802.11 MEDIA ACCESS CONTROL HEADER (MAC HEADER)

Prepared by	**Nagendra Babu Kothapalli**
Reviewed by	**Kumar, Aamod**

The technical term for an 802.11 frame is an 802.11 MAC Protocol Data Unit (MPDU). An 802.11 MPDU consists of the following three basic components:

MAC Header Contains frame control information, duration information, addressing, and sequence control information. Furthermore, QoS data frames contain specific QoS control information.

Frame Body Can be variable in size and contains information that is different depending on the frame type and frame subtype.

Frame Check Sequence (FCS) Comprises 32-bit cyclic-redundancy check (CRC) that is used to validate the integrity of received frames.

MAC HEADER

Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	QOS Control	Frame Body	FCS
2	**2**	**6**	**6**	**6**	**2**	**6**	**2**	**0-2304**	**4**

BYTES

Bits, Bytes, Octets:

A *bit* is a binary digit, taking a value of either 0 or 1. Binary digits are a basic unit of communication in digital computing. A byte of information comprises 8 bits. An *octet* is another name for a byte of data.

The 802.11 *MAC header* has eight major fields, four of which are used for addressing. The four address fields are each 6 bytes in length so that they can carry a standard IEEE 802 MAC address.

The Frame Control field, the Duration/ID field, the Sequence Control field, and the QoS Control field are each 2 bytes in size. If all the fields are used, the maximum size of an 802.11 MAC header is 32 bytes.

The 802.11n amendment adds a new field to the 802.11 MAC header, called the HT Control field.

The HT Control field is 4 bytes long and follows the QoS Control field in the 802.11 MAC header. If the HT Control field is used, the maximum size of an 802.11 MAC header would be 36 bytes.

However, the size of an 802.11 MAC header is not always the same for two reasons.

First, the QoS Control field is used only in QoS Data frames.

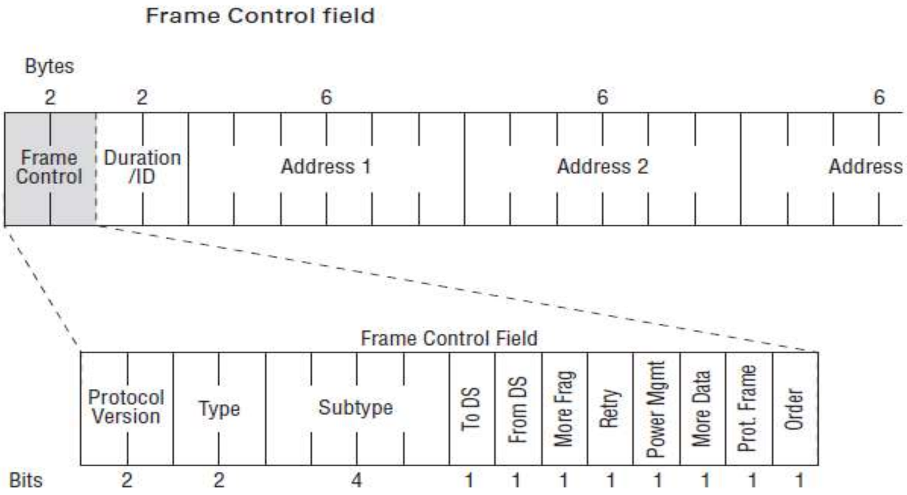
Second, not every frame uses all four address fields.

Most 802.11 frames use only three addresses, and some 802.11 frames such as the acknowledgment (ACK) frame carry only a single address field.

Frame Control Field:

The first two bytes of the MAC header consists of 11 subfields within the *Frame Control field*.

These subfields include Protocol Version, Type, Subtype, To DS, From DS, More Fragments, Retry, Power Management, More Data, Protected Frame, and Order.



Protocol Version(2-bits):

This field is simply used to indicate which protocol version of 802.11 technology is being used by the frame. All 802.11 frames have the value of the Protocol Version field always set to 0. All other values are reserved. In other words, there is currently only one version of 802.11 technology.

Bits	Frame type
0 0	802.11
0 1	Reserved
1 0	Reserved
1 1	Reserved

Type(2-bits):

After the protocol version of a frame has been indicated, the function of the frame must be announced. The *Type field* and *Subtype field* are used together to identify the function of the frame.

The Type field is 2 bits in length, and the Subtype field is 4 bits in length. The three types of 802.11 frames are management, control, and data frames.

The 2-bit Type field identifies whether the frame is a control, data, or management frame. A value of 00 means the type is a management frame, a value of 01 indicates a control frame, and a value of 10 indicates a data frame. The value of 11 is reserved for future use if needed.

Bits	Frame type
0 0	Management frame
0 1	Control frame
1 0	Data frame
1 1	Reserved

Sub Type(4-bits):

There are many kinds of management, control, and data frames, and therefore the 4-bit Subtype field is needed.

Type value b3 b2	Type description	Subtype value b7 b6 b5 b4	Subtype description
0 0	Management	0000	Association request
0 0	Management	0001	Association response
0 0	Management	0010	Reassociation request
0 0	Management	0011	Reassociation response
0 0	Management	0100	Probe request

0 0	Management	0101	Probe response
0 0	Management	1000	Beacon
0 0	Management	1001	Announcement traffic indication message (ATIM)
0 0	Management	1010	Disassociation
0 0	Management	1011	Authentication
0 0	Management	1100	DE authentication
0 0	Management	1101	Action
0 0	Management	1110	Action no ack
0 1	Control	0000-0110	Reserved
0 1	Control	0111	Control wrapper
0 1	Control	1000	Block ack request (BlockAckReq)
0 1	Control	1001	Block ack (BlockAck)
0 1	Control	1010	PS-Poll
0 1	Control	1011	RTS
0 1	Control	1100	CTS
0 1	Control	1101	ACK
0 1	Control	1110	CF-End
0 1	Control	1111	CF-End and CF-Ack
1 0	Data	0101	CF-Ack (no data) [PCF only] 10 Data
1 0	Data	0110	CF-Poll (no data) [PCF only]
1 0	Data	0111	CF-Ack + CF-Poll (no data) [PCF only]
1 0	Data	1000	QoS Data [HCF]
1 0	Data	1001	QoS Data + CF-Ack [HCF]
1 0	Data	1010	QoS Data + CF-Poll [HCF]
1 0	Data	1011	QoS Data + CF-Ack + CF-Poll [HCF]
1 0	Data	1100	QoS Null (no data) [HCF]
1 0	Data	1101	Reserved

1 0	Data	1110	QoS CF-Poll (no data) [HCF]
1 0	Data	1111	QoS CF-Ack + CF-Poll (no data) [HCF]

TO DS(1-bit):

When it set to 1 that indicate data frame is going from client station to Distribution System (DS).

From DS(1-bit):

When it set to 1 that indicate data frame is going from Distribution System (DS) to client station.

Also, this To DS and From DS Field combination (00,01,10,11) indicates different scenarios

To DS=0, From DS=0

It can be management or control frames where it does not go to DS.

Station to station communication in IBSS.

STSL: Station to Station Link where data frame exchange direct client to client.

To DS=0, From DS=1

Downstream traffic from AP to a client station

To DS=1, From DS=0

Up Stream Traffic from a client station to an AP.

To DS=1, From DS=1

Data frames uses four address formats. Usually occurs when Wireless Distribution System (WDS) in use, like Wireless Bridge or Mesh Network.

More Fragments Field(1-bit):

The *More Fragments field* is 1 bit in length and is set to 1 in all data or management type frames that have another fragment of the current MSDU or current MMPDU to follow. It is set to 0 in all other frames.

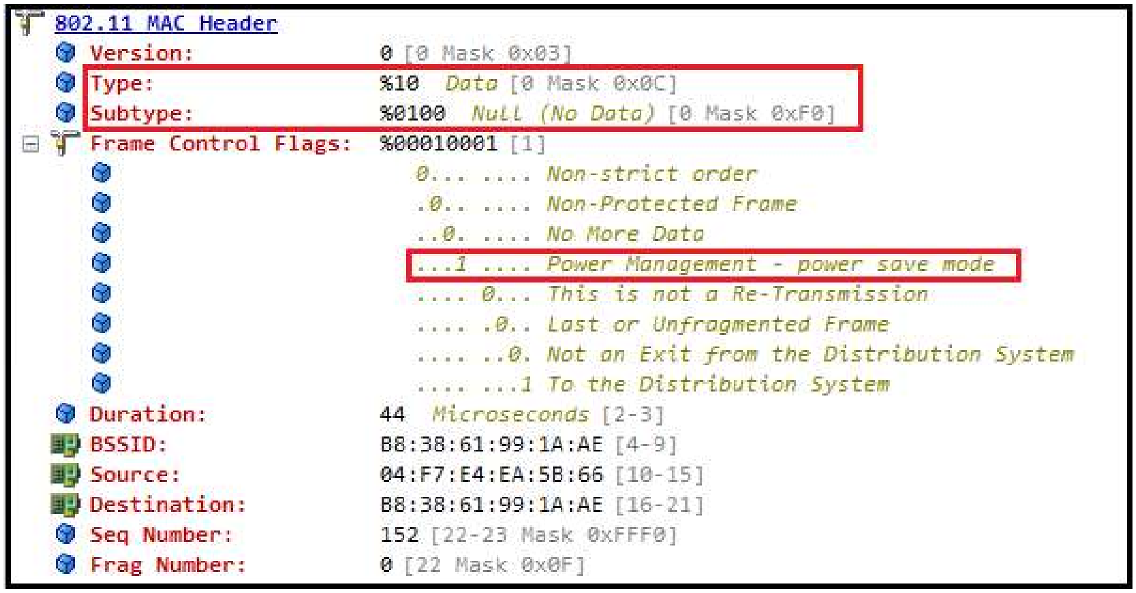
Retry Field(1-bit):

The *Retry field* comprises a single bit of the Frame Control field and is perhaps one of the most important fields in the MAC header.

If the Retry bit has a value of 0, an original transmission of the frame is occurring. If the Retry bit is set to a value of 1 in either a management or data frame, the transmitting radio is indicating that the frame being sent is a retransmission.

Power Management Field(1-bit):

The *Power Management field* is used to indicate the power management mode of a client STA. A value of 1 indicates that the client is using Power Save mode and that buffering of the client traffic on the AP needs to occur. A value of 0 means that no power management is being used, and therefore no buffering is needed.



```
802.11 MAC Header
  Version:              0 [0 Mask 0x03]
  Type:                 %10  Data [0 Mask 0x0C]
  Subtype:              %0100  Null (No Data) [0 Mask 0xF0]
⊟ Frame Control Flags:  %00010001 [1]
                          0... .... Non-strict order
                          .0.. .... Non-Protected Frame
                          ..0. .... No More Data
                          ...1 .... Power Management - power save mode
                          .... 0... This is not a Re-Transmission
                          .... .0.. Last or Unfragmented Frame
                          .... ..0. Not an Exit from the Distribution System
                          .... ...1 To the Distribution System
  Duration:             44  Microseconds [2-3]
  BSSID:                B8:38:61:99:1A:AE [4-9]
  Source:               04:F7:E4:EA:5B:66 [10-15]
  Destination:          B8:38:61:99:1A:AE [16-21]
  Seq Number:           152 [22-23 Mask 0xFFF0]
  Frag Number:          0 [22 Mask 0x0F]
```

More Data Field(1-bit):

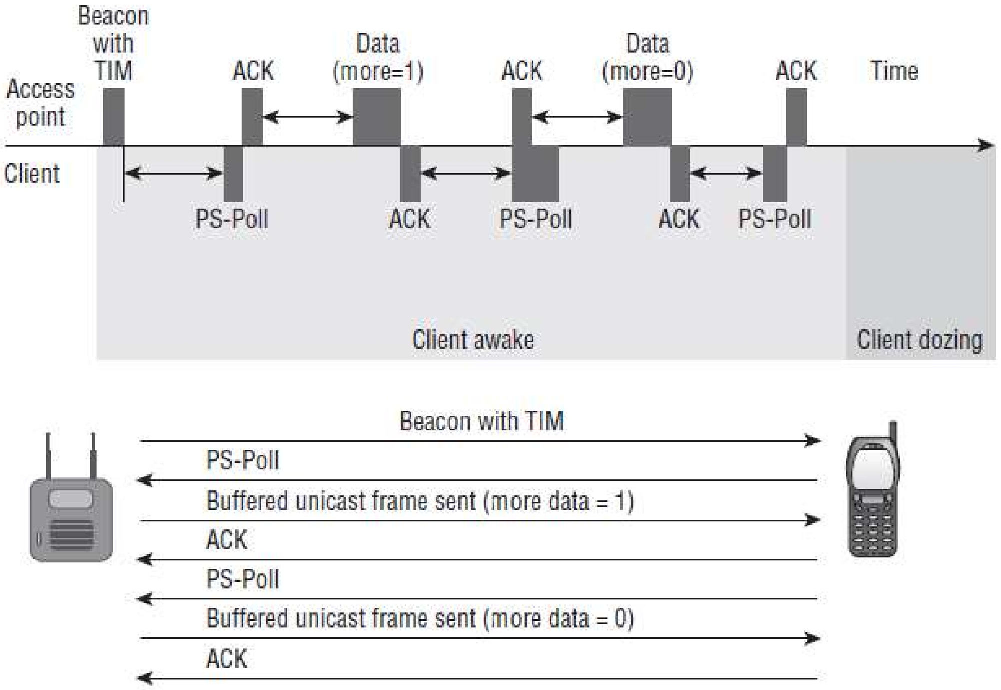
When a client associate to an AP, client receives an association identifier (AID). AP use this AID to keep track of stations associated to the AP & members of BSS.

If AP is buffering data for a station in Power Save mode, when AP transmit its next beacon, the AID of the station will be seen in a field called “traffic indication map– TIM “.

When station receives the beacon during the awake state, it checks to see whether its AID is set in TIM, indicating buffered unicast frame waits. If so, station will remain awake & will send a PS-Poll frame to the AP.

Then AP will send buffered unicast frame to station. To indicate there are more frames AP will set "More Data" field to 1, so station can awake to receive all those frames. Below diagram summarize this process.

FIGURE 3.13 Power Save mode



Protected Frame (1-bit):

This field is used to indicate whether the MSDU payload of a data frame is encrypted. In a Data frame where payload is encrypted indicated by setting protected bit to "1".

Order (1-bit):

If it set to "1" in any non-QoS data frame when a higher layer has requested that the data be sent using a strictly ordered class of service, which tells the receiving station the frames must be processed in order.

This field is set to "0" in all other frames.

Duration/ID field(16-bits):

In 802.11, Duration/ID field can be used for different reasons

1. Virtual Carrier Sense – This is the main purpose which used to reset the NAV timer of the other stations

2. Legacy Power Management – PS Poll frames use this field as an association identifier (AID)

Virtual Carrier Sense:

Virtual Carrier Sense use a timer mechanism known as the NAV (Network Allocation Vector)

When listening STA hears a frame transmission by other STA, the listening STA will set its NAV timer to the value appear in transmitted frame.

listening STA then will use the NAV as a countdown timer, knowing that RF medium will be busy until it reaches 0.

When a client transmits a unicast frame, Duration/ID field use bit 0-14 (value 0 – 32767)

Duration/ID value represent time in µS (microseconds) that is required to transmit the ACK + one SIFS interval.

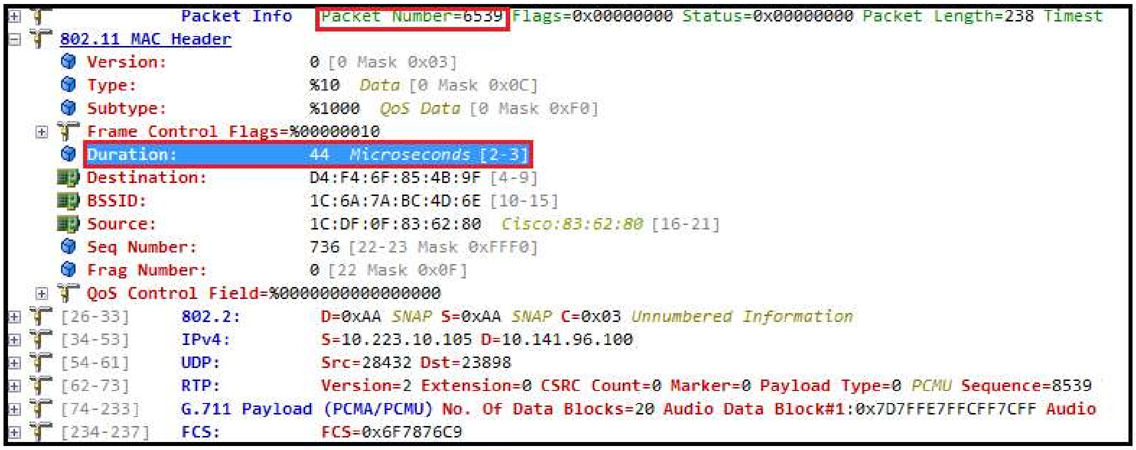
Duration values are always about frame transmission that are to follow.

The client who transmits a frame will calculate how long it will take to receive an ACK frame & include that in the duration field.

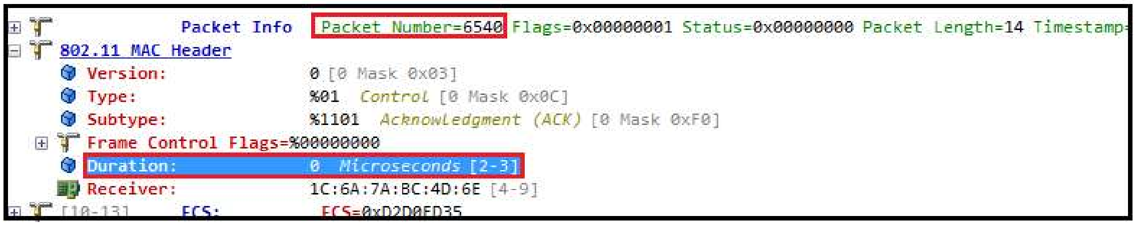
The ACK frame follows the transmitted frame having duration value of 0.

Below shows a frame capture of a unicast frame & ACK followed by the transmission.

As you can see duration value of 44 µS (time for a ACK+SIFS) for tx frame & ACK having 0 µS value.



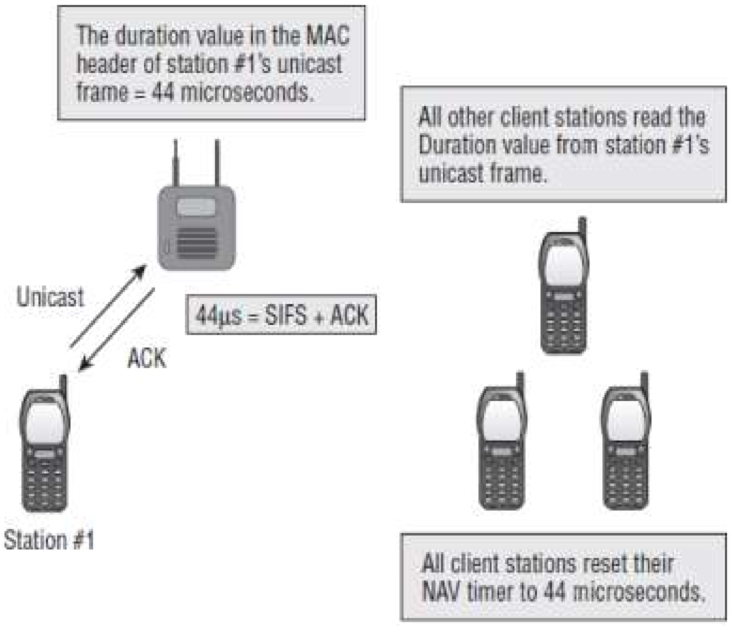
```
⊞     Packet Info   Packet Number=6539 Flags=0x00000000 Status=0x00000000 Packet Length=238 Timest
⊟ 802.11 MAC Header
      Version:              0 [0 Mask 0x03]
      Type:                 %10  Data [0 Mask 0x0C]
      Subtype:              %1000  QoS Data [0 Mask 0xF0]
    ⊞ Frame Control Flags=%00000010
      Duration:             44  Microseconds [2-3]
      Destination:          D4:F4:6F:85:4B:9F [4-9]
      BSSID:                1C:6A:7A:BC:4D:6E [10-15]
      Source:               1C:DF:0F:83:62:80  Cisco:83:62:80 [16-21]
      Seq Number:           736 [22-23 Mask 0xFFF0]
      Frag Number:          0 [22 Mask 0x0F]
    ⊞ QoS Control Field=%0000000000000000
⊞ [26-33]     802.2:       D=0xAA SNAP S=0xAA SNAP C=0x03 Unnumbered Information
⊞ [34-53]     IPv4:        S=10.223.10.105 D=10.141.96.100
⊞ [54-61]     UDP:         Src=28432 Dst=23898
⊞ [62-73]     RTP:         Version=2 Extension=0 CSRC Count=0 Marker=0 Payload Type=0 PCMU Sequence=8539
⊞ [74-233]    G.711 Payload (PCMA/PCMU) No. Of Data Blocks=20 Audio Data Block#1:0x7D7FFE7FFCFF7CFF Audio
⊞ [234-237]   FCS:         FCS=0x6F7876C9
```



```
⊞     Packet Info   Packet Number=6540 Flags=0x00000001 Status=0x00000000 Packet Length=14 Timestamp=
⊟ 802.11 MAC Header
      Version:              0 [0 Mask 0x03]
      Type:                 %01  Control [0 Mask 0x0C]
      Subtype:              %1101  Acknowledgment (ACK) [0 Mask 0xF0]
    ⊞ Frame Control Flags=%00000000
      Duration:             0  Microseconds [2-3]
      Receiver:             1C:6A:7A:BC:4D:6E [4-9]
⊞ [10-13]     FCS:         FCS=0xD2D0ED35
```

When this type of frame is transmitting in the RF all other receiving STA set their NAV to 44 µS

FIGURE 3.18 Virtual carrier-sense


The duration value in the MAC header of station #1's unicast frame = 44 microseconds.
All other client stations read the Duration value from station #1's unicast frame.
Unicast
44µs = SIFS + ACK
ACK
Station #1
All client stations reset their NAV timer to 44 microseconds.

NAV is not updated when the receiver address (RA) is the same as receiving station's MAC address.

Duration value of the Tx STA does not reset the transmitter's NAV timer (as it cannot hear its own tx).

Transmitter NAV will be zero after transmitting.

PS-Poll in Legacy Power Management:

When a STA associate to an AP each STA will get a unique AID (Association Identifier).

If AP buffering data for a station in power save mode, when AP transmit its next beacon, the AID of station will be seen in TIM (Traffic Indicator Map).

TIM field is a list of all stations that have undelivered unicast data buffered on the AP (DTIM is used for multicast buffered data).

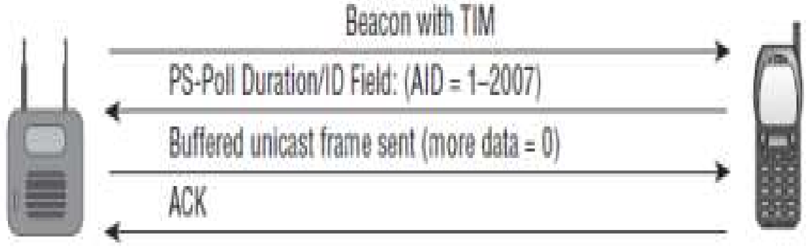
Client will send a PS-Poll frame to request that AP sends the unicast buffered frame to the STA.

In PS-Poll frame Duration/ID field use as an identifier (AID) & not being used for duration or resetting NAV timers.

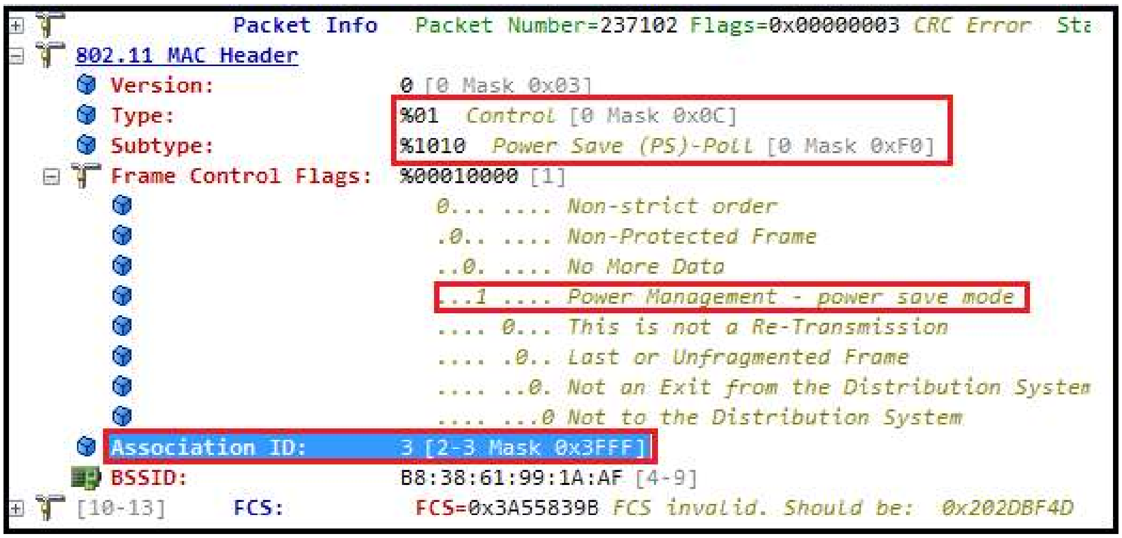
When it uses in PS-Poll frame, two Most Significant Bits (MSB) set to 1 & AID value use rest of the 14 LSB (Least Significant Bits).

But allowable value for AID is 1 – 2007.

FIGURE 3.19 AID


Beacon with TIM
PS-Poll Duration/ID Field: (AID = 1–2007)
Buffered unicast frame sent (more data = 0)
ACK

Below shows a PS-Poll frame capture that shows the AID value (3 in my case) instead of Duration value.



```
⊞ Packet Info           Packet Number=237102 Flags=0x00000003 CRC Error  Sta
⊟ 802.11 MAC Header
    Version:              0 [0 Mask 0x03]
    Type:                 %01  Control [0 Mask 0x0C]
    Subtype:              %1010  Power Save (PS)-Poll [0 Mask 0xF0]
  ⊟ Frame Control Flags:  %00010000 [1]
                            0... .... Non-strict order
                            .0.. .... Non-Protected Frame
                            ..0. .... No More Data
                            ...1 .... Power Management - power save mode
                            .... 0... This is not a Re-Transmission
                            .... .0.. Last or Unfragmented Frame
                            .... ..0. Not an Exit from the Distribution System
                            .... ...0 Not to the Distribution System
    Association ID:       3 [2-3 Mask 0x3FFF]
    BSSID:                B8:38:61:99:1A:AF [4-9]
⊞ [10-13]     FCS:         FCS=0x3A55839B FCS invalid. Should be:  0x202DBF4D
```

MAC Address Fields:

There are four 802.11 MAC address fields respectively called Address 1, Address 2, Address 3, and Address 4. Depending on how the To DS and From DS fields are used, the definition of each of the four MAC address fields will change.

The five definitions are as follows:

Source Address (SA): The MAC address of the original sending station. The source address either can originate from a wireless station or can originate from the wired network.

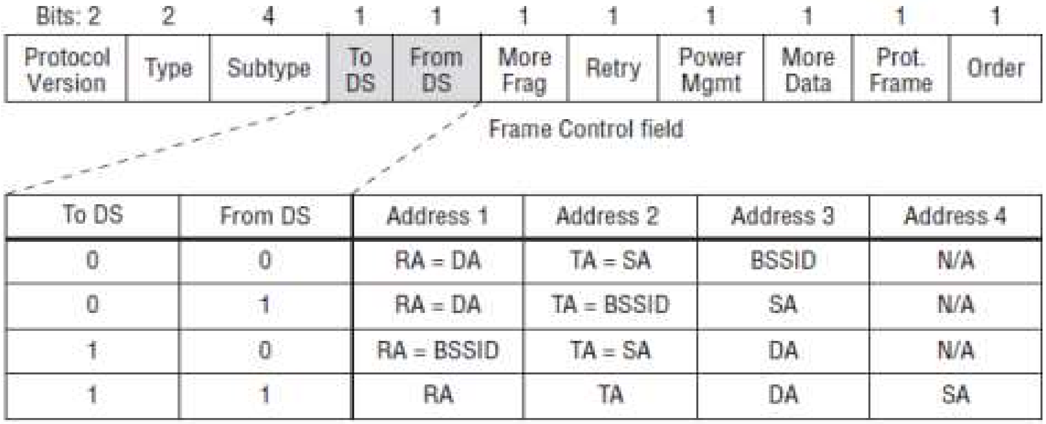
Destination Address (DA): The MAC address that is the final destination of the frame. The final destination could be a wireless station or could be a destination on the wired network such as a server.

Transmitter Address (TA): The MAC address of an 802.11 radio that is transmitting the frame onto the half-duplex 802.11 medium.

Receiver Address (RA): The MAC address of the 802.11 radio that receives the incoming transmission from the transmitting station.

Basic Service Set Identifier (BSSID): The MAC address that is the layer 2 identifier of the basic service set (BSS). The BSSID is the MAC address of the AP's radio or is derived from the MAC address of the AP's radio if multiple basic service sets exist.

FIGURE 3.20 802.11 MAC addressing



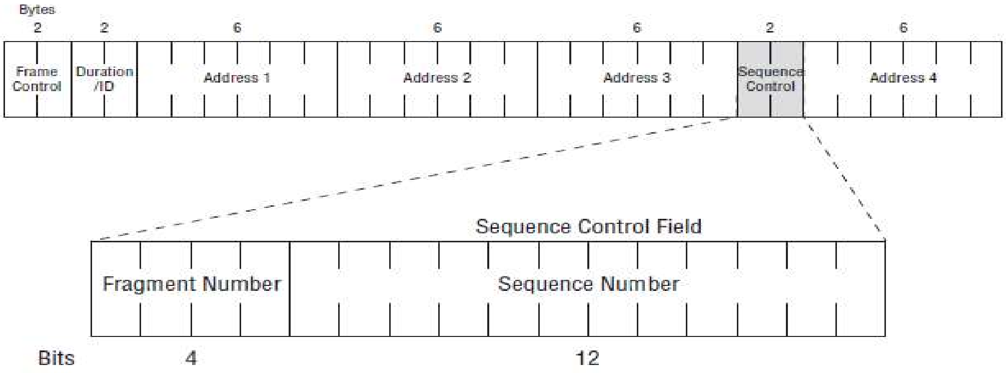
To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	RA = DA	TA = SA	BSSID	N/A
0	1	RA = DA	TA = BSSID	SA	N/A
1	0	RA = BSSID	TA = SA	DA	N/A
1	1	RA	TA	DA	SA

- SA = MAC address of the original sender (wired or wireless)
- DA = MAC address of the final destination (wired or wireless)
- TA = MAC address of the transmitting 802.11 radio
- RA = MAC address of the receiving 802.11 radio
- BSSID = L2 identifier of the basic service set (BSS)

Sequence Control field(16-bits):

The Sequence Control field is 16 bits in length and consists of two subfields, the Sequence Number and the Fragment Number. The sequence Control field is not present in control frames (as no frame body). The format of the Sequence Control field is shown below.

FIGURE 3.30 Sequence Control field



Sequence Number:

The Sequence Number field is a 12-bit field indicating the sequence number of an MSDU, A-MSDU, or MMPDU. Each MSDU, A-MSDU, or MMPDU transmitted by a STA is assigned a sequence number. The sequence number remains constant in all retransmissions of an MSDU, MMPDU, or fragment thereof.

Fragment Number:

The Fragment Number field is a 4-bit field indicating the number of each fragment of an MSDU or MMPDU. The fragment number is set to 0 in the first or only fragment of an MSDU or MMPDU and is incremented by one for each successive fragment of that MSDU or MMPDU. The fragment number remains constant in all retransmissions of the fragment.

Fragments are always sent in what is known as a “fragment burst “. Once Tx STA gains control of the medium, it maintains control through NAV Duration values & SIFS. Value of the Duration field in the MAC header of first fragment is used to reserve the medium for the next fragment. If a fragment is not acknowledged, then retries begin at unacknowledged fragment (using DIFS) & not beginning of the original MSDU.

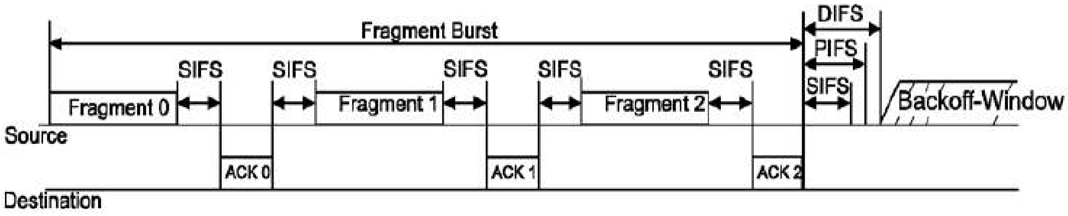
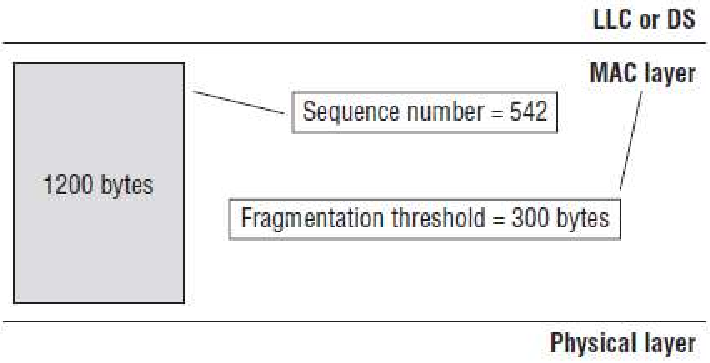


Figure 9-13—Transmission of a multiple-fragment MSDU using SIFS

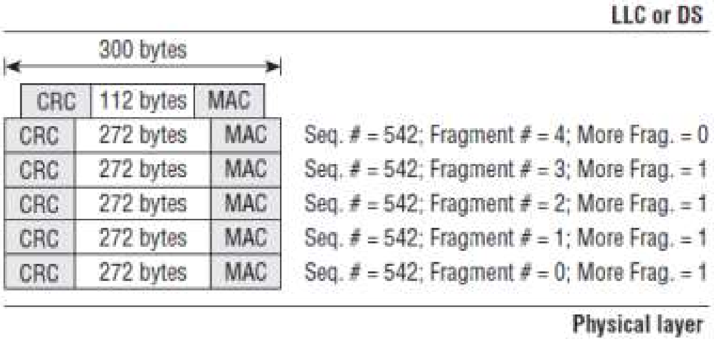
Below shows an example for a STA configured with a fragmentation threshold (min 256 byte) of 300 bytes. So, any MSDU larger than 300 bytes will be fragmented. Fragmentation does not consider frame body expansion due to encryption, thus encrypted fragment may exceed the fragmentation threshold. Given example consider non-QoS data frame with MAC header size of 24 bytes (i.e., 32 -6 -2 bytes where 6 bytes less for 4th address field & 2 bytes less for no QoS control field) and 4-byte CRC. So, fragment size should be 272 bytes (300-28).

FIGURE 3.31 Fragmentation threshold



The first fragment to be transmitted will be fragment#0 & the More Fragment bit in the Frame Control bit set to 1. The More Fragments bit will stay to 1 until the last fragment, at which time it will change to 0 indicating that there are no more fragments (fragment#4 in the below).

FIGURE 3.32 MSDU fragmentation


LLC or DS
300 bytes
CRC
112 bytes
MAC
CRC
272 bytes
MAC
Seq. # = 542; Fragment # = 4; More Frag. = 0
Seq. # = 542; Fragment # = 3; More Frag. = 1
Seq. # = 542; Fragment # = 2; More Frag. = 1
Seq. # = 542; Fragment # = 1; More Frag. = 1
Seq. # = 542; Fragment # = 0; More Frag. = 1
Physical layer

QoS Control Field(16-bits):

QoS Control is a 16-bit field that identifies the Quality of Service (QoS) parameter of a data frame (only in data frame type QoS-Data). It should be noted that not all data frames contain a QoS Control field. The 802.11-2007 standard states, "The QoS Control field is present in all data frames in which the QoS subfield of the Subtype field is set to 1." In other words, the QoS control field is only used in the MAC header of QoS data frames.

The QoS Control field is comprised of five subfields called traffic identifier (TID) subfield, end of service period (ESOP) subfield, ACK policy subfield, and a reserved subfield.

Depending on whether the QoS data frame is sent by an AP or a client station, the five subfields can represent four different types of information. The last 8 bits of the QoS Control field can be used as a TXOP Limit, TXOP Duration Requested, AP PS Buffer State, and Queue Size.

TID (Traffic Indicator-4bits):

4-bit value used to identify the user priority (UP) and traffic Access Category (AC) of a QoS data frame. 802.11 WMM clients use WMM-PS (power save) to indicate to an AP that STA is awake. Unlike in legacy PS, WMM-PS client can ask to deliver more than 1 frame.

EOSP (End of Service Period-1bit):

1 bit value to indicate the end of a service period. If this bit set to 1, then client can go back to asleep.

Acknowledge (2 bits):

Specify the 2-bit Acknowledgement policy. There are four different options available

ACK

No-ACK

No Explicit ACK

Block ACK

Reserved (1 bit):

Allocated for future use

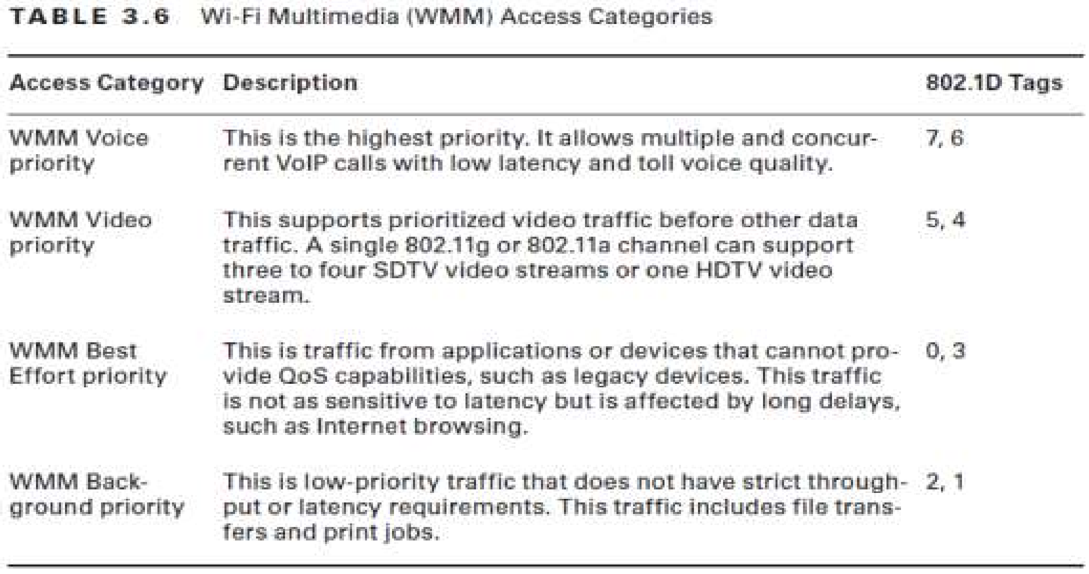


TABLE 3.6 Wi-Fi Multimedia (WMM) Access Categories

Access Category	Description	802.1D Tags
WMM Voice priority	This is the highest priority. It allows multiple and concurrent VoIP calls with low latency and toll voice quality.	7, 6
WMM Video priority	This supports prioritized video traffic before other data traffic. A single 802.11g or 802.11a channel can support three to four SDTV video streams or one HDTV video stream.	5, 4
WMM Best Effort priority	This is traffic from applications or devices that cannot provide QoS capabilities, such as legacy devices. This traffic is not as sensitive to latency but is affected by long delays, such as Internet browsing.	0, 3
WMM Background priority	This is low-priority traffic that does not have strict throughput or latency requirements. This traffic includes file transfers and print jobs.	2, 1