Medium Access Control Layer

UNIT III

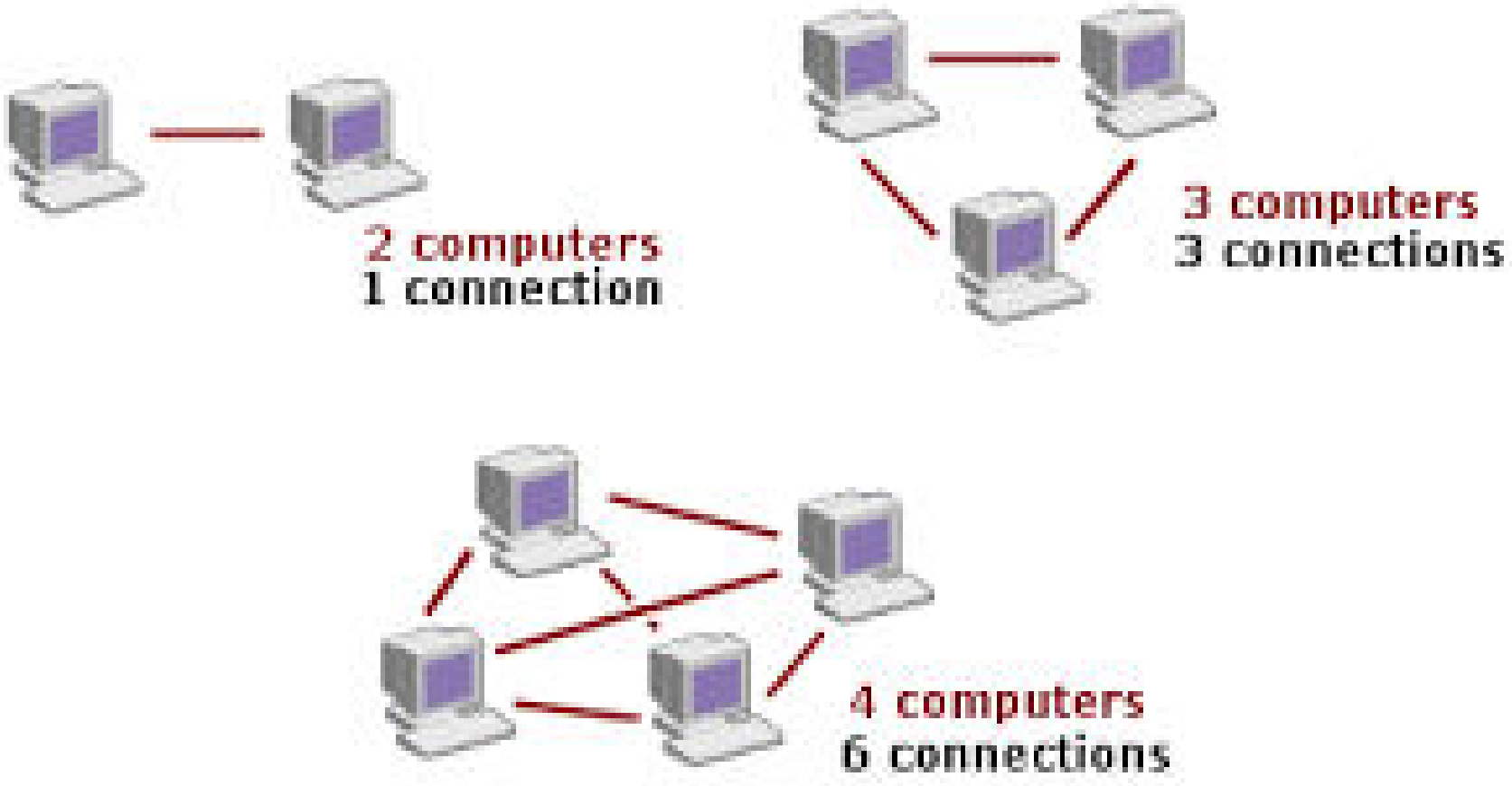
MAC Layer

- Transmission technology can be categorized into two broad categories:

1 Point To Point Networks.

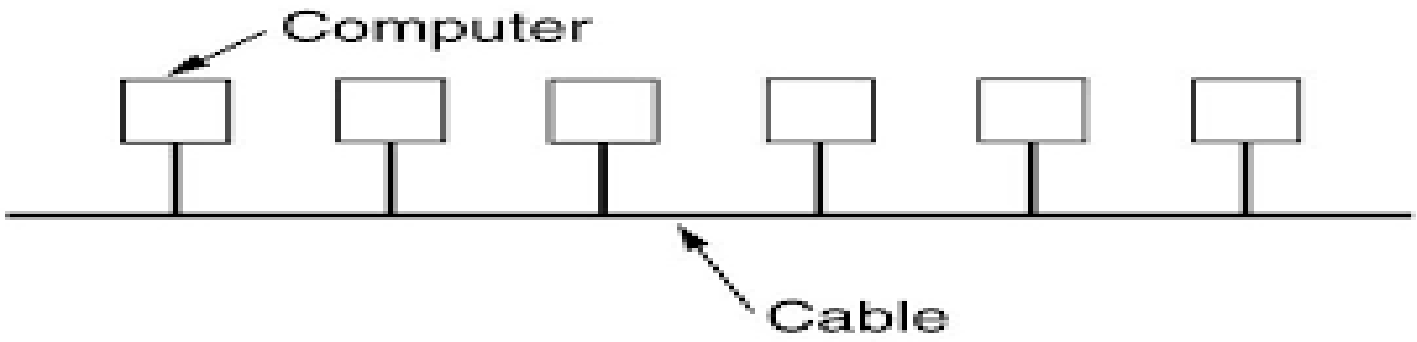
2 Broadcast Networks (Client –Server).

Point To Point Networks



Broadcast Networks

- Single Channel for communication and shared by all the stations.



- Also known as Multi Access Channel or Random Access Channel.

Issues with Multi Access Channel

- Who is going to use the channel?
- When the channel is going to be used?
- For how much time the channel is used?
- Due to shared channel and unregulated traffic over the network collision and data loss occur.
- Some protocol must be followed for regulated and safe transmission over these networks.

Channel Allocation Problem

- What is Channel?
  - The way in which packets/frames can be transferred.
  - Static Channel Allocation.
  - Dynamic Channel Allocation.

Static Channel Allocation

- Path is fix.
- Examples : FDMA, TDMA
- Disadvantage:
  - Busty traffic (too many frames).

Dynamic Channel Allocation

- Assumptions:
  - Independent traffic.
  - Single Channel.
  - Collision Assumption.
  - Time Management:
    - Continuous Time Management.
    - Slotted Time Management.

    —Sensing of Channel:
    - Carrier Sense.
    - No Carrier Sense.

MAC Techniques

Random Channel Protocol	Controlled Access Protocol	Channelization Protocol

• Contention Based
  • Pure Aloha
• Contention Less
  • Slotted Aloha
	• Reservation
	• Pooling
	• Token Passing
		• FDMA
		• TDMA
		• CDMA
		• WDMA

Channelization Protocol

- Frequency Division Multiple Access.
- Time Division Multiple Access.
- Code Division Multiple Access.
- Wavelength Division Multiple Access.

Wavelength Division Multiple Access

- Divide the channel into multiple smaller channels (wavelength bands).
- Allocate channels to users as needed which allow different transmissions to take place at the same time.
- Usually used in fiber optics LANs.
- Each user uses two channels, one small channels to send control packets and another wider channel to send data.

Random Access Protocol

- Contention Based:
  - Multiple computers starts transmission at the same time.
  - Collision occurs.
  - Pure Aloha, CSMA.
- Contention Less:
  - Time slots are provided to transmit the frame.
  - No collision occurs.
  - Slotted Aloha, CSMA/CD, CSMA/CA.

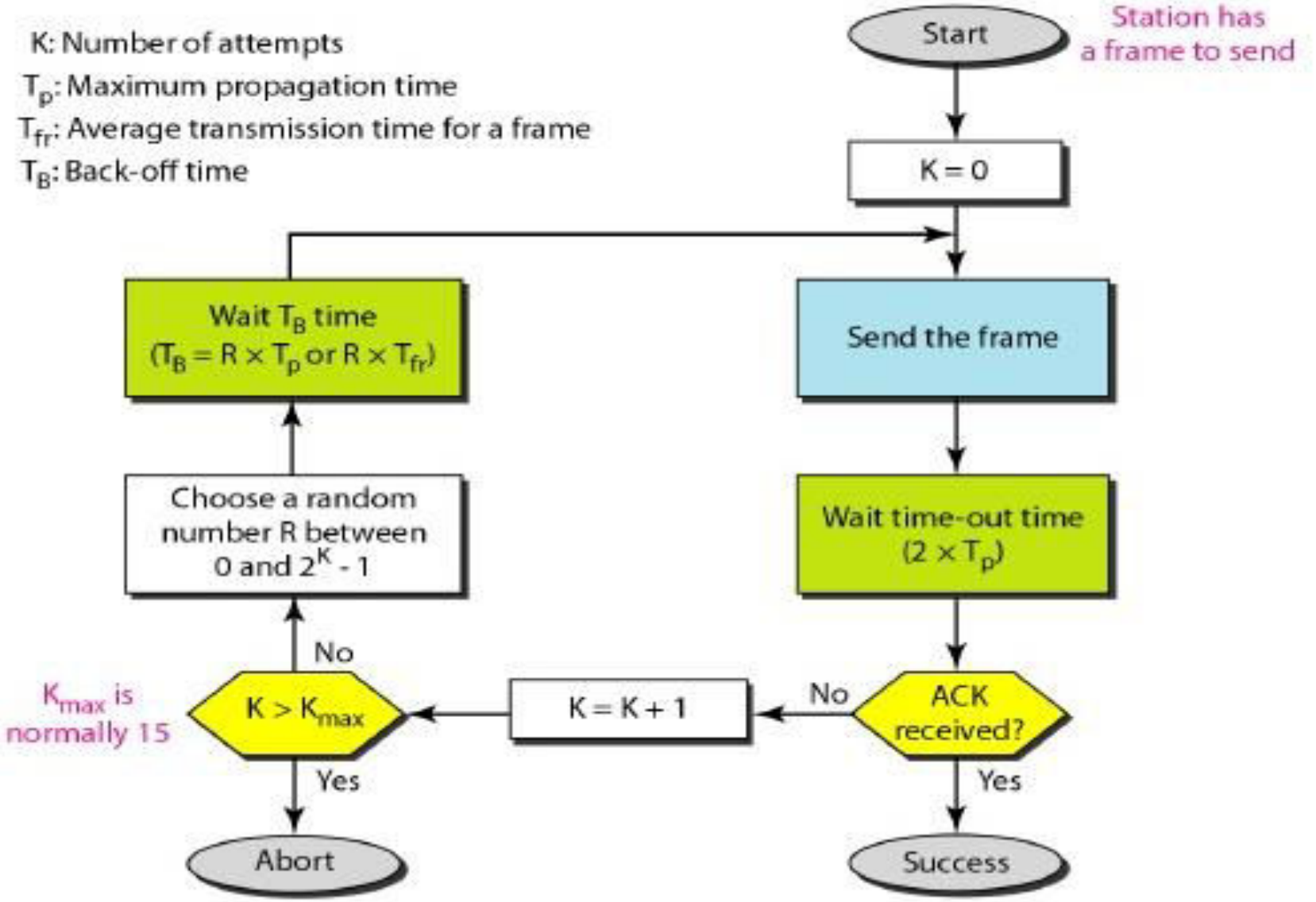
Aloha

- Any time transmit.
- Collision, acknowledgement.
- No need of collision detection.
- After random amount of time (Backoff Time) retransmit, if not get acknowledgement.

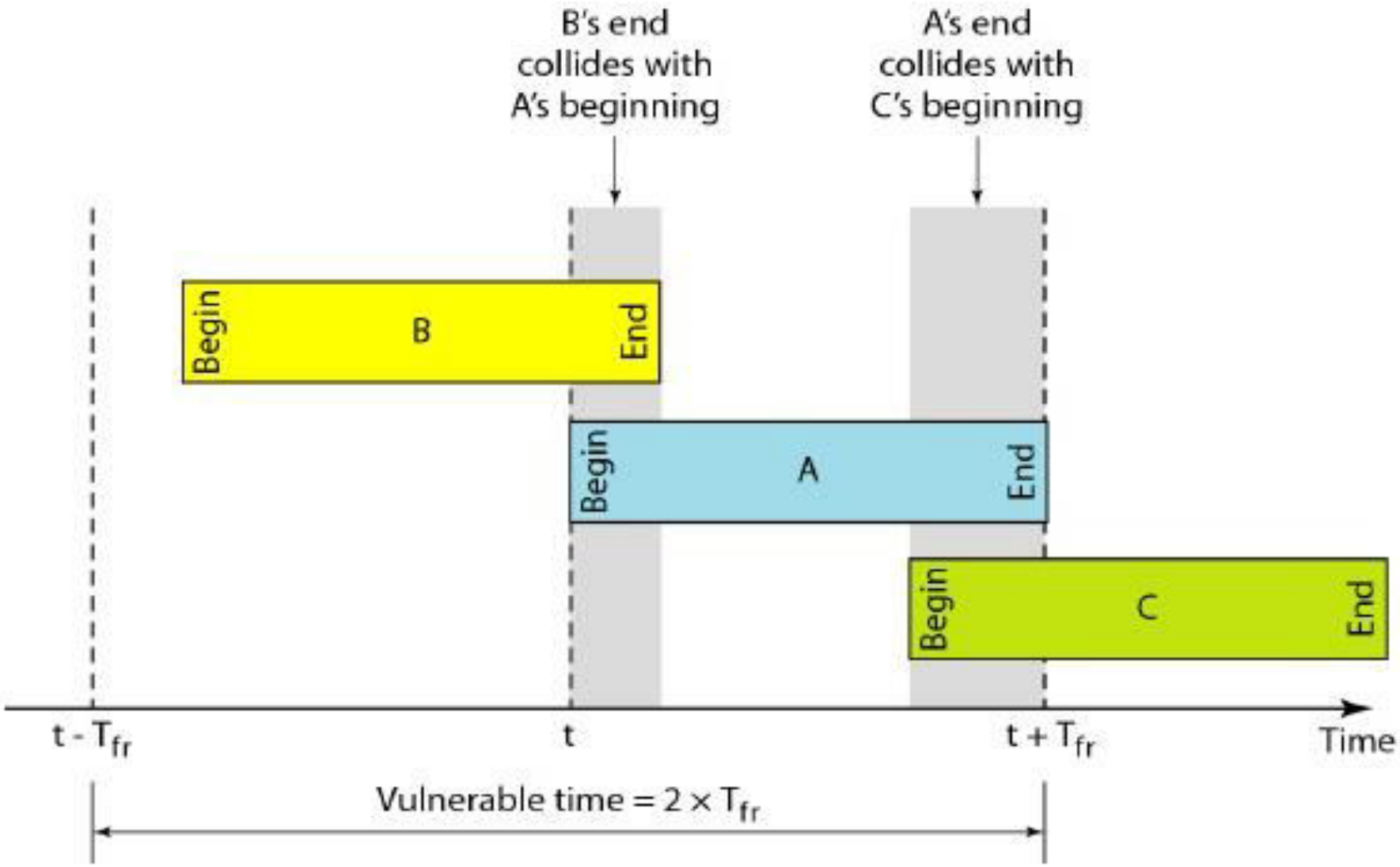
Pure Aloha

- Start transmission of a frame.
- Send the frame.
- Wait for the acknowledgment.
- If ACK is received then the frame successfully delivered to the destination.
- If not then wait for random amount of time (Backoff time) and retransmit the frame.

Procedure for pure ALOHA protocol



Vulnerable time for pure ALOHA protocol

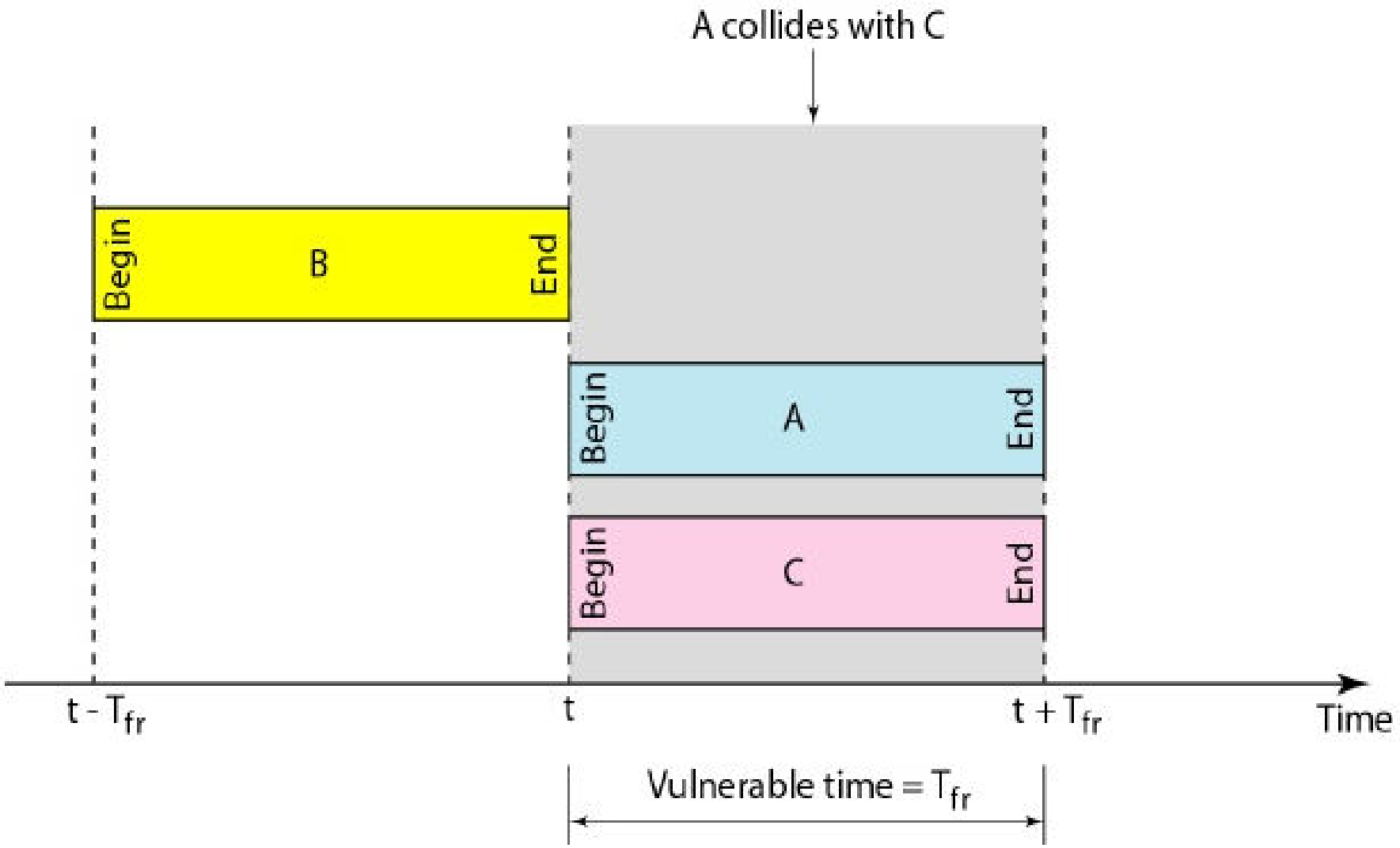


Slotted Aloha

- Divide the time into slots and force the station to send data only beginning of the time slot.
- Throughput:
  - $S = g * e^{-2G}$
- Where

  G = average number of frames generated the system during the transmission.

Vulnerable time for slotted ALOHA protocol



Carrier Sense Multiple Access

- **CSMA** is a **network** protocol that listens to or senses **network** signals on the carrier/medium before transmitting any data.
- **CSMA** is implemented in Ethernet **networks** with more than one computer or **network** device attached to it.
- **CSMA** is part of the Media Access Control (MAC) protocol.

CSMA access modes

- Non Persistent.
- P- Persistent.
  - 1- Persistent
  - P- Persistent

Non Persistent

- Non persistent CSMA is a non aggressive transmission algorithm.
- When the transmitting node is ready to transmit data, it senses the transmission medium for idle or busy.
- If idle, then it transmits immediately.
- If busy, then it waits for a random period of time (during which it does not sense the transmission medium) before repeating the whole logic cycle (which started with sensing the transmission medium for idle or busy) again.
- This approach reduces collision, results in overall higher medium throughput.

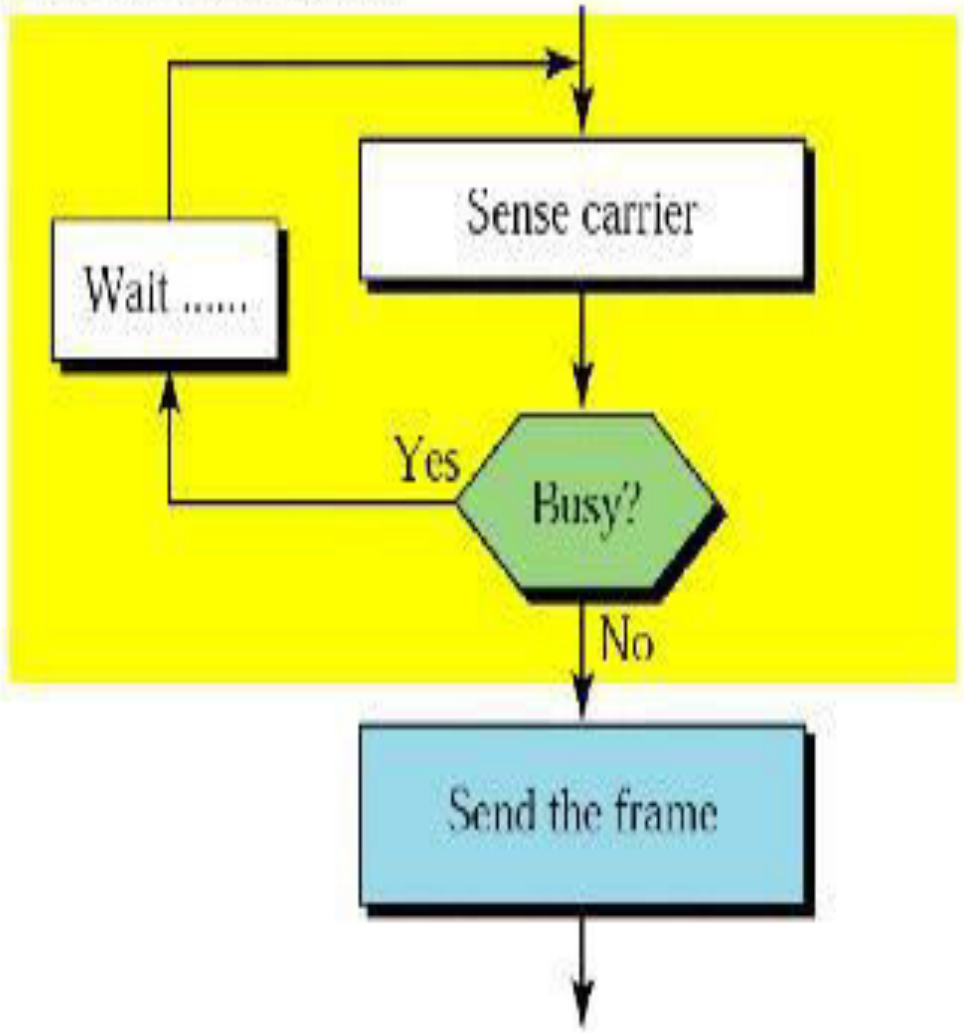
P- Persistent

- 1-persistent CSMA is an aggressive transmission algorithm. When the transmitting node is ready to transmit, it senses the transmission medium for idle or busy.
- If idle, then it transmits immediately.
- If busy, then it senses the transmission medium continuously until it becomes idle, then transmits the message (a frame) unconditionally (i.e. with probability=1).
- In case of a collision, the sender waits for a random period of time and attempts the same procedure again.
- 1-persistent CSMA is used in CSMA/CD systems including Ethernet.

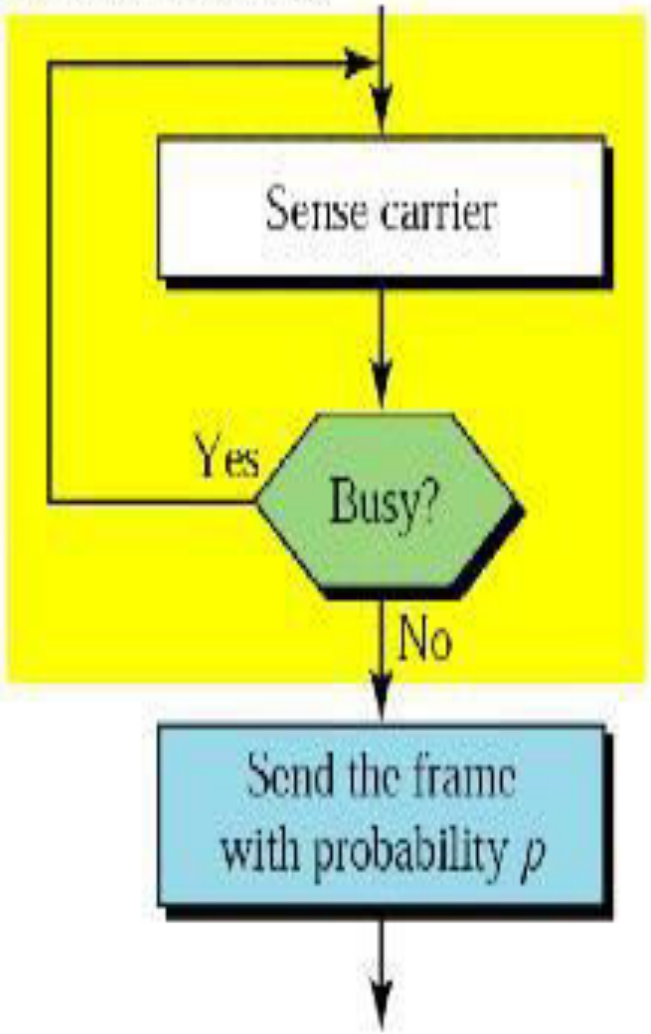
P- Persistent

- This is an approach between 1-persistent and non-persistent CSMA access modes.
- When the transmitting node is ready to transmit data, it senses the transmission medium for idle or busy.
- If idle, then it transmits a frame with probability *p*.
- If busy, then it senses the transmission medium continuously until it becomes idle, then transmits with probability *p*.
- If the node does not transmit (the probability of this event is *1-p*), it waits until the next available time slot.
- If the transmission medium is still not busy, it transmits again with the same probability *p*. This probabilistic hold-off repeats until the frame is finally transmitted or when the medium is found to become busy again (i.e. some other node has already started transmitting).
- In the latter case the node repeats the whole logic cycle (which started with sensing the transmission medium for idle or busy) again.
- p-persistent CSMA is used in CSMA/CA systems including Wi-Fi and other packet radio systems.

Nonpersistent strategy

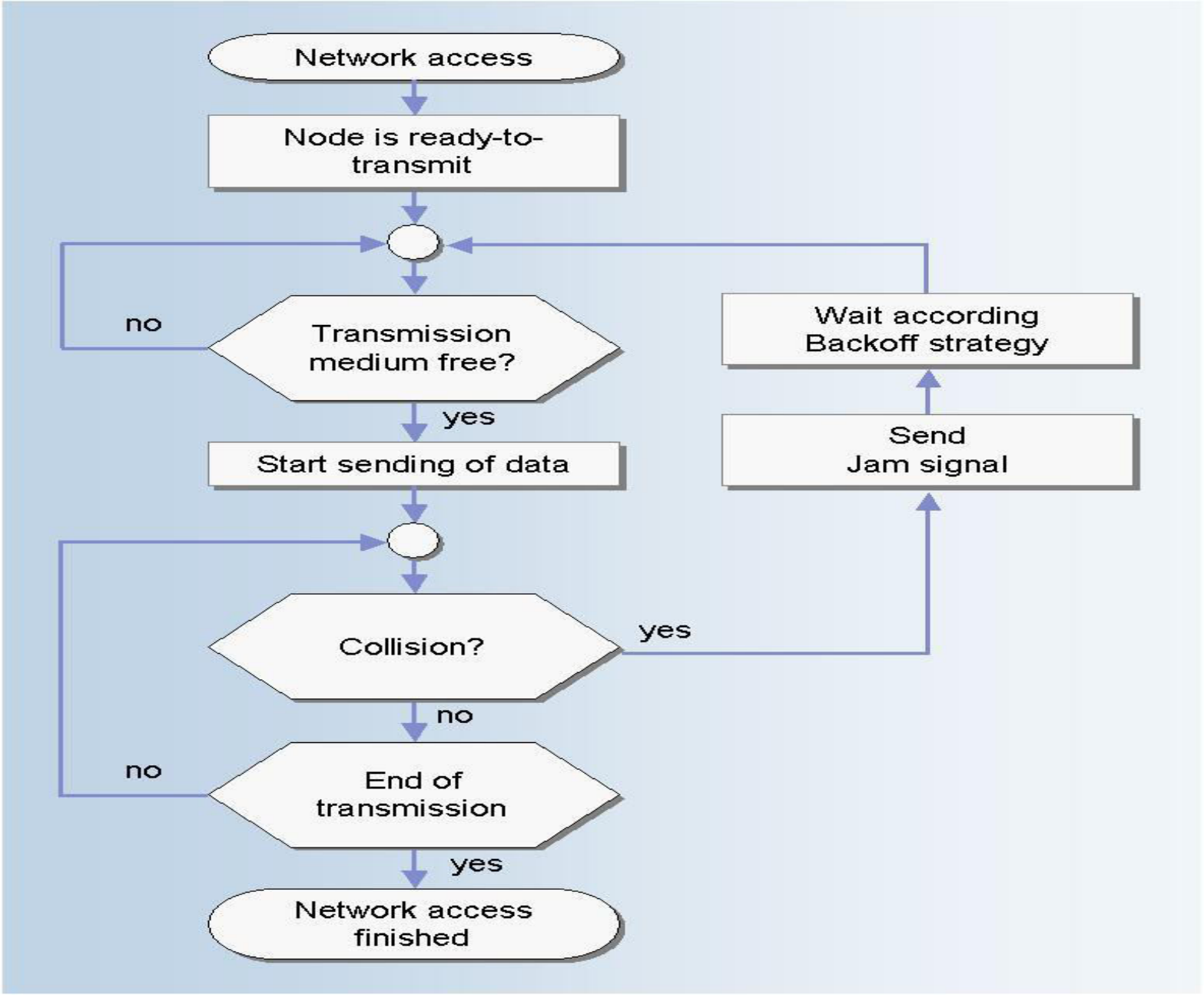


Persistent strategy



CSMA/Collision Detection

- Station checks whether another station is transmitting.
- If not, it sends the first bit of information.
- If no collision is detected, it continues to send the other bits of information while continuously checking whether a collision has been detected.
- If a collision is detected, it calculates a random amount of time to wait and start the process again.
- If the maximal amount of attempts is reached, then no transmission is possible and it is aborted.

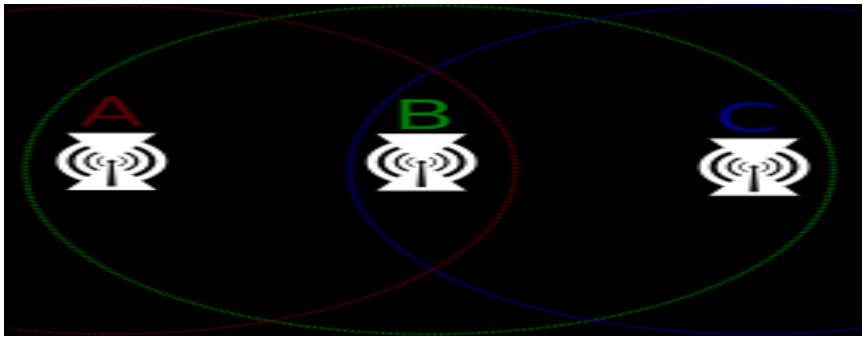

Network access
Node is ready-to-transmit
Transmission medium free?
no
yes
Start sending of data
Collision?
yes
Send Jam signal
Wait according Backoff strategy
no
End of transmission
no
yes
Network access finished

CSMA/CD

- Drawback with CSMA/CD
  - In wireless communication, when a receiver is within the range of two active transmitters, the resulting signal will get garbled(most of the time).
  - CSMA/CD is unsuitable in this situation.

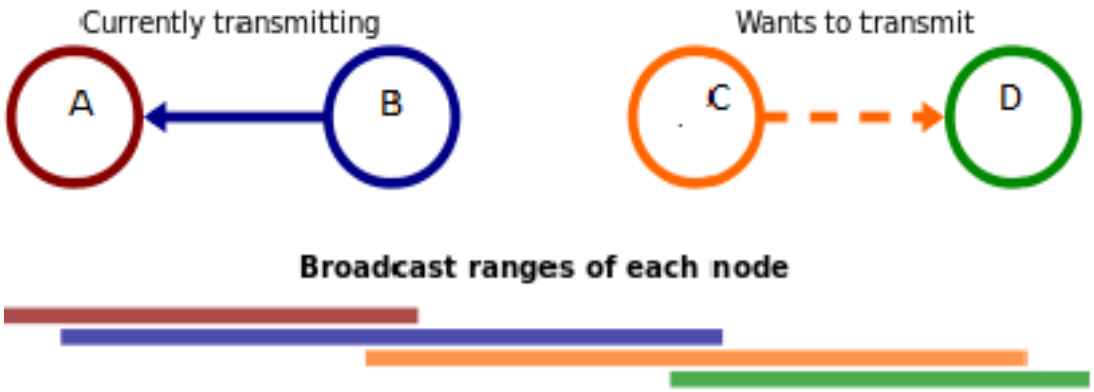
Hidden Node Problem

- Station A can communicate with Station B. Station C can also communicate with Station B. However, Stations A and C cannot communicate with each other since they cannot sense each other on the network, because they are out of range of each other.



Exposed Node Problem

- In wireless networks, exposed node problem occurs when a node is prevented from sending packets to other nodes because of a neighboring node is transmitter.



Carrier Sense Multiple Access/Collision Avoidance

- Sender sends a short frame called Request To Send (RTS) frame of 20 byte to destination.
- Destination responds with a short frame Clear To Send (CTS).
- Four way Handshake protocol:

Standard for LANs

- IEEE 802.2 - LLC.
- IEEE 802.3 – Ethernet.
- IEEE 802.4 – Token Bus.
- IEEE 802.5 – Token Ring.

Ethernet Evolution

Standard Ethernet	Fast Ethernet	Gigabit Ethernet	Ten Gigabit Ethernet
10 Mbps	100 Mbps	1 Gbps	10 Gbps

Standard Ethernet

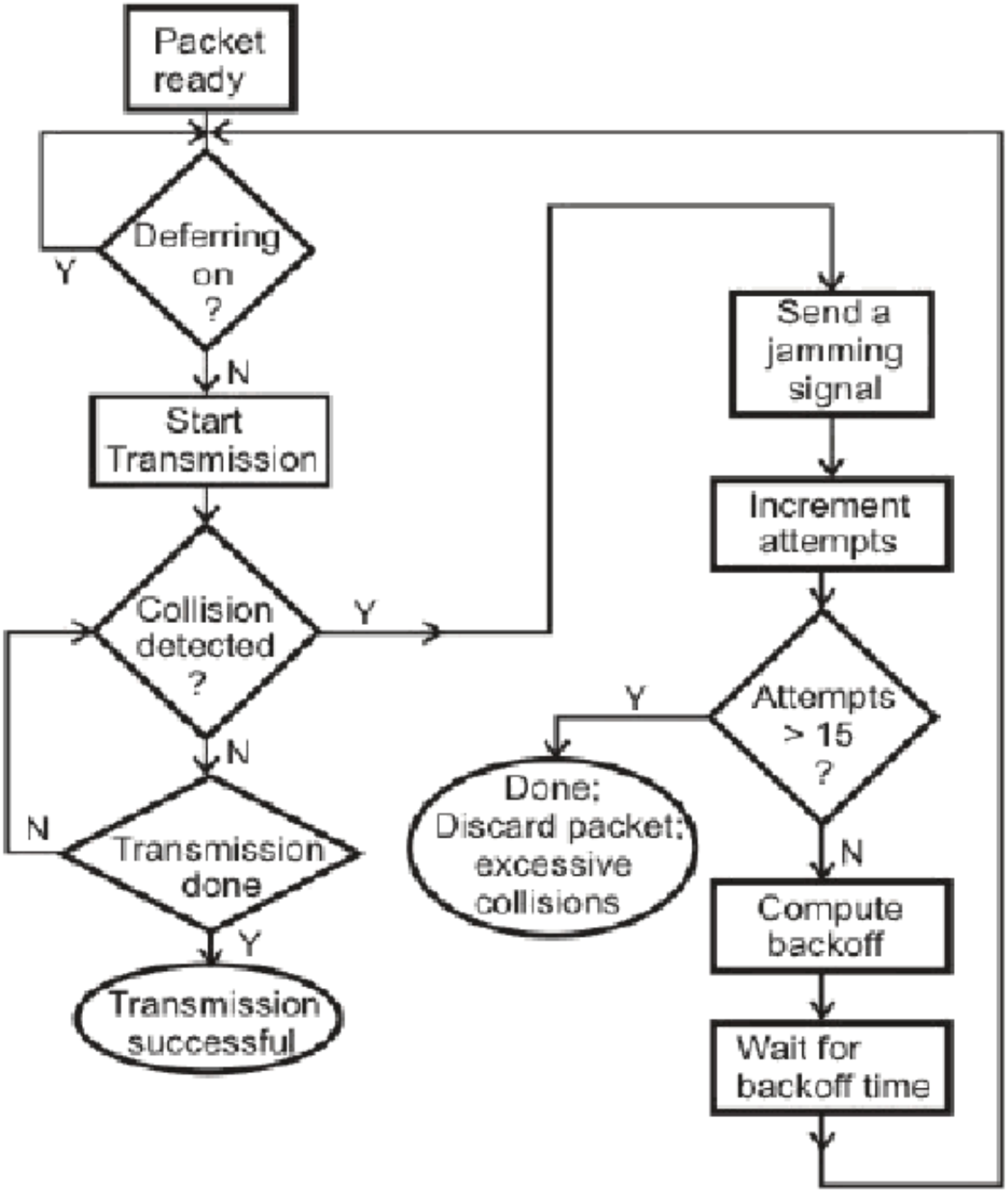
	10 Base 2	**10 Base 5**	**10 Base T**	**10 Base F**
Media	Thin Co axial	Thick Co axial	UTP	Fiber
Max Length (m)	185	500	100	2000
Line Encoding	Manchester Encoding			

Frame Format of 802.3

Preamble 10101010	**Start Frame Delimiter 10101011**	**Destination Address**	**Source Address**	**Type/ Length**	**Data**	**CRC**
7 Byte	1 Byte	6 Byte	6 Byte	2 Byte		4 Byte

Binary Exponential Back -off algorithm

- Binary Exponential Back off (BEB) refers to a collision resolution mechanism used in random access MAC protocols.
- This algorithm is used in Ethernet (IEEE 802.3) wired LANs.
- In Ethernet networks, this algorithm is commonly used to schedule retransmissions after collisions.


Packet ready
Deferring on ?
Y
N
Start Transmission
Collision detected ?
Y
N
Transmission done
N
Y
Transmission successful
Send a jamming signal
Increment attempts
Attempts > 15 ?
Y
N
Done; Discard packet; excessive collisions
Compute backoff
Wait for backoff time

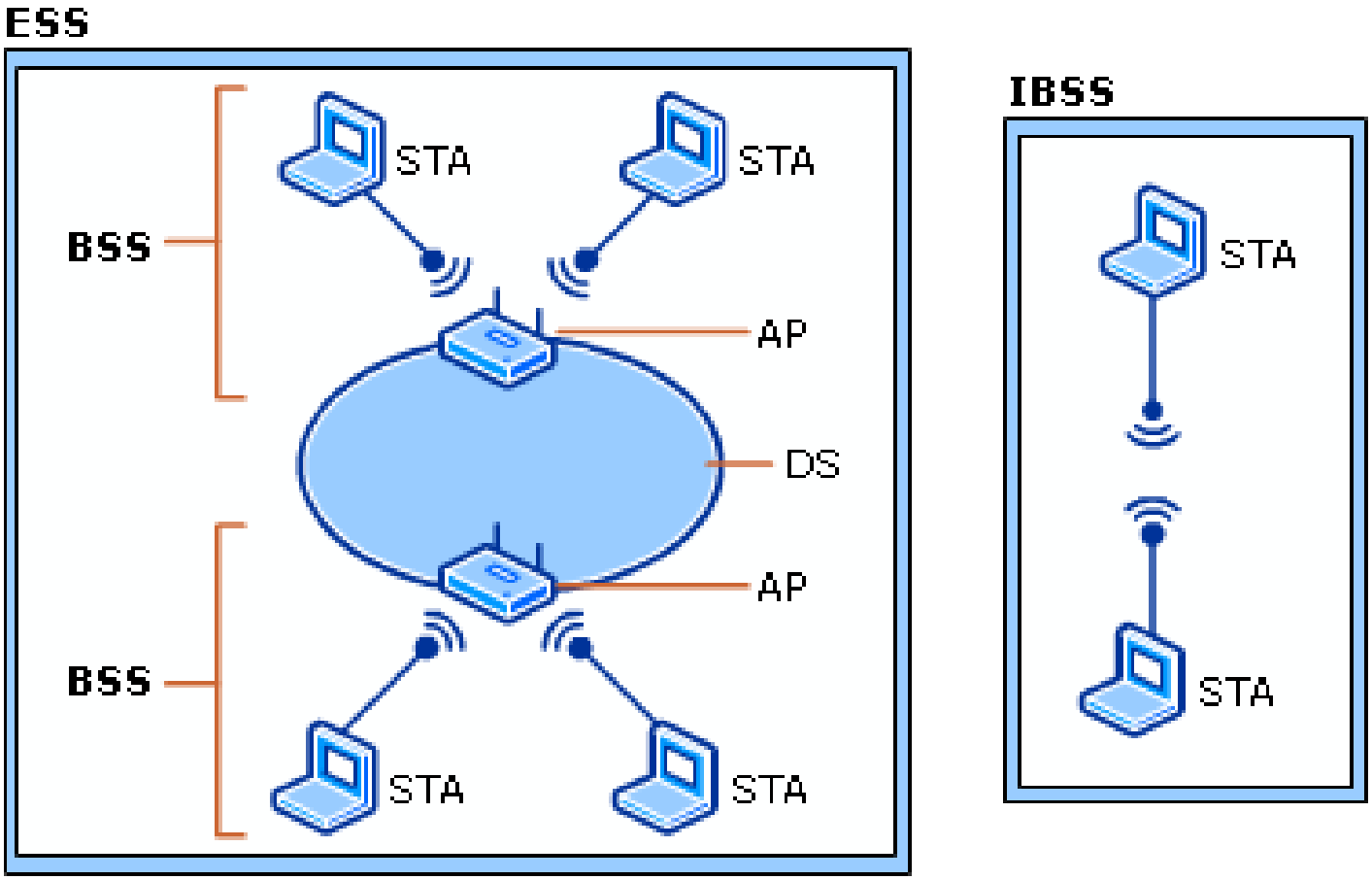
IEEE 802.11

- **IEEE 802.11** is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the 900 MHz and 2.4, 3.6, 5, and 60 GHz frequency bands.

802.11 Architecture

- The 802.11 logical architecture contains several main components: station (STA), wireless access point (AP), independent basic service set (IBSS), basic service set (BSS), distribution system (DS), and extended service set (ESS).
- Some of the components of the 802.11 logical architecture map directly to hardware devices, such as STAs and wireless APs.
- The wireless STA contains an adapter card, PC Card, or an embedded device to provide wireless connectivity.
- The wireless AP functions as a bridge between the

802.11 Architecture

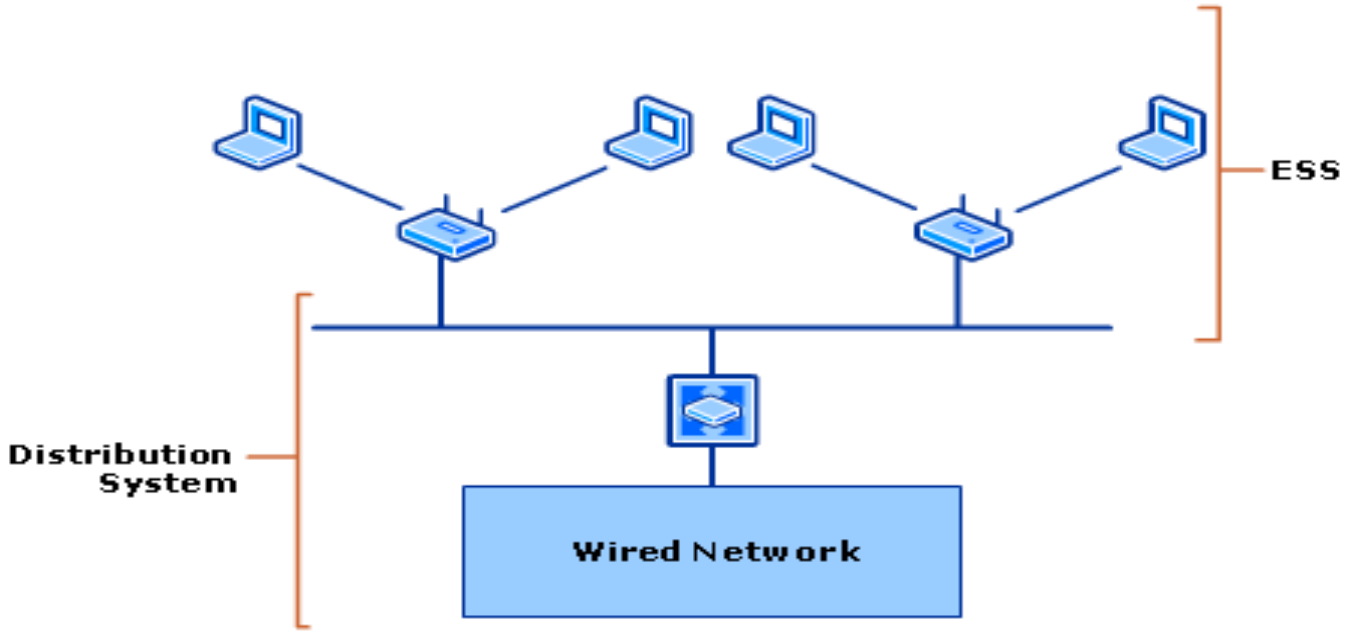


802.11 Operating Modes

- IEEE 802.11 defines the following operating modes:
  - Infrastructure mode
  - Ad hoc mode

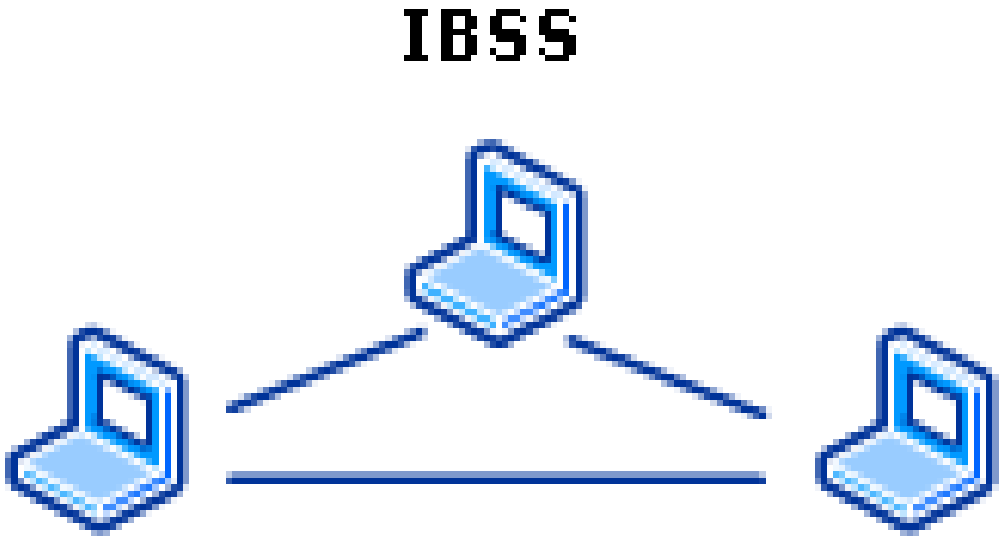
802.11 Infrastructure Mode

- In *infrastructure mod*e, there is at least one wireless AP and one wireless client. The wireless client uses the wireless AP to access the resources of a traditional wired network.

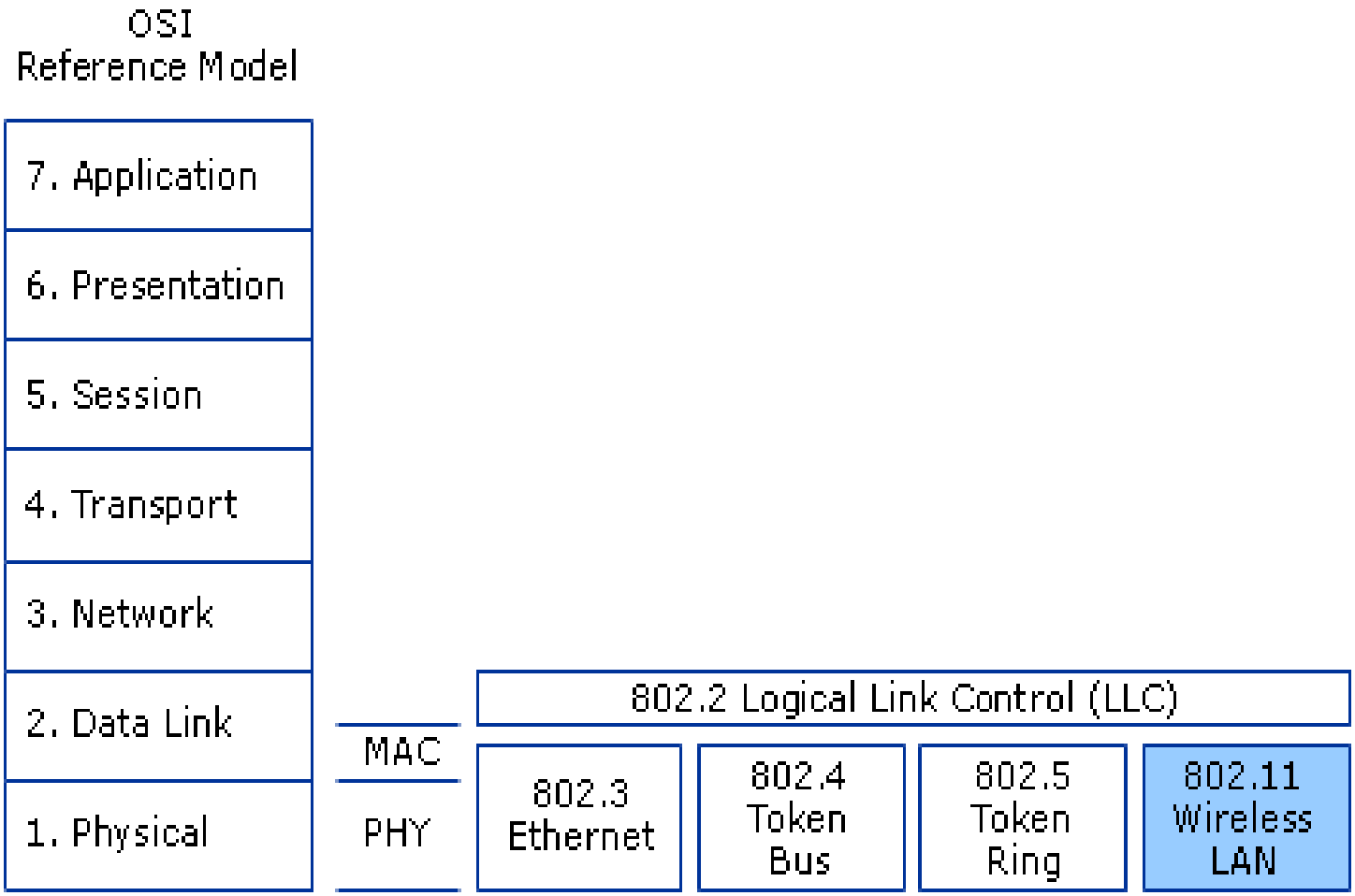


802.11 Ad Hoc Mode

- In *ad hoc mode*, wireless clients communicate directly with each other without the use of a wireless AP.

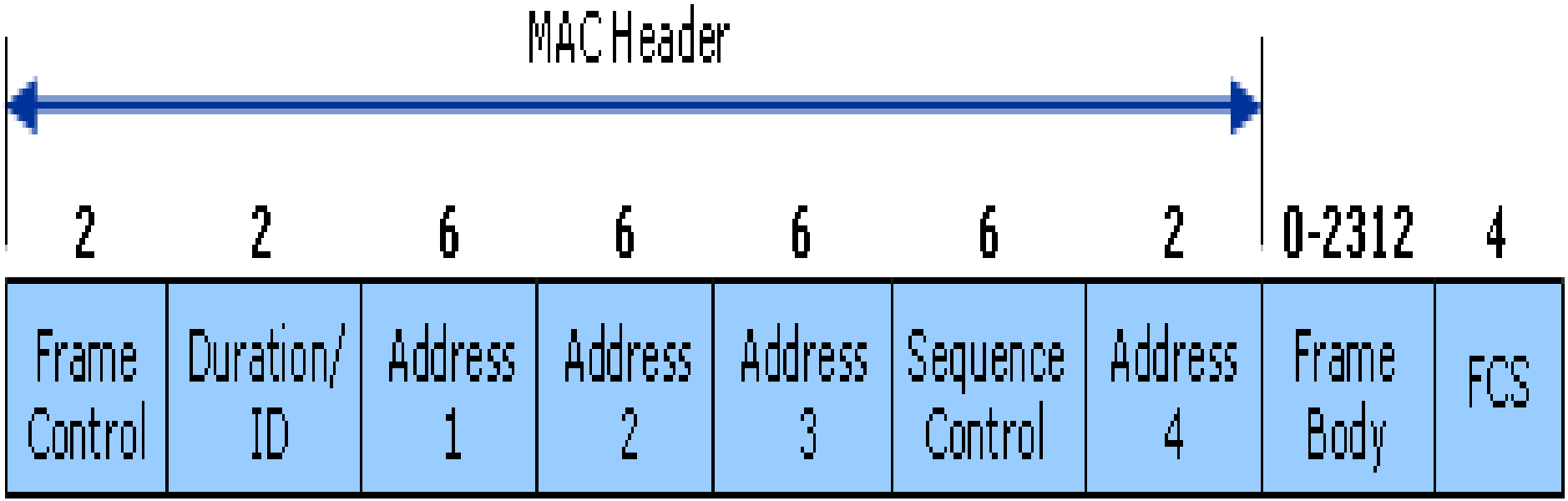


802.11 and OSI Model

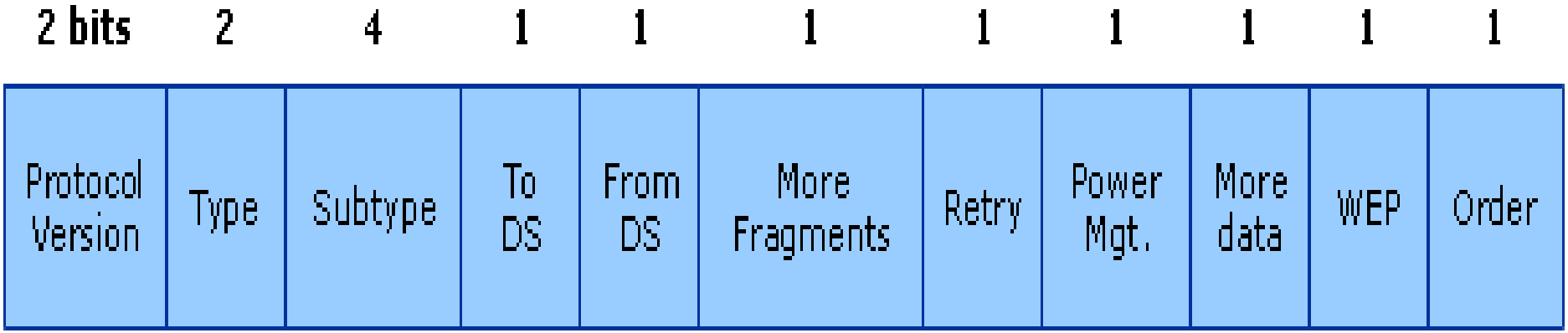


Frame Format of 802.11

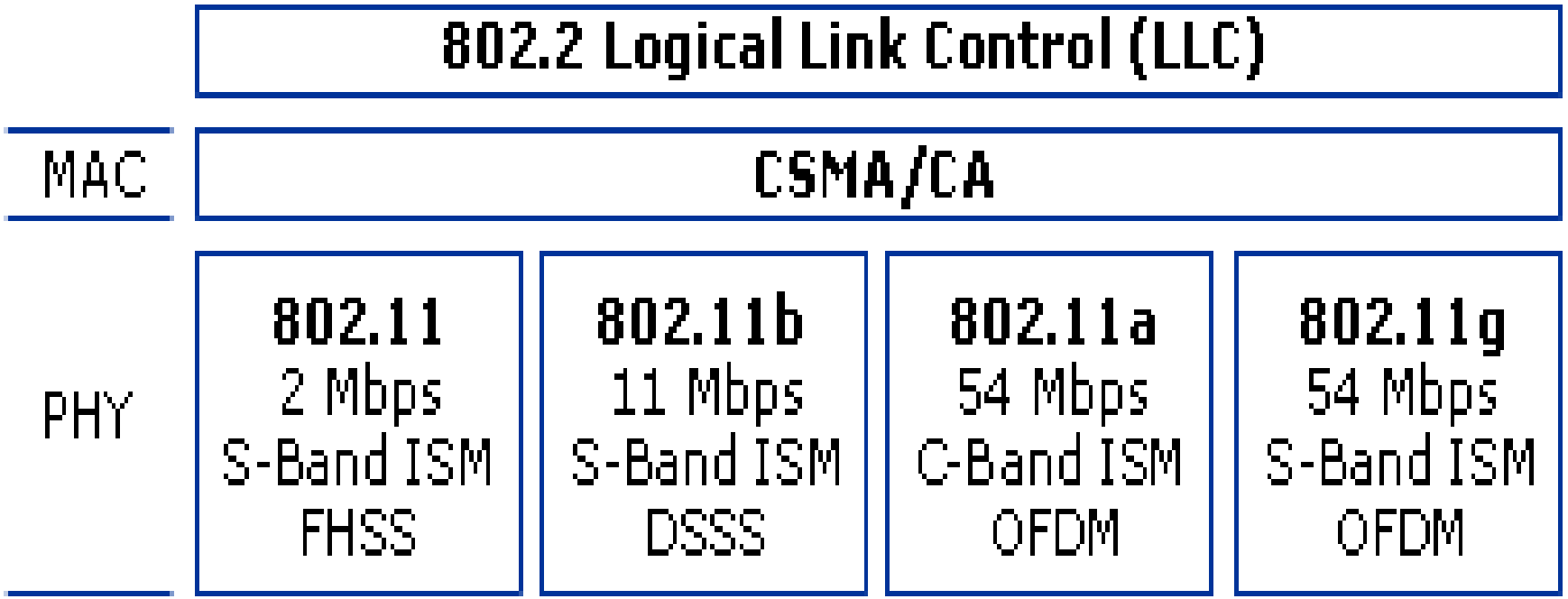
- General frame format of 802.11:



Frame Control Field



Standards for 802.11 at the PHY Layer



Bluetooth - What is Bluetooth?

- Bluetooth is a wireless LAN technology used to connect devices of different functions such as telephones, computers (laptop or desktop), notebooks, cameras, printers.
- Bluetooth devices have a built-in short range radio transmitter. The rate provided is 1Mbps and uses 2.4 GHz bandwidth.
- Bluetooth is that when the device is within the scope of a other devices automatically start the transfer information without the user noticing.
- A small network between the devices is created and the user can accessed as if there were cables.

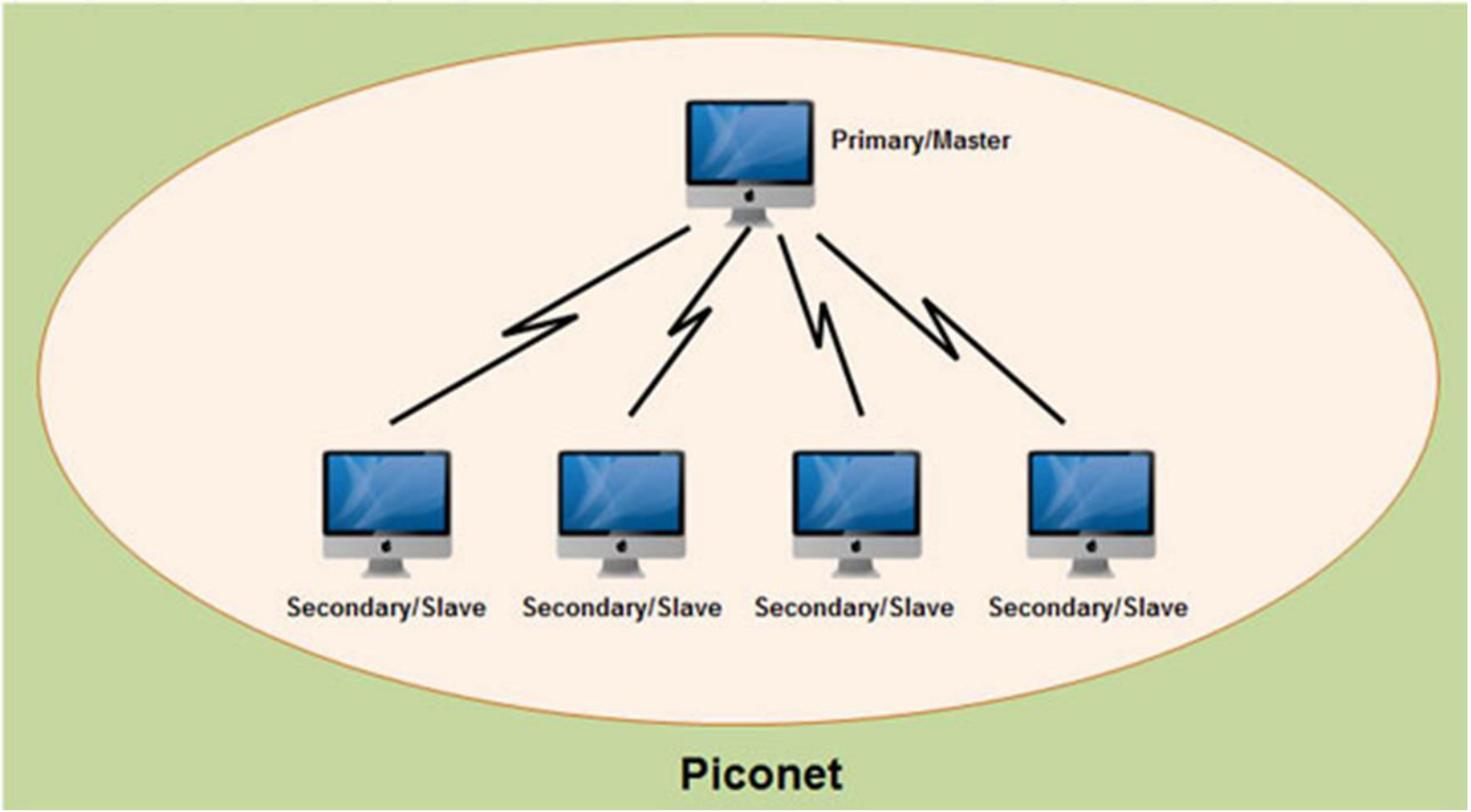
Bluetooth Architecture

- Bluetooth architecture defines two types of networks:
    1. Piconet
    2. Scatternet

Piconet

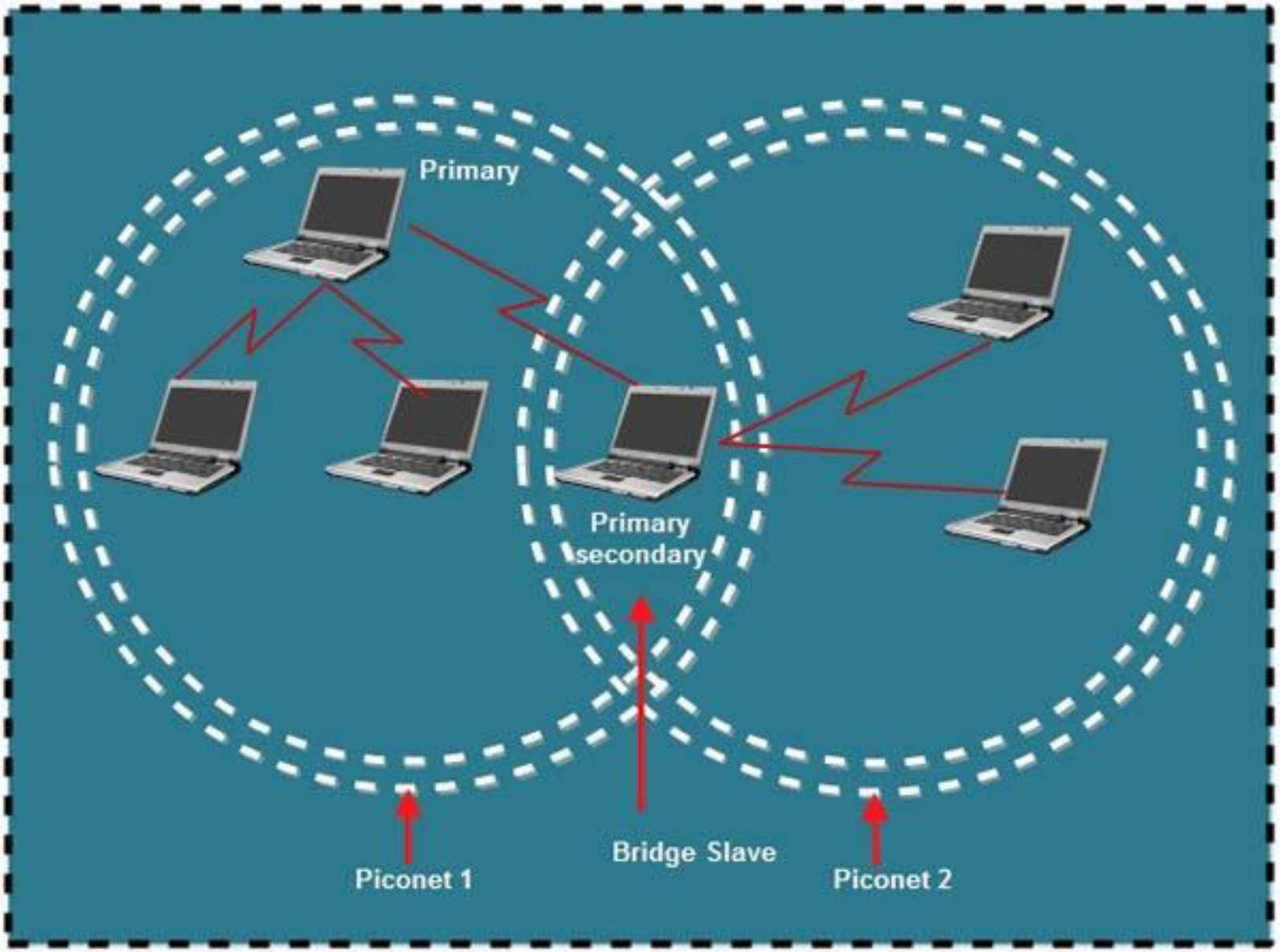
- Piconet is a Bluetooth network that consists of one primary (master) node and seven active secondary (slave) nodes.
- Thus, piconet can have upto eight active nodes (1 master and 7 slaves) or stations within the distance of 10 meters.
- There can be only one primary or master station in each piconet.
- The communication between the primary and the secondary can be one-to-one or one-to-many.

Piconet

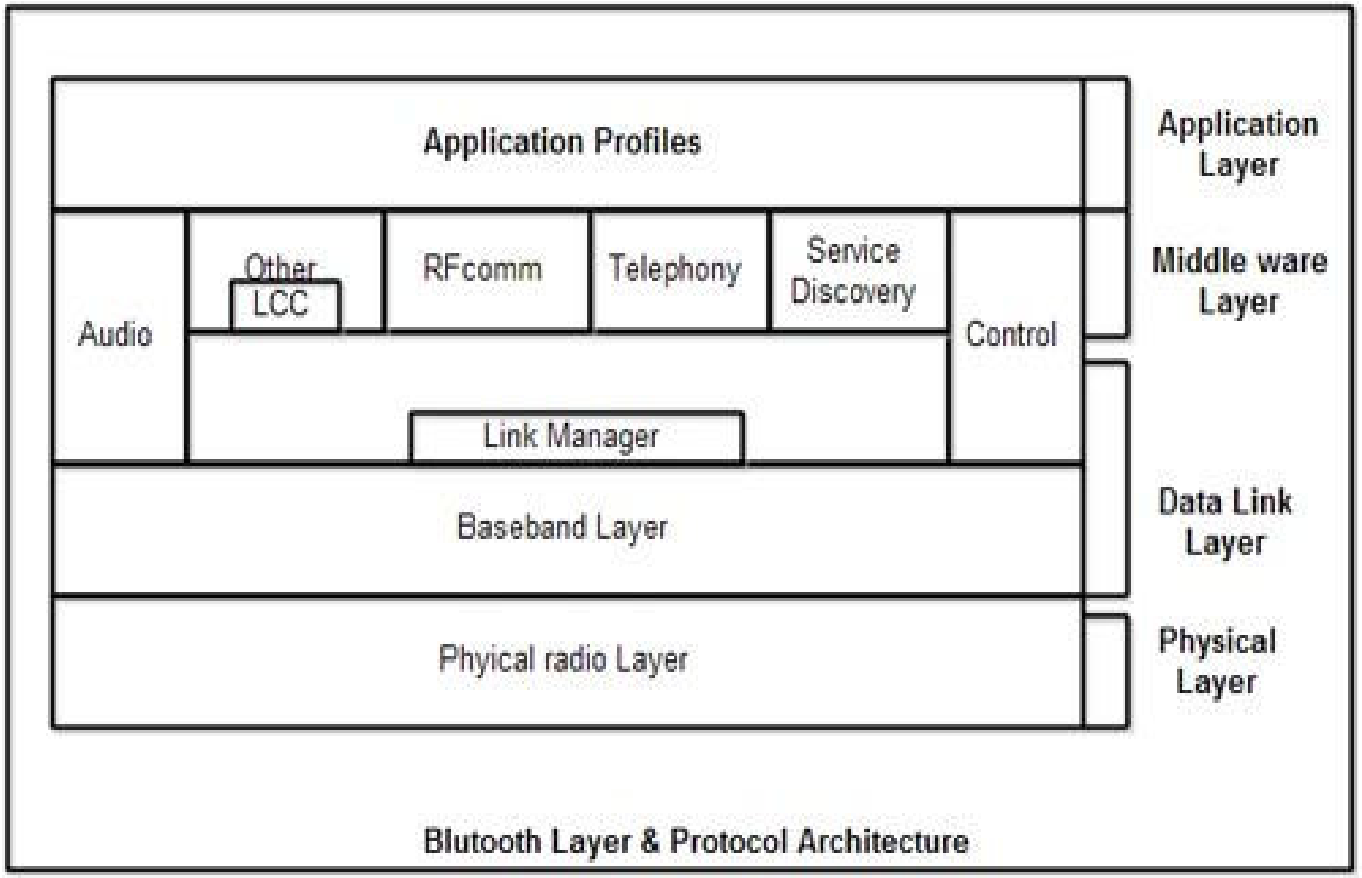

Primary/Master
Secondary/Slave
Secondary/Slave
Secondary/Slave
Secondary/Slave
Piconet

Scatternet

- Scatternet is formed by combining various piconets.
- A slave in one piconet can act as a master or primary in other piconet.
- Such a station or node can receive messages from the master in the first piconet and deliver the message to its slaves in other piconet where it is acting as master. This node is also called bridge slave.
- Thus a station can be a member of two piconets.
- A station cannot be a master in two piconets.


Primary
Primary
secondary
Bridge Slave
Piconet 1
Piconet 2

Bluetooth layers and Protocol Stack



Radio Layer

- The Bluetooth radio layer corresponds to the physical layer of OSI model.
- It deals with ratio transmission and modulation.
- The radio layer moves data from master to slave or vice versa.
- It is a low power system that uses 2.4 GHz ISM band in a range of 10 meters.
- This band is divided into 79 channels of 1MHz each. Bluetooth uses the Frequency Hopping Spread Spectrum (FHSS) method in the physical layer to avoid interference from other devices or networks

Baseband Layer

- Baseband layer is equivalent to the MAC sub layer in LANs.
- Bluetooth uses a form of TDMA called TDD-TDMA (time division duplex TDMA).
- Master and slave stations communicate with each other using time slots.
- The master in each piconet defines the time slot of 625 μsec.
- In TDD- TDMA, communication is half duplex in which receiver can send and receive data but not at the same time.
- If the piconet has only no slave; the master uses even numbered slots (0, 2, 4, ...) and the slave uses odd-numbered slots (1, 3, 5, ...). Both master and slave communicate in half duplex mode. In slot 0, master sends & secondary receives; in slot 1, secondary sends and primary receives.
- If piconet has more than one slave, the master uses even numbered slots. The slave sends in the next odd-numbered slot if the packet in the previous slot was addressed to it.

Logical Link, Control Adaptation Protocol Layer (L2CAP)

- The logical unit link control adaptation protocol is equivalent to logical link control sublayer of LAN.
- The various function of L2CAP is:

1. Segmentation and reassembly

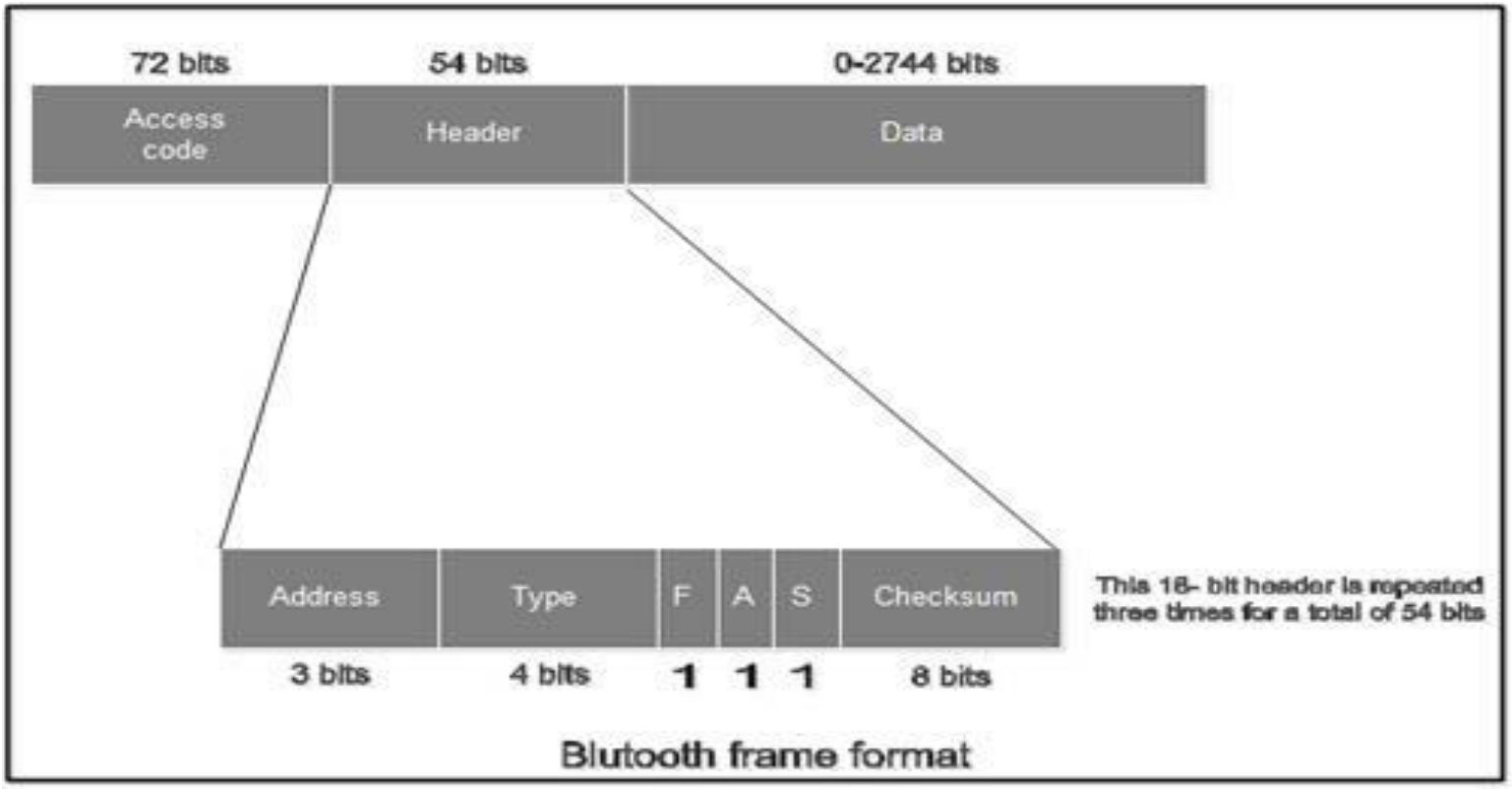
- L2CAP receives the packets of upto 64 KB from upper layers and divides them into frames for transmission.
- It adds extra information to define the location of frame in the original packet.
- The L2CAP reassembles the frame into packets again at the destination.

2. Multiplexing

- L2CAP performs multiplexing at sender side and demultiplexing at receiver side.
- At the sender site, it accepts data from one of the upper layer protocols frames them and deliver them to the Baseband layer.
- At the receiver site, it accepts a frame from the baseband layer, extracts the

- **3. Quality of Service (QOS)**
- L2CAP handles quality of service requirements, both when links are established and during normal operation.
- It also enables the devices to negotiate the maximum payload size during connection establishment.

Bluetooth Frame Format



1. **Access Code**: It is 72 bit field that contains synchronization bits. It identifies the master.

2. **Header**: This is 54-bit field. It contain 18 bit pattern that is repeated for 3 time.

The header field contains following subfields:

(i) **Address**: This 3 bit field can define upto seven slaves (1 to 7). If the address is zero, it is used for broadcast communication from primary to all secondary.

(ii)Type: This 4 bit field identifies the type of data coming from upper layers.

(iii) **F**: This flow bit is used for flow control. When set to 1, it means the device is unable to receive more frames.

(iv) **A**: This bit is used for acknowledgement.

(v) **S**: This bit contains a sequence number of the frame to detect retransmission. As stop and wait protocol is used, one bit is sufficient.

(vi) **Checksum**: This 8 bit field contains checksum to detect errors in header.

3. **Data**: This field can be 0 to 2744 bits long. It contains data or control information coming from upper layers