



# WLAN-Trouble-Shooting

präsentiert von Rolf Leutert



[www.wireshark.ch](http://www.wireshark.ch)

Instruktor: Rolf Leutert, Dipl. Ing.  
Leutert NetServices  
Zürich-Airport, Switzerland

- Netzwerk Analyse & Troubleshooting
- Protokoll Schulungen TCP/IP, WLAN, VoIP, IPv6
- Wireshark® Certified Network Analyst 2010
- Wireshark® Instructor since 2006
- Sniffer® certified Instructor since 1990

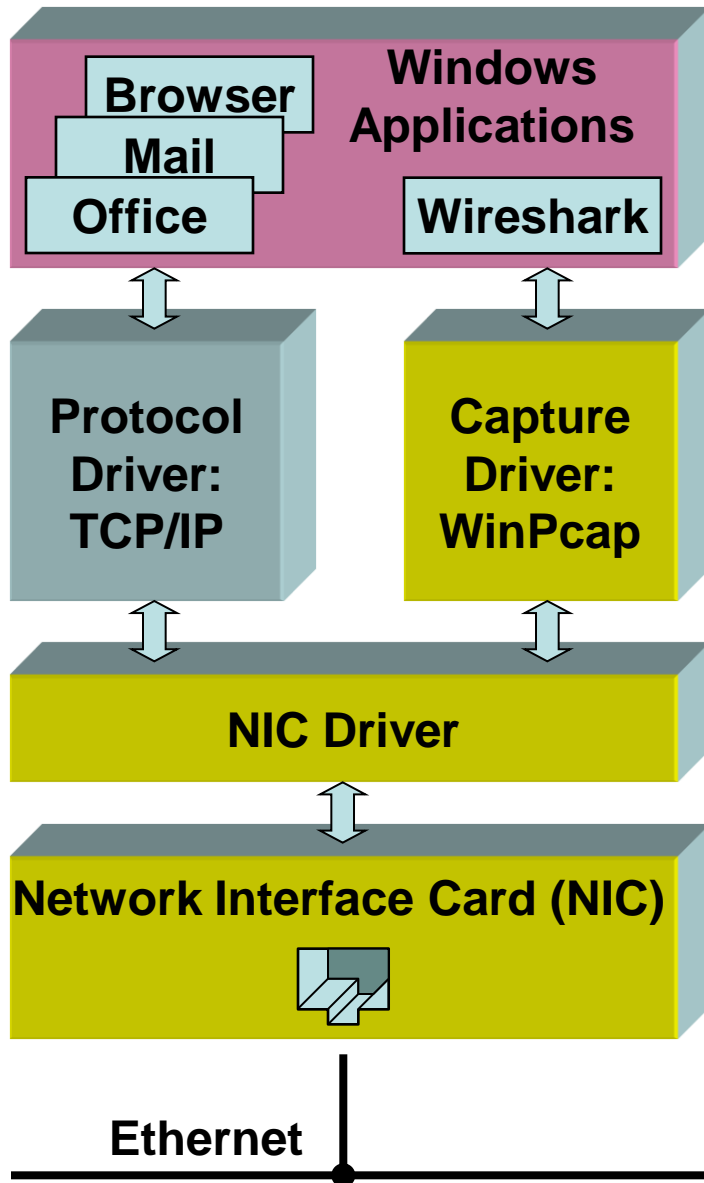
[leutert@wireshark.ch](mailto:leutert@wireshark.ch)  
[www.wireshark.ch](http://www.wireshark.ch)



# Wireshark Network Protocol Analyser



- Der am meisten eingesetzte Protocol Analyser weltweit
- [Open-Source Software](#), d.h. kostenlos einsetzbar, privat oder kommerziell
- Decodiert gegen 1'000 verschiedene Netzwerk-Protokolle
- Unterstützt von allen gängigen Betriebssystemen: [Windows](#), [Unix](#), [Linux](#), [MAC...](#)
- Download von [www.wireshark.org](http://www.wireshark.org)
- In 5 Minuten installiert, runterladen und installieren mit [default](#) Einstellungen
- Kann Tracefiles öffnen, welche mit [TCPdump](#) aufgezeichnet wurden



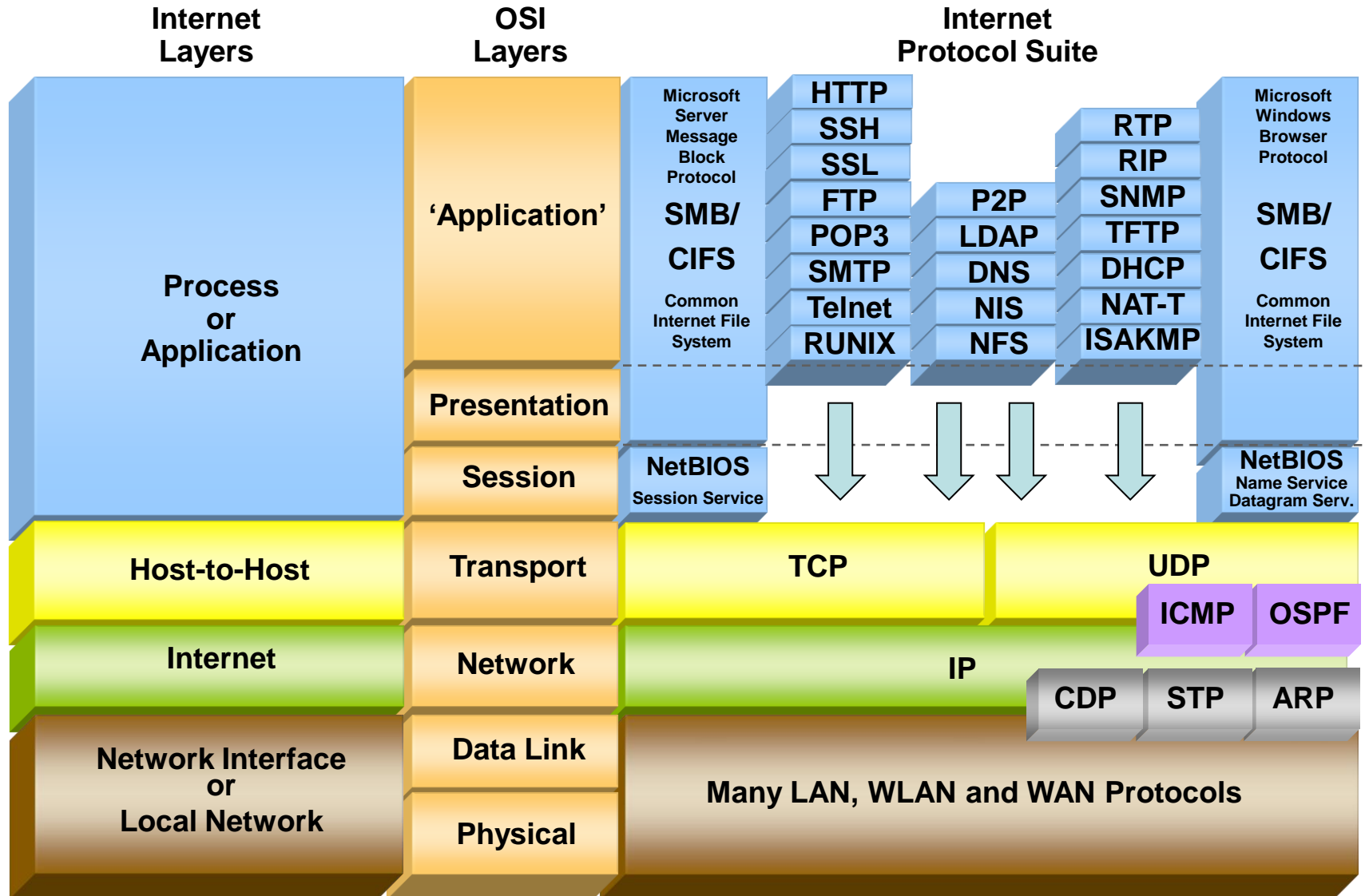
## Wireshark für Ethernet

Wireshark verwendet unter Windows® den Capture Driver **WinPcap**, welcher mit dem NIC Driver kommuniziert.

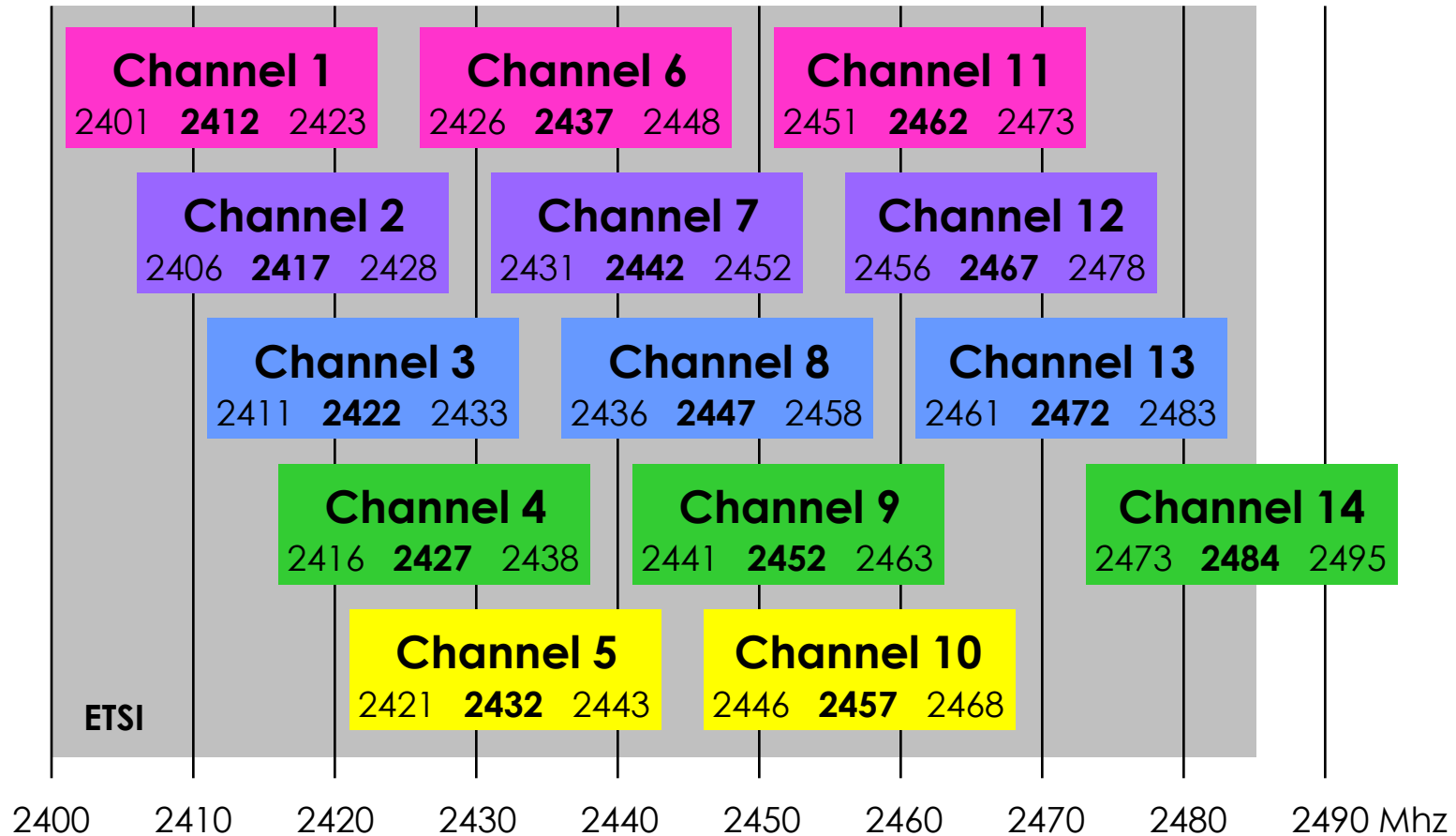
Der NIC Driver kann von WinPcap so konfiguriert werden, dass sämtliche Frames von Ethernet an WinPcap weitergeleitet werden (*Promiscuous Mode*).

Wireshark kann gleichzeitig neben anderen Windows-Anwendungen betrieben werden und kann die von diesen gesendeten oder empfangenen Daten aufzeichnen.

# Die Protokoll Übersicht



# Frequenzaufteilung im 2.4 GHz Band für IEEE 802.11b/g



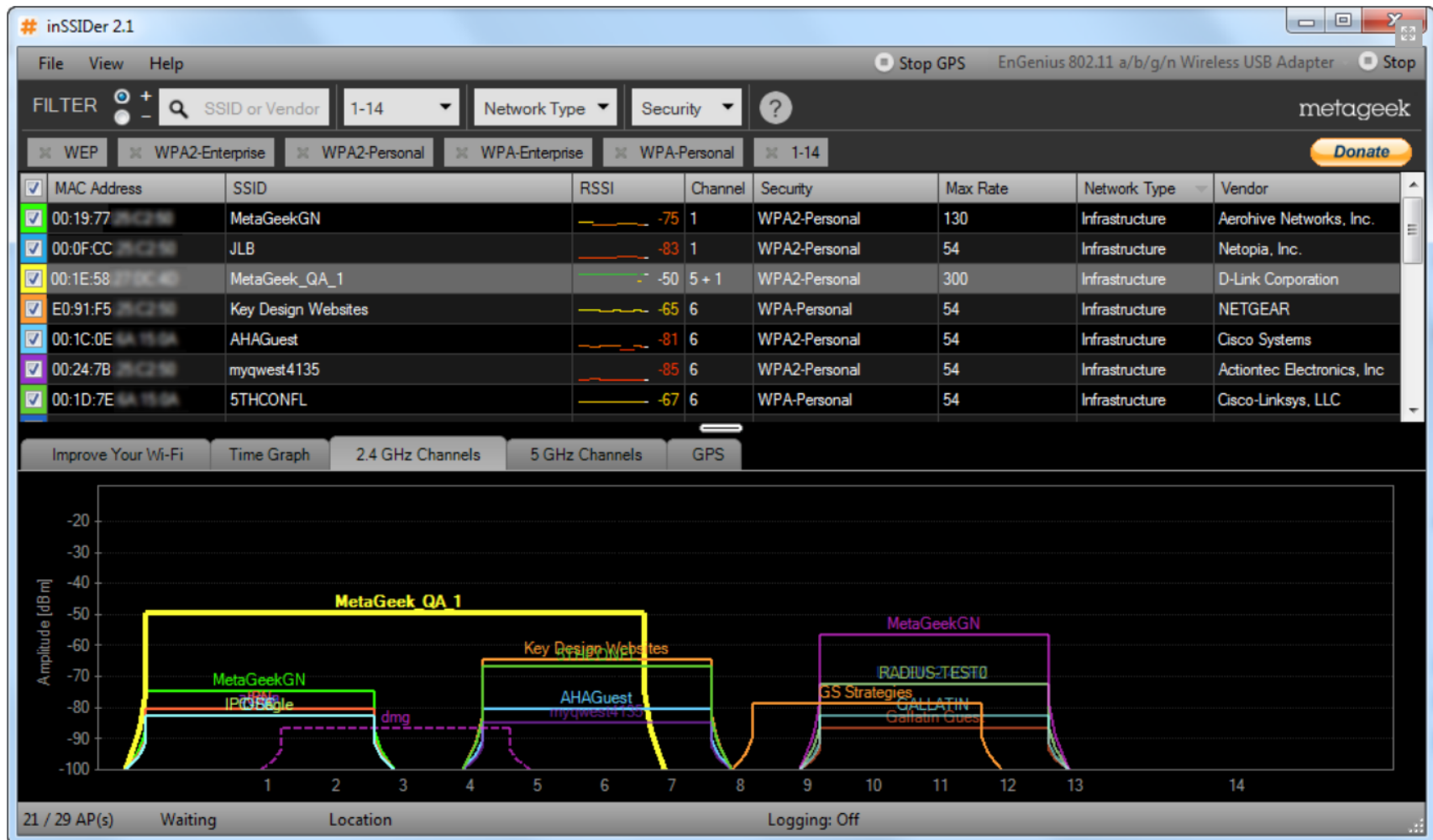
Zugelassene  
Frequenzbereiche:

Ch1 – Ch11 USA (FCC)  
Ch1 – Ch13 Most of the World

Ch1 - Ch14 Japan

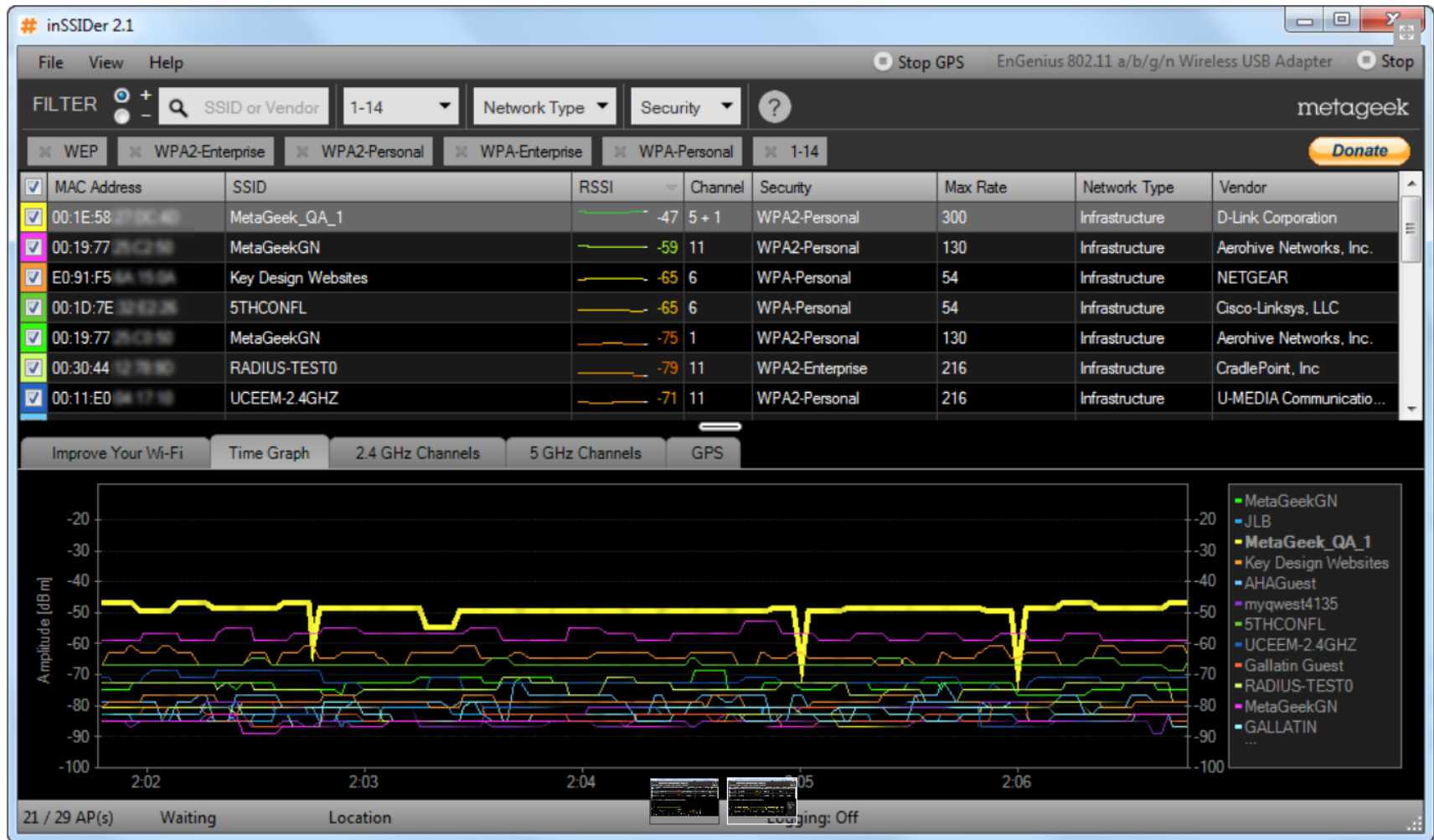
# WLAN Layer 1 Analyse

InSSIDer - die kostenlose WLAN Scanning Software für Windows



# WLAN Layer 1 Analyse

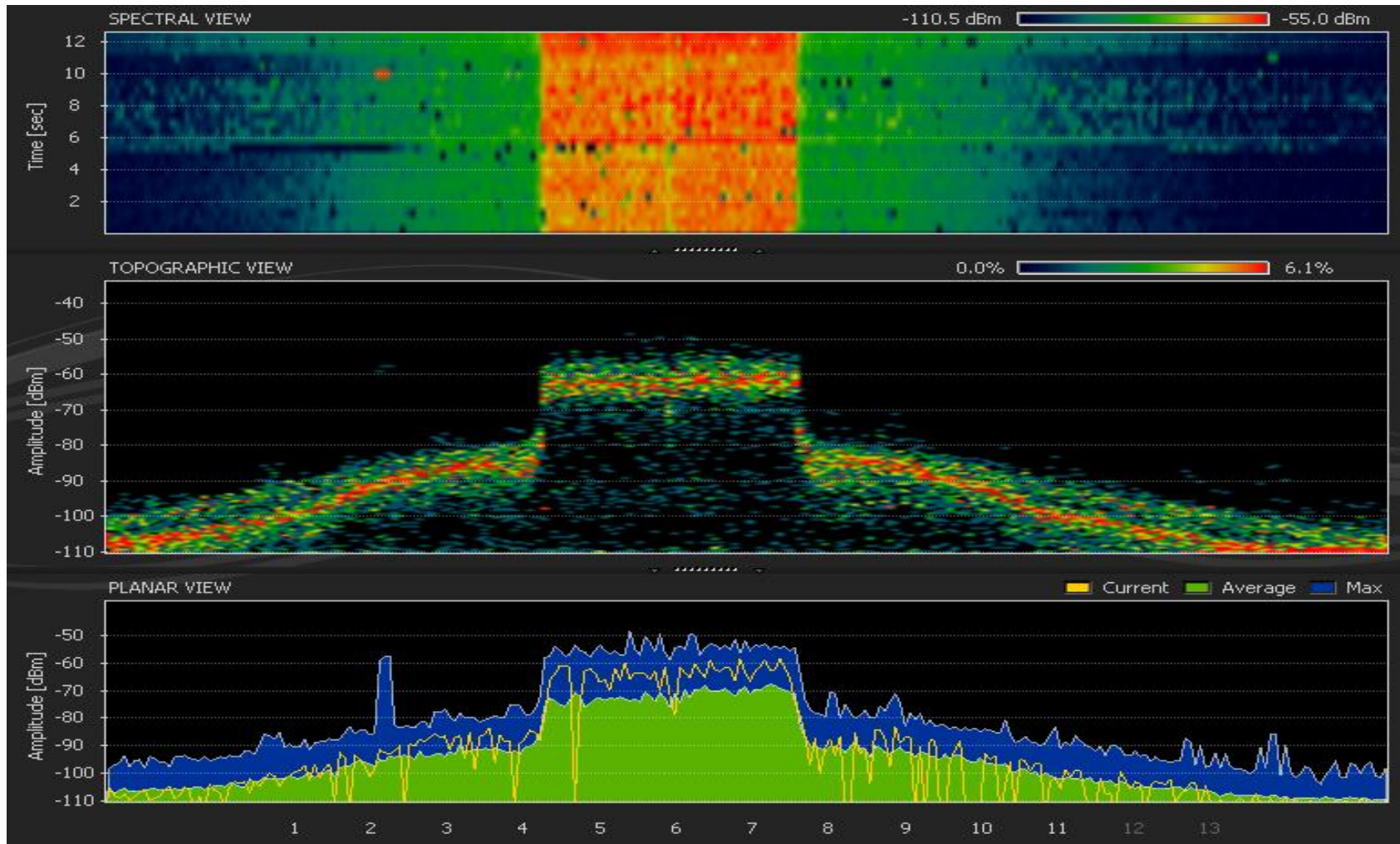
InSSIDer - kostenloser Download von <http://www.metageek.net/>





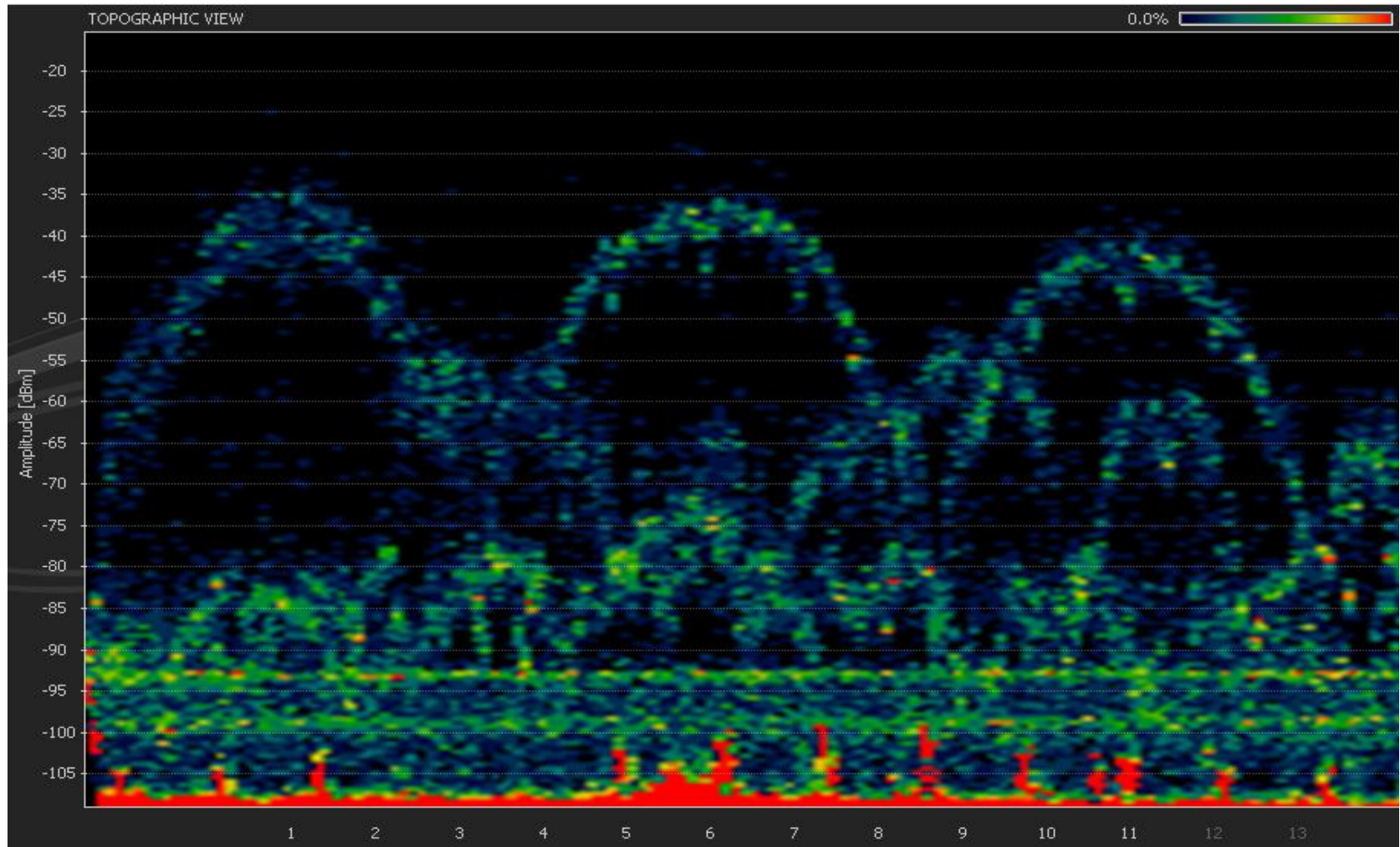
# WLAN Layer 1 Analyse

Wi-Spy - der ‚low cost‘ Spectrum Analyser ([www.metageek.net](http://www.metageek.net))



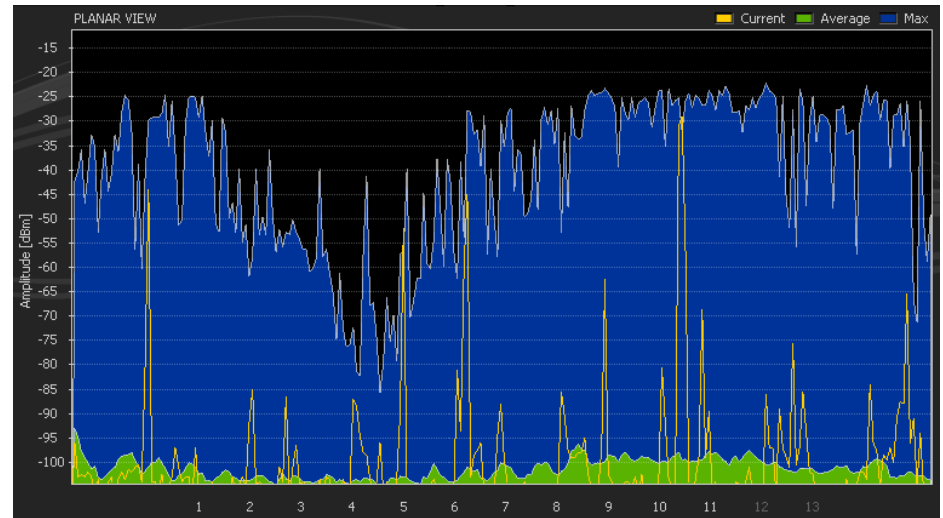
# WLAN Layer 1 Analyse

## Spektrumanalyse der b/g Kanäle

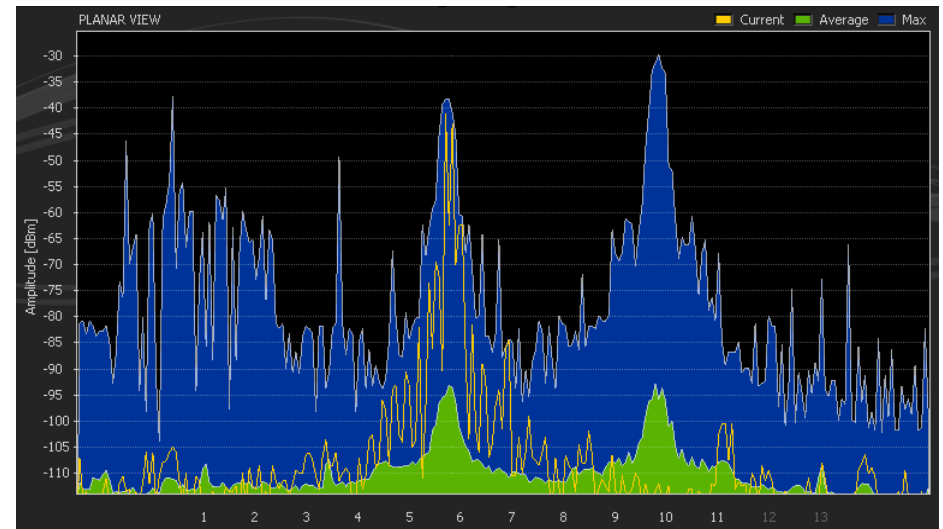


# WLAN Layer 1 Analyse

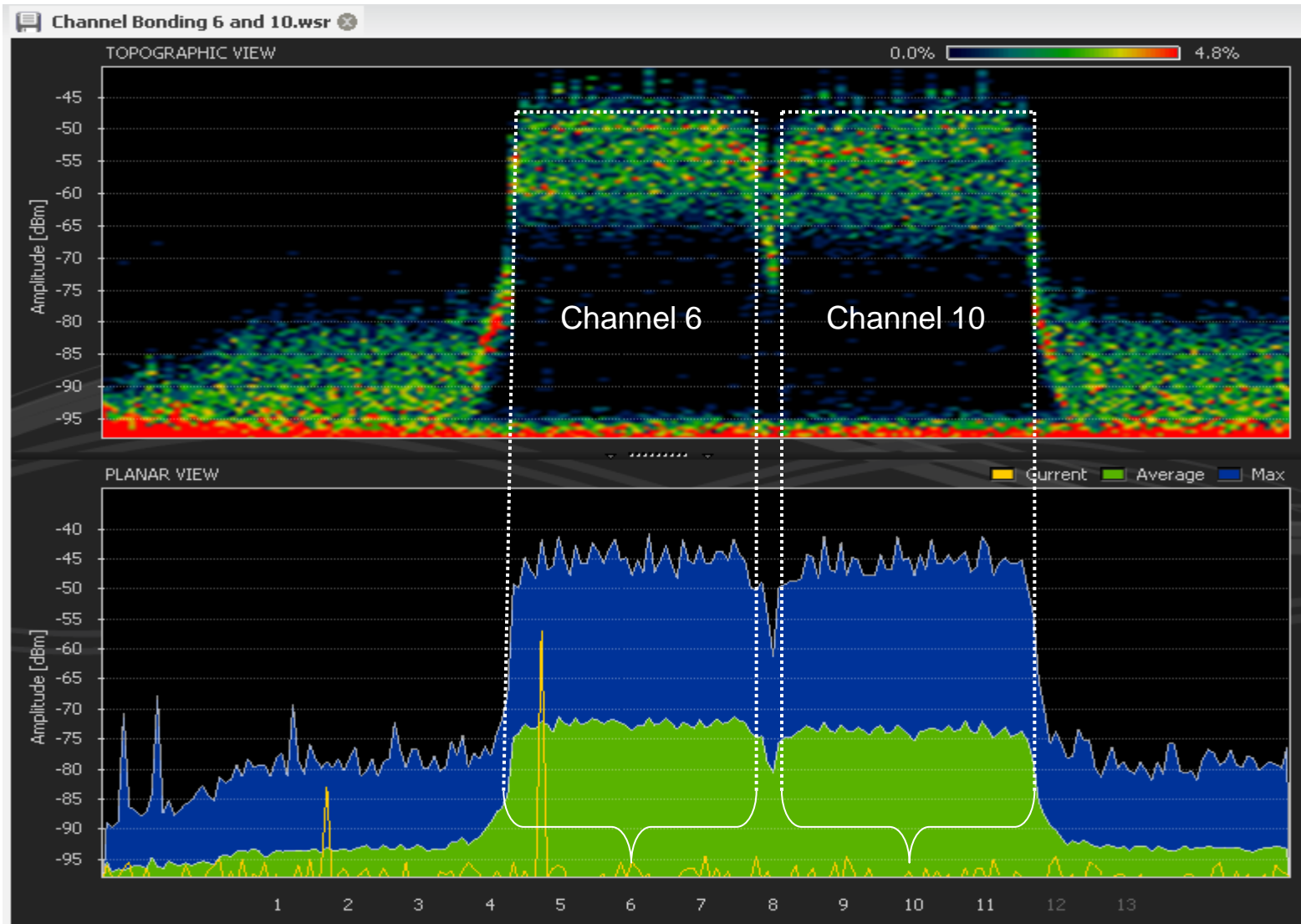
Störsignal eines Mikrowellen-Ofens im 2.4 GHz Band



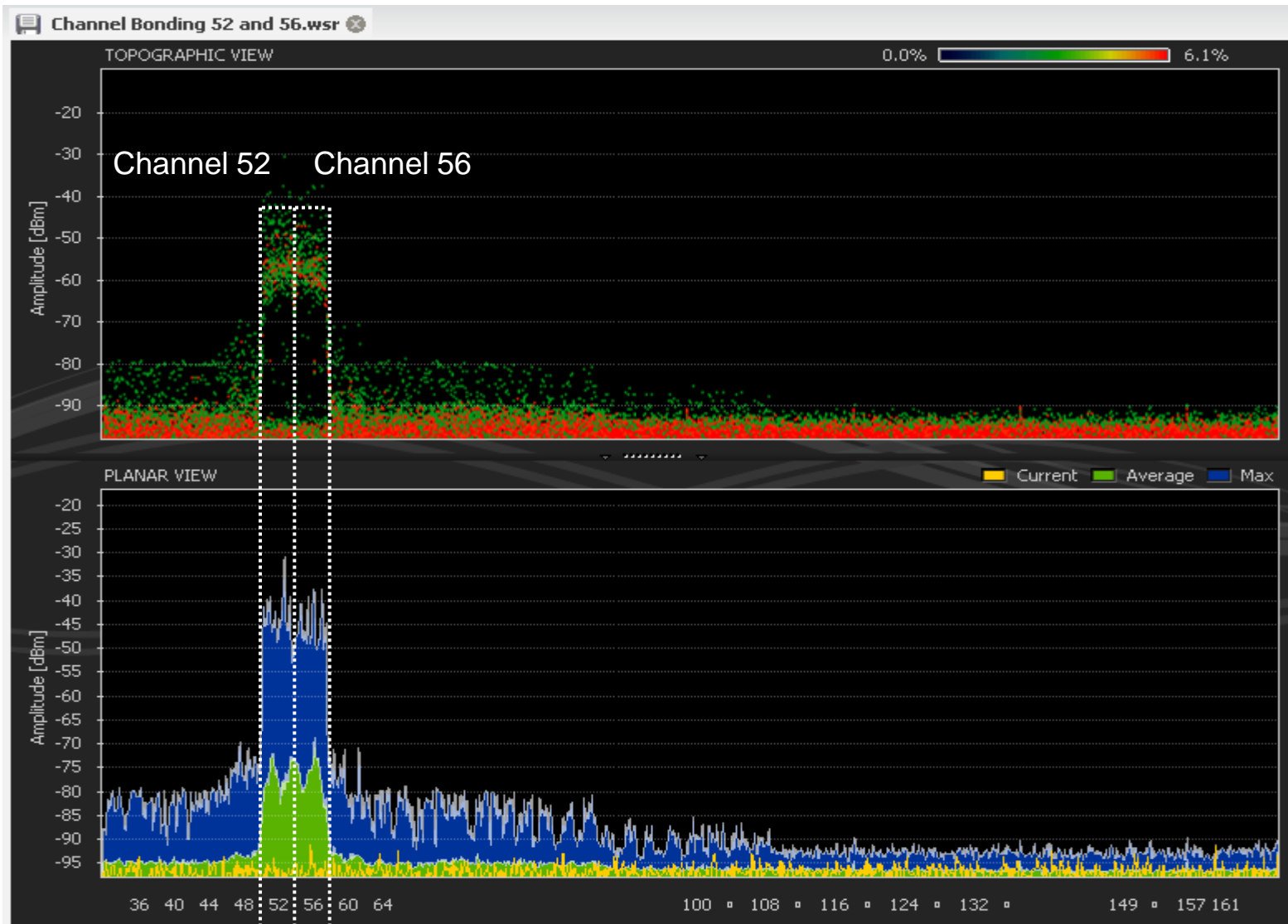
Störsignal eines ‚Frequency Hopping‘ Telefons (z.B. DECT)



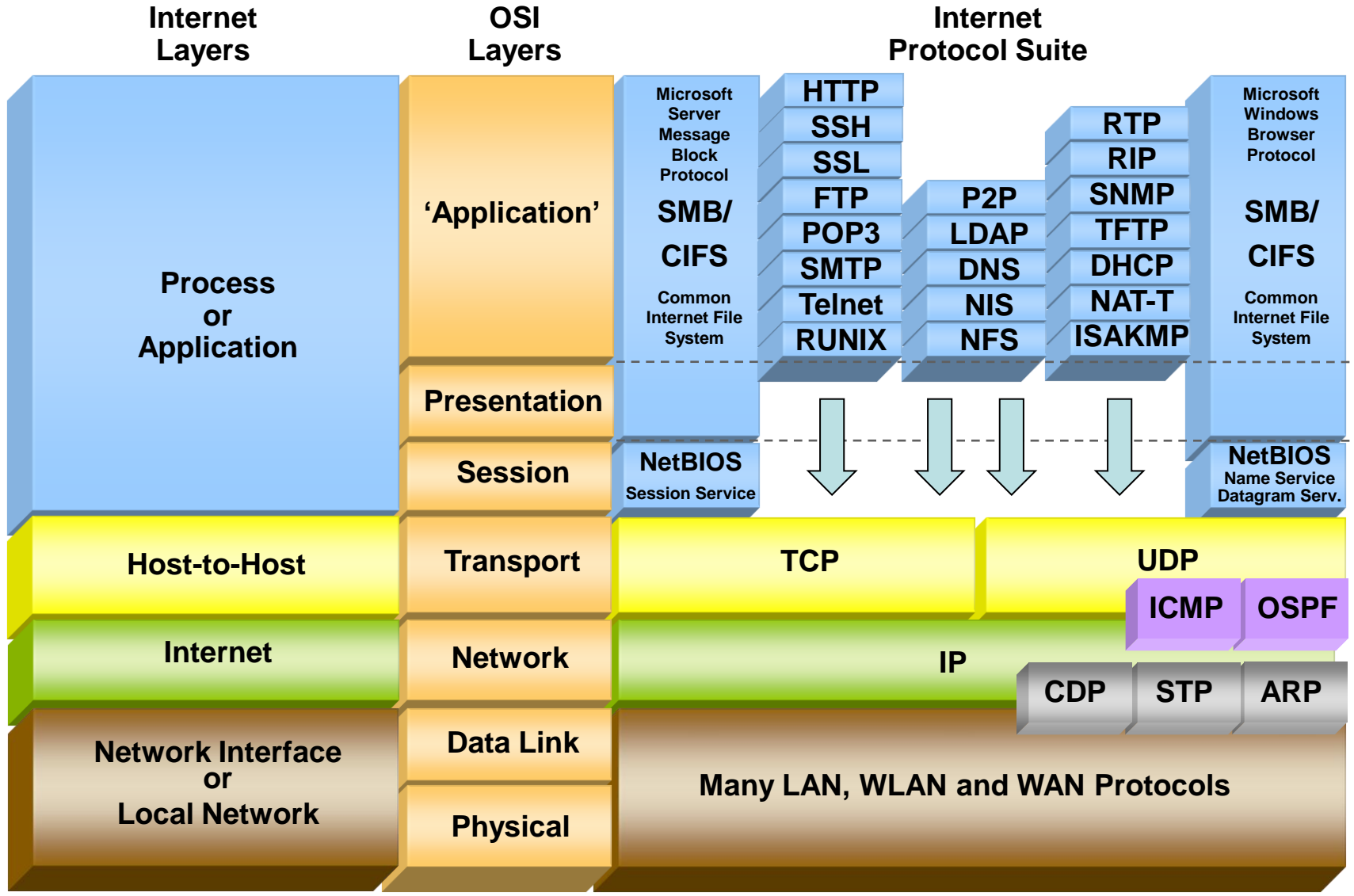
# Channel Bonding im 2.4 GHz Band



# Channel Bonding im 5 GHz Band



# Die Protokoll Übersicht



## WLAN Layer 2 Analyse

### Zugriffssteuerung mit CSMA/CA

Da es sich bei einem Funkkanal um ein gemeinsam genutztes Medium (**shared media**) vergleichbar mit dem früheren Koax-Ethernet handelt, ist eine Zugriffsmethode erforderlich, welche die verfügbare Bandbreite unter den aktiven Stationen möglichst gerecht aufteilt.

Da für den Senden- und Empfangsvorgang derselbe Frequenzkanal verwendet wird, ist eine Übertragung nur in **Halb-Duplex** möglich.

Dies erfordert eine Zugriffsmethode, die eine gerechte Aufteilung der zur Verfügung stehenden Bandbreite gewährleistet. Für 802.11 WLANs wird das Verfahren '**Carrier Sense Multiple Access with Collision Avoidance**' (CSMA/CA) verwendet.



# Übersicht WLAN Standards



Mbps	Coding	Modulation	Description	
1 2	Barker Barker	DBPSK	<b>802.11 DSSS (Clause 15)</b> with ‚Long Preamble‘	<div style="background-color: #FFD700; width: 100px; height: 100px; margin: 0 auto;"></div> <p style="text-align: center;"><b>802.11a</b></p>
5.5 11	CCK CCK	DQPSK	<b>802.11b HR/DSSS (Clause 18)</b> with ‚Short Preamble‘	
6, 9 12, 18 24, 36 48, 54	OFDM OFDM OFDM OFDM	BPSK QPSK 16-QAM 64-QAM	<b>802.11g Extended Rate PHY (ERP)</b>	
7.2-72.2 14.4-144.4	OFDM OFDM	MCS 0-7 MCS 8-15	1 Stream 2 Streams  <b>802.11n High Troughput (HT) Extensions</b>	
2.4 GHz				5 GHz

CCK = Complementary Code Keying  
 DBPSK = Differential Binary Phase-Shift Keying  
 DQPSK = Differential Quadrature Phase-Shift Keying  
 OFDM = Orthogonal Frequency Division Multiplexing

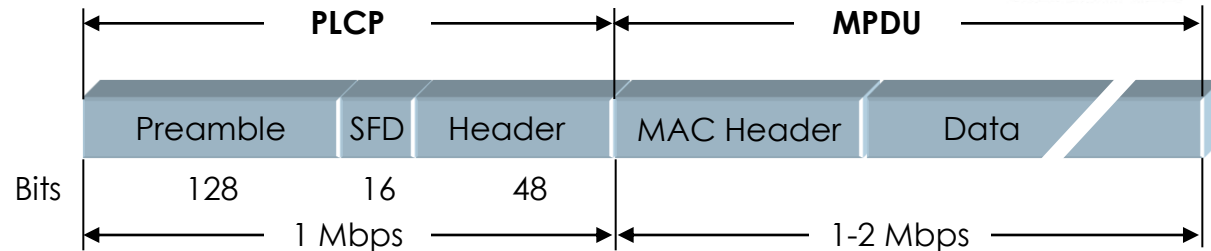
BPSK = Binary Phase-Shift Keying  
 QPSK = Quadrature Phase-Shift Keying  
 QAM = Quadrature Amplitude Modul.  
 MCS = Modulation Coding Scheme



# Übersicht Frame Types (2.4 GHz)



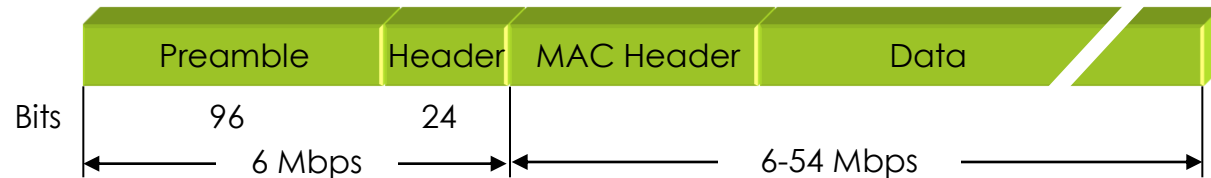
**802.11 DSSS** with  
'Long Preamble'  
Barker Code



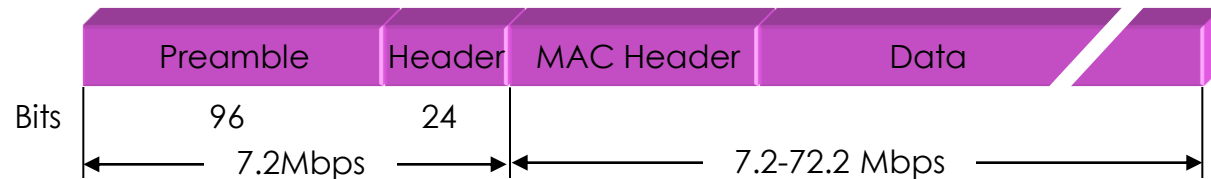
**802.11b HR/DSSS** with  
'Short Preamble'  
Barker / CCK



**802.11g (ERP)**  
Extended Rate PHY  
OFDM



**802.11n (HT)**  
High Throughput  
extended OFDM



PLCP = Physical Layer Convergence Protocol  
MPDU = MAC Layer Protocol Data Unit

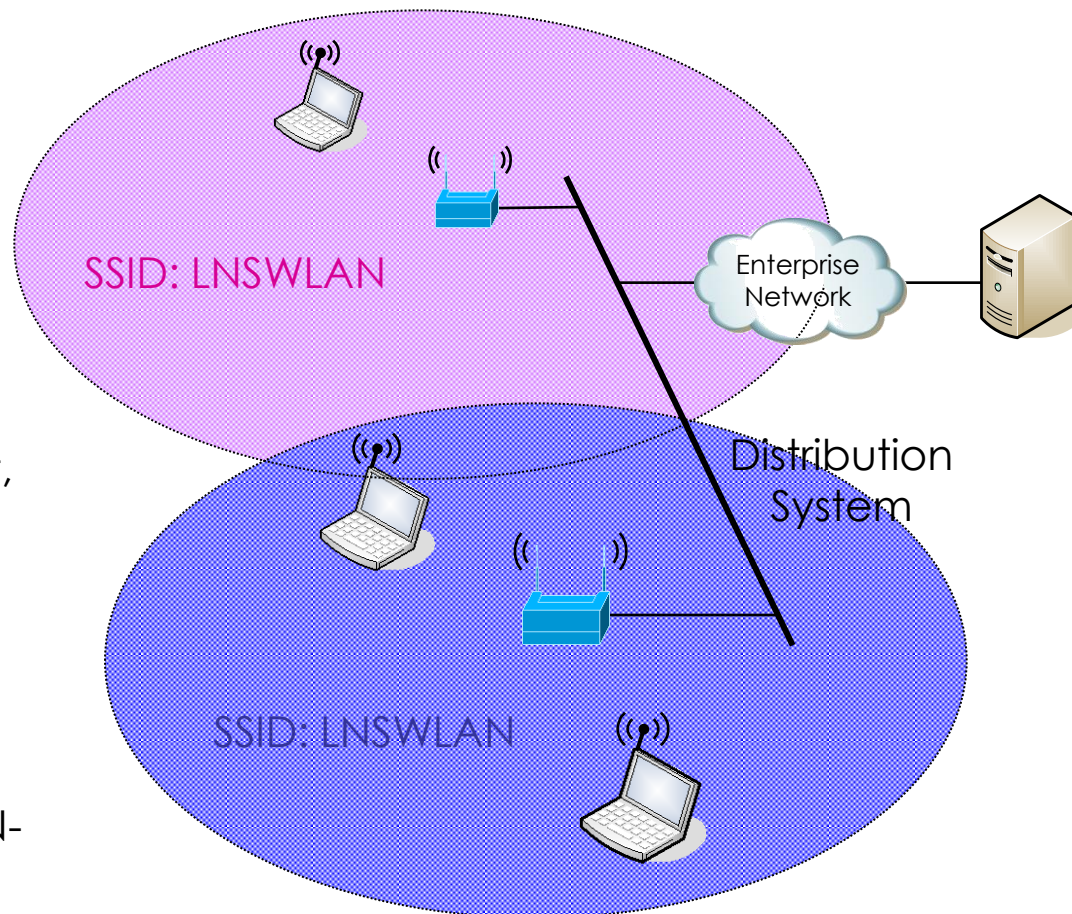
# Architektur von WLANs

Die Namensgebung eines Wireless-Netzwerkes

Die '**Service Set Identity**' (SSID) ist der Name für einen AP oder eine Gruppe von APs. Dieser Name wird beim Einrichten des WLANs in den APs konfiguriert.

Mobile Stationen können so konfiguriert werden, dass sie beim Suchen eines APs die SSID aussenden. Dies bewirkt, dass nur APs mit der gesuchten SSID antworten.

Einige Produkte von APs unterstützen gleichzeitig mehrere SSID-Namen und können damit eine Art WLAN-VLAN bilden.



# Die IEEE 802.11 Frame-Typen

## Die Management Frames:

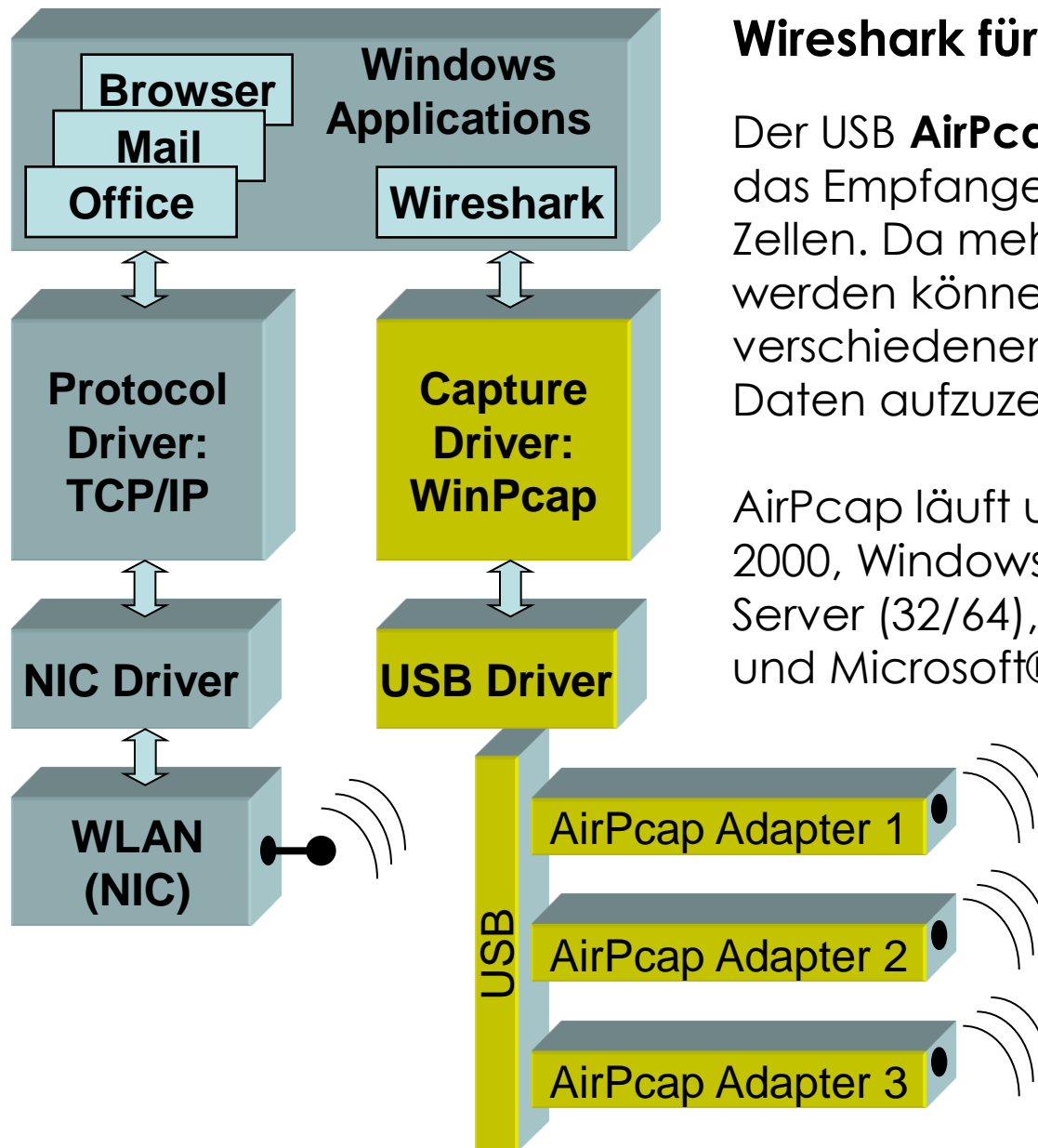
- Beacon
- Probe request and response
- Authentication & Deauthentication
- Association & Disassociation
- Reassociation request and response

## Die Control Frames:

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

## Die Daten Frames:

- Data
- Null Function



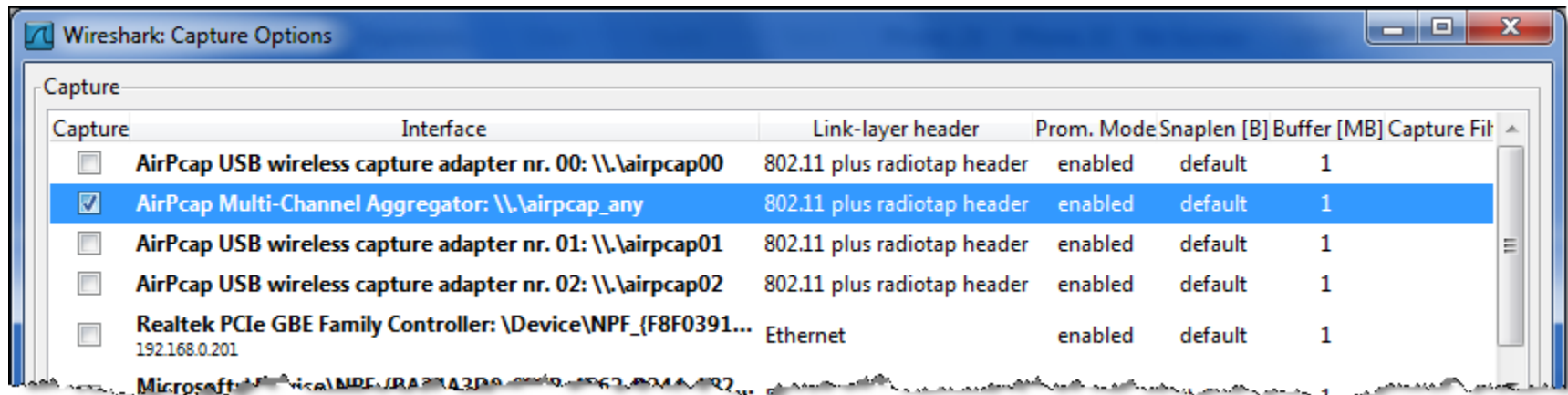
## Wireshark für WLAN 802.11b/g

Der USB **AirPcap** Adapter ermöglicht das Empfangen von Frames in WLAN-Zellen. Da mehrere Adapter installiert werden können, ist es möglich, in verschiedenen Kanälen gleichzeitig Daten aufzuzeichnen.

AirPcap läuft unter Microsoft® Windows 2000, Windows XP (32/64), Windows 2003 Server (32/64), Windows Vista (32/64), und Microsoft® Windows 7 (32/64).

# Konfiguration des Wireshark mit AirPcap

Datenaufzeichnung mit dem **Multi-Channel Aggregator**



Die einzelnen AirPcap Adapter werden z.B. auf die Kanäle **1, 6, 11** oder **1, 7, 13** eingestellt. Dies ermöglicht die lückenlose Aufzeichnung von Roaming Vorgängen.

# Konfiguration des Wireshark mit AirPcap

Datenaufzeichnung mit dem ‚Multi-Channel Aggregator‘

WLAN Probe Request Channel 1 6 11.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter:  Expression... Clear Apply

AirPcap Interface: #ANY | 802.11 Channel: 11,6,1 | FCS Filter: Valid Frame | Decryption Mode: Wireshar | Wireless Settings... Decryption Keys...

No.	Source	Destination	RSSI	Protocol	Info
1	PhilipsC_45:7f:2f	Broadcast	55 dB	IEEE 802.11	Probe Request, SN=54, FN=0, SSID: "\026\022\
2	PhilipsC_45:7f:2f	Broadcast	55 dB	IEEE 802.11	Probe Request, SN=55, FN=0, SSID: "LNSWLAN"
3	PhilipsC_45:7f:2f	Broadcast	55 dB	IEEE 802.11	Probe Request, SN=56, FN=0, SSID: Broadcast
4	PhilipsC_45:7f:2f	Broadcast	56 dB	IEEE 802.11	Probe Request, SN=57, FN=0, SSID: "\026\022\
5	PhilipsC_45:7f:2f	Broadcast	56 dB	IEEE 802.11	Probe Request, SN=58, FN=0, SSID: "LNSWLAN"
6	PhilipsC_45:7f:2f	Broadcast	57 dB	IEEE 802.11	Probe Request, SN=59, FN=0, SSID: Broadcast
7	PhilipsC_45:7f:2f	Broadcast	61 dB	IEEE 802.11	Probe Request, SN=60, FN=0, SSID: "\026\022\
8	PhilipsC_45:7f:2f	Broadcast	61 dB	IEEE 802.11	Probe Request, SN=61, FN=0, SSID: "LNSWLAN"
9	PhilipsC_45:7f:2f	Broadcast	62 dB	IEEE 802.11	Probe Request, SN=62, FN=0, SSID: Broadcast
10	PhilipsC_45:7f:2f	Broadcast	56 dB	IEEE 802.11	Probe Request, SN=63, FN=0, SSID: "\026\022\
11	PhilipsC_45:7f:2f	Broadcast	57 dB	IEEE 802.11	Probe Request, SN=64, FN=0, SSID: "LNSWLAN"
12	PhilipsC_45:7f:2f	Broadcast	56 dB	IEEE 802.11	Probe Request, SN=65, FN=0, SSID: Broadcast
13	PhilipsC_45:7f:2f	Broadcast	56 dB	IEEE 802.11	Probe Request, SN=68, FN=0, SSID: Broadcast
14	PhilipsC_45:7f:2f	Broadcast	55 dB	IEEE 802.11	Probe Request, SN=75, FN=0, SSID: "\026\022\

# Die wichtigsten WLAN-Prozesse

Die Präsenzmarkierung des Access Points ‚Beacon‘

Mit Hilfe des Management Frames ‚**Beacon**‘ (deutsch: Signalfeuer) markiert ein AP seine Präsenz in einer Funkzelle.

Der ‚Beacon‘ Frame enthält wichtige Informationen über die Eigenschaften und Fähigkeiten (Capabilities) des AP wie etwa:

- Zeitstempel
- Beacon-Intervall
- Kanalnummer
- Unterstützte Geschwindigkeiten
- Unterstützung von Verschlüsselung
- BSSID (Basic Services Set ID) MAC-Adresse des AP
- ESSID (Extended Services Set ID) Konfigurierter Name
- NON-ERP Stationen präsent
- TIM (Traffic Indicator Map)
- Herstellerspezifische Optionen
- USW.



# Die wichtigsten WLAN-Prozesse

## Die Präsenzmarkierung des Access Points ‚Beacon‘

**WLAN Beacon.pcap - Wireshark**

File Edit View Go Capture Analyze Statistics Help

Filter:  Expression... Clear Apply

AirPcap Interface: #00 | 802.11 Channel: 1 | FCS Filter: Valid Frame | Decryption Mode: Driver | Wireless Settings... Decryption Keys...

No.	Source	Destination	RSSI	Protocol	Info
1	Cisco 11:1f:60	Broadcast	51 dB	IEEE 802.11	Beacon frame, SN=9, FN=0, BI=100, SSID: "LNSWLAN",
2	Cisco_11:1f:60	Broadcast	50 dB	IEEE 802.11	Beacon frame, SN=10, FN=0, BI=100, SSID: "LNSWLAN",
3	Cisco_11:1f:60	Broadcast	51 dB	IEEE 802.11	Beacon frame, SN=11, FN=0, BI=100, SSID: "LNSWLAN",
4	Cisco_11:1f:60	Broadcast	49 dB	IEEE 802.11	Beacon frame, SN=12, FN=0, BI=100, SSID: "LNSWLAN",
5	Cisco_11:1f:60	Broadcast	51 dB	IEEE 802.11	Beacon frame, SN=13, FN=0, BI=100, SSID: "LNSWLAN",

Frame 1 (188 bytes on wire, 188 bytes captured)

- Radiotap Header v0, Length 18
- IEEE 802.11
- IEEE 802.11 wireless LAN management frame
- Fixed parameters (12 bytes)**
  - Timestamp: 0x00000001F40FA192
  - Beacon Interval: 0.102400 [Seconds]
- Capability Information: 0x0421
- Tagged parameters (134 bytes)**
  - SSID parameter set: "LNSWLAN"
  - Supported Rates: 1.0 (B) 2.0 (B) 5.5 (B) 6.0 9.0 11.0 (B) 12.0 18.0
  - DS Parameter set: Current Channel: 1
  - (TIM) Traffic Indication Map: DTIM 0 of 2 bitmap empty
  - ERP Information: no Non-ERP STAs, do not use protection, short or long preambles
  - Extended Supported Rates: 24.0 36.0 48.0 54.0
  - Cisco Unknown 1 + Device Name
  - Vendor Specific: Aironet Unknown
  - Vendor Specific: Aironet CCX version = 3
  - Vendor Specific: Aironet Qos
  - Vendor Specific: WME



# Die wichtigsten WLAN-Prozesse

## Verbinden mit einem Access Point

WLAN Authentication Open\_01.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: `!(wlan.fc == 0x0080)` Expression... Clear Apply

AirPcap Interface: #02 | 802.11 Channel: 1 | FCS Filter: Valid Frame | Decryption Mode: None | Wireless Settings... Decryption Keys...

No.	Source	Destination	RSSI	Protocol	Info
49	PhilipsC_45:7f:2f	Cisco_92:ad:21	51 dB	IEEE 802.11	Association Request, SN=1, FN=
50		PhilipsC_45:7f:2f (RA)	57 dB	IEEE 802.11	Acknowledgement
51	Cisco_92:ad:21	PhilipsC_45:7f:2f	55 dB	IEEE 802.11	Association Response, SN=152
52		Cisco_92:ad:21 (RA)	52 dB	IEEE 802.11	Acknowledgement
62	Aironet_55:ed:2f	PhilipsC_45:7f:2f	56 dB	WLCCP	WLCCP frame
63		Cisco_92:ad:21 (RA)	52 dB	IEEE 802.11	Acknowledgement

status code: successful (0x0000)

**Association ID: 0x0002**

- Tagged parameters (50 bytes)
  - Supported Rates: 1.0 (B) 2.0 (B) 5.5 11.0
    - Tag Number: 1 (Supported Rates)
    - Tag length: 4
    - Tag interpretation: Supported rates: 1.0 (B) 2.0 (B) 5.5 11.0 [Mbit/sec]

## Die wichtigsten WLAN-Prozesse

Datenübertragung vom und zum AP

Nach erfolgreicher Authentisierung und Assoziierung beim AP kann die mobile Station mit der Übertragung von Benutzerdaten beginnen.

Bedingt durch die Störempfindlichkeit des Übertragungsmediums Luft wird jeder gesendete Frame vom Empfänger unmittelbar bestätigt.

Frames, die bei der Übertragung z.B. durch Störungen beschädigt wurden, werden vom Empfänger nicht bestätigt und lösen damit beim Sender eine erneute Übertragung aus.

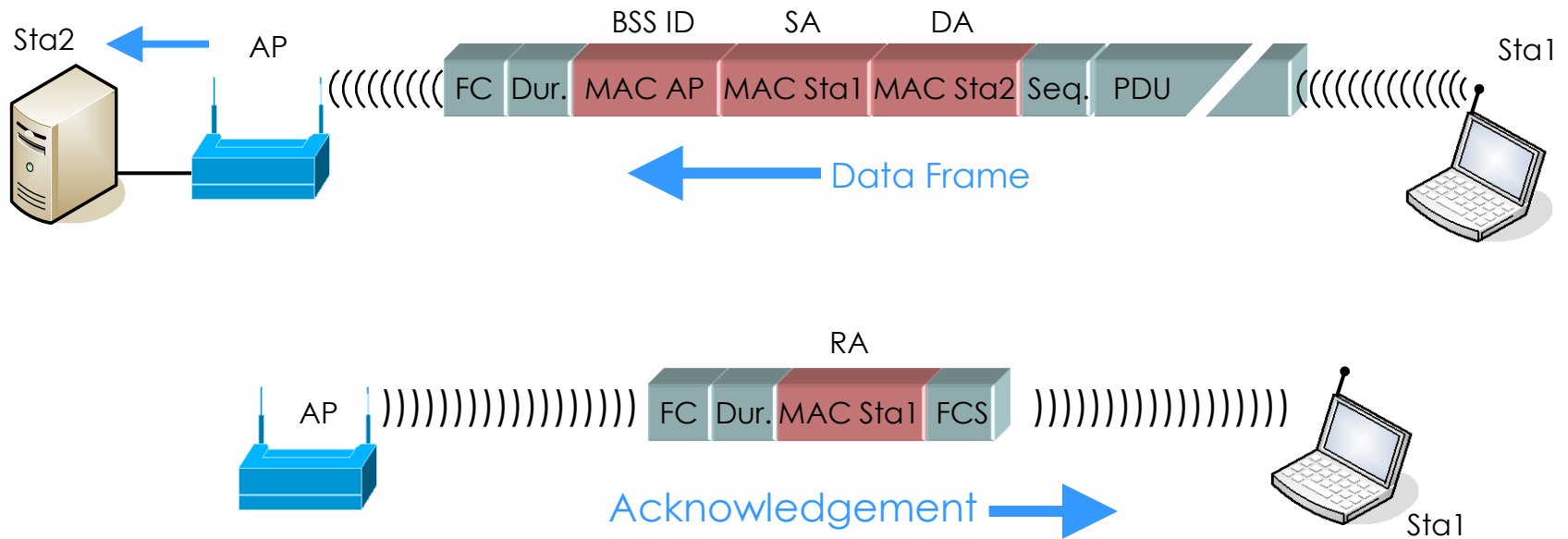
Nach zu vielen nicht bestätigten Frames wird die Übertragungsgeschwindigkeit vom Sender reduziert und erneut versucht, den Frame zu übertragen.



# Die wichtigsten WLAN-Prozesse

Datenübertragung vom und zum AP

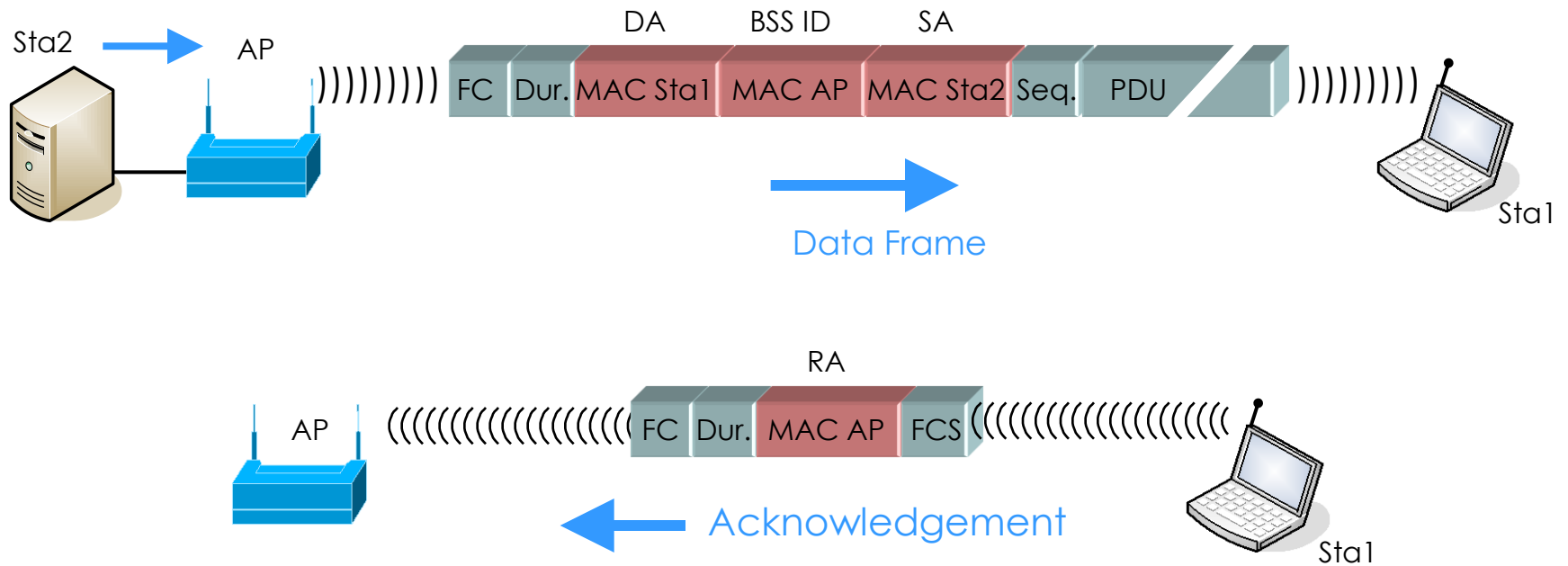
Frame Format für Daten von der mobilen Station Richtung AP:



# Die wichtigsten WLAN-Prozesse

Datenübertragung vom und zum AP

Frame Format für Daten vom AP Richtung mobile Station:



# Die wichtigsten WLAN-Prozesse

Datenübertragung vom und zum AP

**WLAN Data\_01.pcap - Wireshark**

File Edit View Go Capture Analyze Statistics Help

Filter:  Expression... Clear Apply

AirPcap Interface: #02 | 802.11 Channel: 1 | FCS Filter: Valid Frame | Decryption Mode: None | Wireless Settings... Decryption Keys...

No. -	Source	Destination	RSSI	Protocol	Info
119		PhilipsC_45:7f:2f (RA)	44 dB	IEEE 802.11	Acknowledgement
120	192.168.0.202	85.119.154.59	62 dB	HTTP	GET /WIRESHARK.swf HTTP/1.1
121		PhilipsC_45:7f:2f (RA)	43 dB	IEEE 802.11	Acknowledgement
122	85.119.154.59	192.168.0.202	43 dB	HTTP	HTTP/1.1 304 Not Modified
123		Cisco_11:1f:60 (RA)	62 dB	IEEE 802.11	Acknowledgement
124	192.168.0.202	85.119.154.59	61 dB	TCP	2461 > http [ACK] Seq=697 Ack=
125		PhilipsC_45:7f:2f (RA)	43 dB	IEEE 802.11	Acknowledgement

<

- ⊕ Frame 108 (422 bytes on wire, 422 bytes captured)
- ⊕ Radiotap Header v0, Length 24
- ⊕ IEEE 802.11
- ⊕ Logical-Link Control
- ⊕ Internet Protocol, Src: 192.168.0.202 (192.168.0.202), Dst: 85.119.154.59 (85.119.154.59)
- ⊕ Transmission Control Protocol, Src Port: 2461 (2461), Dst Port: http (80), Seq: 1, Ack: 1,
- ⊕ Hypertext Transfer Protocol

# Die wichtigsten WLAN-Prozesse

## Wechsel auf einen anderen AP

Der Wechsel einer mobilen Station auf einen nächsten AP wird Roaming (to roam: herumwandern) genannt.

Bereits während eine mobile Station mit einem AP assoziiert ist, werden in regelmässigen Abständen alle anderen Kanäle nach weiteren APs abgesucht (aktiv oder passiv).

Dies als Vorbereitung, um einen allfälligen Kanalwechsel möglichst unterbruchsfrei abwickeln zu können.



# Die wichtigsten WLAN-Prozesse

## Wechsel auf einen anderen AP

WLAN Roaming\_01.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter:  Expression... Clear Apply

AirPcap Interface: #ANY | 802.11 Channel: 1,6,11 | FCS Filter: Valid Frame | Decryption Mode: None | Wireless Settings... Decryption Keys...

No.	Source	Destination	RSSI	Protocol	Info
194	PhilipsC_45:7f:2f	Cisco_92:ad:21	69 dB	IEEE 802.11	Reassociation Request, SN=284
195		PhilipsC_45:7f:2f (RA)	71 dB	IEEE 802.11	Acknowledgement
196	Cisco_92:ad:21	PhilipsC_45:7f:2f	71 dB	IEEE 802.11	Reassociation Response, SN=750
197		Cisco_92:ad:21 (RA)	77 dB	IEEE 802.11	Acknowledgement
198	Cisco_11:1f:60	Broadcast	24 dB	IEEE 802.11	Beacon frame, SN=2029, FN=0, BI=

Frame 194 (107 bytes on wire, 107 bytes captured)

- Radiotap Header v0, Length 24
- IEEE 802.11
- IEEE 802.11 wireless LAN management frame
  - Fixed parameters (10 bytes)
    - Capability Information: 0x0021
    - Listen Interval: 0x0001
    - Current AP: Cisco\_11:1f:60 (00:0f:24:11:1f:60)**
  - Tagged parameters (45 bytes)
    - SSID parameter set: "LNSWLAN"
    - Supported Rates: 1.0 2.0 5.5 11.0
    - Cisco Unknown 1 + Device Name

## Praxis Problem: Blockierter WLAN Client

- Ein grosses Warenhaus klagt über **sporadische Aufhänger** bei seinen mobilen Barcode Scannern, diese dauern bis in den Minutenbereich.
- Aufwändige Vorabklärungen und Einstellungsänderungen auf den Access Points und den Mobile Clients **über Monate** brachten **keine Verbesserung der Situation**.
- Beide Hersteller verharrten auf dem Standpunkt ihre Geräte verhielten sich konform (**Fingerpointing**).
- Daten sind WPA2 verschlüsselt, der Schlüssel steht **nicht zur Verfügung**.
- Dieses Beispiel zeigt, dass WLAN Probleme auch **ohne Entschlüsselung** der User-Daten eingegrenzt werden können.



# Praxis Problem: Blockierter WLAN Client

Mögliche Ursachen:

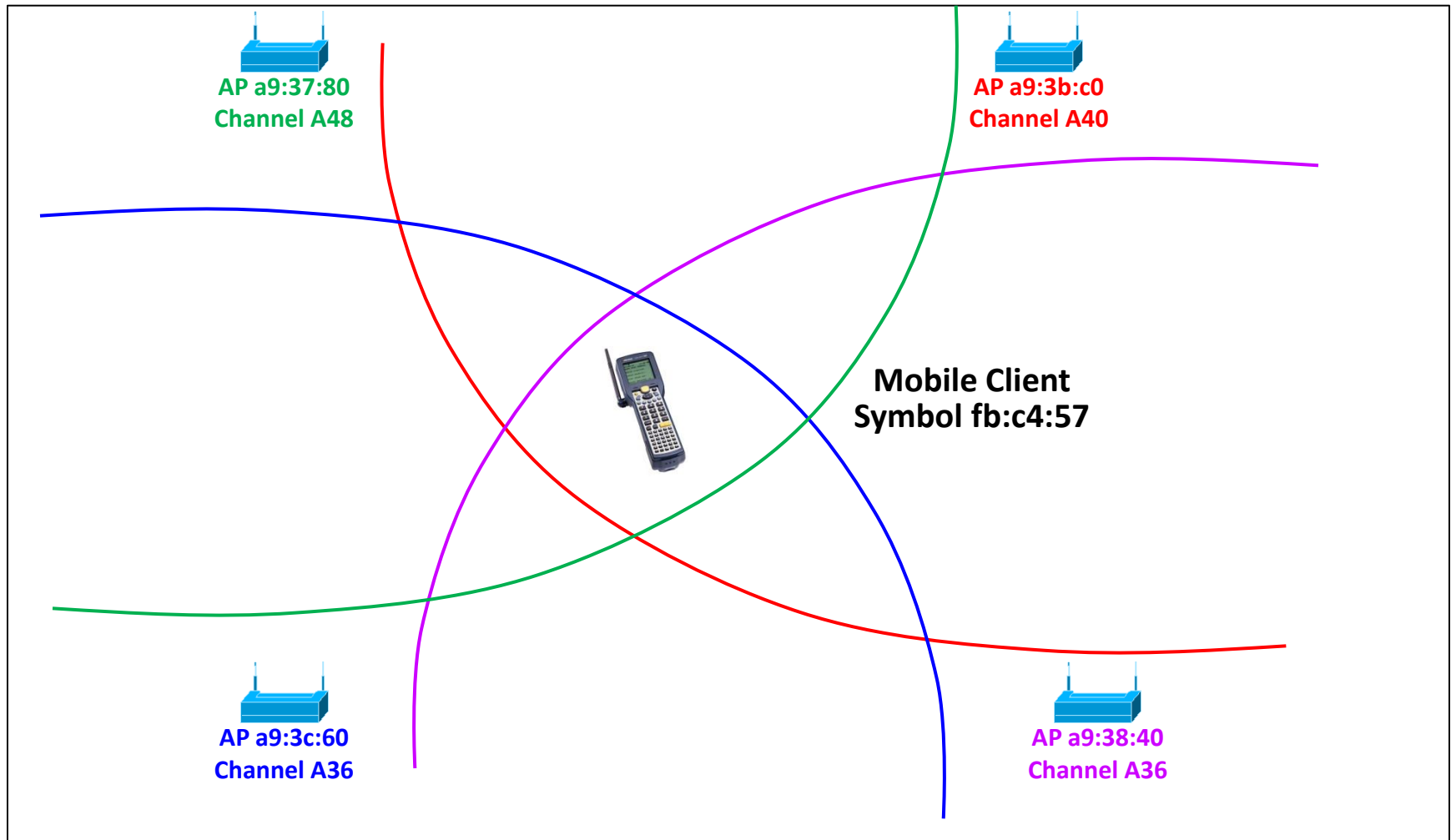
## Layer 1

- **Abdeckungslücken** zwischen den Funkzellen
- **Interferenzen** von Fremdgeräten (Störquellen)
- **Überlastete** Funkzellen (überlappende Zellengrößen)

## Layer 2

- Roaming Problem
- Fehlkonfiguration oder Defekt auf dem **Access Points**
- Fehlkonfiguration oder Defekt auf dem **Mobile Client**
- **Applikation-** oder **Bedienungsproblem**

# Praxis Problem: Blockierter WLAN Client



# Praxis Problem: Blockierter WLAN Client

Systematisches Vorgehen bei der Fehlersuche:

## Ist-Aufnahme

- Wie viele APs sind in Reichweite ? **MAC Adresse und Kanal Nr.**
- Mit welchem AP ist der Client **SymbolTe\_fb:c4:57** assoziiert ?

## Trace-Analyse

- Bleibt der Client mit diesem AP assoziiert, oder **roamt** er weg ?
- Falls ja, ist der Roaming Prozess **erfolgreich**?
- Sind die **blockierten** Zeitabschnitte des Clients zu erkennen?
- Korrigiert sich die Situation **selbsttätig**?

## Schlussfolgerung und weiteres Vorgehen:

- Wo liegt die Ursache: **Client oder Access Point**?

## Praxis Problem: Blockierter WLAN Client

Der **Messpunkt** des Wireshark Analysers ist relevant!

**Wo** soll die Aufzeichnung stattfinden?

- Beschränkt sich das Problem auf eine Zelle, messen Sie in der **Nähe des Access Points**
- Vermuten Sie ein Roaming Problem, messen Sie in der **Nähe des Mobile Client**

**Wie** und **Was** messe ich?

- Verwenden Sie die **S/N ratio** der Beacons und des Clients um Ihre Position zu definieren
- Die **Signal to Noise (S/N) ratio** sollte  $\geq 20$  db sein
- **Eine Grafik sagt mehr als tausend Frames!**

# Praxis Problem: Blockierter WLAN Client

## Signalstärke der verschiedenen Access Points

WLAN Client Blocked.pcap [Wireshark 1.6.8 (SVN Rev 42761 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

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)

Jetzt aufnehmen

- 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

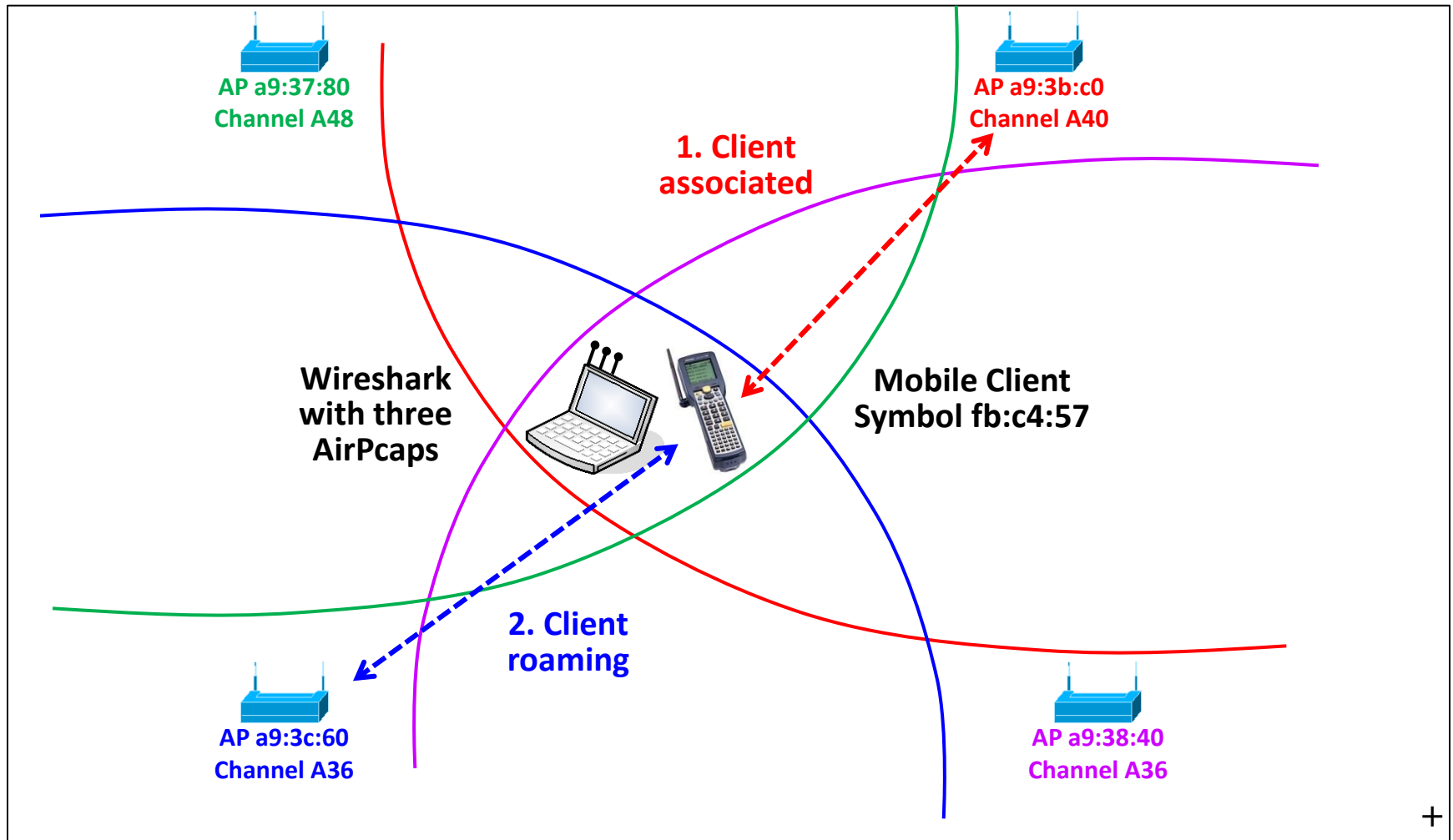
# Praxis Problem: Blockierter WLAN Client

Signalstärke der verschiedenen Access Points

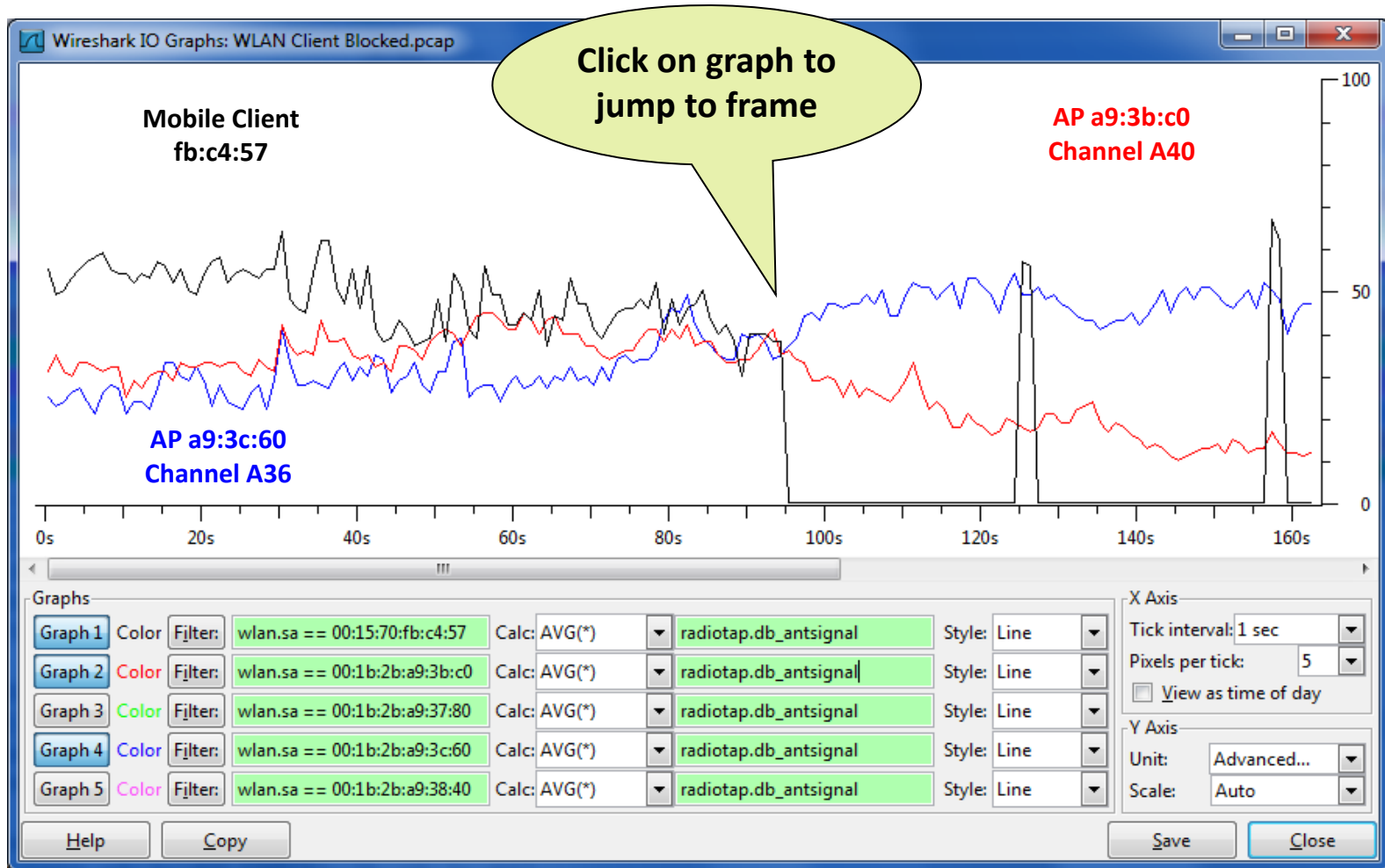


S/N ratio von vier Access Points

# Praxis Problem: Blockierter WLAN Client



# Praxis Problem: Blockierter WLAN Client



S/N ratio von **zwei Access Points** und des **Client**s



# Praxis Problem: Blockierter WLAN Client

Filter auf **MAC Adresse** des Clients (Source oder Destination)

No.	Time	Channel	TX Speed	Signal (dBm)	SNR	Source	Destination	Protocol	Info
5640	0.000000	5200 [A 40]	54.0	-55	41 dB	SymbolTe_fb:c4:57	All-MSRP-routers_00	LLC	U, Tunc=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, FI
5644	0.000356	5180 [A 36]	24.0	-57	39 dB	Cisco_a9:3c:60	SymbolTe_fb:c4:57	802.11	Authentication, SN=502, FI
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	0.000630	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 [RFC3746]
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, FI
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, F
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, FI

- Der AP sendet dem Client in Frame Nr. 5650 den **Request Identity**
- Der Client sollte mit **Response Identity** antworten
- Da diese ausbleibt, sendet AP in Frame Nr. 7331 **Deauthentication**
- Ab Frame Nr. 7415 versucht der Client erneut die **Aufnahme** beim AP
- Der Prozess ist erfolgreich, der Client blockiert jedoch für **weitere 30 sec.**
- Nach dem **dritten** Versuch in Frame 10809 antwortet der Client korrekt.
- Der Client war während rund **90 sec. blockiert.**

## Praxis Problem: Blockierter WLAN Client

Schlussfolgerung und weiteres Vorgehen:

- Der letzte Frame vor der Blockierung war der **Request Identity** vom Access Point
- Wir sahen **keine** Reaktion des Clients
- Ist dieser Frame beim Client **angekommen?**
  
- Wenn **JA**, liegt die Ursache beim **Client!**
- Wenn **NEIN**, liegt die Ursache beim **AP!**



Können wir mit Bestimmtheit feststellen, ob der **Request Identity** beim Client angekommen ist?

**Yes we Can!** Werfen wir einen genaueren Blick auf das Trace File.  
**Nach welcher Art Frame suchen wir?**

Hinweis: Achten Sie auf den Display Filter

# Praxis Problem: Blockierter WLAN Client

Anzeige des Trace Files **ohne** Display Filter

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	0.028598	5200 [A 40]	6.0	-59	36 dB	CISCO_a9:3b:c0	Broadcast	802.11	Beacon frame, SN=3869, 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	0.022409	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

- Im WLAN werden alle Frames mit einem **Acknowledge** bestätigt
- Der Client bestätigt den Request ID in **Frame 5651**
- Der Client sollte den Request verarbeiten und mit **Response ID** antworten
- Ein **Fehler** in der Client Firmware verursachte diese sporadischen Hänger
- Der Hersteller lieferte einen **Upgrade** und das **Problem war gelöst!**

# Danke für Ihre Aufmerksamkeit

Gerne begrüßen wir Sie an einem Kurs von Leutert NetServices

Grundkurse bei Studerus:

- **NET-Analyse** mit Wireshark
- **IPv6-Protokoll** Einführung

LAB-Kurse bei HSR  
(Hochschule Rapperswil)

- **TCP/IP Protokoll**
- **WLAN Analyse**
- **IPv6 Praxisworkshop**



Registrieren sie sich für den technischen Newsletter [www.wireshark.ch](http://www.wireshark.ch)