SharkFest '17 Europe

Troubleshooting WLANs (Part 2)

Troubleshooting WLANs using 802.11 Management & Control Frames

8. November 2017

Breaking News: Including KRACK !!!

Rolf Leutert

Leutert NetServices

Switzerland

www.netsniffing.ch

Rolf Leutert, El. Ing. HTL
Leutert NetServices
Zürich-Airport, Switzerland

- Network Analysis & Troubleshooting
- Protocol Trainings TCP/IP, WLAN, VoIP, IPv6
- Wireshark® Certified Network Analyst 2010
- Wireshark® Instructor since 2006
- Sniffer® certified Instructor since 1990

leutert@netsniffing.ch
www.netsniffing.ch

- Learn why analyzing WiFi layer 2 is a demanding task
- Learn that WiFi frames looks very different from Ethernet
- Learn why WiFi frames have one to four address fields
- Learn how critical processes e.g. Joining, Roaming works
- Learn how to read Wireshark files to isolate WiFi problems

Troubleshooting WiFi requires a full understanding of all 802.11 Management & Control frames and its associated processes!

802.11Frame Types Overview

Management Frames:

- Beacon
- Probe Request & Response
- Authentication & Deauthentication
- Association & Disassociation
- Reassociation Request & Response
- Action

Control Frames:

- Request to Send (RTS)
- Clear to Send (CTS)
- Acknowledge / Block Acknowledge Request / Block Acknowledge
- Power Save Poll

Data Frames:

- Data
- Null Function

- Four different frame formats are used

Acknowledge, Clear to Send

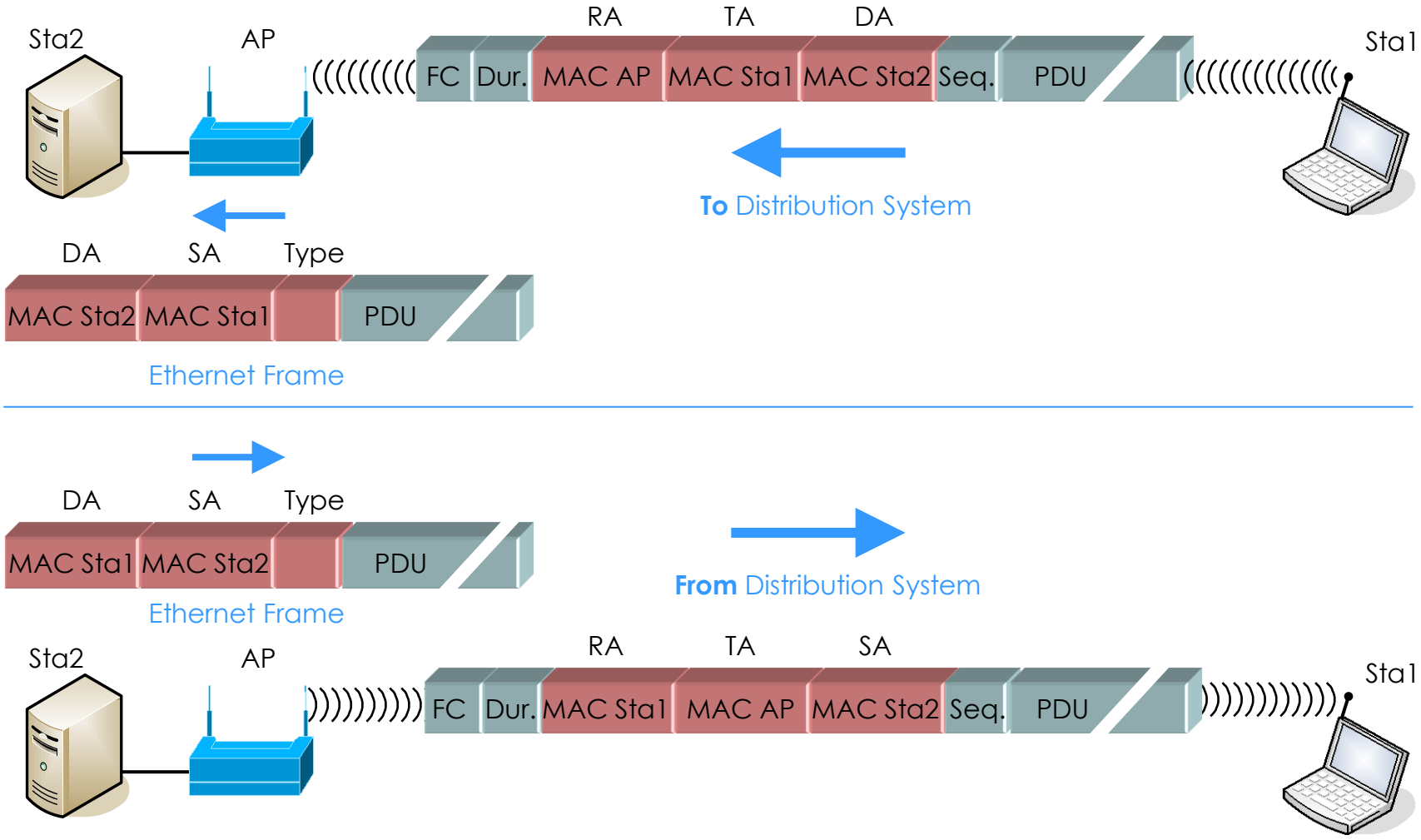
Request to Send

Data Frame, Beacon,
Probe Request, Probe Response,
Authentication, Deauthentication,
Association, Reassociation,
Disassociation

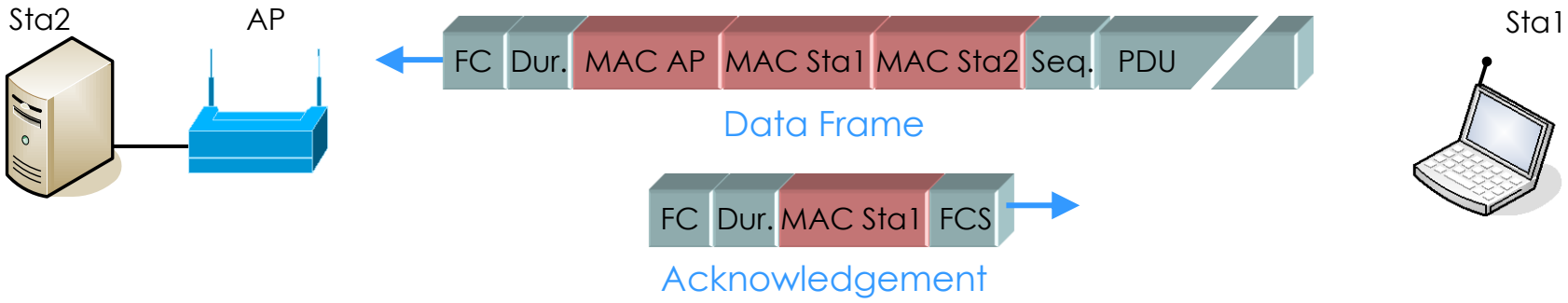
Data Frame through repeater

Field names: FC = Frame Control, Dur. = Duration, RA = Receiver MAC Address,
TA = Transmitter MAC Address; DA = Destination MAC Address,
SA = Source MAC Address, Seq. = Sequence, PDU = Protocol Data Unit,
FC = Frame Check Sequence

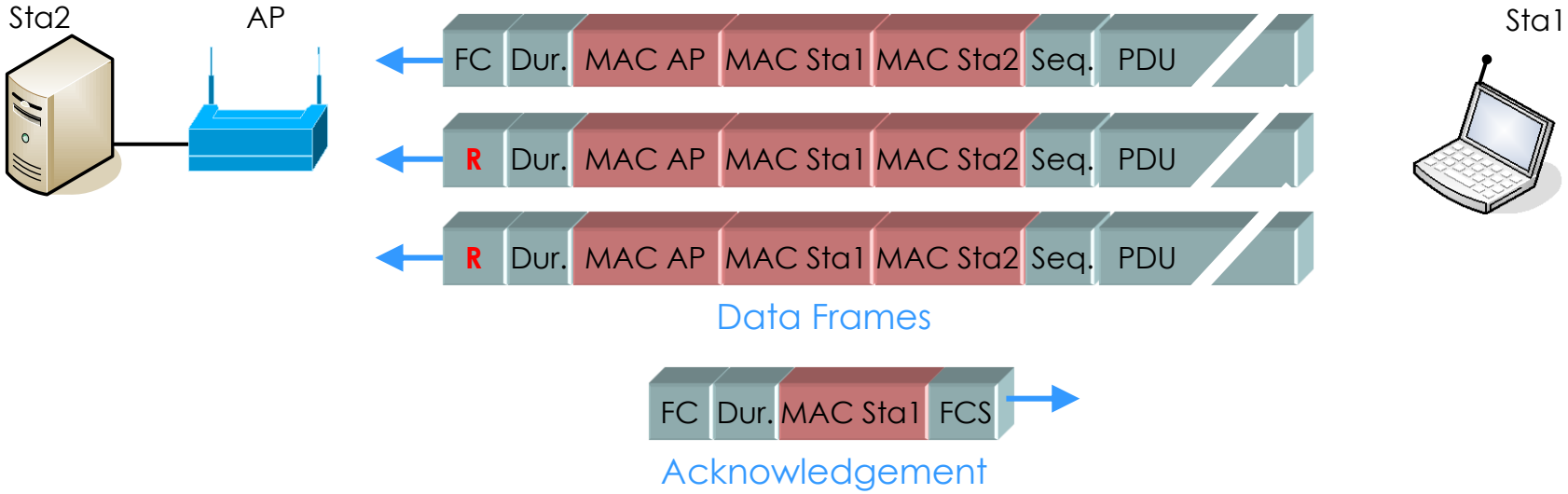
WiFi data frames have three MAC address field



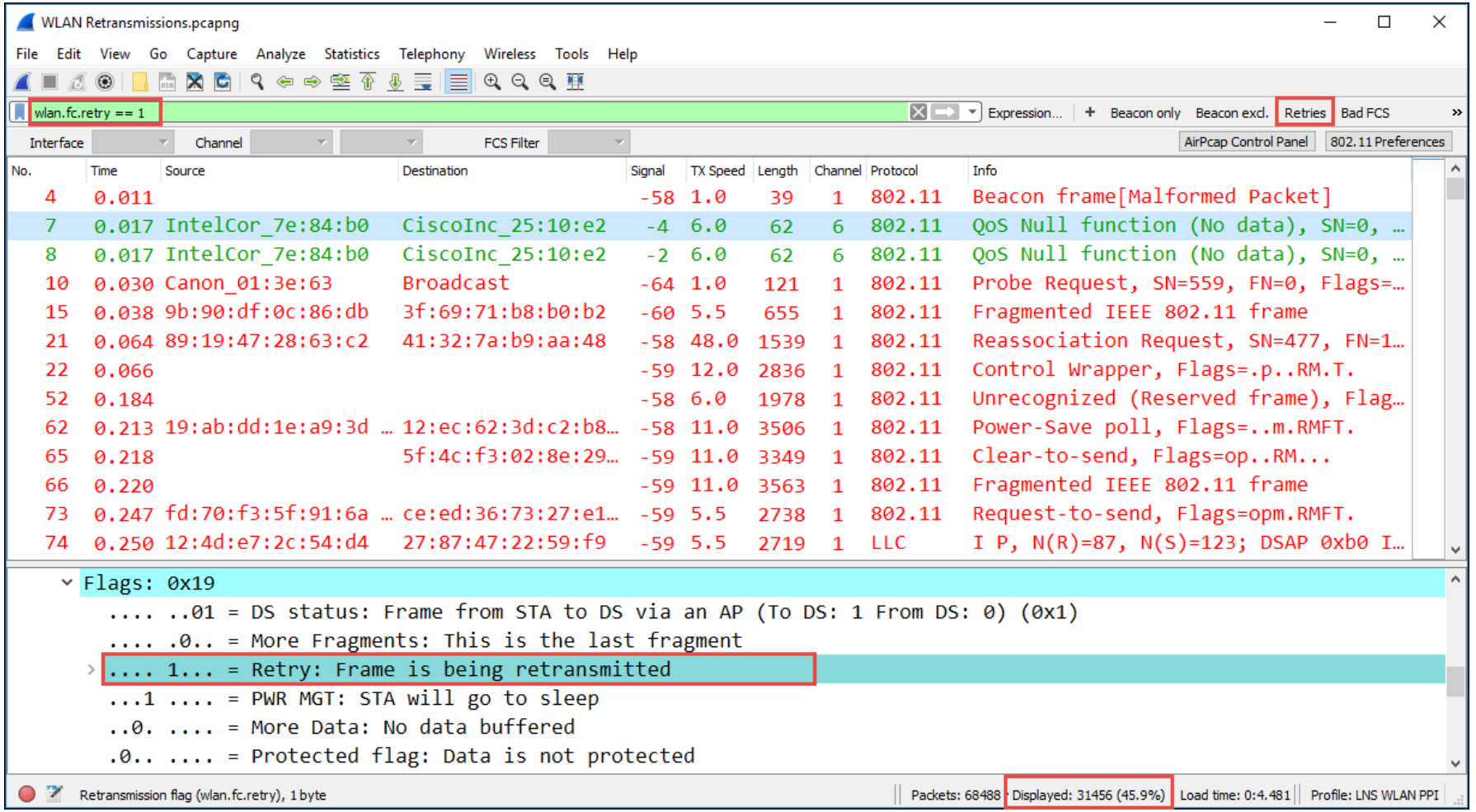
- WiFi data frames are acknowledged or retransmitted



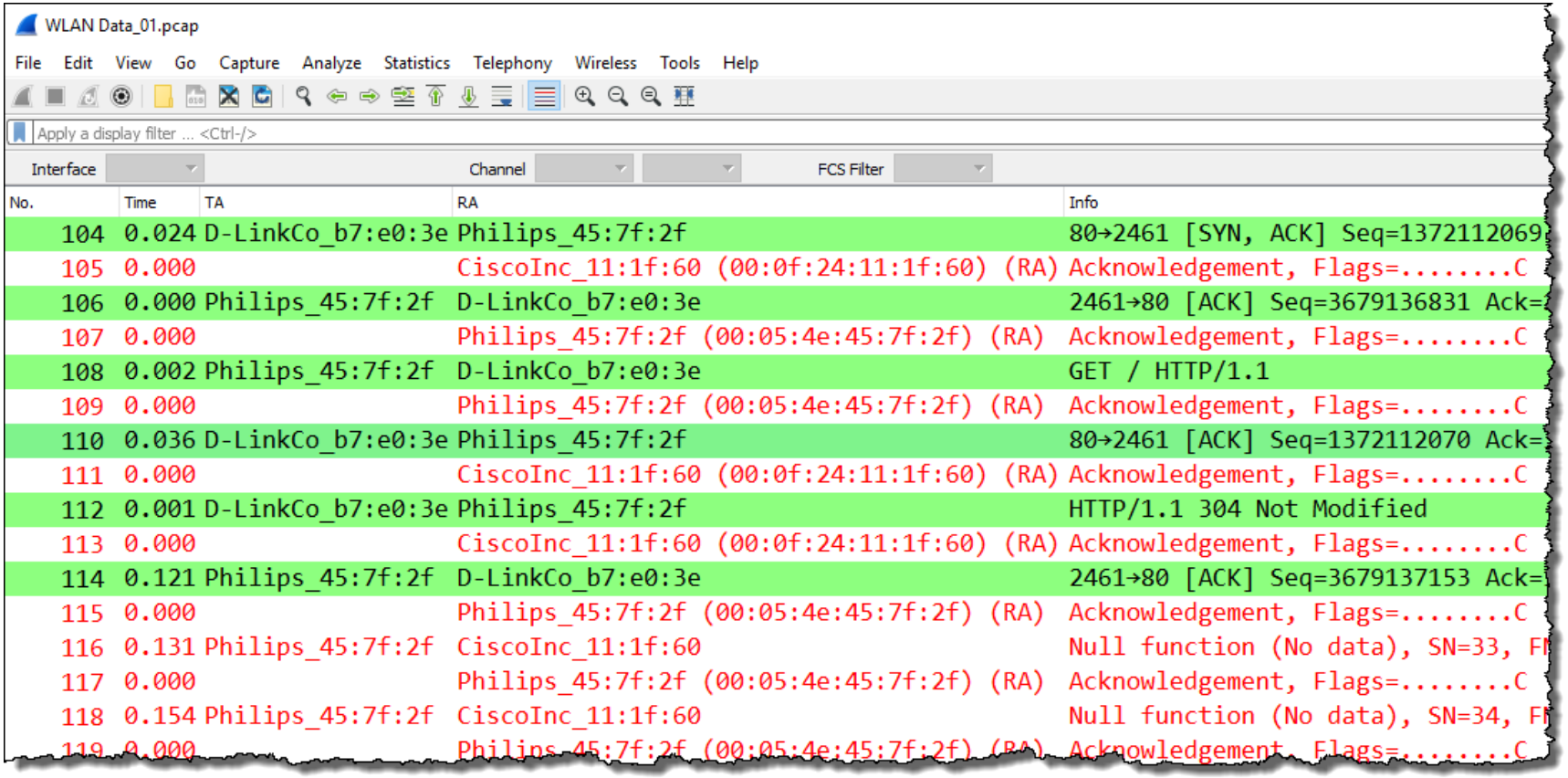
- All retransmitted frames are marked with the Retry Bit



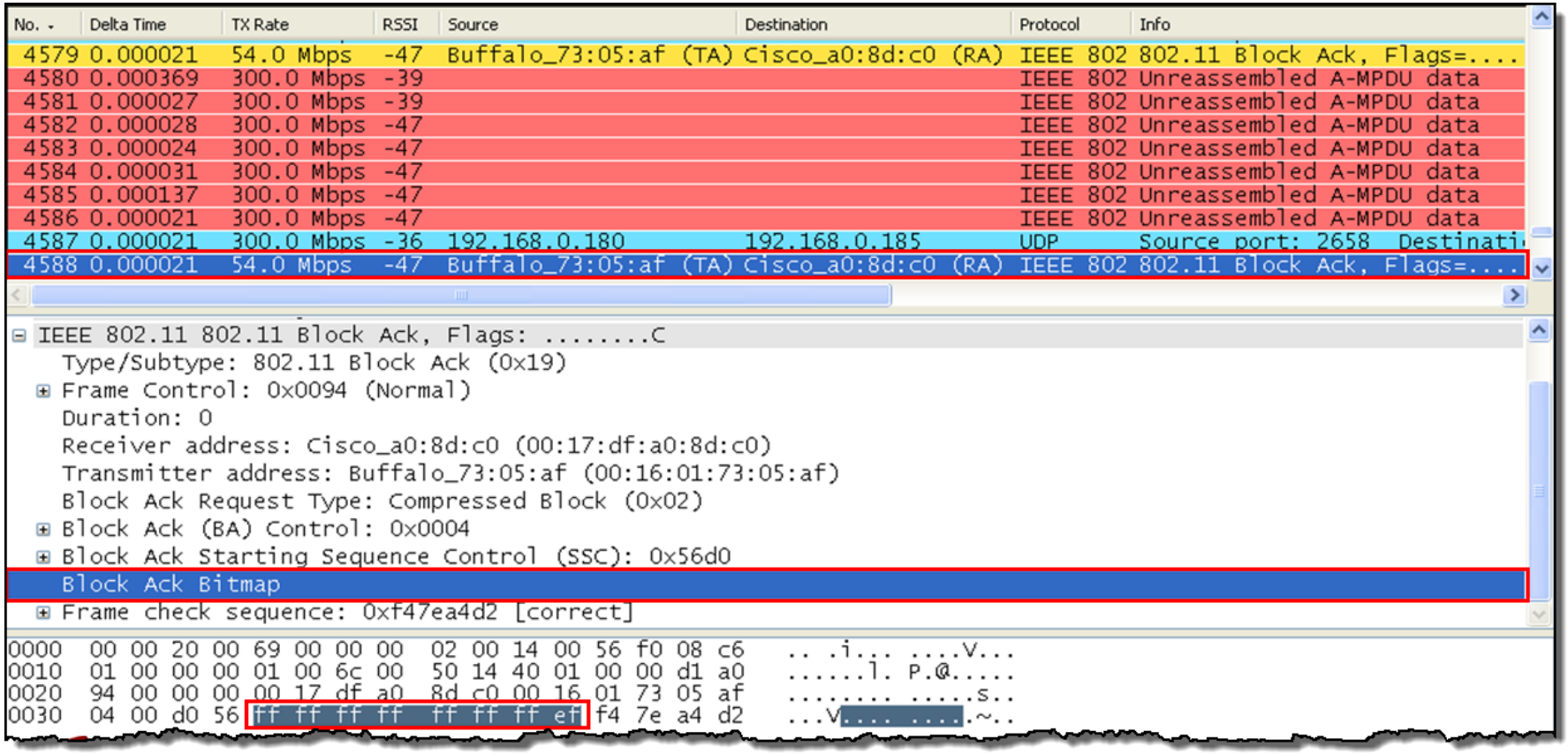
All retransmitted frames are marked with the Retry Bit



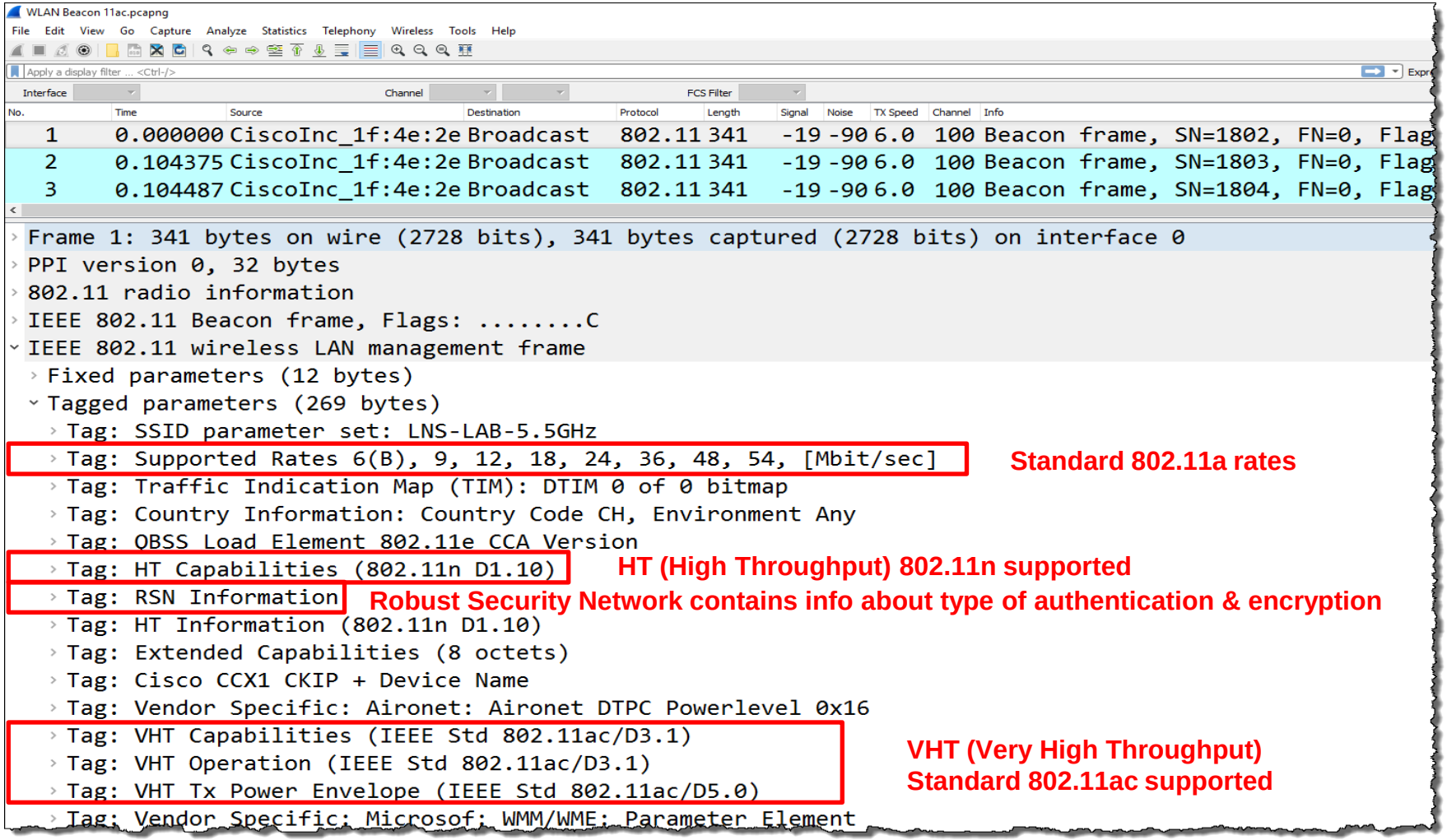
- In non-aggregation mode each packet is acknowledged individually
- The acknowledge frame follows immediately after each data frame
- The (single) acknowledge has no source address field



- 802.11n introduced aggregation mode with a Block Acknowledge (BA)
- In A-MPDU mode up to 64 frames can be acknowledged with one BA

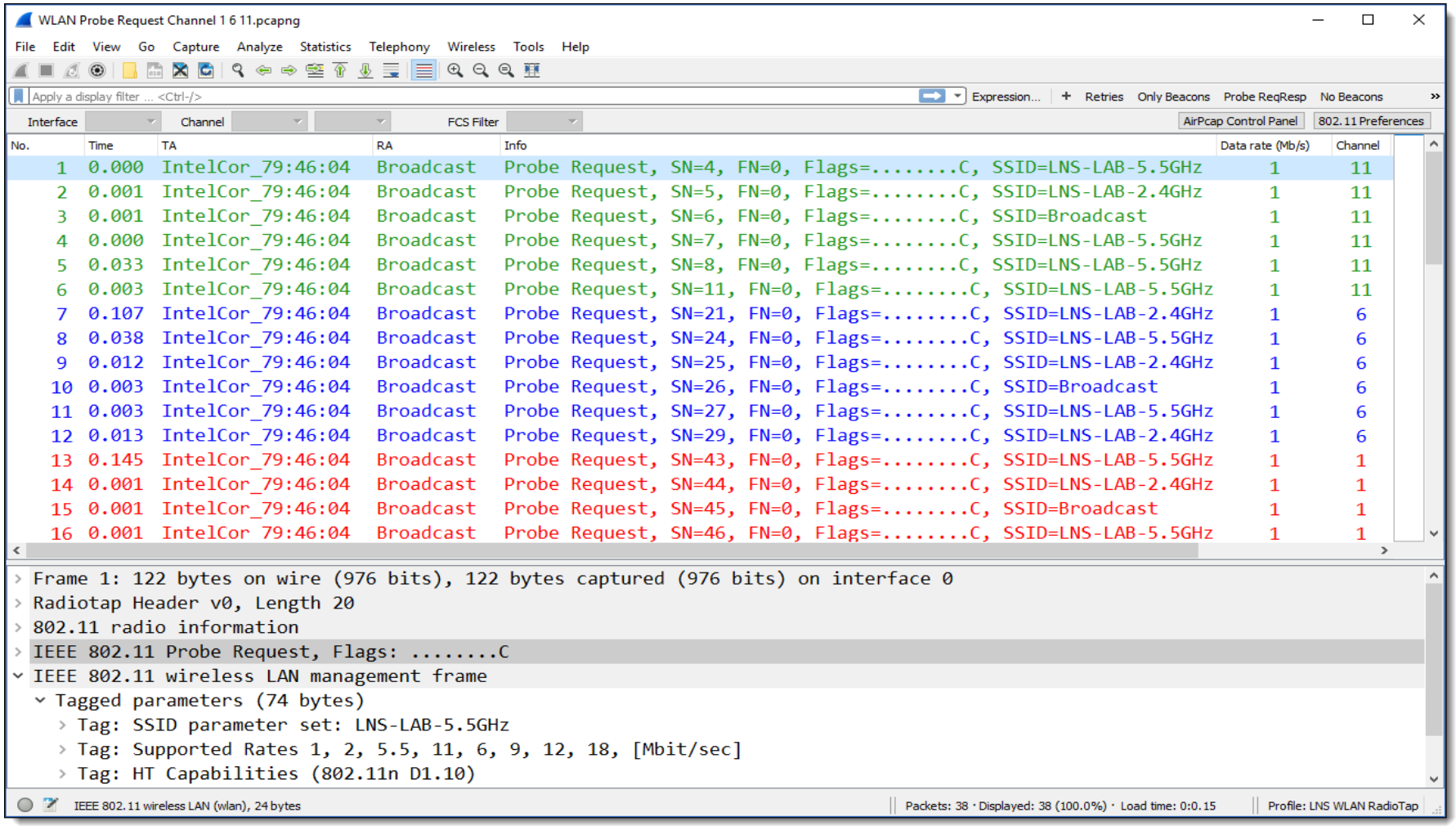


- Beacon tags contain information about supported and required features



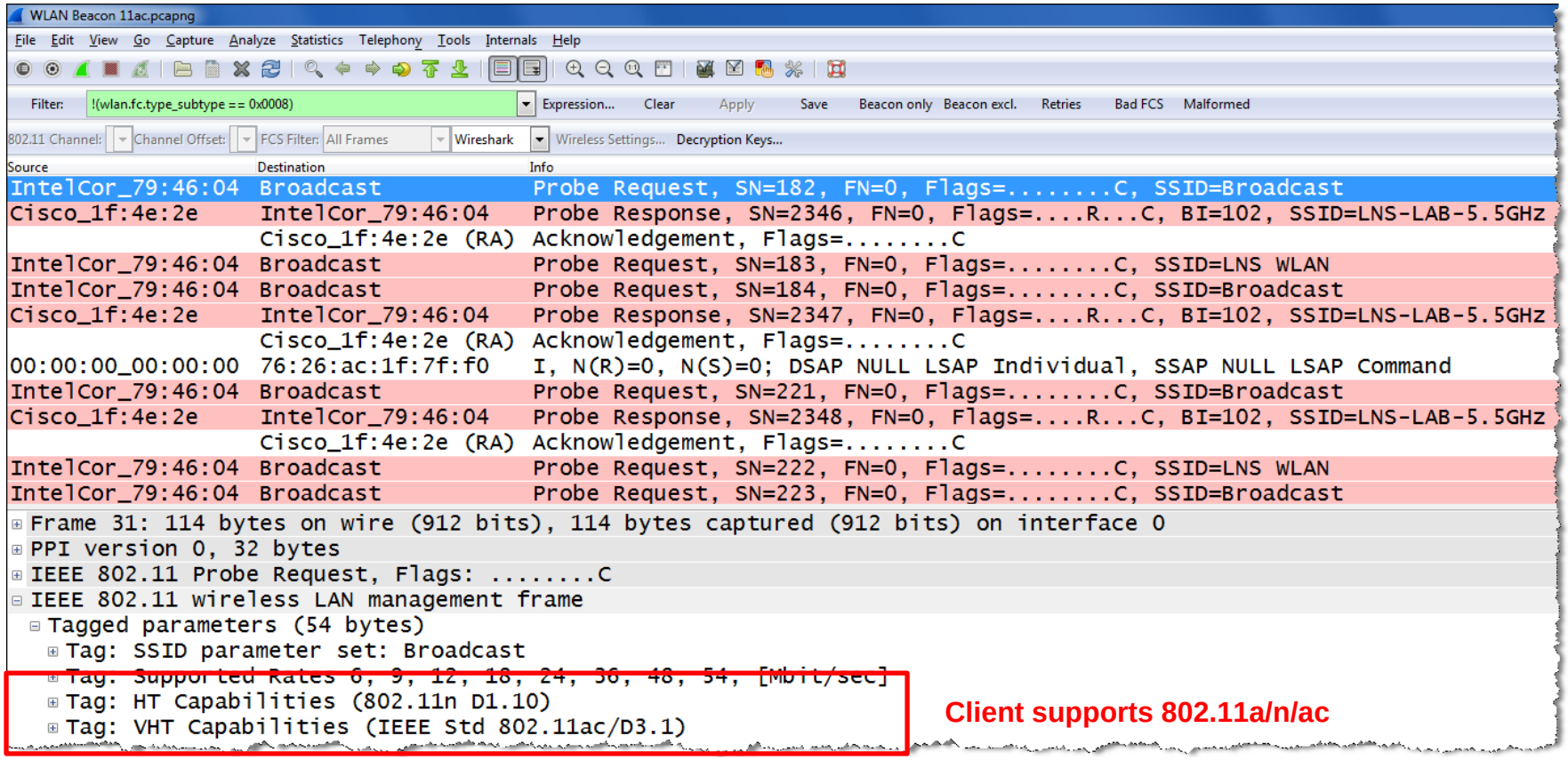
Management Frames: Probe Request & Response

- A client sends Probe Requests to scan the channels for Access Points
- Capturing with multiple AirPcaps shows the scanning process

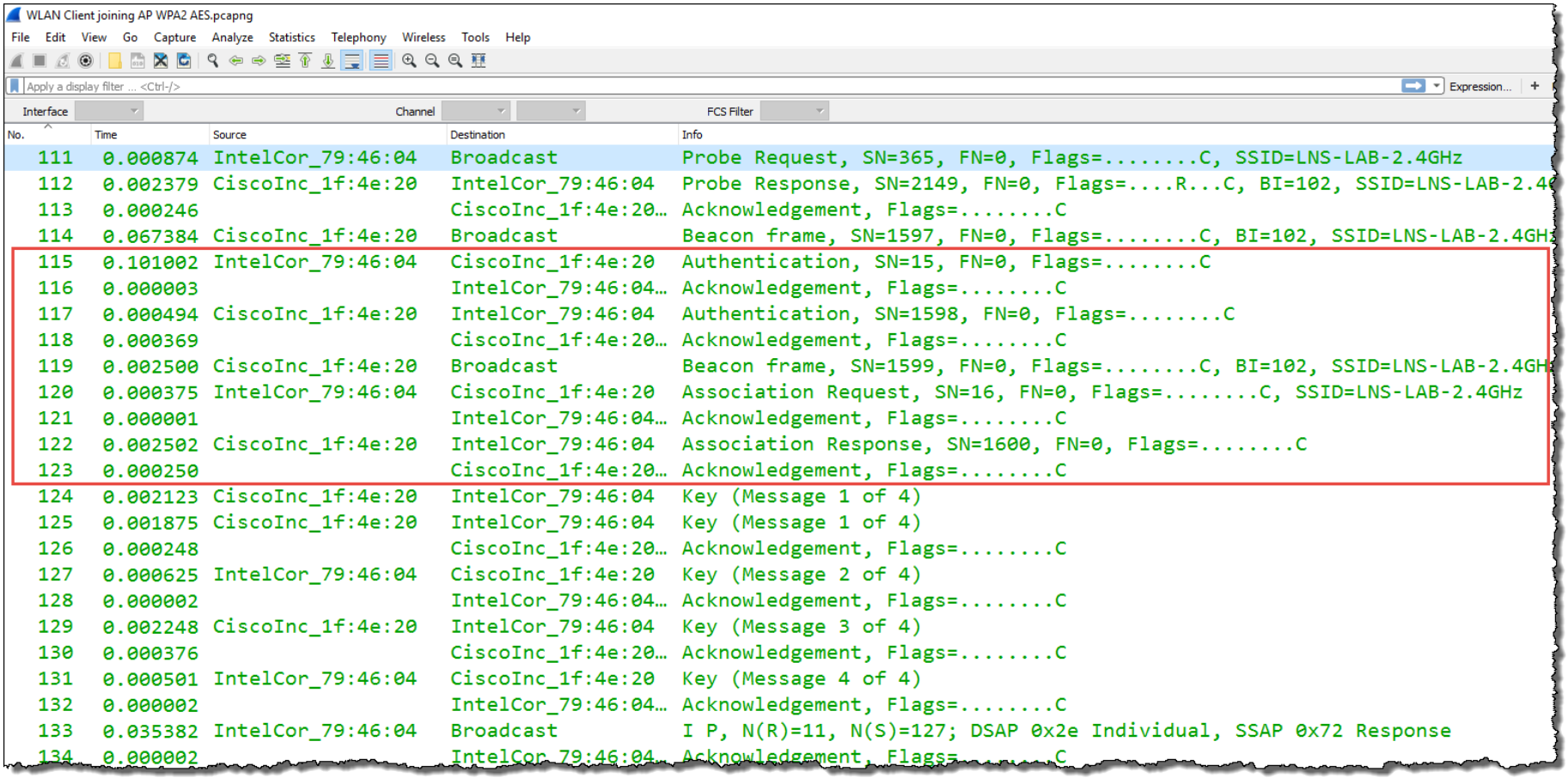


Management Frames: Probe Request & Response

- Probe Request contains client features and a specific or broadcast SSID
- Access Points reply with Probe Response, containing same fields as Beacon

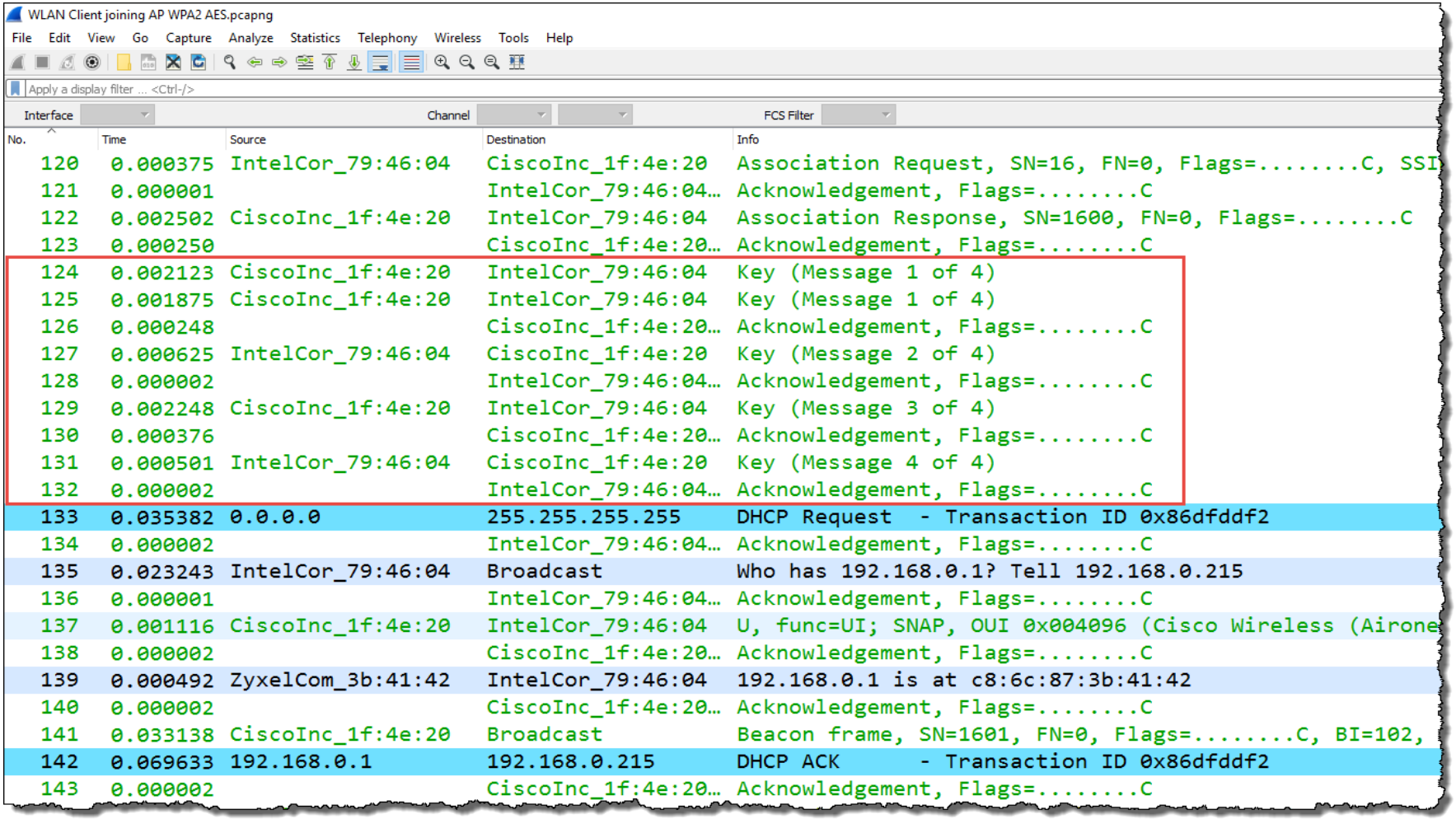


- The client selects an Access Point and sends Authenticate & Associate requests
- Both processes must be successful in order to join the Access Point



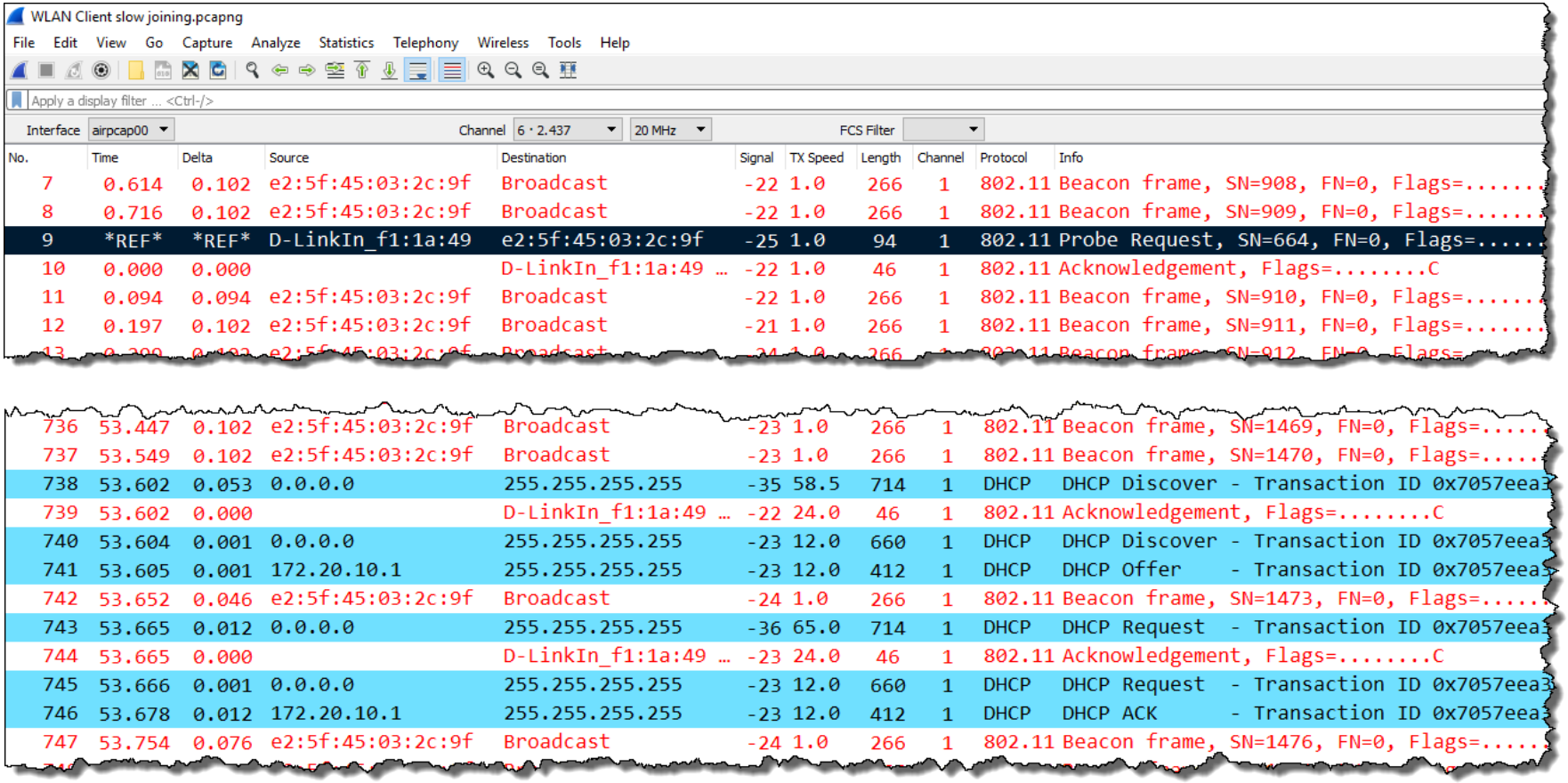
No.	Time	Source	Destination	Info
111	0.000874	IntelCor_79:46:04	Broadcast	Probe Request, SN=365, FN=0, Flags=........C, SSID=LNS-LAB-2.4GHz
112	0.002379	CiscoInc_1f:4e:20	IntelCor_79:46:04	Probe Response, SN=2149, FN=0, Flags=....R...C, BI=102, SSID=LNS-LAB-2.4
113	0.000246		CiscoInc_1f:4e:20...	Acknowledgement, Flags=........C
114	0.067384	CiscoInc_1f:4e:20	Broadcast	Beacon frame, SN=1597, FN=0, Flags=........C, BI=102, SSID=LNS-LAB-2.4GH
115	0.101002	IntelCor_79:46:04	CiscoInc_1f:4e:20	Authentication, SN=15, FN=0, Flags=........C
116	0.000003		IntelCor_79:46:04...	Acknowledgement, Flags=........C
117	0.000494	CiscoInc_1f:4e:20	IntelCor_79:46:04	Authentication, SN=1598, FN=0, Flags=........C
118	0.000369		CiscoInc_1f:4e:20...	Acknowledgement, Flags=........C
119	0.002500	CiscoInc_1f:4e:20	Broadcast	Beacon frame, SN=1599, FN=0, Flags=........C, BI=102, SSID=LNS-LAB-2.4GH
120	0.000375	IntelCor_79:46:04	CiscoInc_1f:4e:20	Association Request, SN=16, FN=0, Flags=........C, SSID=LNS-LAB-2.4GHz
121	0.000001		IntelCor_79:46:04...	Acknowledgement, Flags=........C
122	0.002502	CiscoInc_1f:4e:20	IntelCor_79:46:04	Association Response, SN=1600, FN=0, Flags=........C
123	0.000250		CiscoInc_1f:4e:20...	Acknowledgement, Flags=........C
124	0.002123	CiscoInc_1f:4e:20	IntelCor_79:46:04	Key (Message 1 of 4)
125	0.001875	CiscoInc_1f:4e:20	IntelCor_79:46:04	Key (Message 1 of 4)
126	0.000248		CiscoInc_1f:4e:20...	Acknowledgement, Flags=........C
127	0.000625	IntelCor_79:46:04	CiscoInc_1f:4e:20	Key (Message 2 of 4)
128	0.000002		IntelCor_79:46:04...	Acknowledgement, Flags=........C
129	0.002248	CiscoInc_1f:4e:20	IntelCor_79:46:04	Key (Message 3 of 4)
130	0.000376		CiscoInc_1f:4e:20...	Acknowledgement, Flags=........C
131	0.000501	IntelCor_79:46:04	CiscoInc_1f:4e:20	Key (Message 4 of 4)
132	0.000002		IntelCor_79:46:04...	Acknowledgement, Flags=........C
133	0.035382	IntelCor_79:46:04	Broadcast	I P, N(R)=11, N(S)=127; DSAP 0x2e Individual, SSAP 0x72 Response
134	0.000002		IntelCor_79:46:04...	Acknowledgement, Flags=........C

- Wireshark can decrypt WEP, WPA & WPA2 PSK if the key is available
- To decrypt WPA & WPA2 the key negotiation process must be captured



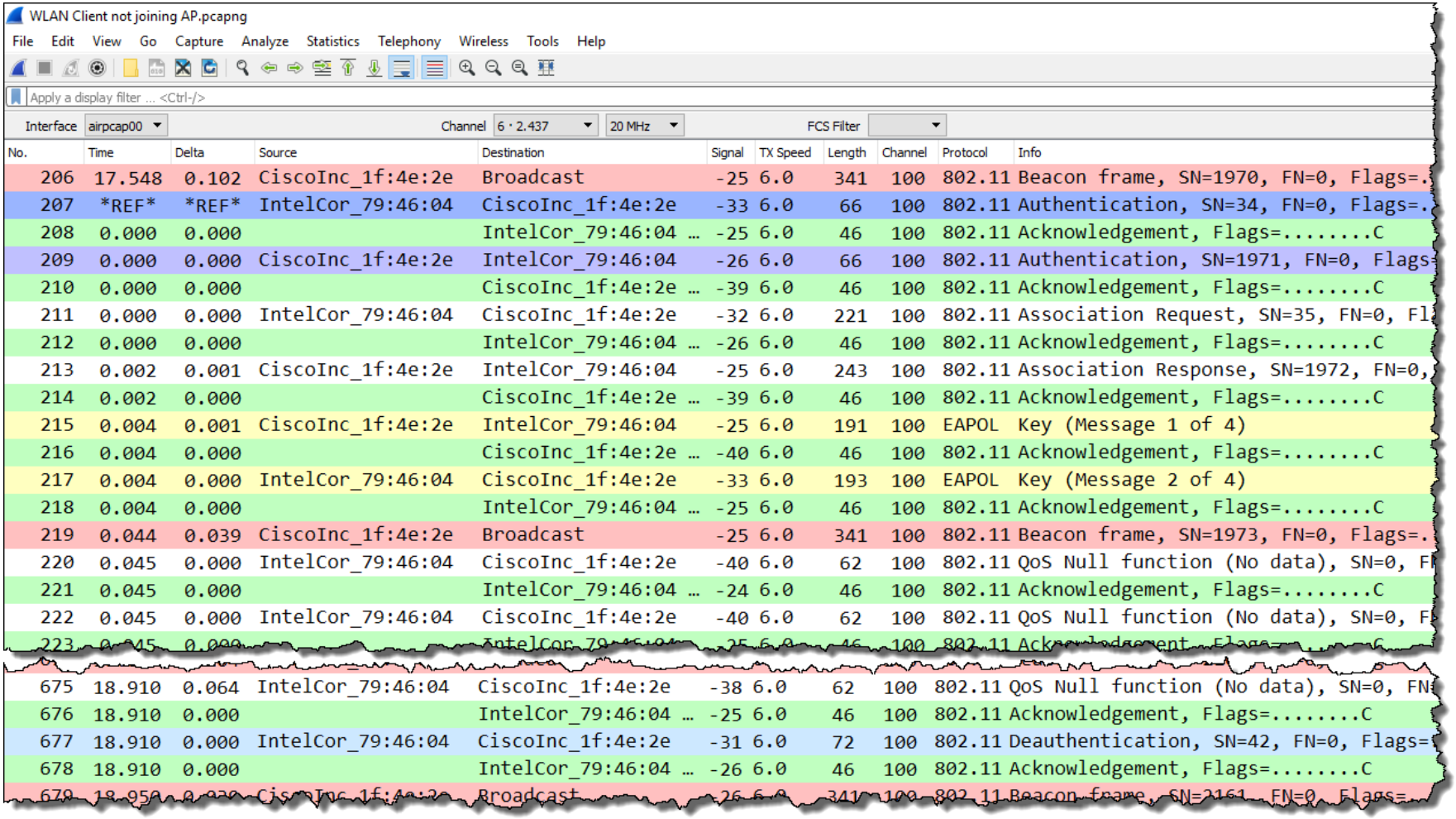
Client joining problem (case one)

- A client needs up to a minute duration to join an Access Point
- Analyzing the trace file discloses the reason

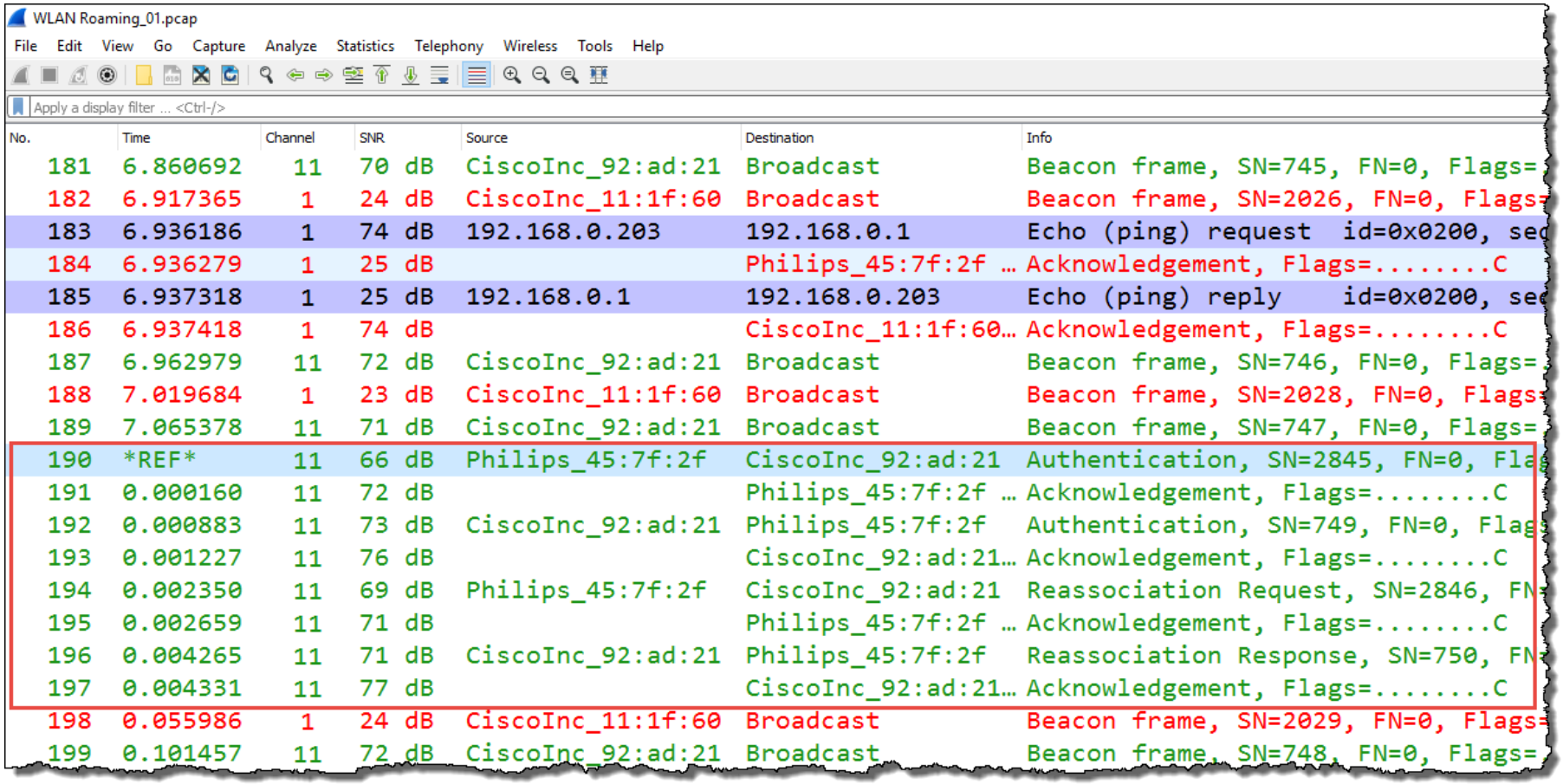


Client joining problem (case two)

- A client is not able to join an Access Point and finally deauthenticates from AP
- Analyzing the trace file discloses the reason



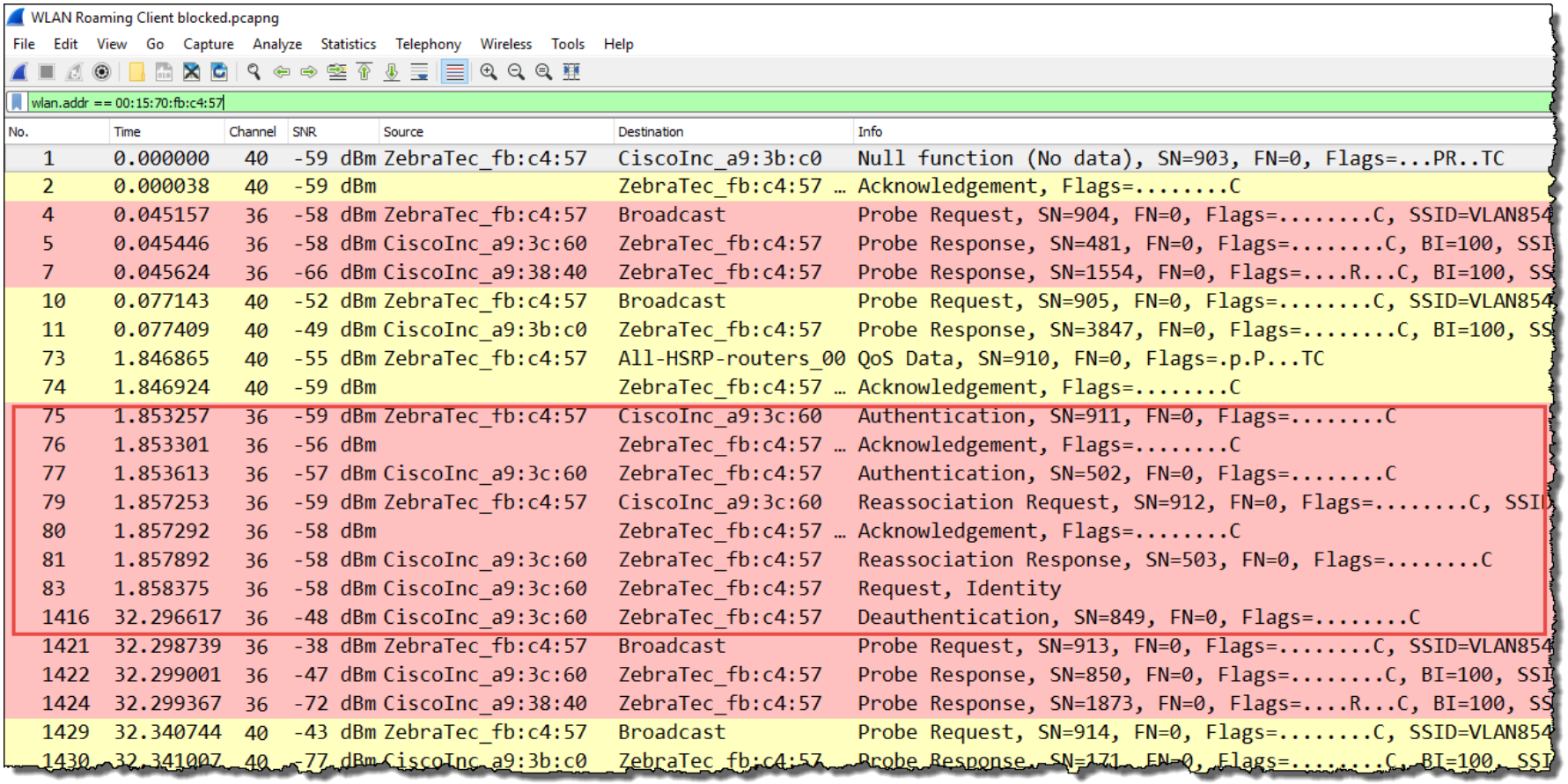
- A client is roaming from channel 1 to 11 because the SNR of the new AP is better
- Following the client with two AirPcaps allows to capture the roaming process



No.	Time	Channel	SNR	Source	Destination	Info
181	6.860692	11	70 dB	CiscoInc_92:ad:21	Broadcast	Beacon frame, SN=745, FN=0, Flags=
182	6.917365	1	24 dB	CiscoInc_11:1f:60	Broadcast	Beacon frame, SN=2026, FN=0, Flags=
183	6.936186	1	74 dB	192.168.0.203	192.168.0.1	Echo (ping) request id=0x0200, seq
184	6.936279	1	25 dB		Philips_45:7f:2f …	Acknowledgement, Flags=.....C
185	6.937318	1	25 dB	192.168.0.1	192.168.0.203	Echo (ping) reply id=0x0200, seq
186	6.937418	1	74 dB		CiscoInc_11:1f:60…	Acknowledgement, Flags=.....C
187	6.962979	11	72 dB	CiscoInc_92:ad:21	Broadcast	Beacon frame, SN=746, FN=0, Flags=
188	7.019684	1	23 dB	CiscoInc_11:1f:60	Broadcast	Beacon frame, SN=2028, FN=0, Flags=
189	7.065378	11	71 dB	CiscoInc_92:ad:21	Broadcast	Beacon frame, SN=747, FN=0, Flags=
190	*REF*	11	66 dB	Philips_45:7f:2f	CiscoInc_92:ad:21	Authentication, SN=2845, FN=0, Flag
191	0.000160	11	72 dB		Philips_45:7f:2f …	Acknowledgement, Flags=.....C
192	0.000883	11	73 dB	CiscoInc_92:ad:21	Philips_45:7f:2f	Authentication, SN=749, FN=0, Flag
193	0.001227	11	76 dB		CiscoInc_92:ad:21…	Acknowledgement, Flags=.....C
194	0.002350	11	69 dB	Philips_45:7f:2f	CiscoInc_92:ad:21	Reassociation Request, SN=2846, FN
195	0.002659	11	71 dB		Philips_45:7f:2f …	Acknowledgement, Flags=.....C
196	0.004265	11	71 dB	CiscoInc_92:ad:21	Philips_45:7f:2f	Reassociation Response, SN=750, FN
197	0.004331	11	77 dB		CiscoInc_92:ad:21…	Acknowledgement, Flags=.....C
198	0.055986	1	24 dB	CiscoInc_11:1f:60	Broadcast	Beacon frame, SN=2029, FN=0, Flags=
199	0.101457	11	72 dB	CiscoInc_92:ad:21	Broadcast	Beacon frame, SN=748, FN=0, Flags=

Client roaming problem (case three)

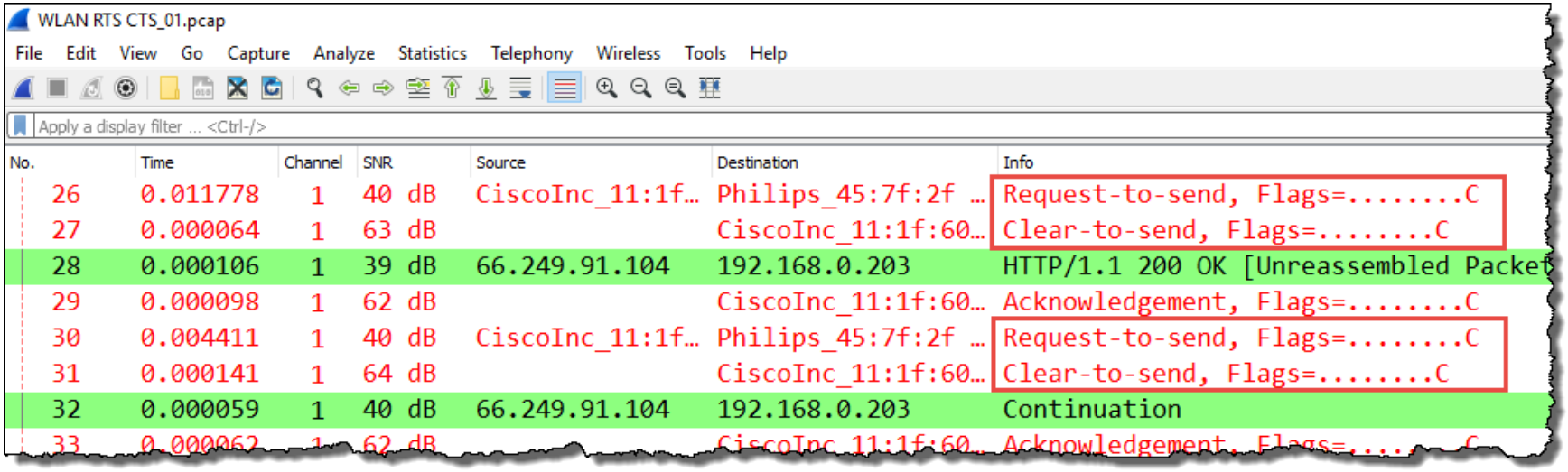
- User is complaining about sporadic hangers in bar code scanners, up to minutes
- Vendors of mobile clients and access points are finger pointing, since month.
- Problem could be assigned to bar code vendor by analyzing trace files.



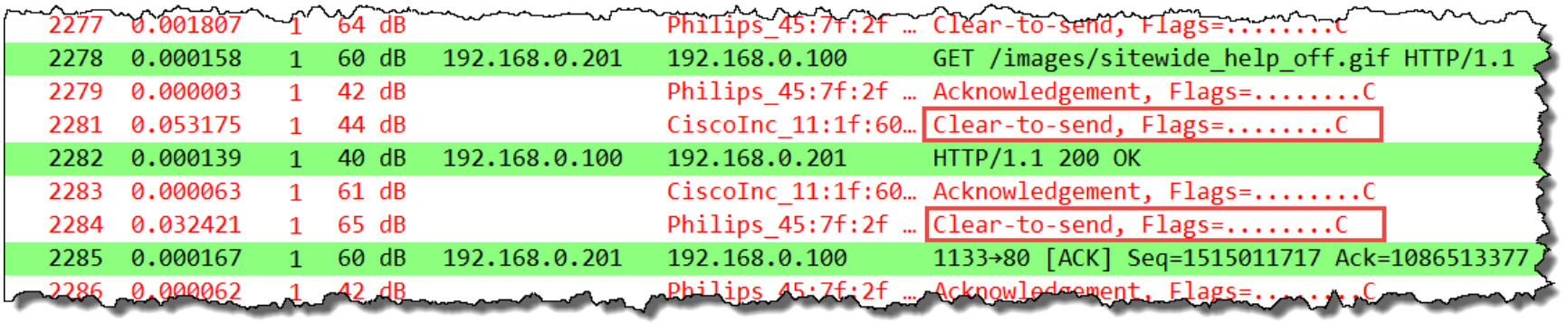
No.	Time	Channel	SNR	Source	Destination	Info
1	0.000000	40	-59 dBm	ZebraTec_fb:c4:57	CiscoInc_a9:3b:c0	Null function (No data), SN=903, FN=0, Flags=...PR..TC
2	0.000038	40	-59 dBm		ZebraTec_fb:c4:57 …	Acknowledgement, Flags=........C
4	0.045157	36	-58 dBm	ZebraTec_fb:c4:57	Broadcast	Probe Request, SN=904, FN=0, Flags=........C, SSID=VLAN854
5	0.045446	36	-58 dBm	CiscoInc_a9:3c:60	ZebraTec_fb:c4:57	Probe Response, SN=481, FN=0, Flags=........C, BI=100, SSI
7	0.045624	36	-66 dBm	CiscoInc_a9:38:40	ZebraTec_fb:c4:57	Probe Response, SN=1554, FN=0, Flags=....R...C, BI=100, SS
10	0.077143	40	-52 dBm	ZebraTec_fb:c4:57	Broadcast	Probe Request, SN=905, FN=0, Flags=........C, SSID=VLAN854
11	0.077409	40	-49 dBm	CiscoInc_a9:3b:c0	ZebraTec_fb:c4:57	Probe Response, SN=3847, FN=0, Flags=........C, BI=100, SS
73	1.846865	40	-55 dBm	ZebraTec_fb:c4:57	All-HSRP-routers_00	QoS Data, SN=910, FN=0, Flags=.p.P...TC
74	1.846924	40	-59 dBm		ZebraTec_fb:c4:57 …	Acknowledgement, Flags=........C
75	1.853257	36	-59 dBm	ZebraTec_fb:c4:57	CiscoInc_a9:3c:60	Authentication, SN=911, FN=0, Flags=........C
76	1.853301	36	-56 dBm		ZebraTec_fb:c4:57 …	Acknowledgement, Flags=........C
77	1.853613	36	-57 dBm	CiscoInc_a9:3c:60	ZebraTec_fb:c4:57	Authentication, SN=502, FN=0, Flags=........C
79	1.857253	36	-59 dBm	ZebraTec_fb:c4:57	CiscoInc_a9:3c:60	Reassociation Request, SN=912, FN=0, Flags=........C, SSID
80	1.857292	36	-58 dBm		ZebraTec_fb:c4:57 …	Acknowledgement, Flags=........C
81	1.857892	36	-58 dBm	CiscoInc_a9:3c:60	ZebraTec_fb:c4:57	Reassociation Response, SN=503, FN=0, Flags=........C
83	1.858375	36	-58 dBm	CiscoInc_a9:3c:60	ZebraTec_fb:c4:57	Request, Identity
1416	32.296617	36	-48 dBm	CiscoInc_a9:3c:60	ZebraTec_fb:c4:57	Deauthentication, SN=849, FN=0, Flags=........C
1421	32.298739	36	-38 dBm	ZebraTec_fb:c4:57	Broadcast	Probe Request, SN=913, FN=0, Flags=........C, SSID=VLAN854
1422	32.299001	36	-47 dBm	CiscoInc_a9:3c:60	ZebraTec_fb:c4:57	Probe Response, SN=850, FN=0, Flags=........C, BI=100, SSI
1424	32.299367	36	-72 dBm	CiscoInc_a9:38:40	ZebraTec_fb:c4:57	Probe Response, SN=1873, FN=0, Flags=....R...C, BI=100, SS
1429	32.340744	40	-43 dBm	ZebraTec_fb:c4:57	Broadcast	Probe Request, SN=914, FN=0, Flags=........C, SSID=VLAN854
1430	32.341007	40	-77 dBm	CiscoInc_a9:3b:c0	ZebraTec_fb:c4:57	Probe Response, SN=171, FN=0, Flags=........C, BI=100, SSI

Control Frames: Request to Send / Clear to Send

- A WLAN node can reserve airtime and refrain all other stations from sending
- RTS/CTS reservation is used in busy cells, Hidden Node situations or in mixed mode



- A short form, so-called CTS-to-Self is often used in cells with B-Only clients present



Rate	Modulation	Description
1 2	Barker/DBPSK Barker/DBPSK	**802.11 DSSS** ‚Long Preamble‘
5.5 11	CCK/DQPSK CCK/DQPSK	**802.11b** **High Rate (HR)** with ‚Short Preamble‘
6, 9 12, 18 24, 36 48, 54	OFDM/BPSK OFDM/QPSK OFDM/16-QAM OFDM/64-QAM	**802.11g** **Extended Rate PHY (ERP)**
From 6.5 up to 600*	OFDM/16-QAM OFDM/64-QAM	**802.11n** **High Throughput (HT) Extensions**

2.4 GHz Band

Rate	Modulation	Description
6, 9 12, 18 24, 36 48, 54	OFDM/BPSK OFDM/QPSK OFDM/16-QAM OFDM/64-QAM	**802.11a**
From 6.5 up to 600*	OFDM/16-QAM OFDM/64-QAM	**802.11n** **HT Extensions**
From 86 up to 6930**	OFDM/16-QAM OFDM/64-QAM OFDM/256-QAM	**802.11ac** **Very High Throughput (VHT)**

5 GHz Band

CCK = Complementary Code Keying
DBPSK = Differential Binary Phase-Shift Keying
DQPSK = Differential Quadrature Phase-Shift Keying
OFDM = Orthogonal Frequency Division Multiplexing
BPSK = Binary Phase-Shift Keying
QPSK = Quadrature Phase-Shift Keying
QAM = Quadrature Amplitude Modulation

* With up to 2 Channels and up to 4 Streams
**With up to 8 Channels and up to 8 Streams

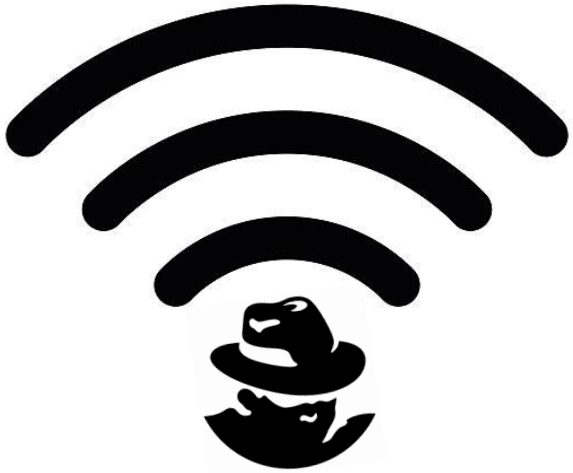
802.11n/ac Physical Rate Table (Mbps)

Number of Streams	Modulation	Antennas Tx x Rx : Spatial Streams	Maximum Rate (Mbps) 1 Ch.	2 Ch.	4 Ch.	8 Ch.	Band Support
802.11n							
One Stream*	64-QAM	1 x 1 : 1	72	150	n.a.	n.a.	2.4 & 5 GHz
Two Streams*	64-QAM	2 x 2 : 2	144	300	n.a.	n.a.	2.4 & 5 GHz
Three Streams	64-QAM	3 x 3 : 3	216	450	n.a.	n.a.	2.4 & 5 GHz
Four Streams	64-QAM	4 x 4 : 4	288	600	n.a.	n.a.	2.4 & 5 GHz
802.11ac Wave 1							
One Stream	256-QAM	1 x 1 : 1	86	200	433	n.a.	5 GHz
Two Streams	256-QAM	2 x 2 : 2	173	400	866	n.a.	5 GHz
Three Streams	256-QAM	3 x 3 : 3	289	600	1300	n.a.	5 GHz
802.11ac Wave 2							
One Stream	256-QAM	1 x 1 : 1	86	200	433	866	5 GHz
Two Streams	256-QAM	2 x 2 : 2	173	400	866	1730	5 GHz
Three Streams	256-QAM	3 x 3 : 3	289	600	1300	2600	5 GHz
Four Streams	256-QAM	4 x 4 : 4	385	800	1730	3470	5 GHz
Eight Streams	256-QAM	8 x 8 : 8	770	1600	3470	6930	5 GHz

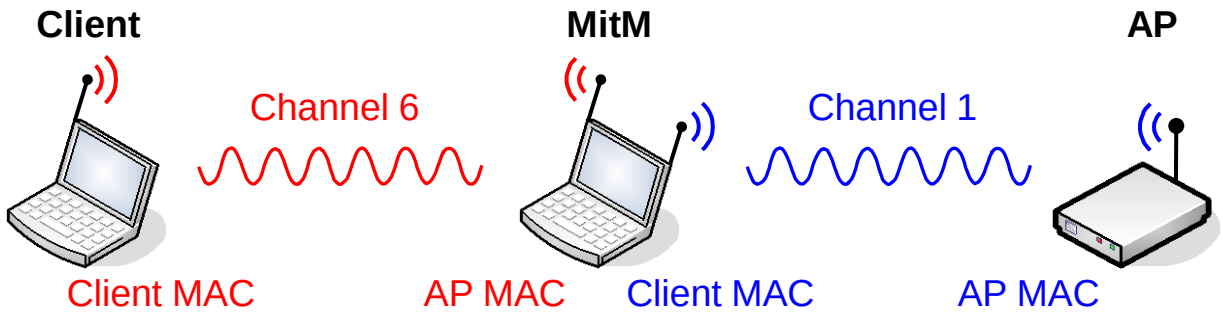
* AirPcap Nx supports 802.11n with up to two Spatial Streams (2x2:2) in Legacy, HT20 or HT40 mode (no SGI & Greenfield mode)

October 2017: Breaking bad news is shocking the WLAN world

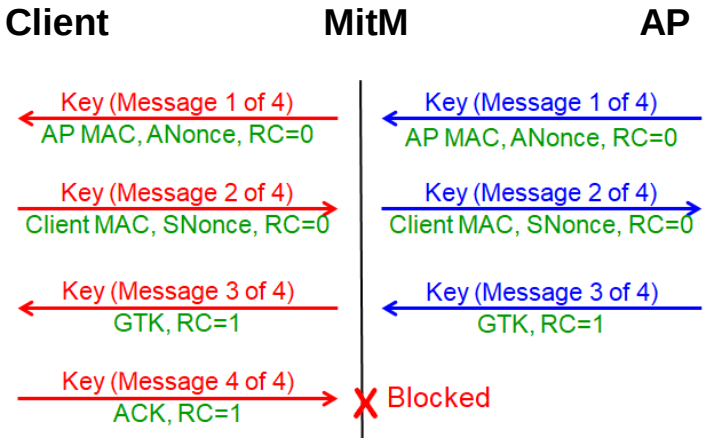
- KRACK is able to decrypt the most widely used WPA & WPA2 security; this in Personal as well as Enterprise mode
- Engineers at University KU Leuven, Belgium have discovered a method called KRACK using Channel based Men in the Middle method
- The attack is achieved by manipulating and replaying cryptographic messages during the initial 4-way WPA/WPA2 handshake
- KRACK decrypts all presently used cipher suites (WPA-TKIP, AES-CCMP and GCMP)
- KRACK does not require any expensive radio equipment, it rather works with cheap of-the-shelf Wi-Fi dongles
- A detailed demonstration and whitepaper is published https://www.krackattacks.com/



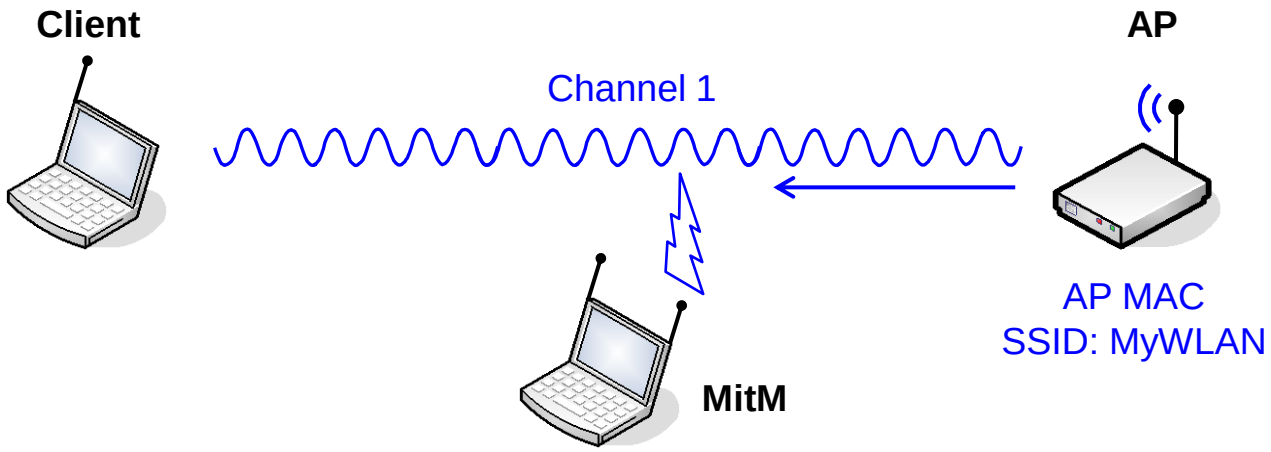
- Step 1: A Men in the Middle (MitM) device is inserted
  - Based on a technique called Channel based MitM attack
  - Can be used to read, drop, insert or manipulate frames



- Step 2: The initial 4-way handshake authentication is manipulated by KRACK
  - Frames are dropped or inserted to force a Nonce value to be reused

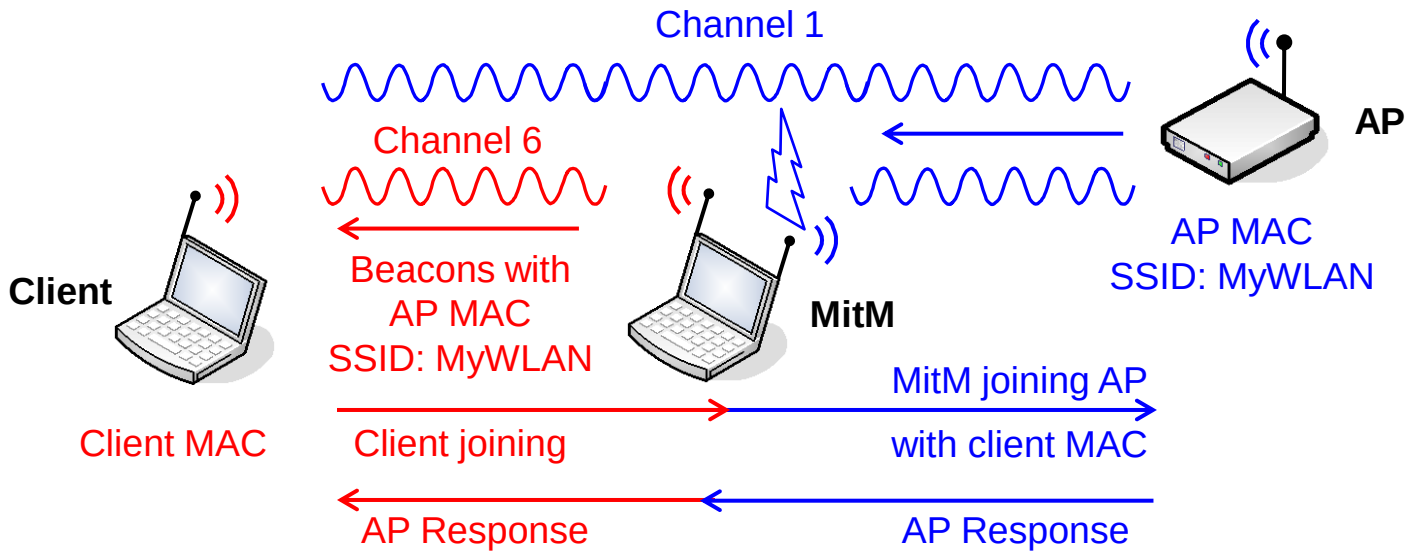


- Phase 1: KRACK starts with jamming an active WLAN channel
  - Continues jamming: MitM device is sending random noise or random Wi-Fi frames to create collisions.
  - Selective jamming: The MitM device reads the frame type and starts jamming only specific frames from the AP (Beacons, Probe responses).
  - Jammed frames will be discarded by a receiver due to bad FCS.



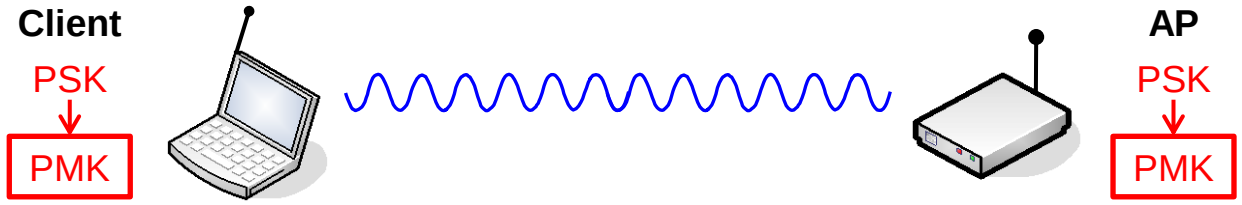
  - Already connected clients will start probing for alternative APs with same SSID in other channels.
  - New clients will continue probing for APs by scanning other channels.

- Phase 2: A client is joining MitM (a faked AP)
  - MitM device is jamming channel and sending Beacons on a different channel.
  - MitM is faking AP by using MAC address and SSID of AP in Beacons

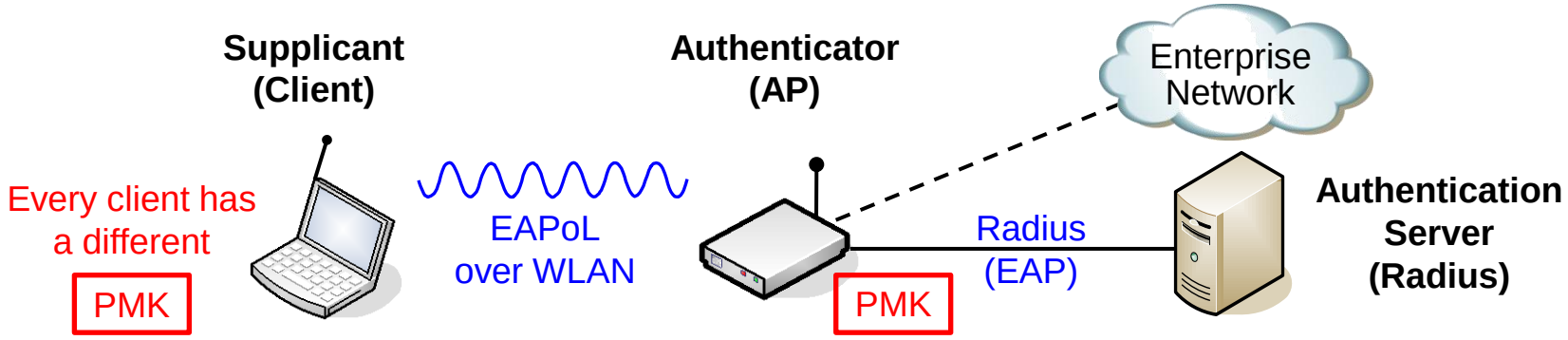


- Client is joining MitM (faked AP) in channel 6
- MitM stops jamming and joins AP in channel 1 using clients MAC address
- AP replies in channel 1, frames are forwarded to client by MitM in channel 6
- MitM is established and can block or forward frames in both directions

- Before the 4-way handshake starts, a session key must be present on client and AP.
  - WPA/2 offers two methods to obtain this key Pairwise Master Key (PMK).
  - The PMK itself is never used directly for authentication or encryption!
- Personal or Pre-Shared Key (PSK) Mode, most widely used in Home/SOHO networks
  - All clients and the AP use the same manually configured Hex string or Passphrase



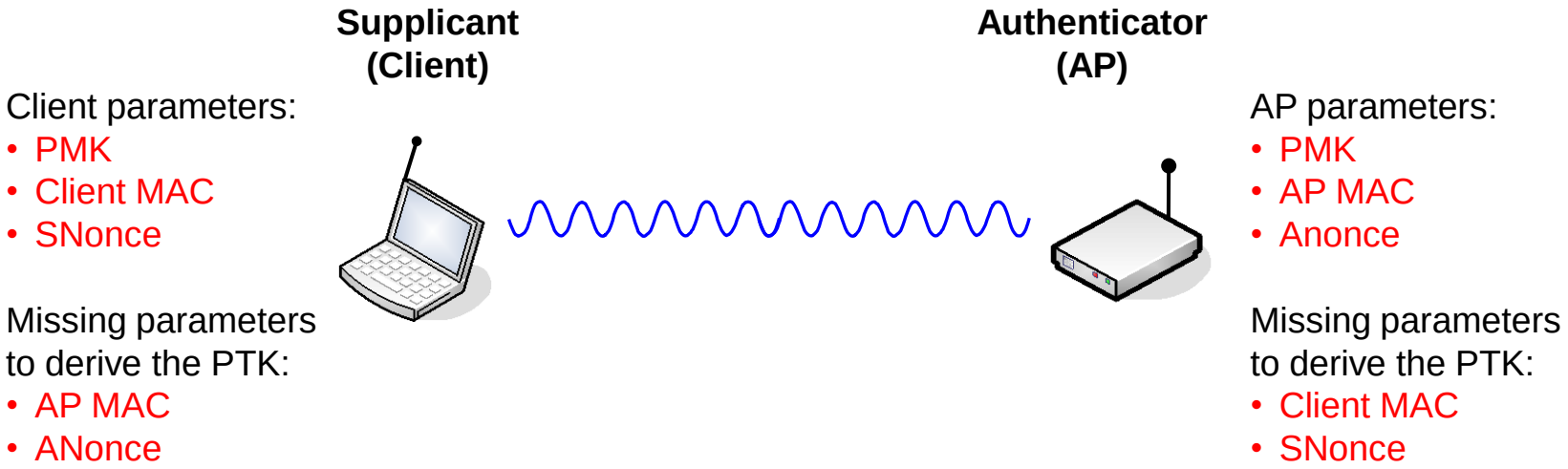
- Enterprise Mode, most widely used in professional environments
  - The Extensible Authentication Protocol (EAP) is used to negotiate the PMK



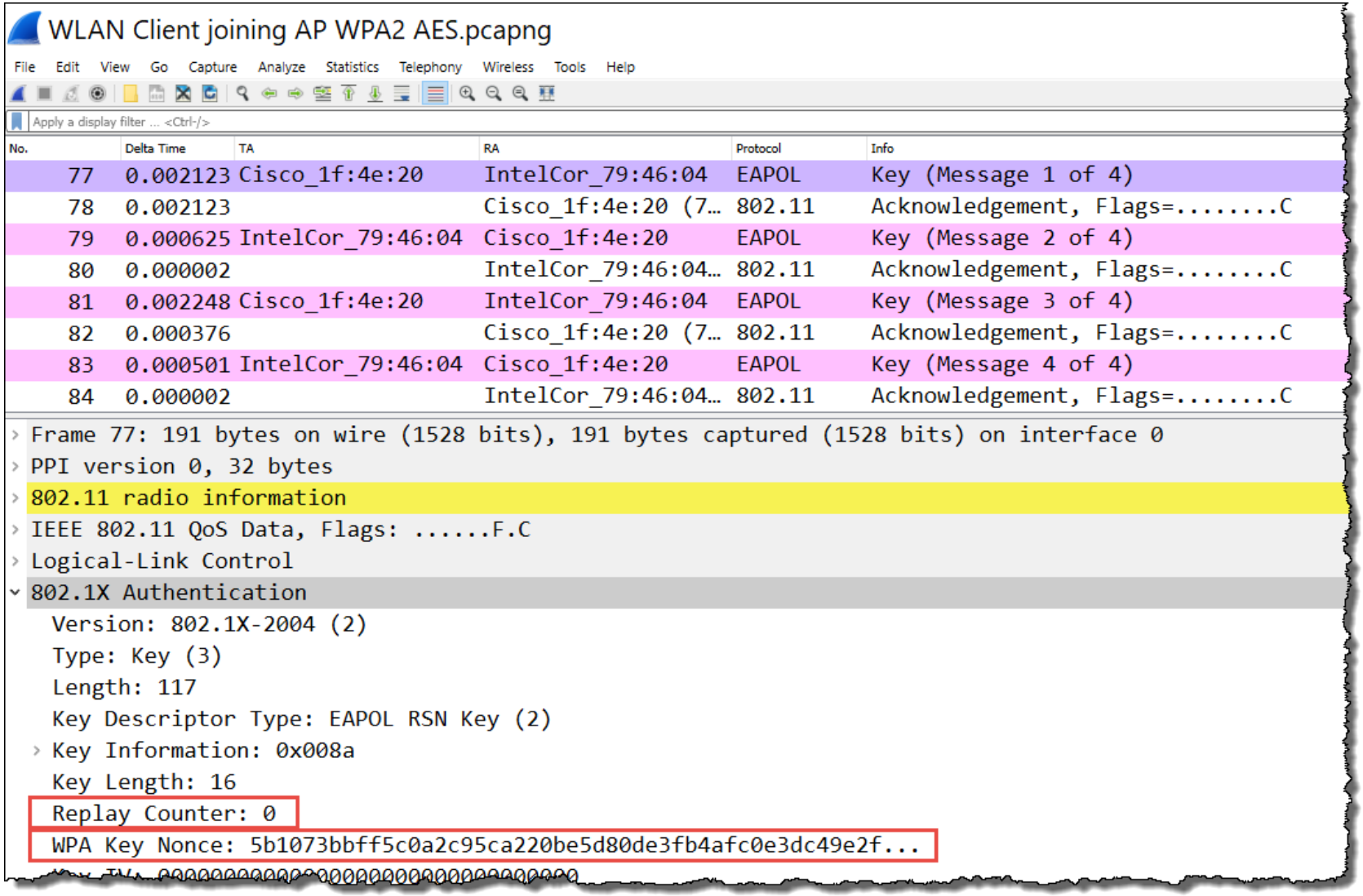
The 4-way handshake authentication process

To understand KRACK, the normal WPA 4-way handshake must be understood

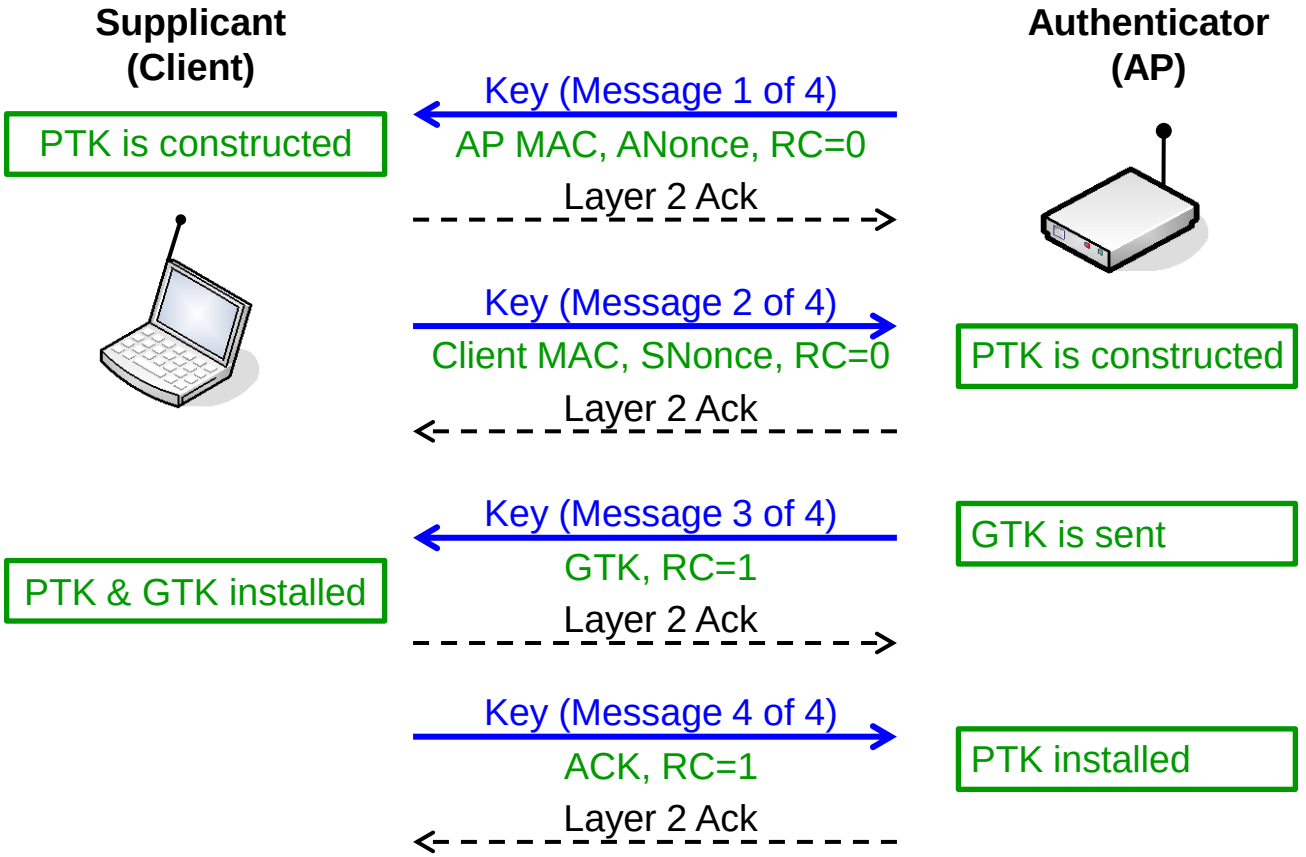
- The handshaek provides mutual authentication and session key agreement.
- To start, both sides need a shared secret called the Pairwise Master Key (PMK).
- A Session Key, called Pairwise Transient Key (PTK) is derived from the PMK.
- The PTK is derived by using five values: PMK, Authenticator Nonce (ANonce), Supplicant Nonce (SNonce), and the MAC addresses of both the Supplicant and Authenticator.
- The Nonce is a random **N**umber used **once** created by the client and the AP.



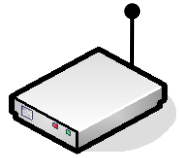
- The 4-way handshake process decoded by Wireshark



- To understand KRACK, the normal WPA 4-way handshake must be understood
  - Messages 1 and 2 provide the missing parameters to derive the PTK (session key)
  - The AP provides the Group Temporal Key (GTK), to decrypt broad/multicasts
  - The Replay Counter (RC) must be increased by one in each new AP message



Step 2: KRACK is manipulating the 4-way handshake process



Supplicant	Channel 6	MitM	Channel 1	Authenticator
PTK is constructed	Key (Message 1 of 4) AP MAC, ANonce, RC=0 Layer 2 Ack		Key (Message 1 of 4) AP MAC, ANonce, RC=0 Layer 2 Ack	
	Key (Message 2 of 4) Client MAC, SNonce, RC=0 Layer 2 Ack		Key (Message 2 of 4) Client MAC, SNonce, RC=0 Layer 2 Ack	PTK is constructed
PTK & GTK installed	Key (Message 3 of 4) GTK, RC=1 Layer 2 Ack		Key (Message 3 of 4) GTK, RC=1 Layer 2 Ack	GTK is sent
	Key (Message 4 of 4) ACK, RC=1 Layer 2 Ack	X Blocked		
Data Transmission	Encrypted Data Layer 2 Ack	X Blocked		
PTK & GTK reinstalled	Key (Message 3 of 4) GTK, RC=2 Layer 2 Ack		Key (Message 3 of 4) GTK, RC=2 Layer 2 Ack	Retransmission
	Key (Message 4 of 4) ACK, RC=2 Layer 2 Ack		Key (Message 4 of 4) ACK, RC=2 Layer 2 Ack	
Data Transmission with reused Nonce	Encrypted Data Layer 2 Ack		Encrypted Data Layer 2 Ack	Data received

- Impact (Bad facts)
  - The KRACK method can decrypt WPA/WPA2 frames by hacking the session key
  - Relatively easy to implement, no expensive equipment required
  - MitM is not easy detectable, as almost no impact on WLAN performance
  - Can intrude in new as well as existing sessions by forcing clients to join the MitM
  - Large installed base of WPA/WPA2 means large field of potential attacks
  - Works in both WPA/WPA2 Personal as well as Enterprise Mode
  - Works for all presently used cipher suites (WPA-TKIP, AES-CCMP, and GCMP)
- Limitations (Good facts)
  - KRACK can not disclose the Pairwise Master Key (PMK)
  - KRACK can not decrypt higher layer encryption like VPN, HTTPS etc.
  - MitM device must be located within radio cell range of client and AP
- Precautions
  - Using higher layer encryption like VPN, HTTPS etc.
  - MitM can be detected by sniffing simultaneously in multiple channels
  - Updating WLAN drivers on clients and APs as soon as available from vendors
  - Using wired networks 

Hope you learned something useful!

Rolf Leutert, Leutert NetServices, www.netsniffing.ch