ars technica CONDÉ NAST

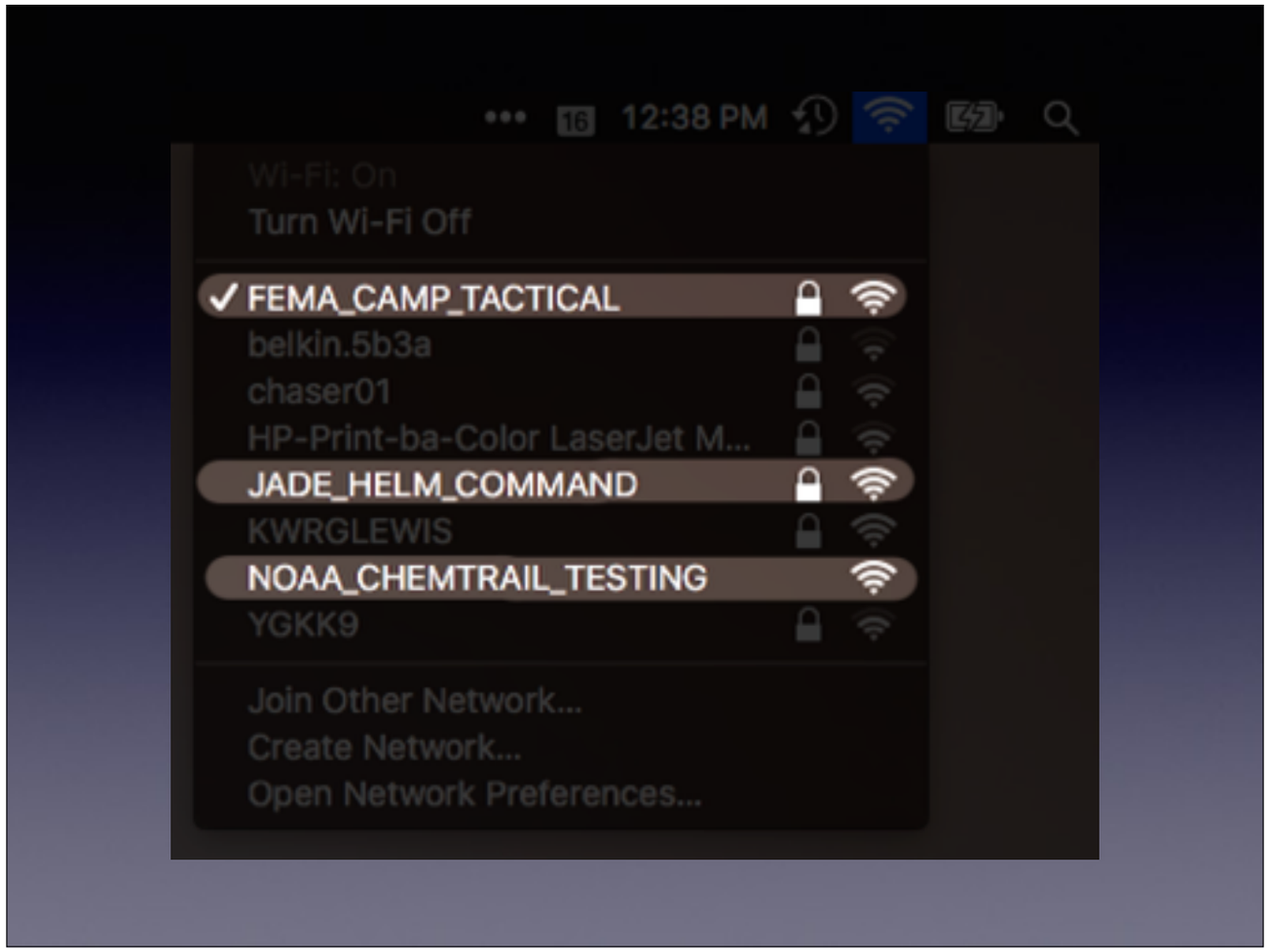
Stupid Wi-Fi Tricks

Lee Hutchinson
Senior Technology Editor

@Lee_Ars
lee.hutchinson@arstechnica.com

Late last year I made a change to my wifi at home. i'd been using an apple airport extreme forever, like most of you guys probably are. it's a fast and solid choice—maybe a little expensive—but it's got a great feature set and it's easy to use. But I'd been thinking about how businesses use wifi in corporate buildings and campuses, and I wanted to switch to something more like that—something with multiple access points that let me seamlessly roam around inside and outside the house. some of the change was driven by my wife, who likes to work out in the garden and stream music—and outside she has to use cellular data, which adds up quick.

I ended up going with three enterprise-grade access points from a company called Ubiquiti. These particular APs all link together via wired ethernet and there's a separate controller you have to run on a dedicated server, but it let me blanket both the inside and outside of my house with great coverage and also let me do some really cool extra management features. For example, if you come over to my house and pull out your laptop or phone, you'll see three SSIDs available:



I like to keep my neighbors on their toes! So I'm broadcasting three SSIDs, and one of them is open. NOAA Chemtrail Testing! That sounds like a great networkt to join. Doesn't look like it requires a password—let's join it.

Again….I like to keep my neighbors on their toes.
SOUNDS SCARY! But obviously, this isn't real—this is a dumb little captive portal page I created. Fun fact, 21 USC section 643 actually deals with business registration names in the meat packing industry. My guest network has a simple password on it, and all you'd need to do—once you were done freaking out, and it's so awesome to watch people run into this for the first time—is put the guess password name into the little code box and hit submit and boom, you're on the guest network. This is just a regular captive portal page, exactly like you'd see at an airport or a hotel—it's just customized some.

Fun things YOU can do

- Quick hits
  Tell Comcast to take a hike!
  Change your admin password!
  Set up a guest network!
  Check your channels!
  Do a site survey!
- More complicated
  Extend your network!
  Create timed access!
  Install custom firmware!
- Crazy stuff you can blow a weekend on if you're just really bored and/or nuts
  802.11X!
  Segregate your network with SSIDs and VLANs!
  Custom guest portal!
  Move DNS & DHCP off-box if you're feeling masochistic!
  *BONUS ROUND: Migrate to IPv6 if you **really** hate yourself!*

You might not want to put in the work to get a whole separate captive portal set up for yourself, but there's a bunch of stuff you can do beyond basic configuration. Most folks pull the router out of the box, turn it on, connect to it, and leave it alone forever. But that's not you guys! You guys are tinkerers and you like fiddling all the knobs—which is why you're here, after all. So we're going to touch on three sort of levels of tweaks and changes to make for your home wifi-router setup, ranging from quick and easy to … not so quick and easy. Now, real quick, I'm not going to walk through detailed setup steps—for one, we'd be here all day, and for two, there are too many variations of how everybody might be set up. But this ought to be enough to get you started on some google trips—everything here is easily googlable and doable at home…with the possible exception of the full IPv6 setup because nobody really understands how it works anyway.

One assumption
before we start…

**You MUST BE
using WPA2!**

One quick thing we're just going to assume right off the bat is that you're using encryption on your home network. If you're not….SHAME ON YOU. SHAME!
The most common objection I've heard to not turning on encryption is that a person might not care that their network is open—maybe you feel neighborly, providing wifi for anyone who walks by! maybe it's just a hassle!

Your internet connection is your responsibility. Leaving your wifi unsecured is way the hell worse than leaving your front door unlocked—if someone breaks into your house and steals your stuff, you might at least be able to file an insurance claim. If someone jumps on your wifi—maybe from a house or two away—and decides to use your connection to pirate software or download child porn or anything else illegal, that's easily tied back to YOU. Your house, your network, your IP address….your culpability. Whether or not you believe that information should be free and keeping open wifi is a philosophical or moral thing to do, the dangers are just TOO great. Secure your network.

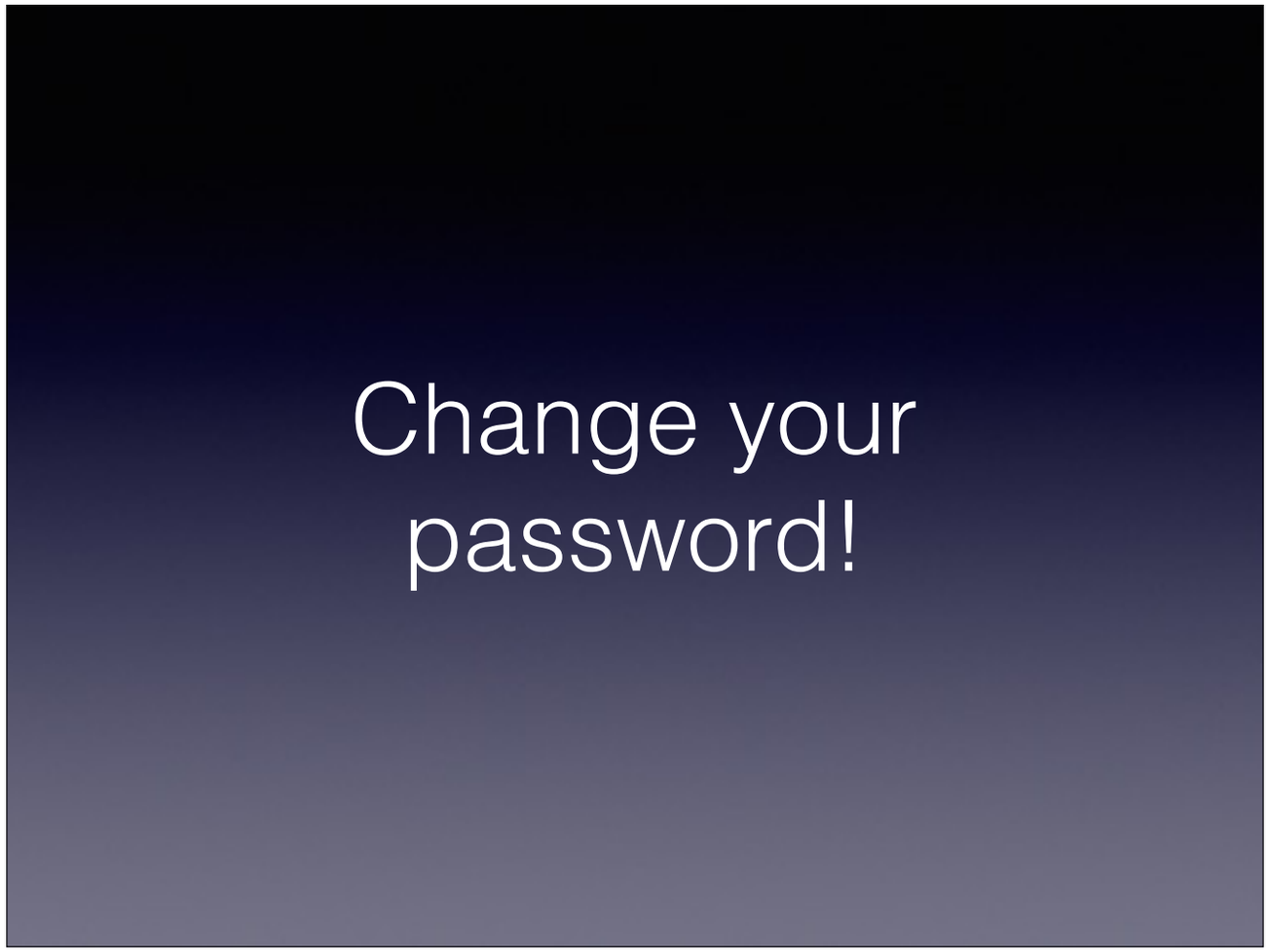
Quick hits

A few easy things to do with your existing setup to maybe make your Wi-Fi a little better

So first, the easy stuff!!

If you’re a comcast xfinity customer, you probably recently had them replace your old router with a new one with this "Xfinity Wi-Fi" thing on it. This is Comcast’s attempt at creating a widespread convenient wifi network for all its customers to use. On the up side, if you’re an xfinity customer, you can log into any Xfinity Wi-Fi device anywhere with your comcast login credentials and access the internet. On the downside, that’s anyone in the universe with comcast credentials logging into YOUR network.

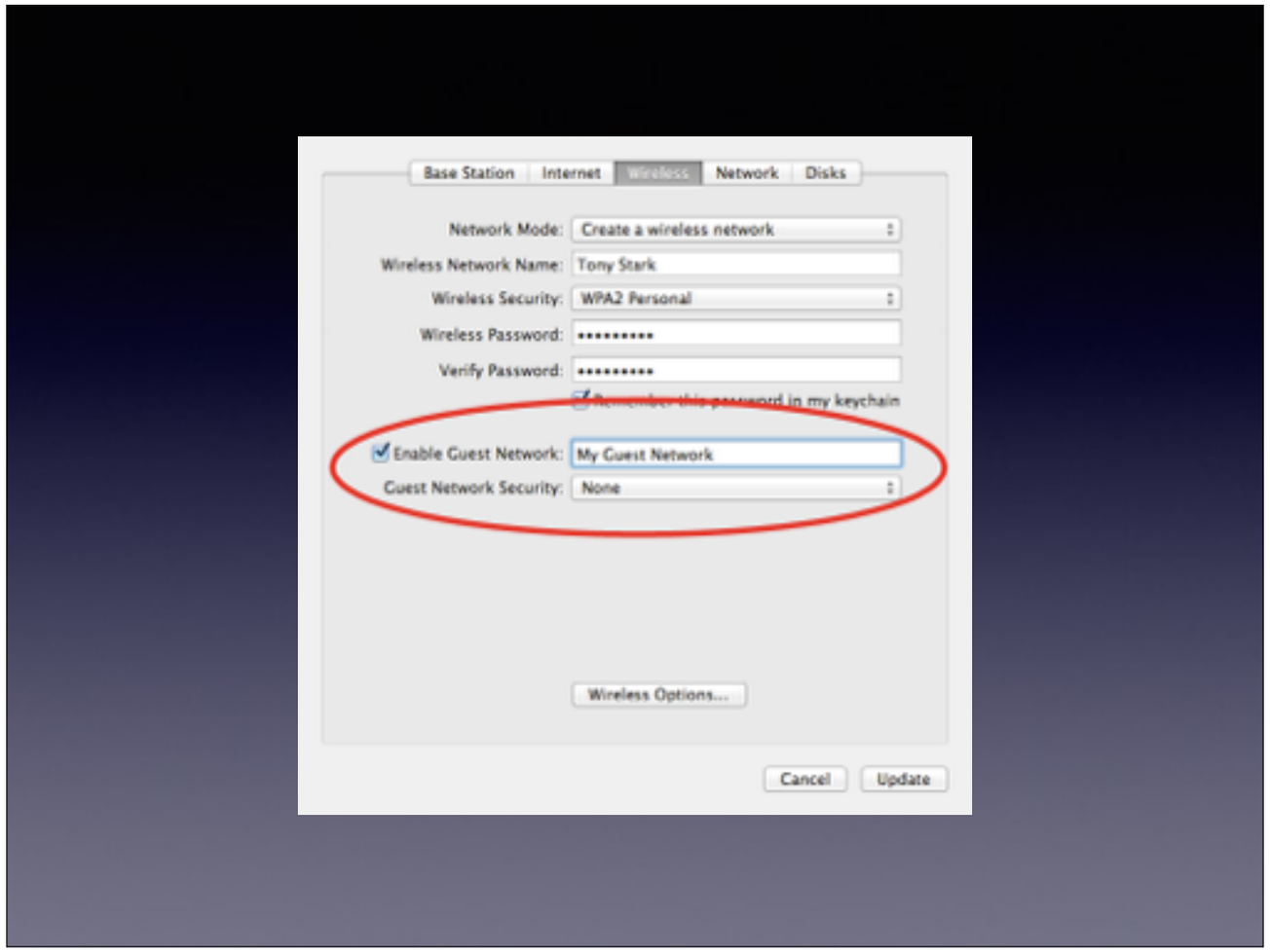
Now, comcast SAYS that they’ve taken the proper precautions with this and guest traffic is segregated from your network, and bandwidth used by guests doesn’t count against your cap or your bandwidth. Comcast SAYS a lot of things. Do you trust them? I sure as hell don’t. Buy your own router/wifi access point and tell Comcast to go get stuffed. You don’t have to help prop up their "free" wifi with your equipment. (This is optional—if you think xfinity wifi is handy and you use it, then keep doing so! but i trust comcast about as far as I can throw their corporate office building, and folks, that ain’t very far. buyer beware.)



Now, this is separate from your SSID password—I'm talking about the admin password on the actual router or wifi access point. If you're using an Apple Airport, you would have had to do this in the first place to log in, but if you're using a different combo wifi router—say a netgear, or linksys, or d-link, or whomever—and you've never logged into it, then your password is "linksys" or "admin" or whatever it was set to in the factory. NOT changing this potentially leaves you open for anyone on your network to do nefarious things—change your router's settings, knock you offline, connect to anything attached to your router like a printer or a shared disk, or any number of other bad things. Always change your admin password!

Set up your OWN guest network!

Your access point—be it an apple airport extreme or something else—almost certainly has guest network functionality. This means instead of having to give out your wifi encryption password to friends and neighbors who want to come over and use your stuff—which ALSO by default puts them on your private internal network where they can, if they want to and if you don't have controls in place, browse around and screw with your private stuff—INSTEAD of that, turn on your wifi guest network. That lets friends connect to the internet on your wifi, but keeps them separate from your internal network!



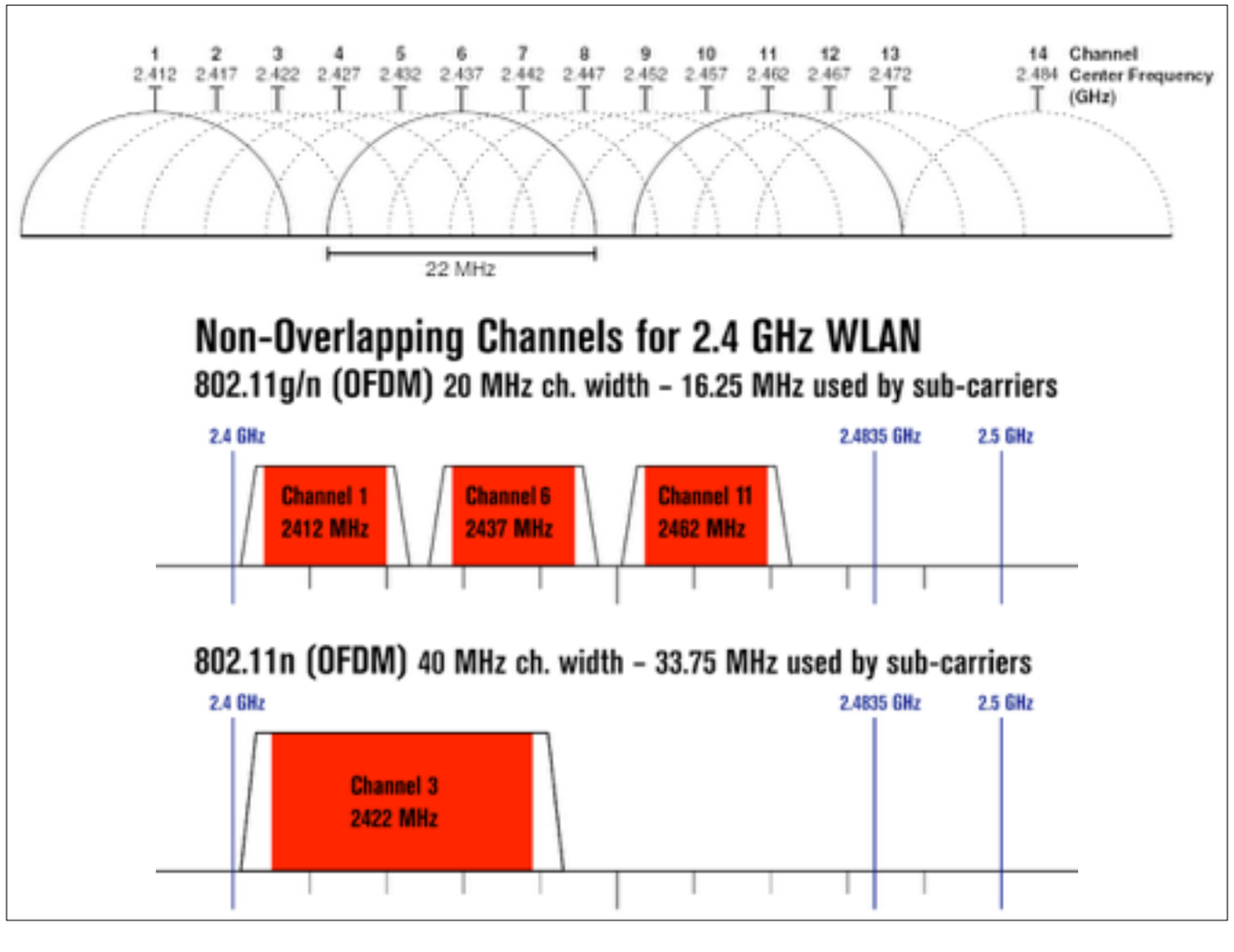
If you have an Apple Airport, all you need to do is pop open your Airport Utility, flip to the Wireless tab, and enable it. You can set a separate WPA2 encryption password—which I'd strongly recommend!—and you're good to go.

Check your channels, part 1: 5GHz is better (usually)

There are two chunks of radio spectrum allocated to consumer Wi-Fi—one in the 2.4GHz range, and one in the 5GHz range. Each chunk is subdivided up into a number of channels. MOST current devices can use both 2.4GHz and 5GHz, and the very first thing you want to do is make sure your AP is listening on both and that your devices are using both! If at all possible, you should have your devices connect using 5GHz instead of 2.4GHz, because the 5GHz bands are a hell of a lot less crowded. Most devices do all this automatically, but it's still a good idea to check your access point to make sure 5GHz is turned on. However, 5GHz radio waves have a harder time penetrating building materials, so it's possible that if your access point is more than a room or two away from your device—whatever the device is—it's being forced to 2.4GHz because the 5GHz signal just can't reach it. So don't just arbitrarily disable 2.4GHz to try to force everything over!

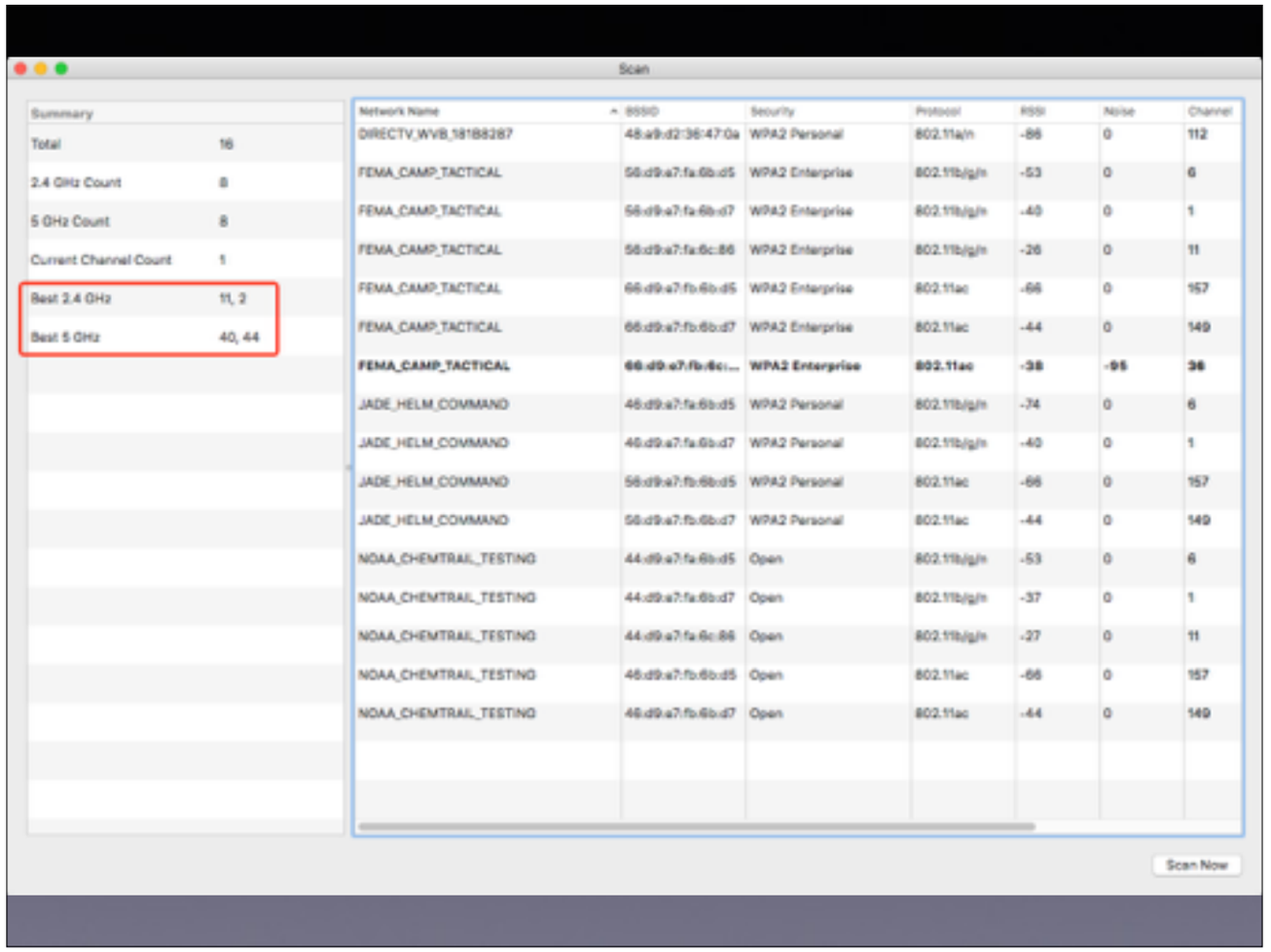
Check your channels, part 2: try your hand at picking the best one

You've probably heard advice about how to pick 2.4GHz channels—there are 11 of them in the US, but there aren't REALLY eleven, because each one is actually at least 20MHz wide and there's some overlap.



The non-overlapping 2.4GHz channels—generally—are channels 1, 6, and 11. Ideally, those are the ones you should be using, since those will be free of interference from other channels. Obviously, this creates its own problem—EVERYBODY wants to use those channels, which is why the intermediate channels exist—sometimes using, say, channel 3 is preferable to fighting your next door neighbor for channel 1.

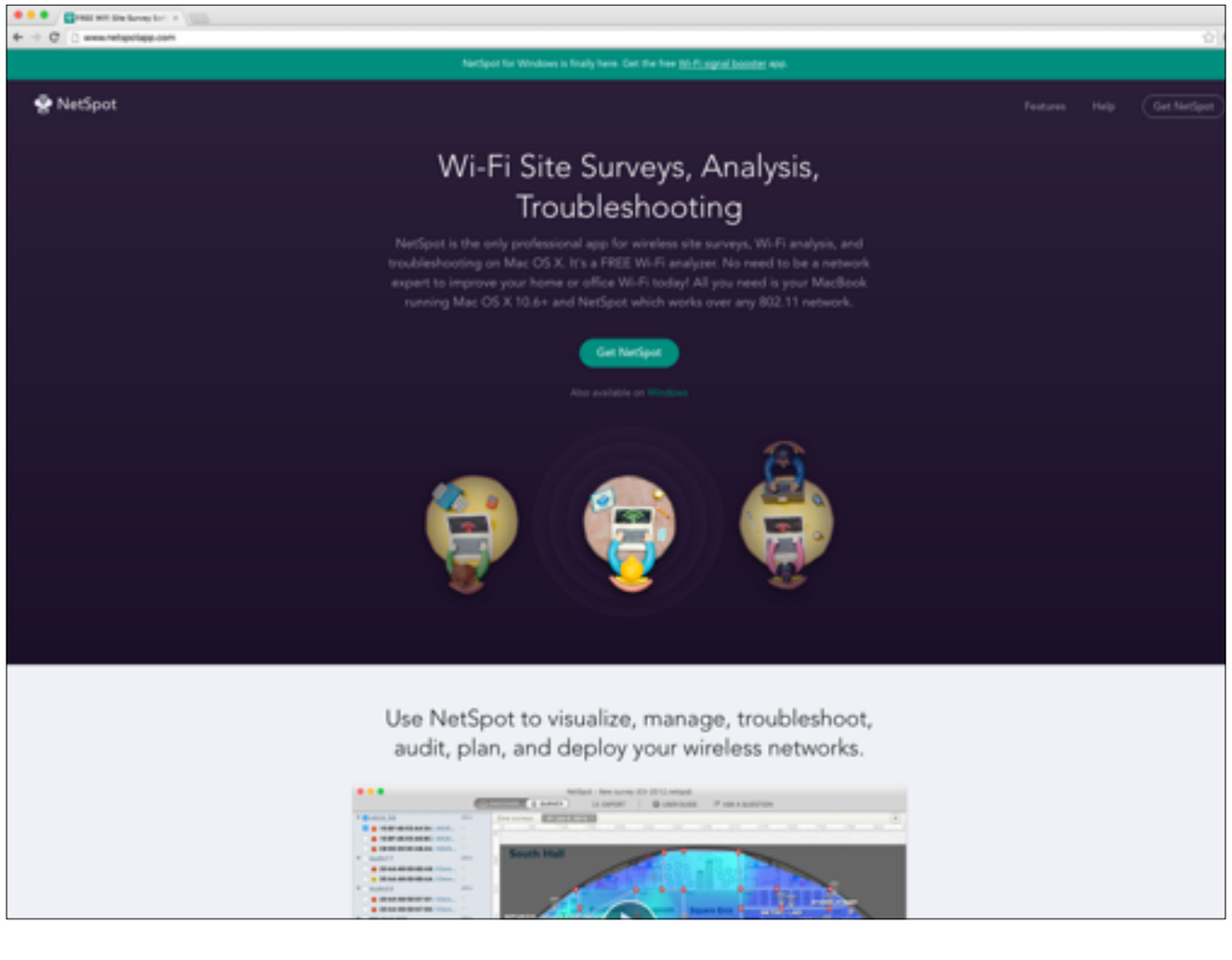
This is only for 2.4GHz, too—the 5GHz bands are generally free from interference, both because there are so many more 2.4GHz devices and also becaue the range on 5GHz signals is so much shorter.



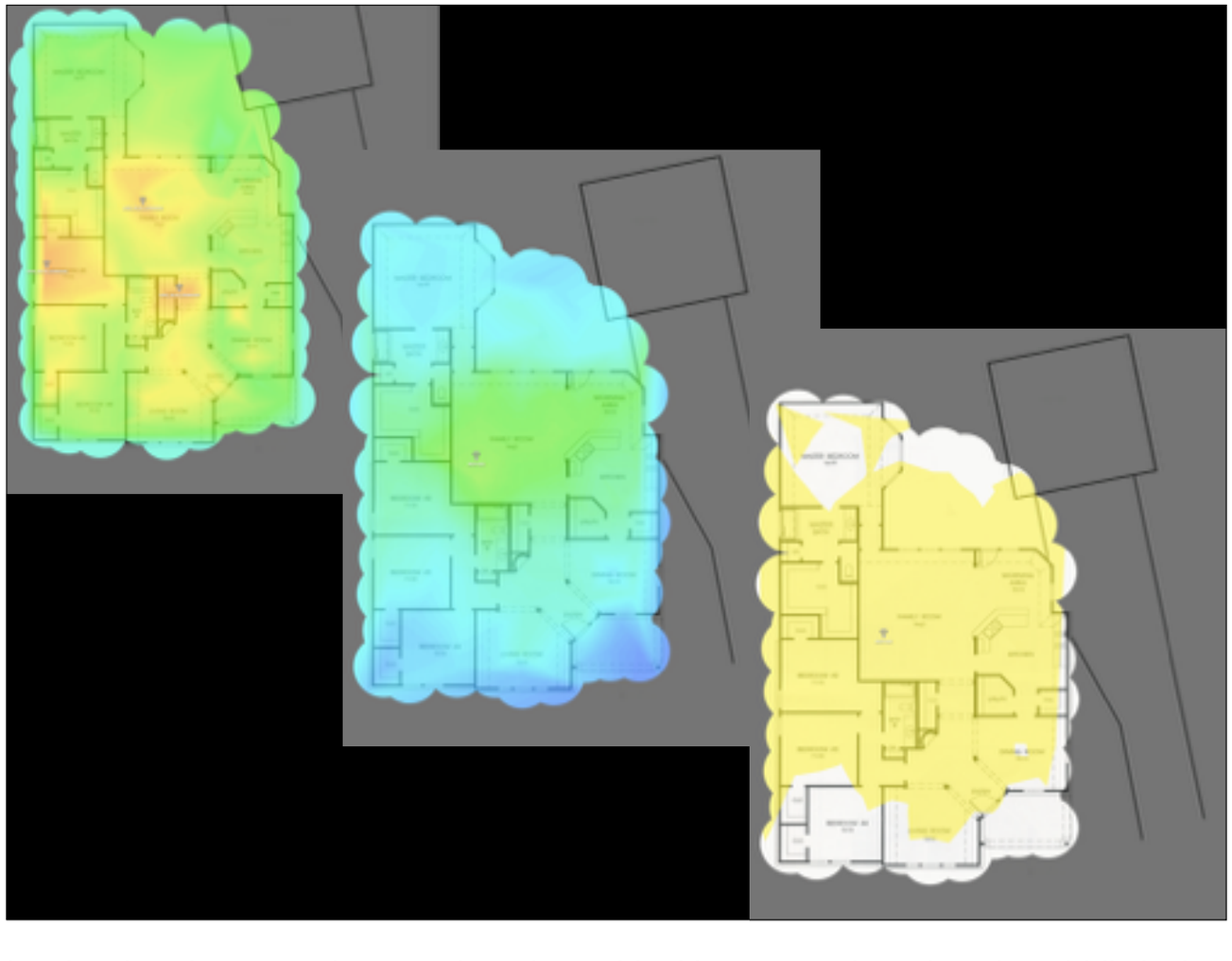
So how do you know what ot pick? Fortunately, your Mac already has a utility built in to tell you. It’s called the Wireless Diagnostic Utility—you can call it up with Spotlight. Once you’ve launched it, hit CMD-4 to invoke the Wi-Fi scanner function (or go up to Window and pick "Scan") and it’ll give you the recommendation for the "best" channels, based on what it finds. You can take that recommendation, log into your access point, and force it t use that channel. Most APs have an "auto" setting for channels, but sometimes it guesses wrong or badly, so this is a way to force the machine to do the right thing. Just be aware that the best channel TODAY might not be the best one tomorrow.

Do a site survey!

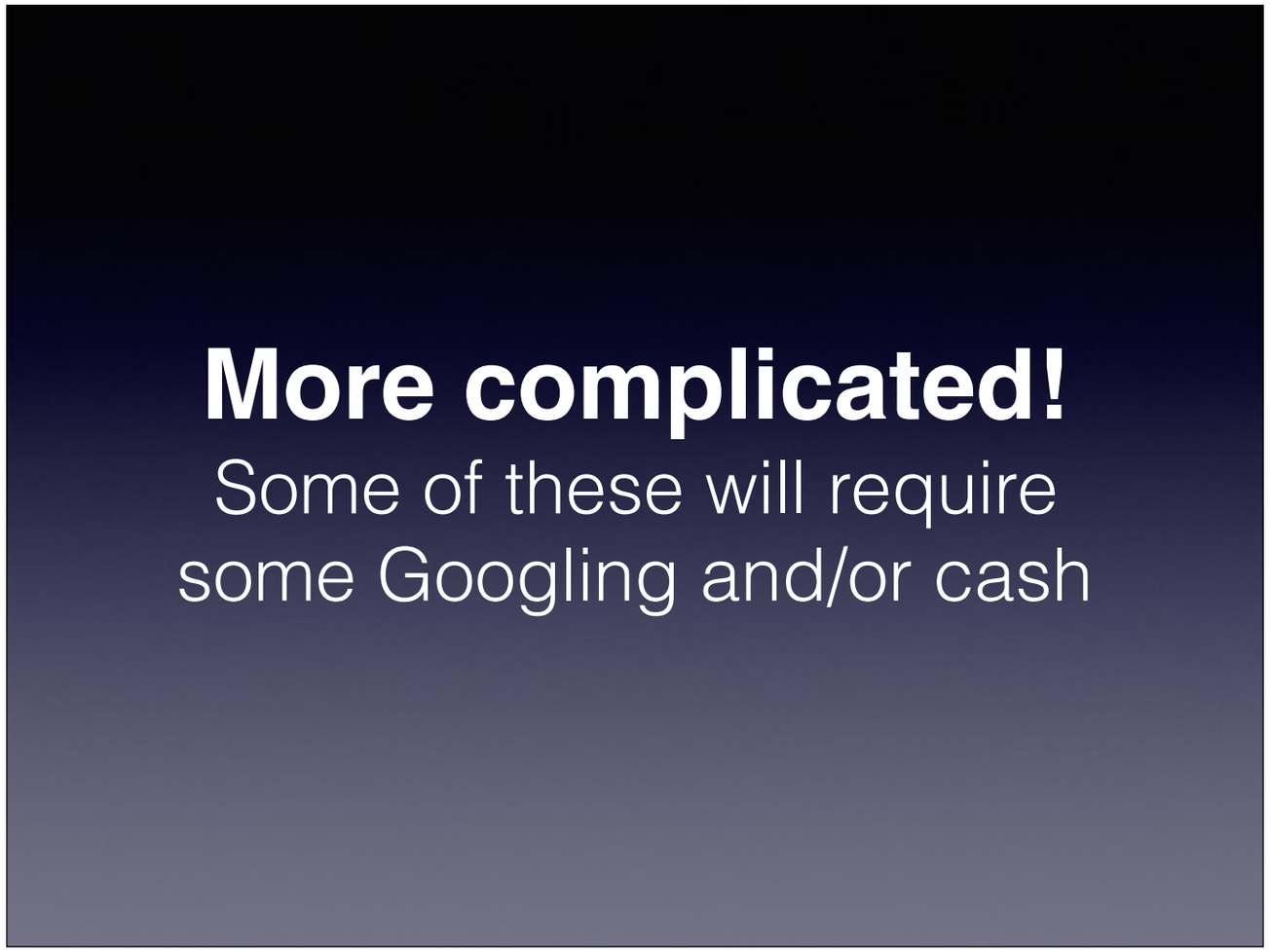
So, let’s say you’ve got a room in your house where you just can’t get a signal. No matter what. You’ve tried everything, but no matter what, you just can’t stream netflix in that room, or whatever. One way to tell for sure if there’s a dead spot or a problem is to do a wireless site survey—literally test the signal at a few points in every room to build up a map of what your wifi signal looks like. How, you ask?



There are several apps you can install on your Mac to use its own wi-fi antennas to scope out your house, but I’m most familiar with NetSpotApp. There’s a free version for home use that will let you take up to fifty sample points—you install the app, drag a picture or floorplan of your house to it and set the scale correctly, then you grab your laptop, walk to a few points in each room of your house, hit the "sample" button and hold still for a few seconds. The program prompts you to click on the floorplan at the spot you’re standing when you take each sample. Eventually you get a nicely produced PDF with a bunch of different measurements that will be really meaningful if you have a double-E background, but even someone like me can see dead spots!



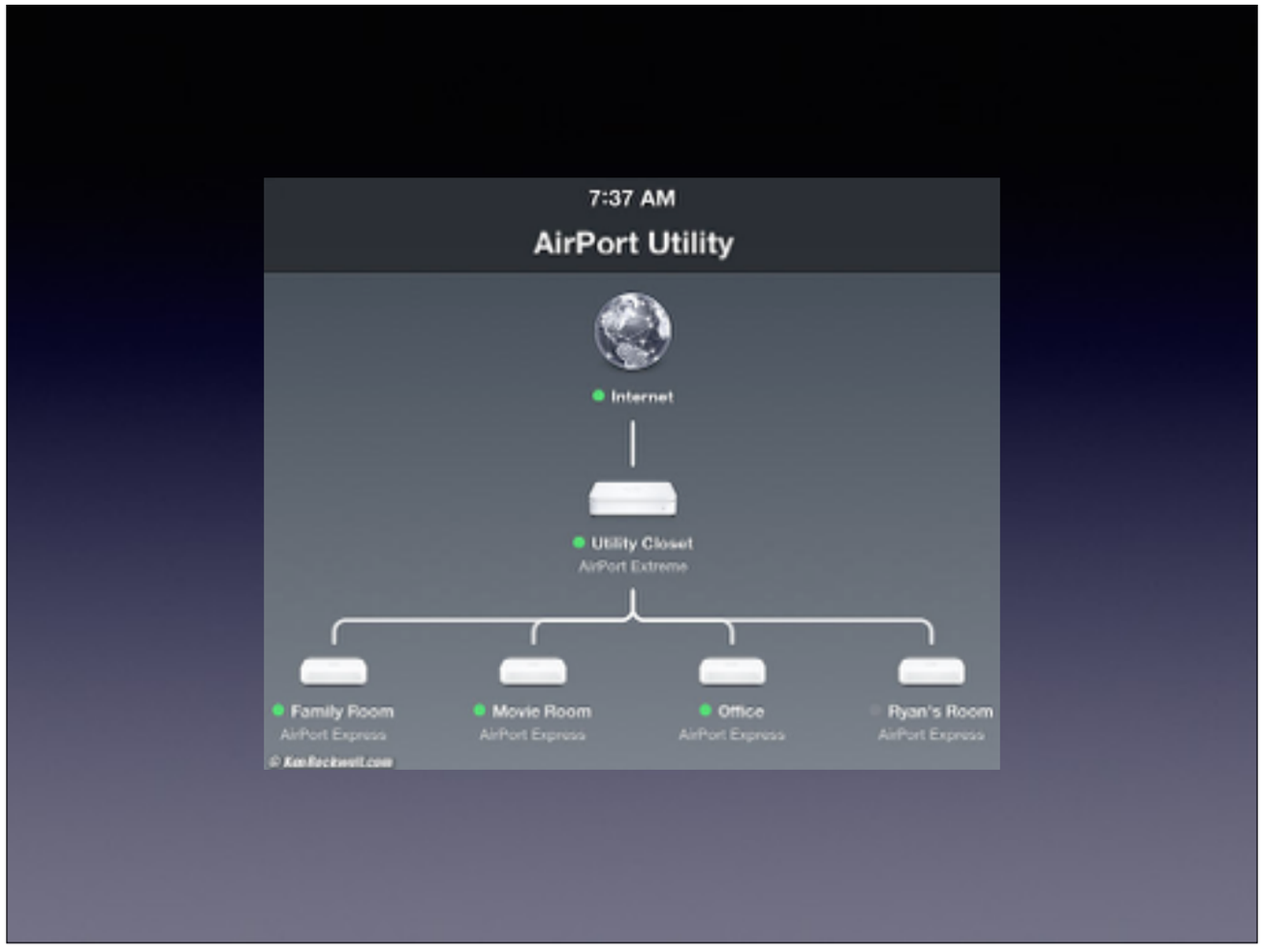
This is what it looks like. Upper left is a signal-to-interference ratio map of my three ubiquiti access points, then the middle is the same map of my single airport, and then the bottom right is a 5GHz dead spot measurement with the old airport. These are individual images that I took out of the report, so there's no legend or scale, but the actual report the app spits out gives you all that so you don't have to guess what the colors mean.



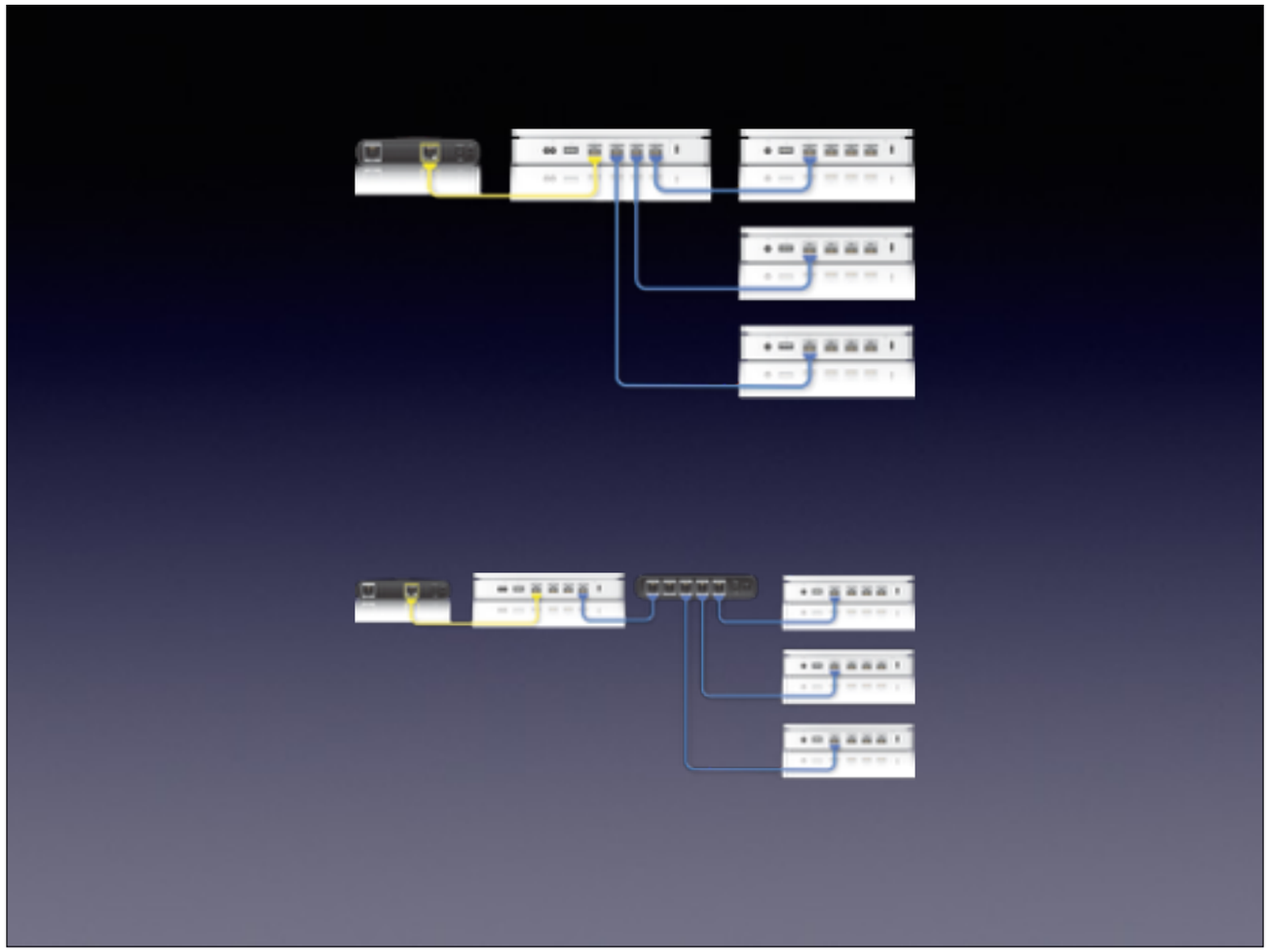
Now we’re gonna leave easy behind. These are some more advanced things you can try to implement—don’t be afraid to tinker here! the worst thing that’s going to happen is you’ll have to factory reset your access point, and that’s okay. but maybe take some screenshots of your configuration before you get started, just in case.

Extend your network!

Sometimes having just one access point isn’t enough, especially if you’re in a multistory house or one with a larger floor plan. if you’ve got dead spots or slow spots and you can’t really mitigate them by moving your one AP around, you can get some more access points and extend your network.



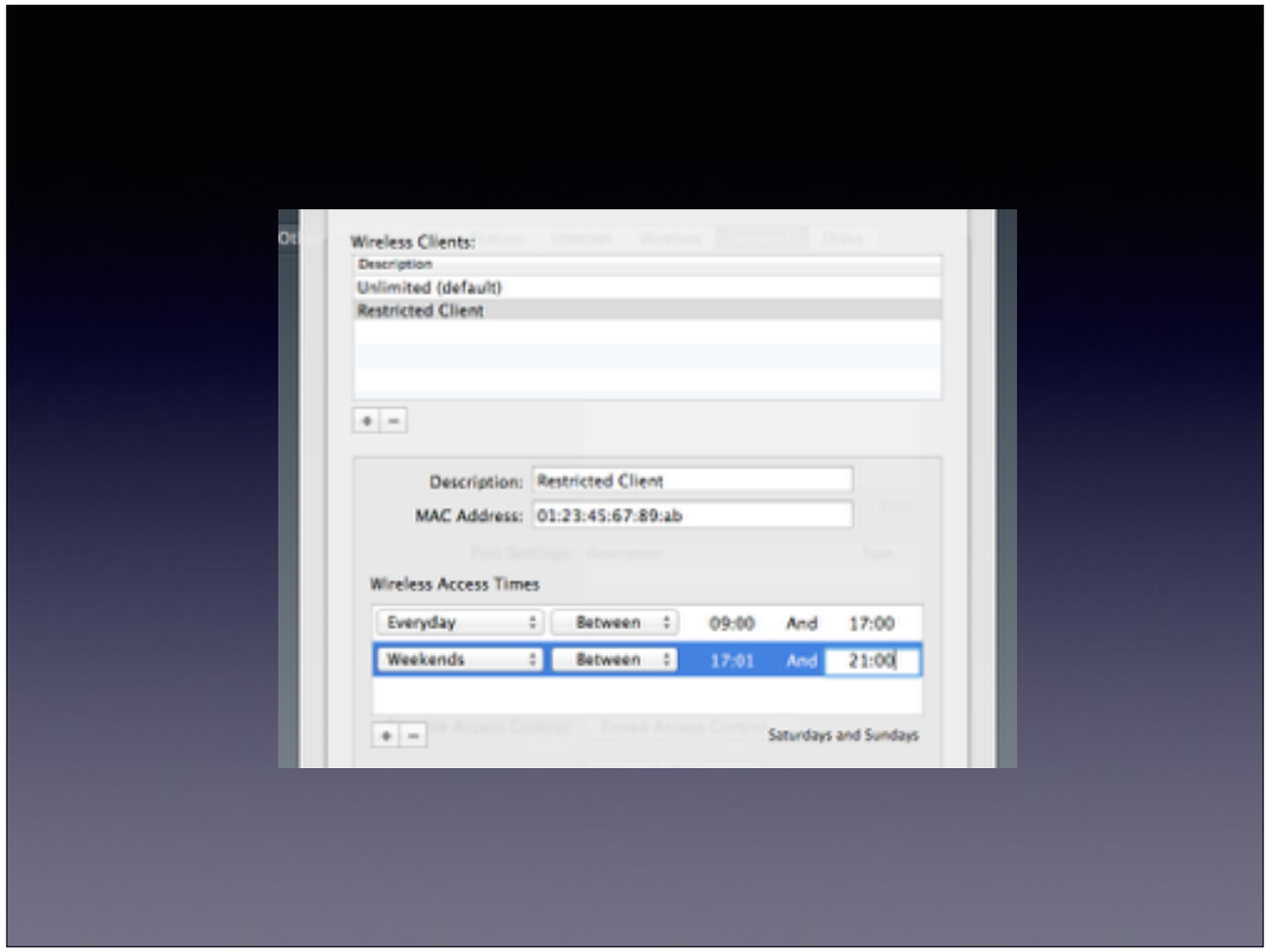
If you're in the apple ecosystem this is relatively easy—just buy another airport extreme or airport express. The Airport Utility will find it and ask if you want to use it to extend your current network. BUT—be aware that there are different ways to do this. The simplest is to stay all wireless, which has the advantage of you not having to run ethernet cables all over your house but the disadvantage of spectrum and radio reuse. What that means is that each access point can only send and receive so much—there are a fixed number of antennas and radios in each AP. If you're wirelessly extending your network, some amount of your wireless bandwidth is used to connect the two access points, and that bandwidth is unavailable for use with your wireless clients. This is actually a pretty complicated area of discussion since the specifics of it vary with manufacturer and I won't spend more time on this, but just know that wirelessly extending your network comes with costs to balance the convenience.



Alternately, you can connect multiple access points together with wired Ethernet. In this case, they'll all work together to extend your network without consuming extra wireless bandwidth for communicating with each other. You run into a different problem here in that the APs all need to avoid each other's frequencies, but that's also a problem with wireless extension. This is the best way to do network extension, but it's also not necessarily the most convenient, because you gotta run wires.

Set up timed access!

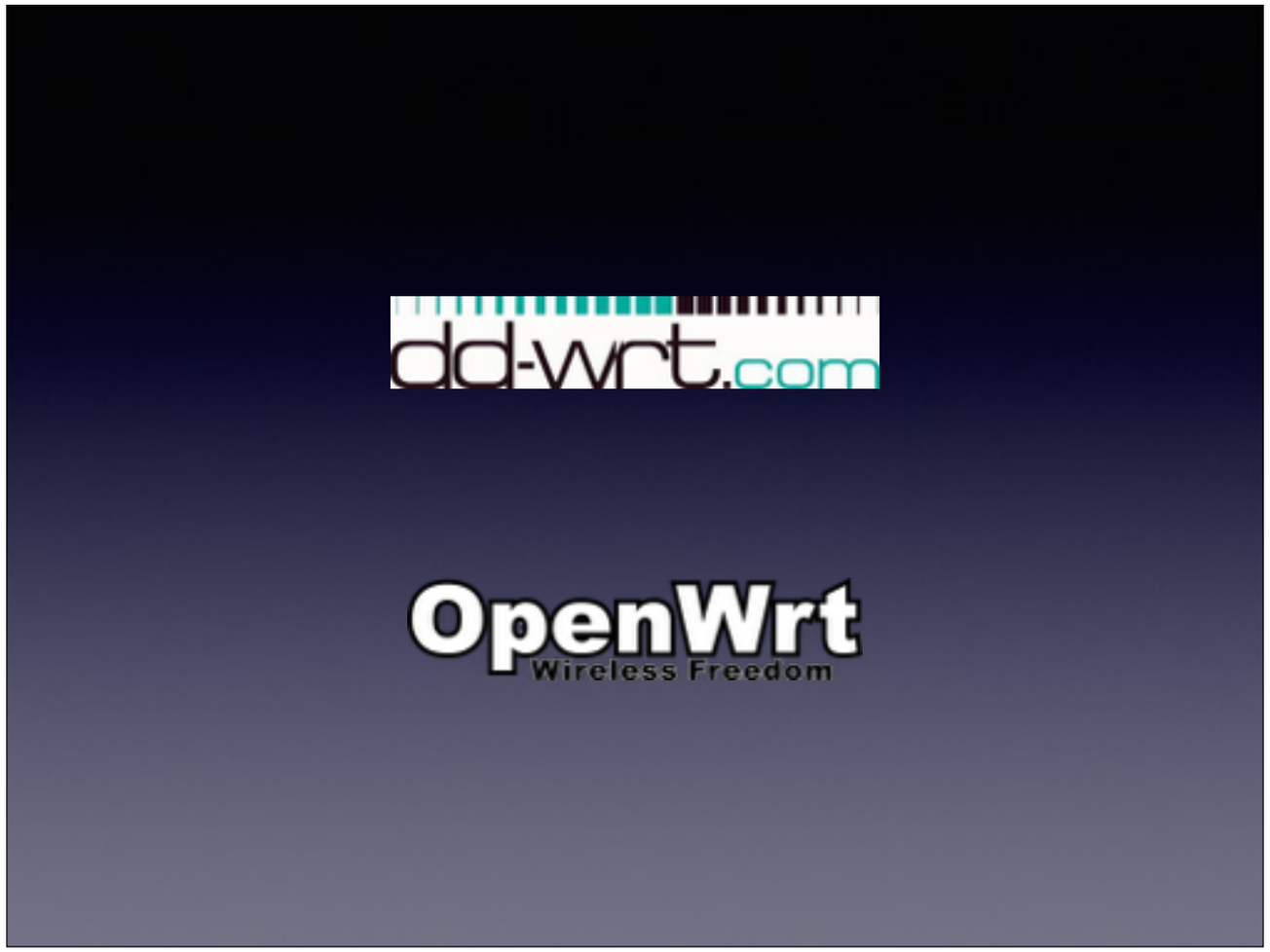
Timed access is a feature you might not know exists, but it’s available on most access points. This one’s particularly useful if you’ve got kids and you want to limit their screen time, or if you want to force yourself to get off the computer every night at 9 and go to bed, or whatever.



For an Apple Airport, you have to dig into the settings a bit but the upshot is you can restrict the hours during which any wireless device is allowed to connect to your access point. The restriction is by MAC address–that's not mac like the computer, but MAC like Media Access Control, the unique identifier in every piece of networking gear. All you need to do is find the MAC address of the device—and most APs will show you a list of connected MAC addresses correlated to network names—and add it to the list and define a schedule. Boom, instant disconnection at 9pm on weeknights!

Install custom firmware!

The Airport Extreme is a fine piece of gear, but not everyone sticks with the apple ecosystem. There are lots of other options from lots of other OEMs, but one thing all those other options have in common is that they generally have clunky interfaces that lack some essential geek features, like being able to work as a VPN endpoint or extra wi-fi tuning options. There's a fix for that, though—you don't have to live with the OEM's interface or feature set. With MOST consumer-grade wifi access points, you can install custom firmware that adds a ton of extra stuff.



The two most common custom firmware distributions you'll hear about are DD-WRT and OpenWRT. DD-WRT is probably easier to install and configure and it's basically one chunk, while OpenWRT is a lot more modular and configurable—and you guys know that "modular and configurable" is also code for "harder to install and understand at first." They also will each work with a different subset of routers. Now, why would you subject yourself to something like this? Because custom firmware gives you a hell of a lot more knobs to turn, if you need them. It'll get you features like VPNs that probably aren't on your regular router, and they'll also give you a lot of tuning abilities for your wifi—stuff like the ability to steer clients to 5GHz only, or adjust your transmit power (up to the FCC's limits!), or other tweaks.

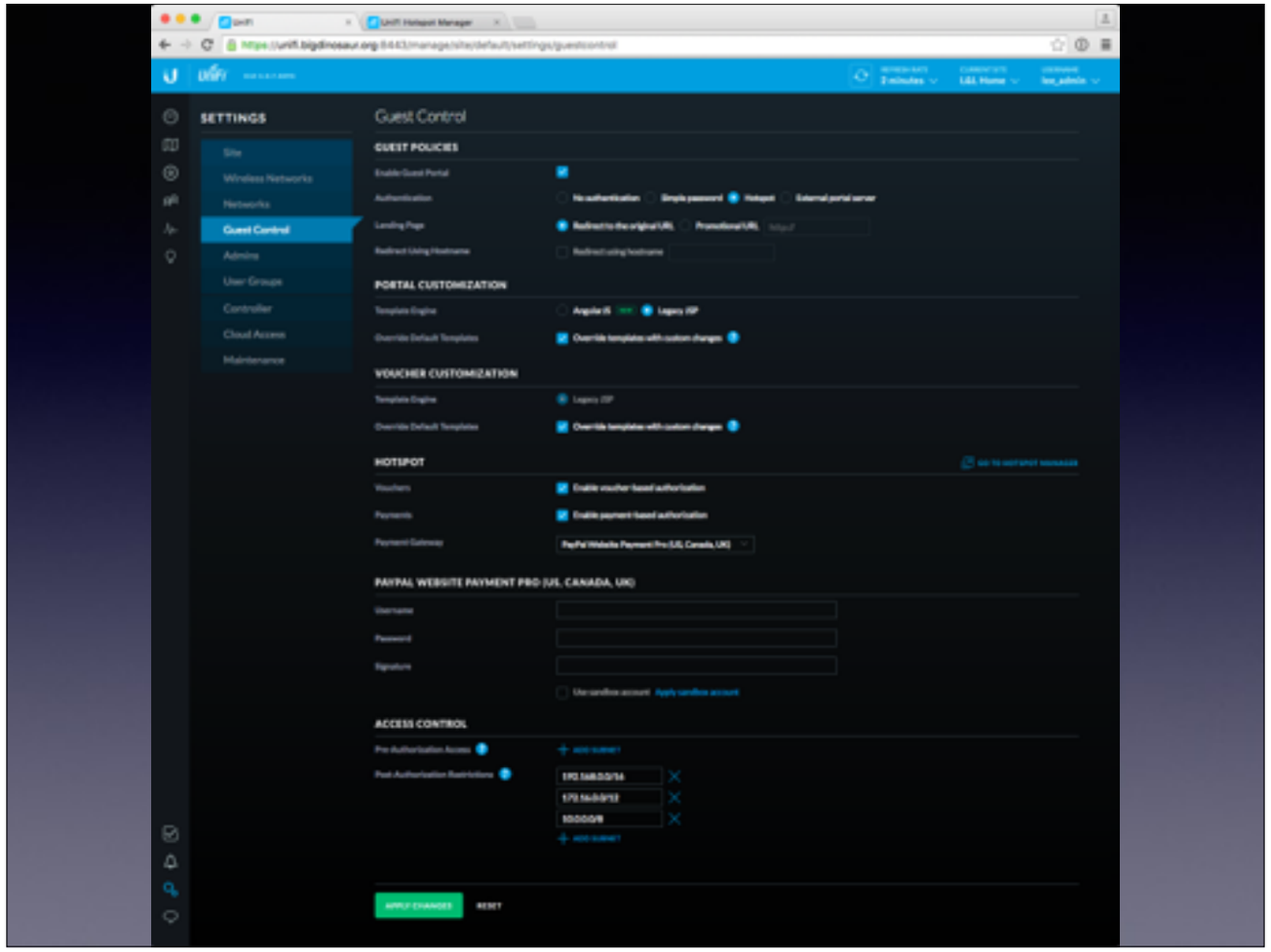
Get crazy!

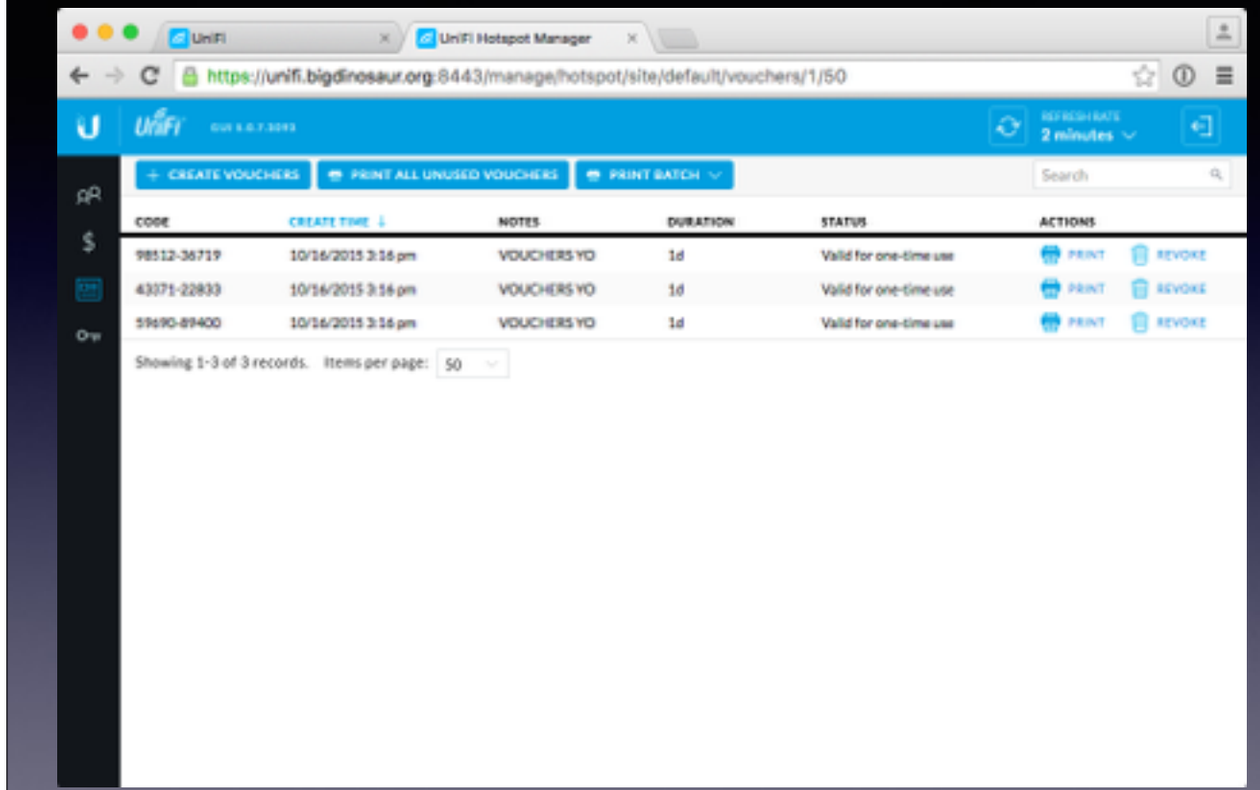
Fun ways to make your wife angry when her iPad won't connect to the wifi anymore because of what you did

OK…none of this is easy. Any one of these ideas is at minimum a full weekend project, and most of them are more trouble than their worth. BUT, the upshot is that you'll learn some neat stuff and the worst thing that'll happen is you take your entire home network down and have to factory reset everything.

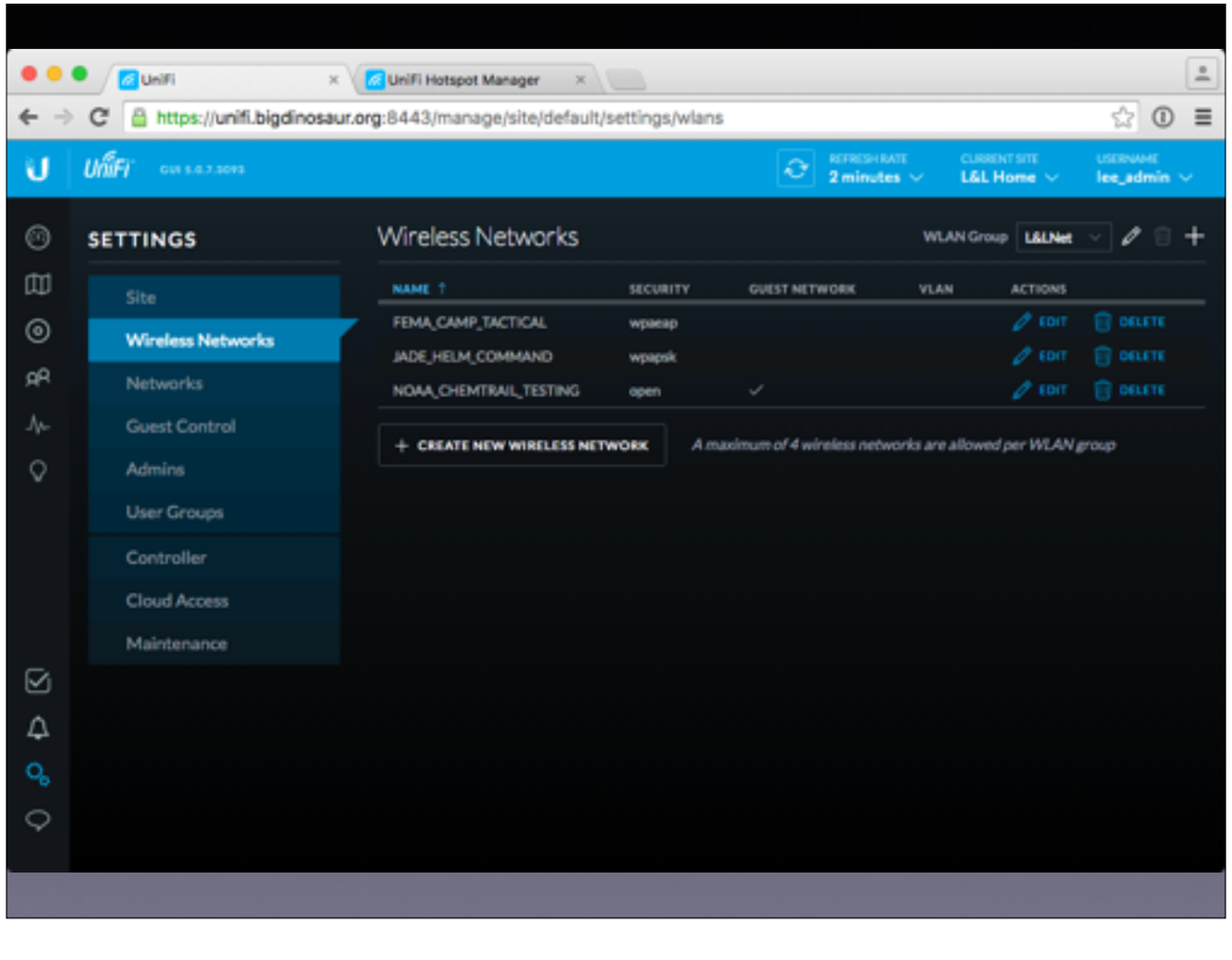
Make a custom guest portal!

That fun government-looking login page I showed at the beginning is just a custom guest portal on my ubiquiti wi-fi access points—actually it runs on a separate control station box, but it's all part of that system. If you have the ability to provide a custom guest login page, you should do it! It's great fun! Freak out your neighbors, or go the serious route and say that this is YOUR guest wifi and make people acknowledge that they won't do anything naughty if they join. Most systems that support a custom guest portal will ALSO support different authentication methods, too—so you could even set up a paypal account and make people pay you $10 a day for access, just like in a hotel! This MIGHT NOT be allowed under your ISP's terms of service, though. Still, fun to learn!


SETTINGS
Site
Wireless Networks
Networks
Guest Control
Admins
User Groups
Controller
Cloud Access
Maintenance
Guest Control
GUEST POLICIES
PORTAL CUSTOMIZATION
VOUCHER CUSTOMIZATION
HOTSPOT
PAYPAL WEBSITE PAYMENT PRO (US, CANADA, UK)
ACCESS CONTROL
APPLY CHANGES
RESET


UniFi
UniFi Hotspot Manager
https://unifi.bigdinosaur.org:8443/manage/hotspot/site/default/vouchers/1/50
UniFi
REFRESH RATE
2 minutes
+ CREATE VOUCHERS
PRINT ALL UNUSED VOUCHERS
PRINT BATCH
Search
CODE
CREATE TIME
NOTES
DURATION
STATUS
ACTIONS
98512-36719
10/16/2015 3:16 pm
VOUCHERS YO
1d
Valid for one-time use
PRINT
REVOKE
43071-22833
10/16/2015 3:16 pm
VOUCHERS YO
1d
Valid for one-time use
PRINT
REVOKE
59690-89400
10/16/2015 3:16 pm
VOUCHERS YO
1d
Valid for one-time use
PRINT
REVOKE
Showing 1-3 of 3 records.
Items per page:
50

Set up multiple SSIDs
and VLANs for security!

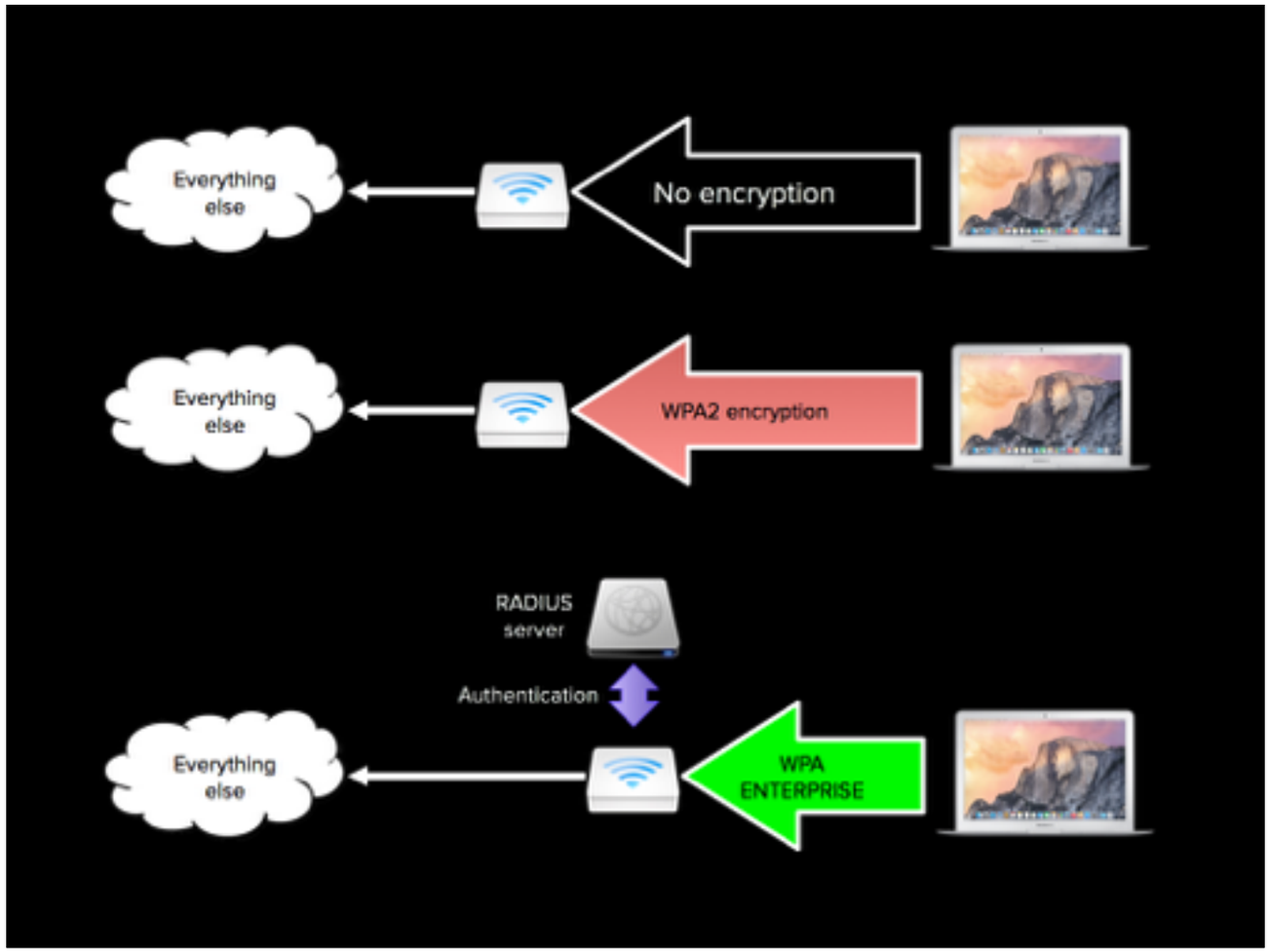


VLANs and SSIDs—this sounds complicated! This gets into setting up your home wi-fi more like how your work's wi-fi might be built. Maybe you've got, say, some "smart devices" like a smartTV or a smart fridge or a smart thermostat or whatever, and they connect via wifi to the internet, but you don't necessarily want them on your home wifi seeing all of your home LAN's traffic. Because honestly, who trusts Samsung or whatever? You can't really put them on a guest network, since you'd have to enter in the guest password on them every day and some devices won't let you do that…so why not set up a second SSID, a second wireless network, for stuff you don't trust but that you can't put on a guest network? Most APs make this relatively easy!

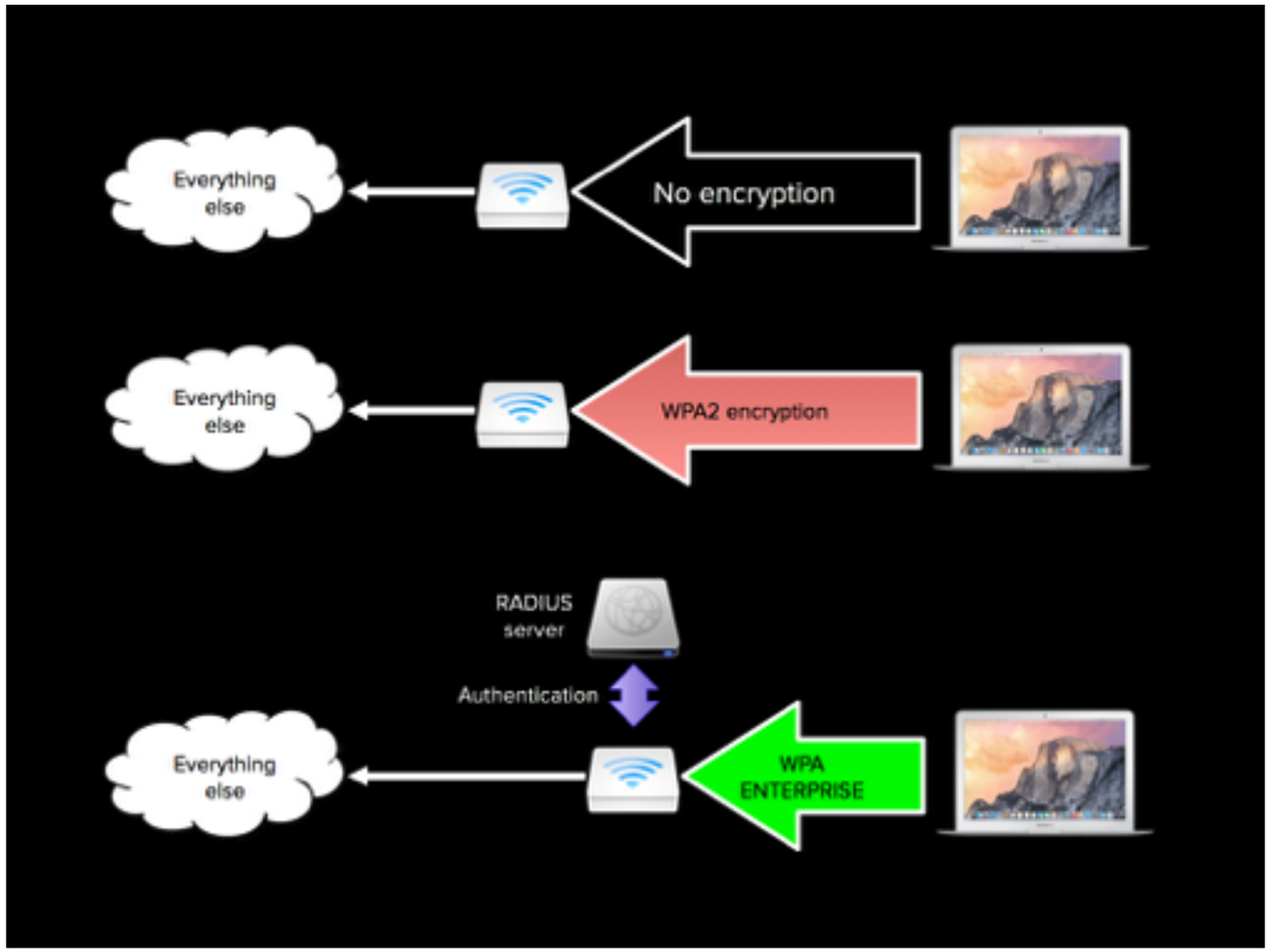
Now there ARE potential config issues for stuff like this, especially if it's a device that, say, needs to talk directly to an app on your phone. But it IS a more secure way of doing things—you just have to be prepared for some config pain.

Set up 802.11X!

Now we’re getting really crazy.



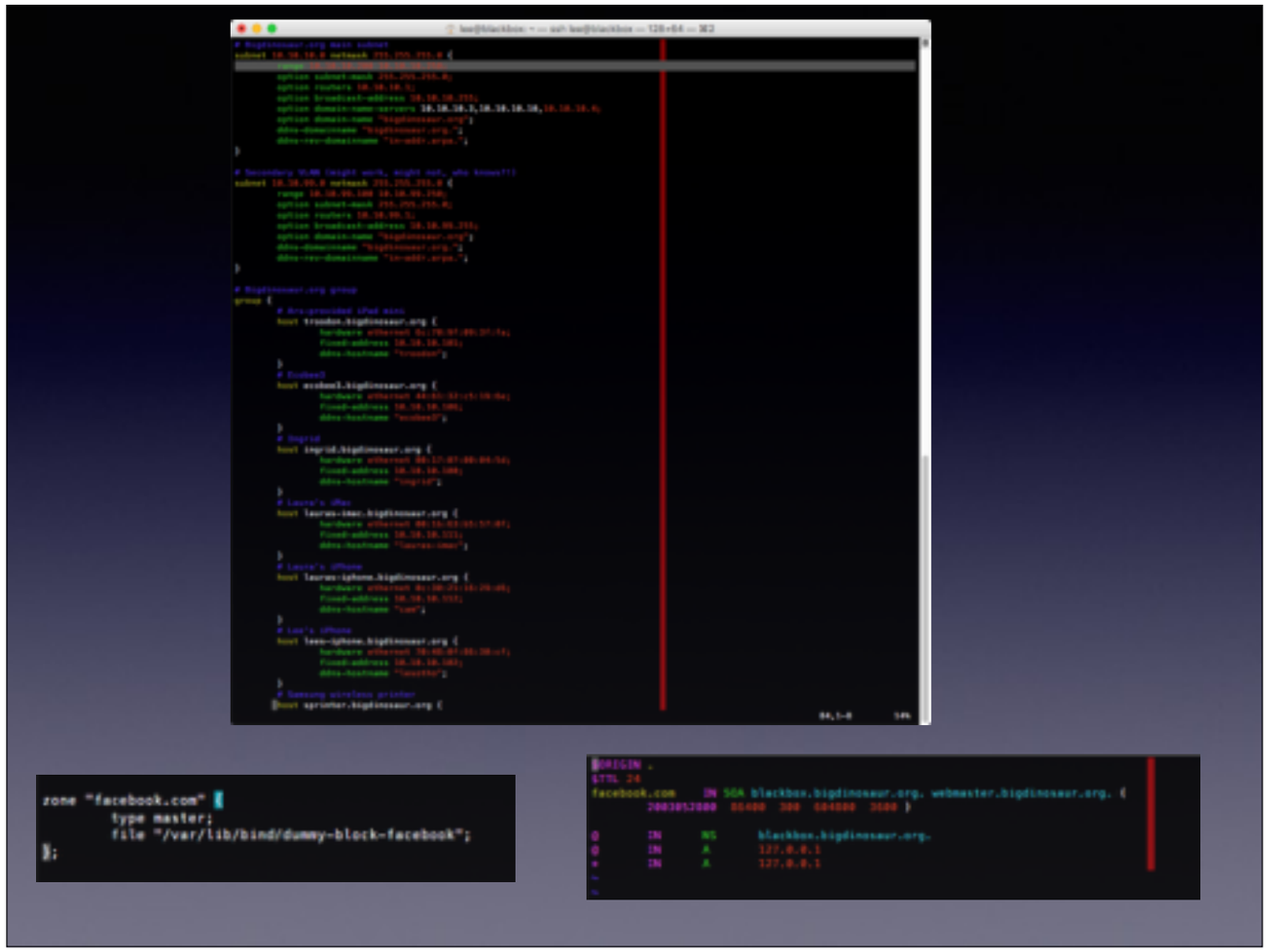
The basic idea with setting up 802.11X on your wireless network is to separate out what part decides what devices can connect, from the part that does the connecting. At the very top here, is unencrypted. Traffic flows in the clear. Then what most folks should have is in the middle: WPA2 Personal, where your access point encrypts wireless traffic between your device and itself. But at the bottom is an 802.11x set-up. Traffic is still encrypted between the laptop and the AP, but there's another server running an application called RADIUS with a list of accounts on it. Those accounts can be for users, or they can be for machines themselves; they can be simple passwords or they can be cryptographic certificates. Rather than one wifi password, everyone—or everything—or both!—gets validated.



This is complicated, but it’s also how most places of business do their wifi configuration—it makes things a lot harder for unwanted people or devices to slip onto your network. It’s also hard to configure and you need an extra server to run the radius software—you can use a linux box and the freeradius package, if you’re so inclined. Your iphones and ipads and laptops will all work with this kind of setup without issue, but older devices can have problems. also some smart devices won’t support WPA Enterprise.

Build a Linux server and
set up bind9 and dhcpd
for greater configurability!

This is not something you'd undertake lightly, but if you've got a lot of time on your hands and you want to do things like take direct control over how IP addresses are handed out or how DNS lookups work, you could quit using your router's built-in DHCP and DNS and instead start up your own instances of the applications that do these things.

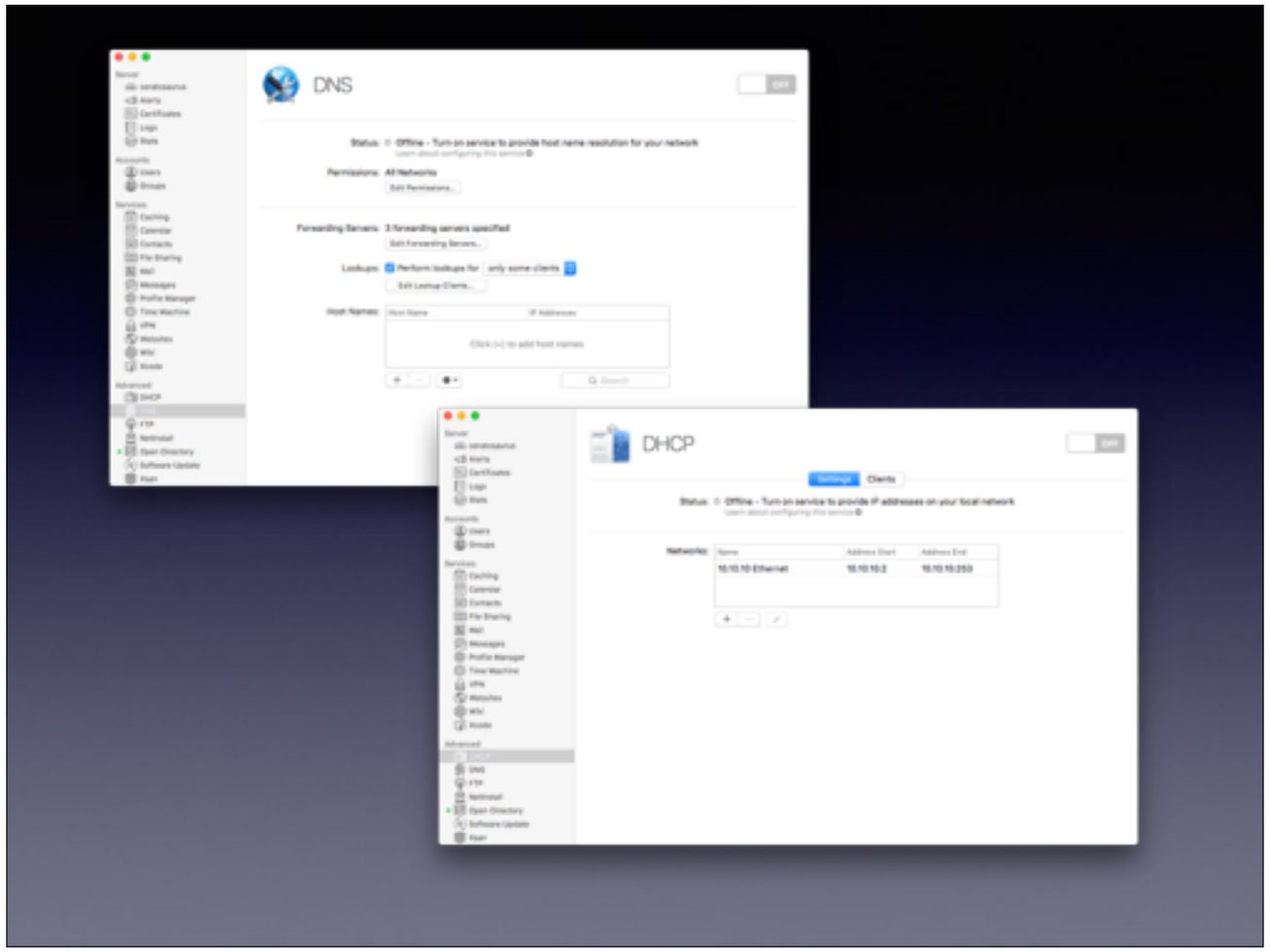


```
zone "facebook.com" {
        type master;
        file "/var/lib/bind/dummy-block-facebook";
};
```

```
$ORIGIN .
$TTL 24
facebook.com    IN SOA blackbox.bigdinosaur.org. webmaster.bigdinosaur.org. (
        2003052000  86400  300  604800  3600 )

@       IN      NS      blackbox.bigdinosaur.org.
@       IN      A       127.0.0.1
*       IN      A       127.0.0.1
~
~
```

You can do it the super-dumb hard way with linux—on top is my set of dhcpd settings to build out my scope, and on the bottom are the two DNS tweaks I use to block facebook DNS lookups at home…



…or you can do it the super-easy way with the Mac OS server utility, which you can grab on the app store for I think $20. Just be careful, because especially with DNS there's a lot to learn about proper sysadmin habits and configuration quirks. The advantages to rolling your own here aren't super huge—you get a lot of configurability and control, but that doesn't necessarily mean much—but you WILL learn a lot. Or break something. Or both!!

BONUS ROUND: IPv6!

I didn’t do a slide for this one because IPv6 is complicated and I don’t fully understand all the implications of rolling it out at home. IPv6 is the next generation of the IP protocol and it massively expands the addressing space available—I’m sure you’ve all heard the whole thing about how we’re running out of IP addresses and stuff? IPv6 is the answer to that—and it also changes a lot of behavior that as both users and admins we’re used to. Rolling it out to your home network wouldn’t be too hard if you have a few devices, but the more complex your setup, the more config quirks you’ll have to take into account. I put this on here just to have a super-difficult but super-rewarding thing to end with, because this is the last thing I had.

The end

Happy to take questions or talk a little more about any of these things!