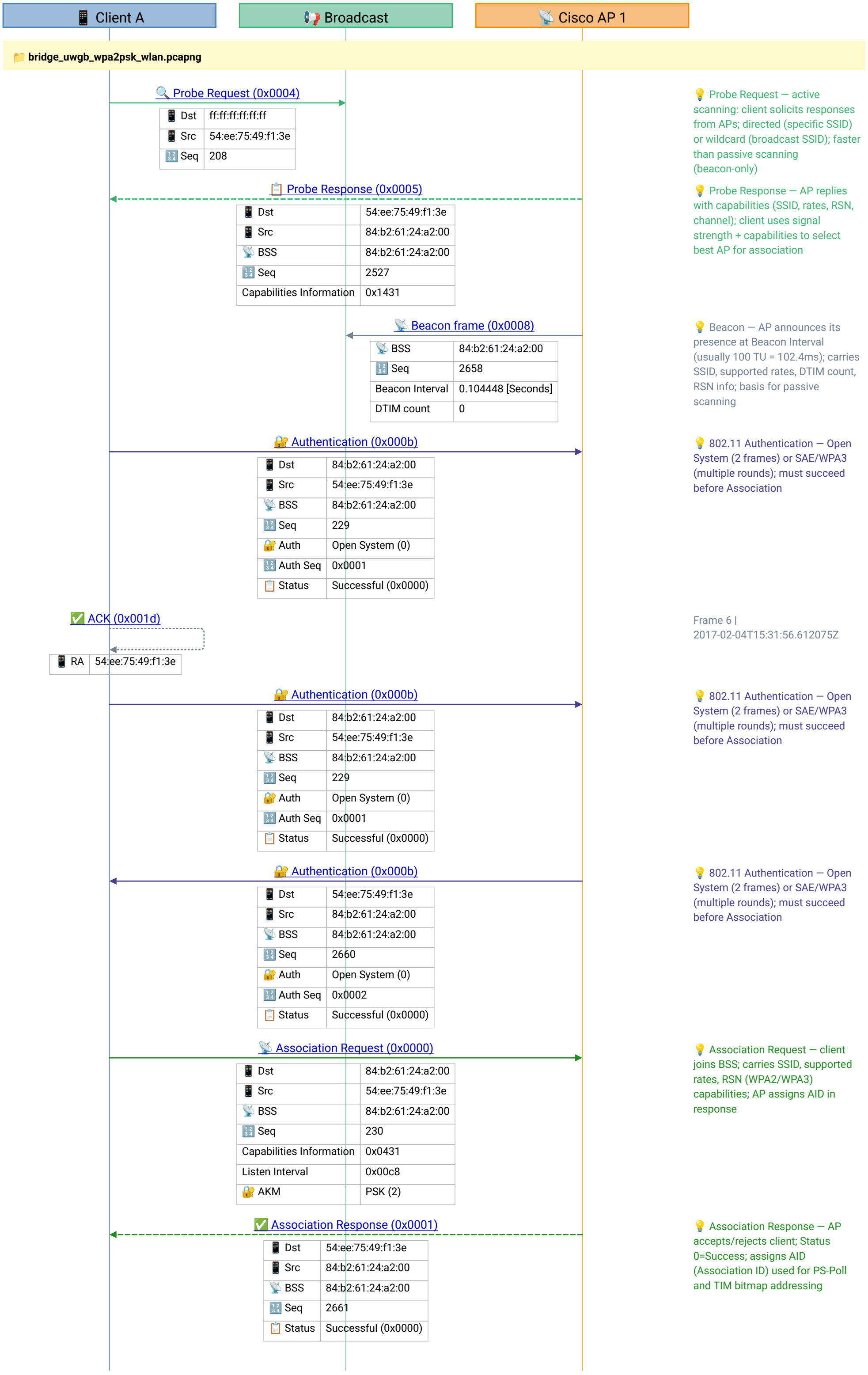
Client A
Broadcast
Cisco AP 1
bridge_uwgb_wpa2psk_wlan.pcapng
Probe Request (0x0004)
Dst ff:ff:ff:ff:ff:ff
Src 54:ee:75:49:f1:3e
Seq 208
Probe Request — active scanning: client solicits responses from APs; directed (specific SSID) or wildcard (broadcast SSID); faster than passive scanning (beacon-only)
Probe Response (0x0005)
Dst 54:ee:75:49:f1:3e
Src 84:b2:61:24:a2:00
BSS 84:b2:61:24:a2:00
Seq 2527
Capabilities Information 0x1431
Probe Response — AP replies with capabilities (SSID, rates, RSN, channel); client uses signal strength + capabilities to select best AP for association
Beacon frame (0x0008)
BSS 84:b2:61:24:a2:00
Seq 2658
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 84:b2:61:24:a2:00
Src 54:ee:75:49:f1:3e
BSS 84:b2:61:24:a2:00
Seq 229
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 54:ee:75:49:f1:3e
Frame 6 | 2017-02-04T15:31:56.612075Z
Authentication (0x000b)
Dst 84:b2:61:24:a2:00
Src 54:ee:75:49:f1:3e
BSS 84:b2:61:24:a2:00
Seq 229
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
Authentication (0x000b)
Dst 54:ee:75:49:f1:3e
Src 84:b2:61:24:a2:00
BSS 84:b2:61:24:a2:00
Seq 2660
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
Association Request (0x0000)
Dst 84:b2:61:24:a2:00
Src 54:ee:75:49:f1:3e
BSS 84:b2:61:24:a2:00
Seq 230
Capabilities Information 0x0431
Listen Interval 0x00c8
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 54:ee:75:49:f1:3e
Src 84:b2:61:24:a2:00
BSS 84:b2:61:24:a2:00
Seq 2661
Status Successful (0x0000)
Association Response — AP accepts/rejects client; Status 0=Success; assigns AID (Association ID) used for PS-Poll and TIM bitmap addressing

📱 Client A | 📢 Broadcast | 📡 Cisco AP 1

🆔 AID	0x0001

🔐 EAPOL Key

📱 Dst	54:ee:75:49:f1:3e
📱 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
WPA Key Nonce	6442d7b6bf4f711d39b1b701d2d93ee9f063c43b5e40f5029cec37c914ead2ae

💡 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 Key

📱 Dst	54:ee:75:49:f1:3e
📱 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
WPA Key Nonce	6442d7b6bf4f711d39b1b701d2d93ee9f063c43b5e40f5029cec37c914ead2ae

💡 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 Key

📱 Dst	84:b2:61:24:a2:00
📱 Src	54:ee:75:49:f1:3e
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	2
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x010a
Key Length	16
Replay Counter	0
WPA Key Nonce	b9fc2f4c75e7dceae78aa905891ebba63dd8f199eb89356f49704ac137639043

💡 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 Key

📱 Dst	54:ee:75:49:f1:3e
📱 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	6442d7b6bf4f711d39b1b701d2d93ee9f063c43b5e40f5029cec37c914ead2ae

💡 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	01:00:0c:cc:cc:cc
📱 Src	fc:99:47:be:c0:66
🔢 Seq	2386
🎯 TID	0
📊 Priority	Best Effort (Best Effort) (0)
📦 Len	386

💡 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)