NAT

проф. д-р инж. Венета Алексиева

Основни моменти

- NAT
- Частни адреси
- Преобразуване
- Предимства и недостатъци
- PAT
- Конфигуриране на NAT с IPtables

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.

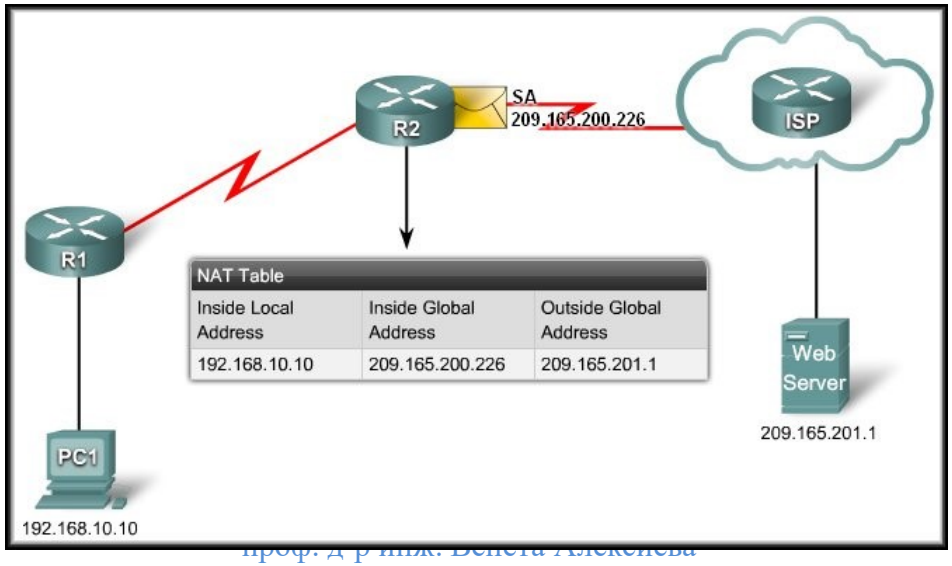
Частни адреси

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

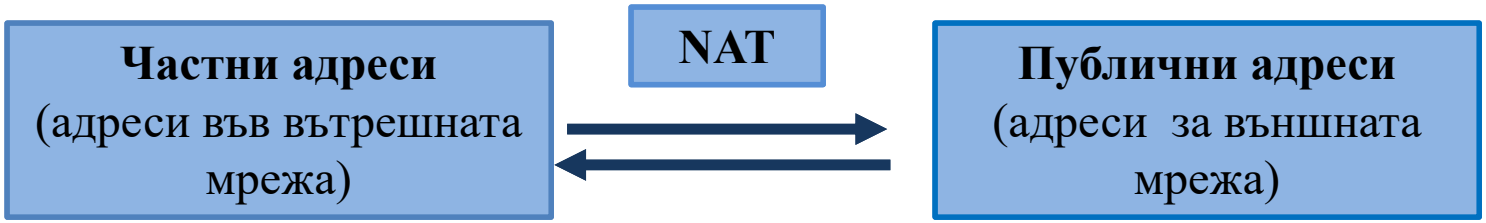
- Те са само за вътрешни мрежи за частна употреба.
- Съгласно RFC 1918 тези адреси не се маршрутизират в Интернет

Проблеми

- Частните адреси не се маршутизират в 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.



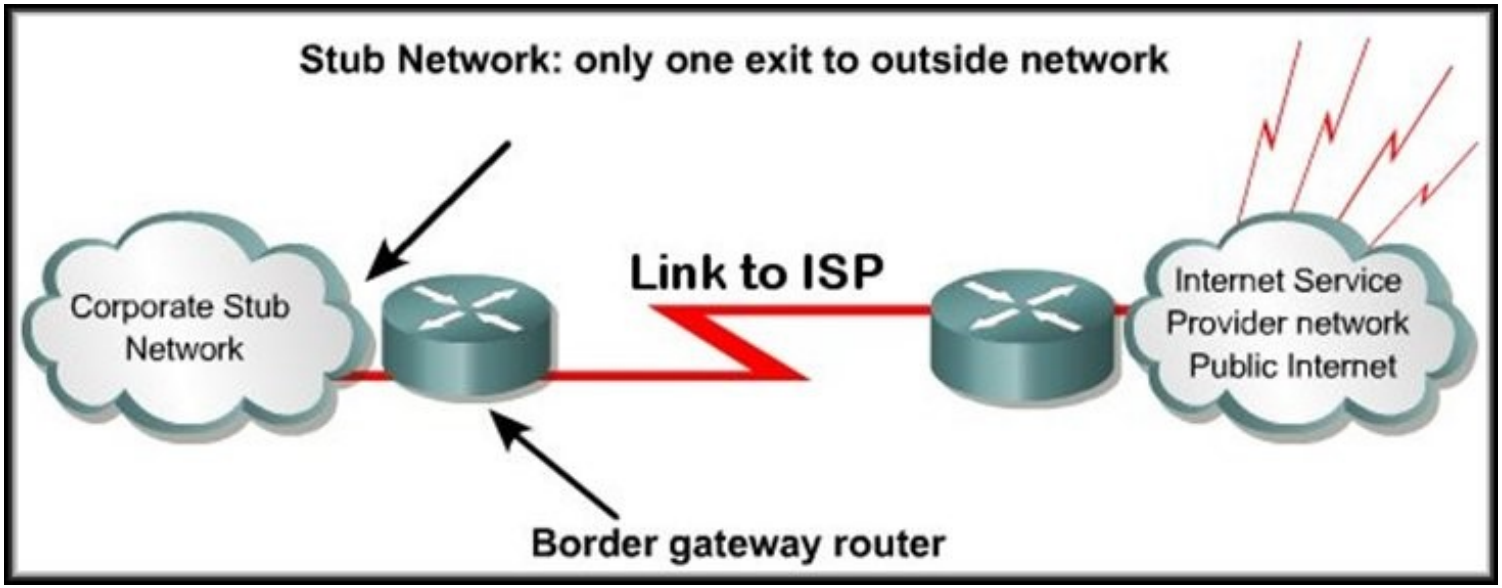
Същност на NAT



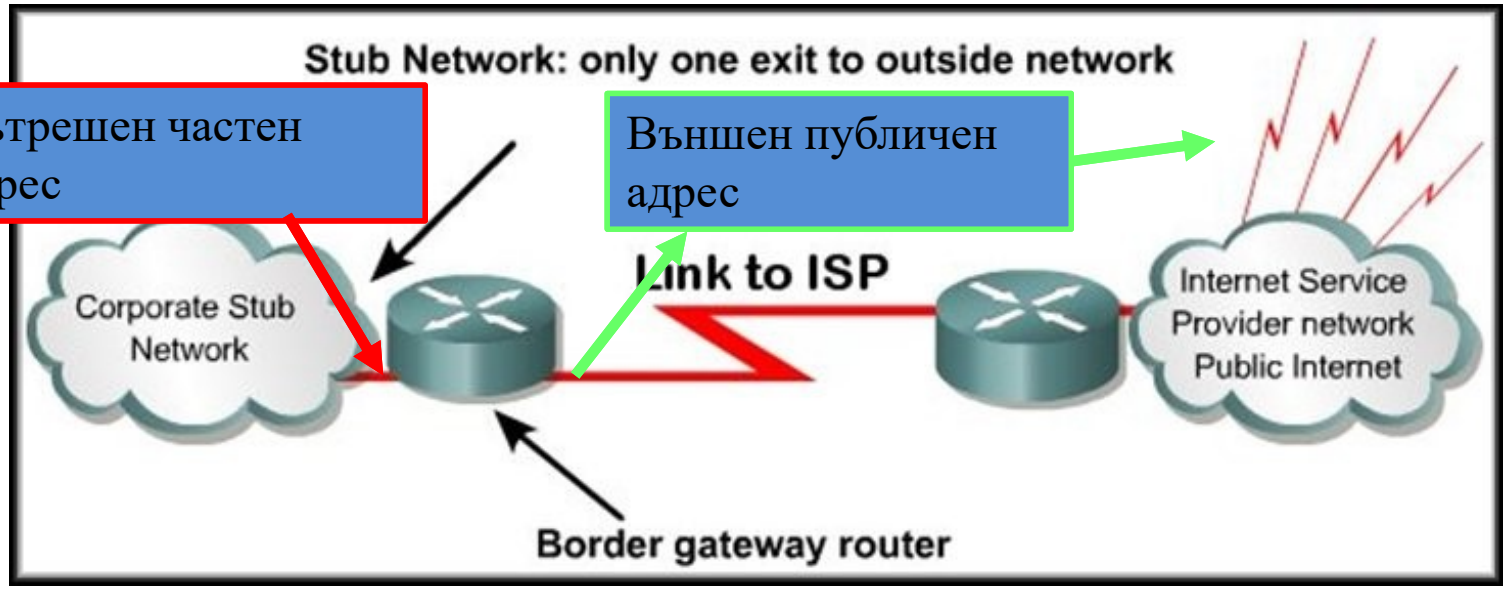
- NAT преобразува вътрешния IP адрес на клиента във външен адрес.
- Когато е конфигуриран NAT на маршрутизатора, той има >=1 публични адреса за външната мрежа.
- За външните потребители, целият трафик от тази мрежа изглежда сякаш идва от 1 адрес (или pool).

Stub мрежа

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

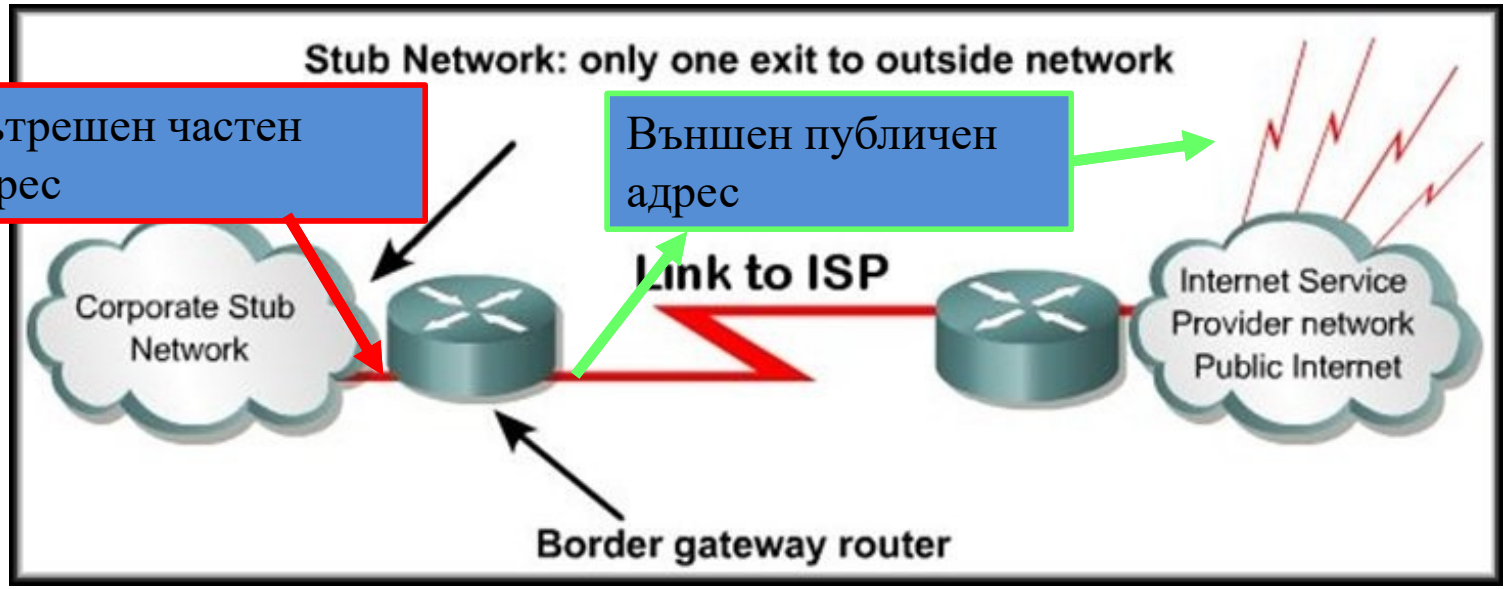


Действие на NAT



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

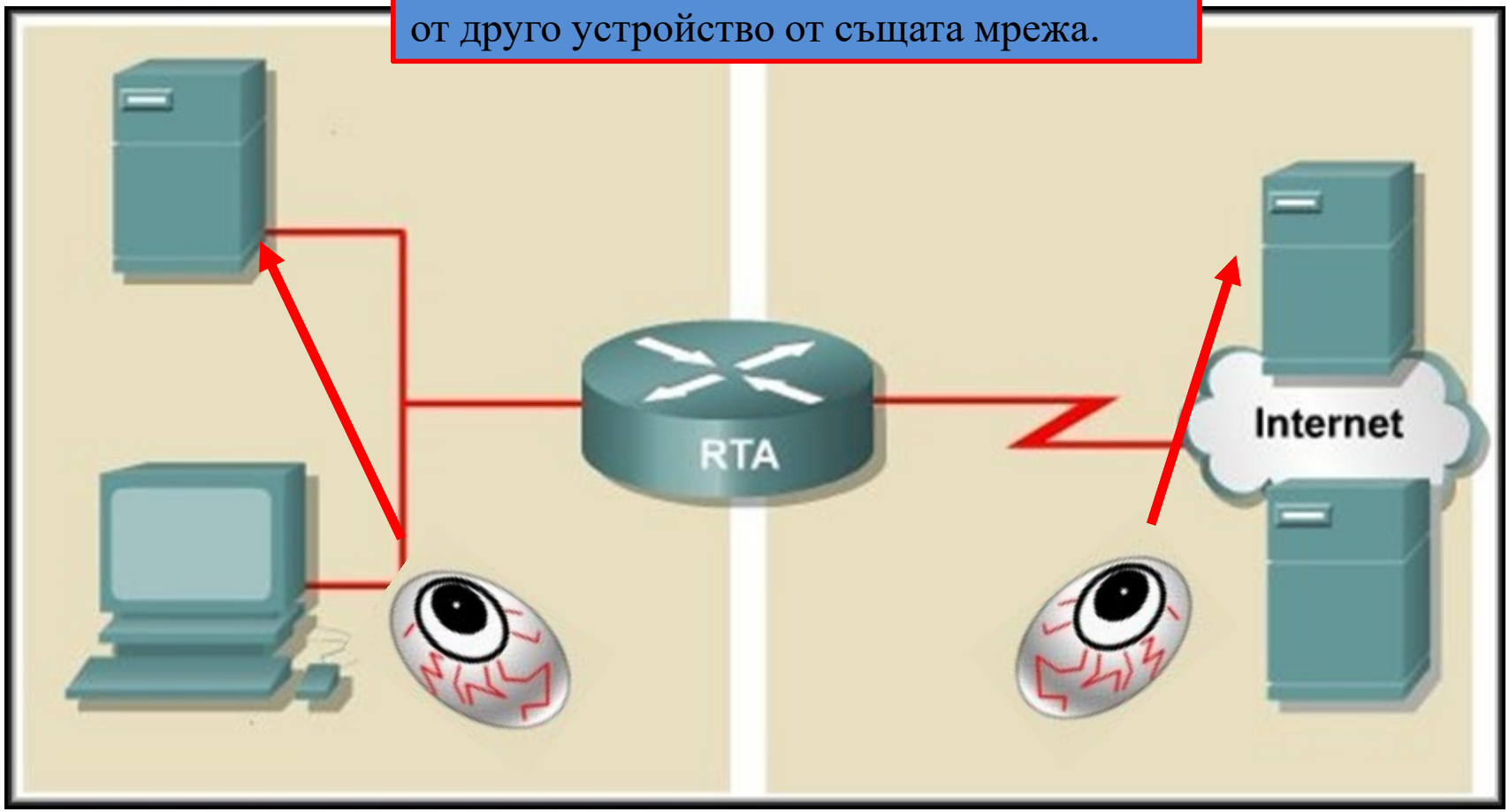
Действие на NAT



- Преобразуването става с помощта на вътрешна таблица за транслиране.
- Съдържанието ѝ зависи от типа на преобразуването, което е избрано: static NAT, dynamic NAT или Port Address Translation (PAT).

NAT терминология

Локални адреси
Как устройствата в мрежата се “виждат” от друго устройство от същата мрежа.



NAT терминология

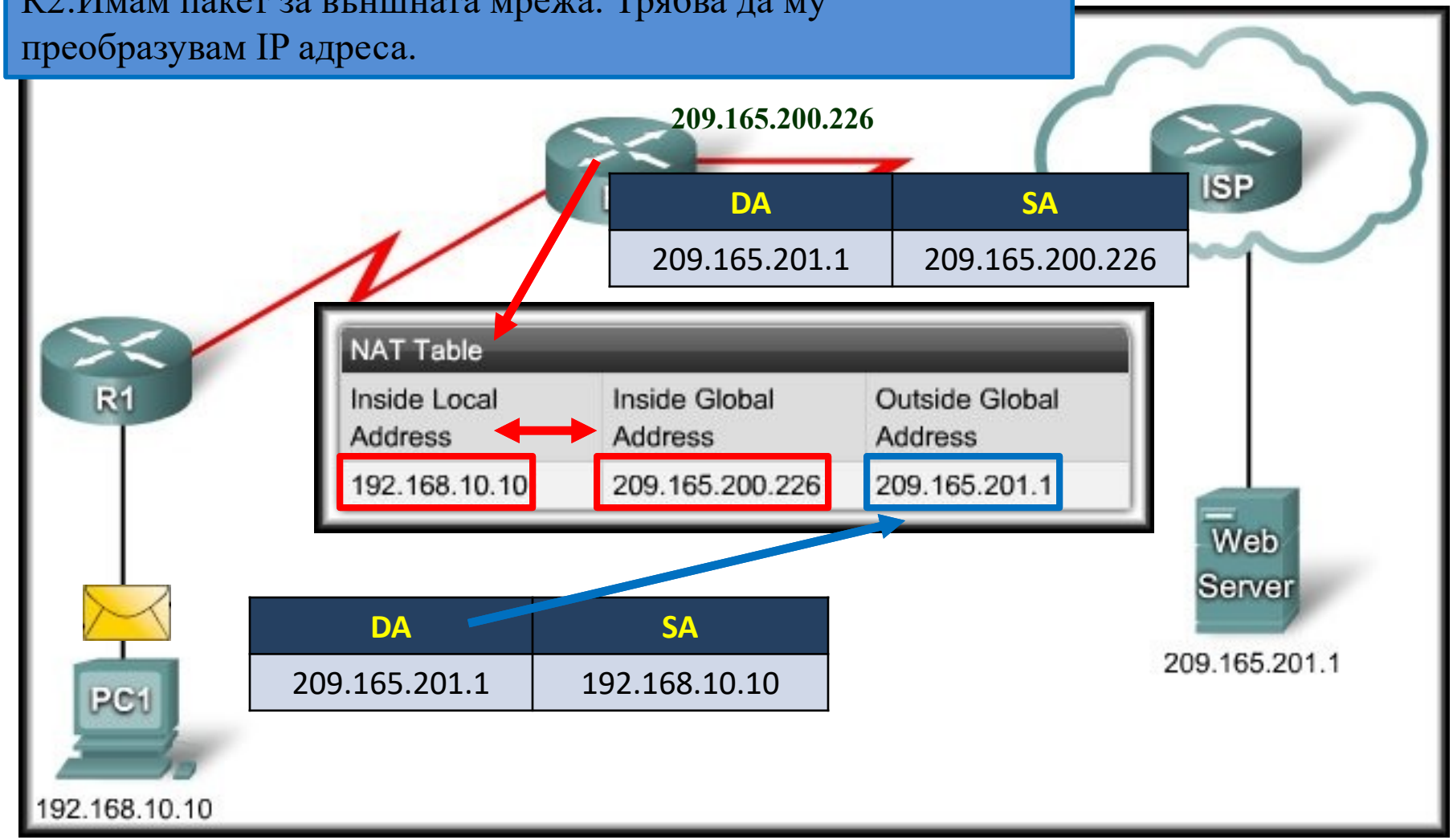
Глобални адреси:
Как устройствата в едната мрежа се “виждат” от друго устройство от другата мрежа.

NAT терминология

- **Inside Local Address:**
  - Съгласно RFC 1918 адресите се присвояват на хост във вътрешната мрежа.
- **Inside Global Address:**
  - Валиден публичен адрес, който хостът от вътрешната мрежа получава когато той излиза от маршрутизатора.
- **Outside Global Address:**
  - Достъпен IP адрес, присвоен на хоста в Internet.
- **Outside Local Address:**
  - Локален адрес, присвоен на хоста във външната мрежа.

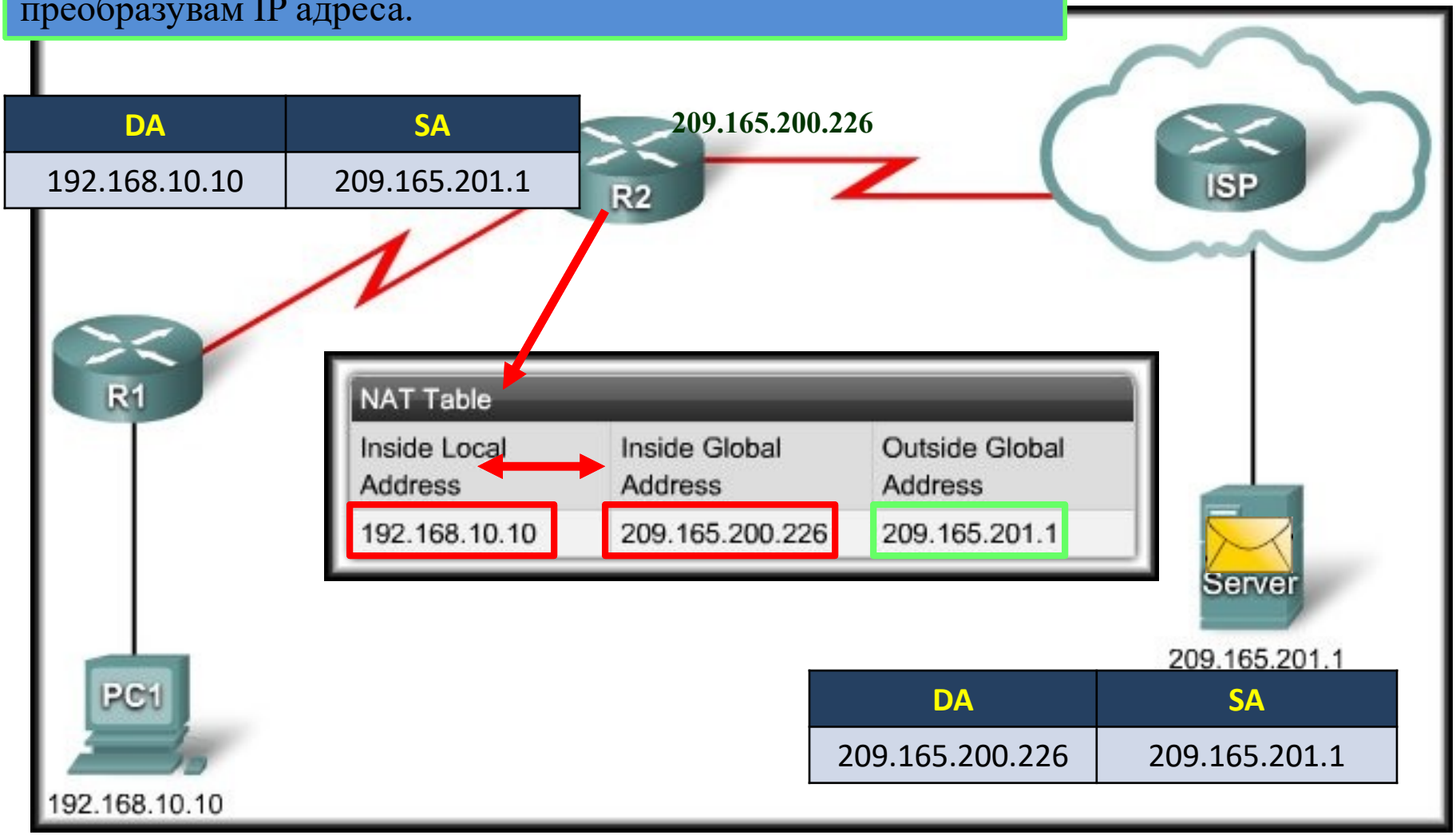
NAT таблица -изпращане

R2:Имам пакет за външната мрежа. Трябва да му преобразувам IP адреса.



NAT таблица -получаване

R2: Имам пакет за вътрешната мрежа. Трябва да му преобразувам IP адреса.



Статичен мапинг

- Съответствието е 1:1 на локален към глобален адрес.
- Само хостовете, чиито адреси са описани в таблицата ще получат външен адрес.
- Броят на външните адреси ограничава броя на хостовете, които могат да ги ползват едновременно.
- Ако хостът не се добави в таблицата, няма да получи външен адрес.

NAT Table	
Inside Local	Inside Global
10.0.0.1	179.9.8.81
10.0.0.2	179.9.8.82
10.0.0.3	179.9.8.83
10.0.0.4	179.9.8.84
10.0.0.5	179.9.8.85
10.0.0.6	179.9.8.86

Динамичен мапинг

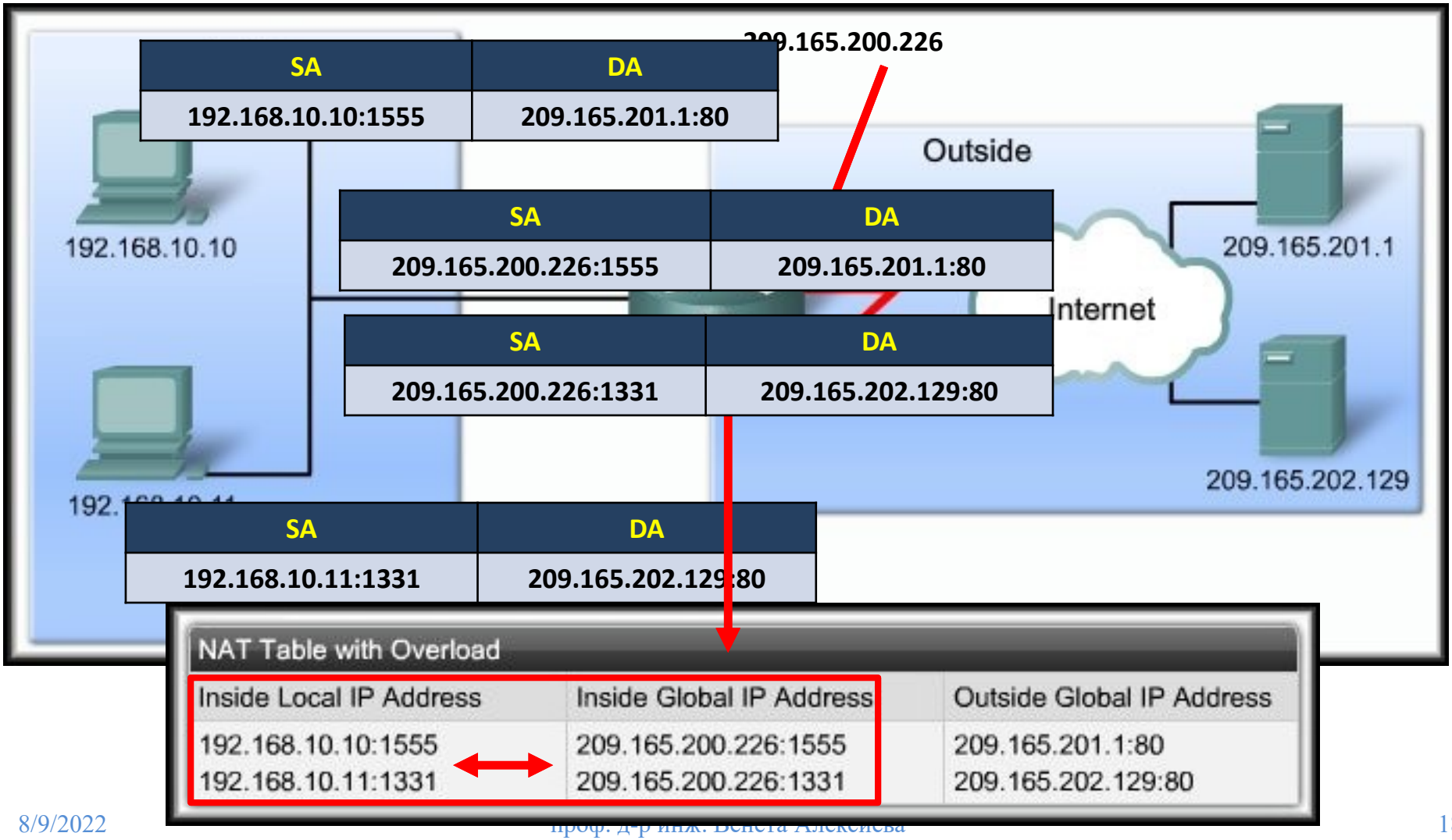
- Свързва локален адрес динамично към адрес от пул с глобални адреси.
- Хостовете, които едновременно могат да ползват NAT са ограничени от броя на адресите в пула.
- NAT устройството динамично присвоява адреси при получаване на заявка. Когато сесията приключи, адресът се връща в пула и може да бъде отдаден на друг.

NAT Table	
Inside Local	Inside Global
10.0.0.1	179.9.8.81
10.0.0.2	
10.0.0.3	
10.0.0.4	
10.0.0.5	
10.0.0.6	179.9.8.86

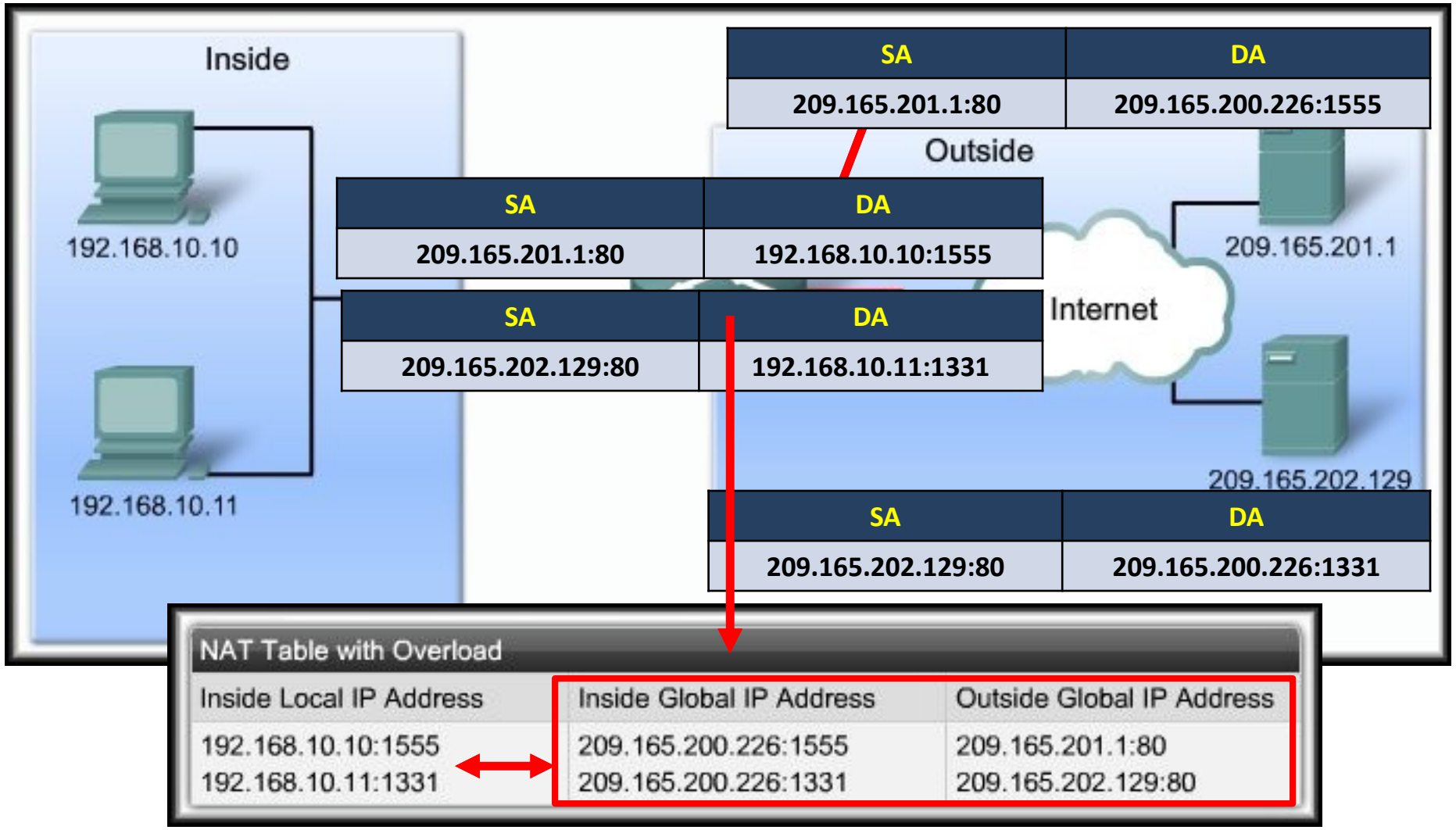
PAT

- Позволява вместо пул да се ползва само 1 публичен IP адрес, към който може да се свържат до 65,536 вътрешни хоста.
- Модифицира TCP/UDP source port при записването на вътрешния хостов адрес.
- Използва и преобразува :
  - Source IP Address.
  - Destination IP Address.
  - TCP/UDP Source Port Number.
- По този начин се идентифицира уникално всяка конекция за всеки поток от трафик.

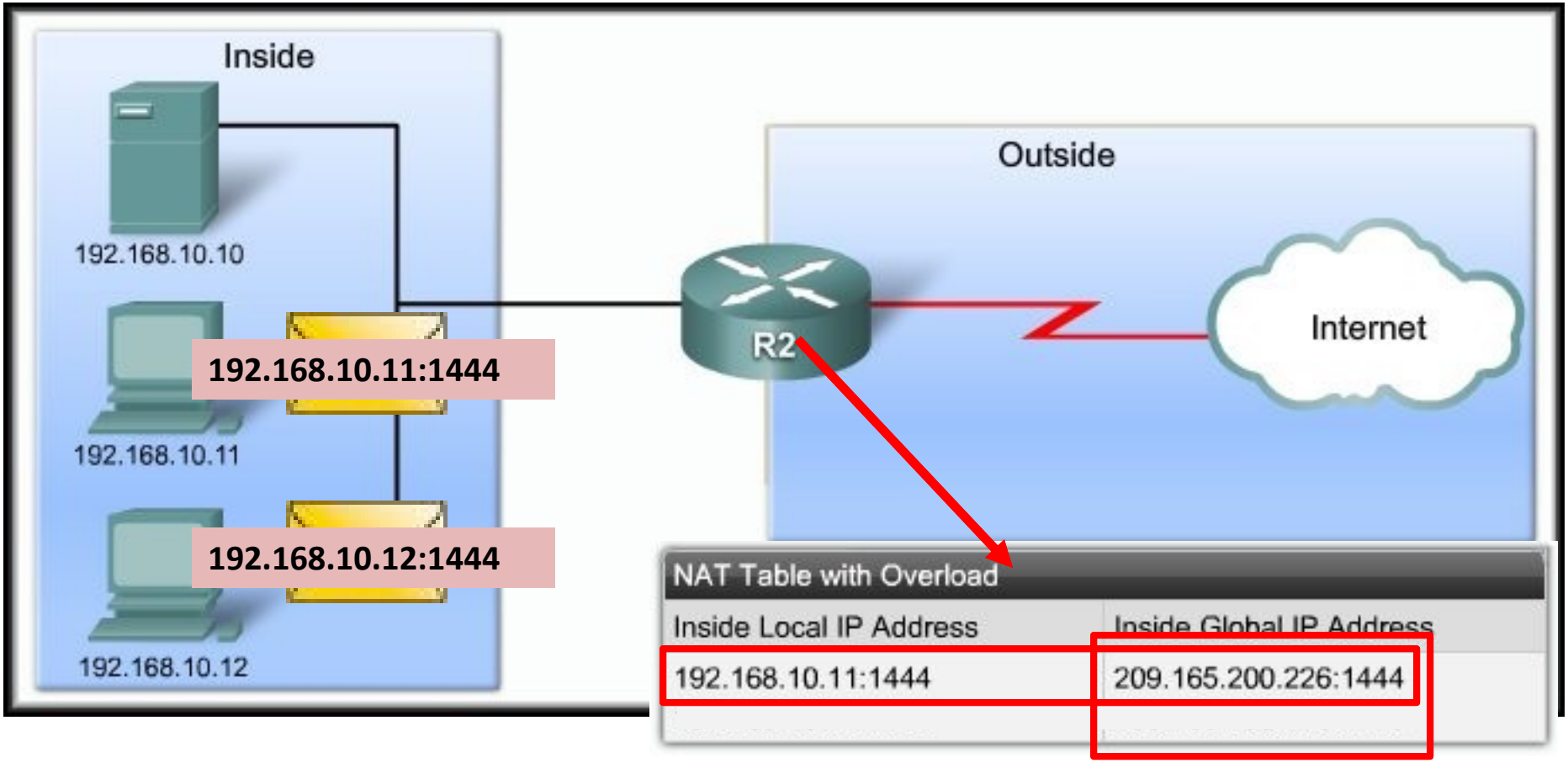
PAT- изпращане



PAT- получаване



PAT – използване на следващ свободен порт



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

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.
- Създаване на TCP конекции може да се прекъсне.
- Може да се наложи мрежовата архитектура да се изгради наново.

Masquerading – статичен NAT

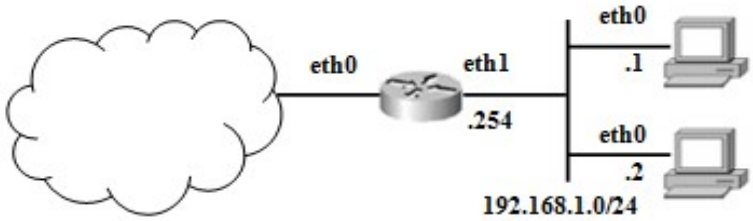
- NAT от тип 1:1:
  - адресът, с който се транслира, е този на външния интерфейс на маршрутизатора
  - не е необходимо да се указва NAT адрес
  - улеснява конфигурирането при използване на автоматично конфигуриране с DHCP.

1. Зарежда се модулът *iptables_nat*
2. Разрешава се маршрутизирането:

   # echo 1 > /proc/sys/net/ipv4/ip_forward

1. Конфигурира се на верига POSTROUTING.
2. На FORWARD веригата трябва:
   1. пакетите, които се отнасят до изходящи NEW и ESTABLISHED конекции да се разрешат,
   2. да се разрешат единствено пакетите на входящите ESTABLISHED конекции.
   3. Това защитава вътрешната мрежа от опити за иницииране на конекции от Интернет.

Конфигуриране на NAT



modprobe iptable_nat

modprobe ip_conntrack

iptables –P INPUT DROP

iptables –P OUTPUT ACCEPT

iptables –P FORWARD ACCEPT

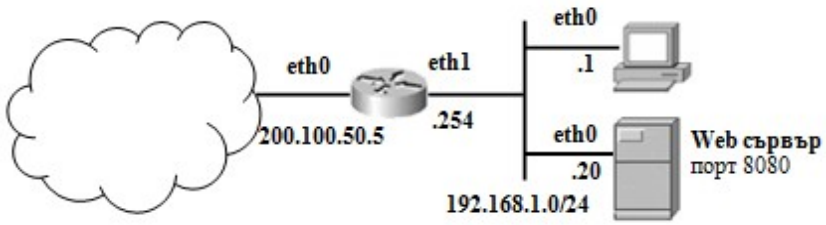
iptables -A POSTROUTING -t nat -o eth0 –s 192.168.1.0/24 -d 0/0 -j MASQUERADE

iptables -A FORWARD -t filter -o eth0 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

iptables -A FORWARD -t filter -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

Редиректване на портове

Да се разреши редиректване на трафика, предназначен за порт 80 на адреса на маршрутизатора, към порт 8080 на сървъра 192.168.1.20



modprobe iptable_nat

modprobe ip_conntrack

iptables –P INPUT DROP

iptables –P OUTPUT ACCEPT

iptables –P FORWARD ACCEPT

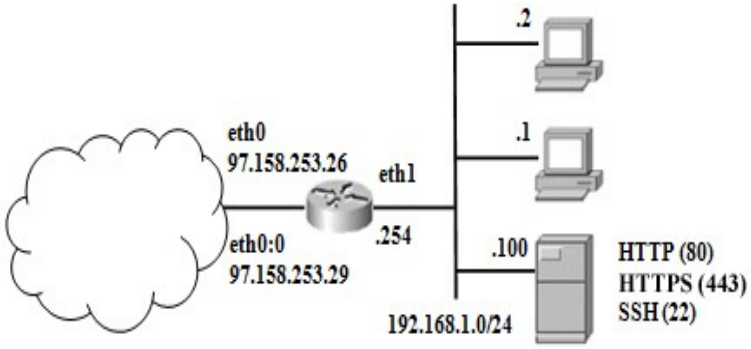
iptables -t nat -A PREROUTING -p tcp -i eth0 –d 200.100.50.5 --dport 80 --sport 1024:65535 -j DNAT --to 192.168.1.20:8080

iptables -A FORWARD -p tcp -i eth0 -o eth1 -d 192.168.1.20 --dport 8080 --sport 1024:65535 -m state --state NEW -j ACCEPT

iptables -A FORWARD -t filter -o eth0 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

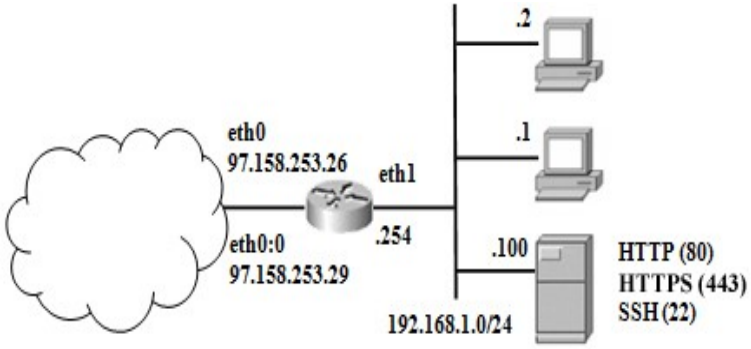
iptables -A FORWARD -t filter -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

Статичен NAT



- Използва се NAT от типа 1:1, чрез който сървърът от вътрешната мрежа с адрес 192.168.1.100 ще се представя в Интернет като 97.158.253.26.
- Създават се множество N:1 NAT за вътрешната мрежа 192.168.1.0, в която всички останали машини ще се представят в Интернет като адрес 97.158.253.29.
- Трябва да се създадат логически интерфейси (*aliases*) за публичния IP адрес за NAT N:1:
- # ifconfig eth0 97.158.253.26
- # ifconfig eth0:0 97.158.253.29

Статичен NAT



iptables -t nat -A PREROUTING -d 97.158.253.26 -i eth0 -j DNAT --to-destination 192.168.1.100

iptables -t nat -A POSTROUTING -s 192.168.1.100 -o eth0 -j SNAT --to-source 97.158.253.26

iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -j SNAT -o eth0 --to-source 97.158.253.29

iptables -A FORWARD -p tcp -i eth0 -o eth1 -d 192.168.1.100 -m multiport --dports 80,443,22 -m state --state NEW -j ACCEPT

iptables -A FORWARD -t filter -o eth0 -m state --state NEW, ESTABLISHED, RELATED -j ACCEPT

iptables -A FORWARD -t filter -i eth0 -m state --state ESTABLISHED, RELATED -j ACCEPT

Въпроси ?

Благодаря за вниманието !