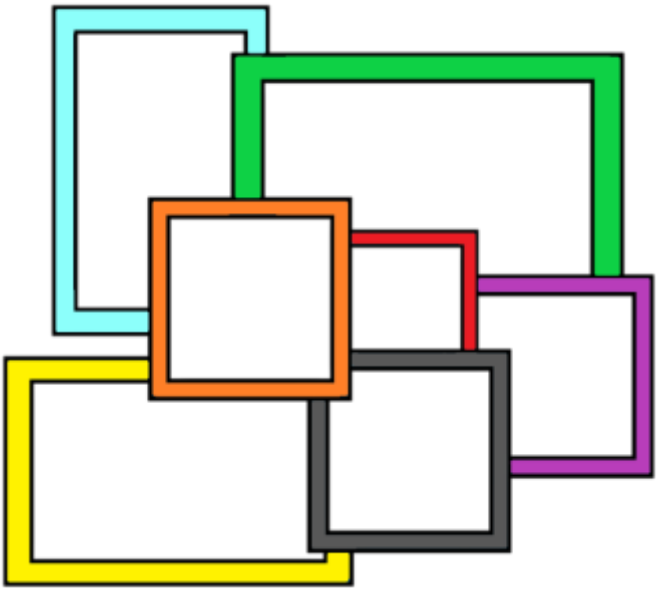
How I WI-FI

A blog about Wi-Fi!

802.11 Frame Types and Formats



There are three types of 802.11 frames: management, control, and data. Management frames are used to mange the BSS, control frames control access to the medium, and data frames contain payloads that are the layer 3-7 information. We will focus on the contents of each frame rather than understanding the context of the frame in the frame exchange process. Separate post to follow that will cover the various frame exchanges. As a consumer of all my own blog posts, I'll be formatting this post in a way that it can be easily used as a reference and be as searchable as possible.

This post covers the information you will be expected to know for the CWNA-107 and CWAP-403 exams about frame types, formatting, and values. As you can see below, the level of knowledge expected for the CWNA exam is much simpler. In the CWAP exam, it is expected that you can identify the frame type, which information elements (IE) contain which values, and understand what each value represents.

CWNA-107 Objectives covered:

- 3.2 Identify and explain the basic frame types defined in the 802.11-2016 standard
  - 3.2.1 General frame format
  - 3.2.2 MAC addressing
  - 3.2.3 Beacon frame
  - 3.2.4 Association frames
  - 3.2.5 Authentication frames
  - 3.2.6 Data frames
  - 3.2.7 Acknowledgement (ACK) frames
  - 3.2.8 Block ACK frames

CWAP-403 Objectives covered:

- 4.2 Identify and use MAC information in captured data for analysis
  - 4.2.1 Management, control, and data frames
  - 4.2.2 MAC Frame Format
    - Frame Control Field
    - To DS and From DS
    - Address Fields
    - Frame Check Sequence (FCS)
  - 4.2.3 802.11 Management Frame Formats
    - Information Elements
    - Authentication
    - Association and Reassociation
    - Beacon
    - Probe Request and Probe Response
  - 4.2.4 Data and QoS Data Frame Formats
  - 4.2.5 802.11 Control Frame Formats
    - Acknowledgement
    - RTS/CTS
    - Block Acknowledgement and related frames

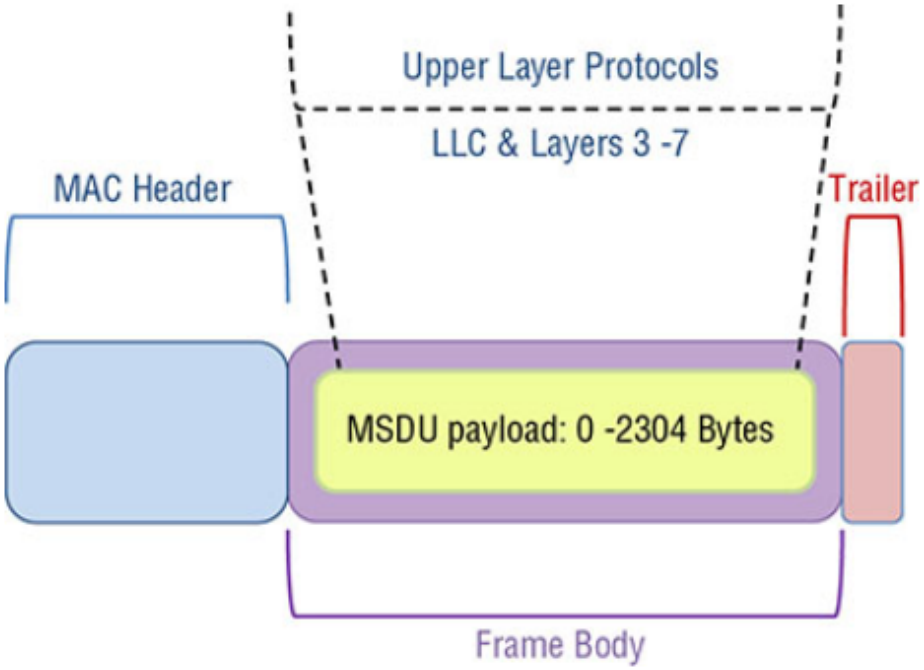
- 4.3 Validate BSS configuration through protocol analysis
  - 4.3.1 Country code
  - 4.3.2 Minimum basic rate
  - 4.3.3 Supported rates
  - 4.3.4 Beacon intervals
  - 4.3.5 WMM settings
  - 4.3.6 RSN settings
  - 4.3.7 HT and VHT operations
  - 4.3.8 Channel width
  - 4.3.9 Primary channel
  - 4.3.10 Hidden or non-broadcast SSIDs

- 4.4 Identify and analyze CRC error frames and retransmitted frames

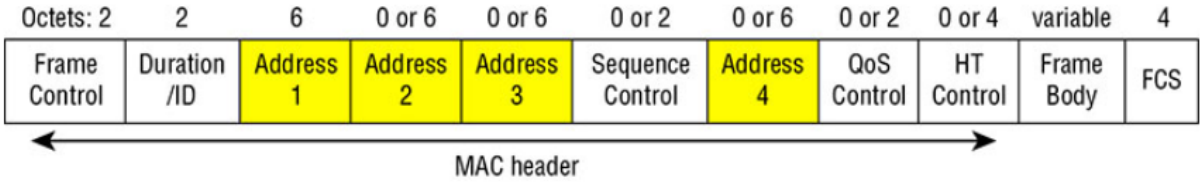
- 5.2 Analyze QoS configuration and operations
  - 5.2.1 Verify QoS parameters in capture files

General Frame Format

802.11 frames consist of three major parts: header, body, and trailer. The CWNA objectives include an understanding of the general frame format. The CWAP exam is all about understanding each frame type, which fields are used, and what each information element (IE) contains information about. We'll cover the basics for now.



Frame Format



Detailed Frame Format

Header

The frame header contains information about the where the frame is going, the data rate, cipher suite used to encrypt data frames, and more! It is important to understand each field in the header. The four address fields are source, destination, transmitter, and receiver. The header contents are different for each frame type; the image below shows that some fields may be 0 bytes when not in use or X bytes. For example, the header of an acknowledgement (ACK) frame only uses one of four address fields, the receiver address (RA). The other values found in the frame control field of the header that are frequently referenced include:

- DS Status – Indicates the directionality of the frame. Refer to the table below from the 802.11-2016 standard for the possible values and their meaning.
- More Fragments – if set to 1, the frame has been fragmented and has more fragments to transmit
- Retry – if set to 1, the previous attempt to transmit this frame failed.

Table 9-3—To/From DS combinations in Data frames

To DS and From DS values	Meaning
To DS = 0 From DS = 0	A Data frame from one STA to another STA within the same IBSS or the same PBSS, a Data frame direct from one non-AP STA to another non-AP STA within the same infrastructure BSS, or a Data frame outside the context of a BSS. This is the only valid combination for Data frames transmitted by an IBSS or PBSS STA, or outside the context of a BSS.
To DS = 1 From DS = 0	A Data frame destined for the DS or being sent by a STA associated with an AP to the Port Access Entity in that AP.
To DS = 0 From DS = 1	A Data frame exiting the DS or being sent by the Port Access Entity in an AP, or a group addressed mesh Data frame with the Mesh Control field present using the three-address MAC header format. This is the only valid combination for Data frames transmitted by an AP and group addressed Data frames transmitted by a mesh STA.
To DS = 1 From DS = 1	A Data frame using the four-address MAC header format. This standard defines procedures for using this combination of field values only in a mesh BSS. This is the only valid combination for individually addressed Data frames transmitted by a mesh STA.

To DS / From DS

The example below is from a QoS Data frame therefor it includes a QoS Control field as well.

```
▾ IEEE 802.11 QoS Data, Flags: .p.....T
    Type/Subtype: QoS Data (0x0028)
  ▾ Frame Control Field: 0x8841
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1000 .... = Subtype: 8
    ▾ Flags: 0x41
        .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
        .... .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
        .1.. .... = Protected flag: Data is protected
        0... .... = Order flag: Not strictly ordered
    .000 0000 0011 0000 = Duration: 48 microseconds
    Receiver address: Netgear_75:81:a1 (9c:3d:cf:75:81:a1)
    Transmitter address: AzureWav_14:94:6d (80:d2:1d:14:94:6d)
    Destination address: Netgear_75:81:a1 (9c:3d:cf:75:81:a1)
    Source address: AzureWav_14:94:6d (80:d2:1d:14:94:6d)
    BSS Id: Netgear_75:81:a1 (9c:3d:cf:75:81:a1)
    STA address: AzureWav_14:94:6d (80:d2:1d:14:94:6d)
    .... .... .... 0000 = Fragment number: 0
    1000 0011 1110 .... = Sequence number: 2110
  ▾ Qos Control: 0x0000
      .... .... .... 0000 = TID: 0
      [.... .... .... .000 = Priority: Best Effort (Best Effort) (0)]
      .... .... ...0 .... = QoS bit 4: Bits 8-15 of QoS Control field are TXOP Duration Requested
      .... .... .00. .... = Ack Policy: Normal Ack (0x0)
      .... .... 0... .... = Payload Type: MSDU
      0000 0000 .... .... = TXOP Duration Requested: 0 (no TXOP requested)
[Packet size limited during capture: IEEE 802.11 truncated]
```

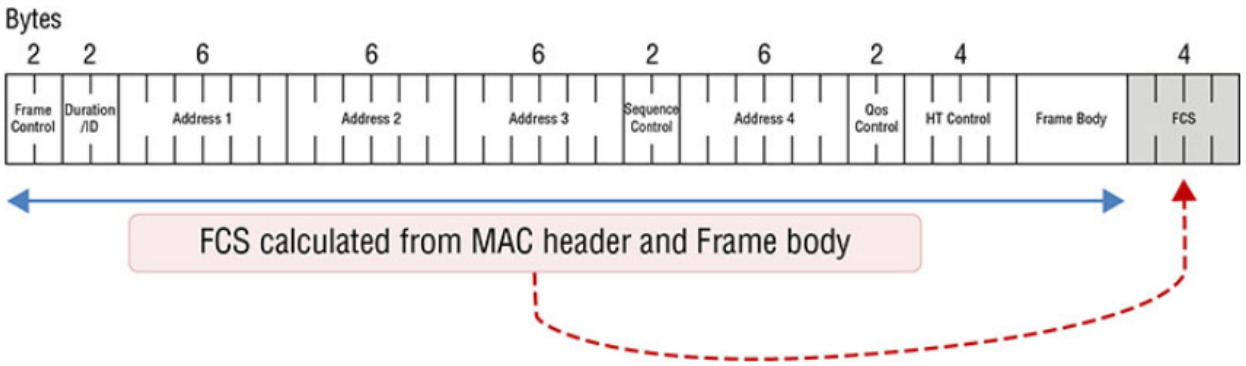
QoS Data Frame

Body

The body of an 802.11 frame contains the layer 3-7 information that is encapsulated and, hopefully, **protected** (encrypted) as well. The body of a frame varies in size depending on the transmission. For example, voice traffic frames will be smaller than a file download that will increase the TCP window based on the speed/reliability of the connection end-to-end.

Trailer

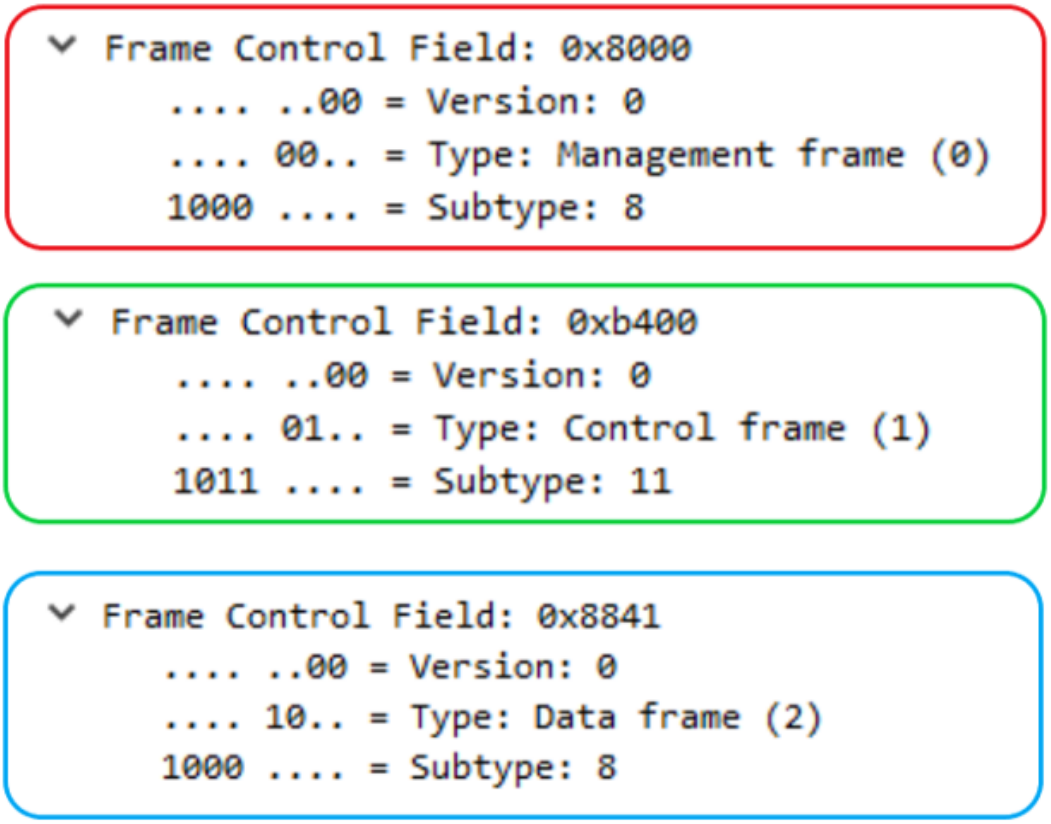
The trailer contains the frame check sequence (FCS). This is a 32-bit cyclic redundancy check (CRC) used to validate that the contents of the entire frame have not been tampered with or become corrupted while being transferred over the wireless medium. All values of the frame header and body are ran through a calculation; the result is held in the FCS field. If the receiver runs the frame through the same calculation but the result is not the same, the frame is corrupt/damaged. The receiver will discard the frame and not send an ACK frame. The sender knows to retransmit the frame because it did not receive acknowledgement. This is typically a result of high interference/collisions. Typically, the station that receives a bad CRC will discard the frame instead of forwarding it onto the operating system so you will not be able to see “bad” frames within protocol analyzers such as Wireshark.



FCS

Frame Types

All 802.11 frames fall under one of the three types: management, control, or data. The 802.11ac-2013 standard states that all data frames be sent as QoS data frames. In the header there is a frame control field that contains the values for type and subtype of the frame. The image below shows the three types of frames. Protocol version will always be 00 to indicate that 802.11 is in use. The **type** field indicates 0-management, 1-control, or 2-data. The **subtype** field indicates the type of management, control, or data frame. In our example here we see 8, 11, and 8 in the subtype fields. The management frame is a beacon, the control frame is a request-to-send (RTS), and the data frame is a QoS Data frame.



Type and Subtype

Management Frames

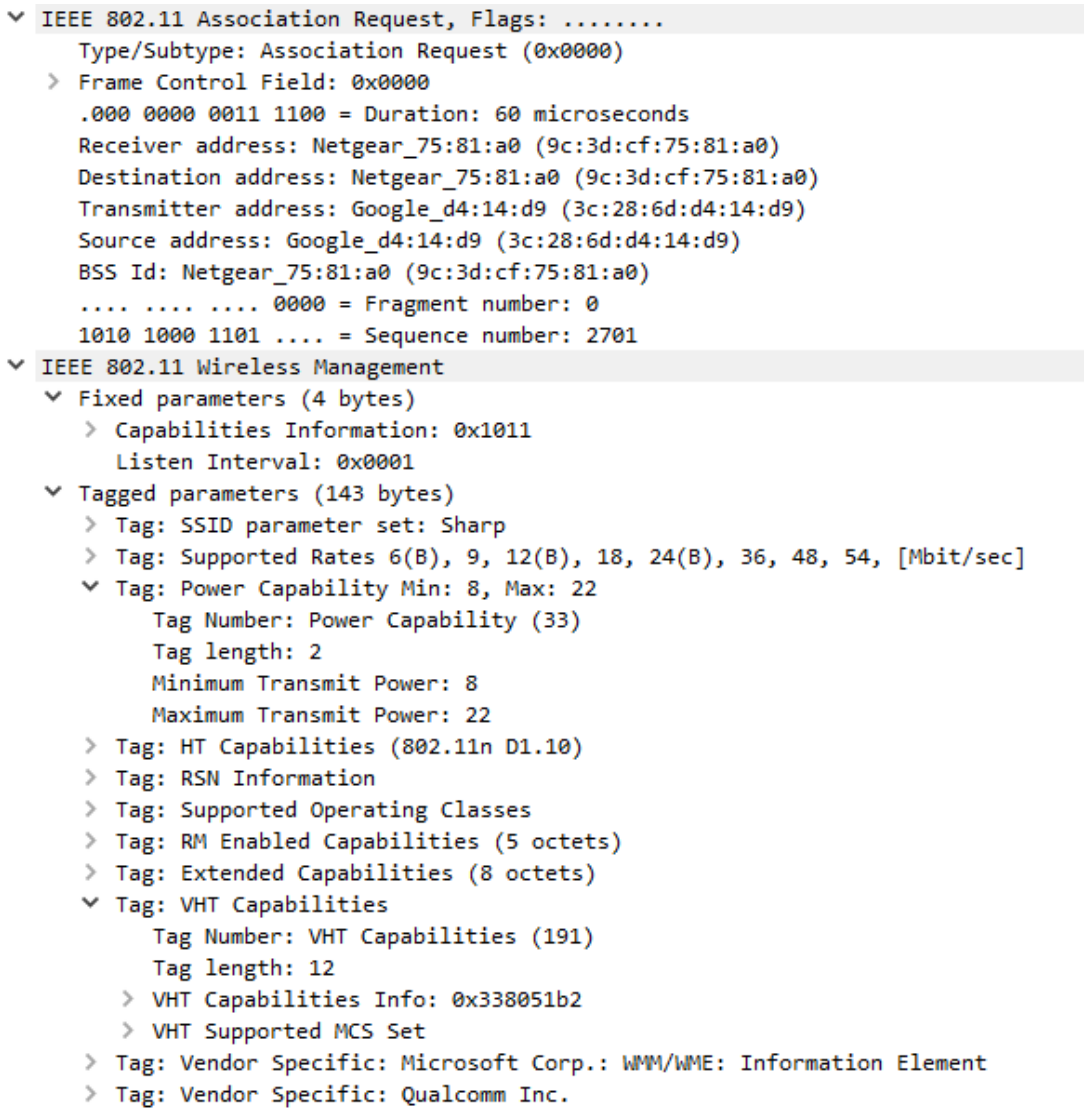
Management frames are used to manage the BSS. This includes probing, associating, roaming, and disconnecting clients from the BSS. As shown above, management frames use a type of 0 in the frame control field within the frame header.

Subtype Field	Description
0000	Association request
0010	Reassociation request
0100	Probe request
0110	Timing advertisement
1000	Beacon
1010	Disassociation
1100	Deauthentication
1011	Authentication
1110	Action
0001	Association response
0011	Reassociation response
0101	Probe response

0111	Reserved

Association Request/Response

Stations send association requests to access points (APs) requesting to join the BSS. In this frame, the station sends all its capabilities to the AP; it will only include capabilities that the AP has also advertised in the beacon or probe response frame. The AP responds to the station using an association response frame that includes an association ID (AID). Each station within the BSS has a unique AID.



Association Request

Reassociation Request/Response

Stations send reassociation requests to APs that wish to roam to. The AP responds to the station the same way it does in the association request/response. The primary difference between reassociation and association requests is that the station will indicate the current AP it is connected to in reassociation requests. If the station does not receive a reassociation response for reasons such as load

balancing, it will remain connected to the original AP and search for other APs to roam to. There are also cases where, after leaving a BSS for a short period of time, a station will send a reassociation request to an AP it was recently connected to.

Table 9-31—Reassociation Request frame body

Order	Information	Notes
1	Capability Information	
2	Listen Interval	
3	Current AP address	
4	SSID	
5	Supported Rates and BSS Membership Selectors	This field is not present if dot11DMGOptionImplemented is true.
6	Extended Supported Rates and BSS Membership Selectors	The Extended Supported Rates and BSS Membership Selectors element is present if there are more than eight supported rates, and it is optional otherwise. This element is not present if dot11DMGOptionImplemented is true.
7	Power Capability	The Power Capability element is present if dot11SpectrumManagementRequired is true or dot11RadioMeasurementActivated is true.
8	Supported Channels	The Supported Channels element is present if dot11SpectrumManagementRequired is true and dot11ExtendedChannelSwitchActivated is false.

Partial Reassociation Request frame body

Probe Request/Response

As part of the active ad passive scanning processes, stations send probe requests with a specific SSID, wildcard, or no value (null) in the “SSID Parameter Set” field to search for wireless networks. When the field is wildcard/null, the client is requesting any AP nearby to respond with all SSIDs using a probe response frame. When the probe request contains a specific SSID, the client is requesting any AP nearby to respond if they support that SSID. The probe response frame is a targeted beacon that is sent to the station who is “probing”. As you can see below, the probe response frame contains all but 3 of the same fields as beacon frames. The three differences are: the probe response frame does not contain a TIM, a QoS capabilities information element, and any information elements requested by the station. Be sure to understand the differences between active and passive scanning for both exams.

```
▼ IEEE 802.11 Probe Request, Flags: ........
    Type/Subtype: Probe Request (0x0004)
  ▶ Frame Control Field: 0x4000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: IntelCor_ac:7e:48 (48:89:e7:ac:7e:48)
    Source address: IntelCor_ac:7e:48 (48:89:e7:ac:7e:48)
    BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
    .... .... .... 0000 = Fragment number: 0
    0011 0100 0100 .... = Sequence number: 836
▼ IEEE 802.11 Wireless Management
  ▼ Tagged parameters (46 bytes)
    ▼ Tag: SSID parameter set: Wildcard SSID
        Tag Number: SSID parameter set (0)
        Tag length: 0
        SSID:
    ▶ Tag: Supported Rates 1, 2, 5.5, 11, 6, 9, 12, 18, [Mbit/sec]
    ▶ Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    ▼ Tag: HT Capabilities (802.11n D1.10)
        Tag Number: HT Capabilities (802.11n D1.10) (45)
        Tag length: 26
      ▶ HT Capabilities Info: 0x09e7
      ▶ A-MPDU Parameters: 0x17
      ▶ Rx Supported Modulation and Coding Scheme Set: MCS Set
      ▶ HT Extended Capabilities: 0x0000
      ▶ Transmit Beam Forming (TxBF) Capabilities: 0x00000000
      ▶ Antenna Selection (ASEL) Capabilities: 0x00
```

Probe Request with Wildcard SSID

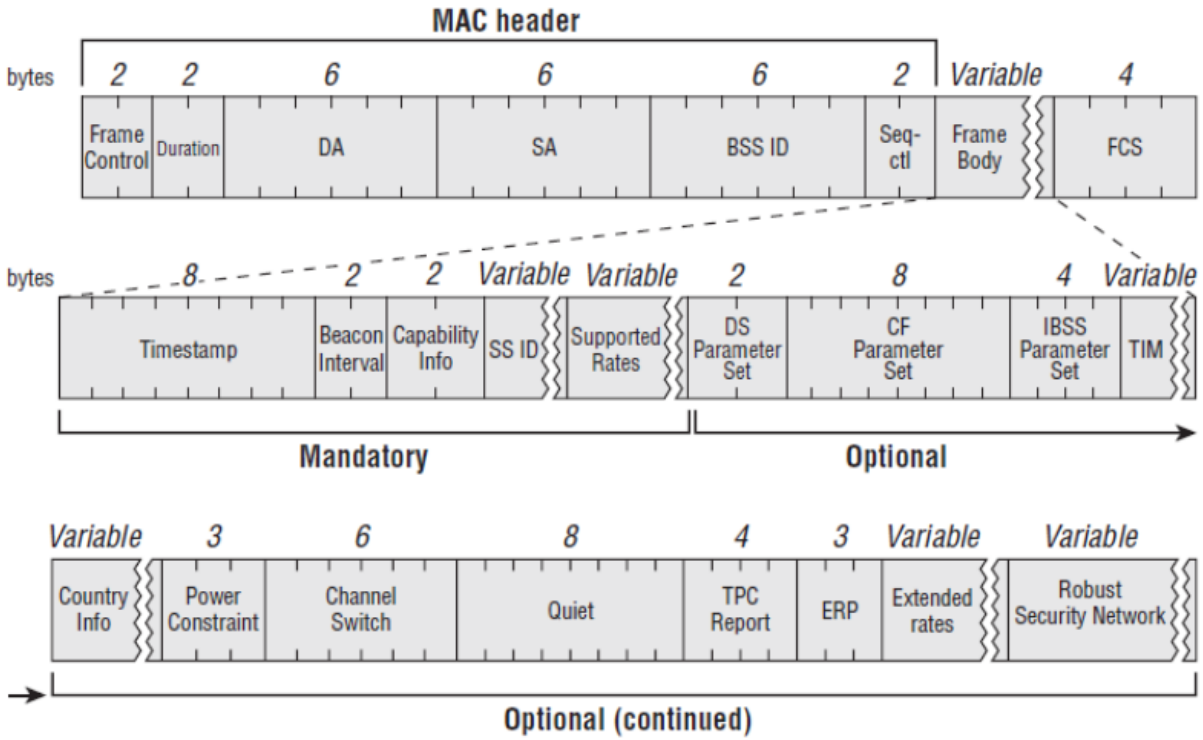
```
IEEE 802.11 Probe Response, Flags: ........
   Type/Subtype: Probe Response (0x0005)
   Frame Control Field: 0x5000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      0101 .... = Subtype: 5
   > Flags: 0x00
   .000 0000 0011 1100 = Duration: 60 microseconds
   Receiver address: IntelCor_ac:7e:48 (48:89:e7:ac:7e:48)
   Destination address: IntelCor_ac:7e:48 (48:89:e7:ac:7e:48)
   Transmitter address: Cisco_ee:2b:ef (2c:d0:2d:ee:2b:ef)
   Source address: Cisco_ee:2b:ef (2c:d0:2d:ee:2b:ef)
   BSS Id: Cisco_ee:2b:ef (2c:d0:2d:ee:2b:ef)
   .... .... .... 0000 = Fragment number: 0
   0100 0001 0111 .... = Sequence number: 1047
IEEE 802.11 Wireless Management
   Fixed parameters (12 bytes)
      Timestamp: 3011473874
      Beacon Interval: 0.102400 [Seconds]
   > Capabilities Information: 0x1011
   Tagged parameters (255 bytes)
      Tag: SSID parameter set: Survey_CDW
         Tag Number: SSID parameter set (0)
         Tag length: 10
         SSID: Survey_CDW
   > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
   > Tag: DS Parameter set: Current Channel: 161
   > Tag: Country Information: Country Code US, Environment Any
   > Tag: RSN Information
   > Tag: QBSS Load Element 802.11e CCA Version
   > Tag: RM Enabled Capabilities (5 octets)
   > Tag: Mobility Domain
   > Tag: HT Capabilities (802.11n D1.10)
   > Tag: HT Information (802.11n D1.10)
   > Tag: Extended Capabilities (8 octets)
   > Tag: VHT Capabilities
   > Tag: VHT Operation
   > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
```

Probe Response

Beacon

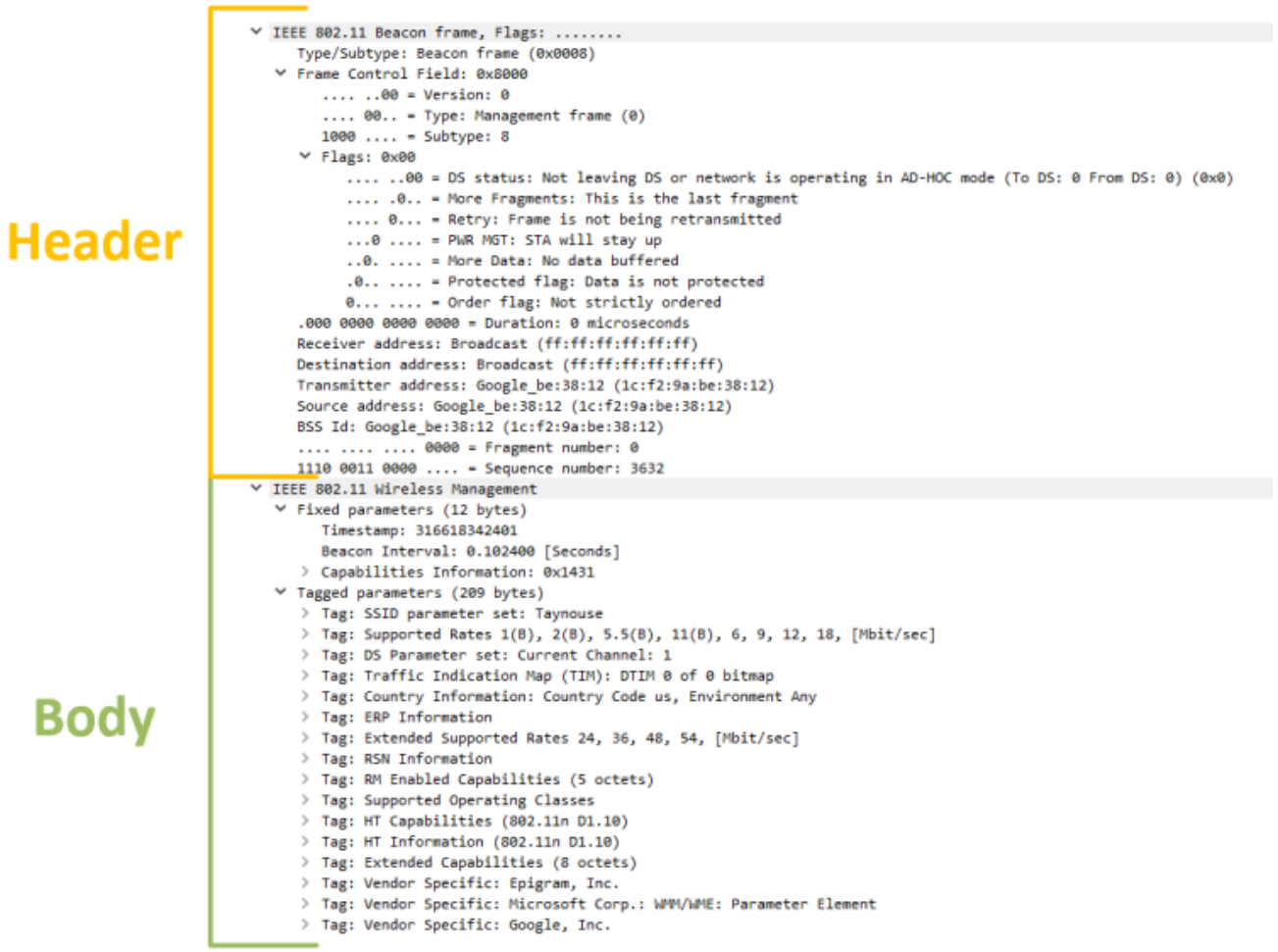
APs send beacons at a regular interval called the target beacon transmit time (TBTT) to advertise the SSIDs they service. Beacons contain the configuration of the WLAN including whether it supports standards such as 802.11k, 802.11r, the required cipher suites and authentication key management (AKM) methods, whether protection mechanisms are required, etc. The presence of certain information elements (IE) indicate whether the related configuration is present. The figure below shows which fields are mandatory in a beacon frame. Note that this information is in the body of the management frame.

FIGURE 4.5 Beacon frame structure

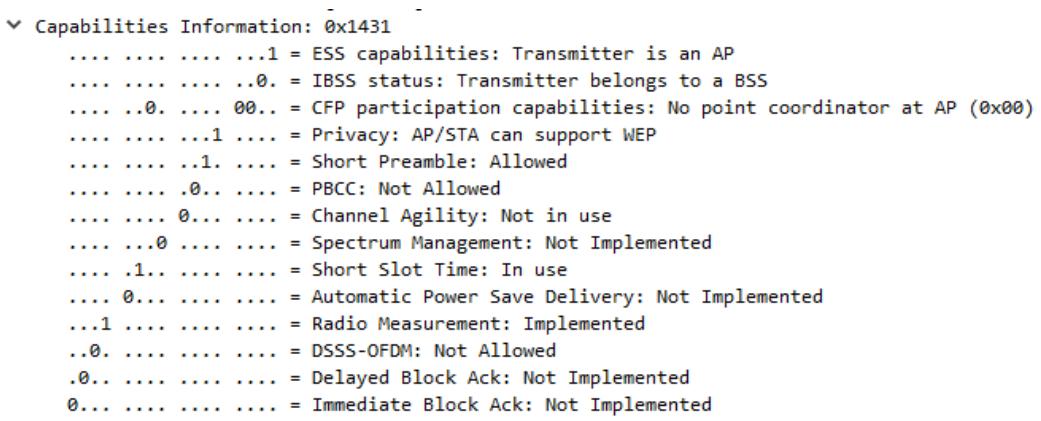


Beacon Frame Format

Below shows a beacon frame in Wireshark. We can see a timestamp of 316618342401 which is used to keep time synchronized among stations in a BSS. Our beacon interval, also known as target beacon transmit time (TBTT) is the default of 102.4ms. The required “Capability Info” field is expanded below. The SSID being advertised by the beacon is “Taynouse” and supported data rates are listed following. It is important to capture your own beacons and start poking around; the number of optional fields is much longer than the required fields. It is important to know the names and purpose of all the beacon fields for the CWAP exam. I highly recommend downloading a copy of the 802.11-2016 standard for free here and searching for each of these fields yourself.

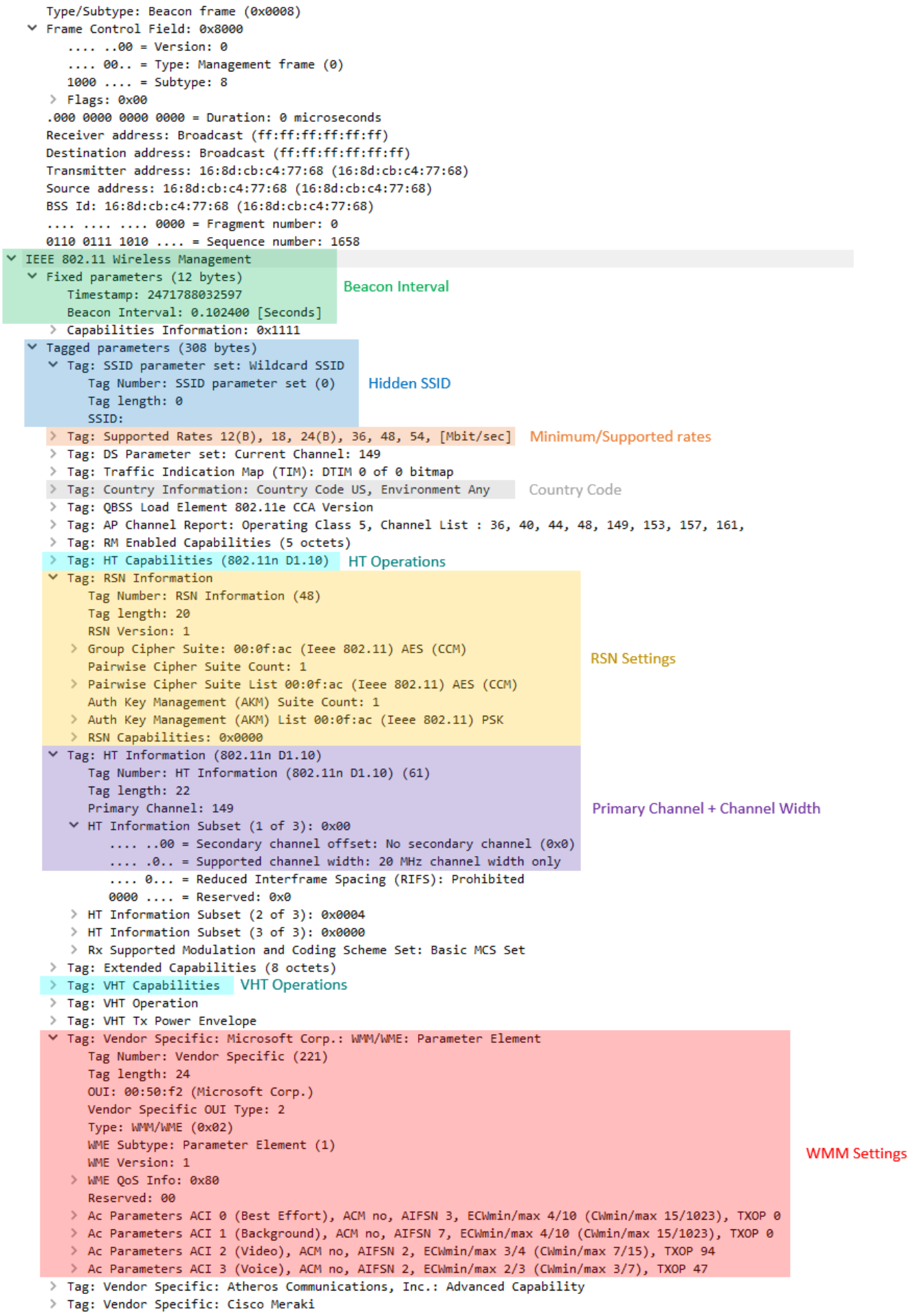


Beacon Header and Body



Required Capabilities Information in Beacons

The CWAP objectives state that you should be able to determine the configuration of a BSS from looking at a decoded BSS frame. I have highlighted the areas of importance below.

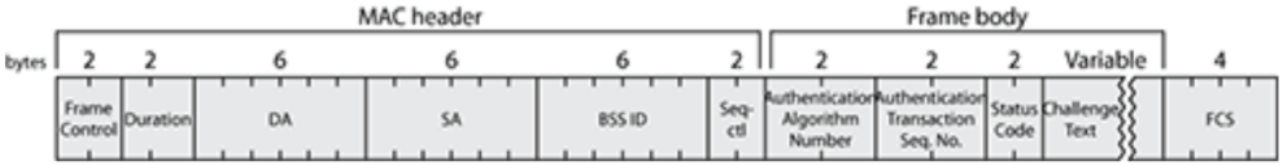


BSS Configuration

Authentication

Authentication frames are used to join the BSS as part of the open system authentication process. Open system authentication is a simple process used to verify that the station attempting to join the BSS has the capabilities to do so. The station sends an authentication request and the AP sends an authentication response. The body of the authentication frame includes the algorithm number, transaction sequence number, and status code. With open system authentication, the authentication algorithm number is 0. The sequence number will either be 1 or 2 to indicate which frame of the two-frame transaction you are viewing. The authentication response frame is always sequence number 2 and will include a status code indicating success or fail.

Figure 4-8: Authentication frame format



Authentication Frame Format

```
▼ IEEE 802.11 Authentication, Flags: ........C
    Type/Subtype: Authentication (0x000b)
  ▼ Frame Control Field: 0xb000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1011 .... = Subtype: 11
    ▶ Flags: 0x00
    .000 0000 0010 1100 = Duration: 44 microseconds
    Receiver address: Apple_e0:30:c0 (40:4d:7f:e0:30:c0)
    Destination address: Apple_e0:30:c0 (40:4d:7f:e0:30:c0)
    Transmitter address: ea:55:2d:c0:75:e0 (ea:55:2d:c0:75:e0)
    Source address: ea:55:2d:c0:75:e0 (ea:55:2d:c0:75:e0)
    BSS Id: ea:55:2d:c0:75:e0 (ea:55:2d:c0:75:e0)
    .... .... .... 0000 = Fragment number: 0
    0011 1011 0001 .... = Sequence number: 945
    Frame check sequence: 0x144184ca [unverified]
    [FCS Status: Unverified]
▼ IEEE 802.11 Wireless Management
  ▼ Fixed parameters (6 bytes)
      Authentication Algorithm: Open System (0)
      Authentication SEQ: 0x0002
      Status code: Successful (0x0000)
```

Authentication Frame

The PCAP below shows deauthentication, disassociation, reassociation, authentication, and the 4-way handshake!

From Deauth to Reassociation PCAP

Disassociation

A type of management frame sent from either the station or the AP. Disassociation frames are used to terminate the station's association; it is a notification and does not expect a response. Clients may disassociate prior to powering off. APs may disassociate clients for various reasons including failure to properly authenticate, for load balancing or timeout reasons, entering a state of maintenance, etc. The 802.11-2016 standard includes a list of disassociation reasons. When a station is disassociated it still maintains its authentication. This makes it easier for the client to associate again in the future. The table below is part of table 9-45 showing reason codes for disassociation from the 802.11-2016 standard.

Table 9-45—Reason codes

Reason code	Name	Meaning
0		Reserved
1	UNSPECIFIED_REASON	Unspecified reason
2	INVALID_AUTHENTICATION	Previous authentication no longer valid
3	LEAVING_NETWORK_DEAUTH	Deauthenticated because sending STA is leaving (or has left) IBSS or ESS
4	REASON_INACTIVITY	Disassociated due to inactivity
5	NO_MORE_STAS	Disassociated because AP is unable to handle all currently associated STAs
6	INVALID_CLASS2_FRAME	Class 2 frame received from nonauthenticated STA
7	INVALID_CLASS3_FRAME	Class 3 frame received from nonassociated STA
8	LEAVING_NETWORK_DISASSOC	Disassociated because sending STA is leaving (or has left) BSS
9	NOT_AUTHENTICATED	STA requesting (re)association is not authenticated with responding STA
10	UNACCEPTABLE_POWER_CAPABILITY	Disassociated because the information in the Power Capability element is unacceptable
11	UNACCEPTABLE_SUPPORTED_CHANNELS	Disassociated because the information in the Supported Channels element is unacceptable
12	BSS_TRANSITION_DISASSOC	Disassociated due to BSS transition management
13	REASON_INVALID_ELEMENT	Invalid element, i.e., an element defined in this standard for which the content does not meet the specifications in Clause 9
14	MIC_FAILURE	Message integrity code (MIC) failure
15	4WAY_HANDSHAKE_TIMEOUT	4-way handshake timeout
16	GK_HANDSHAKE_TIMEOUT	Group key handshake timeout
17	HANDSHAKE_ELEMENT_MISMATCH	Element in 4-way handshake different from (Re)Association Request/Probe Response/Beacon frame

Reason Code Table

In the example below, we can see reason code 8 (LEAVING_NETWORK_DISASSOC): Disassociated because sending STA is leaving (or has left) BSS.

```
IEEE 802.11 Disassociate, Flags: ........
   Type/Subtype: Disassociate (0x000a)
   Frame Control Field: 0xa000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1010 .... = Subtype: 10
   > Flags: 0x00
   .000 0000 0011 1100 = Duration: 60 microseconds
   Receiver address: Cisco_3b:51:c6 (00:08:2f:3b:51:c6)
   Destination address: Cisco_3b:51:c6 (00:08:2f:3b:51:c6)
   Transmitter address: Google_d4:14:d9 (3c:28:6d:d4:14:d9)
   Source address: Google_d4:14:d9 (3c:28:6d:d4:14:d9)
   BSS Id: Cisco_3b:51:c6 (00:08:2f:3b:51:c6)
   .... .... .... 0000 = Fragment number: 0
   0000 0000 0000 .... = Sequence number: 0
IEEE 802.11 Wireless Management
   Fixed parameters (2 bytes)
      Reason code: Disassociated because sending STA is leaving (or has left) BSS (0x0008)
```

Disassociate Frame

Deauthentication

Deauthentication frames are used to reset the state machine for an associated client. The authentication process takes place prior to association therefor, if a station is deauthenticated, it is also disassociated. Deauthentication frames also include a reason code in the body of the frame from the table mentioned above. Know that deauthenticating a client resets their process in the 802.11 state machine back to step 1.

```
IEEE 802.11 Deauthentication, Flags: ........
   Type/Subtype: Deauthentication (0x000c)
   > Frame Control Field: 0xc000
   .000 0000 0011 1100 = Duration: 60 microseconds
   Receiver address: Netgear_75:81:a0 (9c:3d:cf:75:81:a0)
   Destination address: Netgear_75:81:a0 (9c:3d:cf:75:81:a0)
   Transmitter address: Google_d4:14:d9 (3c:28:6d:d4:14:d9)
   Source address: Google_d4:14:d9 (3c:28:6d:d4:14:d9)
   BSS Id: Netgear_75:81:a0 (9c:3d:cf:75:81:a0)
   .... .... .... 0000 = Fragment number: 0
   1010 1000 1110 .... = Sequence number: 2702
IEEE 802.11 Wireless Management
   Fixed parameters (2 bytes)
      Reason code: Deauthenticated because sending STA is leaving (or has left) IBSS or ESS (0x0003)
```

Deauthentication Frame

Action

Action frames are management frames that trigger an action to happen. The list of management frame subtypes had become exhausted, so instead of creating new management frames as new technologies required them, the action frame can be used. Action frames do not expect an ACK. They were first introduced in the 802.11h-2003 standard which also introduced transmit power control (TPC) and dynamic frequency selection (DFS). The 802.11-2016 standard includes action frames for many categories such as spectrum management, QoS, HT, VHT, radio measurements, and many more. The table below from 9.6.2.1 of the 802.11-2016 standard shows the spectrum management action frames.

Table 9-285—Spectrum Management Action field values

Spectrum Management Action field value	Description
0	Measurement Request
1	Measurement Report
2	TPC Request
3	TPC Report
4	Channel Switch Announcement
5–255	Reserved

Spectrum Management Action Frames

Below we can see the action frame type of “Action No Ack” and an example frame used to communicate a compressed beamforming report.

Table 9-39—Action No Ack frame body

Order	Information
1	Action
Last	One or more vendor-specific elements are optionally present. This element follows all other elements.

Action No ACK

```
IEEE 802.11 Action No Ack, Flags: ........
    Type/Subtype: Action No Ack (0x000e)
  > Frame Control Field: 0xe000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Netgear_75:81:a0 (9c:3d:cf:75:81:a0)
    Destination address: Netgear_75:81:a0 (9c:3d:cf:75:81:a0)
    Transmitter address: IntelCor_ac:7e:48 (48:89:e7:ac:7e:48)
    Source address: IntelCor_ac:7e:48 (48:89:e7:ac:7e:48)
    BSS Id: Netgear_75:81:a0 (9c:3d:cf:75:81:a0)
    .... .... .... 0000 = Fragment number: 0
    1111 1111 1111 .... = Sequence number: 4095
IEEE 802.11 Wireless Management
  Fixed parameters
      Category code: VHT (21)
      VHT Action: VHT Compressed Beamforming (0)
    VHT MIMO Control: 0x248491, Nc Index: 2 Columns, Nr Index: 3 Rows, Channel Width: 80 MHz, Grouping (Ng): 1 (No Grouping), Feedback Type: SU
        .... .... .... .... .... .001 = Nc Index: 2 Columns (0x1)
        .... .... .... .... ..01 0... = Nr Index: 3 Rows (0x2)
        .... .... .... .... 10.. .... = Channel Width: 80 MHz (0x2)
        .... .... .... ..00 .... .... = Grouping (Ng): 1 (No Grouping) (0x0)
        .... .... .... .1.. .... .... = Codebook Information: 0x1
        .... .... .... 0... .... .... = Feedback Type: SU (0x0)
        .... .... .000 .... .... .... = Remaining Feedback Segments: 0x0
        .... .... 1... .... .... .... = First Feedback Segments: 0x1
        .... ..00 .... .... .... .... = Reserved: 0x0
        0010 01.. .... .... .... .... = Sounding Dialog Token Number: 0x09
    VHT Compressed Beamforming Report: 18f55299d22285a6a858a5292a52698a7ad399b29e64a6b0…
      Average Signal to Noise Ratio
          Stream 1 - Signal to Noise Ratio:  28.00dB
          Stream 2 - Signal to Noise Ratio:  19.25dB
      PHI and PSI Angle Decode
          PHI(6 bits):    PHI11: 20, PHI21: 41, PHI22: 39
          PSI(4 bits):    PSI21: 4, PSI31: 8, PSI32: 8
      Beamforming Feedback Matrix
```

Action No Ack Frame

This action frame is an “add block ack response” (ADDBA) action frame. It is used to setup the block ack policy for the exchange of blocks of QoS data frames.

```
IEEE 802.11 Action, Flags: ........
    Type/Subtype: Action (0x000d)
  > Frame Control Field: 0xd000
    .000 0000 0011 1100 = Duration: 60 microseconds
    Receiver address: Google_d4:14:d9 (3c:28:6d:d4:14:d9)
    Destination address: Google_d4:14:d9 (3c:28:6d:d4:14:d9)
    Transmitter address: Netgear_75:81:a0 (9c:3d:cf:75:81:a0)
    Source address: Netgear_75:81:a0 (9c:3d:cf:75:81:a0)
    BSS Id: Netgear_75:81:a0 (9c:3d:cf:75:81:a0)
    .... .... .... 0000 = Fragment number: 0
    0110 0011 0001 .... = Sequence number: 1585
IEEE 802.11 Wireless Management
  Fixed parameters
      Category code: Block Ack (3)
      Action code: Add Block Ack Response (0x01)
      Dialog token: 0x01
      Status code: Successful (0x0000)
    Block Ack Parameters: 0x1002, Block Ack Policy
        .... .... .... ...0 = A-MSDUs: Not Permitted
        .... .... .... ..1. = Block Ack Policy: Immediate Block Ack
        .... .... ..00 00.. = Traffic Identifier: 0x0
        0001 0000 00.. .... = Number of Buffers (1 Buffer = 2304 Bytes): 64
      Block Ack Timeout: 0x0000
```

Action ADDBA

Timing Advertisement

Timing advertisement frames were introduced in 802.11p-2010; this standard describes how Wi-Fi can be used in vehicular environments. This type of management frame is not in use today and is expected to be used to communicate time values to devices that cannot maintain their own timing.

Control Frames

Control frames are used to control access to the medium and are used for frame acknowledgement. Control frames only contain a header and trailer, no body. The control frame types bolded in the table below are only used in point coordination function (PCF) based wireless networks. These were never implemented in the real world.

Subtype Field	Description
0100	Beamforming Report Poll
0101	VHT/HE NDP Announcement
0110	Control Frame Extension
0111	Control wrapper
1000	Block ACK Request
1001	Block ACK
1010	PS-Poll
1011	RTS
1100	CTS
1101	ACK
1110	**CF-End**
1111	**CF-END+CF-ACK**

Request to Send – RTS

Stations send RTS frames to reserve the medium for the amount of time, in microseconds, found in the duration field in the frame header. RTS and CTS frames are very simple. The medium will not be reserved for the station until it receives a clear to send frame response from the access point. I explain the RTS/CTS process in detail in my Wireless Contention Mechanisms post. RTS/CTS are used as a NAV distribution method as part of the virtual carrier sense process.

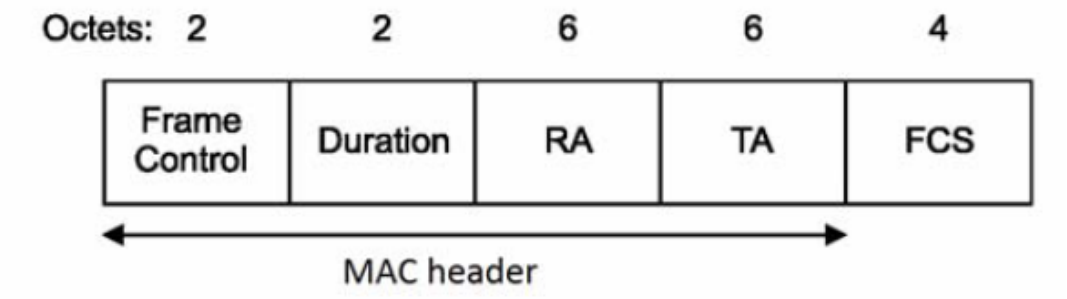


Figure 9-20—RTS frame

RTS Frame Format

```
IEEE 802.11 Request-to-send, Flags: ........
   Type/Subtype: Request-to-send (0x001b)
   Frame Control Field: 0xb400
      .... ..00 = Version: 0
      .... 01.. = Type: Control frame (1)
      1011 .... = Subtype: 11
    > Flags: 0x00
   .000 0000 1001 1010 = Duration: 154 microseconds
   Receiver address: Cisco_30:95:0b (0c:85:25:30:95:0b)
   Transmitter address: MurataMa_1a:e5:e4 (b8:d7:af:1a:e5:e4)
```

RTS Frame

Clear to Send – CTS

Frame sent by an AP in response to an RTS frame sent by a station. CTS messages are sent at the lowest mandatory data rate, allowing them to reach all stations in the BSS. They only use the **receiver address** (RA) field in the header. The station in the receiver address field is the one that will be transmitting frames.

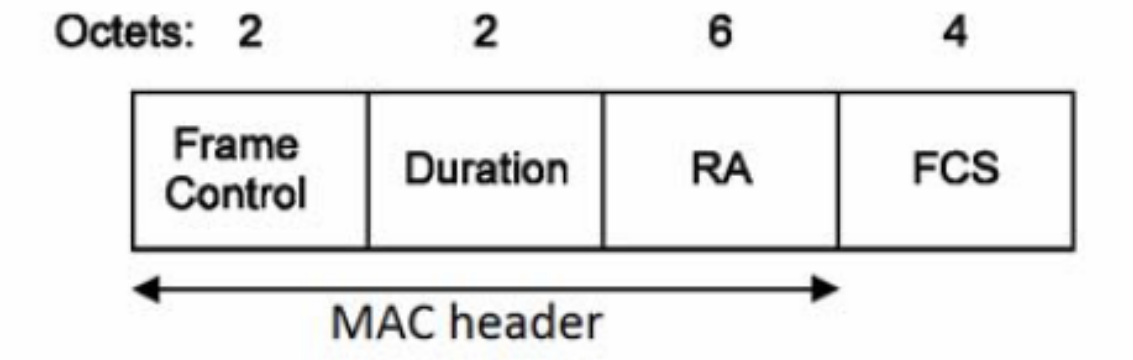
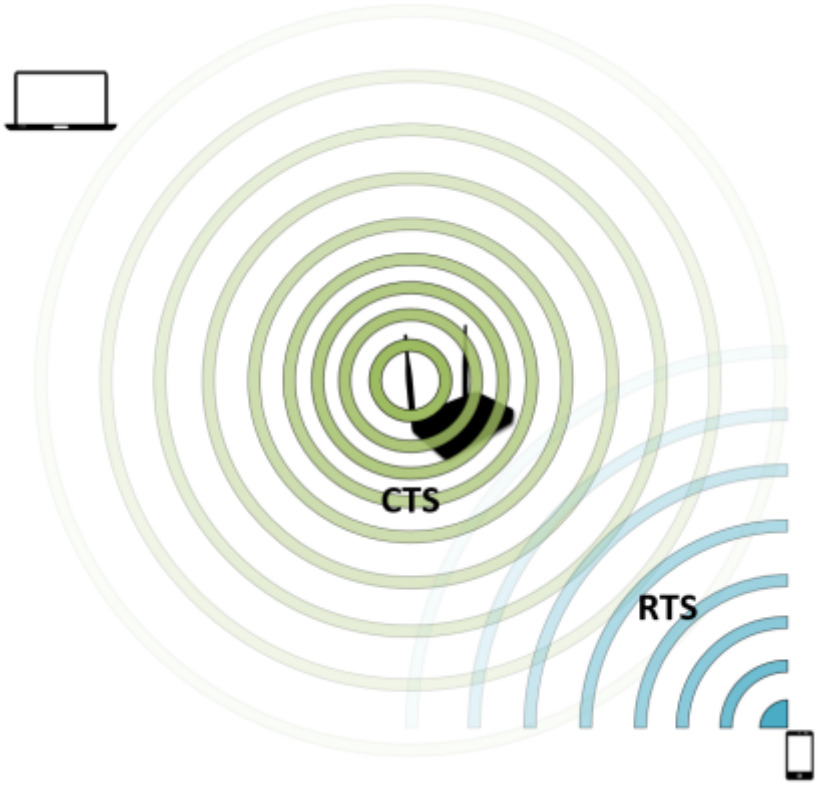


Figure 9-21—CTS frame

CTS Frame Format

```
IEEE 802.11 Clear-to-send, Flags: ........
   Type/Subtype: Clear-to-send (0x001c)
   Frame Control Field: 0xc400
      .... ..00 = Version: 0
      .... 01.. = Type: Control frame (1)
      1100 .... = Subtype: 12
   > Flags: 0x00
   .000 0000 1000 1010 = Duration: 138 microseconds
   Receiver address: Apple_1d:99:c5 (d4:61:da:1d:99:c5)
```

CTS Frame



Acknowledgement – ACK

ACK frames create a delivery verification method; they are expected after the transmission of data frames to confirm receipt of the frame. If the CRC check fails, the receiver will not send an ACK. If the sender does not receive an ACK, it will retransmit the frame.

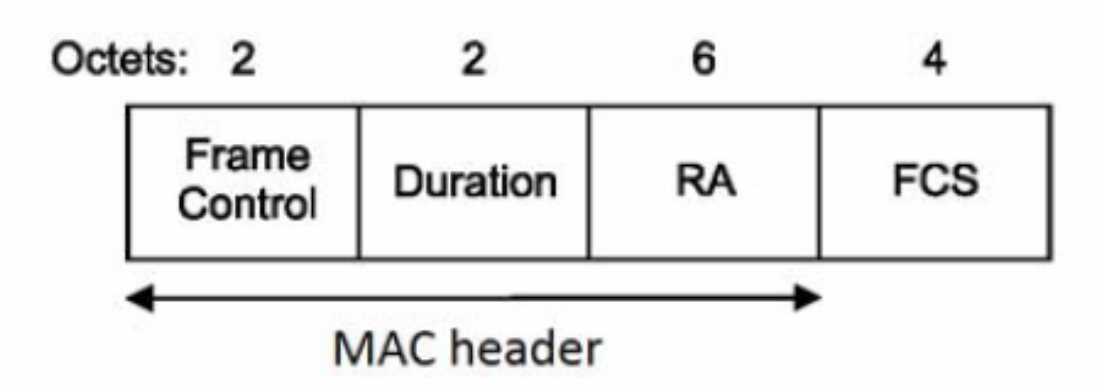
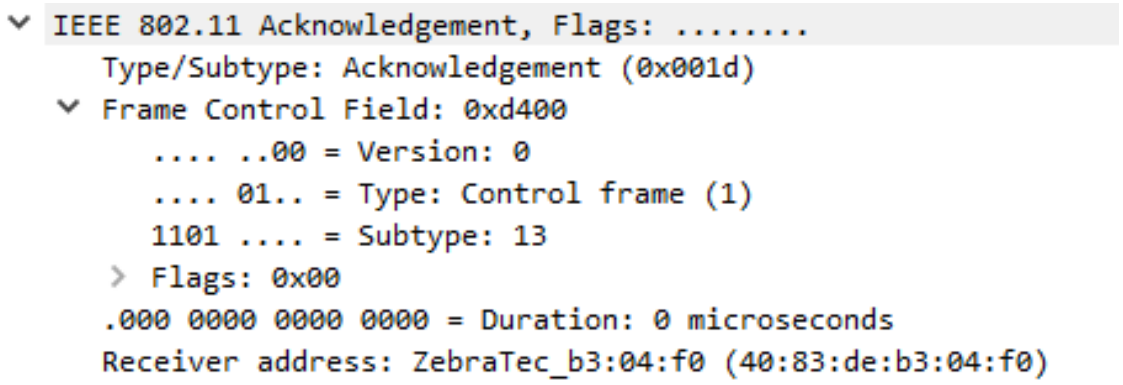


Figure 9-22—Ack frame

ACK Frame Format



ACK Frame

PS-Poll

PS-Poll frames are used in the legacy 802.11-1997 power save method to request frames buffered on the AP while the client was sleeping. Clients include their AID in the Duration/ID field when sending PS-Poll frames. The process is covered in greater detail in my Power Save Methods post.

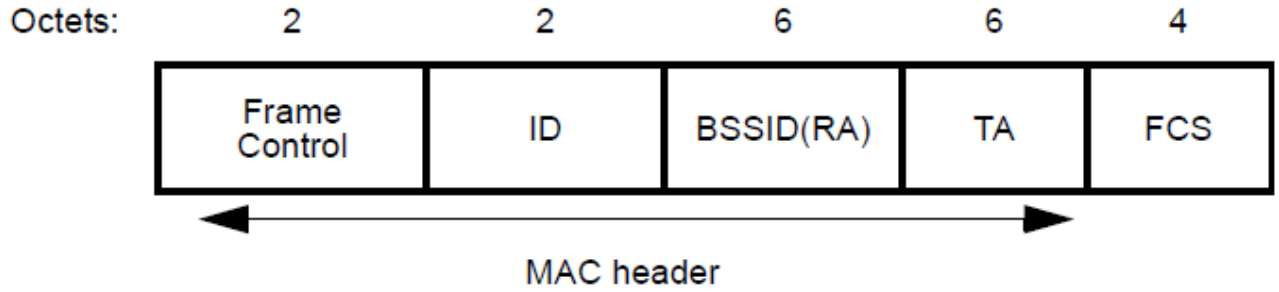


Figure 9-23—PS-Poll frame

PS-Poll Frame Format

Block ACK / Block ACK Request

Introduced in 802.11e-2005, block acknowledgements are used to confirm receipt of a block of QoS data frames. A station will send multiple QoS data frames followed by a block ack request (BAR). The AP will send a block ack frame back that includes a bitmap that indicates which frames were received. With this method, only the frames indicated by the bitmap that weren't received are retransmitted. This increases the overall network efficiency by reducing the amount of ACK frames that need to be sent.

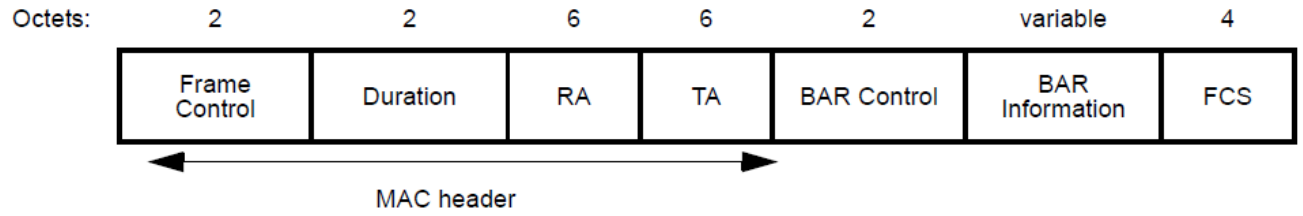


Figure 9-26—BlockAckReq frame

BAR Frame Format

The block ack below shows a BA Ack Policy of 0 meaning immediate acknowledgement of the transmitted frames is required.

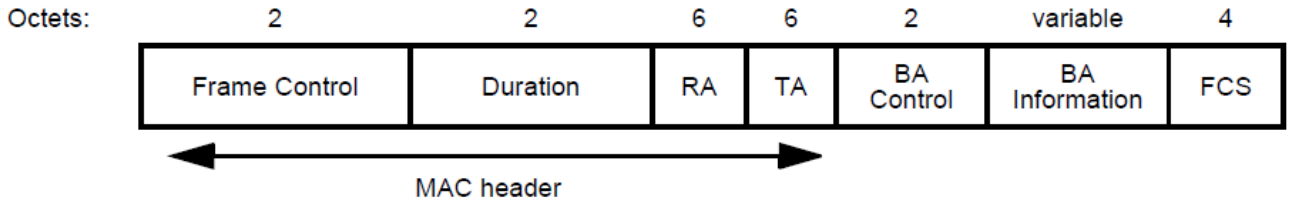


Figure 9-32—BlockAck frame

Block ACK Frame Format

```
IEEE 802.11 802.11 Block Ack, Flags: ........
   Type/Subtype: 802.11 Block Ack (0x0019)
   Frame Control Field: 0x9400
      .... ..00 = Version: 0
      .... 01.. = Type: Control frame (1)
      1001 .... = Subtype: 9
    > Flags: 0x00
   .000 0000 0000 0000 = Duration: 0 microseconds
   Receiver address: Netgear_75:81:a0 (9c:3d:cf:75:81:a0)
   Transmitter address: IntelCor_ac:7e:48 (48:89:e7:ac:7e:48)
   Compressed BlockAck Response
      Block Ack Control: 0x5004
         .... .... .... ...0 = BA Ack Policy: Immediate Acknowledgement Required
         .... .... ...0 010. = BA Type: Compressed BlockAck (0x2)
         .... 0000 000. .... = Reserved: 0x00
         0101 .... .... .... = TID for which a Basic BlockAck frame is requested: 0x5
      Block Ack Starting Sequence Control (SSC): 0xcd40
         .... .... .... 0000 = Fragment: 0
         1100 1101 0100 .... = Starting Sequence Number: 3284
      Block Ack Bitmap: ffffffffffffffff
```

Block ACK Frame

```
IEEE 802.11 802.11 Block Ack Req, Flags: ........
    Type/Subtype: 802.11 Block Ack Req (0x0018)
  Frame Control Field: 0x8400
      .... ..00 = Version: 0
      .... 01.. = Type: Control frame (1)
      1000 .... = Subtype: 8
    Flags: 0x00
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
        .... .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 0010 1100 = Duration: 44 microseconds
  Receiver address: IntelCor_b6:43:cc (e0:9d:31:b6:43:cc)
  Transmitter address: Cisco_b7:ad:2d (7c:0e:ce:b7:ad:2d)
  Compressed BlockAck Request
    Block Ack Control: 0x0004
        .... .... .... ...0 = BA Ack Policy: Immediate Acknowledgement Required
        .... .... ...0 010. = BA Type: Compressed BlockAck (0x2)
        .... 0000 000. .... = Reserved: 0x00
        0000 .... .... .... = TID for which a Basic BlockAck frame is requested: 0x0
    Block Ack Starting Sequence Control (SSC): 0x0160
        .... .... .... 0000 = Fragment: 0
        0000 0001 0110 .... = Starting Sequence Number: 22
```

BAR Frame

Beamforming Report Poll

Beamforming report poll frames are sent from the beamformer (the AP) to beamformees (STAs) to request additional feedback about the RF conditions. This frame is sent to the second and subsequent beamformees; it allows the AP to update its steering matrix for sending in MU-MIMO environments.

	Frame Control	Duration	RA	TA	Feedback Segment Retransmission Bitmap	FCS
Octets:	2	2	6	6	1	4

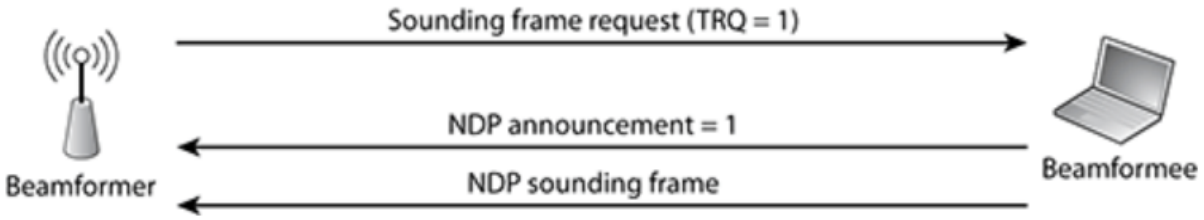
Figure 9-52—Beamforming Report Poll frame format

Beamforming Report Poll Frame Format

VHT/HE NDP Announcement

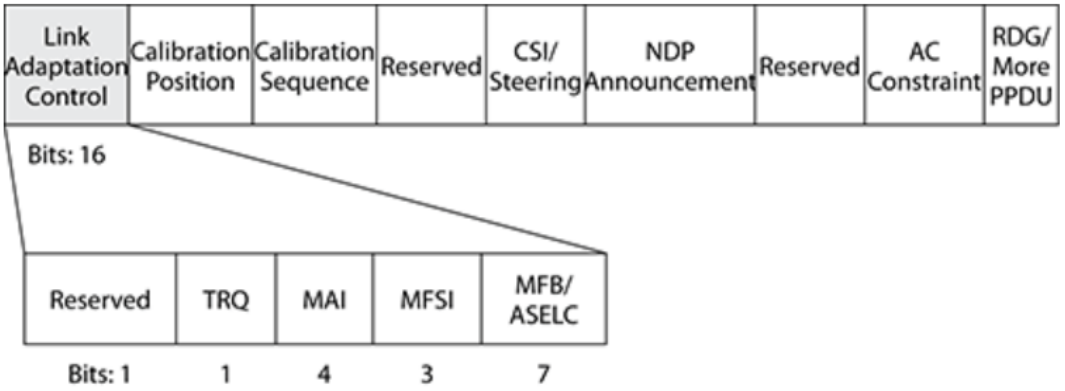
Null data packet (NDP) announcement frames notify the recipient that an NDP will follow. The figure below shows the frame exchange process. The beamformer (AP) will request that the station send an NDP sounding frame by setting the training request (TRQ) value in the Link Adaption Control subfield of the HT Control Field. The information gathered from the sounding frame can be used to calculate a steering matrix for the purpose of using beamforming for future transmissions to the same station.

Figure 10-44: NDP announcement frame exchange



NDP Announcement Frame Exchange

Figure 10-15: Link Adaptation Control subfield format



Link Adaption Control Subfield Format

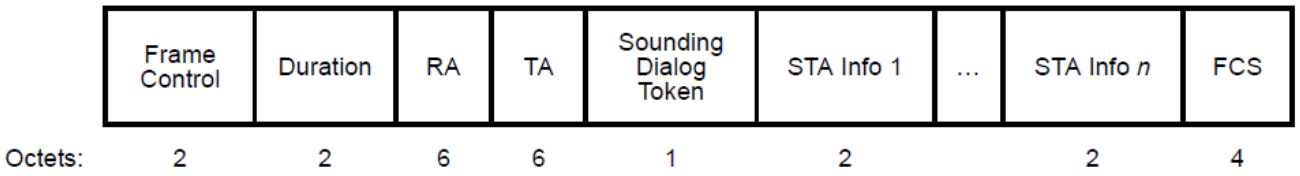


Figure 9-49—VHT NDP Announcement frame format

NDP Announcement Frame Format

```
IEEE 802.11 VHT/HE NDP Announcement, Flags: ........
   Type/Subtype: VHT/HE NDP Announcement (0x0015)
   Frame Control Field: 0x5400
      .... ..00 = Version: 0
      .... 01.. = Type: Control frame (1)
      0101 .... = Subtype: 5
   > Flags: 0x00
   .000 0001 0101 0100 = Duration: 340 microseconds
   Receiver address: IntelCor_a0:07:26 (7c:2a:31:a0:07:26)
   Transmitter address: Cisco_b7:ac:4f (7c:0e:ce:b7:ac:4f)
   Sounding Dialog Token: 0xb0
      .... ...0 = Reserved: 0x0
      .... ..0. = HE: VHT NDP Announcement frame
      1011 00.. = Sounding Dialog Token Number: 44
   STA list
      STA 0
         .... 0000 0000 0101 = AID12: 0x005
         ...0 .... .... .... = Feedback Type: SU feedback requested
         000. .... .... .... = Reserved: 0x0
```

NDP Announcement Frame

Control Wrapper

Per the IEEE 802.11-2016 standard, the control wrapper control frame is used to add the HT control field to other control frames. This is accomplished by “wrapping” (or encapsulating) the original control frame, minus duration/ID, Address 1, and the FCS, in a control wrapper frame. We can see below a “Carried Frame Control” value that indicates the subtype value of the control frame being carried. This is how 802.11n HT capability information is added to control frames.

	Frame Control	Duration/ ID	Address 1	Carried Frame Control	HT Control	Carried Frame	FCS
Octets:	2	2	6	2	4	variable	4

Figure 9-39—Control Wrapper frame

Control Wrapper Frame Format

Control Frame Extension

Added in 802.11ad – Directional Multigigabit (DMG), which defines the use of Wi-Fi in the 60GHz frequency range, control frame extension frames reuse 4 bits of the frame control field (B8-B11) for additional control frames that are used with DMG. The list of additional control frames for DMG can be found in the table below from the 802.11-2016 standard.

Table 9-2—Control Frame Extension

Type value B3 B2	Subtype value B7 B6 B5 B4	Control Frame Extension value B11 B10 B9 B8	Description
01	0110	0000	Reserved
01	0110	0001	Reserved
01	0110	0010	Poll
01	0110	0011	SPR
01	0110	0100	Grant
01	0110	0101	DMG CTS
01	0110	0110	DMG DTS
01	0110	0111	Grant Ack
01	0110	1000	SSW

Control Frame Extension Table

Data Frames

Data frames are used to transfer information **or** trigger an event. Not all data frames contain a payload, some are “null data frames” and only contain a header and trailer. The data frame types bolded in the table below are only used in HCF controlled channel access (HCCA) or point coordination function (PCF) based wireless networks. These were never implemented in the real world. This leaves only 4 to pay attention to.

Subtype Field	Description
0000	Data
0001	**Data + CF-ACK**
0010	**Data + CF-Poll**
0011	**Data + CF-ACK + CF-Poll**
0100	Null (no data)
0101	**CF-ACK (no data)**
0110	**CF-Poll (no data)**
0111	**CF-ACK + CF-Poll (no data)**
1000	QoS Data
1001	**QoS Data + CF-ACK**
1010	**QoS Data + CF-Poll**

1011	**QoS Data + CF-ACK + CF-Poll**
1100	QoS Null (no data)
1101	Reserved
1110	**QoS CF-Poll (no data)**
1111	**QoS CF-ACK + CF-Poll (no data)**

Data

Used when communicating to a non-QoS station. Broadcast/Multicast traffic is typically sent as a simple data frame unless the station knows that all stations within the BSS are QoS capable.

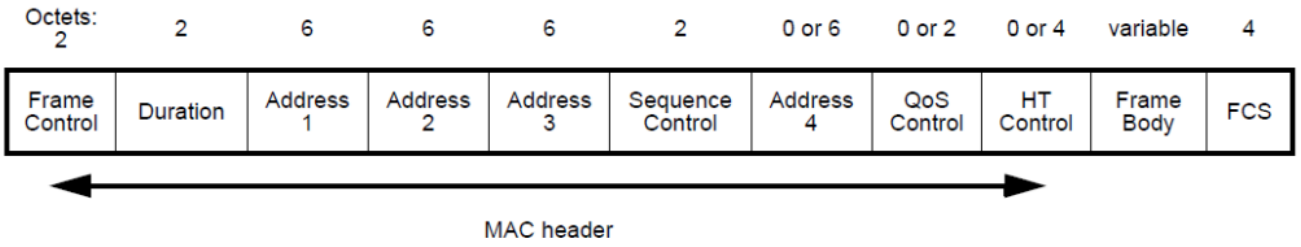


Figure 9-53—Data frame

Data Frame Format

QoS Data

Used when a QoS station transmits to another QoS station. The header in QoS data frames contains a QoS control field that will indicate the access category (AC), policy type, and payload type.

```
▼ Qos Control: 0x0000
    .... .... .... 0000 = TID: 0
    [.... .... .... .000 = Priority: Best Effort (Best Effort) (0)]
    .... .... ...0 .... = EOSP: Service period
    .... .... .00. .... = Ack Policy: Normal Ack (0x0)
    .... .... 0... .... = Payload Type: MSDU
  › 0000 0000 .... .... = QAP PS Buffer State: 0x00
```

QoS Control Field

Null Data / QoS Null Data

Used to transmit control information without carrying any data. Some stations may use null data frames to indicate that they are entering power save mode or that they are waking up.

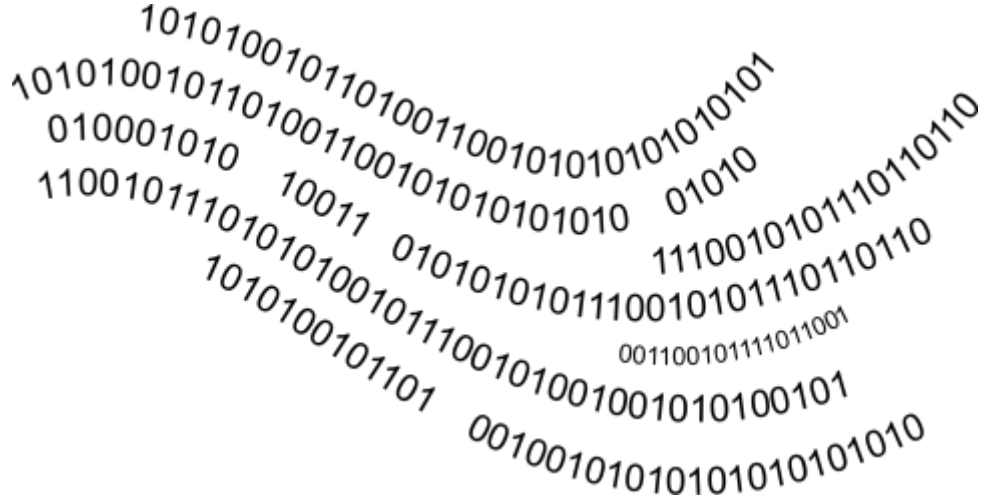
```
IEEE 802.11 QoS Null function (No data), Flags: ...P...T
   Type/Subtype: QoS Null function (No data) (0x002c)
   Frame Control Field: 0xc811
      .... ..00 = Version: 0
      .... 10.. = Type: Data frame (2)
      1100 .... = Subtype: 12
      Flags: 0x11
         .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
         .... .0.. = More Fragments: This is the last fragment
         .... 0... = Retry: Frame is not being retransmitted
         ...1 .... = PWR MGT: STA will go to sleep
         ..0. .... = More Data: No data buffered
         .0.. .... = Protected flag: Data is not protected
         0... .... = Order flag: Not strictly ordered
   .000 0000 0011 1100 = Duration: 60 microseconds
   Receiver address: Netgear_75:81:a0 (9c:3d:cf:75:81:a0)
   Transmitter address: Google_cb:36:b2 (44:07:0b:cb:36:b2)
   Destination address: Netgear_75:81:a0 (9c:3d:cf:75:81:a0)
   Source address: Google_cb:36:b2 (44:07:0b:cb:36:b2)
   BSS Id: Netgear_75:81:a0 (9c:3d:cf:75:81:a0)
   STA address: Google_cb:36:b2 (44:07:0b:cb:36:b2)
   .... .... .... 0000 = Fragment number: 0
   0011 0011 1111 .... = Sequence number: 831
   Qos Control: 0x0007
      .... .... .... 0111 = TID: 7
      [.... .... .... .111 = Priority: Network Control (Voice) (7)]
      .... .... ...0 .... = QoS bit 4: Bits 8-15 of QoS Control field are TXOP Duration Requested
      .... .... .00. .... = Ack Policy: Normal Ack (0x0)
      0000 0000 .... .... = TXOP Duration Requested: 0 (no TXOP requested)
```

QoS Null Data Frame

Example PCAP

Attached is a PCAP file that you can use to apply filters to view the frames for yourself to better understand the frame format and values. The frames that can be found include: association request/response, authentication request/response, probe request/response, 4-way handshake, RTS/CTS, QoS and simple data frames, and more! It also includes captures of the data frames for inspection of layer 3-7.

HowIWiFi PCAP



Basic information:

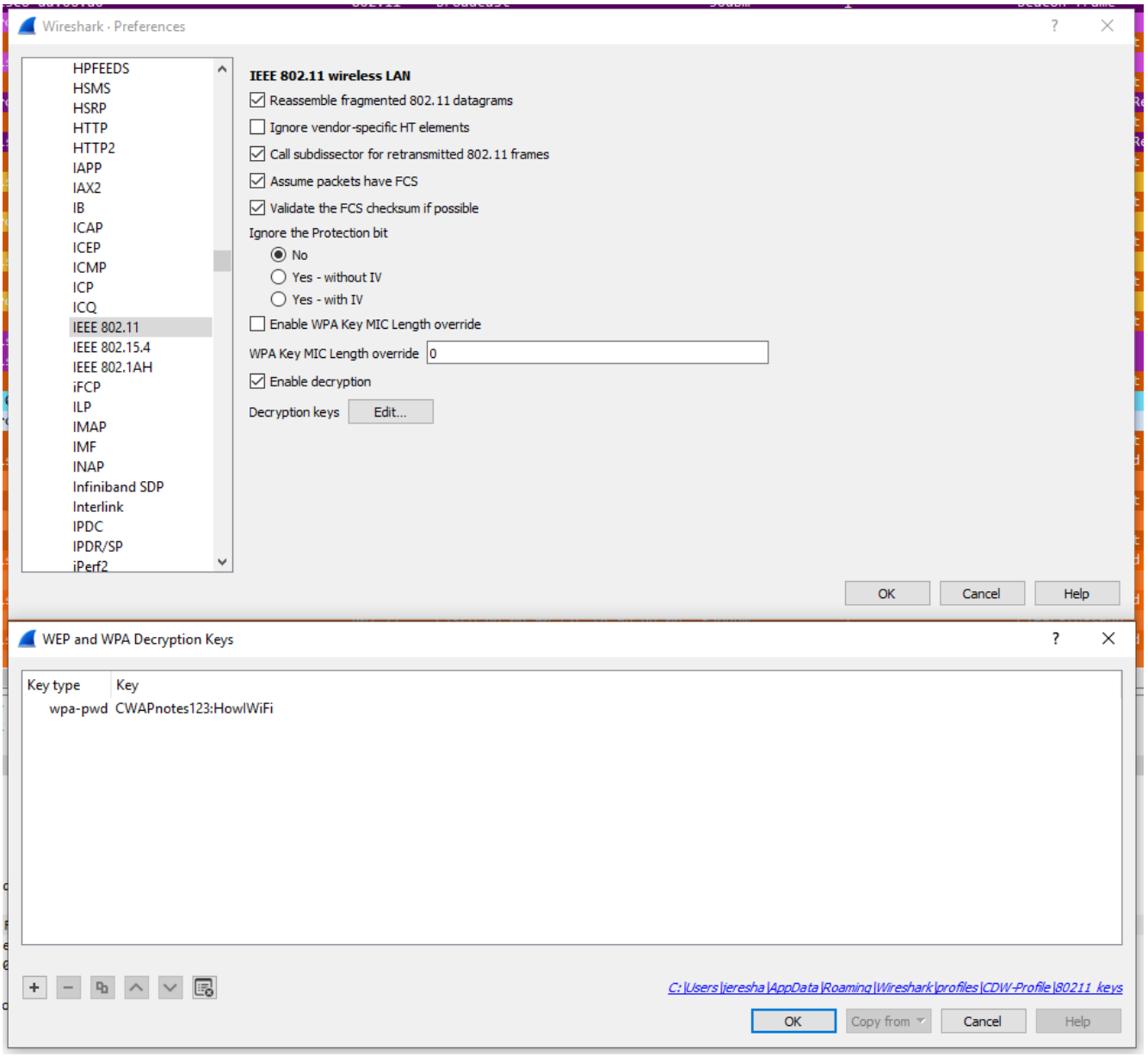
SSID: HowIWiFi

PSK: CWAPnotes123

STA: 00:20:A6:FC:B0:36

AP: 2C:F8:9B:DD:06:A0

To decrypt the data frames in this capture, open preferences, select IEEE 802.11, select “Edit…” next to Decryption keys, and enter the PSK and SSID as shown below.



Enable Decryption

Below is a list of filters you can apply and the types of frames or frame exchange that will be shown.

Filter	Frames
frame.number >= 9250 && frame.number <=9274	Disassociation, Deauthentication, Authentication, Association Request/Response, 4-way handshake (EAPOL), ACKs
frame.number == 4505 || frame.number == 4507	Station using action frame to request 802.11k neighbor report and AP responding with report.

(wlan.fc.pwrmgt == 1) && (wlan.fc.type_subtype == 0x0024)	Station using null data frame to notify the AP that it is going to sleep.
wlan.fc.type_subtype == 0x000a	Station sends disassociation frame to AP with “STA is leaving BSS” reason code. AP sends disassociation frame to STA with “Unknown” reason code.
wlan.fc.retry == 1	Shows number of times a frame had to be retransmitted. 2.4% of frames in capture.
wlan.fc.type_subtype == 0x000c	AP sends deauthentication frames to STA with reason codes “Unknown” and “Class 3 frame received from nonassociated STA” meaning that the STA transmitted frames prior to association.
wlan.fc.type_subtype == 0x0005 || wlan.fc.type_subtype == 0x0004	Shows all probe requests and probe responses.
frame.number >= 15946 && frame.number <= 15949	AP sends RTS to STA, AP sends CTS with RA as itself to indicate that it is clear to transmit frames, AP sends QoS data frame to STA, and STA sends a Block ACK to confirm receipt.

Conclusion

It is very satisfying once you understand how to perform the detective work to troubleshoot a wireless issue that requires protocol analysis. The sheer number of frames and their unique elements may seem overwhelming when studying for the CWAP exam; especially the frames that only show up every so often and aren’t obvious in their intent, such as action and null data frames. Practice makes perfect. Real-world experience with over-the-air packet captures and performing protocol analysis goes a long

way. For some of the more complex processes, such as NDP sounding, I found it best to focus on the basics. Many of these frame types have multiple levels of understanding. A The next step is to understand the frame exchanges in which these frames are used.

I hope these short explanations, visuals, and attached PCAPs help you better understand the purpose of each frame type by showing the format and a decoded frame within Wireshark. I don't believe there is such thing as "too much practice" for the CWAP exam, perform as many packet captures as you can and try to picture the stations communicating with the AP.

References

IEEE 802.11-2016 Standard

CWNA-107 Study Guide

CWAP PW0-270 Study Guide

CWAP-403 Study Guide

IEEE 802 Privacy Threat Analysis

Transmission of IPv6 Packets over IEEE 802.11p Networks

Published by jeremymsharp

View all posts by jeremymsharp

Certification Study, CWAP Study Notes, CWNA Study Notes

802.11 Control Frames, 802.11 Frames, 802.11 Management Frames, 802.11 Packet Capture, 802.11 Wireshark, ACK Frame, Association Frame, Association Request, Association Response, Authentication Frame, Authentication PCAP, Authentication Response, BAR, Beacon Frame, Block ACK Frame, BSS Configuration, Control Frames, Data Frame, Destination Address, Disassociation PCAP, EAPOL PCAP, Fragment, Frame Control Field, General Frame Format, Hidden SSID, HT Capabilities, Information Elements, Management Frames, More Data, Null Data Frame, PHY Header, Primary Channel, Probe Request Frame, Probe Response Frame, Protocol Analyzer, QoS Control Field, QoS Data Frame, QoS Null Data Frame, Receiver Address, Retransmission, Retry, RSN Information Element, Source Address, To DS From DS, Transmitter Address, VHT Capabilities, Wireless Control Frames, Wireless Management Frames, Wireless Packet Capture, Wireless QoS

6 thoughts on “802.11 Frame Types and Formats”

1. Pingback: 802.11 Frame Exchanges – How I WI-FI
2. **Anthony (Tony) Thorpe**

   says:
   July 17, 2020 at 6:00 pm
   Hello There,
   Excellent work, will be up on my office wall, monday.
   I am (still) studying for a CWNA, this will help me a lot.
   Many thanks
   Tony
   PS, now to ‘rummage’ around your site …… good use of a Saturday night, in my book.

   1. **jeremymsharp**

      says:
      July 17, 2020 at 6:16 pm
      Thanks Anthony! Glad I am able to help you achieve your certification goals!

3. **wifi**

   says:
   August 11, 2020 at 7:37 pm
   Excellent work. quick one, you mentioned that If the sender does not receive an ACK, it will retransmit the frame, what about the BlockAck, if it’s corrupted and not received by the receiver, what frame will be retransmitted?

4. **Dmitry Tretyak**

   says:
   November 17, 2020 at 2:13 am
   Thank you very very much! There is lack information about this topic in the internet. Your post is very useful.
   Could you explain how to determine where is access point and where is associated clients in *cap file. Should I use “data” frame type to filter? Or “management” frame type contains this information too?

5. **Alfonso**

   says:
   December 11, 2020 at 11:18 am
   That’s amazing this post have amazing informations about the wireless part that’s great for CCNA and also CCNP studying and of course for understand how wireless is working.
   Pretty intresting!

UP ↑