OTUS

Онлайн образование

otus.ru

Проверить, идет ли запись

Меня хорошо видно && слышно?

Протокол NAT

Андрей Рукин

Инженер ИТ

arukin@m-pr.tv

Правила вебинара

Активно участвуем

Задаем вопросы в чат

Вопросы вижу в чате,
могу ответить не сразу

Условные обозначения

Индивидуально

Время, необходимое на активность

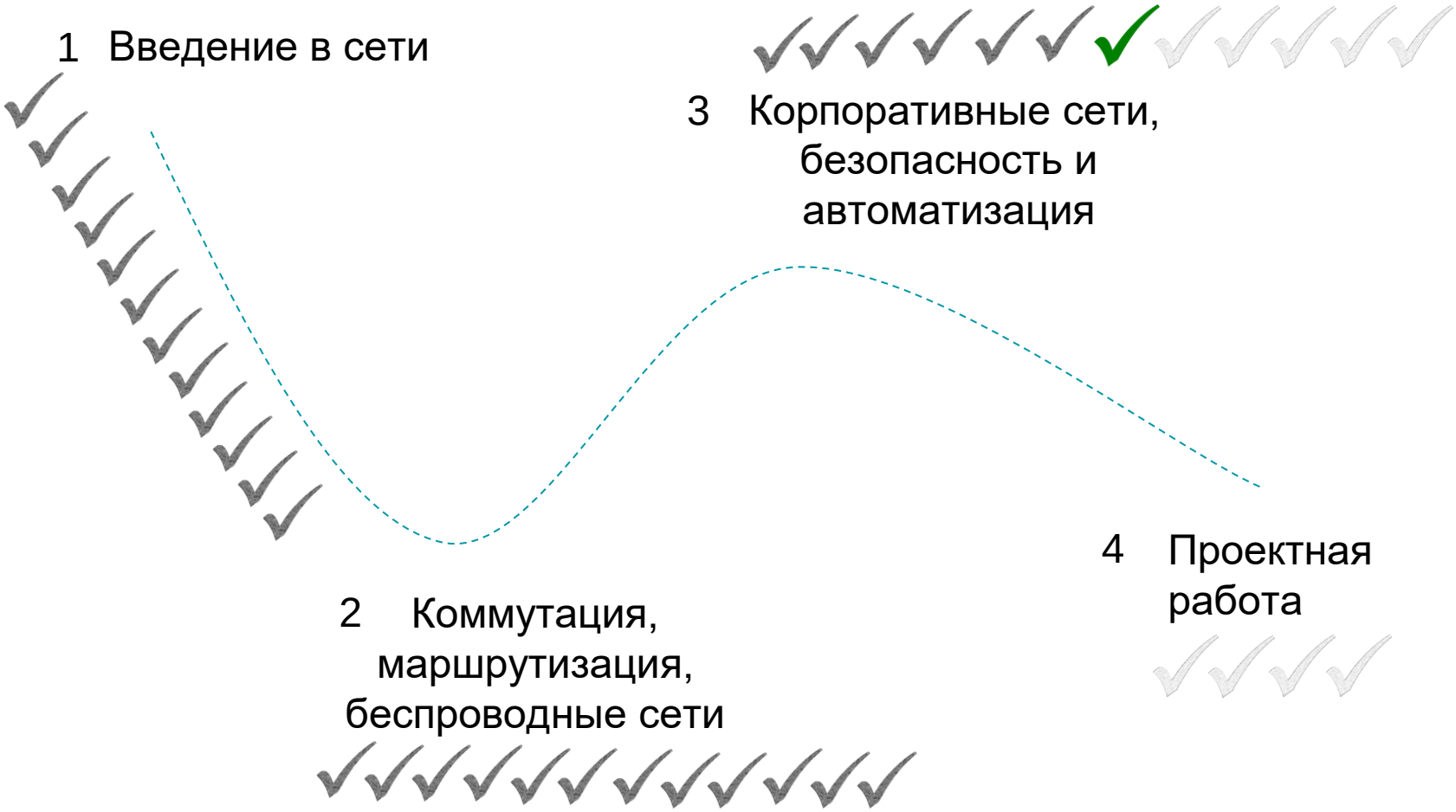
Пишем в чат

Говорим голосом

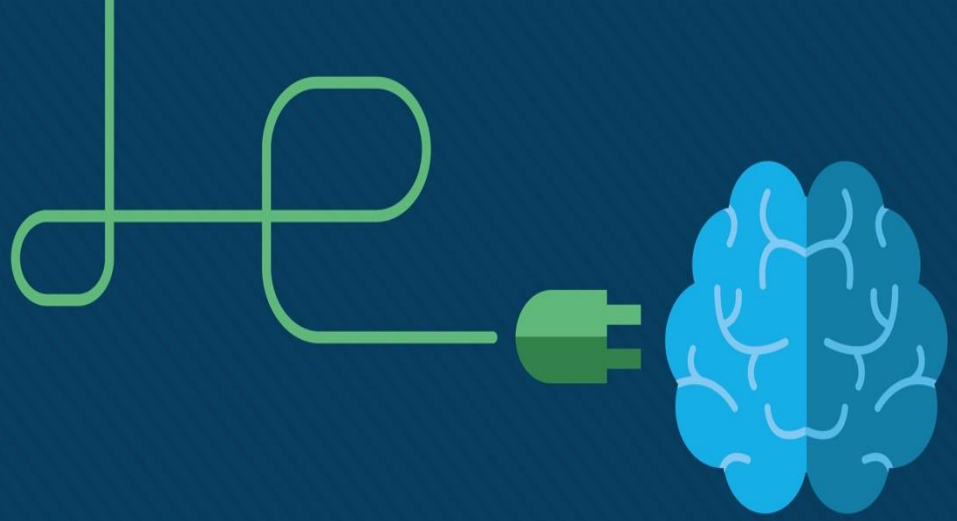
Документ

Ответьте себе или задайте вопрос

Карта курса


1 Введение в сети
3 Корпоративные сети, безопасность и автоматизация
2 Коммутация, маршрутизация, беспроводные сети
4 Проектная работа

Протокол NAT



Модуль 6: NAT для IPv4

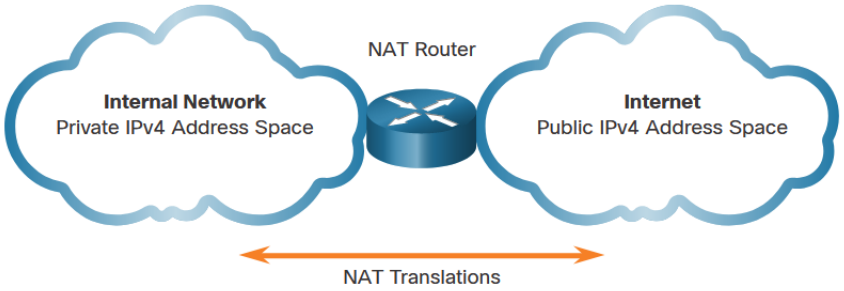
Корпоративные сети, безопасность и автоматизация v7.0 (ENSA)

6.1 Характеристики NAT

Пространство адресов IPv4

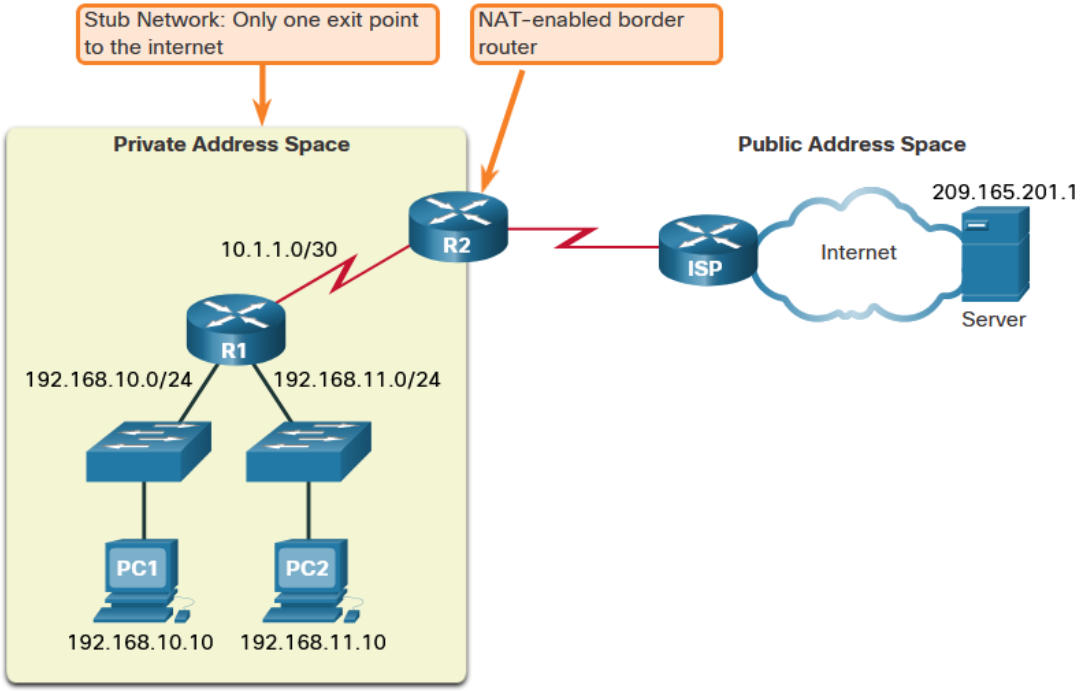
- В большинстве случаев сети реализуются с использованием частных IPv4-адресов в соответствии с RFC 1918.
- Частные адреса IPv4 используются в рамках организации или объекта с целью обеспечения взаимодействия устройств на локальном уровне.
- Для того чтобы разрешить устройству с частным IPv4-адресом получать доступ к устройствам и ресурсам вне локальной сети, частный адрес сначала необходимо преобразовать в публичный адрес.
- NAT обеспечивает преобразование частных адресов в публичные адреса.

Класс	Адреса	Сеть
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



Что такое NAT?

- Основной задачей NAT является экономия публичных IPv4-адресов.
- NAT позволяет сетям внутренне использовать частные адреса IPv4 и преобразовывать их в общедоступный адрес при необходимости.
- Маршрутизатор NAT обычно работает на границе тупиковой сети.
- Когда устройство внутри тупиковой сети хочет взаимодействовать с устройством вне его сети, пакет пересылается на пограничный маршрутизатор, который выполняет процесс NAT, преобразуя внутренний частный адрес устройства в общедоступный, внешний, маршрутизируемый адрес.



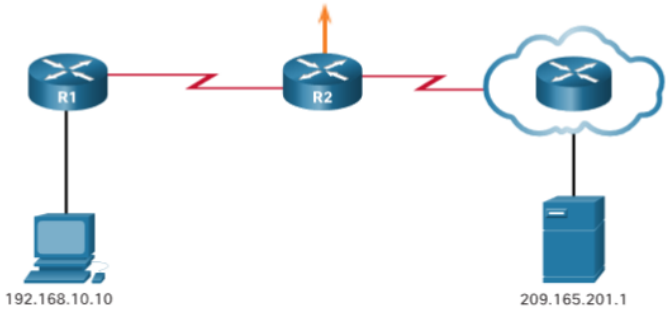
Принципы работы NAT

ПК1 хочет установить связь с внешним веб-сервером с открытым адресом 209.165.201.1.

1. ПК 1 отправляет пакет, адресованный веб-серверу.
2. R2 получает пакет и считывает адрес источника IPv4, чтобы определить, нуждается ли он в переводе.
3. Маршрутизатор R2 добавляет это сопоставление локального и глобального адресов в таблицу NAT.
4. R2 отправляет по назначению пакет с преобразованным адресом источника.
5. Веб-сервер отвечает пакетом, адресованным внутреннему глобальному адресу ПК 1 (209.165.200.226).
6. R2 получает пакет с адресом назначения 209.165.200.226. R2 проверяет таблицу NAT и находит запись для этого сопоставления. R2 использует эту информацию и преобразует внутренний глобальный адрес (209.165.200.226) во внутренний локальный адрес (192.168.10.10), после чего пакет пересылается PC1.

NAT Table

Inside Local	Inside Global	Outside Local	Outside Global
192.168.10.10	209.165.200.226	209.165.201.1	209.165.201.1



Терминология NAT

В NAT предусмотрено 4 типа адресов:

- Внутренний локальный адрес
- Внутренний глобальный адрес
- Внешний локальный адрес
- Внешний глобальный адрес

Терминология NAT всегда применяется с точки зрения устройства с переведенным адресом.

- **Внутренний адрес** — это адрес устройства, преобразуемый механизмом NAT.
- **Внешний адрес** — это адрес устройства назначения.
- **Локальный адрес** — это любой адрес, появляющийся во внутренней части сети.
- **Глобальный адрес** — это любой адрес, появляющийся во внешней части сети.

Терминология NAT (продолжение)

Внутренний локальный адрес

Это адрес источника, видимый из внутренней сети. Обычно это частный IPv4 адрес. Внутренним локальным адресом ПК 1 является 192.168.10.10.

Внутренний глобальный адрес

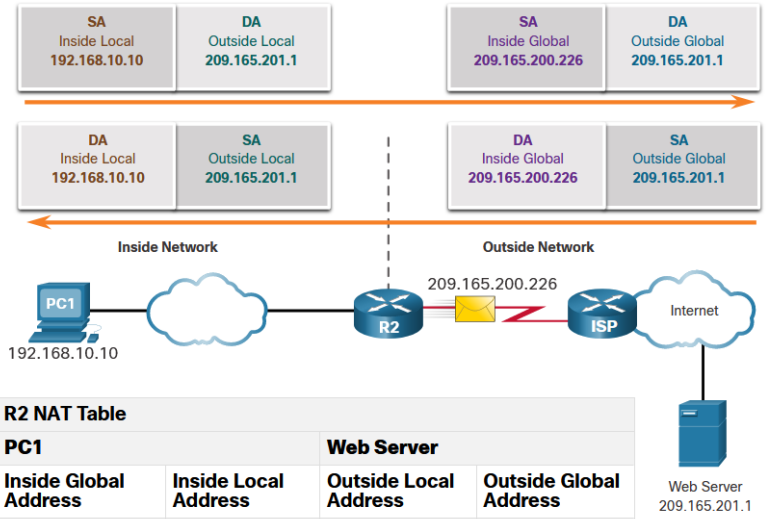
Это адрес источника, видимый из внешней сети. Внутренний глобальный адрес PC1 209.165.200.226

Внешний глобальный адрес

Это адрес назначения, видимый из внешней сети. Внешний глобальный адрес веб-сервера 209.165.201.1

Внешний локальный адрес

Это адрес назначения, видимый из внутренней сети. ПК 1 отправляет трафик веб-серверу с IPv4-адресом 209.165.201.1. В редких случаях этот адрес может отличаться от глобально маршрутизируемого адреса назначения.



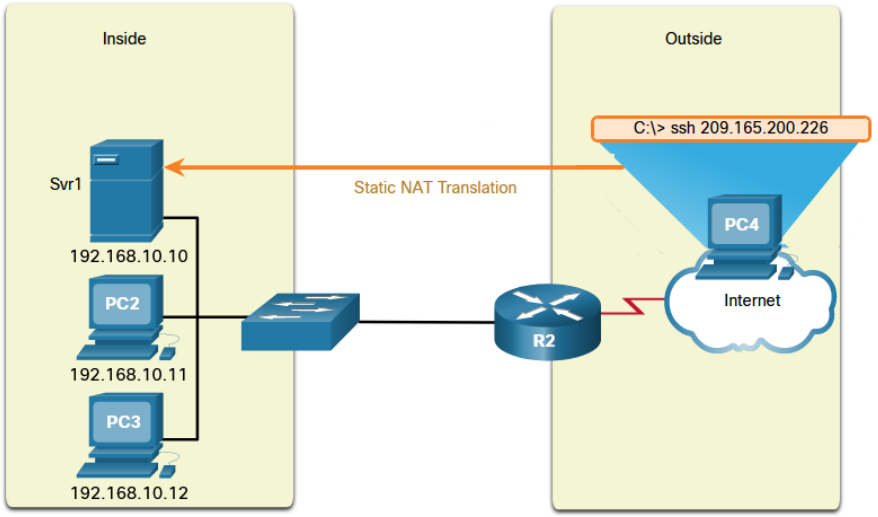
R2 NAT Table			
PC1		Web Server	
Inside Global Address	Inside Local Address	Outside Local Address	Outside Global Address
209.165.200.226	192.168.10.10	209.165.201.1	209.165.201.1

6.2 Типы NAT

Статическое преобразование NAT

Статический NAT использует однозначное сопоставление локальных и глобальных адресов, настроенных сетевым администратором, которые остаются постоянными.

- Метод статического преобразования особенно полезен для веб-серверов или устройств, которые должны иметь постоянный адрес, доступный из Интернета — например, для веб-сервера компании.
- Статический NAT также подходит для устройств, которые должны быть доступны авторизованному персоналу, работающему вне офиса, но при этом оставаться закрытыми для общего доступа через Интернет.



Static NAT Table

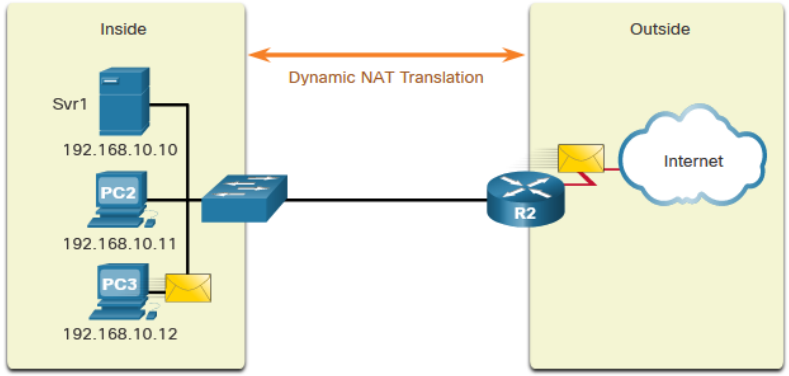
Inside Local Address	Inside Global Address – Addresses reachable via R2
192.168.10.10	209.165.200.226
192.168.10.11	209.165.200.227
192.168.10.12	209.165.200.228

Примечание: Для статического NAT требуется достаточное количество публичных адресов, доступных для общего количества одновременных сеансов пользователей.

Динамическое преобразование NAT

При динамическом преобразовании NAT используется пул публичных адресов, которые назначаются в порядке очереди («первым пришел — первым обслужили»).

- Когда внутреннее устройство запрашивает доступ к внешней сети, динамическое преобразование NAT назначает доступный публичный IPv4-адрес из пула.
- Остальные адреса в пуле по-прежнему доступны для использования.



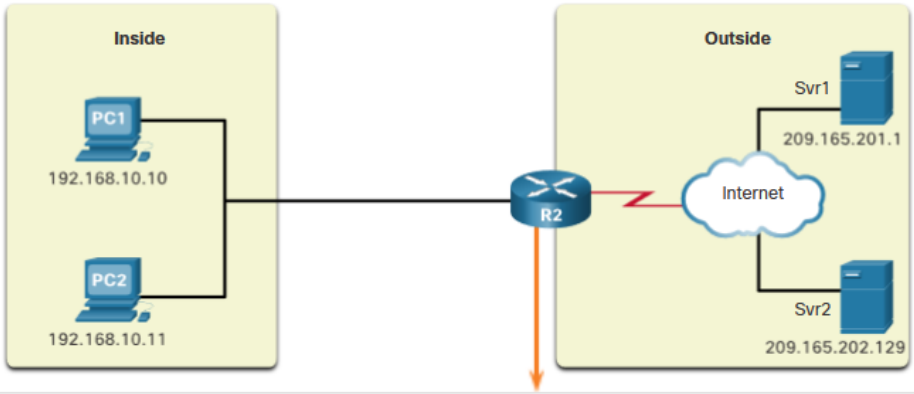
IPv4 NAT Pool	
Inside Local Address	**Inside Global Address Pool - Addresses reachable via R2**
192.168.10.12	209.165.200.226
Available	209.165.200.227
Available	209.165.200.228
Available	209.165.200.229
Available	209.165.200.230

Примечание: Для динамического NAT требуется достаточное количество публичных адресов, доступных для общего количества одновременных сеансов пользователей.

Преобразование адресов портов (PAT)

Преобразование адреса и номера порта (PAT), также называемое NAT с перегрузкой, сопоставляет множество частных IPv4-адресов одному или нескольким публичным IPv4-адресам.

- Если маршрутизатор NAT получает пакет от клиента, он использует свой номер порта источника, чтобы уникальным образом определить конкретное преобразование NAT.
- PAT гарантирует, что устройства будут использовать разные номера портов TCP для каждого сеанса взаимодействия с сервером в Интернете.



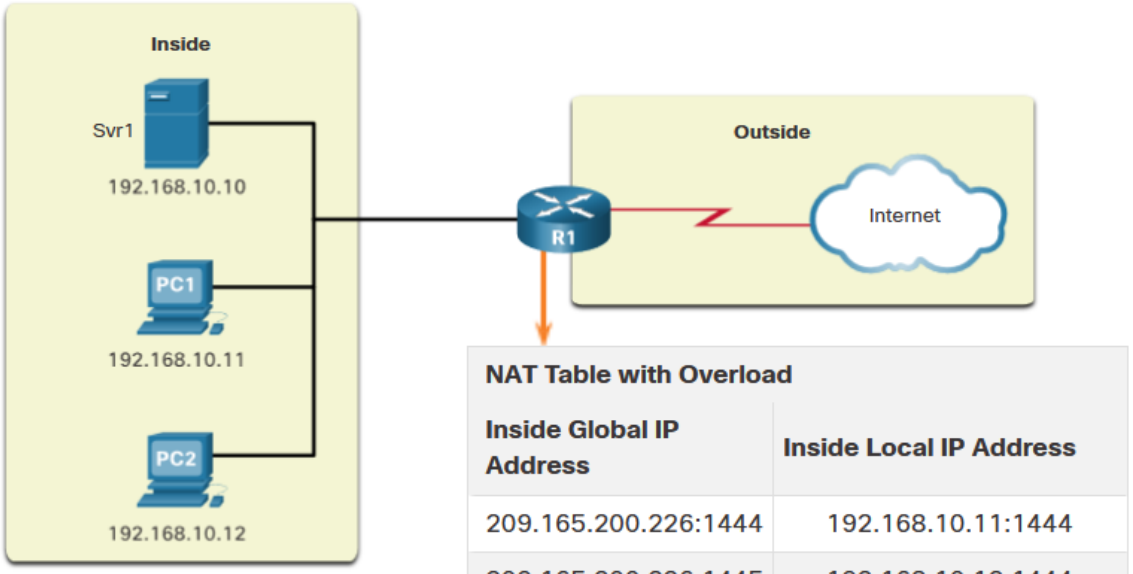
NAT Table with Overload

Inside Local IP Address	Inside Global IP Address	Outside Local IP Address	Outside Global IP Address
192.168.10.10:1555	209.165.200.226:1555	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1331	209.165.200.226:1331	209.165.202.129:80	209.165.202.129:80

Следующий доступный порт

Преобразование PAT пытается сохранить оригинальный порт источника. Если первоначальный порт источника уже используется, PAT назначает первый доступный номер порта, начиная с наименьшего в соответствующей группе портов: 0-511, 512-1,023, или 1,024-65,535.

- Если доступных портов больше нет, а в пуле адресов есть несколько внешних адресов, PAT переходит к следующему адресу, пытаясь выделить первоначальный порт источника.
- Данный процесс продолжается до тех пор, пока не исчерпаются как доступные порты, так и внешние IPv4-адреса в пуле адресов.



NAT Table with Overload

Inside Global IP Address	Inside Local IP Address
209.165.200.226:1444	192.168.10.11:1444
209.165.200.226:1445	192.168.10.12:1444

Сравнение NAT и PAT

Резюме различий между NAT и PAT.

NAT - изменяет только адреса IPv4

Внутренний глобальный адрес	Внутренний локальный адрес
209.165.200.226	192.168.10.10

PAT - В то же время PAT меняет и адрес, и номер порта.

Внутренний глобальный адрес	Внутренний локальный адрес
209.165.200.226:2031	192.168.10.10:2031

NAT	PAT
Сопоставление локальных и глобальных адресов по схеме «один к одному»	Один внутренний глобальный адрес может быть сопоставлен со многими внутренними локальными адресами.
В процессе преобразования использует только адреса IPv4.	Использует IPv4 адреса и номера портов источника TCP или UDP в процессе преобразования.
Уникальный внутренний глобальный адрес необходим для каждого внутреннего узла, обращающегося к внешней сети.	Один уникальный внутренний глобальный адрес может быть общим для многих внутренних узлов, обращающихся к внешней сети.

Пакеты без сегмента 4 уровня

Некоторые пакеты не содержат номера порта уровня 4, например сообщения ICMPv4. Процесс преобразования PAT обрабатывает каждый из этих протоколов по-разному.

Например, сообщения запросов ICMPv4, эхо-запросы и эхо-ответы содержат идентификатор запроса (Query ID). ICMPv4 использует идентификатор запроса (Query ID), чтобы сопоставить эхо-запрос с соответствующим эхо-ответом.

Примечание. Другие сообщения ICMPv4 не используют идентификатор запроса (Query ID). Эти сообщения и другие протоколы, не использующие номера портов TCP и UDP, могут отличаться друг от друга и не рассматриваются в рамках материала настоящего учебного курса.

6.3 Преимущества и недостатки NAT

Преимущества NAT

NAT обеспечивает множество **преимуществ**:

- NAT сохраняет официально зарегистрированную схему адресации, разрешая частное использование внутренних сетей.
- NAT экономит адреса благодаря мультиплексированию приложений на уровне портов.
- NAT повышает гибкость подключений к публичной сети.
- NAT обеспечивает постоянство схем внутренней сетевой адресации.
- NAT позволяет сохранить существующую схему частных IPv4-адресов, одновременно поддерживая простой переход на новую схему публичной адресации.
- NAT скрывает адреса IPv4 пользователей и других устройств.

Недостатки NAT

NAT имеет ряд **недостатков**:

- NAT увеличивает задержки пересылки.
- Конечная адресация теряется.
- Теряется сквозная отслеживаемость IPv4-адресов
- NAT усложняет использование протоколов туннелирования, таких как IPsec.
- Работа служб, требующих инициализации подключений TCP из внешней сети или использующих протоколы без учета состояния, например, на основе UDP, может быть нарушена.

Вопросы?

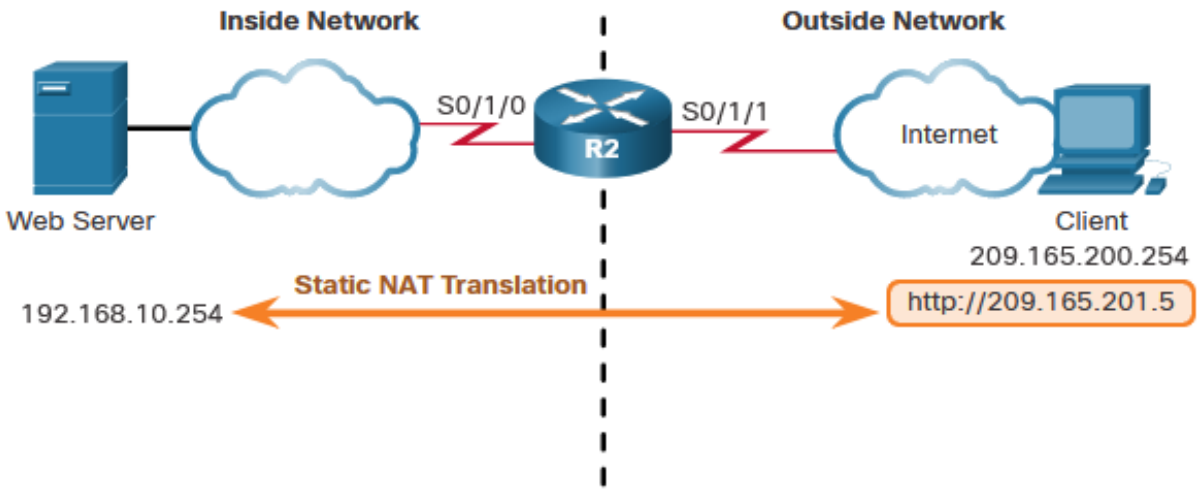
Ставим “+”,
если вопросы есть

Ставим “–”,
если вопросов нет

6.4 Статическое преобразование NAT

Сценарий статического преобразования NAT

- Статическое преобразование NAT — это взаимно-однозначное сопоставление внутреннего и внешнего адресов.
- Статический NAT позволяет внешним устройствам инициировать подключение к внутренним устройствам с помощью статически назначенного публичного адреса.
- Например, внутреннему веб-серверу может быть сопоставлен внутренний глобальный адрес, определенный таким образом, чтобы он был доступен из внешних сетей.



Настройка статического NAT

Настройка статического NAT сопряжена с двумя основными задачами.

- **Шаг 1** - Создание сопоставления между внутренним локальным адресом и внутренними глобальными адресами с помощью команды ip nat inside source static.

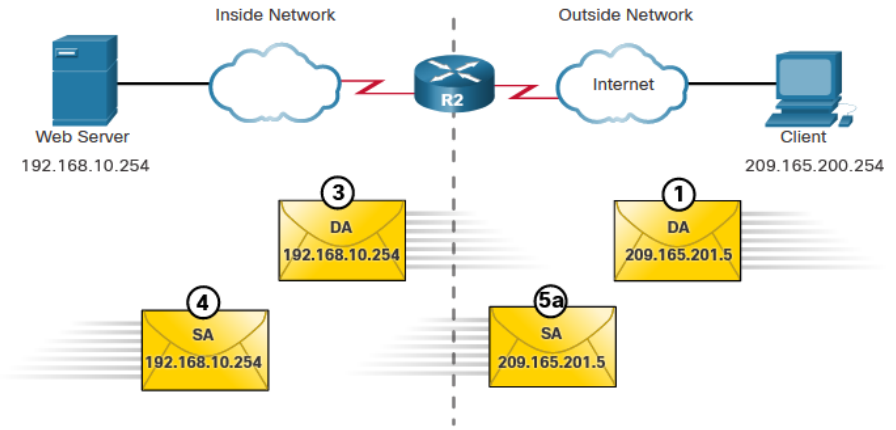
- **Шаг 2** - Интерфейсы, участвующие в преобразовании, настраиваются как внутри, так и снаружи по отношению к NAT с командами ip nat inside и ip nat outside.

```
R2(config)# ip nat inside source static 192.168.10.254 209.165.201.5
R2(config)#
R2(config)# interface serial 0/1/0
R2(config-if)# ip address 192.168.1.2 255.255.255.252
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface serial 0/1/1
R2(config-if)# ip address 209.165.200.1 255.255.255.252
R2(config-if)# ip nat outside
```

Анализ статического преобразования NAT

Статический процесс преобразования NAT между клиентом и веб-сервером:

1. Клиент отправляет пакет на веб-сервер.
2. R2 получает пакеты от клиента по внешнему интерфейсу NAT и проверяет его таблицу NAT.
3. R2 переводит внутренний глобальный адрес на внутренний локальный адрес и пересылает пакет на веб-сервер.
4. Веб-сервер получает пакет и отвечает клиенту, используя внутренний локальный адрес.
5. (a) R2 получает пакет от веб-сервера на свой внутренний интерфейс NAT с адресом источника, соответствующим внутреннему локальному адресу веб-сервера, и (б) переводит исходный адрес во внутренний глобальный адрес.



	Inside Local Address	Inside Global Address	Outside Local Address	Outside Global Address
2 5b	192.168.10.254	209.165.201.5	209.165.200.254	209.165.200.254

Проверка статического NAT

Чтобы проверить операцию NAT, выполните команду **show ip nat translations**.

- Эта команда отображает активные преобразования NAT.
- Поскольку в примере приводится статическая настройка, преобразование всегда присутствует в таблице NAT независимо от активных взаимодействий.
- Если команда вводится во время активного сеанса, выходные данные будут также содержать адрес внешнего устройства.

```
R2# show ip nat translations
Pro Inside global Inside local Outside local Outside global
— 209.165.201.5 192.168.10.254 — —
Total number of translations: 1
```

```
R2# show ip nat translations
Pro Inside global Inside local Outside local Outside global
tcp 209.165.201.5 192.168.10.254 209.165.200.254 209.165.200.254
— 209.165.201.5 192.168.10.254 — —
Total number of translations: 2
```

Проверка статического NAT

Другой полезной командой является **show ip nat statistics**.

- Она выводит сведения о суммарном количестве активных преобразований, параметрах настройки NAT, числе адресов в пуле и числе выделенных адресов.
- Чтобы убедиться в правильности работы преобразования NAT, перед тестированием рекомендуется очистить статистику всех предыдущих преобразований с помощью команды **clear ip nat statistics**.

```
R2# show ip nat statistics
Total active translations: 1 (1 static, 0 dynamic; 0 extended)
Outside interfaces:
  Serial0/1/1
Inside interfaces:
  Serial0/1/0
Hits: 4 Misses: 1
(дальше выходные данные опущены)
```

Вопросы?

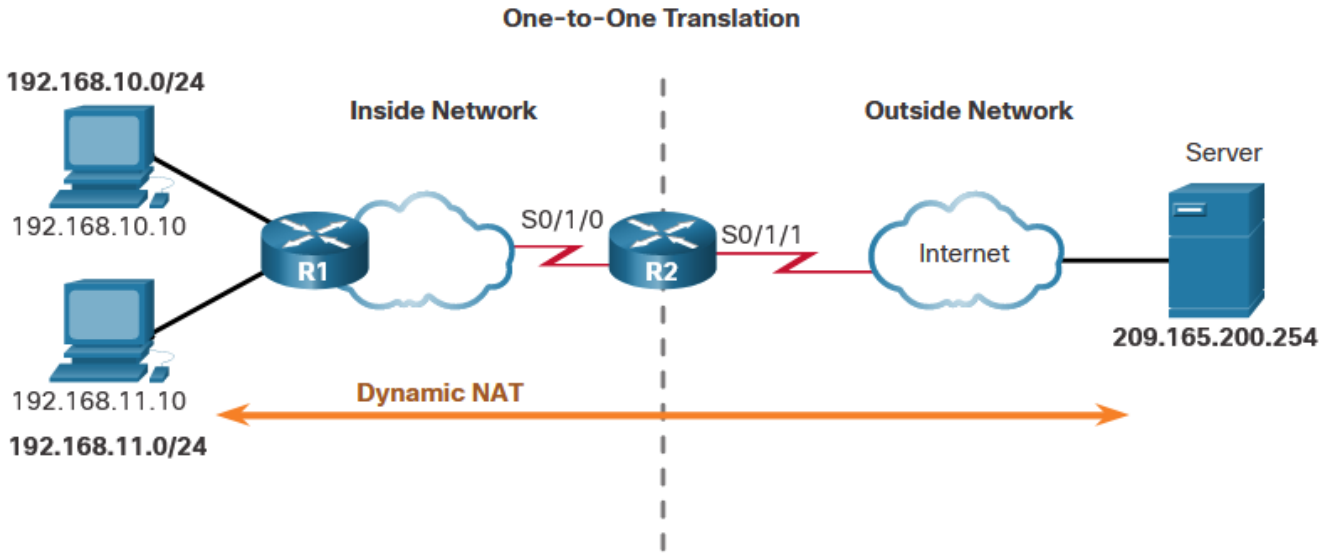
Ставим “+”,
если вопросы есть

Ставим “–”,
если вопросов нет

6.5 Динамическое преобразование NAT

Сценарий динамического преобразования NAT

- Динамический NAT автоматически сопоставляет внутренние локальные адреса с внутренними глобальными адресами.
- Динамическое преобразование NAT использует пул внутренних глобальных адресов.
- Пул внутренних глобальных адресов доступен для любого устройства во внутренней сети в порядке очереди.
- Если использованы все адреса пула, устройство должно дождаться доступного адреса, чтобы получить доступ к внешней сети.



Настройка динамического NAT

Настройка динамического NAT сопряжена с 5 основными задачами.

- **Шаг 1 -** С помощью команды **ip nat pool** определите пул адресов, которые будут использоваться для преобразования.
- **Шаг 2** - Настройте стандартный ACL, чтобы определить (разрешить) только те адреса, которые должны быть преобразованы.
- Шаг 3. Привяжите ACL к пулу, используя команду ip nat inside source list.

```
R2(config)# ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL1
```

Настройка динамического NAT (продолжение)

Настройка динамического NAT сопряжена с 5 основными задачами.

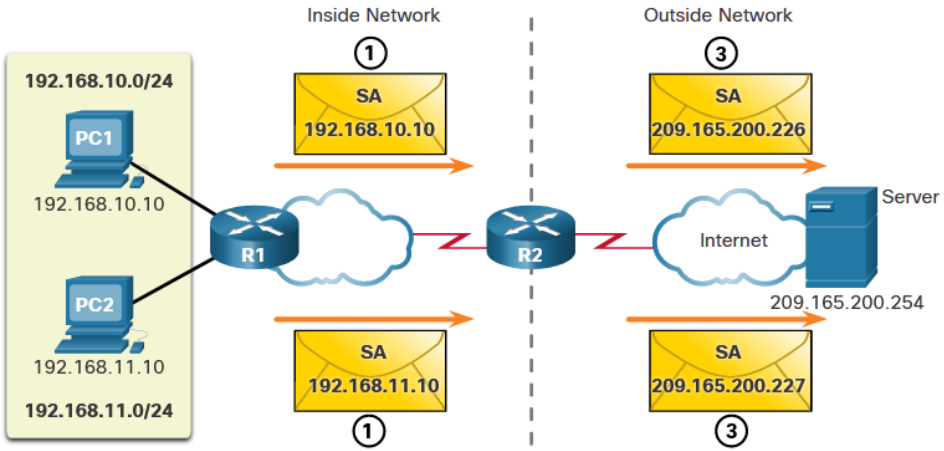
- **Шаг 4** - Определите, какие интерфейсы находятся внутри.
- **Шаг 5** - Определите, какие интерфейсы находятся снаружи.

```
R2(config)# ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL1
R2(config)# interface serial 0/1/0
R2(config-if)# ip nat inside
R2(config-if)# interface serial 0/1/1
R2(config-if)# ip nat outside
```

Анализ динамического NAT

Процесс преобразования динамического NAT

1. PC1 и PC2 отправляют пакеты, запрашивающие подключение к серверу.
2. R2 получает первый пакет от PC1, проверяет ALC, чтобы определить, должен ли пакет быть преобразован, выбирает доступный глобальный адрес и создает запись преобразования в таблице NAT.
3. R2 заменяет внутренний локальный адрес источника ПК 1 (192.168.10.10) используемым для преобразования внутренним глобальным адресом (209.165.200.226) и пересылает пакет. (Те же действия выполняются для пакета, отправленного ПК 2, с использованием для преобразования адреса, соответствующего 209.165.200.227.)

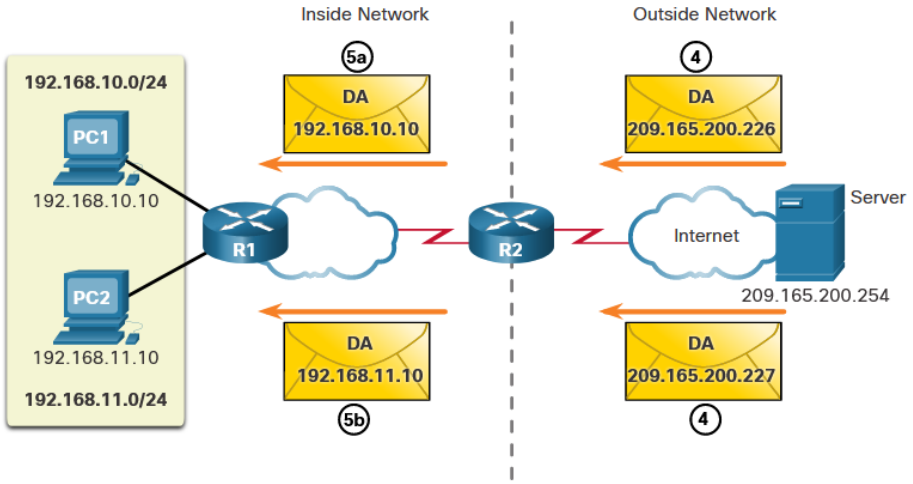


IPv4 NAT Pool	
Inside Local Address Pool	**Inside Global Address**
192.168.10.10	209.165.200.226
192.168.11.10	209.165.200.227

Анализ динамического NAT

Процесс преобразования динамического NAT

4. Сервер получает пакет от ПК 1 и отвечает, используя адрес назначения 209.165.200.226. Сервер получает пакет от ПК 2, и отвечает, используя IPv4-адрес назначения 209.165.200.227.
5. (a) Когда R2 получает пакет с адресом назначения 209.165.200.226; он выполняет поиск таблицы NAT и переводит адрес обратно на внутренний локальный адрес и пересылает пакет на PC1.
(b) Когда R2 получает пакет с адресом назначения 209.165.200.227; он выполняет поиск таблицы NAT и переводит адрес обратно на внутренний локальный адрес 192.168.11.10 и пересылает пакет на PC2.

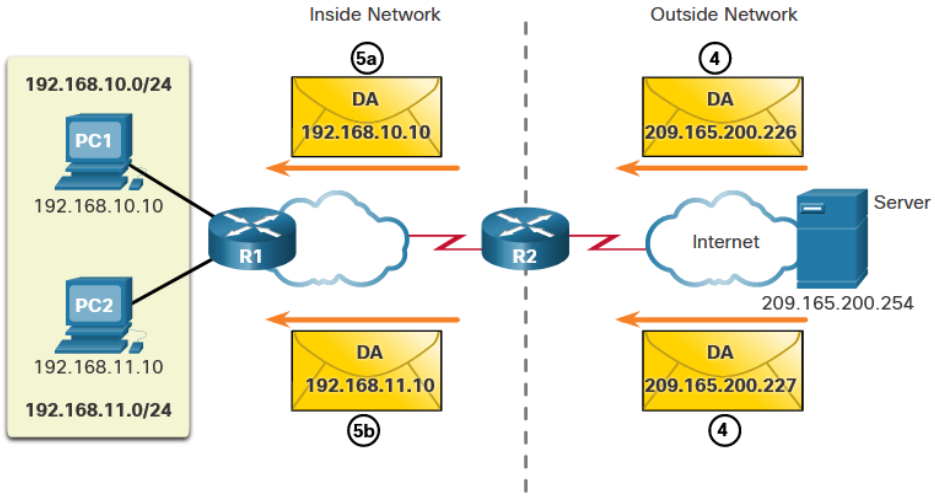


	IPv4 NAT Pool	
	Inside Local Address Pool	Inside Global Address
5a	192.168.10.10	209.165.200.226
5b	192.168.11.10	209.165.200.227

Анализ динамического NAT (продолжение)

Процесс преобразования динамического NAT

6. PC1 и PC2 получают пакеты и продолжают диалог. Маршрутизатор NAT выполняет шаги 2-5 для каждого пакета



	IPv4 NAT Pool	
	Inside Local Address Pool	Inside Global Address
5a	192.168.10.10	209.165.200.226
5b	192.168.11.10	209.165.200.227

Проверка динамического NAT

Команда **show ip nat translations** отображает все настроенные статические преобразования адресов и все динамические преобразования, созданные в результате обработки трафика.

```
R2# show ip nat translations
Pro Inside global Inside local Outside local Outside global
— 209.165.200.228 192.168.10.10 — —
— 209.165.200.229 192.168.11.10 — —
R2#
```

Проверка динамического NAT (продолжение)

Добавление ключевого слова **verbose** выводит дополнительную информацию о каждом преобразовании, включая время, прошедшее после создания и использования записи.

```
R2# show ip nat translation verbose
Pro Inside global Inside local Outside local Outside global
tcp 209.165.200.228 192.168.10.10 --- ---
    create 00:02:11, use 00:02:11 timeout:86400000, left 23:57:48, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 10, lc_entries: 0
tcp 209.165.200.229 192.168.11.10 --- ---
    create 00:02:10, use 00:02:10 timeout:86400000, left 23:57:49, Map-Id(In): 1,
    flags:
none, use_count: 0, entry-id: 12, lc_entries: 0
R2#
```

Проверка динамического NAT (продолжение)

По умолчанию срок действия записей преобразования истекает через 24 часа, если настройка таймеров не была изменена с помощью команды режима глобальной конфигурации **ip nat translation timeout** *timeout-seconds*. Для удаления динамических записей до истечения их времени действия используйте команду привилегированного режима EXEC **clear ip nat translation**

```
R2# clear ip nat translation *
R2# show ip nat translation
```

Команда	Описание
clear ip nat translation *	Удаляет все записи динамического преобразования из таблицы преобразования NAT.
clear ip nat translation inside *global-ip local-ip* [**outside** *local-ip global-ip*]	Удаляет запись простого динамического преобразования, которая содержит преобразование внутренних адресов или преобразования и внешних, и внутренних адресов.
clear ip nat translation *protocol* **inside** *global-ip global-port local-ip local-port* [**outside** *local-ip local-port global-ip global-port*]	Удаляет расширенную запись динамического преобразования.

Проверка динамического NAT (продолжение)

Команда **show ip nat statistics** выводит сведения о суммарном количестве активных преобразований, параметрах настройки NAT, числе адресов в пуле и числе выделенных адресов.

```
R2# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 0 extended)
Peak translations: 4, occurred 00:31:43 ago
Outside interfaces:
  Serial0/1/1
Inside interfaces:
  Serial0/1/0
Hits: 47 Misses: 0
CEF Translated packets: 47, CEF Punted packets: 0
Expired translations: 5
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool NAT-POOL1 refcount 4
 pool NAT-POOL1: netmask 255.255.255.224
        start 209.165.200.226 end 209.165.200.240
        type generic, total addresses 15, allocated 2 (13%), misses 0
(дальше выходные данные опущены)
R2#
```

Проверка динамического NAT (продолжение)

В качестве альтернативы можно воспользоваться командой **show running-config** и найти команды NAT, ACL, интерфейса или пула с нужными значениями.

```
R2# show running-config | include NAT
ip nat pool NAT-POOL1 209.165.200.226 209.165.200.240 netmask 255.255.255.224
ip nat inside source list 1 pool NAT-POOL1
```

Вопросы?

Ставим “+”,
если вопросы есть

Ставим “–”,
если вопросов нет

6.6 – PAT

Настройка PAT для использования одного адреса IPv4

Чтобы настроить PAT на использование одного IPv4-адреса, просто добавьте ключевое слово **overload** в команду **ip nat inside source**.

В этом примере для всех узлов сети 192.168.0.0/16 (соответствующей ACL-списку 1), отправляющих трафик в Интернет через маршрутизатор R2, будет выполняться преобразование в IPv4-адрес 209.165.200.225 (IPv4-адрес интерфейса S0/1/1). Потоки трафика будут определяться номерами портов в таблице NAT, поскольку было использовано ключевое слово **overload**.

```
R2(config)# ip nat inside source list 1 interface serial 0/1/0 overload
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# interface serial 0/1/0
R2(config-if)# ip nat inside
R2(config-if)# exit
R2(config)# interface serial 0/1/1
R2(config-if)# ip nat outside
```

Настройка PAT для использования пула адресов

Интернет-провайдер может выделить организации более одного публичного адреса IPv4. В этом случае организация может настроить PAT для использования пула публичных адресов IPv4 для преобразования.

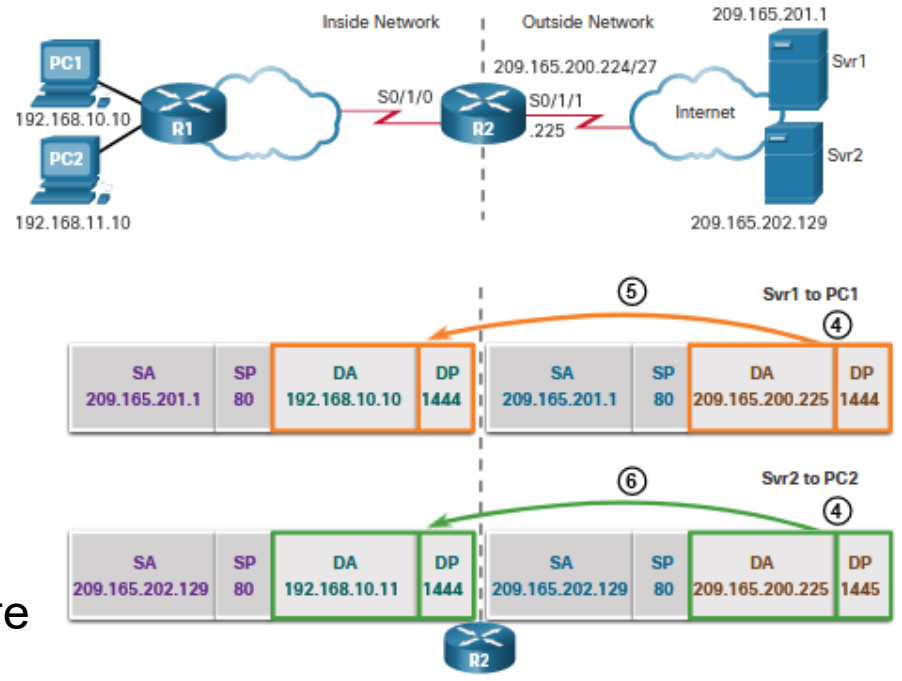
Чтобы настроить PAT для динамического пула адресов NAT, просто добавьте ключевое слово **overload** в команду **ip nat inside source** .

В этом примере NAT-POOL2 привязан к ACL, чтобы разрешить преобразование 192.168.0.0/16. Эти узлы могут совместно использовать IPv4 адрес из пула, так как PAT включен с помощью ключевого слова **overload**.

```
R2(config)# ip nat pool NAT-POOL2 209.165.200.226 209.165.200.240 netmask
255.255.255.224
R2(config)# access-list 1 permit 192.168.0.0 0.0.255.255
R2(config)# ip nat inside source list 1 pool NAT-POOL2 overload
R2(config)# interface serial 0/1/0
R2(config-if)# ip nat inside
R2 (config-if) # interface serial 0/1/0
R2(config-if)# ip nat outside
```

Анализ PAT – От сервера к ПК

1. PC1 и PC2 отправляют пакеты на Svr1 и Svr2.
2. Пакет компьютера ПК 1 первым достигает маршрутизатора R2. R2 изменяет IPv4-адрес источника на 209.165.200.225 (внутренний глобальный адрес). Затем пакет пересылается к Svr1.
3. Пакет от PC2 поступает на R2. PAT изменяет IPv4-адрес источника ПК 2 на внутренний глобальный адрес 209.165.200.225. Однако в этом пакете ПК 2 используется номер порта источника, обеспечивающей преобразование для ПК 1. PAT увеличивает номер порта источника, пока его значение не окажется уникальным для данной таблицы. В данном случае, 1445.

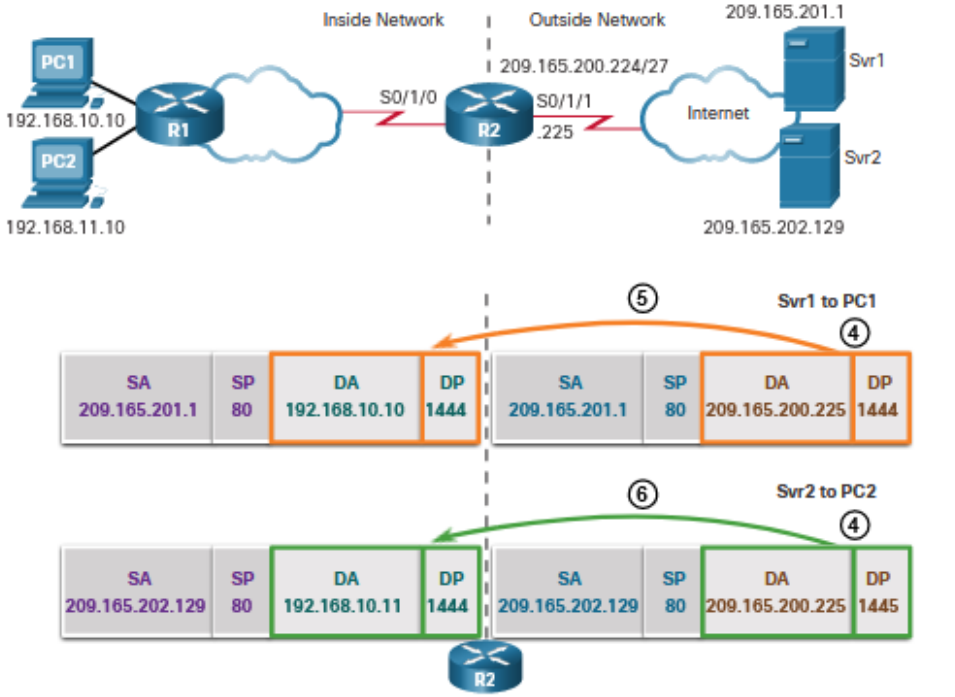


NAT Table

Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.225:1445	209.165.201.129:80	209.165.202.129:80

Анализ PAT — От ПК до сервера

1. PC1 и PC2 отправляют пакеты на Svr1 и Svr2.
2. Пакет компьютера ПК 1 первым достигает маршрутизатора R2. R2 изменяет IPv4-адрес источника на 209.165.200.225 (внутренний глобальный адрес). Затем пакет пересылается к Svr1.
3. Пакет от PC2 поступает на R2. PAT изменяет IPv4-адрес источника ПК 2 на внутренний глобальный адрес 209.165.200.225. Однако в этом пакете ПК 2 используется номер порта источника, обеспечивающей преобразование для ПК 1. PAT увеличивает номер порта источника, пока его значение не окажется уникальным для данной таблицы. В данном случае это 1445.

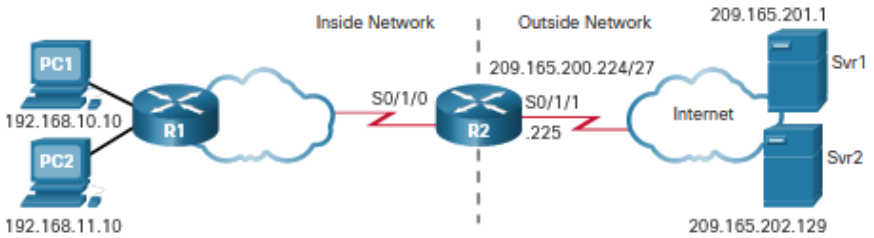


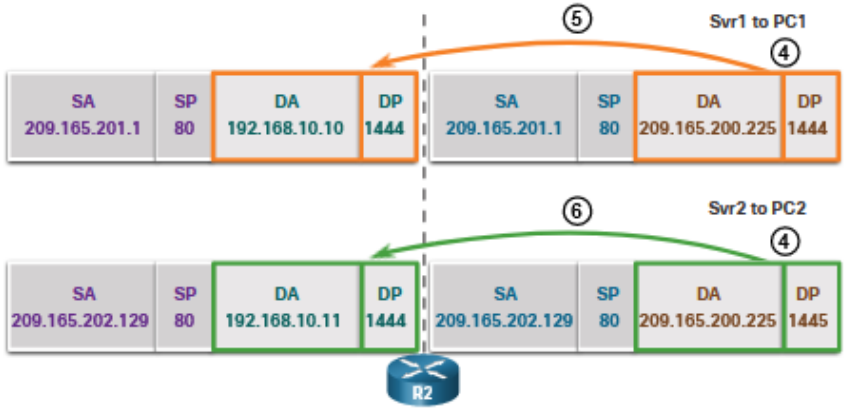
NAT Table

Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.225:1445	209.165.201.129:80	209.165.202.129:80

Анализ PAT — От сервера к ПК

1. Серверы используют для обратного трафика порт источника из полученного пакета в качестве порта назначения и адрес источника — в качестве адреса назначения.
2. R2 изменяет адрес назначения IPv4 пакета с Srv1 с 209.165.200.225 на 192.168.10.10 и пересылает пакет на PC1.
3. R2 изменяет адрес назначения пакета с Srv2. с 209.165.200.225 на 192.168.10.11. и изменяет порт назначения обратно на исходное значение 1444. Затем пакет пересылается компьютеру ПК 2.





NAT Table

Inside Local Address	Inside Global Address	Outside Global Address	Outside Local Address
192.168.10.10:1444	209.165.200.225:1444	209.165.201.1:80	209.165.201.1:80
192.168.10.11:1444	209.165.200.225:1445	209.165.201.129:80	209.165.202.129:80

Проверка PAT

Для проверки PAT используются те же команды, что и для проверки статического и динамического NAT. Команда **show ip nat translations** выводит преобразования для трафика от двух различных узлов к различным веб-серверам. Обратите внимание, что двум различным внутренним узлам выделяется один и тот же IPv4-адрес 209.165.200.226 (внутренний глобальный адрес). Для различения этих двух транзакций в таблице NAT используются номера портов источников.

```
R2# show ip nat translations
Pro Inside global Inside local Outside local Outside global
tcp 209.165.200.225:1444 192.168.10.10:1444 209.165.201.1:80 209.165.201.1:80
tcp 209.165.200.225:1445 192.168.11.10:1444 209.165.202.129:80
209.165.202.129:80
R2#
```

Проверка PAT (продолжение)

Команда **show ip nat statistics** позволяет проверить, что в пуле NAT-POOL2 выделен один адрес для обоих преобразований. В выходных данных команды содержатся сведения о количестве и типе активных преобразований, параметрах настройки NAT, количестве адресов в пуле и количестве выделенных адресов.

```
R2# show ip nat statistics
Total active translations: 4 (0 static, 2 dynamic; 2 extended)
Peak translations: 2, occurred 00:31:43 ago
Outside interfaces:
  Serial0/1/1
Inside interfaces:
  Serial0/1/0
Hits: 4 Misses: 0
CEF Translated packets: 47, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 3] access-list 1 pool NAT-POOL2 refcount 2
 pool NAT-POOL2: netmask 255.255.255.224
        start 209.165.200.225 end 209.165.200.240
        type generic, total addresses 15, allocated 1 (6%), misses 0
(дальше выходные данные опущены)
R2#
```

Вопросы?

Ставим “+”,
если вопросы есть

Ставим “–”,
если вопросов нет

6.7 NAT64

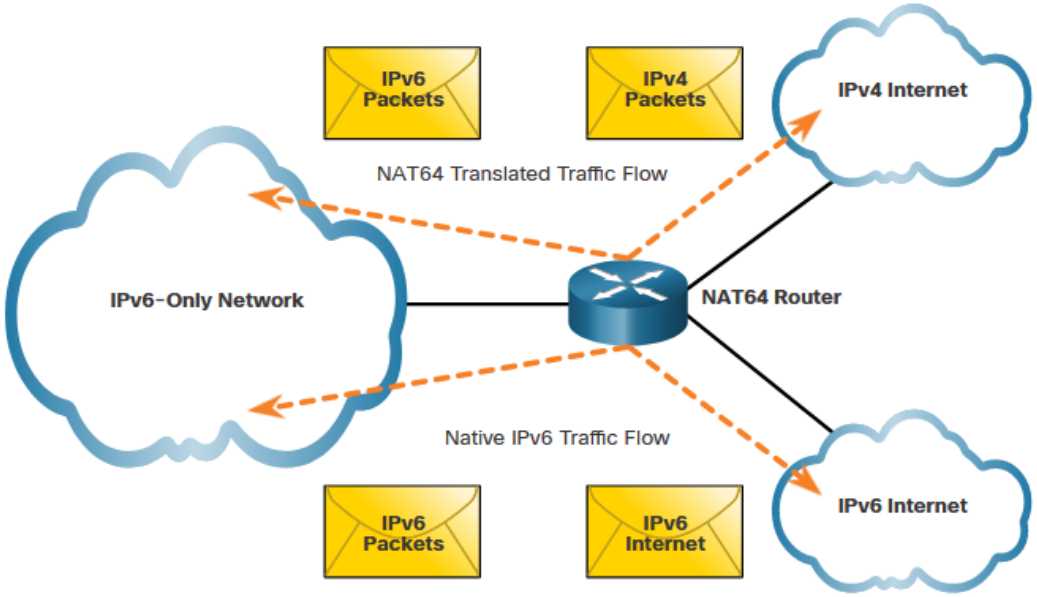
NAT для IPv6?

Протокол IPv6 был разработан, чтобы устранить необходимость в NAT для IPv4 с его преобразованием между публичными и частными IPv4-адресами.

- Однако IPv6 включает собственное частное адресное пространство IPv6, уникальные локальные адреса (ULAs).
- Уникальные локальные IPv6-адреса (unique local addresses, ULA) похожи на частные адреса RFC 1918 в IPv4, но при этом существенно отличаются от них.
- Адреса ULA предназначены только для локальной связи внутри сайта. Адреса ULA не предназначены для предоставления дополнительного адресного пространства IPv6 или обеспечения уровня безопасности.
- IPv6 обеспечивает преобразование протокола между IPv4 и IPv6, известный как NAT64.

NAT64

- NAT для IPv6 используется в совсем другом контексте, нежели NAT для IPv4.
- Разнообразные варианты NAT для IPv6 используются с целью предоставления прозрачного доступа между сетями, в которых используется только протокол IPv6, и сетями, в которых используется только протокол IPv4. NAT для IPv6 не применяется для преобразования частных IPv6-адресов в глобальные IPv6-адреса.
- NAT для IPv6 следует использовать не как долгосрочную стратегию, а лишь как временный механизм, помогающий перейти с IPv4 на IPv6.



Вопросы?

Ставим “+”,
если вопросы есть

Ставим “–”,
если вопросов нет

Заполните, пожалуйста, опрос о занятии

Спасибо за внимание!