# Medium Access Control
# Unit III

Channel allocation: Static and Dynamic

Multiple Access Protocols: Pure and Slotted ALOHA

CSMA, WDMA, IEEE 802.3 Standards and Frame Formats,

CSMA/CD, Fast Ethernet, Gigabit Ethernet

IEEE 802.11a/b/g/n

IEEE 802.15 and IEEE 802.16 Standards, CSMA/CA.

# Multiple access protocols

- Multiple access protocols are generally used to coordinate access to link, here nodes can regulate their transmission onto the shared broadcast channels by using multiple access protocol, It is used on both wired and wireless LAN and satellite network.

- Multiple nodes can transmit frames at the same time, if so the transmitted frame collides at the entire receiver. When there is a collision, there is no acknowledgement to the receiver that the frame is transmitted or not.

- Thus, all frames involved in the collision are lost, and the broadcast channel is wasted during the collision interval. To rectify this problem Multiple Access protocol is implemented.

# Functions of MAC

- The functions performed by Medium Access Protocol are given below –
- It delimits and recognizes the frames
- It is responsible for addressing at layer 2
- Error checking by using frame check sequences (FCS)
- Physical transmission medium's access control

# What is channel allocation in computer network?

- The network channel may be a single cable or optical fiber connecting multiple nodes, or a portion of the wireless spectrum. Channel allocation algorithms allocate the wired channels and bandwidths to the users, who may be base stations, access points or terminal equipment.
- Channel Allocation Schemes

1. Static Channel Allocation
2. Dynamic Channel Allocation

# Static Channel Allocation

- In static channel allocation scheme, a fixed portion of the frequency channel is allotted to each user.
- For N competing users, the bandwidth is divided into N channels using frequency division multiplexing (FDM), and each portion is assigned to one user.
- This scheme is also referred as fixed channel allocation or fixed channel assignment.
- In this allocation scheme, there is no interference between the users since each user is assigned a fixed channel.
- However, it is not suitable in case of a large number of users with variable bandwidth requirements.

# Dynamic Channel Allocation

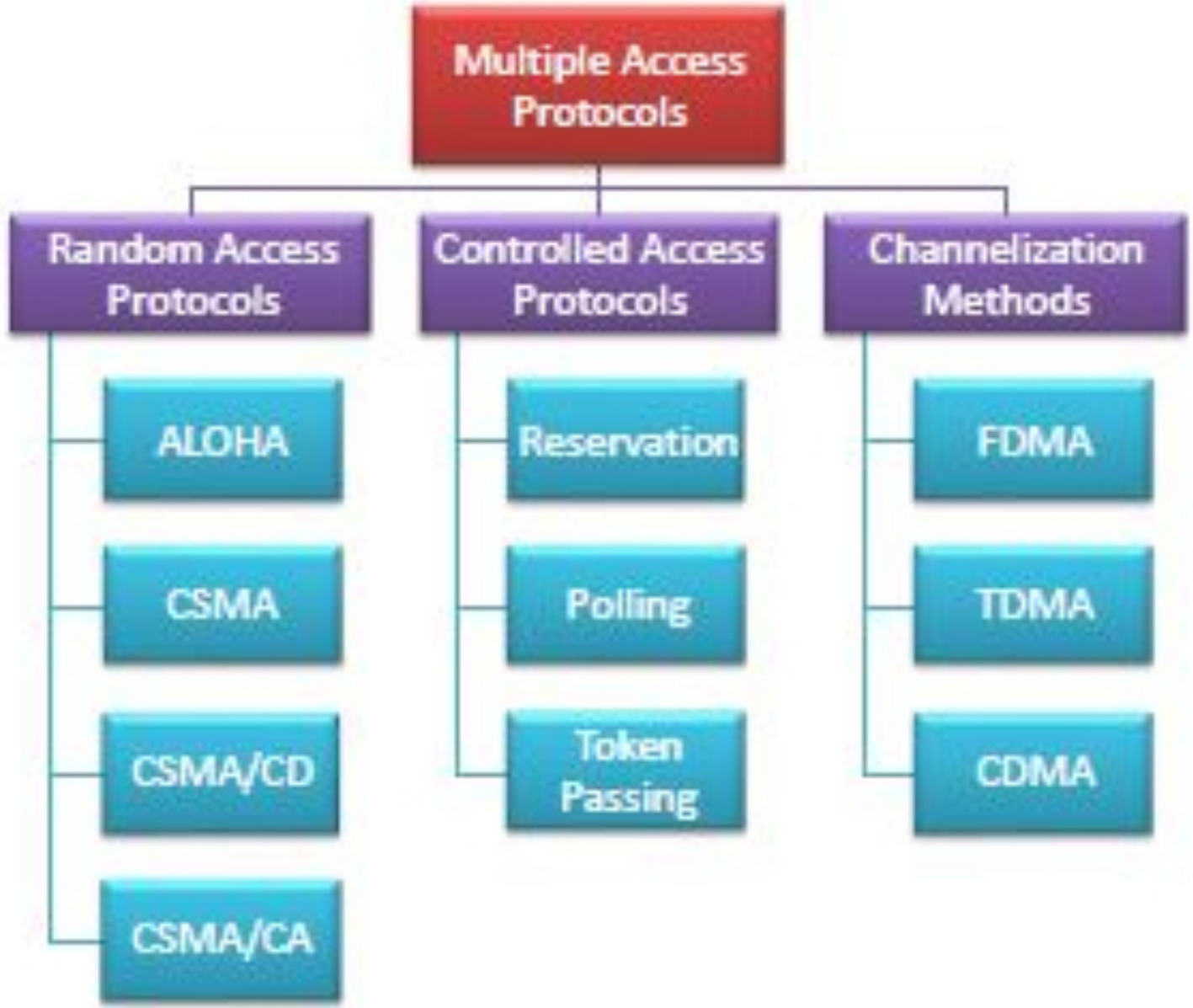
- In dynamic channel allocation scheme, frequency bands are not permanently assigned to the users. Instead channels are allotted to users dynamically as needed, from a central pool. The allocation is done considering a number of parameters so that transmission interference is minimized.

- This allocation scheme optimizes bandwidth usage and results is faster transmissions.

- Dynamic channel allocation is further divided into centralized and distributed allocation.

# Multiple Access Protocols

- Multiple access protocols are a set of protocols operating in the Medium Access Control sublayer (MAC sublayer) of the Open Systems Interconnection (OSI) model.
- These protocols allow a number of nodes or users to access a shared network channel.
- Several data streams originating from several nodes are transferred through the multi-point transmission channel.
- The objectives of multiple access protocols are optimization of transmission time, minimization of collisions and avoidance of crosstalks.


Multiple Access Protocols
Random Access Protocols
Controlled Access Protocols
Channelization Methods
ALOHA
CSMA
CSMA/CD
CSMA/CA
Reservation
Polling
Token Passing
FDMA
TDMA
CDMA

# Random Access Protocols

- Random access protocols assign uniform priority to all connected nodes. Any node can send data if the transmission channel is idle. No fixed time or fixed sequence is given for data transmission.
- The four random access protocols are−

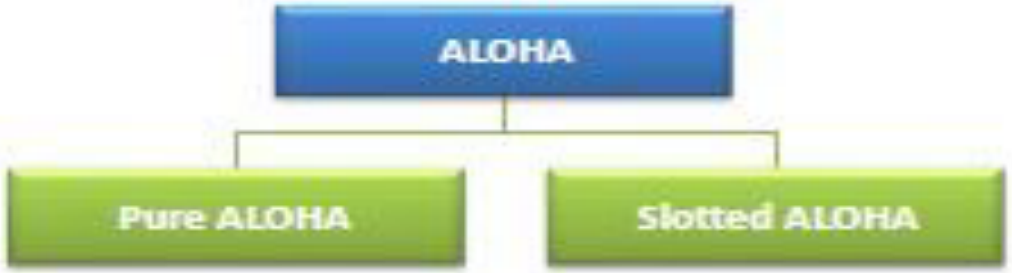
1. ALOHA
2. Carrier sense multiple access (CMSA)
3. Carrier sense multiple access with collision detection (CMSA/CD)
4. Carrier sense multiple access with collision avoidance (CMSA/CA)

# ALOHA

- ALOHA is a multiple access protocol for transmission of data via a shared network channel.
- It operates in the medium access control sub layer (MAC sub layer) of the open systems interconnection (OSI) model.
- Using this protocol, several data streams originating from multiple nodes are transferred through a multi-point transmission channel.
- In ALOHA, each node or station transmits a frame without trying to detect whether the transmission channel is idle or busy.
- If the channel is idle, then the frames will be successfully transmitted.
- If two frames attempt to occupy the channel simultaneously, collision of frames will occur and the frames will be discarded.
- These stations may choose to retransmit the corrupted frames repeatedly until successful transmission occurs.

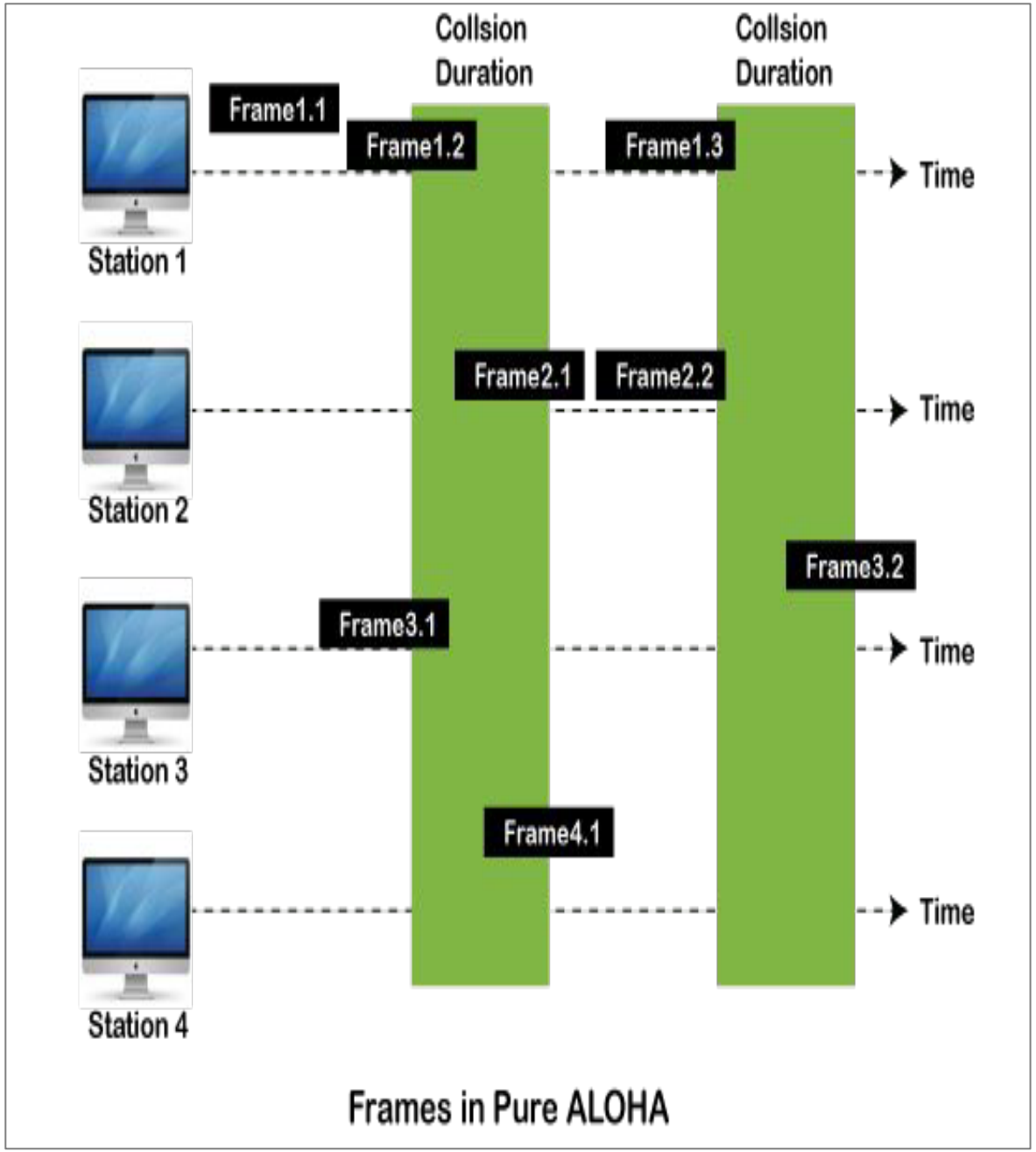
- Aloha Rules

1. Any station can transmit data to a channel at any time.
2. It does not require any carrier sensing.
3. Collision and data frames may be lost during the transmission of data through multiple stations.
4. Acknowledgment of the frames exists in Aloha. Hence, there is no collision detection.
5. It requires retransmission of data after some random amount of time.

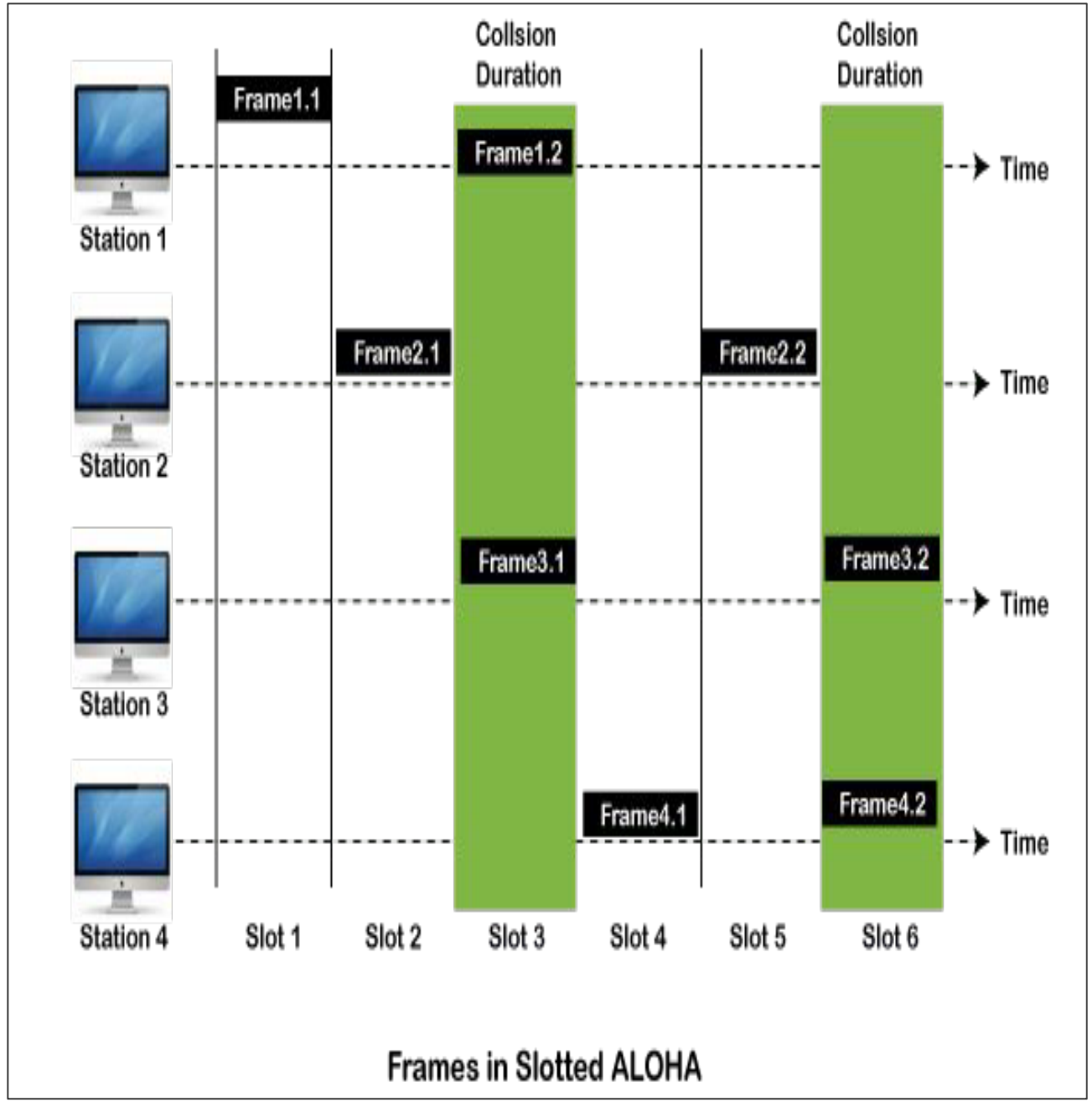



- Pure ALOHA
- In pure ALOHA, the time of transmission is continuous.
- Whenever a station has an available frame, it sends the frame. If there is collision and the frame is destroyed, the sender waits for a random amount of time before retransmitting it.

- Slotted ALOHA
- Slotted ALOHA reduces the number of collisions and doubles the capacity of pure ALOHA.
- The shared channel is divided into a number of discrete time intervals called slots.
- A station can transmit only at the beginning of each slot. However, there can still be collisions if more than one station tries to transmit at the beginning of the same time slot.




Frames in Pure ALOHA




Frames in Slotted ALOHA

# 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.

# Controlled Access Protocols

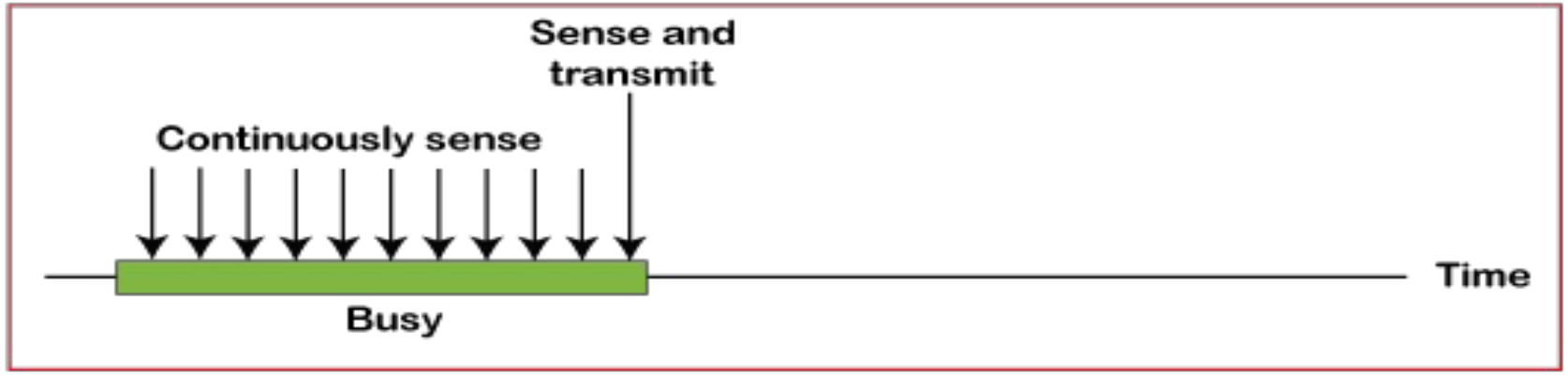
- Controlled access protocols allow only one node to send data at a given time. Before initiating transmission, a node seeks information from other nodes to determine which station has the right to send. This avoids collision of messages on the shared channel.
- The station can be assigned the right to send by the following three methods−

1. Reservation
2. Polling
3. Token Passing

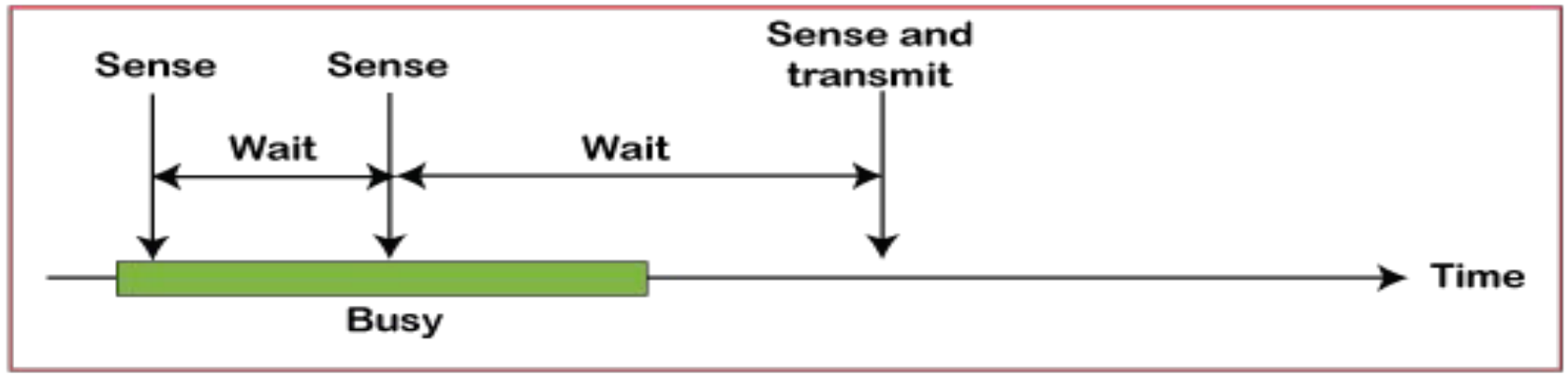
# CSMA Access Modes

- **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.

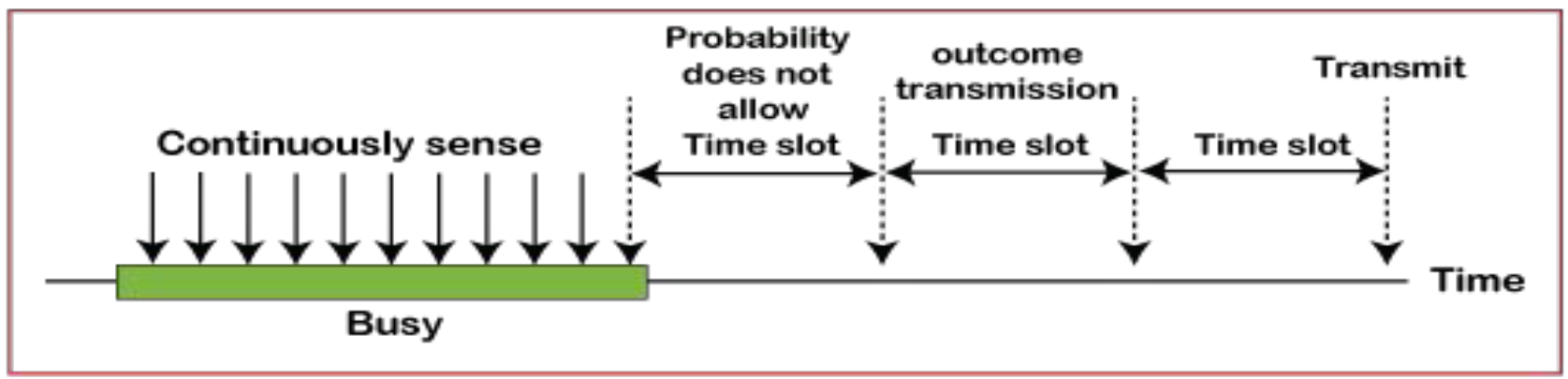
- **P-Persistent:** It is the combination of 1-Persistent and Non-persistent modes. The P-Persistent mode defines that each node senses the channel, and if the channel is inactive, it sends a frame with a **P** probability. If the data is not transmitted, it waits for a (**q = 1-p probability**) random time and resumes the frame with the next time slot.
- **O- Persistent:** It is an O-persistent method that defines the superiority of the station before the transmission of the frame on the shared channel. If it is found that the channel is inactive, each station waits for its turn to retransmit the data.




a. 1-persistent




b. Nonpersistent




c. p-persistent

# CSMA/ CD

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

# CSMA/ CA

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

| S. No | CSMA CD | CSMA CA |
|---|---|---|
| 1. | It is the type of CSMA to detect the collision on a shared channel. | It is the type of CSMA to avoid collision on a shared channel. |
| 2. | It is the collision detection protocol. | It is the collision avoidance protocol. |
| 3. | It is used in 802.3 Ethernet network cable. | It is used in the 802.11 Ethernet network. |
| 4. | It works in wired networks. | It works in wireless networks. |
| 5. | It is effective after collision detection on a network. | It is effective before collision detection on a network. |
| 6. | Whenever a data packet conflicts in a shared channel, it resends the data frame. | Whereas the CSMA CA waits until the channel is busy and does not recover after a collision. |
| 7. | It minimizes the recovery time. | It minimizes the risk of collision. |
| 8. | The efficiency of CSMA CD is high as compared to CSMA. | The efficiency of CSMA CA is similar to CSMA. |
| 9. | It is more popular than the CSMA CA protocol. | It is less popular than CSMA CD. |

# Methods used in the CSMA/ CA to avoid the collision:

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

- In telecommunications and computer networks, a channel access method or multiple access method allows several terminals connected to the same multi-point transmission medium to transmit over it and to share its capacity.
- Examples of shared physical media are wireless networks, bus networks, ring networks and half-duplex point-to-point links.
- A channel-access scheme is based on a multiplexing method, that allows several data streams or signals to share the same communication channel or physical medium.
- Multiplexing is in this context provided by the physical layer. Note that multiplexing also may be used in full-duplex point-to-point communication between nodes in a switched network, which should not be considered as multiple accesses

- A channel-access scheme is also based on a multiple access protocol and control mechanism,
- also known as media access control (MAC). This protocol deals with issues such as addressing,
- assigning multiplex channels to different users, and avoiding collisions. The MAC-layer is a sub-layer
- in Layer 2 (Data Link Layer) of the OSI model and a component of the Link Layer of the TCP/IP model.

# What is WDMA protocol?

Wavelength Division Multiplexing, WDM, is a technology that increases bandwidth by allowing different data streams at different frequencies to be sent over a single optical fiber network.

Signals at WDM wavelengths are independent from each other.

# Frequency Division Multiple Access (FDMA)

- The frequency-division multiple access (FDMA) channel-access scheme is based on the frequency-division multiplexing (FDM) scheme, which provides different frequency bands to different data-streams.
- In the FDMA case, the data streams are allocated to different nodes or devices. An example of FDMA systems were the first-generation (1G) cell-phone systems, where each phone call was assigned to a specific uplink frequency channel, and another downlink frequency channel.
- Each message signal (each phone call) is modulated on a specific carrier frequency

- A related technique is wavelength division multiple access (WDMA), based on wavelength- division multiplexing (WDM), where different data streams get different colors in fiber-optical communications.
- In the WDMA case, different network nodes in a bus or hub network get a different color.
- An advanced form of FDMA is the orthogonal frequency-division multiple access (OFDMA) scheme,
- for example used in 4G cellular communication systems. In OFDMA, each node may use several sub- carriers, making it possible to provide different quality of service (different data rates) to different users.
- The assignment of sub-carriers to users may be changed dynamically, based on the current radio channel conditions and traffic load

# Time division multiple access (TDMA)

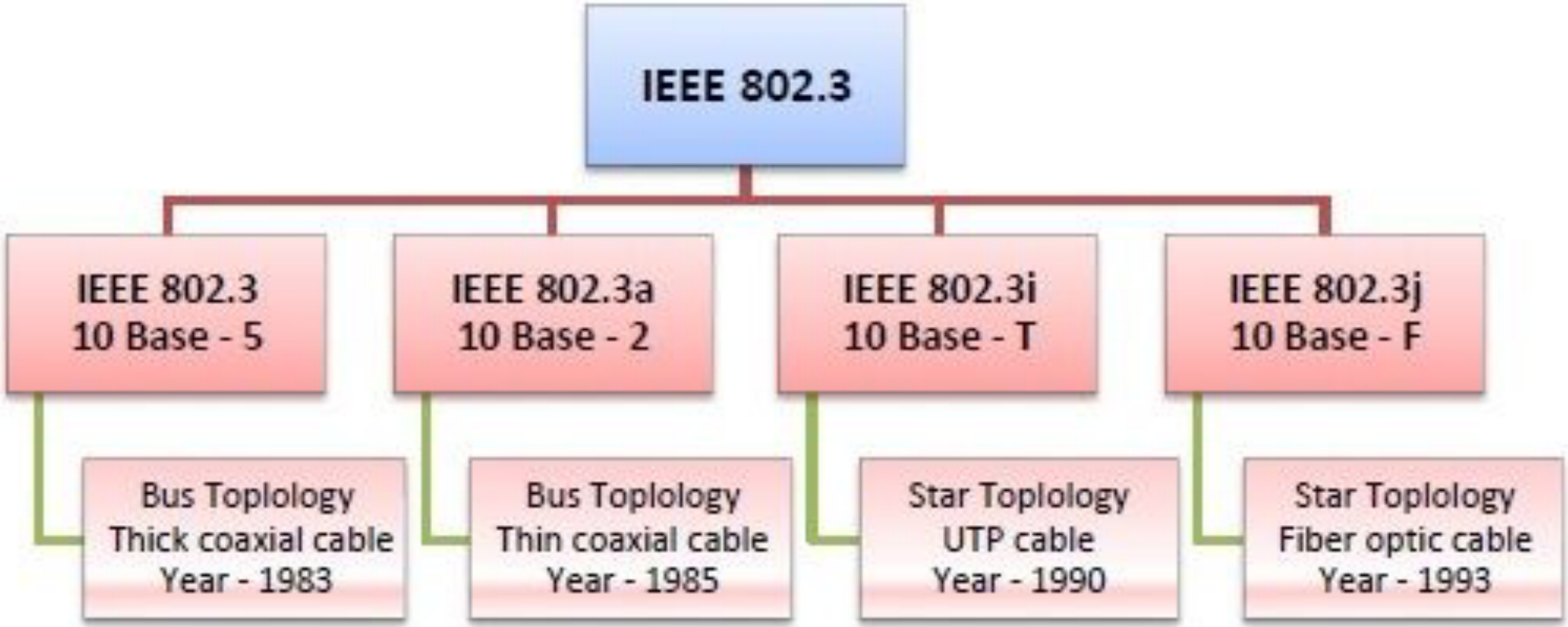
- The time division multiple access (TDMA) channel access scheme is based on the time- division multiplexing (TDM) scheme, which provides different time-slots to different data-streams (in the TDMA case to different transmitters) in a cyclically repetitive frame structure.
- For example, node 1 may use time slot 1, node 2 time slot 2, etc. until the last transmitter.
- Then it starts all over again, in a repetitive pattern, until a connection is ended and that slot becomes free or assigned to another node.
- An advanced form is Dynamic TDMA (DTDMA), where a scheduling may give different time sometimes but some times node 1 may use time slot 1 in first frame and use another time slot in next frame.
- As an example, 2G cellular systems are based on a combination of TDMA and FDMA. Each frequency channel is divided into eight timeslots, of which seven are used for seven phone calls, and one for signaling data.

# IEEE 802.3 and Ethernet

- Ethernet is a set of technologies and protocols that are used primarily in LANs. It was first standardized in 1980s by IEEE 802.3 standard.
- IEEE 802.3 defines the physical layer and the medium access control (MAC) sub-layer of the data link layer for wired Ethernet networks.
- Ethernet is classified into two categories: classic Ethernet and switched Ethernet.
- Classic Ethernet is the original form of Ethernet that provides data rates between 3 to 10 Mbps. The varieties are commonly referred as 10BASE-X. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and X is the type of medium used.
- Most varieties of classic Ethernet have become obsolete in present communication scenario.
- A switched Ethernet uses switches to connect to the stations in the LAN.
- It replaces the repeaters used in classic Ethernet and allows full bandwidth utilization.

# There are a number of versions of IEEE 802.3 protocol

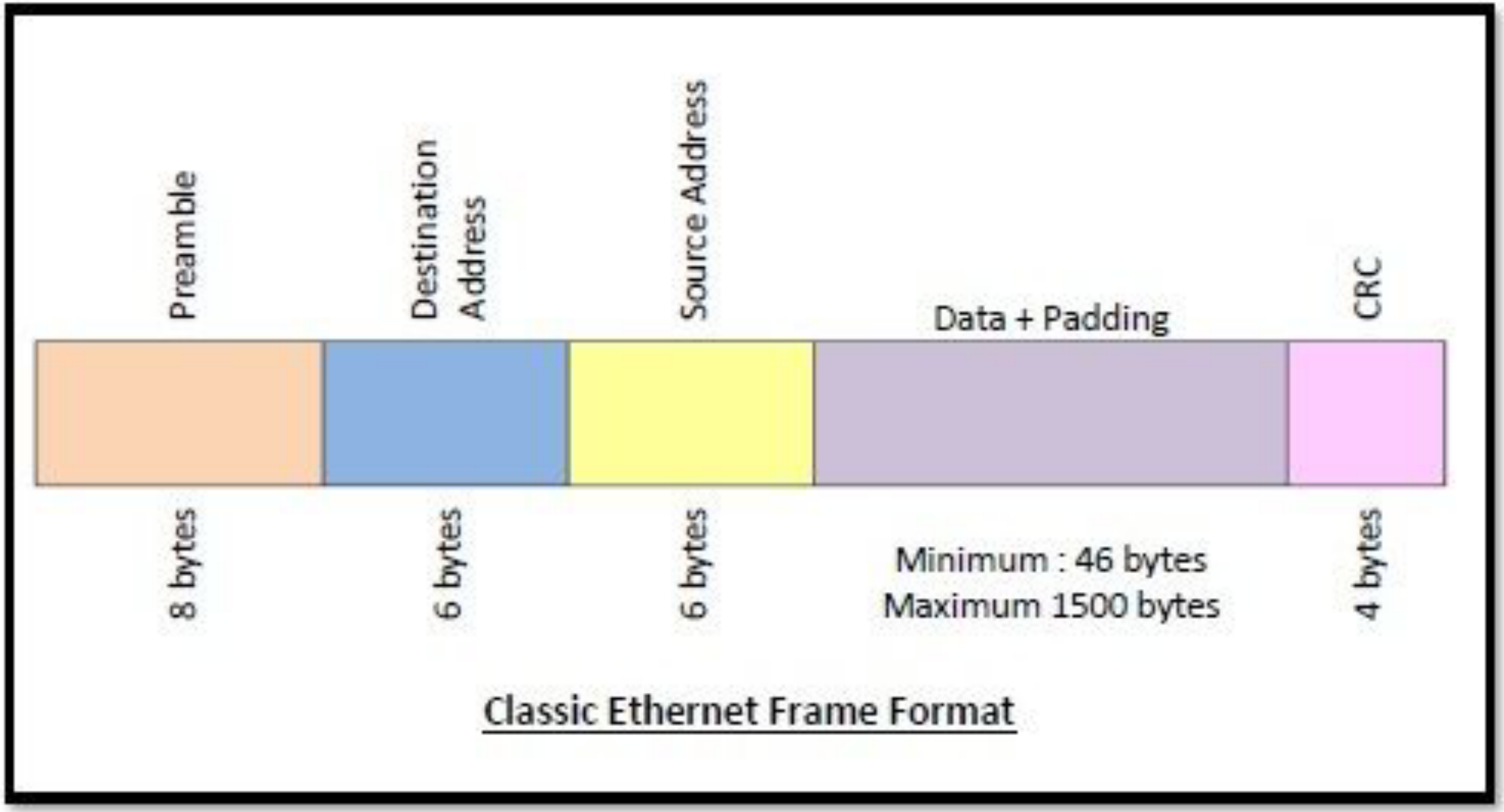
- **IEEE 802.3**: This was the original standard given for 10BASE-5. It used a thick single coaxial cable into which a connection can be tapped by drilling into the cable to the core. Here, 10 is the maximum throughput, i.e. 10 Mbps, BASE denoted use of baseband transmission, and 5 refers to the maximum segment length of 500m.
- **IEEE 802.3a**: This gave the standard for thin coax (10BASE-2), which is a thinner variety where the segments of coaxial cables are connected by BNC connectors. The 2 refers to the maximum segment length of about 200m (185m to be precise).
- **IEEE 802.3i**: This gave the standard for twisted pair (10BASE-T) that uses unshielded twisted pair (UTP) copper wires as physical layer medium. The further variations were given by IEEE 802.3u for 100BASE-TX, 100BASE-T4 and 100BASE-FX.
- **IEEE 802.3i**: This gave the standard for Ethernet over Fiber (10BASE-F) that uses fiber optic cables as medium of transmission.


IEEE 802.3
IEEE 802.3
10 Base - 5
IEEE 802.3a
10 Base - 2
IEEE 802.3i
10 Base - T
IEEE 802.3j
10 Base - F
Bus Toplology
Thick coaxial cable
Year - 1983
Bus Toplology
Thin coaxial cable
Year - 1985
Star Toplology
UTP cable
Year - 1990
Star Toplology
Fiber optic cable
Year - 1993

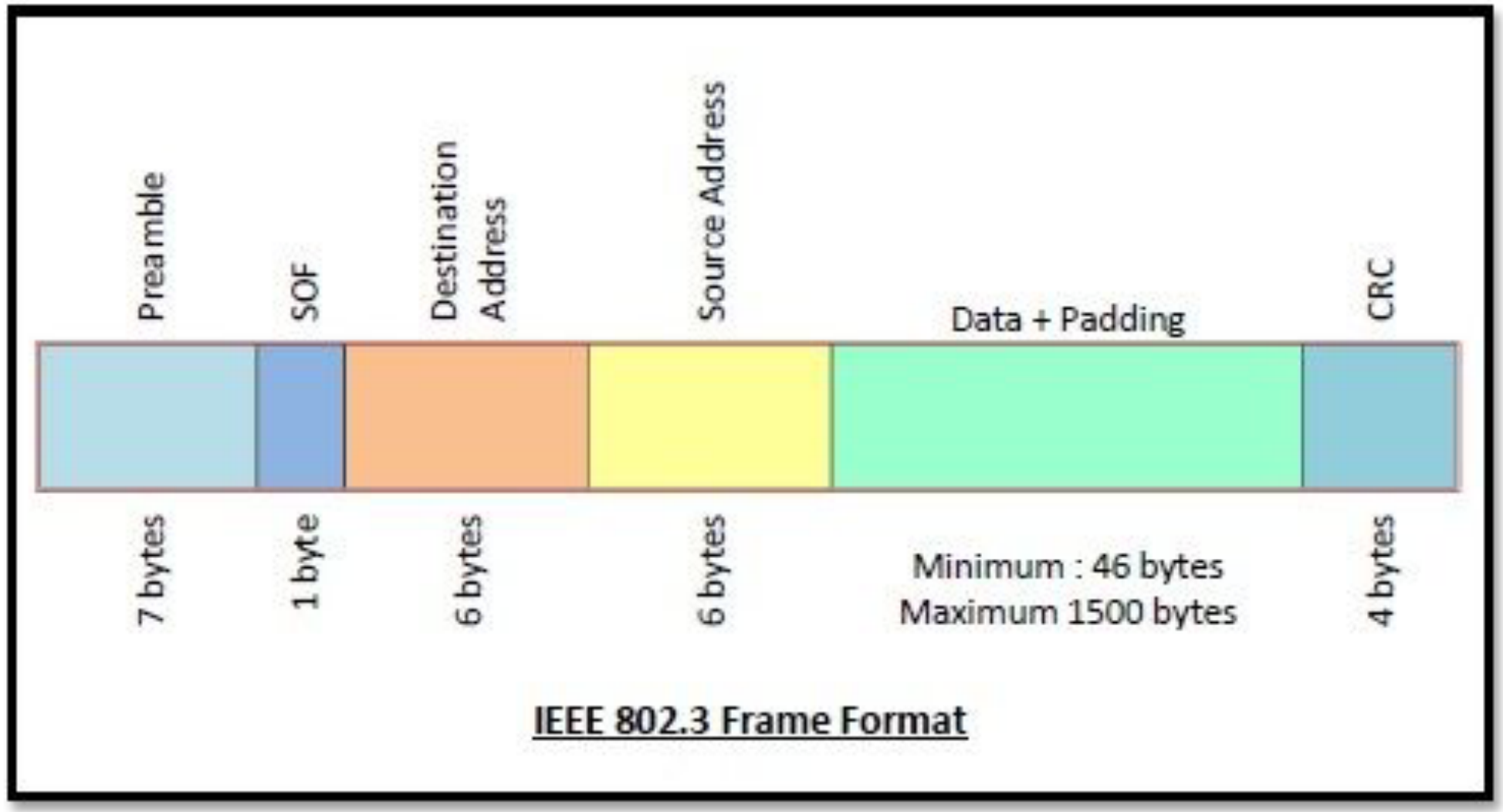
# Frame Format of Classic Ethernet and IEEE 802.3

- The main fields of a frame of classic Ethernet are -

- Preamble: It is the starting field that provides alert and timing pulse for transmission. In case of classic Ethernet it is an 8 byte field and in case of IEEE 802.3 it is of 7 bytes.
- Start of Frame Delimiter: It is a 1 byte field in a IEEE 802.3 frame that contains an alternating pattern of ones and zeros ending with two ones.
- Destination Address: It is a 6 byte field containing physical address of destination stations.
- Source Address: It is a 6 byte field containing the physical address of the sending station.
- Length: It a 7 bytes field that stores the number of bytes in the data field.
- Data: This is a variable sized field carries the data from the upper layers. The maximum size of data field is 1500 bytes.
- Padding: This is added to the data to bring its length to the minimum requirement of 46 bytes.
- CRC: CRC stands for cyclic redundancy check. It contains the error detection information.




Classic Ethernet Frame Format




**IEEE 802.3 Frame Format**

- Ethernet is a set of protocols that are used primarily in LANs, although they can also be used in larger networks like MANs and even WANs. Ethernet was first standardized in the 1980s as the IEEE 802.3 standard. Since then, it has seen several upgrades and its data carrying capacity kept increasing with each upgrade.

- Standard Ethernet can support data speeds up to 10 Mbps.

- Fast Ethernet can carry data at a maximum speed of 100 Mbps.

- With Gigabit Ethernet, the data speeds reached a maximum speed of 1 Gbps.

- 10-Gigabit-Ethernet can carry data at incredibly high speeds of 10 Gbps.

# What is Fast Ethernet?

- The IEEE 802.3u standard defines Fast Ethernet, often known as 100-Base-X or 100 Mbps Ethernet. Here, "100" is the maximum throughput, i.e. 100 Mbps, "BASE" denotes the use of baseband transmission, and "X" is the type of medium used.
- Fast Ethernet refers to a set of protocols that support and deliver data transmission speeds of 100 Mbps. The cable length was limited to 100 meters in copper-based Fast Ethernet, and multiple cable classifications were supported. Fast Ethernet in fiber mode has a range of 400 yards to up to 25 miles.
- Fast Ethernet networks were backward compatible with 10-Base-T networks in every way.

# What is Gigabit Ethernet?

- Gigabit Ethernet is a variation of the Ethernet technology that allows 1 Gbps transmission of Ethernet frames in local area networks (LANs). Many networks, particularly those of large corporations, use it as a backbone.
- Gigabit Ethernet is an upgrade to the previous 802.3 Ethernet standards of 10 Mbps and 100 Mbps. It supports 1,000 Mbps bandwidth while remaining fully compatible with the estimated 100 million Ethernet nodes now in use.
- Gigabit Ethernet typically uses an optical fiber connection to send data quickly over long distances.
- Copper cables and twisted pair connections are utilized for short distances.
- GbE or 1 GigE is the abbreviation for gigabit Ethernet. Dr. Robert Metcalf created Gigabit Ethernet, which Intel, Digital, and Xerox introduced in the early 1970s.
- It gradually grew into a wider LAN technology system for global data and information sharing. The IEEE 802.3 Committee certified the first Gigabit Ethernet standard, known as 802.3z, in 1998.
- Five physical layer standards support Gigabit Ethernet. The IEEE 802.3z standard includes 1000 BASE-SX for multimode optical fiber data transfer.
- In addition, the IEEE 802.3z standard offers 1000 BASELX transmission over single-mode fiber and 1000 BASE-CX transmission over copper cabling.

| Key | Fast Ethernet | Gigabit Ethernet |
| --- | --- | --- |
| Successor | Fast Ethernet is the successor of 10-Base-TEthernet. | Gigabit Ethernet is successor of Fast Ethernet. |
| Network speed | The maximum speed of Fast Ethernet is 100 Mbps. | Gigabit Ethernet speed can reach up to 1 Gbps. |
| Complexity | Fast Ethernet is simple to configure. | Gigabit Ethernet is quite complex to configure. |
| Delay | Fast Ethernet generates ore delay. | Gigabit Ethernet generates less delay than Fast Ethernet. |
| Coverage Limit | The maximum coverage distance for Fast Ethernet is 10 kilometers. | The maximum coverage distance for Gigabit Ethernet is 70 kilometers. |
| Round trip delay | The round trip delay in Fast Ethernet is 100 to 500 bit times. | The round trip delay in Gigabit Ethernet is 4000 bit times. |