

Eye P.A. User Guide

 support.metageek.com/hc/en-us/articles/202298760-Eye-P-A-User-Guide



Table of Contents

- System Requirements
- Installation
- Direct Capture
- Compatible File Formats
- Main Views
- Data Visuals
- Associated Data Table
- Analyze
- Copy to Clipboard
- Frequently Asked Questions
- Understanding Colors
- How to get a PCAP File

System Requirements

OPERATING SYSTEM: **Microsoft® Windows XP, Vista, 7, 8**

OS X VIRTUALIZATION: **VMware Fusion, Parallels**

DISPLAY RESOLUTION: **1024x768**

.NET FRAMEWORK: **4.0 (or better)**

RAM: 4 GB recommended

Installation

Download

MetaGeek Software

AirPcap NX Driver (if using a Riverbed AirPcap NX)

Run the Installer

Locate the installation file and run it. Follow the installer prompts.

If you are using an AirPcap NX to obtain packet captures, install the AirPcap NX driver as well.

Run Eye P.A.

In Windows 7, click the **Start** button, click **All Programs > MetaGeek > Eye P.A.**

In Windows 8, press the **Windows** key on the keyboard, type **Eye P.A.**, and press **Enter** or click the icon.

Direct Capture

Eye P.A. can capture 802.11 packets with an accompanying AirPcap NX USB adapter.

To begin, connect your device to your computer's USB port and open Eye P.A. Click the **Start** tab at the top of the screen. Here you will select the device that you would like to capture with, as well as the band and channel.

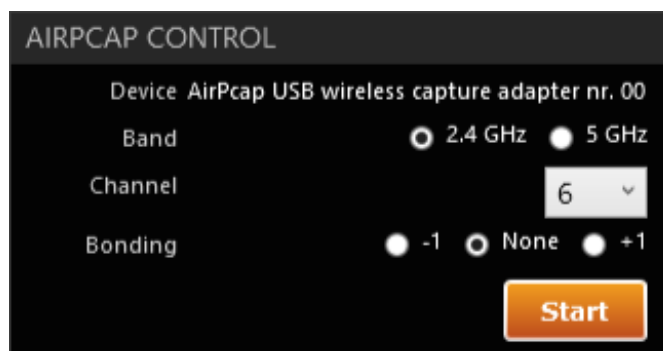


Each AirPcap NX can capture one channel at a time. Up to three AirPcap NX's can be used to capture on multiple channels, simultaneously.

Click **Start Capture** to begin accumulating raw 802.11 frames.

Compatible File Formats

Eye P.A. visualizes 802.11 captures from a variety of sources. Captures can be obtained from within Eye P.A. with an AirPcap NX in Windows, Linux, [the Wireless Diagnostics tool in macOS](#), or from an access point.



Note: Files containing ethernet traffic are not compatible with Eye P.A.

.pcap and .wcap

Not all .pcap files are structured in the same way. Eye P.A. requires Radiotap or 802.11-common headers to calculate wireless packet airtime. The most common tool used to generate compatible captures is Wireshark for Mac or Linux.

.pcapng (Wireshark 1.8)

In 2012, Wireshark changed the default filetype to .pcapng. Any version of Wireshark installed after 2012 will support this filetype. Pcapng allows more flexibility, like extended-interface host information and annotation, but is not compatible with all tools.

.pkt and .apc (WildPackets OmniPeek)

While experimental, WildPackets OmniPeek files that contain 802.11 frames can usually be opened in Eye P.A. if they have the extensions .pkt or .apc. Each of these files will export to Wireshark in the same manner as a .pcap or .pcap-ng file.

.cap (Microsoft Network Monitor)

Limited support for 802.11 capture is available in Windows with the release of Network Monitor 3.4. The full monitor-mode capabilities are limited to certain wireless cards and might provide little-to-no information regarding data rate, RSSI, and 802.11n frames depending on your wireless card.

.ncf (CommView for WiFi)

To acquire full 802.11n captures on a Windows machine without an AirPcap NX, use CommView for WiFi, which supports more wireless adapters than nearly any other packet capture solution, but has limitations much like Microsoft Network Monitor.

Main Views

Visualize



Packets



Work Flow



Across the top of Eye P.A. are 4 different tabs called the **Work Flow**.

- Capture Tab - Open captures, or create new ones with the AirPcap Nx
- Visualize - View captures with time graphs, multilayered pie charts, and data tables
- Analyze - Automatic expert analysis
- Packets - View conversations between AP's and clients

Filter Bar



The top of the filter bar is where the user can filter by SSID or Vendor, MAC address, channel, data rate, RSSI, and subframe type.

Users can apply exclusive filters to quickly remove data by selecting the - before the field. Selecting + will build an inclusive filter.

The **Data Rate** and **RSSI** can also be filtered based on a **greater than** or **less than** selection. For example, these filters could be used to remove all frames with an RSSI less than or equal to -90 dBm.

It can also be helpful to filter out certain types of packets like beacons, acknowledgements, or other non-essential frame types to focus on the packets that matter the most. To remove specific frame types, click **Subframe Filters** drop-down menu, and uncheck the frames as needed.

Filter Bread crumbs

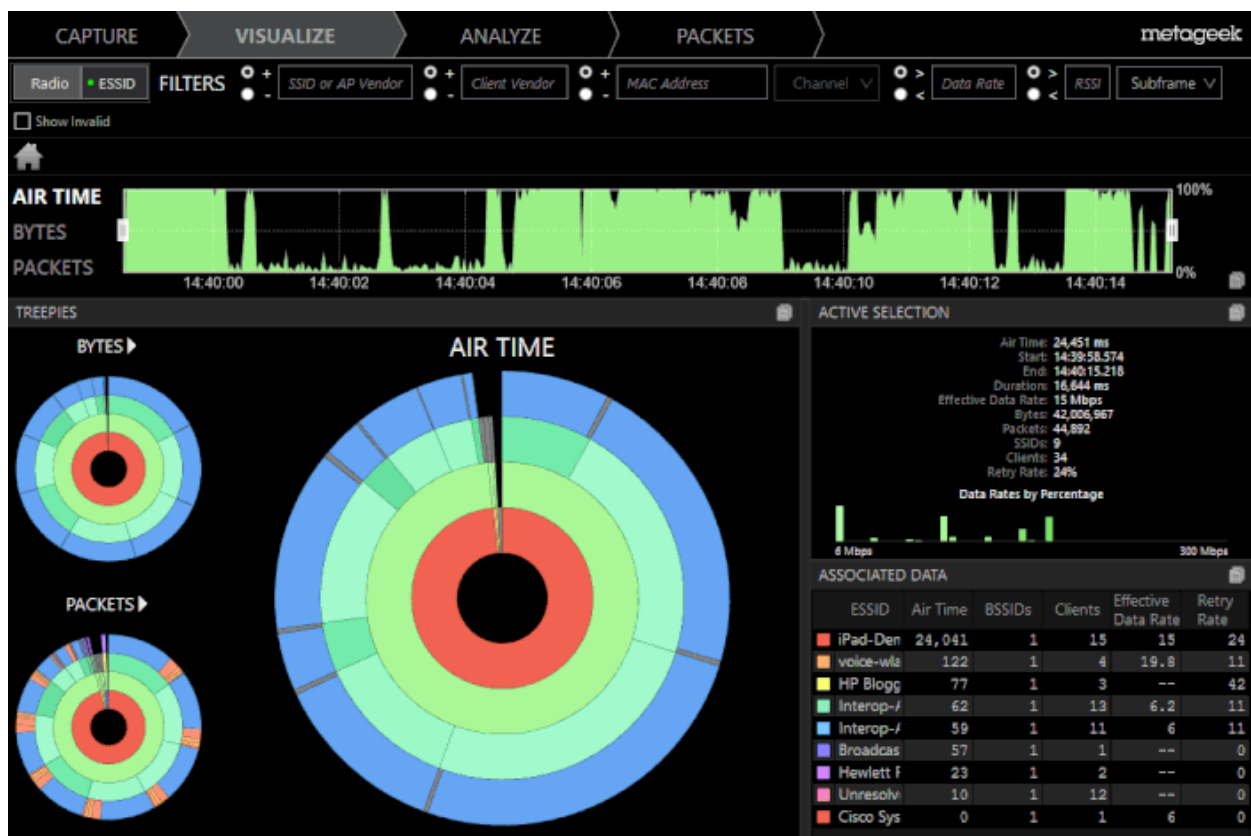


The filter bread crumbs represent the current requirements the user has manually entered as filters or navigated to by means of the multi-layered pie chart. To remove a crumb click the **x**. Bread crumbs will either be black to represent exclusive filters or gray to show inclusive filters.

*Note: Filtering packets will affect the data exported to Wireshark. For example if **beacons** are unchecked from the display filters, they will be excluded from the data export.*

Adjustable Time Graph

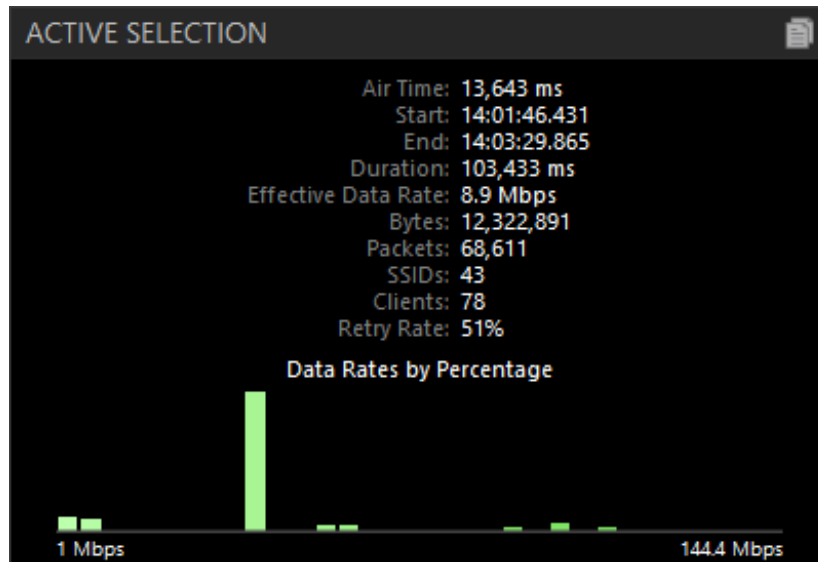
Eye P.A. displays a historical summary of the data capture in the top time slider.



The darker yellow in the background represents all frames in the capture, while the brighter yellow in the foreground of the graph represents the data currently in view after navigation and filters have been applied. Sometimes a capture may have a dark yellow without any filters applied. This means some of the frames were corrupted and are invalid for reliable display. To see them in the graphs add a check to the **Show Invalid** checkbox in the filter bar.

To the left of the Time Graph are toggles for changing the data to reflect **Air Time**, **Bytes**, and **Packets**.

Active Selection



The **Active Selection** legend displays the related data to the center of the multi-layered pie chart. This data will change as the user drills down through layers. It displays total airtime, bytes, number of packets, SSIDs, clients, and retry rate percentages. Below this information is a bar chart displaying the percentage of clients active at each detected data rate.

Associated Data Table

ASSOCIATED DATA						
ESSID	Air Time	BSSIDs	Clients	Effective Data Rate	Retry Rate	
Bronco-Guest	9,506	8	59	8.9	61	
Bronco-Wireless	2,877	8	21	8.9	26	
Unresolved	359	1	45	--	0	
Broadcast	735	1	1	--	0	
Icron Technologies Corporation	135	1	1	5.2	91	
Cisco Systems, Inc	28	23	2	1	0	
Unknown	4	1	1	18	0	

The Associated Data Table provides details for innermost ring of the multi-layered pie chart.

Table Columns

Client - Identifier for each client

Air Time -The amount of time used to transmit

Bytes - The amount of data transferred

Packets - The total number of packets per SSID, client, or subframe type

Effective Data Rate - The average data rate achieved between the client and access point conversation

Retry Rate - The percentage of packets that had to be resent

As you sort the column headers, the treepie will be rearranged. The sorted data is displayed clockwise in the order indicated in the table data.

ESSID and Radio Grouping

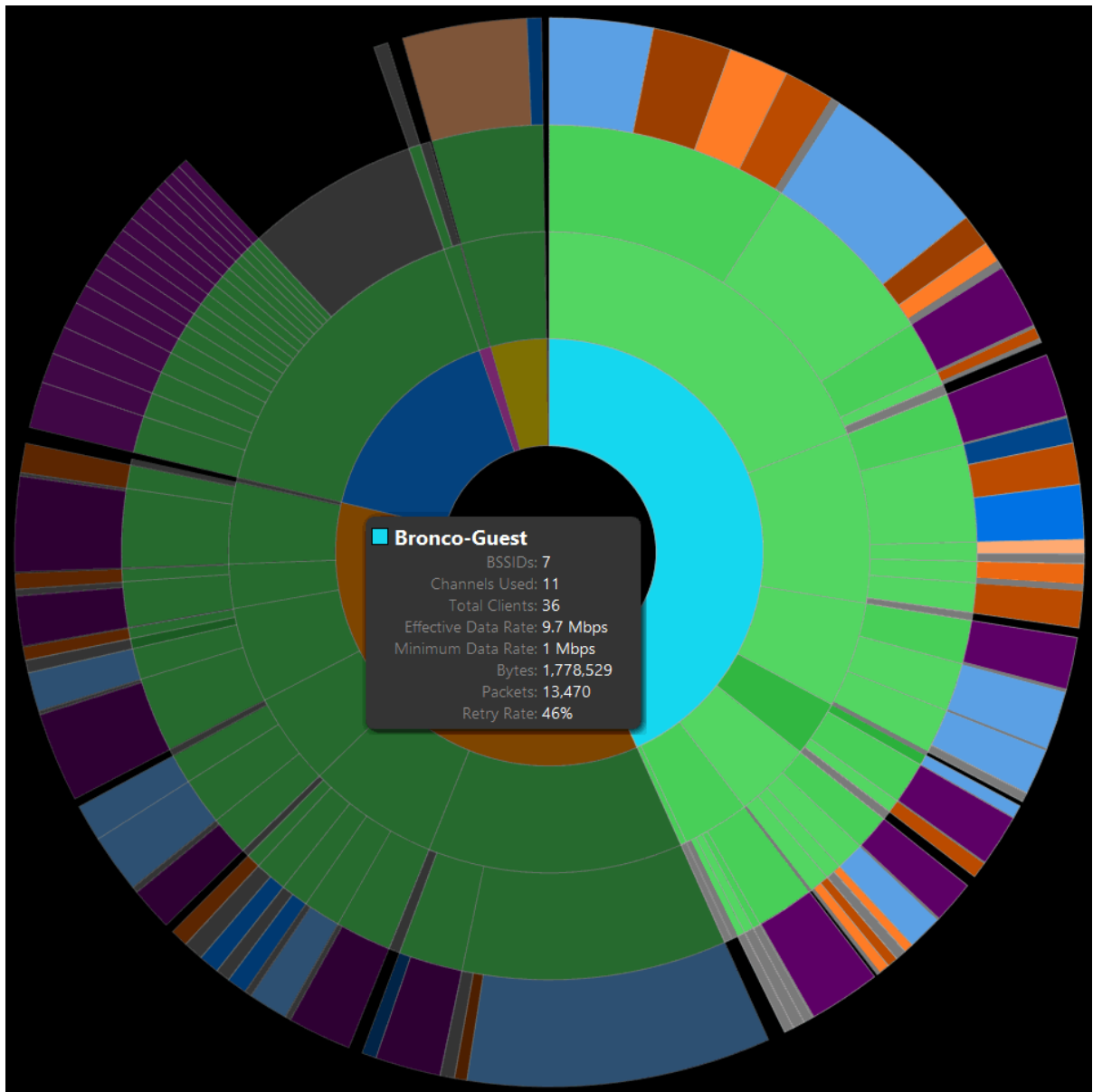
Select the **Radio** button to group virtual SSID's together, or select the **ESSID** button to group access points with the same SSID together in the multi-layered pie chart and Associated Data table.

ESSID Grouping



An **ESSID** refers to a group of unique access points with the same SSID, typically spread out across a building or campus.

When ESSID Grouping is selected, the innermost ring of the multilayered pie chart refers to the **ESSID**, or the name of your network. The next ring in the pie chart shows each individual SSID (or unique access point) that belongs to the ESS.



ESSID Grouping also extends into the Associated Data table; each line of the table groups an ESS.

ASSOCIATED DATA							
ESSID	Air Time	BSSIDs	Clients	Effective Data Rate	Retry Rate	Channels	
Bronco-Guest	1,203.42	7	36	9.7	46	11	
Bronco-Wireless	986.53	7	29	3.5	33	11	
Broadcast	442.60	1	66	--	0	11	
Unknown	24.91	2	7	18	0	11	
CISCO SYSTEMS, INC.	118.10	2	4	1.2	4	11	
CWFN	5.00	1	2	--	0	11	

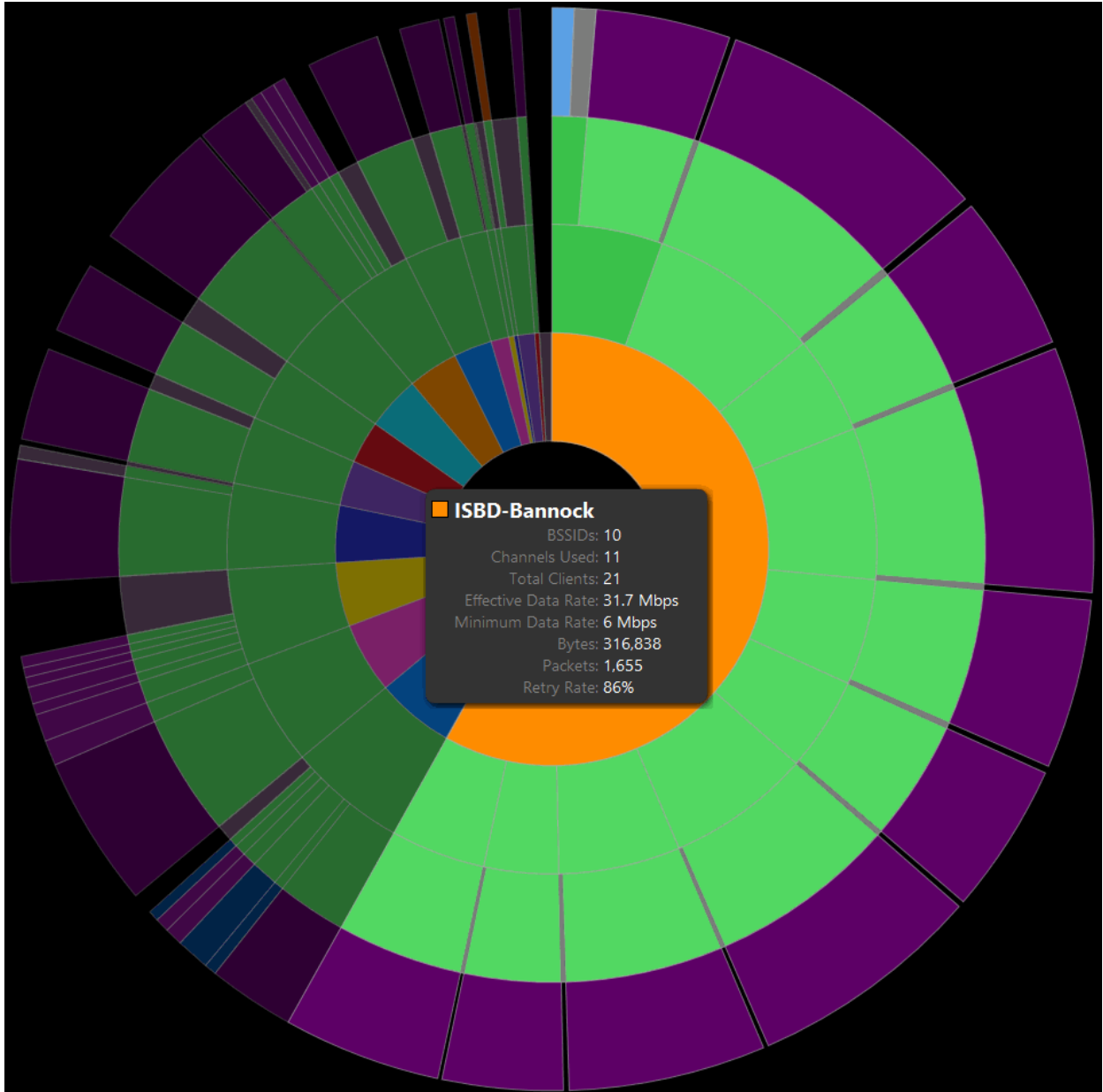
Each line in the Associated Data table represents a group of access points with the same SSID.

Radio Grouping

A **Radio** refers to a group of virtual SSID's on the same access point, such as "MetaGeek-Developers" and "MetaGeek-Operations".

When **Radio Grouping** is selected, the innermost ring of the multilayered pie chart refers to an individual radio, or unique access point on your network. The next ring in the pie chart shows each virtual SSID on that radio.

Note: This network has a lot of virtual SSID's. Notice how much airtime they are consuming, and they are only beaconing. Eye P.A. makes this type of visualization really easy!



ESSID Grouping also extends into the Associated Data table; each line of the table groups an ESS.

If your Aruba or Cisco access point has a name configured, the name will be displayed.

ASSOCIATED DATA						
Radio	AP Alias	Number of SSIDs	Clients	Air Time	Effective Data Rate	
18:33:9D:00:0	AP-mbeb2-common	1	10	7,605	9.3	
18:33:9D:00:0	AP-mbeb2-common	1	7	1,799	7.7	
2C:36:F8:00:0	ap-mbeb-common-	1	17	1,191	5.4	
2C:36:F8:00:0	ap-mbeb-common-	1	7	531	15	
F4:7F:35:00:1	ap-mbeb-outdoor	1	5	228	17.9	
F4:7F:35:00:0	ap-mbeb-outdoor	1	7	122	13.9	
68:BC:0C:00:2	ap-mbeb1106-1	1	9	319	1.4	
68:BC:0C:00:1	ap-mbeb-2010-2	1	8	131	25.5	
68:BC:0C:00:1	ap-mbeb1106-1	1	6	95	15.8	
68:BC:0C:00:0	ap-mbeb-2010-2	1	5	109	12.8	
68:BC:0C:00:3	ap-mbeb1107-1	1	5	95	10.2	
68:BC:0C:00:6	ap-mbeb1107-1	1	12	93	9.7	
FF:FF:FF:FF:F		1	45	359	--	

Each Line in the **Radio** column represents a group of SSID's on the same access point.

Packet Viewer

PACKETS								
Packet Number	Time Stamp	Time Delta (ms)	Flags	Subframe Type	Channel	Data Rate (Mbps)	RSSI (dBm)	SSID
1	14:01:46.43197	0.000		ACK	1	18	-60	Unresolved
2	14:01:46.43223	0.252		QoS Data	1	1	-59	Bronco-Guest
3	14:01:46.43223	0.002		ACK	1	18	-54	Bronco-Guest
4	14:01:46.43273	0.501		ACK	1	18	-69	Bronco-Guest
5	14:01:46.52788	95.154		QoS Data	1	6	-56	Bronco-Guest
6	14:01:46.52789	0.003		QoS Data	1	6	-55	Bronco-Guest
7	14:01:46.52789	0.003		Beacon	1	18	-74	Bronco-Wireless
8	14:01:46.53588	7.989		Beacon	1	18	-57	Bronco-Guest
9	14:01:46.53588	0.003		Data	1	18	-58	Bronco-Guest
10	14:01:46.53798	2.095		QoS Data	1	54	-55	Bronco-Wireless
11	14:01:46.53798	0.002		ACK	1	18	-64	Bronco-Wireless
12	14:01:46.53873	0.753		QoS Data	1	54	-55	Bronco-Wireless
13	14:01:46.53910	0.372		QoS Data	1	54	-55	Bronco-Wireless
14	14:01:46.53911	0.002		ACK	1	18	-64	Bronco-Wireless
15	14:01:46.53985	0.742		QoS Data	1	54	-62	Bronco-Wireless
16	14:01:46.53985	0.001		ACK	1	18	-63	Bronco-Wireless
17	14:01:46.53985	0.003		ACK	1	18	-54	Unresolved
18	14:01:46.54223	2.375		Beacon	1	18	-64	Bronco-Guest
19	14:01:46.54223	0.002		Data	1	18	-65	Bronco-Guest
20	14:01:46.54486	2.635		ACK	1	18	-54	Unresolved
21	14:01:46.56364	18.774		Probe Respo	1	18	-57	Bronco-Guest
22	14:01:46.56386	0.222		Probe Respo	1	18	-58	Bronco-Guest
23	14:01:46.56650	2.642		Beacon	1	18	-58	Bronco-Wireless
24	14:01:46.56824	1.735		QoS Data	1	54	-62	Bronco-Wireless
25	14:01:46.56824	0.002		ACK	1	18	-65	Bronco-Wireless
26	14:01:46.57288	4.642		Beacon	1	18	-64	Bronco-Wireless

Eye P.A. will display the basic details of individual packets in the **Packets Table**, including **Subframe Type**, **RSSI**, **Data Rate**, and **Destination**. The user can define the columns in the packet viewer by right-clicking on a header and selecting the details they wish to view. Apply filters from the Filter Bar or use the treepie on the left to drill down into the packet viewer.


PACKETS						
Packet Number	Time	Source Address	Destination Address	Flags	Subframe Type	
3	14:01:46.56386				ACK	
4	14:01:46.56386				ACK	
5	14:01:46.56386				QoS Data	
6	14:01:46.56386				QoS Data	
7	14:01:46.56386				Beacon	
8	14:01:46.56386				Beacon	
9	14:01:46.56386				Data	
10	14:01:46.56386				QoS Data	
11	14:01:46.56386				ACK	
12	14:01:46.56386				QoS Data	
13	14:01:46.56386				QoS Data	
14	14:01:46.56386				ACK	
15	14:01:46.56386				QoS Data	
16	14:01:46.56386				ACK	
17	14:01:46.56386				ACK	
18	14:01:46.56386				Beacon	
19	14:01:46.56386				Data	
20	14:01:46.56386				ACK	
21	14:01:46.56386				Probe Respo	
22	14:01:46.56386		0.222		Probe Respo	
23	14:01:46.56650		2.642		Beacon	

Eye P.A. will automatically remove columns as they become redundant due to the filtered data set. For example, if the BSSID is the same in every frame, it will no longer be represented in a column.

To bring back any missing columns, right-click at the top of the packet viewer table and select the needed columns.

Flags Column

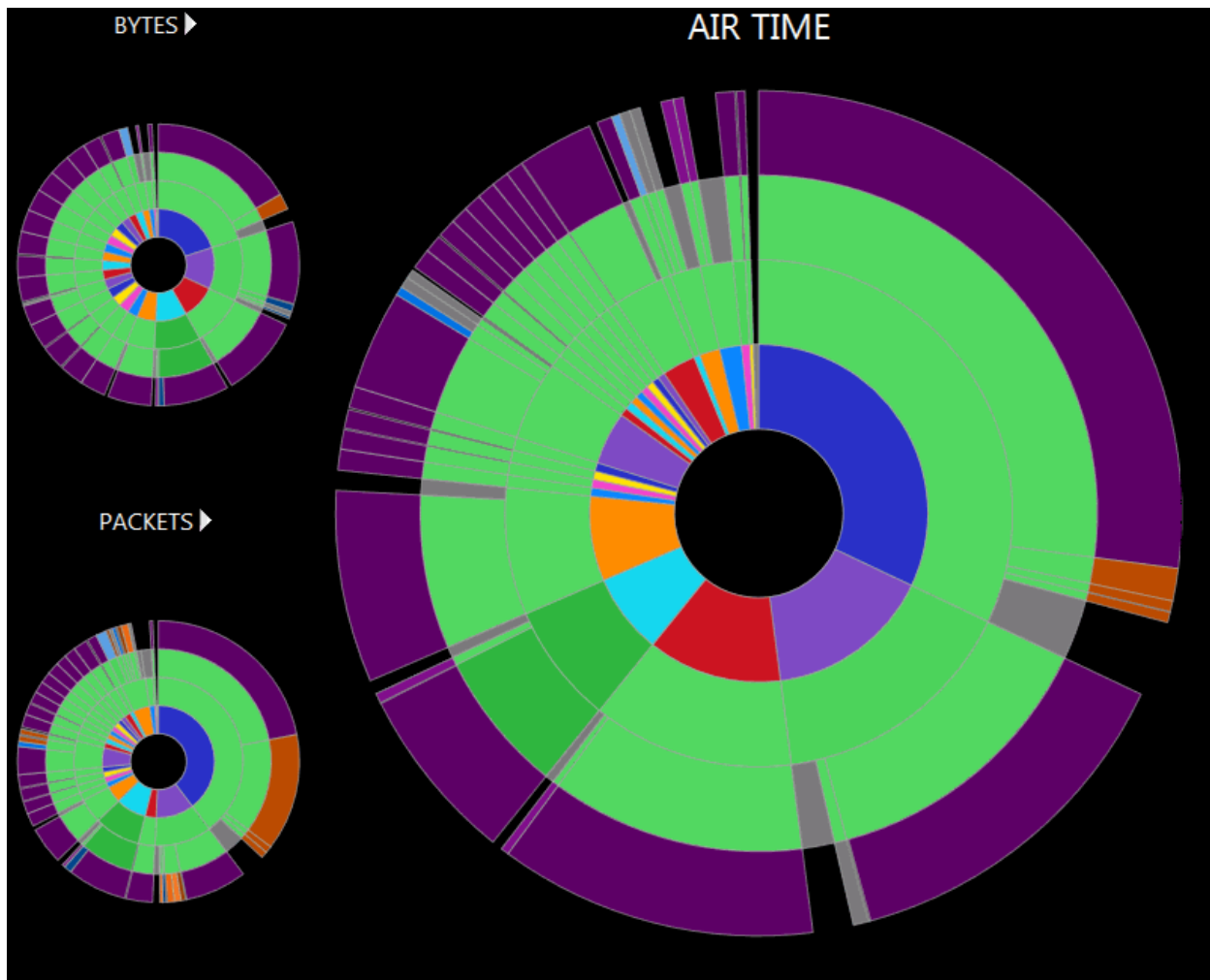
The **Flags** column highlights frames that are:

 - Retransmissions

! - Invalid Frames

Data Visuals

Multi-Layered Pie Charts



There are three multi-layered pie charts in the **Visualize** tab. Eye P.A.'s multi-layered pie charts continually divide each slice into more slices based on percentages.

Ring Order

Starting from the inside and working outward, the default ring order in Eye P.A. is:

1. Radio Group/BSSID Group
2. SSIDs
3. Clients
4. Subframe Types

To alternate between the different types of data, click the arrow above and multi-layered pie chart to select **Air Time**, **Packets**, or **Bytes** to move it to the featured position. The size of each slice is proportionate to the total packets, bytes, or air time utilized.

Data Types

Packets - The proportionate amounts of packets in comparison to the total captured.

Bytes - 100% of the total data captured in bytes. Each slice is the total data sent by BSSID or client.

Air Time - The proportionate amount of air time each station utilized. It is important to note that lower data rates use more air time than higher data rates to transfer the same number of bytes. Wireless communication is half-duplex, so only one device can transmit at a

time. Therefore, the amount of time each station takes prohibits the other stations from transmitting.

Drill-Down

Each element in the multi-layered pie chart can be clicked on, drilling down and breaking the data down into a new pie chart for easy troubleshooting.

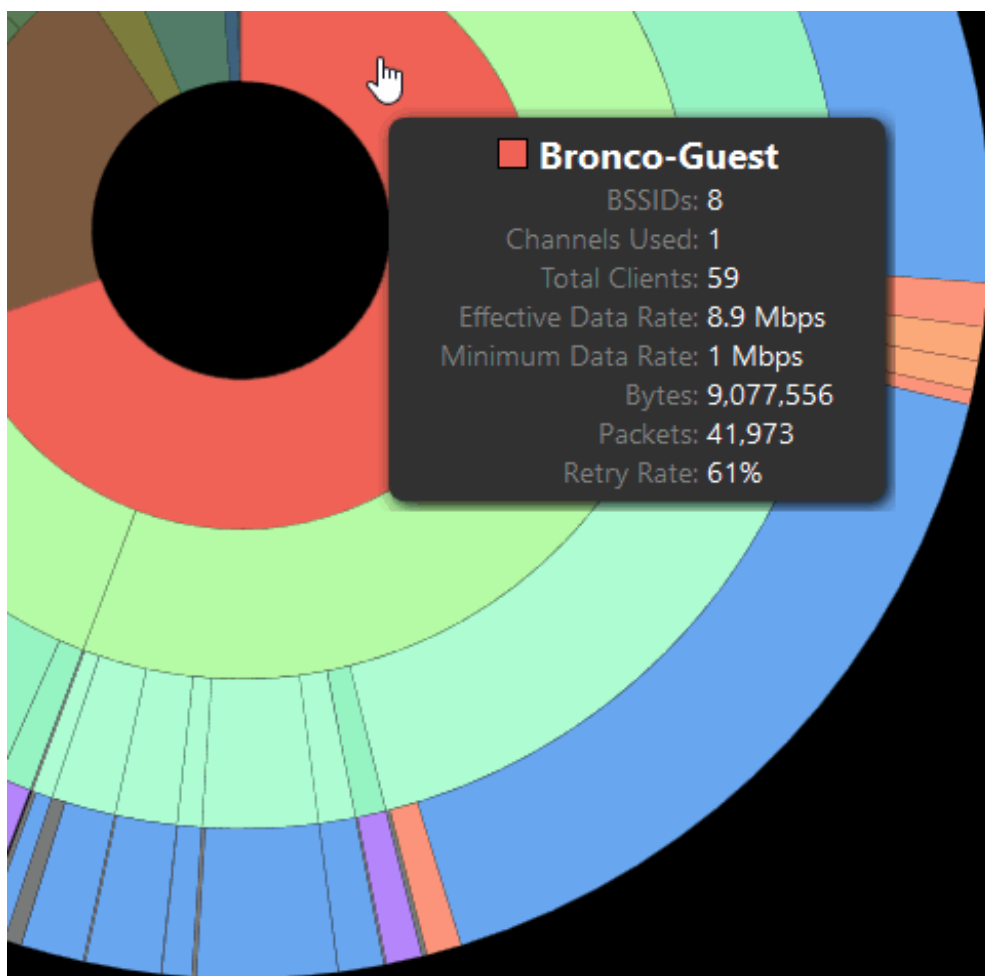
To return to a parent layer, click the center of the pie chart, or the home icon in the top left of the window. The layer directly outside of the center is represented in the table. Double clicking on a row will change the pie charts to reflect the selected data.

Note: If there are multiple channels present in your capture, a message will be displayed across the pie chart.

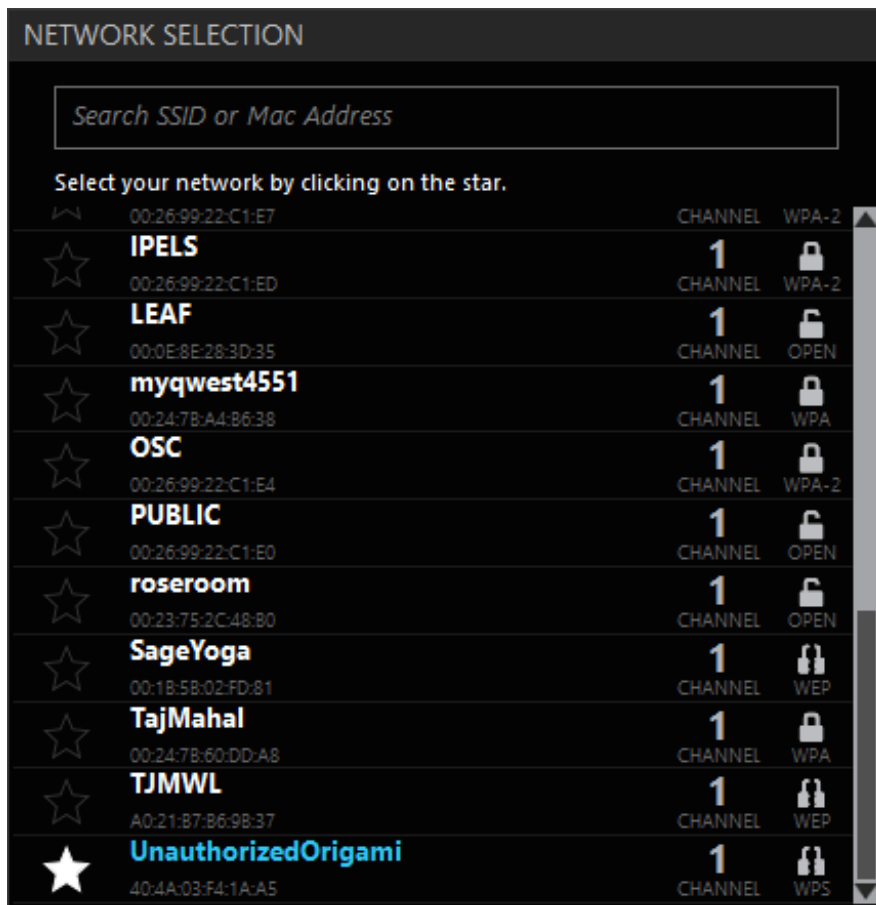
*To correct this, simply select the channel you're most interested in from the **Channels** filter.*

Hover (Inspector Tool)

When hovering the mouse over a slice in the multi-layered pie chart, a tool tip will appear, providing additional details like data rates, packet counts, and retry rates. This information is also displayed in the Associated Data Table.

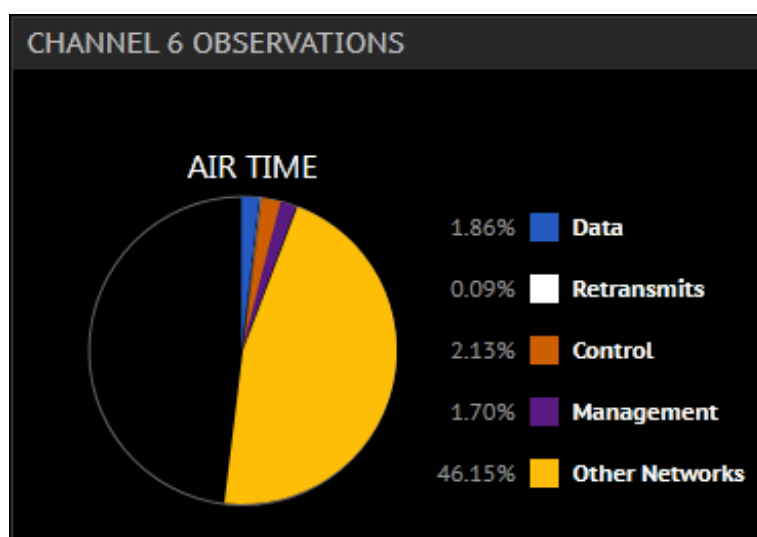


Analyze



Eye P.A. examines a variety of aspects of your capture, and will provide analysis based upon what it finds.

After starring the networks you are interested in, a pie chart will be shown that displays the percentages of the starred network's data, retransmits, control, and management packets compared to the percentage of packets belonging to other networks. The remaining black area of the pie chart represents the amount of available air time.



Below the pie chart, you will find suggestions for adjustments you can make in order to better your wireless network's performance. The areas where Eye P.A. looks for improvements include protection mechanisms, presence of legacy rates, high retransmission rates, encryption settings, and channel choice issues.

UnauthorizedOrigami (F4:1A:A5)

OBSERVED ISSUES
WPS DETECTED [LEARN MORE](#)

SUGGESTED SOLUTIONS
Disable WPS Security Setting [LEARN MORE](#)

OBSERVED ISSUES
LEGACY DATA RATES DETECTED [LEARN MORE](#)

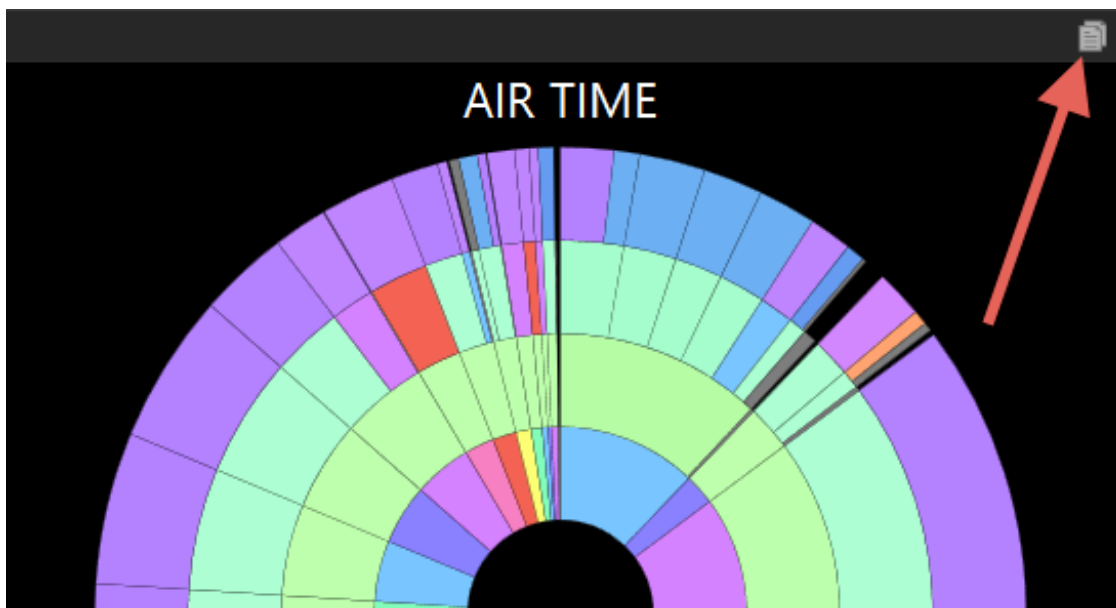
SUGGESTED SOLUTIONS
Disable the data rates 1, 2, 5.5, and 11Mbps unless supporting legacy devices. [LEARN MORE](#)

OBSERVED ISSUES
PROTECTION MECHANISM [LEARN MORE](#)

SUGGESTED SOLUTIONS
Eliminate legacy devices so protection can be disabled [LEARN MORE](#)

Any applicable tips will be shown for each network you star. Clicking the clipboard icon to the right of your selected network's name in the tips window will copy the tips for that network to your clipboard, allowing for easy export.

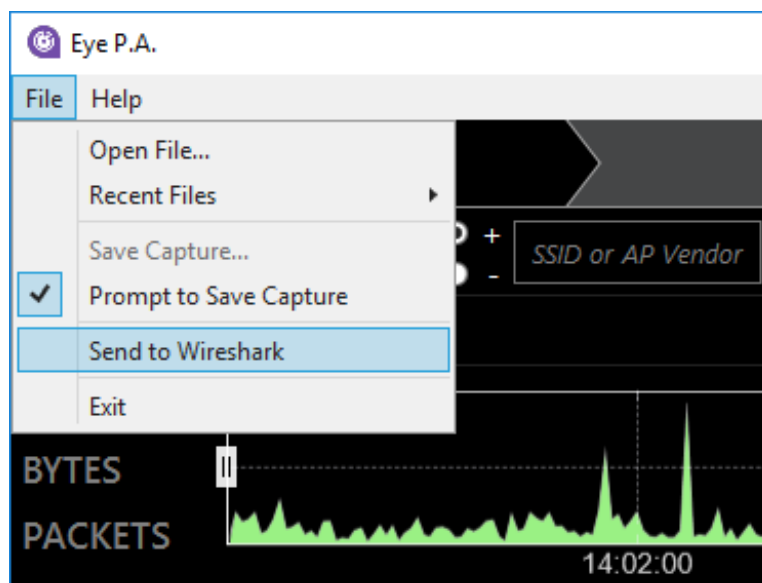
Copy to Clipboard



Eye P.A. contains a clipboard icon in each pane. Clicking this will copy the contents of the pane to the clipboard. The time graph and treepies will be copied as images, while the active selection and associated data table will be copied as text, ready to paste into a text editor or spreadsheet application.

Send to Wireshark

Send any layer of the multi-layer pie chart to WireShark by clicking **File** in the main menu and then **Send to Wireshark**. Conveniently, Eye P.A. automatically bundles up the data in the current multi-layer pie chart, applies the filters you've drilled down to select, and sends all of the packets to Wireshark for more in-depth analysis.



Frequently Asked Questions

What is the "Broadcast" SSID?

In 802.11, clients or stations can broadcast management frames called Probe Requests. Probe requests occur when stations are looking for access points they previously connected with. These do not occur in a network but Eye P.A. groups them into a broadcast group for organizational simplicity.

Why won't Eye P.A. open my .pcap file?

There are currently two types of .pcap files that Eye P.A. can open. The .pcap must contain 802.11 frames with Radiotap or 802.11-common PPI headers. Typically these captures are created using:

- Wireshark with an AirPcap adapter
- OS X with the WiFi Diagnostics tool, or Wireshark in monitor mode
- Linux with Wireshark or Kismet
- A .cap, .pcap, or .pcap-ng from an enterprise access point

Why are packet counts different in Wireshark and Eye P.A.?

Sometimes the capturing device receives packets that are malformed or corrupt. Eye P.A. drops any packets that do not have a proper Frame Check Sequence (FCS) in the packet, even though Wireshark will display those packets.

What is a hidden SSID?

Some wireless network administrators may hide their SSID, which tells the access point to not broadcast its name. Typically the only users who know the name of the wireless network can connect to a hidden SSID.

Note: This method does not provide additional security.

What is the "miscellaneous" grey slice?

The gray slices contain small pieces of valid packet data from a lot of different sources. For example, a capture file may have 10 top talkers that make up 90 percent of the total traffic. However, 100 clients make up the remaining 10 percent. Instead of drawing each slice, Eye P.A. aggregates them into miscellaneous slices.

The miscellaneous slice is colored gray because it may contain management, data, and control frames. To view any of the data in the gray slice, click on its parent slice and all of the data will be drawn.

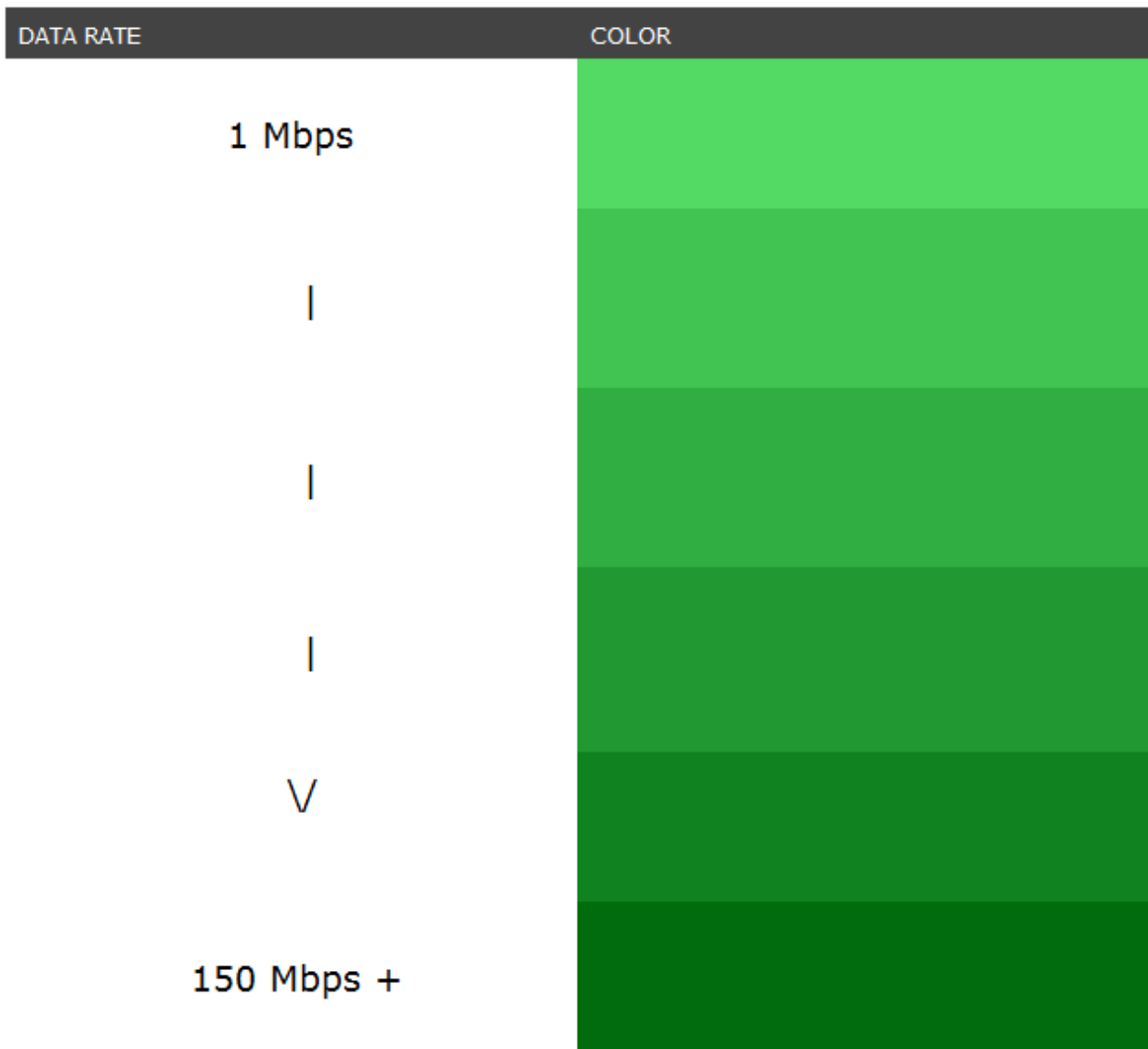
How is the Effective Data Rate calculated?

The effective data rate reflects the data frames transferred to and from a BSSID and client. Eye P.A. takes the total bytes transferred and divides it by the total air time. The air time for each frame is calculated by dividing the bytes in the payload by the data rate for that frame.

Understanding Color

Data Rate

The second layer of the multi-layered pie chart (SSID ring) is colored by the average data rate of the traffic. The shade of green is based on a sliding scale. The minimum average data rate captured is represented by light green, while the highest is represented by dark green, with shades in between.



Data Frames

Data frames carry the actual data passed down from higher layer protocols.

DATA PACKET TYPE	COLOR
QoS Data	Lightest Blue
Data (Other)	Light Blue
QoS Null	Medium Blue
Null Function No Data	Dark Blue
Data (Normal)	Darkest Blue

Management Frames

Usually the majority of frames on the 802.11 network. Used by wireless stations to join and leave networks.

MANAGEMENT PACKET TYPE	COLOR
Disassociation	Lightest Purple
Deauthentication	
Management (Other)	Light Purple
Authentication	Medium-Light Purple
Association Request	Medium Purple
Association Response	
Reassociation Request	Medium-Dark Purple
Reassociation Response	
Probe Request	Dark Purple
Probe Response	
Beacon	Darkest Purple

Control Frames

Control frames help with the delivery of the data frames. Control frames must be able to be heard by all stations; therefore, they must be transmitted at one of the basic rates. Control frames are also used to clear the channel, acquire the channel, and provide unicast frame acknowledgments.

CONTROL PACKET TYPE	COLOR
PS Poll	
Action	
Control (Other)	
RTS	
CTS	
ACK	
Block ACK	
Block ACK REQ	