

SHARKFEST '12

Wireshark Developer and User Conference

Rolf Leutert

Network Expert & Trainer | Leutert NetServices | Switzerland

Analyzing WLAN Roaming Problems

Case Study

Customer is a **large retail store** chain in Switzerland

- Sales areas are **covered with WLANs** for inventory management
- Customer reported **sporadic hang ups** of bar code scanners
- Scanner recovers after delays **up to minutes** back to normal
- Application is **mission critical** for logistic purposes
- **Finger pointing** between scanner vendor and WLAN deployer
- Customer is stuck between a rock and a hard place, **since month!**
- **Task: Analyze WLAN and investigate the source(s) of problems**

Case Study

Situation facts:

- WLANs working in **A-Band** (5 GHz)
- WLANs encrypted with **WPA2 enterprise**
- WPA2 decryption keys are **not** available

Tools used:

- Wireshark with three **AirPcap Nx** Adapters
- **WiSpy DBx** for frequency analysis



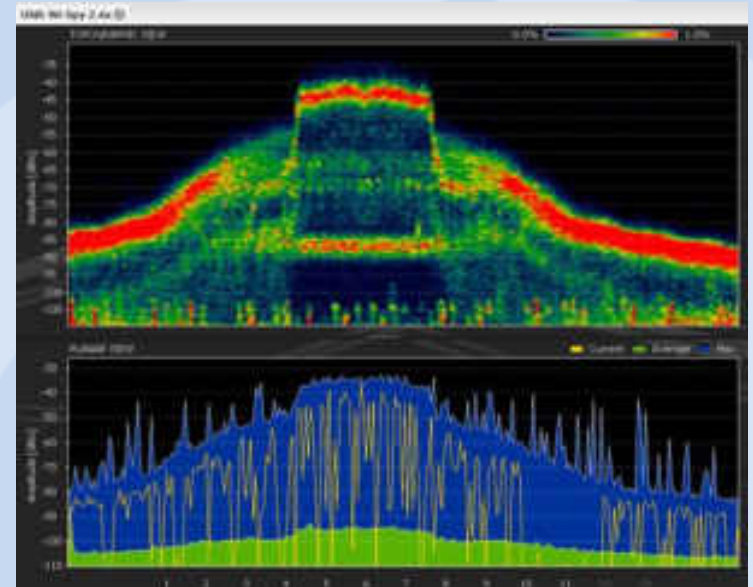
Three AirPcap Nx combined

- **Case demonstrates WLAN troubleshooting with even encrypted data**

WLAN troubleshooting

Possible causes for the hung up problem:

- Radio **gaps** in WLAN covering
- Radio **interferences** from other devices
- **Overloaded** WLAN cells
- Roaming problem
- Settings / defects on **Access Points**
- Settings / defects on **Mobile Clients**
- **Application or handling** problems

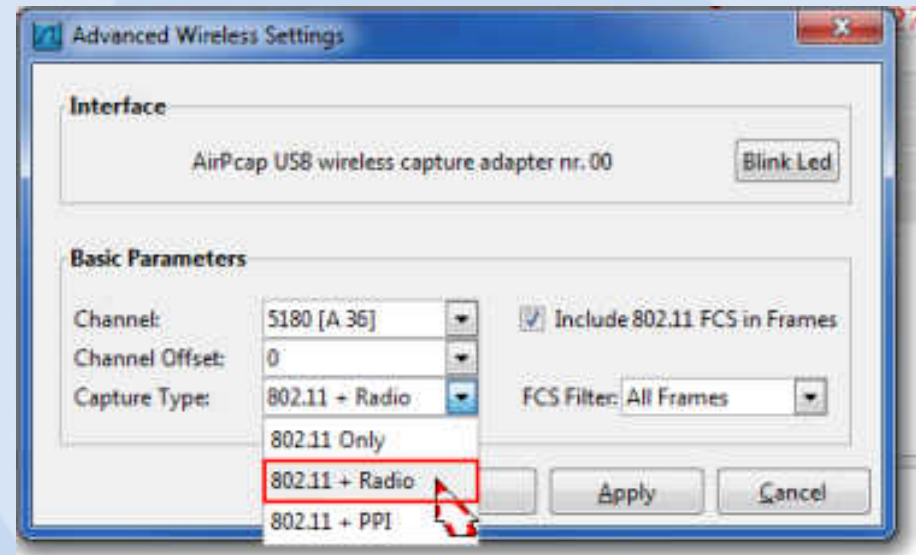


Frequency analysis with WiSpy (MetaGeek)

WLAN troubleshooting

Setup your Wireshark with:

- Choose **802.11+ Radio** for 802.11 A/B/G
- Choose **802.11+ PPI** for 802.11 N (Per-Packet Information)
- This will add a **Radio Tap Header** to each frame with radio values
- Add **columns** to display values
- **Colors** will improve orientation



WLAN troubleshooting

Management Frames:

- Beacon
- Probe request and response
- Authentication
- Deauthentication
- Association request and response
- Reassociation request and response
- Disassociation

Ad-hoc-Networks only:

- Announcement Traffic Indication Message (ATIM)

WLAN troubleshooting

Control Frames:

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

Only for PCF-Mode:

- Contention Free End (CF-End)
- Contention Free End + Acknowledge (CF-End+CF-ACK)

WLAN troubleshooting

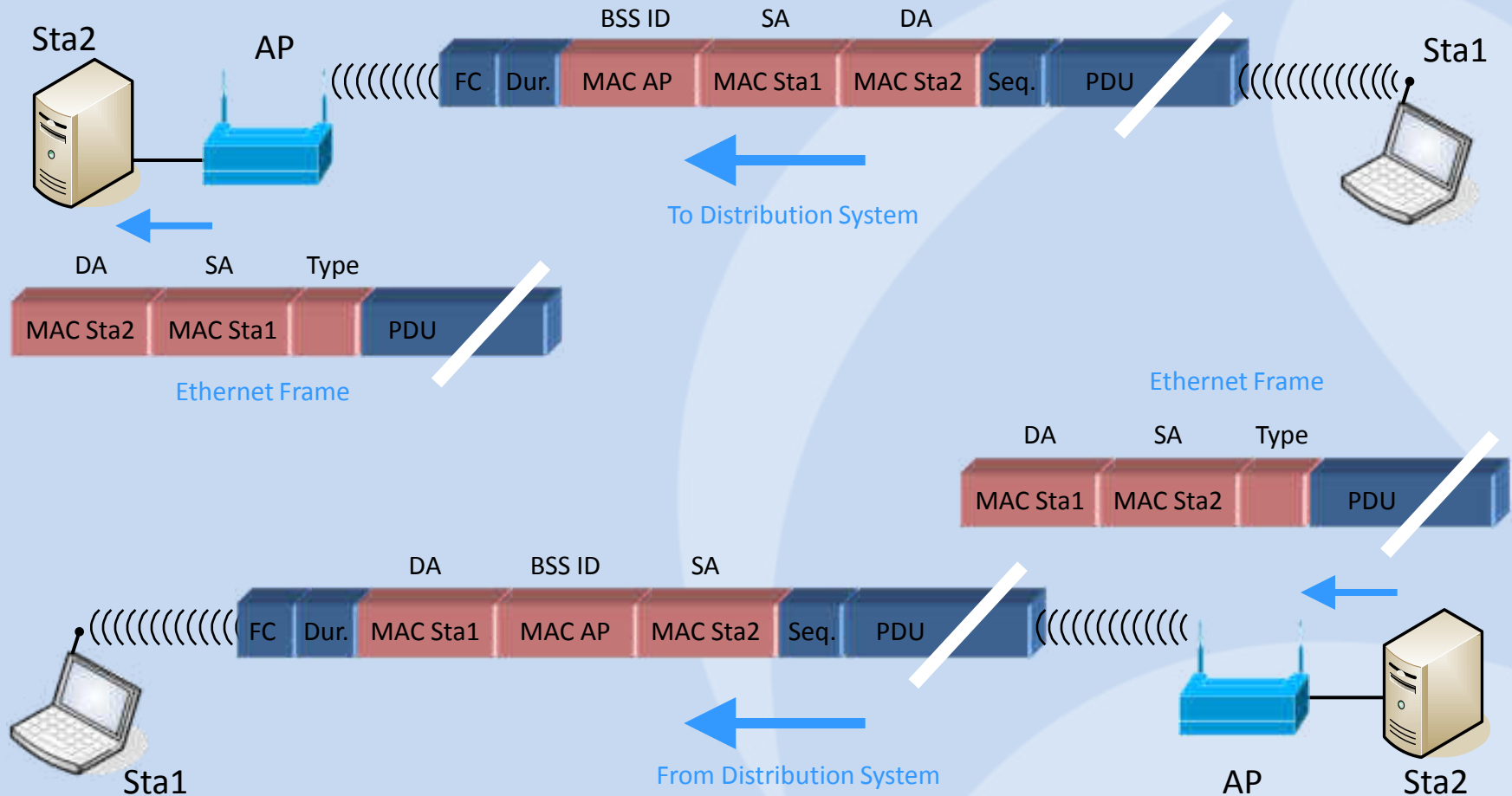
Data Frames:

- Data
- Null Function

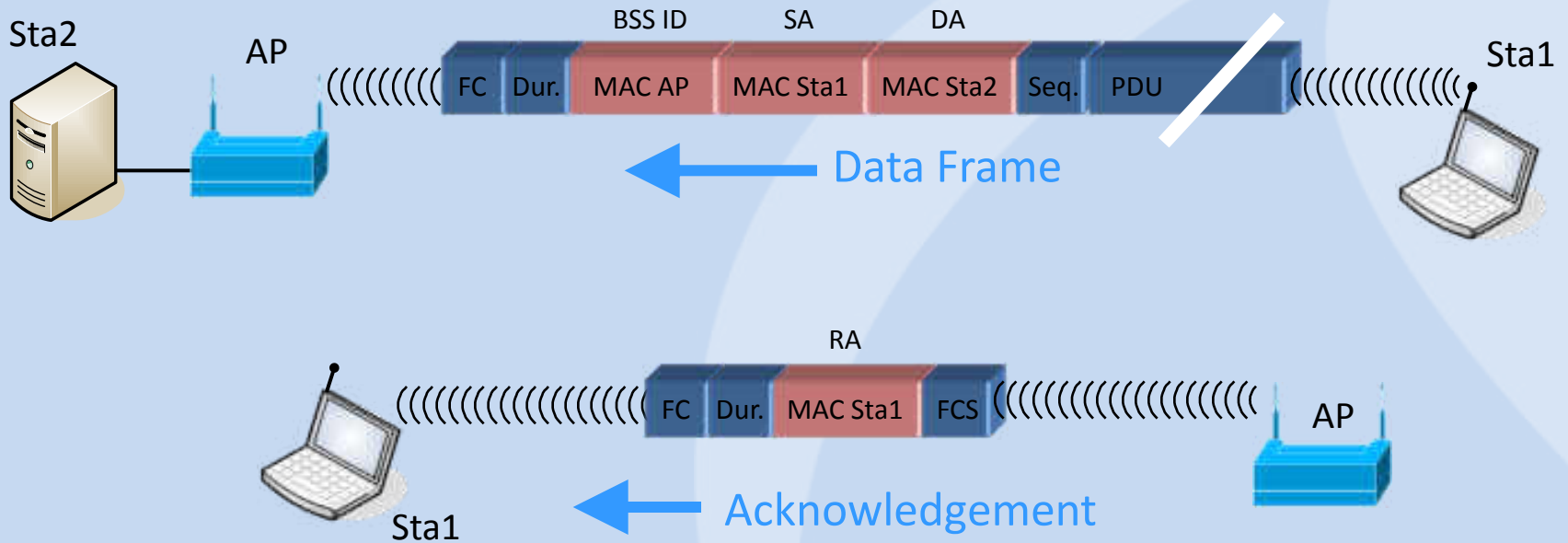
Only for PCF-Mode:

- Data + CF-Ack
- Data + CF-Poll
- Data + CF-Ack + CF-Poll
- CF-Ack (no data)
- CF-Poll (no data)
- CF-Ack + CF-Poll (no data)

WLAN troubleshooting



WLAN troubleshooting



WLAN troubleshooting

The image shows a Wireshark capture of WLAN beacon frames. The main pane displays a list of frames with columns for No., Time, Channel, TX Speed, Signal (dBm), SNR, Source, Destination, Protocol, and Info. The frames are color-coded by channel: 5180 MHz (blue), 5200 MHz (red), and 5240 MHz (green). The detailed view pane shows the structure of a frame, with a red box highlighting the Radiotap Header v0 section.

No.	Time	Channel	TX Speed	Signal (dBm)	SNR	Source	Destination	Protocol	Info
6	0.003059	5180 [A 36]	6.0	-73	22 dB	Cisco_a9:3c:60	Broadcast	802.11	Beacon frame, SN=3656, FN=0
7	0.065324	5200 [A 40]	6.0	-68	27 dB	Cisco_a9:3b:c0	Broadcast	802.11	Beacon frame, SN=2691, FN=0
8	0.006187	5240 [A 48]	6.0	-73	21 dB	Cisco_a9:37:80	Broadcast	802.11	Beacon frame, SN=465, FN=0
9	0.022521	5180 [A 36]	6.0	-68	28 dB	Cisco_a9:38:40	Broadcast	802.11	Beacon frame, SN=544, FN=0
10	0.008326	5180 [A 36]	6.0	-72	24 dB	Cisco_a9:3c:60	Broadcast	802.11	Beacon frame, SN=3657, FN=0
11	0.065204	5200 [A 40]	6.0	-66	29 dB	Cisco_a9:3b:c0	Broadcast	802.11	Beacon frame, SN=2692, FN=0
12	0.006176	5240 [A 48]	6.0	-71	23 dB	Cisco_a9:37:80	Broadcast	802.11	Beacon frame, SN=466, FN=0
13	0.022654	5180 [A 36]	6.0	-69	26 dB	Cisco_a9:38:40	Broadcast	802.11	Beacon frame, SN=545, FN=0

Frame 39: 161 bytes on wire (1288 bits), 161 bytes captured (1288 bits)

- ▣ Radiotap Header v0, Length 28
 - Header revision: 0
 - Header pad: 0
 - Header length: 28
 - ▣ Present flags
 - MAC timestamp: 742490447
 - ▣ Flags: 0x10
 - Data Rate: 6.0 Mb/s
 - Channel frequency: 5180 [A 36]
 - ▣ Channel type: 802.11a (0x0140)
 - SSI Signal: -71 dBm
 - SSI Noise: -95 dBm
 - Signal Quality: 92
 - Antenna: 0
 - SSI Signal: 24 dB
- ▣ IEEE 802.11 Beacon frame, Flags:C
- ▣ IEEE 802.11 wireless LAN management frame

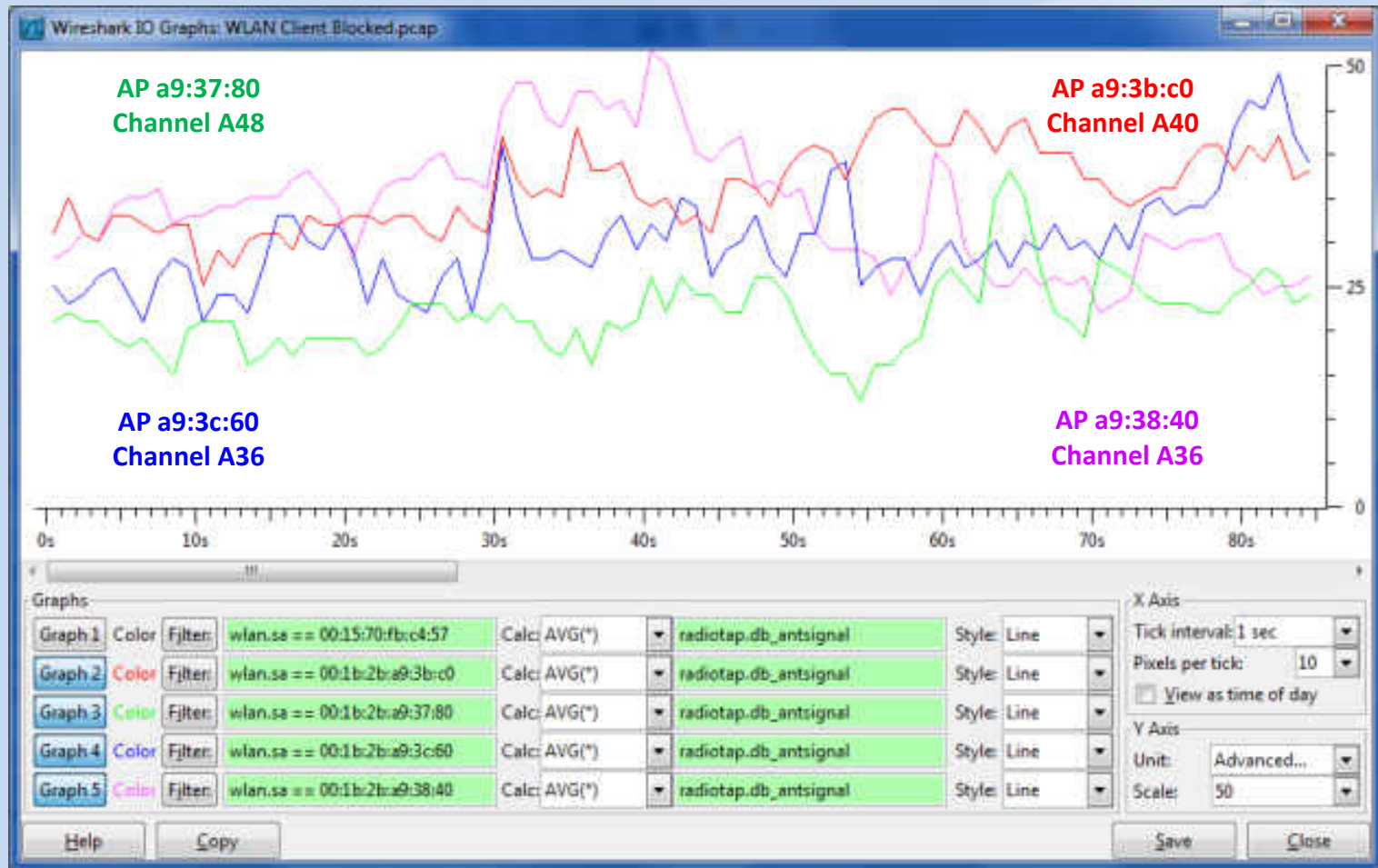
WLAN troubleshooting

The **position** of your Wireshark analyzer is **relevant** for analysis !

Where should you capture?

- If you suspect a **single cell** problem, stay near the **Access Point**
- If you suspect a **roaming** problem, move with the **Mobile Client**
- Use **Beacon S/N ratio** to define your position in relation to APs
- Signal to Noise (S/N) ratio should be **≥ 20 db**
- **Sometimes, a graphic tells us more than a thousand frames**

WLAN troubleshooting



S/N ratio of four Access Points

WLAN troubleshooting

Lets check to which Access Points our Mobile Client is associated

Filter: wlan.addr==00:00:0c:07:ac:00 && wlan.addr==00:15:70:fb:c4:57

No.	Time	Channel	Tx Speed	Signal (dBm)	SNR	Source	Destination	Protocol	Info
28	0.000000	5200 [A 40]	54.0	-41	55 dB	SymbolTe_fb:c4:57	All-MSRP-routers_00	LLC	S P, func=RR, N(R)=65; DSAP 0x7a
87	1.001639	5200 [A 40]	54.0	-47	49 dB	SymbolTe_fb:c4:57	All-MSRP-routers_00	LLC	I P, N(R)=83, N(S)=1; DSAP SNA P
146	1.002545	5200 [A 40]	54.0	-47	49 dB	SymbolTe_fb:c4:57	All-MSRP-routers_00	LLC	S P, func=RR, N(R)=67; DSAP 0x7a

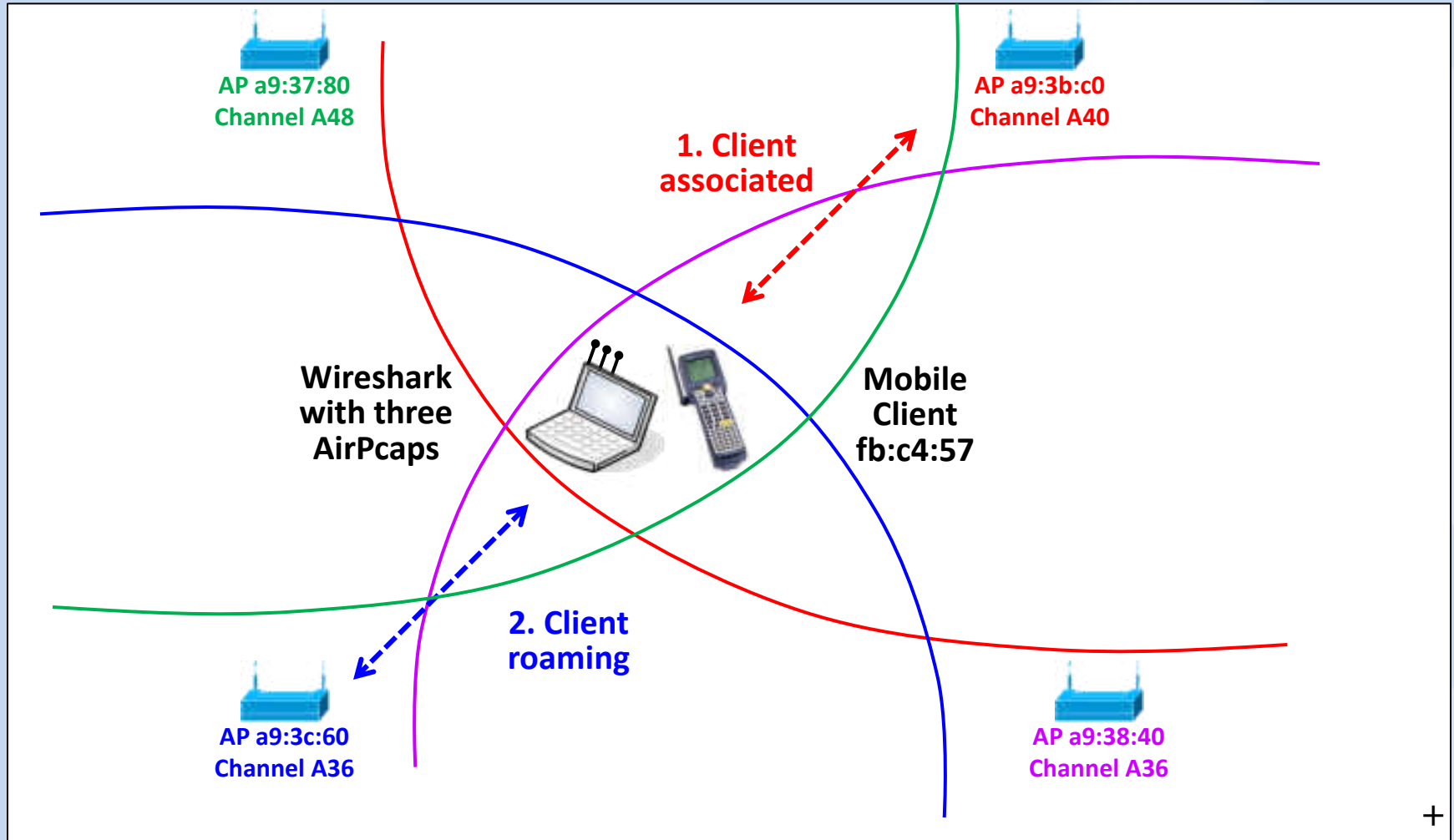
Frame 28: 622 bytes on wire (4976 bits), 622 bytes captured (4976 bits)
Radiotap Header v0, Length 28
IEEE 802.11 QoS Data, Flags: .p.....TC
Type/Subtype: QoS Data (0x28)
Frame Control: 0x4188 (Normal)
Duration: 44
BSS Id: Cisco_a9:3b:c0 (00:1b:2b:a9:3b:c0) **at the beginning of the trace file**
Source address: SymbolTe_fb:c4:57 (00:15:70:fb:c4:57)
Destination address: All-MSRP-routers_00 (00:00:0c:07:ac:00)
Fragment number: 0

Filter: wlan.addr==00:00:0c:07:ac:00 && wlan.addr==00:15:70:fb:c4:57

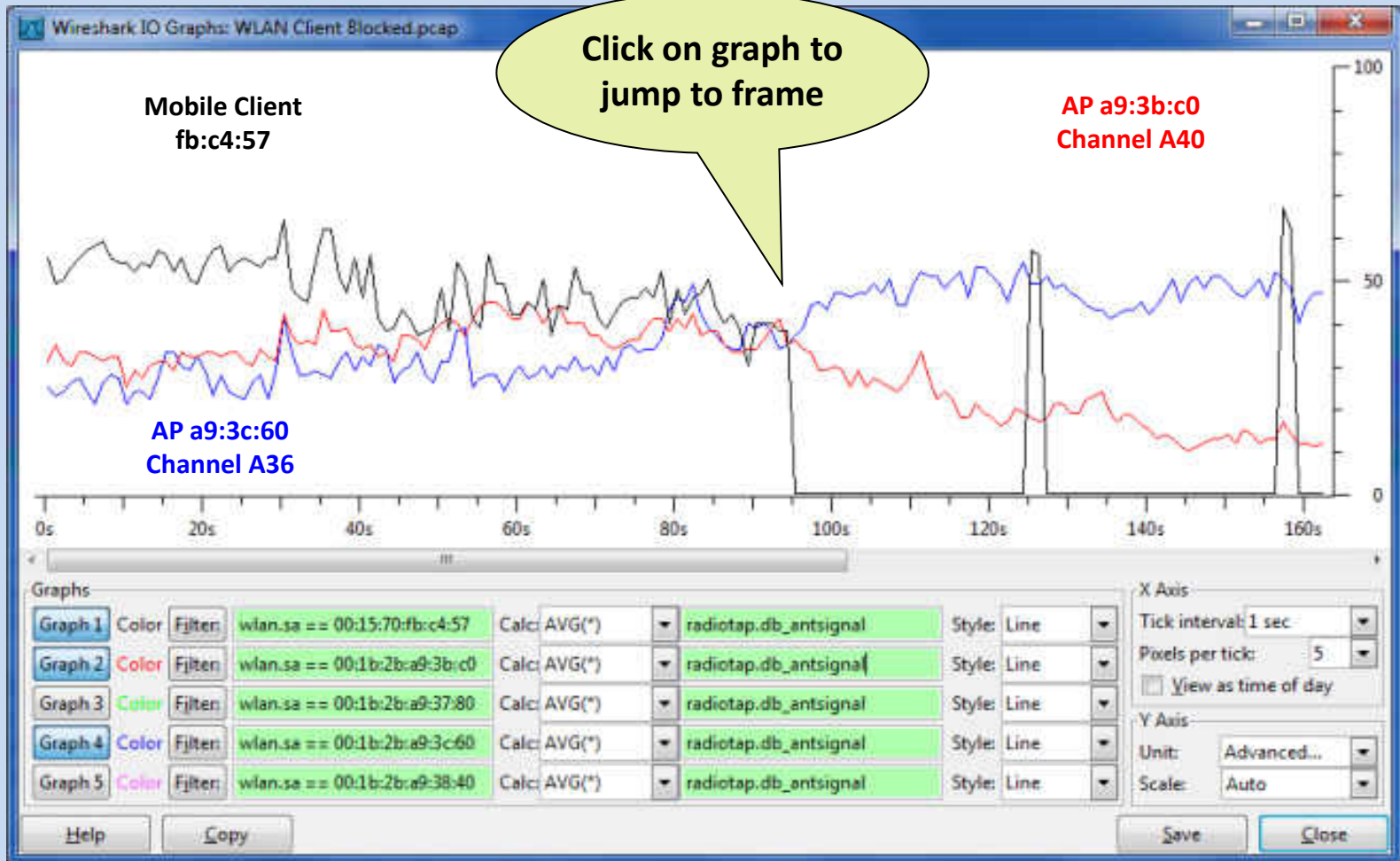
No.	Time	Channel	Tx Speed	Signal (dBm)	SNR	Source	Destination	Protocol	Info
15407	0.987892	5180 [A 36]	54.0	-41	54 dB	SymbolTe_fb:c4:57	All-MSRP-routers_00	LLC	I, N(R)=3, N(S)=125; DSAP 0xa2 Ir
15459	1.013728	5180 [A 36]	54.0	-54	42 dB	SymbolTe_fb:c4:57	All-MSRP-routers_00	LLC	I P, N(R)=77, N(S)=101; DSAP 0x5f
15520	1.001697	5180 [A 36]	54.0	-45	50 dB	SymbolTe_fb:c4:57	All-MSRP-routers_00	LLC	I P, N(R)=93, N(S)=60; DSAP 0x46

Frame 15520: 622 bytes on wire (4976 bits), 622 bytes captured (4976 bits)
Radiotap Header v0, Length 28
IEEE 802.11 QoS Data, Flags: .p.....TC
Type/Subtype: QoS Data (0x28)
Frame Control: 0x4188 (Normal)
Duration: 44
BSS Id: Cisco_a9:3c:60 (00:1b:2b:a9:3c:60) **at the end of the trace file**
Source address: SymbolTe_fb:c4:57 (00:15:70:fb:c4:57)
Destination address: All-MSRP-routers_00 (00:00:0c:07:ac:00)
Fragment number: 0

WLAN troubleshooting



WLAN troubleshooting



S/N ratio of two Access Points and mobile client

WLAN troubleshooting

The image shows a Wireshark capture of WLAN traffic. The filter is set to wlan.addr==001570fb0457. The packet list pane shows several packets, with packet 5650 highlighted in red. The packet details pane shows the structure of the IEEE 802.11 QoS Data, Logical-Link Control, 802.1X Authentication, and Extensible Authentication Protocol (EAP) packet.

No.	Time	Channel	Tx Speed	Signal (dBm)	SNR	Source	Destination	Protocol	Info
5640	0.005951	5200 [A 40]	54.0	-55	41 dB	SymbolTe_fb:c4:57	All-HSRP-routers_UU	LLL	U, Func=unknown; USAP Nes1
5642	0.006392	5180 [A 36]	6.0	-59	37 dB	SymbolTe_fb:c4:57	Cisco_a9:3c:60	802.11	Authentication, SN=911, FT
5644	0.000356	5180 [A 36]	24.0	-57	39 dB	Cisco_a9:3c:60	SymbolTe_fb:c4:57	802.11	Authentication, SN=302, FT
5646	0.003640	5180 [A 36]	6.0	-59	37 dB	SymbolTe_fb:c4:57	Cisco_a9:3c:60	802.11	Reassociation Request, SN-
5648	0.000639	5180 [A 36]	54.0	-58	38 dB	Cisco_a9:3c:60	SymbolTe_fb:c4:57	802.11	Reassociation Response, S
5650	0.000483	5180 [A 36]	54.0	-58	38 dB	Cisco_a9:3c:60	SymbolTe_fb:c4:57	EAP	Request, Identity [RFC374
7331	30.438242	5180 [A 36]	54.0	-48	46 dB	Cisco_a9:3c:60	SymbolTe_fb:c4:57	802.11	Deauthentication, SN=849,
7336	0.002122	5180 [A 36]	6.0	-38	56 dB	SymbolTe_fb:c4:57	Broadcast	802.11	Probe Request, SN=913, FN-
7337	0.000262	5180 [A 36]	6.0	-47	47 dB	Cisco_a9:3c:60	SymbolTe_fb:c4:57	802.11	Probe Response, SN=850, F
7339	0.000366	5180 [A 36]	6.0	-72	22 dB	Cisco_a9:38:40	SymbolTe_fb:c4:57	802.11	Probe Response, SN=1873,]
7345	0.041377	5200 [A 40]	6.0	-43	52 dB	SymbolTe_fb:c4:57	Broadcast	802.11	Probe Request, SN=914, FN-
7346	0.000263	5200 [A 40]	6.0	-77	18 dB	Cisco_a9:3b:c0	SymbolTe_fb:c4:57	802.11	Probe Response, SN=171, F
7347	0.000264	5200 [A 40]	6.0	-78	17 dB	Cisco_a9:3b:c0	SymbolTe_fb:c4:57	802.11	Probe Response, SN=171, F
7349	0.041269	5220 [A 44]	6.0	-36	58 dB	SymbolTe_fb:c4:57	Broadcast	802.11	Probe Request, SN=915, FN-
7353	0.041995	5240 [A 48]	6.0	-30	64 dB	SymbolTe_fb:c4:57	Broadcast	802.11	Probe Request, SN=916, FN-
7354	0.000391	5240 [A 48]	6.0	-64	30 dB	Cisco_a9:37:80	SymbolTe_fb:c4:57	802.11	Probe Response, SN=1870,]
7415	1.161554	5180 [A 36]	6.0	-38	57 dB	SymbolTe_fb:c4:57	Cisco_a9:3c:60	802.11	Authentication, SN=919, FT

IEEE 802.11 QoS Data, Flags:F.C
Logical-Link Control
802.1X Authentication
Version: 1
Type: EAP Packet (0)
Length: 46
Extensible Authentication Protocol
Code: Request (1)
Id: 1
Length: 46
Type: Identity [RFC3748] (1)
Identity (41 bytes): \000networkid=VLAN854,nasid=bash322,portid=0

Frame (frame): 116 bytes | Packets: 13527 Displayed: 698 Marked: 0 Load time: 0:00:26 | Profile: WLAN_Radio_Tap

WLAN troubleshooting

Findings:

- Last frame seen before hang up: **Request ID**
- **No reaction** from the client at this point
- After 30 sec the client is **deauthenticated** by AP

Important question: Did the frame **arrive** at client?

- If **YES** → Client should **reply** with: Response ID
- If **NO** → AP should **retransmit** the Request ID

Can we tell if the Request ID has arrived at the client? **Yes we can!**

- **Have a closer look at the trace file and you will find the answer !**
(Hint be careful with display filter)



WLAN troubleshooting: The Solution

The image shows a Wireshark capture of WLAN traffic. The interface includes a menu bar, a toolbar, and a packet list pane. The packet list pane displays the following data:

No.	Time	Channel	Tx Speed	Signal (dBm)	SNR	Source	Destination	Protocol	Info
5647	0.000039	5180 [A 36]	6.0	-58	38 dB		SymbolTe_fb:c4:57 (RA)	802.11	Acknowledgement, Flags=.....
5648	0.000600	5180 [A 36]	54.0	-58	38 dB	Cisco_a9:3c:60	SymbolTe_fb:c4:57	802.11	Reassociation Response, SN=503
5649	0.000060	5180 [A 36]	24.0	-59	37 dB		Cisco_a9:3c:60 (RA)	802.11	Acknowledgement, Flags=.....
5650	0.000423	5180 [A 36]	54.0	-58	38 dB	Cisco_a9:3c:60	SymbolTe_fb:c4:57	EAP	Request, Identity [RFC3748]
5651	0.000044	5180 [A 36]	24.0	-60	36 dB		Cisco_a9:3c:60 (RA)	802.11	Acknowledgement, Flags=.....
5652	0.028398	5200 [A 40]	6.0	-39	36 dB	Cisco_a9:3b:c0	Broadcast	802.11	Beacon frame, SN=3669, FN=0, F
5653	0.005999	5240 [A 48]	6.0	-62	32 dB	Cisco_a9:37:80	Broadcast	802.11	Beacon frame, SN=1523, FN=0, F
5654	0.022596	5180 [A 36]	6.0	-68	27 dB	Cisco_a9:38:40	Broadcast	802.11	Beacon frame, SN=1573, FN=0, F
5655	0.008660	5180 [A 36]	6.0	-61	34 dB	Cisco_a9:3c:60	Broadcast	802.11	Beacon frame, SN=504, FN=0, F
5656	0.065075	5200 [A 40]	6.0	-68	27 dB	Cisco_a9:3b:c0	Broadcast	802.11	Beacon frame, SN=3870, FN=0, F
5657	0.006124	5240 [A 48]	6.0	-63	31 dB	Cisco_a9:37:80	Broadcast	802.11	Beacon frame, SN=1524, FN=0, F
5658	0.027409	5180 [A 36]	6.0	-72	23 dB	Cisco_a9:38:40	Broadcast	802.11	Beacon frame, SN=1574, FN=0, F
5659	0.008622	5180 [A 36]	6.0	-69	26 dB	Cisco_a9:3c:60	Broadcast	802.11	Beacon frame, SN=505, FN=0, F
5660	0.065096	5200 [A 40]	6.0	-58	37 dB	Cisco_a9:3b:c0	Broadcast	802.11	Beacon frame, SN=3871, FN=0, F

- In WLAN, all frames correctly received **are acknowledged** !
- The client **does** acknowledge the reception of Request ID in **frame 5651**
- The client should now **process** the request and **reply** with a Response ID
- **A bug** in the client firmware caused this sporadic misbehavior
- **The client vendor provided an upgrade and the problem was solved** !

Thanks for visiting



Rolf Leutert, Leutert NetServices, www.wireshark.ch