Window Networking Commands: netstat

Connect with me: Youtube | LinkedIn | WhatsApp Channel | Web | Facebook | Twitter

- Download PDF
- To access the updated handouts, please click on the following link:
  https://yasirbhutta.github.io/windows/docs/netstat.html

Here are practical tasks for the netstat (network statistics) command in Windows to help you understand and apply its functionality:

1. Display All Active Connections

Task: View all active TCP connections on your machine.

Command:

```
netstat
```

Goal: Understand which local and remote IP addresses are connected, and observe the connection states.

2. Display Active Connections with Application Details

Task: View active connections along with the application/process that initiated them.

Command:

```
netstat -b
```

Goal: Identify which applications are responsible for each network connection.

3. Display Active Connections and Resolve IP Addresses to Domain Names

Task: View all active connections and resolve the IP addresses of remote systems to domain names.

Command:

```
netstat -a -n
```

Goal: Recognize which domain each IP belongs to, which is helpful for identifying connections to known or unknown hosts.

4. Display Listening Ports

Task: Show all listening ports on your system (i.e., services or applications that are waiting for inbound connections).

Command:

```
netstat -an | find "LISTEN"
```

Goal: Identify which ports are open and waiting for connections, useful for security checks.

5. Display Protocol Statistics

Task: View statistical data for each protocol (TCP, UDP, ICMP, etc.) on your system.

Command:

```
netstat -s
```

Goal: Analyze the performance and usage of various network protocols on your system.

6. Monitor Network Connections in Real-Time

Task: Continuously monitor active connections and view updated statistics every few seconds.

Command:

```
netstat -an 5
```

Goal: Watch live network activity on your system and monitor changes in connections as they occur.

7. Show All Active UDP Connections

Task: Display all current UDP connections on your system.

Command:

```
netstat -anp udp
```

Goal: Understand which applications are using UDP, a protocol that doesn't establish connections like TCP.

8. Find Established Connections Only

Task: List only connections that are in the "ESTABLISHED" state.

Command:

```
netstat -an | find "ESTABLISHED"
```

Goal: Focus on connections that are actively transmitting data and analyze their endpoints.

9. View Active Network Connections by Process ID (PID)

Task: Display all network connections with the associated process ID (PID).

Command:

```
netstat -o
```

Goal: Identify which process is using each network connection, useful for troubleshooting performance issues or security concerns.

10. Display Ethernet Statistics

Task: View detailed statistics about your Ethernet interface, including data sent/received, errors, and discards.

Command:

```
netstat -e
```

Goal: Monitor Ethernet performance and check for transmission or reception errors on your network interface.

11. Display Routing Table

Task: Display the current routing table on your machine, showing how traffic is routed based on destination IPs.

Command:

```
netstat -r
```

Goal: Understand how your system routes network traffic and verify if any static or dynamic routes are configured.

12. Display Connection Statistics for IPv4 and IPv6

Task: View network statistics for both IPv4 and IPv6 connections.

Command:

```
netstat -sp tcp
```

Goal: Analyze connection performance and error statistics for IPv4/IPv6 connections.

13. Track Connections to a Specific Remote Host

Task: Monitor network activity to/from a specific remote IP address or hostname.

Command:

```
netstat -an | find "<Remote IP or Hostname>"
```

Goal: Focus on traffic involving a specific external server, which is useful for troubleshooting connections to a particular service.

14. Find Connections on a Specific Port

Task: Display all connections or services using a specific port (e.g., port 80 for HTTP).

Command:

```
netstat -an | find ":80"
```

Goal: Identify which applications are using a particular port and check for suspicious or unauthorized activity.

15. Save netstat Output to a File

Task: Save the output of the netstat command to a file for later analysis or reporting.

Command:

```
netstat -an > netstat_output.txt
```

Goal: Generate a log of active connections that can be shared or analyzed later.