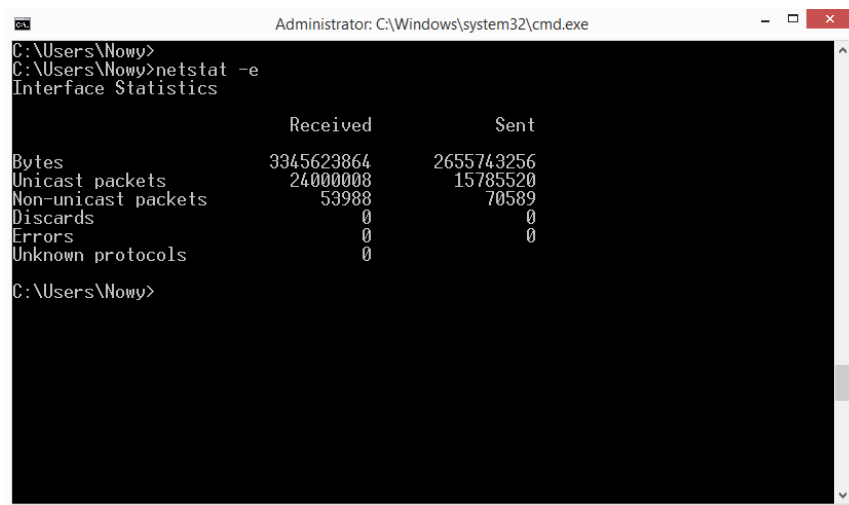


## NETSTAT – checking open ports and interface statistics

Netstat (Network Statistics) is a program that allows you to examine the traffic that is generated on specific network interfaces and ports. The program is available on most platforms, one may differ in switches. The most frequently used queries, using the netstat program on the Windows platform, will be presented below.

### Interface statistics



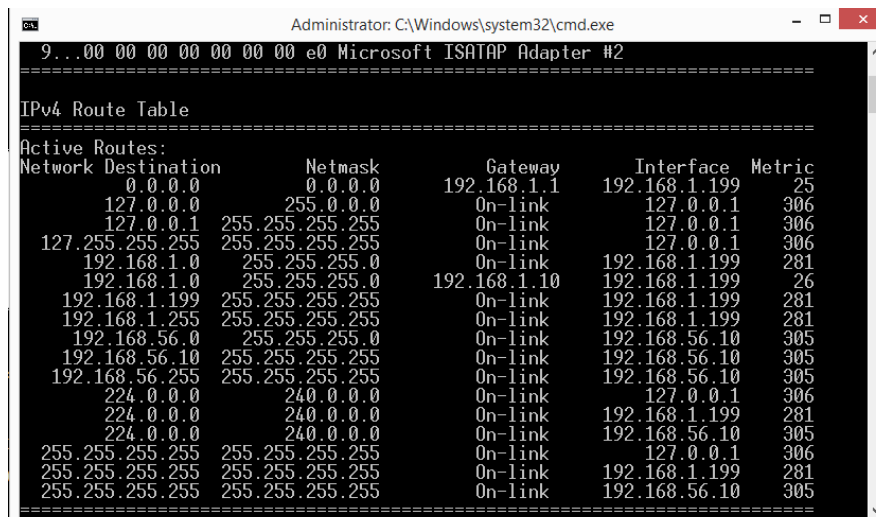
```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Nowy>
C:\Users\Nowy>netstat -e
Interface Statistics

                Received                Sent
Bytes           3345623864           2655743256
Unicast packets 24000008             15785520
Non-unicast packets 53988             70589
Discards        0                     0
Errors          0                     0
Unknown protocols 0
C:\Users\Nowy>
```

### Routing table

Example command:

netstat -r



```
Administrator: C:\Windows\system32\cmd.exe
9...00 00 00 00 00 00 e0 Microsoft ISATAP Adapter #2
=====
IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.1.1     192.168.1.199    25
127.0.0.0                  255.0.0.0        0n-link        127.0.0.1        306
127.0.0.1                  255.255.255.255 0n-link        127.0.0.1        306
127.255.255.255           255.255.255.255 0n-link        127.0.0.1        306
192.168.1.0                255.255.255.0   0n-link        192.168.1.199    281
192.168.1.0                255.255.255.0   192.168.1.10  192.168.1.199    26
192.168.1.199             255.255.255.255 0n-link        192.168.1.199    281
192.168.1.255             255.255.255.255 0n-link        192.168.1.199    281
192.168.56.0              255.255.255.0   0n-link        192.168.56.10    305
192.168.56.10            255.255.255.255 0n-link        192.168.56.10    305
192.168.56.255           255.255.255.255 0n-link        192.168.56.10    305
224.0.0.0                 240.0.0.0        0n-link        127.0.0.1        306
224.0.0.0                 240.0.0.0        0n-link        192.168.1.199    281
224.0.0.0                 240.0.0.0        0n-link        192.168.56.10    305
255.255.255.255           255.255.255.255 0n-link        127.0.0.1        306
255.255.255.255           255.255.255.255 0n-link        192.168.1.199    281
255.255.255.255           255.255.255.255 0n-link        192.168.56.10    305
=====
```

## Protocols statistics

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Nowy>netstat -s -p TCP

TCP Statistics for IPv4

Active Opens           = 496524
Passive Opens         = 10278
Failed Connection Attempts = 93437
Reset Connections     = 23627
Current Connections   = 8
Segments Received     = 526630431
Segments Sent         = 503461046
Segments Retransmitted = 3018163

Active Connections

Proto Local Address          Foreign Address         State
TCP   127.0.0.1:43471        Lenovo:43472            ESTABLISHED
TCP   127.0.0.1:43472        Lenovo:43471            ESTABLISHED
TCP   127.0.0.1:43473        Lenovo:43474            ESTABLISHED
TCP   127.0.0.1:43474        Lenovo:43473            ESTABLISHED
TCP   127.0.0.1:43475        Lenovo:43476            ESTABLISHED
TCP   127.0.0.1:43476        Lenovo:43475            ESTABLISHED
TCP   192.168.1.199:5633    UBUNTU:microsoft-ds    ESTABLISHED
TCP   192.168.1.199:6051    DANE:microsoft-ds      ESTABLISHED
```

## Check list of processes assigned with existing connections

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Nowy>netstat -o

Active Connections

Proto Local Address          Foreign Address         State          PID
TCP   127.0.0.1:43471        Lenovo:43472            ESTABLISHED    6892
TCP   127.0.0.1:43472        Lenovo:43471            ESTABLISHED    6892
TCP   127.0.0.1:43473        Lenovo:43474            ESTABLISHED    12812
TCP   127.0.0.1:43474        Lenovo:43473            ESTABLISHED    12812
TCP   127.0.0.1:43475        Lenovo:43476            ESTABLISHED    12060
TCP   127.0.0.1:43476        Lenovo:43475            ESTABLISHED    12060
TCP   192.168.1.199:5633    UBUNTU:microsoft-ds    ESTABLISHED    4
TCP   192.168.1.199:6051    DANE:microsoft-ds      ESTABLISHED    4

C:\Users\Nowy>
```

### Description states of network from command netstat:

- **SYN\_SEND** - server sent SYN (Active open)
- **SYN\_RECEIVED** - server received SYN from client
- **ESTABLISHED** - server resent SYN to client, connection is established
- **LISTENING** - server is ready for incoming connection
- **FIN\_WAIT\_1** - server sent FIN (active close)
- **TIMED\_WAIT** - client status after received FIN from server
- **CLOSE\_WAIT** - server received FIN from client (passive close)
- **FIN\_WAIT\_2** - client received confirming packet after sent FIN
- **LAST\_ACK** - server sent FIN
- **CLOSED** - server received ACK from client, connection is closed