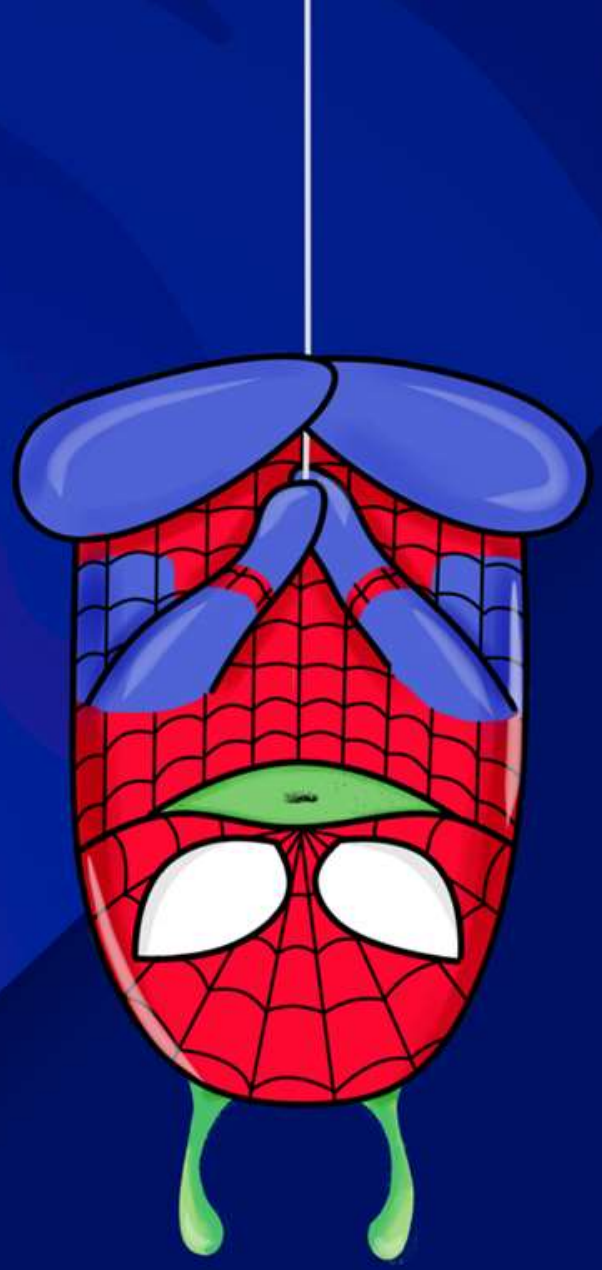
NAT



Спикер:
Роман Козлов

NAT

- Концепция NAT, его необходимость в IPv4
- Почему пока не взлетел IPv6 (IPv4 vs IPv6) - стоит ли учить IPv6
- Цепочки NAT - Prerouting – dst-nat, redirect
- Цепочки NAT - Postrouting – src-nat, masquerade
- HarpinNAT, netmap

Концепция NAT, его необходимость в IPv4

Спикер:
Роман Козлов

КОЦЕПЦИЯ NAT, ЕГО НЕОБХОДИМОСТЬ В IPv4

- **4 294 967 296** IPv4 адресов оказалось недостаточно
- С распространением персональных вычислений, мобильных устройств, рост интернета в 4,3 миллиарда адресов IPv4 будет недостаточно
- Долгосрочным решением было IPv6, но требовались более быстрое решение для устранения нехватки адресов. И этим решением стал NAT (Network Address Translation)
- RFC 1631 / 3022
- Связанное RFC 1918
- Ломает прямую модель подключения (end to end connectivity model)

NAT

Правила NAT находится в таблице NAT, изменения в заголовке пакета адреса назначения происходит в цепочке PREROUTING, а изменения адреса источника происходят в цепочке POSTROUTING

RAW	MANGLE	NAT	FILTER	SECURITY
PREROUTING	PREROUTING	PREROUTING	INPUT	INPUT
OUTPUT	INPUT	INPUT	FORWARD	FORWARD
	FORWARD	OUTPUT	OUTPUT	OUTPUT
	OUTPUT	POSTROUTING		
	POSTROUTING			

iptables –t nat

01

Работа по принципу «Если-то»

02

Упорядочены в цепочки

03

Существуют предопределенные цепочки

04

Пользователи могут создавать собственные цепочки

iptables –t nat -L

Это предопределенные цепочки

- **PREROUTING** (Цепочка до решения о маршрутизации)
- **INPUT** (Пакеты, предназначенные HOST)
- **OUTPUT** (Пакеты, сгенерированные HOST)
- **POSTROUTING** (Цепочка после решения о маршрутизации)

iptables

Просмотр таблиц и цепочек

```
iptables [-t имя таблицы] [-L имя цепочки]
```

```
root@ubuntu22-server:~# iptables -S -t nat -v
-P PREROUTING ACCEPT -c 104 20210
-P INPUT ACCEPT -c 30 9041
-P OUTPUT ACCEPT -c 273 16789
-P POSTROUTING ACCEPT -c 34 2238
-A POSTROUTING -o ens3 -c 2 168 -j SNAT --to-source 192.0.2.254
```

```
iptables -S [-t имя таблицы]
```

```
root@ubuntu22-server:~# iptables -S -t nat
-P PREROUTING ACCEPT
-P INPUT ACCEPT
-P OUTPUT ACCEPT
-P POSTROUTING ACCEPT
-A POSTROUTING -o ens3 -j SNAT --to-source 192.0.2.254
```

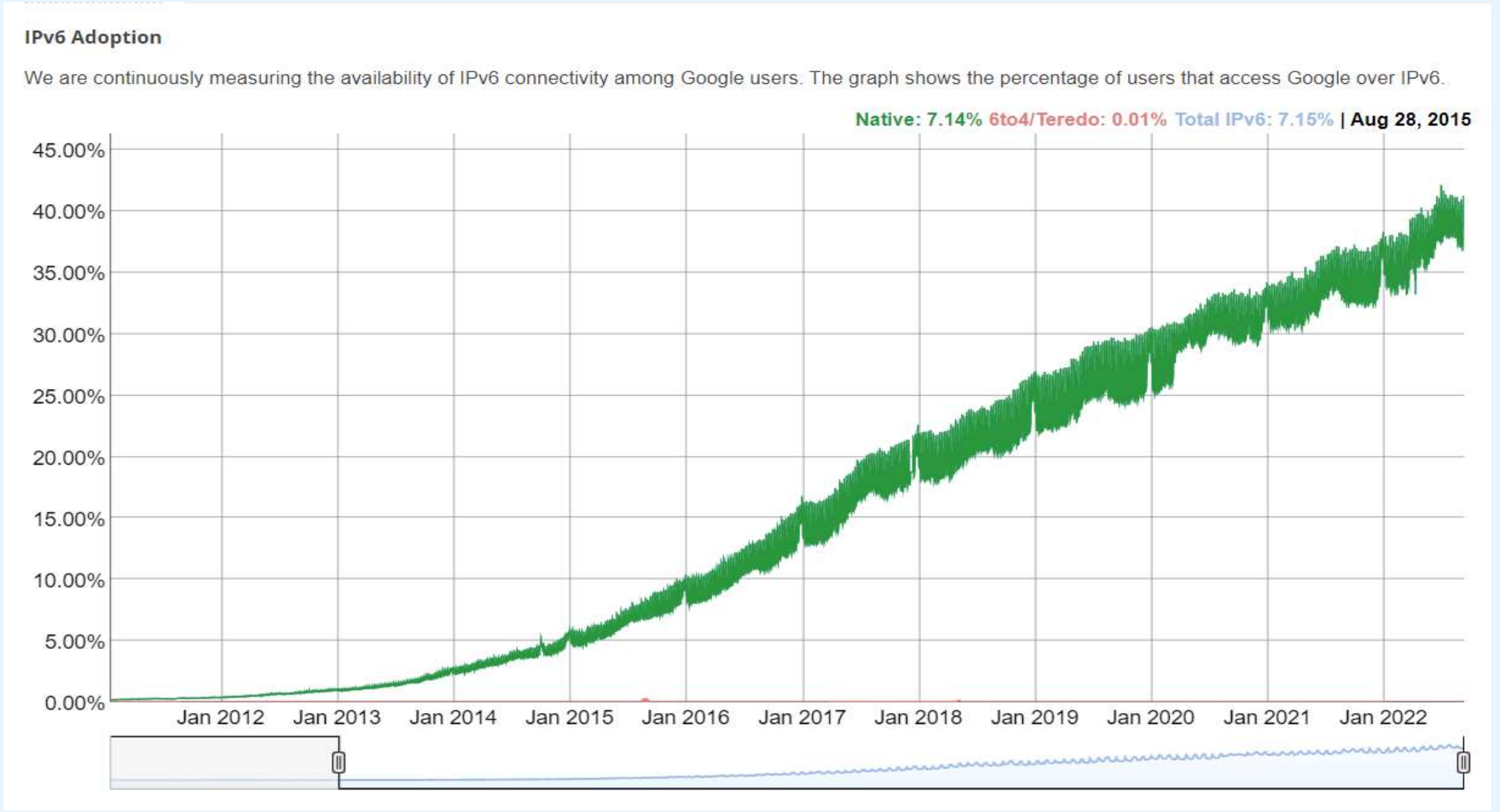
Добавление правил

```
iptables -t таблица действие цепочка дополнительные_параметры
```

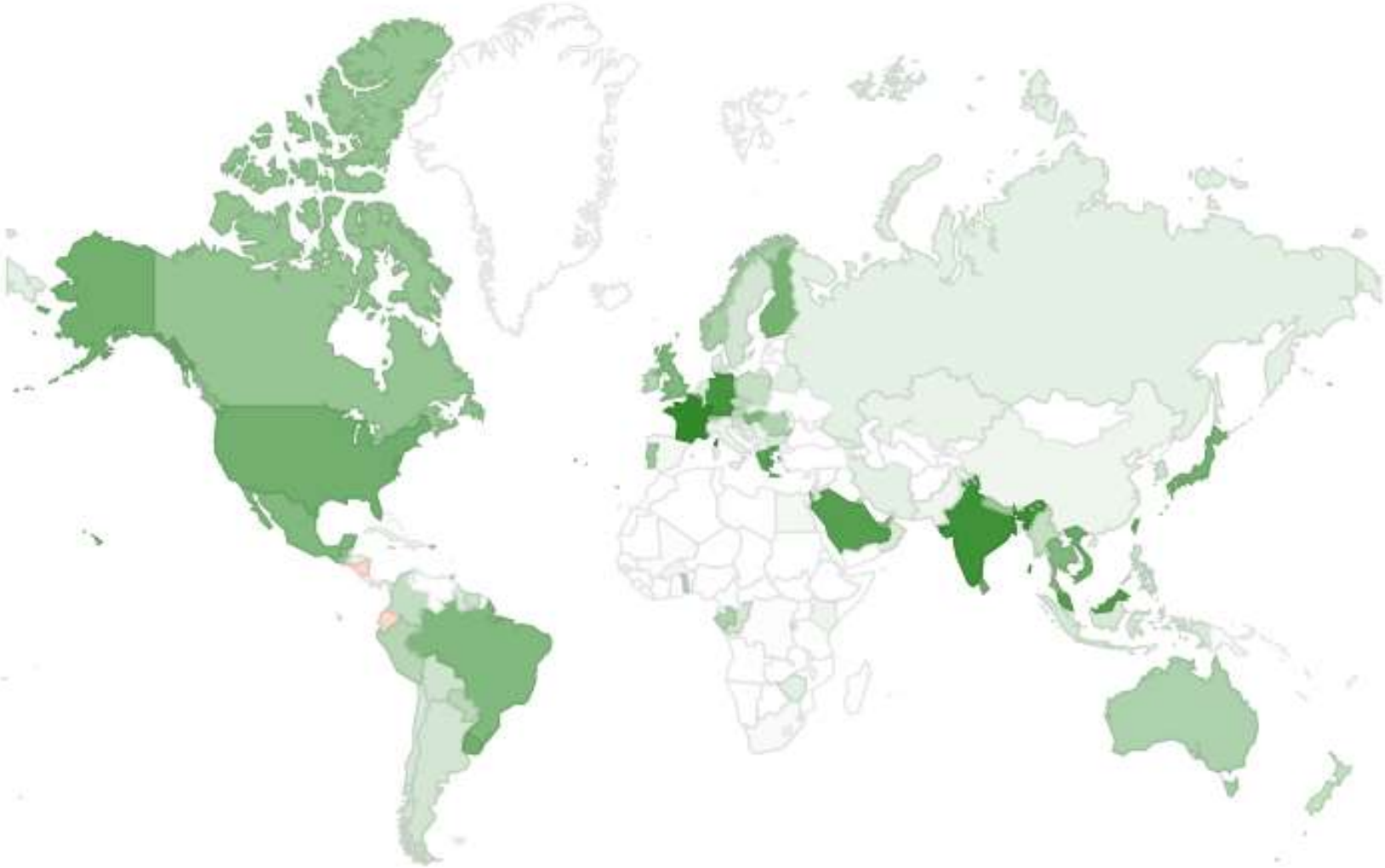
Почему пока не взлетел IPv6 (IPv4 vs IPv6) - стоит ли учить IPv6

Спикер:
Роман Козлов

РАСПРОСТРАНЕНИЕ IPv6



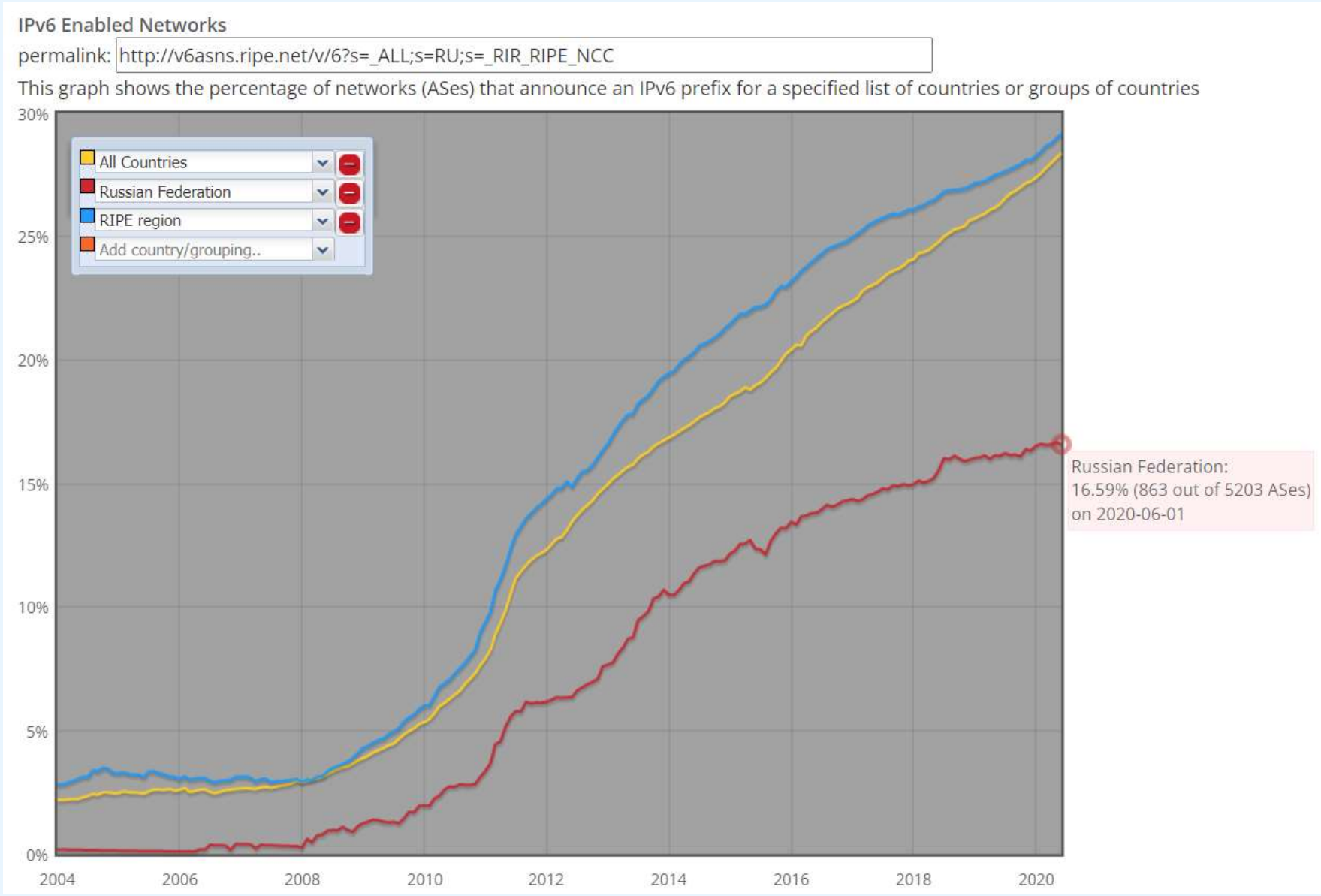
РАСПРОСТРАНЕНИЕ IPv6



СЛОЖНОСТИ С ВНЕДРЕНИЕМ IPv6 У ОПЕРАТОРОВ СВЯЗИ

- Требуется частичная или полная замена оборудования с полноценной поддержкой IPv6
- Переработка схемы учета трафика и схемы ограничения скоростей для абонентов
- Обучение персонала работе с новым протоколом
- Одновременная поддержка двух протоколов IP
- Отсутствие прямых выплат от абонентов за использование IPv6
- При дальнейшем переходе на IPv6-only поддержка схем работы NAT4to6, NAT6to4
- Переработка схемы работы с СОРМ и списками Роскомнадзора

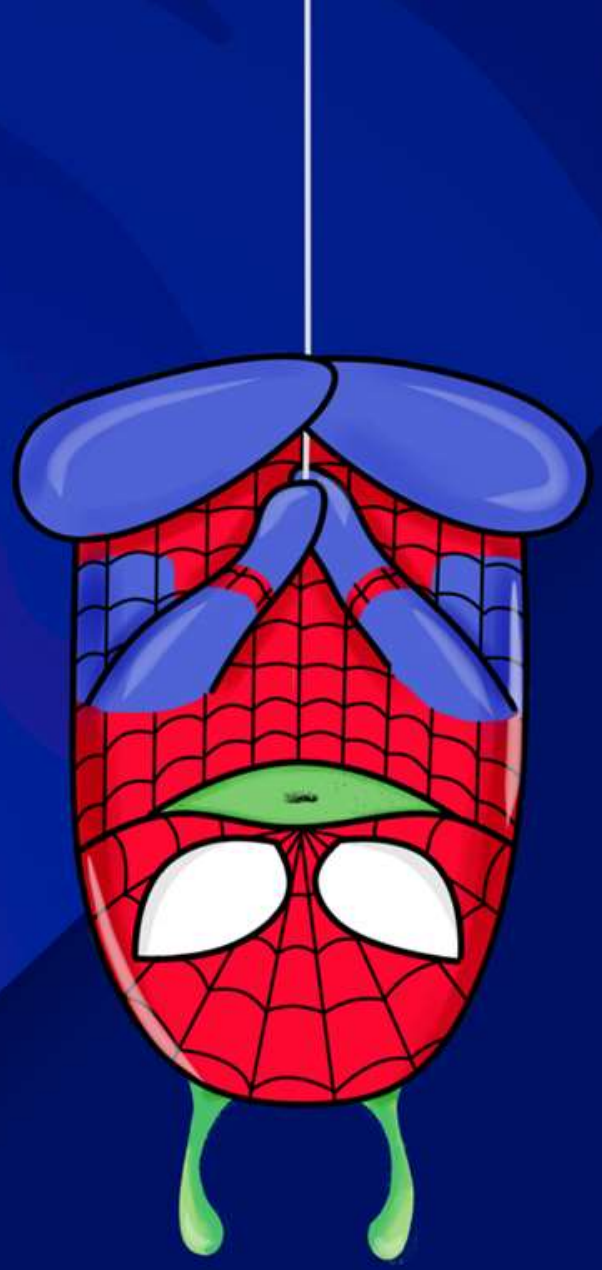
СЛОЖНОСТИ С ВНЕДРЕНИЕМ IPv6 У ОПЕРАТОРОВ СВЯЗИ



ПЛЮСЫ ОТ ПЕРЕХОДА НА IPv6

- Отсутствие необходимости постоянной покупки IPv4 адресов
- Полная связанность всех устройств
- Отсутствие проблем с протоколами не поддерживающими NAT (SIP, FTP)
- Снижение нагрузки на NAT маршрутизаторы у операторов связи
- Полноценно работающий IPSEC и прочие протоколы требующие прямой связанности устройств
- Отказ от local net и повсеместное использование Global Unicast адресов
- Не нужно настраивать локальные адреса и заботиться о пересечении корпоративных сетей

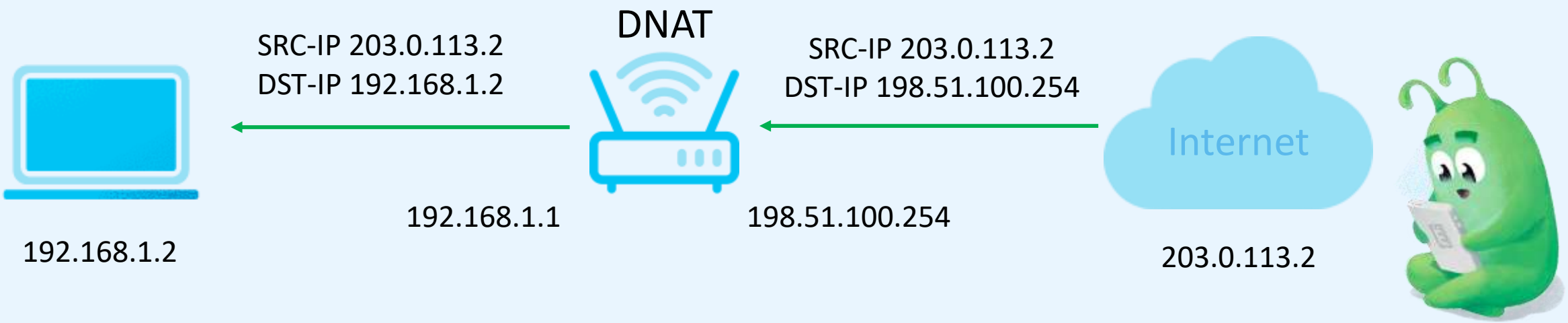
Цепочки NAT - Prerouting - dst-nat,redirect



Спикер:
Роман Козлов

PREROUTING ПОЛУЧЕНИЯ ДОСТУПА К ЛОКАЛЬНЫМ РЕСУРСАМ

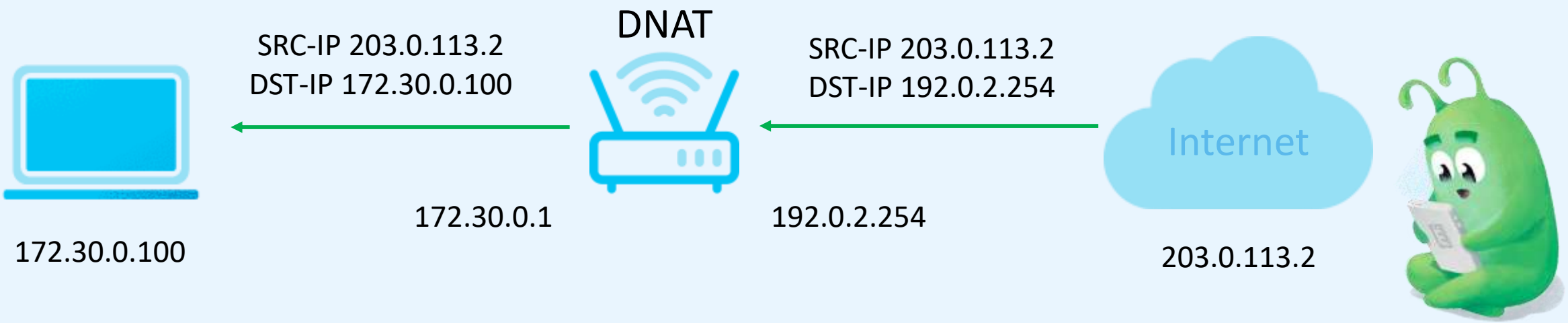
- Обычно используется для обеспечения доступа из внешней сети на локальный ресурс (dst-nat или проброс порта)
- Заменяет в заголовках пакетов адреса назначения



iptables -t nat -A PREROUTING DNAT

Правило для доступа к веб-серверу с внешнего интерфейса ens3 находящегося в локальной сети на адресе 172.30.0.100

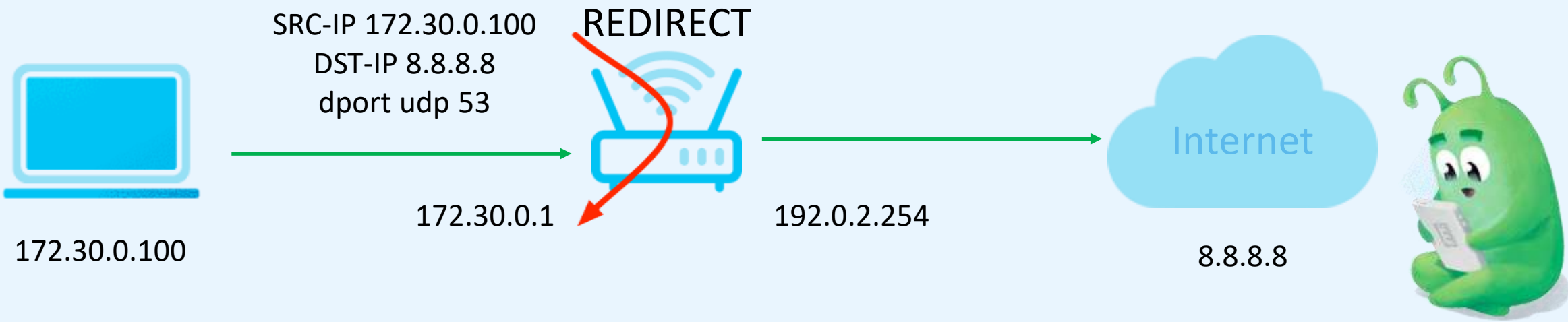
```
iptables –t nat -A PREROUTING -i ens3 -p tcp -m tcp --dport 80 -j DNAT --to-
destination 172.30.0.100:80
```



iptables -t nat -A PREROUTING REDIRECT

- **Особый тип DNAT позволяющий отправить пакеты на сам HOST**
- **Используется для подмены прозрачных запросов DNS, HTTP**

```
iptables -t nat -A PREROUTING -p udp -i ens4 -m udp --dport 53 -j REDIRECT
```



iptables -t nat -A PREROUTING

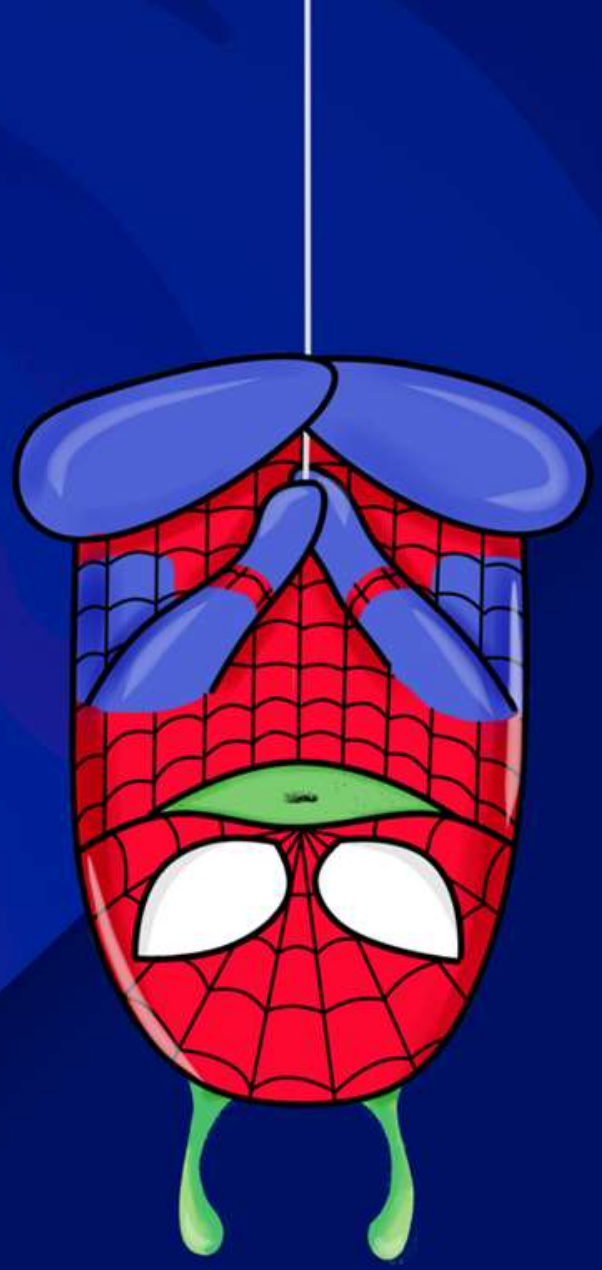
iptables -L PREROUTING -t nat -n -v

```
root@ubuntu22-server:~# iptables -L PREROUTING -t nat -n -v
Chain PREROUTING (policy ACCEPT 159 packets, 30821 bytes)
 pkts bytes target     prot opt in     out     source               destination
    1    60 DNAT       tcp  --  ens3   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80 to:172.30.0.100
    0     0 DNAT       tcp  --  ens3   *       0.0.0.0/0            0.0.0.0/0            tcp dpt:80 to:172.30.0.100:8080
```

iptables -S -t nat

```
root@ubuntu22-server:~# iptables -S -t nat
-P PREROUTING ACCEPT
-P INPUT ACCEPT
-P OUTPUT ACCEPT
-P POSTROUTING ACCEPT
-A PREROUTING -i ens3 -p tcp -m tcp --dport 80 -j DNAT --to-destination 172.30.0.100
-A PREROUTING -i ens3 -p tcp -m tcp --dport 80 -j DNAT --to-destination 172.30.0.100:8080
-A POSTROUTING -o ens3 -j SNAT --to-source 192.0.2.254
```

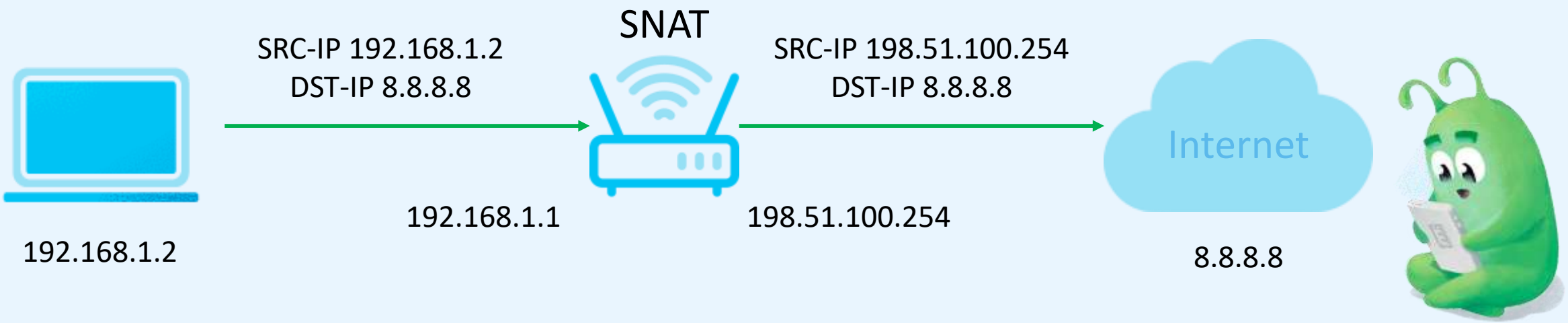
POSTROUTING выход в интернет



Спикер:
Роман Козлов

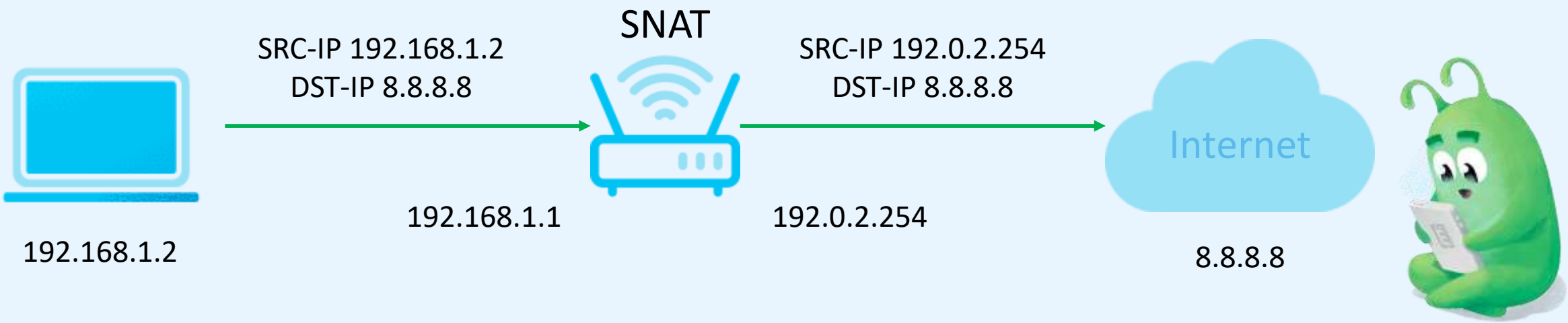
POSTROUTING ВЫХОД В ИНТЕРНЕТ

- Обычно используется для обеспечения доступа к внешней сети из локальной сети, которая использует частные IP-адреса (src-nat)
- Заменяет в заголовках пакетов адреса источника



iptables -t nat -A POSTROUTING

- **Правило для выхода из локальной сети со статическим адресом 192.0.2.254 через интерфейс ens3**
  `iptables –t nat -A POSTROUTING -o ens3 -j SNAT --to-source 192.0.2.254`
- **Правило для выхода из локальной сети без статического адреса через интерфейс ens3**
  iptables -t nat -A POSTROUTING -o ens3 -j MASQUERADE



iptables -t nat -L POSTROUTING

iptables -t nat -L POSTROUTING -n

```
root@ubuntu22-server:~# iptables -t nat -L POSTROUTING -n
Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
SNAT       all  --  0.0.0.0/0            0.0.0.0/0            to:192.0.2.254
```

iptables -S -t nat

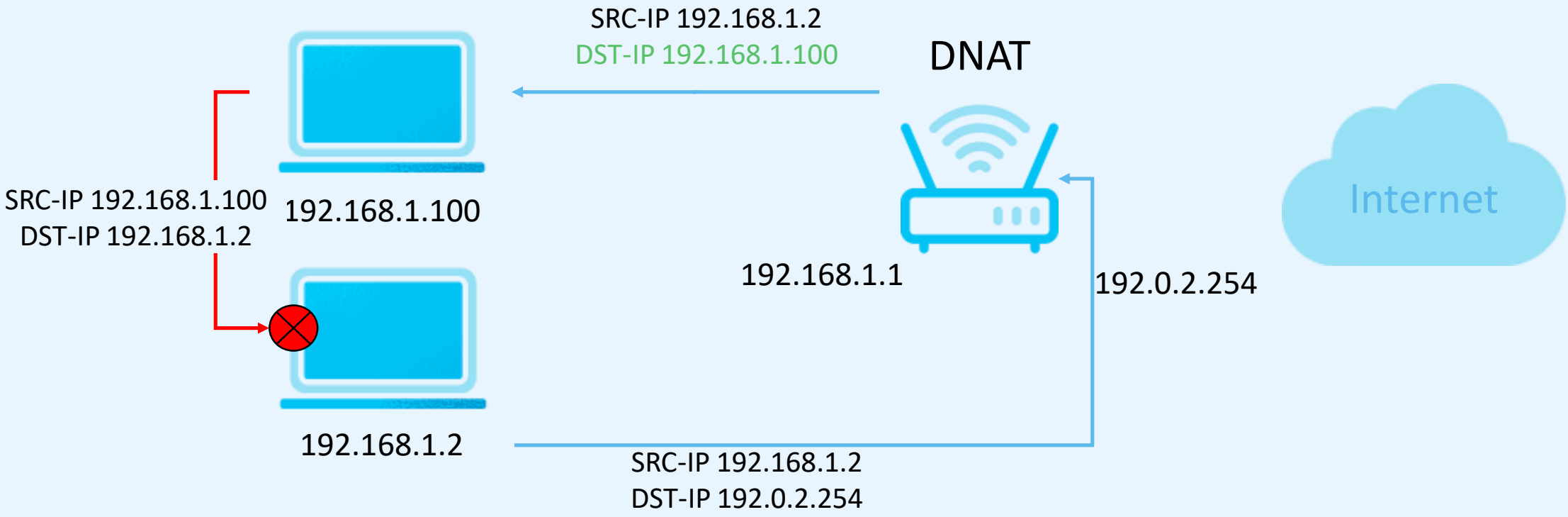
```
root@ubuntu22-server:~# iptables -S -t nat
-P PREROUTING ACCEPT
-P INPUT ACCEPT
-P OUTPUT ACCEPT
-P POSTROUTING ACCEPT
-A POSTROUTING -o ens3 -j SNAT --to-source 192.0.2.254
```

HarpinNAT,netmap

Спикер:
Роман Козлов

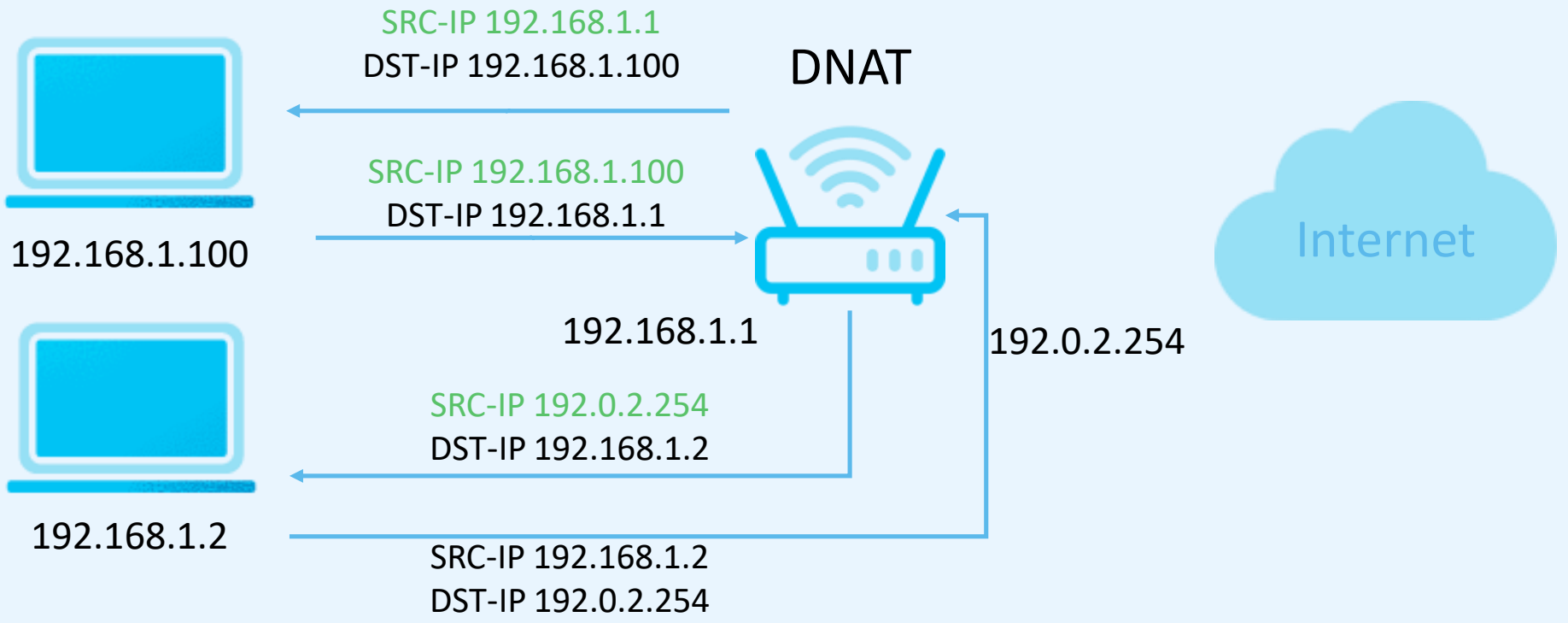
harpinNAT

HarpinNAT помогает в ситуации, когда с внешнего адреса маршрутизатора проброшен порт на сервер внутри сети, но при этом попасть на сервер по внешнему адресу изнутри сети не получается



harpinNAT

HarpinNAT помогает, когда с внешнего адреса маршрутизатора проброшен порт на сервер внутри сети, но при этом попасть на сервер по внешнему адресу изнутри сети не получается



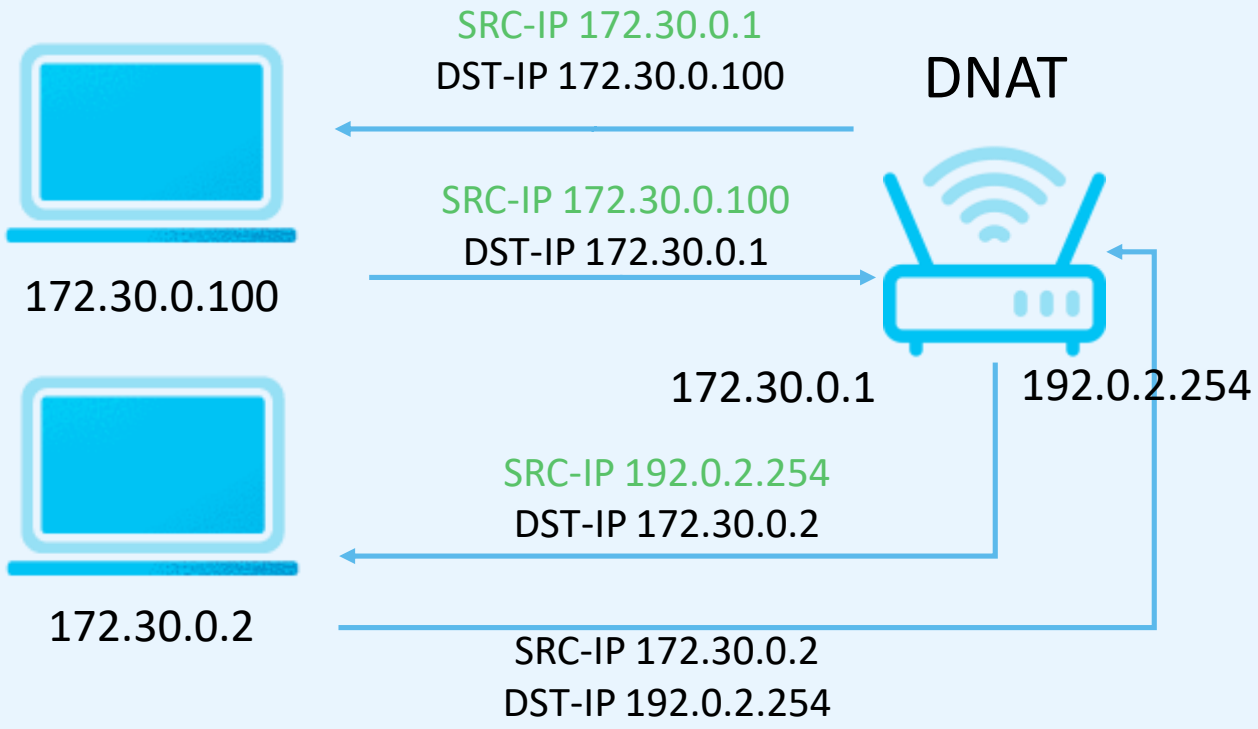
harpinNAT

- **Правило для доступа к веб-серверу с внешнего интерфейса ens3 находящегося в локальной сети на адресе 172.30.0.100**

```
iptables –t nat -A PREROUTING -i
ens3 -p tcp -m tcp --dport 80 -j
DNAT --to-destination
172.30.0.100:80
```

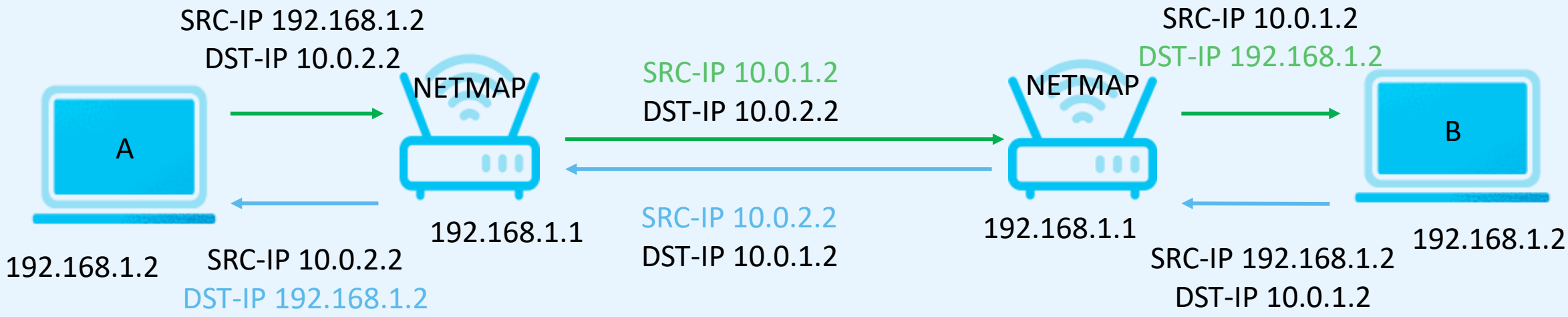
- **Правило HarpinNAT для замены SRC-IP в заголовках пакета на адрес роутера в локальной сети**

```
iptables -t nat -A POSTROUTING  -s
172.30.0.0/24 -d 172.30.0.100 -p tcp
--dport 80 -j SNAT --to-source
172.30.0.1
```



iptables -t nat –J NETMAP

- **NETMAP** – механизм, позволяющий менять в заголовках пакетов адреса сетей источников и назначений один к одному (транслирует одну сеть в другую)
- Данный механизм поможет объединить сети с полным пересечением адресации через дополнительные адреса
- В данном примере сеть компании A транслируется из сети 192.168.1.0/24 в сеть 10.0.1.0/24, а сеть компании B транслируется из 192.168.1.0/24 в сеть 10.0.2.0/24



iptables -t nat –J NETMAP

- root@RouterAr:~# iptables -t nat -I POSTROUTING -s 192.168.1.0/24 -d 10.0.2.0/24 -j NETMAP --to 10.0.1.0/24
- root@RouterAr:~# iptables -t nat -I PREROUTING -s 10.0.2.0/24 -d 10.0.1.0/24 -j NETNAP --to 192.168.1.0/24
- root@RouterB:~# iptables -t nat -I POSTROUTING -s 192.168.1.0/24 -d 10.0.1.0/24 -j NETMAP --to 10.0.2.0/24
- root@RouterBr:~# iptables -t nat -I PREROUTING -s 10.0.1.0/24 -d 10.0.2.0/24 -j NETNAP --to 192.168.1.0/24