SharkFest '19 Europe

Troubleshooting WLANs (Part 2)

Troubleshooting WLANs using
802.11 Management & Control Frames

Rolf Leutert

Leutert NetServices
Switzerland
www.netsniffing.ch

Rolf Leutert, El. Eng. 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

Session One

- Analysing Layer 1 (Physical Access) with Spectrum Analyser
- Use case: Finding the source interfering with a WLAN
- Wi-Fi Scanners: Free tools, their functions and limitations
- Analysing Layer 2: Capturing Wi-Fi packets with built in WLAN cards
- Using the Radiotap and PPI pseudo-header information
- Wi-Fi Access Control with CSMA/CA
- Capturing multiple Wi-Fi channels (for analysing roaming problems)

Session Two

- WLAN Layer 2 Analysis using 802.11 Mgmt. & Control frames
- The four different IEEE 802.11 Frame Formats
- WiFi Data Transmission & Retransmission
- Management Frames: Beacon, Probe Request & Response
- Management Frames: Authentication & Association
- Control Frames: Request to Send / Clear to Send
- Decrypting WEP, WPA & WPA2 PSK
- Use case: Isolating a Client roaming problem
- Analysing 802.11n/ac Frame Aggregation A-MSDU & A-MPDU

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

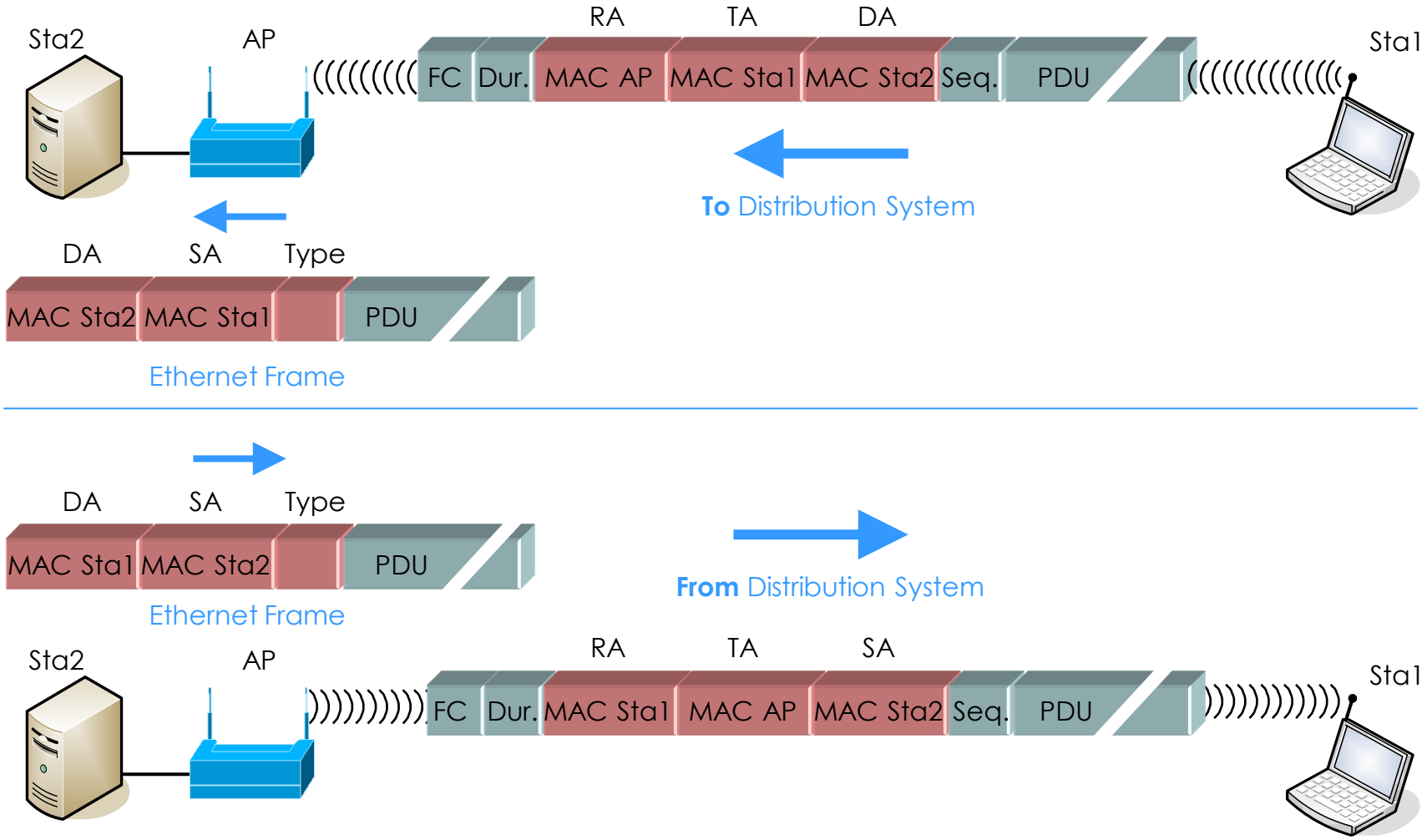
Request to Send

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

Data Frame through repeater

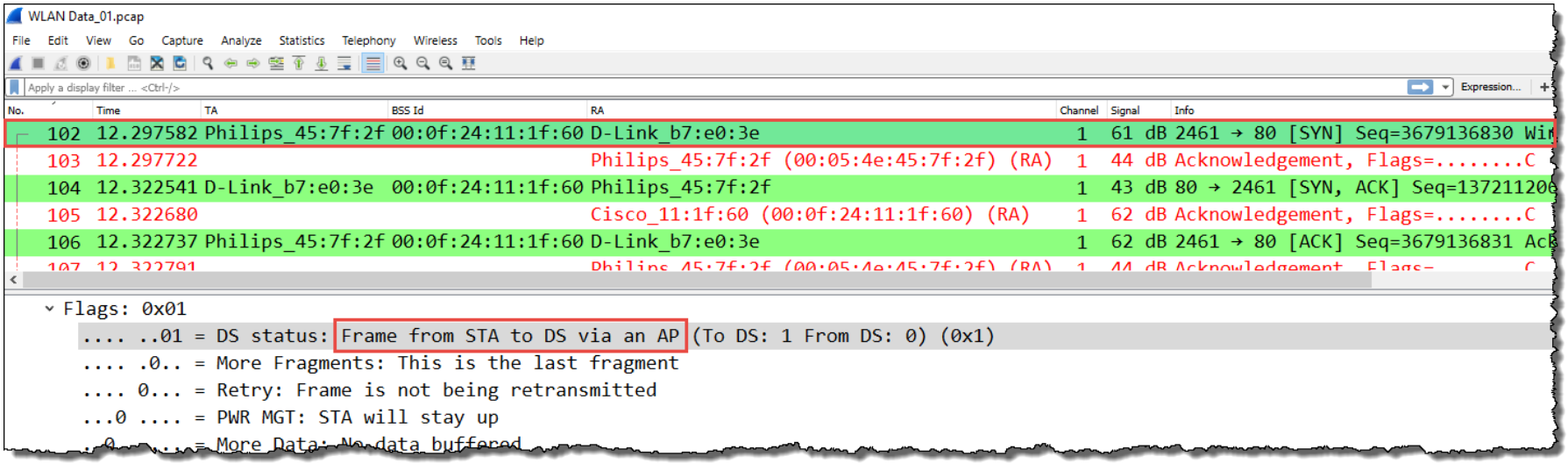
Field names: FC = Frame Control, Dur. = Duration, RA = Receiver MAC Address,
TA = Transmitter MAC Address; DA = Destination MAC Address,
SA = Source MAC Address, Seq. = Sequence, PDU = Protocol Data Unit,
FC = Frame Check Sequence

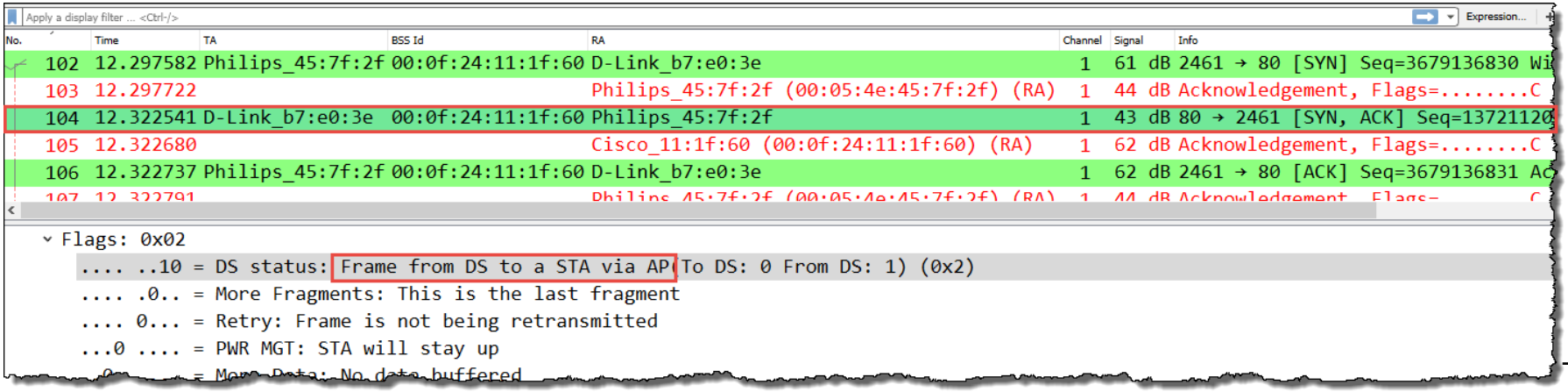
- WiFi data frames have three MAC address field



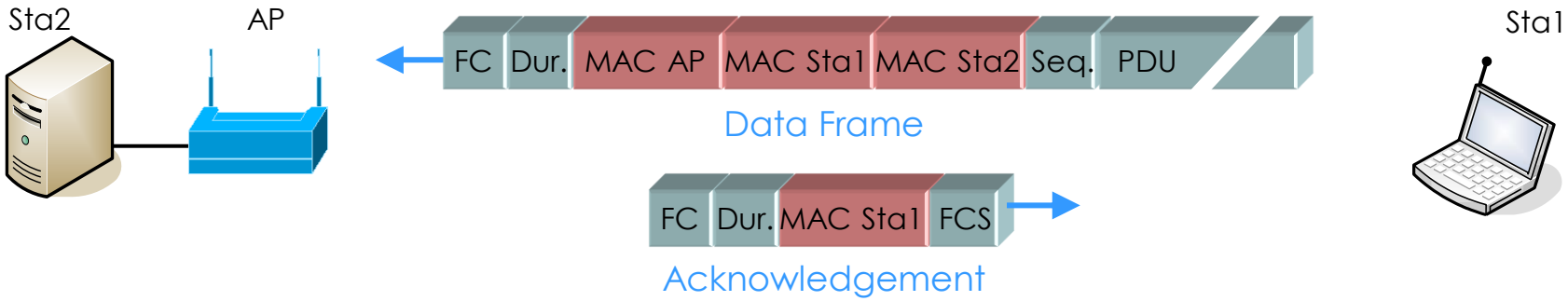
WiFi Data Transmission

- Frames are marked with a direction bit (To or From Distribution System)
- Only Data frames are marked (not management and control frames)

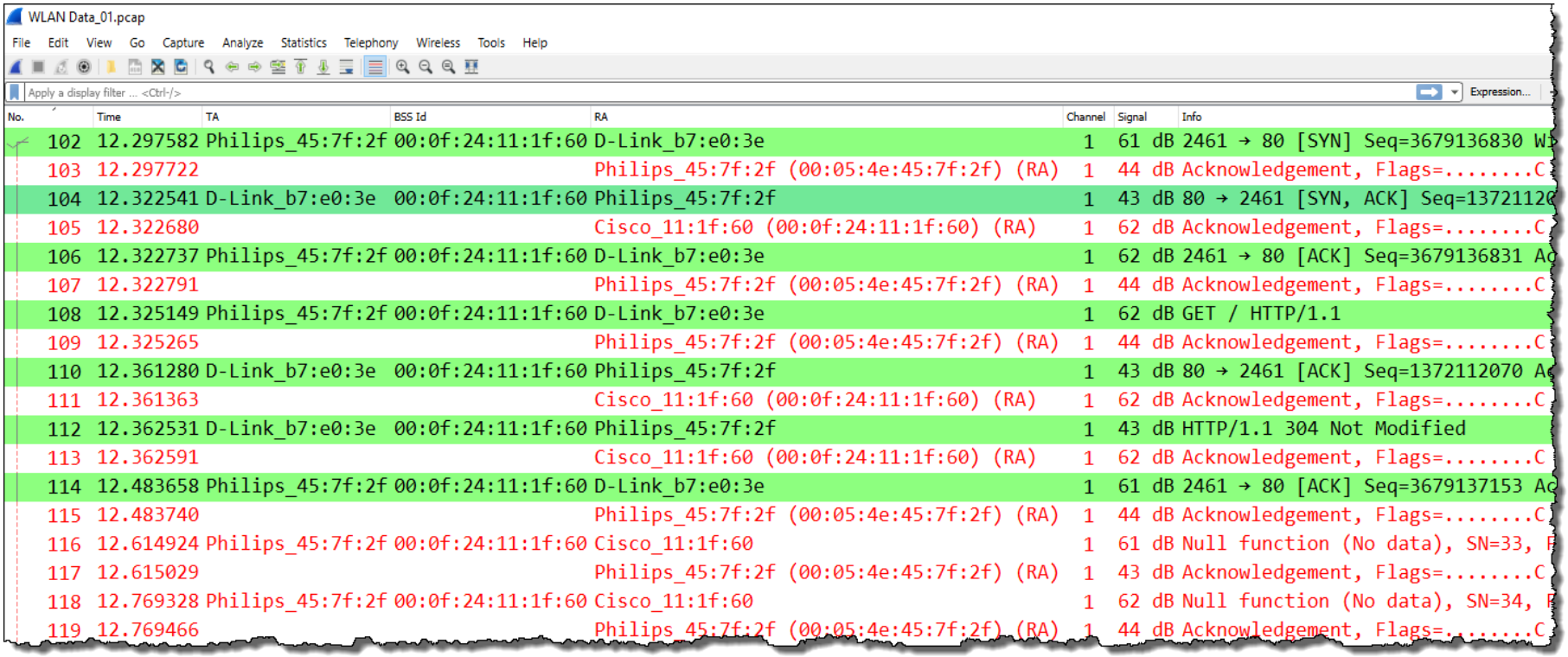




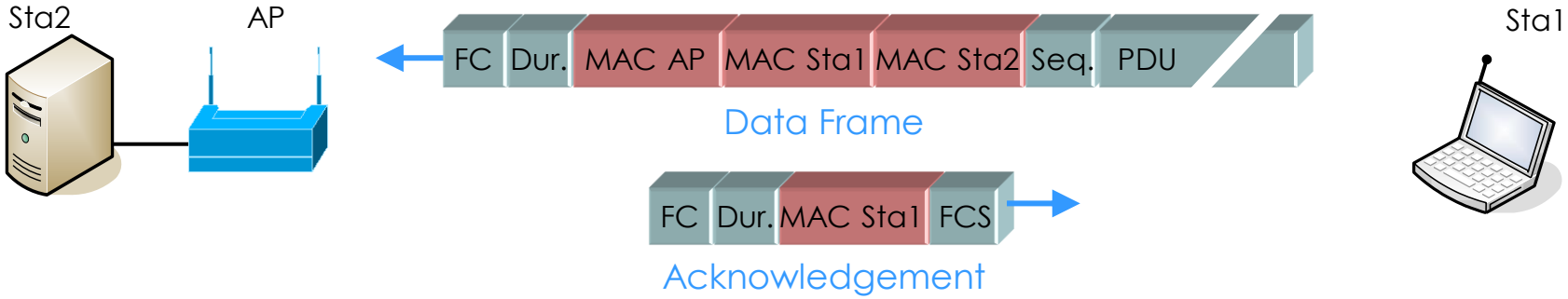
- WiFi data frames are acknowledged or retransmitted



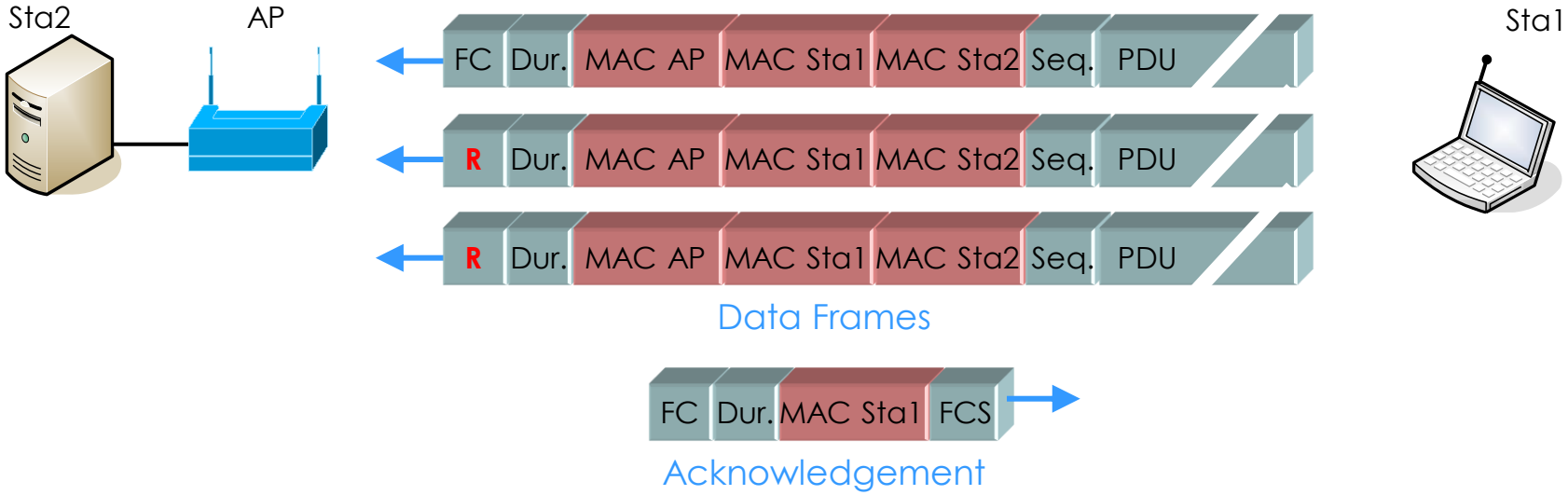
- In non-aggregation mode each packet is acknowledged individually
- The acknowledge frame follows immediately after each data frame
- The (single) acknowledge has no source address field



- 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

WLAN Retransmissions.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.fc.retry == 1 | Expression... | Beacon only | Beacon excl. | Retries | Bad FCS

Interface | Channel | FCS Filter | AirPcap Control Panel | 802.11 Preferences

No.	Time	Source	Destination	Signal	TX Speed	Length	Channel	Protocol	Info
4	0.011			-58	1.0	39	1	802.11	Beacon frame[Malformed Packet]
7	0.017	IntelCor_7e:84:b0	CiscoInc_25:10:e2	-4	6.0	62	6	802.11	QoS Null function (No data), SN=0, …
8	0.017	IntelCor_7e:84:b0	CiscoInc_25:10:e2	-2	6.0	62	6	802.11	QoS Null function (No data), SN=0, …
10	0.030	Canon_01:3e:63	Broadcast	-64	1.0	121	1	802.11	Probe Request, SN=559, FN=0, Flags=…
15	0.038	9b:90:df:0c:86:db	3f:69:71:b8:b0:b2	-60	5.5	655	1	802.11	Fragmented IEEE 802.11 frame
21	0.064	89:19:47:28:63:c2	41:32:7a:b9:aa:48	-58	48.0	1539	1	802.11	Reassociation Request, SN=477, FN=1…
22	0.066			-59	12.0	2836	1	802.11	Control Wrapper, Flags=.p..RM.T.
52	0.184			-58	6.0	1978	1	802.11	Unrecognized (Reserved frame), Flag…
62	0.213	19:ab:dd:1e:a9:3d …	12:ec:62:3d:c2:b8…	-58	11.0	3506	1	802.11	Power-Save poll, Flags=..m.RMFT.
65	0.218		5f:4c:f3:02:8e:29…	-59	11.0	3349	1	802.11	Clear-to-send, Flags=op..RM...
66	0.220			-59	11.0	3563	1	802.11	Fragmented IEEE 802.11 frame
73	0.247	fd:70:f3:5f:91:6a …	ce:ed:36:73:27:e1…	-59	5.5	2738	1	802.11	Request-to-send, Flags=opm.RMFT.
74	0.250	12:4d:e7:2c:54:d4	27:87:47:22:59:f9	-59	5.5	2719	1	LLC	I P, N(R)=87, N(S)=123; DSAP 0xb0 I…

```
Flags: 0x19
    .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
    .... .0.. = More Fragments: This is the last fragment
    .... 1... = Retry: Frame is being retransmitted
    ...1 .... = PWR MGT: STA will go to sleep
    ..0. .... = More Data: No data buffered
    .0.. .... = Protected flag: Data is not protected
```

Retransmission flag (wlan.fc.retry), 1 byte | Packets: 68488 | Displayed: 31456 (45.9%) | Load time: 0:4.481 | Profile: LNS WLAN PPI

- During retransmissions, the transmit speed is reduced by the sender
- The reason for these retransmissions is the high noise level

ping von mitte zu pos 2.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

((wlan.sa == 00:13:5f:d9:60:00) && (wlan.seq == 1450)) || (frame.number == 6438)

No.	Time	Source	BSS Id	Destination	TX Speed	Signal (dBm)	Noise (dBm)	Info
6356	*REF*	Cisco_d9:60:00	00:23:ab:25:10:e2	IntelCor_7e:84:b0	48,0	-55dBm	-69dBm	I, N(R)=2, N(S)=62
6357	0.000400	Cisco_d9:60:00	00:23:ab:25:10:e2	IntelCor_7e:84:b0	36,0	-51dBm	-69dBm	I, N(R)=2, N(S)=62
6360	0.000595	Cisco_d9:60:00	00:23:ab:25:10:e2	IntelCor_7e:84:b0	24,0	-51dBm	-69dBm	I, N(R)=2, N(S)=62
6361	0.000674	Cisco_d9:60:00	00:23:ab:25:10:e2	IntelCor_7e:84:b0	18,0	-55dBm	-69dBm	I, N(R)=2, N(S)=62
6363	0.001139	Cisco_d9:60:00	00:23:ab:25:10:e2	IntelCor_7e:84:b0	12,0	-51dBm	-69dBm	I, N(R)=2, N(S)=62
6366	0.000930	Cisco_d9:60:00	00:23:ab:25:10:e2	IntelCor_7e:84:b0	11,0	-55dBm	-69dBm	I, N(R)=2, N(S)=62
6367	0.001232	Cisco_d9:60:00	00:23:ab:25:10:e2	IntelCor_7e:84:b0	9,0	-51dBm	-69dBm	I, N(R)=2, N(S)=62
6378	0.002359	Cisco_d9:60:00	00:23:ab:25:10:e2	IntelCor_7e:84:b0	6,0	-50dBm	-69dBm	I, N(R)=2, N(S)=62
6384	0.001909	Cisco_d9:60:00	00:23:ab:25:10:e2	IntelCor_7e:84:b0	5,5	-50dBm	-69dBm	I, N(R)=2, N(S)=62
6389	0.001517	Cisco_d9:60:00	00:23:ab:25:10:e2	IntelCor_7e:84:b0	2,0	-54dBm	-69dBm	I, N(R)=2, N(S)=62
6437	0.046557	Cisco_d9:60:00	00:23:ab:25:10:e2	IntelCor_7e:84:b0	1,0	-56dBm	-69dBm	I, N(R)=2, N(S)=62
6438	0.001961			Cisco_25:10:e2 (0…	1,0	-19dBm	-69dBm	Acknowledgement, Fl

```
Flags: 0x4a
    .... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
    .... .0.. = More Fragments: This is the last fragment
    .... 1... = Retry: Frame is being retransmitted
    ...0 .... = PWR MGT: STA will stay up
    ..0. .... = More Data: No data buffered
    .1.. .... = Protected flag: Data is protected
    0... .... = Order flag: Not strictly ordered
```

Overview WiFi 802.11 Standards

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

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

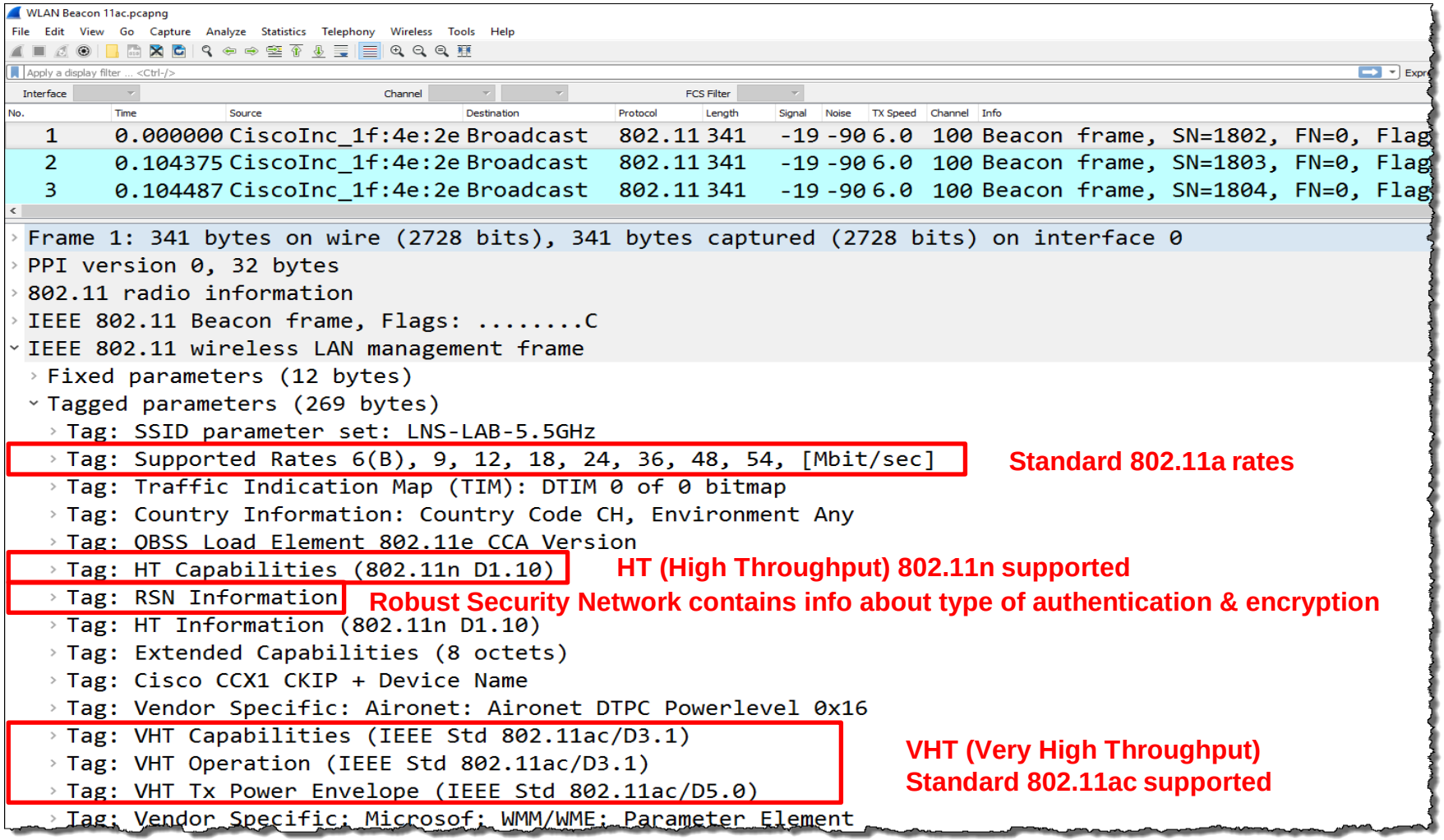
Rate	Modulation	Description
6, 9 12, 18 24, 36 48, 54	OFDM/BPSK OFDM/QPSK OFDM/16-QAM OFDM/64-QAM	**802.11a**
From 6.5 up to 600*	OFDM/16-QAM OFDM/64-QAM	**802.11n** **HT Extensions**
From 86 up to 6930**	OFDM/16-QAM OFDM/64-QAM OFDM/256-QAM	**802.11ac** **Very High Throughput (VHT)**

5 GHz Band

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

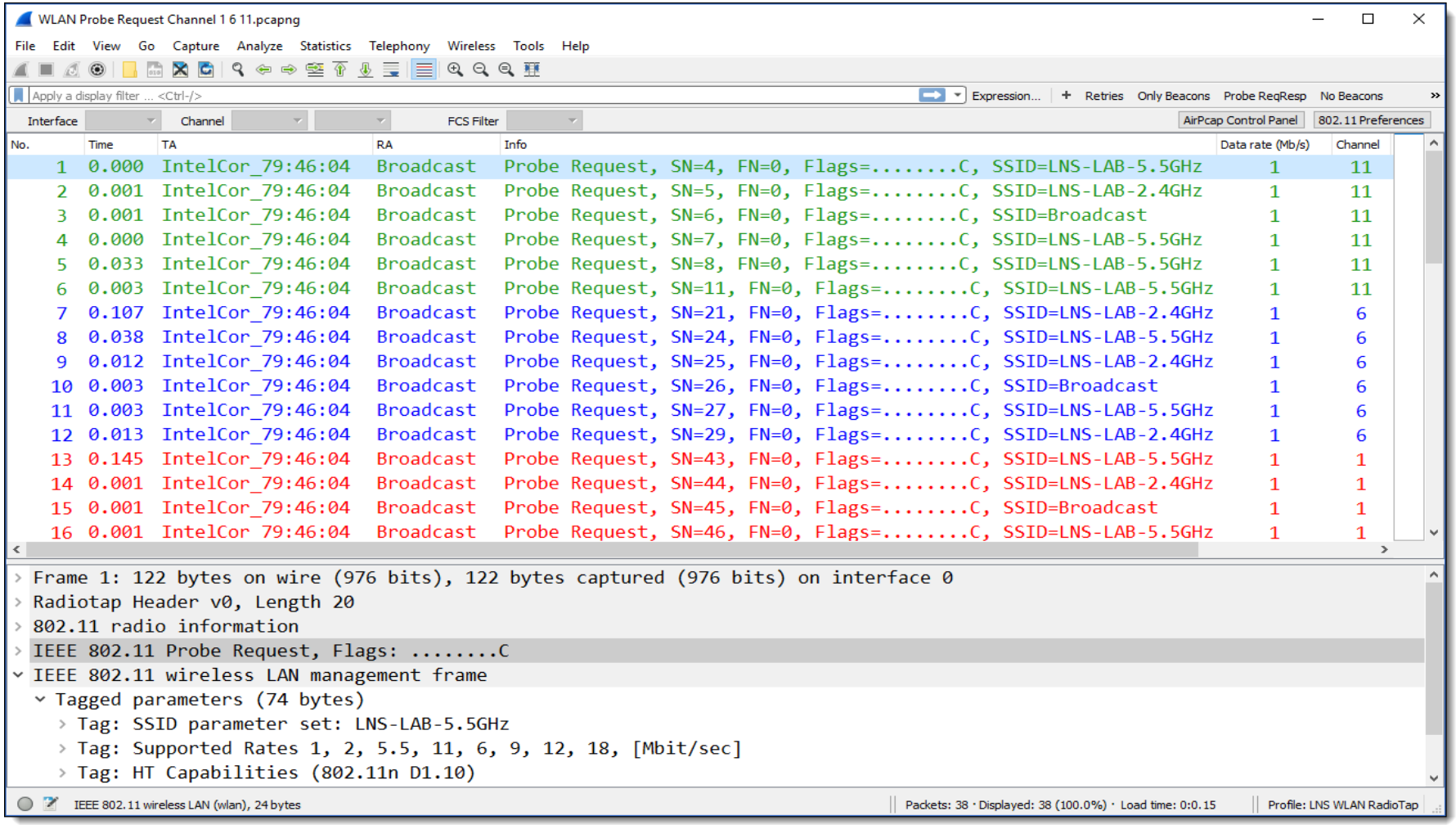
Management Frame: Beacon

- Beacon tags contain information about supported and required features



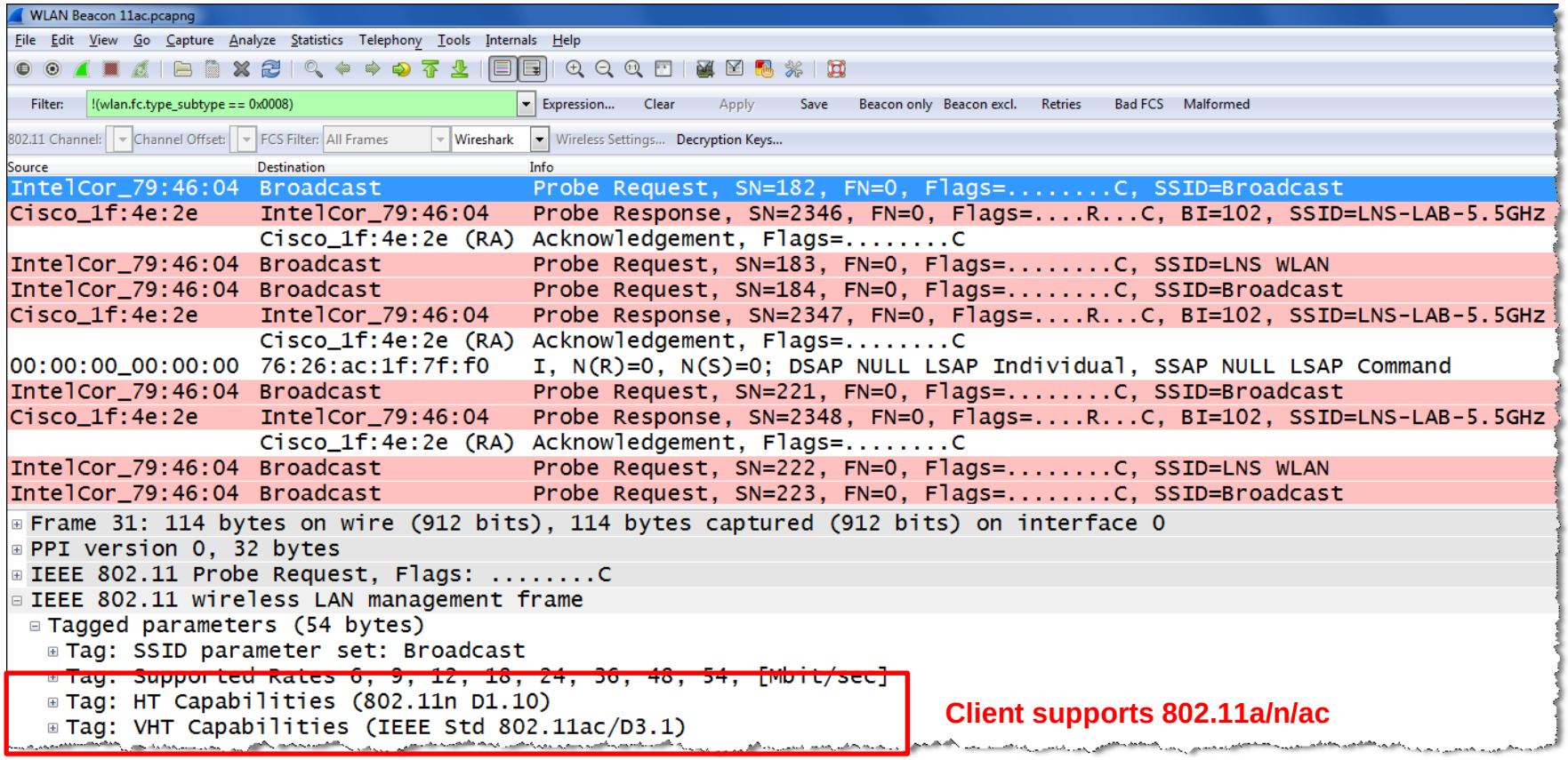
Management Frames: Probe Request & Response

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



Management Frames: Probe Request & Response

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



Management Frames: Authentication & Association

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

WLAN Client joining AP WPA2 AES.pcapng

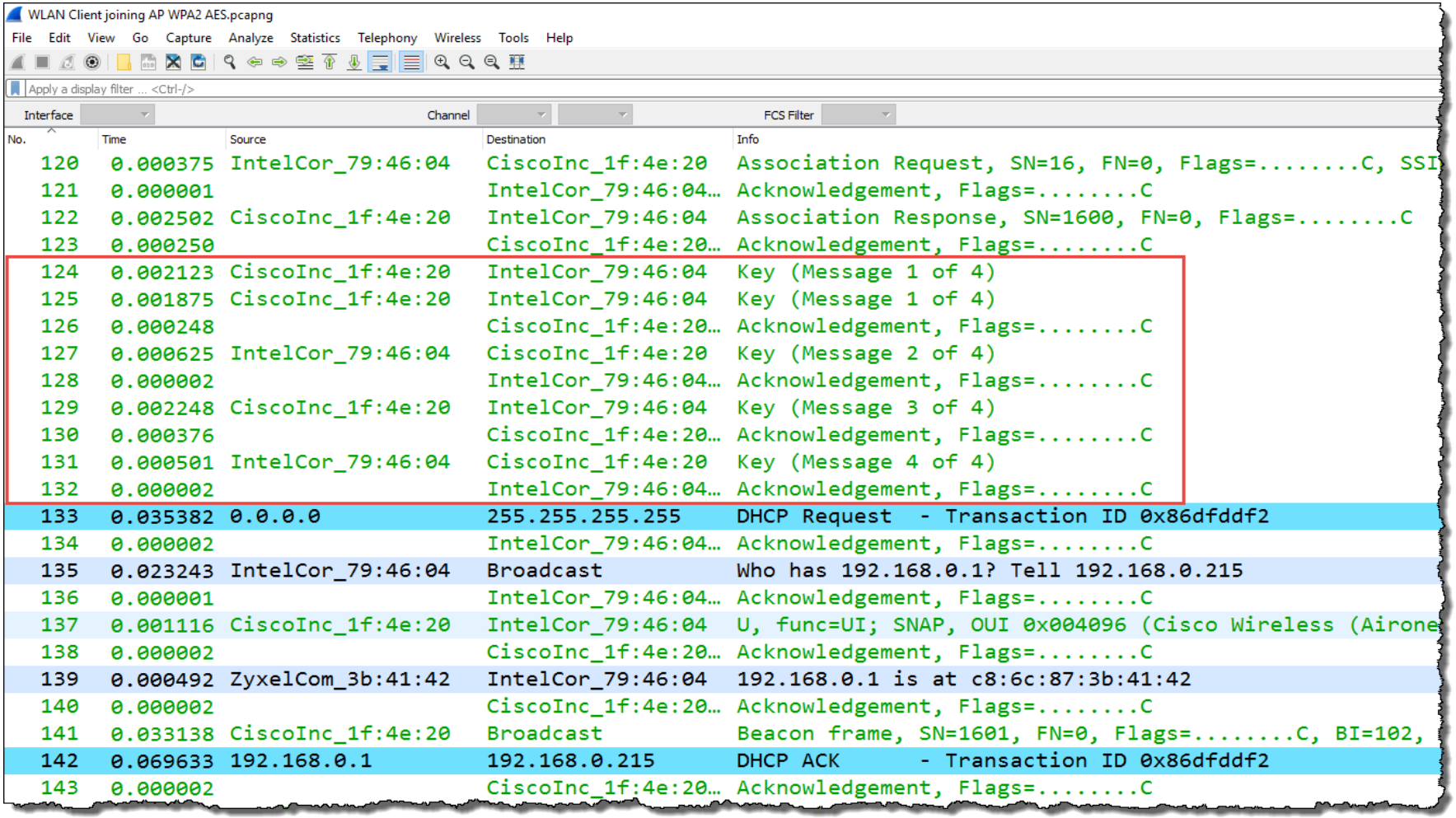
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/> Expression...

Interface Channel FCS Filter

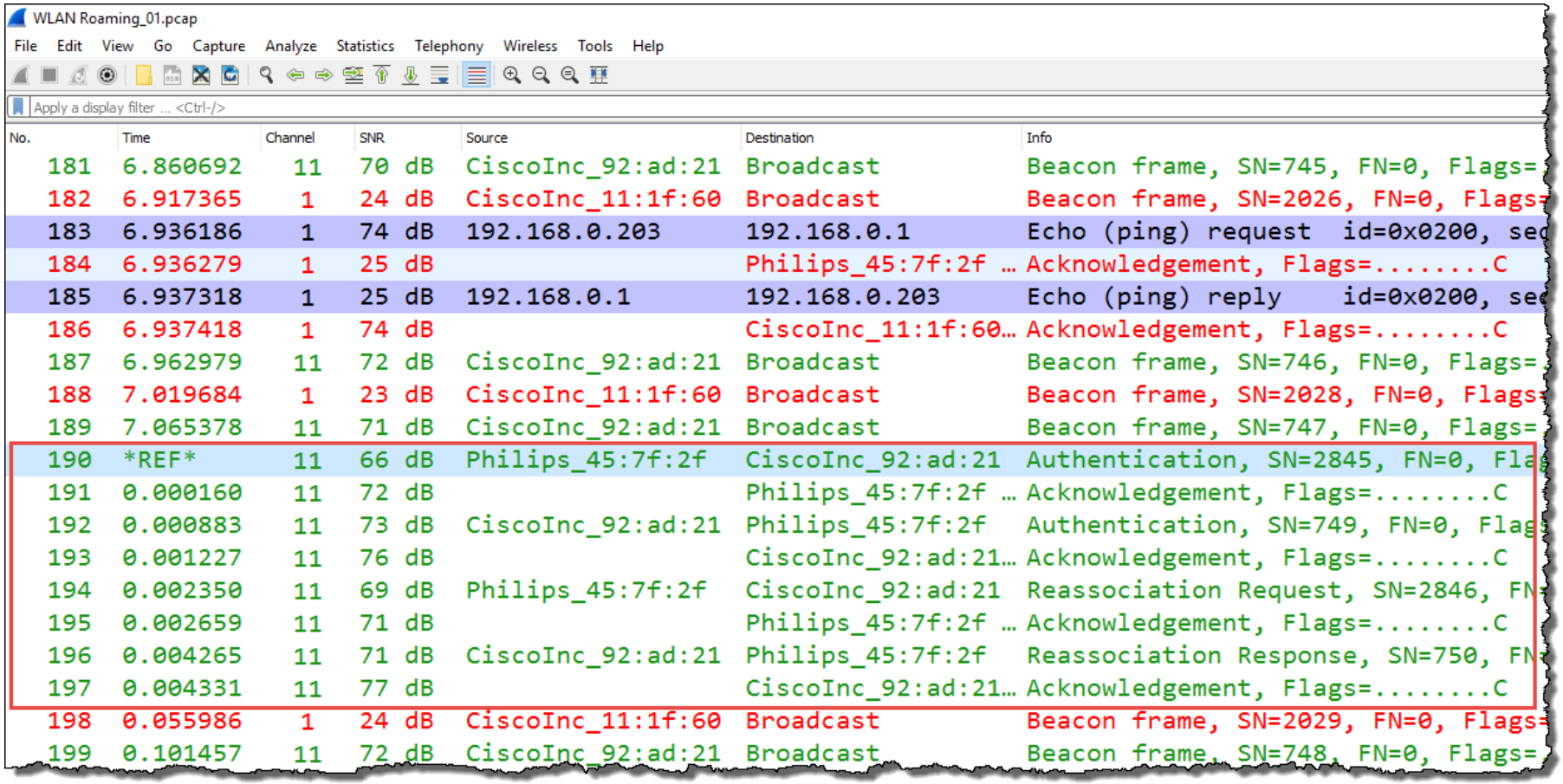
No.	Time	Source	Destination	Info
111	0.000874	IntelCor_79:46:04	Broadcast	Probe Request, SN=365, FN=0, Flags=........C, SSID=LNS-LAB-2.4GHz
112	0.002379	CiscoInc_1f:4e:20	IntelCor_79:46:04	Probe Response, SN=2149, FN=0, Flags=....R...C, BI=102, SSID=LNS-LAB-2.4
113	0.000246		CiscoInc_1f:4e:20...	Acknowledgement, 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



Analyzing the WiFi roaming process

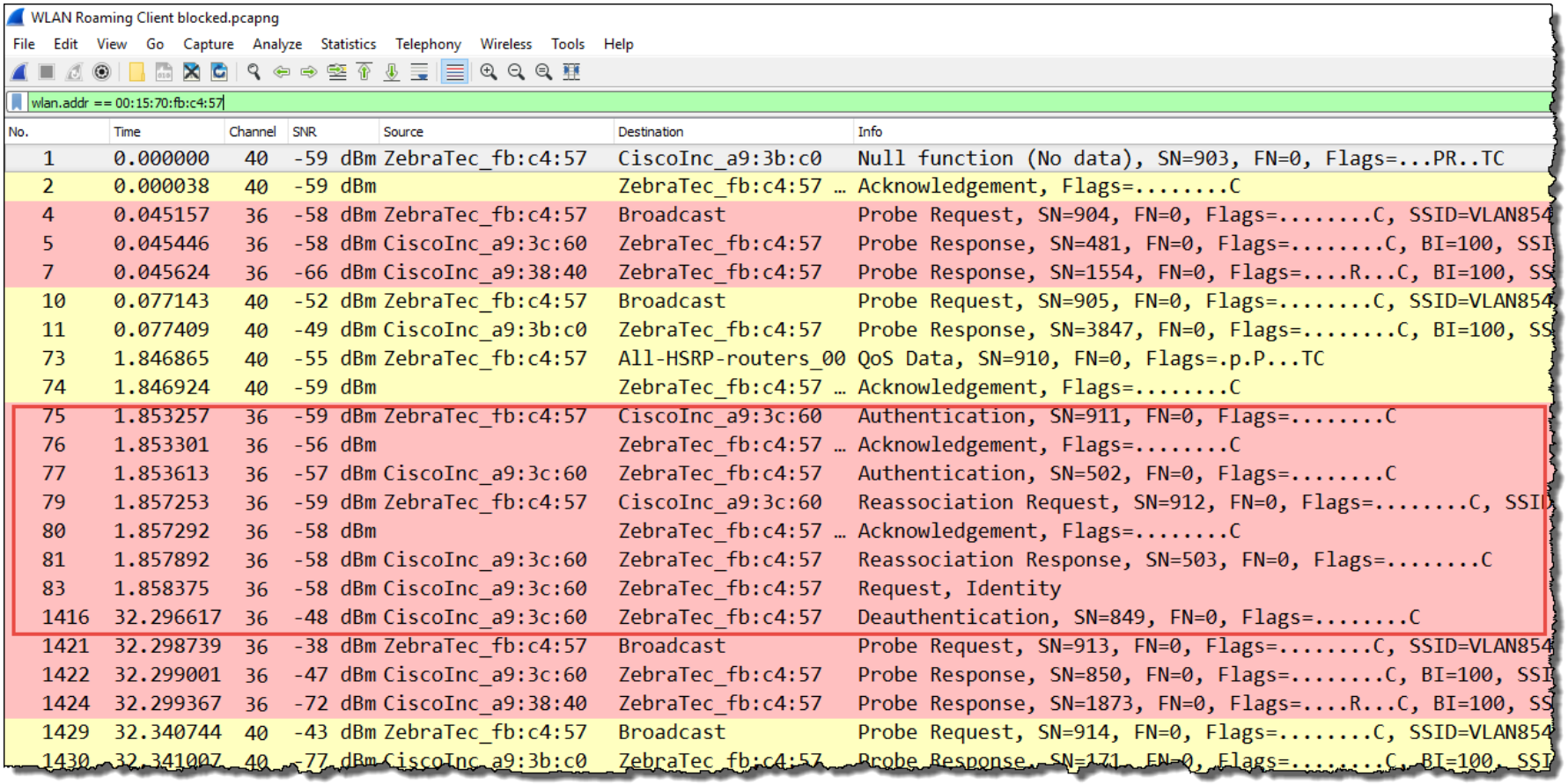
- A client is roaming from channel 1 to 11 because the SNR of the new AP is better
- Capturing the roaming process requires multi-channel equipment



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=

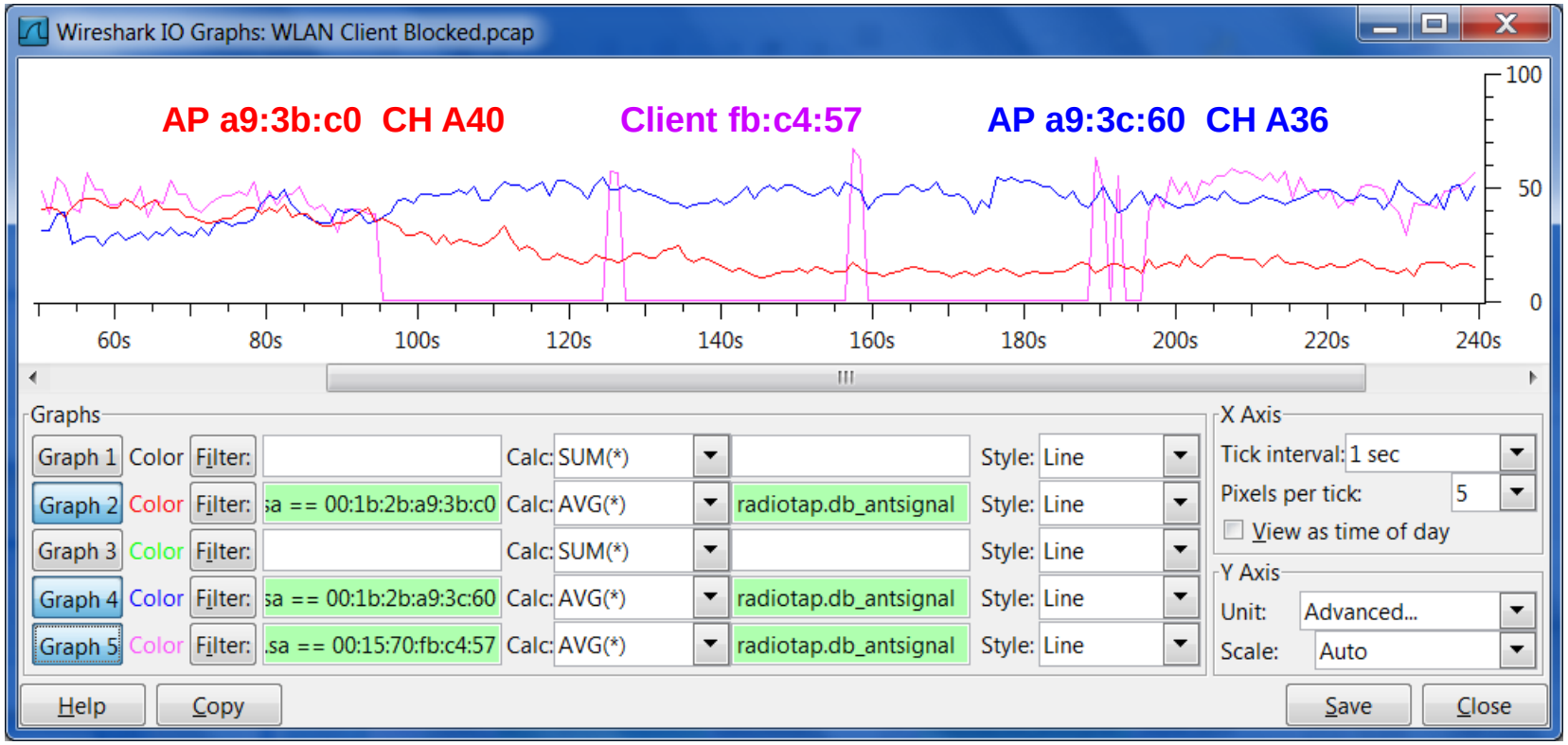
Client roaming problem

- 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

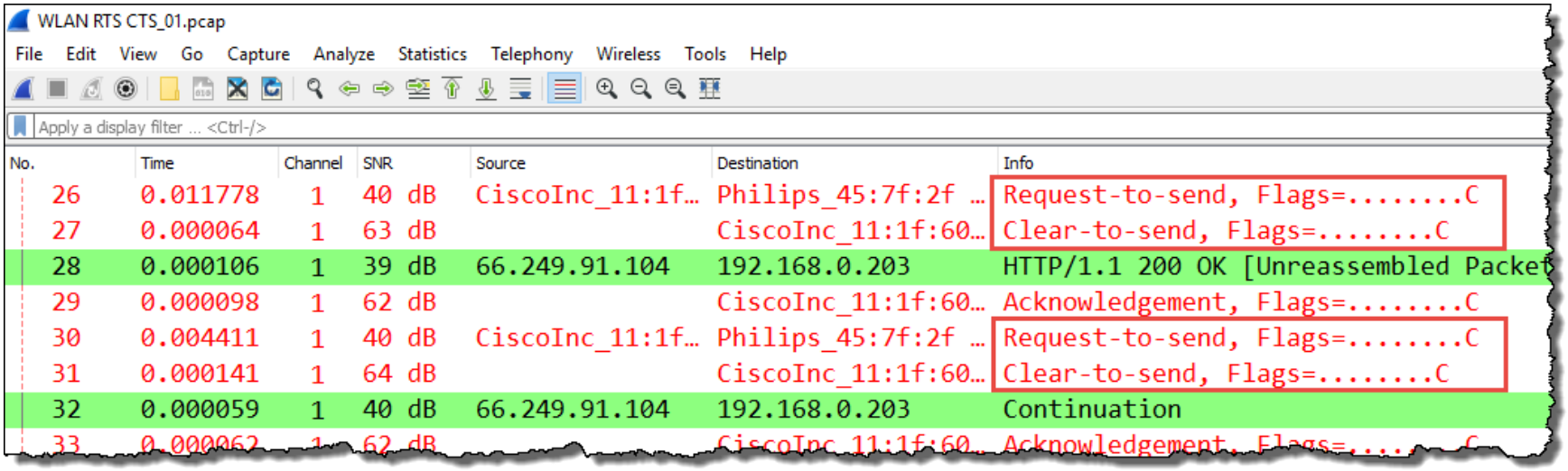
- Using IO Graph to show signal strength of different sources



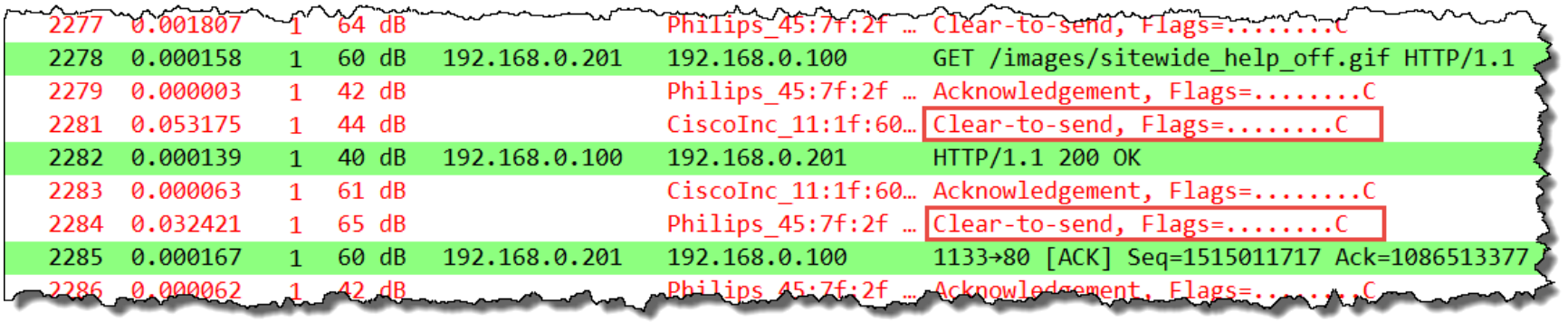
Graph 2 Color Filter: wlan.sa == 00:1b:2b:a9:3b:c0
Graph 4 Color Filter: wlan.sa == 00:1b:2b:a9:3c:60
Graph 5 Color Filter: wlan.sa == 00:15:70:fb:c4:57

Control Frames: Request to Send / Clear to Send

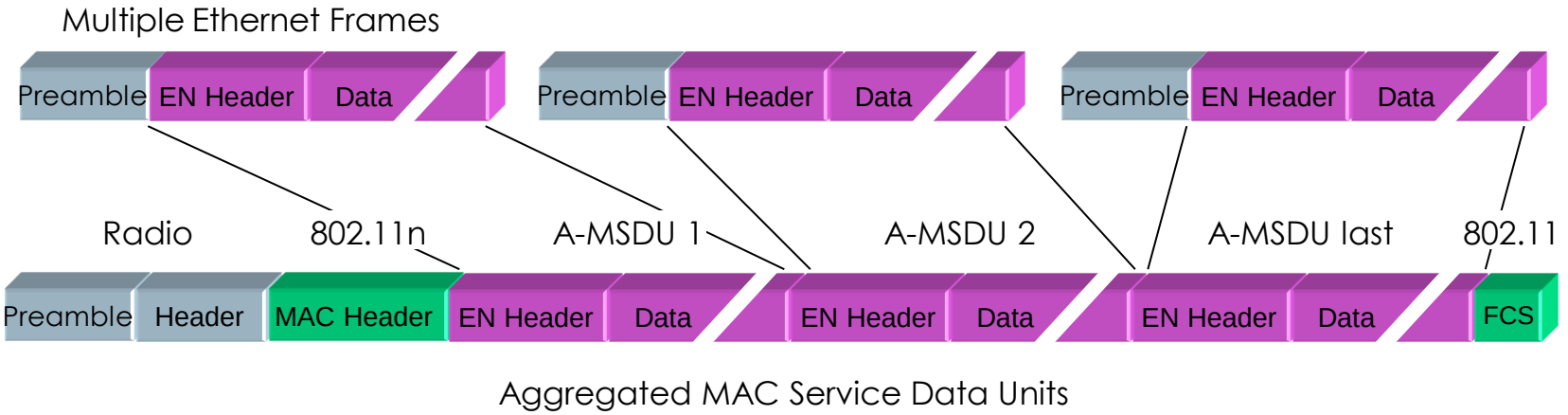
- A WLAN node can reserve airtime and refrain all other stations from sending
- RTS/CTS reservation is used in busy cells, Hidden Node situations or in mixed mode

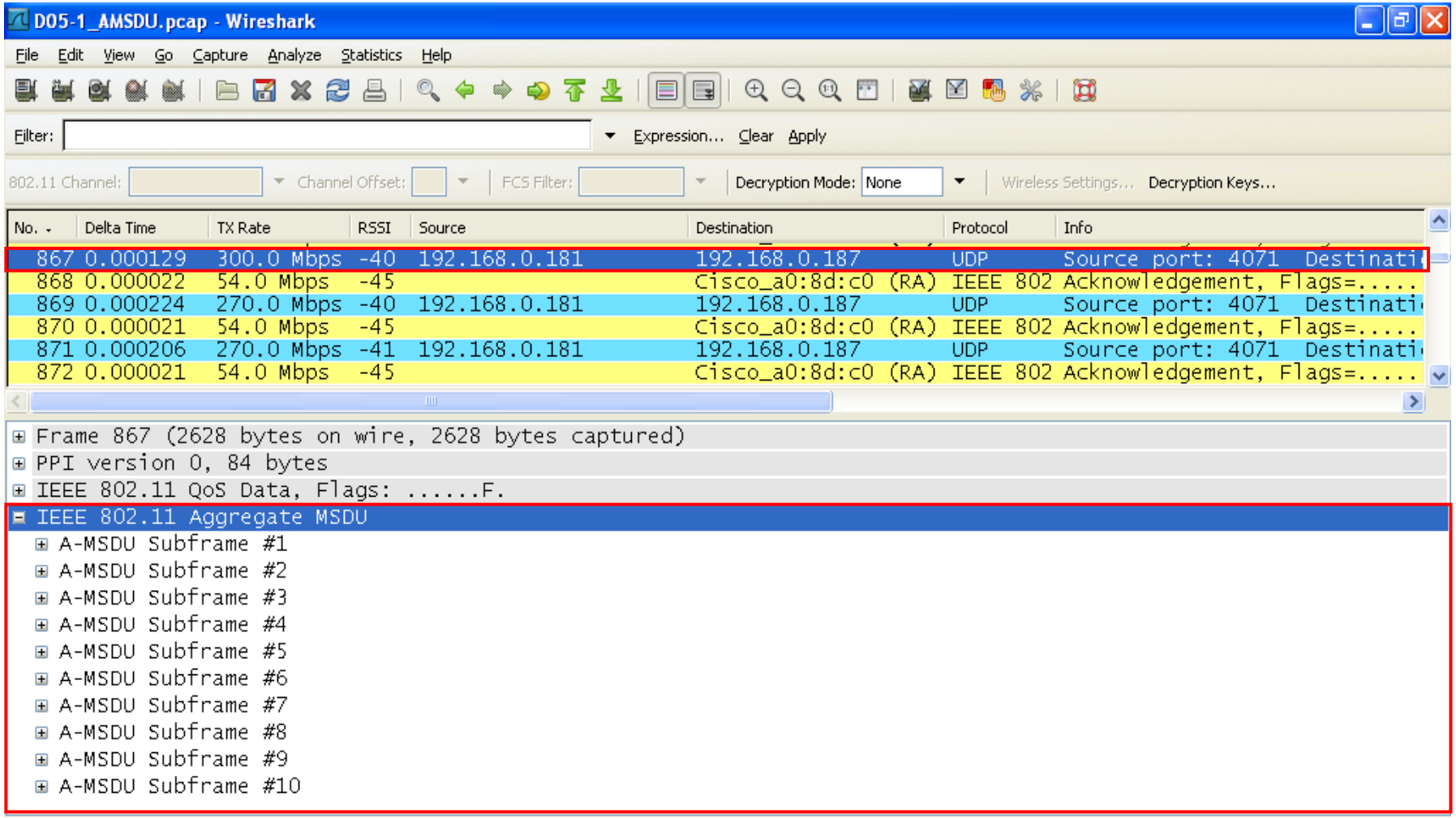


- A short form, so-called CTS-to-Self is often used in cells with B-Only clients present

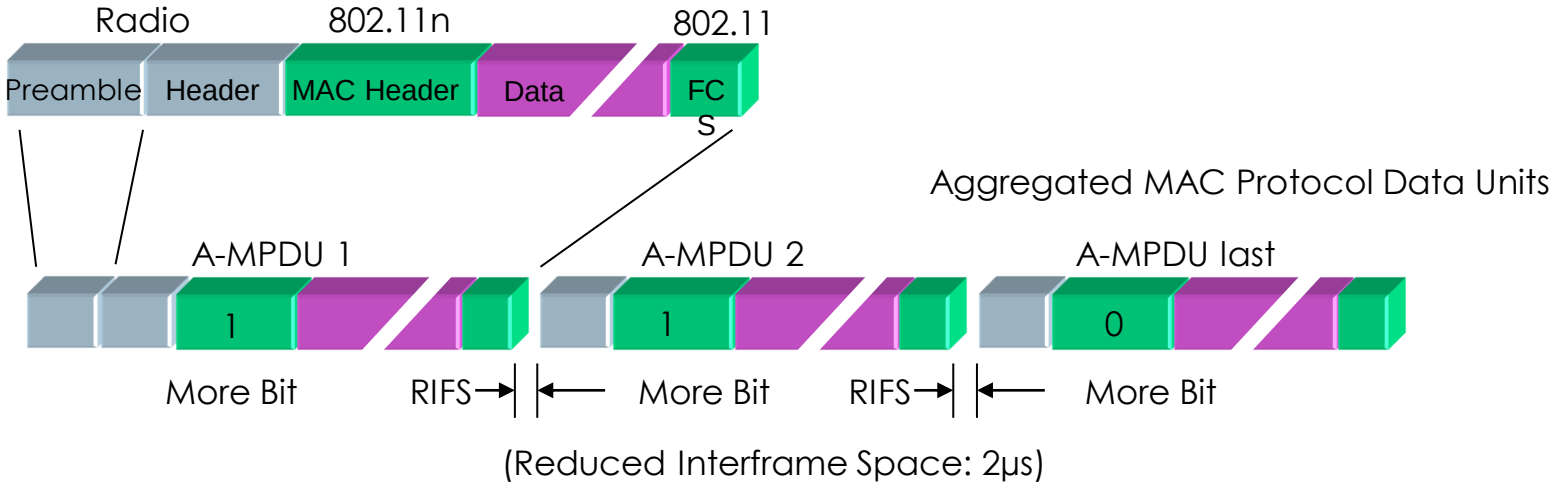


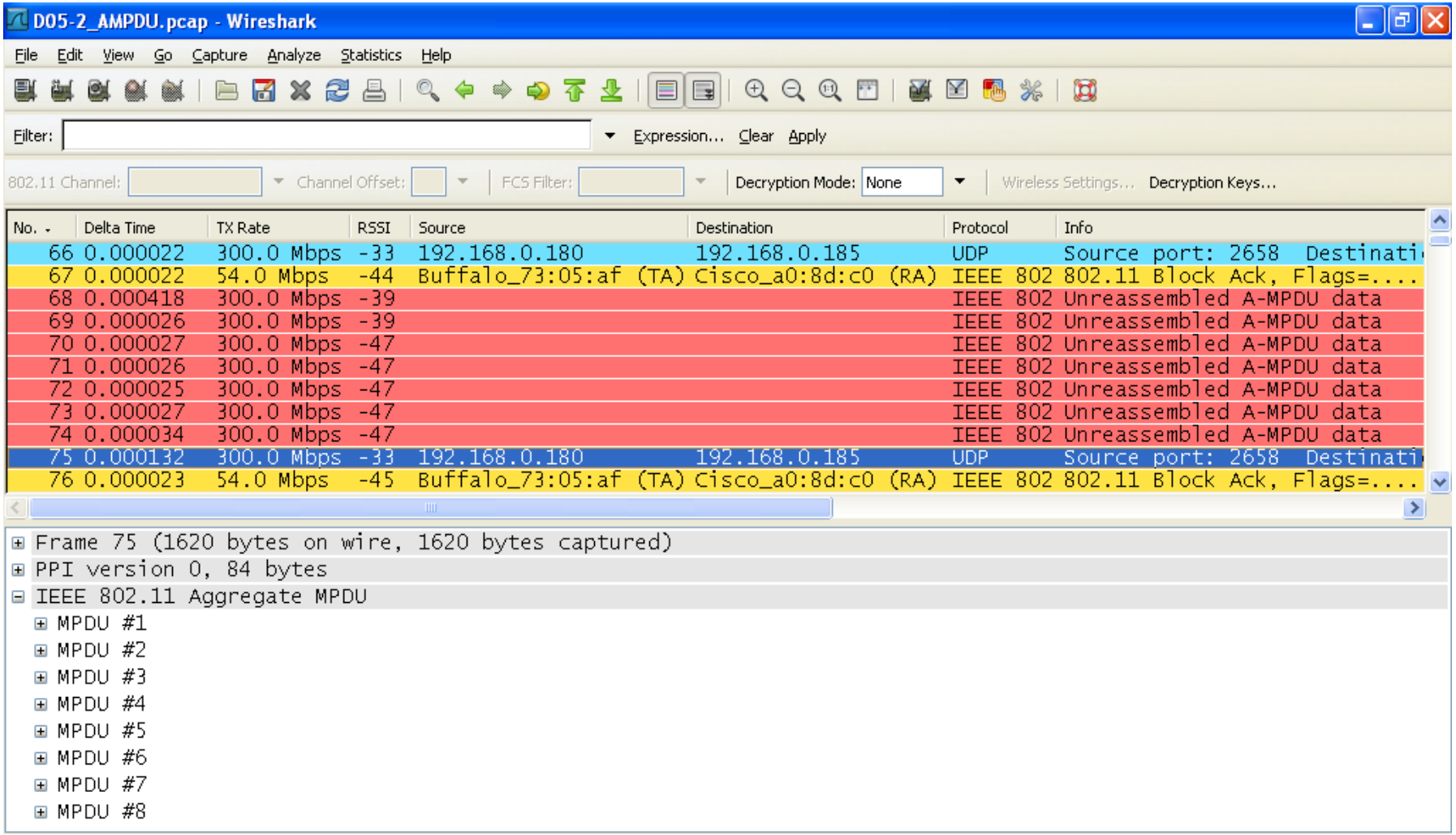
- Aggregate-MAC Service Data Unit (A-MSDU) wraps multiple Ethernet frames into one 802.11 frame up to 8KB size
- If frame has FCS error, the whole frame has to be retransmitted
- Not suitable for noisy environment

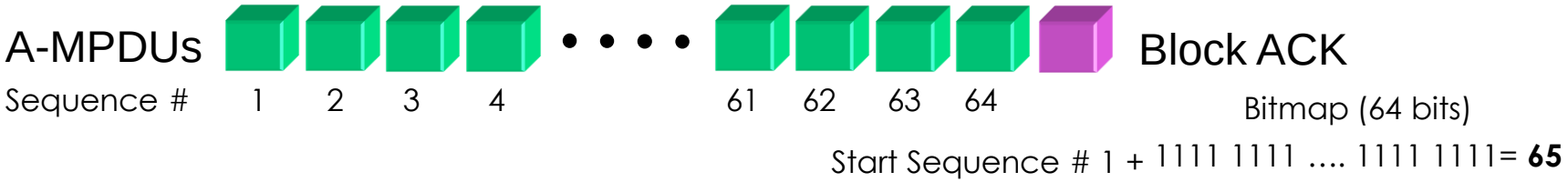


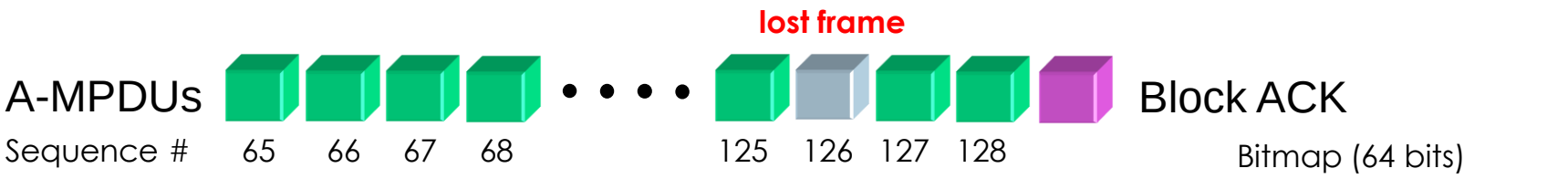

D05-1_AMSDU.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
802.11 Channel: Channel Offset: FCS Filter: Decryption Mode: None Wireless Settings... Decryption Keys...
No. Delta Time TX Rate RSSI Source Destination Protocol Info
867 0.000129 300.0 Mbps -40 192.168.0.181 192.168.0.187 UDP Source port: 4071 Destinati
868 0.000022 54.0 Mbps -45 Cisco_a0:8d:c0 (RA) IEEE 802 Acknowledgement, Flags=.....
869 0.000224 270.0 Mbps -40 192.168.0.181 192.168.0.187 UDP Source port: 4071 Destinati
870 0.000021 54.0 Mbps -45 Cisco_a0:8d:c0 (RA) IEEE 802 Acknowledgement, Flags=.....
871 0.000206 270.0 Mbps -41 192.168.0.181 192.168.0.187 UDP Source port: 4071 Destinati
872 0.000021 54.0 Mbps -45 Cisco_a0:8d:c0 (RA) IEEE 802 Acknowledgement, Flags=.....
Frame 867 (2628 bytes on wire, 2628 bytes captured)
PPI version 0, 84 bytes
IEEE 802.11 QoS Data, Flags: ......F.
IEEE 802.11 Aggregate MSDU
A-MSDU Subframe #1
A-MSDU Subframe #2
A-MSDU Subframe #3
A-MSDU Subframe #4
A-MSDU Subframe #5
A-MSDU Subframe #6
A-MSDU Subframe #7
A-MSDU Subframe #8
A-MSDU Subframe #9
A-MSDU Subframe #10

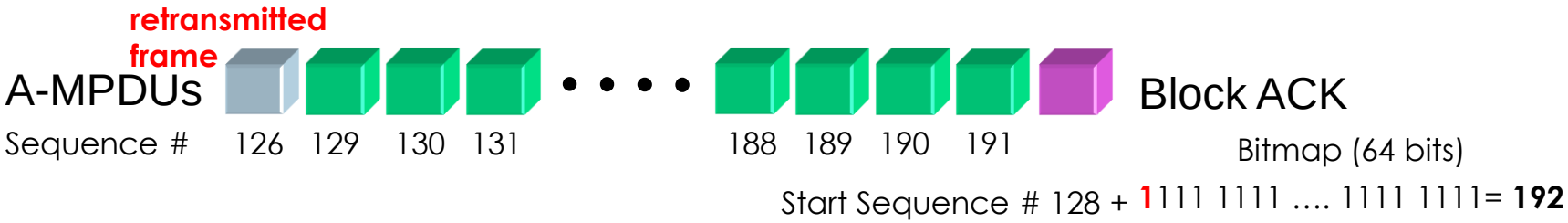
- Aggregate-MAC Protocol Data Unit (A-MPDU) allows bursting up to 64 802.11 frames
  - Reduced Interframe Space keeps receiver synchronized
  - New Block ACK allows to confirm up to 64 frames individually
  - Only bad frames need to be retransmitted



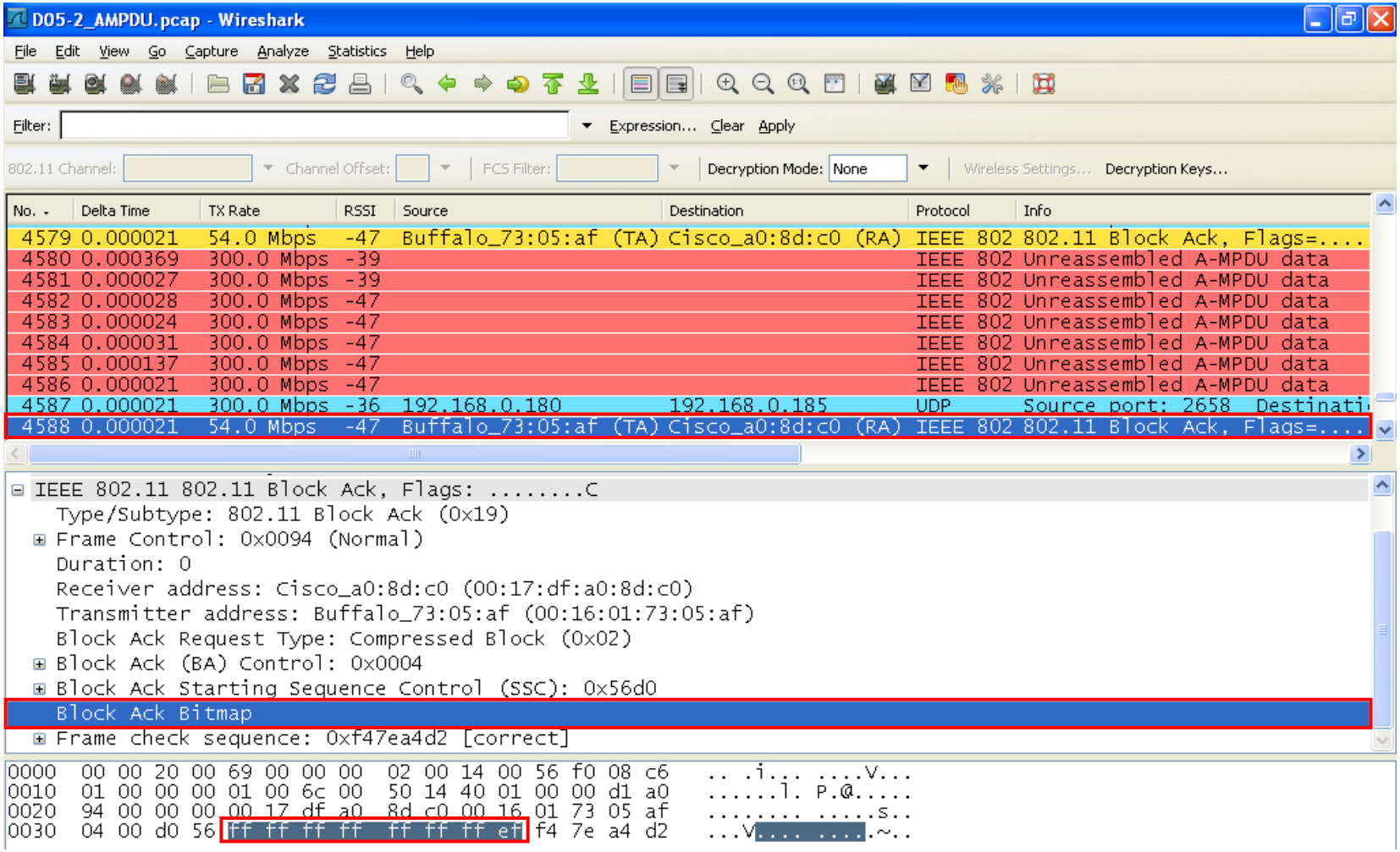

D05-2_AMPDU.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter: Expression... Clear Apply
802.11 Channel: Channel Offset: FCS Filter: Decryption Mode: None Wireless Settings... Decryption Keys...
No. Delta Time TX Rate RSSI Source Destination Protocol Info
66 0.000022 300.0 Mbps -33 192.168.0.180 192.168.0.185 UDP Source port: 2658 Destinati
67 0.000022 54.0 Mbps -44 Buffalo_73:05:af (TA) Cisco_a0:8d:c0 (RA) IEEE 802 802.11 Block Ack, Flags=....
68 0.000418 300.0 Mbps -39 IEEE 802 Unreassembled A-MPDU data
69 0.000026 300.0 Mbps -39 IEEE 802 Unreassembled A-MPDU data
70 0.000027 300.0 Mbps -47 IEEE 802 Unreassembled A-MPDU data
71 0.000026 300.0 Mbps -47 IEEE 802 Unreassembled A-MPDU data
72 0.000025 300.0 Mbps -47 IEEE 802 Unreassembled A-MPDU data
73 0.000027 300.0 Mbps -47 IEEE 802 Unreassembled A-MPDU data
74 0.000034 300.0 Mbps -47 IEEE 802 Unreassembled A-MPDU data
75 0.000132 300.0 Mbps -33 192.168.0.180 192.168.0.185 UDP Source port: 2658 Destinati
76 0.000023 54.0 Mbps -45 Buffalo_73:05:af (TA) Cisco_a0:8d:c0 (RA) IEEE 802 802.11 Block Ack, Flags=....
Frame 75 (1620 bytes on wire, 1620 bytes captured)
PPI version 0, 84 bytes
IEEE 802.11 Aggregate MPDU
MPDU #1
MPDU #2
MPDU #3
MPDU #4
MPDU #5
MPDU #6
MPDU #7
MPDU #8


A-MPDUs
Sequence #
1
2
3
4
61
62
63
64
Block ACK
Bitmap (64 bits)
Start Sequence # 1 + 1111 1111 …. 1111 1111= 65


lost frame
A-MPDUs
Sequence #
65
66
67
68
125
126
127
128
Block ACK
Bitmap (64 bits)
Start Sequence # 65 + 1111 1111 …. 1111 1011= 129


retransmitted frame
A-MPDUs
Sequence #
126
129
130
131
188
189
190
191
Block ACK
Bitmap (64 bits)
Start Sequence # 128 + 1111 1111 …. 1111 1111= 192

802.11n/ac Frame Aggregation A-MPDU Block-Ack



...ff ef = ...11111111 **1110**1111 indicates that **fourth-to-last** packet is missing

SharkFest '19 Europe

Hope you learned something useful!

WLAN Trainings with Wireshark & WaveXpert available all over Europe