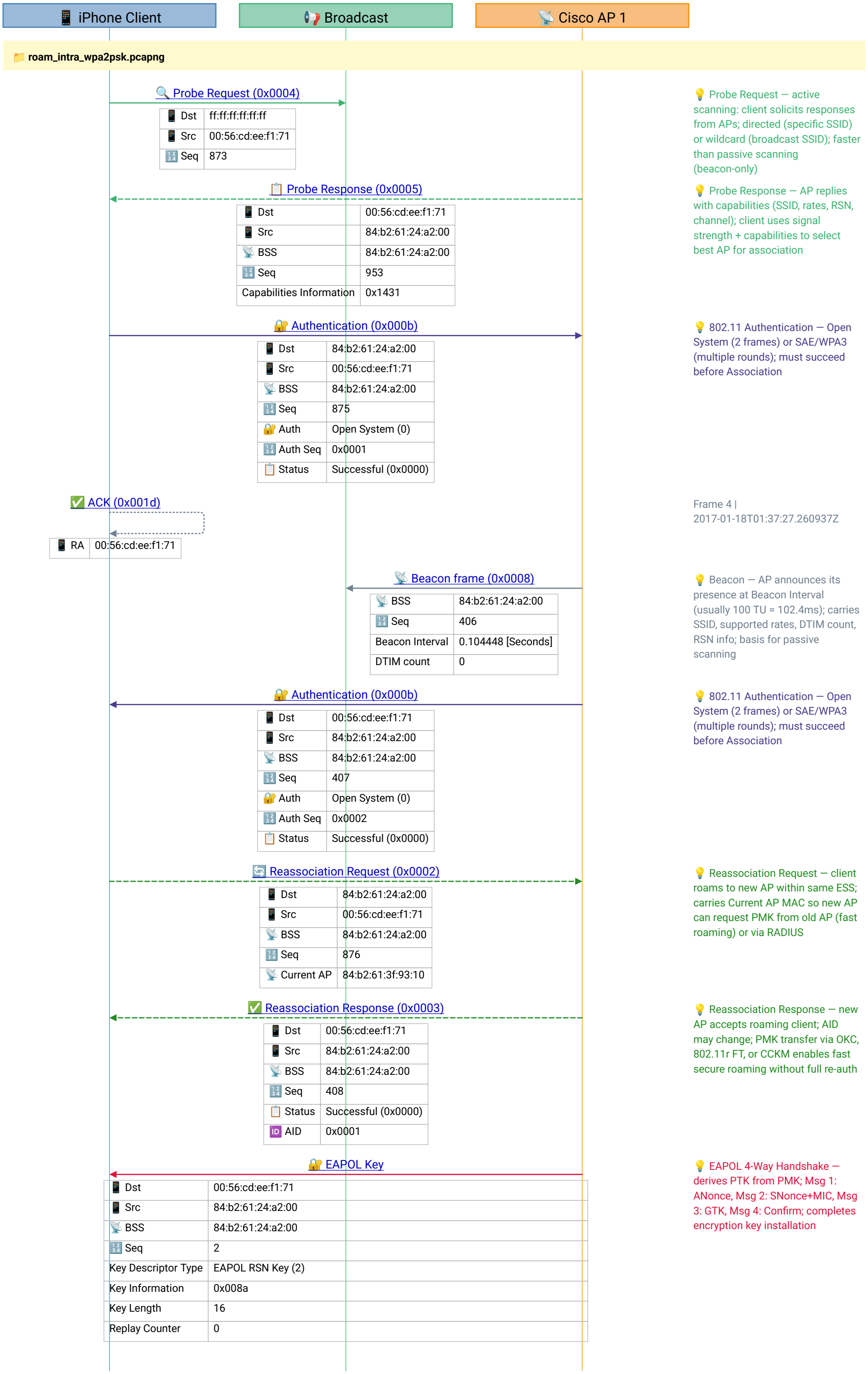
📱 iPhone Client
📢 Broadcast
📡 Cisco AP 1
📁 roam_intra_wpa2psk.pcapng
🔍 Probe Request (0x0004)
📱 Dst ff:ff:ff:ff:ff:ff
📱 Src 00:56:cd:ee:f1:71
🔢 Seq 873
💡 Probe Request — active scanning: client solicits responses from APs; directed (specific SSID) or wildcard (broadcast SSID); faster than passive scanning (beacon-only)
📋 Probe Response (0x0005)
📱 Dst 00:56:cd:ee:f1:71
📱 Src 84:b2:61:24:a2:00
📡 BSS 84:b2:61:24:a2:00
🔢 Seq 953
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 84:b2:61:24:a2:00
📱 Src 00:56:cd:ee:f1:71
📡 BSS 84:b2:61:24:a2:00
🔢 Seq 875
🔐 Auth Open System (0)
🔢 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 | 2017-01-18T01:37:27.260937Z
📡 Beacon frame (0x0008)
📡 BSS 84:b2:61:24:a2:00
🔢 Seq 406
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
🔐 Authentication (0x000b)
📱 Dst 00:56:cd:ee:f1:71
📱 Src 84:b2:61:24:a2:00
📡 BSS 84:b2:61:24:a2:00
🔢 Seq 407
🔐 Auth Open System (0)
🔢 Auth Seq 0x0002
📋 Status Successful (0x0000)
💡 802.11 Authentication — Open System (2 frames) or SAE/WPA3 (multiple rounds); must succeed before Association
🔄 Reassociation Request (0x0002)
📱 Dst 84:b2:61:24:a2:00
📱 Src 00:56:cd:ee:f1:71
📡 BSS 84:b2:61:24:a2:00
🔢 Seq 876
📡 Current AP 84:b2:61:3f:93:10
💡 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 84:b2:61:24:a2:00
📡 BSS 84:b2:61:24:a2:00
🔢 Seq 408
📋 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
🔐 EAPOL Key
📱 Dst 00:56:cd:ee:f1:71
📱 Src 84:b2:61:24:a2:00
📡 BSS 84:b2:61:24:a2:00
🔢 Seq 2
Key Descriptor Type EAPOL RSN Key (2)
Key Information 0x008a
Key Length 16
Replay Counter 0
💡 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 | 📡 Cisco AP 1

WPA Key Nonce	f440970663c77ba67bed5f343a585e0bf56b1eaa58fb1b039c31ad9a11320e29

📋 Action (0x000d)

Frame 11 | 2017-01-18T01:37:27.291327Z

📱 Dst	84:b2:61:24:a2:00
📱 Src	00:56:cd:ee:f1:71
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	877
📋 Category	Block Ack (3)
📋 Action	Add Block Ack Request (0x00)

🔐 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	84:b2:61:24:a2:00
📱 Src	00:56:cd:ee:f1:71
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	0
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x010a
Key Length	16
Replay Counter	0
WPA Key Nonce	af5442af157dabeeafbb7ddd1116bba722c0e9fd580ac052014a0a505280b5ff

📋 Action (0x000d)

Frame 15 | 2017-01-18T01:37:27.296191Z

📱 Dst	00:56:cd:ee:f1:71
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	409
📋 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	00:56:cd:ee:f1:71
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	3
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x13ca
Key Length	16
Replay Counter	1
WPA Key Nonce	f440970663c77ba67bed5f343a585e0bf56b1eaa58fb1b039c31ad9a11320e29

✅ 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

🔐 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	84:b2:61:24:a2:00
📱 Src	00:56:cd:ee:f1:71
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	1
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x030a
Key Length	16
Replay Counter	1
WPA Key Nonce	0000000000000000000000000000000000000000000000000000000000000000

📦 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	84:b2:61:24:a2:00
🔢 Seq	0

📱 iPhone Client | 📢 Broadcast | 📡 Cisco AP 1

🎯 TID	6
📊 Priority	Voice (Voice) (6)
📦 Len	44

📋 Action (0x000d)

Frame 23 | 2017-01-18T01:37:27.313574Z

📱 Dst	00:56:cd:ee:f1:71
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	410
📋 Category	Block Ack (3)
📋 Action	Add Block Ack Request (0x00)

📋 Action (0x000d)

Frame 24 | 2017-01-18T01:37:27.313585Z

📱 Dst	84:b2:61:24:a2:00
📱 Src	00:56:cd:ee:f1:71
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	878
📋 Category	Block Ack (3)
📋 Action	Add Block Ack Response (0x01)