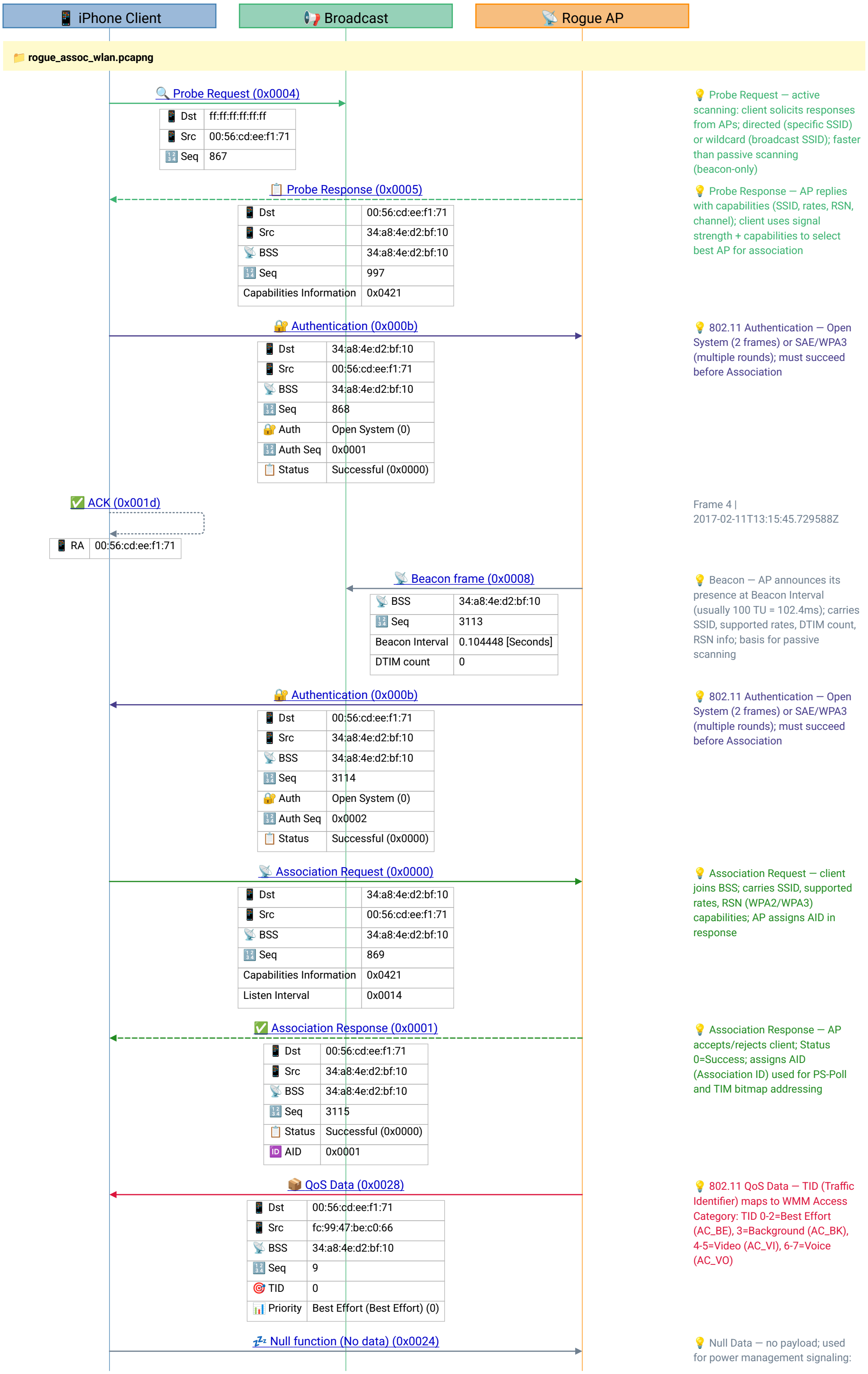
📱 iPhone Client
📢 Broadcast
📡 Rogue AP
📁 rogue_assoc_wlan.pcapng
🔍 Probe Request (0x0004)
📱 Dst ff:ff:ff:ff:ff:ff
📱 Src 00:56:cd:ee:f1:71
🔢 Seq 867
💡 Probe Request — active scanning: client solicits responses from APs; directed (specific SSID) or wildcard (broadcast SSID); faster than passive scanning (beacon-only)
📋 Probe Response (0x0005)
📱 Dst 00:56:cd:ee:f1:71
📱 Src 34:a8:4e:d2:bf:10
📡 BSS 34:a8:4e:d2:bf:10
🔢 Seq 997
Capabilities Information 0x0421
💡 Probe Response — AP replies with capabilities (SSID, rates, RSN, channel); client uses signal strength + capabilities to select best AP for association
🔐 Authentication (0x000b)
📱 Dst 34:a8:4e:d2:bf:10
📱 Src 00:56:cd:ee:f1:71
📡 BSS 34:a8:4e:d2:bf:10
🔢 Seq 868
🔐 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 | 2017-02-11T13:15:45.729588Z
📡 Beacon frame (0x0008)
📡 BSS 34:a8:4e:d2:bf:10
🔢 Seq 3113
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 34:a8:4e:d2:bf:10
📡 BSS 34:a8:4e:d2:bf:10
🔢 Seq 3114
🔐 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 34:a8:4e:d2:bf:10
📱 Src 00:56:cd:ee:f1:71
📡 BSS 34:a8:4e:d2:bf:10
🔢 Seq 869
Capabilities Information 0x0421
Listen Interval 0x0014
💡 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 34:a8:4e:d2:bf:10
📡 BSS 34:a8:4e:d2:bf:10
🔢 Seq 3115
📋 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
📦 QoS Data (0x0028)
📱 Dst 00:56:cd:ee:f1:71
📱 Src fc:99:47:be:c0:66
📡 BSS 34:a8:4e:d2:bf:10
🔢 Seq 9
🎯 TID 0
📊 Priority Best Effort (Best Effort) (0)
💡 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)
💤 Null function (No data) (0x0024)
💡 Null Data — no payload; used for power management signaling:

📱 iPhone Client | 📢 Broadcast | 📡 Rogue AP

💤 Power	STA will stay up
📱 Dst	34:a8:4e:d2:bf:10
📱 Src	00:56:cd:ee:f1:71
📡 BSS	34:a8:4e:d2:bf:10
🔢 Seq	870

PWR MGT=1 tells AP the client is going to sleep (AP buffers frames); PWR MGT=0 means client is awake