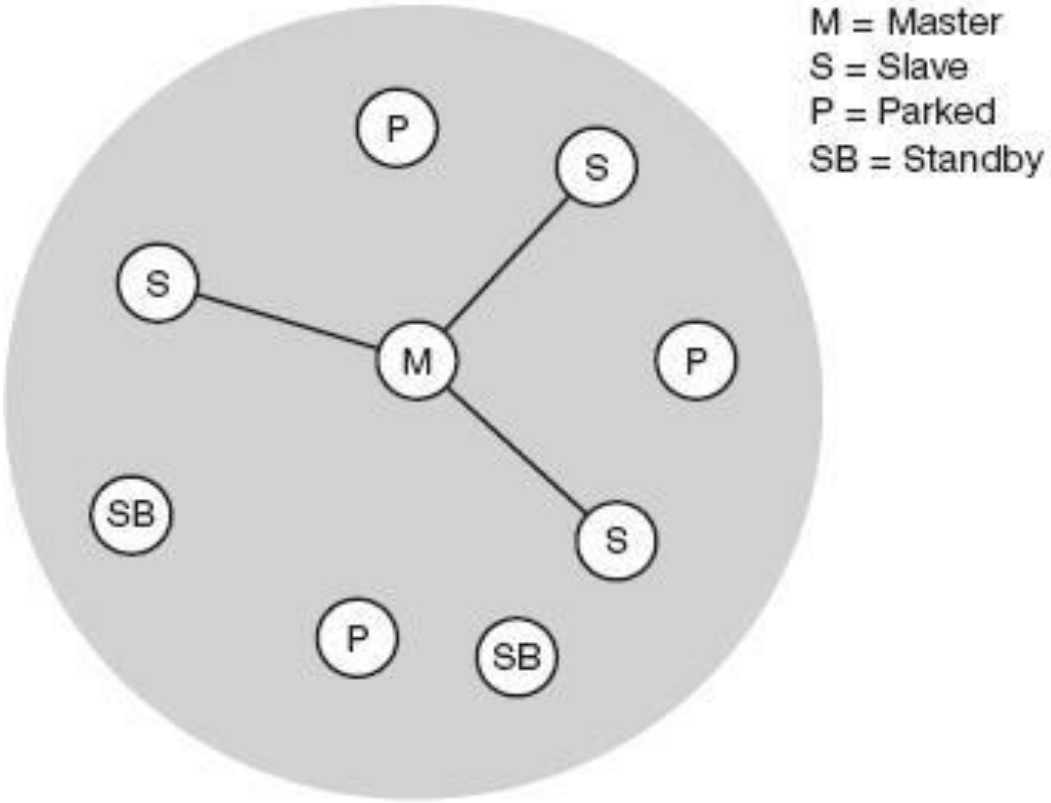
iii) Stand-by Device / State

→ **Not connected to the piconet**.

→ They **do not participate in the piconet** currently but **may take part at a later time.**

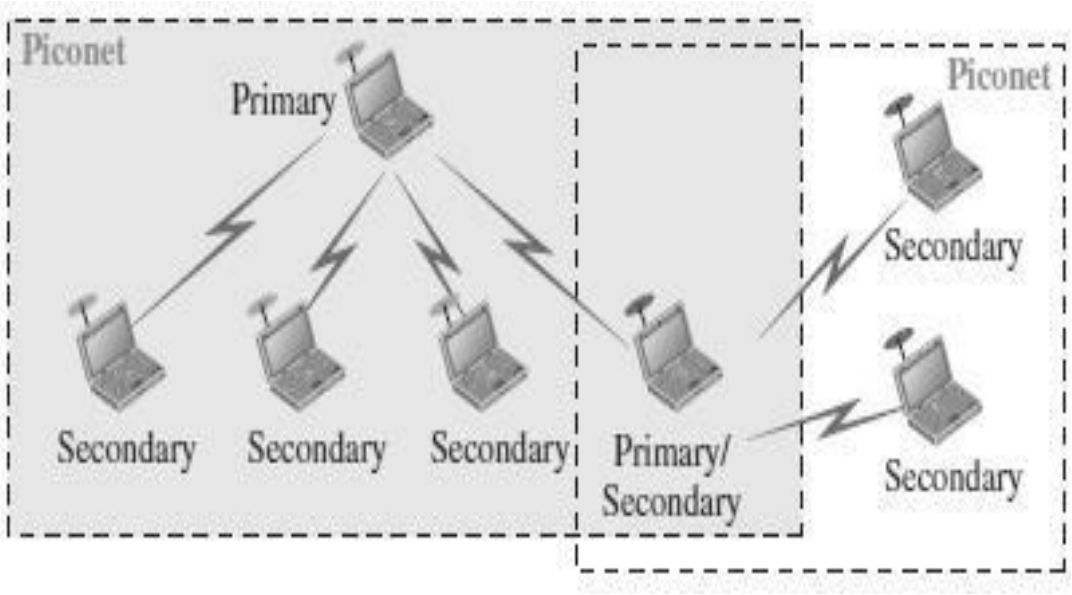
→ **Devices in stand-by do not need an address.**

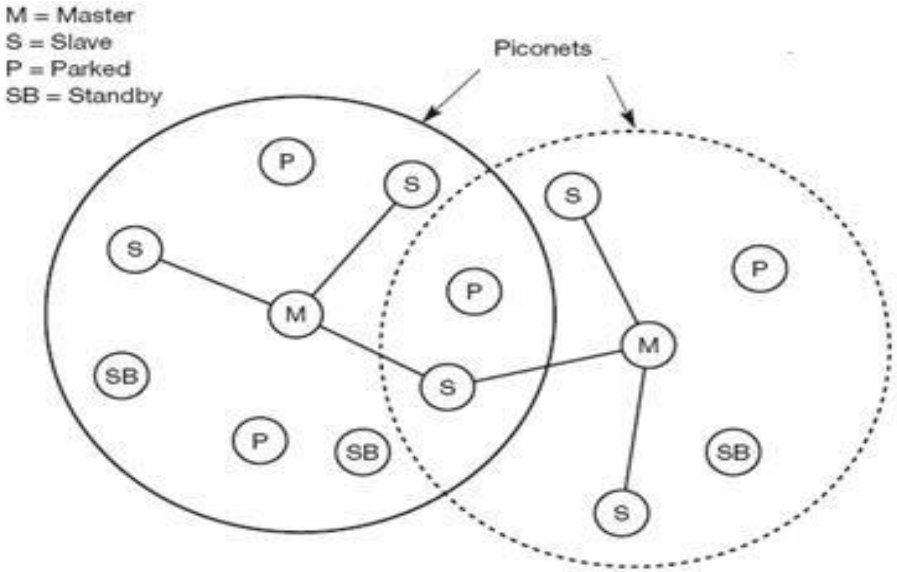
- **If a parked device wants to communicate and there are already seven active slaves, one slave has to switch to park state to allow the parked device** to switch to active state.



SCATTERNET

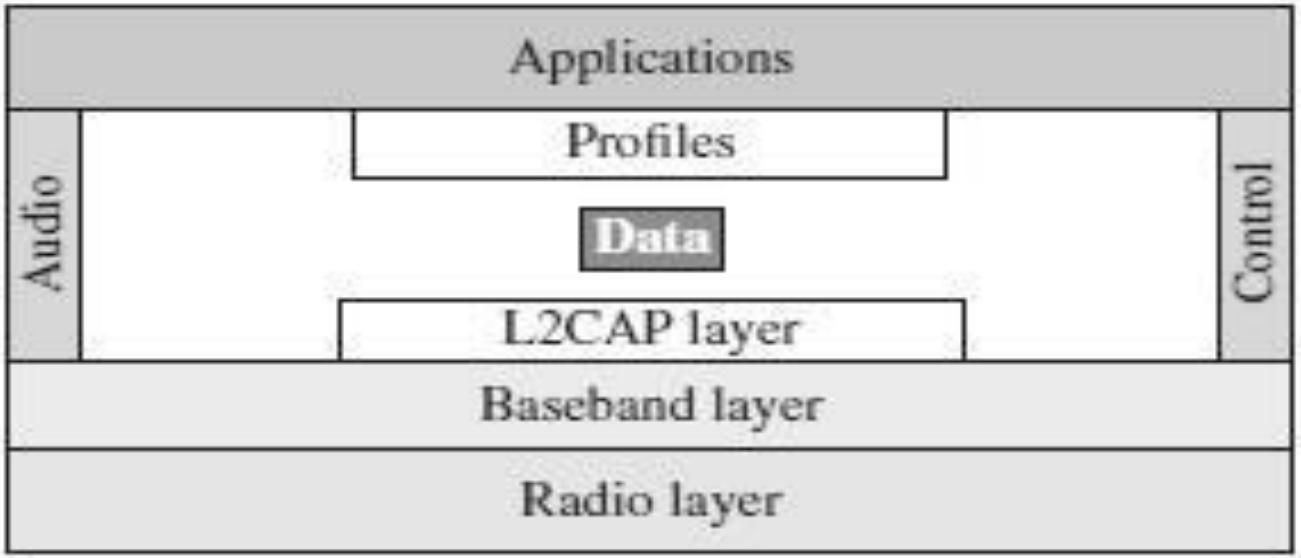
- **Piconets can be combined to form what is called a scatternet.**
- Many **piconets with overlapping coverage** can exist simultaneously, called Scatternet.
- A secondary station in one piconet can be the primary in another piconet.
- **This station can receive messages from the primary in the first piconet (as a secondary)** and, acting as a primary, deliver them to secondaries in the second piconet.
- A station can be a member of two piconets.
- In the example given below, there are two piconets, in which one slave participates in two different piconets.
- **Master of one piconet cannot act as the master of another piconet.**
- But the **Master of one piconet can act as a Slave** in another piconet


Piconet
Primary
Secondary
Secondary
Secondary
Primary/
Secondary
Piconet
Secondary
Secondary


M = Master
S = Slave
P = Parked
SB = Standby
Piconets
P
S
S
S
P
M
P
M
SB
S
P
SB
SB
S

BLUETOOTH LAYERS

- **Radio Layer**
  - The radio layer is **roughly equivalent to the physical layer** of the Internet model.
  - Bluetooth uses the **frequency-hopping spread spectrum (FHSS)** method in the physical layer to avoid interference from other devices or other networks.
  - Bluetooth **hops 1600 times per second**, which **means that each device changes its modulation frequency 1600 times per second**.

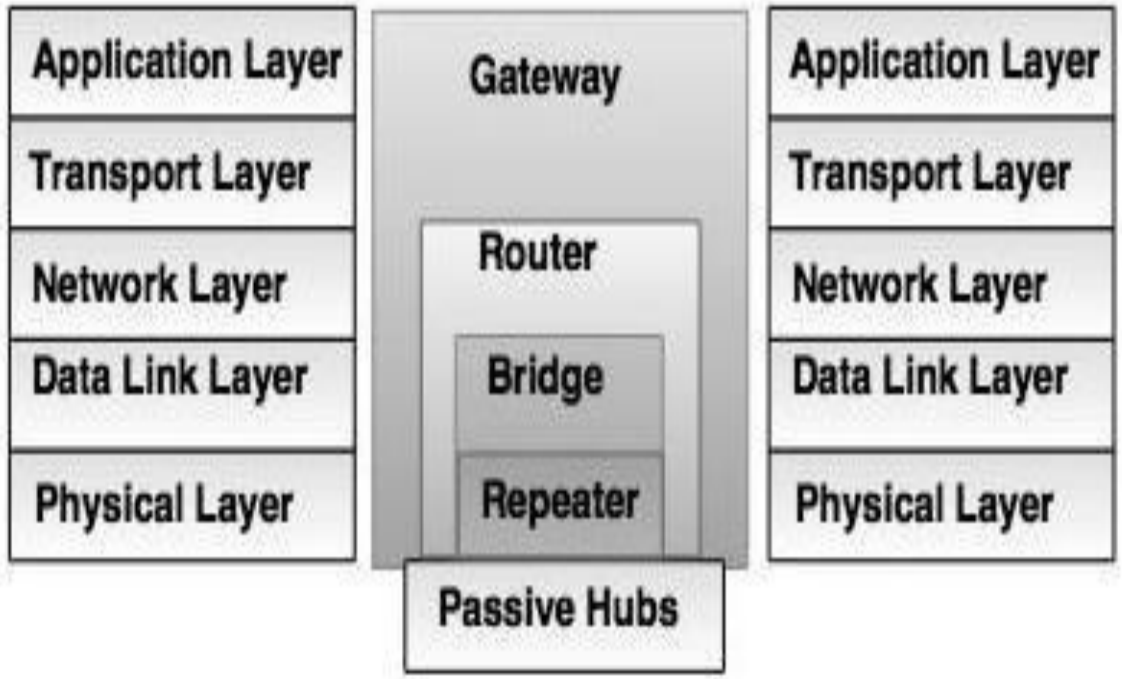


- **Baseband Layer**
  - The baseband layer is roughly **equivalent to the MAC sublayer** in LANs.
  - The **access method is TDMA.**
  - The primary and secondary stations communicate with each other using time slots. The **length of a time slot is exactly 625 µs**.
  - During that time, a primary sends a frame to a secondary, or a secondary sends a frame to the primary.

CONNECTING DEVICES

CONNECTING DEVICES

- Connecting devices are used **to connect hosts together to make a network** or to connect networks together to make an internet.
- Connecting **devices can operate in different layers** of the Internet model.



- Connecting devices are divided into **five different categories on the basis of layers** in which they operate in the network.

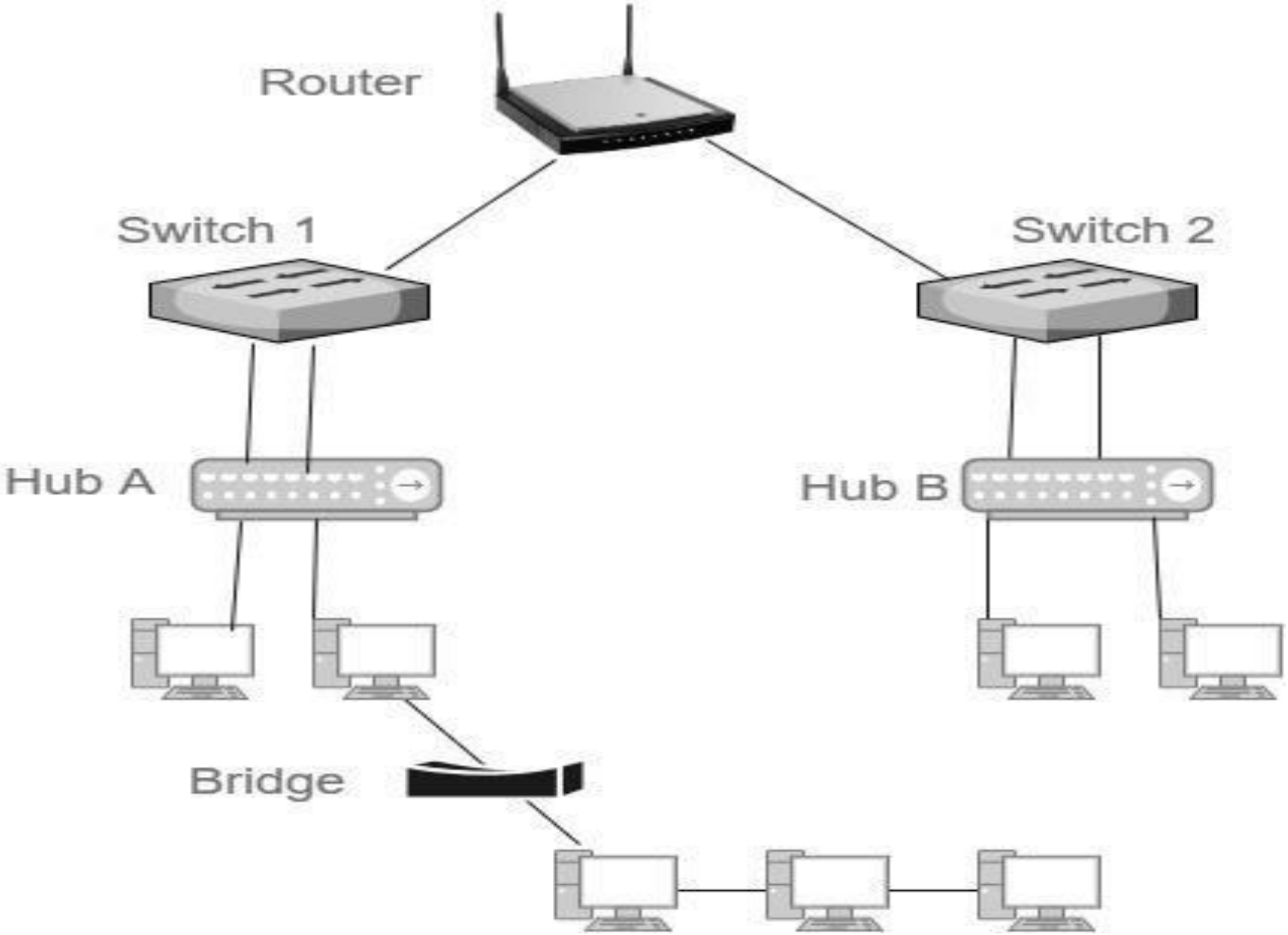
i) Devices which operate below the physical layer - **Passive hub**.

ii) Devices which operate at the physical layer - **Repeater**.

iii) Devices which operate at the physical and data link layers - **Bridge**.

iv) Devices which operate at the physical layer, data link layer and network layer – **Router**.

v) Devices which operate at all five layers - **Gateway**.

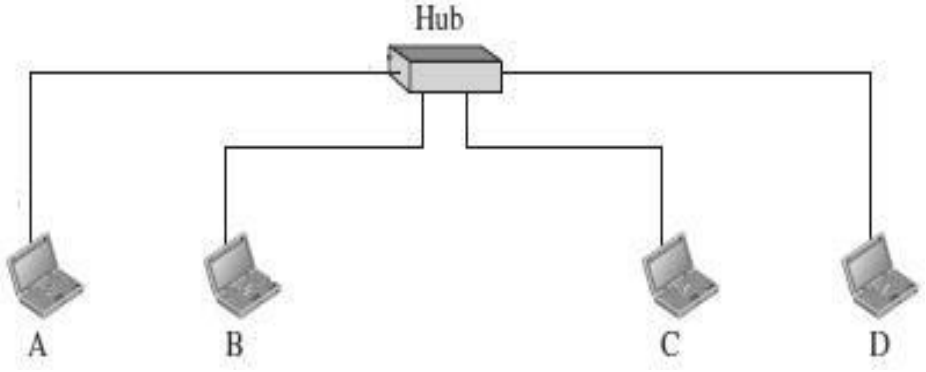

Router
Switch 1
Switch 2
Hub A
Hub B
Bridge

HUBS

– Several networks need a **central location to connect media segments together.** These central locations are **called as hubs**.

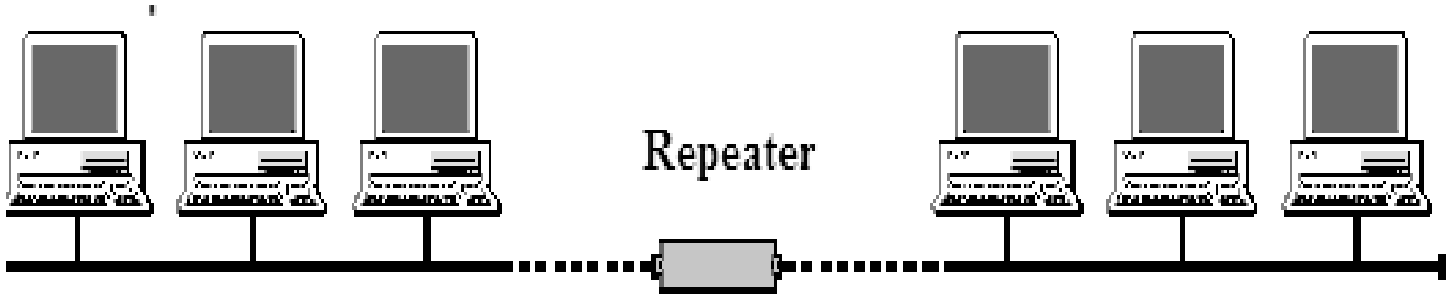
The three types of hubs are:

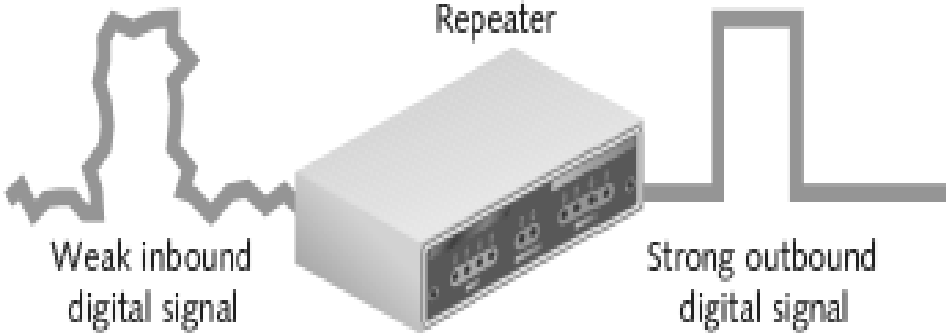
- **Passive hub**
  - It is a connector, which connects wires coming from the different branches.
  - By using passive hub, each computer can receive the signal which is sent from all other computers connected in the hub.
- **Active Hub**
  - It is a **multiport repeater, which can regenerate the signal**.
  - It is used to create connections between two or more stations in a physical star topology.
- **Intelligent Hub**
  - Intelligent hub contains a program of network management and intelligent path selection.



REPEATERS

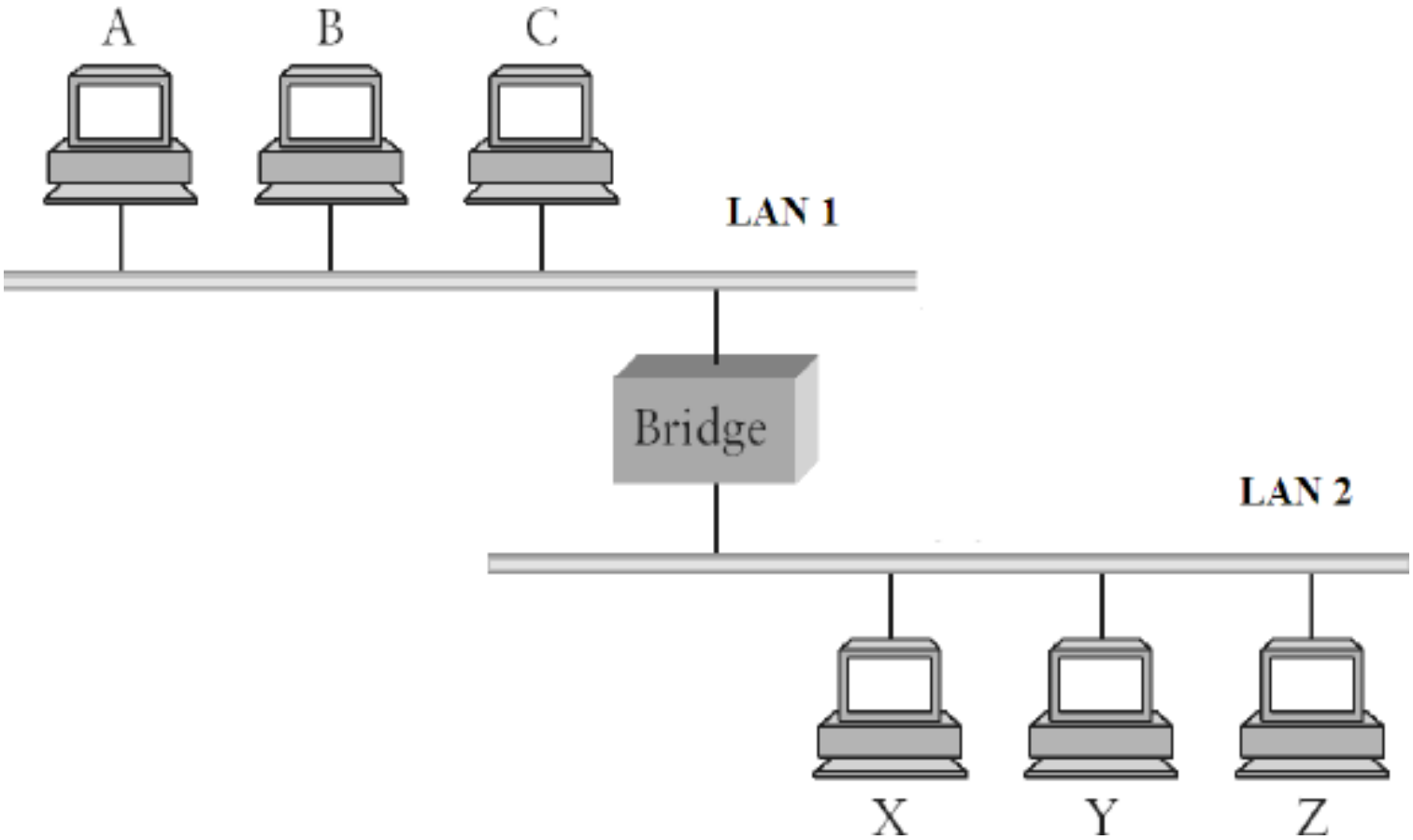
- A repeater receives the signal and it regenerates the signal in original bit pattern before the signal gets too weak or corrupted.
- It is used to extend the physical distance of LAN.
- Repeater works on physical layer.
- A repeater has no filtering capability.
- A repeater is implemented in computer networks to expand the coverage area of the network, repropagate a weak or broken signal and or service remote nodes.
- Repeaters **amplify the received/input signal** to a higher frequency domain so that it is reusable, scalable and available.
- Repeaters are also known as **signal boosters** or **range extender.**
- A repeater **cannot connect two LANs**, **but it connects two segments of the same LAN.**


Repeater


Repeater
Weak inbound
digital signal
Strong outbound
digital signal

BRIDGES

- Bridges operate in physical layer as well as data link layer.
- **As a physical layer device,** they regenerate the receive signal.
- **As a data link layer device**, the bridge checks the physical (MAC) address (of the source and the destination) contained in the frame.
- The **bridge has a filtering feature.**
- It can check the destination address of a frame and decides, if the **frame should be forwarded or dropped.**
- Bridges are used **to connect two or more LANs** working on the same protocol.


A
B
C
LAN 1
Bridge
LAN 2
X
Y
Z

Types of Bridges

Transparent Bridges

- These are the bridge in which the **stations are completely unaware of the bridge's existence** i.e. whether or not a bridge is added or deleted from the network , reconfiguration of the stations is unnecessary.

Source Routing Bridges

- In these bridges, **routing operation is performed by source station** and the frame specifies which route to follow.

Translation Bridges

- These bridges **connect networks with different architectures**, **such as Ethernet and Token Ring**. These bridges appear as:

  → Transparent bridges to an Ethernet host

  → Source-routing bridges to a Token Ring host

SWITCHES

- A switch is a small hardware device which is **used to join multiple computers together with one local area network (LAN).**
- A switch is a mechanism that allows us to interconnect links to form a large network.
- Switch is data **link layer device.**
- A switch is a **multi port bridge with a buffer**.
- Switches are used to **forward the packets based on MAC addresses**.
- It is operated in **full duplex mode.**
- **Packet collision is minimum** as it directly communicates between source and destination.
- It **does not broadcast the message** as it **works with limited bandwidth.**

- A **switch's primary job** is to receive incoming packets on one of its links and **to transmit them on some other link.**
- A Switch is used to **transfer the data only to the device that has been addressed.**
- Input ports receive stream of packets, analyzes the header, **determines the output port and passes the packet** onto the fabric.
- Ports contain buffers to hold packets before it is forwarded.
- **If buffer space is unavailable**, then packets are dropped.

- If packets at several input ports queue for a single output port, then only one of them is forwarded.

Types of Switch

- **Two- Layer Switch**
  - The two-layer switch **performs at the physical and the data link layer.**
  - It is a bridge with **many ports and design allows faster performance.**
  - A bridge is used **to connect different LANs together**.
  - The two- layer switch **can make a filtering decision** bases on the MAC address of the received frame. However, two- layer switch **has a buffer which holds the frame for processing**.
- **Three- Layer Switch**
  - The three-layer **switch is a router.**
  - The switching fabric in a three-layer **allows a faster table lookup and forwarding mechanism.**

ROUTERS

- A router is a **three-layer device.**
- It operates in the physical, data-link, and network layers.
- **As a physical-layer device**, it regenerates the signal it receives.
- **As a link-layer device**, the router checks the physical addresses (source and destination) contained in the packet.
- **As a network-layer device,** a router checks the network-layer addresses.
- A router is a device like a switch that **routes data packets based on their IP addresses.**

ROUTERS (Contd…)

- A router **can connect networks.**
- A router **connects the LANs and WANs on the internet**.
- A router is an internetworking device.
- It connects independent networks to form an internetwork.
- The **key function of the router is** to determine the shortest path to the destination.
- **Router has a routing table**, which **is used to make decision on selecting the route.**
- The **routing table is updated dynamically** based on which they make decisions on routing the data packets.

GATEWAY

- A gateway is a device, which **operates in all five layers of the internet** or **seven layers of OSI model.**
- It is usually a combination of hardware and software.
- Gateway **connects two independent networks.**
- Gateways are generally more complex than switch or router.
- Gateways basically **works as the messenger agents** that take data from one system, interpret it, and transfer it to another system.
- Gateways are also called **protocol converters**
- A gateway **accepts a packet formatted for one protocol** and **converts it to a packet formatted to another protocol** before forwarding it.
- The gateway must adjust the data rate, size and data format.