



roam_interL3_wpa2psk_wired.pcapng

Probe Request (0x0004)

Dst	84:b2:61:24:a2:00
Src	00:00:00:00:00:00
Seq	0

Reassociation Request (0x0002)

Dst	84:b2:61:24:a2:00
Src	00:56:cd:ee:f1:71
BSS	84:b2:61:24:a2:00
Seq	16
Current AP	84:b2:61:3f:93:10

Reassociation Response (0x0003)

Dst	00:56:cd:ee:f1:71
Src	84:b2:61:24:a2:00
BSS	84:b2:61:24:a2:00
Seq	0
Status	Successful (0x0000)
AID	0x01c0

DTLS Application Data (23)

Version	DTLS 1.0 (0xfeff)
Epoch	1
Length	480

DTLS Application Data (23)

Version	DTLS 1.0 (0xfeff)
Epoch	1
Length	80

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 RSN Key (2)
Key Information	0x008a

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

💡 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 – 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

Frame 4 | 2017-01-28T14:29:16.180422Z

Frame 5 | 2017-01-28T14:29:16.181677Z

💡 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

Cisco AP 1

iPhone Client

AP wired A

AP wired B

IPv4 Multicast

IPv6 All Nodes

WLC E

WLC F

Key Length	16
Replay Counter	0
WPA Key Nonce	43614baf30cbfcb1ee472bc 49c9df4756291136ed33eab e33fb7a1f39dbb8be7

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	0x010a
Key Length	16
Replay Counter	0
WPA Key Nonce	0d3469a54d2c34b3a59d2c e8b3a19d0917b05ec109f62 7d83ec009ffd8033fe5

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 RSN Key (2)
Key Information	0x13ca
Key Length	16
Replay Counter	1
WPA Key Nonce	43614baf30cbfcb1ee472bc 49c9df4756291136ed33eab e33fb7a1f39dbb8be7

EAPOL Key

Dst	84:b2:61:24:a2:00
Src	00:56:cd:ee:f1:71
BSS	84:b2:61:24:a2:00
Seq	256
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x030a
Key Length	16
Replay Counter	1

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 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 4-Way Handshake – derives PTK from PMK; Msg 1: ANonce, Msg 2: SNonce+MIC, Msg 3: GTK, Msg 4: Confirm; completes encryption key installation

