# IEEE 802.11

The standard defines a wireless physical interface and the MAC layer while LLC layer is defined in 802.2.
The standardization process, started in 1990, is still going on; some versions are:

| Standard | Description |
|---|---|
| 802.11 | original standard |
| 802.11 a | transmission at 5 GHz<br>bit rate 54 Mbit/s |
| 802.11 b | support for 5.5 and<br>11 Mbit/s |
| 802.11 e | QoS |
| 802.11 g | trasmission at 2.4 GHz<br>bit rate 54 Mbit/s<br>compatibility with b |
| 802.11 i | security |
| 802.11 p | vehicular networks |
| 802.11 s | mesh networks |

More in detail:

| Caratteristica | 802.11 | 802.11 a | 802.11 b | 802.11 g |
|---|---|---|---|---|
| bandwidth ( MHz) | 83.5 | 300 | 83.5 | 83.5 |
| op. frequecies ( GHz) | 2.4/2.4835 | 5.15/5.35<br>5.725/5.825 | 2.4/2.4835 | 2.4/2.4835 |
| n. of channels | 3 indoor/<br>3 outdoor | 4 indoor +<br>4 in/outdoor | 3 indoor/<br>3 outdoor | 3 indoor /<br>3 outdoor |
| bit rate ( Mbit/s) | 1,2 | 6,9,12,18,24<br>36,48,54 | 1,2,5.5,11 | 1,2,5.5,6,9<br>11,12,18,24<br>36,48,54 |
| physical layer | FHSS/<br>DSSS | OFDM | DSSS | DSSS/<br>OFDM |

## Joining a BSS

A new node to communicate needs to be connected to the BSS; according to the following criteria, it is possible distinguish:

. BSS with AP: when there is an infrastructure;

. BSS without AP: in ad hoc mode.

According to this classification the join operation follows different rules:

. for BSS with AP are mandatory: scanning, authentication and association;

. for BSS without AP jus scanning is required.

### Scanning

The scanning is the operation that allows to detect the frequency of a BSS (usually different BSSs uses different frequencies). It can be done in two ways:

. *passive scanning* when the node sense the channel to discover a *beacon* frame periodically transmitted by BSS;

. *active scanning* when the node sent itself a request with a *ProbeRequest* frame.

Typically, the channel selected is the one with the highest SNR ratio.

### Authentication

This operation is performed one a node has discovered a BSS; it can be done in two modes:

. open system authentication: the AP has a list of MACs that are allowed to be authenticated; it is a simple mechanism;

. shared key authentication: also called *challenge & response*, it involves the use of encryption; the way in which the secret key is distributed is fundamental for the security (802.11 i).

### Association

To transmit and receive data frame, a station after being authenticated, has to be associated to a BSS. The association process allows to exchange informations like capabilities and roaming (possibility of moving); it happens with the following procedure:

. transmission of a *AssociateRequest* frame from the station to the AP;

. transmission of a *AssociationResponse* frame from the AP to the station.

### IEEE 802.11/802.11 b

The access techniques at physical layer are:

. infrared (IR);

. frequency hopping spread spectrum (FHSS);

. direct sequence spread spectrum (DSSS).

The first one in practise is not used; the FHSS technique has not much popularity despite of DSSS.

#### DSSS in 802.11

The radiated power is limited, 85 mW; the frequency band is free from licences: ISM 2.4 GHz (ISM: Industrial, Scientific and Medical) and is divided into 14 channels, where each one is 22 MHz.

Considering a trasmission range of 1 or 2 Mbit/s the spreading is realized with sequences of 11 chip and, according to which modulation is used, there are different spreading factors:

. DBPSK: 11 Mchip/s $\longrightarrow$ 1 Msym/s $\longrightarrow$ 1 Mbit/s con SF = 11;

. DQPSK: 11 Mchip/s $\longrightarrow$ 2 Msym/s $\longrightarrow$ 2 Mbit/s con SF = 5.5.

Using an high spreading factor with these modulation allows to have a good protection against errors (due to fading for example); using much complex modulations (it implies less robustness) it is better have lower spreading factors.

For bit rate 5.5 and 11 Mbit/s CCK (Complementary Code Keying) is used: this mechanism allows to codify more data bit on a single chip using 8 sequence of 64 bit. Codifying simultaneously 4 bits it is possible reach 5.5 Mbit/s while 11 Mbit/s are obtained codifying words of 8 bit.

The card measures always the SNR ratio and propagation conditions: if they are good, a complex modulation can be used to achieve high bit rates, otherwise a simpler modulation is selected.

In practise, the rate is adapted dynamically. An exception are control information frames: they are always transmitted at the basic rate.

### The MAC protocol

The MAC protocol provide functions like:

. resource allocation;

. data segmentation and reassembly;

. MPDU address (the MAC address);

. MPDU format;

. error control;

and defines three type of frames:

. control frames (ACK, handshaking like RTS and CTS);

. data frames;

. management frames (authentication, establishment / release of a connection, synchronization).

According to the type of traffic, data transfer can be:

. asynchronous data transfer for delay-tolerant traffic implemented with DCF (Distributed Coordination Function);

. synchronous data transfer for real-time traffic implemented with PCF (Point Coordination Function).

DCF is always implemented in all cards while PCF is optional; it is important just because the standard that implements QoS (802.11 e) uses some principles of it.

### Time Slot e IFS

Slots, or time interval, represent the temporal unit for the system and their duration is not fixed, but depends on the implementation of the physical layer.

For example, in 802.11 b, the slot duration ($t_{slot}$) is 20 $\mu$s:

$$5\,\mu\text{s}\ [\text{di turnaround}]\ + 15\,\mu\text{s}\ [\text{di power detection}]$$

Interval slots among transmissions are called IFS (Interframe Spaces) and there are 4 types:

. SIFS: divides two transmission of the same dialogue;

. PIFS: gives priority to PCF;

. DIFS: is used by stations when they have to sense the channel;

. EIFS: is used by stations when the physical layer notify at MAC layer that a transmission has not been understood.

This slots time are increasing in time duration.

## DCF Access Scheme

DCF implements CSMA/CA (Carrier Sense Multiple Access/Collision Avoidance): in all devices, infact, there is only one transceiver therefore, to avoid a collision, the only thing to do is wait that the channel is free (avoidance phase). In Ethernet, instead, there two transceivers so, it is possible sense the channel and verify if it is free also during a transmission (detection phase).

DCF is completely distributed so it is implemented both by Access Point and users; there are two modalities in which it can be used:

. DCF base;

. DCF with handshaking.

### DCF base

A node that wants to transmit a packet must sense the channel for a time equal to DIFS; if it is free, it can sent its frame and, after a wait of SIFS, it will be receive the acknowledge (ACK).

The dialogue is single, therefore once the communication has started, packets are divided in time by the shortest IFS, SIFS; this allow to offer the highest priority to a communication already set up. Infact, another station that want to transmit, first has to wait for DIFS, which is longer than SIFS, therefore it will not interfere before the ACK is received by the station that transmited the packet.

A node that is not transmitting nothing is idle: it sense the channel, reads headers of packets that are passing and sets a counter called NAV (Network Allocation Vector). The NAV is set for the entire duration of the current communication and decreases by time: when it reach 0 the channel is surely free.

The sensing procedure is double: it is realized both at the physical layer (measuring the SNR ratio on the channel) and at MAC layer (it is called virtual sensing) based on NAV: the total time required by a communication is PDU+SIFS+ACK. A transmission may failure (the CRC present in data frames is checked) due to collision: the ARQ scheme implemented is *stop* & *wait* with *backoff procedure*.

When a station realize that has failed a transmission extracts a random number from a window between values $[0, \mathrm{CW}_{\min}]$ with, usually, $\mathrm{CW}_{\min}$=31. This random number is multiplied by the time slot ($20\,\mu$s) obtaining the global time for which that station has to wait before trying to retransmit.

If there is another collision, possible values are not taken between 0 e $\mathrm{CW}_{\min}$, but:

$$\mathrm{CW}_i = [2 \cdot (\mathrm{CW}_{i-1} + 1)] - 1$$

where $i$ is the number of attemps of retransmission ($i > 1$).

Considering $n$, number of possible values of the window $[0, \mathrm{CW}_{\min}]$, and knowing that the distribution is uniform, the probability of choosing the same value by two different stations is:

$$\mathcal{P}\left(collision\right) = \frac{1}{n+1}$$

Therefore, the probability of having a collision, globally (it means for all station on a given channel) is:

$$\sum_{i=1}^{n+1} \frac{1}{n+1} \cdot \frac{1}{n+1} = (n+1) \cdot \frac{1}{(n+1)^2} = \frac{1}{n+1}$$

In practise, values double at each failed tentative until a maximum value, usually 1023; the reason is simply: the algorithm try to increase the probability that two stations extract different backoffs to avoid collisions (infact this is how the avoidance mechanism is actually implemented); this is the de-synchronization function of the backoff. Supposing that the load over the network is high, doubling the window allow to extract higher backoff values, therefore those station will delay their transmission when, probably, the load will be lower. But, if the load is not high and collisions are due to bad channel conditions, doubling the contention window is not the best choice.

The backoff is decreased (as the NAV) until it reaches 0: a peculiar feature is that, it can be decreased only if the channel is free while, when other communications take place, the backoff is frozen. Once it is 0, the station can immediately transmit the packets that higher levels sent without waiting DIFS. This choice makes sense because the channel is surely free during the backoff for a period of time that, perhaps, can be either higher than DIFS.

Also stations that succeed in transmitting a frame have to perform the bakcoff: it is called *post-backoff*. It is necessary to have fairness among nodes: infact, if a station has several packets in queue at MAC layer, it will occupy the channel for a long period while other station are shut up. Fairness is provide on the number of packets transmitted and not on the bit rate: it can happen that two stations transmit the same number of packets with very different throughputs. Moreover, the fairness is guaranteed on the long period.

Frames can be fragmented if their size is above a given threshold called *fragmentation threshold*. Fragmentation allows to reach a better quality reducing the probability of having errors, but in each fragments physical and MAC layer header have to be present increasing the overhead. If a fragment is lost a re-contention phase of the channel takes place, but the contention window in which extract the backoff value double each time, to highlight that the transmission is of a single frame; infact fragments are transmitted

at distance SIFS+ACK+SIFS. If the transmission succeeds, the post-backoff is performed just at the end of the transmission of the last fragment, never before in intermediate fragments.

### DCF with Handshaking

This method allows to reserve the channel and, therefore, radio resources. It is used in the following cases:

. with hidden terminals;

. when there are lots of nodes that contend simultaneously the channel;

. to transmit very long packets because in case of failure of them lots of radio resources are lost (in terms of bandwidth and time).

In general, when the packets size is greater than a threshold, called RTS Threshold, the method used is DCF with Handshaking while, on the contrary DCF base is implemented.

L'handshaking introduces two more packets that are always transmitted at the basic rate:

. RTS: it takes 20 Byte and it is sent by the transmitter to reserve the channel;

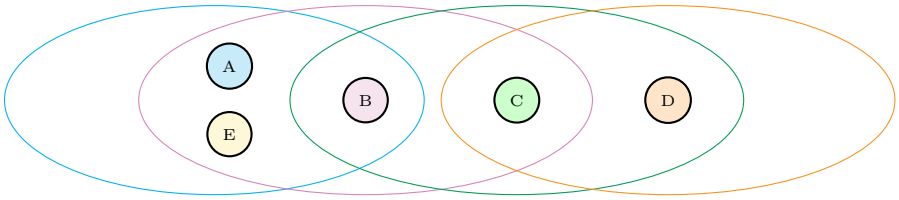
. CTS: it takes 14 Byte and is the positive answer to an RTS.

**Procedure** A station that wants to reserve radio resources sends an RTS; all nodes that sensing the channel understand the RTS have to set their NAV for the entire duration of the transmission. The node that receives the RTS answers with a CTS; as before, all nodes that are in the transmission range of that station have to set their NAV.

In this way the transmission can take place without interferences by other nodes and, therefore, with a small probability of collision. Infact, a probability of fail the transmission is still present since it is possible that the CTS has not been understood causing the retransmission of the RTS using the backoff procedure. The standard says that a station that sent an RTS and does not receive a CTS within a given timeout realize that the destination is unreachable, therefore has to start the backoff procedure.

CTS losses are issues that makes inefficient the network: all nodes within the interference range of both the station that transmitted the RTS and the station that tried to send the CTS, set their NAV although it is not necessary. That time is definitively lost in an useless way.

**Issues** In a situation like the one shown in the following picture, the *hidden terminals problem* is considered:

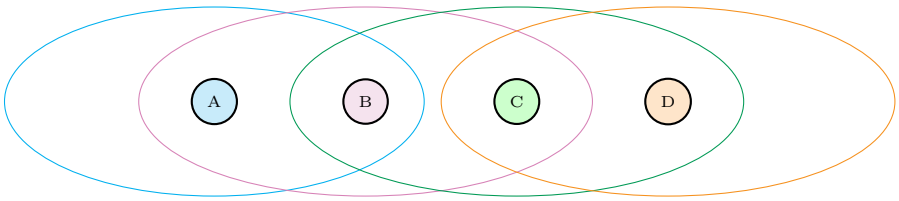



two possible collision situation can take place:

. if A transmits to E, B can hear the communication and, therefore, can not hear the CTS transmit from C to D as an answer of a previous RTS: in this situation the collision occurs in B;

. if D transmits to C and, simultaneously B transmit an RTS to C a collision in C takes place.

MACA (Multiple Access with Collision Avoidance) is a proposal by Karn not accepted in the standard. It originates RTS/CTS mechanism, but although avoids hidden terminals problem, just *try to solve* the exposed terminal problem. Consider:




the situation in which C sends to D an RTS. B of course hearing that communication sets its NAV although, when D answer to C with a CTS B can not understand the transmission since it is not within the interference range of D. Therefore, while D is answering to C, B could transmit to A without create collisions to D. Moreover, if D fails the transmission of the CTS, B is however blocked by the NAV.

MACA, tries to solve the exposed terminals problem in such a way:

. if a station detects an RTS message, it will set its NAV accordingly;

. however, if it does not hear the corresponding CTS within a certain timeout, it should attempt to access to the channel and resets its NAV.

**Counters** Each station uses two counters accordingly to the MPDU size:

. if it is larger than the RTS Threshold, it uses the LRC (Long Retry Counter);

. otherwise the SRC (Short Retry Counter).

Both of them have an independent maximum value called limit and they are used to adapt the retransmission scheme to the type of data carried: for voice packet that are more urgent, the SRC is used, while the LRC is incremented when data packets are transmitted.

### PCF Access Scheme

It is a centralized access scheme used fore services that require QoS because provides a contention-free access to the channel. A Point Coordinator (PC) is needed to poll stations and the PC is usually the access point, therefore PCF can be implemented in presence of infrastructure. Stations that wants to use it have to declare their participation in the CFP (contention free period) phase during the Association Request: after that first step, the PC builds the polling list based on requests; the polling list is static and its implementation is usually done by the system operator. In a CFP period, nodes can transmit only to answer a CP's poll or to acknowledge a MPDU.

PCF and DCF coexist and the CFP starts with a beacon signal periodically broadcast by AP to synchronized nodes; it ends with a particular frame called CF_end. The duration is determined by the PC based on the traffic load; when a CFP starts, all stations that hear the beacon set their NAV to CFP_Max_Duration, a parameter that specify the maximum duration of the period: it is included in the beacon, therefore each node is able to detect it.

To start a new CFP, the CP senses the channel for PIFS: if it is idle, the PC broadcast the beacon frame; then, after SIFS from the beacon, the CP can transmit:

. a CF-Poll frame;

. a data frame;

. a data frame and a CF-Poll frame;

. a CFP_end frame to end immediately the CFP period.

If the CFP is not ended immediately, the polled station can reply, after a SIFS, with:

. a data frame;

. a data frame and a CF-ACK (in case it had received correctly previous data);

. a null frame if it had received any data.

When the PC receives a data frame and a CF-ACK, it has to wait for SIFS and then it can poll another station. In the case in which the PC does not receive a data frame and a CF-ACK, it waits for PIFS and then can poll the following station present in the polling list.

PCF was designed to obtain QoS to real-time traffic, but following issues make it difficult:

. unpredictable beacon delay at the beginning of CFP period (larger the frame size implies longer beacon delay);

. unknown transmission duration;

. the static polling list implies a relevant polling overhead.

### 802.11 a

The physical layer works at higher frequencies (5 GHz) with respect to 802.11 b; in Europe was difficult to implement (Hyperlan) but now it is approved (802.11 h). As transmission technology uses OFDM (Orthogonal Frequency Division Multiplexing) which allows to reach higher throughputs since distributes data over multiple frequency channels, 52 at 300 kHz; each one has a narrow bandwidth carrier with zeros exactly in correspondence of other carries: it implies that co-channel interference is avoided.

Each user can transmits over those multiple narrow-band channel in parallel at a low bit rate: in this way the communication is more robust and a low power consumption is required to make a transmission.

OFDM allows to manage a shorter contention window (15 instead 31: in this way the backoff procedure may take less time) and shorter time intervals. The transmission should occur up to 54 Mbit/s, but usually 2 frequency channel are combined to reach, globally, a speed up to 108 Mbit/s.

### 802.11 g

Approved in June 2003 it uses both OFDM and DSSS to have compatibility with the standard b. Consequently, the power consumption is similar to that standard and avaiable data rates are, in practise, the combination of both standards b and a.

When 802.11 g works not in compatibility with standard b, it can reach higher throughput ($\approx 20$ Mbit/s) thanks to the possibility of using short slot time (9 $\mu$s instead 20 $\mu$s) and shorter time intervals.

That optimization is not provided when 802.11 g works in compatibility with standard b: in this scenario, all nodes must be able to detect preambles and headers, therefore they are transmitted with DSSS using OFDM just

for the payload. If g users wants to transmit only with OFDM, first they have to implement some protection mechanisms:

. CTS (transmit at basic rate) to itself: notify the duration of the transmission to all;

. RTS/CTS: reaches the same purpose, but it is more robust in presence of hidden terminals.

In this situation the throughput reached is $\approx 10\,\text{Mbit/s}$.