

# Сеть и сетевые протоколы: NAT

Александр Гришин  
Эксперт в области системного администрирования



# Александр Гришин

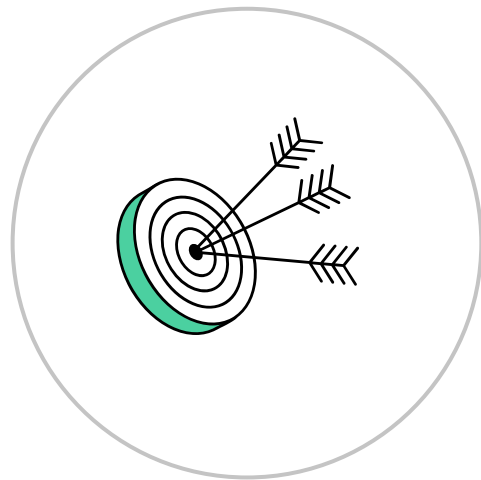
О спикере:

- Инженер в компании YADRO



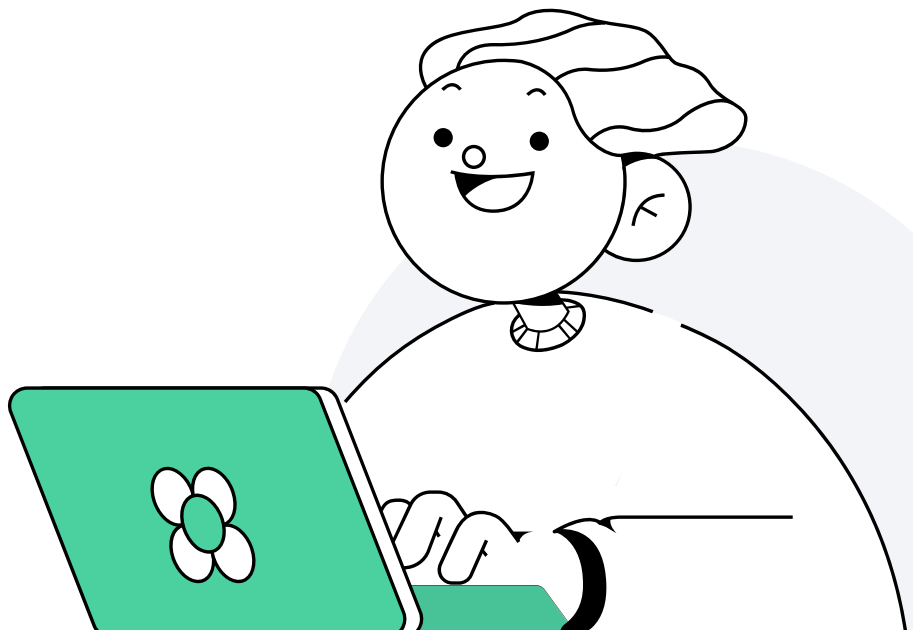
# Цели занятия

- Познакомиться с базовыми представлениями технологии трансляции сетевых адресов и предпосылками к появлению NAT.
- Узнать о различных способах реализации NAT и особенностях применения
- Получить практический навык базовой настройки NAT в Linux

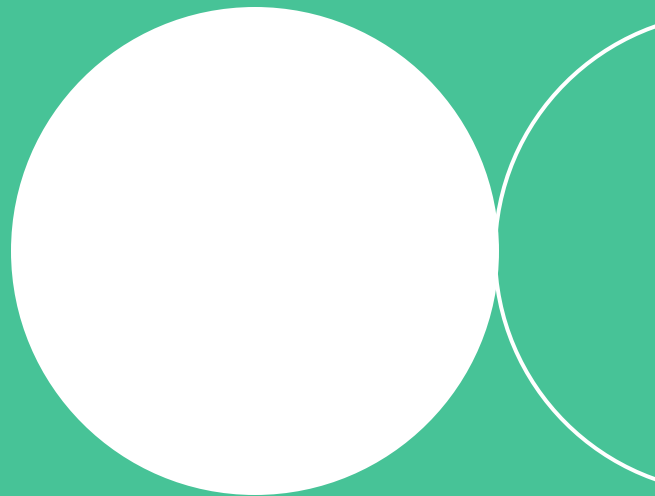


# План занятия

- ① [Приватные и публичные сети](#)
- ② [Static NAT / Dynamic NAT](#)
- ③ [Source NAT](#)
- ④ [Destination NAT](#)
- ⑤ [Примеры настройки NAT](#)
- ⑥ [Итоги](#)
- ⑦ [Домашнее задание](#)

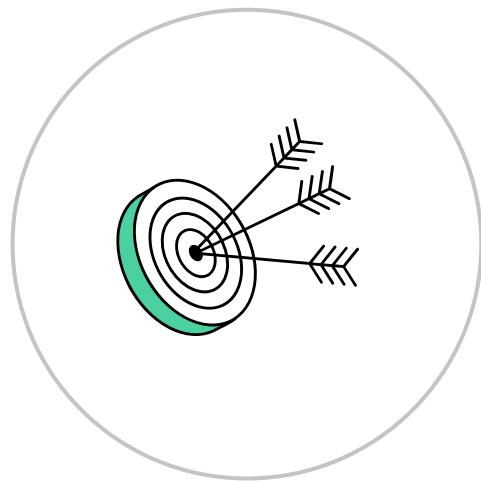


# Приватные и публичные сети



# Цели темы

- Вспомнить диапазоны IPv4 адресов, их назначение
- Закрепить знания об адресации в публичных сетях
- Поговорить о проблематике взаимодействия публичных и частных адресов



# IPv4 адреса бывают двух типов:

1

**Публичные**  
**(public)**

Белые или внешние

2

**Приватные**  
**(private)**


Серые, частные  
или внутренние



**Почему IPv4 адреса  
разделили на два типа?**



# Предпосылки к созданию частных сетей



**Ограниченное  
количество IP-адресов  
(4,3 млрд)**

**Сети, которым  
не нужно ни с кем  
взаимодействовать**

# Идентификация устройств в интернете




**Число уникальных адресов  
ограничено, поэтому было  
определено так называемое  
частное пространство IP-  
адресов**

# Частные IPv4-адреса

Используются в локальных  
компьютерных сетях

Не маршрутизируются в  
глобальную сеть интернет



**Частные IPv4-адреса**  
**не являются уникальными**  
**и могут использоваться**  
**во внутренней сети**

# Блоками частных адресов являются:



Адреса в этих блоках адресов не допустимы для использования в Интернете и должны отклоняться интернет-маршрутизаторами

# Виды сетей

Публичные (почти все остальные)

62.217.185.1/24

62.217.185.151/24

172.16.0.0/12

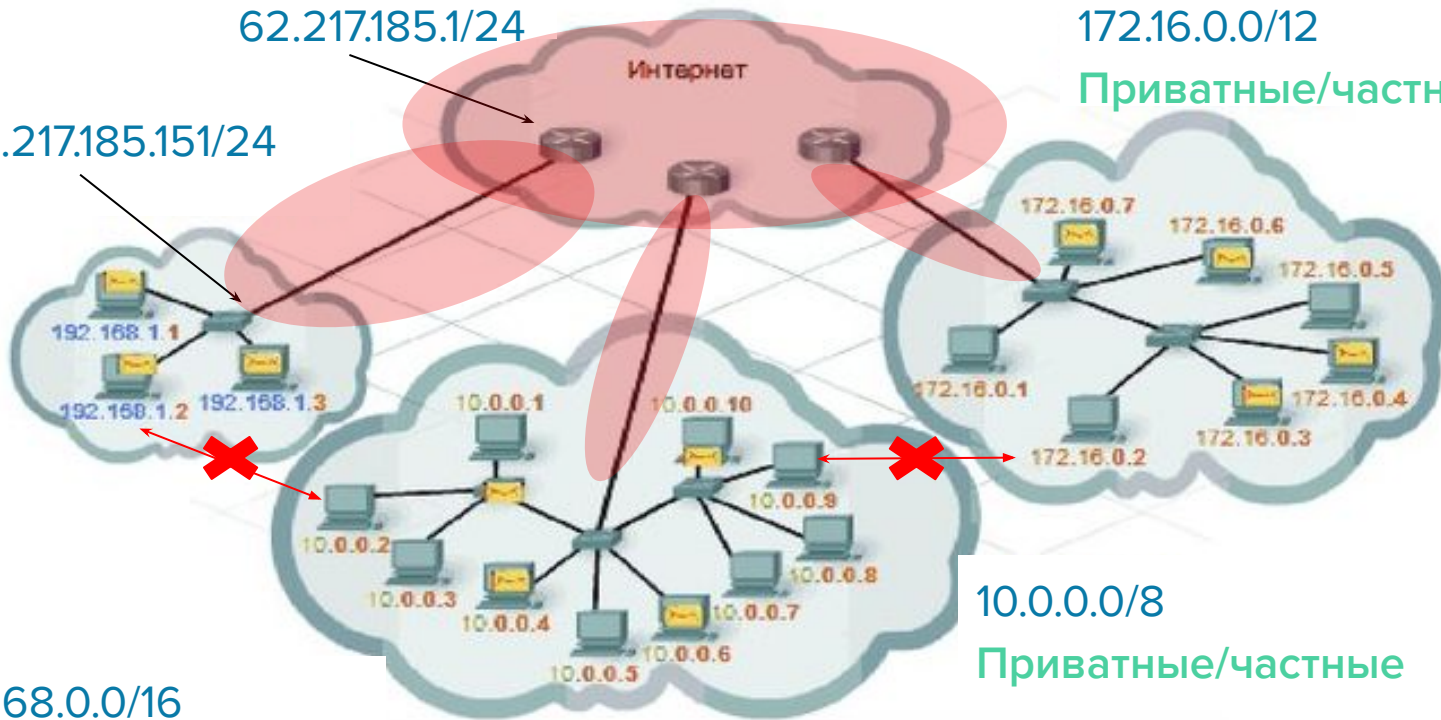
Приватные/частные

192.168.0.0/16

Приватные/частные

10.0.0.0/8

Приватные/частные



# Ситуация

Вы выдали сотрудникам в офисе  
много частных адресов

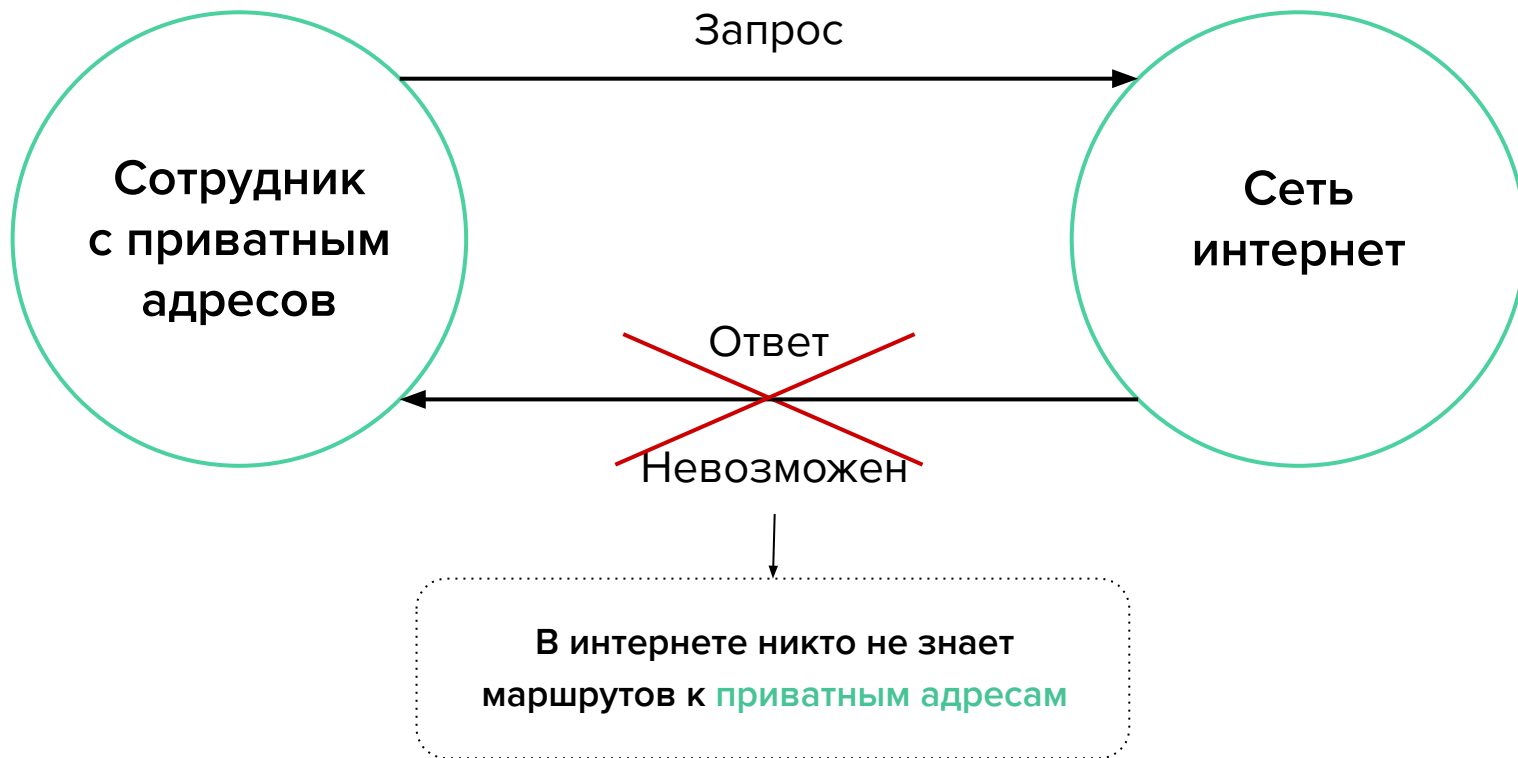
Вопрос:

Как сотрудники будут сидеть  
в интернет?





# Ситуация



# Способы выхода в интернет с частных адресов

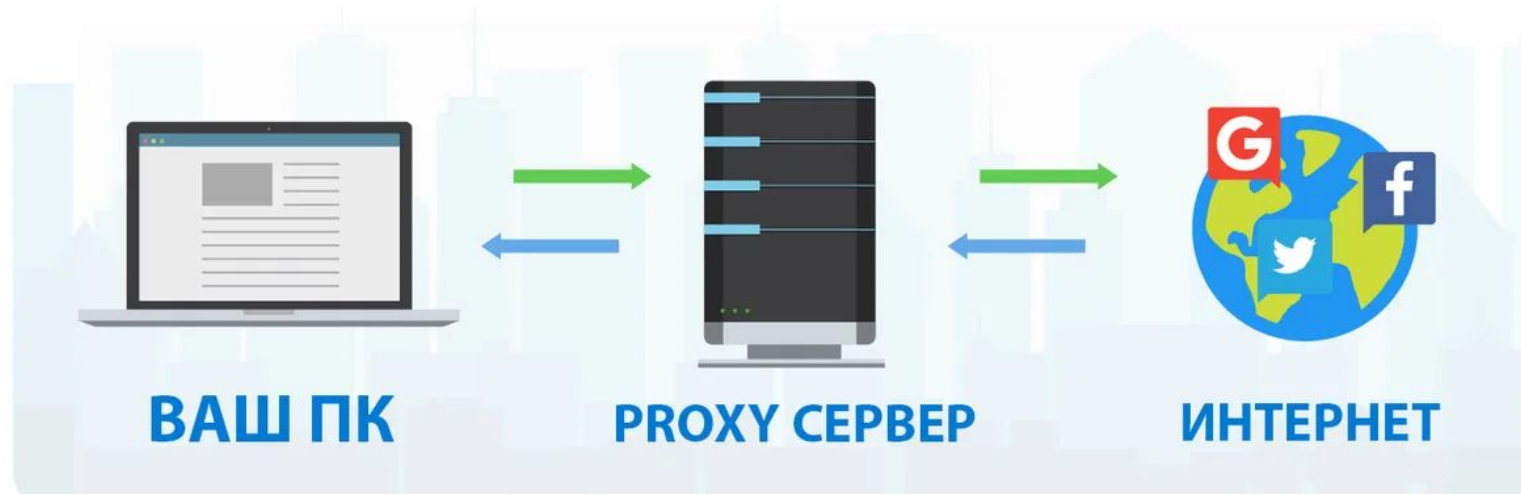
1

Использование  
сервера **PROXY**

2

Подмена адресов  
**NAT**

# Использование PROXY для выхода в интернет с частных адресов



# Использование NAT для выхода в интернет с частных адресов



# Дословный перевод NAT

**Network Address  
Translation**



**Преобразование  
сетевых адресов**



## NAT

**специальный механизм, реализованный в сетях TCP/IP, который позволяет изменять IP-адреса и/или номера портов TCP/UDP в пересылаемых пакетах**



# Механизм NAT

Реализуется через маршрутизатор,  
на программном уровне



# Виды NAT

Static NAT / One to one NAT

Source NAT / NAT Overload /  
Masquerade / Many to one

Dynamic NAT

Destination NAT (PAT)



# Преимущества NAT

- Под одним внешним IPv4 адресом может сидеть в глобальной паутине множество пользователей одновременно
- Скрывает ваш настоящий внутренний IP в частной сети и показывает лишь внешний. Так, все устройства из вне видят только ваш общедоступный IP
- В определенной степени выполняет функции фаервола – если на устройство с NAT извне приходит пакет, который не ожидался — то он категорически не будет допущен

# Недостатки NAT

- Невысокая скорость передачи данных для протоколов реального времени, например, для VoIP. Когда NAT переделывает заголовки пакета — происходят задержки
- Проблемы с идентификацией – под одним IP может находиться сразу несколько человек.
- Сервис может заблокировать внешний IP-адрес из-за злоумышленника (который, например, подбирает пароли), а работать перестанет у всех, кто закрывается этим адресом

# Итоги темы

- 1 Ограниченность адресного пространства IPv4 подтолкнула к широкому использованию частных IP адресов
- 2 Адресацию частных адресов можно решать двумя путями: через прокси-сервер или через подмену адресов (NAT)
- 3 В отличии от прокси-серверов использование NAT не ограничивает использование протоколов, что лучше для конечных пользователей

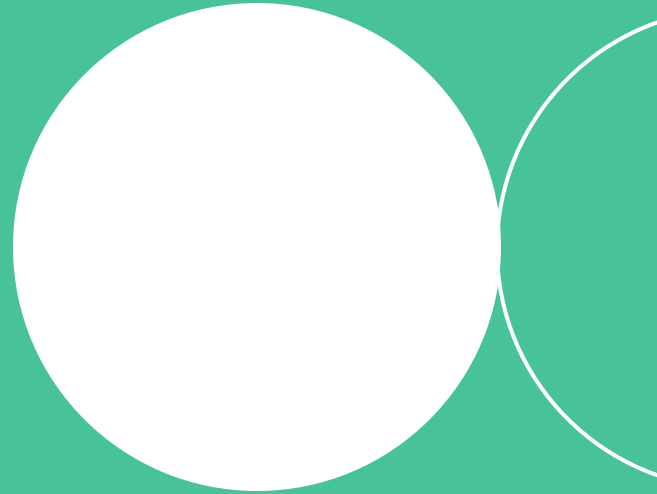


# Итоги темы

- 4 Существует множество реализаций NAT, одним из самых востребованных является Source NAT или Masquerade
- 5 Преимущества и недостатки NAT заключаются в одном – за одним IP адресом может скрываться большое количество пользователей. Поэтому с экономией адресного пространства приходит риск общей блокировки из-за действий одного пользователя

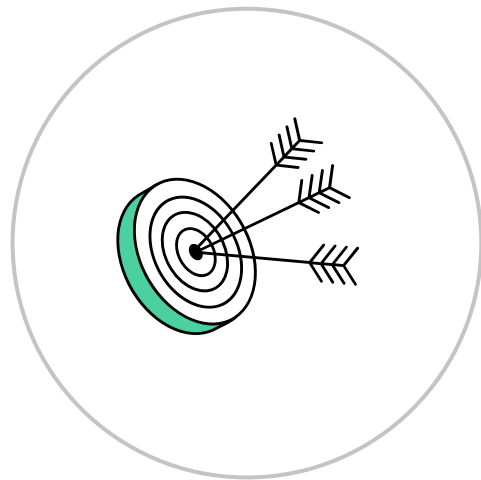


# Static NAT / Dynamic NAT



# Цели темы

- Узнать о принципах работы Static NAT
- Понять, как происходит подмена адресов
- Познакомиться с особенностями Dynamic NAT и его ограничениями



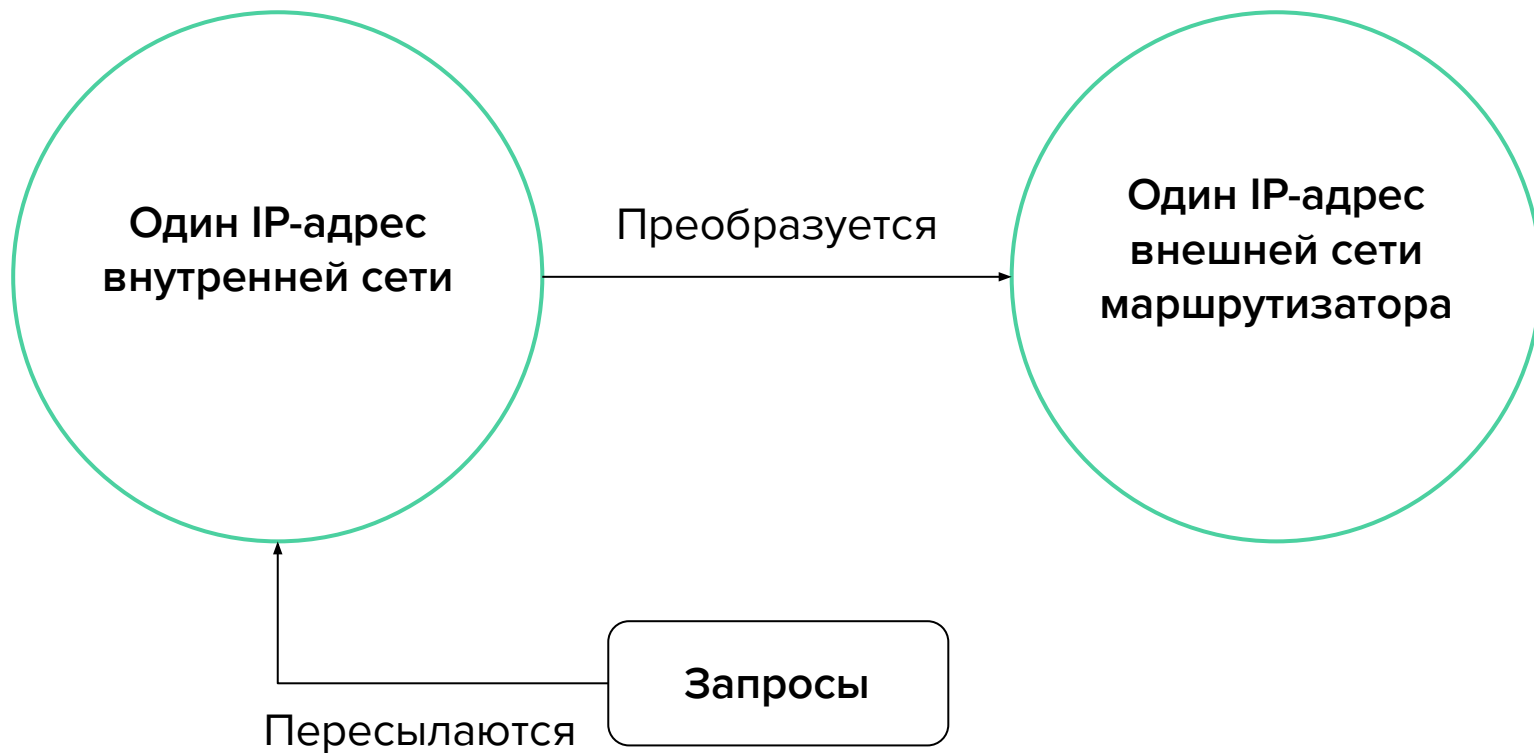


## Static NAT

**сопоставление локального IP-адреса с глобальным IP-адресом на основании один к одному**



# Принцип действия Static NAT





# Для всемирной паутины



Выглядит  
одинаково



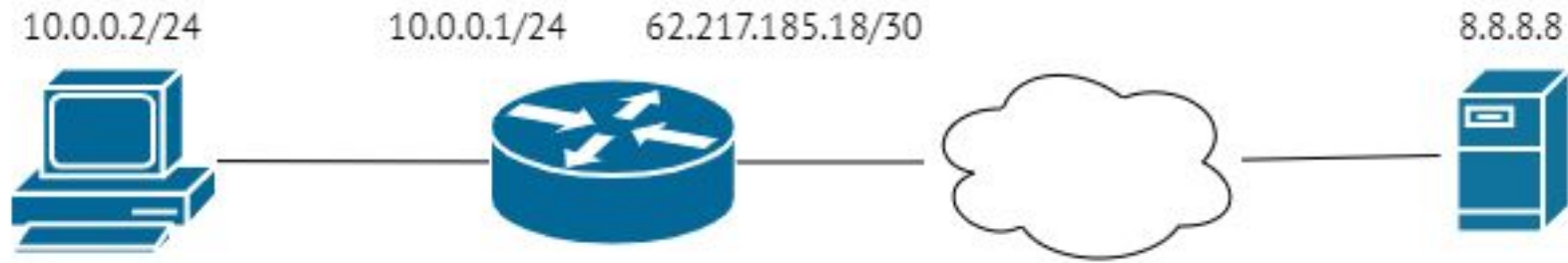
## Static NAT

**используется при  
необходимости «опубликовать»  
внутренний сервер компании в  
интернет, причём не один,  
а все сервисы сразу**



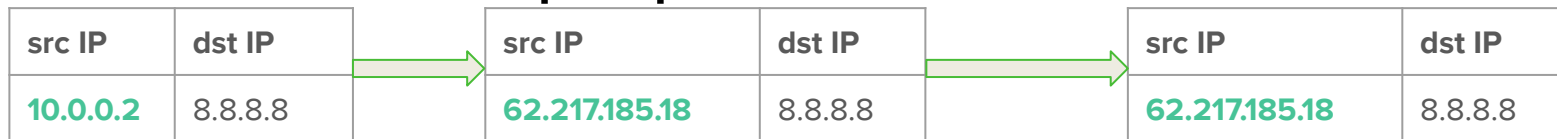
**Несмотря на то, что у сервера «серый» адрес, он полноценно отвечает на запросы извне (по другому, «белому» адресу)**

# Cxema Static NAT

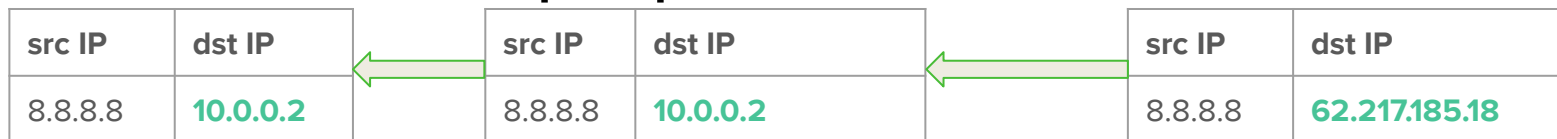


# Схема Static NAT

## Преобразование



## Преобразование



# Из локальной сети в интернет

- Наш сервер 10.0.0.2 обращается ко внешнему серверу на 8.8.8.8, отправляет пакет данных на шлюз
- Шлюз 10.0.0.1, на котором настроен NAT переписывает в пакете IP-адрес отправителя (поле “source ip” IP-пакета) в белый адрес 62.217.185.15 (выдан провайдером)
- Всё взаимодействие этого компьютера в интернете идёт через белый IP-адрес 62.217.185.15, ответ от сервера 8.8.8.8 отправляется также на этот адрес, т.к. в интернете никто ничего не знает про 10.0.0.2 благодаря трансляции

# Из локальной сети в интернет

- Из интернета происходит попытка подключения к нашему серверу по адресу 62.217.185.15 (т.к. про 10.0.0.2 никто ничего не знает, т.к. сеть немаршрутизируемая и пакеты до неё ни от кого не дойдут)
- На нашем шлюзе есть трансляция, преобразующая все пакеты из 10.0.0.2 в 62.217.185.15 и из 62.217.185.15 в 10.0.0.2
- На основании этого правила шлюз преобразовывает в IP-пакете поле destination IP из 62.217.185.15 в 10.0.0.2 и отправляет его уже в локальной сети



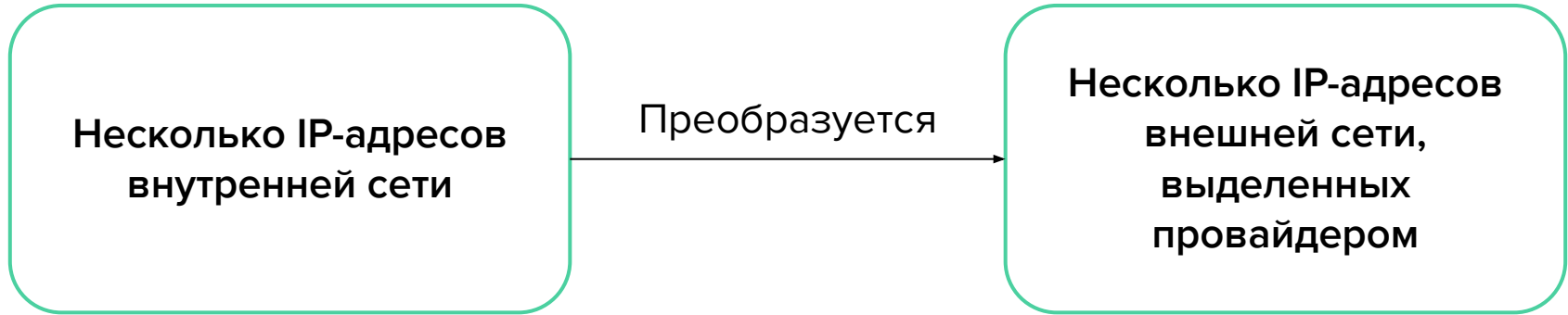
## Dynamic NAT

**динамическая адресная трансляция, в которой адреса сопоставляются по принципу «многие ко многим»**



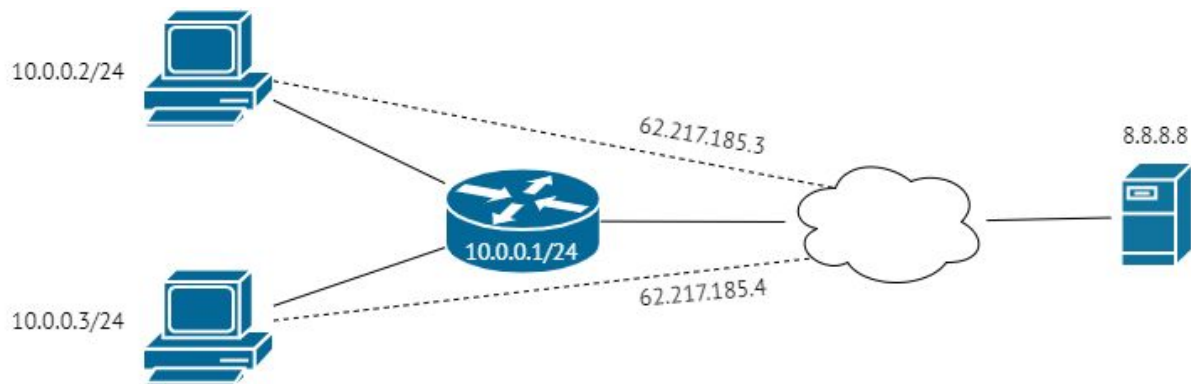


# Принцип действия Dynamic NAT



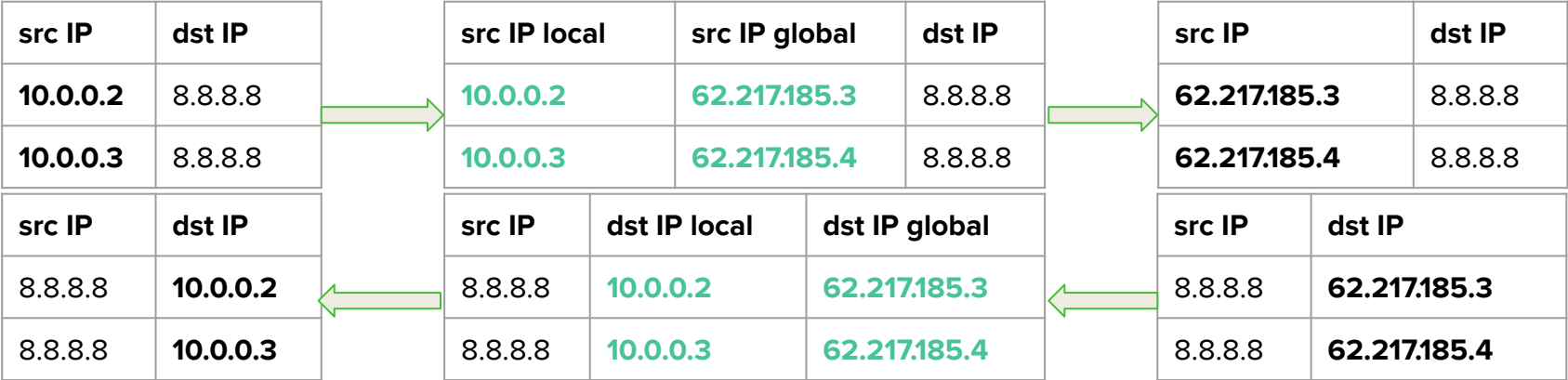
**Реальные адреса выдаются  
динамически каждому  
нуждающемуся пользователю  
во внутренней сети, а не одному  
определенному узлу**

# Схема Dynamic NAT



# Схема Dynamic NAT

Таблица преобразований



# Ограничения Dynamic NAT

Вопрос:

Если внешних адресов, например, 10, а пользователей 300?

# Ограничения Dynamic NAT

**Вопрос:**

Если внешних адресов, например, 10, а пользователей 300?

**Ответ:**

Те хосты, кто успел первым, те и смогут их использовать

# Ограничения Dynamic NAT

## Вопрос:

Если внешних адресов, например, 10, а пользователей 300?

## Ответ:

Те хосты, кто успел первым, те и смогут их использовать

Dynamic NAT – используется редко

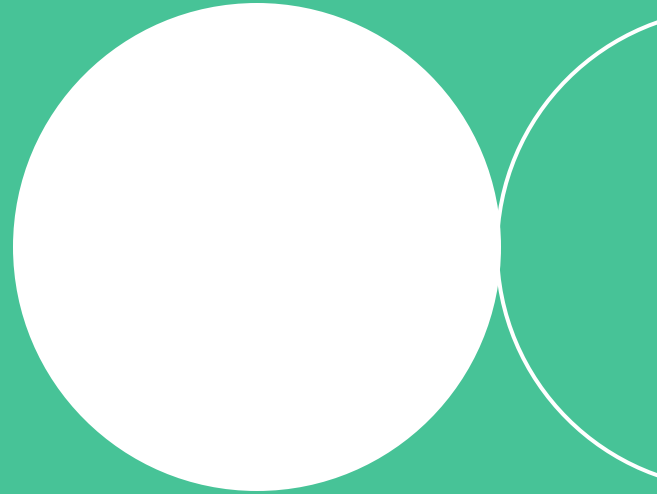
# Итоги темы

- 1 Использование Static NAT целесообразно, когда нам необходимо полностью опубликовать все сервисы узла в публичной сети
- 2 Подмена адреса отправителя/получателя осуществляется маршрутизатором на границе сетей
- 3 Отличие Dynamic NAT заключается в динамическом сопоставлении внешних адресов по внутренним клиентам



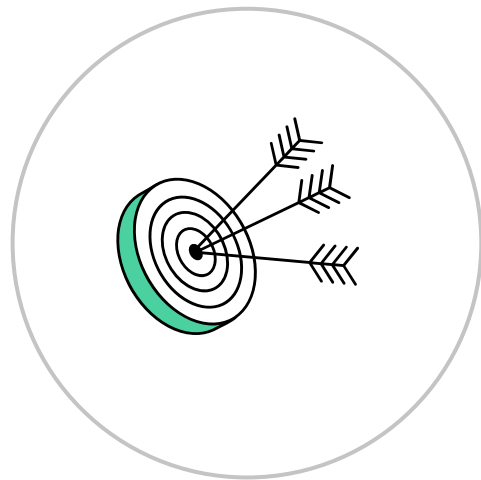


# Source NAT



# Цели темы

- Познакомиться с особенностями Source NAT
- Разобраться с ключевыми отличиями Source NAT от других реализаций
- Узнать об отличиях Source NAT и Masquerading





## Механизм Source NAT (SNAT)

**позволяет изменить исходный IP-адрес сетевого пакета на другой IP-адрес, а также увеличить безопасность и сохранить конфиденциальность, поскольку маскируются и скрываются частные IP-адреса устройств**



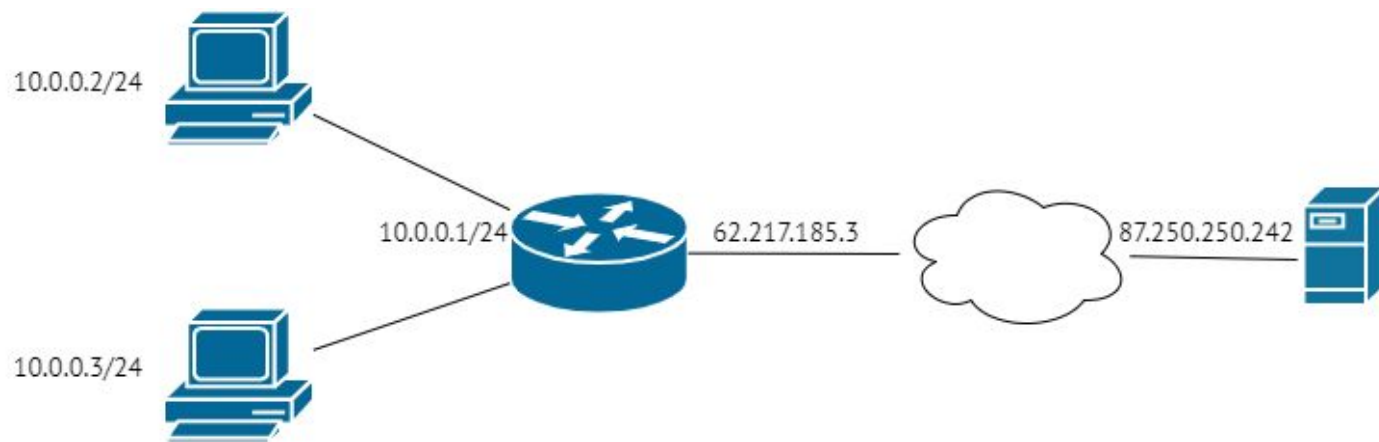
## Source NAT

**используются для выхода в  
интернет группы компьютеров  
с внутренними адресами  
через один внешний адрес**



**Снаружи на внешний адрес пропускаются только пакеты, содержащиеся в таблице трансляций**

# Схема Source NAT



# Схема Source NAT

Таблица преобразований (динамическая)

src IP:port	dst IP:port	src IP local:port	src IP global:port	dst IP:port
10.0.0.2:2001	87.250.250.242:80	10.0.0.2:2001	62.217.185.3:3500	87.250.250.242:80
10.0.0.3:4999	87.250.250.242:80	10.0.0.3:4999	62.217.185.3:2999	87.250.250.242:80

# Из локальной сети в интернет

- Наши компьютеры **10.0.0.0/24** обращаются ко внешним серверам, например на **87.250.250.242:80**, отправляют пакеты на шлюз, подставляя случайный порт в качестве **src port**
- Шлюз **10.0.0.1**, на котором настроен NAT, переписывает в пакете IP-адрес и порт отправителя (поля “source ip”, “source port” IP-пакета) в белый адрес **62.217.185.3** и случайный **src port**
- Далее он записывает в таблицу NAT трансляций запись:

**10.0.0.2:2001 - 62.217.185.3:3500 - 87.250.250.242:80**

для того, чтобы правильно обработать ответный пакет



# Из локальной сети в интернет

Запись в таблицу NAT трансляций:

```
10.0.0.2:2001 - 62.217.185.3:3500 - 87.250.250.242:80
```

# Из интернета в локальную сеть

Шлюз пропустит только пакеты, соответствующие существующим NAT трансляциям, остальные будут отброшены

```
10.0.0.2:2001 - 62.217.185.3:3500 - 87.250.250.242:80
10.0.0.3:4999 - 62.217.185.3:2999 - 87.250.250.242:80
```

Разрешены будут пакеты:

src IP:port	dst IP:port
87.250.250.242:80	62.217.185.3:3500
87.250.250.242:80	62.217.185.3:2999

\* Через некоторый таймаут строка из таблицы трансляций удалится



## NAT Masquerading

**тип трансляции сетевого адреса, при которой внешний адрес отправителя подставляется динамически, в зависимости от назначенного провайдером адреса**



## **NAT Masquerading**

**используются для выхода в  
интернет группы компьютеров  
с внутренними адресами  
через один внешний адрес**



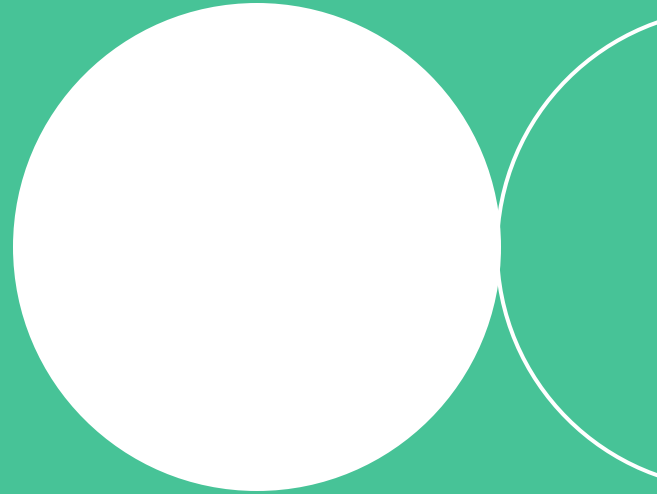
**IP-адрес, в который происходит подмена, должен быть  
прописан на **интерфейсе****

# Итоги темы

- 1 Source NAT использует таблицу трансляции для идентификации потоков. Благодаря этому через один внешний сетевой адрес может подключаться множество клиентов
- 2 В Source NAT можно подставлять любой внешний адрес
- 3 Отличие Masquerade в том, что подставляется адрес, привязанный к внешнему интерфейсу маршрутизатора

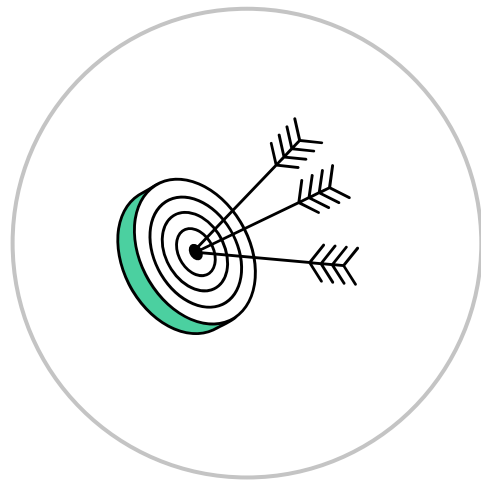


# Destination NAT



# Цели темы

- Узнать о назначении технологии Destination NAT
- Разобраться в особенностях ее реализации







## Destination NAT / PAT (DNAT)

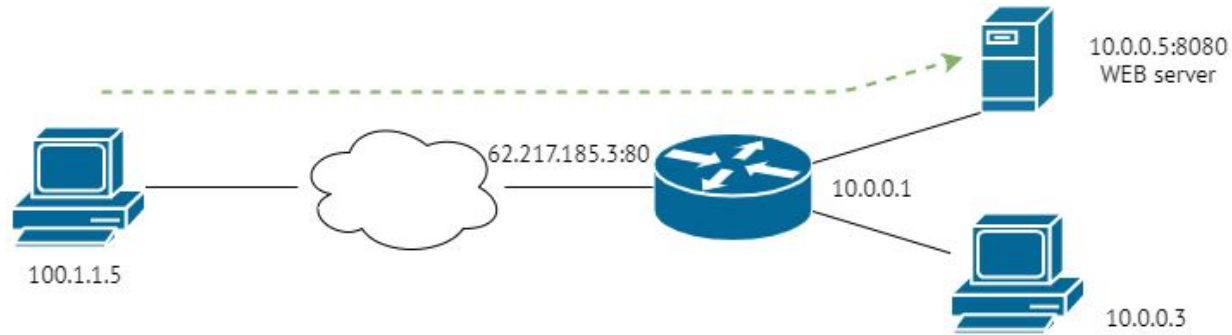
**технология трансляции сетевого адреса в зависимости от TCP/UDP-порта получателя**



## **Destination NAT / PAT**

**используются для публикации  
сервиса (port), находящегося  
внутри сети, для внешних  
пользователей**

# Cxema Destination NAT



# Схема Destination NAT

Таблица преобразований (статическая)

src IP:port	dst IP:port
100.11.5:2222	<b>62.217.185.3:80</b>

src IP	dst IP global:port	dst IP local:port
100.11.5:2222	<b>62.217.185.3:80</b>	<b>10.0.0.5:8080</b>

# Снаружи в локальную сеть

Существует одна статическая трансляция, которая преобразовывает трафик снаружи на конкретный хост внутри сети

```
62.217.185.3:80 - 10.0.0.5:8080
```

Порты могут быть разными, они не обязаны совпадать

# Снаружи в локальную сеть

Статическая трансляция

62.217.185.3:80 - 10.0.0.5:8080

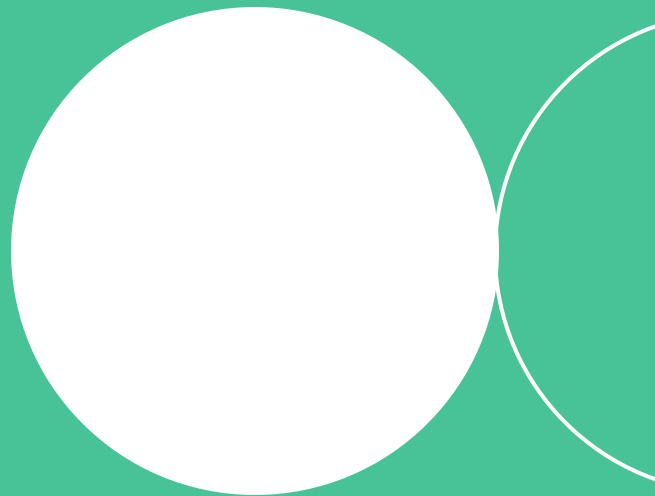
Порты могут быть разными,  
они не обязаны совпадать

# Итоги темы

- 1 Destination NAT применяется для того, чтобы опубликовать в сети доступ к внутреннему ресурсу с частным адресом
- 2 Destination NAT используют, если доступ нужно открыть к ограниченному количеству сервисов по их транспортным адресам (портам)



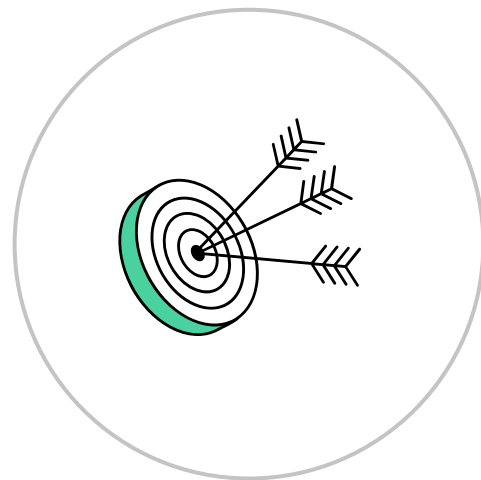
# Примеры настройки NAT





# Цели темы

- Узнать о способах настройки NAT в Linux
- Получить практический навык настройки SNAT
- Совместно настроить DNAT в Linux

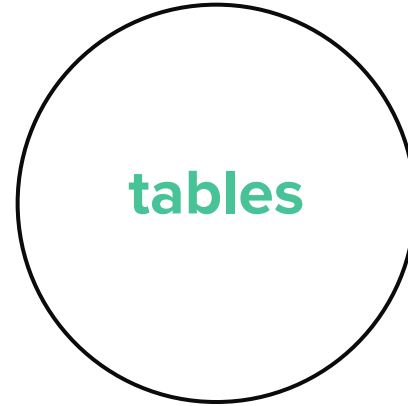
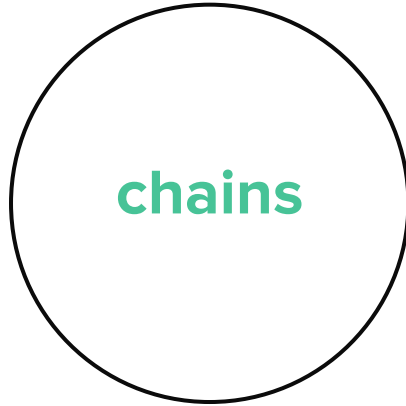


**NAT в Linux реализуется с помощью**

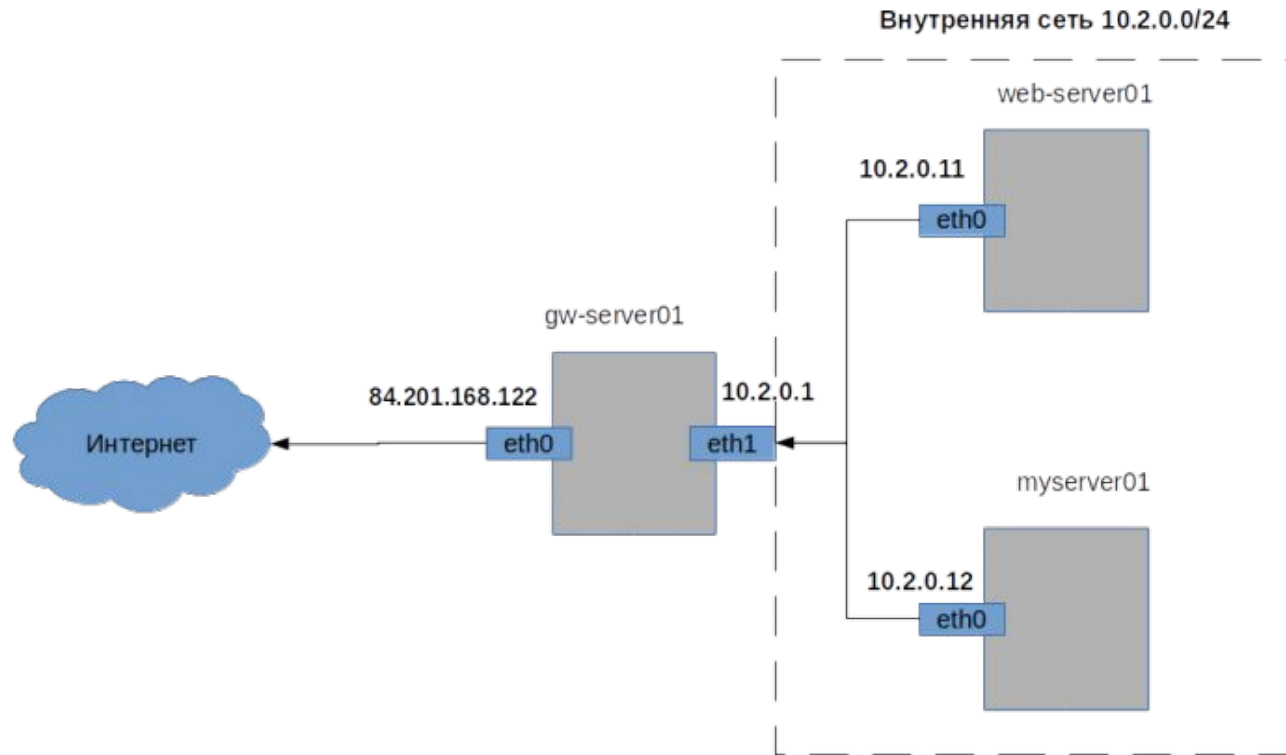


iptables

# iptables оперирует сущностями

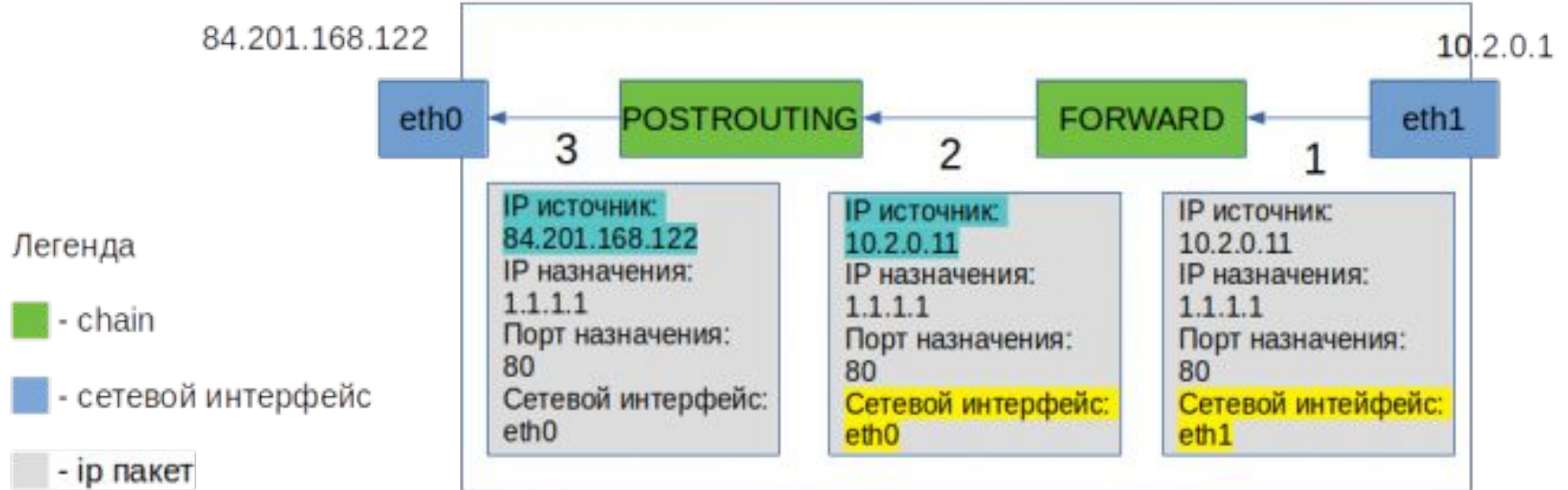


# Настройка SNAT: доступ из LAN в интернет



# SNAT

gw-server01



# SNAT

- IP пакет поступил на внутренний интерфейс **eth1** сервера **gw-server01**
- После для IP пакета определяется исходящий сетевой интерфейс, с которого он должен быть отправлен, это отмечено желтым цветом
- В конце IP пакет проходит цепочку **POSTROUTING**, в которой происходит подмена IP адреса **источника**, на IP адрес **внешнего** интерфейса **eth0** сервера **gw-server01**

# Команды routing в Linux

Для начала необходимо разрешить пересылку пакетов с одного интерфейса на другой (по умолчанию в Linux это отключено)

```
# до перезагрузки  
sudo sysctl -w net.ipv4.ip_forward=1
```

```
# на постоянной основе  
/etc/sysctl.conf =>  
net.ipv4.ip_forward = 1
```

```
$ sudo sysctl -p /etc/sysctl.conf
```

# Команды routing в Linux

```
# до перезагрузки  
sudo sysctl -w net.ipv4.ip_forward=1
```

```
# на постоянной основе  
/etc/sysctl.conf =>  
net.ipv4.ip_forward = 1
```

```
$ sudo sysctl -p /etc/sysctl.conf
```



# Команды SNAT в Linux

Создадим правило в iptables, разрешающее передачу пакетов между внутренним (eth1) и внешним (eth0) интерфейсом и разрешим передавать между интерфейсами пакеты, относящиеся к уже установленным соединениям

```
iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
```

```
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

- **-A** – add
- **-i / -o** – input/output
- **-m** – использовать доп.модуль
- **-j** – действие

# Команды SNAT в Linux

```
iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
```

```
iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
```

- **-A** – add
- **-i / -o** – input/output
- **-m** – использовать доп.модуль
- **-j** – действие

# Команды SNAT в Linux

## Включим SNAT:

```
iptables -t nat -A POSTROUTING -s 10.2.0.0/24 -o eth1 -j SNAT --to-source 84.201.168.122
```

- **-A** – add;
- **-t** – таблица;
- **-s** – source (необязательно);
- **-j** – действие;
- **--to-source** – должен быть адресом на интерфейсе, с которого планируется выпускать во внешнюю сеть IP пакеты

# Команды NAT, iptables в Linux

Посмотрим получившуюся конфигурацию для таблицы **filter** и цепочки **FORWARD** (вывод обрезан):

```
iptables -L -n -v
```

```
Chain FORWARD (policy DROP 0 packets, 0 bytes)
  pkts bytes target    prot opt in     out     source            destination
   136  8863 ACCEPT    all  --  eth1   eth0    0.0.0.0/0         0.0.0.0/0
    12  1234 ACCEPT    all  --  *      *       0.0.0.0/0         0.0.0.0/0          state RELATED,ESTABLISHED

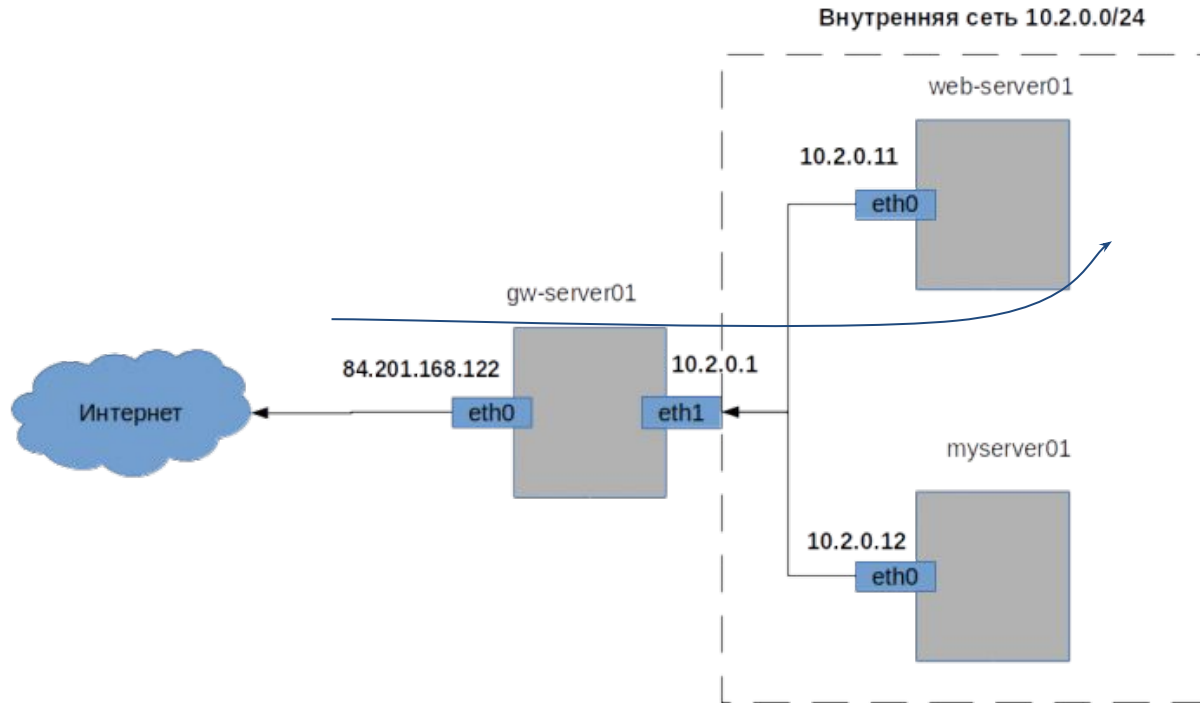
Chain OUTPUT (policy ACCEPT 96 packets, 10160 bytes)
  pkts bytes target    prot opt in     out     source            destination
```

и конфигурацию для таблицы **nat** (вывод обрезан):

```
iptables -t nat -L -n -v
```

```
Chain POSTROUTING (policy ACCEPT 8 packets, 556 bytes)
  pkts bytes target    prot opt in     out     source            destination
     0     0 SNAT      all  --  *      eth0    10.2.0.0/24       0.0.0.0/0          to:84.201.168.122
```

# Настройка DNAT: доступ из LAN в интернет



# DNAT

- IP пакет поступил на внешний интерфейс **eth0** сервера **gw-server01**
- После в IP пакете меняется **destination IP** и при необходимости **destination port**
- Далее происходит маршрутизация в соответствии с правилами на сервере (таблица маршрутизации)

# Команды DNAT в Linux

Сначала разрешим передачу пакетов с внешнего интерфейса (eth0) на внутренний (eth1) интерфейс:

При необходимости можно отдельным правилом запретить подключение через NAT для отдельных IP адресов или подсетей

```
iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT
```

```
iptables -I FORWARD 1 -o eth1 -s 167.71.67.136 -j DROP
```

# Команды DNAT в Linux

```
iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT
```

```
iptables -I FORWARD 1 -o eth1 -s 167.71.67.136 -j DROP
```



# Команды DNAT в Linux

- Теперь перенаправим все соединения на порт 80 интерфейса внешней сети (eth0) на IP адрес веб сервера внутренней сети **web-server01**
- И все соединения на порт **13389** перенаправлять на порт **3389** сервера внутренней сети (в целях безопасности)

```
iptables -t nat -A PREROUTING -p tcp --dport 80 -i eth0 -j DNAT --to-destination 10.2.0.11
```

```
iptables -t nat -A PREROUTING -p tcp --dport 13389 -i eth0 -j DNAT --to-destination 10.2.0.12:3389
```

# Команды DNAT в Linux

```
iptables -t nat -A PREROUTING -p tcp --dport 80 -i eth0 -j DNAT --to-destination 10.2.0.11
```

```
iptables -t nat -A PREROUTING -p tcp --dport 13389 -i eth0 -j DNAT --to-destination 10.2.0.12:3389
```

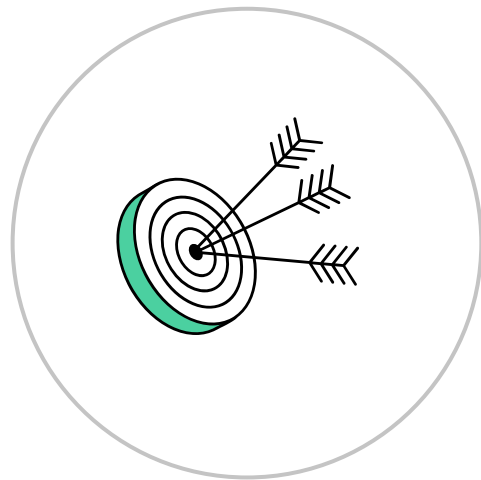
# Итоги темы

- 1 Для того чтобы начать настройку NAT необходимо разрешить пересылку пакетов между интерфейсами с помощью переменной `net.ipv4.ip_forward=1`
- 2 В качестве инструмента настройки NAT в Linux используется `iptables`
- 3 При настройке SNAT мы добавляем правила в цепочки FORWARD таблицы filter и POSTROUTING таблицы nat. А при настройке DNAT – в цепочки FORWARD таблицы filter и PREROUTING таблицы nat



# Общие итоги занятия

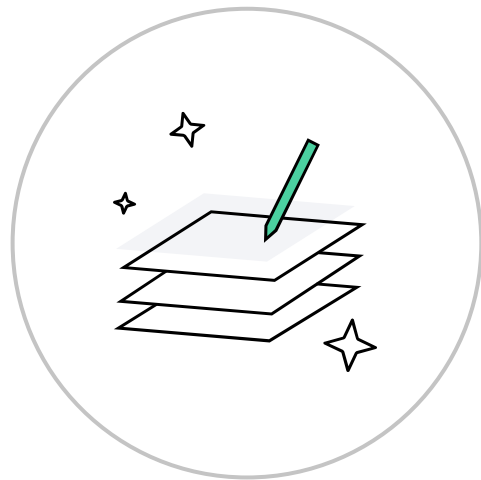
- Познакомились с базовыми представлениями технологии трансляции сетевых адресов и предпосылками к появлению NAT
- Узнали о различных способах реализации NAT и особенностях применения
- Получили практический навык базовой настройки NAT в Linux



# Домашнее задание

## Давайте посмотрим вашу практику после лекции

- 1 Практика: домашнее задание (обязательное) с проверкой от преподавателя
- 2 Вопросы по домашнему заданию задавайте в чате учебной группы
- 3 Задачи можно сдавать по частям.  
Зачёт по домашней работе ставят после того, как приняты все задачи



# Задавайте вопросы. Оставляйте обратную связь по вебинару

Александр Гришин  
Эксперт в области системного администрирования

