Translacja adresów sieciowych (NAT - Network Address Translation)

NAT jest to technika umożliwiająca ograniczenie liczby publicznych adresów IP i wykorzystanie prywatnych adresów IP w sieciach wewnętrznych.

Przypomnienie:

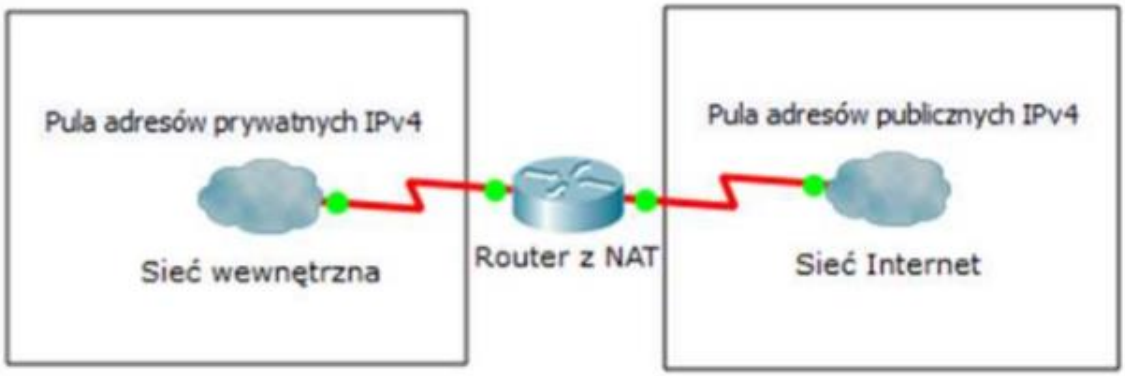
Adresy prywatne:

klasa A 10.0.0.0 do 10.255.255.255

klasa B 172.16.0.0 do 172.31.255.255

klasa C 192.168.0.0 do 192.168.255.255

Te prywatne, wewnętrzne adresy poddawane są translacji na adresy publiczne, które mogą być routowane.



Router mapuje prywatny adres wewnętrzny oraz adres publiczny i dokonuje zamiany adresu IP zarówno, gdy pakiet wychodzi z sieci jak również gdy do niej wraca. Dzięki temu na przykład posiadając nawet jeden publiczny adres IP firma może zapewnić komunikację z Internetem wielu hostom znajdującym się w sieci firmowej.

NAT przyczynił się do żywotności protokołu IPv4, ale ma on również inne zastosowania. Pozwala on dodatkowo na ukrycie informacji o sieci wewnętrznej. Osoba będąca na zewnątrz sieci nie ma informacji na temat adresacji wewnętrznej, widzi tylko adres publiczny, czyli już po tłumaczeniu NAT.NAT daje również możliwość używania pokrywających się podsieci – taka sytuacja może mieć miejsce np. gdy dojdzie do połączenia dwóch korporacji – dzięki translacji adresów możliwe będzie używanie takich samych podsieci, a jednocześnie zapewnienie komunikacji między nimi.

NAT nie jest jednak pozbawiony wad. Użycie translacji może utrudnić bądź uniemożliwić inicjalizowanie połączeń z zewnątrz – domyślnie NAT dopuszcza połączenia z sieci wewnętrznej do zewnętrznej, w przypadku niezestawionych sesji

będzie blokować połączenia z zewnątrz do wewnątrz. Nie da się ukryć, że wprowadza on również dodatkową złożoność w sieci. Trzeba wiedzieć, gdzie i jak jest skonfigurowany, by nie doprowadzić do błędów w konfiguracji. Kolejną rzeczą, na którą należy zwrócić uwagę to zwiększone zużycie zasobów urządzenia dokonującego translacji NAT. Mapowanie dużej puli adresów może wyraźnie zwiększyć wymagania w zakresie mocy obliczeniowej urządzenia, co naturalnie może się przełożyć na jego koszt.

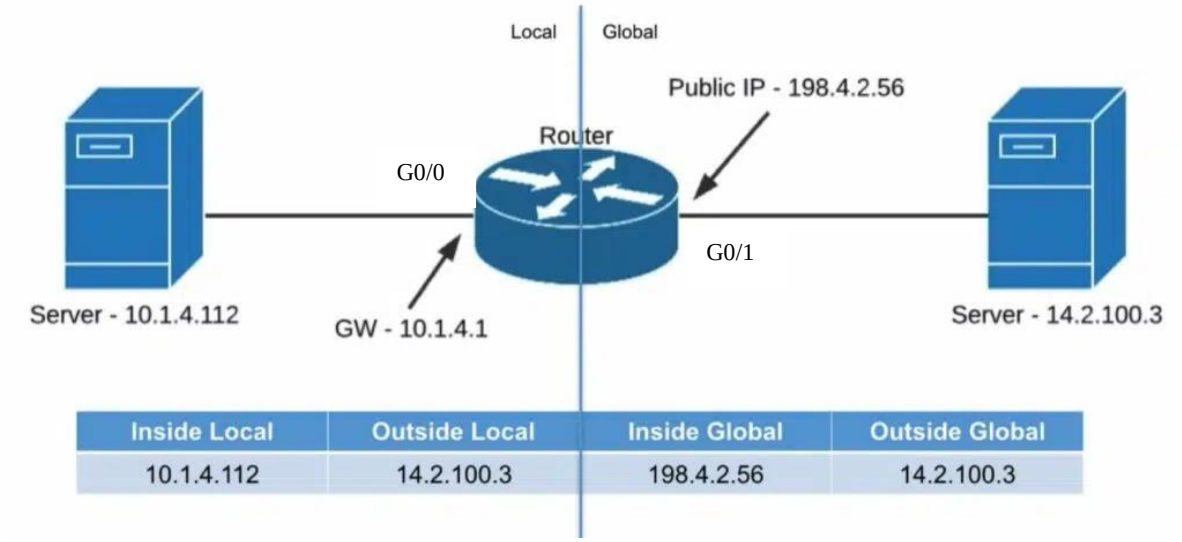
Możemy wyróżnić 3 rodzaje NAT, z czego każda z nich oferuje inne możliwości i ma różne zastosowania:

- Static NAT,
- Dynamic NAT
- NAT overload, nazywany wymiennie Port Address Translation (PAT).

Statyczna translacja NAT to dość proste rozwiązanie, które polega na translacji adresów ***jeden do jednego***. Oznacza to, że jeden adres prywatny z sieci wewnętrznej tłumaczony jest na jeden adres publiczny dostępny w Internecie. Co ważne Static NAT w przeciwieństwie do pozostałych odmian jest dwukierunkowy – umożliwia również działanie odwrotne, czyli mapowanie IP publicznego na prywatne. Ta metoda oczywiście nie zwiększa nam dostępnej puli adresów, ale przede wszystkim umożliwia ukrycie faktycznego adresu naszego urządzenia. Typowym przykładem użycia będą serwery. W przeciwieństwie do zwykłych hostów, zmiana adresu serwera może mieć duży wpływ na dostępność usług, więc jest niepożądana. Statycznie przypisanie zarówno adresu prywatnego jak i publicznego gwarantuje, że serwer będzie osiągalny wewnątrz i na zewnątrz sieci.

Terminologia NAT wyróżnia 4 rodzaje adresów:

- Inside local – rzeczywisty adres IP przydzielony hostowi znajdującemu się w sieci wewnętrznej
- Outside local – adres IP zewnętrznego hosta widziany z perspektywy sieci wewnętrznej
- Inside global – jest to adres hosta znajdującego się w sieci wewnętrznej, ale widziany z poziomu Internetu
- Outside global – rzeczywisty adres hosta znajdującego się poza siecią wewnętrzną



Inside Local	Outside Local	Inside Global	Outside Global
10.1.4.112	14.2.100.3	198.4.2.56	14.2.100.3

Konfiguracja dla powyższego przykładu:

Krok 1 – mapujemy adres prywatny na publiczny

```
Router(config)#ip nat inside source static 10.1.4.112 198.4.2.56
```

Krok 2 – określamy, który port będzie interfejsem wewnętrznym

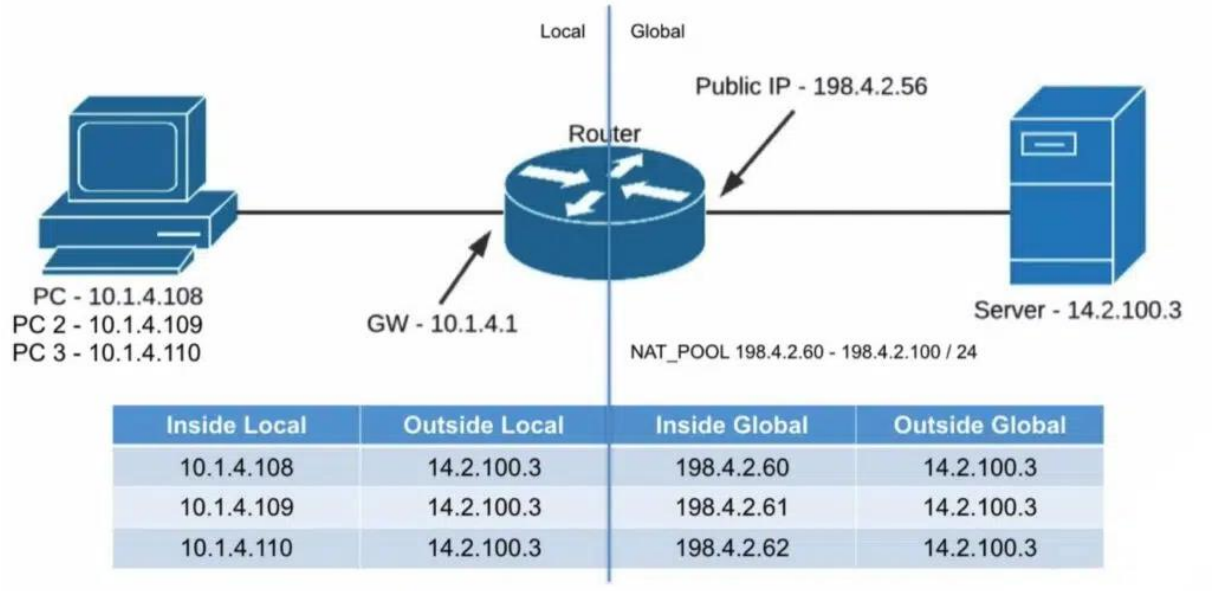
```
Router(config)#interface GigabitEthernet 0/0
Router(config-if)#ip nat inside
```

Krok 3 – określamy, który port będzie interfejsem zewnętrznym

```
Router(config)#interface GigabitEthernet 0/1
Router(config-if)#ip nat outside
```

Dynamiczna translacja NAT służy do odwzorowania prywatnego adresu IP na adres publiczny. Tutaj jednak w przeciwieństwie do Statycznego NAT mamy translację ***wiele do wielu***. Router zamiast jednego adresu ma skonfigurowaną pulę wielu możliwych do wykorzystania adresów. Wybiera on wolny adres z puli i przydzielenie go hostowi. Jeśli przez określony czas host nie będzie aktywny w sieci adres ten zostaje zwolniony (lub jeśli wpisy w tablicy adresów zostaną usunięte ręcznie) i może być przydzielony innemu hostowi. W Dynamic NAT może się zdarzyć tak, że pula adresów lokalnych będzie większa niż liczba dostępnych adresów globalnych. Router będzie przydzielać kolejne adresy globalne, aż do ich wyczerpania. Jeśli zabraknie adresu dla hosta, będzie on musiał czekać, aż zwolni się miejsce w tablicy adresów NAT.

Dynamic NAT nie jest rozwiązaniem spotykanym dość często. Najczęściej będzie używany w firmach mających duże pule publicznych adresów IP, co wiąże się z wysokimi kosztami.



Inside Local	Outside Local	Inside Global	Outside Global
10.1.4.108	14.2.100.3	198.4.2.60	14.2.100.3
10.1.4.109	14.2.100.3	198.4.2.61	14.2.100.3
10.1.4.110	14.2.100.3	198.4.2.62	14.2.100.3

Na powyższym przykładzie widzimy grupę hostów w podsieci 10.1.4.0/24, które mają korzystać z puli publicznych adresów w zakresie od 192.4.2.60/24 do 198.4.2.100/24. Konfiguracja Dynamic NAT przebiega następująco:

Krok 1 – Poprzez access listę określamy listę adresów wewnętrznych, dla których ma być wykonana translacja NAT.

```
Router(config)#access-list 1 permit 10.1.4.0 0.0.0.255
```

Krok 2 – Definiujemy pulę adresów publicznych, które będą służyły do translacji.

```
Router(config)# ip nat pool NAT_POOL 198.4.2.60 198.4.2.100 netmask
255.255.255.0
```

Krok 3 – włączamy Dynamic NAT odwołując się do utworzonej puli adresów i access-listy z kroków 1-2

```
Router(config)#ip nat inside source list 1 pool NAT_POOL
```

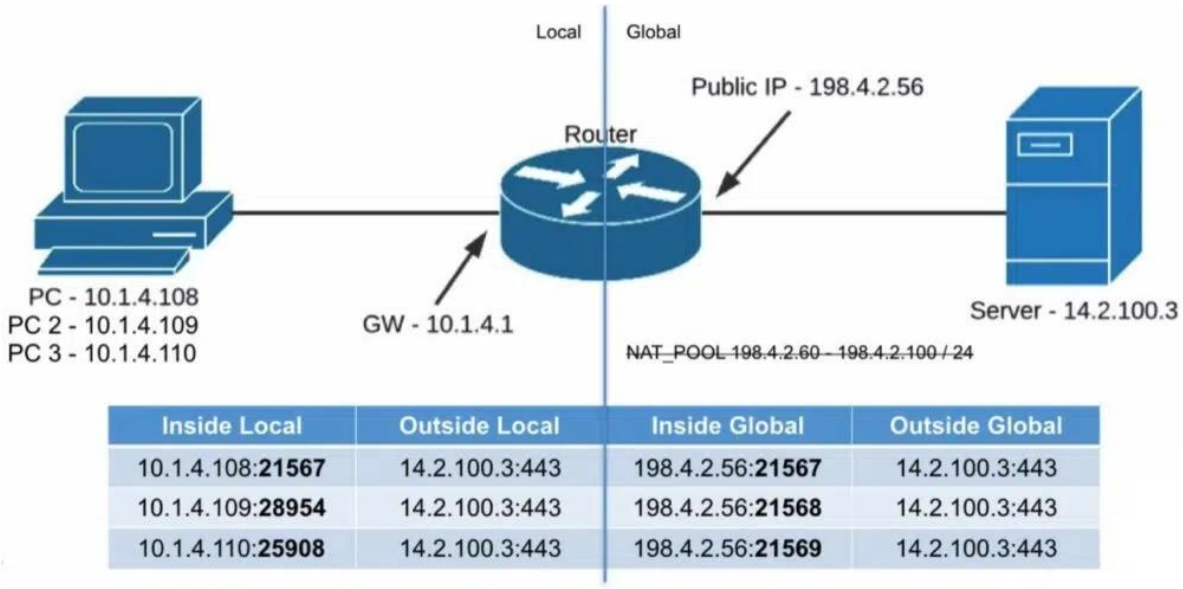
Krok 4 – określamy, który port będzie interfejsem wewnętrznym

```
Router(config)#interface GigabitEthernet 0/0

Router(config-if)#ip nat inside
```

Krok 5 – określamy, który port będzie interfejsem zewnętrznym

```
Router(config)#interface GigabitEthernet 0/1

Router(config-if)#ip nat outside
```

NAT Overload (inaczej **PAT** - Port Address Translation) służy do odwzorowania wielu prywatnych adresów IP na jeden publiczny adres IP. Takie rozwiązanie jest możliwe dzięki przydzieleniu do prywatnego adresu IP dynamicznego numeru portu. Dzięki takiemu zabiegowi jeden adres publiczny może obsługiwać 65 000 adresów wewnętrznych! (typ ***wiele-do-jednego***).



Inside Local	Outside Local	Inside Global	Outside Global
10.1.4.108:**21567**	14.2.100.3:443	198.4.2.56:**21567**	14.2.100.3:443
10.1.4.109:**28954**	14.2.100.3:443	198.4.2.56:**21568**	14.2.100.3:443
10.1.4.110:**25908**	14.2.100.3:443	198.4.2.56:**21569**	14.2.100.3:443

Zobaczmy jak w tym przypadku wygląda mapowanie adresów. Szczególną uwagę należy przywiązać do portów, które są przypisane do komunikacji. Przykładowo podczas pierwszej sesji NAT dokonywanej przez router host 10.1.4.108 z przypisanym portem dynamicznym **21567** otrzymał adres publiczny 198.4.2.56 z tożsamy numerem portu – **21567**. Kolejna sesja została nawiązana przez hosta 10.1.4.109 z portem **28954**. Dostał on również adres 198.4.2.56, ale port został zmieniony na kolejny następujący po wcześniejszym, czyli **21568.**

Przejdźmy do konfiguracji PAT:

Krok 1 – Poprzez access listę określamy listę adresów wewnętrznych, dla których ma być wykonana translacja NAT.

```
Router(config)#access-list 1 permit 10.1.4.0 0.0.0.255
```

Krok 2 – włączamy NAT overload odwołując się do utworzonej access-listy z kroku 1

```
Router(config)#ip nat inside source list 1 interface Gi0/1 overload
```

Krok 3 – określamy, który port będzie interfejsem wewnętrznym

```
Router(config)#interface GigabitEthernet 0/0

Router(config-if)#ip nat inside
```

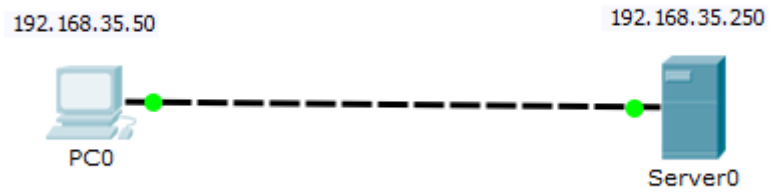
Krok 4 – określamy, który port będzie interfejsem zewnętrznym

```
Router(config)#interface GigabitEthernet 0/1
Router(config-if)#ip nat outside
```

Ćwiczenie

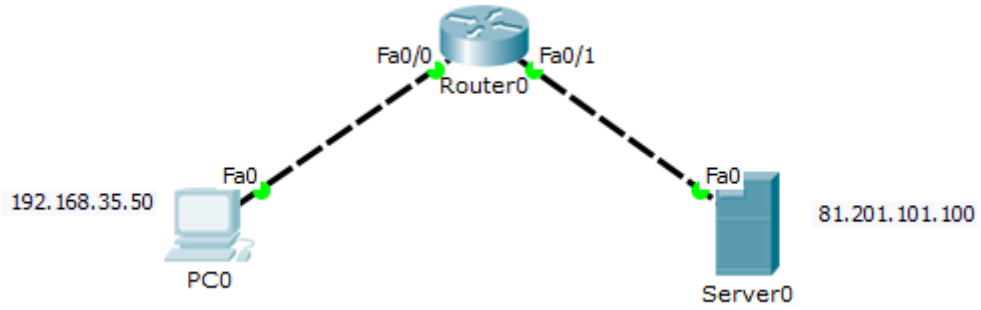
1. Działanie serwera www

Zrealizuj topologię jak na rysunku i sprawdź, czy komputer posiada połączenie z serwerem.



2. Konfiguracja podstawowa routera.

Zrealizuj topologię sieci wewnętrznej (LAN) i zewnętrznej (WAN) wg rysunku.
Zmień adres IP serwera, skonfiguruj interfejsy routera zgodnie z zasadą spójności sieci.



Sprawdź, czy komputer posiada połączenie z routerem (ping) i serwerem (www).

3. Realizacja NAT

Przetestujemy teraz translację adresów.
Pierwsza konfiguracja dotyczy pojedynczego hosta w sieci lokalnej, druga konfiguracja pozwoli na użycie NAT w stosunku do wszystkich hostów w sieci LAN, trzecia konfiguracja NAT overload.
Wykonaj zrzut ekranu potwierdzający wykonanie polecenia po każdej poniższej konfiguracji

Konfiguracja 1 – NAT Statyczny

Zmodyfikuj topologie sieci, rozbudowując sieć LAN o co najmniej 3 komputery.

Skonfiguruj NAT statyczny

Sprawdź połączenie PC0 z serwerem www i wykonaj na routerze polecenie,

```
show ip nat translations
```

Porównaj z poniższą tablicą. Jeżeli masz inne adresy lub nie masz adresów w tablicy nat to sprawdź poprawność konfiguracji.

```
sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
tcp 81.201.101.1:1026  192.168.35.50:1026 81.201.101.100:80  81.201.101.100:80
```

Sprawdź czy działa połączenie z innego PC niż PC0 z serwerem www.

Konfiguracja 2 – NAT Dynamiczny

Teraz włączymy NAT dla całej sieci LAN.
Usuń z routera poprzednią zasadę translacji adresów

```
Router0(config)#
no ip nat inside source static 192.168.35.50 81.201.101.1
```

Skonfiguruj NAT dynamiczny

Sprawdź teraz czy możesz z każdego komputera połączyć się do serwera www i wykonaj na routerze polecenie.

Konfiguracja 3 – NAT overload

Usuń z routera poprzednią zasadę translacji adresów
Skonfiguruj NAT overload
Sprawdź teraz czy możesz z każdego komputera połączyć się do serwera www i wykonaj na routerze polecenie.