📡 Cisco AP 1	📢 Broadcast	📱 iPhone Client

📁 **dot11w_pmf_wlan.pcapng**

📡 Beacon frame (0x0008)

📡 BSS	84:b2:61:24:a2:00
🔢 Seq	2467
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	2127
🔐 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)

Frame 3 | 2017-02-04T16:42:19.710223Z

📱 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	2468
🔐 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	2128
Capabilities Information	0x1431
Listen Interval	0x0014
🔐 AKM	PSK (SHA256) (6)

💡 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	2469
📋 Status	Successful (0x0000)
🆔 AID	0x0002

💡 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	21
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x008b
Key Length	16
Replay Counter	0
WPA Key Nonce	64a435e4ff860b9ac3252cdb2ebd5a8805bf7722a24f264177fec9b8ab059248

💡 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	2129
📋 Category	Block Ack (3)
📋 Action	Add Block Ack Request (0x00)

Frame 9 | 2017-02-04T16:42:19.737738Z

📡 Cisco AP 1 | 📢 Broadcast | 📱 iPhone Client

🔐 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 RSN Key (2)
Key Information	0x010b
Key Length	16
Replay Counter	0
WPA Key Nonce	00e50729e3591acbd658a69e34f4d3d09e83f41dd0777c41f1068836df267c9b

💡 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	2470
📋 Category	Block Ack (3)
📋 Action	Add Block Ack Response (0x01)

Frame 13 | 2017-02-04T16:42:19.737983Z

✅ Block Ack Req (0x0018)

📋 Policy	Immediate Acknowledgement Required
📋 Type	Compressed BlockAck

✅ 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

💡 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	22
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x13cb
Key Length	16
Replay Counter	1
WPA Key Nonce	64a435e4ff860b9ac3252cdb2ebd5a8805bf7722a24f264177fec9b8ab059248

💡 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	0x030b
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

🔍 Probe Request (0x0004)

📱 Dst	ff:ff:ff:ff:ff:ff
📱 Src	00:56:cd:ee:f1:71
🔢 Seq	2413

💡 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	2891
Capabilities Information	0x1431

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

📡 Disassociate

📱 Dst	00:56:cd:ee:f1:71

Frame 22 | 2017-02-04T16:42:34.638524Z

📡 Cisco AP 1	📢 Broadcast	📱 iPhone Client
	📱 Src 84:b2:61:24:a2:00 📡 BSS 84:b2:61:24:a2:00	