How to find open and blocked TCP / UDP ports

Most likely you are reading this article because an application you are trying to run indicates a port is blocked or you have read the documentation that leaving certain ports open on the network could cause security issues.

Most likely you are reading this article because an application you are trying to run indicates a port is blocked or you have read the documentation that leaving certain ports open on the network could cause security issues.

In this article, **TipsMake.com** will explain what a TCP / UDP port is and how to check your computer for open or closed ports.

What is a TCP / UDP port?

The two common types of ports on modern networks are called TCP and UDP. These two types of ports use different network protocols.

Both types of ports are built on the basic Internet Protocol (IP), which makes the Internet and home network work well. However, they are suitable for different applications.

The big difference is that when you send information via UDP, the sender doesn't have to establish a connection with the recipient before starting the conversation. This is almost like sending a letter. You don't know if other people will receive your message and there is no guarantee that you will get any feedback.

On the other hand, TCP is more like making phone calls. The recipient must receive connection data and have a flow of information back and forth until someone deliberately hung up.

UDP messages are usually broadcast over the network to anyone listening on the designated UDP port. This makes it the perfect choice for network-related messages, streaming Voice over Internet Protocol (VoIP), video games and broadcasts.

These applications benefit from the low latency and unrelated information flow of UDP. TCP is much more common than UDP and completely ensures that all data received is error free.

Which ports are usually opened by default?

There are many ports. The port number can range from **0** to **65535** ! But that doesn't mean that any application can choose an arbitrary port, since there are standards and ranges set.

Ports **0 - 1023** are linked to some of the most basic and important network services. This makes sense, since the lower numbered ports are pre-assigned. For example, the **SMTP** protocol for email is used exclusively by port

25.

Ports **1024 - 49151** are called registered ports and are assigned to important common services, such as **OpenVPN** on port **1194** or **Microsoft SQL** on ports **1433** and **1434.**

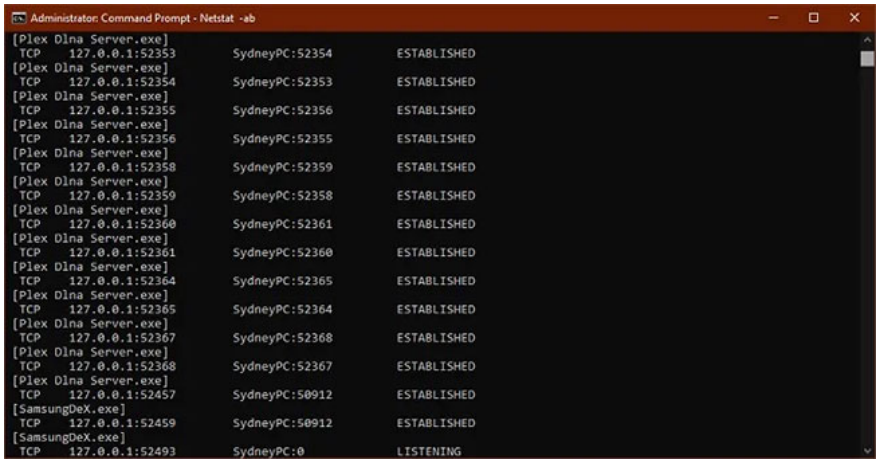
The rest of the port numbers are called dynamic or private ports. These ports are not reserved and anyone can use them online to support a specific service. The only problem arises when two or more services on the same network are using the same port.

While it is not possible to list all important ports, here are some common and very useful ports to know:

1. **20** - FTP (File Transfer Protocol)
2. **22** - Secure Shell (SSH)
3. **25** - Simple Mail Transfer Protocol (SMTP)
4. **53** - Domain Name System (DNS)
5. **80** - Hypertext Transfer Protocol (HTTP)
6. **110** - Post Office Protocol (POP3)
7. **143** - Internet Message Access Protocol (IMAP)
8. **443** - HTTP Secure (HTTPS)

Because there are thousands of common port numbers, the easiest approach is to memorize ranges. This will tell you whether a given port is reserved or not. Thanks to Google, you can also look up services that use a specific port without spending a lot of time.

Find open ports in Windows



Open ports in Windows
Now you have all the basic knowledge of TCP and UDP ports. It's time to find out which ports are open and used on your computer.

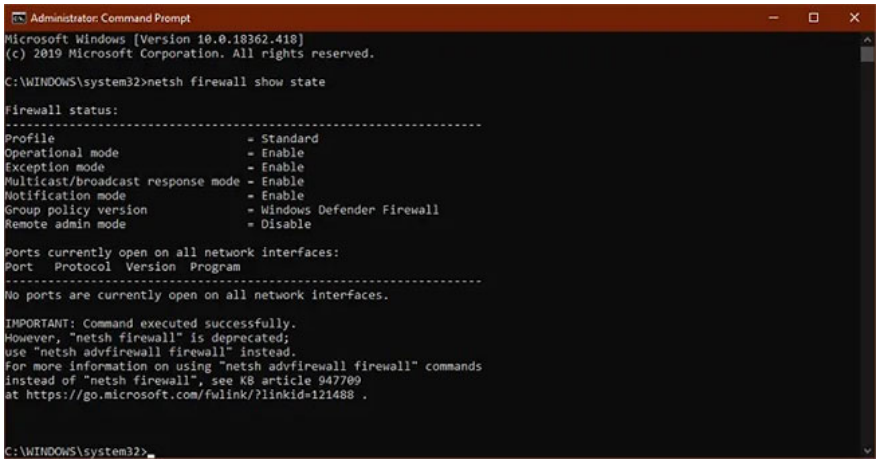
Refer to the article: Check the port (port) is open, the connection is being made in the system for details.

Scan for blocked ports

The above section focuses on finding out which ports are being used by which applications, but does not tell us which ports are being blocked by Windows Firewall.

1. Again, open the Command Prompt with admin rights.
2. With the Command Prompt open, type:

```
netsh firewall show state
```

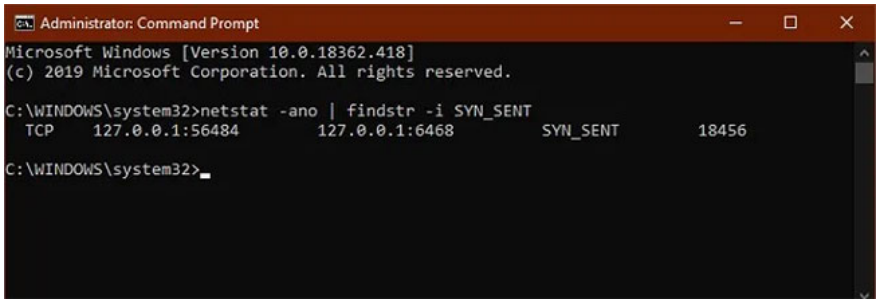


The port is being blocked by Windows Firewall
Currently, using the **show state** command is the quickest and easiest way to get portal information.

Windows Firewall does not block a port does not mean that the router or ISP. Therefore, it is necessary to check if any external blocking is happening.

1. Open Command Prompt with admin rights.
2. With the Command Prompt open, type:

```
netstat -ano | findstr -i SYN_SENT
```



Check for external blocking
If you do not see anything listed, it means that no ports have been blocked. If several ports are listed, that means they are being blocked. If a port not blocked by Windows is shown here, you may want to check your router or send an email to your ISP, if you can't switch to another port.