Understanding 802.11 Frame Types

- The 802.11 standard defines various frame types that stations (NICs and access points) use for communications, as well as managing and controlling the wireless link.

- A working knowledge of and familiarity with the basic 802.11 frame types is essential when analyzing or troubleshooting the operation of a wireless LAN.

- This is especially useful when examining wireless network traffic using tools such as **Wireshark**.

- There are three main frame types:

    - **Data Frames** – Used for station-to-station traffic.
    - **Control Frames** – Control functions (ACKs, channel acquisition,, etc)
    - **Management Frames** – Supervisory functions (associations, disassociations, etc).

- Each frame consists of the following basic components:

    - A **MAC header**, which comprises frame control, duration, address, and sequence control information.

    - A variable length **frame body** which contains information specific to the frame **type**.

    - A **frame check sequence** (FCS), which contains an IEEE 32-bit cyclic redundancy code (CRC).

- Every frame has a control field that depicts the 802.11 protocol version, frame type, and various indicators, such as whether WEP is on, power management is active, and so on.

- In addition all frames contain MAC addresses of the source and destination station (and access point), a frame sequence number, frame body and frame check sequence (for error detection).

- 802.11 data frames carry protocols and data from higher layers within the frame body.

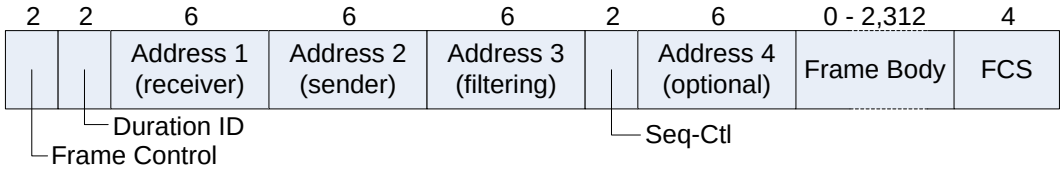
- A data frame, for example, could be carrying the HTML code from a Web page (complete with TCP/IP headers) that the user is viewing.

- Other frames that stations use for management and control carry specific information regarding the wireless link in the frame body.

- For example, a beacon's frame body contains the service set identifier (SSID), timestamp, and other pertinent information regarding the access point.

Data Frames

- The main function of a wireless LAN is to transport data between stations and Access point.
- 802.11 defines a data frame type as one that carries packets from higher layers, such as web pages, printer control data, etc., within the body of the frame.
- When 802.11 data frames are captured with a packet analyzer, the payload contents can generally be examined to see what packets that the 802.11 data frames are transporting.
- The following diagram depicts a generic data frame:



Generic Data Frame

- The fields Address 2, Address 3, Sequence Control, Address 4, and Frame Body may or may not be present depending on the particular frame type.
- The different data frame types can be categorized according function as follows:

Frame Type	Contention-Based Service	Contention-Free Service	Data Carried	No Data Carried
Data	√		√	
Data+CF-ACK		√	√	
Data+CF-POLL		AP Only	√	
Data+CF-ACK+CF-POLL		AP Only	√	
Null	√	√		√
CF-ACK		√		√
CF-POLL		AP Only		√
CF-ACK+CF-POLL		AP Only		√

Frame Control Field

- The Frame Control field consists of the following subfields: **Protocol Version**, **Type**, **Subtype**, **To DS**, **From DS**, **More Fragments**, **Retry**, **Power Management**, **More Data**, **Wired Equivalent Privacy** (WEP), and **Order**.
- **Protocol Version field**
    - The Protocol Version field is 2 bits in length and is a constant sized field.
    - For 802.11 the value of the protocol version is 0.
- **Type and Subtype fields**
    - The Type field is 2 bits in length, and the Subtype field is 4 bits in length.
    - The Type and Subtype fields together identify the function of the frame.
    - There are three frame types: control, data, and management.
- **To DS field**
    - The To DS field is 1 bit in length and is set to 1 in data type frames destined for the DS.
    - This includes all data type frames sent by STAs associated with an AP. The To DS field is set to 0 in all other frames.
- **From DS field**
    - The From DS field is 1 bit in length and is set to 1 in data type frames exiting the DS. It is set to 0 in all other frames.
- **More Fragments field**
    - 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 MAC Service Data Unit (MSDU) or current MAC Protocol Data Unit (MPDU) to follow.
    - It is set to 0 in all other frames.
- **Retry field**
    - The Retry field is 1 bit in length and is set to 1 in any data or management type frame that is a retransmission of an earlier frame.
    - It is set to 0 in all other frames. A receiving station uses this indication to aid in the process of eliminating duplicate frames.

- **Power Management field**
    - The Power Management field is 1 bit in length and is used to indicate the power management mode of a STA.
    - The value of this field remains constant in each frame from a particular STA within a frame exchange sequence.
    - The value indicates the mode in which the station will be after the successful completion of the frame exchange sequence.
    - A value of 1 indicates that the STA will be in power-save mode. A value of 0 indicates that the STA will be in active mode.
    - This field is always set to 0 in frames transmitted by an AP.

- **More Data field**
    - The More Data field is 1 bit in length and is used to indicate to a STA in power-save mode that more MSDUs, or MPDUs are buffered for that STA at the AP.
    - The More Data field is valid in directed data or management type frames transmitted by an AP to an STA in power-save mode.
    - A value of 1 indicates that at least one additional buffered MSDU, or MPDU, is present for the same STA.
    - The More Data field may be set to 1 in directed data type frames transmitted by a contention-free (CF)-Pollable STA to the point coordinator (PC) in response to a CF-Poll to indicate that the STA has at least one additional buffered MSDU available for transmission in response to a subsequent CF-Poll.
    - The More Data field is set to 0 in all other directed frames.
    - The More Data field is set to 1 in broadcast/multicast frames transmitted by the AP, when additional broadcast/multicast MSDUs, or MPDUs, remain to be transmitted by the AP during this beacon interval.
    - The More Data field is set to 0 in broadcast/multicast frames transmitted by the AP when no more broadcast/multicast MSDUs, or MMPDUs, remain to be transmitted by the AP during this beacon interval and in all broadcast/multicast frames transmitted by non-AP stations.

- **WEP field**
    - The WEP field is 1 bit in length. It is set to 1 if the Frame Body field contains information that has been processed by the WEP algorithm.
    - The WEP field is only set to 1 within frames of type Data and frames of type Management, subtype Authentication.
    - The WEP field is set to 0 in all other frames.

- **Order field**
    - The Order field is 1 bit in length and is set to 1 in any data type frame that contains an MSDU, or fragment thereof, which is being transferred using the StrictlyOrdered service class.
    - This field is set to 0 in all other frames.

Address fields

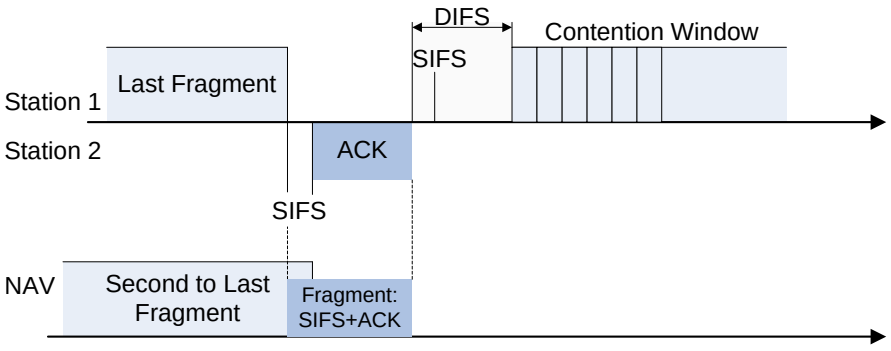
- There are four address fields in the data frame format. These fields are used to indicate the **BSSID**, **source address**, **destination address**, **transmitting station address**, and **receiving station** address.
- The usage of the four address fields in each frame type is indicated by the abbreviations **BSSID**, **DA**, **SA**, **RA**, and **TA**, indicating Basic Service Set Identifier (**BSSID**), Destination Address, Source Address, Receiver Address, and Transmitter Address, respectively.
- Certain frames may not contain some of the address fields. Certain address field usage is specified by the relative position of the address field (1–4) within the MAC header, independent of the type of address present in that field.
- For example, receiver address matching is always performed on the contents of the Address 1 field in received frames, and the receiver address of CTS and ACK frames is always obtained from the Address 2 field in the corresponding RTS frame, or from the frame being acknowledged.
- The following table summarizes the use the address fields in data frames.

Function	To DS	From DS	Address 1 (Receiver)	Address 2 (Transmitter)	Address 3	Address 4
IBSS	0	0	DA	SA	BSSID	Not Used
To AP (Infrastruture)	1	0	BSSID	SA	DA	Not Used
From AP (Infrastruture)	0	1	DA	BSSID	SA	Not Used
WDS (bridge)	1	1	RA	TA	DA	SA

- The BSSID field is a 48-bit field of the same format as an IEEE 802 MAC address.
- This field uniquely identifies each BSS. The value of this field, in an infrastructure BSS, is the MAC address currently in use by the STA in the AP of the BSS.
- The value of all 1s is used to indicate the broadcast BSSID. A broadcast BSSID may only be used in the BSSID field of management frames of subtype probe request.

Duration Field

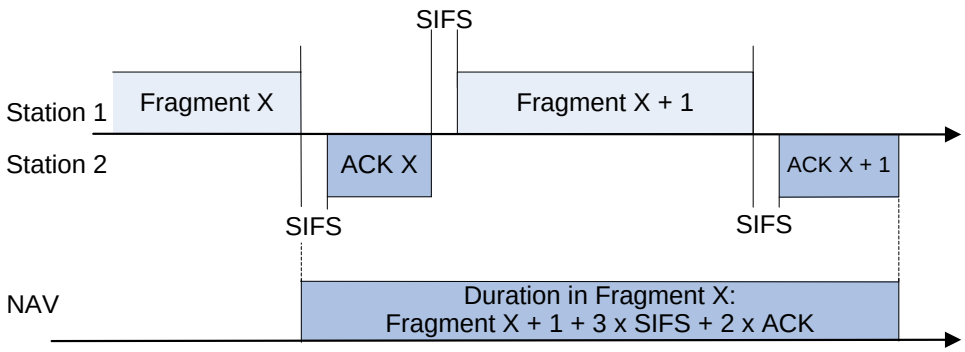
- The Duration/ID field is 16 bits in length. The contents of this field are set as follows:
    - In control type frames of subtype Power Save (PS)-Poll, the Duration/ID field carries the association identity (AID) of the station that transmitted the frame in the 14 least significant bits (LSB), with the 2 most significant bits (MSB) both set to 1.
    - The value of the AID is in the range 1–2007.
    - In all other frames, the Duration/ID field contains a duration value as defined for each frame type.
    - For frames transmitted during the contention-free period (CFP), the duration field is set to 32 768.
    - Whenever the contents of the Duration/ID field are less than 32 768, the duration value is used to update the network allocation vector (NAV).
- If the More Fragments bit in the Frame Control Field is 0, no more fragments remain in the frame.
- The Duration field is set to the amount of time required for one Short Interframe Space (SIFS) and the fragment ACK.
- The following diagram illustrates this process:



Duration Setting on Final Fragment

- If the More Fragments bit in the Frame Control Field is 1, more fragments remain in the frame.
- The Duration field is set to the amount of time required to transmit 2 ACKs, plus three SIFS, plus the time required to send the next fragment.
- Essentially, nonfinal fragments will set the NAV just as an RTS would. Hence the term, virtual RTS.

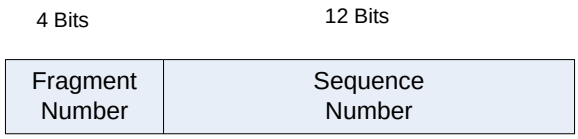
- The following diagram illustrates this process:



Duration Settings on Nonfinal Fragment

Sequence Control Field

- The Sequence Control field is 16 bits in length and consists of two subfields, the **Sequence Number** and the **Fragment Number**.
- The format of the Sequence Control field is illustrated below:



Sequence Control Field

- **Sequence Number field**
  - The Sequence Number field is a 12-bit field indicating the sequence number of an MSDU or MPDU.
  - Each MSDU or MPDU transmitted by a STA is assigned a sequence number. Sequence numbers are assigned from a single modulo 4096 counter, starting at 0 and incrementing by 1 for each MSDU or MPDU.
  - Each fragment of an MSDU or MPDU contains the assigned sequence number. The sequence number remains constant in all retransmissions of an MSDU, MPDU, or fragment.
- **Fragment Number field**
  - The Fragment Number field is a 4-bit field indicating the number of each fragment of an MSDU or MPDU.
  - The fragment number is set to zero in the first or only fragment of an MSDU or MPDU and is incremented by one for each successive fragment of that MSDU or MPDU.
  - The fragment number remains constant in all retransmissions of the fragment.

Frame Body field

- The Frame Body is a **variable length field** that contains information specific to individual frame types and subtypes.
- The minimum frame body is 0 octets. The maximum length frame body is defined by the maximum length (MSDU + ICV + IV), where ICV and IV are the WEP fields.

Frame Check Sequence (FCS) field

- The FCS field is a 32-bit field containing a **32-bit CRC**.
- The FCS is calculated over all the fields of the MAC header and the Frame Body field. These are referred to as the **calculation fields.**
- The FCS is calculated using the following standard generator polynomial of degree 32:

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

- The FCS is the 1's complement of the sum (modulo 2) of the following:
  - The remainder of $x^k \times (x^{31} + x^{30} + x^{29} \ldots\ldots\ldots x^2 + x + 1)$ divided (modulo 2) by G(x), where k is the number of bits in the calculation fields, and
  - The remainder after multiplication of the contents (treated as a polynomial) of the calculation fields by x^{32} and then division by $G(x)$.
- The FCS field is transmitted commencing with the coefficient of the highest-order term.
- As a typical implementation, at the transmitter, the initial remainder of the division is preset to all 1's and is then modified by division of the calculation fields by the generator polynomial $G(x)$.
- The 1's complement of this remainder is transmitted, with the highest-order bit first, as the FCS field.
- At the receiver, the initial remainder is preset to all 1's and the serial incoming bits of the calculation fields and FCS, when divided by $G(x)$, results in the absence of transmission errors, in a unique nonzero remainder value.
- This unique remainder value is the polynomial:

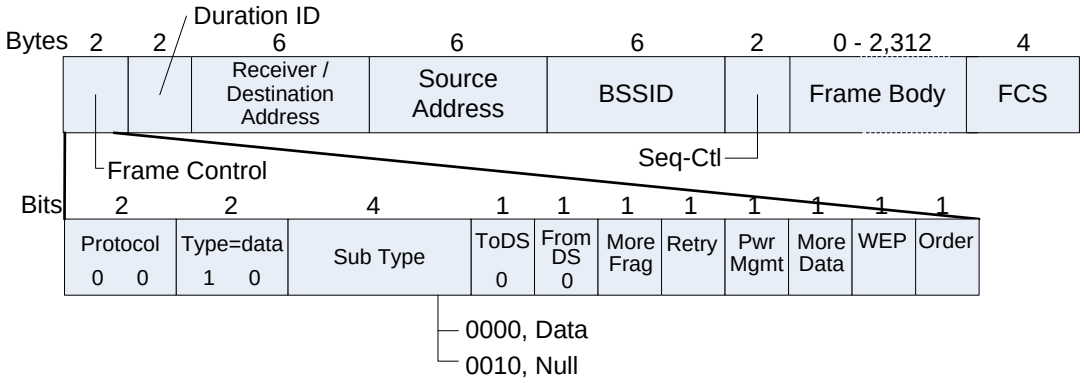
$$x^{31} + x^{30} + x^{26} + x^{25} + x^{24} + x^{18} + x^{15} + x^{14} + x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^5 + x^4 + x^3 + x + 1$$

Applied Data Framing

- This form of data frames depends on the network. The exact subtype of the frame is determined by the subtype field setting.

IBSS Frames

- An IBSS frame has three addressing fields as shown below:

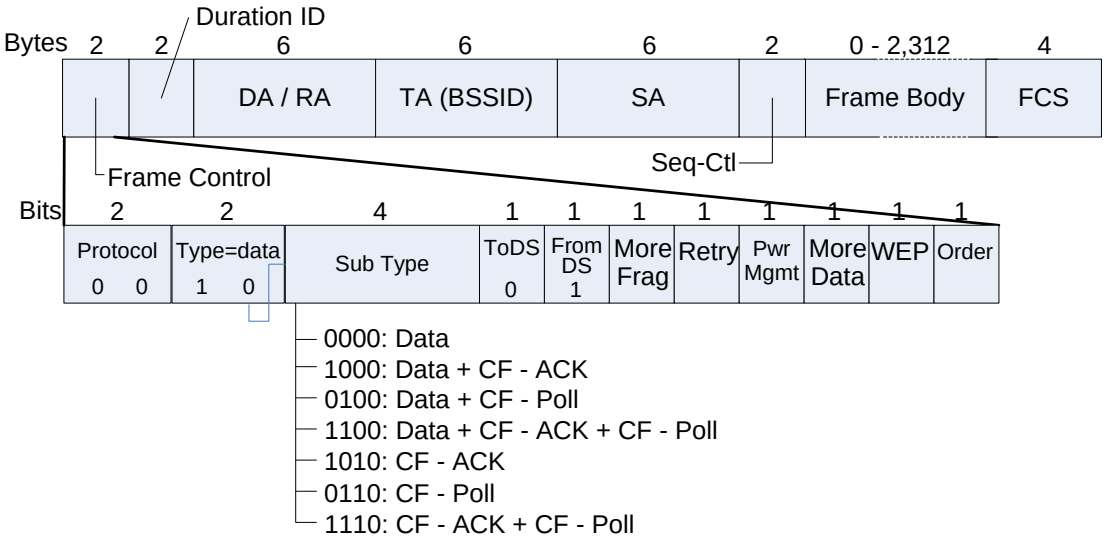


IBSS Data Frame

- The first address field identifies the receiver, which also the destination address in an IBSS.
- The second address is the source address .
- The third address is the BSSID, which is used to label all data frames in an IBSS.
- This field is used ensure that all frames that match the station's current BSSID are passed on to the higher layers.

Frames from the AP

- The following diagram shows the format of a frame that is sent from an AP to a STA:

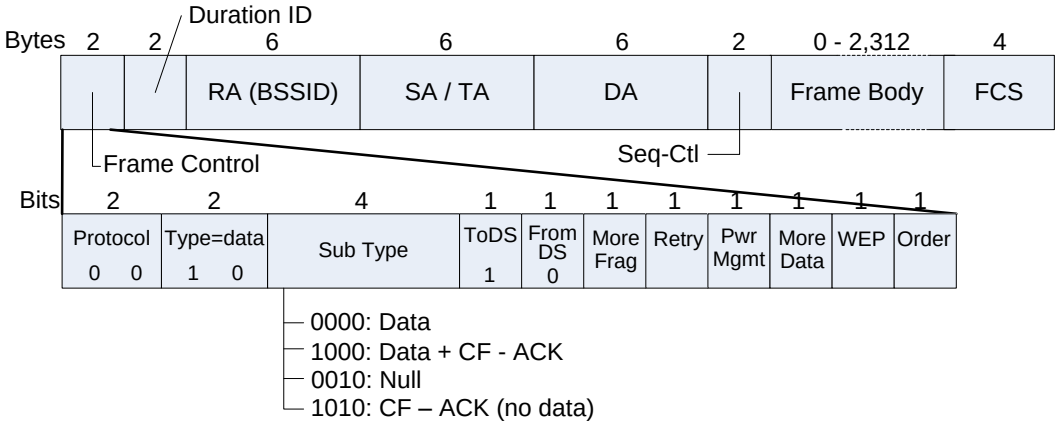


Data Frames from the AP

- The first address field (DA/RA) identifies the receiver of the frame on the wireless network, i.e., the destination.
- The second address field (SA) identifies the transmitter.
- On infrastructure networks this is the address of the station in the AP, which is also the BSSID.
- The thirst address field (SA) is the source MAC address of the frame.

Frames to the AP

- The following diagram shows the format of a frame that is sent from a STA in an infrastructure network to an AP:

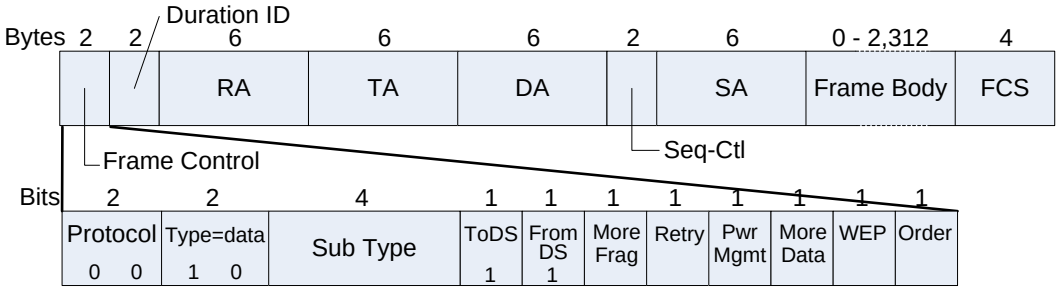


Data Frames from to the AP

- The receiver address (RA) is the BSSID, which is taken from the MAC address of the STA in the AP.
- The rest of the address fields are as described earlier.
- Frames from the Distribution System have the ToDS bit set, but the FromDS is set to 0.

WDS Frames

- When an AP is deployed in a wireless bridge, or WDS topology, all four address fields as shown below are used:



WDS Frames

- Just as before, the first and the second address fields identify the receiver and transmitter of the frame respectively.
- The MAC uses these two addresses for ACKs and control traffic such as RTS, CTS, and ACK frames.
- Two more addresses (DA and SA) are necessary to identify the source and destination of the frame and distinguish them from the wireless link addresses.

Control Frames

- 802.11 control frames assist in the delivery of data frames between stations.
- They manage access to the wireless channel and provide MAC-layer reliability functions.
- The following diagrams illustrates the format of control frames and the default bit settings for each of the fields:

Bits	2		2		4				1	1	1	1	1	1	1	1
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	Protocol		Type= Control		Sub Type				ToDS	From DS	More Frag	Retry	Pwr Mgmt	More Data	WEP	Order
	0	0	0	1					0	0	0	0	0	0	0	0

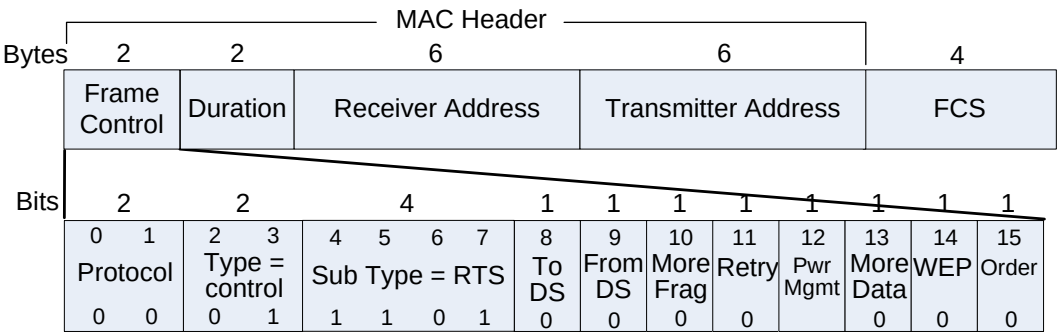
Frame Control Field in Control Frames

- All control frames are assigned a 01 Type identifier. The following are common 802.11 control frame subtypes:

Request to Send (RTS) Frame

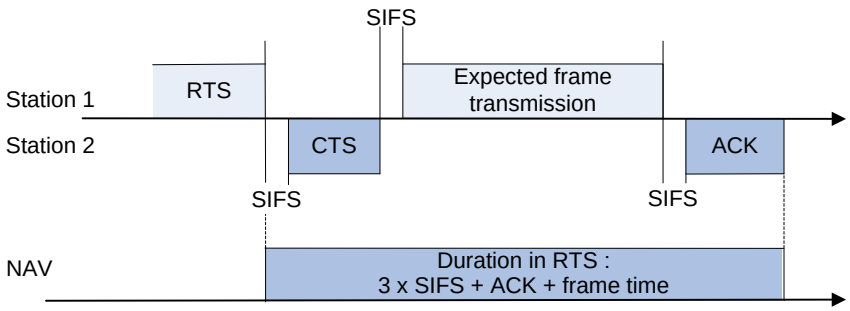
- The RTS/CTS function is optional and reduces frame collisions present when hidden stations have associations with the same access point.
- A station sends a RTS frame to another station as the first phase of a two-way handshake necessary before sending a data frame.

- The following diagram shows the format of a RTS frame:



RTS Frame

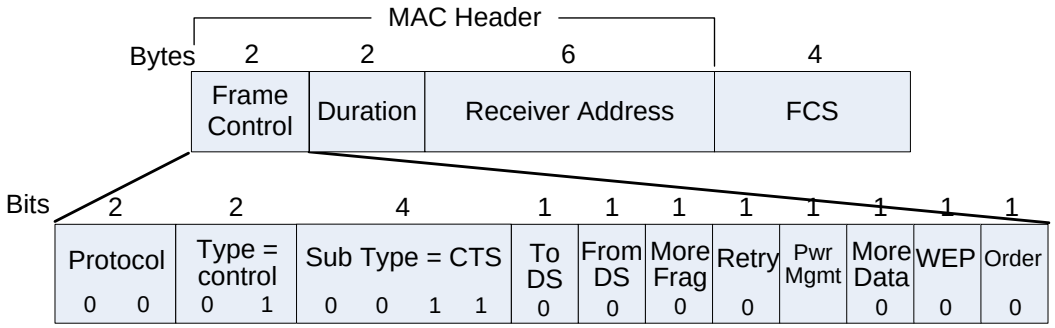
- The RA of the RTS frame is the address of the STA, on the wireless network, that is the intended immediate recipient of the directed data or management frame.
- The TA is the address of the STA transmitting the RTS frame.
- The duration value is the time, in microseconds, required to transmit the pending data or management frame, plus one CTS frame, plus one ACK frame, plus three SIFS intervals.
- This sets the NAV value as illustrated in the next diagram.



Duration Field in RTS Frame

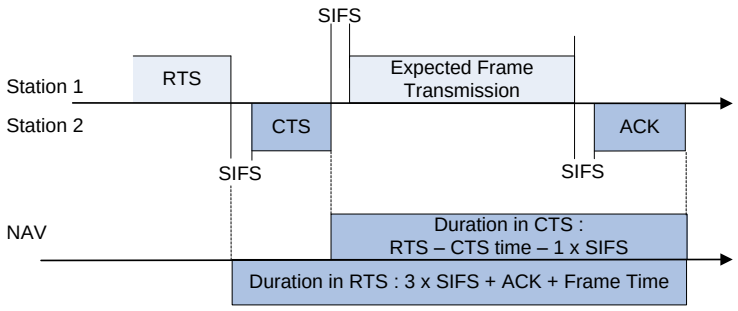
Clear to Send (CTS) Frame

- A station responds to a RTS with a CTS frame, providing clearance for the requesting station to send a data frame.
- The CTS includes a time value that causes all other stations (including hidden stations) to hold off transmission of frames for a time period necessary for the requesting station to send its frame.
- This minimizes collisions among hidden stations, which can result in higher throughput if you implement it properly.
- The following diagram shows the format of a CTS frame:



CTS Frame

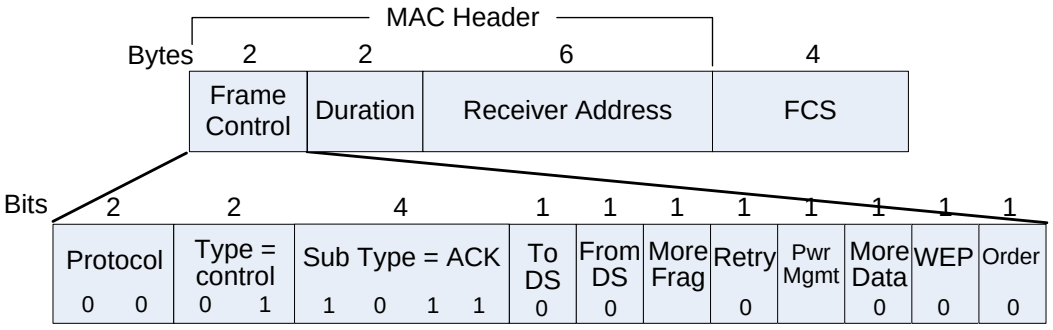
- The RA of the CTS frame is copied from the TA field of the immediately previous RTS frame to which the CTS is a response to.
- The duration value is the value obtained from the Duration field of the immediately previous RTS frame, minus the time, in microseconds, required to transmit the CTS frame and its SIFS interval.
- The term “immediately previous” frame means a frame whose reception concluded within the prior Short Inter-Frame Space (SIFS) interval.
- This sets the NAV value as illustrated in the next diagram.



CST Duration

Acknowledgement (ACK) Frame

- After receiving a data frame, the receiving station will utilize an error checking process to detect the presence of errors.
- The receiving station will send an ACK frame to the sending station if no errors are found.
- If the sending station doesn't receive an ACK after a period of time, the sending station will retransmit the frame.
- The following diagram shows the format of an ACK frame:

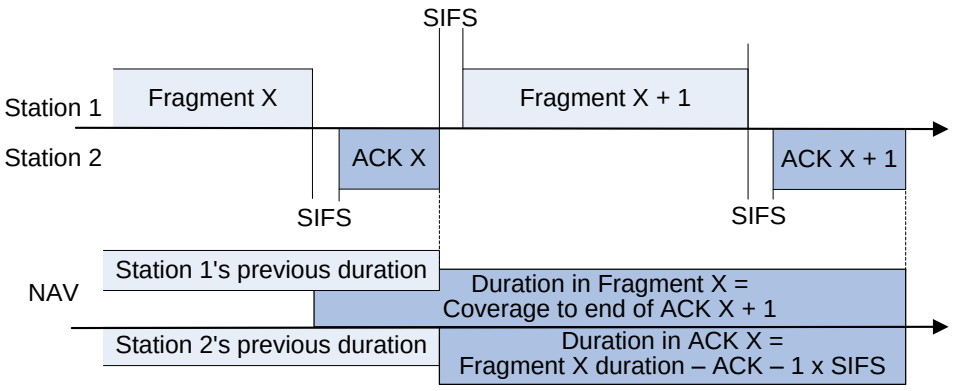


ACK Frame

- The RA of the ACK frame is copied from the Address 2 field of the immediately previous directed data, management, or PS-Poll control frame.
- If the More Fragment bit was set to 0 in the Frame Control field of the immediately previous directed data or management frame, the duration value is set to 0.

- If the More Fragment bit was set to 1 in the Frame Control field of the immediately previous directed data or management frame, the duration value is the value obtained from the Duration field of the immediately previous data or management frame, minus the time, in microseconds, required to transmit the ACK frame and its SIFS interval.

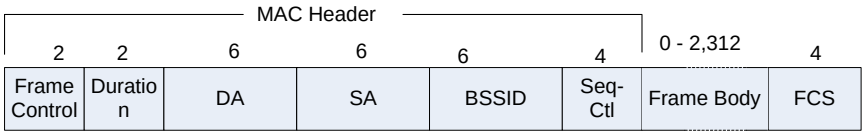
- This sets the NAV value as illustrated in the next diagram.



Duration in non-final ACK Frames

Management Frames

- 802.11 management frames enable stations to establish and maintain communications.



Generic Management Frame

- The address fields for management frames do not vary by frame subtype.
- The BSSID of the management frame is determined as follows:
    - If the station is an AP or is associated with an AP, the BSSID is the address currently in use by the STA contained in the AP.
    - If the station is a member of an IBSS, the BSSID is the BSSID of the IBSS.
    - In Management frames of subtype Probe Request, the BSSID is either a specific BSSID, or the broadcast BSSID.
- The DA is the destination of the frame.
- The SA is the address of the station transmitting the frame.
- Within all management type frames sent during the contention free period (CFP), the Duration field is set to the value 32 768.
- Within all management type frames sent during the contention period, the Duration field is set according to the following rules:
    - If the DA field contains a group address, the duration value is set to 0.
    - If the More Fragments bit is set to 0 in the Frame Control field of a frame and the DA contains an individual address, the duration value is set to the time, in microseconds, required to transmit one ACK frame, plus one SIFS interval.
    - If the More Fragments bit is set to 1 in the Frame Control field of a frame, and the DA contains an individual address, the duration value is the time, in microseconds, required to transmit the next fragment of this management frame, plus two ACK frames, plus three SIFS intervals.
- These frames form a very large component of the 802.11 specification. The following are the most common 802.11 management frame subtypes:

Authentication frame

- 802.11 authentication is a process whereby the access point either accepts or rejects the identity of a wireless NIC.
- The NIC begins the process by sending an authentication frame containing its identity to the access point.
- With open system authentication (the default), the NIC sends only one authentication frame, and the access point responds with an authentication frame as a response indicating acceptance (or rejection).
- With the optional shared key authentication, the radio NIC sends an initial authentication frame, and the access point responds with an authentication frame containing challenge text.
- The NIC must send an encrypted version of the challenge text (using its WEP key) in an authentication frame back to the access point.
- The access point ensures that the radio NIC has the correct WEP key (which is the basis for authentication) by seeing whether the challenge text recovered after decryption is the same that was sent previously.
- Based on the results of this comparison, the access point replies to the radio NIC with an authentication frame signifying the result of authentication.

Deauthentication frame

- A station sends a deauthentication frame to another station if it wishes to terminate secure communications.

Association request frame

- 802.11 association enables the access point to allocate resources for and synchronize with a wireless NIC.
- A NIC begins the association process by sending an association request to an access point.
- This frame carries information about the NIC (e.g., supported data rates) and the SSID of the network it wishes to associate with.
- After receiving the association request, the access point considers associating with the NIC, and (if accepted) reserves memory space and establishes an association ID for the NIC.

Association response frame

- An access point sends an association response frame containing an acceptance or rejection notice to the wireless NIC requesting association.
- If the access point accepts the NIC, the frame includes information regarding the association, such as association ID and supported data rates.
- If the outcome of the association is positive, the NIC can utilize the access point to communicate with other NICs on the network and systems on the distribution (i.e., Ethernet) side of the access point.

Reassociation request frame

- If a wireless NIC roams away from the currently associated access point and finds another access point having a stronger beacon signal, the radio NIC will send a reassociation frame to the new access point.
- The new access point then coordinates the forwarding of data frames that may still be in the buffer of the previous access point waiting for transmission to the radio NIC.

Reassociation response frame

- An access point sends a reassociation response frame containing an acceptance or rejection notice to the wireless NIC requesting reassociation.
- Similar to the association process, the frame includes information regarding the association, such as association ID and supported data rates.

Disassociation frame

- A station sends a disassociation frame to another station if it wishes to terminate the association.
- For example, a radio NIC that is shut down gracefully can send a disassociation frame to alert the access point that the NIC is powering off.
- The access point can then relinquish memory allocations and remove the radio NIC from the association table.

Beacon frame

- The access point periodically sends a beacon frame to announce its presence and relay information, such as timestamp, SSID, and other parameters regarding the access point to wireless NICs that are within range.
- NICs continually scan all 802.11 wireless channels and listen to beacons as the basis for choosing which access point is best to associate with.

Probe request frame

- A station sends a probe request frame when it needs to obtain information from another station.
- For example, a NIC would send a probe request to determine which access points are within range.

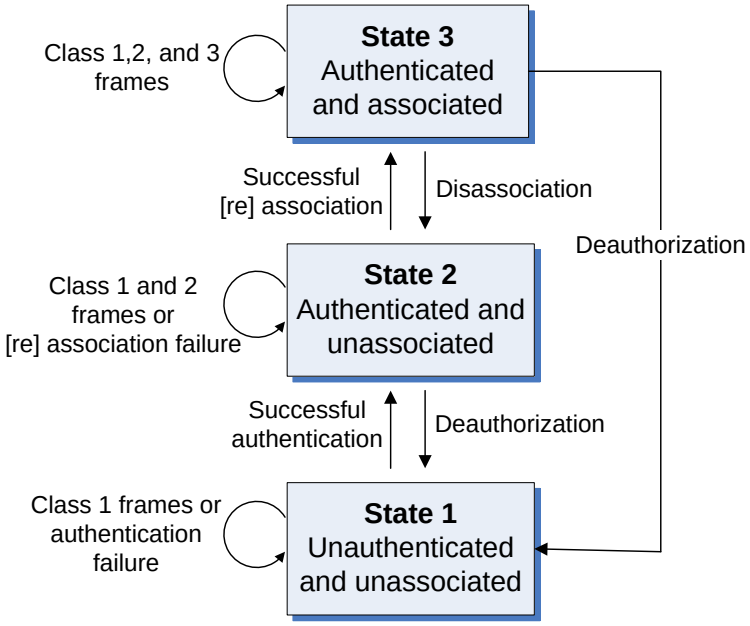
Probe response frame

- A station will respond with a probe response frame, containing capability information, supported data rates, etc., when after it receives a probe request frame.

Frame Transmission and Association and Authentication States

- The allowed frame types vary with the association and authentication states. A STA keeps two state variables for each STA with which direct communication via the wireless network is required:
- **Authentication state:**
    - The values are unauthenticated and authenticated.
- **Association state:**
    - The values are unassociated and associated.
- These two variables create three local states for each remote STA:
- **State 1**:
    - Initial start state, unauthenticated, unassociated.
- **State 2:**
    - Authenticated, not associated.
- **State 3:**
    - Authenticated and associated.

- The relationships between these station state variables and the services are given in diagram shown.



Overall 802.11 State Diagram

- The current state existing between the source and destination station determines the IEEE 802.11 frame types that may be exchanged between that pair of STAs.
- The state of the sending STA is illustrated above with respect to the intended receiving STA.
- The allowed frame types are grouped into classes and the classes correspond to the station state.
- In State 1, only Class 1 frames are allowed.
- In State 2, either Class 1 or Class 2 frames are allowed.
- In State 3, all frames are allowed (Classes 1, 2, and 3).

- The frame classes are defined as follows:

Class 1 frames (permitted from within States 1, 2, and 3)

- **Control frames**
    - Request to send (RTS)
    - Clear to send (CTS)
    - Acknowledgment (ACK)
    - Contention-Free (CF)-End+ACK
    - CF-End

- **Management frames**
    - Probe request/response
    - Beacon
    - Authentication: Successful authentication enables a station to exchange Class 2 frames.Unsuccessful authentication leaves the STA in State 1.
    - Deauthentication: Deauthentication notification when in State 2 or State 3 changes the STA's state to State 1. The STA shall become authenticated again prior to sending Class 2 frames.
    - Announcement traffic indication message (ATIM)

- **Data frames**
    - Data: Data frames with frame control (FC) bits "To DS" and "From DS" both false.

Class 2 frames (if and only if authenticated; allowed from within States 2 and 3 only)

- **Management frames:**
    - Association request/response
    - Successful association enables Class 3 frames.
    - Reassociation request/response
    - Disassociation o utilize the DS.

Class 3 frames (if and only if associated; allowed only from within State 3)

- **Data frames**
    - Data subtypes: Data frames allowed. That is, either the "To DS" or "From DS" FC bits may be set to true to utilize DSSs.

- **Management frames**
    - Deauthentication: Deauthentication notification when in State 3 implies disassociation as well, changing the STA's state from 3 to 1.
    - The station shall become authenticated again prior to another association.

- **Control frames**
    - PS-Poll