Exploring roam_interL2_wpa2psk_wired.pcapng

⚫ Null MAC | 📱 Client C | 📡 AP wired G | 📡 AP wired I | 📱 iPhone Client

📁 **roam_interL2_wpa2psk_wired.pcapng**

🔍 Probe Request (0x0004)

📱 Dst	f8:c2:88:07:58:80
📱 Src	00:00:00:00:00:00
🔢 Seq	0

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

Frame 3 | 2017-02-25T15:20:58.772222Z

🔒 DTLS Application Data (23)

📋 Version	DTLS 1.0 (0xfeff)
🔢 Epoch	1
📦 Length	64

🔒 DTLS Application Data (23)

📋 Version	DTLS 1.0 (0xfeff)
🔢 Epoch	1
📦 Length	80

Frame 4 | 2017-02-25T15:20:58.772797Z

🔄 Reassociation Request (0x0002)

📱 Dst	f8:c2:88:07:58:80
📱 Src	00:56:cd:ee:f1:71
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	16
📡 Current AP	00:d7:8f:d3:53:d0

💡 Reassociation Request — client roams to new AP within same ESS; carries Current AP MAC so new AP can request PMK from old AP (fast roaming) or via RADIUS

✅ Reassociation Response (0x0003)

📱 Dst	00:56:cd:ee:f1:71
📱 Src	f8:c2:88:07:58:80
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	0
📋 Status	Successful (0x0000)
🆔 AID	0x01c0

💡 Reassociation Response — new AP accepts roaming client; AID may change; PMK transfer via OKC, 802.11r FT, or CCKM enables fast secure roaming without full re-auth

🔐 EAPOL Key

📱 Dst	00:56:cd:ee:f1:71
📱 Src	f8:c2:88:07:58:80
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	0
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x008a
Key Length	16
Replay Counter	0
WPA Key Nonce	5fdef386daea32efe5d9047b1562237a961140038392be7904cb7790194f19dd

💡 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	f8:c2:88:07:58:80
📱 Src	00:56:cd:ee:f1:71
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	16
📋 Category	Radio Measurement (5)
📋 Action	Neighbor Report Request (4)

Frame 10 | 2017-02-25T15:20:59.421613Z

📋 Action (0x000d)

📱 Dst	00:56:cd:ee:f1:71
📱 Src	f8:c2:88:07:58:80
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	0
📋 Category	Radio Measurement (5)
📋 Action	Neighbor Report Response (5)

Frame 11 | 2017-02-25T15:20:59.42215Z

🔐 EAPOL Key

📱 Dst	f8:c2:88:07:58:80
📱 Src	00:56:cd:ee:f1:71
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	0
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x010a

💡 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

⚫ Null MAC | 📱 Client C | 📡 AP wired G | 📡 AP wired I | 📱 iPhone Client

Key Length	16
Replay Counter	0
WPA Key Nonce	d2899448aede76f62427213809c6271bc722e375e455dd52754baa5ca9714b8e

🔐 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	00:56:cd:ee:f1:71
📱 Src	f8:c2:88:07:58:80
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	0
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x13ca
Key Length	16
Replay Counter	1
WPA Key Nonce	5fdef386daea32efe5d9047b1562237a961140038392be7904cb7790194f19dd

🔐 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	f8:c2:88:07:58:80
📱 Src	00:56:cd:ee:f1:71
📡 BSS	f8:c2:88:07:58:80
🔢 Seq	256
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x030a
Key Length	16
Replay Counter	1
WPA Key Nonce	0000000000000000000000000000000000000000000000000000000000000000