
SHARKFEST '13
Wireshark Developer and User Conference
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**

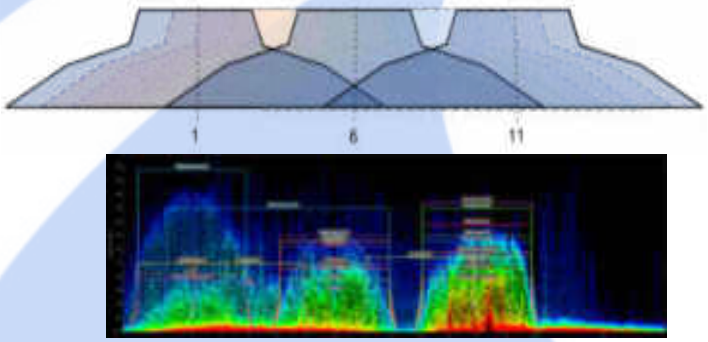
Additional Considerations

- 2.4 & 5 GHz Public ISM bands
- Non-Wi-Fi Transmitters
- Tx Power Restrictions
- Overlapping Channels

802.11 Wireless Medium

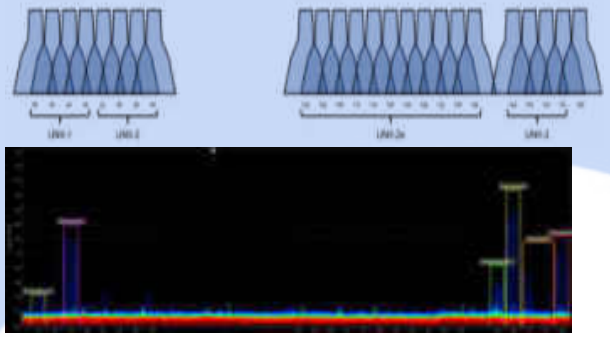
2.4 GHz

- 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:

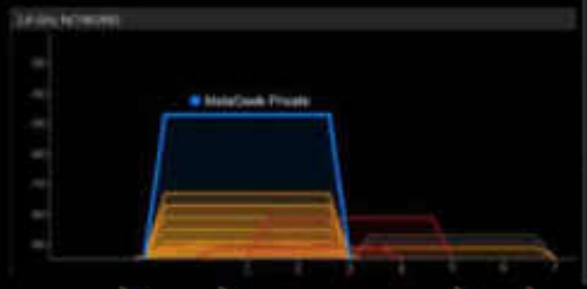
- Signal Strength of Access Points
- Visualize Co-Channel & Overlapping Networks

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.

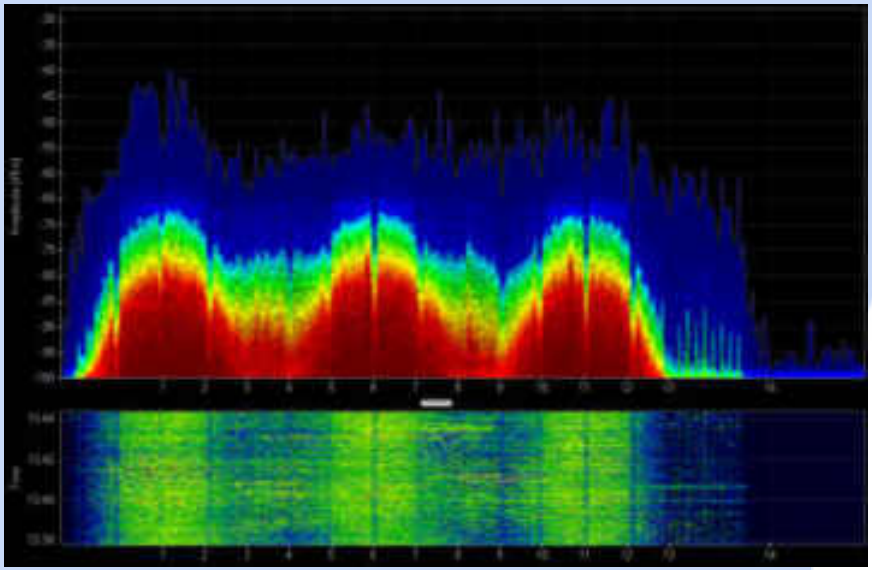
Network on the Same Channel

Your Starred Network

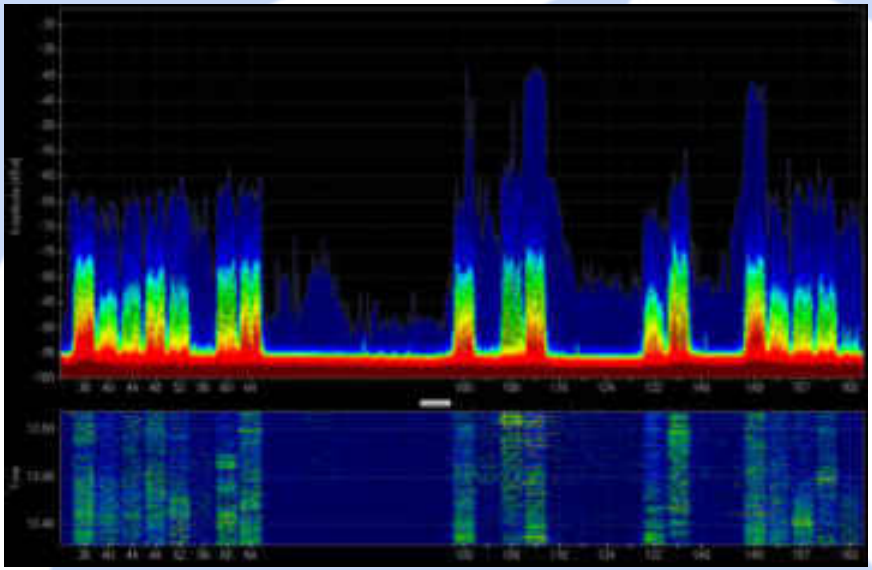
Network on an

Visualizing Channel Density

INTEROP 2013



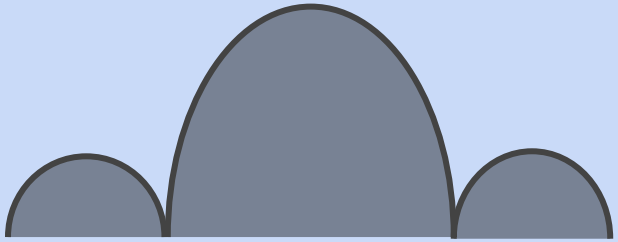
2.4 GHz



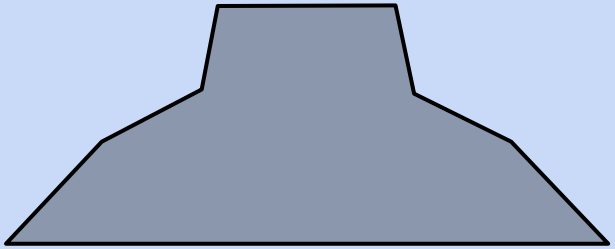
5 GHz

Visualizing Wi-Fi Patterns

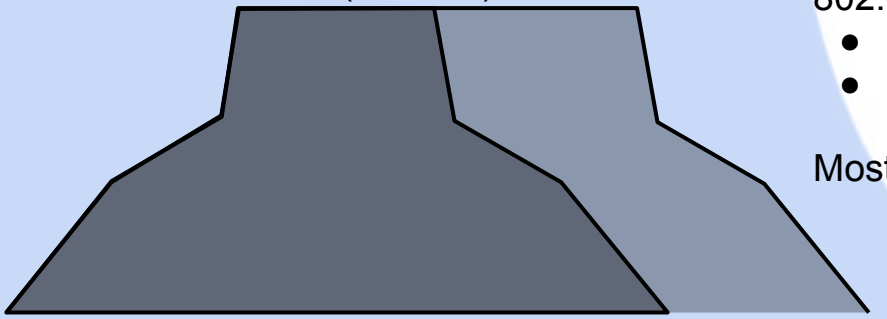
Phase Shift Keying Modulation



OFDM (20 MHz)



OFDM (40 MHz)



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.

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.

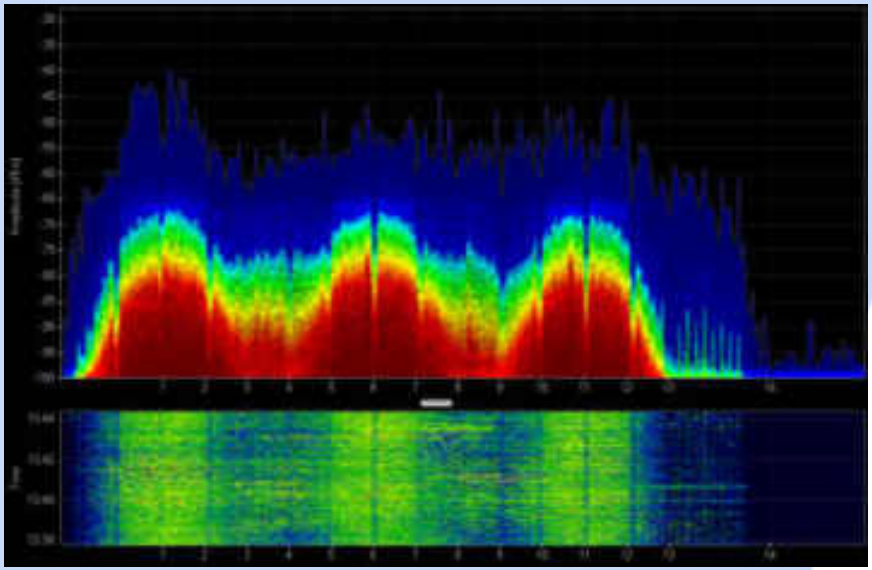
802.11n

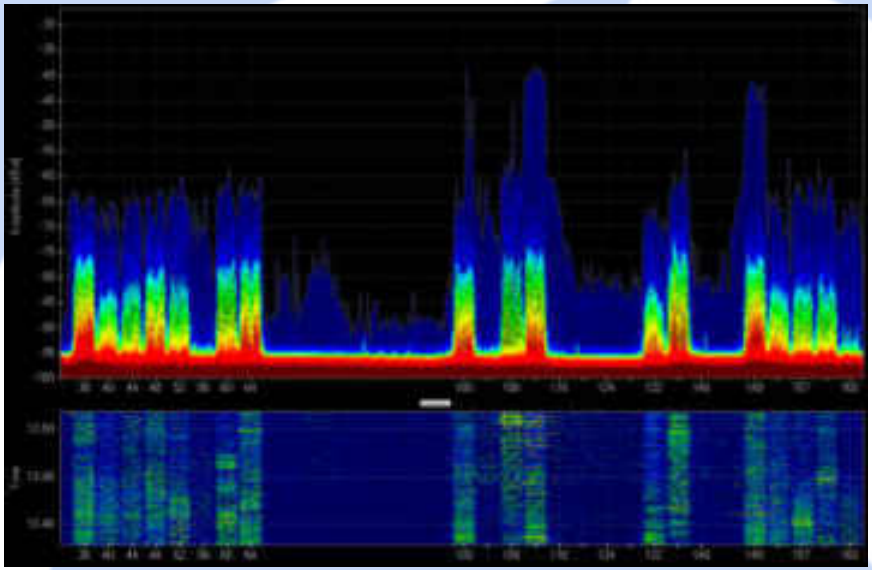
- 13.5 - 600 Mbps
- 2.4 or 5 GHz

Most commonly used to transmit Data Frames.

Spectrum Pattern Diagnosis

INTEROP 2013

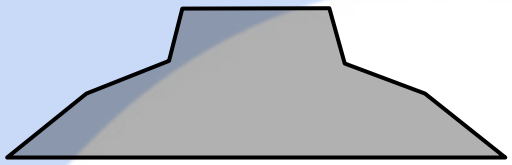




2.4 GHz
(Very Dense)

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

5 GHz
(Less Dense - Unused Channels)



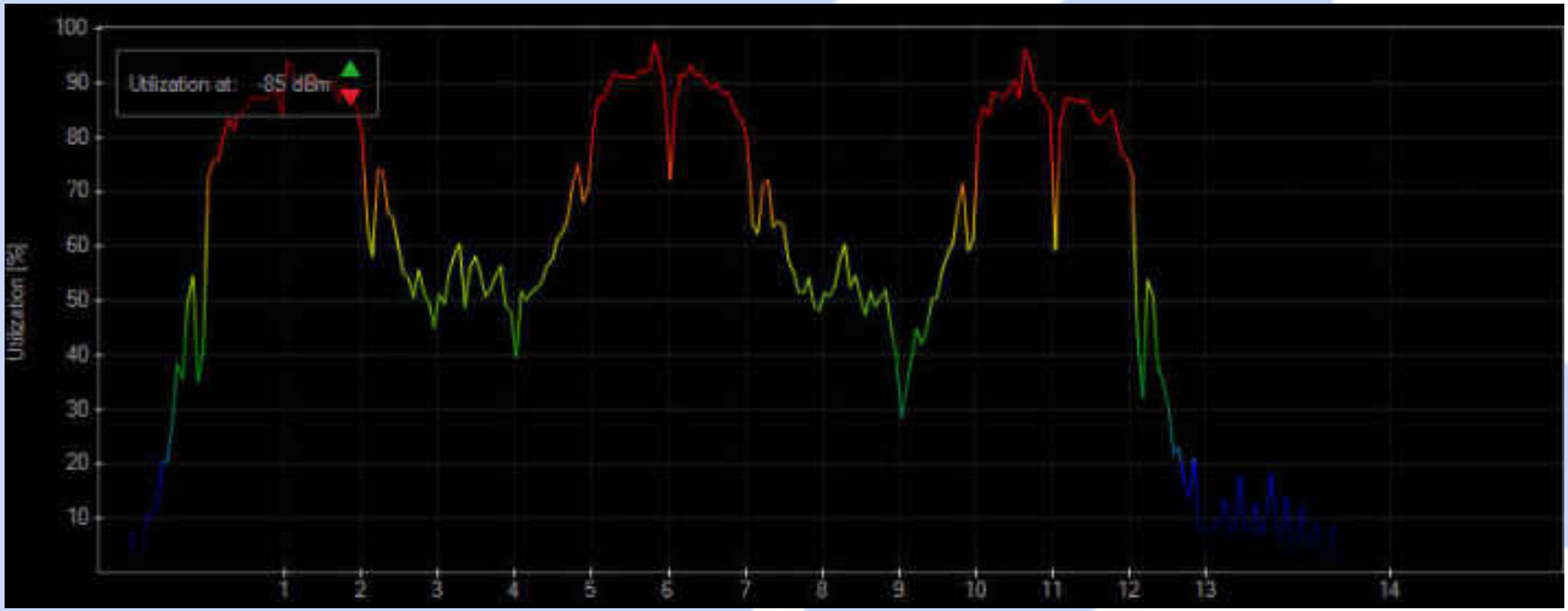
Minimum data rate is 6 Mbps.

Legacy Data Rates - So What?

Wi-Fi stations are very polite.

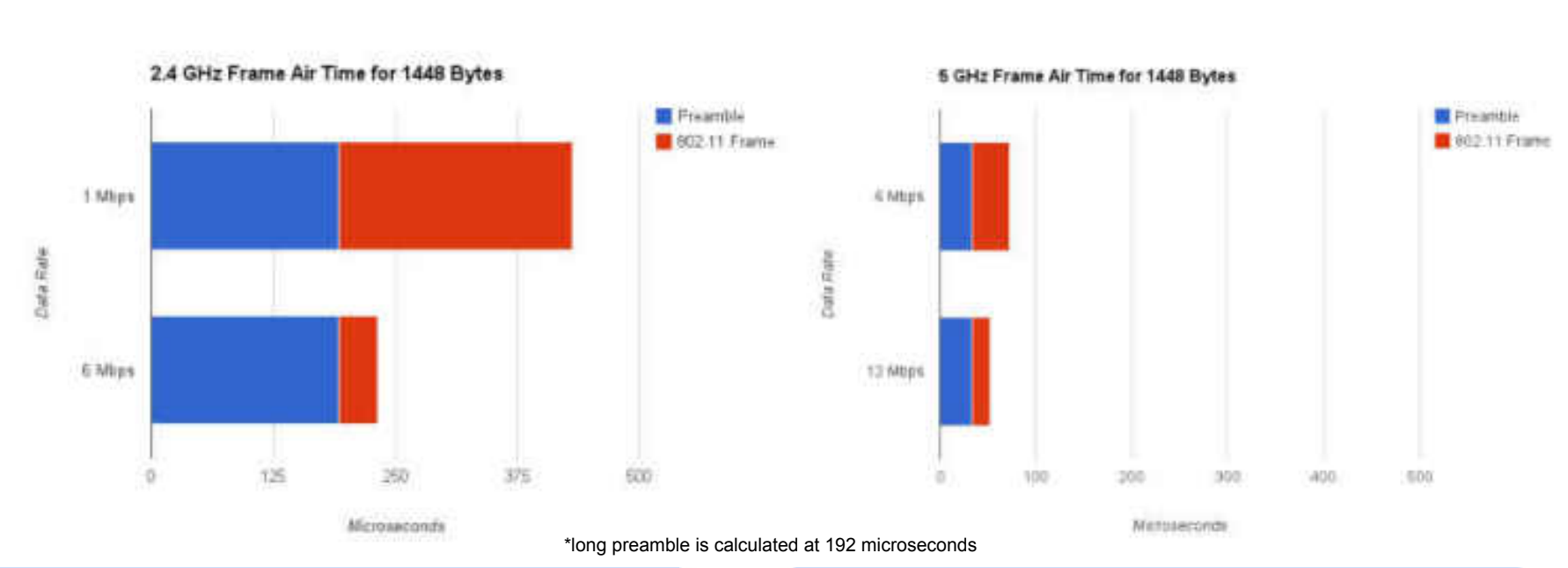
They will back off for any transmission above -85dBm.

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



*long preamble is calculated at 192 microseconds

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

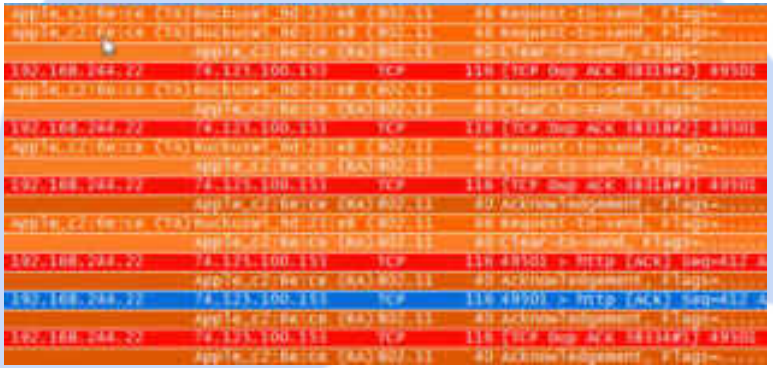
This is used for synchronization and collision avoidance.

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.

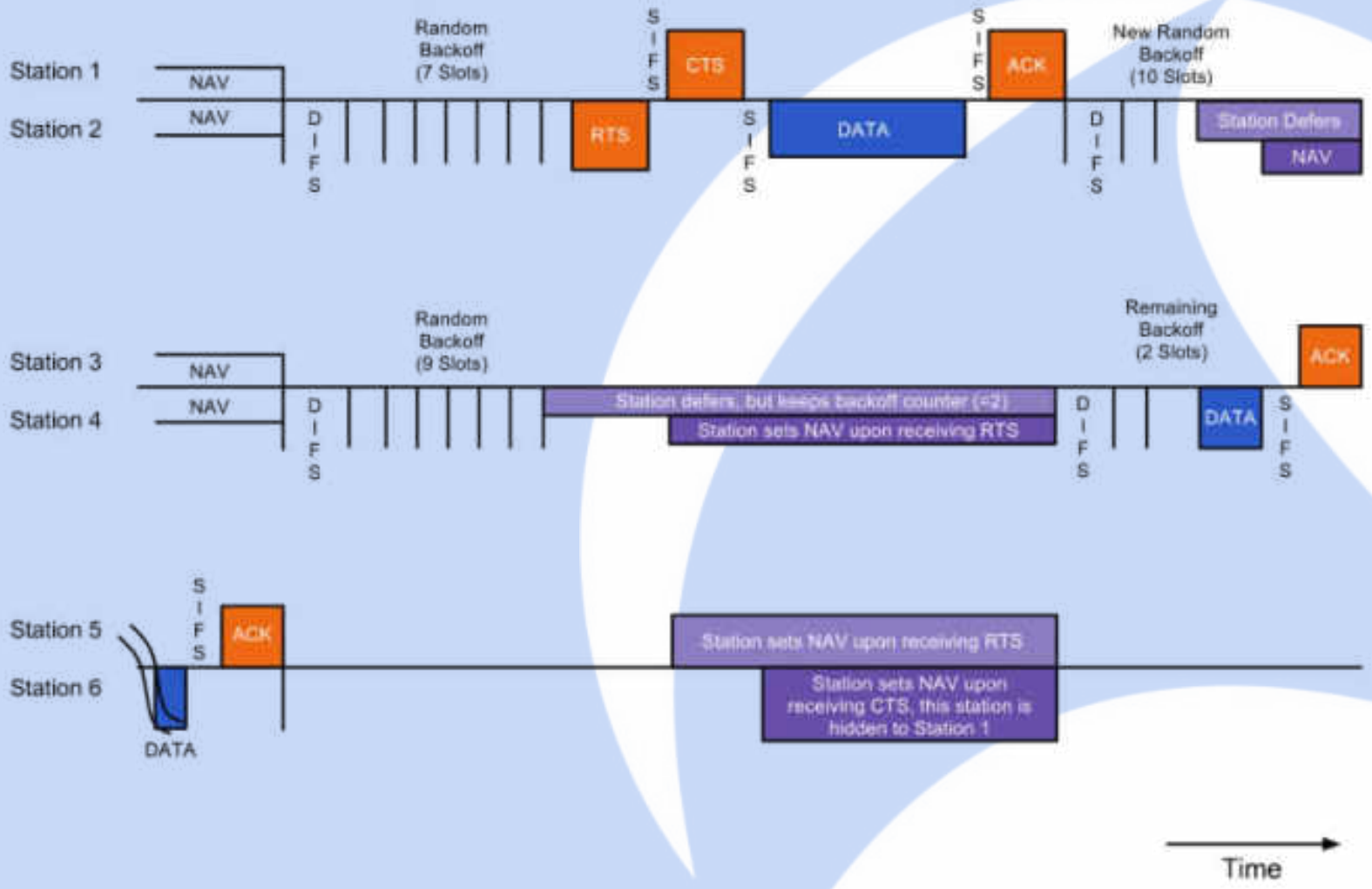
ERP Protection

```
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
```

Subframe T	Air Time	Bytes	Packets	Retry Rate
QoS Data	18,338.40	19,053,944	25,836	39
RTS	2,388.45	150,820	7,541	0
ACK	1,237.91	121,562	8,683	0
Block ACK	66.42	97,088	3,034	0
CTS	751.70	53,340	3,810	0
QoS Null	31.81	2,130	71	34
Probe Resp	10.01	2,034	9	44
Probe Requ	16.13	1,652	14	0
Action	0.52	39	1	0



Arbitration and RTS / CTS

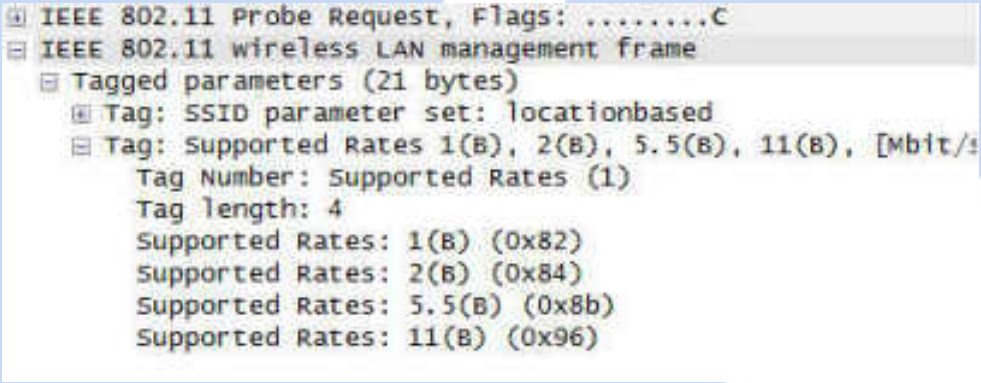


How to Find Legacy Devices

Look in the Probe Requests!

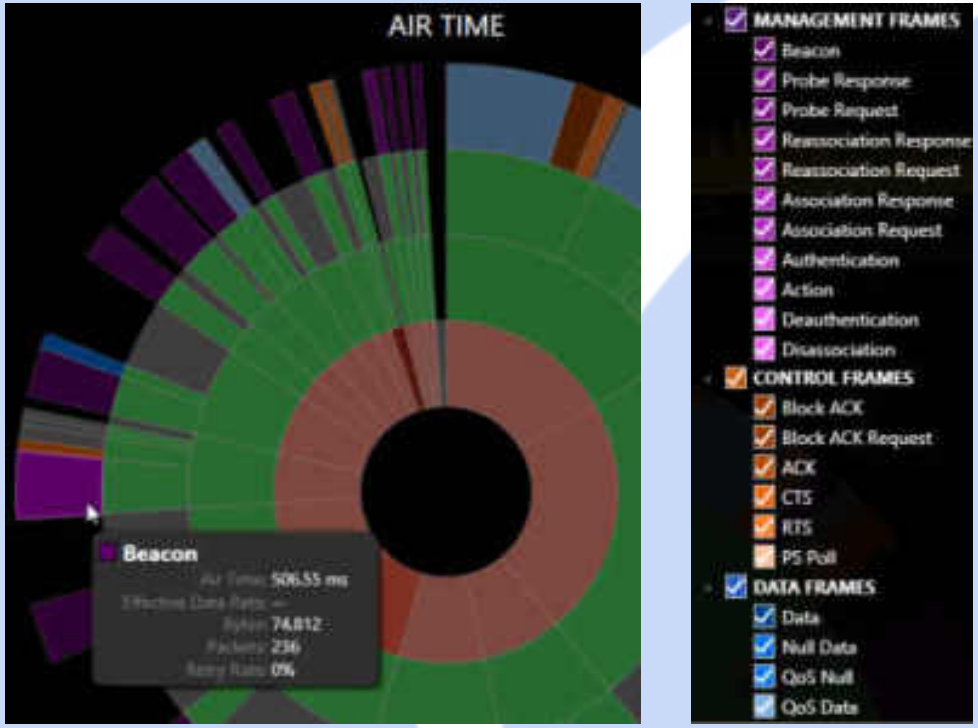
wlan.fc.type_subtype == 0x04

Learn all about what the client device supports: data rates, RF bands, beamforming and security.



802.11 Overhead

INTEROP 2013 Channel 11

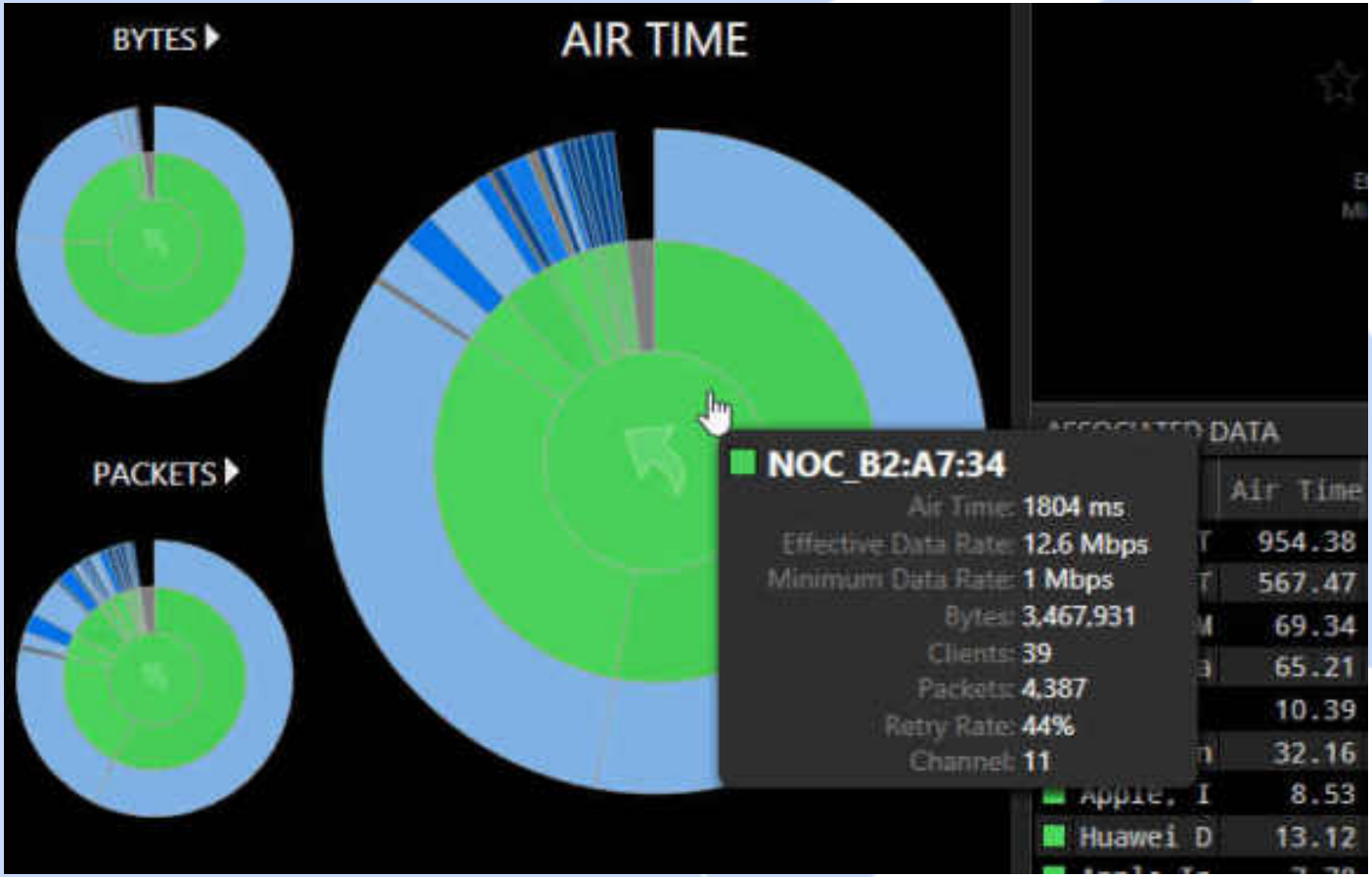


Co-Channel Interference and 802.11 overhead are excluded when troubleshooting wireless issues over the wire.

802.11 Overhead is all Management and Control Frames.

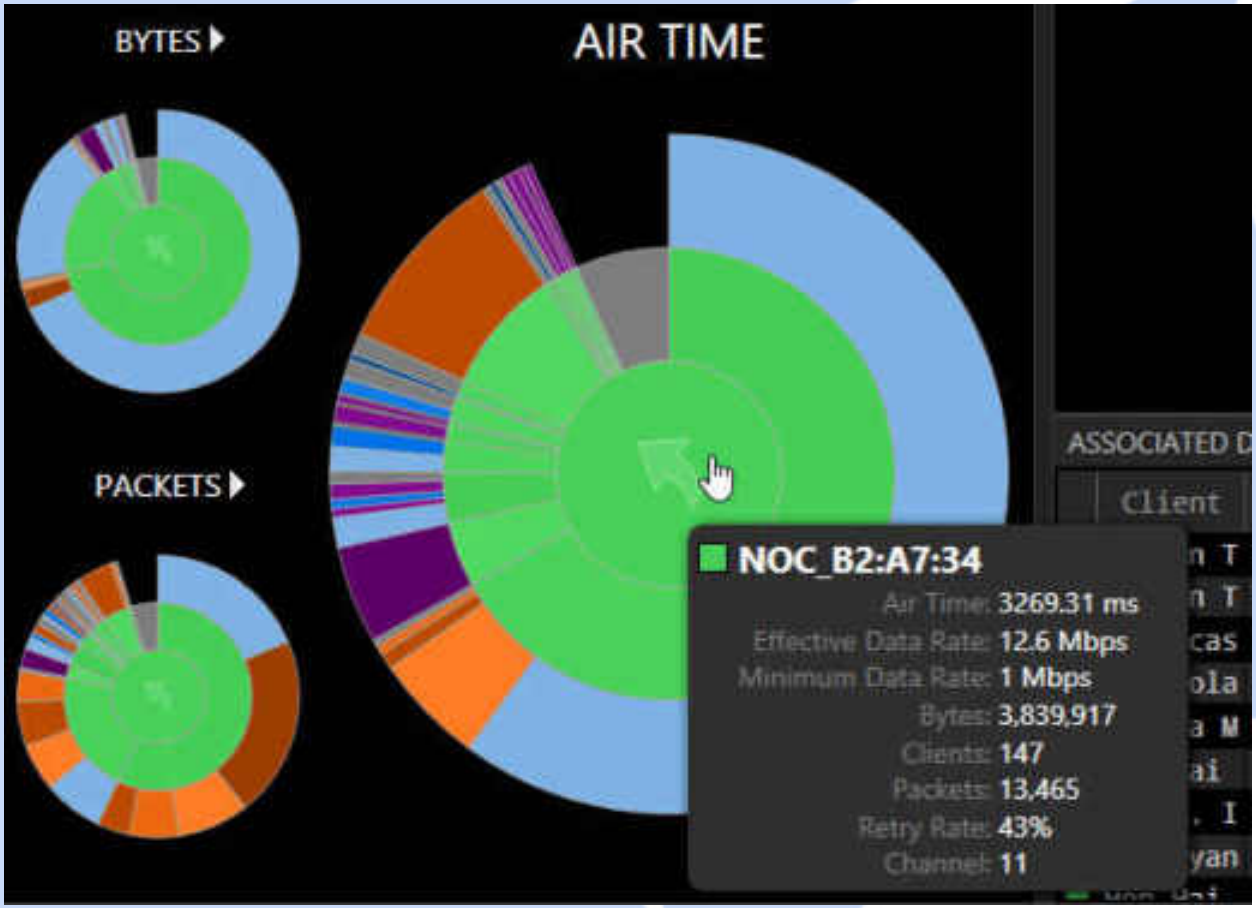
What Comes Through the Wire

INTEROP 2013 SSID "NOC"



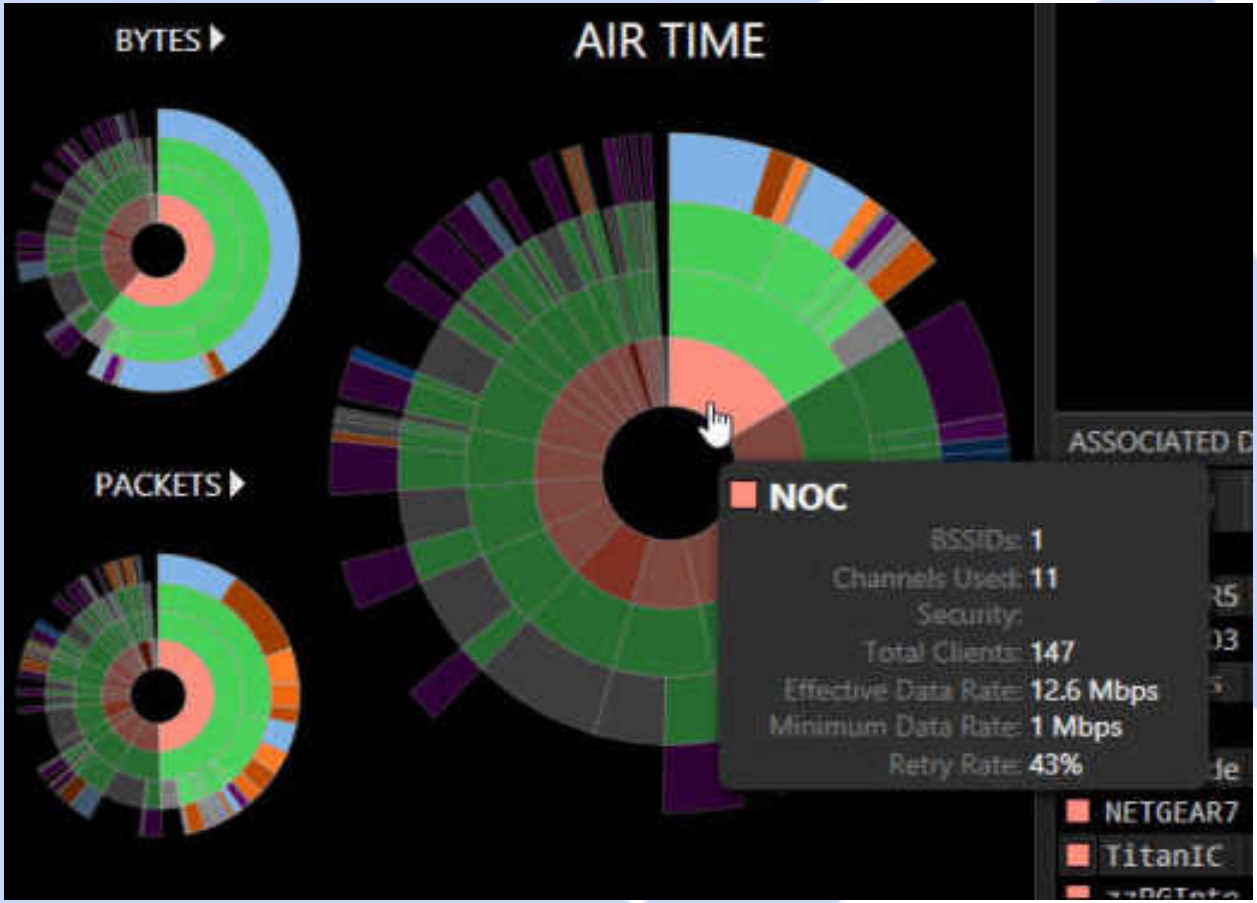
Add the 802.11 Overhead for BSSID

INTEROP 2013 SSID "NOC"



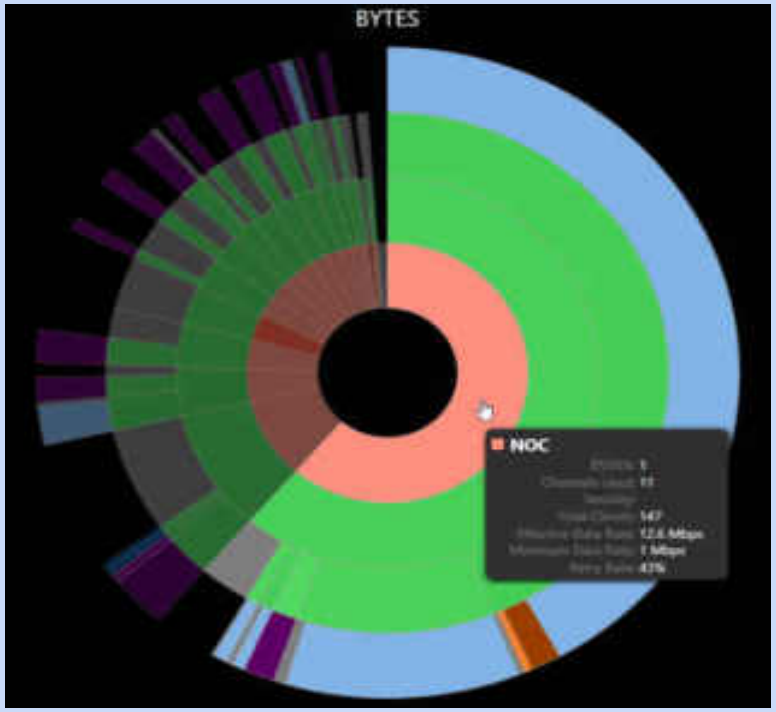
Add the Competing Traffic on Channel 11

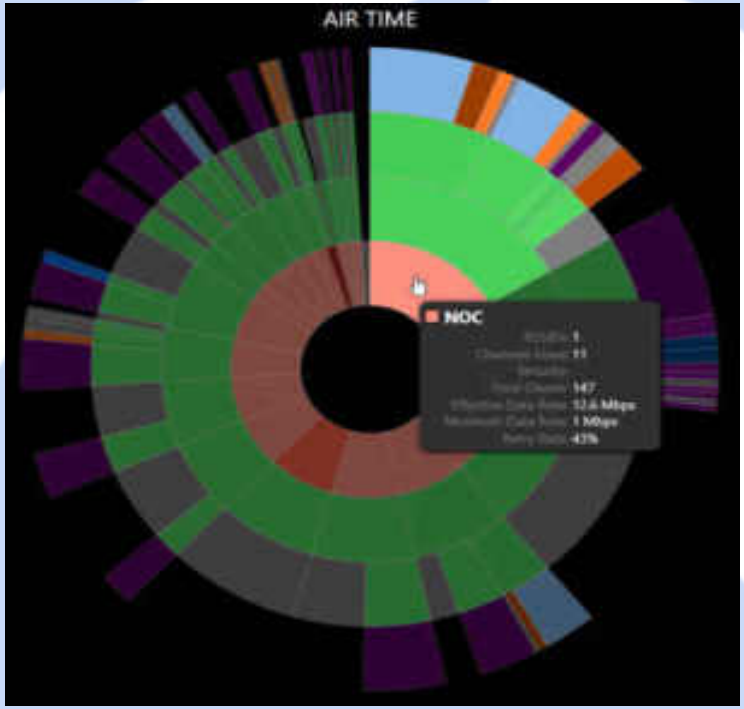
INTEROP 2013 SSID "NOC"



Sharing is Caring?

INTEROP 2013 Channel 11





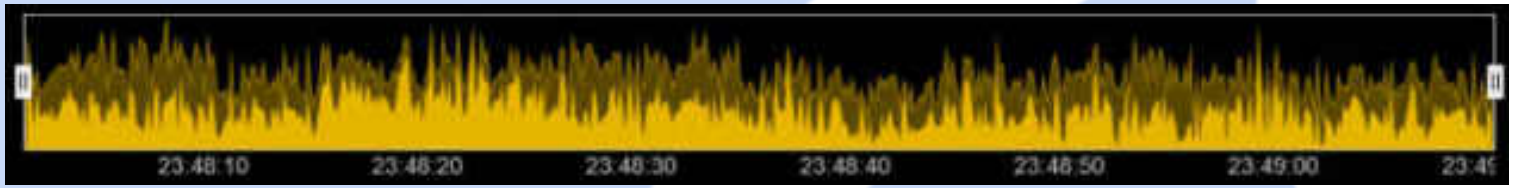
Even though stations within "NOC" easily sent the most bytes, they only contributed to a small portion of the Air Time saturation.

What is all of the other traffic?

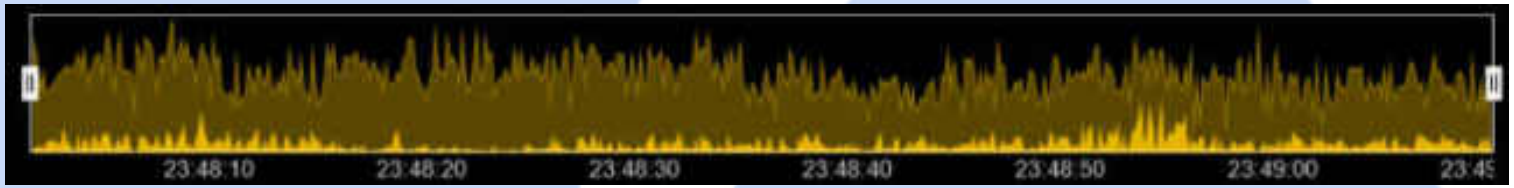
802.11 Air Time of Legacy Data Rates

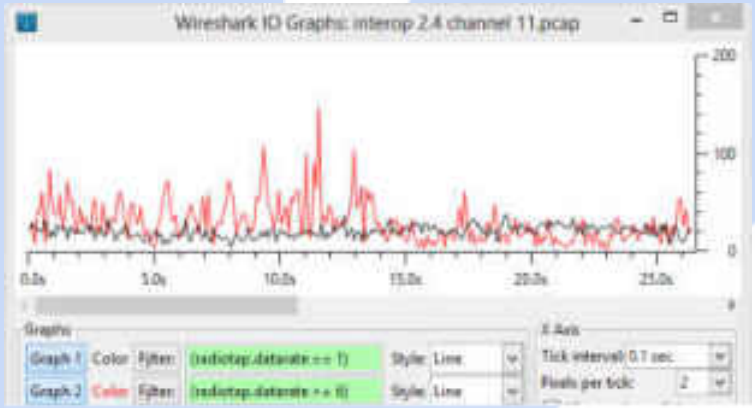
INTEROP 2013 Channel 11

1 Mbps



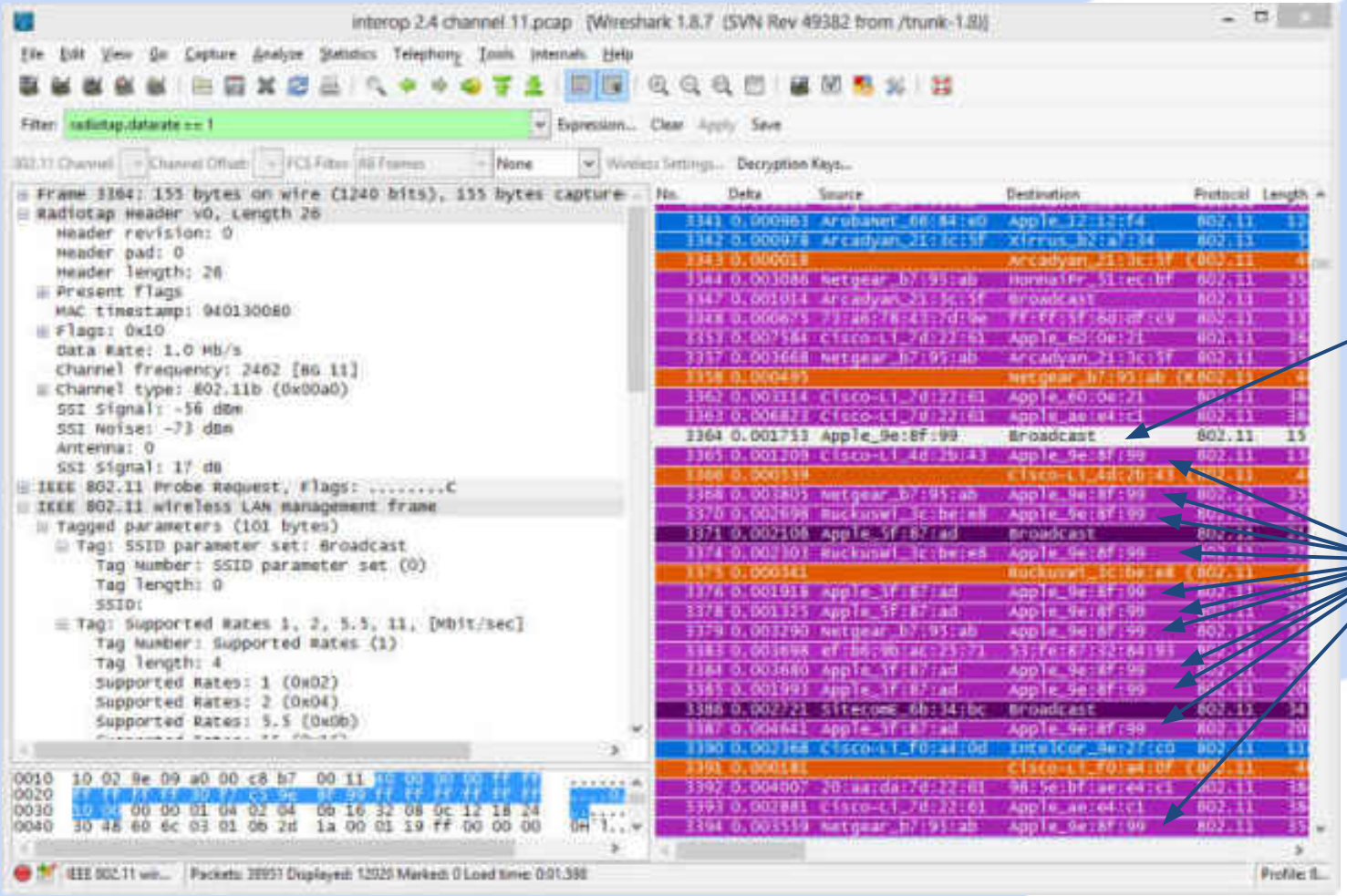
>= 6 Mbps





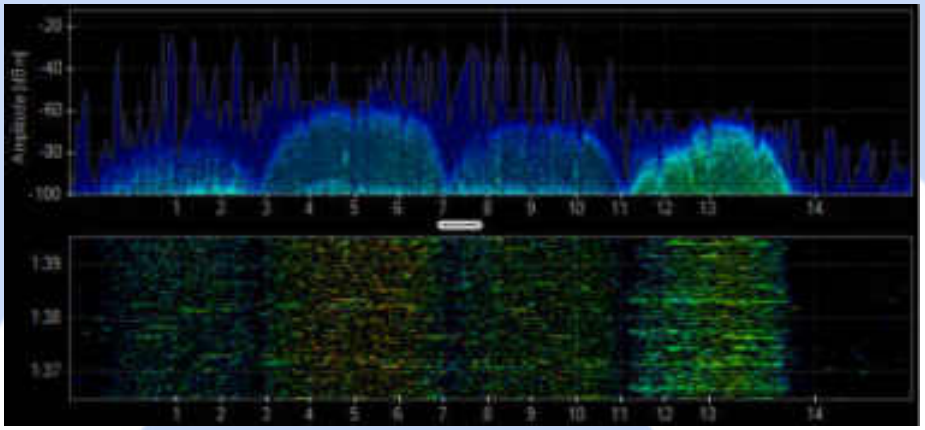
What are all of the 1 Mbps frames?

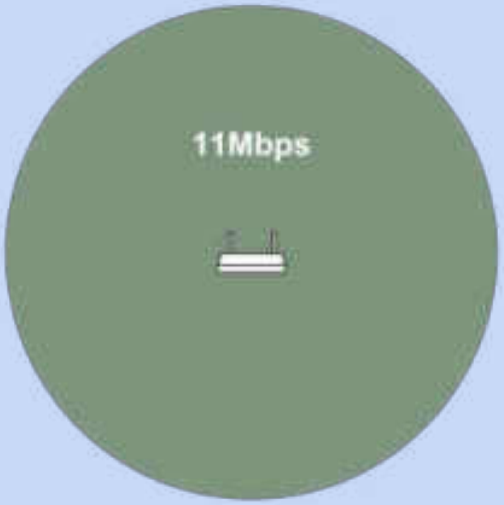
Probe Requests and Responses



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.

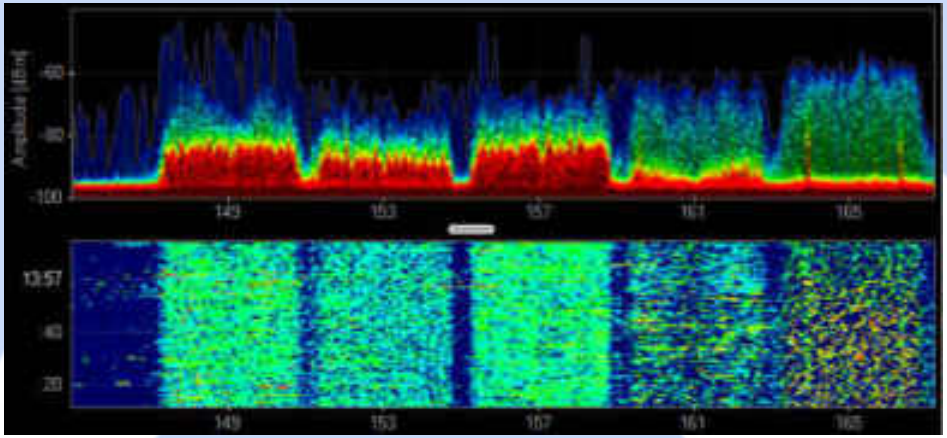





```
Frame 19665: 185 bytes on wire (1480 bits), 185 bytes captured (1480 bits)
Radiotap Header v0, Length 26
    Header revision: 0
    Header pad: 0
    Header length: 26
  Present flags: 0x0000186f
    MAC timestamp: 354203615
  Flags: 0x10
    Data Rate: 1.0 Mb/s
    Channel frequency: 2412 [BG 1]
  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

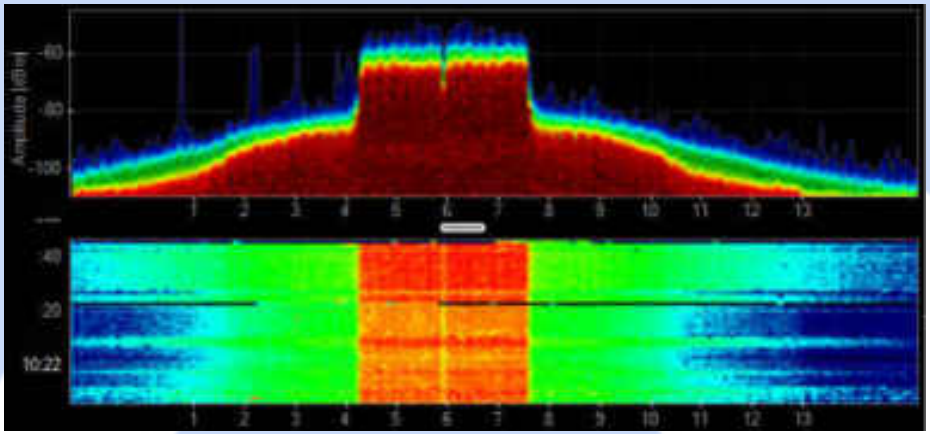
- 5 GHz-only
- 20 MHz Wide
- 6-54 Mbps
- OFDM Modulation




```
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

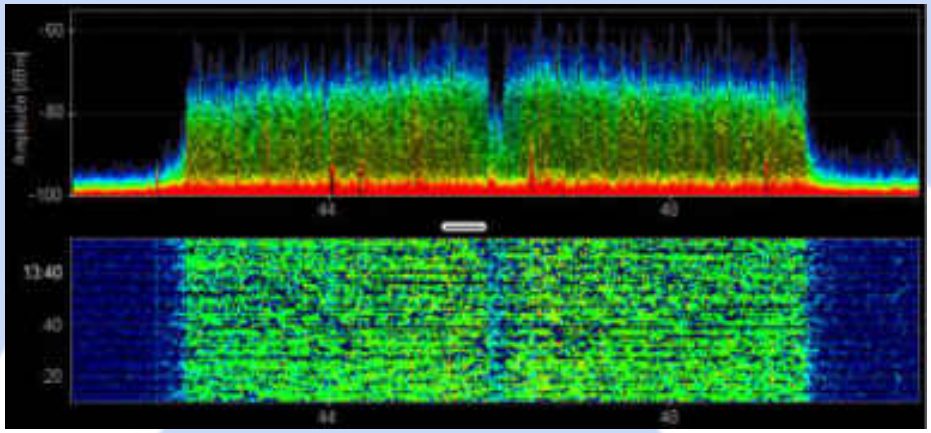
- 2.4 GHz-only
- 20 MHz Wide
- 6-54Mbps
- ERP-OFDM Modulation

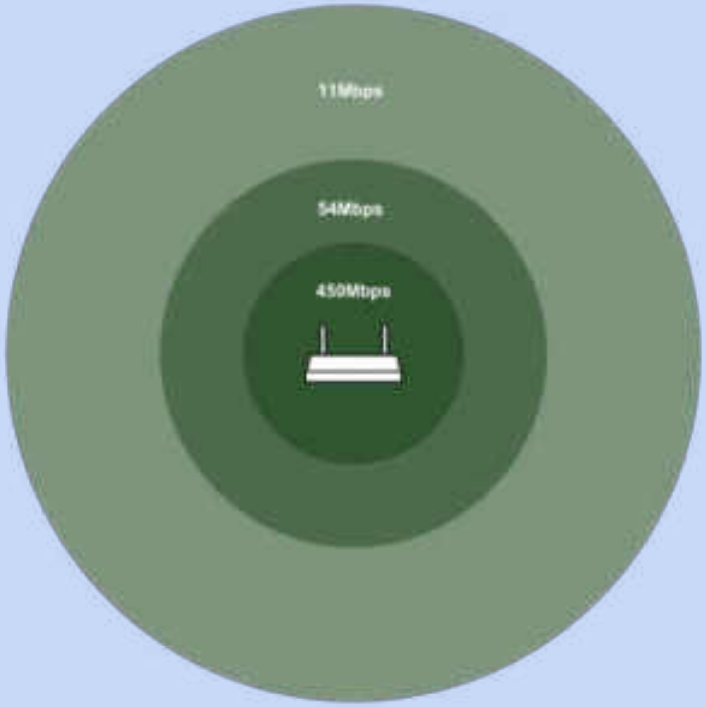



```
Radiotap Header v0, Length 26
    Header revision: 0
    Header pad: 0
    Header length: 26
  Present flags: 0x0000186f
    MAC timestamp: 266566899
  Flags: 0x10
    Data Rate: 52.0 Mb/s
    Channel frequency: 2412 [BG 1]
  Channel type: 802.11g (pure-g) (0x00c0)
      .... .... ...0 .... = Turbo: 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

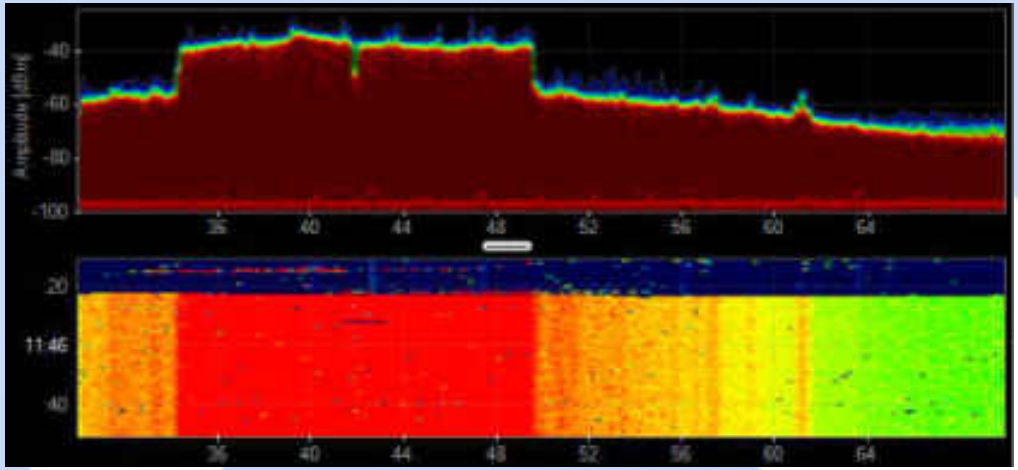


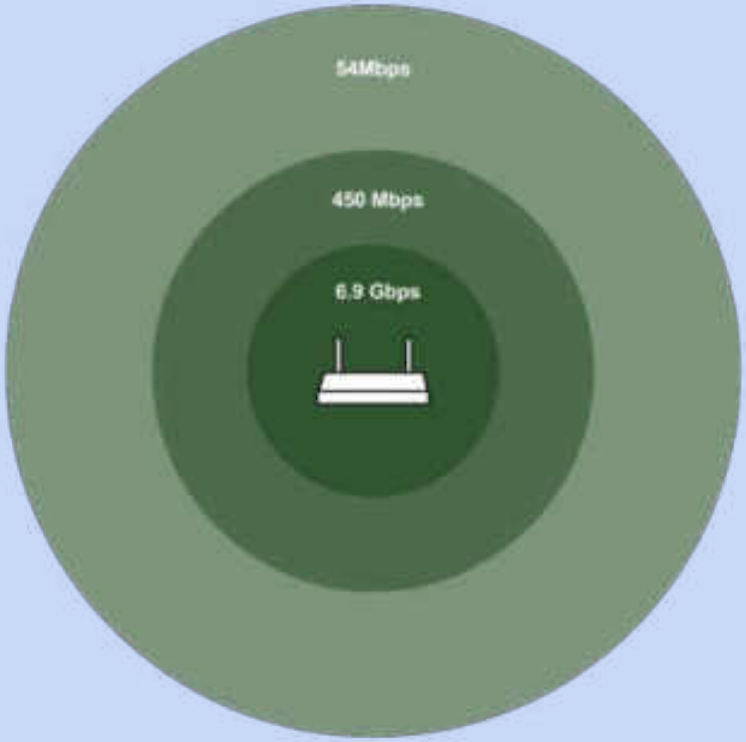



```
MCS information
  Known MCS information: 0x1f
    .... ..00 = Bandwidth: 20 MHz (0)
    .... .0.. = Guard interval: long (0)
    .... 1... = Format: greenfield (1)
    ...0 .... = FEC: BCC (0)
    MCS index: 5
  [Data Rate: 52.0 Mb/s]
IEEE 802.11 QoS Data, Flags: .p....F.
```

802.11ac

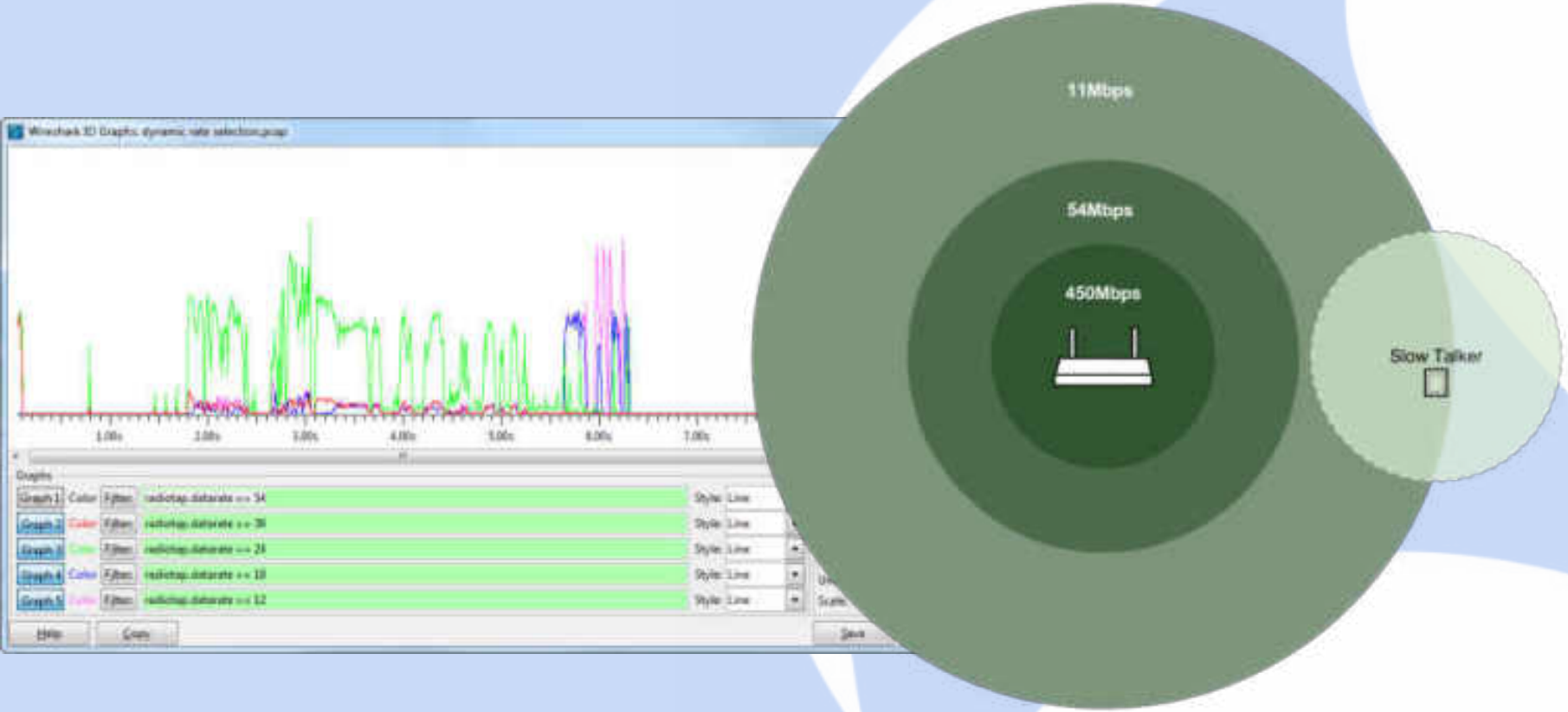
- 5 GHz
- 20-160 MHz Wide
- 6 Mbps - 6.9 Gbps
- OFDM Modulation





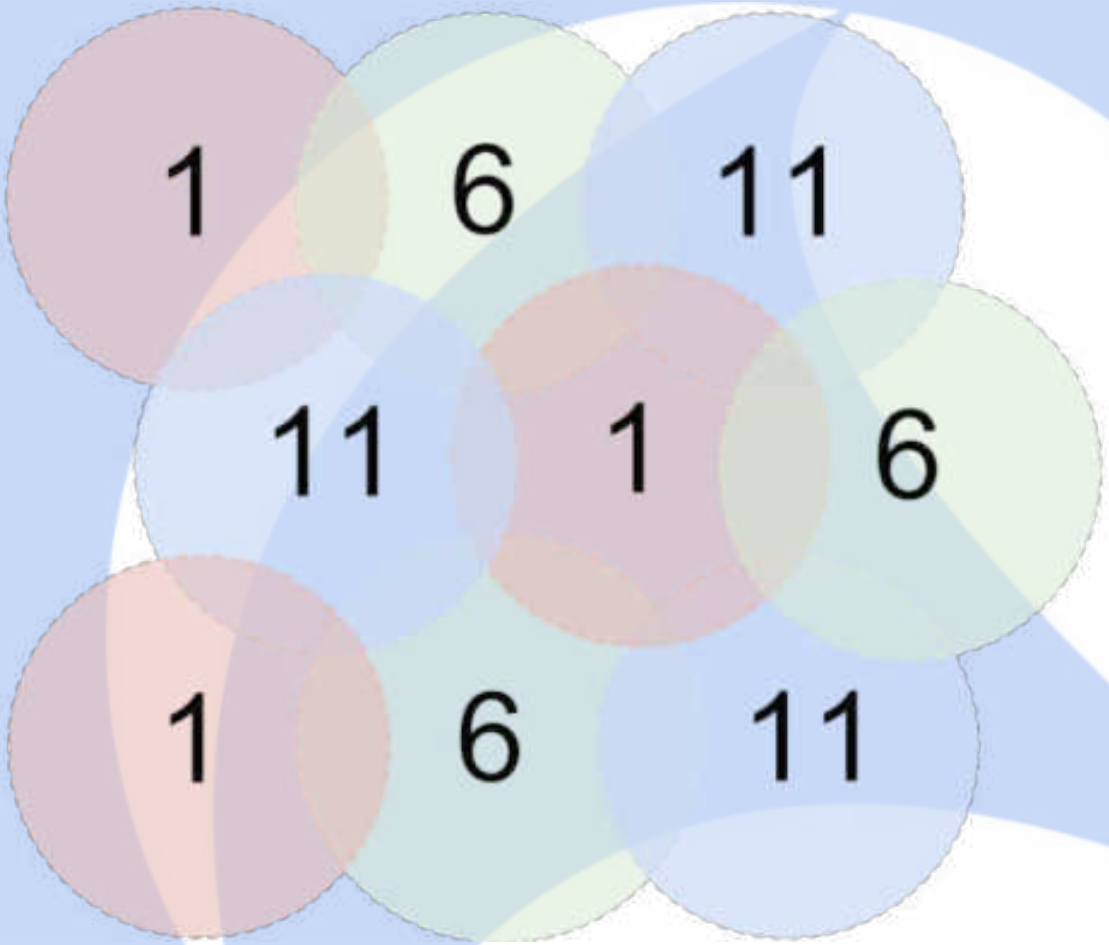
Dynamic Rate Switching

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



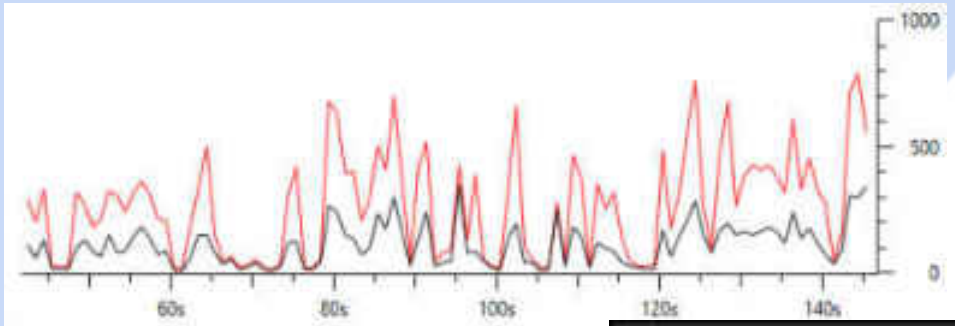
Reduce Co-Channel Interference

Channel
Antenna Pattern
Physical Barriers
Transmit Power



Measuring Retransmissions

(wlan.fc.type == 2) && (wlan.fc.retry == 1)



Graphs

Graph 1 Color Filter: (wlan.fc.type == 2) && (wlar Style: Line

Graph 2 Color Filter: wlan.fc.type == 2 Style: Line

Wireshark: Coloring Rules - Profile: 802.11

List is processed in order until match is found

String

wlan.fc.retry == 1

wlan.fc.type_subtype == 0x0a

wlan.fc.type_subtype == 0xd

wlan.fc.type_subtype == 8

wlan.fc.type_subtype == 5

wlan.fc.type_subtype == 0

wlan.fc.type_subtype == 4

Move selected filter up or down

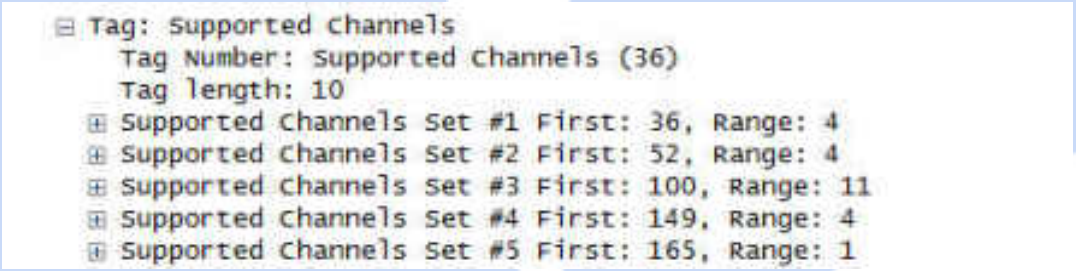
Client	Air Time	Bytes	Effective	Retry Rate
Apple, Inc._00:0A:02	1,437.79	7,202,204	23.8	38
Apple, Inc._00:41:00	5,022.28	6,069,674	1.7	22
Apple, Inc._00:88:03	1,217.38	5,742,861	1.3	24
Apple, Inc._00:8B:03	2,612.96	5,670,300	3.2	15
Apple, Inc._00:3D:03	1,081.03	5,020,056	26.8	15
Apple, Inc._00:93:03	2,506.89	4,393,883	2.5	30
Apple, Inc._00:07:00	607.53	3,604,828	34.5	9
Apple, Inc._00:09:00	396.99	1,919,950	2.9	45

5 GHz Channel Mysteries (DFS)

How do I know what 5 GHz channels my client device supports?

Look in the Association Requests!

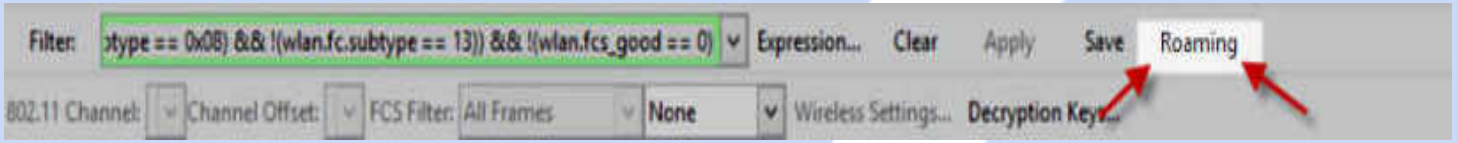
wlan.fc.type_subtype == 0x00



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!

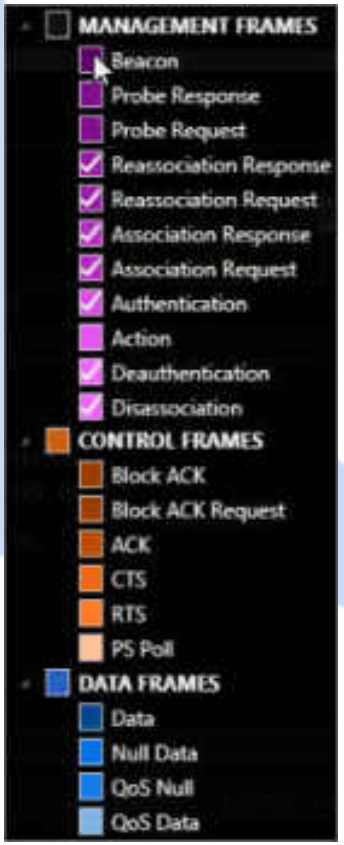


(((!(wlan.fc.type == 1)) && !(wlan.fc.type == 2)) && !(wlan.fc.type_subtype == 0x08) && !(wlan.fc.subtype == 13)) && !(wlan.fcs_good == 0)

Modify the Filter to Follow a Specific Station

(((((!(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

Download

Trial software available for learning:

www.metageek.com

Fin.

Trent Cutler

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