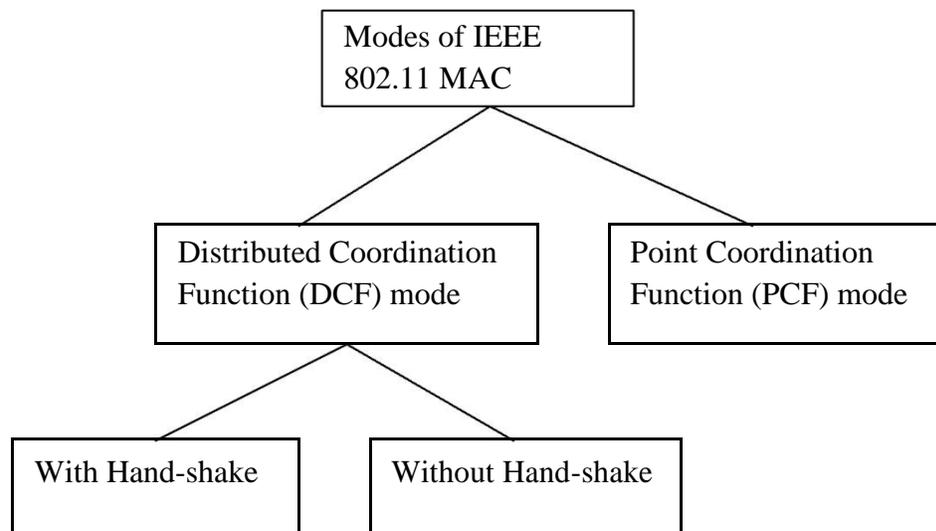


## Different modes of operation of IEEE 802.11 MAC protocol

---

Before discussing the details of the IEEE 802.11 MAC protocol, it is useful to understand the different modes of operation of the protocol as classified below.



## **Figure W1: Different modes of operation of MAC protocol in a WLAN**

### PCF mode of operation

In this mode of operation, an AP acts as the central controller for all the computers lying within the radio range of the AP. The AP decides who transmits when. Thus, there is no contention among computers for medium access. The AP can, but not necessarily, follow a round-robin policy to assign time slots to individual computers, thereby guaranteeing a certain amount of bandwidth to each computer. Because of this guarantee of allocation of bandwidth, this mode of operation can support real-time traffic. However, if the amount of traffics generated by different computers widely vary, this mode is not suitable. This is due to the fact that the AP may allocate bandwidth to a computer which may not have much data to transmit. Finally, the IEEE 802.11 standard says that implementation of the PCF mode of operation is *optional*.

### DCF mode of operation

In this mode of operation, the presence of an AP is not essential. For example, computers can communicate among themselves using the DCF mode of operation without the assistance of an AP. In such a case, we say that the computers have formed an *ad hoc* network, where there is an absence of infrastructure, such as APs. However, to construct a wireless LAN with the capability to connect to the Internet, it is essential to have an AP which is connected to a router as shown in Figure W1. Whether or not there is an AP, in the DCF mode of operation all the computers compete for medium access, because there is no central controller—if there is an AP, it does not act as a central controller. Because of contention among computers for medium access, there is no guarantee of bandwidth and there is no bound on message delay. Thus, the DCF mode of operation is not suitable for real-time traffic. Rather, data delivery is made on a *best effort* basis—the network makes an effort to deliver data across the wireless medium, but there is no guarantee of bandwidth or bound on delay. Finally, the IEEE 802.11 standard says that implementation of the DCF mode of operation is *mandatory*, that is, the DCF mode of operation must be supported by a network card claiming to implement IEEE 802.11.

*Note:* We have said that the PCF mode is optional, whereas the DCF mode is mandatory. If an AP implements both the modes, the following is a scenario in which both the modes can be used alternatively. For example, the network can run in the PCF mode for  $T_1$  seconds, followed by the DCF mode for  $T_2$  seconds, followed by the PCF mode for  $T_1$  seconds, and so on. In this manner, all, or, some, computers get a guaranteed bandwidth during the PCF mode, whereas all the computers compete for bandwidth in the DCF mode. Those computers without data to be transmitted will not compete for medium access during the DCF mode, thereby allowing those computers with data to enter the contention phase.



**Figure W2: Alternative use of PCF and DCF modes**

DCF with hand-shake

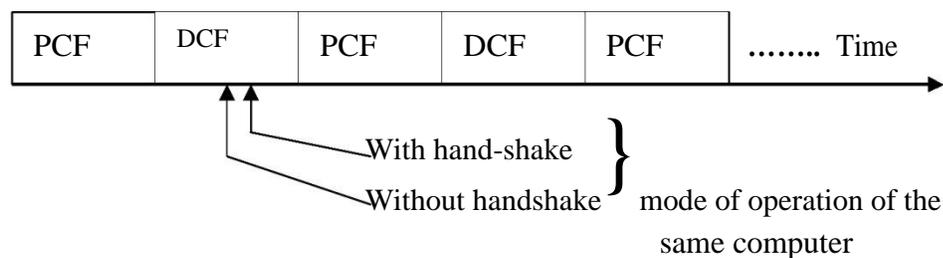
In this mode, a sender obtains permission from an intended receiver before transmitting a packet to the receiver. This is achieved by the sender transmitting a Request To Send (RTS) packet to the intended receiver, and the receiver granting permission by transmitting a Clear To Send (CTS) packet back to the sender. The intended receiver may refuse to grant permission by remaining silent, i.e. not transmitting a CTS packet back to the sender. The sequence of RTS and CTS control packets is known as the process of hand-shake. An intended receiver can refuse to receive a packet from the sender for a variety of reasons, such as lack of buffer and lack of interest in communicating with the sender, to name a few. This mode of operation is preferred where the network traffic is high or if the packet to be transmitted is a long one. In either case, if hand-shake is not used, the packet will collide with another packet at the receiver with high probability. Thus, it is recommended to use the hand-shake mode of DCF when traffic is very high in the network or a packet is very long. The flip side of using hand-shake is the extra overhead of exchanging RTS/CTS control frames. Essentially, before transmitting a long packet, a sender not only informs the intended receiver about the upcoming transmission, but also both the sender and the intended receiver inform their neighbors—via the RTS and CTS control frames—about the upcoming transmission so that the neighbors do not initiate their own transmissions while the packet is being transmitted and *acknowledged*. (The idea of data packet acknowledgement at the MAC level will be explained in a later part of this section.)

DCF without hand-shake

In this mode of operation, a sender does not take permission from an intended receiver before transmitting a data packet. That is, RTS/CTS control frames are not exchanged between a sender and a receiver before the sender transmits a data packet. Rather, the sender just transmits the packet when certain medium sensing conditions are satisfied. These conditions will be explained in a later part of these notes. Thus, there is no coordination between a sender and a receiver prior to a data packet being transmitted. This lack of coordination increases the probability of packet collision. If data traffic is low or packets are short, then this mode of data transmission avoids the overhead due to hand-shaking.

*Note:* The two modes of DCF operation, namely with hand-shake and without hand-shake, are not mutually exclusive. Rather, both coexist, and the two modes can be selected on a packet basis. For example, the dotRTSThreshold variable in the MAC management database can be used to choose a certain mode of operation. The dotRTSThreshold variable is initialized with an integer value representing a threshold

packet length in bytes. If the length of a data packet is equal to or greater than the dotRTSThreshold value, then the MAC layer chooses the “with hand-shake” mode. On the other hand, if the packet length is smaller than the dotRTSThreshold value, then the “without hand-shake” mode is chosen to transmit the data packet. This situation has been further explained in Figure W3. Figure W3 shows that a wireless LAN can alternatively operate in the PCF and DCF modes, and within the same DCF mode duration, a computer can successively transmit two data packets in the “without hand-shake” and the “with hand-shake” modes.



**Figure W3: Alternative use of PCF and DCF modes and consecutive appearances of “with hand-shake” and “without hand-shake” modes in the same DCF period.**

Source : [http://nprcet.org/e\\_content/Misc/e-Learning/ECE/IV\\_year-VIII\\_semester/EC1016\\_WIRELESS\\_NETWORKS.pdf](http://nprcet.org/e_content/Misc/e-Learning/ECE/IV_year-VIII_semester/EC1016_WIRELESS_NETWORKS.pdf)