Visualizing 802.11 Wireshark Data

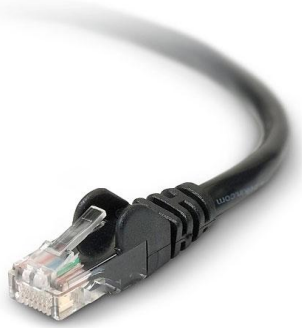
Tuesday, July 26th, 2012

Ryan Woodings

Chief Geek | MetaGeek

@metageek

Wired vs Wireless



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

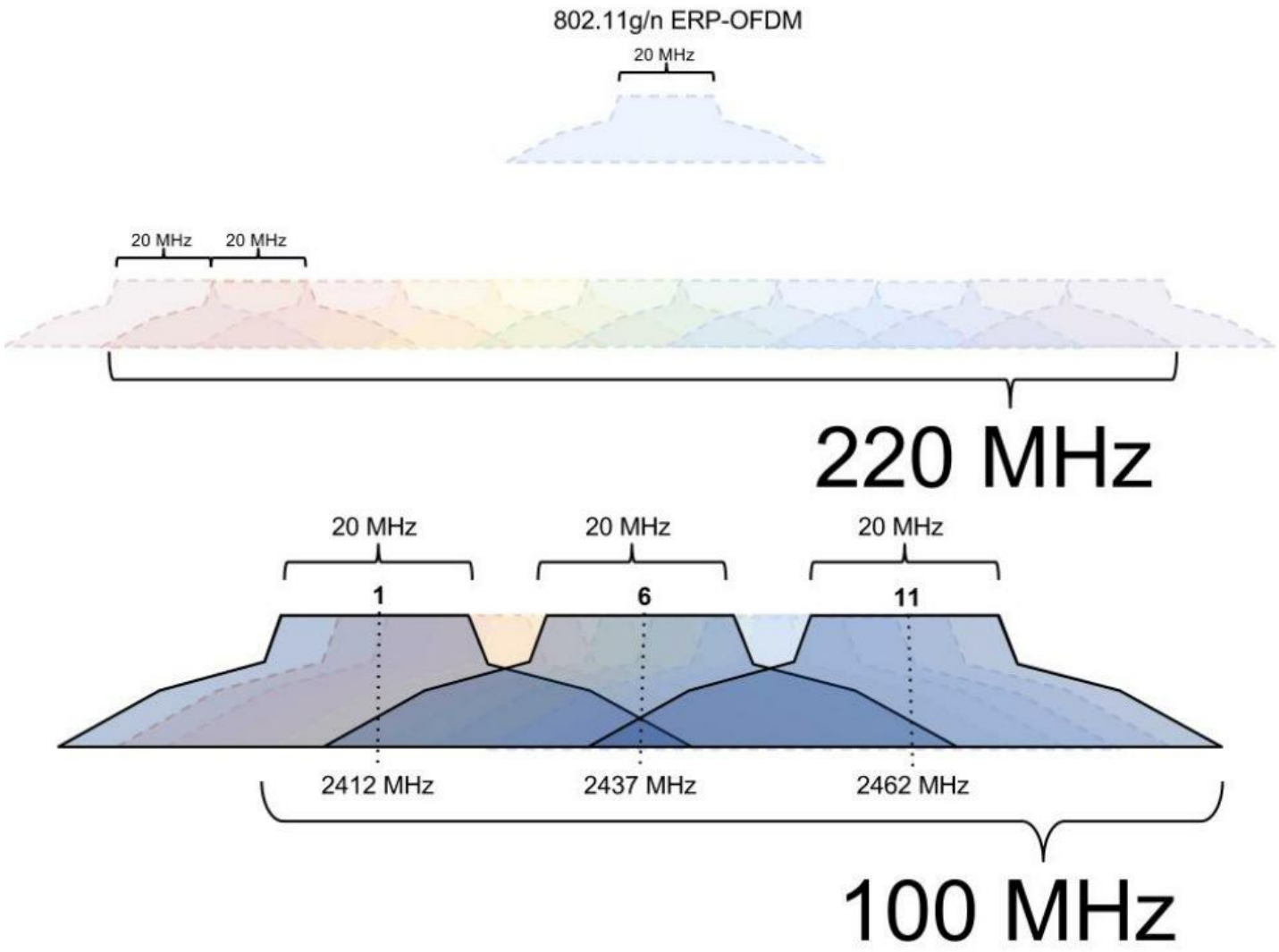
5 GHz

- 9 non-DFS (US)
- 12 DFS (US)
- 4 non-DFS (Europe)
- 15 DFS (Europe)

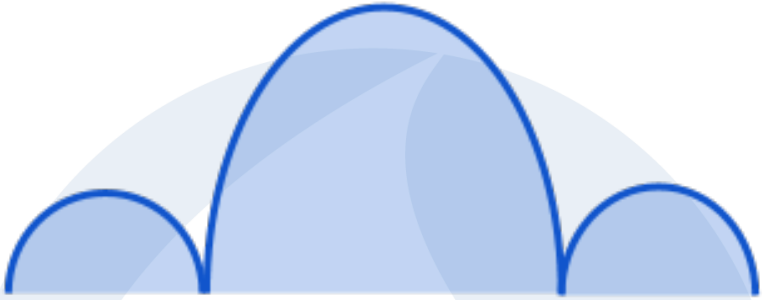
Detailed List

http://en.wikipedia.org/wiki/List_of_WLAN_channels

Channel Overlap



Physical Layer Modulation



CCK (HR-DSSS Phase Shift Keying)

OFDM (Orthogonal Frequency Division Multiplexing)

Channel Contention

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.

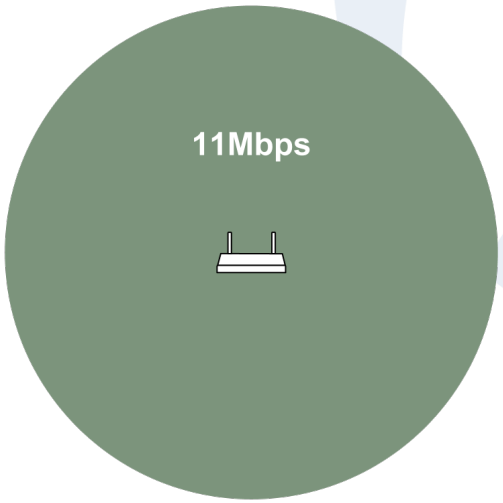
Non-Wi-Fi: non-802.11 devices also compete for medium access.

Physical Layer Modulation

Live Demo

802.11b

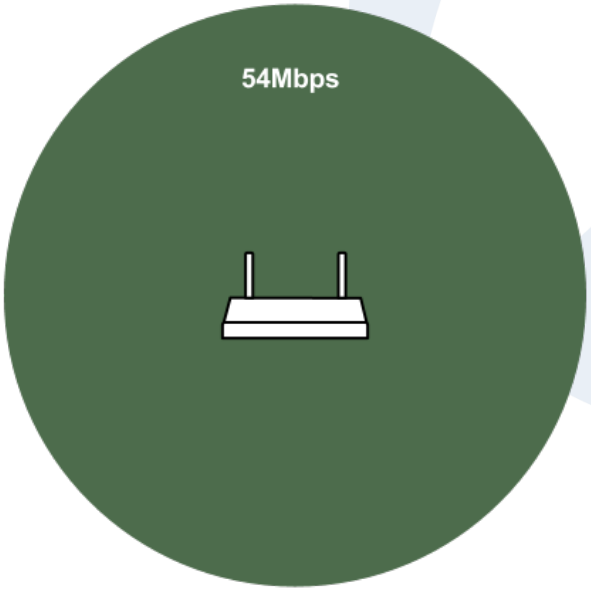
- 2.4 GHz-only
- 22 MHz Wide
- 1-11 Mbps
- HR-DSSS BPSK w/ CCK Modulation
- Good for longer range but low data rate.




```
⊞ Frame 19665: 185 bytes on wire (1480 bits), 185 bytes captured (1480 bits)
⊟ Radiotap Header v0, Length 26
    Header revision: 0
    Header pad: 0
    Header length: 26
  ⊞ Present flags: 0x0000186f
    MAC timestamp: 354203615
  ⊞ Flags: 0x10
    Data Rate: 1.0 Mb/s
    Channel frequency: 2412 [BG 1]
  ⊟ Channel type: 802.11b (0x00a0)
      .... .... ...0 .... = Turbo: False
      .... .... ..1. .... = Complementary Code Keying (CCK): True
      .... .... .0.. .... = Orthogonal Frequency-Division Multiplexing (OFDM): F
      .... .... 1... .... = 2 GHz spectrum: True
      .... ...0 .... .... = 5 GHz spectrum: False
      .... ..0. .... .... = Passive: False
      .... .0.. .... .... = Dynamic CCK-OFDM: False
      .... 0... .... .... = Gaussian Frequency Shift Keying (GFSK): False
      ...0 .... .... .... = GSM (900MHz): False
      ..0. .... .... .... = Static Turbo: False
      .0.. .... .... .... = Half Rate Channel (10MHz Channel Width): False
      0... .... .... .... = Quarter Rate Channel (5MHz Channel Width): False
```

802.11a

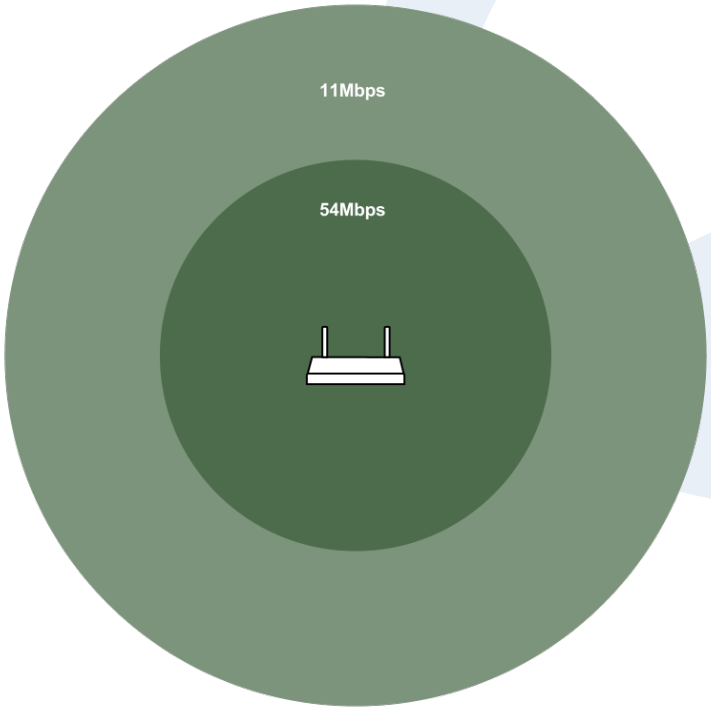
- 5 GHz-only
- 20 MHz Wide
- 6-54 Mbps
- OFDM Modulation




```
⊟ Radiotap Header v0, Length 26
    Header revision: 0
    Header pad: 0
    Header length: 26
  ⊞ Present flags: 0x0000186f
    MAC timestamp: 35002796143208
  ⊞ Flags: 0x10
    Data Rate: 52.0 Mb/s
    Channel frequency: 5745 [A 149]
  ⊞ Channel type: 802.11a (0x0140)
    SSI Signal: -68 dBm
    SSI Noise: -85 dBm
    Antenna: 0
    SSI Signal: 17 dB
```

802.11g

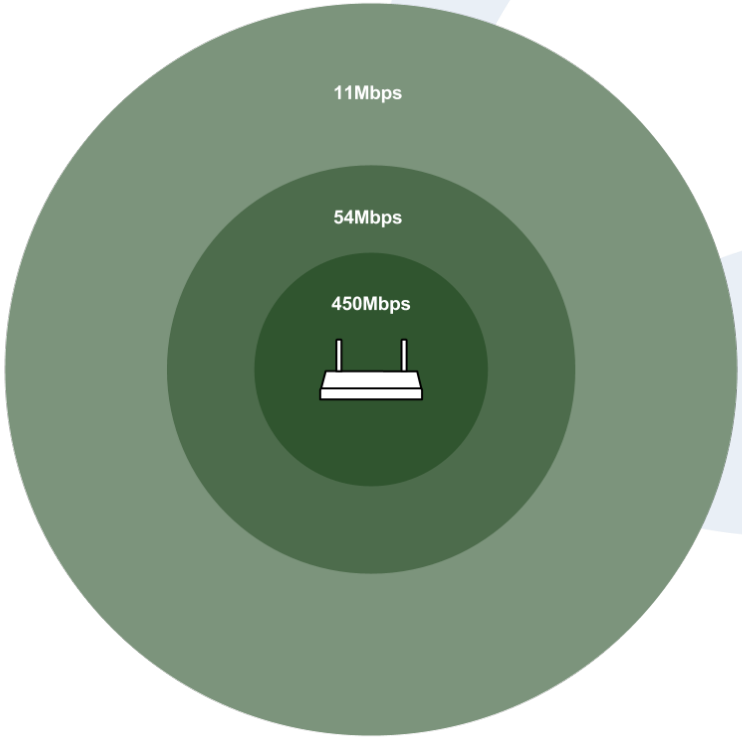
- 2.4 GHz-only
- 20 MHz Wide
- 6-54Mbps
- ERP-OFDM Modulation




```
Radiotap Header v0, Length 26
    Header revision: 0
    Header pad: 0
    Header length: 26
  + Present flags: 0x0000186f
    MAC timestamp: 266566899
  + Flags: 0x10
    Data Rate: 52.0 Mb/s
    Channel frequency: 2412 [BG 1]
  - Channel type: 802.11g (pure-g) (0x00c0)
      .... .... ...0 .... = Turbo: False
      .... .... ..0. .... = Complementary Code Keying (CCK): False
      .... .... .1.. .... = Orthogonal Frequency-Division Multiplexing (OFDM): Tr
      .... .... 1... .... = 2 GHz spectrum: True
      .... ...0 .... .... = 5 GHz spectrum: False
      .... ..0. .... .... = Passive: False
      .... .0.. .... .... = Dynamic CCK-OFDM: False
      .... 0... .... .... = Gaussian Frequency Shift Keying (GFSK): False
      ...0 .... .... .... = GSM (900MHz): False
      ..0. .... .... .... = Static Turbo: False
      .0.. .... .... .... = Half Rate Channel (10MHz Channel Width): False
      0... .... .... .... = Quarter Rate Channel (5MHz Channel Width): False
    SSI Signal: -47 dBm
    SSI Noise: -70 dBm
    Antenna: 0
    SSI Signal: 23 dB
```

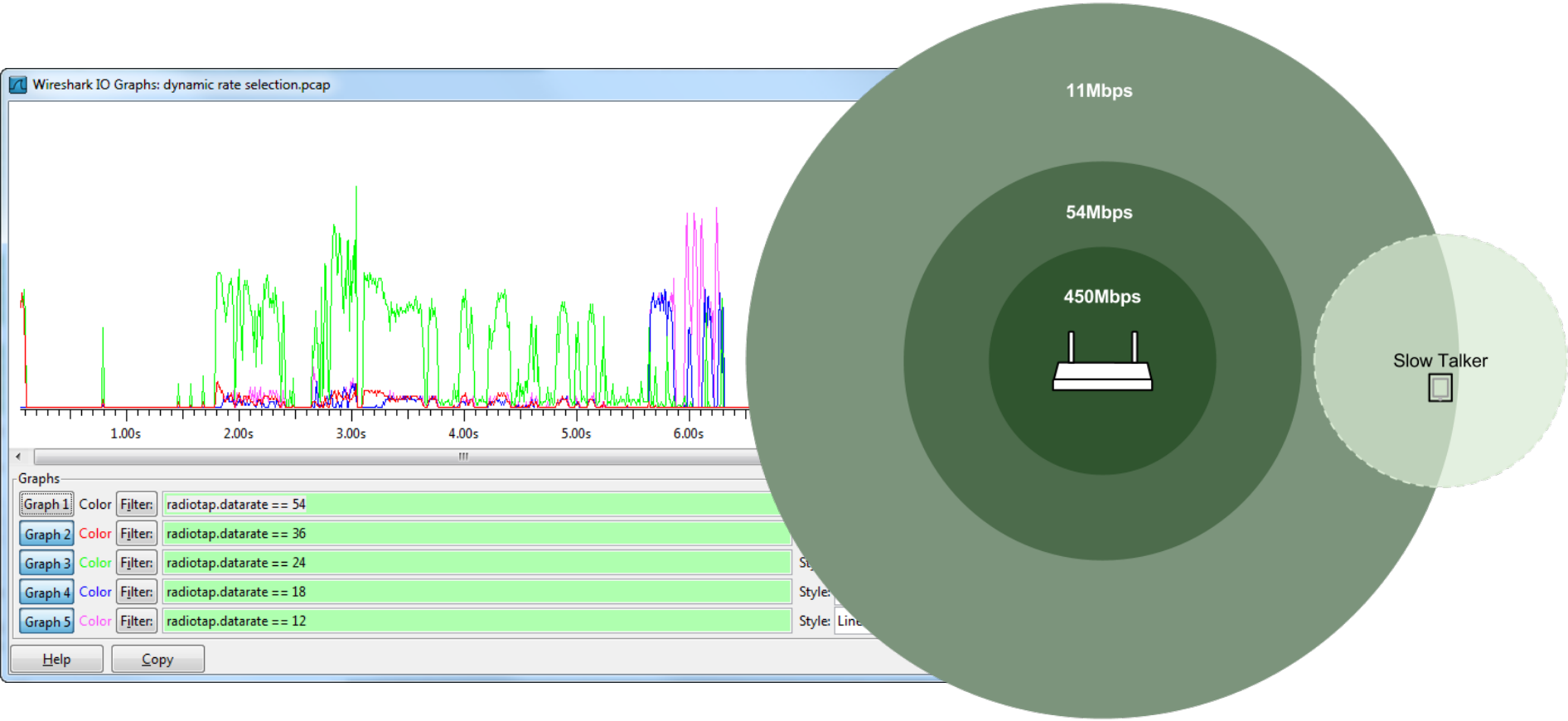
802.11n

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

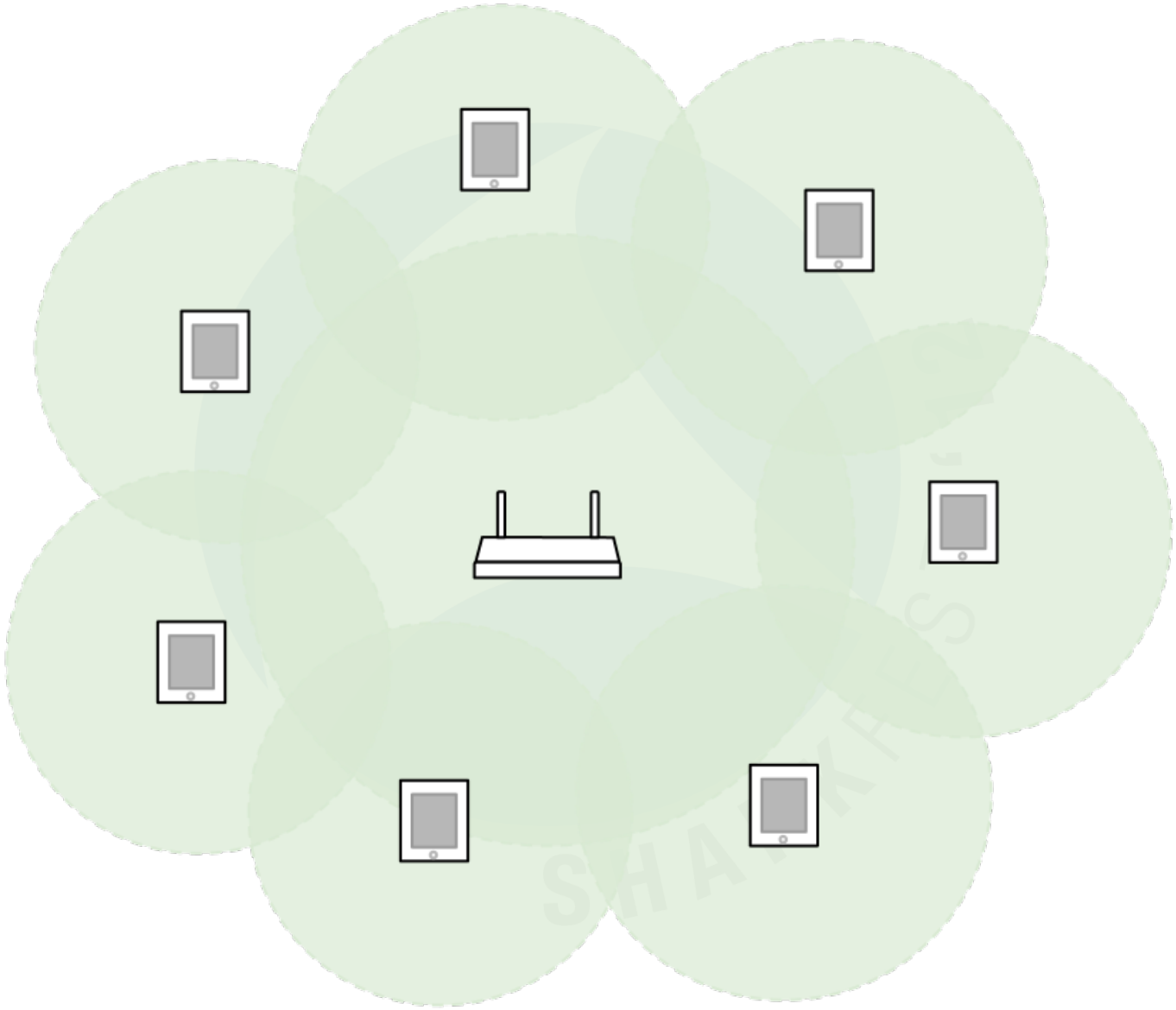


Dynamic Rate Selection

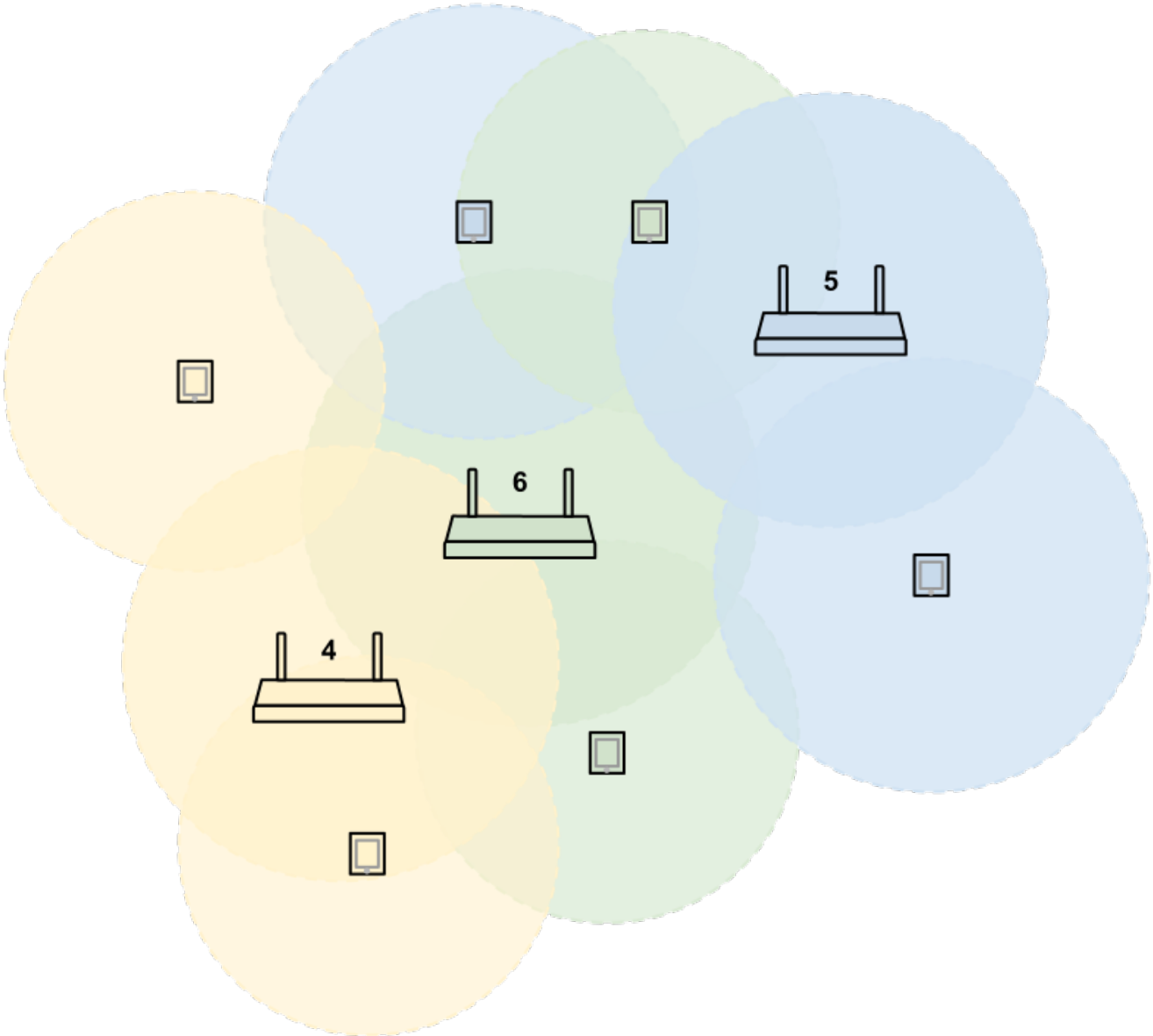
As clients are further away from an Access point they choose a lower modulation rate.



Channel Contention



Channel Contention



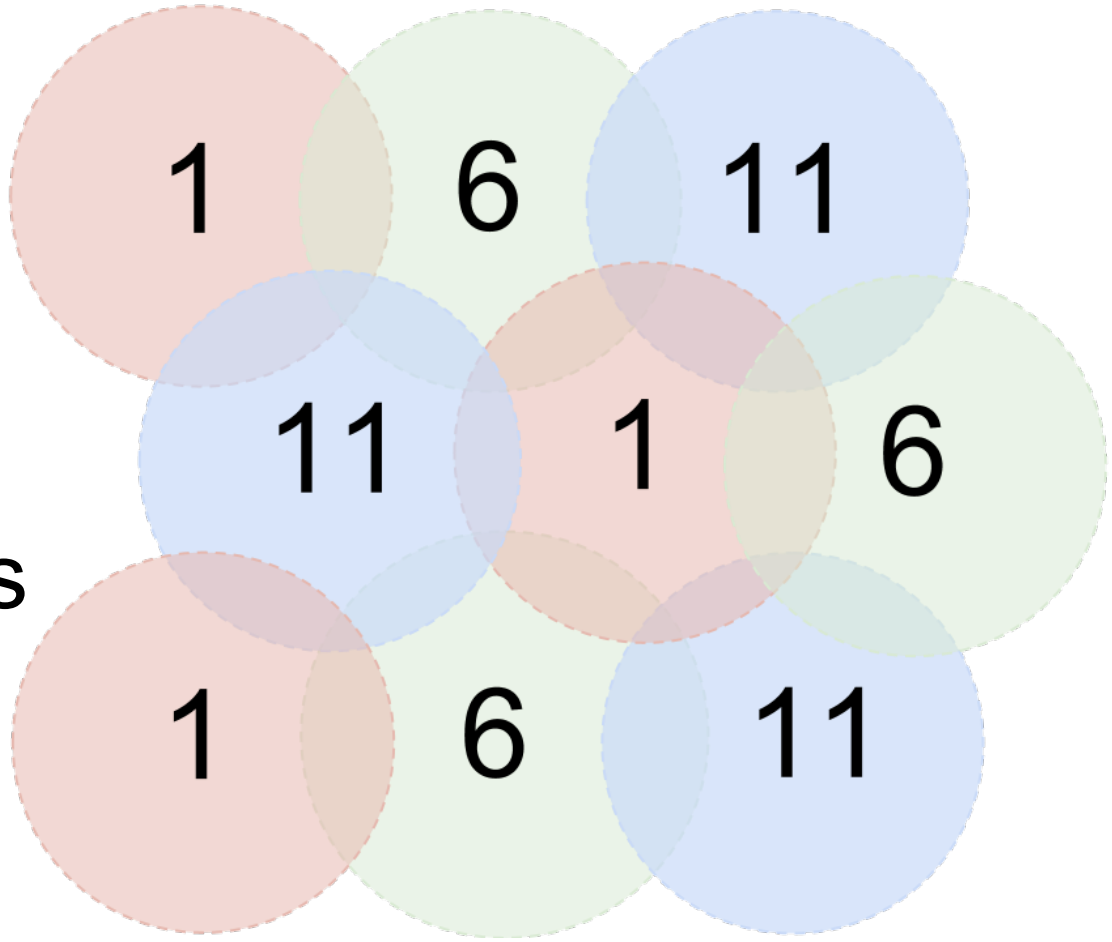
Contention Domains

Channel

Antenna Pattern

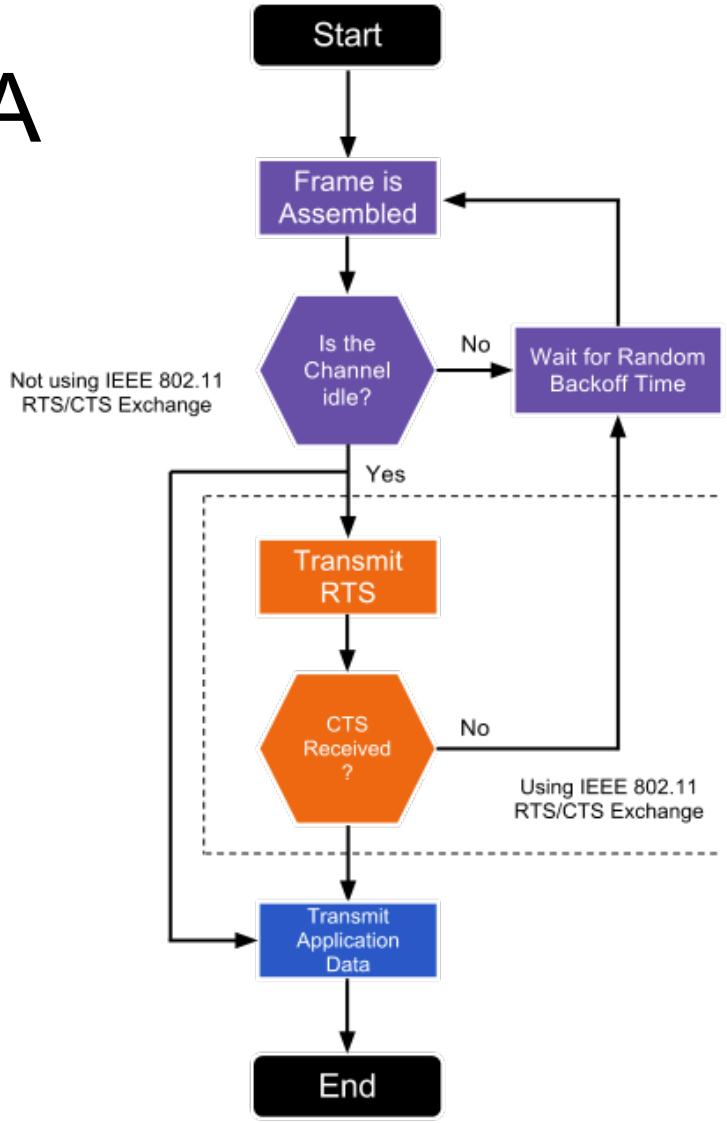
Physical Barriers

Transmit Power

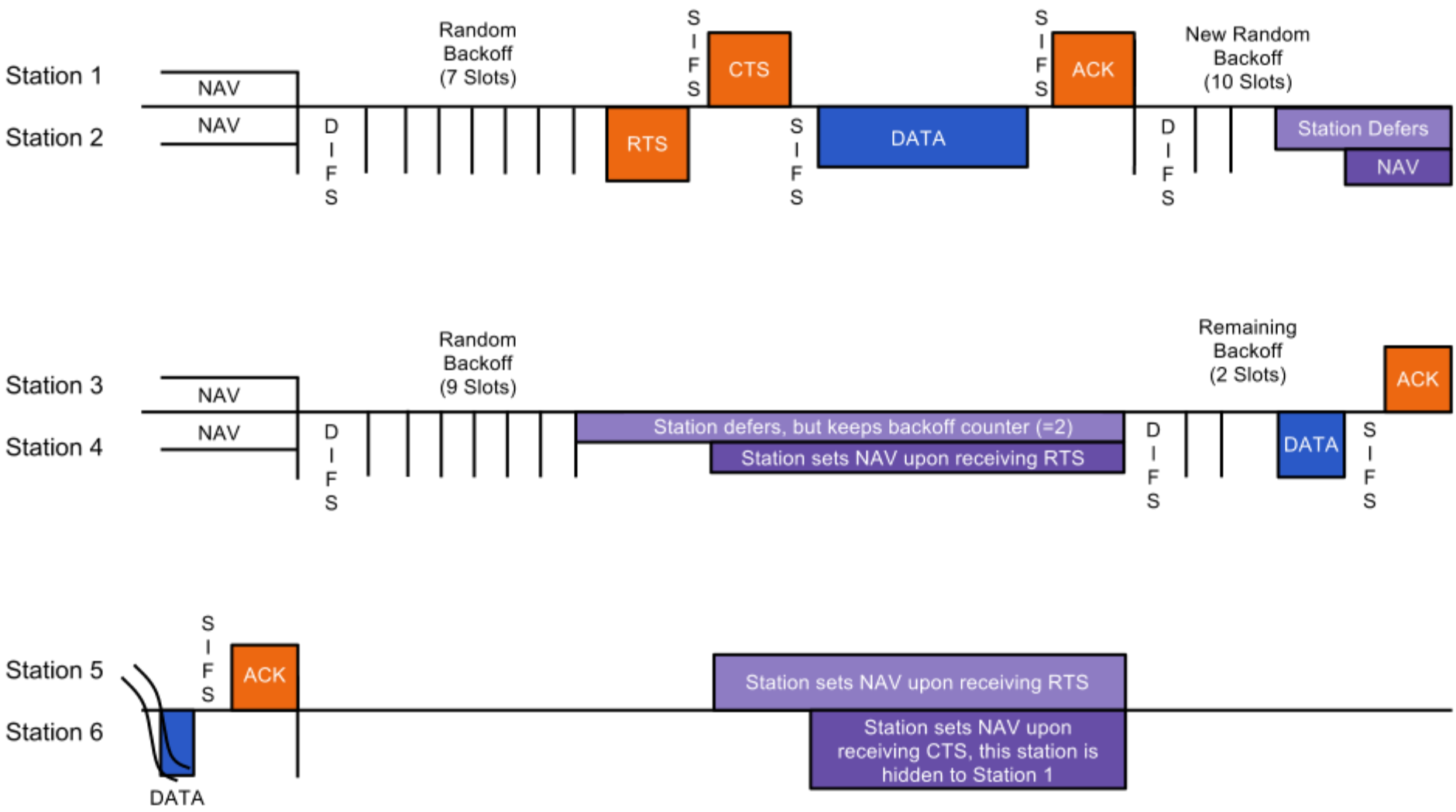


Wireless Medium Access

CSMA w/ CA



Wireless Medium Access



802.11 Frame Types

Management Frames

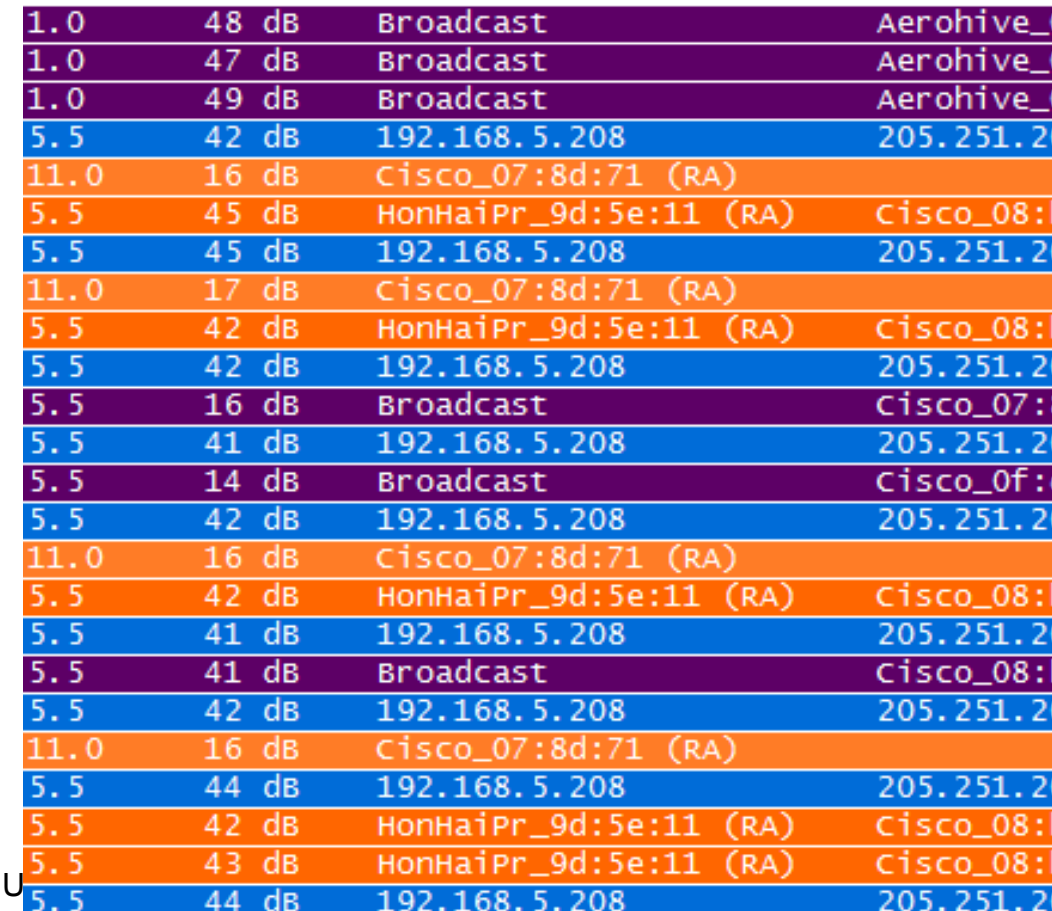
wlan.fc.type == 0

Control

wlan.fc.type == 1

Data

wlan.fc.type == 2



Management Frames

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

SubType	Data Rate	RSSI	Destination	Source
Probe Response	1.0	25 dB	SenaoInt_8d:29:2e	Aerohiv
Probe Response	1.0	25 dB	SenaoInt_8d:29:2e	Aerohiv
Probe Response	1.0	25 dB	SenaoInt_8d:29:2e	Aerohiv
Probe Response	1.0	26 dB	SenaoInt_8d:29:2e	Aerohiv
Probe Response	1.0	26 dB	SenaoInt_8d:29:2e	Aerohiv
Disassociate	1.0	58 dB	Aerohive_25:c2:50	SenaoIn
Deauthentication	1.0	56 dB	Aerohive_25:c2:50	SenaoIn
Deauthentication	1.0	59 dB	Aerohive_25:c2:50	SenaoIn
Probe Request	1.0	54 dB	Aerohive_25:c2:50	SenaoIn
Probe Request	1.0	58 dB	Aerohive_25:c2:50	SenaoIn
Probe Response	1.0	24 dB	SenaoInt_8d:29:2e	Aerohiv
Authentication	1.0	56 dB	Aerohive_25:c2:50	SenaoIn
Authentication	1.0	58 dB	Aerohive_25:c2:50	SenaoIn
Authentication	1.0	24 dB	SenaoInt_8d:29:2e	Aerohiv
Association Reque	1.0	57 dB	Aerohive_25:c2:50	SenaoIn
Association Reque	1.0	59 dB	Aerohive_25:c2:50	SenaoIn
Association Respo	1.0	24 dB	SenaoInt_8d:29:2e	Aerohiv
Disassociate	1.0	22 dB	SenaoInt_8d:29:2e	Aerohiv
Deauthentication	1.0	22 dB	SenaoInt_8d:29:2e	Aerohiv
Probe Response	1.0	20 dB	SenaoInt_8d:29:2e	Aerohiv
Probe Response	1.0	21 dB	SenaoInt_8d:29:2e	Aerohiv
Probe Response	1.0	21 dB	SenaoInt_8d:29:2e	Aerohiv
Probe Response	1.0	20 dB	SenaoInt_8d:29:2e	Aerohiv
Probe Response	1.0	22 dB	SenaoInt_8d:29:2e	Aerohiv
Probe Response	1.0	22 dB	SenaoInt_8d:29:2e	Aerohiv
Probe Request	1.0	60 dB	Aerohive_25:c2:50	SenaoIn
Probe Request	1.0	54 dB	Aerohive_25:c2:50	SenaoIn
Probe Response	1.0	24 dB	SenaoInt_8d:29:2e	Aerohiv

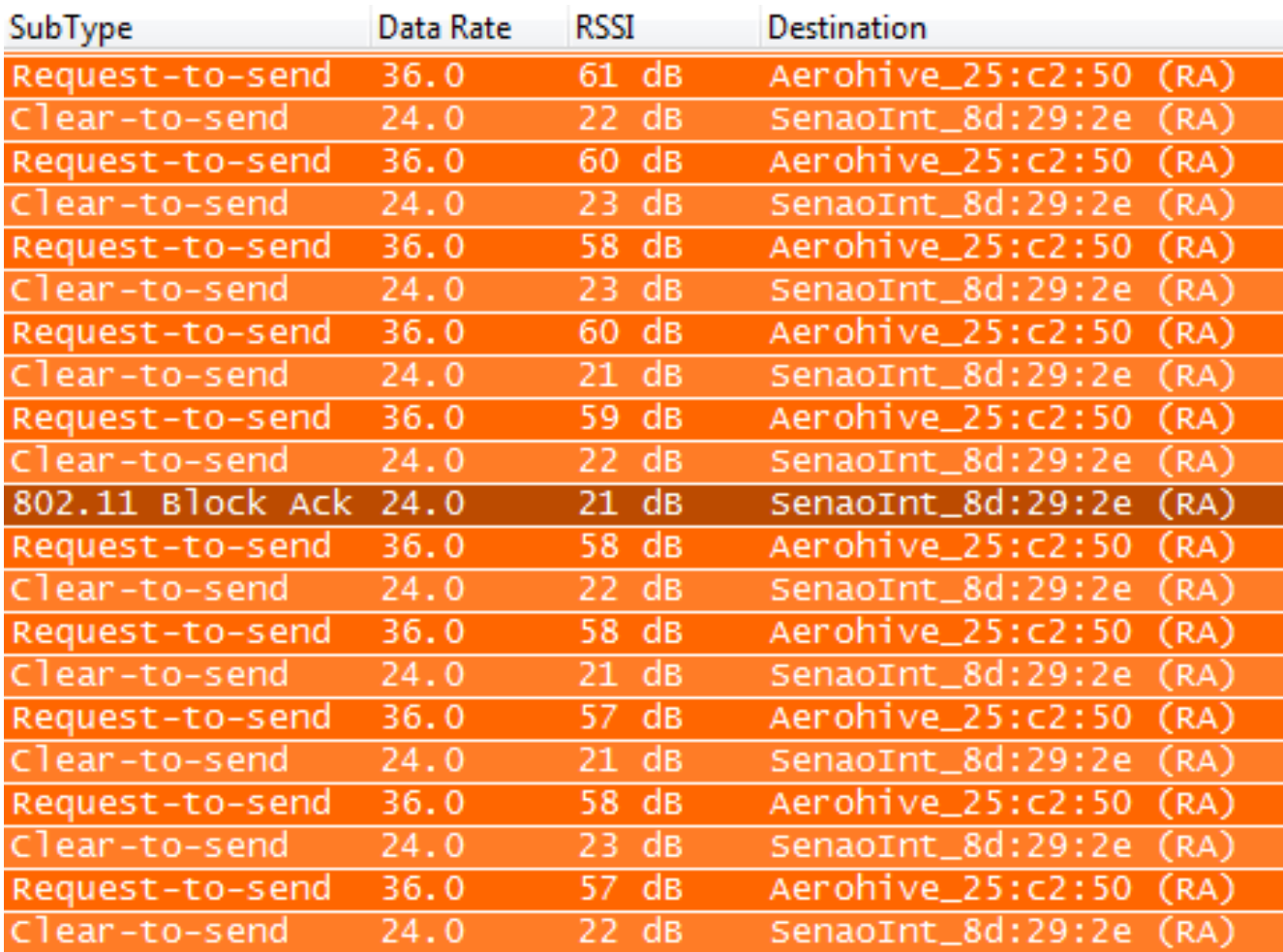
Control Frames

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



SubType	Data Rate	RSSI	Destination
Request-to-send	36.0	61 dB	Aerohive_25:c2:50 (RA)
Clear-to-send	24.0	22 dB	SenaoInt_8d:29:2e (RA)
Request-to-send	36.0	60 dB	Aerohive_25:c2:50 (RA)
Clear-to-send	24.0	23 dB	SenaoInt_8d:29:2e (RA)
Request-to-send	36.0	58 dB	Aerohive_25:c2:50 (RA)
Clear-to-send	24.0	23 dB	SenaoInt_8d:29:2e (RA)
Request-to-send	36.0	60 dB	Aerohive_25:c2:50 (RA)
Clear-to-send	24.0	21 dB	SenaoInt_8d:29:2e (RA)
Request-to-send	36.0	59 dB	Aerohive_25:c2:50 (RA)
Clear-to-send	24.0	22 dB	SenaoInt_8d:29:2e (RA)
802.11 Block Ack	24.0	21 dB	SenaoInt_8d:29:2e (RA)
Request-to-send	36.0	58 dB	Aerohive_25:c2:50 (RA)
Clear-to-send	24.0	22 dB	SenaoInt_8d:29:2e (RA)
Request-to-send	36.0	58 dB	Aerohive_25:c2:50 (RA)
Clear-to-send	24.0	21 dB	SenaoInt_8d:29:2e (RA)
Request-to-send	36.0	57 dB	Aerohive_25:c2:50 (RA)
Clear-to-send	24.0	21 dB	SenaoInt_8d:29:2e (RA)
Request-to-send	36.0	58 dB	Aerohive_25:c2:50 (RA)
Clear-to-send	24.0	23 dB	SenaoInt_8d:29:2e (RA)
Request-to-send	36.0	57 dB	Aerohive_25:c2:50 (RA)
Clear-to-send	24.0	22 dB	SenaoInt_8d:29:2e (RA)

Data Frames

Data Frames carry higher-level protocol data

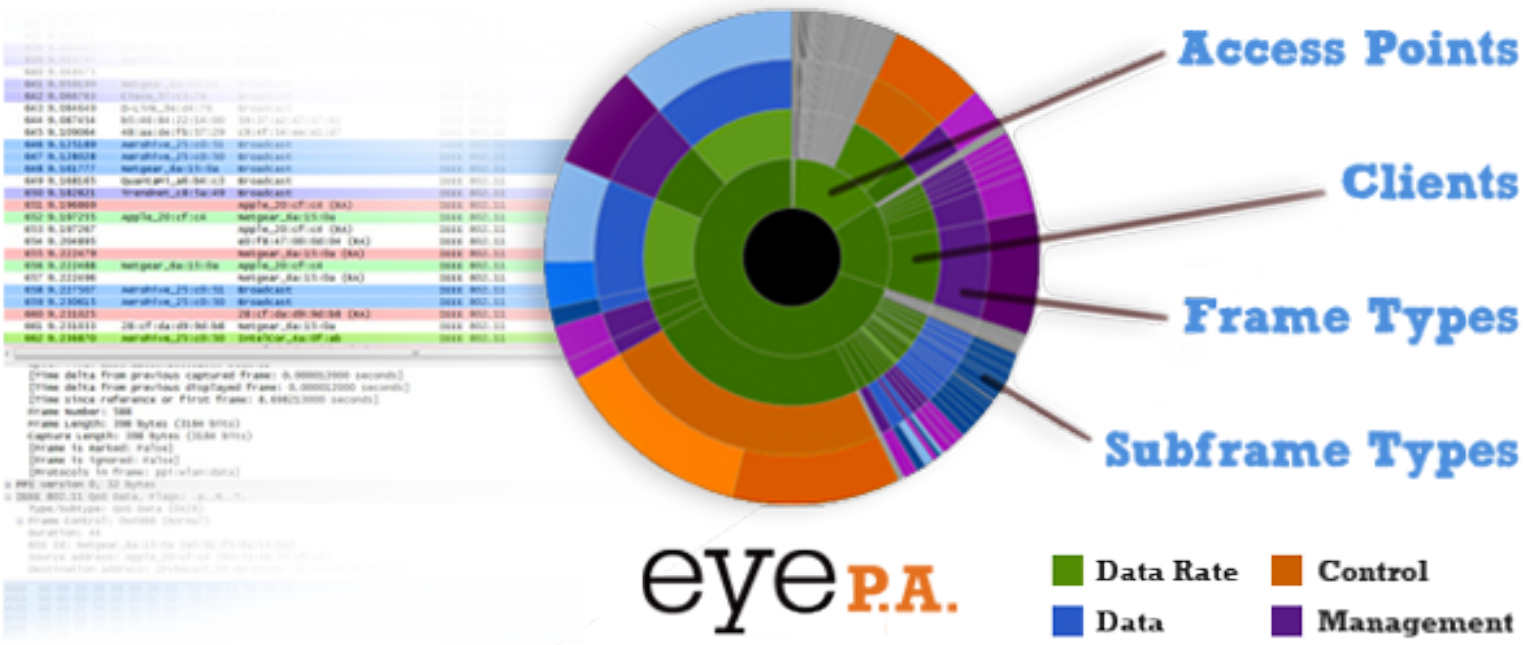
For Example,

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

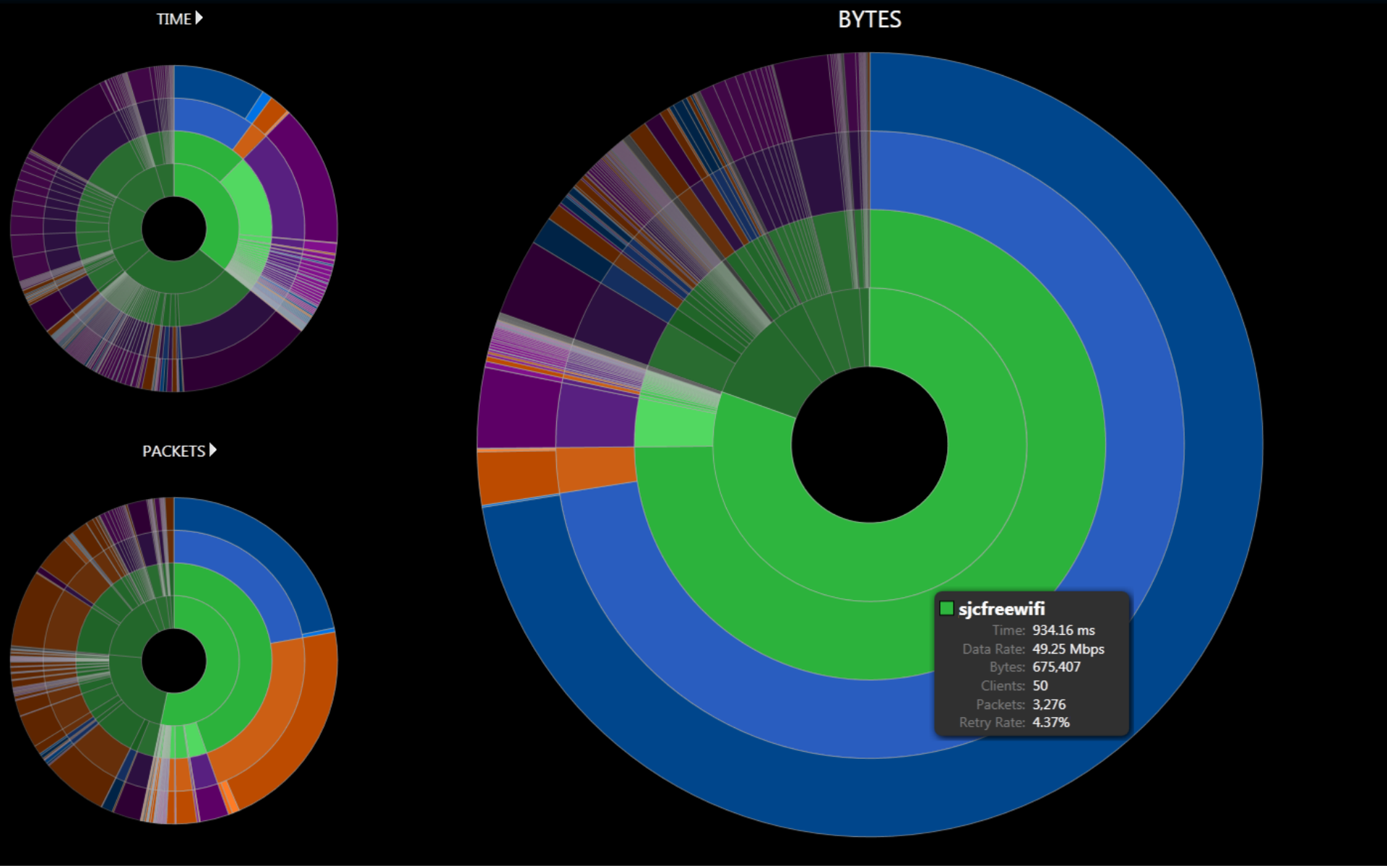
SubType	Data Rate	RSSI	Destination
Data	1.0	24 dB	Broadcast
Null function (No	6.5	24 dB	Aerohive_25:c2:
Data	1.0	26 dB	Broadcast
QoS Data	6.5	24 dB	IPv4mcast_00:00
QoS Data	52.0	23 dB	Apple_0b:93:2a
Null function (No	6.5	24 dB	Aerohive_25:c2:
Null function (No	6.5	24 dB	Aerohive_25:c2:
Null function (No	6.5	24 dB	Aerohive_25:c2:
QoS Data	6.5	23 dB	IPv6mcast_00:00
QoS Data	6.5	24 dB	IPv6mcast_00:00
QoS Data	6.5	23 dB	e8:b7:48:3b:8b:
QoS Data	6.5	24 dB	e8:b7:48:3b:8b:
QoS Data	6.5	24 dB	e8:b7:48:3b:8b:
QoS Data	1.0	26 dB	e8:b7:48:3b:8b:
QoS Data	6.5	24 dB	e8:b7:48:3b:8b:
Data	1.0	25 dB	IPv4mcast_00:00
Data	1.0	24 dB	IPv6mcast_00:00
Data	1.0	25 dB	Broadcast
QoS Data	39.0	23 dB	Apple_0b:93:2a
QoS Data	39.0	24 dB	Apple_0b:93:2a

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.

WireShark Config Profiles

Additional Columns to Consider:

SubType
wlan.fc.type_subtype

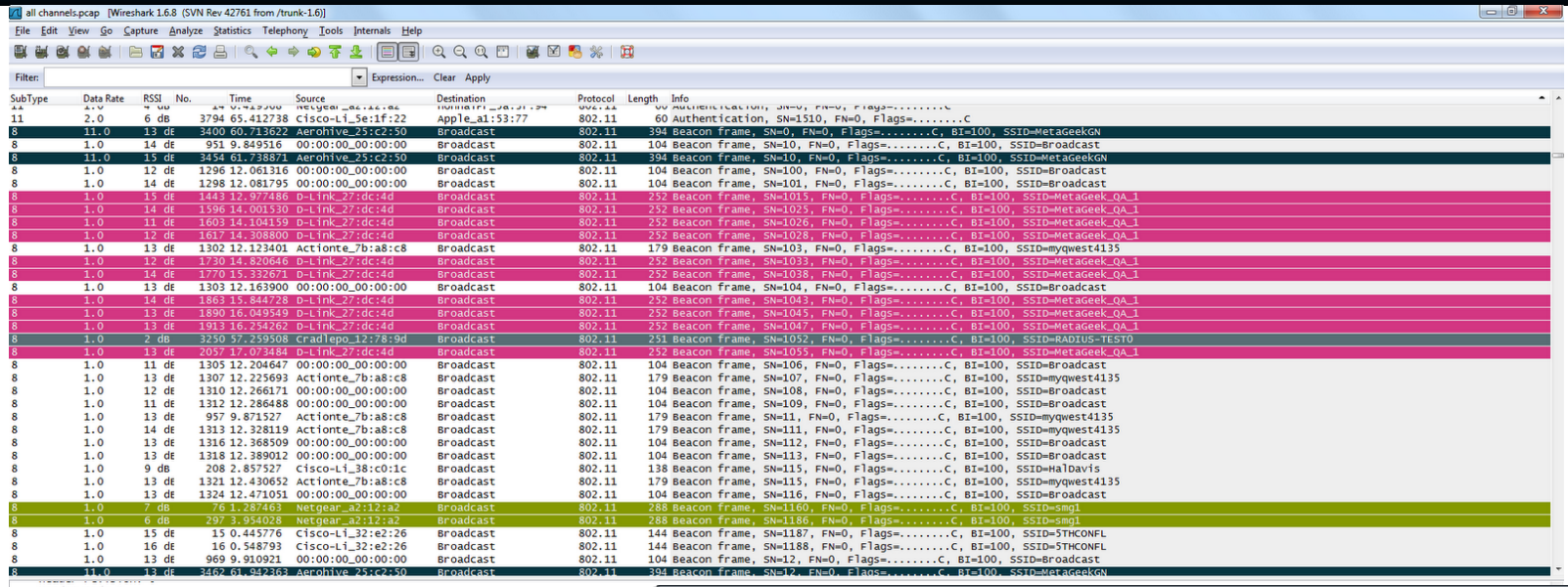
Data Rate
IEEE 802.11 TX rate (existing field type)

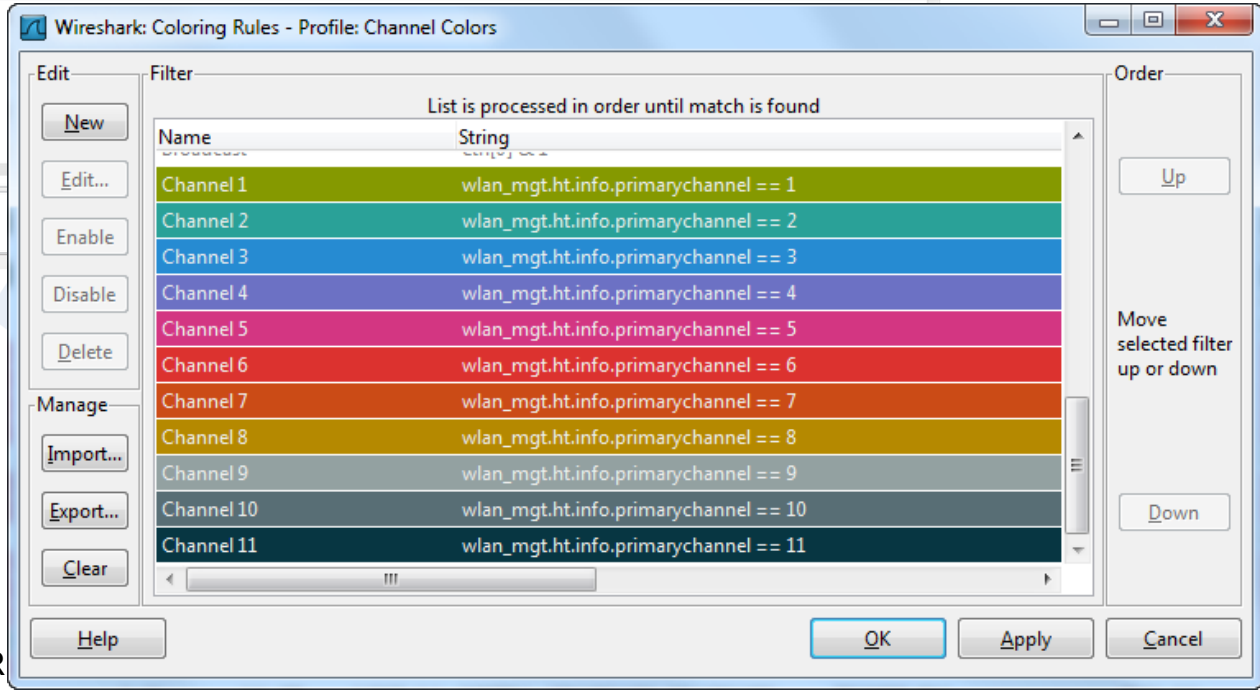
RSSI
IEEE 802.11 RSSI (existing field type)

Packet Type Profile

SubType	Data Rate	RSSI	Destination	Source	Protocol	To/From DS
Beacon frame	11.0	20 dB	Broadcast	Cisco_7d:de:da	IEEE 802.11	Not leaving DS or
QoS Data	1.0	17 dB	e8:b7:48:3b:8b:f2	MurataMa_5c:1f:7a	IEEE 802.11	Frame from STA to
Acknowledgement	1.0	22 dB	MurataMa_5c:1f:7a (RA)		IEEE 802.11	Not leaving DS or
Beacon frame	1.0	22 dB	Broadcast	Aerohive_25:c2:50	IEEE 802.11	Not leaving DS or
Beacon frame	11.0	20 dB	Broadcast	Cisco_7d:de:db	IEEE 802.11	Not leaving DS or
QoS Data	1.0	21 dB	MurataMa_5c:1f:7a	e8:b7:48:3b:8b:f2	IEEE 802.11	Frame from DS to a
Acknowledgement	1.0	17 dB	Aerohive_25:c2:50 (RA)		IEEE 802.11	Not leaving DS or
QoS Data	1.0	23 dB	MurataMa_5c:1f:7a	e8:b7:48:3b:8b:f2	IEEE 802.11	Frame from DS to a
Acknowledgement	1.0	16 dB	Aerohive_25:c2:50 (RA)		IEEE 802.11	Not leaving DS or
QoS Data	1.0	22 dB	MurataMa_5c:1f:7a	e8:b7:48:3b:8b:f2	IEEE 802.11	Frame from DS to a
Acknowledgement	1.0	17 dB	Aerohive_25:c2:50 (RA)		IEEE 802.11	Not leaving DS or
QoS Data	1.0	22 dB	MurataMa_5c:1f:7a	e8:b7:48:3b:8b:f2	IEEE 802.11	Frame from DS to a
Acknowledgement	1.0	19 dB	Aerohive_25:c2:50 (RA)		IEEE 802.11	Not leaving DS or
QoS Data	1.0	22 dB	MurataMa_5c:1f:7a	e8:b7:48:3b:8b:f2	IEEE 802.11	Frame from DS to a
Acknowledgement	1.0	18 dB	Aerohive_25:c2:50 (RA)		IEEE 802.11	Not leaving DS or
Beacon frame	11.0	18 dB	Broadcast	Cisco_7d:de:dc	IEEE 802.11	Not leaving DS or
QoS Data	1.0	22 dB	MurataMa_5c:1f:7a	e8:b7:48:3b:8b:f2	IEEE 802.11	Frame from DS to a
Acknowledgement	1.0	18 dB	Aerohive_25:c2:50 (RA)		IEEE 802.11	Not leaving DS or
QoS Data	1.0	20 dB	e8:b7:48:3b:8b:f2	MurataMa_5c:1f:7a	IEEE 802.11	Frame from STA to
Acknowledgement	1.0	22 dB	MurataMa_5c:1f:7a (RA)		IEEE 802.11	Not leaving DS or
QoS Data	1.0	22 dB	MurataMa_5c:1f:7a	e8:b7:48:3b:8b:f2	IEEE 802.11	Frame from DS to a
Acknowledgement	1.0	18 dB	Aerohive_25:c2:50 (RA)		IEEE 802.11	Not leaving DS or
QoS Data	1.0	17 dB	e8:b7:48:3b:8b:f2	MurataMa_5c:1f:7a	IEEE 802.11	Frame from STA to
Acknowledgement	1.0	22 dB	MurataMa_5c:1f:7a (RA)		IEEE 802.11	Not leaving DS or
QoS Data	1.0	21 dB	MurataMa_5c:1f:7a	e8:b7:48:3b:8b:f2	IEEE 802.11	Frame from DS to a
Acknowledgement	1.0	17 dB	Aerohive_25:c2:50 (RA)		IEEE 802.11	Not leaving DS or
QoS Data	1.0	19 dB	MurataMa_5c:1f:7a	e8:b7:48:3b:8b:f2	IEEE 802.11	Frame from DS to a
QoS Data	1.0	23 dB	MurataMa_5c:1f:7a	e8:b7:48:3b:8b:f2	IEEE 802.11	Frame from DS to a
Acknowledgement	1.0	17 dB	Aerohive_25:c2:50 (RA)		IEEE 802.11	Not leaving DS or
QoS Data	1.0	18 dB	e8:b7:48:3b:8b:f2	MurataMa_5c:1f:7a	IEEE 802.11	Frame from STA to
Beacon frame	6.0	16 dB	Broadcast	Cisco_41:18:a0	IEEE 802.11	Not leaving DS or
QoS Data	1.0	19 dB	e8:b7:48:3b:8b:f2	MurataMa_5c:1f:7a	IEEE 802.11	Frame from STA to
QoS Data	1.0	16 dB	e8:b7:48:3b:8b:f2	MurataMa_5c:1f:7a	IEEE 802.11	Frame from STA to
QoS Data	1.0	18 dB	e8:b7:48:3b:8b:f2	MurataMa_5c:1f:7a	IEEE 802.11	Frame from STA to
Acknowledgement	1.0	22 dB	MurataMa_5c:1f:7a (RA)		IEEE 802.11	Not leaving DS or

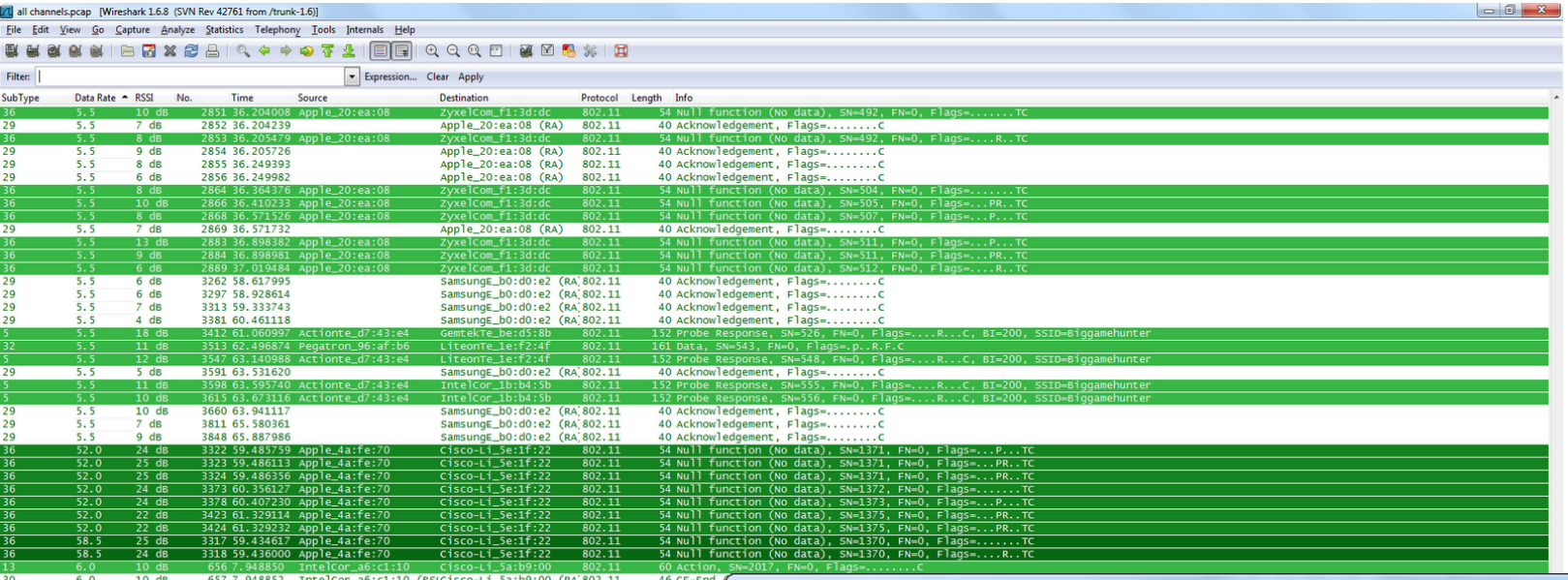
Channel Profile

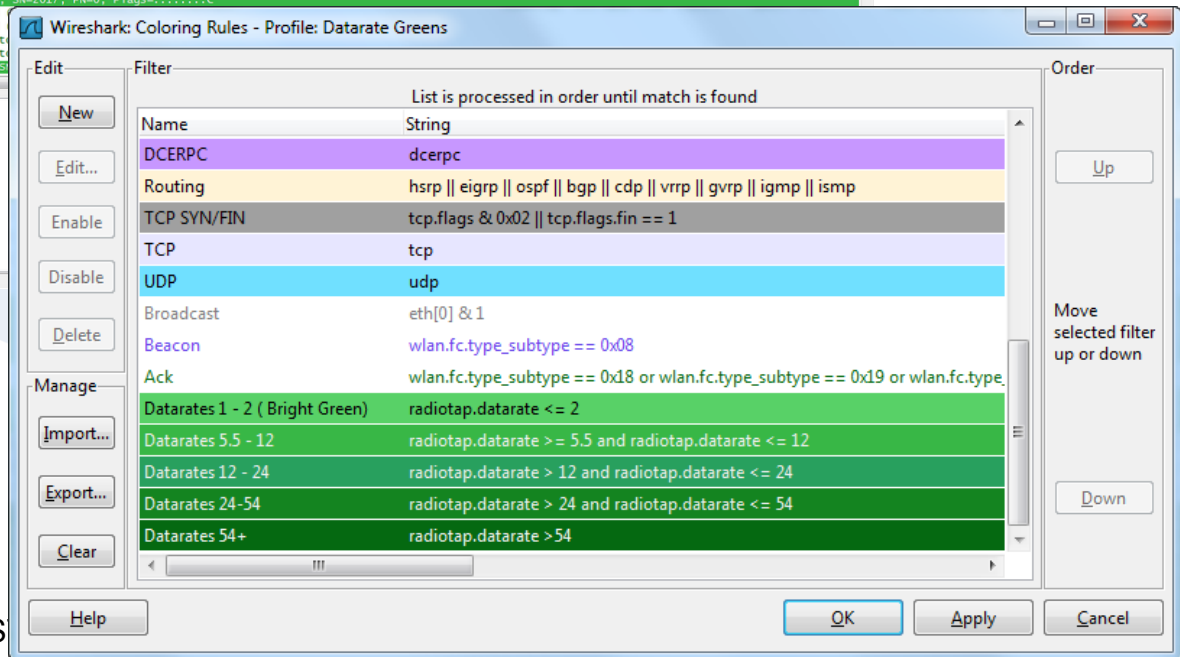




SHAR

Data Rate Profile





Fin.

Visualizing 802.11 Wireshark Data

Tuesday, July 26th, 2012

Ryan Woodings

Chief Geek | MetaGeek

@metageek