WiFi in the real world

Tim Moors
23/March/2015
Channels and bands

Australian radiofrequency spectrum allocations

WiFi 2.4GHz channels:

"2.4 GHz Wi-Fi channels (802.11b,g WLAN)" by Michael Gauthier, Wireless Networking in the Developing World
WiFi architecture

Basic Service Set (BSS) & BSS ID

Extended Service Set (ESS) & SSID

Distribution System (DS)

Internet
WiFi frame format

Figure 8-1—MAC frame format

Figure 8-2—Frame Control field

Figure 8-3—Sequence Control field

Figures from 802.11-2012
## Funky WiFi addressing

DA = Destination Address, SA = Source Address
Address1 = Receiver (RA), Address2 = Transmitter (TA)

<table>
<thead>
<tr>
<th>DS activity</th>
<th>Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>to</td>
<td>from</td>
</tr>
<tr>
<td>×</td>
<td>×</td>
</tr>
<tr>
<td>√</td>
<td>×</td>
</tr>
<tr>
<td>×</td>
<td>√</td>
</tr>
<tr>
<td>√</td>
<td>√</td>
</tr>
</tbody>
</table>

Control/Management frames follow data frame ordering as if neither to nor from DS.
Control frames

- RTS/CTS
- ACK, Block ACK
Management frames

• Discovery: **Beacons, Probe** (request/response)
• Engagement:
  – *(de)Authentication* (may be multi-stage)
    • Data frame support: 802.1x Authentication
  – **Association** (request/response)

• Others (not in capture file)
  – Disassociation
  – Reassociation
  – generic Action subtype → a whole lot more!