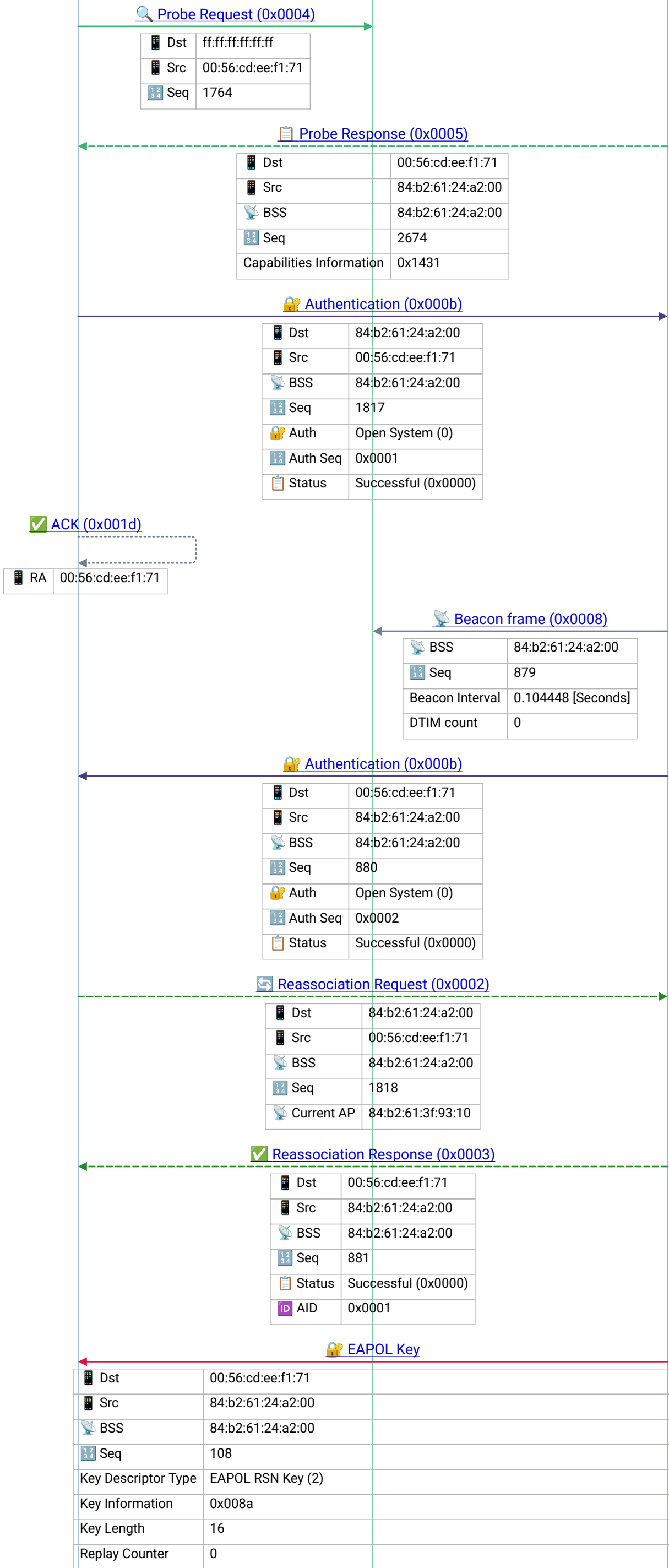


roam_interL3_wpa2psk_wlan.pcapng



💡 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 | 2017-01-28T14:29:15.933894Z

💡 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

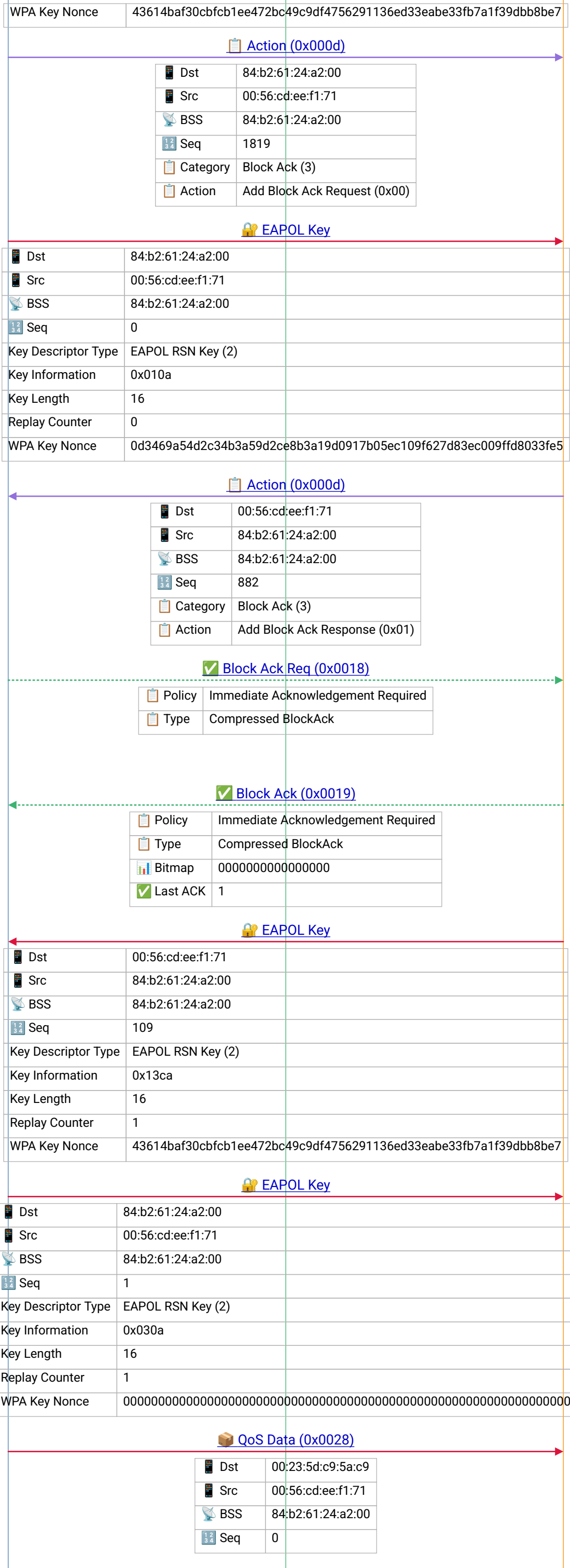
💡 802.11 Authentication – Open System (multiple rounds); must succeed before Association

💡 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

💡 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
---------------	-----------	------------



Frame 11 | 2017-01-28T14:29:15.961254Z

💡 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

Frame 15 | 2017-01-28T14:29:15.961451Z

💡 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

💡 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

💡 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

💡 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

💡 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)

iPhone Client

Broadcast

Cisco AP 1

TID	6
Priority	Voice (Voice) (6)
Len	44

Action (0x000d)



Dst	00:56:cd:ee:f1:71
Src	84:b2:61:24:a2:00
BSS	84:b2:61:24:a2:00
Seq	885
Category	Block Ack (3)
Action	Add Block Ack Request (0x00)

Frame 23 |
2017-01-28T14:29:15.986552Z

Action (0x000d)



Dst	84:b2:61:24:a2:00
Src	00:56:cd:ee:f1:71
BSS	84:b2:61:24:a2:00
Seq	1820
Category	Block Ack (3)
Action	Add Block Ack Response (0x01)

Frame 24 |
2017-01-28T14:29:15.986563Z