TC 4.0 Wireless networks

From last time:

Network speed testing

There are two aspects of this: your connection to the network, and the network to the internet.

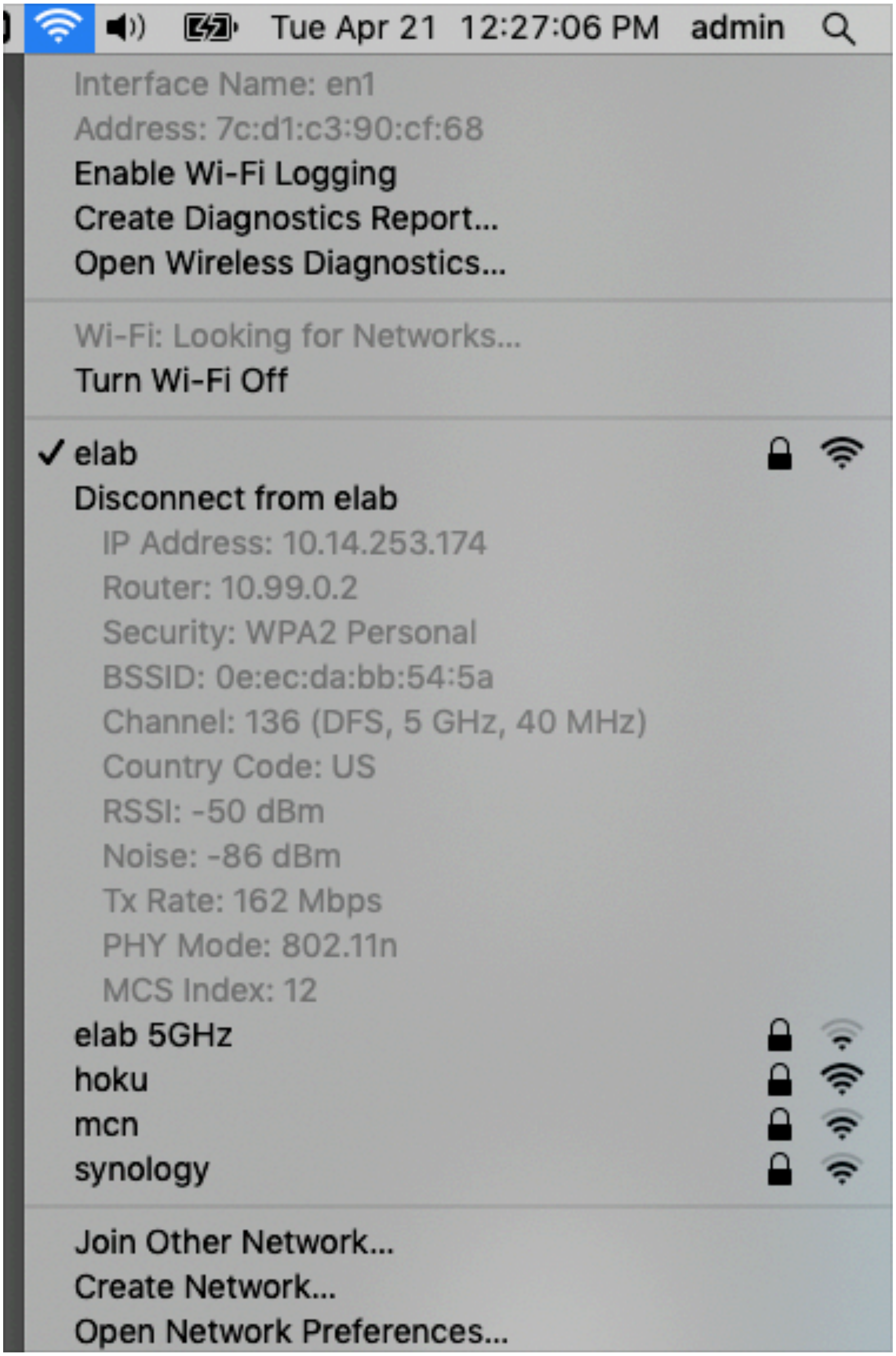
Wired:

If you are connected by a wire (e.g. ethernet) you can expect that the speed is limited only by the router and/or the internet connection to the internet. This could be an issue if:

1. cables are worn or damaged
2. your ethernet drivers are defective
3. there is physical damage to the ports on your computer, router or switch

Wireless:

This is more fun and nebulous. There is a solution: on a mac, hold option while touching the fan icon at the upper right:



Tue Apr 21 12:27:06 PM admin

Interface Name: en1
Address: 7c:d1:c3:90:cf:68
Enable Wi-Fi Logging
Create Diagnostics Report...
Open Wireless Diagnostics...

Wi-Fi: Looking for Networks...
Turn Wi-Fi Off

✓ elab
Disconnect from elab
IP Address: 10.14.253.174
Router: 10.99.0.2
Security: WPA2 Personal
BSSID: 0e:ec:da:bb:54:5a
Channel: 136 (DFS, 5 GHz, 40 MHz)
Country Code: US
RSSI: -50 dBm
Noise: -86 dBm
Tx Rate: 162 Mbps
PHY Mode: 802.11n
MCS Index: 12
elab 5GHz
hoku
mcn
synology

Join Other Network...
Create Network...
Open Network Preferences...

There is a great deal here:

1. look at the network name, make sure this is the one you intend
2. IP address is the address given to you by the DHCP server on the router. DHCP is where a pool of addresses is “leased” to computers for temporary use. Notice that the third octet is 253.

Look for 253, 254 or other numbers like this to detect if you have a DHCP address.

3. Security: WPA2 Personal means the password authentication is held on the router, not at one central server (usually RADIUS), in which case you'd see WPA2 Enterprise. RADIUS is what we used to use in dial-up modem days, it stands for remote access dial in user services.
4. BSSID is the MAC address of the wireless card in the router or access point. This is important if you find you are joining a distant access point instead of the one you hoped for.
5. Channel and Country code are fixed by the access point and computer respectively. Note that the channel includes band, in this case 5 gHz. 2.4 gHz is the older wireless spectrum, which goes farther, but is slower. It is also susceptible to microwave ovens. 5 gHz is the newer faster network with shorter range, but higher speeds. The mHz (40 mHz) is the width of the channels used. Wider channels have higher speeds, but interfere more with other channels
6. RSSI is the signal strength (in minus numbers) so -50 is better than -70. Think of an elevator that goes underground or a submarine.
7. Noise is the same thing: smaller numbers are better, so -70 is better than -50.
8. Tx rate is transmission rate, the effective speed of your link. This may be faster than your internet connection, but it also impacts how fast you share files or download stuff on your local area network (LAN).
9. Related to this is PHY mode, which is the encoding on your wireless link, based on the iEEE 802.11 protocols: b is slowest at 11 mb/s, g is better (54 mb/s), n is even better, a is faster, and ac is the most common super fast one now, peaking at about 1300 mb/s.

What you might want to consider is trying this around your house or office and notice what changes, particularly if you have more access points, or MIMO (multiple in, multiple out) and band steering. More on this soon.

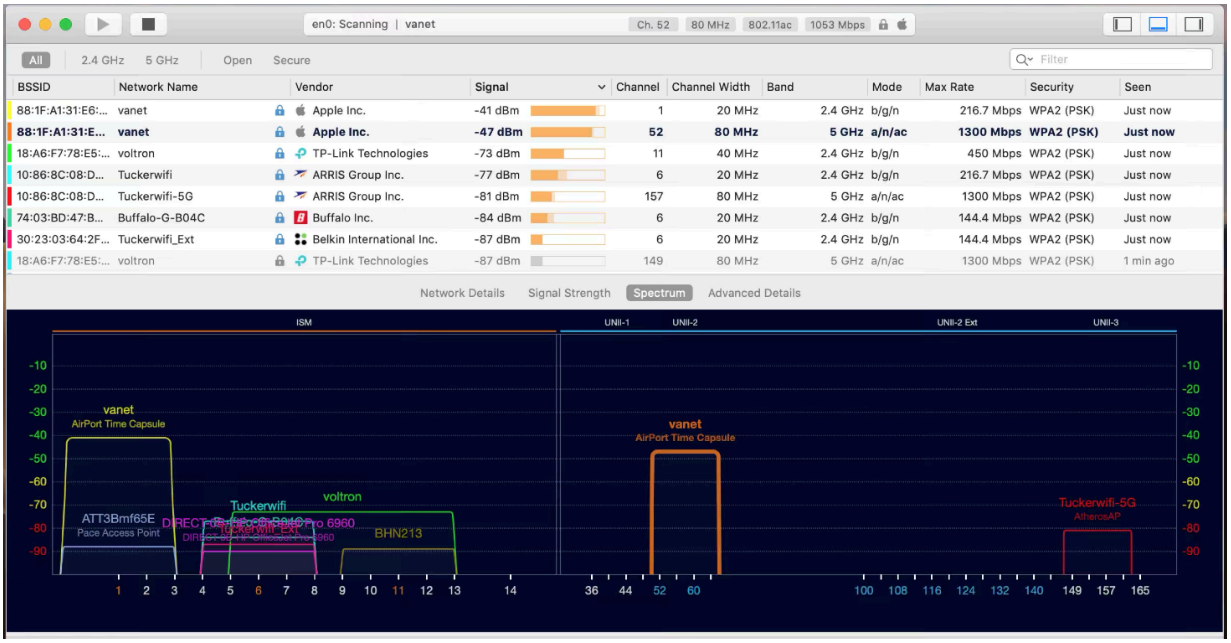
Wireless scanning:

What you used above tells you how YOUR computer is interacting with the wireless access point, but what if you want to know more about that noise level, or why you can't get a fast speed, even though you are close to an access point (AP)?

This is where wireless scanners come in:

There are three types: active, mapping and passive

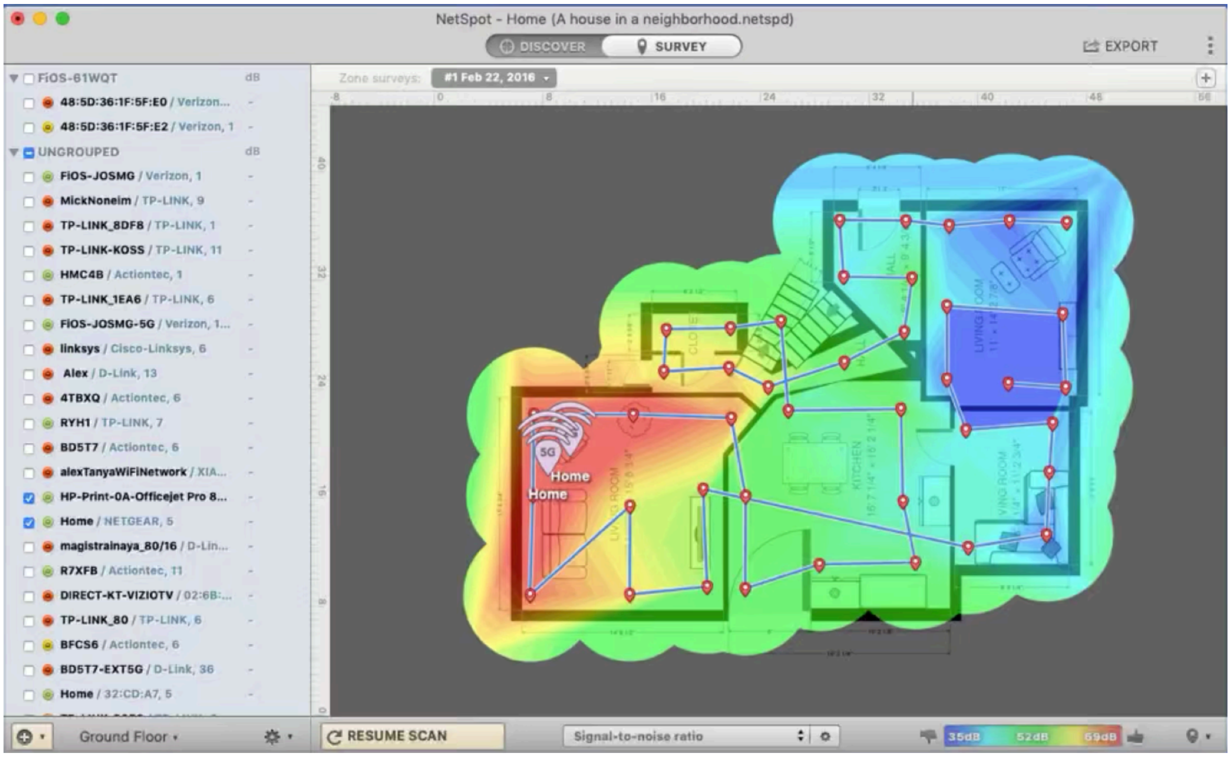
1. Active or "casual" wireless scanners: tell you what channels are being used, how strong the signals are, and in some cases a graphical representation of the channel spectrum. There are two spectra you will be seeing these days: the 2.4 gHz band and the 5.8 gHz band. Each one has channels, which just like a radio station have to be separate to work properly. You will also see different channel widths: 20 or 40 mHz for 2.4 gHZ and 20, 40 or 80 mHz for the higher 5.8 gHz band. Here's an example of an active scanner:



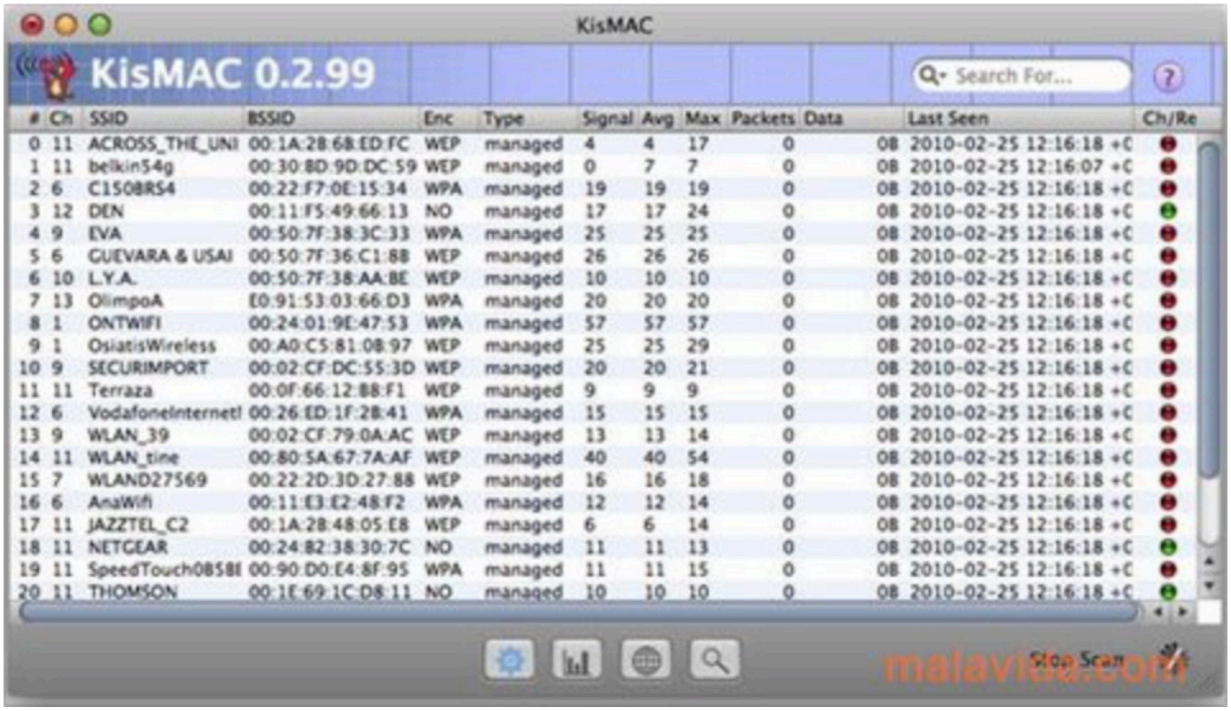
en0: Scanning | vanet — Ch. 52 | 80 MHz | 802.11ac | 1053 Mbps

BSSID	Network Name	Vendor	Signal	Channel	Channel Width	Band	Mode	Max Rate	Security	Seen
88:1F:A1:31:E6:...	vanet	Apple Inc.	-41 dBm	1	20 MHz	2.4 GHz	b/g/n	216.7 Mbps	WPA2 (PSK)	Just now
88:1F:A1:31:E...	**vanet**	**Apple Inc.**	**-47 dBm**	**52**	**80 MHz**	**5 GHz**	**a/n/ac**	**1300 Mbps**	**WPA2 (PSK)**	**Just now**
18:A6:F7:78:E5:...	voltron	TP-Link Technologies	-73 dBm	11	40 MHz	2.4 GHz	b/g/n	450 Mbps	WPA2 (PSK)	Just now
10:86:8C:08:D...	Tuckerwifi	ARRIS Group Inc.	-77 dBm	6	20 MHz	2.4 GHz	b/g/n	216.7 Mbps	WPA2 (PSK)	Just now
10:86:8C:08:D...	Tuckerwifi-5G	ARRIS Group Inc.	-81 dBm	157	80 MHz	5 GHz	a/n/ac	1300 Mbps	WPA2 (PSK)	Just now
74:03:BD:47:B...	Buffalo-G-B04C	Buffalo Inc.	-84 dBm	6	20 MHz	2.4 GHz	b/g/n	144.4 Mbps	WPA2 (PSK)	Just now
30:23:03:64:2F...	Tuckerwifi_Ext	Belkin International Inc.	-87 dBm	6	20 MHz	2.4 GHz	b/g/n	144.4 Mbps	WPA2 (PSK)	Just now
18:A6:F7:78:E5:...	voltron	TP-Link Technologies	-87 dBm	149	80 MHz	5 GHz	a/n/ac	1300 Mbps	WPA2 (PSK)	1 min ago

2. Wireless mapping tools: these are great if you are setting up wireless in your home, office or school. They scan the network from different physical locations, using a diagram or map that you create representing your home, office or school. It then creates a "heat map" of signal strength, which is not only cool to see, it is really useful in adjusting AP location, channels and signal strength (power). Here's an example of a mapping tool:



3. Wireless passive scanners/poaching tools: these rely usually on a mode called “promiscuous mode” meaning the wireless device (your laptop, or using a wireless adapter) accepts ALL wireless traffic, no matter who it was originally intended for. While in this mode, your computer is effectively invisible, but listening to all wireless traffic. A metaphor would be if you were invisible, yet standing in the middle of a party-you would hear even confidential conversations since the speakers have no idea you are there. This is used by hackers in various ways, which we’ll cover in cybersecurity later on. Here’s an example of a passive scanning tool:



#	Ch	SSID	BSSID	Enc	Type	Signal	Avg	Max	Packets	Data	Last Seen	Ch/Re
0	11	ACROSS_THE_UNI	00:1A:28:68:ED:FC	WEP	managed	4	4	17	0	0B	2010-02-25 12:16:18 +C	🔴
1	11	belkin54g	00:30:8D:9D:DC:59	WEP	managed	0	7	7	0	0B	2010-02-25 12:16:07 +C	🔴
2	6	C150BRS4	00:22:F7:0E:15:34	WPA	managed	19	19	19	0	0B	2010-02-25 12:16:18 +C	🔴
3	12	DEN	00:11:F5:49:66:13	NO	managed	17	17	24	0	0B	2010-02-25 12:16:18 +C	🟢
4	9	EVA	00:50:7F:38:3C:33	WPA	managed	25	25	25	0	0B	2010-02-25 12:16:18 +C	🔴
5	6	GUEVARA & USAI	00:50:7F:36:C1:88	WEP	managed	26	26	26	0	0B	2010-02-25 12:16:18 +C	🔴
6	10	L.Y.A.	00:50:7F:38:AA:BE	WEP	managed	10	10	10	0	0B	2010-02-25 12:16:18 +C	🔴
7	13	OlimpoA	E0:91:53:03:66:D3	WPA	managed	20	20	20	0	0B	2010-02-25 12:16:18 +C	🔴
8	1	ONTWIFI	00:24:01:9E:47:53	WPA	managed	57	57	57	0	0B	2010-02-25 12:16:18 +C	🔴
9	1	OsiatisWireless	00:A0:C5:81:08:97	WEP	managed	25	25	29	0	0B	2010-02-25 12:16:18 +C	🔴
10	9	SECURIMPORT	00:02:CF:DC:55:3D	WEP	managed	20	20	21	0	0B	2010-02-25 12:16:18 +C	🔴
11	11	Terraza	00:0F:66:12:88:F1	WEP	managed	9	9	9	0	0B	2010-02-25 12:16:18 +C	🔴
12	6	VodafoneInternetI	00:26:ED:1F:28:41	WPA	managed	15	15	15	0	0B	2010-02-25 12:16:18 +C	🔴
13	9	WLAN_39	00:02:CF:79:0A:AC	WEP	managed	13	13	14	0	0B	2010-02-25 12:16:18 +C	🔴
14	11	WLAN_tine	00:80:5A:67:7A:AF	WEP	managed	40	40	54	0	0B	2010-02-25 12:16:18 +C	🔴
15	7	WLAND27569	00:22:2D:3D:27:88	WEP	managed	16	16	18	0	0B	2010-02-25 12:16:18 +C	🔴
16	6	AnaWifi	00:11:E3:E2:48:F2	WPA	managed	12	12	14	0	0B	2010-02-25 12:16:18 +C	🔴
17	11	JAZZTEL_C2	00:1A:28:48:05:E8	WEP	managed	6	6	14	0	0B	2010-02-25 12:16:18 +C	🔴
18	11	NETGEAR	00:24:B2:38:30:7C	NO	managed	11	11	13	0	0B	2010-02-25 12:16:18 +C	🟢
19	11	SpeedTouch0B58I	00:90:D0:E4:8F:95	WPA	managed	11	11	15	0	0B	2010-02-25 12:16:18 +C	🔴
20	11	THOMSON	00:1E:69:1C:D8:11	NO	managed	10	10	10	0	0B	2010-02-25 12:16:18 +C	🟢

CAUTION:
Be very careful about where you use these tools: the first two are legal in most countries, while the last group are illegal in many countries, particularly in the EU.

Programs to check out:
wifi explorer lite
istumbler
netspot
linux: wavemon, linSSID, wifite

<u>Some wireless basics:</u>
Wireless radio signals are a form of radio waves, that behave much like light: you can imagine your access point as a lighthouse, and your laptop or phone as a ship at sea. If you are close enough and have a clear path to the lighthouse, you can "see" the network. Now imagine there are many lighthouses with different colors (channels). You may want to join the red lighthouse, while the blue one is much brighter. This is where channels come in.
Another thing: if you want to see the lighthouse from farther away, you could use a telescope or binoculars. This is the same as having an external antenna on your laptop. Sadly, there is no such device for

phones (yet), except for special scanning devices.
Wireless signals use very short wavelengths, much shorter than normal radio signals, yet longer than light, so they can bend a bit, but not much. They can also be reflected or blocked by thick walls, metal, any wire mesh (like a fence) and even some window tinting products, since they use metal particles.
The difference between 2.4 gHz (the older system) and 5.8 gHz is range and speed: 2.4 Ghz (this means giga-Hertz) is slower, but travels farther using less power. 5.8 gHz is faster, uses more power, but is usually shorter range.
However, one key difference is water and microwaves: 2.4 gHz just happens to be the resonant frequency of a water molecule, which is how your microwave oven heats up anything with water in it. You may notice your wifi signal going dead when the microwave oven in on. The higher 5.8 gHz channel is immune to this.
BTW, the same 2.4 gHz signal is used by radar speed guns…

a, b, g, n, ac and what?
There are several types of wifi network you will see on the scanners: the oldest is 802.11b. This is an agreed set of rules, channels and frequencies from the 1990's. 802.11 means the rules set out by the IEEE, an electronics group.
802.11b is slow, about 10 mb/s at 2.4 gHz
802.11g is faster, about 58 mb/s also at 2.4 gHz
802.11a is faster still, about 100 mb/s, at 5.8 gHz
802.11n combines g and a to make something much faster, using both networks
802.11ac is the latest, topping out at about 1300 mb/s, which is faster than most wired networks

Wired vs. wireless
Even though the latest 802.11ac is theoretically faster than a wired 1 gb/s network, there isi a catch: wired networks can both talk and listen at the same time, with a pair of wires for each (TX+ TX- and RX+, RX-). We call this full duplex.
Wireless networks are half-duplex, meaning they can EITHER talk or listen, but not both at the same time.
SO
This means a 1 gb/s (gigabit ethernet) is effectively similar to a 2000

mb/s (2 gigabit) wireless network, which does not exist yet.
Another thing: wired networks know who is on the network, and if there is too much traffic, or collisions, they can be resolved quickly.
Wireless networks have what is known as the “hidden man” problem: the access point can see person A and person B, but A cannot see B. So the access point has to negotiate their traffic alone. This is tough and even tougher when A is far away and B is close.
This is why one slow or distant person on a wireless network can bring the entire network slower.
Not an issue with wired networks.

———————end of Module 4: Wireless Networking ———————————