IEEE 802.11

Wireless Access method and Physical Layer Specification

Proposed Text for Section 4
Based on responses to Draft D1 Letter Ballot processed at May, 1995 Meeting of IEEE P802.11

Simon Black
Symbionics Networks Ltd
Cambridge CB4 4WS UK
Phone: (44)-1223 421025
Fax: (44) 1223 421031
E-mail: sab@symbionics.co.uk

Abstract: This paper presents the changes to section 4 in the Draft Standard P802.11/D1 as a result of the Response to Draft D1 Letter Ballot processed at the May, 1995 meeting of IEEE P802.11.

Action: Adopt the changes in this paper to replace the relevant portions of P802.11/D1.1.

4. Frame and MPDU Formats

4.1. MAC Frame Formats

Each frame shall consist of the following basic components:

a) A *MAC Header*, which comprises~~includes~~ frame control ~~information~~, duration, address~~ing~~ and ~~,~~ sequence~~ing~~ control information, ~~fragmentation identification and duration~~.
b) A variable length *Frame Body*, that ~~may~~ contains information specific to the~~various~~ frame *type~~s~~*.
c) An IEEE 32-bit CRC.

4.1.1. General Frame Format

The MAC frame format comprises a set of fields that shall occur in a fixed order in all frames. ~~Some fields may be absent from some frame types.~~

Figure 4-1 depicts the general MAC frame format ~~and field order~~. The fields that appear shaded are only present in certain frame types. Each field is defined in section 4.1.2. The format of the each of the individual frame types is defined in section 4.2. ~~The format of the MAC header for each of the frame types is defined subsequently. Subsequent sections define each of the fields of the MAC header.~~

A frame is an ordered octet string. The order of transmission of the octets of a frame shall be from left to right.

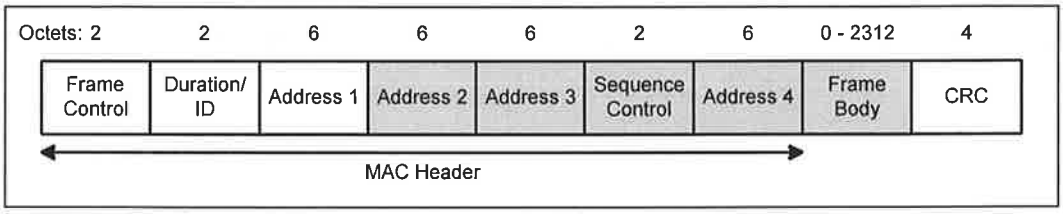


Figure 4-1: MAC Frame Format

4.1.2. Frame Fields

4.1.2.1. Frame Control Field

The Frame Control field shall consist of the following sub-fields: Protocol Version, Type, Subtype, To DS, From DS, Last Fragment, Retry, Power Management and WEP~~Elements Present~~. The remaining subfields in the Frame Control field are reserved. All reserved bits and fields shall be set to~~sent as~~ '0'. Reserved bits and fields shall be ignored on reception.

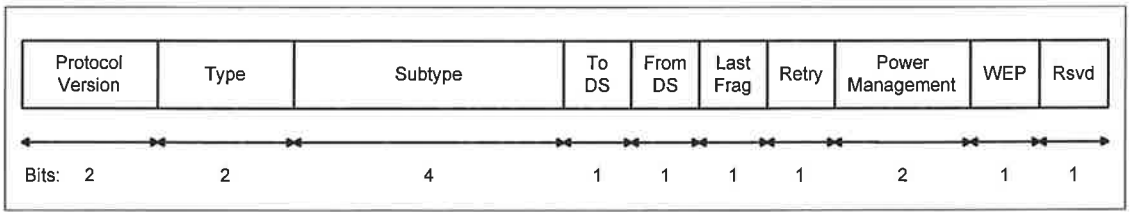


Figure 4-2: Frame Control Field

4.1.2.1.1. Protocol Version

The protocol version ~~This two bit~~ field shall be two bits in length and shall be invariant in size and placement across all revisions of the 802.11 standard. For this revision of the standard the value of the protocol version shall be 0. All other values are reserved. ~~The values shall be assigned sequentially starting with the value zero.~~ The revision level shall be incremented only when a fundamental incompatibility exists between a new revision and this revision of the standard~~a lower revision and the current standard~~. A device that receives a frame with a higher revision level than it can understand shall discard the frame without indication to LLC.

4.1.2.1.2. Type and Subtype

The Type field shall be two bits and the Subtype field four bits in length. The Type and Subtype fields shall together identify the function ~~and interpretation~~ of the~~a~~ frame. There are three frame types: control, data and management. Each of the frame types ~~may~~ have several defined subtypes. The table below defines~~lists~~ the valid combinations of Type and Subtype.

Type Value	Type Description	Subtype Value	Subtype Description
00	Management	0000	Association Request
00	Management	0001	Association Response
00	Management	0010	Reassociation Request
00	Management	0011	Reassociation Response
00	Management	0100	Probe Request
00	Management	0101	Probe Response
~~00~~	~~Management~~	~~0110~~	~~Privacy Request~~Reserved
~~00~~	~~Management~~	~~0111~~	~~Privacy Response~~Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication~~Connection Request~~
00	Management	1101	~~Grant~~ Connection Request
00	Management	1110	Grant~~End~~ Connection
00	Management	1111	End Connection~~Reserved~~
01	Control	0000-1001~~10~~	Reserved
01	Control	1010	PS-Poll
01	Control	1011	RTS
01	Control	1100	CTS
01	Control	1101	ACK
01	Control	1110	CF End
01	Control	1111	CF End + CF-ACK~~Poll~~
10	~~Asynchronous~~ Data	0000	Data
10	~~Asynchronous~~ Data	0001	Data + CF-Ack
10	~~Asynchronous~~ Data	0010	Data + CF-Poll
10	~~Asynchronous~~ Data	0011	Data + CF-Ack + CF-Poll
10	~~Asynchronous~~ Data	0100	Null Function (no data)
10	~~Asynchronous~~ Data	0101	CF-Ack (no data)
10	~~Asynchronous~~ Data	0110	CF-Poll (no data)

10	~~Asynchronous~~ Data	0111	CF-Ack + CF-Poll (no data)
10	~~Asynchronous~~ Data	1000-1111	Reserved
11	Reserved	0000-1111	Reserved

Table 4-1: Valid Type/Subtype Combinations

4.1.2.1.3. To DS

The To DS field shall be one bit in length and shall be set to '1' in Data Type frames destined for the Distribution System. ~~This one bit field shall indicate that the frame is destined for the distribution system in an infrastructure network. This bit shall be transmitted as a one only if the frame Type = Data and the frame is entering the distribution system.~~ It shall be set to '0' in all other frames~~transmitted as a zero, otherwise~~.

4.1.2.1.4. From DS

The From DS field shall be one bit in length and shall be set to '1' in Data Type frames exiting the Distribution System. ~~This one bit field shall indicate that the frame is being distributed from the distribution system in an infrastructure network. This bit shall be transmitted as a one only if the frame Type = Data and the frame is exiting the distribution system.~~ It shall be set to '0' in all other frames~~transmitted as a zero, otherwise~~.

The permitted~~possible~~ To/From DS bit combinations and their meaning are given in ~~the following~~ table 4.2.~~:~~

To/From DS Values	~~Description~~ Meaning
To DS = '0'~~False~~ From DS = '0'~~DS False.~~	A Data Frame direct from one STA~~tation~~ to another STA~~tation~~ within the same BSS.
To DS = '1'~~True~~ From DS = '0'~~False~~	Data Frame entering the DS.
To DS = '0'~~False~~ From DS = '1'~~True~~	Data Frame exiting the DS.
To DS = '1'~~True~~ From DS = '1'~~True~~	WDS frame being distributed ~~f~~From one AP to another AP.

Table 4-2: To / From DS Combinations

4.1.2.1.5. Last Fragment

The Last Fragment field shall be one bit in length and ~~This one bit field~~ shall be set to '1' in a frame containing ~~indicate that this frame is~~ the last fragment of a fragmented MSDU, or the sole fragment of an unfragmented MSDU.

4.1.2.1.6. Retry

The Retry field shall be one bit in length and ~~This one bit field~~ shall be set to '1' in a Data Type frame that ~~indicate that the frame~~ is a retransmission of an earlier frame. A station shall~~may~~ use this indication to aid in the process of eliminating duplicate frames.

4.1.2.1.7. Power Management

The Power Management field shall be two bits in length and ~~The two bit field~~ shall be used to indicate the power management state and buffered traffic state of the station. The value of this field shall remain constant in each frame within a frame sequence defined in section 4.3. The value ~~sent~~ shall indicate the state

in which the station will be after the completion of the ~~transmission of the~~ frame sequence. The permitted values for this field and their meaning are given in table 4~~–32~~.

Value	Description
00	Active Mode ~~(CAM or TAM)~~, with More buffered frames
01	PSP - Power Save, Polling
~~10~~	~~PSNP - Power Save, No Polling~~
11	Active Mode ~~(CAM or TAM)~~, without More buffered frames

Table 4-3: Power Management Values

~~*4.1.2.1.8. Elements Present*~~

~~If a frame's "Elements Present" control field is 1, then the frame body shall include one or more "elements". Certain frame types require that specific elements be present. These are defined in Section 4.2.3.~~

4.1.2.1.8 WEP

The WEP field shall be one bit in length. It shall be set to '1' if the Frame Body field contains information that has been processed by the WEP algorithm. The WEP bit may only be set to '1' within frames of Type Data and frames of Type Management, Subtype Authentication. The WEP bit shall be set to '0' in all other frames.

4.1.2.2. Duration~~/ or Connection~~ ID

The Duration/ID field shall be 16 bits in length. The contents of the this field shall be as follows:

a) In Data Type frames transmitted during the contention free period that have frame body information associated with a time-bounded connection, the Duration/ID field shall carry the connection identity of the time-bound connection.
b) In Control Type frames of SubType PS-Poll, the Duration/ID field shall carry the station identity (SID) of the station that transmitted the frame.
c) In all other frames the Duration/ID field shall contain a duration value. For frames transmitted during the contention period the duration value shall be set to the time in microseconds from the end of the current frame to the end of the next anticipated frame of Type Control and Subtype ACK. For frames transmitted during the contention free period the duration value shall be set to 0. The duration value shall be used to update the Net Allocation Vector according to the procedures defined in section 5.

~~The Duration field is a 16-bit field. It shall be used to distribute a value that shall update the Network Allocation Vector in stations receiving the frame. The duration shall be specified in microseconds. See section 5.xx for details of calculating the value for the duration field. During the contention free period the duration field may be replaced by a connection ID field. (Note: only contention free time-bounded data used a connection ID; contention based data and contention free asynchronous data do not use connection IDs).~~

4.1.2.3. Address Fields

There are four address fields in the MAC frame format. These fields are used ~~variously~~ to indicate the BSSID, source address, destination address, transmitting station address and receiving station address. The

usage of the four address fields in each frame type will be indicated by the abbreviations BSSID, DA, SA, RA, TA indicating BSS Identifier, Destination Address, Source Address, Receiver Address and Transmitter Address, respectively. Some frames may omit some of the address fields.

4.1.2.3.1. Address Representation

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

4.1.2.3.2. Address Designation

A MAC Sublayer address is of one of two types:

a) -Individual Address. The address associated with a particular station on the network.
b) -Group Address. A Multidestination address, associated with one or more stations on a given network. There are two kinds of Group Addresses:
   1) -Multicast-Group Address. An address associated by higher-level convention with a group of logically related stations.
   2) -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 shall be predefined 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 recognize the Broadcast Address. It is not necessary that a station be capable of generating the broadcast address.

The address space shall also be partitioned into locally administered and globally administered addresses. The nature of a 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)

4.1.2.3.3. BSS Identifier

The BSS Identifier (BSSID) shall be a 48-bit field of the same format as an IEEE 802 MAC address. This field shall uniquely identify each BSS in an infrastructure LAN. The value of this field, in an infrastructure LAN, shall be the MAC address of the STA in the AP~~access point~~ of the BSS. The mechanisms used to ensure the uniqueness of MAC addresses also create unique BSS Identifiers. The Individual/Group bit of the address shall be transmitted as zero.

In an ad hoc LAN, this field shall be transmitted with the BSS ID of the ad hoc network. ~~This field shall be a locally administered multicast group address. The value of this field shall be chosen by the station that establishes the ad hoc LAN.~~ The value of this field, in an ad-hoc LAN, shall be the MAC address of the STA that initiated the ad-hoc network.~~Measures shall be taken in the selection of the value of this field to differentiate it from other ad hoc LANs in the vicinity.~~

4.1.2.3.4. Destination Address

The destination address (DA) field shall contain an IEEE MAC individual or group address that identifies the MAC entity or entities intended as the final recipient(s) of the MSDU (or fragment thereof) contained in the frame body field.~~The Destination Address (DA) field shall identify the destination addressee(s) for which the frame is intended.~~

4.1.2.3.5. Source Address

The source address (SA) field shall contain an IEEE MAC individual address that identifies the MAC entity from which the transfer of the MSDU (or fragment thereof) contained in the frame body field was initiated. ~~The Source Address (SA) field identifies the station from which the frame was initiated.~~ The Individual/Group bit shall always be transmitted as a zero in the source address~~.~~

4.1.2.3.6. Receiver Address

The receiver address (RA) field shall contain an IEEE MAC individual or group address address that identifies the intended immediate recipient STA(s), on the wireless medium, for the MPDU contained in the frame body field. ~~The Receiver Address (RA) field identifies the IEEE MAC address of the intended recipient of a wireless transmission. The Individual/Group bit shall always be transmitted as a zero.~~

4.1.2.3.7. Transmitter Address

The transmitter address (TA) field shall contain an IEEE MAC individual address that identifies the STA which transmitted, onto the wireless medium, the MPDU contained in the frame body field. ~~The Transmitter Address (TA) field identifies the IEEE MAC address of the transmitter of a wireless transmission.~~ The Individual/Group bit shall always be transmitted as a zero.

4.1.2.4. Sequence Control

The Sequence Control field shall be 16 bits in length and ~~This 16 bit field~~ shall consist of ~~contain~~ two subfields, the Sequence Number ~~Dialog Token~~ and the Fragment number. The format of the Sequence Control field is illustrated in figure 4-3.

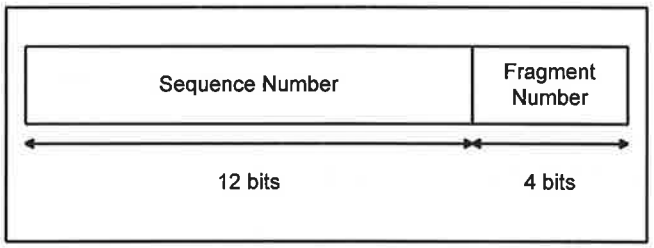


Figure 4-3: Sequence Control Field

4.1.2.4.1. Sequence Number ~~Dialog Token~~

The Sequence Number shall be a 12 bit field indicating the sequence number of the MSDU. MSDUs shall be numbered sequentially starting at zero. Each transmission of an MSDU or fragment thereof shall contain the sequence number of that MSDU. The sequence number shall remain constant in all retransmissions of an MSDU or fragment. ~~This 12 bit field shall contain an incrementing value. The value shall be incremented for the initial transmission of an MSDU. The same value shall be used for all fragments of the same MSDU. The Sequence Number value shall not be incremented for retransmissions of the same MSDU or its fragments.~~

4.1.2.4.2. Fragment Number

The Fragment Number shall be a 4 bit field indicating the number of each fragment of an MSDU. The fragment shall be set to zero in the first or only fragment of an MSDU and shall be incremented by one for each successive fragment of that MSDU. ~~The Fragment Number is a 4 bit field. It shall indicate the number of each individual fragment. The format of this field is shown in figure 4-4.~~

4.1.2.5. Frame Body

The Frame Body shall be~~is~~ a variable length field and shall contain ~~that may vary from zero to 2304 bytes. i~~Information specific to individual frame types and subtypes ~~shall be placed in the Frame Body~~. The minimum frame body shall be zero octets and the maximum 2312 octets. The maximum length frame body is defined by the maximum length MSDU + ICV + IV; where ICV and IV are the WEP fields defined in section n.n.

4.1.2.6. CRC

The CRC field shall be a 32 bit field containing a 32-bit Cyclic Redundancy Check (CRC). The CRC shall be calculated over all the fields of the MAC header and the frame body field. These are referred to as the calculation fields.

The CRC shall be calculated using the following standard generator polynomial of degree 32:

~~The CRC shall be 4 octets in length. Data encoding shall start with the version field.~~

~~The encoding shall be defined by the following generating polynomial.~~

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

The CRC shall be the one's complement of the sum (modulo 2) of the following:

1) The remainder of $x^k*(x^{31} + x^{30} + x^{29} + ... + x^2 + x + 1)$ divided (modulo 2) by G(x), where k is the number of bits in the calculation fields, and

2) The remainder after multiplication of the contents (treated as a polynomial) of the calculation fields by x^{32} and then division by G(x).

The CRC field shall be transmitted commencing with the coefficient of the highest order term.

As a typical implementation, at the transmitter, the initial remainder of the division is preset to all ones and is then modified by division of the calculation fields by the generator polynomial G(x). The ones complement of this remainder is transmitted, with the most significant bit first, as the CRC field.

At the receiver, the initial remainder is preset to all ones and the serial incoming bits of the calculation fields and CRC, when divided by G(x) results in the absence of transmission errors, in a unique non-zero remainder value. The unique remainder value is the polynomial:

$$x^{31} + x^{30} + x^{26} + x^{25} + x^{24} + x^{18} + x^{15} + x^{14} + x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^5 + x^4 + x^3 + x + 1$$

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

~~a) The first 32 bits of the frame are complemented.~~

b) 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.
c) M(x) is multiplied by x^{32} and divided by G(x), producing a remainder R(x) of degree <31.
d) The coefficients of R(x) are considered to be a 32 bit sequence.
e) The bit sequence is complemented and the result is the CRC.

4.2. Format of Individual Frame Types

4.2.1.Control Frames

In the following descriptions, "immediately previous" frame means a frame, the reception of which concluded within the prior SIFS interval.

The subfields within the Frame Control field of Control frames shall be set as illustrated in figure 4-4 below.

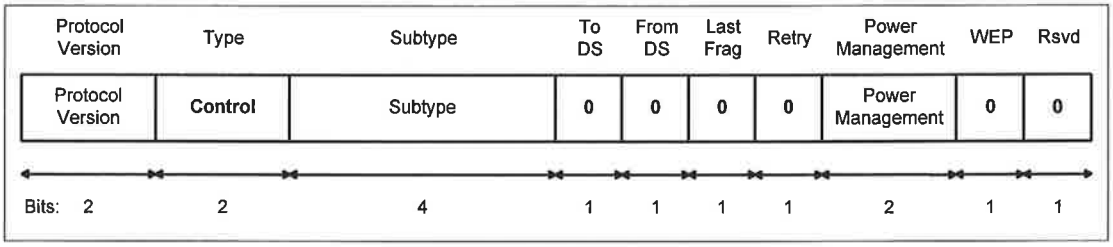


Figure 4-4: Frame Control field subfield values within Control Frames

4.2.1.1. RTS Frame Format

The frame format for the~~an~~ RTS frame shall be as defined~~is shown~~ in Figure 4-54.

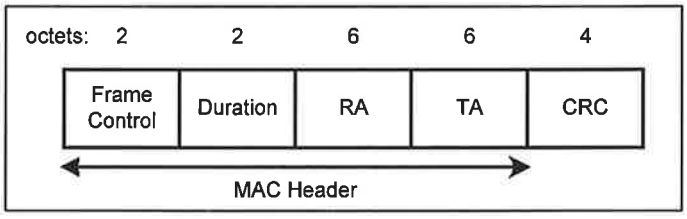


Figure 4-5: RTS Frame

The RA of the RTS frame shall be the address of the STA, on the wireless medium, that is the intended immediate recipient of the pending directed Data or Management frame.

In an infrastructure BSS, the RA shall always designate the AP with which the STA transmitting the RTS frame is associated.

The TA shall be the address of the STA transmitting the RTS frame.

~~The DA of this frame shall be the address of the immediate station receiving the frame. In an infrastructure LAN, the DA shall be the address of the AP with which the station is associated. In an ad hoc LAN, the DA shall be the destination of the subsequent data or management frame. The SA shall be the address of the station transmitting the frame.~~

4.2.1.2. CTS Frame Format

The frame format for the~~an~~ CTS frame shall be as defined~~is shown~~ in Figure 4-6~~5~~.

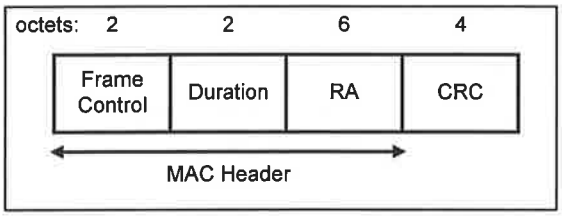


Figure 4-6~~5~~: CTS Frame

The Receiver~~destination~~ Address (RA) of the CTS frame shall be copied~~taken~~ from the Transmitter~~source~~ Address (TA) field of the immediately previous RTS frame to which the CTS is a response.

4.2.1.3. ACK Frame Format

The frame format for the ACK frame shall be as defined~~is shown~~ in Figure 4-7~~6~~.

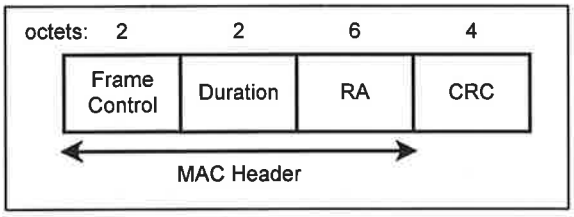


Figure 4-7~~6~~: ACK Frame

The Receiver Address~~DA~~ of the ACK frame shall be copied from~~the address contained in~~ the Address 2 field of the immediately previous directed Data or Management frame.

4.2.1.4. PS-Poll Frame Format

The frame format for the Power Save Poll (PS-Poll) frame shall be as defined~~is shown~~ in Figure 4-8~~7~~.

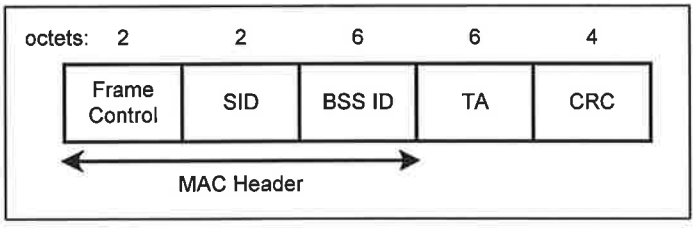


Figure 4-8~~7~~: PS-Poll Frame

The BSS Identifier shall be the address of the STA contained in the AP. The Transmitter~~Source~~ Address (TA) shall be the address of the STA~~station~~ transmitting the frame. The SID shall be the value assigned by the AP in the Associate Response frame.

4.2.1.6 CF-End Frame Format

The frame format for the Contention Free-End (CF-END) frame shall be as defined in Figure 4-9.

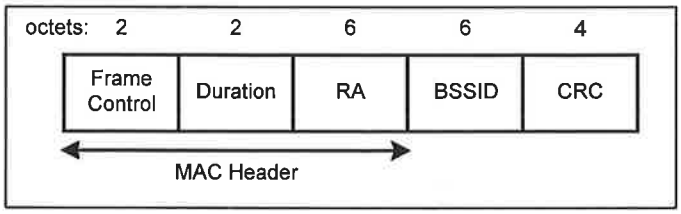


Figure 4-9: CF-End Frame

The BSS Identifier shall be the address of the STA contained in the AP. The Receiver Address (RA) shall be the broadcast group address.

The Duration field shall be set to 0.

4.2.1.5 CF-End+CF-ACK Frame Format

The frame format for the Contention Free-End Acknowledge (CF-END + CF-ACK) frame shall be as defined in Figure 4-10.

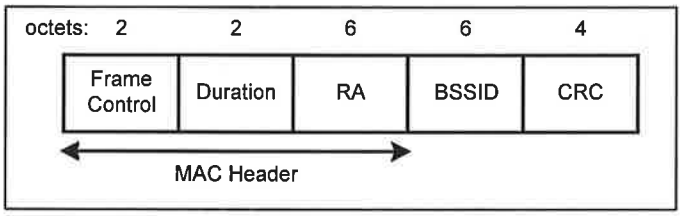


Figure 4-10: CF-End + CF-ACK Frame

The BSS Identifier shall be the address of the STA contained in the AP. The Receiver Address (RA) shall be the broadcast group address.

The Duration field shall be set to 0.

4.2.2.Data Frames

4.2.2.1. DATA Frame Format

The frame format for a Data frame is independent of subtype and shall be as defined~~is shown~~ in Figure 4-11~~8~~.

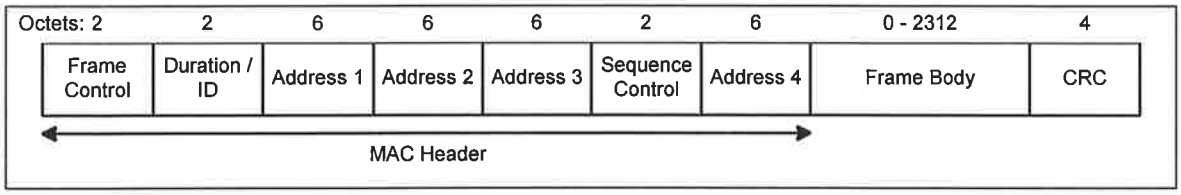


Figure 4-11~~8~~: DATA Frame

The contents of the Address fields of the Data frame shall be dependent upon the values of the To DS and From DS bits and are defined in table 4-4, below. Where the content of a field is shown as N/A, the field shall be omitted.

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

Table 4-4: Address Field Contents

A station shall use the contents of Address 1 field to perform address matching for receive decisions. In cases where the Address 1 field contains a group address, the BSSID must also be validated to ensure that the broadcast, or multicast originated in the same BSS.

A station shall use the contents of the Address 2 field to direct the acknowledgement if an acknowledgement is necessary.

The DA shall be ~~the destination of the frame, i.e.~~ the destination of the MSDU (or fragment thereof) in the frame body field.~~.~~

The SA shall be the address of the MAC entity~~station~~ initiating the transmission of the MSDU (or fragment thereof) in the frame body field.~~transmitting the frame.~~

The RA shall be the address of the STA contained in the AP~~access point~~ in the wireless distribution system that is the next immediate intended recipient of the frame.

The TA shall be the address of the STA contained in the AP~~access point~~ in the wireless distribution system that is transmitting the frame.

The BSSID of the Data frame shall be determined as follows:

a) If the station is an AP or is ~~a~~ associated with an AP, the BSS Identifier shall be the address of the STA contained in the AP.
b) If the station is a member of an ad hoc LAN, the BSS Identifier shall be the BSS ID of the ad hoc LAN.

The Frame Body shall be the MSDU or a fragment thereof, plus the WEP IV and ICV if the WEP subfield in the frame control field is set to '1'. The frame body is null (zero octets length) in Data frames of Subtype 01xx.

Data frames sent during the contention period shall use the Data Subtypes (0000, or 0100). Data frames sent by the PCF during the contention free period shall use the appropriate ones of the Data Subtypes 0000–0111 based upon the usage rules:

Data Subtypes 0010, 0011, 0110, and 0111 shall only be sent by a PCF.

Data Subtypes 0000, 0001, 0100, and 0101 may be sent by any CF-aware station.

Stations receiving Data frames shall only process the Data frame body, and shall only consider the frame body as the basis of a possible indication to LLC, if the Data Subtype is of the form= 00xx. Stations capable of transmitting in response to polling by a PCF shall interpret all Subtype bits of received Data frames for CF purposes, but shall only inspect the frame body if the Subtype is of the form 00xx.

All stations shall process the duration field contents of valid data frames to update their NAV settings as appropriate under the coordination function rules.

4.2.3. Management Frames

The frame format for a Management frame is independent of subtype and shall be as definedis shown in Figure 4-129.

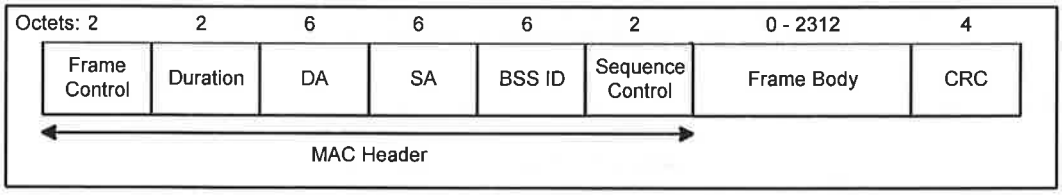


Figure 4-129: Management Frame Format

The address fields for Management frames shall not vary by frame subtype.

The BSS Identifier of the Management frame shall be determined as follows:

a) If the station is an AP or is a associated with an AP, the BSS Identifier shall be the address of the STA contained in the AP.
b) If the station is a member of an ad hoc LAN, the BSS Identifier shall be the BSS ID of the ad hoc LAN.
c) In Management frames of Subtype Probe, the BSSID shall either be a specific BSSID, or the broadcast BSSID as defined in the procedures specified in section 7.

The DA shall be the destination of the frame.

The SA shall be the address of the station transmitting the frame.

The Frame Body shall consist of the fixed fields and information elements defined for each management frame subtype.be the information elements described for each management frame subtype, below. All fixed

fields and information elements are mandatory unless stated otherwise and shall only appear in the specified order.

~~Elements shall be used strictly in Management frames, and shall be used after the fixed fields in the payloads of such frames. Elements within the payload of any particular Management frame shall be ordered by increasing element type code value.~~ Stations encountering an element type they do not understand shall ignore that element. Element type codes not explicitly defined in the standard are reserved, and shall not appear in any frames.

4.2.3.1. BEACON Frame Format

The Frame Body of a Management frame of Subtype Beacon shall contain~~comprise~~ the following information: ~~time stamp, weight, beacon interval, DTIM period, DTIM count, channel sync information, ESS ID, TIM and broadcast indicator.~~

Order	Information	Note
1	Timestamp	
2	Beacon Interval	
3	Regulatory Domain	
4	Capability Information	
5	ESS ID	
6	Supported Rates	
7	FH Parameter Set	1
8	CF Parameter Set	2
9	DTIM	
10	TIM	

Notes:

1 The FH Parameter Set information shall be mandatory only within Beacon Frames generated by STAs using Frequency Hopping Physical Layers

2 The CF Parameter Set information shall be mandatory only within Beacon Frames generated by APs supporting a PCF

~~*4.2.3.2. ATIM Frame Format*~~

~~The Frame Body shall be null.~~

4.2.3.3. Disassociation Frame Format

The Frame Body of a Management frame of Subtype Disassociation shall contain the following information:~~this frame is null.~~

Order	Information	Note
1	Status Code	

4.2.3.4. Association Request Frame Format

The Frame Body of a Management frame of Subtype Association Request shall contain the following information:~~shall consist of the privacy algorithm number and the supported rates.~~

Order	Information	Note
1	Capability Information	
2	ESSID	
3	Supported Rates	

4.2.3.5. Association Response Frame Format

The Frame Body of a Management frame of Subtype Association Response shall contain the following information:~~consist of a status value, an error indication, the supported rates and the station ID assigned (SID).~~

Order	Information	Note
1	Capability Information	
2	Status Code	
3	Station ID (SID)	
4	Supported Rates	

4.2.3.6. Reassociation Request Frame Format

The Frame Body of a Management frame of Subtype Reassociation Request shall contain the following information:~~consist of the current AP address and the privacy algorithm number.~~

Order	Information	Note
1	Capability Information	
2	Current AP Address	
3	ESSID	
4	Supported Rates	

4.2.3.7. Reassociation Response Frame Format

The Frame Body of a Management frame of Subtype Reassociation Response shall contain the following information:~~consist of a status value, an error indication and the station ID (SID) assigned.~~

Order	Information	Note
1	Capability Information	
2	Status Code	
3	Station ID (SID)	
4	Supported Rates	

4.2.3.8. Probe Request Frame Format

The Frame Body of a Management frame of Subtype Probe Response shall contain the following information:~~consist of the supported rates.~~

Order	Information	Note
1	Capability Information	
2	ESSID	
3	Supported Rates	

4.2.3.9. Probe Response Frame Format

The Frame Body of a Management frame of Subtype Probe Response shall contain the following information: ~~shall consist of time stamp, weight, beacon interval, DTIM period, DTIM count, channel sync information, supported rates and ESS ID.~~

Order	Information	Note
1	Timestamp	
2	Beacon Interval	
3	Regulatory Domain	
4	Capability Information	
5	ESS ID	
6	Supported Rates	
7	FH Parameter Set	1
8	CF Parameter Set	2

Notes:

1 The FH Parameter Set information shall be mandatory only within Probe Response Frames generated by STAs using Frequency Hopping Physical Layers

2 The CF Parameter Set information shall be mandatory only within Probe Response Frames generated by APs supporting a PCF

~~*4.2.3.10. Privacy Request Frame Format*~~

~~The Frame body of this frame shall consist of a supported algorithm list.~~

~~*4.2.3.11. Privacy Response Frame Format*~~

~~The Frame body of this frame shall consist of status value, an error indication and a privacy algorithm number.~~

4.2.3.12. Authentication Frame Format

The Frame Body of a Management frame of Subtype Authentication shall contain the following information:

Order	Information	Note
1	Authentication Algorithm Number	
2	Authentication Transaction Sequence Number	
3	Status Code	1
4	Challenge Text	2

Notes:

1 The Status Code information shall be reserved and set to 0 in the Authentication frames defined in the table below.

2 The Challenge Text Information shall only be present in the Authentication frames defined in the table below.

Authentication Algorithm Number	Authentication Trans. Sequence Number	Status Code	Challenge Text
Open System	1	reserved	not present
Open System	2	status	not present
Shared Key	1	reserved	not present
Shared Key	2	reserved	present
Shared Key	3	reserved	present
Shared Key	4	status	not present

~~The Frame Body of the Authentication frame shall comprise a transaction sequence and additional information dependent upon the value of the transaction sequence. If the transaction sequence is 1, the remainder of the Frame Body shall comprise the supported algorithm list. If the transaction sequence is 2, the remainder of the Frame Body shall comprise a status value, an error indication, an identity assertion and the selected authentication algorithm number. If the transaction sequence is 3, the remainder of the Frame Body shall comprise an identity challenge and an identity assertion. If the transaction sequence is 4, the remainder of the Frame Body shall comprise a challenge response and an identity challenge. If the transaction sequence is 5, the remainder of the Frame Body shall comprise, a challenge result and a challenge response. If the transaction sequence is 6, the remainder of the frame body shall comprise a challenge result.~~

4.2.3.13 *Deauthentication*

The Frame Body of a Management frame of Subtype Deauthentication shall contain the following information:

Order	Information	Note
1	Status Code	

4.2.3.14 *Connection Request*

The Frame Body of a Management frame of Subtype Connection Request shall contain the following information:

Order	Information	Note
TBD		

4.2.3.15 *Grant Connection*

The Frame Body of a Management frame of Subtype Grant Connection shall contain the following information:

Order	Information	Note
TBD		

4.2.3.16 *End Connection*

The Frame Body of a Management frame of Subtype End Connection shall contain the following information:

Order	Information	Note
TBD		

4.3. Frame Exchange Sequences

The following frame sequences are possible:

a) DATA
b) DATA - ACK
c) RTS - CTS - DATA - ACK
d) DATA - ACK - DATA - ACK (fragmented MSDU)
e) RTS - CTS - DATA - ACK - DATA - ACK (fragmented MSDU)
f) POLL - DATA - ACK
g) POLL - DATA - ACK - DATA - ACK (fragmented MSDU)
h) POLL - ACK (no data)
i) ATIM - ACK
j) REQUEST - ACK
k) RESPONSE - ACK

4.4. Management Frame Body Components~~Element Content Definitions~~

Within Management frames, fixed length mandatory frame body components are defined as fixed fields, variable length mandatory and all optional frame body components are defined as information elements.

4.4.1 Fixed Fields

4.4.1.1 Timestamp

This field shall represent the value of the TSFTIMER of a frame's source. The element specific field length is eight octets.

4.4.1.2 Beacon Interval

The Beacon Interval field shall represent the number of milliseconds between Beacon generations. The length of the Beacon Interval field is one octet.

4.4.1.3 Regulatory Domain

The Regulatory Domain field shall identify a regulatory domain. The following values are defined:

1 USA
2 Europe
3 Japan
All other values are reserved

The length of the Regulatory Domain field is one octet.

4.4.1.4 Capability Information

The Capability Information field contains a number of subfields that are used to indicate requested or advertised capabilties. The length of the Capability Information octet is one octet. The following subfields are defined:

Bit 0: Infrastructure BSS
Bit 1: Ad-hoc BSS
Bit 2: CF-aware
Bit 3: CF Polling Request
Bits 4 - 7: Reserved

4.4.1.5 Station ID (SID)

The Station ID (SID) field shall be a value assigned by an AP during association and shall represent the 16-bit ID of a station. The length of the SID field is two octets.

4.4.1.6 Current AP Address

The Current AP Address field shall be the MAC address of the access point with which the station is currently associated. The length of the Current AP Address field is six octets.

4.4.1.7 Authentication Algorithm Number

The Authentication Algorithm Number field shall indicate a single authentication algorithm. The length of the Authentication Algorithm Number field is two octets. The following values are defined:

Authentication Algorithm Number = 0: Open System
Authentication Algorithm Number = 1: Shared Key
All other values of Authentication Number shall be reserved.

4.4.1.8 Authentication Transaction Sequence Number

The Authentication Transaction Sequence Number field shall indicate the current state of progress through a multi-step transaction. The length of the Authentication Transaction Sequence Number is one octet.

4.4.1.9 Status Code

This Status Code shall be used to indicate the success of failure of an operation. The length of the status code field is one octet. If an operation is successful then the Status Code shall be set to 0. If an operation results in failure the Status Code shall indicate a failure cause. The following failure cause codes are defined: *TBD*

4.4.2 Information Elements

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

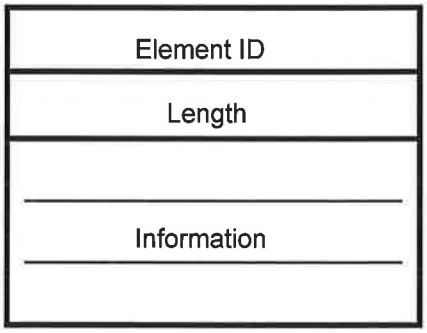


Figure 4-130, Element Format

The set of valid~~possible~~ elements is defined below. ~~For each element type, the size of element specific field is given.~~

Information Element	Element ID
ESSID	0
Supported Rates	1
FH Parameter Set	2
CF Parameter Set	3
DTIM	4
TIM	5
Challenge Text	6

~~4.4.1.Beacon Interval~~

~~This field shall represent the number of milliseconds between Beacon generations. The element specific field length is one octet.~~

4.4.2.1 DTIM ~~Count~~

The DTIM element shall contain two fields DTIM Count and DTIM Period.

Element ID	1 octet
Length	1 octet
DTIM Period	1 octet
DTIM Count	1 octet

The DTIM count~~is~~ field shall indicate how many Beacons~~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 a DTIM. The DTIM count field shall be a single octet. ~~The element specific field length is one octet.~~

~~4.4.3.DTIM Period~~

The~~is~~ DTIM period field shall indicate the number of Beacon~~TIM~~ intervals between successive DTIMs. If all TIMs are DTIMs, the DTIM Period field shall have value 1. The DTIM period field shall be a single octet. ~~The element specific field length is one octet.~~

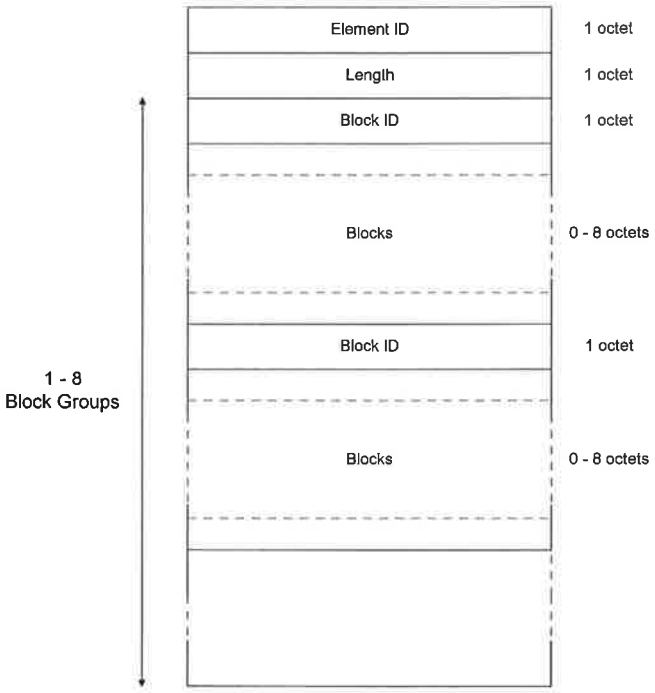
~~4.4.4.Broadcast Indicator~~

~~This field 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). The element specific field length is zero octets.~~

~~4.4.5.Station ID (SID)~~

~~This field shall be a value assigned by an AP during association representing the 16 bit Station ID of a station. The element specific field length is two octets.~~

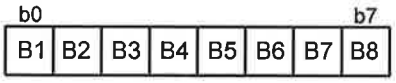
4.4.26.2 Traffic Indication Map (TIM)



The TIM Element information fField shall contain between one and eighta ~~variable number of~~ *block groups*, with each block group consisting of a *block identifier* followed by 0 to 87 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. The virtual bit map is maintained within the access point; the actual transmitted TIM is a compressed representation of the virtual bit map. ~~The element-specific field length is between one and eight octets~~.

Block Group: Consists of a Block Identifier followed by from 0 to 87 Blocks.

BI: Block Identifier (1 octet)



Bit N (N = 1..87) 0 = Nth block in this group is absent
1 = Nth block in this group is present
~~M: More0 = This is the last block group~~
~~1 = Another block group follows~~

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.

~~**4.4.7. Short Time Stamp**~~

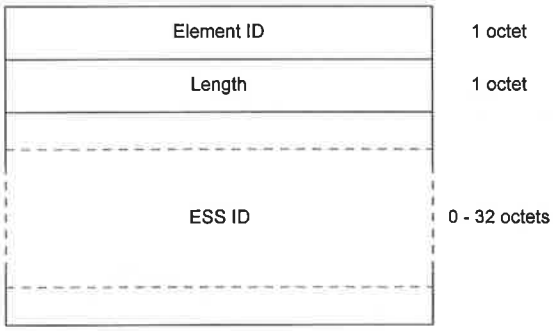
~~This field shall represent the value of the TSFTIMER of a frame's source. The element specific field length is four octets.~~

~~**4.4.8. Long Time Stamp**~~

~~This field shall represent the value of the TSFTIMER of a frame's source. The element specific field length is eight octets.~~

4.4.2.39. ESS ID

The ESSID element~~is field~~ shall indicate the identity of the Extended Service Set.



The ESSID Information field shall be between 0 and 32 octets. A zero octet information field shall indicate the broadcast ESSID. ~~The element specific field length is a variable number of octets.~~

~~**4.4.10. Request/Response Indicator**~~

~~This field shall be a boolean indicator. When the value of this field is true (1), the indication is for a response. When the value of this field is false (0), the indication is for a request. The element specific field length is zero octets.~~

~~**4.4.11. Privacy Algorithm Number**~~

~~This field shall indicate a single privacy algorithm as identified in 802.10xx. The element specific field length is two octets.~~

~~**4.4.12. Status Value**~~

~~This field shall be a boolean value indicating the success or failure of an operation. When this field is true (1), the indication is for success. When this field is false (0), the indication is for failure. The element specific field length is one octet.~~

~~**4.4.13. Error Indicator**~~

~~This field shall indicate a reason code for operations that resulted in a Status Value of failure. The element specific field length is zero octets.~~

~~**4.4.14. Current AP Address**~~

~~This field shall be the MAC address of the access point with which the station is currently associated. The element specific field length is six octets.~~

~~**4.4.15. Transaction Sequence**~~

~~This field shall indicate the current state of progress through a multi-step transaction. The element-specific field length is one octet.~~

~~**4.4.16. Supported Algorithm List**~~

~~This field shall indicate the list of privacy and/or authentication algorithms supported by a station. The element-specific field length is a variable number of octets.~~

~~**4.4.17. Authentication Algorithm Number**~~

~~This field shall indicate a single authentication algorithm as identified in 802.10xx. The element-specific field length is two octets.~~

~~**4.4.18. Identity Challenge**~~

~~This field shall be the bit string used to challenge the identity of a station during the authentication process. The element-specific field length is a variable number of octets.~~

~~**4.4.19. Challenge Response**~~

~~This field shall be the bit string resulting from the response to the Identity Challenge during the authentication process. The element-specific field length is a variable number of octets.~~

~~**4.4.20. Challenge Result**~~

~~This field shall be a bit string resulting from the processing of the Challenge Response during the authentication process. The element-specific field length is a variable number of octets.~~

~~**4.4.21. Regulatory Domain**~~

~~This field shall identify a regulatory domain from the following list:~~

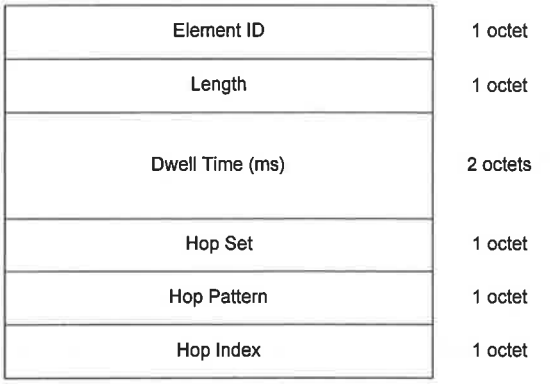
~~1.~~

~~The element specific field length is one octet.~~

~~*[Editor's note (GE): Need list of domains]*~~

4.4.2.4~~22.~~ *FH Parameter Set*

The FH Parameter Set element shall contain the set of parameters necessary to allow synchronisation for STAs using a Frequency Hopping (FH) Physical Layer. The information field shall contain Dwell Time, Hop Set, Hop Pattern and Hop Index parameters. The total length of the information field shall be 5 octets.



The Dwell Time field shall be two octets in length and contain the Dwell Time in ms.~~Set~~

The Hop Set field~~is field~~ shall identify the particular set of hop patterns and shall be a single octet.~~. The element specific field length is one octet.~~

~~4.4.23. Pattern~~

The Hop Pattern~~is~~ field shall identify the individual pattern within a set of hop patterns and shall be a single octet. ~~The element specific field length is one octet.~~

~~4.4.24. Index~~

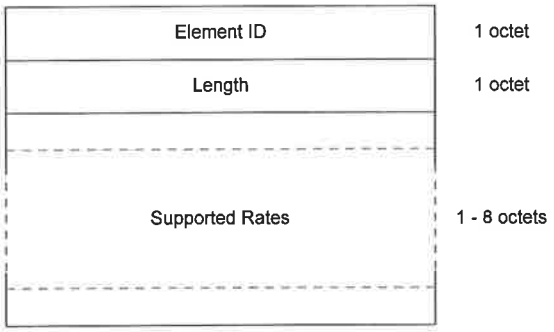
The Hop Index~~is~~ field shall select the channel index within a pattern and shall be a single octet.~~The element specific field length is one octet.~~

~~4.4.25. Hop Timing~~

~~This field shall provide a time reference to the station regarding the current hop sequence. The first field is a 32 bit time in microseconds from the beginning of the hop pattern to the time reference of the frame that includes this element. The second field is a 32 bit time in microseconds for the length of a hop. The element specific field length is eight octets.~~

4.4.2.5~~6.~~ Supported Rates

The Supported Rates element~~is field~~ shall specify all the rates in which this station is capable to receive. The information field~~It~~ is encoded as 1 to 8~~a variable number of~~ octets where each octet describes a single supported rate in units of 100 kbit/s (e.g. a 1 Mbps rate will be encoded as 0x0A).



~~The element specific field length is a variable number of octets.~~

~~**4.4.27. Payload**~~

~~This field shall contain two subfields, the maximum payload and the mean request interval. The maximum payload shall specify the maximum number of bytes that may be sent as the payload of a time-bounded data packet. This subfield shall be two octets. The mean request interval subfield shall specify the mean interval between requests for time bounded service. The value of this subfield shall be measured in milliseconds. The length of this subfield shall be one octet. The element specific length of the Payload information element is three octets.~~

4.4.2.6~~28~~. Connection ID

The Connection ID element~~is field~~ shall be used to specify a unique identifier for a time bounded connection to transfer data between an access point and a station. Each connection ID shall be unique for a given station. The element specific field length is two octets.

[needs work - SAB]

4.4.2.7 CF Parameter Set

The CF Parameter Set element shall contain the set of parameters necessary to support the PCF. The information field shall contain CF Maximum Duration and ?? parameters. The total length of the information field shall be n octets.

[needs work - SAB]

4.4.2.8 Challenge Text

The Challenge Text element shall contain the challenge text within Authentication exchanges. The element information field shall be 128 octets in length.

[needs work - SAB]

4.3. Frame Exchange Sequences

The following frame sequences are valid:

a) DATA
b) DATA-DATA (fragmented broadcast MSDU)
c) DATA - ACK
d) RTS - CTS - DATA - ACK
e) DATA - ACK - DATA - ACK (fragmented MSDU)
f) RTS - CTS - DATA - ACK - DATA - ACK (fragmented MSDU)
g) POLL - DATA - ACK
h) POLL - DATA - ACK - DATA - ACK (fragmented MSDU)
i) POLL - ACK (no data)
j) REQUEST - ACK
k) RESPONSE - ACK