Exploring clientassoc_wpapsk_fail_wlan.pcapng

📱 iPhone Client	📢 Broadcast	📡 Cisco AP 1	📱 Client AX	📱 Client AW

📁 **clientassoc_wpapsk_fail_wlan.pcapng**

🔍 Probe Request (0x0004)

📱 Dst	ff:ff:ff:ff:ff:ff
📱 Src	00:56:cd:ee:f1:71
🔢 Seq	2964

💡 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	1406
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	2965
🔐 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	2677
🔐 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

🔐 Authentication (0x000b)

📱 Dst	00:56:cd:ee:f1:71
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	2677
🔐 Auth	Open System (0)
🔢 Auth Seq	0x0002
📋 Status	Successful (0x0000)

Frame 4 | 2017-01-16T02:16:36.22017Z

✅ 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	2678
📋 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	3
Key Descriptor Type	EAPOL WPA Key (254)
Key Information	0x008a
Key Length	16
Replay Counter	0
WPA Key Nonce	7cfe6d07fa7cd85dc901776ad8addafe49e43c9d2e1cb65cbb676e1c1e9f12b7

💡 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)

Frame 9 | 2017-01-16T02:16:36.252451Z

📱 iPhone Client | 📢 Broadcast | 📡 Cisco AP 1 | 📱 Client AX | 📱 Client AW

📱 Dst	84:b2:61:24:a2:00
📱 Src	00:56:cd:ee:f1:71
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	2967
📋 Category	Block Ack (3)
📋 Action	Add Block Ack Request (0x00)

📦 QoS Data (0x0028)

📱 Dst	84:52:56:96:6e:8f
📱 Src	00:56:cd:ee:f1:71
📡 BSS	77:09:27:12:f0:01
🔢 Seq	2024
🎯 TID	8
📊 Priority	Best Effort (Best Effort) (0)
📦 Len	121

💡 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)

🔐 EAPOL Key

📱 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 WPA Key (254)
Key Information	0x010a
Key Length	16
Replay Counter	0
WPA Key Nonce	863cce1ec785c3d70f5f8507141e507b83dff080840410104042fdedf7b6bdb3

💡 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	00:56:cd:ee:f1:71
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	2679
📋 Category	Block Ack (3)
📋 Action	Add Block Ack Response (0x01)

Frame 14 | 2017-01-16T02:16:36.252802Z

✅ 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	ff01000000000000
✅ Last ACK	9

💡 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

📡 Beacon frame (0x0008)

📡 BSS	84:b2:61:24:a2:00
🔢 Seq	2680
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

🔐 EAPOL Key

📱 Dst	00:56:cd:ee:f1:71
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	4
Key Descriptor Type	EAPOL WPA Key (254)
Key Information	0x008a
Key Length	16
Replay Counter	1
WPA Key Nonce	7cfe6d07fa7cd85dc901776ad8addafe49e43c9d2e1cb65cbb676e1c1e9f12b7

💡 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

💡 EAPOL 4-Way Handshake — derives PTK from PMK; Msg 1: ANonce, Msg 2: SNonce+MIC, Msg 3: GTK, Msg 4: Confirm; completes

📱 iPhone Client | 📢 Broadcast | 📡 Cisco AP 1 | 📱 Client AX | 📱 Client AW

📱 Src	00:56:cd:ee:f1:71
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	1
Key Descriptor Type	EAPOL WPA Key (254)
Key Information	0x010a
Key Length	16
Replay Counter	1
WPA Key Nonce	9c8b722d9168ba5fd2fe6808bfbd0108f7be21077be1df0983dbe1207b7d2411

encryption key installation

📋 Probe Response (0x0005)

📱 Dst	72:6b:7e:59:d8:70
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	1407
Capabilities Information	0x1431

💡 Probe Response — AP replies with capabilities (SSID, rates, RSN, channel); client uses signal strength + capabilities to select best AP for association

📋 Probe Response (0x0005)

📱 Dst	72:6b:7e:59:d8:70
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	1407
Capabilities Information	0x1431

💡 Probe Response — AP replies with capabilities (SSID, rates, RSN, channel); client uses signal strength + capabilities to select best AP for association

📋 Probe Response (0x0005)

📱 Dst	72:6b:7e:59:d8:70
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	1407
Capabilities Information	0x1431

💡 Probe Response — AP replies with capabilities (SSID, rates, RSN, channel); client uses signal strength + capabilities to select best AP for association

🔐 EAPOL Key

📱 Dst	00:56:cd:ee:f1:71
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	5
Key Descriptor Type	EAPOL WPA Key (254)
Key Information	0x008a
Key Length	16
Replay Counter	2
WPA Key Nonce	7cfe6d07fa7cd85dc901776ad8addafe49e43c9d2e1cb65cbb676e1c1e9f12b7

💡 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	00:56:cd:ee:f1:71
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	2
Key Descriptor Type	EAPOL WPA Key (254)
Key Information	0x010a
Key Length	16
Replay Counter	2
WPA Key Nonce	cbd1a17785ddd114775c451beb905c838df1907683b50ed48958da9d2b1558ad

💡 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

🚫 Deauthentication (0x000c)

📱 Dst	00:56:cd:ee:f1:71
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	2709
📋 Reason	4-way handshake timeout (0x000f)

💡 Deauthentication — forces client to re-authenticate; reason codes: 1=Unspecified, 2=Auth expired, 3=Leaving, 4=Inactivity