

ALOHA, CSMA protocols

ALOHA and CSMA are two different protocols used in computer networking to control the access of multiple devices to a shared communication medium.

ALOHA (Additive Link On-line Hawaii Area):

ALOHA is a simple, but widely used protocol in wireless networks. In ALOHA, each device can transmit data whenever it wants, without checking whether the communication medium is free or not. If two or more devices transmit data at the same time, a collision occurs and the data gets corrupted. ALOHA protocol tries to reduce the probability of collision by randomly choosing the time to transmit data. ALOHA has a high probability of collisions, but it is simple and easy to implement.

CSMA (Carrier Sense Multiple Access):

CSMA is a protocol that allows devices to share the communication medium by sensing whether it is idle or not. If a device senses that the medium is idle, it starts transmitting data. However, if two or more devices start transmitting data at the same time, a collision occurs, and the data gets corrupted. CSMA tries to reduce the probability of collisions by using techniques like CSMA/CD (Carrier Sense Multiple Access with Collision Detection) or CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) to handle the collisions.

In CSMA/CD, if a collision is detected, the devices stop transmitting and wait for a random time before trying again. In CSMA/CA, devices request permission to transmit before sending the data, and wait for acknowledgement before starting the transmission.

Overall, both protocols are used to minimize the probability of collisions in shared communication mediums, but CSMA is more widely used in modern networks as it is more efficient in handling the collisions.

Controlled Access: Polling, Reservation, Token Passing

Controlled Access is another protocol used in computer networking to control the access of multiple devices to a shared communication medium. In contrast to ALOHA and CSMA, Controlled Access protocols allocate the access to the devices in a controlled and orderly manner. Some examples of Controlled Access protocols are Polling, Reservation, and Token Passing.

Polling:

Polling is a protocol in which a central device, called the Polling Station, sends a signal to the devices on the network one by one to check if they have any data to transmit. If a device has data, it responds to the Polling Station and sends its data. If not, the next device is polled. This protocol is efficient when the number of devices on the network is small, and the data transfer is of uniform size.

Reservation:

Reservation is a protocol in which a device first sends a request to the network's central control point for permission to transmit data. The central control point then assigns a reservation slot to the device. During the reservation slot, the device can transmit data without any competition from other devices. This protocol is useful when the data transfer is of a variable size, and the devices are not always available to transmit data.

Token Passing:

Token Passing is a protocol in which a token, a unique bit pattern, is circulated on the network. A device can transmit data only when it has the token. When a device completes its transmission, it passes the token to the next device in the network. This protocol is useful when the devices on the network are geographically dispersed, and the data transfer is of a variable size.

Overall, Controlled Access protocols allocate the access to the devices in a controlled and orderly manner, which can lead to more efficient use of the shared communication medium. However, these protocols are more complex than ALOHA and CSMA and may require more overhead and processing power.

Examples of IEEE Standards(802.2,802.3,802.4, 802.5)

The IEEE 802 standards are a series of protocols that define the physical and data link layer specifications for local area networks (LANs). Here are some examples of IEEE 802 standards:

IEEE 802.2:

IEEE 802.2 is a standard that defines the logical link control (LLC) sublayer of the data link layer. The LLC sublayer is responsible for providing a common interface between the network layer and the media access control (MAC) sublayer.

IEEE 802.3:

IEEE 802.3 is a standard that defines the physical and MAC layer specifications for Ethernet LANs. It specifies the data transfer rates, signalling, and media access control for Ethernet LANs. This standard is also known as the Ethernet standard.

IEEE 802.4:

IEEE 802.4 is a standard that defines the physical and MAC layer specifications for token bus LANs. It specifies the data transfer rates, signalling, and media access control for token bus LANs. Token bus networks use a token-passing mechanism to control access to the shared communication medium.

IEEE 802.5:

IEEE 802.5 is a standard that defines the physical and MAC layer specifications for token ring LANs. It specifies the data transfer rates, signalling, and media access control for token ring LANs.

LANs. Token ring networks use a token-passing mechanism to control access to the shared communication medium.

Overall, IEEE 802 standards are essential in defining the physical and data link layer specifications for LANs, and they provide a common framework for LAN equipment vendors to develop and implement compatible network devices.

Basics of Wi-Fi (802.11)

Wi-Fi (Wireless Fidelity) is a set of protocols that allow devices to wirelessly connect to a local area network (LAN) or the internet. Wi-Fi is based on the IEEE 802.11 family of standards and operates in the 2.4 GHz and 5 GHz frequency bands.

Here are some basics of Wi-Fi (802.11):

Wi-Fi Modes:

Wi-Fi devices operate in two modes: Infrastructure mode and Ad hoc mode. In Infrastructure mode, devices connect to a central access point (AP) that is connected to a wired network. In Ad hoc mode, devices directly connect to each other without an AP, creating a peer-to-peer network.

Wi-Fi Standards:

Wi-Fi standards are part of the IEEE 802.11 family of standards. The standards define the data transfer rates, range, frequency bands, and other specifications for Wi-Fi devices. The most common Wi-Fi standards are 802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax.

Wi-Fi Security:

Wi-Fi networks can be secured using various security protocols like Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), and WPA2. These security protocols encrypt the data being transmitted over the network, protecting it from unauthorized access.

Wi-Fi Channels:

Wi-Fi devices operate on specific channels within the 2.4 GHz and 5 GHz frequency bands. The channels are spaced apart to minimize interference between adjacent channels. The number of available channels depends on the Wi-Fi standard and the regulatory domain.

Wi-Fi Range:

The range of a Wi-Fi network depends on various factors like the power output of the access point, the location of the access point, the obstacles in the environment, and the sensitivity of the client device. Wi-Fi range can be extended using techniques like repeaters, range extenders, and mesh networks.