📱 iPhone Client | 📢 Broadcast | 📡 Cisco AP 1 | 📱 Client J | 📡 Cisco AP 5

📁 **clientassoc_wpa2psk_fail_wlan.pcapng**

🔍 Probe Request (0x0004)

📱 Dst	ff:ff:ff:ff:ff:ff
📱 Src	00:56:cd:ee:f1:71
🔢 Seq	184

💡 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	1509
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	185
🔐 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 | 2017-01-16T02:19:15.64926Z

📡 Beacon frame (0x0008)

📡 BSS	84:b2:61:24:a2:00
🔢 Seq	125
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	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	126
🔐 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	00:56:cd:ee:f1:71
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	186
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	127
📋 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	8
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x008a

💡 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

📱 iPhone Client | 📢 Broadcast | 📡 Cisco AP 1 | 📱 Client J | 📡 Cisco AP 5

Key Length	16
Replay Counter	0
WPA Key Nonce	7cfe6d07fa7cd85dc901776ad8addafe49e43c9d2e1cb65cb b676e1c1e9f12b9

📋 Action (0x000d)

Frame 11 | 2017-01-16T02:19:15.690238Z

📱 Dst	84:b2:61:24:a2:00
📱 Src	00:56:cd:ee:f1:71
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	187
📋 Category	Block Ack (3)
📋 Action	Add Block Ack Request (0x00)

🔐 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	8ef388652195f35432ae6a8e55c5ae2f4742c5eed08b422ee e8d45cb2e5c72e6

📋 Action (0x000d)

Frame 15 | 2017-01-16T02:19:15.690534Z

📱 Dst	00:56:cd:ee:f1:71
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	128
📋 Category	Block Ack (3)
📋 Action	Add Block Ack Response (0x01)

✅ Block Ack Req (0x0018)

💡 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

📋 Policy	Immediate Acknowledgement Required
📋 Type	Compressed BlockAck

✅ Block Ack (0x0019)

💡 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

📋 Policy	Immediate Acknowledgement Required
📋 Type	Compressed BlockAck
📊 Bitmap	ff00000000000000
✅ Last ACK	8

📋 Probe Response (0x0005)

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

📱 Dst	c0:d9:62:33:fb:15
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	1510
Capabilities Information	0x1431

📋 Probe Response (0x0005)

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

📱 Dst	c0:d9:62:33:fb:15
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	1510
Capabilities Information	0x1431

📋 Probe Response (0x0005)

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

📱 Dst	c0:d9:62:33:fb:15
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	1510
Capabilities Information	0x1431

📋 Probe Response (0x0005)

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

📱 Dst	c0:d9:62:33:fb:15

📱 iPhone Client | 📢 Broadcast | 📡 Cisco AP 1 | 📱 Client J | 📡 Cisco AP 5

📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	1511
Capabilities Information	0x1431

best AP for association

📋 Probe Response (0x0005)

📱 Dst	c0:d9:62:33:fb:15
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	1511
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	c0:d9:62:33:fb:15
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	1511
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	9
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x008a
Key Length	16
Replay Counter	1
WPA Key Nonce	7cfe6d07fa7cd85dc901776ad8addafe49e43c9d2e1cb65cbb676e1c1e9f12b9

💡 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	1
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x010a
Key Length	16
Replay Counter	1
WPA Key Nonce	e0357f29f94fe53e6b0758383e39f8e5c7283946e519d736a327e6c164f993e7

💡 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	00:56:cd:ee:f1:71
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	10
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x008a
Key Length	16
Replay Counter	2
WPA Key Nonce	7cfe6d07fa7cd85dc901776ad8addafe49e43c9d2e1cb65cbb676e1c1e9f12b9

💡 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 RSN Key (2)
Key Information	0x010a
Key Length	16
Replay Counter	2
WPA Key Nonce	56194f32866fe643cde6c866bccd0cc9332499279b63db1f9380b1ff7005c015

💡 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

📋 Probe Response (0x0005)

💡 Probe Response — AP replies with capabilities (SSID, rates, RSN,

iPhone Client | Broadcast | Cisco AP 1 | Client J | Cisco AP 5

Dst	a4:08:ea:1e:0b:5b
Src	84:b2:61:24:a2:00
BSS	84:b2:61:24:a2:00
Seq	1512
Capabilities Information	0x1431

channel); client uses signal strength + capabilities to select best AP for association

Probe Response (0x0005)

Dst	a4:08:ea:1e:0b:5b
Src	84:b2:61:24:a2:00
BSS	84:b2:61:24:a2:00
Seq	1512
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	a4:08:ea:1e:0b:5b
Src	84:b2:61:24:a2:00
BSS	84:b2:61:24:a2:00
Seq	1512
Capabilities Information	0x1431

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

Deauthentication (0x000c)

Dst	00:56:cd:ee:f1:71
Src	84:b2:61:24:a2:00
BSS	84:b2:61:24:a2:00
Seq	159
Reason	4-way handshake timeout (0x000f)

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