<https://www.youtube.com/watch?v=qsZ8Qcm6_8k&list=PLhTjy8cBISErYuLZUvVOYsR1giva2payF&index=4>

Pycharm Installation community version

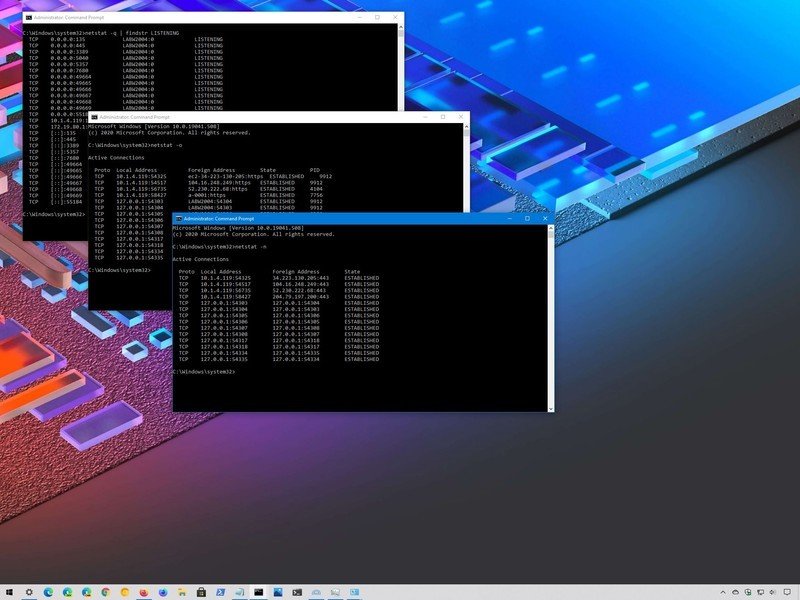
Static IP Address--- Servers and WebSite

Ip Address—City and Street No

PORTs---Exact House or apartment no

How Exact Port No in your computer

**How to use netstat command on Windows 10**

*[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2020/10/windows-10-netstat-commands_.jpg)*Source: Windows Central

On [Windows 10](https://www.windowscentral.com/windows-10), netstat (network statistics) has been around for a long time, and it's a command-line tool that you can use in Command Prompt to display statistics for all network connections. It allows you to understand open and connected ports to monitor and troubleshoot networking problems for system or applications.

When using this tool, you can list active networks (incoming and outgoing) connections and listening ports. You can view network adapter statistics as well as statistics for protocols (such as IPv4 and IPv6). You can even display the current routing table, and much more.

In this [Windows 10 guide](https://www.windowscentral.com/windows-10-help), we'll walk you through the steps to use the netstat command to examine connections to discover open and connected network ports.

[**VPN Deals: Lifetime license for $16, monthly plans at $1 & more**](https://www.androidcentral.com/best-vpn-deals)

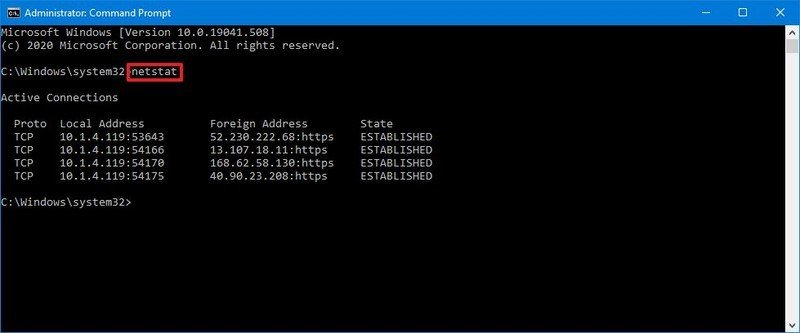
* [How to use netstat on Windows 10](https://www.windowscentral.com/how-use-netstat-command-windows-10#netstat_command_windows10)
* [How to use netstat parameters on Windows 10](https://www.windowscentral.com/how-use-netstat-command-windows-10#netstat_parameters_windows10)
* [How to search netstat details on Windows 10](https://www.windowscentral.com/how-use-netstat-command-windows-10#netstat_search_windows10)

**How to use netstat on Windows 10**

To get started with netstat, use these steps:

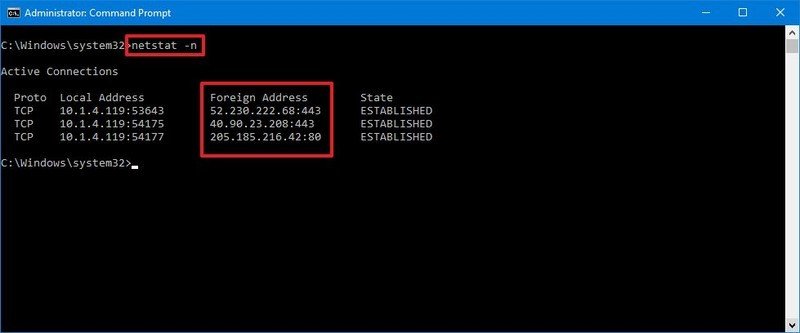
1. Open **Start**.
2. Search for **Command Prompt**, right-click the top result, and select the **Run as administrator** option.
3. Type the following command to show all active TCP connections and press **Enter**:

netstat

*[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2020/10/netstat-cmd-windows-10.jpg)*Source: Windows Central

1. (Optional) Type the following command to display active connections showing numeric IP address and port number instead of trying to determine the names and press **Enter**:

netstat -n

*[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2020/10/netstat-n-command.jpg)*Source: Windows Central

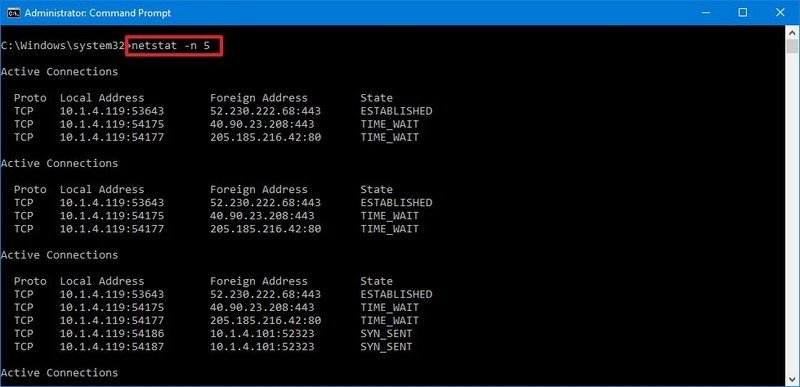
1. (Optional) Type the following command to refresh the information at a specific interval and press **Enter**:

netstat -n INTERVAL

In the command, make sure to replace **INTERVAL** for the number (in seconds) you want to redisplay the information.

This example refreshes the command in question every five seconds:

netstat -n 5

*[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2020/10/netstat-interval-command.jpg)*Source: Windows Central

**Quick note:** When using the interval parameter, you can terminate the command using the **Ctrl + C** keyboard shortcut in the console.

Once you execute the command, it'll return a list of all active connections in four columns, including:

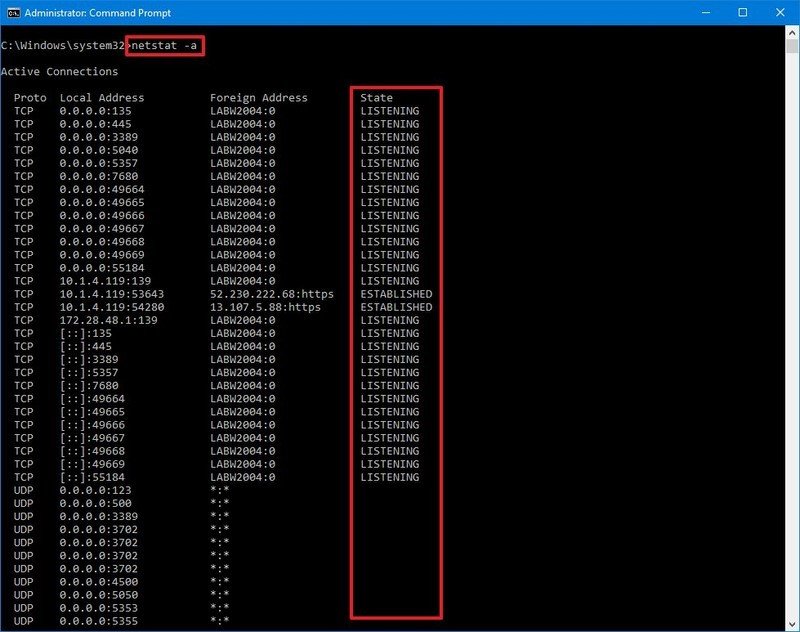
* **Proto:** Shows the connection protocol (TCP or UDP).
* **Local Address:** Shows the computer's IP address followed by a semicolon with a port number of the connection. The double-semicolon inside brackets indicates the local IPv6 address, and "0.0.0.0" refers to the local address too.
* **Foreign Address:** Lists the remote device's IP (or FQDN) address with the port number after semicolon port name (for example, https, http, microsoft-ds, wsd).
* **State:** Indicates where the connection is active (established), the local port has been closed (time\_wait), and the program hasn't closed the port (close\_wait). Other status include, closed, fin\_wait\_1, fin\_wait\_2, last\_ack, listen, syn\_received, syn\_send, and timed\_wait.

**How to use netstat parameters on Windows 10**

The tool also includes several parameters that you can use in Command Prompt to display different information about the network connections.

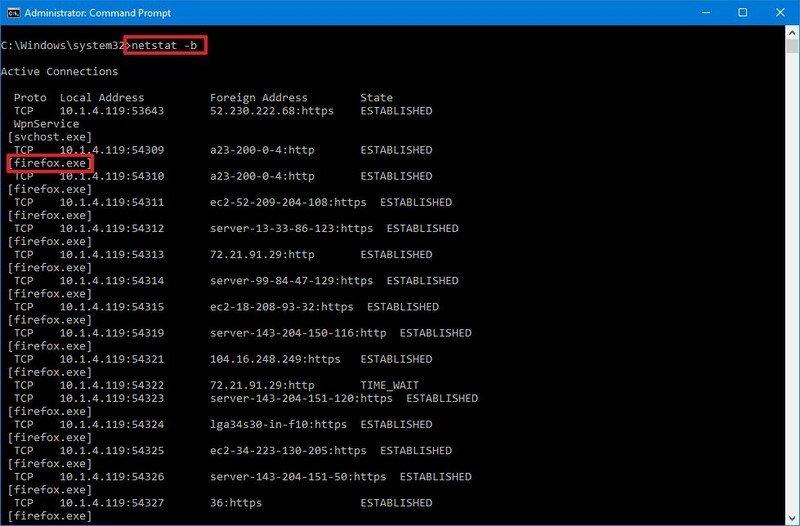
**Show active and inactive connections**

The netstat -a command displays all active and inactive connections, and the TCP and UDP ports the device is currently listening.

*[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2020/10/netstat-a-command.jpg)*Source: Windows Central

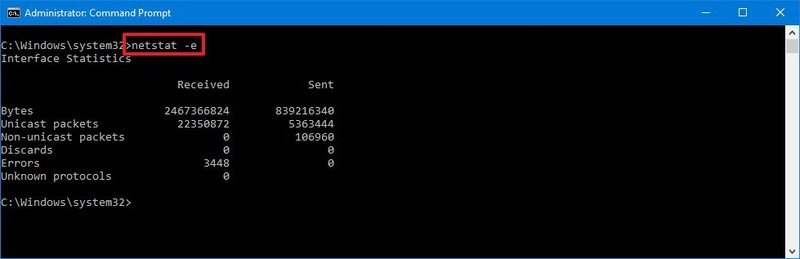
**Show executable information**

The netstat -b command lists all the executables (applications) associated with each connection. Sometimes, applications may open multiple connections.

*[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2020/10/netstat-b-app-associated-connection.jpg)*Source: Windows Central

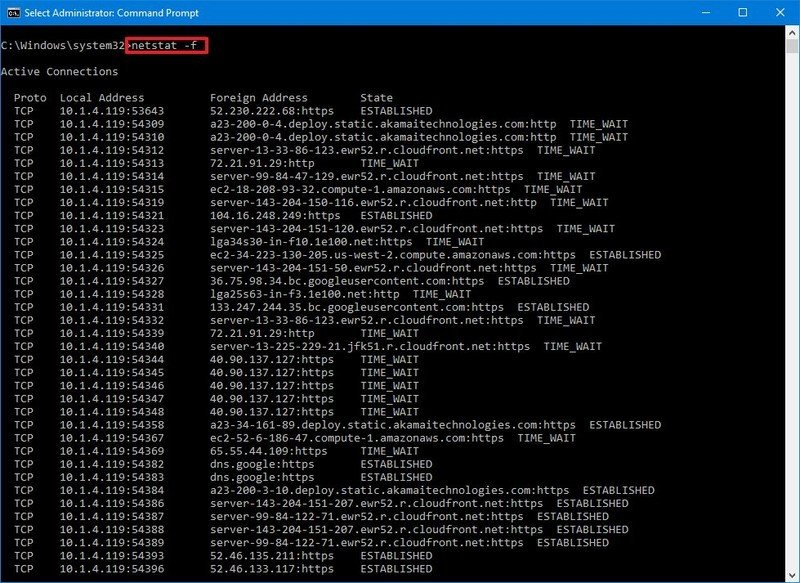
**Show network adapter statistics**

The netstat -e command generates a statistic of the network interface, which shows information like the number of bytes, unicast and non-unicast sent and received packets. You can also see discarded packets and errors and unknown protocols, which can you troubleshoot networking problems.

*[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2020/10/netstat-e-network-statistics.jpg)*Source: Windows Central

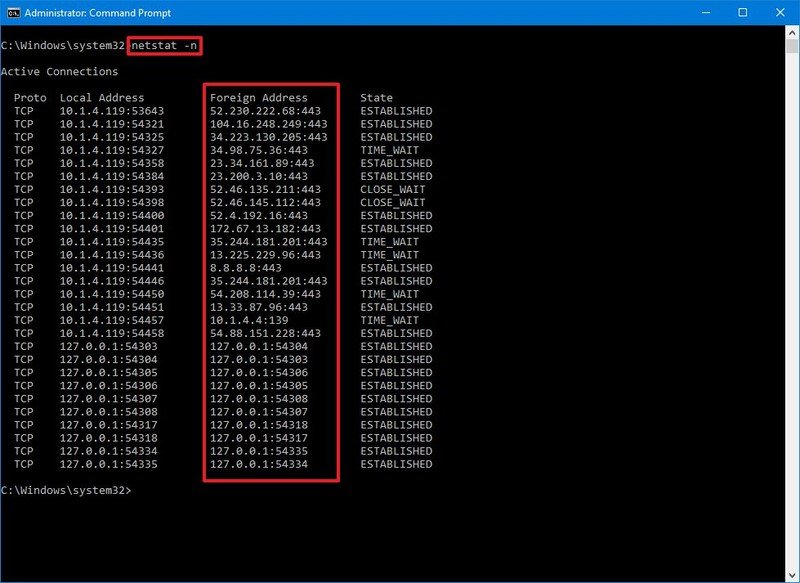
**Show FQDNS for foreign addresses**

The netstat -f command shows the fully qualified domain name (FQDN) for foreign addresses. For example, "server-54-230-157-50.otp50.r.cloudfront.net:http" instead of "server-54-230-157-50:http" or "54.230.157.50".

*[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2020/10/netstat-f-fqdn.jpg)*Source: Windows Central

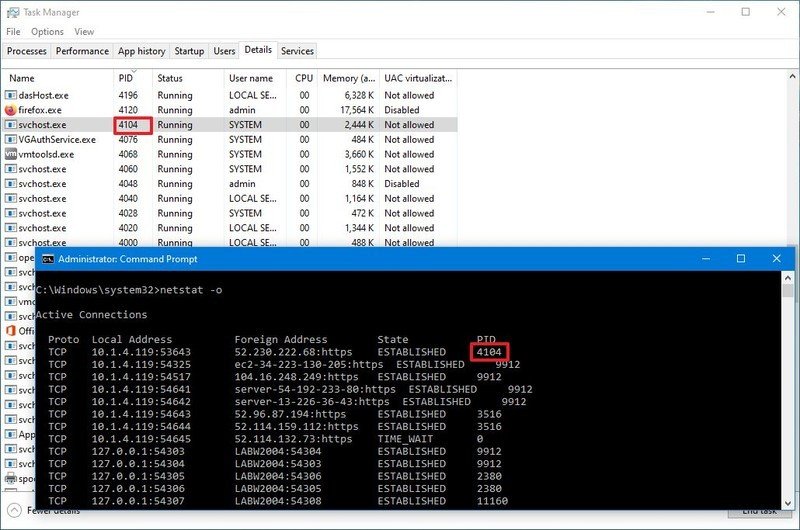
**Show numerical form**

The netstat -n command displays the addresses and ports in numerical form. For example, 54.230.157.50:443.

*[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2020/10/netstat-n-port-address-numeric.jpg)*Source: Windows Central

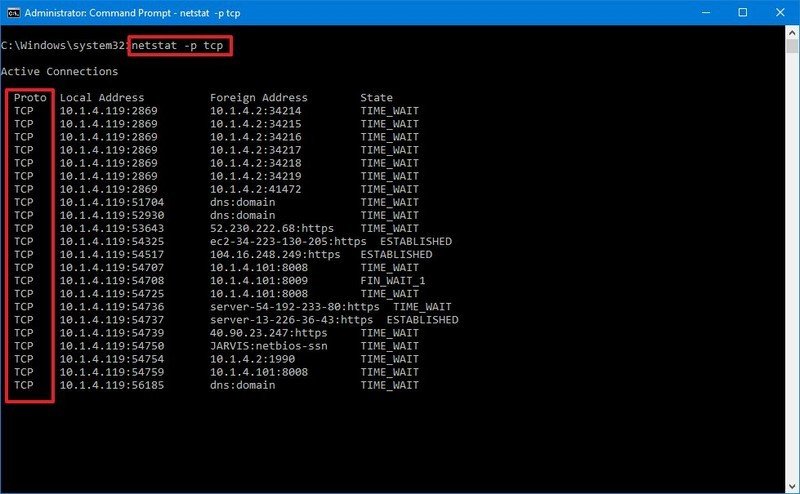
**Show process ID**

The netstat -o command shows all active TCP connections like netstat, but with the difference that adds a fifth column to display the Process ID (PID) for each connection. The processes available in this view are the same in the "Details" tab of Task Manager, which also reveals the application using the connection.

*[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2020/10/task-manager-netsttato-pid.jpg)*Source: Windows Central

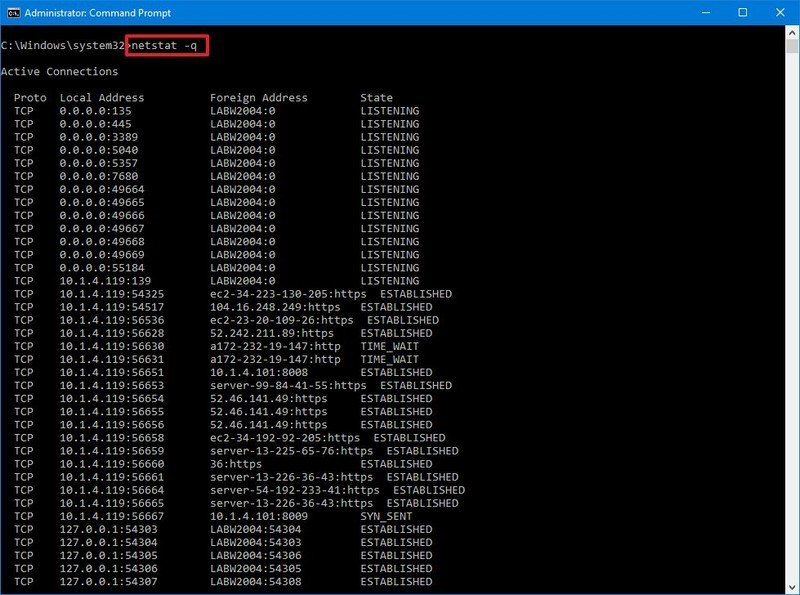
**Show connections by Protocol**

The netstat -p can be used to display connections per-protocol that you have to specify using tcp, udp, tcpv6, or udpv6 next to the command. For example, you can use the netstat -p tcp to view a list of TCP connections.

*[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2020/10/netstat-p-tcp.jpg)*Source: Windows Central

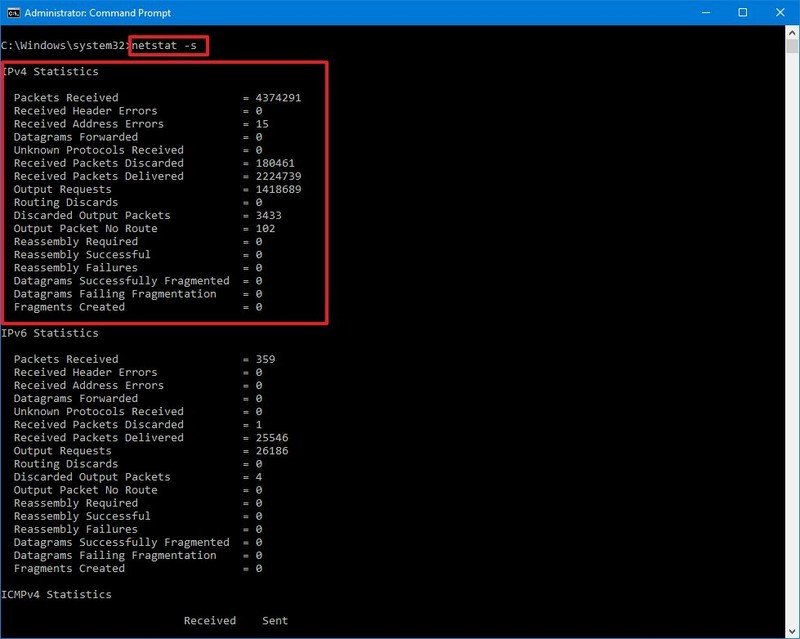
**Show listening and non-listening ports**

The netstat -q commands can produce a list of all the connections with the listening and bound non-listening ports.

*[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2020/10/netstat-q-listening-nonlistenting.jpg)*Source: Windows Central

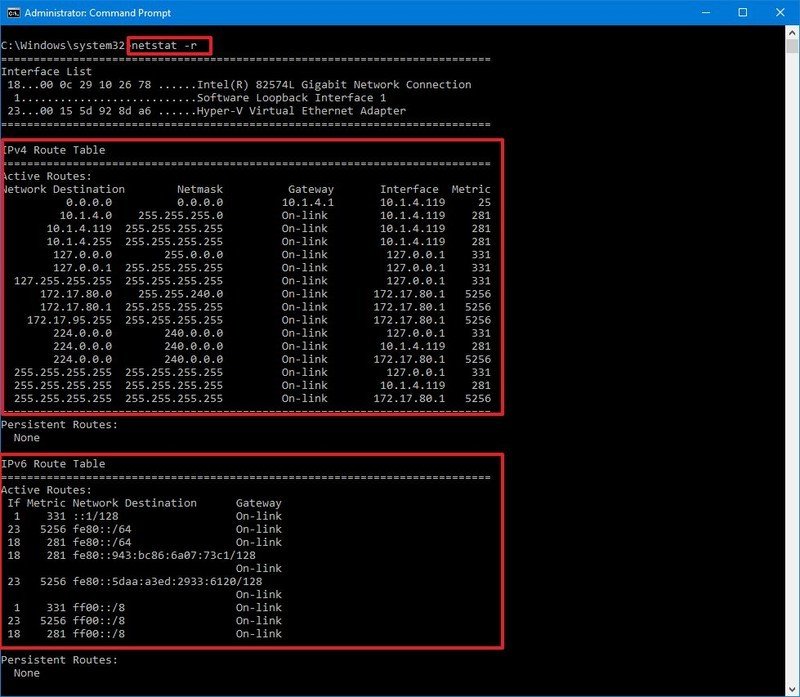
**Show statistics by Protocol**

The netstat -s shows network statistics for all available protocols, including TCP, UDP, ICMP, and IP protocols (version 4 and 6).

*[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2020/10/netstat-s-network-statistics.jpg)*Source: Windows Central

**Show routing table**

The netstat -r command displays the current network routing table that lists all the routes to destinations and matrics known by the device, for IP version 4 and version 6 (if applicable). If the returned information looks familiar, it's because you can also output the data using the route print command.

*[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2020/10/netstat-routing-table.jpg)*Source: Windows Central

**Show offload state connections**

The netstat -t command generates a list of the current connection offload state. The offload state refers to the [TCP Chimney Offload](https://support.microsoft.com/en-us/help/951037/information-about-the-tcp-chimney-offload-receive-side-scaling-and-net), which is a feature that transfers the network workload from the processor to the network adapter during data transmissions. The "InHost" value indicates that offloading isn't enabled, and the "Offload" means that the feature is transferring the workload to the network adapter. (This feature is only present on supported network adapters.)

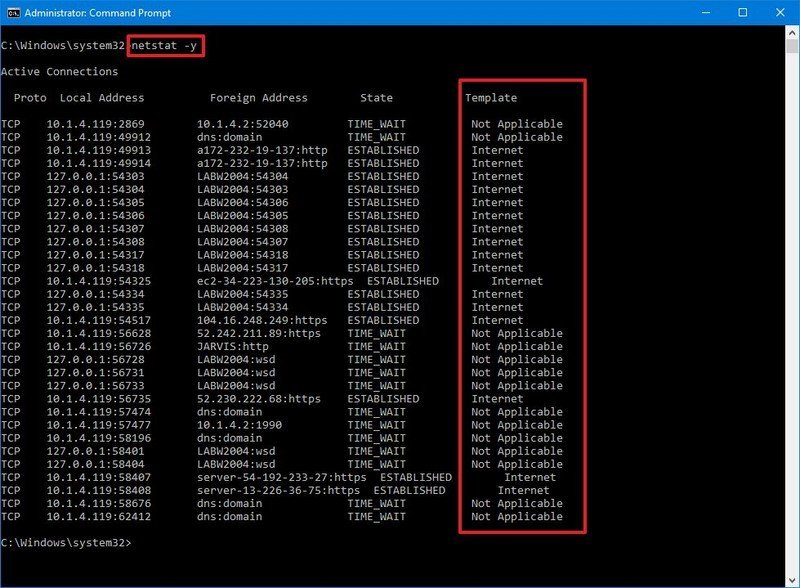
**Show NetworkDirect connections**

The netstat -x is another supported command on Windows 10, and it produces a list of NetworkDirect connections, shared endpoints, and listeners.

[NetworkDirect](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh997033(v=ws.11)) is a specification for Remote Direct Memory Access (RDMA), which is a process that allows fast data transfers using the network adapter, freeing up the processor to perform other tasks. Usually, you'll never use this command unless you're using the server version of Windows or a high-performance application with a network adapter that supports this feature.

**Show connection template**

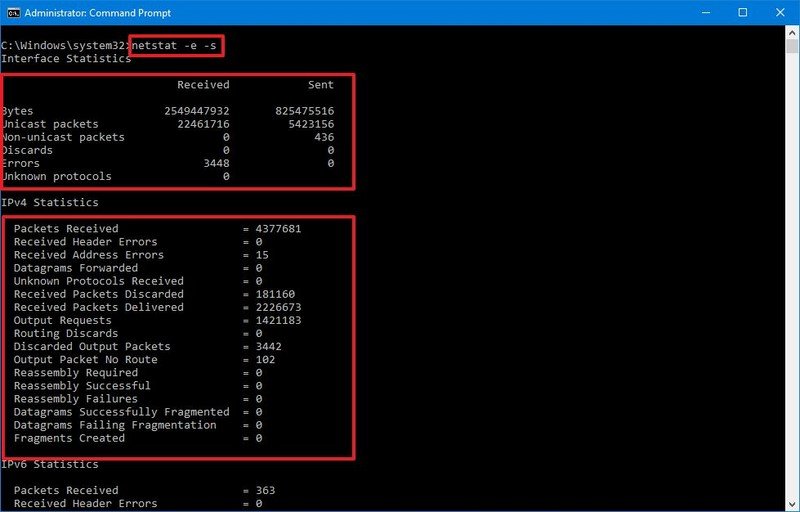
The netstat -y command displays TCP connections templates for all connections.

*[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2020/10/netstat-y-template.jpg)*Source: Windows Central

**Combine parameters**

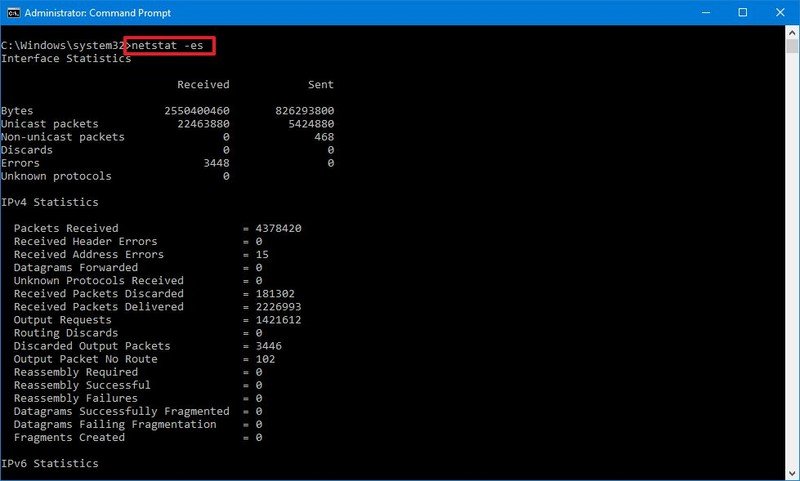
When using the netstat command, you can also combine the parameters to display various information together for many cases.

For example, the -e parameter can also be used with the -s parameter to see statistics for each available protocol, and the -o parameter can be combined with -a, -n, and -p as necessary.

*[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2020/10/netstates-command.jpg)*Source: Windows Central

With the netstat -p command, you append the s parameter, you can display statistics from even more protocols, including icmp, ip, icmpv6, and ipv6.

Also, when using more than one parameter, you can combine them with a single -. For example, instead of writing the command netstat -e -s, you can write it like this: netstat -es.

*[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2020/10/netstat-es-parameters.jpg)*Source: Windows Central

If you want to see all the available parameters and additional help, you can always use the netstat /? command.

**How to search netstat details on Windows 10**

In addition to displaying all the available statistic information, you can also output only the certain details you need using these steps:

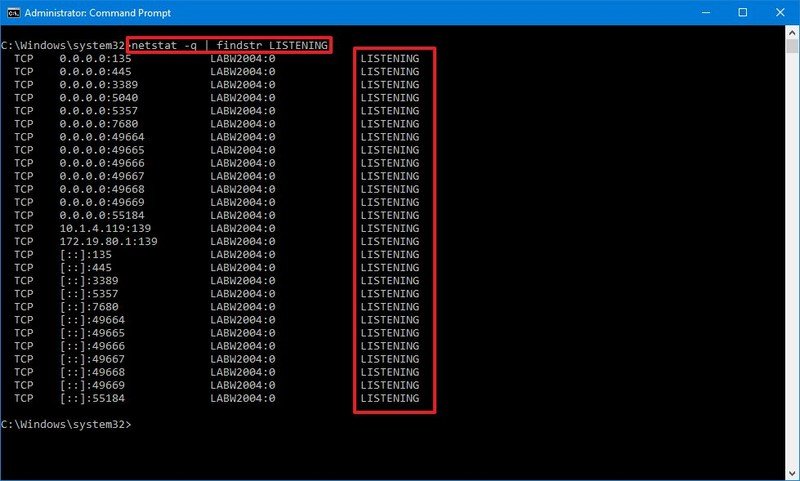
1. Open **Start**.
2. Search for **Command Prompt**, right-click the top result, and select the **Run as administrator** option.
3. Type the following command to list all the connections that have the state set to LISTENING and press **Enter**:

netstat -q | findstr STRING

In the command, make sure to replace STRING for the information you want to list. Also, the **findstr** option is case sensitive, which means that you must enter the string you want to find with the exact casing.

This example lists all the connections that have the state set to "LISTENING."

netstat -q | findstr LISTENING

*[](https://www.windowscentral.com/sites/wpcentral.com/files/styles/xlarge/public/field/image/2020/10/findstr-netstat-command.jpg)*Source: Windows Central

This other example shows all the connections from a foreign server FQDN, in this case, Amazon:

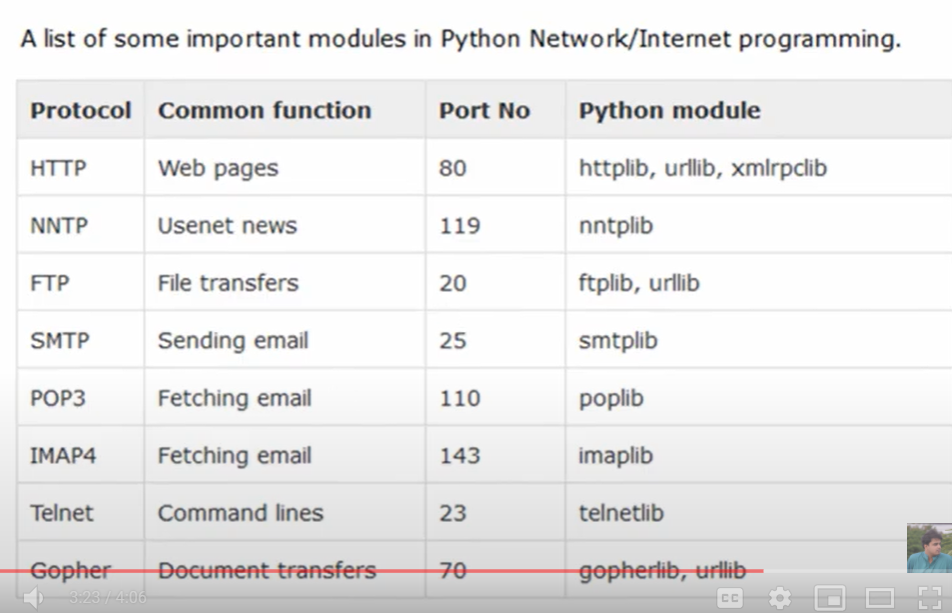
netstat -f | findstr amazon

As you can see, you only need to type part of the string to return a result.

The **findstr** command isn't part of the **netstat** tool. It's a simple command to search for a text string in a file, but you can use it with many of the netstat commands to make more sense of the information you're viewing.

The netstat command is available on Windows 10, but you can also find it on Windows Server, Windows 8.x, Windows 7, and older versions. The tool is not exclusive to Windows either, as it's also available across platforms, including Linux and macOS. Even though the parameters and syntax may be different, they all are very similar.

**PORT No**



**SOCKETS**

Socket command in Python

Socket.socket() :- create a socket

s.bind(host,port) :- bind a host and port to the socket

s.send():- and send the message

s.listen():-

s.recv():-

s.close():- after all then close socket

**DIRECT + REVERSE CONNECTION**

**Direct Connection:--** To Remotely connected Directly to another computer known as Direct connection

Req Both computer IP Address

Create a Cloud Sever on DigitalOcean