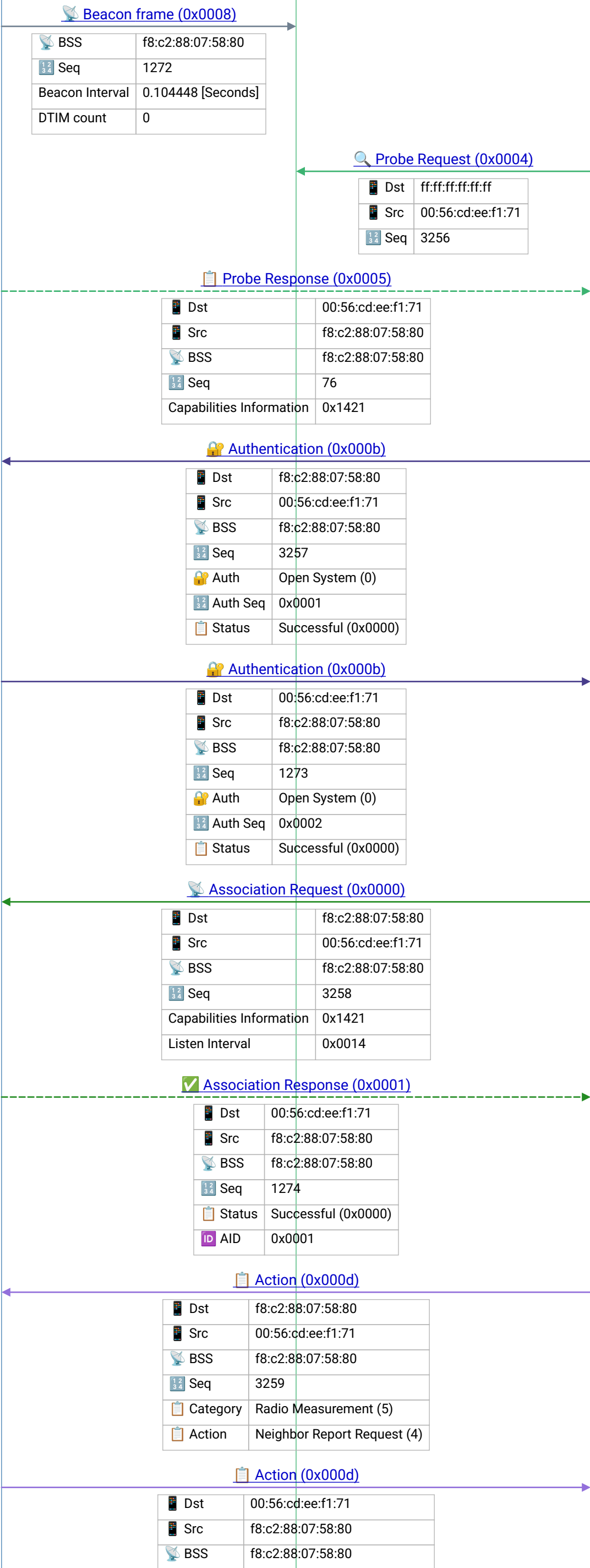


Client C

Broadcast

iPhone Client

roam_intra_dot11k_actions.pcapng



Beacon – AP announces its presence at Beacon Interval (usually 100 TU = 102.4ms); carries SSID, supported rates, DTIM count, RSN info; basis for passive scanning

Probe Request – active scanning: client solicits responses from APs; directed (specific SSID) or wildcard (broadcast SSID); faster than passive scanning (beacon-only)

Probe Response – AP replies with capabilities (SSID, rates, RSN, channel); client uses signal strength + capabilities to select best AP for association

802.11 Authentication – Open System (2 frames) or SAE/WPA3 (multiple rounds); must succeed before Association

802.11 Authentication – Open System (2 frames) or SAE/WPA3 (multiple rounds); must succeed before Association

Association Request – client joins BSS; carries SSID, supported rates, RSN (WPA2/WPA3) capabilities; AP assigns AID in response

Association Response – AP accepts/rejects client; Status 0=Success; assigns AID (Association ID) used for PS-Poll and TIM bitmap addressing

Frame 8 | 2017-02-25T13:34:15.705969Z

Frame 9 | 2017-02-25T13:34:15.711411Z

Client C

Broadcast

iPhone Client

Seq	1276
Category	Radio Measurement (5)
Action	Neighbor Report Response (5)

QoS Data (0x0028)

Dst	00:23:5d:c9:5a:c7
Src	00:56:cd:ee:f1:71
BSS	f8:c2:88:07:58:80
Seq	58
TID	11
Priority	Excellent Effort (Best Effort) (3)
Len	75

802.11 QoS Data – TID (Traffic Identifier) maps to WMM Access Category: TID 0-2=Best Effort (AC_BE), 3=Background (AC_BK), 4-5=Video (AC_VI), 6-7=Voice (AC_VO)