IEEE 802.11
Wireless Access Method and Physical Layer Specification

Title: **MAC Frame Formats**

Presented By: Chris Zegelin
Tel: (408) 369-2667
Email: chrisz@psd.symbol.com

Symbol Technologies
1101 S. Winchester Blvd.
San Jose, CA. 95128

Sarosh Vesuna, Greg Ennis

Abstract: **This paper proposes a frame format for the 802.11 MAC.**

Introduction: **The goal of this paper is to provide a clean up of the existing draft standard. Fields have been moved and consolidated with an emphasis on not changing or adding to existing functionality. Additional text has been added to clarify fields and their use.**

An inconsistency exists concerning the Contention Free frames. The standard is in limbo concerning the use or not of the method. This paper did not attempt to fix the inconsistencies.

1. General

2. General Description

3. MAC Services Definition

4. Frame and MSDU Formats

4.1. Basic Frame Format

Each frame shall consist of the following basic components:

1) A fixed-length *Fixed Header*, which includes a Version Field, a frame Type field, a Control field, the Network ID (NID) and an MSDU-ID.

2) A variable length field the format of which contains a (possibly empty) set of optional *elements.*

3) A variable length *Frame Body*, including

   a) A (possibly empty) set of *type-dependent fields.*

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

   c) A variable length Data field for *Data Frames*. DATA Frames may be fragments of an MSDU. These fragments are created and reassembled by the MAC management entity.

4) An IEEE 32-bit CRC.

4.1.1. PHY dependencies

The protocol is intended to work with many different PHY layers. Each layer has its own set of management and configuration needs. These special needs are accommodated using the optional Element fields that may be present in any frame. The basic frame formats thus remain common across all PHY's.

4.1.2. Fixed Header

The Fixed Header is the collection of fields at the beginning of each frame that is consistent for all frame types.

4.1.3. Elements

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. These are defined in Section 4.4.

This basic mechanism is used to convey information that may or may not need to be present in any given frame type. The mechanism is consistent for all Elements so that a Element that is either not recognized or not needed can be discarded while retaining the remainder of the frame. This allows for both PHY independent implementations of MAC level controllers and a possibility for backwards compatibility in the event that this standard is modified sometime in the future (A new PHY).

4.1.4. Fragmentation

Fragmentation of an MSDU is an integral part of the protocol. The basic methodology is that fragments are sent in consecutive DATA frames with a positive acknowledgment between each one.

4.1.5.General Frame Format Diagram

Figure 4-1 depicts the general frame format. 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.

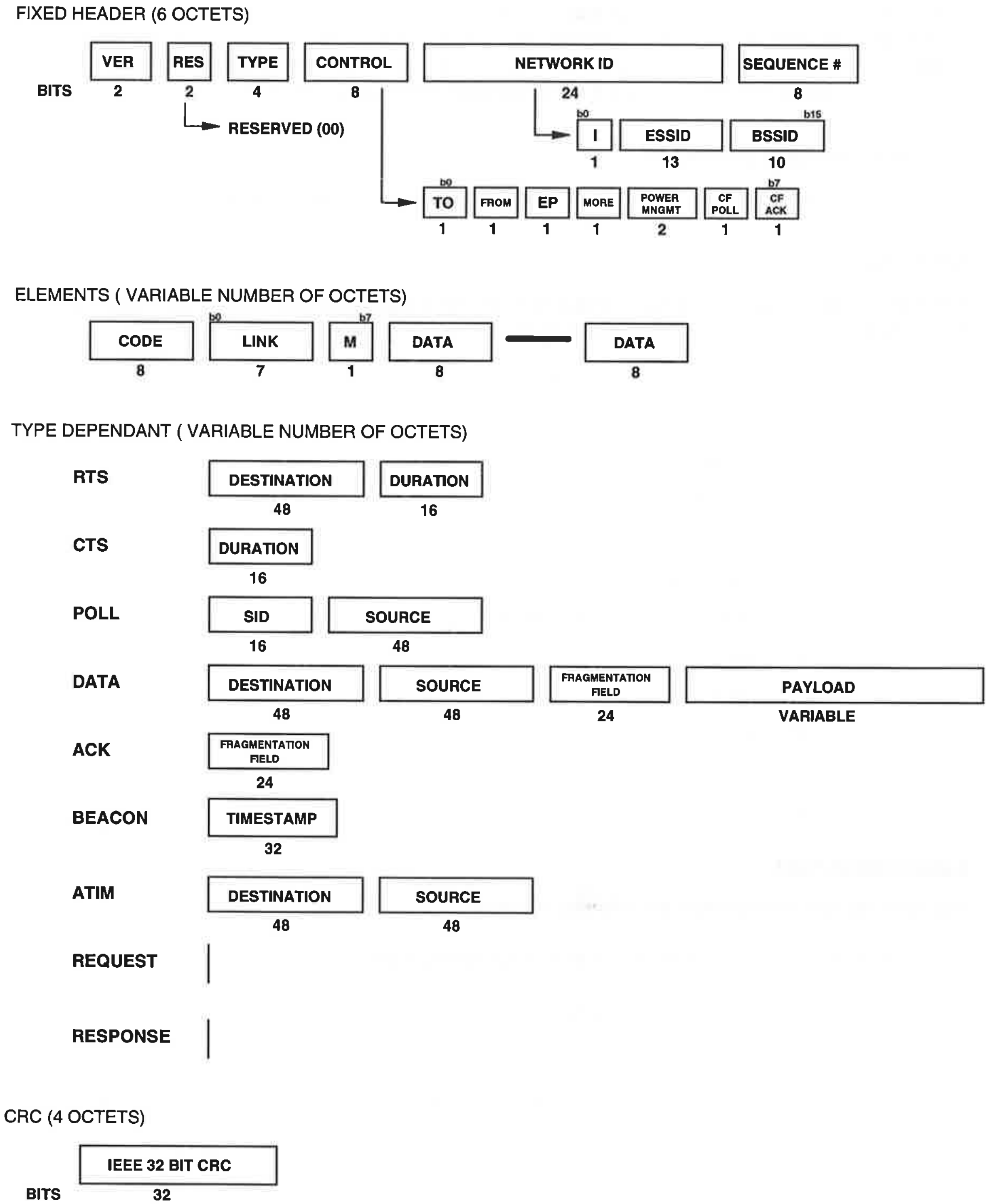


Figure 4-1, General MAC Frame Format

4.2. Frame Fields

4.2.1. Protocol Version

This 2 bit field is invariant in size and placement across all revisions of the 802.11 standard. The values shall be assigned sequentially starting with the value 1. The revision level is incremented only when a fundamental incompatibility exists between a lower revision and the current standard. A device that receives a frame with a higher revision level than it can understand should discard the frame.

4.2.2. Reserved Bits and Fields

All reserved bits and fields must be sent as '0'. They should be ignored on reception.

4.2.3. Type

The TYPE field indicates the contents (or lack there of) of the type dependent fields in the frame. The TYPE shall take one of the following hexadecimal values:

1	RTS (Request to Send)
2	CTS (Clear to Send)
3	POLL
4	DATA
5	ACK
8	BEACON
9	ATIM (Ad-hoc Traffic Indication Map)
A	REQUEST
B	RESPONCE
C	CF-Up
D	CF-Down
E	CF-ACK

4.2.4. Control Field

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

CACK	Contention free service acknowledgment
CPOLL	Contention free service poll

Power Management Mode

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

00	CAM
01	PSP
10	PSNP
11	TAM

MORE — Indicates that additional data frames are buffered within the AP for the destination.

EP — Indicates that elements are in the frame.

FROM AP — This bit shall be set to 1 whenever a frame is transmitted by the AP, and shall be set to 0 otherwise.

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

4.2.4.1. Network ID

The Network ID (NID) is a 3-octet 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.

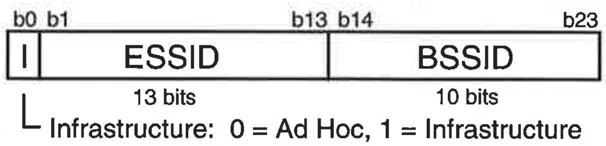


Figure 4-xx, NID Format

The contents of the ESS-ID field and the BSS-ID fields are arbitrary with the understanding that for Infrastructure mode: A station will usually only associate with Access Points that have the same ESS-ID. This is not a requirement of the protocol. The BSS-ID is unique to an Access Point within an ESS.

The methodology for setting the values for the ESS-ID and BSS-ID are left to the system implementation.

4.2.5.Sequence Number/ConnID

This 8 bit field shall contain the Sequence Number for asynchronous frames and the Connection ID for asynchronous contention free frames. The Sequence Number value is chosen by the station or AP that initiates the data transfer. The contents may be any arbitrary value consistent with the goal of being able to significantly reduce the propagation of duplicate packets.

The same Sequence Number is used for all aspects of a data transfer. It is included in the optional RTS and CTS frames, as well as the DATA and ACK frames. Fragments of a MSDU are all assigned the same Sequence Number. The Sequence Number in a POLL frame is used for the subsequent DATA and ACK frames, and the Sequence Number used during a REQUEST is returned in the RESPONSE.

Asynchronous contention free ConnectionIDs are assigned when the station requests asynchronous contention free service in a management Request message.

4.2.6.Elements

The *Elements* always follow the fixed header when they exist in a frame. The basic frame format allows the inclusion of elements in all frame types, however the currently defined elements will only occur in specific frame types.

The format of an element shall include a one octet Code field, a one bit More indicator, and a seven bit Link field, followed by a variable length data field. The Link field indicates the number of data octets in the element. Some code fields do not need any data, so the Link field may contain a value of zero.

The implementation should ignore elements that are not defined or are not needed for a given implementation, yet still complete the processing of the element. This mechanism will allow for PHY independent MAC controllers and to maintain the possibility of backward compatibility for future revisions of this specification.

NOTE: A device may not claim compliance with this specification if it violates either of the following rules:

1) A device may not transmit an Element that is not defined in the specification.
2) A device must ignore any undefined Element that it might receive while continuing to accept the remainder of the frame.

4.2.7.Address Fields

Each MAC Frame may contain a combination of the following address fields depending on the type of MAC Frame, see 4.1.xx Type designation for field usage. The relative order of the Address fields will always be DEST followed by SRC. Relative order will be maintained even if one or more are not included in a particular type MAC Frame.

4.2.7.1. 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.

4.2.7.2. DEST & SRC Address Representation

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

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

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

b) 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.

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

3) 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).
4) 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

4.2.8. Type-Dependent Fields

Additional type-dependent fields shall be present, depending upon the frame type. The following are defined:

Duration: The duration field is provided to allow a station or AP to keep an accurate NAV. The field contains the sum of time in microseconds for a frame's transmission, the time for a maximum SIFS, and the time for a subsequent acknowledgment, if any.

Fragment: The fragment field provides the state of a fragmented MSDU. The three octets contain three sub-fields, a bit to indicate subsequent fragments, and a fragment number to indicate which fragment is being provided, and a duration field. Fragments are never sent out of sequence.

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

Timestamp The timestamp is provided in a Beacon frame to provide a time reference for a BSS. The AP keeps a free running time in units of microseconds. The timestamp field contains the value of the free running time at the point when the last bit of the SFD is transmitted for the Beacon frame.

Station ID This field is a short address for a power saving station that indicates which bit in the TIM is intended for the station. This ID is passed to the AP in a POLL frame to cross check the ID with the station address.

4.2.9. Frame Check Sequence (FCS) Field (CRC)

The FCS is a 32-bit frame checking sequence, based upon the following standard generator polynomial of degree 32:

$$X^{32} + X^{26} + X^{23} + X^{22} + X^{16} + X^{12} + X^{11} + X^{10} + X^{8} + X^{7} + X^{5} + X^{4} + X^{2} + X + 1$$

The FCS is the one's complement of the sum (modulo 2) of

1. The remainder of $X^K * (X^{31} + X^{30} + X^{29} + \ldots\ldots + X^2 + X + 1)$, divided (modulo 2) by the standard 32-bit generating polynomial, where K is the number of bits in the Frame Control, address (SA and DA), and MAC Data-Unit fields, and

2. The remainder of the division (modulo 2) by the standard generator polynomial of the product of X^{12} by the content of the Frame Control, address (SA and DA), and MAC Data-Unit fields.

The FCS is transmitted commencing with the coefficient of the highest degree term.

As a typical implementation, at the transmitter, the initial content of the register of the device computing the remainder of the division is preset to all ones and is then modified by the generator polynomial (as described above) on the frame control, address, and information fields. The one's complement of the resulting remainder is transmitted as the 32-bit FCS sequence.

At the receiver, the initial content of the register of the device computing the remainder is preset to all ones. The serial incoming protected bits and the FCS, when divided by the generator polynomial, result, in the absence of transmission errors, in a unique non zero remainder value. The unique remainder value for the 32-bit FCS is the polynomial:

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

NOTE: To test the FCS generation and checking logic in a station, an implementation should provide a means of bypassing the FCS generation circuitry and providing an FCS from an external source. The ability to pass frames that have FCS errors along with the received FCS value and an error indication, to higher levels of the protocol, is another desirable testability feature.

4.2.10. Fragmentation Field

The fragmentation field consists of three octets contain three sub-fields, a bit to indicate subsequent fragments, and a fragment number to indicate which fragment is being provided, and a duration field.

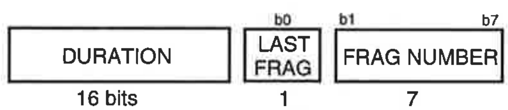


Figure 4-xx: Fragmentation Field

The fields are defined as follows:

Duration: The duration field is provided to allow a station or AP to keep an accurate NAV. The field contains the sum of time in microseconds for the next fragment frame's transmission including any pre-amble, the time for two maximum SIFS, and the time for a subsequent acknowledgment, if any. This field is NULL if this is the last fragment of the MSDU

Last Frag: This bit is set to a 1 if this is the last fragment of the MSDU.

Frag Num: This field is the binary representation of the fragment number of the MSDU (fragment 1 - 0000001, fragment 2 - 0000010, ...)

4.3. Type Dependent Frame Formats

4.3.1. RTS Frame Format

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

FIXED HEADER	DEST	Duration	CRC32
6 octets	6	2	4

Figure 4-xx: RTS Frame

The fields of the data frame are defined as follows:

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

Duration: This field is the sum of the time for this RTS, a CTS, the DATA frame, an ACK frame, and 3 Max_SIFS. The start time is the standard time reference of "the end of the last bit of the SFD as it is transmitted to the airwaves". The time units are microseconds.

4.3.2. CTS Frame Format

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

FIXED HEADER	Duration	CRC32
6 octets	2	4

Figure 4-xx: CTS Frame

The fields of the data frame are defined as follows:

Duration: This field is the sum of the time for this CTS, the DATA frame, an ACK frame, and 2 Max_SIFS. The start time is the standard time reference of "the end of the last bit of the SFD as it is transmitted to the airwaves". The time units are microseconds.

4.3.3. POLL Frame Format

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

FIXED HEADER	SID	SRC	CRC32
6 octets	2	6	4

Figure 4-xx: POLL Frame

The fields of the data frame are defined as follows:

SID: This field is the 16 bit Station ID.

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

4.3.4. DATA Frame Format

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

FIXED HEADER	DEST	SRC	Fragmention Field	Payload	CRC32
6 octets	6	6	3	1 to aFragment_Payload	4

Figure 4-xx: DATA Frame With Fragmentation

The fields of the data frame are defined as follows:

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: This field describes the fragment. It contains the fragment number, a flag to indicate last fragment, and the duration field. The field is NULL if the MSDU is not fragmented.

Payload: This field is all or part of a MSDU. It ranges in size from 1 to aPayload_Max or aFragment_Payload octets.

4.3.5. ACK Frame Format

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

FIXED HEADER	Fragmention Field	CRC32
6 octets	3	4

Figure 4-xx: ACK Frame With Fragmentation

The field of the ACK frame are defined as follows:

Fragment: This field describes the fragment. It contains the fragment number, a flag to indicate last fragment, and the duration field. This field is copied from the data frame that is being acknowledged. The field is NULL if the MSDU is not fragmented, or if a frame other than a DATA type is being acknowledged.

4.3.6. BEACON Frame Format

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

FIXED HEADER	Elements	TimeStamp	CRC32
6 octets	Variable	4	4

Figure 4-xx: BEACON Frame

The fields of the BEACON frame are defined as follows:

TimeStamp: This field contains a time reference. The standard time reference for all frames is "the end of the last bit of the SFD as it is transmitted to the airwaves". The

TimeStamp is the value of a free running 32 bit timer at the reference point for this BEACON frame. The time units are microseconds.

4.3.7. ATIM Frame Format

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

FIXED HEADER	DEST	SRC	CRC32
6 octets	6	6	4

Figure 4-xx: ATIM Frame

The fields of the ATIM frame are defined as follows:

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

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

4.3.8. REQUEST Frame Format

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

FIXED HEADER	Elements	CRC32
6 octets	Variable	4

Figure 4-xx: REQUEST Frame

The Elements in a REQUEST frame may include an ASSOCIATE element, and optionally a PREVIOUS AP element, or a PROBE element.

4.3.9. RESPONSE Frame Format

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

FIXED HEADER	Elements	CRC32
6 octets	Variable	4

Figure 4-xx: RESPONSE Frame

The Elements in a RESPONSE frame may include an ASSOCIATE element, in which case a STATION ID, DTIM period, and BEACON Interval elements will be included. A PROBE response element will include a TIMESTAMP.

4.4. MAC Service Data Units (MSDU)

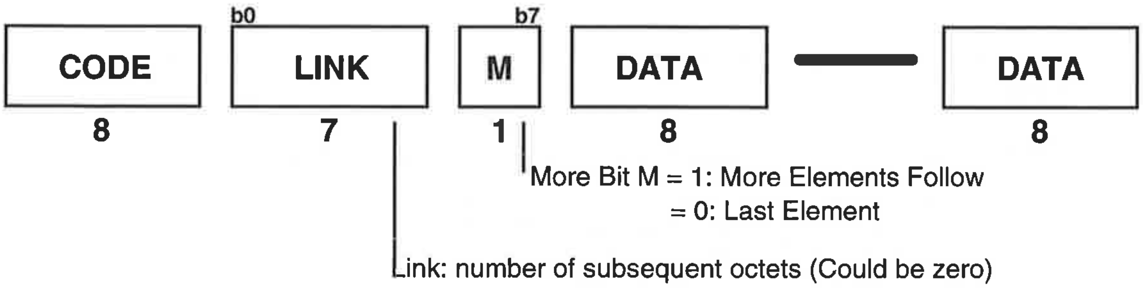
A MAC Service Data Unit (MSDU) is defined as a sequence of one or more frames which are transmitted successively to accomplish a single function. The frame sequences which can make up a valid MSDU are as follows:

1. DATA
2. DATA - ACK
3. RTS - CTS - DATA - ACK
4. DATA - ACK - DATA - ACK (fragmented MSDU)
5. RTS - CTS - DATA - ACK - DATA - ACK (fragmented MSDU)
6. POLL - DATA - ACK
7. POLL - DATA - ACK - DATA - ACK (fragmented MSDU)
8. POLL - ACK (no data)
9. ATIM - ACK
10. REQUEST - ACK
11. RESPONSE - ACK

The frames within an MSDU shall contain the same MSDU-ID.

4.5. Element Definitions

The general format of all elements is defined as follows:



Defined elements include the following:

CODE	ELEMENT
0	No Operation
1	BEACON INTERVAL
2	DTIM COUNT
3	DTIM PERIOD
4	BROADCAST INDICATOR
5	STATION ID
6	TRAFFIC INDICATOR MAP (TIM)
7	PROBE
8	SOURCE NID
9	ASSOCIATE
10	WEIGHT

4.5.1. Beacon Interval

One octet, representing number of milliseconds between Beacon generations.

4.5.2. DTIM Count

One octet. 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.

4.5.3. DTIM Period

One octet. This element shall indicate the number of TIM intervals between successive DTIMs. If all TIMs are DTIMs, the DTIM Period element shall have value 1.

4.5.4. Broadcast Indicator

Zero octets. If present, this element 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).

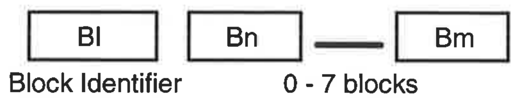
4.5.5. Station ID

Two octets, representing the 16-bit Station ID of a station.

4.5.6.Traffic Indication Map (TIM)

This Element has a variable number of octets. 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. The virtual bit map is maintained within the access point; the actual transmitted TIM is a compressed representation of the virtual bit map.

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



BI: Block Identifier (1 octet)

b0							b7
B1	B2	B3	B4	B5	B6	B7	M

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

1 = Nth block in this group is present

M: More 0 = 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.

4.5.7.Probe

Zero octets. Used only in Request or Response frames. This element, if present, shall indicate that the frame is a Probe Request or a Probe Response.

4.5.8.Source NID

Three octets. Represents source NID of transmitting station. Used in Probe Responses.

4.5.9.Associate

Zero octets. If present in a REQUEST frame generated by a station, this element shall indicate a desire on the part of the station to associate with a given access point. If present in a RESPONSE frame generated by an access point, this element shall indicate that this is a response to a prior association request.

4.5.10. Weight

Two octets. 16 bit value indicating weight of station. Used within Beacons and Probe Responses.

4.6. Elements Within the Frame Types

The formats of the frame types shall consist of the basic format (defined in 4.1) with specific values within the Type field as defined in Section 4.3. The various types shall also include elements as described below.

RTS	There are no mandatory elements for an RTS.
CTS	There are no mandatory elements for a CTS.
POLL	The *StationID* element is mandatory.
DATA	There are no mandatory elements for a DATA.
ACK	There are no mandatory elements for an ACK.
BEACON	The *TIM, DTIM Period,* and *Broadcast* element may be present.
ATIM	There are no mandatory elements for an ATIM.
REQUEST	If an *Associate* element is present, then the *Previous AP Address* element must also be present.
RESPONSE	If an Associate element is present, then the *Timestamp*, *Station ID*, *DTIM Period,* and *Beacon Interval* elements must also be present. A Probe Response includes *Weight*, *Timestamp*, and *Source NID.*

4.7. Parsing a Receive Frame

The following flow chart provides a general guide to how a machine might parse an incoming frame.