Exploring bridge_wgb_wpa2psk_wlan.pcapng

📡 Cisco AP 1	📱 Client B	📢 Broadcast

📁 **bridge_wgb_wpa2psk_wlan.pcapng**

📋 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	2940
Capabilities Information	0x1431

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

📡 Beacon frame (0x0008)

📡 BSS	84:b2:61:24:a2:00
🔢 Seq	1725
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	fc:99:47:be:c0:66
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	774
🔐 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)

📱 RA	fc:99:47:be:c0:66

Frame 5 | 2017-02-04T15:44:29.310682Z

🔐 Authentication (0x000b)

📱 Dst	fc:99:47:be:c0:66
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	1727
🔐 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	fc:99:47:be:c0:66
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	775
Capabilities Information	0x0431
Listen Interval	0x00c8
🔐 AKM	PSK (2)

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

✅ 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	1728
📋 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	fc:99:47:be:c0:66
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	8
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x008a
Key Length	16
Replay Counter	0
WPA Key Nonce	6442d7b6bf4f711d39b1b701d2d93ee9f063c43b5e40f5029cec37c914ead2b3

💡 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

💡 EAPOL 4-Way Handshake — derives PTK from PMK; Msg 1:

📡 Cisco AP 1	📱 Client B	📢 Broadcast

📱 Dst	fc:99:47:be:c0:66
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	8
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x008a
Key Length	16
Replay Counter	0
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	12
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x010a
Key Length	16
Replay Counter	0
WPA Key Nonce	f0e42b70972656232d16d701f821de23fd151d3bd13812be8c7f12a64cf2c306

💡 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	fc:99:47:be:c0:66
📱 Src	84:b2:61:24:a2:00
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	9
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x13ca
Key Length	16
Replay Counter	1
WPA Key Nonce	6442d7b6bf4f711d39b1b701d2d93ee9f063c43b5e40f5029cec37c914ead2b3

💡 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	fc:99:47:be:c0:66
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	13
Key Descriptor Type	EAPOL RSN Key (2)
Key Information	0x030a
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

🔐 EAPOL Key ←

📱 Dst	84:b2:61:24:a2:00
📱 Src	fc:99:47:be:c0:66
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	13
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

📡 Cisco AP 1	📱 Client B	📢 Broadcast

WPA Key Nonce	0000000000000000000000000000000000000000000000000000000000000000

📦 QoS Data (0x0028)

📱 Dst	84:b2:61:24:a2:00
📱 Src	fc:99:47:be:c0:66
📡 BSS	84:b2:61:24:a2:00
🔢 Seq	3394
🎯 TID	0
📊 Priority	Best Effort (Best Effort) (0)
📦 Len	92

💡 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)