

THE COMPLETE **WINDOWS NETWORK** TROUBLESHOOTING GUIDE

by Yusuf Limalia



The Complete Windows Network Troubleshooting Guide

Written by Yusuf Limalia

Published January 2018.

Read the original article here: <https://www.makeuseof.com/tag/windows-network-troubleshooting-guide/>

This ebook is the intellectual property of MakeUseOf. It must only be published in its original form. Using parts or republishing altered parts of this ebook is prohibited without permission from [MakeUseOf.com](https://www.makeuseof.com).

Table of contents

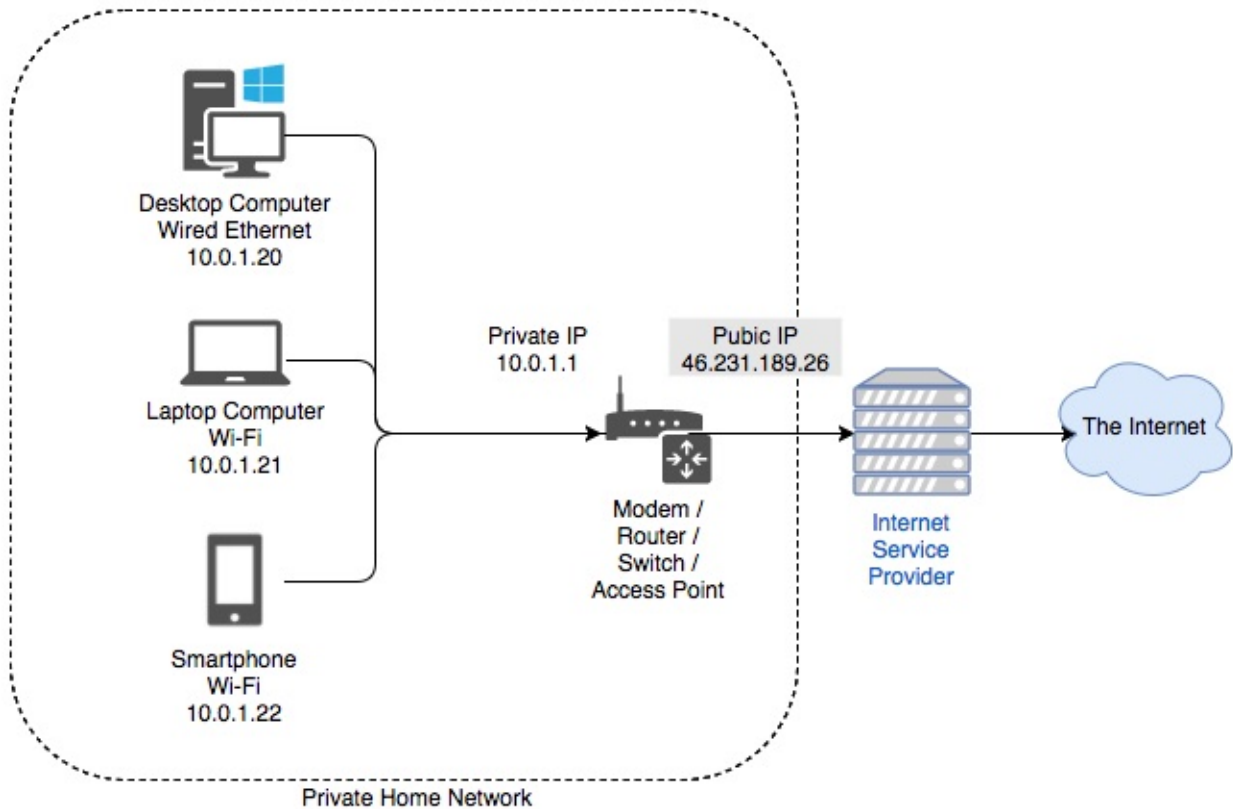
An Introduction to Networks	4
Network Diagrams	4
Internet Protocol (IP) Address and Hostname	5
DHCP	7
Domain Name System (DNS)	9
Mbps versus MBps	10
Wired Networks	10
Wireless Networks	12
Wireless Settings for Best Results	13
Guest Network	15
Consolidation	16
Drawing Your Own Network	17
Troubleshooting Your Network	17
Troubleshooting Methodology	17
Basic Diagnosis	18
Browser Issues	19
Area Outages	21
Intermediate Diagnosis	22
DNS	24
Firewalls and Anti-Malware	27
Uninstalling the Network Adapter	30
Network Reset (Windows 10)	31
Wired Ethernet Problems	33
Wired Hardware Faults	36
Resetting Your Router	36
Wi-Fi Problems	36
Your Network Issues Resolved?	38

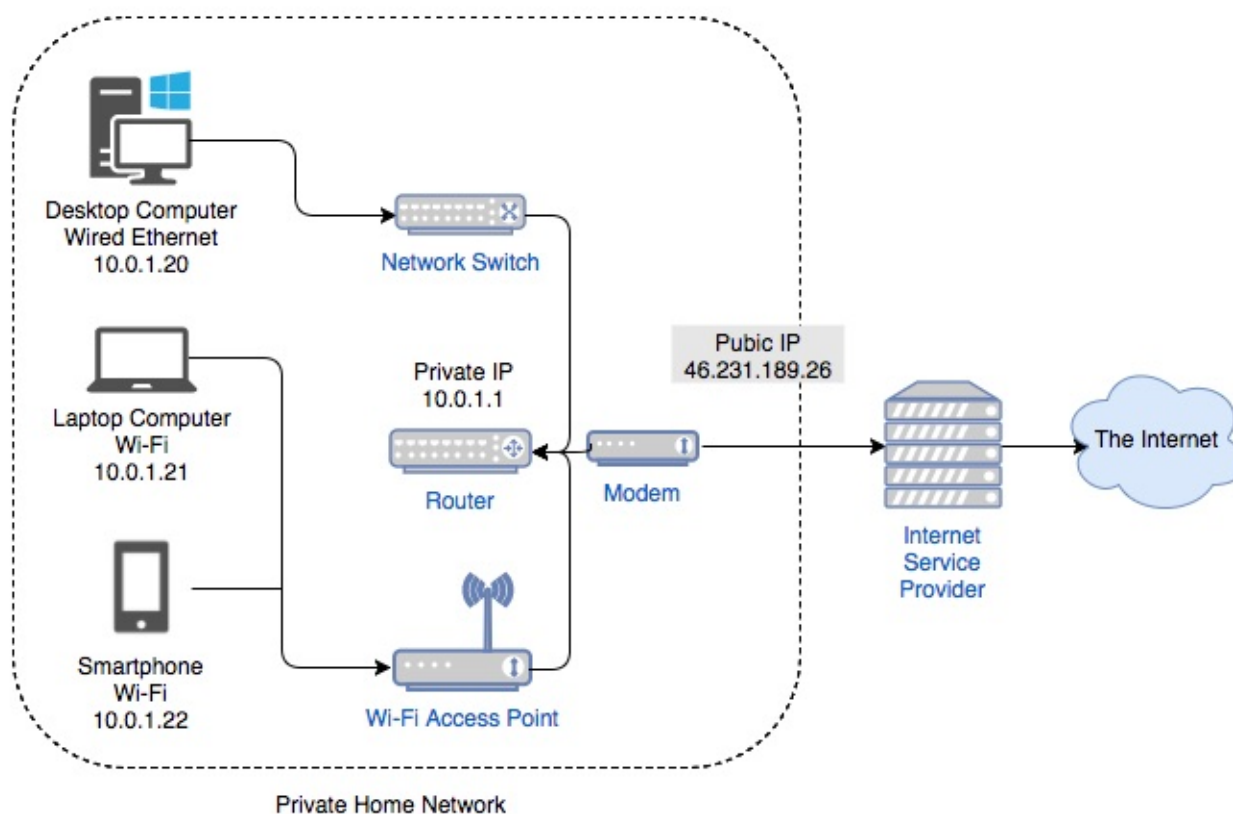
When you have internet or network issues, it may feel like a regression back to the stone age. Let's try and understand networks and look at some troubleshooting techniques to bring you back into the world of the living.

An Introduction to Networks

Network Diagrams

Here's what your network setup may look like.





The above diagrams are basic representations of what a typical home network consists of. There are typically two cases. The first case is a central device acting as the modem, router, switch and wireless access point. The second diagram shows another case, where the roles are split into multiple devices.

Each method has pros and cons. Having a single device is much easier to set up, but there is a single point of failure. Having different devices is the method most larger companies choose. While setup can get extremely complicated, it's far more scalable. Let's take a look at some of the services that a network requires to function.

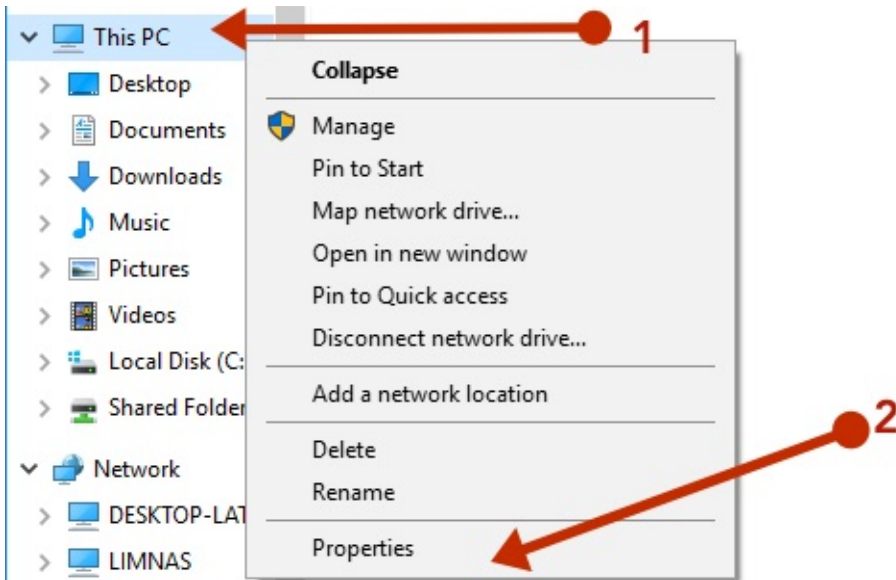
Internet Protocol (IP) Address and Hostname

An IP address is an identifying number for a piece of network hardware. Having an IP address allows a device to communicate with other devices over an IP-based network like the internet. Each device on a network must have a unique IP.

The most common form of IP we see today is IP version 4 (IPv4). IPv4 is comprised of four sets of numbers, between 0 and 255, separated by a decimal point. Example IPv4 addresses looks like:

- 10.0.0.1
- 192.168.0.254
- 172.16.254.6

A **hostname** should be more human readable. All devices on your network should also have a unique hostname. Having multiples devices on your network with the same hostname can cause a network malfunction. You can view your computer's hostname by right-clicking on **My Computer / This PC > Properties**.



Clicking on the **Change Settings** link, will allow you to set a custom name for your PC.

View basic information about your computer

Windows edition

Windows 10 Pro

© 2017 Microsoft Corporation. All rights reserved.



System

Processor: Intel(R) Core(TM) i7-7567U CPU @ 3.50GHz 3.50 GHz
 Installed memory (RAM): 2.00 GB
 System type: 64-bit Operating System, x64-based processor
 Pen and Touch: No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

Computer name: DESKTOP-LATSD8D
 Full computer name: DESKTOP-LATSD8D
 Computer description:
 Workgroup: WORKGROUP

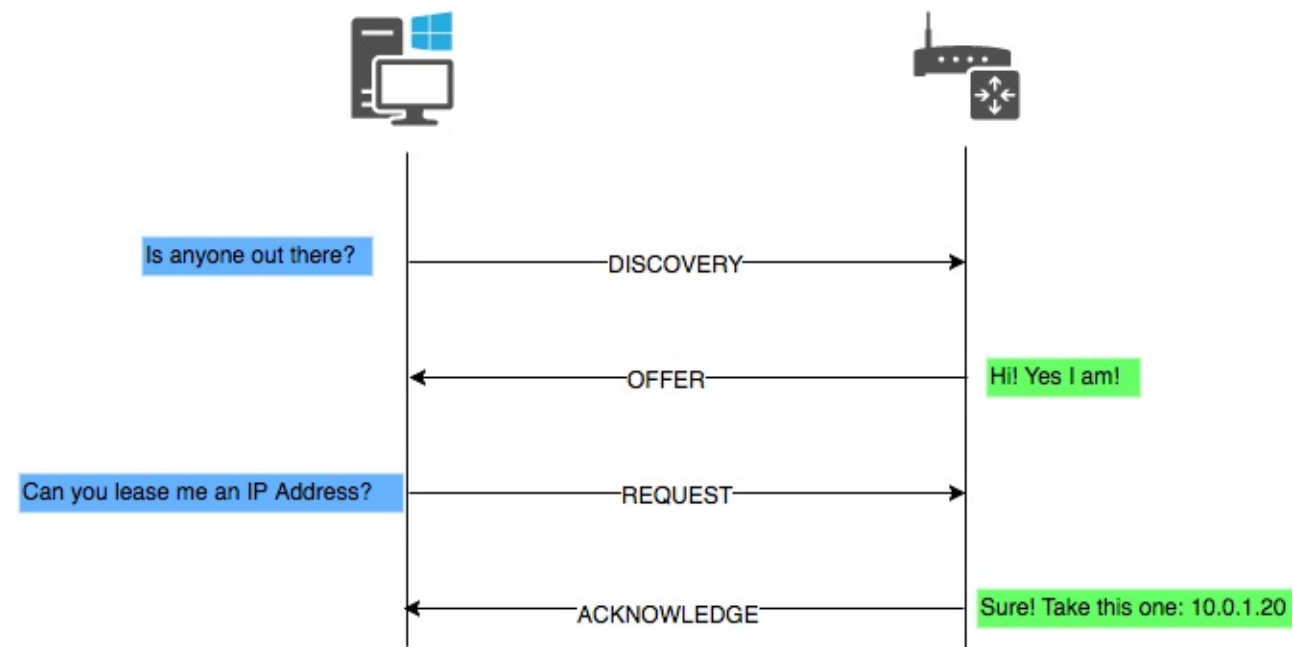
[Change settings](#)



Just ensure all devices on your home network have a unique name and IP address and you should be golden.

DHCP

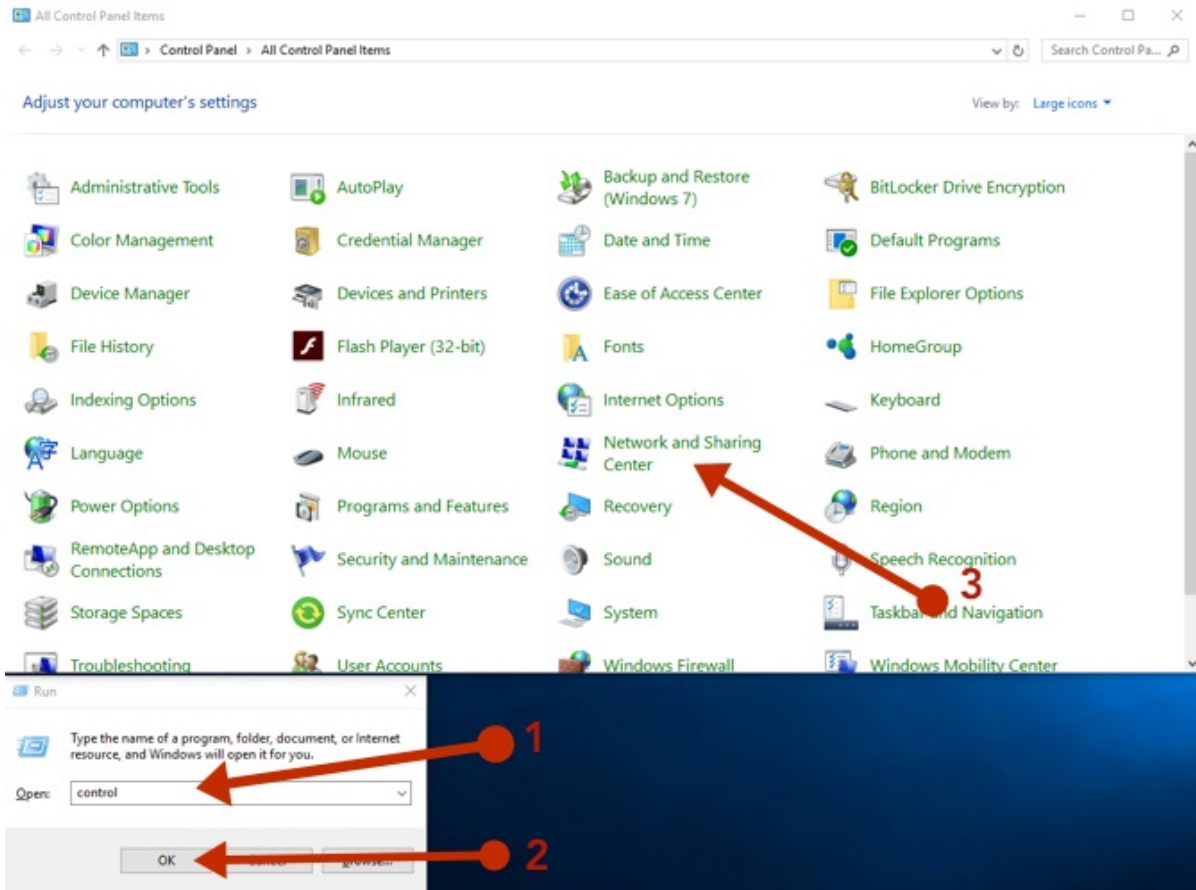
The Dynamic Host Configuration Protocol (DHCP) is a protocol where some network information is exchanged between a client and a server. In a home network, this is a role that is covered by the router.



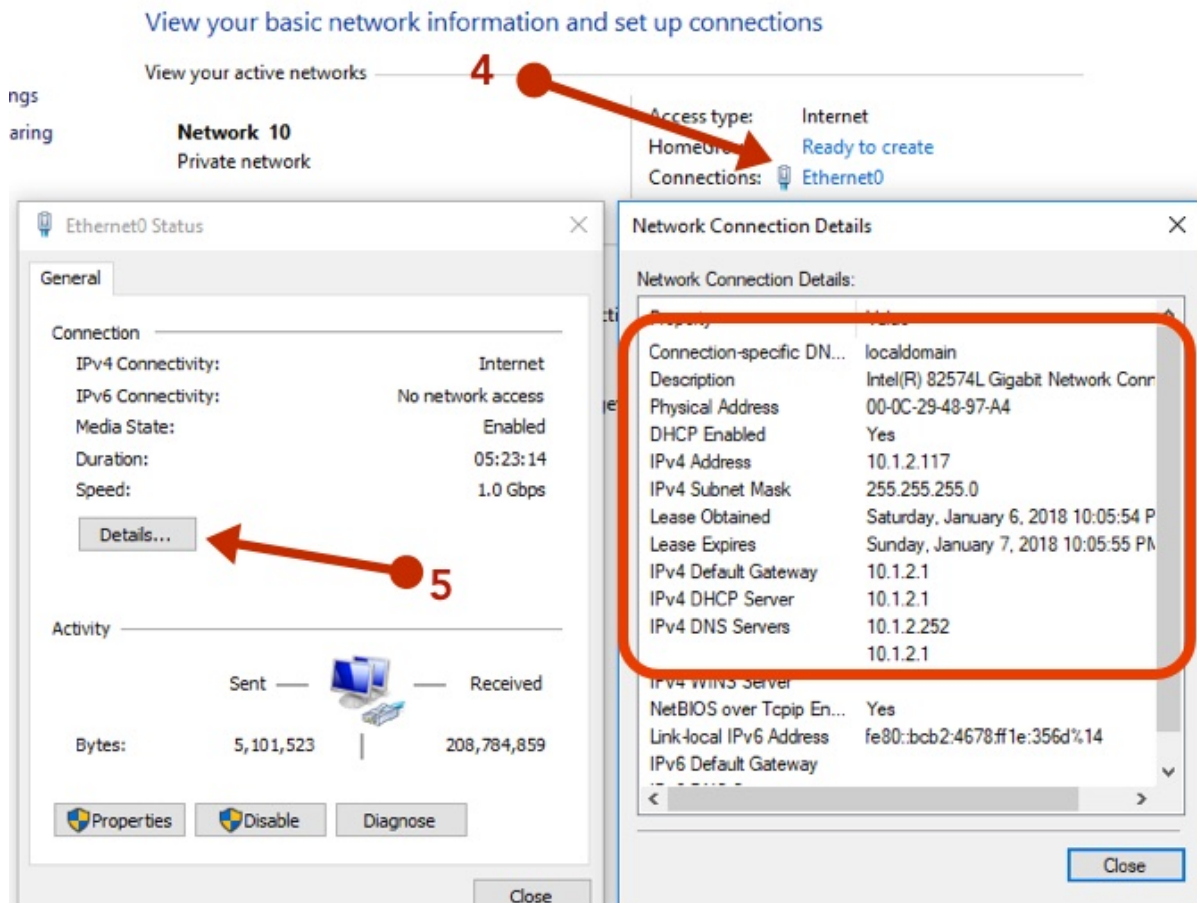
In a home network always ensure that there is only one DHCP server. DHCP provides information such as IP address, Subnet Mask, Gateway and Domain Name Service (DNS).

The DHCP server keeps a list of which device is leasing which IP address. This ensures that no two devices will get assigned the same IP. Having two devices on your network with the same IP can cause one or both of them to malfunction. To view your current network settings go to **Control Panel > Network And Sharing Centre > [Connection] > Details**. A shortcut to getting to the control panel:

1. **WinKey + R** on your keyboard. Or you could open the start menu and type **Run**.
2. Now enter **control** in the **Run Command** box followed by the **Return key**.



Control Panel > All Control Panel Items > Network and Sharing Center





The relevant information here is:

- DHCP enabled: should be Yes
- Address: this devices IP
- Subnet Mask: this devices subnet mask
- Default Gateway: should be your router's address
- DHCP Server: should be your router's address
- DNS Servers: should be your router's address

The numbers that you will see will be slightly different. Generally speaking, routers default to one of the following addresses:

- 10.0.0.1
- 192.168.0.1
- 192.168.1.1

All other devices on your network will only have the last number incremented. Our example diagram has the router at the address 10.0.0.1 and the other devices starting at 10.0.0.20. It is a good idea to reserve a few IP addresses for devices you would like to assign static IPs to. These can include the router, some servers, or even certain workstations.

Domain Name System (DNS)

If everything was addressed by their IP address, life would be challenging. Is it easier to remember 216.58.212.78 or Google.com? **A DNS server** is the device that translates the www.google.com you type in your browser to the 216.58.212.78 IP address that it really is. You can try this by typing the IP address in your browser window, and Google should pop up!

In a home network, your router acts as a DNS server, translating hostnames to IP addresses. If you need to access another device on your network, your router has a database of everyone that is on the network and will translate a computer's hostname to an IP. If you need to access a device on the internet, your router will forward the request to another DNS server on the internet and send the reply to the device that requested it.

In most cases, two DNS servers, a primary and a secondary server, are automatically configured on your router and/or computer when connecting to your internet Service Provider (ISP) via DHCP. You can configure two DNS servers in case one of them happens to fail, after which the device will resort to using the secondary server.

While many DNS servers are operated by ISPs and intended to be used only by their customers, several public-access ones are also available. Generally speaking, your primary DNS server should be your router.

Mbps versus MBps

Megabits Per Second (Mbps) is not the same as Megabytes Per Second (MBps). It takes 8 Megabits to equal 1 Megabyte. You will generally see Mbps when network speed is being referenced, and MBps indicates the amount of file data transferred per second. **When an ISP advertises network speed**, it's always in Megabits. This might be slightly confusing so let's take an example.

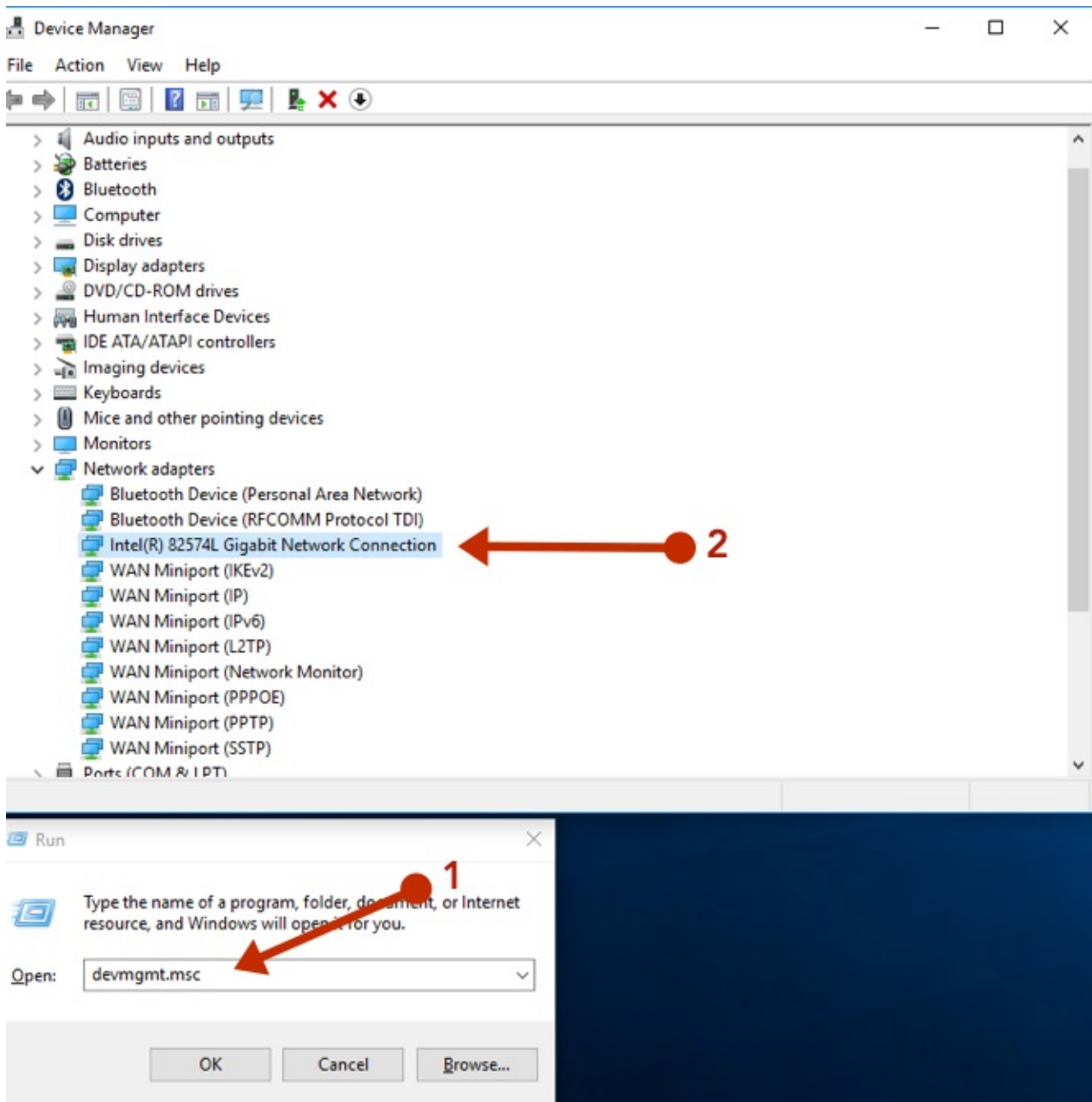
If you want to download a short video, and the file size is 10 MB (Megabytes). Your internet connection gives you download speeds up to 16 Mbps. First, convert your Mbps into MBps by dividing 16 by 8 which equals 2 MBps. Now divide the file size (10 MB) by your MBps (2) to get the amount of time it will take to download the file. $10 \text{ MB} / 2 \text{ MBps} = 5 \text{ seconds}$. It will take approximately 5 seconds to download your 10 MB file with an internet connection of 16 Mbps.

Wired Networks

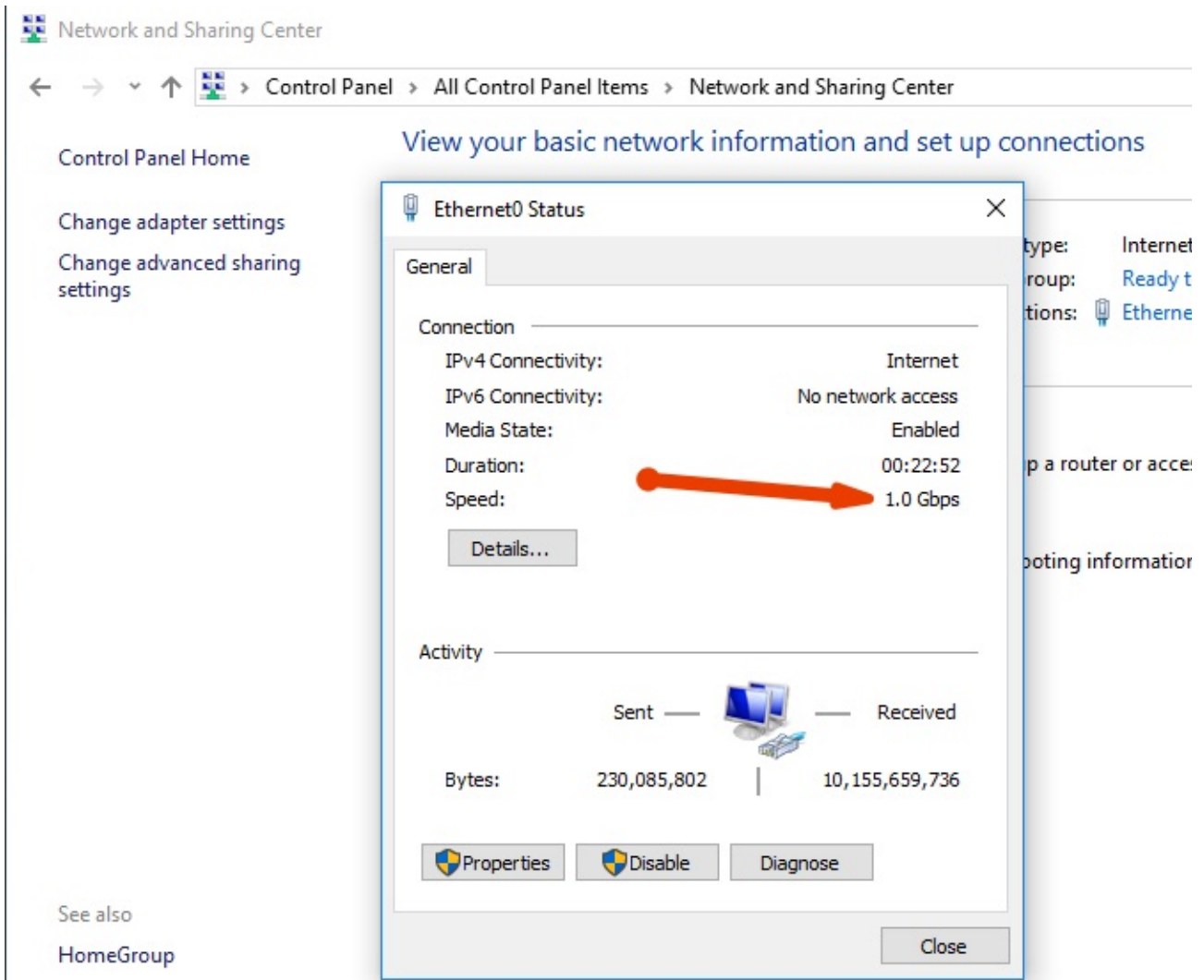
Wired networks have been around since the 1980s. They are currently faster, more stable and less susceptible to attacks compared to wireless networks. Some notation for wired networks you will come across are 10/100/1000, and 10 GbE.

10/100/1000 means that device can support 10 Mbps, 100 Mbps or 1000 Mbps. 10 GbE just means 10 Gigabit Ethernet. The vast majority of consumer **devices will come standard with 1 GbE**. For now, this is sufficient as 10 GbE is relatively much more expensive. This is guaranteed to change shortly as our data demands and internet speeds increase over time. As technology is adopted by the wider market, it also becomes cheaper to manufacture.

You can view what network adapter your computer has from the Windows Device Manager window. In the **Run Command** dialog box type **devmgmt.msc** followed by the return key.



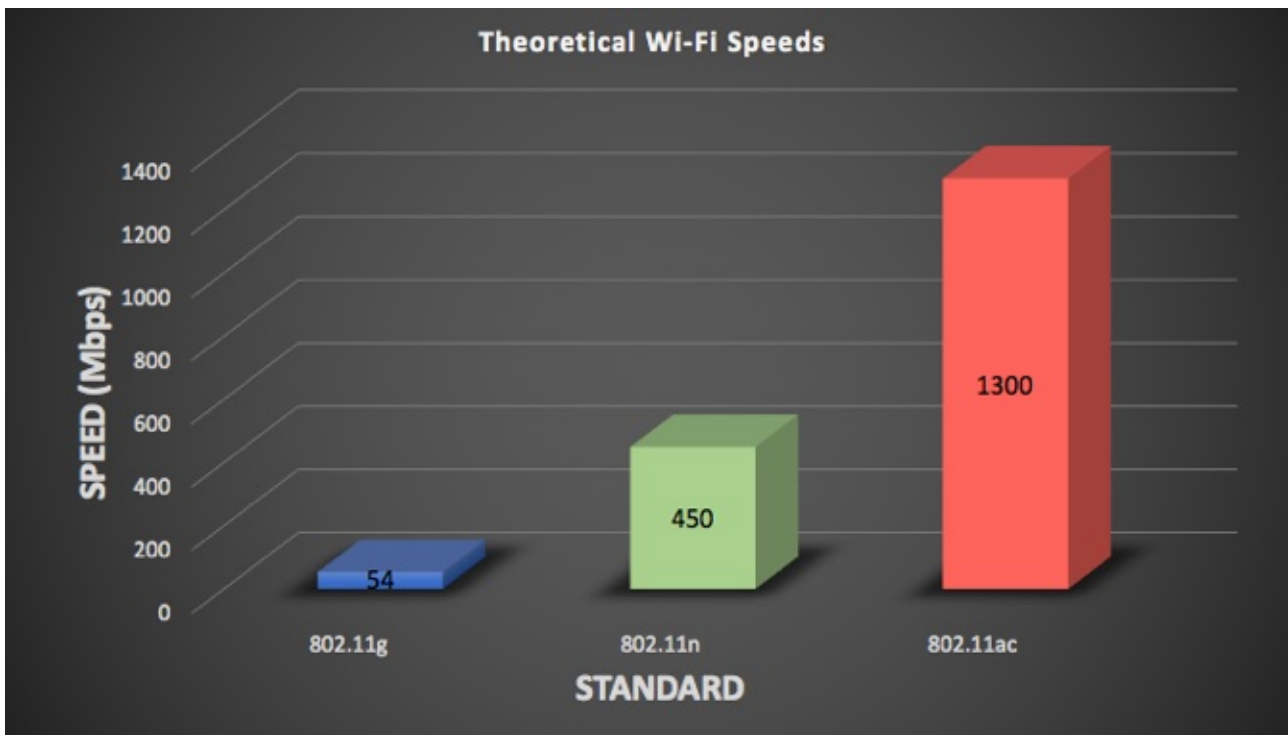
If you expand the Network adapters, you should see what Network Interface Card (NIC) your computer is sporting. To see what your network speed is you can go to **Control Panel > Network And Sharing Centre > [Connection]**. The best practice in a home network setup is to have all your wired devices connected to the same network switch to avoid any bottlenecks when communicating with each other.



Wireless Networks

Wireless networks are the most convenient but are slightly more complex to configure and manage. They are also susceptible to interference from other wireless radios and other electrical and electronic hardware. Wireless networking can be a little tricky to understand, but we can try to demystify its terrible naming conventions.

Wireless Fidelity (Wi-Fi) is governed by a set of standards which you will commonly see as 802.11g, 802.11n, and 802.11ac or something similar. The character on the end will indicate the theoretical max speed. The problem is is that these theoretical speeds are nonsense, and in real-world scenarios, you never get close to the theoretical speeds.



One of the contributing factors in never reaching the theoretical speeds is the antennas. 802.11ac can support up to eight antennas each running at over 400Mbps each. You may have seen some of these routers that resemble Lord Sauron himself such as the ASUS ROG GT-AC5300. While such devices adorn eight antennas, the device being used to connect to them will almost certainly not have that many. Your typical smart device may only have two or three antennas which makes it a bottleneck for the theoretical speed.

802.11ac only works on the 5 GHz frequency while 802.11n supports both 5 GHz and 2.4 GHz. The key difference between the two frequencies is coverage versus bandwidth. 2.4 GHz is much more capable at long range but cannot compete with the speed of the 5 GHz network.

Wireless Settings for Best Results

When you first received your wireless router, chances have you probably changed the administrator login password and **chose a cool name for your Wi-Fi**. The other settings may have been ignored in the overly complicated dashboard. It's probably best not to try and tweak every little setting like a mad scientist, but there are a few settings that could enhance your Wi-Fi experience.

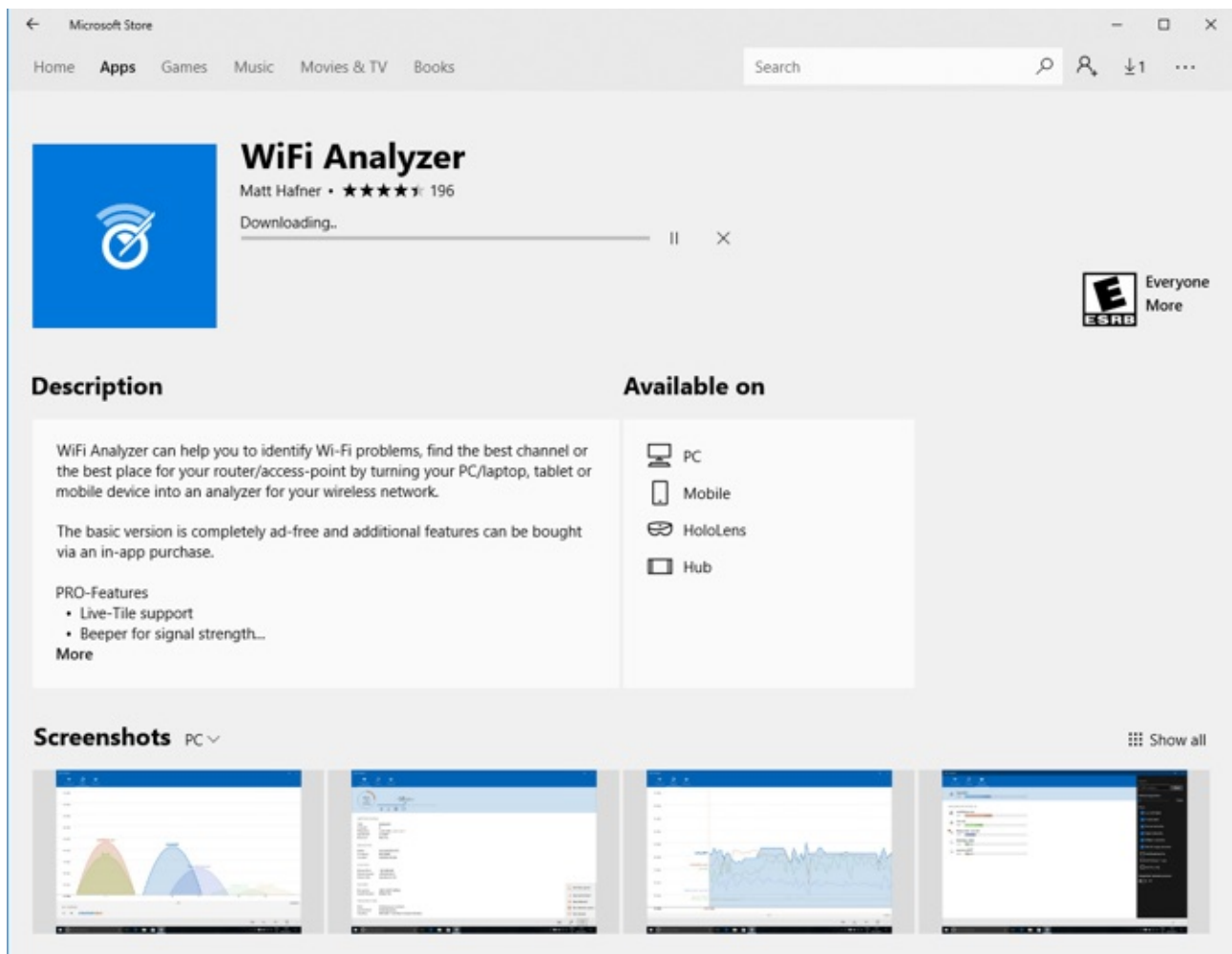
Wireless LAN(2.4GHz) >> Security Settings

SSID 1	SSID 2	SSID 3	SSID 4
Mode:			WPA2/PSK
<u>WPA</u>			
Encryption Mode:			TKIP for WPA/AES for WPA2
Pre-Shared Key(PSK):		

Regarding security, I strongly recommend using the WPA2/PSK mode and choosing AES as the encryption. Other options are just less secure. Under no circumstances should WEP be used as it can be easily hacked by a malintentioned individual armed with a laptop lurking outside your house.

Next, you should choose a channel. A channel is simply a slice of the 2.4 GHz or 5 GHz band that your router is broadcasting on. Most modern day routers will choose a channel automatically. If you are getting slower than expected speeds, a congested channel may be the culprit, especially if you live in an apartment complex with lots of other Wi-Fi routers in the area.

You can grab the **WiFi Analyzer app** from the Microsoft Store, which will turn your PC into a wireless scanner. It will show you which channels are congested and even make a recommendation on which one to choose for best performance.



Lastly, ensure that the correct Wi-Fi standard is chosen. Most modern-day devices support 802.11n and 802.11ac, so ensure those are selected. If however, you have a legacy device, such as a Nintendo 3DS that is not detecting your Wi-Fi, you may have to enable 802.11g.

Guest Network

If your router supports an option for a guest Wi-Fi network, it would be a great idea to enable it. Guest Wi-Fi networks can have different passwords, so you don't have to share your main Wi-Fi network password. The best part is that any device connected to the guest network will not have access to local computers or files on the main network.

	Enable	Hide SSID	SSID	Isolate Member	Isolate VPN
1	<input type="checkbox"/>	<input type="checkbox"/>	MakeUseOf-Main	<input type="checkbox"/>	<input type="checkbox"/>
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	MakeUseOf-Guest	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>

Note:
 Enabling the Isolate Member configuration will forbid the wireless clients associated to the same SSID from connecting to each other.

The isolate VPN configuration will isolate the wireless traffic from VPN connections and thus, wireless clients will not be able to access the VPN network under this setting.

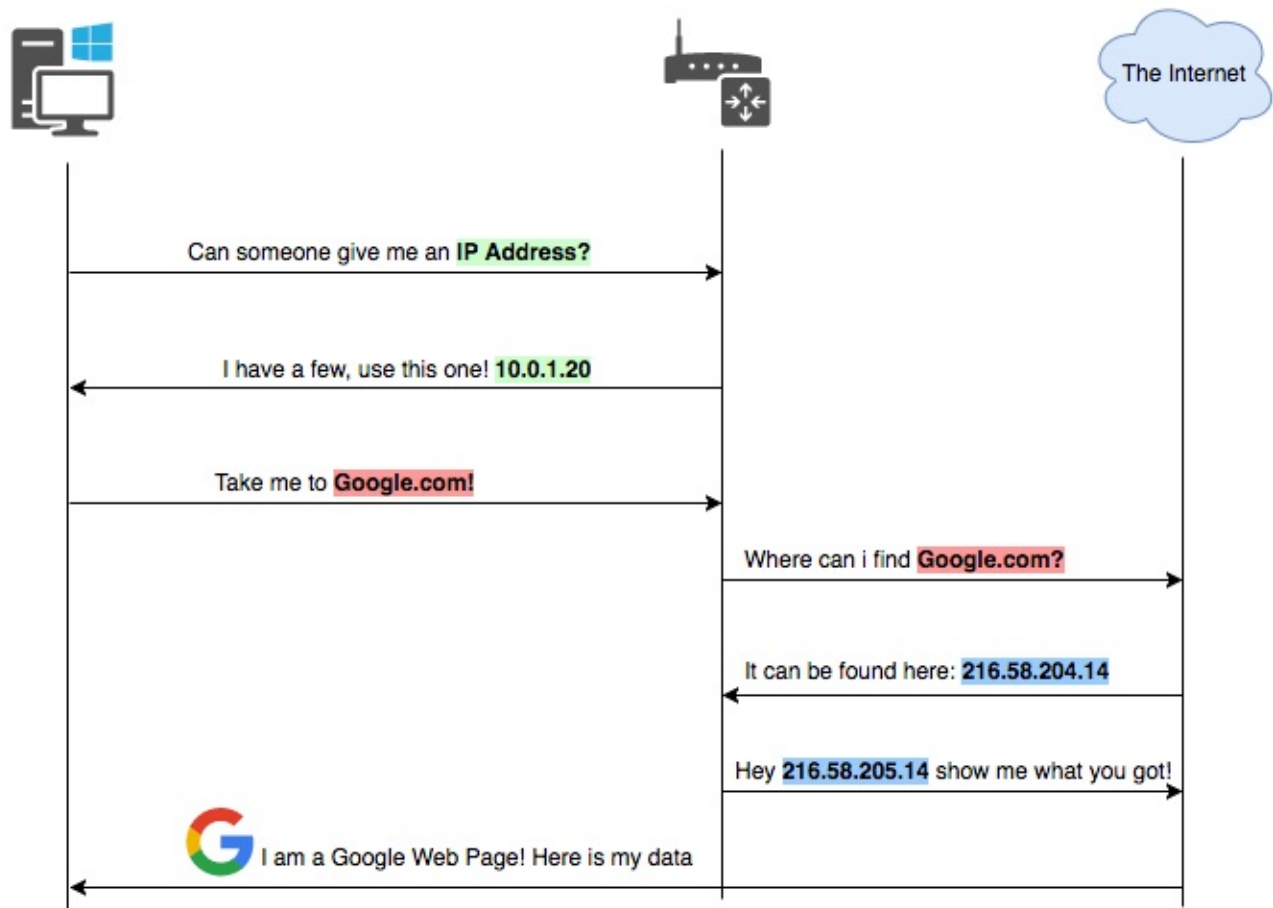
Rate Control		Enable	Upload	Download
SSID 1	<input type="checkbox"/>	<input type="checkbox"/>	30000 kbps	30000 kbps
SSID 2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	10000 kbps	1000 kbps
SSID 3	<input type="checkbox"/>	<input type="checkbox"/>	30000 kbps	30000 kbps
SSID 4	<input type="checkbox"/>	<input type="checkbox"/>	30000 kbps	30000 kbps

Your router treats the guest network as a completely different LAN. You may even have options for throttling or setting limits on clients connected to the guest network, to ensure your friends are not hogging your lovely internet.

At a glance, these are some of the settings you could tweak. Overall, it would be a good idea to make a small change, then run a speed test to see how that has affected your Wi-Fi. Then try the same speed test in a different part of your house. If you're unsatisfied, make another single change, then run your speed tests again. Making too many changes at once may lead to being unable to isolate the problem area.

Consolidation

There is a lot going on when it comes to networking. The above is by no means exhaustive, but it should be enough to give you an understanding of what's happening under the hood.

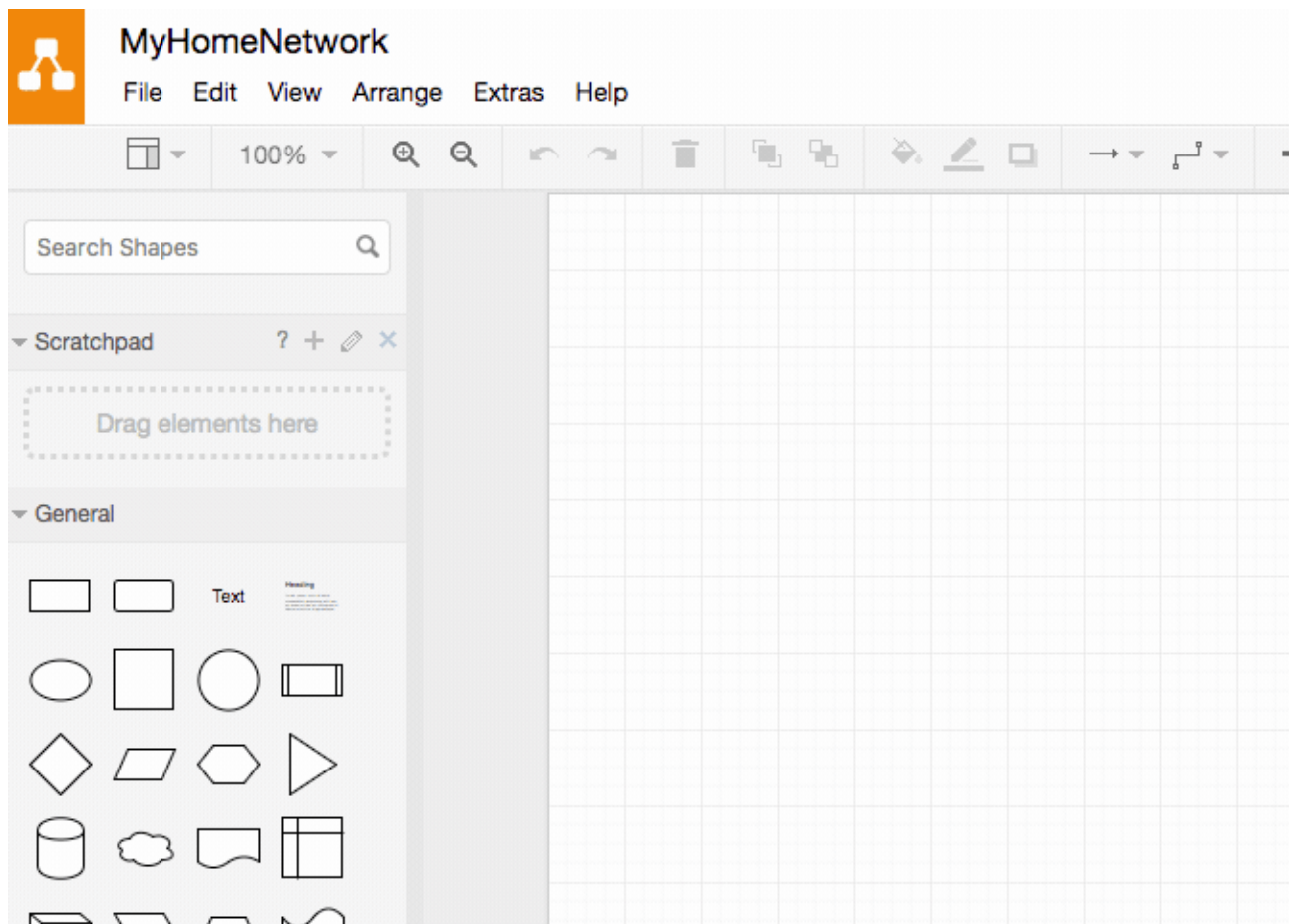


The above diagram shows a flow example of how some of these services fit together.

1. Your computer gets a network connection and starts looking for a device that is a DHCP server.
2. The DHCP server will check that it has a free IP address and lease one to the client.
3. A user will type in a web address like Google.com in a browser window.
4. This address needs to be converted into an IP address that computers can understand; this is done via a DNS server.
5. Once the DNS is resolved, the web page can be found, and a connection is opened up between the user's computer and the web server hosting the web page.

Drawing Your Own Network

If your network is quite complex, it may be a good idea to have it drawn out, to help troubleshoot any issues. There's a great tool over at draw.io that makes drawing anything technical super simple. It's also completely free!



Everything is entirely drag-and-drop, and the user interface is about as simple as it gets. Enter something you'd like in the search box and hit return. Once, you've found an item that you like, just drag and drop it onto the canvas. From there you can join items and just double-click either on them or on the canvas to name them.

Our diagrams in this article were done entirely on draw.io and can be very helpful even when planning out a new network or finding potential problems in an existing one.

Troubleshooting Your Network

Troubleshooting Methodology

Have you come across the principle of Occam's Razor? In a nutshell, it states that the simplest answer, or the one with the least assumptions, is usually the correct one. This is often the case when looking at problems, especially when it comes to technology.

When diagnosing network issues, it is extremely rare for the problem to be a hardware one. It's not unheard of, but NICs, switches, and routers are much less likely to be the problem relative to some silly software setting.

Once you've drawn out your network, and applied some of the recommendations above, it will be easy to get to the bottom of any network issues you may have. The best way of going about networking issues is using the process of elimination. As mentioned above, making too many changes at once can make diagnosing a problem much more difficult.

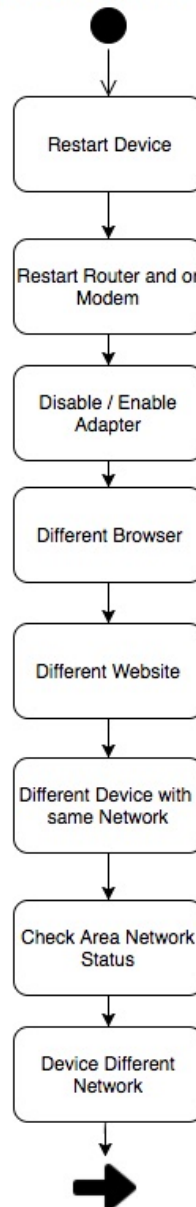
You can use this guide as a top-down approach. The guide starts with suggestions on what to try first before moving to the next step. If at some point you notice the behavior is unexpected, there is a possibility that your problem is at that point. Bearing these principles in mind let's get to the bottom of it!

Basic Diagnosis

Oh no! That fateful day where you open a browser window and nothing loads. If you're the IT person in the family, this is sometimes followed by "Sam! The Wi-Fi isn't working!" or some similar bellowing. Now, before things begin to get a little heated, there is a good chance you can solve this in a few seconds.



Web Page Doesn't Load

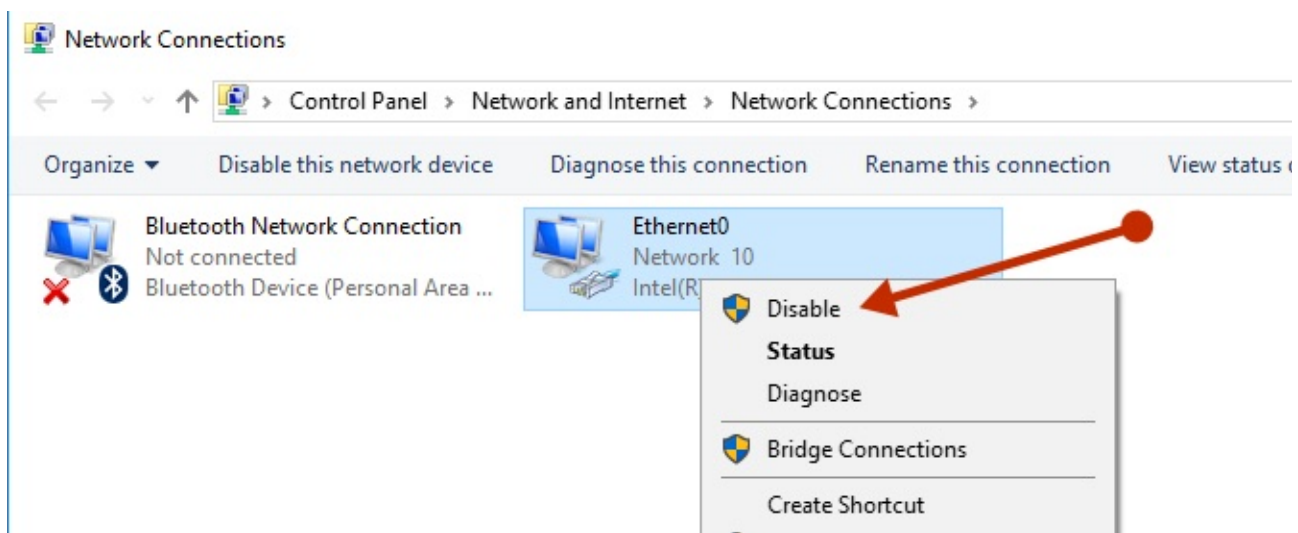


Intermediate Diagnosis

Our basic flow goes like this:

1. Restart the device.
2. Restart the router and or modem.
3. Disable and enable the network adapter.
4. Try a different browser. If you're using Google Chrome, try Microsoft Edge.
5. Try a different website.
6. Try a different device that is on the same network. So if your device that can't connect is wired, try another device that is on the wired network.
7. Check your area's network status.
8. Try using a device that is on a different network. So if your device that can't connect is wired, try using a device that is on the wireless network.

To disable and enable an adapter go to **Control Panel > Network and Sharing Center > Change adapter settings**. Right-click on your network connection and select **Disable**. The adapter will turn grey, and after a few seconds, you can right-click on the device and select **Enable**.

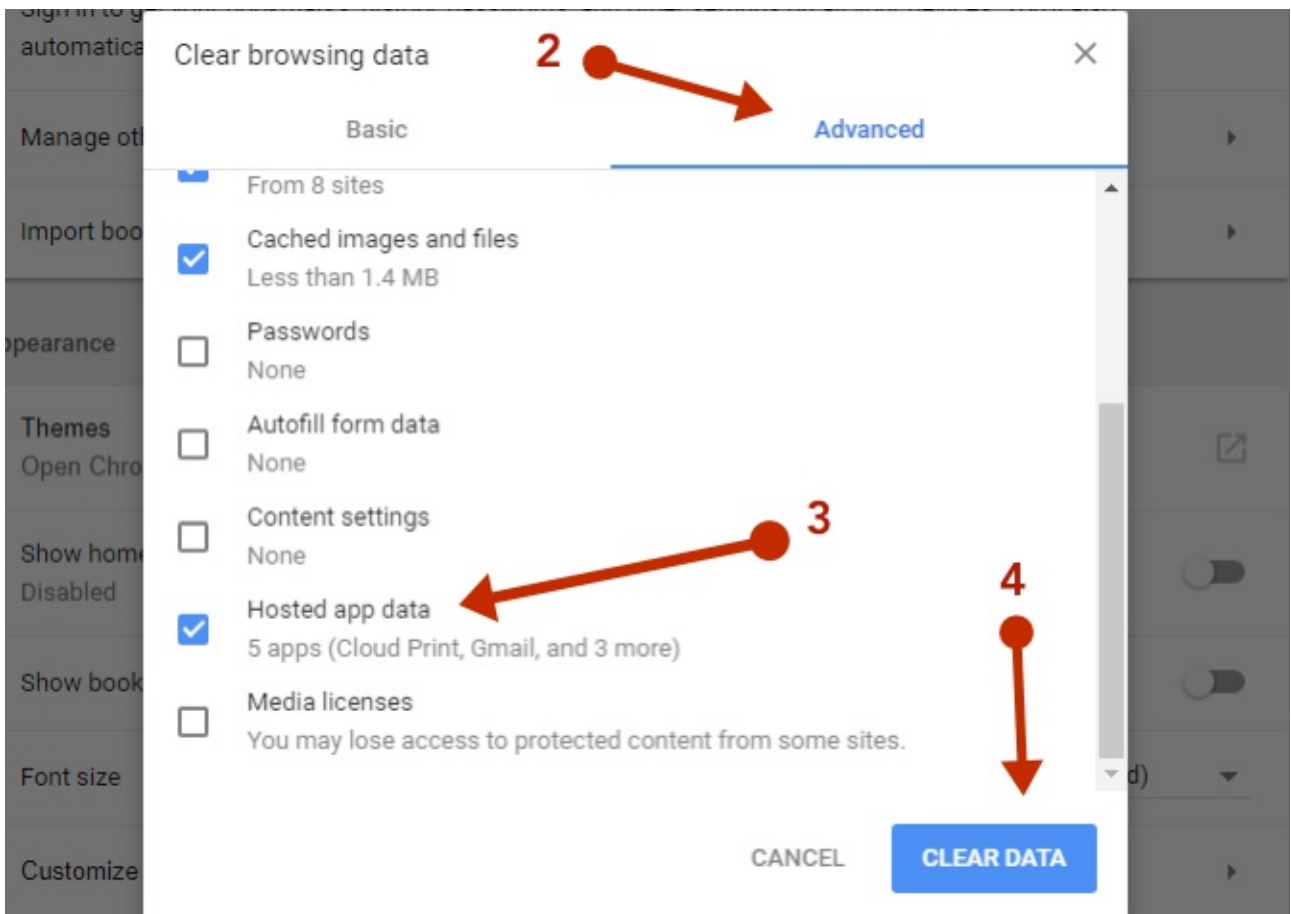
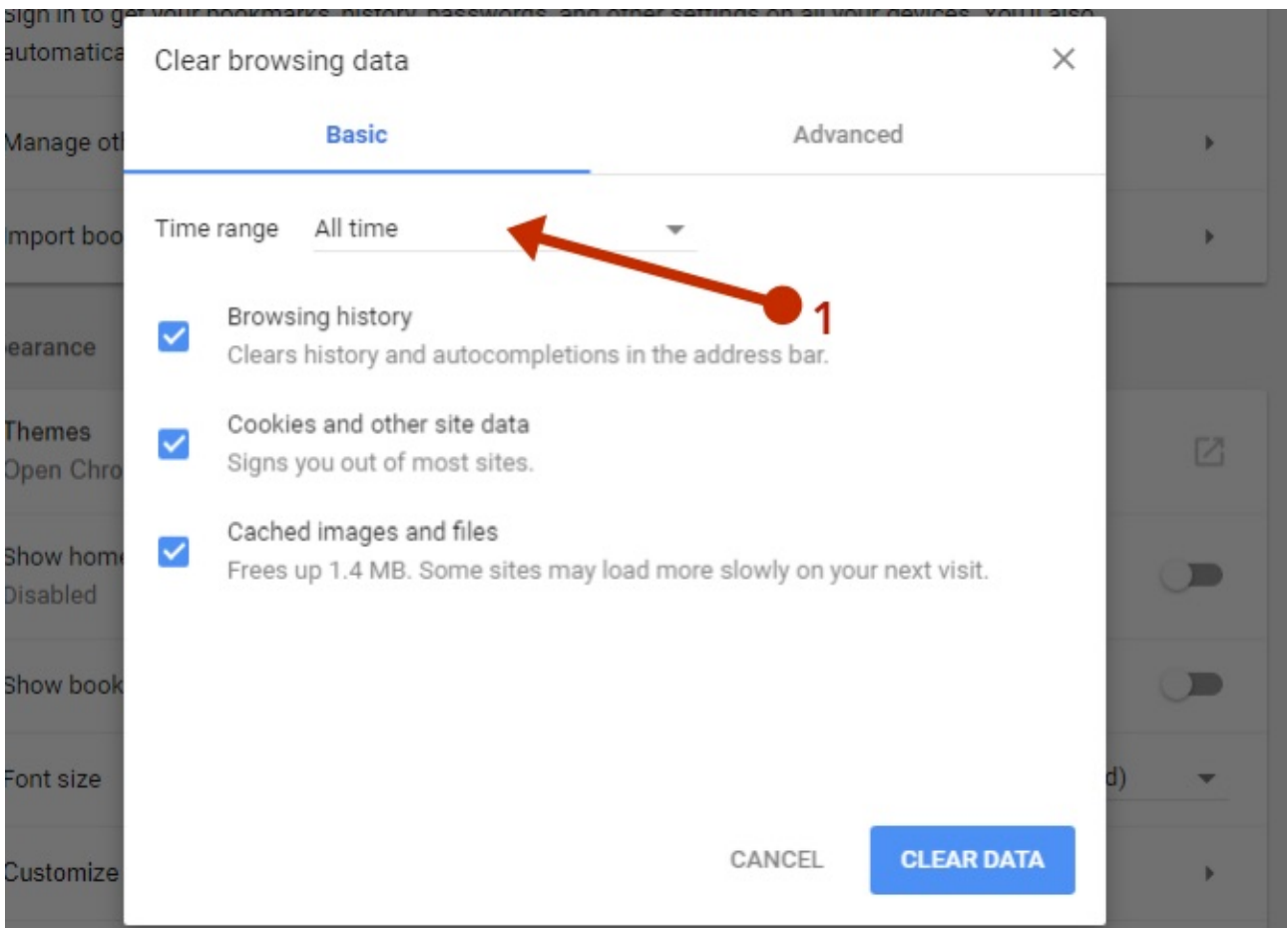


As you can see, using the process of elimination, you can quickly get to the bottom of where the problem may lie. Restarting your devices will in most cases solve the issues.

Browser Issues

If a different website works, the website you initially tried to load may be down. If a different browser works, your initial browser may need its **cache and residual files to be cleared**.

This can be done in Chrome by going to Settings > More Tools > Clear browsing data. In the dialog box that pops up, select All time from the Time range selection. Under the Advanced tab select Hosted app data, and finally, click the Clear Data button.



This will require you to sign in to any websites you were previously signed into and clear your browsing history. Ensure that any sites you need to refer back to are bookmarked.

Area Outages

Depending on where you live and who your ISP is this is generally uncommon but not unheard of. There is a website which has an awesome community that reports if there is a fault with common internet services, namely [Downdetector](#).

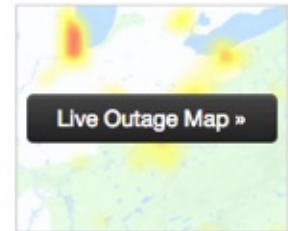
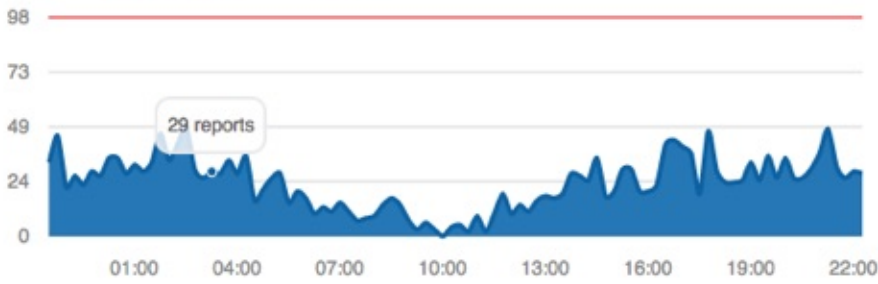
Comcast

Comcast offers cable television, internet and home phone service. Services are branded Xfinity in areas where digital triple play services are available. Xfinity TV offers television over the internet (IPTV). Comcast serves homes and businesses in 40 states and the District of Columbia. Comcast is a majority shareholder of NBC Universal.



Possible problems at Comcast

Comcast problems last 24 hours

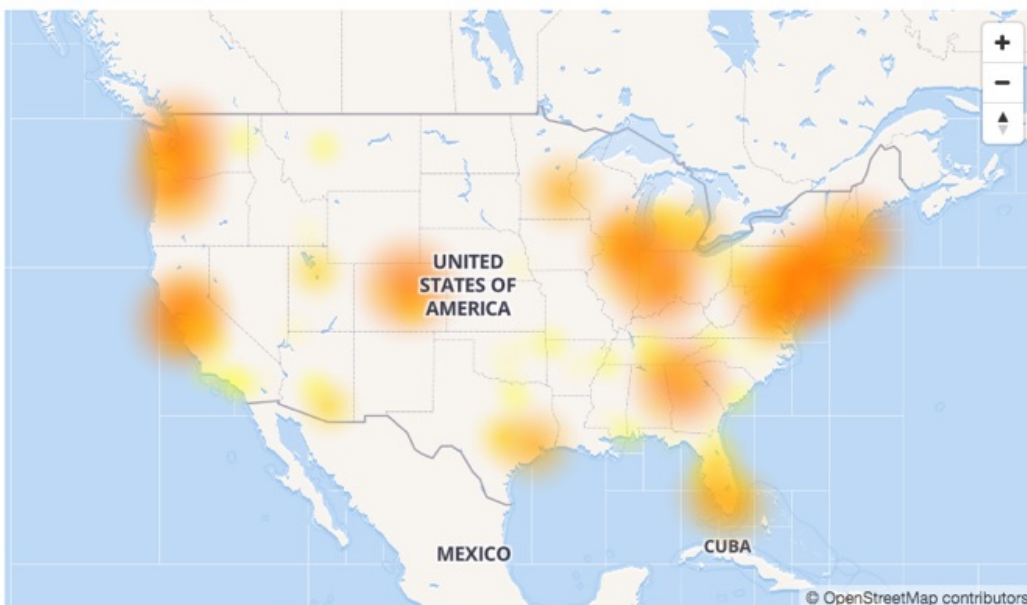


Using Downdetector, you can check the status of your ISP network according to what other people are reporting. If you see that many people are reporting an issue, there might be a problem with your ISP.

Comcast outage map

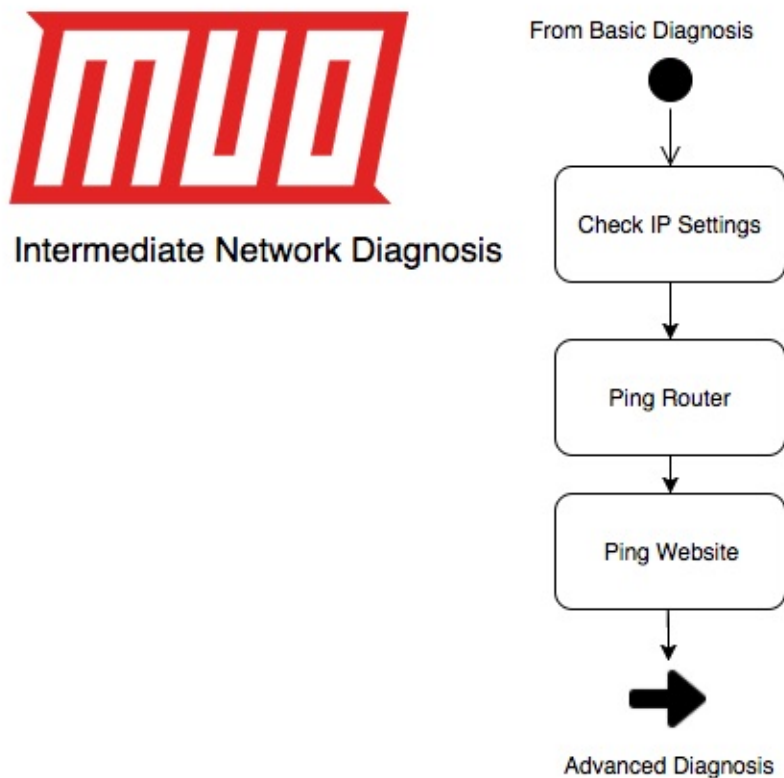
Recent reports mostly originate from: [Mountain View](#), [Chicago](#), [Bronx](#), [Seattle](#), [Houston](#), [Denver](#), [Washington](#), [Miami](#), [San Francisco](#), and [Portland](#).

Comcast outage chart



You can also use the Live Outage Map to make sure whether or not your specific area is affected. If you still suspect an area outage, you could check with your neighbors and finally call your ISP to make sure everything is dandy in your area.

Intermediate Diagnosis



If all of the above hasn't worked, it will now require further diagnosis. Our flow goes like this:

1. Check IP Settings.
2. Can you ping your router?
3. Can you ping a website?

You can check your IP settings, as shown above by going to **Control Panel > Network And Sharing Centre > [Connection] > Details**. Alternatively, open a command prompt by typing cmd into the run dialog box, and type this command:

```
ipconfig /all
```

```
C:\Users\MM>ipconfig /all

Windows IP Configuration

Host Name . . . . . : MM-PC
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . :
    Description . . . . . : Intel(R) 82567LM-3 Gigabit Network Connection
    Physical Address. . . . . : B8-AC-6F-24-6C-E0
    DHCP Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    Autoconfiguration IPv4 Address. . : 169.254.188.19(Preferred)
    Subnet Mask . . . . . : 255.255.0.0
    Default Gateway . . . . . :
    NetBIOS over Tcpip. . . . . : Enabled
```

If you notice that the IP address looks like the image above, your device is having a problem getting its IP settings from the DHCP server. If your IP settings look fine, you should try a ping. A ping is a utility used to check the reachability of a device via its IP address or hostname. It can also provide insight as to whether DNS is working and how long it is taking for a device to respond. Our flow shows trying to ping the router first, so in your command prompt type:

```
ping [IP-address-of-router]
```

```
C:\Users\Yusuf Limalia>ping 10.1.2.1

Pinging 10.1.2.1 with 32 bytes of data:
Reply from 10.1.2.1: bytes=32 time=6ms TTL=64
Reply from 10.1.2.1: bytes=32 time=13ms TTL=64
Reply from 10.1.2.1: bytes=32 time=1ms TTL=64
Reply from 10.1.2.1: bytes=32 time=3ms TTL=64

Ping statistics for 10.1.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 13ms, Average = 5ms
```

If you see a constant response, like the one above, your connection between your device and your router is perfect. If your ping looks something similar to this:

```
C:\Users\Yusuf Limalia>ping 172.31.45.1

Pinging 172.31.45.1 with 32 bytes of data:
PING: transmit failed. General failure.
Reply from 172.31.45.1: bytes=32 time=4ms TTL=63
General failure.
General failure.

Ping statistics for 172.31.45.1:
    Packets: Sent = 4, Received = 1, Lost = 3 (75% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 4ms, Average = 4ms
```

In the above case, there is a problem between your device and the router. If your local ping is fine, try pinging a website on the internet. There are two things that happen with a ping to a website on the internet. Our sequence diagram above shows that a DNS server first has to resolve the hostname into an IP address. Once the name is resolved, the ping will begin. A healthy ping will show the IP address next to the website you're trying to ping like this:

```
C:\Users\Yusuf Limalia>ping google.com

Pinging google.com [216.58.201.46] with 32 bytes of data:
Reply from 216.58.201.46: bytes=32 time=7ms TTL=55
Reply from 216.58.201.46: bytes=32 time=7ms TTL=55
Reply from 216.58.201.46: bytes=32 time=7ms TTL=55
Reply from 216.58.201.46: bytes=32 time=8ms TTL=55

Ping statistics for 216.58.201.46:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 7ms, Maximum = 8ms, Average = 7ms
```

A ping result like this might indicate that there is a DNS problem:

```
C:\Users\Yusuf Limalia>ping google.com
Ping request could not find host google.com. Please check the name and try again.



C:\Users\Yusuf Limalia>
```

DNS

By default, your ISP will assign you a primary and a secondary DNS server. Your computer or smart device may only show the router being the primary device, but your router is just acting as an intermediary or a forwarder.

Changing the default assignment actually might have some benefits. These benefits may include better security and a faster browsing experience. Google's public DNS servers can be a viable option on which DNS server you should use.

LAN >> General Setup

LAN 1 Ethernet TCP / IP and DHCP Setup	LAN 1 IPv6 Setup
Network Configuration For NAT Usage IP Address: <input type="text" value="10.1.2.1"/>  Subnet Mask: <input type="text" value="255.255.255.0"/> RIP Protocol Control: <input type="button" value="Disable"/> 	DHCP Server Configuration <input checked="" type="radio"/> Enable Server <input type="radio"/> Disable Server <input type="checkbox"/> Enable Relay Agent Start IP Address: <input type="text" value="10.1.2.10"/> IP Pool Counts: <input type="text" value="200"/> Gateway IP Address: <input type="text" value="10.1.2.1"/> Lease Time: <input type="text" value="86400"/> (s) <input checked="" type="checkbox"/> Clear DHCP lease for inactive clients periodically
	DNS Server IP Address Primary IP Address: <input type="text" value="8.8.8.8"/> Secondary IP Address: <input type="text" value="8.8.4.4"/>

Your router's DNS options are generally found under the DHCP settings, and you could set it to the Google public DNS as follows:

- Primary: 8.8.8.8
- Secondary: 8.8.4.4

Once these are set and saved on your router, you can refresh your device's IP settings for good measure. An easy way to do this without restarting is by running the following in a command prompt:

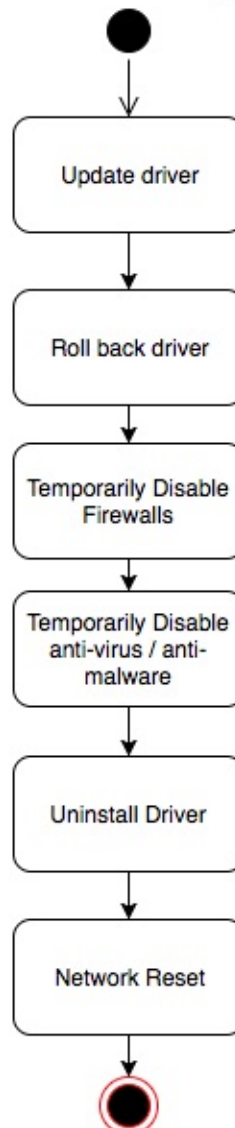
```
ipconfig /flushdns  
  
ipconfig /release ipconfig /renew
```

The above will first clear your cached DNS entries, then release and renew your IP settings.

Advanced Diagnosis



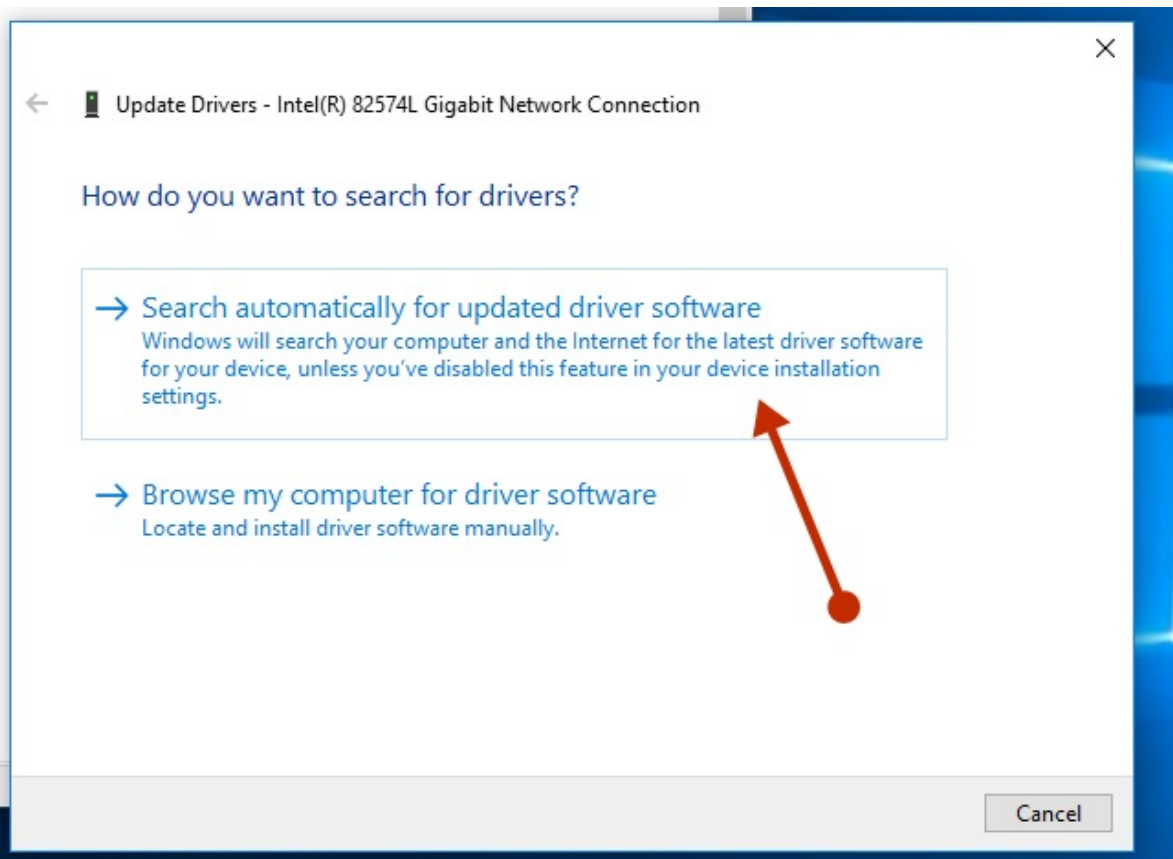
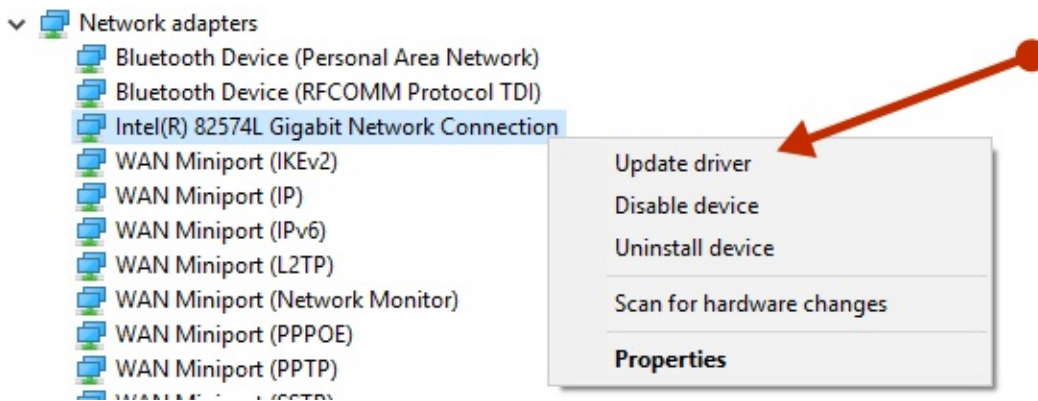
From Intermediate Diagnosis



1. Update the adapter driver.
2. Roll back the network adapter driver.
3. Temporarily turn off firewalls.
4. Temporarily turn off anti-virus or anti-malware software.
5. Uninstall the network adapter driver.
6. Perform a network reset.

An outdated or incompatible network adapter driver can cause connection problems. If you recently upgraded to Windows 10, it's possible that the current driver was designed for a previous version of Windows. You can find all your PC components drivers under the **Device Manager**. There's a shortcut on how to get there in the **Wired section above**.

Right-click on the network adapter and select Update driver and select Search automatically for updated driver software.

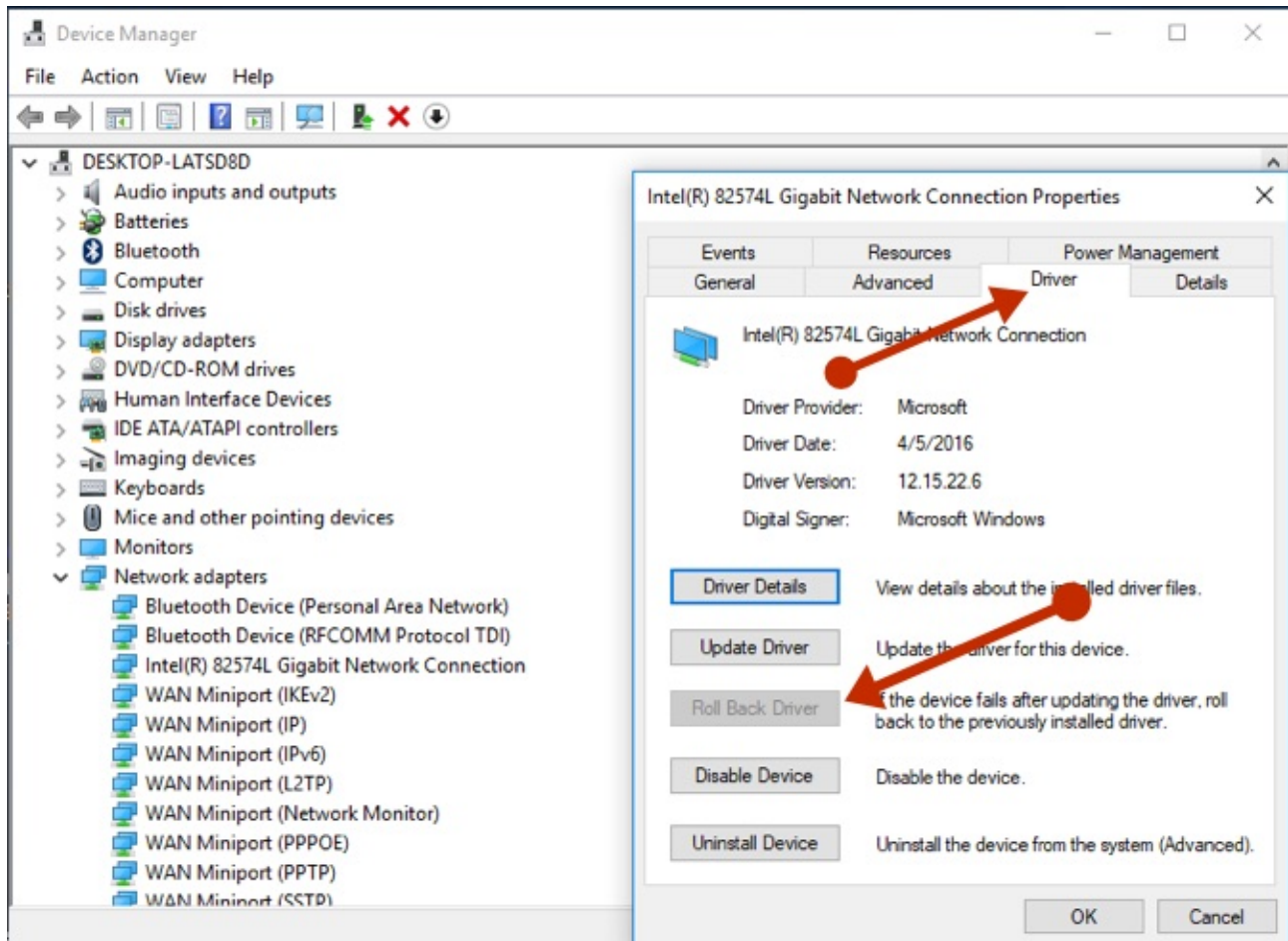


While you may not have an internet connection, Windows may have a local updated driver. Restart your PC and check your network.

You can also go to your PC or motherboard manufacturers website and get the latest version of the driver. You will need another computer to do so and a USB drive to transfer the driver to your problem PC for installation.

It's possible a newly installed network driver is causing an issue, so you can **roll the driver back**.

In Device Manager, right-click the adapter and click on **Properties**. Under the **Driver** tab, look for the **Roll Back Driver** button. If the button is greyed out, there is no driver to roll back to. If you can click it, follow the steps and restart your PC, then check your network connection.

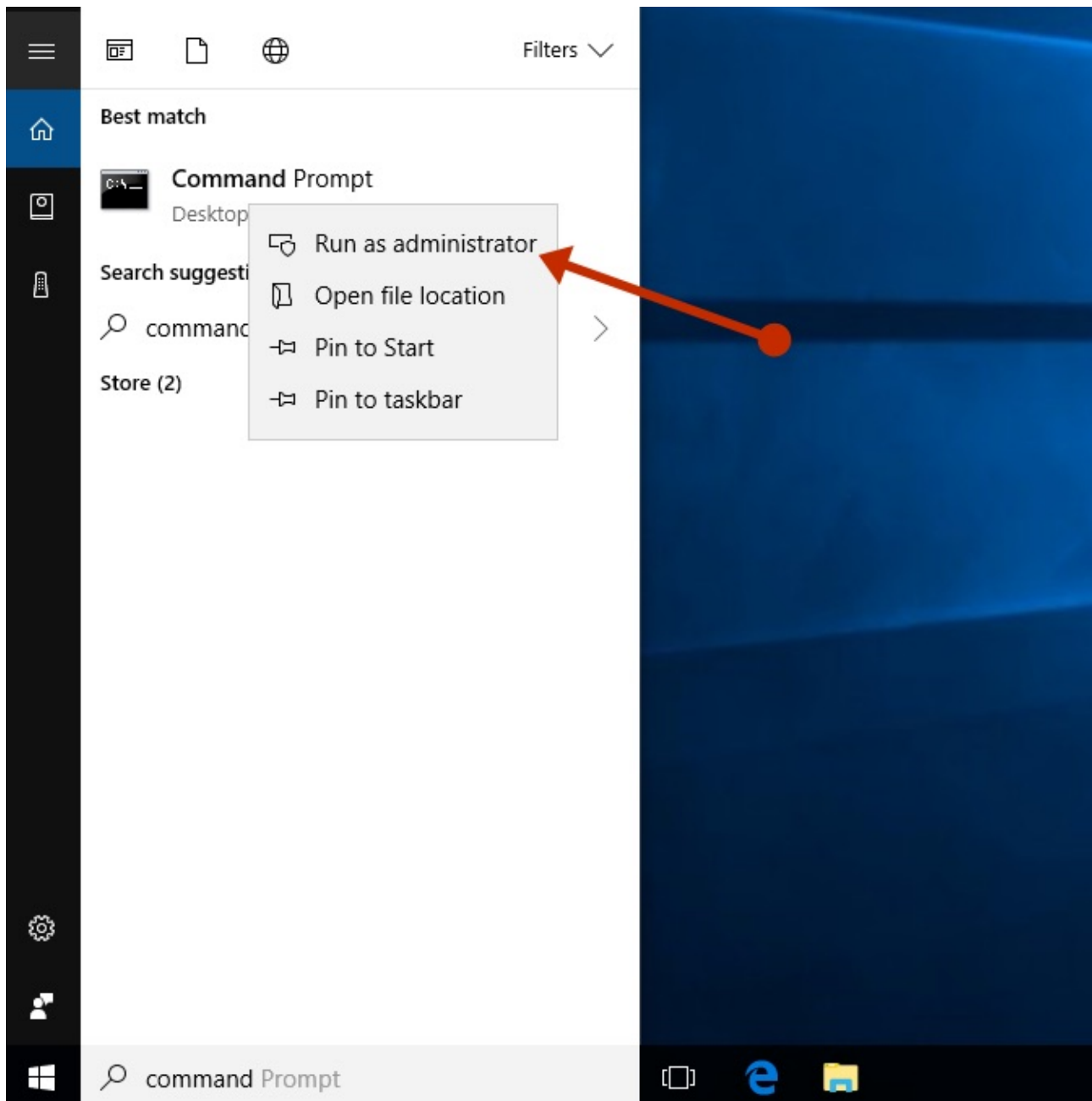


Firewalls and Anti-Malware

Sometimes, firewall software might prevent you from getting connected. You can see if the connection issue is caused by a firewall by turning it off temporarily and then trying to visit a website you trust.

The steps to turn off a firewall depend on the firewall software you're using. Check the documentation for your firewall software to learn how to turn it off. While disabling your firewall makes your PC vulnerable, doing it temporarily and visiting a site you trust should be okay. Make sure you turn it back on as soon as possible.

To turn the windows firewall off, search for **Command prompt** in the **Start Menu**, right-click it and select **Run as administrator** followed by **Yes**.



At the command prompt type:

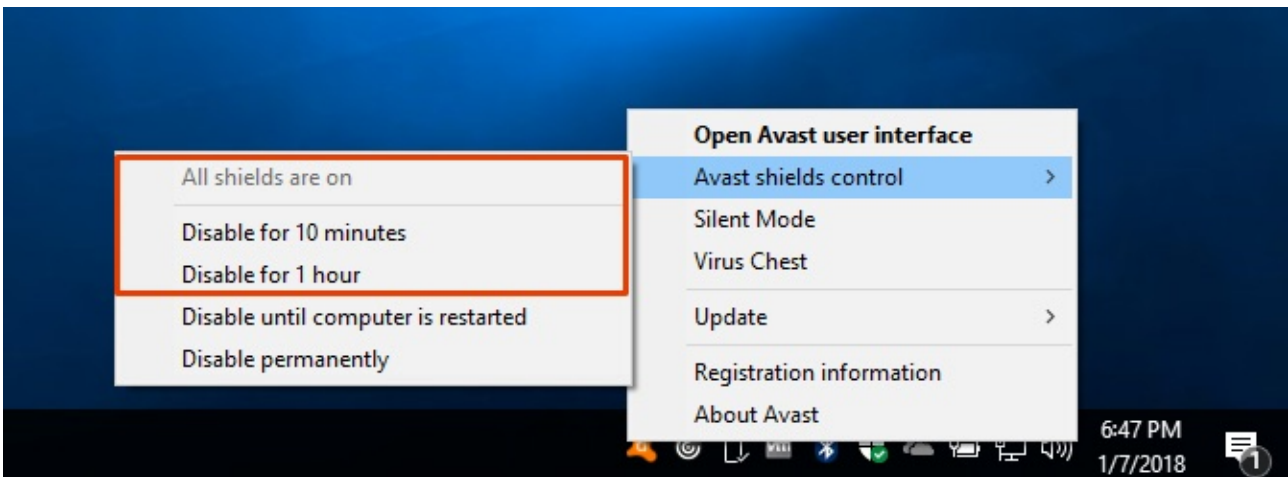
```
netsh advfirewall set allprofiles state off
```

Open a browser and visit a website you trust to see if your network is working. If it doesn't then your firewall is not causing the issue. To turn it back on, in the same command prompt type:

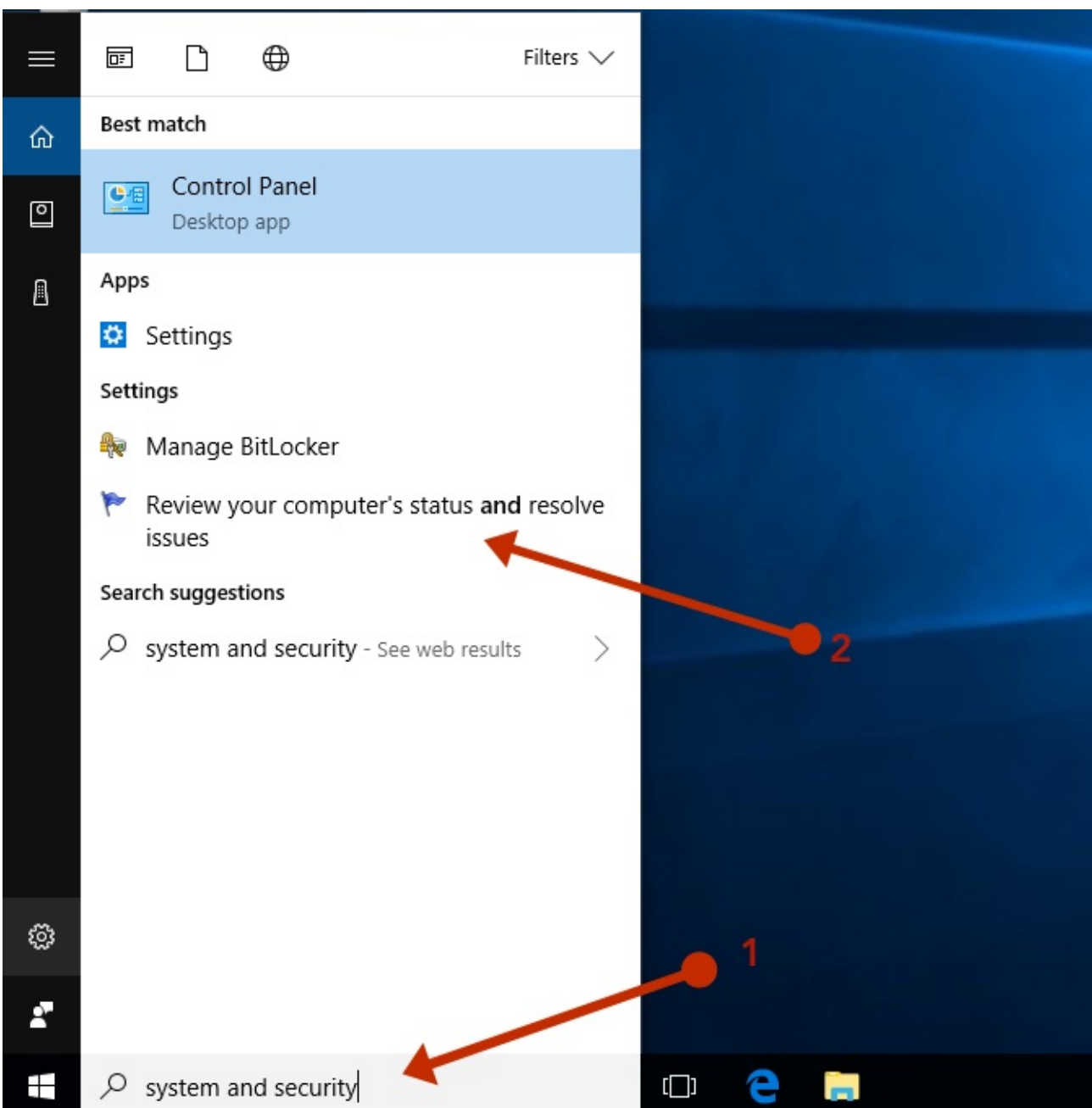
```
netsh advfirewall set allprofiles state on
```

If you find the firewall software is causing the connection issues, contact the software vendor or visit their website to check and see if updated software is available. You could also check your firewall rules to make sure there is nothing blocking your network connection in there.

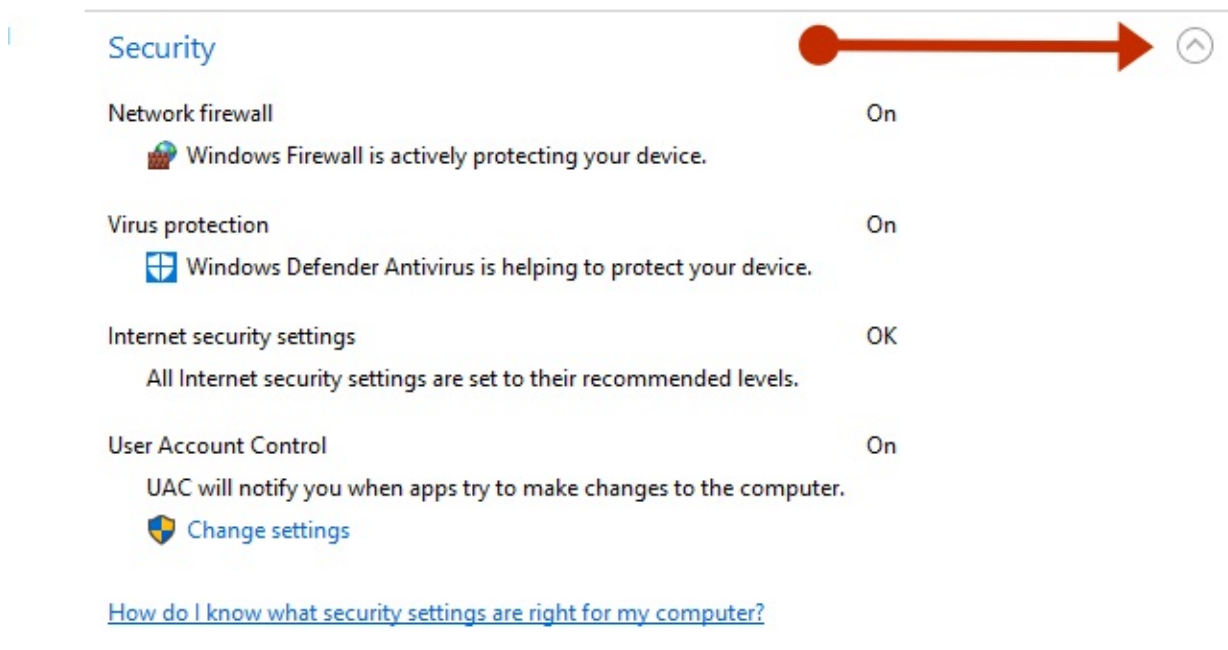
It's also possible that antivirus or anti-malware software is the root of your problem. Typically, you could pause protection by right-clicking the icon in the Taskbar and selecting **Disable**.



In Windows 10, you could check what security software you have installed. Type **system and security** in the Start Menu and select **Review your computer's status and resolve issues**.



Under the **Security** section, look for any third-party security software that's installed.

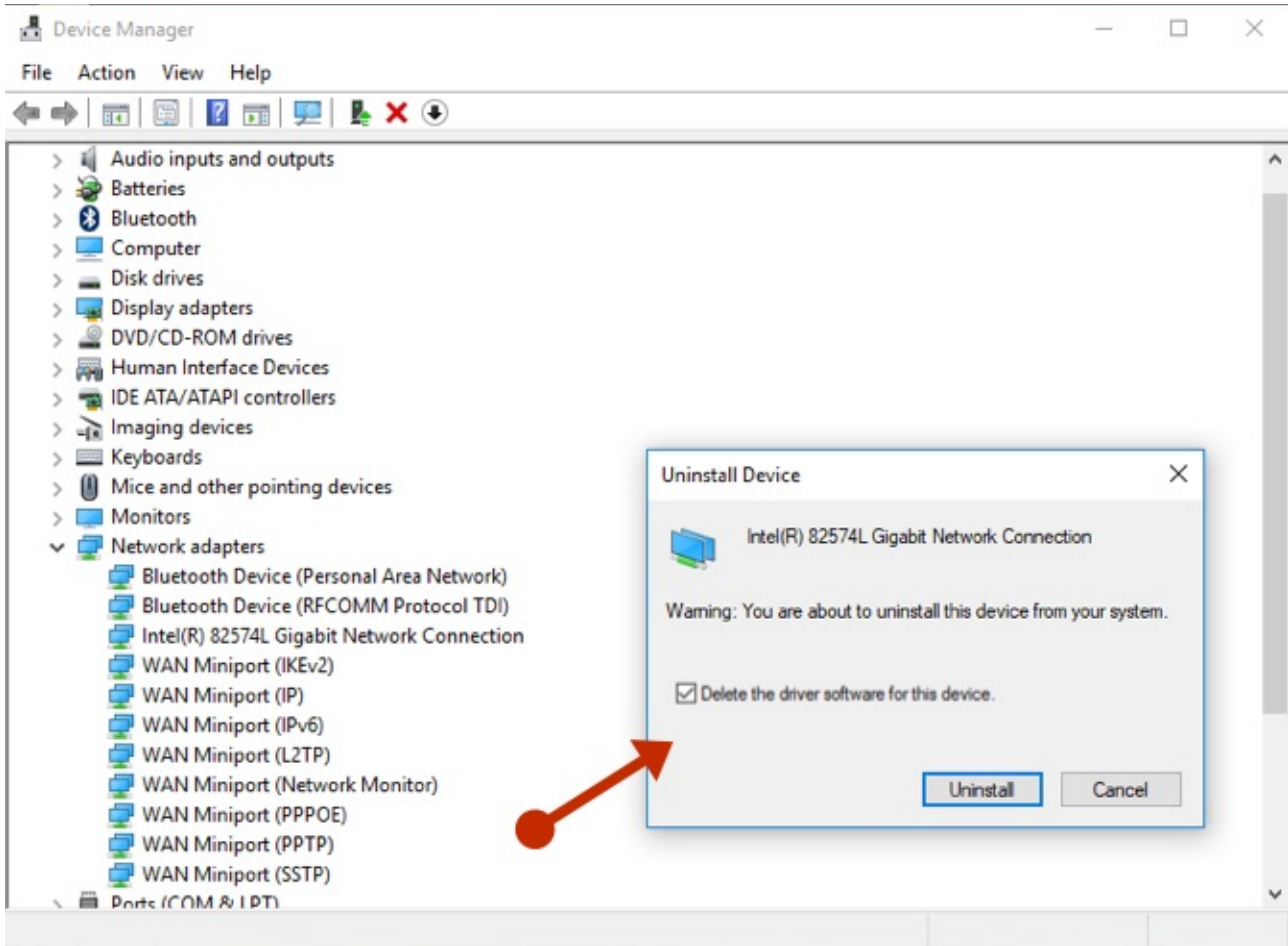


Uninstalling the Network Adapter

If the previous steps didn't work, try uninstalling the network adapter driver, and then restart your computer and have Windows **automatically install the latest driver**. Consider this approach if your network connection stopped working properly after a recent update.

To be safe, ensure you have drivers available as a backup. Visit the PC manufacturer's website and download the latest network adapter driver from there. You may have to do this on another PC and copy it to USB drive.

Right-click your adapter in the Device Manager and select Uninstall device. If there is a checkbox which shows Delete the driver software for this device select it and click Uninstall. Now restart your computer.

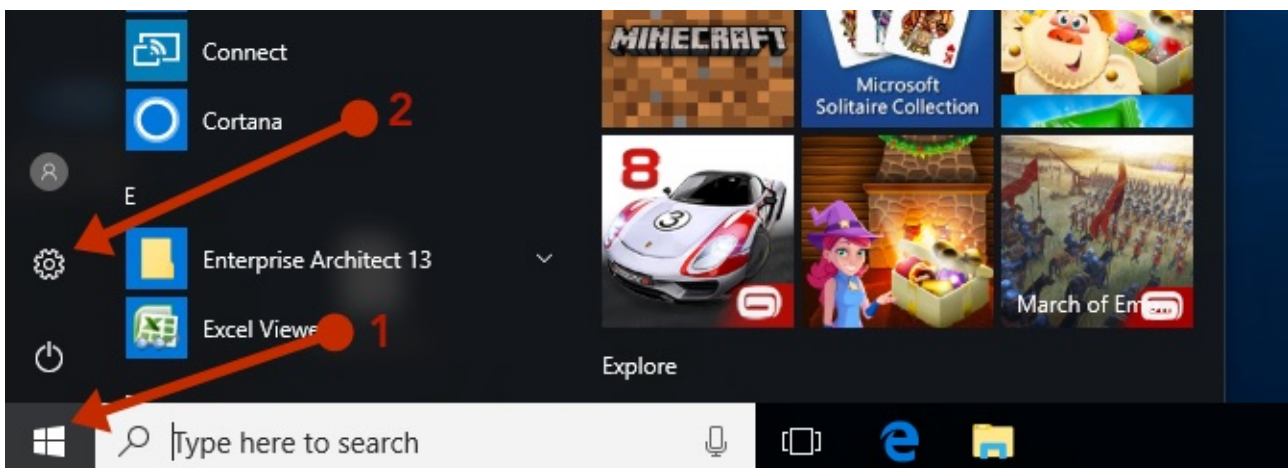


After your PC restarts, Windows will automatically look for and install the network adapter driver. Check to see if that fixes your connection problem. If Windows doesn't automatically install a driver, try to install the backup driver you saved before uninstalling.

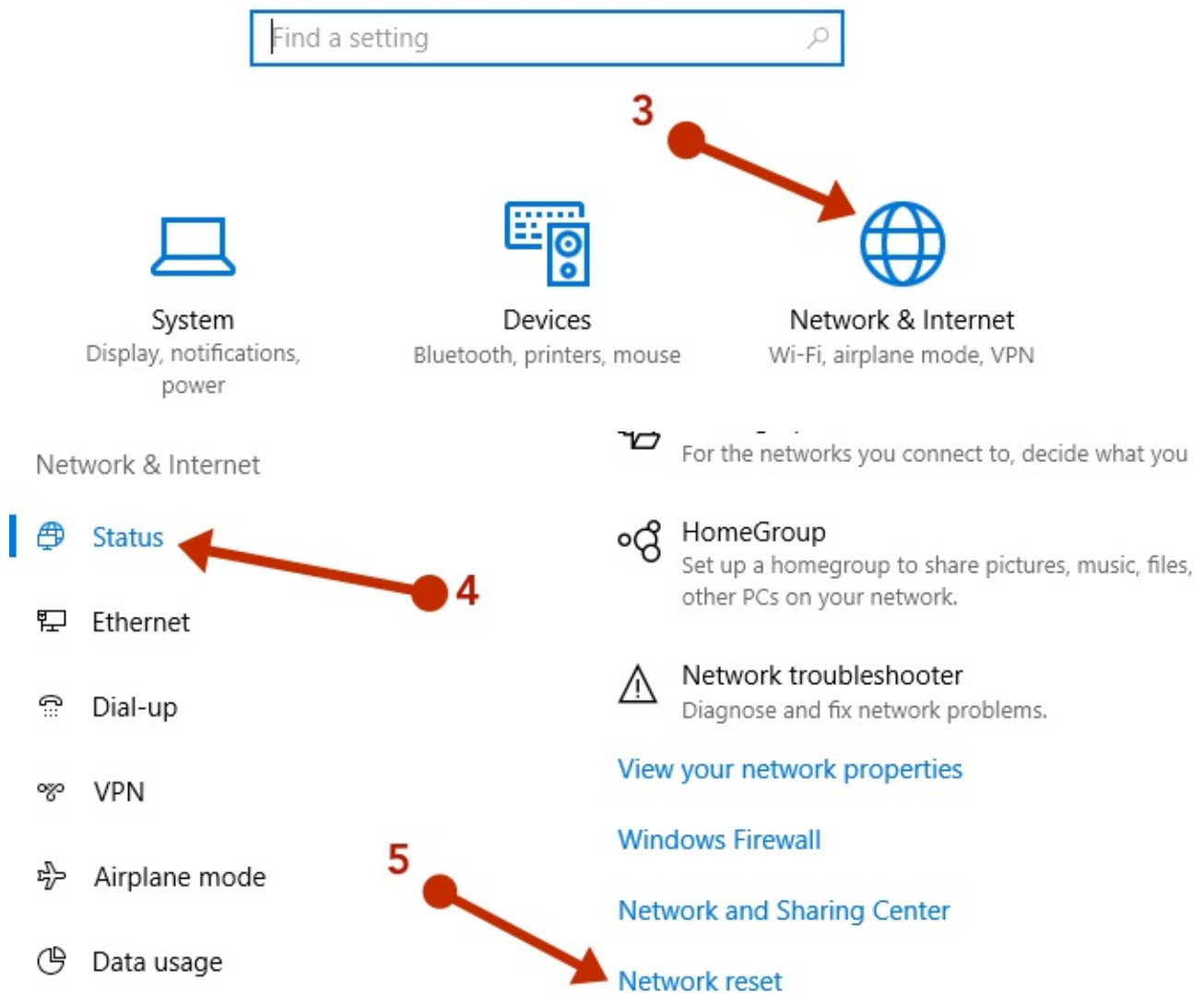
Network Reset (Windows 10)

This option removes any network adapters you have installed and the settings for them. After your PC restarts, any network adapters are reinstalled, and the settings for them are set to the defaults.

Select the **Start** button, then select **Settings > Network & internet > Status > Network reset**. On the Network reset screen, select **Reset now > Yes** to confirm. Wait for your PC to restart and see if that fixes the problem.

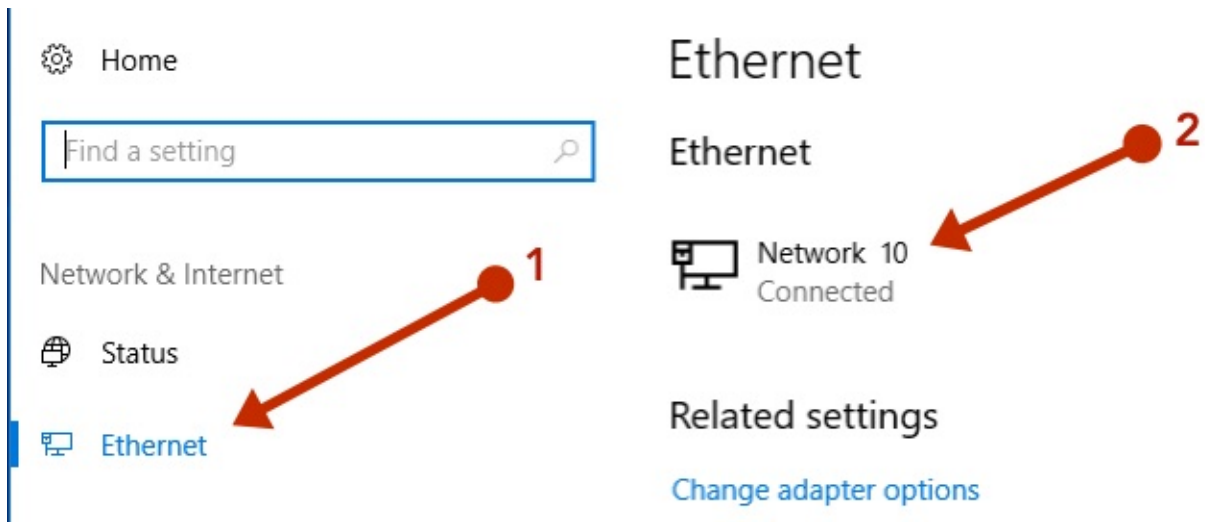


Windows Settings



Network reset might set each one of your known network connections to a public network profile. In a public network profile, your PC is not discoverable to other PCs and devices on the network. However, if your PC is part of a homegroup or used for file or printer sharing, you'll need to make your PC discoverable again by setting it to use a private network profile.

This can be done from the same menu. Depending on the type of network connection that you use. Ethernet will show you your current network connection which can be either your LAN cable connection or your Wi-Fi connection. Click on the connection name on the right under Ethernet. It should be the name of your LAN or Wi-Fi network. Check the switch **Find devices and content**.



Network 10

Make this PC discoverable

Allow your PC to be discoverable by other PCs and devices on this network. We recommend turning this on for private networks at home or work, but turning it off for public networks to help keep your stuff safe.



Wired Ethernet Problems

If your problem device is on a wired ethernet connection and another device that is also on a wired connection works, you've narrowed it down to the wired connection being a problem.

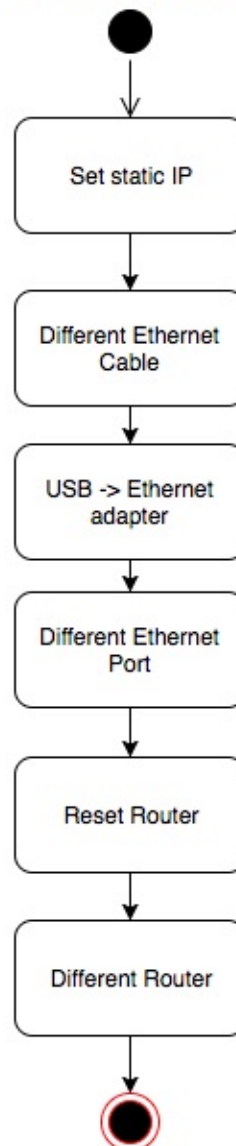
Always start with the simplest solution first. After going through the basic, intermediate and advanced diagnosis above, start by eliminating possibilities. If your device is connected first to a switch, which is in turn connected to the router, try connecting your problem device directly to the router.

You should now have the shortest path between your problem device and the internet. **Device > Router / Modem > internet.**



Wired Ethernet Problems

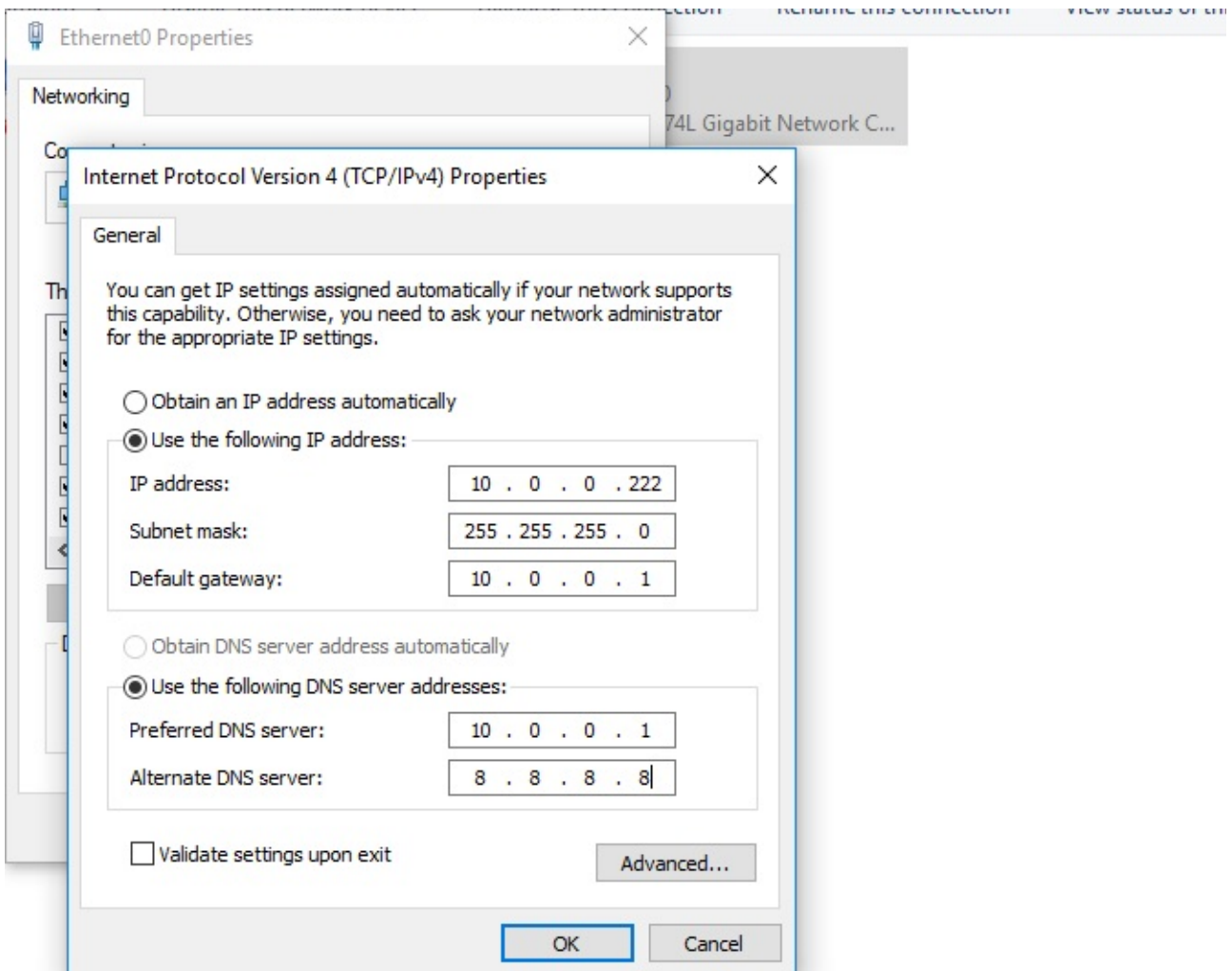
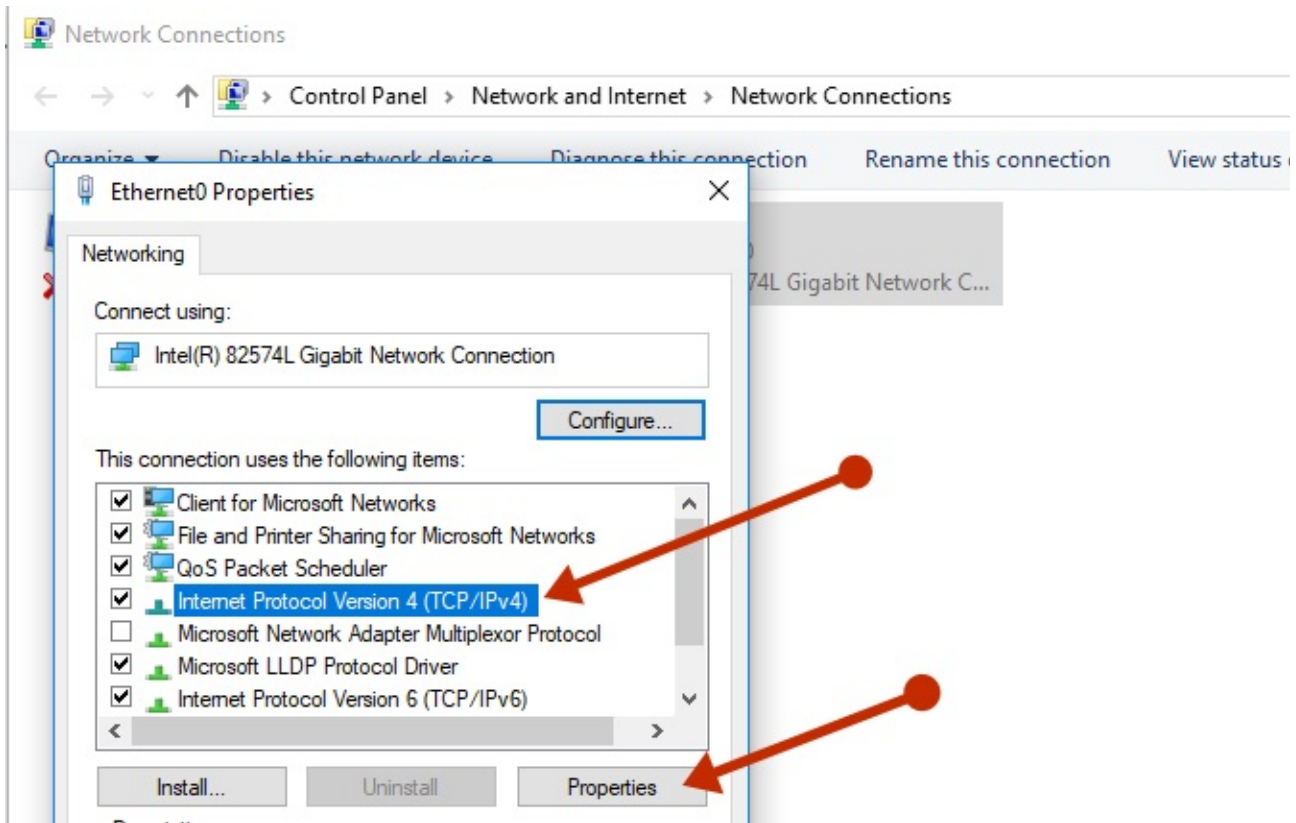
From Advanced Diagnosis



The last few troubleshooting steps you could try now is:

1. Set a static IP.
2. Use a different ethernet cable that you know is working.
3. Try a USB to ethernet adapter.
4. Try a different ethernet port on your router.
5. Reset your router to factory settings.
6. Try a different modem/router that you know is working.

To set a static IP, go to Control Panel > Network and Sharing Center > Change adapter settings. Right-click on your adapter and select Properties. Highlight the item which shows (TCP/IPv4) and click on Properties. Set the following items according to your network:





1. IP address: an IP with the same first three numbers as your router, followed by an arbitrarily number that is unlikely to be used by another device on your network. This must be between 0 and 255.
2. Subnet mask: this is typically 255.255.255.0
3. Default gateway: IP address of your router, typically ends in .1
4. Preferred DNS server: IP address of your router
5. Alternate DNS server: a public DNS server like 8.8.8.8

If at this point your internet starts working there may be an issue with your DHCP server as it is not issuing the correct IP settings.

Wired Hardware Faults

The final steps will be testing the hardware to find the fault. You can grab a USB to ethernet adapter which is relatively inexpensive. If that works, your PC's ethernet adapter may be faulty. If your PC's ethernet adapter is onboard, that might raise concerns for the health of your motherboard.

Getting your hands on another modem/router might be slightly tricky. Your ISP may require a specific modem, but you will be spoilt for choice when it comes to a router. Try and borrow one temporarily and swap yours out to see if it makes a difference.

Resetting Your Router

Resetting your router to its factory settings needs some consideration. Note that your Wi-Fi, DHCP, and other settings will all be back to their default settings. This might be a good thing. It's possible one of the settings you've tweaked has caused your network to be malfunctioning.

The method of resetting your router will depend on the model and manufacturer. In general, there will be a little reset button on the back that needs to be pressed using a pin. Refer to your manufacturers manual for further information.

Some routers will allow a backup and restore of settings, but doing so might restore a setting that's causing your network woes!

Wi-Fi Problems

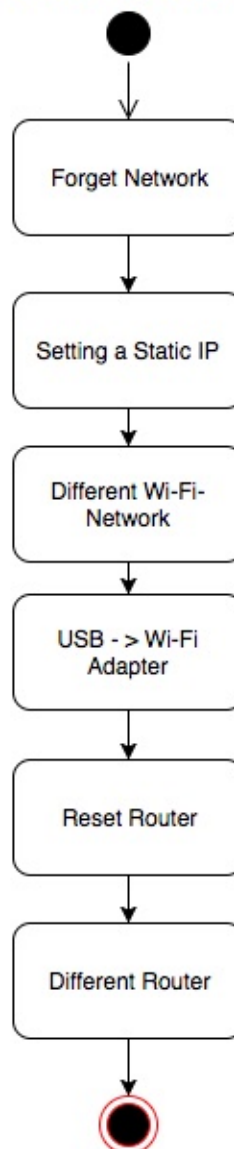
Wi-Fi can be tricky to troubleshoot because of the added variables in the equation. You have to eliminate interference from other devices, and there are more settings to take into account.

After you've configured your Wi-Fi with some of the suggestions above, and gone through the basic, intermediate and advanced diagnosis, we can start our elimination process. To eliminate interference issues sit as close as possible to the access point/router. If your internet works when you're close to your router but doesn't when you're far away, you may want to consider extending your wifi network.



Wi-Fi Problems

From Advanced Diagnosis



1. Forget and reconnect to your network.
2. Set a static IP.
3. Try a different Wi-Fi network.
4. Try a USB Wi-Fi Adapter.
5. Reset your router to factory settings.
6. Try a different modem/router that you know is working.

To forget your Wi-Fi network go to **Control Panel > Network and Sharing Center** and click **Manage wireless networks**. Right-click the connection you'd like to forget and click **Remove network**. You can try reconnecting to the removed network as normal.

Setting a static IP is the same as it's done on wired. To quickly try another Wi-Fi network, use your smart device as a hotspot. USB Wi-Fi adapters are also quite inexpensive.

Your Network Issues Resolved?

We've summarised all the steps in [this interactive checklist](#) which you can use on your PC or print out and step through. Remember our methodology on trying the simplest solutions before moving on to more advanced steps. As Occam's Razor states, the simplest solution is probably the likeliest! Happy networking!

What is your ideal network setup? How often do you have troublesome network issues? Let us know in [the comments section](#).

Read more stories like this at

