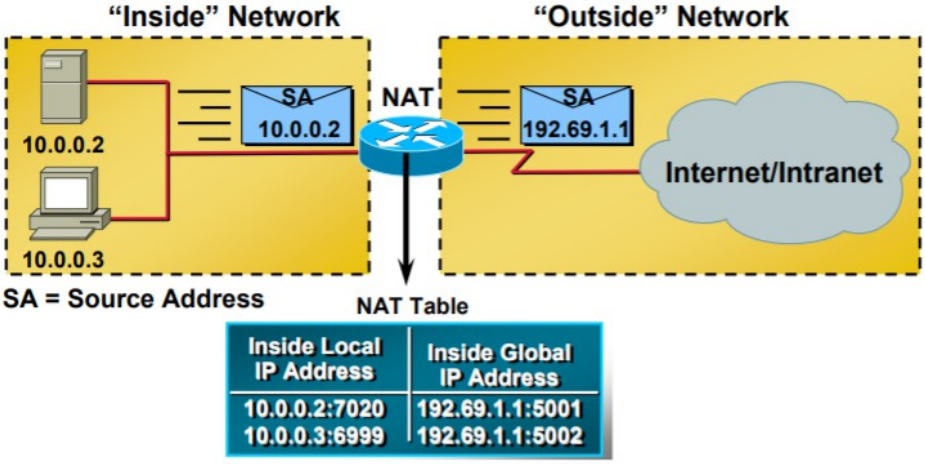
Działanie PAT:

- tłumaczy parę (adres IP, port) na (adres IP, port)
- różne adresy wewnętrzne są tłumaczone na **ten sam** zewnętrzny adres IP, ale różne porty
- multipleksuje adres IP za pomocą portów
- świat na zewnątrz widzi całą sieć jako ten jeden router, tak jakby on wszystko nadawał; jak coś przyjdzie z zewnątrz do tego routera, to przychodzi jednak na konkretny port, dzięki czemu on wie, gdzie to przesłać wewnątrz



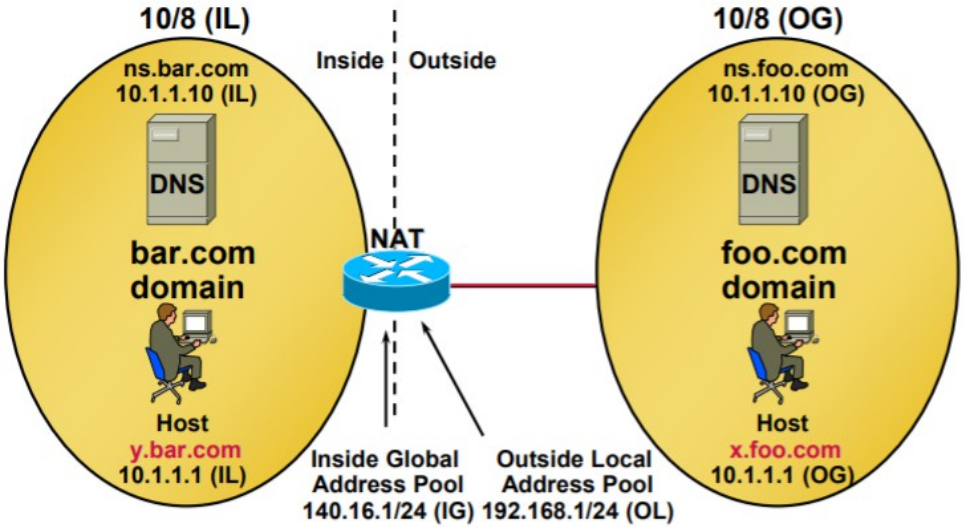
Współpraca sieci o nakładających się adresach:

Weźmy sytuację taką, jak na rysunku poniżej. Mamy włączony NAT (ale nie PAT!) na routerze brzegowym sieci wewnętrznej (ta po lewej).

Parę założeń co do DNSa:

- serwery DNS są autorytatywne dla swoich sieci, domyślne dla pokazanych hostów i odpytują rekurencyjnie
- serwer DNS ns.foo.com jest nadrzędny dla ns.bar.com, to on łączy się z wyższymi w hierarchii serwerami DNS
- chcemy, żeby hosty z obu sieci mogły się komunikować ze sobą za pomocą DNSa

Jak widać, adresy się nakładają i to prywatne adresy IP, więc trzeba NATa do komunikacji.



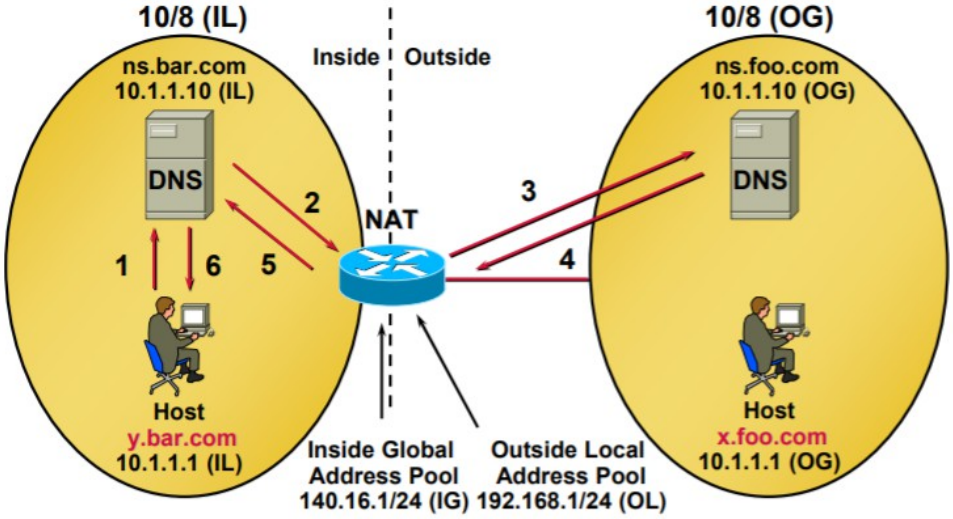
Żeby spełnić powyższe wymagania, NAT musi zrobić pełne tłumaczenie IL -> IG (żeby ci na zewnątrz mogli komunikować się z wewnętrzną siecią) oraz OG -> OL (żeby ci wewnątrz mogli komunikować się z zewnętrzną siecią).

Tłumaczymy więc, używając pul adresów z rysunku. Adresy po tłumaczeniu są dowolnymi adresami z puli. Komunikacja między hostami póki co nie zachodziła, więc w tablicy NAT będą tylko adresy dla serwerów DNS (bo one muszą się komunikować) - wpisy statyczne.

Adres oryginalny	Typ	Adres przetłumaczony	Typ
10.1.1.10	IL	140.16.1.254	IG
140.16.1.254	IG	10.1.1.10	IL
10.1.1.10	OG	192.168.1.254	OL
192.168.1.254	OL	10.1.1.10	OG

Jak widać, mamy dwukierunkowe tłumaczenie odpowiednich adresów. Serwery DNS mogą dzięki tej tablicy się ze sobą komunikować.

Załóżmy teraz, że host wewnętrzny y.bar.com chce skomunikować się z hostem zewnętrznym x.foo.com. Najpierw potrzebuje jego adresu IP, więc robi DNS Query.



1. Host pyta swój lokalny serwer DNS o adres:
   - oba są w sieci wewnętrznej, więc komunikują się z użyciem swoich adresów IL
   - 10.1.1.1 IL -> 10.1.1.10 IL
2. Serwer DNS nie zna adresu IP, więc pyta swój nadrzędny serwer ns.foo.com:
   - serwer z wewnątrz komunikuje się z zewnętrznym, ale tłumaczenie już znamy
   - 10.1.1.10 IL -> 192.168.1.254 OL
3. Router przesyła dalej zapytanie:
   - od nadawcy (adres IG) trzeba wysłać do odbiorcy (adres OG)
   - 140.16.1.254 IG -> 10.1.1.10 OG

4. Serwer DNS ns.foo.com zna adres IP hosta x.foo.com i może odpowiedzieć:
   - dokładnie to, co powyżej, tylko w drugą stronę
   - 10.1.1.10 OG -> 140.16.1.254 IG
5. Router przesyła odpowiedź do serwera ns.bar.com, który wysłał zapytanie:
   - jak krok 2, ale w drugą stronę
   - 192.168.1.254 OL -> 10.1.1.10 IL
6. Serwer odsyła odpowiedź z adresem IP x.foo.com hostowi y.bar.com, który o to pytał:
   - jak krok 1, ale w drugą stronę
   - 10.1.1.10 IL -> 10.1.1.1 IL

Podsumowując:

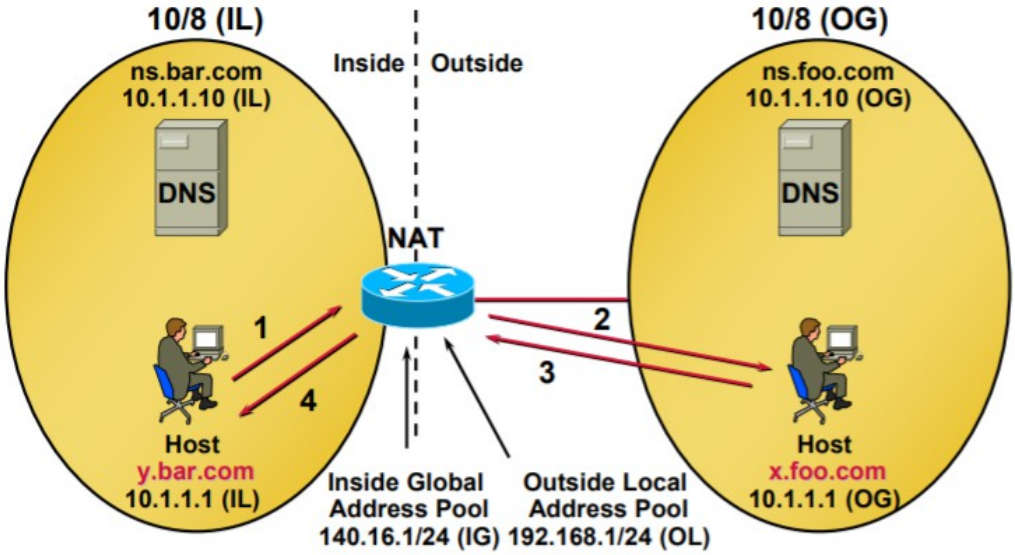
Krok	Adres oryginalny	Typ	Adres przetłumaczony	Typ
1	10.1.1.1	IL	10.1.1.10	IL
2	10.1.1.10	IL	192.168.1.254	OL
3	140.16.1.254	IG	10.1.1.10	OG
4	10.1.1.10	OG	140.16.1.254	IG
5	192.168.1.254	OL	10.1.1.10	IL
6	10.1.1.10	IL	10.1.1.1	IL

Jak widać, jest sporo “odwróconych” wpisów, tzn. w tych dalszych krokach robimy to, co we wcześniejszych, ale “w drugą stronę”. Wynika to z tego, że jest to jednokierunkowe tłumaczenie.

Załóżmy, że adres OL x.foo.com to 192.168.1.75, przy czym jego prawdziwy adres OG to 10.1.1.1. Do tablicy NAT dojdą więc wpisy dynamiczne dla tego adresu (dla oszczędności miejsca nie przepisywałem adresów statycznych).

Adres oryginalny	Typ	Adres przetłumaczony	Typ
10.1.1.1	OG	192.168.1.75	OL
192.168.1.75	OL	10.1.1.1	OG

Host y.bar.com zna więc już adres x.foo.com i widzi go jako 192.168.1.75. Może więc nastąpić komunikacja między hostami. Załóżmy, że będzie tam i z powrotem, np. pingowanie.



1. Host y.bar.com wysyła pakiet zaadresowany do x.foo.com, wysyła więc do swojego routera:
   - router widzi pakiet, który idzie od 10.1.1.1 (IL y.bar.com) do 192.168.1.75 (OL x.foo.com)
   - wie, że będzie musiał podmienić adres nadawcy (musi być IG, a nie IL) oraz adres odbiorcy (musi być OG, a nie OL)
2. Router przesyła pakiet dalej:
   - nie ma żadnego wpisu IL -> IG dla 10.1.1.1 (bo to pierwsza komunikacja hosta ze światem zewnętrznym), więc musi dodać wpis IL -> IG, dodaje jakiś adres z puli IG
   - 10.1.1.10 IL -> 140.16.1.55 IG
   - router ma tłumaczenie OL -> OG dla adresu 192.16.1.75 (wpis dynamiczny 192.16.1.75 OL -> 10.1.1.1 OG), więc może podmienić
   - pakiet zmienia swój adres nadawcy i odbiorcy:
     (10.1.1.1, 192.16.1.75) -> (140.16.1.55, 10.1.1.1)
3. Host x.foo.com dostaje pakiet i odpowiada, przesyłając pakiet do routera:
   - trzeba zmapować OG (adres źródłowy x.foo.com) na IG
   - 10.1.1.1 OG -> 140.16.1.55 IG
4. Router przesyła pakiet do y.bar.com:
   - trzeba zmapować OL (adres docelowy x.foo.com) na IL
   - 192.168.1.75 OL -> 10.1.1.1 IL

Podsumowując:

Krok	Adres oryginalny	Typ	Adres przetłumaczony	Typ
1	10.1.1.1	IL	192.168.1.75	OL
2	140.16.1.55	IG	10.1.1.1	OG
3	10.1.1.1	OG	140.16.1.55	IG
4	192.168.1.75	OL	10.1.1.1	IL

Do tablicy NAT dodaliśmy kolejne dynamiczne wpisy, tym razem pochodzące od y.bar.com.

Adres oryginalny	Typ	Adres przetłumaczony	Typ
10.1.1.1	IL	140.16.1.55	IG
140.16.1.55	IG	10.1.1.1	IL

Podsumowując, cała tablica NAT:

Adres oryginalny	Typ	Adres przetłumaczony	Typ
10.1.1.10	IL	140.16.1.254	IG
140.16.1.254	IG	10.1.1.10	IL
10.1.1.10	OG	192.168.1.254	OL
192.168.1.254	OL	10.1.1.10	OG
10.1.1.1	OG	192.168.1.75	OL
192.168.1.75	OL	10.1.1.1	OG
10.1.1.1	IL	140.16.1.55	IG
140.16.1.55	IG	10.1.1.1	IL

Pierwsza część - statyczne wpisy z DNSa
Druga część - dynamiczne wpisy od x.foo.com
Trzecia część - dynamiczne wpisy od y.bar.com

W przypadku PAT na powyższym przykładzie router miałby po prawej stronie (publiczna sieć) jeden adres IP, po lewej (prywatna sieć) drugi. Host y.bar.com wysyłałby coś do routera z własnego adresu i portu, port wysyłałby to do x.foo.com z adresem nadawcy podmienionym na własny (oraz portem reprezentującym y.bar.com), tak samo z powrotem. Istotą PAT jest jeden adres routera w części zewnętrznej i używanie po 1 porcie na każdego hosta wewnątrz prywatnej sieci.