



Troubleshooting WLANs (Part 1)

Layer 1 & 2 Analysis Using Wireshark, Wi-Spy & Other Tools



Rolf Leutert

Leutert NetServices Switzerland www.netsniffing.ch







Rolf Leutert, El. Ing. HTL Net ervices 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







- Learn what you can see on WLAN layer 1 and layer 2
- Learn which tools can help you finding WLAN problems
- Learn how to use WiSpy to isolate layer 1 issues
- Learn how to use Radiotap and PPI header information
- Learn how to customize Wireshark to show you specific WLAN information



Troubleshooting wireless networks is a demanding task and requires detailed understanding of important functions on layer 1 and 2 !





802.1	L Channel:	Channel Offset:	FCS Filter: All Fram	es v Wireshark	- Wi	reless Sett	ings De	cryption K	evs			
No.	Time	Source		Destination	Signal	Noise	TX Speed	1	Channel			info
11	10.0	0 IntelCor	_79:46:04	Broadcast	-30	-87	1.0	Mbps	2437	[BG 6	5]	Probe Request, SN=365, FN=0,
11	2 0.0	2 Cisco_1f	:4e:20	IntelCor_7	-27	-87	1.0	Mbps	2437	[BG 6	5]	Probe Response, SN=2149, FN=
11	3 0.0	00		Cisco_1f:4	-30	-87	1.0	Mbps	2437	[BG 6	5]	Acknowledgement, Flags=
11	4 0.0	7 Cisco_1f	:4e:20	Broadcast	-27	-87	1.0	Mbps	2437	[BG 6	5]	Beacon frame, SN=1597, FN=0,
11	5 0.1	1 IntelCor	_79:46:04	Cisco_1f:4	-27	-87	6.0	Mbps	2437	[BG 6	5]	Authentication, SN=15, FN=0,
11	5 0.0	00		IntelCor_7	-27	-87	6.0	Mbps	2437	[BG 6	5]	Acknowledgement, Flags=
11	7 0.0	0 Cisco_1f	:4e:20	IntelCor_7	-27	-87	1.0	Mbps	2437	[BG 6	5]	Authentication, SN=1598, FN=
11	8 0.0	00		Cisco_1f:4	-31	-87	1.0	Mbps	2437	[BG 6	5]	Acknowledgement, Flags=
11	9 0.0	2 Cisco_1f	:4e:20	Broadcast	-26	-87	1.0	Mbps	2437	[BG 6	5]	Beacon frame, SN=1599, FN=0,
12	0.00	0 IntelCor	_79:46:04	Cisco_1f:4	-27	-87	6.0	Mbps	2437	[BG 6	5]	Association Request, SN=16,
12	10.0	00		IntelCor_7	-27	-87	6.0	Mbps	2437	[BG 6	5]	Acknowledgement, Flags=
12	2 0.0	2 Cisco_1f	:4e:20	IntelCor_7	-27	-87	1.0	Mbps	2437	[BG 6	5] .	Association Response, SN=160
12	3 0.0	00		Cisco_1f:4	-45	-87	1.0	Mbps	2437	[BG 6	5] .	Acknowledgement, Flags=
12	4 0.0	2 Cisco_1f	:4e:20	IntelCor_7	-26	-87	1.0	Mbps	2437	[BG 6	5]	Key (Message 1 of 4)
12	5 0.0	1 Cisco_1f	:4e:20	IntelCor_7	-26	-87	1.0	Mbps	2437	[BG 6	5]	Key (Message 1 of 4)
12	5 0.0	00		Cisco_1f:4	-45	-87	1.0	Mbps	2437	[BG 6	5] .	Acknowledgement, Flags=

Layer 1 - Physical Access

FH, DSSS, OFDM, coding, modulation, bands, channels, frequencies, noise, signal strength, interferences etc.

Clients: WiFi and non-WiFi devices like surveillance cameras, remote control, microwave, health gadgets etc.

Tools: Spectrum Analyser (e.g. Wi-Spy)

 Layer 2 - Data Link Control
 WiFi Standards 802.11 a/b/g/n/ac framing, management, access control, security, encryption etc.
 Clients: WiFi compatible devices only
 Tools: Wireshark, AirPcap, WaveXpert





- WLAN WIFI devices are working in the 2.4 GHz ISM* and 5 GHz UNII** bands
- But both bands are free for any use, WiFi as well as non-WiFi devices
- Especially the 2.4 GHz band is often crowded with non-WiFi devices
- *i* The only limitation is max. radiated power according to country regulations
- Non-WiFi clients use any kind of modulation and may interfere with WiFi
- Layer 2 tools like Wireshark can not detect non-WiFi devices
- Spectrum analyzers scan the bands and show shape and strength of all signals

Wi-Spy[®] DBx spectrum scanner and Chanalizer[®] software displays and records all layer 1 signals in both 2.4 GHz and 5 GHz bands.

www.metageek.com



* ISM Industrial, Scientific and Medical **UNII Unlicensed National Information Infrastructure



WiFi Device Signature in 2.4 GHz Band





Non-WiFi Device Signatures in 2.4 GHz Band



Home trainers in a fitness center



Microwave oven



Remote control of model airplanes



Wireless guitar

WiFi 802.11ac with four bonded channels in 5MHz Band







LIVE DEMONSTRATION WI-SPY & CHANALYZER



10

Large logistic enterprise, depending on WLAN for day-to-day operations
Two container cranes to load/unload trains require WLAN connections



11

User complain about log-in timeouts and disconnections during operations
 Crane #2 is hardly usable due to unreliable WLAN connection
 Tech-Support has already changed WiFi channels and added additional AP



12

Starting with layer 2 analysis near crane #2 in channels 1, 6, and 11

Wireshark shows up to 70% of frames with bad FCS or the Retry Flag set

🖌 ping von mitte zu pos 2.pcapng		
<u>File Edit View Go Capture Analyze Statistics Telephony</u> <u>T</u> ools Internals <u>H</u> elp		
● ● ◢ ■ ◢ ⊨ ≞ ೫ ₴ ٩ 수 ㅎ ₽ ₮ ⊻ 🗐 🗐 ٩ २ ९	% 🛛 🖸	
Filter: (wlan.fcs_bad == 1) (wlan.fc.retry == 1) Expression Clear Apply 	Save Beacon only Malformed Beacon excl. Bad FCS	
802.11 Channel: 💌 Channel Offset: 💌 FCS Filter: All Frames 💌 Wireshark 💌 Wireless Settings Decryption Keys		
No. Time Source Destination Signal Nois	🖉 🖉 Wireshark IO Graphs: ping von mitte zu pos 2.pcapng	
504 0.004 Intercor_settetas d9:a0:41:02.09.e0 = 55 =		- 1000
504 0.000 Intelcor 7e:84:b0 Cisco 25:10:e2 -9 -1		
504 0.000 IntelCor 7e:84:b0 Cisco 25:10:e2 -9 -	- Packets total	100
504 0.000 IntelCor_7e:84:b0 Cisco_25:10:e2 -9 -	- Packets with Retry Bit set	2 - 2
504 0.000 IntelCor_7e:84:b0 Cisco_25:10:e2 -8 -	- Packets with FCS error	-
504 0.011 IntelCor_7e:84:b0 Cisco_25:10:e2 -76 -	<u>2</u>	
504 0.000 IntelCor_7e:84:b0 Cisco_25:10:e2 -71 -	31	
504 0.000 b3:09:70:1a:02:82 (TA) 27:64:c5:af:77:ec -57 -		- 500
504 0.000 IntelCor_7e:84:b0 Cisco_25:10:e2 -9 -		- I
504 0.000 IntelCor 7e:84:b0 Cisco 25:10:e2 -9 -		
Transmitter address: Inte/Cor_5e:1e:a5 (e0:9d:31:5e:1e		-
Source address: IntelCor_5e:1e:a5 (e0:9d:31:5e:1e:a5)		5 - 5
Destination address: d9:ab:41:b2:d9:e6 (d9:ab:41:b2:d9		
Fragment number: 0	Association	
Sequence number: 0		
Frame check sequence: 0x0a821f53 [incorrect, should be	34.0s 35.0s 36.0s 37.0s 38.0s 39	1.0s 40.0s
[GOOd: Faise]		
[Bad: True]	Graphs	T X Axis
	Granh 1 Color Eiltern	Tick interval: 0.1 sec
0000 00 00 20 00 69 00 00 00 02 00 14 00 c6 ce e8 52		Divels per tick
0020 c8 19 a2 00 00 23 ab 25 10 e2 e0 9d 31 5e 1e a5	Graph 2 Color Filter: wlan.fc.retry == 1 Style: Line 🔽 Smooth	
0030 d9 ab 41 b2 d9 e6 00 00 00 00 53 1f 82 0a	Graph 3 Color Filter; Style: Line 🔻 🕅 Smooth	view as time of day
		Y Axis
😑 💅 Frame Check Sequence (FCS) (wlan.fcs), 4 bytes 🛛 🛛 Packets: 214875 - Displayed: 15	u Graph 4 Color Filter: wlan.fcs_bad = = 1 Style: Line ✓ Smooth	Unit: Packets/Tick
	Graph 5 Color Filter: Style: Line ▼ 🖉 Smooth	Scale: Auto 💌
		Smooth: No filter
	Help	Save Close
	Tich Fobl	2010



Continuing with layer 1 analysis near crane #2 in 2.4 GHz band
Strong interference with non-WiFi signals on all three channels detected



✓ Signal source is outside of customers campus' → Swiss radio authority informed
✓ If this transmitting power is within legal limits → Change to 5 GHz band required



Swiss radio authority (BAKOM) scanned the 2.4 GHz band with their own tool
They detected a strongly interfering signal caused by a railway induction loop



Traffic monitoring induction loop

#sf18eu • Imperial Riding School Renaissance Vienna • Oct 29 - Nov 2

14





- WiFi scanners show you available access points with lots of information like SSID, channel no, channel width, max. rate, security mode etc.
- Some tools are able to perform throughput simulations
- Mo adapter required, WiFi scanners are using internal WLAN cards









Acrylic WiFi scanner



Ekahau HeatMapper



(((())) NetStumbler

Wifi Analyzer (Android)

WifilnfoView

inSSIDer

www.acrylicwifi.com

www.ekahau.com

www.metageek.com

www.netstumbler.com

play.google.com

www.nirsoft.net

WifiScanner

WifiScanner

wifiscanner.sourceforge.net



Wifi Scanner <u>www.apple.com/osx/apps/app-store</u>



Remark: Apple IOS (iPhone/iPad) has locked direct access to the WiFi interface for stability and other unknown reasons. Jailbreak is required to install and run WiFi Scanner apps on these devices.





All these tools have the following limitations in common:

Scanning on layer 2, therefore only WiFi devices can be detected.

Non-802.11 sources like surveillance cameras etc. are invisible.

WiFi scanners read data from Beacon and other management frames



WiFi Scanners will not provide any information if Beacon frames interfere with non 802.11 devices on layer 1!



Capturing 802.11 traffic with **built-in NICs** is very platform/network adapter/driver/libpcap dependent, and might not be possible at all !

- Windows is very limited here:
 - → Captures only broadcasts & your own traffic No management/control frames, fake Ethernet
- Some OSs (i.e. MAC OS) support Monitor Mode
 → Captures all traffic and provides Radio Infos
- Can I simultaneously capture multiple channels?
 - \rightarrow Yes, with external hardware
- Can I decrypt 802.11 data packets?

→ Yes, if shared keys are used, if the key is available and the key negotiation process is captured

More information:

wiki.wireshark.org/CaptureSetup/WLAN

#sf18eu • Imperial Riding School Renaissance Vienna • Oct 29 - Nov 2

Ch1

Ch6

Ch11

https://wiki.wireshark.org/CaptureSetup/WLAN

Windows:

- Npcap is an update of WinPcap using NDIS 6 and has many added features <u>https://nmap.org/npcap/#download</u>
- Instruction link: <u>https://wiki.wireshark.org/CaptureSetup/WLAN#Starting_from</u> <u>Windows_Vista:_Npcap</u>

Linux:

- Instruction link: <u>https://wiki.wireshark.org/CaptureSetup/WLAN#Linux</u>
- Existing Linux Wireless drivers: <u>https://wireless.wiki.kernel.org/en/users/drivers</u>

MAC OS:

- Instruction link: <u>https://wiki.wireshark.org/CaptureSetup/WLAN#Mac_OS_X</u>
- Free Airtool for Wireshark captures from Mac's built-in Wi-Fi adapter: <u>https://www.adriangranados.com/apps/airtool</u>



MMAP, ORG	Installation Options Please review the following options before installing Npcap 0.92
Automatically start	the Npcap driver at boot time
Support loopback to	raffic ("Npcap Loopback Adapter" will be created)
Use DLT_NULL as t	he loopback interface' link layer protocol instead of DLT_EN10MB
Restrict Npcap driv	er's access to Administrators only
Support raw 802.1	1 traffic (and monitor mode) for wireless adapters
Support 802. 1Q VL	AN tag when capturing and sending data
Install Npcap in Wir	Pcap API-compatible Mode
Nullsoft Install System v2.51	< Back Install Cancel



Most of newer Access Points offer remote controlled packet capture features

- Some allow capturing during operation, other must be put into monitor mode
- Even cloud controlled APs (i.e. Meraki) support capturing on wire- or wireless side

Packet capture - Meraki	Da × +	
https://n140.meraki.co	om/Live-Demo-Univer/n/k7W8Ndmc/manage/dashboard/tcpdump 🛛 🛡 📿 🗌 🔍	bst time \rightarrow 2 e $rac{1}{2}$
	Explore dashboard: Wireless LAN Tour Security Appliances Te	Dur Access Switches Tour
cisco Merak	Network: Live Demo - University Wireless 🔻	leutert@wireshark.ch my profile sign out Q Search dashboard
Network-wide	Packet capture	
Wireless	Access point: Armington Hall D, lounge × Capture Type: wireless •	Sample filter expressions host 10.1.27.253 packets to and from ip address 10.1.27.952 host 10.1.27.253 and port Offnen von WLAN_Armington_Hall.pcap
Help	Duration (secs): 60	packets to and from ip addr 53 (DNS) icmp[icmptype] != icmp-e
	Filter expression: File name: WLAN_Armington_Hall	all ICMP packets that are n packets): ether host 11:22:33:44:55: packets to and from etherne See more examples.
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	Start capture	The capture will stop after 6 have been captured. Packet capture logs
	Source: Cisco	Meraki OK Abbrechen

Capturing with some built-in WLAN NICs may display faked Ethernet frames only
Only Data frames and no Radio or WLAN header will be seen

🚄 *Dra	ahtlo	snetzw	erkver	bindung	[Wiresha	rk 1.10.0r	c2 (S	SVN Rev 49	)526 from	/trunk-1	10)]								
<u>F</u> ile <u>I</u>	<u>E</u> dit	<u>V</u> iew	<u>G</u> o	<u>C</u> apture	<u>A</u> nalyze	<u>S</u> tatist	ics	Telephony	<u>T</u> ools	<u>I</u> nternal	s <u>H</u> elp								
0 0	) (		Ø.	E 🔓	* 2	)   Q		۵	7 ⊻		: (÷		0, 11	]   🎽 🗹	褐 💥   🕽	0			
Filte	er:									•	Express	ion	Clear	Apply	Save	Layer 2 only	ТСР		UDP
No.		Time			Source				Destina	tion				Protocol L	ength	Info			
1		0.	000	0000	192	.168	.0	.217	192	.168	.0.2	55		NBNS	92	Name	quer	-у	NB
2		0.	258	3232	192	.168	.0.	.201	192	.168	.0.2	55		NBNS	92	Name	quer	•у	NB 👌
3		0.	069	9601	192	.168	.0.	. 217	239	.255	.255	.250	0	SSDP	175	M-SE/	ARCH	*	HTT
4		0.	237	7969	192	.168	.0.	.201	239	.255	.255	.250	0	SSDP	175	M-SE/	ARCH	*	HTT
5		0.	199	9400	192	.168	.0.	. 217	224	.0.0	.252			LLMNR	66	Stan	dard	qu	ery
6		0.	107	7298	192	.168	.0.	.201	224	.0.0	.252			LLMNR	66	Stan	dard	qu	ery
7		0.	001	L103	192	.168	.0.	.217	224	.0.0	.252			LLMNR	66	Stan	dard	qu	ery
8		0.	203	3786	192	.168	.0.	.217	192	.168	.0.2	55		NBNS	92	Name	quer	·y	NB
9		0.	102	2408	192	.168	.0.	.201	224	.0.0	.252			LLMNR	66	Stan	dard	qu	ery
10	)	0.	002	2094	192	.168	.0.	.201	192	.168	.0.2	55		NBNS	92	Name	quer	·y	NB
11		0.	659	9450	192	.168	.0.	.217	192	.168	.0.2	55		NBNS	92	Name	quer	'y	NB 🕴
<																			
⊕ Fr	am	ne 1	: 9	)2 bv	tes	on w	ir	e (73	6 bi	ts).	92	bvte	es d	capture	ed (736	bits)			
	he	rne	+ 1	т s	rct	Tnte	$\frac{1}{1}$	$r^{73}$	.68.	54 (	00.2	1:6	h:7	3:68:54	4) Dst	: Broa	deast	- (	ff
⊡ Tn	nte	rne	+ •	Proto	col	Vers	io	n 4	Src	192	168	0	217	(192 1	168 0 2	17) D	st.	192	16
	er		tac	iram	Prot		.01	Src P	ort.	net	hios	-ns	(1:	37) 04	st Port	· neth	ios-r	152	(13
			N	ma E	orvi	0001	, ,	SIC P	or c.	neu	0103	-113	(1.	<i>, 0</i>	SUFUL	. netb	103-1	13	(1)
± ne	LD	TOS	Ne	fille 2	ervi	ce			م	man for	يمسيدهن		· · · · · · · · · · · · · · · · · · ·			and a second second			. And

Revision	Pad	Length	Present Flags	Data Fields	Data Fields
		F	Radiotap or PPI He	eader	

- The Radiotap or the PPI (Per Packet Information) are so called Link-layer pseudo-headers because they are not transmitted with the frame.
- They are added by the driver during reception and contain additional radio information about the incoming frame.
- Z Provides Receive Signal Strength, bit rate, channel number and other fields
- **Z** These fields can be used as columns in Wireshark and support troubleshooting
- Some drivers (i.e. MAC OS) offer a selection of different Link-layer headers, however, the Radiotap header is the most widely supported type.

More detailed information:Radiotap:<a href="https://www.radiotap.org/">https://www.radiotap.org/</a>List of Pseudo-headers:<a href="https://www.adriangranados.com/blog/link-layer-header-types">https://www.adriangranados.com/blog/link-layer-header-types</a>

00 00 00 00 01 00 0c 00 7c 15 40 01 00 00 ed a6

80.00 00 00 EFOEL FENER AF EF ZANGEN AD DO

0010

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
In Paper a usaget mer in Schryz Angeler Schryz Schr
1 0.000 CiscoInc 11:1f:60 Broadcast 802.11 188 Beacon frame, SN=9, FN=0, Flags= BI=100, SSID=LNSWL
2 0 025 CiscoInc 11:1f:60 Broadcast 802 11 188 Beacon frame SN-10 EN-0 Elags- BT-100 SSID-1NSW
$2 0.023$ Ciscolne_11.11.00 Broadcast 002.11 100 Beacon frame, SN=10, TN=0, Tidgs=, BI=100, SSID=LNSW
3 0.102 CISCOINC_II:IT:00 Broducast 802.11 188 Beacon Trame, SN=II, FN=0, FIAgS=, BI=100, SSID=LNSW
> Frame 1: 188 bytes on wire (1504 bits), 188 bytes captured (1504 bits)
Radiotap Header v0, Length 18
Radiotap Pseudo-Header added by WLAN receiver
TEEE 802 11 Beacon frame Elags:
TEEE 802.11 beacon frame, frags
PIELE 802.11 WIRELESS LAN MANAgement frame
WLAN Beacon 11ac.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter <ctrl-></ctrl-> Expression + No beacons Only beacons Probe Reg or
No. Time Source Destination Protocol Length Info
1 0.000000 CiscoInc_1f:4e:2e Broadcast 802.11 341 Beacon frame, SN=1802, FN=0, Flags=C, BI=102, SSID=LNS-LAF
2 0.104375 CiscoInc_1f:4e:2e Broadcast 802.11 341 Beacon frame, SN=1803, FN=0, Flags=C, BI=102, SSID=LNS-LAF
3 0.104487 CiscoInc_1f:4e:2e Broadcast 802.11 341 Beacon frame, SN=1804, FN=0, Flags=C, BI=102, SSID=LNS-LAE
3 0.104487 CiscoInc_1f:4e:2e Broadcast 802.11 341 Beacon frame, SN=1804, FN=0, Flags=C, BI=102, SSID=LNS-LAE
3 0.104487 CiscoInc_1f:4e:2e Broadcast 802.11 341 Beacon frame, SN=1804, FN=0, Flags=C, BI=102, SSID=LNS-LAE
3 0.104487 CiscoInc_1f:4e:2e Broadcast 802.11 341 Beacon frame, SN=1804, FN=0, Flags=C, BI=102, SSID=LNS-LAE
<ul> <li>3 0.104487 CiscoInc_1f:4e:2e Broadcast 802.11 341 Beacon frame, SN=1804, FN=0, Flags=C, BI=102, SSID=LNS-LAB</li> <li>&gt; Frame 1: 341 bytes on wire (2728 bits), 341 bytes captured (2728 bits) on interface 0</li> <li>&gt; PPI version 0, 32 bytes</li> <li>&gt; 802.11 radio information</li> </ul>
<pre>3 0.104487 CiscoInc_1f:4e:2e Broadcast 802.11 341 Beacon frame, SN=1804, FN=0, Flags=C, BI=102, SSID=LNS-LAE </pre> 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
<pre>3 0.104487 CiscoInc_1f:4e:2e Broadcast 802.11 341 Beacon frame, SN=1804, FN=0, Flags=C, BI=102, SSID=LNS-LAR </pre>
<pre>3 0.104487 CiscoInc_1f:4e:2e Broadcast 802.11 341 Beacon frame, SN=1804, FN=0, Flags=C, BI=102, SSID=LNS-LAR </pre> 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  IEEE 802.11 wireless LAN management frame
<pre>3 0.104487 CiscoInc_1f:4e:2e Broadcast 802.11 341 Beacon frame, SN=1804, FN=0, Flags=C, BI=102, SSID=LNS-LAR &gt; Frame 1: 341 bytes on wire (2728 bits), 341 bytes captured (2728 bits) on interface 0 &gt; PPI version 0, 32 bytes &gt; 802.11 radio information &gt; IEEE 802.11 Beacon frame, Flags:C &gt; IEEE 802.11 wireless LAN management frame</pre>

#sf18eu • Imperial Riding School Renaissance Vienna • Oct 29 - Nov 2

. @ . . . .





- Create a Wireshark profile for WLAN settings
- Add columns with radio information values from the PPI header

Add specific Quick Filter buttons with management & control frames

🚄 WLAN Be	acon 11ac.pcapng												ام ام ۸	0:	l. Eilten buitten	- 0
File Edit	View Go Capture	e Analyze Statistics Telephony W	ireless Tools	Help									Add	QUIC	K Fliter button	IS
🛋 🔳 🙇 🤇	ی 🖪 🔚 🕞	। ९ 🗢 🗢 🕾 🕢 📃 📃 Ө	00													4
Apply a disp	olay filter <ctrl-></ctrl->												Expression	+ Nob	eacons Only beacons Probe Req o	or Resp Retries
Interface	~	Channel	7	~	FCS Filter	~					_				AirPcap Control Par	nel 802.11 Prefi
No.	Time	Source	Destination		Protocol	Length	Signal	Noise	TX Speed	Channel	Info					
1	0.00000	CiscoInc_1f:4e:2e	Broadc	ast	802.11	341	-19	-90	6.0	100	Beacon	frame,	SN=1802,	FN=0,	Flags=	C, BI=1
2	0.104375	CiscoInc_1f:4e:2e	Broadc	ast	802.11	341	-19	-90	6.0	100	Beacon	frame,	SN=1803,	FN=0,	Flags=	C, BI=1
3	0.104487	CiscoInc_1f:4e:2e	Broadc	ast	802.11	341	-19	-90	6.0	100	Beacon	frame,	SN=1804,	FN=0,	Flags=	C, BI=1
4	0.104489	CiscoInc_1f:4e:2e	Broadc	ast	802.11	341	-19	-90	6.0	100	Beacon	frame,	SN=1805,	FN=0,	Flags=	C, BI=1
5	0.104381	CiscoInc_1f:4e:2e	Broadc	ast	802.11	341	-19	-90	6.0	100	Beacon	frame,	SN=1806,	FN=0,	Flags=	C, BI=1
6	0.104517	CiscoInc_1f:4e:2e	Broadc	ast	802.11	341	-19	-90	6.0	100	Beacon	frame,	SN=1807,	FN=0,	Flags=	C, BI=1
7	0.104361	CiscoInc_1f:4e:2e	Broadc	ast	802.11	341	-19	-90	6.0	100	Beacon	frame,	SN=1808,	FN=0,	Flags=	C, BI=1
Frame	e 1: 341 b	oytes on wire (2728	bits),	341 b	oytes ca	ptured	(272	8 bits	s) on	inter	face 0					
> PPI \	version 0,	32 bytes														}
~ 802.1	l1 radio i	Information														ļ
PHY	'type: 80	2.11a (5)														1
Tur	bo type:	Non-turbo (0)														
Dat	a rate: 6	.0 Mb/s	1 ←													
Cha	nnel: 100		1 6		these	fields	• • •									4
Fre	auencv: 5	500 MHz		050	liese	neius										
Sig	nal stren	gth (dBm): -19 dBm	1 🗲	App	oly as C	Colum	In									5
Noi	se level	(dBm): -90 dBm	1 4													}
TSF	timestam	p: 3313588701	J 🔨													1
	ration: 4	36 usl														1
Lund		A minimum	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		~~~~~			~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~~~~~	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	······			~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~		
									_							

0%) · Load time: 0:0.0

Profile: LNS WLAN PPI



#### $\checkmark$ To add different channel colors select $\rightarrow$ View $\rightarrow$ Coloring Rules...

	WLAN F	Probe Reque	st Channel 1 6 11.pcapng									
File	Edit	View Go	Capture Analyze Statistics	Telephony Wire	less Tools Help							1
		•	ै 🔀 🛅 । ९ 👄 🔿 警 👔	ي چ 📃 🛃 🚯	e, e, 🎹							4
	opply a d	isplay filter	<ctrl-></ctrl->									
Ir	terface			Channel	v v	FC	S Filter		~			
No.		Time	ТА	RA	Data rate (Mb/s)	Channel	SNR		Length	Info		
	1	0.000	IntelCor 79:46:04	Broadcast	1	11	-29	dBm	122	Probe	Request,	SN=4,
	2	0.001	IntelCor 79:46:04	Broadcast	1	11	-30	dBm	122	Probe	Request,	SN=5,
	3	0.001	IntelCor 79:46:04	Broadcast	1	11	-30	dBm	108	Probe	Request.	SN=6.1
	4	0.000	IntelCor 79:46:04	Broadcast	1	11	- 30	dBm	Wires	hark · Colori	ing Rules - LNS W	/LAN RadioTap
	5	0 033	IntelCor 79:46:04	Broadcast	1	11	- 31	dBm			-	
	6	0.000	IntelCor 79:46:04	Broadcast	1	11	31	dBm	Name			Filter
	0	0.005	IntelCon 70.46.04	Broadcast	1	11	- 22	dDm	✓ Bad	TCP State Char	100	tcp.analysis.flags
		0.107	Intercor_79:46:04	Broadcast	1	6	-32	abm		ning Tree To	opology Change	stp.type == 0x80
	8	0.038	IntelCor_79:46:04	Broadcast	1	6	-33	dBm	SPI OSPI	State Chan	ige S	ospf.msg != 1
	9	0.012	IntelCor_79:46:04	Broadcast	1	6	-30	dBm		^o errors		icmp.type eq 3    icmp.type eq 4    icmp.ty
	10	0.003	IntelCor 79:46:04	Broadcast	1	6	-31	dBm		)		arp icmp II icmpv6
	11	0.003	IntelCor 79:46:04	Broadcast	1	6	- 38	dBm	✓ TCP	RST		tcp.flags.reset eq 1
	12	0 013	IntelCor 79:46:04	Broadcast	1	6	- 32	dBm	🗹 TTL	ow or unexp	pected	(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !;
	12	0.015	IntelCon_70:40:04	Droadcast	1	0	- 52	dDm	Cheo	ksum Errors	5	cdp.checksum_bad==1    edp.checksum_k
	13	0.145	IntelCor_79:46:04	Broadcast	1	1	-37	abm		p		http://tcp.port == 80
	14	0.001	IntelCor_79:46:04	Broadcast	1	1	-38	dBm	✓ IPX			ipx    spx
	15	0.001	IntelCor_79:46:04	Broadcast	1	1	-40	dBm	DCEI	RPC		dcerpc
_	16	0,001	IntelCor 79:46:04	Broadcast	1	1	-43	dBm	Rout	ing SVNI/EINI		hsrp    eigrp    ospf    bgp    cdp    vrrp    gve
-	~~~~~	νου <u>-</u> γ						-		STIN/FIIN		tcp.nags & 0x02    tcp.nags.nn == 1
									UDP			udp
									Broa	dcast		eth[0] & 1
									Char	nnel 1		radiotap.channel.freq == 2412
									Char	nnel 6		radiotap.channel.freq == 2437
									I√I Char	nnel 11		radiotap.channel.freg == 2462

CSMA/CA offers different Inter Frame Spaces (IFS) to control media access:

 SIFS (Short Inter Frame Space)
 802.11b/g = 10 µs
 802.11a = 16 µs

 DIFS (DCF Inter Frame Space)
 (2x Slot time + SIFS)
 802.11b=50µs
 802.11g=28µs
 802.11a=34µs

 Slot Time 802.11b = 20 µs (max. 31x)
 Short Slot Time 802.11a/g = 9 µs (max. 15x)



- Stations can send anytime if media is free, but hold back if media is busy.
- If air becomes free, stations are waiting DIFS and a random number of Slot Times before sending
- Receiving stations verify Frame Check Sequence, if OK are sending ACK after SIFS











## You may have to start Wireshark in Admin Mode to see the AirPcap I/Fs

Verify the settings on the Capture Interfaces pane

erface	Traffic	Link-layer Header	Promis	Snaplen (	Buffer (MB)	Monitor Mode	e Capture	Filt
AirPcap USB wireless capture adapter nr	. 00 minutes and the second se	Per-Packet Information	$\checkmark$	default	2	_		
AirPcap Multi-Channel Aggregator	man hit was	Per-Packet Information		default	2	_		
AirPcap USB wireless capture adapter nr	. 01 Munner W	Per-Packet Information	$\leq$	default	2	_		
AirPcap USB wireless capture adapter nr	. 02 Arman Marca	Per-Packet Information	$\leq$	default	2	_		
Bluetooth-Netzwerkverbindung				default	2	_		
Drahtlosnetzwerkverbindung		Ethen		default	2	_		
LAN-Verbindung* 3		Ethernet		detault	2	_		
LAN-Verbindung	L	Etherna 1.	Selec	t		_		
LAN-Verbindung* 2		Eth			)			
		Virtua	I Adal	nter				
		Virtua	I Ada	pter				
		Virtua	I Ada	pter				
		Virtua	I Ada	pter				
		Virtua		pter				
	2 Proce	Virtua	I Ada	pter				
	2. Press	to	I Ada	pter				
nable promiscuous mode on all interfaces	2. Press Start Captu	to	I Ada	pter		Ма	nage Interfa	aces
inable promiscuous mode on all interfaces	2. Press Start Captu	to	IAda	pter		Ma	nage Interfa	ices

Key features:

- WiFi radios can use multiple 20 MHz channels (n/ac) to increase throughput
- Each radio cell is a shared media and is controlled by an Access Point (AP)
- A mobile client can be associated with only one AP at the time
- Radio cell access is controlled by managements and control frames
- Wireshark with AirPcap can capture and analyze these frames
- Understanding of these frames is crucial for WLAN troubleshooting





29

# Softing IT Networks introduces the new WaveXpert

- Includes 4 wireless adapter with 16 integrated antennas
- Supports 4x4 MIMO up to IEEE 802.11ac Wave 2
- USB-C type plug for data and unit power
- 2.4 GHz or 5 GHz versions available
- 4 x 4 : 4 up to 4 Channels (1'730 Mbps)
- 2 x 2 : 2 up to 8 Channels (1'730 Mbps)
- pcapng files incl. Radiotap header
- Retail price: EUR 1'950
  Availability: planned for 1st Qu. 2019

**A**Requirements:

- LINUX notebook and USB-C (Thunderbolt 3)
- Supporting most Linux's and Mac OS



		1100	1-1	110	
111.	Tratter				
IIII mun					
			Power Doess     But	Cot. Power In	
1		4	Overtemp	13-20v3c	

Multi-Channel WLAN Sniffer

Joint development of: Softing IT Networks GmbH 85540 Haar, Germany and GHMT AG 66450 Bexbach, Germany

# #sf18eu • Imperial Riding School Renaissance Vienna • Oct 29 - Nov 2

╋



+

Number of Chargens	Madulation	Antennas	Spatial	Maxi	mum R	ate (Mb	ops)	Band	
Number of Streams	Modulation	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 GH	
Two Streams*	64-QAM	2 x 2 :	2	144	300*	n.a.	n.a.	2.4 & 5 GH	
Three Streams	64-QAM	3 x 3 :	3	216	450	n.a.	n.a.	2.4 & 5 GH	
Four Streams	64-QAM	4 x 4 :	4	288	600	n.a.	n.a.	2.4 & 5 GH	

* AirPcap Nx supports Legacy, HT20 or HT40 mode (no SGI & Greenfield mode)

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

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	3	8	770	1600	3470	6930	5 GHz

** Softing WaveXpert supports up to 8 channels per WLAN adapter



802.11n



802.11ac Wave 1





802.11ac Wave 2

#### 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





That's it for Part 1, hope to see you back for:

# Troubleshooting WLANs (Part 2)

Troubleshooting WLANs using 802.11 Management & Control Frames

© Rolf Leutert, Leutert NetServices, <u>www.netsniffing.ch</u>

WLAN Trainings with Wireshark & WaveXpert available in Germany and Switzerland