# 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

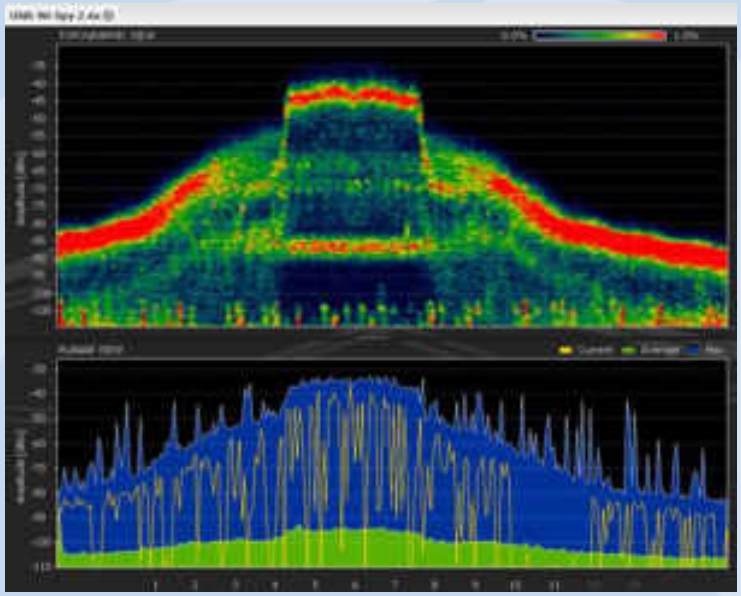
Three AirPcap Nx combined

- 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

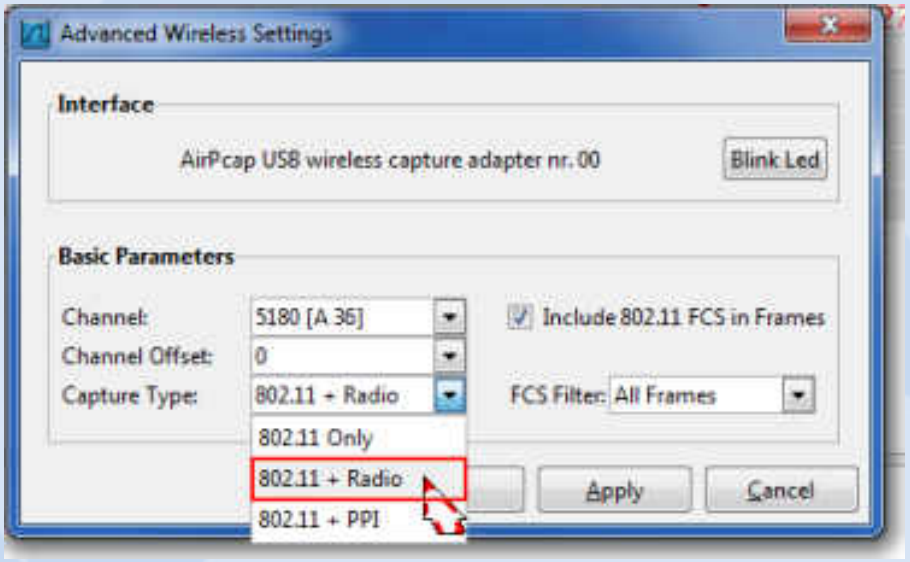


Frequency analysis with WiSpy (MetaGeek)

# 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

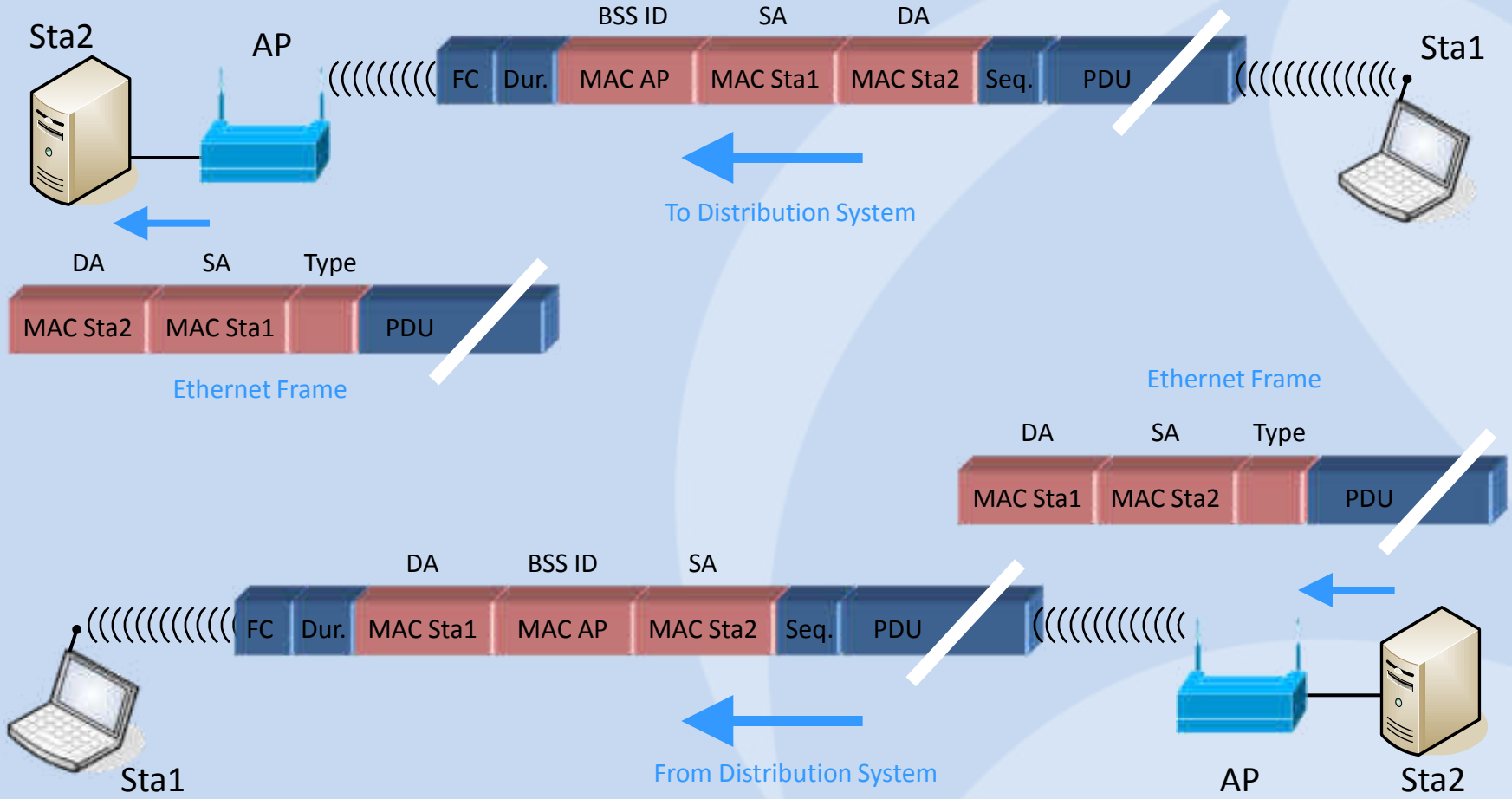
Data Frames:

- Data
- Null Function

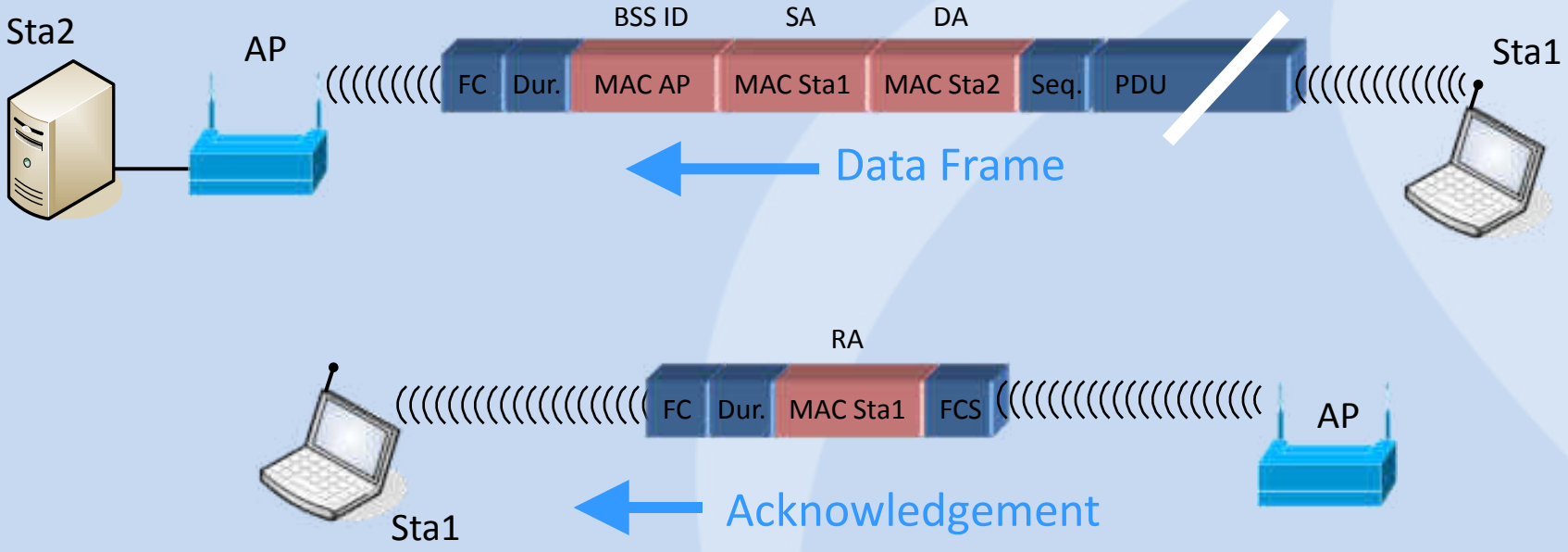
Only for PCF-Mode:

- 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)

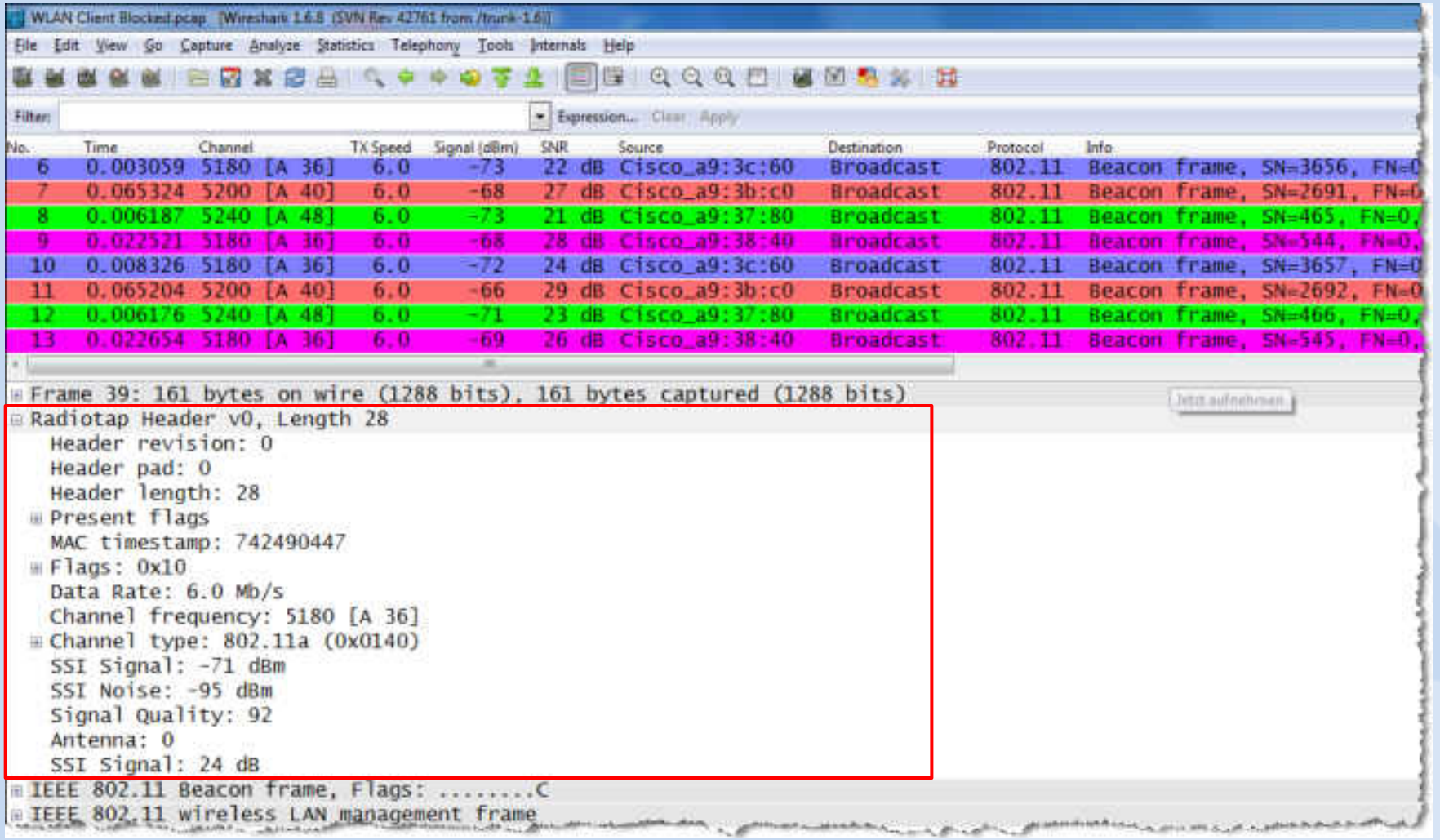
# WLAN troubleshooting



# WLAN troubleshooting



# WLAN troubleshooting



# 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

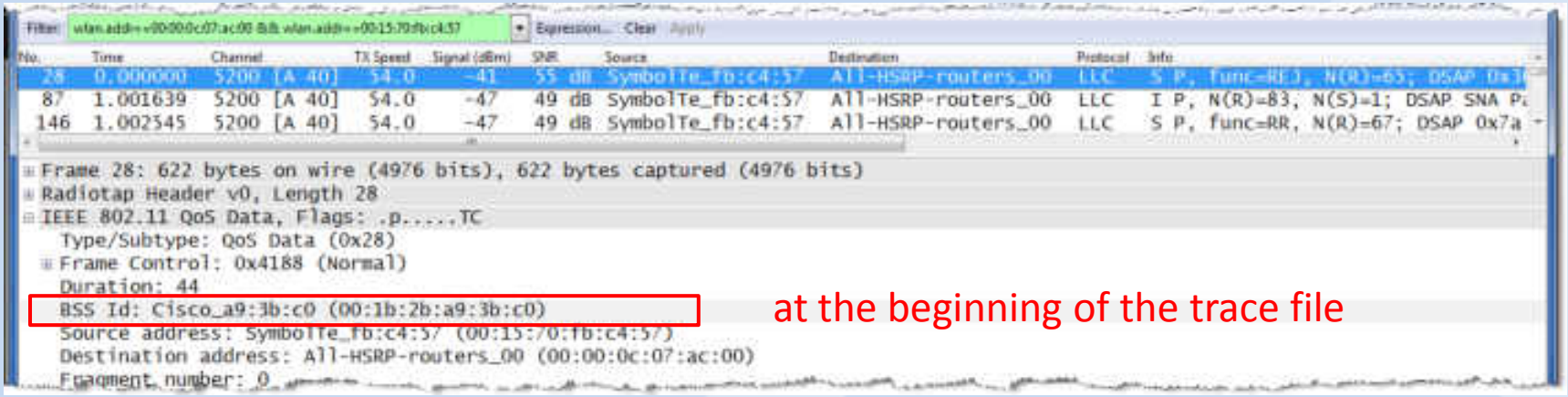
- Sometimes, a graphic tells us more than a thousand frames

# WLAN troubleshooting

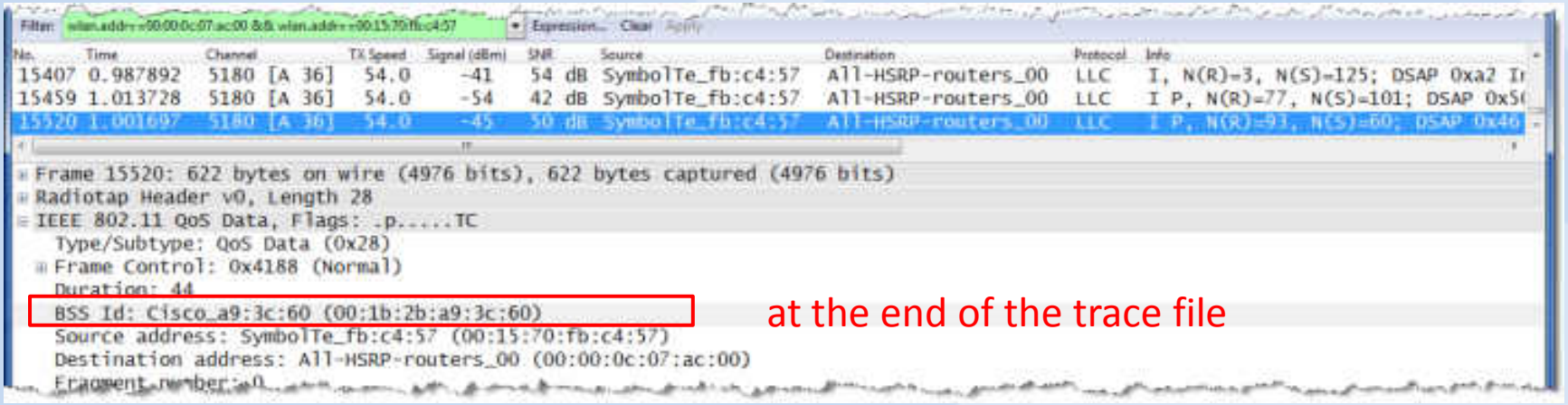

S/N ratio of four Access Points

# WLAN troubleshooting

Lets check to which Access Points our Mobile Client is associated

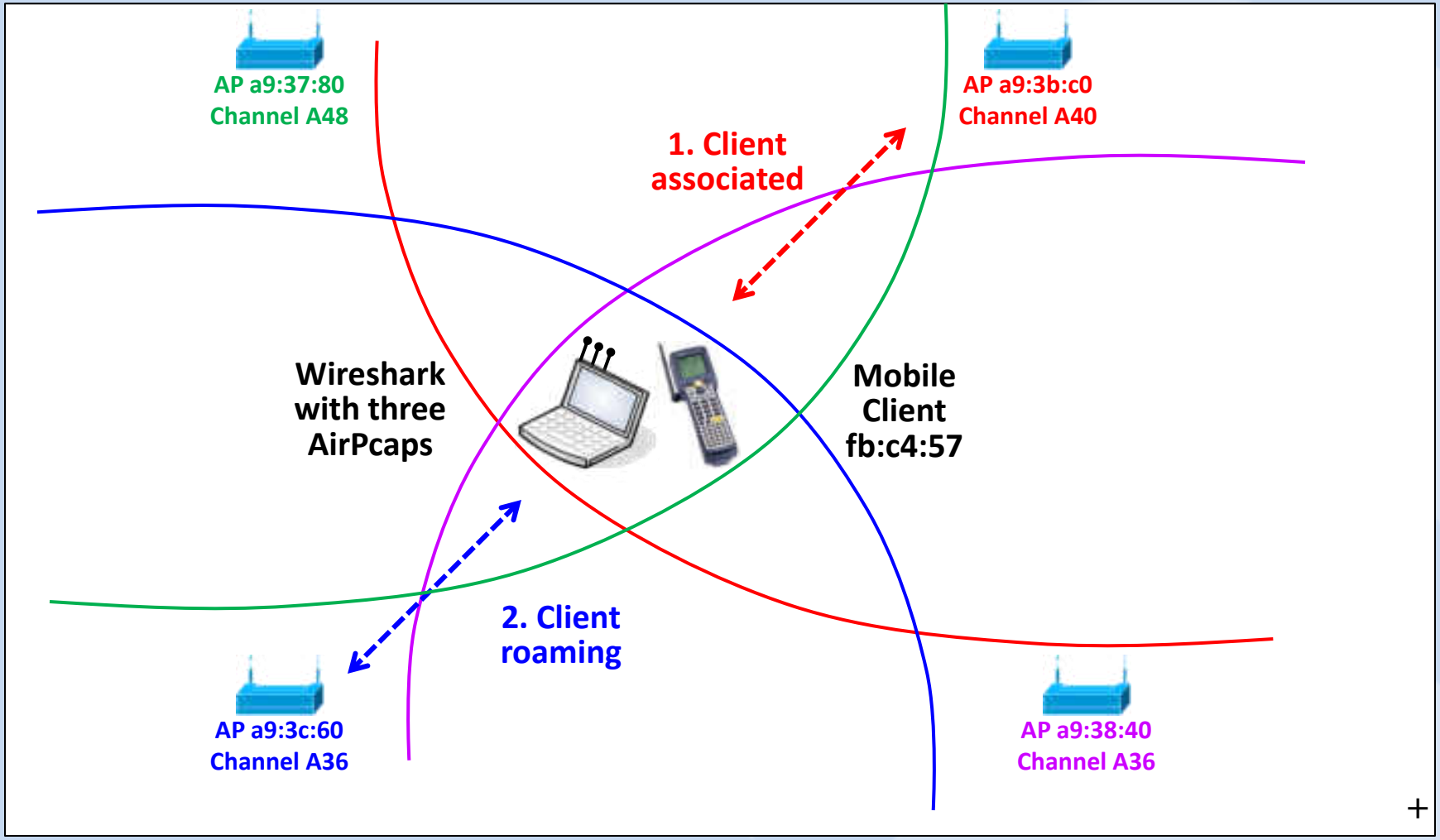



at the beginning of the trace file

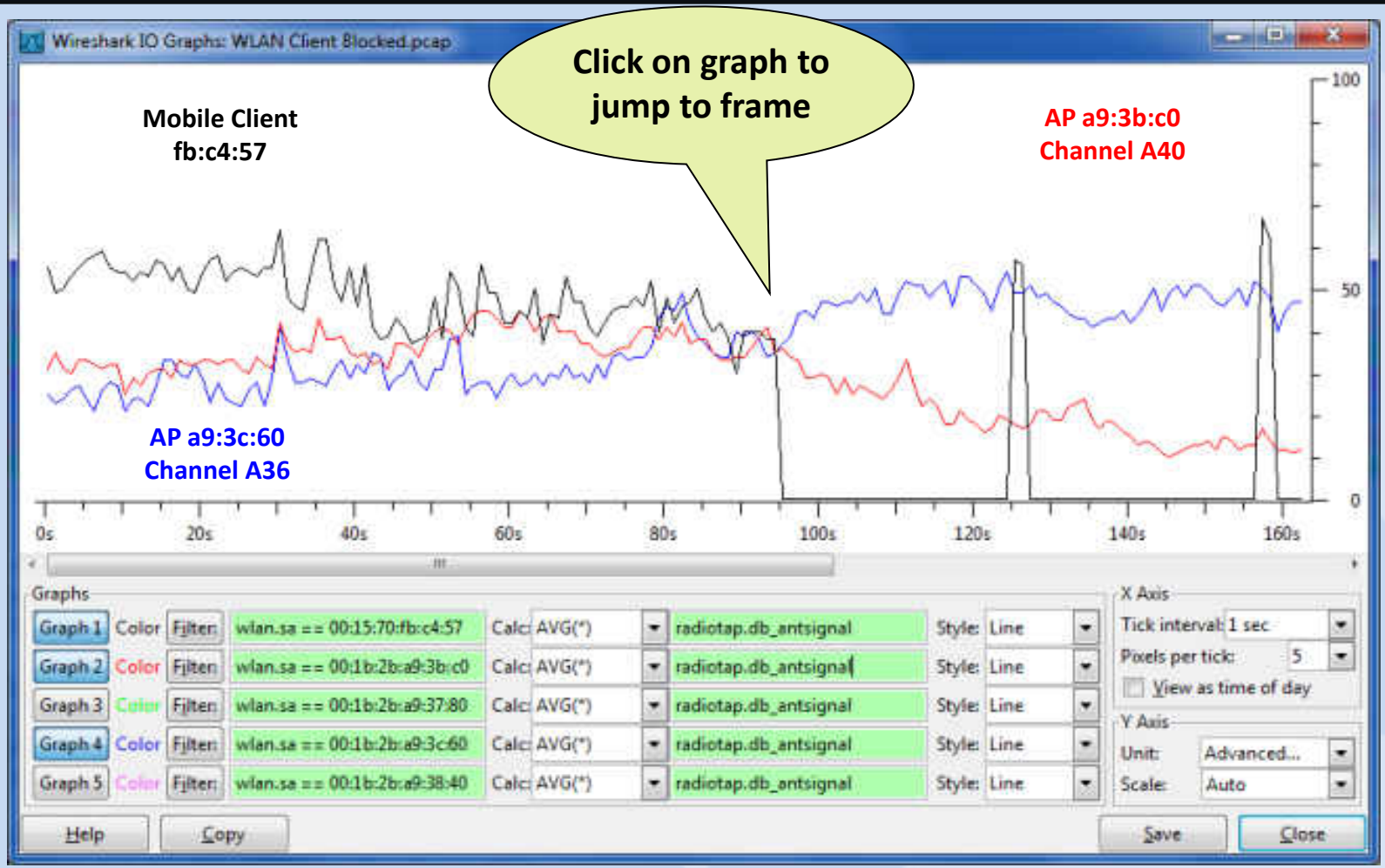



at the end of the trace file

# WLAN troubleshooting

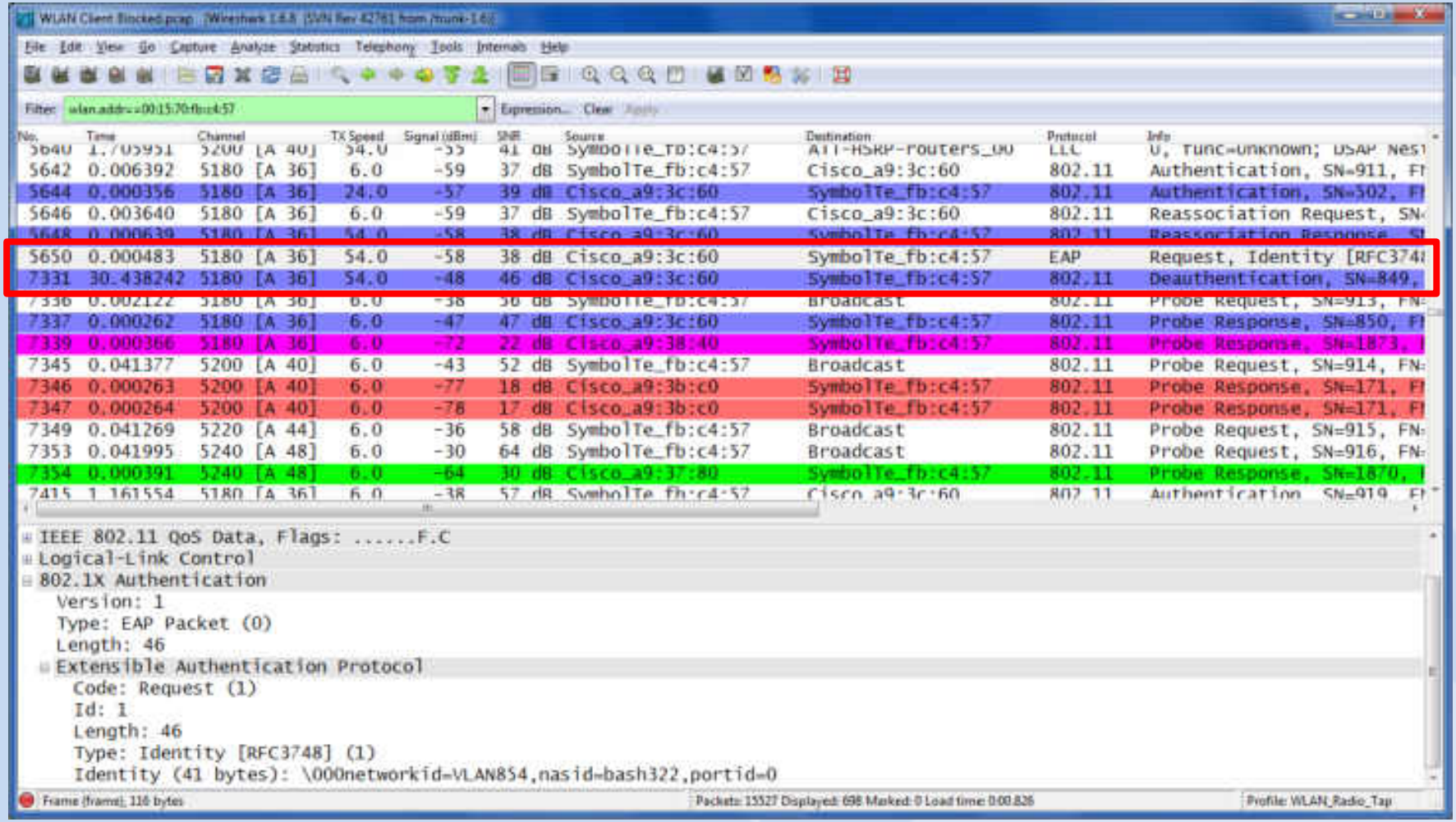


# WLAN troubleshooting




S/N ratio of two Access Points and mobile client

# WLAN troubleshooting



# 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?

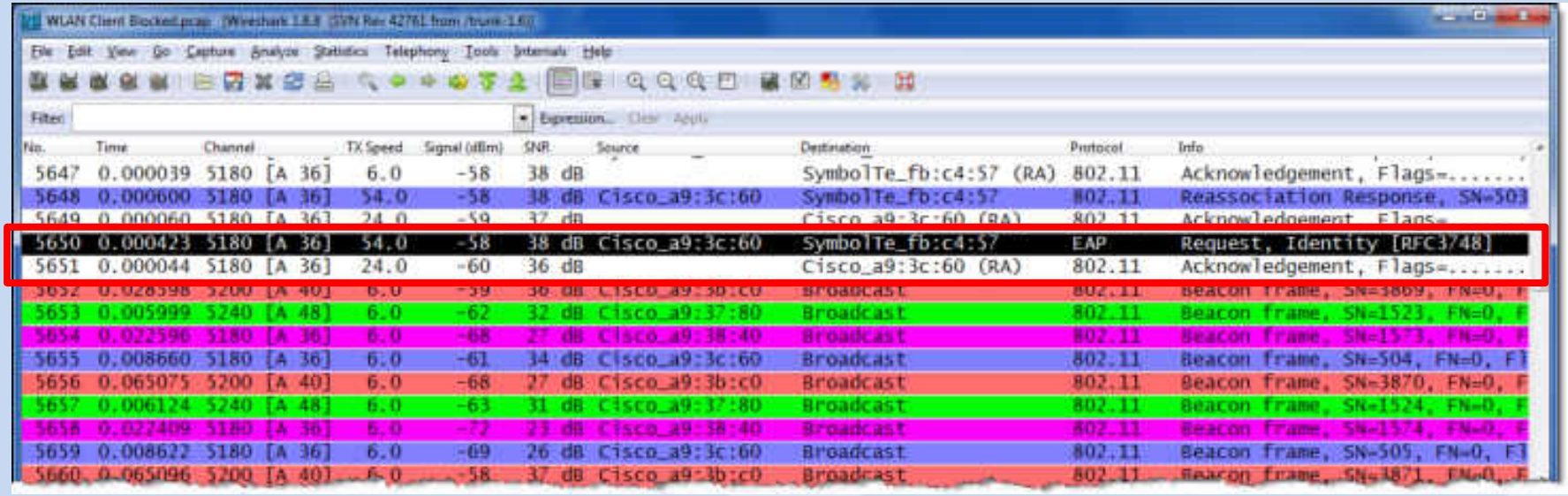
- If YES → Client should reply with: Response ID
- If NO → AP should retransmit the Request ID

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




- 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