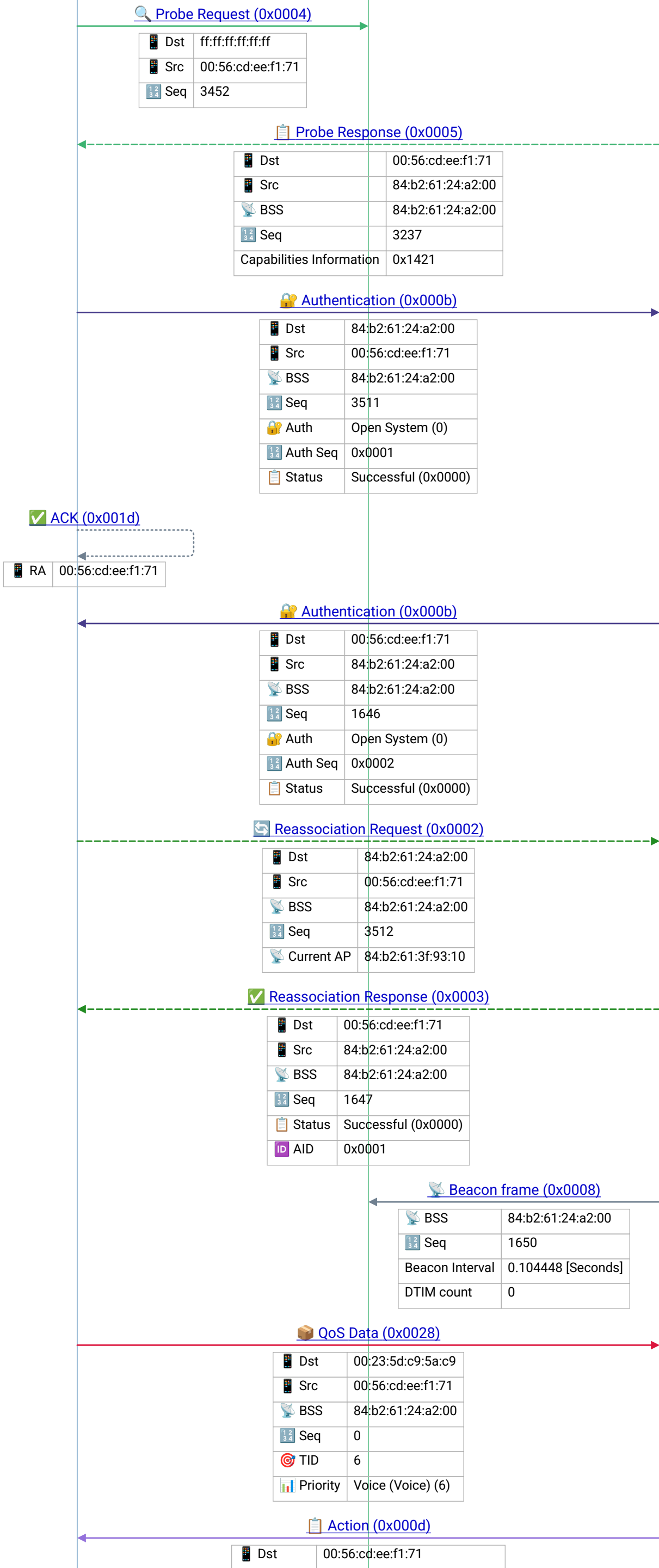


iPhone Client

Broadcast

Cisco AP 1

roam_interL3_open_wlan.pcapng



💡 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

Frame 4 | 2017-01-28T14:37:38.938544Z

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

💡 Reassociation Request – client roams to new AP within same ESS; carries Current AP MAC so new AP can request PMK from old AP (fast roaming) or via RADIUS


💡 Reassociation Response – new AP accepts roaming client; AID may change; PMK transfer via OKC, 802.11r FT, or CCKM enables fast secure roaming without full re-auth

💡 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






💡 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)


Frame 12 | 2017-01-28T14:37:38.990334Z







 iPhone Client

 Broadcast








 Cisco AP 1

 Src	84:b2:61:24:a2:00
 BSS	84:b2:61:24:a2:00
 Seq	1651
 Category	Block Ack (3)
 Action	Add Block Ack Request (0x00)


 Action (0x000d)

 Dst	84:b2:61:24:a2:00
 Src	00:56:cd:ee:f1:71
 BSS	84:b2:61:24:a2:00
 Seq	3513
 Category	Block Ack (3)
 Action	Add Block Ack Response (0x01)

 QoS Data (0x0028)

 Dst	00:56:cd:ee:f1:71
 Src	00:23:5d:c9:5a:c9
 BSS	84:b2:61:24:a2:00
 Seq	291
 TID	0
 Priority	Best Effort (Best Effort) (0)
 Len	36

Frame 13 |
2017-01-28T14:37:38.990362Z

 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)