SharkFest ‘16 Europe

Troubleshooting WLANs (Part 2)

Troubleshooting WLANs using 802.11 Management & Control Frames
19. October 2016

Welcome!

Rolf Leutert

Leutert NetServices
Switzerland
www.netsniffing.ch

#sf16eu

Introduction

LEUTERT NetServices

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

Sniffer Certified MASTER

Wireshark University WIRESHARK® CERTIFIED NETWORK ANALYST

Session Objectives

- 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

Licensed by iStockphoto.com

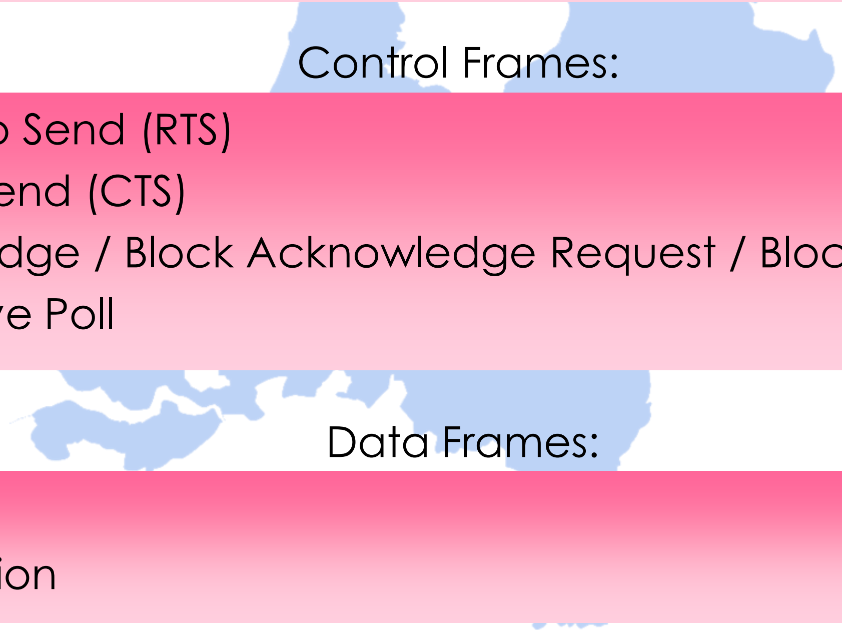
Troubleshooting WiFi requires a full understanding of all 802.11 Management & Control frames and its associated processes!

WLAN 802.11 Management, Control and Data Frames

802.11Frame Types Overview

Management Frames:

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



Control Frames:

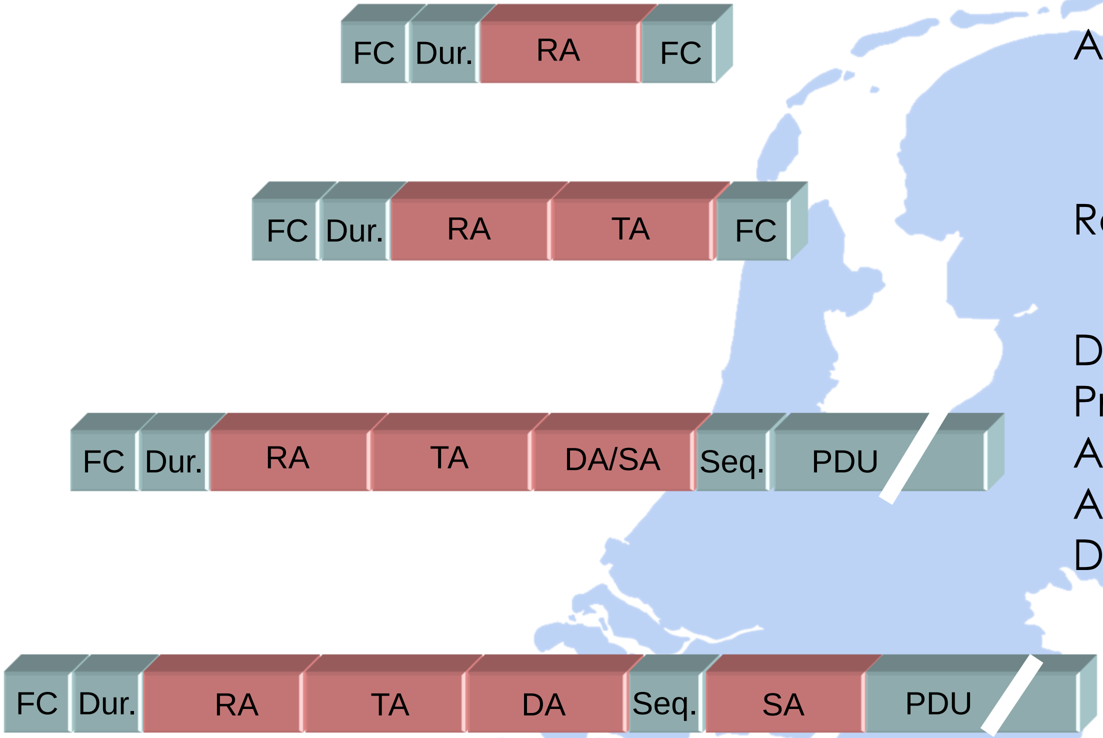
- Request to Send (RTS)
- Clear to Send (CTS)
- Acknowledge / Block Acknowledge Request / Block Acknowledge
- Power Save Poll

Data Frames:

- Data
- Null Function

The IEEE 802.11 Frame Formats

- Four different frame formats are used



FC, Dur., RA, FC

Acknowledge, Clear to Send

FC, Dur., RA, TA, FC

Request to Send

FC, Dur., RA, TA, DA/SA, Seq., PDU

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

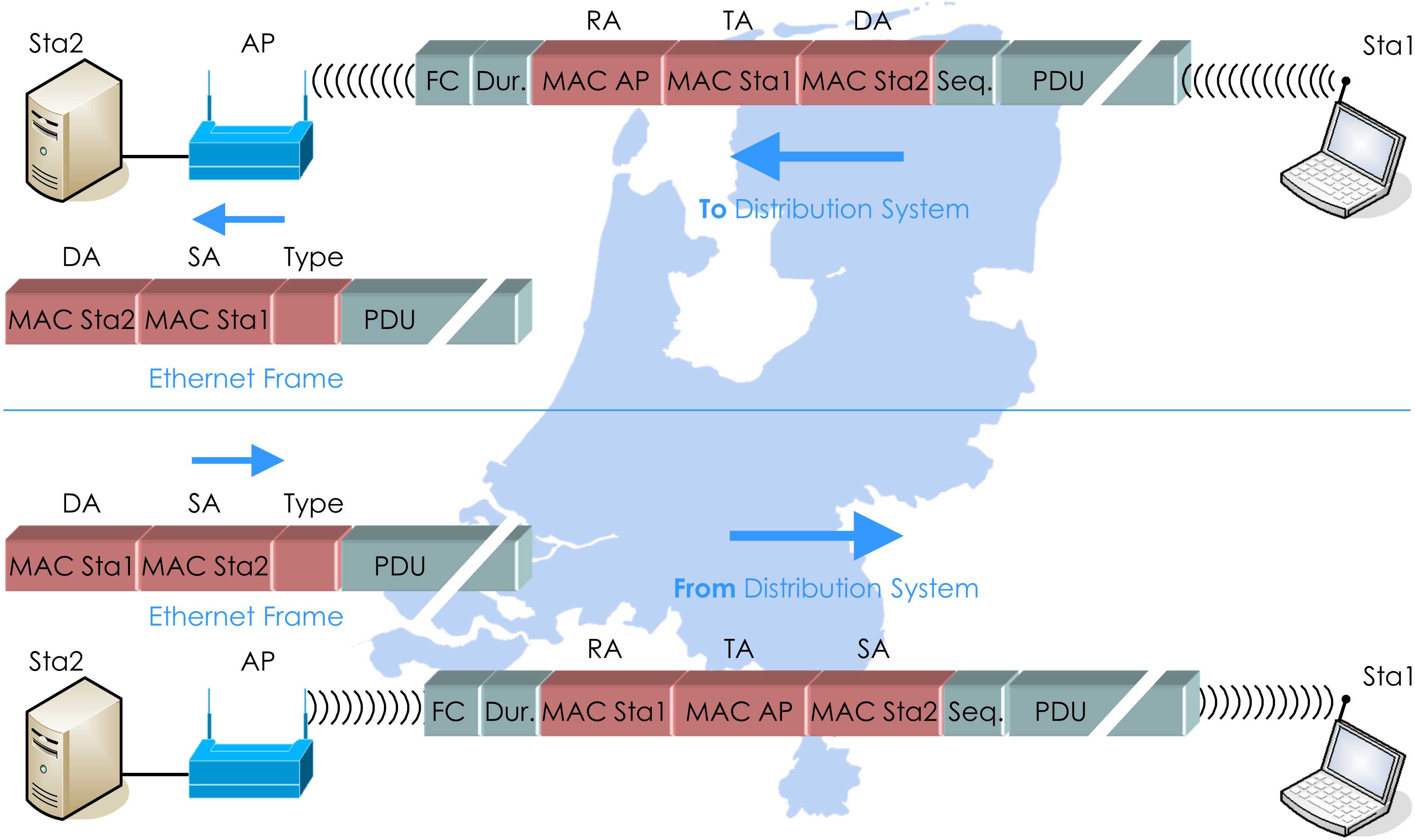
FC, Dur., RA, TA, DA, Seq., SA, PDU

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 Transmission

- WiFi data frames have three MAC address field



		RA	TA	DA		
FC	Dur.	MAC AP	MAC Sta1	MAC Sta2	Seq.	PDU

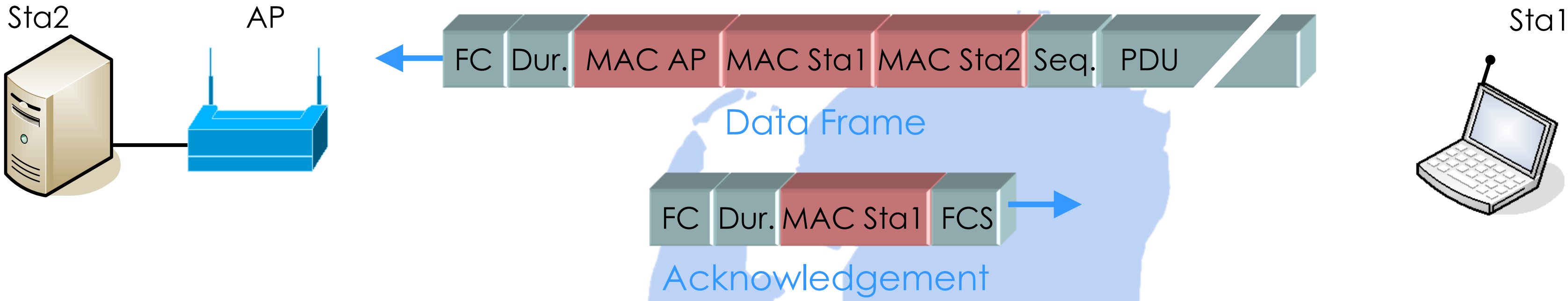
DA	SA	Type	
MAC Sta2	MAC Sta1		PDU

DA	SA	Type	
MAC Sta1	MAC Sta2		PDU

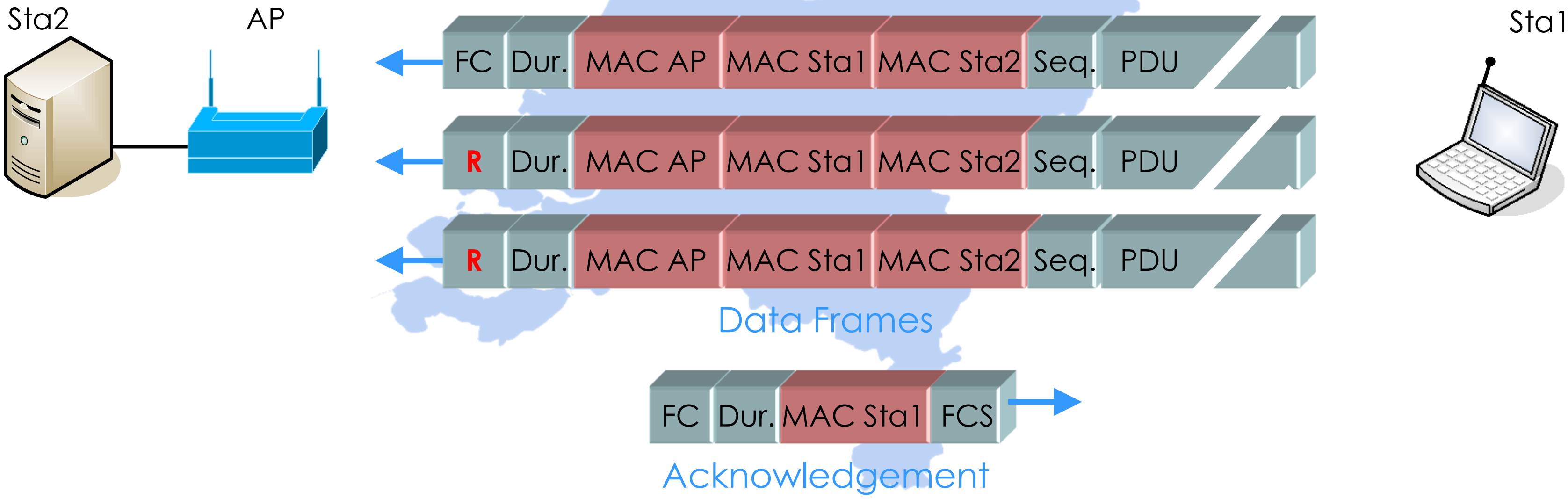
		RA	TA	SA		
FC	Dur.	MAC Sta1	MAC AP	MAC Sta2	Seq.	PDU

WiFi Data Transmission & Retransmission

- WiFi data frames are acknowledged or retransmitted

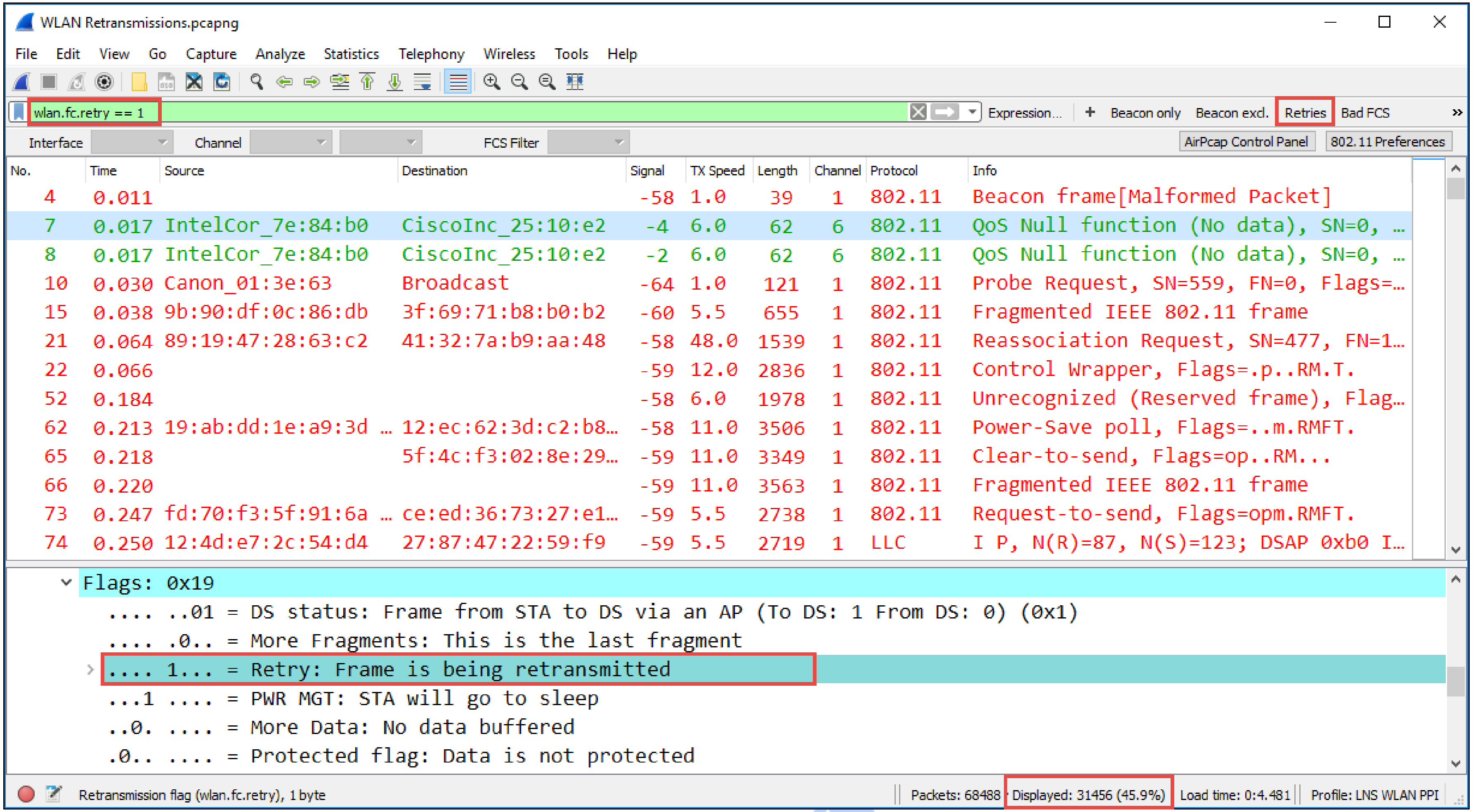


- All retransmitted frames are marked with the Retry Bit



WiFi Data Transmission & Retransmission

- All retransmitted frames are marked with the Retry Bit



WLAN Retransmissions.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Expression…
+ Beacon only Beacon excl. Retries Bad FCS
Interface Channel FCS Filter
AirPcap Control Panel 802.11 Preferences

wlan.fc.retry == 1

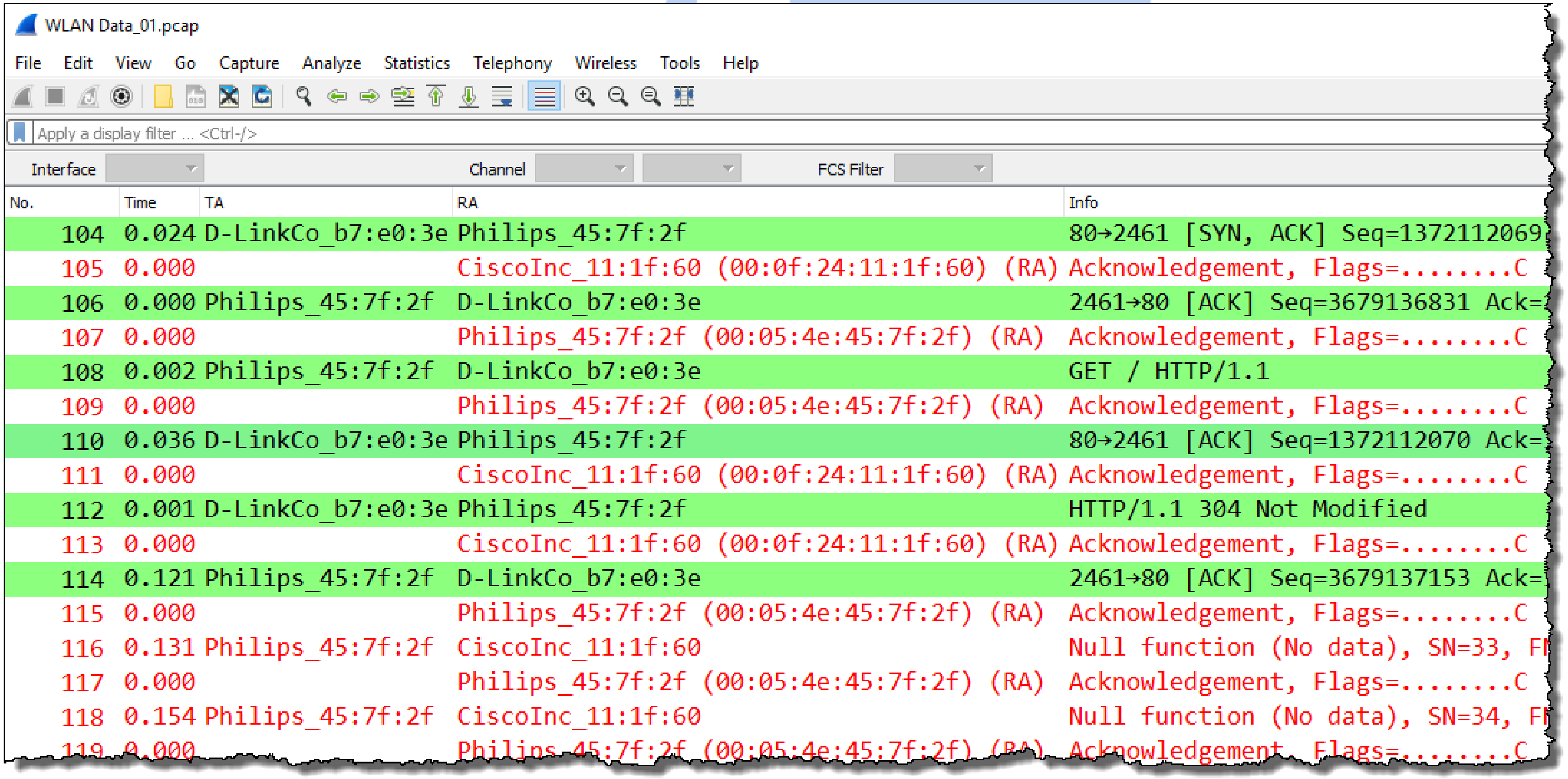
No.	Time	Source	Destination	Signal	TX Speed	Length	Channel	Protocol	Info
4	0.011			-58	1.0	39	1	802.11	Beacon frame[Malformed Packet]
7	0.017	IntelCor_7e:84:b0	CiscoInc_25:10:e2	-4	6.0	62	6	802.11	QoS Null function (No data), SN=0, …
8	0.017	IntelCor_7e:84:b0	CiscoInc_25:10:e2	-2	6.0	62	6	802.11	QoS 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

WiFi Data Transmission

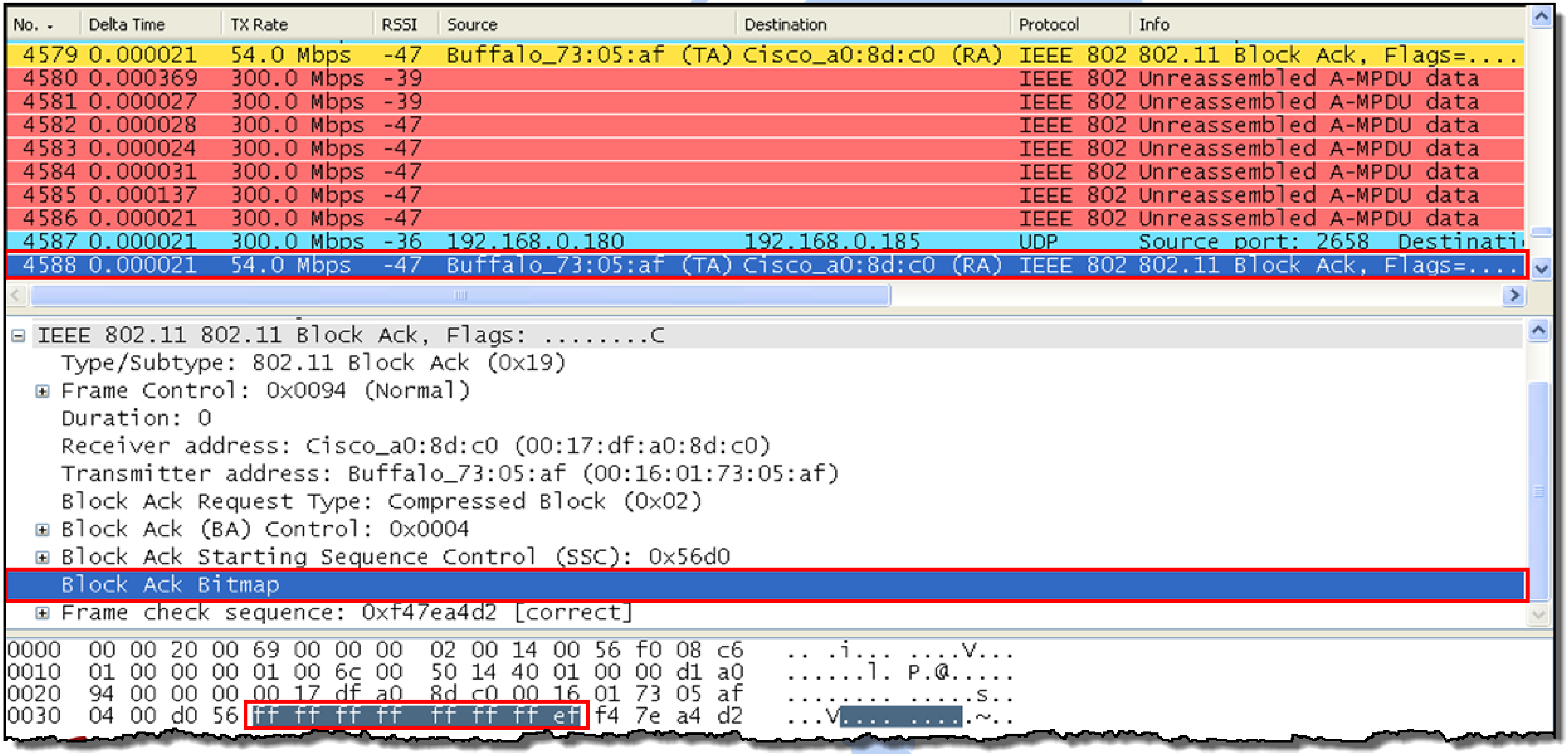
- In non-aggregation mode each packet is acknowledged individually
- The acknowledge frame follows immediately after each data frame
- The (single) acknowledge has no source address field


WLAN Data_01.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Interface
Channel
FCS Filter

No.	Time	TA	RA	Info
104	0.024	D-LinkCo_b7:e0:3e	Philips_45:7f:2f	80→2461 [SYN, ACK] Seq=1372112069
105	0.000		CiscoInc_11:1f:60 (00:0f:24:11:1f:60) (RA)	Acknowledgement, Flags=........C
106	0.000	Philips_45:7f:2f	D-LinkCo_b7:e0:3e	2461→80 [ACK] Seq=3679136831 Ack=
107	0.000		Philips_45:7f:2f (00:05:4e:45:7f:2f) (RA)	Acknowledgement, Flags=........C
108	0.002	Philips_45:7f:2f	D-LinkCo_b7:e0:3e	GET / HTTP/1.1
109	0.000		Philips_45:7f:2f (00:05:4e:45:7f:2f) (RA)	Acknowledgement, Flags=........C
110	0.036	D-LinkCo_b7:e0:3e	Philips_45:7f:2f	80→2461 [ACK] Seq=1372112070 Ack=
111	0.000		CiscoInc_11:1f:60 (00:0f:24:11:1f:60) (RA)	Acknowledgement, Flags=........C
112	0.001	D-LinkCo_b7:e0:3e	Philips_45:7f:2f	HTTP/1.1 304 Not Modified
113	0.000		CiscoInc_11:1f:60 (00:0f:24:11:1f:60) (RA)	Acknowledgement, Flags=........C
114	0.121	Philips_45:7f:2f	D-LinkCo_b7:e0:3e	2461→80 [ACK] Seq=3679137153 Ack=
115	0.000		Philips_45:7f:2f (00:05:4e:45:7f:2f) (RA)	Acknowledgement, Flags=........C
116	0.131	Philips_45:7f:2f	CiscoInc_11:1f:60	Null function (No data), SN=33, FN
117	0.000		Philips_45:7f:2f (00:05:4e:45:7f:2f) (RA)	Acknowledgement, Flags=........C
118	0.154	Philips_45:7f:2f	CiscoInc_11:1f:60	Null function (No data), SN=34, FN
119	0.000		Philips_45:7f:2f (00:05:4e:45:7f:2f) (RA)	Acknowledgement, Flags=........C

WiFi Data Transmission

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



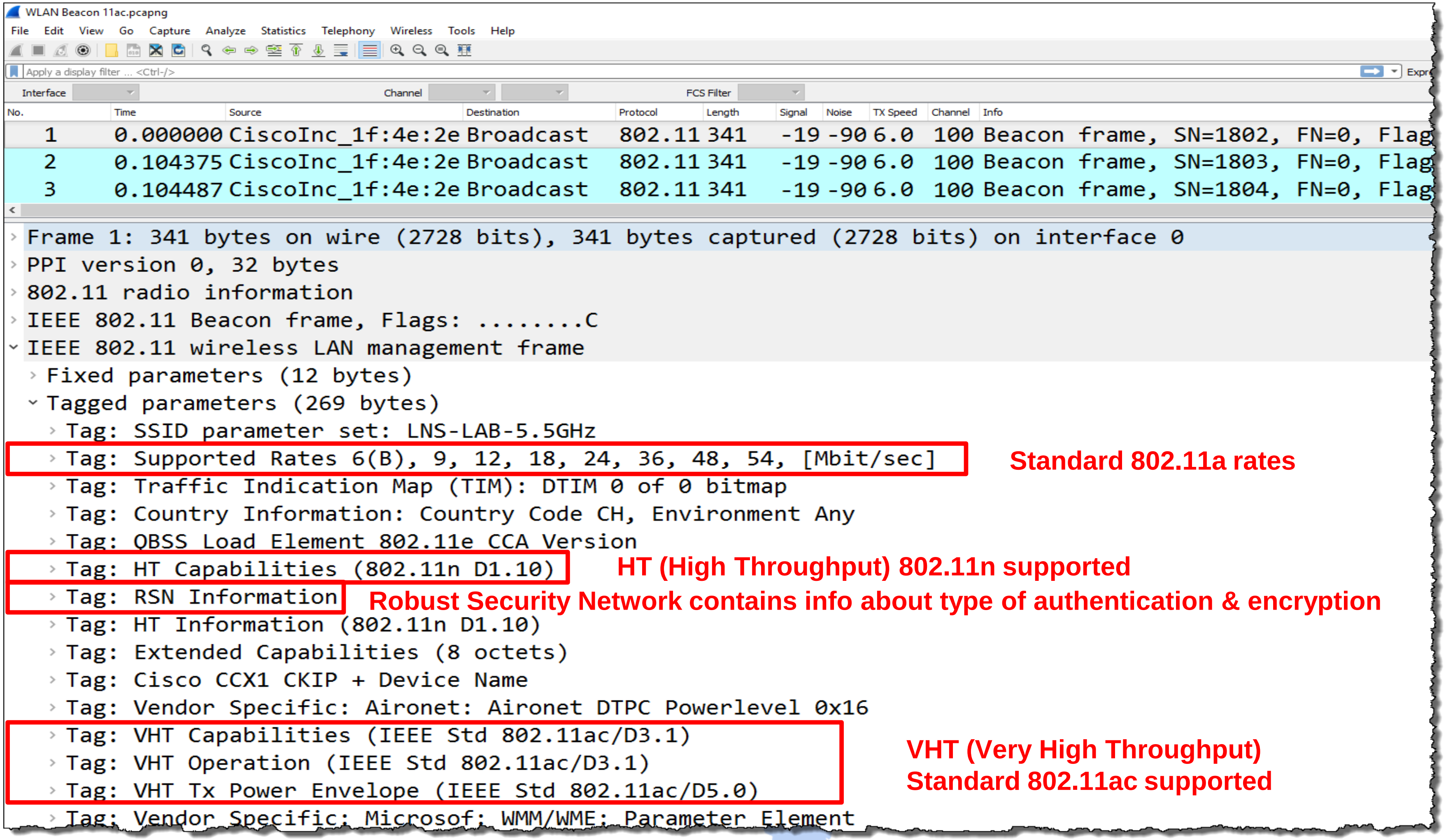
```
No.  Delta Time  TX Rate      RSSI  Source                   Destination               Protocol  Info
4579 0.000021    54.0 Mbps    -47   Buffalo_73:05:af (TA)   Cisco_a0:8d:c0 (RA)      IEEE 802  802.11 Block Ack, Flags=....
4580 0.000369    300.0 Mbps   -39                                                      IEEE 802  Unreassembled A-MPDU data
4581 0.000027    300.0 Mbps   -39                                                      IEEE 802  Unreassembled A-MPDU data
4582 0.000028    300.0 Mbps   -47                                                      IEEE 802  Unreassembled A-MPDU data
4583 0.000024    300.0 Mbps   -47                                                      IEEE 802  Unreassembled A-MPDU data
4584 0.000031    300.0 Mbps   -47                                                      IEEE 802  Unreassembled A-MPDU data
4585 0.000137    300.0 Mbps   -47                                                      IEEE 802  Unreassembled A-MPDU data
4586 0.000021    300.0 Mbps   -47                                                      IEEE 802  Unreassembled A-MPDU data
4587 0.000021    300.0 Mbps   -36   192.168.0.180            192.168.0.185             UDP       Source port: 2658  Destinati
4588 0.000021    54.0 Mbps    -47   Buffalo_73:05:af (TA)   Cisco_a0:8d:c0 (RA)      IEEE 802  802.11 Block Ack, Flags=....
```

```
⊟ IEEE 802.11 802.11 Block Ack, Flags: ........C
    Type/Subtype: 802.11 Block Ack (0x19)
  ⊞ Frame Control: 0x0094 (Normal)
    Duration: 0
    Receiver address: Cisco_a0:8d:c0 (00:17:df:a0:8d:c0)
    Transmitter address: Buffalo_73:05:af (00:16:01:73:05:af)
    Block Ack Request Type: Compressed Block (0x02)
  ⊞ Block Ack (BA) Control: 0x0004
  ⊞ Block Ack Starting Sequence Control (SSC): 0x56d0
    Block Ack Bitmap
  ⊞ Frame check sequence: 0xf47ea4d2 [correct]
```

```
0000  00 00 20 00 69 00 00 00  02 00 14 00 56 f0 08 c6   .. .i...  ....V...
0010  01 00 00 00 01 00 6c 00  50 14 40 01 00 00 d1 a0   ......l.  P.@.....
0020  94 00 00 00 00 17 df a0  8d c0 00 16 01 73 05 af   ........  .....s..
0030  04 00 d0 56 ff ff ff ff  ff ff ff ef f4 7e a4 d2   ...V....  .....~..
```

Management Frame: Beacon

- Beacon tags contain information about supported and required features



No.	Time	Source	Destination	Protocol	Length	Signal	Noise	TX Speed	Channel	Info
1	0.000000	CiscoInc_1f:4e:2e	Broadcast	802.11	341	-19	-90	6.0	100	Beacon frame, SN=1802, FN=0, Flag
2	0.104375	CiscoInc_1f:4e:2e	Broadcast	802.11	341	-19	-90	6.0	100	Beacon frame, SN=1803, FN=0, Flag
3	0.104487	CiscoInc_1f:4e:2e	Broadcast	802.11	341	-19	-90	6.0	100	Beacon frame, SN=1804, FN=0, Flag

```
> Frame 1: 341 bytes on wire (2728 bits), 341 bytes captured (2728 bits) on interface 0
> PPI version 0, 32 bytes
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: ........C
v IEEE 802.11 wireless LAN management frame
  > Fixed parameters (12 bytes)
  v Tagged parameters (269 bytes)
    > Tag: SSID parameter set: LNS-LAB-5.5GHz
    > Tag: Supported Rates 6(B), 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
    > Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
    > Tag: Country Information: Country Code CH, Environment Any
    > Tag: QBSS Load Element 802.11e CCA Version
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: RSN Information
    > Tag: HT Information (802.11n D1.10)
    > Tag: Extended Capabilities (8 octets)
    > Tag: Cisco CCX1 CKIP + Device Name
    > Tag: Vendor Specific: Aironet: Aironet DTPC Powerlevel 0x16
    > Tag: VHT Capabilities (IEEE Std 802.11ac/D3.1)
    > Tag: VHT Operation (IEEE Std 802.11ac/D3.1)
    > Tag: VHT Tx Power Envelope (IEEE Std 802.11ac/D5.0)
    > Tag: Vendor Specific: Microsof: WMM/WME: Parameter Element
```

Standard 802.11a rates

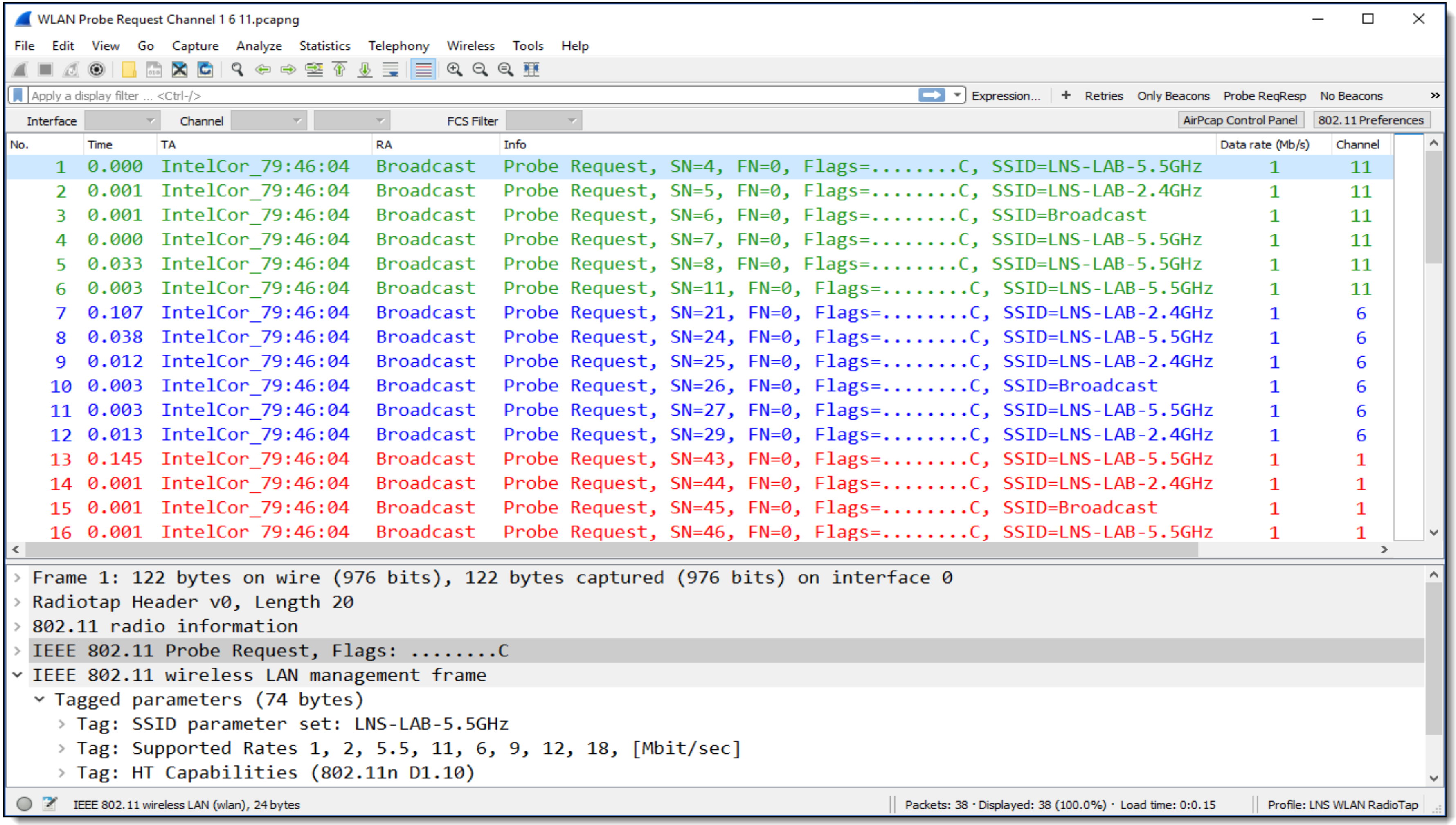
HT (High Throughput) 802.11n supported

Robust Security Network contains info about type of authentication & encryption

**VHT (Very High Throughput)
Standard 802.11ac supported**

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


WLAN Probe Request Channel 1 6 11.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+
Retries
Only Beacons
Probe ReqResp
No Beacons
Interface
Channel
FCS Filter
AirPcap Control Panel
802.11 Preferences

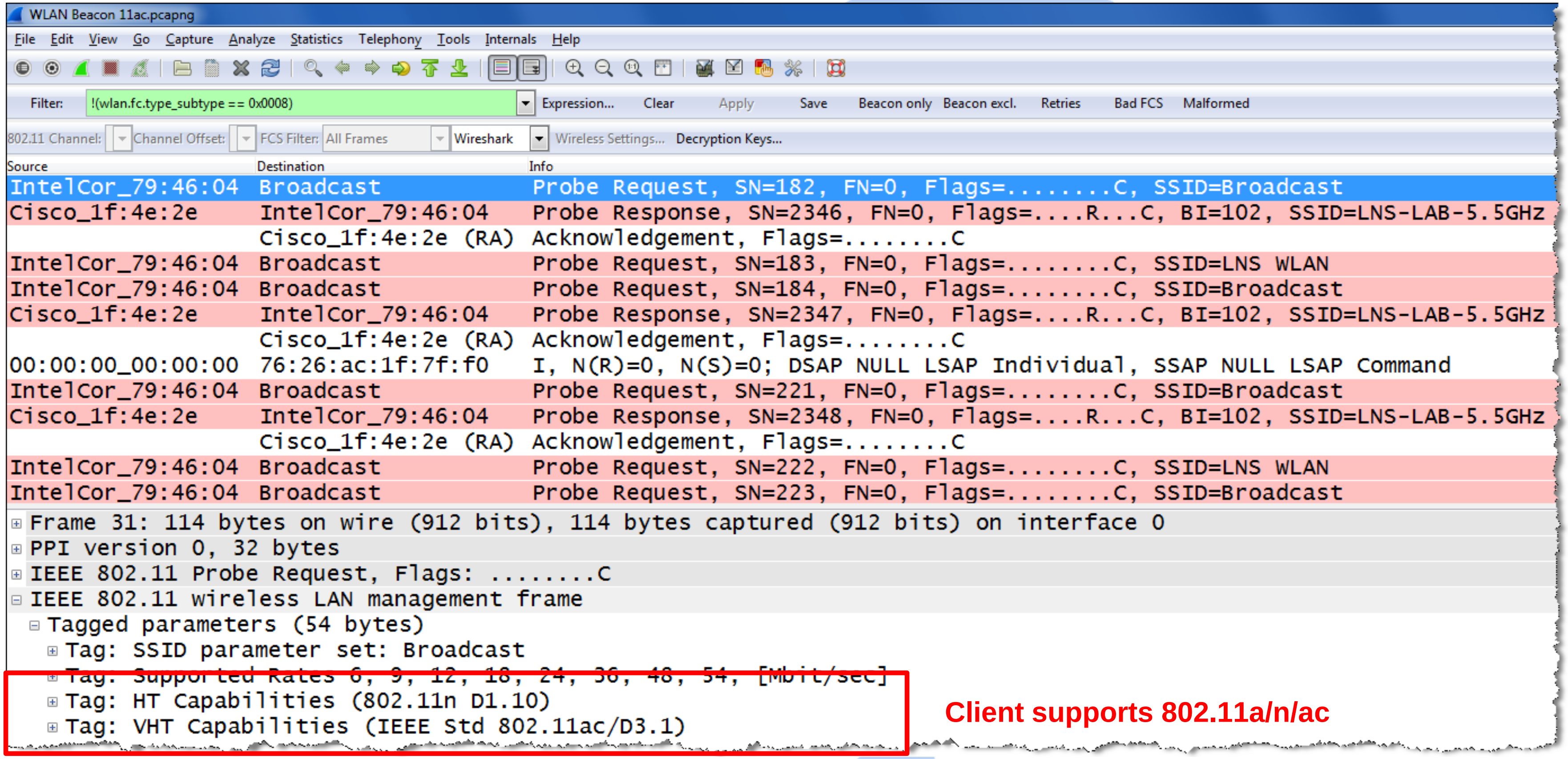
No.	Time	TA	RA	Info	Data rate (Mb/s)	Channel
1	0.000	IntelCor_79:46:04	Broadcast	Probe Request, SN=4, FN=0, Flags=........C, SSID=LNS-LAB-5.5GHz	1	11
2	0.001	IntelCor_79:46:04	Broadcast	Probe Request, SN=5, FN=0, Flags=........C, SSID=LNS-LAB-2.4GHz	1	11
3	0.001	IntelCor_79:46:04	Broadcast	Probe Request, SN=6, FN=0, Flags=........C, SSID=Broadcast	1	11
4	0.000	IntelCor_79:46:04	Broadcast	Probe Request, SN=7, FN=0, Flags=........C, SSID=LNS-LAB-5.5GHz	1	11
5	0.033	IntelCor_79:46:04	Broadcast	Probe Request, SN=8, FN=0, Flags=........C, SSID=LNS-LAB-5.5GHz	1	11
6	0.003	IntelCor_79:46:04	Broadcast	Probe Request, SN=11, FN=0, Flags=........C, SSID=LNS-LAB-5.5GHz	1	11
7	0.107	IntelCor_79:46:04	Broadcast	Probe Request, SN=21, FN=0, Flags=........C, SSID=LNS-LAB-2.4GHz	1	6
8	0.038	IntelCor_79:46:04	Broadcast	Probe Request, SN=24, FN=0, Flags=........C, SSID=LNS-LAB-5.5GHz	1	6
9	0.012	IntelCor_79:46:04	Broadcast	Probe Request, SN=25, FN=0, Flags=........C, SSID=LNS-LAB-2.4GHz	1	6
10	0.003	IntelCor_79:46:04	Broadcast	Probe Request, SN=26, FN=0, Flags=........C, SSID=Broadcast	1	6
11	0.003	IntelCor_79:46:04	Broadcast	Probe Request, SN=27, FN=0, Flags=........C, SSID=LNS-LAB-5.5GHz	1	6
12	0.013	IntelCor_79:46:04	Broadcast	Probe Request, SN=29, FN=0, Flags=........C, SSID=LNS-LAB-2.4GHz	1	6
13	0.145	IntelCor_79:46:04	Broadcast	Probe Request, SN=43, FN=0, Flags=........C, SSID=LNS-LAB-5.5GHz	1	1
14	0.001	IntelCor_79:46:04	Broadcast	Probe Request, SN=44, FN=0, Flags=........C, SSID=LNS-LAB-2.4GHz	1	1
15	0.001	IntelCor_79:46:04	Broadcast	Probe Request, SN=45, FN=0, Flags=........C, SSID=Broadcast	1	1
16	0.001	IntelCor_79:46:04	Broadcast	Probe Request, SN=46, FN=0, Flags=........C, SSID=LNS-LAB-5.5GHz	1	1

```
> Frame 1: 122 bytes on wire (976 bits), 122 bytes captured (976 bits) on interface 0
> Radiotap Header v0, Length 20
> 802.11 radio information
> IEEE 802.11 Probe Request, Flags: ........C
v IEEE 802.11 wireless LAN management frame
  v Tagged parameters (74 bytes)
    > Tag: SSID parameter set: LNS-LAB-5.5GHz
    > Tag: Supported Rates 1, 2, 5.5, 11, 6, 9, 12, 18, [Mbit/sec]
    > Tag: HT Capabilities (802.11n D1.10)
```

IEEE 802.11 wireless LAN (wlan), 24 bytes | Packets: 38 · Displayed: 38 (100.0%) · Load time: 0:0.15 | Profile: LNS WLAN RadioTap

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


WLAN Beacon 11ac.pcapng
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save Beacon only Beacon excl. Retries Bad FCS Malformed
802.11 Channel: Channel Offset: Wireless Settings... Decryption Keys...

Filter: !(wlan.fc.type_subtype == 0x0008)

FCS Filter: All Frames Wireshark

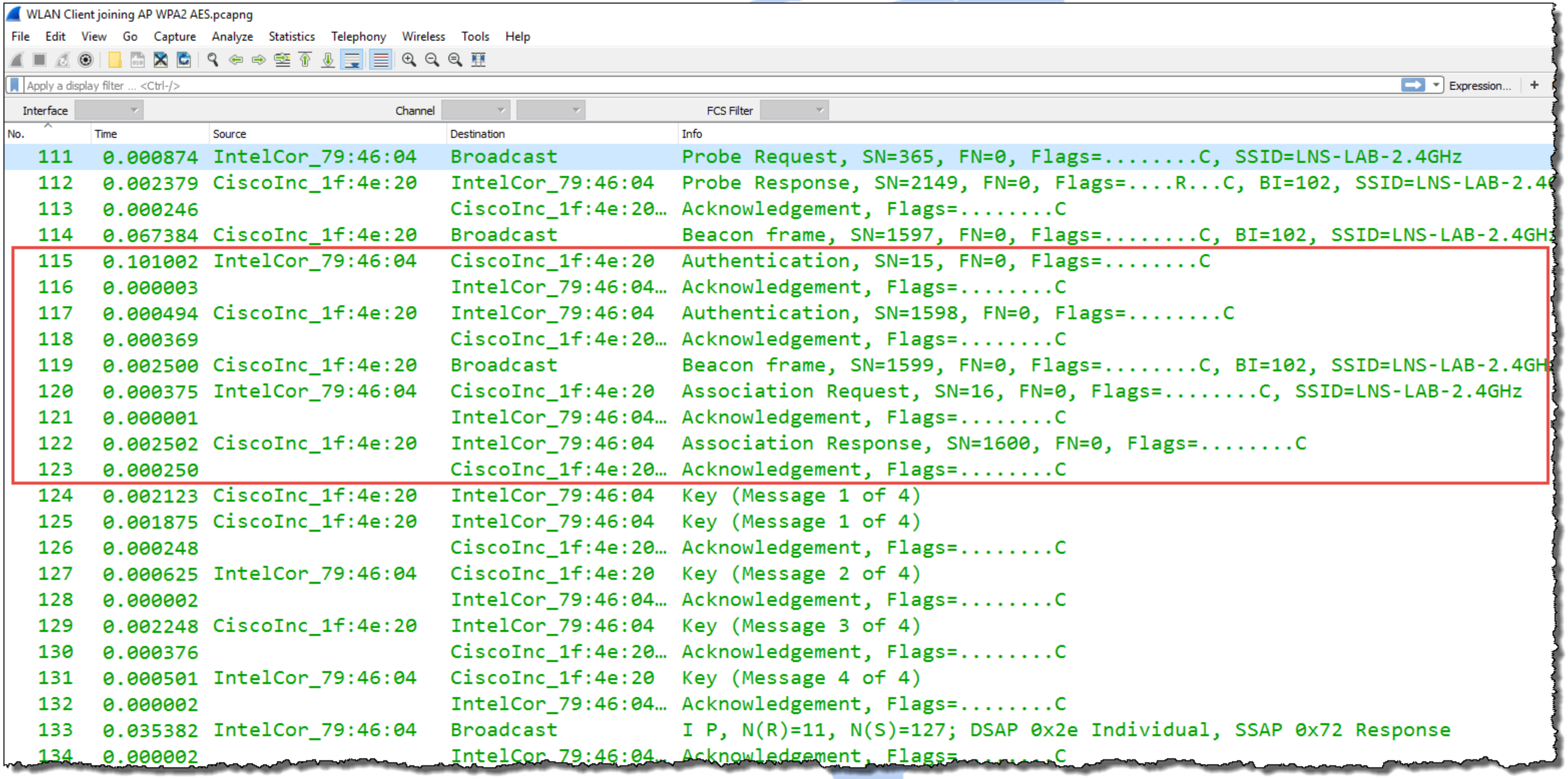
```
Source             Destination           Info
IntelCor_79:46:04  Broadcast             Probe Request, SN=182, FN=0, Flags=........C, SSID=Broadcast
Cisco_1f:4e:2e     IntelCor_79:46:04     Probe Response, SN=2346, FN=0, Flags=....R...C, BI=102, SSID=LNS-LAB-5.5GHz
                   Cisco_1f:4e:2e (RA)   Acknowledgement, Flags=........C
IntelCor_79:46:04  Broadcast             Probe Request, SN=183, FN=0, Flags=........C, SSID=LNS WLAN
IntelCor_79:46:04  Broadcast             Probe Request, SN=184, FN=0, Flags=........C, SSID=Broadcast
Cisco_1f:4e:2e     IntelCor_79:46:04     Probe Response, SN=2347, FN=0, Flags=....R...C, BI=102, SSID=LNS-LAB-5.5GHz
                   Cisco_1f:4e:2e (RA)   Acknowledgement, Flags=........C
00:00:00_00:00:00  76:26:ac:1f:7f:f0     I, N(R)=0, N(S)=0; DSAP NULL LSAP Individual, SSAP NULL LSAP Command
IntelCor_79:46:04  Broadcast             Probe Request, SN=221, FN=0, Flags=........C, SSID=Broadcast
Cisco_1f:4e:2e     IntelCor_79:46:04     Probe Response, SN=2348, FN=0, Flags=....R...C, BI=102, SSID=LNS-LAB-5.5GHz
                   Cisco_1f:4e:2e (RA)   Acknowledgement, Flags=........C
IntelCor_79:46:04  Broadcast             Probe Request, SN=222, FN=0, Flags=........C, SSID=LNS WLAN
IntelCor_79:46:04  Broadcast             Probe Request, SN=223, FN=0, Flags=........C, SSID=Broadcast
```

```
⊞ Frame 31: 114 bytes on wire (912 bits), 114 bytes captured (912 bits) on interface 0
⊞ PPI version 0, 32 bytes
⊞ IEEE 802.11 Probe Request, Flags: ........C
⊟ IEEE 802.11 wireless LAN management frame
  ⊟ Tagged parameters (54 bytes)
    ⊞ Tag: SSID parameter set: Broadcast
    ⊞ Tag: Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
    ⊞ Tag: HT Capabilities (802.11n D1.10)
    ⊞ Tag: VHT Capabilities (IEEE Std 802.11ac/D3.1)
```

Client supports 802.11a/n/ac

Management Frames: Authentication & Association

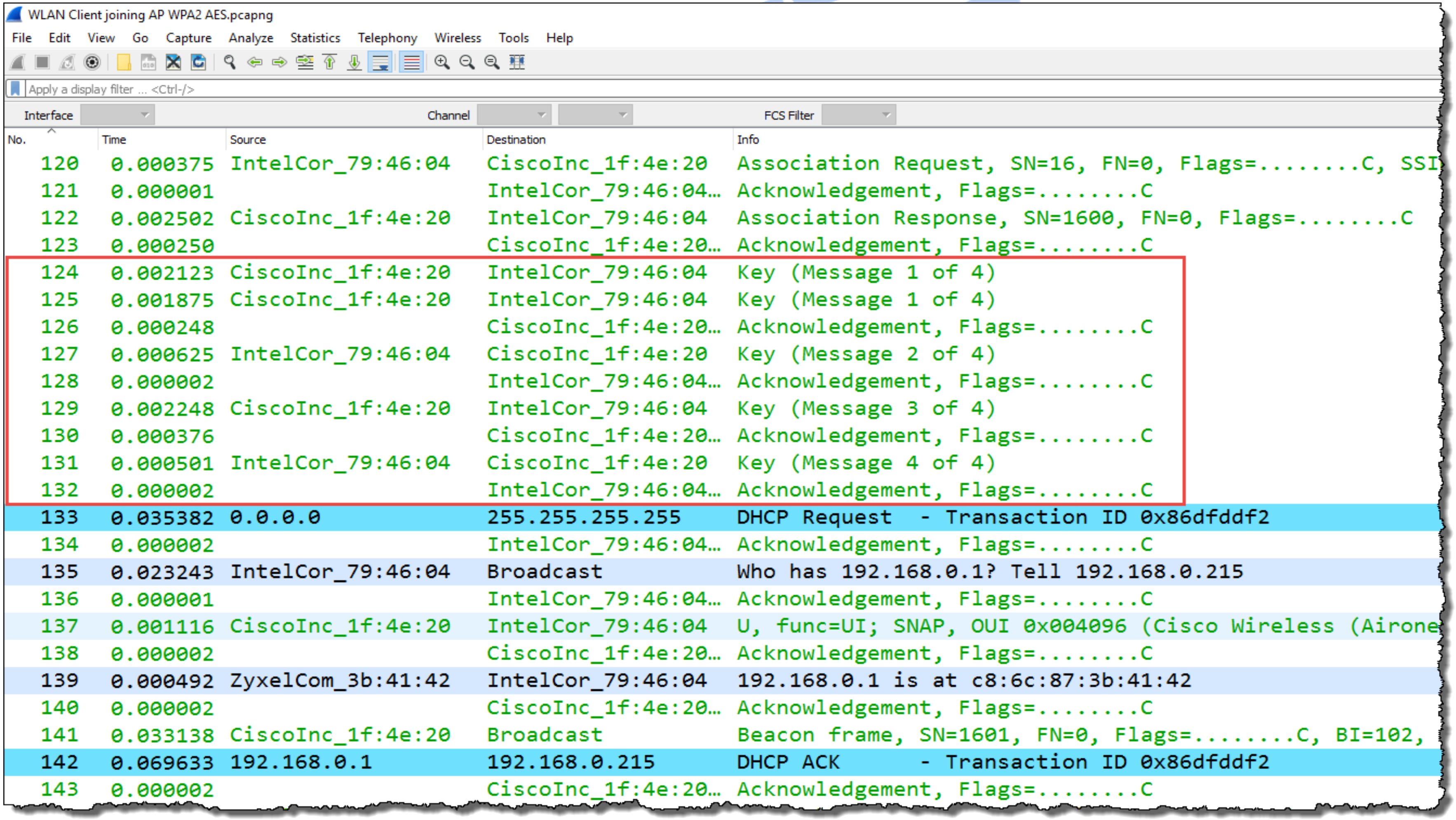
- The client selects an Access Point and sends Authenticate & Associate requests
- Both processes must be successful in order to join the Access Point


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
```

Decrypting WEP, WPA & WPA2 PSK

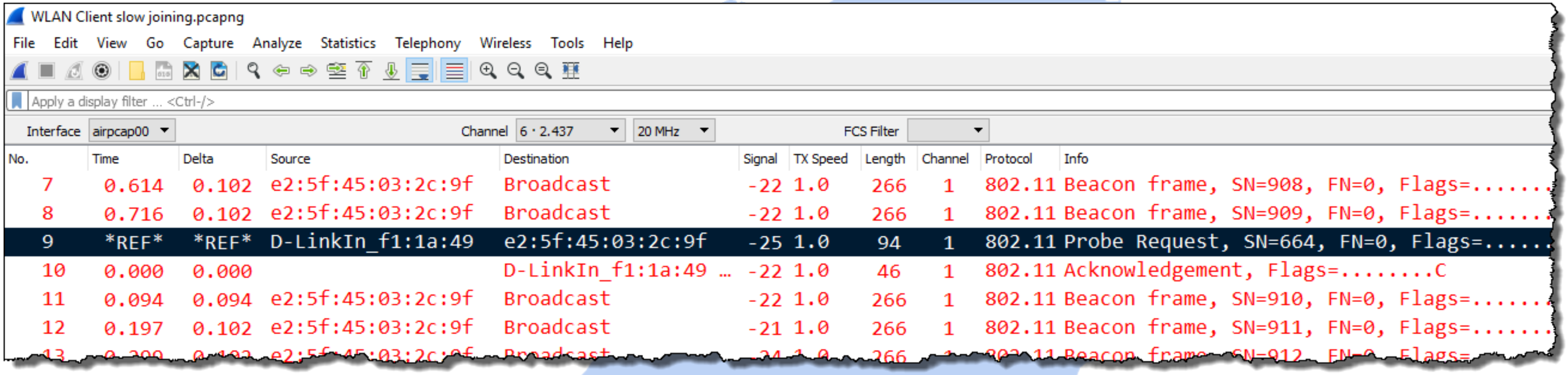
- Wireshark can decrypt WEP, WPA & WPA2 PSK if the key is available
- To decrypt WPA & WPA2 the key negotiation process must be captured


WLAN Client joining AP WPA2 AES.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Interface
Channel
FCS Filter

No.	Time	Source	Destination	Info
120	0.000375	IntelCor_79:46:04	CiscoInc_1f:4e:20	Association Request, SN=16, FN=0, Flags=........C, SSI
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	0.0.0.0	255.255.255.255	DHCP Request - Transaction ID 0x86dfddf2
134	0.000002		IntelCor_79:46:04…	Acknowledgement, Flags=........C
135	0.023243	IntelCor_79:46:04	Broadcast	Who has 192.168.0.1? Tell 192.168.0.215
136	0.000001		IntelCor_79:46:04…	Acknowledgement, Flags=........C
137	0.001116	CiscoInc_1f:4e:20	IntelCor_79:46:04	U, func=UI; SNAP, OUI 0x004096 (Cisco Wireless (Airone
138	0.000002		CiscoInc_1f:4e:20…	Acknowledgement, Flags=........C
139	0.000492	ZyxelCom_3b:41:42	IntelCor_79:46:04	192.168.0.1 is at c8:6c:87:3b:41:42
140	0.000002		CiscoInc_1f:4e:20…	Acknowledgement, Flags=........C
141	0.033138	CiscoInc_1f:4e:20	Broadcast	Beacon frame, SN=1601, FN=0, Flags=........C, BI=102,
142	0.069633	192.168.0.1	192.168.0.215	DHCP ACK - Transaction ID 0x86dfddf2
143	0.000002		CiscoInc_1f:4e:20…	Acknowledgement, Flags=........C

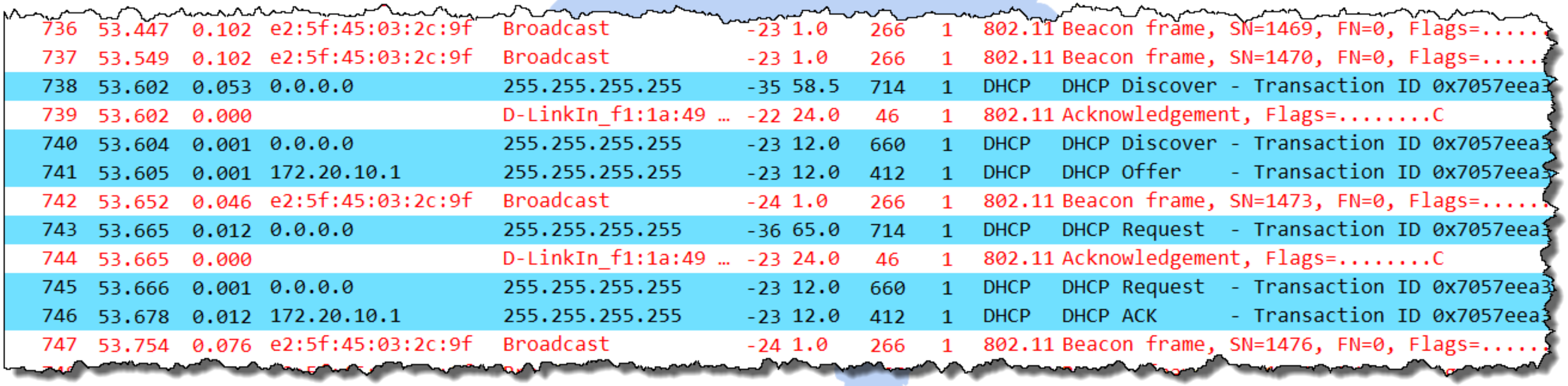
Client joining problem (case one)

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


WLAN Client slow joining.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

Interface: airpcap00 · Channel: 6 · 2.437 · 20 MHz · FCS Filter

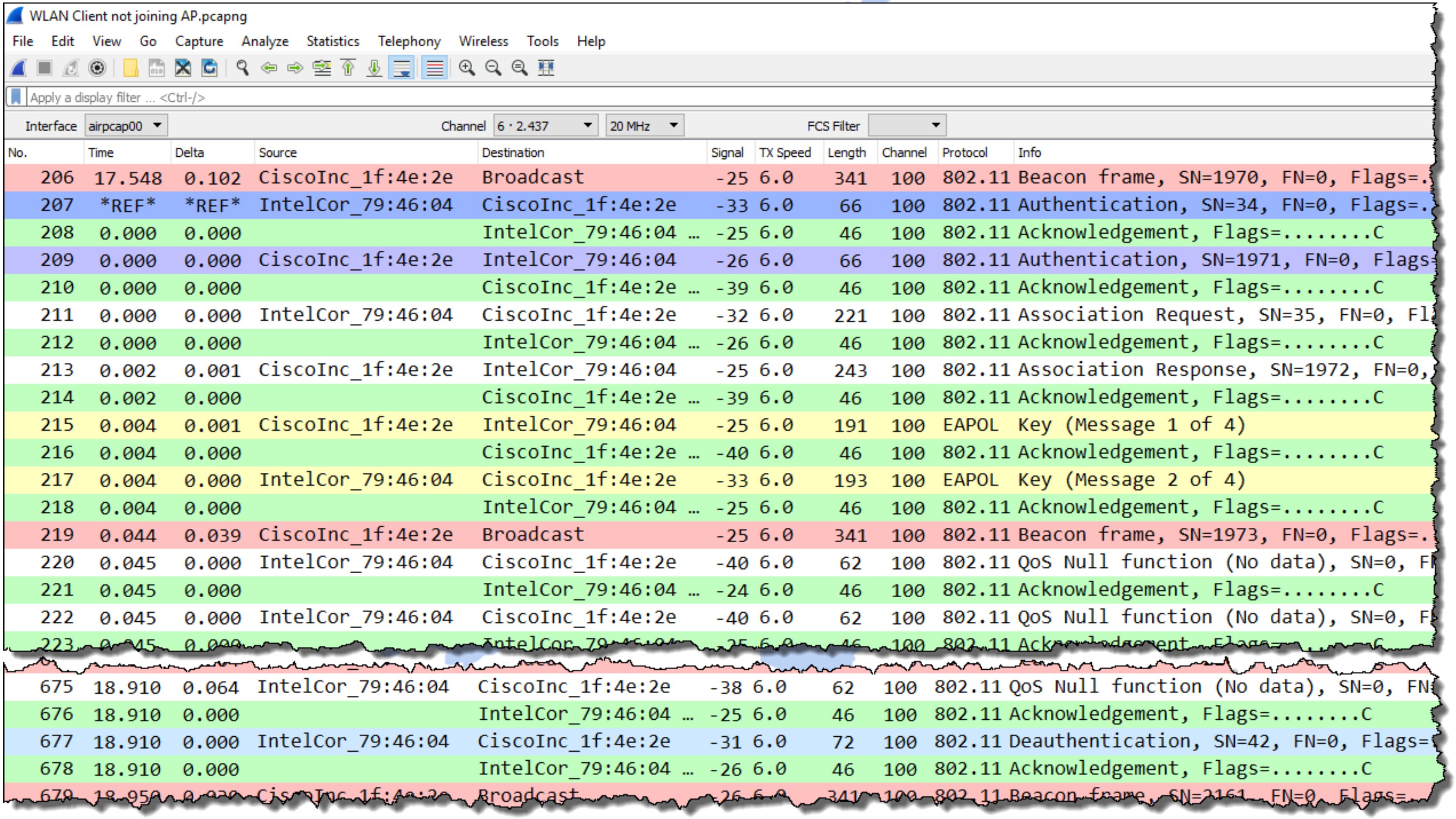
```
No.  Time    Delta  Source              Destination          Signal TX Speed Length Channel Protocol Info
7    0.614   0.102  e2:5f:45:03:2c:9f   Broadcast            -22  1.0   266  1  802.11 Beacon frame, SN=908, FN=0, Flags=......
8    0.716   0.102  e2:5f:45:03:2c:9f   Broadcast            -22  1.0   266  1  802.11 Beacon frame, SN=909, FN=0, Flags=......
9    *REF*   *REF*  D-LinkIn_f1:1a:49   e2:5f:45:03:2c:9f    -25  1.0    94  1  802.11 Probe Request, SN=664, FN=0, Flags=.....
10   0.000   0.000                      D-LinkIn_f1:1a:49 …  -22  1.0    46  1  802.11 Acknowledgement, Flags=........C
11   0.094   0.094  e2:5f:45:03:2c:9f   Broadcast            -22  1.0   266  1  802.11 Beacon frame, SN=910, FN=0, Flags=......
12   0.197   0.102  e2:5f:45:03:2c:9f   Broadcast            -21  1.0   266  1  802.11 Beacon frame, SN=911, FN=0, Flags=......
13   0.300   0.102  e2:5f:45:03:2c:9f   Broadcast            -21  1.0   266  1  802.11 Beacon frame, SN=912, FN=0, Flags=
```



```
736  53.447  0.102  e2:5f:45:03:2c:9f   Broadcast            -23  1.0   266  1  802.11 Beacon frame, SN=1469, FN=0, Flags=.....
737  53.549  0.102  e2:5f:45:03:2c:9f   Broadcast            -23  1.0   266  1  802.11 Beacon frame, SN=1470, FN=0, Flags=.....
738  53.602  0.053  0.0.0.0             255.255.255.255      -35 58.5   714  1  DHCP   DHCP Discover - Transaction ID 0x7057eea3
739  53.602  0.000                      D-LinkIn_f1:1a:49 …  -22 24.0    46  1  802.11 Acknowledgement, Flags=........C
740  53.604  0.001  0.0.0.0             255.255.255.255      -23 12.0   660  1  DHCP   DHCP Discover - Transaction ID 0x7057eea3
741  53.605  0.001  172.20.10.1         255.255.255.255      -23 12.0   412  1  DHCP   DHCP Offer    - Transaction ID 0x7057eea3
742  53.652  0.046  e2:5f:45:03:2c:9f   Broadcast            -24  1.0   266  1  802.11 Beacon frame, SN=1473, FN=0, Flags=.....
743  53.665  0.012  0.0.0.0             255.255.255.255      -36 65.0   714  1  DHCP   DHCP Request  - Transaction ID 0x7057eea3
744  53.665  0.000                      D-LinkIn_f1:1a:49 …  -23 24.0    46  1  802.11 Acknowledgement, Flags=........C
745  53.666  0.001  0.0.0.0             255.255.255.255      -23 12.0   660  1  DHCP   DHCP Request  - Transaction ID 0x7057eea3
746  53.678  0.012  172.20.10.1         255.255.255.255      -23 12.0   412  1  DHCP   DHCP ACK      - Transaction ID 0x7057eea3
747  53.754  0.076  e2:5f:45:03:2c:9f   Broadcast            -24  1.0   266  1  802.11 Beacon frame, SN=1476, FN=0, Flags=.....
```

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



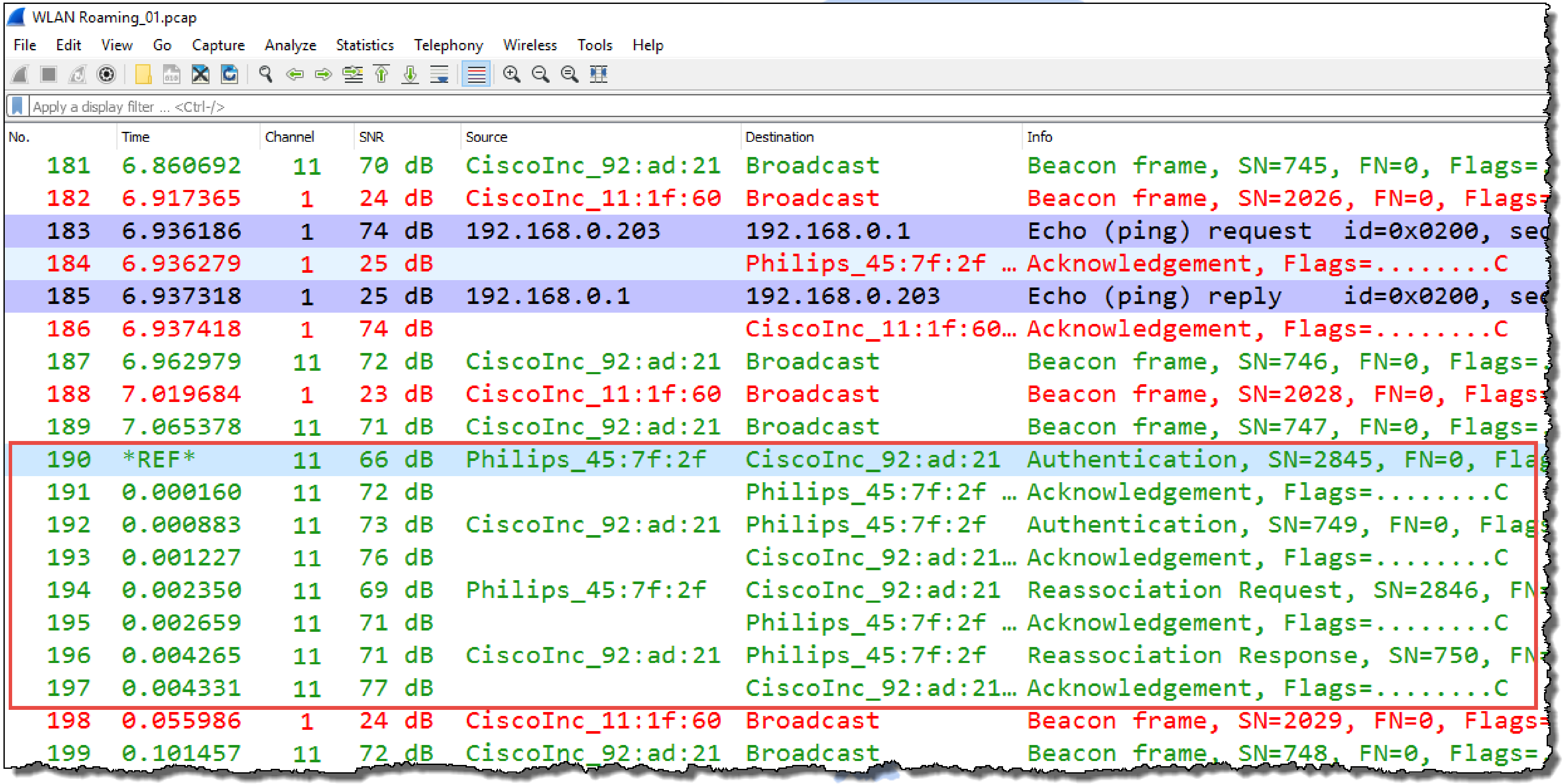
WLAN Client not joining AP.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

Interface airpcap00 Channel 6 · 2.437 20 MHz FCS Filter

No.	Time	Delta	Source	Destination	Signal	TX Speed	Length	Channel	Protocol	Info
206	17.548	0.102	CiscoInc_1f:4e:2e	Broadcast	-25	6.0	341	100	802.11	Beacon frame, SN=1970, FN=0, Flags=.
207	*REF*	*REF*	IntelCor_79:46:04	CiscoInc_1f:4e:2e	-33	6.0	66	100	802.11	Authentication, SN=34, FN=0, Flags=.
208	0.000	0.000		IntelCor_79:46:04 …	-25	6.0	46	100	802.11	Acknowledgement, Flags=........C
209	0.000	0.000	CiscoInc_1f:4e:2e	IntelCor_79:46:04	-26	6.0	66	100	802.11	Authentication, SN=1971, FN=0, Flags
210	0.000	0.000		CiscoInc_1f:4e:2e …	-39	6.0	46	100	802.11	Acknowledgement, Flags=........C
211	0.000	0.000	IntelCor_79:46:04	CiscoInc_1f:4e:2e	-32	6.0	221	100	802.11	Association Request, SN=35, FN=0, Fl
212	0.000	0.000		IntelCor_79:46:04 …	-26	6.0	46	100	802.11	Acknowledgement, Flags=........C
213	0.002	0.001	CiscoInc_1f:4e:2e	IntelCor_79:46:04	-25	6.0	243	100	802.11	Association Response, SN=1972, FN=0,
214	0.002	0.000		CiscoInc_1f:4e:2e …	-39	6.0	46	100	802.11	Acknowledgement, Flags=........C
215	0.004	0.001	CiscoInc_1f:4e:2e	IntelCor_79:46:04	-25	6.0	191	100	EAPOL	Key (Message 1 of 4)
216	0.004	0.000		CiscoInc_1f:4e:2e …	-40	6.0	46	100	802.11	Acknowledgement, Flags=........C
217	0.004	0.000	IntelCor_79:46:04	CiscoInc_1f:4e:2e	-33	6.0	193	100	EAPOL	Key (Message 2 of 4)
218	0.004	0.000		IntelCor_79:46:04 …	-25	6.0	46	100	802.11	Acknowledgement, Flags=........C
219	0.044	0.039	CiscoInc_1f:4e:2e	Broadcast	-25	6.0	341	100	802.11	Beacon frame, SN=1973, FN=0, Flags=.
220	0.045	0.000	IntelCor_79:46:04	CiscoInc_1f:4e:2e	-40	6.0	62	100	802.11	QoS Null function (No data), SN=0, F
221	0.045	0.000		IntelCor_79:46:04 …	-24	6.0	46	100	802.11	Acknowledgement, Flags=........C
222	0.045	0.000	IntelCor_79:46:04	CiscoInc_1f:4e:2e	-40	6.0	62	100	802.11	QoS Null function (No data), SN=0, F
223	0.045	0.000		IntelCor_79:46:04	-25	6.0	46	100	802.11	Acknowledgement, Flags=........C
675	18.910	0.064	IntelCor_79:46:04	CiscoInc_1f:4e:2e	-38	6.0	62	100	802.11	QoS Null function (No data), SN=0, FN
676	18.910	0.000		IntelCor_79:46:04 …	-25	6.0	46	100	802.11	Acknowledgement, Flags=........C
677	18.910	0.000	IntelCor_79:46:04	CiscoInc_1f:4e:2e	-31	6.0	72	100	802.11	Deauthentication, SN=42, FN=0, Flags=
678	18.910	0.000		IntelCor_79:46:04 …	-26	6.0	46	100	802.11	Acknowledgement, Flags=........C
679	18.950	0.040	CiscoInc_1f:4e:2e	Broadcast	-26	6.0	341	100	802.11	Beacon frame, SN=2161, FN=0, Flags=.

Analyzing the WiFi roaming process

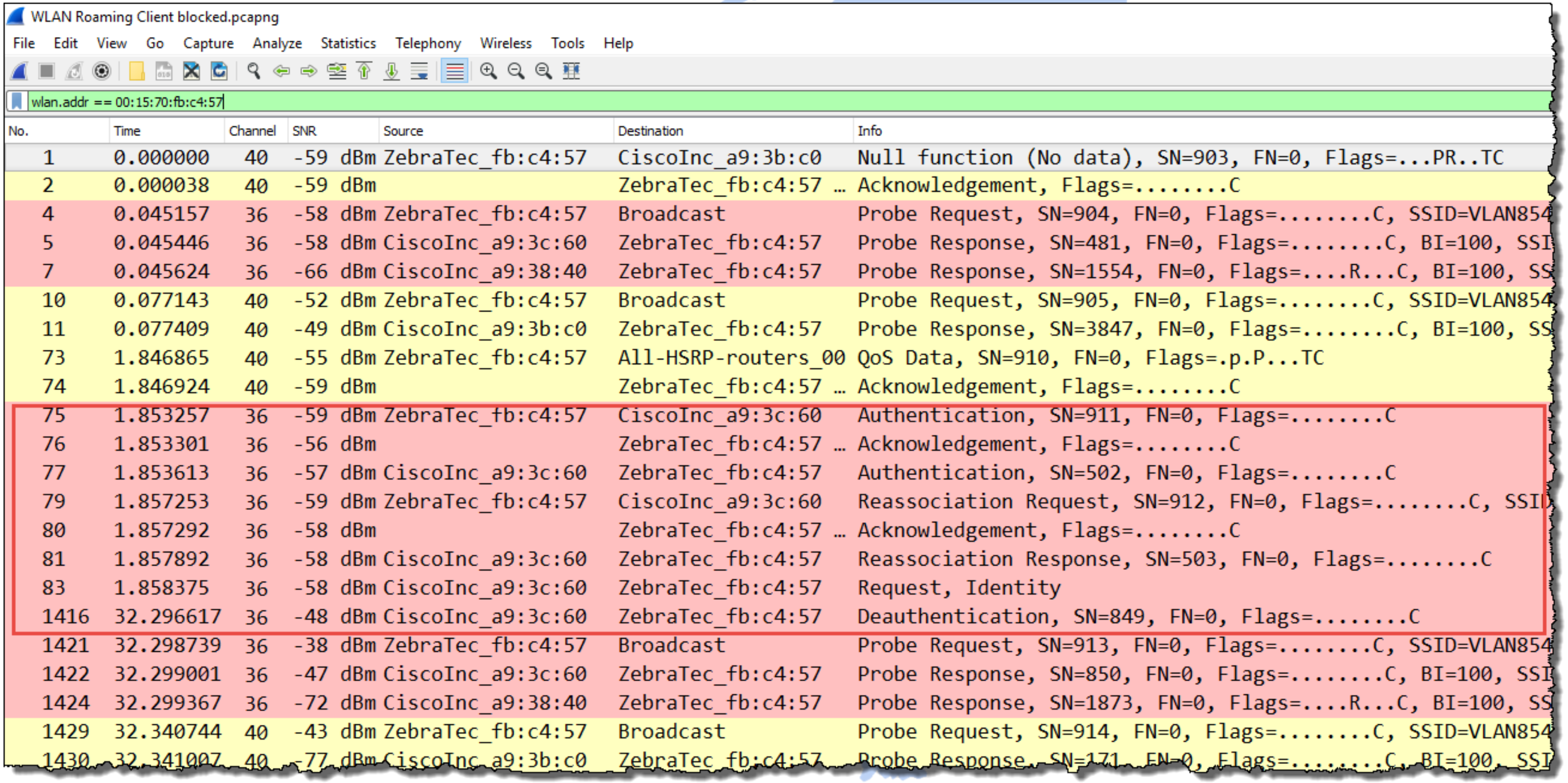
- A client is roaming from channel 1 to 11 because the SNR of the new AP is better
- Following the client with two AirPcaps allows to capture the roaming process


WLAN Roaming_01.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
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.



WLAN Roaming Client blocked.pcapng

wlan.addr == 00:15:70:fb:c4:57

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

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

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)**

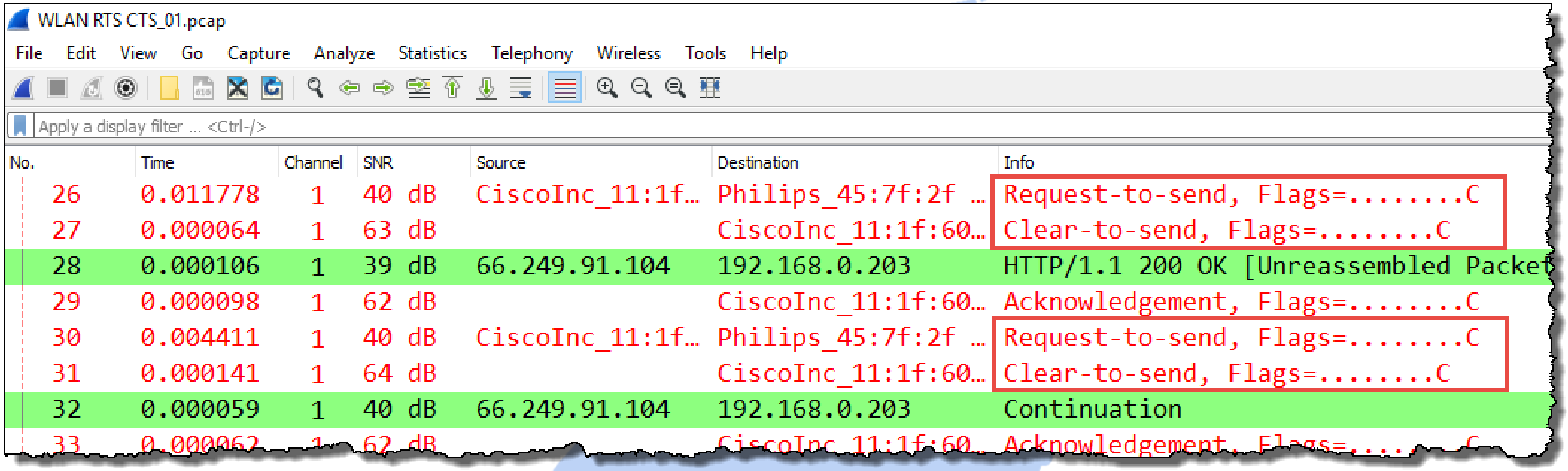
5 GHz Band

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

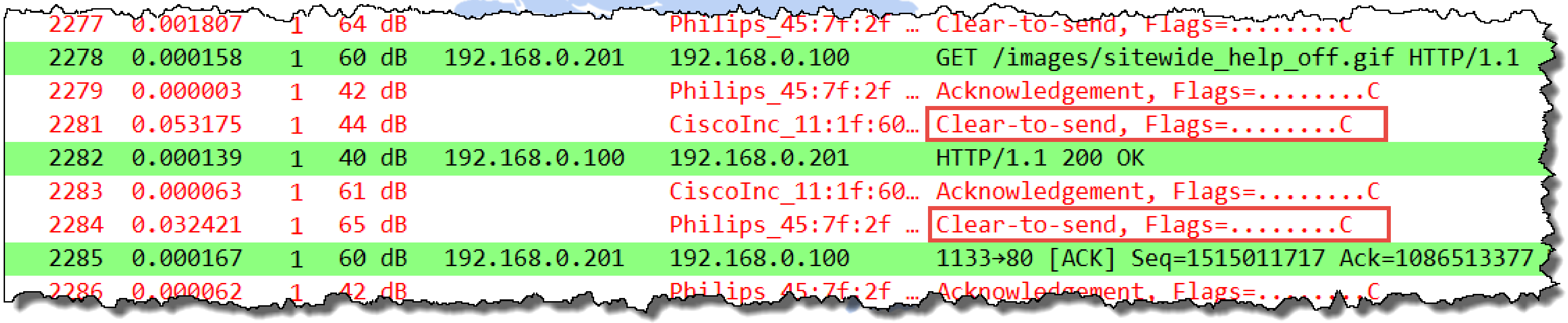
Control Frames: Request to Send / Clear to Send

- 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



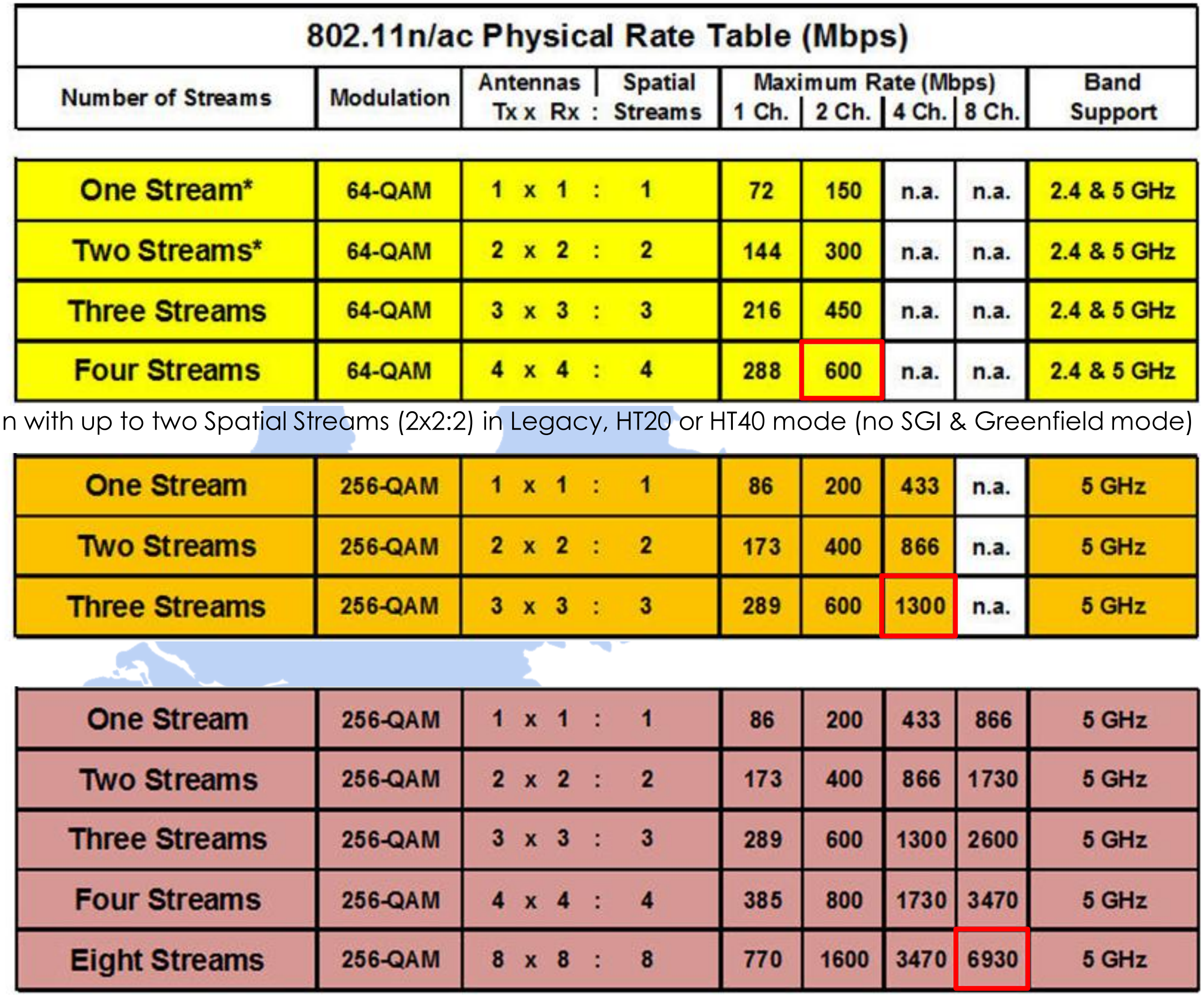
No.	Time	Channel	SNR	Source	Destination	Info
26	0.011778	1	40 dB	CiscoInc_11:1f…	Philips_45:7f:2f …	Request-to-send, Flags=........C
27	0.000064	1	63 dB		CiscoInc_11:1f:60…	Clear-to-send, Flags=........C
28	0.000106	1	39 dB	66.249.91.104	192.168.0.203	HTTP/1.1 200 OK [Unreassembled Packet
29	0.000098	1	62 dB		CiscoInc_11:1f:60…	Acknowledgement, Flags=........C
30	0.004411	1	40 dB	CiscoInc_11:1f…	Philips_45:7f:2f …	Request-to-send, Flags=........C
31	0.000141	1	64 dB		CiscoInc_11:1f:60…	Clear-to-send, Flags=........C
32	0.000059	1	40 dB	66.249.91.104	192.168.0.203	Continuation
33	0.000062	1	62 dB		CiscoInc_11:1f:60…	Acknowledgement, Flags=........C

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



2277	0.001807	1	64 dB		Philips_45:7f:2f …	Clear-to-send, Flags=........C
2278	0.000158	1	60 dB	192.168.0.201	192.168.0.100	GET /images/sitewide_help_off.gif HTTP/1.1
2279	0.000003	1	42 dB		Philips_45:7f:2f …	Acknowledgement, Flags=........C
2281	0.053175	1	44 dB		CiscoInc_11:1f:60…	Clear-to-send, Flags=........C
2282	0.000139	1	40 dB	192.168.0.100	192.168.0.201	HTTP/1.1 200 OK
2283	0.000063	1	61 dB		CiscoInc_11:1f:60…	Acknowledgement, Flags=........C
2284	0.032421	1	65 dB		Philips_45:7f:2f …	Clear-to-send, Flags=........C
2285	0.000167	1	60 dB	192.168.0.201	192.168.0.100	1133→80 [ACK] Seq=1515011717 Ack=1086513377
2286	0.000062	1	42 dB		Philips_45:7f:2f …	Acknowledgement, Flags=........C

Overview WiFi 802.11n/ac Raw Rates



802.11n/ac Physical Rate Table (Mbps)

802.11n

Number of Streams	Modulation	Antennas	Spatial	Maximum Rate (Mbps)				Band
		Tx x Rx :	Streams	1 Ch.	2 Ch.	4 Ch.	8 Ch.	Support
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

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

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

Hope you learned something useful!

© SeaPics.com

Rolf Leutert, Leutert NetServices, www.netsniffing.ch