PA-12 WLAN Troubleshooting with Wireshark and AirPcap
Rolf Leutert, Leutert NetServices, Switzerland
Troubleshooting WLAN problems can be a very challenging task. The wireless media is known to be unreliable. **Signal interferences, low signal areas or overloaded cells** are just a few of possible issues. In addition, the compatibility between the different IEEE standards and the vendor's way of implementation is not always granted.

Having so many factors potentially impacting the performance of a wireless LAN, a **systematic root-cause analysis** will be more promising than the trial and error method.
Frequently Asked Questions:
• Can I use my built-in WLAN NIC with Wireshark?
• Why would I need AirPcaps to analyze WLAN?
• Why are there different types of AirPcaps?
• Can I combine different types of AirPcaps?
• Can I use AirPcaps to join a WLAN?
• Will name resolution work with AirPcaps?
• Will AirPcaps show me Radio Interferences?
• How do I troubleshoot encrypted WLANs?
Frequently Given Answers:
• Yes you can use the built in WLAN NIC with Wireshark!

But with a lot of restrictions:
• No promiscuous mode, only the own traffic visible
• Frames will be displayed in Ethernet format
• No radio information like SNR, channel no, speed etc.
• One channel only, not suitable for roaming analysis

And the biggest limitation:
• No management or control frames visible!
• But these are the ones you need for troubleshooting

(Exception: under Linux some NICs support more features)
### WLAN Troubleshooting with Wireshark and AirPcap

Capturing with built-in WLAN card

- Capturing on built-in WLAN NIC will display **Ethernet like frames**
- Only **Data** frames and no **Radio** or **WLAN** header will be seen

![Wireshark Capture](image)

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.000000</td>
<td>192.168.0.217</td>
<td>192.168.0.255</td>
<td>NBNS</td>
<td>92</td>
<td>Name query NB</td>
</tr>
<tr>
<td>2</td>
<td>0.258232</td>
<td>192.168.0.201</td>
<td>192.168.0.255</td>
<td>NBNS</td>
<td>92</td>
<td>Name query NB</td>
</tr>
<tr>
<td>3</td>
<td>0.069601</td>
<td>192.168.0.217</td>
<td>239.255.255.250</td>
<td>SSDP</td>
<td>175</td>
<td>M-SEARCH * HTTP</td>
</tr>
<tr>
<td>4</td>
<td>0.237969</td>
<td>192.168.0.201</td>
<td>239.255.255.250</td>
<td>SSDP</td>
<td>175</td>
<td>M-SEARCH * HTTP</td>
</tr>
<tr>
<td>5</td>
<td>0.199400</td>
<td>192.168.0.217</td>
<td>224.0.0.252</td>
<td>LLMNR</td>
<td>66</td>
<td>Standard query</td>
</tr>
<tr>
<td>6</td>
<td>0.107298</td>
<td>192.168.0.201</td>
<td>224.0.0.252</td>
<td>LLMNR</td>
<td>66</td>
<td>Standard query</td>
</tr>
<tr>
<td>7</td>
<td>0.001103</td>
<td>192.168.0.217</td>
<td>224.0.0.252</td>
<td>LLMNR</td>
<td>66</td>
<td>Standard query</td>
</tr>
<tr>
<td>8</td>
<td>0.203786</td>
<td>192.168.0.217</td>
<td>192.168.0.255</td>
<td>NBNS</td>
<td>92</td>
<td>Name query NB</td>
</tr>
<tr>
<td>9</td>
<td>0.102408</td>
<td>192.168.0.201</td>
<td>224.0.0.252</td>
<td>LLMNR</td>
<td>66</td>
<td>Standard query</td>
</tr>
<tr>
<td>10</td>
<td>0.002094</td>
<td>192.168.0.201</td>
<td>192.168.0.255</td>
<td>NBNS</td>
<td>92</td>
<td>Name query NB</td>
</tr>
<tr>
<td>11</td>
<td>0.659450</td>
<td>192.168.0.217</td>
<td>192.168.0.255</td>
<td>NBNS</td>
<td>92</td>
<td>Name query NB</td>
</tr>
</tbody>
</table>

Frame 1: 92 bytes on wire (736 bits), 92 bytes captured (736 bits)

Ethernet II, Src: IntelCor_73:68:54 (00:21:6b:73:68:54), Dst: Broadcast (ff:ff:ff:ff:ff:ff)


User Datagram Protocol, Src Port: netbios-ns (137), Dst Port: netbios-ns (13)

NetBIOS Name Service
Frequently Given Answers:

- AirPcaps support the following features:
  - Promiscuous mode, all traffic in a radio cell visible
  - Frames will be displayed original WLAN format
  - Lots of radio information like SNR, channel no, speed etc.
  - Capturing in multiple channels with multiple adapters
  - All frame types visible (Data, Management and Control)
WLAN Troubleshooting with Wireshark and AirPcap

Different AirPcap Adapters

Frequently Given Answers:
- Different AirPcaps for different 802.11 standards
- Different features at different costs
- Different AirPcaps can be combined together
- AirPcaps can not join a WLAN, are for capturing only
- Name resolution will not work for above reason
- Radio interferences can not be detected directly with AirPcaps
- Supported by all popular Windows versions up to Win7

New features within near future:
- 802.11ac standard support
- Win 8 drivers
- USB 3.0 support for NX (Classic and TX today)
WLAN Troubleshooting with Wireshark and AirPcap

Additional Wireshark Columns

• AirPcaps add a Radiotap Header with useful information to each captured frame
• Verify that the Radio option is turned on

Use the fields to add columns for:
• Channel #, TX Speed, SNR
WLAN Troubleshooting with Wireshark and AirPcap

Frame Types Overview

The Management Frames:

- Beacon
- Probe Request & Response
- Authentication & Deauthentication
- Association & Disassociation
- Reassociation Request & Response
- Action

The Control Frames:

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

The Data Frames:

- Data
- Null Function
WLAN Troubleshooting with Wireshark and AirPcap

Frame Type: Beacon

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple_6b:5e:fb</td>
<td>Broadcast</td>
<td>802.11</td>
<td>Beacon frame, SN=1873, FN=0, Flags=........C, BI=100</td>
</tr>
<tr>
<td>Apple_6b:5e:fb</td>
<td>Broadcast</td>
<td>802.11</td>
<td>Beacon frame, SN=1874, FN=0, Flags=........C, BI=100</td>
</tr>
<tr>
<td>Apple_6b:5e:fb</td>
<td>Broadcast</td>
<td>802.11</td>
<td>Beacon frame, SN=1875, FN=0, Flags=........C, BI=100</td>
</tr>
</tbody>
</table>

Frame 1: 238 bytes on wire (1904 bits), 238 bytes captured (1904 bits)

- Radiotap Header v0, Length 20
- IEEE 802.11 Beacon frame, Flags: ........C
- IEEE 802.11 wireless LAN management frame
  - Fixed parameters (12 bytes)
  - Tagged parameters (178 bytes)
    - Tag: SSID parameter set: LNS WLAN
    - Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 6, 9, 12, 18, [Mbit/sec]
    - Tag: DS Parameter set: Current Channel: 1
    - Tag: Traffic Indication Map (TIM): DTIM 1 of 0 bitmap
    - Tag: Country Information: Country Code CH, Environment Any
    - Tag: ERP Information
    - Tag: Extended Supported Rates 24, 36, 48, 54, [Mbit/sec]
    - Tag: RSN Information
    - Tag: HT Capabilities (802.11n D1.10)
    - Tag: HT Information (802.11n D1.10)
    - Tag: RM Enabled Capabilities (5 octets)
    - Tag: Vendor Specific: Microsoft
    - Tag: Vendor Specific: WMM/WME: Parameter Element
    - Tag: Vendor Specific: AppleCom
    - Tag: Vendor Specific: AppleCom
WLAN Troubleshooting with Wireshark and AirPcap

Frame Types: Probe Request / Probe Response

```
Frame 287: 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits)
The Radiotap Header v0, Length 20
IEEE 802.11 Probe Request, Flags: .......C
IEEE 802.11 wireless LAN management frame

- Tagged parameters (109 bytes)
  - Tag: SSID parameter set: LNS WLAN
  - Tag: Supported Rates 1, 2, 5.5, 11, [Mbit/sec]
  - Tag: Extended Supported Rates 6, 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
  - Tag: DS Parameter set: Current Channel: 1
  - Tag: HT Capabilities (802.11n D1.10)
  - Tag: Vendor Specific: Broadcom
  - Tag: Vendor Specific: Epigram: HT Capabilities (802.11n D1.10)
  - Tag: Vendor Specific: Microsoft: Unknown 8
```
WLAN Troubleshooting with Wireshark and AirPcap

Frame Types: Authentication Request / Authentication Response
WLAN Troubleshooting with Wireshark and AirPcap

Frame Types: Association Request / Association Response

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple_6b:5e:fb</td>
<td>Apple_6b:5e:fb</td>
<td>802.11 Association Request, SN=11, FN=0, Flag</td>
</tr>
<tr>
<td>Apple_af:36:f6</td>
<td>Apple_6b:5e:fb</td>
<td>802.11 Acknowledgement, Flags=........C</td>
</tr>
<tr>
<td>Apple_6b:5e:fb</td>
<td>Apple_af:36:f6</td>
<td>802.11 Association Response, SN=3370, FN=0, F</td>
</tr>
<tr>
<td>Apple_6b:5e:fb</td>
<td>Apple_6b:5e:fb (RA)</td>
<td>802.11 Acknowledgement, Flags=........C</td>
</tr>
</tbody>
</table>

- Frame 511: 195 bytes on wire (1560 bits), 195 bytes captured (1560 bits)
- Radiotap Header v0, Length 20
- IEEE 802.11 Association Request, Flags: ........C
- IEEE 802.11 wireless LAN management frame
  - Fixed parameters (4 bytes)
  - Tagged parameters (143 bytes)
    - Tag: SSID parameter set: LNS WLAN
    - Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 18, 24, 36, 54, [Mbit/sec]
    - Tag: Power Capability Min: 13, Max :22
    - Tag: Supported Channels
    - Tag: RSN Information
    - Tag: Extended Supported Rates 6, 9, 12, 48, [Mbit/sec]
    - Tag: HT Capabilities (802.11n D1.10)
    - Tag: RM Enabled Capabilities (5 octets)
    - Tag: Vendor Specific: Broadcom
    - Tag: Vendor Specific: Epigram: HT Capabilities (802.11n D1.10)
    - Tag: Vendor Specific: Microsoft: WMM/WME: Information Element
WLAN Troubleshooting with Wireshark and AirPcap

Frame Types: EAPOL Key Messages

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple_6b:5e:fb</td>
<td>Apple_af:36:f6</td>
<td>EAPOL</td>
<td>Key (Message 1 of 4)</td>
</tr>
<tr>
<td>Apple_6b:5e:fb</td>
<td>Apple_6b:5e:fb</td>
<td></td>
<td>802.11 Acknowledgement, Flags=.............C</td>
</tr>
<tr>
<td>Apple_6b:5e:fb</td>
<td>Apple_6b:5e:fb (RA)</td>
<td></td>
<td>802.11 Action, SN=15, FN=0, Flags=.............C</td>
</tr>
<tr>
<td>Apple_6b:5e:fb</td>
<td>Apple_af:36:f6 (RA)</td>
<td></td>
<td>802.11 Acknowledgement, Flags=.............C</td>
</tr>
<tr>
<td>Apple_6b:5e:fb</td>
<td>Apple_af:36:f6</td>
<td>EAPOL</td>
<td>Key (Message 2 of 4)</td>
</tr>
<tr>
<td>Apple_6b:5e:fb</td>
<td>Apple_6b:5e:fb</td>
<td></td>
<td>802.11 Acknowledgement, Flags=.............C</td>
</tr>
<tr>
<td>Apple_6b:5e:fb</td>
<td>Apple_6b:5e:fb (RA)</td>
<td></td>
<td>802.11 Acknowledgement, Flags=.............C</td>
</tr>
</tbody>
</table>

Frame 523: 155 bytes on wire (1240 bits), 155 bytes captured (1240 bits)
Radiotap Header v0, Length 20
IEEE 802.11 Data, Flags: ......F.C
Logical-Link Control
802.1X Authentication
Version: 802.1X-2004 (2)
Type: Key (3)
Length: 95
Key Descriptor Type: EAPOL RSN Key (2)
Key Information: 0x008a
Key Length: 16
Replay Counter: 363
WPA Key Nonce: 2a2624820cefa9f5908a09b4ddee72a5baceb3541e656...
Key IV: 00000000000000000000000000000000000000000000000000000
WPA Key RSC: 00000000000000000000000000000000
WPA Key ID: 000000000000000000000000
WPA Key MIC: 00000000000000000000000000000000000000000000000000000
WPA Key Data Length: 0
WLAN Troubleshooting with Wireshark and AirPcap

Frame Type: Action

**Frame 525**: 57 bytes on wire (456 bits), 57 bytes captured (456 bits)

- Radiotap Header v0, Length 20
- IEEE 802.11 Action, Flags: ........C
- IEEE 802.11 wireless LAN management frame

**Fixed parameters**
- Category code: Block Ack (3)
- **Action code: Add Block Ack Request (0x00)**
- Dialog token: 0x00e
- Block Ack Parameters: 0x1002, Block Ack Policy
  - ......... .......0 = A-MSDUs: Not Permitted
  - ......... .......1. = Block Ack Policy: Immediate Block Ack
  - ......... .......00 00.. = Traffic Identifier: 0x0000
  - 0001 0000 00..... = Number of Buffers (1 Buffer = 2304 Bytes): 64
  - Block Ack Timeout: 0x0000
- Block Ack Starting Sequence Control (SSC): 0x0000
  - ......... .......0000 = Fragment: 0
  - 0000 0000 0000 .... = Starting Sequence Number: 0
WLAN Troubleshooting with Wireshark and AirPcap

Frame Types: Decrypted Data Frame followed by Block Acknowledge

- **WEP and WPA1/2 personal mode** (shared key) can be decrypted by Wireshark
- To enable WPA decryption, the **key negotiation process** must be captured too
- Shared Key decryptions is possible during **capturing** or offline from a **stored file**
WLAN Troubleshooting with Wireshark and AirPcap

Frame Types: Null Function Data followed by Acknowledge

- The Null Function frame is often used as keep-alive message from the client
- Another purpose is to inform the AP if the client is changing the power save status
**WLAN Troubleshooting with Wireshark and AirPcap**

Frame Types: Request-to-send (RTS) and Clear-to-send (CTS)

- RTS /CTS are used to reserve airtime in **hidden node situations** or **busy networks**
- Another purpose is to **hinder old clients** from interfering with clients of **new standards**

---

![Wireshark Screenshot](image.png)

**Frame 835: 46 bytes on wire (368 bits), 46 bytes captured (368 bits)**

- Radiotap Header v0, Length 26
- IEEE 802.11 Request-to-send, Flags: ........C
  - Type/Subtype: Request-to-send (0x1b)
  - Frame Control Field: Ox400
  - **.000 0000 0101 0000 = Duration: 80 microseconds**
  - Receiver address: Apple_6b:5e:fb (e4:ce:8f:6b:5e:fb)
  - Frame check sequence: 0x38822ca4 [correct]
WLAN Troubleshooting with Wireshark and AirPcap

Frame Types: Data and Acknowledges

- In the air, every Data frame is acknowledged or otherwise retransmitted.
- 802.11 a/b/g every single Data frame is acknowledged. 802.11n introduced Block Acks.
- Single Acks must follow immediately after a Data frame and have no source address.

![Wireshark Capture of WLAN DataFrames](image-url)
WLAN Troubleshooting with Wireshark and AirPcap

Filter on Retransmitted frames

• Retransmitted frames are marked with the Retry Bit by the sender
• Create a Display Filter on retransmitted frames and save it as a Quick Filter Button
• Watch the percentage of retransmitted versus original frames in the bottom line
WLAN Troubleshooting with Wireshark and AirPcap

Where to capture WLAN frames

• The physical location within a radio cell is relevant for your capturing results

Rules of thumb

For analyzing problems in a single cell:
• Stay near the Access Point
• All traffic flows through the AP
• Clients must not hear each other

For analyzing roaming problems:
• Stay near the roaming client
• Capture with multiple AirPcaps
• Use Beacons to define your location
WLAN Troubleshooting with Wireshark and AirPcap

Graphical presentation of Radio Signal Strength with Wireshark IO Graphs

- Using the field `radiotap.db_antsignal` from two AirPcap NX tuned in two channels

```
Graph 2 Color Filter: wlan.sa == 00:1b:2b:a9:3b:c0  → Access Point in Channel A40
Graph 4 Color Filter: wlan.sa == 00:1b:2b:a9:3c:60  → Access Point in Channel A36
Graph 5 Color Filter: wlan.sa == 00:15:70:fb:c4:57  → Mobile Client followed with Wireshark
```
**WLAN Troubleshooting with Wireshark and AirPcap**

Overview of WLAN standards

<table>
<thead>
<tr>
<th>Mbps</th>
<th>Coding</th>
<th>Modulation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Barker</td>
<td>DBPSK</td>
<td>802.11 DSSS (Clause 15) with 'Long Preamble'</td>
</tr>
<tr>
<td>2</td>
<td>Barker</td>
<td>DBPSK</td>
<td></td>
</tr>
<tr>
<td>5.5</td>
<td>CCK</td>
<td>DQPSK</td>
<td>802.11b HR/DSSS (Clause 18) with 'Short Preamble'</td>
</tr>
<tr>
<td>11</td>
<td>CCK</td>
<td>DQPSK</td>
<td></td>
</tr>
<tr>
<td>6, 9</td>
<td>OFDM</td>
<td>BPSK, QPSK</td>
<td>802.11g Extended Rate PHY (ERP)</td>
</tr>
<tr>
<td>12, 18</td>
<td>OFDM</td>
<td>BPSK, QPSK</td>
<td></td>
</tr>
<tr>
<td>24, 36</td>
<td>OFDM</td>
<td>BPSK, QPSK</td>
<td></td>
</tr>
<tr>
<td>48, 54</td>
<td>OFDM</td>
<td>BPSK, QPSK</td>
<td></td>
</tr>
<tr>
<td>7.2-72.2</td>
<td>OFDM</td>
<td>MCS 0-7, 8-15</td>
<td>802.11n High Throughput (HT) Extensions</td>
</tr>
<tr>
<td>14.4-144.4</td>
<td>OFDM</td>
<td>MCS 0-7, 8-15</td>
<td></td>
</tr>
</tbody>
</table>

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
WLAN Troubleshooting with Wireshark and AirPcap

Outlook to WLAN products and standards

• 802.11n products using **4 streams** will go up to **600 Mbps** (PHY data rate)
• 802.11n products using **Beamforming** to focus RF energy and improve radio signal
• 802.11z **Direct Link Setup** to allow direct client to client communication
• 802.11w **Management Frame Protection** to increase security level against intruders

• 802.11ac **5G WiFi** is an improvement to 802.11n. Uses **5GHz band** and defines up to a maximum of **6.93 Gbps** with up to **8 streams** and up to **8 bonded** channels (160 MHz)

• 802.11ad **WiGig** for short range WLANs using **60GHz band** with up to **7Gbps**