IEEE 802.11
Wireless Access Method and Physical Layer Specification

Title: **Draft text for MAC Frame Formats with Encodings**

Rick White
Mark Demange

Motorola, Inc.
50 East Commerce Drive
Schaumberg, IL 60173

Bob O'Hara
Dave Roberts
Dave Bagby

Advanced Micro Devices
One AMD Place
Sunnyvale, CA 94088

Jon Rosdahl

Novell, Inc.
122 East 1700 South
Provo, UT 84003

Abstract: **This paper builds on 94/213, adding draft standard text for the information encoding presented in 94/215a.**

1. General

1.6 Conventions

1. This standard represents information fields as octet strings of various lengths. The least significant bit (LSB) of each octet is defined as bit zero (0) for that octet. All octets are represented in figures with the LSB on the right.

2. General Description

3. MAC Services Definition

4. Frame and MPDU Formats

4.1. MAC Frame Formats

Each frame shall consist of the following basic components:

1) A *MAC Header*, which includes control information, addressing, sequencing, fragmentation identification and duration.
2) A variable length *Frame Body*, that may contain information specific to various frame *types*.
3) 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 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.

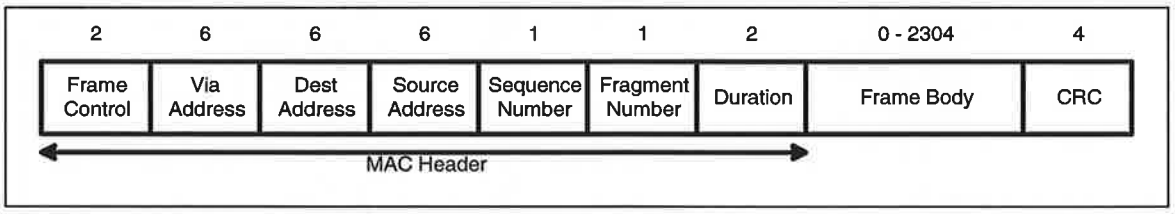


Figure 4-1: MAC Frame Format

4.1.2. Frame Fields

4.1.2.1. Frame Control Field

The Frame Control field shall consist of the following subfields: Protocol Version, Type, Subtype, To AP, More, Retry, Power Management, CF ACK, and CF Poll. The remaining subfields in the Frame Control field are reserved. All reserved bits and fields shall be sent as '0'. Reserved bits and fields shall be ignored on reception.

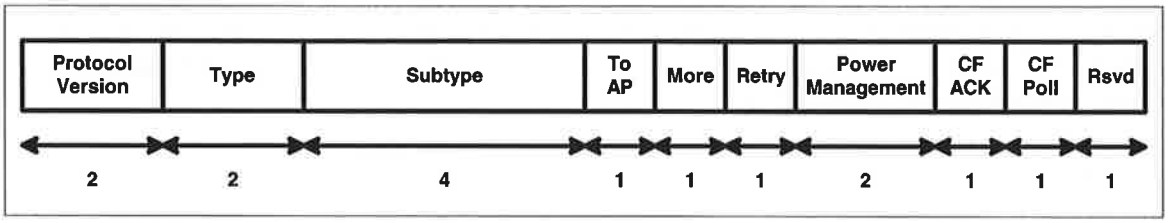


Figure 4-2: Frame Control Field

4.1.2.1.1. Protocol Version

This two bit field shall be invariant in size and placement across all revisions of the 802.11 standard. 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 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.

4.1.2.1.2. Type and Subtype

The Type and Subtype fields shall identify the function and interpretation of a frame. There are three frame types: control, data and management. Each of the frame types may have several subtypes. The table below lists the valid combination of Type and Subtype.

Type Value	Type Description	Subtype Value	Subtype Description
00	Management	0000	Power Save Poll
00	Management	0001	Beacon
00	Management	0010	ATIM
00	Management	0011	Probe
00	Management	0100	Association
00	Management	0101	Reassociation
00	Management	0110	Disassociation
00	Management	0111	Authentication
00	Management	1000	Privacy
00	Management	1001-1111	Reserved
01	Data	0000	Asynchronous Data
01	Data	0001	CF Up
01	Data	0010	CF Down
01	Data	0011-1111	Reserved
10	Control	0000	RTS
10	Control	0001	CTS
10	Control	0010	ACK
10	Control	0011	CF ACK
11	Reserved	0000-1111	Reserved

Table 4-1: Valid Type/Subtype Combinations

4.1.2.1.3. To AP

This one bit field shall indicate that the frame is destined for the access point in an infrastructure network. This bit shall be transmitted as a one when the frame is destined for the access point, either directly to the AP's destination address or to another station via the distribution system services provided by the AP. It shall be transmitted as a zero, otherwise.

4.1.2.1.4. More

This one bit field shall indicate that the AP holds additional frames buffered for the station identified by the destination address of the frame. This bit shall only be set by an AP when a frame is being transmitted to a destination address for which there are additional frames buffered.. A station shall always transmit this bit as a zero.

4.1.2.1.5. Retry

This one bit field shall indicate that the frame is a retransmission of an earlier frame. A station may use this indication to aid in the process of eliminating duplicate frames.

4.1.2.1.6. Power Management

This two bit field shall indicate the power management state in which the station will be after the completion of the transmission of the frame. The values for this field are given in table 4-2.

Value	Description
00	CAM - Continuous Active Mode
01	PSP - Power Save, Polling
10	PSNP - Power Save, No Polling
11	TAM, Temporary Active Mode

Table 4-2: Power Management Values

4.1.2.1.7. CF ACK

This one bit field shall be used to acknowledge the previously received frame in a stream of contention free data frames. If the immediately prior frame in a contention free burst was received successfully, the station shall transmit this bit as a one to acknowledge the frame reception. Otherwise, this bit shall be transmitted as a zero.

4.1.2.1.8. CF Poll

This one bit field shall act as a "clear to send" for a contention free data stream. If a station is prepared to receive a contention free data stream, it shall transmit this bit as a one in a contention free frame. Otherwise, this bit shall be transmitted as a zero.

4.1.2.1.9. Reserved

This one bit field is reserved. It shall be transmitted as a zero. Upon receipt, it shall be ignored.

4.1.2.2. Address Fields

There are three address fields in the MAC frame format, Via Address, Destination Address and Source Address. Some frames may omit some of the address fields.

4.1.2.2.1. Address Representation

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

4.1.2.2.2. Address Designation

A MAC Sublayer address is of one of two types:

1) Individual Address. The address associated with a particular station on the network.
2) Group Address. A Multidestination address, associated with one or more stations on a given 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.

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)

4.1.2.2.3. Via Address

The Via Address (VA) 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 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 address of the source station. The Individual/Group bit of the address shall be transmitted as zero.

4.1.2.2.4. Destination Address

The Destination Address (DA) field shall identify the destination addressee(s) for which the frame is intended.

4.1.2.2.5. Source Address

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.

4.1.2.3. Sequence Number

This 8 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. Fragment Number

The Fragment Number is an 8-bit field. It shall consist of a 1-bit subfield to indicate the last fragment and a 7-bit subfield for the number of each individual fragment. The format of this field is shown in figure 4-4.

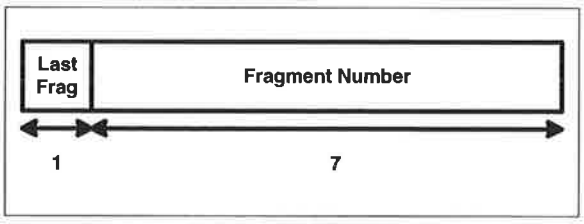


Figure 4-4: Fragment Number Field

4.1.2.5. Duration

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.

4.1.2.6. Frame Body

The Frame Body is a variable length field that may vary from zero to 2304 bytes. Information specific to individual frame types and subtypes shall be placed in the Frame Body.

4.1.2.7. CRC

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.

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

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.

4.2. Format of Individual Frame Types

4.2.1.Control Frames

4.2.1.1. RTS Frame Format

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

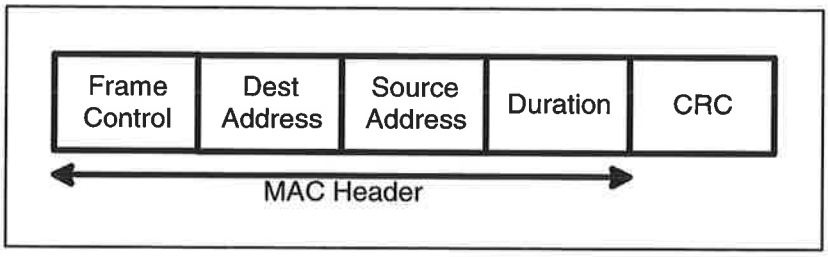


Figure 4-xx: RTS Frame

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

4.2.1.2. CTS Frame Format

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

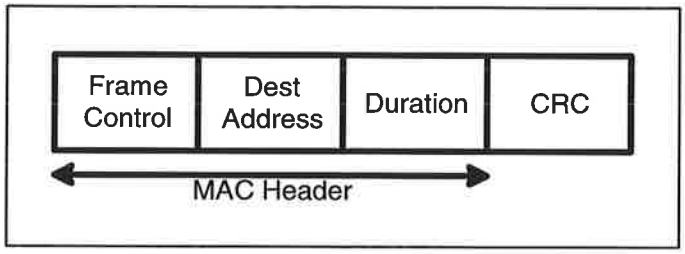


Figure 4-xx: CTS Frame

The destination address of the CTS frame shall be taken from the source address field of the RTS frame to which the CTS is a response.

4.2.1.3. ACK Frame Format

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

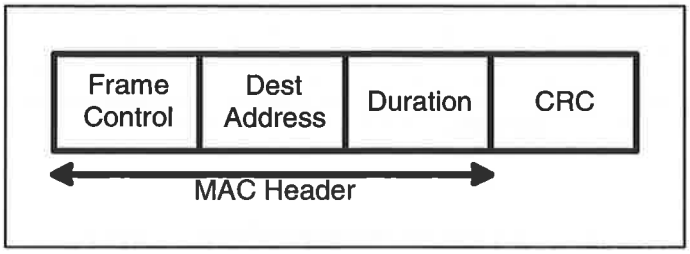


Figure 4-xx: ACK Frame

The destination address of the ACK frame shall be the source address field of the immediately previous data or management frame, if the station is an AP. The destination address shall be the Via address of the immediately previous data or management frame, if the station is not an AP.

4.2.2.Data Frames

4.2.2.1. DATA Frame Format

The frame format for a Data frame is independent of subtype and is shown in Figure 4-xx.

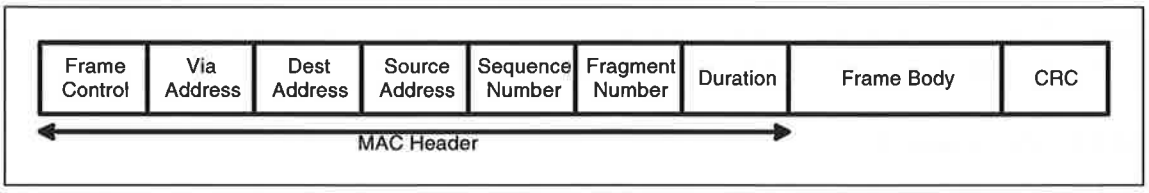


Figure 4-xx: DATA Frame

The Via Address of the Data frame shall be determined as follows:

1) If the station is an AP or is a member of an infrastructure LAN, the Via Address shall be the address of the AP.
2) If the station is a member of an ad hoc LAN, the Via Address shall be the address of the station transmitting the frame.

The Destination Address shall be the destination of the frame, i.e. the destination of the MSDU.

The Source Address shall be the address of the station transmitting the frame.

The Frame Body shall be the MSDU or a fragment thereof.

4.2.3.Management Frames

The frame format for a Management frame is independent of subtype and is shown in Figure 4-xx.

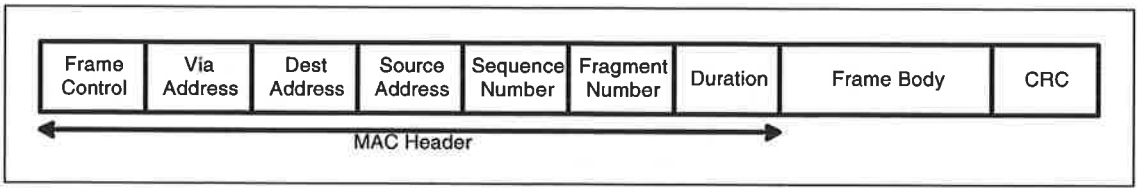


Figure 4-xx: Management Frame Format

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

The Via Address of the Management frame shall be determined as follows:

1) If the station is an AP or is in an infrastructure LAN, the Via Address shall be the address of the AP.
2) If the station is in an ad hoc LAN, the Via Address shall be the address of the station transmitting the frame.

The Destination Address shall be the ultimate destination of the frame, i.e. the destination of the MSDU.

The Source Address shall be the address of the station transmitting the frame.

Certain Management frame types require that specific frame body fields be present in a specific order. These are defined in Section 4.2.3.n.

4.2.3.1. POLL Frame Format

The Poll Frame Body shall consist of the following fields transmitted in the following order; the Station ID (SID).

4.2.3.2. BEACON Frame Format

The Frame Body shall consist of the following fields transmitted in the following order; time stamp, weight, beacon interval, DTIM period, DTIM count, channel sync information, ESS ID, TIM and broadcast indicator.

4.2.3.3. ATIM Frame Format

The Frame Body shall consist of the following fields transmitted in the following order; Null.

4.2.3.4. Probe Frame Format

The Frame Body shall consist of the following fields transmitted in the following order; A request/response indicator, subsequent information dependent on the value of the request/response field. If the frame is a Probe Request, the remainder of the Frame Body shall be Null. If the frame is a Probe Response, the remainder of the Frame Body shall be: time stamp, weight, beacon interval, DTIM period, DTIM count, channel sync information and ESS ID.

4.2.3.5. Association Frame Format

The Frame Body shall consist of the following fields transmitted in the following order; a request/response indicator and additional fields dependent on the value of the request/response field. If the frame is an Association Request, the Frame Body shall be a privacy algorithm number. If the frame is an Association Response, the remainder of the Frame Body shall be a status value, and the station ID assigned (SID).

4.2.3.6. Reassociation Frame Format

The Frame Body shall consist of the following fields transmitted in the following order; a request/response indicator and additional fields dependent on the value of the request/response field. If the frame is a Reassociation Request, the Frame Body shall be: the current AP address and the privacy algorithm number. If the frame is a Reassociation Response, the remainder of the Frame Body shall be: a status value, and the station ID (SID) assigned.

4.2.3.7. Disassociation Frame Format

The Frame Body shall consist of the following fields transmitted in the following order; Null.

4.2.3.8. Privacy Frame Format

The Frame Body shall consist of the following fields transmitted in the following order; a transaction sequence and additional frames dependent upon the value of the transaction sequence field. If the transaction sequence is 1, the Frame Body shall be: a supported algorithm list. If the transaction sequence is 2, the Frame Body shall be: a status value, and a privacy algorithm number.

4.2.3.9. Authentication Frame Format

The Frame Body shall consist of the following fields transmitted in the following order; a transaction sequence and additional frames dependent upon the value of the transaction sequence. If the transaction sequence is 1, the remainder of the Frame Body shall be: the supported algorithm list. If the transaction sequence is 2, the remainder of the Frame Body shall be: a status value, and the selected authentication algorithm number. If the transaction sequence is 3, the remainder of the Frame Body shall be: an identity challenge and an identity assertion. If the transaction sequence is 4, the remainder of the Frame Body shall be: a challenge response and an identity challenge. If the transaction sequence is 5, the remainder of the Frame Body shall be: a challenge result and a challenge response. If the transaction sequence is 6, the remainder of the frame body shall be: a challenge result.

4.3. 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.

4.4. Frame Body Field Definitions

The fields used within Management Frame Bodies are defined. The set of possible fields is defined below.

4.4.1.Null

This field shall be used for frame bodies which do not contain any other fields. The field length is zero octets.

4.4.2.Beacon Interval

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

4.4.3.DTIM Count

This field 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 a DTIM. The field length is one octet.

4.4.4.DTIM Period

This field shall indicate the number of TIM intervals between successive DTIMs. If all TIMs are DTIMs, the DTIM Period field shall have value 1. The field length is one octet.

4.4.5.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 field length is zero octets.

4.4.6.Station ID

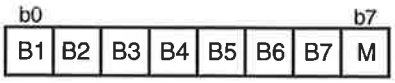
This field shall be a value assigned by an AP during association representing the 16-bit Station ID of a station. The field length is two octets.

4.4.7.Traffic Indication Map (TIM)

The TIM Field 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. The field length is between one and eight octets.

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

BI: Block Identifier (1 octet)



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.

4.4.8. Time Stamp

This field shall represent the value of the TSFTIMER of a frame's source. The most significant bit, when set, shall indicate that the station is synchronized within its BSS. The field length is four octets.

4.4.9.Weight

This field shall indicate the degree to which a station is synchronized within its BSS. Larger values shall indicate a greater degree of synchronization. The field length is two octets.

4.4.10. Channel Sync Information

This field shall contain the information necessary for a station to be able to remain synchronized with a particular BSS that is using a multi-channel PHY. The field length is a variable number of octets. The first two octets comprise a non-inclusive length, in octets, of the remainder of the field.

4.4.11. ESS ID

This field shall indicate the identity of the Extended Service Set. The field length is a variable number of octets. The first octet comprises a non-inclusive length, in octets, of the remainder of the field. The maximum length of the field, inclusive of the length octet, is 129 octets.

4.4.12. 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 field length is one octet. Bit zero of the octet is used for the boolean indicator.

4.4.13. Privacy Algorithm Number

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

4.4.14. Status Value / Error Indicator

This field shall indicate the success or failure of an operation. When this field is zero, the indication is for success. When this field is greater than zero, the indication is for failure and the value of the field is the error code. The field length is one octet.

4.4.15. Current AP Address

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

4.4.16. Transaction Sequence

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

4.4.17. Authentication Algorithm Number

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

4.4.18. Supported Algorithm List

This field shall indicate the list of privacy or authentication algorithms supported by a station. The field length is a variable number of octets. The first octet is the number of Algorithm Number fields within the list. The subsequent octets are Algorithm Number fields. The Algorithm Number fields shall be placed in the Algorithm List in decending order of preference.

4.4.19. Identity Challenge

This field shall be the Identity Challenge of a station's identity. The field length is a variable number of octets. The first two octets comprise a non-inclusive length, in octets, of the remainder of the field. The remainder of the field contains the Identity Challenge bit string. The contents of the bit string is Authentication Algorithm dependent. The bit string is not interpreted or modified by 802.11.

4.4.20. Challenge Response

This field shall be the Challenge Response to an Identity Challenge. The field length is a variable number of octets. The first two octets comprise a non-inclusive length, in octets, of the remainder of the field. The remainder of the field contains the Challenge Response bit string. The contents of the bit string is Authentication Algorithm dependent. The bit string is not interpreted or modified by 802.11.

4.4.21. Challenge Result

This field shall be the Challenge Result from a Challenge Response. The field length is a variable number of octets. The first two octets comprise a non-inclusive length, in octets, of the remainder of the field. The remainder of the field contains the Challenge Result bit string. The contents of the bit string is Authentication Algorithm dependent. The bit string is not interpreted or modified by 802.11.