Tutorial
ELEC3506/9506
Communication Networks

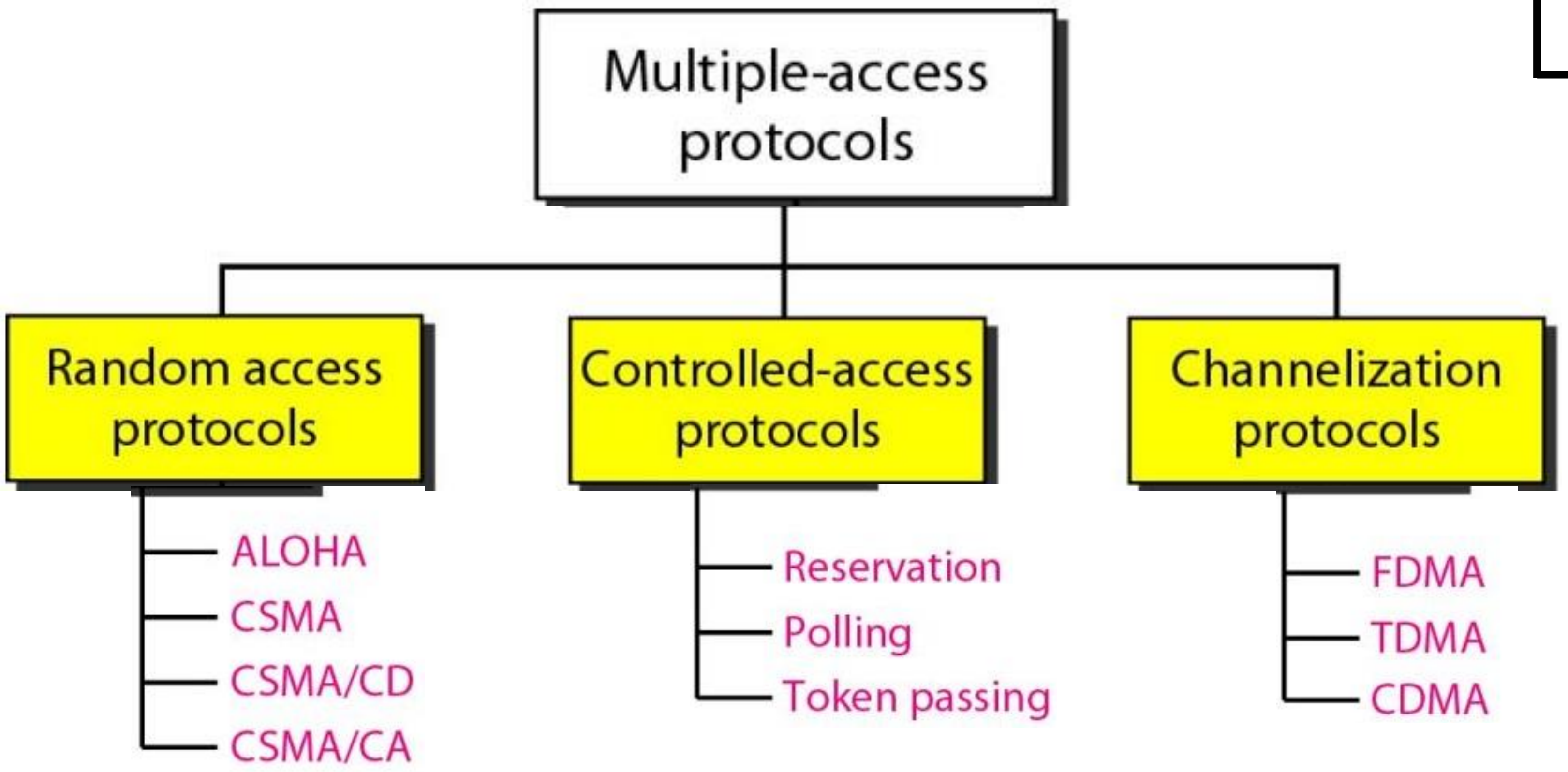
School of Electrical and Information Engineering
The University of Sydney

Dr. Shuvashis Saha
shuvashis.saha@sydney.edu.au

Tutorial 04

Multiple Access Protocols

- Data-link layer is divided into two sublayers
  - Data link control (DLC): Framing, Error & Flow control
  - Media access control (MAC): access method for LANs
    - Goal 1: Prevent any collision
    - Goal 2: Handle the collision



Q1. Define the random-access mechanism and give examples.

❑ **Random-Access**: The method, which allows the stations to access the transmission medium (channel) randomly at any time, is known as random access method.

Random-access Mechanisms

❑ **No Superiority**: No station is superior to another station, and none is assigned the control over another.

❑ **Random Access**: There is no scheduled time for a station to transmit. Transmission is random among the stations.

❑ **Contention Methods:** No rules specify which station should send next. Stations compete with one another to access the medium.

❑ **No Controlling**: Each station has the right to the medium without being controlled by any other station.

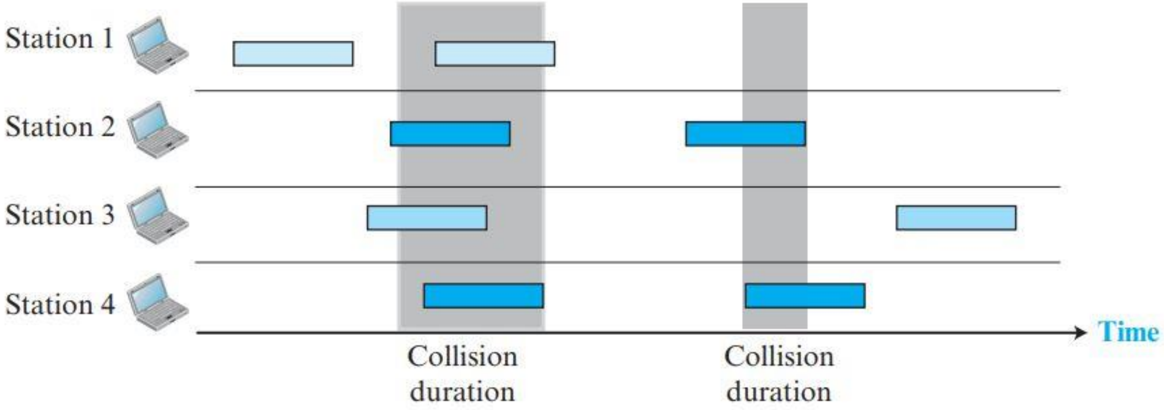
❑ **Collision**: If more than one station tries to send, there is an access conflict—collision.

Examples of Random-access Method

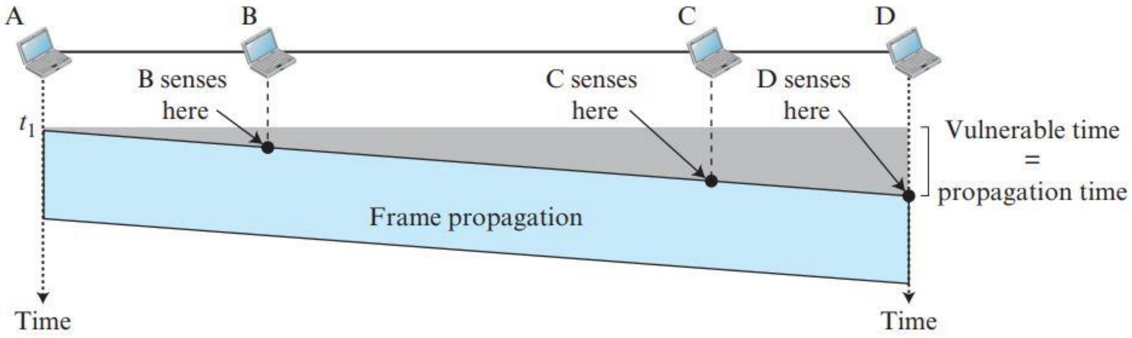
- ALOHA
- Carrier sense multiple access (CSMA)
- Carrier sense multiple access with collision detection (CSMA/CD)
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)

Example of Random-access Protocols

ALOHA



CSMA



CSMA/CD

CSMA/CA

Q2. Define controlled access mechanism and give examples

- **Controlled-Access**: In controlled access, the stations consult one another to find which station has the right to send.

Controlled-access Mechanisms

- **Consulting**: The stations consults each other to find which station has right to send.
- **Permission**: Controlled access protocols grants permission to send only one node at a time, to avoid collision of messages on the shared medium.
- **Authorization**: A station cannot send data unless it is authorized by the other stations.

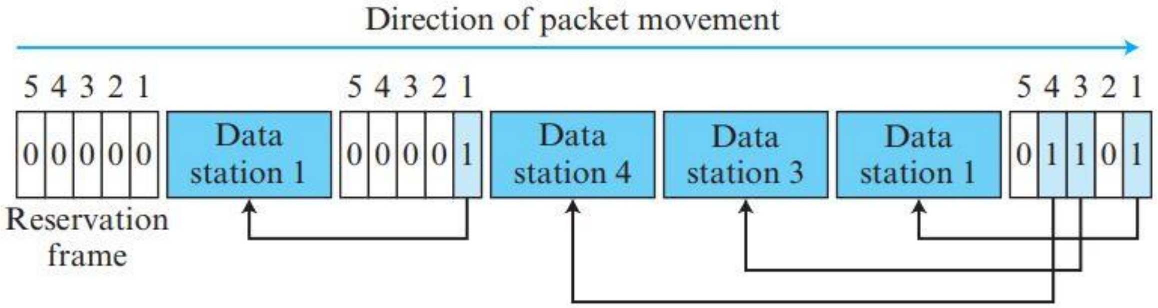
Examples of Controlled-access Method

There are three controlled access methods, namely,

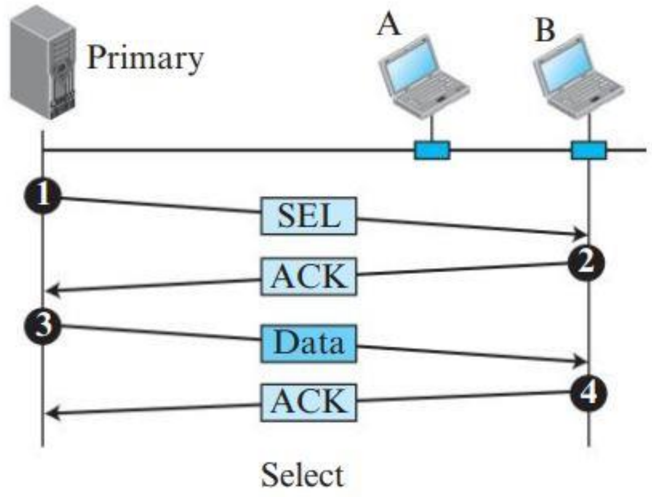
- Reservation
- Polling
- Token Passing

Example of Controlled-access Protocols

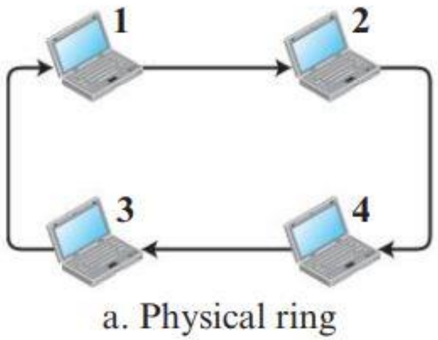
Reservation

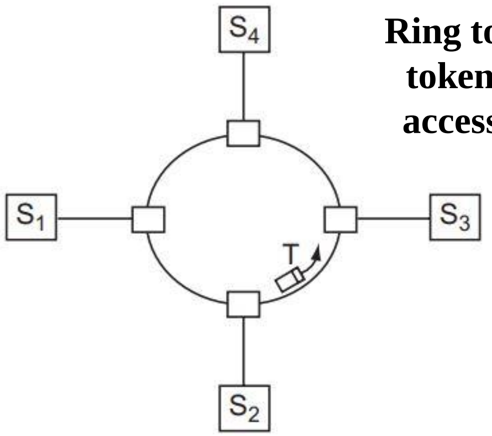


Polling



Token Passing





Ring topology in token-passing access method

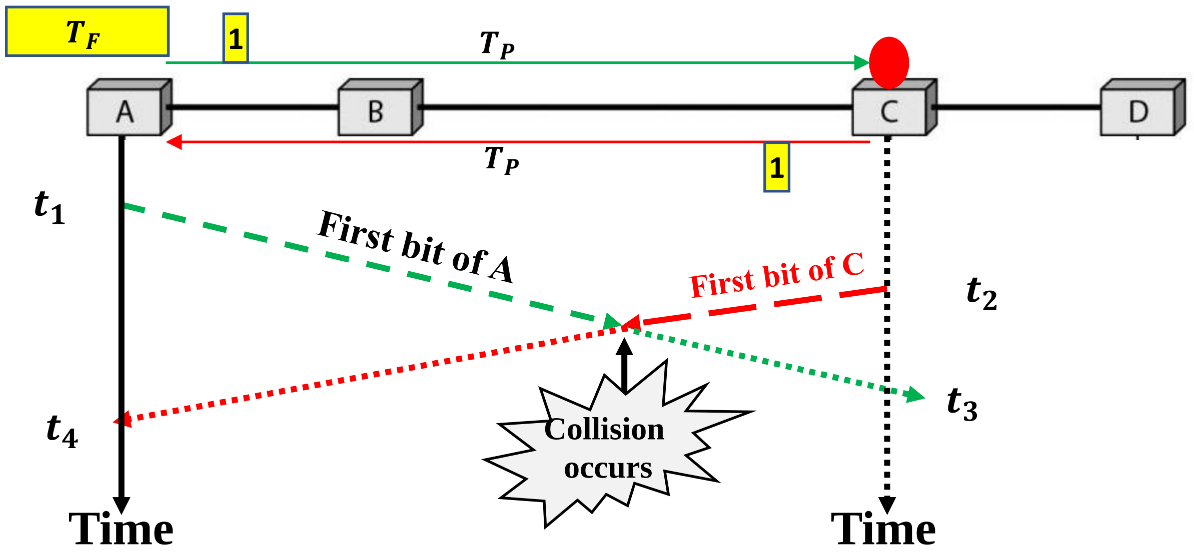
Q3. Compare and contrast a random-access protocol with a controlled access protocol. Define why collision is an issue in a random-access protocol but not in a controlled access protocol.

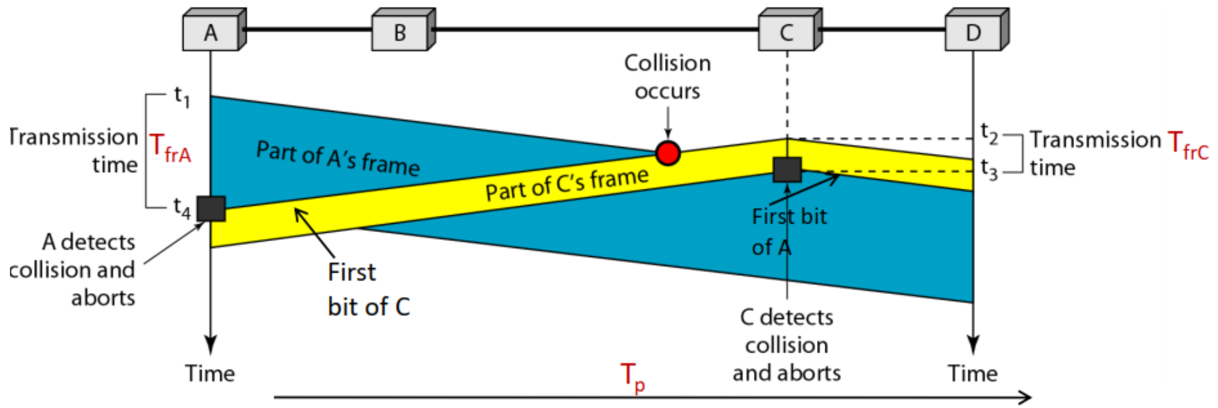
Random Access Protocol	Controlled Access Protocol
❑ There is no control; access is based on contention.	❑ Either a central authority (in polling) or other stations (in reservation and token passing) control the access.
❑ No station is superior to another station.	❑ Authorized station has the superiority.
❑ Collision common.	❑ Collison free.
❑ Examples: ALOHA, CSMA, CSMA/CD, and CSMA/CA.	❑ Examples: Reservation, Polling and Token Passing

- ❑ In a **random-access protocol**, a device assumes it can transmit if it detects no signal on the medium. If multiple independent devices decide to transmit "**at the same time**" their messages will interfere with each other or **collide**.

- ❑ In **controlled access protocol**, a device waits until it has explicit permission to transmit. Without authorization, no stations are allowed to transmit data.
- ❑ Since multiple devices cannot independently decide to transmit in a controlled access network, there can never be a collision.

Collision and Abortion in CSMA/CD





- Propagation delay (T_P) is needed time for one bit to reach to the other end of the link.

- Frame Transmission delay (T_{fr}) is the time needed to put the entire Frame on the link.

- Before sending the last bit of the frame, the sending station must detect a collision.

- If two stations involved in a collision are maximum distance apart, the signal from the first takes time T_P to reach the second, and the effect of the collision takes another T_P to return to the first.

- In case of CSMA/CD network, the frame transmission time, T_{fr} must be at least two times of the maximum propagation time, T_p to detect the collision. Therefore,

$$T_{fr} = 2 \times T_p$$

Q4. In a CSMA/CD network with a data rate of 10 Mbps, the minimum frame size is found to be 512 bits for the correct operation of the collision detection process. What should be the minimum frame size if we increase the date rate to 100 Mbps?

- Here given, data rate, $B = 10\ Mbps = 10 \times 10^6\ bps$; minimum frame size $F_{min} = 512\ bits$

- Frame transmission time, $T_{fr} = \frac{F_{min}}{B} = \frac{512\ bits}{10 \times 10^6\ bps} = 51.2 \times 10^{-6}\ sec = 51.2\ \mu s$

- In case of CSMA/CD network, the frame transmission time, T_{fr} must be at least two times of the maximum propagation time, T_p to detect the collision. Therefore,

$$T_{fr} = 2 \times T_p$$

- Maximum propagation time, T_p to detect the collision in case of CSMA/CD is:

$$T_p = \frac{T_{fr}}{2} = \frac{F_{min}}{2 \times B} = \frac{512\ bits}{2 \times 10 \times 10^6\ bps} = 25.6 \times 10^{-6}\ sec = 25.6\ \mu s$$

- If the data rate, $B = 100\ Mbps = 100 \times 10^6\ bps$; Then minimum frame size, $F_{min} = ?$.

- Minimum frame size F_{min}, to detect the collision in case of CSMA/CD is:

$$F_{min} = 2 \times B \times T_p = 2 \times 100 \times 10^6 \times 25.6 \times 10^{-6} = 5120\ bits$$

Ans: minimum frame size $F_{min} = 5120\ bits$

Q5. In a CSMA/CD network with a data rate of 10 Mbps, the maximum distance between any station pair is found to be 2500 m for the correct operation of the collision detection process. What should be the maximum distance if we increase the date rate to 100 Mbps?

- Here given, data rate, $B = 10\ Mbps = 10 \times 10^6\ bps$; maximum distance, $D_{max} = 2500\ m$.
- We know,

$$Max\ distance(m) = Max\ Propagation\ time(sec) \times Propagation\ speed(m\ /\ sec)$$

- From Q4 we have found,

$$Max\ Propagation\ time(sec) = \frac{Minimum\ frame\ size\ (bits)}{2 \times Data\ rate\ (bits/sec)}$$

$$Max\ distance(m) = \frac{Minimum\ frame\ size\ (bits)}{2 \times Data\ rate\ (bits/sec)} \times Propagation\ speed(m\ /\ sec)$$

- Here, $Propagation\ speed$ and $Minimum\ frame\ size$ will remain constant for the same system. So,

$$Max\ distance(m) \propto \frac{1}{Data\ rate\ (bits/sec)}$$

- **Maximum distance is inversely proportional to the data rate for a constant minimum frame size**
- If data rate is increased by a factor of 10, maximum distance will be decreased by a factor of 10:

Q5. In a CSMA/CD network with a data rate of 10 Mbps, the maximum distance between any station pair is found to be 2500 m for the correct operation of the collision detection process. What should be the maximum distance if we increase the date rate to 100 Mbps?

- In the given problem, when data rate is 10 Mbps, the maximum distance for the correct operation of the collision detection process will be 2500 m.

- Now, If we increase the data rate to 100 Mbps, that means 10 times.
- The maximum distance for the correct operation of the collision detection process will be decreased by 10 times.
- Therefore, the maximum distance for the date rate of 100 Mbps will be,

$$D_{max} = \frac{2500\ m}{10} = 250\ m$$

Ans: Maximum distance $D_{max} = 250\ m$

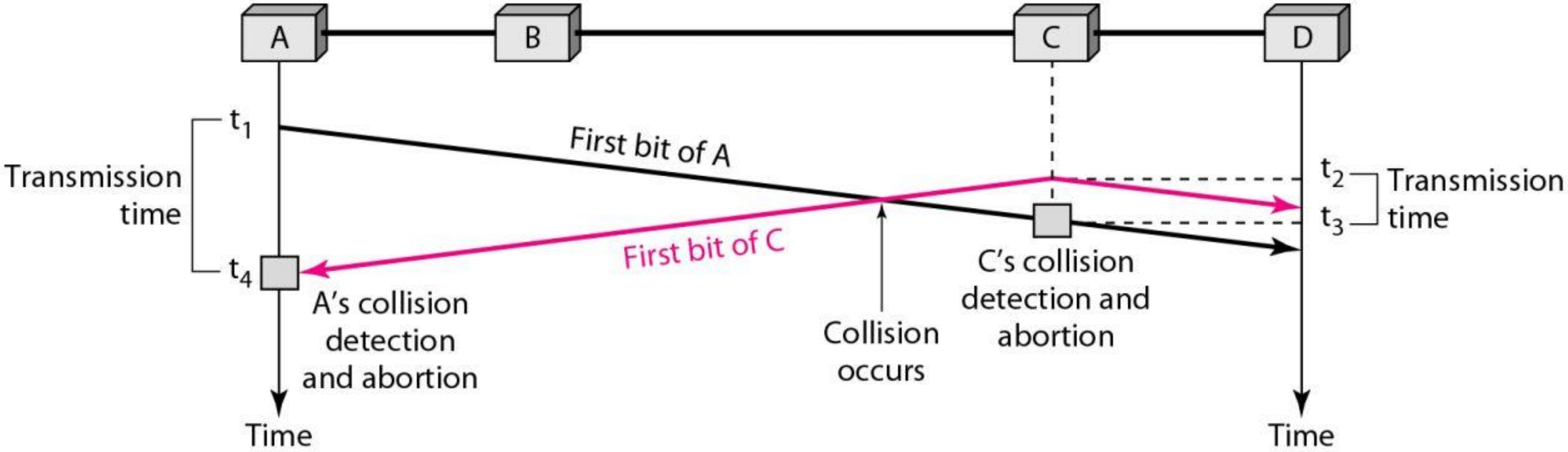
Q6. In the below figure, the data rate is 10 $Mbps$, the distance between station A and C is 2000 m, and the propagation speed is $2 \times 10^8\ m\ /\ s$. Station A starts sending a long frame at time $t_1 = 0$; station C starts sending a long frame at time $t_2 = 3\ \mu s$. The size of the frame is long enough to guarantee the detection of collision by both stations. Find:?

a) The time when station C hears the collision (t_3)

b) The time when station A hears the collision (t_4)

c) The number of bits station A has sent before detecting the collision

d) The number of bits station C has sent before detecting the collision



- Here given, data rate, $B = 10\ Mbps = 10 \times 10^6\ bps$;
- Distance between Station A to C, $L_{AC} = 2000\ m$;
- Propagation speed, $S = 2 \times 10^8\ m\ /\ s$.
- A starts sending a long frame at time, $t_1 = 0$;
- C starts sending a long frame at time, $t_2 = 3\ \mu s$;

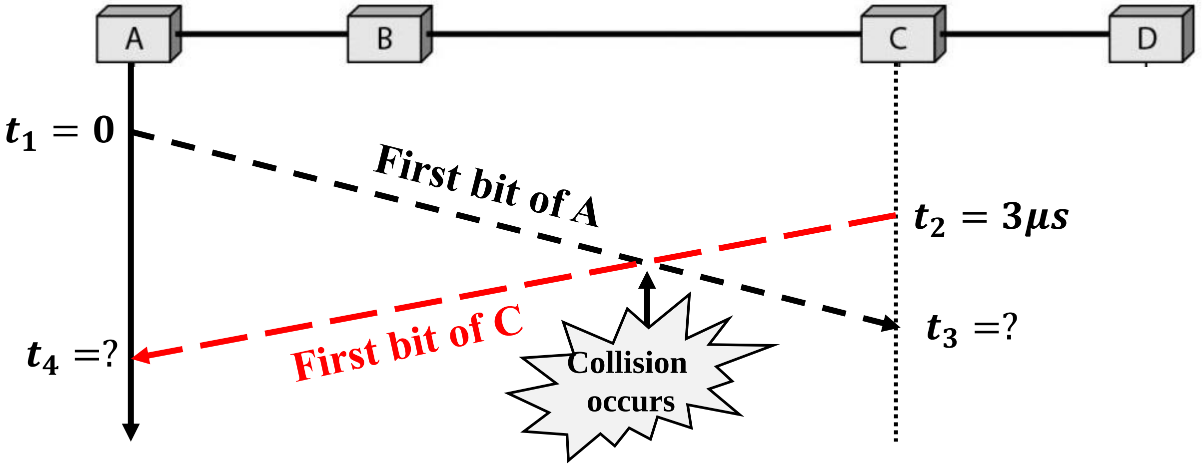
- Transmission time, $T = \frac{Distance\ (m)}{Propagation\ speed\ (m/s)}$
- Number of bits transmitted (F),

$$F = Transmission\ duration(s) \times Data\ rate(bps)$$

Q6. In the below figure, the data rate is 10 $Mbps$, the distance between station A and C is 2000 m, and the propagation speed is $2 \times 10^8\ m/s$. Station A starts sending a long frame at time $t_1 = 0$; station C starts sending a long frame at time $t_2 = 3\ \mu s$. The size of the frame is long enough to guarantee the detection of collision by both stations. Find:?

a) The time when station C hears the collision (t_3)

b) The time when station A hears the collision (t_4)



a) The time when station C hears the collision (t_3)

When the first bit of **A** reached to **C** (time, t_3), station **C** hears the collision.

- Time taken for the first bit of **A** to reach **C**, t_{AC}

$$t_{AC} = \frac{Distance\ (m)}{Propagation\ speed\ (m/s)} = \frac{2000\ m}{2 \times 10^8\ m/s}$$

$$t_{AC} = 10\ \mu s$$

- The time when station C hears the collision (t_3)

$$t_3 = t_1 + t_{AC} = (0 + 10) = 10\ \mu s$$

b) The time when station A hears the collision (t_4)

When the first bit of **C** reached to **A** (time, t_4), station **A** hears the collision.

- Time taken for the first bit of **C** to reach **A**, t_{CA}

$$t_{CA} = \frac{Distance\ (m)}{Propagation\ speed\ (m/s)} = \frac{2000\ m}{2 \times 10^8\ m/s}$$

$$t_{CA} = 10\ \mu s$$

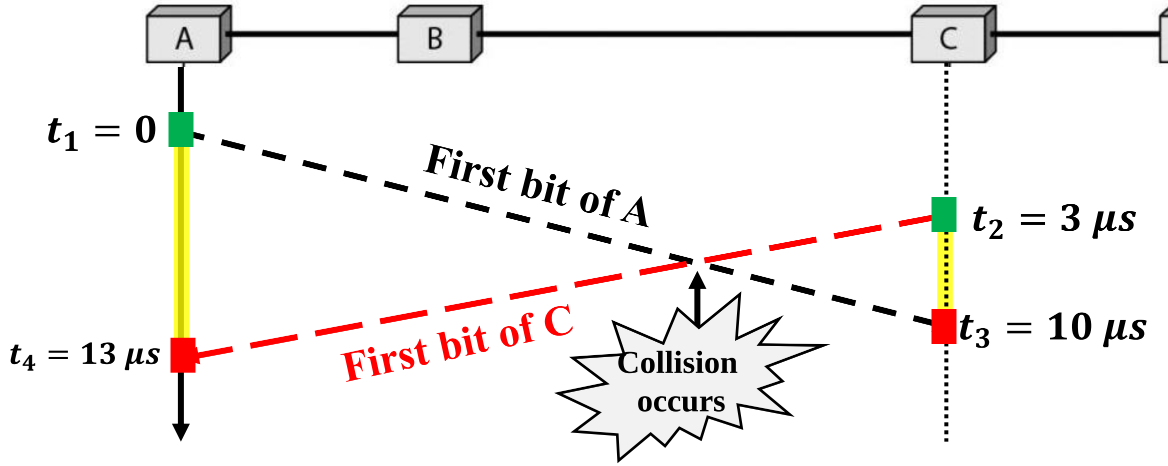
- The time when station A hears the collision (t_3)

$$t_4 = t_2 + t_{CA} = (3 + 10) = 13\ \mu s$$

Q6. In the below figure, the data rate is 10 $Mbps$, the distance between station A and C is 2000 m, and the propagation speed is $2 \times 10^8\ m/s$. Station A starts sending a long frame at time $t_1 = 0$; station C starts sending a long frame at time $t_2 = 3\ \mu s$. The size of the frame is long enough to guarantee the detection of collision by both stations. Find:?

c) The number of bits station A has sent before detecting the collision

d) The number of bits station C has sent before detecting the collision



c) Number of bits transmitted (F),

$$F = Transmission\ duration(s) \times Data\ rate(bps)$$

- The number of bits station A has sent before detecting the collision

$$F_A = (t_4 - t_1) \times B = \left((13 - 0) \times 10^{-6}\right) \times 10 \times 10^6$$

$$F_A = 130\ bits$$

- The number of bits station A has sent before detecting the collision, $F_A = 130\ bits$.

d) Number of bits transmitted (F),

$$F = Transmission\ duration(s) \times Data\ rate(bps)$$

- The number of bits station C has sent before detecting the collision

$$F_C = (t_3 - t_2) \times B$$

$$= \left((10 - 3) \times 10^{-6}\right) \times 10 \times 10^6$$

$$F_A = 70\ bits$$

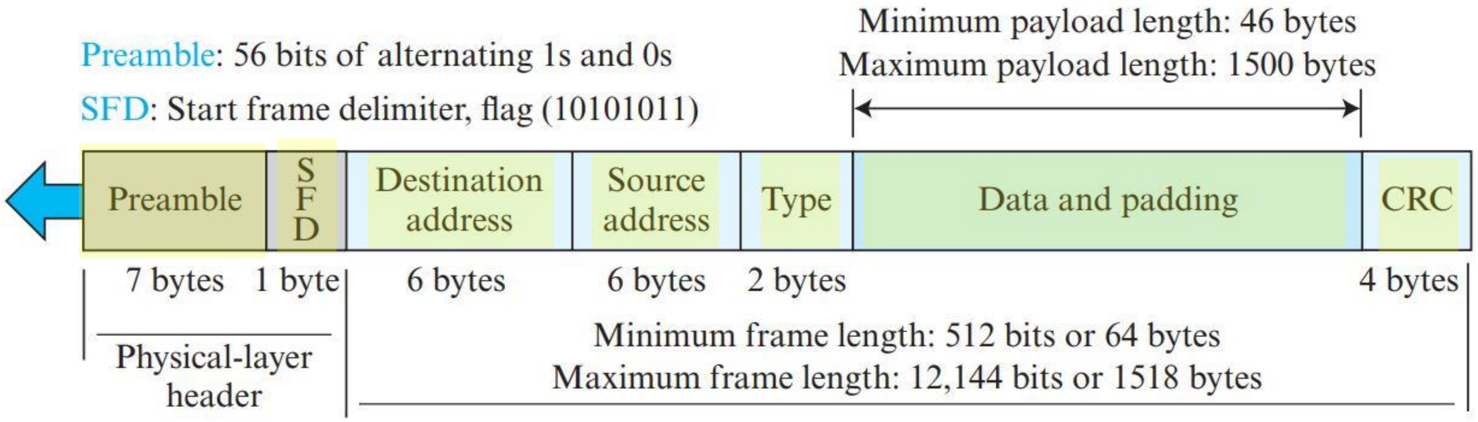
- The number of bits station C has sent before detecting the collision, $F_C = 70\ bits$.

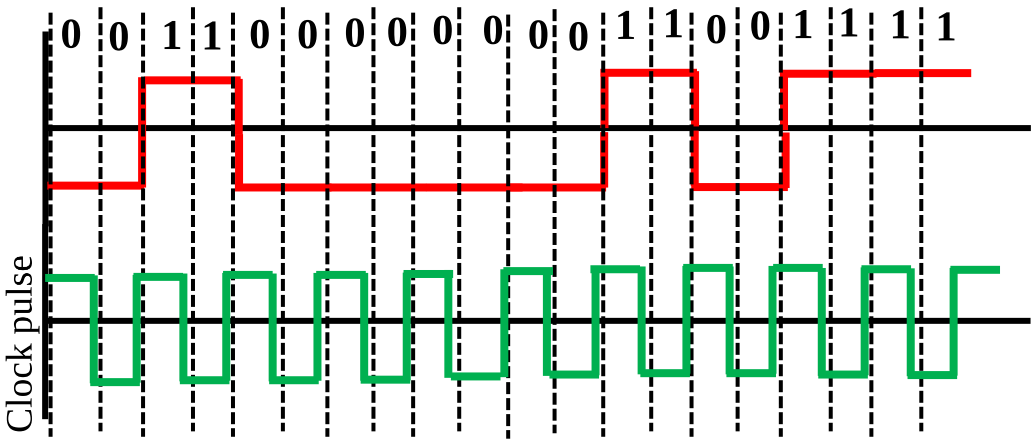
Q7. How is the preamble field of the IEEE 802.3 MAC Frame different from the SFD field?

- ❑ IEEE 802.3 has specified a type of an MAC frame for Ethernets. This frame consists of seven fields is shown in below Fig.

Preamble

- ❑ First field of the Ethernet frame.
- ❑ It contains 7 bytes of alternating 0s and 1s.
- ❑ 10101010101010101 ….
- ❑ Used for the synchronization as a pulse.



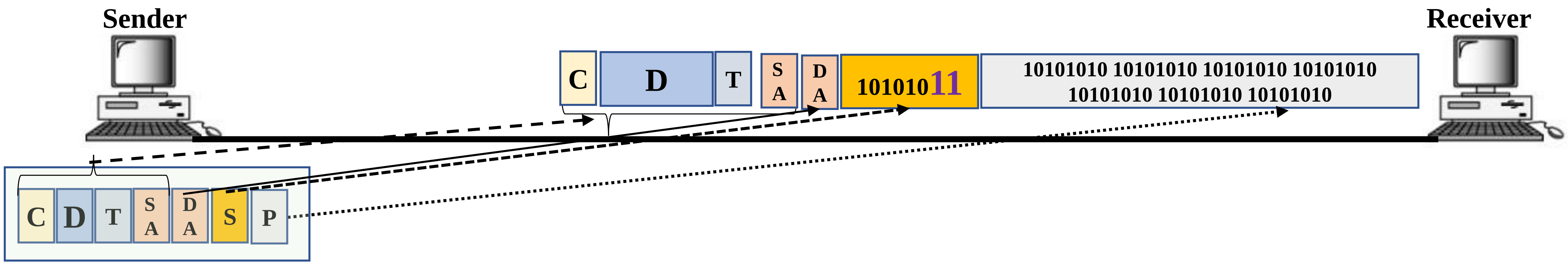


Start frame delimiter (SFD)

- ❑ It is a 1-byte long field.
- ❑ Used to determine the beginning of the frame.
- ❑ The last two bits of this field are set to 11 to indicate the receiver that the next field is destination address
- ❑ last chance for the receiver to synchronize its input timing

Q7. How is the preamble field of the IEEE 802.3 MAC Frame different from the SFD field?

❑ Differentiating between Preamble and SFD field in IEEE 802.3 MAC Frame.



Preamble

- ❑ In frame, first 7 bytes that means 56 bits of alternating 0s and 1s represent the Preamble filed, which is mainly used for the **Synchronization**.

Start frame delimiter (SFD)

- ❑ After counting 56 bits by the Receiver, next 1 byte that means 8 bits (10101011) represent the SFD field. **This is a signal of the beginning of the frame.**
- ❑ The SFD warns the station or stations that this is the last chance for synchronization (101010)
- ❑ The last 2 bits are $(11)_2$ and alert the receiver that the next field is the **Destination Address**.

- ❑ **Rest of the Field:** After receiving $(11)_2$ from the **SFD** field, receiver or intermediate node collects the necessary information from the Frame (DA, SA, Type, Data, CRC).

Q8. What are the advantages of dividing an Ethernet LAN with a bridge?

Bridges have two effects on an Ethernet LAN

1) They raise the bandwidth
2) They separate collision domains

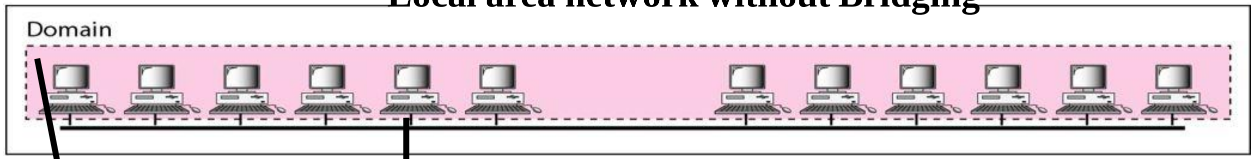
Raising the Bandwidth

- In case of no Bridge, LAN of N devices and 10 $Mbps$ data rate, then total bandwidth is shared among all stations $\frac{10}{N}$ $Mbps$.
- However, A bridge divides the network into two or more networks.
- Bandwidth-wise, each network is independent.

Separating Collision Domains

- With bridging, the collision domain becomes much smaller, and the probability of collision is reduced tremendously.
- From Figure, Without bridging, 12 stations contend for access to the medium.
- With bridging only 3 stations contend for access to the medium.

Local area network without Bridging



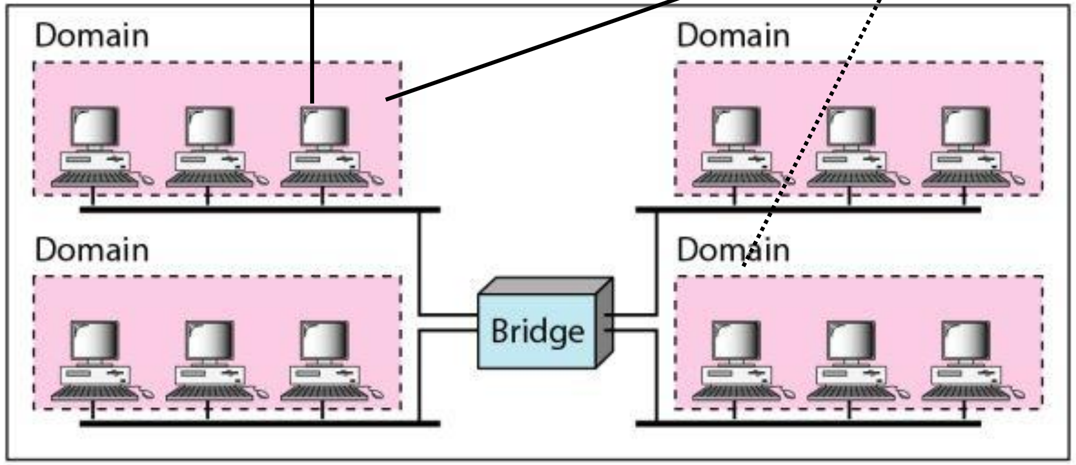
$BW_D = 10\ Mbps$

$BW = \frac{10}{12}\ Mbps$

- **Which is almost 4 times more than an unbridged network**

BW *lower than individual bandwidth*

$BW_D = 10\ Mbps$

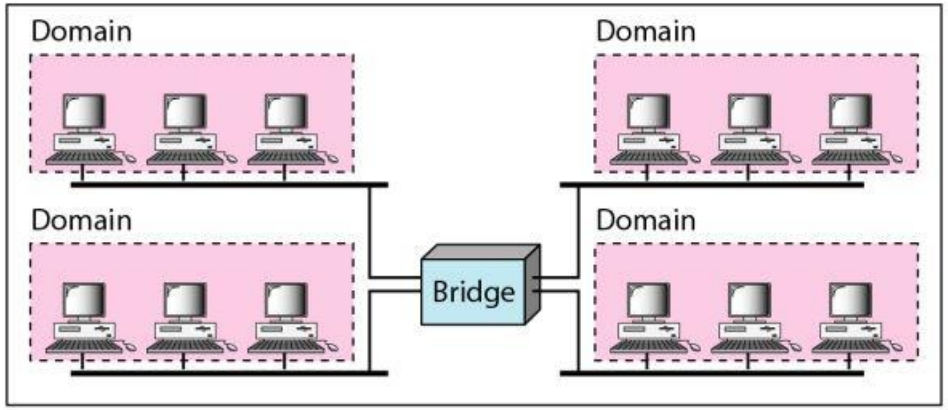


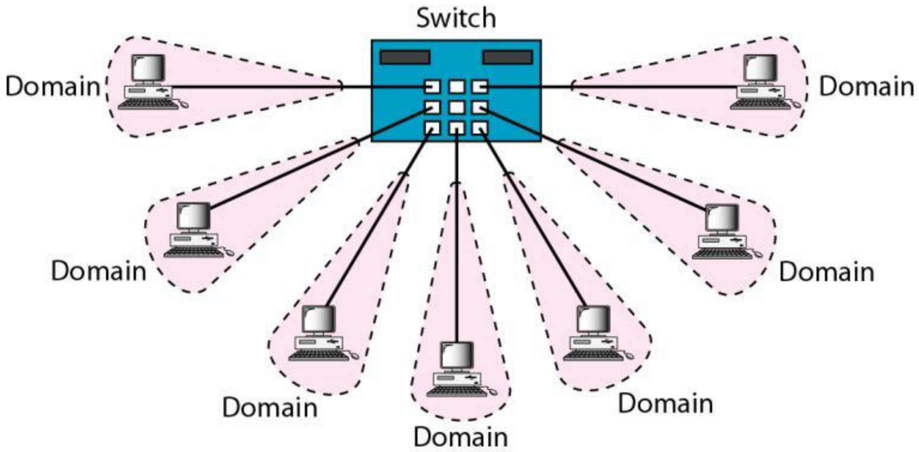
Local area network with Bridge

Q9. What is the relationship between a switch and a bridge?

Relationship between a switch and a bridge

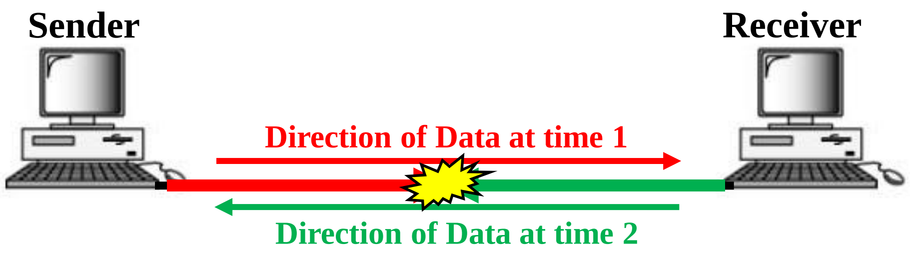
- A **two-layer switch** is a **bridge with many ports** and a design that allows **better (faster)** performance.
- Main reasons of using Bridge and switch (Layer-2) are to increase bandwidth and reduce collision domain.
- Both operate in physical and data link layers.
- Both make filtering decisions based on the physical address of the frame they receive.
- Both Bridge and Switch have forwarding table of MAC address and port number.
- Two-layer Switch uses store and forward, cut-through, or fragment-free method to forward frame, while Bridge uses only store and forward method.





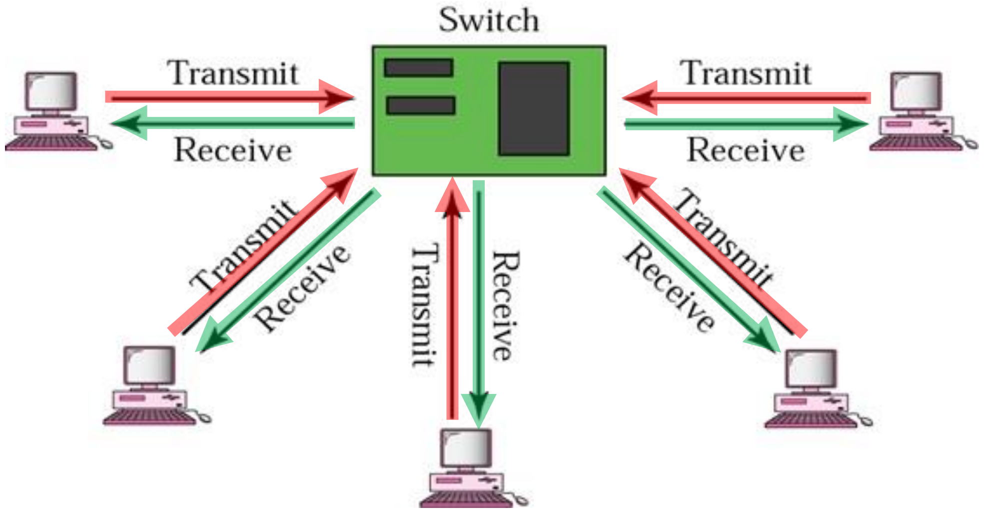
Q10. Why is there no need for CSMA/CD on a full-duplex LAN?

- One of the limitations of 10Base5 and 10Base2 is that communication is half-duplex.
- There is need for the **CSMA/CD** method to avoid collision.



Full-duplex LAN with Switch

- In a fullduplex switched Ethernet, each station is connected to the switch via two separate links (Tx & Rx).
- Each station or switch can send and receive independently without worrying about collision.
- There is no longer a need for carrier sensing as there is no longer a need for collision detection.

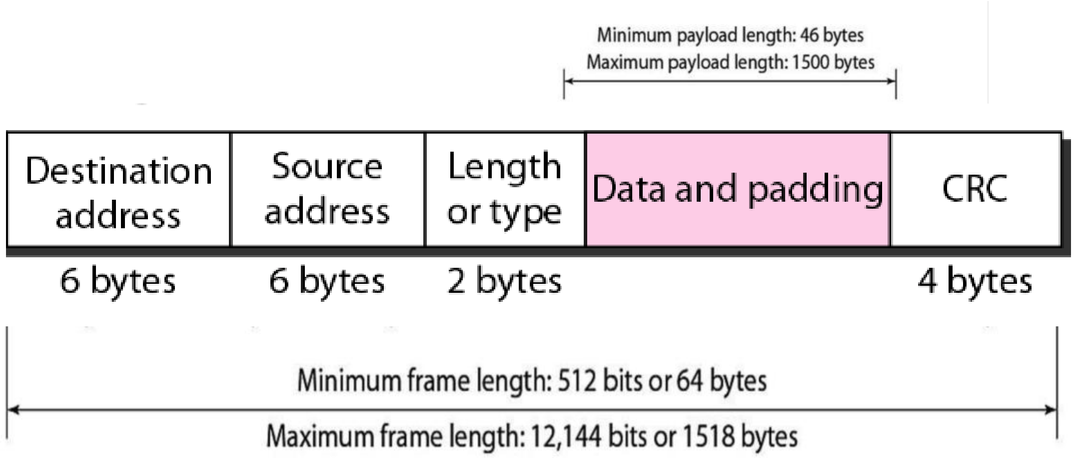


Each link is a point-to-point dedicated path between the station and the switch.

Q11. An Ethernet MAC layer receives 42 bytes of data from the upper layer. How many bytes of padding must be added to the data?

- The minimum frame length in Ethernet is 64 bytes and the maximum is 1518 bytes
  - 6 bytes for the Destination address
  - 6 bytes for the Source address
  - 2 bytes for length/ethernet type
  - 46 – 1500 bytes for data
  - 4 bytes of CRC

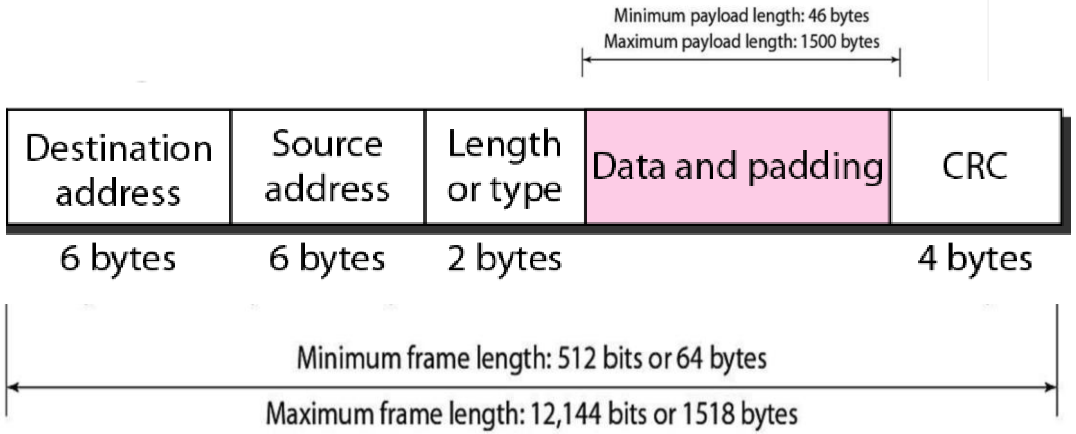
- We need to append 4 bytes of padding data (zeros) to the data (46-42 =4)



Q12. An Ethernet MAC layer receives 1510 bytes of data from the upper layer. Can the data be encapsulated in one frame? If not, how many frames need to be sent? What is the size of data in each frame?

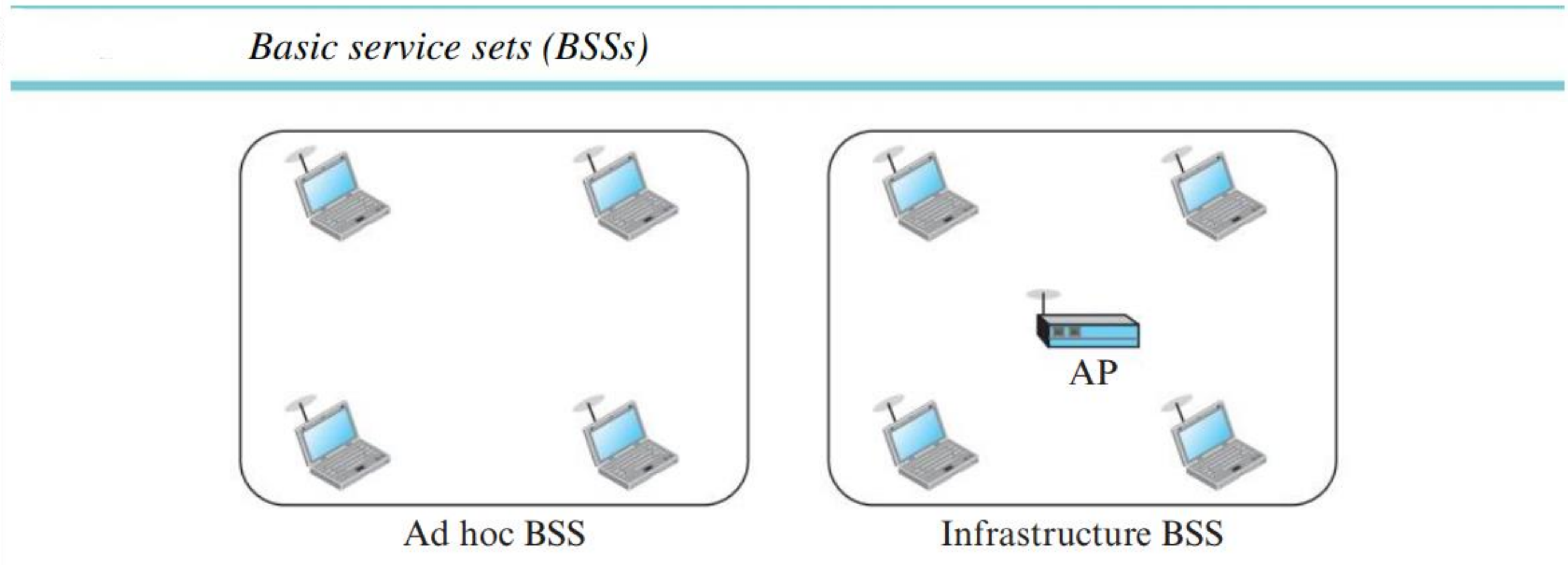
- The **maximum** data size in the Standard Ethernet is 1500 bytes. The data of 1510 bytes, therefore, must be split between two frames:
  - Data size for the first frame: 1500 bytes
  - Data size for the second frame: 46 bytes (with padding)

- The standard dictates that the first frame must carry the maximum possible number of bytes (1500); the second frame then needs to carry only 10 bytes of data.
- Therefore, it is not possible to split the 1510 bytes into two frames of data size 755 bytes.



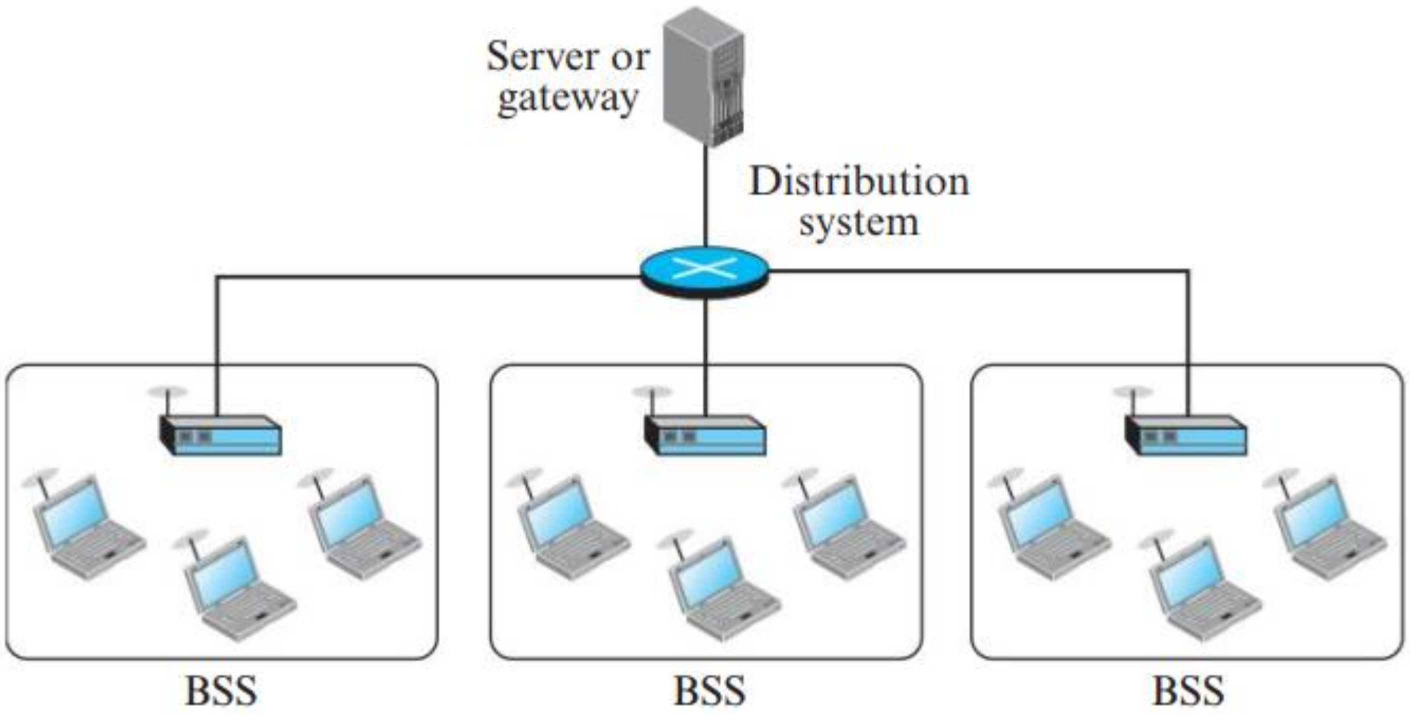
Q13. What is the difference between a BSS and an ESS?

- The basic service set (BSS) is the building block of a wireless LAN.
  - A BSS without an AP is called an ad hoc architecture.
  - A BSS with an AP is sometimes referred to as an infrastructure network.



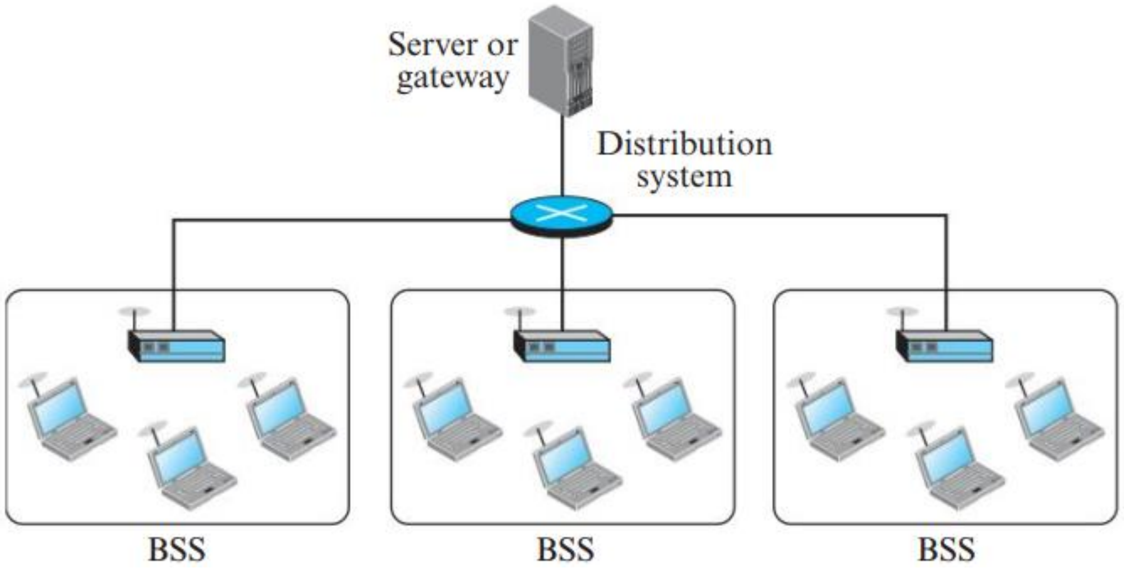
Q13. What is the difference between a BSS and an ESS?

- An extended service set (ESS) is made up of two or more BSSs with APs. In this case, the BSSs are connected through a distributed system, which is usually a wired LAN.



Q14. Discuss the three types of mobility in a WLAN?

- There are three types of stations based on their mobility in a wireless LAN:
  - No-transition mobility
  - BSS-transition mobility
  - ESS-transition mobility



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

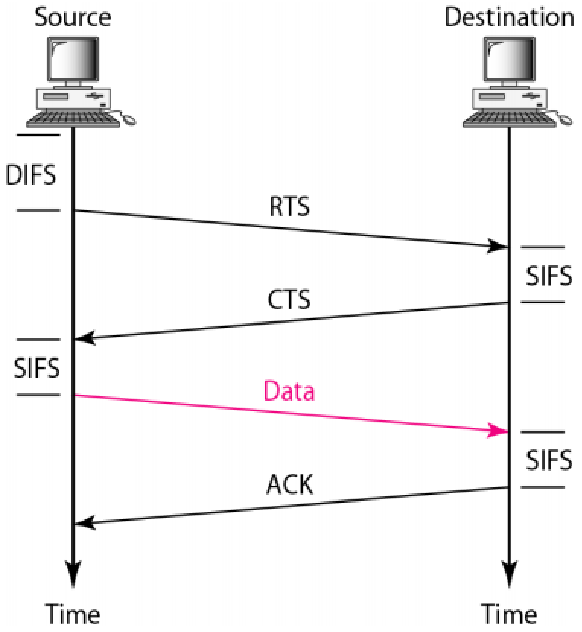
Q15. What is the access method used by WLANs?

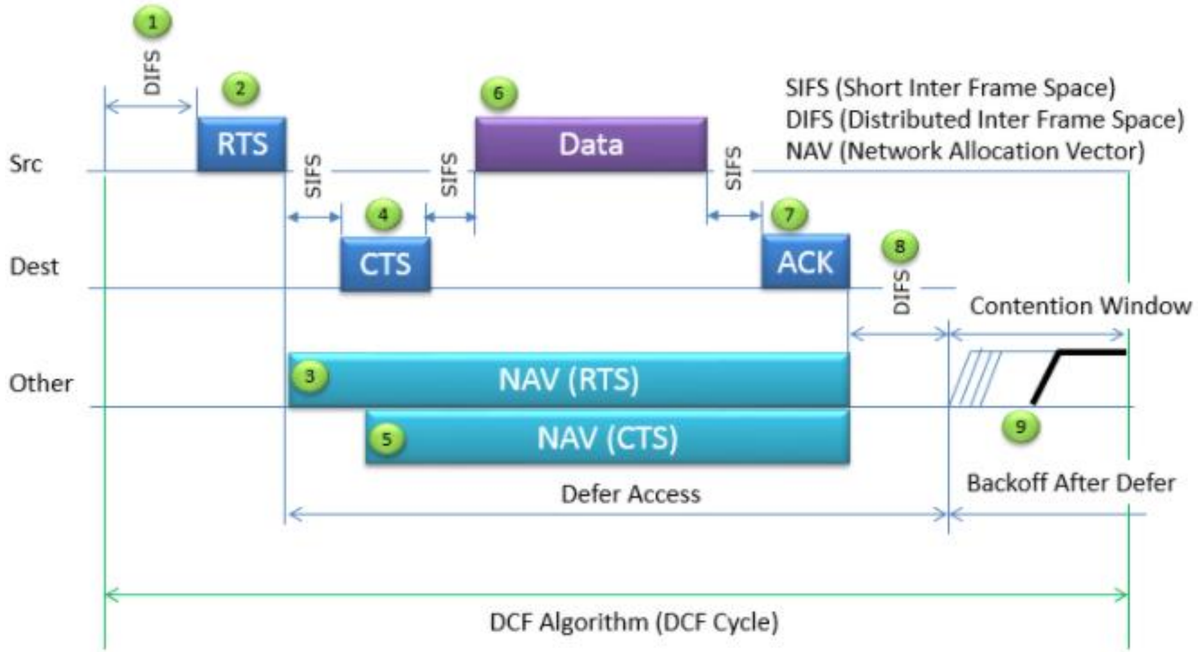
- Two protocols are defined by IEEE at the MAC sublayer: distributed coordination function (DCF) and point coordination function (PCF).
- DCF uses CSMA/CA as the access method

- Wireless LANs cannot implement CSMA/CD for following reasons:
  - In a wireless network, collisions do not add enough energy for stations to effectively detect them.
  - High costs and increased bandwidth requirements.
  - Collision may not be detected because of the hidden station problem.
  - Signal fading could prevent a station at one end from hearing a collision at the other end.

Q15. What is the access method used by WLANs?

- The CSMA/CA method used in DCF works as follows:





- After finding an idle channel, the source waits for Distributed Inter Frame Space (DIFS).
- The source then sends a Request to Send (RTS) control frame to the destination.
- The destination, after receiving RTS, waits for Short Inter Frame Space (SIFS) and sends a Clear to Send (CTS) control frame to the source.
- The source waits for SIFS before sending the data.
- The destination waits another SIFS before sending an Acknowledgement (ACK).
- Collision Avoidance (CA) uses persistent methods, randomly selects a Contention Window (CW), and decrements it.
- CSMA/CA waits for ACK before sending additional frames.
- DIFS, SIFS, and a time slot are 50 μs, 20 μs, and 10 μs, respectively.

Q15. What is the access method used by WLANs?

PCF

- PCF is an optional access method that can be implemented in an infrastructure network (not in ad hoc network)

- PCF has a centralized, contention-free polling access method. The AP performs polling for stations that are capable of being polled. The stations are polled one after another, sending any data they have to the AP.

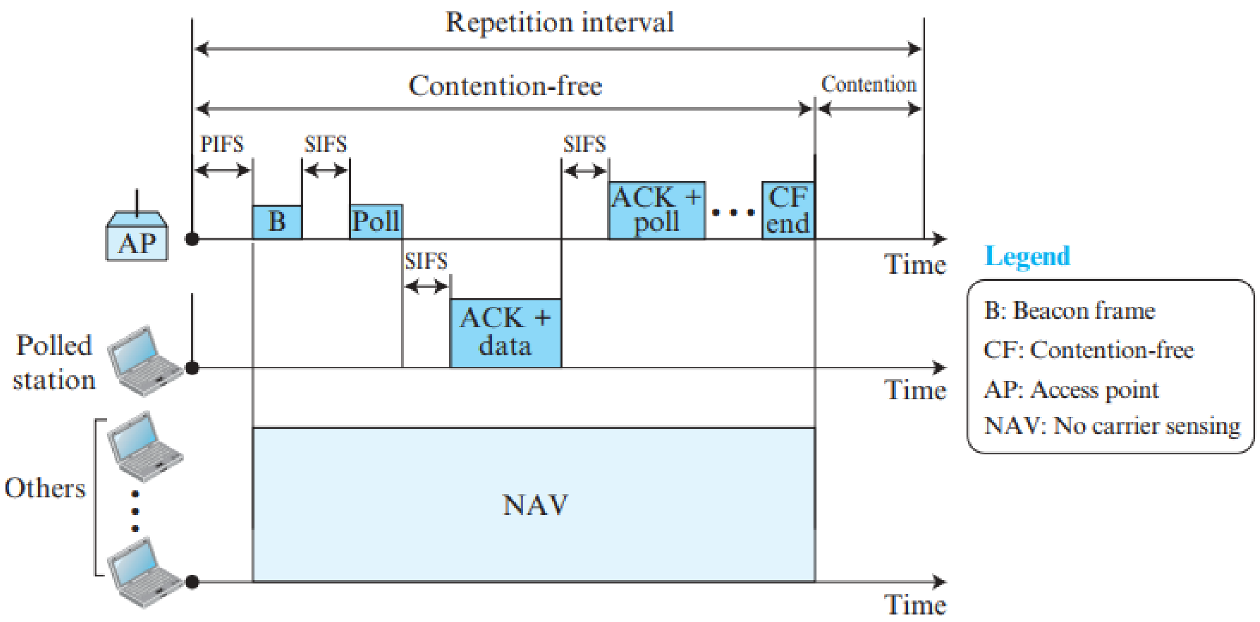
- To give priority to PCF over DCF, another set of interframe spaces has been defined: PIFS (point Interframe Space) (where, SIFS<PIFS<DIFS)

Q15. What is the access method used by WLANs?

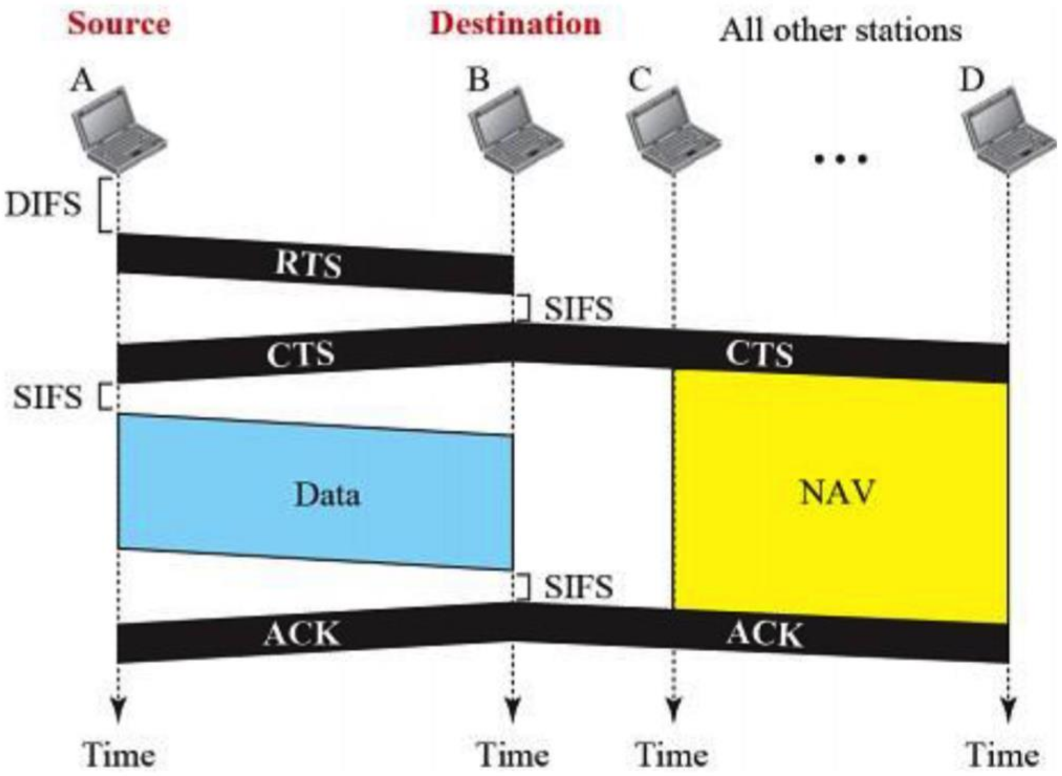
- Due to the priority of PCF over DCF, stations that only use DCF may not gain access to the medium

- To prevent this, a beacon frame that is periodically transmitted is used to cover both contention-free (PCF) and contention-based (DCF) traffic

- When the stations hear the beacon, they start their network allocation vector (NAV) for the duration of the contention-free period.



Q16. What is the purpose of the NAV?



Network Allocation Vector (NAV):

- The stations listening on the wireless medium read the Duration field and set their NAV, which is an indicator for a station on how long it must defer from accessing the medium (like a timer that counts down to zero)

- To prevent stations from accessing medium and causing contention.

Q17. Compare and contrast CSMA/CD with CSMA/CA?

CSMA/CD
- ❑ Used in: Wired networks (e.g., Ethernet).
- ❑ Function: Detects collisions after they occur.
- ❑ Collision Handling: Stops transmission and retries after a random backoff time.
- ❑ Efficiency: Good in low traffic, but performance degrades with high traffic.

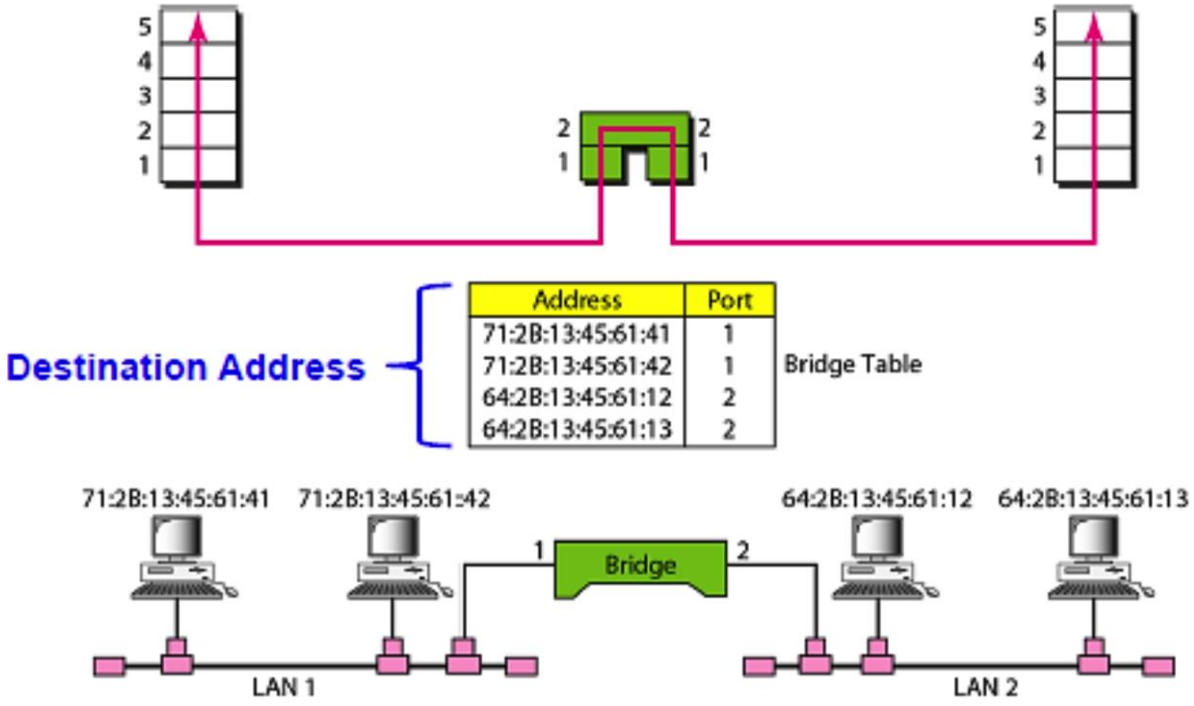
CSMA/CA
- ❑ Used in: Wireless networks (e.g., Wi-Fi).
- ❑ Function: Avoids collisions before they occur.
- ❑ Collision Handling: Uses backoff timers and waits for a clear channel before transmitting.
- ❑ Efficiency: Essential for wireless communication, but overhead can reduce throughput.

- ❑ In CSMA/CD, the protocol allows collisions to happen. If there is a collision, it will be detected, transmission is terminated and the frame will be resent. CSMA/CA uses RTS/CTS mechanism to prevent collision.
- ❑ CSMA/CD cannot be used in a wireless medium because
  - ❑ Wireless collisions do not add enough energy for effective detection.
  - ❑ Collision may not be detected because of hidden node problem
  - ❑ Distance between stations may be great and signal fading could prevent a station at one end from hearing a collision at the other end.
- ❑ Therefore, we need to avoid collisions on wireless networks because they cannot be detected. Therefore we use CSMA/CA.

Q18. What do we mean when we say that a bridge can filter traffic? Why is filtering important?

- Bridges have access to station physical addresses and can forward a packet to the appropriate segment of the network. In this way, they filter traffic.

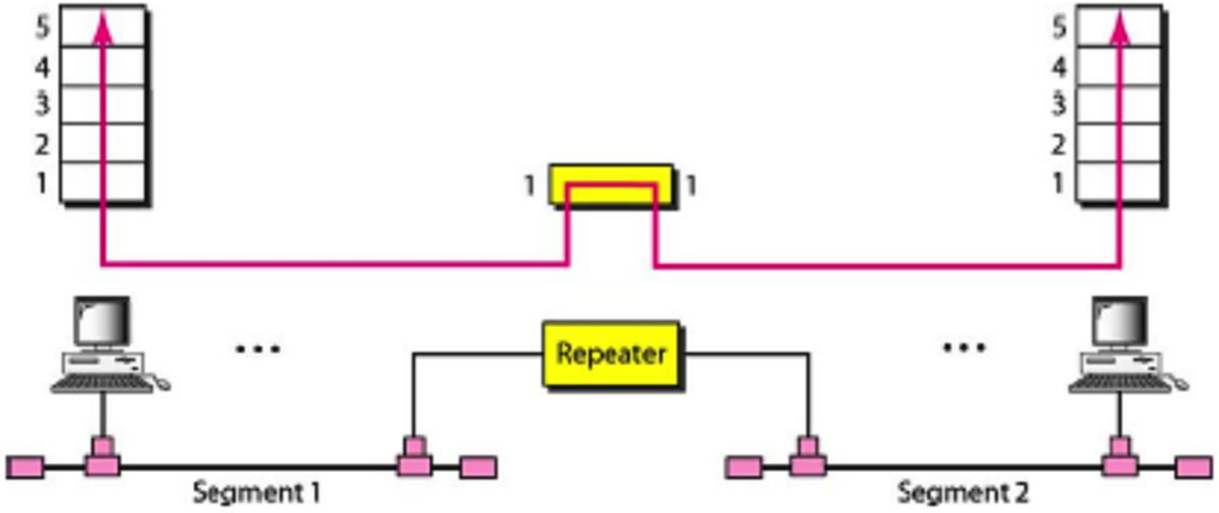
- Filtering helps in controlling the congestion because it prevents a frame from reaching network segments where it is not needed. Filtering also improves security by restricting which ports receive traffic.



Q19. How does a repeater extend the length of a LAN?

- 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. A repeater thus can extend the physical length of a LAN.



Q20. How does a VLAN reduce network traffic?

- VLANs can form multiple broadcast domains (workgroups) by breaking up a large network into smaller independent segments.

- Each workgroup member can send broadcast messages to others in the workgroup. This eliminates the need for broadcasting the message to all other stations and all the overhead messages associated with it. Thus, it reduces the traffic in the network.