IEEE 802.11
Wireless Access Method and Physical Layer Specifications

Title: **MAC Frame Formats**

Symbionics
St John's Innovation Park
Cowley Road
Cambridge, UK
CB4 4WS

Presented by: Tim Phipps
Tel: +44 223 421025
Fax: +44 223 421031
Email: tgcp@symbionics.co.uk

Abstract: **This paper proposes a frame format for MPDUs in IEEE 802.11.**

1. Introduction

The aim of this paper is to generate a full and self consistent set of frame format definitions for MAC Physical Data Units (MPDUs). There is also a precise definition of the Message Information Contents for MPDUs which support MAC services. If accepted in full then this document would replace section 4 and section 2.7 of the draft standard [reference 1].

2. Frame and MPDU Formats

2.1. Basic Frame Format

Each frame shall consist of the following basic components:

A fixed-length *Fixed Header*, which includes a Version field, Type field and Control field

A fixed length MPDU-ID.

A variable length *Frame Body*, including

Possible Duration field, dependant on the frame's type.

Possible Station ID field, dependant on the frame's type.

Address fields, which shall include one or more fields with Network ID, Destination Address, and/or Source Address, depending on the frame's type.

Variable length components, including a (possibly empty) set of *elements* and a (possibly empty) set of *type-dependent fields.*

A 32-bit CRC applied over the frame.

Subsequent sections define each of the fields. The octets of a frame are transmitted from left to right. Each octet of the MAC frame, with the exception of the CRC, is transmitted low order bit first.

2.1.1. Protocol Version

This 4 bit field is invariant in size and placement across all revisions of the 802.11 standard. The values of the field are defined as follows:

> Revision level of the 802.11 MAC protocol. The values shall be assigned sequentially starting with the value 1.

There is a reserved value for future expansion, this value shall be assigned only after all other available protocol revision values have been used. When this value, which is 0, is assigned the standard shall also specify an extension of the header to include an additional Protocol Version field.

The value of this field shall be 1 at the initial release of the standard.

Version Field Format

Version				Reserved			
b0	b1	b2	b3	b4	b5	b6	b7

2.1.2. Type

One octet, including a 2 bit type field, and a 4 bit subtype field. There are two reserved bits which shall be zero.

Type Field Format

Type		Res.	Sub-type				Res.
b0	b1	b2	b3	b4	b5	b6	b7

The type field indicates whether the frame is of type Management, Data, or Control. The type sub-field shall take the following values:

Type

0	Management
1	Control
2	Reserved
3	Data

The sub-type sub-field shall take the following values:

Management Sub-type

0	Associate Request

1	Associate Response
2	Reassociate Request
3	Reassociate Response
4	Dissociate Request
5 - 7	Reserved
8	Authentication msg-1
9	Authentication msg-2
10	Authentication msg-3
11	Authentication msg-4
12	Authentication msg-5
13	Authentication msg-6
14	Privacy msg-1
15	Privacy msg-2

Data Sub-type

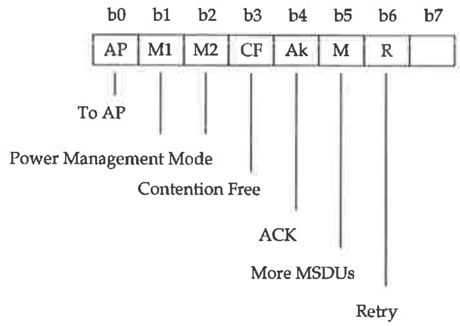
0	Plain Data
1	Encrypted Data
2 to 15	Reserved

Control Sub-type

0	RTS (Request to Send)
1	CTS (Clear to Send)
2	ACK
3	(Power Saving) Poll
4	Beacon
5	ATIM
6	Probe
7	Probe Response
8	CF-ACK
9 to 15	Reserved

2.1.3. Control Field

Control Field Format



Control Field

Bit 0	To AP
Bits 1,2	Power Management Mode
Bit 3	Contention Free
Bit 4	ACK
Bit 5	More MSDUs
Bit 6	Retry
Bit 7	Reserved (set to zero)

One octet, the bits of which have the following meaning:

To AP: This bit shall be set to 1 whenever the transmitted frame is targeted for the AP (either directly to the AP's destination address, or to another station but relayed through the AP), and shall be 0 otherwise.

Power Management Mode

Two bits, indicating the current mode of the transmitting station, as follows:

0	CAM
1	PSP
2	PSNP
3	TAM

Contention Free: 1 = this frame is in the contention free period, 0 = contention period.
(Note: CF-Up = Contention Free AND Data frame type AND To AP bit set; CF-Down = Contention Free AND Data frame type AND To AP bit not set).

Ack: acknowledge a frame when in contention free period (1 = ACK, 0 = NOT ACK).

More: Indicates that additional MSDUs are buffered within the transmitting station.

Retry: 1 = this is a retransmitted frame, 0 = new frame

Editor's Note: the last, reserved bit, could be used to specify an extension control field in future versions of the standard.

2.1.4. Duration

Two octets. Time in microseconds that should be written to the NAV if this frame is received correctly. The use of the NAV is explained elsewhere in this document.

2.1.5. MPDUID

This 16 bit field shall contain an identifying field.

The purpose of the field is as follows:

To provide a means to link a chain of MPDUs into a logical sequence (e.g. Data and ACK will have the same MPDUID).

To allow duplicate detection to be performed on data MPDUs.

To derive an MSDUID. The MSDUID is used to link different data MPDUs into a single data MSDU.

The MPDUID is formed by a hash over the source address and an incrementing 2 octet sequence number.

The sequence number incremented for every new MSDU, CF ACK, management frame, beacon, probe, probe response poll and ATIM. Note that it is NOT incremented for RTS (except when it is for a new MSDU), CTS, data MPDUs within an MSDU and ACK frames.

The hash function is CCITT CRC-16 operated first on the 6 octet source address and then the 2 octet sequence number in transmission order.

For data packets it is also necessary to include the fragment number. The fragment number is XORed with the hash. The XORed number will be the MPDUID for this data frame, the hash number will be a unique identifier for this MSDU, allowing all MPDUs within an MSDU to be reassembled.

2.1.6. Address Fields

Each MAC Frame may contain a combination of the following address fields depending on the type of MAC Frame. The relative order of the Address fields will always be SID, NID, DEST, SRC. Relative order will be maintained even if one or more are not included in a particular type MAC Frame.

2.1.6.1. Station ID

Two octets. A unique station identity number, within a BSS, that is assigned to a station, by an access point, when (re)association is successful.

2.1.6.2. NID

The NID is a 3-octet Network ID field, consisting of a 1-bit "Infrastructure" indicator (0 denotes Ad Hoc, 1 denotes Infrastructure), a 13 bit ESS ID field, and an 10 bit BSS ID field.

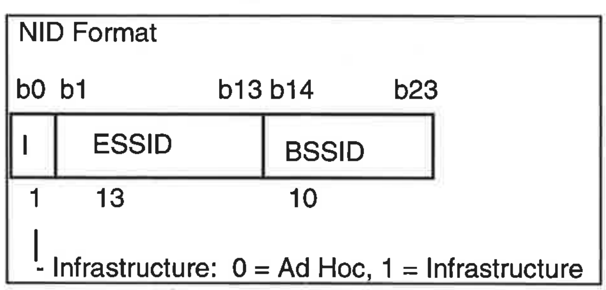


Figure 4-xx, NID Format

2.1.6.3. DEST & SRC Address Fields

The Destination Address (DEST) field identifies the destination addressee(s) for which the frame is intended. The Source address (SRC) field identifies the station from which the frame was initiated.

The representation of each address field shall be as follows (see fig. 4.1.4.2):

Each Address field shall contain a 48 bits address as defined in Section 5.2 of IEEE Std 802-1990.

The first bit (LSB) shall be used in the Destination Address field as an address type designation bit to identify the Destination Address either as an individual or as a group address. If this bit is 1, it shall indicate that the Destination address field contains a group address that identifies none, one or more, or all of the stations connected to the local area network.

There are two kinds of Group Addresses:

Multicast-Group Address. An address associated by higher-level convention with a group of logically related stations.

Broadcast Address. A distinguished, predefined multicast address that always denotes the set of all stations on a given local area network. All 1's in the Destination Address field is defined to be the Broadcast address. This group shall be predefined for each communication medium to consist of all stations actively connected to that medium; it shall be used to broadcast to all the active stations on that medium. All stations shall be able to recognise the Broadcast Address. It is not necessary that a station be capable of generating the broadcast address.

In the Source address field, the first bit is reserved and set to 0.

The second bit shall be used to distinguish between locally or globally administered addresses. For globally administered (or U, universal) addresses, the bit is set to 0. If an address is to be assigned locally, this bit shall be set to 1. Note that for the broadcast address, this bit is also a 1. The nature of an administrative body and the procedures by which it administers these global (U) addresses is beyond the scope of this standard. (Please refer to the IEEE Standard Overview and Architecture, IEEE Std 802-1990, ISBN 1-55937-052-1).

Each Octet of each address field shall be transmitted least significant bit first.

48 Bit Address Format

I/G	U/L	46 bit address (bit transmission ordered)

Example: 01-35-AC-F8-46-DB (Canonical Format)

10000000 10101100 00110101 00011111 01100010 11011011

Fig. 4-xx, Dest & Src Address Field Format

2.1.7. Elements

Variable length field containing zero or more elements.

Element format shall include 1 octet Code field, 1 bit More indicator, and 7 bit Link field.

Link field shall indicate the number of remaining octets in the element.

2.1.8. Data

Data: variable length data field. This field contains octets from the MAC Service data unit (MSDU). Its length shall not exceed 2304 octets.

2.1.9. CRC

4 octets. Data encoding starts with the version field.

The encoding is defined by the following generating polynomial.

$G(x) = x^{32} + x^{26} + x^{23} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^{8} + x^{7} + x^{5} + x^{4} + x^{2} + x + 1$

Mathematically, the cyclic redundancy check (CRC) value corresponding to a given frame is defined by the following procedure:

(1) The first 32 bits of the frame are complemented.

(2) The n bits of the frame are then considered to be the coefficients of a polynomial M(x) of degree n-1.The first bit encoded corresponds to the x^{n-1} term and the last bit of data encoded corresponds to the x^0 term).

(3) M(x) is multiplied by x^{32} and divided by G(x), producing a remainder R(x) of degree <31.

(4) The coefficients of R(x) are considered to be a 32 bit sequence.

(5) The bit sequence is complemented and the result is the CRC.

The 32 bits of the CRC are transmitted in the order $x^{31}, x^{30}, \ldots, x^{1}, x^{0}$.

2.1.10. Frame Formats

The following figure displays the type-dependent fields within the various frame types.

RTS	Ver	Type	Cntl	MPDUID	Duration	NID	Destination	CRC-32			
CTS	Ver	Type	Cntl	MPDUID	Duration	CRC-32					
Data CF Data	Ver	Type	Cntl	MPDUID	Duration	NID	Destination	Source	Frag #	Data	CRC-32
Ack CF Ack	Ver	Type	Cntl	MPDUID	Duration	CRC-32					
Management Beacon Probe Probe Response	Ver	Type	Cntl	MPDUID	Duration	NID	Destination	Source	Elements	CRC-32	
Poll	Ver	Type	Cntl	MPDUID	SID	NID	CRC-32				
ATIM	Ver	Type	Cntl	MPDUID	Duration	NID	Destination	Source	CRC-32		

2.1.10.1. RTS Frame Format

The frame format for an RTS frame is shown in Figure 4-xx.

Fixed Hdr	Duration	NID	DEST	CRC32
5 octets	2	3	6	4

Figure 4-xx: RTS Frame

The fields of the frame are defined as follows:

Fixed Header: The field consists of the Type, Control, and MPDU ID fields.

Duration: This field defines the medium occupancy time to the end of the ACK frame for the next MSDU fragment.

NID: This field is a 3 octet field that defines the Network ID.

DEST: This field is the 48 bit IEEE address of the destination.

Elements: No elements are permitted in an RTS frame.

CRC32: This field is 32-bit FCS generated over the entire frame, from beginning of the Fixed Header.

2.1.10.2. CTS Frame Format

The frame format for a CTS frame is shown in Figure 4-xx.

Fixed Hdr	Duration	NID	CRC32
5 octets	2	3	4

Figure 4-xx: CTS Frame

The fields of the frame are defined as follows:

Fixed Header: The field consists of the Type, Control, and MPDU ID fields. (Note: the MPDUID is copied from the preceding RTS).

Duration: This field defines the medium occupancy time to the end of the ACK frame for the next MSDU fragment.

NID: This field is a 3 octet field that defines the Network ID.

Elements: No elements are permitted in a CTS frame.

CRC32: This field is 32-bit FCS generated over the entire frame, from beginning of the Fixed Header.

2.1.10.3. Data Frame Format (including CF Data)

The frame format for a Data frame is shown in Figure 4-xx. The Fragment Number is always required in the data frame even if the MSDU is a single fragment.

Fixed Hdr	Duration	NID	DEST	SRC	Fragment Number	Payload	CRC32
5 octets	2	3	6	6	1	0 tox aFragment_Payload	4

Figure 4-xx: Data Frame

The fields of the data frame are defined as follows:

Fixed Header: The field consists of the Type, Control, and MPDU ID fields. (The MSDU ID, which can be derived simply from the MPDUID, is the same for all fragments of an MSDU).

Duration: This field defines the medium occupancy time to the end of the ACK frame for the next MSDU fragment. This field is always required even if RTS/CTS were not used to initiate the transfer. (Note: in the contention free period the duration field has no meaning, since the NAV is set for the duration of the CFP, the duration should therefore be ignored).

NID: This field is a 3 octet field that defines the Network ID.

DEST: This field is the 48 bit IEEE address of the destination.

SRC: This field is the 48 bit IEEE address of the source.

Fragment Number: This field defines the fragment number within a given MSDU. More detailed information of the Fragment Number field is given below. This field is always required even if the MSDU is a single fragment.

Elements: No elements are permitted in a data frame.

Payload: This field is all or part of a MSDU. It ranges in size from 0 to aFragment_Payload octets.

CRC32: This field is 32-bit FCS generated over the entire frame, from beginning of the Fixed Header.

The Fragment Number field of a Data frame in shown in Figure 4-xx.

b0	b1 … b7
Last Frag	Fragment Number

Figure 4-xx: Fragment Number Field for a Data Frame

The fields of the Fragment Number are defined as follows:

Last Fragment: This field is a single bit and indicates if the current fragment is the last fragment of the MSDU. A ‘one’ indicates the last fragment of a MSDU.

Fragment Number: This field is a binary representation of the fragment number of the MSDU.

2.1.10.4. Acknowledgement Frame Format (including CF-ACK)

The frame format for the acknowledgement frame is shown in Figure 4-xx.

Fixed Hdr	Duration	CRC 32
5 octets	2	4

Figure 4-xx: Acknowledgement Frame

The fields of the acknowledgement frame are defined as follows:

Fixed Header: The field consists of the Type, Control, and MPDU ID fields. The MPDU ID is copied from the data frame that is being acknowledged. (Note: CF-ACK has its own MPDUID).

Duration: This field defines the medium occupancy time to the end of the ACK frame for the next MSDU fragment. The field is set to 'zero' if this is the last fragment of a MSDU. This field is always required even if RTS/CTS were not used to initiate the transfer.

Elements: No elements are permitted in an ACK frame.

CRC32: This field is the FCS generated over the entire frame, from beginning of the Fixed Header.

2.1.10.5. Management Frame Format

The frame format for a management frame is shown in Figure 4-xx.

Fixed Hdr	Duration	NID	DEST	SRC	Elements	CRC32
5 octets	2	3	6	6	X	4

Figure 4-xx: Management Frame

The fields of the frame are defined as follows:

Fixed Header: The field consists of the Type, Control, and MPDU ID fields.

Duration: The duration field to set the NAV.

NID: This field is a 3 octet field that defines the Network ID.

DEST: This field is the 48 bit IEEE address of the destination.

SRC: This field is the 48 bit IEEE address of the source.

Elements: The elements used with management packets are defined in the section "Message Information contents which support the Services". They must be present as specified (in the order specified).

CRC32: This field is 32-bit FCS generated over the entire frame, from beginning of the Fixed Header.

2.1.10.6. Beacon Frame Format

The frame format for a beacon frame is shown in Figure 4-xx.

Fixed Hdr	Duration	NID	DEST	SRC	Elements	CRC32
5 octets	2	3	6	6	X	4

Figure 4-xx: Beacon Frame

The fields of the frame are defined as follows:

Fixed Header: The field consists of the Type, Control, and MPDU ID fields.

Duration: Set to zero, since this frame is not acknowledged.

NID: This field is a 3 octet field that defines the Network ID.

DEST: This field is the 48 bit IEEE address of the destination.

SRC: This field is the 48 bit IEEE address of the source.

Elements: The following elements must be present, in this order: time-stamp, beacon interval, hop dwell (FH PHY only), DTIM period, DTIM count and TIM.

CRC32: This field is 32-bit FCS generated over the entire frame, from beginning of the Fixed Header.

2.1.10.7. Probe Frame Format

The frame format for a probe frame is shown in Figure 4-xx.

Fixed Hdr	Duration	NID	DEST	SRC	CRC32
5 octets	2	3	6	6	4

Figure 4-xx: Probe Frame

The fields of the frame are defined as follows:

Fixed Header: The field consists of the Type, Control, and MPDU ID fields.

Duration: Set to zero, since this frame is not acknowledged.

NID: This field is a 3 octet field that defines the Network ID.

DEST: This field is the 48 bit IEEE address of the destination.

SRC: This field is the 48 bit IEEE address of the source.

Elements: No elements are permitted in a probe frame.

CRC32: This field is 32-bit FCS generated over the entire frame, from beginning of the Fixed Header.

2.1.10.8. Probe Response Frame Format

The frame format for a probe response frame is shown in Figure 4-xx.

Fixed Hdr	Duration	NID	DEST	SRC	Elements	CRC32
5 octets	2	3	6	6	X	4

Figure 4-xx: Probe Response Frame

The fields of the frame are defined as follows:

Fixed Header: The field consists of the Type, Control, and MPDU ID fields.

Duration: Duration field to set the NAV.

NID: This field is a 3 octet field that defines the Network ID.

DEST: This field is the 48 bit IEEE address of the destination.

SRC: This field is the 48 bit IEEE address of the source.

Elements: The following elements must be present, in this order: time-stamp, beacon interval, hop dwell (FH PHY only) and source NID. (note: the source NID is only included if the NID is not specific).

CRC32: This field is 32-bit FCS generated over the entire frame, from beginning of the Fixed Header.

2.1.10.9. Poll Frame Format

The frame format for a Poll frame is shown in Figure 4-xx.

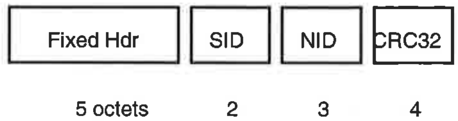


Figure 4-xx: Poll Frame

The fields of the poll frame are defined as follows:

Fixed Header: The field consists of the Type, Control, and MPDU ID fields.

(Duration: Note there is no duration field since the receiver may reply with either an ACK or a data frame).

NID: This field is a 3 octet field that defines the Network ID.

(DEST: Note there is no destination field since only an AP may be polled. The To AP bit should be set).

Elements: No elements are permitted in a poll frame.

CRC32: This field is 32-bit FCS generated over the entire frame, from beginning of the Fixed Header.

2.1.10.10. ATIM Frame Format

The frame format for an ATIM frame is shown in Figure 4-xx.

Figure 4-xx: ATIM Frame

The fields of the frame are defined as follows:

Fixed Header: The field consists of the Type, Control, and MPDU ID fields.

Duration: The duration value to set the NAV.

NID: This field is a 3 octet field that defines the Network ID.

DEST: This field is the 48 bit IEEE address of the destination.

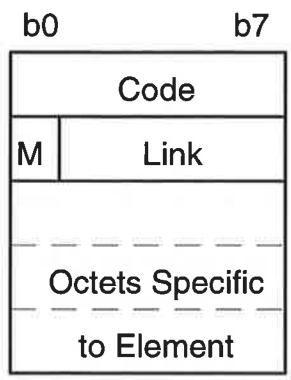
Elements: No elements are permitted in an ATIM frame.

CRC32: This field is 32-bit FCS generated over the entire frame, from beginning of the Fixed Header.

2.2. Elements

The general format of all elements is defined as follows:

General Element Format



More Bit M = 1: More Elements Follow
= 0: Last Element

Link (7 bits): number of subsequent octets

Elements are defined to have a common general format consisting of a one-octet Code field, a 1 bit More indicator (identifying whether additional elements are present), a 7-bit Link field, and a variable-length element-specific field. Each element is assigned a unique code as defined in this specification. The Link field shall be the number of additional octets in the element (which may be zero).

Certain frame types require that specific elements be present.

Defined elements are listed below. Note that elements may only be included in frames as specified.

2.2.1. Time-stamp

Element Number: 1

Additional Octets: 4

This element shall be 4 octets long. The value represents the current TSFTIMER value of frame's source in microseconds.

2.2.2. Beacon Interval

Element Number: 2

Additional Octets: 4

The number of microseconds between beacon generations.

2.2.3. Hop Dwell

Element Number: 3

Additional Octets: 4

Indicates the length, in microseconds, of the hop dwell time (for frequency hopping systems only).

2.2.4. Traffic Indication Map (TIM)

Element Number: 4

Additional Octets: variable

The TIM element shall contain a variable number of *block groups*, with each block group consisting of a *block identifier* followed by 0 to 7 one-octet *blocks*. Each bit within a block shall indicate whether a frame is currently buffered for a station with a particular Station ID. There is a one-to-one mapping between the bits in a *virtual bit-map* and the station IDs which is maintained within the access point; the actual transmitted TIM is a compressed representation of the virtual bit-map.

Note that SID zero is used to indicate that there is broadcast traffic available. If set, this bit shall indicate that a broadcast or multicast frame will be transmitted by the Access Point following the next DTIM (or after the current frame if this frame includes a DTIM).

Block (8 bits)

Each bit corresponds to a specific station within the block. If this block represents the Nth block within the virtual bit-map, then Bit M within the block shall correspond to the station with Station ID equal to 8*(N-1) + M.

Bit = 1: There is a frame pending for this station

Bit = 0: There is no frame pending for this station.

BI: Block Identifier (1 octet)

M	B1	B2	B3	B4	B5	B6	B7

Bit 0: More 0 = This is the last block group

= Another block group follows

Bit N (N = 1..7) 0 = Nth block in this group is absent

= Nth block in this group is present

Block Group: Consists of a Block Identifier followed by 0 through 7 Blocks.

BI	Blocks
Block Identifier	0 - 7 blocks

2.2.5. DTIM Count

Element Number: 5

Additional Octets: 1

This element shall indicate how many TIMs (including the TIM in the current frame, if any) will appear before the next DTIM. A DTIM Count of 0 shall indicate that the current TIM is in fact a DTIM.

2.2.6. DTIM Period

Element Number: 6

Additional Octets: 1

This element shall indicate the number of TIM intervals between successive DTIMs. If all TIMs are DTIMs then this element shall have the value 1.

2.2.7. Station ID

Element Number: 7

Additional Octets: 2

The Station ID that will be assigned to this station.

2.2.8. Source NID

Element Number: 8

Additional Octets: 3

The NID of the transmitting station.

2.2.9. Result

Element Number: 9

Additional Octets: 1

Result of a transaction. All zeros for success, any other value for fail.

2.2.10. Current AP

Element Number: 10

Additional Octets: 6

The IEEE address of the AP with which this station is currently associated.

2.2.11. Privacy Algorithm

Element Number: 11

Additional Octets: Not defined

Identifies a privacy algorithm.

2.2.12. Authentication Algorithm

Element Number: 12

Additional Octets: Not defined

Identifies an authentication algorithm.

2.2.13. Contention Free Capable

Element Number: 13

Additional Octets: 0

Signifies that this station is capable of operation within the rules of the contention free period.

2.2.14. Authentication Assertion

Element Number: 14

Additional Octets: Not defined

Assertion of identity.

2.2.15. Authentication Challenge

Element Number: 15

Additional Octets: Not defined

Challenge of identity assertion.

2.2.16. Authentication Response

Element Number: 16

Additional Octets: Not defined

Response to a challenge

2.2.17. Authentication Result

Element Number: 17

Additional Octets: Not defined

The result of the response to an authentication challenge.

3. Message information contents which support the services

3.1. Data Distribution

When a station wishes to send data to another station it use the following message.

3.1.1. Data Messages

Message Type:
  Data
Message sub-type:
  none
Source:
  IEEE source address of message
Destination:
  IEEE destination address of message
Elements:
  none
Direction of message:
  any

3.2. Association

When a STA wishes to Associate, the association service use the following message.

3.2.1. Association Request

Message Type:
  Management
Message sub-type:
  Association Request
Source:
  IEEE address of station initiating the association
Destination:
  IEEE address of the AP the initiating station desires to associate with
Elements:
  CF capable
Direction of message:
  From STA to AP

3.2.2. Association Response

This message is sent to confirm the success (or otherwise) of the association.

Message Type:
  Management
Message sub-type:
  Association Response
Source:
  IEEE address of the AP the initiating station desires to associate with
Destination:
  IEEE address of station initiating the association
Elements:
  Result, SID (note: SID is not valid if result is not successful)
Direction of message:
  From AP to STA

3.3. Reassociation

When a STA wishes to Reassociate, the Reassociation service uses the following message.

3.3.1. Reassociation Request

This request is different from the association request in that the current AP must be informed of the implicit dissociation that will occur and the current privacy algorithm must be communicated to the AP with which this STA wants to associate.

Message Type:
  Management
Message sub-type:
  Reassociation request
Source:
  IEEE address of station initiating the reassociation
Destination:
  IEEE address of the AP the initiating station desires to associate with
Elements:
  CF capable, IEEE address of current AP, Current privacy algorithm
Direction of message:
  From STA to AP

3.3.2. Reassociation Response

This message is sent to confirm the success (or otherwise) of the reassociation.

Message Type:
  Management
Message sub-type:
  Reassociation response
Source:
  IEEE address of the AP the initiating station desires to associate with
Destination:
  IEEE address of station initiating the reassociation
Elements:
  Result, SID (note: SID is not valid if result is not successful).
Direction of message:
  From AP to STA

3.4. Dissociation

When a STA wishes to terminate an active association, the Dissociation service uses the following message. Note that the same message can also be used when an AP wishes to initiate the dissociation of a STA. (Note: there is no response, dissociation is a unilateral decision).

3.4.1. Dissociate Request

Message Type:
  Management
Message sub-type:
  Dissociate Request
Source/Destination:
  IEEE address of the AP which the station is currently associated with
Destination/Source:
  IEEE address of the station which is being dissociated
Elements:
  none
Direction of message:
  From STA to AP **OR** From AP to STA

3.5. Privacy

When two STAs wish to negotiate and set up a privacy algorithm for use, the privacy service causes the following message sequence to occur.

3.5.1. Privacy Msg-1

STA1 sends a list of acceptable algorithms to STA2.

Message Type:
    Management
Message sub-type:
    Privacy msg-1
Source:
    STA1
Destination:
    STA2
Elements:
    Any number of instances of the Privacy Algorithm element
Direction of message:
    From STA1 to STA2

3.5.2. Privacy Msg-2

Result of the requested privacy Setup. STA2 communicates to STA1 a mutually acceptable privacy algorithm.

Message Type:
    Management
Message sub-type:
    Privacy msg-2
Source:
    STA1
Destination:
    STA2
Elements:
    Result element and privacy algorithm element (note: algorithm is not valid if result is not successful).
Direction of message:
    From STA1 to STA2

3.6. Authentication

3.6.1. Authentication Msg-1

STA1 sends a list of acceptable algorithms to STA2.

Message Type:
    Management
Message sub-type:
    Authentication msg-1
Source:
    STA1
Destination:
    STA2
Elements:
    Any number of instances of the authentication algorithm element
Direction of message:
    From STA1 to STA2

3.6.2. Authentication Msg-2

Result of the requested authentication algorithm Setup. STA2 communicates to STA1 a mutually acceptable authentication algorithm.

Message Type:	Management
Message sub-type:	Authentication msg-2
Source:	STA2
Destination:	STA1
Elements:	Result, algorithm selected (note: algorithm is not valid if result is not successful).
Direction of message:	From STA2 to STA1

3.6.3. Authentication Msg-3

STA 1 challenges the identity assertion by STA2. STA1 makes an assertion of identity.

Message Type:
    Management
Message sub-type:
    Authentication msg-3
Source:
    STA1
Destination:
    STA2
Elements:
    Authentication challenge, authentication assertion.
Direction of message:
    From STA1 to STA2

3.6.4. Authentication Msg-4

STA2 responds to the challenge of identity assertion from STA1. STA2 challenges the assertion of identity made by STA1.

Message Type:
    Management
Message sub-type:
    Authentication msg-4
Source:
    STA2
Destination:
    STA1
Elements:
    Authentication response, authentication challenge
Direction of message:
    From STA2 to STA1

3.6.5. Authentication Msg-5

STA1 responds to the challenge of identity assertion from STA2. STA1 gives the result of the response made by STA2 to a challenge of an identity assertion.

Message Type:
    Management
Message sub-type:
    Authentication msg-5
Source:
    STA1
Destination:
    STA2

Elements:

Authentication response, authentication result.

Direction of message:

From STA1 to STA2

3.6.6. Authentication Msg-6

STA2 gives the result of the response made by STA1 to a challenge of an identity assertion.

Message Type:

Management

Message sub-type:

Authentication msg-6

Source:

STA2

Destination:

STA1

Elements:

Authentication result.

Direction of message:

From STA2 to STA1

4. References

"Draft Standard IEEE 802.11 Wireless LAN", Doc IEEE P802.11-93/20b2.