Visualizing 802.11 Wireshark Data
Tuesday, July 26th, 2012

Ryan Woodings
Chief Geek | MetaGeek

@metageek
802.3 - Wired
1. CSMA CD
2. Distributed Access Scheme

802.11 - Wireless
1. CSMA CA
   • Distributed Access Scheme

Additional Considerations
2.4 & 5 GHz Public ISM bands
Overlapping Channels
Non-Wi-Fi Transmitters
Tx Power Restrictions
Channels

2.4 GHz
• 11 (US) 3 Non-Overlapping
• 13 (Europe) 4 Non-Overlapping

5 GHz
• 9 non-DFS (US)
• 12 DFS (US)
• 4 non-DFS (Europe)
• 15 DFS (Europe)

Detailed List
Channel Overlap
Physical Layer Modulation

CCK (HR-DSSS Phase Shift Keying)

OFDM (Orthogonal Frequency Division Multiplexing)
Co-Channel: Every station and access point on the same channel competes for the time to talk.

Adjacent Channel: Every Station and access point on an overlapping channel competes for time to talk.

Non-Wi-Fi: non-802.11 devices also compete for medium access.
802.11b

- 2.4 GHz-only
- 22 MHz Wide
- 1-11 Mbps
- HR-DSSS BPSK w/ CCK Modulation
- Good for longer range but low data rate.
802.11a

- 5 GHz-only
- 20 MHz Wide
- 6-54 Mbps
- OFDM Modulation
802.11g

- 2.4 GHz-only
- 20 MHz Wide
- 6-54Mbps
- ERP-OFDM Modulation
802.11n

- 2.4 & 5 GHz
- 20-40 MHz Wide
- 6-450 Mbps
- OFDM Modulation
Dynamic Rate Selection

As clients are further away from an Access point they choose a lower modulation rate.
Channel Contention
Channel Contention
Contention Domains

Channel
Antenna Pattern
Physical Barriers
Transmit Power
CSMA w/ CA

Wireless Medium Access

Start

Frame is Assembled

Is the Channel idle?

No → Wait for Random Backoff Time

Yes → Transmit RTS

CTS Received?

No → Transmit Application Data

Using IEEE 802.11 RTS/CTS Exchange

End
Wireless Medium Access

Station 1
- NAV
- Random Backoff (7 Slots)
- CTS
- ACK
- New Random Backoff (10 Slots)

Station 2
- NAV
- DIFS
- RTS
- SIFS
- DATA
- DIFS
- Station Defers
- NAV

Station 3
- NAV
- Random Backoff (9 Slots)
- Station defers, but keeps backoff counter (=2)
- Station sets NAV upon receiving RTS
- Remaining Backoff (2 Slots)
- ACK

Station 4
- NAV
- DIFS
- SIFS
- DATA
- SIFS

Station 5
- NAV
- SIFS
- ACK
- SIFS
- Station sets NAV upon receiving RTS
- Station sets NAV upon receiving CTS, this station is hidden to Station 1

Station 6
- DATA
- SIFS
- Station sets NAV upon receiving RTS
- Station sets NAV upon receiving CTS, this station is hidden to Station 1
802.11 Frame Types

Management Frames
wlan.fc.type == 0

Control
wlan.fc.type == 1

Data
wlan.fc.type == 2
Management frames "manage" stations joining and leaving a WLAN. These frames exist only in the 802.11 MAC layer.

For Example,
- Beacons
- Probes
- Authentications
- Associations

wlan.fc.type == 0
Control Frames

Control Frames "control" the RF medium and aid in delivery of data and management frames.

For Example,

• ACK
• Block-ACK
• RTS
• CTS

wlan.fc.type == 1
Data Frames carry higher-level protocol data

For Example,

- Data
- Data+CF-Ack
- Data+CF-Poll
- QoS data

```
wlan.fc.type == 2
```
Visual Packet Analysis
Packets vs. Bytes vs. Time
Packet Analysis Demo

Live Demo
WireShark Config Profiles

WLAN Frame Types
Data, Management and Control

Data Rates
Highlight frames sent slow/fast

Channels
For captures with multiple adapters.
Additional Columns to Consider:

SubType
wlan.fc.type_subtype

Data Rate
IEEE 802.11 TX rate (existing field type)

RSSI
IEEE 802.11 RSSI (existing field type)
## Packet Type Profile

<table>
<thead>
<tr>
<th>SubType</th>
<th>Data Rate</th>
<th>RSSI</th>
<th>Destination</th>
<th>Source</th>
<th>Protocol</th>
<th>To/From DS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Beacon frame</td>
<td>11.0</td>
<td>20 db</td>
<td>Broadcast</td>
<td>Cisco_7d:de:da</td>
<td>IEEE 802.11</td>
<td>Not leaving DS or</td>
</tr>
<tr>
<td>QoS Data</td>
<td>1.0</td>
<td>17 db</td>
<td>e8:b7:48:3b:8b:f2</td>
<td>MurataMa_5c:1f:7a</td>
<td>IEEE 802.11</td>
<td>Frame from STA to</td>
</tr>
<tr>
<td>Acknowledgement</td>
<td>1.0</td>
<td>22 db</td>
<td>MurataMa_5c:1f:7a (RA)</td>
<td>Aerohive_25:c2:50</td>
<td>IEEE 802.11</td>
<td>Not leaving DS or</td>
</tr>
<tr>
<td>Beacon frame</td>
<td>1.0</td>
<td>22 db</td>
<td>Broadcast</td>
<td>Aerohive_25:c2:50</td>
<td>IEEE 802.11</td>
<td>Not leaving DS or</td>
</tr>
<tr>
<td>Beacon frame</td>
<td>1.0</td>
<td>20 db</td>
<td>Broadcast</td>
<td>Cisco_7d:de:db</td>
<td>IEEE 802.11</td>
<td>Not leaving DS or</td>
</tr>
<tr>
<td>QoS Data</td>
<td>1.0</td>
<td>21 db</td>
<td>MurataMa_5c:1f:7a</td>
<td>e8:b7:48:3b:8b:f2</td>
<td>IEEE 802.11</td>
<td>Frame from DS to</td>
</tr>
<tr>
<td>Acknowledgement</td>
<td>1.0</td>
<td>17 db</td>
<td>Aerohive_25:c2:50 (RA)</td>
<td>MurataMa_5c:1f:7a</td>
<td>IEEE 802.11</td>
<td>Not leaving DS or</td>
</tr>
<tr>
<td>QoS Data</td>
<td>1.0</td>
<td>23 db</td>
<td>MurataMa_5c:1f:7a</td>
<td>e8:b7:48:3b:8b:f2</td>
<td>IEEE 802.11</td>
<td>Frame from DS to</td>
</tr>
<tr>
<td>Acknowledgement</td>
<td>1.0</td>
<td>16 db</td>
<td>Aerohive_25:c2:50 (RA)</td>
<td>MurataMa_5c:1f:7a</td>
<td>IEEE 802.11</td>
<td>Not leaving DS or</td>
</tr>
<tr>
<td>QoS Data</td>
<td>1.0</td>
<td>22 db</td>
<td>MurataMa_5c:1f:7a</td>
<td>e8:b7:48:3b:8b:f2</td>
<td>IEEE 802.11</td>
<td>Frame from DS to</td>
</tr>
<tr>
<td>Acknowledgement</td>
<td>1.0</td>
<td>17 db</td>
<td>Aerohive_25:c2:50 (RA)</td>
<td>MurataMa_5c:1f:7a</td>
<td>IEEE 802.11</td>
<td>Not leaving DS or</td>
</tr>
<tr>
<td>QoS Data</td>
<td>1.0</td>
<td>22 db</td>
<td>MurataMa_5c:1f:7a</td>
<td>e8:b7:48:3b:8b:f2</td>
<td>IEEE 802.11</td>
<td>Frame from DS to</td>
</tr>
<tr>
<td>Acknowledgement</td>
<td>1.0</td>
<td>19 db</td>
<td>Aerohive_25:c2:50 (RA)</td>
<td>MurataMa_5c:1f:7a</td>
<td>IEEE 802.11</td>
<td>Not leaving DS or</td>
</tr>
<tr>
<td>QoS Data</td>
<td>1.0</td>
<td>22 db</td>
<td>MurataMa_5c:1f:7a</td>
<td>e8:b7:48:3b:8b:f2</td>
<td>IEEE 802.11</td>
<td>Frame from DS to</td>
</tr>
<tr>
<td>Acknowledgement</td>
<td>1.0</td>
<td>18 db</td>
<td>Aerohive_25:c2:50 (RA)</td>
<td>MurataMa_5c:1f:7a</td>
<td>IEEE 802.11</td>
<td>Not leaving DS or</td>
</tr>
<tr>
<td>Beacon frame</td>
<td>11.0</td>
<td>18 db</td>
<td>Broadcast</td>
<td>Cisco_7d:de:dc</td>
<td>IEEE 802.11</td>
<td>Not leaving DS or</td>
</tr>
<tr>
<td>QoS Data</td>
<td>1.0</td>
<td>22 db</td>
<td>MurataMa_5c:1f:7a</td>
<td>e8:b7:48:3b:8b:f2</td>
<td>IEEE 802.11</td>
<td>Frame from DS to</td>
</tr>
<tr>
<td>Acknowledgement</td>
<td>1.0</td>
<td>18 db</td>
<td>Aerohive_25:c2:50 (RA)</td>
<td>MurataMa_5c:1f:7a</td>
<td>IEEE 802.11</td>
<td>Not leaving DS or</td>
</tr>
<tr>
<td>QoS Data</td>
<td>1.0</td>
<td>20 db</td>
<td>e8:b7:48:3b:8b:f2</td>
<td>MurataMa_5c:1f:7a</td>
<td>IEEE 802.11</td>
<td>Frame from STA to</td>
</tr>
<tr>
<td>Acknowledgement</td>
<td>1.0</td>
<td>22 db</td>
<td>MurataMa_5c:1f:7a (RA)</td>
<td>MurataMa_5c:1f:7a</td>
<td>IEEE 802.11</td>
<td>Not leaving DS or</td>
</tr>
<tr>
<td>QoS Data</td>
<td>1.0</td>
<td>22 db</td>
<td>MurataMa_5c:1f:7a</td>
<td>e8:b7:48:3b:8b:f2</td>
<td>IEEE 802.11</td>
<td>Frame from DS to</td>
</tr>
<tr>
<td>Acknowledgement</td>
<td>1.0</td>
<td>18 db</td>
<td>Aerohive_25:c2:50 (RA)</td>
<td>MurataMa_5c:1f:7a</td>
<td>IEEE 802.11</td>
<td>Not leaving DS or</td>
</tr>
<tr>
<td>QoS Data</td>
<td>1.0</td>
<td>17 db</td>
<td>e8:b7:48:3b:8b:f2</td>
<td>MurataMa_5c:1f:7a</td>
<td>IEEE 802.11</td>
<td>Frame from STA to</td>
</tr>
<tr>
<td>Acknowledgement</td>
<td>1.0</td>
<td>22 db</td>
<td>MurataMa_5c:1f:7a (RA)</td>
<td>MurataMa_5c:1f:7a</td>
<td>IEEE 802.11</td>
<td>Not leaving DS or</td>
</tr>
</tbody>
</table>
Channel Profile

<table>
<thead>
<tr>
<th>Channel</th>
<th>Filter Expression</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>wlan_mgt.ht.info.primarychannel == 1</td>
</tr>
<tr>
<td>2</td>
<td>wlan_mgt.ht.info.primarychannel == 2</td>
</tr>
<tr>
<td>3</td>
<td>wlan_mgt.ht.info.primarychannel == 3</td>
</tr>
<tr>
<td>4</td>
<td>wlan_mgt.ht.info.primarychannel == 4</td>
</tr>
<tr>
<td>5</td>
<td>wlan_mgt.ht.info.primarychannel == 5</td>
</tr>
<tr>
<td>6</td>
<td>wlan_mgt.ht.info.primarychannel == 6</td>
</tr>
<tr>
<td>7</td>
<td>wlan_mgt.ht.info.primarychannel == 7</td>
</tr>
<tr>
<td>8</td>
<td>wlan_mgt.ht.info.primarychannel == 8</td>
</tr>
<tr>
<td>9</td>
<td>wlan_mgt.ht.info.primarychannel == 9</td>
</tr>
<tr>
<td>10</td>
<td>wlan_mgt.ht.info.primarychannel == 10</td>
</tr>
<tr>
<td>11</td>
<td>wlan_mgt.ht.info.primarychannel == 11</td>
</tr>
</tbody>
</table>

**Table:**

- **Data Type:** Sniffed packets from an 802.11 network.
- **Time Range:** June 24–27, 2012.
- **Protocol:** 802.11 with detailed packet analysis.

**Image:**

- WireShark tool interface showing channel analysis.
- Intercepted packets illustrating channel utilization.
- Filter configuration for channel differentiation.

**Functionality:**

- **New Filter:** Add new rules.
- **Edit Filter:** Modify existing rules.
- **Enable/Disable:** Activate/deactivate filters.
- **Ordering:** Reorder filters for optimized analysis.

**Analysis:**

- Channels 1-11 are configured with specific filters to analyze different aspects of the network traffic.
- Packet counts and types are categorized under each channel.
- This tool is essential for network monitoring and debugging.
## Data Rate Profile

<table>
<thead>
<tr>
<th>SubType</th>
<th>Rate</th>
<th>RSS</th>
<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>29</td>
<td>3.5</td>
<td>7</td>
<td>db</td>
<td>2852 36 204239</td>
<td>apple,20,4b,08  (AK)</td>
<td>802.11</td>
<td>40</td>
<td>Acknowledgment, Flags:.......C</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>5</td>
<td>9</td>
<td>db</td>
<td>2855 36 205926</td>
<td>apple,20,4b,08  (AK)</td>
<td>802.11</td>
<td>40</td>
<td>Acknowledgment, Flags:.......C</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>5</td>
<td>8</td>
<td>db</td>
<td>2855 36 249303</td>
<td>apple,20,4b,08  (AK)</td>
<td>802.11</td>
<td>40</td>
<td>Acknowledgment, Flags:.......C</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>6</td>
<td>9</td>
<td>db</td>
<td>2856 36 249982</td>
<td>apple,20,4b,08  (AK)</td>
<td>802.11</td>
<td>40</td>
<td>Acknowledgment, Flags:.......C</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>10</td>
<td>10</td>
<td>db</td>
<td>2856 36 410333</td>
<td>apple,20,4b,08  (AK)</td>
<td>802.11</td>
<td>40</td>
<td>Acknowledgment, Flags:.......C</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>5</td>
<td>5</td>
<td>db</td>
<td>2861 36 136200</td>
<td>apple,20,4b,08  (AK)</td>
<td>802.11</td>
<td>40</td>
<td>Acknowledgment, Flags:.......C</td>
<td></td>
</tr>
<tr>
<td>29</td>
<td>5</td>
<td>7</td>
<td>db</td>
<td>2864 60 651188</td>
<td>apple,20,4b,08  (AK)</td>
<td>802.11</td>
<td>40</td>
<td>Acknowledgment, Flags:.......C</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>2</td>
<td>de</td>
<td>3260 58 617290</td>
<td>Samsung,800,4E (CA)</td>
<td>802.11</td>
<td>40</td>
<td>Acknowledgment, Flags:.......C</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>7</td>
<td>7</td>
<td>db</td>
<td>3261 59 332743</td>
<td>Samsung,800,4E (CA)</td>
<td>802.11</td>
<td>40</td>
<td>Acknowledgment, Flags:.......C</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>7</td>
<td>3</td>
<td>db</td>
<td>3261 59 332743</td>
<td>Samsung,800,4E (CA)</td>
<td>802.11</td>
<td>40</td>
<td>Acknowledgment, Flags:.......C</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>10</td>
<td>db</td>
<td>3261 59 332743</td>
<td>Samsung,800,4E (CA)</td>
<td>802.11</td>
<td>40</td>
<td>Acknowledgment, Flags:.......C</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>8</td>
<td>db</td>
<td>3261 59 332743</td>
<td>Samsung,800,4E (CA)</td>
<td>802.11</td>
<td>40</td>
<td>Acknowledgment, Flags:.......C</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>10</td>
<td>db</td>
<td>3261 59 332743</td>
<td>Samsung,800,4E (CA)</td>
<td>802.11</td>
<td>40</td>
<td>Acknowledgment, Flags:.......C</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>8</td>
<td>db</td>
<td>3261 59 332743</td>
<td>Samsung,800,4E (CA)</td>
<td>802.11</td>
<td>40</td>
<td>Acknowledgment, Flags:.......C</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>10</td>
<td>db</td>
<td>3261 59 332743</td>
<td>Samsung,800,4E (CA)</td>
<td>802.11</td>
<td>40</td>
<td>Acknowledgment, Flags:.......C</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>8</td>
<td>db</td>
<td>3261 59 332743</td>
<td>Samsung,800,4E (CA)</td>
<td>802.11</td>
<td>40</td>
<td>Acknowledgment, Flags:.......C</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>10</td>
<td>10</td>
<td>db</td>
<td>3261 59 332743</td>
<td>Samsung,800,4E (CA)</td>
<td>802.11</td>
<td>40</td>
<td>Acknowledgment, Flags:.......C</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The data rates and RSS values are specific to the devices and times indicated. The protocol and length information are standard for 802.11 wireless networks.
Visualizing 802.11 Wireshark Data
Tuesday, July 26th, 2012

Ryan Woodings
Chief Geek | MetaGeek
@metageek