

Sieci i SSH w Linuksie

Bartosz M. Kojak

Białostocka Grupa Użytkowników Linuksa, Wydział Informatyki
Politechnika Białostocka

14 maja 2008 r.

Jak pewnie wszyscy wiedzą, ping służy do sprawdzania połączeń sieciowych. Ping korzysta z protokołu ICMP, opierając się na dwóch rodzajach wiadomości — 0 (echo reply) oraz 8 (echo request).

Jak pewnie wszyscy wiedzą, ping służy do sprawdzania połączeń sieciowych. Ping korzysta z protokołu ICMP, opierając się na dwóch rodzajach wiadomości — 0 (echo reply) oraz 8 (echo request). Jeśli dany host nie odpowiada na pinga, nie musi to znaczyć, że jest wyłączony — po prostu może blokować odpowiedzi na ping.

Przykładowe użycie pinga

Sieci i SSH
w Linuksie

Bartosz M.
Kojak

Podstawowe
polecenia

Ping

Przykładowe
użycie pinga

Ważniejsze
opcje pinga

Traceroute

Przykładowe
użycie
traceroute

Routing loop

Opcje
traceroute

Host

Przykład
użycia hosta

Opcje hosta

Dig

Przykład
użycia dig

Opcje dig

Whois

Przykład
użycia Whois

Ifconfig

Przykład
użycia ifconfig

SSH

Netstat

```
$ ping wp.pl
PING wp.pl (212.77.100.101) 56(84) bytes of data.
64 bytes from www.wp.pl (212.77.100.101): icmp_seq=1 ttl=121 time=13.4 ms
64 bytes from www.wp.pl (212.77.100.101): icmp_seq=2 ttl=121 time=13.4 ms
64 bytes from www.wp.pl (212.77.100.101): icmp_seq=3 ttl=121 time=13.2 ms
64 bytes from www.wp.pl (212.77.100.101): icmp_seq=4 ttl=121 time=13.6 ms

--- wp.pl ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3012ms
rtt min/avg/max/mdev = 13.248/13.446/13.646/0.141 ms
```

- **-i N** — ustawia interwał N sekund między zapytaniami
- **-s N** — rozmiar pakietu (przydatne przy testowaniu samodzielnie zrobionych kabli ;-))
- **-c N** — wysyła N pakietów (domyślnie jest to aż do ctrl-c)
- **-f** — tzw. flood ping (wymaga uprawnień roota)
- **-n** — adresy hostów nie będą tłumaczone

Traceroute służy do badania tras między dwoma hostami. Może pokazać, czy na jakimś styku są problemy oraz jaka mamy trasę do danego hosta. Czasami zamiast programu traceroute mamy tracepath o zbliżonym działaniu. Traceroute korzysta z protokołu ICMP oraz UDP.

Przykładowe użycie traceroute

Sieci i SSH
w Linuksie

Bartosz M.
Kojak

Podstawowe
polecenia

Ping

Przykładowe
użycie pinga

Ważniejsze
opcje pinga

Traceroute

Przykładowe
użycie

traceroute

Routing loop

Opcje

traceroute

Host

Przykład
użycia hosta

Opcje hosta

Dig

Przykład
użycia dig

Opcje dig

Whois

Przykład
użycia Whois

Ifconfig

Przykład
użycia ifconfig

SSH

Netstat

```
$ traceroute bgul.org
traceroute to bgul.org (212.33.90.248), 30 hops max, 40 byte packets
 1 85-10-197-129.clients.your-server.de (85.10.197.129) 0.534 ms 0.453 ms 0.640 ms
 2 hos-tr1.juniper1.rz6.hetzner.de (213.239.229.1) 0.577 ms 1.058 ms 0.559 ms
 3 * * *
 4 lambdanet-gw.hetzner.de (213.239.242.213) 1.185 ms 0.849 ms 0.708 ms
 5 VIE-5-pos200.at.lambdanet.net (217.71.105.82) 11.523 ms 11.539 ms 11.586 ms
 6 vix1.Wien1.ACO.net (193.203.0.1) 11.756 ms 11.757 ms 11.825 ms
 7 * z-ACOnet.poznan-gw1.10Gb.rtr.pionier.gov.pl (212.191.224.149) 27.545 ms 27.55
 8 z-poznan-gw1.bialystok.10Gb.rtr.pionier.gov.pl (212.191.224.38) 35.342 ms 35.23
 9 212.33.92.114 (212.33.92.114) 35.404 ms 35.486 ms 35.429 ms
10 65gw.35pb.biaman.pl (212.33.69.234) 35.476 ms 40.898 ms 35.346 ms
11 * * *
12 kwi.wi.pb.edu.pl (212.33.90.248) 35.591 ms 35.976 ms 36.105 ms
```

Routing loop

Sieci i SSH
w Linuksie

Bartosz M.
Kojak

Podstawowe
polecenia

Ping

Przykładowe
użycie pinga

Ważniejsze
opcje pinga

Traceroute

Przykładowe
użycie
traceroute

Routing loop

Opcje
traceroute

Host

Przykład
użycia hosta

Opcje hosta

Dig

Przykład
użycia diga

Opcje diga

Whois

Przykład
użycia Whois

Ifconfig

Przykład
użycia ifconfig

SSH

Netstat

```
...
19 35pb.65gw.biaman.pl (212.33.69.233) 9.209 ms 9.197 ms 9.187 ms
20 65gw.35pb.biaman.pl (212.33.69.234) 11.114 ms * 8.548 ms
21 35pb.65gw.biaman.pl (212.33.69.233) 7.917 ms 7.926 ms 7.918 ms
22 * * 65gw.35pb.biaman.pl (212.33.69.234) 11.150 ms
23 35pb.65gw.biaman.pl (212.33.69.233) 6.663 ms 8.135 ms 8.103 ms
24 65gw.35pb.biaman.pl (212.33.69.234) 10.472 ms 10.471 ms *
25 35pb.65gw.biaman.pl (212.33.69.233) 8.530 ms 12.398 ms 12.386 ms
...
```

- `-m N` — liczba hopów (domyślnie 30)
- `-n` — nie rozwiązuje adresów
- `-w N` — czas w sekundach na odpowiedź (domyślnie 3)
- `-p N` — port

Polecenie `host` służy do odpytywania serwerów DNS na temat adresów IP i revDNS. Używając innego niż nasz serwera DNS możemy sprawdzić, czy nasza domena już jest widoczna na danym serwerze.

Przykład użycia hosta

Sieci i SSH
w Linuksie

Bartosz M.
Kojak

Podstawowe
polecenia

Ping

Przykładowe
użycie pinga

Ważniejsze
opcje pinga

Traceroute

Przykładowe
użycie
traceroute

Routing loop

Opcje
traceroute

Host

Przykład
użycia hosta

Opcje hosta

Dig

Przykład
użycia diga

Opcje diga

Whois

Przykład
użycia Whois

Ifconfig

Przykład
użycia ifconfig

SSH

Netstat

```
$ host bgul.org dns.tpsa.pl
```

```
Using domain server:
```

```
Name: dns.tpsa.pl
```

```
Address: 194.204.159.1\#53
```

```
Aliases:
```

```
bgul.org has address 212.33.90.248
```

```
bgul.org mail is handled by 1 poczta.bgul.org.
```

- `adres adresdns` — sprawdzi, czy *adres* jest widoczny spod DNS-a *adresdns*
- `-l adres` — wypisze hosty należące do hosta *adres*
- `-t rekord` — wyświetla dany rekord DNS

Dig służy do odpytywania serwerów DNS.

Przykład użycia dig

Sieci i SSH
w Linuksie

Bartosz M.
Kojak

Podstawowe
polecenia

Ping
Przykładowe
użycie pinga

Ważniejsze
opcje pinga
Traceroute

Przykładowe
użycie
traceroute

Routing loop

Opcje
traceroute

Host
Przykład
użycia hosta

Opcje hosta

Dig

Przykład
użycia diga

Opcje diga

Whois

Przykład
użycia Whois

Ifconfig

Przykład
użycia ifconfig

SSH

Netstat

```
$ dig wp.pl
; <<>> DiG 9.4.1-P1 <<>> wp.pl
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18584
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 1

;; QUESTION SECTION:
;wp.pl.                IN      A

;; ANSWER SECTION:
wp.pl.                2439    IN      A      212.77.100.101

;; AUTHORITY SECTION:
wp.pl.                784     IN      NS      ns2.wp.pl.
wp.pl.                784     IN      NS      dns.task.gda.pl.
wp.pl.                784     IN      NS      ns1.wp.pl.

;; ADDITIONAL SECTION:
dns.task.gda.pl.     89282   IN      A      153.19.250.100

;; Query time: 2 msec
;; SERVER: 212.33.90.253\#53(212.33.90.253)
;; WHEN: Tue May 13 22:23:38 2008
;; MSG SIZE rcvd: 118
```

- `-t rekord adres albo rekord adres` — wyświetla dany rekord DNS dla danego adresu
- `-x IP` — coś jako *host IP*
- `@serwerdns adres` — wyświetla informację o *adres* używając innego serwera DNS

Whois służy do uzyskiwania informacji odnośnie zarejestrowanej domeny lub adresie IP.

Przykład użycia Whois

Sieci i SSH
w Linuksie

Bartosz M.
Kojak

Podstawowe
polecenia

Ping

Przykładowe
użycie pinga

Ważniejsze
opcje pinga

Traceroute

Przykładowe
użycie
traceroute

Routing loop

Opcje
traceroute

Host

Przykład
użycia hosta

Opcje hosta

Dig

Przykład
użycia diga

Opcje diga

Whois

**Przykład
użycia Whois**

Ifconfig

Przykład
użycia ifconfig

SSH

Netstat

```
$ whois bgul.org
$ whois 212.33.90.248
```

Ifconfig jest narzędziem do konfiguracji interfejsów sieciowych.

Przykład użycia ifconfig

Sieci i SSH
w Linuksie

Bartosz M.
Kojak

Podstawowe
polecenia

Ping

Przykładowe
użycie pinga

Ważniejsze
opcje pinga

Traceroute

Przykładowe
użycie
traceroute

Routing loop

Opcje
traceroute

Host

Przykład
użycia hosta

Opcje hosta

Dig

Przykład
użycia diga

Opcje diga

Whois

Przykład
użycia Whois

Ifconfig

Przykład
użycia ifconfig

SSH

Netstat

- `ifconfig eth0` — informacje o interfejsie eth0
- `ifconfig eth0 hw ether 00:69:66:FF:34:45` — zmienia adres MAC dla eth0
- `ifconfig eth0 ADRES netmask MASKA broadcast BROADCAST`

- `ssh user@host -L 666:www.wp.pl:80` — po wpisaniu `localhost:666` będzie widoczna strona `wp.pl`

- `ssh user@host -L 666:www.wp.pl:80` — po wpisaniu `localhost:666` będzie widoczna strona `wp.pl`
- `ssh user@host -D 666` — tworzy serwer SOCKS na porcie 666, możemy potem w przeglądarkach użyć tego jako proxy

- `-a` — wszystkie aktywne połączenia
- `-s` — statystyki
- `-p` protokół — połączenia dla danego protokołu

- `port 80` — pokazuje tylko połączenia na danym porcie
- `host wp.pl` — pokazuje tylko połączenia z hostem
- `-i eth0` — wybiera interfejs
- `-n` — nie konwertuje adresów

- Wireshark — sniffer
- IPtraf — ukazuje połączenia
- Nmap — skaner portów
- hping — skaner, generator pakietów i wiele, wiele innych

Prezentacja wykonana przy użyciu pakietu Beamer z systemu \LaTeX .
Prezentacja dostępna na licencji Creative Commons z uznaniem autorstwa
(<http://creativecommons.org/licenses/by/2.5/pl/>).