WLAN - Frame Structure

Home : www.sharetechnote.com

As you may noticed from other technology that I posted, the way I study about a communication technology is always same. Study and understand the details of frame structure and then understand how these frames are exchanged at each step of communication process (protocol).

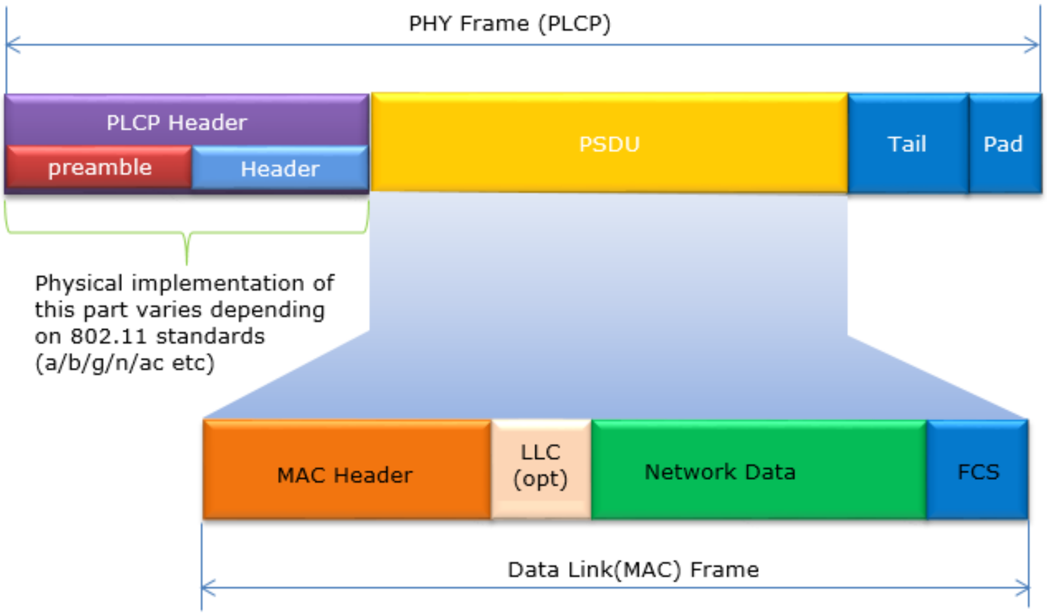
Overview of WLAN Frame

Followings are some of the bullelts for WLAN Frame. (The list would get longer as I learn more)

- WLAN doesn't use 802.3 Ethernet frames
- There three different types of WLAN frame named Control, Management and Data frame.
- Max Frame size is 2346 bytes and they are typically fragmented at 1516 bytes.
- Preamble is always sent at 1 Mbps

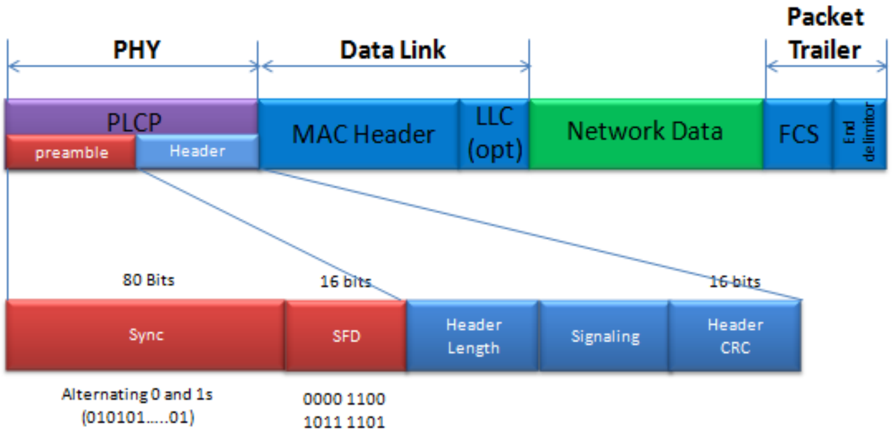
PHY/MAC Frame

This is the frame being exchanged between the mobile device and Access point. The overall frame is structed as shown below.
The 'Network Data' shown in Green is the part which are eventually eventually conveyed to wired backbone and all the other portion (PHY, DataLink, Packet Trailer) are used for communicating between the mobile client and access point. PHY and 'Data Link' part will be main subject of WLAN frame.



PLCP (Physical Layer Convergence Protocol) Structure

Now let's look into the details of PLCP. PLCP is a kind of header deing added at PHY layer. It consists of two main parts, preamble and Header as shown below.



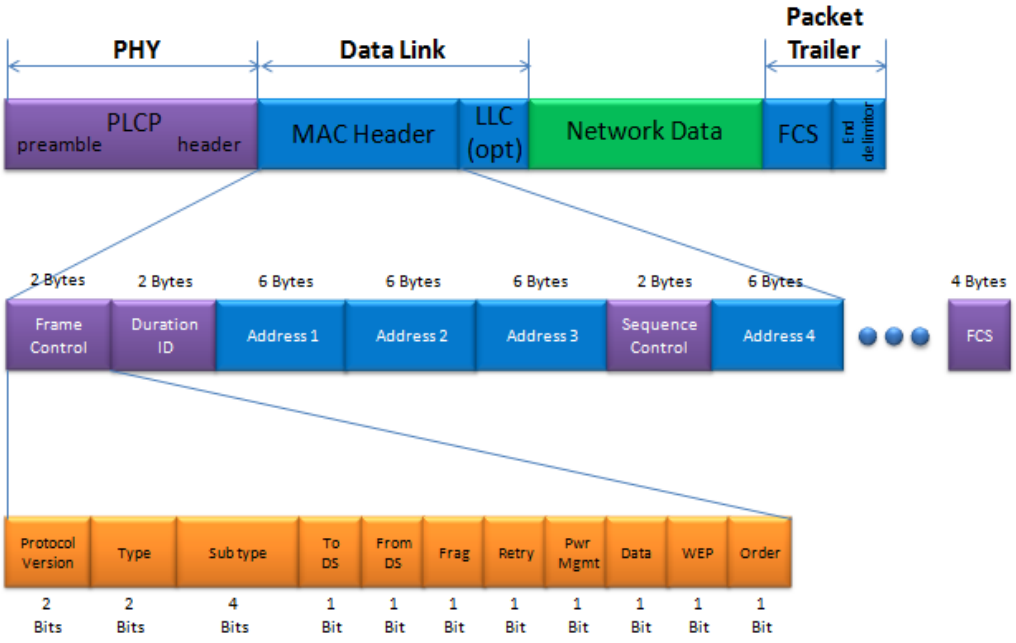
The first part of PLCP is for 'Sync' (Synchronization). This is a part made of 80 bits of alternation 0 and 1s. The next portion is SFD (Start Frame Delimiter). This is a kind of tag indicating the start of physical frame and it is a specifically determined 16 bit sequence (0000110010111101).

MAC Header Structure

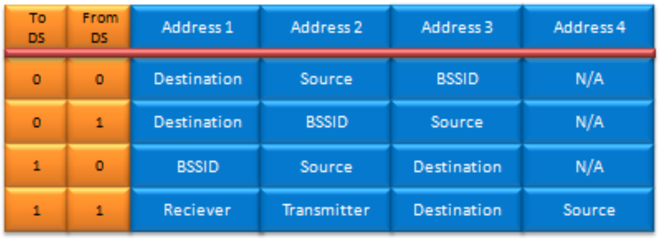
MAC Header would be a most complicated structure of the frame. The most important information contained in the MAC header would be as follows.

- What is the type of frame ?
- What are the source and destination address for the frame.

< Frame Control Field Structure >



You see four different locations allocated for Address. What kind of address is assigned to which address field is determined by 'To DS' and 'From DS' field. The mapping between DS field and Address field are specified as follows.



To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	Destination	Source	BSSID	N/A
0	1	Destination	BSSID	Source	N/A
1	0	BSSID	Source	Destination	N/A
1	1	Reciever	Transmitter	Destination	Source

Regardless of the contents in the frame, the structure of MAC header is same. Then how do we (the WLAN device) knows what kind of the information (data) is contained in the frame. 'Type' and 'Sub Type' field determines the characteristics of the frame.
Type field (2 bits) determines the major characteristics of the contents carried by the frame and 'Sub type' defines the details of the information.
The 'Type'/'Sub Type' and characteristics of the contents are mapped as shown in the following table. This table is mostly for 802.11 a,b,g and there is some changes (additions) in recent specification (e.g, 802.11ac, 802.11ad). Regarding the changes in recent specification, I would not list in this table and I will list those changes in separate pages dealing with 802.11ac or 802.11ad.

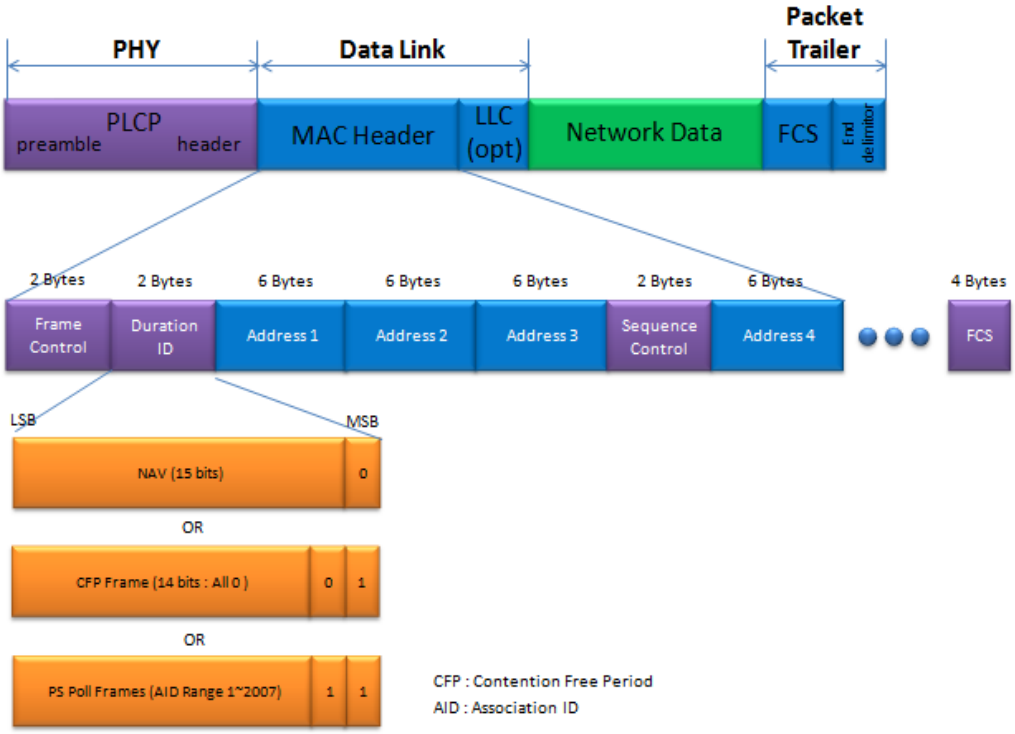
< Frame Type Table >

Type	Type Description	Sub Type	Sub Type 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	0100-0111	Reserved
00	Management	1000	Beacon
00	Management	1001	ATIM
00	Management	1010	Dissociation

00	Management	1011	Authentication
00	Management	1100	Deauthentication
00	Management	1101-1111	Reserved
01	Control	0000-1001	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
01	Control	1010	PS-Poll
10	Data	0000	Data
10	Data	0001	Data + CF ACK
10	Data	0010	Data + CF Poll
10	Data	0011	Data + CF ACK + CF Poll
10	Data	0100	Null Function(No Data)
10	Data	0101	CF ACK(no Data)
10	Data	0110	CF Poll(no Data)
10	Data	0111	CF ACK + CF Poll(no Data)
10	Data	1000-1111	Reserved
11	Reserved	0000-1111	Reserved

< Duration ID Field Structure >

The value in the duration field has different meaning (interpretation) depending on the one or two bits at Most Significant Bits (MSB) as shown below.

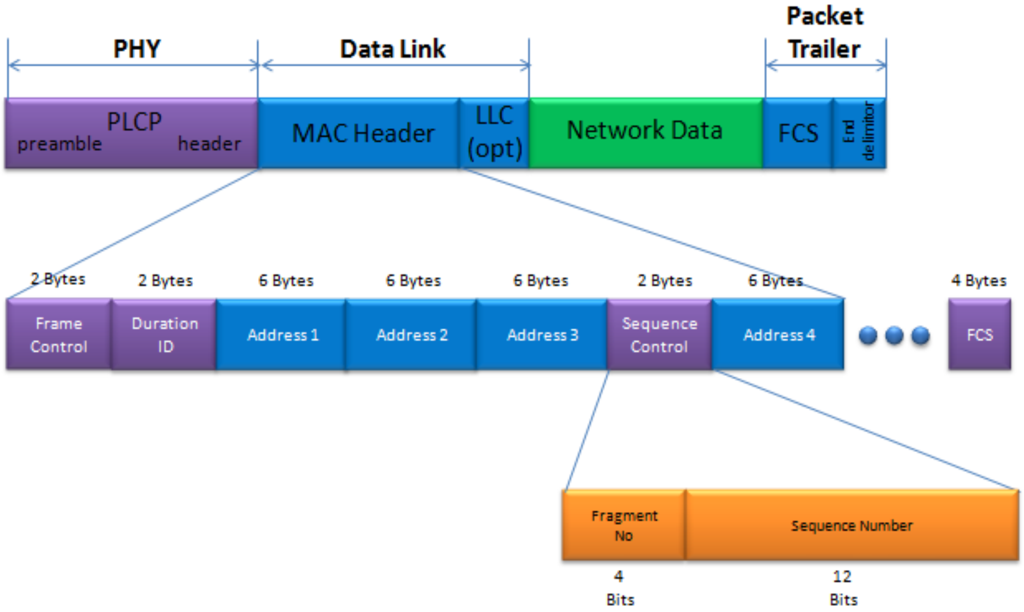


CFP : Contention Free Period
AID : Association ID

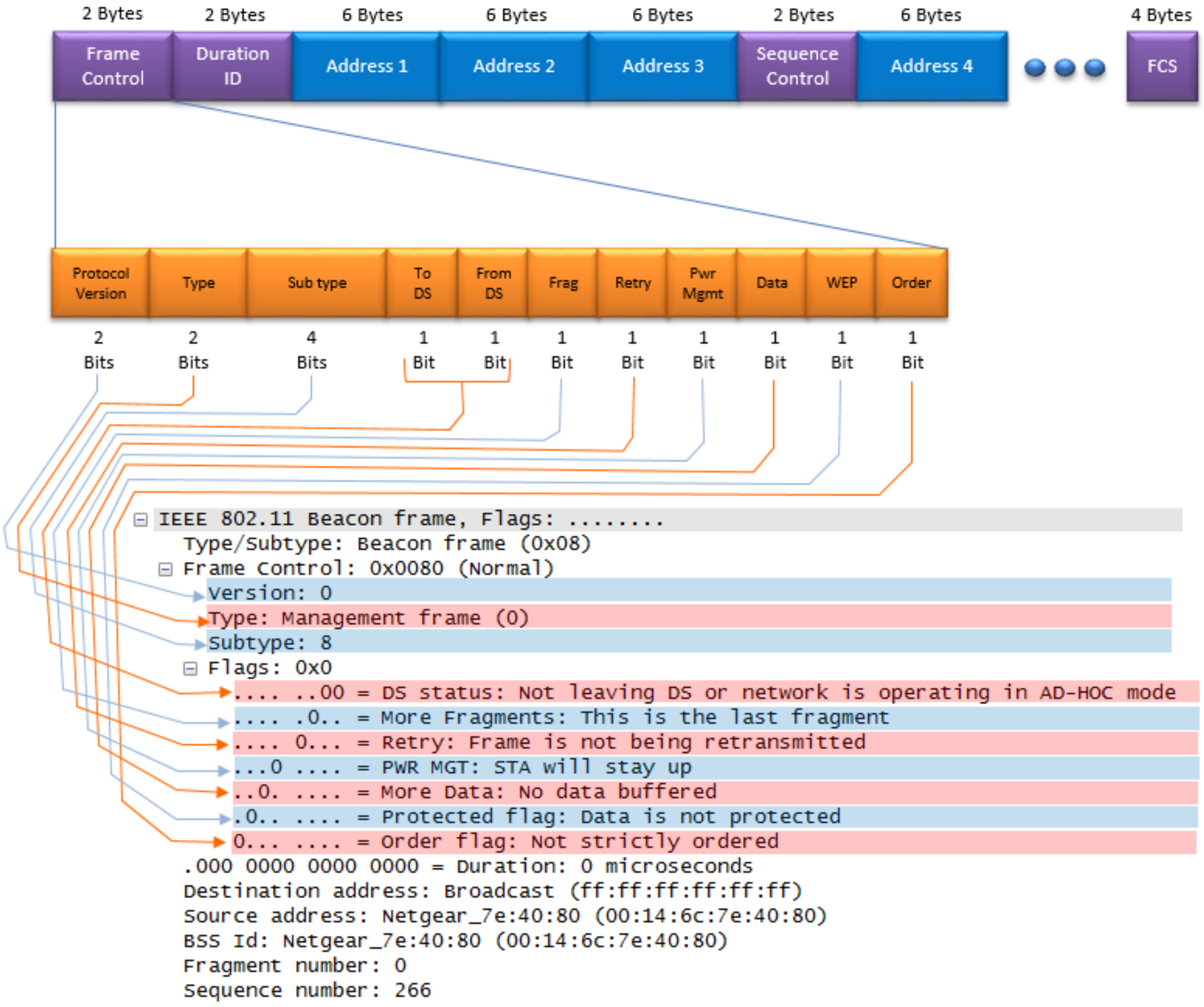
< Sequence Control Field Structure >

When a packet comes into the MAC layer from higher layer, a sequence number is assigned at 'Sequence Number'

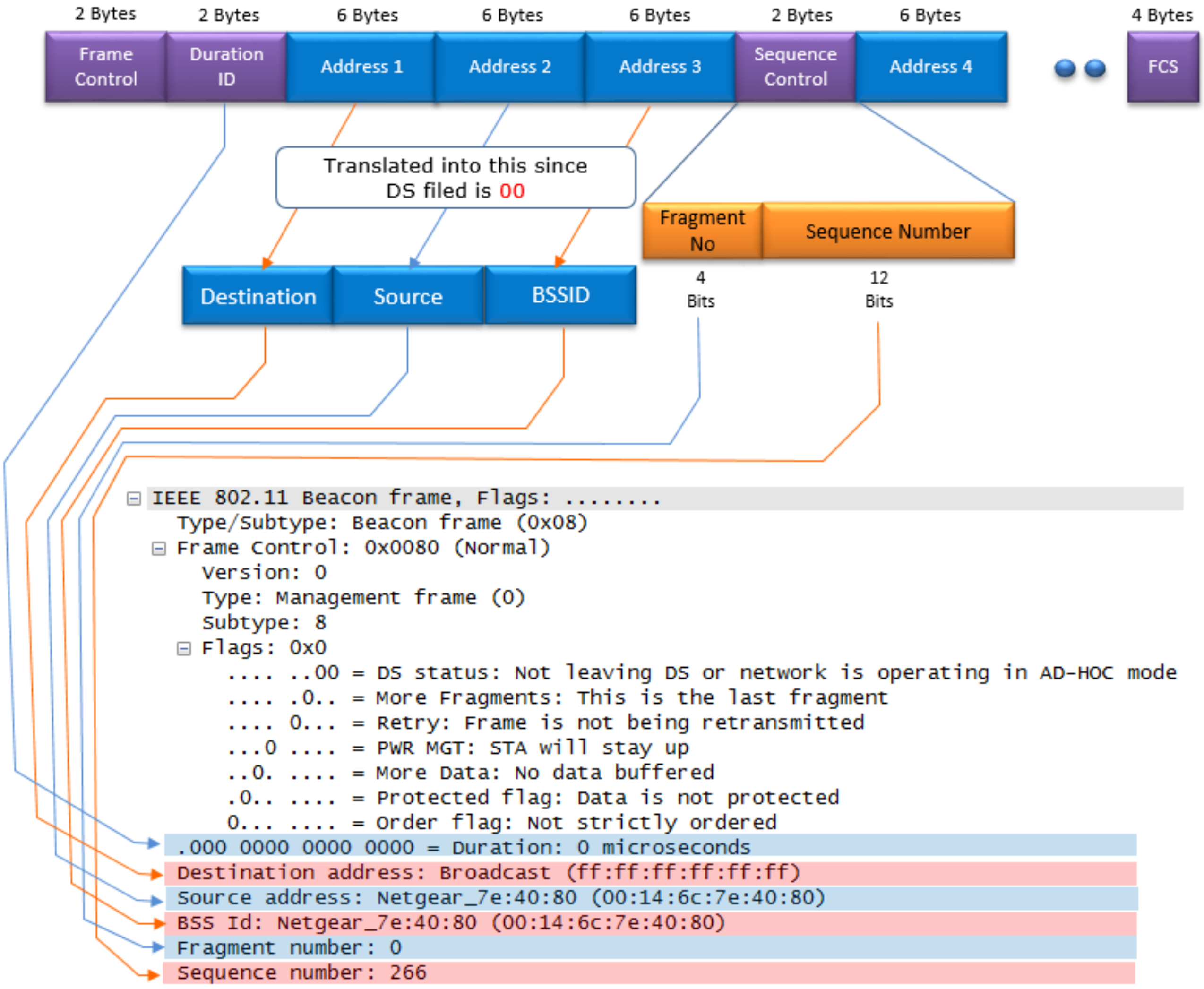
field. If the incoming packet is too big for a single MAC frame, it be splitted into multiple fragment. In this case, a fragment number is assigned at 'Fragment No' field. When a packet gets into multiple MAC frame, those fragmented frame gets the same value at 'Sequence Number' field and different values at 'Fragment No' field.
802.11 can transmit the max 2304 bytes of higher layer packet. Considering WEP overhead and 8 bytes LLC header, the maximum MAC frame size should be 2296 bytes.



Example 1 > MAC Header / Beacon Frame

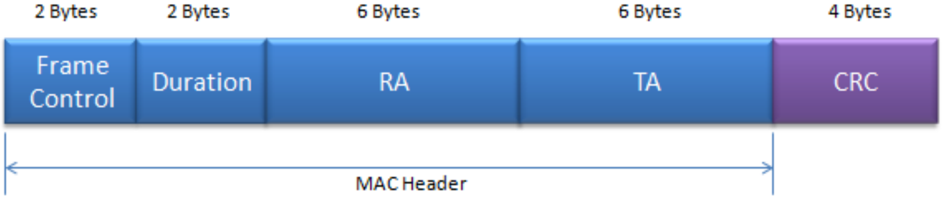


```
⊟ IEEE 802.11 Beacon frame, Flags: ........
    Type/Subtype: Beacon frame (0x08)
  ⊟ Frame Control: 0x0080 (Normal)
      Version: 0
      Type: Management frame (0)
      Subtype: 8
    ⊟ Flags: 0x0
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    .000 0000 0000 0000 = Duration: 0 microseconds
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: Netgear_7e:40:80 (00:14:6c:7e:40:80)
    BSS Id: Netgear_7e:40:80 (00:14:6c:7e:40:80)
    Fragment number: 0
    Sequence number: 266
```



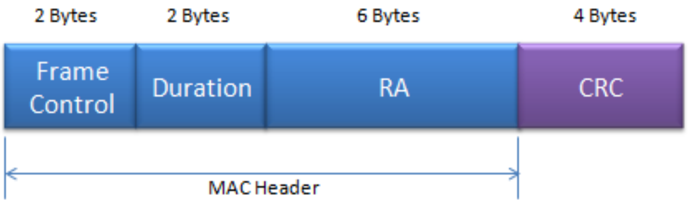
```
⊟ IEEE 802.11 Beacon frame, Flags: ........
    Type/Subtype: Beacon frame (0x08)
  ⊟ Frame Control: 0x0080 (Normal)
      Version: 0
      Type: Management frame (0)
      Subtype: 8
    ⊟ Flags: 0x0
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    .000 0000 0000 0000 = Duration: 0 microseconds
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Source address: Netgear_7e:40:80 (00:14:6c:7e:40:80)
    BSS Id: Netgear_7e:40:80 (00:14:6c:7e:40:80)
    Fragment number: 0
    Sequence number: 266
```

RTS Frame



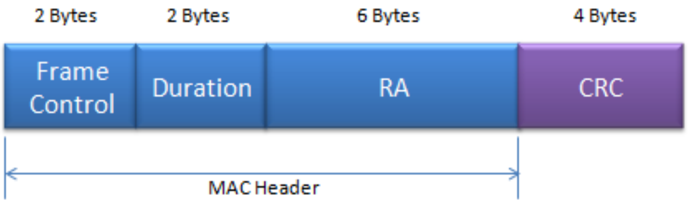
- Duration : Time in microseconds. This is the time required for "Data/Management Frame + CTS + ACK + 3 SIFS"
- RA : Reciever Address
- TA : Transmitter Address

CTS Frame



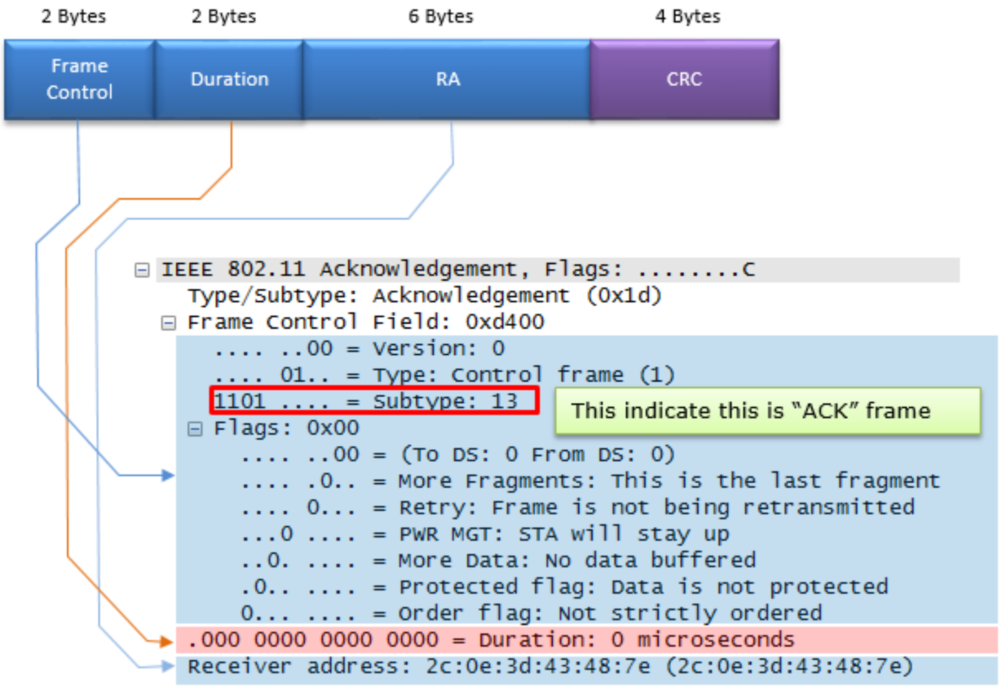
- Duration : Time in microseconds.
- RA : Reciever Address
- TA : Transmitter Address

ACK Frame



Example 1 > MAC Header / ACK Frame

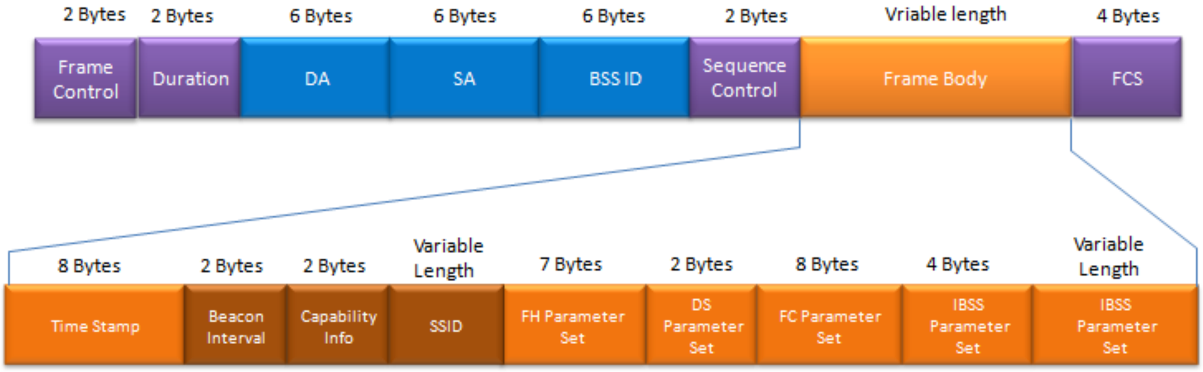
- Duration : Time in microseconds.
- RA : Reciever Address
- TA : Transmitter Address



```
⊟ IEEE 802.11 Acknowledgement, Flags: ........C
    Type/Subtype: Acknowledgement (0x1d)
  ⊟ Frame Control Field: 0xd400
      .... ..00 = Version: 0
      .... 01.. = Type: Control frame (1)
      1101 .... = Subtype: 13
    ⊟ Flags: 0x00
        .... ..00 = (To DS: 0 From DS: 0)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = Order flag: Not strictly ordered
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: 2c:0e:3d:43:48:7e (2c:0e:3d:43:48:7e)
```

This indicate this is "ACK" frame

Beacon Frame



The contents of the Beacon Frame (Beacon Body) is a huge structure, so I created a separate page for Beacon and it's contents.

Reference

- Packets never lie: An in-depth overview of 802.11 frames
- 802.11ac Analysis Webinar