Преобразование сетевых адресов (NAT)

Типы преобразований, типовые кейсы, реализация на различном оборудовании

Сергей Розанов
Сетевой инженер

Сергей Розанов

О спикере:

- Инженер ЛВС, БЛВС, Security, NMS
- В сфере IT с 2007 года
- Сертификация Cisco CCNA, CCNP, Huawei, H3C
- Реализовал проекты для частных и государственных компаний

Вспоминаем прошлое занятие

Вопрос: как называется атака, использующая уязвимость протокола ARP для подмены mac-адреса получателя пакета на свой?

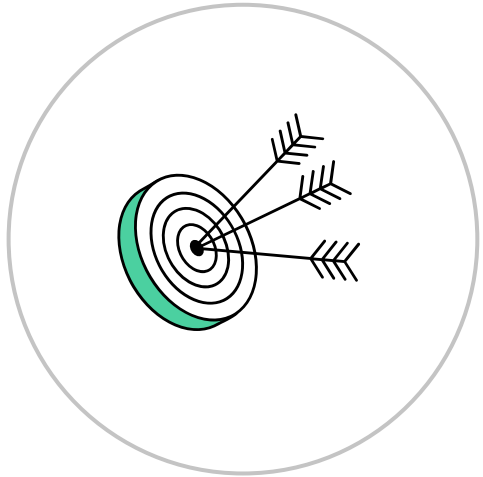
Вспоминаем прошлое занятие

Вопрос: как называется атака, использующая уязвимость протокола ARP для подмены mac-адреса получателя пакета на свой?

Ответ: ARP spoofing

Цели занятия

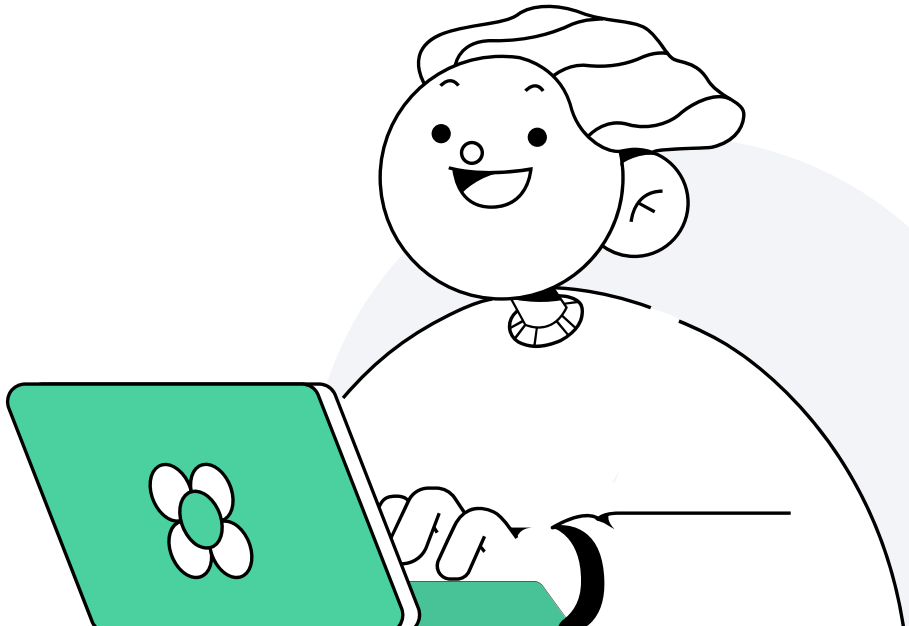
- Узнать о проблеме ограниченного количества IPv4-адресов и способах её решения
- Разобраться в терминологии NAT
- Научиться различать типы NAT и выбирать нужный тип под конкретную задачу
- Настроить NAT на оборудовании Cisco
- Узнать плюсы и минусы технологии



План занятия

1. Адресация IPv4. Необходимость преобразования адресов
2. Классификация NAT
3. Примеры настройки NAT
4. Плюсы и минусы технологии NAT
5. Итоги
6. Домашнее задание

*Нажми на нужный раздел для перехода



Адресация IPv4

Необходимость преобразования адресов

1

Проблема IPv4

Протокол IPv4, созданный в 1981 году, может использовать всего 232 или ~4,3 млрд уникальных адресов:

- от 0.0.0.0 до 255.255.255.255.

По мере распространения этого стандарта более остро вставал вопрос масштабирования

Проблема IPv4

В 1996 году был разработал **IPv6**. Этот протокол поддерживает $\mathbf{2^{128}}$ или 3.4×10^{38} уникальных IP-адресов, это эквивалентно 340 триллионам триллионов триллионов IP-адресов.

Однако переход на новый стандарт требует:

- большого количества времени для создания новых протоколов
- обучения специалистов
- замены и перенастройки оборудования
- изменения логики работы сетей

Спустя 26 лет переход ещё не выполнен

Проблема IPv4

В 1994 для решения проблемы с IPv4 было решено разбить IP-адреса на два типа:

- публичные
- приватные

Обеспечив между ними обмен данными с помощью новой технологии NAT

Вспоминаем прошлое занятие

Вопрос: попробуйте назвать все пулы приватных IPv4-адресов

Вспоминаем прошлое занятие

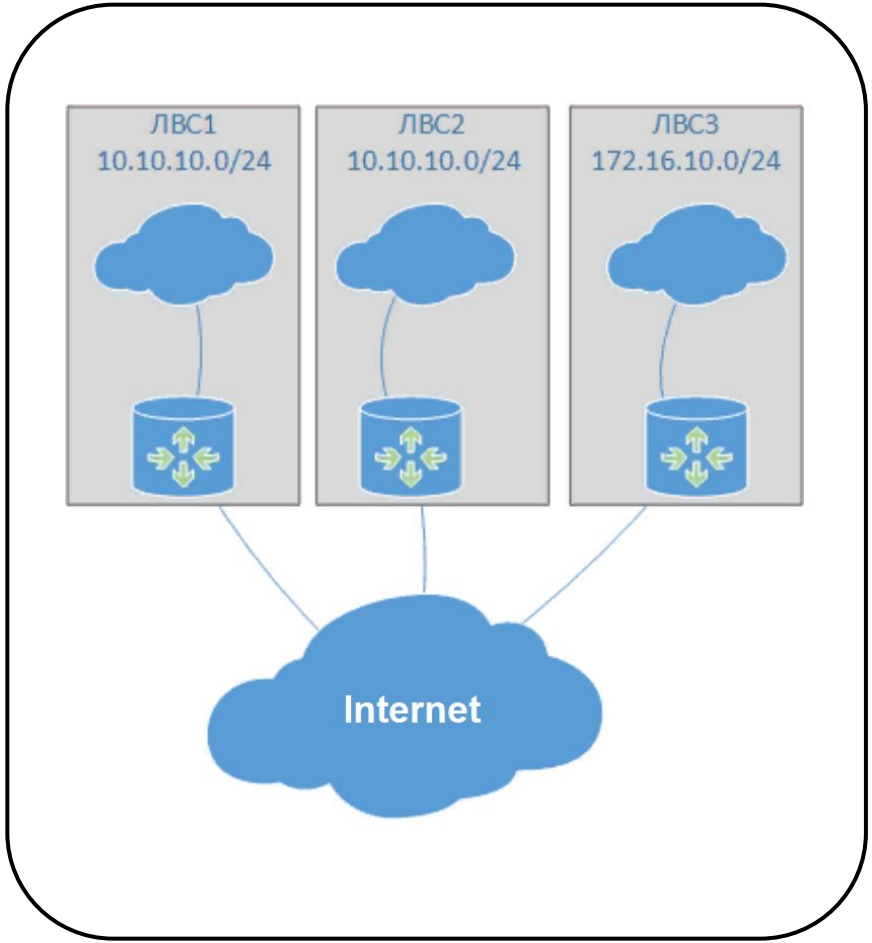
Вопрос: попробуйте назвать все пулы приватных IPv4-адресов

Ответ:

- 10.0.0.0 — 10.255.255.255
- 172.16.0.0 — 172.31.255.255
- 192.168.0.0 — 192.168.255.255

Приватные адреса

- Они используются для обмена трафиком только внутри сети организации, поэтому могут быть повторно использованы во многих ЛВС
- Этим обеспечивается почти неограниченный
запас приватных IPv4-адресов
- Для выхода в интернет по-прежнему требуется хотя бы один публичный адрес



Публичные адреса

Для обмена трафиком в интернете получатель и отправитель должны иметь уникальный IP-адрес.

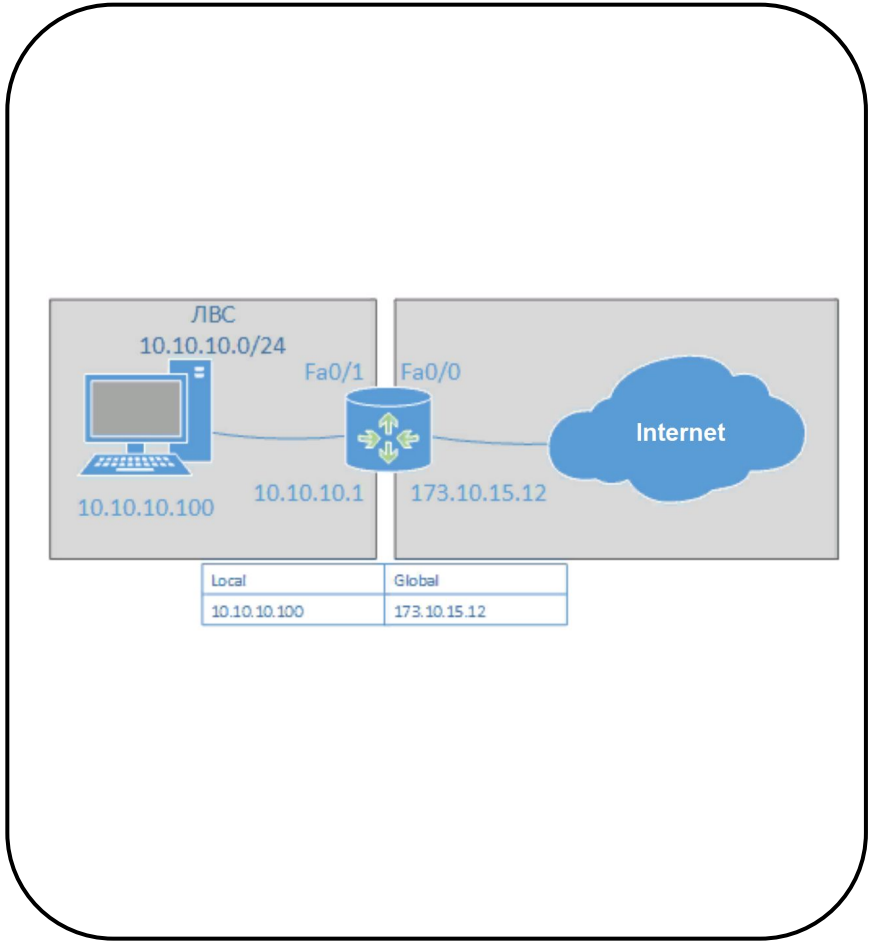
Получить выделенный адрес можно у любого интернет-провайдера, он, в свою очередь, арендует более крупные блоки у локальных и региональных регистраторов, для которых крупные подсети и BGP AS выделяют IANA

Источник

Как хосты с приватными адресами могут обмениваться данными в интернете?

Сетевая трансляция

Для этого была разработана технология трансляции сетевых адресов NAT. С помощью неё устройство на границе ЛВС и интернета может заменять приватный адрес публичным в поле отправителя, после чего пакет может достигнуть хоста в публичной сети. Этими функциями технология NAT не ограничивается



Знакомство с технологией NAT

2

Преобразование пакета

Простейшее преобразование пакета, отправленного из приватной сети серверу во внешней.

Чтобы ответные пакеты из интернета находили адресата в локальной сети, маршрутизатор хранит в памяти данные обо всех NAT-трансляциях

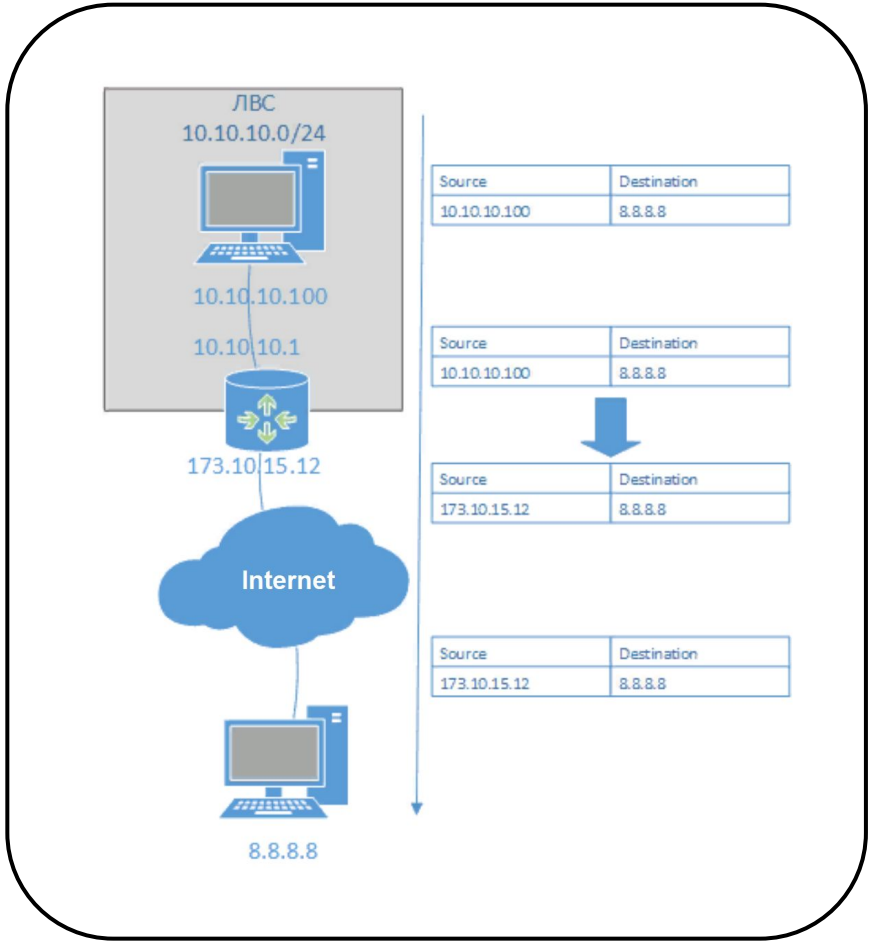


Таблица трансляции на примере Cisco

Для каждой пары «отправитель — порт» и «получатель — порт» в памяти маршрутизатора создаётся строка в таблице NAT-трансляций.

Для просмотра таблицы трансляции нужно использовать команду:

```
show ip nat translation
Pro  Inside global       Inside local          Outside local   Outside global
tcp  173.10.15.12:4129   10.10.10.100:33046    8.8.8.8:2553    8.8.8.8:2
```

Таблица трансляции на примере Cisco

Для каждой пары «отправитель — порт» и «получатель — порт» в памяти маршрутизатора создаётся строка в таблице NAT-трансляций.

Для просмотра таблицы трансляции нужно использовать команду:

```
show ip nat translation
Pro  Inside global       Inside local          Outside local   Outside global
tcp  173.10.15.12:4129   10.10.10.100:33046    8.8.8.8:2553    8.8.8.8:2
```

Inside global — адрес и порт отправителя в интернете после процедуры трансляции на маршрутизаторе

Inside local — адрес и порт отправителя в оригинальном пакете до процедуры трансляции

Outside local — адрес и порт получателя в оригинальном пакете до процедуры трансляции

Outside global — адрес и порт получателя пакета в интернете после процедуры трансляции

Порядок обработки пакетов

Для преобразования пакета на пограничном устройстве Cisco можно настроить две опции в зависимости от ситуации: **ip nat inside <>** и **ip nat outside <>**.

ip nat inside	• Преобразует поле источника IP пакета, проходящего из inside-интерфейса в outside-интерфейс. • Преобразует поле получателя IP пакета, проходящего из outside-интерфейса в inside-интерфейс.
ip nat outside	• Преобразует поле источника IP пакета, проходящего из outside-интерфейса в inside-интерфейс. • Преобразует поле получателя IP пакета, проходящего из inside-интерфейса в outside-интерфейс.

Порядок обработки пакетов

Пакеты, проходящие из inside-интерфейса в outside и из outside в inside обрабатываются по-разному:

inside-outside	outside-inside
• политика IPSec • проверка input access list • policy routing • routing • **NAT inside to outside (local to global translation)**	• политика IPSec • проверка input access list • **NAT outside to inside (global to local translation)** • policy routing • routing

Важно! При настроенной опции ip nat outside <> пакет, движущийся из inside в outside на подменный адрес получателя изучается роутером. Если в таблице маршрутизации отсутствует маршрут до подменного адреса, пакет **отбрасывается**. Нужен явно прописанный роутинг до этого адреса!

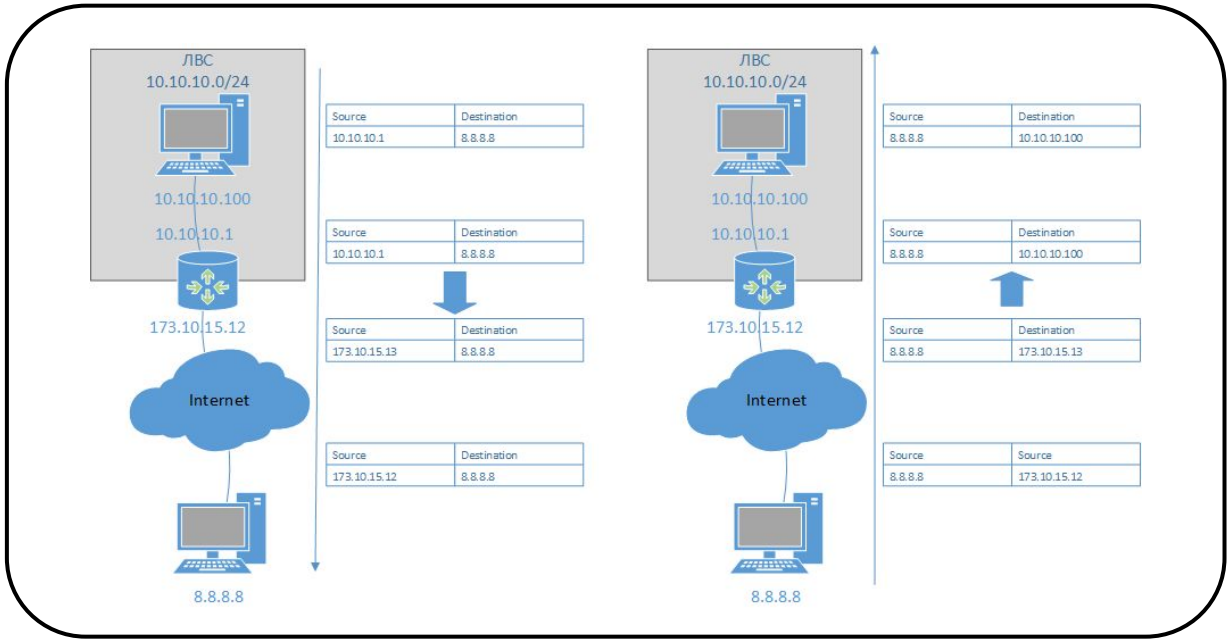
Классификация NAT

3

Static NAT

Простейшее преобразование пакета один к одному. Происходит подмена внутреннего IP-адреса внешним. Используется для выдачи «белого» адреса внутреннему хосту.

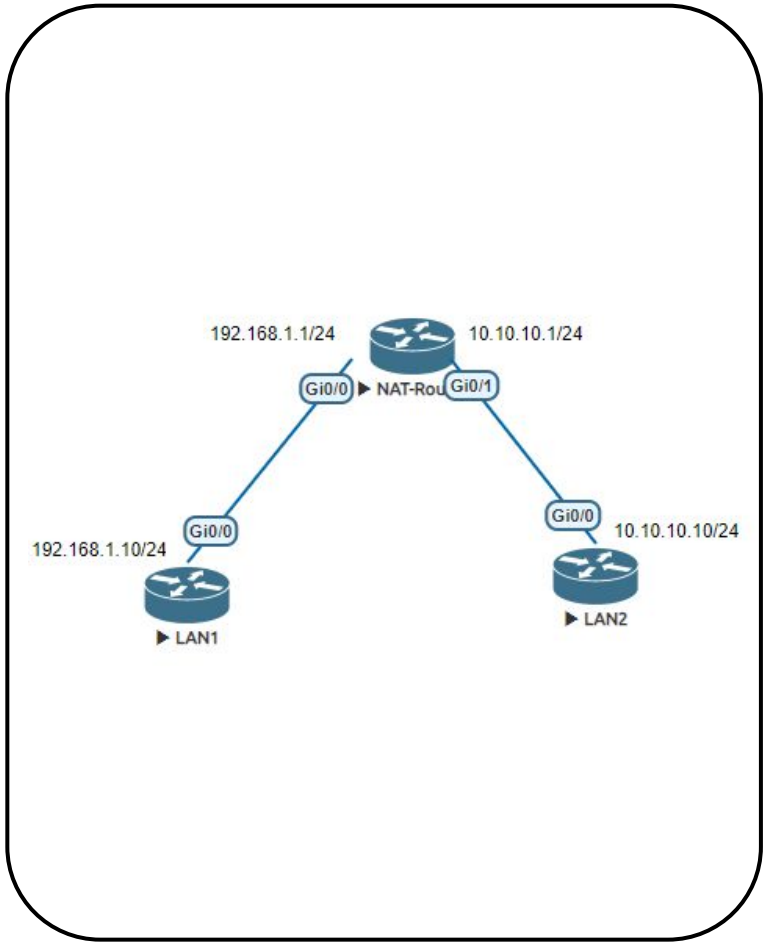
В этом случае внутренний хост доступен из интернета так, как будто на нём настроен публичный IP-адрес



Настройка static NAT (twice NAT) на примере Cisco

1. Выбираем inside-интерфейс. На него приходит пакет, который должен быть преобразован. Важно: один интерфейс не может быть одновременно inside и outside

```
interface GigabitEthernet0/0
 ip nat inside
```



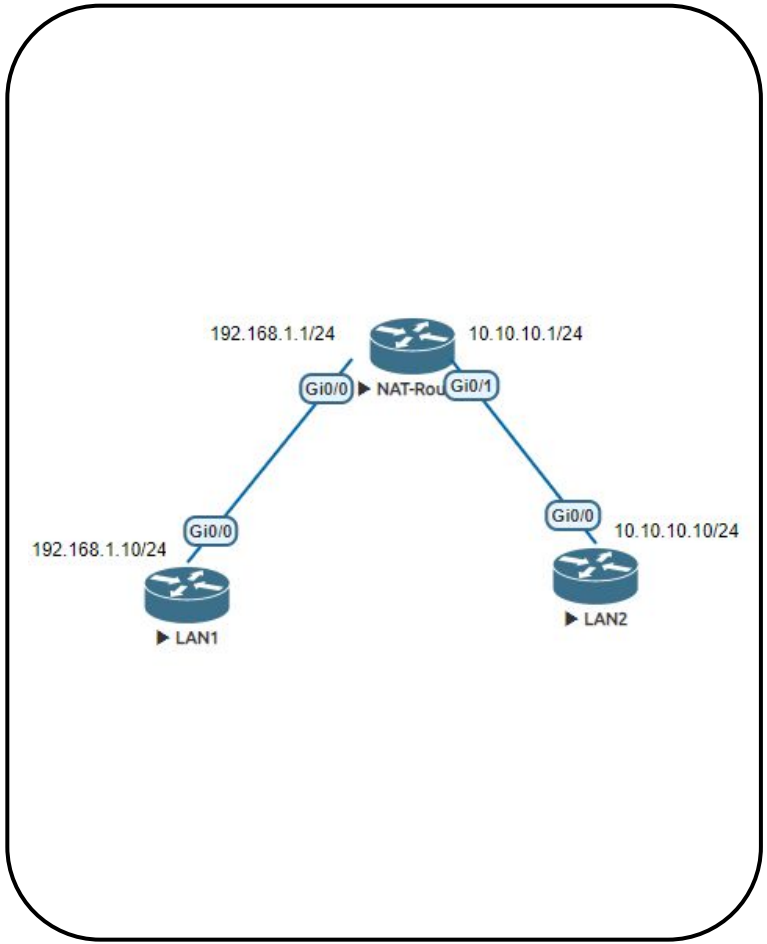
Настройка static NAT (twice NAT) на примере Cisco

1. Выбираем inside-интерфейс. На него приходит пакет, который должен быть преобразован. Важно: один интерфейс не может быть одновременно inside и outside

```
interface GigabitEthernet0/0
 ip nat inside
```

2. Выбираем outside-интерфейс

```
interface GigabitEthernet0/1
 ip nat outside
```



Настройка static NAT (twice NAT) на примере Cisco

1. Выбираем inside-интерфейс. На него приходит пакет, который должен быть преобразован. Важно: один интерфейс не может быть одновременно inside и outside

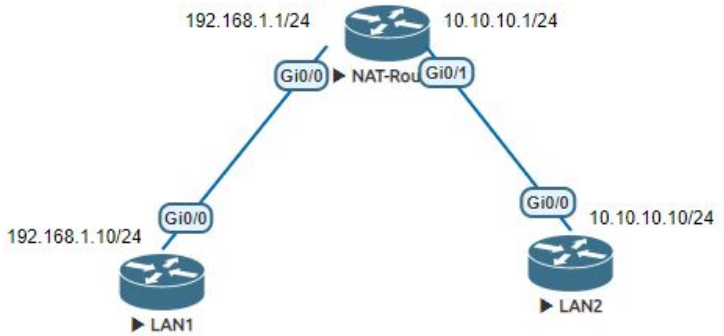
```
interface GigabitEthernet0/0
 ip nat inside
```

2. Выбираем outside-интерфейс

```
interface GigabitEthernet0/1
 ip nat outside
```

3. Пишем правила обработки пакетов

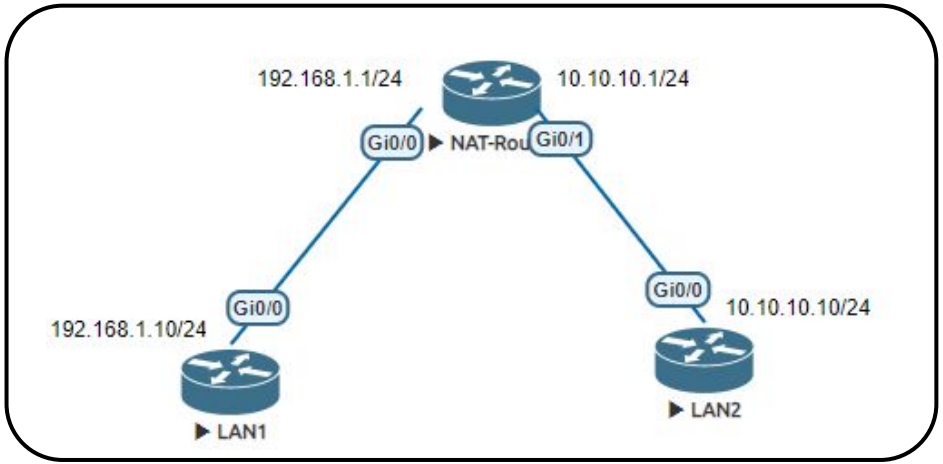
```
ip nat inside source static 192.168.1.10 10.10.10.2
ip nat outside source static 10.10.10.10 192.168.1.2
ip route 192.168.1.2 255.255.255.255 10.10.10.10
или
ip nat inside source static 192.168.1.10 10.10.10.2
ip nat outside source static 10.10.10.10 192.168.1.2 add-route
```



Настройка static NAT (twice NAT) на примере Cisco

После завершения настройки в памяти маршрутизатора создаётся постоянная запись в таблице трансляций. Маршрутизатор будет обрабатывать пакеты, отправленные на внешний адрес, указанный в этой таблице

```
nat#sh ip nat tra
Pro      Inside global     Inside local      Outside local     Outside global
---      ---               ---               192.168.1.2       10.10.10.10
---      10.10.10.2        192.168.1.10      ---               ---
```



Проверка настройки

При обмене данными между узлами, указанными в правиле трансляций, создаётся временная запись для каждой сессии.

На этом примере трафик отправлен с адреса 192.168.1.10 (inside local) на адрес 192.168.1.2 (outside local), затем адрес отправителя изменён на 10.10.10.2 (inside global), а получатель на 10.10.10.10 (outside global)

```
nat#sh ip nat tra
Pro   Inside global      Inside local         Outside local      Outside global
---   ---                ---                  192.168.1.2        10.10.10.10
tcp   10.10.10.2:36461   192.168.1.10:36461   192.168.1.2:23     10.10.10.10:23
---   10.10.10.2         192.168.1.10         ---                ---
```

Вопрос: что будет, если при настройке статического NAT настроить в качестве inside global внешний IP-адрес маршрутизатора?

Вопрос: что будет, если при настройке статического NAT настроить в качестве inside global внешний IP-адрес маршрутизатора?

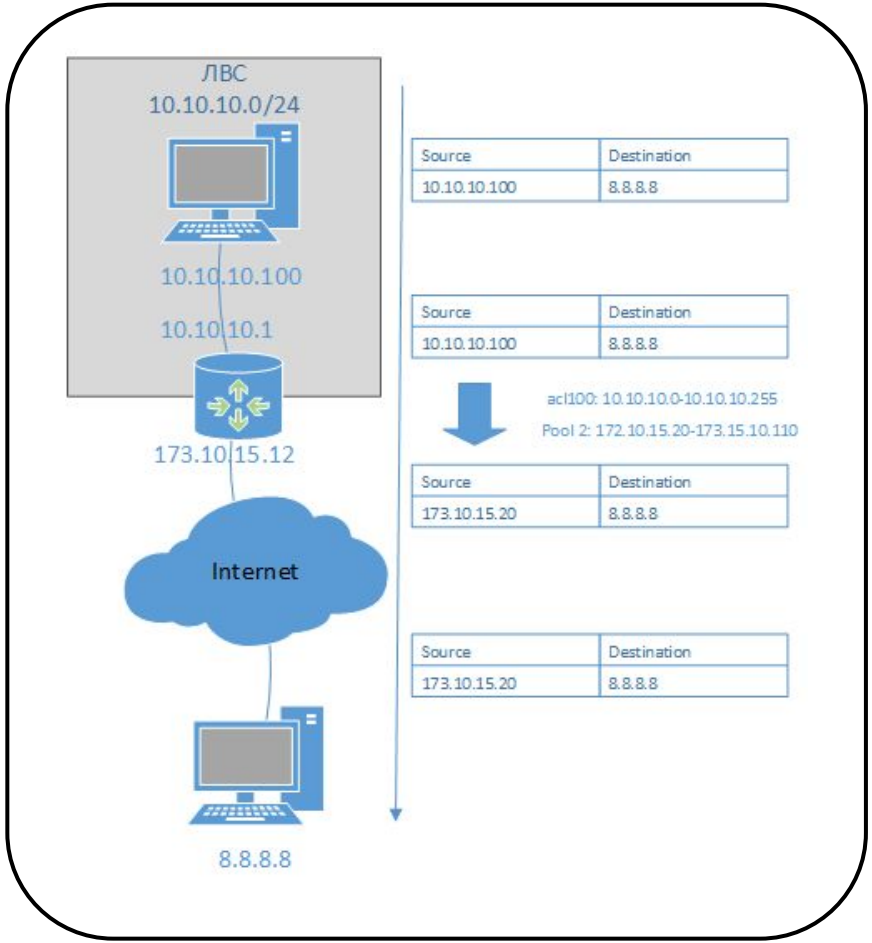
Ответ: по правилу трансляции все пакеты будут перенаправляться внутреннему хосту, но до маршрутизатора никакие пакеты доходить не будут

Dynamic NAT

Технология похожа на статический NAT.

Один внутренний адрес транслируется во внешний.

Маршрутизатор, получив пакет, проверяет, содержится ли IP-адрес отправителя в списке адресов для трансляции, и подставляет вместо него адрес из пула публичных адресов



Настройка dynamic NAT на примере Cisco

1. Выбираем inside-интерфейс. На него приходит пакет, который должен быть преобразован. Важно: один интерфейс не может быть одновременно inside и outside

Настройка dynamic NAT на примере Cisco

1. Выбираем inside-интерфейс. На него приходит пакет, который должен быть преобразован. Важно: один интерфейс не может быть одновременно inside и outside
2. Выбираем outside-интерфейс. С этого интерфейса пакет отправляется к получателю, или на него приходит ответный пакет

Настройка dynamic NAT на примере Cisco

1. Выбираем inside-интерфейс. На него приходит пакет, который должен быть преобразован. Важно: один интерфейс не может быть одновременно inside и outside
2. Выбираем outside-интерфейс. С этого интерфейса пакет отправляется к получателю, или на него приходит ответный пакет
3. Создаём пул публичных IP-адресов

```
ip nat pool pool2 173.10.15.20 173.10.15.110
```

Настройка dynamic NAT на примере Cisco

1. Выбираем inside-интерфейс. На него приходит пакет, который должен быть преобразован. Важно: один интерфейс не может быть одновременно inside и outside
2. Выбираем outside-интерфейс. С этого интерфейса пакет отправляется к получателю, или на него приходит ответный пакет
3. Создаём пул публичных IP-адресов

```
ip nat pool pool2 173.10.15.20 173.10.15.110
```

4. Создаём acl для фильтрации внутренних IP-адресов

```
access-list 100 permit ip 10.10.10.0 0.0.0.255 any
```

Настройка dynamic NAT на примере Cisco

1. Выбираем inside-интерфейс. На него приходит пакет, который должен быть преобразован. Важно: один интерфейс не может быть одновременно inside и outside
2. Выбираем outside-интерфейс. С этого интерфейса пакет отправляется к получателю, или на него приходит ответный пакет
3. Создаём пул публичных IP-адресов

```
ip nat pool pool2 173.10.15.20 173.10.15.110
```

4. Создаём acl для фильтрации внутренних IP-адресов

```
access-list 100 permit ip 10.10.10.0 0.0.0.255 any
```

5. Пишем правило преобразования пакета. В нём описывается, какие пакеты должны быть транслированы

```
ip nat inside source list 100 pool2
```

Проверка настройки

После завершения настройки и начала обмена трафиком в памяти маршрутизатора динамически создаётся запись в таблице трансляций.

Пока трансляция есть в памяти маршрутизатора, пакеты могут приходить на внутренние хосты внешней сети

```
sh ip nat tra
Pro   Inside global         Inside local       Outside local      Outside global
icmp  173.10.15.20:3        10.10.10.100:3     8.8.8.8:3          8.8.8.8:3
---   173.10.15.20          10.10.10.100
icmp  173.10.15.21:4        10.10.10.101:4     8.8.8.8:4          8.8.8.8:4
---   173.10.15.21          10.10.10.101
```

Вопрос: что будет, если
при работе с динамическим NAT
закончится пул внешних адресов?

Вопрос: что будет, если
при работе с динамическим NAT
закончится пул внешних адресов?

Ответ: новые хосты не смогут
обмениваться данными с внешней сетью,
пока пул не освободится

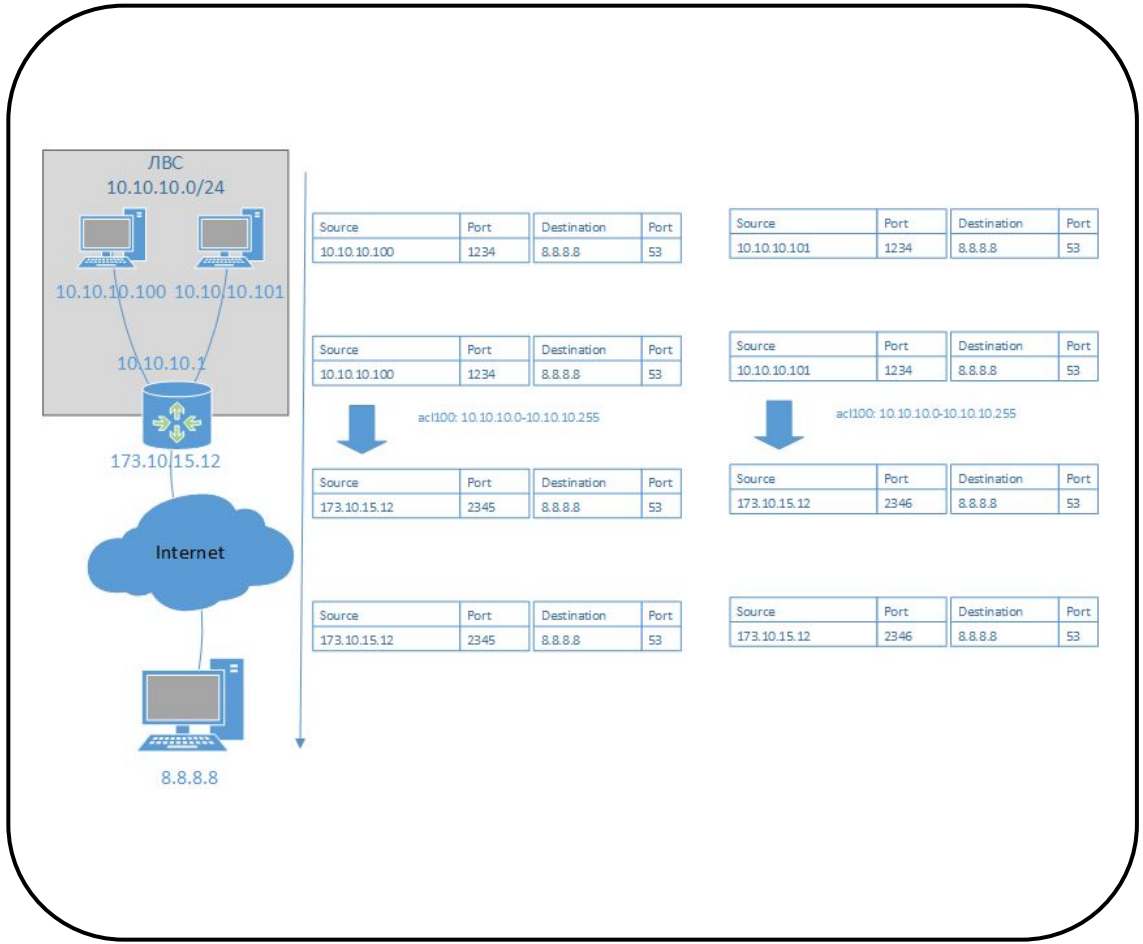
PAT

Port address translation

Именно эта технология позволяет не нуждаться в большом количестве публичных IPv4-адресов для доступа в интернет.

Пограничное устройство может менять внутри пакета не только адрес, но и порт, сохраняя все изменения в своей таблице трансляций.

Частные случаи PAT — проброс портов и PAT overload



Настройка PAT на примере Cisco

Проброс портов:

1. Выбираем inside-интерфейс
2. Выбираем outside-интерфейс
3. Пишем правило преобразования пакета. В нём описывается, какие пакеты должны быть транслированы

```
ip nat inside source static tcp 10.10.10.100 23 173.10.15.12 2323
```

Настройка PAT на примере Cisco

Проброс портов:

1. Выбираем inside-интерфейс
2. Выбираем outside-интерфейс
3. Пишем правило преобразования пакета. В нём описывается, какие пакеты должны быть транслированы

```
ip nat inside source static tcp 10.10.10.100 23 173.10.15.12 2323
```

→ В качестве inside global может выступать как адрес интерфейса маршрутизатора, так и другой. Номера портов global и local могут быть разными или совпадать

Проверка настройки

После завершения настройки в памяти маршрутизатора создаётся постоянная запись в таблице трансляций.

Пакеты из интернета с адресом назначения Inside global и портом 2323 будут перенаправлены на 10.10.10.100, порт 23

```
sh ip nat tra
Pro  Inside global      Inside local     Outside local    Outside global
tcp  173.10.15.12:2323  10.10.10.100:23  ---              ---
```

Настройка PAT на примере Cisco

PAT overload:

1. Выбираем inside-интерфейс

Настройка PAT на примере Cisco

PAT overload:

1. Выбираем inside-интерфейс
2. Выбираем outside-интерфейс

Настройка PAT на примере Cisco

PAT overload:

1. Выбираем inside-интерфейс
2. Выбираем outside-интерфейс
3. Задаём ACL, фильтрующий внутренние адреса, требующие трансляции

```
access-list 100 permit ip 10.10.10.0 0.0.0.255 any
```

Настройка PAT на примере Cisco

PAT overload:

4* Для настройки адреса inside global можно задать пул адресов или настроить использование IP-адреса интерфейса

Настройка PAT на примере Cisco

PAT overload:

4* Для настройки адреса inside global можно задать пул адресов или настроить использование IP-адреса интерфейса

5 Пишем правило преобразования пакета. В нём описывается, какие пакеты должны быть транслированы

```
ip nat inside source list 100 interface GigabitEthernet0/0 overload
```

или

```
ip nat inside source list 100 pool pool2 overload
```

Проверка настройки

После завершения настройки и начала обмена данными в памяти маршрутизатора создаётся временная запись в таблице трансляций.

Пока эта запись существует, к внутреннему хосту открыт доступ из внешней сети по данным из столбца inside global. Эту проблему может решить межсетевой экран

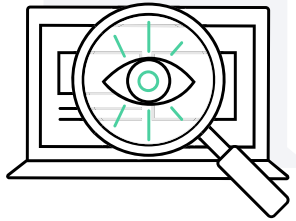
```
sh ip nat tra
Pro Inside global       Inside local       Outside local  Outside global
icmp 173.10.15.12:7     10.10.10.100:7     8.8.8.8:7      8.8.8.8:7
icmp 173.10.15.12:8     10.10.10.100:8     8.8.8.8:8      8.8.8.8:8
icmp 173.10.15.12:9     10.10.10.101:9     8.8.8.8:9      8.8.8.8:9
icmp 173.10.15.12:10    10.10.10.102:10    8.8.8.8:10     8.8.8.8:10
```

Примеры настройки NAT

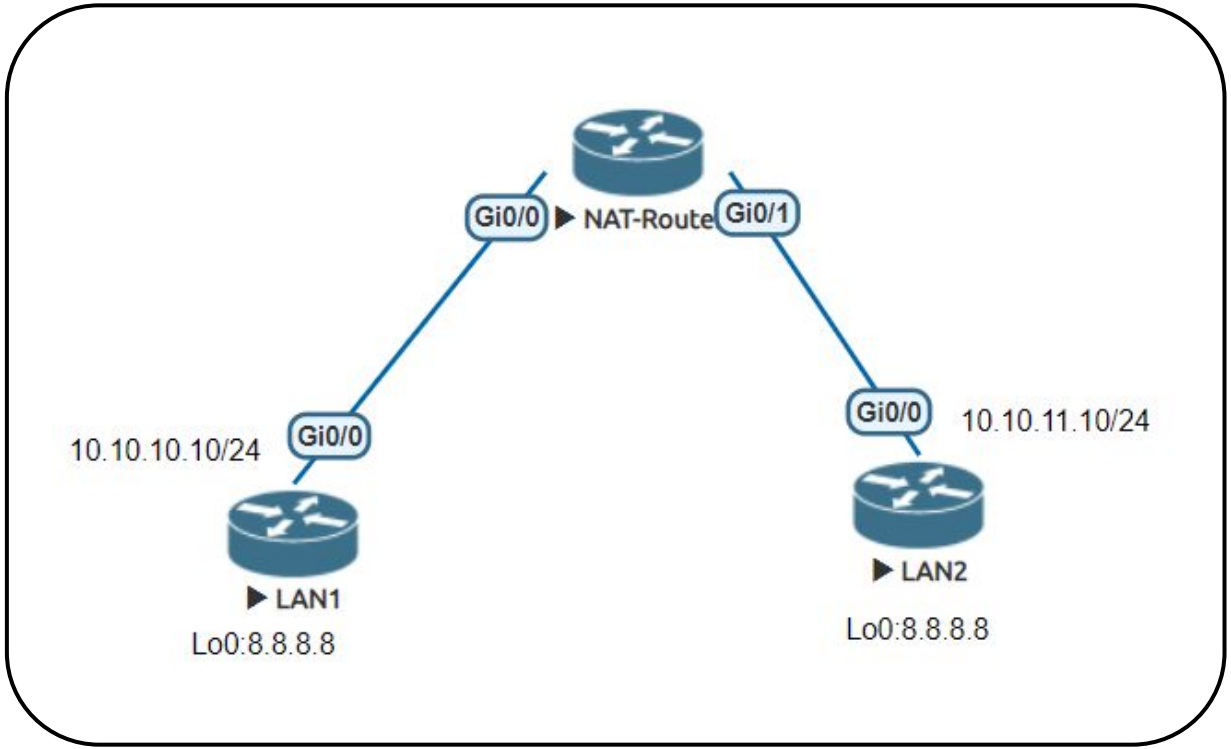
4

Демонстрация работы

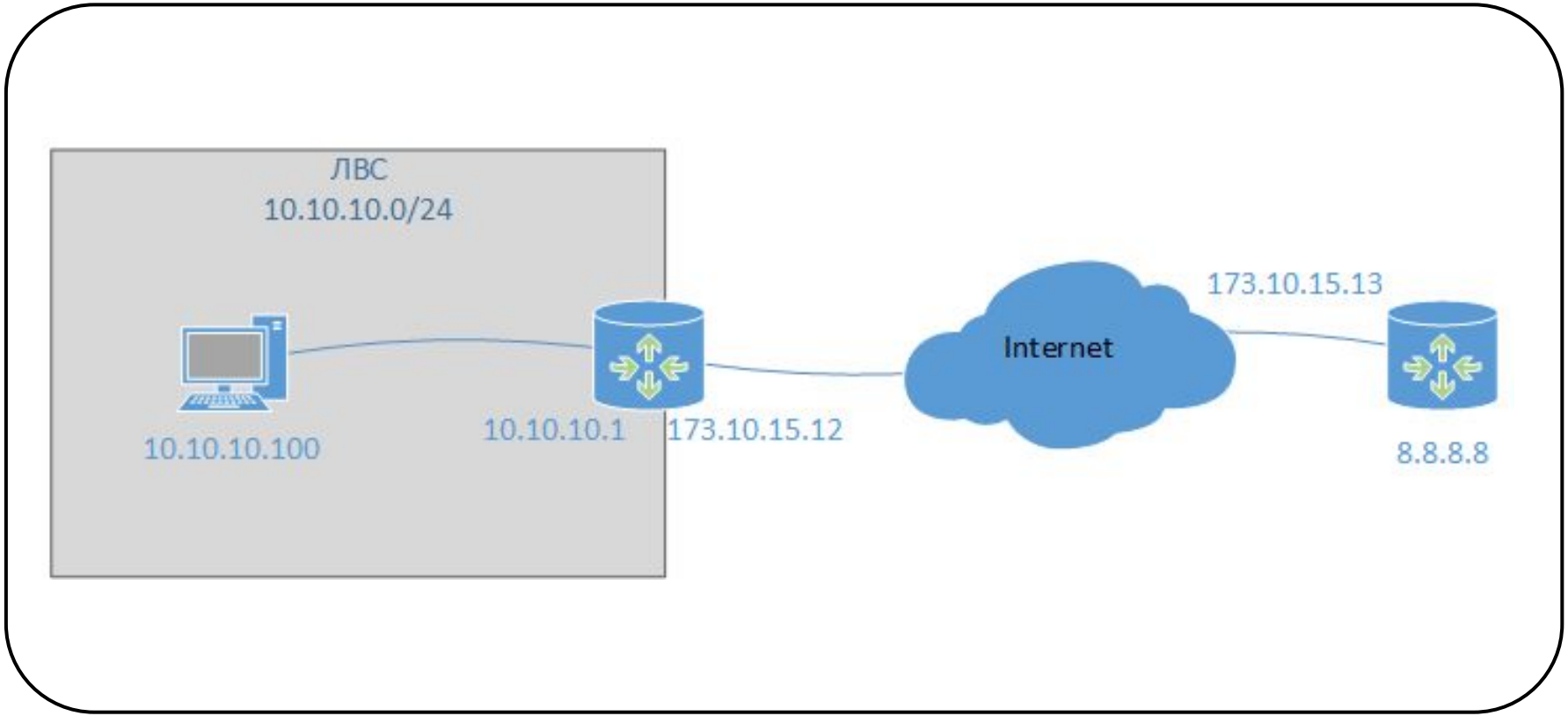
Посмотрим, как работает NAT на примере трёх моделей сетей



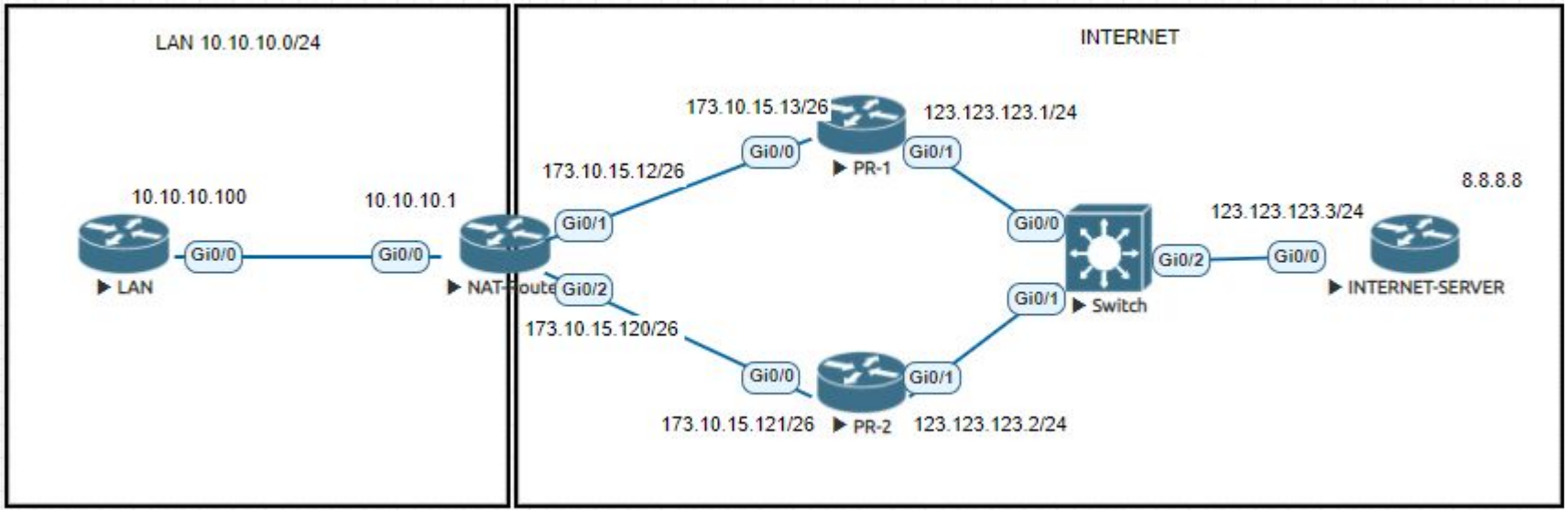
Настройка NAT на устройствах Cisco. Пересекающиеся сети



Настройка NAT на устройствах MikroTik



Настройка NAT с резервированием на Cisco. Проблема ассиметричного роутинга



Плюсы и минусы технологии NAT

5

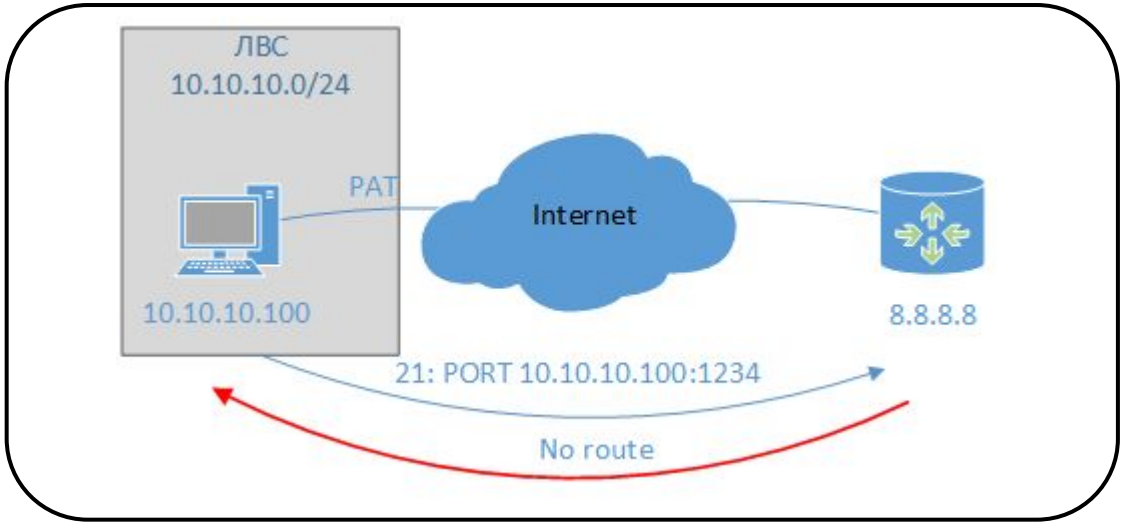
Преимущества

- ✓ Позволяет экономить адресное пространство IPv4
- ✓ Выполняет базовую защиту периметра сети от проникновения извне
- ✓ Реальная адресация ЛВС неизвестна внешним устройствам
- ✓ Позволяет маскировать порты, открытые на внутренних устройствах, и скрывает сервисы, запущенные на них

Недостатки

- В базовой настройке (без ALG) не работает с некоторыми протоколами (ftp, sip)

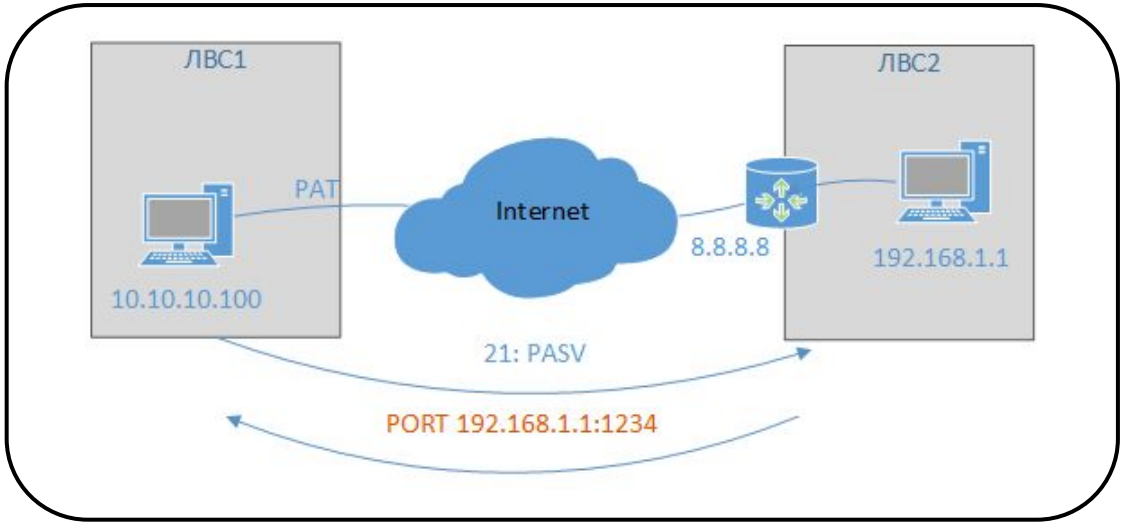
  В активном режиме клиент сообщает серверу свой IP-адрес и порт. В случае, если клиент за PAT overload, связь не установится. Клиент и сервер должны иметь публичные адреса



Недостатки

- В базовой настройке (без ALG) не работает с некоторыми протоколами (ftp, sip)

В пассивном режиме FTP-сервер сообщает клиенту на уровне приложений свой IP-адрес и порт, чтобы клиент мог установить соединение для передачи данных. Когда сервер находится за NAT, он должен отправлять внешний IP-адрес шлюза и порт из того диапазона, который шлюз пробрасывает



Недостатки

- В базовой настройке (без ALG) не работает с некоторыми протоколами (ftp, sip)
- Увеличивает нагрузку на пограничное устройство
- PAT overload для некоторых ресурсов может выглядеть как DoS-атака
- Невозможность идентифицировать реальный источник трафика, находясь в публичной сети

Итоги

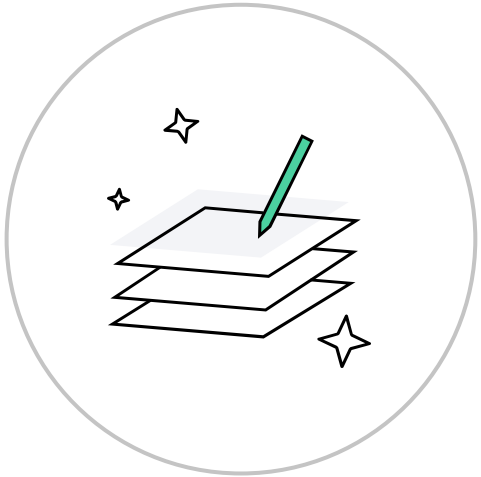
Сегодня мы:

1. Узнали о проблеме ограниченного количества IPv4-адресов и способах её решения
2. Разобрались в терминологии NAT
3. Научились различать типы NAT и выбирать нужный тип под конкретную задачу
4. Рассмотрели плюсы и минусы технологии
5. Попробовали настроить NAT на настоящем оборудовании

Домашнее задание

Давайте посмотрим ваше домашнее задание

1. Вопросы по домашней работе задавайте в чате группы
2. Задачи можно сдавать по частям
3. Зачёт по домашней работе ставят после того, как приняты все задачи



Задавайте вопросы и пишите отзыв о лекции

Сергей Розанов
Сетевой инженер