metageek

Wireless Packet Analysis with

metageek

EyeP.A.

Introduction

Joel Crane, CWNA, CWAP

Human Interface (Training and Support)

Contact: support.metageek.com

Twitter: @FuelCellWiFi

metageek

Housekeeping

Questions?

Feel free to use the Question tool if you have a question or comment that relates to the presentation

Audio or Video Problems?

If you experience audio or video problems, it's not you. It's me. Let me know with the question tool.

Webinar Recording

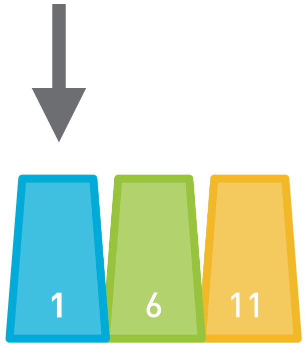
This webinar will be available for offline viewing within 24 hours of the end of the presentation.

Search for **Wireless Packet Analysis Webinar** on our knowledgebase at: support.metageek.com

Dual-Band Wi-Fi

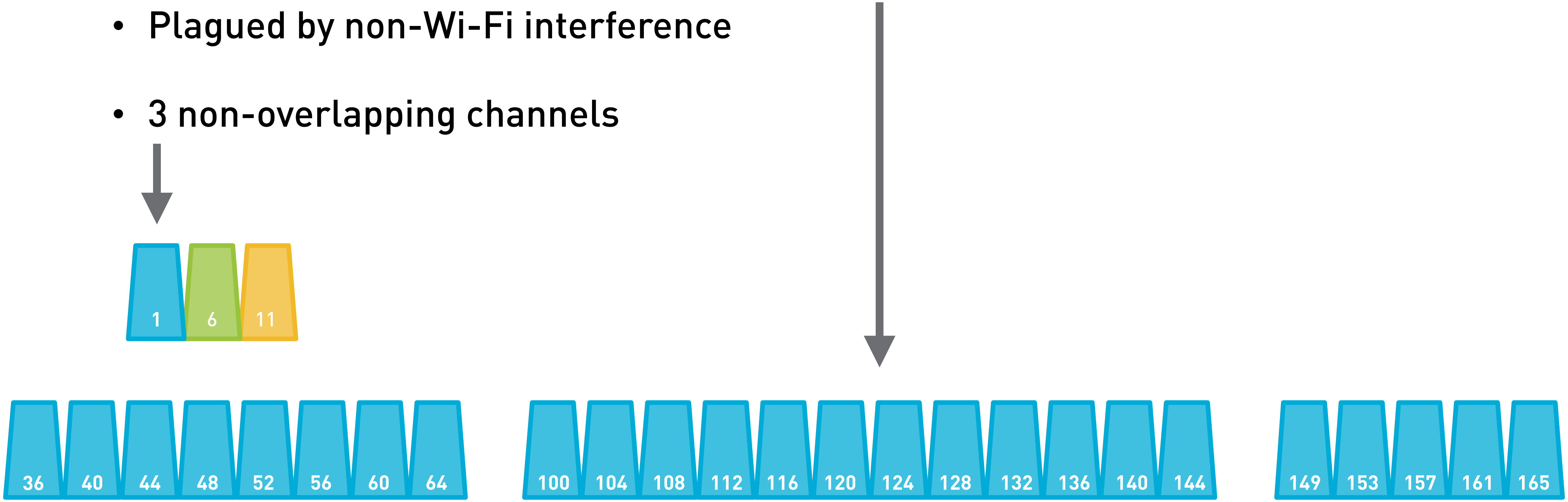
2.4 GHz (802.11b/g/n)

- Greater Range (~300 ft)
- Universal Compatibility
- Congested with Wi-Fi
- Plagued by non-Wi-Fi interference
- 3 non-overlapping channels



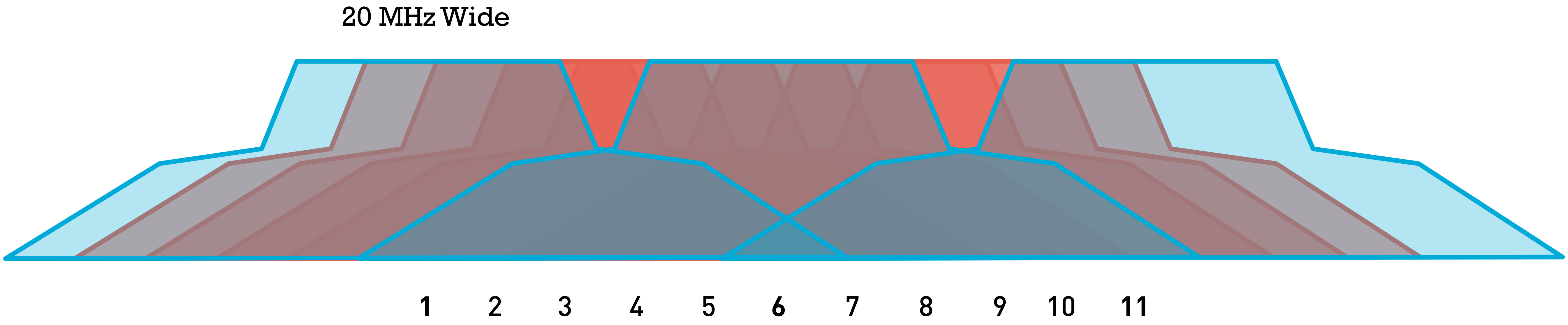
5 GHz (802.11a/n/ac)

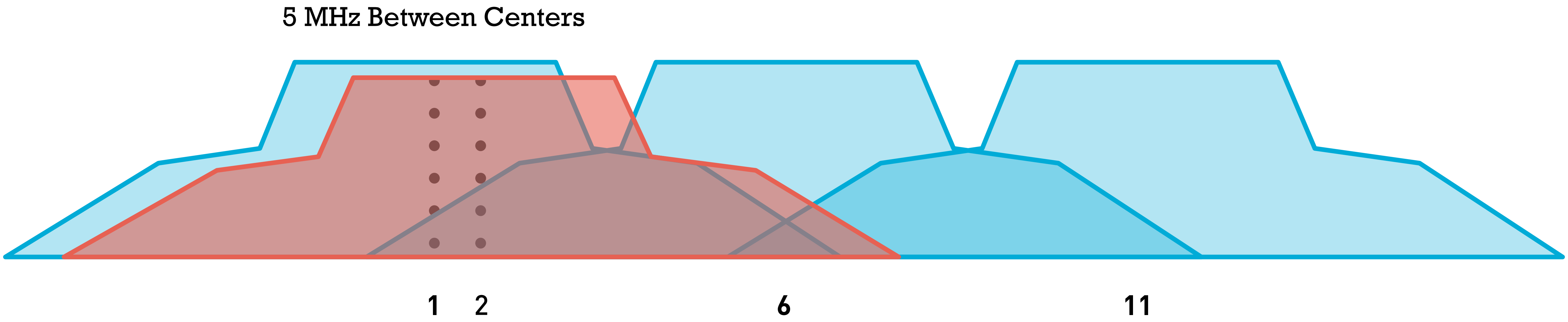
- Lower Indoor Range (~90 ft)
- Limited Compatibility (**a**/n/**ac**)
- 24 non-overlapping channels



metageek

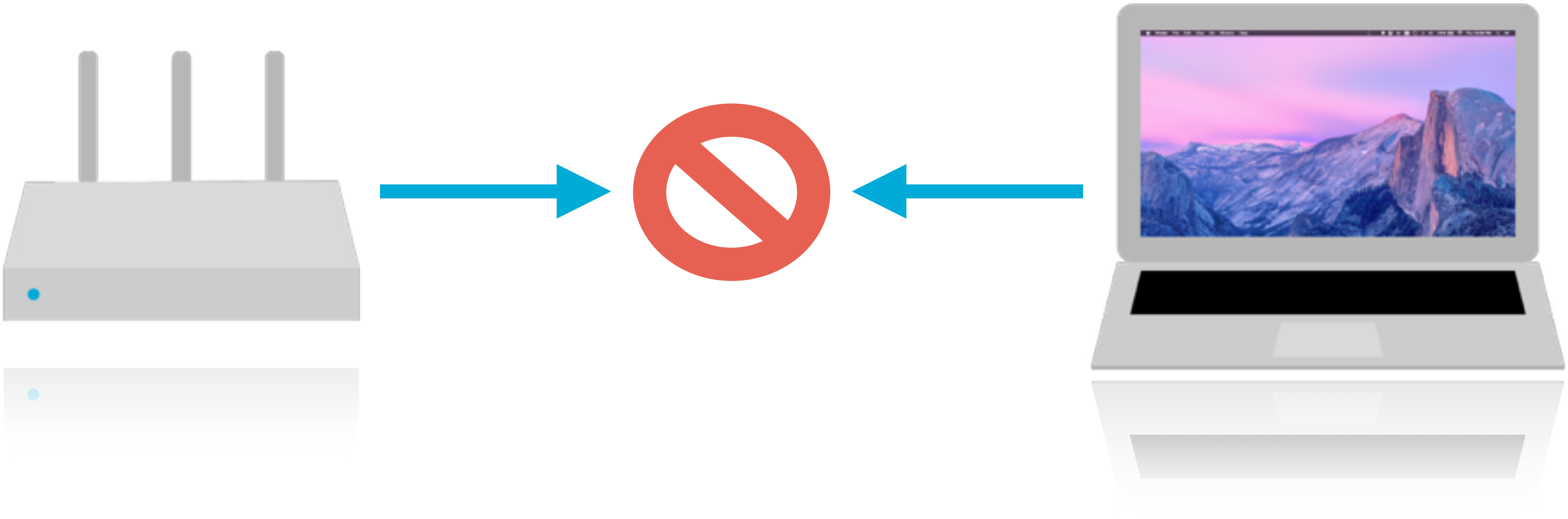
2.4 GHz Channels



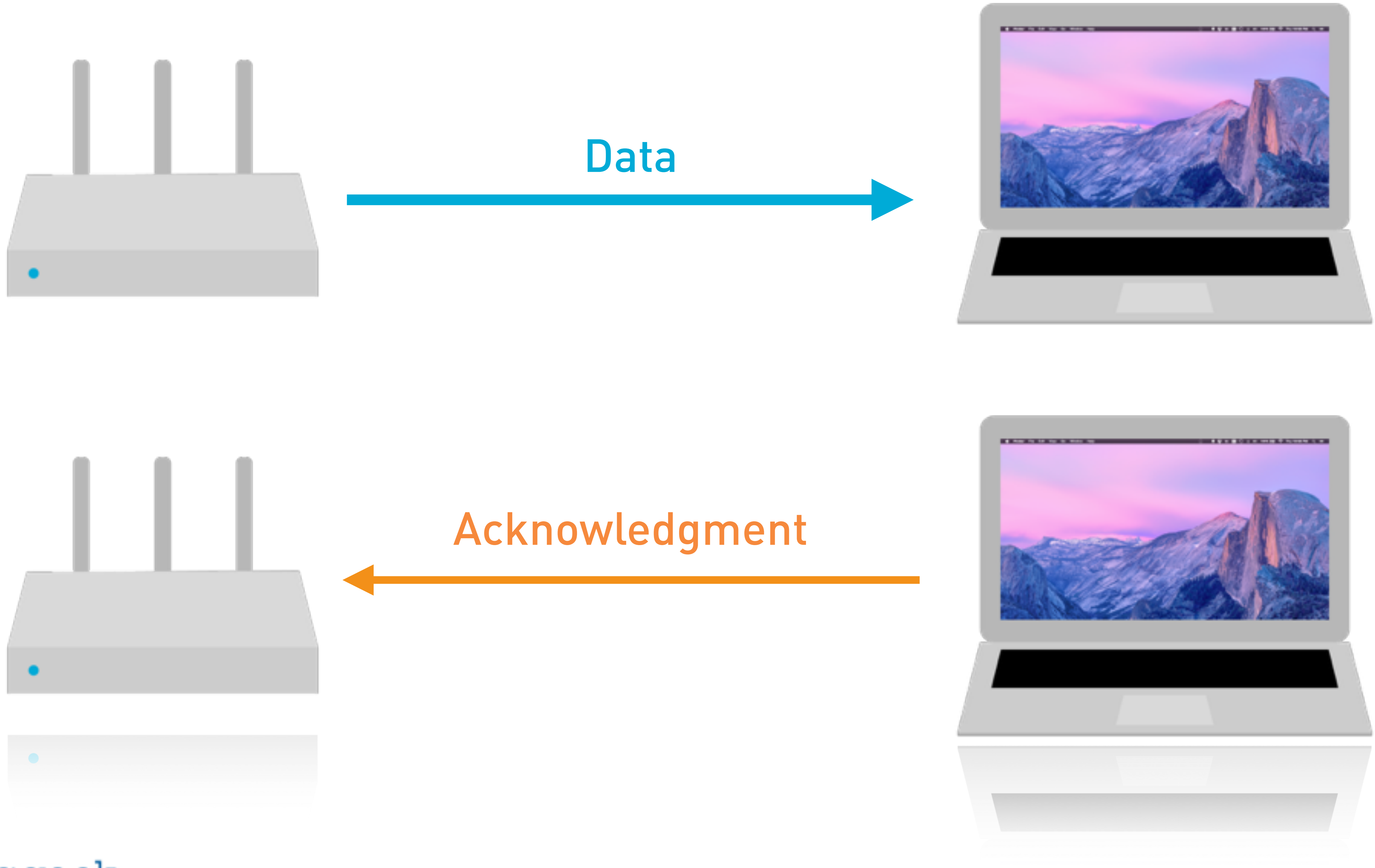


metageek

Half-Duplex



Half-Duplex

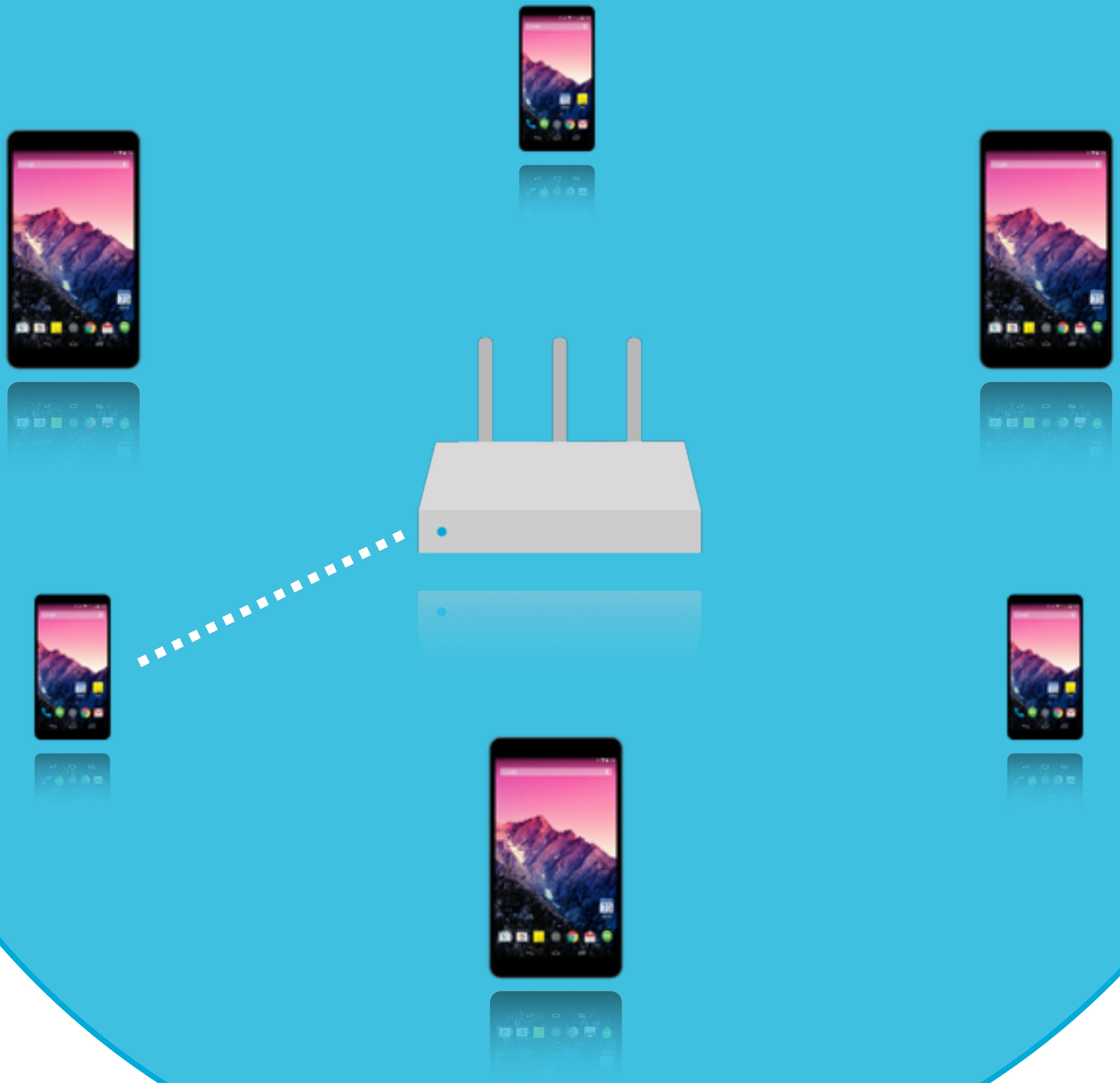


Data

Acknowledgment

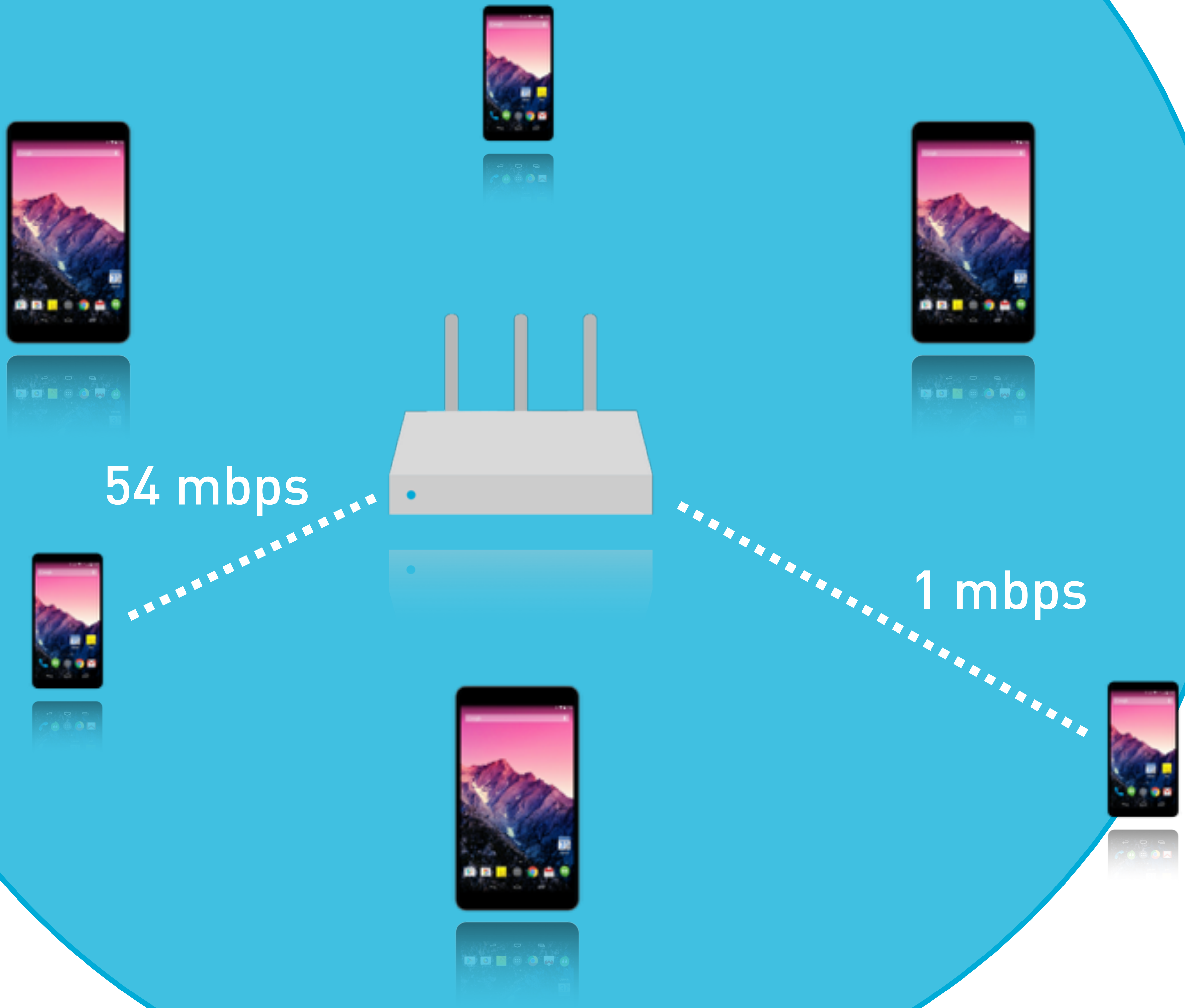
Taking Turns

The more devices on the channel, the less time left to talk



Slow Talkers

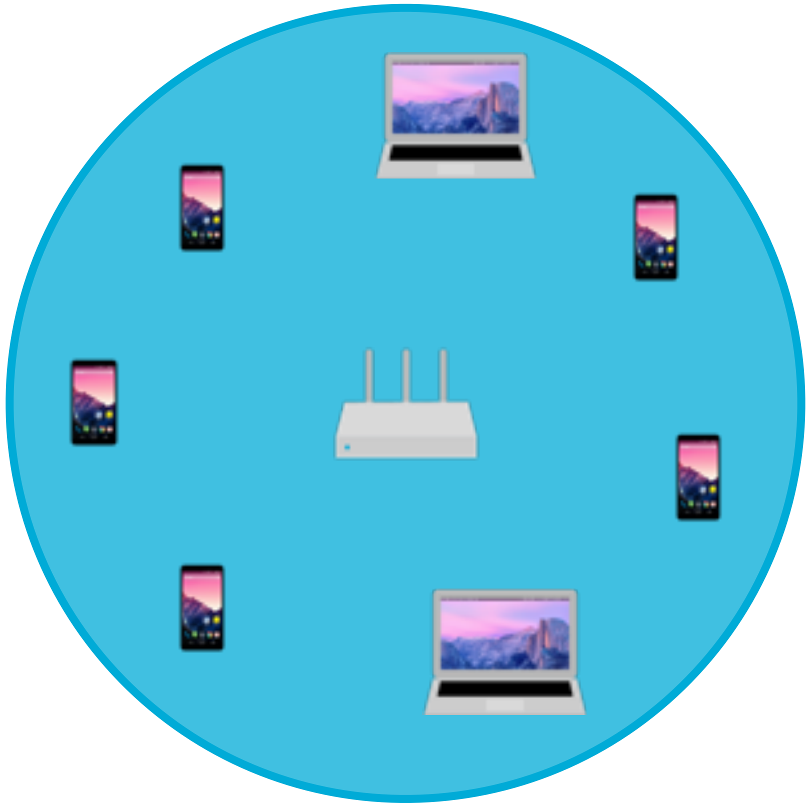
Slower conversations take more time



metageek

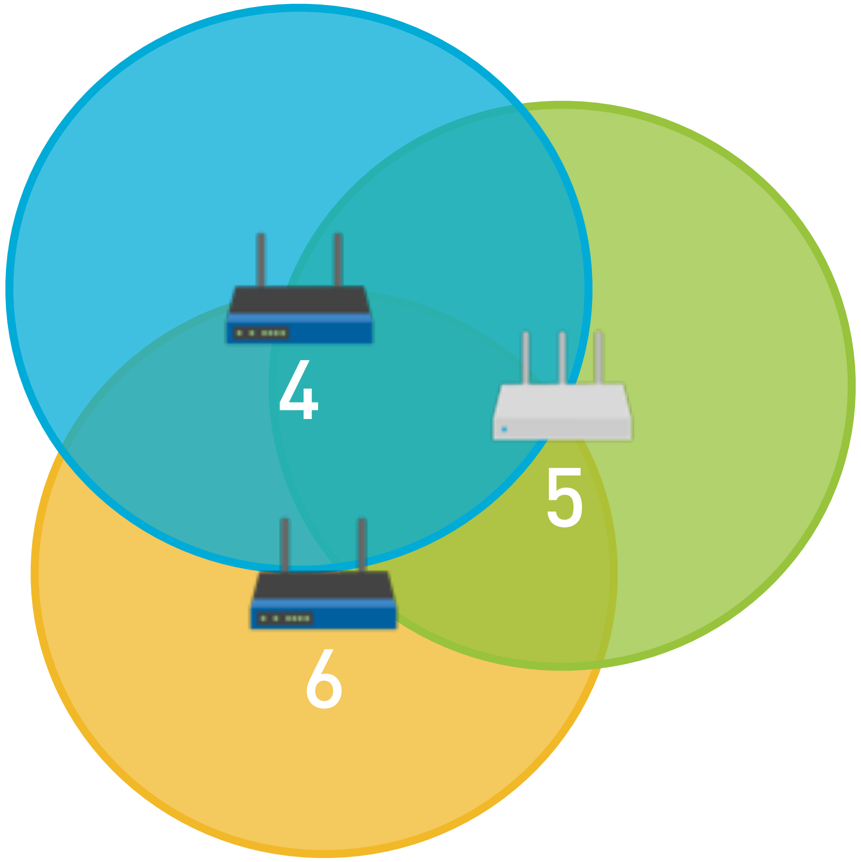
Types of Interference

Co-Channel



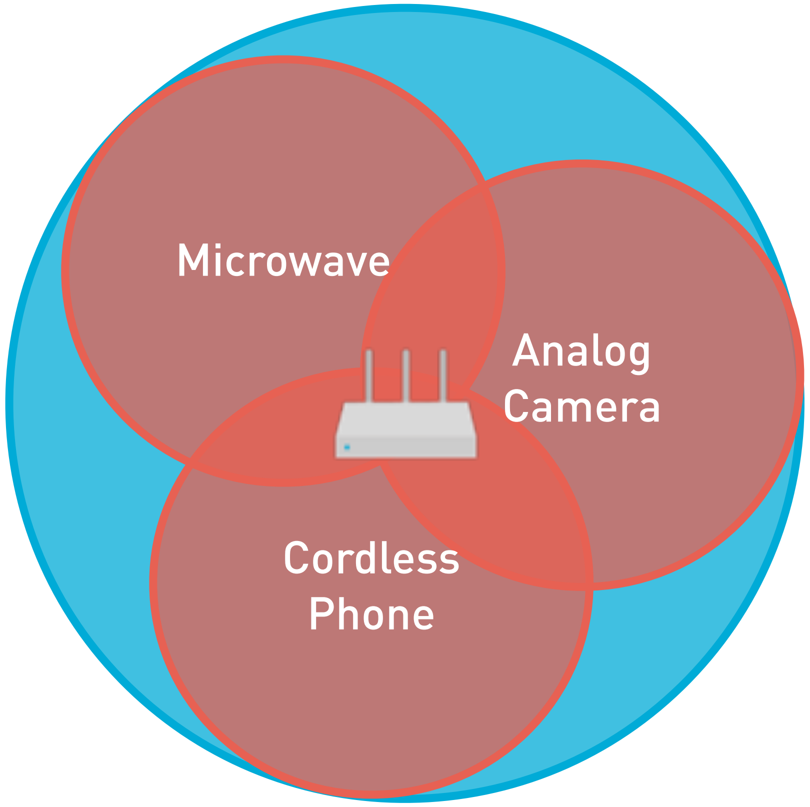
Every client and access point on the same channel competes for time to talk.

Adjacent-Channel



Every client and access point on overlapping channels talk over each other.

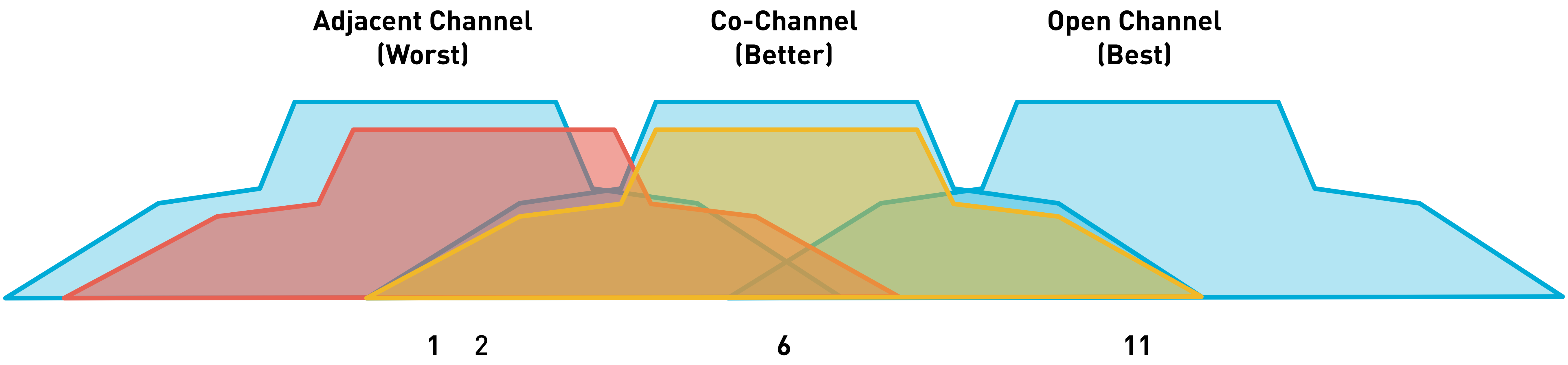
Non-Wi-Fi



Non-802.11 devices compete for medium access.

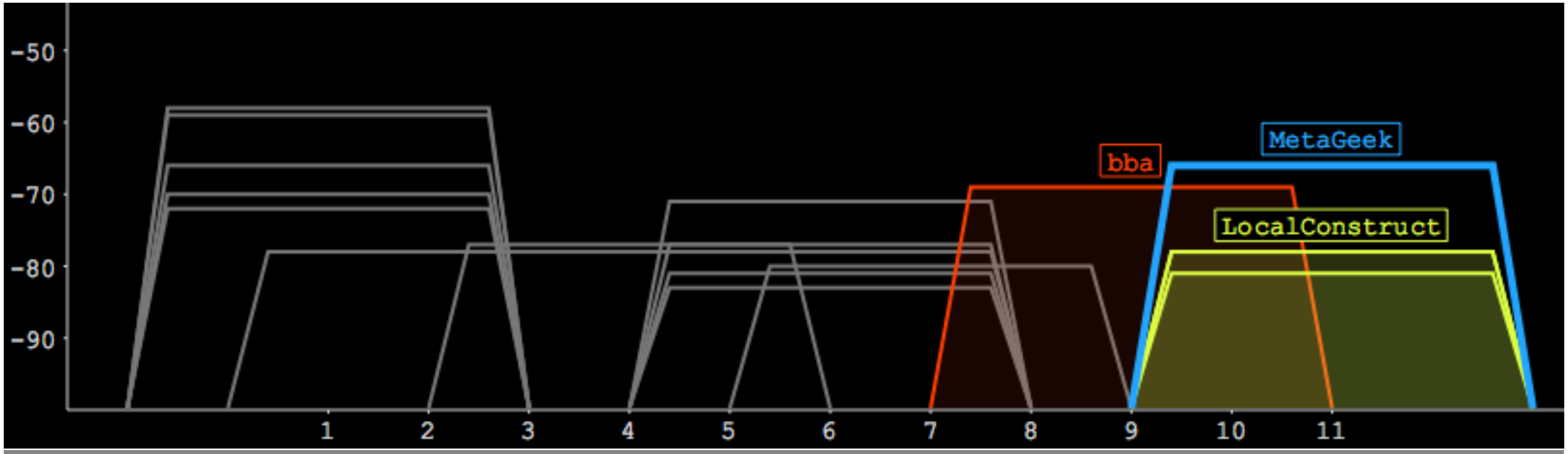
metageek

Wi-Fi Scanner

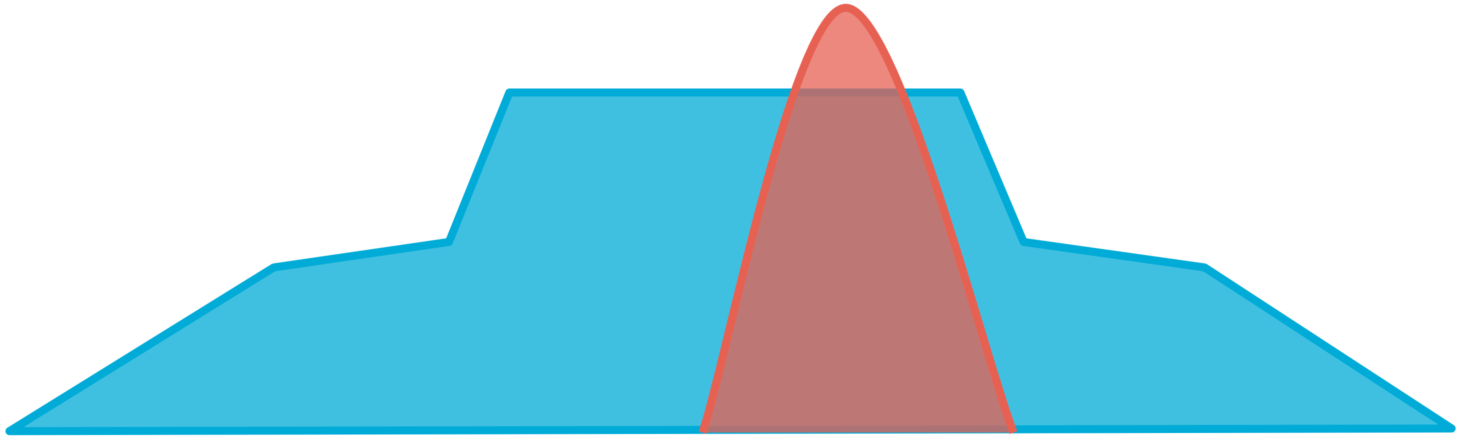

Adjacent Channel
(Worst)

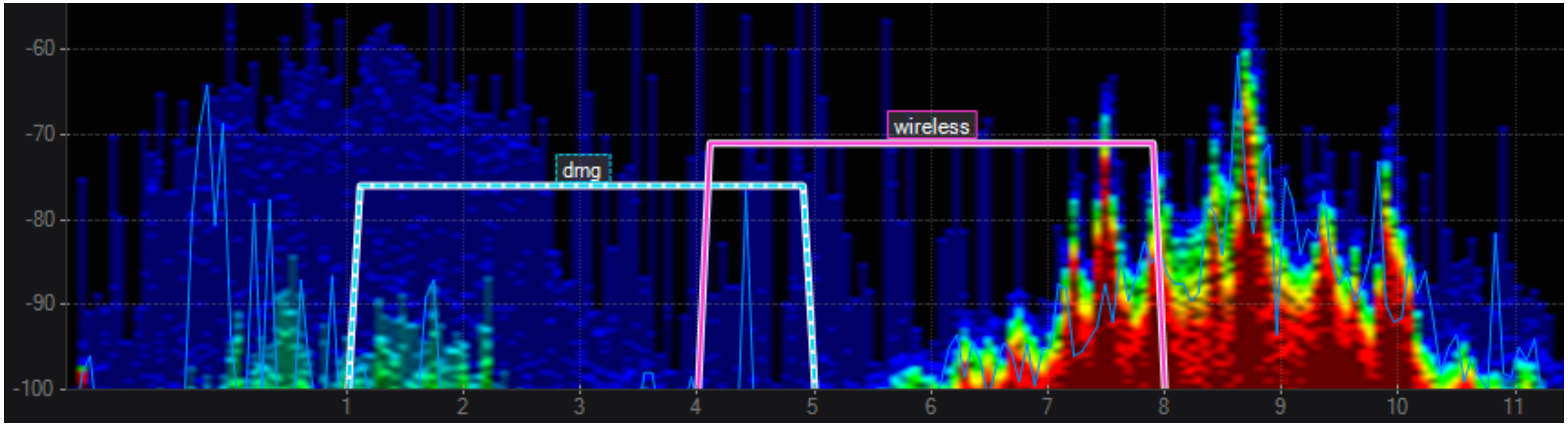
Co-Channel
(Better)

Open Channel
(Best)



Spectrum Analyzer

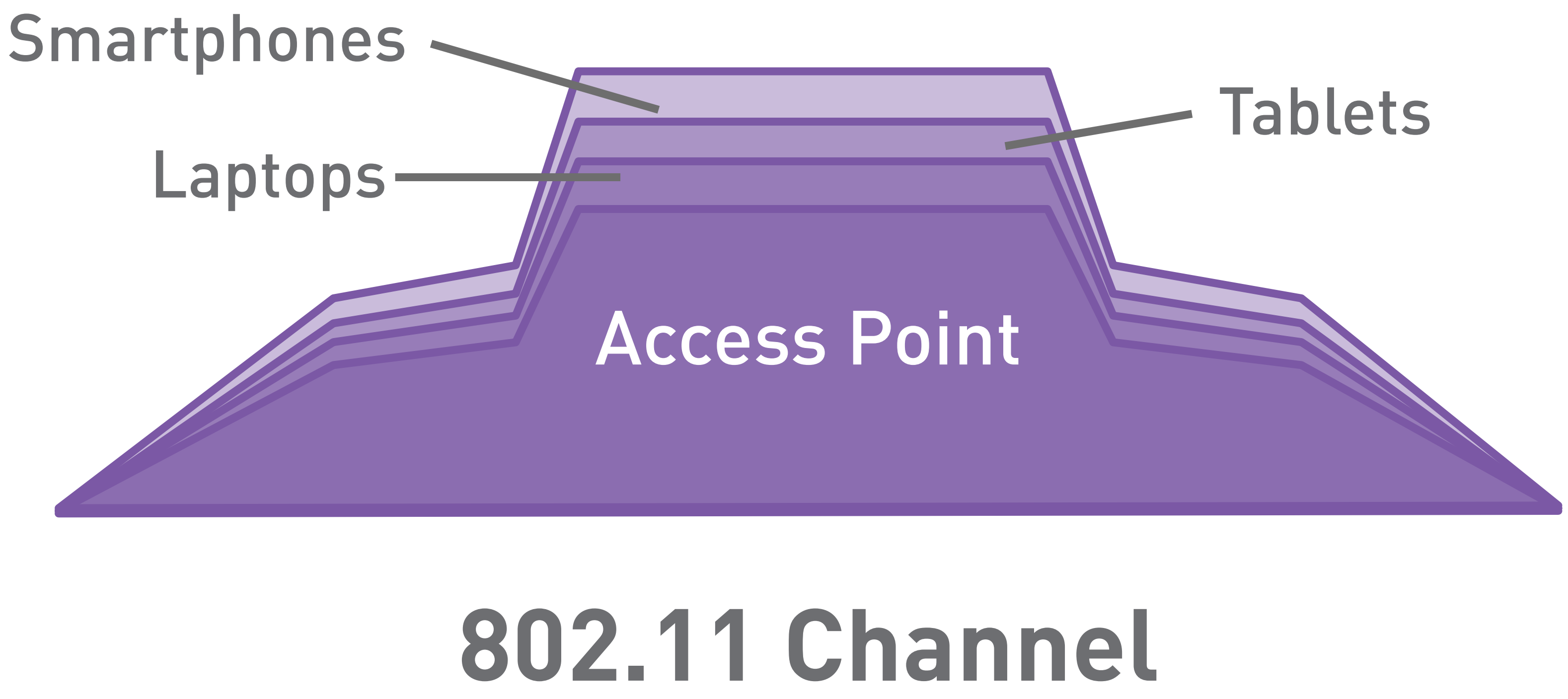




metageek

Packet Analysis

- All activity from AP's, laptops, tablets, smartphones
- MAC addresses of wireless clients
- Utilization of each 802.11 station
- Retransmission percentage by client
- Data rates for wireless clients



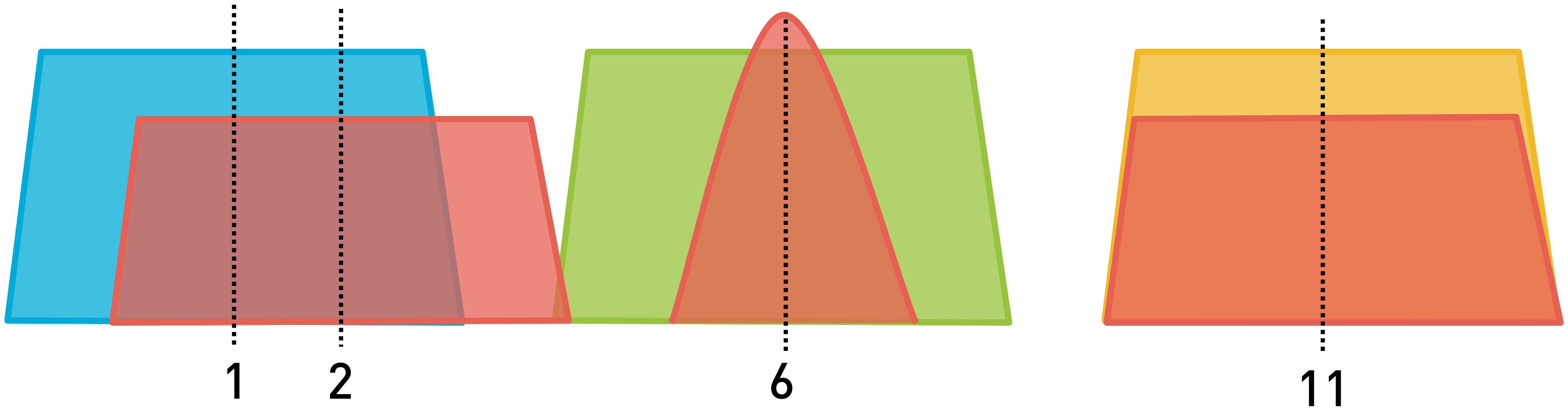
metageek

Different Tools for Different Jobs

Adjacent-Channel

Non-Wi-Fi

Co-Channel



metageek inSSIDer OFFICE

metageek chanalyzer

+

metageek wi Spy

metageek Eye P.A.

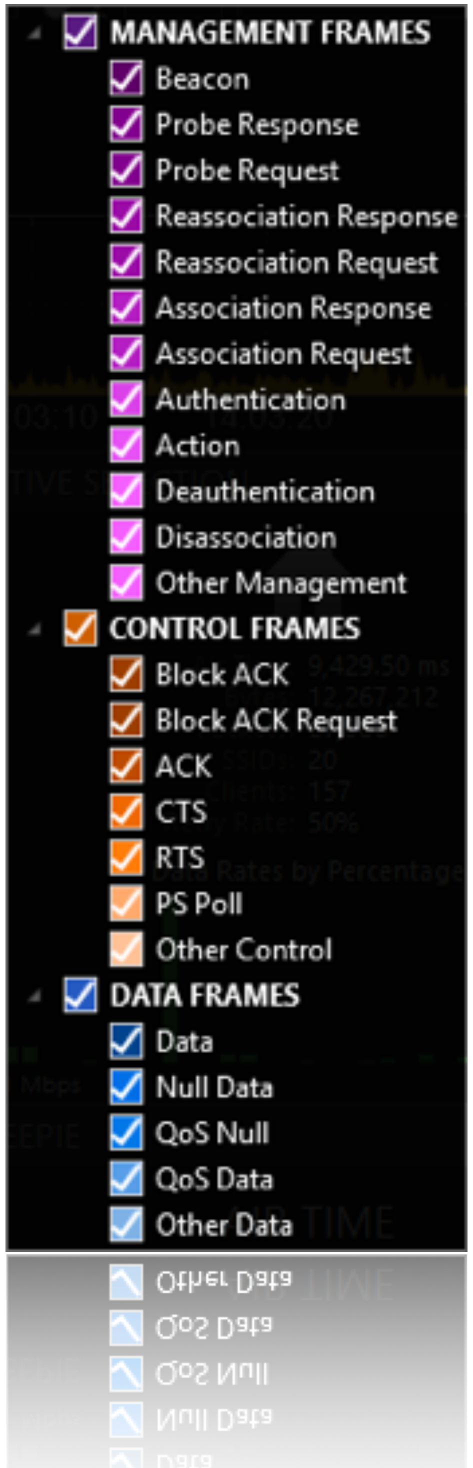
metageek

Wireless Frame Types

Each frame type gets a unique color

3 Frame Types:

- **Management**
- **Control**
- **Data**



- ☑ MANAGEMENT FRAMES
  - ☑ Beacon
  - ☑ Probe Response
  - ☑ Probe Request
  - ☑ Reassociation Response
  - ☑ Reassociation Request
  - ☑ Association Response
  - ☑ Association Request
  - ☑ Authentication
  - ☑ Action
  - ☑ Deauthentication
  - ☑ Disassociation
  - ☑ Other Management
- ☑ CONTROL FRAMES
  - ☑ Block ACK
  - ☑ Block ACK Request
  - ☑ ACK
  - ☑ CTS
  - ☑ RTS
  - ☑ PS Poll
  - ☑ Other Control
- ☑ DATA FRAMES
  - ☑ Data
  - ☑ Null Data
  - ☑ QoS Null
  - ☑ QoS Data
  - ☑ Other Data

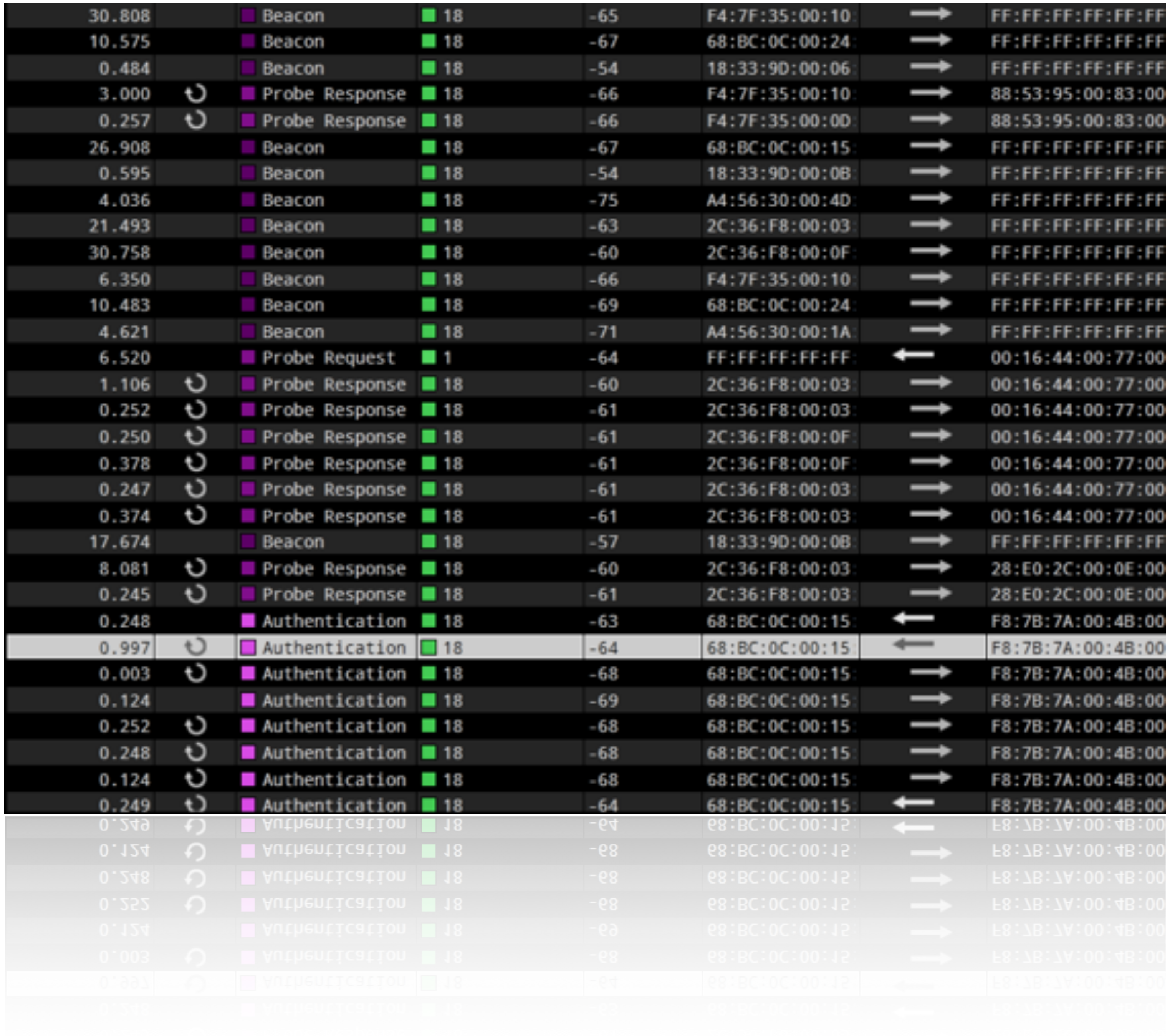
metageek

Management Frames

WHAT THEY DO:

“Manage” stations joining and leaving wireless networks.

- Beacons
- Probes
- Authentication
- Association



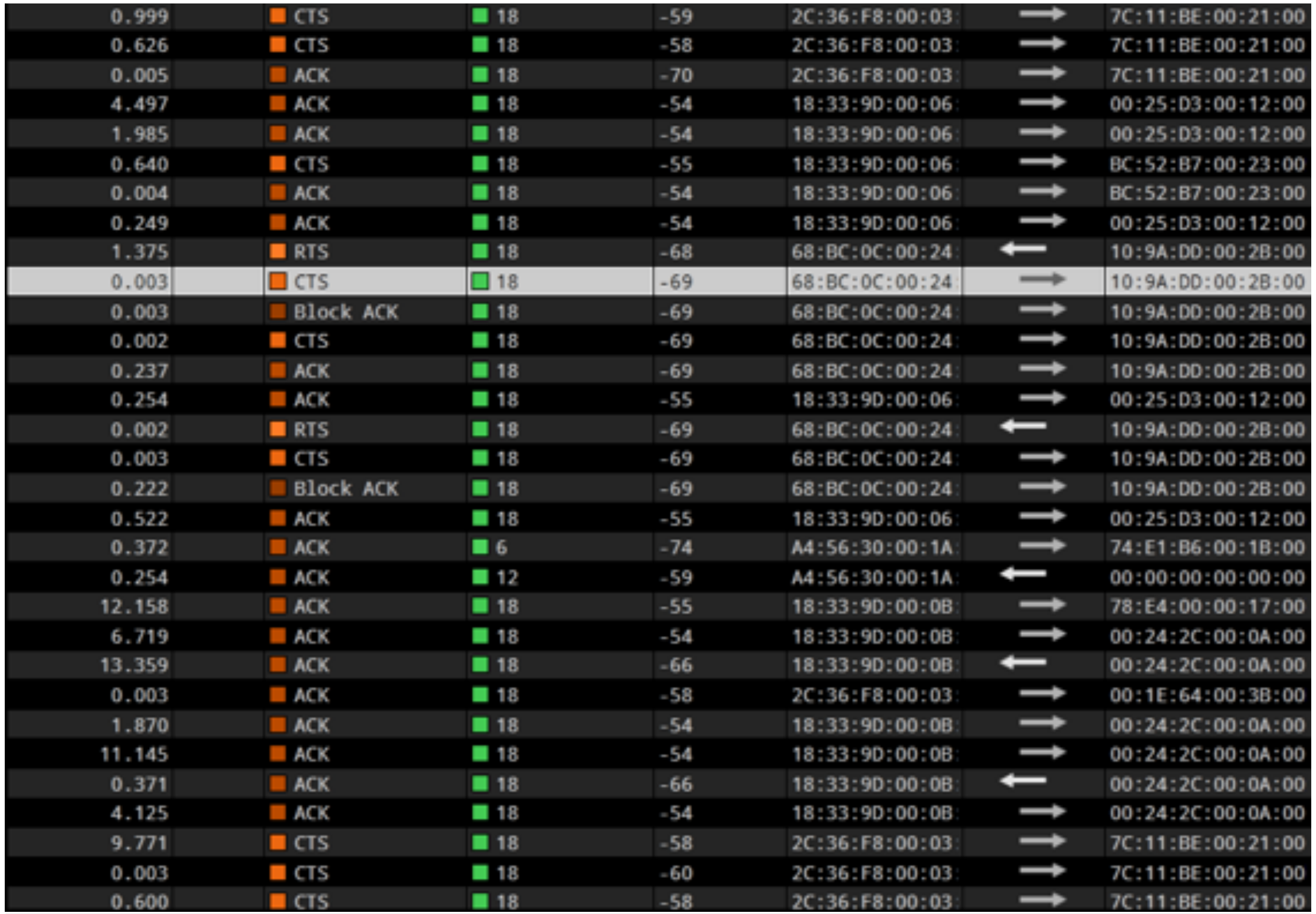
30.808		Beacon	18	-65	F4:7F:35:00:10	→	FF:FF:FF:FF:FF:FF
10.575		Beacon	18	-67	68:BC:0C:00:24	→	FF:FF:FF:FF:FF:FF
0.484		Beacon	18	-54	18:33:9D:00:06	→	FF:FF:FF:FF:FF:FF
3.000	↻	Probe Response	18	-66	F4:7F:35:00:10	→	88:53:95:00:83:00
0.257	↻	Probe Response	18	-66	F4:7F:35:00:0D	→	88:53:95:00:83:00
26.908		Beacon	18	-67	68:BC:0C:00:15	→	FF:FF:FF:FF:FF:FF
0.595		Beacon	18	-54	18:33:9D:00:0B	→	FF:FF:FF:FF:FF:FF
4.036		Beacon	18	-75	A4:56:30:00:4D	→	FF:FF:FF:FF:FF:FF
21.493		Beacon	18	-63	2C:36:F8:00:03	→	FF:FF:FF:FF:FF:FF
30.758		Beacon	18	-60	2C:36:F8:00:0F	→	FF:FF:FF:FF:FF:FF
6.350		Beacon	18	-66	F4:7F:35:00:10	→	FF:FF:FF:FF:FF:FF
10.483		Beacon	18	-69	68:BC:0C:00:24	→	FF:FF:FF:FF:FF:FF
4.621		Beacon	18	-71	A4:56:30:00:1A	→	FF:FF:FF:FF:FF:FF
6.520		Probe Request	1	-64	FF:FF:FF:FF:FF	←	00:16:44:00:77:00
1.106	↻	Probe Response	18	-60	2C:36:F8:00:03	→	00:16:44:00:77:00
0.252	↻	Probe Response	18	-61	2C:36:F8:00:03	→	00:16:44:00:77:00
0.250	↻	Probe Response	18	-61	2C:36:F8:00:0F	→	00:16:44:00:77:00
0.378	↻	Probe Response	18	-61	2C:36:F8:00:0F	→	00:16:44:00:77:00
0.247	↻	Probe Response	18	-61	2C:36:F8:00:03	→	00:16:44:00:77:00
0.374	↻	Probe Response	18	-61	2C:36:F8:00:03	→	00:16:44:00:77:00
17.674		Beacon	18	-57	18:33:9D:00:0B	→	FF:FF:FF:FF:FF:FF
8.081	↻	Probe Response	18	-60	2C:36:F8:00:03	→	28:E0:2C:00:0E:00
0.245	↻	Probe Response	18	-61	2C:36:F8:00:03	→	28:E0:2C:00:0E:00
0.248		Authentication	18	-63	68:BC:0C:00:15	←	F8:7B:7A:00:4B:00
0.997	↻	Authentication	18	-64	68:BC:0C:00:15	←	F8:7B:7A:00:4B:00
0.003	↻	Authentication	18	-68	68:BC:0C:00:15	→	F8:7B:7A:00:4B:00
0.124		Authentication	18	-69	68:BC:0C:00:15	→	F8:7B:7A:00:4B:00
0.252	↻	Authentication	18	-68	68:BC:0C:00:15	→	F8:7B:7A:00:4B:00
0.248	↻	Authentication	18	-68	68:BC:0C:00:15	→	F8:7B:7A:00:4B:00
0.124	↻	Authentication	18	-68	68:BC:0C:00:15	→	F8:7B:7A:00:4B:00
0.249	↻	Authentication	18	-64	68:BC:0C:00:15	←	F8:7B:7A:00:4B:00

Control Frames

WHAT THEY DO:

“Control” the RF medium and aid in the delivery of management and data frames.

- ACK
- Block-ACK
- RTS/CTS



0.999	CTS	18	-59	2C:36:F8:00:03	→	7C:11:BE:00:21:00
0.626	CTS	18	-58	2C:36:F8:00:03	→	7C:11:BE:00:21:00
0.005	ACK	18	-70	2C:36:F8:00:03	→	7C:11:BE:00:21:00
4.497	ACK	18	-54	18:33:9D:00:06	→	00:25:D3:00:12:00
1.985	ACK	18	-54	18:33:9D:00:06	→	00:25:D3:00:12:00
0.640	CTS	18	-55	18:33:9D:00:06	→	BC:52:B7:00:23:00
0.004	ACK	18	-54	18:33:9D:00:06	→	BC:52:B7:00:23:00
0.249	ACK	18	-54	18:33:9D:00:06	→	00:25:D3:00:12:00
1.375	RTS	18	-68	68:BC:0C:00:24	←	10:9A:DD:00:2B:00
0.003	CTS	18	-69	68:BC:0C:00:24	→	10:9A:DD:00:2B:00
0.003	Block ACK	18	-69	68:BC:0C:00:24	→	10:9A:DD:00:2B:00
0.002	CTS	18	-69	68:BC:0C:00:24	→	10:9A:DD:00:2B:00
0.237	ACK	18	-69	68:BC:0C:00:24	→	10:9A:DD:00:2B:00
0.254	ACK	18	-55	18:33:9D:00:06	→	00:25:D3:00:12:00
0.002	RTS	18	-69	68:BC:0C:00:24	←	10:9A:DD:00:2B:00
0.003	CTS	18	-69	68:BC:0C:00:24	→	10:9A:DD:00:2B:00
0.222	Block ACK	18	-69	68:BC:0C:00:24	→	10:9A:DD:00:2B:00
0.522	ACK	18	-55	18:33:9D:00:06	→	00:25:D3:00:12:00
0.372	ACK	6	-74	A4:56:30:00:1A	→	74:E1:B6:00:1B:00
0.254	ACK	12	-59	A4:56:30:00:1A	←	00:00:00:00:00:00
12.158	ACK	18	-55	18:33:9D:00:0B	→	78:E4:00:00:17:00
6.719	ACK	18	-54	18:33:9D:00:0B	→	00:24:2C:00:0A:00
13.359	ACK	18	-66	18:33:9D:00:0B	←	00:24:2C:00:0A:00
0.003	ACK	18	-58	2C:36:F8:00:03	→	00:1E:64:00:3B:00
1.870	ACK	18	-54	18:33:9D:00:0B	→	00:24:2C:00:0A:00
11.145	ACK	18	-54	18:33:9D:00:0B	→	00:24:2C:00:0A:00
0.371	ACK	18	-66	18:33:9D:00:0B	←	00:24:2C:00:0A:00
4.125	ACK	18	-54	18:33:9D:00:0B	→	00:24:2C:00:0A:00
9.771	CTS	18	-58	2C:36:F8:00:03	→	7C:11:BE:00:21:00
0.003	CTS	18	-60	2C:36:F8:00:03	→	7C:11:BE:00:21:00
0.600	CTS	18	-58	2C:36:F8:00:03	→	7C:11:BE:00:21:00

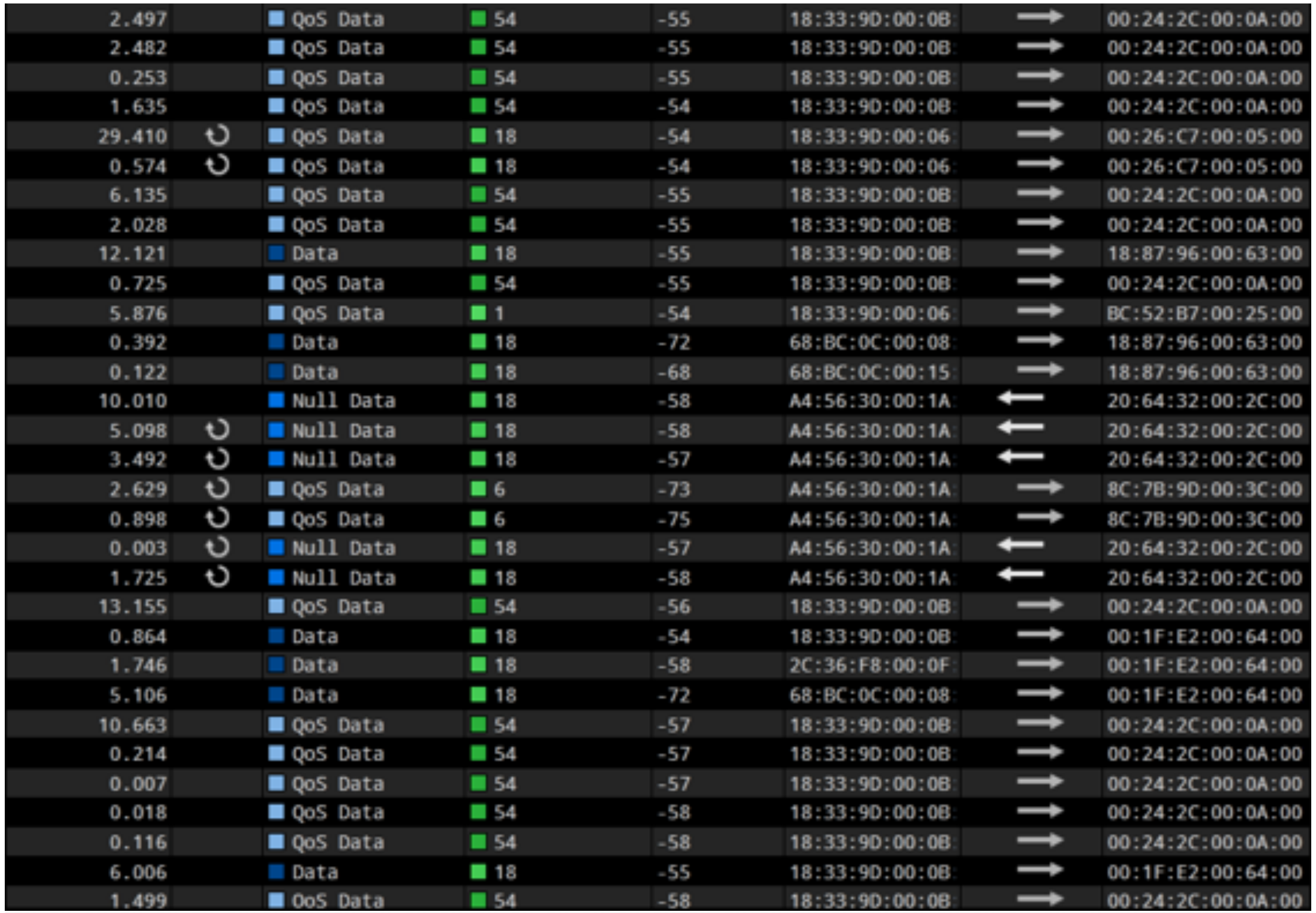
metageek

Data Frames

WHAT THEY DO:

Carry higher-level protocol data.

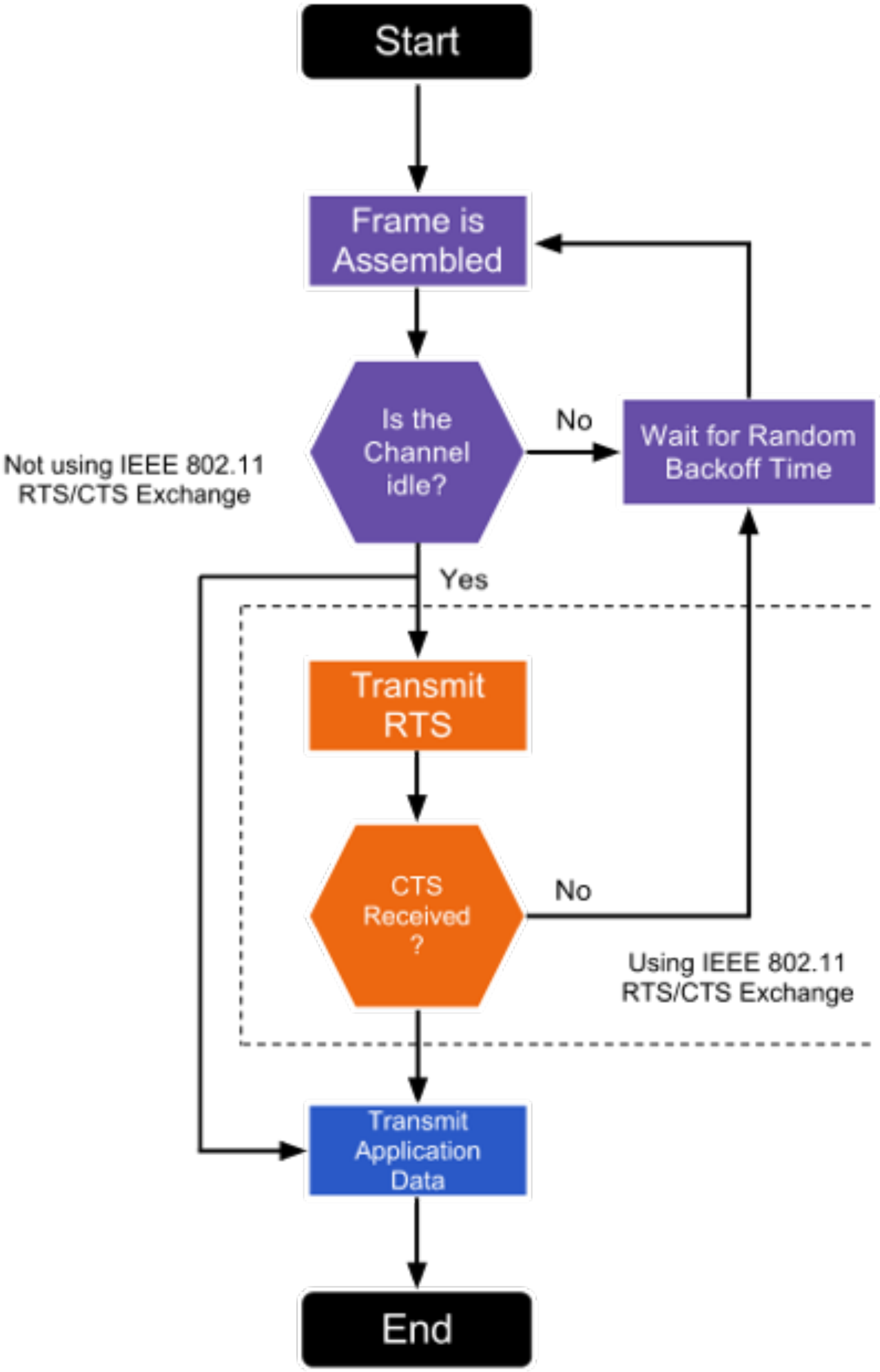
- Data
- QoS Data
- Null Data



2.497		QoS Data	54	-55	18:33:9D:00:0B	→	00:24:2C:00:0A:00
2.482		QoS Data	54	-55	18:33:9D:00:0B	→	00:24:2C:00:0A:00
0.253		QoS Data	54	-55	18:33:9D:00:0B	→	00:24:2C:00:0A:00
1.635		QoS Data	54	-54	18:33:9D:00:0B	→	00:24:2C:00:0A:00
29.410	↻	QoS Data	18	-54	18:33:9D:00:06	→	00:26:C7:00:05:00
0.574	↻	QoS Data	18	-54	18:33:9D:00:06	→	00:26:C7:00:05:00
6.135		QoS Data	54	-55	18:33:9D:00:0B	→	00:24:2C:00:0A:00
2.028		QoS Data	54	-55	18:33:9D:00:0B	→	00:24:2C:00:0A:00
12.121		Data	18	-55	18:33:9D:00:0B	→	18:87:96:00:63:00
0.725		QoS Data	54	-55	18:33:9D:00:0B	→	00:24:2C:00:0A:00
5.876		QoS Data	1	-54	18:33:9D:00:06	→	BC:52:B7:00:25:00
0.392		Data	18	-72	68:BC:0C:00:08	→	18:87:96:00:63:00
0.122		Data	18	-68	68:BC:0C:00:15	→	18:87:96:00:63:00
10.010		Null Data	18	-58	A4:56:30:00:1A	←	20:64:32:00:2C:00
5.098	↻	Null Data	18	-58	A4:56:30:00:1A	←	20:64:32:00:2C:00
3.492	↻	Null Data	18	-57	A4:56:30:00:1A	←	20:64:32:00:2C:00
2.629	↻	QoS Data	6	-73	A4:56:30:00:1A	→	8C:7B:9D:00:3C:00
0.898	↻	QoS Data	6	-75	A4:56:30:00:1A	→	8C:7B:9D:00:3C:00
0.003	↻	Null Data	18	-57	A4:56:30:00:1A	←	20:64:32:00:2C:00
1.725	↻	Null Data	18	-58	A4:56:30:00:1A	←	20:64:32:00:2C:00
13.155		QoS Data	54	-56	18:33:9D:00:0B	→	00:24:2C:00:0A:00
0.864		Data	18	-54	18:33:9D:00:0B	→	00:1F:E2:00:64:00
1.746		Data	18	-58	2C:36:F8:00:0F	→	00:1F:E2:00:64:00
5.106		Data	18	-72	68:BC:0C:00:08	→	00:1F:E2:00:64:00
10.663		QoS Data	54	-57	18:33:9D:00:0B	→	00:24:2C:00:0A:00
0.214		QoS Data	54	-57	18:33:9D:00:0B	→	00:24:2C:00:0A:00
0.007		QoS Data	54	-57	18:33:9D:00:0B	→	00:24:2C:00:0A:00
0.018		QoS Data	54	-58	18:33:9D:00:0B	→	00:24:2C:00:0A:00
0.116		QoS Data	54	-58	18:33:9D:00:0B	→	00:24:2C:00:0A:00
6.006		Data	18	-55	18:33:9D:00:0B	→	00:1F:E2:00:64:00
1.499		QoS Data	54	-58	18:33:9D:00:0B	→	00:24:2C:00:0A:00

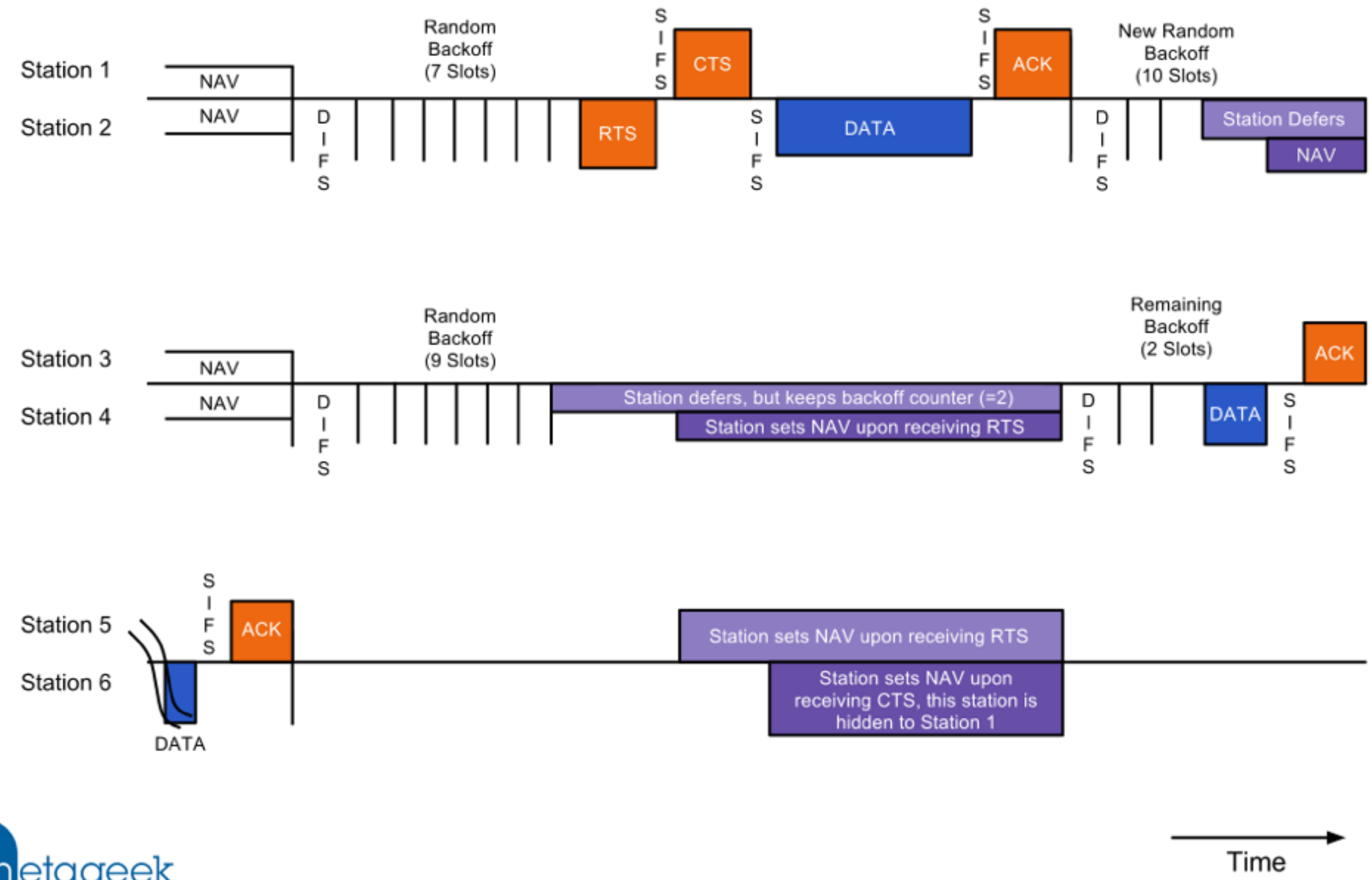
metageek

One AP/One Client Conversation


Start
Frame is Assembled
Is the Channel idle?
No
Wait for Random Backoff Time
Not using IEEE 802.11 RTS/CTS Exchange
Yes
Transmit RTS
CTS Received ?
No
Using IEEE 802.11 RTS/CTS Exchange
Transmit Application Data
End

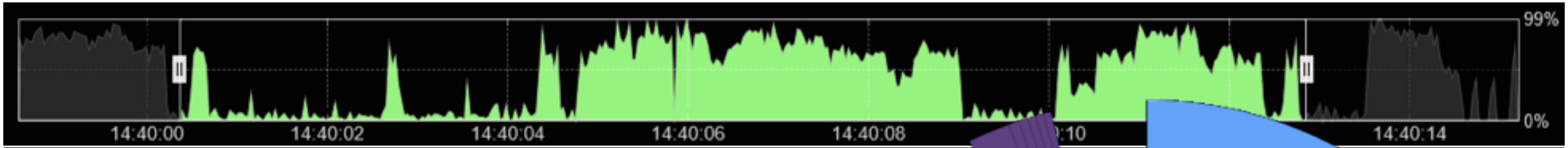
metageek

Multiple Stations


Station 1
NAV
Station 2
NAV
DIFS
Random Backoff (7 Slots)
RTS
SIFS
CTS
SIFS
DATA
SIFS
ACK
DIFS
New Random Backoff (10 Slots)
Station Defers
NAV
Station 3
NAV
Station 4
NAV
DIFS
Random Backoff (9 Slots)
Station defers, but keeps backoff counter (=2)
Station sets NAV upon receiving RTS
DIFS
Remaining Backoff (2 Slots)
DATA
SIFS
ACK
Station 5
Station 6
DATA
SIFS
ACK
Station sets NAV upon receiving RTS
Station sets NAV upon receiving CTS, this station is hidden to Station 1
Time

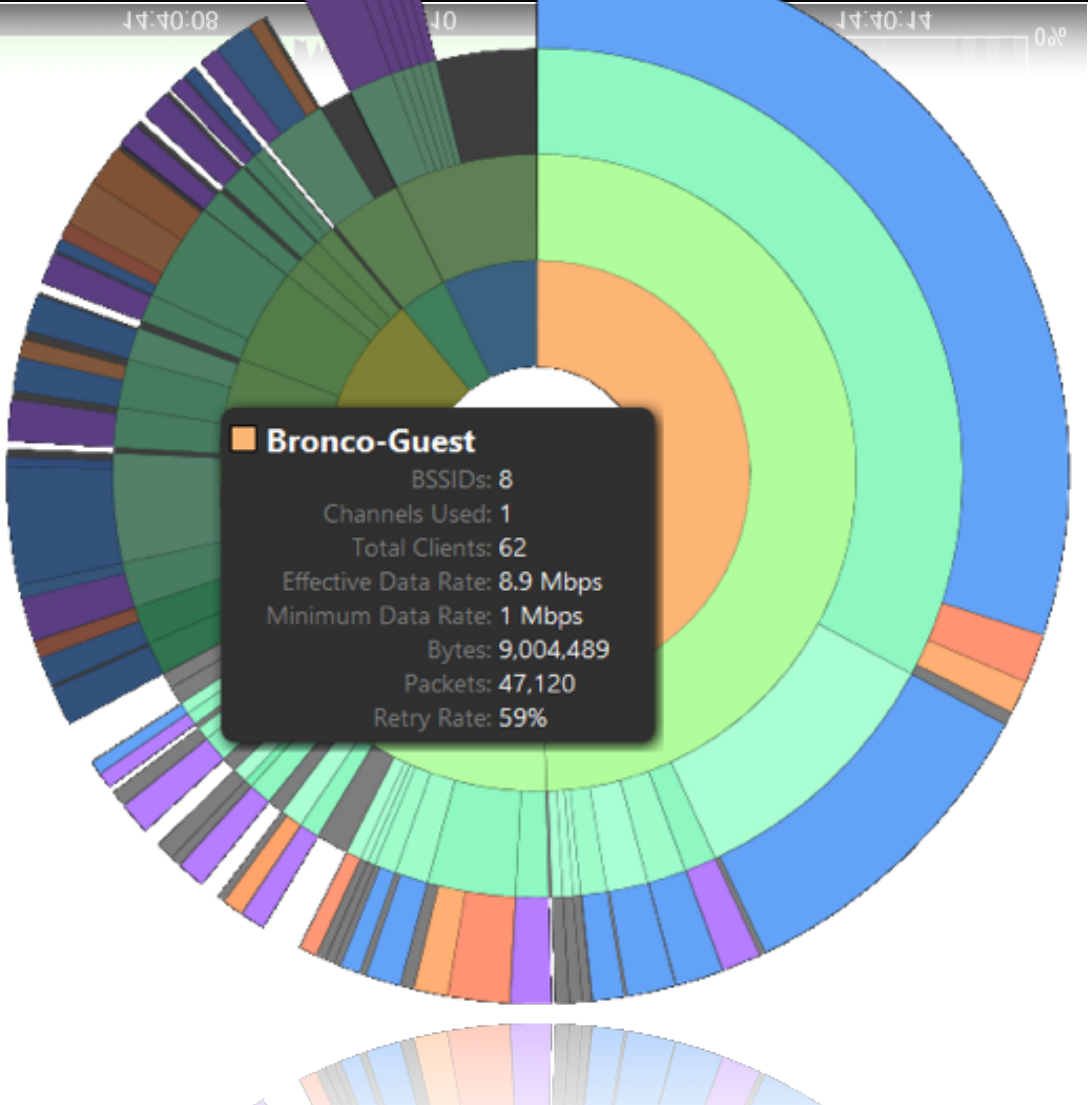
metageek

Packet Analysis Reimagined



How Eye P.A. Visualizes Data

- Time Graph
- Multilayered Pie Charts (Treepies)
- Color Usage
- Data Tables

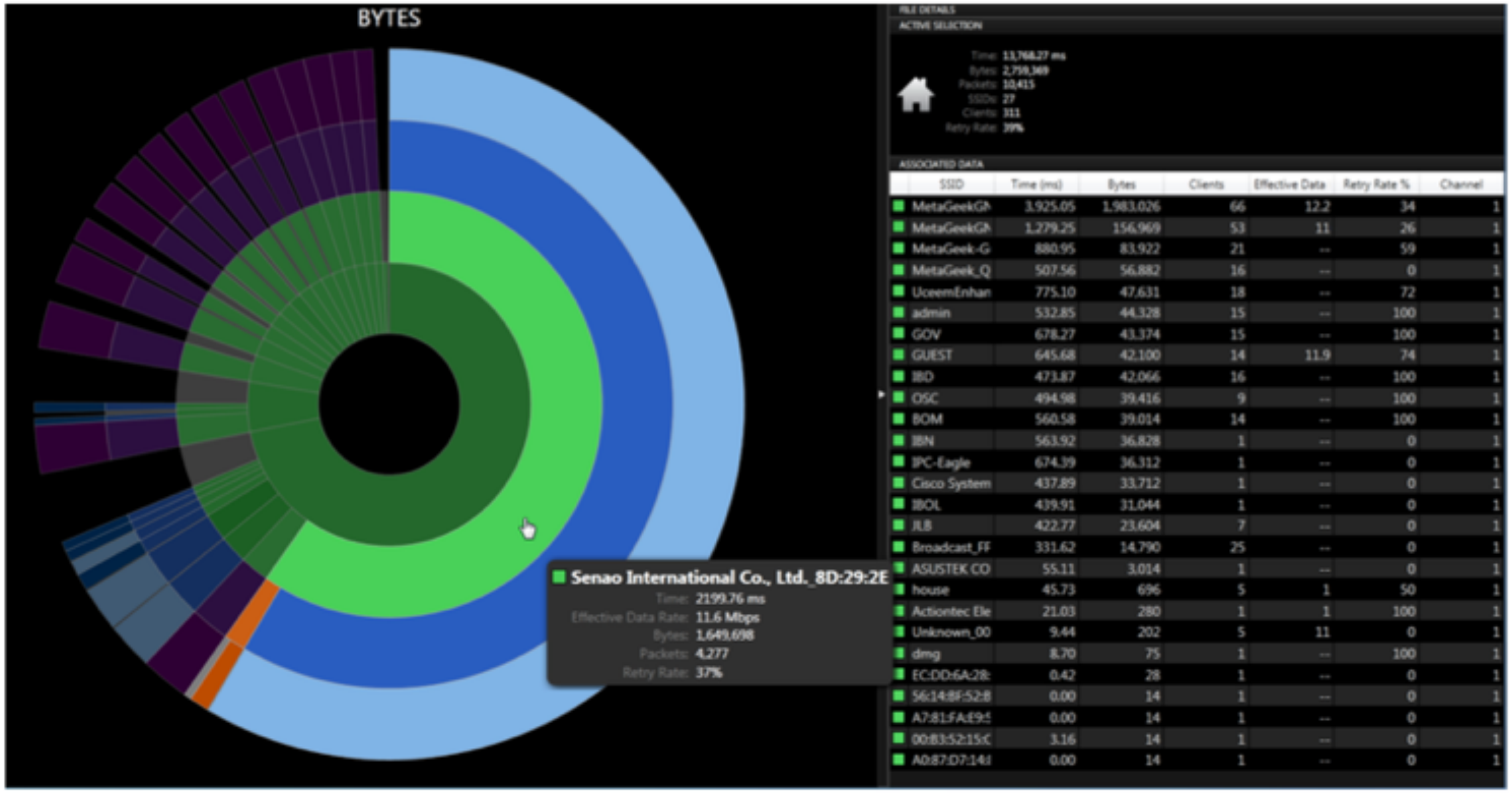


Bronco-Guest

BSSIDs: 8
Channels Used: 1
Total Clients: 62
Effective Data Rate: 8.9 Mbps
Minimum Data Rate: 1 Mbps
Bytes: 9,004,489
Packets: 47,120
Retry Rate: 59%

metageek

2.4 GHz Congestion



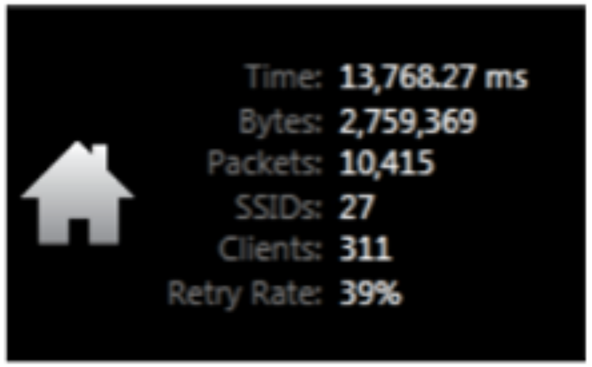
Time: 13,768.27 ms
Bytes: 2,759,369
Packets: 10,415
SSIDs: 27
Clients: 311
Retry Rate: 39%

🟩 Senao International Co., Ltd._8D:29:2E
Time: 2199.76 ms
Effective Data Rate: 11.6 Mbps
Bytes: 1,649,698
Packets: 4,277
Retry Rate: 37%

ASSOCIATED DATA

	SSID	Time (ms)	Bytes	Clients	Effective Data	Retry Rate %	Channel
🟩	MetaGeekGN	3,925.05	1,983,026	66	12.2	34	1
🟩	MetaGeekGN	1,279.25	156,969	53	11	26	1
🟩	MetaGeek-G	880.95	83,922	21	--	59	1
🟩	MetaGeek_Q	507.56	56,882	16	--	0	1
🟩	UceemEnhan	775.10	47,631	18	--	72	1
🟩	admin	532.85	44,328	15	--	100	1
🟩	GOV	678.27	43,374	15	--	100	1
🟩	GUEST	645.68	42,100	14	11.9	74	1
🟩	IBD	473.87	42,066	16	--	100	1
🟩	OSC	494.98	39,416	9	--	100	1
🟩	BOM	560.58	39,014	14	--	100	1
🟩	IBN	563.92	36,828	1	--	0	1
🟩	IPC-Eagle	674.39	36,312	1	--	0	1
🟩	Cisco System	437.89	33,712	1	--	0	1
🟩	IBOL	439.91	31,044	1	--	0	1
🟩	JLB	422.77	23,604	7	--	0	1
🟩	Broadcast_FF	331.62	14,790	25	--	0	1
🟩	ASUSTEK CO	55.11	3,014	1	--	0	1
🟩	house	45.73	696	5	1	50	1
🟩	Actiontec Ele	21.03	280	1	1	100	1
🟩	Unknown_00	9.44	202	5	11	0	1
🟩	dmg	8.70	75	1	--	100	1
🟩	EC:DD:6A:28:	0.42	28	1	--	0	1
🟩	56:14:8F:52:8	0.00	14	1	--	0	1
🟩	A7:81:FA:E9:5	0.00	14	1	--	0	1
🟩	00:83:52:15:C	3.16	14	1	--	0	1
🟩	A0:87:D7:14:I	0.00	14	1	--	0	1

Video Streaming from same location.

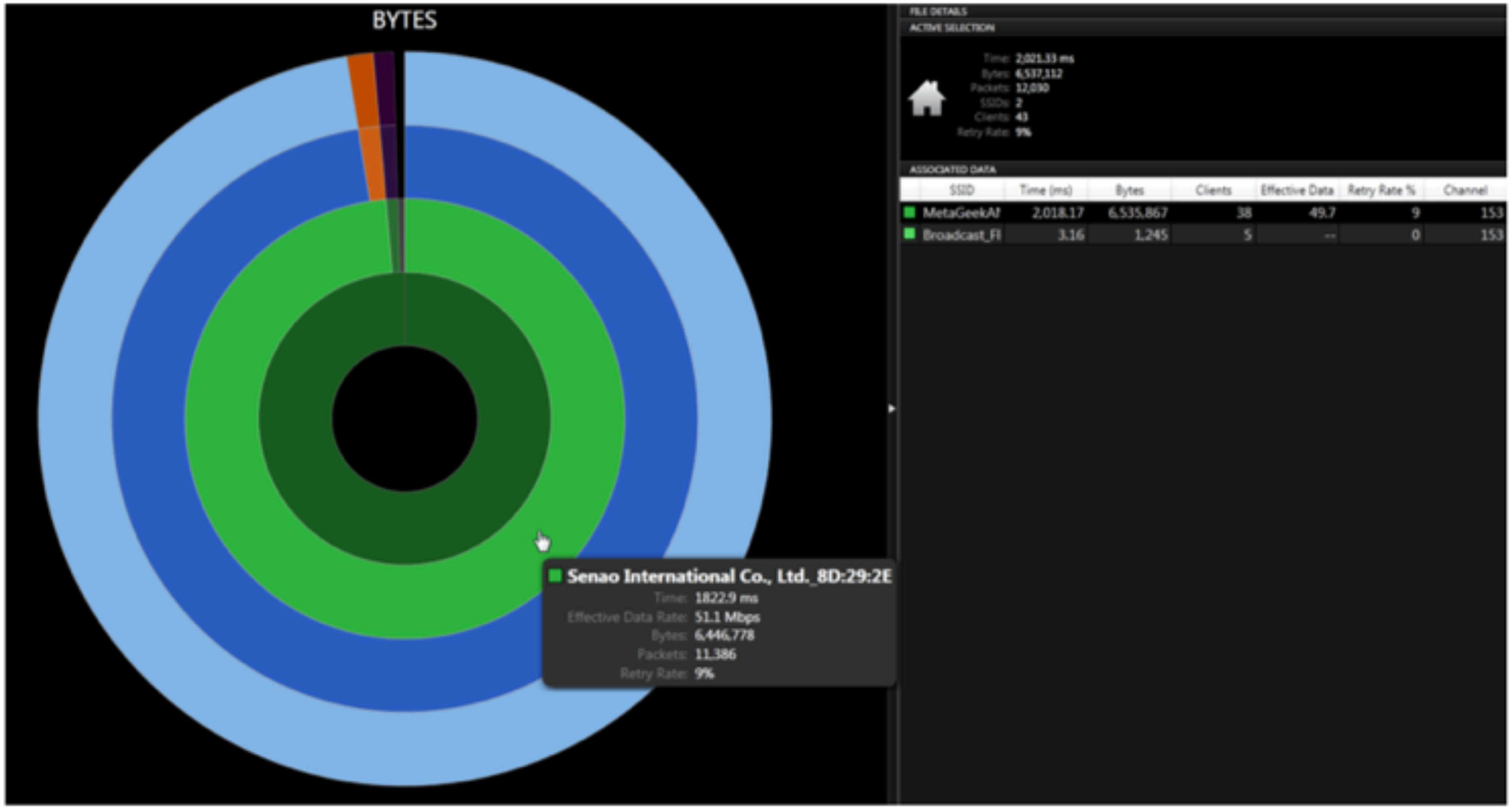


Time: 13,768.27 ms
Bytes: 2,759,369
Packets: 10,415
SSIDs: 27
Clients: 311
Retry Rate: 39%

Client-Level Analysis

- Air Time: 2199ms
- Data Rate: 11 Mbps
- Bytes: 1,649,698
- Packets: 4,277
- Retry: 37%

5 GHz Congestion



Senao International Co., Ltd._8D:29:2E
Time: 1822.9 ms
Effective Data Rate: 51.1 Mbps
Bytes: 6,446,778
Packets: 11,386
Retry Rate: 9%

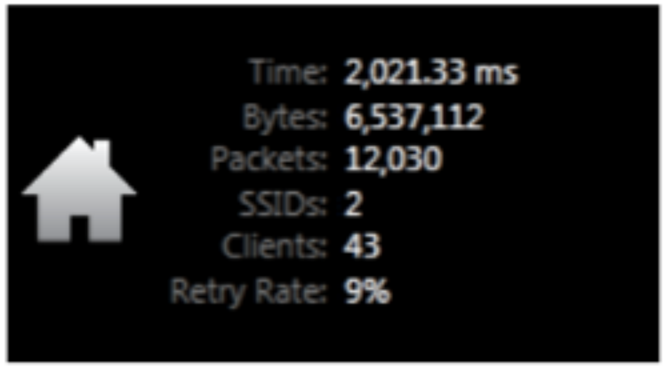
FILE DETAILS

ACTIVE SELECTION

Time: 2,021.33 ms
Bytes: 6,537,112
Packets: 12,030
SSIDs: 2
Clients: 43
Retry Rate: 9%

ASSOCIATED DATA

	SSID	Time (ms)	Bytes	Clients	Effective Data	Retry Rate %	Channel
🟩	MetaGeekAf	2,018.17	6,535,867	38	49.7	9	153
🟩	Broadcast_FI	3.16	1,245	5	--	0	153


Time: 2,021.33 ms
Bytes: 6,537,112
Packets: 12,030
SSIDs: 2
Clients: 43
Retry Rate: 9%

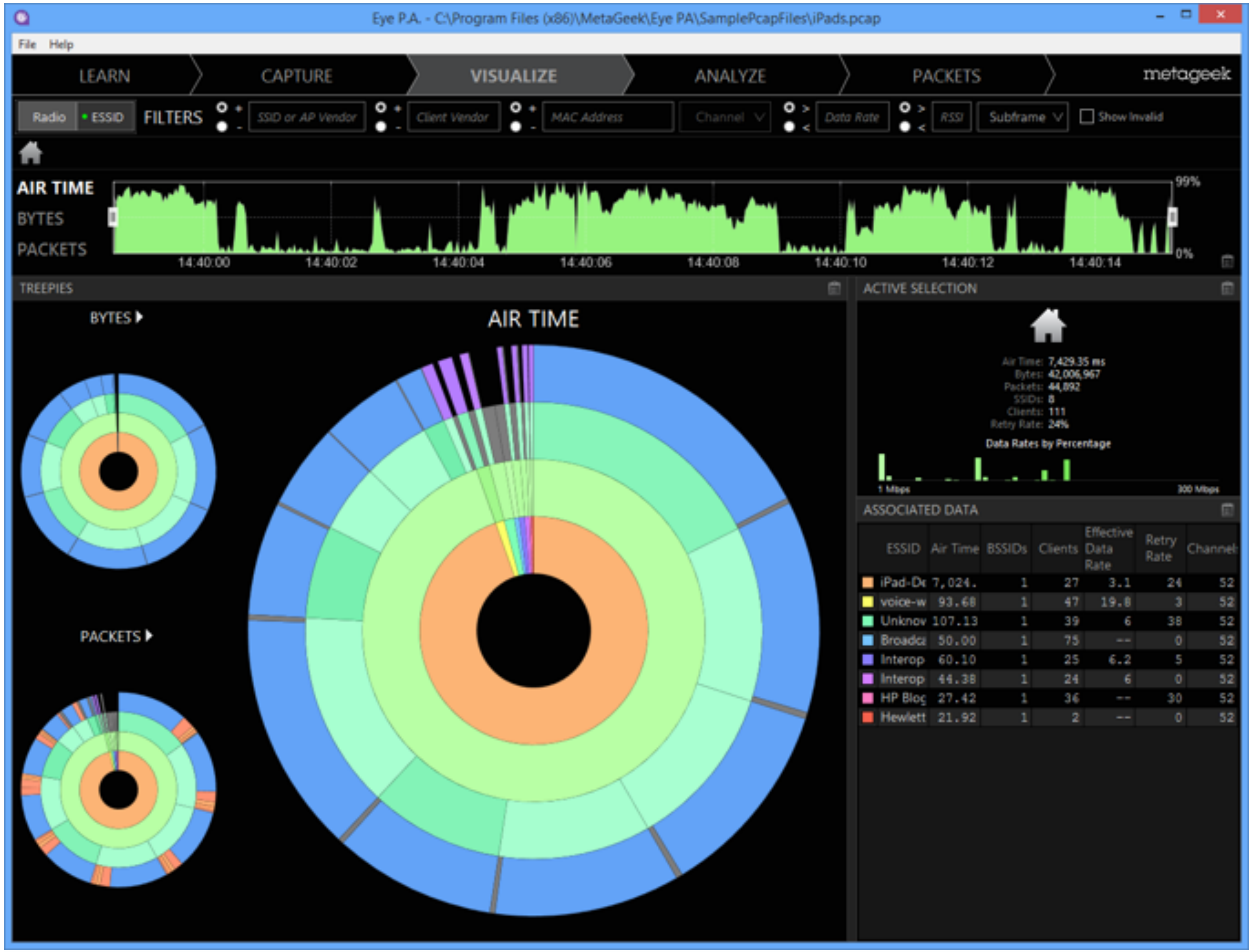
Client-Level Analysis

- Air Time: 1822.9
- Data Rate: 51 Mbps
- Bytes 6,446,778
- Packets: 11,386
- Retry: 9%

Video Streaming from same location.

metageek

Demo



Air Time: 7,429.35 ms
Bytes: 42,006,967
Packets: 44,892
SSIDs: 8
Clients: 111
Retry Rate: 24%

	ESSID	Air Time	BSSIDs	Clients	Effective Data Rate	Retry Rate	Channel
🟧	iPad-De	7,024.	1	27	3.1	24	52
🟨	voice-w	93.68	1	47	19.8	3	52
🟩	Unknov	107.13	1	39	6	38	52
🟦	Broadca	50.00	1	75	--	0	52
🟪	Interop	60.10	1	25	6.2	5	52
🟪	Interop	44.38	1	24	6	0	52
🟥	HP Blog	27.42	1	36	--	30	52
🟥	Hewlett	21.92	1	2	--	0	52

metageek

Free 7-day Trial

www.metageek.com/downloads

metageek
EyeP.A.

Free WireShark Color Profile

tinyurl.com/lbss2dy

Pricing

metageek Eye P.A.

Capture with
AN AP, MAC,
OR LINUX

$499

metageek Eye P.A. +

Capture in Windows with
RIVERBED
AIRPCAP NX

+

$1149
($50 off)

AIRPCAP NX FEATURES

- Native Eye P.A. Support
- Capture full 802.11n
- 802.11ac airtime calculations
- 2x2 MIMO

Questions?

Joel Crane, CWNA, CWAP

Human Interface (Training and Support)

Contact: support.metageek.com

Twitter: @FuelCellWiFi

metageek

metageek

Thanks for Attending!