Exploring roam_interL3_wep_wlan.pcapng

📱 iPhone Client	📢 Broadcast	📱 Client C

📁 **roam_interL3_wep_wlan.pcapng**

🔍 Probe Request (0x0004)

📱 Dst	ff:ff:ff:ff:ff:ff
📱 Src	00:56:cd:ee:f1:71
🔢 Seq	1121

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

📋 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	1474
Capabilities Information	0x1431

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

🔐 Authentication (0x000b)

📱 Dst	f8:c2:88:07:58:80
📱 Src	00:56:cd:ee:f1:71
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	1123
🔐 Auth	Shared key (1)
🔢 Auth Seq	0x0001
📋 Status	Successful (0x0000)

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

✅ ACK (0x001d)

📱 RA	00:56:cd:ee:f1:71

Frame 4 | 2017-02-25T19:43:04.237769Z

🔐 Authentication (0x000b)

📱 Dst	00:56:cd:ee:f1:71
📱 Src	f8:c2:88:07:58:80
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	2797
🔐 Auth	Shared key (1)
🔢 Auth Seq	0x0002
📋 Status	Successful (0x0000)

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

🔐 Authentication (0x000b)

📱 Dst	f8:c2:88:07:58:80
📱 Src	00:56:cd:ee:f1:71
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	1124
📦 Len	147

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

🔐 Authentication (0x000b)

📱 Dst	00:56:cd:ee:f1:71
📱 Src	f8:c2:88:07:58:80
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	2798
🔐 Auth	Shared key (1)
🔢 Auth Seq	0x0004
📋 Status	Successful (0x0000)

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

🔄 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	1125
📡 Current AP	00:d7:8f:d3:53:d0

💡 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 (0x0003)

📱 Dst	00:56:cd:ee:f1:71
📱 Src	f8:c2:88:07:58:80
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	2799
📋 Status	Successful (0x0000)
🆔 AID	0x0001

💡 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

📱 iPhone Client	📢 Broadcast	📱 Client C

📋 Action (0x000d)

📱 Dst	f8:c2:88:07:58:80
📱 Src	00:56:cd:ee:f1:71
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	1126
📋 Category	Radio Measurement (5)
📋 Action	Neighbor Report Request (4)

Frame 12 | 2017-02-25T19:43:04.247803Z

📋 Action (0x000d)

📱 Dst	00:56:cd:ee:f1:71
📱 Src	f8:c2:88:07:58:80
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	2802
📋 Category	Radio Measurement (5)
📋 Action	Neighbor Report Response (5)

Frame 14 | 2017-02-25T19:43:04.249614Z

📦 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	0
🎯 TID	6
📊 Priority	Voice (Voice) (6)
📦 Len	36

💡 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)

📦 QoS Data (0x0028)

📱 Dst	00:56:cd:ee:f1:71
📱 Src	00:23:5d:c9:5a:c7
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	34
🎯 TID	0
📊 Priority	Best Effort (Best Effort) (0)
📦 Len	54

💡 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)

📡 Beacon frame (0x0008)

📡 BSS	f8:c2:88:07:58:80
🔢 Seq	2803
Beacon Interval	0.104448 [Seconds]
DTIM count	0

💡 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

💤 Null function (No data) (0x0024)

💤 Power	STA will go to sleep
📱 Dst	f8:c2:88:07:58:80
📱 Src	00:56:cd:ee:f1:71
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	1127

💡 Null Data — no payload; used for power management signaling: PWR MGT=1 tells AP the client is going to sleep (AP buffers frames); PWR MGT=0 means client is awake