Multiple Access Protocols in Computer Network

Last Updated : 28 Jun, 2024

Multiple Access Protocols are methods used in computer networks to control how data is transmitted when multiple devices are trying to communicate over the same network. These protocols ensure that data packets are sent and received efficiently, without collisions or interference. They help manage the network traffic so that all devices can share the communication channel smoothly and effectively.

Who is Responsible for the Transmission of Data?

The **Data Link Layer** is responsible for the transmission of data between two nodes. Its main functions are:

- Data Link Control
- Multiple Access Control

Data Link Control

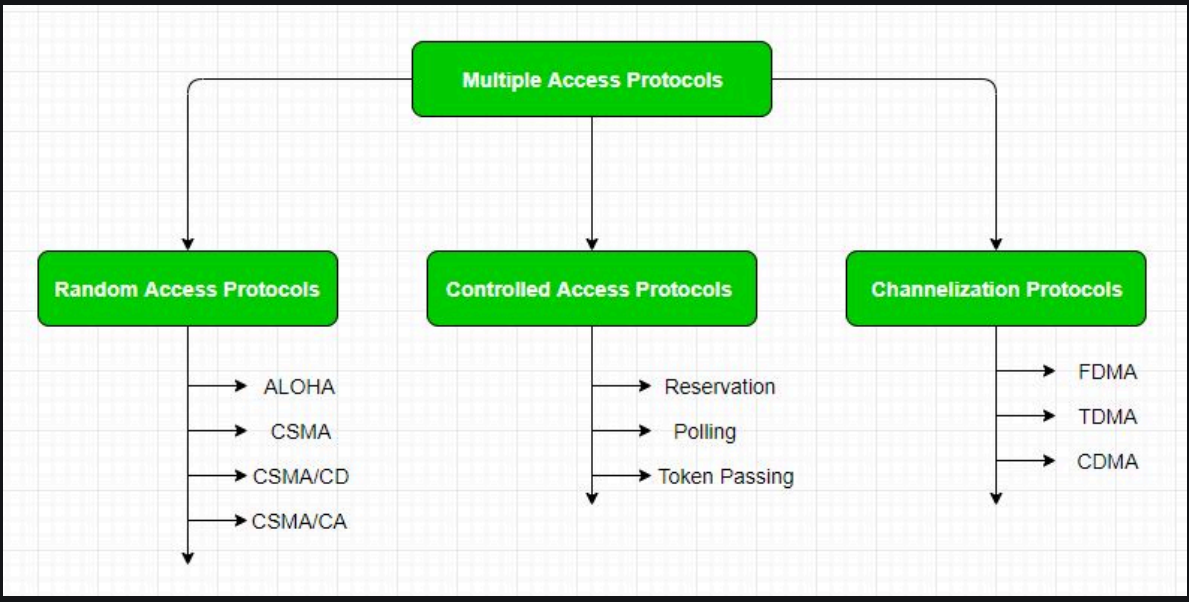
The data link control is responsible for the reliable transmission of messages over transmission channels by using techniques like framing,

error control and flow control. For Data link control refer to – Stop and Wait ARQ.

Multiple Access Control

If there is a dedicated link between the sender and the receiver then data link control layer is sufficient, however if there is no dedicated link present then multiple stations can access the channel simultaneously. Hence multiple access protocols are required to decrease collision and avoid crosstalk. For example, in a classroom full of students, when a teacher asks a question and all the students (or stations) start answering simultaneously (send data at same time) then a lot of chaos is created(data overlap or data lost) then it is the job of the teacher (multiple access protocols) to manage the students and make them answer one at a time.

Thus, protocols are required for sharing data on non dedicated channels. Multiple access protocols can be subdivided further as



1. Random Access Protocol

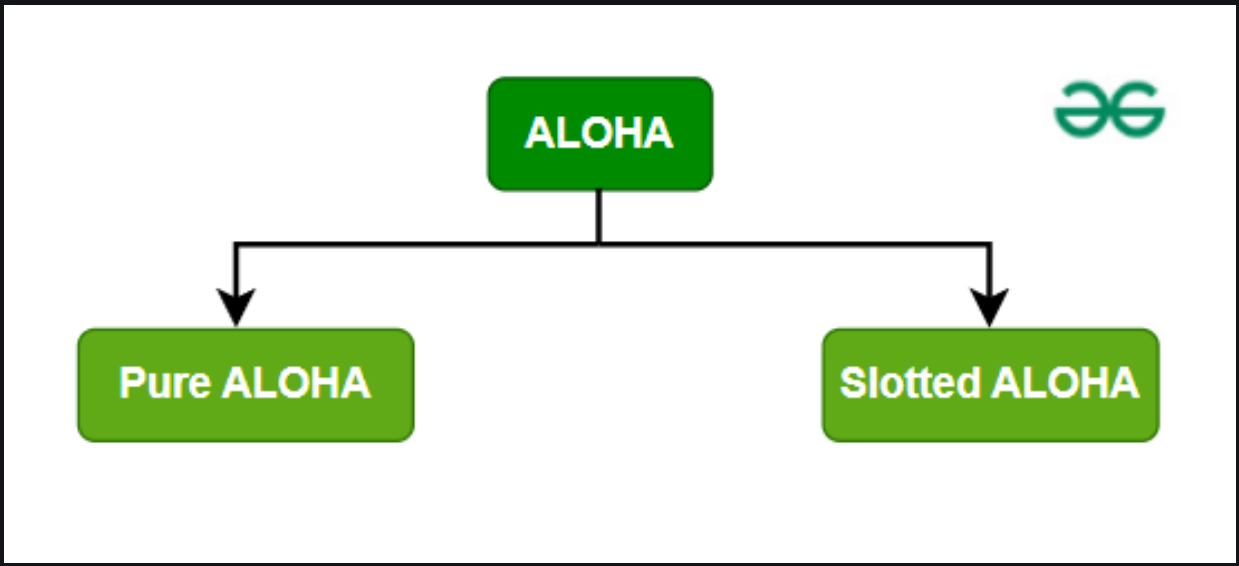
In this, all stations have same superiority that is no station has more priority than another station. Any station can send data depending on medium's state(idle or busy). It has two features:

- There is no fixed time for sending data
- There is no fixed sequence of stations sending data

The Random access protocols are further subdivided as:

ALOHA

It was designed for wireless LAN but is also applicable for shared medium. In this, multiple stations can transmit data at the same time and can hence lead to collision and data being garbled.

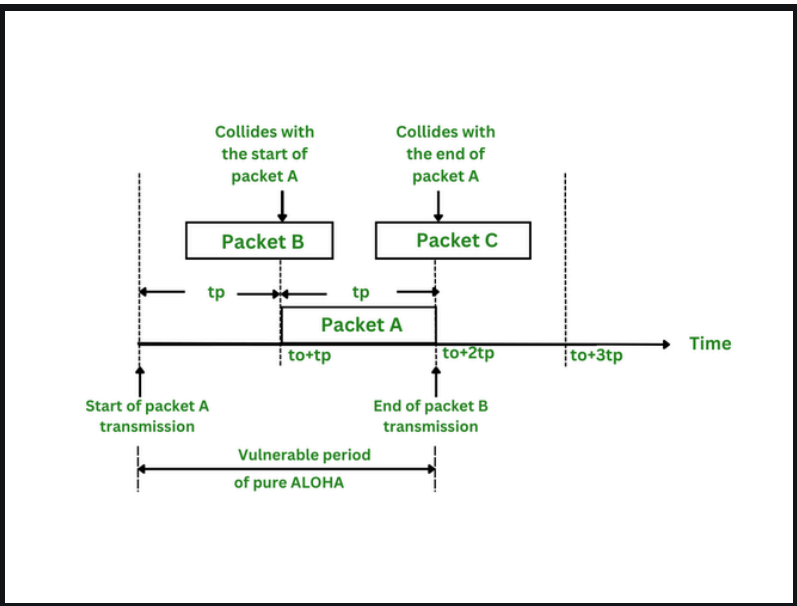


Types of Aloha

Pure ALOHA

When a station sends data it waits for an acknowledgement. If the acknowledgement doesn't come within the allotted time then the station waits for a random amount of time called back-off time (Tb) and re-sends the data. Since different stations wait for different amount of time, the probability of further collision decreases.

```
Vulnerable Time = 2* Frame transmission time
Throughput =  G exp{-2*G}
Maximum throughput = 0.184 for G=0.5
```

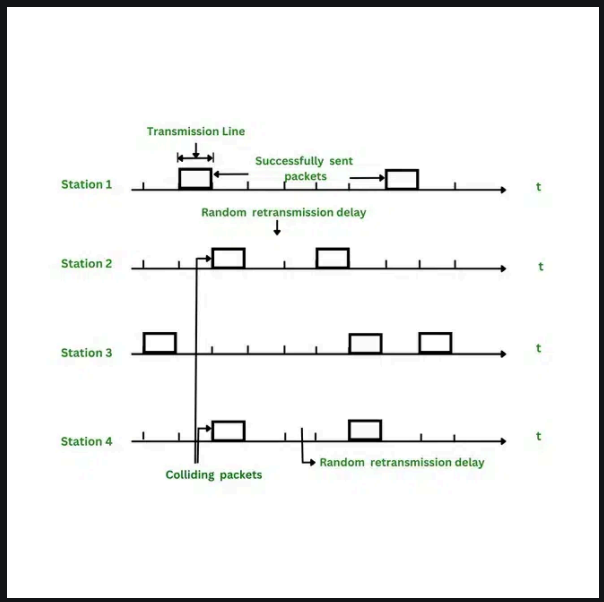


Pure Aloha

Slotted ALOHA

It is similar to pure aloha, except that we divide time into slots and sending of data is allowed only at the beginning of these slots. If a station misses out the allowed time, it must wait for the next slot. This reduces the probability of collision.

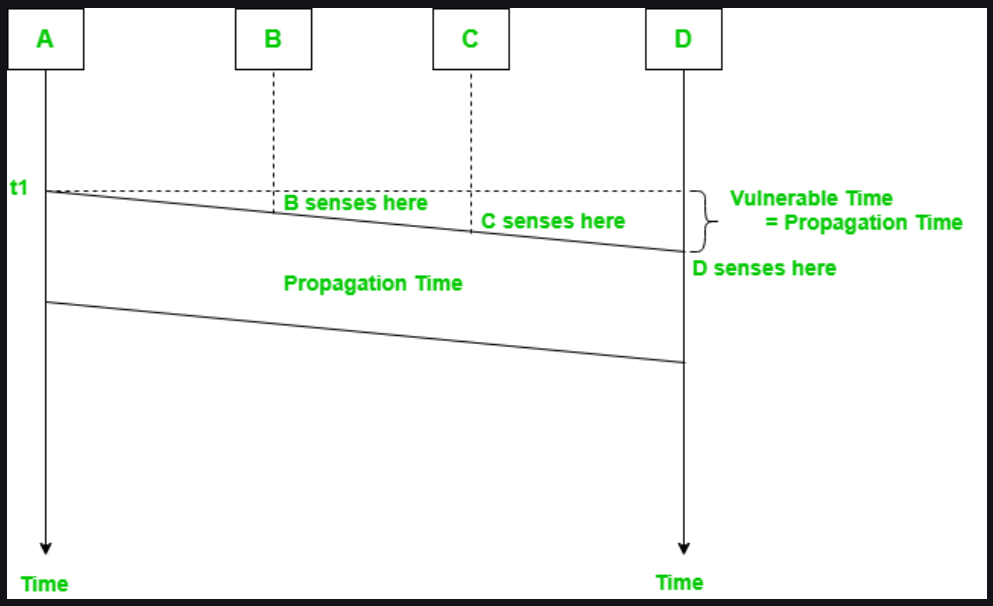
```
Vulnerable Time =  Frame transmission time
Throughput =  G exp{-*G}
Maximum throughput = 0.368 for G=1
```



Slotted ALOHA

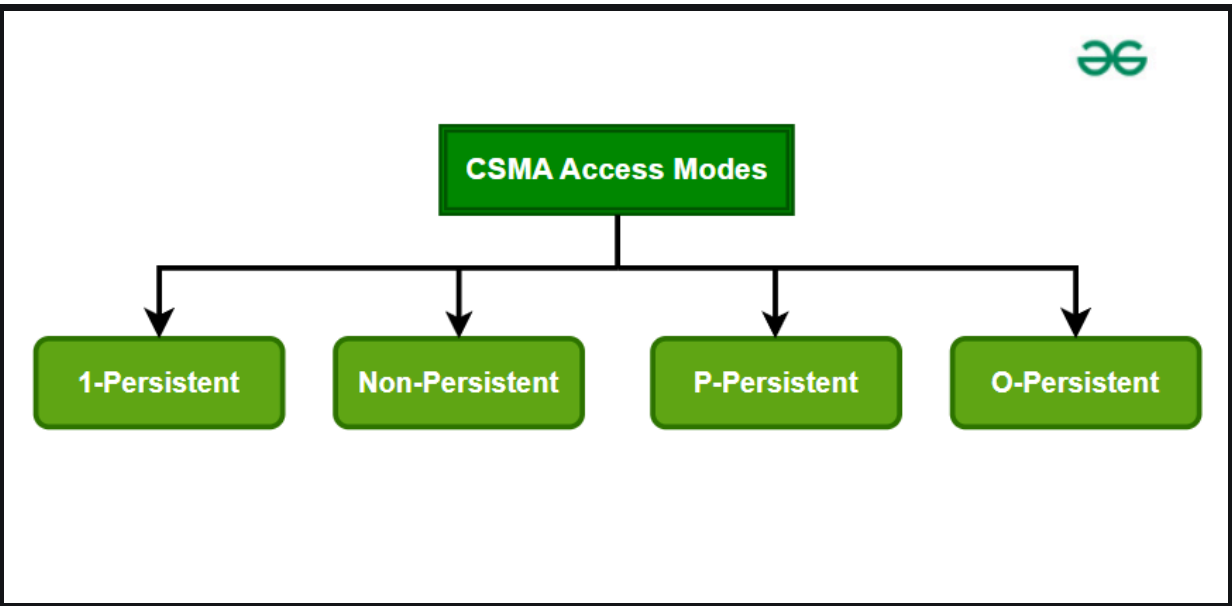
CSMA

Carrier Sense Multiple Access ensures fewer collisions as the station is required to first sense the medium (for idle or busy) before transmitting data. If it is idle then it sends data, otherwise it waits till the channel becomes idle. However there is still chance of collision in CSMA due to propagation delay. For example, if station A wants to send data, it will first sense the medium.If it finds the channel idle, it will start sending data. However, by the time the first bit of data is transmitted (delayed due to propagation delay) from station A, if station B requests to send data and senses the medium it will also find it idle and will also send data. This will result in collision of data from station A and B.



CSMA

CSMA Access Modes



CSMA Access Modes

- **1-Persistent:** The node senses the channel, if idle it sends the data, otherwise it continuously keeps on checking the medium for being idle and transmits unconditionally(with 1 probability) as soon as the channel gets idle.
- **Non-Persistent:** The node senses the channel, if idle it sends the data, otherwise it checks the medium after a random amount of time (not continuously) and transmits when found idle.
- **P-Persistent:** The node senses the medium, if idle it sends the data with p probability. If the data is not transmitted ((1-p) probability) then it waits for some time and checks the medium again, now if it is found idle then it send with p probability. This repeat continues until the frame is sent. It is used in Wifi and packet radio systems.
- **O-Persistent:** Superiority of nodes is decided beforehand and transmission occurs in that order. If the medium is idle, node waits for its time slot to send data.

CSMA/CD

Carrier sense multiple access with collision detection. Stations can terminate transmission of data if collision is detected. For more details refer – Efficiency of CSMA/CD.

CSMA/CA

Carrier sense multiple access with collision avoidance. The process of collisions detection involves sender receiving acknowledgement signals. If there is just one signal(its own) then the data is successfully sent but if there are two signals(its own and the one with which it has collided) then it means a collision has occurred. To distinguish between these two cases, collision must have a lot of impact on received signal. However it is not so in wired networks, so CSMA/CA is used in this case.

CSMA/CA Avoids Collision By

- **Interframe Space:** Station waits for medium to become idle and if found idle it does not immediately send data (to avoid collision due to propagation delay) rather it waits for a period of time called Interframe space or IFS. After this time it again checks the medium for being idle. The IFS duration depends on the priority of station.
- **Contention Window:** It is the amount of time divided into slots. If the sender is ready to send data, it chooses a random number of slots as wait time which doubles every time medium is not found idle. If the medium is found busy it does not restart the entire process, rather it restarts the timer when the channel is found idle again.
- **Acknowledgement:** The sender re-transmits the data if acknowledgement is not received before time-out.

2. Controlled Access

Controlled access protocols ensure that only one device uses the network at a time. Think of it like taking turns in a conversation so everyone can speak without talking over each other.

In this, the data is sent by that station which is approved by all other stations. For further details refer – Controlled Access Protocols.

3. Channelization

In this, the available bandwidth of the link is shared in time, frequency and code to multiple stations to access channel simultaneously.

- **Frequency Division Multiple Access (FDMA)** – The available bandwidth is divided into equal bands so that each station can be allocated its own band. Guard bands are also added so that no two bands overlap to avoid crosstalk and noise.
- **Time Division Multiple Access (TDMA)** – In this, the bandwidth is shared between multiple stations. To avoid collision time is divided into slots and stations are allotted these slots to transmit data. However there is a overhead of synchronization as each station needs to know its time slot. This is resolved by adding synchronization bits to each slot. Another issue with TDMA is propagation delay which is resolved by addition of guard bands.
  For more details refer – Circuit Switching
- **Code Division Multiple Access (CDMA)** – One channel carries all transmissions simultaneously. There is neither division of bandwidth nor division of time. For example, if there are many people in a room all speaking at the same time, then also perfect reception of data is possible if only two person speak the same language. Similarly, data from different stations can be transmitted simultaneously in different code languages.
- **Orthogonal Frequency Division Multiple Access (OFDMA)** – In OFDMA the available bandwidth is divided into small subcarriers in order to increase the overall performance, Now the data is transmitted through these small subcarriers. it is widely used in the 5G technology.

Advantages of OFDMA

- High data rates
- Good for multimedia traffic
- Increase in efficiency

Disadvantages OFDMA

- Complex to implement
- High peak to power ratio

- **Spatial Division Multiple Access (SDMA)** – SDMA uses multiple antennas at the transmitter and receiver to separate the signals of multiple users that are located in different spatial directions. This technique is commonly used in MIMO (Multiple-Input, Multiple-Output) wireless communication systems.

Advantages SDMA

- Frequency band uses effectively
- The overall signal quality will be improved
- The overall data rate will be increased

Disadvantages SDMA

- It is complex to implement
- It require the accurate information about the channel

Features of Multiple Access Protocols

- **Contention-Based Access:** Multiple access protocols are typically contention-based, meaning that multiple devices compete for access to the communication channel. This can lead to collisions if two or more devices transmit at the same time, which can result in data loss and decreased network performance.
- **Carrier Sense Multiple Access (CSMA):** CSMA is a widely used multiple access protocol in which devices listen for carrier signals on the communication channel before transmitting. If a carrier signal is detected, the device waits for a random amount of time before attempting to transmit to reduce the likelihood of collisions.
- **Collision Detection (CD):** CD is a feature of some multiple access protocols that allows devices to detect when a collision has occurred

and take appropriate action, such as backing off and retrying the transmission.

- **Collision Avoidance (CA):** CA is a feature of some multiple access protocols that attempts to avoid collisions by assigning time slots to devices for transmission.
- **Token Passing:** Token passing is a multiple access protocol in which devices pass a special token between each other to gain access to the communication channel. Devices can only transmit data when they hold the token, which ensures that only one device can transmit at a time.
- **Bandwidth Utilization:** Multiple access protocols can affect the overall bandwidth utilization of a network. For example, contention-based protocols may result in lower bandwidth utilization due to collisions, while token passing protocols may result in higher bandwidth utilization due to the controlled access to the communication channel.

Conclusion

In conclusion, Multiple Access Protocols are essential for managing how devices share a network. They help ensure that data is transmitted smoothly and efficiently, preventing collisions and interference. By organizing network traffic, these protocols allow multiple devices to communicate over the same channel without issues, making networks work better for everyone.

Frequently Asked Questions on Multiple Access Protocols – FAQs

Why are Multiple Access Protocols important?

*Multiple Access Protocols is importantbecause, **t**hey ensure data is sent and received efficiently without collisions or interference.*

How do Multiple Access Protocols work?

Multiple Access Protocols manage network traffic by organizing how and when each device can send data.

What are some common Multiple Access Protocols?

common Multiple Access Protocols include CSMA/CD (used in Ethernet), CSMA/CA (used in Wi-Fi), and TDMA (used in cellular networks).

What is CSMA/CD?

Carrier Sense Multiple Access with Collision Detection (CSMA/CD) is a protocol that detects collisions on the network and manages data transmission to avoid them.

Comment More info Advertise with us

Next Article

Carrier Sense Multiple Access (CSMA)

Similar Reads

Difference Between Network Layer Protocols and Application Layer...

Protocols are the set of rules that govern communication between devices in computer network. These rules command how devices should send and...

5 min read

Controlled Access Protocols in Computer Network

Controlled Access Protocols (CAPs) in computer networks control how data packets are sent over a common communication medium. These protocols...

6 min read

Difference Between Network Topology and Network Protocols

Network Topology and Network Protocols are closely related but distinct concepts in the field of computer networking. Network Topology refers to t...

5 min read

Collision-Free Protocols in Computer Network

Almost all collisions can be avoided in CSMA/CD but they can still occur during the contention period. The collision during the contention period...

4 min read

Routing v/s Routed Protocols in Computer Network

The Network Layer of the OSI Model is responsible for providing logical addressing, which routers use to select best path for routing packets. There...

6 min read

Link Access Procedure (LAP) Protocols

Link Access Procedure (LAP) is basically considered as an ITU family of Data Link Layer (DLL) protocols that are subsets of High-Level Data Link Control...

2 min read

Types of Virtual Private Network (VPN) and its Protocols

VPN stands for Virtual Private Network (VPN), that allows a user to connect to a private network over the Internet securely and privately. VPN creates a...

7 min read

Network Protocols

Network Protocols are a set of guidelines governing the exchange of information in a simple, dependable and secure way. Network protocols are...

3 min read

Network Protocols and Communications

Data communication are the exchange of data between two nodes via some form of link (transmission medium) such as cable. Now these Data are...

2 min read

14 Most Common Network Protocols And Their Vulnerabilities

Network Protocols are a set of established rules which control and govern the interchange of information by following a secure, reliable, and easy...

8 min read