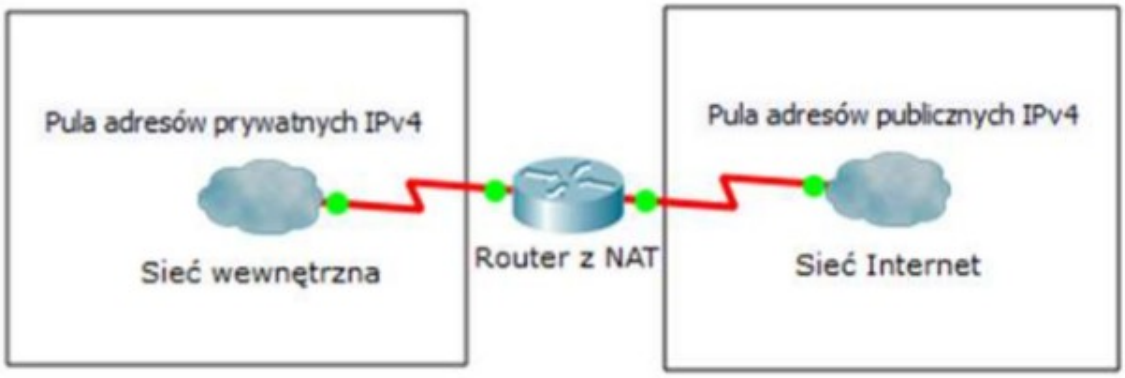
2. Translacja adresów sieciowych (NAT - Network Address Translation)

NAT jest to technika umożliwiająca ograniczenie liczby publicznych adresów IP i wykorzystanie prywatnych adresów IP w sieciach wewnętrznych.
Te prywatne, wewnętrzne adresy poddawane są translacji na adresy publiczne, które mogą być routowane.
Router realizujący translację NAT zazwyczaj działa na granicy sieci stub. **Sieć stub** to sieć, która ma pojedyncze połączenie z sąsiednią siecią.



Gdy host w sieci stub chce przesłać dane do hosta znajdującego się na zewnątrz, przekazuje pakiet do routera brzegowego. Router brzegowy realizuje proces NAT.
W terminologii mechanizmu NAT:

- sieć wewnętrzna to zbiór sieci, których adresy poddawane są translacji
- sieć zewnętrzna to wszystkie pozostałe adresy

Translacje NAT mogą być wykorzystywane do różnych celów, a przetłumaczone adresy mogą być przydzielane dynamicznie lub statycznie.

Statyczna translacja NAT umożliwia odwzorowanie typu ***jeden-do-jednego*** pomiędzy adresami lokalnymi i globalnymi. Jest to szczególnie przydatne w wypadku hostów, które muszą mieć stały adres dostępny z Internetu. Takimi wewnętrznymi hostami mogą być np. serwery.

Dynamiczna translacja NAT służy do odwzorowania prywatnego adresu IP na adres publiczny. Hostowi w sieci jest przypisywany dowolny adres z puli publicznych adresów IP - (typ ***wiele-do-wielu***).

Technika przeciążenia (inaczej **PAT** - Port Address Translation) służy do odwzorowania wielu prywatnych adresów IP na jeden publiczny adres IP. Istnieje taka możliwość, ponieważ z każdym adresem prywatnym związany jest inny numer portu (typ ***wiele-do-jednego***).

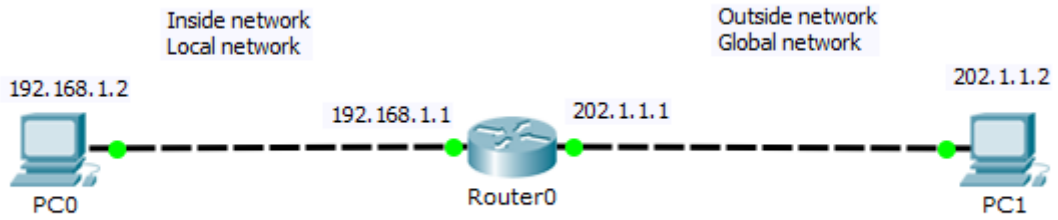
Zastosowanie technologii NAT zapewnia następujące korzyści:

- Eliminacja konieczności ponownego przypisania adresów IP do każdego hosta po zmianie dostawcy usług internetowych (ISP) - korzystanie z adresacji prywatnej w sieci wewnętrznej.
- Zmniejszenie liczby adresów przy użyciu dostępnej w aplikacji funkcji multipleksowania na poziomie portów (PAT)
- Zwiększenie poziomu bezpieczeństwa w sieci - gdyż w przypadku sieci prywatnej nie są rozgłaszane wewnętrzne adresy ani informacje o wewnętrznej topologii, sieć taka pozostaje wystarczająco zabezpieczona, gdy dostęp zewnętrzny odbywa się z wykorzystaniem translacji NAT.

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**



Inside/Outside (wewnętrzny/zewnętrzny) odnosi się do położenia urządzenia.
Local/Global (lokalny/globalny) oznacza bieżącą lokalizację pakietu.

Przyjrzyjmy się pakietowi przesyłanemu pomiędzy PC0 i PC1

- gdy jest przesyłany przez sieć lokalną, to jest to adres IP:
  1 -> 192.168.1.2
  2 -> 202.1.1.2
- gdy jest przesyłany w sieci globalnej to ma adresy IP:
  3 -> 202.1.1.1
  4 -> 202.1.1.2

I teraz nazwijmy te adresy IP:

1. 192.168.1.2
   - położenie pakietu - lokalny
   - położenie urządzenia - lokalizacja wewnętrzna (jest to PC0)
     wewnętrzny lokalny adres IP urządzenia (inside local)

2. 202.1.1.2
    - położenie pakietu - lokalny
    - położenie urządzenia - lokalizacja zewnętrzna (PC1)

      zewnętrzny lokalny adres IP urządzenia (outside local)
3. 202.1.1.1
    - położenie pakietu - globalny
    - położenie urządzenia - lokalizacja wewnętrzna (PC0)

      wewnętrzny globalny adres IP urządzenia (inside global)
4. 202.1.1.2
    - położenie pakietu - globalny
    - położenie urządzenia - lokalizacja zewnętrzna (PC1)

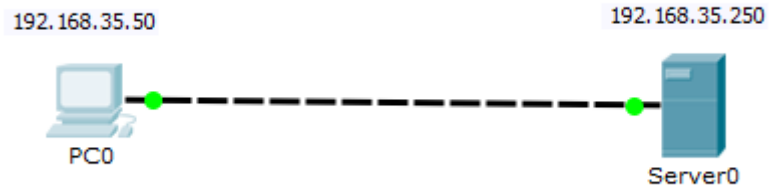
      zewnętrzny globalny adres IP urządzenia (outside global)

```
Router#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 202.1.1.1:1       192.168.1.2:1      202.1.1.2:1        202.1.1.2:1
```

Ćwiczenie

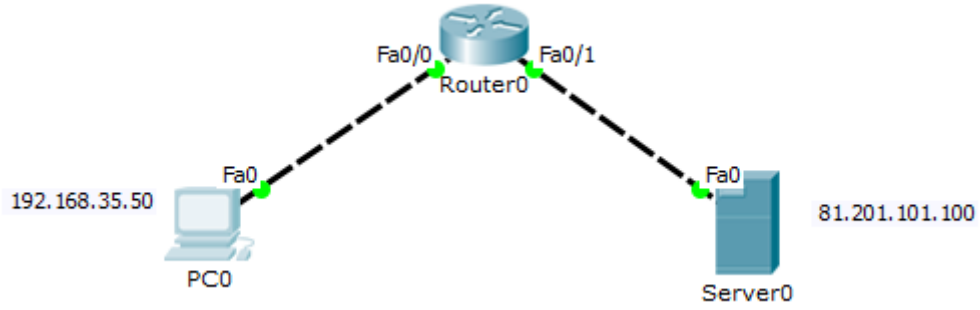
1. Działanie serwera www

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.

Konfiguracja 1

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

Zdefiniuj zasady translacji adresu komputera PC0 na adres zewnętrzny routera.

```
Router0# conf t
Router0(config)#
ip nat inside source static 192.168.35.50 81.201.101.1
```

Teraz włącz NAT na odpowiednich interfejsach routera

```
Router0(config)# interface fa0/1
Router0(config-if)#ip nat outside
Router0(config-if)#exit
Router0(config)#interface fa0/0
Router0(config-if)#ip nat inside
```

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
```

Konfiguracja 2

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
```

Utwórz listę adresów wewnętrznych, które będą ulegały translacji.

```
Router0(config)#access-list 10 permit 192.168.35.0 0.0.0.255
```

Zdefiniuj listę adresów zewnętrznych

```
Router0(config)#ip nat pool lan_nat 81.201.100.80
81.201.100.81 netmask 255.255.255.0
```

Zdefiniuj zasady translacji adresów

```
Router0(config)#ip nat inside source list 10 pool lan_nat
```

Sprawdź teraz czy możesz z każdego komputera połączyć się do serwera www.

?!