

Polecenie nslookup to narzędzie linii poleceń w systemach operacyjnych, służące do uzyskiwania informacji o rekordach DNS (Domain Name System). Za pomocą nslookup można sprawdzić, jaki adres IP jest przypisany do określonej nazwy domeny oraz odwrotnie - jakie nazwy domenowe odpowiadają podanemu adresowi IP. Narzędzie nslookup jest przydatne podczas diagnozowania problemów z połączeniem internetowym, w szczególności związanych z błędnymi wpisami DNS lub z nieprawidłową konfiguracją serwerów DNS. Po wprowadzeniu polecenia nslookup użytkownik może wpisać nazwę domeny lub adres IP, dla którego chce uzyskać informacje DNS, a następnie otrzyma odpowiedź od serwera DNS.

```
C:\Users\local>nslookup
DNS request timed out.
    timeout was 2 seconds.
Default Server:  UnKnown
Address:  213.184.8.5

> nslookup www.nss.et.put.poznan.pl
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Can't find address for server www.nss.et.put.poznan.pl: Timed out
> nslookup
Server:  UnKnown
Address:  213.184.8.5

DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Request to UnKnown timed-out
> nslookup http://centralops.net/
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
DNS request timed out.
    timeout was 2 seconds.
*** Can't find address for server http://centralops.net/: Timed out
>
```

Polecenie netstat to narzędzie linii poleceń w systemach operacyjnych, służące do wyświetlania informacji o połączeniach sieciowych (zarówno aktywnych, jak i oczekujących) oraz o portach sieciowych używanych przez aplikacje na danym komputerze. Dzięki netstat można monitorować aktywność sieciową i zidentyfikować procesy, które używają sieci w danym momencie. Netstat może wyświetlić informacje o

adresach IP i portach, z których pochodzą lub do których są kierowane połączenia sieciowe, a także o stanie tych połączeń (np. established, waiting, listening). Netstat jest przydatnym narzędziem do diagnostyki problemów z siecią oraz do zabezpieczenia sieci przed atakami typu DoS (Denial of Service), dzięki możliwości wykrycia nieautoryzowanych połączeń.

```
C:\Users\local>netstat
```

# Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:11300	view-localhost:50146	ESTABLISHED
TCP	127.0.0.1:50146	view-localhost:11300	ESTABLISHED
TCP	192.168.13.19:50127	testad:2222	ESTABLISHED
TCP	192.168.13.19:50128	um11:http	CLOSE_WAIT
TCP	192.168.13.19:50131	h3-epnsbroker01:8883	ESTABLISHED
TCP	192.168.13.19:50132	h3-epnsbroker01:8883	ESTABLISHED
TCP	192.168.13.19:50139	40.113.110.67:https	ESTABLISHED
TCP	192.168.13.19:50643	8:https	ESTABLISHED
TCP	192.168.13.19:51785	172.64.133.15:https	ESTABLISHED
TCP	192.168.13.19:51787	172.64.145.94:https	ESTABLISHED
TCP	192.168.13.19:51791	a104-81-116-7:https	ESTABLISHED
TCP	192.168.13.19:51792	a104-81-116-7:https	ESTABLISHED
TCP	192.168.13.19:51805	104.17.90.28:https	ESTABLISHED
TCP	192.168.13.19:51807	server-18-66-233-126:https	ESTABLISHED
TCP	192.168.13.19:51809	server-18-66-233-88:https	ESTABLISHED
TCP	192.168.13.19:51811	server-18-66-233-75:https	ESTABLISHED
TCP	192.168.13.19:51816	69.173.144.140:https	TIME_WAIT
TCP	192.168.13.19:51820	ec2-3-69-101-43:https	ESTABLISHED
TCP	192.168.13.19:51827	waw07s05-in-f1:https	ESTABLISHED
TCP	192.168.13.19:51831	37.157.5.142:https	ESTABLISHED
TCP	192.168.13.19:51836	104.18.11.47:https	ESTABLISHED
TCP	192.168.13.19:51839	ec2-3-71-149-231:https	ESTABLISHED
TCP	192.168.13.19:51840	a0f671730127a0812:https	ESTABLISHED
TCP	192.168.13.19:51843	ip21:https	TIME_WAIT
TCP	192.168.13.19:51852	198.148.27.133:https	ESTABLISHED
TCP	192.168.13.19:51854	213.19.162.31:https	TIME_WAIT
TCP	192.168.13.19:51855	960:https	TIME_WAIT
TCP	192.168.13.19:51864	185.170.60.47:https	TIME_WAIT
TCP	192.168.13.19:51866	ec2-52-209-191-165:https	ESTABLISHED
TCP	192.168.13.19:51870	37.157.2.249:https	TIME_WAIT
TCP	192.168.13.19:51881	ec2-54-85-216-131:https	ESTABLISHED
TCP	192.168.13.19:51884	ec2-54-85-216-131:https	TIME_WAIT
TCP	192.168.13.19:51885	ec2-54-185-138-62:https	ESTABLISHED
TCP	192.168.13.19:51886	ec2-54-185-138-62:https	TIME_WAIT
TCP	192.168.13.19:51887	124.146.215.51:https	CLOSE_WAIT
TCP	192.168.13.19:51888	124.146.215.51:https	ESTABLISHED
TCP	192.168.13.19:51889	124.146.215.51:https	TIME_WAIT
TCP	192.168.13.19:51890	server-108-138-47-59:http	ESTABLISHED
TCP	192.168.13.19:51891	server-108-138-47-59:http	ESTABLISHED
TCP	192.168.13.19:51892	104.18.20.226:http	ESTABLISHED
TCP	192.168.13.19:51893	ec2-3-121-39-140:https	ESTABLISHED
TCP	192.168.13.19:51894	ec2-3-121-39-140:https	TIME_WAIT
TCP	192.168.13.19:51896	69.173.144.165:https	TIME_WAIT
TCP	192.168.13.19:51898	193.0.160.131:https	ESTABLISHED
TCP	192.168.13.19:51899	s145:https	ESTABLISHED
TCP	192.168.13.19:51900	s145:https	TIME_WAIT
TCP	192.168.13.19:51901	s145:https	ESTABLISHED
TCP	192.168.13.19:51902	146.75.116.134:https	ESTABLISHED
TCP	192.168.13.19:51904	151.101.192.134:https	ESTABLISHED
TCP	192.168.13.19:51905	server-108-138-51-67:https	ESTABLISHED
TCP	192.168.13.19:51906	server-108-138-51-67:https	TIME_WAIT
TCP	192.168.13.19:51908	server-108-138-51-67:https	ESTABLISHED
TCP	192.168.13.19:51909	waw02s22-in-f2:https	ESTABLISHED
TCP	192.168.13.19:51910	146.75.116.134:https	ESTABLISHED
TCP	192.168.13.19:51912	xx-fbcdn-shv-01-waw1:https	ESTABLISHED
TCP	192.168.13.19:51918	xx-fbcdn-shv-01-waw1:https	ESTABLISHED
TCP	192.168.13.19:51920	xx-fbcdn-shv-01-waw1:https	TIME_WAIT
TCP	192.168.13.19:51921	xx-fbcdn-shv-01-waw1:https	TIME_WAIT

Polecenie "netstat -a" to jedna z opcji polecenia netstat w systemach operacyjnych.

Wykonanie tego polecenia w wierszu poleceń wyświetla listę wszystkich aktywnych połączeń sieciowych na komputerze, wraz z informacjami na temat adresów IP, portów, stanu połączenia oraz protokołów używanych przez te połączenia. Opcja "-a" oznacza "all" i powoduje, że netstat wyświetla informacje o wszystkich połączeniach sieciowych, zarówno aktywnych, jak i oczekujących na połączenie. Dzięki temu można dokładnie monitorować aktywność sieciową i zidentyfikować procesy, które używają sieci w danym momencie. Polecenie "netstat -a" jest przydatne w diagnostyce problemów z siecią oraz w zabezpieczaniu sieci przed atakami typu DoS (Denial of Service), dzięki możliwości wykrycia nieautoryzowanych połączeń.

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

Active Connections

 Proto Local Address           Foreign Address         State
TCP    0.0.0.0:135             DESKTOP-718DGH2:0      LISTENING
TCP    0.0.0.0:445             DESKTOP-718DGH2:0      LISTENING
TCP    0.0.0.0:902             DESKTOP-718DGH2:0      LISTENING
TCP    0.0.0.0:912             DESKTOP-718DGH2:0      LISTENING
TCP    0.0.0.0:5040            DESKTOP-718DGH2:0      LISTENING
TCP    0.0.0.0:11100           DESKTOP-718DGH2:0      LISTENING
TCP    0.0.0.0:49664           DESKTOP-718DGH2:0      LISTENING
TCP    0.0.0.0:49665           DESKTOP-718DGH2:0      LISTENING
TCP    0.0.0.0:49666           DESKTOP-718DGH2:0      LISTENING
TCP    0.0.0.0:49667           DESKTOP-718DGH2:0      LISTENING
TCP    0.0.0.0:49668           DESKTOP-718DGH2:0      LISTENING
TCP    0.0.0.0:49678           DESKTOP-718DGH2:0      LISTENING
TCP    127.0.0.1:11200         DESKTOP-718DGH2:0      LISTENING
TCP    127.0.0.1:11300         DESKTOP-718DGH2:0      LISTENING
TCP    127.0.0.1:11300         view-localhost:50146   ESTABLISHED
TCP    127.0.0.1:50146         view-localhost:11300   ESTABLISHED
TCP    127.0.0.1:50682         DESKTOP-718DGH2:0      LISTENING
TCP    169.254.159.126:139     DESKTOP-718DGH2:0      LISTENING
TCP    169.254.214.205:139     DESKTOP-718DGH2:0      LISTENING
TCP    192.168.13.19:139       DESKTOP-718DGH2:0      LISTENING
TCP    192.168.13.19:50127     testad:2222            ESTABLISHED
TCP    192.168.13.19:50128     um11:http              CLOSE_WAIT
TCP    192.168.13.19:50131     h3-epnsbroker01:8883   ESTABLISHED
TCP    192.168.13.19:50132     h3-epnsbroker01:8883   ESTABLISHED
TCP    192.168.13.19:50139     40.113.110.67:https     ESTABLISHED
TCP    192.168.13.19:50643     8:https                ESTABLISHED
TCP    192.168.13.19:51791     a104-81-116-7:https     ESTABLISHED
TCP    192.168.13.19:51792     a104-81-116-7:https     ESTABLISHED
TCP    192.168.13.19:51805     104.17.90.28:https      ESTABLISHED
TCP    192.168.13.19:51807     server-18-66-233-126:https ESTABLISHED
TCP    192.168.13.19:51809     server-18-66-233-88:https ESTABLISHED
TCP    192.168.13.19:51820     ec2-3-69-101-43:https   ESTABLISHED
TCP    192.168.13.19:51827     waw07s05-in-f1:https    ESTABLISHED
TCP    192.168.13.19:51836     104.18.11.47:https      ESTABLISHED
TCP    192.168.13.19:51840     a0f671730127a0812:https ESTABLISHED
TCP    192.168.13.19:51890     server-108-138-47-59:http TIME_WAIT
TCP    192.168.13.19:51891     server-108-138-47-59:http TIME_WAIT
TCP    192.168.13.19:51892     104.18.20.226:http      TIME_WAIT
TCP    192.168.13.19:51898     193.0.160.131:https     ESTABLISHED
TCP    192.168.13.19:51902     146.75.116.134:https    ESTABLISHED
TCP    192.168.13.19:51904     151.101.192.134:https    ESTABLISHED
TCP    192.168.13.19:51905     server-108-138-51-67:https ESTABLISHED
TCP    192.168.13.19:51908     server-108-138-51-67:https ESTABLISHED
TCP    192.168.13.19:51909     waw02s22-in-f2:https    ESTABLISHED
TCP    192.168.13.19:51910     146.75.116.134:https    ESTABLISHED
TCP    192.168.56.1:139       DESKTOP-718DGH2:0      LISTENING
TCP    [::]:135               DESKTOP-718DGH2:0      LISTENING
TCP    [::]:445               DESKTOP-718DGH2:0      LISTENING
TCP    [::]:11100             DESKTOP-718DGH2:0      LISTENING
TCP    [::]:49664             DESKTOP-718DGH2:0      LISTENING
TCP    [::]:49665             DESKTOP-718DGH2:0      LISTENING
TCP    [::]:49666             DESKTOP-718DGH2:0      LISTENING
TCP    [::]:49667             DESKTOP-718DGH2:0      LISTENING
TCP    [::]:49668             DESKTOP-718DGH2:0      LISTENING
TCP    [::]:49678             DESKTOP-718DGH2:0      LISTENING
```

Opcja "netstat-e" pozwala na wyświetlenie informacji o liczbie odebranych i wysłanych bajtów, pakietów oraz błędów dla każdego interfejsu sieciowego. Dzięki temu można

dokładnie monitorować wykorzystanie łącza sieciowego przez poszczególne procesy i zidentyfikować potencjalne problemy z przepustowością sieci. Polecenie "netstat -e" jest szczególnie przydatne dla administratorów sieci, którzy chcą kontrolować i optymalizować wykorzystanie łącz sieciowych w danym środowisku.

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

	Received	Sent
Bytes	1078767568	2486004276
Unicast packets	1093902	32327712
Non-unicast packets	29838	123218
Discards	0	0
Errors	0	0
Unknown protocols	0	0

Polecenie "netstat -n" to jedna z opcji polecenia netstat w systemach operacyjnych. Wykonanie tego polecenia w wierszu poleceń wyświetla listę aktywnych połączeń sieciowych na komputerze, ale w przeciwieństwie do opcji "-a", wyświetla adresy IP i numery portów w formie liczbowej, zamiast próbować przetłumaczyć je na nazwy domenowe i usługi. Opcja "-n" oznacza "numeric" i pozwala na wyświetlenie adresów IP i numerów portów w formie liczbowej, co może być przydatne w przypadku problemów z rozpoznawaniem nazw domenowych lub usług. Dzięki temu można dokładnie monitorować aktywność sieciową i zidentyfikować, które połączenia są nawiązane z jakimi adresami IP i numerami portów. Polecenie "netstat -n" jest przydatne w diagnostyce problemów z siecią oraz w zabezpieczaniu sieci przed atakami typu DoS (Denial of Service), dzięki możliwości wykrycia nieautoryzowanych połączeń i identyfikacji nieznanego adresu IP i numerów portów.

```
C:\Users\local>netstat -n

Active Connections

Proto Local Address          Foreign Address         State
TCP   127.0.0.1:11300         127.0.0.1:50146        ESTABLISHED
TCP   127.0.0.1:50146        127.0.0.1:11300        ESTABLISHED
TCP   192.168.13.19:50127    213.184.0.58:2222      ESTABLISHED
TCP   192.168.13.19:50128    91.228.166.88:80        CLOSE_WAIT
TCP   192.168.13.19:50131    91.228.167.171:8883     ESTABLISHED
TCP   192.168.13.19:50132    91.228.167.171:8883     ESTABLISHED
TCP   192.168.13.19:50139    40.113.110.67:443       ESTABLISHED
TCP   192.168.13.19:50643    35.244.159.8:443        ESTABLISHED
TCP   192.168.13.19:51820    3.69.101.43:443         ESTABLISHED
TCP   192.168.13.19:51827    142.250.186.193:443     TIME_WAIT
TCP   192.168.13.19:51840    13.248.245.213:443      TIME_WAIT
TCP   192.168.13.19:51898    193.0.160.131:443       ESTABLISHED
TCP   192.168.13.19:51902    146.75.116.134:443      ESTABLISHED
TCP   192.168.13.19:51904    151.101.192.134:443     ESTABLISHED
TCP   192.168.13.19:51909    142.250.203.194:443     TIME_WAIT
TCP   192.168.13.19:51910    146.75.116.134:443      ESTABLISHED
TCP   192.168.13.19:51944    213.19.162.51:443       TIME_WAIT
TCP   192.168.13.19:51945    37.157.6.233:443        ESTABLISHED
TCP   192.168.13.19:51948    37.157.2.248:443        TIME_WAIT
TCP   192.168.13.19:51949    37.157.6.233:443        TIME_WAIT
```

Polecenie "netstat -p" to jedna z opcji polecenia netstat w systemach operacyjnych. Wykonanie tego polecenia w wierszu poleceń wyświetla listę aktywnych połączeń sieciowych na komputerze, ale w przeciwieństwie do opcji "-a", "-n", itp., wyświetla również nazwy procesów, które są powiązane z danymi połączeniami. Opcja "-p" oznacza "process" i pozwala na wyświetlenie nazw procesów, które używają poszczególnych połączeń sieciowych. Dzięki temu można dokładnie monitorować aktywność sieciową i zidentyfikować, które procesy wykorzystują łącza sieciowe, co jest szczególnie przydatne w przypadku wykrywania nieautoryzowanych lub podejrzanych działań. Polecenie "netstat -p" jest szczególnie przydatne dla administratorów systemów, którzy chcą kontrolować i optymalizować wykorzystanie łącz sieciowych przez poszczególne procesy i zidentyfikować potencjalne problemy z wykorzystaniem



```
C:\Users\local>netstat -p TCP
```

#### Active Connections

Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:11300	view-localhost:50146	ESTABLISHED
TCP	127.0.0.1:50146	view-localhost:11300	ESTABLISHED
TCP	192.168.13.19:50127	testad:2222	ESTABLISHED
TCP	192.168.13.19:50128	um11:http	CLOSE_WAIT
TCP	192.168.13.19:50131	h3-epnsbroker01:8883	ESTABLISHED
TCP	192.168.13.19:50132	h3-epnsbroker01:8883	ESTABLISHED
TCP	192.168.13.19:50139	40.113.110.67:https	ESTABLISHED
TCP	192.168.13.19:50643	8:https	ESTABLISHED
TCP	192.168.13.19:52654	104.16.88.20:https	ESTABLISHED
TCP	192.168.13.19:52661	ip-185-184-8-90:https	ESTABLISHED
TCP	192.168.13.19:52667	104.18.3.114:https	ESTABLISHED
TCP	192.168.13.19:52668	185.64.189.112:https	ESTABLISHED
TCP	192.168.13.19:52684	a2-16-172-16:https	ESTABLISHED
TCP	192.168.13.19:52686	a104-81-116-210:https	ESTABLISHED
TCP	192.168.13.19:52689	69.173.144.139:https	ESTABLISHED
TCP	192.168.13.19:52706	69.173.144.138:https	ESTABLISHED
TCP	192.168.13.19:52715	a0f671730127a0812:https	ESTABLISHED
TCP	192.168.13.19:52722	a2-18-13-10:https	ESTABLISHED
TCP	192.168.13.19:52725	185.64.189.110:https	ESTABLISHED
TCP	192.168.13.19:52756	194:https	ESTABLISHED
TCP	192.168.13.19:52765	218:https	ESTABLISHED
TCP	192.168.13.19:52767	185.64.190.78:https	ESTABLISHED
TCP	192.168.13.19:52770	a2-16-172-27:https	ESTABLISHED
TCP	192.168.13.19:52778	52.46.128.147:https	ESTABLISHED
TCP	192.168.13.19:52827	104.16.204.22:https	ESTABLISHED
TCP	192.168.13.19:52829	server-108-138-51-74:https	ESTABLISHED
TCP	192.168.13.19:52834	104.16.123.175:https	ESTABLISHED
TCP	192.168.13.19:52836	21:https	ESTABLISHED
TCP	192.168.13.19:52838	192.229.221.95:http	TIME_WAIT
TCP	192.168.13.19:52839	server-108-138-51-94:https	ESTABLISHED
TCP	192.168.13.19:52841	server-108-138-51-94:https	ESTABLISHED
TCP	192.168.13.19:52842	a104-81-112-127:https	TIME_WAIT
TCP	192.168.13.19:52844	server-108-138-51-34:https	ESTABLISHED
TCP	192.168.13.19:52849	a23-45-136-198:https	ESTABLISHED
TCP	192.168.13.19:52850	server-52-84-195-16:https	ESTABLISHED
TCP	192.168.13.19:52856	server-18-66-233-5:https	ESTABLISHED
TCP	192.168.13.19:52862	server-108-138-47-59:http	TIME_WAIT
TCP	192.168.13.19:52867	146.75.117.230:https	ESTABLISHED
TCP	192.168.13.19:52869	a92-123-189-10:http	TIME_WAIT
TCP	192.168.13.19:52870	a92-123-189-10:http	TIME_WAIT
TCP	192.168.13.19:52871	236:https	ESTABLISHED
TCP	192.168.13.19:52873	waw07s03-in-f3:http	TIME_WAIT
TCP	192.168.13.19:52874	82:https	ESTABLISHED
TCP	192.168.13.19:52877	ec2-34-237-184-165:http	TIME_WAIT
TCP	192.168.13.19:52883	um15:http	TIME_WAIT
TCP	192.168.13.19:52891	204.79.197.239:https	ESTABLISHED
TCP	192.168.13.19:52895	bingforbusiness:https	ESTABLISHED
TCP	192.168.13.19:52899	vip0x008:http	ESTABLISHED
TCP	192.168.13.19:52900	13.107.21.239:https	ESTABLISHED
TCP	192.168.13.19:52901	vip0x008:http	ESTABLISHED
TCP	192.168.13.19:52902	a-0001:https	ESTABLISHED
TCP	192.168.13.19:52906	52.113.196.254:https	ESTABLISHED
TCP	192.168.13.19:52907	52.98.229.114:https	ESTABLISHED
TCP	192.168.13.19:52908	192.229.221.95:http	ESTABLISHED
TCP	192.168.13.19:52909	13.107.6.254:https	ESTABLISHED
TCP	192.168.13.19:52910	204.79.197.222:https	ESTABLISHED

zasobów.

Polecenie "netstat -r" to jedna z opcji polecenia netstat w

systemach operacyjnych. Wykonanie tego polecenia w wierszu poleceń wyświetla tablicę routingu IP, która zawiera informacje o sieciach, do których można dotrzeć bezpośrednio i pośrednio, a także o bramach domyślnych. Opcja "-r" oznacza "routing" i pozwala na wyświetlenie informacji o trasowaniu pakietów w sieci. Dzięki temu można dokładnie monitorować, jakie trasy są używane do przesyłania danych i jakie sieci są dostępne dla danego komputera. Polecenie "netstat -r" jest szczególnie przydatne dla administratorów sieci, którzy chcą kontrolować i optymalizować wykorzystanie sieci, a także diagnozować problemy z połączeniem. Na podstawie tablicy routingu IP można np. wykryć, które sieci są niedostępne lub jakie bramy domyślne są używane, co ułatwia rozwiązywanie problemów z siecią.



```
C:\Users\local>netstat -r
```

```
=====
Interface List
```

```
19...0a 00 27 00 00 13 .....VirtualBox Host-Only Ethernet Adapter
13...bc ae c5 cd 83 50 .....Realtek PCIe GbE Family Controller
15...00 50 56 c0 00 01 .....VMware Virtual Ethernet Adapter for VMnet1
9...00 50 56 c0 00 08 .....VMware Virtual Ethernet Adapter for VMnet8
4...00 40 95 30 f4 57 .....Realtek RTL8139/810x Family Fast Ethernet NIC
1.....Software Loopback Interface 1
=====
```

```
IPv4 Route Table
```

```
=====
Active Routes:
```

Network	Destination	Netmask	Gateway	Interface	Metric
	0.0.0.0	0.0.0.0	192.168.13.1	192.168.13.19	25
	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	255.255.255.255	On-link	127.0.0.1	331
	169.254.0.0	255.255.0.0	On-link	169.254.159.126	291
	169.254.0.0	255.255.0.0	On-link	169.254.214.205	291
169.254.159.126	255.255.255.255	255.255.255.255	On-link	169.254.159.126	291
169.254.214.205	255.255.255.255	255.255.255.255	On-link	169.254.214.205	291
169.254.255.255	255.255.255.255	255.255.255.255	On-link	169.254.159.126	291
169.254.255.255	255.255.255.255	255.255.255.255	On-link	169.254.214.205	291
	192.168.13.0	255.255.255.0	On-link	192.168.13.19	281
	192.168.13.19	255.255.255.255	On-link	192.168.13.19	281
	192.168.13.255	255.255.255.255	On-link	192.168.13.19	281
	192.168.56.0	255.255.255.0	On-link	192.168.56.1	281
	192.168.56.1	255.255.255.255	On-link	192.168.56.1	281
192.168.56.255	255.255.255.255	255.255.255.255	On-link	192.168.56.1	281
	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	192.168.56.1	281
	224.0.0.0	240.0.0.0	On-link	192.168.13.19	281
	224.0.0.0	240.0.0.0	On-link	169.254.214.205	291
	224.0.0.0	240.0.0.0	On-link	169.254.159.126	291
255.255.255.255	255.255.255.255	255.255.255.255	On-link	127.0.0.1	331
255.255.255.255	255.255.255.255	255.255.255.255	On-link	192.168.56.1	281
255.255.255.255	255.255.255.255	255.255.255.255	On-link	192.168.13.19	281
255.255.255.255	255.255.255.255	255.255.255.255	On-link	169.254.214.205	291
255.255.255.255	255.255.255.255	255.255.255.255	On-link	169.254.159.126	291

```
=====
Persistent Routes:
```

```
None
```

```
IPv6 Route Table
```

```
=====
Active Routes:
```

If	Metric	Network	Destination	Gateway
1	331	:::1/128		On-link
19	281	fe80::/64		On-link
13	281	fe80::/64		On-link
9	291	fe80::/64		On-link
15	291	fe80::/64		On-link
9	291	fe80::7e4d:7386:5dc4:ac0/128		On-link
19	281	fe80::8885:c812:f884:6259/128		On-link
13	281	fe80::c919:3e59:b9fe:116/128		On-link
15	291	fe80::d1c7:c291:8bc0:1a43/128		On-link
1	331	ff00::/8		On-link
19	281	ff00::/8		On-link
13	281	ff00::/8		On-link
9	291	ff00::/8		On-link
15	291	ff00::/8		On-link

Polecenie "netstat -s" to jedna z opcji polecenia netstat w systemach operacyjnych. Wykonanie tego polecenia w wierszu poleceń wyświetla statystyki sieciowe dotyczące różnych protokołów, takich jak TCP, UDP, IP, ICMP i inne. Opcja "-s" oznacza "statistics" i pozwala na uzyskanie szczegółowych informacji dotyczących wykorzystania sieci przez poszczególne protokoły. Dzięki temu można dokładnie monitorować aktywność sieciową i zidentyfikować, które protokoły są najczęściej używane oraz czy występują jakieś nieprawidłowości lub problemy z wykorzystaniem sieci. Polecenie "netstat -s" jest przydatne w diagnozowaniu problemów z siecią oraz w zabezpieczaniu sieci przed atakami typu DoS (Denial of Service), dzięki możliwości wykrycia nieautoryzowanych połączeń i identyfikacji nieznanych adresów IP i numerów portów. Ponadto, uzyskane statystyki mogą pomóc w optymalizacji wykorzystania łącz sieciowych i zapobieganiu przeciążeniom.

```
C:\Users\local>netstat -s
```

#### IPv4 Statistics

Packets Received	= 10263982
Received Header Errors	= 0
Received Address Errors	= 3699890
Datagrams Forwarded	= 0
Unknown Protocols Received	= 0
Received Packets Discarded	= 108191
Received Packets Delivered	= 6614034
Output Requests	= 4111211
Routing Discards	= 0
Discarded Output Packets	= 8014
Output Packet No Route	= 1250
Reassembly Required	= 0
Reassembly Successful	= 0
Reassembly Failures	= 0
Datagrams Successfully Fragmented	= 0
Datagrams Failing Fragmentation	= 0
Fragments Created	= 0

#### IPv6 Statistics

Packets Received	= 97489
Received Header Errors	= 0
Received Address Errors	= 19049
Datagrams Forwarded	= 0
Unknown Protocols Received	= 0
Received Packets Discarded	= 19370
Received Packets Delivered	= 81018
Output Requests	= 17146
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

	Received	Sent
Messages	9837	2598
Errors	0	0
Destination Unreachable	9828	2565
Time Exceeded	0	0
Parameter Problems	0	0
Source Quenches	0	0
Redirects	0	0
Echo Replies	4	0
Echos	5	33
Timestamps	0	0
Timestamp Replies	0	0
Address Masks	0	0
Address Mask Replies	0	0
Router Solicitations	0	0
Router Advertisements	0	0

#### ICMPv6 Statistics

	Received	Sent
Messages	247	396
Errors	0	0
Destination Unreachable	0	0
Packet Too Big	0	0
Time Exceeded	0	0
Parameter Problems	0	0
Echos	0	0
Echo Replies	0	0
MLD Queries	0	0
MLD Reports	0	0
MLD Dones	0	0
Router Solicitations	0	237
Router Advertisements	0	0
Neighbor Solicitations	0	81
Neighbor Advertisements	247	78
Redirects	0	0
Router Renumberings	0	0

#### TCP Statistics for IPv4

Active Opens	= 26544
Passive Opens	= 686
Failed Connection Attempts	= 7232
Reset Connections	= 4847
Current Connections	= 9
Segments Received	= 5212783
Segments Sent	= 4159392
Segments Retransmitted	= 15371

#### TCP Statistics for IPv6

Active Opens	= 78
Passive Opens	= 20
Failed Connection Attempts	= 458
Reset Connections	= 40
Current Connections	= 0
Segments Received	= 5440
Segments Sent	= 5324
Segments Retransmitted	= 116

#### UDP Statistics for IPv4

Datagrams Received	= 1809547
No Ports	= 14576
Receive Errors	= 90143
Datagrams Sent	= 463204

#### UDP Statistics for IPv6

Datagrams Received	= 126670
No Ports	= 4407
Receive Errors	= 14963
Datagrams Sent	= 10812

Polecenie `odstep/Interval`

Polecenie "arp -a" to polecenie wykonywane w wierszu poleceń w systemach operacyjnych, które pozwala na wyświetlenie tablicy ARP (Address Resolution Protocol) zawierającej informacje o przyporządkowaniu adresów fizycznych (MAC) do adresów IP w sieci lokalnej. Opcja "-a" oznacza "all" i powoduje wyświetlenie wszystkich wpisów w tablicy ARP. Wykonanie polecenia "arp -a" pozwala na uzyskanie informacji na temat urządzeń sieciowych znajdujących się w sieci lokalnej i przyporządkowanych im adresów MAC oraz IP. Dzięki temu można np. sprawdzić, czy urządzenia są poprawnie skonfigurowane, czy nie występują konflikty adresów IP, czy nie ma nieznanymi urządzeń w sieci, itp. Polecenie "arp -a" jest przydatne dla administratorów sieci, którzy chcą kontrolować i monitorować wykorzystanie sieci przez poszczególne urządzenia, a także diagnozować problemy z siecią.

```
C:\Users\local>arp -a
```

```
Interface: 169.254.214.205 --- 0x9
```

Internet Address	Physical Address	Type
169.254.255.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

```
Interface: 192.168.13.19 --- 0xd
```

Internet Address	Physical Address	Type
192.168.13.1	fc-f9-38-a3-a1-4f	dynamic
192.168.13.13	bc-ae-c5-cd-89-e0	dynamic
192.168.13.137	98-28-a6-0e-1a-94	dynamic
192.168.13.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

```
Interface: 169.254.159.126 --- 0xf
```

Internet Address	Physical Address	Type
169.254.255.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

```
Interface: 192.168.56.1 --- 0x13
```

Internet Address	Physical Address	Type
192.168.56.255	ff-ff-ff-ff-ff-ff	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static