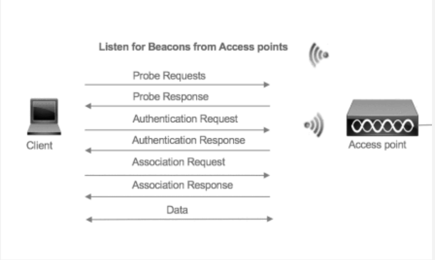
Cheatography

802.11 Cheat Sheet

by shorttcircuitt (shortt_circuitt) via cheatography.com/77499/cs/18993/

802.11 Connection Basics



Connection Status

State 1	Unauthenticated and Unassociated
State 2	Authenticated, Unassociated
State 3	Authenticated, Associated

STA must be in State 3 before connection is established.

Control Frames

ACK: After receiving a data frame, the receiver will send and ACK frame if no errors were found. If the transmitter doesn't receive an ACK within a predetermined period, it will retransmit the frame

RTS: The transmitter sends an optional RTS frame before sending any data frames.

CTS: The receiver responds to the RTS with a CTS frame, clearing the transmitter to send its data frame. The CTS provides collision control management by including a time value were all other devices are to hold off transmission while the RTS transmitter sends its data

Management Frames

1000	**Beacon**: Sent periodically from an AP to announce its presence and relay information that is required by the STAs to connect to the wireless network.
0100	**Probe Request**: Sent from a STA to discover 802.11 networks within its proximity. Probe requests advertise the STAs supported data rates and 802.11 capabilities such as 802.11n.
0101	**Probe Response**: Sent from an AP after receiving a Probe Request and having at least one common supported data rate. Advertises the SSID, supported data rates, encryption types, and other 802.11 capabilities.
1011	**Authentication Request**: The STA chooses a SSID/network from the probe responses it receives. It also checks the compatibility on encryption type. Once compatible networks are discovered the STA will attempt low-level 802.11 authentication with compatible APs. The STA sends a low-level 802.11 authentication frame to an AP, setting the authentication to open and the sequence to 0x0001.
1011	**Authentication Response:** The AP receives the authentication frame and responds to the STA with authentication frame set to open indicating a sequence. *If an AP receives any frame other than an authentication or probe request from a STA that is not authenticated it will respond with a deauthentication frame placing the mobile into an unauthenticated and unassociated state. The STA will have to begin the association process from the low level authentication step.* At this point the STA is authenticated but not yet associated.
1100	**Deauthentication**
0000	**Association Request:** Once the STA determines which AP it would like to associate to, it will send an association request to that AP. The association request contains chosen encryption types and other compatible 802.11 capabilities.
0001	**Association Response:** If the elements of association request match the capabilities of the AP, it will create an Association ID for the STA and respond with an association response, with a success message granting network access to the STA.
0010	**Reassociation Request**
0011	**Reassociation Response**
1010	**Disassociation**

Beacon Frame

The AP broadcasts a Beacon frame at regular intervals, typically every **100ms**. This is called the **Target Beacon Transmit Time (TBTT)**

The Beacon carries regulatory, capability and BSS management information such as **Supported Data Rates**, **SSID** and **Timestamp**.

A Beacon is also used to advertise the AP capabilities. This is used by clients doing a passive scan to make a decision to connect to the AP. This is necessary to keep all clients synchronized with the AP in order for the clients to perform functions like power save.