Troubleshooting 802.11 with Monitoring Mode
Finding Patterns in your pcaps

19.10.2016

#sf16eu

Freelance Network & Security Troubleshooter | iwaxx Sàrl
About

• Freelance Network & Security troubleshooter
• Professional services in Switzerland
• Wireshark trainer
  • Practical hands-on onsite trainings
  • Custom needs: proprietary protocols, Lua dissection, malware analysis
• Creator of Debookee, a macOS network analyzer
  • Includes Wireshark & Lua scripts
  • Wi-Fi Monitoring module
Wi-Fi Monitoring ≠ Promiscuous mode
Wi-Fi Monitoring

• Promiscuous mode (in case of Ethernet)
  • Not really a packet capture "mode", more an "option"
  • Capture packets destined to another layer 2 network interface
  • Available on Wire / Wireless
  • Connection state: cable plugged (!) / Wireless: associated to an AP
  • Lowest protocol seen: Ethernet (IEEE 802.3)
  • OSI model level: Data Link Layer (Mac)
  • Packets not seen: Bad FCS packets: may be dropped by the network interface before the capture library can be aware of them
• Ethernet packet (not in Wi-Fi Monitoring mode)

- Frame 5683: 1180 bytes on wire (9440 bits), 1180 bytes captured (9440 bits) on interface 0
    - Source: Apple_ec:4a:73 (b4:18:d1:ec:4a:73)
    - Type: IPv4 (0x0800)
  - Session Initiation Protocol (INVITE)
Wi-Fi Monitoring

• **Wi-Fi Monitoring mode**
  • Available on Wireless only
  • Connection state: Must be disassociated of any network, but configured with a specific channel & channel width (20 – 80MHz)
  • Lowest protocol seen: IEEE 802.11
  • OSI model level: Physical (PHY) Layer + Data Link Layer (Mac)
• Data packet Wi-Fi Monitoring mode

- Frame 5: 146 bytes on wire (1168 bits), 146 bytes captured (1168 bits) on interface 0
- Radiotap Header v0, Length 48
- 802.11 radio information
  - PHY type: 802.11n (7)
  - MCS index: 0
  - Bandwidth: 20 MHz + 20 MHz lower (2)
  - Short GI: False
  - Greenfield: False
  - FEC: BEC (0)
  - Data rate: 6.5 Mb/s
  - Channel: 116
  - Frequency: 5580 MHz
  - Signal strength (dBm): -39 dBm
  - Noise level (dBm): -93 dBm
  - TSF timestamp: 345424326
- IEEE 802.11 Data, Flags: .p....F.C
- Data (62 bytes)
<table>
<thead>
<tr>
<th>Interface</th>
<th>Traffic</th>
<th>Link-layer Header</th>
<th>Promisc</th>
<th>Snaplen (B)</th>
<th>Buffer (MB)</th>
<th>Monitor</th>
<th>Capture Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wi-Fi: en0</td>
<td></td>
<td>802.11 plus radiotap header</td>
<td>✓</td>
<td>default</td>
<td>2</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>awdl0</td>
<td></td>
<td></td>
<td>default</td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thunderbolt Bridge: bridge0</td>
<td></td>
<td></td>
<td>default</td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thunderbolt 1: en1</td>
<td></td>
<td></td>
<td>default</td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Thunderbolt 2: en2</td>
<td></td>
<td></td>
<td>default</td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>p2p0</td>
<td></td>
<td></td>
<td>default</td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Loopback: lo0</td>
<td></td>
<td></td>
<td>default</td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco remote capture: cisco</td>
<td></td>
<td></td>
<td>default</td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Random packet generator: randpkt</td>
<td></td>
<td></td>
<td>default</td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSH remote capture: ssh</td>
<td></td>
<td></td>
<td>default</td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: [Enter a capture filter ...]
Practical theory of 802.11
• Characteristics of a Wi-Fi connection

• Channel
  • 2.4 GHz - Channel 1 to 14 (common used: 1, 6, 11) - 802.11/b/g/ng
  • 5 GHz - Channel 36 to 165 - 802.11a/na/ac

• Channel Width: 20, 40, 80 MHz (160 MHz soon with .11ac Wave 2)
• Characteristics of a Wi-Fi connection

• SSID - Name of your network
• BSSID - MAC address of the AP or ad-hoc
• Number of streams
  • Revolution of 802.11n - Spatial multiplexing
  • Independant data signals can be sent simultaneously by multiple TX antennas
• **Characteristics of a Wi-Fi connection**

  • **TX Signal Power** (emitted by the AP)
    • From 1 dBm (1 mW) to 20 dBm (100 mW)
  
  • **RX Signal Power** (received by the Client)
    • -30 dBm (0.001 mW) - Client is touching the AP (signal divided by 100'000 directly when going out the AP)
    • -50 dBm (10 nW) - Excellent
    • -60 dBm (1 nW) - Good
    • -70 dBm (100 pW) - Time to roam
    • -80 dBm (10 pW) - Time to cable?
    • -90 dBm (1 pW - 1 billion of mW) - Common noise
• Let's buy a Microwave Oven

Let's compare 900kg and 1ng
Wait... Where is speed? Gimme Mb/s
• **Speed is the correlation of:**
  - Channel width (20, 40, 80, 160 MHz)
  - Number of streams (1-3, coming 4 they say in blogs/coffee machine)
  - Guard Interval (Short or Long - Time interval between each frames)
  - Modulation or MCS index

• **Speed is set per packet, not once per connection**

• **Your best friend:** [http://mcsindex.com](http://mcsindex.com)
<table>
<thead>
<tr>
<th>HT MCS Index</th>
<th>Spatial Streams</th>
<th>Modulation &amp; Coding</th>
<th>Data Rate 20MHz</th>
<th>Data Rate 20MHz</th>
<th>Data Rate 40MHz</th>
<th>Data Rate 40MHz</th>
<th>Data Rate 80MHz</th>
<th>Data Rate 80MHz</th>
<th>Data Rate 160MHz</th>
<th>Data Rate 160MHz</th>
<th>VHT MCS Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>BPSK 1/2</td>
<td>6.5</td>
<td>7.2</td>
<td>13.5</td>
<td>15</td>
<td>29.3</td>
<td>32.5</td>
<td>58.5</td>
<td>65</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>QPSK 1/2</td>
<td>13</td>
<td>14.4</td>
<td>27</td>
<td>30</td>
<td>58.5</td>
<td>65</td>
<td>117</td>
<td>130</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>QPSK 3/4</td>
<td>19.5</td>
<td>21.7</td>
<td>40.5</td>
<td>45</td>
<td>87.8</td>
<td>97.5</td>
<td>175.5</td>
<td>195</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>16-QAM 1/2</td>
<td>26</td>
<td>28.9</td>
<td>54</td>
<td>60</td>
<td>117</td>
<td>130</td>
<td>234</td>
<td>260</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>16-QAM 3/4</td>
<td>39</td>
<td>43.3</td>
<td>81</td>
<td>90</td>
<td>175.5</td>
<td>195</td>
<td>351</td>
<td>390</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>64-QAM 2/3</td>
<td>52</td>
<td>57.8</td>
<td>108</td>
<td>120</td>
<td>234</td>
<td>260</td>
<td>468</td>
<td>520</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>64-QAM 3/4</td>
<td>58.5</td>
<td>65</td>
<td>121.5</td>
<td>135</td>
<td>263.3</td>
<td>292.5</td>
<td>526.5</td>
<td>585</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>64-QAM 5/6</td>
<td>65</td>
<td>72.2</td>
<td>135</td>
<td>150</td>
<td>292.5</td>
<td>325</td>
<td>585</td>
<td>650</td>
<td>7</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>256-QAM 3/4</td>
<td>78</td>
<td>86.7</td>
<td>162</td>
<td>180</td>
<td>351</td>
<td>390</td>
<td>702</td>
<td>780</td>
<td>8</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>256-QAM 5/6</td>
<td>n/a</td>
<td>n/a</td>
<td>180</td>
<td>200</td>
<td>390</td>
<td>433.3</td>
<td>780</td>
<td>866.7</td>
<td>9</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>BPSK 1/2</td>
<td>13</td>
<td>14.4</td>
<td>27</td>
<td>30</td>
<td>58.5</td>
<td>65</td>
<td>117</td>
<td>130</td>
<td>0</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>QPSK 1/2</td>
<td>26</td>
<td>28.9</td>
<td>54</td>
<td>60</td>
<td>117</td>
<td>130</td>
<td>234</td>
<td>260</td>
<td>1</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>QPSK 3/4</td>
<td>39</td>
<td>43.3</td>
<td>81</td>
<td>90</td>
<td>175.5</td>
<td>195</td>
<td>351</td>
<td>390</td>
<td>2</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>16-QAM 1/2</td>
<td>52</td>
<td>57.8</td>
<td>108</td>
<td>120</td>
<td>234</td>
<td>260</td>
<td>468</td>
<td>520</td>
<td>3</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
<td>16-QAM 3/4</td>
<td>78</td>
<td>86.7</td>
<td>162</td>
<td>180</td>
<td>351</td>
<td>390</td>
<td>702</td>
<td>780</td>
<td>4</td>
</tr>
<tr>
<td>13</td>
<td>2</td>
<td>64-QAM 2/3</td>
<td>104</td>
<td>115.6</td>
<td>216</td>
<td>240</td>
<td>468</td>
<td>520</td>
<td>936</td>
<td>1040</td>
<td>5</td>
</tr>
<tr>
<td>14</td>
<td>2</td>
<td>64-QAM 3/4</td>
<td>117</td>
<td>130.3</td>
<td>243</td>
<td>270</td>
<td>526.5</td>
<td>585</td>
<td>1053</td>
<td>1170</td>
<td>6</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td>64-QAM 5/6</td>
<td>130</td>
<td>144.4</td>
<td>270</td>
<td>300</td>
<td>585</td>
<td>650</td>
<td>1170</td>
<td>1300</td>
<td>7</td>
</tr>
</tbody>
</table>
How do I set Monitoring Mode?
Wi-Fi Monitoring

- Details for all OS: talk of Thomas d’Otreppe at SharkFest 16 US

**Linux**
- Natively with command lines or in Wireshark directly (free)

**macOS**
- Natively with command line or in Wireshark directly (free)
- also best hardware: 802.11ac 3x3
Wi-Fi Monitoring

• **Windows**
  
  • External dongles:
    
    • Riverbed external Airpcap dongles: 802.11n 2x2 ($700!)
      
      *Warning: Windows 7 + USB3 = BSOD!*
    
    • Savvius external dongles: 802.11n 3x3 ($60) - 802.11ac 2x2 ($150)
      
      *Works with Omnipeek only, not Wireshark or need a trick with npcap*
  
  • Using your internal Wi-Fi interface or external dongles:
    
    • Acrylic Wi-Fi Professional: NDIS 6 / Airpcap drivers ($40)
    
    • npcap: NDIS 6 (free)
      
      *Does your interface support NDIS 6? Driver support your interfaces? Support of 5GHz? Ability to configure channel bandwidth?*
<table>
<thead>
<tr>
<th>Interface</th>
<th>Traffic</th>
<th>Link-layer Header</th>
<th>Promi:</th>
<th>Snaplen (B)</th>
<th>Buffer (MB)</th>
<th>Monitor Mode</th>
<th>Capture Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirPcap USB wireless capture adapter nr. 00</td>
<td></td>
<td>Per-Packet Information</td>
<td>✓</td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ethernet</td>
<td></td>
<td>Ethernet</td>
<td>✓</td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wi-Fi</td>
<td></td>
<td>Ethernet</td>
<td>✓</td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connexion au réseau local</td>
<td></td>
<td>Ethernet</td>
<td>✓</td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connexion au réseau local* 15</td>
<td></td>
<td>Ethernet</td>
<td>✓</td>
<td>default</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Connexion réseau Bluetooth</td>
<td></td>
<td>USBPcap</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td></td>
<td></td>
</tr>
<tr>
<td>USBPcap1</td>
<td></td>
<td>USBPcap</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td></td>
<td></td>
</tr>
<tr>
<td>USBPcap2</td>
<td></td>
<td>USBPcap</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td></td>
<td></td>
</tr>
<tr>
<td>USBPcap3</td>
<td></td>
<td>USBPcap</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Enable promiscuous mode on all interfaces

Capture filter for selected interfaces: Enter a capture filter...
SharkFest ’16 Europe • Arnhem, Netherlands • October 17-19, 2016 • #sf16eu

Administrateur : Invite de commandes

```
C:\Windows\System32\Npcap>
C:\Windows\System32\Npcap>WlanHelper.exe -i
WlanHelper [Interactive Mode]:
*****************************************************************************
0. d0c88ca7-ce11-4fe6-8922-101e0b2de3bd
   Name: Wi-Fi
   Description: Carte rûseau sans fil Qualcomm Atheros AR5BWB222
   State: "disconnected"
   Operation Mode: "Network Monitor (NetMon)"
Enter the choice (0, 1,..) of the wireless card you want to operate on:
0
Enter the operation mode (0, 1 or 2) you want to switch to for the chosen wireless card:
0: Extensible Station (ExtSTA)
1: Network Monitor (NetMon)
2: Extensible Access Point (ExtAP)
1
SetInterface success!
C:\Windows\System32\Npcap>WlanHelper.exe d0c88ca7-ce11-4fe6-8922-101e0b2de3bd channel 1
Error: makeOIDRequest::My_PacketRequest error, error code = 1
Failure
```
Debookee @debookee · Oct 15
@hsluoyz Any plan to have the ability to set the channel bandwidth? 20/40/80MHz? Can’t set 5GHz channel, is it normal behavior or my interf?

Yang Luo
@hsluoyz

@debookee For 2nd question, it depends on your adapter, Please install 0.10 r8 and provide me the feedback of WlanHalper NAME channel XX.

9:54 AM - 16 Oct 2016
Ok, got hw, what should I do?
Ok, got hw, what should I do?
-> On which channel is your device?
Wi-Fi Monitoring

- A Wi-Fi scanner will help if only 1 BSSID per SSID

- If lot of APs with same SSID, must know where your device is associated
Wi-Fi Monitoring

- `netsh wlan show interface`

![Image of Wi-Fi monitoring output]

SharkFest ’16 Europe • Arnhem, Netherlands • October 17-19, 2016 • #sf16eu
Back to pcap - Lab#1
Radiotap / PPI headers
SSI Signal: -67 dBm
SSI Noise: -95 dBm
Antenna: 0
Channel number: 6
Channel frequency: 2437
Channel flags: 0x00010480, 2 GHz spectrum, Dynamic CCK-OFDM, HT Channel (20MHz Channel Width)

MCS information

- Known MCS information: 0x1f, Bandwidth, MCS index, Guard interval, Format, FEC type
  - .... 00 = Bandwidth: 20 MHz (0)
  - .... 1.. = Guard interval: short (1)
  - .... 0.. = Format: mixed (0)
  - ...0 .... = FEC type: BCC (0)

MCS index: 15
Data Rate: 144.4 Mb/s
• Back to pcap

SSI Signal: -67 dBm
SSI Noise: -95 dBm
Antenna: 0
Channel number: 6
Channel frequency: 2437

Channel flags: 0x00010480, 2 GHz spectrum, Dynamic CCK-OFDM, HT Channel (20MHz Channel Width)

MCS information

- Known MCS information: 0x1f, Bandwidth, MCS index, Guard interval, Format, FEC type
  - .... ..00 = Bandwidth: 20 MHz (0)
  - .... .1.. = Guard interval: short (1)
  - .... 0... = Format: mixed (0)
  - ...0 .... = FEC type: BCC (0)
- MCS index: 15
- [Data Rate: 144.4 Mb/s]
mcsindex.com pro tip: CTRL+F is your friend
<table>
<thead>
<tr>
<th>HT MCS Index</th>
<th>Spatial Streams</th>
<th>Modulation &amp; Coding</th>
<th>Data Rate GI = 800ns</th>
<th>Data Rate SGI = 400ns</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>BPSK 1/2</td>
<td>6.5</td>
<td>7.2</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>QPSK 1/2</td>
<td>13.0</td>
<td>14.4</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>QPSK 3/4</td>
<td>19.5</td>
<td>21.7</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>16-QAM 1/2</td>
<td>26.0</td>
<td>28.9</td>
</tr>
<tr>
<td>4</td>
<td>1</td>
<td>16-QAM 3/4</td>
<td>39.0</td>
<td>43.3</td>
</tr>
<tr>
<td>5</td>
<td>1</td>
<td>64-QAM 2/3</td>
<td>52.0</td>
<td>57.8</td>
</tr>
<tr>
<td>6</td>
<td>1</td>
<td>64-QAM 3/4</td>
<td>58.5</td>
<td>65.0</td>
</tr>
<tr>
<td>7</td>
<td>1</td>
<td>64-QAM 5/6</td>
<td>65.0</td>
<td>72.2</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>BPSK 1/2</td>
<td>13.0</td>
<td>14.4</td>
</tr>
<tr>
<td>9</td>
<td>2</td>
<td>QPSK 1/2</td>
<td>26.0</td>
<td>28.9</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>QPSK 3/4</td>
<td>39.0</td>
<td>43.3</td>
</tr>
<tr>
<td>11</td>
<td>2</td>
<td>16-QAM 1/2</td>
<td>52.0</td>
<td>57.8</td>
</tr>
<tr>
<td>12</td>
<td>2</td>
<td>16-QAM 3/4</td>
<td>78.0</td>
<td>86.7</td>
</tr>
<tr>
<td>13</td>
<td>2</td>
<td>64-QAM 2/3</td>
<td>104.0</td>
<td>115.6</td>
</tr>
<tr>
<td>14</td>
<td>2</td>
<td>64-QAM 3/4</td>
<td>117.0</td>
<td>130.3</td>
</tr>
<tr>
<td>15</td>
<td>2</td>
<td>64-QAM 5/6</td>
<td>130.0</td>
<td>144.4</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>256-QAM 3/4</td>
<td>156.0</td>
<td>173.3</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>256-QAM 5/6</td>
<td>156.0</td>
<td>324.0</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>n/a</td>
<td>156.0</td>
<td>360.0</td>
</tr>
</tbody>
</table>
Lab#2
Monitoring with Airpcap dongles
Lab#3

-> Capturing a 40 MHz flow at 20 MHz?
-> Is 44,+1 = 48,-1?
Lab#4
Why don't I see any data packets?
Why is my Wi-Fi slow?
Some indicators
• Is FCS a good metric in a Wi-Fi Monitoring capture?
  • NO!
  • FCS is a subjective metric of the monitoring station
  • You captured bad FCS seen by your monitoring station, not the client device
  • Lot of bad FCS if you're too close to the client
    • Radio orthogonality / Signal too strong / ???
    • Don't capture too close a client (< 2m)
• Use 802.11 Retries

  • `wlan.fc.retries == 1`
  • Set by the 802.11 device if previous data packet not ACKed
  • Check both Tx and Rx retries (<10-15% in a pro environment)
  • if Rx & Tx retries are high -> Check Layer 1 / Co-Channel Interferences
  • if Rx Retries >>> Tx Retries -> Power Mismatch (common with mobiles & professionnal Access Points)
• **Lab#5**

  - wlan.da == e0:2c:b2:3c:88:35 && wlan.fc.type == 2 - 382 pkts
  - wlan.da == e0:2c:b2:3c:88:35 && wlan.fc.type == 2 && wlan.fc.retry == 1 - 297 pkts
  - 78% Rx retries!
<table>
<thead>
<tr>
<th>MAC Address</th>
<th>Vendor</th>
<th>Associated with BSSID</th>
<th>dBm</th>
<th>c</th>
<th>c</th>
<th>Tx Bytes</th>
<th>Rx Bytes</th>
<th>%</th>
<th>Tx Throughput</th>
<th>% Rx Throughput</th>
<th>% Rx Retries</th>
<th>% Tx Retries</th>
<th>Tx Data Rate</th>
<th>Rx Data Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>ac:cf:5c:5e:32:de</td>
<td>Apple</td>
<td>40:0e:85:32:1f:6c</td>
<td>-63</td>
<td>-</td>
<td>-</td>
<td>2962290</td>
<td>91348221</td>
<td>19.5 k/s</td>
<td>1.2 MB/s</td>
<td>17</td>
<td>31</td>
<td>72.2</td>
<td>65</td>
<td></td>
</tr>
<tr>
<td>50:2e:5c:e4:46:b3</td>
<td>HTC Cor</td>
<td>8c:b6:4f:c9:5e:c4</td>
<td>-77</td>
<td>-</td>
<td>-</td>
<td>1304102</td>
<td>45777939</td>
<td>3.3 k/s</td>
<td>114 k/s</td>
<td>12</td>
<td>23</td>
<td>28.9</td>
<td>28.9</td>
<td></td>
</tr>
<tr>
<td>64:80:99:86:b0:0a</td>
<td>Intel C</td>
<td></td>
<td>-61</td>
<td>-</td>
<td>-</td>
<td>46078</td>
<td>13661790</td>
<td>0 B/s</td>
<td>0 B/s</td>
<td>5</td>
<td>47</td>
<td>65</td>
<td>57.8</td>
<td></td>
</tr>
<tr>
<td>08:70:45:6d:46:21</td>
<td>Apple</td>
<td>8c:b6:4f:c9:5e:c4</td>
<td>-87</td>
<td>-</td>
<td>-</td>
<td>488733</td>
<td>70458335</td>
<td>0 B/s</td>
<td>0 B/s</td>
<td>61 B/s</td>
<td>3</td>
<td>8</td>
<td>72.2</td>
<td>57.8</td>
</tr>
<tr>
<td>00:61:71:be:46:f8</td>
<td>Apple</td>
<td></td>
<td>-76</td>
<td>-</td>
<td>-</td>
<td>153362</td>
<td>764778</td>
<td>0 B/s</td>
<td>0 B/s</td>
<td>13</td>
<td>30</td>
<td>72.2</td>
<td>65</td>
<td></td>
</tr>
<tr>
<td>00:7a:b5:96:bc:82</td>
<td>HUAWEI</td>
<td>8c:b6:4f:c9:5e:c4</td>
<td>-69</td>
<td>-</td>
<td>-</td>
<td>3041478</td>
<td>682447</td>
<td>78.1 k/s</td>
<td>3.6 k/s</td>
<td>24</td>
<td>27</td>
<td>43.3</td>
<td>57.8</td>
<td></td>
</tr>
<tr>
<td>80:4e:81:6b:e8:59</td>
<td>Samsung</td>
<td></td>
<td>-54</td>
<td>-</td>
<td>-</td>
<td>94626</td>
<td>627847</td>
<td>0 B/s</td>
<td>0 B/s</td>
<td>37</td>
<td>66</td>
<td>57.8</td>
<td>65</td>
<td></td>
</tr>
</tbody>
</table>
Why is my Wi-Fi slow?
Practical theory of 802.11 #2
• What does a device before sending a packet?
  
  • Listen in the air for energy / ED (Energy Detection)
    • Is a microwave oven currently speaking?
    • Am I hearing bad CRC frames as noise?
  
  • Listen in the air for 802.11 frames / CS (Carrier Sense)
    • Save the NAV timer of heard packet (indicate when media will be freed)
  
  • When free, calculate a random number and wait while decreasing it
  • If media busy meanwhile, put random timer on hold
  • When random timer ends, if clear, send packet(s)
  • Wait for ACK, else resend packet with wlan.fc.retry = 1
The most important WLAN processes

Access Control with CSMA/CA

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 = 50 µs 802.11g = 28 µs 802.11a = 34 µs
- **Slot Time** 802.11b = 20 µs (max. 31x) 802.11a/g = 9 µs (max. 15x)

**Media free**

- AP: Data → Ack → Data
- Sta1: Ack
- Sta2: wait → DIFS → Data → DIFS → DIFS
- Sta3: wait → DIFS → DIFS → DIFS → DIFS → Data

- 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 and if OK are sending ACK after SIFS.
Forget Throughput - Think Airtime
# Throughput is a BAD metric for Wi-Fi

<table>
<thead>
<tr>
<th>Switched Ethernet</th>
<th>Wi-Fi</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Consistent link data rate</td>
<td>• Adaptive link data rate</td>
</tr>
<tr>
<td>• Consistent client capabilities</td>
<td>• Variable client capabilities</td>
</tr>
<tr>
<td>• No contention</td>
<td>• Contention prevalent</td>
</tr>
<tr>
<td>• Little overhead</td>
<td>• Significant overhead (positive ack, retransmissions, etc.)</td>
</tr>
</tbody>
</table>

- Throughput ≈ Link utilization
- Throughput ≠ Link utilization
- Airtime = Link utilization

Throughput is not a consistent measure of WLAN performance or capacity

SharkFest ’16 Europe • Arnhem, Netherlands • October 17-19, 2016 • #sf16eu
Lab#6
Why the device doesn't ACK these valid packets?
<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Data rate [Mb/s]</th>
<th>SSID</th>
<th>Signal</th>
<th>Retry</th>
<th>SeqNum</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>32457</td>
<td>25.7879</td>
<td>CiscoInc_c9:5</td>
<td>10.83.59.136</td>
<td>802.11</td>
<td>39</td>
<td>11</td>
<td>-62</td>
<td>0</td>
<td>0</td>
<td>Acknowledgement, Flags=........P........C</td>
<td></td>
</tr>
<tr>
<td>32530</td>
<td>25.8537</td>
<td>CiscoInc_c9:5</td>
<td>10.83.59.136</td>
<td>802.11</td>
<td>49</td>
<td>11</td>
<td>-32</td>
<td>0</td>
<td>0</td>
<td>802.11 Block Ack Req, Flags=.............</td>
<td></td>
</tr>
<tr>
<td>32570</td>
<td>25.8837</td>
<td>CiscoInc_c9:5</td>
<td>10.83.59.136</td>
<td>802.11</td>
<td>39</td>
<td>6</td>
<td>-77</td>
<td>0</td>
<td>0</td>
<td>Acknowledgement, Flags=..............C</td>
<td></td>
</tr>
<tr>
<td>32597</td>
<td>25.8938</td>
<td>10.83.63.26</td>
<td>52.27.109.112</td>
<td>TLSv1</td>
<td>687</td>
<td>13</td>
<td>-77</td>
<td>0</td>
<td>396</td>
<td>Application Data</td>
<td></td>
</tr>
<tr>
<td>32600</td>
<td>25.8996</td>
<td>10.83.63.26</td>
<td>52.27.109.112</td>
<td>TCP</td>
<td>664</td>
<td>11</td>
<td>-74</td>
<td>0</td>
<td>396</td>
<td>[TCP Retransmission] 37691-443 [PSH, ACK] Seq=35</td>
<td></td>
</tr>
<tr>
<td>32691</td>
<td>25.9649</td>
<td>CiscoInc_c9:5</td>
<td>10.83.59.136</td>
<td>802.11</td>
<td>39</td>
<td>6</td>
<td>-62</td>
<td>0</td>
<td>0</td>
<td>Acknowledgement, Flags=..............C</td>
<td></td>
</tr>
<tr>
<td>33145</td>
<td>26.3210</td>
<td>CiscoInc_c9:5</td>
<td>10.83.59.136</td>
<td>802.11</td>
<td>39</td>
<td>6</td>
<td>-33</td>
<td>0</td>
<td>0</td>
<td>Acknowledgement, Flags=..............C</td>
<td></td>
</tr>
<tr>
<td>33147</td>
<td>26.3212</td>
<td>10.83.63.26</td>
<td>179.60.192.2</td>
<td>TLSv1.2</td>
<td>194</td>
<td>26</td>
<td>-74</td>
<td>0</td>
<td>397</td>
<td>Application Data</td>
<td></td>
</tr>
<tr>
<td>33237</td>
<td>26.3649</td>
<td>10.83.63.26</td>
<td>52.27.109.112</td>
<td>TCP</td>
<td>687</td>
<td>39</td>
<td>-75</td>
<td>0</td>
<td>398</td>
<td>[TCP Retransmission] 37691-443 [PSH, ACK] Seq=35</td>
<td></td>
</tr>
<tr>
<td>33242</td>
<td>26.3659</td>
<td>CiscoInc_c9:5</td>
<td>10.83.59.136</td>
<td>802.11</td>
<td>39</td>
<td>6</td>
<td>-75</td>
<td>0</td>
<td>0</td>
<td>Acknowledgement, Flags=..............C</td>
<td></td>
</tr>
</tbody>
</table>
Lab#7
iperf - Let see slowness in the air
3 scenarios - Alone on channel 100

Cabled iperf Server

Access Point

802.11ac client
Connected at 878Mbps

Upload: 536Mb/s

Cabled iperf Server

Access Point

802.11n
Connected at 243Mbps

145Mb/s

Cabled iperf Server

Access Point

802.11ac
Connected at 878Mbps

215Mb/s

802.11n client
Connected at 243Mbps

90Mb/s
### Statistics

<table>
<thead>
<tr>
<th>Measurement</th>
<th>Captured</th>
<th>Displayed</th>
<th>Marked</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets</td>
<td>50569</td>
<td>193 (0.4%)</td>
<td>N/A</td>
</tr>
<tr>
<td>Time span, s</td>
<td>8.704</td>
<td>0.019</td>
<td>N/A</td>
</tr>
<tr>
<td>Average pps</td>
<td>5809.7</td>
<td>10221.4</td>
<td>N/A</td>
</tr>
<tr>
<td>Average packet size, B</td>
<td>1313.5</td>
<td>1606.5</td>
<td>N/A</td>
</tr>
<tr>
<td>Bytes</td>
<td>66439372</td>
<td>309974 (0.5%)</td>
<td>0</td>
</tr>
<tr>
<td>Average bytes/s</td>
<td>7632 k</td>
<td>16 M</td>
<td>N/A</td>
</tr>
<tr>
<td>Average bits/s</td>
<td>61 M</td>
<td><strong>131 M</strong></td>
<td>N/A</td>
</tr>
</tbody>
</table>
• True fact: capture is dropping packet
  • We see gaps in sequence number every 18-20ms
  • Internal buffer of the laptop drops packet to reach a max of 172Mbps
  • Should increase buffer? (default 2M, to be tested)
  • Except baselining, no need to monitor data packets at such speed to troubleshoot, most troubleshooting is done with Mgt/Ctrl frames
  • See Chris Greer videos on packet losses on personal laptops
536Mb/s
Retries: 1%

Wireshark IO Graphs: 07a

Bits/10 ms

0

250000

500000

750000

1,000,000

1,250,000

Time (s)

0

1

2

3

4

5

6
145 Mb/s
Retries: 1.6%
305Mb/s
Retries: 2.1%
Some Topic

• CWNP Certification Program
  • https://www.cwnp.com

• Some Wi-Fi guys
  • https://twitter.com/KeithRParsons
  • http://www.revolutionwifi.net/revolutionwifi/
  • http://divdyn.com/blog/
Thank you!

contact@iwaxx.com
twitter.com/tomlabade