

Null MAC | Cisco AP 1 | AP wired B | AP wired A | Client B

bridge_wgb_wpa2psk_wired.pcapng

Probe Request (0x0004)

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

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

Probe Request (0x0004)

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

Probe Request (0x0004)

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

Association Request (0x0000)

Dst	84:b2:61:24:a2:00
Src	fc:99:47:be:c0:66
BSS	84:b2:61:24:a2:00
Seq	16
Capabilities Information	0x3104
Listen Interval	0xc800
AKM	PSK (2)

Association Response (0x0001)

Dst	fc:99:47:be:c0:66
Src	84:b2:61:24:a2:00
BSS	84:b2:61:24:a2:00
Seq	0
Status	Successful (0x0000)
AID	0x02c0

EAPOL Key

Dst	fc:99:47:be:c0:66
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
Key Length	16
Replay Counter	0
WPA Key Nonce	6442d7b6bf4f711d39b1b701d2d93ee9f063c43b5e40f5029cec37c914ead2b3

EAPOL Key

Dst	84:b2:61:24:a2:00
Src	fc:99:47:be:c0:66
BSS	84:b2:61:24:a2:00
Seq	3072
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x010a
Key Length	16
Replay Counter	0
WPA Key Nonce	f0e42b70972656232d16d701f821de23fd151d3bd13812be8c7f12a64cf2c306

EAPOL Key

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

Frame 2 | 2017-02-04T15:44:25.845496Z

Frame 3 | 2017-02-04T15:44:25.845646Z

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

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

Association Request – client joins BSS; carries SSID, supported rates, RSN (WPA2/WPA3) capabilities; AP assigns AID in response

Association Response – AP accepts/rejects client; Status 0=Success; assigns AID (Association ID) used for PS-Poll and TIM bitmap addressing

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:

Null MAC | Cisco AP 1 | AP wired B | AP wired A | Client B

Dst	fc:99:47:be:c0:66
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	6442d7b6bf4f711d39b1b701d2d93ee9f063c43b5e40f5029cec37c914ead2b3

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	fc:99:47:be:c0:66
BSS	84:b2:61:24:a2:00
Seq	3328
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x030a
Key Length	16
Replay Counter	1
WPA Key Nonce	00

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

Data (0x0020)

Dst	84:b2:61:24:a2:00
Src	fc:99:47:be:c0:66
BSS	84:b2:61:24:a2:00
Seq	525

Frame 29 | 2017-02-04T15:44:28.923331Z