

## Netstat

Dzięki NETSTAT można poznać szczegóły połączeń sieciowych, takie jak adresy IP i porty używane przez poszczególne procesy, informacje o błędach i ilości przesyłanych danych. To narzędzie może być przydatne w diagnostyce problemów z siecią, w zabezpieczaniu systemu przed zagrożeniami sieciowymi oraz w monitorowaniu wydajności sieci.

```
C:\Users\Chorus>netstat
```

### Active Connections

Proto	Local Address	Foreign Address	State
TCP	10.202.14.168:51838	server-18-66-233-122:https	ESTABLISHED
TCP	10.202.14.168:51841	waw07s06-in-f10:https	CLOSE_WAIT
TCP	10.202.14.168:51843	192.178.25.170:https	ESTABLISHED
TCP	10.202.14.168:51844	40.113.103.199:https	ESTABLISHED
TCP	10.202.14.168:51856	162.159.133.234:https	ESTABLISHED
TCP	10.202.14.168:51875	waw02s22-in-f10:https	CLOSE_WAIT
TCP	10.202.14.168:51880	1f-in-f188:5228	ESTABLISHED
TCP	10.202.14.168:51915	edge-star-shv-01-waw1:https	ESTABLISHED
TCP	10.202.14.168:51917	edge-dgw-shv-01-waw1:https	ESTABLISHED
TCP	10.202.14.168:51947	ec2-3-66-97-52:https	ESTABLISHED
TCP	10.202.14.168:51953	edge-star-shv-01-waw1:https	ESTABLISHED
TCP	10.202.14.168:51957	edge-star-shv-01-waw1:https	ESTABLISHED
TCP	10.202.14.168:51971	162-254-197-39:27024	ESTABLISHED
TCP	10.202.14.168:51974	ec2-3-66-97-52:https	ESTABLISHED
TCP	10.202.14.168:52127	waw02s17-in-f10:https	CLOSE_WAIT
TCP	10.202.14.168:52158	waw07s06-in-f10:https	CLOSE_WAIT
TCP	10.202.14.168:52245	waw02s17-in-f14:https	ESTABLISHED
TCP	10.202.14.168:52248	waw02s22-in-f10:https	CLOSE_WAIT
TCP	10.202.14.168:52251	waw02s13-in-f3:https	ESTABLISHED
TCP	10.202.14.168:52255	waw02s22-in-f4:https	ESTABLISHED
TCP	10.202.14.168:52257	waw02s22-in-f10:https	CLOSE_WAIT
TCP	10.202.14.168:52261	40.115.3.253:https	ESTABLISHED
TCP	10.202.14.168:52283	waw07s05-in-f14:https	TIME_WAIT
TCP	10.202.14.168:52315	172.67.68.167:https	ESTABLISHED
TCP	10.202.14.168:52318	172.67.73.9:https	ESTABLISHED
TCP	10.202.14.168:52319	waw02s14-in-f14:https	TIME_WAIT
TCP	10.202.14.168:52320	waw07s06-in-f10:https	TIME_WAIT
TCP	10.202.14.168:52321	192.178.25.170:https	TIME_WAIT
TCP	10.202.14.168:52322	104.18.3.161:https	ESTABLISHED
TCP	10.202.14.168:52323	104.18.6.185:https	ESTABLISHED
TCP	10.202.14.168:52325	a23-64-12-59:https	CLOSE_WAIT
TCP	10.202.14.168:52326	a23-64-12-59:https	CLOSE_WAIT
TCP	10.202.14.168:52333	104.18.13.135:https	ESTABLISHED
TCP	10.202.14.168:52341	waw07s05-in-f13:https	TIME_WAIT
TCP	10.202.14.168:52342	192.178.25.161:https	TIME_WAIT
TCP	10.202.14.168:52343	waw07s05-in-f3:https	TIME_WAIT
TCP	10.202.14.168:52344	waw02s14-in-f14:https	TIME_WAIT
TCP	10.202.14.168:52345	waw07s03-in-f14:https	TIME_WAIT
TCP	10.202.14.168:52346	waw07s03-in-f14:https	TIME_WAIT
TCP	10.202.14.168:52349	20.93.28.56:https	ESTABLISHED
TCP	10.202.14.168:52350	20.93.28.56:https	ESTABLISHED
TCP	10.202.14.168:52354	waw07s05-in-f13:https	TIME_WAIT

### netstat -a

wyświetla wszystkie połączenia i porty oczekujące

Komenda netstat -a wyświetla wszystkie połączenia i nasłuchiwanie porty. Po użyciu tej komendy można zobaczyć:

- Aktywne połączenia TCP i UDP z ich adresami IP i portami.
- Nasłuchiwanie porty, na których procesy nasłuchują połączeń przychodzących.
- Stan połączenia, taki jak ESTABLISHED (ustanowione), LISTENING (nasłuchiwanie), WAITING (oczekiwanie) i inne.
- Adresy IP, z których połączenia zostały nawiązane, a także porty używane przez te połączenia.
- ID procesów, które są związane z każdym połączeniem.

Te informacje mogą pomóc w zdiagnozowaniu problemów z siecią, identyfikowaniu połączeń sieciowych, które zostały nawiązane i wykrywaniu aktywności sieciowej, która może być podejrzana.

```
C:\Users\Chorus>netstat -a
```

#### Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:135	DESKTOP-DJPTOCG:0	LISTENING
TCP	0.0.0.0:445	DESKTOP-DJPTOCG:0	LISTENING
TCP	0.0.0.0:1462	DESKTOP-DJPTOCG:0	LISTENING
TCP	0.0.0.0:5040	DESKTOP-DJPTOCG:0	LISTENING
TCP	0.0.0.0:7680	DESKTOP-DJPTOCG:0	LISTENING
TCP	0.0.0.0:8501	DESKTOP-DJPTOCG:0	LISTENING
TCP	0.0.0.0:27036	DESKTOP-DJPTOCG:0	LISTENING
TCP	0.0.0.0:49664	DESKTOP-DJPTOCG:0	LISTENING
TCP	0.0.0.0:49665	DESKTOP-DJPTOCG:0	LISTENING
TCP	0.0.0.0:49666	DESKTOP-DJPTOCG:0	LISTENING
TCP	0.0.0.0:49667	DESKTOP-DJPTOCG:0	LISTENING
TCP	0.0.0.0:49668	DESKTOP-DJPTOCG:0	LISTENING
TCP	0.0.0.0:49670	DESKTOP-DJPTOCG:0	LISTENING
TCP	10.202.14.168:139	DESKTOP-DJPTOCG:0	LISTENING
TCP	10.202.14.168:51846	waw02s16-in-f10:https	ESTABLISHED
TCP	10.202.14.168:51862	lq-in-f188:5228	ESTABLISHED
TCP	10.202.14.168:51868	40.113.110.67:https	ESTABLISHED
TCP	10.202.14.168:51884	waw02s14-in-f14:https	ESTABLISHED

**netstat-e** wyświetla statystyki Ethernet-u. Ta opcja może być używana razem z opcją -s. Komenda netstat -e wyświetla statystyki sieciowe Ethernet. Po użyciu tej komendy można zobaczyć:

- Ilość wysłanych i odebranych pakietów.
- Ilość błędów transmisji (np. pakietów odrzuconych, błędnie przesłanych).
- Ilość pakietów otrzymanych z błędem CRC (suma kontrolna cykliczna).
- Ilość unieważnionych pakietów (np. duplikaty).
- Ilość pakietów odrzuconych z powodu zbyt małej wielkości.
- Ilość pakietów wysłanych z powodu konfliktu adresów.
- Ilość pakietów odrzuconych z powodu przepełnienia bufora.
- Ilość błędów protokołu (np. nieobsługiwane protokoły).
- Ilość pakietów wygasłych (przekroczenie czasu życia).

Te statystyki mogą pomóc w identyfikacji problemów z siecią i pomóc w ustaleniu, czy połączenia sieciowe działają prawidłowo.

```
C:\Users\Chorus>netstat -e
Interface Statistics
```

	Received	Sent
Bytes	323324688	44823834
Unicast packets	220440	149208
Non-unicast packets	726	2766
Discards	0	0
Errors	0	0
Unknown protocols	0	

Komenda **netstat -n** wyświetla adresy i numery portów w postaci numerycznej. Po użyciu tej komendy można zobaczyć:

- Adresy IP w postaci numerycznej.
- Numery portów w postaci numerycznej.
- Stan połączenia, taki jak ESTABLISHED (ustanowione), LISTENING (nasłuchiwanie), WAITING (oczekiwanie) i inne.
- ID procesów, które są związane z każdym połączeniem.

Użycie tej opcji może pomóc w szybkim identyfikowaniu połączeń sieciowych i portów, które są używane przez procesy systemowe lub aplikacje, co może być przydatne w analizie i monitorowaniu wydajności sieci.

```
C:\Users\Chorus>netstat -n
Active Connections
```

Proto	Local Address	Foreign Address	State
TCP	10.202.14.168:56285	172.67.73.9:443	ESTABLISHED
TCP	10.202.14.168:56290	172.217.16.42:443	CLOSE_WAIT
TCP	10.202.14.168:56306	104.18.2.161:443	ESTABLISHED
TCP	10.202.14.168:56309	104.18.6.185:443	ESTABLISHED
TCP	10.202.14.168:56332	142.250.203.202:443	CLOSE_WAIT
TCP	10.202.14.168:56336	142.250.75.10:443	TIME_WAIT
TCP	10.202.14.168:56339	216.58.215.106:443	TIME_WAIT
TCP	10.202.14.168:56344	104.81.116.49:80	TIME_WAIT
TCP	10.202.14.168:56345	104.81.116.49:80	TIME_WAIT
TCP	10.202.14.168:56349	216.58.215.78:443	ESTABLISHED
TCP	10.202.14.168:56350	94.130.182.214:443	ESTABLISHED
TCP	10.202.14.168:56351	172.217.16.3:443	ESTABLISHED
TCP	10.202.14.168:56352	216.58.209.10:443	ESTABLISHED
TCP	10.202.14.168:56353	142.250.203.202:443	ESTABLISHED
TCP	10.202.14.168:56354	142.250.203.202:443	ESTABLISHED
TCP	10.202.14.168:56355	40.113.110.67:443	ESTABLISHED
TCP	10.202.14.168:56356	31.13.81.36:443	ESTABLISHED
TCP	10.202.14.168:56358	31.13.81.13:443	ESTABLISHED
TCP	10.202.14.168:56359	8.241.46.121:80	ESTABLISHED
TCP	10.202.14.168:56360	216.58.209.3:443	ESTABLISHED
TCP	10.202.14.168:56361	142.250.203.196:443	ESTABLISHED
TCP	10.202.14.168:61461	64.233.165.188:5228	ESTABLISHED
TCP	10.202.14.168:61463	40.113.103.199:443	ESTABLISHED
TCP	10.202.14.168:61464	142.250.203.142:443	ESTABLISHED
TCP	10.202.14.168:61471	172.217.16.46:443	ESTABLISHED
TCP	10.202.14.168:61472	162.159.130.234:443	ESTABLISHED
TCP	10.202.14.168:61473	20.93.28.56:443	ESTABLISHED
TCP	10.202.14.168:61474	20.93.28.56:443	ESTABLISHED
TCP	10.202.14.168:61479	216.58.215.106:443	ESTABLISHED
TCP	10.202.14.168:61514	23.64.12.59:443	CLOSE_WAIT
TCP	10.202.14.168:61515	23.64.12.59:443	CLOSE_WAIT
TCP	10.202.14.168:61518	152.199.19.161:443	CLOSE_WAIT
TCP	10.202.14.168:61519	152.199.21.118:443	CLOSE_WAIT
TCP	10.202.14.168:61526	31.13.81.9:443	ESTABLISHED
TCP	10.202.14.168:61527	31.13.81.9:443	ESTABLISHED
TCP	10.202.14.168:61528	31.13.81.7:443	ESTABLISHED
TCP	10.202.14.168:61539	31.13.81.9:443	ESTABLISHED
TCP	127.0.0.1:51822	127.0.0.1:65001	ESTABLISHED
TCP	127.0.0.1:51829	127.0.0.1:59020	ESTABLISHED
TCP	127.0.0.1:59020	127.0.0.1:51829	ESTABLISHED
TCP	127.0.0.1:65001	127.0.0.1:51822	ESTABLISHED

Komenda **netstat -p** protokół wyświetla połączenia z określonym protokołem. Po użyciu tej komendy można zobaczyć:

- Aktywne połączenia z wybranym protokołem, np. TCP, UDP, ICMP.
- Nazwy aplikacji lub procesów, które są związane z każdym połączeniem.
- Adresy IP i numery portów źródłowych i docelowych.

Użycie tej opcji może pomóc w identyfikacji aplikacji lub procesów, które używają określonego protokołu i wykrywaniu aktywności sieciowej związanej z tym protokołem. To może być szczególnie przydatne w analizie wydajności i monitorowaniu sieci.

```
C:\Users\Chorus>netstat -p

Active Connections

    Proto Local Address          Foreign Address         State
C:\Users\Chorus>netstat -r

=====
Interface List
 3...d8 bb c1 25 cb a5 .....Realtek PCIe GbE Family Controller
17...28 d0 ea e0 05 0c .....Microsoft Wi-Fi Direct Virtual Adapter
 9...2a d0 ea e0 05 0b .....Microsoft Wi-Fi Direct Virtual Adapter #2
16...28 d0 ea e0 05 0b .....Intel(R) Wi-Fi 6 AX201 160MHz
11...28 d0 ea e0 05 0f .....Bluetooth Device (Personal Area Network)
 1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway       Interface    Metric
0.0.0.0                  0.0.0.0          10.202.14.1   10.202.14.168  45
10.202.14.0              255.255.255.0    On-link       10.202.14.168  301
10.202.14.168            255.255.255.255  On-link       10.202.14.168  301
10.202.14.255            255.255.255.255  On-link       10.202.14.168  301
127.0.0.0                 255.0.0.0        On-link       127.0.0.1      331
127.0.0.1                 255.255.255.255  On-link       127.0.0.1      331
127.255.255.255          255.255.255.255  On-link       127.0.0.1      331
224.0.0.0                 240.0.0.0        On-link       127.0.0.1      331
224.0.0.0                 240.0.0.0        On-link       10.202.14.168  301
255.255.255.255          255.255.255.255  On-link       127.0.0.1      331
255.255.255.255          255.255.255.255  On-link       10.202.14.168  301
=====
Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1       331 ::1/128             On-link
16      301 fe80::/64           On-link
16      301 fe80::779e:8fa0:5c5e:9c35/128
                                           On-link
1       331 ff00::/8             On-link
16      301 ff00::/8             On-link
=====
```

Komenda **netstat -r** wyświetla tablicę routingu systemu. Po użyciu tej komendy można zobaczyć:

- Listę wszystkich interfejsów sieciowych systemu i ich adresy IP.
- Bramki domyślne, które są używane do przesyłania ruchu sieciowego do innych sieci.
- Tabele routingu dla każdego interfejsu sieciowego, zawierające informacje o trasach sieciowych, które są dostępne poprzez dany interfejs.
- Metryki i flagi routingu, takie jak koszt trasy, jakość połączenia i dostępność.

Użycie tej opcji może pomóc w diagnozowaniu problemów z połączeniami sieciowymi, identyfikowaniu ścieżek sieciowych, które są używane do przesyłania ruchu sieciowego, oraz określaniu, czy dane połączenie jest poprawnie skonfigurowane.

```

C:\Users\Chorus>netstat -r
=====
Interface List
 3...d8 bb c1 25 cb a5 .....Realtek PCIe GbE Family Controller
17...28 d0 ea e0 05 0c .....Microsoft Wi-Fi Direct Virtual Adapter
 9...2a d0 ea e0 05 0b .....Microsoft Wi-Fi Direct Virtual Adapter #2
16...28 d0 ea e0 05 0b .....Intel(R) Wi-Fi 6 AX201 160MHz
11...28 d0 ea e0 05 0f .....Bluetooth Device (Personal Area Network)
 1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          10.202.14.1      10.202.14.168    60
10.202.14.0                255.255.255.0    On-link          10.202.14.168    316
10.202.14.168              255.255.255.255  On-link          10.202.14.168    316
10.202.14.255              255.255.255.255  On-link          10.202.14.168    316
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        331
127.0.0.1                  255.255.255.255  On-link          127.0.0.1        331
127.255.255.255            255.255.255.255  On-link          127.0.0.1        331
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        331
224.0.0.0                  240.0.0.0        On-link          10.202.14.168    316
255.255.255.255            255.255.255.255  On-link          127.0.0.1        331
255.255.255.255            255.255.255.255  On-link          10.202.14.168    316
=====
Persistent Routes:
None

IPv6 Route Table
=====
Active Routes:
If Metric Network Destination      Gateway
1    331 ::1/128                      On-link
16   316 fe80::/64                    On-link
16   316 fe80::779e:8fa0:5c5e:9c35/128
                                         On-link
1    331 ff00::/8                      On-link
16   316 ff00::/8                      On-link
=====
Persistent Routes:
None

```

Komenda **netstat -s** wyświetla statystyki protokołów sieciowych i interfejsów sieciowych systemu. Po użyciu tej komendy można zobaczyć:

- Liczbę wysłanych i otrzymanych pakietów sieciowych dla każdego protokołu sieciowego, takiego jak TCP, UDP, ICMP i inne.
- Liczbę błędów protokołów sieciowych, takich jak nieudane wysyłanie pakietów, błędy CRC i inne.
- Statystyki interfejsów sieciowych, takie jak liczba wysłanych i otrzymanych bajtów, liczba wysłanych i otrzymanych pakietów, liczba błędów interfejsów i inne.
- Inne szczegółowe informacje na temat wykorzystania protokołów sieciowych i interfejsów sieciowych.

Użycie tej opcji może pomóc w analizie wydajności sieci, identyfikacji problemów z protokołami sieciowymi lub interfejsami sieciowymi, a także w monitorowaniu aktywności sieciowej na dłuższą metę.

```

C:\Users\Chorus>netstat -s

IPv4 Statistics

Packets Received                = 3559630
Received Header Errors          = 0
Received Address Errors        = 51
Datagrams Forwarded             = 0
Unknown Protocols Received     = 43
Received Packets Discarded     = 151327
Received Packets Delivered     = 3593422
Output Requests                 = 2873743
Routing Discards                = 0
Discarded Output Packets       = 3990
Output Packet No Route         = 198
Reassembly Required            = 0
Reassembly Successful          = 0
Reassembly Failures            = 0
Datagrams Successfully Fragmented = 0
Datagrams Failing Fragmentation = 0
Fragments Created              = 0

IPv6 Statistics

Packets Received                = 5069
Received Header Errors          = 0
Received Address Errors        = 0
Datagrams Forwarded             = 0
Unknown Protocols Received     = 0
Received Packets Discarded     = 81
Received Packets Delivered     = 6765
Output Requests                 = 3275
Routing Discards                = 0
Discarded Output Packets       = 0
Output Packet No Route         = 0
Reassembly Required            = 0
Reassembly Successful          = 0
Reassembly Failures            = 0
Datagrams Successfully Fragmented = 0
Datagrams Failing Fragmentation = 0
Fragments Created              = 0

ICMPv4 Statistics

```

Komenda netstat odstęp wyświetla informacje o zmianach w połączeniach sieciowych co określony czas. Po użyciu tej komendy można zobaczyć:

- Aktualną listę aktywnych połączeń sieciowych wraz z adresami IP i numerami portów.
- Zmiany w aktywnych połączeniach sieciowych, takie jak nowe połączenia, zamknięcie połączeń lub zmiany stanów połączeń.
- Informacje o wykorzystaniu protokołów sieciowych i interfejsów sieciowych.
- Inne szczegółowe informacje o aktywności sieciowej.

Użycie tej opcji może pomóc w monitorowaniu aktywności sieciowej w czasie rzeczywistym i diagnozowaniu problemów z połączeniami sieciowymi. Można ustawić czas odstępu między aktualizacjami, co pozwala na śledzenie zmian w połączeniach sieciowych w sposób bardziej kontrolowany.