Wireless Network Optimization

Trent Cutler, Jedi Trainer
MetaGeek

- Founded in 2005
- HQ in Boise, Idaho
- Founded & 100% owned by MetaGeek employees
MetaGeek

Wireless Layer 1

- Wi-Spy Hardware
- Chanalyzer Software
- Device Finder
  - 2.4 GHz Directional Antenna
Wired vs. Wireless

802.3 - Wired
- Distributed Access Scheme
- CSMA-CD

802.11 - Wireless
- Distributed Access Scheme
- CSMA-CA

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

2.4 GHz
- Greater Range
- Wi-Fi Congestion
- 802.11b/g/n devices
- 3-Non-Overlapping Channels
- Plagued by Non-Wi-Fi Interference

5 GHz
- Lower Indoor Range
- Largely Unused
- Greater Performance
- Varying Tx Restrictions
- 802.11 a/n/ac
**Types of 802.11 Interference**

- **Co-Channel**: Every station and access point on the same channel cooperate time to talk.

- **Adjacent Channel**: Every station and access point on an overlapping channel talk over each other.

- **Non-Wi-Fi**: Non-802.11 devices also compete for medium access.
Co-Channel And Overlapping Interference

Visible:
- Signal Strength of Access Points
- Visualize Co-Channel & Overlapping Networks

Invisible:
- Which networks hog bandwidth.
- Number of clients.
- Actual data rates used.
- Client Usage
Co-Channel And Overlapping Interference

inSSIDer's Color Scheme

15 Networks in your area share your starred networks channel but the highest signal strength of the nearest is about -75dBm.

3 Networks use non-standard channels and overlap your starred network with a signal strength of -80dBm.

Your Link Score represents your signal strength compared to the competing networks on your channel. The highest possible score is 100.
Visualizing Channel Density

INTEROP 2013

2.4 GHz

5 GHz
Visualizing Wi-Fi Patterns

Phase Shift Keying Modulation

Legacy 802.11b Data Rates
- 1, 2, 5.5 or 11Mbps
- 2.4 GHz Only

When the minimum supported rate is 1, 2, 5.5, or 11 Mbps all 802.11 Overhead is sent at this PHY type.

OFDM (20 MHz)

802.11a/g/n
- 6-216.7 Mbps
- 2.4 or 5 GHz

Most commonly used to transmit Data Frames and all frames in modern Wi-Fi networks.

OFDM (40 MHz)

802.11n
- 13.5 - 600 Mbps
- 2.4 or 5 GHz

Most commonly used to transmit Data Frames.
Spectrum Pattern Diagnosis

INTEROP 2013

2.4 GHz
(Very Dense)

5 GHz
(Less Dense - Unused Channels)

All Wi-Fi overhead is sent at a legacy data rate.

Minimum data rate is 6 Mbps.
Legacy Data Rates - So What?

Wi-Fi stations are very polite.

They will back off for any transmission above -85dBm.

Lower data rates take more airtime and prevent other devices from transmitting.

Percent of activity above -85dBm at INTEROP 2013
Overhead Required for Legacy Devices

Every 802.11 frame includes a PLCP header (not reported in Packet Analysis).

This is used for synchronization and collision avoidance.

The PHY header is always sent at the most robust (or lowest) data rate even if the 802.11 frame is sent at a much faster data rate.
ERP Protection

### IEEE 802.11 wireless LAN management frame

- **Fixed parameters (12 bytes)**
- **Tagged parameters (223 bytes)**
  - **Tag:** SSID parameter set: NETGEAR52
  - **Tag:** Supported Rates 1(B), 2(B), 5.5, 11, 18, 24, 36, 54, [Mbit/sec]
  - **Tag:** DS Parameter set: Current Channel: 11
  - **Tag:** Traffic Indication Map (TIM): DTIM 1 of 0 bitmap
  - **Tag:** ERP Information
    - **Tag Number:** ERP Information (42)
    - **Tag length:** 1
    - **ERP Information:** 0x02
      - .......0 = Non ERP Present: Not set
      - .......1 = Use Protection: Set
      - .......0.. = Barker Preamble Mode: Not set
      - 0000 0... = Reserved: 0x00

### Table

<table>
<thead>
<tr>
<th>Subframe T</th>
<th>Air Time</th>
<th>Bytes</th>
<th>Packets</th>
<th>Retry Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS Data</td>
<td>18.338.40</td>
<td>19,053,944</td>
<td>25,836</td>
<td>39</td>
</tr>
<tr>
<td>RTS</td>
<td>2.388.45</td>
<td>150,820</td>
<td>7,541</td>
<td>0</td>
</tr>
<tr>
<td>ACK</td>
<td>1.237.91</td>
<td>121,562</td>
<td>8,683</td>
<td>0</td>
</tr>
<tr>
<td>Block ACK</td>
<td>66.42</td>
<td>97,088</td>
<td>3,034</td>
<td>0</td>
</tr>
<tr>
<td>CTS</td>
<td>751.70</td>
<td>53,340</td>
<td>3,810</td>
<td>0</td>
</tr>
<tr>
<td>QoS Null</td>
<td>31.81</td>
<td>2,130</td>
<td>71</td>
<td>34</td>
</tr>
<tr>
<td>Probe Resp</td>
<td>10.01</td>
<td>2,034</td>
<td>9</td>
<td>44</td>
</tr>
<tr>
<td>Probe Requ</td>
<td>16.13</td>
<td>1,652</td>
<td>14</td>
<td>0</td>
</tr>
<tr>
<td>Action</td>
<td>0.52</td>
<td>39</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
Arbitration and RTS / CTS

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

Station 2
- NAV
- RTS
- DATA
- Station Defers
- NAV

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

Station 4
- NAV
- Station sets NAV upon receiving RTS
- DATA
- Station sets NAV upon receiving RTS

Station 5
- SIFS
- ACK

Station 6
- DATA
- Station sets NAV upon receiving RTS
- Station sets NAV upon receiving CTS, this station is hidden to Station 1
How to Find Legacy Devices

Look in the Probe Requests!

wlan.fc.type_subtype == 0x04

Learn all about what the client device supports: data rates, RF bands, beamforming and security.
Co-Channel Interference and 802.11 overhead are excluded when troubleshooting wireless issues over the wire.

802.11 Overhead is all Management and Control Frames.
What Comes Through the Wire

INTEROP 2013 SSID "NOC"
Add the 802.11 Overhead for BSSID

INTEROP 2013 SSID "NOC"
Add the Competing Traffic on Channel 11

INTEROP 2013 SSID "NOC"
Even though stations within "NOC" easily sent the most bytes, they only contributed to a small portion of the Air Time saturation.

What is all of the other traffic?
802.11 Air Time of Legacy Data Rates

INTEROP 2013 Channel 11

1 Mbps

>= 6 Mbps
What are all of the 1 Mbps frames?

Probe Requests and Responses

Apple device express interest in Wi-Fi Connection (Probe Request)

Access Points responding to probe request at 1 Mbps.
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
802.11ac

- 5 GHz
- 20-160 MHz Wide
- 6 Mbps - 6.9 Gbps
- OFDM Modulation
Dynamic Rate Switching

As clients are further away from an Access point they choose a lower modulation rate.
Reduce Co-Channel Interference

Channel
Antenna Pattern
Physical Barriers
Transmit Power
Measuring Retransmissions

\[(\text{wlan.fc.type} == 2) && (\text{wlan.fc.retry} == 1)\]
How do I know what 5 GHz channels my client device supports?

Look in the Association Requests!

wlan.fc.type_subtype == 0x00
Roaming Analysis

- Roaming may happen across multiple channels. Multiple capture interfaces is recommended.
- If you don't have multiple devices monitor the AP you think it will roam to next.

Use a Quick Filter!

Use a Quick Filter!

Modify the Filter to Follow a Specific Station

```c
((!(wlan.fc.type == 1)) && !(wlan.fc.type == 2)) && !(wlan.fc.type_subtype == 0x08) && !(wlan.fc.subtype == 13)) && !(wlan.fcs_good == 0)

(((!(wlan.fc.type == 1)) && !(wlan.fc.type == 2)) && !(wlan.fc.type_subtype == 0x08) && !(wlan.fc.subtype == 13)) && !(wlan.fcs_good == 0)

((!(wlan.fc.type == 1)) && !(wlan.fc.type == 2)) && !(wlan.fc.type_subtype == 0x08) && !(wlan.fc.subtype == 13)) && !(wlan.fcs_good == 0) &&

(wlan.sa == STATIONMAC || wlan.da == STATIONMAC ))
```
Profile Considerations for 802.11 Analysis

Live Demo
Trial software available for learning:

www.metageek.com
Trent Cutler

YouTube: /user/trentcutler
Twitter: @metageek, @firemywires