Discover WLAN with Wireshark, AirPcap and WiSpy
Rolf Leutert, Leutert NetServices
Discover WLAN with Wireshark, AirPcap and WiSpy

Session objectives:

- Learn what you can see on layer 1 and layer 2.
- Learn which tools can help you finding WLAN problems.
- Learn how Management- and Control frames assists you in root cause analysis.
- Learn how to customize Wireshark to show you specific WLAN information.
Discover WLAN with Wireshark, AirPcap and Wi-Spy

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.

Client: WiFi compatible devices only

Tools: Wireshark, AirPcap, Scanners
WLAN Layer 1 Analysis

- 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
WLAN Layer 1 Analysis

Non-WiFi Devices’ Signatures

- Home trainers in a fitness center
- Microwave oven
- Remote control of model airplanes
- Wireless guitar
WLAN Layer 1 Analysis

WiFi 802.11ac with four bonded channels
WLAN Layer 1 Analysis (Case one)

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
WLAN Layer 1 Analysis (Case one)

- 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
WLAN Layer 1 Analysis (Case one)

 продолжаю анализ на уровне 1 на пути к крану №2 в диапазоне 2.4 ГГц

Сильное влияние от сигналов, не являющихся WiFi, на все три канала было обнаружено

Причина - источник находится за пределами территории клиентов’ → уведомлено чиновниками Swiss radio

Если передающая мощность находится в пределах законных пределов → требование сменить на 5 ГГц
WLAN Layer 1 Analysis (Case one)

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.

BAKOM scan result

Traffic monitoring induction loop
WiFi Scanners

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)

- Acrylic WiFi scanner: [www.acrylicwifi.com](http://www.acrylicwifi.com)
- Ekahau HeatMapper: [www.ekahau.com](http://www.ekahau.com)
- inSSIDer: [www.metageek.com](http://www.metageek.com)
- NetStumbler: [www.netstumbler.com](http://www.netstumbler.com)
- Wifi Analyzer (Android): [play.google.com](http://play.google.com)
- WifilInfoView: [www.nirsoft.net](http://www.nirsoft.net)
- WifiScanner: [wifiscanner.sourceforge.net](http://wifiscanner.sourceforge.net)

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!
WLAN Layer 2 Analysis

Key features:

- 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/
WLAN Layer 2 Analysis

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
WLAN Layer 2 Analysis

Capturing with the built-in WLAN NIC will display Ethernet-like frames.

Only Data frames and no Radio or WLAN header will be seen.

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</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).
NetBIOS Name Service.
WLAN Layer 2 Analysis

AirPcap is adding a Radio Tap or PPI (Per Packet Information) pseudo header.

The Pseudo-Header contains helpful infos like channel no, signal strength etc.

PPI version 0, 32 bytes
- version: 0
- Flags: 0x00
- Header Length: 32
- DLT: 105
- 802.11-Common
  - Field type: 802.11-Common (2)
  - Field length: 20
  - TSFT: 3091835552
- Flags: 0x0001
- Rate: 6.0 Mbps
- Channel Frequency: 5200 [A 40]
- Channel type: 802.11a (0x0140)
  - FHSS hopset: 0x00
  - FHSS pattern: 0x00
  - dBm antenna signal: -19
  - dBm antenna noise: -89

← PPI Pseudo Header added by AirPcap
Customize Wireshark for WLAN Analysis

- Create a new profile and customize your Wireshark before analyzing WLANs
- Turn on Wireless Toolbar and add columns with useful layer 1 information
- Configure AirPcap to add a Pseudo Header (PPI) to each frame at reception

Add Quick Filter buttons

Select Capture Type to include PPI

Use these fields and Apply as Column

Open the Per Packet Information pseudo header

Version: 0
Flag: 0x00
Header length: 32
DLT: 105
802.11-common
  Field type: 802.11-common (2)
  Field length: 20
  TSFT: 3313588701
  Flags: 0x0001
  Rate: 6.0 Mbps
  Channel frequency: 5500 [A 100]
Channel type: 802.11a (0x0140)
  FHSS hopset: 0x00
  FHSS pattern: 0x00
dBm antenna signal: -19
dBm antenna noise: -90
IEEE 802.11 Beacon frame, Flags: ..........C
IEEE 802.11 wireless LAN management frame
Customize Wireshark for WLAN Analysis

Adding a coloring rule per channel enhances readability.

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Channel</th>
<th>TX Speed</th>
<th>SNR</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.00000002462 [BG 11]</td>
<td>1.0</td>
<td>71 db</td>
<td>IntelCor_79:46:04 Broadcast</td>
<td>802.11 Probe Request, SN=4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>0.00124802462 [BG 11]</td>
<td>1.0</td>
<td>70 db</td>
<td>IntelCor_79:46:04 Broadcast</td>
<td>802.11 Probe Request, SN=5</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Wireshark: Coloring Rules**

List is processed in order until match is found.

- **Low TTL**: ip.ttl < 5
- **Checksum Err**: ether.checksum bad=1 || ip.checksum bad=1 || tcp.checksum bad=1
- **SMB**: smb || nbns || nbnx || nmb || nmbx || pico || netbios
- **HTTP**: http || tcp.port == 80
- **IPX**: ipx || spx
- **DCERPC**: dcerpc
- **Routing**: hsrp || eigrp || ospf || bgp || cdp || vrrp || grp || igmp || ismp
- **TCP SYN/FIN**: tcp.flags & 0x02 || tcp.flags.fin == 1
- **TCP**: tcp
- **UDP**: udp
- **Broadcast**: eth(0) & 1
- **Channel 1**: radiotap.channel.freq == 2412
- **Channel 6**: radiotap.channel.freq == 2437
- **Channel 11**: radiotap.channel.freq == 2452

22:50,5888492437 [BG 6] | 1.0 | 72 db | IntelCor_79:46:04 Broadcast | 802.11 Probe Request, SN=68 |
WLAN Layer 2 Analysis

802.11 frames look different from Ethernet frames
WLAN frames have from one to four MAC addresses
WLAN Layer 2 Analysis

Data Transmission (single packets)

Acks must follow immediately after a Data frame and have no source address.
WLAN Layer 2 Analysis

Access method Carrier Sense, Multiple Access w. Collision Avoidance CSMA/CA

Different time spaces control the access to the shared media

<table>
<thead>
<tr>
<th>SIFS (Short Inter Frame Space)</th>
<th>802.11b/g = 10 µs</th>
<th>802.11a = 16 µs</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIFS (DCF Inter Frame Space) (2x Slot time + SIFS)</td>
<td>802.11b=50µs 802.11g=28µs 802.11a=34µs</td>
<td></td>
</tr>
</tbody>
</table>

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

If media is free, each station waits **DIFS** and a random number of **Slot Times**
## WLAN Layer 2 Analysis

### 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
WLAN Layer 2 Analysis

Beacon Tags

Beacons tags contain information about supported and required features.

- IEEE 802.11 wireless LAN management frame
- Fixed parameters (12 bytes)
- Tagged parameters (269 bytes)
  - Tag: SSID parameter set: LNS-LAB-5.5GHz
  - Tag: Supported Rates 6(8), 9, 12, 18, 24, 36, 48, 54, [Mbit/sec]
  - Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
  - Tag: Country Information: Country Code CH, Environment Any
  - Tag: OBSS Load Element 802.11e CCA Version
  - Tag: HT Capabilities (802.11n D1.10)
  - Tag: RSN Information
  - Tag: HT Information (802.11n D1.10)
  - Tag: Extended Capabilities (8 octets)
  - Tag: Cisco CCX1 CKIP + Device Name
  - Tag: Vendor Specific: Aironet: Aironet DTPC Powerlevel] 0x16
  - Tag: VHT Capabilities (IEEE Std 802.11ac/D3.1)
  - Tag: VHT Operation (IEEE Std 802.11ac/D3.1)
  - Tag: VHT Tx Power Envelope (IEEE Std 802.11ac/D5.0)
  - Tag: Vendor Specific: Microsoft: WMM/WME: Parameter Element

- Standard 802.11a rates
- HT (High Throughput) 802.11n supported
- RSN (Robust Security Network) contains info about type of authentication & encryption
- VHT (Very High Throughput) Standard 802.11ac supported
WLAN Layer 2 Analysis

Probe Request / Probe Response

Clients scan for Access Points through all channels using **Probe Request**.

- **Probe Request** contains client features and a **specific or broadcast SSID**.

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

- **Client supports 802.11a/n/ac**

- Clients scan for Access Points through all channels using **Probe Request**.
- **Probe Request** contains client features and a **specific or broadcast SSID**.
- Access Points reply with **Probe Response**, containing the same fields as **Beacon**.
### WLAN Layer 2 Analysis

Following a roaming client with two AirPcap adapters

Using the packet capture tool Wireshark, we can analyze the network traffic of a roaming client with two AirPcap adapters. The screenshot below shows a fragment of the packet capture.

#### Packet Details

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Channel</th>
<th>Source MAC</th>
<th>Destination</th>
<th>Length</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>178</td>
<td>0.056</td>
<td>2412 [BG 1]</td>
<td>Cisco_11:1f:60</td>
<td>Broadcast</td>
<td>197</td>
<td>802.11</td>
<td>Beacon frame, SN=2024,</td>
</tr>
<tr>
<td>179</td>
<td>0.045</td>
<td>2462 [BG 11]</td>
<td>Cisco_92:ad:21</td>
<td>Broadcast</td>
<td>152</td>
<td>802.11</td>
<td>Beacon frame, SN=744,</td>
</tr>
<tr>
<td>180</td>
<td>0.056</td>
<td>2412 [BG 1]</td>
<td>Cisco_11:1f:60</td>
<td>Broadcast</td>
<td>197</td>
<td>802.11</td>
<td>Beacon frame, SN=2025,</td>
</tr>
<tr>
<td>181</td>
<td>0.045</td>
<td>2462 [BG 11]</td>
<td>Cisco_92:ad:21</td>
<td>Broadcast</td>
<td>152</td>
<td>802.11</td>
<td>Beacon frame, SN=745,</td>
</tr>
<tr>
<td>182</td>
<td>0.056</td>
<td>2412 [BG 1]</td>
<td>Cisco_11:1f:60</td>
<td>Broadcast</td>
<td>197</td>
<td>802.11</td>
<td>Beacon frame, SN=2026,</td>
</tr>
<tr>
<td>183</td>
<td>0.018</td>
<td>2412 [BG 1]</td>
<td>192.168.0.203</td>
<td>192.168.0.1</td>
<td>120</td>
<td>ICMP</td>
<td>Echo (ping) request</td>
</tr>
<tr>
<td>184</td>
<td>0.000</td>
<td>2412 [BG 1]</td>
<td>Philips_45:7f:2f</td>
<td>38</td>
<td>802.11</td>
<td>Acknowledgement, Flags</td>
<td></td>
</tr>
<tr>
<td>185</td>
<td>0.001</td>
<td>2412 [BG 1]</td>
<td>192.168.0.1</td>
<td>192.168.0.203</td>
<td>120</td>
<td>ICMP</td>
<td>Echo (ping) reply</td>
</tr>
<tr>
<td>186</td>
<td>0.000</td>
<td>2412 [BG 1]</td>
<td>Cisco_11:1f:60</td>
<td>Philips_45:7f:2f</td>
<td>38</td>
<td>802.11</td>
<td>Acknowledgement, Flags</td>
</tr>
<tr>
<td>187</td>
<td>0.025</td>
<td>2462 [BG 11]</td>
<td>Cisco_92:ad:21</td>
<td>Broadcast</td>
<td>152</td>
<td>802.11</td>
<td>Beacon frame, SN=746,</td>
</tr>
<tr>
<td>188</td>
<td>0.056</td>
<td>2412 [BG 1]</td>
<td>Cisco_11:1f:60</td>
<td>Broadcast</td>
<td>197</td>
<td>802.11</td>
<td>Beacon frame, SN=2028,</td>
</tr>
<tr>
<td>189</td>
<td>0.045</td>
<td>2462 [BG 11]</td>
<td>Cisco_92:ad:21</td>
<td>Broadcast</td>
<td>152</td>
<td>802.11</td>
<td>Beacon frame, SN=747,</td>
</tr>
<tr>
<td>190</td>
<td>0.000</td>
<td>2462 [BG 11]</td>
<td>Philips_45:7f:2f</td>
<td>Cisco_92:ad:21</td>
<td>58</td>
<td>802.11</td>
<td>Authentication, SN=284,</td>
</tr>
<tr>
<td>191</td>
<td>0.000</td>
<td>2462 [BG 11]</td>
<td>Philips_45:7f:2f</td>
<td>Philips_45:7f:2f</td>
<td>38</td>
<td>802.11</td>
<td>Authentication, Flags,</td>
</tr>
<tr>
<td>192</td>
<td>0.000</td>
<td>2462 [BG 11]</td>
<td>Cisco_92:ad:21</td>
<td>Philips_45:7f:2f</td>
<td>58</td>
<td>802.11</td>
<td>Authentication, Flags,</td>
</tr>
<tr>
<td>193</td>
<td>0.000</td>
<td>2462 [BG 11]</td>
<td>Cisco_92:ad:21</td>
<td>Philips_45:7f:2f</td>
<td>38</td>
<td>802.11</td>
<td>Authentication, Flags,</td>
</tr>
<tr>
<td>194</td>
<td>0.001</td>
<td>2462 [BG 11]</td>
<td>Philips_45:7f:2f</td>
<td>Cisco_92:ad:21</td>
<td>107</td>
<td>802.11</td>
<td>Reassociation Request,</td>
</tr>
<tr>
<td>195</td>
<td>0.000</td>
<td>2462 [BG 11]</td>
<td>Philips_45:7f:2f</td>
<td>Philips_45:7f:2f</td>
<td>38</td>
<td>802.11</td>
<td>Reassociation Response,</td>
</tr>
<tr>
<td>196</td>
<td>0.001</td>
<td>2462 [BG 11]</td>
<td>Cisco_92:ad:21</td>
<td>Philips_45:7f:2f</td>
<td>108</td>
<td>802.11</td>
<td>Reassociation Response,</td>
</tr>
<tr>
<td>197</td>
<td>0.000</td>
<td>2462 [BG 11]</td>
<td>Cisco_92:ad:21</td>
<td>Philips_45:7f:2f</td>
<td>38</td>
<td>802.11</td>
<td>Reassociation Response,</td>
</tr>
<tr>
<td>198</td>
<td>0.051</td>
<td>2412 [BG 1]</td>
<td>Cisco_11:1f:60</td>
<td>Broadcast</td>
<td>197</td>
<td>802.11</td>
<td>Beacon frame, SN=2029,</td>
</tr>
<tr>
<td>199</td>
<td>0.045</td>
<td>2462 [BG 11]</td>
<td>Cisco_92:ad:21</td>
<td>Broadcast</td>
<td>152</td>
<td>802.11</td>
<td>Beacon frame, SN=748,</td>
</tr>
<tr>
<td>200</td>
<td>0.056</td>
<td>2412 [BG 1]</td>
<td>Cisco_11:1f:60</td>
<td>Broadcast</td>
<td>197</td>
<td>802.11</td>
<td>Beacon frame, SN=2030,</td>
</tr>
</tbody>
</table>
### WLAN Layer 2 Analysis

**Association Request / Association Response**

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>IntelCor_79:46:04</td>
<td>Cisco_1f:4e:20</td>
<td>Authentication, SN=15, FN=0, Flags=........C</td>
</tr>
<tr>
<td>Cisco_1f:4e:20</td>
<td>IntelCor_79:46:04</td>
<td>Acknowledgement, Flags=........C</td>
</tr>
<tr>
<td>IntelCor_79:46:04</td>
<td>Cisco_1f:4e:20</td>
<td>Authentication, SN=1598, FN=0, Flags=........C</td>
</tr>
<tr>
<td>Cisco_1f:4e:20</td>
<td>IntelCor_79:46:04</td>
<td>Acknowledgement, Flags=........C</td>
</tr>
<tr>
<td>IntelCor_79:46:04</td>
<td>Cisco_1f:4e:20</td>
<td>Association Request, SN=16, FN=0, Flags=........C</td>
</tr>
<tr>
<td>Cisco_1f:4e:20</td>
<td>IntelCor_79:46:04</td>
<td>Acknowledgement, Flags=........C</td>
</tr>
<tr>
<td>Cisco_1f:4e:20</td>
<td>IntelCor_79:46:04</td>
<td>Acknowledgement, Flags=........C</td>
</tr>
<tr>
<td>Cisco_1f:4e:20</td>
<td>IntelCor_79:46:04</td>
<td>Key (Message 1 of 4)</td>
</tr>
<tr>
<td>Cisco_1f:4e:20</td>
<td>IntelCor_79:46:04</td>
<td>Key (Message 1 of 4)</td>
</tr>
<tr>
<td>IntelCor_79:46:04</td>
<td>Cisco_1f:4e:20</td>
<td>Acknowledgement, Flags=........C</td>
</tr>
<tr>
<td>Cisco_1f:4e:20</td>
<td>IntelCor_79:46:04</td>
<td>Key (Message 2 of 4)</td>
</tr>
<tr>
<td>Cisco_1f:4e:20</td>
<td>IntelCor_79:46:04</td>
<td>Key (Message 3 of 4)</td>
</tr>
<tr>
<td>Cisco_1f:4e:20</td>
<td>IntelCor_79:46:04</td>
<td>Key (Message 4 of 4)</td>
</tr>
<tr>
<td>IntelCor_79:46:04</td>
<td>Cisco_1f:4e:20</td>
<td>Acknowledgement, Flags=........C</td>
</tr>
<tr>
<td>0.0.0.0</td>
<td>255.255.255.255</td>
<td>DHCP Request - Transaction ID 0x86dfddf2</td>
</tr>
<tr>
<td>IntelCor_79:46:04</td>
<td>Broadcast</td>
<td>Acknowledgement, Flags=........C</td>
</tr>
<tr>
<td>IntelCor_79:46:04</td>
<td>Broadcast</td>
<td>Key (Message 4 of 4)</td>
</tr>
</tbody>
</table>

Key messages 1 - 4 must be captured to enable Wireshark to encrypt data.

- **Authentication** is old WEP legacy stuff; still there, but has no function.
- **Clients associates** with Access Point and **negotiates** WPA session key.
- All frames are **acknowledged** or retransmitted by the sender.
WLAN Layer 2 Analysis

Data Transmission (multiple packets in aggregation mode)

802.11n/ac supports up to 64 packet in a burst with a single Block Acknowledge.

Block Ack contains Bitmap to ack only good packets, other will be sent again.
WLAN Layer 2 Analysis

Interoperability between WLAN generations

Interoperability between 802.11b/g/n and 802.11a/n/ac is granted.

Mixed operations come at a cost: lower throughput.

Indicated throughput values are valid for non-mixed environment and small cells.

Clients at the border of cells transmit at low speed and use longer airtime.

Shrink your cell size and gain bandwidth by disabling lower rates in Access Points.

Try to get rid of old clients (especially B-only) before upgrading your APs.

<table>
<thead>
<tr>
<th>No.</th>
<th>Source</th>
<th>Destination</th>
<th>RSSI</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1150</td>
<td>PhilipsC_45:7f:2f (RA)</td>
<td>192.168.0.201</td>
<td>65</td>
<td>IEEE 802.11</td>
<td>Clear-to-send</td>
</tr>
<tr>
<td>1151</td>
<td>192.168.0.201</td>
<td>192.168.0.100</td>
<td>59</td>
<td>HTTP</td>
<td>GET /appsui.js HTTP/1.1</td>
</tr>
<tr>
<td>1152</td>
<td>PhilipsC_45:7f:2f (RA)</td>
<td>192.168.0.201</td>
<td>40</td>
<td>IEEE 802.11</td>
<td>Acknowledgement</td>
</tr>
<tr>
<td>1153</td>
<td>Cisco_11:1f:60 (RA)</td>
<td>192.168.0.201</td>
<td>44</td>
<td>IEEE 802.11</td>
<td>Clear-to-send</td>
</tr>
<tr>
<td>1154</td>
<td>192.168.0.100</td>
<td>192.168.0.201</td>
<td>40</td>
<td>HTTP</td>
<td>Continuation or non-HTTP</td>
</tr>
<tr>
<td>1155</td>
<td>Cisco_11:1f:60 (RA)</td>
<td>192.168.0.201</td>
<td>62</td>
<td>IEEE 802.11</td>
<td>Acknowledgement</td>
</tr>
<tr>
<td>1156</td>
<td>Cisco_11:1f:60 (RA)</td>
<td>192.168.0.201</td>
<td>44</td>
<td>IEEE 802.11</td>
<td>Clear-to-send</td>
</tr>
<tr>
<td>1157</td>
<td>192.168.0.100</td>
<td>192.168.0.201</td>
<td>40</td>
<td>HTTP</td>
<td>Continuation or non-HTTP</td>
</tr>
<tr>
<td>1158</td>
<td>Cisco_11:1f:60 (RA)</td>
<td>192.168.0.201</td>
<td>62</td>
<td>IEEE 802.11</td>
<td>Acknowledgement</td>
</tr>
</tbody>
</table>

Old clients must be silenced with Request-to-Send / Clear-to-send (RTS/CTS) or Clear-to-Send-Self (CTS-Self) frames sent before each data frame.

This process will significantly reduce the total cell throughput.
WLAN Layer 2 Analysis (Case two)

Customer problem analyzed and solved with Wireshark and AirPcap

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.
WLAN technology coming soon...

<table>
<thead>
<tr>
<th>Number of Streams</th>
<th>Modulation</th>
<th>Antennas Tx Rx</th>
<th>Spatial Streams</th>
<th>Maximum Rate (Mbps) 1 Ch.</th>
<th>Maximum Rate (Mbps) 2 Ch.</th>
<th>Maximum Rate (Mbps) 4 Ch.</th>
<th>Maximum Rate (Mbps) 8 Ch.</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>150</td>
<td>n.a.</td>
<td>n.a.</td>
<td>2.4 &amp; 5 GHz</td>
<td></td>
</tr>
<tr>
<td>Two Streams*</td>
<td>64-QAM</td>
<td>2 x 2 : 2</td>
<td>144</td>
<td>300</td>
<td>n.a.</td>
<td>n.a.</td>
<td>2.4 &amp; 5 GHz</td>
<td></td>
</tr>
<tr>
<td>Three Streams</td>
<td>64-QAM</td>
<td>3 x 3 : 3</td>
<td>216</td>
<td>450</td>
<td>n.a.</td>
<td>n.a.</td>
<td>2.4 &amp; 5 GHz</td>
<td></td>
</tr>
<tr>
<td>Four Streams</td>
<td>64-QAM</td>
<td>4 x 4 : 4</td>
<td>288</td>
<td>600</td>
<td>n.a.</td>
<td>n.a.</td>
<td>2.4 &amp; 5 GHz</td>
<td></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)
WLAN technology coming soon...

Unofficially announced: A new AirPcap adapter from Riverbed

Supporting Short Guard Interval (SGI), 3x3 MIMO, AC and more...
Planned availability: early 2016

<table>
<thead>
<tr>
<th>Product Requirements</th>
<th>Atheros AR9342 with Qualcomm/Atheros QCA9880</th>
</tr>
</thead>
<tbody>
<tr>
<td>3x3 MIMO</td>
<td>X</td>
</tr>
<tr>
<td>USB 3.0 (5Gbps or 640MB/s)</td>
<td>USB 2.0 (480Mbps or 60MB/s)</td>
</tr>
<tr>
<td>802.11ac (Theoretical max. 6,933Mbps or 900MB/s - Up to 8x 866.7Mbps channels)</td>
<td>X</td>
</tr>
<tr>
<td>802.11abgn (802.11n max. 600MB/s)</td>
<td>X</td>
</tr>
<tr>
<td>Win8</td>
<td></td>
</tr>
<tr>
<td>External Antenna</td>
<td>3</td>
</tr>
<tr>
<td>USB stick form factor</td>
<td>External USB Enclosure</td>
</tr>
<tr>
<td>Short Guard Interval</td>
<td>X</td>
</tr>
<tr>
<td>Channel Support</td>
<td>2.412-2.472Ghz, 5.180-5.825Ghz, TBD</td>
</tr>
</tbody>
</table>

Source: Riverbed Technology (specs. without commitment)
Thank you for your attention

Hope you learned something useful

Rolf Leutert, Leutert NetServices, www.wireshark.ch