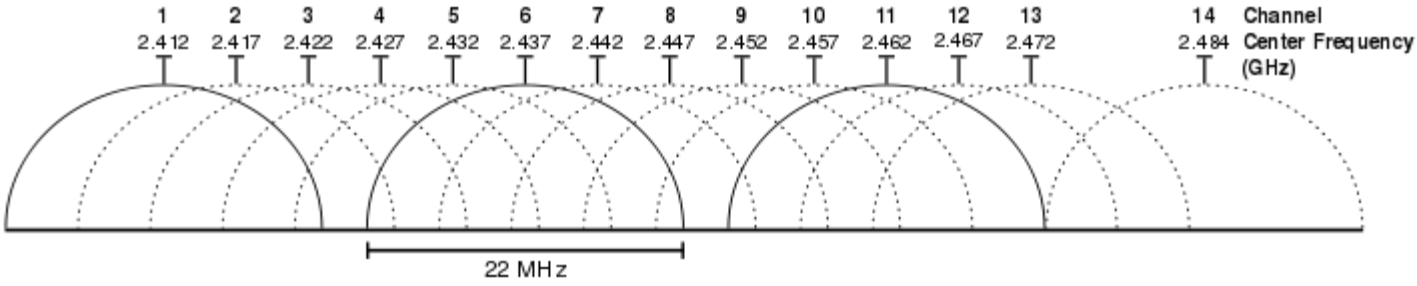
CHANNELS, INTERNATIONAL COMPATIBILITY AND FRAMES



Graphical representation of Wi-Fi channels in 2.4 GHz band

802.11 divide each of the above-described bands into channels, analogously to how radio and TV broadcast bands are sub-divided. For example the 2.4000–2.4835 GHz band is divided into 13 channels spaced 5 MHz apart, with channel 1 centered on 2.412 GHz and 13 on 2.472 GHz (to which Japan added a 14th channel 12 MHz above channel 13 which was only allowed for 802.11b). 802.11b was based on DSSS waveforms which used 22 MHz and did not have sharp borders. Consequently only three channels did not overlap. Even now many devices are shipped with channels 1, 6 and 11 as preset options even though with the newer 802.11g standard there are four non-overlapping channels: 1, 5, 9 and 13. There are now four because 802.11g signals use 20 MHz signals with OFDM waveforms.

Availability of channels is regulated by country, constrained in part by how each country allocates radio spectrum to various services. At one extreme, Japan permits the use of all 14 channels for 802.11b, while other countries such as Spain initially allowed only channels 10 and 11, and France only allowed 10, 11, 12 and 13. They now allow channels 1 through 13. North America and some Central and South American countries allow only 1 through 11.

Besides specifying the centre frequency of each channel, 802.11 also specify a spectral mask defining the permitted distribution of power across each channel. The mask requires that the signal be attenuated by at least 30 dB from its peak energy at ±11 MHz from the centre frequency, the sense in which channels are effectively 22 MHz wide. One consequence is that stations can only use every fourth or fifth channel without overlap, typically 1, 6 and 11 in the Americas, and in theory, 1, 5, 9 and 13 in Europe although 1, 6, and 11 is typical there too. Another is that channels 1–13 effectively require the band 2.401–2.483 GHz, the actual allocations being, for example, 2.400–2.4835 GHz in the UK, 2.402–2.4735 GHz in the US, etc.

Since the spectral mask only defines power output restrictions up to ±11 MHz from the center frequency to be attenuated by −50 dBr, it is often assumed that the energy of the channel extends no further than these limits. It is more correct to say that, given the separation between channels 1, 6, and 11, the signal on any channel should be sufficiently attenuated to minimally interfere with a transmitter on any other channel. Due to the near-far problem a transmitter can impact a receiver on a "non-overlapping" channel, but only if it is close to the victim receiver (within a meter) or operating above allowed power levels.

A regdomain in IEEE 802.11 is a regulatory region. Different countries define different levels of allowable transmitter power, time that a channel can be occupied, and different available channels.[19] Domain codes are specified for the United States, Canada, ETSI (Europe), Spain, France, Japan, and China.

Most wifi devices default to regdomain 0, which means least common denominator settings, i.e. the device will not transmit at a power above the allowable power in any nation, nor will it use frequencies that are not permitted in any nation.

The regdomain setting is often made difficult or impossible to change so that the end users do not conflict with local regulatory agencies such as the Federal Communications Commission.

Frames

Current 802.11 standards define "frame" types for use in transmission of data as well as management and control of wireless links. Frames are divided into very specific and standardized sections. Each frame consists of a MAC header, payload and frame check sequence (FCS). Some frames may not have the payload. The first two bytes of the MAC header form a frame control field specifying the form and function of the frame. The frame control field is further subdivided into the following sub-fields:

- **Protocol Version:** two bits representing the protocol version. Currently used protocol version is zero. Other values are reserved for future use.

- **Type:** two bits identifying the type of WLAN frame. Control, Data and Management are various frame types defined in IEEE 802.11.

- **Sub Type:** Four bits providing addition discrimination between frames. Type and Sub type together to identify the exact frame.

- **ToDS and FromDS:** Each is one bit in size. They indicate whether a data frame is headed for a distribution system. Control and management frames set these values to zero. All the data frames will have one of these bits set. However communication within an IBSS network always set these bits to zero.

- **More Fragments:** The More Fragments bit is set when a packet is divided into multiple frames for transmission. Every frame except the last frame of a packet will have this bit set.

- **Retry:** Sometimes frames require retransmission, and for this there is a Retry bit which is set to one when a frame is resent. This aids in the elimination of duplicate frames.

- **Power Management:** This bit indicates the power management state of the sender after the completion of a frame exchange. Access points are required to manage the connection and will never set the power saver bit.

- **More Data:** The More Data bit is used to buffer frames received in a distributed system. The access point uses this bit to facilitate stations in power saver mode. It indicates that at least one frame is available and addresses all stations connected.

- **WEP:** The WEP bit is modified after processing a frame. It is toggled to one after a frame has been decrypted or if no encryption is set it will have already been one.

- **Order:** This bit is only set when the "strict ordering" delivery method is employed. Frames and fragments are not always sent in order as it causes a transmission performance penalty.

The next two bytes are reserved for the Duration ID field. This field can take one of three forms: Duration, Contention-Free Period (CFP), and Association ID (AID).

An 802.11 frame can have up to four address fields. Each field can carry a MAC address. Address 1 is the receiver, Address 2 is the transmitter, Address 3 is used for filtering purposes by the receiver.

- The Sequence Control field is a two-byte section used for identifying message order as well as eliminating duplicate frames. The first 4 bits are used for the fragmentation number and the last 12 bits are the sequence number.
- An optional two-byte Quality of Service control field which was added with 802.11e.
- The Frame Body field is variable in size, from 0 to 2304 bytes plus any overhead from security encapsulation and contains information from higher layers.
- The Frame Check Sequence (FCS) is the last four bytes in the standard 802.11 frame. Often referred to as the Cyclic Redundancy Check (CRC), it allows for integrity check of retrieved frames. As frames are about to be sent the FCS is calculated and appended. When a station receives a frame it can calculate the FCS of the frame and compare it to the one received. If they match, it is assumed that the frame was not distorted during transmission.

Management Frames allow for the maintenance of communication. Some common 802.11 subtypes include:

- Authentication frame: 802.11 authentications begin with the WNIC sending an authentication frame to the access point containing its identity. With an open system authentication the WNIC only sends a single authentication frame and the access point responds with an authentication frame of its own indicating acceptance or rejection. With shared key authentication, after the WNIC sends its initial authentication request it will receive an authentication frame from the access point containing challenge text. The WNIC sends an authentication frame containing the encrypted version of the challenge text to the access point. The access point ensures the text was encrypted with the correct key by decrypting it with its own key. The result of this process determines the WNIC's authentication status.
- Association request frame: sent from a station it enables the access point to allocate resources and synchronize. The frame carries information about the WNIC including supported data rates and the SSID of the network the station wishes to associate with. If the request is accepted, the access point reserves memory and establishes an association ID for the WNIC.
- Association response frame: sent from an access point to a station containing the acceptance or rejection to an association request. If it is an acceptance, the frame will contain information such an association ID and supported data rates.
- Beacon frame: Sent periodically from an access point to announce its presence and provide the SSID, and other parameters for WNICs within range.
- Deauthentication frame: Sent from a station wishing to terminate connection from another station.
- Disassociation frame: Sent from a station wishing to terminate connection. It's an elegant way to allow the access point to relinquish memory allocation and remove the WNIC from the association table.
- Probe request frame: Sent from a station when it requires information from another station.
- Probe response frame: Sent from an access point containing capability information, supported data rates, etc., after receiving a probe request frame.

- Reassociation request frame: A WNIC sends a reassociation request when it drops from range of the currently associated access point and finds another access point with a stronger signal. The new access point coordinates the forwarding of any information that may still be contained in the buffer of the previous access point.
- Reassociation response frame: Sent from an access point containing the acceptance or rejection to a WNIC reassociation request frame. The frame includes information required for association such as the association ID and supported data rates.

Control frames facilitate in the exchange of data frames between stations. Some common 802.11 control frames include:

- Acknowledgement (ACK) frame: After receiving a data frame, 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 frame within a predetermined period of time, the sending station will resend the frame.
- Request to Send (RTS) frame: The RTS and CTS frames provide an optional collision reduction scheme for access point with hidden stations. A station sends a RTS frame to as the first step in a two-way handshake required before sending data frames.

Source : http://nprcet.org/e%20content/Misc/e-Learning/IT/VIII%20Sem/IT1452%20-%20Fundamentals%20of%20Pervasive%20Computing.pdf