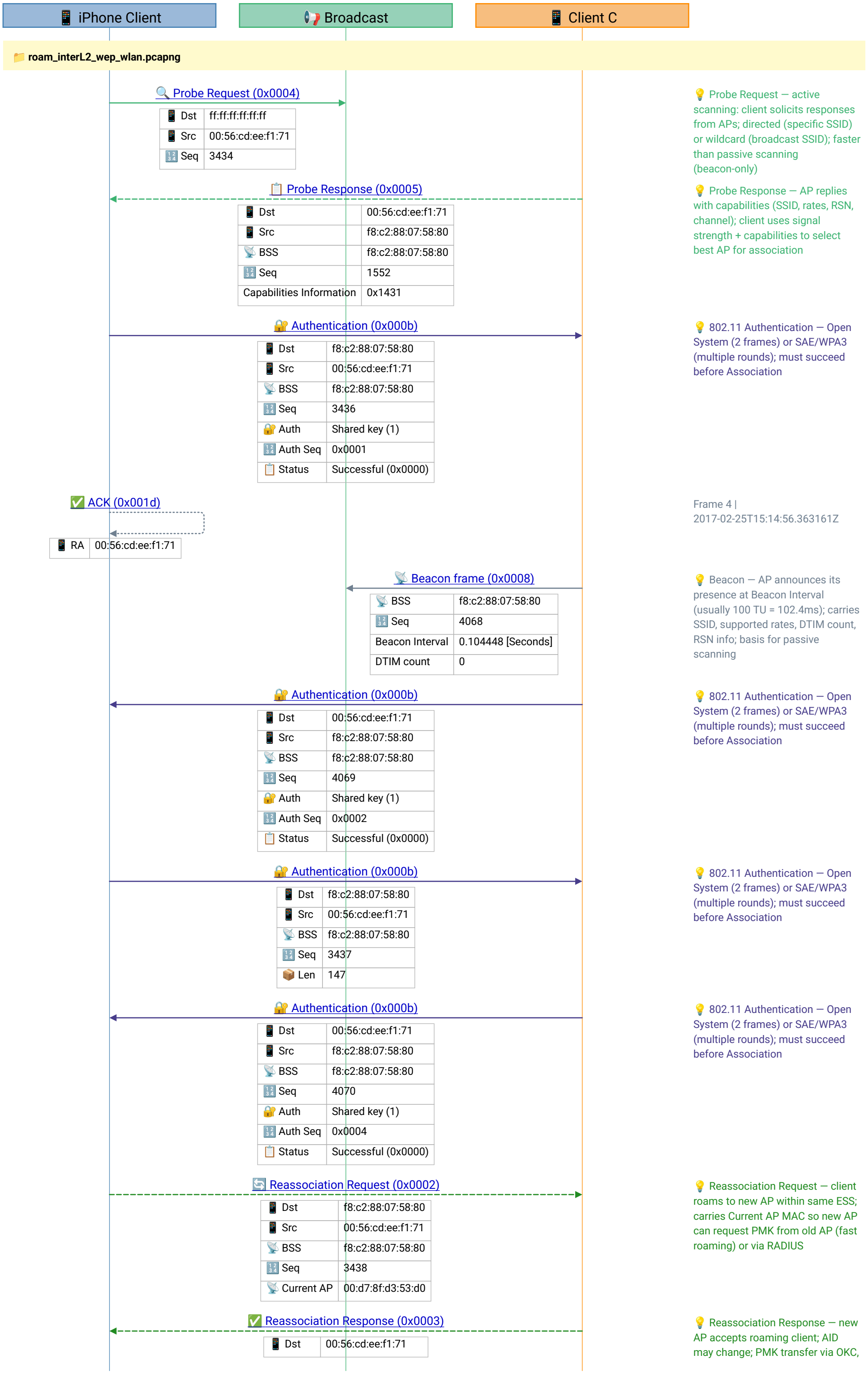
iPhone Client
Broadcast
Client C
roam_interL2_wep_wlan.pcapng
Probe Request (0x0004)
Dst ff:ff:ff:ff:ff:ff
Src 00:56:cd:ee:f1:71
Seq 3434
Probe Response (0x0005)
Dst 00:56:cd:ee:f1:71
Src f8:c2:88:07:58:80
BSS f8:c2:88:07:58:80
Seq 1552
Capabilities Information 0x1431
Authentication (0x000b)
Dst f8:c2:88:07:58:80
Src 00:56:cd:ee:f1:71
BSS f8:c2:88:07:58:80
Seq 3436
Auth Shared key (1)
Auth Seq 0x0001
Status Successful (0x0000)
ACK (0x001d)
RA 00:56:cd:ee:f1:71
Beacon frame (0x0008)
BSS f8:c2:88:07:58:80
Seq 4068
Beacon Interval 0.104448 [Seconds]
DTIM count 0
Authentication (0x000b)
Dst 00:56:cd:ee:f1:71
Src f8:c2:88:07:58:80
BSS f8:c2:88:07:58:80
Seq 4069
Auth Shared key (1)
Auth Seq 0x0002
Status Successful (0x0000)
Authentication (0x000b)
Dst f8:c2:88:07:58:80
Src 00:56:cd:ee:f1:71
BSS f8:c2:88:07:58:80
Seq 3437
Len 147
Authentication (0x000b)
Dst 00:56:cd:ee:f1:71
Src f8:c2:88:07:58:80
BSS f8:c2:88:07:58:80
Seq 4070
Auth Shared key (1)
Auth Seq 0x0004
Status Successful (0x0000)
Reassociation Request (0x0002)
Dst f8:c2:88:07:58:80
Src 00:56:cd:ee:f1:71
BSS f8:c2:88:07:58:80
Seq 3438
Current AP 00:d7:8f:d3:53:d0
Reassociation Response (0x0003)
Dst 00:56:cd:ee:f1:71
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 | 2017-02-25T15:14:56.363161Z
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 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
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,

📱 iPhone Client	📢 Broadcast	📱 Client C

📱 Src	f8:c2:88:07:58:80
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	4071
📋 Status	Successful (0x0000)
🆔 AID	0x0001

802.11r FT, or CCKM enables fast secure roaming without full re-auth

📋 Action (0x000d)

Frame 13 | 2017-02-25T15:14:56.397605Z

📱 Dst	f8:c2:88:07:58:80
📱 Src	00:56:cd:ee:f1:71
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	3439
📋 Category	Radio Measurement (5)
📋 Action	Neighbor Report Request (4)

📋 Action (0x000d)

Frame 15 | 2017-02-25T15:14:56.39943Z

📱 Dst	00:56:cd:ee:f1:71
📱 Src	f8:c2:88:07:58:80
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	4073
📋 Category	Radio Measurement (5)
📋 Action	Neighbor Report Response (5)

📦 QoS Data (0x0028)

💡 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)

📱 Dst	00:23:5d:c9:5a:c7
📱 Src	00:56:cd:ee:f1:71
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	0
🎯 TID	6
📊 Priority	Voice (Voice) (6)
📦 Len	36