- 1. 1. 4. Networking essentials -

Modern computing is defined by our ability to communicate and share with one another by using devices of all shapes and sizes.

These days, most of that activity happens over the world's largest global network, the internet, using a variety of widely accepted hardware and software standards.

The internet is also the driving force behind cloud-based services, which are transforming the way we work and play.

The same network standards that allow connections to the internet can also be used to create a local area network (LAN), which makes it possible to share files, printers, and other resources in a home or an office.

In the not-so-distant past, setting up a network connection was a painful process, one that often required professional help.

Today, network hardware is ubiquitous, and setting up a network connection in Microsoft Windows 10 requires little or no technical knowledge.

That doesn't mean the process is entirely pain free; troubleshooting network problems can be maddeningly frustrating, and understanding the basics of networking is tremendously helpful in isolating and fixing problems.

Getting started with Windows 10 networking

Before you can connect to the internet or to a local area network, your Windows 10 device needs a network adapter, properly installed with working drivers.

Since the release of Windows 7, Microsoft's hardware certification requirements have mandated that every desktop PC, laptop, all-in-one, and portable device include a certified Ethernet or Wi-Fi adapter.

You'll typically find wired Ethernet adapters in desktop PCs and all-in-ones, where a permanent wired network connection is appropriate.

These adapters can be integrated into the motherboard or installed in an expansion slot and accept RJ45 plugs at either end of shielded network cables.

Most modern wired adapters support either the Fast Ethernet standard (also known as 100Base-T), which transfers data at 100 megabits per second, or the more modern Gigabit Ethernet standard, which allows data transfers at 1 gigabit (1,000 megabits) per second.

In an office or a home that is wired for Ethernet, you can plug your network adapter into a wall jack that connects to a router, hub, or switch at a central location called a patch panel.

In a home or an office without structured wiring, you need to plug directly into a network device.

In recent years, wireless networking technology has enjoyed an explosion in popularity.

Wireless access points are a standard feature in most home routers and cable modems, and Wi-Fi connections are practically ubiquitous.

You can connect to Wi-Fi, often for free, in hotels, trains, buses, ferries, and airplanes in addition to the more traditional hotspot locations such as cafés and libraries.

All laptops and mobile devices designed for Windows 10 include a Wi-Fi adapter, which consists of a transceiver and an antenna capable of communicating with a wireless access point.

Wireless adapters are also increasingly common in desktop and all-in-one computer designs, allowing them to be used in homes and offices where it is impractical or physically impossible to run network cables.

Ethernet and Wi-Fi are the dominant networking technologies in homes and offices.

Alternatives include phone-line networks, which plug into telephone jacks in older homes, and powerline technology, which communicates using adapters that plug into the same AC receptacles you use for power.

The availability of inexpensive wireless network gear has relegated phone-line and power-line technologies to niche status; they're most attractive in older homes and offices, where adding network cable is impractical and wireless networks are unreliable because of distance, building materials, or interference.

A hybrid approach, useful in some environments, allows you to plug a Wi-Fi extender into an existing power line to increase signal strength in a remote location.

You don't need to rely exclusively on one type of network.

If your cable modem includes a router and a wireless access point, you can plug network cables into it and use its wireless signal for mobile devices or for computers located in areas where a network jack isn't available.

When you upgrade to Windows 10, the setup program preserves your existing network connection.

If you perform a clean setup of Windows 10, your wired internet connection should be detected automatically; you're prompted to enter the access key for a wireless connection during the setup process.

Checking your network's status

As we noted earlier, most network connections in Windows 10 should configure themselves automatically during setup.

Three tools included with Windows 10 allow you to inspect the status of the current connection and either make changes or troubleshoot problems.

Using the network icon and flyout

The most easily accessible network tool is the status icon that appears by default in the notification area at the right side of the taskbar.

Its icon indicates the current network type (wired or wireless) and the status of the network.

Click that icon to display the network flyout, which displays options relevant to your type of network connection.

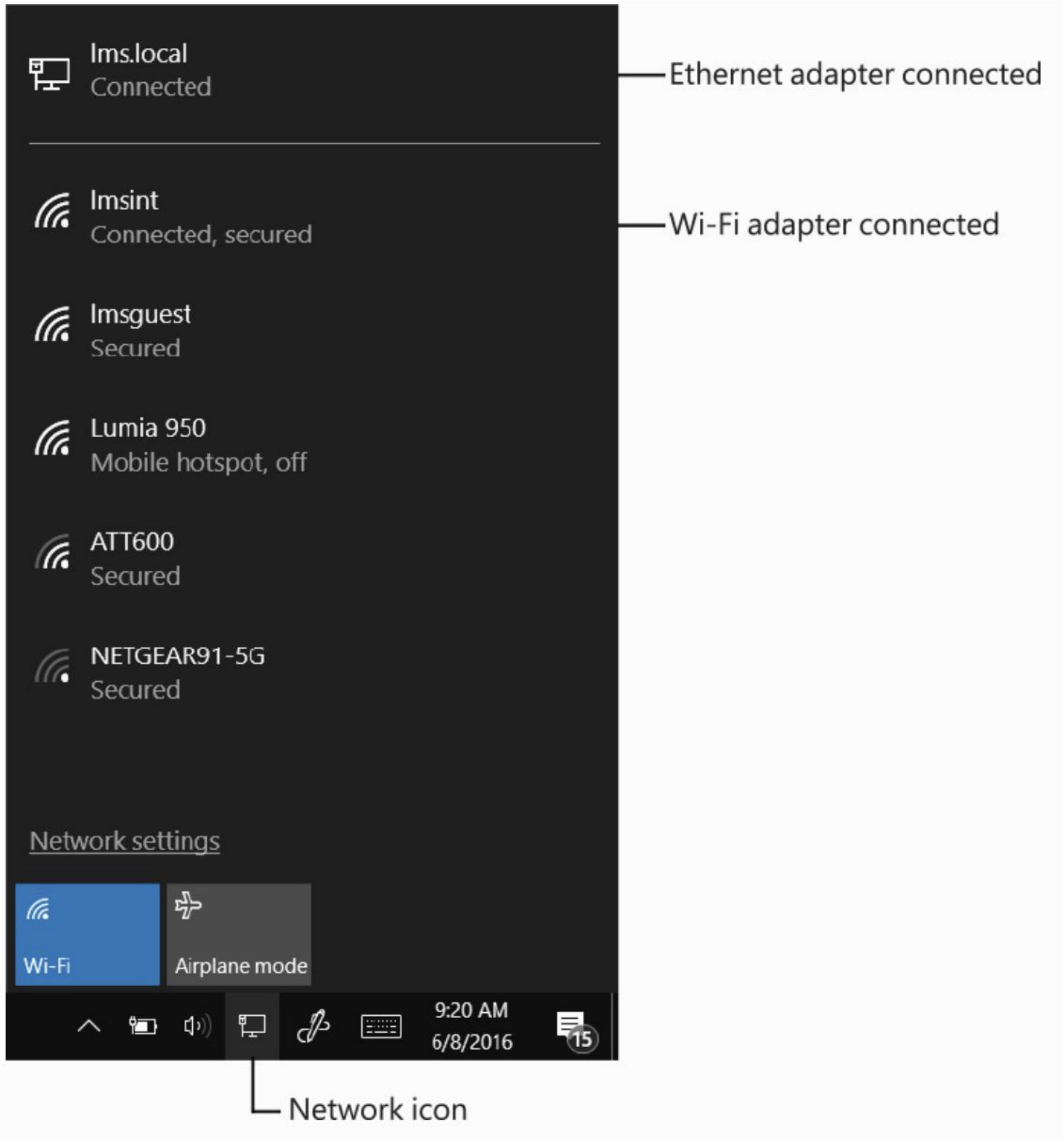
A portable computer with no physical Ethernet adapter sometimes shows the icon for a wired connection rather than wireless.

That can occur when you have a virtual network adapter set up for virtual machines as well as when you have a USB Ethernet adapter.

The following image shows the network flyout for a tablet with a USB Ethernet adapter connected to a wired network and a Wi-Fi connection to the "Lmsint" access point.

Both networks appear to be operating properly.

A status of "Limited" indicates problems with the network’s ability to connect to the internet.



Ethernet adapter connected

Wi-Fi adapter connected

Network icon

Every available network is shown on this list, including wired connections and wireless access points that are broadcasting their names.

In the previous figure, the PC is connected to both a wired network and a wireless access point.

Because the wired connection is faster, it gets priority, sitting at the top of the list with a line separating it from the wireless networks.

The icon for each access point indicates its signal strength, with the better signals rising to the top of the list.

Two buttons at the bottom of the network flyout are available on laptops and mobile devices.

Click or tap "Wi-Fi" to temporarily disable Wi-Fi connections; tap again to reconnect to a wireless network.

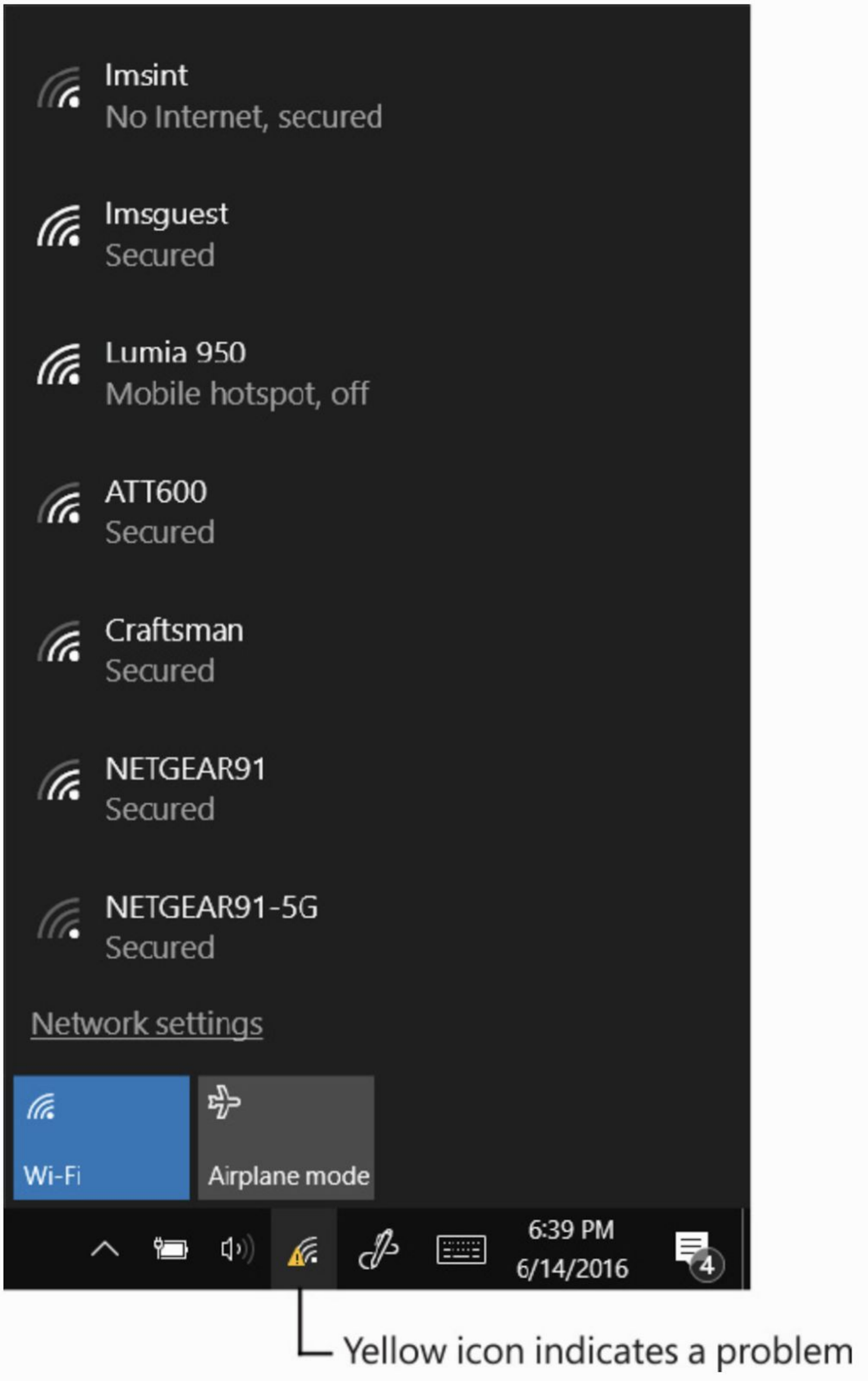
Clicking or tapping "Airplane Mode" shuts down all wireless communications, including Wi-Fi, Bluetooth, cellular, GPS, and near field communication (NFC).

You can selectively enable wireless devices by opening Settings > Network & Internet > Airplane Mode.

A red X or yellow triangle over the network icon means your connection is not working properly.

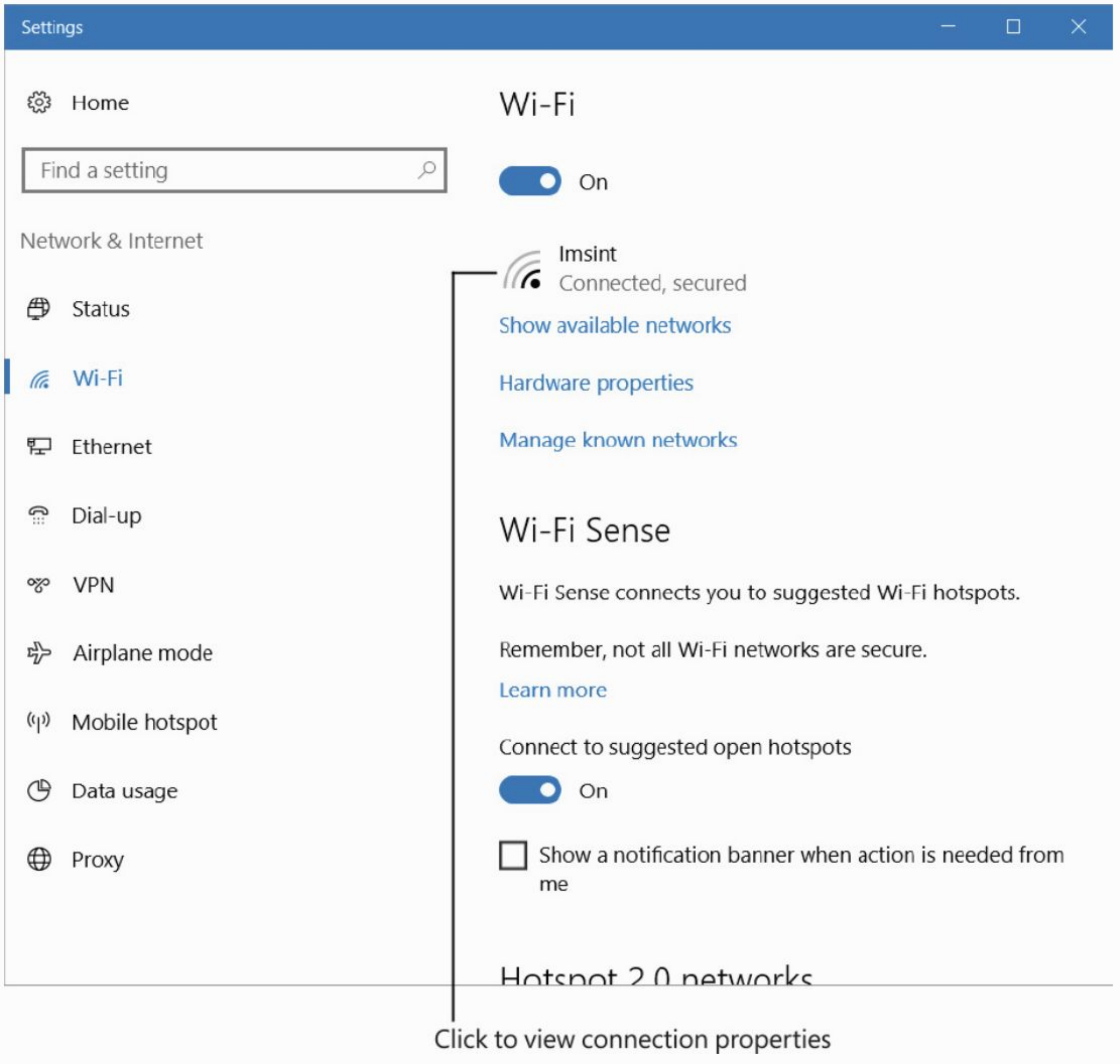
In the next figure, for example, the yellow triangle with an exclamation point is Windows 10's way of warning that something's wrong with that connection.

The network flyout shows that the wireless adapter is connected to an access point but isn't able to reach the internet.



The "Network Settings" link at the bottom of the network flyout leads to "Network & Internet" in Settings, with details for the current network shown by default.

On a tablet with a wireless connection, that page looks something like the one shown in the following figure:



Settings

Home

Find a setting

Network & Internet

Status

Wi-Fi

Ethernet

Dial-up

VPN

Airplane mode

Mobile hotspot

Data usage

Proxy

Wi-Fi

On

Imsint
Connected, secured

Show available networks

Hardware properties

Manage known networks

Wi-Fi Sense

Wi-Fi Sense connects you to suggested Wi-Fi hotspots.

Remember, not all Wi-Fi networks are secure.

Learn more

Connect to suggested open hotspots

On

□ Show a notification banner when action is needed from me

Hotspot 2.0 networks

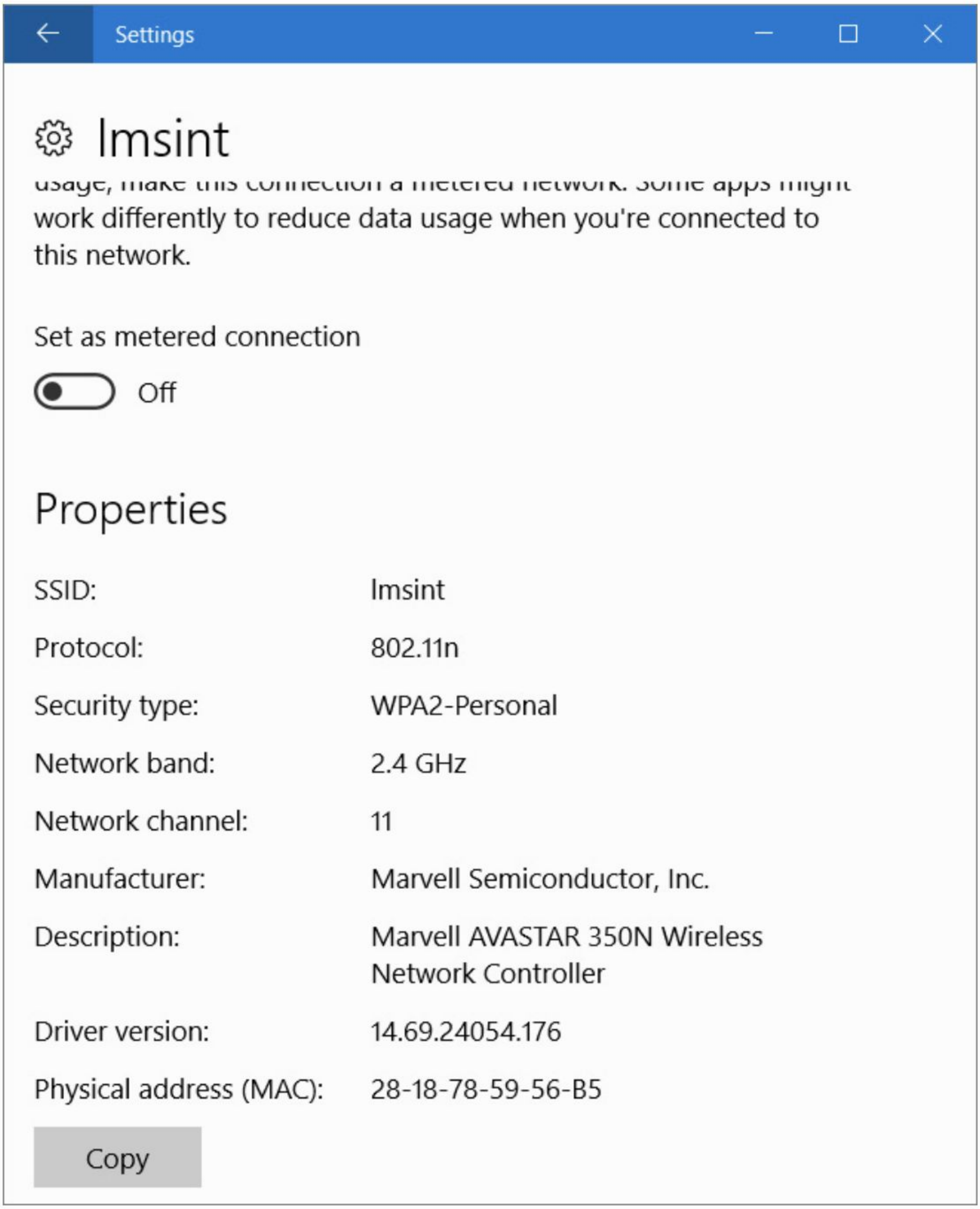
Click to view connection properties

Clicking the icon for a wired connection in the flyout displays details about that connection: its IP addresses, Domain Name System (DNS) settings, and network adapter (including manufacturer name and current driver version).

You can get to the equivalent information for a wireless connection by clicking the icon in the flyout and then clicking or tapping Properties.

For either type of connection, you can reach the same details by clicking the network’s icon in Settings > Network & Internet, as shown in the previous image.

The following image shows the properties for a wireless network connection, which includes details about the wireless network and the network adapter:



Imsint

usage, make this connection a metered network. Some apps might work differently to reduce data usage when you're connected to this network.

Set as metered connection

● Off

Properties

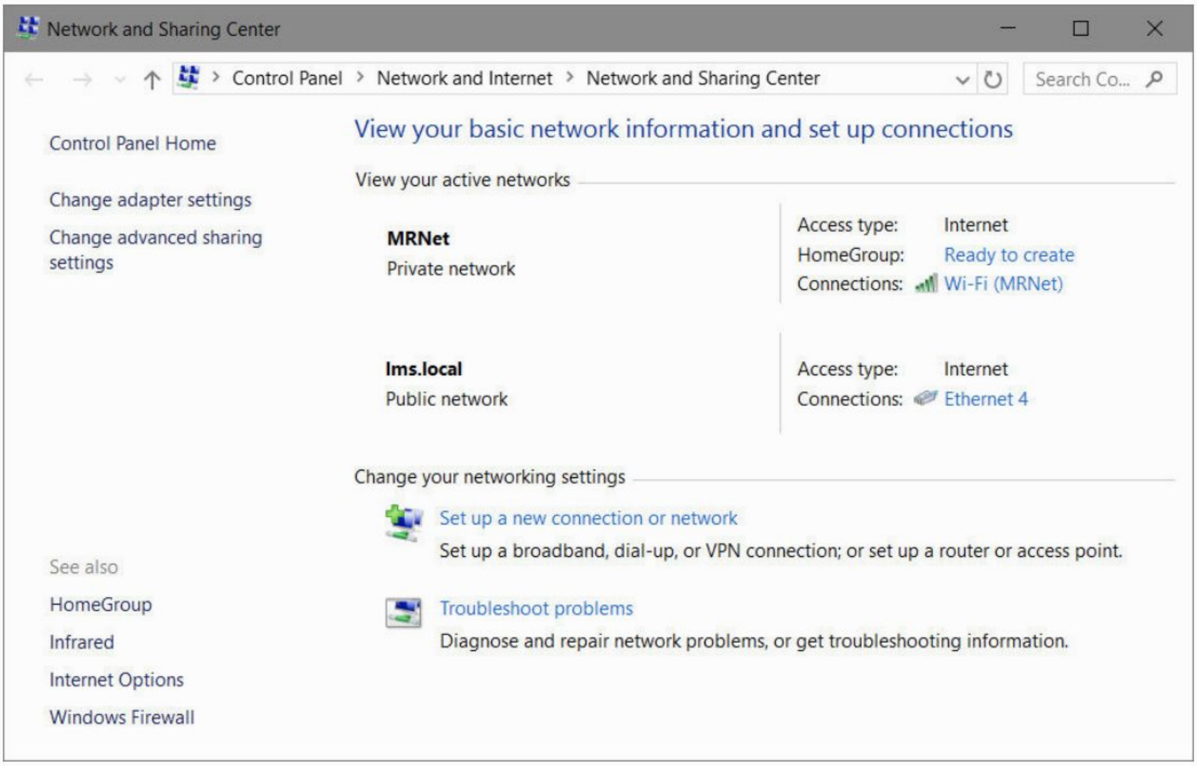
SSID:	Imsint
Protocol:	802.11n
Security type:	WPA2-Personal
Network band:	2.4 GHz
Network channel:	11
Manufacturer:	Marvell Semiconductor, Inc.
Description:	Marvell AVASTAR 350N Wireless Network Controller
Driver version:	14.69.24054.176
Physical address (MAC):	28-18-78-59-56-B5

These details for a network connection are essential for troubleshooting networking problems.

Click the "Copy" button to save the settings to the Clipboard to paste into a help desk ticket or an email message.

Network And Sharing Center

If you've managed a network in Windows 7, you're probably already familiar with "Network And Sharing Center", which was the hub of almost all networking activities.


Network and Sharing Center
Control Panel > Network and Internet > Network and Sharing Center
Search Co...
Control Panel Home
Change adapter settings
Change advanced sharing settings
See also
HomeGroup
Infrared
Internet Options
Windows Firewall

View your basic network information and set up connections

View your active networks

MRNet
Private network

Access type: Internet
HomeGroup: Ready to create
Connections: Wi-Fi (MRNet)

lms.local
Public network

Access type: Internet
Connections: Ethernet 4

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

Network And Sharing Center provides a snapshot of the active network (or networks, as shown here) and includes links to nearly every relevant related task or setting.

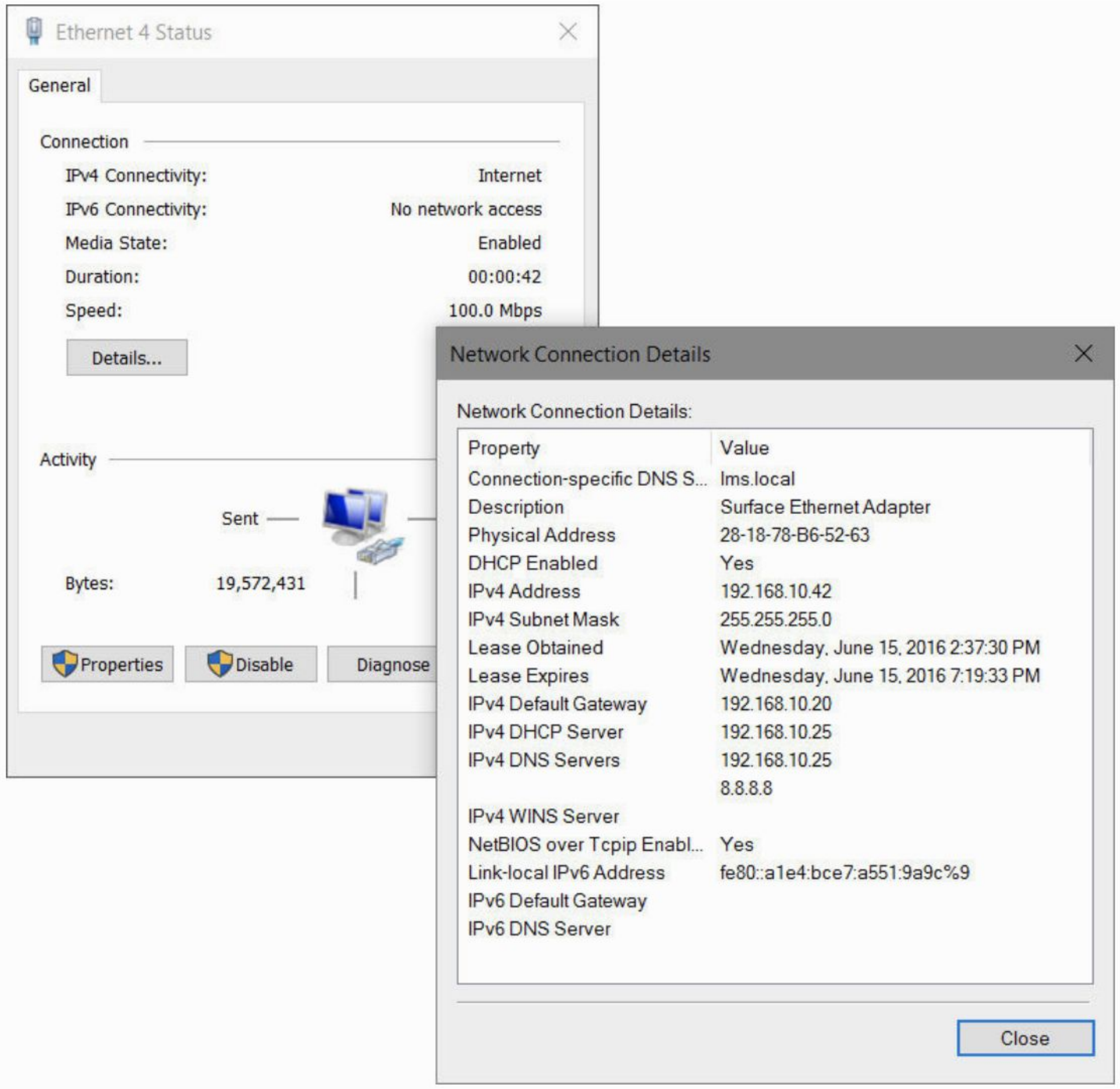
In the previous image, you can see that this computer is connected to two networks.

One is a wireless connection that is configured to be private, allowing other PCs and devices on the same network to view shared resources.

The Ethernet connection is currently set up as a public network, such as one in a public location like an airport or hotel.

Clicking the name of an active connection—in this example, Ethernet 4—leads to a status dialog box, where a Details button leads to additional information.

The list of network details is a bit longer than its counterpart in the Settings app, as the following image illustrates:



IPv4 Connectivity: Internet
IPv6 Connectivity: No network access
Media State: Enabled
Duration: 00:00:42
Speed: 100.0 Mbps

Bytes: 19,572,431

Network Connection Details:

Property	Value
Connection-specific DNS S...	lms.local
Description	Surface Ethernet Adapter
Physical Address	28-18-78-B6-52-63
DHCP Enabled	Yes
IPv4 Address	192.168.10.42
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Wednesday, June 15, 2016 2:37:30 PM
Lease Expires	Wednesday, June 15, 2016 7:19:33 PM
IPv4 Default Gateway	192.168.10.20
IPv4 DHCP Server	192.168.10.25
IPv4 DNS Servers	192.168.10.25
	8.8.8.8
IPv4 WINS Server	
NetBIOS over Tcpip Enabl...	Yes
Link-local IPv6 Address	fe80::a1e4:bce7:a551:9a9c%9
IPv6 Default Gateway	
IPv6 DNS Server	

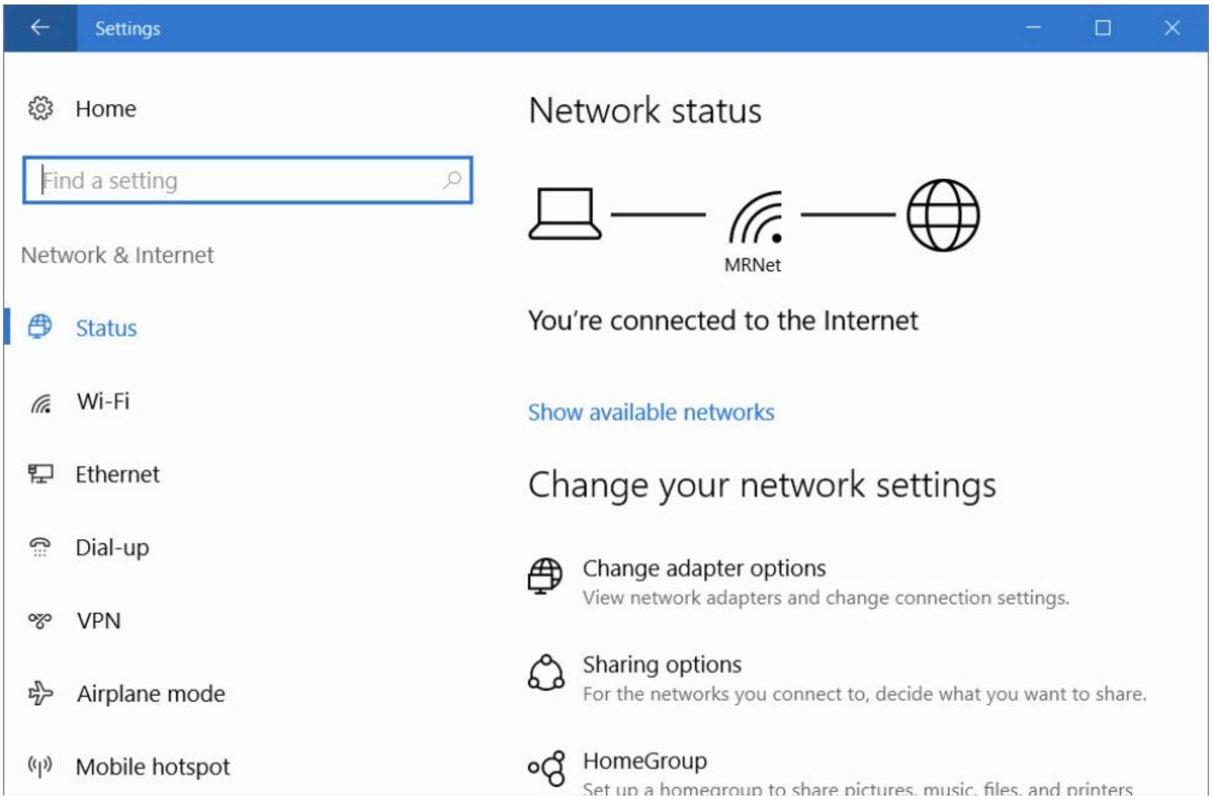
Although there’s no obvious way to copy information from the Network Connections Details dialog box (to share with a support engineer, for example, or to paste into a post on a community support forum), it is possible to do so.

Use your mouse to select a single row, or hold down Ctrl or Shift and click to select multiple rows, and then press Ctrl+C to copy the selection to the Clipboard.

Network And Sharing Center in Control Panel?! What about Settings?

Windows 10 marks the debut appearance of Settings, Network & Internet, Status—another step in the move away from the old Control Panel settings.

You might find this page, shown here, to be more convenient than using Network And Sharing Center:



Network status

You're connected to the Internet

Show available networks

Change your network settings

Change adapter options
View network adapters and change connection settings.

Sharing options
For the networks you connect to, decide what you want to share.

HomeGroup
Set up a homegroup to share pictures, music, files, and printers

The Network Status page offers much of the same information and links to additional tools such as Network And Sharing Center—indeed, the links go to the same old Control Panel destinations.

It even has a link (not shown in the figure) directly to Network And Sharing Center, which is kind of handy because the latter shows more information about your network, which is why we still prefer it.

The Network Status page does have one neat trick you won't find in Network And Sharing Center: a link (also not visible in the figure) to "Network Reset".

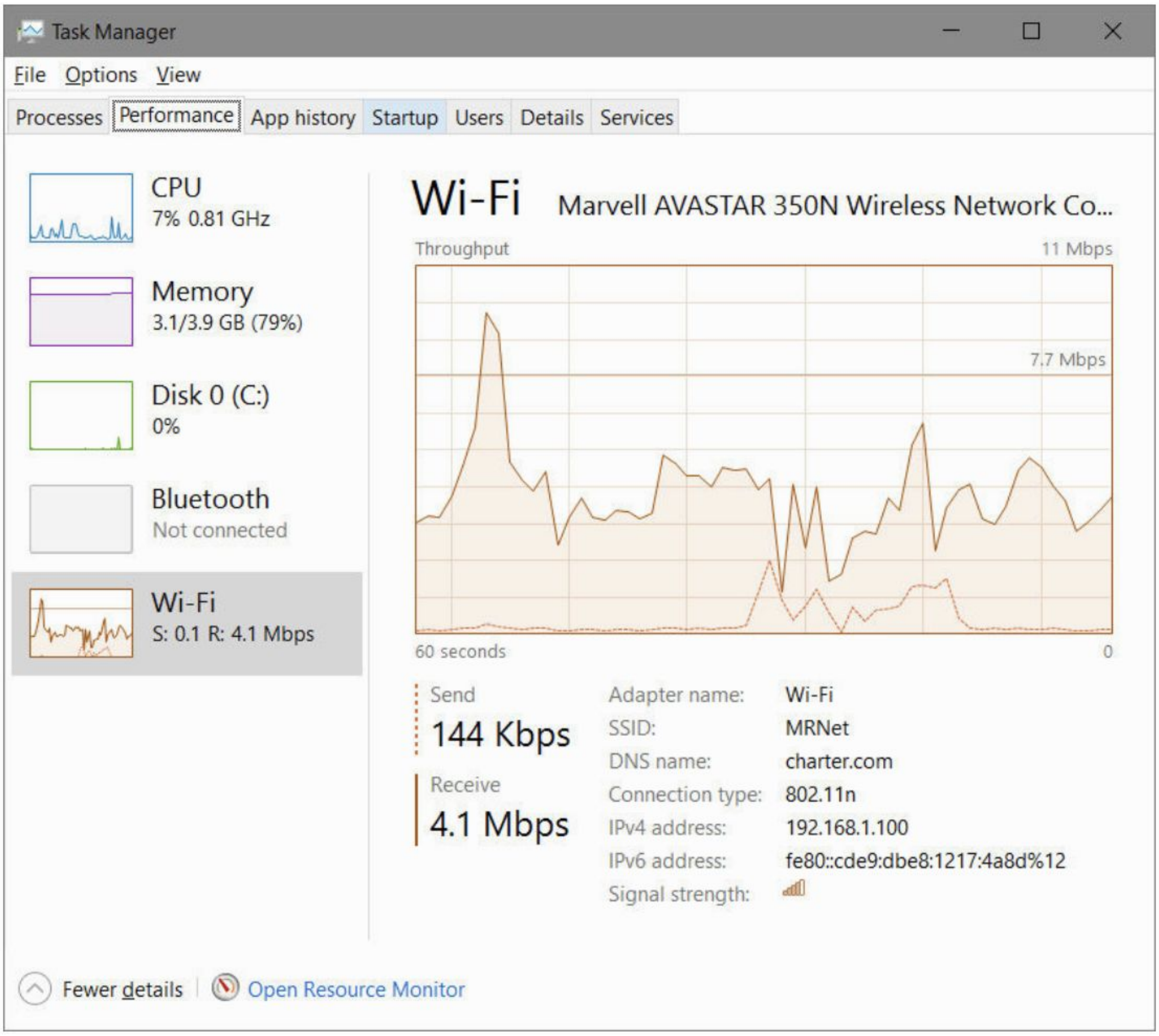
If you're unable to resolve networking problems using the network troubleshooter, click "Network Reset" to remove your network adapters, reinstall them, set other networking components to their default settings, and restart your computer.

Monitoring network performance in Task Manager

Sometimes it's useful to know not just whether a network connection is working but how well it's handling its primary job of transmitting and receiving packets of data.

For a real-time graph of network throughput, open Task Manager, click the Performance tab, and then select a connection name from the list on the left.

Next image shows a file download in progress on a Wi-Fi connection:



CPU
7% 0.81 GHz

Memory
3.1/3.9 GB (79%)

Disk 0 (C:)
0%

Bluetooth
Not connected

Wi-Fi
S: 0.1 R: 4.1 Mbps

Wi-Fi Marvell AVASTAR 350N Wireless Network Co...

Send
144 Kbps

Receive
4.1 Mbps

Adapter name:	Wi-Fi
SSID:	MRNet
DNS name:	charter.com
Connection type:	802.11n
IPv4 address:	192.168.1.100
IPv6 address:	fe80::cde9:dbe8:1217:4a8d%12
Signal strength:	

IPv6 and Windows 10

The longer you've worked with Windows, the more likely you are to be familiar with the granddaddy of Windows networking, Internet Protocol version 4, also known as IPv4.

A default network connection in Windows 10, wired or wireless, uses IPv4 but also enables the newer IP version 6.

IPv6 is on by default and has been the preferred protocol in all desktop and server versions of Windows for nearly a decade, since the release of Windows Vista.

Without getting into the minutiae of network addressing, suffice it to say that IPv4, with its addresses based on four groups of numbers from 0 to 255, has a big problem.

When the internet was young, that address space, consisting of 4.3 billion unique combinations of dotted addresses, like 192.168.1.108 or 10.0.0.242, seemed huge.

Unfortunately, nobody anticipated just how big the internet would become, and the authorities who assign IP addresses on the internet have literally run out of IPv4 addresses.

The solution is IPv6, which uses 128-bit addresses and therefore has a maximum address space of 3.4 x 10 ^ 38 addresses, which we are confident is enough to last for the next few generations of internet users.

IPv6 is slowly but surely taking over large swaths of the internet.

The giant American internet and cable provider Comcast has fully enabled its network for IPv6, with most of its competition not far behind.

Major mobile carriers are also providing the majority of traffic on native IPv6 connections.

Major content providers are enabled for IPv6 as well.

Almost all of Google's services now work over IPv4 and IPv6, as does Yahoo.

Facebook's giant data centers now run IPv6 exclusively, and Netflix has supported IPv6 for years.

Windows veterans might be tempted to shy away from IPv6, preferring the more familiar IPv4.

Probably that's a mistake. IPv6 is here to stay. Learn about it and embrace it.

Setting network locations

A desktop PC connected to a wired home or small office network typically remains in a single location.

In contrast, mobile devices running Windows 10 can connect to different types of networks—a corporate domain, a wireless hotspot at a coffee shop, or a private home network.

Each type of network has its own security requirements.

Windows uses network locations to categorize each network and then applies appropriate security settings.

When you connect to a new network, Windows applies one of three security settings:

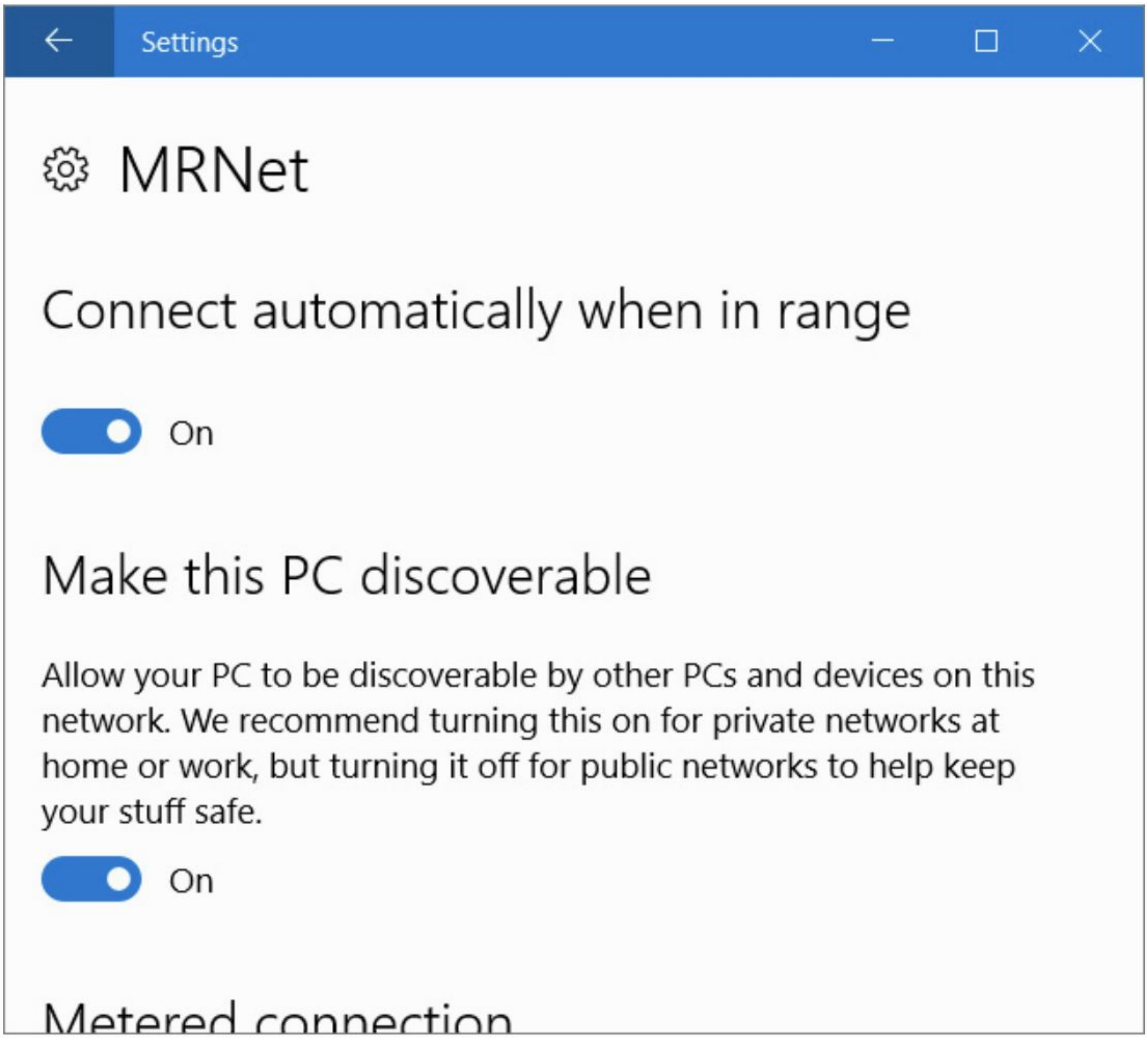
- Public. This is the default setting for any new, untrusted network connection. Network discovery is turned off for public networks, making it impossible for other people on the same access point to connect to your computer. This option is appropriate for networks in public places, such as wireless hotspots in coffee shops, hotels, airports, and libraries. It's also the correct choice if your desktop or laptop PC is directly connected to a cable modem or other broadband connection without the protection of a router and hardware firewall.

- Private. This option is appropriate when you're connecting to a trusted network, such as your own network at home—if and only if that network is protected by a router or residential gateway (a consumer device that combines a cable modem, router, and wireless access point in a single box) or comparable internet defense. When you make this choice, Windows enables network discovery and allows you to enable the HomeGroup feature for sharing with other users on the network.
- Domain. This option is applied automatically when you sign in to Windows using a computer that's joined to a Windows domain, such as your company network. In this scenario, network discovery is enabled, allowing you to see other computers and servers on the network by using accounts and permissions controlled by a network administrator.

The location of the current network is shown in Network And Sharing Center, below the name of the network.

To change a public network to a private one, or vice versa, open Settings > Network & Internet, and then tap or click the Wi-Fi or Ethernet heading in the list on the left.

Click or tap the icon for the connection to open the properties dialog box for the active connection, shown in the following image:



MRNet

Connect automatically when in range

On

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.

On

Metered connection

When "Make This PC Discoverable" is Off, the network is public.

Slide the switch to "On" to make the network private.

Workgroups vs. domains

Computers on a network can be part of a workgroup or a domain.

In a workgroup, the security database for each computer (including, most significantly, the list of user accounts and the privileges granted to each one) resides on that computer.

When you sign in to a computer in a workgroup, Windows checks its local security database to see whether you provided a user name and password that matches one in the database.

Similarly, when network users attempt to connect to your computer, Windows again consults the local security database.

All computers in a workgroup must be on the same subnet.

A workgroup is sometimes called a peer-to-peer network.

By contrast, a domain consists of computers that share a security infrastructure, Active Directory, which in turn is managed on one or more domain controllers running Windows Server.

Microsoft's cloud-based alternative, Azure Active Directory, provides similar infrastructure without requiring IT departments to manage local servers.

Active Directory and Azure Active Directory can be combined to create effective hybrid environments.

When you sign in using a domain account, Windows authenticates your credentials against the security database defined by your network administrator.

In this "Windows 10" chapter, we focus primarily on workgroup networks.

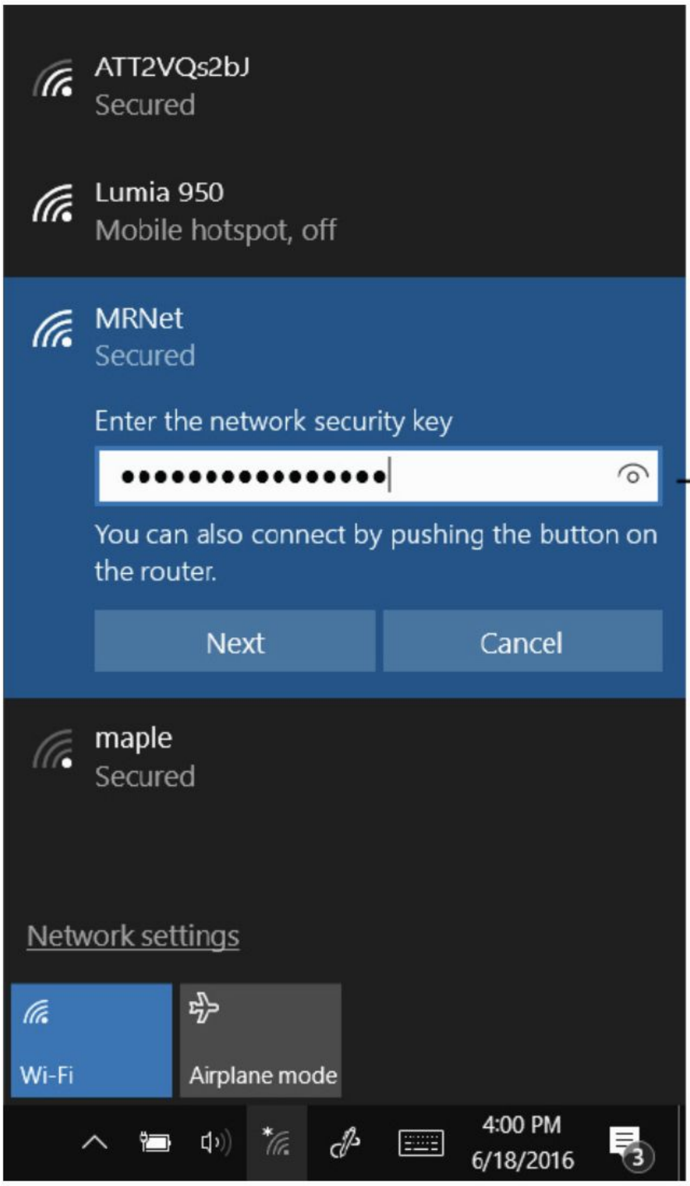
Connecting to a wireless network

Whenever your computer's wireless network adapter is installed and turned on, Windows scans for available wireless access points.

If it finds at least one (and you're not already connected to a wireless network), it alerts you via the wireless network icon, which looks a bit like an antenna.

If you see a bright dot at the end of an otherwise gray antenna, connections are available.

Clicking or tapping the entry for a secured access point reveals a box in which you're expected to enter a passphrase, as in the following figure:



Enter the network security key

••••••••••••••••

You can also connect by pushing the button on the router.

A router that supports Wi-Fi Protected Setup (WPS) offers a way to connect without entering a security key

If what you enter matches what's stored in the access point's configuration, you're in.

Getting in is easy on a network you control, where you set the network security key.

For a secured access point controlled by someone else—a doctor's waiting room, a coffee shop, a friend's office—you need to ask the network owner for the passphrase or key.

Before you reach that security prompt, you're asked whether you want to connect automatically to that network in the future.

If this is a place you expect to visit again (or in the case of a coffee shop, again and again and again . . .), say yes to save the credentials.

Note that saved Wi-Fi network security keys are synced between devices when you sign in with a Microsoft account, so you might find that a brand-new device, one you’ve never used before, automatically connects to your home or office Wi-Fi without having to ask you.

To disconnect from a Wi-Fi access point, click or tap its entry in the network flyout and then tap "Disconnect".

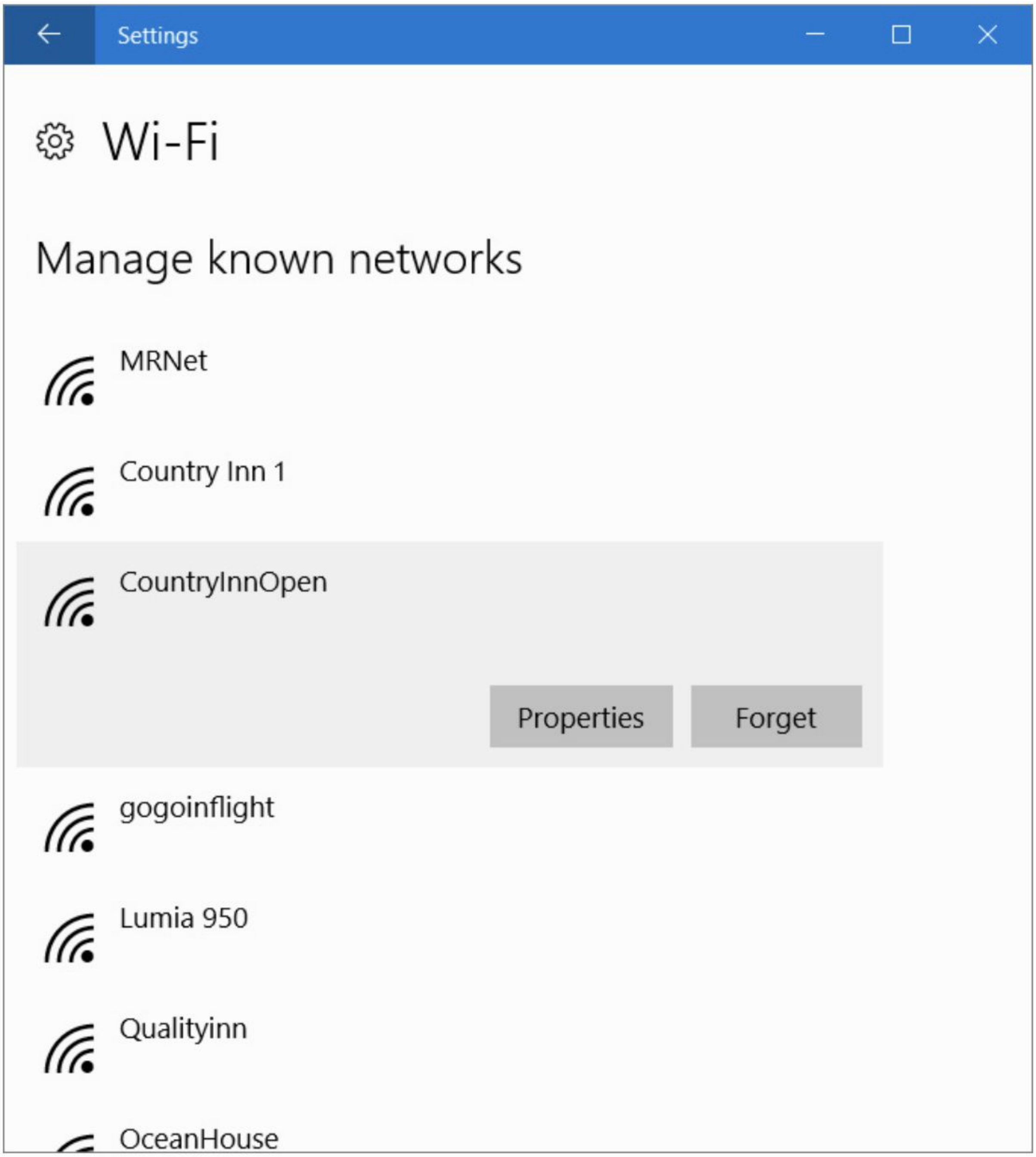
Doing so automatically turns off the option to connect automatically to that network in the future.

Windows 10 saves credentials for every Wi-Fi access point you connect to, giving you the option to connect with a tap when you revisit.

If that thought makes you uncomfortable, you can see and manage the full list of networks by opening Settings > Network & Internet > Wi-Fi and clicking "Manage Known Networks".

That list can be startling, especially if you’re a frequent traveler.

Tap any name in the list, and you’ll see two buttons, as in the next figure:



Tapping "Properties" shows information about the network, as shown earlier in the previous figures.

Tapping the "Forget" button deletes any saved security information and removes the network name from the list.

Decoding Wi-Fi standards

The most popular wireless networks use one of several variants of the IEEE (Institute of Electrical and Electronics Engineers) 802.11 standard, also known as Wi-Fi.

On modern Wi-Fi networks, you're likely to encounter one of the following three standards (going from oldest to newest):

- 802.11g. This standard was current up until 2009, just before the release of Windows 7. It's still in wide use on older PCs and wireless access points. It can transfer data at a maximum rate of 54 megabits per second using radio frequencies in the 2.4-GHz range. 802.11g-based networks largely supplanted those based on an earlier standard, 802.11b, which offers a maximum speed of 11 megabits per second.
- 802.11n. Using this standard, adopted in 2009, you can expect to see dramatic improvements in speed (600 megabits per second) as well as significantly greater range. Unlike the earlier standards, the 802.11n standard allows use of the 5-Ghz frequency range as well as 2.4 GHz. However, not all 802.11n hardware supports both bands.
- 802.11ac. This standard, finalized in 2014, builds on the 802.11n specification and allows multiple links at both ends of the wireless connection, advertising throughput rates of 500 megabits per second per link, with a theoretical maximum speed of up to 2,600 megabits per second.

Although the newer Wi-Fi standards are backward compatible with hardware that uses the older, slower standards, be aware that all traffic on your network runs at the speed of the slowest wireless standard in use; if you just bought an 802.11ac router, you'll see the faster speed only if you replace your old network adapters.

Wireless security

On a conventional wired network, especially in a private home or office, physical security is reasonably easy to maintain: if someone plugs a computer into a network jack or a switch, you can trace the physical wire back to the intruder's computer.

On wireless networks, however, anyone who comes into range of your wireless access point can tap into your network and intercept signals from it.

If you run a small business, you might want to allow internet access to your customers by using an open internet connection.

Some internet service providers create secure guest accounts on their customers' cable modems that allow other customers of that service to connect using their network credentials.

Other than those scenarios, however, you probably want to secure your network so that the only people who can connect to it are those you specifically authorize.

Doing that means configuring security settings on your wireless access point or router.

When you connect to a network, known or unknown, the level of security is determined by the encryption standard chosen by the network owner and supported by network hardware on both sides of the connection.

Depending on the age of your hardware, you should have a choice of one or more of the following options, listed in order of preference:

- Wi-Fi Protected Access 2 (WPA2). Based on the 802.11i standard, WPA2 provides the strongest protection for consumer-grade wireless networks. It uses 802.1x-based authentication and Advanced Encryption Standard (AES) encryption; combined, these technologies ensure that only authorized users can access the network and that any intercepted data cannot be deciphered. WPA2 comes in two flavors: WPA2-Personal and WPA2-Enterprise. WPA2-Personal uses a passphrase to create its encryption keys and is currently the best available security for wireless networks in homes and small offices. WPA2-Enterprise requires a server to verify network users. All wireless products sold since early 2006 must support WPA2 to bear the Wi-Fi CERTIFIED label.
- Wi-Fi Protected Access (WPA). WPA is an earlier version of the encryption scheme that has since been replaced by WPA2. It was specifically designed to overcome weaknesses of WEP. On a small network that uses WPA, clients and access points use a shared network password (called a preshared key, or PSK) that consists of a 256-bit number or a passphrase that is from 8 to 63 bytes long. A longer passphrase produces a stronger key. With a sufficiently strong key based on a truly random sequence, the likelihood of a successful outside attack is slim. Most modern network hardware supports WPA only for backward compatibility.
- Wired Equivalent Privacy (WEP). WEP is a first-generation scheme that dates back before the turn of the century. It suffers from serious security flaws that make it inappropriate for use on any network that contains sensitive data. Most modern Wi-Fi equipment supports WEP for backward compatibility with older hardware, but we strongly advise against using it unless no other options are available.

You must use the same encryption option on all wireless devices on your network—access points, routers, network adapters, print servers, cameras, and so on—so choose the best option that's supported by all your devices.

If you have an older device that supports only WEP (and it can't be upgraded with a firmware update), consider retiring or replacing that device.

Security at the access point

If your data is sensitive and your network is in an apartment building or an office complex where you can reasonably expect other people to wander into range with wireless adapters, you should take extra security precautions in addition to enabling WPA.

Consider any or all of the following measures to protect your wireless access point from intruders:

- Change the network name (SSID) and the password of your access point to one that doesn't match the hardware defaults and doesn't give away any information about you or your business.
- Hide the network name (SSID) of your access point so other people cannot see your SSID in the Wi-Fi lists.
- Create a list of devices that filter by MAC address, so the only devices that can connect to your Wi-Fi network are those in the list.
- Disable remote administration of the access point; if you need to change settings, you can do so directly, using a wired connection.
- Whether you decide to allow remote administration of the access point or not, set a strong password so that a visitor can't tamper with your network settings.
- Check the firmware and drivers for wireless hardware (access points and adapters) at regular intervals and install the most recent versions, which might incorporate security fixes.
- Consider using a virtual private network (VPN) for wireless connections. A VPN sends all wireless traffic over an encrypted connection, making it impossible for others to snoop on your wireless traffic. Corporate network administrators can help set up a VPN using your company's security infrastructure. For unmanaged Windows 10 devices, VPN software and services are available.

When setting up a wireless access point for a home or small office, choose a strong passphrase.

A passphrase for WPA or WPA2 can be up to 63 characters long and can contain letters (case-sensitive), numbers, and spaces (no spaces at the beginning or end, however).

Many devices generate a random alphanumeric key, but you might prefer to use a memorable phrase instead of random characters.

If you do, choose a phrase that's not easily guessed and make it long.

Also consider incorporating letter substitution or misspellings to thwart attackers.

Because the phrase can be saved and synced between devices, you shouldn't need to enter it often.

- Vocabulary -

- to snoop: curiosear / husmear.
- to thwart: impedir / evitar.
- to run out: agotarse / quedarse sin (existencias).
- trusted: de confianza.
- untrusted: no confiable.
- subnet: subred.

- Exercises - 1. 1. 4. Networking essentials -

Open the following Google Document that you have created in a previous sub-unit:

"1. 1. Getting started with Windows 10 - Apellidos, Nombre"

being "Apellidos, Nombre" your Last Name and Name.

Inside this Google Document you are going to copy and answer all the "Exercises" of this sub-unit:

1. Go to Settings -> Network & Internet -> Ethernet -> Change adapter options -> Ethernet Status -> Properties -> Internet Protocol Version 4, and check your computer’s TCP/IP settings.
2. Go to Settings -> Network & Internet -> Status -> Network reset. Do not “Reset now” your network. What happens if you do so?
3. Go to Task Manager -> More details -> Performance -> Ethernet.