

Wireshark Developer and User Conference

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

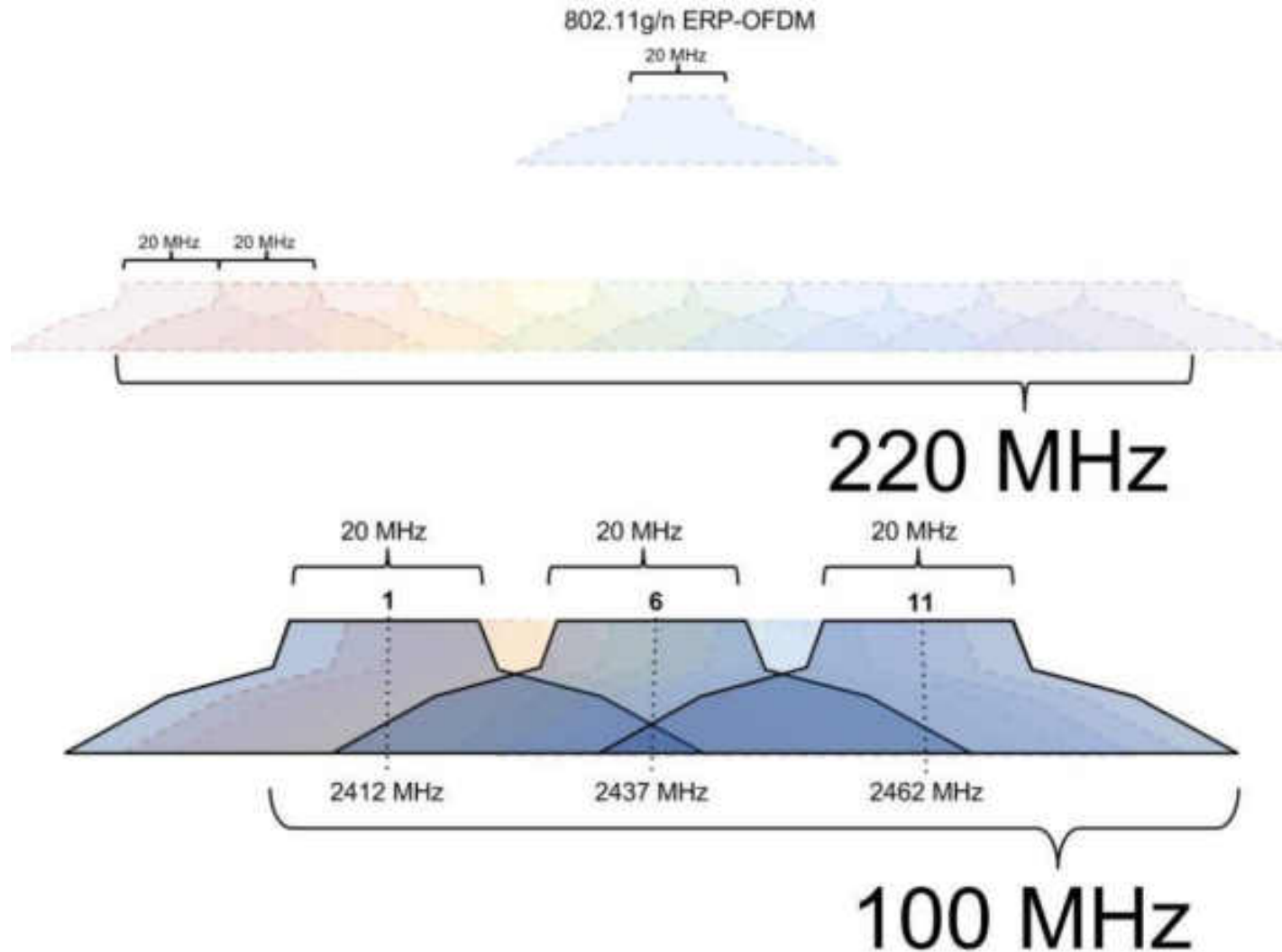
5 GHz

- 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.

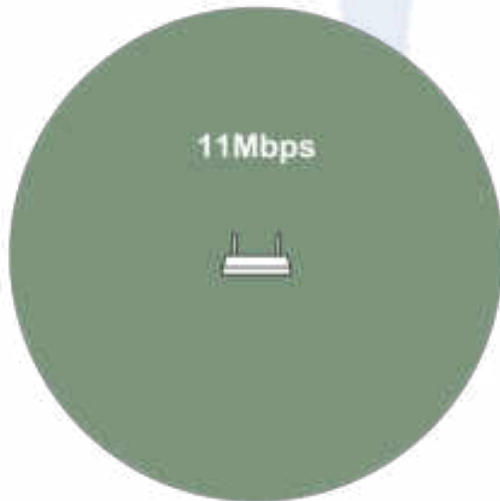
Physical Layer Modulation



Live Demo

802.11b

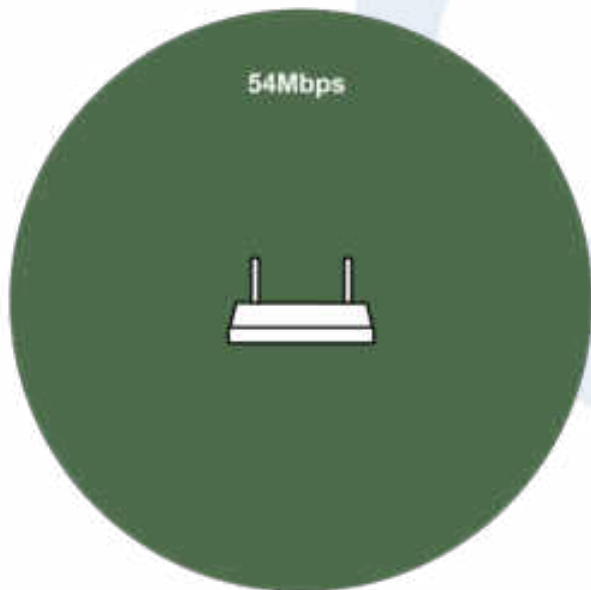
- 2.4 GHz-only
- 22 MHz Wide
- 1-11 Mbps
- HR-DSSS BPSK w/ CCK Modulation
- Good for longer range but low data rate.



```
Frame 19665: 185 bytes on wire (1480 bits), 185 bytes captured (1480 bits) on 0
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): False
    ... .. 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

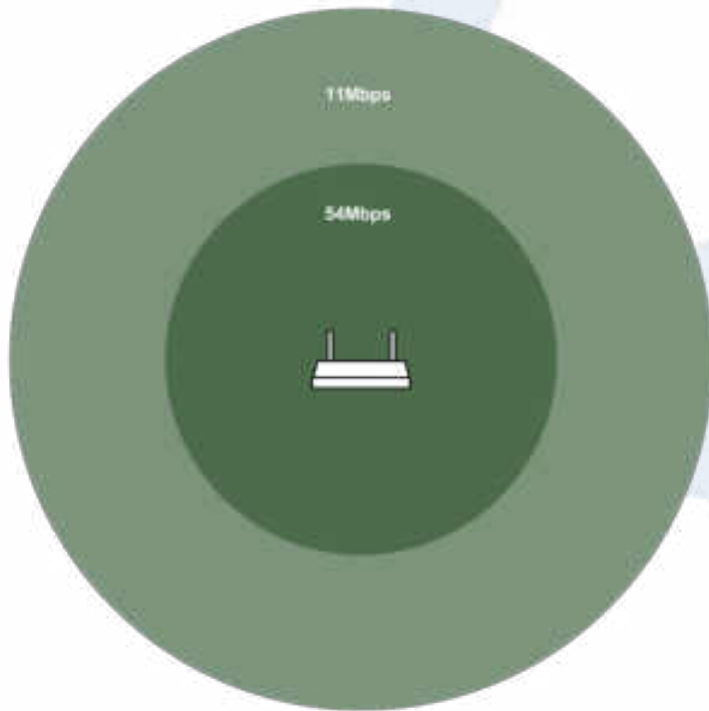
- 5 GHz-only
- 20 MHz Wide
- 6-54 Mbps
- OFDM Modulation



```
▣ 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

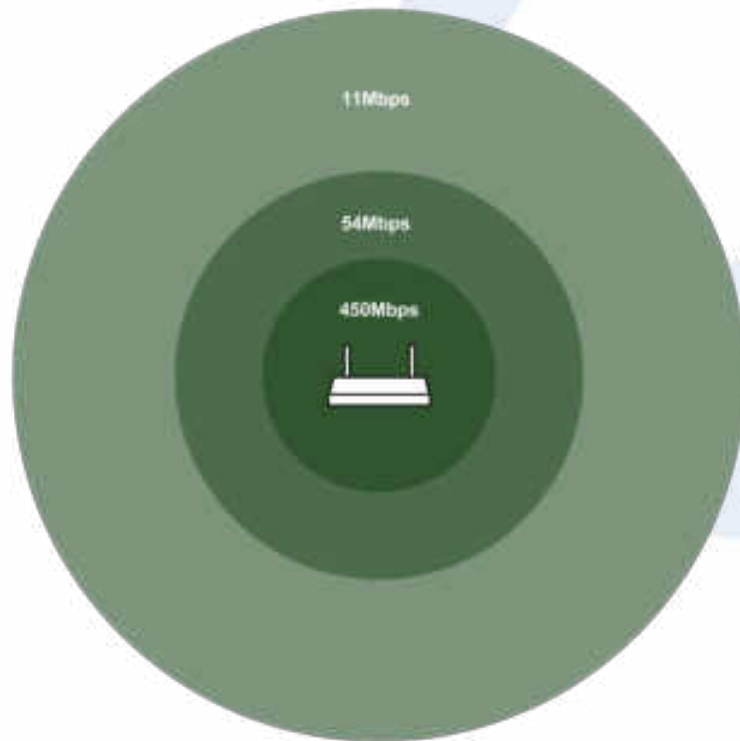
- 2.4 GHz-only
- 20 MHz Wide
- 6-54Mbps
- ERP-OFDM Modulation



```
▣ 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 [8G 1]
▣ Channel type: 802.11g (pure-g) (0x00c0)
.....0..... = Turbo: False
.....0..... = Complementary Code Keying (CCK): False
.....1..... = Orthogonal Frequency-Division Multiplexing (OFDM): True
.....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

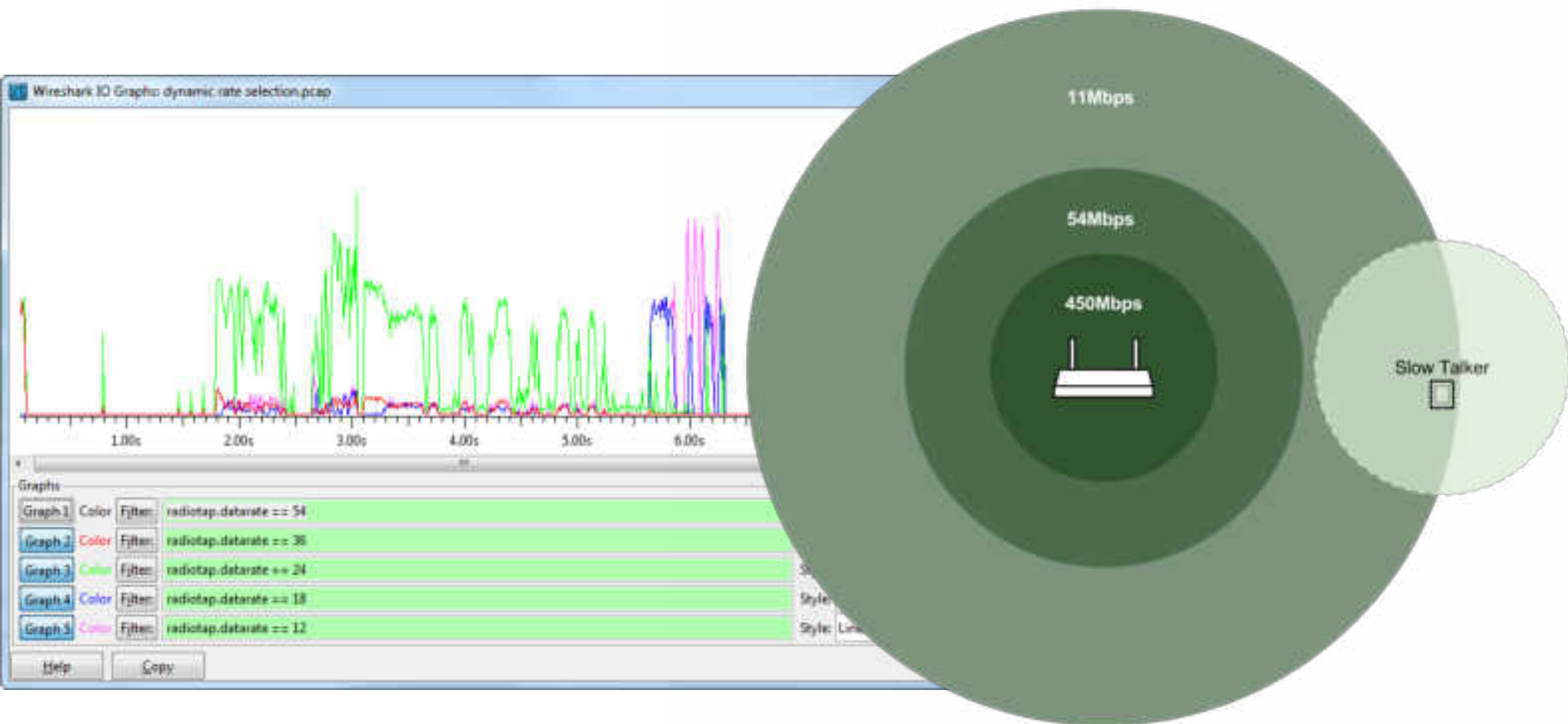
- 2.4 & 5 GHz
- 20-40 MHz Wide
- 6-450 Mbps
- OFDM Modulation



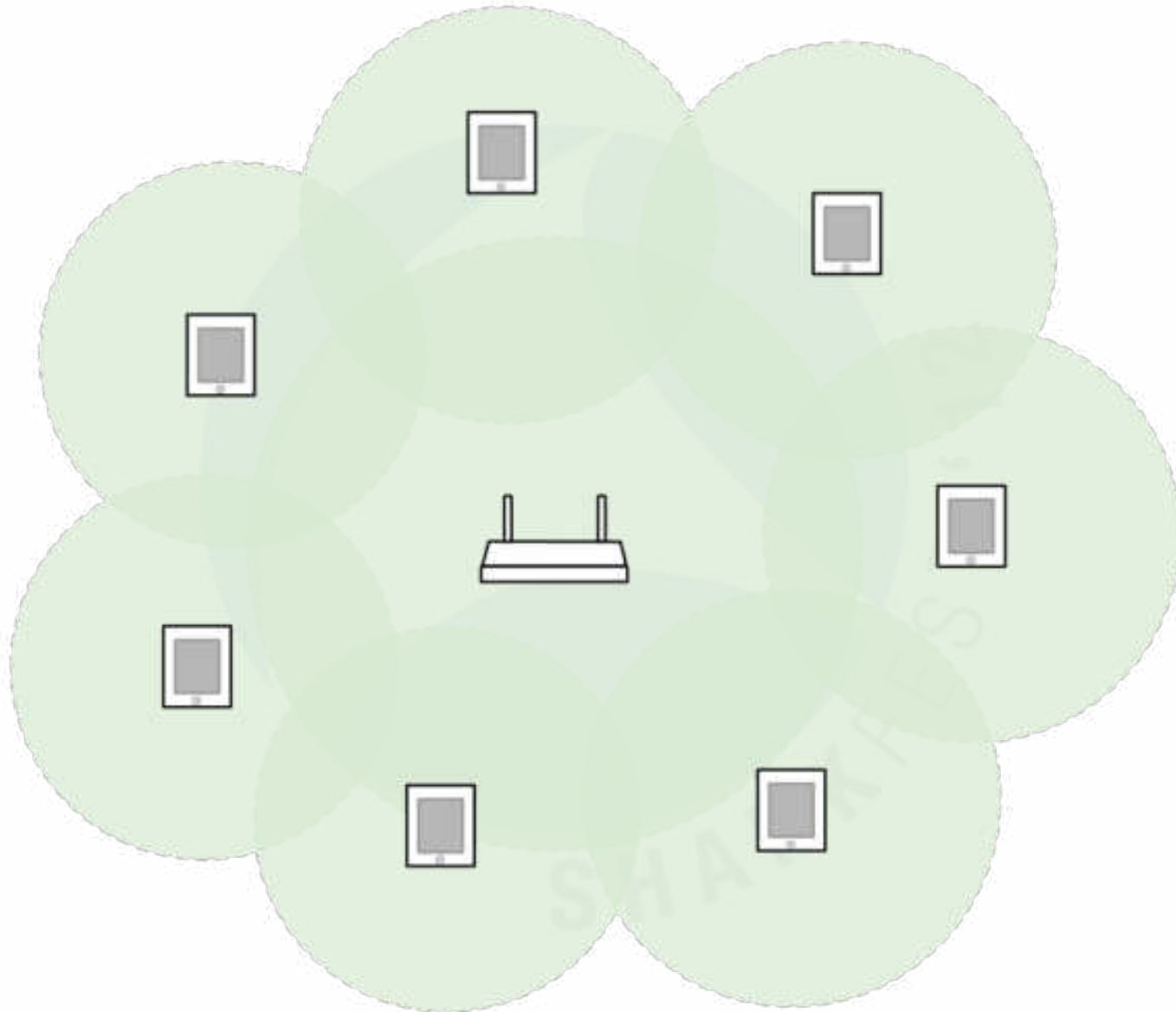
SHARKFEST '12

Dynamic Rate Selection

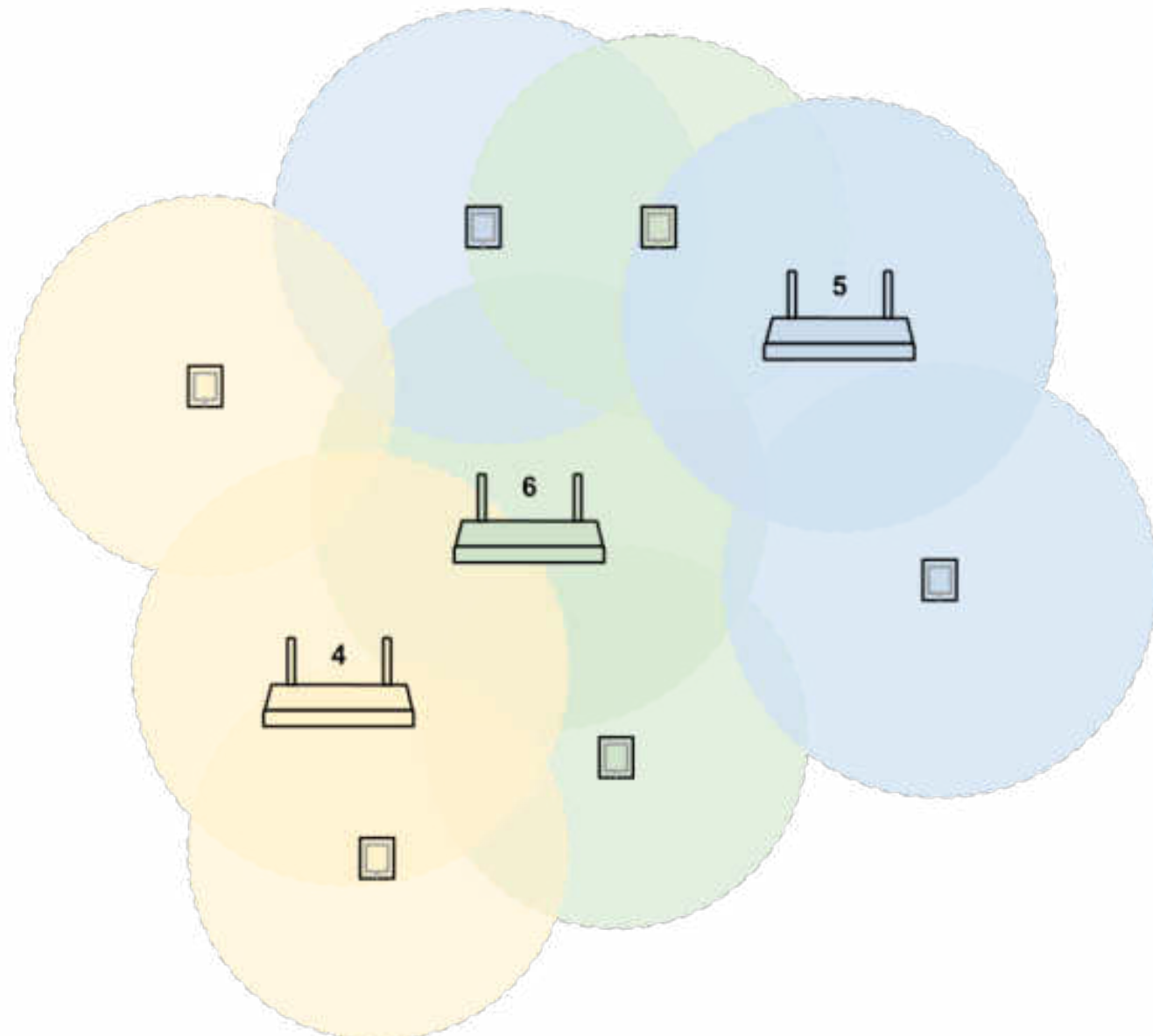
As clients are further away from an Access point they choose a lower modulation rate.



Channel Contention



Channel Contention



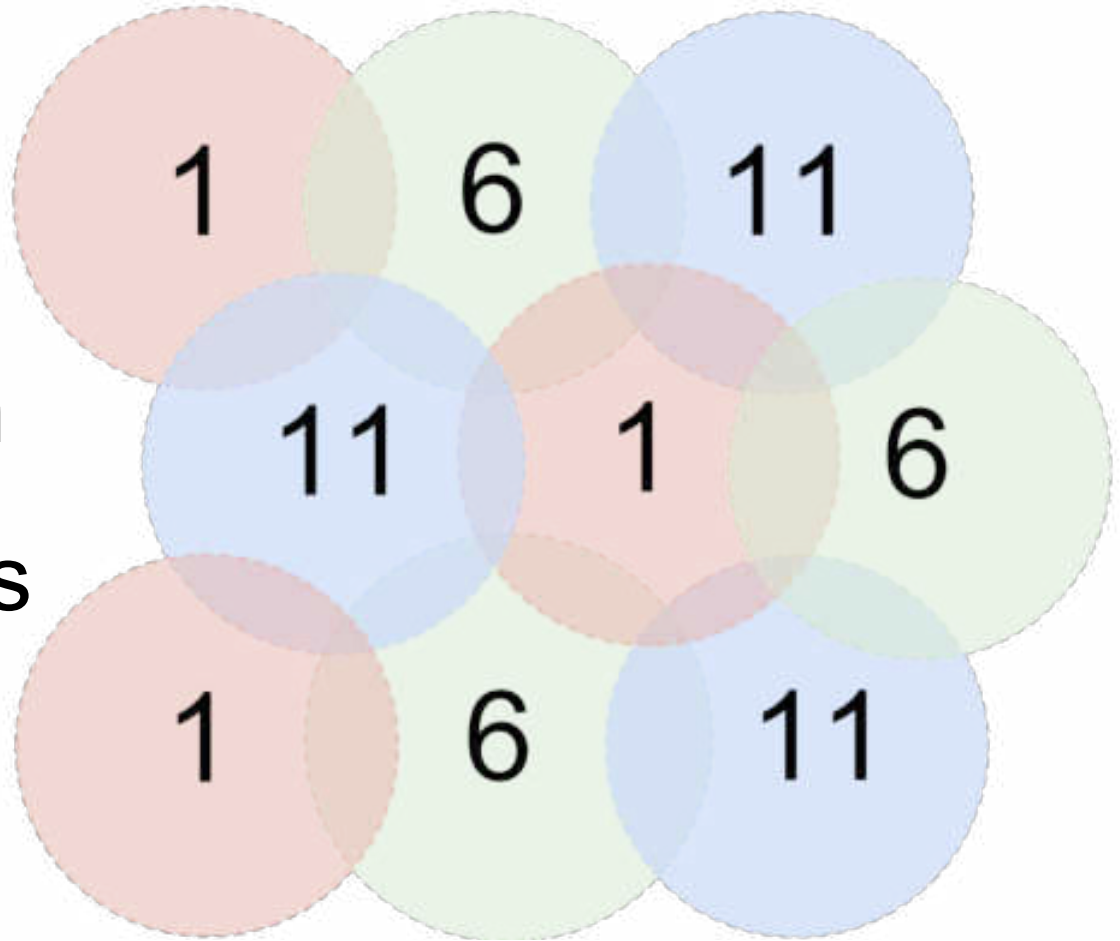
Contention Domains

Channel

Antenna Pattern

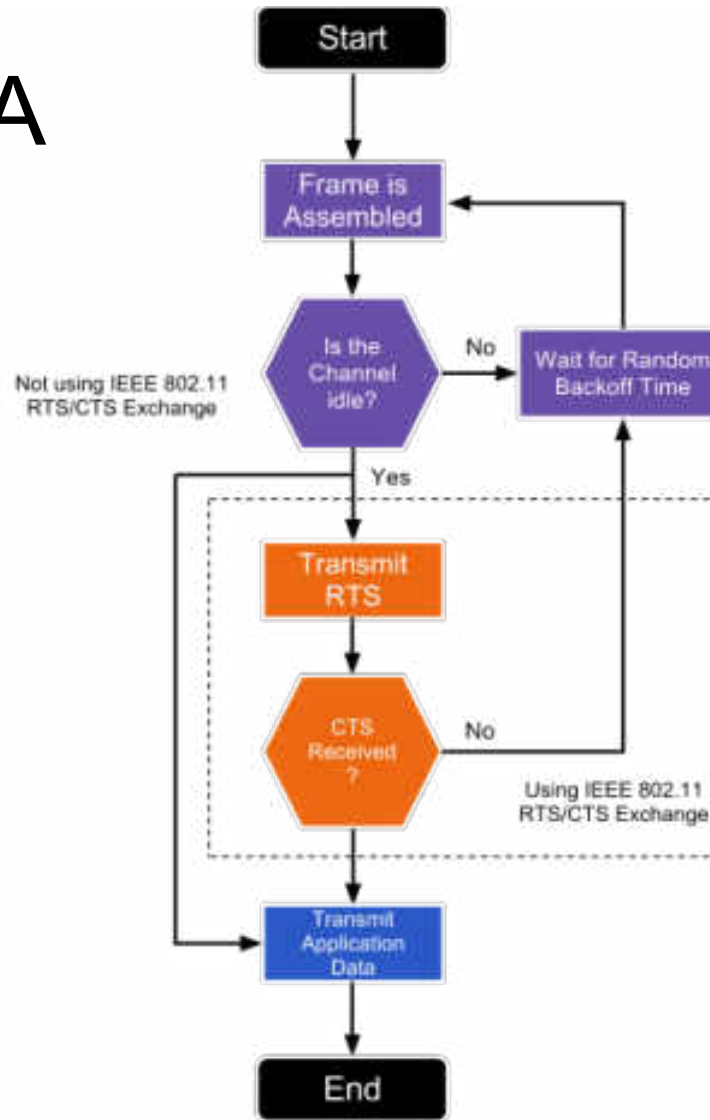
Physical Barriers

Transmit Power

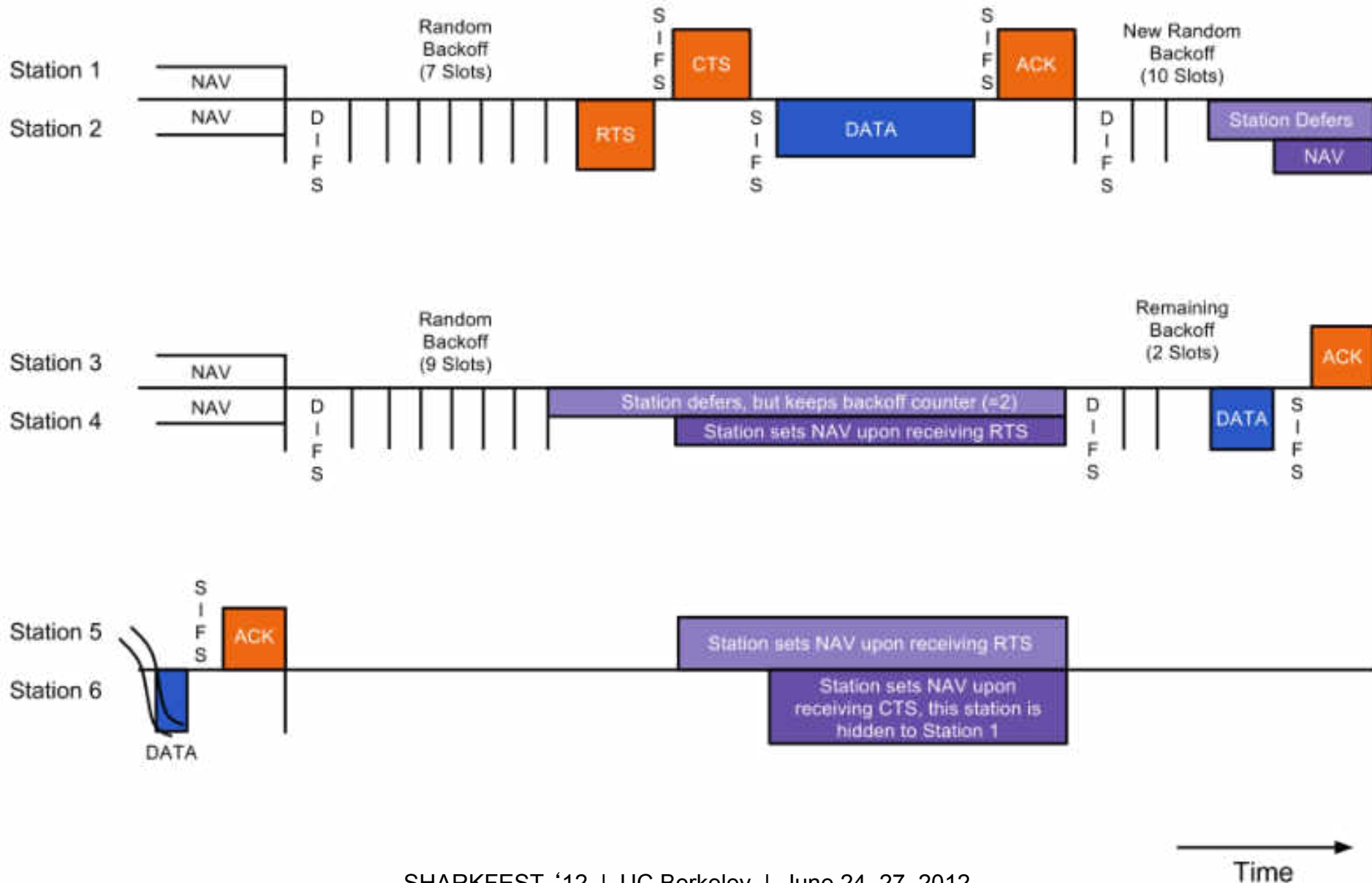


Wireless Medium Access

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

1.0	48 dB	Broadcast	Aerohive_
1.0	47 dB	Broadcast	Aerohive_
1.0	49 dB	Broadcast	Aerohive_
5.5	42 dB	192.168.5.208	205.251.2
11.0	16 dB	Cisco_07:8d:71 (RA)	
5.5	45 dB	HonHaiPr_9d:5e:11 (RA)	Cisco_08:
5.5	45 dB	192.168.5.208	205.251.2
11.0	17 dB	Cisco_07:8d:71 (RA)	
5.5	42 dB	HonHaiPr_9d:5e:11 (RA)	Cisco_08:
5.5	42 dB	192.168.5.208	205.251.2
5.5	16 dB	Broadcast	Cisco_07:
5.5	41 dB	192.168.5.208	205.251.2
5.5	14 dB	Broadcast	Cisco_0f:
5.5	42 dB	192.168.5.208	205.251.2
11.0	16 dB	Cisco_07:8d:71 (RA)	
5.5	42 dB	HonHaiPr_9d:5e:11 (RA)	Cisco_08:
5.5	41 dB	192.168.5.208	205.251.2
5.5	41 dB	Broadcast	Cisco_08:
5.5	42 dB	192.168.5.208	205.251.2
11.0	16 dB	Cisco_07:8d:71 (RA)	
5.5	44 dB	192.168.5.208	205.251.2
5.5	42 dB	HonHaiPr_9d:5e:11 (RA)	Cisco_08:
5.5	43 dB	HonHaiPr_9d:5e:11 (RA)	Cisco_08:
5.5	44 dB	192.168.5.208	205.251.2

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

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)

wlan.fc.type == 1

Data Frames

Data Frames carry higher-level protocol data

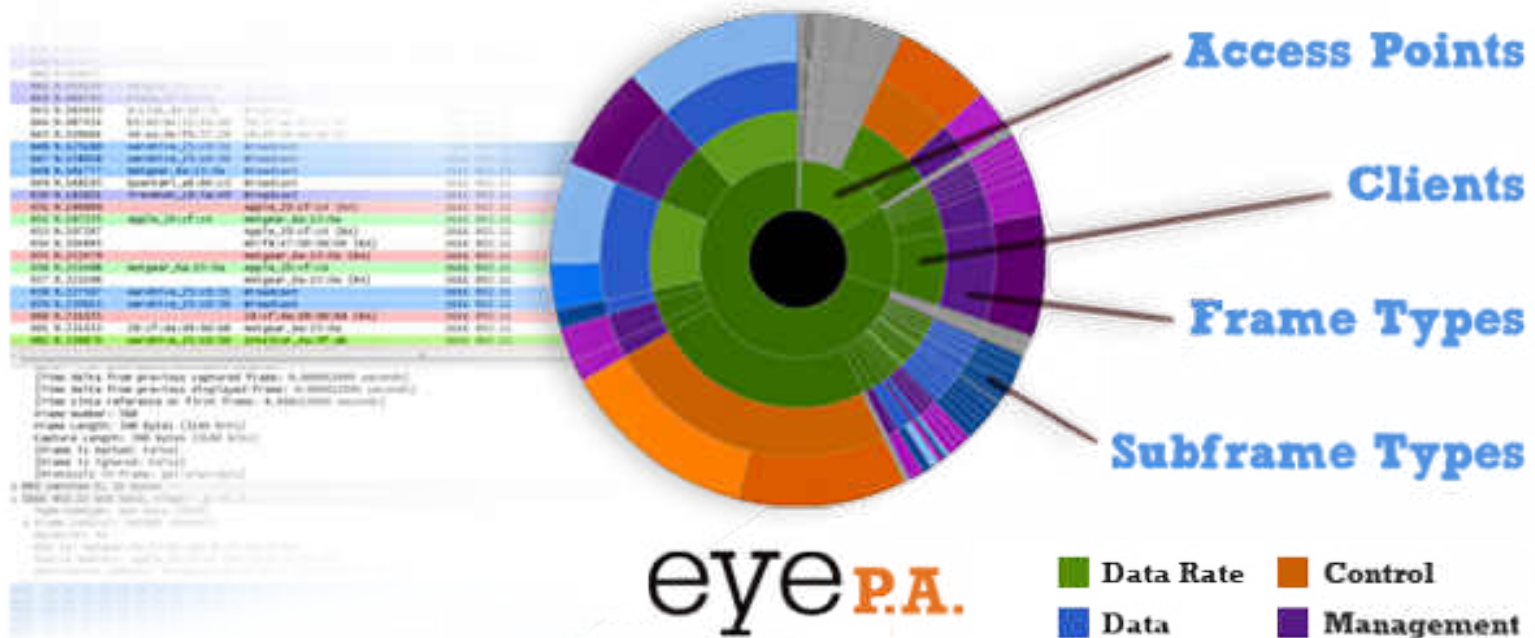
For Example,

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

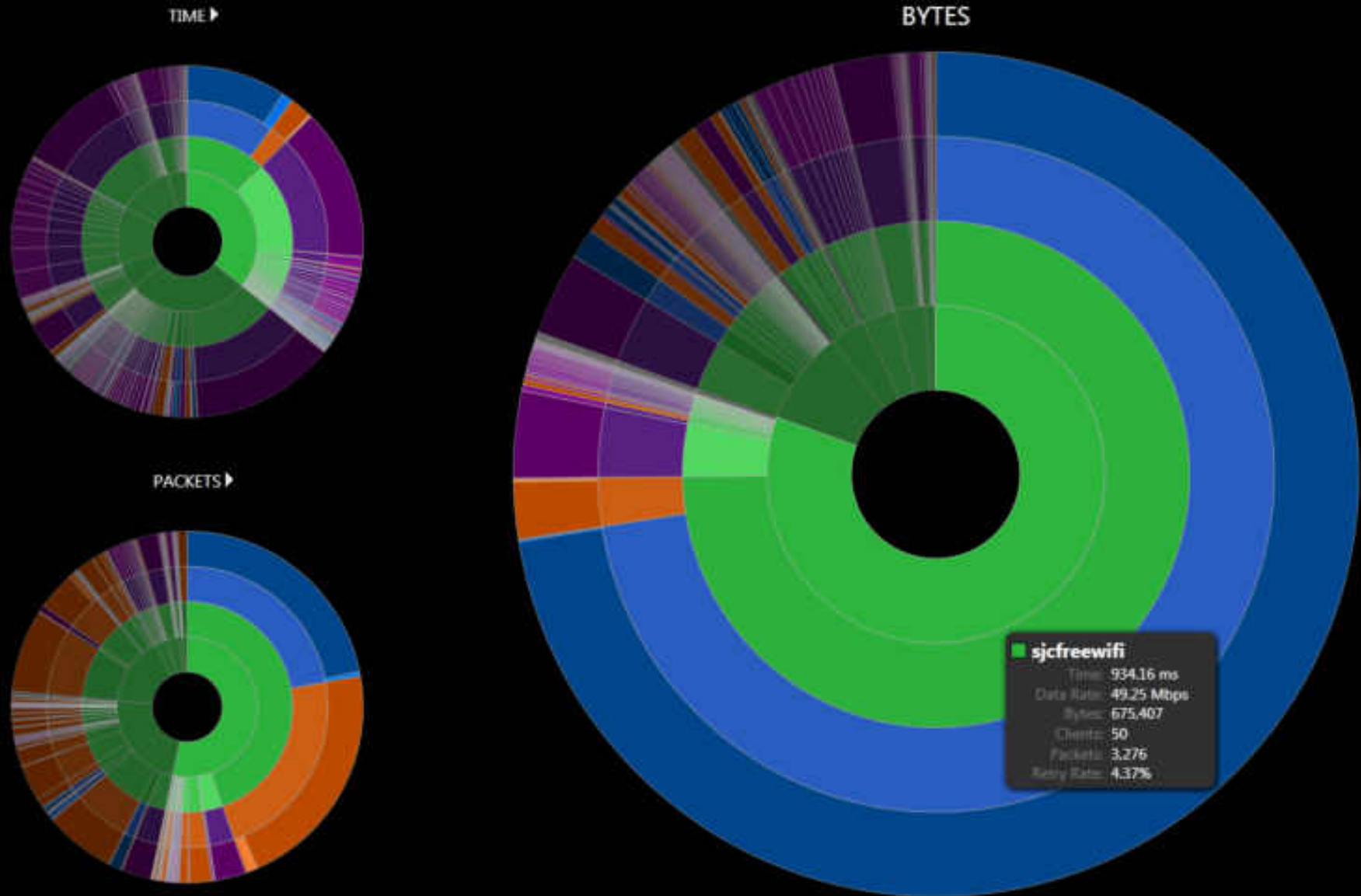
SubType	Data Rate	RSSI	Destination
Data	1.0	24 dB	Broadcast
Null function (No	6.5	24 dB	Aerohive_25:c2:
Data	1.0	26 dB	Broadcast
QoS Data	6.5	24 dB	IPv4mcast_00:00
QoS Data	52.0	23 dB	Apple_0b:93:2a
Null function (No	6.5	24 dB	Aerohive_25:c2:
Null function (No	6.5	24 dB	Aerohive_25:c2:
Null function (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)

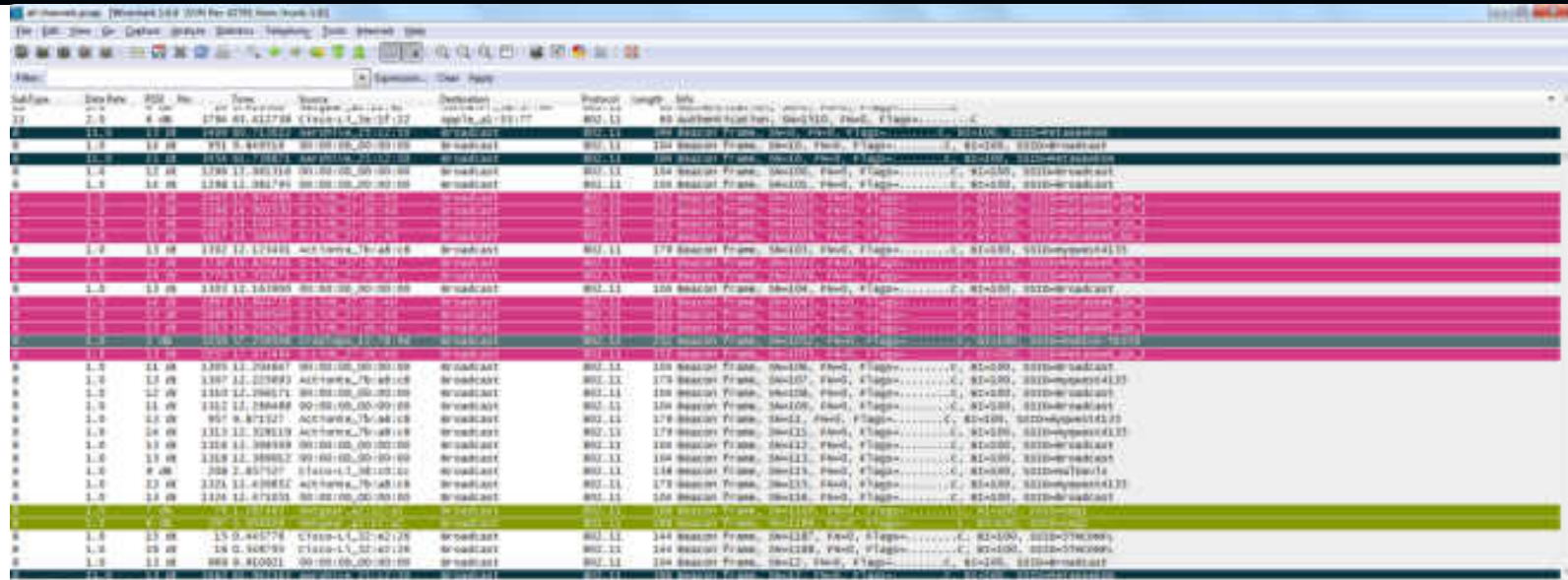
RSSI

IEEE 802.11 RSSI (existing field type)

Packet Type Profile

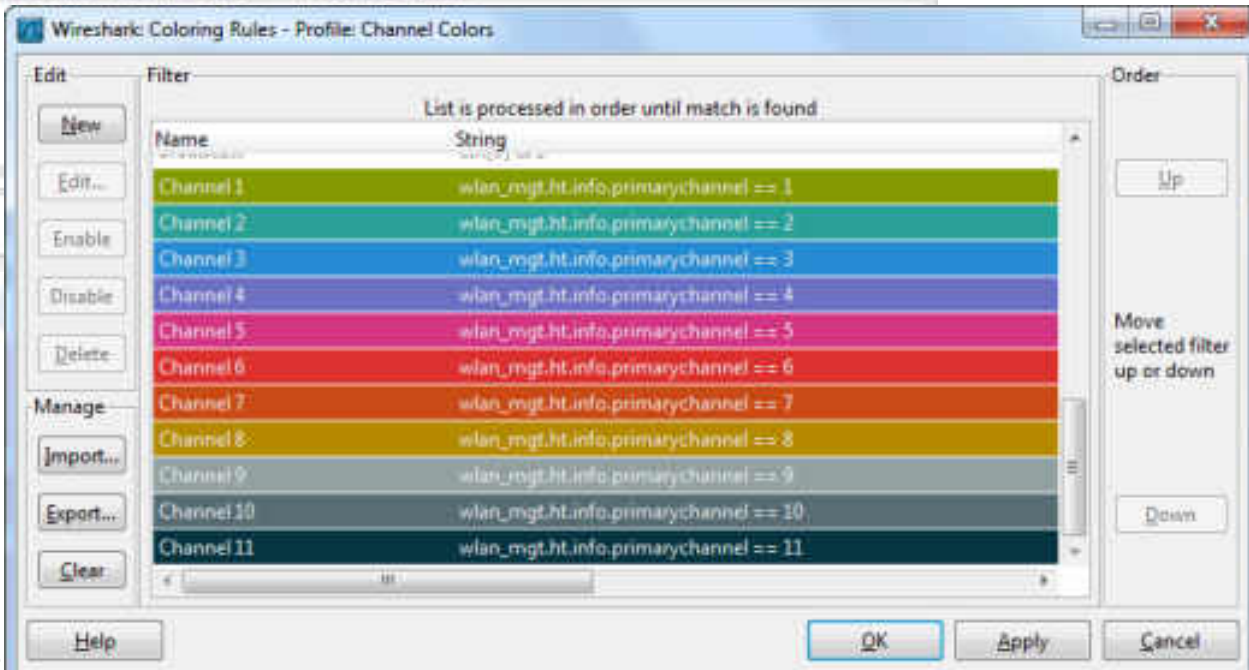
SubType	Data Rate	RSSI	Destination	Source	Protocol	To/From DS
Beacon frame	11.0	20 dB	Broadcast	Cisco_7d:de:da	IEEE 802.11	Not leaving DS or
QoS Data	1.0	17 dB	e8:b7:48:3b:8b:f2	MurataMa_5c:1f:7a	IEEE 802.11	Frame from STA to
Acknowledgement	1.0	22 dB	MurataMa_5c:1f:7a (RA)		IEEE 802.11	Not leaving DS 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



The image shows a Wireshark packet capture of WLAN management frames. The main pane displays a list of frames with columns for Time, Source, Destination, Protocol, Length, and Info. The frames are color-coded according to a channel profile. The bottom pane shows the details of a selected frame, including the WLAN Management Frame structure and the Channel field.

Time	Source	Destination	Protocol	Length	Info
1.0	192.168.1.1	192.168.1.2	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=100, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.2	192.168.1.1	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=101, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.1	192.168.1.2	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=102, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.2	192.168.1.1	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=103, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.1	192.168.1.2	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=104, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.2	192.168.1.1	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=105, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.1	192.168.1.2	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=106, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.2	192.168.1.1	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=107, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.1	192.168.1.2	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=108, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.2	192.168.1.1	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=109, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.1	192.168.1.2	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=110, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.2	192.168.1.1	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=111, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.1	192.168.1.2	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=112, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.2	192.168.1.1	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=113, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.1	192.168.1.2	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=114, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.2	192.168.1.1	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=115, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.1	192.168.1.2	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=116, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.2	192.168.1.1	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=117, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.1	192.168.1.2	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=118, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.2	192.168.1.1	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=119, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.1	192.168.1.2	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=120, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.2	192.168.1.1	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=121, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.1	192.168.1.2	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=122, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.2	192.168.1.1	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=123, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.1	192.168.1.2	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=124, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.2	192.168.1.1	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=125, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.1	192.168.1.2	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=126, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.2	192.168.1.1	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=127, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.1	192.168.1.2	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=128, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.2	192.168.1.1	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=129, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.1	192.168.1.2	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=130, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.2	192.168.1.1	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=131, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.1	192.168.1.2	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=132, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.2	192.168.1.1	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=133, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.1	192.168.1.2	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=134, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.2	192.168.1.1	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=135, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.1	192.168.1.2	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=136, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.2	192.168.1.1	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=137, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.1	192.168.1.2	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=138, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.2	192.168.1.1	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=139, Pwr=0, Flags=.....C, SI=000, SSID=MySSID
1.0	192.168.1.1	192.168.1.2	WLAN Mgmt	100	WLAN Mgmt Frame, Seq=140, Pwr=0, Flags=.....C, SI=000, SSID=MySSID



The image shows the 'Wireshark: Coloring Rules - Profile: Channel Colors' dialog box. It contains a table of rules for coloring packets based on their channel. The rules are listed in order, and the first rule that matches is used for coloring.

Name	String
Channel 1	wlan_mgt.ht.info.primarychannel == 1
Channel 2	wlan_mgt.ht.info.primarychannel == 2
Channel 3	wlan_mgt.ht.info.primarychannel == 3
Channel 4	wlan_mgt.ht.info.primarychannel == 4
Channel 5	wlan_mgt.ht.info.primarychannel == 5
Channel 6	wlan_mgt.ht.info.primarychannel == 6
Channel 7	wlan_mgt.ht.info.primarychannel == 7
Channel 8	wlan_mgt.ht.info.primarychannel == 8
Channel 9	wlan_mgt.ht.info.primarychannel == 9
Channel 10	wlan_mgt.ht.info.primarychannel == 10
Channel 11	wlan_mgt.ht.info.primarychannel == 11

Data Rate Profile

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
2	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
3	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
4	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
5	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
6	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
7	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
8	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
9	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
10	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
11	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
12	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
13	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
14	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
15	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
16	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
17	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
18	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
19	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
20	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
21	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
22	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
23	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
24	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
25	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
26	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
27	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
28	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
29	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
30	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
31	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
32	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
33	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
34	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
35	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
36	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
37	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
38	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
39	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
40	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
41	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
42	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
43	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
44	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
45	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
46	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
47	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
48	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes
49	0.000000	192.168.1.100	192.168.1.1	ICMP	60	Echo (ping) 60 bytes
50	0.000000	192.168.1.1	192.168.1.100	ICMP	60	Reply 60 bytes

Wireshark: Coloring Rules - Profile: Datarate Greens

Edit Filter: List is processed in order until match is found

Name	Filter
DCERPC	dcerpc
Routing	hrrp eigrp ospf bgp cdp vrrp gvrp igmp ismp
TCP SYN/FIN	tcp.flags & 0x02 tcp.flags.fin == 1
TCP	tcp
UDP	udp
Broadcast	eth[0] & 1
Bescon	wlan.fc.type_subtype == 0x08
Ack	wlan.fc.type_subtype == 0x18 or wlan.fc.type_subtype == 0x19 or wlan.fc.type_subtype == 0x20
Datarates 1 - 2 (Bright Green)	radiotap.datarate <= 2
Datarates 3 - 12	radiotap.datarate >= 3 and radiotap.datarate <= 12
Datarates 12 - 24	radiotap.datarate > 12 and radiotap.datarate <= 24
Datarates 24 - 34	radiotap.datarate > 24 and radiotap.datarate <= 34
Datarates 34+	radiotap.datarate > 34

Buttons: New, Edit, Enable, Disable, Delete, Manage, Import, Export, Clear, Help, OK, Apply, Cancel

Fin.

Visualizing 802.11 Wireshark Data

Tuesday, July 26th, 2012



Ryan Woodings

Chief Geek | MetaGeek



@metageek