📱 iPhone Client | 📢 Broadcast | 📡 Cisco AP 1

📁 **clientassoc_wpapsk_wlan.pcapng**

🔍 Probe Request (0x0004)

📱 Dst	ff:ff:ff:ff:ff:ff
📱 Src	00:56:cd:ee:f1:71
🔢 Seq	1870

💡 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	1811
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	00:56:cd:ee:f1:71
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	1871
🔐 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 | 2017-01-16T02:15:06.873918Z

🔐 Authentication (0x000b)

📱 Dst	84:b2:61:24:a2:00
📱 Src	00:56:cd:ee:f1:71
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	1871
🔐 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

📋 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	1359
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	00:56:cd:ee:f1:71
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	1812
🔐 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	1872
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)

📱 Dst	00:56:cd:ee:f1:71
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	1813
📋 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

📱 iPhone Client	📢 Broadcast	📡 Cisco AP 1

🔐 EAPOL Key

📱 Dst	00:56:cd:ee:f1:71
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	0
Key Descriptor Type	EAPOL WPA Key (254)
Key Information	0x008a
Key Length	16
Replay Counter	0
WPA Key Nonce	7cfe6d07fa7cd85dc901776ad8addafe49e43c9d2e1cb65cbb676e1c1e9f12b6

💡 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	0
Key Descriptor Type	EAPOL WPA Key (254)
Key Information	0x008a
Key Length	16
Replay Counter	0
WPA Key Nonce	7cfe6d07fa7cd85dc901776ad8addafe49e43c9d2e1cb65cbb676e1c1e9f12b6

💡 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	84:b2:61:24:a2:00
📱 Src	00:56:cd:ee:f1:71
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	1873
📋 Category	Block Ack (3)
📋 Action	Add Block Ack Request (0x00)

Frame 14 | 2017-01-16T02:15:06.949613Z

📋 Action (0x000d)

📱 Dst	00:56:cd:ee:f1:71
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	1814
📋 Category	Block Ack (3)
📋 Action	Add Block Ack Response (0x01)

Frame 16 | 2017-01-16T02:15:06.949657Z

🔐 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	c947251dd7175c5fe2f9e830a0c3f9e61866c331198e663a31d7c75e3af1d78a

💡 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

✅ 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	0000000000000000
✅ Last ACK	1

💡 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

🔐 EAPOL Key

📱 Dst	00:56:cd:ee:f1:71
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	1
Key Descriptor Type	EAPOL WPA Key (254)

💡 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

Key Information	0x01ca
Key Length	16
Replay Counter	1
WPA Key Nonce	7cfe6d07fa7cd85dc901776ad8addafe49e43c9d2e1cb65cbb676e1c1e9f12b6

🔐 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 WPA Key (254)
Key Information	0x010a
Key Length	16
Replay Counter	1
WPA Key Nonce	0000000000000000000000000000000000000000000000000000000000000000

💡 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	00:56:cd:ee:f1:71
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	2
🎯 TID	7
📊 Priority	Network Control (Voice) (7)
📦 Len	139

💡 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)

📦 QoS Data (0x0028)

📱 Dst	84:b2:61:24:a2:00
📱 Src	00:56:cd:ee:f1:71
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	2
🎯 TID	0
📊 Priority	Best Effort (Best Effort) (0)
📦 Len	115

💡 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)

📋 Action (0x000d)

📱 Dst	00:56:cd:ee:f1:71
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	1816
📋 Category	Block Ack (3)
📋 Action	Add Block Ack Request (0x00)

Frame 30 | 2017-01-16T02:15:07.039576Z

📋 Action (0x000d)

📱 Dst	84:b2:61:24:a2:00
📱 Src	00:56:cd:ee:f1:71
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	1874
📋 Category	Block Ack (3)
📋 Action	Add Block Ack Response (0x01)

Frame 32 | 2017-01-16T02:15:07.03997Z