

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

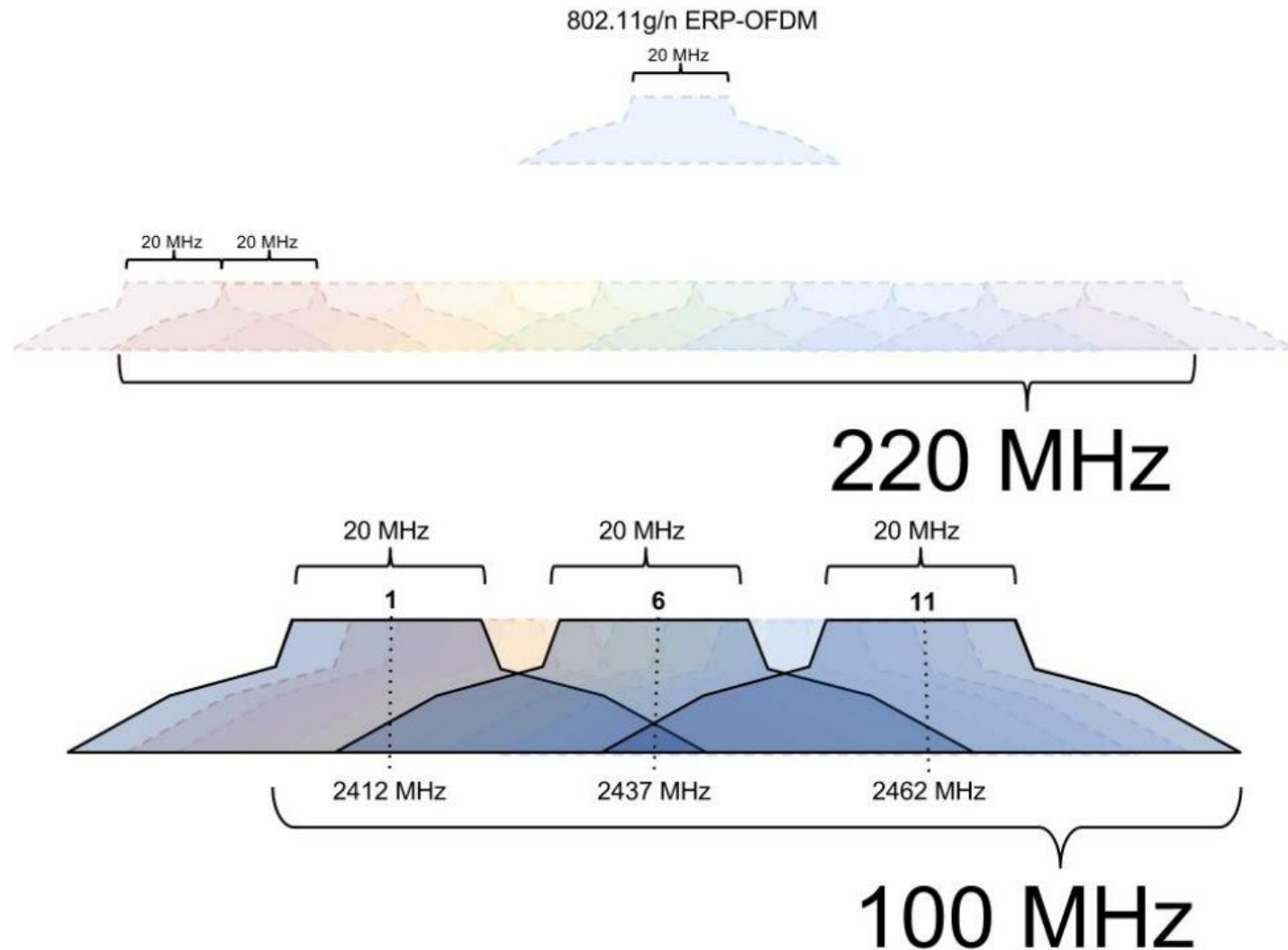
5 GHz

- 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)

The diagram shows a waveform for CCK (HR-DSSS Phase Shift Keying). It consists of three distinct, rounded pulses of varying heights, each representing a different phase shift. The pulses are arranged horizontally, with the middle pulse being the tallest and the two side pulses being shorter and of equal height.



OFDM (Orthogonal Frequency Division Multiplexing)

The diagram shows a waveform for OFDM (Orthogonal Frequency Division Multiplexing). It is a trapezoidal shape, wider at the base and narrower at the top, representing the frequency spectrum of the signal. The shape is centered horizontally and has a flat top and bottom.

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.

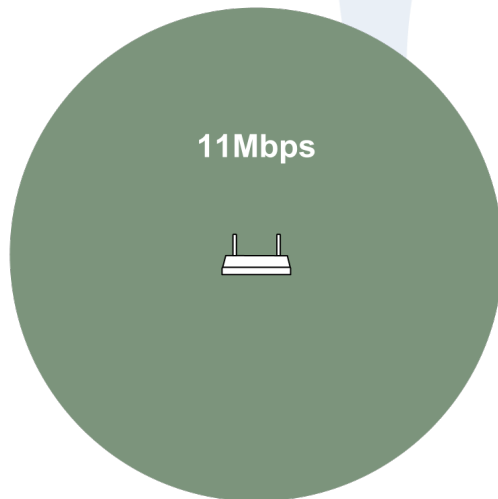
Physical Layer Modulation

A large, light blue watermark logo is centered in the background. It features a circular design composed of four curved, leaf-like segments. The text "SHARKFEST '12" is written in a light blue, sans-serif font, following the curve of the bottom half of the circle.

Live Demo

802.11b

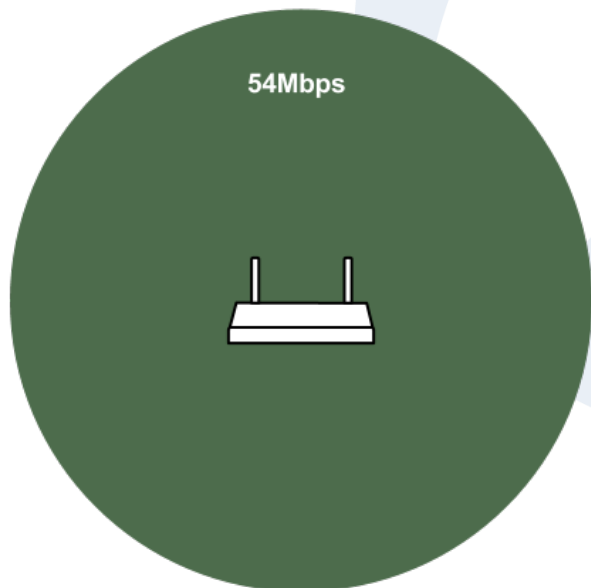
- 2.4 GHz-only
- 22 MHz Wide
- 1-11 Mbps
- HR-DSSS BPSK w/ CCK Modulation
- Good for longer range but low data rate.



```
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

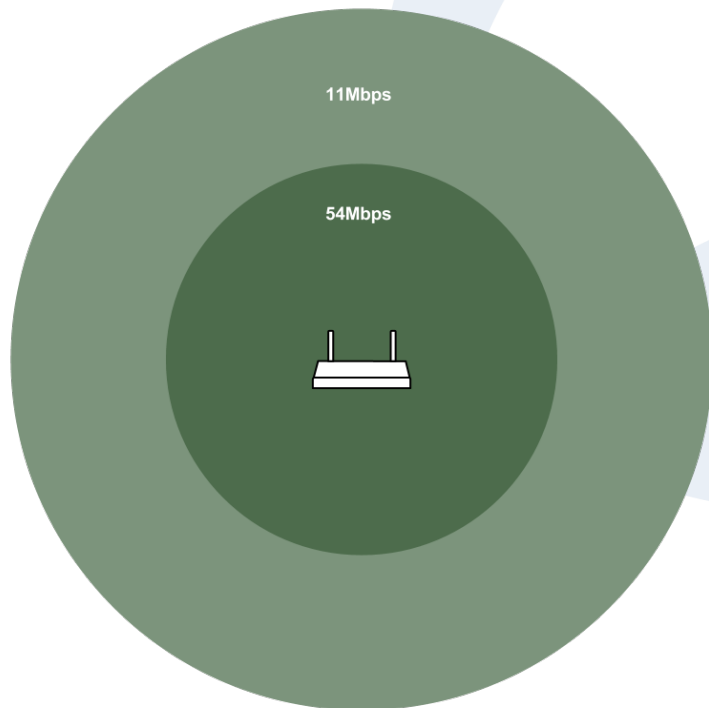
- 5 GHz-only
- 20 MHz Wide
- 6-54 Mbps
- OFDM Modulation



```
[-] 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

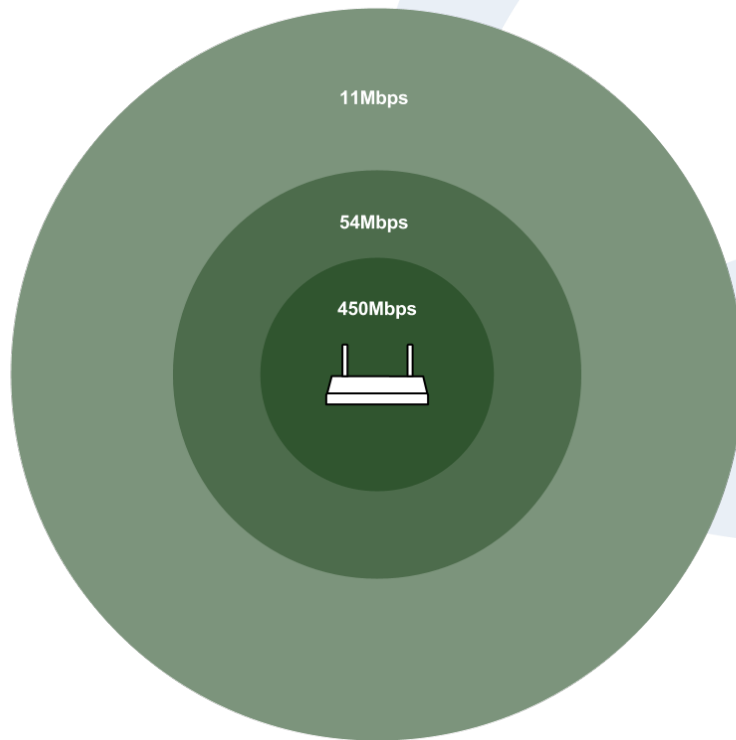
- 2.4 GHz-only
- 20 MHz Wide
- 6-54Mbps
- ERP-OFDM Modulation



```
▣ 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 [BG 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

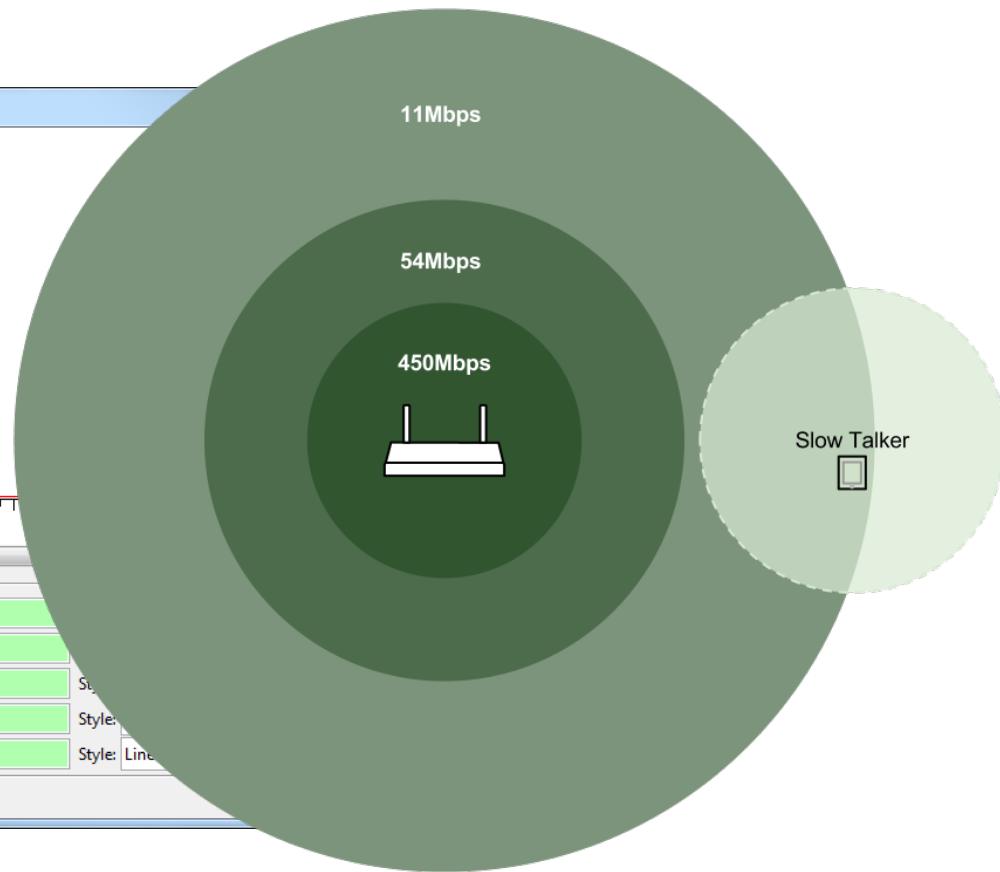
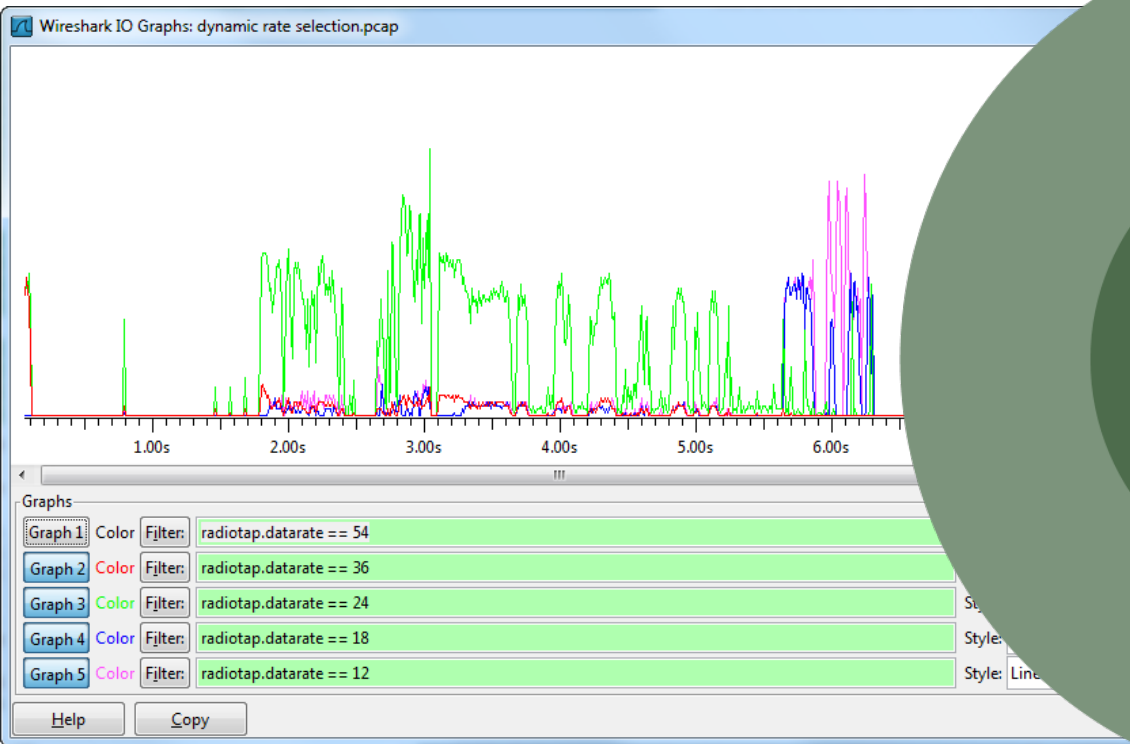
- 2.4 & 5 GHz
- 20-40 MHz Wide
- 6-450 Mbps
- OFDM Modulation



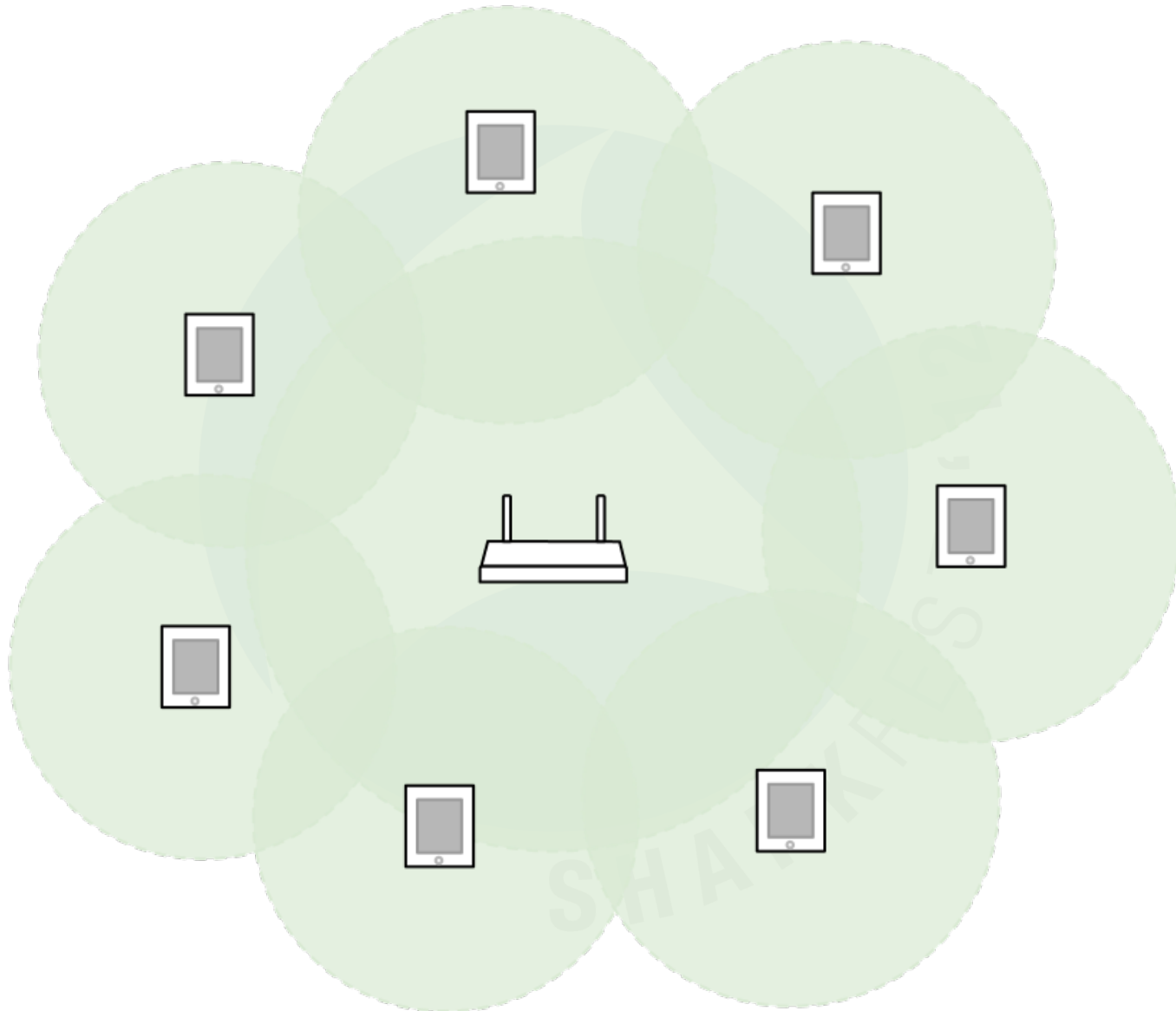
SHARKFEST '12

Dynamic Rate Selection

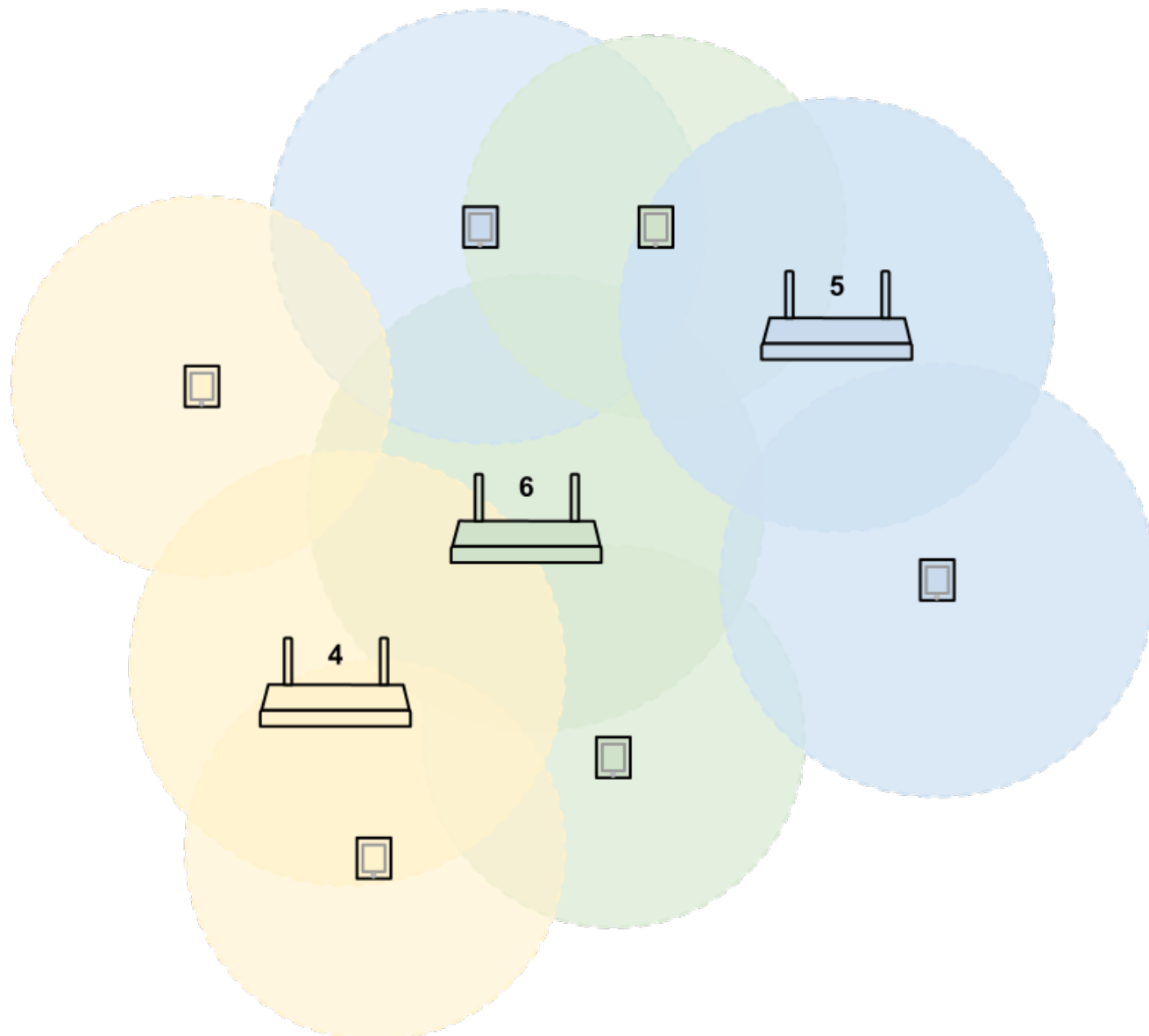
As clients are further away from an Access point they choose a lower modulation rate.



Channel Contention



Channel Contention



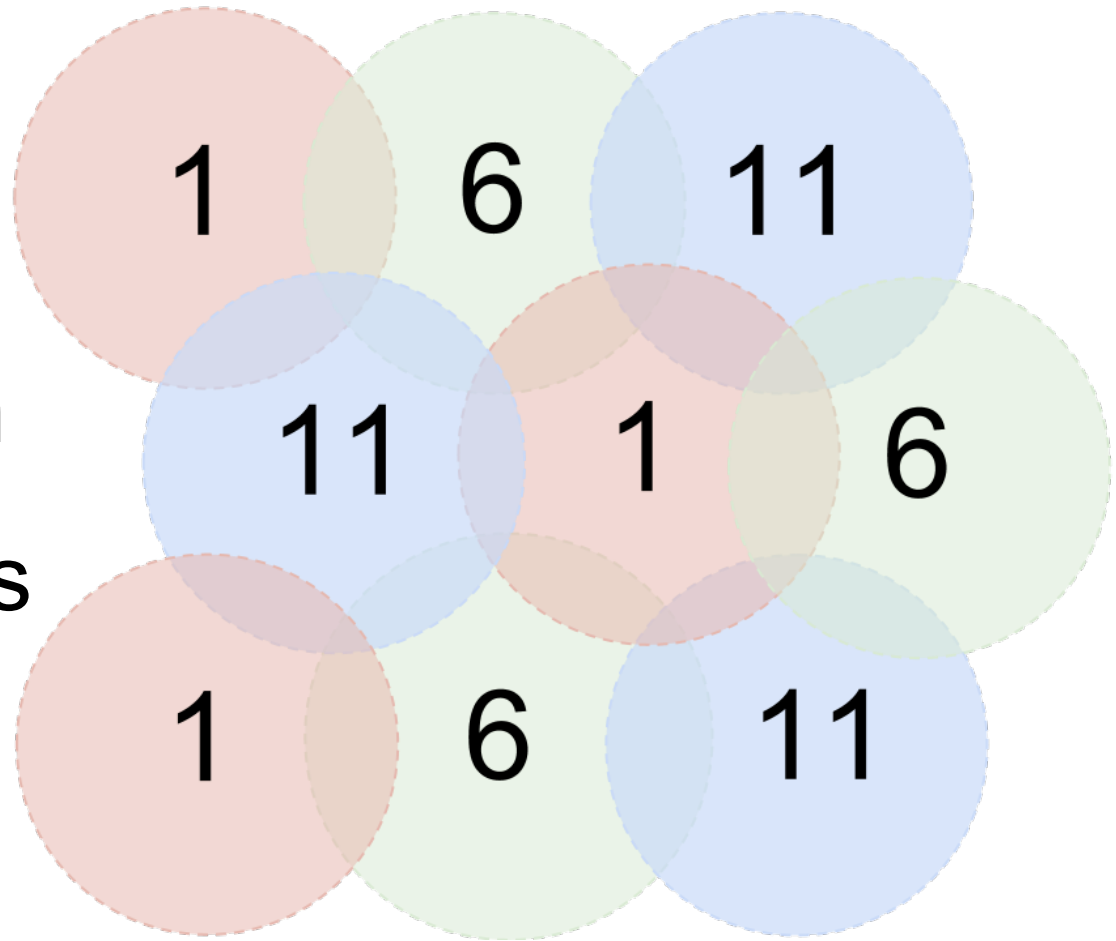
Contention Domains

Channel

Antenna Pattern

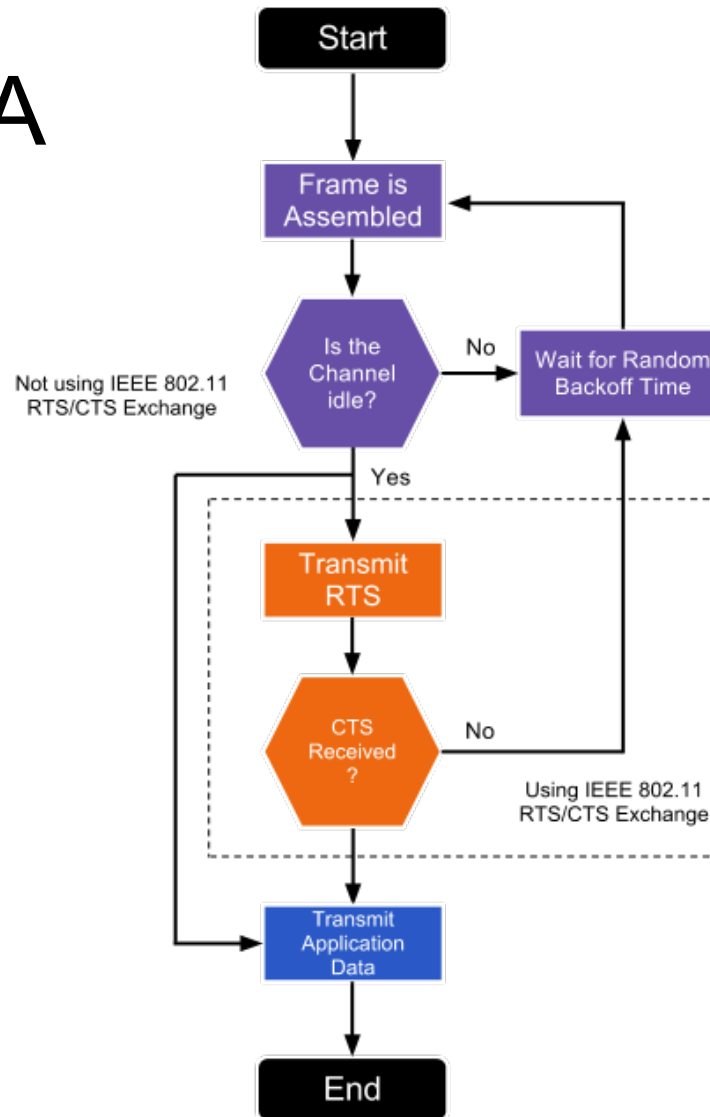
Physical Barriers

Transmit Power

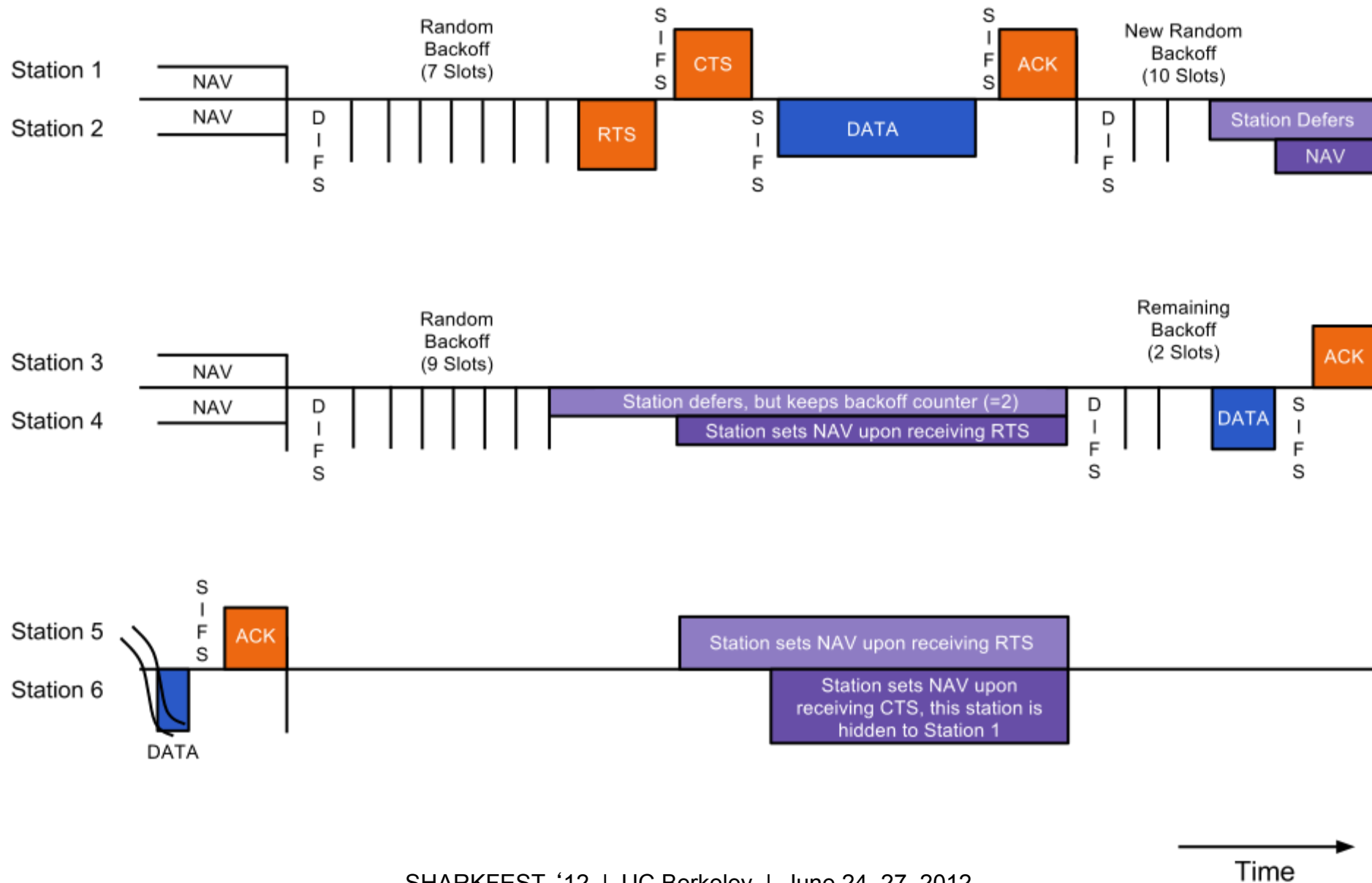


Wireless Medium Access

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

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

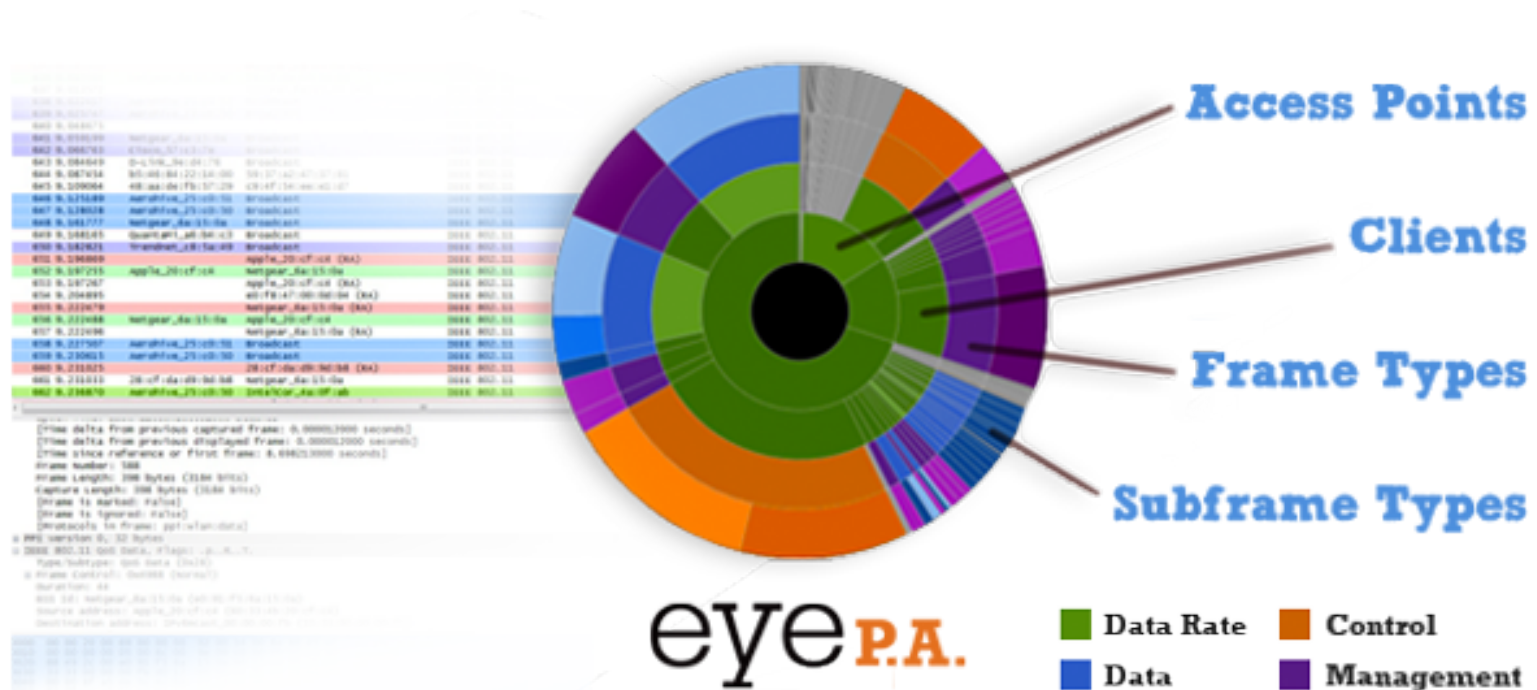
For Example,

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

wlan.fc.type == 2

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

Visual Packet Analysis

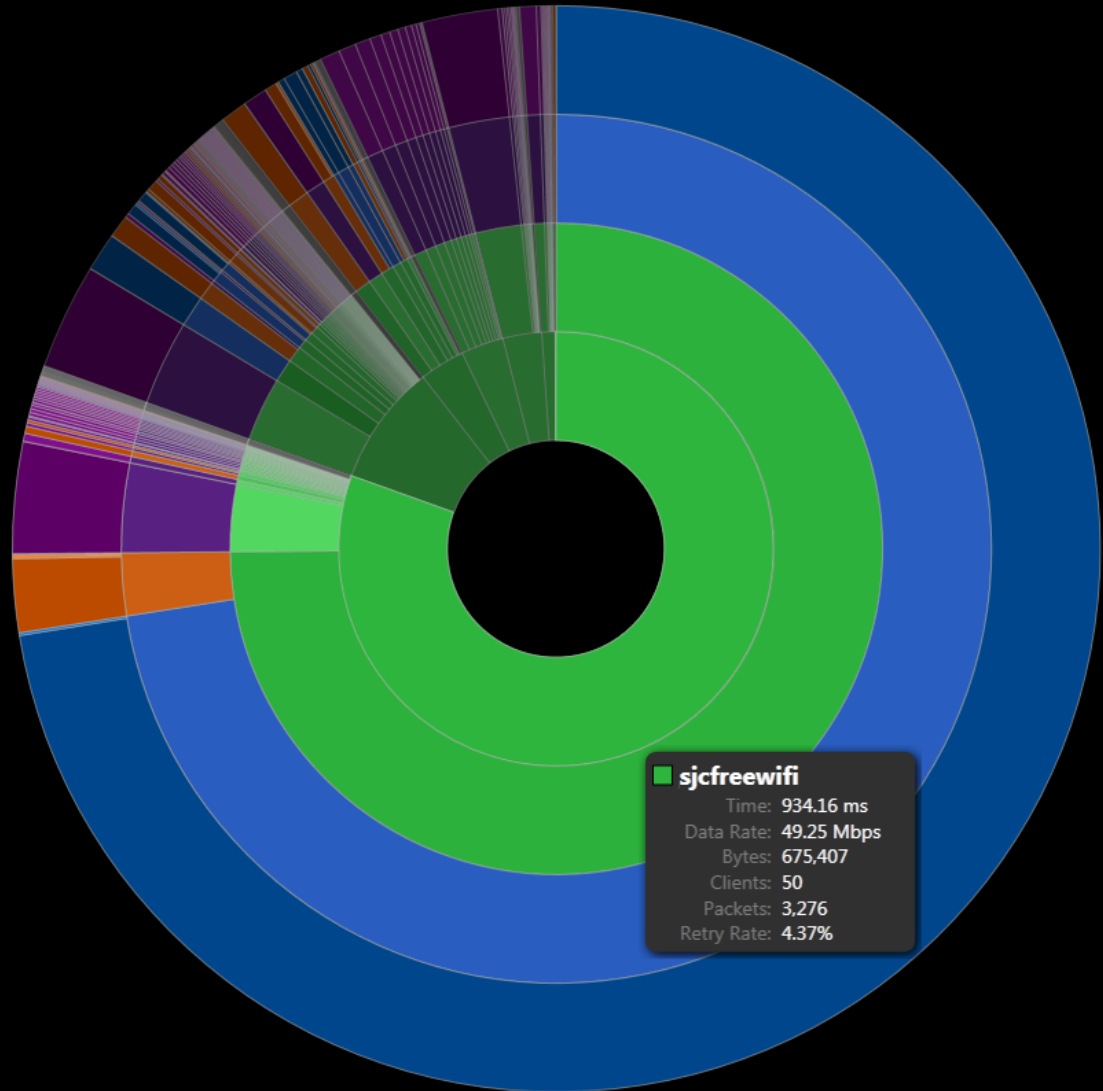


Packets vs. Bytes vs. Time

TIME ▶

BYTES

PACKETS ▶



Packet Analysis Demo

A large, light blue watermark logo is centered in the background. It features a circular design with three curved segments and the text "SHARKFEST '12" curved along the bottom.

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

all channels.pcap [Wireshark 1.6.8 (SVN Rev 42761 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

SubType	Data Rate	RSSI	No.	Time	Source	Destination	Protocol	Length	Info
11	2.0	6 db	3794	65.412738	Cisco-Li_5e1f:22	Apple_ai:53:77	802.11	60	Authentication, SN=0, FN=0, Flags=.....C
8	1.0	14 db	3795	65.412738	Cisco-Li_5e1f:22	Apple_ai:53:77	802.11	30	Beacon frame, SN=0, FN=0, Flags=.....C, BI=100, SSID=Metageek
8	1.0	14 db	951	9.849516	00:00:00:00:00:00	00:00:00:00:00:00	802.11	104	Beacon frame, SN=10, FN=0, Flags=.....C, BI=100, SSID=Broadcast
8	11.0	15 db	3454	61.738871	Aerohive_25:c2:50	00:00:00:00:00:00	802.11	394	Beacon frame, SN=10, FN=0, Flags=.....C, BI=100, SSID=Metageek
8	1.0	12 db	1296	12.061316	00:00:00:00:00:00	00:00:00:00:00:00	802.11	104	Beacon frame, SN=100, FN=0, Flags=.....C, BI=100, SSID=Broadcast
8	1.0	14 db	1298	12.081795	00:00:00:00:00:00	00:00:00:00:00:00	802.11	104	Beacon frame, SN=101, FN=0, Flags=.....C, BI=100, SSID=Broadcast
8	1.0	15 db	1443	12.977486	D-Link_27:dc:4d	00:00:00:00:00:00	802.11	252	Beacon frame, SN=1015, FN=0, Flags=.....C, BI=100, SSID=Metageek_QA_1
8	1.0	14 db	1596	14.001530	D-Link_27:dc:4d	00:00:00:00:00:00	802.11	252	Beacon frame, SN=1023, FN=0, Flags=.....C, BI=100, SSID=Metageek_QA_1
8	1.0	11 db	1603	14.104159	D-Link_27:dc:4d	00:00:00:00:00:00	802.11	252	Beacon frame, SN=1026, FN=0, Flags=.....C, BI=100, SSID=Metageek_QA_1
8	1.0	12 db	1617	14.308800	D-Link_27:dc:4d	00:00:00:00:00:00	802.11	252	Beacon frame, SN=1028, FN=0, Flags=.....C, BI=100, SSID=Metageek_QA_1
8	1.0	13 db	1302	12.123401	Actionte_7b:a8:c8	00:00:00:00:00:00	802.11	179	Beacon frame, SN=103, FN=0, Flags=.....C, BI=100, SSID=myqwest4135
8	1.0	12 db	1730	14.820646	D-Link_27:dc:4d	00:00:00:00:00:00	802.11	252	Beacon frame, SN=1033, FN=0, Flags=.....C, BI=100, SSID=Metageek_QA_1
8	1.0	14 db	1770	15.192671	D-Link_27:dc:4d	00:00:00:00:00:00	802.11	252	Beacon frame, SN=1038, FN=0, Flags=.....C, BI=100, SSID=Metageek_QA_1
8	1.0	13 db	1303	12.163900	00:00:00:00:00:00	00:00:00:00:00:00	802.11	104	Beacon frame, SN=104, FN=0, Flags=.....C, BI=100, SSID=Broadcast
8	1.0	14 db	1863	15.844728	D-Link_27:dc:4d	00:00:00:00:00:00	802.11	252	Beacon frame, SN=1043, FN=0, Flags=.....C, BI=100, SSID=Metageek_QA_1
8	1.0	13 db	1890	16.049549	D-Link_27:dc:4d	00:00:00:00:00:00	802.11	252	Beacon frame, SN=1045, FN=0, Flags=.....C, BI=100, SSID=Metageek_QA_1
8	1.0	13 db	1913	16.254262	D-Link_27:dc:4d	00:00:00:00:00:00	802.11	252	Beacon frame, SN=1047, FN=0, Flags=.....C, BI=100, SSID=Metageek_QA_1
8	1.0	2 db	3250	57.259508	cradlepo_12:78:9d	00:00:00:00:00:00	802.11	251	Beacon frame, SN=1052, FN=0, Flags=.....C, BI=100, SSID=RADIUS-TEST0
8	1.0	15 db	2057	17.070714	D-Link_27:dc:4d	00:00:00:00:00:00	802.11	252	Beacon frame, SN=1063, FN=0, Flags=.....C, BI=100, SSID=Metageek_QA_1
8	1.0	11 db	1305	12.204647	00:00:00:00:00:00	00:00:00:00:00:00	802.11	104	Beacon frame, SN=106, FN=0, Flags=.....C, BI=100, SSID=Broadcast
8	1.0	13 db	1307	12.225693	Actionte_7b:a8:c8	00:00:00:00:00:00	802.11	179	Beacon frame, SN=107, FN=0, Flags=.....C, BI=100, SSID=myqwest4135
8	1.0	12 db	1310	12.266171	00:00:00:00:00:00	00:00:00:00:00:00	802.11	104	Beacon frame, SN=108, FN=0, Flags=.....C, BI=100, SSID=Broadcast
8	1.0	11 db	1312	12.286488	00:00:00:00:00:00	00:00:00:00:00:00	802.11	104	Beacon frame, SN=109, FN=0, Flags=.....C, BI=100, SSID=Broadcast
8	1.0	13 db	957	9.871527	Actionte_7b:a8:c8	00:00:00:00:00:00	802.11	179	Beacon frame, SN=11, FN=0, Flags=.....C, BI=100, SSID=myqwest4135
8	1.0	14 db	1313	12.328119	Actionte_7b:a8:c8	00:00:00:00:00:00	802.11	179	Beacon frame, SN=111, FN=0, Flags=.....C, BI=100, SSID=myqwest4135
8	1.0	13 db	1316	12.368509	00:00:00:00:00:00	00:00:00:00:00:00	802.11	104	Beacon frame, SN=112, FN=0, Flags=.....C, BI=100, SSID=Broadcast
8	1.0	13 db	1318	12.389012	00:00:00:00:00:00	00:00:00:00:00:00	802.11	104	Beacon frame, SN=113, FN=0, Flags=.....C, BI=100, SSID=Broadcast
8	1.0	9 db	208	2.857527	Cisco-Li_32:e2:26	00:00:00:00:00:00	802.11	138	Beacon frame, SN=115, FN=0, Flags=.....C, BI=100, SSID=HalDavis
8	1.0	13 db	1321	12.430652	Actionte_7b:a8:c8	00:00:00:00:00:00	802.11	179	Beacon frame, SN=115, FN=0, Flags=.....C, BI=100, SSID=myqwest4135
8	1.0	13 db	1324	12.471051	00:00:00:00:00:00	00:00:00:00:00:00	802.11	104	Beacon frame, SN=116, FN=0, Flags=.....C, BI=100, SSID=Broadcast
8	1.0	7 db	76	1.237463	Netgear_32:12:92	00:00:00:00:00:00	802.11	288	Beacon frame, SN=118, FN=0, Flags=.....C, BI=100, SSID=smpl
8	1.0	6 db	297	1.954028	Netgear_32:12:92	00:00:00:00:00:00	802.11	288	Beacon frame, SN=1186, FN=0, Flags=.....C, BI=100, SSID=smpl
8	1.0	15 db	15	0.445776	Cisco-Li_32:e2:26	00:00:00:00:00:00	802.11	144	Beacon frame, SN=1187, FN=0, Flags=.....C, BI=100, SSID=5THCONFL
8	1.0	16 db	16	0.548793	Cisco-Li_32:e2:26	00:00:00:00:00:00	802.11	144	Beacon frame, SN=1188, FN=0, Flags=.....C, BI=100, SSID=5THCONFL
8	1.0	13 db	969	9.910921	00:00:00:00:00:00	00:00:00:00:00:00	802.11	104	Beacon frame, SN=12, FN=0, Flags=.....C, BI=100, SSID=Broadcast
8	1.0	15 db	304	15.844728	Aerohive_25:c2:50	00:00:00:00:00:00	802.11	394	Beacon frame, SN=12, FN=0, Flags=.....C, BI=100, SSID=Metageek

Header pad: 0
Header length: 26
Present Flags:
MAC timestamp: 2612402077267
Flags: 0x10
Data Rate: 1.0 Mb/s
Channel frequency: 2437 [8G 6]
Channel type: 802.11b (0x00a0)
SSID signal: -55 dbm
SSID noise: -84 dbm
Antenna: 0
SSID signal: 29 db
IEEE 802.11 Probe Request, Flags:C
Type/Subtype: Probe Request (0x04)
0000 00 00 1a 00 0f 18 00 00 53 3e 4c 3f 60 02 00 00S>?<...
0010 10 02 85 00 00 c9 ac 00 1d 40 00 00 00 ff ffD..E.....
0020 ff ff ff ff 44 88 84 45 45 97 ff ff ff ff ff ffD..E.....
0030 00 00 00 01 04 02 04 0b 16 32 08 0c 12 18 240h11111111\$
0040 30 48 60 2d 1a 0c 10 19 ff 00 00 00 00 00 000h11111111\$
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 000h11111111\$
File: C:\Users\MetaGeek\Desktop\all channels.pcap Packets: 3913 Displayed: 3913 Marked: 0 Load time: 0:00:181

Wireshark: Coloring Rules - Profile: Channel Colors

Edit Filter

List is processed in order until match is found

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

Order

Up

Move selected filter up or down

Down

OK Apply Cancel

Data Rate Profile

all channels.pcap [Wireshark 1.6.8 (SVN Rev 42761 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply

SubType	Data Rate	RSSI	No.	Time	Source	Destination	Protocol	Length	Info
36	5.5	10 dB	2851	36.204008	Apple_20:ea:08	ZyxeIcom_f1:3d:dc	802.11	54	Null Function (No data), SN=492, FN=0, Flags=.....TC
29	5.5	7 dB	2852	36.204239	Apple_20:ea:08 (RA)	Apple_20:ea:08 (RA)	802.11	40	Acknowledgement, Flags=.....C
36	5.5	8 dB	2853	36.205479	Apple_20:ea:08	ZyxeIcom_f1:3d:dc	802.11	54	Null Function (No data), SN=492, FN=0, Flags=.....R..TC
29	5.5	9 dB	2854	36.205726	Apple_20:ea:08 (RA)	Apple_20:ea:08 (RA)	802.11	40	Acknowledgement, Flags=.....C
29	5.5	8 dB	2855	36.249393	Apple_20:ea:08 (RA)	Apple_20:ea:08 (RA)	802.11	40	Acknowledgement, Flags=.....C
29	5.5	6 dB	2856	36.249982	Apple_20:ea:08 (RA)	Apple_20:ea:08 (RA)	802.11	40	Acknowledgement, Flags=.....C
36	5.5	8 dB	2864	36.364376	Apple_20:ea:08	ZyxeIcom_f1:3d:dc	802.11	54	Null Function (No data), SN=504, FN=0, Flags=.....TC
36	5.5	10 dB	2866	36.410233	Apple_20:ea:08	ZyxeIcom_f1:3d:dc	802.11	54	Null Function (No data), SN=505, FN=0, Flags=.....PR...TC
36	5.5	8 dB	2868	36.571526	Apple_20:ea:08	ZyxeIcom_f1:3d:dc	802.11	54	Null Function (No data), SN=507, FN=0, Flags=.....P...TC
29	5.5	7 dB	2869	36.571732	Apple_20:ea:08 (RA)	Apple_20:ea:08 (RA)	802.11	40	Acknowledgement, Flags=.....C
36	5.5	13 dB	2883	36.838382	Apple_20:ea:08	ZyxeIcom_f1:3d:dc	802.11	54	Null Function (No data), SN=511, FN=0, Flags=.....P...TC
36	5.5	9 dB	2884	36.898981	Apple_20:ea:08	ZyxeIcom_f1:3d:dc	802.11	54	Null Function (No data), SN=511, FN=0, Flags=.....PR...TC
36	5.5	6 dB	2889	37.019484	Apple_20:ea:08	ZyxeIcom_f1:3d:dc	802.11	54	Null Function (No data), SN=512, FN=0, Flags=.....R...TC
29	5.5	6 dB	3262	58.617995	SamsungE_b0:d0:e2	(RA) 802.11	40	Acknowledgement, Flags=.....C	
29	5.5	6 dB	3297	58.928614	SamsungE_b0:d0:e2	(RA) 802.11	40	Acknowledgement, Flags=.....C	
29	5.5	7 dB	3313	59.333743	SamsungE_b0:d0:e2	(RA) 802.11	40	Acknowledgement, Flags=.....C	
29	5.5	4 dB	3381	60.461118	SamsungE_b0:d0:e2	(RA) 802.11	40	Acknowledgement, Flags=.....C	
5	5.5	18 dB	3412	61.060997	Actionte_d7:43:e4	GemtekE-be:d5:b0	802.11	152	Probe Response, SN=526, FN=0, Flags=.....R...C, BI=200, SSID=Biggamehunter
32	5.5	11 dB	3513	62.496874	Pegatron_96:af:b6	LiteontE_1e:f2:4f	802.11	161	Data, SN=543, FN=0, Flags=.....p...R..F.C
5	5.5	12 dB	3547	63.140988	Actionte_d7:43:e4	LiteontE_1e:f2:4f	802.11	152	Probe Response, SN=548, FN=0, Flags=.....R...C, BI=200, SSID=Biggamehunter
29	5.5	5 dB	3591	63.531620	SamsungE_b0:d0:e2	(RA) 802.11	40	Acknowledgement, Flags=.....C	
5	5.5	11 dB	3598	63.595740	Actionte_d7:43:e4	IntelCor_1b:b4:5b	802.11	152	Probe Response, SN=555, FN=0, Flags=.....R...C, BI=200, SSID=Biggamehunter
5	5.5	10 dB	3615	63.673116	Actionte_d7:43:e4	IntelCor_1b:b4:5b	802.11	152	Probe Response, SN=556, FN=0, Flags=.....R...C, BI=200, SSID=Biggamehunter
29	5.5	10 dB	3660	63.941117	SamsungE_b0:d0:e2	(RA) 802.11	40	Acknowledgement, Flags=.....C	
29	5.5	7 dB	3811	65.580361	SamsungE_b0:d0:e2	(RA) 802.11	40	Acknowledgement, Flags=.....C	
29	5.5	9 dB	3848	65.887986	SamsungE_b0:d0:e2	(RA) 802.11	40	Acknowledgement, Flags=.....C	
36	52.0	24 dB	3322	59.485759	Apple_4a:fe:70	Cisco-L1_5e:1f:22	802.11	54	Null Function (No data), SN=1371, FN=0, Flags=.....P...TC
36	52.0	25 dB	3323	59.486113	Apple_4a:fe:70	Cisco-L1_5e:1f:22	802.11	54	Null Function (No data), SN=1371, FN=0, Flags=.....PR...TC
36	52.0	25 dB	3324	59.486356	Apple_4a:fe:70	Cisco-L1_5e:1f:22	802.11	54	Null Function (No data), SN=1371, FN=0, Flags=.....PR...TC
36	52.0	24 dB	3373	60.356127	Apple_4a:fe:70	Cisco-L1_5e:1f:22	802.11	54	Null Function (No data), SN=1372, FN=0, Flags=.....P...TC
36	52.0	24 dB	3378	60.407230	Apple_4a:fe:70	Cisco-L1_5e:1f:22	802.11	54	Null Function (No data), SN=1373, FN=0, Flags=.....P...TC
36	52.0	22 dB	3423	61.329114	Apple_4a:fe:70	Cisco-L1_5e:1f:22	802.11	54	Null Function (No data), SN=1375, FN=0, Flags=.....PR...TC
36	52.0	22 dB	3424	61.329232	Apple_4a:fe:70	Cisco-L1_5e:1f:22	802.11	54	Null Function (No data), SN=1375, FN=0, Flags=.....PR...TC
36	58.5	25 dB	3317	59.434617	Apple_4a:fe:70	Cisco-L1_5e:1f:22	802.11	54	Null Function (No data), SN=1370, FN=0, Flags=.....R...TC
36	58.5	24 dB	3318	59.436000	Apple_4a:fe:70	Cisco-L1_5e:1f:22	802.11	54	Null Function (No data), SN=1370, FN=0, Flags=.....R...TC
13	6.0	10 dB	656	7.948850	IntelCor_a6:c1:10	Cisco-L1_5a:b9:00	802.11	60	Action, SN=2017, FN=0, Flags=.....C
30	6.0	10 dB	657	7.948852	IntelCor_a6:c1:10	(BS)Cisco-L1_5a:b9:00 (RA) 802.11	46	CF-End	
30	6.0	9 dB	1460	13.265403	IntelCor_a6:c1:10	(BS)Cisco-L1_5a:b9:00 (RA) 802.11	46	CF-End	
28	6.0	26 dB	3320	59.443763	Apple_4a:fe:70 (RA)	Apple_4a:fe:70 (RA)	802.11	40	Clear-t
28	6.0	25 dB	3321	59.456264	Apple_4a:fe:70 (RA)	Apple_4a:fe:70 (RA)	802.11	40	Clear-t
32	6.0	10 dB	3792	65.373489	Apple_c0:60:ea	Broadcast	802.11	110	Data, S

Wireshark: Coloring Rules - Profile: Datarate Greens

Filter

```
0000 00 00 1a 00 0f 18 00 00 53 3e 4c 3f 60 02 00 00 .....0...S>L?...
0010 10 02 85 09 a0 00 c9 ac 00 1d 40 00 00 00 ff ff .....0...E...
0020 ff ff ff ff 44 08 84 45 45 9f ff ff ff ff ff .....0...E...
0030 90 00 00 00 01 04 02 04 0b 16 32 08 0c 12 18 24 .....2...$
0040 30 48 60 6c 2d 1a 0c 10 19 ff 00 00 00 00 00 00 .....0H 1...
0050 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
0060 03 01 07 d0 09 00 10 18 02 00 00 04 00 00 dd 1e .....3...
0070 00 90 4c 33 0c 10 19 ff 00 00 00 00 00 00 00 00 .....
0080 00 00 00 00 00 00 00 00 00 00 00 00 00 58 09 .....X...
0090 29 24 }
```

File: "C:\Users\MetaGeek\Desktop\all channel... Packets: 3913 Displayed: 3913 Marked: 0 Load time: 0.00.163

Wireshark: Coloring Rules - Profile: Datarate Greens

Edit Filter

List is processed in order until match is found

Name	String
DCERPC	dcerpc
Routing	hsrp 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
Beacon	wlan.fc.type_subtype == 0x08
Ack	wlan.fc.type_subtype == 0x18 or wlan.fc.type_subtype == 0x19 or wlan.fc.type...
Datarates 1 - 2 (Bright Green)	radiotap.datarate <= 2
Datarates 5.5 - 12	radiotap.datarate >= 5.5 and radiotap.datarate <= 12
Datarates 12 - 24	radiotap.datarate > 12 and radiotap.datarate <= 24
Datarates 24-54	radiotap.datarate > 24 and radiotap.datarate <= 54
Datarates 54+	radiotap.datarate > 54

Move selected filter up or down

OK Apply Cancel

Fin.

Visualizing 802.11 Wireshark Data

Tuesday, July 26th, 2012



Ryan Woodings

Chief Geek | MetaGeek



@metageek