Welcome!

Rolf Leutert
Leutert NetServices
Switzerland
www.netsniffing.ch

#sf16eu

Troubleshooting WLANs (Part 2)
Troubleshooting WLANs using 802.11 Management & Control Frames
19. October 2016
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 why analyzing WiFi layer 2 is a demanding task

Learn that WiFi frames looks very different from Ethernet

Learn why WiFi frames have one to four address fields

Learn how critical processes e.g. Joining, Roaming works

Learn how to read Wireshark files to isolate WiFi problems

Troubleshooting WiFi requires a full understanding of all 802.11 Management & Control frames and its associated processes!
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
Four different frame formats are used

- **Data Frame, Beacon, Probe Request, Probe Response, Authentication, Deauthentication, Association, Reassociation, Disassociation**

- **Acknowledge, Clear to Send**

- **Request to Send**

- **Data Frame through repeater**

Field names:
- FC = Frame Control
- Dur. = Duration
- RA = Receiver MAC Address
- TA = Transmitter MAC Address
- DA = Destination MAC Address
- SA = Source MAC Address
- Seq. = Sequence
- PDU = Protocol Data Unit
- FC = Frame Check Sequence
WiFi data frames have three MAC address fields.

Ethernet Frame:
- DA: Destination Address
- SA: Source Address
- Type

MAC Sta2, MAC Sta1, PDU

To Distribution System:
- MAC AP
- MAC Sta1
- MAC Sta2
- Seq.
- PDU

From Distribution System:
- RA: Receiver Address
- TA: Transmitter Address
- SA

Ethernet Frame:
- DA: Destination Address
- SA: Source Address
- Type

MAC Sta1, MAC Sta2, PDU

WiFi data frames have three MAC address fields.
WiFi data frames are acknowledged or retransmitted.

All retransmitted frames are marked with the Retry Bit.
All retransmitted frames are marked with the **Retry Bit**

---

```
Flags: 0x19

....   = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x11)
....   = More Fragments: This is the last fragment
   1.... = Retry: Frame is being retransmitted

...1 .... = PWR MGT: STA will go to sleep
...0 .... = More Data: No data buffered
.0... .... = Protected flag: Data is not protected
```

---

WiFi Data Transmission & Retransmission
In **non-aggregation mode** each packet is acknowledged individually.

The acknowledge frame follows **immediately after** each data frame.

The (single) acknowledge has **no source address field**.
802.11n introduced aggregation mode with a **Block Acknowledge (BA)**. In A-MPDU mode **up to 64 frames** can be acknowledged with one BA.
Management Frame: Beacon

Beacon tags contain information about supported and required features.

<table>
<thead>
<tr>
<th>Number</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Signal</th>
<th>Noise</th>
<th>TX Speed</th>
<th>Channel</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.0000000</td>
<td>CiscoInc_1f:4e:2e Broadcast</td>
<td>802.11 341</td>
<td>-19 -90 6.0</td>
<td>100 Beacon frame, SN=1802, FN=0, Flag</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0.104375</td>
<td>CiscoInc_1f:4e:2e Broadcast</td>
<td>802.11 341</td>
<td>-19 -90 6.0</td>
<td>100 Beacon frame, SN=1803, FN=0, Flag</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>0.104487</td>
<td>CiscoInc_1f:4e:2e Broadcast</td>
<td>802.11 341</td>
<td>-19 -90 6.0</td>
<td>100 Beacon frame, SN=1804, FN=0, Flag</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Standard 802.11a rates**
- **HT (High Throughput) 802.11n supported**
- **Robust Security Network contains info about type of authentication & encryption**
- **VHT (Very High Throughput)**
- **Standard 802.11ac supported**

SharkFest ’16 Europe • Arnhem, Netherlands • October 17-19, 2016 • #sf16eu • © Leutert NetServices
A client sends **Probe Requests** to scan the channels for Access Points. Capturing with **multiple AirPcaps** shows the scanning process.

---

### Management Frames: Probe Request & Response

![Image of Wireshark capture showing probe request frames](wlan probe request channel 1 6 11.png)

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>RA</th>
<th>Channel</th>
<th>Info</th>
<th>Data rate (Mbps)</th>
<th>Channel</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.000</td>
<td></td>
<td></td>
<td>Probe Request, SN=4, FN=0, Flags=........C, SSID=LNS-LAB-5.5GHz</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>2</td>
<td>0.001</td>
<td></td>
<td></td>
<td>Probe Request, SN=5, FN=0, Flags=........C, SSID=LNS-LAB-2.4GHz</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>3</td>
<td>0.001</td>
<td></td>
<td></td>
<td>Probe Request, SN=6, FN=0, Flags=........C, SSID=Broadcast</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>4</td>
<td>0.000</td>
<td></td>
<td></td>
<td>Probe Request, SN=7, FN=0, Flags=........C, SSID=LNS-LAB-5.5GHz</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>5</td>
<td>0.033</td>
<td></td>
<td></td>
<td>Probe Request, SN=8, FN=0, Flags=........C, SSID=LNS-LAB-5.5GHz</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>6</td>
<td>0.003</td>
<td></td>
<td></td>
<td>Probe Request, SN=11, FN=0, Flags=........C, SSID=LNS-LAB-5.5GHz</td>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>7</td>
<td>0.107</td>
<td></td>
<td></td>
<td>Probe Request, SN=21, FN=0, Flags=........C, SSID=LNS-LAB-2.4GHz</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>8</td>
<td>0.038</td>
<td></td>
<td></td>
<td>Probe Request, SN=24, FN=0, Flags=........C, SSID=LNS-LAB-5.5GHz</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>9</td>
<td>0.012</td>
<td></td>
<td></td>
<td>Probe Request, SN=25, FN=0, Flags=........C, SSID=LNS-LAB-2.4GHz</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>10</td>
<td>0.003</td>
<td></td>
<td></td>
<td>Probe Request, SN=26, FN=0, Flags=........C, SSID=Broadcast</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>11</td>
<td>0.003</td>
<td></td>
<td></td>
<td>Probe Request, SN=27, FN=0, Flags=........C, SSID=LNS-LAB-5.5GHz</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>12</td>
<td>0.013</td>
<td></td>
<td></td>
<td>Probe Request, SN=29, FN=0, Flags=........C, SSID=LNS-LAB-2.4GHz</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>13</td>
<td>0.145</td>
<td></td>
<td></td>
<td>Probe Request, SN=43, FN=0, Flags=........C, SSID=LNS-LAB-5.5GHz</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>14</td>
<td>0.001</td>
<td></td>
<td></td>
<td>Probe Request, SN=44, FN=0, Flags=........C, SSID=LNS-LAB-2.4GHz</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>15</td>
<td>0.001</td>
<td></td>
<td></td>
<td>Probe Request, SN=45, FN=0, Flags=........C, SSID=Broadcast</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>16</td>
<td>0.001</td>
<td></td>
<td></td>
<td>Probe Request, SN=46, FN=0, Flags=........C, SSID=LNS-LAB-5.5GHz</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

---

**IEEE 802.11 Probe Request, Flags:** .........C

**IEEE 802.11 wireless LAN management frame**

- **Tagged parameters (74 bytes)**
  - Tag: SSID parameter set: LNS-LAB-5.5GHz
  - Tag: Supported Rates: 1, 2, 5.5, 11, 6, 9, 12, 18, [Mbit/sec]
  - Tag: HT Capabilities (802.11n D1.10)
Probe Request contains client features and **specific or broadcast SSID**

Access Points reply with **Probe Response**, containing same fields as **Beacon**

Client supports **802.11a/n/ac**
The client selects an Access Point and sends **Authenticate & Associate requests**

Both processes must be successful in order to join the Access Point.
Wireshark can decrypt WEP, WPA & WPA2 PSK if the key is available.

To decrypt WPA & WPA2 the key negotiation process must be captured.
A client needs up to a minute duration to join an Access Point

Analyzing the trace file discloses the reason.

### WLAN Client slow joining.pcapng

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Delta</th>
<th>Source</th>
<th>Destination</th>
<th>Signal</th>
<th>TX Speed</th>
<th>Length</th>
<th>Channel</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>0.614</td>
<td>0.102</td>
<td>e2:5f:45:03:2c:9f</td>
<td>Broadcast</td>
<td>-22</td>
<td>1.0</td>
<td>266</td>
<td>1</td>
<td>802.11 Beacon frame, SN=908, FN=0, Flags=........</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>0.716</td>
<td>0.102</td>
<td>e2:5f:45:03:2c:9f</td>
<td>Broadcast</td>
<td>-22</td>
<td>1.0</td>
<td>266</td>
<td>1</td>
<td>802.11 Beacon frame, SN=909, FN=0, Flags=........</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td><em>REF</em></td>
<td><em>REF</em></td>
<td>D-LinkIn_f1:1a:49</td>
<td>e2:5f:45:03:2c:9f</td>
<td>-25</td>
<td>1.0</td>
<td>94</td>
<td>1</td>
<td>802.11 Probe Request, SN=664, FN=0, Flags=........</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>0.000</td>
<td>0.000</td>
<td>D-LinkIn_f1:1a:49</td>
<td>-22</td>
<td>1.0</td>
<td>46</td>
<td>1</td>
<td>802.11 Acknowledgement, Flags=........</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>0.004</td>
<td>0.004</td>
<td>e2:5f:45:03:2c:9f</td>
<td>Broadcast</td>
<td>-22</td>
<td>1.0</td>
<td>266</td>
<td>1</td>
<td>802.11 Beacon frame, SN=910, FN=0, Flags=........</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>0.107</td>
<td>0.102</td>
<td>e2:5f:45:03:2c:9f</td>
<td>Broadcast</td>
<td>-21</td>
<td>1.0</td>
<td>266</td>
<td>1</td>
<td>802.11 Beacon frame, SN=911, FN=0, Flags=........</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>0.200</td>
<td>0.102</td>
<td>e2:5f:45:03:2c:9f</td>
<td>Broadcast</td>
<td>-21</td>
<td>1.0</td>
<td>266</td>
<td>1</td>
<td>802.11 Beacon frame, SN=912, FN=0, Flags=........</td>
<td></td>
</tr>
</tbody>
</table>
Client joining problem (case two)

A client is not able to join an Access Point and finally deauthenticates from AP.

Analyzing the trace file discloses the reason.
Analyzing the WiFi roaming process

A client is roaming from channel 1 to 11 because the SNR of the new AP is better. Following the client with two AirPcaps allows to capture the roaming process.
User is complaining about **sporadic hangers** in bar code scanners, up to minutes.

Vendors of **mobile clients** and **access points** are finger pointing, since month.

Problem could be assigned to **bar code vendor** by analyzing trace files.
### Overview WiFi 802.11 Standards

<table>
<thead>
<tr>
<th>Rate</th>
<th>Modulation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2</td>
<td>Barker/DBPSK Barker/DBPSK</td>
<td>802.11 DSSS, 'Long Preamble'</td>
</tr>
<tr>
<td>5.5, 11</td>
<td>CCK/DQPSK CCK/DQPSK</td>
<td>802.11b High Rate (HR)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>with 'Short Preamble'</td>
</tr>
<tr>
<td>6, 9, 12, 18, 24, 36, 48, 54</td>
<td>OFDM/BPSK OFDM/QPSK OFDM/16-QAM OFDM/64-QAM</td>
<td>802.11g Extended Rate PHY (ERP)</td>
</tr>
<tr>
<td>From 6.5 up to 600*</td>
<td>OFDM/16-QAM OFDM/64-QAM</td>
<td>802.11n High Throughput (HT) Extensions</td>
</tr>
</tbody>
</table>

#### 2.4 GHz Band

- **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 Modulation

#### 5 GHz Band

- *With up to 2 Channels and up to 4 Streams*
- **With up to 8 Channels and up to 8 Streams**
A WLAN node can reserve airtime and refrain all other stations from sending. RTS/CTS reservation is used in busy cells, Hidden Node situations or in mixed mode.

WLAN RTS CTS_01.pcap

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Channel</th>
<th>SNR</th>
<th>Source</th>
<th>Destination</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>26</td>
<td>0.011778</td>
<td>1</td>
<td>40 dB</td>
<td>CiscoInc_11:1f_60</td>
<td>Philips_45:7f:2f</td>
<td>Request-to-send, Flags=...........C</td>
</tr>
<tr>
<td>27</td>
<td>0.000064</td>
<td>1</td>
<td>63 dB</td>
<td>CiscoInc_11:1f_60</td>
<td>Philips_45:7f:2f</td>
<td>Clear-to-send, Flags=...........C</td>
</tr>
<tr>
<td>28</td>
<td>0.000106</td>
<td>1</td>
<td>39 dB</td>
<td>66.249.91.104</td>
<td>192.168.0.203</td>
<td>HTTP/1.1 200 OK [Unreassembled Packet]</td>
</tr>
<tr>
<td>29</td>
<td>0.000098</td>
<td>1</td>
<td>62 dB</td>
<td>CiscoInc_11:1f_60</td>
<td>Philips_45:7f:2f</td>
<td>Request-to-send, Flags=...........C</td>
</tr>
<tr>
<td>30</td>
<td>0.004411</td>
<td>1</td>
<td>40 dB</td>
<td>CiscoInc_11:1f_60</td>
<td>Philips_45:7f:2f</td>
<td>Clear-to-send, Flags=...........C</td>
</tr>
<tr>
<td>31</td>
<td>0.000141</td>
<td>1</td>
<td>64 dB</td>
<td>CiscoInc_11:1f_60</td>
<td>Philips_45:7f:2f</td>
<td>Clear-to-send, Flags=...........C</td>
</tr>
<tr>
<td>32</td>
<td>0.000059</td>
<td>1</td>
<td>40 dB</td>
<td>66.249.91.104</td>
<td>192.168.0.203</td>
<td>Continuation</td>
</tr>
<tr>
<td>33</td>
<td>0.000062</td>
<td>1</td>
<td>62 dB</td>
<td>CiscoInc_11:1f_60</td>
<td>Philips_45:7f:2f</td>
<td>Acknowledgement, Flags=...........C</td>
</tr>
</tbody>
</table>

A short form, so-called CTS-to-Self is often used in cells with B-Only Clients present.

2277 0.001807 | 1 | 64 dB | Philips_45:7f:2f | Clear-to-send, Flags=...........C
2278 0.000158 | 1 | 60 dB | 192.168.0.201 | 192.168.0.100 | GET /images/sitewide_help_off.gif HTTP/1.1
2279 0.000003 | 1 | 42 dB | Philips_45:7f:2f | Acknowledgement, Flags=...........C
2281 0.053175 | 1 | 44 dB | CiscoInc_11:1f_60 | Clear-to-send, Flags=...........C
2282 0.000139 | 1 | 40 dB | 192.168.0.100 | 192.168.0.201 | HTTP/1.1 200 OK
2283 0.000063 | 1 | 61 dB | CiscoInc_11:1f_60 | Acknowledgement, Flags=...........C
2284 0.032421 | 1 | 65 dB | Philips_45:7f:2f | Clear-to-send, Flags=...........C
2285 0.000167 | 1 | 60 dB | 192.168.0.201 | 192.168.0.100 | 1133→80 [ACK] Seq=1515011717 Ack=1086513377
2286 0.000062 | 1 | 42 dB | Philips_45:7f:2f | Acknowledgement, Flags=...........C

SharkFest ’16 Europe • Arnhem, Netherlands • October 17-19, 2016 • #sf16eu • © Leutert NetServices
# Overview WiFi 802.11n/ac Raw Rates

<table>
<thead>
<tr>
<th>Number of Streams</th>
<th>Modulation</th>
<th>Antennas Tx x Rx : Spatial Streams</th>
<th>Maximum Rate (Mbps)</th>
<th>Band Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>One Stream*</td>
<td>64-QAM</td>
<td>1 x 1 : 1</td>
<td>72</td>
<td>n.a.</td>
</tr>
<tr>
<td>Two Streams*</td>
<td>64-QAM</td>
<td>2 x 2 : 2</td>
<td>144</td>
<td>n.a.</td>
</tr>
<tr>
<td>Three Streams</td>
<td>64-QAM</td>
<td>3 x 3 : 3</td>
<td>216</td>
<td>n.a.</td>
</tr>
<tr>
<td>Four Streams</td>
<td>64-QAM</td>
<td>4 x 4 : 4</td>
<td>288</td>
<td><strong>600</strong></td>
</tr>
</tbody>
</table>

* AirPcap Nx supports 802.11n with up to two Spatial Streams (2x2:2) in Legacy, HT20 or HT40 mode (no SGI & Greenfield mode)

<table>
<thead>
<tr>
<th>Number of Streams</th>
<th>Modulation</th>
<th>Antennas Tx x Rx : Spatial Streams</th>
<th>Maximum Rate (Mbps)</th>
<th>Band Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>One Stream</td>
<td>256-QAM</td>
<td>1 x 1 : 1</td>
<td>86</td>
<td>200</td>
</tr>
<tr>
<td>Two Streams</td>
<td>256-QAM</td>
<td>2 x 2 : 2</td>
<td>173</td>
<td>400</td>
</tr>
<tr>
<td>Three Streams</td>
<td>256-QAM</td>
<td>3 x 3 : 3</td>
<td>289</td>
<td><strong>600</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Number of Streams</th>
<th>Modulation</th>
<th>Antennas Tx x Rx : Spatial Streams</th>
<th>Maximum Rate (Mbps)</th>
<th>Band Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>One Stream</td>
<td>256-QAM</td>
<td>1 x 1 : 1</td>
<td>86</td>
<td>200</td>
</tr>
<tr>
<td>Two Streams</td>
<td>256-QAM</td>
<td>2 x 2 : 2</td>
<td>173</td>
<td>400</td>
</tr>
<tr>
<td>Three Streams</td>
<td>256-QAM</td>
<td>3 x 3 : 3</td>
<td>289</td>
<td><strong>600</strong></td>
</tr>
<tr>
<td>Four Streams</td>
<td>256-QAM</td>
<td>4 x 4 : 4</td>
<td>385</td>
<td>800</td>
</tr>
<tr>
<td>Eight Streams</td>
<td>256-QAM</td>
<td>8 x 8 : 8</td>
<td>770</td>
<td><strong>1600</strong></td>
</tr>
</tbody>
</table>

SharkFest ’16 Europe • Arnhem, Netherlands • October 17-19, 2016 • #sf16eu • © Leutert NetServices
Hope you learned something useful!

Rolf Leutert, Leutert NetServices, [www.netsniffing.ch](http://www.netsniffing.ch)