

Translacja adresów sieciowych - NAT

Network Address Translation - NAT odnosi się do konkretnego procesu, który polega na zamianie pojedynczego adresu IP na inny, często publiczny adres IP, poprzez zmianę informacji o sieci i informacji adresowych, które znajdują się w nagłówku pakietu danych IP. Sieci lokalne posiadają prywatne adresy IP, które odnoszą się do konkretnych urządzeń w sieci. Poprzez system NAT te prywatne adresy są tłumaczone na publiczny adres IP, gdy wychodzące żądania z urządzeń sieciowych są przesyłane do Internetu. Proces odwrotny ma miejsce, gdy przychodzące dane, zwykle w odpowiedzi na konkretne żądania, są wysyłane do sieci lokalnej. W tym przypadku NAT zmienia publiczny adres IP na prywatny adres IP określonego urządzenia, do którego skierowany jest pakiet danych. Publiczny adres IP jest wielokrotnie używany przez router łączący komputery z Internetem.

Funkcjonalność

Proces ten został pierwotnie wprowadzony w życie jako metoda przekierowywania pakietów podczas transferu poszczególnych sieci hostów. Obecnie jest on postrzegany jako globalne rozwiązanie problemu braku dostępnych adresów IPv4. Pracuje w celu optymalizacji wykorzystania dostępnych adresów IP poprzez umożliwienie dostępu do wielu urządzeń za pomocą jednego publicznego adresu IP. Prywatny adres IP jest następnie używany do przekierowywania pakietów danych w sieci lokalnej.

Innymi słowy, NAT umożliwia specyficznemu urządzeniu, takiemu jak router, jak również innym urządzeniom, działanie jako moderator pomiędzy siecią publiczną, taką jak Internet, a siecią lokalną lub prywatną, taką jak sieć domowa lub biurowa. Pozwala to na to, aby pojedynczy adres IP, który jest unikalny na skalę światową, reprezentował całą sieć prywatną, w tym wszystkie podłączone w jej obrębie urządzenia.

System ten został wykorzystany do rozwiązywania problemów, które pojawiły się w związku z rosnącą popularnością i wykorzystaniem Internetu. Przede wszystkim dostępne adresy IP nie były w stanie zaspokoić zapotrzebowania na połączenie na całym świecie, ponieważ coraz więcej osób zaczęło korzystać z Internetu. Chociaż pierwotnie opracowane jako rozwiązanie tymczasowe, NAT jest szeroko stosowane i stosowane przez wszystkich dostawców sieci, producentów sprzętu i firm technologicznych.

Rodzaje

Istnieją 4 rodzaje NAT, które mogą być używane do rozwiązywania różnych rodzajów sytuacji i scenariuszy. Poniżej znajduje się opis i próbki do wglądu:

Przeciążenie lub tłumaczenie adresu portu (PAT)

Tłumaczenie adresów portów jest jednym z najczęściej używanych systemów NAT. Wiele połączeń z różnych wewnętrznych hostów jest multipleksowanych w celu utworzenia jednego publicznego adresu IP, który wykorzystuje różne numery portów źródłowych. Maksymalnie

65 536 połączeń wewnętrznych można przetłumaczyć na jeden publiczny adres IP. Sprawia to, że jest on bardzo skuteczny w sytuacjach, gdy dostawca usług przydzielił tylko jeden publiczny adres IP.

Dynamiczne NAT

Dynamiczny NAT opiera się na puli różnych publicznych adresów IP, które są wykorzystywane w określonych sieciach prywatnych. Są one przypisywane przez lokalnego dostawcę usług internetowych. Dla tego typu NAT, każdy wewnętrzny host, który chce uzyskać dostęp do Internetu, będzie miał swój prywatny adres IP przetłumaczony przez router NAT na pierwsze dostępne publiczne IP w publicznej puli.

Statyczny NAT

Statyczny NAT zapewnia stałe mapowanie publicznego adresu IP na prywatny adres IP utworzony przez prywatny router sieciowy. Ten typ NAT jest najbardziej odpowiedni dla hostów, które muszą być dostępne poza siecią. Jest to najbardziej odpowiednie do zapewnienia dostępu do serwerów takich jak serwery poczty elektronicznej i serwery internetowe.

Przekierowanie portu

Ten typ NAT umożliwia na dostęp z pojedynczego publicznego adres IP, do jednego lub kilku różnych serwerów –hostów w sieci prywatnej.

Skutki

Chociaż NAT jest uważany za użyteczny w wielu scenariuszach, ma swoje ograniczenia i wady w niektórych przypadkach. Niektóre z poniższych zalet i wad są wymienione poniżej:

Zalety

- Pomaga to w ograniczeniu wyczerpywania się globalnej przestrzeni publicznych adresów IP.
- Sieci mogą teraz korzystać z prywatnej przestrzeni adresowej RFC 1918 wewnętrznie, mając jednocześnie dostęp do Internetu.
- Zwiększa poziom bezpieczeństwa poprzez ukrywanie schematu adresowania i wewnętrznej topologii sieci.

Wady

- Protokoły tunelowania stają się skomplikowane, ponieważ NAT zmienia wartości w nagłówkach pakietów, co będzie miało wpływ na kontrolę integralności tych protokołów.
- Ponieważ adresy wewnętrzne są ukryte za jednym publicznie dostępnym adresem, niemożliwe byłoby zainicjowanie przez zewnętrznego hosta komunikacji z hostem

wewnętrznym bez specjalnej konfiguracji na zaporze ogniowej, aby to umożliwić trzeba skonfigurować przekierowanie portów.

- Aplikacje wykorzystujące Voice over IP (VoIP), wideokonferencje i inne funkcje peer-to-peer muszą wykorzystywać techniki NAT traversal, aby mogły one funkcjonować.

Przez cały czas technika NAT tworzyła różne pochodne i innowacje od momentu jej pierwszej ewolucji. Oferuje podwójne funkcje ochrony adresów i bezpieczeństwa, które są zazwyczaj wdrażane w środowiskach zdalnego dostępu.

Tłumaczenie adresów sieciowych jest bardzo ważnym aspektem bezpieczeństwa firewalla. Ogranicza to liczbę adresów publicznych wykorzystywanych w organizacji, co pozwala na ściślejszą kontrolę dostępu do zasobów po obu stronach firewalla.

Oprogramowanie

W przypadku systemu operacyjnego GNU/Linux funkcje NAT definiowane są za pomocą programów iptables lub ipchains (wcześniejsza wersja obecnie nie używana).

Konfiguracja routingu z usługą NAT na Ubuntu Server 20.04.

Przed przystąpieniem do konfiguracji usługi, powinniśmy sprawdzić:

- konfigurację kart sieciowych serwera
- komunikację serwera z Internetem
- konfigurację kart sieciowych klienta (desktop)
- komunikację klienta (desktop) z serwerem i Internetem

```

us3n00@ks23-3n00: ~
us3n00@ks23-3n00:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: WAN: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:52:84:c4 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic WAN
        valid_lft 85834sec preferred_lft 85834sec
    inet6 fe80::a00:27ff:fe52:84c4/64 scope link
        valid_lft forever preferred_lft forever
3: LAN: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:52:53:74 brd ff:ff:ff:ff:ff:ff
    inet 172.22.0.1/24 brd 172.22.0.255 scope global LAN
        valid_lft forever preferred_lft forever
    inet 172.22.0.2/24 brd 172.22.0.255 scope global secondary LAN
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe52:5374/64 scope link
        valid_lft forever preferred_lft forever
us3n00@ks23-3n00:~$

```

Dostęp do Internetu z serwera sprawdzamy pingując dowolną istniejącą w Internecie witrynę

```

us3n00@ks23-3n00: ~
us3n00@ks23-3n00:~$ ping ubuntu.com -c3
PING ubuntu.com (91.189.88.181) 56(84) bytes of data.
64 bytes from davybones.canonical.com (91.189.88.181): icmp_seq=1 ttl=54 time=62.9 ms
64 bytes from davybones.canonical.com (91.189.88.181): icmp_seq=2 ttl=54 time=60.7 ms
64 bytes from davybones.canonical.com (91.189.88.181): icmp_seq=3 ttl=54 time=62.4 ms

--- ubuntu.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 60.693/61.999/62.931/0.951 ms
us3n00@ks23-3n00:~$

```

```

ud3n00@k1d23-3n00: ~
ud3n00@k1d23-3n00:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:1c:82:d3 brd ff:ff:ff:ff:ff:ff
    inet 172.22.0.99/24 brd 172.22.0.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::52b9:4bb4:9b68:e064/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
ud3n00@k1d23-3n00:~$

```

```

ud3n00@k1d23-3n00: ~
ud3n00@k1d23-3n00:~$ ping 172.22.0.1 -c3
PING 172.22.0.1 (172.22.0.1) 56(84) bytes of data.
64 bytes from 172.22.0.1: icmp_seq=1 ttl=64 time=0.631 ms
64 bytes from 172.22.0.1: icmp_seq=2 ttl=64 time=0.514 ms
64 bytes from 172.22.0.1: icmp_seq=3 ttl=64 time=0.536 ms

--- 172.22.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2030ms
rtt min/avg/max/mdev = 0.514/0.560/0.631/0.050 ms
ud3n00@k1d23-3n00:~$

```

```

ud3n00@k1d23-3n00: ~
ud3n00@k1d23-3n00:~$ ping ubuntu.com -c3
ping: ubuntu.com: Odwzorowanie nazwy jest chwilowo niemożliwe
ud3n00@k1d23-3n00:~$

```

Jak widać powyżej, połączenie klienta z serwerem jest, ale klient nie ma dostępu do Internetu.

Na wszelki wypadek, sprawdzamy czy na desktopie jest skonfigurowana brama i DNS. Jeżeli nie konfigurujemy oba parametry.

Anuluj
Przewodowe
Zastosuj

Informacje
Tożsamość
IPv4
IPv6
Zabezpieczenia

Prędkość połączenia 1000 Mb/s
Adres IPv4 172.22.0.99
Adres IPv6 fe80::52b9:4bb4:9b68:e064
Adres sprzętowy 08:00:27:1C:82:D3
Domyślna trasa 172.22.0.1
DNS 8.8.8.8

☒ Łączenie automatyczne
☒ Dostępna dla innych użytkowników
☐ Mierzone połączenie: ma ograniczenia danych lub wiąże się z opłatami
Aktualizacje oprogramowania i inne duże pobierania nie będą rozpoczynane automatycznie.

Usun profil połączenia

Będzie to możliwe, gdy na serwerze, skonfigurujemy routing z usługą NAT.

Aby to zrobić należy na serwerze:

1. Zainstalować pakiet iptables-persistent

```
sudo apt install iptables-persistent -y
```

us3n00@ks23-3n00: ~

Konfiguracja pakietu

Konfiguracja pakietu iptables-persistent

Bieżące reguły iptables mogą zostać zachowane do pliku konfiguracyjnego /etc/iptables/rules.v4. Będą one wówczas ładowane automatycznie podczas uruchamiania systemu.

Reguły są zachowywane automatycznie jedynie podczas instalacji pakietu. Proszę zapoznać się ze stroną podręcznika iptables-save(8), aby dowiedzieć się jak zachowywać plik reguł w stanie zaktualizowanym.

Zachować bieżące reguły IPv4?

<Tak>
<Nie>

Zachowujemy bieżące reguły IPv4

```

us3n00@ks23-3n00: ~
Konfigurowanie pakietu iptables-persistent (1.0.14ubuntu1) ...
update-alternatives: użycie /lib/systemd/system/netfilter-persistent.service jako dostarczającego /
lib/systemd/system/iptables.service (iptables.service) w trybie automatycznym
Przetwarzanie wyzwalaczy pakietu man-db (2.9.1-1)...
Przetwarzanie wyzwalaczy pakietu systemd (245.4-4ubuntu3.15)...
us3n00@ks23-3n00:~$

```

2. Włączyć przekazywanie pakietów IPv4

Aby, na serwerze, włączyć przekazywanie pakietów IPv4, należy w pliku:

/etc/sysctl.conf

odznaczyć ("odhaszować") wpis

#net.ipv4.ip_forward = 1.

```

Otwórz ▼ [ikona] sysctl.conf [Tylko do odczytu] Zapisz [ikona] - □ ×
/etc
23 # See http://lwn.net/Articles/277146/
24 # Note: This may impact IPv6 TCP sessions too
25 #net.ipv4.tcp_syncookies=1
26
27 # Uncomment the next line to enable packet forwarding for IPv4
28 net.ipv4.ip_forward=1
29
30 # Uncomment the next line to enable packet forwarding for IPv6
Zwykły tekst Szerokość tabulacji: 8 Wrsz 28, kol 1 WST

```

Wykorzystując np. edytor nano (**sudo nano /etc/sysctl.conf**)

Po restarcie systemu, spowoduje to zmianę wartości z 0 na 1, w pliku

/proc/sys/net/ipv4/ip_forward.

Aby zastosować zmiany natychmiast wydajemy polecenie: **sudo sysctl -p**

Możemy również sprawdzić aktualną wartość parametru poleceniem:

sysctl net.ipv4.ip_forward

```

us3n00@ks23-3n00: ~
us3n00@ks23-3n00:~$ sudo sysctl -p
net.ipv4.ip_forward = 1
us3n00@ks23-3n00:~$ sysctl net.ipv4.ip_forward
net.ipv4.ip_forward = 1
us3n00@ks23-3n00:~$

```

3. Dokonać korekty w zaporze, skonfigurować maskaradę

Wydajemy polecenie

sudo iptables -t nat -A POSTROUTING -o WAN -j MASQUERADE

gdzie **WAN** jest interfejsem serwera łączącym z Internetem.

Dostęp do Internetu już jest jednak, aby zachować wprowadzone zmiany na stałe należy wprowadzone reguły zapisać. Możemy to zrobić, jako Root.

Wydajemy polecenia:

```
sudo su
```

```
iptables-save > /etc/iptables/rules.v4
```

```
us3n00@ks23-3n00: ~  
us3n00@ks23-3n00:~$ sudo -s  
root@ks23-3n00:/home/us3n00# iptables-save > /etc/iptables/rules.v4  
root@ks23-3n00:/home/us3n00# exit  
exit  
us3n00@ks23-3n00:~$
```

Polecenie zapisu jest wykonane bezobjawowo. Zmiany widzimy w pliku /etc/iptables/rules.v4

```
rules.v4 [Tylko do odczytu]  
/etc/iptables  
Otwórz [v] Zapisz [v]  
sysctl.conf x rules.v4 x  
1 # Generated by iptables-save v1.8.4 on Tue Feb  1 20:41:10 2022  
2 *nat  
3 :PREROUTING ACCEPT [14:1387]  
4 :INPUT ACCEPT [2:468]  
5 :OUTPUT ACCEPT [0:0]  
6 :POSTROUTING ACCEPT [0:0]  
7 -A POSTROUTING -o WAN -j MASQUERADE  
8 COMMIT  
9 # Completed on Tue Feb  1 20:41:10 2022  
10 # Generated by iptables-save v1.8.4 on Tue Feb  1 20:41:10 2022  
11 *filter  
12 :INPUT ACCEPT [713:944901]  
13 :FORWARD ACCEPT [535:42884]  
14 :OUTPUT ACCEPT [511:40118]  
15 COMMIT  
16 # Completed on Tue Feb  1 20:41:10 2022  
Zwykły tekst Szerokość tabulacji: 8 Wrsz 16, kol 40 WST
```

Jak widać routing działa poprawnie

```
ud3n00@k1d23-3n00: ~  
ud3n00@k1d23-3n00:~$ ping ubuntu.com -c3  
PING ubuntu.com (185.125.190.29) 56(84) bytes of data:  
64 bytes from website-content-cache-3.canonical.com (185.125.190.29): icmp_seq=1 ttl=53 time=60.2 ms  
64 bytes from website-content-cache-3.canonical.com (185.125.190.29): icmp_seq=2 ttl=53 time=66.6 ms  
64 bytes from website-content-cache-3.canonical.com (185.125.190.29): icmp_seq=3 ttl=53 time=62.9 ms  
--- ubuntu.com ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2004ms  
rtt min/avg/max/mdev = 60.176/63.220/66.590/2.628 ms  
ud3n00@k1d23-3n00:~$ ip r  
default via 172.22.0.1 dev enp0s3 proto static metric 100  
169.254.0.0/16 dev enp0s3 scope link metric 1000  
172.22.0.0/24 dev enp0s3 proto kernel scope link src 172.22.0.99 metric 100  
ud3n00@k1d23-3n00:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:1c:82:d3 brd ff:ff:ff:ff:ff:ff  
    inet 172.22.0.99/24 brd 172.22.0.255 scope global noprefixroute enp0s3  
        valid_lft forever preferred_lft forever  
    inet6 fe80::52b9:4bb4:9b68:e064/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
ud3n00@k1d23-3n00:~$
```

Jeżeli adres jest konfigurowany z DHCP, dopisujemy adres bramy w konfiguracji DHCP.

Modyfikujemy plik `/etc/dhcp/dhcpd.conf` dopisując linię:

```
option routers 172.22.y.1;
```

gdzie y to nr z dziennika

```
us3n00@ks23-3n00: ~
us3n00@ks23-3n00:~$ tail -n 7 /etc/dhcp/dhcpd.conf
subnet 172.22.0.0 netmask 255.255.255.0 {
    range 172.22.0.20 172.22.0.30;
    option routers 172.22.0.1;
    host k2d23-3n00{
        hardware Ethernet 08:00:27:7d:18:bb;
        fixed-address 172.22.0.19;}
}
```

Restartujemy serwer DHCP

```
us3n00@ks23-3n00:~$ sudo systemctl restart isc-dhcp-server
us3n00@ks23-3n00:~$ sudo systemctl status isc-dhcp-server
● isc-dhcp-server.service - ISC DHCP IPv4 server
   Loaded: loaded (/lib/systemd/system/isc-dhcp-server.service; enabled; vendor preset: ►
   Active: active (running) since Tue 2022-02-01 22:02:06 UTC; 3s ago
     Docs: man:dhcpd(8)
    Main PID: 4490 (dhcpd)
      Tasks: 4 (limit: 2268)
     Memory: 4.8M
    CGroup: /system.slice/isc-dhcp-server.service
            └─4490 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/dhcp-server/dhcpd.pid -c►

lut 01 22:02:06 ks23-3n00 dhcpd[4490]: Wrote 0 deleted host decls to leases file.
lut 01 22:02:06 ks23-3n00 dhcpd[4490]: Wrote 0 new dynamic host decls to leases file.
lut 01 22:02:06 ks23-3n00 dhcpd[4490]: Wrote 0 leases to leases file.
lut 01 22:02:06 ks23-3n00 dhcpd[4490]: Listening on LPF/LAN/08:00:27:52:53:74/172.22.0.0/24
lut 01 22:02:06 ks23-3n00 sh[4490]: Listening on LPF/LAN/08:00:27:52:53:74/172.22.0.0/24
lut 01 22:02:06 ks23-3n00 sh[4490]: Sending on LPF/LAN/08:00:27:52:53:74/172.22.0.0/24
lut 01 22:02:06 ks23-3n00 sh[4490]: Sending on Socket/fallback/fallback-net
lut 01 22:02:06 ks23-3n00 dhcpd[4490]: Sending on LPF/LAN/08:00:27:52:53:74/172.22.0.0/24
us3n00@ks23-3n00:~$
```

Konfigurujemy kartę sieciową na desktopie tak, aby adres był uzyskiwany z serwera DHCP. Restartujemy kartę sieciową na desktopie.

Anuluj

Przewodowe

Zastosuj

Informacje

Tożsamość

IPv4

IPv6

Zabezpieczenia

Metoda IPv4

☒ Automatycznie (DHCP)

☐ Tylko Link-Local

☐ Ręcznie

☐ Wyłączone

☐ Udostępniane innym komputerom

DNS

Automatycznie ☒

Należy oddzielić adresy IP przecinkami

Trasy

Automatycznie ☒

Adres

Maska sieci

Brama

Parametry

☐ Używanie tego połączenia tylko dla zasobów w jej sieci

Anuluj

Przewodowe

Zastosuj

Informacje

Tożsamość

IPv4

IPv6

Zabezpieczenia

Prędkość połączenia

1000 Mb/s

Adres IPv4

172.22.0.19

Adres IPv6

fe80::a7da:5e81:ac2a:8ae0

Adres sprzętowy

08:00:27:7D:18:BB

Domyślna trasa

172.22.0.1

DNS

☒ Łączenie automatyczne

☒ Dostępna dla innych użytkowników

☐ Mierzone połączenie: ma ograniczenia danych lub wiąże się z opłatami
Aktualizacje oprogramowania i inne duże pobierania nie będą rozpoczynane automatycznie.

Usuń profil połączenia

```

ud3n00@k2d23-3n00: ~
ud3n00@k2d23-3n00:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:7d:18:bb brd ff:ff:ff:ff:ff:ff
    inet 172.22.0.19/24 brd 172.22.0.255 scope global dynamic noprefixroute enp0s3
        valid_lft 413sec preferred_lft 413sec
    inet6 fe80::a7da:5e81:ac2a:8ae0/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
ud3n00@k2d23-3n00:~$ ip r
default via 172.22.0.1 dev enp0s3 proto dhcp metric 20100
169.254.0.0/16 dev enp0s3 scope link metric 1000
172.22.0.0/24 dev enp0s3 proto kernel scope link src 172.22.0.19 metric 100
ud3n00@k2d23-3n00:~$

```

Sprawdzamy działanie routingu po IP i po nazwie

```

ud3n00@k2d23-3n00: ~
ud3n00@k2d23-3n00:~$ ping 8.8.8.8 -c3
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data:
64 bytes from 8.8.8.8: icmp_seq=1 ttl=118 time=34.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=35.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=35.7 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 34.569/35.375/35.897/0.578 ms
ud3n00@k2d23-3n00:~$ ping ubuntu.com -c3
ping: ubuntu.com: Odwzorowanie nazwy jest chwilowo niemożliwe
ud3n00@k2d23-3n00:~$

```

I routing po IP działa poprawnie.

Jak widać ubuntu.com jest nieznany. Karta sieciowa na desktopie nie ma przypisanego adresu serwera DNS, który rozpozna nazwę i zwróci adres IP.

Jeżeli adres jest konfigurowany z DHCP, dopisujemy adres serwera DNS w konfiguracji DHCP.

Modyfikujemy plik `/etc/dhcp/dhcpd.conf` dopisując linię:

```
option domain-name-servers 8.8.8.8, 192.168.118.1;
```

Adres 192.168.118.1 jest adresem routera pracowni i jest potrzebny tylko w szkole ze względu na specyfikę sieci w szkole.

```
us-3n00@ks23-3n00: /  
us-3n00@ks23-3n00:/$ tail -n 8 /etc/dhcp/dhcpd.conf  
subnet 172.22.0.0 netmask 255.255.255.0 {  
    range 172.22.0.20 172.22.0.30;  
    option routers 172.22.0.1;  
    option domain-name-servers 8.8.8.8, 192.168.118.1;  
    host k2d23-3n00 {  
        hardware Ethernet 08:00:27:f0:c3:5f;  
        fixed-address 172.22.0.18;}  
}  
us-3n00@ks23-3n00:/$
```

Restartujemy serwer DHCP

Restartujemy kartę sieciową na desktopie.

Te zrzuty (do końca) umieszczamy w dokumentacji

Anuluj **Przewodowe** Zastosuj

Informacje Tożsamość IPv4 IPv6 Zabezpieczenia

Prędkość połączenia 1000 Mb/s

Adres IPv4 172.22.0.18

Adres IPv6 fe80::b6ed:392f:daea:3002

Adres sprzętowy 08:00:27:F0:C3:5F

Domyślna trasa 172.22.0.1

DNS 8.8.8.8 192.168.118.1

☒ Łączenie automatyczne

☒ Dostępna dla innych użytkowników

☐ Mierzone połączenie: ma ograniczenia danych lub wiąże się z opłatami
Aktualizacje oprogramowania i inne duże pobierania nie będą rozpoczynane automatycznie.

Usuń profil połączenia

```

ud-3n00@k2d23-3n00:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:f0:c3:5f brd ff:ff:ff:ff:ff:ff
    inet 172.22.0.18/24 brd 172.22.0.255 scope global dynamic noprefixroute enp0s3
        valid_lft 535sec preferred_lft 535sec
    inet6 fe80::b6ed:392f:daea:3002/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
ud-3n00@k2d23-3n00:~$ ping ubuntu.com -c3
PING ubuntu.com (185.125.190.29) 56(84) bytes of data.
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=1 ttl=49 time=48.0 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=2 ttl=49 time=52.2 ms
64 bytes from website-content-cache-3.ps5.canonical.com (185.125.190.29): icmp_seq=3 ttl=49 time=54.3 ms

--- ubuntu.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 48.000/51.501/54.264/2.609 ms
ud-3n00@k2d23-3n00:~$

```

Jak widać wszystko jest OK, połączenie z Internetem po nazwie jest poprawne.

Możemy już na klientach korzystać z Internetu.

