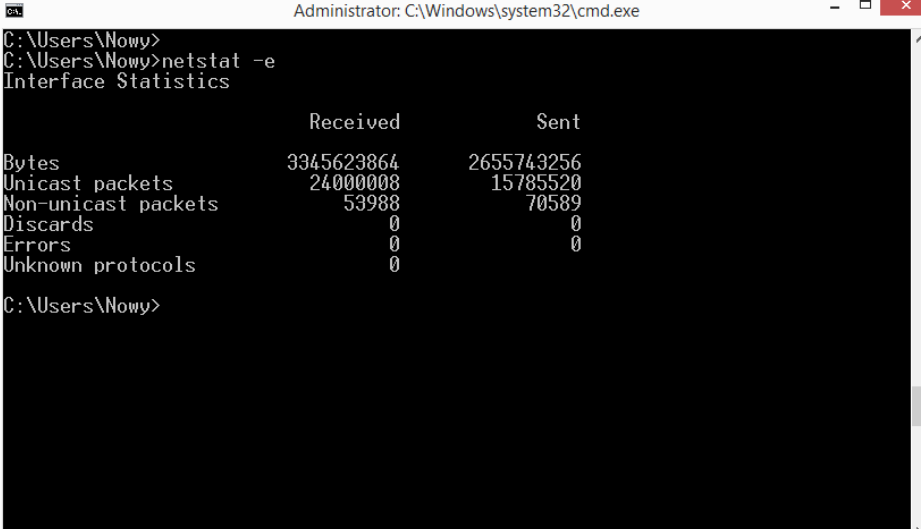


NETSTAT – sprawdzanie otwartych portów oraz statystyki interfejsów

Netstat (Network Statistics) jest programem, który pozwala zbadać ruch, jaki jest generowany na określonych interfejsach sieciowych oraz portach. Program jest dostępny na większości platform, może się jedna różnić przełącznikami.

Poniżej zostaną przedstawiona najczęściej wykorzystywane zapytania, z wykorzystaniem programu netstat na platformie Windows.

Statystyki interfejsu

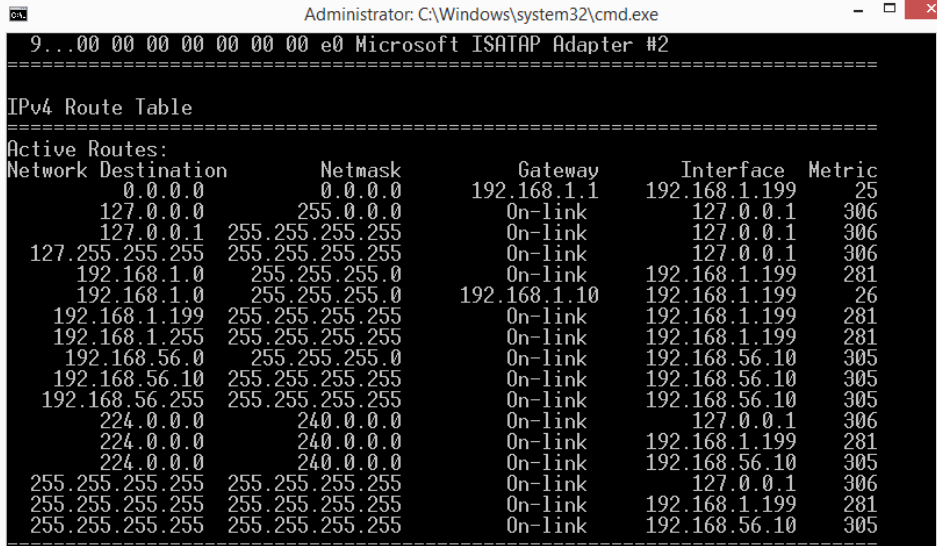


```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Nowy>
C:\Users\Nowy>netstat -e
Interface Statistics

                Received            Sent
Bytes           3345623864            2655743256
Unicast packets 240000008                15785520
Non-unicast packets 53988                    70589
Discards        0
Errors          0
Unknown protocols 0

C:\Users\Nowy>
```

Tablice routingu



```
Administrator: C:\Windows\system32\cmd.exe
9...00 00 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        On-link         127.0.0.1       306
127.0.0.1              255.255.255.255 On-link         127.0.0.1       306
127.255.255.255        255.255.255.255 On-link         127.0.0.1       306
192.168.1.0            255.255.255.0    On-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 On-link         192.168.1.199   281
192.168.1.255          255.255.255.255 On-link         192.168.1.199   281
192.168.56.0           255.255.255.0    On-link         192.168.56.10   305
192.168.56.10          255.255.255.255 On-link         192.168.56.10   305
192.168.56.255         255.255.255.255 On-link         192.168.56.10   305
224.0.0.0              240.0.0.0        On-link         127.0.0.1       306
224.0.0.0              240.0.0.0        On-link         192.168.1.199   281
224.0.0.0              240.0.0.0        On-link         192.168.56.10   305
255.255.255.255        255.255.255.255 On-link         127.0.0.1       306
255.255.255.255        255.255.255.255 On-link         192.168.1.199   281
255.255.255.255        255.255.255.255 On-link         192.168.56.10   305
```

Statystyki protokołów

```
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               = 508461046
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
```

Sprawdzanie listy procesów powiązanych z istniejącymi połączeniami

```
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>
```

Opis stanów sieci, jakie mogą być zwracane w wyniku działania programu netstat:

- **SYN_SEND** serwer wysłał pakiet SYN (Active open)
- **SYN_RECEIVED** Serwer otrzymał pakiet SYN od klienta
- **ESTABLISHED** Serwer odesłał pakiet SYN do klienta, połączenie zostało zestawione
- **LISTENING** Serwer gotowy jest na przyjęcie połączenia
- **FIN_WAIT_1** Serwer wysłał pakiet FIN (active close)
- **TIMED_WAIT** Status klienta po otrzymaniu pakietu FIN on serwera
- **CLOSE_WAIT** Serwer otrzymał pakiet FIN od klienta (passive close)
- **FIN_WAIT_2** Klient otrzymał pakiet potwierdzający wysłany FIN
- **LAST_ACK** Serwer wysłał pakiet FIN
- **CLOSED** Serwer otrzymał pakiet ACK od klienta, połączenie jest zamknięte