eye P.A.

visual packet analysis

metageek

Eye P.A. visual packet analysis

Table Of Contents

SYSTEM REQUIREMENTS

1) Microsoft .NET Framework 4 Client Profile
   (Eye P.A. installer will direct you to download)

2) Microsoft .NET Framework 4 Extended
   (Eye P.A. installer will direct you to download)

INSTALLATION

1) Download the latest version of Eye P.A. from MetaGeek
   http://www.metageek.net/products/eye-pa/download

2) Once the file has finished downloading, double-click on the installer. Go through the installation dialogue. The program will install under the directory "MetaGeek."

3) Double click on the icon "Eye P.A." to start the application.

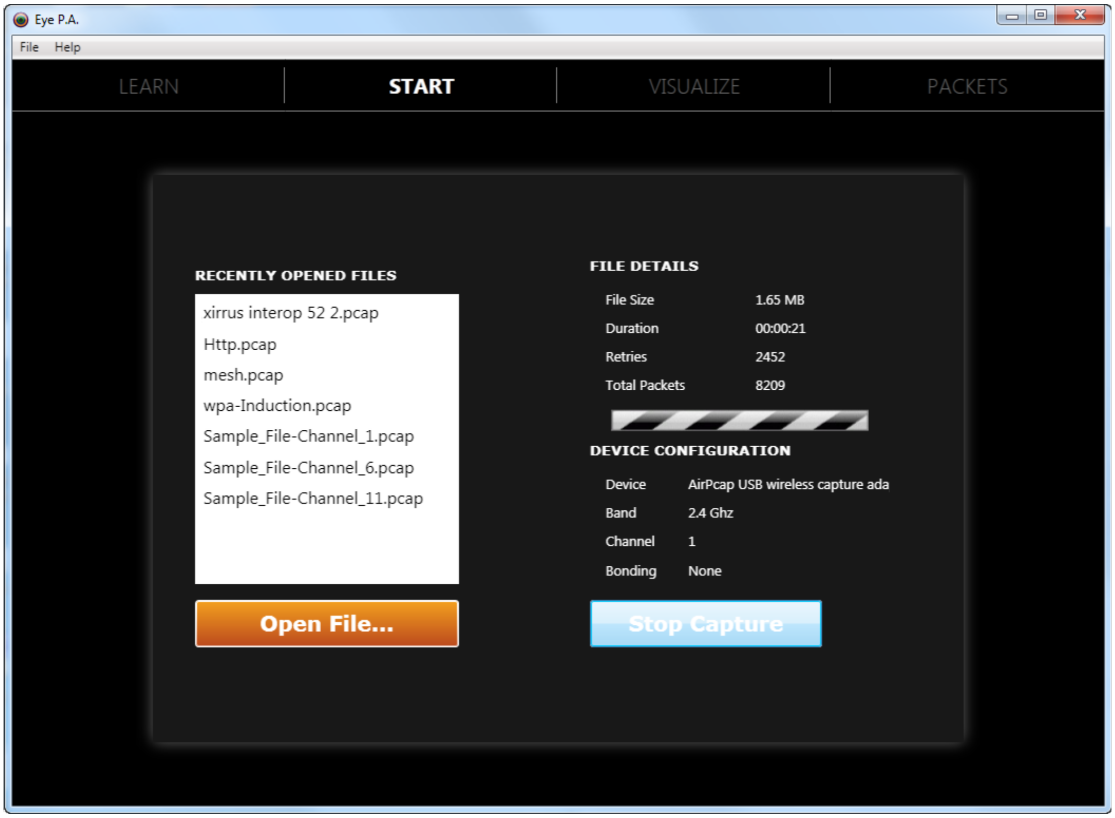
If this is the first time Eye P.A. is run, it will ask for a license key.

If you do not have a license key, click the "Continue Trial" button to run Eye P.A. in full evaluation mode free for 15 days.

LIVE 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 and open Eye P.A. Click the START category at the top of the screen. Here you will select your AirPcap, the 2.4 or 5 GHz band and the channel that you wish to scan. Click START CAPTURE to begin accumulating raw 802.11 frames.



RECENTLY OPENED FILES

xirrus interop 52 2.pcap
Http.pcap
mesh.pcap
wpa-Induction.pcap
Sample_File-Channel_1.pcap
Sample_File-Channel_6.pcap
Sample_File-Channel_11.pcap

FILE DETAILS

File Size	1.65 MB
Duration	00:00:21
Retries	2452
Total Packets	8209

DEVICE CONFIGURATION

Device	AirPcap USB wireless capture ada
Band	2.4 Ghz
Channel	1
Bonding	None

COMPATIBLE FILE FORMATS

Eye P.A. visualizes 802.11 captures from a variety of sources.
Files containing ethernet traffic are not compatible with Eye P.A.

.pcap

Not all .pcap files are structured in the same format. Eye P.A. requires the use of the Radiotap or 802.11-common headers to calculate the airtime of the wireless packets. The most common program to generate compatible captures is WireShark for Windows, Mac or Linux.

.pcapng (WireShark 1.8)

WireShark did change its default file type in 2012 to .pcap-ng. Any version of Wireshark installed within the last year will support this file type. Pcap-NG allows more flexibility like extended-interface and host information, and contains expanded annotation, but it is not compatible with all tools.

.pkt & .apc (WildPackets Omnipeek)

WildPackets Omnipeek files containing 802.11 frames can be opened in Eye P.A. if they have the extension .pkt or .apc. Each of these files will export to WireShark in the same manner .pcap or .pcapng will.

.cap (Microsoft Network Monitor)

Microsoft added limited support for 802.11 captures 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 access card. However, it is free.

CommView for Wi-Fi (.ncf)

Acquire full 802.11n captures on a windows machine without an AirPcap Nx, use CommView for Wi-Fi. Supporting more wireless adapters than other packet analysis applications, it may have limitations similar to Microsoft Network Monitor.

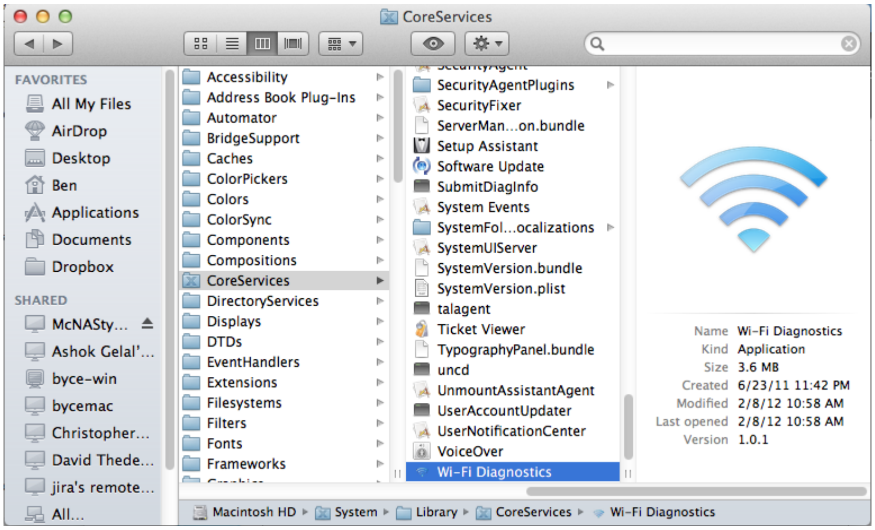
HOW TO GET A .pcap FILE

Eye P.A. is a wireless network data visualization tool. It sorts and displays data that has been captured in a .pcap file in order to make it easy for you to troubleshoot problems with your wireless network.

You can get a .pcap file in a lot of different ways. The ways listed below are the ones we're accustomed to gathering them with. We'd love to hear more about how you use .pcap files in our user forum.

WITH **Mac OS X Lion and WireShark**

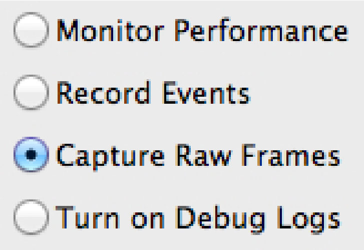
There are two methods in capturing 802.11 frames in Mac OS X Lion.
1) Use the included utility application, "Wi-Fi Diagnostics".



Name Wi-Fi Diagnostics
Kind Application
Size 3.6 MB
Created 6/23/11 11:42 PM
Modified 2/8/12 10:58 AM
Last opened 2/8/12 10:58 AM
Version 1.0.1

Open Finder and navigate to: **/System/Library/CoreServices/**
Scroll down and select the Wi-Fi Diagnostics application.
(you can also make an alias or drag the icon to your dock for easier access later)

Select "Capture Raw Frames"

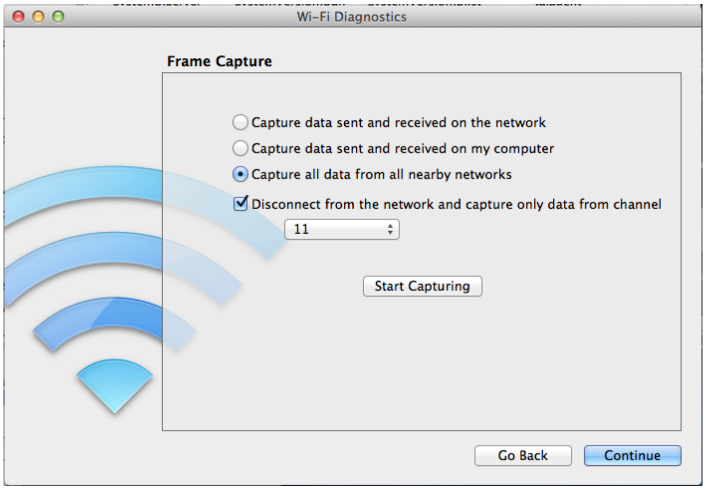


○ Monitor Performance
○ Record Events
● Capture Raw Frames
○ Turn on Debug Logs

Select "**Capture all data from all nearby networks**" and

"**Disconnect from the network and capture only data from channel**"

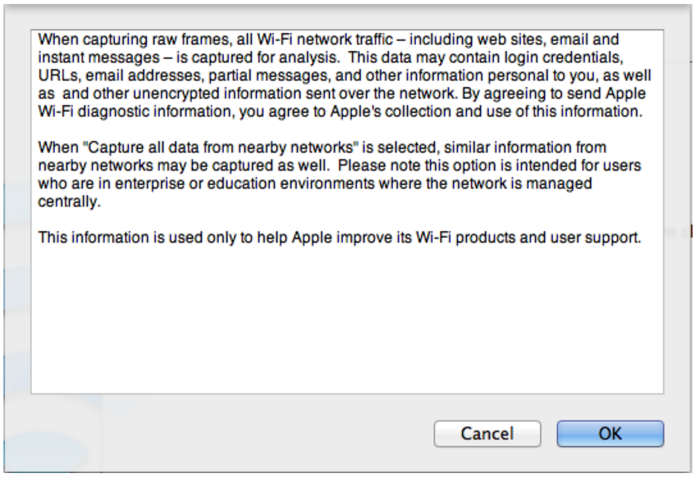
Choose the channel you wish to monitor.



Frame Capture

○ Capture data sent and received on the network
○ Capture data sent and received on my computer
● Capture all data from all nearby networks
☑ Disconnect from the network and capture only data from channel
11

Click "OK" on the text dialogue window.



When capturing raw frames, all Wi-Fi network traffic – including web sites, email and instant messages – is captured for analysis. This data may contain login credentials, URLs, email addresses, partial messages, and other information personal to you, as well as and other unencrypted information sent over the network. By agreeing to send Apple Wi-Fi diagnostic information, you agree to Apple's collection and use of this information.

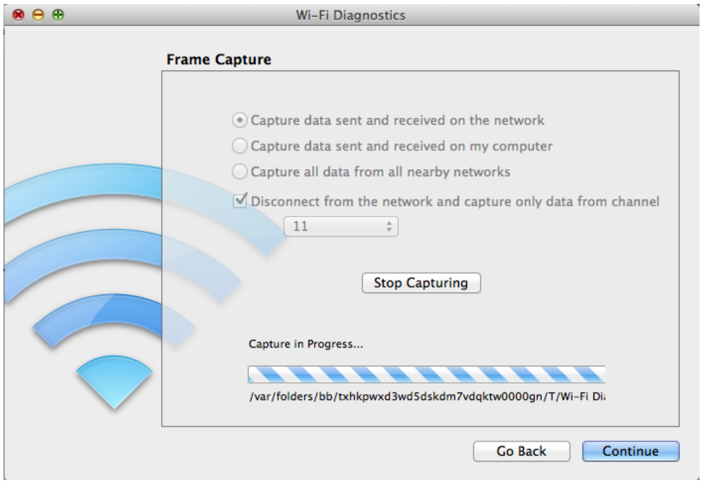
When "Capture all data from nearby networks" is selected, similar information from nearby networks may be captured as well. Please note this option is intended for users who are in enterprise or education environments where the network is managed centrally.

This information is used only to help Apple improve its Wi-Fi products and user support.

Click “Start Capture.”

(Don't make the mistake of clicking “Continue” before making your capture).

Click “Stop Capture” when you are satisfied with the length of time.



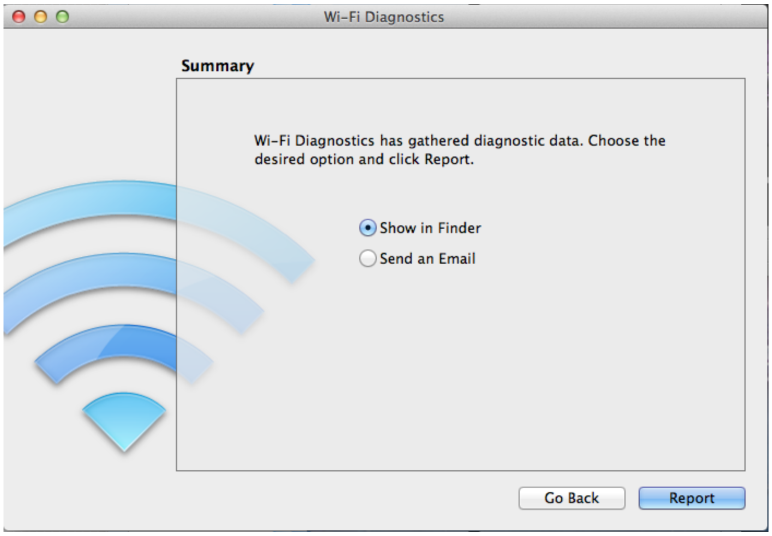
Frame Capture

● Capture data sent and received on the network
○ Capture data sent and received on my computer
○ Capture all data from all nearby networks
☑ Disconnect from the network and capture only data from channel
11

Capture in Progress...

/var/folders/bb/txhkpwxd3wd5dskdm7vdqktw0000gn/T/Wi-Fi Di

Choose "Show in Finder" and extract the .tgz file to reveal a .pcap file that can be opened in WireShark or Eye P.A.



Summary

Wi-Fi Diagnostics has gathered diagnostic data. Choose the desired option and click Report.

● Show in Finder
○ Send an Email

2) Use WireShark to create a pcap file using the internal wireless network interface. Select the **adapter en1** and click **options** to go into the advanced settings. Select "**Capture packets in monitor mode**" and then click **start**. WireShark will begin to log all of the wireless frames. Click **File > Save** to create a .pcap which will create a file that can be opened by Eye P.A.

WITH **Microsoft Network Monitor**

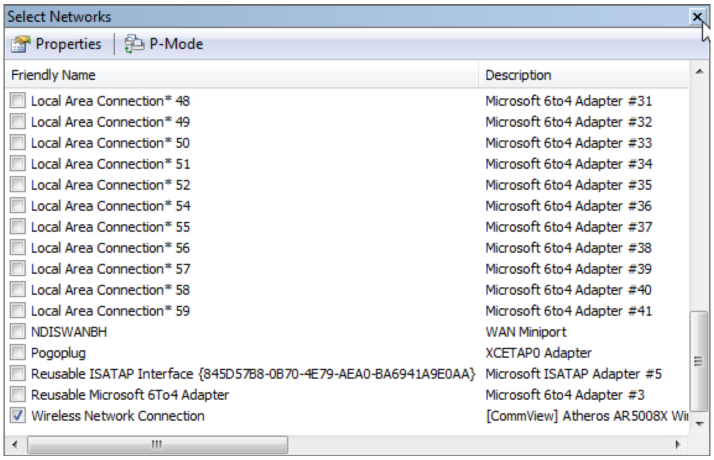
Microsoft Network Monitor is a free tool, but unfortunately it does not accurately portray HT 802.11n frames and data rates. MetaGeek recommends using an AirPcap adapter or CommView for Wi-Fi instead. However, the following will help you create files compatible with Eye P.A.

A list of Network Monitor supported Wi-Fi adapters:

http://social.technet.microsoft.com/Forums/en-US/netmon/thread/737def6e-b927-4deb-997a-6a11e0aa94e2

To download Microsoft Network Monitor 3.4 visit:
http://www.microsoft.com/en-us/download/details.aspx?id=4865

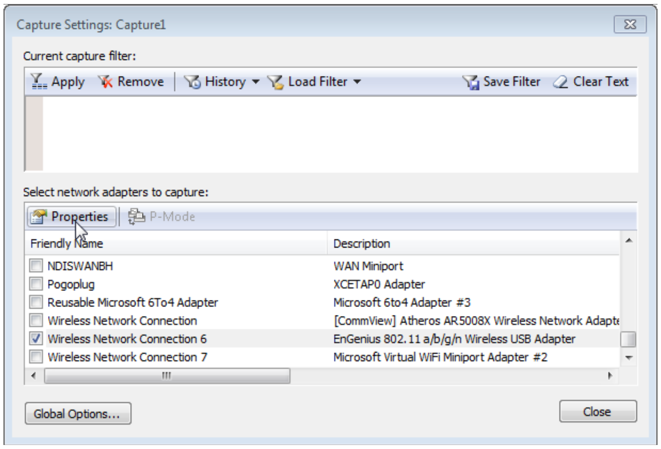
To capture 802.11 frames, deselect all of the adapters except for the wireless card in the "**Select Networks**" pane.



Friendly Name	Description
□ Local Area Connection* 48	Microsoft 6to4 Adapter #31
□ Local Area Connection* 49	Microsoft 6to4 Adapter #32
□ Local Area Connection* 50	Microsoft 6to4 Adapter #33
□ Local Area Connection* 51	Microsoft 6to4 Adapter #34
□ Local Area Connection* 52	Microsoft 6to4 Adapter #35
□ Local Area Connection* 54	Microsoft 6to4 Adapter #36
□ Local Area Connection* 55	Microsoft 6to4 Adapter #37
□ Local Area Connection* 56	Microsoft 6to4 Adapter #38
□ Local Area Connection* 57	Microsoft 6to4 Adapter #39
□ Local Area Connection* 58	Microsoft 6to4 Adapter #40
□ Local Area Connection* 59	Microsoft 6to4 Adapter #41
□ NDISWANBH	WAN Miniport
□ Pogoplug	XCETAP0 Adapter
□ Reusable ISATAP Interface {845D57B8-0B70-4E79-AEA0-BA6941A9E0AA}	Microsoft ISATAP Adapter #5
□ Reusable Microsoft 6To4 Adapter	Microsoft 6to4 Adapter #3
☑ Wireless Network Connection	[CommView] Atheros AR5008X Wi

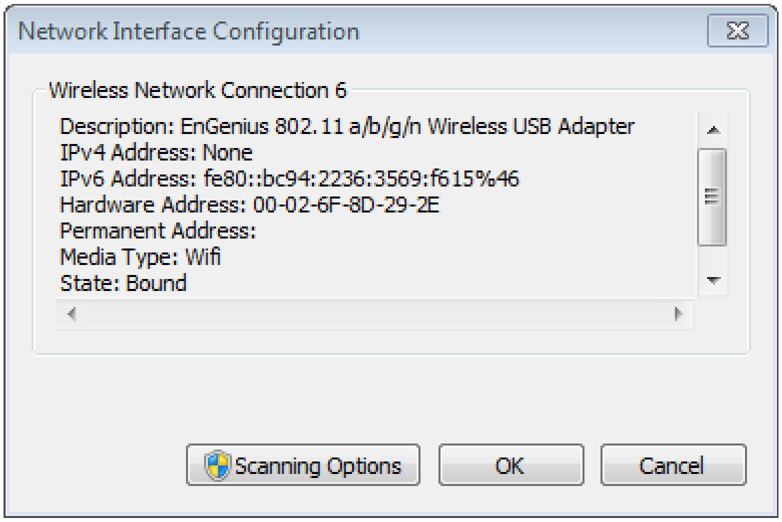
Click "**New Capture**" in the top left of the screen.

Click “**Capture Settings**” underneath the main menu. A new window will appear. Select your Wi-Fi adapter, and then click properties.



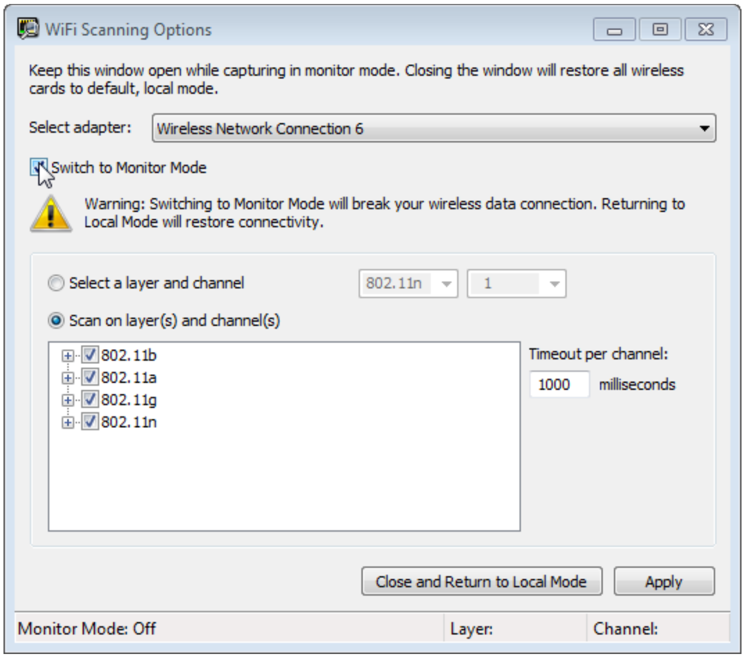
Friendly Name	Description
□ NDISWANBH	WAN Miniport
□ Pogoplug	XCETAP0 Adapter
□ Reusable Microsoft 6To4 Adapter	Microsoft 6to4 Adapter #3
□ Wireless Network Connection	[CommView] Atheros AR5008X Wireless Network Adapte
☑ Wireless Network Connection 6	EnGenius 802.11 a/b/g/n Wireless USB Adapter
□ Wireless Network Connection 7	Microsoft Virtual WiFi Miniport Adapter #2

Click “**Scanning Options**” to put the Wi-Fi card in Monitor Mode.


Network Interface Configuration
Wireless Network Connection 6
Scanning Options
OK
Cancel

Description: EnGenius 802.11 a/b/g/n Wireless USB Adapter
IPv4 Address: None
IPv6 Address: fe80::bc94:2236:3569:f615%46
Hardware Address: 00-02-6F-8D-29-2E
Permanent Address:
Media Type: Wifi
State: Bound

Put a check next to "**Switch to Monitor Mode**" and then select the Wi-Fi channels and time you would like Microsoft Monitor to spend on each channel.



WiFi Scanning Options

Keep this window open while capturing in monitor mode. Closing the window will restore all wireless cards to default, local mode.

Select adapter: Wireless Network Connection 6

☑ Switch to Monitor Mode

Warning: Switching to Monitor Mode will break your wireless data connection. Returning to Local Mode will restore connectivity.

○ Select a layer and channel 802.11n 1

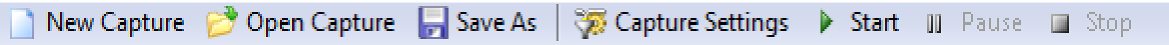
● Scan on layer(s) and channel(s)

- ☑ 802.11b
- ☑ 802.11a
- ☑ 802.11g
- ☑ 802.11n

Timeout per channel: 1000 milliseconds

Monitor Mode: Off | Layer: | Channel:

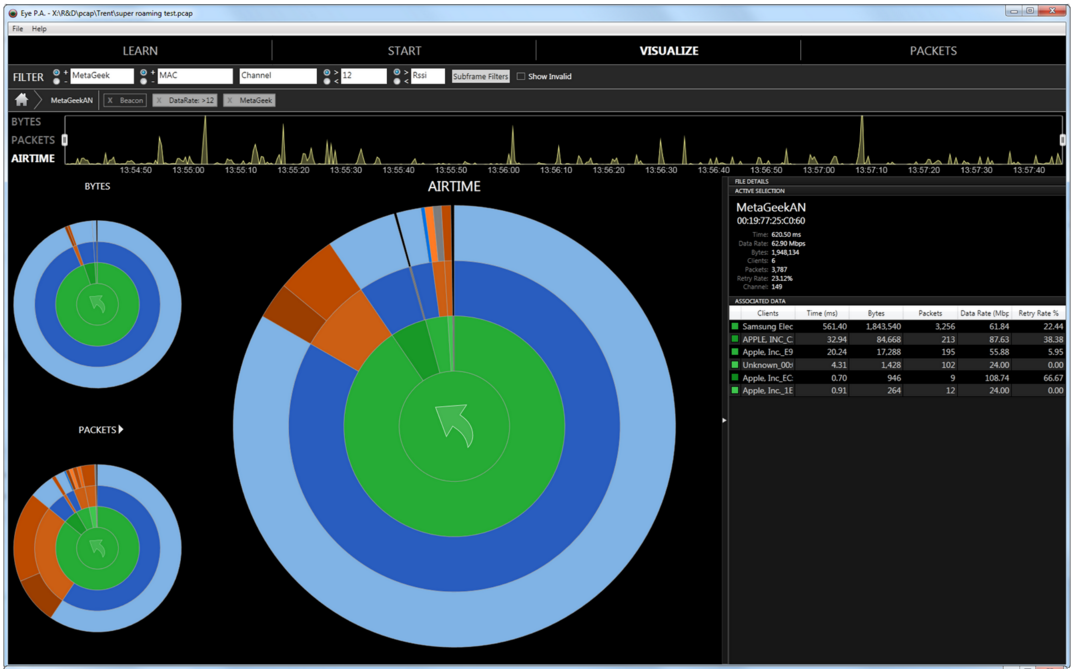
Click "**Apply.**" And leave the window open. Return to the main window and click "**Start.**"



Do not click "**Close and Return to Local Mode**" in the "**Wi-Fi Scanning Options**" unless you are done scanning.

To save the file click "**Save As**" underneath the main menu.

MAIN VIEWS



FILTER ● + MetaGeek | ● + MAC | Channel | ● > 12 | ● > Rssi

FILE DETAILS

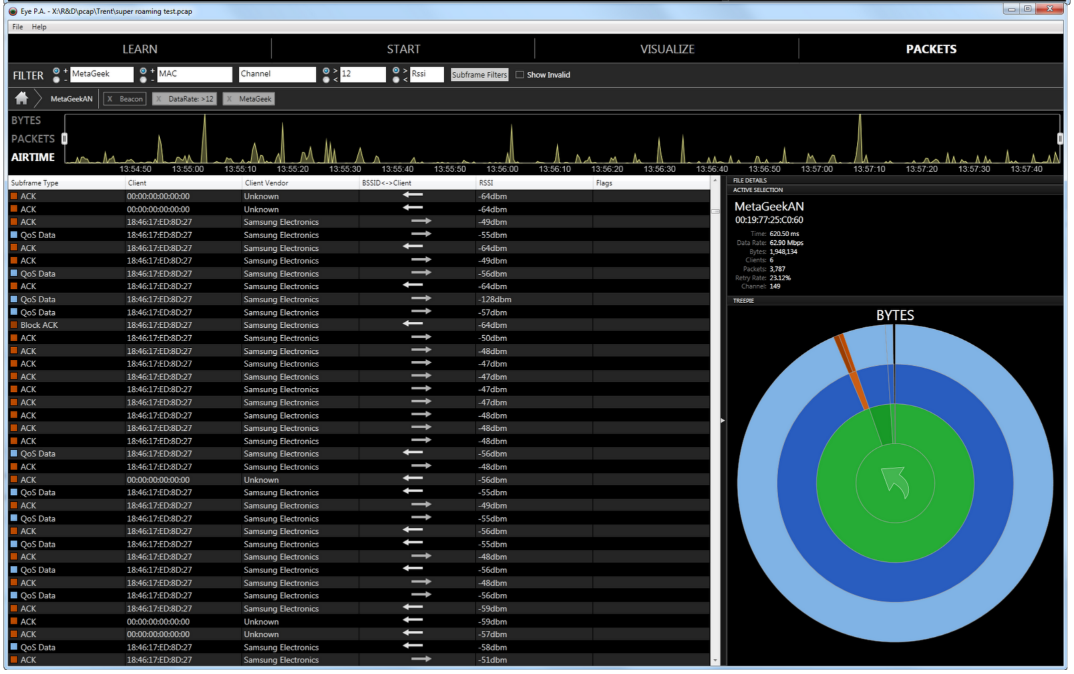
ACTIVE SELECTION

MetaGeekAN
00:19:77:25:C0:60

Time: 620.50 ms
Data Rate: 62.90 Mbps
Bytes: 1,948,134
Clients: 6
Packets: 3,787
Retry Rate: 23.12%
Channel: 149

ASSOCIATED DATA

	Clients	Time (ms)	Bytes	Packets	Data Rate (Mbp	Retry Rate %
🟩	Samsung Elec	561.40	1,843,540	3,256	61.84	22.44
🟩	APPLE, INC_C.	32.94	84,668	213	87.63	38.38
🟩	Apple, Inc._E9	20.24	17,288	195	55.88	5.95
🟩	Unknown_00:	4.31	1,428	102	24.00	0.00
🟩	Apple, Inc_EC:	0.70	946	9	108.74	66.67
🟩	Apple, Inc._1E	0.91	264	12	24.00	0.00



FILTER ● + MetaGeek | ● + MAC | Channel | ● > 12 | ● > Rssi

Subframe Type	Client	Client Vendor	BSSID<->Client	RSSI	Flags
🟧 ACK	00:00:00:00:00:00	Unknown	←	-64dbm	
🟧 ACK	00:00:00:00:00:00	Unknown	←	-64dbm	
🟧 ACK	18:46:17:ED:8D:27	Samsung Electronics	→	-49dbm	
🟦 QoS Data	18:46:17:ED:8D:27	Samsung Electronics	→	-55dbm	
🟧 ACK	18:46:17:ED:8D:27	Samsung Electronics	←	-64dbm	
🟧 ACK	18:46:17:ED:8D:27	Samsung Electronics	→	-49dbm	
🟦 QoS Data	18:46:17:ED:8D:27	Samsung Electronics	→	-56dbm	
🟧 ACK	18:46:17:ED:8D:27	Samsung Electronics	←	-64dbm	
🟦 QoS Data	18:46:17:ED:8D:27	Samsung Electronics	→	-128dbm	
🟦 QoS Data	18:46:17:ED:8D:27	Samsung Electronics	→	-57dbm	
🟧 Block ACK	18:46:17:ED:8D:27	Samsung Electronics	←	-64dbm	
🟧 ACK	18:46:17:ED:8D:27	Samsung Electronics	→	-50dbm	
🟧 ACK	18:46:17:ED:8D:27	Samsung Electronics	→	-48dbm	
🟧 ACK	18:46:17:ED:8D:27	Samsung Electronics	→	-47dbm	
🟧 ACK	18:46:17:ED:8D:27	Samsung Electronics	→	-47dbm	
🟧 ACK	18:46:17:ED:8D:27	Samsung Electronics	→	-47dbm	
🟧 ACK	18:46:17:ED:8D:27	Samsung Electronics	→	-47dbm	
🟧 ACK	18:46:17:ED:8D:27	Samsung Electronics	→	-48dbm	
🟧 ACK	18:46:17:ED:8D:27	Samsung Electronics	→	-48dbm	
🟧 ACK	18:46:17:ED:8D:27	Samsung Electronics	→	-48dbm	
🟦 QoS Data	18:46:17:ED:8D:27	Samsung Electronics	←	-56dbm	
🟧 ACK	18:46:17:ED:8D:27	Samsung Electronics	→	-48dbm	
🟧 ACK	00:00:00:00:00:00	Unknown	←	-56dbm	
🟦 QoS Data	18:46:17:ED:8D:27	Samsung Electronics	←	-55dbm	
🟧 ACK	18:46:17:ED:8D:27	Samsung Electronics	→	-49dbm	
🟦 QoS Data	18:46:17:ED:8D:27	Samsung Electronics	→	-55dbm	
🟧 ACK	18:46:17:ED:8D:27	Samsung Electronics	←	-56dbm	
🟦 QoS Data	18:46:17:ED:8D:27	Samsung Electronics	←	-55dbm	
🟧 ACK	18:46:17:ED:8D:27	Samsung Electronics	→	-48dbm	
🟦 QoS Data	18:46:17:ED:8D:27	Samsung Electronics	←	-56dbm	
🟧 ACK	18:46:17:ED:8D:27	Samsung Electronics	→	-48dbm	
🟦 QoS Data	18:46:17:ED:8D:27	Samsung Electronics	→	-56dbm	
🟧 ACK	18:46:17:ED:8D:27	Samsung Electronics	←	-59dbm	
🟧 ACK	00:00:00:00:00:00	Unknown	←	-59dbm	
🟧 ACK	00:00:00:00:00:00	Unknown	←	-57dbm	
🟦 QoS Data	18:46:17:ED:8D:27	Samsung Electronics	←	-58dbm	
🟧 ACK	18:46:17:ED:8D:27	Samsung Electronics	→	-51dbm	

FILE DETAILS

ACTIVE SELECTION

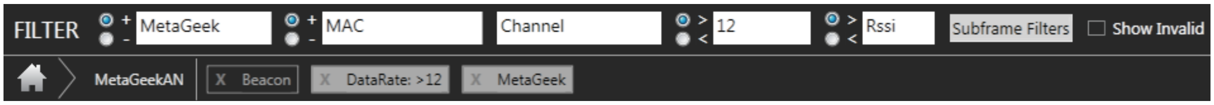
MetaGeekAN
00:19:77:25:C0:60

Time: 620.50 ms
Data Rate: 62.90 Mbps
Bytes: 1,948,134
Clients: 6
Packets: 3,787
Retry Rate: 23.12%
Channel: 149

Work Flow

Across the top of Eye P.A. are 4 different categories called the Work Flow. Eye P.A. helps users learn how to use its core features in the "LEARN" section. The "START" section is where users can open packet captures, or create their own capture using an AirPcap Nx. "VISUALIZE" takes the entire capture and generates Time Graphs, multi-layered pie charts and data tables. After visually filtering the data necessary to perform the analysis the "PACKETS" section will display the individual packets for a more in-depth analysis.

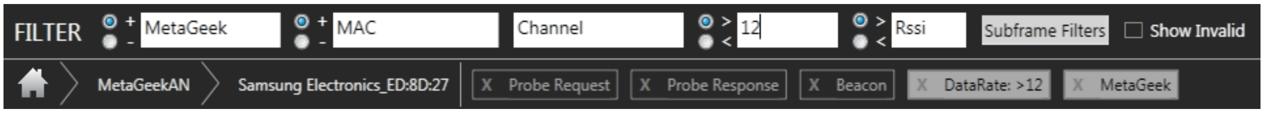
Filter Bar



Eye P.A. provides both manual and GUI entry for packet filtering. The top of the filter bar is where the user can type in the name, MAC, Channel, Data Rate or RSSI. Users can apply exclusive filters to quickly remove data from a particular access point or client by selecting the "-" before the text entry field. Selecting a "+" will build an inclusive filter. The Data Rate and RSSI can also filter based on a greater than or less than selection. With this filter users can remove all frames with a RSSI less than or equal to -90dBM.

It can also be helpful to filter out certain types of packets like beacons, acknowledgements, or other non-essential frame types to bring out the packets that matter the most. To remove specific frame types from the multi-layered pie charts, click "Subframe Filters" in the Filter Bar at the top of the application. Checking and unchecking frame types allows the user to selectively choose the which packets Eye P.A. will graph.

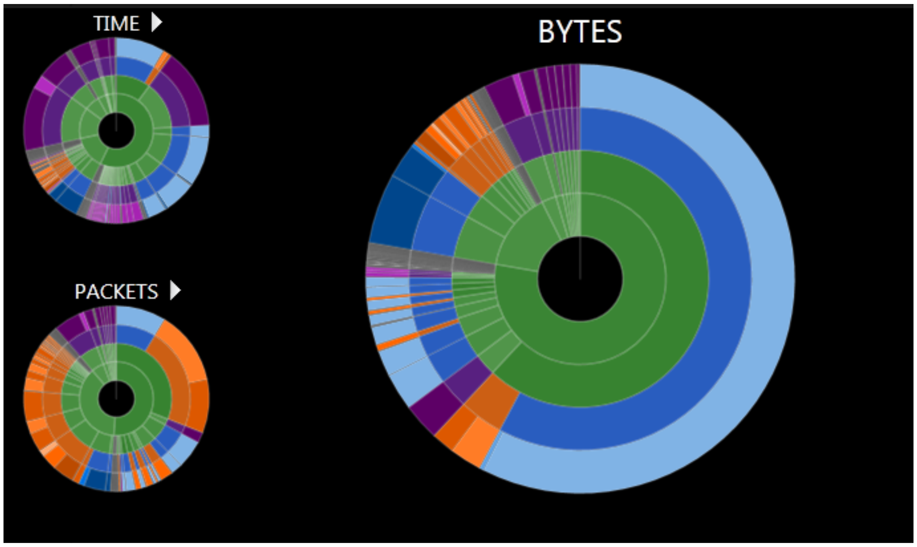
Filter Breadcrumbs



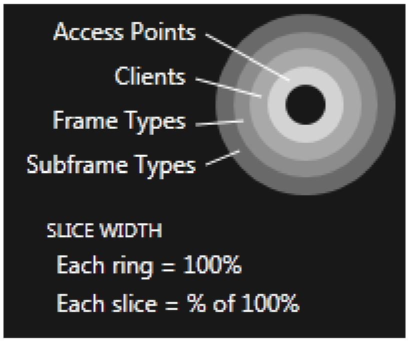
The filter bread crumbs represent the current requirements the user has manually entered as filters or navigated to by means of the multi-layered pie chart. To remove a crumb click the x. Bread crumbs will either be black to represent exclusive filters or gray to show inclusive filters.

Note: Filtering packets will affect the data exported to WireShark. If "Beacons" are unchecked from the display filters, they will be excluded from the data you can export to WireShark.

Multi-Layered Pie Charts



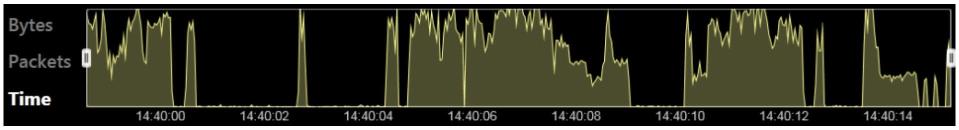
Eye P.A. uses multi-layered pie charts to display overall utilization of total packets, total bytes and total amount of air time. The size of the slices in the rings are proportionate to the total, while the colors represent the type of data being displayed.



The data is a hierarchical breakdown by SSID > Client > Frame Type > Subframe Type. Each slice is divided into smaller slices in the next layer.

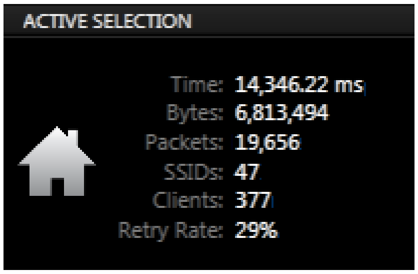
For example, by clicking on a client, Eye P.A. will draw a new multi-layered pie chart with all of the data for that particular client.

Adjustable Time Graph



Eye P.A. displays a historical summary of the data capture in the top time slider. By default, the Adjustable Time Graph in Eye P.A. selects the capture in its entirety. The user can select a different window of time by dragging the start and stop handles on either side of the time slider. When the user selects a smaller time range both the data visuals and tables will update, only displaying data from the selected range to help you narrow in on unusual network activity.

Active Selection

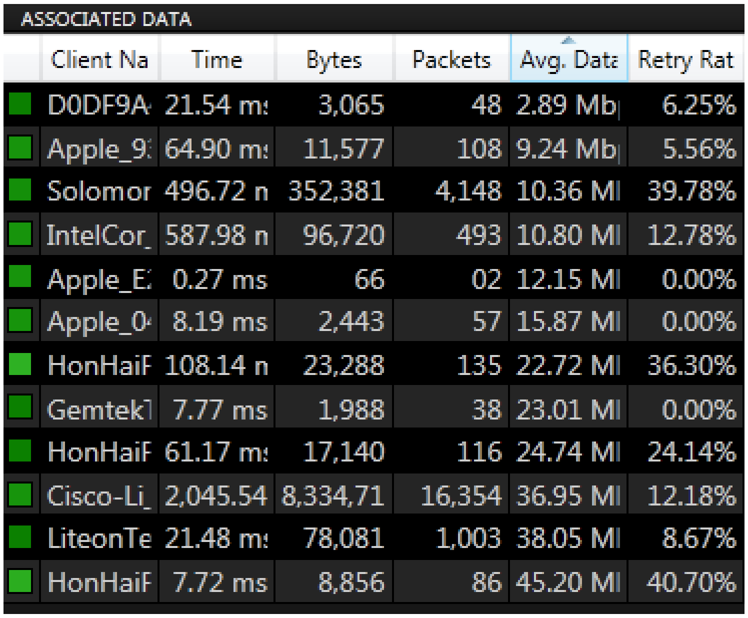


ACTIVE SELECTION

Time: 14,346.22 ms
Bytes: 6,813,494
Packets: 19,656
SSIDs: 47
Clients: 377
Retry Rate: 29%

The Active Selection legend located in the top right displays the related data to the center of the multi-layer pie chart. This data will change as the user drills down through layers. It displays total time, bytes, number of packets, BSSIDs, clients, and retry rate.

Associated Data Table



ASSOCIATED DATA

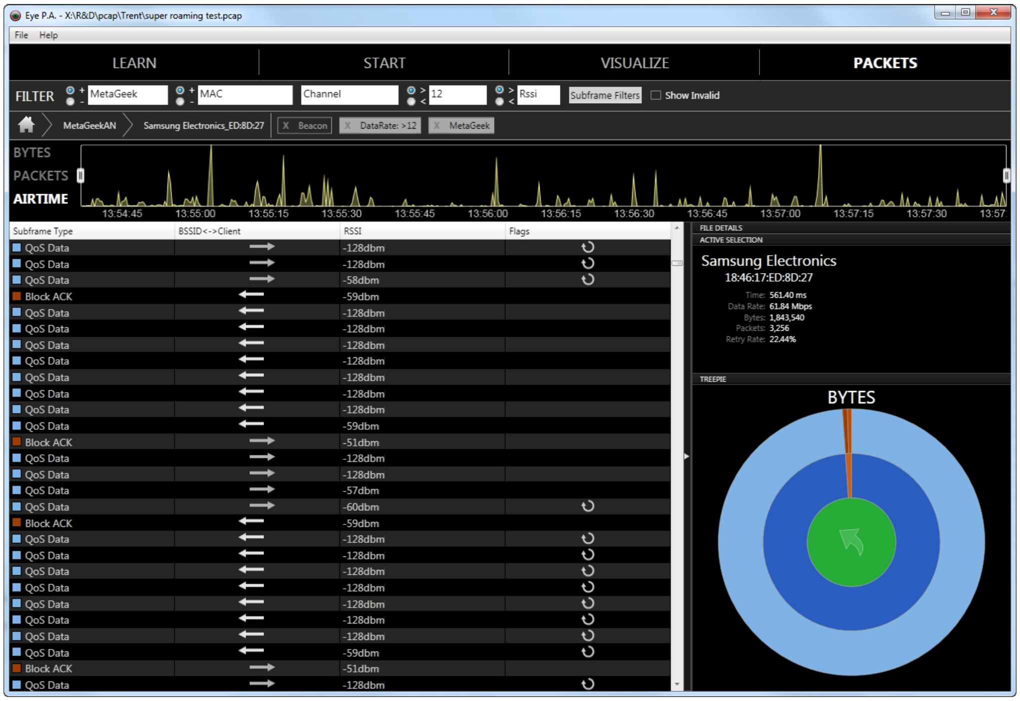
	Client Na	Time	Bytes	Packets	Avg. Data	Retry Rat
🟩	D0DF9A	21.54 m:	3,065	48	2.89 Mb	6.25%
🟩	Apple_9:	64.90 m:	11,577	108	9.24 Mb	5.56%
🟩	Solomor	496.72 n	352,381	4,148	10.36 MI	39.78%
🟩	IntelCor_	587.98 n	96,720	493	10.80 MI	12.78%
🟩	Apple_E:	0.27 ms	66	02	12.15 MI	0.00%
🟩	Apple_0	8.19 ms	2,443	57	15.87 MI	0.00%
🟩	HonHaiF	108.14 n	23,288	135	22.72 MI	36.30%
🟩	Gemtek1	7.77 ms	1,988	38	23.01 MI	0.00%
🟩	HonHaiF	61.17 m:	17,140	116	24.74 MI	24.14%
🟩	Cisco-Li_	2,045.54	8,334,71	16,354	36.95 MI	12.18%
🟩	LiteonTe	21.48 m:	78,081	1,003	38.05 MI	8.67%
🟩	HonHaiF	7.72 ms	8,856	86	45.20 MI	40.70%

The table displays quantifiable metrics for the layer on the next ring out from the center (ring 1). This table can be either BSSIDs, Clients, Frame Types, or Sub-Frame Types. Upon opening a .pcap file, the table will show each BSSID, the total amount of airtime utilized, bytes, number of clients associated, average data frame rate and retry rate.

The multi-layered pie chart can be rearranged by clicking the table's column headers to sort the data by Total Bytes, Packets or Retry Rate. Similar to a clock, the sorting will start at the 12 position and display clockwise in the pie chart with its order indicated in the table data.

Packet Viewer

Eye P.A. will display the basic details of individual packets in the “Packet Viewer” like Subframe Type, RSSI, Retry, and Destination. The user can define the columns in the packet viewer by right-clicking on a column header and selecting the details they wish to view. Apply filters from the Filter Bar or use the Treepie in the left pane to drill-down in the packet viewer.



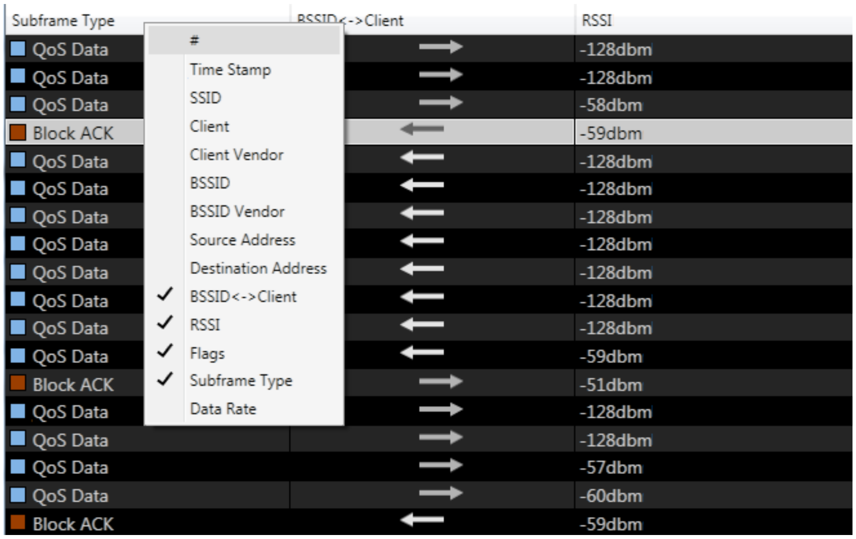
Subframe Type	BSSID<->Client	RSSI	Flags
🟦 QoS Data	→	-128dbm	↻
🟦 QoS Data	→	-128dbm	↻
🟦 QoS Data	→	-58dbm	↻
🟧 Block ACK	←	-59dbm	
🟦 QoS Data	←	-128dbm	
🟦 QoS Data	←	-128dbm	
🟦 QoS Data	←	-128dbm	
🟦 QoS Data	←	-128dbm	
🟦 QoS Data	←	-128dbm	
🟦 QoS Data	←	-128dbm	
🟦 QoS Data	←	-128dbm	
🟦 QoS Data	←	-59dbm	
🟧 Block ACK	→	-51dbm	
🟦 QoS Data	→	-128dbm	
🟦 QoS Data	→	-128dbm	
🟦 QoS Data	→	-57dbm	
🟦 QoS Data	→	-60dbm	↻
🟧 Block ACK	←	-59dbm	
🟦 QoS Data	←	-128dbm	↻
🟦 QoS Data	←	-128dbm	↻
🟦 QoS Data	←	-128dbm	↻
🟦 QoS Data	←	-128dbm	↻
🟦 QoS Data	←	-128dbm	↻
🟦 QoS Data	←	-128dbm	↻
🟦 QoS Data	←	-128dbm	↻
🟦 QoS Data	←	-59dbm	↻
🟧 Block ACK	→	-51dbm	
🟦 QoS Data	→	-128dbm	↻

Samsung Electronics
18:46:17:ED:8D:27

Time: 561.40 ms
Data Rate: 61.84 Mbps
Bytes: 1,843,540
Packets: 3,256
Retry Rate: 22.44%

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 as a column.

To bring any missing columns back into view right-click at the top of the packet viewer table and select the columns you would like visible.



Subframe Type	BSSID<->Client	RSSI
🟦 QoS Data	→	-128dbm
🟦 QoS Data	→	-128dbm
🟦 QoS Data	→	-58dbm
🟫 Block ACK	←	-59dbm
🟦 QoS Data	←	-128dbm
🟦 QoS Data	←	-128dbm
🟦 QoS Data	←	-128dbm
🟦 QoS Data	←	-128dbm
🟦 QoS Data	←	-128dbm
🟦 QoS Data	←	-128dbm
🟦 QoS Data	←	-128dbm
🟦 QoS Data	←	-59dbm
🟫 Block ACK	→	-51dbm
🟦 QoS Data	→	-128dbm
🟦 QoS Data	→	-128dbm
🟦 QoS Data	→	-57dbm
🟦 QoS Data	→	-60dbm
🟫 Block ACK	←	-59dbm

MULTI-LAYERED PIE CHARTS

To alternate visually between the different types of data, click the arrow above any pie chart to select TIME, PACKETS, or BYTES and move it to the featured position. This will change the main pie chart and the Time Graph to that type of data.

Packets

This view represents the proportionate amounts of packets in comparison to the total captured.

Bytes

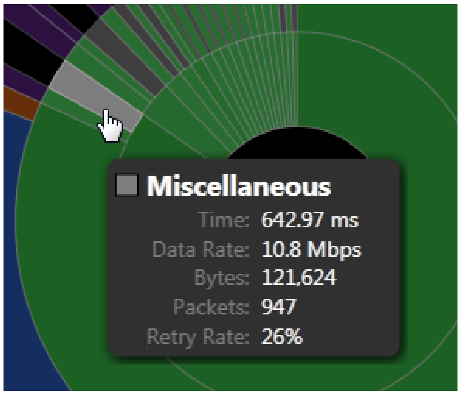
This view represents 100% of the total data captured in Bytes. Each slice is the total data sent by BSSID or client.

Time

This view represents the proportionate amount of airtime each station utilized. It is important to note that lower data rates use more airtime than higher data rates to transfer the same number of bytes.

Wireless is similar to wired communication in the sense that no two devices can "talk" at the same time. Therefore the amount of time each station takes prohibits the other stations from transmitting.

To simplify and increase the performance speed of Eye P.A., the software will aggregate any small packets into a gray slice labeled "Miscellaneous." To see the contents of a gray slice, use the associated data table and double click on it. If the gray slice is on the outside of a green ring, expand its parent by clicking on it. Eye P.A. will redraw all of the outer sections to display the data that was aggregated in a gray "Miscellaneous" slice.

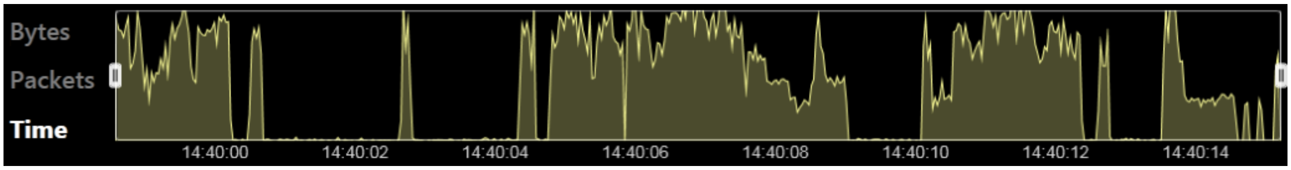


■ Miscellaneous

Time: 642.97 ms
Data Rate: 10.8 Mbps
Bytes: 121,624
Packets: 947
Retry Rate: 26%

Time Graph

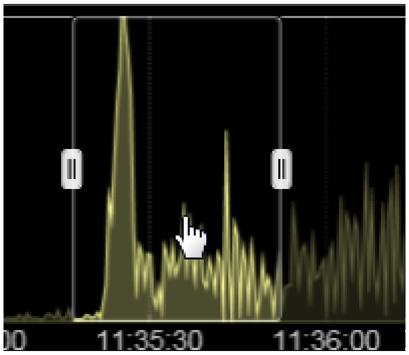
Time Segment Analysis



Wireless environments can look different within minutes. Issues may be erratic and intermittent. By adjusting the time span in the slider, users can omit time when the WLAN was functioning properly and focus on a smaller time window when an issue occurred.

Adjusting the Time Span

The time span is the line graph at the bottom of the display. When opening a .pcap file in Eye P.A., the software will automatically adjust the time span to the beginning and end of the capture. The time window has two handles that can be adjusted in and out to help you choose select times of the capture.



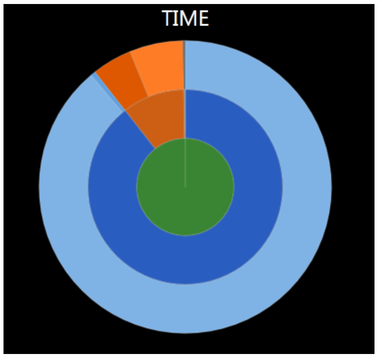
To move the time span, click in the middle of the handle and drag it to another location in time.

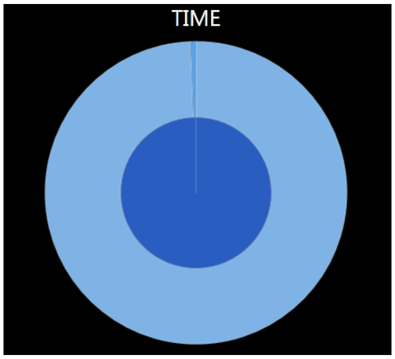
Packets, Bytes, and Time

The left hand side of the Time Graph will toggle between total bytes transferred, total packets, and total airtime utilized. The line graph represents the current largest multi-layered pie chart and will automatically change when the user toggles between the pie charts.

DATA VISUALS

Multi-Layered Pie Charts



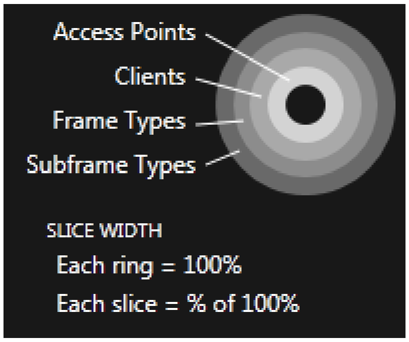


There are three multi-layered pie charts in the main window. Eye P.A.’s multi-layered pie charts continually divide each slice into more slices based on percentages. The size of each slice is proportionate to the total packets, bytes or time utilized.

Ring Order

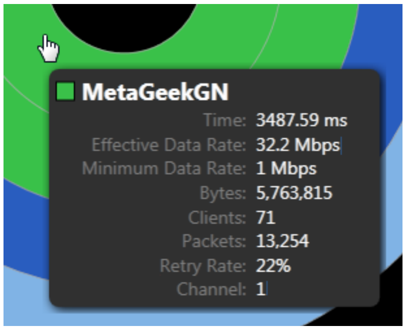
The default ring order in Eye P.A.

1. BSSID
2. Associated Clients
3. Frame Type
4. Subframe Type



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.



🟩 **MetaGeekGN**

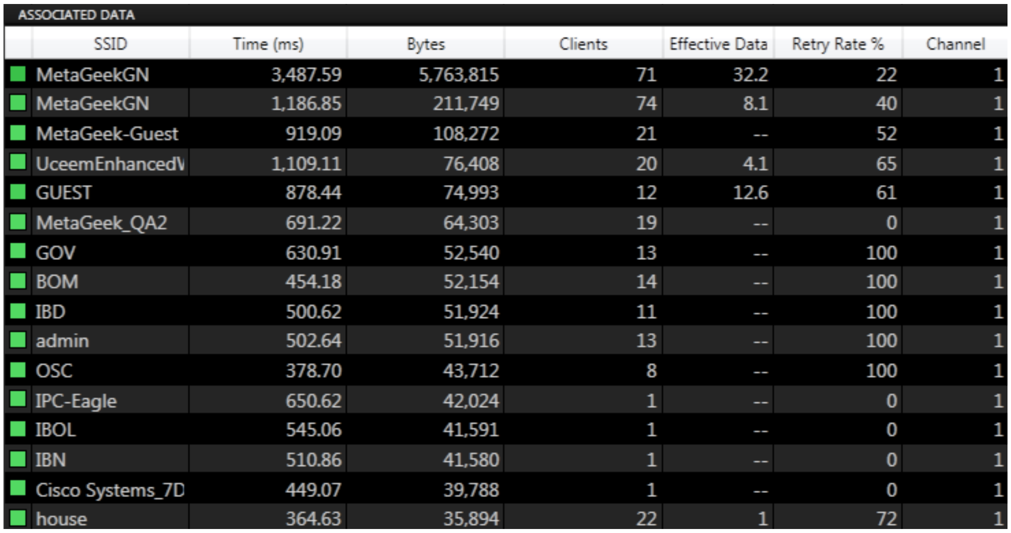
Time:	3487.59 ms
Effective Data Rate:	32.2 Mbps
Minimum Data Rate:	1 Mbps
Bytes:	5,763,815
Clients:	71
Packets:	13,254
Retry Rate:	22%
Channel:	1

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.

Hover (Inspector Tool)

When a user hovers over a slice in the pie chart, a tool tip box will appear, providing additional details like data rate, packet count and retry rate. This information is also displayed in the Associated Data Table.

ASSOCIATED DATA TABLE



ASSOCIATED DATA

	SSID	Time (ms)	Bytes	Clients	Effective Data	Retry Rate %	Channel
🟩	MetaGeekGN	3,487.59	5,763,815	71	32.2	22	1
🟩	MetaGeekGN	1,186.85	211,749	74	8.1	40	1
🟩	MetaGeek-Guest	919.09	108,272	21	--	52	1
🟩	UceemEnhancedV	1,109.11	76,408	20	4.1	65	1
🟩	GUEST	878.44	74,993	12	12.6	61	1
🟩	MetaGeek_QA2	691.22	64,303	19	--	0	1
🟩	GOV	630.91	52,540	13	--	100	1
🟩	BOM	454.18	52,154	14	--	100	1
🟩	IBD	500.62	51,924	11	--	100	1
🟩	admin	502.64	51,916	13	--	100	1
🟩	OSC	378.70	43,712	8	--	100	1
🟩	IPC-Eagle	650.62	42,024	1	--	0	1
🟩	IBOL	545.06	41,591	1	--	0	1
🟩	IBN	510.86	41,580	1	--	0	1
🟩	Cisco Systems_7D	449.07	39,788	1	--	0	1
🟩	house	364.63	35,894	22	1	72	1

The Associated Data Table provides details for the innermost ring (Ring 1) of the Multi Layer Pie Chart.

Table Columns

SSID - This is the network name of the Access Point

MAC - A unique identifier for each network interface

Time - The amount of time used to transmit

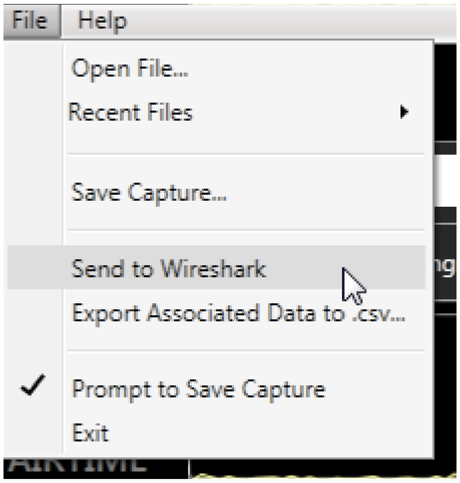
Bytes - The amount of data transferred

Packets - The total # of packets per BSSID

Retransmit - The percentage of packets that had to be resent

Effective Data Rate - The average data rate achieved by the client including interframe spacing and network allocation vector times.

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 SSID 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 Airpcap adapter
- Mac OS X with Wi-Fi Diagnostics or WireShark in Monitor Mode
- Linux with WireShark or Kismet
- Export a .cap or .pcap from a wireless access point

Why are the 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 router not to broadcast its name. Typically only users who know the name of the wireless network can connect to a hidden SSID.

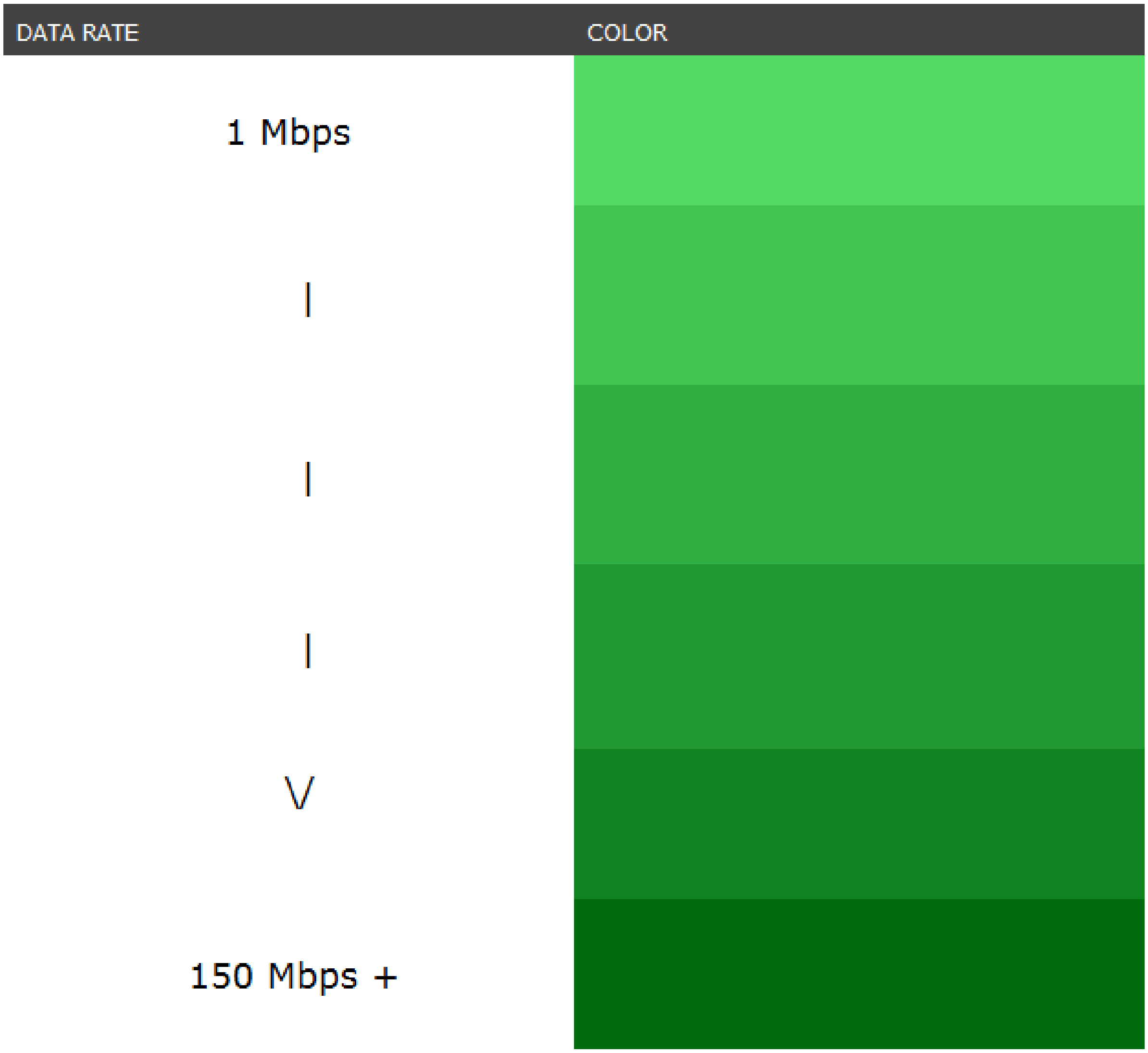
What is the “Miscellaneous” gray slice?

The gray slices contain valid packet data from a high amount 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. They are colored gray because they 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 redrawn.

UNDERSTANDING COLOR

Data Rate

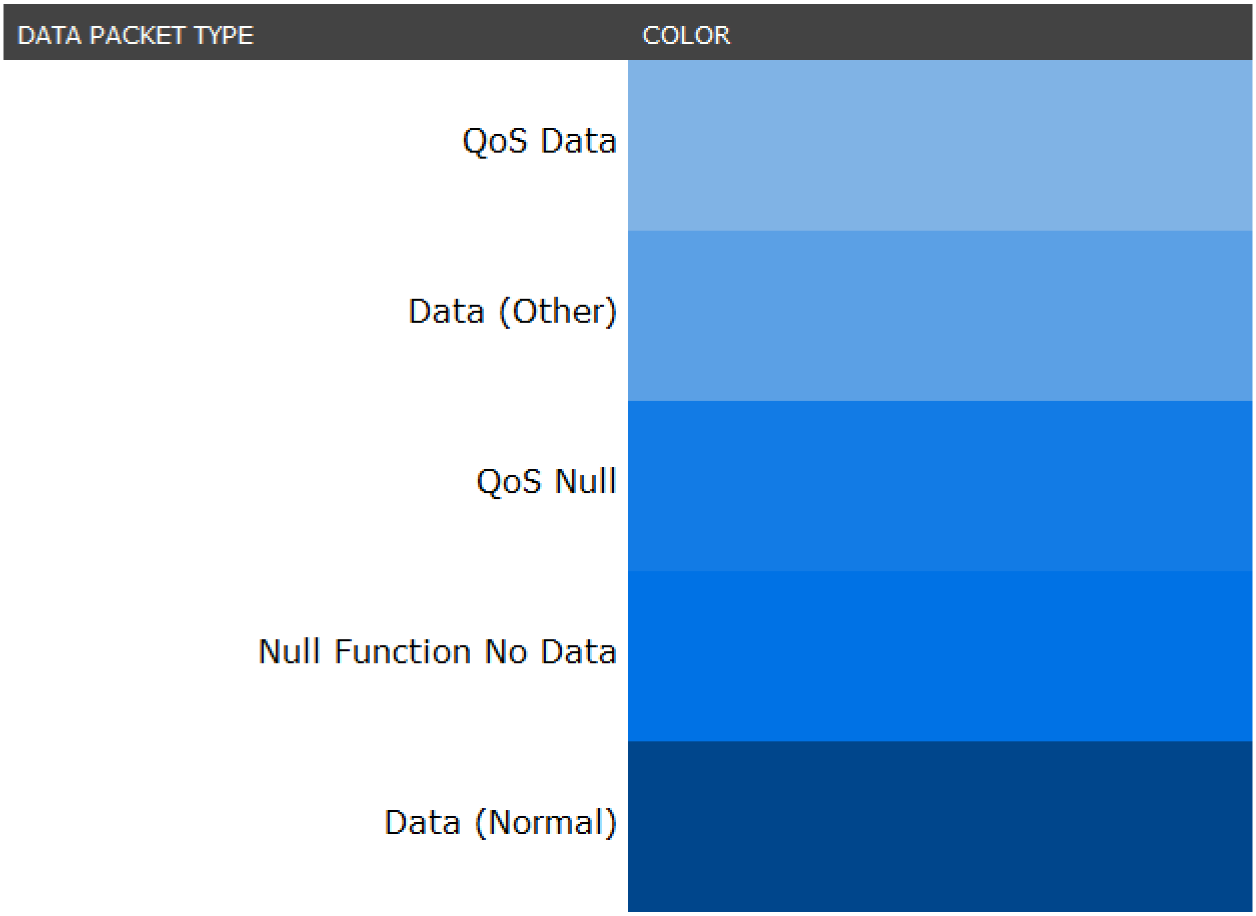
The first two layers in the multi-layered pie chart are colored by the average data rate of the traffic. The shade of green is based on a sliding scale. The minimum average data rate captured is represented by light green, while the highest is represented by dark green, with shades in between.



DATA RATE	COLOR
1 Mbps	🟩
|	🟩
|	🟩
|	🟩
V	🟩
150 Mbps +	🟩

Data Frames

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

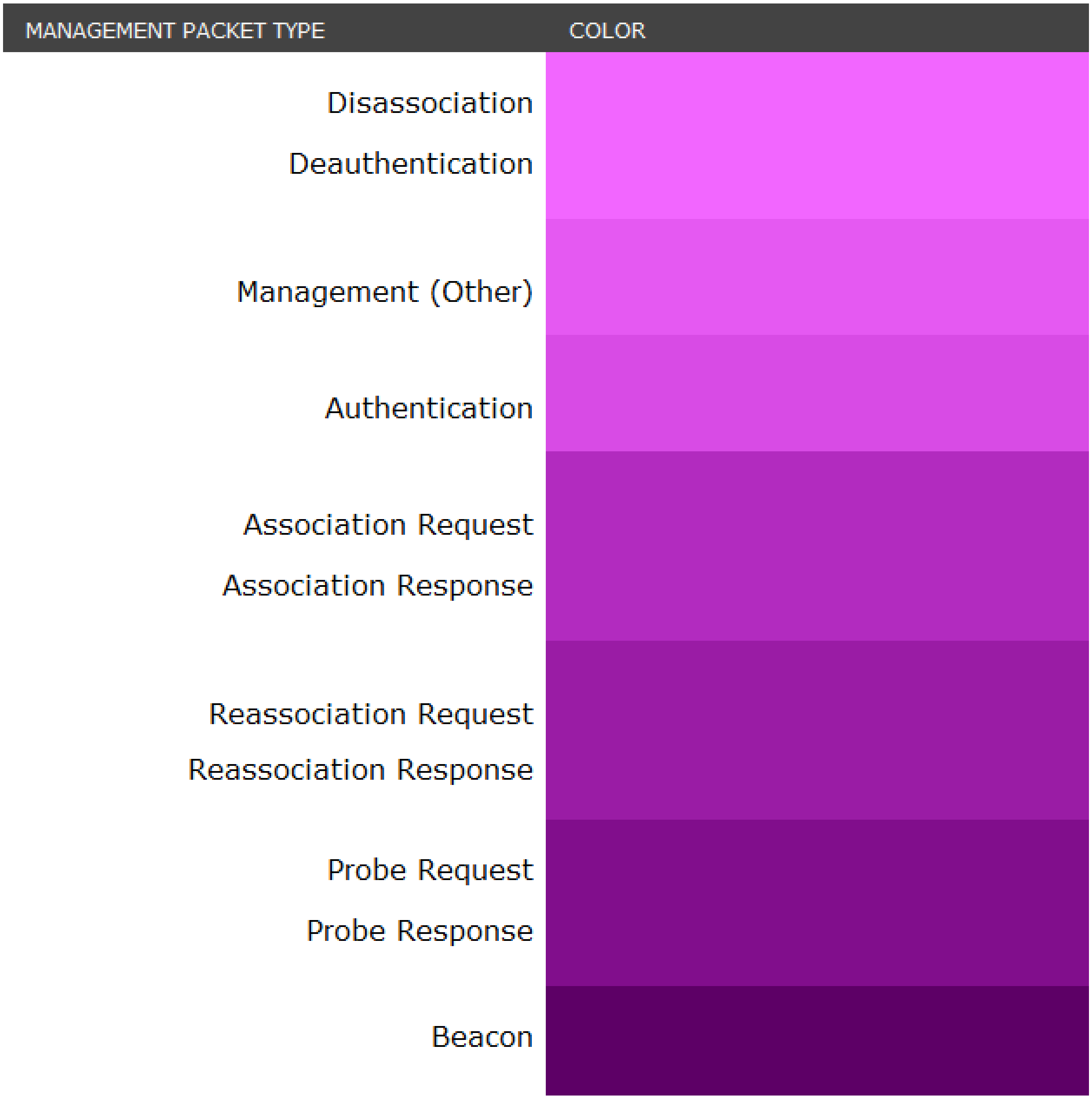


DATA PACKET TYPE	COLOR
QoS Data	🟦
Data (Other)	🟦
QoS Null	🟦
Null Function No Data	🟦
Data (Normal)	🟦

Management Frames

A majority of the frame types in an 802.11 network.

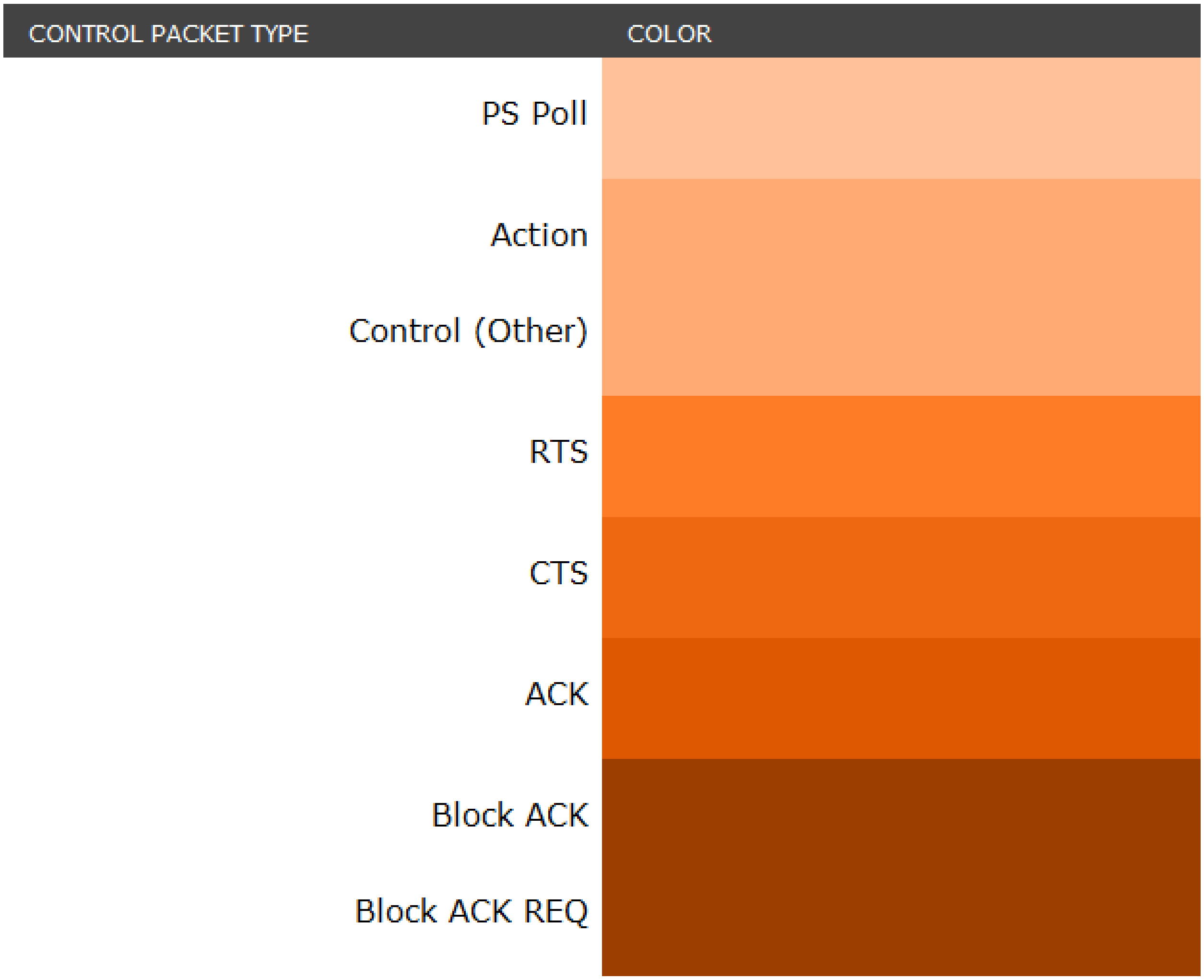
Used by wireless stations to join and leave the network.



MANAGEMENT PACKET TYPE	COLOR
Disassociation Deauthentication	🟪
Management (Other)	🟪
Authentication	🟪
Association Request Association Response	🟪
Reassociation Request Reassociation Response	🟪
Probe Request Probe Response	🟪
Beacon	🟪

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	

LEARN MORE

You can learn more about Eye P.A. at our website

http://www.metageek.net/products/eye-pa