

Linux: Polecenia Sieciowe w Systemie Linux

Poniżej znajdziesz przegląd najważniejszych poleceń sieciowych z opisami ich zastosowania oraz przydatnymi parametrami.

ping

Sprawdzenie dostępności hosta - wysyła pakiety ICMP Echo Request do docelowego hosta i czeka na odpowiedź. Służy do testowania połączenia sieciowego i pomiaru czasu odpowiedzi.

Przydatne parametry:

- `-c` *liczba* - liczba pakietów do wysłania (Linux, macOS)
- `-W` *timeout* - czas oczekiwania na odpowiedź w milisekundach
- `-i` *interwał* - interwał między wysyłaniem pakietów w sekundach
- `-s` *rozmiar* - rozmiar pakietu danych (domyślnie 56 bajtów)

Przykład: `ping -c 4 -i 0.5 8.8.8.8`

ifconfig

Wyświetlenie konfiguracji interfejsów sieciowych - pokazuje szczegóły wszystkich aktywnych interfejsów sieciowych (IP, maska, MAC, statystyki). Na nowszych systemach zastępowane przez `ip`.

Przydatne parametry:

- `ifconfig nazwa_interfejsu` - informacje o konkretnym interfejsie
- `ifconfig -a` - wyświetla wszystkie interfejsy (aktywne i nieaktywne)
- `ifconfig nazwa_interfejsu up/down` - włączenie/wyłączenie interfejsu
- `ifconfig nazwa_interfejsu IP netmask MASKA` - ustawienie adresu IP

Przykład: `ifconfig eth0 192.168.1.100 netmask 255.255.255.0`

ip a (ip addr)

Nowoczesne wyświetlenie konfiguracji IP - zamiennik `ifconfig` oferujący bardziej szczegółowe

informacje o adresach IP, routach i interfejsach. Część pakietu iproute2.

Przydatne parametry:

- `ip address show nazwa_interfejsu` - informacje o konkretnym interfejsie
- `ip addr add IP/MASKA dev nazwa_interfejsu` - dodanie adresu IP
- `ip addr del IP/MASKA dev nazwa_interfejsu` - usunięcie adresu IP
- `ip link set nazwa_interfejsu up/down` - włączenie/wyłączenie interfejsu

Przykład: `ip addr add 192.168.1.50/24 dev eth0`

—

route

Wyświetlenie i zarządzanie tablicą routingu - pokazuje, w jaki sposób pakiety są kierowane do różnych sieci. Pozwala na dodawanie, usuwanie i modyfikowanie tras.

Przydatne parametry:

- `route -n` - wyświetlenie tablicy routingu w formacie numerycznym
- `route add default gw IP` - ustawienie bramy domyślnej
- `route add -net SIEĆ netmask MASKA gw IP` - dodanie trasy do sieci
- `route del -net SIEĆ netmask MASKA` - usunięcie trasy
- `route del default gw IP` - usunięcie bramy domyślnej

Przykład: `route add default gw 192.168.1.1`

—

ip route

Nowoczesne zarządzanie routinguem - nowszy zamiennik polecenia `route` z bardziej intuicyjną składnią, część pakietu iproute2.

Przydatne parametry:

- `ip route show` - wyświetlenie wszystkich tras
- `ip route add SIEĆ/MASKA via IP` - dodanie trasy
- `ip route del SIEĆ/MASKA via IP` - usunięcie trasy
- `ip route add default via IP dev INTERFEJS` - ustawienie bramy domyślnej
- `ip route get IP` - sprawdzenie, przez którą trasę przejdzie pakiet do adresu

Przykład: `ip route add 192.168.2.0/24 via 192.168.1.254`

arp

Wyświetlenie i zarządzanie tabelą ARP - mapuje adresy IP na adresy MAC (fizyczne) w sieci lokalnej. Arp Resolution Protocol służy do rozpoznawania adresów sprzętowych.

Przydatne parametry:

- `arp -a` - wyświetlenie całej tabeli ARP
- `arp -n` - wyświetlenie tabeli ARP w formacie numerycznym
- `arp -d IP` - usunięcie wpisu z tabeli ARP
- `arp -s IP MAC` - dodanie statycznego wpisu ARP
- `arp -i nazwa_interfejsu` - wyświetlenie ARP tylko dla konkretnego interfejsu

Przykład: `arp -a -n`

ip neigh

Nowoczesne zarządzanie tabelą sąsiadów (ARP) - nowszy zamiennik polecenia `arp` z bogatszymi możliwościami, część pakietu `iproute2`.

Przydatne parametry:

- `ip neigh show` - wyświetlenie tabeli sąsiadów
- `ip neigh add IP lladdr MAC dev INTERFEJS` - dodanie wpisu
- `ip neigh del IP dev INTERFEJS` - usunięcie wpisu
- `ip neigh flush all` - wyczyszczenie całej tabeli
- `ip neigh show dev nazwa_interfejsu` - wyświetlenie dla konkretnego interfejsu

Przykład: `ip neigh show dev eth0`

traceroute

Śledzenie ścieżki pakietów do celu - pokazuje każdy router (hop) na drodze od Twojego komputera do hosta docelowego, wraz z czasem odpowiedzi. Bardzo przydatne do diagnostyki problemów sieciowych.

Przydatne parametry:

- -m liczba_hopów - maksymalna liczba hopów (domyślnie 30)
- -w timeout - czas oczekiwania na odpowiedź w sekundach
- -q liczba - liczba pytań wysyłanych do każdego hopów (domyślnie 3)
- -n - wyświetlenie adresów IP bez rozwiązywania nazw DNS
- -p port - port docelowy (dla TCP traceroute)

Przykład: traceroute -m 15 -n 8.8.8.8

—

mtr

Interaktywne śledzenie tras z ciągłym monitoringiem - kombinacja ping i traceroute wyświetlająca statystyki w czasie rzeczywistym. Narzędzie do zaawansowanej diagnostyki sieci.

Przydatne parametry:

- -c liczba - liczba pakietów do wysłania (zakończ po wysłaniu)
- -r - raport nie-interaktywny
- -n - wyświetlanie tylko adresów IP
- -w - zwiększona szerokość kolumn
- -s rozmiar - rozmiar pakietu

Przykład: mtr -c 50 -n 8.8.8.8

—

netstat

Wyświetlenie statystyk sieciowych i aktywnych połączeń - pokazuje otwarte porty, aktywne połączenia, statystyki protokołów i routing. Może monitorować aktywność sieciową w czasie rzeczywistym.

Przydatne parametry:

- -tułn - wyświetlenie otwartych portów TCP/UDP w formacie numerycznym
- -a - wszystkie połączenia (zarówno nasłuchujące jak i nawiązane)
- -p - wyświetlenie procesu (PID) odpowiadającego za połączenie
- -s - statystyki dla każdego protokołu
- -r - tablica routingu (równoważne route -n)

Przykład: netstat -tułn

SS

Nowoczesny zamiennik netstat - szybsze wyświetlanie informacji o gniazdach sieciowych. Część pakietu iproute2, preferowana w nowszych dystrybucjach.

Przydatne parametry:

- -t^ulⁿ - otwarte porty TCP/UDP w formacie numerycznym
- -t^ap - wszystkie połączenia z informacją o procesach
- -s - statystyki sieciowe
- -i - informacje o interfejsach
- -l - tylko nasłuchujące gniazda

Przykład: ss -t^ulⁿ

dig

Zapytania DNS o rekordy domenowe - narzędzie do zaawansowanych zapytań DNS pozwalające na sprawdzenie rekordów A, AAAA, MX, NS i innych.

Przydatne parametry:

- dig domena - zapytanie o rekord A
- dig domena MX - zapytanie o serwery mailowe
- dig domena NS - zapytanie o serwery nazw
- +short - skrócony format odpowiedzi
- @serwer_DNS - zapytanie konkretnego serwera DNS

Przykład: dig example.com +short

nslookup

Prostsza wersja zapytań DNS - narzędzie do rozpoznawania nazw domen i odwrotnego rozpoznawania (IP na domenę). Bardziej przystępne niż dig.

Przydatne parametry:

- `nslookup domena` - rozpoznanie IP domeny
- `nslookup IP` - odwrotne rozpoznanie (IP na domenę)
- `nslookup domena @serwer_DNS` - zapytanie konkretnego serwera DNS
- Tryb interaktywny - wpisanie samego `nslookup` bez argumentów

Przykład: `nslookup google.com 8.8.8.8`

—

host

Rozpoznawanie nazw i adresów IP - proste narzędzie do sprawdzenia mapowania IP/domena. Bardziej minimalistyczne niż `dig` czy `nslookup`.

Przydatne parametry:

- `host domena` - rozpoznanie adresu IP
- `host IP` - odwrotne rozpoznanie domeny
- `host domena serwer_DNS` - zapytanie konkretnego serwera
- `-t typ` - zapytanie o konkretny typ rekordu (A, MX, NS itp.)

Przykład: `host google.com`

—

curl / wget

Pobieranie zawartości stron i plików przez HTTP/HTTPS - `curl` wyświetla odpowiedź, `wget` pobiera pliki na dysk. Narzędzia do testowania połączeń HTTP i pobierania danych.

Przydatne parametry (curl):

- `-I` - pobranie tylko nagłówków HTTP
- `-X metoda` - wybór metody HTTP (GET, POST, PUT)
- `-d dane` - wysłanie danych POST
- `-H „nagłówek”` - dodanie niestandardowego nagłówka
- `-o plik` - zapis odpowiedzi do pliku

Przykład: `curl -I https://example.com`

—

tcpdump

Przechwytywanie i analiza pakietów sieciowych - narzędzie do szczegółowej analizy ruchu sieciowego na poziomie pakietów. Wymaga uprawnień administratora.

Przydatne parametry:

- `-i` interfejs - przechwytywanie na konkretnym interfejsie
- `-n` - wyświetlenie adresów IP zamiast nazw
- `host IP` - filtrowanie pakietów konkretnego hosta
- `port PORT` - filtrowanie konkretnego portu
- `-w plik.pcap` - zapis pakietów do pliku

Przykład: `tcpdump -i eth0 -n host 8.8.8.8`

—

Szybka tabela referencyjna

Polecenie	Zastosowanie	Nowoczesny zamiennik
ping	Test dostępności hosta	-
ifconfig	Konfiguracja interfejsów	<code>ip a / ip link</code>
route	Zarządzanie routowaniem	<code>ip route</code>
arp	Tablica ARP/MAC	<code>ip neigh</code>
netstat	Statystyki sieciowe	<code>ss</code>
tracert	Śledzenie trasy pakietów	<code>mtr</code>
dig/nslookup	Zapytania DNS	-

—

Ten poradnik powinien dać Ci solidne podstawy do pracy z siecią w Linuksie. Pamiętaj, że większość z tych poleceń wymaga dostępu do Internetu lub sieci lokalnej, a niektóre (jak `tcpdump` czy modyfikacja konfiguracji) wymagają uprawnień `sudo`.