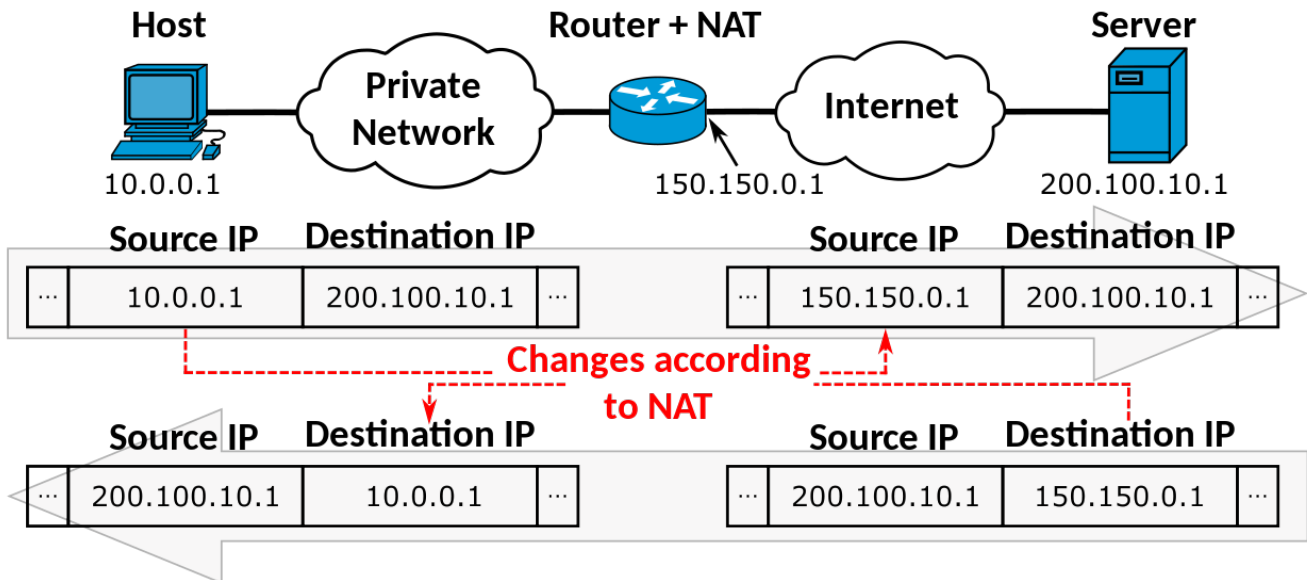


# Network: Rodzaje translacji adresów NAT

Fragment z Ostrowski, K. (2025). Leksykon: Sieci Komputerowe - Dla inżynierów oraz techników (1.0). Zenodo. <https://doi.org/10.5281/zenodo.15341381>

Leksykon: Sieci Komputerowe



Przedstawienie translacji SNAT pomiędzy siecią WAN i siecią LAN

Translacja adresów w sieciach IP (ang. Address Translation) jest techniką umożliwiającą mapowanie adresów IP z jednej przestrzeni adresowej na inną. Jest szczególnie przydatna w zarządzaniu adresacją sieciową, zapewnianiu bezpieczeństwa oraz umożliwianiu komunikacji między różnymi sieciami. Istnieje kilka metod translacji adresów, z których najczęściej wykorzystywane to: SNAT (Source Network Address Translation), DNAT (Destination Network Address Translation) oraz PAT (Port Address Translation).

## SNAT (Source Network Address Translation)

SNAT jest procesem translacji adresu źródłowego w pakietach IP. Wykorzystywany jest głównie w scenariuszach, gdy urządzenia wewnętrzne (np. komputery w sieci lokalnej) chcą komunikować się z zewnętrzną siecią (np. Internetem), ale nie mają publicznych adresów IP. Dzięki SNAT, pakiety wychodzące z sieci wewnętrznej są zmieniane tak, by wyglądały, jakby pochodziły od urządzenia z publicznym adresem IP. Typowym przykładem jest router pełniący rolę bramy domyślnej, który zamienia prywatne adresy IP na jeden publiczny adres.

### Praktyczne zastosowania SNAT:

- Łączenie urządzeń wewnętrznych z Internetem przy użyciu pojedynczego publicznego adresu IP.
- Maskowanie prawdziwego adresu źródłowego w celu ochrony prywatności wewnętrznych urządzeń.
- Optymalizacja wykorzystania publicznych adresów IP w przypadku ograniczonej liczby

dostępnych zasobów.

## DNAT (Destination Network Address Translation)

DNAT to proces translacji adresu docelowego w pakietach IP. Jest wykorzystywany, gdy pakiety przychodzące do sieci muszą być skierowane do odpowiednich urządzeń wewnętrznych, mimo iż posiadają one prywatne adresy IP. Najczęściej stosowane w scenariuszach, w których serwery wewnętrzne muszą być dostępne z Internetu, np. serwer WWW, serwer FTP, czy serwer pocztowy. Przy pomocy DNAT, router lub zaporę sieciową zmienia adresy docelowe pakietów, przekierowując je do odpowiednich serwerów wewnętrznych.

### Praktyczne zastosowania DNAT:

- Udostępnianie serwerów wewnętrznych (np. serwery WWW, FTP) w Internecie.
- Kierowanie ruchu przychodzącego na różne serwery w zależności od portu docelowego (np. HTTP na jeden serwer, FTP na inny).
- Umożliwienie komunikacji z urządzeniami posiadającymi prywatne adresy IP w środowiskach zewnętrznych.

## PAT (Port Address Translation)

PAT, znane również jako *NAT z translacją portów*, to technika, w której wiele urządzeń wewnętrznych korzysta z jednego publicznego adresu IP, ale różne połączenia wychodzące są identyfikowane na podstawie numeru portu. Jest to najbardziej popularna forma NAT, stosowana w sytuacjach, gdy w sieci lokalnej znajduje się wiele urządzeń, ale tylko jeden publiczny adres IP. Każde połączenie wychodzące z sieci wewnętrznej jest przypisane do unikalnego numeru portu, co pozwala na zróżnicowanie wielu połączeń wychodzących z jednego adresu IP.

### Praktyczne zastosowania PAT:

- Umożliwienie wielu urządzeniom w sieci lokalnej korzystania z jednego publicznego adresu IP.
- Efektywne zarządzanie ograniczoną liczbą publicznych adresów IP.
- Użycie w domowych routerach, gdzie wiele urządzeń korzysta z internetu poprzez jeden publiczny adres IP.

## DMZ (Demilitarized Zone)

DMZ, czyli *strefa zdemilitaryzowana*, to segment sieci, który znajduje się pomiędzy zewnętrzną siecią (np. Internetem) a wewnętrzną siecią korporacyjną. Jest to specjalnie wydzielona strefa, w której znajdują się serwery, które muszą być dostępne zarówno z sieci wewnętrznej, jak i z Internetu, np. serwery WWW, FTP, czy pocztowe. Celem DMZ jest zwiększenie bezpieczeństwa, ponieważ pozwala na oddzielenie serwerów, które muszą być dostępne z zewnątrz, od wewnętrznej sieci, chroniąc ją przed bezpośrednim dostępem z Internetu.

### Praktyczne zastosowania DMZ:

- Izolowanie serwerów dostępnych z Internetu (np. serwery WWW, serwery pocztowe) od

wewnętrznej sieci firmowej.

- Zwiększenie bezpieczeństwa organizacji poprzez segmentację ruchu sieciowego.
- Zapewnienie kontroli dostępu do wrażliwych zasobów, ograniczając dostęp do serwerów wewnętrznych z zewnątrz.

## Podsumowanie

Translacja adresów w sieciach IP stanowi niezbędny element w zarządzaniu ruchem sieciowym, zapewnianiu bezpieczeństwa oraz efektywnym wykorzystaniu dostępnych zasobów adresowych. Techniki takie jak SNAT, DNAT, PAT oraz koncepcja DMZ pozwalają na skuteczną kontrolę dostępu oraz zarządzanie komunikacją między różnymi segmentami sieci. Poprzez zastosowanie tych technologii, możliwe jest zarówno zapewnienie prywatności urządzeń wewnętrznych, jak i udostępnienie zasobów sieciowych na zewnątrz w sposób bezpieczny i kontrolowany.