**Chapter 05: IEEE 802.11 Wireless Local Area Network**

Table of Contents

[5.1 Scope of 802.11 2](#_Toc106753254)

[5.2 Reference Model, Architecture, Service, Frame Formats 2](#_Toc106753255)

[5.2.2 Architecture 2](#_Toc106753256)

[5.2.3 Services 3](#_Toc106753257)

[5.4 Medium Access Control Protocol 4](#_Toc106753258)

[5.4.1 Distributed Coordination Function 4](#_Toc106753259)

[5.4.2 Synchronization and Cell Search 8](#_Toc106753260)

[5.5 Medium Access Control with Support for Quality of Service 9](#_Toc106753261)

[5.5.1 Point Coordination Function 9](#_Toc106753262)

[5.5.2 QoS Support for PCF 9](#_Toc106753263)

[5.5.3 QoS Support Mechanism of 802.11E 10](#_Toc106753264)

[5.5.5 Contention-Based Medium Access 11](#_Toc106753265)

[5.5.6 EDCA Parameters per AC 13](#_Toc106753266)

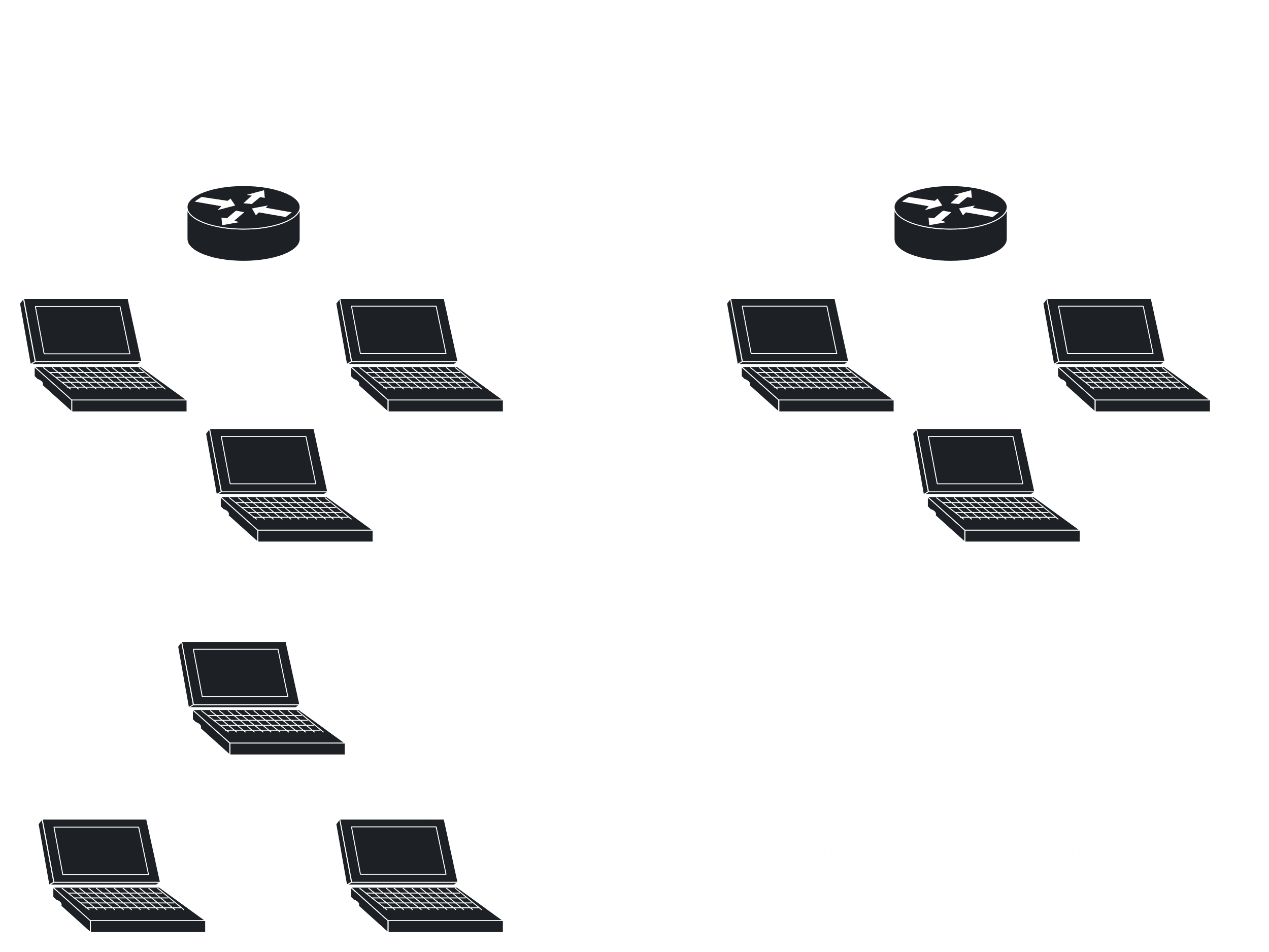
[5.5.8 Controlled Medium Access 15](#_Toc106753267)

## 5.1 Scope of 802.11

The **IEEE 802.11** standard focuses on the lower two layers of the OSI model, the **physical layer** and the **data link layer**. In the physical layer, it defines transmission schema. In the data link layer, it defines the MAC protocol for the MAC sublayer. It does not work with the Logical Link Control sublayer of the data link layer.

## 5.2 Reference Model, Architecture, Service, Frame Formats

### 5.2.2 Architecture



The basic element of IEEE 802.11 networks is called a **Basic Service Set** (BSS). This is a group of stations controlled by a **Coordination Function** (CF), which manages access to the wireless medium. There are two types of Coordination Functions, the **Distributed Coordination Function** (DCF) and the **Point Coordination Function** (PCF). Both of these are concepts for spectrum management and medium access. DCF is used by all the stations in the BSS. Essentially, all the stations fight for control of the channel. PCF is an optional extension that is used to support Quality of Service. For PCF, a coordinator decides which station gets control of the channel, which is how Quality of Service can be ensured.

The **Independent Basic Service Set** (IBSS) is the simplest 802.11 network type. It consists of two or more stations and none of the stations have priority over any of the others. The responsibility of coordinating the medium access is distributed amongst all the stations.

An infrastructure-based BSS includes one station that has access to the wired network, called the **Access Point** (AP).

A Basic Service Set may also be part of a larger network, called an **Extended Service Set** (ESS). An Extended Service Set consists of multiple Basic Service Sets connected over a **Distribution System** (DS). Basics Service Sets and Distribution Systems operate independently, on different media. Basic Service Sets operate on wireless channels, while the Distribution System typically uses the Distribution System Medium (DSM). The 802.11 architecture does not specify media, so the Distribution System Medium may use different variants of the IEEE 802 networks, such as Ethernet.

### 5.2.3 Services

The Distribution System provides the service of transporting **MAC Service Data Units** (MSDUs) between stations that are not in direct communication. An Access Point provides the Distribution System Services (DSS) that enable the MAC to transport MSDUs between stations that cannot communicate over a single instance of radio channel.

There are two categories of services in the IEEE 802.11, the **Station Services** (SS) and the **Distribution System Services** (DSS). Distribution System Services are not available in Independent Basics Service Sets. The main Station Service of a Basic Service Set is the MSDU delivery. Other Stations Services include authentication, de-authentication and privacy.

Distribution System Services include association, re-association, disassociation and integration. The integration service allows delivery of MSDUs between non-802.11 LANs and the Distribution System via a **portal**. A portal is the logical point where a non-802.11 LAN is connected to the Distribution System for communication across different types of LANs.

## 5.4 Medium Access Control Protocol

The 802.11 MAC protocol is built with the help of two coordination functions, the **Distributed Coordination Function**, for traffic without QoS, referred to as **asynchronous services**, and the **Point Coordination Function**, for traffic with QoS, referred to as **synchronous services**.

### 5.4.1 Distributed Coordination Function

In this section, we will be considering an infrastructure-based Basic Service Set, which consists of an Access Point and several stations connected to the Access Point.

#### 5.4.1.1 Listen Before Talk

Before sending a packet from a station to the Access Point, we need to make sure that the **channel is free**. This means that no other station in the same access network is transmitting any information. The channel sensing function is called **Clear Channel Assessment** (CCA). There is a **threshold value**, -82dBm, and if the power level in the channel is detected to be above this, the channel is considered to be busy.

The **Network Allocation Vector** (NAV) is used to **reserve** the channel for some time. When a station starts transmitting, they send out an NAV to every station in the network. The NAV defines how long the transmission may take, during which time the other stations don’t bother sensing the channel.

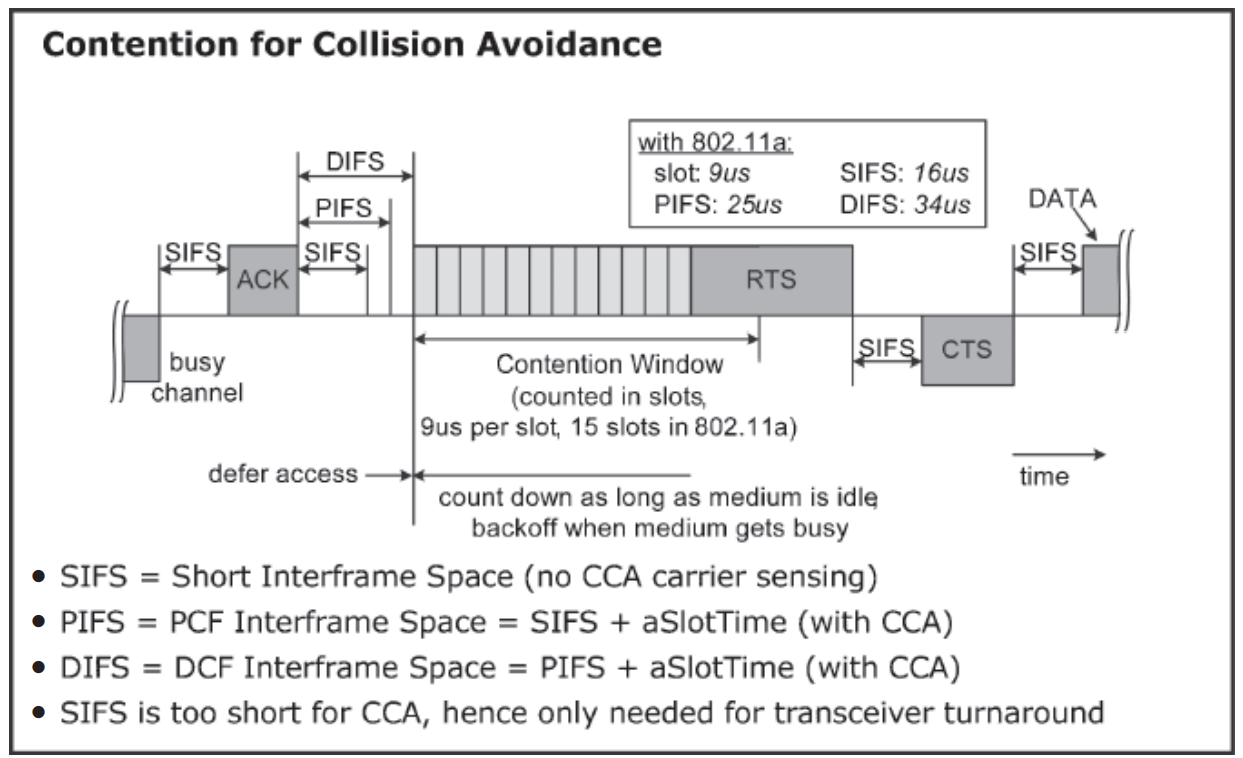
#### 5.4.1.2 Timing and Interframe Spacing

After each MAC frame transmission, IEEE 802.11 requires an idle period called the **Interframe Space** (IFS). This allows us to understand when a transmission has ended and gives us time to figure out what should be transmitted next, based on priority.

In IEEE 802.11, there are four types of IFS defined:

1. Short Interframe Space (SIFS)
2. Point Coordination Function Interframe Space (PIFS)
3. Distributed Coordination Function Interframe Space (DIFS)
4. Extended Interframe Space (EIFS)

Under normal conditions, SIFS, PIFS and DIFS are used. They represent different **priority levels** for medium access. To maintain the different times, an **aSlotTime** is specified which is used to specify the other times. IEEE 802.11 defines this time as .



The **SIFS time** is used to prioritize ACK, CTS and RTS frames. This is the shortest time at . After the last ACK frame from the pervious transmission, we wait a duration of the SIFS time before sending any ACK, CTS or RTS frames.

The **PIFS time** is used to give priority to stations that use PCF and the beacon. If no control frames were sent after the SIFS time, then the PIFS time is used. This time is set to the SIFS time + the aSlotTime, which comes to .

The **DIFS time** is used by stations that use DCF. This time is set to the SIFS time + twice the aSlotTime, which comes to .

The **EIFS time** has a variable value and is only used if an error occurs.

#### 5.4.1.3 Collision Avoidance

When multiple stations try to transmit at the same time, a **collision** occurs. To avoid collisions, the IEEE 802.11 defines a **Collision Avoidance** (CA) mechanism. Each station that needs to transmit must wait for an additional amount of time after the DIFS. This is a random amount of time that is a **multiple of the aSlotTime**.

Every station under DCF maintains a **Contention Window** (CW), which has the number of slots that the station must wait at most. The station picks a random number of slots from the Contention Window and based on that, decides how long to wait. Basically, suppose the Contention Window has 8 slots and the station picks the number 6. Then the additional amount of time the station will wait is 6 x aSlotTime.

When a collision occurs, the Content Window size doubles. This is called the **backoff procedure**. Note however that it is not possible to differentiate between a collision and a missed ACK frame. Both are treated as collisions.

#### 5.4.1.7 Hidden Stations and RTS/CTS

The **Hidden Station Problem** occurs when one station, Station A, is within reach of two different stations, Station B and Station C, but those two stations are not within reach of each other. This may result in one station thinking the channel is idle even while a different one is transmitting.

To deal with this, we use **Request To Send** (RTS) and **Clear To Send** (CTS) frames. Suppose Station B wants to send some data to Station A. First, it sends an RTS frame. When Station A receives this, it **broadcasts** a CTS frame. Both Stations B and C receive this CTS frame. This serves two purposes. It gives Station B permission to start transmitting and informs Station C that some other station that it cannot reach is currently transmitting.

Both the RTS and CTS frames contain information about how long it will take to finish sending the data and the ACK frame. This information is used to set the NAV times by all the other stations. The other stations will not try to transmit within this time.

Between each of the RTS, CTS, data and ACK frames, there is an SIFS. Since stations must wait for the DIFS, and the SIFS is shorter, this gives higher priority to these frames.

### 5.4.2 Synchronization and Cell Search

Within a single BSS, all the stations are **synchronized** to a single clock. To maintain the synchronization, a management frame called a **beacon** is used. The beacon frame is transmitted periodically after a certain period of time called the **Target Beacon Transmission Time** (TBTT). Each beacon frame specifies the TBTT time after which the next beacon will arrive. Beacon frames wait for the PIFS time. However, the beacon frame is **delayed** if there is an ongoing transmission (which can only be high-priority frames that transmit during the SIFS).

## 5.5 Medium Access Control with Support for Quality of Service

### 5.5.1 Point Coordination Function

PCF allows stations to have **priority access** to the radio channel, coordinated by a station called the **Point Coordinator** (PC), which typically resides inside the Access Point.

The entire operation time is divided into sections called **superframes**. Each superframe starts with a beacon, followed by the PCF period, called the Contention Free Period, followed by the DCF period, called the Contention Period. It is mandatory that the Contention Period be at least long enough to allow the delivery of one packet under DCF. If PCF is not being used at all, the Contention Free Period will not exist.

During the Contention Free Period, the Point Coordinator **polls** the other stations one by one until the period ends. The order of polling is what determines the quality of service, since stations polled later have a lower chance of being able to transmit this cycle. After each poll is sent out by the coordinator, it waits for the duration of **one SIFS** for a response, after which it moves on to the next station. At the end of the period, a **CF-End** control frame is transmitted.

### 5.5.2 QoS Support for PCF

If a station is found that has data to send, the coordinator will allow it to start sending data. This causes an issue. The **beacon frame** was set to be transmitted at the end of the Target Beacon Transmission Time. However, for the beacon to be sent, the channel needs to be free for at least the duration of one PIFS. If the polled station is still transmitting during that time, the beacon will be delayed. How long other stations will be delayed is determined by how long the beacon is delayed. Since the exact duration is literally unpredictable, the other stations may end up with poor quality service.

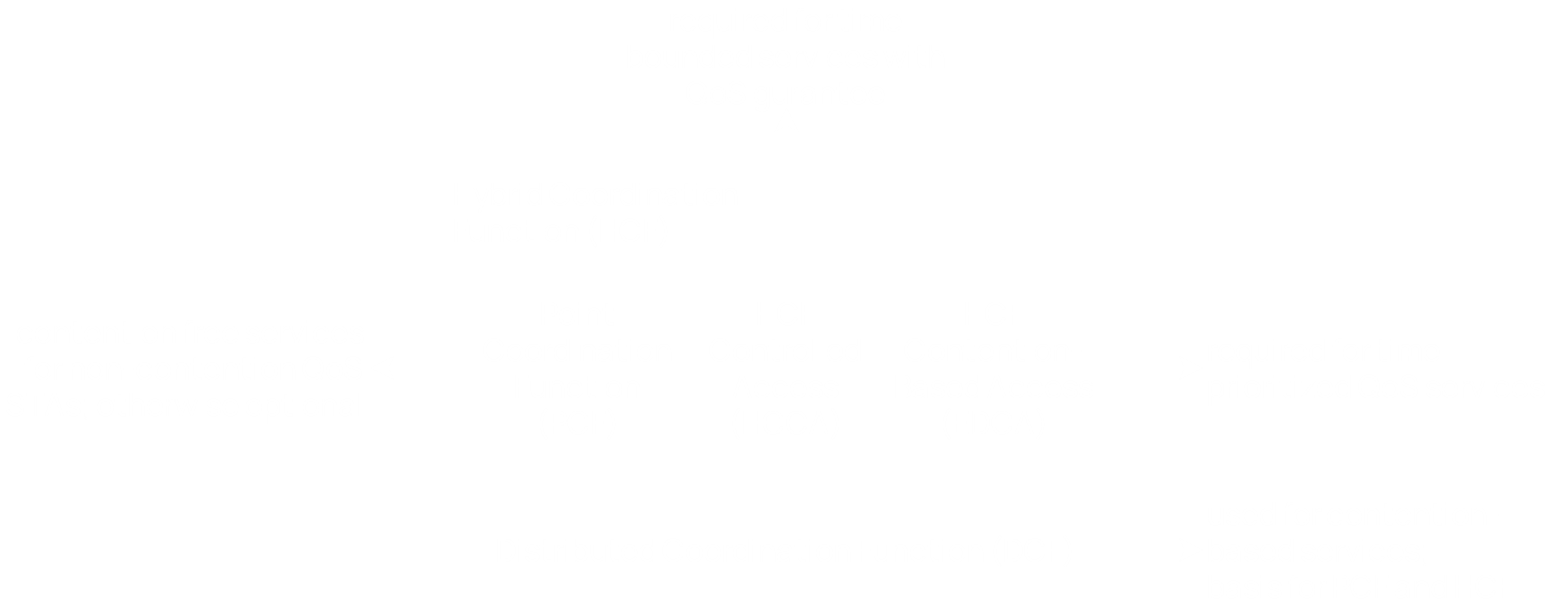
### 5.5.3 QoS Support Mechanism of 802.11E

**802.11E** is an extension of the 802.11 with some extra enhancements for additional **quality of service support**. This extension introduces the **Hybrid Coordination Function** (HCF).

The HCF has two channel access mechanisms, contention-based and controlled. The contention-based channel access mechanism is formally called the **Enhanced Distributed Channel Access** (EDCA) and the controlled channel access is formally called the **HCF Controlled Channel Access** (HCCA). As can be expected, the contention-based channel access is used during the contention period while the controlled channel access is used during the contention-free period. PCF and DCF are used to support older devices in the respective channels.

The coordinator is called the **Hybrid Coordinator** (HC) and usually resides in the **access point**. A Basic Service Set which uses a Hybrid Coordinator and only has stations that support IEEE 802.11E is called a **QoS Supporting Basic Service Set** (QBSS).

Thus, the 802.11E protocol defines a **new MAC layer**, shown below. This supports DCF and HCF separately, with HCF containing PCF, HCCA and EDCA.



Notice that everything is built on top of **DCF**. This is because DCF is a very simple protocol in that it does not require communication between stations. Each station just picks a **random number** and transmits at some point based on it given that the channel is free at the time. Collisions are resolved by using the **backoff strategy** and **retransmissions**. Any attempt to communicate beforehand to ensure collision free transmission actually ends up congesting the network even more, which is why DCF is used.

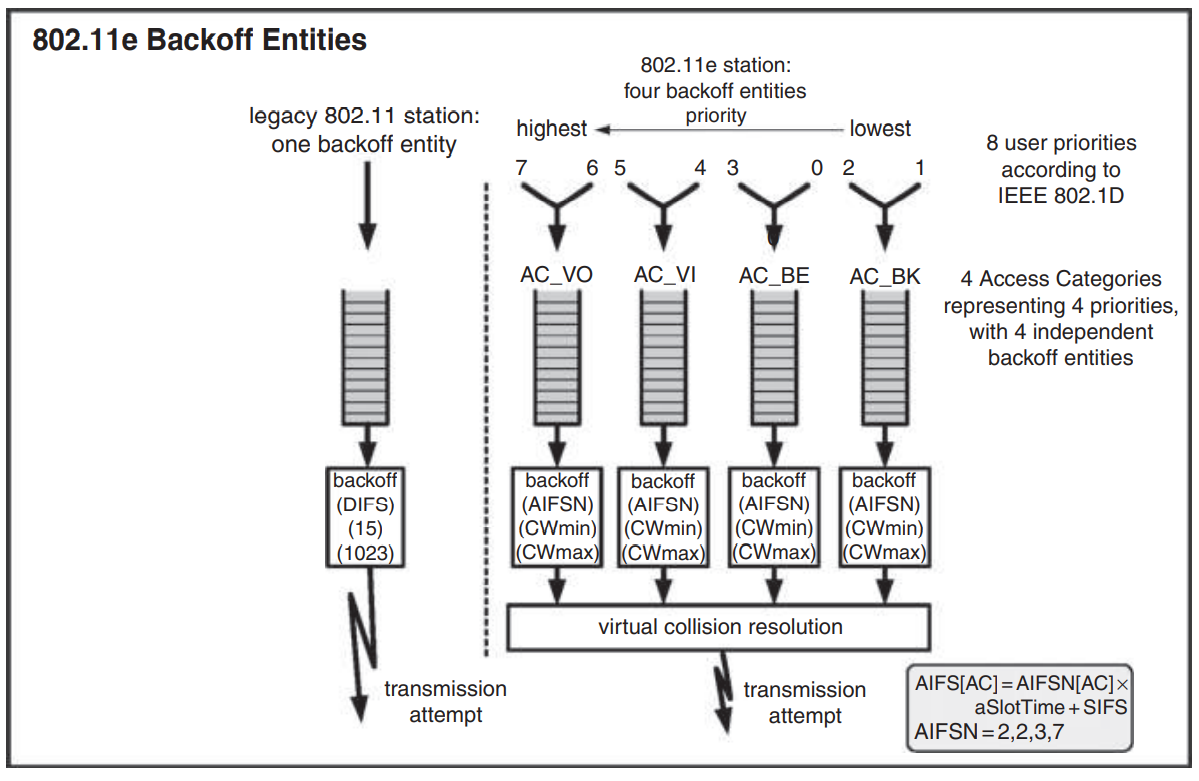
### 5.5.5 Contention-Based Medium Access

Under the Enhanced Distributed Channel Access method, each station places incoming packets into one of four **categories** based on the data type.

|  |  |  |  |
| --- | --- | --- | --- |
| **Priority** | **802.1D User**  **Priority** | **802.11e Access**  **Category (AC)** | **Service Type** |
| lowest | 1 | AC\_BK | background |
|  | 2 | AC\_BK | background |
|  | 0 | AC-BE | best effort |
|  | 3 | AC-BE | best effort |
|  | 4 | AC\_VI | video |
|  | 5 | AC\_VI | video |
|  | 6 | AC\_VO | voice |
| highest | 7 | AC\_VO | voice |

Based on which category some data belongs to, it will start its countdown at a different time. This requires maintaining **separate queues** for each category.

If multiple categories end up finishing their count down together, the station can manually give priority to the most important category, avoiding a collision. However, if different queues in different stations finish their count down together, there will be a collision.



Each queue has a different **backoff entity**, which results in different backoff times. Thus, the station is actively choosing to send data types that have a lower priority later. However, just because a data type has the highest priority does not guarantee it will be sent successfully. The data type will be chosen by a single station, but that station still needs to contend with the other stations for access of the medium. The winning station gets a **transmission opportunity** (TXOP), which is a duration of time during which that station alone can transmit, even if they have multiple packets.

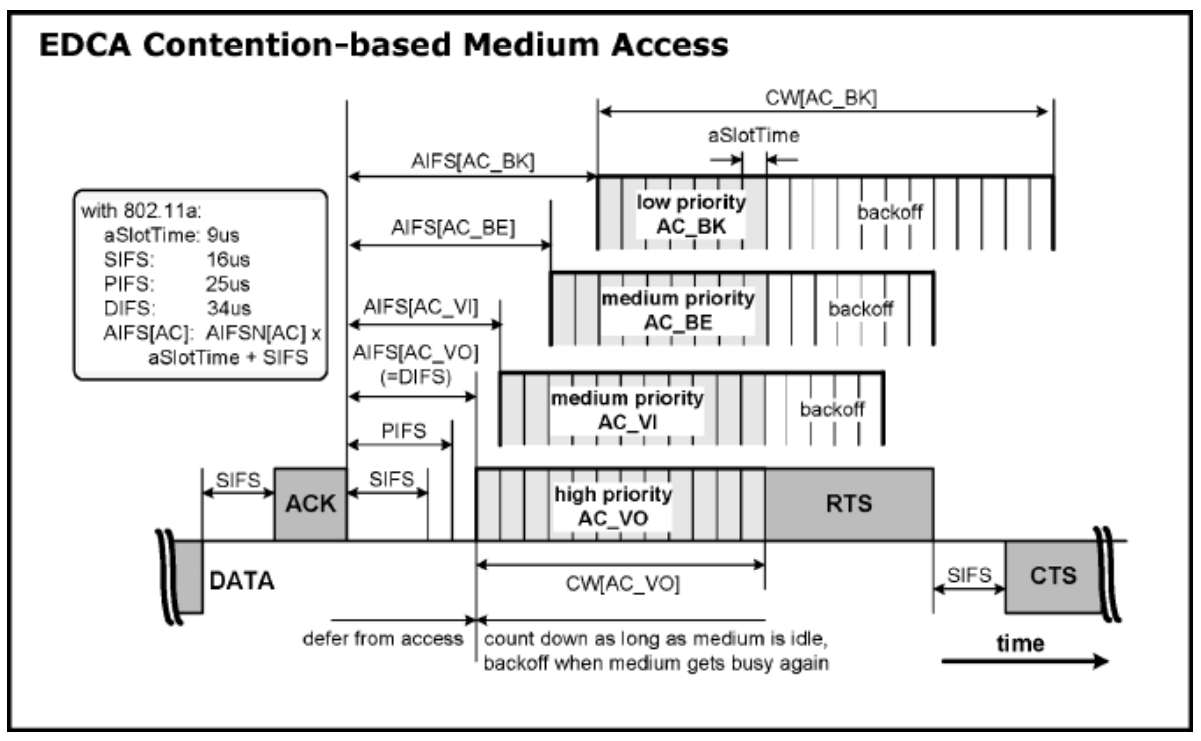
Note that all of this is happening in the **MAC layer**.

Despite its lower performance however, **DCF** is still preferred due to its simplicity.

### 5.5.6 EDCA Parameters per AC

Every station first tries to detect that the medium is idle for a period called the **Arbitration Interframe Space** (AIFS). This is the new term used instead of DIFS in IEEE 802.11E. The AIFS is a combination of the SIFS and a multiple for the aSlotTime, called the **Arbitration Interframe Space Number** (AIFSN). Thus,

To give data in different categories different priorities, we can simply give them **different AIFSN numbers**. Data with a higher priority will have a lower AIFSN number, which means that the AIFS value will be smaller and they will wait for less time. The smallest possible value of the AIFS is equal to the DIFS.



Once the AIFS period has expired, the stations start the **backoff timer**. This backoff time is picked from a **contention window**. Thus, if we assign a smaller contention window to a data type, that data type will likely pick a smaller backoff time and thus start transmission earlier.

Default values for the contention window sizes and the AIFSN values are given below. These values can be adjusted and are specified for the entire Basic Service Set by the Hybrid Coordinator.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **AC** | **CWmin** | **CWmax** | **AIFSN** | **AIFS\*** |
| Legacy 802.11 | 15 | 1023 | 2 | 34μs |
| AC\_BK | 15 | 1023 | 7 | 79μs |
| AC\_BE | 15 | 1023 | 3 | 43μs |
| AC\_VI | 7 | 15 | 2 | 34μs |
| AC\_VO | 3 | 7 | 2 | 34μs |

Based on these values, each category is assigned a contention window size using the following formula:

Thus, each category picks a random value in the range to . Here, refers to the attempt number, i.e. there have been unsuccessful attempts to send data of this category before this.

Picking backoff times from these windows ensures that **mostly**, higher priority data is transferred, with some cases where lower priority data channels end up picking a smaller number and get the opportunity to transmit.

### 5.5.8 Controlled Medium Access

The **HCF Controlled Channel Access** works in the same way as PCF, using **polling**. To do this, some time must be allocated to the hybrid coordinator itself. This time is known as the **Controlled Access Phase** (CAP).