Wi-Fi
The Good, the Bad, & the Ugly
By Mike Quinn
Three Main Types of Data Connections

- Point-to-Point
- Broadcast
- Network
Point-to-Point

- Tin can & string
- USB cable
- Lightning cable
- Ethernet Cable
- Fiber optics
- whisper

Pros:
Much More Secure (harder to listen in on)
You know who you’re talking to

Cons:
You can only talk to 1 person

Examples:
USB cable between your phone or printer and computer
Broadcast

- Wi-Fi
- BlueTooth
- NFC
- Shouting

Pros:
Easy to use
Can be used in a point-to-point mode (but everyone can still hear you)

Cons:
Not secure at all - everybody hears you
Difficult to be sure who you’re talking to
Network

- Combo of p2p & broadcast
- Like a “gossip line”

Pro:
You can talk to anyone on the network
Uses routers and switches as the “agents” to switch from 1 point-to-point or broadcast area to another

Con:
Can’t be entirely sure of who you’re talking to or whose listening (at least without “extra” stuff)
Relies on “truthfullness”
Wi-Fi is an RF Broadcast

- Many Flavors
  - Wi-Fi 1 in 1999 (802.11b)
    - 2.4 GHz @ 11 Mbps
  - Wi-Fi 2 in 1999 (802.11a)
    - 5 GHz @ 11 Mbps
  - Wi-Fi-3 in 2003 (802.11g)
    - 2.4 GHz @ 54 Mbps
  - Wi-Fi 4 in 2009 (802.11n)
    - 2.4 & 5 GHz @ 600 Mbps
    - MIMO
  - Wi-Fi 5 in 2014 (802.11ac)
    - 2.4 & 5 GHz @ ~1.3 Gbps
    - 1 user @ ~500Mbps
    - Multiple users at a time
  - Wi-Fi 6 coming soon (802.11ax)
    - 1-7GHz @ ~11 Gbps

Wi-Fi does not stand for anything - it’s a trademark of the Wi-Fi Alliance
Light (the colors red thru violet are immediately after EHF on the chart above)

5G will be in the 600MHz to 6Ghz area (the same as 4G LTE), but will also add 24-86 GHz in the EHF area in the chart above
Only 5G in the 24-86 GHz will be significantly faster than current 4G LTE

Wi-Fi 1-3 are not widely used anymore
MIMO = Multiple-Input and Multiple-Output (uses multiple antennas for input and output)
MU-MIMO = Multi-User Multiple-Input and Multiple-Output
The Good

- Don’t need to run wires through the house
- Can connect to networks at coffee shops without wires
- Mature technology which is fast enough for most internet applications
- Many printers can be hooked up via Wi-Fi now, rather than USB
The Good

- Lots of neat features in Wi-Fi-routers
  - Guest networks
  - Dual Band (2.4 & 5 GHz)
  - Beam-forming
  - VPN server
  - QoS

- Mesh networks are getting pretty good

Guest networks - guest sign on to a different SSID than you use, and they can't see any of the devices on your home network, just get access to the internet

Beam-forming - the router increase the power to the proper antenna in the direction of the client device

VPN server - you can use VPN software on your phone or computer to connect to your home network. Most of you probably don’t need this feature, but it’s handy in some instances.

QoS - Quality of Service - good for things like a VOIP phone and streaming - to give it the highest priority, or if you’re a gamer to give your games high priority

Mesh networks - we’ll talk about those in a future slide
The Bad

- Broadcast technology
  - anybody can listen in
  - Use encryption (WPA2)
  - Use a VPN in an unencrypted environment unless you only use HTTPS: and encrypted e-mail (with secure certificates)
- Setup can be complicated because of “The Ugly”
- Configuration can be daunting if you want to do things that aren’t default

Even in an encrypted environment, even https: and encrypted e-mail can be messed with - someone on the same Wi-Fi can pretend to be your target website or mail server, and if you allow an insecure certificate, you can be fooled - more on this next month).

WPA3 (next generation connection standard) will actually take care of this problem by eliminating these “Man in the middle” attacks.
The Ugly

- 2.4 GHz is unregulated
  - Bluetooth
  - Wireless phones
  - Medical equipment
  - Baby Monitors
  - Garage door openers
- Microwave ovens can interfere
- Metal studs can attenuate the signal

Since 2.4 GHz is unregulated, lots of things use it.
The Ugly

- Your body will block Wi-Fi
- Health concerns
- Limited number of channels
  - 1, 6, 11 only non-overlapping on 2.4 GHz
  - 5 GHz has more channels
- Radar interferes with 5 GHz Wi-Fi

Your body block Wi-Fi because water is a good absorber of radio frequencies and you’re mostly water.

Routers have to stop transmitting and change channels if they detect a radar signal (DFS)
Choosing a channel

- Your router will try to choose a good channel
  - Better at it for 5 GHz than 2.4
- If you want more control, get a Wi-Fi Analyzer app for your smartphone
  - Many apps will tell you what channels are better
  - Visually determine if your Wi-Fi is in a good spot
  - Log in to the router and change the channel
- If you name your 2.4 & 5 GHz SSID the same, the client device will choose.

Using the same SSID for both is usually good - Androids have logic to choose the best throughput that’s supposed to be pretty good. This is especially useful in a house where the 5 GHz gets weak in some of the rooms, so you might want to switch to the 2.4 GHz.

Personally, I’ve found that phones aren’t very aggressive about switching to a better throughput Wi-Fi if they can still talk to the current Wi-Fi, so in my house, we have different SSIDs for 2.4 and 5 GHz so we can force which one we want to connect through. YMMV (Your mileage may vary).
Connecting to Wi-Fi

- Encrypted login
  - WEP & WPA
    - Password based
    - “Cracked” - never use them
  - WPA2
    - Password based
    - Current encryption you should use
  - WPS
    - “Push button” login
    - Don’t use it - too easy to un-encrypt
  - WPA3
    - Coming soon - definitely want to use
  - Wi-Fi EasyConnect
    - QR codes
- Captive Portal
  - NOT encrypted

WPS allows you to push a button on your router, and have your device immediately connect without entering a password. The problem is that behind the scenes it uses a randomly generated 7-digit pin code - a computer can quickly run through the 10 million codes to decrypt your data.

Captive Portal simply means you have to go to a web page and login in some way shape or form before you can use the network. It’s a bit annoying because if you’re using an email program, it just sits there and can’t use the network until you bring up a browser and try to browse somewhere. Most phones and computers these days are aware of this and will automatically bring up the browser. If captive portal is being used….

Wi-Fi EasyConnect - you scan a QR code on your router, then a QR code on your device, and they’re securely connected. This is very handy for “internet of things” - doorbells, door locks, smart lites, etc, where the device only has an interface to a smart phone.
Helpful Additions

- Booster (Repeater)
  - Just repeats what it hears
  - Old tech
- Range Extender
  - Rebroadcasts on a different channel
  - By default uses a separate SSID

Since a repeater repeats what it hears, it effectively cuts the bandwidth in half.

You can use the same SSID, but most devices won't switch the channel until the original signal is gone, so if you're wandering around the house, your performance will drop to almost nothing before the phone will switch. With a separate SSID, you have to manually switch (turning Wi-Fi off and back on, will also do it on phones, since they will then choose the strongest signal that the phone knows the password for).
Helpful Additions

- Network Extender
  - Uses “backhaul” to extend
  - Allow much faster Wi-Fi
- Mesh
  - Intelligent range extending
  - Knows which device the client is connected to
  - Can use “backhaul” to be even faster
  - Figures out the best paths & channels to use to create the mesh.

A “backhaul” is just a physical port (usually ethernet) on the extender, so that the extender can forward the data back to the Wi-Fi router via the cable rather than rebroadcasting it.
Example Mesh Network

- Xfinity XG6 (Bridge Mode; no hotspot; 1Gbit Plan)
- TP-Link TL-SG108
- 4x Cat6 lines to Rooms in House, 1x Cat6 to Xfinity Home Security Router
- RBS50
- 2x Ring Floodlight Cam, Roku Streaming Stick+
- Samsung TV
- Onkyo Receiver
- PowerHub for Blinds
- Arlo Pro Base Station
- RBS50
- 2x Ring Pro Doorbells, 2x Ring Chimes, 2x Roku Streaming Sticks, 2x Thermostats, 2x LG Appliances, Blu-ray Player, Solar System
- TP-Link TL-SG105
- 1x Ring Floodlight Cam, GE Appliance
- 2x iPhones, 2x iPads, MacBook Pro, MacBook Air, Dell Laptop
- iMac
- HP Printer
- MyQ
Things you should do

● At home
  ○ Change your SSID (optional)
  ○ Change your password from the one on the box (optional, but good idea)
  ○ Create guest network if you ever give the password to someone you don’t trust 100%
Things you should do

- Using an outside network
  - If you connect with a password, be sure it’s WPA2-PSK
  - Use a VPN (Virtual Private Network) if no password, captive portal, WPA or WEP, or doing really private stuff.
    - Extra cost, but not too expensive if you do it a lot
  - Always use https:// on any website you don’t want “sniffed”
    - NEVER go on if a browser informs you the certificate is invalid

With WPA2-PSK everybody who logs onto the network can decrypt everybody else’s traffic just by seeing the logon. If they missed the logon, they can forcibly log you out, and when your phone logs back on, they’ll see the new logon.

Using HTTPS:// uses a second level of encryption so the fact that your packets can be decrypted doesn’t help. HTTPS:// can only be hacked by a Man in the Middle attack, but that causes the site certificate to be invalid.

VPNs sends traffic to someone’s server out in the world, and all your traffic looks like it’s coming from that server. What you send is encrypted. Some secure websites don’t work properly with a VPN (schwab.com is one that comes to mind - I have to shut off my VPN to talk to schwab).

We’ll talk more about VPNs next month.
Things you should do

- Verify that Security is WPA2-PSK
  - Android- press on current network name and choose “Manage Network settings”, click “Show advanced options”, and it’ll show you this.
  - iOS- no easy way to do it. If Password was 16 characters, it’s probably WEP, otherwise, it’s probably WPA2
    ■ There are 3rd party apps that will show you.

Don’t need to do this if you didn’t enter a password to logon.

Remember, captive portal, where you log in via a web page, has no encryption…..
Not the lock icon and the https:// in front of the URL. I just typed google.com - google automatically converted it to https://. Most good websites will do that automatically, but you can force it by manually typing the https://. If they don’t support https://, it won’t bring up the website.

Baidu.com is the Chinese google. Note they do not switch over to https:// and there’s no lock icon. However, in their case, if you type https://baidu.com, they will use https:// and you’ll get the lock icon.
Things you should NOT do

Don’t continue on to websites that put this kind of dialog up. It means the certificate that’s used by the website cannot validate that they are who they say they are. Sometimes, this is an oversight by the website because the certificate expired (they have to be renewed every few years), but it can also mean that someone is impersonating the website.