

roam\_interL2\_open\_wlan.pcapng

Authentication (0x000b)

Dst	84:b2:61:24:a2:00
Src	00:56:cd:ee:f1:71
BSS	84:b2:61:24:a2:00
Seq	3398
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 2 | 2017-01-22T14:50:56.92771Z

Authentication (0x000b)

Dst	00:56:cd:ee:f1:71
Src	84:b2:61:24:a2:00
BSS	84:b2:61:24:a2:00
Seq	2260
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	3399
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	2261
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

QoS Data (0x0028)

Dst	00:23:5d:c9:5a:c7
Src	00:56:cd:ee:f1:71
BSS	84:b2:61:24:a2:00
Seq	0
TID	6
Priority	Voice (Voice) (6)

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	84:b2:61:24:a2:00
Seq	2264
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

Action (0x000d)

Dst	00:56:cd:ee:f1:71
Src	84:b2:61:24:a2:00
BSS	84:b2:61:24:a2:00
Seq	2265
Category	Block Ack (3)
Action	Add Block Ack Request (0x00)

Frame 10 | 2017-01-22T14:50:56.982793Z

Action (0x000d)

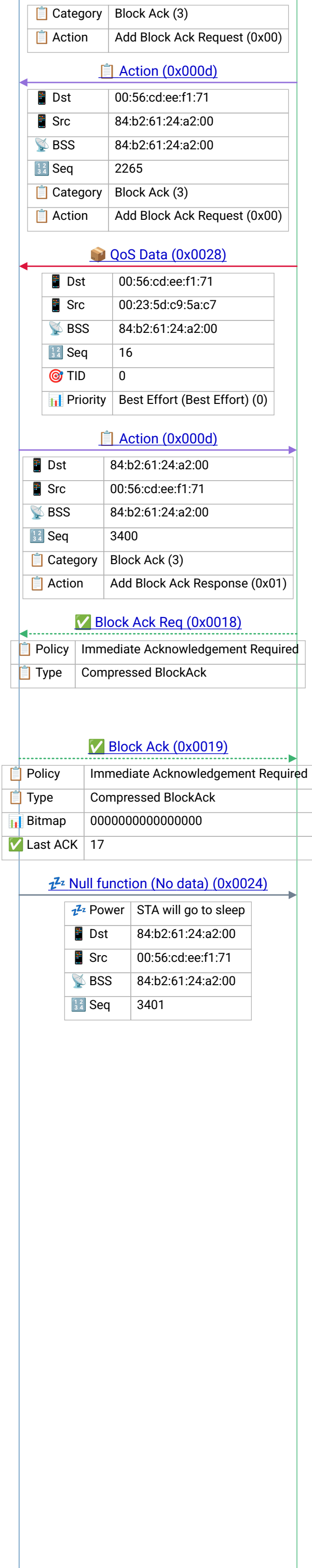
Dst	00:56:cd:ee:f1:71
Src	84:b2:61:24:a2:00
BSS	84:b2:61:24:a2:00
Seq	2265

Frame 11 | 2017-01-22T14:50:56.982843Z

**iPhone Client**

**Cisco AP 1**

**Broadcast**



Frame 12 |  
2017-01-22T14:50:56.983194Z

💡 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)

Frame 14 |  
2017-01-22T14:50:56.985134Z

💡 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

💡 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