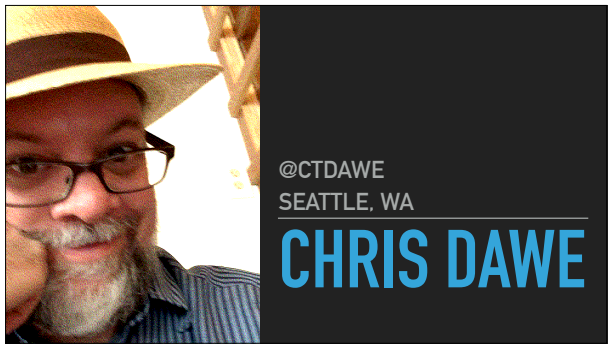
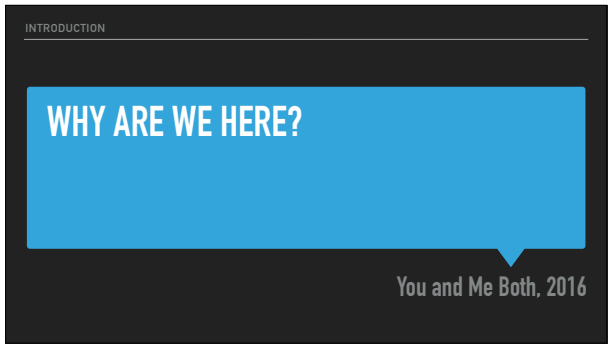

1




2

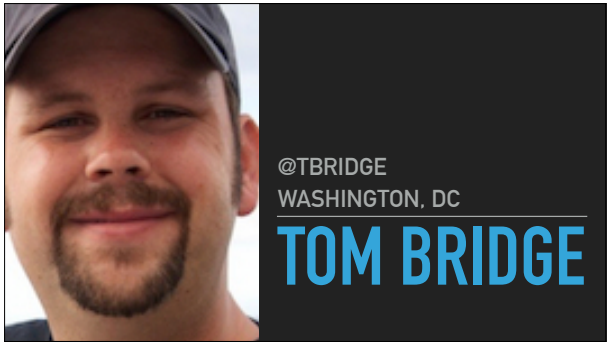
Chris Dawe is a consultant in Seattle, WA who handles Mac, iOS, and network planning, deployments and troubleshooting for small business and education, and provides planning and project management services around Apple in IT. In addition, Chris also has Thoughts about food, whiskey, and politics.




3

Show of hands: How many of y'all have users whom you have tried to convince that connecting their MacBook Pro to the Ethernet cable will give them a faster and more reliable connection? How many of you were successful in altering user behavior?

In one sense we're here because the rise of iOS and OS X mobility has transformed Wi-Fi from a "nice to have" add-on to to a necessary and critical component of our networks. We now have hundreds or thousands of devices, most of which do not connect to an Ethernet cable, and a huge number of which *cannot connect using an Ethernet cable.*




4

In another sense, we're here because of this guy.

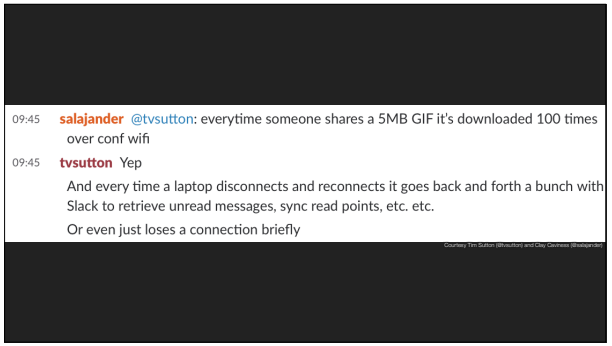
Two years ago at the Mac Admins 2014, I suggested to Tom that I was thinking about submitting a session on the fundamentals of Wi-Fi. Tom called my bluff, and six months later he dragged me kicking and screaming were submitting the proposal for what became 2015's workshop "Fundamentals of Wi-Fi". We have since distilled some of what we learned into a presentation at the MacAdUK conference in London, and re-mounted the workshop at Cascadia IT conference in Seattle. In order to re-mount the workshop in Seattle, we compressed the same material into 2/3 the time, so we also

---


5

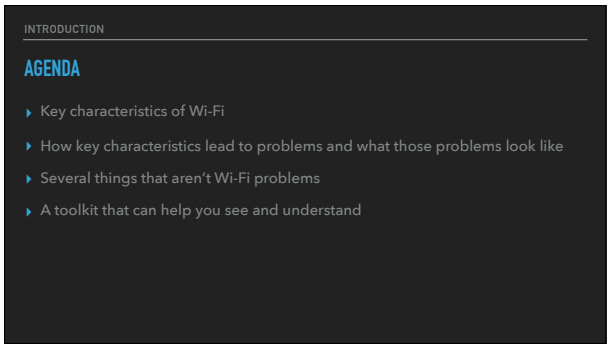
For Mac Admins 2016, I have adapted our workshop sections on troubleshooting and network design into individual but related talks, with a focus on converting the troubleshooting section into a standalone piece that backs away from some of the granular detail and focuses on fundamental principles. My goal is to introduce some of the fundamental concepts of Wi-Fi and to help non-network admins recognize some of the warning signs. Finally I hope to provide you with a toolkit to assess your Wi-Fi and understand what might go wrong.

---




6

At the very least, I hope to give you an idea of what's happening when 60 Macs and 30 iOS devices associate to a single AP and everyone starts Slacking gifs at once.



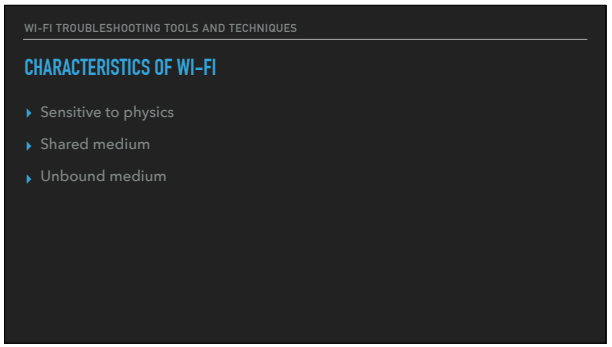

7

So we are going to talk about several things today. We're going to keep this fairly high-level due to our time constraints, and we'll try not to get into the weeds too much.

---

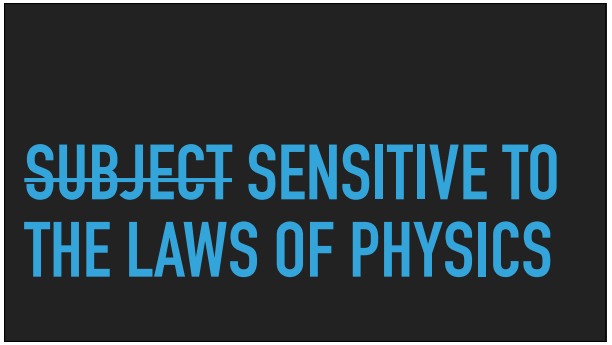

8

---




9

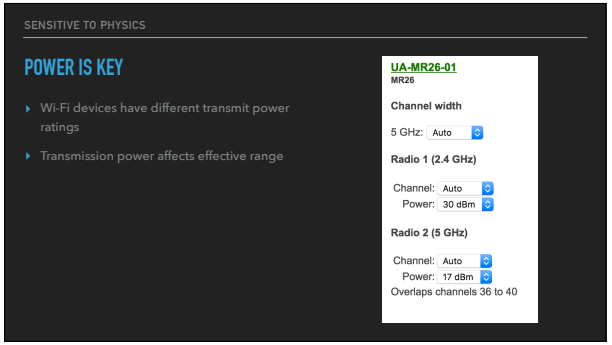
Naturally, these aren't all of the characteristics of Wi-Fi you need to know, but these are three core areas that play a major role in Wi-Fi breaking.




10

It's not as though other network technologies aren't subject to the laws of physics, but wi-fi is susceptible to their effects in far more obvious ways than, say, Ethernet.

---

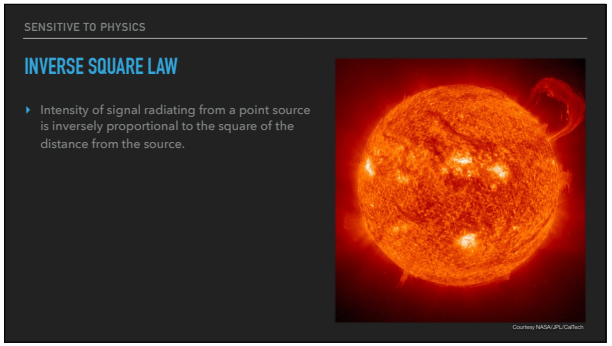



11

Transmitters convert electricity to signals. Wi-Fi transmission power is usually rated in milliwatts or decibel milliwatts (dBm). For our purposes we're going to stick with dBM because that's how Apple and most Mac-based tools report it. You can convert them back and forth, but that's beyond the scope of this talk.

Power is a key element to producing a Wi-Fi signal. Different devices (clients and access points) transmit using different levels of power, and the power rating affects the effective range of transmission.

---




12

Equally important to the discussion is the inverse square law, which describes how a signal loses intensity over distance.

If you're only a few million kilometers from he sun, it radiates at a *high* level of intensity.

SENSITIVE TO PHYSICS

## INVERSE SQUARE LAW

- In other words, the further you get from a signal source, the lower its intensity will be


13

If you move off to Mars, the amount of the sun's energy reaching you is going to be vastly lower.

---

SENSITIVE TO PHYSICS

## ATTENUATION

- Loss of signal intensity
  - Over distance
  - Through materials

14

We refer to the loss of signal intensity over distance or through materials as "attenuation". Different materials attenuate Wi-Fi signals differently.

---

SENSITIVE TO PHYSICS

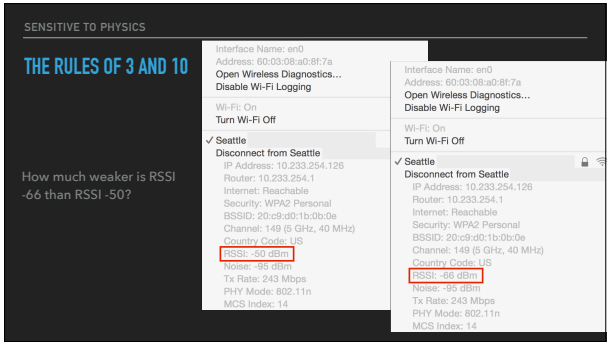
## THE RULES OF 3 AND 10

- A decrease in RSSI of 3 dBm represents a halving of signal intensity
- An increase of 3 dBM RSSI represents a doubling of signal intensity
- A 10 dBm increase represents an order of magnitude (10x) increase
- A 10 dBm decrease represents an order of magnitude decrease (1/10)

(Combine these together in calculations)

15

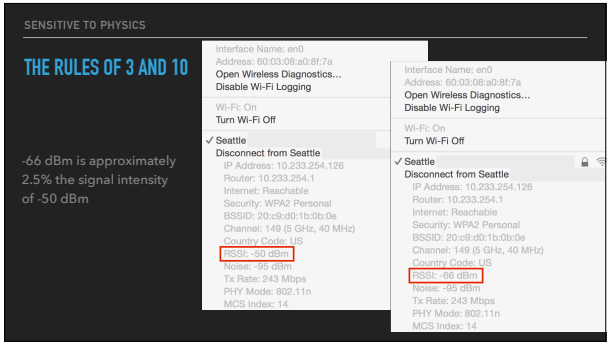
This leads us to a handy rule of thumb for calculating the increase and decrease in signal intensity.




16

Who wants to take a shot at this?

---

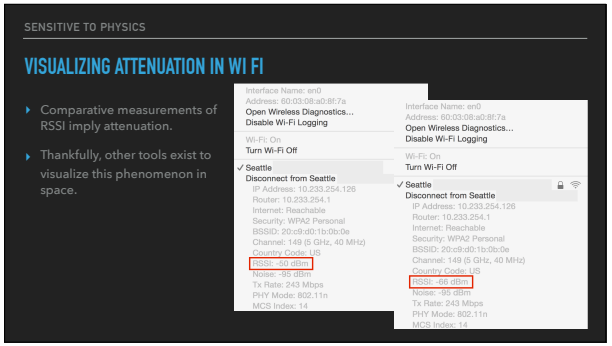



17

-66 dBm is 1/40th the signal strength of or 2.5%

On some level it's amazing that you can lose that much in the way of signal strength and have Wi-Fi even continue to work, and that is a real testament to the robustness of the design.

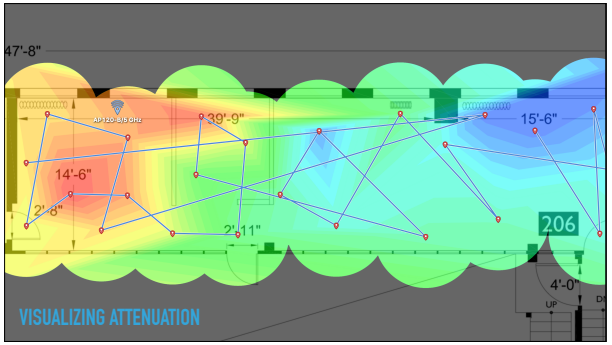
---




18

Comparative measurements of RSSI in the Wi-Fi menu demonstrate the loss of intensity and imply attenuation.

That's great to know anecdotally, but is there has to be a better way to document this for my facility.




19

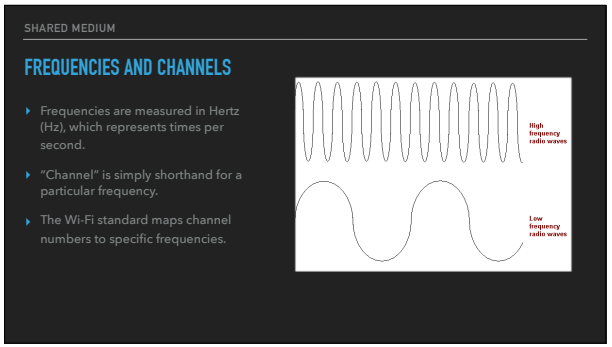
For example, you could use a heat mapper to run a passive site survey in which you walk through a facility and take signal readings you assign to a location on a floor plan. The heat mapper can then interpret the information you recorded and produce a visual display of your signal or signal to noise levels. In this heat map, NetSpot Pro represents the stronger signals as warmer colors, and weaker signals as cooler colors.

---


20

The second key characteristic of Wi-Fi is its use of a shared medium.

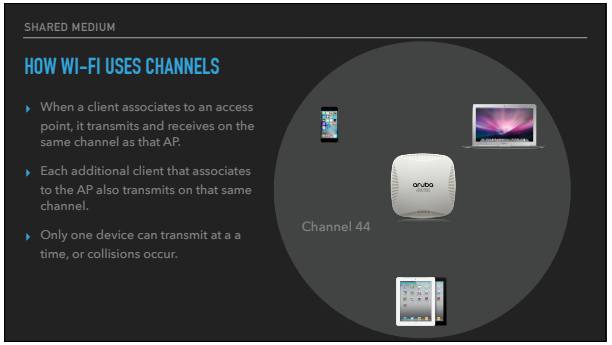
---




21

Wi-Fi uses radios that broadcast into the air using different frequencies. Frequencies are measured in Hertz, which is a unit describing how many times something happens per second. For our purposes “channel” is shorthand for an agreed-upon frequency.

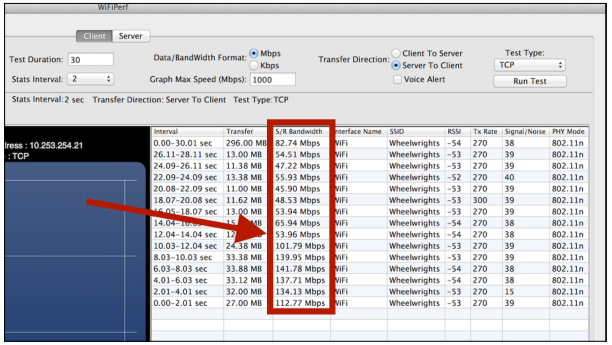
Many technical documents (such as FCC compliance and testing documentation) utilize direct references to frequency bands instead of using channels, so for the purposes of our discussion, a channel is a shorthand way to refer to an agreed-upon frequency, but you will ultimately need to become familiar with the frequencies themselves.




22

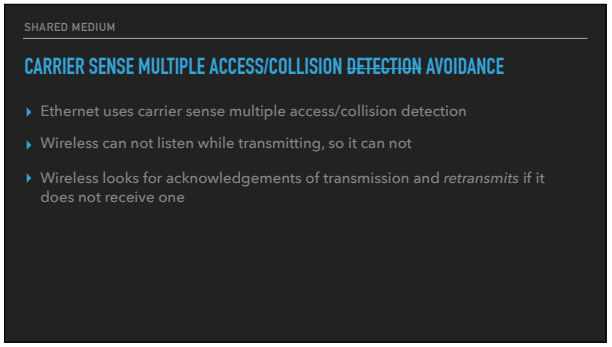
A Wi-Fi access point is configured to transmit and receive on a particular channel. When a Wi-Fi device associates to an access point (usually referred to as a BSSID), it configures its wireless interface to transmit and receive on the same channel (frequency) as the access point. Each additional client that associates to the access point also begins using that channel.

So let's pretend you and a friend are talking, you both get excited about something, and you start talking over one another, then have to stop and repeat yourself. Now imagine this at a bar table with 10 people. This is a key point.: in a shared medium such as radio, only one device can transmit at a




23

The practical implication is that as more devices transmit on a channel, the performance *per-client* falls because every client has to wait their turn. In this illustration, I was running an iPerf TCP performance test between two systems, and then added a second pair of systems running an iPerf test. The illustration shows the sudden drop in TCP throughput on the first client as the second client begins testing.

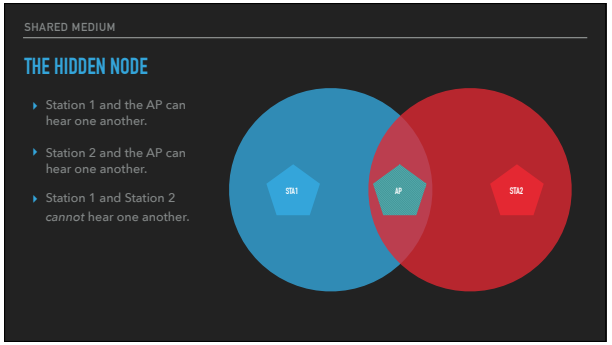



24

In wired Ethernet nodes listen while they transmit, and if they detect a collision they cease transmission immediately. They back off for a random amount of time and then try again.

Wireless is unable to listen while transmitting, so it instead depends on avoidance of simultaneous transmission; listen for quiet, then send.

Because wireless is unable to listen while transmitting, a transmitter also waits for an acknowledgement that a frame has been received by the AP; if it does not receive one, it retransmits. This is where our troubles begin.

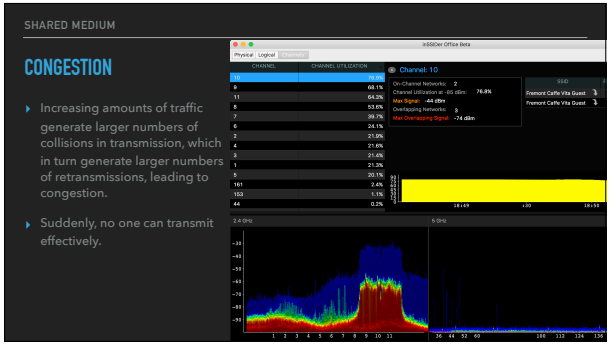



25

Up until now we've assumed that everyone can hear everyone else. And that leads to what may be one of the biggest problems in Wi-Fi: the hidden node problem. Remember that I said that clients wait for quiet, and then transmit. To illustrate the problem, look at the diagram above.

Station 1 is associated to an AP.
Station 2 is associated to an AP.
Station 1 can transmit to and receive from the AP.
Station 2 can transmit to and receive from the AP.
Station 1 and Station 2 do not have powerful enough radios or sensitive

---




26

The screen shot from my neighborhood coffee shop in Seattle shows network utilization sustained at approximately 75%. At that level of utilization, multiple clients associated with the network on channel 10 are likely sending a large amount of data, and may be suffering from proximity to other networks, which in turn causes collisions, forces retransmits, causing the utilization to go up.

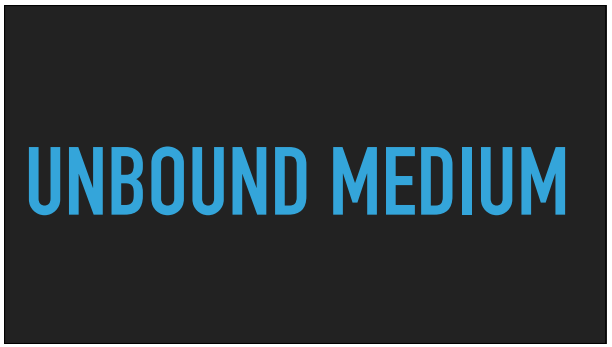
Suddenly, no one can transmit effectively.

---


27

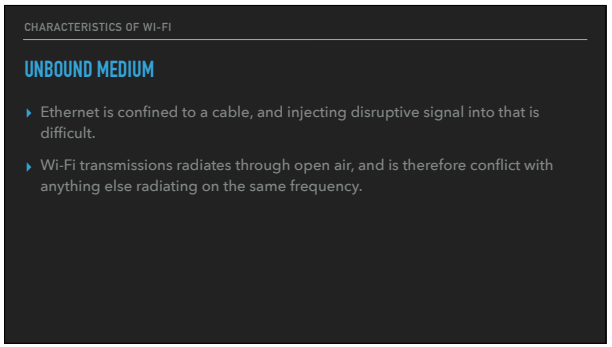
This problem can be bad in well-designed network with lots of clients trying to send to and receive from a single access point. The problem grows worse when you have multiple access points and their clients on the same channel that are within transmission/receiving range of one another; it gets worse still if you have multiple networks whose channel assignments overlap your network without being on the same channel.

In either case the transmits and retransmits start to multiply as the various access points also fall victim to the need to transmit and then retransmit to compensate for the collisions caused by several APs in range of one another



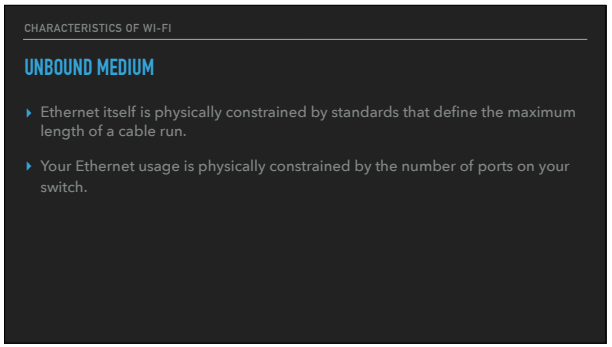

28

The third key characteristic of Wi-Fi that causes problems is that Wi-Fi uses an unbound medium.



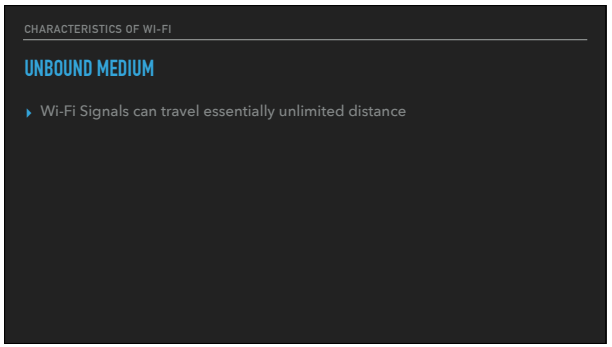

29

That Wi-Fi transmits through the air means that Wi-Fi is subject to interference from other sources transmitting through the air.




30

In addition, Ethernet cable is significantly more constrained. “If your cable run is longer than 100 meters, well that’s just too bad.”




31

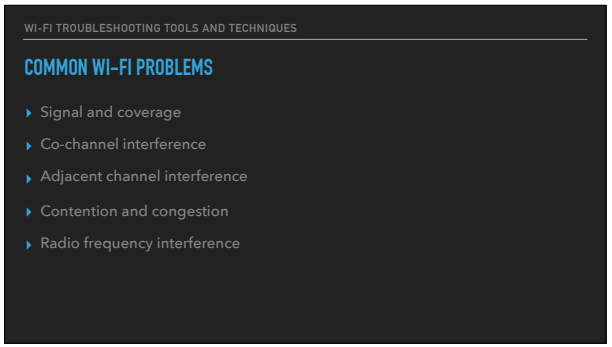
Remember that the inverse square law dictates that the further a signal radiates from its source, the weaker it gets.

---


32

These three characteristics of Wi-Fi lead to its most common problems and failures.

---




33

We’re going to talk about 5 of the more common problems.

# SIGNAL AND COVERAGE

34

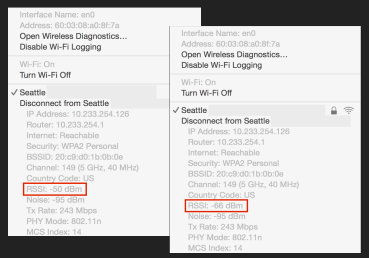
Signal and coverage are our most basic.

---

SIGNAL LEVELS AND COVERAGE

## LOW SIGNAL

- Compare RSSI reported in the Wi-Fi menu item to observe different signal strengths




35

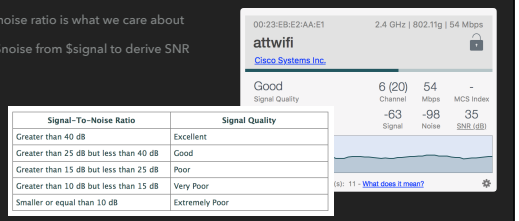
Again we'll just perform a quick comparison of RSSI to see that one signal is significantly weaker than other signals.

---

SIGNAL LEVELS AND COVERAGE

## THE IMPORTANCE OF THE SIGNAL TO NOISE RATIO

- Signal to noise ratio is what we care about
- Subtract $noise from $signal to derive SNR

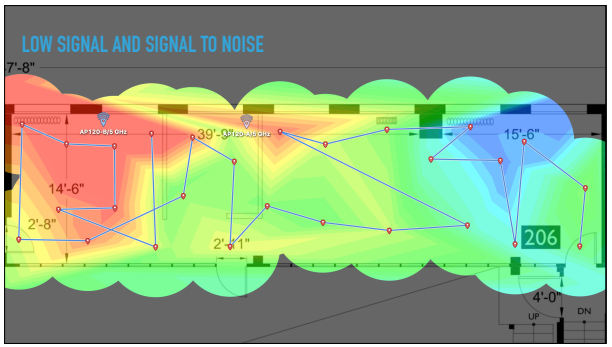



| Signal-To-Noise Ratio | Signal Quality |
|---|---|
| Greater than 40 dB | Excellent |
| Greater than 25 dB but less than 40 dB | Good |
| Greater than 15 dB but less than 25 dB | Poor |
| Greater than 10 dB but less than 15 dB | Very Poor |
| Smaller or equal than 10 dB | Extremely Poor |

36

Signal to noise is a way of describing how much stronger than background radio noise your signal is. The stronger the signal is in comparison, the better the quality of your connection. A variety of applications include documentation interpreting these values.

In short, a client that moves further away from its associated AP will suffer a decline in signal strength, which in turn reduces its signal to noise ratio, which causes the client's transmit rate to fall, eventually resulting in an inability to transmit and receive.




37

And looking at our heat map again, notice that on the far right there is an area that is very blue. This is an area of low signal to noise in my Seattle office.

---


38

A particularly frustrating example of this became more common with the rise in mobile devices. To understand it, let's first look at a functional connection.

1. An access point continually announces its presence using what are called beacon frames.
2. A client associated to the access point has something to transmit, and asks if the AP is available to receive the transmission.

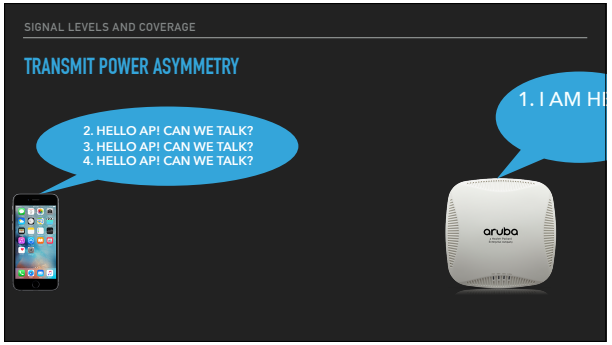
15 dBm phone versus 18 dBM access point

---


39

3. The access point gives an "all clear" (known as "Clear to Send")
4. The client device receives the "Clear to Send" and begins transmitting.

15 dBm phone versus 18 dBM access point




40

So you leave your home or your office and walk out into the driveway or parking lot or out onto the street. You pull your phone out to look for directions to your dinner restaurant and see that the phone still shows signal. You go to load the review site of your choice, and the app won't connect even though you still have the happy Wi-Fi bars displayed at the top of your screen. WHY?

The answer may lie in the fact that your phone can only transmit at 15 dBm, while your AP id transmitting at, say, 18 dBM. Once I'm out on the street, my phone can still hear the AP well enough to report that it is there, but the AP


41

The second common problem are lies in what's called "Co-channel Interference"


42

As I discussed previously, access points using the same channel that are able to hear one another will generate a larger number of transmission collisions, backoffs, and retransmissions. They can't stop won't stop.


43

Imagine co-channel interference like this. In this diagram…

1. Both APs are going to hear transmissions from the another, and all of the devices in range of each.
2. Client devices in range of both APs (such as the iPhone at the top) are going to hear all the transmissions from both APs and be forced to take them into account when deciding when to transmit.

---

# ADJACENT CHANNEL INTERFERENCE

44

The third and slightly different problem is adjacent channel interference.

---


45

Looking again at the channel image of our the “hamstring” network, not only do you see the four “hamstring” access points sitting on top of one another causing co-channel interference, you also see several other APs sitting on channel four whose signal each overlap “hamstring”.

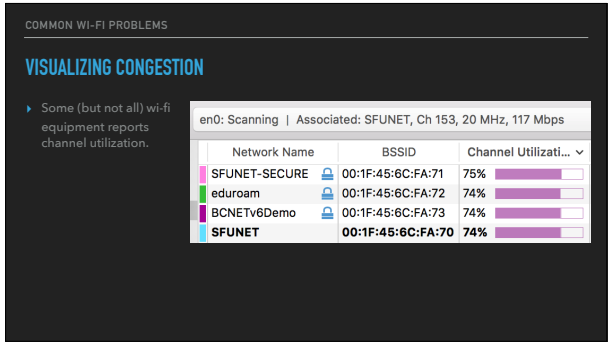
When these networks transmit, they are also going to cause collisions and retransmits, but because they are not on the same channel as “hamstring”, they do not get the benefits of using request to send/clear to send in order to try to manage the collisions.

# CONTENTION AND CONGESTION

46

Any of these phenomena are going to generate contention in which clients compete for resources to transmit, and congestion in which multiple clients suffer from reduced performance. There are a number of ways to identify this.

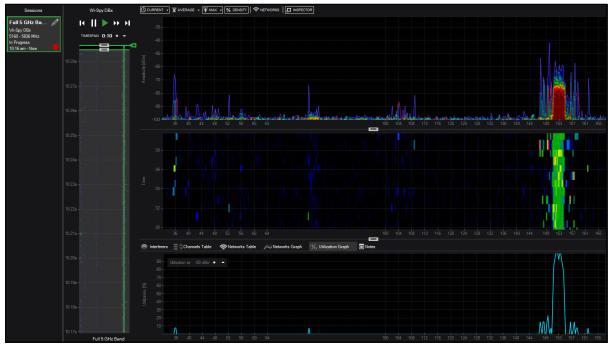
---




47

Some–but not all–access points can be configured to report utilization information about themselves. Wi-Fi Explorer can display channel utilization that the APs report. Keep in mind that this utilization is from the *access point's* perspective.

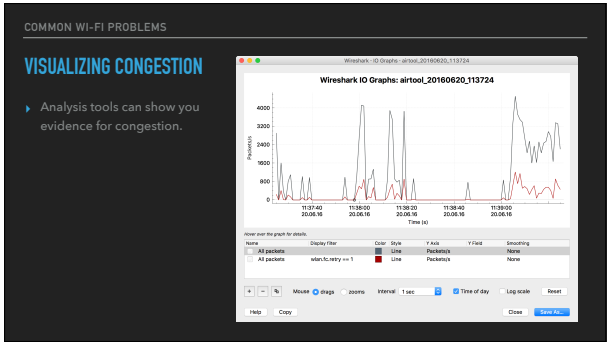
---



48

A spectrum analyzer attached to a computer can sample and report on the radio spectrum utilization as viewed from the computer's location. This is a screen shot from Metageek's Chanalyzer Pro. It's display is divided into several sections.

1. At the bottom we see a live utilization graph that shows how heavily the radio spectrum is being used on a channel-by-channel basis.
2. At the top we see a visual representation of the density of the network's utilization for a given sample period. Red represents the heaviest utilization, blue the lightest, and there is a range of colors in between.




49

A third way to visualize contention/congestion is a packet analysis tool. You can capture network traffic and search and categorize it.

In this example, I captured a quarter million frames at MacDevOps Vancouver and used WireShark to creat an I/O graph that displays all packets. I then added a filter that displays retransmits on the same graph. A quick look shows that at one point roughly 1100-1200 frames out of roughly 4500-4600 were retransmits, meaning that in some places 25% of the traffic was traffic that couldn't get through the first time so it had to be re-sent.

---


50

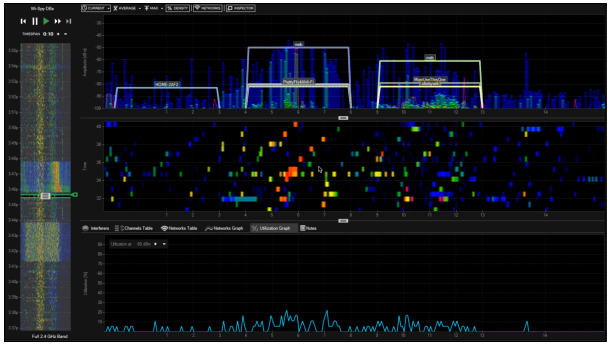
For our final problem, we arrive at Radio Frequency Interference.

---


51

Pretend you're sitting at a coffee shop having a conversation with a friend and half the local fire department goes by with sirens screaming. You can't hear one another or even hear yourselves think, right? In other words, RF Interference is anything that modifies or disrupts a signal as it travels.

You know this exists in the Wi-Fi world because people tells you it exists, but let me show you an example so you can see what it looks like.



52

This capture is from a residential network belonging to a colleague in Seattle. At bottom you'll see live rendering of the utilization of the 2.4 GHz frequency band, at the top a density readout describing percentage utilization over a 10 second window. In the middle is the second-by-second waterfall visualization of the utilization density. Pay special attention to the bottom and top as the video plays.

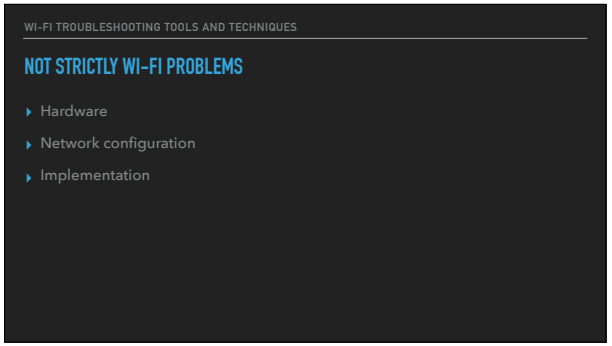
You can see the utilization spike all across the 2.4 GHz band, and both the pattern of the new signal and the way that the display expands beyond the outlines of the networks strongly suggests that whatever is generating this

---


53

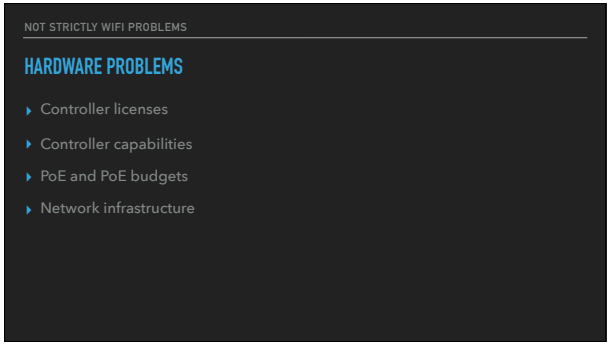
Now that you've seen a series of Wi-Fi-specific problems, I want to talk about a few things that are *not* Wi-Fi problems but often present as Wi-Fi problems.

---




54

Hardware
Network configuration
Implementation problems

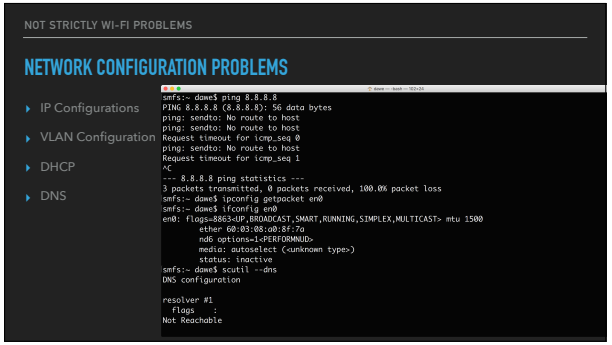



55

Understanding Wi-Fi hardware can be complicated. Some vendors require hardware controllers, some use cloud-based controllers, and some use no controller at all. The role of the controller changes from vendor to vendor.

Your controller might not be able to support all 12 of your access points because you have only licensed it for 8.
Your controller may not have the horsepower to manage all of the APs or manage all of the traffic passing through it, or you may see performance degradation as your AP count or network traffic load begins to approach a vendor's stated maximums.

---

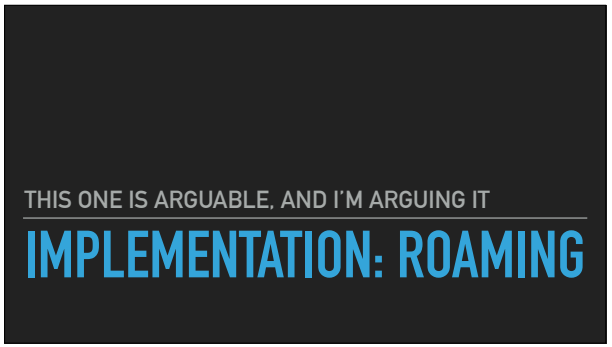



56

Your IP configuration or your DNS configuration may be set up incorrectly.
Your VLAN configuration may be such that your Wi-Fi traffic routes incorrectly, or your DNS lookups fail to resolve correctly.
Your DHCP server's lease scope may be too small to handle the number of clients on the network.
Your DHCP server lease time may be too long, and clients are leaving the network without releasing the lease.

Some of these problems may present oddly. I dealt with an issue where a macOS client was failing to join a network and then reporting an incorrect

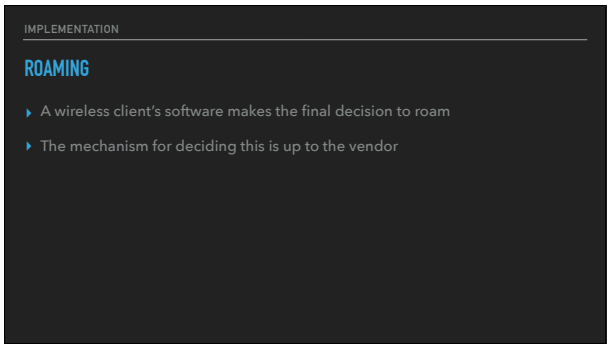
---




57

Beyond configuration issues, we also have implementation issues.

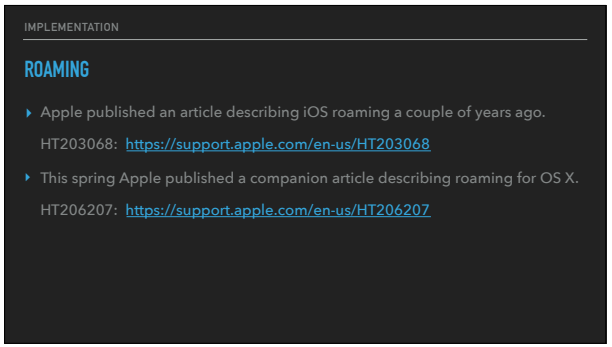
I'm going to argue that roaming and "sticky client" issues reflect vendor implementation problems and lack of administrator understanding of vendor implementations than they reflect a problem with Wi-Fi itself.




58

In principle, roaming happens when a client's signal to the associated access point (BSSID) degrades to the point where it decides to look for a new access point. Note that this is generally going to be the client's decision, and that the criteria to do this is up to the vendor.

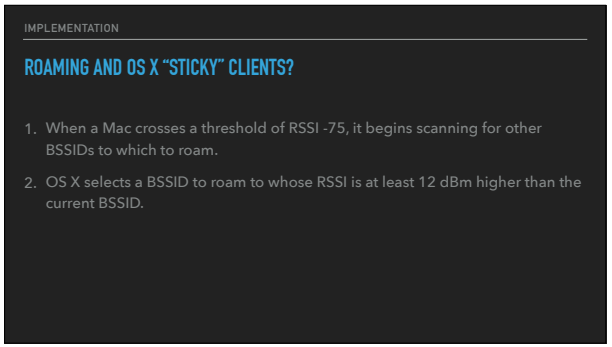
---




59

1. When a Mac crosses a threshold of RSSI -75, it begins scanning for a roam candidate.
    A. OS X will prefer a 5 GHz connection to a 2.4 GHz connect, *so long as the RSSI is -68 or greater.*
    B. OS X prefers 802.11ac to 802.11n or 802.11a
    C. OS X prefers 802.11n to 802.11a
    D. OS X prefers 80 MHz channels over 40 MHz channels and 20 MHz channels
    E. OS X prefers 40 MHz channels over 20 MHz channels
2. OS X selects and roams to a BSSID to roam to whose RSSI is 12 dBm

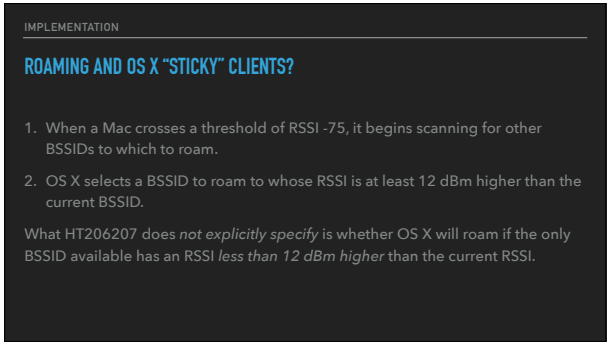
---




60

So I asked Apple about this, and Apple confirmed for me that if the next strongest BSSID does not provide RSSI 12 dBM or more higher than the existing, OS X *will not roam.*

We're going to touch on this a lot more when we talk about design in the next section, but in essence, Apple telling us this allows us to game out when OS X will roam and when it will not. I just learned this in the last week, so I still have some thinking to do about it.




61

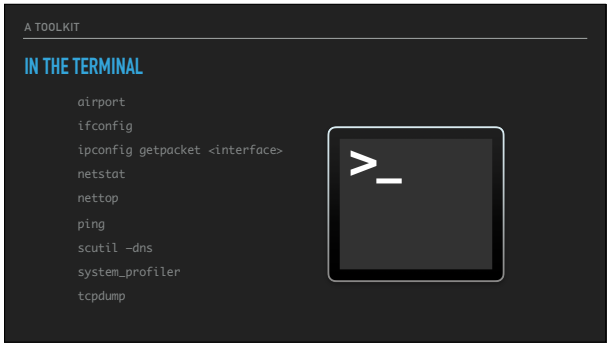
So I asked Apple about this, and Apple confirmed for me that if the next strongest BSSID does not provide RSSI 12 dBM or more higher than the existing, OS X *will not roam.*

We're going to touch on this a lot more when we talk about design in the next section, but in essence, Apple telling us this allows us to game out when OS X will roam and when it will not. I just learned this in the last week, so I still have some thinking to do about it.

---


62

---




63

`airport` is a hidden tool that will display information about the Wi-Fi interface on a machine, allows enabling and disabling logging of certain events, and will scan for networks available to the machine.

`ifconfig` shows network interface configurations

`ipconfig getpacket <interface>` shows the information received in the DHCP lease on the relevant interface

`netstat` shows network information in a number of different ways

`nettop` shows live information about network connection

`ping` queries a host to see if it responds


64

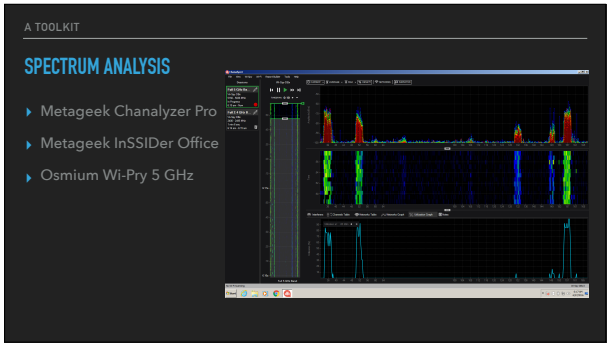
Wi-Fi Explorer
Wi-Fi Signal
`airport -> /System/Library/PrivateFrameworks/Apple80211.framework/Versions/Current/Resources/airport`
NetSpot Discovery Mode
InSSIDer Office

---


65

NetSpot Pro is the only Mac-native tool at the moment
Tamograph Site Survey Pro
Ekahau Site Survey Pro
Netscout Airmagnet

---




66

Metageek Chanalyzer Pro
Metageek InSSIDer Office
Oscium WiPry 5 GHz


67

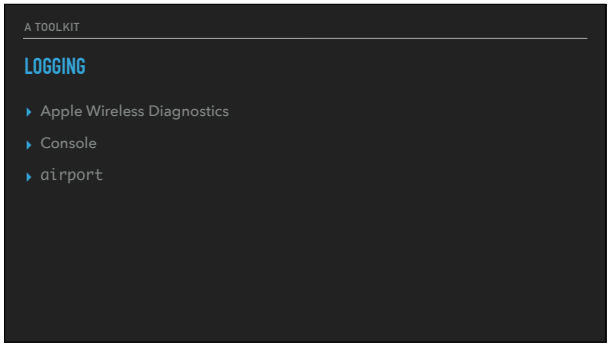
AirTool
WireShark
CloudShark
Others

---


68

WireShark
Metageek Eye P.A.

---




69

airport CLI
Console
Wireless Diagnostics

WE'LL DO IT LIVE!

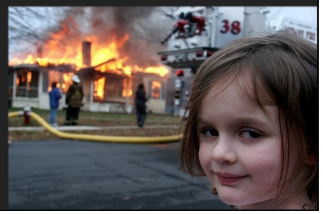
# DEMOS

70



## DEMOS

- Explore with WiFi Explorer and WiFi Signal
- Review a NetSpot heat map
- Demonstrate radio frequency interference using Metageek's Chanalyzer and Wi-Spy
- Stomp on the network and view spectrum while the world burns



71

# THANK YOU. QUESTIONS?

72

HTTPS://BIT.LY/PSUMAC2016-90

# FEEDBACK URL