

Checking for Open Ports

So this is what we have learnt so far.

Your web browser (example: chrome) sends a search request to Google's IP on port 443 from a temporary port on your device, lets say, 45695. Your IP address and this Port number is written on the packet as source address. This packet reaches Google's web server and the server looks at the destination port number, which is 443 and accordingly gives the packet to the Website’s handling software. This software processes the request, collects the search results, and sends a reply back to the your IP address and Port that was written on the packet. The response reaches your device and is forwarded to your web browser application that requested for the page.

Now let’s check what applications are running on our computers/laptops. For this we will look at the open ports running on our machines.

To check for open ports on a windows machine:

1. Go to the start menu and type cmd.

2. Right click on the command prompt and click on the ‘run as administrator’ option.

3. Type netstat -a | find /i "listening"

You will see a list of all ports that are listening for a request.

To check for open ports on a Mac OS:

1. Open the terminal and run the following command.

2. netstat -an | grep LISTEN

To check for open ports on a Linux machine:

1. Open the terminal and run the following command.

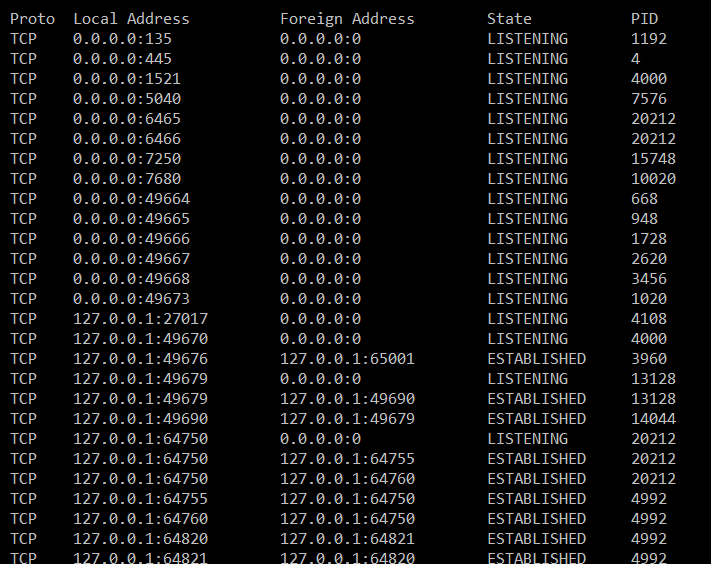
2. netstat -lpnt

Exercise

Q1. Run the netstat command and see what ports are running on your system. Use Google and find out what these ports are used for and then deduce why your system is waiting for a connection on each of these ports.

On Windows, Run cmd as administrator and inside it, “netstat -aon”.

Here is a sample output:



As you can see we have 5 columns.

Proto: This is the base protocol being used (TCP/UDP)

Local address: This is the IP address and Port number (separated by a colon) of your computer being used to communicate.

Now you can see that in the screenshot, we have various IP addresses: 0.0.0.0 , 10.0.75.1 , 127.0.0.1

This IP address tells you which network is this entry for. For example, if you are connected via LAN cable and get the IP 192.168.12.123, then all communications via the LAN cable will have this IP. Parallelly, if you also have WiFi connected with the IP address 10.0.0.145 then for WiFi connections, this IP will be shown.

Also, 0.0.0.0 simply means all interfaces, be it Local, LAN, WiFi etc. And 127.0.0.1 means communication is happening locally within your own computer between different applications.

Foreign Address: This is the address of the device your system is communicating with. So let’s say you visit Google.com on port 443 and Google’s IP address is 1.2.3.4 then in the foreign address, you will see 1.2.3.4:443 and in the local address, you will see the IP address of the network interface being used to connect to Google (Like your LAN IP or your WiFi IP etc)

State: This is a very important column as it tells you the state of the connection. In the above screenshot, you can see ‘Listening’, which means your system is waiting for a connection on the given port. Similarly, ‘Established’ means a connection has already been made and communication is probably happening.

PID: This is the process ID of the software handling the communication. You can use ‘tasklist’ command to see all running programs and their respective process ID.

Now let us break down the 1st entry in the output

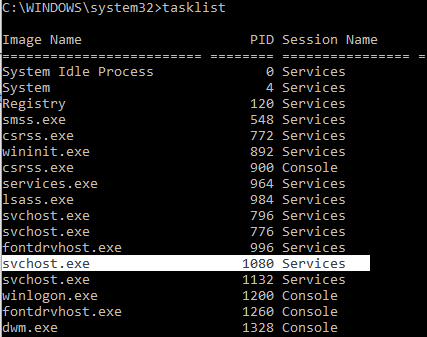
Here the Protocol is TCP

As the state is listening, and the local address is 0.0.0.0:135 it means that our computer is waiting for connections on port 135 and 0.0.0.0 means from anywhere, so anyone in your network whether WiFi, LAN or from your own computer, can connect to your IP on port 135.

In listening, the foreign address doesn't matter too much.

The PID here is 1080.

Below is the output of tasklist command showing what exactly is 1080.



So this means that svchost.exe is listening on port 135 for incoming connections from anywhere (0.0.0.0)

Now your task was to find open ports on your computer which are waiting for connections i.e.state is Listening.

From the 1st screenshot, we can see that our system is listening for connections on the following ports:

135, 445, 903, 913, 1536, 1537 and many more (you might have more or less ports)

You can search about these ports on Google to see what they are used for and why your system is waiting for the connection.

For example, the port 135 is used by an internal Windows Service responsible for your system to communicate with other Windows machines in the network for file sharing, authentication, etc.

Same is for 445.

Summary

Now that we have come to the end of this topic, you should be able to:

1. Understand how clients and servers interact with each other in a network

2. Describe the role played by port numbers in this interaction

3. Explain the purpose of ports and their internal working

4. Differentiate between local and remote ports