Wireless LAN Networks : 802.11 Frame

Vinh Ho (8 mins)

Let's discuss a little about the 802.11 frame. Wireless 802.11 frame, as you can see, consists of a header, payload, and FCS. The 802.11 frame format is similar to the Ethernet frame format, with the exception that it contains more fields. The 802.11 Wireless frames contain the following fields:

- Frame Control, which identifies the type of wireless frame and contains subfields for protocol version, frame type, address type, power management, and security settings.
- Duration - this field typically use to indicate the remaining duration needed to receive the next frame transmission.
- Address1 - usually contains the MAC address of the receiving wireless device or AP.
- Address2 - usually contains the MAC address of the transmitting wireless device or AP.
- Address3 - sometimes contains the MAC address of the destination, such as the router interface, the default gateway to which the AP is attached.
- Sequence Control - contains the Sequence Number and the Fragment Number subfields.
- The Sequence Number indicates the sequence number of each frame.
- The Fragment Number indicates the number of each frame sent of a fragmented frame.
- Address4 - usually missing because it is used only in adhoc mode.
- After that is the payload. Payload always contains the data for transmission.
- And the final one is Frame Check Sequence. FCS is used for error control.

You can see that the figure shows the different fields in the frame header. Remember the content of the Address field vary depending on settings in the Frame Control field.

Talking about Wireless frame type, remember, the frame types and frame subtype fields are used to identify the type of wireless transmission. As shown in the figure there, a Wireless frame can be one of the three frame types :

- Management Frame, which is used in the maintenance of communication, such as finding, authenticating, and associating with an AP.
- Control Frame, used to facilitate in the exchange of data frames between wireless clients.
- Data Frame, used to carry the payload information such as web pages and files.

Let's go into more details with the Management Frame. Management frames, as you can see, there are many subfield types. Management frames are used exclusively to find, authenticate, and associate with an AP.

The figure displays the field value of common Management frames including:

- Association Request frame with a hexadecimal of 00 (0x00) there. Association Request frame - sent from a wireless client to enable the AP to allocate resources and synchronize. The frame carries information about the wireless connection including supported data rates and SSID of the network to the wireless client that wants to associate. If the request is accepted, the AP reserves memory and establishes the association ID for the device.
- The next subtype is the Association Response type, sent from an AP to a wireless client containing the acceptance or rejection to an association request. If it is an acceptance, the frame contains information, such as an Association ID and supported data rates.
- Reassociation Request frame subtype - When a device sends a Reassociation Request when it drops from range of the currently associated AP and finds another AP with a stronger signal. The new AP coordinates the forwarding of any information that may still be contained in the buffer of the previous AP.
- Another subtype which is Reassociation Response frame. Sent from an AP containing the acceptance or rejection to a device Reassociation Request frame. The frame includes information required for association, such as the Association ID and supported data rates.
- Probe Request Frame - Sent from a wireless client when it requires information from another wireless client.
- Probe Response Frame - Sent from an AP containing capability information, such as the supported data rates, after receiving a Probe Request Frame.
- Beacon Frame - sent periodically from an AP to announce its presence and provide the SSID and other preconfigured parameters.
- Disassociation Frame - sent from the device wanting to terminate a connection, allows the AP to relinquish memory allocation and remove the device from the association table.
- The Authentication Frame - the sending device sends an Authentication Frame to the AP containing its identity.
- The last subtype, the Deauthentication Frame - sent from the wireless client wanting to terminate connection from another wireless client. Beacons are the only management frame that may regularly be broadcast by an AP. All other probing, authentication, and association frames are used only during the association (or reassociation) process.

The next frame type is the Control Frames. As you can see on the screen, there are three subtypes for these Control Frames, which are Request-to-Send, Clear-to-Send and Acknowledgement.

Control Frames are used to manage the information exchange between a wireless client and an AP. They help prevent collisions from occurring on the wireless medium. The figure displays the three subtypes.

- The first is Request-to-Send (RTS) frame. The RTS and CTS frames provide an optional collision reduction scheme for APs with hidden wireless clients. A wireless client sends a RTS frame as the first step in an two-way handshake, which is required before sending data frames.

- Clear-to-Send (CTS) frame subtype, is a wireless AP response to an RTS frame with a CTS frame. It provides clearance for the requesting wireless client to send a data frame. The CTS contributes to collision control management by including a time value. This time delay minimizes the chance that other wireless clients will transmit while the requesting client transmits.
- Finally, the Acknowledgment (ACK) subtype frame. After receiving a data frame, the receiving wireless client sends an ACK frame to the sending client if no errors are found. If the sending client does not receive an ACK frame within a predefined period of time, the sending client resends the frame, who is integral to Wireless transmission and play a significant role in the media contention method used by Wireless, known as Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).