Network Address Translation (NAT)

Христо Вълчанов
Технически Университет - Варна

Частни и публични адреси

Public Internet addresses are regulated by five Regional Internet Registries (RIRs):

- ARIN
- RIPE NCC
- APNIC
- LACNIC
- AfriNIC

- Всички публични Internet адреси трябва да бъдат регистрирани в Regional Internet Registry (RIR) (5 региона).
- Организациите наемат адреси от ISP.
- Само регистриран притежател на публичен интернет адрес може да зададе този адрес на мрежово устройство.

Частни адреси

Клас	Обхват	CIDR Prefix
A	10.0.0.0-10.255.255.255	10.0.0.0/8
B	172.16.0.0-172.31.255.255	172.16.0.0/12
C	192.168.0.0-192.168.255.255	192.168.0.0/16

- Те са само за вътрешни мрежи за частна употреба.
- Съгласно RFC 1918 тези адреси не се маршрутизиратв Интернет

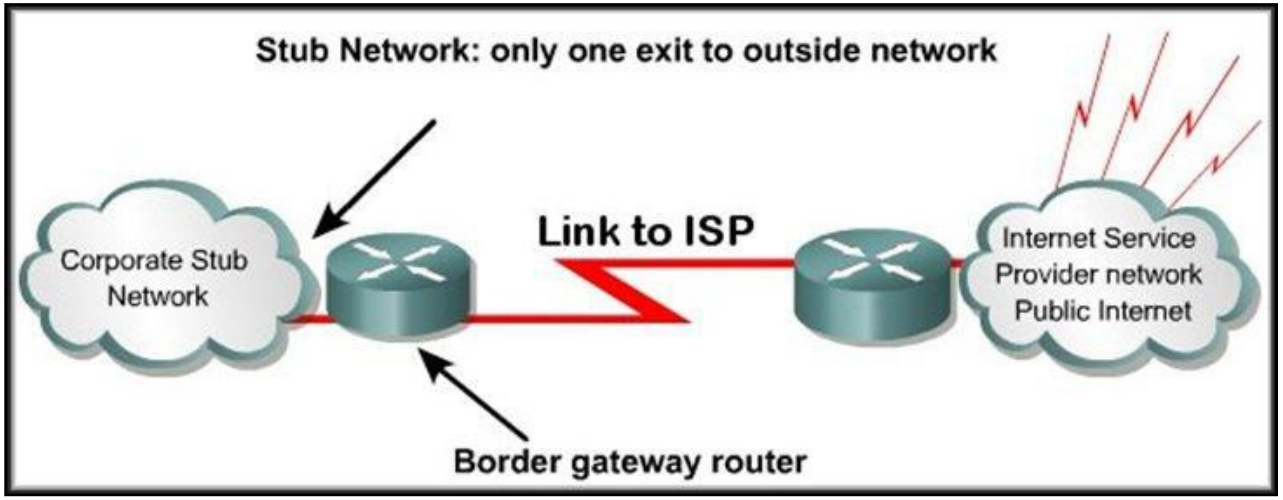
Проблеми

- Частните адреси не се маршрутизиратв Интернет.
- Няма достатъчно публични IPv4 адреси.
- Мрежите се нуждаят от механизъм за двупосочно преобразуване на частни в публични адреси на граничните устройства за мрежата - NAT.

Същност на NAT

- NAT преобразува вътрешния IP адрес на клиента във външен адрес.
- Когато е конфигуриран NAT на рутера, той има >=1 публични адреса за външната мрежа.
- За външните потребители, целият трафик от тази мрежа изглежда сякаш идва от 1 адрес (или pool).

Stub мрежа



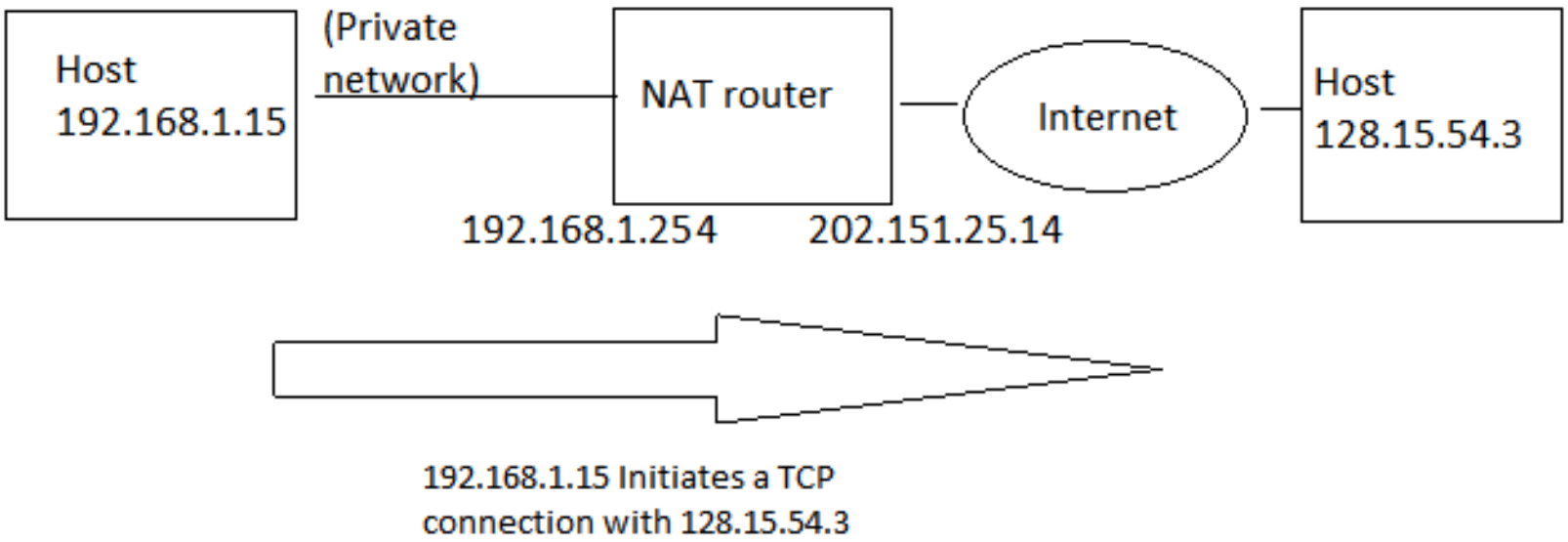
- Stub мрежа е мрежа, която има само 1 връзка към нейната съседна мрежа.
- NAT работи на гранично устройство между тези мрежи.

Типове NAT

- Static NAT
- Pool NAT
- PAT (Port Address Translation)

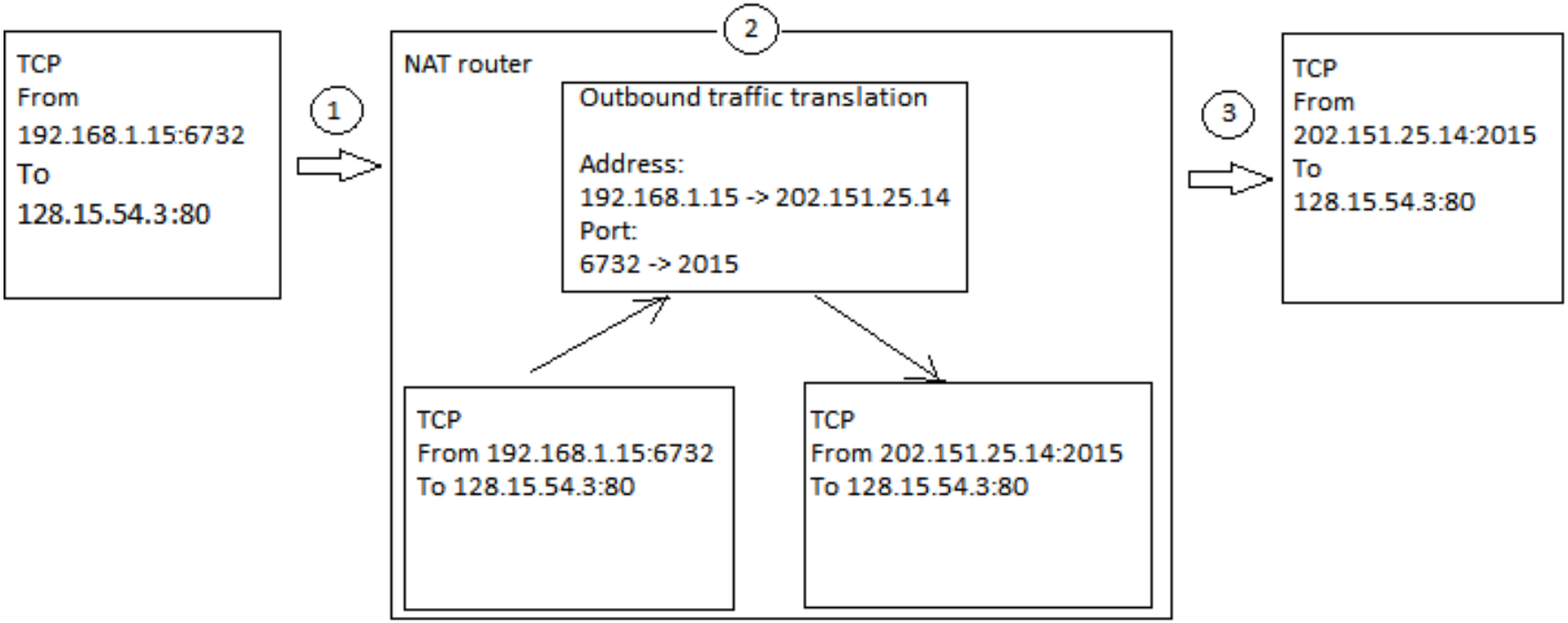
NAT Type	Example
Static	192.168.1.47 -> 192.0.2.252
Pool	192.168.1.17 -> 192.0.2.10 192.168.1.21 -> 192.0.2.11 192.168.1.56 -> 192.0.2.12
PAT	192.168.1.* -> 192.0.2.20

Функциониране на NAT



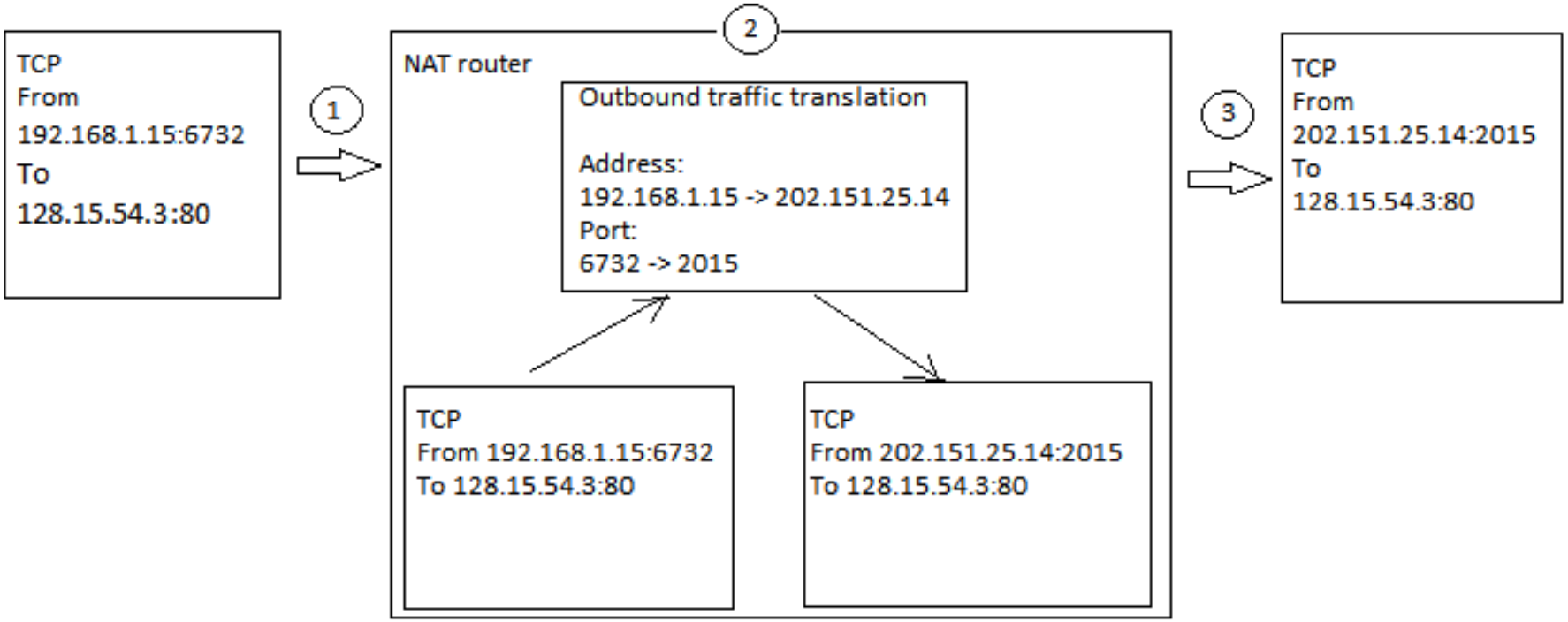
- Щом хост от вътрешната мрежа иска достъп до външната мрежа, пакетът се изпраща на граничния рутер.
- Граничният рутер (gateway) изпълнява NAT и преобразува вътрешния частен адрес във външен публичен адрес

Изпращане на пакет



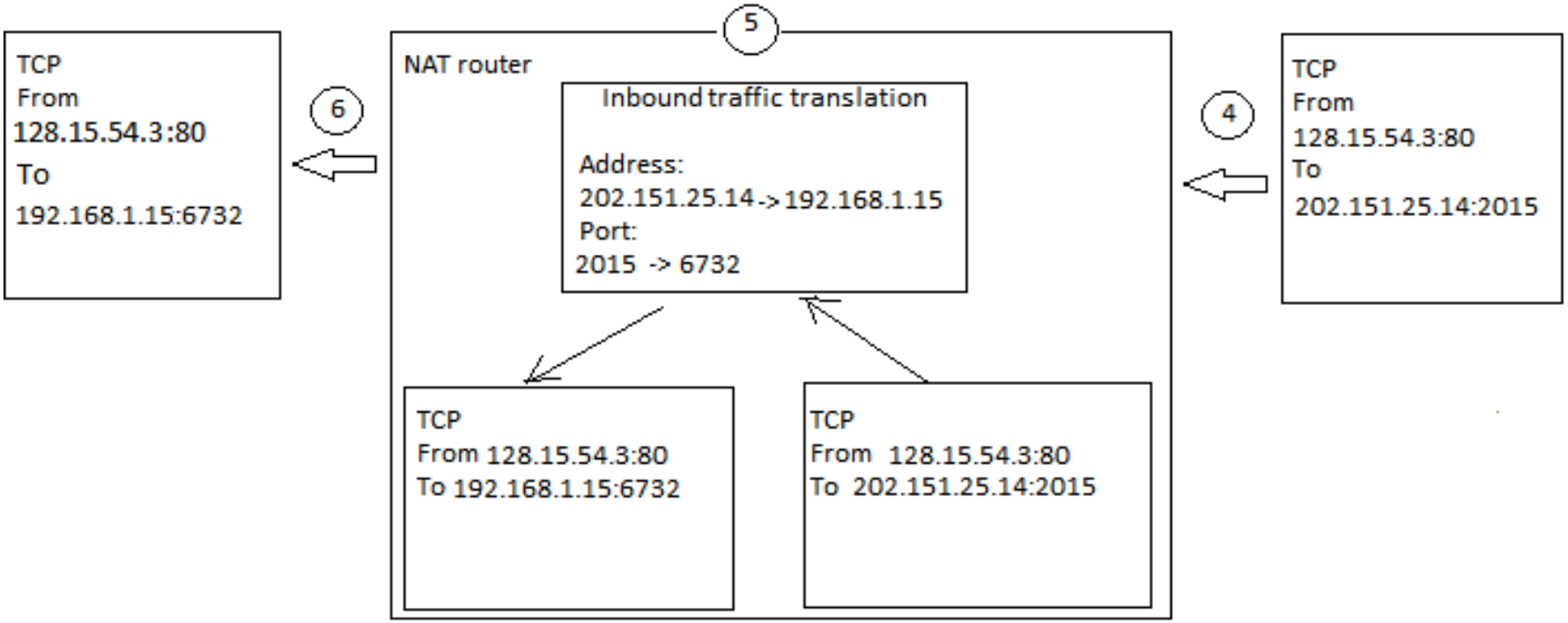
1. Клиентът изпраща TPC SYN пакет към HTTP сървър
2. Пакетът се получава на вътрешния (private) интерфейс на рутера. Прилага се правилото за изходящия трафик.

Изпращане на пакет



3. Пакетът се изпраща от изходния интерфейс на рутера с IP адреса на източник 202.151.25.14 и порт 2015

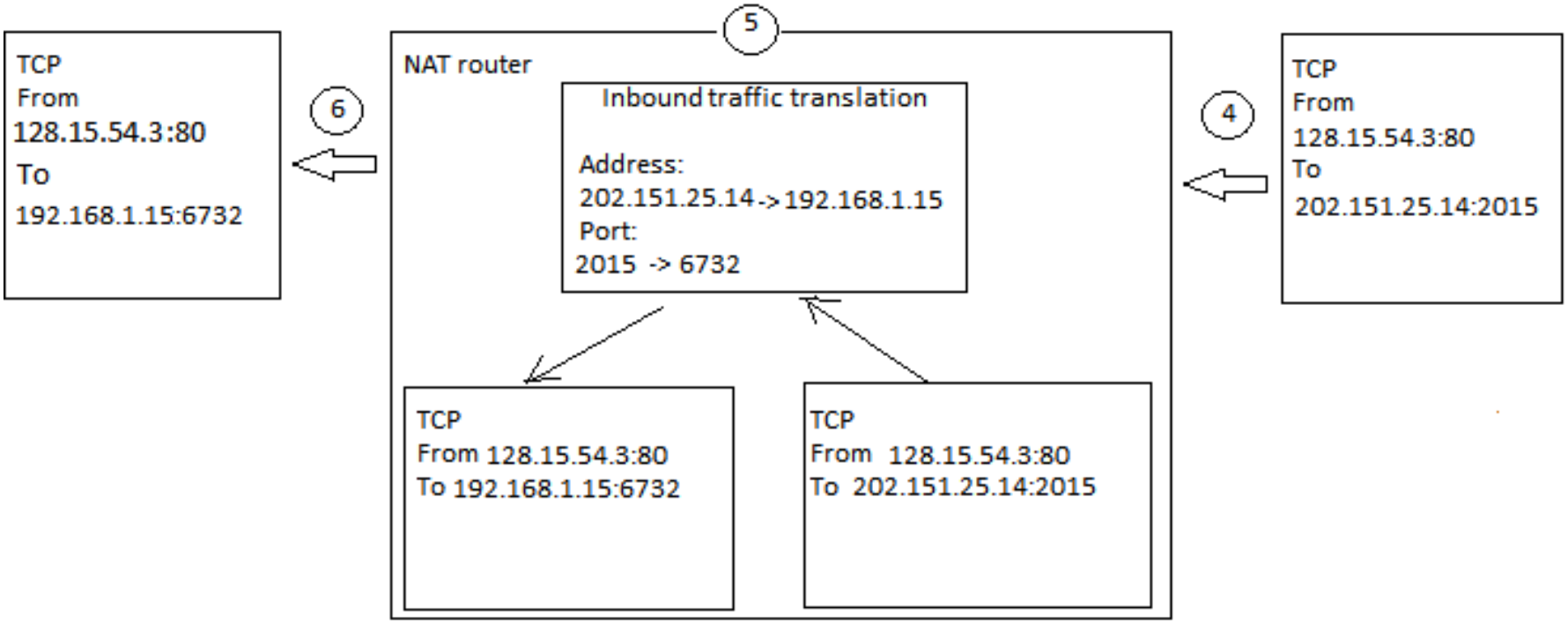
Получаване на отговор



4. Отговорът се изпраща към IP 202.151.25.14 (рутера)

5. Прилага се правилото за входящ трафик. IP адресът на получателя се сменя на оригиналния клиентски адрес и порт.

Получаване на отговор



6. Пакетът се препраща по вътрешния интерфейс на рутера към клиента

Предимства на NAT

- Пести брой на нужните публични адреси.
- Увеличава гъвкавостта на връзките в публичната мрежа.
- Осигурява съгласуваност между адресите от вътрешната и външната мрежа.
- Осигурява мрежова сигурност.

Недостатъци на NAT

- Производителността на мрежата намалява.
- Функционалността End-to-end намалява.
- Губи се проследяването на End-to-end.
- Тунелирането е по-сложно за създаване.
- Създаването на TCP конекции може да се прекъсне.
- Може да се наложи мрежовата архитектура да се изгради наново.

Какво (не)поддържа NAT

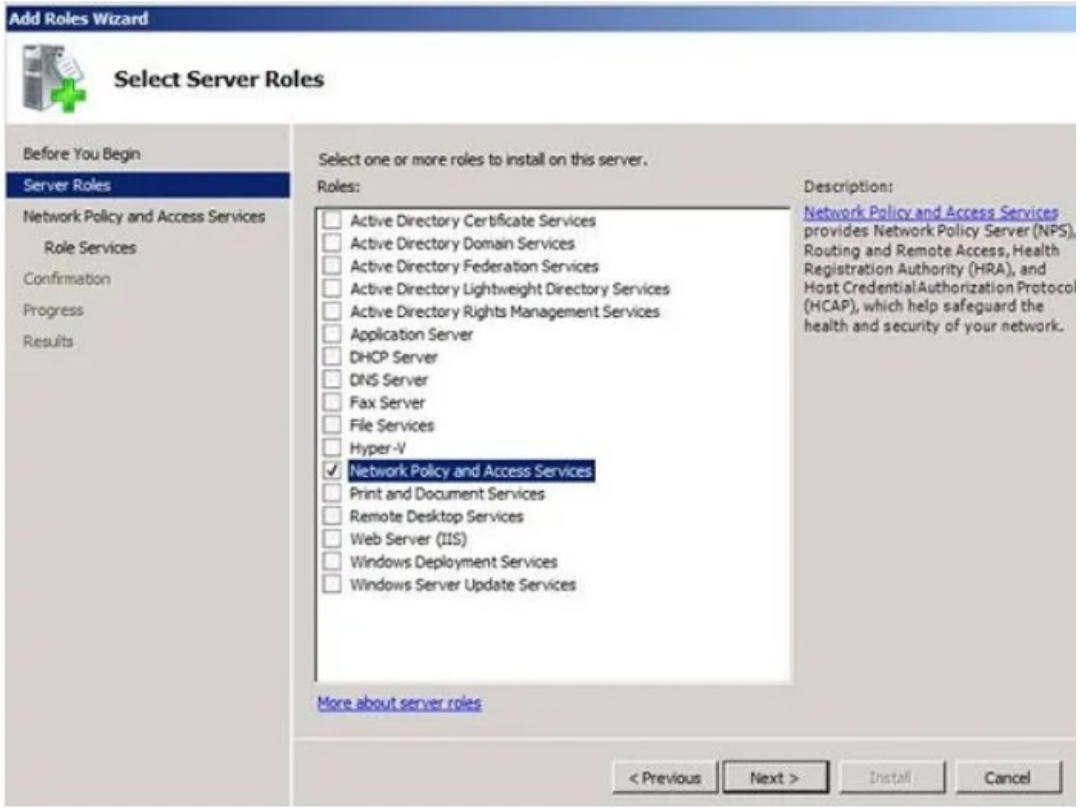
Поддържа:

- ICMP
- FTP
- Progressive Network‟s Real Audio
- XING technologies Streamworks
- DNS „A‟
- Netmeeting

Не поддържа:

- Routing & table updates
- DNS zone transfers
- BOOTP
- Talk, ntalk
- SNMP
- Netshow

Конфигуриране на Windows Server за NAT

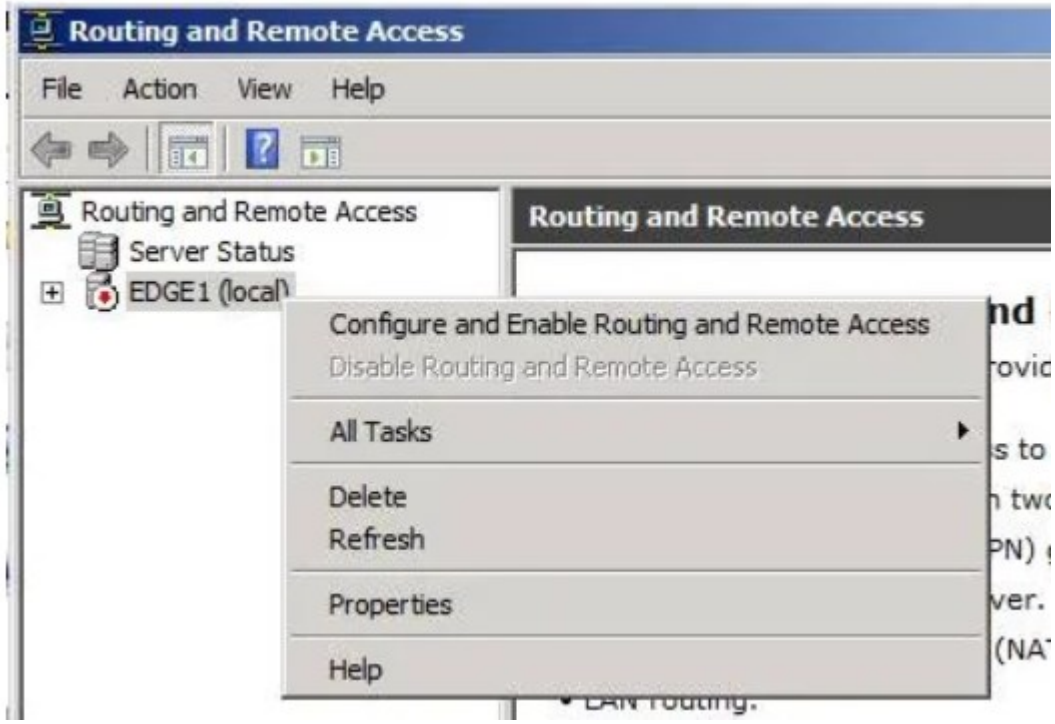


Необходимо е инсталиране на роля **Network Policy and Access Services** от конзолата на Server Manager.

Конфигуриране на Windows Server за NAT

От услугите на ролята се избира **Routing and Remote Access Services**.

Конфигуриране на Windows Server за NAT



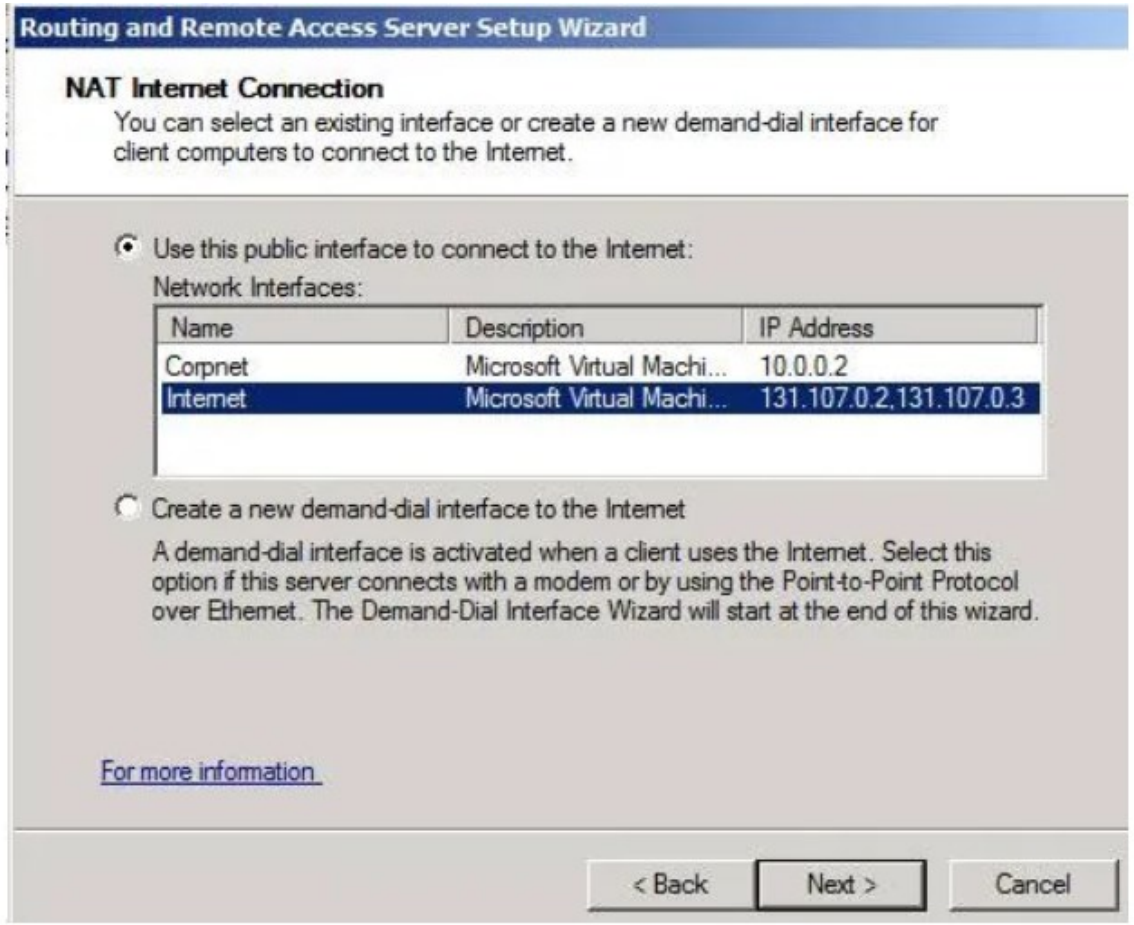
След инсталиране на ролята се отваря конзолата на RRAS и се преминава към конфигуриране на ролята (десен бутон върху името на сървъра).

Конфигуриране на Windows Server за NAT

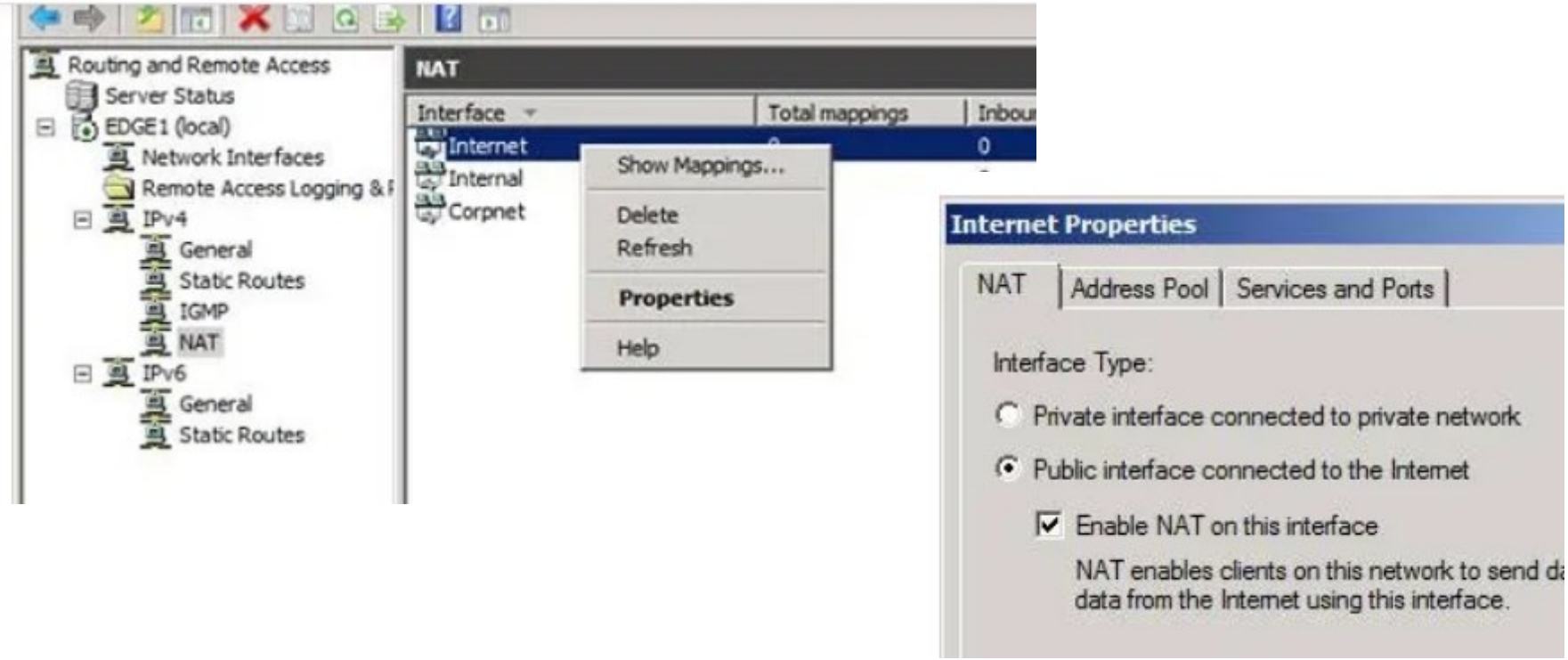
Избира се услугата NAT.

Конфигуриране на Windows Server за NAT

Трябва да се укаже кой интерфейс е свързан към Интернет.



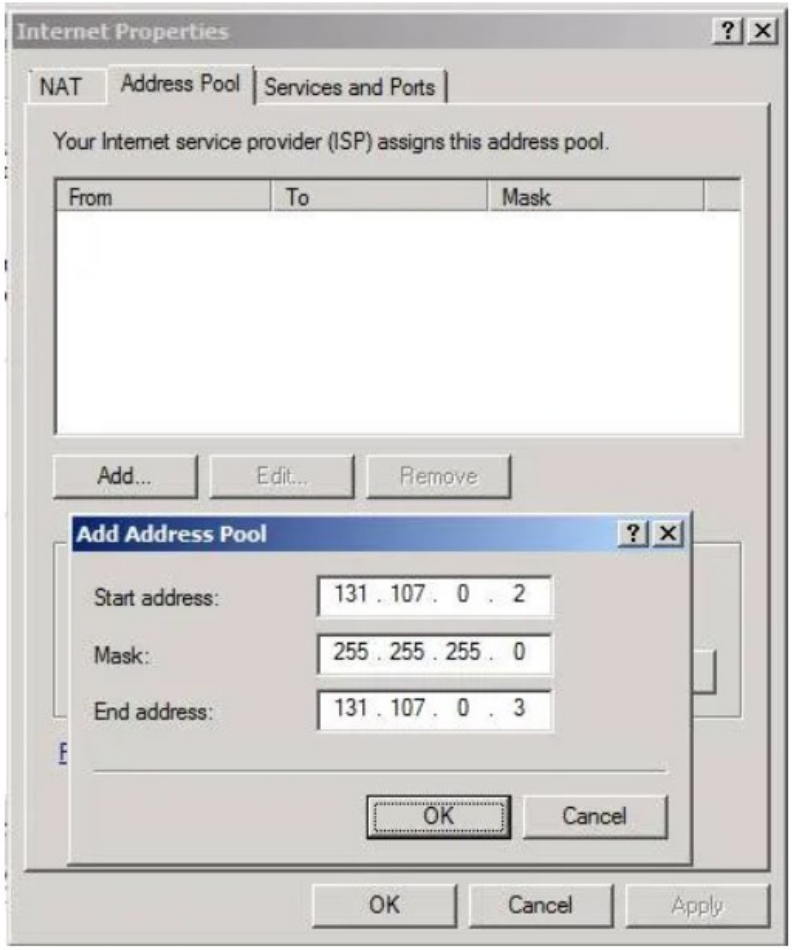
Конфигуриране на Windows Server за NAT



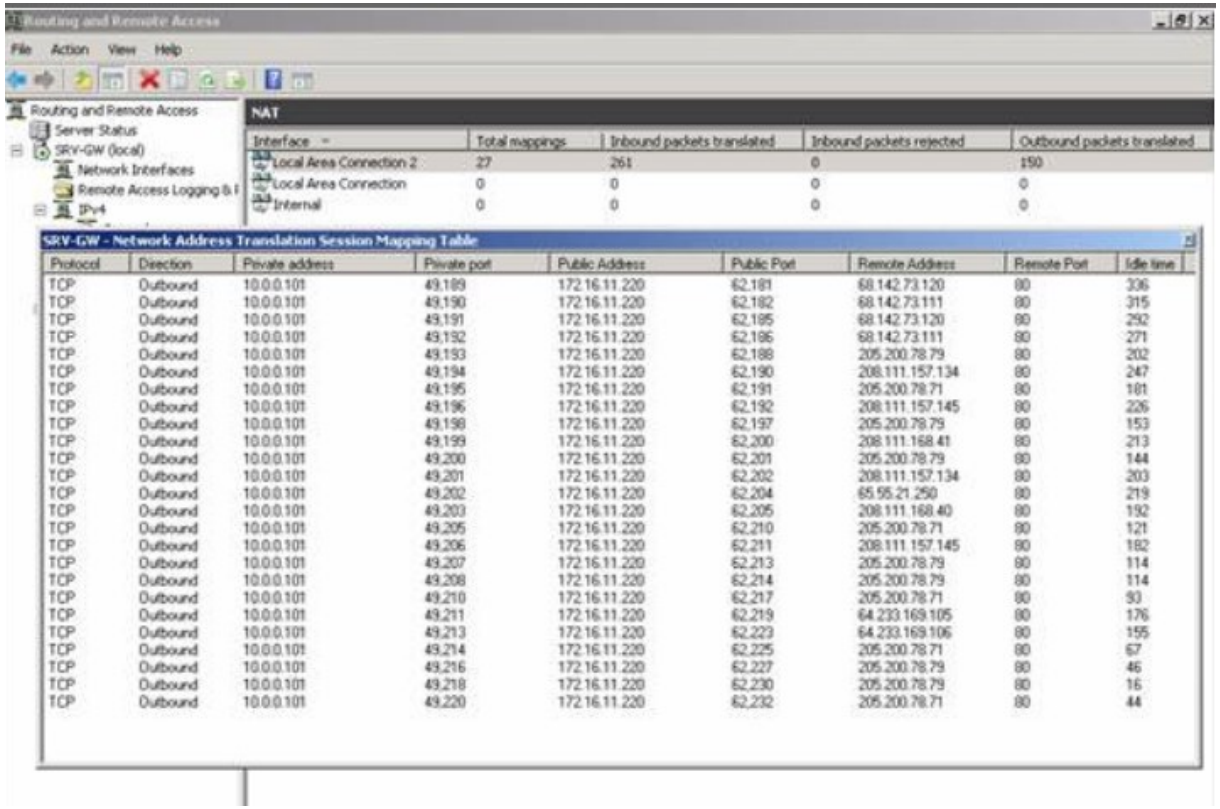
След конфигурирането трябва да се появи и ролята NAT в конзолата RRAS. Проверява се за коректност на настройката на публичния интерфейс и разрешаване на NAT на него (от **Properties**).

Конфигуриране на Windows Server за NAT

Ако ще се използват няколко публични IP адреса за транслиране, се задава адресен пул.

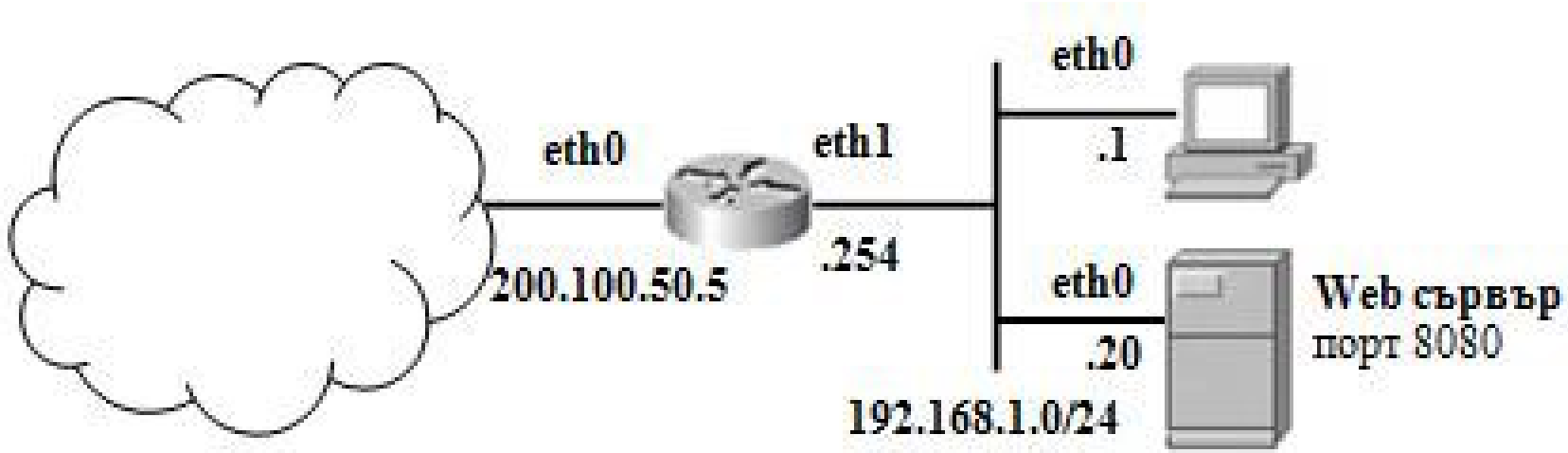


Проверка за функциониране на NAT



Избира се интерфейса и с **Show mapping** се наблюдава транслирането.

Предоставяне на услуги от вътрешна мрежа

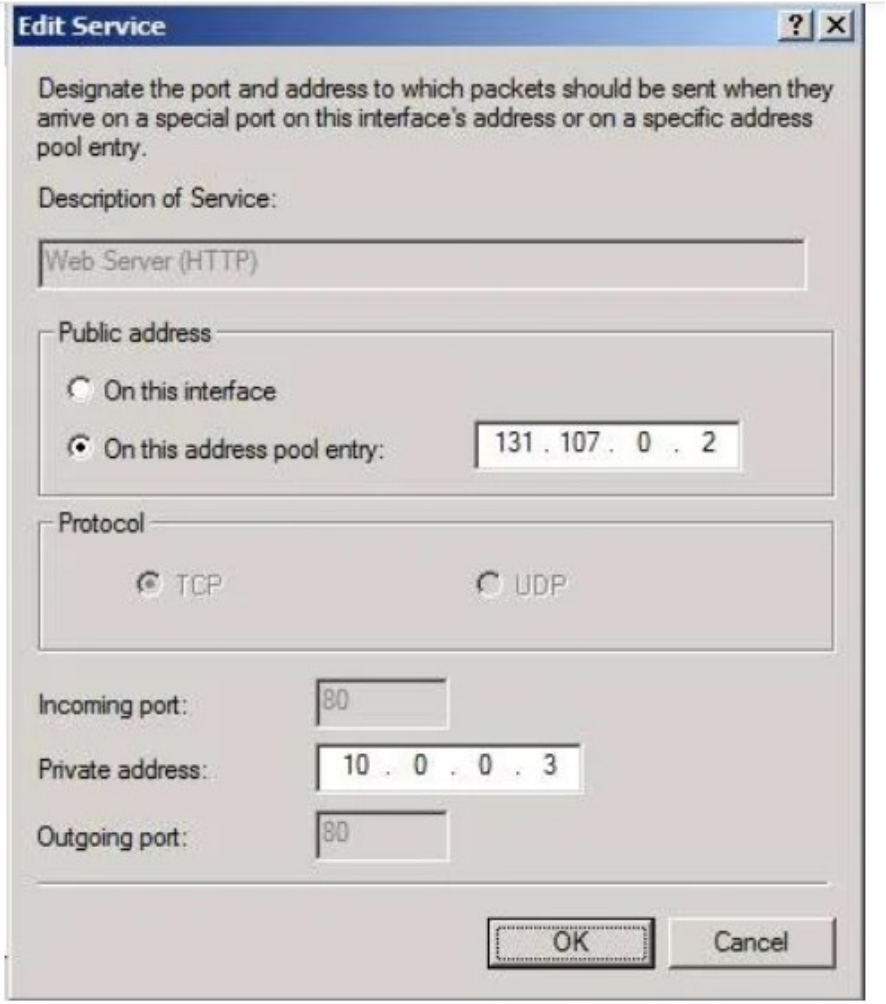


Редиректване на портове

От **Properties** на интерфейса се отваря **Services and Ports**. Избира се съответната услуга във вътрешната мрежа. Ако е специфична, може да се добави.

Редиректване на портове

От **Edit** се конфигурира редиректването към вътрешната машина.



Въпроси?