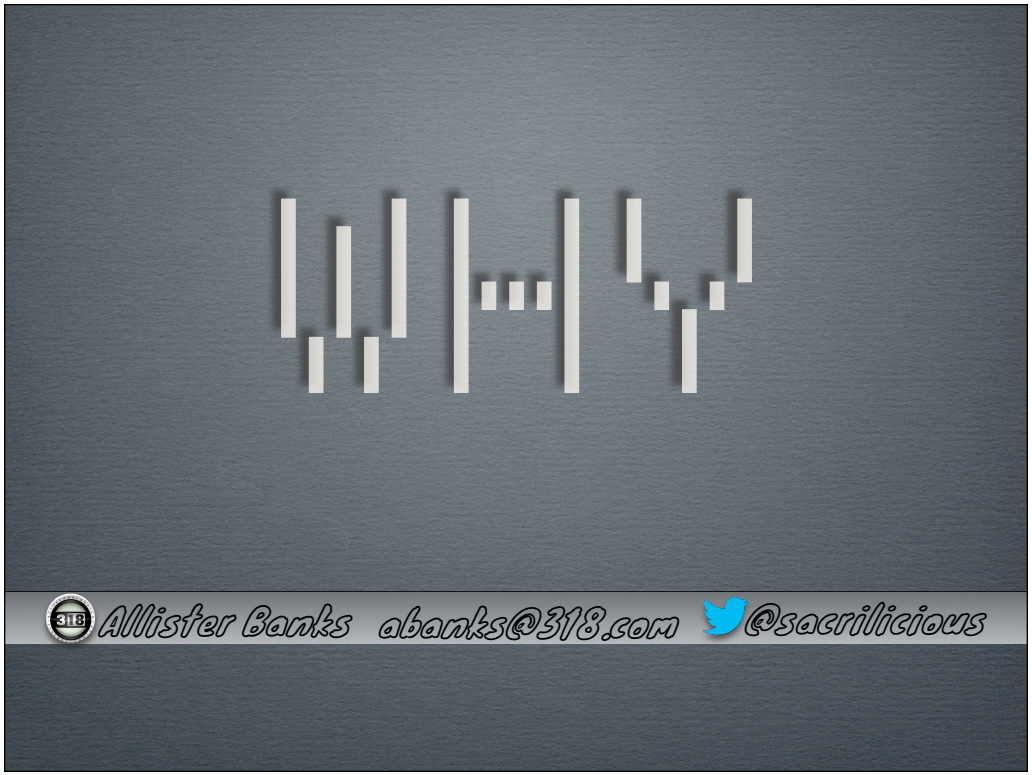
PENNSTATE

1855

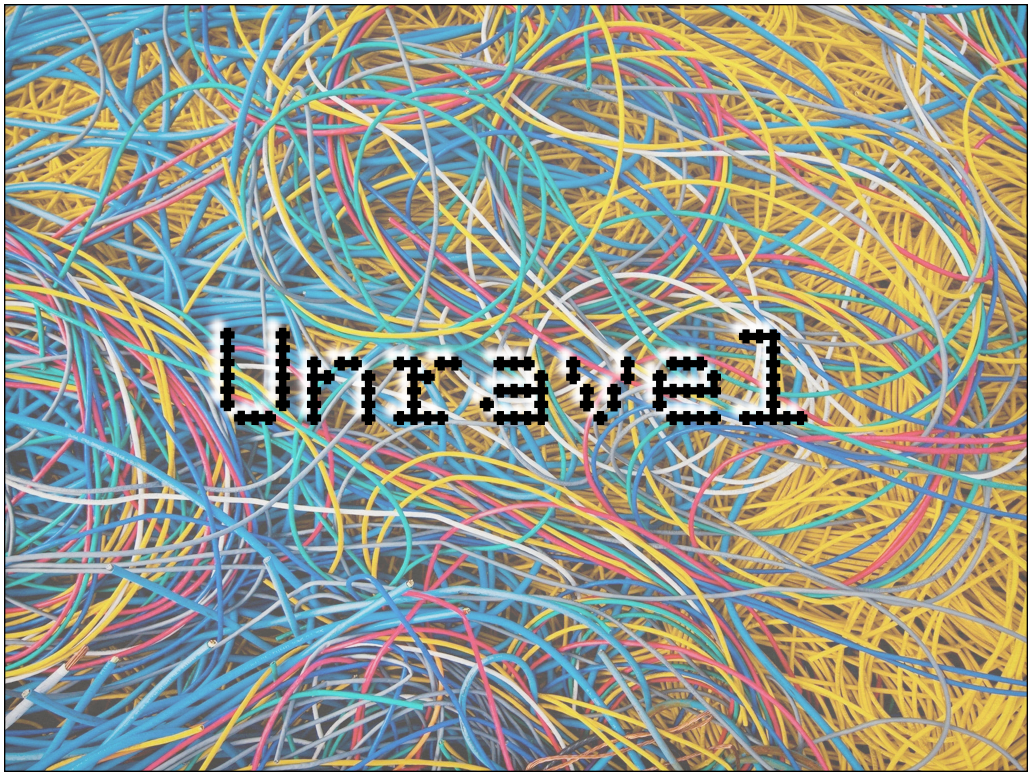
MacAdmins Conference 2013

Enough Networking To Be Dangerous

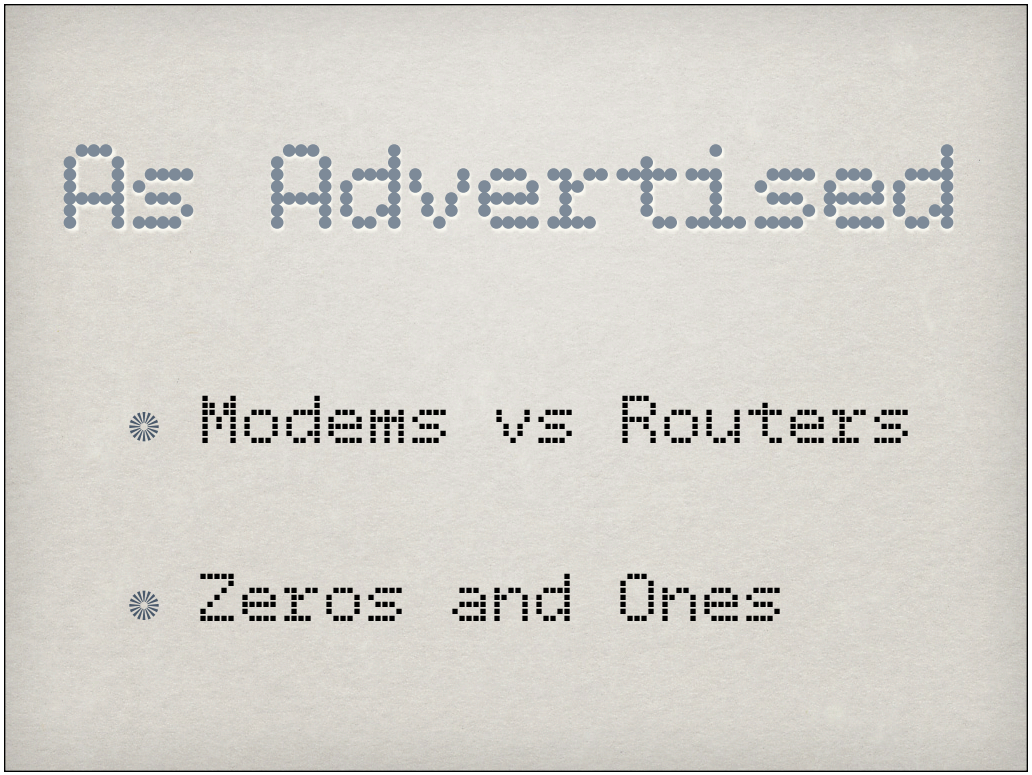
Allister Banks abanks@318.com @sacrilicious



I guess I'm up at the front with a microphone because I'm somewhat acronym-complaint, meaning I'm halfway to my Cisco Certified Network Admin or CCNA cert, and have received all the certifications acknowledged by the company behind some cool yet not inexpensive wireless access points, Aerohive. And if you don't use either of that gear and consider yourself somewhere around a beginner, well I still think you're in the right place:

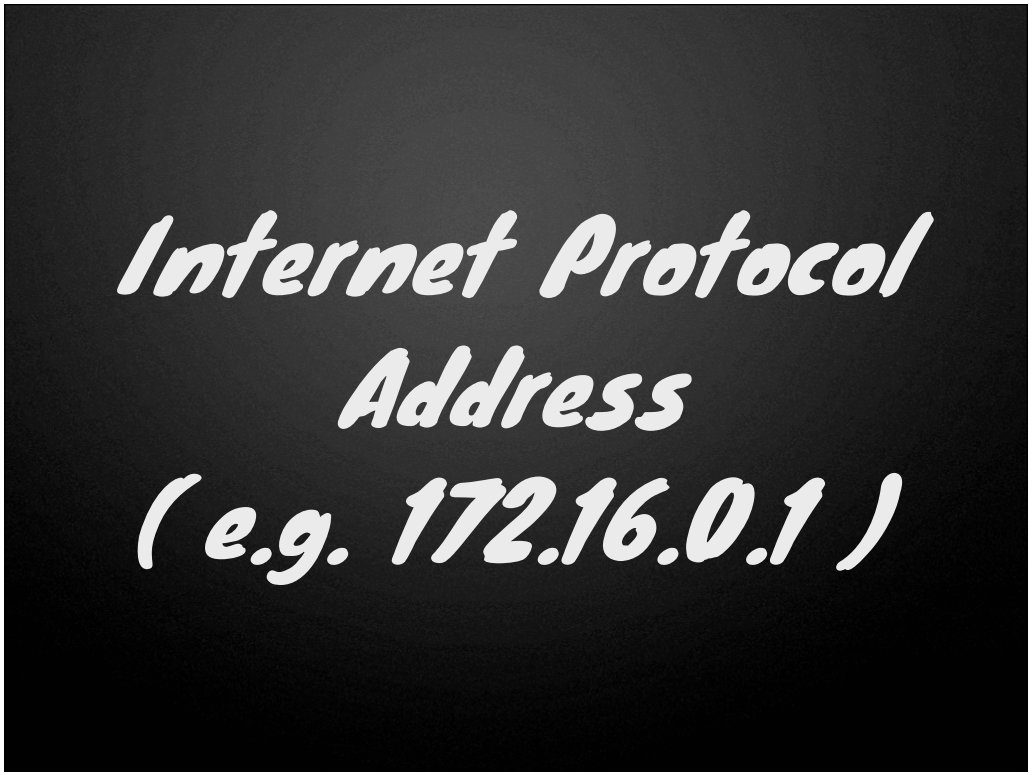


I don't care about alphabet soup certs with proprietary systems and terminology, but I think that often when starting out being interested in a topic we could learn best from an advanced beginner, since they've only recently turned the corner on the frustrations we commonly face when tackling and unravelling a big topic like this, like networking.



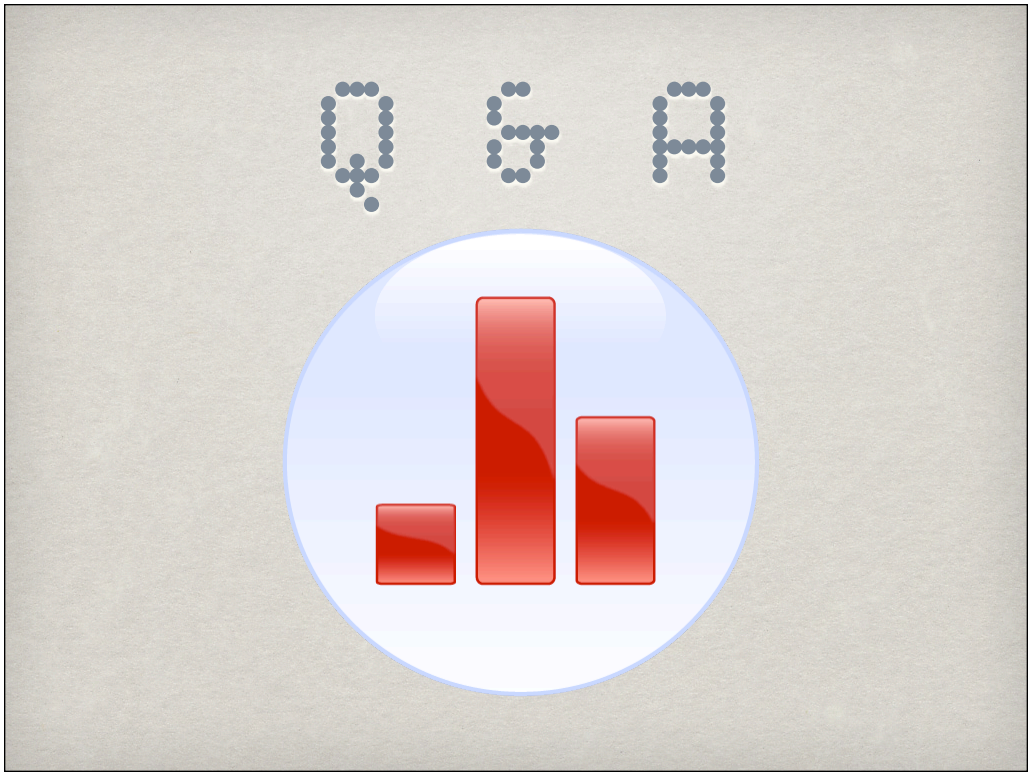
3

So in the session description I mentioned two things, What is a modem in comparison to a router and a more betterer understanding of how zero's and ones flow over networks - neither of which is mac-specific stuff, we'll touch on a few things later, but stop short of VLANs and proxies, because maybe that's above our pay grade - maybe, I don't know about you folk. We're going to detour in the modem vs. router part first and the whole picture won't come together until later on. It's going to be consumer-focused until later as well, so we can all relate to the stuff we have in our homes and kindof know how it works....



I think the only real prerequisite is you need to understand what an IP address is and looks like, that's a local network ip, like the one that starts with 192.168, folks know the third?

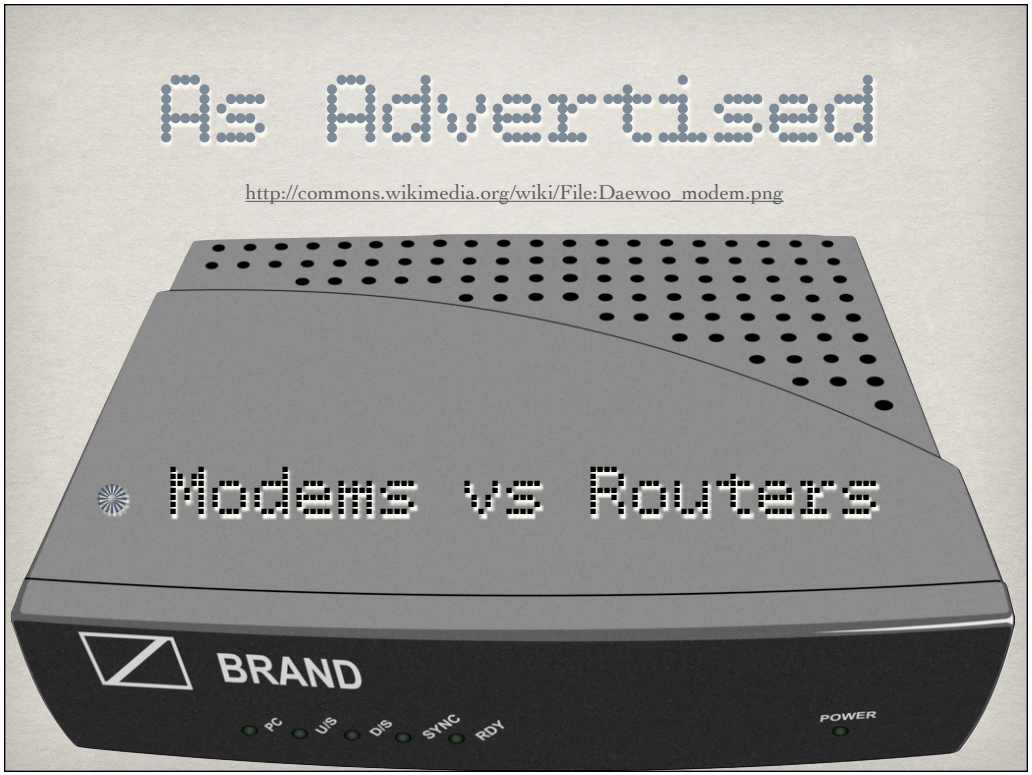
and what DNS means functionally and that it's important.



In the past I've used a question gathering service like polleverywhere to not be interrupted while going through my spiel, and I do hope that things I won't be covering, but you may want to ask about can be held off until Q&A. This time however we're going to hopefully have a little fun so that the folks who aren't just here to surf the internet will feel a little more engaged and that you can totally interrupt me with questions this time, just please refine it for two purposes:

one is that an acronym you don't know or buzzword has been detected – I'll try my best to explain any term you'd like. And for anyone in here who feels they're probably already pretty knowledgable about networking, and you'd like to call me on my mularkey, or to be gracious, possibly imprecise, go ahead and raise your hand and you can tell me what is the more accurate way to explain or define a process or concept. Please, do get involved, let's mix it up.

If you have an iPhone that can reach internets, i even encourage you, although i may regret this later, to download Service Bell from the app store and join in. Be aware, I may hold up the 'we'll get to that' sign, please forgive me if I ask you to hold off and try to keep your questions within the current topic or as it relates to the ones I'm covering.

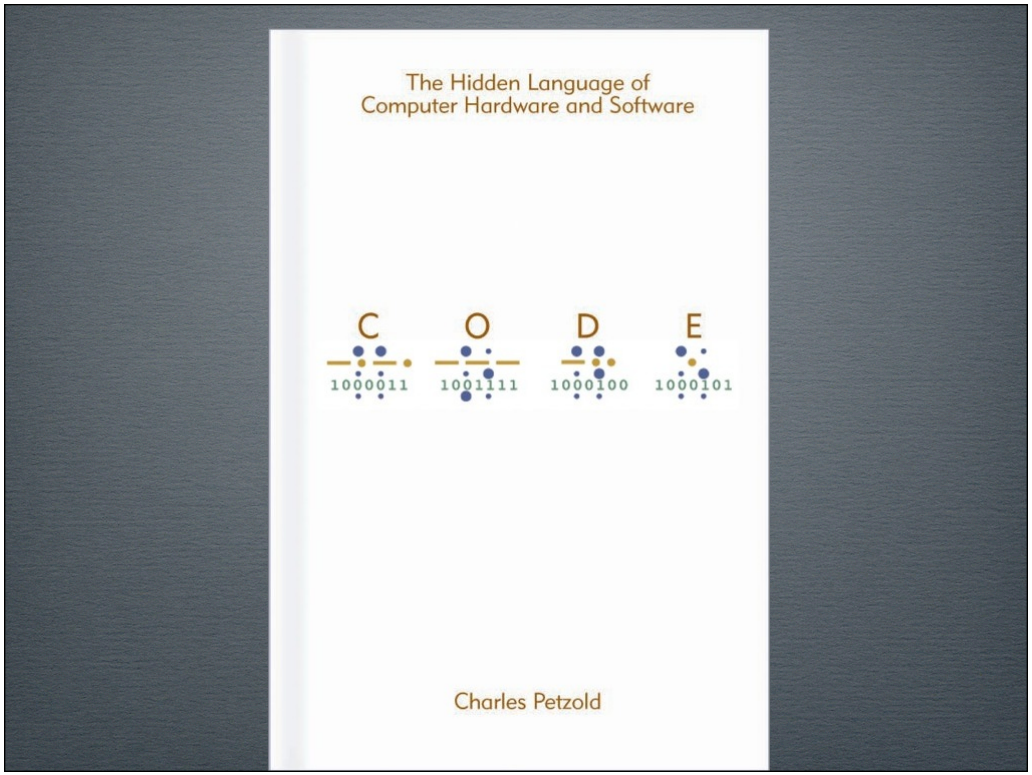


Now, I'm into instant gratification, so without further delay, let's get into that Modem explanation in comparison to a router. The naming modem is a word made up of two other words, otherwise known as a Portmanteau http://en.wikipedia.org/wiki/Portmanteau like wikipedia's favorite example

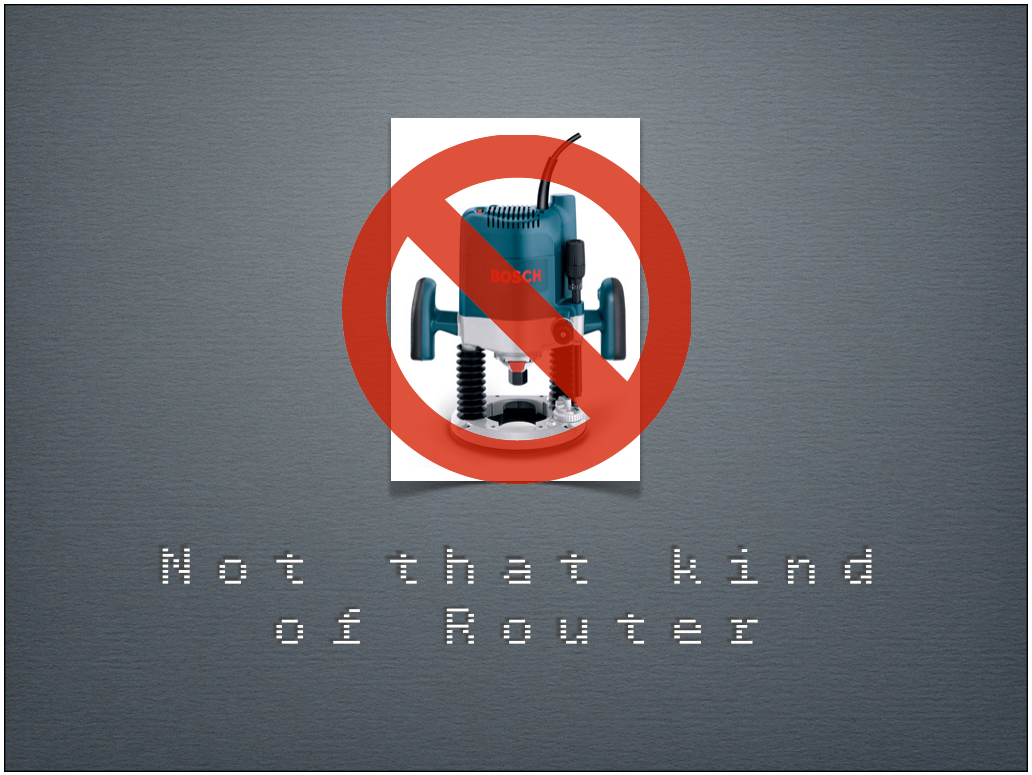
the Spork, and the concept of a modem has to do with receiving a 'physical' electrical pulse or analog signal over some sort of media meaning what cabling or other pathway it passed through to get to our box,

the media we deal with traditionally is usually copper, and the job of modems is to convert an analog signal to a digital standard, or a series of zero's and ones interpreted via Modulation and demodulation. And I can explain that concept by doing the electric boogaloo - wavy over here and pulsing in a standardized way on the other side. Imagine there's a metronome counting out cycles and when on each tick, depending on where my right arm is doing the wave, the left arm converts that into a 0 or a one to transmit and you've got the concept behind modulation and demodulation, I'm using the metronome to help me decode the signal.

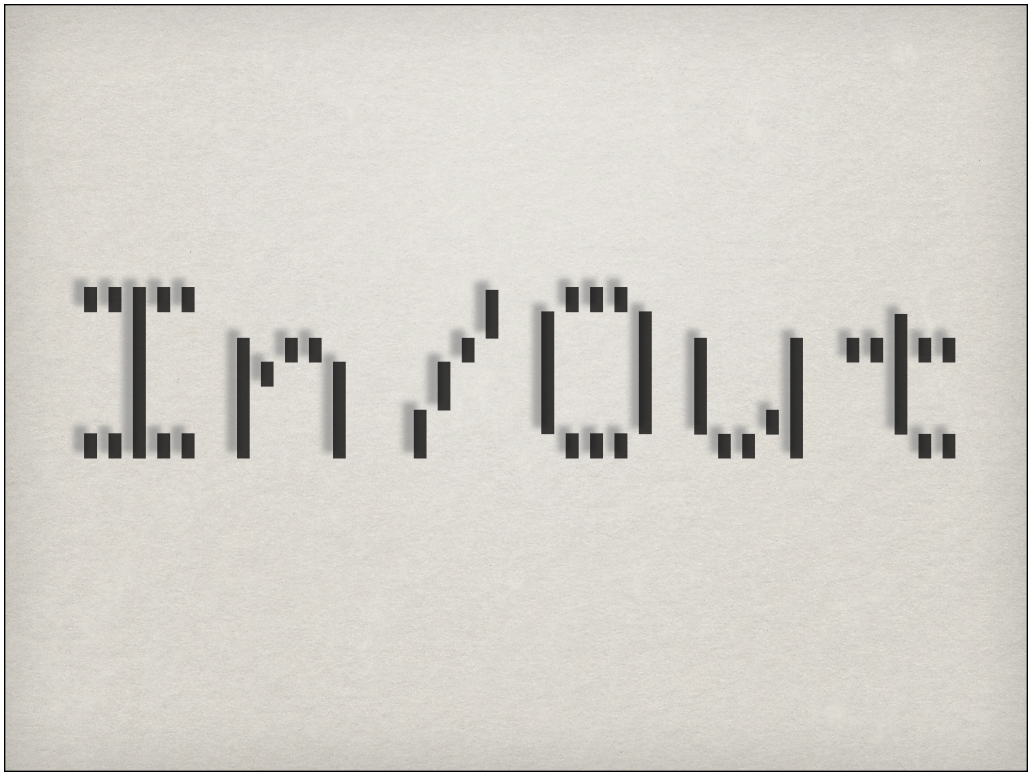
And that word signal, the audio connection implied is is an important one: the main distinguishing feature where you see the word modem used for new devices instead of the old telephone handset in the movie War Games is the fact there's an analog to digital conversion where the internet service provider has a signal they're sending, and for our computer to standardly interpret it wether it be WiMax or a cellular dongle you tether to your computer and the carriers signal gets converted to the communication a computer expects.



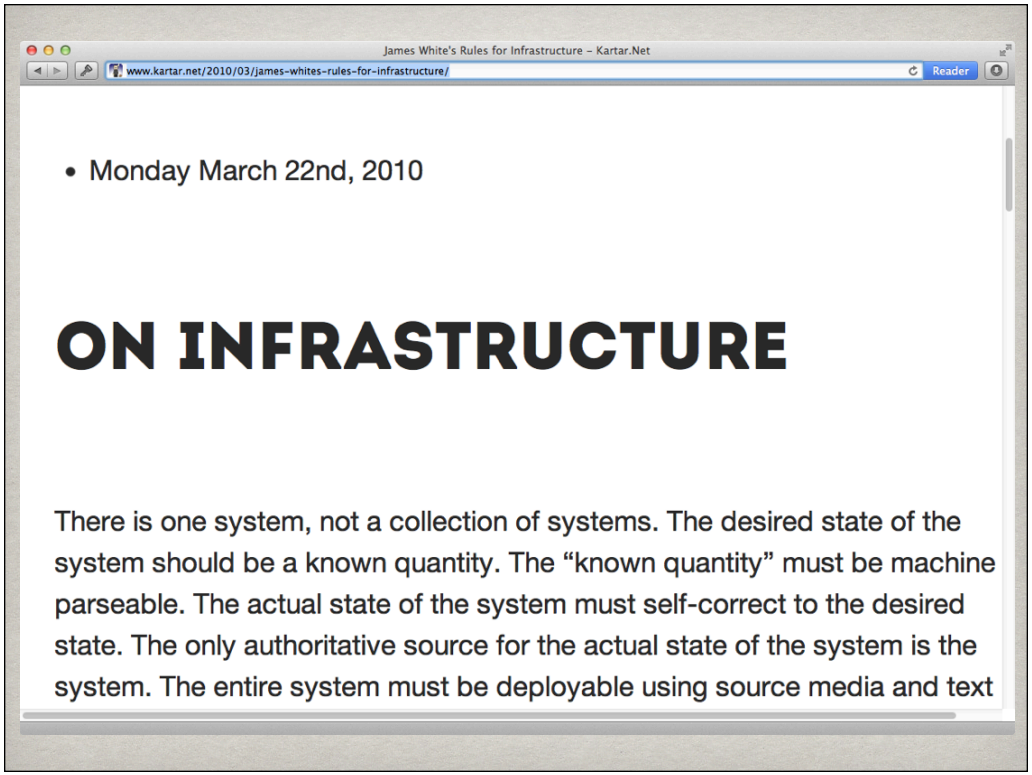
And this stuff is actually crucially interesting to me after reading the book Code which goes through the history of how Computers were invented, most primally to perform math, but through increasing more ingenious concepts everything we now know computers can do was enabled, including communication. I can guess that a lot of you didn't catch Ed Marczak's presentation from yesterday, and I can assure you you'll want to watch it as soon as these videos are available on the YouTubes. And if you liked his presentation you'll love this book. Without getting into the mathematical rabbit hole, those pulses my left arm was doing has to do with bits, which is actually another Portmaneau for binary digit.



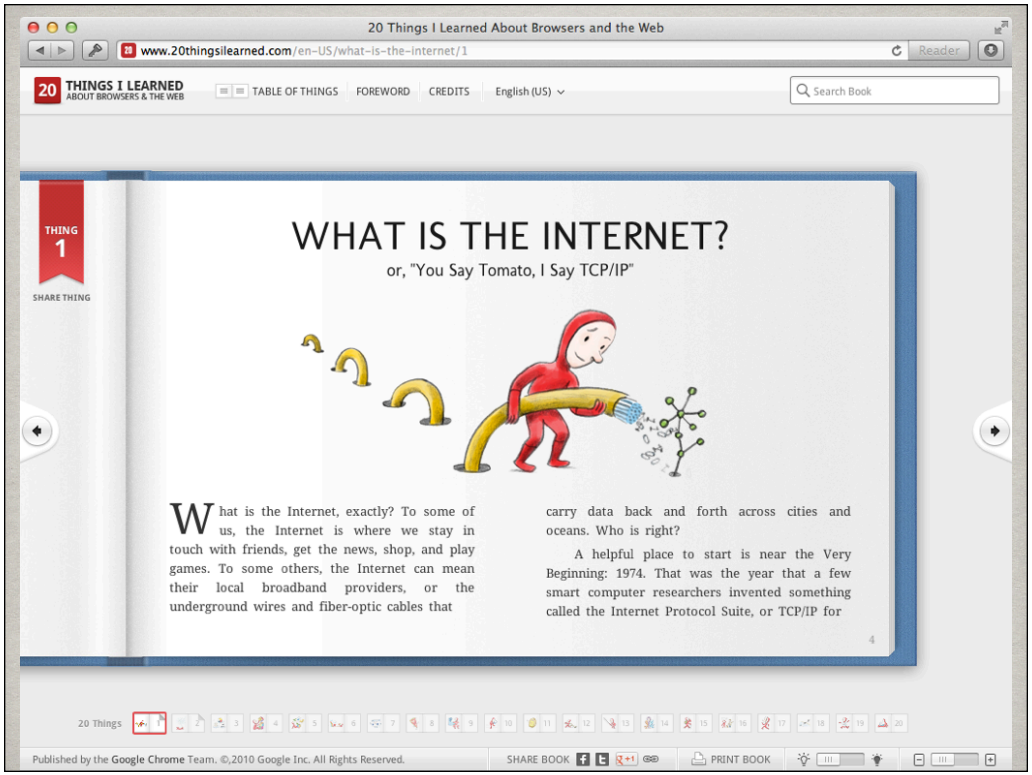
Enough fun and dancing, let's get back to routers, in comparison to a modem, which is conceptually simple,
A router is a pointer from one network segment to another, to designate what's inside the local network or outside - no physical carrier signal conversion, but its functionality can be bundled into a modem since



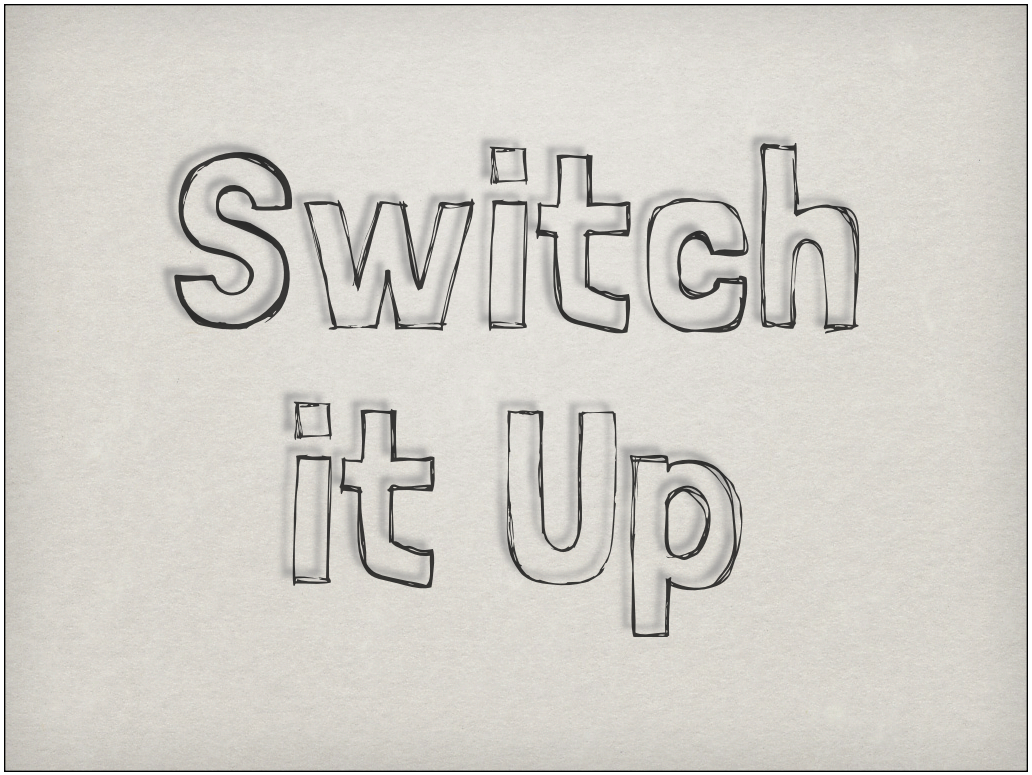
they're usually both found at where our network air-quotes 'physically' meets the internet.
And just to get sidetracked having fun about terminology, Apple doesn't refer to their computers as laptops, because they don't want to confine their usage to your lap, and to the same effect I get caught on using the singular when I talk about the system I administrate - it's all connected, and one thing in the singular environment I'm supporting affects everything else. I judge a good job posting if they spell the job title system administrator singular,



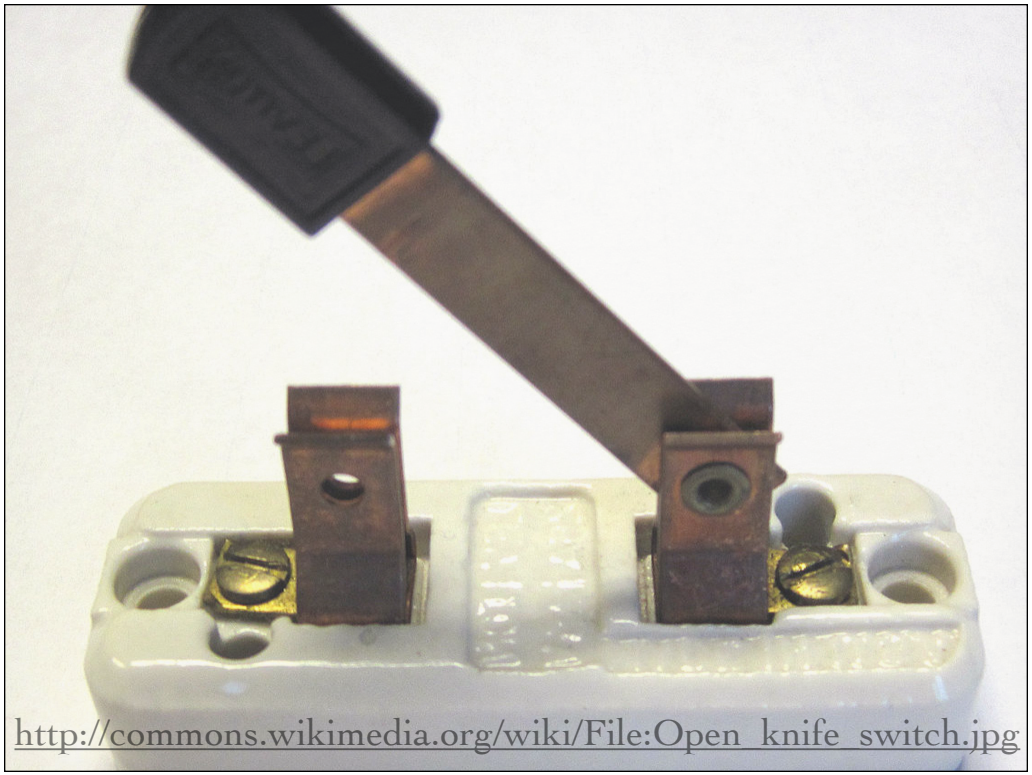
and here's a more eloquent diatribe that drilled that point home for me, it's james whites rules for infrastructure
http://www.kartar.net/2010/03/james-whites-rules-for-infrastructure/
There is one system, not a collection of systems - we talk about our LAN local area network as one of many, but what good is a computer that isn't connected to the internet, and isn't that one big entity? So all a router is doing is, it isn't necessarily involved in the minutia of decoding signals, it's more about making handoffs and finding paths.



Router's functionally also understand IP addresses, which sometimes folks who want to customize their home networks will take that ip addressing responsibility away from the combo modem/router they get from their ISP or internet service provider like Verizon or Comcast or Cox, time Warner. To summarize, routers have a specific technical purpose, whereas modems may integrate that functionality but are often named such due to the media or type of service or cabling that feeds them, for example phone lines in a DSL modem or coax for cable are when you hear this, whereas Routers are more generic. I think we can leave modem's behind for the rest of the talk - any questions just between modems and routers?

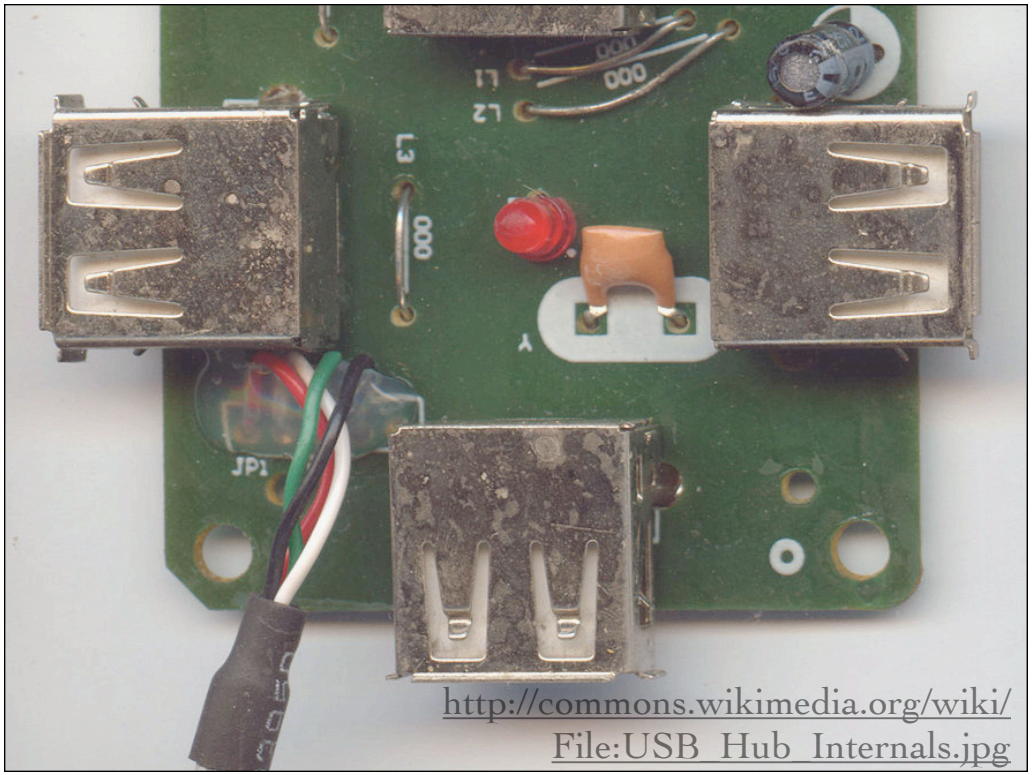


Okay so now we have the internet at our doorstep and the onramp is in place to make a highway metaphor, let's talk about the splitting up of that connection from a basic perspective, cabling. And in particular we'll talk about the gear that is often an integrated component in a router. Hopefully many of you weren't around for the debates of Switch vs. hub? Let's just instead assume we were all born yesterday and don't know what hubs are, so I can spread the pain. There are a bunch of ways hubs sucked, but history lessons - also boring. Instead, let's talk about the problems switches solved and we'll actually initially be answering our 'how do 0's and 1's get over the network' question.



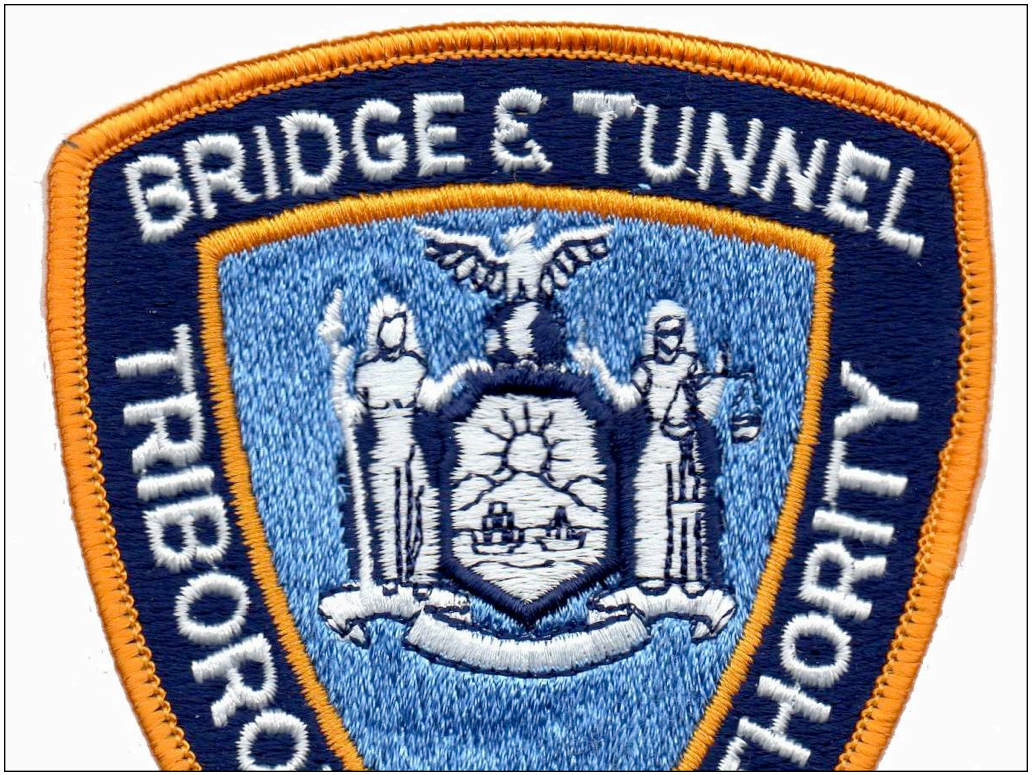
http://commons.wikimedia.org/wiki/File:Open_knife_switch.jpg

There are commonly two kinds of switches, and you may not have dealt all that much with the more expensive kind, which are referred to as 'smart' or 'managed'. Both kinds have logic going on in them, they are not, to use an electrical analogy, a cube tap or surge protector power strip. Each individual port, meaning place to plug in your cable, on a switch becomes aware of the device on the other end, wether it's a server, a UPS uninterruptible power supply, a laptop or desktop, or a godforesaken printer. What does it know about that device and how? Well, when the device tries to become a full-fledged, able to send+receive member of the network, it needs to get an identifier thats somewhat hardcoded recognized and spread out about it, and that's its MAC address. Media Access Control, which is a series of characters that every network communication device uses to, theoretically globally and for all time if not more realistically the next few years, uniquely identify itself.

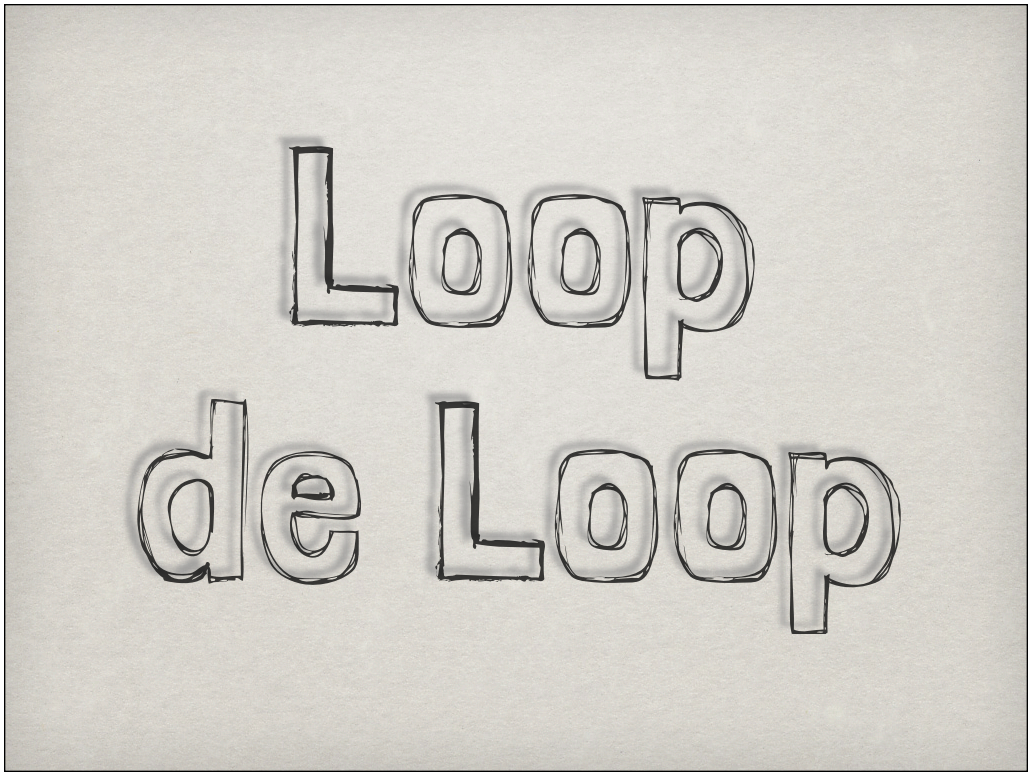


http://commons.wikimedia.org/wiki/File:USB_Hub_Internals.jpg

To bring it back to Hubs, they were so dumb, they never learned anything about anyone and ended up broadcasting everything everywhere everytime one node or point that could be talked to wanted to communicate with another.



Imagine there's no-charge toll lanes fed by separate roads before a tunnel: a switch allows a transmission to hop on the other side of the toll gate to go back through whichever exact other road it wants, or out the tunnel as a route it could be pointed to, and the toll gate also would govern any return trips.

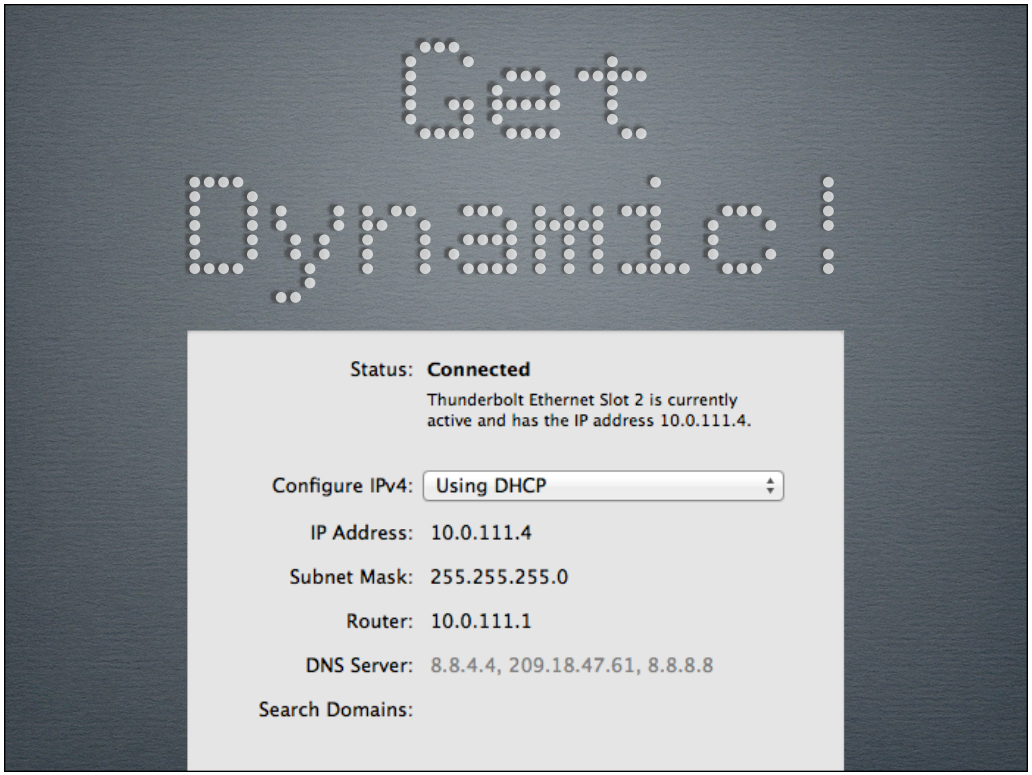


A hub is more like a paperboy mindlessly servicing a cul-de-sac, a circular road at a dead-end: every message gets thrown at every house since the paperboy doesn't care who's who. Even with a switch, if it's too cheap to prevent certain failure scenarios(cough belkin) you could do what's called loop a network, where the cleaning person sees a cable unplugged that's already in the switch and plugs the other end of it into the same switch thinking they knocked it out of place and therefore the whole network thinks the whole network is also on the other side of each end of that cable - long story short, it can go nuts if the switch doesn't police itself to detect and turn that off.
Switches are usually intelligent about keeping track of the MAC address it needs to return responses to so it can send data to and from the device, but say it's the first time a packet comes into the network for a host with a particular mac address, if it doesn't know or can't recall who a packet of data is for it'll just ask everybody once if they're the intended recipient before dropping it.

And if we're only talking about a few devices talking in a way they each know about each other no router is actually necessary, you could just manually set some things say on a Mac in the Network Pane of SysPrefs meaning system preferences.

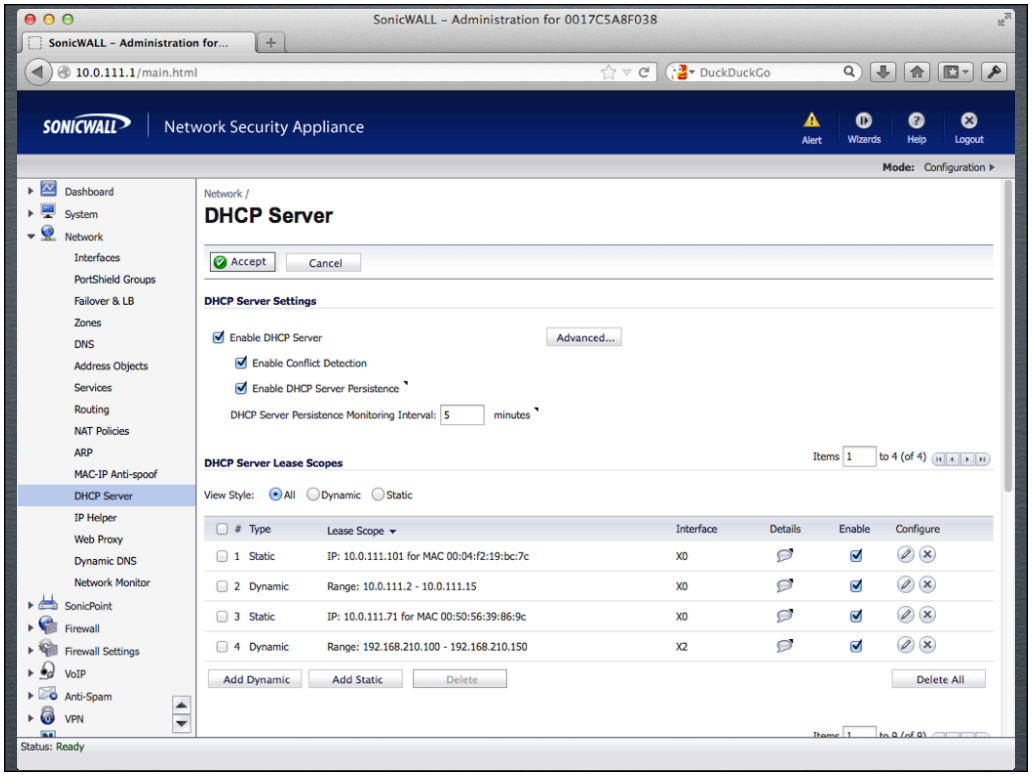
As a side note, you may hear terminology used for a smart managed switch versus something that can't be assigned an IP address, something about that being the difference between a layer 2 and three switch, besides the layer 3 being about $400 more expensive. There's a whole model chart seven-layer cake, which I will touch on just at the very end, but when starting out you only need to concentrate most critically on the first three: the physical, 'is it plugged in' layer, layer two is where MAC addresses and advanced features of WiFi and VLANs operate, and layer 3 is IP addresses.

But manual interaction with networking doesn't sound like fun, being without internet is the biggest annoyance there is which we should all be painfully familiar with by now, and the failure scenarios when things we manually interacted with change are annoying. It's also not the stuff you see most often or interact with in SysPrefs, you see stuff like DHCP which stands for dynamic host configuration protocol. A protocol means kind of the rules of the game or perhaps more appropriately the rules of engagement, so what DHCP does is it on the fly helps a 'host' which is another way to refer to a device or a node, get on a network and talk, it let's a process happen on-demand so that host can 'inherit' a configuration. And the config we're interested in it inheriting is an IP or internet protocol address. There's that protocol word again.



But let's jump with both feet into the rest of the settings you see: there's Subnet masks and Routers which is also referred to as the Gateway, and still more numbers should be present for the DNS or domain name systems server – possibly along with a search domain. We're concentrating, for now, on the two subtly different places DHCP can be implemented for an environment – either the same server you could administrate for other purposes like file sharing sets it up or a hardware appliance is delegated that role. In either case whats known as a pool is allotted to say after I've been allowed into a particular part of my network you'll get the next available address in the pool or a certain range handed to you.

When the DHCP service is running to hand stuff out, the DHCP server says I'll show you, mr host, how to find your way beyond this local network to say the internet by telling you where your router is and I'll let you know when you'd be better off finding other local hosts on your same network without even bothering the router. That's where the local subdivision of a greater network, or another portmanteau – I am all portmanteau all teh time, huh? that's where subnets comes in, and we specifically define how much of a greater network we can see or communicate with, with what's called the subnet mask.
Well a normal costume party mask only reveals as much as we want to be on display, so the metaphor works here: you don't need to go through the router when it's not blocked by the mask.



I had said we weren't going to get too math-heavy, so let's just leave it that most common subnet mask let's you communicate directly with anything that has the first three numbered sections the same as yours.

All of this can seem kindof dry, so as a quick departure let's discuss why windows folks want to use a windows server for DHCP, and why that usually ends up sucking for us mac folk: The last two things in that sys pref view are DNS server and search domain. Windows admins want to be able to dynamically find hosts by their assigned hostname, but when they're handed out an IP address dynamically by DHCP, if it's a windows server doing that handout they can tell everybody else where to find that host. Except that's only semi-guaranteed to work for windows hosts. Windows servers don't update certain DNS records for Macs properly, so that neat trick ends up at best being accurate for a small period of time or, what's more common, ends up with the pointer going to a now old and reassigned by DHCP IP address when people look for that macs hostname. I personally also like it when the networking team guarantees the appliances they support, which we need to perform other functions anyway, often you get DHCP for free and don't require as much dynamic naming for hosts. Of course, if you weren't aware, you can statically assign IP addresses based on the MAC address which is a nice failsafe if something loses its manual assignment... except with things like thunderbolt ethernet adapters... which would therefore allow any other computer using that adapter to receive the same static assignment.

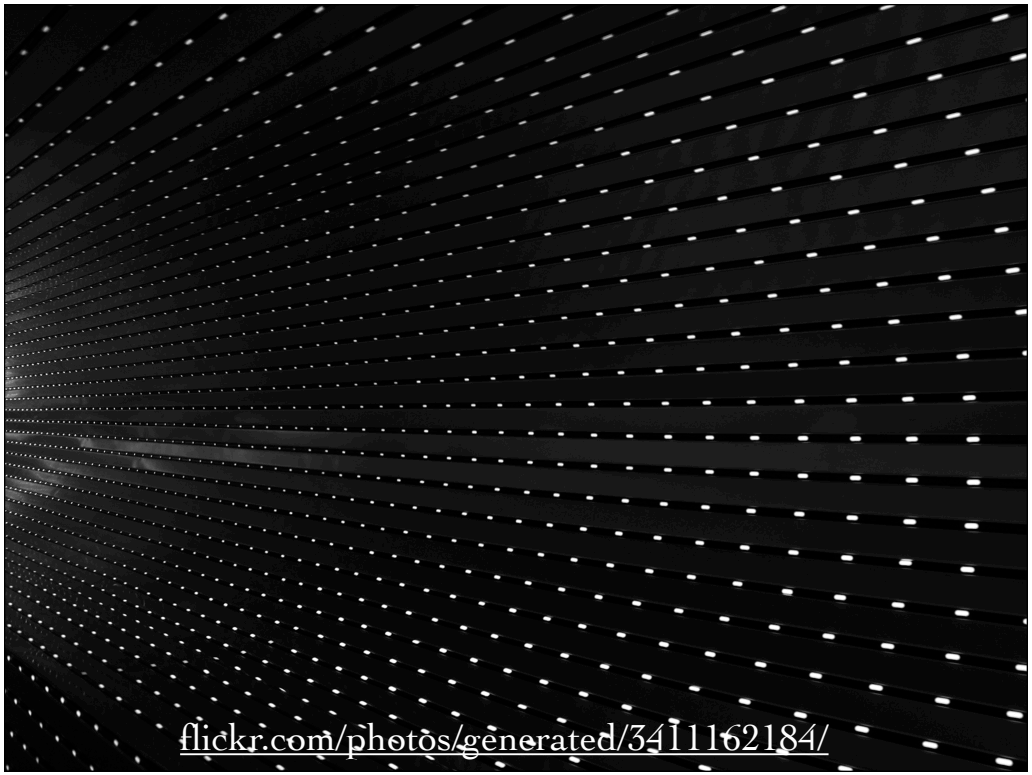
So as part of the DHCP protocol of handing out settings, it also helps you do name-to-number lookups by pointing you at the DNS service. We can of course either run that internally or look straight outside, but if we want to set up our own named domain to build up a hostname from, like mini.private, we'd like to not have to type .private every time. That's where the search domain comes in, telling the client that if it looks for just 'mini' the network can interpret that as mini.private and send the composited name out when it's doing a DNS lookup.

commons.wikimedia.org/wiki/File:Crm_post_office_car.jpg

Alright that got complex for a bit, I used the terms manual and static in close proximity, is everyone okay so far? Too mind-numbingly basic? Let me just finish off one last hardware definitions before we move on to practical, mac-focused questions Firewalls are all about the fact that computers need to allow communication by a process of listening and sending with a systematic division of its main channel of communication. Our IP address is a portal through which we see and are seen by the network, but the machine is sending all sorts of messages even without a valid address and expecting to have that routed out and back in properly. A simple example may be that an ssh session can be open while a web browser is open. Standards have been agreed upon so that ports are defined for every class of information you'd need to send, and as the messages are returned, ports are the slot through which that information is returned. On the receiving end of a request for information, like a web server seeing a request for the same page however many other people are trying to access, the request is assigned a number so the appropriate response is returned to the appropriate requester, and when it gets back to the machine the slot is referred to as a port.

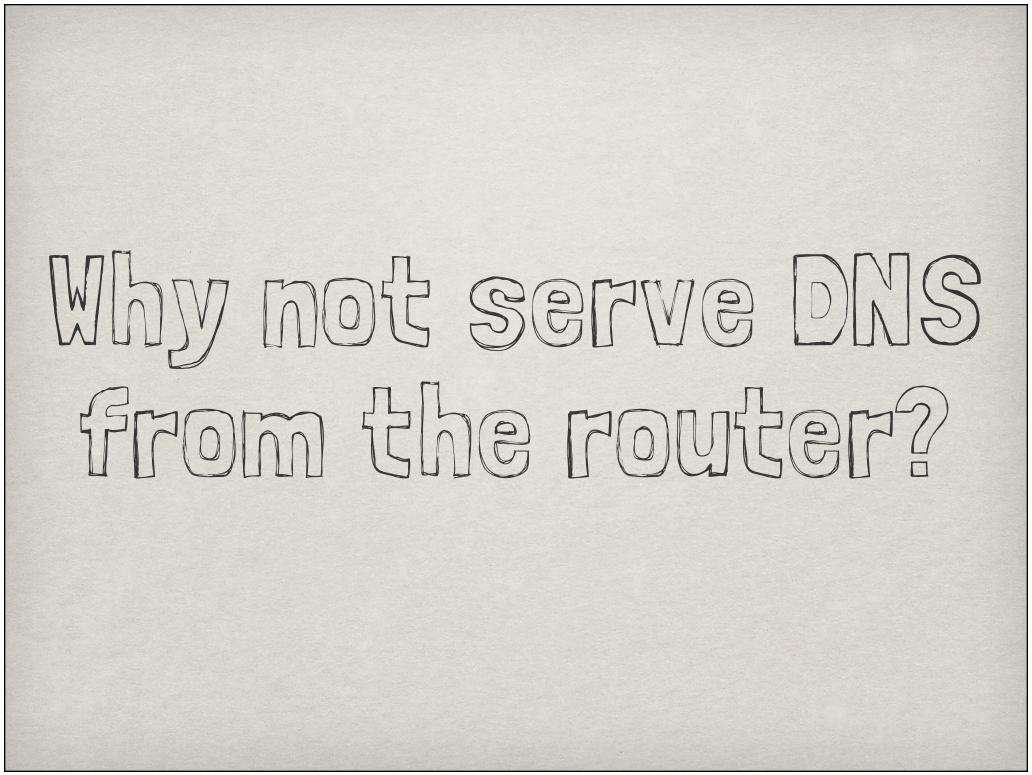
Just like DHCP servers, Firewalls can be software or hardware, but whichever is active, it makes decisions based on ports and IP addresses. You can leave the defaults of a firewall on, which is to block all quote-unquote 'incoming connections', because it's like the mechanism by which sandboxing acts on when you request access to the filesystem in a Mountain Lion or greater OS - by you showing intent to for example open a file, the OS lets the application you're running show a view of the files and open the one you choose. Firewalls interpret the concept of an established connection once your computer has 'hooked up' a channel of communication with them. Firewall appliances commonly being advanced routers mean they have a lot of other useful features, including making decisions based on IP address or MAC address, for example: bandwidth 'shaping,' or dedicating bandwidth to certain hosts.

When outside the organizations local network, if there are services that should be accessible because they can perform well over the internet, a secure connection can be established with what's called a Virtual Private Network. A hardware appliance can set that up, or again, a server with standard directory services can use that user database to provide authentication when folks connect. After they're allowed in, DHCP takes over according with the subnet it's configured to give access to.



A slightly more advanced topic can be split tunnels, as you don't necessarily want extra load on the internet connection of wherever you're making that VPN connection to, so you can say every connection for the rest of the internet doesn't need to be routed through the remote network. The common way a VPN works is a network interface is simulated in software with that handshake to the remote VPN endpoint, and from that point forward it's like an SSH connection where all communication across the wire is considered encrypted and not able to be read if intercepted.

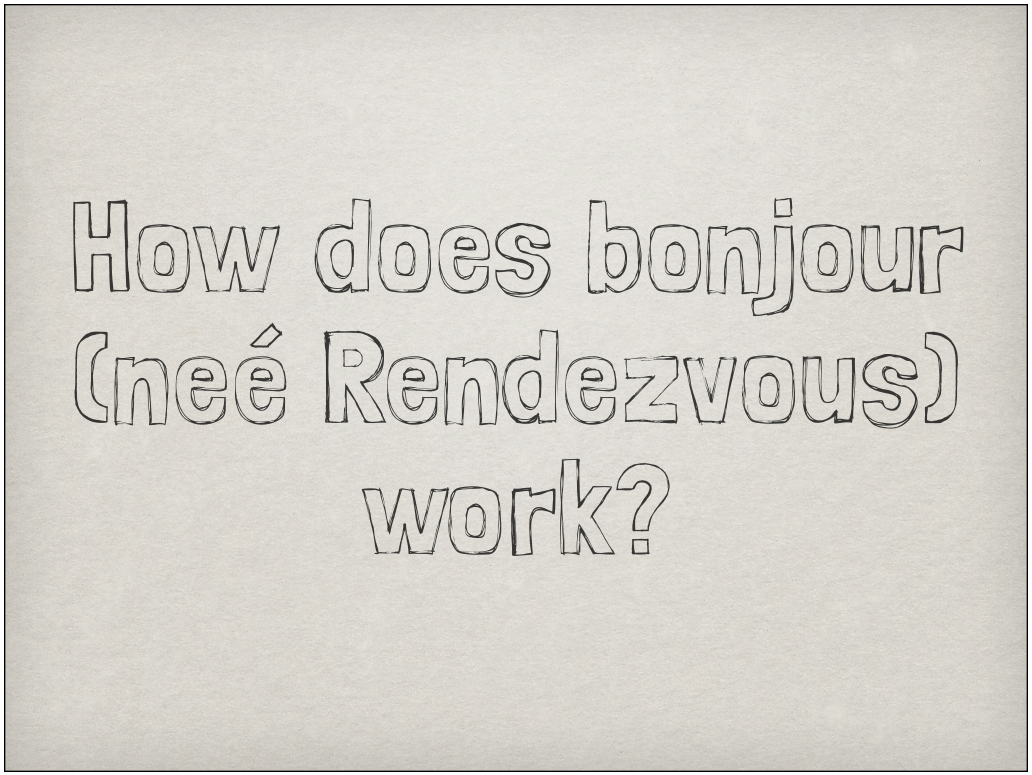
The last topic I'll be mentioning just briefly enough to say I talked about it at all is WiFi. A common point of confusion for people when it comes to setting up even a home network is how little you can optionally do with a wireless access point or wifi base station. They can often be routers for a network if you need that functionality, but often people are too lazy and put them in what's called transparent or bridge mode, which is actually the first term they used for a switch was a bridge. There are two modern developments regarding WiFi, one is the addition of a separate piece of hardware called a controller and more recently is the pushing of the logic employed by a controller down to the access points themselves. A WiFi controller helps the handoff between base stations by ensuring the presence of the same authentication process to validate access across a bunch of wireless access points, or WAPs. You may also want to encourage sign-up of guests or give them a usage agreement before they get on the WiFi network, which can be provided by a controller. Some environments have a static, unchanging single password for their WiFi wether guest or staff, they don't worry about bandwidth usage by guests, and they don't worry about access to the resources on the internal network being restricted or not, whereas others search out rogue access points or things trying to offer services to other clients on the same network. It really starts with policy and then there's multiple ways to restrict or allow access based on those requirements.



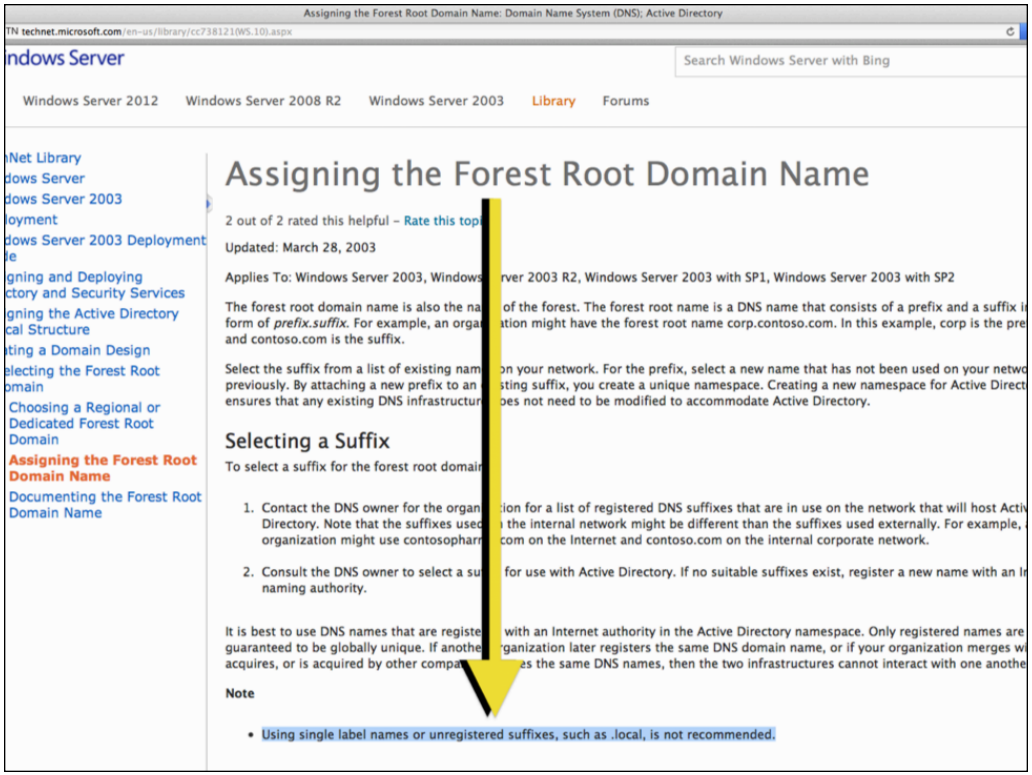
I think that covers the absolute minimum of the standard stuff a networking newbie needs to know about what the common moving parts are and how they interoperate. Let's get into some answerable and less defined questions about networking, starting with an interesting theoretical question:
Why don't networking appliances like routers act as DNS servers? My current favorite reasoning behind why firewall and router vendors commonly DON'T decide to do this is that the referral process whereby DNS does lookups to upstream, servers that are considered 'authoritative' for DNS responses means that at all times we're trusting those responses as long as they vouch for themselves by just literally telling us they're authoritative - it's the equivalent to a web browser running untrusted code, routers are what you're network relies upon, and if you're upstream DNS server is compromised in some way you are way more likely to be socially engineered by phishing attacks.

That being said. Yes, enthusiasts find running a DNS server on the router a way to offload that function from a server OS running on that local network, since that information can be pretty static or unchanging on your LAN, and there's firmware you can flash certain models of consumer or prosumer hardware running broadcom chipsets, with names like tomato and DD-wrt.

So that was a tad over-geeky, how about How does AirDrop work?
It sets up a wifi adhoc network for the purposes of filesharing, and with a hack can even be enabled over ethernet, in which case you're using it less for the network discovery and connection than for the simplified authentication handshake after the connection is made via bonjour.



Taking a step back, How does bonjour(neé Rendezvous) work? Is it proprietary? Does it exist on Windows/elsewhere?
Bonjour is a standard ratified in 2003 to govern the dynamic configuration of devices with link-local addresses so they can still talk with hostnames on a network - so lets work backwards from there, what's link local - if you don't have a DHCP server or router on a network, but the device can tell there's something that it can communicate with it will eventually assign itself an address that starts with 169, which you may have seen. As part of the bonjour or zeroconf(which is what they called it when ratifying) spec, There are two other parts besides making sure nobody else has your linklocal address to map to your localhostname - 1. with multicast, meaning one-to-many transmissions, you send requests so you can find devices by hostname without a DNS server and 2. you can tell specific services like a printer apart from an appleTV, which is also be called service discovery or DNS-SD. By the way, there's avahi to enable bonjour on Linux and Apple makes an installer for Windows as well. And another more fun note, is the sleep proxy service introduced during 10.6 which is how you can do some semblance to wake-on-lan without ethernet, that also utilizes bonjour, as it is a flexible and extensible standard.



Why is dot local domains kryptonite for us?
What did the consortium of vendors, including microsoft, choose to use as the search domain(remember we discussed those) for the zeroconf network? dotlocal. Way back in 2003 Microsoft went so far as to recommend against using that name for your domain in their docs, even though it's all over examples they use. They've since switched to contoso or fabrikham. So when a computer wants to send a message to something it assumes is a bonjour hosts address, it assumes it needs to use multicast instead of unicast, unicast being what we normally use without bonjour if we were talking to a host whose IP address we already knew or we knew to rely on the DNS server to point us to. The DNS plumbing in Macs have been overhauled multiple times to work around this, since it would always prefer the multicast response, for example if you had a host incorrectly broadcasting a bonjour name like 'server' when you wanted to get to the Windows host name server.local.

41

So hopefully that's something like we were looking for in the way of content, quick wrap-up before we get to full-on Q&A:

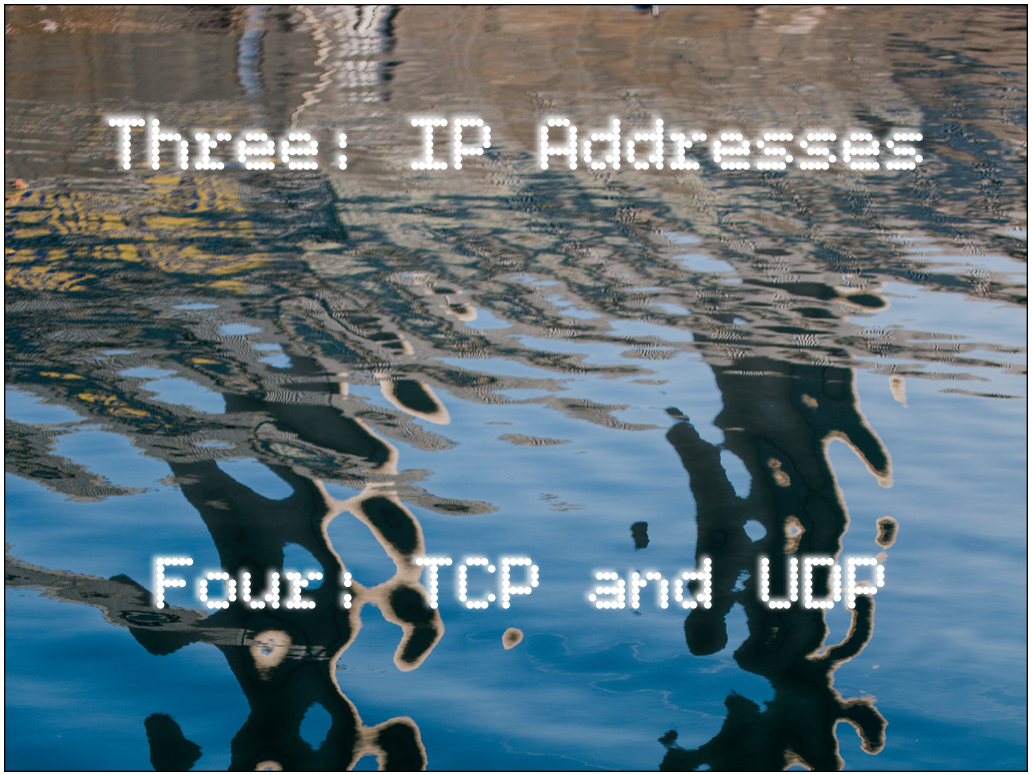
Modems most often hand off a carrier signal from an internet service provider and convert it to digital

http://www.geograph.ie/photo/3322334

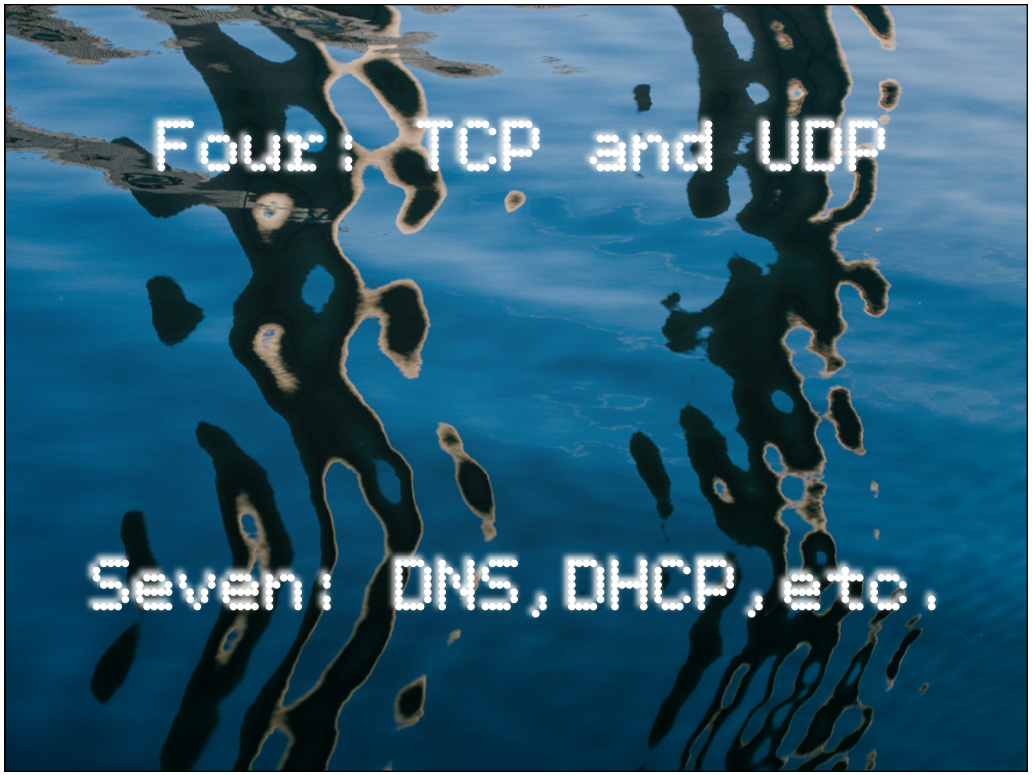
Routers sit at the border between networks and help create paths and forwards requests

Switches hear MAC addresses when devices send information and help route it back

Network stack layers we commonly interact with are:
- layer one for physical connections like copper ethernet-slash-fiber-slash-coax or radio waves for WiFi
- two where the MAC address actually lives and more complicated information like VLAN tagging happens, but I promised I wouldn't discuss that



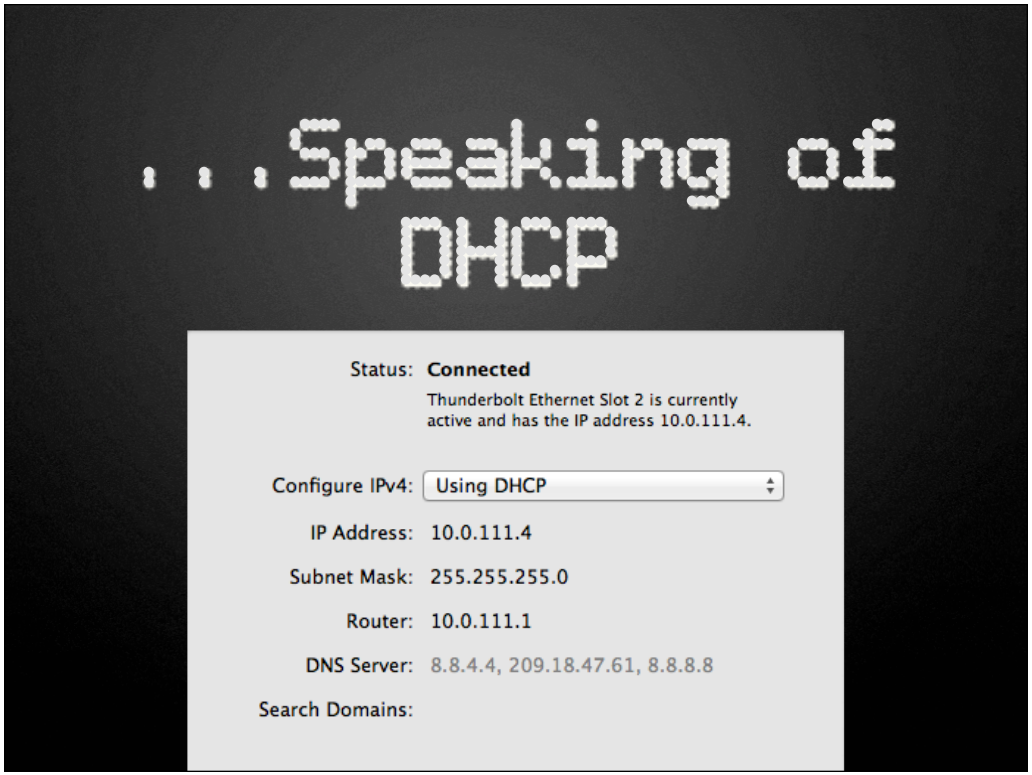
– and three is where IP addresses are
– since we're in wrapup mode, it might be nice to mention what helps govern how IP gets implemented is the transmission control protocol you hear mentioned, the other part of TCP/IP, which is up at layer 4 with other protocols like UDP which is what DNS uses.



– and three is where IP addresses are
– since we're in wrapup mode, it might be nice to mention what helps govern how IP gets implemented is the transmission control protocol you hear mentioned, the other part of TCP/IP, which is up at layer 4 with other protocols like UDP which is what DNS uses.

DNS itself is up in 7 with AFP, HTTP and DHCP, if you're also curious about those.

DNS itself is up in 7 with AFP, HTTP and DHCP, if you're also curious about those.



speaking of which, DHCP gets inherited after seeking out and successfully talking to either a router or server, and the information it gets provided with is:
- what IP it should have on the network,
- where the boundaries are when it comes to hosts it should be able to directly connect to on the local network not figuratively 'blocked' by the subnet mask
- where the router is
- which DNS server it should specifically ask to do the name to number conversion, wether just for within the local network or otherwise
and what domain name can be tagged onto the end of DNS lookups for common requests, called the search domain
And link-local I'm referring to as a name for the 169 address you get when you can tell you're connected to network gear but a DHCP server hasn't handed you info yet so you self-assign an address.

Bonjour can take over and allow discovery of services and hostnames so you can do a good amount of communication without the rest of that infrastructure cooperating.

PENNSTATE

MACADMINS CONFERENCE 2013

Enough Networking To Be Dangerous

Allister Banks abanks@318.com @sacrilicious

Thanks!