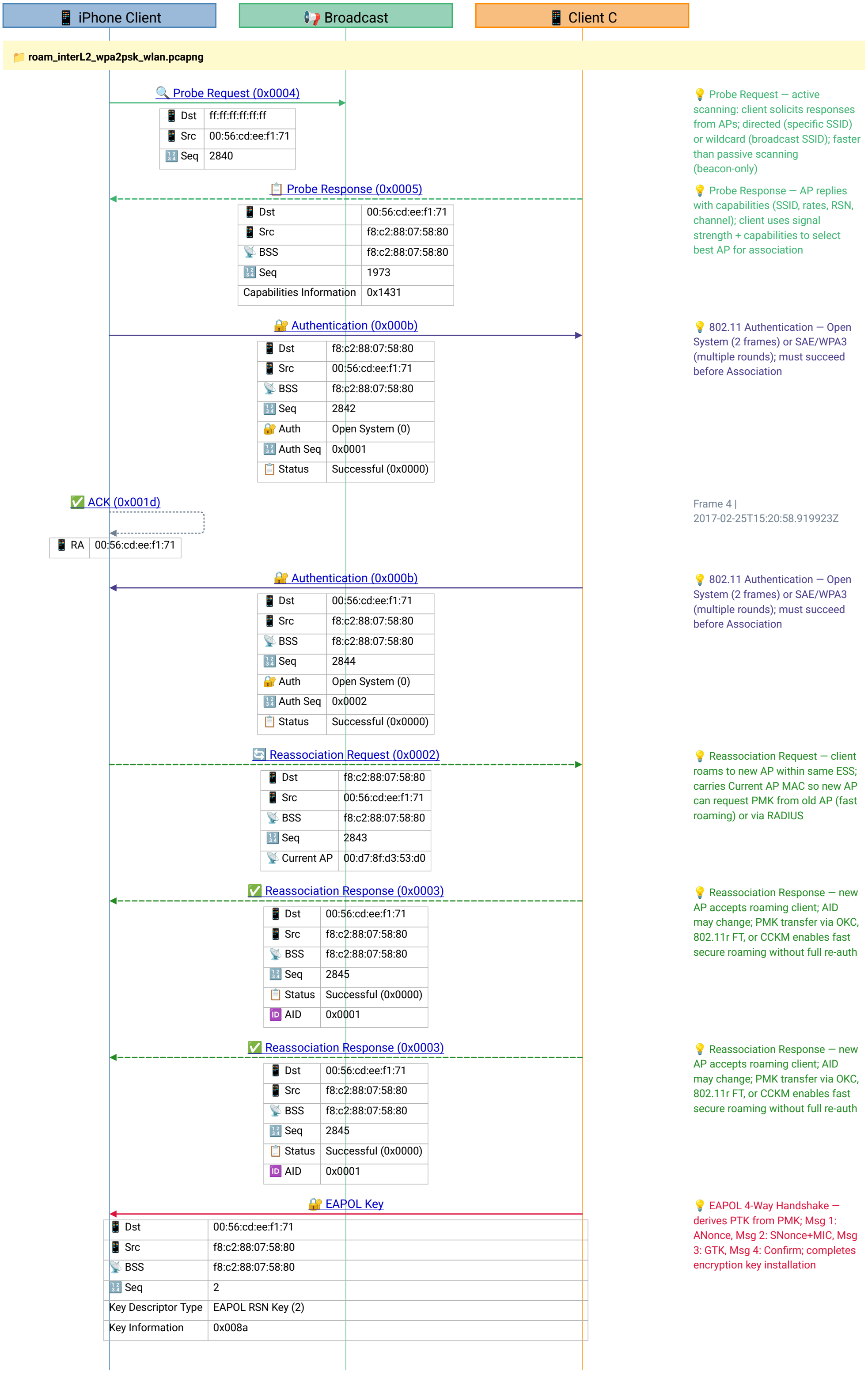
iPhone Client
Broadcast
Client C
roam_interL2_wpa2psk_wlan.pcapng
Probe Request (0x0004)
Dst ff:ff:ff:ff:ff:ff
Src 00:56:cd:ee:f1:71
Seq 2840
Probe Response (0x0005)
Dst 00:56:cd:ee:f1:71
Src f8:c2:88:07:58:80
BSS f8:c2:88:07:58:80
Seq 1973
Capabilities Information 0x1431
Authentication (0x000b)
Dst f8:c2:88:07:58:80
Src 00:56:cd:ee:f1:71
BSS f8:c2:88:07:58:80
Seq 2842
Auth Open System (0)
Auth Seq 0x0001
Status Successful (0x0000)
ACK (0x001d)
RA 00:56:cd:ee:f1:71
Authentication (0x000b)
Dst 00:56:cd:ee:f1:71
Src f8:c2:88:07:58:80
BSS f8:c2:88:07:58:80
Seq 2844
Auth Open System (0)
Auth Seq 0x0002
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 2843
Current AP 00:d7:8f:d3:53:d0
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 2845
Status Successful (0x0000)
AID 0x0001
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 2845
Status Successful (0x0000)
AID 0x0001
EAPOL Key
Dst 00:56:cd:ee:f1:71
Src f8:c2:88:07:58:80
BSS f8:c2:88:07:58:80
Seq 2
Key Descriptor Type EAPOL RSN Key (2)
Key Information 0x008a
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 | 2017-02-25T15:20:58.919923Z
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
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
EAPOL 4-Way Handshake — derives PTK from PMK; Msg 1: ANonce, Msg 2: SNonce+MIC, Msg 3: GTK, Msg 4: Confirm; completes encryption key installation

📱 iPhone Client	📢 Broadcast	📱 Client C

Key Length	16
Replay Counter	0
WPA Key Nonce	5fdef386daea32efe5d9047b1562237a961140038392be7904cb7790194f19dd

📋 Action (0x000d)

Frame 11 | 2017-02-25T15:20:58.96031Z

📱 Dst	f8:c2:88:07:58:80
📱 Src	00:56:cd:ee:f1:71
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	2844
📋 Category	Radio Measurement (5)
📋 Action	Neighbor Report Request (4)

📋 Action (0x000d)

Frame 13 | 2017-02-25T15:20:58.960904Z

📱 Dst	f8:c2:88:07:58:80
📱 Src	00:56:cd:ee:f1:71
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	2845
📋 Category	Block Ack (3)
📋 Action	Add Block Ack Request (0x00)

📋 Action (0x000d)

Frame 15 | 2017-02-25T15:20:58.961007Z

📱 Dst	00:56:cd:ee:f1:71
📱 Src	f8:c2:88:07:58:80
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	2847
📋 Category	Block Ack (3)
📋 Action	Add Block Ack Response (0x01)

🔐 EAPOL Key

💡 EAPOL 4-Way Handshake — derives PTK from PMK; Msg 1: ANonce, Msg 2: SNonce+MIC, Msg 3: GTK, Msg 4: Confirm; completes encryption key installation

📱 Dst	f8:c2:88:07:58:80
📱 Src	00:56:cd:ee:f1:71
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	0
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x010a
Key Length	16
Replay Counter	0
WPA Key Nonce	d2899448aede76f62427213809c6271bc722e375e455dd52754baa5ca9714b8e

✅ Block Ack Req (0x0018)

💡 Block Ack — acknowledges multiple MPDUs in a single frame (A-MPDU aggregation); bitmap indicates which sequence numbers were received; improves throughput by reducing per-frame ACK overhead

📋 Policy	Immediate Acknowledgement Required
📋 Type	Compressed BlockAck

✅ Block Ack (0x0019)

💡 Block Ack — acknowledges multiple MPDUs in a single frame (A-MPDU aggregation); bitmap indicates which sequence numbers were received; improves throughput by reducing per-frame ACK overhead

📋 Policy	Immediate Acknowledgement Required
📋 Type	Compressed BlockAck
📊 Bitmap	0000000000000000
✅ Last ACK	1

📋 Action (0x000d)

Frame 20 | 2017-02-25T15:20:58.961909Z

📱 Dst	00:56:cd:ee:f1:71
📱 Src	f8:c2:88:07:58:80
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	2848
📋 Category	Radio Measurement (5)
📋 Action	Neighbor Report Response (5)

🔐 EAPOL Key

💡 EAPOL 4-Way Handshake — derives PTK from PMK; Msg 1: ANonce, Msg 2: SNonce+MIC, Msg 3: GTK, Msg 4: Confirm; completes encryption key installation

📱 Dst	00:56:cd:ee:f1:71
📱 Src	f8:c2:88:07:58:80
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	3
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x13ca
Key Length	16
Replay Counter	1

📱 iPhone Client | 📢 Broadcast | 📱 Client C

WPA Key Nonce	5fdef386daea32efe5d9047b1562237a961140038392be7904cb7790194f19dd

🔐 EAPOL Key

📱 Dst	f8:c2:88:07:58:80
📱 Src	00:56:cd:ee:f1:71
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	1
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x030a
Key Length	16
Replay Counter	1
WPA Key Nonce	0000000000000000000000000000000000000000000000000000000000000000

💡 EAPOL 4-Way Handshake — derives PTK from PMK; Msg 1: ANonce, Msg 2: SNonce+MIC, Msg 3: GTK, Msg 4: Confirm; completes encryption key installation

📦 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	44

💡 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)