Rolf Leutert, El. Ing. HTL
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
Session Objectives

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!
Troubleshooting WLANs comprises Layer 1 and Layer 2

### 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, Scanners
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. 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
Non-WiFi Devices’ Signatures

- Home trainers in a fitness center
- Microwave oven
- Remote control of model airplanes
- Wireless guitar
WiFi 802.11ac with four bonded channels
Large logistic enterprise, depending on WLAN for day-to-day operations
Two container cranes to load/unload trains require WLAN connections
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
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.
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.
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.

No adapter required, WiFi scanners are using internal WLAN cards.
### WiFi Scanners (just a few popular ones)

<table>
<thead>
<tr>
<th>Acrylic WiFi scanner</th>
<th><a href="http://www.acrylicwifi.com">www.acrylicwifi.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Ekahau HeatMapper</td>
<td><a href="http://www.ekahau.com">www.ekahau.com</a></td>
</tr>
<tr>
<td>inSSIDer</td>
<td><a href="http://www.metageek.com">www.metageek.com</a></td>
</tr>
<tr>
<td>NetStumbler</td>
<td><a href="http://www.netstumbler.com">www.netstumbler.com</a></td>
</tr>
<tr>
<td>Wifi Analyzer (Android)</td>
<td><a href="http://play.google.com">play.google.com</a></td>
</tr>
<tr>
<td>WifInfoView</td>
<td><a href="http://www.nirsoft.net">www.nirsoft.net</a></td>
</tr>
<tr>
<td>WifiScanner</td>
<td><a href="http://wifiscanner.sourceforge.net">wifiscanner.sourceforge.net</a></td>
</tr>
</tbody>
</table>

**BTW:** For iPhone/iPad, IOS Apple has locked direct access to the WiFi card 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!
Frequently Asked Questions:

- Can I use my built-in WLAN NIC with Wireshark?
  - Only your own traffic and no management and control frames will be captured
- Why would I need multiple AirPcaps?
  - To capture roaming processes
- Can I use AirPcaps to join a WLAN?
  - No, AirPcaps are monitoring devices only.
- Can I decrypt data with AirPcap adapter?
  - Yes, if shared keys are used, key is available and key negotiation is captured

MAC OS X and some Linux Drivers also support WLAN monitoring:
http://linuxwireless.org/en/users/Drivers
Capturing with the built-in WLAN NIC may display faked Ethernet frames only. Only Data frames and no Radio or WLAN header will be seen.
Radio cells use one or 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

AirPcap Nx 802.11a/b/g/n USB - adapter works with Wireshark and captures WiFi packets in both 2.4 GHz and 5 GHz bands.

www.riverbed.com/products/
AirPcap Nx Driver Support:

### Version 4.1.1:
(Unless otherwise noted, both 32 and 64 bit are supported.)
- Windows 2000 (32-bit only)
- Windows XP
- Windows Vista
- Windows 2000 Server (32-bit only)
- Windows Server 2003
- Windows Server 2008

### Version 4.1.3:
(Unless otherwise noted, both 32 and 64 bit are supported.)
- Windows 7 **Note 1**
- Windows 8
- Windows 8.1
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Chart notes:
1. Windows 7 does **not officially support USB 3.0**, so inserting an AirPcap adapter into some USB 3.0 interfaces may crash a system. When an AirPcap Nx adapter is inserted into a USB 3.0 port of Intel Series 7 or 8 chipset, Windows 7 will crash. Some third-party USB 3.0 controllers, for example, Fresco Logic xHCI (USB3) Controller FL1100 Series or VIA USB eXtensible Host Controller, works fine.

Release notes:
[https://support.riverbed.com/content/support/software/steelcentral-npm/airpcap.html](https://support.riverbed.com/content/support/software/steelcentral-npm/airpcap.html)
WLAN Layer 2 Analysis with AirPcap

1. Turn on Wireless Toolbar
2. Click on AirPcap Control Panel
3. Configure AirPcap Settings
You may have to start Wireshark in **Admin Mode** to see the AirPcap I/Fs

Verify the settings on the **Capture Interfaces** pane.

1. **Select Virtual Adapter**

2. **Press to Start Capturing**
The AirPcap Radiotap and PPI pseudo-header

- **Radiotap** or the newer **PPI (Per Packet Information)** are so called **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 frame.
- Receive signal strength, bit rate, channel number and other fields are added
- These fields can be added as columns in Wireshark and support troubleshooting
- Some other driver (i.e. MAC OS X) may also add these headers

More detailed information:
- Radiotap: [http://www.radiotap.org/Radiotap](http://www.radiotap.org/Radiotap)
- PPI manual: [http://www.cacetech.com/documents/PPI_Header_format_1.0.1.pdf](http://www.cacetech.com/documents/PPI_Header_format_1.0.1.pdf)
The AirPcap Radiotap and PPI pseudo-header

Radiotap Pseudo-Header added by AirPcap Classic

PPI Pseudo-Header added by AirPcap NX

SharkFest ’16 Europe • Arnhem, Netherlands • October 17-19, 2016 • #sf16eu • © Leutert NetServices
Customize Wireshark for WLAN analysis

- 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
Customize Wireshark for WLAN analysis

To add different **channel colors** select → **View** → Coloring Rules...

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>TA</th>
<th>RA</th>
<th>Data rate (Mb/s)</th>
<th>Channel</th>
<th>SNR</th>
<th>FCS Filter</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.000</td>
<td>IntelCor_79:46:04</td>
<td>Broadcast</td>
<td>1</td>
<td>11</td>
<td>-29 dBm</td>
<td></td>
<td>122 Probe Request, SN=4,</td>
</tr>
<tr>
<td>2</td>
<td>0.001</td>
<td>IntelCor_79:46:04</td>
<td>Broadcast</td>
<td>1</td>
<td>11</td>
<td>-30 dBm</td>
<td></td>
<td>122 Probe Request, SN=5,</td>
</tr>
<tr>
<td>3</td>
<td>0.001</td>
<td>IntelCor_79:46:04</td>
<td>Broadcast</td>
<td>1</td>
<td>11</td>
<td>-30 dBm</td>
<td></td>
<td>108 Probe Request, SN=6,</td>
</tr>
<tr>
<td>4</td>
<td>0.000</td>
<td>IntelCor_79:46:04</td>
<td>Broadcast</td>
<td>1</td>
<td>11</td>
<td>-30 dBm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>0.033</td>
<td>IntelCor_79:46:04</td>
<td>Broadcast</td>
<td>1</td>
<td>11</td>
<td>-31 dBm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>0.003</td>
<td>IntelCor_79:46:04</td>
<td>Broadcast</td>
<td>1</td>
<td>11</td>
<td>-31 dBm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>0.107</td>
<td>IntelCor_79:46:04</td>
<td>Broadcast</td>
<td>1</td>
<td>6</td>
<td>-32 dBm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>0.038</td>
<td>IntelCor_79:46:04</td>
<td>Broadcast</td>
<td>1</td>
<td>6</td>
<td>-33 dBm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>0.012</td>
<td>IntelCor_79:46:04</td>
<td>Broadcast</td>
<td>1</td>
<td>6</td>
<td>-30 dBm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>0.003</td>
<td>IntelCor_79:46:04</td>
<td>Broadcast</td>
<td>1</td>
<td>6</td>
<td>-31 dBm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>0.003</td>
<td>IntelCor_79:46:04</td>
<td>Broadcast</td>
<td>1</td>
<td>6</td>
<td>-38 dBm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>0.013</td>
<td>IntelCor_79:46:04</td>
<td>Broadcast</td>
<td>1</td>
<td>6</td>
<td>-32 dBm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>0.145</td>
<td>IntelCor_79:46:04</td>
<td>Broadcast</td>
<td>1</td>
<td>1</td>
<td>-37 dBm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>0.001</td>
<td>IntelCor_79:46:04</td>
<td>Broadcast</td>
<td>1</td>
<td>1</td>
<td>-38 dBm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>0.001</td>
<td>IntelCor_79:46:04</td>
<td>Broadcast</td>
<td>1</td>
<td>1</td>
<td>-40 dBm</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>0.001</td>
<td>IntelCor_79:46:04</td>
<td>Broadcast</td>
<td>1</td>
<td>1</td>
<td>-43 dBm</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Diagram:**

![Wireshark - Coloring Rules - LNS WLAN RadioTap](image)
802.11 Frame 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! Let’s have a break and hope to see you back for:

Troubleshooting WLANs (Part 2)

Troubleshooting WLANs using 802.11 Management & Control Frames
19. October 2016

Rolf Leutert
Leutert NetServices
Switzerland
www.netsniffing.ch
#sf16eu