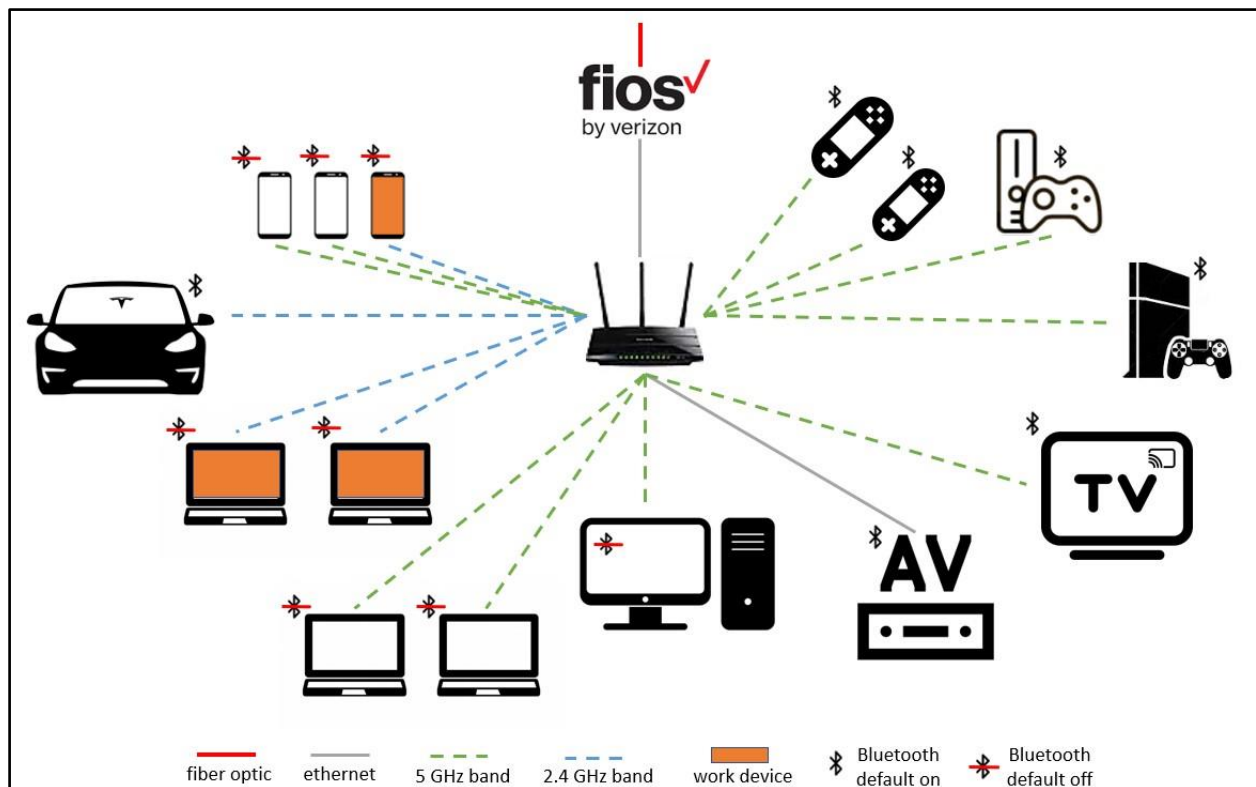


Unsurprising in the age of Internet of Things (IoT) and work-from-home (WFH), our household's wireless local area network (WLAN) has many devices connected to it (Figure 1). Our IoT devices include our car, our home theater's receiver, and a smart TV. Other nodes on the network include multiple game systems, several computers, and our phones. Two of these computers and one of the phones are work devices that allow my husband and I do work remotely. What Figure 1 does not depict, is how these WFH devices provide remote connections to the resources on our employers' campus area networks (CANs) through employer-provided virtual private networks (VPNs). Figure 1 also does not account for a handful of devices that are non-persistent parts of our network and do not connect to our WiFi, such as some of our Bluetooth devices and devices like our printer that require a physical connection.

Figure 1
Our Home Network



Verizon is our internet service provider (ISP). We use their Fios service for fast internet speeds delivered via fiber optic cable. Our router (our home's switch) is a [dual-band router](#), allowing us the option to connect our devices to either a 5GHz or 2.4GHz WiFi frequency. The 5GHz band allows us to take full advantage of the speeds our Verizon Fios subscription provides but has a shorter range and does not connect as well through walls and floors. The 2.4GHz band limits our speed but can reach further and penetrate through walls and floors better. As such, we connect our car and work devices to the 2.4GHz band but connect the rest of our devices to the 5GHz band.¹ The car needs to connect from outside the house for software updates and our work devices need a reliable connection from our upstairs de facto "offices," but do not need fast download speeds. Our computers, phones, game systems, and smart TV, however, are used for heavy amounts of streaming and large downloads and thus benefit from the faster speeds available on our 5GHz band. Most of these are also located in close proximity to our router. There are several ways to find out more information about my network, such as the IP and MAC addresses of devices on it and the DNS server(s) being used to connect me to websites. As a Windows user, the easiest way for me is to open up the Command Prompt and use the **ipconfig** command to figure out my router's IP address (the IP address listed as "default gateway" on the text returned) and then plug this address into a web browser to subsequently access my router. Once logged into my router, I can easily navigate through various menus to see the IP and MAC addresses of all devices connected to my network (Figure 2). I can also look to see what DNS server is being used (Figure 3).

¹ Our home theater receiver is currently connected to our router via ethernet cable due to some app-based calibration shenanigans that did not want to work otherwise. Normally, it is also connected via WiFi.

Figure 2

IP and MAC Addresses of Devices Connected to Home Network


DHCP Client List				
Total Clients: 6			 Refresh	
ID	Client Name	MAC Address	Assigned IP Address	Lease Time
1	Tesla_Model_3	4C-FC-AA-01-A0-2B	192.168.0.247	1:54:2
2	AOS-80MSNN2-WL	34-41-5D-A7-4F-F9	192.168.0.245	1:10:35
3	--	86-1D-86-80-D6-31	192.168.0.231	1:19:46
4	--	90-73-5A-C0-13-50	192.168.0.136	1:57:54
5	DESKTOP-G3UVJ5Q	3C-9C-0F-54-5C-59	192.168.0.164	0:41:53
6	DESKTOP-AUM7RU0	04-EA-56-DD-FE-B9	192.168.0.163	1:55:13

Figure 3

DNS Servers

Internet

IPv4 | IPv6

MAC Address:

AC-84-C6-C5-01-40

IP Address:

173.79.23.182

Subnet Mask:

255.255.255.0

Default Gateway:

173.79.23.1

Primary DNS:

71.252.0.12

Secondary DNS:

71.242.0.12

Connection Type:

Dynamic IP

For security, we try to practice basic cyber hygiene to protect the devices on our network, such as keeping our devices (including our router) up to date with the latest software and firmware updates. We also make sure to change default login credentials and use passwords that are not generic, easy to guess, or reused across multiple devices/accounts. This is the most basic form of cybersecurity, but can often be [overlooked](#) with routers, despite how critical they are to a network. We also follow some of the other [best practices](#) suggested for improving home network security, such as changing the default name of our network to make it less obvious to outsiders what model of router we use.

However, our home network is definitely nowhere near as secure as large enterprise networks that are actively monitored for malicious activity. Our network defenses are primarily passive, relying on proper configuration, strong passwords, and firewalls. One aspect of our network that generally makes me uncomfortable is how many Bluetooth devices are on it, with these devices generally difficult to hide from public view and lacking good authentication practices for making sure that unwelcome users cannot connect to them. Where possible, we try to toggle Bluetooth off and only enable it when it is actively in use, such as depicted in Figure 1 for our phones and computers.