

TOM BRIDGE AND CHRIS DAWE

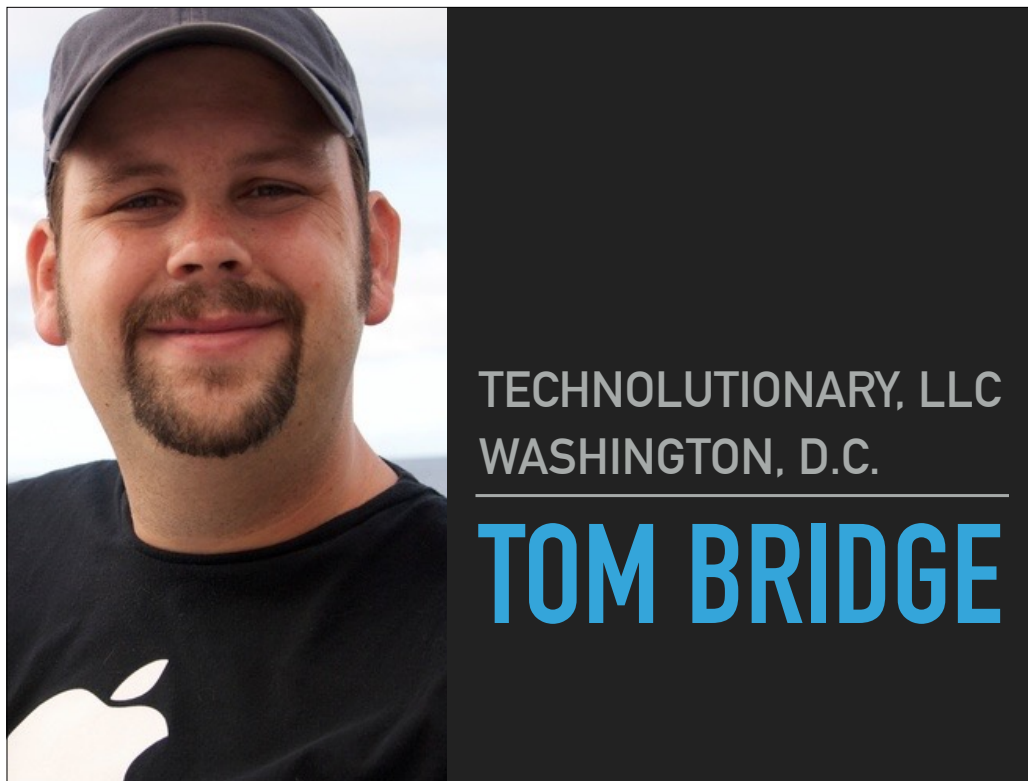
A WIFI TOOLKIT



WHEELWRIGHTS, LLC
SEATTLE, WA

CHRIS DAWE

Chris Dawe is Principal Systems Engineer at Wheelwrights, LLC, in Seattle, Washington. Chris focuses on MacOS, iOS, and networking, and handles everything from customer assessment to system design, deployment, and support. When not working, Chris reads, cooks, and appreciates both whiskey and whisky.



Tom Bridge is a founding partner at Technolutionary LLC, based in Washington DC. Technolutionary supports 400 users from small business to medium enterprise in a mix of Mac and PC, with a dash of Linux and a healthy serving of iOS devices. He lives in Brookland, DC, with his wife, Tiffany, their son Charlie, and their cats, Macro and Bokeh.

TODAY'S AGENDA

- ▶ Review of the tools we use every day
- ▶ Discuss capabilities and limitations

This talk reflects our development as consultants handling WiFi installations, and focuses on the tools available for Mac OS, with discussion of important tools for WiFi that are *not* available for Mac OS.

GOALS FOR TODAY

- ▶ An idea of which tools to deploy, when, and why.
- ▶ A reference library for things we lack time to discuss.

The presenter notes include links to important resources.

ORGANIZING OUR TOOLS

- ▶ Exploration
- ▶ Troubleshooting (and analysis)
- ▶ Planning

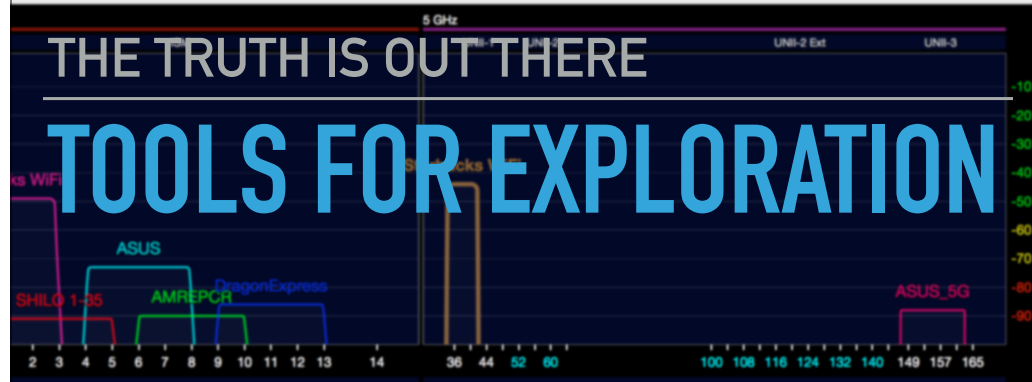
The distinctions among these tools are a bit arbitrary, and we'll see that tools overlap from one area to another.

associated: Starbucks WiFi, Ch 40, 40 MHz, 216 Mbps

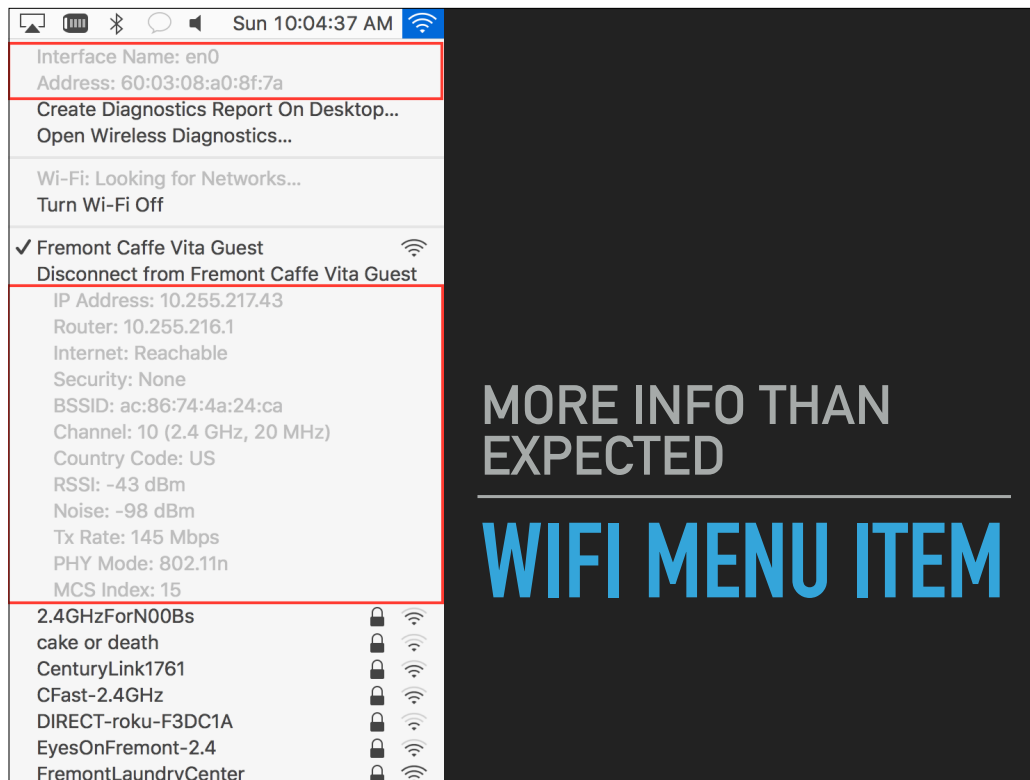
All Networks Q Filter

BSSID	Vendor	Band	Channel	SNR	Signal	Noise	Channel Utilization	Max Rate
00:A0:D5:12:3B:09	SIERRA WIRELESS INC.	2.4 GHz	8	6 dB	-90	-96		54 Mbps
F0:79:59:E3:F1:D0	ASUSTeK Computer Inc.	2.4 GHz	6	23 dB	-73	-96	41%	144 Mbps
F0:79:59:E3:F1:D4	ASUSTeK Computer Inc.	5 GHz	149	8 dB	-88	-96	3%	867 Mbps
10:5F:06:9A:1D:A5	Actiontec Electronics, Inc	2.4 GHz	11	10 dB	-86	-96	11%	144 Mbps
4C:9E:FF:90:F4:82	ZyXEL Communications Corp.	2.4 GHz	11	4 dB	-92	-96		144 Mbps
4C:9E:FF:90:F2:C0	ZyXEL Communications Corp.	2.4 GHz	3	5 dB	-91	-96		144 Mbps
9C:1C:12:24:18:50	Aruba Networks Inc.	2.4 GHz	1	47 dB	-49	-96	24%	130 Mbps
9C:1C:12:24:18:58	Aruba Networks Inc.	5 GHz	40,-1	51 dB	-44	-95	0%	300 Mbps

Network Details Signal Strength Channels Advanced Details







Apple makes information about the WiFi connection available in the OS. Option-clicking that same WiFi menu item gives a significant amount of connection information for your computer, including:

1. The computer's network interface.
2. IP address, router, and Internet connectivity information.
3. Associated BSSID (connected access point) and channel.
4. Signal and noise levels.
5. Connection performance information.

AIRPORT CLI UTILITY AND WIFI MENU ITEM



```
✓ Fremont Caffè Vita Guest
Disconnect from Fremont Caffè Vita Guest
IP Address: 10.255.217.43
Router: 10.255.216.1
Internet: Reachable
Security: None
BSSID: ac:86:74:4a:24:ca
Channel: 10 (2.4 GHz, 20 MHz)
Country Code: US
RSSI: -43 dBm
Noise: -98 dBm
Tx Rate: 145 Mbps
PHY Mode: 802.11n
MCS Index: 15

Last login: Sat Jan 30 22:21:28 on ttys000
smfs:~ dawe$ airport -I
agrCtlRSSI: -45
agrExtRSSI: 0
agrCtlNoise: -93
agrExtNoise: 0
state: running
op mode: station
lastTxRate: 145
maxRate: 144
lastAssocStatus: 0
802.11 auth: open
link auth: none
BSSID: ac:86:74:4a:24:ca
SSID: Fremont Caffè Vita Guest
MCS: 15
channel: 10
smfs:~ dawe$
```

Apple has a quasi-hidden utility for querying the WiFi located at:
`/System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources/airport`

You may want to create a symlink to the airport tool:

```
sudo ln -s /System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources/airport /usr/local/bin/airport
```

AIRPORT CLI

```

smfs:~ dawe$ airport -s
      SSID BSSID      RSSI CHANNEL HT CC SECURITY (auth/unicast/group)
Ladybug Nugget dc:9b:9c:f3:e0:6e -85 11 Y US WPA2 (PSK/AES/AES)
CFast-2.4GHz 4c:60:de:41:13:a3 -85 1 Y -- WPA2 (PSK/AES/AES)
FremontLaundryCenter c0:ea:e4:bc:61:b5 -74 2 Y US WPA (PSK/AES/AES)
xfinitywifi 0c:54:a5:72:74:fa -68 161,-1 Y US NONE
HOME-D5D1-5 0c:54:a5:72:74:f8 -68 161,-1 Y US WPA (PSK/AES, TKIP/TKIP) WPA2 (PSK/AES, TKIP/TKIP)
VitaFremont5 c4:04:15:14:48:80 -71 153,-1 Y -- WPA2 (PSK/AES/AES)
Via Tribunali 88:1f:a1:2e:ab:9e -70 6 Y US WPA2 (PSK/AES/AES)
xfinitywifi 0c:54:a5:71:a1:f2 -56 6 Y US NONE
HOME-D5D1-2.4 0c:54:a5:71:a1:f0 -90 6 Y US WPA (PSK/AES, TKIP/TKIP) WPA2 (PSK/AES, TKIP/TKIP)
HOME-64E0-2.4 74:85:2a:f2:05:48 -79 1 Y US WPA (PSK/AES, TKIP/TKIP) WPA2 (PSK/AES, TKIP/TKIP)
pecado 08:86:3b:41:a8:ea -93 11 Y TW WPA (PSK/AES/AES) WPA2 (PSK/AES/AES)
HOME-2FE8 44:32:c8:cf:2f:e8 -82 11 Y -- WPA (PSK/AES, TKIP/TKIP) WPA2 (PSK/AES, TKIP/TKIP)
Fremont Caffè Vita Guest ac:86:74:4a:24:ca -42 10 Y US NONE
Fremont Caffè Vita Guest ac:86:74:4a:24:7a -53 10 Y US NONE
smfs:~ dawe$

```

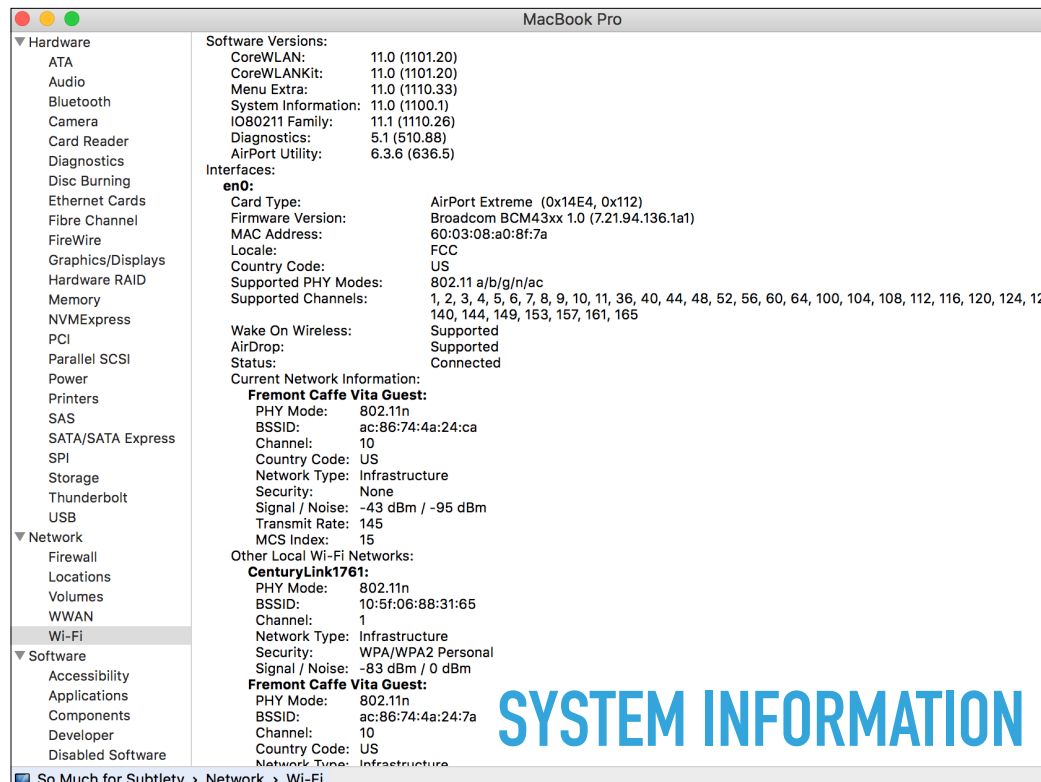
In addition to displaying information about the connected network a la WiFi Menu, the airport CLI tool will do some other interesting things:

1. Scan for available networks.
2. Adjust some preferences for the WiFi interface.
3. Adjust logging events for WiFi.

None of this is particularly well-documented, but the web site OS X Daily dug into the tool and posted the following writeup. The logging tools will especially require experimentation:

<http://osxdaily.com/2007/01/18/airport-the-little-known-command-line-wireless-utility/>

Note that the OS X Daily article has you create the symlink in a SIP-protected directory. Create it in /usr/local instead.



This information and more also shows up in System Information, System Profiler, or whatever Apple is calling it this week. Locate it in /Applications/Utilities, or run the command `system_profiler`.

System information will add to your system's picture of its WiFi configuration by including CoreWLAN and other software versions, interface information for your WiFi interface, chipset information, and a list of networks near enough to your computer to be heard.

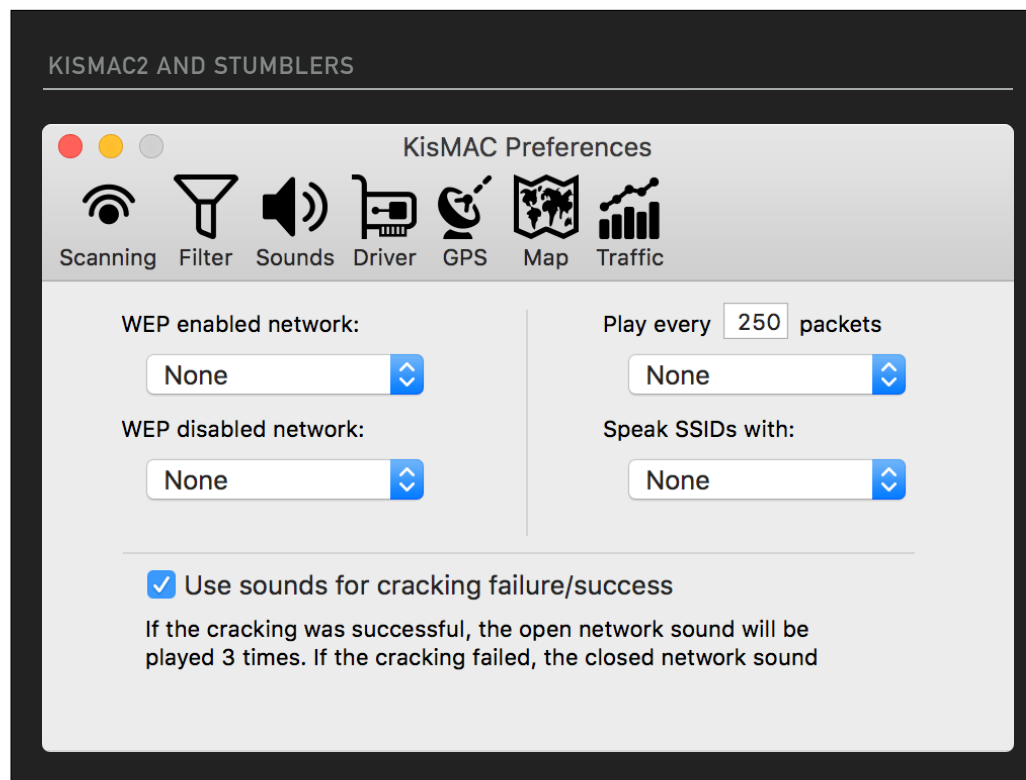
A cartoon duck character with a pink hood and a red pitchfork, standing on a dark background with concentric circles behind it.

WHERE IT REALLY STARTED

KISMAC2

KisMAC													
KisMac v0.3.4													
Ch	SSID	BSSID	Enc	Type	Signal	Avg	MaxSignal	Packets	Data	Last Seen	Ch...		
10	Fremont Caffè Vita Guest	AC:86:74:4A:24:CA	NO	managed	55	55	56	0	0B	2016-01-31 17:24:23 +0000	●		
10	Fremont Caffè Vita Guest	AC:86:74:4A:24:7A	NO	managed	47	47	49	0	0B	2016-01-31 17:24:23 +0000	●		
11	Ladybug Nugget	DC:9B:9C:F3:E0:6E	WPA	managed	18	18	18	0	0B	2016-01-31 17:24:23 +0000	●		
11	HOME-2FE8	44:32:C8:CF:2F:E8	WPA	managed	0	17	25	0	0B	2016-01-31 17:24:00 +0000	●		
6	xfinitywifi	0C:54:A5:71:A1:F2	NO	managed	0	0	0	0	0B	2016-01-31 17:24:23 +0000	●		
6	2001_a_space_odyssey	8C:04:FF:78:8B:05	WPA	managed	0	0	0	0	0B	2016-01-31 17:23:06 +0000	●		
1	xfinitywifi	74:85:2A:F2:05:4A	NO	managed	0	0	0	0	0B	2016-01-31 17:24:23 +0000	●		
1	xfinitywifi	CE:03:FA:3B:97:CA	NO	managed	0	0	0	0	0B	2016-01-31 17:22:22 +0000	●		
6	Via Tribunali	88:1F:A1:2E:AB:9E	WPA	managed	0	0	0	0	0B	2016-01-31 17:24:23 +0000	●		
1	viatriblueguest	40:4A:03:F4:02:C9	WPA	managed	0	0	0	0	0B	2016-01-31 17:24:23 +0000	●		
153	VitaFremont5	C4:04:15:14:48:80	WPA	managed	0	0	0	0	0B	2016-01-31 17:24:23 +0000	●		
161	HOME-D5D1-5	0C:54:A5:72:74:F8	WPA	managed	0	0	0	0	0B	2016-01-31 17:24:23 +0000	●		
11	Not the WiFi You're Look For	C8:B3:73:53:E1:EB	WPA	managed	0	0	9	0	0B	2016-01-31 17:24:23 +0000	●		
1	eap3	40:3C:FC:05:CF:41	WPA	managed	0	0	0	0	0B	2016-01-31 17:24:12 +0000	●		
1	xfinitywifi	46:32:C8:24:B0:74	NO	managed	0	0	0	0	0B	2016-01-31 17:21:29 +0000	●		
1	CenturyLink1761	10:5F:06:88:31:65	WPA	managed	0	0	0	0	0B	2016-01-31 17:24:23 +0000	●		
3	EyesOnFremont-2.4	00:71:C2:51:23:E8	WPA	managed	0	0	0	0	0B	2016-01-31 17:24:22 +0000	●		
6	HOME-D5D1-2.4	0C:54:A5:71:A1:F0	WPA	managed	0	0	0	0	0B	2016-01-31 17:24:23 +0000	●		
1	HOME-64E0-2.4	74:85:2A:F2:05:48	WPA	managed	0	0	0	0	0B	2016-01-31 17:24:23 +0000	●		
161	xfinitywifi	0C:54:A5:72:74:FA	NO	managed	0	0	0	0	0B	2016-01-31 17:24:23 +0000	●		
11	xfinitywifi	CE:35:40:45:C8:A3	NO	managed	0	0	10	0	0B	2016-01-31 17:24:23 +0000	●		
11	xfinitywifi	46:32:C8:CF:2F:EA	NO	managed	0	0	17	0	0B	2016-01-31 17:24:00 +0000	●		
36	DIRECT-roku-F3DC1A	B8:3E:59:B5:8C:35	WPA	managed	0	0	0	0	0B	2016-01-31 17:21:30 +0000	●		
2	FremontLaundryCenter	C0:EA:E4:BC:61:95	WPA	managed	0	0	0	0	0B	2016-01-31 17:24:23 +0000	●		
1	Cfast-2.4GHz	4C:60:DE:41:13:A3	WPA	managed	0	0	42	0	0B	2016-01-31 17:24:00 +0000	●		
6	IAMBATMAN	E8:37:7A:E8:E7:34	WPA	managed	0	0	0	0	0B	2016-01-31 17:21:39 +0000	●		
11	PyronetCL	58:8B:F3:09:05:AE	WPA	managed	0	0	12	0	0B	2016-01-31 17:24:23 +0000	●		
11	AHERN	C4:39:3A:07:0D:58	WPA	managed	0	0	0	0	0B	2016-01-31 17:22:00 +0000	●		
5	MAGFLOSOR	10:0D:7F:DD:6F:52	WPA	managed	0	0	0	0	0B	2016-01-31 17:24:00 +0000	●		
11	WinterIsComing	20:4E:7F:2F:C2:EA	WPA	managed	0	0	0	0	0B	2016-01-31 17:22:11 +0000	●		
8	CenturyLink8603	B2:B2:DC:14:04:10	WPA	managed	0	0	0	0	0B	2016-01-31 17:22:11 +0000	●		
1	HOME-97C8	CC:03:FA:3B:97:C8	WPA	managed	0	0	0	0	0B	2016-01-31 17:22:44 +0000	●		
11	HOME-C8A1	CC:35:40:45:C8:A1	WPA	managed	0	6	6	0	0B	2016-01-31 17:23:06 +0000	●		
1	HOME-B072	44:32:C8:24:B0:72	WPA	managed	0	0	0	0	0B	2016-01-31 17:22:55 +0000	●		
11	ten22home Network	40:3C:FC:08:01:E5	WPA	managed	0	0	0	0	0B	2016-01-31 17:23:33 +0000	●		
6	HOME-B14B-2.4	D8:97:BA:D9:54:88	WPA	managed	0	0	0	0	0B	2016-01-31 17:23:17 +0000	●		
132	Via Tribunali	88:1F:A1:2E:AB:9F	WPA	managed	0	0	0	0	0B	2016-01-31 17:24:23 +0000	●		
4	2.4GHzForN00Bs	84:1B:5E:03:DF:D5	WPA	managed	0	0	0	0	0B	2016-01-31 17:24:23 +0000	●		

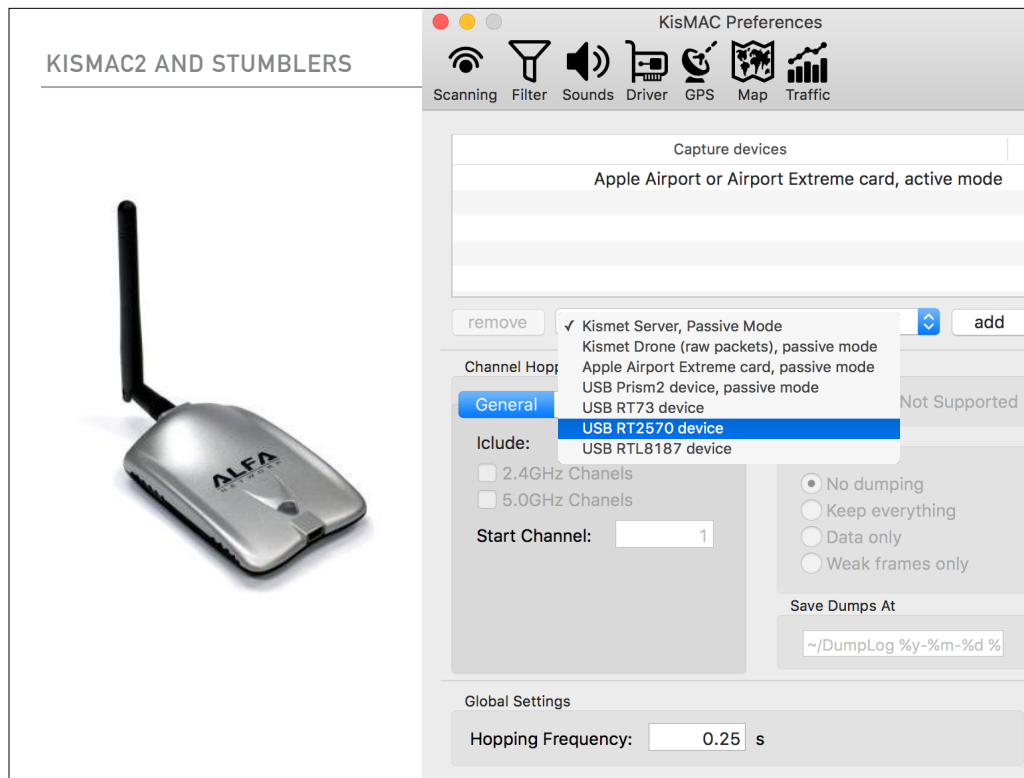
Kismac was an early Mac tool to look at what was going on around you, and was/is based on an open source project called Kismet. Kismac listed the networks that it found, and provided information regarding signal levels and encryption types.



The real appeal of a stumbler like Kismac lay in its features for wardriving.

1. It was able to discover “hidden” networks.
2. It could map them.
3. It could attack weak keys, especially WEP keys.

After a while, Apple changed their wireless frameworks and drivers to disallow discovery of the hidden networks, exiling early stumblers to the Island of Misfit Toys.



Development picked up again when IGRSoft forked the project and moved it to GitHub (<https://github.com/IGRSoft/KisMac2>)

In theory, you can pick up a USB WiFi card using one of the shown chipsets and regain the lost stumbling features. The card pictured is an Alfa AWUS036H adapter, which is 2.4 GHz only. I stood on the front steps of the Grange Wellington Hotel following my arrival and detected 212 unique BSSIDs using the 9 dB gain antenna. Using his built-in WiFi interface, Tom picked up 24 from the same location.

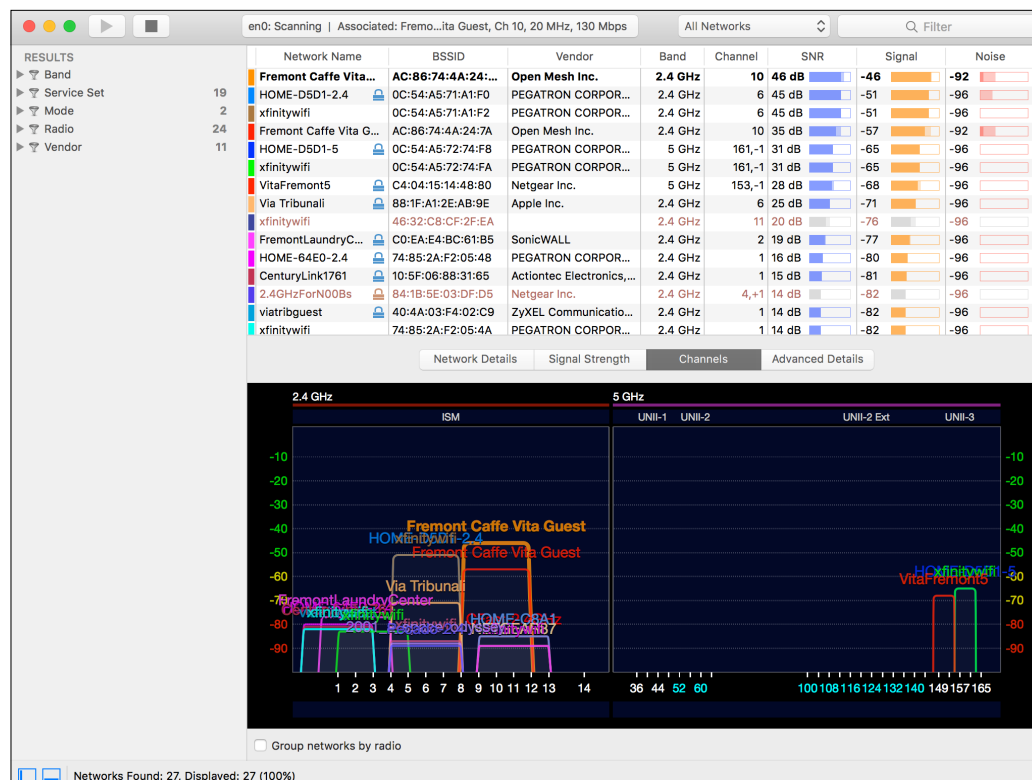
Thankfully, only one of the 212 networks visible from the Grange Wellington still utilizes WEP security. I did *not* attempt to crack it.

Product development seems to be both volunteer-based *and* sporadic, so use at your own risk, and be prepared to experiment.

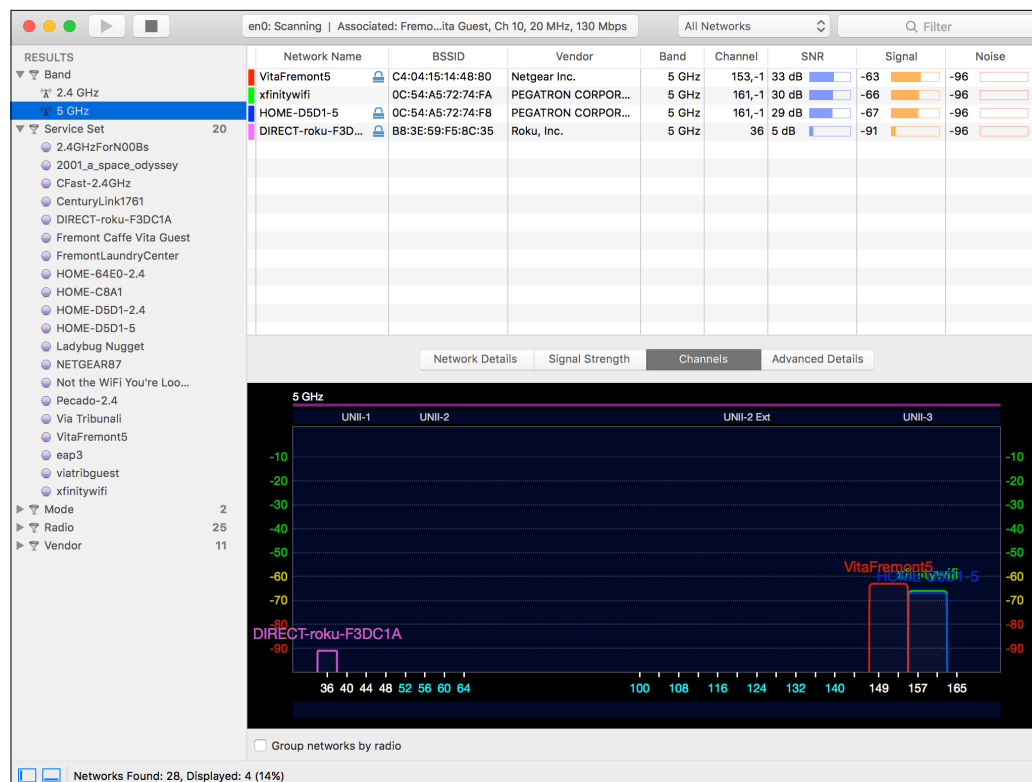


WiFi Explorer is written by independent developer Adrian Granados, is currently available at the Mac App Store or via <http://www.adriangranados.com>, costs US \$15 (£10.99) and is worth every penny.

WiFi Explorer takes advantage of information that it gathers from the OS to display extensive information about networks that your computer can see.

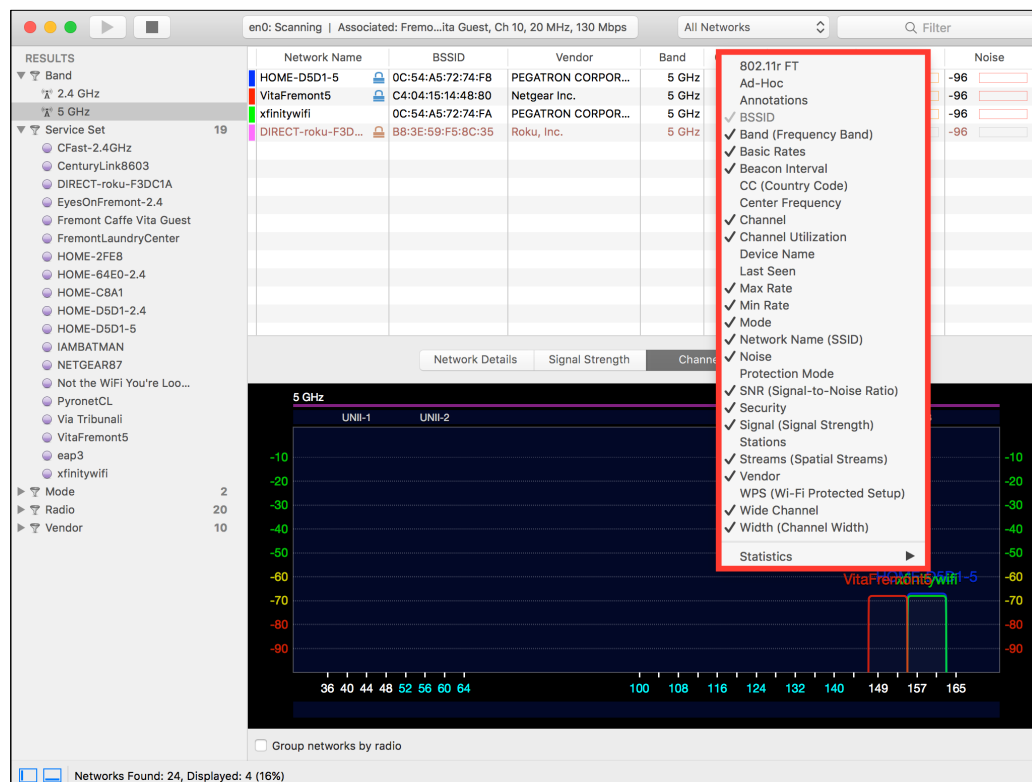


Generally, WiFi Explorer shows a three pane view with network information at the top and details at the bottom. In the Channels view, WiFi explorer provides easily readable information about channel use of the various networks it detects, the widths of those channels, and the signal strength of those networks as detected by the computer running WiFi Explorer.



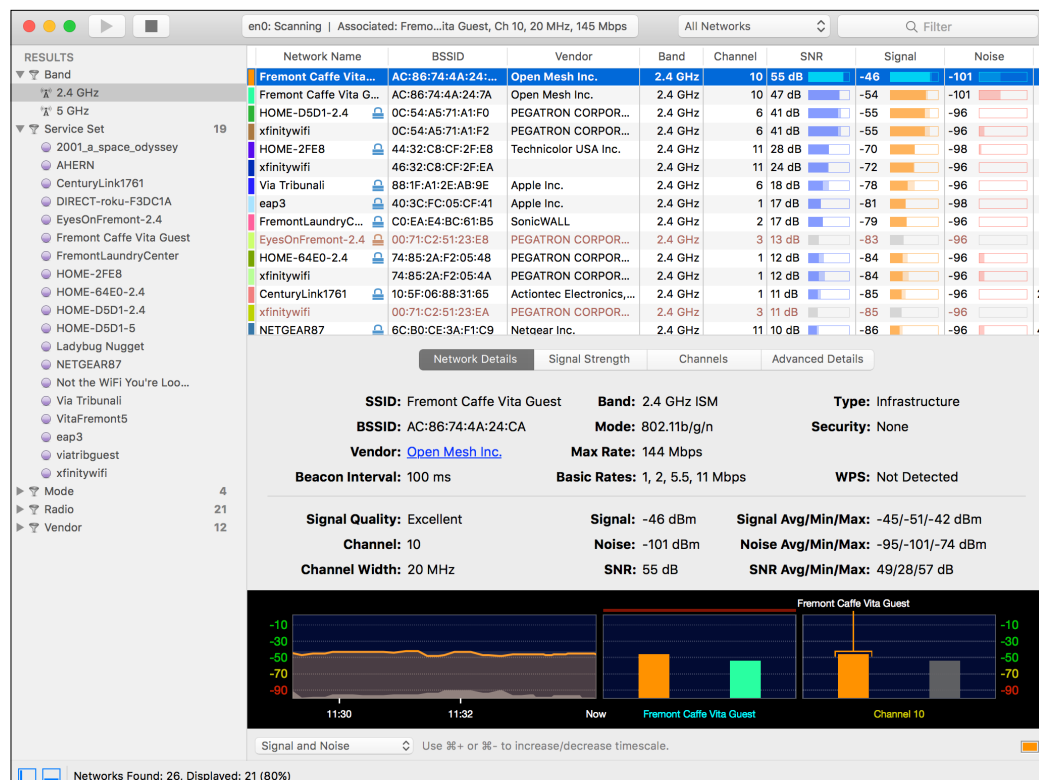
On the left, prebuilt filters give you the option to refine your view according to one of several criteria, making it possible to narrow your examination to items of interest:

1. Frequency Band
2. SSID
3. Network Mode
4. Radio
5. Vendor



Control clicking on one of the columns at the top of the window gives you a list of all the information that WiFi Explorer can display. Most of it comes from the beacon frames that access points use to advertize their networks.

This information doesn't reasonably fit on a 13" display, even at highest resolution.



If there's a particular network you're interested in, select it and click the "Network Details" button in the middle of the screen, and WiFi Explorer will give you a nice summary in a more human-readable format. Looking at Advanced Details will show you the content of the beacon frames directly.

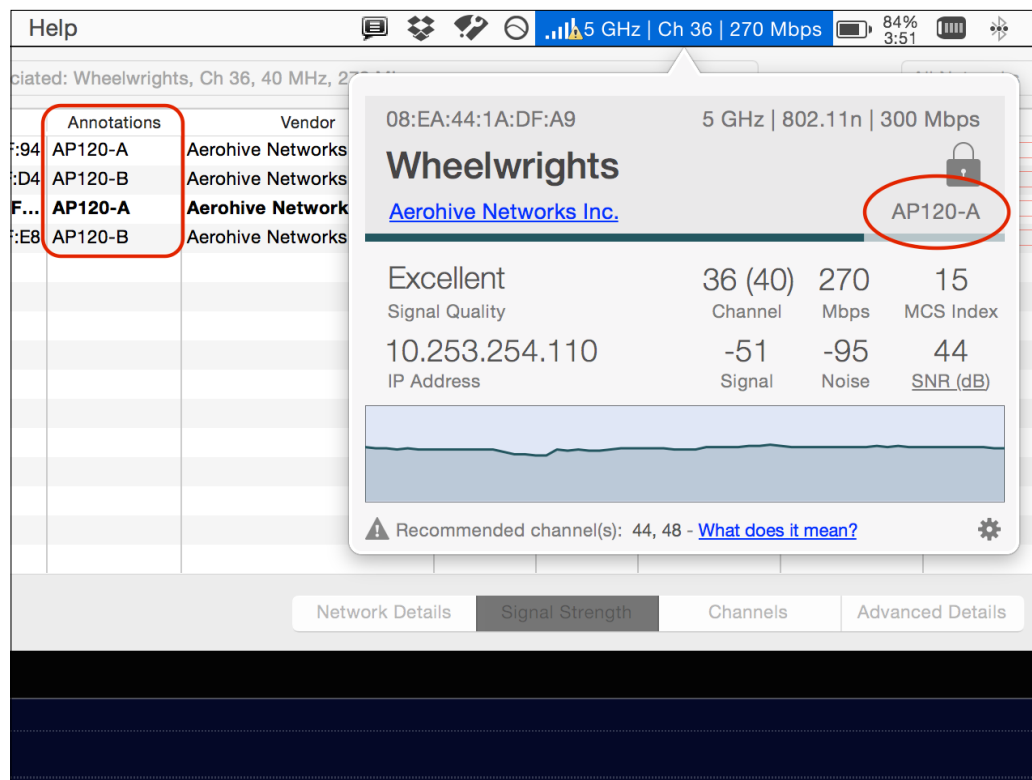


WiFi Signal is also by Adrian Granados, and costs US \$3.



WiFi Signal builds on the same information used by the WiFi menu item, but provides a more readable view as well as some additions:

1. WiFi Signal provides customizable display of information in the Menu bar.
2. WiFi Signal calculates Signal to Noise ratio.
3. WiFi Signal also provides an evaluation of the connection quality, and will attempt to recommend better channels.

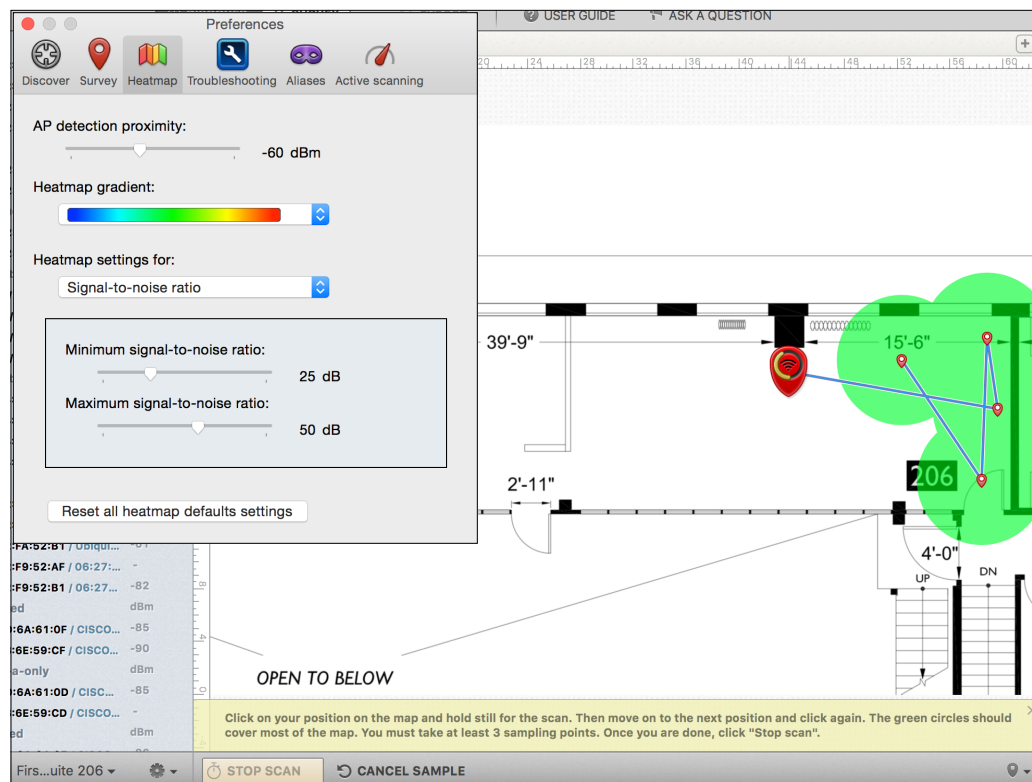


A subtle feature of WiFi Explorer and WiFi Signal lies in the ability to include annotations of networks in WiFi Explorer. WiFi Signal will then display the annotations in its window. In my case, I use this to provide more readable labels for my APs, so that I can tell which AP I'm associated to without having to memorize its BSSID MAC address. This can be handy for understanding when you are in a sticky client situation.



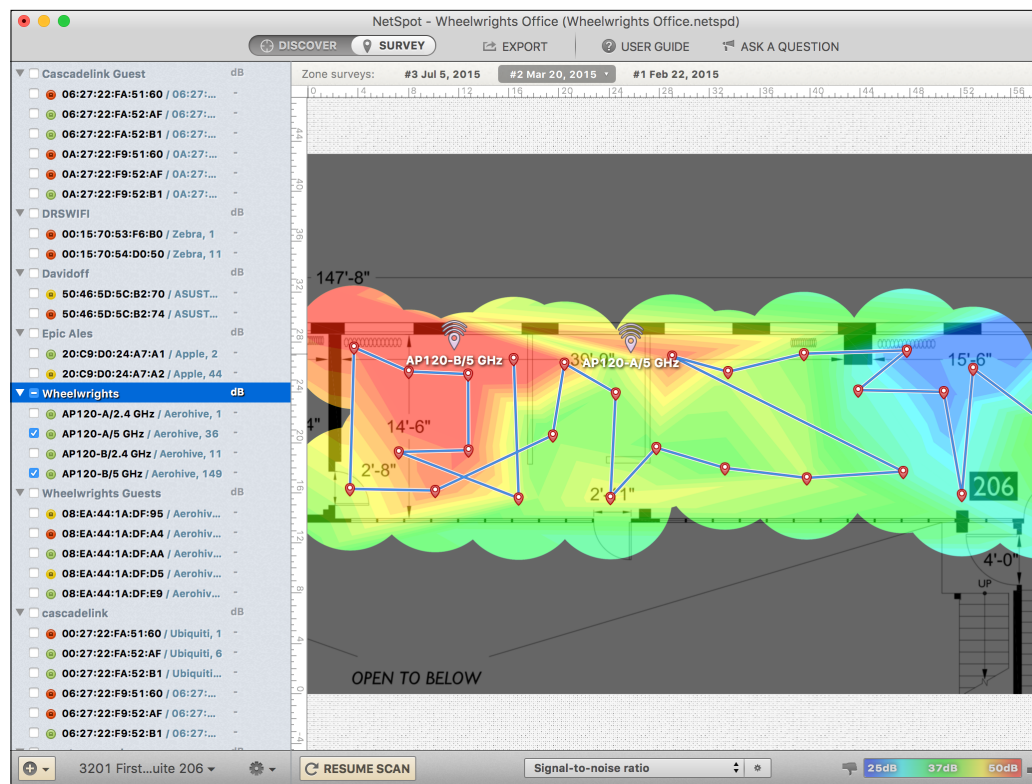
Tools like WiFi explorer provide a large amount of information, but that information is limited by being specific to the computer's location at the time it took the sample. To more fully understand a WiFi network, you will want information from multiple locations around a network. A heat mapper will do this.

Netspot Pro (<http://netspotapp.com>) is a heat mapper and reporting tool from Etwok (Autocorrect likes to change Etwok to Ewok). NetSpot Pro (in version 2 at the time of this writing) costs US \$149 for an individual license, and the vendor offers volume licensing as well. To our knowledge, it is *currently* the only Mac OS-native tool.



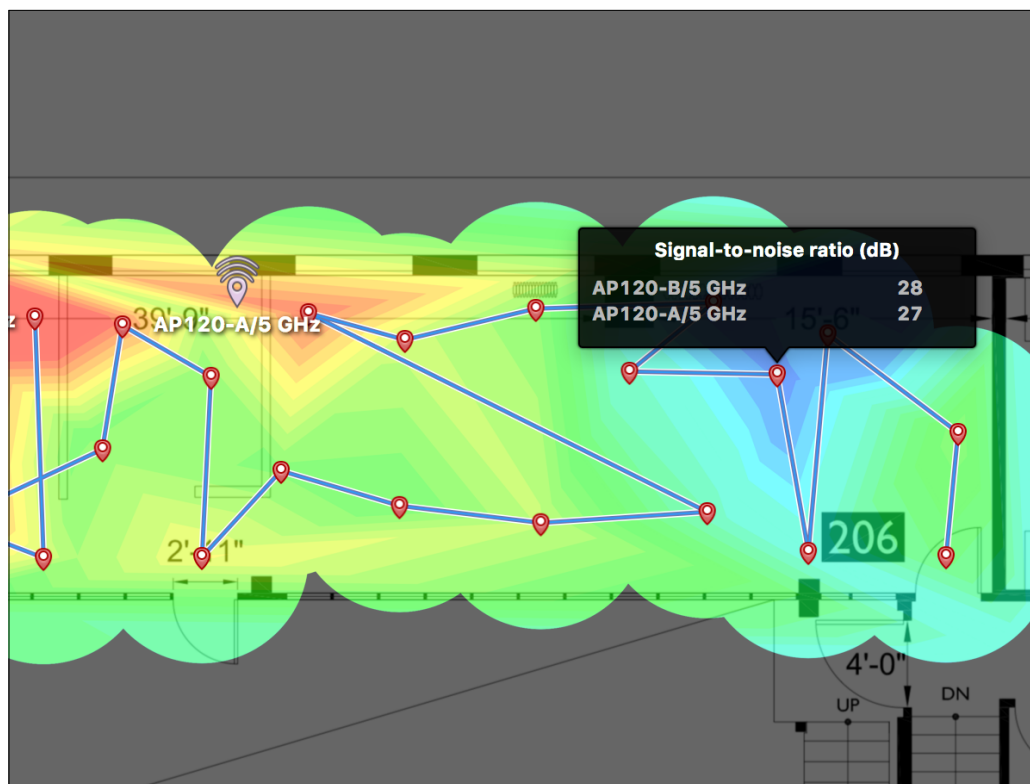
In order to use NetSpot Pro to map a network, do the following:

1. Decide on settings to use to define your thresholds, and set the threshold in preferences. In this case, I've decided on a maximum (best)/minimum (worst) SNR of 50 dB and 25 db, respectively.
2. Import and scale a floorpan of your facility.
3. Walk through the facility with your laptop and click your location to trace your walking path.
4. Each time you click your location, NetSpot will draw a green circle around you containing the area where it thinks it can estimate coverage.
5. Step-click through the facility until you fill it with green.
6. Click "Stop Scan", and NetSpot will run calculations to display your selected visualization.

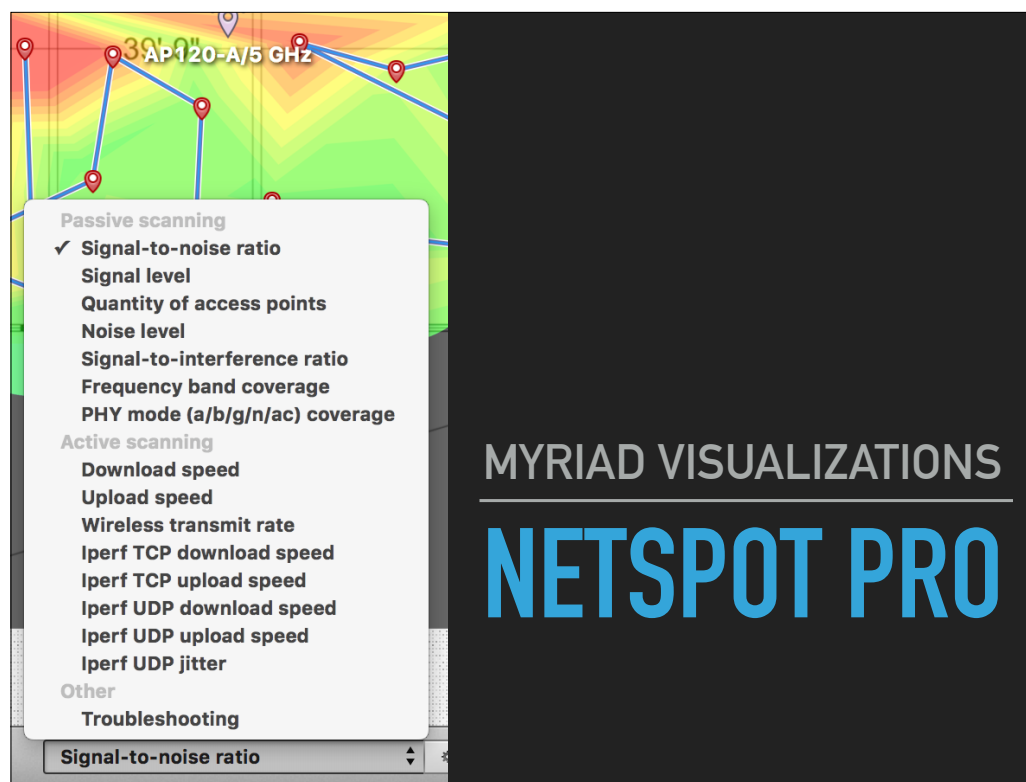


When you complete the scan, NetSpot will generate a heat map of your facility based on the access points you choose in the list of APs it detects. NetSpot will calculate results and display one of several visualizations. In the example, I generated a signal-to-noise (SNR) visualization for the Wheelwrights 5 GHz network. Note the following:

1. Locations of the access points, unevenly distributed through the office.
2. Significantly cooler colors toward the upper right, indicating poorer signal-to-noise ratio.



Within a visualization, NetSpot allows you to click on a given sample point to view the data NetSpot gathered at that point. Note that NetSpot provides a separate listing for each access point it detected at that sample point.



Signal-to-noise will likely be the most desirable visualization, but NetSpot Pro provides a variety of visualizations, and will rebuild them dynamically based on your selection. Note that NetSpot is doing a lot of calculating, so large reports can take significant time to export.

Wheelwrights Office

Visualization #1.1.2: Signal-to-noise ratio 5GHz

Zone and snapshot:

3201 First Avenue S., Suite 206

#2 Mar 20, 2015

Visualization settings:

Min signal-to-noise ratio

25dB

Max signal-to-noise ratio

50dB

Requirements: 25dB 37dB 50dB

Figure 1.1.2: 3201 First Avenue S., Suite 206 > #2 Mar 20, 2015 > Signal-to-noise ratio 5GHz

This visualization was also exported individually per Access Point, you can find all individual reports in the following folder: /images/3201 First Avenue S., Suite 206 - #2 Mar 20, 2015

#	Network name	MAC-address	Ch	Mode	Security	Max SNR	Vendor
1	Wheelwrights AP120-A/5 GHz	08:EA:44:1A:DF:A9	36	a/n	WPA2 Personal	40dB	Aerohive
2	Wheelwrights AP120-B/5 GHz	08:EA:44:1A:DF:E8	149	a/n	WPA2 Personal	54dB	Aerohive

Make sure the networks you would like to see in the exported report are selected in the sidebar. The report is built based on this selection

☒ Export only surveyed part of the map
 ☒ Open report after exporting

Export multiple zones

Generate a customizable enterprise-level report on the current survey.

Advanced export

Export current visualization

Quickly generate an overview PDF report on the current visualization. No customization.

Quick export

Save this heatmap into an image

Save the heatmap you see now as an image. Image size will equal your area map's size.

☒ Include legend

Current heatmap

Cancel

EXPORT REPORTS

NETSPOT PRO

Being able to examine only one visualization at a time becomes annoying after a point. NetSpot also allows export of heat maps to reports that detail the content of the visualizations in print. Because the reports can list information on a per-access point basis, they can become quite long.

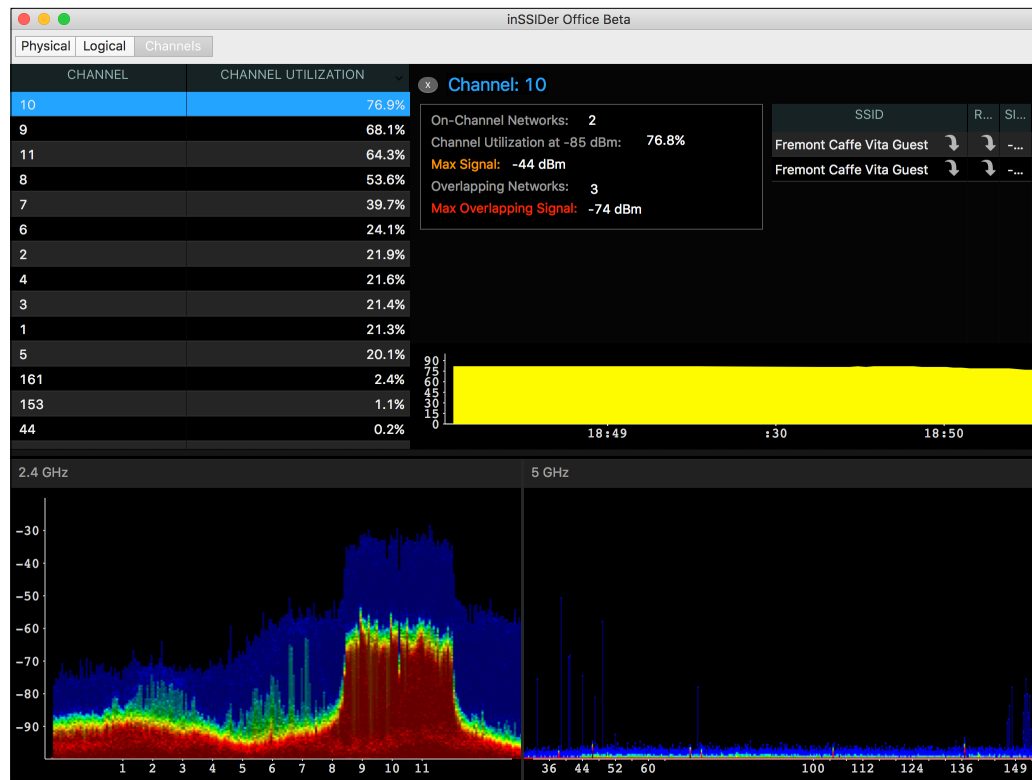


Both WiFi Explorer and NetSpot are taking advantage of information that they obtain from Mac OS. Both report information obtained by Apple's frameworks and drivers. This can be limiting, because there are a lot of things in WiFi that are not necessarily WiFi.

Metageek's InSSIDer Office (beta) is a US\$149 application intended for basic exploration of the WiFi radio spectrum.



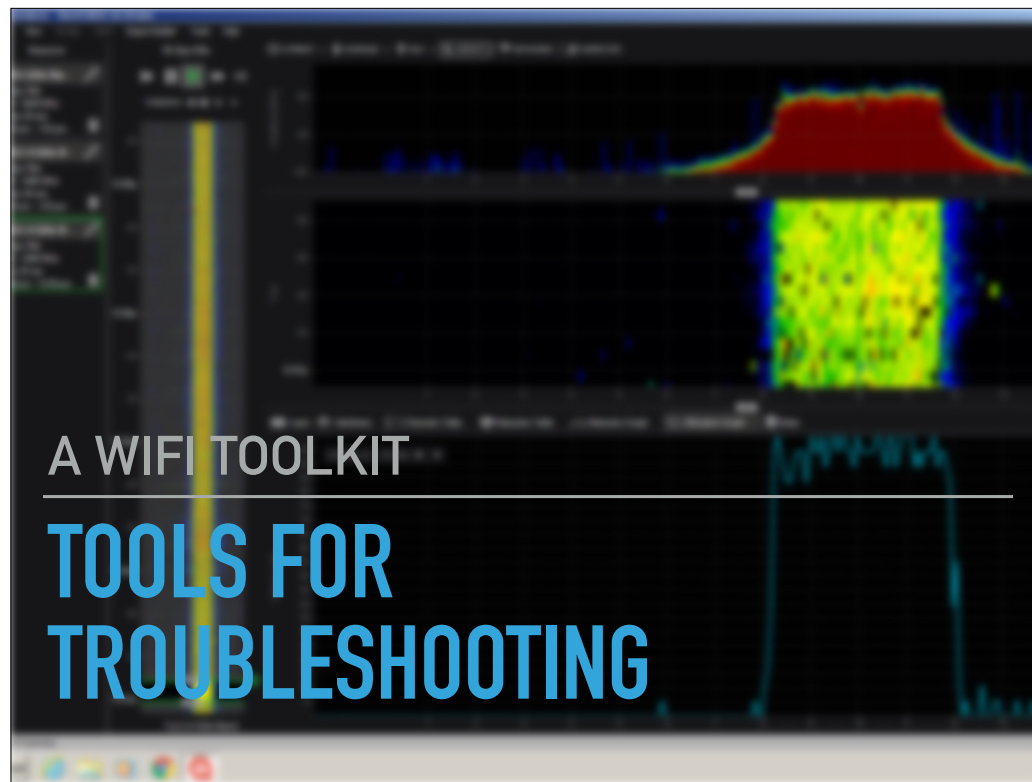
InSSIDer Office is a companion application to Metageek's Wi-Spy series of spectrum analyzers. Without the Wi-Spy attached, the application is not that much different from WiFi Explorer, and is actually less well-organized.



Using InSSIDer Office with the Wi-Spy allows interpretation of raw radio signals in the 2.4 GHz and 5 GHz frequency bands that WiFi uses. In other words, InSSIDer and Wi-Spy see the WiFi signals, but also hear the non-WiFi signals, and provide measurements for how intense the use of the radio spectrum is. In this example, InSSIDer shows high utilization of Channel 10 in the 2.4 GHz spectrum.

InSSIDer provides *basic* information on spectrum use, but has limitations:

- ▶ The timespans for capture are limited, and InSSIDer displays a simple aggregate of use over the selected time period. The shortest period is two minutes.
- ▶ Data gathered is limited to the computer running the program.
- ▶ InSSIDer will not identify hidden networks.

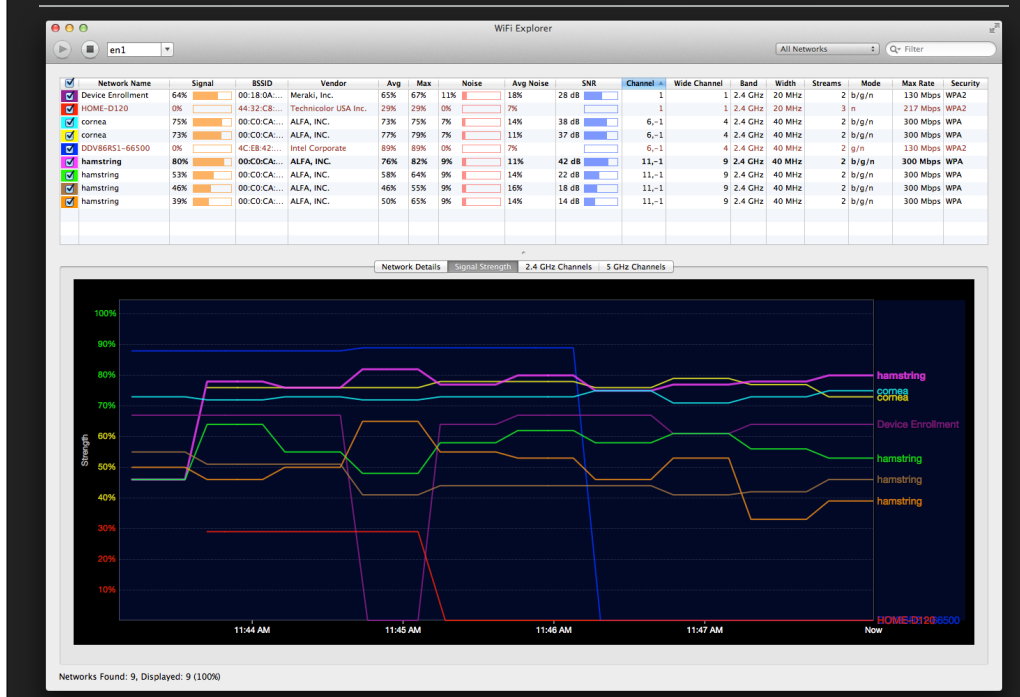




Many of the tools we saw for exploration provide information useful in troubleshooting, particularly with respect to basic network design.

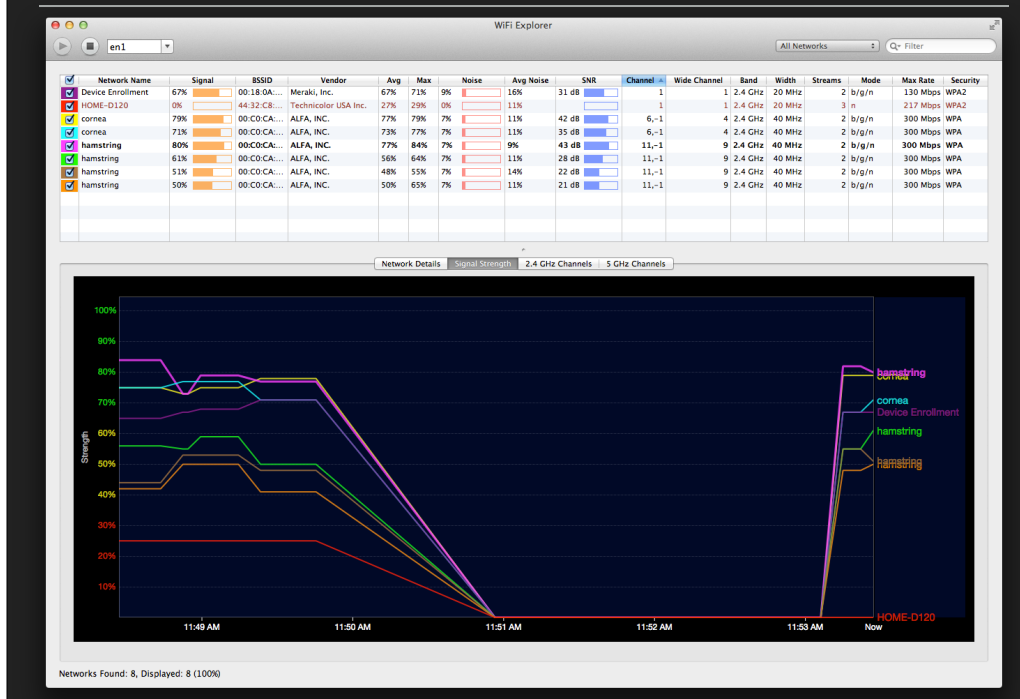
WiFi Explorer is good at visualizing signal level, while NetSpot is good at making maps, while inSSIDer Office can give you the basics of spectrum analysis with an attached analyzer. Let's talk about using these more for troubleshooting.

TROUBLESHOOTING WITH WIFI EXPLORER - SIGNAL DROPS



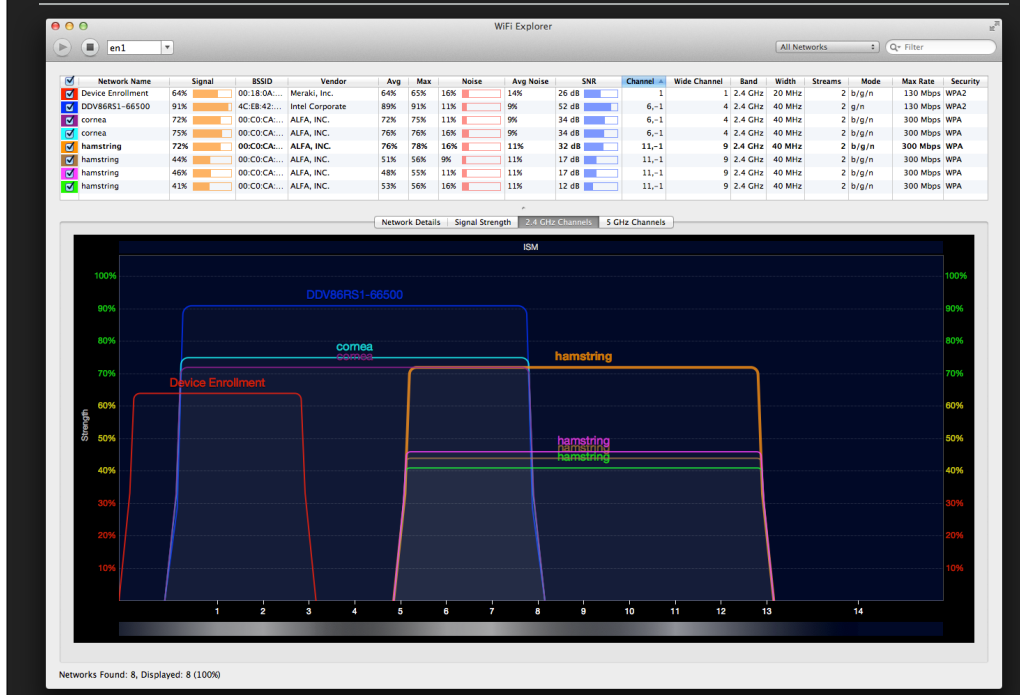
WiFi Explorer's Signal Strength pane will show you fluctuation in signal strength in the networks around you, and in this case shows that the AP Chris brought to perform iOS MDM enrollments was dropping out on an erratic basis.

TROUBLESHOOTING WITH WIFI EXPLORER - SIGNAL DROPS



A few minutes later, the Signal Strength pane showed that all visible networks dropped out just as soon as a nearby laptop began downloading a Microsoft Office 2011 full installer. Oh my. Let's look more at this network design, shall we?

TROUBLESHOOTING WITH WIFI EXPLORER - CHANNEL PROBLEMS



Where to start?

Looking at the Channels pane gave me some additional information:

1. Whoever designed the network “hamstring” chose to place all APs on the same channel in the 2.4 Ghz Spectrum.
2. Whoever designed the network “hamstring” chose to use 40 MHz wide channels, guaranteeing overlap (and adjacent channel interference) with the network “cornea”, also using 40 MHz channels.

WiFi Explorer showed me that the network “hamstring” was poorly designed.



40 MHZ CHANNEL WIDTHS IN 2.4?!

WEEHAWKEN. DAWN.
GUNS. DRAWN.









Where to start?

Looking at the Channels pane gave me some additional information:

1. Whoever designed the network “hamstring” chose to place all APs on the same channel in the 2.4 Ghz Spectrum. This is a bad idea. Co-channel interference demands that for each additional AP or SSID on the same radio frequency, you lose 3.225% overall traffic. In this case, 12.90% of the traffic is being wasted because of co-channel interference that isn’t necessary.
2. Whoever designed the network “hamstring” chose to use 40 MHz wide channels, guaranteeing overlap (and adjacent channel interference) with the network “cornea”, also using 40 MHz channels.

WiFi Explorer showed me that the network “hamstring” was poorly designed.

Fixes in this case would include decreasing the channel width to 20Mhz, and spreading out the APs to take advantage of distance between the APs before re-using a given channel. This could reduce overhead from 13% to 3.2%. Given that interference hurts 40Mhz bands more than 20Mhz bands, there is also a gain to be had.

<input checked="" type="checkbox"/>	Network Name	Signal	BSSID	Vendor
<input checked="" type="checkbox"/>	Device Enrollment	64% 	00:18:0A:...	Meraki, Inc.
<input checked="" type="checkbox"/>	DDV86RS1-66500	91% 	4C:EB:42:...	Intel Corporate
<input checked="" type="checkbox"/>	cornea	72% 	00:C0:CA:...	ALFA, INC.
<input checked="" type="checkbox"/>	cornea	75% 	00:C0:CA:...	ALFA, INC.
<input checked="" type="checkbox"/>	hamstring	72% 	00:C0:CA:...	ALFA, INC.
<input checked="" type="checkbox"/>	hamstring	44% 	00:C0:CA:...	ALFA, INC.
<input checked="" type="checkbox"/>	hamstring	46% 	00:C0:CA:...	ALFA, INC.
<input checked="" type="checkbox"/>	hamstring	41% 	00:C0:CA:...	ALFA, INC.

“WAIT A MINUTE... WTAF?”

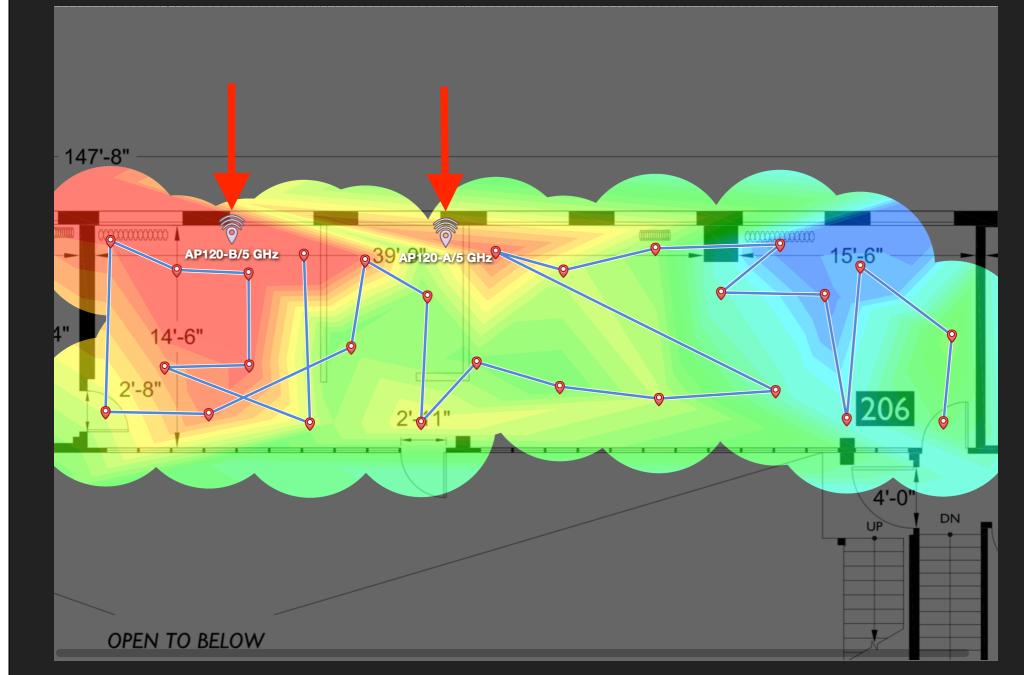
Chris Dawe and Tom Bridge

An additional problem only became apparent when I realized that all of the equipment from both the “hamstring” and “cornea” networks consisted of equipment from ALFA, INC.

Ultimately, we realized that the vendor had found hamstring to be less reliable than they liked, and had installed cornea as a backup for when hamstring wasn’t working.

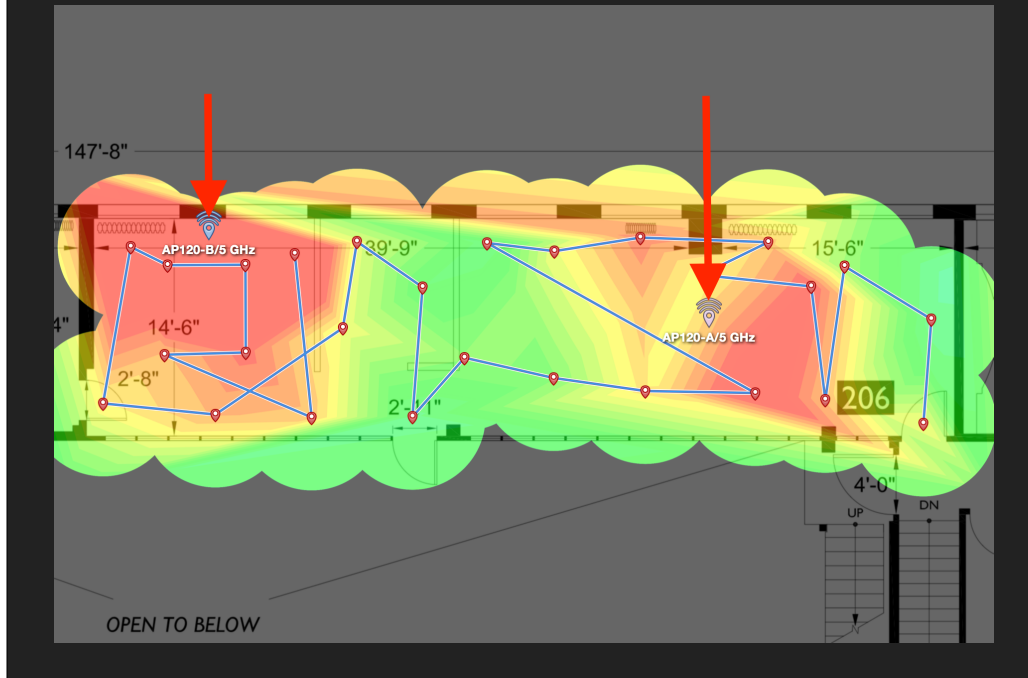
In other words, they deployed a flawed design and compounded it with another flawed design. Everything went to the same LAN, so what was the point of a secondary backup?

TROUBLESHOOTING WITH NETSPOT (BEFORE!)



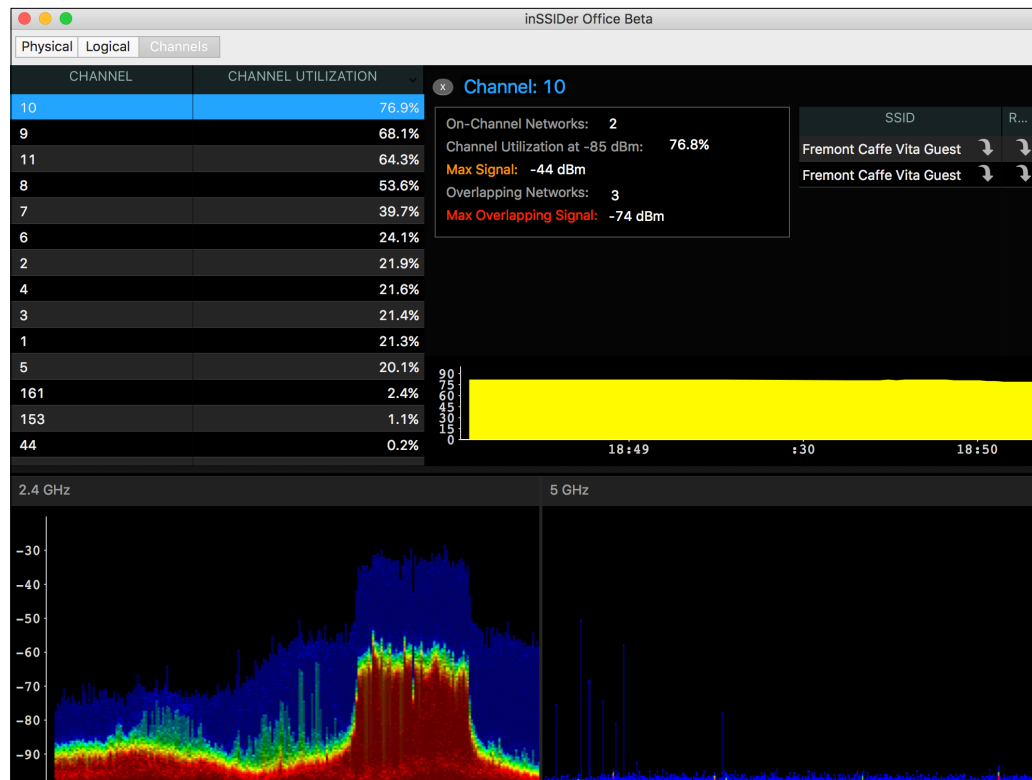
NetSpot's ability to display information from multiple samples *and* map locations of access points comes in handy as well. In the case of my office, NetSpot showed that my APs placement resulted in a low SNR area toward the front of the office, in the area where we have meetings and white board conversations.

Being able to visualize this area of low SNR gave me ideas about where I ought to move an AP in order to improve coverage.



So AP A went on the ceiling on the right side of the diagram.

Measuring after you move is just as important as measuring before. Make sure to document your changes to look for the unexpected.



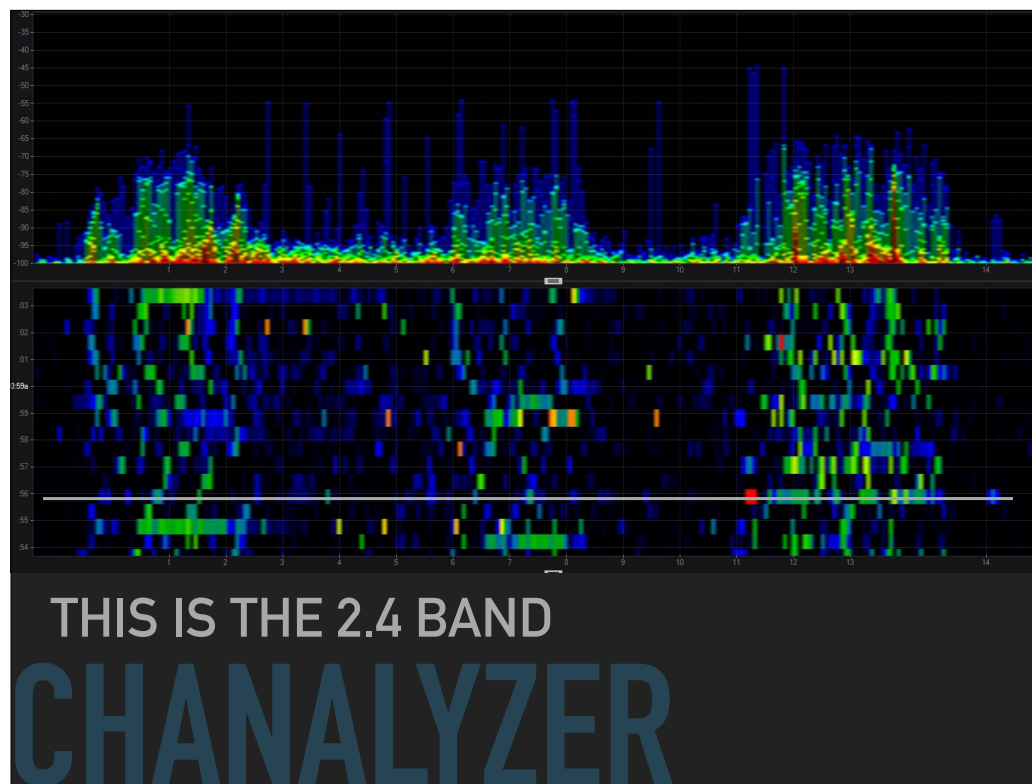
InSSIDer office confirmed for me that users in a local coffee shop were beating hard on the available 2.4 GHz network. This was visually obvious in the density graph at the bottom left, and using the “Channels” view in the top left corner, then selecting the channel with the highest reported utilization provides a graph of utilization over time.



Furthermore, InSSIDer Office was able to identify the networks most likely to be interfering with the coffee shop network. This didn't fit well in the screen capture, but note that selecting the "Physical" tab in the top left corner, then selecting the wireless network you care about displays this information.

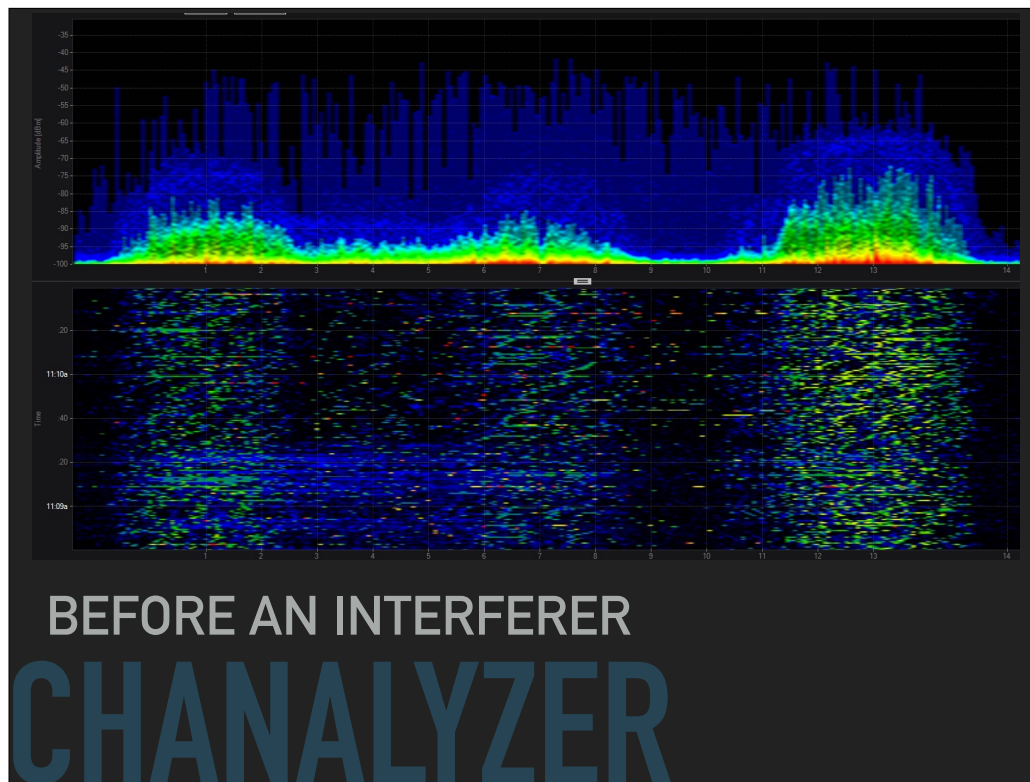


Not all 2.4GHz or 5GHz traffic is 802.11 traffic. Sometimes there's a bunch of RF in there, too, and that's really what you need a spectrum analyzer to see.

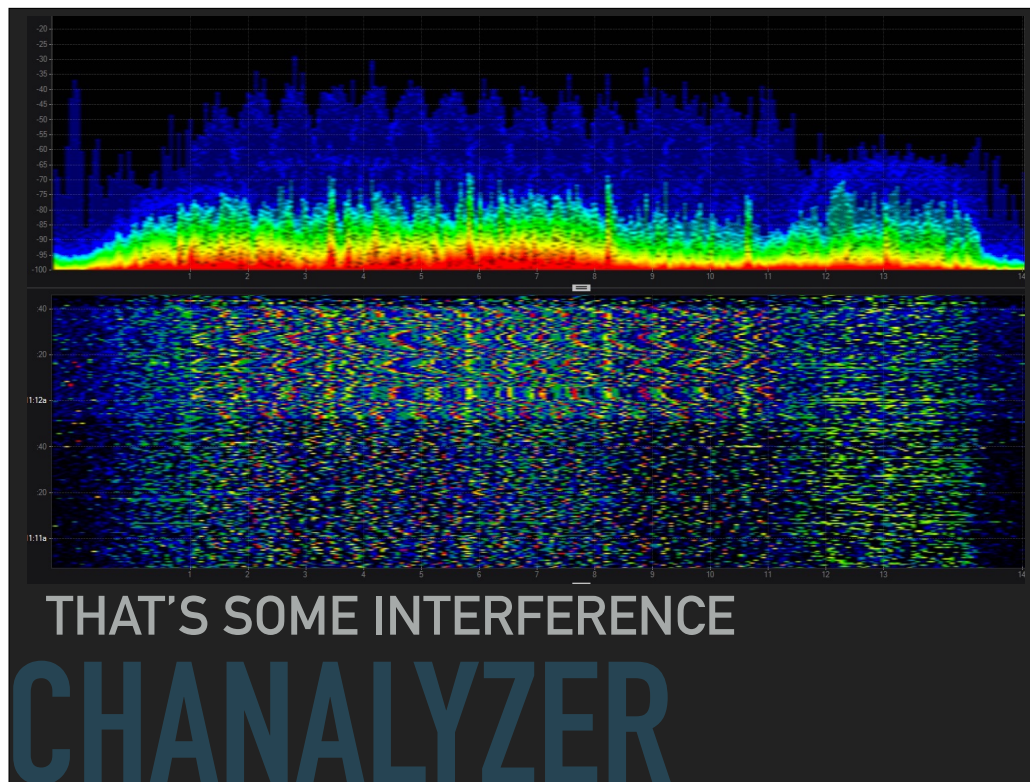


This is a full-spectrum capture of the 2.4GHz band of an active hotel network. You can see it's fairly clear with patterns of activity on Channels 1, 6 and 11. This network is active, but not incredibly busy.

The bottom waterfall display will let us see signal intensity patterns in realtime, while the power graph above lets us see the intensity over time through colored highlights.



Here's our before shot. This is a two minute intensity sample, and you can see that we have super active band on 11, with some good activity on 1 and 6.



BOOM. Look at all that interference. That's a Baby Monitor. We've got it with us, and for the low low price of some beers at the pub, we won't plug it in right now for a live demonstration.

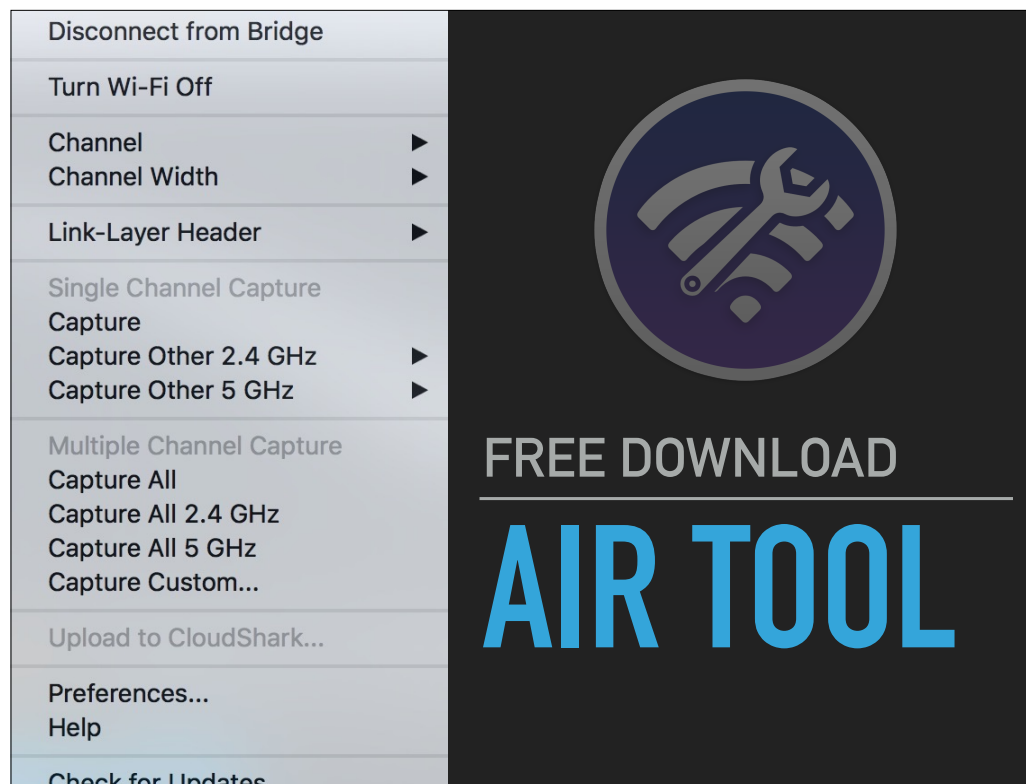
What's that? We should? Okay, here goes. You're on the hook for beer later...



Okay, we're going to switch over to my other laptop here and take a look at a live spectrum analysis that we've had running since we started.



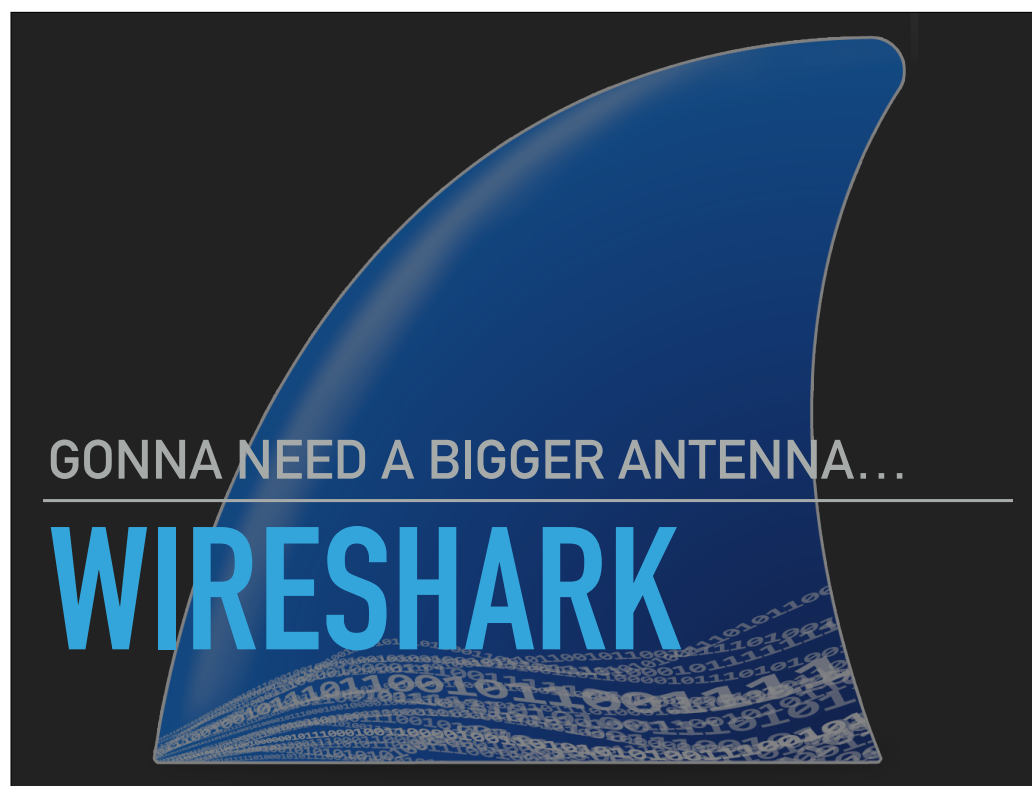
The first up is Adrian Granados' AirTool. It's designed to capture raw packet data on one or more channel, which will include the physical layer traffic that Wireshark won't necessarily grab while just monitoring your AirPort card.



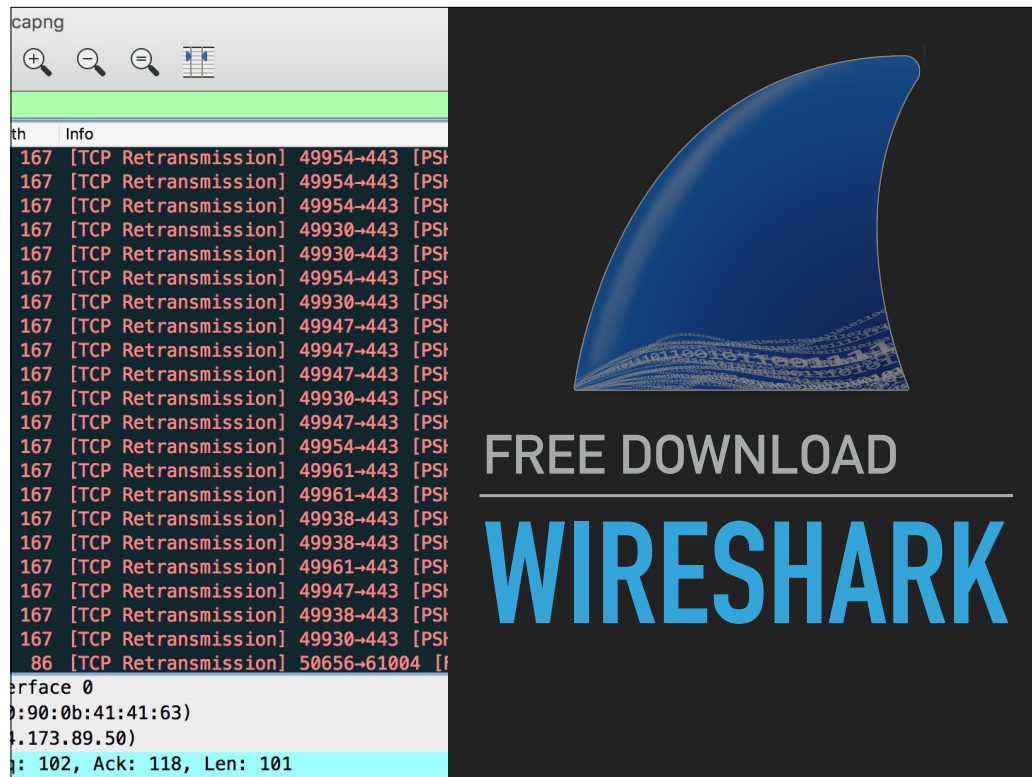
The interface is fairly straightforward, and will let you specify a channel and channel width, and then it will capture the data you're looking for, but while it's capturing, you will not be connected to the network in the traditional way. All you'll be doing is grabbing traffic, not participating in it.

AirTool is primarily a tool for gathering 802.11 data from the AirPort card in your Mac. It will grab data on a per-channel basis, or it will grab all the channels in a given spectrum. That can be a lot to look at once, so unless you're planning on a lot of data munging, or maybe some surveillance tasks

It operates as a Menu Bar Extra, so if you already have a bunch of menu bar extras, I'm sorry, you're adding one more...



Not all Wi-Fi problems are interference problems.
Seeing the raw traffic can provide answers no other tools can provide
But it comes at a mental cost.



Wireshark is an open source tool, good for reviewing raw data frames from your Wired & Wi-Fi networks.

Works with any .pcap file

Searching and filtering that data to find useful trends

Good Cheat Sheet: <https://slack-files.com/files-pri-safe/T04QVKUQG-F0KMM9MC4/>

[wireshark_802.11_wifi_filters_reference.pdf?c=1454971990-c5f3aa5855ce8f143ca57af0dbae67c8ec1f79bd](https://slack-files.com/files-pri-safe/T04QVKUQG-F0KMM9MC4/wireshark_802.11_wifi_filters_reference.pdf?c=1454971990-c5f3aa5855ce8f143ca57af0dbae67c8ec1f79bd)

140	1_	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request	- Transaction ID 0xf37a7f5e
143	1_	10.0.50.1	255.255.255.255	DHCP	358	DHCP ACK	- Transaction ID 0xf37a7f5e
225	1_	0.0.0.0	255.255.255.255	DHCP	350	DHCP Discover	- Transaction ID 0x6d28
226	1_	10.0.50.1	255.255.255.255	DHCP	344	DHCP Offer	- Transaction ID 0x6d28
231	1_	0.0.0.0	255.255.255.255	DHCP	350	DHCP Request	- Transaction ID 0x3f4f
232	1_	10.0.50.1	255.255.255.255	DHCP	344	DHCP ACK	- Transaction ID 0x3f4f

DHCP LEASES

If you're having issues with addressing, you can watch the DHCP process live and diagnose why it is you're ending up in 169.254. If you're seeing the full Request/ACK/Discover/Offer cycle, check to make sure that you're only seeing one set of transactions...

```
▼ IEEE 802.11 Beacon frame, Flags: .....C
  Type/Subtype: Beacon frame (0x0008)
  ► Frame Control Field: 0x8000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: RuckusWi_35:78:cc (2c:c5:d3:35:78:cc)
    Source address: RuckusWi_35:78:cc (2c:c5:d3:35:78:cc)
    BSS Id: RuckusWi_35:78:cc (2c:c5:d3:35:78:cc)
    .... .... 0000 = Fragment number: 0
    0100 1010 1100 .... = Sequence number: 1196
  ► Frame check sequence: 0xe6ebae6 [correct]
```

BEACON FRAMES

If you've never figured out what percentage of your total Wi-Fi traffic is your beacon frames, then you need to do that. Multiple radios on one channel decrease available throughput, and so do multiple SSIDs on multiple radios. If you've got three SSIDs and three same-channel radios, you lose 30% of your available throughput to beacon frames.

Link for SSID Calculator: <http://www.revolutionwifi.net/revolutionwifi/p/ssid-overhead-calculator.html>

<http://www.revolutionwifi.net/revolutionwifi/p/ssid-overhead-calculator.html>

You can also look at the capture traffic to find out what else is broadcasting in a given space. Looking at the capture traffic is going to show you when you're overlapping with another access point that could be causing issues.

You can also review the settings for each given beacon frame.

```

▼ Fixed parameters (12 bytes)
  Timestamp: 0x0000021f4f9a903b
  Beacon Interval: 0.102400 [Seconds]
▼ Capabilities Information: 0x0111
  .... 1 = ESS capabilities: Transmitter is an AP
  .... 0. = IBSS status: Transmitter belongs to a BSS
  .... 0. 00.. = CFP participation capabilities: No point coordinator at AP (0x0000)
  .... 1 .... = Privacy: AP/STA can support WEP
  .... 0. .... = Short Preamble: Not Allowed
  .... 0. .... = PBCC: Not Allowed
  .... 0... .... = Channel Agility: Not in use
  .... 1 .... .... = Spectrum Management: Implemented
  .... 0... .... = Short Slot Time: Not in use
  .... 0... .... = Automatic Power Save Delivery: Not Implemented
  .... 0 .... .... = Radio Measurement: Not Implemented
  .... 0. .... .... = DSSS-OFDM: Not Allowed
  .... 0... .... = Delayed Block Ack: Not Implemented
  .... 0... .... = Immediate Block Ack: Not Implemented

```

BEACON FRAMES

The beacon frames are the rules of the road for Wi-Fi. Want to do short guard interval but not sure if the AP supports it? Check in the Beacon Frame. Looking for a specific feature? Check in the Beacon Frame.

More on Management Frames: <http://flylib.com/books/en/2.519.1.35/1/>
<http://shop.oreilly.com/product/9780596001834.do>

10	0	NestLabs_e5:7e:65	95:2b:89:03:78:cc	802.11	272	Disassociate, SN=738, FN=5, Flags=op.PRMFTC
21903	5	4e:7a:6b:e7:94:bd	0a:44:1b:dd:a2:ac	802.11	57	Disassociate, SN=1862, FN=4, Flags=.pmPR..TC
34173	9	RuckusWi_35:78:cc	Apple_dd:de:a0	802.11	55	Disassociate, SN=15, FN=0, Flags=.....C
46724	1	NestLabs_4f:2a:a9	RuckusWi_35:78:cc	802.11	57	Disassociate, SN=0, FN=0, Flags=...P..F.., SSID=Broadcast

IEEE 802.11 wireless LAN management frame

Fixed parameters (2 bytes)

Reason code: Previous authentication no longer valid (0x0002)

IEEE 802.11 wireless LAN management frame

Fixed parameters (2 bytes)

Reason code: Unknown (0x0000)

Tagged parameters (2 bytes)

Tag: SSID parameter set: Broadcast

IEEE 802.11 Disassociate, Flags: .pmPR..T.

Type/Subtype: Disassociate (0x000a)

Frame Control Field: 0xa379

..11 = Version: 3

..00.. = Type: Management frame (0)

1010 = Subtype: 10

Flags: 0x79

...01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x01)

...0.. = More Fragments: This is the last fragment

...1... = Retry: Frame is being retransmitted

...1 = PWR MGT: STA will go to sleep

..1. = More Data: Data is buffered for STA at AP

..1.. = Protected flag: Data is protected

0... = Order flag: Not strictly ordered

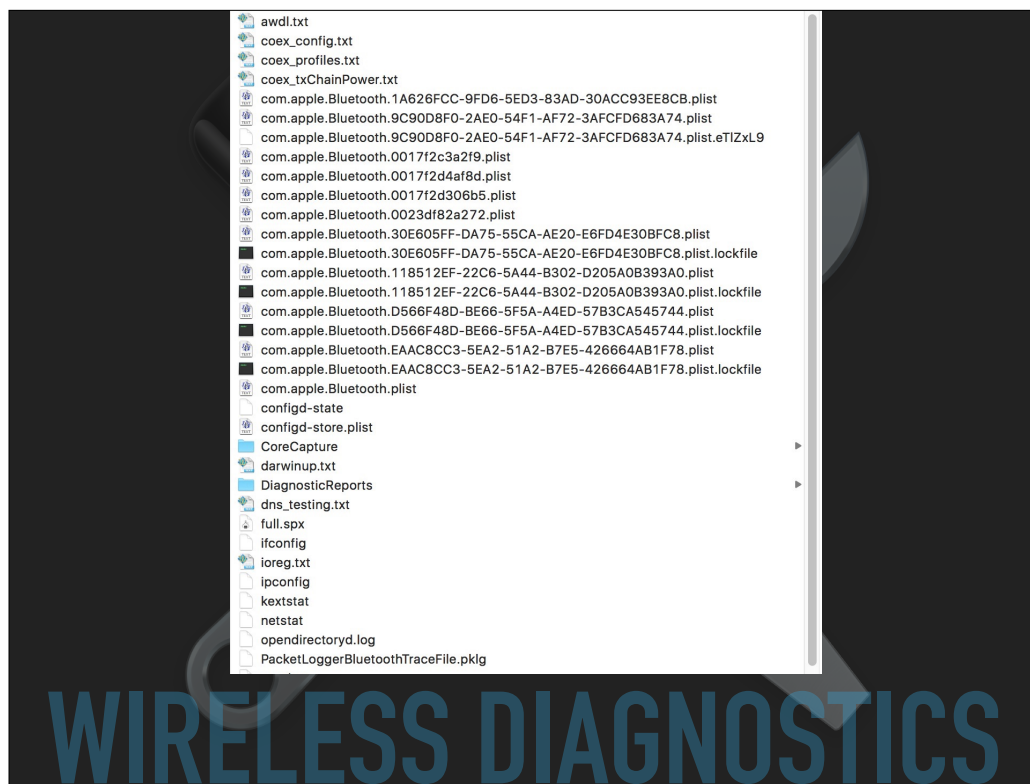
DISASSOCIATION

Sometimes, disconnects are a failure mode that you'll see in specific cases where there's something else acting as a rogue, working to act as a denial of service for your Wi-Fi. This is exactly what got Marriott hotels in trouble with the FCC in the United States. If they saw a competing wireless network, their APs could spit out Disassociation commands on behalf of the other competing APs.

It's dirty pool, but it happens.

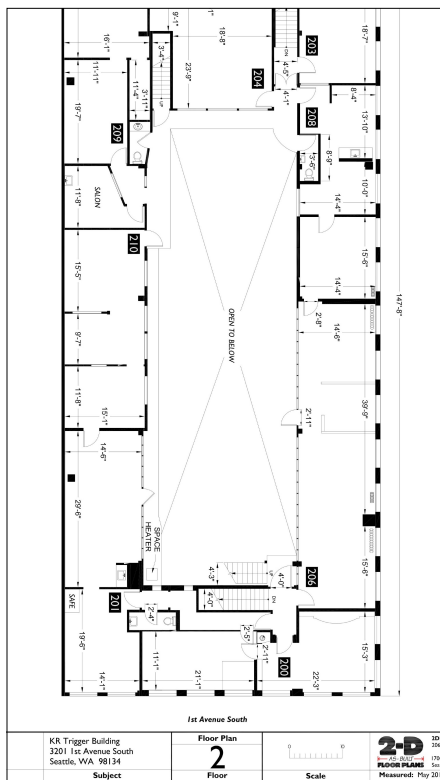


Found in `/System/Library/CoreServices/Applications`, the Wireless Diagnostics application built into every Mac will give you literally everything associated with the Wireless on the Mac side of things.



It dumps out all of the various log files, including some system level files for helping troubleshoot everything. This is a good way to get some actually useful information from a remote user without having to be where they are. While you won't need everything it grabs, it's worth it to get what it grabs in case you need something.





A WIFI TOOLKIT

TOOLS FOR PLANNING

OS X TOOLS

So, what Apple ecosystem tools are available for planning and designing Wi-Fi networks based on predictive or gathered data models?



OS X TOOLS (Yet)

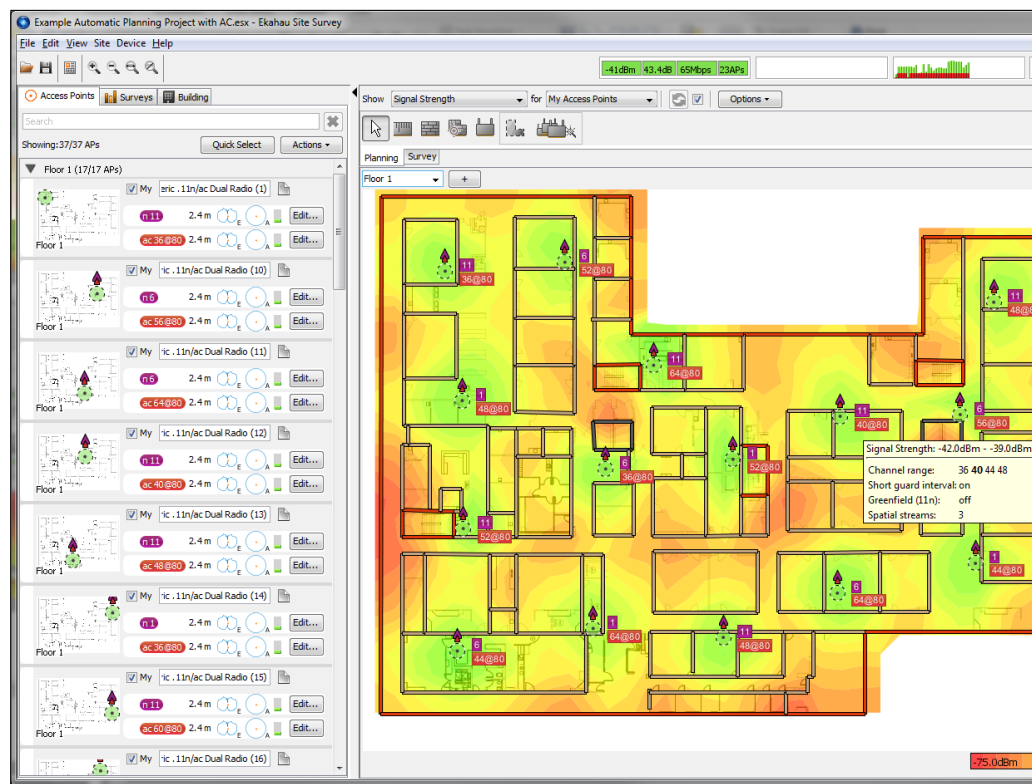
There are not currently any good tools for this directly on the Mac. Yet.



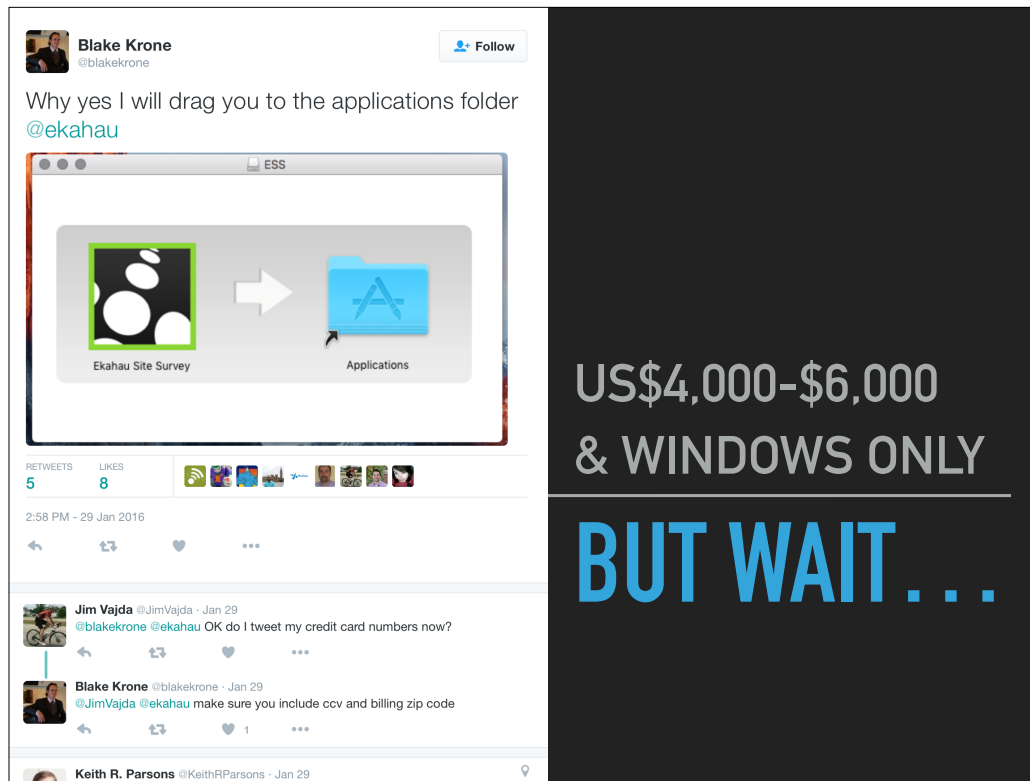
LET SOFTWARE DO THE WORK

PREDICTIVE SITE SURVEY

Predictive site survey software will take an architectural floor plan and information about your equipment and model a network for you, including recommending placement of wireless APs. Ekahau Site Survey is currently the big gun in this space, while Tamograph Site Survey is coming along rather rapidly. NetSpot has also begun to make noises regarding implementation of predictive site survey, but no public releases are available.



Ekahau Site Survey is the big gun in this market, and includes not only the predictive site survey tools, but also the ability to perform onsite measurements (active and passive surveys) as well as spectrum analyzer integration. Essentially, Ekahau Site Survey rolls the bulk of what we've seen so far into a single application. The only drawbacks are the cost of US\$4,000 to US \$6,000, and the Windows platform requirement.



Watching the WiFi engineering community, numerous posts have suggested that Ekahau site survey is coming for the Mac. Screen shots of development versions have been appearing informally for around a year at the time of this writing, and it seems that the dam might finally be breaking on the “industry standard” tools for Mac OS.

WIFI PLANNING: SITE SURVEY

Conference Room: 30' from AP

Interface Name: en0
Address: 60:03:08:a0:8f:7a
Open Wireless Diagnostics...
Disable Wi-Fi Logging

Wi-Fi: On
Turn Wi-Fi Off

✓ Seattle
Disconnect from Seattle
IP Address: 10.233.254.126
Router: 10.233.254.1
Internet: Reachable
Security: WPA2 Personal
BSSID: 20:c9:d0:1b:0b:0e
Channel: 149 (5 GHz, 40 MHz)
Country Code: US
RSSI: -66 dBm
Noise: -95 dBm
Tx Rate: 243 Mbps
PHY Mode: 802.11n
MCS Index: 14

Workroom: 15' from AP

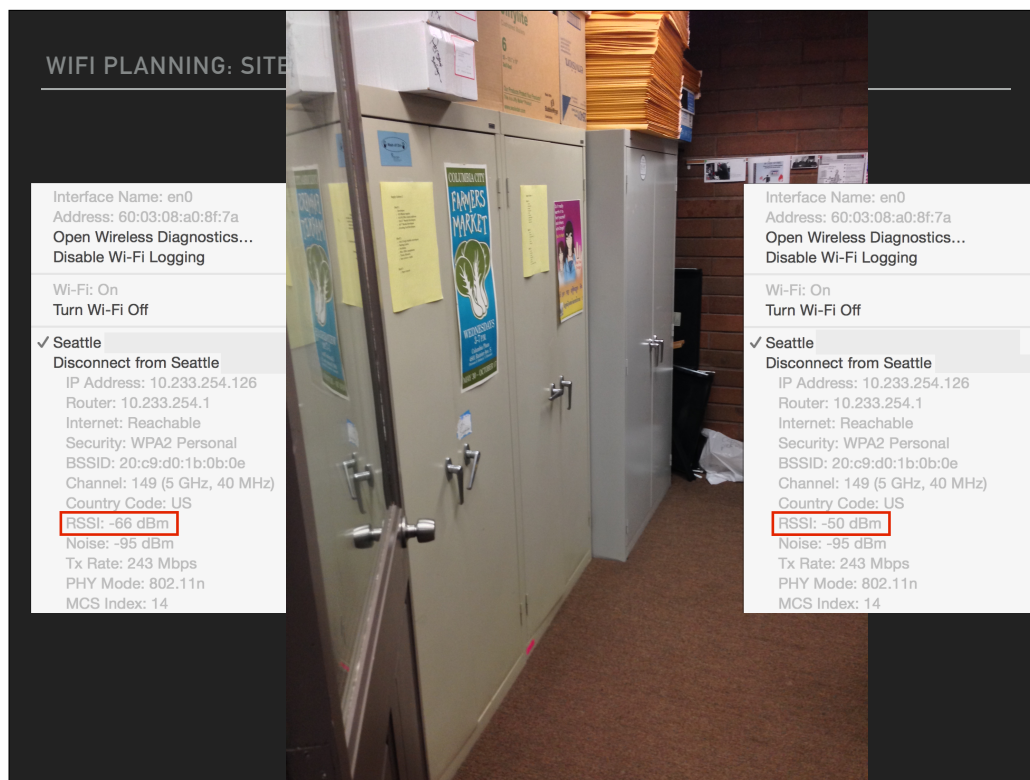
Interface Name: en0
Address: 60:03:08:a0:8f:7a
Open Wireless Diagnostics...
Disable Wi-Fi Logging

Wi-Fi: On
Turn Wi-Fi Off

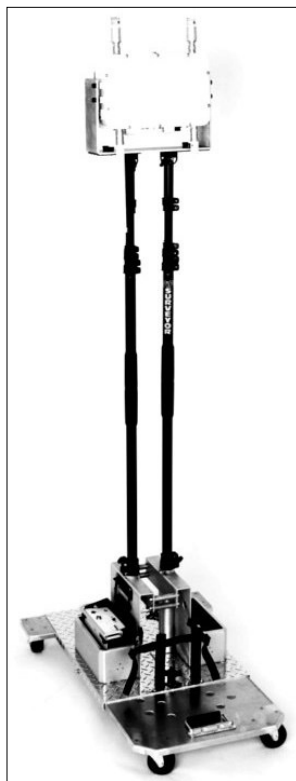
✓ Seattle
Disconnect from Seattle
IP Address: 10.233.254.126
Router: 10.233.254.1
Internet: Reachable
Security: WPA2 Personal
BSSID: 20:c9:d0:1b:0b:0e
Channel: 149 (5 GHz, 40 MHz)
Country Code: US
RSSI: -50 dBm
Noise: -95 dBm
Tx Rate: 243 Mbps
PHY Mode: 802.11n
MCS Index: 14

As attractive as it might be to have software do all the work for us, though, key information about a site does not always show up in architectural floor-plans.

Here we have two separate RSSI readings from the WiFi Menu. Moving from the customer workroom 15' (~5 meters) from the AP to the customer conference room 30' (10 meters) from the AP results in a net RSSI drop of 16 dBm. Keeping in mind that a 3 dBm drop reflects 50% signal intensity loss, dropping 16 dBm is a huge loss over a 15' distance.



This series of metal filing cabinets stands in the direct line of site between the AP and the conference room. This kind of obstacle is exceedingly unlikely to appear on an architectural floor plan, especially in a facility that has been occupied for some time. For that reason alone, relying on predictive site survey alone will be problematic, and you should still plan to evaluate sites in person as well.



EMPIRICAL
MEASUREMENT

ONSITE SURVEY

We sometimes call the onsite survey “AP on a Stick”, but this is a misnomer. AP on a Stick literally means putting an AP in place and taking measurements around it in an effort to predict coverage. It’s an older type of survey, and represents only one type of onsite survey. Over time, though, this has developed into a practice of on-site surveying that is much more extensive, using what are called “active” and “passive” site surveys, with the goals of identifying sources of signal loss that might not show up on a floor, as well as obtaining a variety of other information, such as secondary RSSI readings (second strongest AP at a given location).

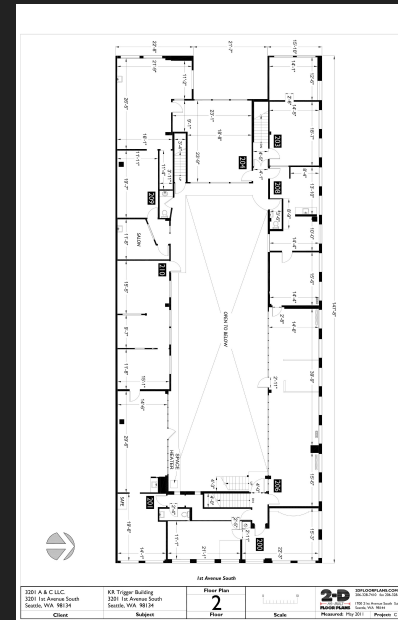
THE CONCEPTUAL TOOLSET

- ▶ Site survey information
- ▶ Documented site goals
- ▶ Understanding WiFi
- ▶ Flexibility, patience, and a willingness to learn

Beyond the software tools, you must bring a non-product toolset to bear in order to deploy WiFi successfully.

SITE SURVEY

- ▶ Facility Size
- ▶ Construction and obstacles
- ▶ Usage and key spaces
- ▶ Neighboring networks
- ▶ Existing network infrastructure



Understanding a site where a network is to be installed is critical.

CUSTOMER GOALS

- ▶ Coverage and density
- ▶ Client devices to serve
- ▶ Airtime
- ▶ Quality of Service
- ▶ Budget

Understanding customer needs is critical for building a network that works for them. The Aerohive High Density design guide is an excellent resource for this discussion.



[HTTP://CWNP.COM](http://cwnp.com)

CERTIFIED WIRELESS NETWORK PROFESSIONALS

Certified Wireless Network Professional develops and administers a series of deep technical certifications for WiFi networking. The certifications go into the deep arcana of WiFi, and attaining one or more of them will provide a deep level of technical knowledge.

VENDOR TOOLS AND RESOURCES

- ▶ Aerohive and Meraki High Density Design Guides
- ▶ Cisco Enterprise Best Practices for Apple Devices on Cisco Wireless LAN
- ▶ Just about every vendor has something, and WiFi is a standard.

Find the Cisco guide at http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-2/b_Enterprise_Best_Practices_for_Apple_Devices_on_Cisco_Wireless_LAN.pdf

Find the Meraki guide at https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/High_Density_Wi-Fi_Deployment_Guide

Find the Aerohive guide at <http://docs.aerohive.com/pdfs/Aerohive-Whitepaper-Hi-Density%20Principles.pdf>

Of these, the Aerohive guide is the oldest.

CONFERENCES AND COMMUNITY RESOURCES

- ▶ Conferences
 - ▶ CWNP: Prague and New Orleans
 - ▶ Wireless LAN Professionals Conference
- ▶ Community
 - ▶ [Andrew von Nagy](#) (Revolution WiFi)
 - ▶ Keith Parsons (WLAN Pros)
 - ▶ [Nigel Bowden](#) (WiFi Nigel)



The MacAdmins slack instance includes a number of rooms Individual rooms sprout like mushrooms, so it's worth looking for new ones on a regular basis.

[REVOLUTIONWIFI.NET](http://revolutionwif.net)

- ▶ High-density design guide
- ▶ Videos
- ▶ Capacity Planner
- ▶ SSID Overhead Calculator

Andrew von Nagy's site Revolution WiFi (revolutionwif.net) is invaluable, as Mr. von Nagy has written extensively on WiFi network design, recorded and posted a number of videos on the subject, and has even gone so far as to build planning tools to help determine network capacity requirements, including the Capacity Planner and SSID Overhead Calculator, which shows you why not to use too many SSIDs, even if your vendor makes 16 available on each AP.

**ANY SUFFICIENTLY ADVANCED
TECHNOLOGY IS
INDISTINGUISHABLE FROM MAGIC.**

Arthur C. Clarke

The larger and more sophisticated the network you're planning, the less likely you are to get it right the first time. Getting it right is hard, and is likely to require multiple passes through an environment to plan, deploy, and adjust. You'll find that as WiFi advances, both the capabilities and requirements will change, AND your wireless can do things that seem *like magic*.



But the real concern is that if you treat the magic with disrespect, you get in trouble.



But given a willingness to learn, you can develop your skills, and become a wizards *and* heroes.

THANK YOU!

Tom Bridge

tom@technolutionary.com

@tbridge

Chris Dawe

dawe@wheelwrights-llc.com

@ctdawe

<http://j.mp/macadukwifitoolkit>