Investigation of IEEE standard 802.11 Medium Access Control (MAC) layer in ad-hoc networks and comparison with IEEE 802.16 distributed mesh networks

Master thesis performed in Electronics Systems
by
Fernando Garcia Torre
LiTH-ISY-EX--06/3890--SE
Linköping May 2006
Investigation of IEEE standard 802.11 Medium Access Control (MAC) layer in ad-hoc networks and comparison with IEEE 802.16 distributed mesh networks

Master thesis in Electronics System at Linköping Institute of Technology by

Fernando Garcia Torre

LiTH-ISY-EX--06/3890--SE

Supervisor: Kent Palmkvist
Examiner: Kent Palmkvist
Linköping May 2006
Investigation of IEEE standard 802.11 Medium Access Control (MAC) layer in ad-hoc networks and comparison with IEEE 802.16 distributed mesh networks

Author(s)
Fernando García Torre

Abstract
This thesis involved a research of mechanisms of MAC layer in the ad-hoc networks environment, the ad-hoc networks in the terminology of the standard are called IBSS Independent Basic Service, these type of networks are very useful in real situation where there are not the possibility of display a infrastructure, when there isn’t a network previous planning.

The connection to a new network is one of the different with the most common type of Wireless Local Area Networks (WLAN) that are the ones with infrastructure. The connection is established without the presence of a central station, instead the stations discover the others with broadcast messages in the coverage area of each station. In the context of standard 802.11 networks the communication between the stations is peer to peer, only with one hop. To continue with initiation process is necessary the synchronization between the different stations of his timers.

The other capital mechanism that is treated is the medium access mechanism, to hold a shared and unreliable medium, all the heavy of this issue goes to the distributed coordination function DCF.

In this moment there is an emergent technology, WIMAX or standard IEEE 802.16, like the standard 802.11 is a wireless communication protocol. Some comparison between the MAC layer mechanisms would be realized between these two standards

Keywords
MAC, 802.11, Ad-hoc networks, Access control, Coordination functions, Initiation, Scanning, Synchronization
Abstract

This thesis involved a research of mechanisms of MAC layer in the ad-hoc networks environment, the ad-hoc networks in the terminology of the standard are called IBSS Independent Basic Service, these type of networks are very useful in real situation where there are not the possibility of display a infrastructure, when there isn’t a network previous planning.

The connection to a new network is one of the different with the most common type of Wireless Local Area Networks (WLAN) that are the ones with infrastructure. The connection is established without the presence of a central station, instead the stations discover the others with broadcast messages in the coverage area of each station. In the context of standard 802.11 networks the communication between the stations is peer to peer, only with one hop. To continue with initiation process is necessary the synchronization between the different stations of his timers.

The other capital mechanism that is treated is the medium access mechanism, to hold a shared and unreliable medium, all the heavy of this issue goes to the distributed coordination function DCF.

In this moment there is an emergent technology, WIMAX or standard IEEE 802.16, like the standard 802.11 is a wireless communication protocol. Some comparison between the MAC layer mechanisms would be realized between these two standards.
1 Introduction ............................................................................................................... 1
1.1 Types topologies ................................................................................................. 2
  1.1.1 Infrastructure networks .................................................................................. 2
  1.1.2 IBSS or Ad hoc networks ............................................................................. 3
1.2 Logical Link Control LCC ................................................................................... 4
  1.2.1 IEEE 802.2 LLC services ............................................................................. 5
    1.2.1.1 Unacknowledge connectionless service .................................................. 5
    1.2.1.2 Connection-oriented service ................................................................... 5
    1.2.1.3 Acknowledged connectionless service .................................................... 6
1.3 IEEE 802.11 reference model .............................................................................. 7
1.4 IEEE 802.11 Physical Layer ............................................................................... 8
  1.4.1 Physical Sublayers ......................................................................................... 9
  1.4.2 Radio Spectrum ............................................................................................ 9
1.5 IEEE 802.11 Medium Access Control “MAC sublayer” .................................... 10
2 Types of frames ........................................................................................................ 11
2.1 Data frames ......................................................................................................... 11
  2.1.1 Frame control field ....................................................................................... 12
  2.1.2 Duration field ............................................................................................... 12
  2.1.3 Sequence control field .................................................................................. 12
  2.1.4 FCS field ....................................................................................................... 12
2.2 Control Frames .................................................................................................. 13
  2.2.1 RTS ................................................................................................................ 13
  2.2.2 CTS ................................................................................................................. 13
  2.2.3 ACK ................................................................................................................. 14
2.3 Management Frames ......................................................................................... 14
  2.3.1 Beacon frame ............................................................................................... 15
    2.3.1.1 Timestamp field ...................................................................................... 15
    2.3.1.2 Beacon Interval field ............................................................................. 15
    2.3.1.3 Capability Information field ................................................................... 15
    2.3.1.4 Service Set Identity (SSID) element ....................................................... 15
    2.3.1.5 Supported Rates element ..................................................................... 16
    2.3.1.6 IBSS Parameter Set element ................................................................. 16
  2.3.2 Probe Request frame format ........................................................................ 16
  2.3.3 Probe Response frame format ...................................................................... 16
  2.3.4 Announcement traffic indication map (ATIM) frame .................................... 16
3 Initiation a wireless network ................................................................................ 17
3.1 Mac management functions .............................................................................. 17
  3.1.1 Address Filtering ......................................................................................... 18
  3.1.2 MLME SAP interface message ................................................................... 19
    3.1.2.1 Scan ....................................................................................................... 21
    3.1.2.2 Synchronization .................................................................................... 23
    3.1.2.3 Reset ...................................................................................................... 24
    3.1.2.4 Start ....................................................................................................... 24
  3.1.3 Scanning ....................................................................................................... 26
    3.1.3.1 Passive scanning ................................................................................... 27
    3.1.3.2 Active scanning .................................................................................... 29
    3.1.3.3 More about Probe request ..................................................................... 31
  3.1.4 Starting a BSS ............................................................................................. 32
# List of figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fig 1</td>
<td>Environs of 802.11 stack</td>
<td>1</td>
</tr>
<tr>
<td>Fig 2</td>
<td>Infrastructure topology</td>
<td>3</td>
</tr>
<tr>
<td>Fig 3</td>
<td>Independent topology</td>
<td>3</td>
</tr>
<tr>
<td>Fig 4</td>
<td>Relation between data link sublayers</td>
<td>4</td>
</tr>
<tr>
<td>Fig 5</td>
<td>802.11 protocol stack</td>
<td>7</td>
</tr>
<tr>
<td>Fig 6</td>
<td>Standard 802.11 stack</td>
<td>8</td>
</tr>
<tr>
<td>Fig 7</td>
<td>Data frame</td>
<td>11</td>
</tr>
<tr>
<td>Fig 8</td>
<td>Control field</td>
<td>12</td>
</tr>
<tr>
<td>Fig 9</td>
<td>Sequence control field</td>
<td>12</td>
</tr>
<tr>
<td>Fig 10</td>
<td>RTS frame</td>
<td>13</td>
</tr>
<tr>
<td>Fig 11</td>
<td>CTS frame</td>
<td>13</td>
</tr>
<tr>
<td>Fig 12</td>
<td>ACK frame</td>
<td>14</td>
</tr>
<tr>
<td>Fig 13</td>
<td>General management frame</td>
<td>14</td>
</tr>
<tr>
<td>Fig 14</td>
<td>Beacon frame body</td>
<td>15</td>
</tr>
<tr>
<td>Fig 15</td>
<td>Probe Request body</td>
<td>16</td>
</tr>
<tr>
<td>Fig 16</td>
<td>Probe Response body</td>
<td>16</td>
</tr>
<tr>
<td>Fig 17</td>
<td>Graphic of Mac services</td>
<td>18</td>
</tr>
<tr>
<td>Fig 18</td>
<td>Management SAP of 802.11 MAC</td>
<td>19</td>
</tr>
<tr>
<td>Fig 19</td>
<td>Resume of every involved parameters in management operations</td>
<td>20</td>
</tr>
<tr>
<td>Fig 20</td>
<td>Table of parameters involve in the scan request</td>
<td>21</td>
</tr>
<tr>
<td>Fig 21</td>
<td>Table of parameters involve in the scan confirm</td>
<td>21</td>
</tr>
<tr>
<td>Fig 22</td>
<td>Table of parameters inside the BSSIDDescription</td>
<td>22</td>
</tr>
<tr>
<td>Fig 23</td>
<td>Table of parameters involve in the scan request</td>
<td>23</td>
</tr>
<tr>
<td>Fig 24</td>
<td>Table of parameters involve in the join confirm</td>
<td>23</td>
</tr>
<tr>
<td>Fig 25</td>
<td>Table of parameters involve in the reset request</td>
<td>24</td>
</tr>
<tr>
<td>Fig 26</td>
<td>Table of parameters involve in the reset.confirm</td>
<td>24</td>
</tr>
<tr>
<td>Fig 27</td>
<td>Table of parameters involve in the start request</td>
<td>25</td>
</tr>
<tr>
<td>Fig 28</td>
<td>Table of parameters involve in the start confirm</td>
<td>26</td>
</tr>
<tr>
<td>Fig 29</td>
<td>Example of new station situation in presence of two IBSS</td>
<td>26</td>
</tr>
<tr>
<td>Fig 30</td>
<td>Passive scanning</td>
<td>28</td>
</tr>
<tr>
<td>Fig 31</td>
<td>Active scanning</td>
<td>30</td>
</tr>
<tr>
<td>Fig 32</td>
<td>Probe request sequence</td>
<td>31</td>
</tr>
<tr>
<td>Fig 33</td>
<td>Timing synchronization function</td>
<td>33</td>
</tr>
<tr>
<td>Fig 34</td>
<td>Logical architecture of MAC layer</td>
<td>35</td>
</tr>
<tr>
<td>Fig 35</td>
<td>Basic access method</td>
<td>36</td>
</tr>
<tr>
<td>Fig 36</td>
<td>Interframes spaces</td>
<td>37</td>
</tr>
<tr>
<td>Fig 37</td>
<td>Virtual carrier-sense diagram</td>
<td>38</td>
</tr>
<tr>
<td>Fig 38</td>
<td>Contention window</td>
<td>39</td>
</tr>
<tr>
<td>Fig 39</td>
<td>Backoff procedure</td>
<td>41</td>
</tr>
</tbody>
</table>
Fig 40 ACK procedure....................................................................................................42
Fig 41 Hidden node problem...........................................................................................44
Fig 42 RTS/CTS..............................................................................................................45
Fig 43 Exposed station problem......................................................................................45
Fig 44 SDU Fragmentation..............................................................................................46
Fig 45 Fragmentation exchange......................................................................................47
Fig 46 ACK sequence....................................................................................................49
Fig 47 RTS/CTS sequence..............................................................................................49
Fig 48 Fragmentation sequence......................................................................................50
Fig 49 RTS/CTS with fragmentation sequence...............................................................50
Fig 50 Table of general comparison parameters of the two standard.........................54
Fig 51 Table of MAC layer comparison parameters between the two standard..........58
1 Introduction

In the last ten years the use of wireless networks have firmly establish in the common field of the present society. With the develop of these technologies was necessary the implantation of a unique standard, it was the IEEE organization the mandated of this labour, the name of this standard is “Wireless LAN Medium Access and Control (MAC) and Physical Layer (PHY) Specifications” and it’s known like “ANSI/IEEE Std 802.11 1999 Edition”, in the following years appear new revisions and new standard like 802.11a, 802.11b and 802.11g, they focus in changes over the physical layer, and basically the Mac layer is the same than in the original standard.

The 802.11 protocol provides the core framing operations and the interaction with a wired network backbone. The framework of the protocol stack is showed in the next figure and is a good starting point.

![Fig 1 Environments of 802.11 stack.](image)
The standard 802.11 must treat with many difficult because of the type of medium over the communications are achieving, unlike Ethernet networks that use a more reliable medium. Some of these issues are frequency allocation, in unlicensed frequency bands where the quality of the channel is changing with time-varying and asymmetric propagation properties, and where different device are sharing the same band, that means interferences and noisy medium. The security in a shared medium, where there aren’t physical boundaries with the possibility of superposition of LANs, and like the devices could be mobile power consumption of the RF equipment is managed to low rates of consumption.

This paper approach to the initiate process of and ad hoc network that is described in the standard and the main mechanism of medium access for this type of topology, with the intention of help at the time of decide to choose a MAC layer for a communication system that could be develop in the environment of a non infrastructure network with low overhead of control load. In the last chapter the Wimax mesh topology is going to be compared, focus on the MAC operations.

### 1.1 Types topologies

IEEE 802.11 supports two basic topologies for Wireless LANs:

- Independent networks
- Infrastructure networks

To understand these topologies, it’s necessary to define what basic service set (BSS) is; it’s a group of 802.11 stations communicating one with another that are under the control of a unique distribution coordination function DCF, in the independent networks case, the geographical area where the BSS offer coverage is known as the basic service area BSA, is similar to a cell in a cellular communication network.

#### 1.1.1 Infrastructure networks

It’s known like infrastructure BSS, it’s requires a specialized station known as an access point (AP). The communication is taken two hops:

- First hop, the sender transmits to the access point.
- Second hop, the access point transmits to the received station.

All the communications must be relayed through the access point, which give a fundamental role in the network architecture; it’s costly for dynamic environments, because it must have a previous network planning. Give advantages in the problem of saving energy of the portable devices, and increases the coverage of the network opposite the ad hoc networks, because the standard give the possibility of create Extended Service Ares (ESS), that is a group of access points constituting a large network throughout a distribution system (DS), and with the possibility of connect to external network.
1.1.2 IBSS or Ad hoc networks

A group of wireless stations that communicate directly to exchange information in a peer to peer mode, without any coordinator, timing is controlled in a distributed manner. The coverage area that ad hoc network provide is limited, and in general is not connect to any large network. In the standard there isn’t a limit for the number of devices that are allowed at the same time, but the throughput decrease with the amount of stations. There is not a mechanism for a rely function in an IBSS the problem of the hidden node can cause impossibility of communication between some stations, but this would be treat in a proximate chapter. The direct communication between the stations provide a increase of the network capacity, but oblige a the stations to maintain relationships with all the other mobile stations. Typically this topology is used for short lived networks for specific purpose like occasional meetings.
1.2 Logical Link Control LCC

The target of LCC is to exchange data between LAN’s users using a 802-based MAC. The main features of LCC, as known like the IEEE standard 802.2 can be resumed in the next ideas.

- LLC is independent of:
  - Topology
  - Transmission medium
  - MAC Type

- LCC provides:
  - Data link control
  - Addressing

The next figure show a photo of the relation of the LCC with higher layers and with the 802.11 Mac layer.

The LCC communicates with 802.11 MAC sublayer via the next protocol primitives:

- **MA-UNITDATA.request.** The LLC layer send this primitive to MAC layer to ask for transfer a data frame (MSDU) to another LLC entity on a different station. The MAC sublayer must append all MAC specified fields and pass it to the physical layer. The length of the MSDU must be less than or equal to 2304 octets.

- **MA-UNITDATA-Status.indication.** The MAC communicates to the LCC the status information, for the previous request primitive. It has local significance.

- **MA-UNITDATA.indication.** The Mac layer send this primitive to LCC to transfer it a date frame after check that the frame received from physical layer is correct, this mean a valid standard frame, without errors, and with a correct MAC address.
1.2.1 IEEE 802.2 LLC services

The services afford the communication between peer LLC entities, one in the source station and the other in the end station. The LLC provides three types of services for the network layer Protocol:

- Unreliable Unacknowledge connectionless service
- Reliable Connection-oriented service
- Reliable Acknowledged connectionless service

1.2.1.1 Unacknowledge connectionless service

Unacknowledge connectionless service use datagram, without establishment of a logical connection with the distant station, without any error control or flow control mechanisms, this service sends and receivers LLC PDUs without acknowledgement of delivered and data link layer connection, the reliability delivery is given by a higher layer that assure the delivery. The advantages are:

- When is not necessary to have information of the successful delivery of the data, such as applications involving the periodic sampling of data sources, for example monitoring sensors. With this service we are free of overhead of connection establishment and maintenance.
- When a higher layer protocol provides the necessary error control, flow control and reliability, it would be inefficient to duplicate them in the LCC

1.2.1.2 Connection-oriented service

The connection-oriented service establishes a logical connection between two peer LLCs that provides error control and flow control. The mechanism has three steps, connection establishment, data transfer, and connection termination.

The used error control mechanism is the ARQ (Automatic repeat request), ARQ treats with two different errors: Lost PDU and Damaged PDU.

The general performance of ARQ is:

a. The transmitter sends the frame.

b. When the frame is in the receiver, the station checks whether there are any errors in the frame using a Cyclic Redundancy Check (CRC).

c. The receiver send one acknowledge or a negative acknowledge depend whether the result of CRC.

d. The transmitter will retransmit the frame if receive a negative ACK or doesn’t receive any ACK. LLC could use two different ARQ:

- Continuous ARQ

  The station transmits frames continuous until a error occurs, when the station must retransmit could retransmit only the error frame, this is selective repeat technique or retransmit every frame after the error, go-back-n technique.
IEEE 802.11 MAC layer

- **Stop and wait ARQ**
  
The sending station transmits a frame and then stops waiting for an acknowledged from the receiver. Then if the ACK is positive could transmit the next frame or if the ACK is negative must retransmit the frame.

### 1.2.1.3 Acknowledged connectionless service

The different with unacknowledged connectionless service, it’s that the receiver stations confirm successful delivery of datagram, and the error and flow control is handed through ARQ method, stop and wait. The advantages are in process control and automated factory environments and time-critical alarm or emergency control signals are the scenarios where acknowledged connectionless service distinguishes because the delivery is assured and is not necessary to wait for a connection to be established.
1.3 IEEE 802.11 reference model

Fig 5 802.11 protocol stack

- **Mac entity**: basic access mechanism, fragmentation, encryption.

- **Mac Layer management Entity (MLME)**: synchronization, power management, roaming, Mac MIB, scan for stations, Authenticate relationship between other Mac entity, De-authenticate, Associate with an AP, Reassociate with another AP, Disassociate, reset, Start.

- **Physical layer management Entity (PLME)**: provide the PHY operational characteristics and parameters, channel tuning, PHY MIB, select the channel.

- **Physical Layer Convergence Protocol (PLCP)**: PHY-specific, supports common PHY SAP, provides Clear Channel Assessment signal (carrier sense) (CS/CCA) procedure (carrier sense/clear channel assessment)

- **Physical Medium Dependent Sublayer (PMD)**: modulation and encoding

- **Station Management Entity (SME)**: Provides correct MAC operation. Interacts with both MAC Management and PHY Management. Is necessary for functions as the gathering of layer-dependent status from different layer management entities and settings of layer-specific parameters. The exact operation is not described in this standard.
- Management Information Base (MIB): it store information about the ongoing network characteristics.

The interfaces drawing with double arrows are not describing in this standard. Mac-MLME, PHY-PLME

### 1.4 IEEE 802.11 Physical Layer

The 802.11 Physical layers essentially provide wireless transmission mechanisms for the MAC, in addition to supporting secondary functions such as assessing the state of the wireless medium and reporting it to the MAC. Each physical standard 802.11 has its own PLCP and PMD sublayers like is reflecting in the next draw.

![Fig 6 Standard 802.11 stack](image)

The physical sublayer specifies five permitted transmission techniques, that give to the Mac sublayer the possibility of send the frames by the air medium from one station to another, the big different between them is the technology that they used and the speeds that develop. In this paper it is not the target to discuss about these technologies. But we are going to enumerate some general characteristic.

The original standard 802.11 contain three different physical layers: 2.4 GHz frequency hopping spread spectrum (FHSS) that supports data rates of 1 and 2 Mbps and 2.4 GHz direct sequence spread spectrum (DSSS) that support of data rates of 1 and 2 Mbps and the infrared method that is similar to TV remote technology. The standard 802.11a supports Orthogonal Frequency Division Multiplexing (OFDM) for 5 GHz. It provided mandatory data rates up to 24 Mbps and optional rates up to 54 Mbps. It’s based in code division multiple access (CDMA), which put multiple transmissions onto a single carrier; OFDM encodes a single transmission into multiple subcarriers, OFDM use overlapping carriers, because it can distinguish from one another subcarrier the name for this is orthogonally. It has 12 non-overlapping channels.

The standard 802.11b permits high-rate DSSS (HR-DSSS) support data rates of 5.5 and 11 Mbps. 14 channels, only 3 non-overlapping. The standard 802.1.g supports ERP-ORFM, The ERP (Extended rate physical), introduces ERP to provide support for data
rates up to 54 Mbps in the 2.4 GHz band. It has 4 channels, only 3 non-overlapping. It was an attempt to combine the best of both 802.11a and 802.11b.

1.4.1 Physical Sublayers

PLCP Physical Layer Convergence Procedure
Is essentially a handshaking layer that enables MAC protocol data units (MPDUs) to be transferred between MAC stations over the PMD, adapts the capabilities PMD system to the PHY service.

It’s has data primitives that provide the interface for the transfer of data octets between the MAC and the PMD, a method of mapping the IEEE 802.11 MPDUs into a framing format suitable for sending and receiving data through the wireless medium.

The most important mechanism in this sublayer is carrier sense/clear channel assessment (CS/CCA) procedure; this procedure detects the start of a signal from a different station and determines whether the channel is clear for transmitting.

PMD Physical Medium Dependant
The PLCP converts the frame into a binary bit stream and passes this bit stream to the PMD sublayer, and then the PMD provide a method of transmitting and receiving data, by the wireless medium between two stations.

1.4.2 Radio Spectrum

Radio spectrum allocation is rigorously controlled by regulatory authorities through licensing processes. European allocation is performed by the European Radio communications Office (ERO). Other allocation work is done by the International Telecommunications Union (ITU). The standard 802.11 is a protocol that operate on what is known as unlicensed spectrum, where is not require the operator to obtain an exclusive license to transmit on a given frequency in a given region, these bands are open for anyone to transmit within certain technical parameters such as power limits.

To prevent overlapping uses of the radio waves, frequency is allocated in bands, which are simply ranges of frequencies available to specified applications. The Unlicensed bands that use wireless are two:

- S-Band ISM 2.4-2.5 GHz
- C-Band ISM 5.725 5.875 GHz
1.5 IEEE 802.11 Medium Access Control “MAC sublayer”

The primary service of the 802.11 standard is to deliver MAC service data units (MSDUs) between peer logical link controls (LLCs). The IEEE 802.11 MAC layer provides three principal operations in support of LLC sublayer:

- Joining a wireless network.
- Provide Access control functions to the wireless sharing-medium such as:
  - Addressing
  - Access coordination, controls the transmission of user data into the air.
  - Frame check sequence generation and checking
  - LLC PDU delimiting
- Providing authentication and privacy

Furthermore, 802.11 MAC performs tasks with the physical layers of the standard IEEE 802.11, the MAC rides on every physical layer and permits the interoperate of different transmission speeds. Different physical layers may provide different transmission speeds, all of which are supposed to interoperate.

In this paper we are going to omit talk about authentication and privacy issues, for focus in joining and providing access issues in the next chapters, there is a chapter where it's showed a brief description of the frames of this standard that will be used along the explications.

In the fifth chapter, it is added a comparison between the Standard 802.11 MAC layer in ad-hoc networks and the IEEE Standard 802.16 MAC Layer in Distributed Mesh Network. This comparison is realized with the help of the thesis “Investigation of IEEE standard 802.16 Medium Access Control (MAC) layer in Distributed Mesh Networks and comparison with IEEE 802.16 ad-hoc networks” written by Pedro Francisco Robles Rico.
2 Types of frames

The specification determines three types of frames: data frames, control frames and management frames. The next issues are going to show the specify frames for Independent BSS.

2.1 Data frames

They carry higher-level protocol data in the frame body such as MSDU from the LCC; two different types of frame data are defined:

- **Data**: carries frame body between two stations.
- **Null**: perform management functions for power-saving, with the frame body empty.

The frame is showed in the next figure:

![Frame Control and Data](image)

The main fields are explaining briefly in the next points.
2.1.1 Frame control field

The next figure shows the frame control field.

<table>
<thead>
<tr>
<th>Protocol version</th>
<th>Type</th>
<th>Subtype</th>
<th>To DS</th>
<th>From DS</th>
<th>More Frag</th>
<th>Retry</th>
<th>Pwr Mgt</th>
<th>More data</th>
<th>WEP</th>
<th>Order</th>
</tr>
</thead>
</table>

Frame control field

*Fig 8 Control field*

The next two parameters are useful for the fragmentation:

**More Fragments field**

It’s set to 1 in all data or management type frames that have another fragment of the current MSDU or current MMPDU to follow.

**Retry field**

It’s set to 1 in any data or management type frame that is a retransmission of a previous frame. With this information the station can begin the process of eliminating duplicate frames.

2.1.2 Duration field

This field contains a duration value for each frame, and allows the NAV to be updated.

2.1.3 Sequence control field

The next figure shows the frame sequence control field.

<table>
<thead>
<tr>
<th>Fragment number</th>
<th>Sequence number</th>
</tr>
</thead>
</table>

Sequence control field

*Fig 9 Sequence control field*

**Sequence Number field**

This number is assigned to each MSDU or MMPDU transmitted by a STA, start in zero and is incrementing by one for each new MSDU or MMPDU.

**Fragment Number field**

With this field every frame has an indicator of each fragment of and MSDU or MMPDU, it’s zero in the first fragment and it would be increment by one for each successive fragment.

2.1.4 FCS field

The FCS field containing a 32-bit cyclic redundancy code CRC. The FCS is calculated over all the fields of the MAC header and the Frame Body field.
2.2 Control Frames

This type of frames provides functionality to perform the deliver of the frames. Within the IBSS networks only three control frames are used:

- RTS
- CTS
- ACK

In the other topology, infrastructure BSS:

- PS-Poll

2.2.1 RTS

The RTS frame format is showed by the next figure:

<table>
<thead>
<tr>
<th>Frame Control</th>
<th>Duration</th>
<th>RA</th>
<th>TA</th>
<th>FCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac header</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Fig 10 RTS frame

- The **Receiver Address field**: is the address of the STA, on the WM, that is the intended immediate recipient of the pending directed data or management frame.
- The **Transmitter Address field**: is the address of the STA transmitting the RTS frame.
- The **Duration field**: this value is in microseconds, required to transmit the pending data or management frame, plus one CTS frame, plus one ACK frame, plus three SIFS intervals

2.2.2 CTS

The CTS frame format is showed by the next figure:

<table>
<thead>
<tr>
<th>Frame Control</th>
<th>Duration</th>
<th>RA</th>
<th>FCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac header</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Fig 11 CTS frame

- The **Receiver Address field**: is the address of the STA, on the WM, that is the intended immediate recipient of the pending directed data or management frame is copied from the TA field of the previous RTS frame.
- The **Duration field**: this value is in microseconds, required to transmit the pending data or management frame, plus one ACK frame, plus two SIFS intervals and it’s obtain from the previous RTS minus the time of the CTS and its SIFS.
2.2.3 ACK

The ACK frame format is showed by the next figure:

![Fig 12 ACK frame](image)

- The **Receiver Address field**: is the address of the STA, on the WM, that is the intended immediate recipient of the pending directed data or management frame and it’s copied from the address 2 field of the immediately previous data or management frame.

- The **Duration field**: this value is in microseconds, required to transmit the pending. If there aren’t more fragments the duration field would be zero, but if there are more fragments is the immediately previous data or management frame, minus the time of the ack and its SIFS interval.

2.3 Management Frames

The management frames provides the performance to establish the communications between stations. In the two possible topologies exit the next subtypes:

- **Beacon**
- **Probe request**
- **Probe response**
- **IBSS Announcement Traffic Indication Message (ATIM)**
- **Authentication**
- **Deauthentication**

Only in infrastructure BSS:

- **Disassociation**
- **Association request**
- **Association response**
- **Reassociation request**
- **Reassociation response**

The management frame format is showed by the next figure:

![Fig 13 General management frame](image)
Inside the frame body there are many variable fields, the manner to identify is the order. For the object of explain the performance of the initiation of the 802.11 network, it’s presented in more detail the beacon frame, the probe request and probe response:

2.3.1 Beacon frame

In the next figure the draw of the beacon frame body is showed.

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Beacon interval</th>
<th>Capability Info</th>
<th>SSID information</th>
<th>Supporter rate</th>
<th>DS or FH parameter set</th>
<th>IBBS parameter set</th>
</tr>
</thead>
</table>

Beacon Frame body

*Fig 14 Beacon frame body*

The minimum subfields of the frame body are in the next issues.

2.3.1.1 Timestamp field

This field represents the value of the TSFTIMER (timing synchronization time) of a frame’s source, allows synchronization between the stations in a BSS.

2.3.1.2 Beacon Interval field

The Beacon Interval field represents the number of time units (TUs) between target beacon transmission times (TBTTs). Beacon frames announce the existence of an 802.11 network with periodicity; in these frames the stations find the information about the BSS parameters.

2.3.1.3 Capability Information field

The Capability Information field contains a number of subfields that are used to indicate requested or advertised capabilities. The Capability Information field consists of the following subfields:

- ESS, IBSS, CF-Pollable, CF-Poll Request, and Privacy, and the remaining part of the Capability Information field is reserved, only the two first are used in IBSS.

Advertise the network's capabilities are its goal, a station that hasn’t that features can not join to the network. Stations within an IBSS set: ESS subfield to 0, IBSS subfield to 1.

2.3.1.4 Service Set Identity (SSID) element

The SSID element indicates the identity of an ESS or IBSS that is a 802.11 network in broadest sense. The length of the SSID information field is between 0 and 32 octets. It’s the name of the BSS, a string of bytes that labels the BSSID. A 0 length information field indicates the broadcast SSID, which is used in the probe request frames to discover all the 802.11 networks.
2.3.1.5 Supported Rates element
The Supported Rates element specifies the rates in the Operational Rate Set as described in the MLME-Join.request and MLME-Start.request primitives. The information field is encoded as 1 to 8 octets where each octet describes a single supported rate in units of 500 kbit/s. Some of the rates are mandatory if you want to join to the BSS, and must be supported by the station.

2.3.1.6 IBSS Parameter Set element
The IBSS Parameter Set element only contains one parameter:
- ATIM Window parameter: It indicates the number of time units (TUs) between ATIM frames in an IBSS, and used only in IBSS Beacon frames

2.3.2 Probe Request frame format
The probe request frame is used to scan for existing 802.11 networks, and within frame body is contained only to subfields in this order: SSID and Supported rates.

![Fig 15 Probe Request body](image1)

2.3.3 Probe Response frame format
The frame body of a management frame of subtype Probe Response contains the information in this order: Timestamp, Beacon interval, Capability information, SSID, Supported rates, physical parameter, IBSS Parameter Set.

![Fig 16 Probe Response body](image2)

When a network receives a probe request with compatible parameters must answer with a probe response, in a IBSS the station who sent the last beacon is the responsible for answer.

2.3.4 Announcement traffic indication map (ATIM) frame
It’s a management frame without frame body. It’s used to notify the receiver, it has buffered data for it, and the recipient is in low-power mode.
3 Initiation a wireless network

3.1 Mac management functions

The next issues are problematical features on the kind of scenarios that wireless medium present:

- Medium is unreliable
- The power consumption is critical
- Unauthorized access can occur because of the lack of physical boundaries

The goal of management operations is reduce this kind of problems. The MAC functions offers several management services to the stations communicating with each other. The main management functions of the MAC layer are listed:

- Synchronization
- Session Management
- Privacy
- Power Management
Session management refers to such association and authentication of the stations, address filtering upon data delivery. The privacy is held up by the encryption algorithms and is necessary because the wireless medium is not very reliable against others listeners. With the Power management it’s extending the live of the batteries. In this chapter we are going to talk about the synchronization between stations clocks, and for this is necessary to initiating the station, scanning the BSS’s joining and later maintains the synchronization. The Privacy and the power management are not mandatory in an independent BSS, and only the address filtering of the session management.

One way to understand the performance is show in the next scheme, where the access to the MIB by the management services is implementing according to MLME SAP interface that will be explained in the next paragraph.

![Diagram of MAC services](image)

**Fig 17 Graphic of Mac services**

### 3.1.1 Address Filtering

The addressing in MAC layer is made with 48 bit address according to IEEE 802.1990. In independent BSS all the frames are transmitted inside the BSS, wherefore the bits ToDS and FromDS are set to zero in the frame control field of every frame. Furthermore the fields of address in an independent BSS’s frames are:

- Address 1= Destination Address (DA)
- Address 2= Source Address (SA)
- Address 3= BSSID.
This last is the Basic service set identifier, that’s a basic service set identifier, in a Independent BSS all the frames carry the same BSSID and must be created, generate 46 random bits plus two special bits: The U/L bit, with a one that’s mean local address and I/G bit with a zero that’s mean individual address. The all-1s BSSID is the broadcast BSSID.

The address filtering mechanism in the IEEE 802.11 the receiver must examine more than the destination address to make a correct receiver decisions. In the same localization and the same channel, could be, that more than one station were transmitting, the receiver’s station must check more than the destination address, for the properly performance of the Mac layer, in the IBSS are three different directions. With the BSSID the receiver can discard the frames sent from another BSS, this is very important for the no saturation with the broadcast messages.

### 3.1.2 MLME SAP interface message

This interface, MAC layer management entity, is the one between the SME and the MLME, and it take over of several tasks in the Mac Management side, for the object of explain the performance of the initiation and synchronization of the 802.11 network. It’s explained the bellow MLME messages:

- **Scan**
- **Synchronization**
- **Reset**
- **Start**

The next figure showed the part of the standard 802.11 architecture that is used for these functions:

---

**Fig 18 Management SAP of 802.11 MAC**
In the next table shows the different parameters between the primitive messages of management, in the next items it’s explained more deeply:

<table>
<thead>
<tr>
<th>Parameters in MLME message</th>
<th>Parameters in BSSDescriptionSet</th>
<th>Scan request</th>
<th>Scan confirm</th>
<th>Join request</th>
<th>Join confirm</th>
<th>Reset request</th>
<th>Reset confirm</th>
<th>Start request</th>
<th>Start confirm</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSSType</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BSSID</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSID</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ScanType</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ChannelList</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ProbeDelay</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MinChannelTime</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MaxChannelTime</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BSSDescriptionSet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BSSType</th>
<th>BSSID</th>
<th>SSID</th>
<th>BSSType</th>
<th>Beacon Period</th>
<th>DTIM Period</th>
<th>Timestamp</th>
<th>Local Time</th>
<th>PHY Parameterset</th>
<th>CF Parameter set</th>
<th>IBSS parameter set</th>
<th>CapabilityInformation</th>
<th>BSSBasicRateSet</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Resultcode</th>
<th>JoinFailureTimeout</th>
<th>OperationRateSet</th>
<th>STAAddress</th>
<th>SerDefaultMIB</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Fig 19 Resume of every involved parameters in management operations
3.1.2.1 Scan
The next two messages support the mechanism of determining the characteristics of the available BSSs.

3.1.2.1.1 MLME-SCAN.request
These primitive requests a survey of potential BSSs that the STA may later elect to try to join; it is generated by the SME for a STA to determine if there are other BSSs that it may join.

It initiates the scan process when the current frame exchange sequence is completed. Many parameters are used in the scanning procedure. In the next chart we show them:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSSType</td>
<td>Determines whether Infrastructure BSS, Independent BSS, or both, are included in the scan</td>
</tr>
<tr>
<td>BSSID</td>
<td>Identifies a specific or broadcast BSSID</td>
</tr>
<tr>
<td>SSID</td>
<td>Specifies the desired SSID or the broadcast SSID</td>
</tr>
<tr>
<td>ScanType</td>
<td>Indicates either active or passive scanning</td>
</tr>
<tr>
<td>ChannelList</td>
<td>Specifies a list of channels that are examined when scanning for a BSS</td>
</tr>
<tr>
<td>ProbeDelay</td>
<td>Delay (in µs) to be used prior to transmitting a Probe frame during active scanning</td>
</tr>
<tr>
<td>MinChannelTime</td>
<td>The minimum time (in TU) to spend on each channel when scanning</td>
</tr>
<tr>
<td>MaxChannelTime</td>
<td>The maximum time (in TU) to spend on each channel when scanning</td>
</tr>
</tbody>
</table>

*Fig 20 Table of parameters involve in the scan request*

3.1.2.1.2 MLME-SCAN.confirm

This primitive returns the descriptions of the set of BSSs detected by the scan process; it is generated by the MLME as a result of an MLME-SCAN.request to ascertain the operating environment of the STA.

Two parameters are used in the scanning confirm procedure. In the next chart we show them:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSSDescriptionSet</td>
<td>The BSSDescriptionSet is returned to indicate the results of the scan request. It is a set containing zero or more instances of a BSSDescription.</td>
</tr>
<tr>
<td>ResultCode</td>
<td>Indicates the result of the MLMESCAN.confirm: success or invalid parameters.</td>
</tr>
</tbody>
</table>

*Fig 21 Table of parameters involve in the scan confirm*
Each **BSSDescription**, is like a scan report, and consists of the following elements:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Use in IBSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSSID</td>
<td>The BSSID of the found BSS</td>
<td>Yes</td>
</tr>
<tr>
<td>SSID</td>
<td>The SSID of the found BSS</td>
<td>Yes</td>
</tr>
<tr>
<td>BSSType</td>
<td>The type of the found BSS</td>
<td>Yes</td>
</tr>
<tr>
<td>Beacon Period</td>
<td>The Beacon period of the found BSS (in TU)</td>
<td>Yes</td>
</tr>
<tr>
<td>DTIM Period</td>
<td>The DTIM period of the BSS (in beacon periods)</td>
<td>NO</td>
</tr>
<tr>
<td>Timestamp</td>
<td>The timestamp of the received frame (probe response/beacon) from the found BSS</td>
<td>Yes</td>
</tr>
<tr>
<td>Local Time</td>
<td>The value of the STA’s TSF timer at the start of reception of the first octet of the timestamp field of the received frame (probe response or beacon) from the found BSS</td>
<td>Yes</td>
</tr>
<tr>
<td>PHY parameter set</td>
<td>The parameter set relevant to the PHY</td>
<td>Yes</td>
</tr>
<tr>
<td>CF parameter set</td>
<td>The parameter set for the CF periods, if found BSS supports CF mode</td>
<td>NO</td>
</tr>
<tr>
<td>IBSS parameter set</td>
<td>The parameter set for the IBSS, if found BSS is an IBSS (ATIM Window)</td>
<td>Yes</td>
</tr>
<tr>
<td>CapabilityInformation</td>
<td>The advertised capabilities of the BSS</td>
<td>Yes</td>
</tr>
<tr>
<td>BSSBasicRateSet</td>
<td>The set of data rates (in units of 500 kb/s) that must be supported by all STAs that desires to join this BSS. The STAs must be able to receive at each of the data rates listed in the set.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

*Fig 22 Table of parameters inside the BSSDescription*
3.1.2.2 Synchronization

3.1.2.2.1. MLME-JOIN.request

This primitive requests synchronization with a BSS. It is generated by the SME for a STA to establish synchronization with a BSS, it initiates a synchronization procedure once the current frame exchange sequence is complete. The MLME synchronizes its timing with the specified BSS based on the elements provided in the BSSDescription parameter.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BSSDescription</td>
<td>The BSSDescription of the BSS to join. The BSSDescription is a member of the set of descriptions that was returned as a result of a MLME-SCAN.request.</td>
</tr>
<tr>
<td>JoinFailureTimeout</td>
<td>The time limit, in units of beacon intervals, after which the join procedure will be terminated</td>
</tr>
<tr>
<td>ProbeDelay</td>
<td>Delay (in µs) to be used prior to transmitting a Probe frame during active scanning</td>
</tr>
<tr>
<td>OperationalRateSet</td>
<td>The set of data rates (in units of 500 kbit/s) that the STA may use for communication within the BSS. The STA must be able to receive at each of the data rates listed in the set. The OperationalRateSet is a superset of the BSSBasicRateSet advertised by the BSS.</td>
</tr>
</tbody>
</table>

*Fig 23 Table of parameters involve in the scan request*

3.1.2.2.2. MLME-JOIN.confirm

This primitive confirms synchronization with a BSS, it is generated by the MLME as a result of an MLME-JOIN.request to establish synchronization with a BSS.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ResultCode</td>
<td>Indicates the result of the MLME-JOIN.request: Success, invalid parameters or timeout</td>
</tr>
</tbody>
</table>

*Fig 24 Table of parameters involve in the join confirm*
3.1.2.3 Reset
This mechanism supports the process of resetting the MAC.

3.1.2.3.1.MLME-RESET.request

This primitive requests that the MAC entity be reset; it’s generated by the SME to reset the MAC to initial conditions.
The MLME-RESET.request primitive must be used prior to use of the MLME-START.request primitive.
This primitive sets the MAC to initial conditions, clearing all internal variables to the default values. MIB attributes may be reset to their implementation-dependent default values by setting the SetDefaultMIB flag to true.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>STAAddress</td>
<td>Specifies the MAC address that is to be used by the MAC entity that is being reset. This value may be used to provide a locally administered STA address.</td>
</tr>
<tr>
<td>SetDefaultMIB</td>
<td>If true, all MIB attributes are set to their default values. The default values are implementation dependent. If false, the MAC is reset, but all MIB attributes retain the values that were in place prior to the generation of the MLME-RESET.request primitive.</td>
</tr>
</tbody>
</table>

Fig 25 Table of parameters involve in the reset request

3.1.2.3.2.MLME-RESET.confirm
This primitive reports the results of a reset procedure, it’s generated by the MLME as a result of an MLME-RESET.request to reset the MAC entity, and a way to notify the SME of the results of the reset procedure.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ResultCode</td>
<td>Indicates the result of the MLME-RESET.request</td>
</tr>
</tbody>
</table>

Fig 26 Table of parameters involve in the reset.confirm

3.1.2.4 Start
This mechanism supports the process of creating a new BSS.

3.1.2.4.1.MLME-START.request
This primitive requests that the MAC entity start a new BSS, it’s generated by the SME for starting an independent BSS (with the MAC entity acting as the first STA in the IBSS).
The MLME-START.request primitive must be generated after an MLME-RESET.request primitive has been used to reset the MAC entity and before an MLME-JOIN.request primitive has been used to successfully join an existing independent BSS. The MLME-START.request primitive must not be used after successful use of the MLME-START.request primitive or successful use of the MLME-JOIN.request without generating an intervening MLME-RESET.request primitive.

This primitive initiates the BSS initialization procedure once the current frame exchange sequence is complete.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSID</td>
<td>The SSID of the BSS</td>
</tr>
<tr>
<td>BSSType</td>
<td>The type of the BSS</td>
</tr>
<tr>
<td>Beacon Period</td>
<td>The Beacon period of the BSS (in TU)</td>
</tr>
<tr>
<td>DTIM Period</td>
<td>The DTIM Period of the BSS (in beacon periods)</td>
</tr>
<tr>
<td>CF parameter set</td>
<td>The parameter set for CF periods, if the BSS supports CF mode. aCFPPeriod is modified as a side effect of the issuance of an MLME-START.request primitive.</td>
</tr>
<tr>
<td>PHY parameter set</td>
<td>The parameter set relevant to the PHY</td>
</tr>
<tr>
<td>IBSS parameter set</td>
<td>The parameter set for the IBSS, if BSS is an IBSS</td>
</tr>
<tr>
<td>ProbeDelay</td>
<td>Delay (in µs) to be used prior to transmitting a Probe frame during active scanning</td>
</tr>
<tr>
<td>CapabilityInformation</td>
<td>The capabilities to be advertised for the BSS</td>
</tr>
<tr>
<td>BSSBasicRateSet</td>
<td>The set of data rates (in units of 500 kbit/s) that must be supported by all STAs to join this BSS. The STA that is creating the BSS must be able to receive and transmit at each of the data rates listed in the set.</td>
</tr>
<tr>
<td>OperationalRateSet</td>
<td>The set of data rates (in units of 500 kbit/s) that the STA may use for communication within the BSS. The STA must be able to receive at each of the data rates listed in the set. The OperationalRateSet is a superset of the BSSBasicRateSet advertised by the the BSS.</td>
</tr>
</tbody>
</table>

*Fig 27 Table of parameters involve in the start request*
3.1.2.4.2.MLME-START.confirm

This primitive reports the results of a BSS creation procedure, it’s generated by the MLME as a result of an MLME-START.request to create a new BSS, and notified to the SME of the results of the BSS creation procedure.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ResultCode</td>
<td>Indicates the result of the MLME-START.Request: success, invalid parameters, BSS already started or joined</td>
</tr>
</tbody>
</table>

*Fig 28 Table of parameters involve in the start confirm*

3.1.3 Scanning

Before use any network, it is necessary first find the network, this process of track existing networks in the actual area is called scanning. In and ad-hoc mode, it’s looked for another station.

When the scanning process is finished, then, there are a set of information about available BSS with their corresponding parameters that we can nominate like scan report. Typically exist two different types:

- **Passive scanning**, the best issue of this type is that you are minimizing the power expended.
- **Active scanning**, the best issue of this type is that you are minimizing the time spent scanning.

*Fig 29 Example of new station situation in presence of two IBSS*
3.1.3.1 Passive scanning

The station is moving to each channel on the channel list and waits for Beacon frames. In the passive scanning procedure, the station sweeps from channel to channel, waiting for beacon frames and records information from any Beacons it receives, for no longer than a maximum duration defined by the ChannelTime parameter. Beacons are designed to allow a station to find out everything it needs to match parameters with the basic service set (BSS) and begin communications (see 2.3.1).

1. The SME send a MLME-SCAN.request primitive, a receiver STA shall perform scanning. The service set identifier SSID parameter indicates the SSID for which to scan, or if it’s a broadcast SSID, the STA shall passively scan for any Beacon frames.

2. To become a member of a particular BSS using passive scanning:

   STA shall scan for Beacon frames containing that BSS’s SSID. Returning all Beacon frames matching the desired SSID in the BSSDescriptionSet parameter of the corresponding MLME-SCAN.confirm primitive with the appropriate bits in the Capabilities Information field (beacon frame), indicating whether the beacon came from an Infrastructure BSS or IBSS.

3.a If a Station scanning result, the station begin a joining process upon received a MLME-JOIN.request.

3.b If a station scanning does not result in finding a BSS with the desired SSID and of the desired type, or does not result in finding any BSS, the STA may start an IBSS upon receipt of the MLME-START.request.

Continuation, it’s showed show you an example, with two IBSS working, and one station trying to joining to the “Red” network. The right part of the scheme represents the management side of the process that take place in the management architecture.
IEEE 802.11 MAC layer

Fig 30 Passive scanning
3.1.3.2 Active scanning

Rather than listening for that network to announce itself, an active scanning attempts to find the network on each channel.

Stations using active scanning employ the following procedure for each channel in the channel list to become a member of a particular BSS:

1. The SME send a MLME-SCAN.request primitive, a receiver STA shall perform scanning. The SSID parameter indicates the SSID for which to scan, could be a broadcast SSID.
2. Move to the channel and wait for:
   a. Either an indication of an incoming frame (PHYRxStart.indication), then the channel is in use and can be probed
   b. or for the ProbeDelay timer to expire, prevents that the entire procedure block
3. Actively scan, the STA shall send a Probe request containing the desired destination, SSID or the broadcast SSID, are used to wait for responses from a network desired. It’s necessary to gain access to the medium using the Basic access procedure
4. Clear and start a Probe timer
5. Wait for the minimum channel time, MinChannelTime, to elapse:
   a. If the medium was never busy (PHYCCA.indication), there is no network in that channel.
   b. If the medium was busy during the MinChannelTime interval, wait until the maximum time MaxChannelTime is reached, and then process all Probe Response frames. Probe Response frames are generated by networks when they hear a Probe Request that is searching for the BSS which this station belongs but scanning stations can also use a broadcast SSID, which triggers a Probe Response from all 802.11 networks in the area.
6. Clear the NAV and move to the next channel and begin a new scan
7. When all channels in the ChannelList have been scanned, completion of scanning, an MLME-SCAN.confirm is issued by the MLME indicating all of the BSS information received during the scan, with the BSSDescriptionSet.
8. To finished the procedure we have to possibilities:
   a. If a Station scanning result, the station begin a joining process upon received a MLME-JOIN.request
   b. If a Station scanning does not result in finding a BSS with the desired SSID and desired type, or does not result in finding any BSS, the STA may start an IBSS upon receipt of the MLME-START.request.
Continuation, it's showed show you an example, with two IBSS working, and one station trying to joining to the “Red” network. The right part of the scheme represents the management side of the process that take place in the management architecture.

Fig 31 Active scanning
### 3.1.3.3 More about Probe request

One station is responsible for responding to Probe Requests in each BSS. The station that transmitted the last Beacon frame remain in the awake state and shall respond to probe requests until a Beacon frame with the current BSSID is received. IBSSs pass around the responsibility of sending Beacon frames, so the station that transmits Probe Response frames varies.

It’s possible multiple Probe Responses to be transmitted as a result of a single Probe Request. The purpose of the scanning procedure is to find every basic service area that the scanning station can join, so a broadcast Probe Request results in a response from any overlapping independent BSSs may respond.

Probe Responses are unicast management frames and are therefore subject to the positive acknowledgment requirement of the MAC, with normal frame transmission rules. There may be more than one STA in an IBSS that responds to any given probe request, particularly in cases where more than one STA transmitted a Beacon frame following the most recent TBTT, either due to not receiving successfully a previous beacon or due to collisions between beacon transmissions. Example: The figure shows the relationship between the transmission of Probe frames and the various timing intervals that can be configured as part of a scan.

![Fig 32 Probe request sequence](image)

The scanning station transmits the Probe Request after gaining access to the medium. Both Stations respond with a Probe Response that reports their network's parameters. The first response is send before the minimum response time elapses, and the Station A must wait until the finish of maximum response time, if we are expecting a lot of probes response we may configure the MaxChannelTime longer.
3.1.4 Starting a BSS

A STA may start its own BSS without first scanning for a BSS to join, or in the case that no station had been scanned in the previous process.

Upon receipt of an MLME-Start.request, a STA shall determine:

- Generation of BSS’s BSSID. In IBSS, the BSSID shall be an individual locally administered IEEE MAC address Standard 802-1990, that is chosen after a random process for it.
- Select channel synchronization information.
- Select a beacon period,
- Initialize and start its TSF timer.

When all this parameters are determined, the station can begin to send beacons frames, after send a message of MLME-Start.confirm.

3.1.5 Joining process or synchronizing with a BSS

It is a purely a local process, and occurs in the station. Joining to a BSS requires that all station's MAC and PHY parameters be synchronized with the BSS that it’s chosen

Upon receipt of an MLME-Join.request, the station will join a BSS; the STA shall adopt the next parameters from BSSdescription in the request:

- BSSID
- channel synchronization information, PHY parameters
- TSF timer value
- Beacon period

After the MLME receives MLME-Join.request, there are two possibilities:

1. Upon receipt of a Beacon frame from the BSS, the MLME shall issue an MLME-Join.confirm indicating the operation was successful.
2. If the JoinFailureTimeout expires prior to the receipt of a Beacon frame from the BSS, the MLME shall issue an MLME-Join.confirm indicating the operation was unsuccessful.

Once this process is complete, the mobile station is said to have joined the BSS and is ready to begin communicating with the other stations in the BSS. For the sending of a Beacon or Probe response frames is necessary, wait for the receipt of a Beacon or probe response frame from a member of the IBSS. In IBSS the authentication is optional.
3.1.6 Timing synchronization function (TSF)

With TSF 802.11 protocol keeps the timers for all Stations in the same BSS synchronized. In an IBSS the function TSF is implemented with a distributed algorithm, all the members must participate in the Beacon generation. For this function are very important three features:

- Local TSF timer is a local timer in all the stations.
- ABeaconPeriod timing that is determinate for the station that instantiates the IBSS.
- TBTT Target beacon transmission time, is the beginning of a new beacon period, is the guideline of beacon generation.

For transmission this are the steps:

1. Every Station shall begin this process when TBBT is reached. All the traffic is suspended, only beacon and ATIM frames are allowed from this moment.

2. A backoff timer begin, with the target of transmit a beacon frame.

3. The first station that gain the backoff timer, when the random delay is finished, transmit the beacon frame, and the rest of stations cancelled the beacon transmission if a beacon is received.

In the other hand the stations that receive at beacon frame shall adopt the timestamp if the Local TSF timer is slowest (Local TSF timer is later) than the new time received.

![Fig 33 Timing synchronization function](image)
4 Access control and Coordination functions

In IEEE 802.11 protocol there are two different manners to gain access to the wireless medium:

- Distributed coordination Function is a contention based protocol that allows multiple independent stations to interact without central control. That is a Carrier-sense multiple access with collision avoidance (CSMA/CA) mechanism.
- Point coordination function (PCF), is restricted to infrastructure BSS, is a contention-free access protocol, that is to say the medium is provided without contention used a centralized access control method. It has special stations called point coordinator (PC) that reside in access points.

In this dissertation we are interested in independent BSS, and for this type of topology the standard only permit the distributed Function, the point coordination function will not explain in this paper.

Fig 34 Logical architecture of MAC layer
4.1 Distributed coordination Function and contention based access

The contention-based service allows multiple stations access to the medium without central control, in 802.11 networks is not possible to transmit and receive to the same time, that is the reason because can’t detect collisions implicitly, the collisions waste transmission capacity, due to this, 802.11 protocol try to avoid them, Carrier-sense multiple access with collision avoidance (CSMA/CA).

The main idea of how behave the DCF is a listen before talk mechanism with deferral access:
The station checks whether the medium is idle or busy before attempts to transmit.

- If the medium is busy the station defer the access to the medium, and when the medium is idle for the DIFS, begins a backoff contention window to try avoid the collisions
- If the medium has been idle for the DIFS or EIFS (the previous transmission contains an error) transmission can begin immediately.

To describe how DCF implement the CSMA/CA, it is important to describe some 802.11 key components first:

- Interframe space
- Carrier sense mechanism
- Backoff mechanism
- Acknowledgment procedure
- Request to Send & Clear to Send medium reservation
4.1.1 Interframe space

The interframe space is the time interval between frames. The four different interframes spaces provide four different priority levels for different types of frames. The amount of time is fixed and independent of the transmission speed between stations, but could be different between each physical layer kind.

![Interframes spaces](image)

**Fig 36 Interframes spaces**

4.1.1.1 Short interframe space (SIFS)

The SIFS gives the highest priority to the next frames, and procure a mechanic to perform the frame exchange sequence, when a station have seized the medium and need to continued with it.

- ACK frame
- CTS frame
- The second or subsequent MSDU of a fragment burst

These frames can begin once the SIFS has elapsed, and the medium becomes busy again.

4.1.1.2 PCF interframe space (PIFS)

This interframe space is used by the PCF during contention-free operation, in Independent BSS is not used. This interval gives to PCF based stations a higher priority than DCF based stations for transmitting frames.

4.1.1.3 DCF interframe space (DIFS)

The stations shall have immediate access to the medium after it has been free longer than the DIFS that is the minimum medium idle for contention based services, the next type of frames use it:

- data frames (MPDUs)
- management frames (MMPDUs)

4.1.1.4 Extended interframe space (EIFS)

The EIFS is used by the DCF when ever the PHY layer has indicated to the MAC that there is an error in the transmission of a complete MAC frame with a incorrect FCS value. The receiving station has enough time to send an ACK frame to communicate free-error transmission and then continue with normal DFC function.
4.1.2 Carrier-sense mechanism

There are two different mechanisms to determinate the state of the medium, this is essential for CSMA/CA, because provide sufficient information for the Mac to decide the status of the channel.

- **Physical carrier-sense mechanism**, it’s provided by the Physical layer, check the channel, and see whether a carrier is present, by analyzing all detected packets or detects activity by the signal strength from other stations. The physical layer sends to the Mac coordination the result of the physical channel assessment.

- **Virtual carrier-sense mechanism**. It’s provided by the Mac. It’s based on reservation the medium with the information of the duration field that every frame has it. In the duration field you can find the time that frame is holding the channel.

In every station there is a timer that indicates the amount of time the medium will be reserved, this timer is called network allocation vector (NAV), every station shall update their NAV, when receive a valid frame, with the information of the duration field of this frame, the algorithm is very simple, the NAV is update if the received value is greater and the frame is not addressed to this station.

Once the NAV reaches zero, the medium is idle, the station can begin with the backoff process, when NAV isn’t zero the carrier sense indicate that the medium is busy.

![Fig 37 Virtual carrier-sense diagram](image-url)
4.1.3 Backoff procedure

Random backoff period is an additional deferred time before transmit, that minimizes collisions during contention process between multiple stations that try to gain the medium. This process minimizes collisions during contention between multiple Stations that have been deferring to the same event. It’s a mechanism to manage congestion, due the number of nodes could attempt to transmit at the same moment are changing with time, to deal this situation the DCF dynamically adjust the contention window.

4.1.3.1 Contention window CW parameter

It is an integer between aCWmin and aCWmax, these values are PHY characteristics in the MIB and the CW shall take an initial value of aCWmin and shall be sequentially ascending integer of two, minus one, until achieve the aCWmax. The exponentially increment maintains stable the access protocol procures minimum collisions and maximize the throughput under high-load conditions.

![Contestion window](Fig 38 Contention window)

The CW take next value in the sequence every time an unsuccessful attempt to transmit and MPDU, increase either station retry counter, when the CW reaches aCWmax value, the CW must remain it until will be reset. The CW shall be reset to aCWmin after every successful attempt to transmit an MPDU, or when any of the retry counters (SLRC, SSRC) reaches theirs limits LongRetryLimit, or ShortRetryLimit, and the frame is discarded.
4.1.3.1.1 Station short retry count (SSRC)

This counter is local to every station and is incrementing when a short frame transmission fails and there is a retransmission. The station begins with this counter if the frame that is transmitting is shorter than the RTS threshold.

The short retry counter is reset to zero whenever:
- A CTS frame is received in response to an RTS frame.
- A Mac ACK frame is received in response to an MPDU transmission.
- A broadcast or multicast is transmitted.

The maximum number of short frames retransmission is set by ShortRetryLimit, the default value is seven.

4.1.3.1.2 Station long retry count (SLRC)

This counter is local to every station and is incrementing when a long frame transmission fails and there is a retransmission. The station begins with this counter if the frame that is transmitting is longer than the RTS threshold.

The long retry counter is reset to zero whenever:
- A Mac ACK frame is received in response to transmission of an MPDU of length greater than RTS Threshold,
- A broadcast or multicast is transmitted.

The maximum number of long frames retransmission is set by LongRetryLimit, the default value is four.

4.1.3.2 Backoff interval time

It is generated by a random process in the station using the following formula:

\[ \text{Backoff Time} = \text{Random ( )} \times \text{aSlotTime} \]

- Random: is a pseudorandom integer drawn from a uniform distribution over the interval [0, CW]
- aSlotTime is a constant parameter of each physical layer

In every station there is a local Backoff timer that is updated to the backoff time if it contains zero value, in other way maintain the value of the count in progress.
4.1.3.3 Operating of backoff procedure

Backoff procedure is invoke for a station that try to send a frame when the carrier-sense mechanism indicates that the medium is busy or when the transmitting station inquire that the last transmission is wrong, after wait this station that the medium was idle for DIFS or EIFS period depends which of the two situations will be.

When the backoff procedure begins the station must set its backoff timer to random backoff time. Then in each backoff slot shall use the carrier sense mechanism to know whether there is any activity in the medium:

- If the medium is without activity in that slot the backoff timer can decrement one slot time.
- If the medium is busy the procedure is suspended for the time being. And the backoff procedure begin after the medium would be determined idle for the space of DIFS or EIFS period and the backoff timer continues count down from the remained slot.

When the backoff timer reaches zero the transmission of the frame is possible for the station that wins the contention. After a successful transmission from a station, this station needs to calculate again a new CW, which assures that frames from a station are always separated by at least one backoff interval.

In the next figure is shown the procedure.

Fig 39 Backoff procedure
4.1.4 ACK procedure

In 802.11 wireless networks the radio link quality is one of the subject matters that this protocol has to face, because the frequencies used are localized in unlicensed ISM bands, the noise and interferences are present in this environment, unlike other Mac protocols it’s not assumed that the destination receives the frame correctly. Furthermore multipath fading may also lead to situations where a node is in a dead spot and the frames cannot be transmitted. In contrast to other protocols of link layer, 802.11 own positive acknowledge.

The sender begin the transmission of the data frame, the receiver of the data frame, respond with a acknowledge after a SIFS period out of normal contention mechanism that regard to the busy/idle state of the medium if the FCS of the received frame is correct.

The Sender will consider lost the data frame if after wait an ACK timeout doesn’t receive any ACK frame from the destination and the data frame must be retransmitted for the scenario of wireless protocol a collision has occurred. The failure could occur in the data frame transmission or in the ACK frame transmission; this protocol can not distinguish between them.
4.1.5 Error recovery mechanisms:

During a transmission could occur a lot of different errors, interference, collisions, and bit errors in the frames. Because of that the Mac must perform error recovery Mechanisms. The 802.11 provides reliability with retransmission.

The station that begins a sequence frame exchange must detect and correct any error in the transmission. It’s important, that we realize that the retransmission is of the complete sequence, and if the whole sequence is not completed with successful it will be retransmission.

When an error is detected, this station must retransmit the frame, the retry counters are incremented when frames are retransmitted, for example when the station was waiting the acknowledge from the destination station, after a period of time if there is no response, it will begin the recovery mechanisms because the sequence transmission has failed. Every Failed transmission increment the retry counter of the frame (or fragment). If the retry limit is reached, the frame is discarded, and its loss is reported to higher-layer protocols. This mechanism is an Automatic repeat-request (ARQ).

In addition to the associated retry count, the MAC gives lifetime to the fragments of a LLC frame. When the burst of fragments begins the lifetime is started, and when this counter reaches its limit and the last fragment hasn’t arrived the frame is discarded.

The higher-layer protocols can detect any loss and retransmit the data, separately of the 802.11 MAC; for example when a higher-level protocol such as LCC retransmits data, the frame would be a new frame to the 802.11 MAC with all the retry counters set at the starting position.

4.1.6 RTS/CTS clearing technique

4.1.6.1 The Hidden Node Problem

Let us suppose stations C and B can not hear each other and station A is in the transmission range of stations C and B, the lines around the stations in the figure represent the coverage radio of the stations.

- Each node may not be able to directly communicate with every other node in the wireless network; C can’t communicate directly with B, because obstacles or signal attenuation. In this case node B is hidden node for C.

- If station C is transmitting to A and B has a frame to be transmitted to A, in accordance with DCF, it senses the medium, like is not able to hear B’s frames the medium appear free, and C station begin the transmission and the collision occur in A.
• Only the received station A can detect the collision, is impossible to detect the collision for B and C, stations B and C hasn’t any notice of the error. The collision is local to A.

This problem exist when two stations are too far away one from the other (out of range) that they are not able to detect a collision. Because the wireless transceivers are half-duplex the collisions resulting from hidden nodes are hard to detect. In small 802.11 networks, hidden problem is not a great problem because there is very little risk of simultaneous transmission, and there is enough frame space for retry the frame transmission without a important decrease of efficiency.

**RTS/CTS clearing technique**

The CTS/RTS clearing technique reduce the possibility of collisions, reserving the radio link for transmission and clear out the area because it silences any station that hear the RTS or the CTS. This procedure adds latency before the transmission of the data frame, use capacity of the network. Then it’s used in high capacity networks.

1. Station C has a frame to send.
2. Station C sends a RTS frame. Every station in the coverage of station C are silence, and the radio link is reserving for transmission.
3. The station A receives the RTS and send a CTS, with this CTS hidden nodes for the C station are silence, because every station in the range of A can hear the CTS to C.
4. Station C receives the CTS and the RTS/CTS exchange sequence is complete and it can transmit without interference from a hidden node.

If RTS/CTS technique is used every frame must use the positive acknowledge procedure.
4.1.6.2 The exposed station problem

Let us suppose stations C and B can hear the transmissions from A, and the station C can not hear transmissions from B.
In this situation when station A transmit to C, if station B wants to send a frame , it use DCF and sense the medium, it will hear the transmission A-C , the medium appear like seized, wherewith B may not send to station D, although would not cause a collision in station C. The interference is only local between B and A.
This problem causes degradation in throughput, because Station B is waiting without necessity.A node can identify itself as an exposed node if it hears an RTS frame but not a CTS frame from the other transmitting node in this case from station C. Therefore, it concludes that it can have a simultaneous transmission.
4.1.7 Fragmentation

The fragmentation in the MAC layer consist in the partition of MAC service data unit MSDU from the LLC or management protocol data unit MMPDU from MLME, into smaller frames, that are converting in Mac protocol data units MPDU. It’s achieved two targets:

- Fit the packets from higher layers to the wireless medium
- Increase the reliability in the presence of interference, because with smaller frames the probability of successful transmission in a noise environment, the effective throughput increase, but increase the overhead under good channel conditions.

The defragmentation is the opposite case, is the process of recombining and reassembly MPDUs into MSDU or MMPDU.

The fragmentation is only possible for unicast frames, and it’s allowed for broadcast and multicast frames. The sequence number is the same in all the fragments, and the fragment number is ascending to aid in the defragmentation. And with the more fragments bit in the frame control is indicated whether more fragments exists.

The limit of sized for a frame to be divided or not is the fragmentation threshold, if the higher-level packet or SDU is longer than the fragmentation threshold it shall be divides in smaller fragments. It’s habitual that this fragmentation threshold coincide with the RTS threshold, in this case fragmentation and RTS/CTS procedure occur in the same sequence. Each fragment has independent acknowledge, if there is a collision the process is halt by the source and this station must compete for the medium again, if no problems happen the transmission ends. The transmission of all the SDU behaves like a burst.
The fragmentation in higher layers has the disadvantage of reassembly occur in the final destination, if one of the fragments is lost the whole packet must be retransmitted. With the use of Mac fragmentation we solve this issue. With short frames we achieve that the probability of radio interference from high energy burst decrease.

Fig 45 Fragmentation exchange
4.1.8 Sequence of frames by the DCF for contention-based service

In the next section, it’s indicated the sequences that we can find within a IBSS, coordinated by the DCF, this sequences behave like a atomic exchanges, they are a single unit, it’s a technique of "all or nothing", that move the data on a 802.11 network. Either every step in the sequence will complete successfully, or the whole operation is considered a failure. These sequences are considered a single indivisible operation. IEEE 802.11 achieve the transmission of the sequence are not interrupted by other stations intent to take the medium for transmission, due to allow stations to lock out contention during the complete sequence. The next exchanges begins after a DIFS, when the station seize the medium.

4.1.8.1 Group Frames

The group frames are destined for more than one station, they have a broadcast or multicast addresses in the address 1 field, in the environment of IEEE 802.11 they are:

- Broadcast management frames (probe request, beacon and IBSS ATIM frames).
- Broadcast data
- Multicast data

The frame exchange is a single-frame sequence, because there is not acknowledgement, and can not be fragmented. This single sequence is sent according to the rules of the contention-based access control. Because there is not ACK it could occur that some broadcast of multicast traffic would miss, and the 802.11 MAC hasn’t a mechanism to Retransmitting this traffic, thus the service quality it could be very low. These frames don’t use virtual carrier sense to lock the medium because the sequence is a single-frame exchange.

4.1.8.2 Individual or Unicast Frames

Unicast frames are destined for a single receiving station and to ensure reliability, must be acknowledged.

- Positive acknowledgment
- Fragmentation
- RTS/CTS
- RTS/CTS with fragmentation

All the sequences in this section apply to any unicast frame and thus can apply to management frames and data frames, are called directed data by the 802.11 standard.
4.1.8.2.1. Positive acknowledgment

This is the most simple case, the transmission of a unicast data frame between two stations, like was told, the reliable that the Mac provide, is through an acknowledge Frame, if the ack isn’t receives by the transmitter is assumed to be lost.
The next figure shows this sequence, that it’s like a unit for the transmission procedure.

The medium is reserved with the NAV by the sender with the virtual carrier mechanism after send the unicast data frame and the complete sequence can happen with guarantee that the receiver can send the acknowledge, without the intromission of other station.

![Fig 46 ACK sequence](image)

4.1.8.2.2. RTS/CTS

The RTS/CTS exchange sequence is showed in the next figure. With the RTC and CTS frames and theirs respective NAV the medium is guarantee reserved for data transmission. With the RTS threshold is possible to control the size for a frame use this sequence, if it’s smaller the frame will use the positive ack sequence, and in the other case will use the RTS/CTS sequence.

![Fig 47 RTS/CTS sequence](image)
4.1.8.2.3. Fragmentation

The transmission of all the fragments of a LLC frame is considered an atomic sequence. In the More Fragments field of the MAC frame indicates with 1 that it’s a fragment.

The sequence consists in each data fragment from the sender frame continued after a SIFS by an Acknowledge of the receiver and a SIFS before the next fragment. The virtual sense mechanism is present in this sequence; the last fragment (with a 0 in the More fragments field) is exchanged like the previous sequence the positive acknowledge. The rest of the fragments (with a 1 in the More fragments field), from the first until the last, lock the medium for the next frame, so these fragment set the NAV for a long enough period to accommodate its ACK, the next fragment and its correspondent acknowledge.

In the other hand, all nonfinal ACKs extend the lock for the next data fragment and its correspondent ACK.

The level of fragmentation is controlled by the fragmentation threshold parameter in the MAC, which means any frame larger than this threshold is fragmented. The place that takes the fragmentation threshold is a compromise situation:

If the fragmentation threshold is high the traffic of the information would be with low overhead, but delicate against the cost to a damaged or a lost frame.

If the fragmentation threshold is low there will increase the overhead, but in the other hand the MAC procedure is robustness to bad conditions of the medium and the cost to a retransmission is lower.

---

**Fig 48 Fragmentation sequence**
4.1.8.2.4. RTS/CTS with fragmentation

The last sequence is RTS/CTS combined with fragmentation, the RTS/CTS contribute to the sequence guarantee the access to the medium, free from contention from hidden nodes.

![Diagram of RTS/CTS with fragmentation sequence.](image-url)

*Fig 49 RTS/CTS with fragmentation sequence.*
5 Comparison with standard IEEE 802.16

In this chapter two different comparisons are present. The first one is an introduction to the technology of these features, and makes the reader notices the general features of each one. This aspect is important to obtain a global idea in order to provide enough knowledge in case of treating a wireless networks planning. The second one is the produce of the previous Mac layer research; work out in the anterior chapters in the case of standard 802.11, and for standard 802.16 in the paper of Pedro Francisco Robles Rico with are named like “Research of IEEE standard 802.16 MAC layer in Distributed Mesh Networks and comparison with IEEE 802.11 ad hoc networks”.
5.1 General features

In the next table it is shown a comparison between standards 802.11 and standard 802.16 in general different aspects.

<table>
<thead>
<tr>
<th>Standard</th>
<th>802.11</th>
<th>802.16</th>
</tr>
</thead>
<tbody>
<tr>
<td>Max distance coverage</td>
<td>Optimized for 100 m</td>
<td>Optimized for 7 – 10 km</td>
</tr>
<tr>
<td>Channel bandwidth</td>
<td>22 MHz</td>
<td>10, 20 MHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3,5,7,14 MHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3,6 MHz</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The channel bandwidth can be chosen by the operator</td>
</tr>
<tr>
<td>Frequency band</td>
<td>Unlicensed bands</td>
<td>Licensed bands</td>
</tr>
<tr>
<td></td>
<td>- 2.4-2.5 GHz</td>
<td>- 10-66 GHz</td>
</tr>
<tr>
<td></td>
<td>- 5.725 5.875 GHz</td>
<td>Unlicensed bands</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Below 11 GHz</td>
</tr>
<tr>
<td>Max data rate</td>
<td>1 Mbps, 11 Mbps, 54 Mbps</td>
<td>75 Mbps, 100 Mbps, 134 Mbps</td>
</tr>
<tr>
<td></td>
<td>Efficiency 2,7 bps/ Hz</td>
<td>Efficiency 5 bps/ Hz</td>
</tr>
<tr>
<td>Physical technology</td>
<td>DSSS</td>
<td>SC</td>
</tr>
<tr>
<td></td>
<td>FHSS</td>
<td>SCa</td>
</tr>
<tr>
<td></td>
<td>OFDM</td>
<td>OFDM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OFDMA</td>
</tr>
<tr>
<td>QoS</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Users</td>
<td>Supports 10’s of users</td>
<td>Supports thousands of users</td>
</tr>
<tr>
<td>Line of sight</td>
<td>Optimized for indoor non-line-of-sight (NLOS)</td>
<td>Optimized for outdoor NLOS</td>
</tr>
<tr>
<td>Topology</td>
<td>In the future mesh networks shall be supported</td>
<td>Support mesh network topology</td>
</tr>
</tbody>
</table>

Fig 50 Table of general comparison parameters of the two standard
5.2 MAC layer of the two standards

If we watch the upper layer of the 802.11 MAC, immediately is found the LLC sublayer (see 1.2), that characteristic makes 802.11 protocol seems to networks layers like a network based in Ethernet, this feature relieves complexity to network layer protocols, and make a perfect insertion in the previous protocol architecture. Like was explaining the introduction the LLC provide an extra reliable functions to 802.11, with their three different services, and ARQ mechanism.

In the other hand the standard 802.16 MAC treats directly with upper network layers, for solving this situation the 802.16 introduce a sublayer, Service-Specific Convergence sublayer (CS)(see ), that provides any transformation or mapping of external network data. As consequence the MAC layer is composed by three different sublayers. The main sublayer is the MAC common Part Sublayer which is connected with the CS through the MAC SAP. The third sublayer, Security Sublayer, is located below the MAC common Part Sublayer and it is a small sublayer. It is not necessary a SAP between them. Below the Security Sublayer, or if it is preferred, below the MAC layer it is found the Physical Layer, both Layers are connected through the PHY SAP.

Below the 802.11 MAC layer (see 1.4) there may be different physical layers, for making understandable the MAC with different transmission techniques, it is introduced a convergence sublayer only with the objective of comprehension.

In the previous overview it was repassed the layers around the 802.11 MAC layer and the 802.16 MAC common Part Sublayer, with this glance, the proper Mac layer of the two standards were located in the stack of protocols involved in wireless communications. For finishing with the comparison it is going to insert within the own mechanisms of this layer. The main aspects of these MAC layers are as follows.

5.2.1 Topologies

In the standard 802.16 are distinguished two different topologies; PMP and Mesh mode although for the research only Mesh mode has been studied. This Mesh mode is composed by Stations with the same importance. Only the station connected to the backhaul services outside the Mesh network is defined different, it is termed Mesh Base Station. All the Station included the Mesh BS can transmit each other. The point of interest of Mesh mode has been the Distributed Scheduling since it was seek a manner to manage the Network without a central or manager node, been a more flexible configuration if one node is moving out.

In the standard 802.11 the configuration that make good with this requirement is the Independent Basic Service Set topology, the great disadvantages with 802.16 is that 802.11 protocol is not allowed more than one hop, if the stations has not direct sight, there aren’t a routing protocol that saves this situation, therefore the communication will not possible between this stations.
5.2.2 Initiation and Synchronization

The initiation and synchronization of the ad hoc 802.11 network or the greeting to the new station is a process that it is resumed in four steps; scanning for BSSs, initiating BSSs, joining to an IBSS and timing synchronization. In contrast the process of initialization in Mesh mode is fairly complex. While the new node is receiving different packets from the network, it must construct the physical neighbor list. In addition the new node has to ask a regular node to be its Sponsor node, this supposes that the new node must process a large amount of information. In both cases, during the initialization, the node must acquire synchronization with the others in order to know about the other transmissions.

5.2.3 Channel separation

In the 802.11 control and management frames and the data frames share the same channel, they compete for the use of the channel. Unlike 802.11, the control and data channel are separated in the standard 802.16. The Mesh frame is divided into two subframes: Control subframe and Data subframe. This separation of the subframes is realized in order to provide coordination to the Network.

5.2.4 Overall transmission scheme

In the standard 802.11 the stations use a “listen before send” mechanism. At the same time in order to decrease the possibility of beginning the transmission at the same time two stations use a backoff procedure, that introduces some dead times in the use of the medium. This derives in a disadvantage. On the other hand the IEEE 802.16 is a slotted system where all the transmission must be synchronized, that supposes the station does not require to sense the channel since it has assigned some slots for transmitting. With these restrictions the transmission of control messages are scheduled in a collision free manner.

5.2.5 Collision avoidance

The standard 802.11 implement a medium access technique to avoid the collisions, CSMA/CA, with the introduction of two control frames RTS/CTS in the basic sequence of transmission achieves reduce the collisions that the known hidden problem cause.

As it has been mentioned in the previous point, the standard 802.16 avoids the collisions by using a slotted frame. At the same time Distributed Scheduling uses a three-way handshaking to set up connection before data. As well as the standard 802.11 with the introduction of medium access technique to avoid the collisions, CSMA/CA, with two control frames RTS/CTS in the basic sequence of transmission achieves reduce the collisions that the known hidden problem cause. The difference between both mechanisms may be that in standard 802.16 the aim is avoiding the collision and in standard 802.11 it is enough with reducing the collisions.
5.2.6 Competing for data transmission

Another major difference is that in standard 802.16 multiple slots are reserved by the node for exchanging control messages. However, each node in their eligible transmission opportunity must compete with others eligible competing nodes for transmitting their corresponding packets. The winner node is chosen by using the Distributed election Algorithm. Whereas in 802.11 each node must compete for the channel for every packet and among all of them.

5.2.7 Construction of MAC PDUs

This is one of the most important features of the MAC layer. In the construction of MAC PDUs it can be seen how efficiency is the use of the offered capacity for payload. Both standards 802.11 and 802.16 are similar in the aspect that both use fragmentation and CRC with the difference that Mesh mode requires fragmentation subheaders when fragmentation is presented. However, the main difference is that standard 802.16 may use packing. By using packing the PDU can be used in a better manner in the case of receiving from upper layers a SDU small enough to insert more than one in the same PDU. In the standard 802.11 the fragmentation serve to the propose of fit the packets to the size of the physical layer frames, furthermore increase the transmit reliability in the presence of interference.

5.2.8 Error recovery mechanism

The 802.11 MAC layer provides an error recovery mechanism with retransmission procedure, it is an automatic repeat-request (ARQ). This is implemented with the support of ACK responses from the receiver. Furthermore a lifetime is assigned to the fragments, after this period the frames will be discard. In the standard 802.16 the implementation of ARQ mechanism is optional. But when it is implemented it provides a complete ARQ mechanism. It uses sliding window and as in the case of 802.11 a lifetime is assigned to the fragments.
IEEE 802.11 MAC layer

The next table treat to resume the most important ideas of the two MAC layers, that was explain a long this paper.

<table>
<thead>
<tr>
<th>Standard</th>
<th>802.11 ad hoc mode</th>
<th>802.16 mesh mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topologies</td>
<td>Ad hoc. Only with one hop</td>
<td>Mesh Multiple hops</td>
</tr>
<tr>
<td>Initiation and Synchronization</td>
<td>Four steps, With storage of local information</td>
<td>Complex, with storage of neighbour information</td>
</tr>
<tr>
<td>Channel separation</td>
<td>Not separated between control and data channel</td>
<td>Control and data channel are separated (contention in control channel does not affect the current data transmission)</td>
</tr>
<tr>
<td>Overall transmission scheme</td>
<td>Sensing the channel before transmission</td>
<td>TDD Slotted system (All nodes are synchronized)</td>
</tr>
<tr>
<td>Collision avoidance</td>
<td>Physical carrier sensing or RTS/CTS/DATA/ACK exchange</td>
<td>Request/Grant/Confirm message exchange</td>
</tr>
<tr>
<td>Competing for data transmission</td>
<td>Competing for every data packet</td>
<td>Reservation of multiple slots without additional control message exchange</td>
</tr>
<tr>
<td>Construction Of MAC PDUs</td>
<td>Fragmentation CRC</td>
<td>Fragmentation CRC Packing</td>
</tr>
<tr>
<td>Error recovery mechanism</td>
<td>ACK Fragments lifetime</td>
<td>ARQ mechanism is optional</td>
</tr>
</tbody>
</table>

Fig 51 Table of MAC layer comparison parameters between the two standard
6 Conclusions and future work

6.1 Conclusions

The objective at begin of this investigation was to search for information of all the mechanism that 802.11 Mac provide in at ad hoc configuration. It was dedicated special attention to the start process of a new station in independent BSS mode, it was describe every frame that is transmitted over the medium, the positive aspect is the lack of a central station or coordinator, that provides a great independent and flexibility, the deficit of multi hop is the biggest deficiency of the network configuration, other weak aspect is the lack of storage information about other stations information.

The second great issue that treats the MAC layer is the way to access the medium, and solve the problems that carry a shared and unlicensed medium, the 802.11 ca not detect collision, for solve this treat to avoid the maximum number of collision with a CSMA/AC protocol that is the core of the MAC. It fits perfectly in an Ethernet type network, it reduces the number of changes necessary in this networks. The control information that introduces the MAC layer could be reduced adjust the threshold parameter, the same that the fragmentation level of the network.

6.2 Open issues and future work

After this study several issues could be investigated in the future, there are two challenges that could changes the MAC structure, the first is try to study the advantages of separate the control information in a different channel from the data channel, it could label single channel against multiple channels. The other would be to introduce a architecture that allow the existence of multiple channels, that distinguish like the big opportunity for a real useful of ad hoc networks.

Other issue could be the study of fairness schemes, in situation of competition among stations, trying to improve the fairness of the actual MAC layer contention layer.

Immediately finished the theoretic study of this networks, it would be very useful implement a ad hoc simulation model.

The last issue in all study is performance measurements in a real situation that give a appreciation of the possibilities of this protocol in live test.
In connection with this paper there are two IEEE task that are working in the development of two new standards that improves some of the topic that was told along the antecedent chapters and could be interesting:

- Task Group S and the proximate standard “IEEE 802.11s Extended Service Set Mesh networking”, it’s supposed to be ready for the early 2007, and will contribute with a mesh networking extension, and it will facilitate the possibility of multi-hop 802.11 networks, auto configuration features and auto-discovery of every station.

- Task Group N will publish a new standard with the next designation 802.11n, and is known like MIMO PHY (multiple-input/multiple-output) or the High-Throughput PHY 802.11 standard. This new standard will not change the MAC layer on his core, it will focus on the physical layer, with the introduction of new techniques like simultaneous receiver processing, and breaking up the single frames and multiplexed across multiple spatial streams, with the consequential reassembled at the receiver. It’s going to be compatible with the original standard, with the coexistence of other wireless networks.

Other organization the Internet Engineering Task Force IETF in his investigation area of Mobile ad hoc networks (MANET) is studying the development of dynamic routing protocols that can efficiently look for intermediate stations in the communication between two stations members of an ad hoc networks.
### 7 Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACK</td>
<td>acknowledgment</td>
</tr>
<tr>
<td>AP</td>
<td>access point</td>
</tr>
<tr>
<td>ARQ</td>
<td>automatic repeat request</td>
</tr>
<tr>
<td>ATIM</td>
<td>announcement traffic indication message</td>
</tr>
<tr>
<td>BSA</td>
<td>basic service area</td>
</tr>
<tr>
<td>BSS</td>
<td>basic service set</td>
</tr>
<tr>
<td>BSSID</td>
<td>basic service set identification</td>
</tr>
<tr>
<td>CCA</td>
<td>clear channel assessment</td>
</tr>
<tr>
<td>CDMA</td>
<td>code division multiple access</td>
</tr>
<tr>
<td>CF</td>
<td>contention free</td>
</tr>
<tr>
<td>CFP</td>
<td>contention-free period</td>
</tr>
<tr>
<td>CP</td>
<td>contention period</td>
</tr>
<tr>
<td>CRC</td>
<td>cyclic redundancy code</td>
</tr>
<tr>
<td>CS</td>
<td>carrier sense</td>
</tr>
<tr>
<td>CSMA/CA</td>
<td>carrier-sense multiple access with collision avoidance</td>
</tr>
<tr>
<td>CTS</td>
<td>clear to send</td>
</tr>
<tr>
<td>CW</td>
<td>contention window</td>
</tr>
<tr>
<td>DA</td>
<td>destination address</td>
</tr>
<tr>
<td>DCF</td>
<td>distributed coordination function</td>
</tr>
<tr>
<td>DIFS</td>
<td>distributed (coordination function) interframe space</td>
</tr>
<tr>
<td>DLL</td>
<td>data link layer</td>
</tr>
<tr>
<td>DS</td>
<td>distribution system</td>
</tr>
<tr>
<td>DSAP</td>
<td>destination service access point</td>
</tr>
<tr>
<td>DSS</td>
<td>distribution system service</td>
</tr>
<tr>
<td>DSSS</td>
<td>direct sequence spread spectrum</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>DTIM</td>
<td>delivery traffic indication message</td>
</tr>
<tr>
<td>EIFS</td>
<td>extended interframe space</td>
</tr>
<tr>
<td>ERP</td>
<td>extended rate physical</td>
</tr>
<tr>
<td>ERS</td>
<td>extended rate set</td>
</tr>
<tr>
<td>ESA</td>
<td>extended service area</td>
</tr>
<tr>
<td>ESS</td>
<td>extended service set</td>
</tr>
<tr>
<td>FC</td>
<td>frame control</td>
</tr>
<tr>
<td>FCS</td>
<td>frame check sequence</td>
</tr>
<tr>
<td>FH</td>
<td>frequency hopping</td>
</tr>
<tr>
<td>FHSS</td>
<td>frequency-hopping spread spectrum</td>
</tr>
<tr>
<td>IBSS</td>
<td>independent basic service set</td>
</tr>
<tr>
<td>IDU</td>
<td>interface data unit</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet engineering task force</td>
</tr>
<tr>
<td>IFS</td>
<td>interframe space</td>
</tr>
<tr>
<td>IR</td>
<td>infrared</td>
</tr>
<tr>
<td>ISM</td>
<td>industrial, scientific, and medical</td>
</tr>
<tr>
<td>IV</td>
<td>initialization vector</td>
</tr>
<tr>
<td>LAN</td>
<td>local area network</td>
</tr>
<tr>
<td>LLC</td>
<td>logical link control</td>
</tr>
<tr>
<td>LME</td>
<td>layer management entity</td>
</tr>
<tr>
<td>LRC</td>
<td>long retry count</td>
</tr>
<tr>
<td>MAC</td>
<td>medium access control</td>
</tr>
<tr>
<td>MANET</td>
<td>mobile ad-hoc networks</td>
</tr>
<tr>
<td>MIB</td>
<td>management information base</td>
</tr>
<tr>
<td>MLME</td>
<td>MAC sublayer management entity</td>
</tr>
<tr>
<td>MMPDU</td>
<td>MAC management protocol data unit</td>
</tr>
<tr>
<td>MPDU</td>
<td>protocol data unit</td>
</tr>
<tr>
<td>MSDU</td>
<td>service data unit</td>
</tr>
<tr>
<td>N/A</td>
<td>not applicable</td>
</tr>
<tr>
<td>NAV</td>
<td>network allocation vector</td>
</tr>
<tr>
<td>PC</td>
<td>point coordinator</td>
</tr>
<tr>
<td>PCF</td>
<td>point coordination function</td>
</tr>
<tr>
<td>PDU</td>
<td>protocol data unit</td>
</tr>
<tr>
<td>PHY</td>
<td>physical (layer)</td>
</tr>
<tr>
<td>PHY-SAP</td>
<td>physical layer service access point</td>
</tr>
<tr>
<td>PIFS</td>
<td>point (coordination function) interframe space</td>
</tr>
<tr>
<td>PLCP</td>
<td>physical layer convergence protocol</td>
</tr>
<tr>
<td>PLME</td>
<td>physical layer management entity</td>
</tr>
<tr>
<td>PMD</td>
<td>physical medium dependent</td>
</tr>
<tr>
<td>PMD-SAP</td>
<td>physical medium dependent service access point</td>
</tr>
<tr>
<td>PPDU</td>
<td>protocol data unit</td>
</tr>
<tr>
<td>PS</td>
<td>power save (mode)</td>
</tr>
<tr>
<td>RA</td>
<td>receiver address</td>
</tr>
<tr>
<td>RF</td>
<td>radio frequency</td>
</tr>
<tr>
<td>RTS</td>
<td>request to send</td>
</tr>
<tr>
<td>RX</td>
<td>receive or receiver</td>
</tr>
<tr>
<td>SA</td>
<td>source address</td>
</tr>
<tr>
<td>SAP</td>
<td>service access point</td>
</tr>
<tr>
<td>SDU</td>
<td>service data unit</td>
</tr>
<tr>
<td>SIFS</td>
<td>short interframe space</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Full Form</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------</td>
</tr>
<tr>
<td>SLRC</td>
<td>station long retry count</td>
</tr>
<tr>
<td>SME</td>
<td>station management entity</td>
</tr>
<tr>
<td>SMT</td>
<td>station management</td>
</tr>
<tr>
<td>SRC</td>
<td>short retry count</td>
</tr>
<tr>
<td>SS</td>
<td>station service</td>
</tr>
<tr>
<td>SSAP</td>
<td>source service access point</td>
</tr>
<tr>
<td>SSID</td>
<td>service set identifier</td>
</tr>
<tr>
<td>SSRC</td>
<td>station short retry count</td>
</tr>
<tr>
<td>STA</td>
<td>station</td>
</tr>
<tr>
<td>TA</td>
<td>transmitter address</td>
</tr>
<tr>
<td>TBTT</td>
<td>target beacon transmission time</td>
</tr>
<tr>
<td>TIM</td>
<td>traffic indication map</td>
</tr>
<tr>
<td>TSF</td>
<td>timing synchronization function</td>
</tr>
<tr>
<td>TU</td>
<td>time unit</td>
</tr>
<tr>
<td>TX</td>
<td>transmit or transmitter</td>
</tr>
<tr>
<td>WAN</td>
<td>wide area network</td>
</tr>
<tr>
<td>WDM</td>
<td>wireless distribution media</td>
</tr>
<tr>
<td>WDS</td>
<td>wireless distribution system</td>
</tr>
<tr>
<td>WEP</td>
<td>wired equivalent privacy</td>
</tr>
<tr>
<td>WIMAX</td>
<td>worldwide Interoperability for Microwave Access</td>
</tr>
<tr>
<td>WLAN</td>
<td>wireless Local Area Network</td>
</tr>
<tr>
<td>WM</td>
<td>wireless medium</td>
</tr>
</tbody>
</table>
8 References


http://www.ieee802.org/11/
http://www.wi-fi.org/
www.efis.dk European frequency information system
www.ero.dk European radiocommunications office
www.eto.dk European telecommunications office
Detta dokument hålls tillgängligt på Internet – eller dess framtida ersättare – under en längre tid från publiceringsdatum under förutsättning att inga extraordinära omständigheter uppstår.

Tillgång till dokumentet innebär tillstånd för var och en att läsa, ladda ner, skriva ut enstaka kopior för enskilt bruk och att använda det oförändrat för ickekommersiell forskning och för undervisning. Överföring av upphovsrätten vid en senare tidpunkt kan inte upphäva detta tillstånd. All annan användning av dokumentet kräver upphovsmannens medgivande. För att garantera äktheten, säkerheten och tillgängligheten finns det lösningar av teknisk och administrativ art. Upphovsmannens ideella rätt innefattar rätt att bli nämnd som upphovsman i den omfattning som god sed kräver vid användning av dokumentet på ovan beskrivna sätt samt skydd mot att dokumentet ändras eller presenteras i sådan form eller i sådant sammanhang som är kränkande för upphovsmannens litterära eller konstnärliga anseende eller egenart.

För ytterligare information om Linköping University Electronic Press se fölagets hemsida [http://www.ep.liu.se/](http://www.ep.liu.se/)

---

In English

The publishers will keep this document online on the Internet -or its possible replacement - for a considerable time from the date of publication barring exceptional circumstances.

The online availability of the document implies a permanent permission for anyone to read, to download, to print out single copies for your own use and to use it unchanged for any non-commercial research and educational purpose. Subsequent transfers of copyright cannot revoke this permission. All other uses of the document are conditional on the consent of the copyright owner. The publisher has taken technical and administrative measures to assure authenticity, security and accessibility.

According to intellectual property law the author has the right to be mentioned when his/her work is accessed as described above and to be protected against infringement.

For additional information about the Linköping University Electronic Press and its procedures for publication and for assurance of document integrity, please refer to its WWW home page: [http://www.ep.liu.se/](http://www.ep.liu.se/)

© [Författarens för- och efternamn]

Fernando García Torre