📱 iPhone Client	📢 Broadcast	📡 Cisco AP 1

📁 **clientassoc_wpa2psk_wlan.pcapng**

🔍 Probe Request (0x0004)

📱 Dst	ff:ff:ff:ff:ff:ff
📱 Src	00:56:cd:ee:f1:71
🔢 Seq	3862

💡 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	1490
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	3863
🔐 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

🔐 Authentication (0x000b)

📱 Dst	00:56:cd:ee:f1:71
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	3933
🔐 Auth	Open System (0)
🔢 Auth Seq	0x0002
📋 Status	Successful (0x0000)

Frame 4 | 2017-01-16T02:18:46.13406Z

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

📡 Association Request (0x0000)

📱 Dst	84:b2:61:24:a2:00
📱 Src	00:56:cd:ee:f1:71
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	3864
Capabilities Information	0x1431
Listen Interval	0x0014
🔐 AKM	PSK (2)

💡 Association Request — client joins BSS; carries SSID, supported rates, RSN (WPA2/WPA3) capabilities; AP assigns AID in response

✅ Association Response (0x0001)

📱 Dst	00:56:cd:ee:f1:71
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	3934
📋 Status	Successful (0x0000)
🆔 AID	0x0001

💡 Association Response — AP accepts/rejects client; Status 0=Success; assigns AID (Association ID) used for PS-Poll and TIM bitmap addressing

🔐 EAPOL Key

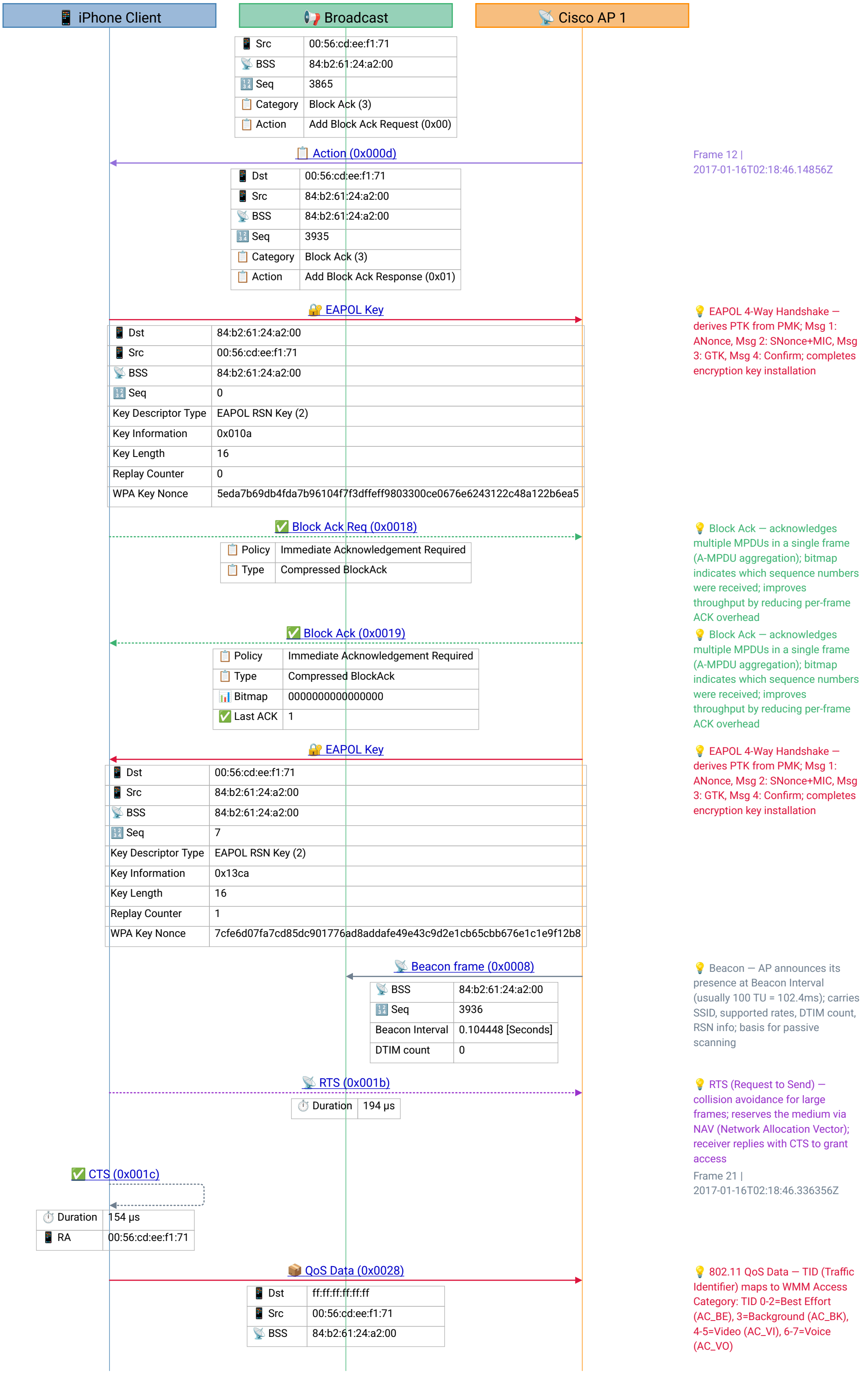
📱 Dst	00:56:cd:ee:f1:71
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	6
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x008a
Key Length	16
Replay Counter	0
WPA Key Nonce	7cfe6d07fa7cd85dc901776ad8addafe49e43c9d2e1cb65cbb676e1c1e9f12b8

💡 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

📋 Action (0x000d)

📱 Dst	84:b2:61:24:a2:00

Frame 10 | 2017-01-16T02:18:46.14549Z


iPhone Client
Broadcast
Cisco AP 1
Src 00:56:cd:ee:f1:71
BSS 84:b2:61:24:a2:00
Seq 3865
Category Block Ack (3)
Action Add Block Ack Request (0x00)
Action (0x000d)
Frame 12 | 2017-01-16T02:18:46.14856Z
Dst 00:56:cd:ee:f1:71
Src 84:b2:61:24:a2:00
BSS 84:b2:61:24:a2:00
Seq 3935
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 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 5eda7b69db4fda7b96104f7f3dffeff9803300ce0676e6243122c48a122b6ea5
Block Ack Req (0x0018)
Policy Immediate Acknowledgement Required
Type Compressed BlockAck
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 (0x0019)
Policy Immediate Acknowledgement Required
Type Compressed BlockAck
Bitmap 0000000000000000
Last ACK 1
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 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 7
Key Descriptor Type EAPOL RSN Key (2)
Key Information 0x13ca
Key Length 16
Replay Counter 1
WPA Key Nonce 7cfe6d07fa7cd85dc901776ad8addafe49e43c9d2e1cb65cbb676e1c1e9f12b8
Beacon frame (0x0008)
BSS 84:b2:61:24:a2:00
Seq 3936
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
RTS (0x001b)
Duration 194 µs
RTS (Request to Send) — collision avoidance for large frames; reserves the medium via NAV (Network Allocation Vector); receiver replies with CTS to grant access
Frame 21 | 2017-01-16T02:18:46.336356Z
CTS (0x001c)
Duration 154 µs
RA 00:56:cd:ee:f1:71
QoS Data (0x0028)
Dst ff:ff:ff:ff:ff:ff
Src 00:56:cd:ee:f1:71
BSS 84:b2:61:24:a2:00
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
🔢 Seq 2
🎯 TID 0
📊 Priority Best Effort (Best Effort) (0)
📦 Len 344
✅ Block Ack (0x0019)
📋 Policy Immediate Acknowledgement Required
📋 Type Compressed BlockAck
📊 Bitmap 0700000000000000
✅ Last ACK 3
💡 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