Exploring clientassoc_wep_wlan.pcapng

📱 iPhone Client | 📢 Broadcast | 📡 Cisco AP 1

📁 **clientassoc_wep_wlan.pcapng**

🔍 Probe Request (0x0004)

📱 Dst	ff:ff:ff:ff:ff:ff
📱 Src	00:56:cd:ee:f1:71
🔢 Seq	820

💡 Probe Request — active scanning: client solicits responses from APs; directed (specific SSID) or wildcard (broadcast SSID); faster than passive scanning (beacon-only)

📡 Beacon frame (0x0008)

📡 BSS	84:b2:61:24:a2:00
🔢 Seq	3577
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

📋 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	1211
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	821
🔐 Auth	Shared key (1)
🔢 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 5 | 2017-01-16T02:11:05.70929Z

🔐 Authentication (0x000b)

📱 Dst	00:56:cd:ee:f1:71
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	3578
🔐 Auth	Shared key (1)
🔢 Auth Seq	0x0002
📋 Status	Successful (0x0000)

💡 802.11 Authentication — Open System (2 frames) or SAE/WPA3 (multiple rounds); must succeed before 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	822
📦 Len	147

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

🔐 Authentication (0x000b)

📱 Dst	00:56:cd:ee:f1:71
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	3579
🔐 Auth	Shared key (1)
🔢 Auth Seq	0x0004
📋 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	00:56:cd:ee:f1:71
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	823
Capabilities Information	0x1431
Listen Interval	0x0014

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

✅ Association Response (0x0001)

💡 Association Response — AP accepts/rejects client; Status

📱 iPhone Client | 📢 Broadcast | 📡 Cisco AP 1

📱 Dst	00:56:cd:ee:f1:71
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	3580
📋 Status	Successful (0x0000)
🆔 AID	0x0001

0=Success; assigns AID (Association ID) used for PS-Poll and TIM bitmap addressing

💤 Null function (No data) (0x0024)

💤 Power	STA will stay up
📱 Dst	84:b2:61:24:a2:00
📱 Src	00:56:cd:ee:f1:71
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	824

💡 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

📦 QoS Data (0x0028)

📱 Dst	ff:ff:ff:ff:ff:ff
📱 Src	00:56:cd:ee:f1:71
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	0
🎯 TID	0
📊 Priority	Best Effort (Best Effort) (0)
📦 Len	336

💡 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)