UNIT II

Channelization Protocols

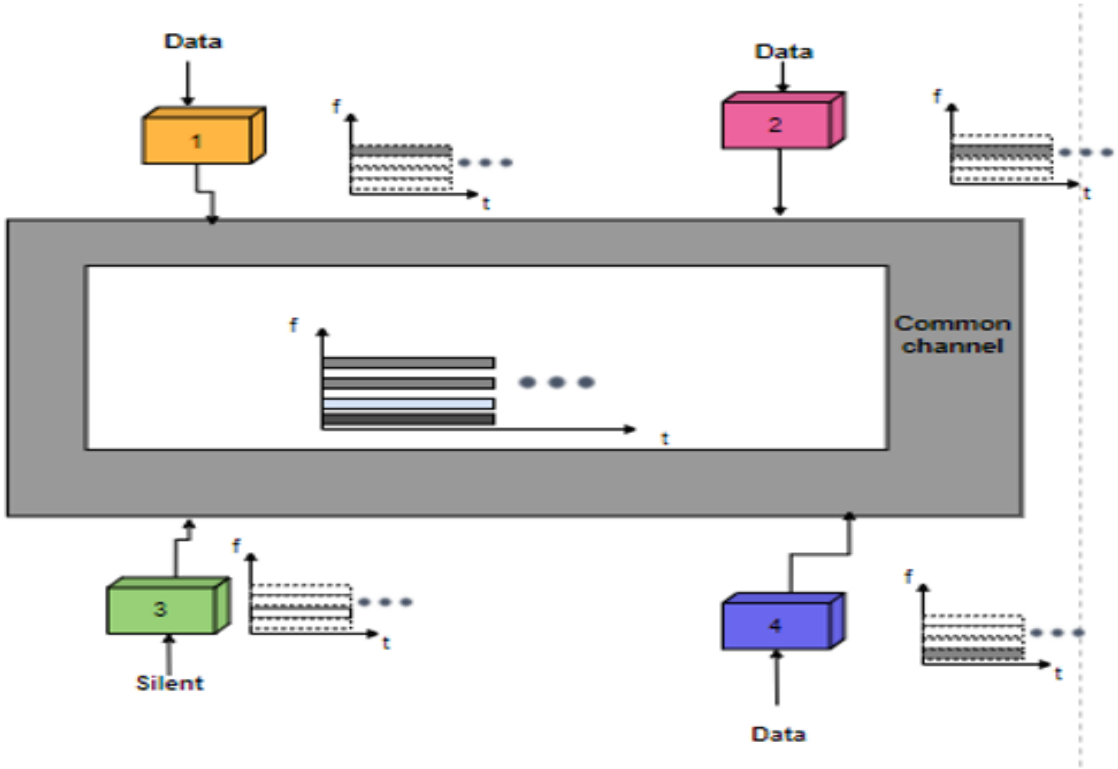
•Channelization Protocols are broad classified as follows:

1. FDMA(Frequency-Division Multiple Access)
2.TDMA(Time-Division Multiple Access)
3.CDMA(Code-Division Multiple Access)

1. Frequency-Division Multiple Access

- With the help of this technique, the available bandwidth is divided into frequency bands.
- Each station is allocated a band in order to send its data. Or in other words, we can say that each band is reserved for a specific station and it belongs to the station all the time.
- Each station makes use of the bandpass filter in order to confine the frequencies of the transmitter.
- In order to prevent station interferences, the allocated bands are separated from one another with the help of small guard bands.

FDMA

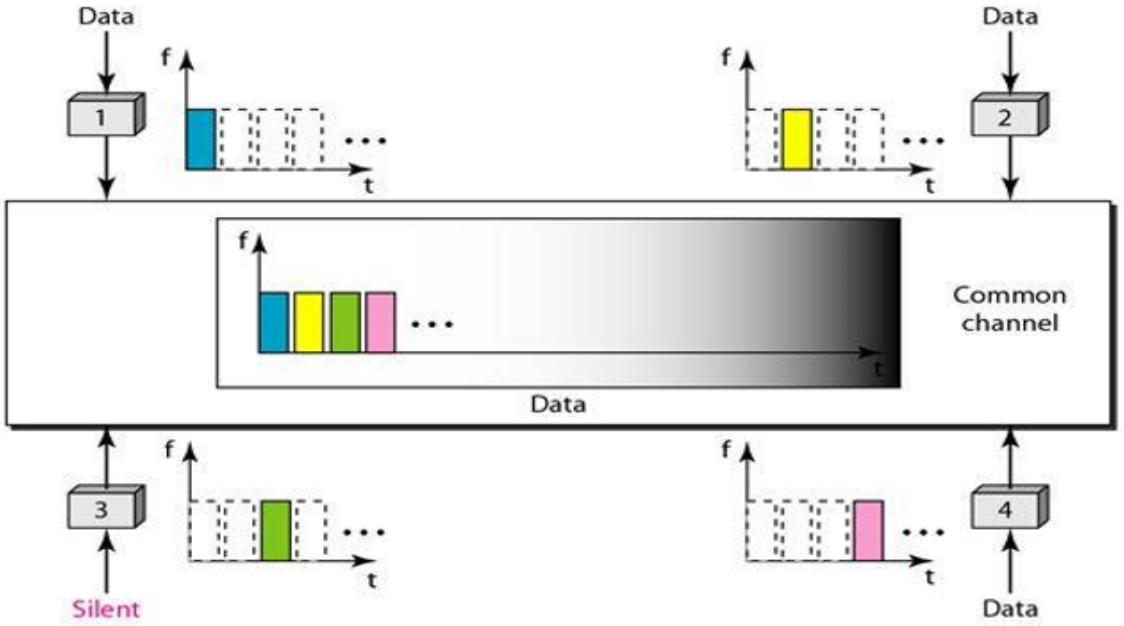


Time-Division Multiple Access

- Time-Division Multiple access is another method to access the channel for shared medium networks.
- With the help of this technique, the stations share the bandwidth of the channel in time.
- A time slot is allocated to each station during which it can send the data.
- Data is transmitted by each station in the assigned time slot.
- There is a problem in using TDMA and it is due to TDMA the synchronization cannot be achieved between the different stations.

TDMA

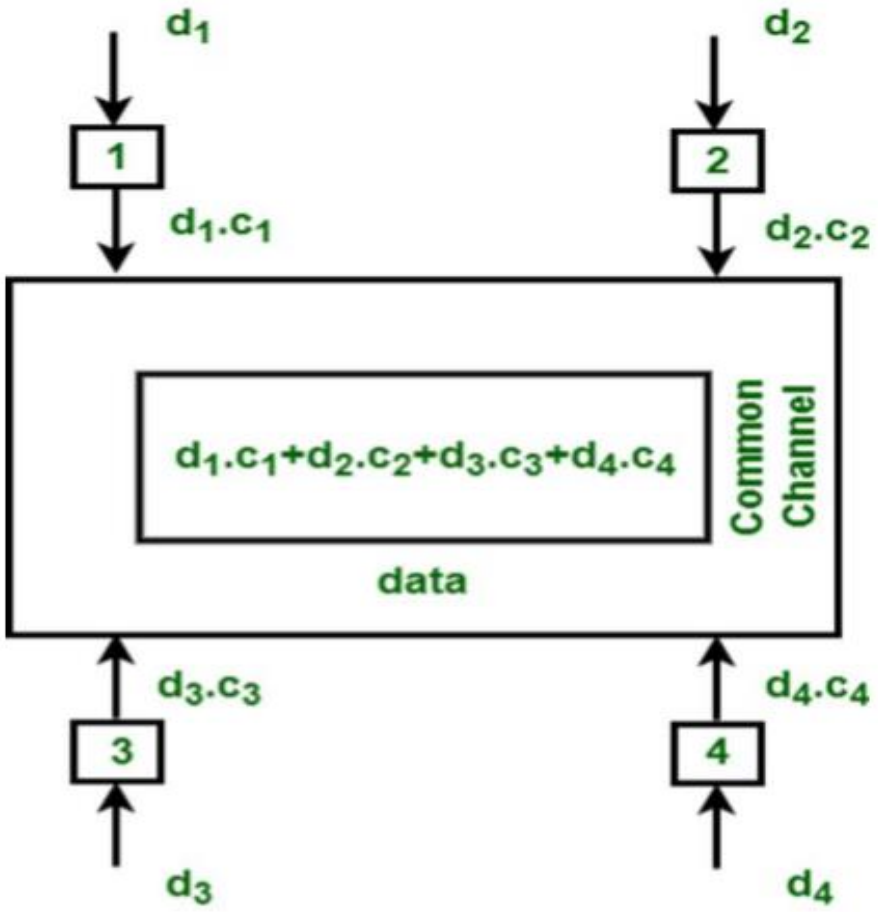
When using the TDMA technique then each station needs to know the beginning of its slot and the location of its slot.



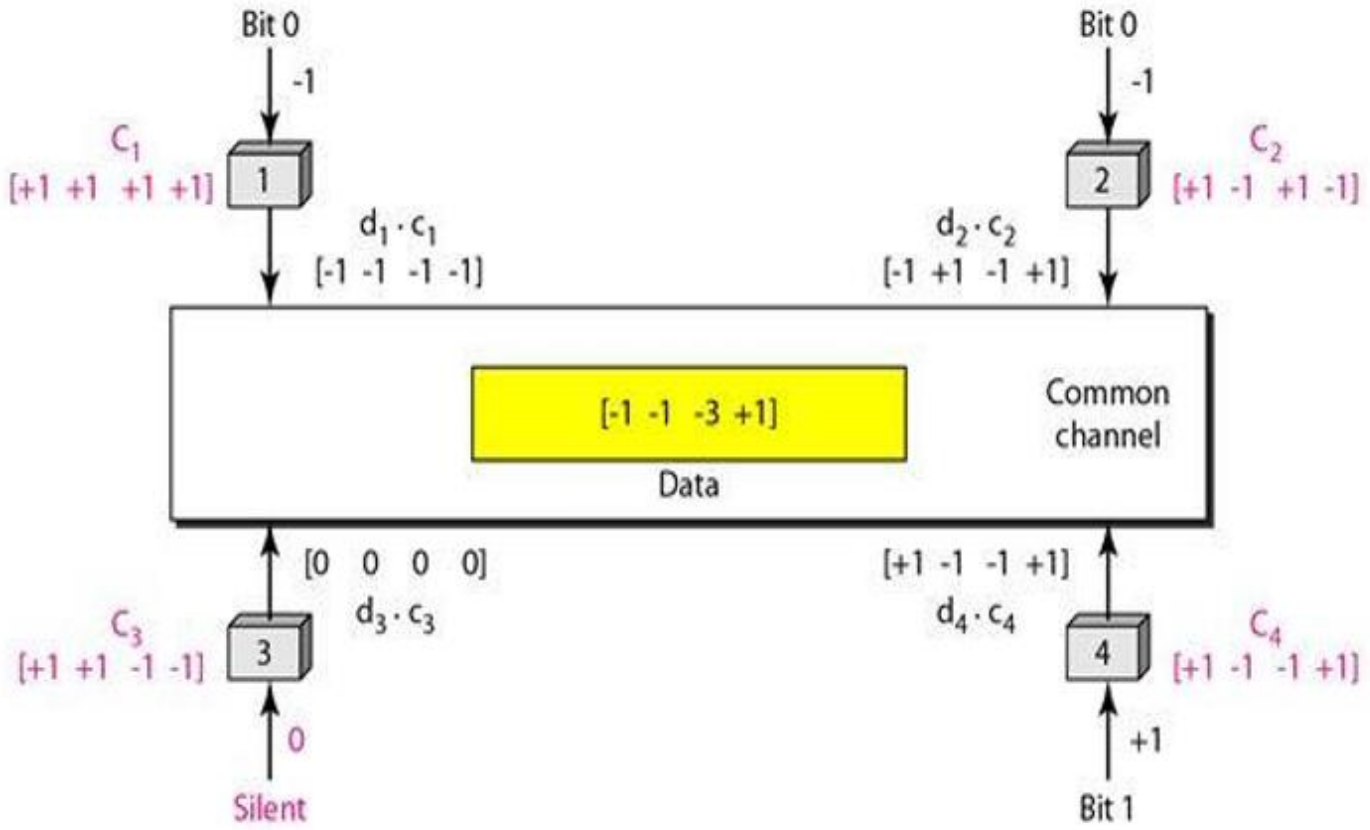
Code-Division Multiple Access

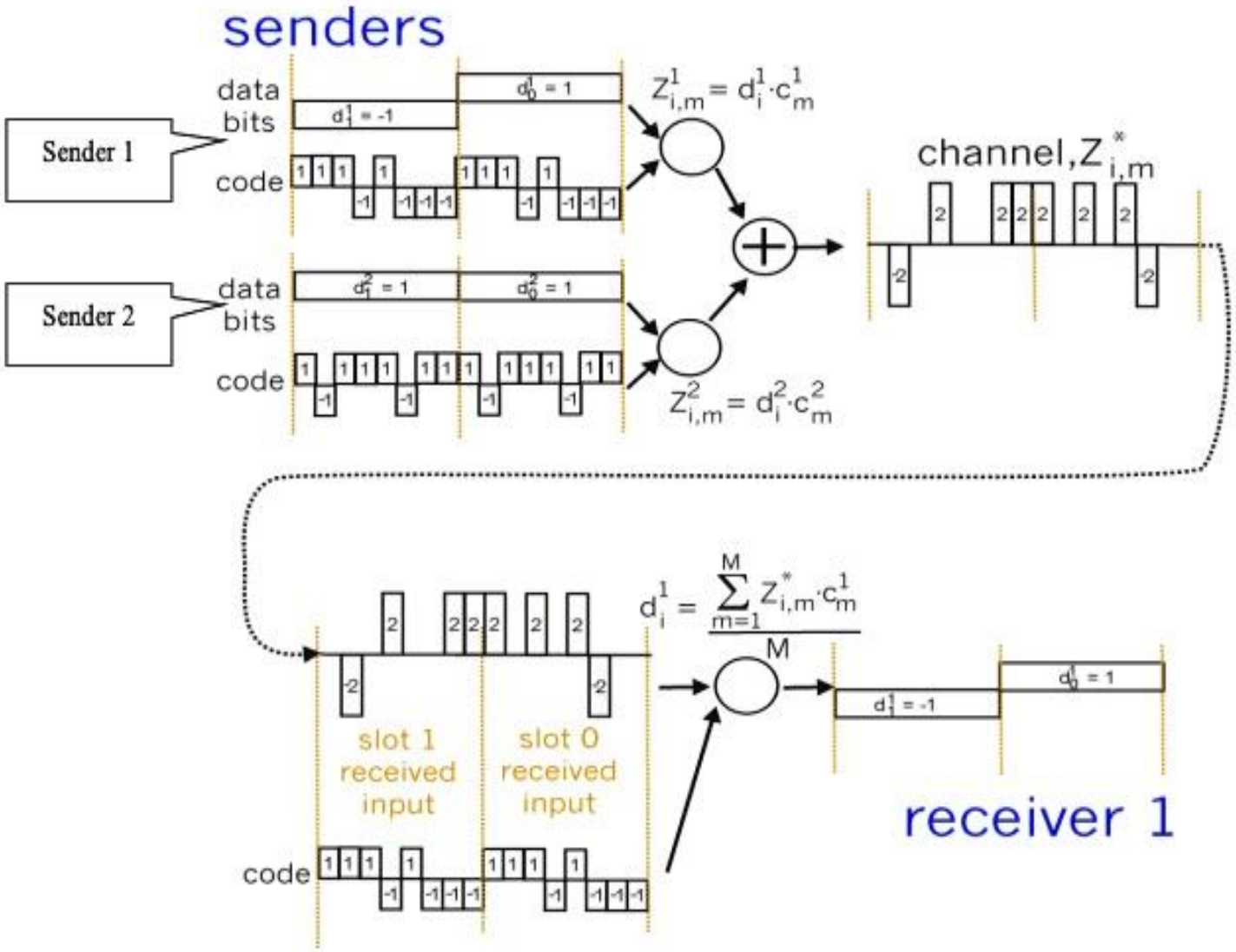
- CDMA(code-division multiple access) is another technique used for channelization.
- CDMA technique differs from the FDMA because only one channel occupies the entire bandwidth of the link.
- The CDMA technique differs from the TDMA because all the stations can send data simultaneously as there is no timesharing.
- The CDMA technique simply means communication with different codes.
- In the CDMA technique, there is only one channel that carries all the transmission simultaneously.

CDMA


d_1
d_2
1
2
$d_1.c_1$
$d_2.c_2$
$d_1.c_1+d_2.c_2+d_3.c_3+d_4.c_4$
Common Channel
data
$d_3.c_3$
$d_4.c_4$
3
4
d_3
d_4

CDMA


Bit 0
-1
C_1
[+1 +1 +1 +1]
1
$d_1 \cdot c_1$
[-1 -1 -1 -1]
Bit 0
-1
C_2
[+1 -1 +1 -1]
2
$d_2 \cdot c_2$
[-1 +1 -1 +1]
[-1 -1 -3 +1]
Data
Common channel
[0 0 0 0]
$d_3 \cdot c_3$
C_3
[+1 +1 -1 -1]
3
0
Silent
[+1 -1 -1 +1]
$d_4 \cdot c_4$
C_4
[+1 -1 -1 +1]
4
+1
Bit 1


senders
Sender 1
Sender 2
data bits
code
channel, $Z^*_{i,m}$
$Z^1_{i,m} = d^1_i \cdot c^1_m$
$Z^2_{i,m} = d^2_i \cdot c^2_m$
$d^1_i = \frac{\sum_{m=1}^{M} Z^*_{i,m} \cdot c^1_m}{M}$
slot 1 received input
slot 0 received input
receiver 1

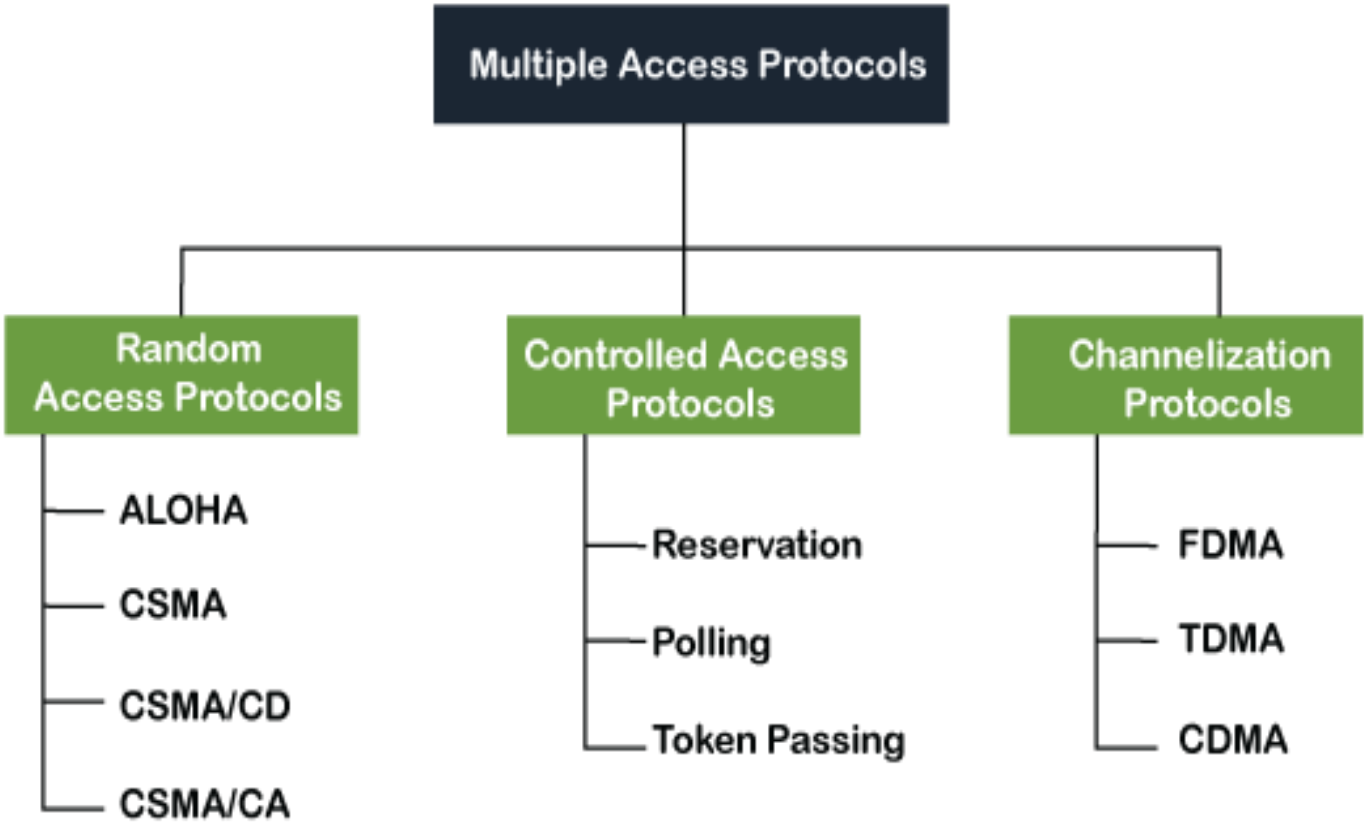
Media access control

- The MAC sublayer is the bottom part of the data link layer. The protocols used to determine who goes next on a multiaccess channel belong to a sublayer of the data link layer called the MAC (Medium Access Control) sublayer.

- The MAC sublayer is especially important in LANs, particularly wireless ones because wireless is naturally a broadcast channel. broadcast channels are sometimes referred to as multi-access channels or random access

  Channels.

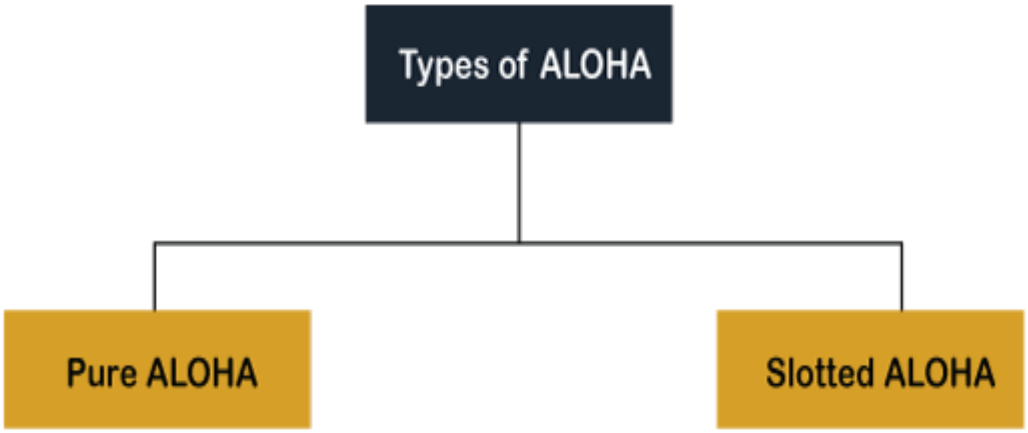
MULTIPLE ACCESS PROTOCOL



Random Access Protocol

- In this protocol, all the station has the equal priority to send the data over a channel. In random access protocol, one or more stations cannot depend on another station nor any station control another station.

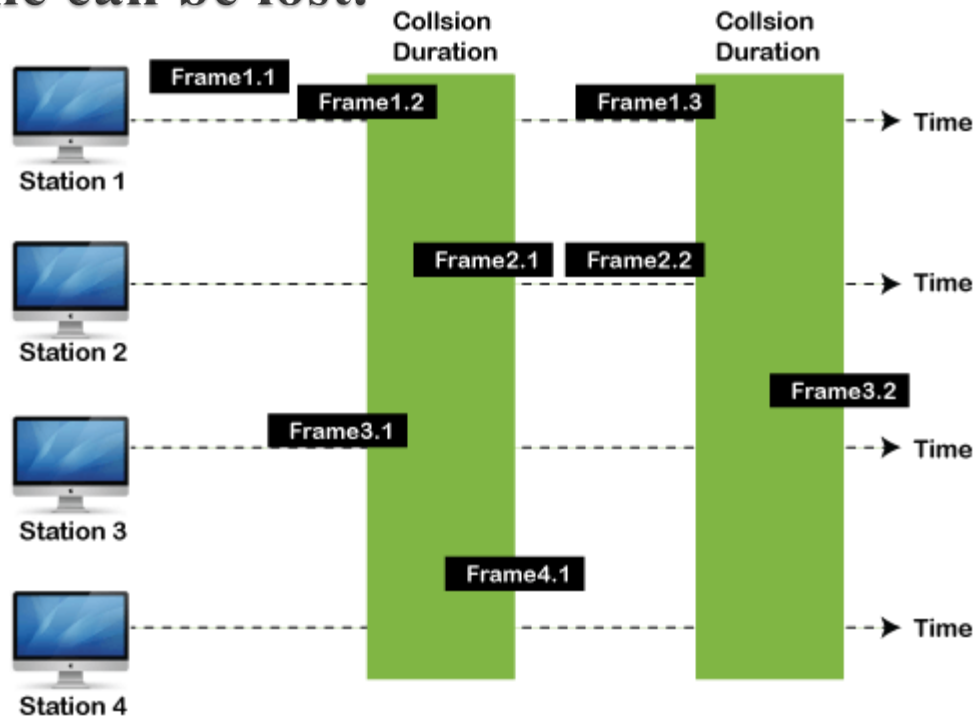
- Depending on the channel's state (idle or busy), each station transmits the data frame. However, if more than one station sends the data over a channel, there may be a collision or data conflict.



- **Aloha Rules**
- Any station can transmit data to a channel at any time.
- It does not require any carrier sensing.
- Collision and data frames may be lost during the transmission of data through multiple stations.

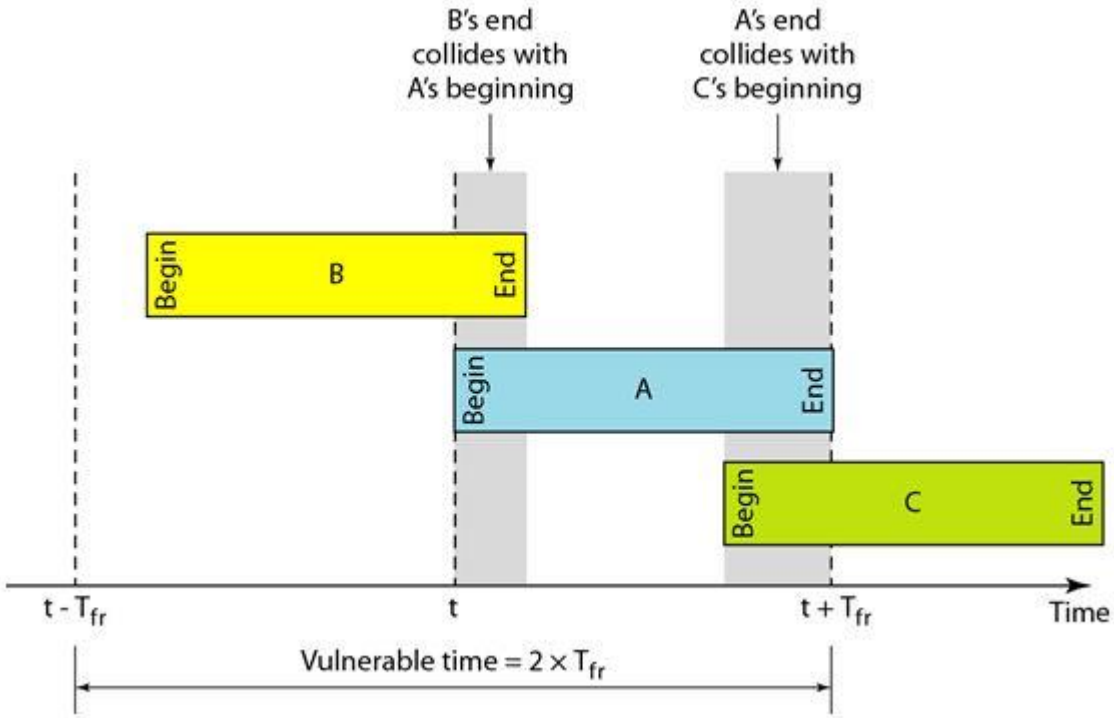
Pure Aloha

Whenever data is available for sending over a channel at stations, we use Pure Aloha. In pure Aloha, when each station transmits data to a channel without checking whether the channel is idle or not, the chances of collision may occur, and the data frame can be lost.



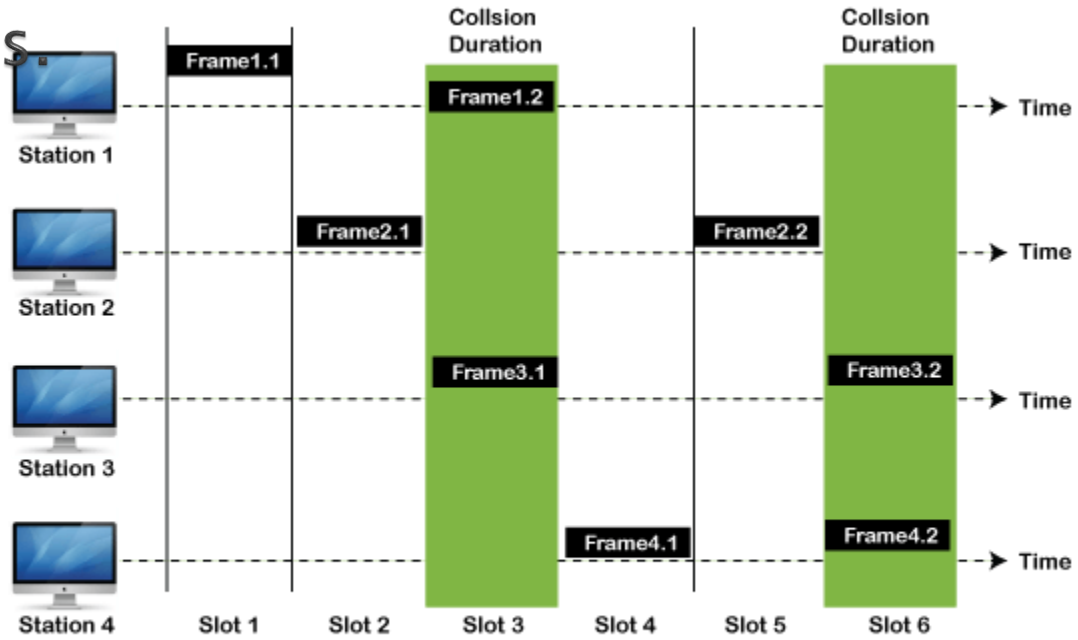
Frames in Pure ALOHA

In case of pure ALOHA, the vulnerable time period so that collision does not occur between two frames is equal to two frame times, i.e. 2TT. In 2T time,average number of transmission attempts is 2G



Slotted Aloha

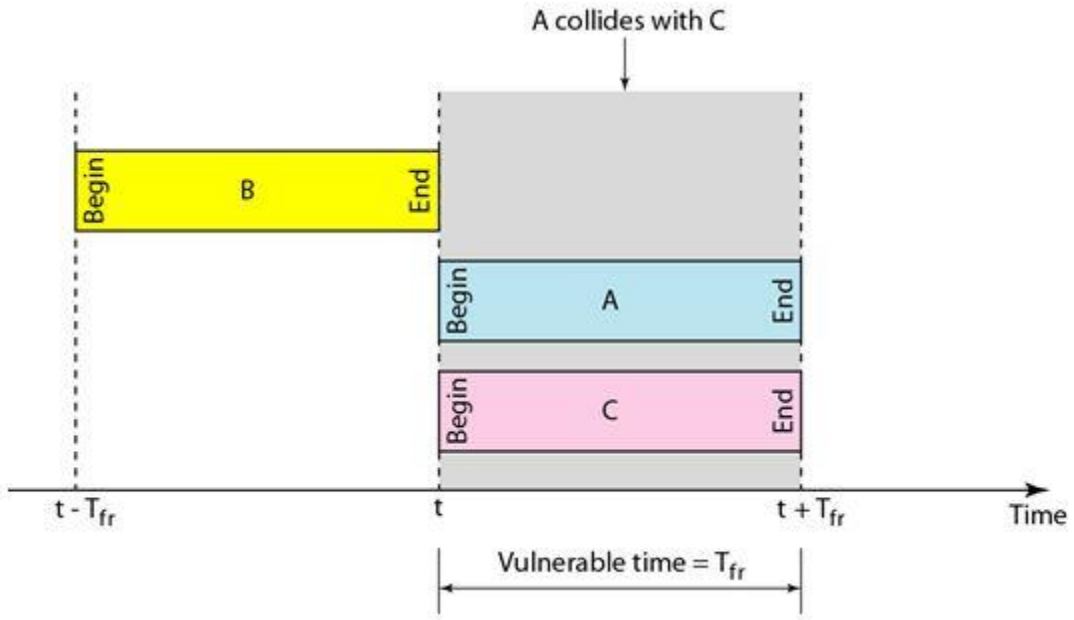
The slotted Aloha is designed to overcome the pure Aloha's efficiency because pure Aloha has a very high possibility of frame hitting. In slotted Aloha, the shared channel is divided into a fixed time interval called slots.



Frames in Slotted ALOHA

Vulnerable case in Slotted Aloha

In case of slotted ALOHA, the vulnerable time period for collision between two frames is equal to time duration of 1 slot, which is equal to 1 frame time, i.e. T.In T time, average number of transmission attempts is G

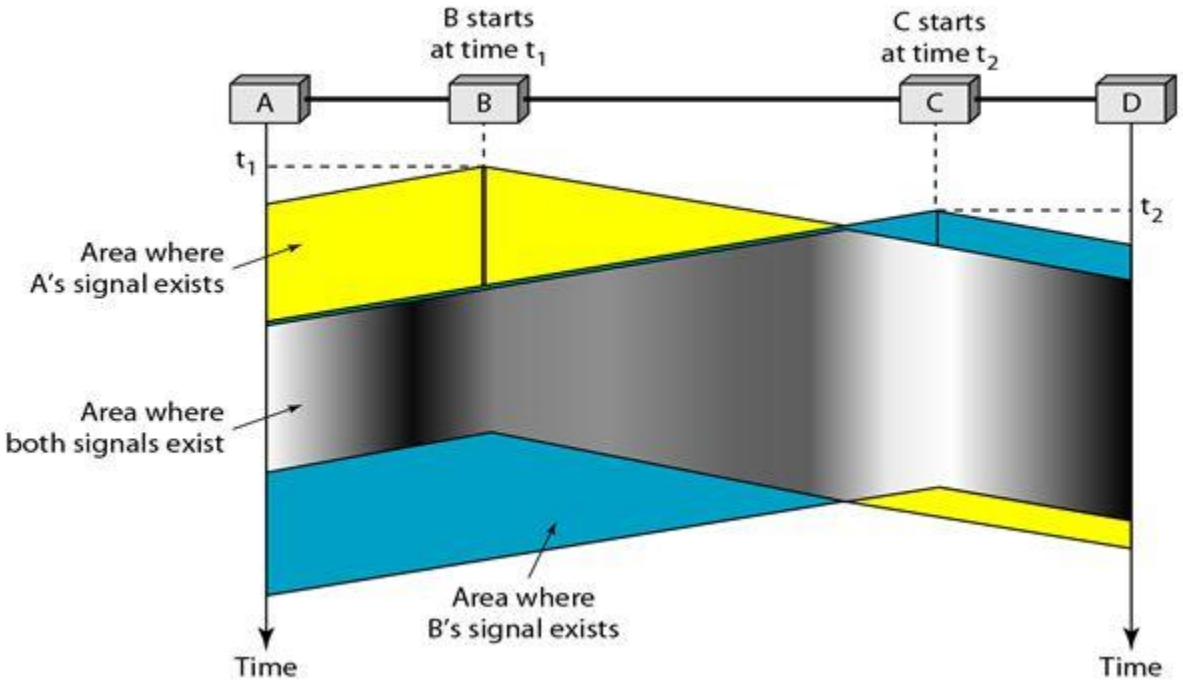


CSMA (Carrier Sense Multiple Access)

It is a carrier sense multiple access based on media access protocol to sense the traffic on a channel (idle or busy) before transmitting the data. It means that if the channel is idle, the station can send data to the channel. Otherwise, it must wait until the channel becomes idle. Hence, it reduces the chances of a collision on a transmission medium.

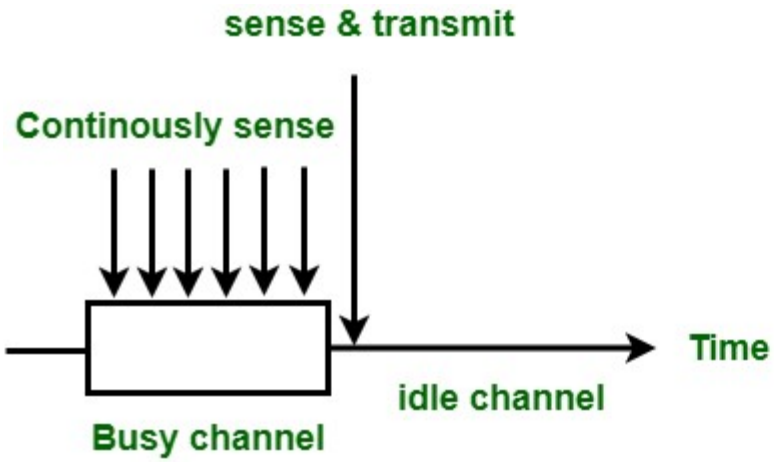
- CSMA Access Modes
- 1-Persistent
- Non-Persistent
- P-Persistent

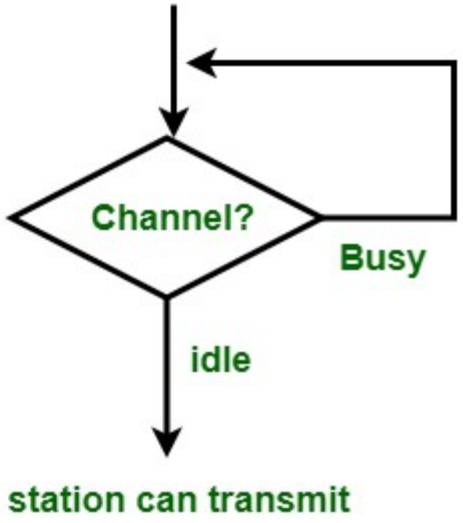
Carrier Sense Multiple Access Protocol



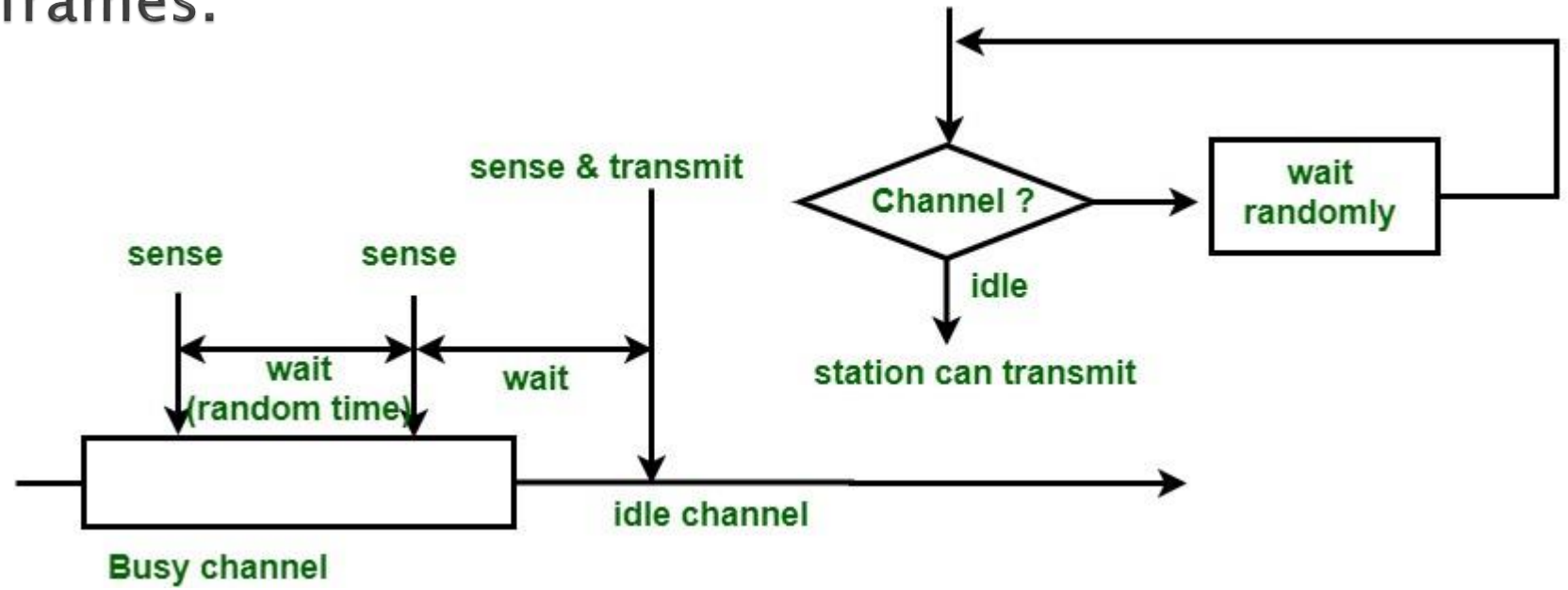
CSMA Access Modes

1-Persistent: In the 1-Persistent mode of CSMA that defines each node, first sense the shared channel and if the channel is idle, it immediately sends the data. Else it must wait and keep track of the status of the channel to be idle and broadcast the frame unconditionally as soon as the channel is idle.





Non-Persistent: It is the access mode of CSMA that defines before transmitting the data, each node must sense the channel, and if the channel is inactive, it immediately sends the data. Otherwise, the station must wait for a random time (not continuously), and when the channel is found to be idle, it transmits the frames.

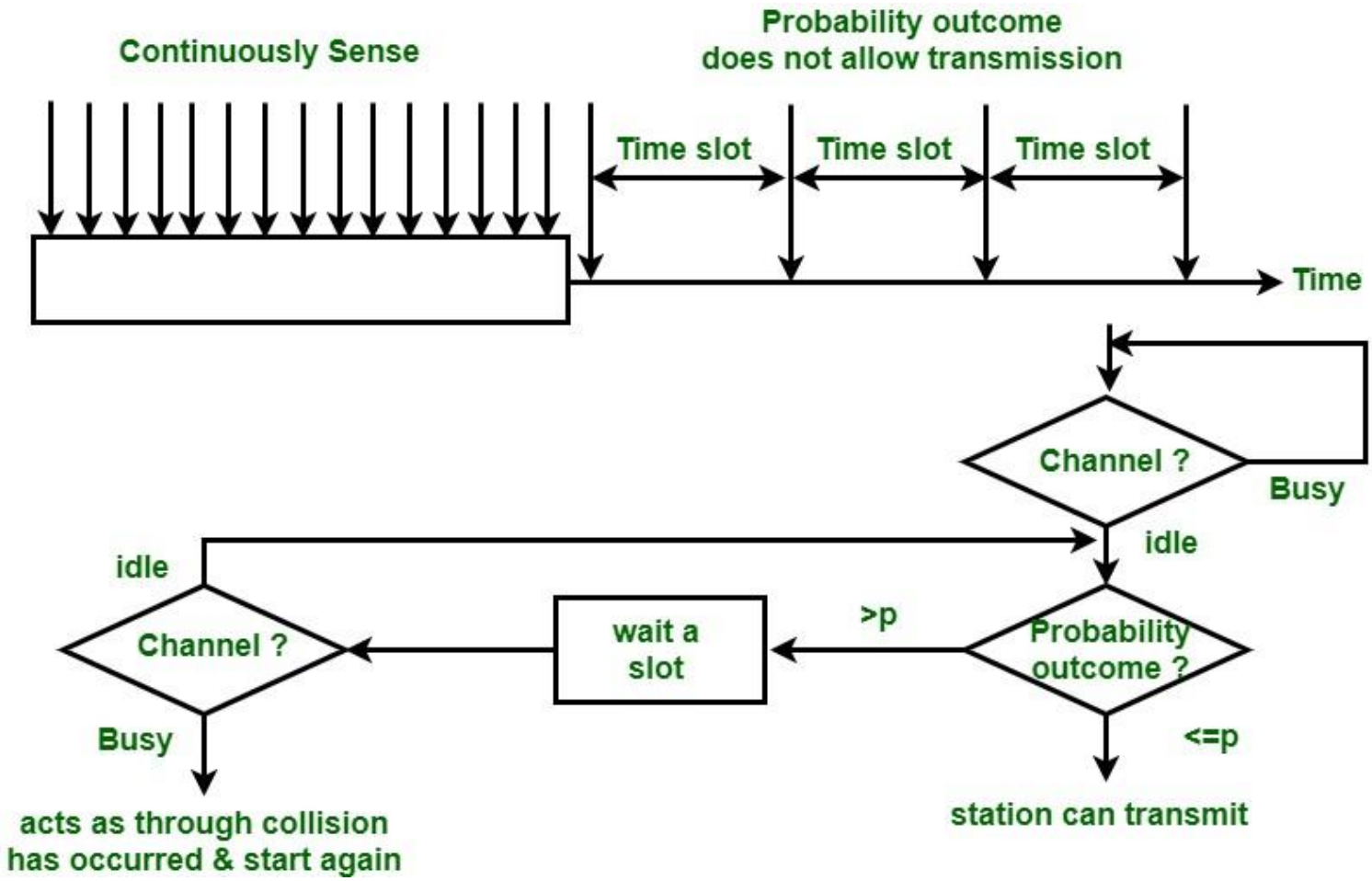


P-Persistent

It is the combination of 1-Persistent and Non-persistent modes. The P-Persistent mode defines that each node senses the channel, and if the channel is inactive, it sends a frame with a P probability.

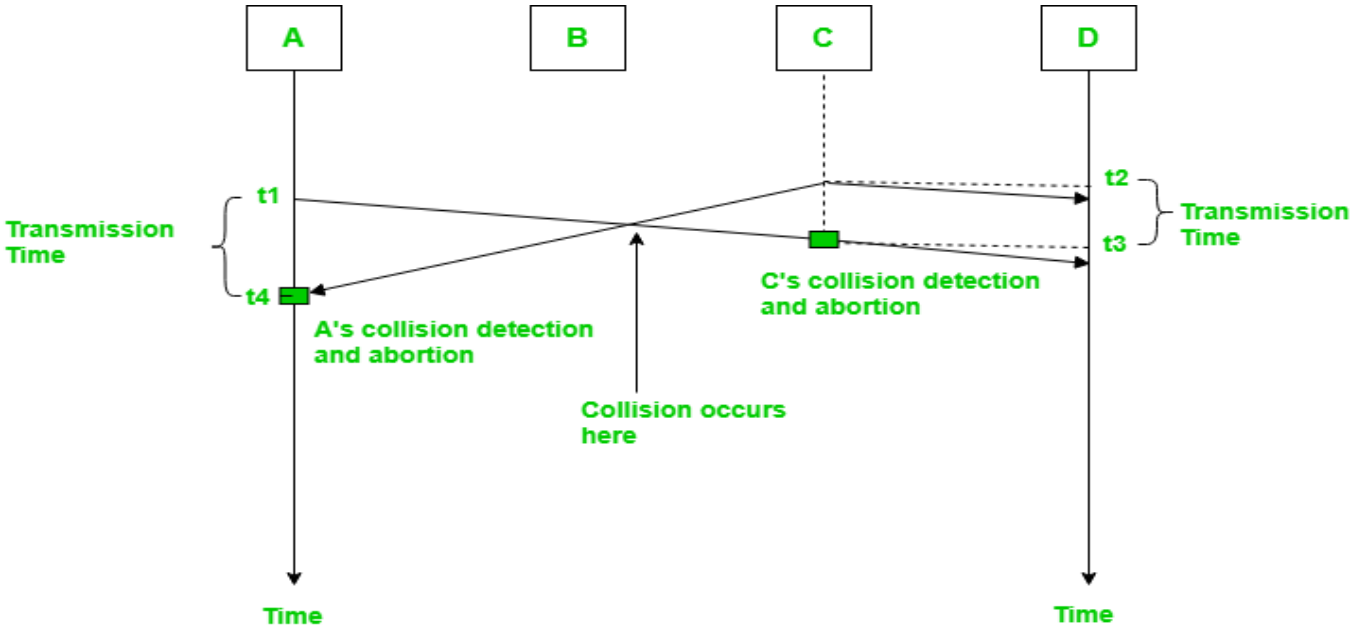
If the data is not transmitted, it waits for a (q = 1-p probability) random time and resumes the frame with the next time slot.

P-Persistent



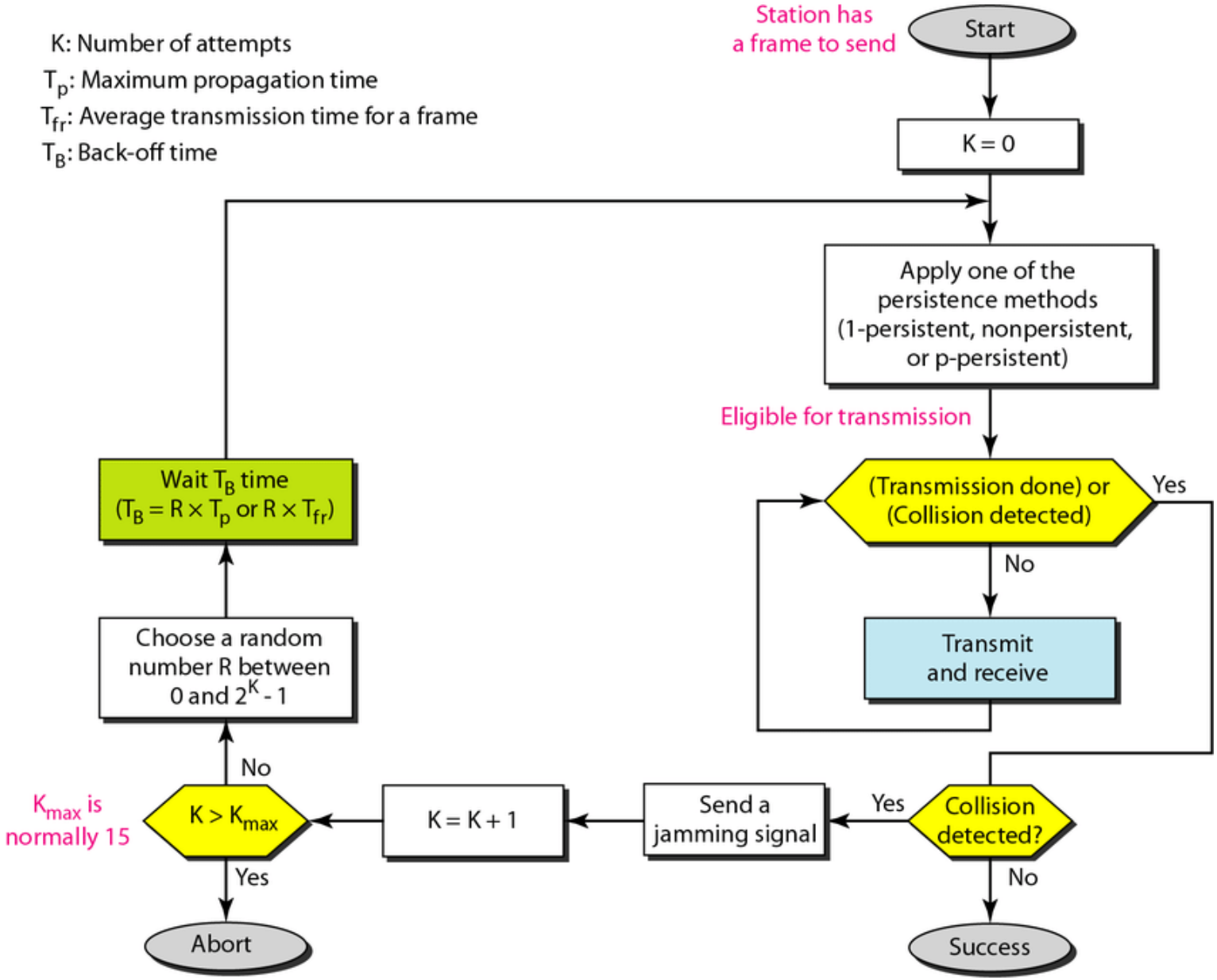
1. Carrier Sense Multiple Access with Collision Detection (CSMA/CD):

In this method, a station monitors the medium after it sends a frame to see if the transmission was successful. If successful, the transmission is finished, if not, the frame is sent again.



- In the diagram, starts sending the first bit of its frame at t1 and since C sees the channel idle at t2, starts sending its frame at t2. C detects A's frame at t3 and aborts transmission. A detects C's frame at t4 and aborts its transmission. Transmission time for C's frame is, therefore, t3-t2 and for A's frame is t4-t1

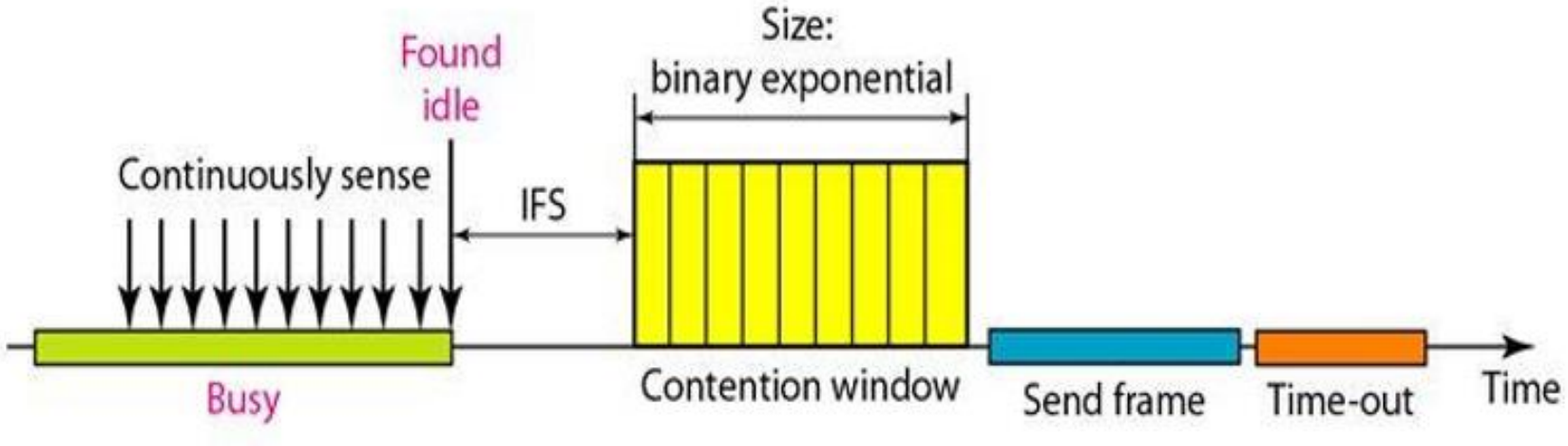
- So, the frame transmission time (Tfr) should be at least twice the maximum propagation time (Tp). This can be deduced when the two stations involved in a collision are a maximum distance apart.


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

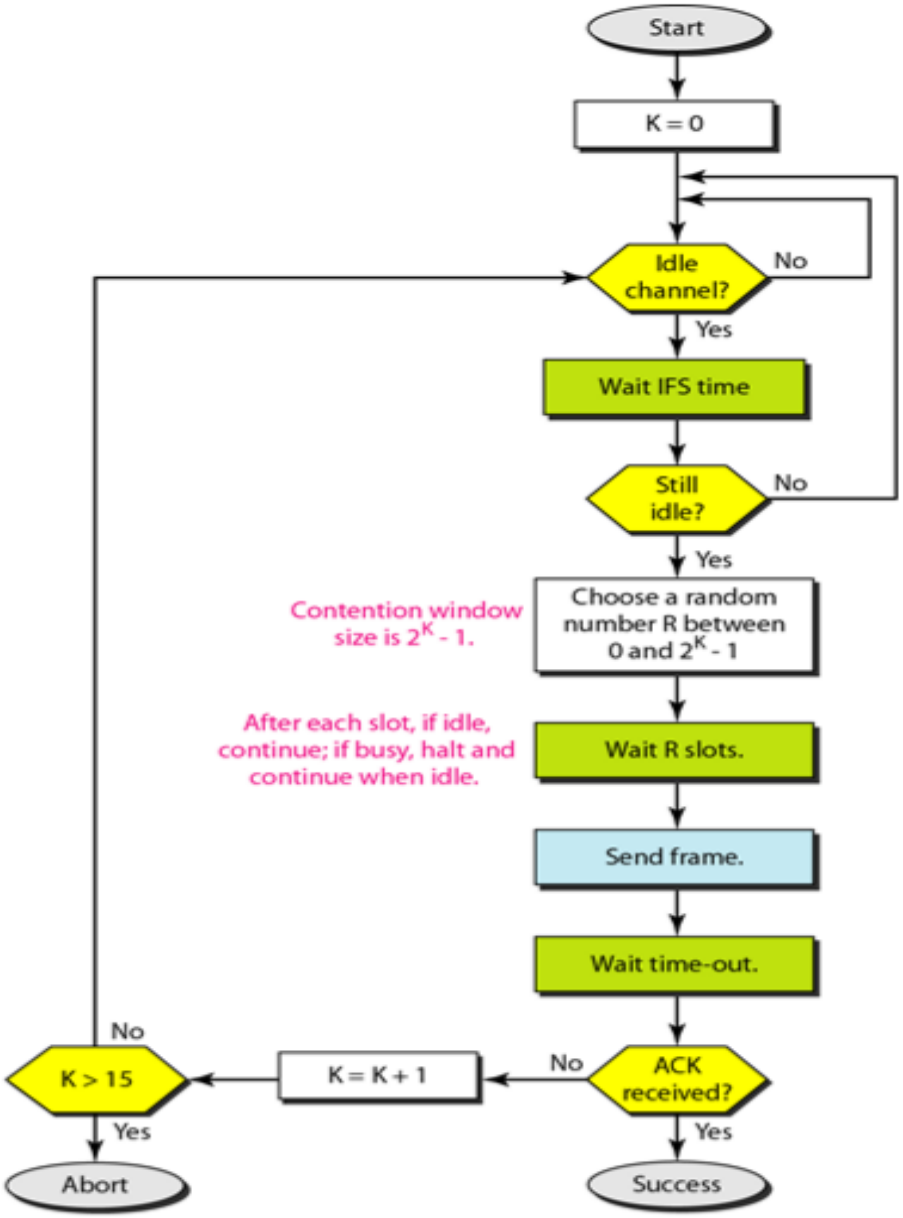
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) • The basic idea behind CSMA/CA is that the station should be able to receive while transmitting to detect a collision from different stations.
- In wired networks, if a collision has occurred then the energy of the received signal almost doubles, and the station can sense the possibility of collision. • In the case of wireless networks, most of the energy is used for transmission, and the energy of the received signal increases by only 5-10% if a collision occurs. It can’t be used by the station to sense collision.

- Therefore CSMA/CA has been specially designed for wireless networks. • These are three types of strategies:
- • InterFrame Space (IFS): When a station finds the channel busy it senses the channel again, when the station finds a channel to be idle it waits for a period of time called IFS time. IFS can also be used to define the priority of a station or a frame. Higher the IFS lower is the priority.
- • Contention Window: It is the amount of time divided into slots. A station that is ready to send frames chooses a random number of slots as wait time.
- • Acknowledgments: The positive acknowledgments and time-out timer can help guarantee a successful transmission of the frame.

- CSMA/CA avoids the collisions using three basic techniques. (i) Interframe space (ii) Contention window (iii) Acknowledgements



Flow diagram for CSMA/CA

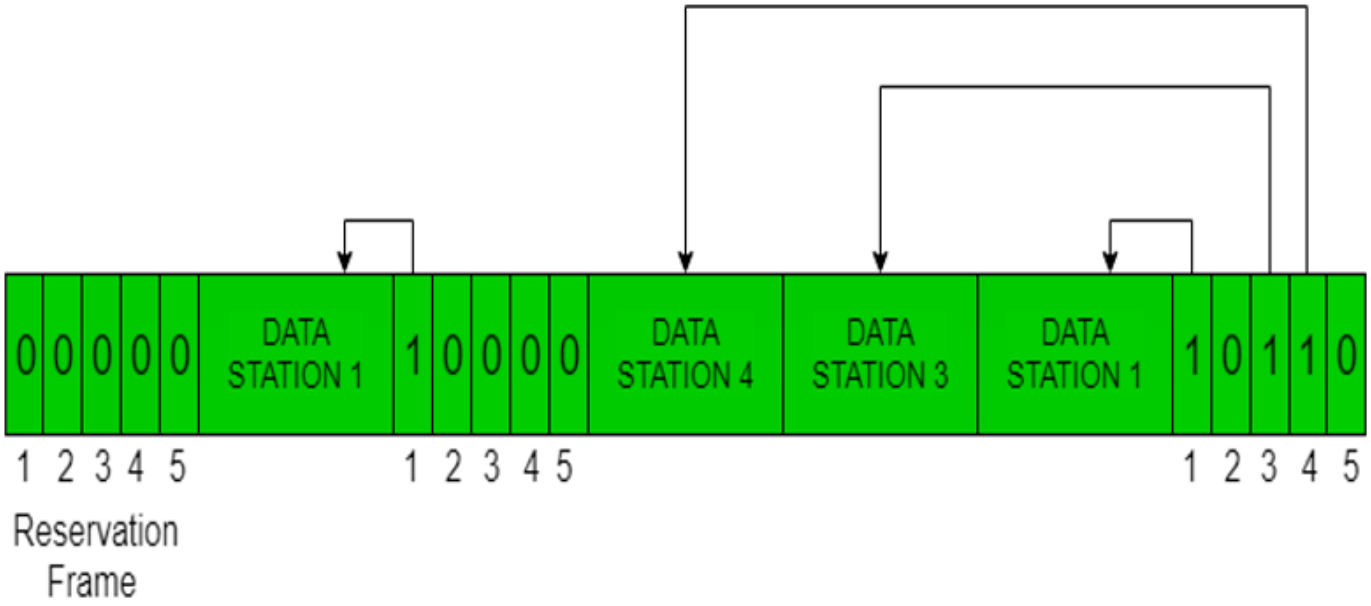


- Controlled Access Protocols
- • In controlled access, the stations seek information from one another to find which station has the right to send. It allows only one node to send at a time, to avoid the collision of messages on a shared medium. The three controlled-access methods are:
- Reservation
- Polling
- Token Passing

- Reservation
- In the reservation method, a station needs to make a reservation before sending data.
- The timeline has two kinds of periods:
- – Reservation interval of fixed time length
- – Data transmission period of variable frames.
- If there are M stations, the reservation interval is divided into M slots, and each station has one slot.
- Suppose if station 1 has a frame to send, it transmits 1 bit during the slot 1. No other station is allowed to transmit during this slot.

Reservation

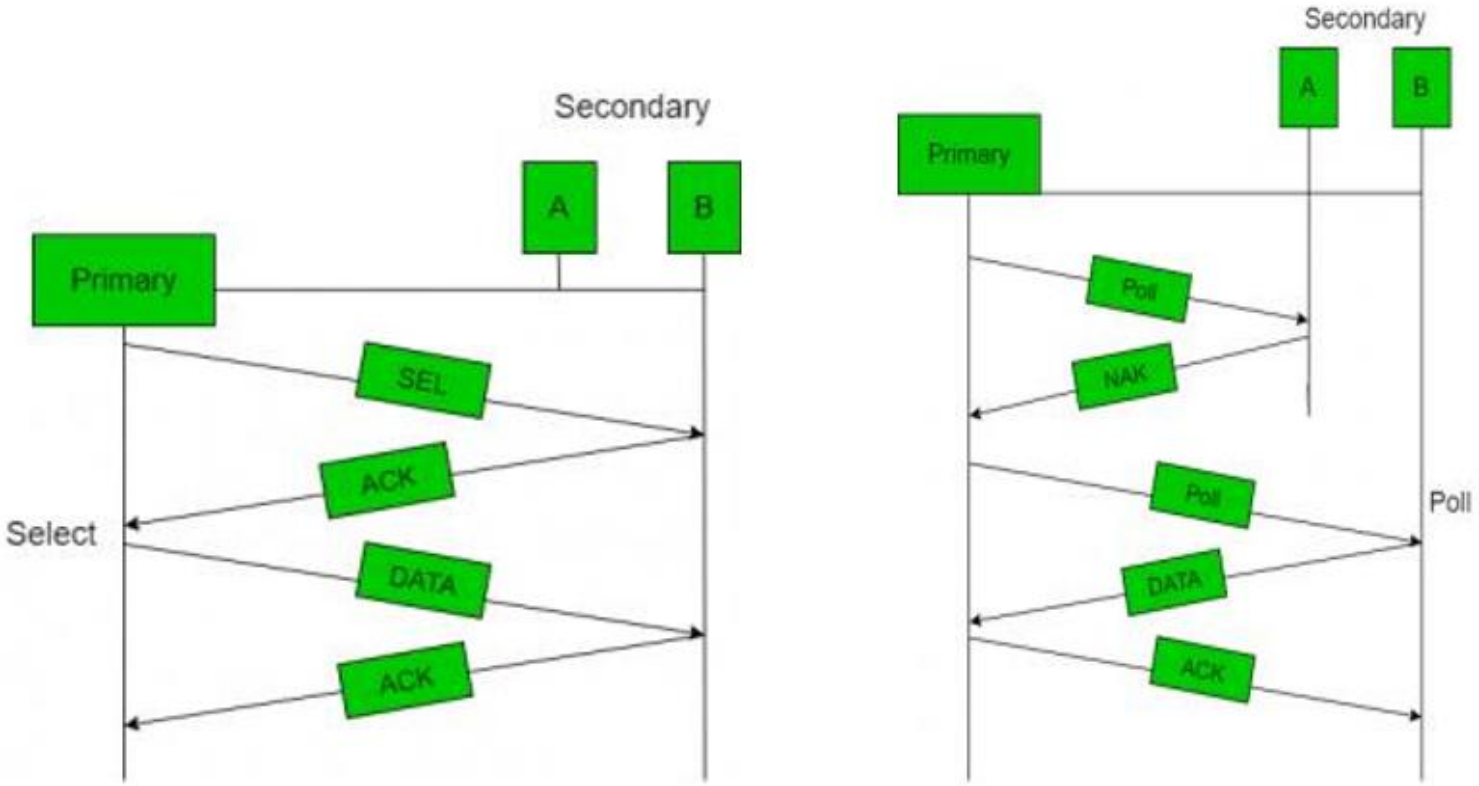
The following figure shows a situation with five stations and a five-slot reservation frame. In the first interval, only stations 1, 3, and 4 have made reservations. In the second interval, only station 1 has made a reservation.



Polling

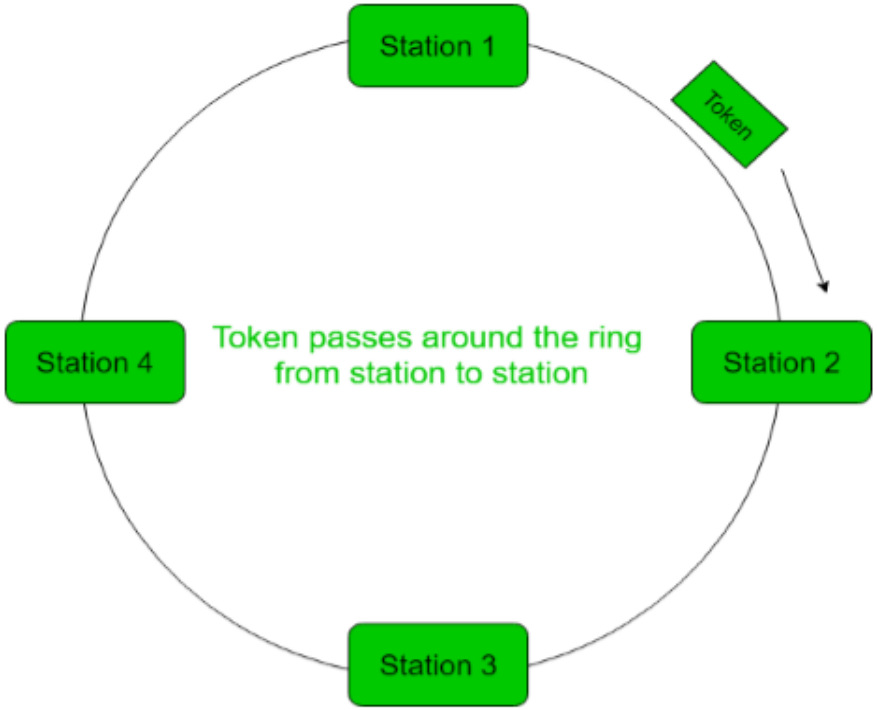
- Polling process is similar to the roll-call performed in class. Just like the teacher, a controller sends a message to each node in turn.
- In this, one acts as a primary station(controller) and the others are secondary stations. All data exchanges must be made through the controller.
- The message sent by the controller contains the address of the node being selected for granting access.

Polling


Secondary
A
B
Primary
SEL
ACK
Select
DATA
ACK
Secondary
A
B
Primary
Poll
NAK
Poll
Poll
DATA
ACK

- Token Passing
- In token passing scheme, the stations are connected logically to each other in form of ring and access to stations is governed by tokens.
- A token is a special bit pattern or a small message, which circulate from one station to the next in some predefined order.
- In Token ring, token is passed from one station to another adjacent station in the ring whereas incase of Token bus, each station uses the bus to send the token to the next station in some predefined order.

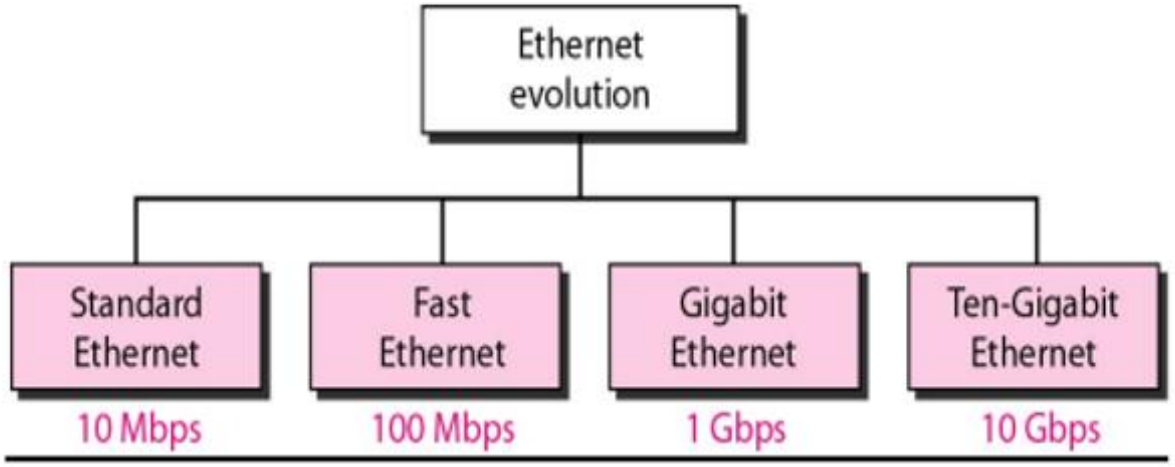
In both cases, token represents permission to send. If a station has a frame queued for transmission when it receives the token, it can send that frame before it passes the token to the next station. If it has no queued frame, it passes the token simply.



STANDARD ETHERNET

Ethernet:

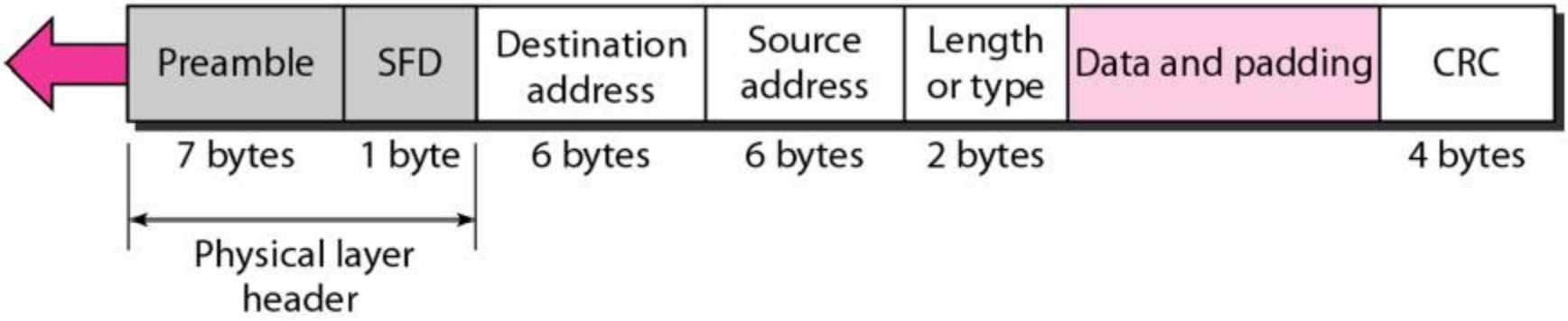
- The original Ethernet was created in 1976 at Xerox's Palo Alto Research Center (PARC). It has gone through four generations: Standard Ethernet (10 Mbps), Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps), and Ten-Gigabit Ethernet (10 Gbps), as shown in Figure.



802.3 MAC Frame

Preamble: 56 bits of alternating 1s and 0s.

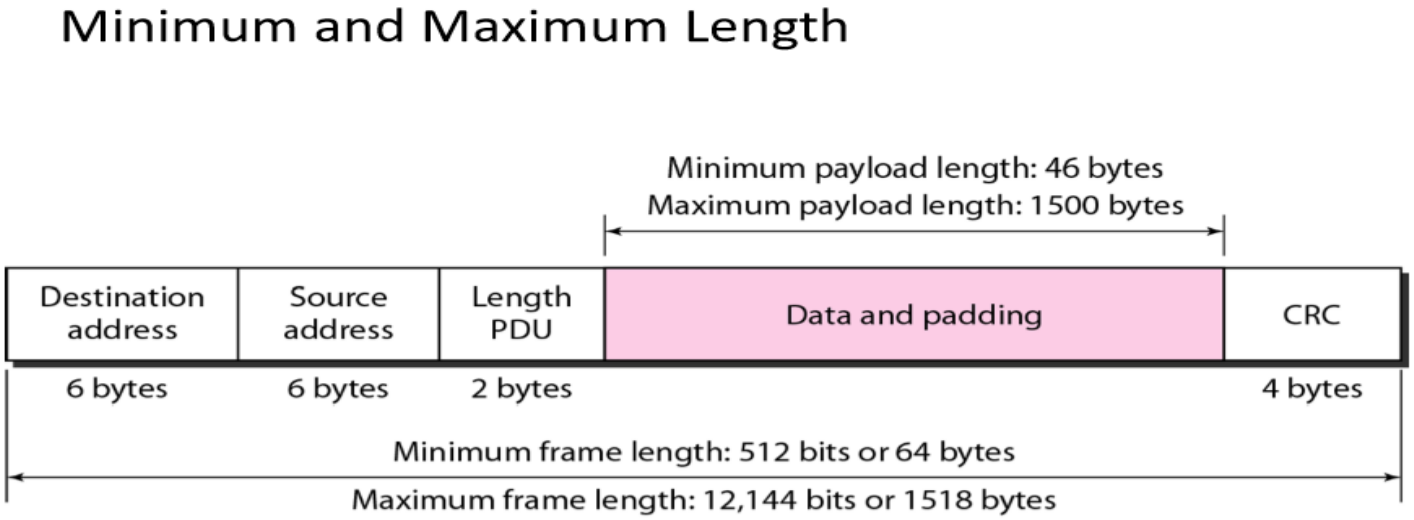
SFD: Start frame delimiter, flag (10101011)



Preamble is the first section of 7 bytes in a frame. The first seven bytes of the preamble are all the same 10101010. Only one bit even the start one or last one is slightly different like 10101011. The 8 bytes of the preamble and the Start of Frame create a pattern of 64 bits. They are not officially counted as part of the Ethernet frame.

- Start Frame Delimiter (SFD) for Ethernet Basic concept in Networking The preamble is seven octets and the SFD is one octet. An Ethernet frame starts with preamble followed by the SFD. The actual frame data starts after the SFD
- Destination for Ethernet Basic concept in Networking It is the 48 bits MAC address of the destination. Destination address used by receiving devices to determine the correct destination.
- Source for Ethernet Basic concept in Networking • The source is similar to destination of 48 bits. It is also a MAC address of the source of data transmitting device.
- Type for Ethernet Basic concept in Networking • 802.3 uses a Type or length field, but the Ethernet-II frame uses a Type field only. Type field used to identify the Network layer protocol. Network layer protocol may be TCP , UDP or IPX etc.

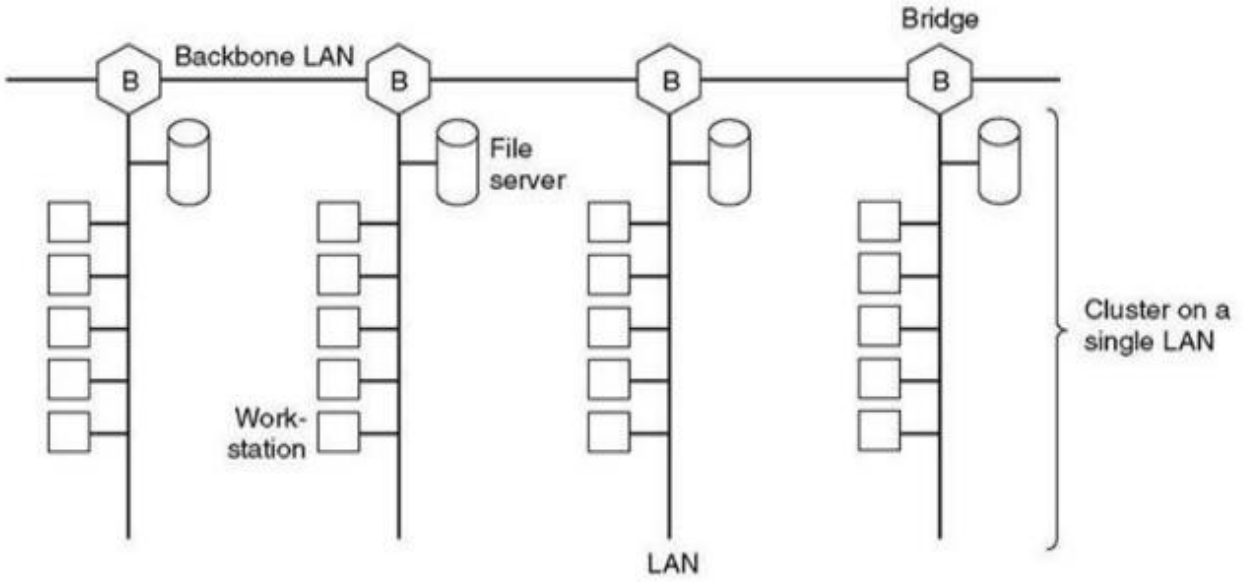
- Data for Ethernet Basic concept in Networking • This segment of 46 – 1500 bytes contains the information. This part of the frame will change for each packet.
- Frame Check Sequence (FCS) for Ethernet Basic concept in Networking • FCS is the last segment of a frame. It is 4 bytes long only. FCS used to store the cyclic redundancy check (CRC) reply.



Data Link Layer Switching

- Many organizations have multiple LANs and wish to connect them. LANs can be connected by devices called bridges, which operate in the data link layer. Bridges examine the data layer link addresses to do routing.
- Network switching is the process of forwarding data frames or packets from one port to another leading to data transmission from source to destination

Data Link Layer Switching



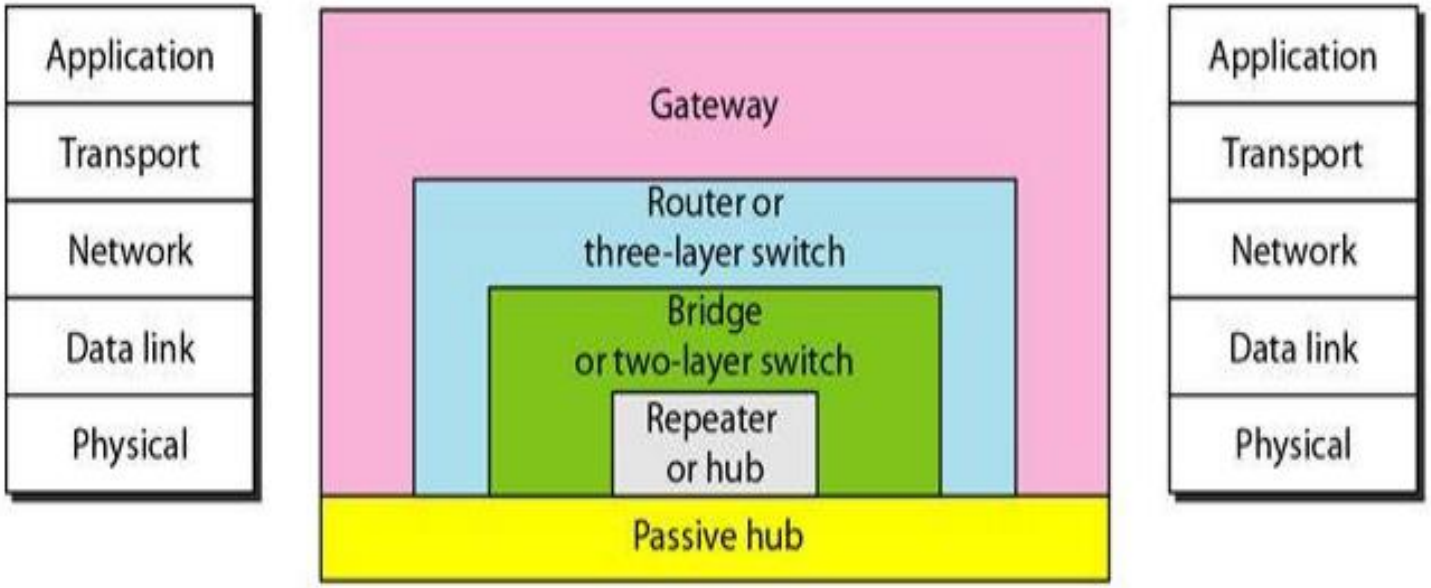
Multiple LANs connected by a backbone to handle a total load higher than the capacity of a single LAN.

Use of Bridges

- A bridge in a computer network is a device that connects two or more LANs or network segments, enabling them to communicate with each other.
- It operates at the data link layer of the OSI model in computer networks and reads the source address of incoming data packets, forwarding them only to their target destination instead of broadcasting them to all connected segments. This helps reduce network congestion and improve performance.
- A Bridge in computer networks can also improve network security by breaking up large LANs into smaller ones, reducing the risk of unauthorized access.

Connecting Devices

- **Connecting devices are divided into 5 different categories based on the layer in which they operate in a network.**



Passive Hubs:

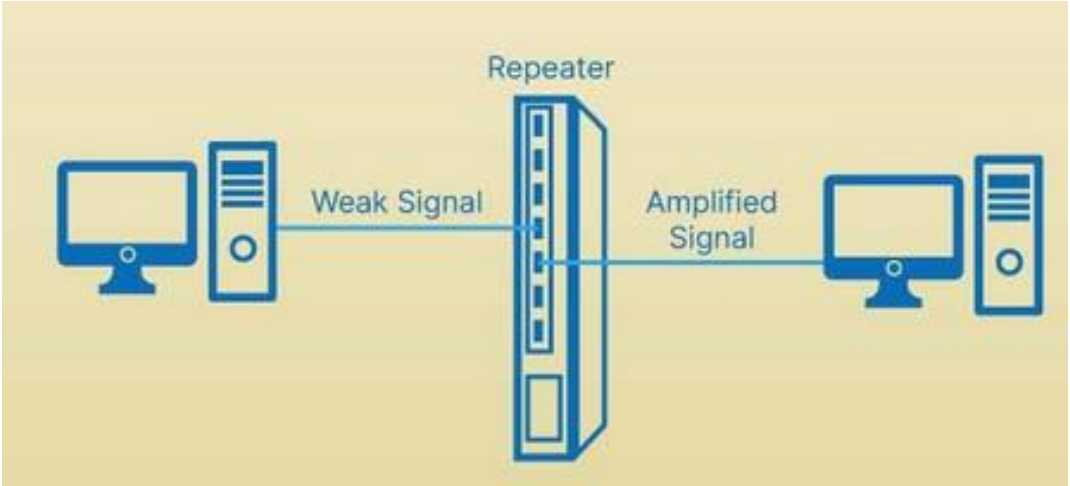
- **Passive Hubs** −Passive hubs connects nodes in a star configuration by collecting wiring from nodes. They broadcast signals onto the network without amplifying or regenerating them. As they cannot extend the distance between nodes, they limit the size of the LAN.

Active Hub

- **Active Hubs** −Active hubs amplify and regenerate the incoming electrical signals before broadcasting them. They have their own power supply and serves both as a repeater as well as connecting centre. Due to their regenerating capabilities, they can extend the maximum distance between nodes, thus increasing the size of LAN.

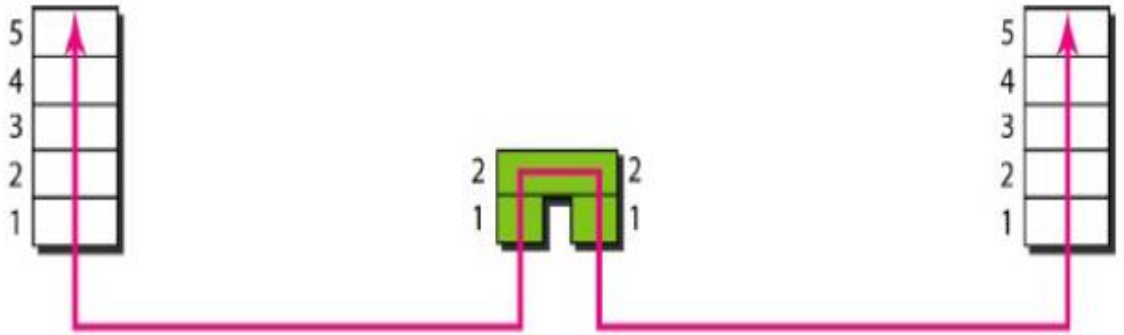
Repeaters

- A repeater is a device that operates only in the physical layer. Signals that carry information within a network can travel a fixed distance before attenuation endangers the integrity of the data.
- A repeater receives a signal and, before it becomes too weak or corrupted, regenerates the original bit pattern. The repeater then sends the refreshed signal.



Bridges

- A bridge operates in both the physical and the data link layer. As a physical layer device, it
- regenerates the signal it receives. As a data link layer device, the bridge can check the
- physical (MAC) addresses (source and destination) contained in the frame.
- A bridge has filtering capability. It can check the destination address of a frame and decide
- if the frame should be forwarded or dropped. If the frame is to be forwarded, the decision
- must specify the port. A bridge has a table that maps addresses to ports.



Address	Port
71:2B:13:45:61:41	1
71:2B:13:45:61:42	1
64:2B:13:45:61:12	2
64:2B:13:45:61:13	2

Bridge Table

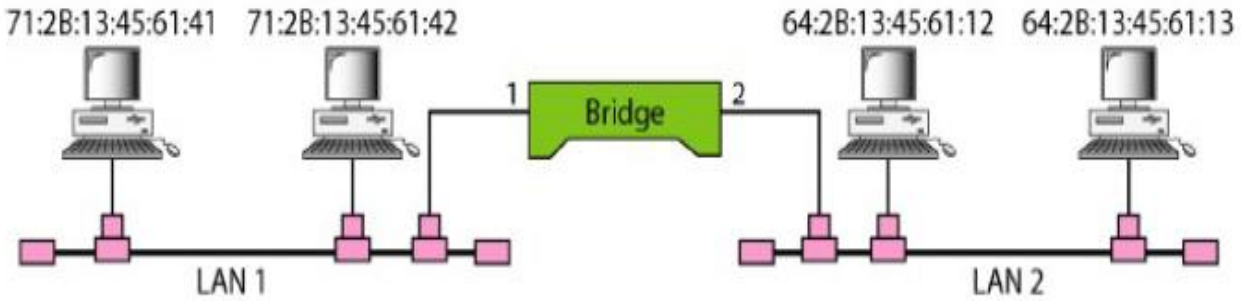
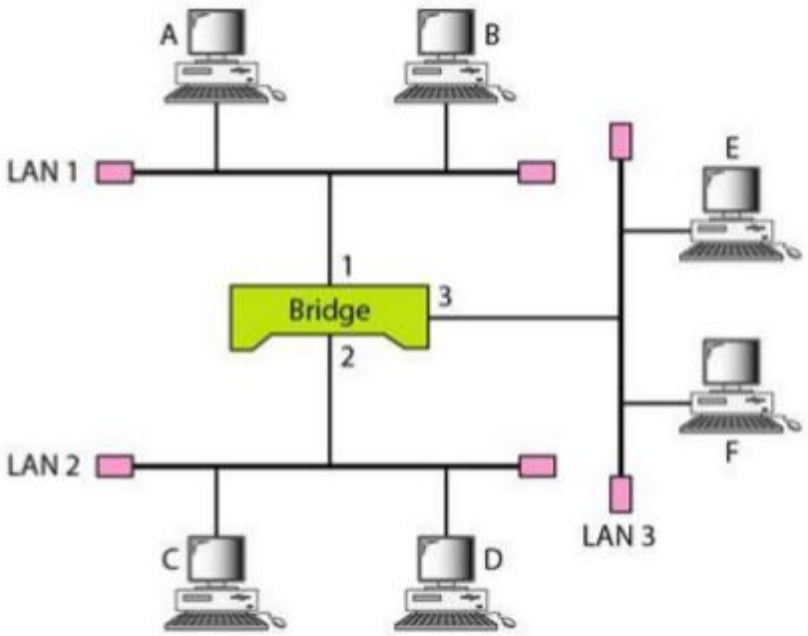


Figure 15.5 A bridge connecting two LANs

Transparent Bridges

- A transparent bridge is a bridge in which the stations are completely unaware of the bridge's existence. If a bridge is added or deleted from the system, reconfiguration of the stations is unnecessary.
- Frames must be forwarded from one station to another.
- The forwarding table is automatically made by learning frame movements in the network.
- Loops in the system must be prevented

Learning Bridges



Address	Port

a. Original

Address	Port
A	1

b. After A sends a frame to D

Address	Port
A	1
E	3

c. After E sends a frame to A

Address	Port
A	1
E	3
B	1

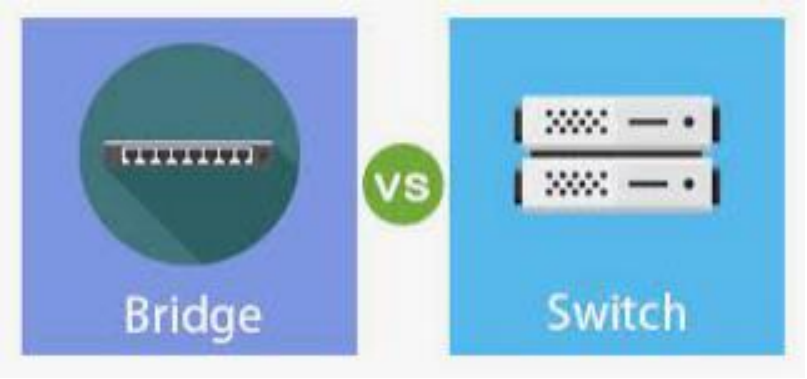
d. After B sends a frame to C

- A learning bridge has all the capabilities of a basic bridge, but it has one advantage.
- A learning bridge listens to all frames in the two LAN segments just as a basic bridge does and learns where each physical address is located.
- The learning bridge makes a list of the physical addresses and which port they are connected to.
- Because it stores each frame as it receives it, it then forwards frames selectively based on the LAN to which that physical address is located.

Two-Layer Switches

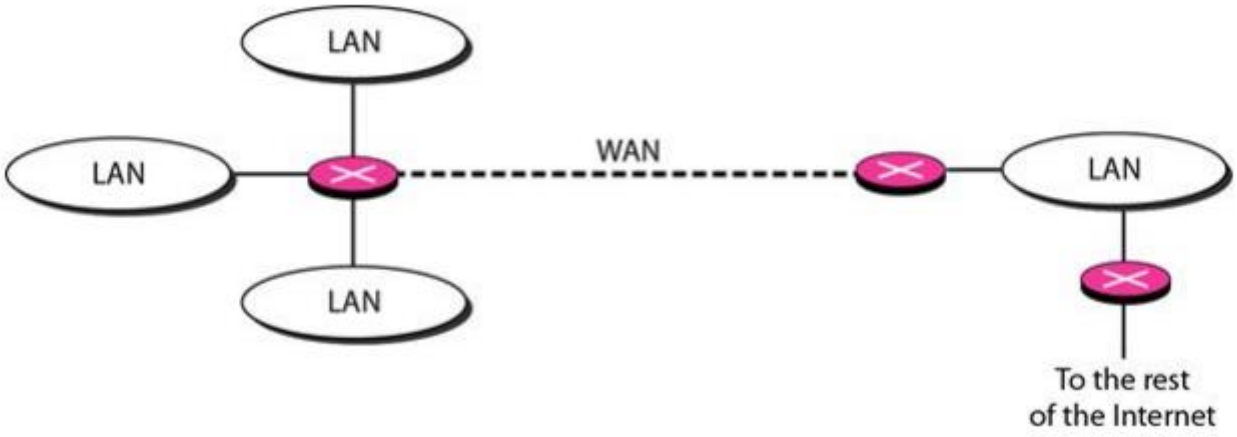
- Switches
- When we use the term switch, we must be careful because a switch can mean two different
- things. We must clarify the term by adding the level at which the device operates. We can have:
- **Two-layer switch: performs at the physical and data link layers.**
- **Three-layer switch. is used at the network layer; it is a kind of router.**

- A two-layer switch is a bridge, a bridge with many ports and a design that allows better(faster) performance.
- A bridge with a few ports can connect a few LANs together.
- A bridgewith many ports may be able to allocate a unique port to each station, with each station on its own independent entity.



Routers

- A router is a three-layer device that routes packets based on their logical addresses (host-tohost addressing).
- A router normally connects LANs and WANs in the Internet and has a routing table that is used for making decisions about the route.
- The routing tables are normally dynamic and are updated using routing protocols.



Gateway

- A gateway is a network node used in telecommunications that connects two networks with different transmission protocols together.
- Gateways serve as an entry and exit point for a network as all data must pass through or communicate with the gateway prior to being routed.