How to use the Netstat command in Windows 11 to monitor network activity

Netstat is a command-line utility that helps you monitor all the technical characteristics of your active network connections.

Netstat is a command-line utility that helps you monitor all the technical characteristics of your active network connections. It provides a quick way to see all open ports, active connections, and network services running on your system.

If this all sounds too technical for you, don't worry. The article will explain everything in a simple way to do this. First, let's look at what netstat is and how to use netstat on Windows to monitor your network.

What is the Netstat command on Windows?

The netstat command is mainly used by IT professionals or network troubleshooters on Windows and Linux systems. The command, when executed, will display a list of active TCP connections, listening ports, Ethernet statistics, addresses and ports in use by your system, etc.

Simply put, this command allows you to see which network connections are active and which applications are using them in the background at any given time.

To help you understand better, here are some examples of what netstat can show you:

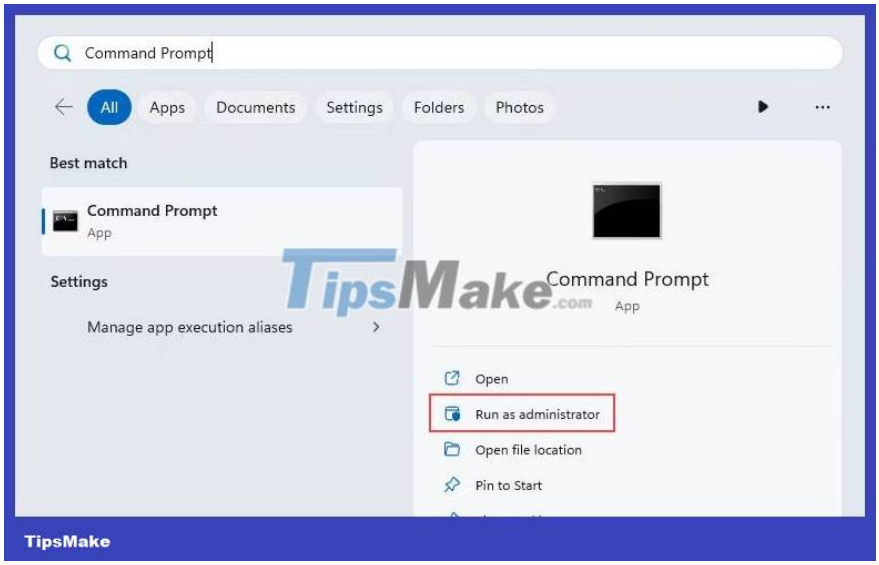
1. All incoming and outgoing connections are on your PC.
2. Information about which ports are open or listening for connections.
3. Connection and process of using the Internet.
4. Any suspicious connections from unknown applications or services.

How to use Netstat command on Windows

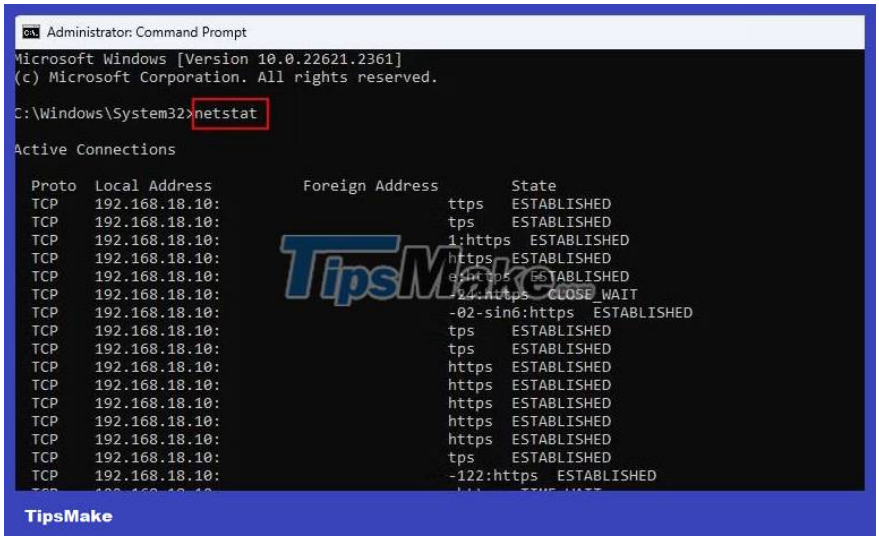
As mentioned earlier, the netstat command is only accessible from Command Prompt. If you don't know the steps, follow the steps below to run netstat from Command Prompt:

1. Click the **Search** button on your taskbar and search for the Command Prompt application.

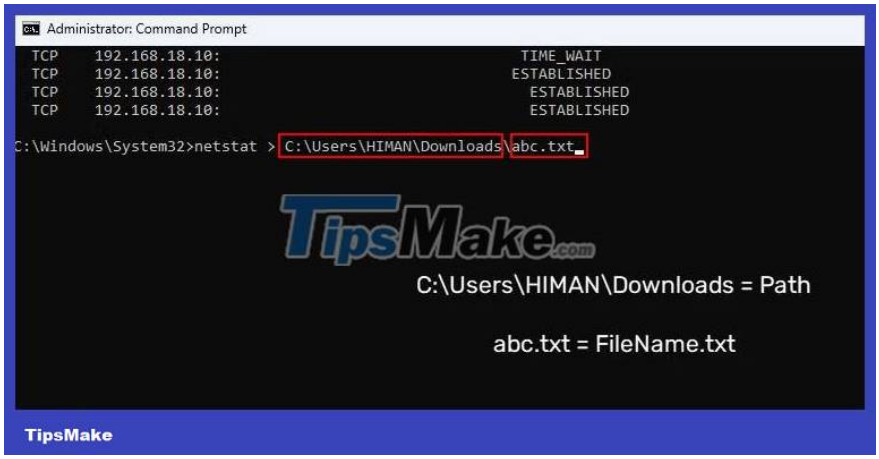
2. Next to the appropriate search result, click **Run as administrator** . This will launch Command Prompt with admin rights.



3. On Command Prompt, type **netstat** and press **Enter.** The command, once executed, will give a list of active connections along with their status.



4. For example, if you need to share the output with the technical support team, use this command to copy the results in a text file: " **netstat > PathFileName.txt"** . In this command, **Path** is the location of any folder where you want to save the file and **FileName.txt** is the name of your exported file.



The highlight of netstat is that you can further use it with some parameters (or syntax) to filter the generated output. The article will introduce you to some useful parameters that you can use with the **"netstat -parameter"** format in the next section.

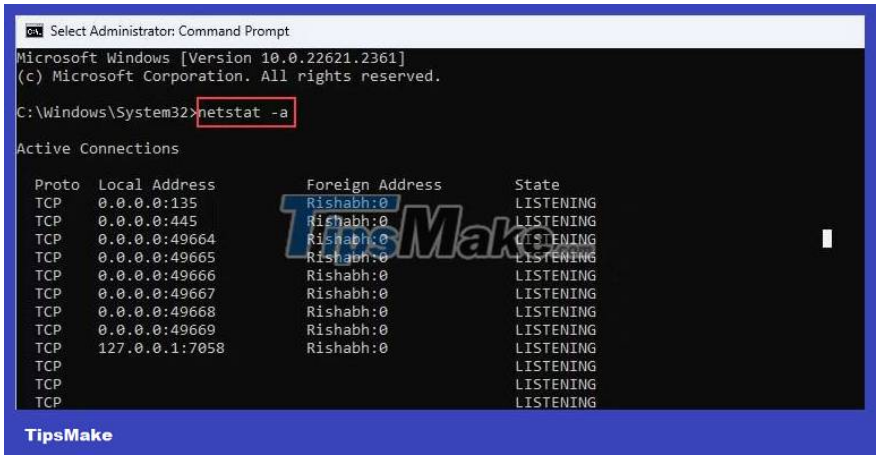
If you want to learn more about other such commands, see this list of useful commands for managing Windows networks.

Netstat parameters are useful for Windows users

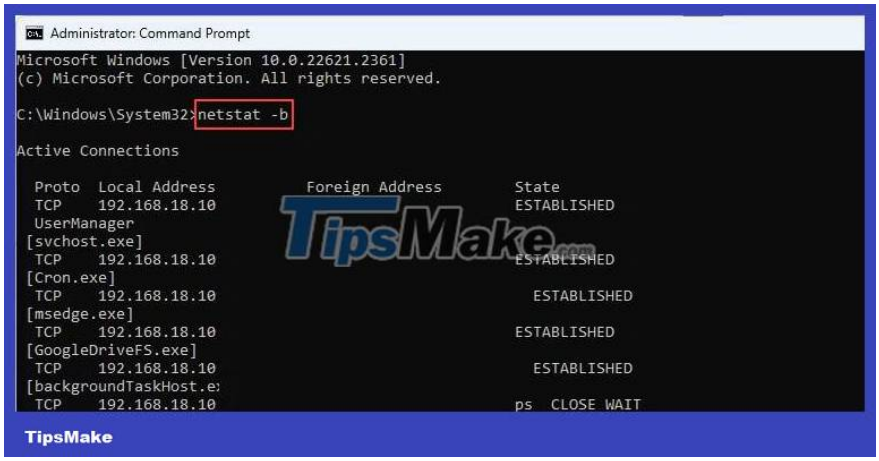
In layman's terms, parameters mean some symbols or letters that allow you to modify what the netstat command displays. When you use the parameter in the format **"netstat -parameter"** , it helps you see detailed information about traffic and different connections on the local network.

Let's look at some useful netstat parameters to get specific and filtered information from netstat:

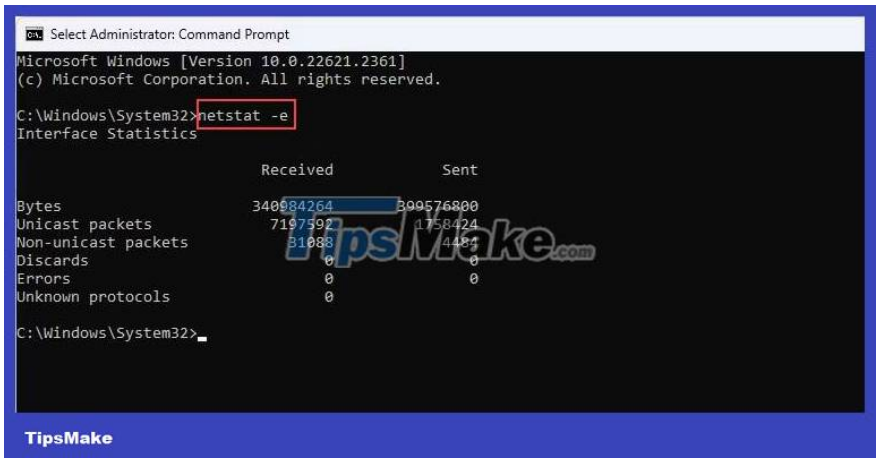
1. **netstat -a** : Command to display all running TCP and UDP connections and listening ports. If there are any failed connection attempts, they will also be displayed here. In addition to the -a parameter, check out other alternatives to .



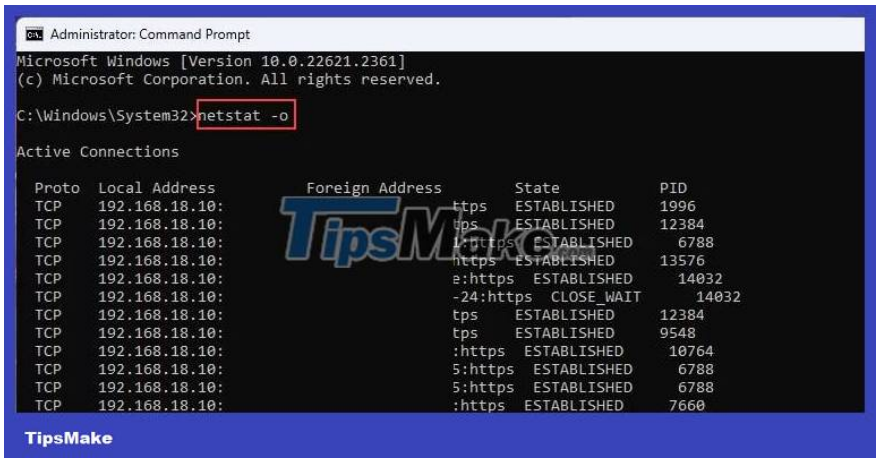
1. **netstat -b** : The -b parameter displays the executable (.EXE) file involved in creating each connection or listening port. It is mainly useful for people troubleshooting network problems in a Windows server or part of a domain's computers.



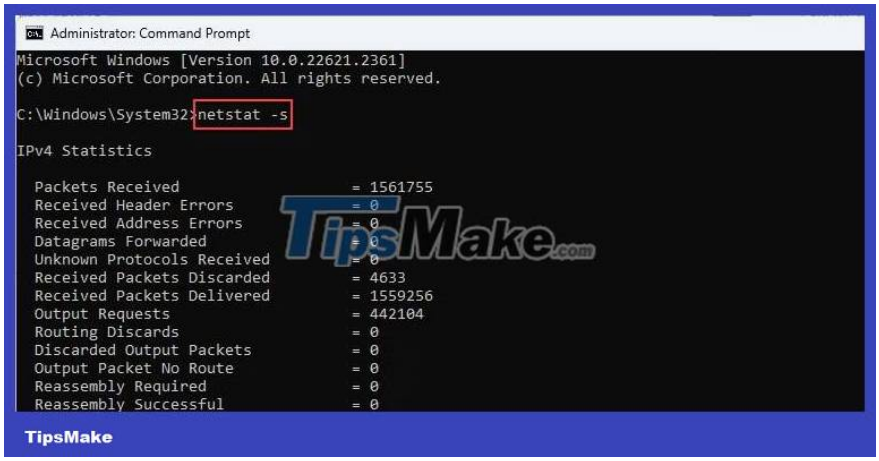
1. **netstat -e** : If you use an Ethernet connection instead, the -e parameter can show you detailed Ethernet statistics, like link speed, total bytes sent/received, and some statistics other techniques.



1. **netstat -o** : Suppose you installed an app (from an untrusted website), in which case you can check if the app is doing anything suspicious with the connection . This is because the -o parameter displays the process ID (PID) of every connection that you can match from .



1. **netstat -s** : This shows per-protocol statistics like packets sent/received, errors, dropped packets, etc. This is useful if you want to understand bandwidth usage based on each protocol.



Now that you have an idea of ??some useful commands, try running them in Command Prompt. Note that you should only run Command Prompt with admin rights because some connections are only visible with admin privileges.

Note : If you don't like entering commands multiple times, combine parameters. For example, netstat -e -s will show you Ethernet network details along with bandwidth usage based on each protocol in one view.

You finished reading the article "**How to use the Netstat command in Windows 11 to monitor network activity**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
