

Client B

Broadcast

Cisco AP 1

Client BD

bridge_wgb_cckm_peap_wlan.pcapng

Probe Request (0x0004)

Dst	ff:ff:ff:ff:ff:ff
Src	fc:99:47:be:c0:66
Seq	230

Probe Response (0x0005)

Dst	fc:99:47:be:c0:66
Src	84:b2:61:24:a2:00
BSS	84:b2:61:24:a2:00
Seq	3292
Capabilities Information	0x1431

Beacon frame (0x0008)

BSS	84:b2:61:24:a2:00
Seq	1606
Beacon Interval	0.104448 [Seconds]
DTIM count	0

Authentication (0x000b)

Dst	84:b2:61:24:a2:00
Src	fc:99:47:be:c0:66
BSS	84:b2:61:24:a2:00
Seq	251
Auth	Open System (0)
Auth Seq	0x0001
Status	Successful (0x0000)

ACK (0x001d)

RA	fc:99:47:be:c0:66
----	-------------------

Authentication (0x000b)

Dst	fc:99:47:be:c0:66
Src	84:b2:61:24:a2:00
BSS	84:b2:61:24:a2:00
Seq	1608
Auth	Open System (0)
Auth Seq	0x0002
Status	Successful (0x0000)

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	252
Capabilities Information	0x0431
Listen Interval	0x00c8
AKM	0

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	1609
Status	Successful (0x0000)
AID	0x0001

QoS Data (0x0028)

Dst	fc:99:47:be:c0:66
Src	84:b2:61:24:a2:00
BSS	84:b2:61:24:a2:00
Seq	81

- [Frame 1] Probe Request – active scanning: client solicits responses from APs; directed (specific SSID) or wildcard (broadcast SSID); faster than passive scanning (beacon-only)
- [Frame 2] Probe Response – AP replies with capabilities (SSID, rates, RSN, channel); client uses signal strength + capabilities to select best AP for association
- [Frame 3] 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
- [Frame 5] 802.11 Authentication – Open System (2 frames) or SAE/WPA3 (multiple rounds); must succeed before Association
- Frame 6 | 2017-02-05T13:45:49.031354Z
- [Frame 7] 802.11 Authentication – Open System (2 frames) or SAE/WPA3 (multiple rounds); must succeed before Association
- [Frame 8] Association Request – client joins BSS; carries SSID, supported rates, RSN (WPA2/WPA3) capabilities; AP assigns AID in response
- [Frame 10] Association Response – AP accepts/rejects client; Status 0=Success; assigns AID (Association ID) used for PS-Poll and TIM bitmap addressing
- [Frame 11] 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)

