WLAN-Trouble-Shooting

präsentiert von Rolf Leutert

www.wireshark.ch

LEUTERT NetServices

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

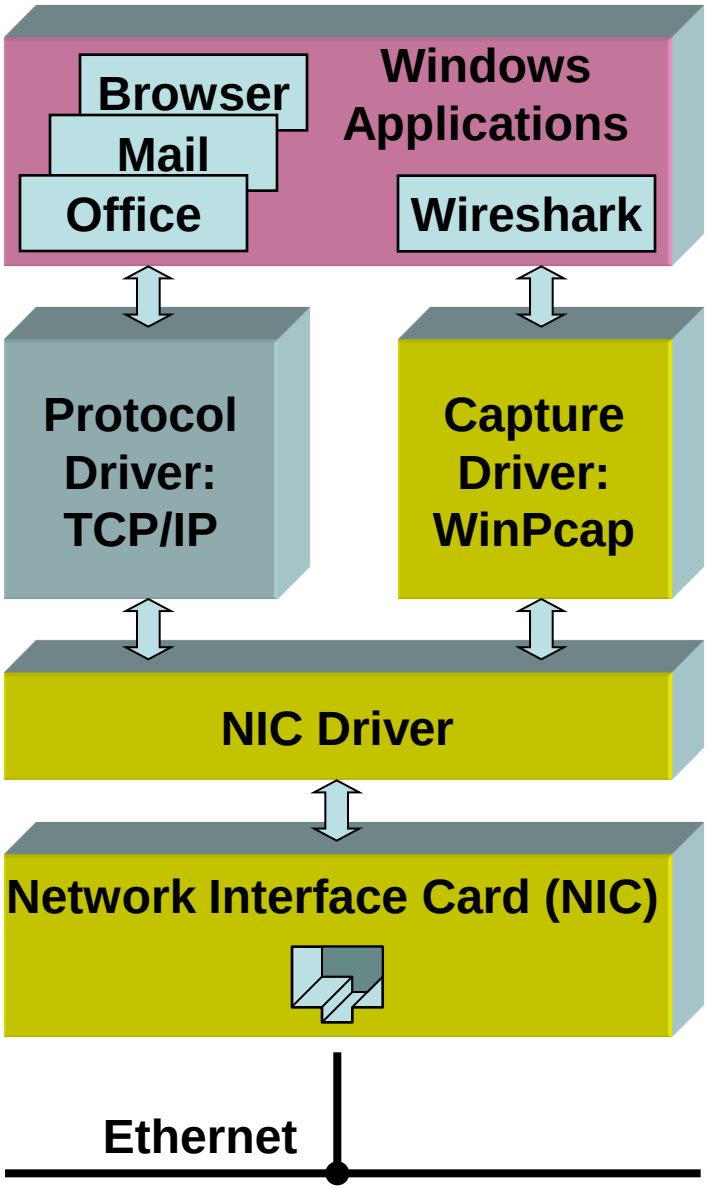
leutert@wireshark.ch
www.wireshark.ch

Sniffer Certified MASTER

Wireshark University WIRESHARK® CERTIFIED NETWORK ANALYST

Wireshark Network Protocol Analyser

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



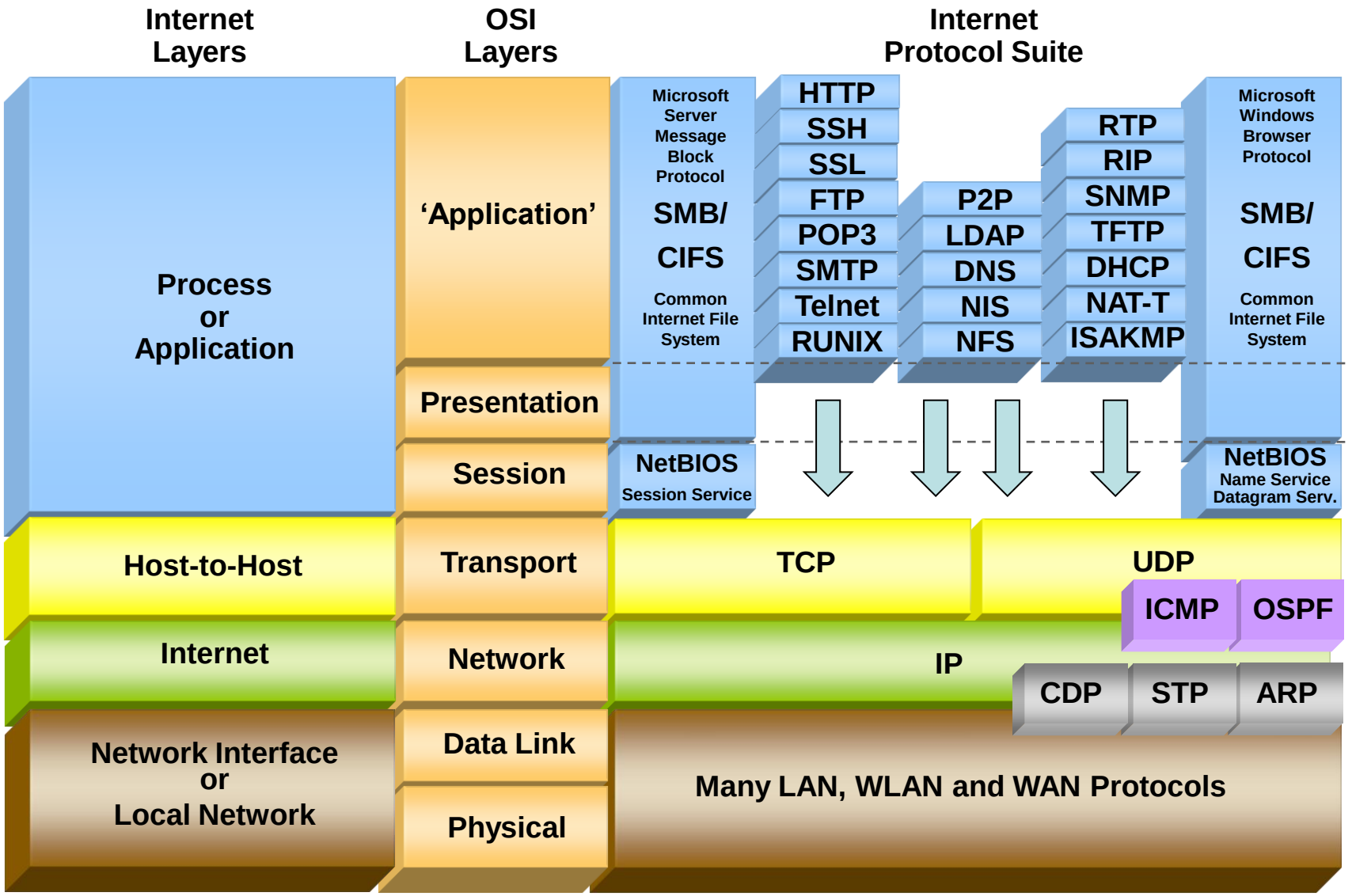
Wireshark für Ethernet

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

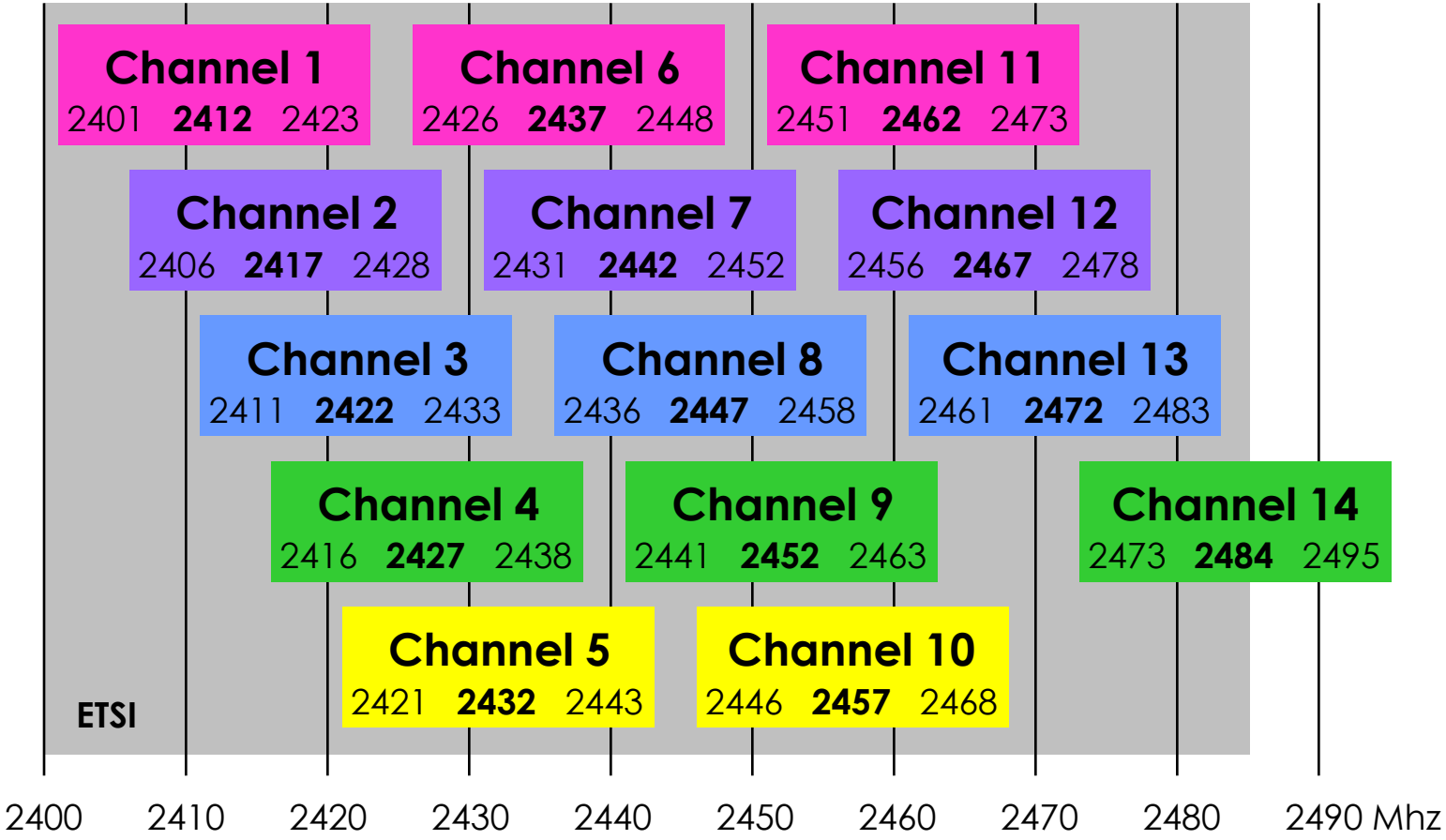
Der NIC Driver kann von WinPcap so konfiguriert werden, dass sämtliche Frames von Ethernet an WinPcap weitergeleitet werden *(Promiscuous Mode)*.

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

Die Protokoll Übersicht



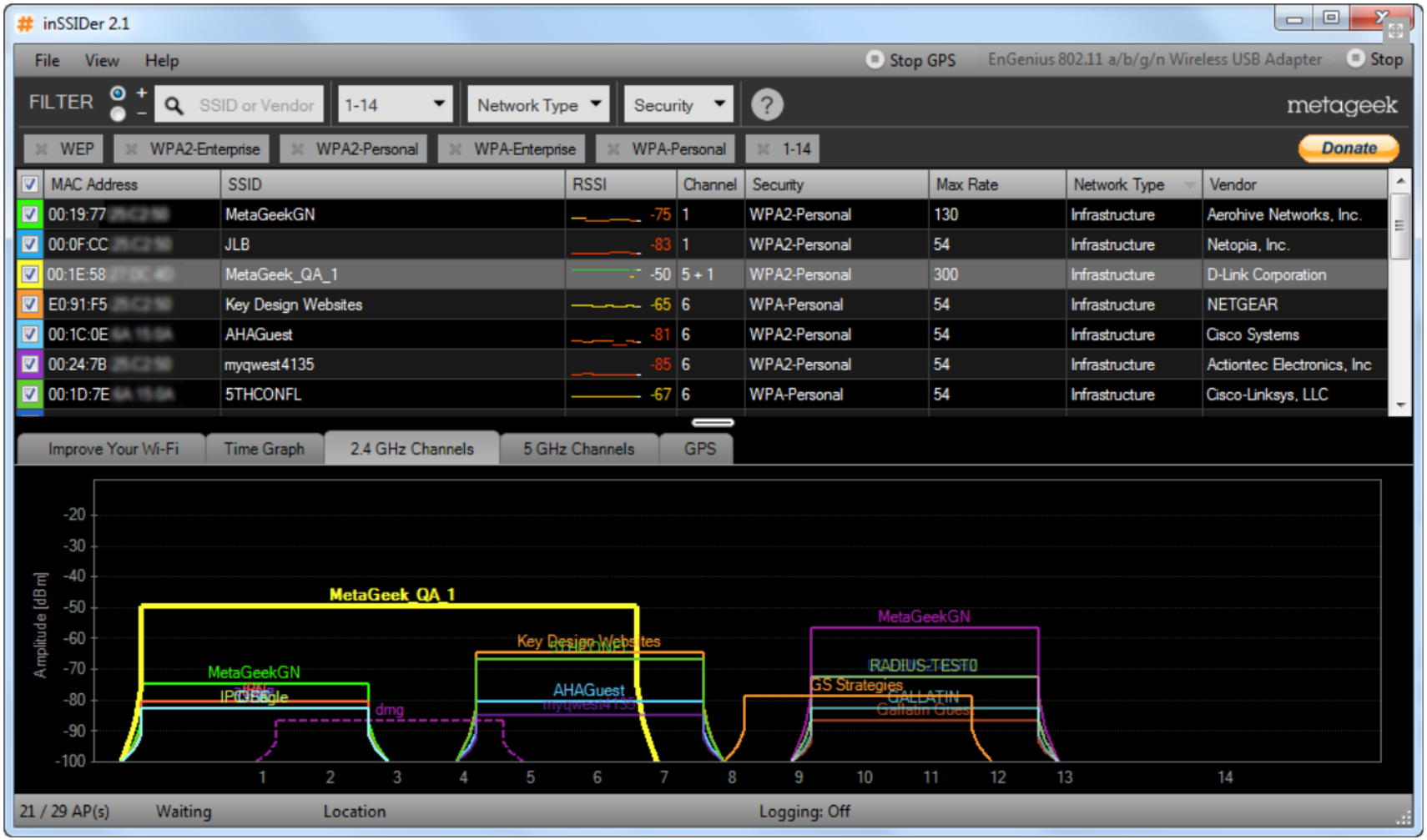
Frequenzaufteilung im 2.4 GHz Band für IEEE 802.11b/g



Zugelassene Frequenzbereiche:	Ch1 – Ch11 USA (FCC)	Ch1 - Ch14 Japan
	Ch1 – Ch13 Most of the World	

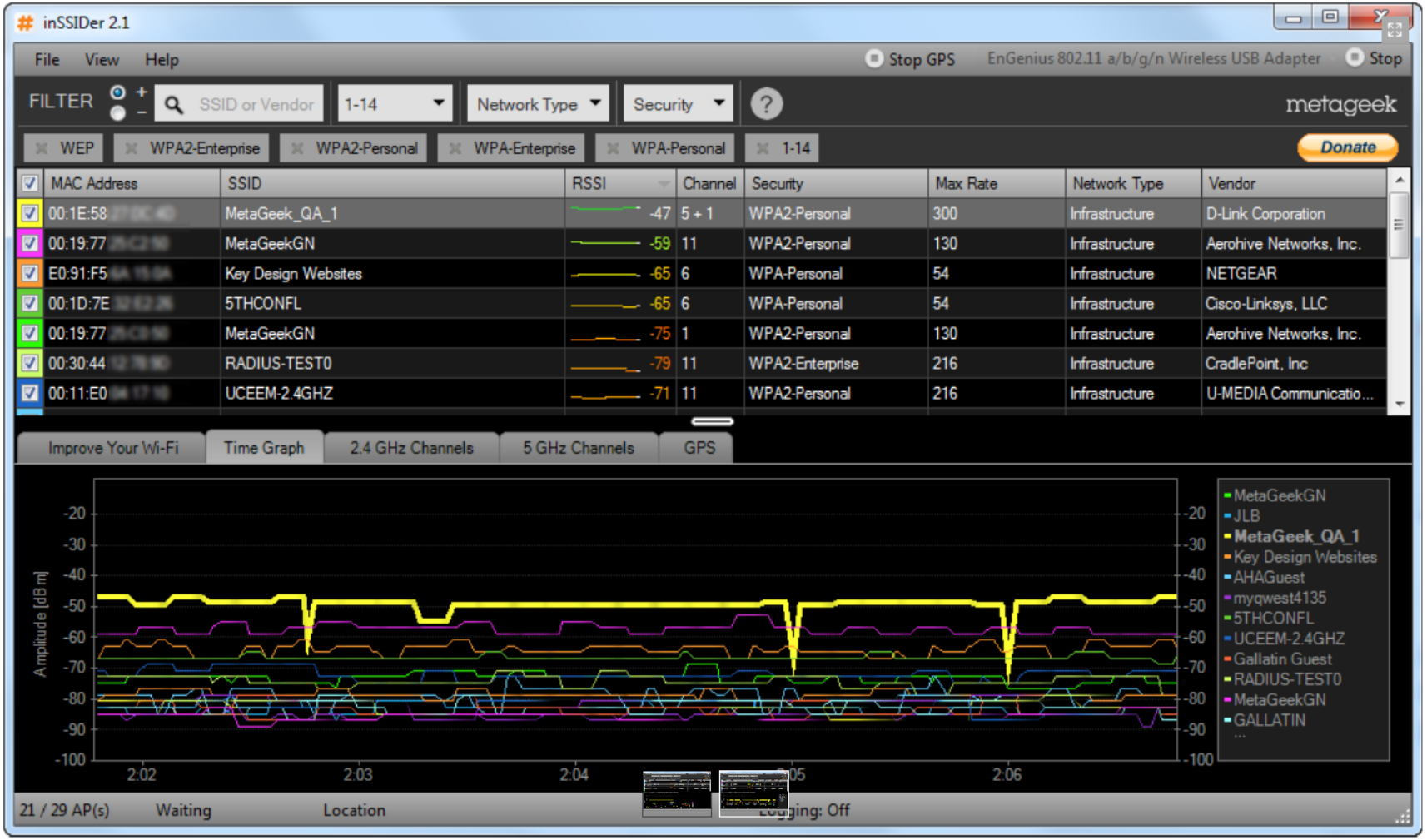
WLAN Layer 1 Analyse

InSSIDer - die kostenlose WLAN Scanning Software für Windows



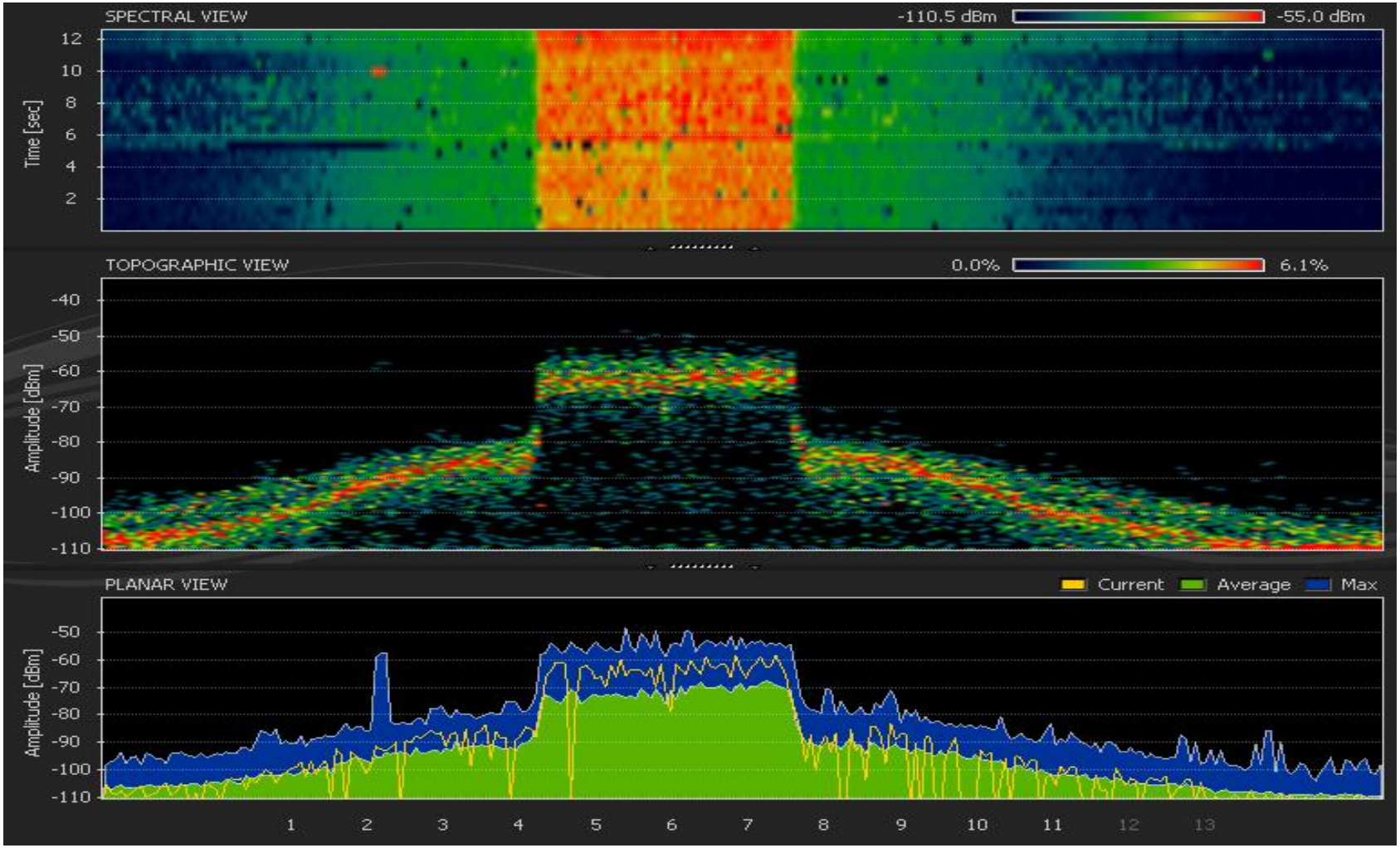
WLAN Layer 1 Analyse

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



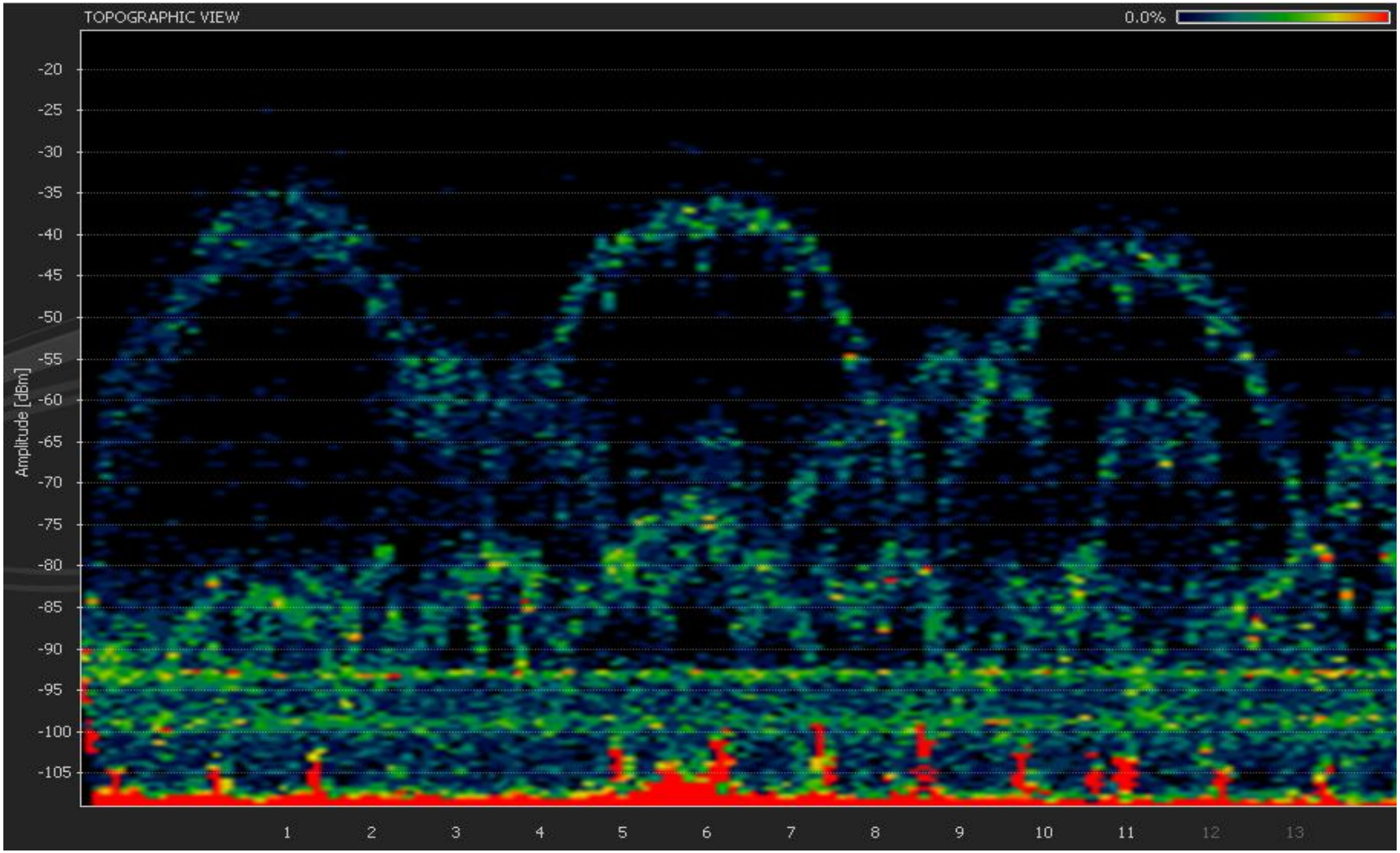
WLAN Layer 1 Analyse

Wi-Spy - der ‚low cost' Spectrum Analyser (www.metageek.net)



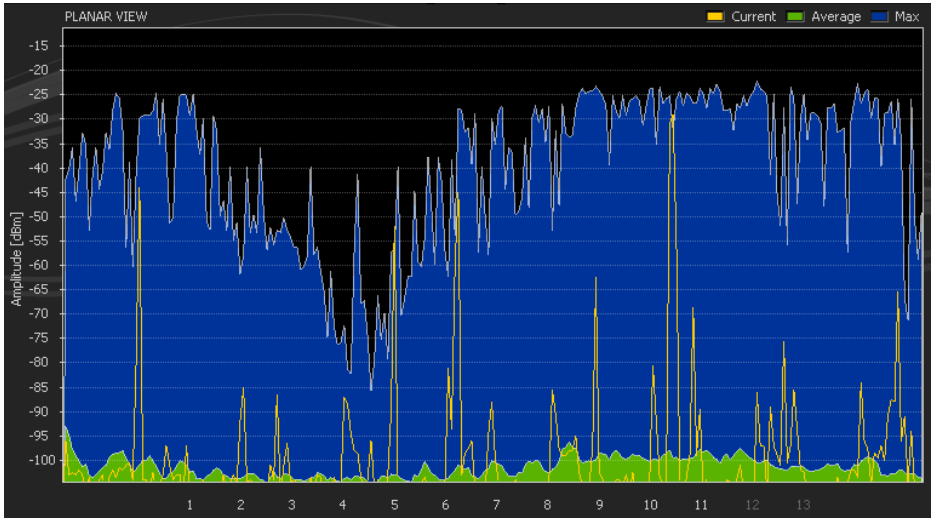
WLAN Layer 1 Analyse

Spektrumanalyse der b/g Kanäle

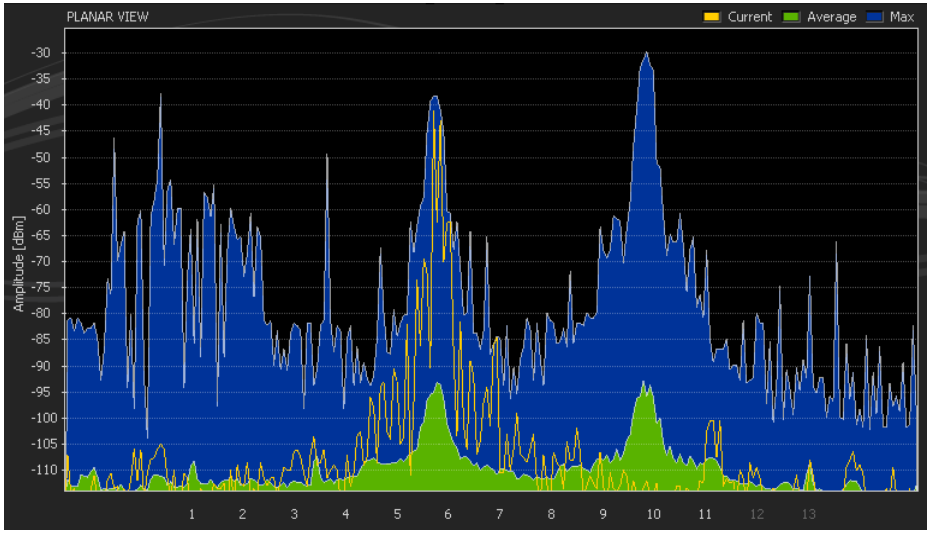


WLAN Layer 1 Analyse

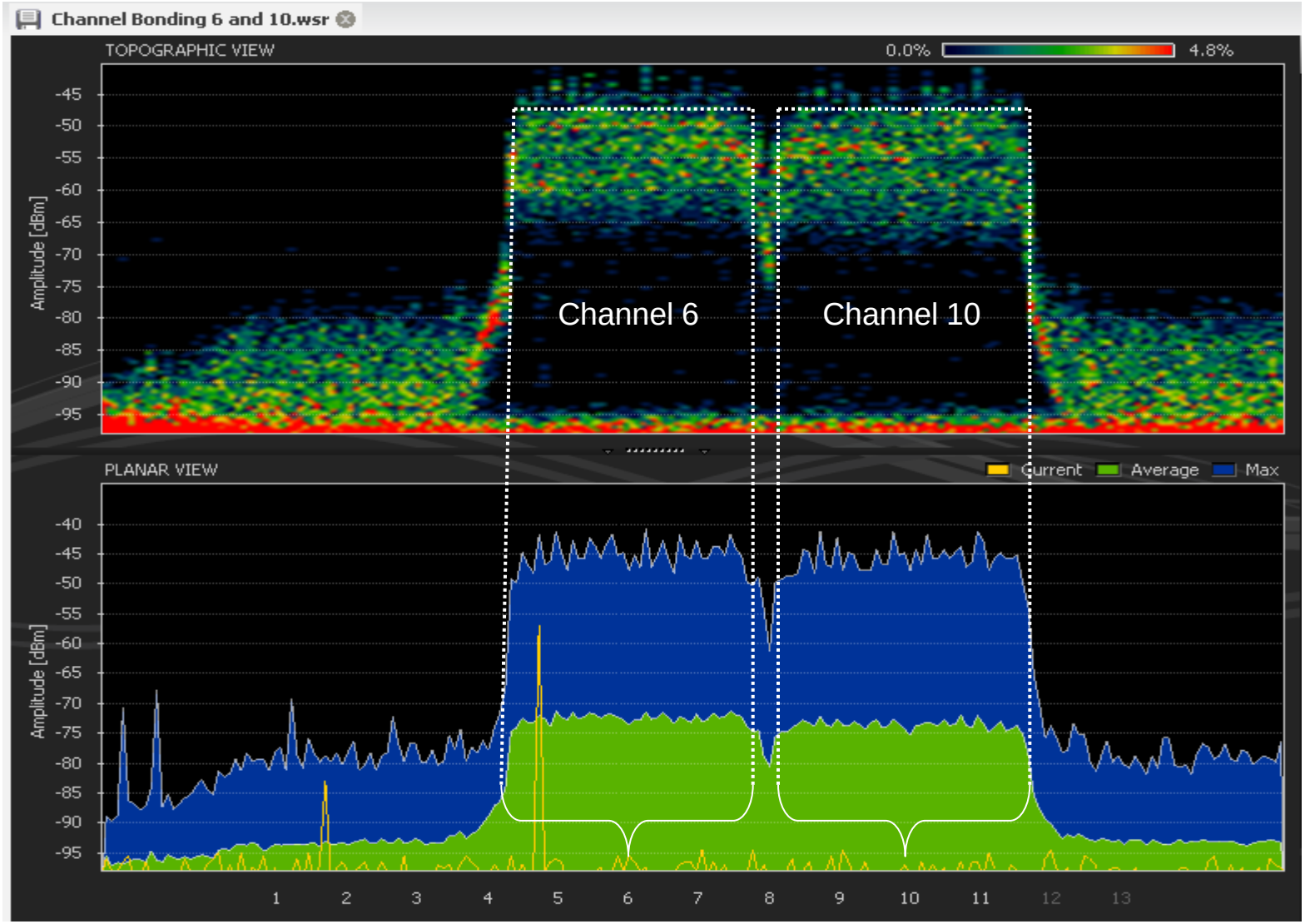
Störsignal eines Mikrowellen-Ofens im 2.4 GHz Band



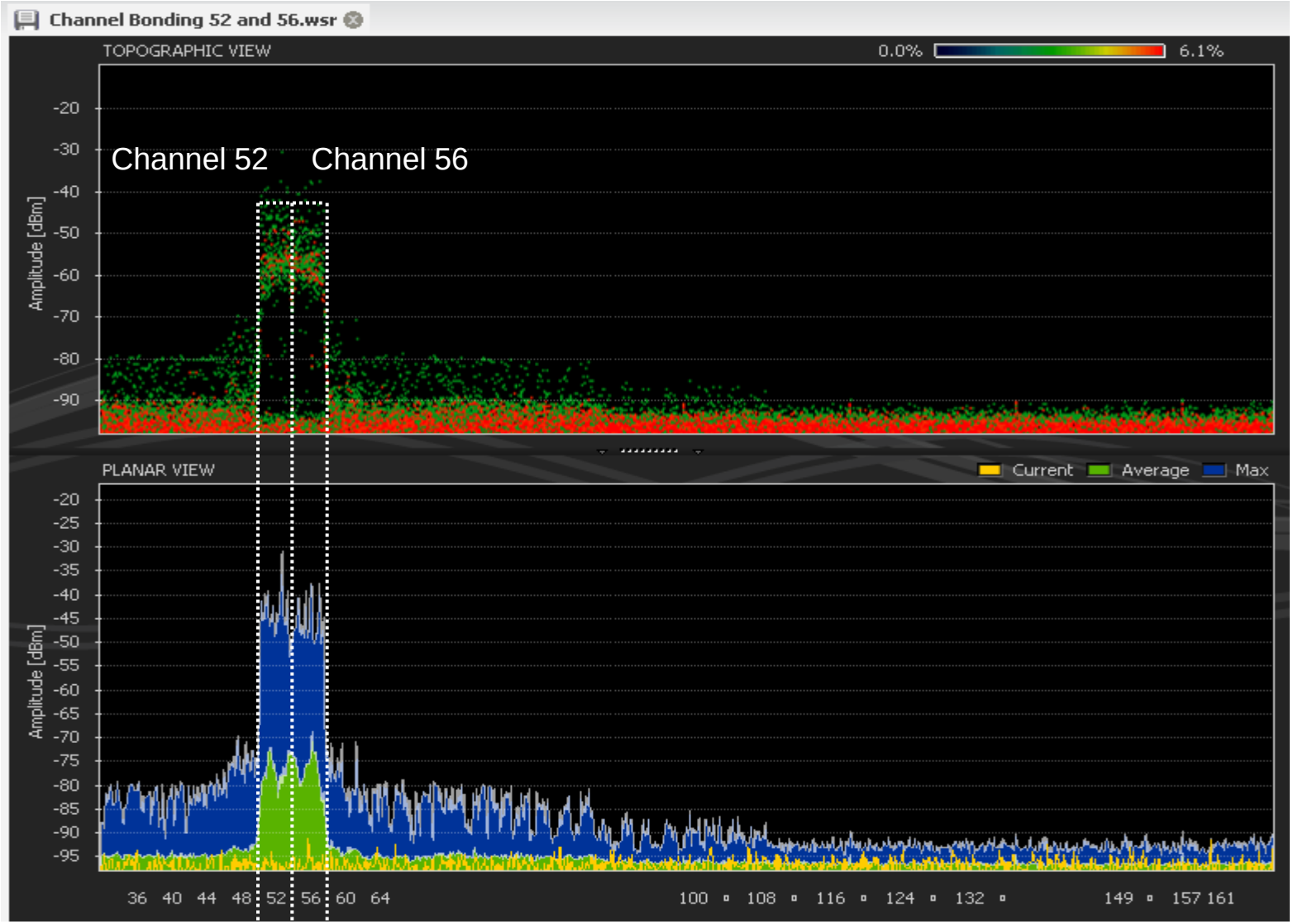
Störsignal eines ‚Frequency Hopping' Telefons (z.B. DECT)



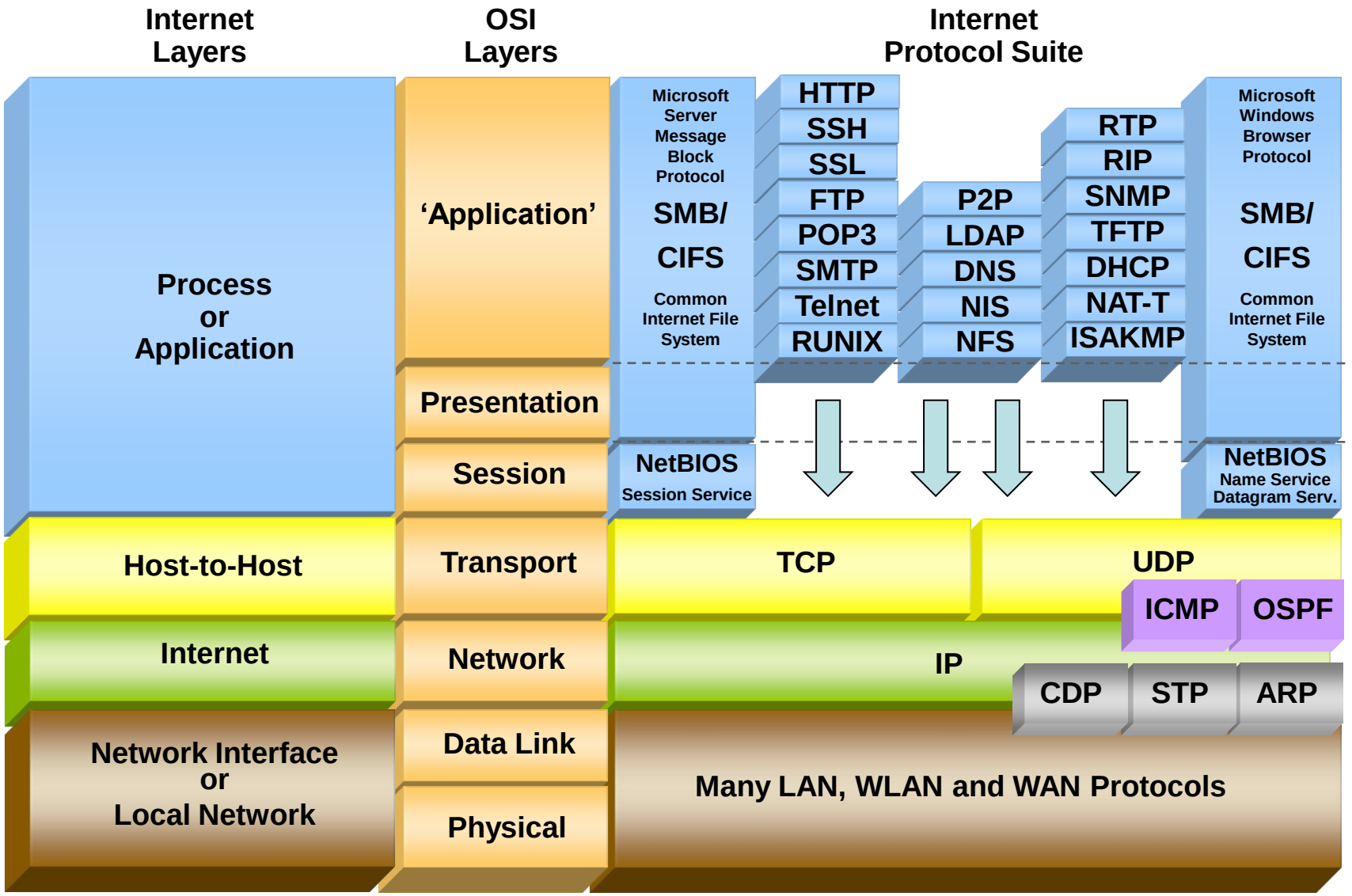
Channel Bonding im 2.4 GHz Band



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 Sende- 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

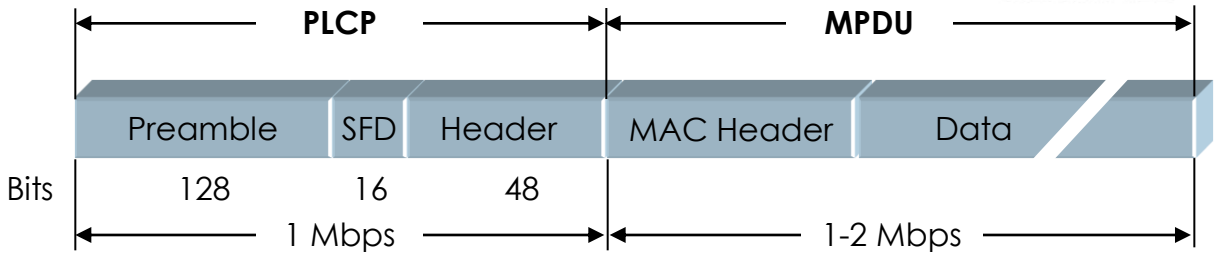
Mbps	Coding	Modulation	Description		
1 2	Barker Barker	DBPSK	**802.11** **DSSS (Clause 15)** with ‚Long Preamble‘		
5.5 11	CCK CCK	DQPSK	**802.11b** **HR/DSSS (Clause 18)** with ‚Short Preamble‘		
6, 9 12, 18 24, 36 48, 54	OFDM OFDM OFDM OFDM	BPSK QPSK 16-QAM 64-QAM	**802.11g** **Extended Rate PHY** **(ERP)**		**802.11a**
7.2-72.2 14.4-144.4	OFDM OFDM	MCS 0-7 MCS 8-15	1 Stream 2 Streams	**802.11n** **High Troughput (HT)** **Extensions**	
			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

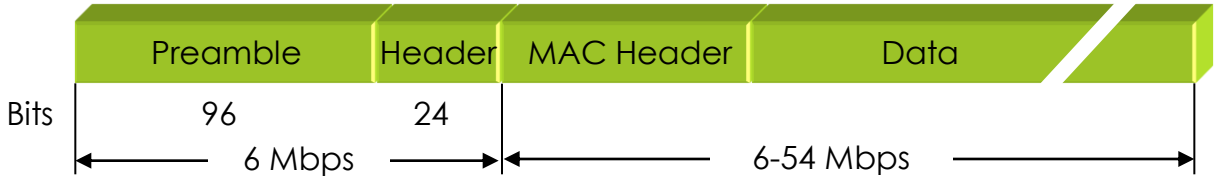
Übersicht Frame Types (2.4 GHz)

802.11 DSSS with
‚Long Preamble'
Barker Code

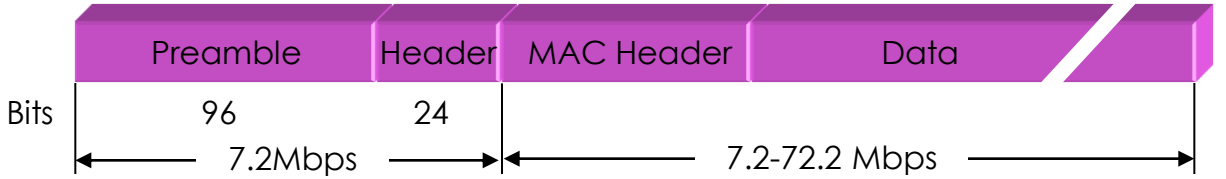


802.11b HR/DSSS with
‚Short Preamble'
Barker / CCK

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

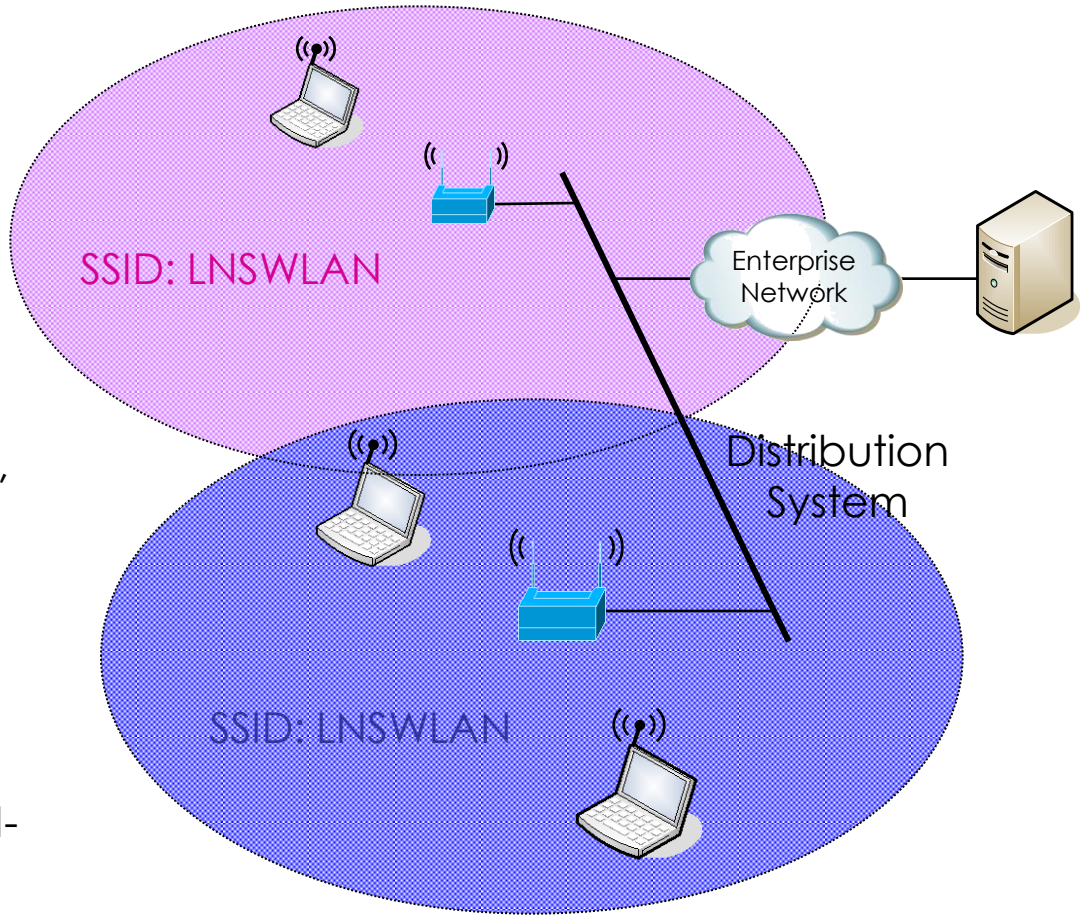
Architektur von WLANs

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:

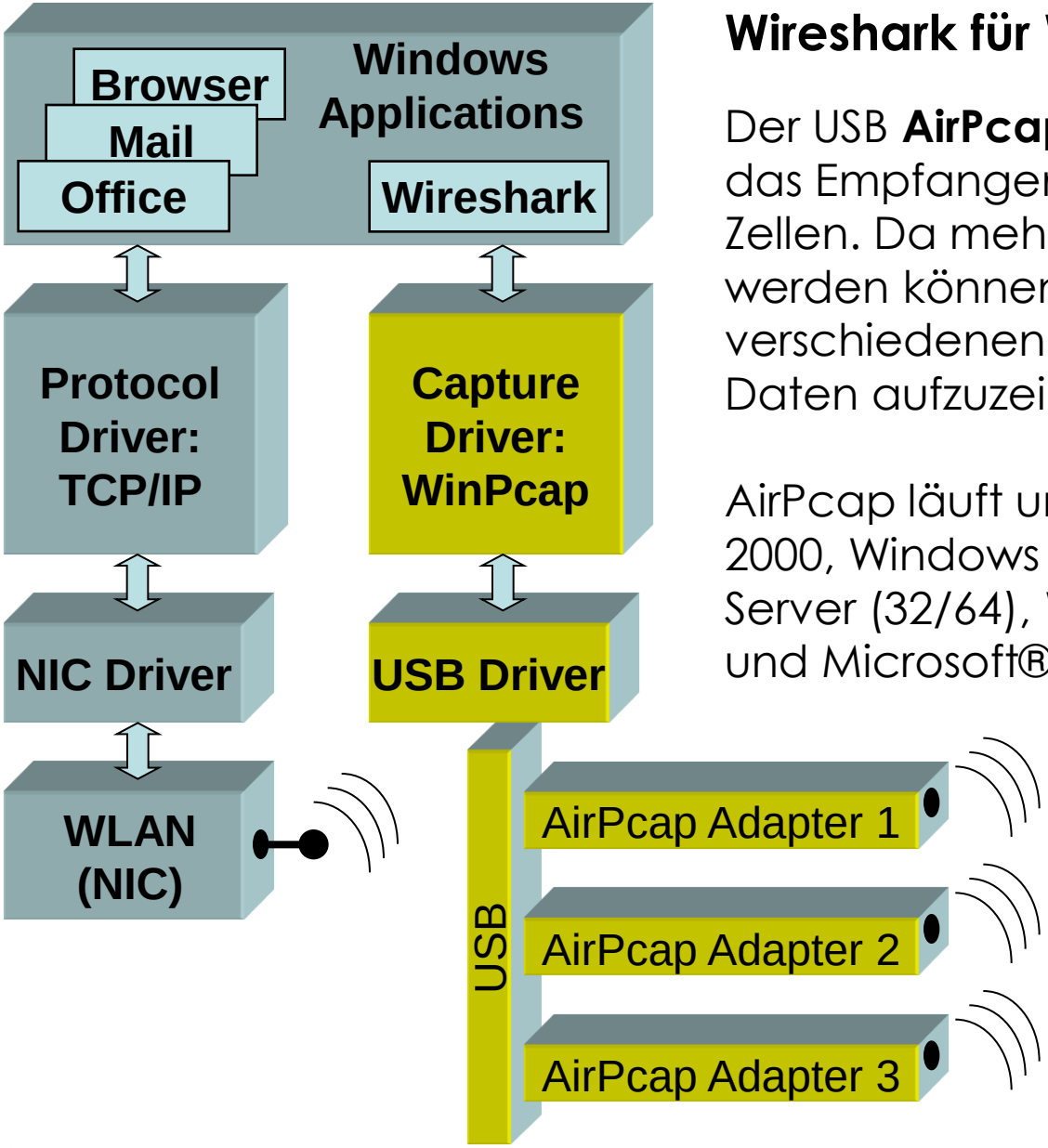
- Beacon
- Probe request and response
- Authentication & Deauthentication
- Association & Disassociation
- Reassociation request and response

Die Control Frames:

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

Die Daten Frames:

- Data
- Null Function



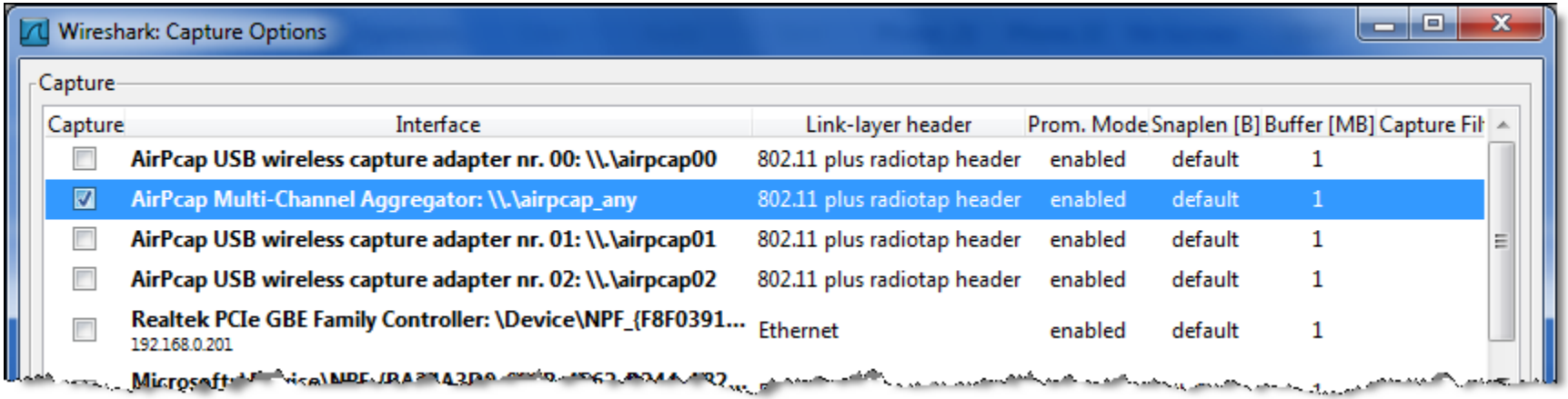
Wireshark für WLAN 802.11b/g

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

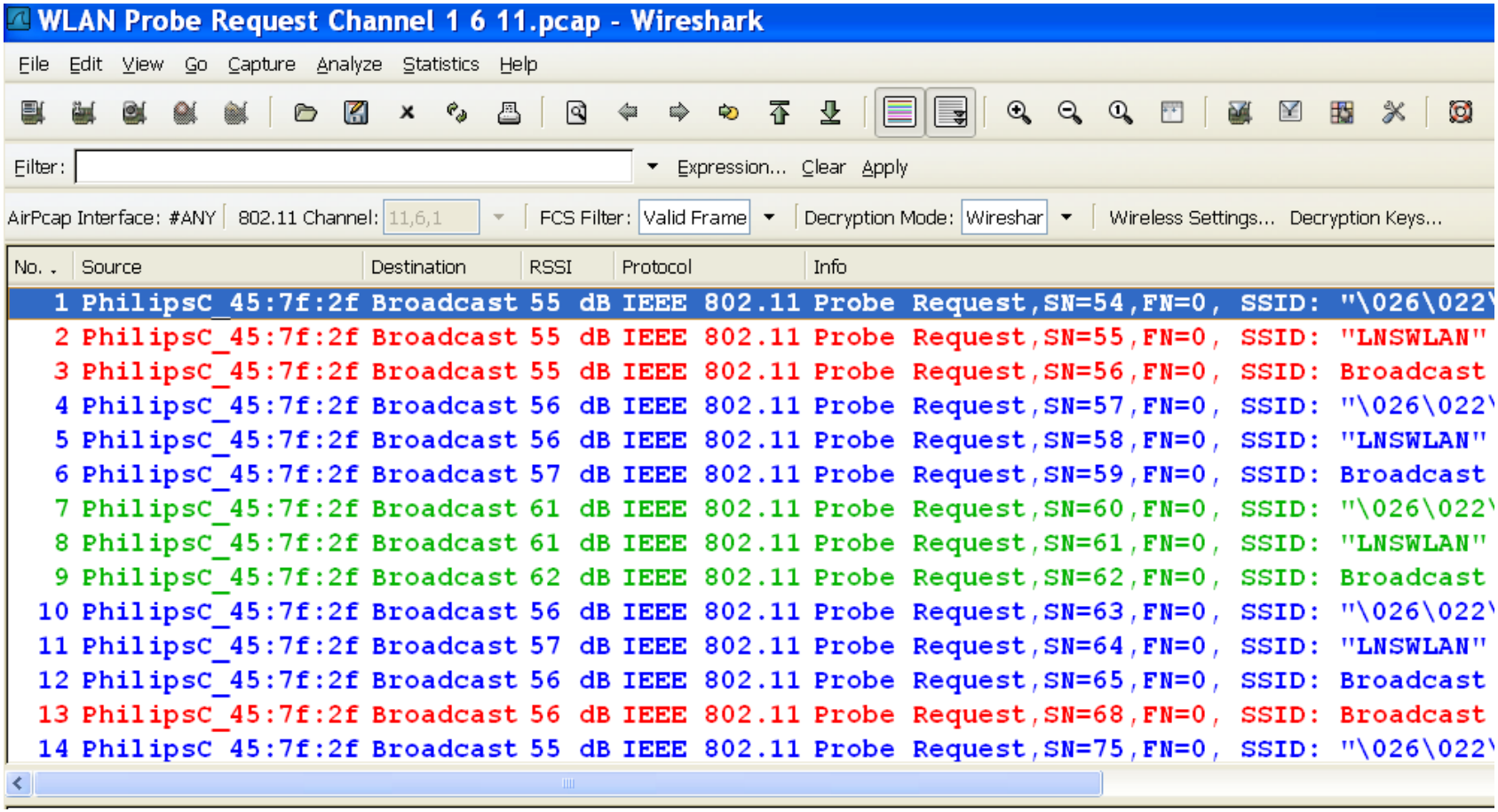
Datenaufzeichnung mit dem Multi-Channel Aggregator



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'



Die wichtigsten WLAN-Prozesse

Die Präsenzmarkierung des Access Points ‚Beacon'

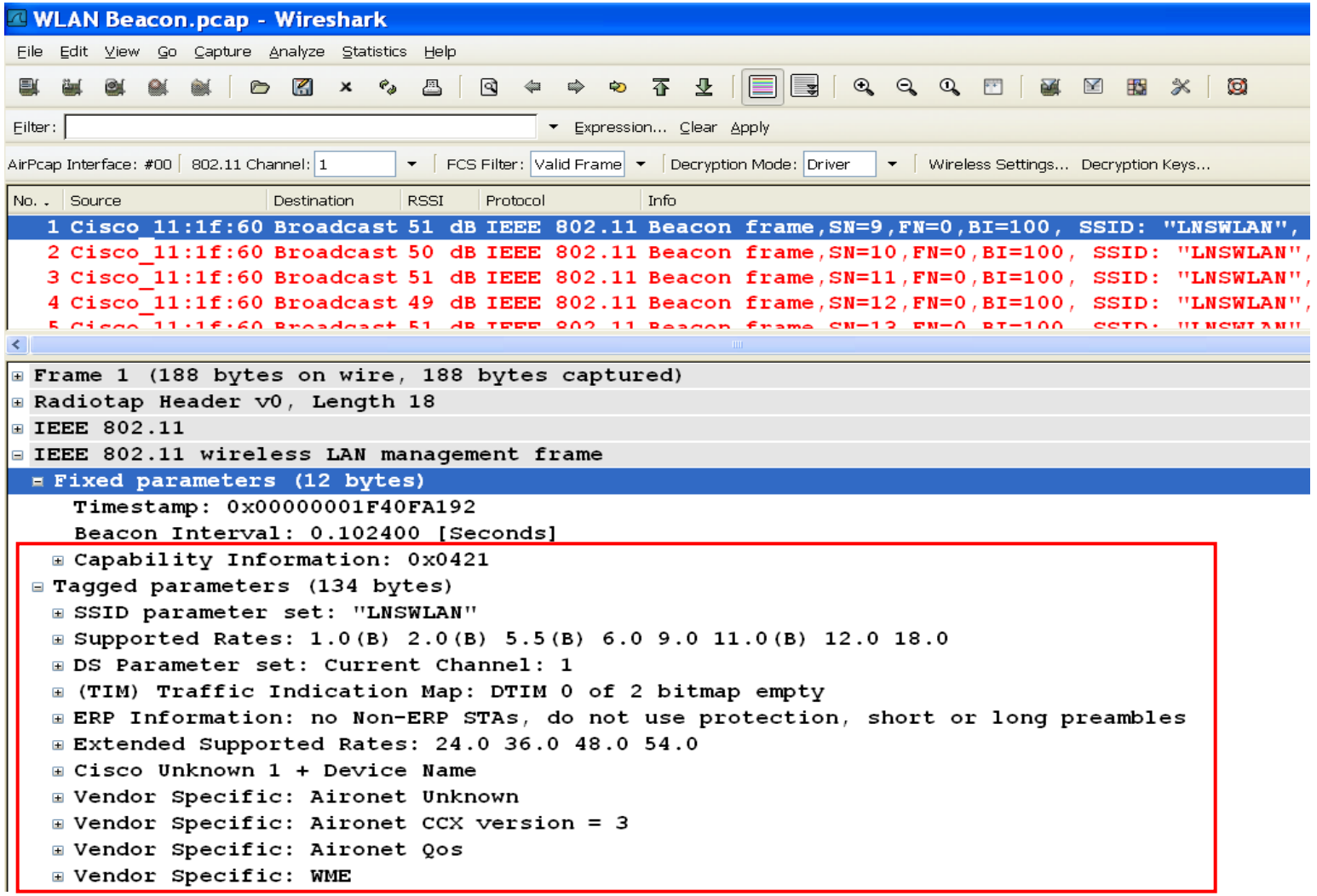
Mit Hilfe des Management Frames **‚Beacon'** (deutsch: Signalfeuer) markiert ein AP seine Präsenz in einer Funkzelle.

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.

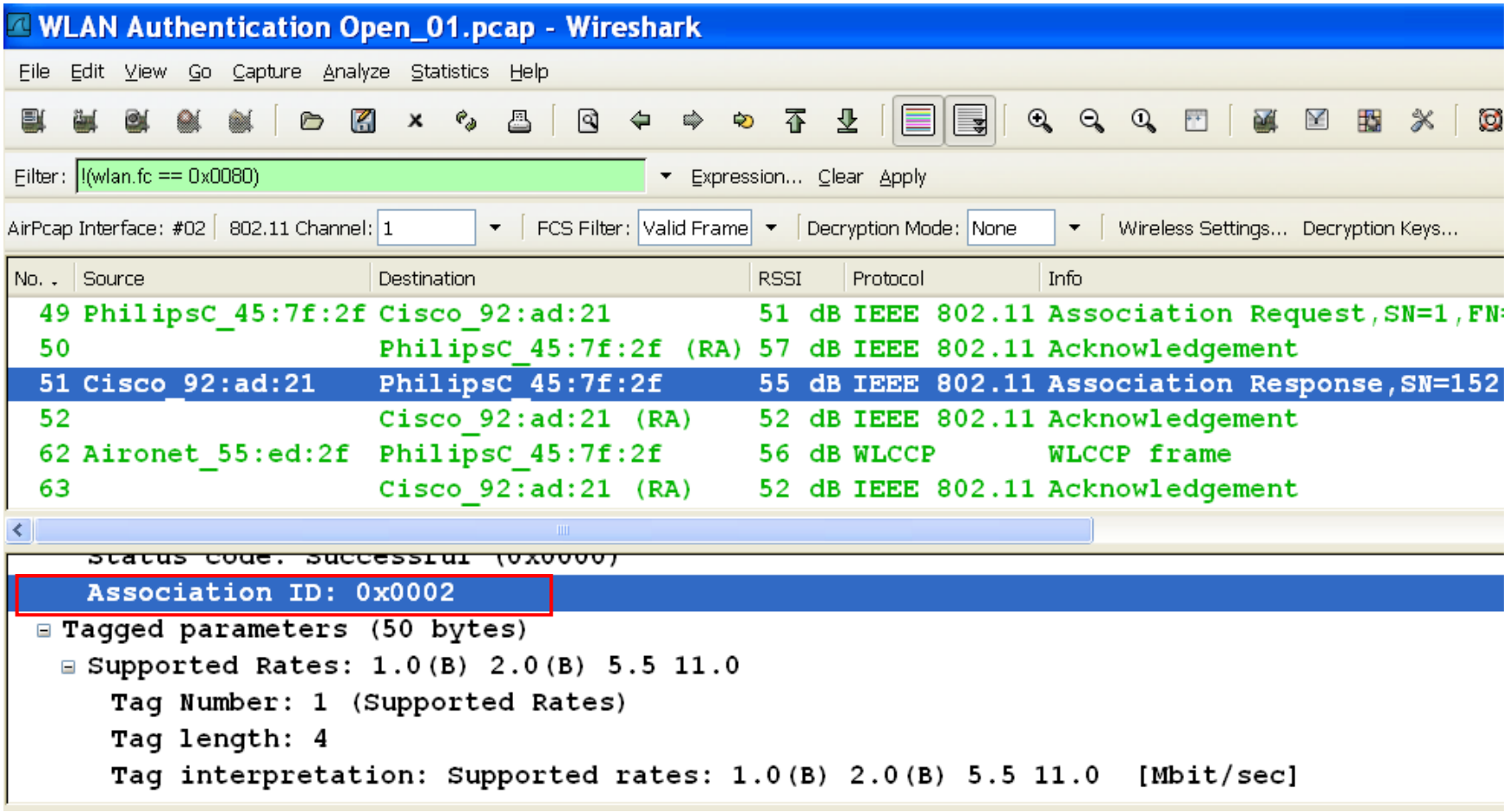
Die wichtigsten WLAN-Prozesse

Die Präsenzmarkierung des Access Points ‚Beacon'



Die wichtigsten WLAN-Prozesse

Verbinden mit einem Access Point



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.

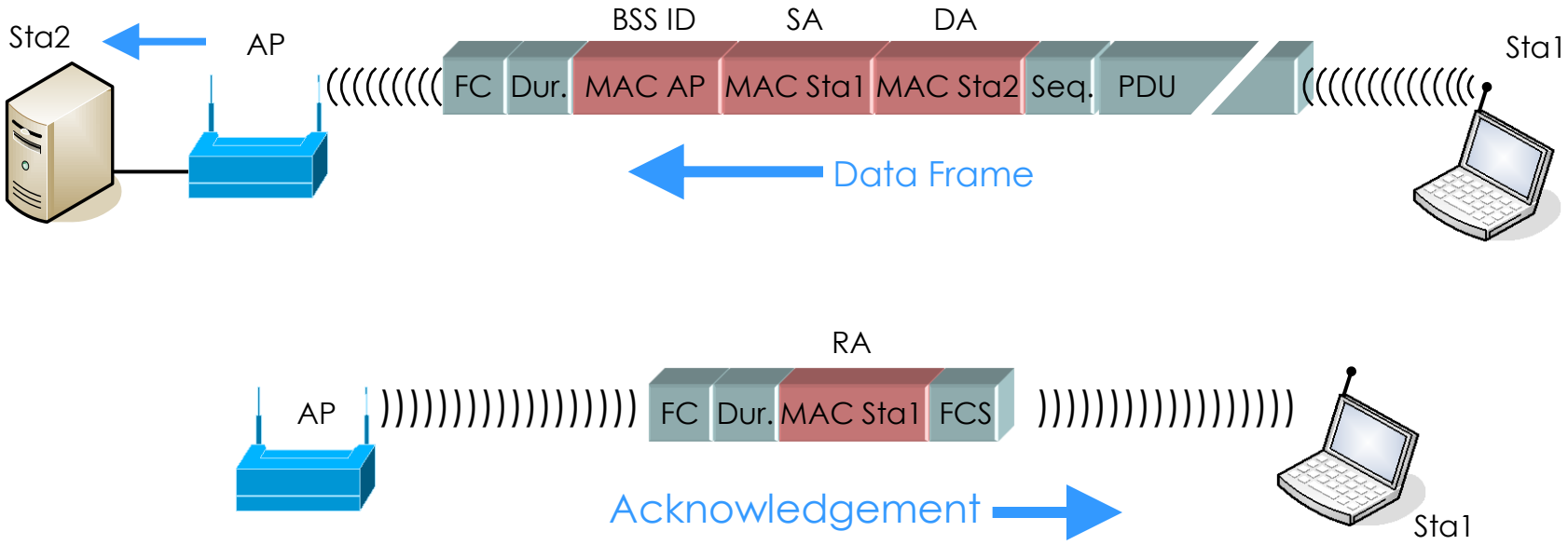
Frames, die bei der Übertragung z.B. durch Störungen beschädigt wurden, werden vom Empfänger nicht bestätigt und lösen damit beim Sender eine erneute Übertragung aus.

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

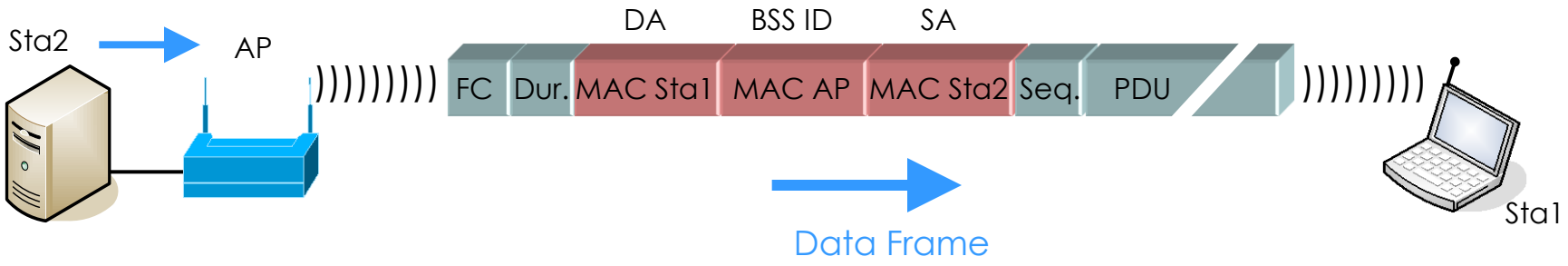
Frame Format für Daten von der mobilen Station Richtung AP:

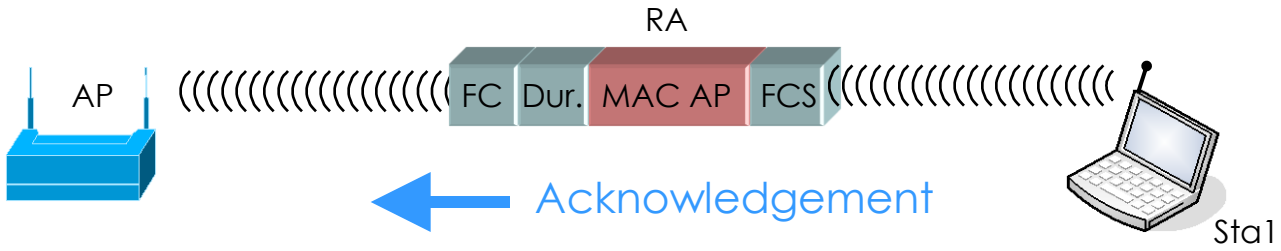


Die wichtigsten WLAN-Prozesse

Datenübertragung vom und zum AP

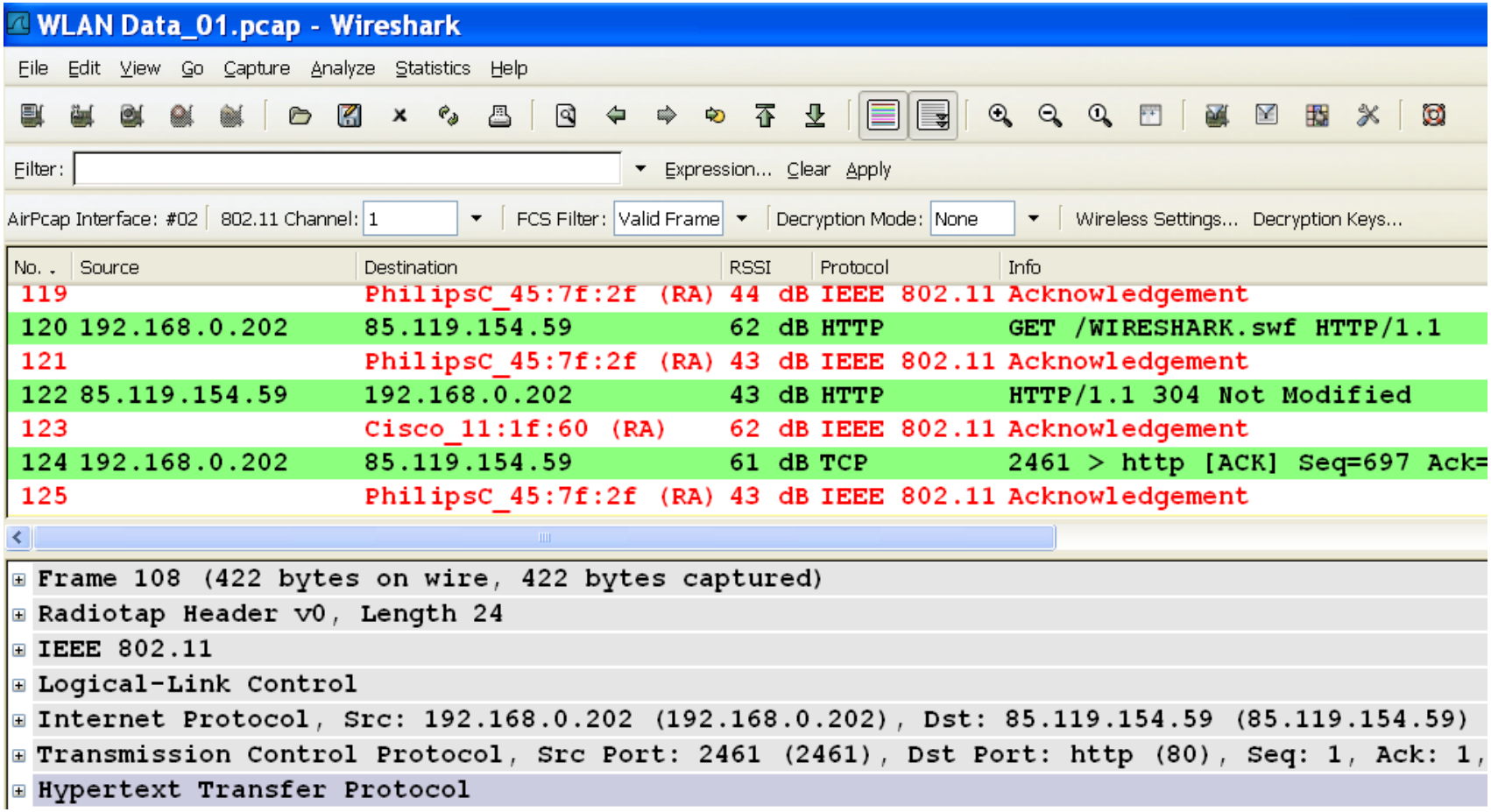
Frame Format für Daten vom AP Richtung mobile Station:





Die wichtigsten WLAN-Prozesse

Datenübertragung vom und zum AP



Die wichtigsten WLAN-Prozesse

Wechsel auf einen anderen AP

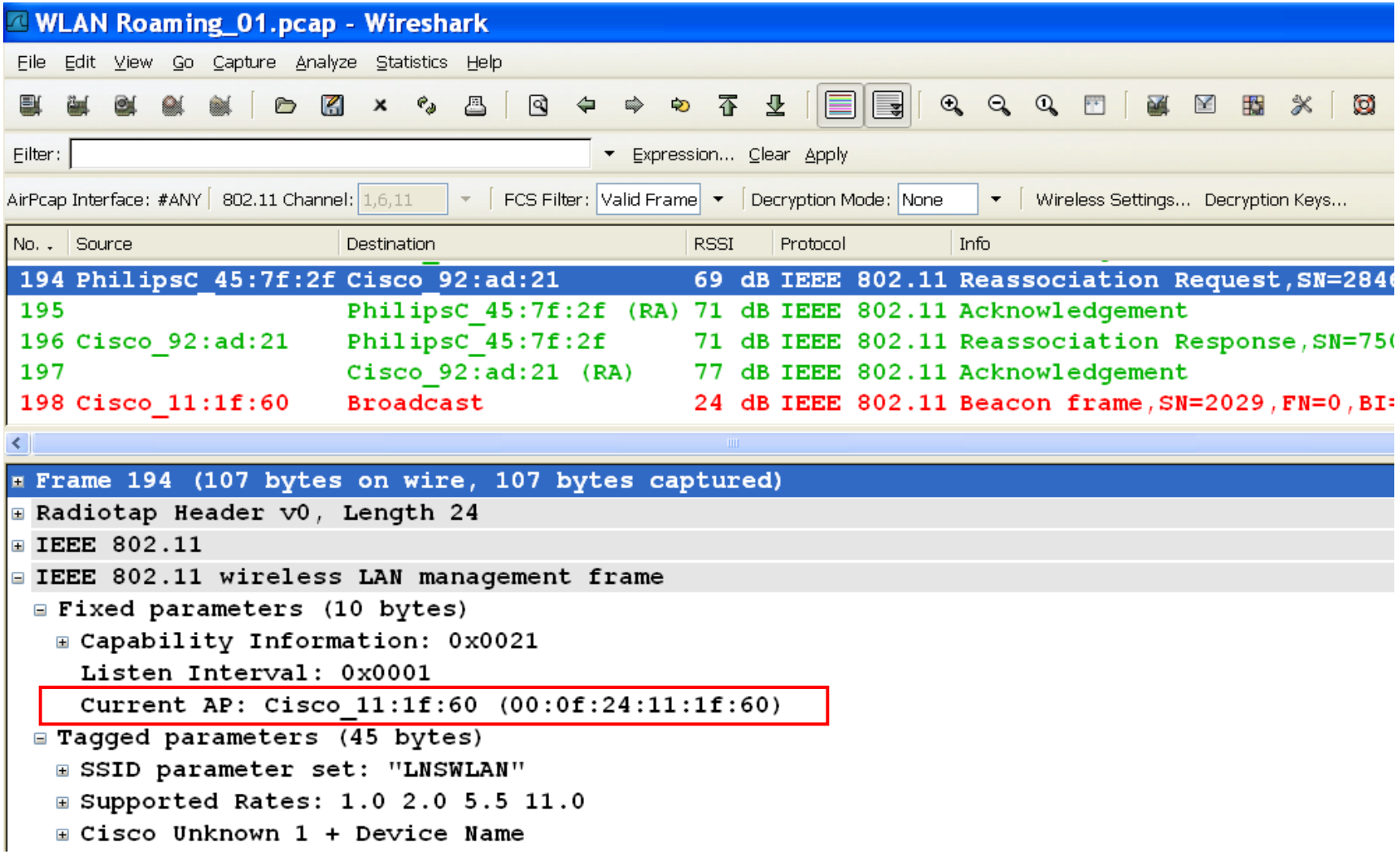
Der Wechsel einer mobilen Station auf einen nächsten AP wird Roaming (to roam: herumwandern) genannt.

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



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:

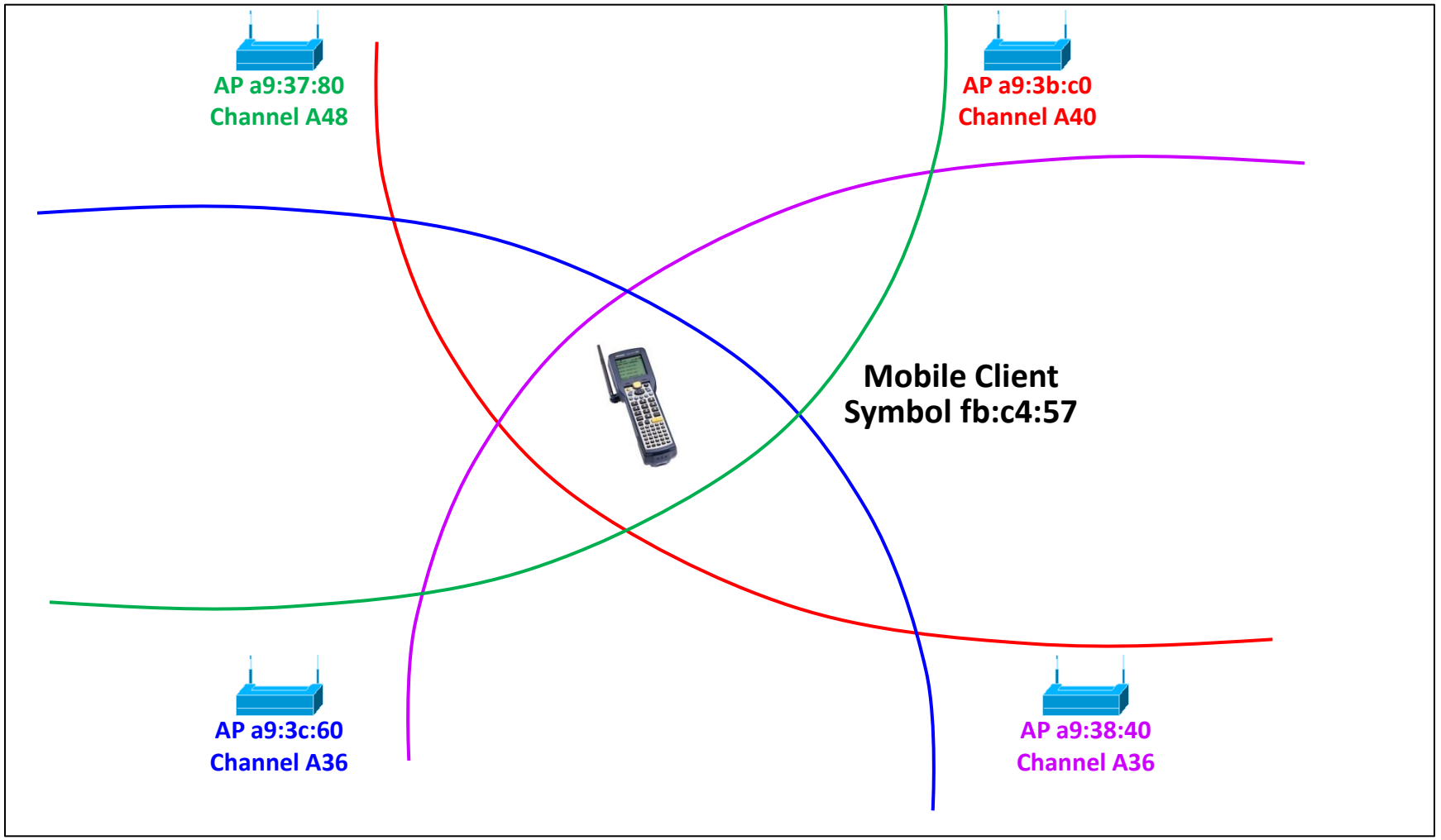
Layer 1

- 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

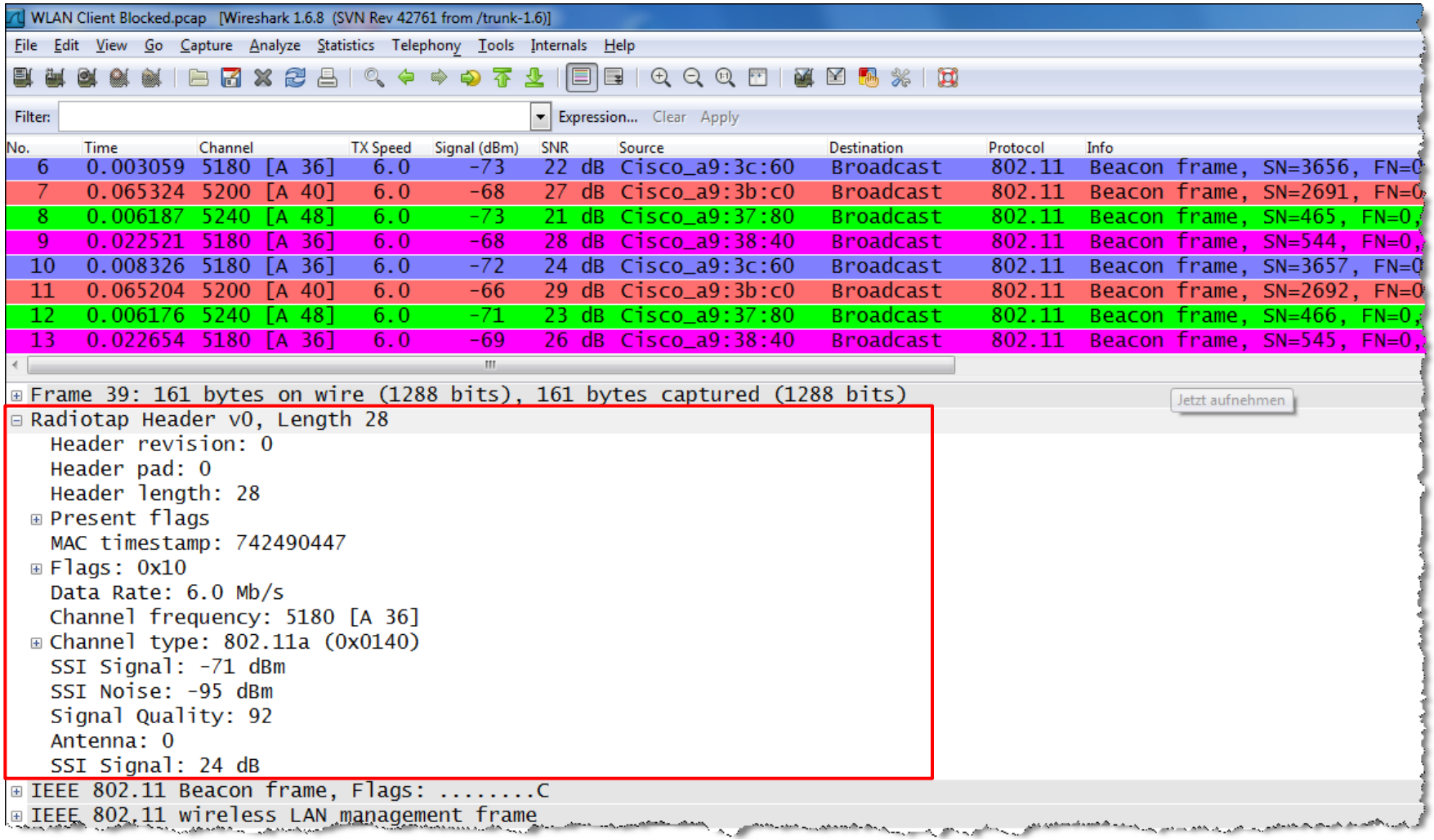
Wie und Was messe ich?

- Verwenden Sie die S/N ratio der Beacons und des Clients um Ihre Position zu definieren
- Die Signal to Noise (S/N) ratio sollte ≥ 20 db sein

- Eine Grafik sagt mehr als tausend Frames!

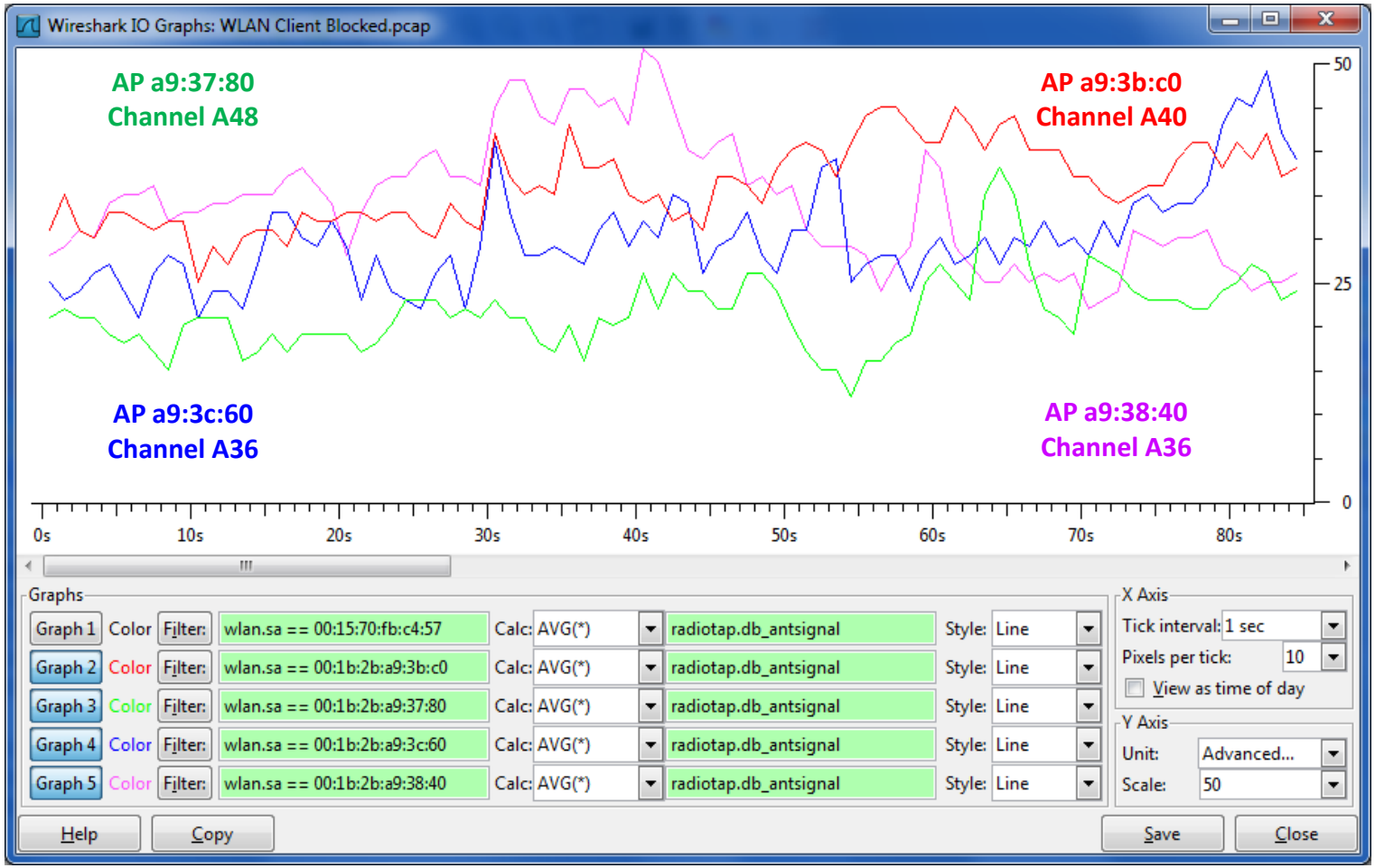
Praxis Problem: Blockierter WLAN Client

Signalstärke der verschiedenen Access Points



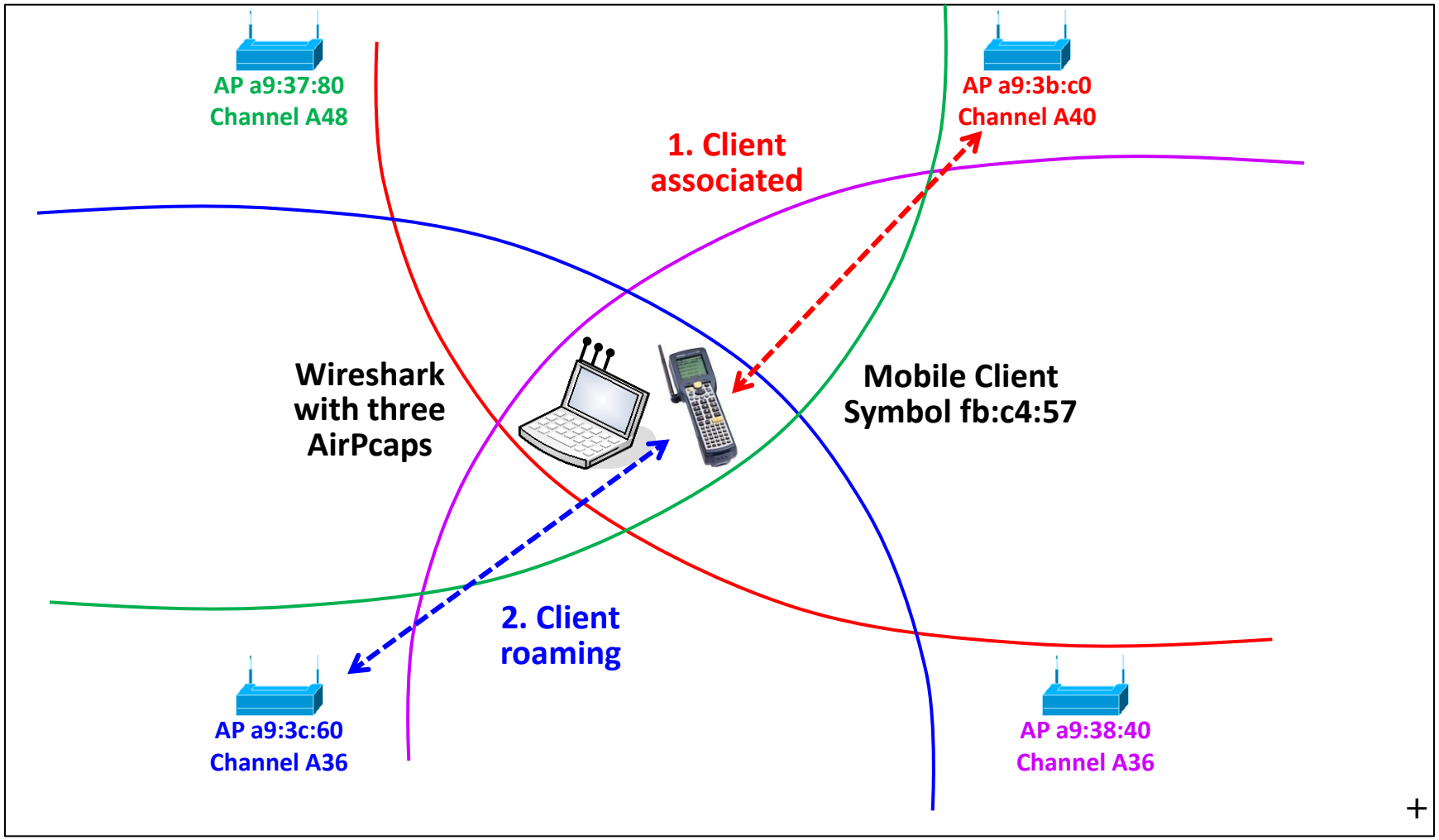
Praxis Problem: Blockierter WLAN Client

Signalstärke der verschiedenen Access Points

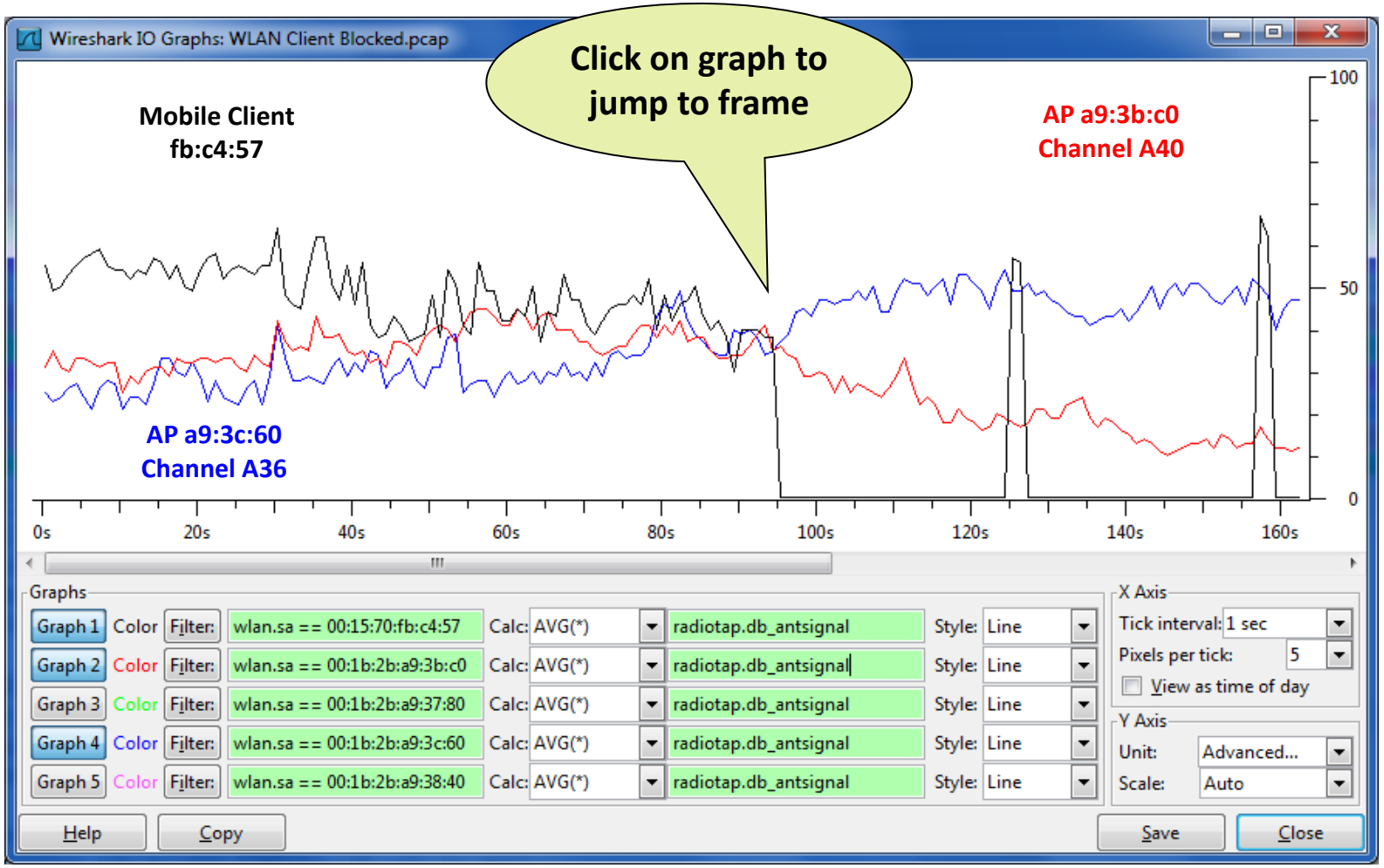


S/N ratio von vier Access Points

Praxis Problem: Blockierter WLAN Client



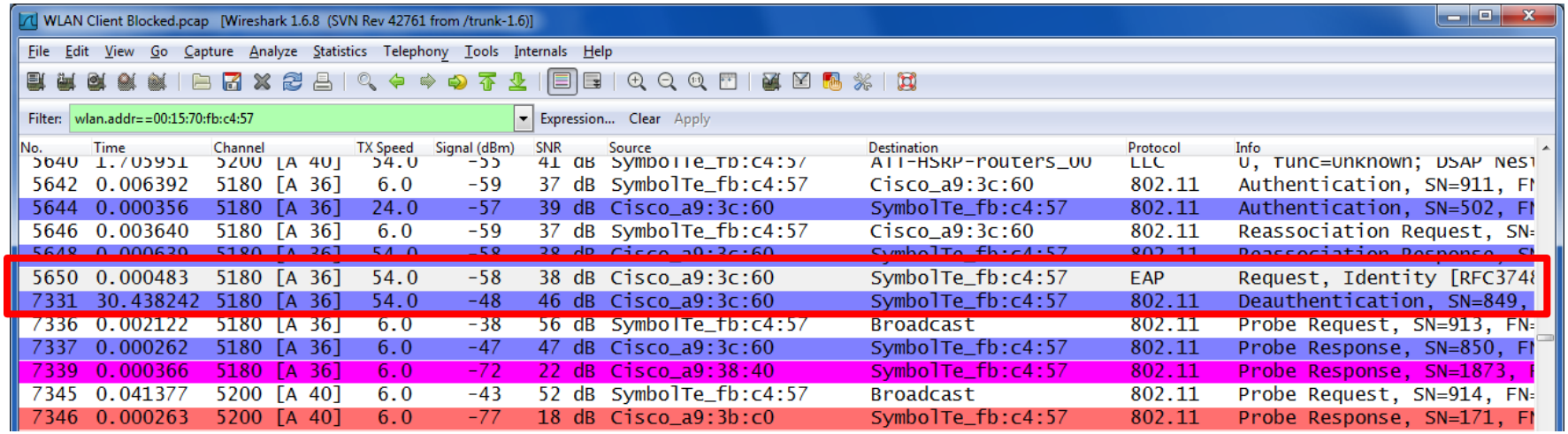
Praxis Problem: Blockierter WLAN Client



S/N ratio von zwei Access Points und des Clients

Praxis Problem: Blockierter WLAN Client

Filter auf MAC Adresse des Clients (Source oder Destination)



- 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 letze 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?

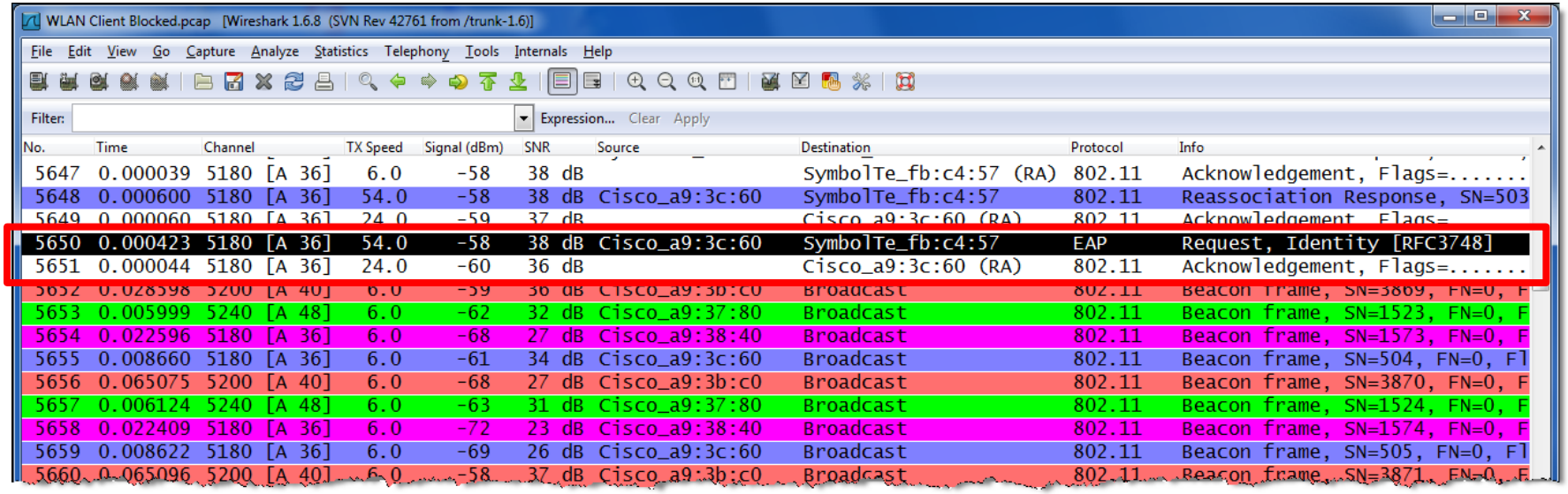
Yes we Can! Werfen wir einen genaueren Blick auf das Trace File.

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



- 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