Преобразование NAT для IPv4

# Введение 1 Принцип работы NAT

## 1.1 Характеристики NAT

1.1.1 Пространство частных IРv4-адресов

1.1.2 Что такое NAT?

1.1.3 Терминология NAT

1.1.4 Терминология NAT (продолжение)

1.1.5 Принцип работы NAT

1.1.6 Интерактивное задание. Определение терминологии NAT

## 1.2 Типы NAT

1.2.1 Статическое преобразование NAT

1.2.2 Динамическое преобразование NAT

1.2.3 Преобразование адресов портов (РАТ)

1.2.4 Следующий доступный порт

1.2.5 Сравнение NAT и РАТ

1.2.6 Практическая работа NAT-1. Исследование принципа работы NAT

## 1.3 Преимущества преобразования NAT

1.3.1 Преимущества NAT

1.3.2 Недостатки NAT

# 2 Настройка NAT

## 2.1 Настройка статического NAT

2.1.1 Настройка статического NAT

2.1.2 Анализ статического преобразования NAT

2.1.3 Проверка статического NAT

2.1.4 Практическая работа NAT-2.Настройка статического NAT

## 2.2 Настройка динамического NAT

2.2.1 Принцип работы динамического NAT

2.2.2 Настройка динамического NAT

2.2.3 Анализ динамического NAT

2.2.4 Проверка динамического NAT

2.2.5 Практическая работа NAT-3.Настройка динамического NAT

2.2.6 Лабораторная работа NAT-4. Настройка динамического и статического NAT

## 2.3 Настройка РАТ

2.3.1 Настройка РАТ. Пул адресов

2.3.2 Настройка РАТ. Единый адрес

2.3.3 Анализ РАТ 2.3.4 Проверка РАТ

2.3.5 Интерактивное задание. Определение информации об адресе на каждом переходе

2.3.6 Практическая работа NAT-5.Реализация статического и динамического NAT

2.3.7 Лабораторная работа NAT-6. Настройка преобразования адреса и номера порта (РАТ)

## 2.4 Настройка перенаправления портов

### 2.4.1 Перенаправление портов

### 2.4.2 Пример маршрутизатора беспроводной связи

### 2.4.3 Настройка перенаправления портов с помощью IOS

### 2.4.4 Практическая работа NAT-7.Настройка перенаправления портов на маршрутизаторе беспроводной связи

2.5 NAT и IPv6

2.5.1 NAT для IPv6?

2.5.2 Уникальные локальные IРv6-адреса

2.5.3 Протокол NAT для IPv6

# 3 Поиск и устранение неполадок NAT

## 3.1 Команды поиска и устранения неполадок, связанных с NAT

3.1.1 Команды " show ip nat"

3.1.2 Команда " debug ip nat"

3.1.3 Сценарий поиска и устранения неполадок, связанных с NAT

3.1.4 Практическая работа NAT-8.Проверка и отладка настроек NAT

3.1.5 Лабораторная работа NAT-9. Отладка настроек NAT

# 4 Заключение

4.1.1 Проверка NAT

4.1.2 Практическая работа NAT-10.Отработка комплексных практических навыков

# Преобразование NAT для IPv4

# Введение

Все публичные IPv4-адреса, подключаемые к Интернету, должны быть зарегистрированы у регионального регистратора Интернета (RIR). Организации могут арендовать общедоступные адреса у поставщика услуг. Зарегистрированный владелец общедоступного IP-адреса может назначить этот адрес сетевому устройству.

Теоретически максимально допустимое количество IPv4-адресов составляет 4,3 миллиарда, что жестко ограничивает адресное пространство IPv4. Когда в 1981 году Боб Кан (Bob Kahn) и Винт Серф (Vint Cerf) разработали пакет протоколов TCP/IP, включая IPv4, они не имели представления о том, во что превратится Интернет. В то время персональный компьютер был диковинкой для заинтересованных, а до появления интернет-пространства, «Всемирной паутины» (World Wide Web), оставалось еще более десятка лет.

С распространением персональных компьютеров и наступлением эры интернет-пространства стало очевидно, что 4,3 миллиарда IPv4-адресов будет недостаточно. Долгосрочным решением стало появление протокола IPv6, однако наряду с этим потребовались более быстрые способы устранения проблемы исчерпания адресного пространства. Организация IETF разработала ряд краткосрочных решений, в том числе преобразование (NAT) и частные IPv4-адреса в соответствии с RFC 1918. В данной главе описывается, как механизм преобразования NAT в сочетании с использованием диапазона частных адресов применяется для сохранения и более эффективного назначения IPv4-адресов с целью обеспечения доступа к Интернету сетям любых масштабов. Материал данной главы охватывает следующие аспекты:

* характеристики, терминология и общие принципы работы NAT;
* различные типы преобразования, включая статический NAT, динамический NAT и NAT с перегрузкой;
* преимущества и недостатки NAT;
* настройка, проверка и анализ статического NAT, динамического NAT и NAT с перегрузкой;
* использование перенаправления портов для доступа к внутренним устройствам из сети Интернет;
* отладка NAT с помощью команд **show** и **debug**;
* применение NAT для протокола IPv6 с целью преобразования между IPv6- и IPv4-адресами.

# 1 Принцип работы NAT

## 1.1 Характеристики NAT

### 1.1.1 Пространство частных IPv4-адресов

Количества публичных IPv4-адресов недостаточно, чтобы назначить уникальные адреса всем устройствам, подключенным к Интернету. В большинстве случаев сети реализуются с использованием частных IPv4-адресов в соответствии с RFC 1918. На рис. 1 показан диапазон адресов, включенных в RFC 1918. Вероятнее всего, компьютеру, на котором вы сейчас просматриваете материал учебного курса, назначен частный адрес.

Эти частные адреса используются в рамках организации или объекта с целью обеспечения взаимодействия устройств на локальном уровне. Но поскольку эти адреса не определяют конкретную компанию или организацию, частные IPv4-адреса нельзя использовать для маршрутизации через Интернет. 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.

Как показано на рис. 2, NAT обеспечивает преобразование частных адресов в публичные адреса. Это позволяет устройству с частным IPv4-адресом получать доступ к ресурсам вне своей частной сети, включая ресурсы в Интернете. В сочетании с частными IPv4-адресами NAT продемонстрировал свою целесообразность в отношении экономии публичных IPv4-адресов. Один публичный IPv4-адрес может совместно использоваться сотнями, даже тысячами устройств, для каждого из которых настроен уникальный частный IPv4-адрес.

Без использования NAT адресное пространство IPv4 было бы исчерпано задолго до наступления 2000 года. Несмотря на свои преимущества, NAT имеет ряд ограничений, которые будут подробно рассматриваться далее в этой главе. Решением проблемы исчерпания пространства IPv4-адресов и ограничений NAT является окончательный переход на IPv6.





1.1.2 Что такое NAT?

Преобразование NAT используется в различных целях, однако основной задачей данного механизма является экономия публичных IPv4-адресов. Это достигается за счет того, что для внутреннего взаимодействия в сетях используются частные IPv4-адреса, а преобразование в публичные адреса происходит только в случае необходимости.

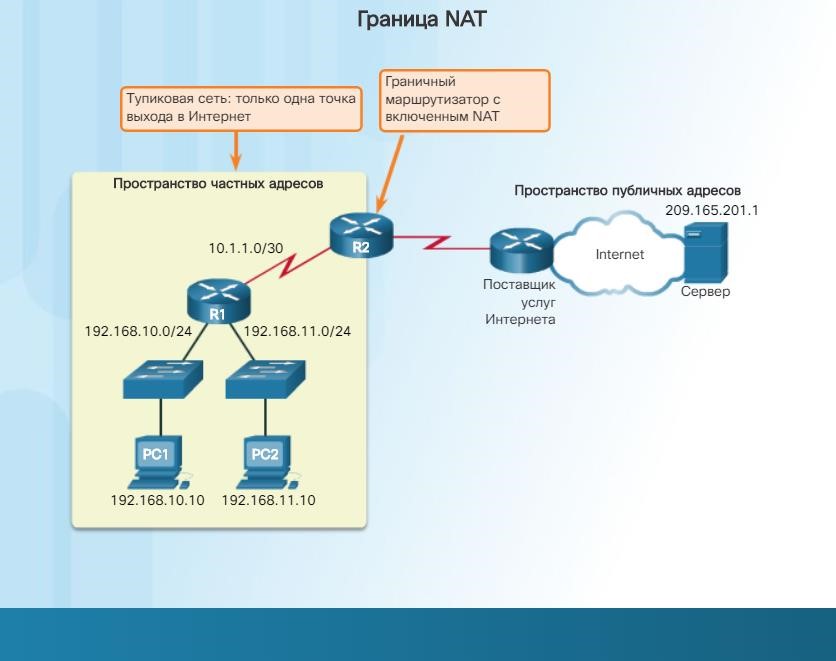
Дополнительное преимущество NAT — повышение степени конфиденциальности и безопасности сети — объясняется тем, что данный механизм скрывает внутренние IPv4-адреса от внешних сетей.

Для маршрутизатора с поддержкой NAT можно настроить один или несколько действующих публичных IPv4-адресов. Эти публичные адреса известны как пул адресов NAT. Если внутреннее устройство отправляет трафик за пределы сети, маршрутизатор с поддержкой NAT преобразует внутренний IPv4-адрес устройства в публичный адрес из пула NAT. Внешним устройствам кажется, что весь трафик, входящий в сеть и выходящий из нее, использует публичные IPv4адреса из предоставленного пула адресов.

Маршрутизатор NAT обычно работает на границе тупиковой сети. Тупиковая сеть — это сеть, у которой есть только одно подключение к соседней сети, и, как следствие, единственный путь наружу и единственный путь до этой сети. В примере, показанном на рисунке, R2 является граничным маршрутизатором. С точки зрения интернет-провайдера, маршрутизатор R2 создает тупиковую сеть.

Когда устройству в тупиковой сети требуется подключение к устройству вне его сети, пакет пересылается граничному маршрутизатору. Граничный маршрутизатор выполняет процесс NAT, преобразуя внутренний частный адрес устройства в публичный, внешний, маршрутизируемый адрес.

**Примечание**. Подключение к сети интернет-провайдера может использовать частный адрес или публичный адрес, совместно используемый клиентами провайдера. В рамках рассматриваемой темы в качестве примера приведен публичный адрес.



### 1.1.3 Терминология NAT

В терминологии NAT под «внутренней сетью» подразумевается набор сетей, чьи адреса будут транслироваться. Термин «внешняя сеть» относится ко всем остальным сетям.

При использовании NAT IPv4-адреса представляют разные точки назначения в зависимости от того, где они находятся: в частной или в публичной сети (Интернет), а также от того, является ли трафик входящим или исходящим.

В NAT предусмотрено 4 типа адресов:

* Внутренний локальный адрес
* Внутренний глобальный адрес
* Внешний локальный адрес
* Внешний глобальный адрес

При определении используемого типа адреса важно помнить, что терминология NAT всегда применяется с точки зрения устройства, адрес которого будет транслироваться:

* **Внутренний адрес** — это адрес устройства, преобразуемый механизмом NAT.
* **Внешний адрес** — это адрес устройства назначения.

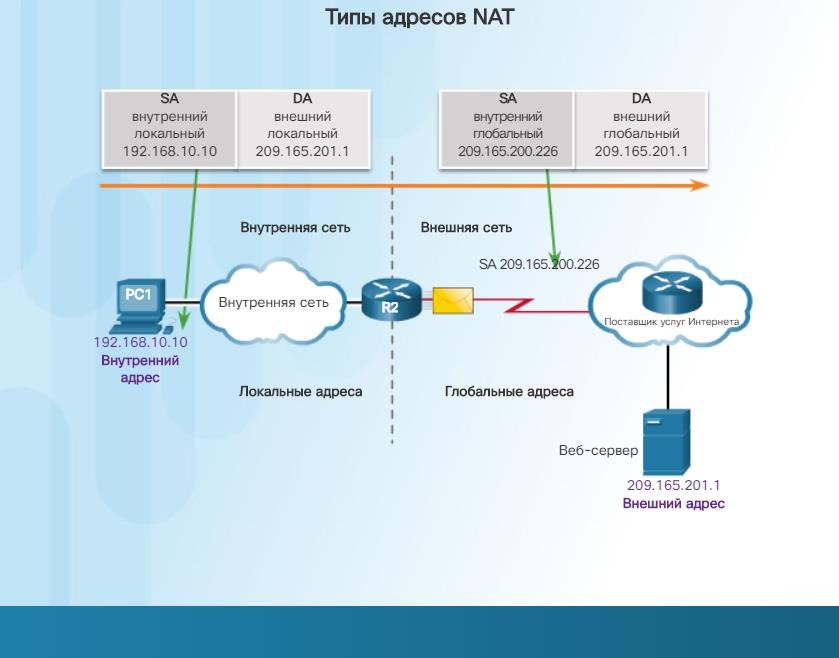
В рамках NAT по отношению к адресам также используется понятие локальности или глобальности:

* **Локальный адрес** — это любой адрес, появляющийся во внутренней части сети.
* **Глобальный адрес** — это любой адрес, появляющийся во внешней части сети.

На рисунке внутренним локальным адресом ПК 1 является 192.168.10.10. С точки зрения ПК 1 веб-сервер использует внешний адрес 20165.201.1. Если пакеты отправляются от ПК 1 на глобальный адрес веб-сервера, внутренний локальный адрес ПК 1 преобразуется в 20165.200.226 (внутренний глобальный адрес). Адрес внешнего устройства обычно не преобразуется, так как этот адрес обычно уже является публичным IPv4-адресом.

Обратите внимание, что для ПК 1 используются разные локальный и глобальный адреса, а для веб-сервера в обоих случаях используется один публичный IPv4-адрес. С точки зрения веб-сервера трафик, исходящий от ПК 1, представляется поступающим с внутреннего глобального адреса 20165.200.226.

Маршрутизатор NAT (R2 на рисунке) представляет собой точку разграничения между внутренней и внешней сетями, а также между локальными и глобальными адресами.



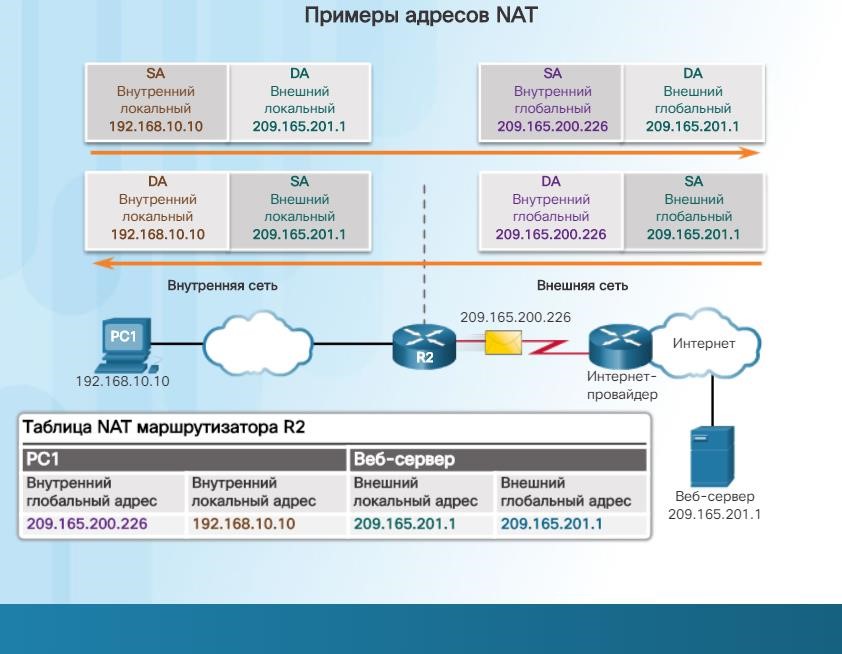
### 1.1.4 Терминология NAT (продолжение)

Термины «внутренний» и «внешний» используются в сочетании с терминами «локальный» и «глобальный», когда речь идет о конкретных адресах. На рисунке маршрутизатор R2 настроен на использование механизма NAT. Он использует пул публичных адресов, назначаемых внутренним узлам.

* **Внутренний локальный адрес** — это адрес источника, видимый из внутренней сети. На рисунке ПК 1 назначен IPv4-адрес 192.168.10.10. Это внутренний локальный адрес ПК 1.
* **Внутренний глобальный адрес** — это адрес источника, видимый из внешней сети. На рисунке, если ПК 1 отправляет трафик веб-серверу с адресом 20165.201.1, R2 преобразует внутренний локальный адрес во внутренний глобальный адрес. В этом случае R2 меняет IPv4-адрес источника с 192.168.10.10 на 20165.200.226. В терминологии NAT внутренний локальный адрес 192.168.10.10 преобразуется во внутренний глобальный адрес 20165.200.226.
* **Внешний глобальный адрес** — это адрес назначения, видимый из внешней сети. Это глобально маршрутизируемый IPv4-адрес, назначенный узлу в Интернете. Например, веб-сервер доступен по IPv4-адресу 20165.201.1. В большинстве случаев внешний локальный и внешний глобальный адреса совпадают.
* **Внешний локальный адрес** — это адрес назначения, видимый из внутренней сети. В этом примере ПК 1 отправляет трафик веб-серверу с IPv4-адресом 20165.201.1. В редких случаях этот адрес может отличаться от глобально маршрутизируемого адреса назначения.

На рисунке показано, как адресуется трафик, отправленный внутренним компьютером внешнему веб-серверу через маршрутизатор с поддержкой NAT. Также показано, как первоначально адресуется и преобразуется обратный трафик.

**Примечание**. Использование внешнего локального адреса не рассматривается в материале настоящего учебного курса.



### 1.1.5 Принцип работы NAT

В этом примере компьютеру ПК 1 с частным адресом 192.168.10.10 нужно связаться с внешним веб-сервером с публичным адресом 20165.201.1.

Для просмотра анимации нажмите кнопку «Воспроизведение».

ПК 1 отправляет пакет, адресованный веб-серверу. Пакет пересылается маршрутизатором R1 маршрутизатору R2.

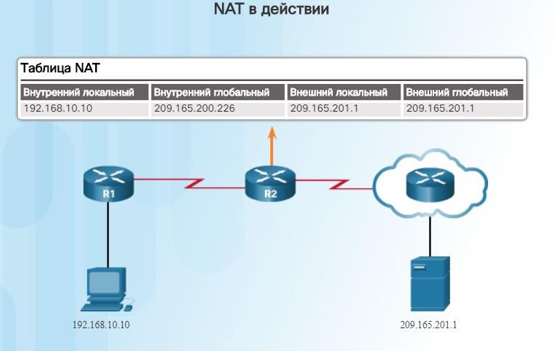
Получив пакет, маршрутизатор R2, поддерживающий выполнение NAT для данной сети, считывает IPv4-адрес источника пакета, чтобы определить, соответствует ли пакет критериям, определенным для преобразования.

В данном случае IPv4-адрес источника соответствует критериям и преобразуется из 192.168.10.10 (внутренний локальный адрес) в 20165.200.226 (внутренний глобальный адрес). Маршрутизатор R2 добавляет это сопоставление локального и глобального адресов в таблицу NAT.

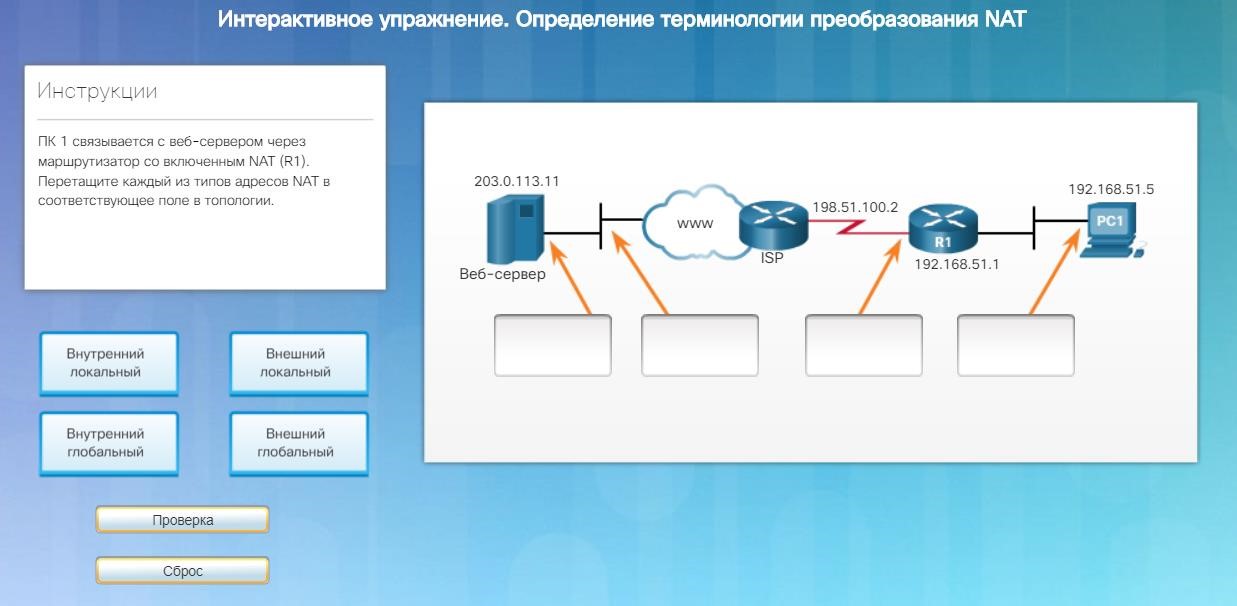
R2 отправляет по назначению пакет с преобразованным адресом источника.

Веб-сервер отвечает пакетом, адресованным внутреннему глобальному адресу ПК 1 (20165.200.226).

R2 получает пакет с адресом назначения 20165.200.226. R2 проверяет таблицу NAT и находит запись для этого сопоставления. R2 использует эту информацию и преобразует внутренний глобальный адрес (20165.200.226) во внутренний локальный адрес (192.168.10.10), после чего пакет пересылается PC1.

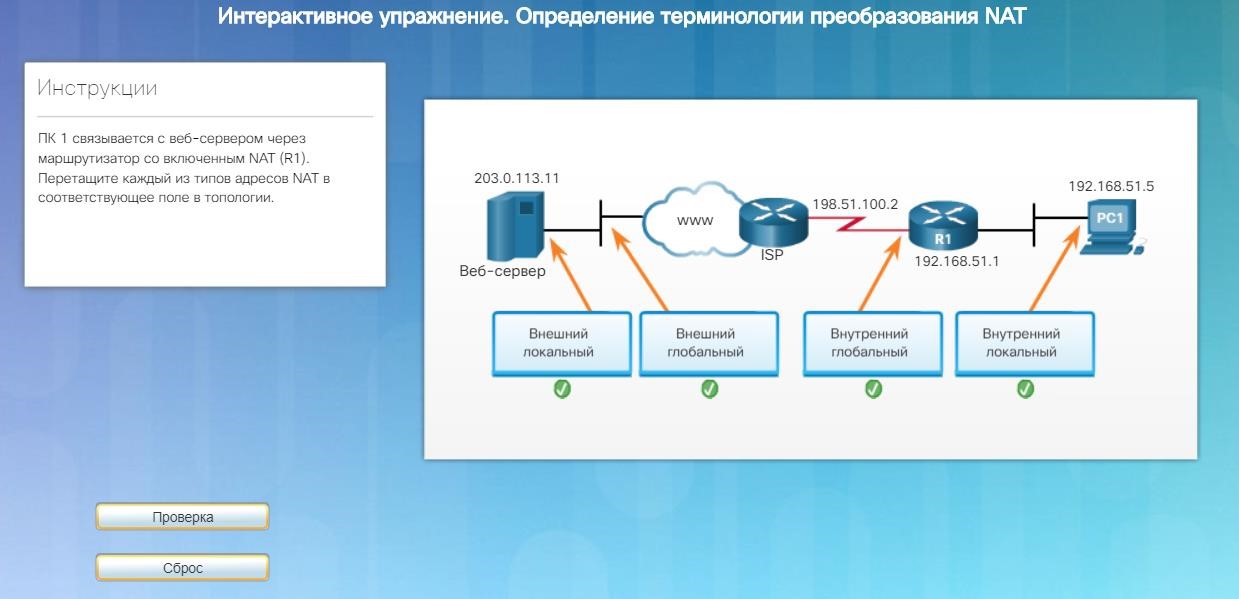


### 1.1.6 Интерактивное задание. Определение терминологии NAT



Проверьте себя!

Ответ:



## 1.2 Типы NAT

### 1.2.1 Статическое преобразование NAT

Существуют три механизма преобразования:

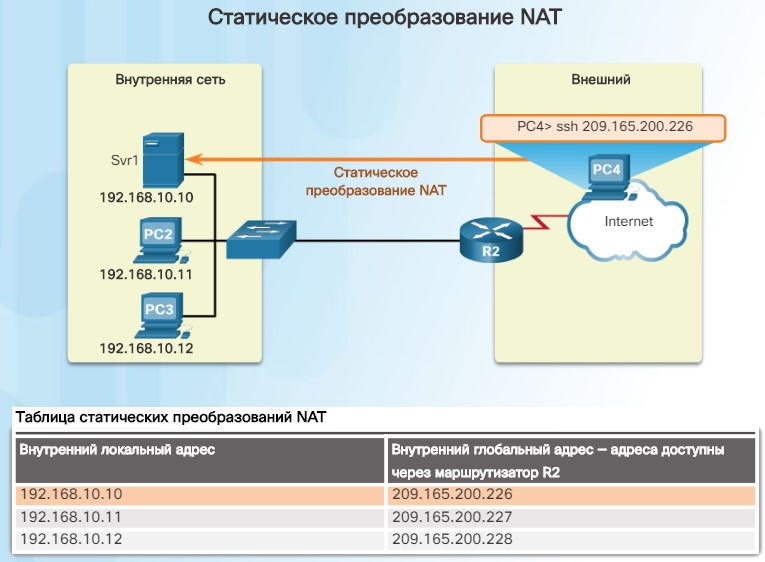
* **Статическое преобразование (статический NAT)** — это взаимно-однозначное соответствие между локальным и глобальным адресами.
* **Динамическое преобразование (динамический NAT)** — это сопоставление адресов по схеме «многие ко многим» между локальными и глобальными адресами. Преобразования выполняются по наличию. Например, если имеется 100 внутренних локальных адресов и 10 внутренних глобальных адресов, в любой момент времени могут быть преобразованы только 10 из 100 внутренних локальных адресов. Из-за такого ограничения динамическое преобразование NAT подходит для производственных сетей гораздо меньше, чем преобразование адресов портов.
* **Преобразование адреса и номера порта (PAT)** — это сопоставление адресов по схеме «многие к одному» между локальными и глобальным адресами. Данный метод также называется перегрузкой (NAT с перегрузкой). Например, если имеется 100 внутренних локальных адресов и 10 внутренних глобальных адресов, PAT использует порты в качестве дополнительного параметра для создания эффекта умножения сложности. Это позволяет повторно использовать любой из 10 внутренних глобальных адресов до 65 536 раз (в зависимости от процесса: UDP, TCP или ICMP).

#### Статическое преобразование NAT

Статический NAT использует сопоставление локальных и глобальных адресов по схеме «один в один». Эти соответствия задаются администратором сети и остаются неизменными.

На рисунке для маршрутизатора R2 настроены статические соответствия для внутренних локальных адресов Сервера 1, ПК 2 и ПК 3. Когда эти устройства отправляют трафик в Интернет, их внутренние локальные адреса преобразуются в заданные внутренние глобальные адреса. Для внешних сетей эти устройства используют публичные IPv4-адреса.

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. Например, сетевой администратор может с ПК 4 подключиться с помощью SSH к внутреннему глобальному адресу Svr1 (20165.200.226). Маршрутизатор R2 преобразует этот внутренний глобальный адрес во внутренний локальный адрес и подключает сеанс администратора к Svr1. Для статического NAT требуется достаточное количество публичных адресов, доступных для общего количества одновременных сеансов пользователей.

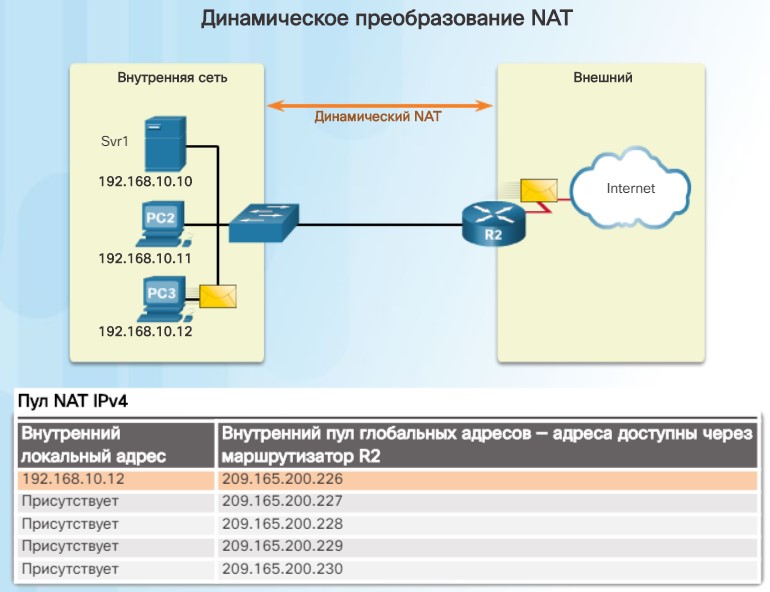


### 1.2.2 Динамическое преобразование NAT

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.

На рисунке ПК 3 получает доступ к Интернету, используя первый доступный адрес в пуле динамического NAT. Другие адреса по-прежнему доступны для использования. Как и для статического NAT, для динамического NAT требуется достаточное количество публичных адресов, способное обеспечить общее количество одновременных сеансов пользователей.



### 1.2.3 Преобразование адресов портов (РАТ)

Преобразование адреса и номера порта (PAT), также называемое NAT с перегрузкой, сопоставляет множество частных IPv4-адресов одному или нескольким публичным IPv4-адресам. Так работает большинство домашних маршрутизаторов. Интернет-провайдер назначает один адрес маршрутизатору, при этом еще несколько домашних устройств могут одновременно получать доступ к Интернету. NAT с перегрузкой — это наиболее распространенный метод преобразования.

С помощью данного метода множество адресов могут быть сопоставлены одному или нескольким адресам, поскольку каждый частный адрес также отслеживается по номеру порта. Когда устройство запускает сеанс TCP/IP, создается значение исходного порта TCP или UDP либо специально назначенный идентификатор запроса для ICMP для определения этого сеанса уникальным образом. Если маршрутизатор NAT получает пакет от клиента, он использует свой номер порта источника, чтобы уникальным образом определить конкретное преобразование NAT.

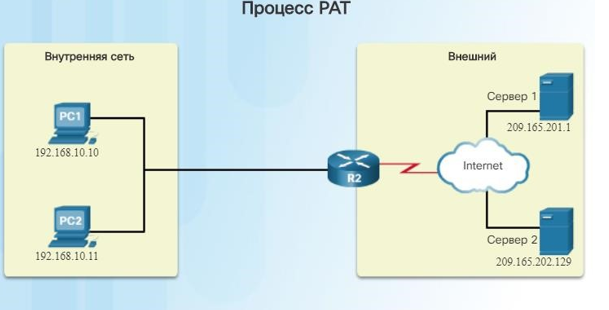
PAT гарантирует, что устройства будут использовать разные номера портов TCP для каждого сеанса взаимодействия с сервером в Интернете. При возвращении ответа от сервера номер порта источника, который становится номером порта назначения при обратной передаче, определяет, какому устройству маршрутизатор перешлет соответствующие пакеты. Процесс PAT также проверяет, были ли запрошены входящие пакеты, таким образом повышая степень безопасности сеанса.

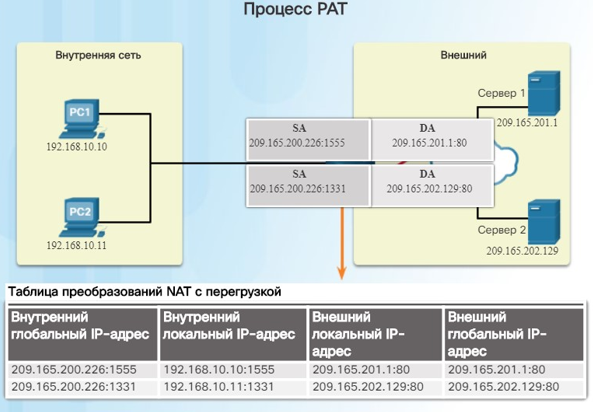
Для управления анимацией используйте кнопки «Воспроизведение» и «Пауза» на рисунке.

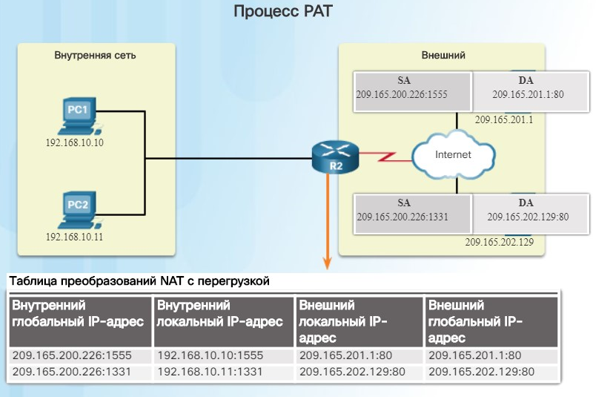
Анимация иллюстрирует процесс преобразования адресов портов (PAT). Чтобы различать преобразования, механизм PAT добавляет уникальные номера портов источника к внутреннему глобальному адресу.

Поскольку маршрутизатор R2 обрабатывает каждый пакет, он использует номер порта (в рассматриваемом примере 1331 и 1555) для идентификации устройства, с которого поступил пакет. Адрес источника (SA) — это внутренний локальный адрес с добавленным назначенным номером порта TCP/IP. Адрес назначения (DA) — это внешний локальный адрес с добавленным номером порта требуемой службы. В данном примере порт службы равен 80, т. е. порту для протокола HTTP.

Для адреса источника маршрутизатор R2 преобразует внутренний локальный адрес во внутренний глобальный адрес с добавленным номером порта. Адрес назначения не меняется, но теперь он считается внешним глобальным IPv4адресом. Когда веб-сервер отвечает, путь повторяется, только в обратном порядке.







### 1.2.4 Следующий доступный порт

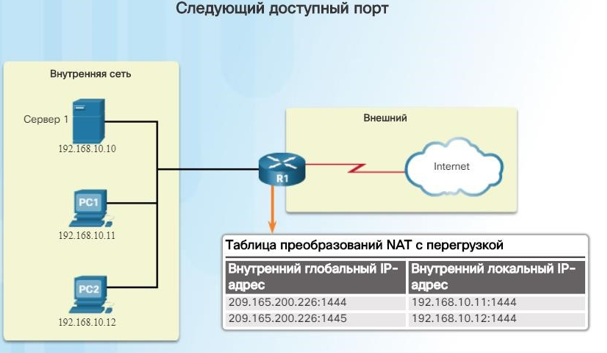
В предыдущем примере номера портов клиента, 1331 и 1555, не изменялись на маршрутизаторе с поддержкой NAT. Данная ситуация не очень вероятна, поскольку велика вероятность того, что эти номера портов уже используются для других активных сеансов.

Преобразование PAT пытается сохранить оригинальный порт источника. В том случае, если первоначальный порт источника уже используется, PAT назначает первый доступный номер порта, начиная с наименьшего в соответствующей группе портов — 0-511, 512-1023 или 1024-65535. 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.

Для ознакомления с принципом работы PAT нажмите кнопку «Воспроизведение» на рисунке. В рассматриваемом примере в процессе преобразования PAT второму адресу узла назначается следующий доступный порт (1445).

В анимации узлы выбирают один и тот же номер порта — 1444. Это допустимо для внутреннего адреса, поскольку хостам назначаются уникальные частные IPv4-адреса. Но на маршрутизаторе с поддержкой NAT номера портов необходимо изменить. В противном случае пакеты от двух различных узлов выходили бы из R2 с одинаковым адресом источника. В данном примере предположим, что первые 420 портов в диапазоне 1024–65 535 уже используются. То есть следующий доступный номер порта — 1445.





### 1.2.5 Сравнение NAT и РАТ

Сформулированные ниже различия между NAT и PAT помогут понять особенности каждого из этих методов преобразования.

Как показано на рисунке, NAT преобразует IPv4-адреса, исходя из схемы 1:1 для частных IPv4-адресов и публичных IPv4адресов. В то же время PAT меняет и адрес, и номер порта.

NAT пересылает входящие пакеты получателю, используя входящий IPv4-адрес источника, предоставленный узлом в публичной сети. При использовании PAT обычно задействуется только один или небольшое количество публично представленных IPv4-адресов. Входящие пакеты из публичной сети направляются адресатам в частной сети с помощью таблицы на маршрутизаторе с NAT. Данная таблица отслеживает пары публичных и частных портов. Это называется отслеживанием соединений.

#### Пакеты без сегмента 4 уровня

Что же происходит с пакетами IPv4, передающими данные, не являющиеся сегментом TCP или UDP? Данные пакеты не содержат номера порта уровня 4. PAT преобразует большинство основных протоколов, передаваемых с помощью IPv4 и не использующих TCP или UDP в качестве протокола транспортного уровня. Самым распространенным среди таких протоколов является протокол ICMPv4. Процесс преобразования PAT обрабатывает каждый из этих протоколов поразному. 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. Идентификатор запроса увеличивается с каждым отправленным эхо-запросом. PAT использует идентификатор запроса вместо номера порта уровня 4.

**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.



### 1.2.6 Packet Tracer. Исследование принципа работы NAT

Известно, что при передаче кадра по сети MAC-адреса изменяются. В то же время, при пересылке пакета устройством, поддерживающим NAT, IPv4-адреса также могут меняться. Во время выполнения этого задания мы увидим, что происходит с IPv4-адресами в процессе преобразования NAT.

[Практическая работа NAT-1. Изучение работы NAT. Инструкции](files/Практическая%20работа%20NAT-1_Изучение%20работы%20NAT.docx)

[Packet Tracer NAT-1. Изучение работы NAT.PKA](files/Практическая%20работа%20NAT-1_Изучение%20работы%20NAT.pka)

## 1.3 Преимущества преобразования NAT

### 1.3.1 Преимущества NAT

NAT обеспечивает множество преимуществ, в том числе следующие:

* NAT сохраняет официально зарегистрированную схему адресации, разрешая частное использование внутренних сетей. NAT экономит адреса благодаря мультиплексированию приложений на уровне портов. При использовании NAT с перегрузкой внутренние узлы могут использовать для всех внешних взаимодействий один публичный IPv4адрес. При этом типе настройки для поддержки множества внутренних узлов требуется очень небольшое количество внешних адресов.
* NAT повышает гибкость подключений к публичной сети. Для обеспечения надежных подключений к публичной сети можно создать множественные пулы, резервные пулы и пулы распределения нагрузки.
* NAT обеспечивает постоянство схем внутренней сетевой адресации. Если в сети не используются частные IPv4адреса и NAT, изменение схемы публичных IPv4-адресов потребует изменения адресов всех узлов существующей сети. Затраты на изменение адресации узлов могут оказаться существенными. NAT позволяет сохранить существующую схему частных IPv4-адресов, одновременно поддерживая простой переход на новую схему публичной адресации. Это означает, что организация может сменить интернет-провайдера, не меняя настроек своих внутренних клиентов.
* NAT скрывает IPv4-адреса конечного пользователя. Благодаря использованию IPv4-адресов в соответствии с RFC 1918, побочным эффектом преобразования NAT является скрытие IPv4-адресов пользователей и других устройств.

Некоторые считают это функцией безопасности, однако большинство экспертов утверждают, что преобразование NAT не обеспечивает безопасность. Межсетевой экран с контролем состояния подключений — вот что обеспечивает безопасность на границе сети.



### 1.3.2 Недостатки NAT

Преобразование сетевых адресов (NAT) имеет ряд недостатков. Тот факт, что узлы в Интернете взаимодействуют непосредственно с устройством, поддерживающим NAT, а не с фактическим узлом частной сети, создает ряд проблем. Один из недостатков использования NAT связан с производительностью сети, особенно это касается протоколов реального времени, таких как VoIP. NAT увеличивает задержки пересылки, поскольку преобразование каждого IPv4адреса в заголовках пакетов требует времени. Коммутация первого пакета диалога всегда является программным процессом; этот пакет всегда проходит более медленным путем. Маршрутизатор должен анализировать каждый пакет, чтобы решить, требуется ли его преобразование. Маршрутизатор должен изменить заголовок IPv4 и, возможно, изменить заголовок TCP или UDP. При каждом преобразовании должна быть пересчитана контрольная сумма заголовка IPv4, а также контрольная сумма TCP или UDP. Если в кэше есть соответствующая запись, остальные пакеты проходят по пути для быстрой коммутации. В противном случае они тоже задерживаются.

Другим недостатком использования NAT является потеря сквозной адресации. Многие интернет-протоколы и приложения зависят от сквозной адресации от источника до узла назначения. Некоторые приложения не совместимы с NAT. Например, некоторые приложения безопасности, такие как цифровые подписи, не работают с NAT, поскольку IPv4-адрес источника изменяется по пути к узлу назначения. Приложения, использующие физические адреса вместо доменных имен, не могут достигнуть узлов назначения при прохождении через маршрутизатор с NAT. В некоторых случаях этой проблемы можно избежать с помощью статических сопоставлений NAT.

Кроме того, утрачивается возможность сквозной трассировки IPv4. Очень сильно усложняется трассировка пакетов, подвергающихся многочисленным изменениям адреса пакета при прохождении нескольких участков NAT, что, в свою очередь, затрудняет устранение неполадок.

Использование NAT также усложняет работу с туннельными протоколами, такими как IPsec, поскольку преобразование NAT изменяет значения в заголовках, что приводит к сбою проверки целостности.

Работа служб, требующих инициализации подключений TCP из внешней сети или использующих протоколы без учета состояния, например, на основе UDP, может быть нарушена. Если на маршрутизаторе NAT не настроена поддержка таких протоколов, входящие пакеты не смогут достичь своего назначения. Некоторые протоколы могут поддерживать один экземпляр NAT между узлами-участниками (например, FTP в пассивном режиме), но не работают, если обе системы отделены от Интернета посредством NAT.



# 2 Настройка NAT

## 2.1 Настройка статического NAT

### 2.1.1 Настройка статического 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.

На рис. 1 показана внутренняя сеть, имеющая веб-сервер с частным IPv4-адресом. На маршрутизаторе R2 настроен статический NAT, чтобы предоставить доступ к веб-серверу устройствам из внешней сети (Интернет). Клиент из внешней сети обращается к веб-серверу, используя публичный IPv4-адрес. Статический NAT преобразует публичный IPv4-адрес в частный IPv4-адрес.

Настройка статического NAT сопряжена с двумя основными задачами.

**Шаг 1.** Первой задачей является создание соответствия между внутренним локальным и внутренним глобальным адресами. Например, на рис. 1 в качестве статического преобразования NAT настроены внутренний локальный адрес 192.168.10.254 и внутренний глобальный адрес 20165.201.5.

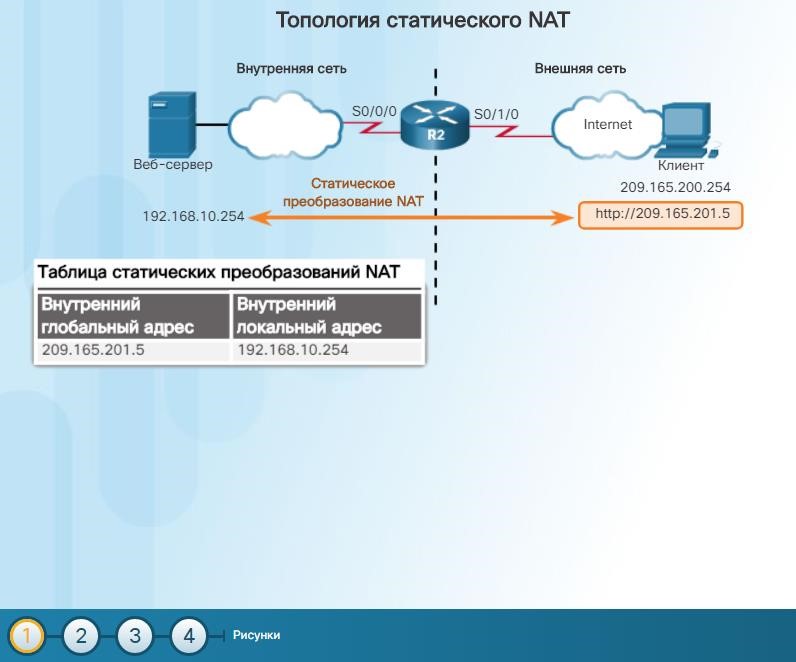
**Шаг 2.** После настройки соответствия интерфейсы, участвующие в преобразовании, настраиваются как внутренние или внешние относительно NAT. В этом примере интерфейс Serial 0/0/0 маршрутизатора R2 является внутренним, а Serial 0/1/0 — внешним интерфейсом.

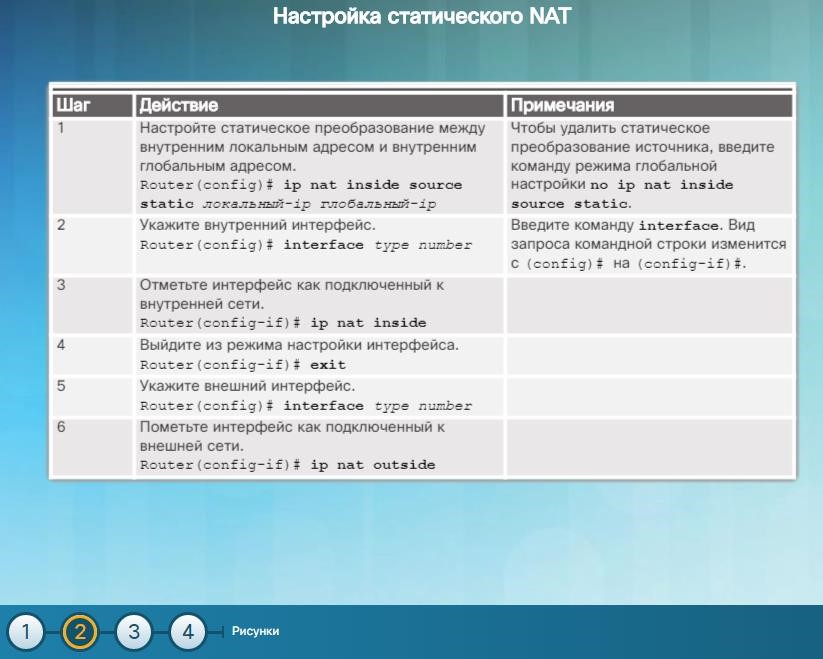
Пакеты, поступающие на внутренний интерфейс маршрутизатора R2 (Serial 0/0/0) от настроенного внутреннего локального IPv4-адреса (192.168.10.254), преобразуются, а затем передаются во внешнюю сеть. Пакеты, поступающие на внешний интерфейс маршрутизатора R2 (Serial 0/1/0), адресованные настроенному внутреннему глобальному IPv4адресу (20165.201.5), преобразуются для передачи внутреннему локальному адресу (192.168.10.254) и затем передаются во внутреннюю сеть.

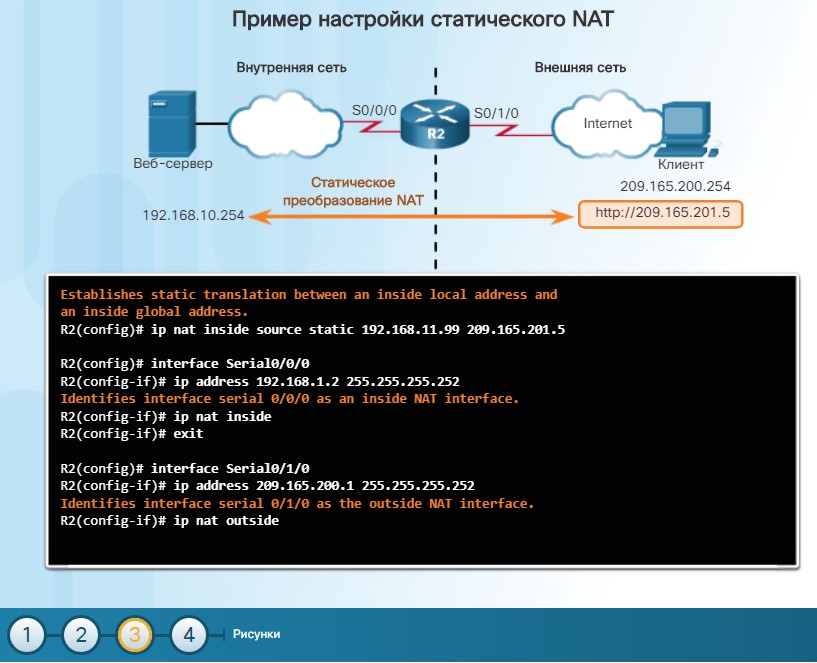
На рис. 2 приведены команды, необходимые для настройки статического NAT.

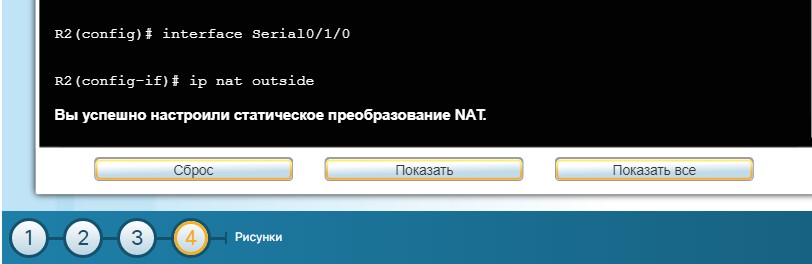
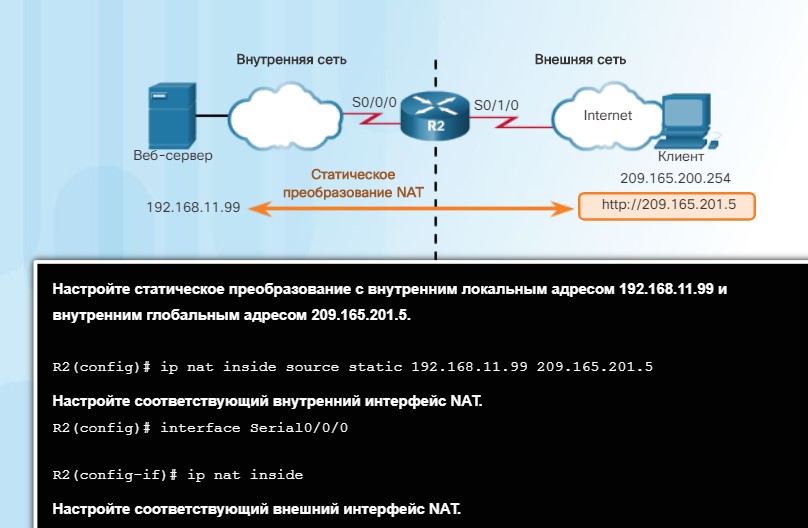
На рис. 3 показаны команды, необходимые для создания на маршрутизаторе R2 статического сопоставления NAT для веб-сервера в примере топологии. В рамках показанной настройки R2 преобразует в пакетах, отправленных вебсервером, адрес 192.168.10.254 в публичный IPv4-адрес 20165.201.5. Клиент из Интернета направляет веб-запросы на публичный IPv4-адрес 20165.201.5. Маршрутизатор R2 пересылает этот трафик веб-серверу по адресу 192.168.10.254.

Используйте средство проверки синтаксиса (см. рис. 4) для настройки дополнительной записи статического преобразования NAT на маршрутизаторе R2.









### 2.1.2 Анализ статического преобразования NAT

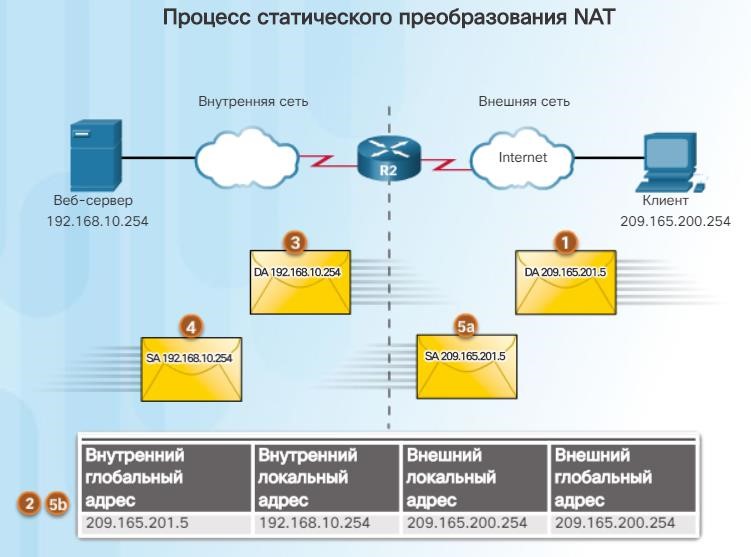
На этом рисунке показан процесс статического преобразования NAT между клиентом и веб-сервером с использованием предыдущей настройки. Статические преобразования обычно используются, когда клиентам из внешней сети (Интернет) нужно обратиться к серверам внутренней сети.

1. Клиенту нужно подключиться к веб-серверу. Клиент отправляет пакет на веб-сервер, используя публичный IPv4-адрес назначения 20165.201.5. Это внутренний глобальный адрес веб-сервера.
2. Первый пакет, полученный маршрутизатором R2 от клиента на внешнем интерфейсе NAT, заставляет R2 проверить свою таблицу NAT. IPv4-адрес назначения находится в таблице NAT, и маршрутизатор выполняет соответствующее преобразование.
3. R2 заменяет внутренний глобальный адрес 20165.201.5 внутренним локальным адресом 192.168.10.254. Затем R2 пересылает пакет веб-серверу.
4. Веб-сервер получает пакет и отвечает клиенту, используя внутренний локальный адрес 192.168.10.254.

5a. R2 получает пакет от веб-сервера на свой внутренний интерфейс NAT с адресом источника, соответствующим внутреннему локальному адресу веб-сервера, 192.168.10.254.

5b. R2 проверяет таблицу NAT на предмет наличия преобразования для внутреннего локального адреса. Этот адрес присутствует в таблице NAT. R2 выполняет преобразование адреса источника во внутренний глобальный адрес 20165.201.5 и пересылает пакет клиенту.

6. Клиент получает пакет и продолжает диалог. Маршрутизатор NAT выполняет шаги 2-5b для каждого пакета (шаг 6 на рисунке не показан).



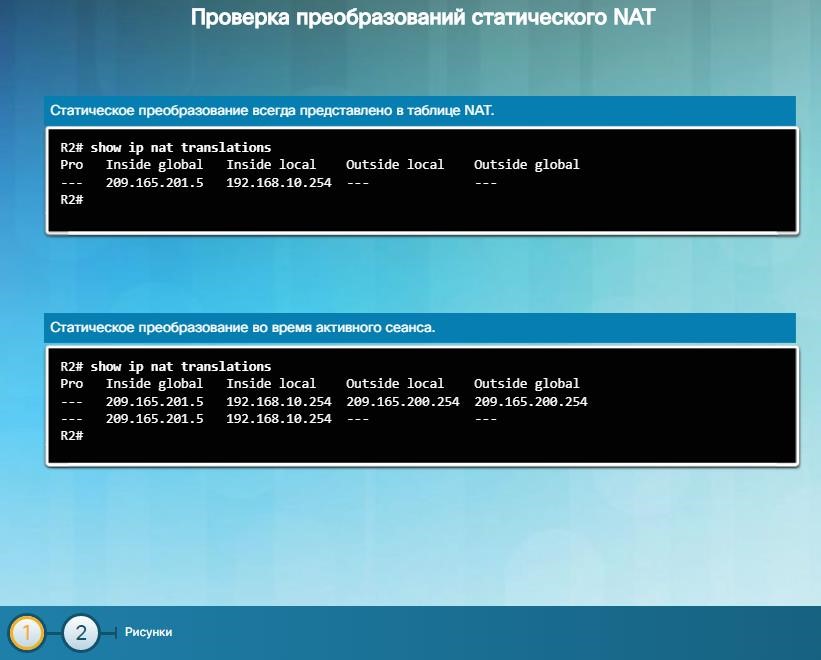
### 2.1.3 Проверка статического NAT

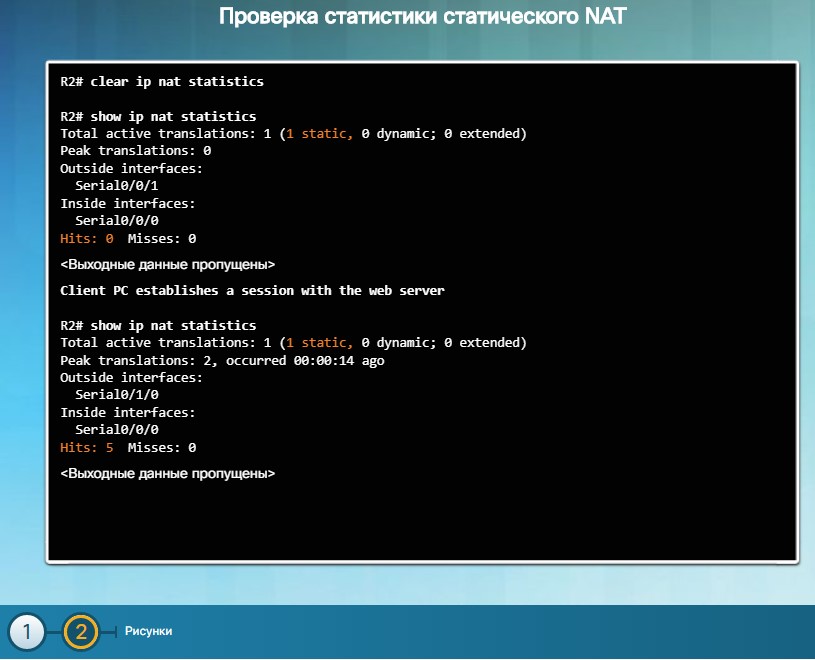
Для проверки работы NAT используется команда **show ip nat translations**. Эта команда отображает активные преобразования NAT. В отличие от динамических преобразований, статические преобразования всегда присутствуют в таблице NAT. На рис. 1 показан результат этой команды для предыдущего примера настройки. 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, как показано на рис. 1.

Другой полезной командой является **show ip nat statistics**. Как показано на рис. 2, команда **show ip nat statistics** 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**.

До начала взаимодействия с веб-сервером команда **show ip nat statistics** не должна показывать каких-либо совпадений. После установки клиентом сеанса связи с веб-сервером в выходных данных команды **show ip nat statistics** количество совпадений во внутреннем интерфейсе увеличивается до 5 (Serial0/0/0). Этим подтверждается выполнение статического преобразования NAT на R2.





### 2.1.4 Packet Tracer. Настройка статического NAT

В сетях, настроенных по протоколу IPv4, для клиентов и серверов используется частная адресация. Перед выходом из сети в Интернет пакеты с частной адресацией должны быть преобразованы в пакеты с публичной адресацией. Серверам, доступным за пределами сети компании, обычно назначают как общедоступные, так и частные статические IP-адреса. В рамках задания необходимо настроить статический NAT таким образом, чтобы внешние устройства могли получать доступ к внутреннему серверу по публичному адресу.

[Практическая работа NAT-2. Настройка статического NAT. Инструкции](files/Практическая%20работа%20NAT-2_Настройка%20статического%20NAT.docx)

[Packet Tracer NAT-2. Настройка статического NAT. PKA](files/Практическая%20работа%20NAT-2_Настройка%20статического%20NAT.pka)

## 2.2 Настройка динамического NAT

### 2.2.1 Принцип работы динамического NAT

В то время как статическое преобразование NAT обеспечивает постоянное соответствие между внутренним локальным адресом и внутренним глобальным адресом, динамическое преобразование NAT поддерживает автоматическое сопоставление внутренних локальных адресов внутренним глобальным адресам. Эти внутренние глобальные адреса обычно являются публичными IPv4-адресами. В динамическом NAT для преобразования используется группа или пул публичных IPv4-адресов.

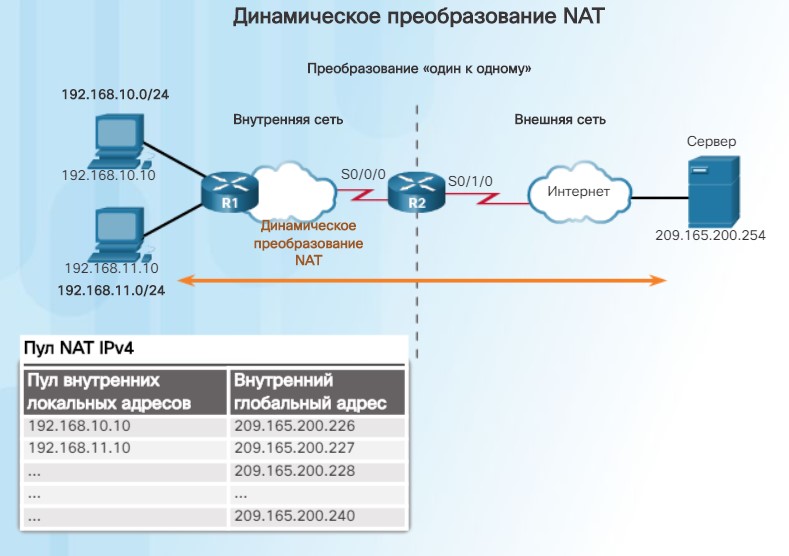
Для динамического NAT, как и для статического NAT, требуется настройка внутреннего и внешнего интерфейсов, участвующих в преобразовании NAT. Однако если статическое преобразование NAT создает постоянное сопоставление с одним адресом, для динамического NAT используется пул адресов.

**Примечание**. Преобразование между публичными и частными IPv4-адресами является самым распространенным применением NAT. Тем не менее, преобразования NAT могут возникать между любыми парами адресов.

В примере топологии, показанном на рисунке, внутренняя сеть использует адреса из пространства частных адресов, определенного в RFC 1918. К маршрутизатору R1 подключены две локальных сети — 192.168.10.0/24 и 192.168.11.0/24.

Граничный маршрутизатор R2 настроен на динамическое преобразование NAT с использованием пула публичных IPv4адресов от 20165.200.226 до 20165.200.240.

Пул публичных IPv4-адресов (внутренний пул глобальных адресов) доступен любому устройству во внутренней сети по принципу очереди («первым пришел — первым обслужили»). При динамическом преобразовании NAT один внутренний адрес преобразуется в один внешний адрес. Для этого типа преобразования в пуле должно быть достаточно адресов, чтобы охватить все внутренние устройства, которым одновременно требуется доступ к внешней сети. Если использованы все адреса пула, устройство должно дождаться доступного адреса, чтобы получить доступ к внешней сети.



### 2.2.2 Настройка динамического NAT

На рис. 1 показаны шаги и команды, используемые для настройки динамического NAT. **Шаг 1.** С помощью команды **ip nat pool** определите пул адресов, которые будут использоваться для преобразования. Данный пул адресов обычно является группой публичных адресов. Эти адреса определяются с помощью указания начального и конечного IPv4-адресов пула. Ключевое слово **netmask** или **prefix-length** указывает, какие биты адреса относятся к сети, а какие — к диапазону адресов узлов.

**Шаг 2.** Настройте стандартный ACL, чтобы определить (разрешить) только те адреса, которые должны быть преобразованы. Список контроля доступа со слишком большим количеством разрешающих инструкций может привести к непредсказуемым результатам. Помните, что в конце каждого ACL подразумевается строка **deny all**.

**Шаг 3.** Выполните привязку ACL к пулу. Команда **ip nat inside source list** *номер списка доступа* **pool** *имя*

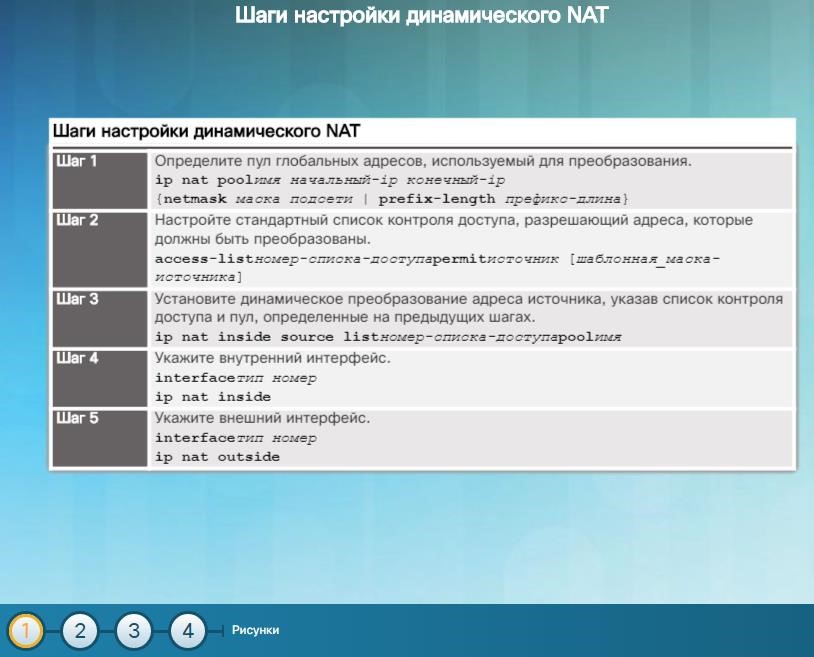
*пула* используется для привязки списка контроля доступа к пулу. Эта настройка используется маршрутизатором, чтобы определить, какие устройства (**list**) получают какие адреса (**pool**).

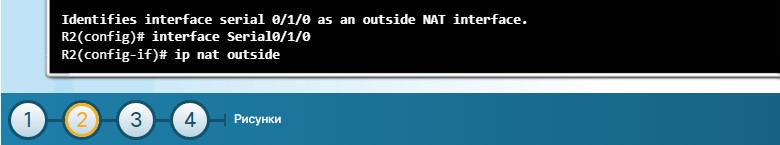
**Шаг 4.** Определите интерфейсы, являющиеся внутренними по отношению к NAT, т. е. все интерфейсы, подключенные к внутренней сети.

**Шаг 5.** Определите интерфейсы, являющиеся внешними относительно NAT; это все интерфейсы, подключенные к внешней сети.

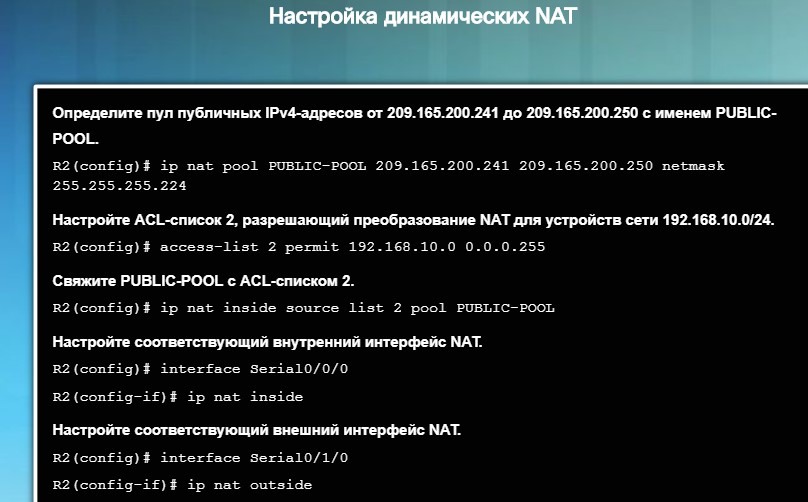
На рис. 2 приведен пример топологии и соответствующая настройка. Данная настройка разрешает преобразование для всех узлов сети 192.168.0.0/16, содержащей локальные сети 192.168.10.0 и 192.168.11.0, когда узлы создают трафик, входящий в S0/0/0 и выходящий из S0/1/0. Адреса этих узлов преобразуются в доступный адрес из пула в диапазоне от 20165.200.226 до 20165.200.240.

На рис. 3 показана топология, используемая для настройки в инструменте проверки синтаксиса. Используйте средство проверки синтаксиса на рис. 4, чтобы настроить динамическое преобразование NAT на маршрутизаторе R2.









### 2.2.3 Анализ динамического NAT

На приведенных рисунках показан процесс динамического преобразования NAT между двумя клиентами и веб-сервером с использованием предыдущей настройки.

На рис. 1 показан поток трафика изнутри наружу.

1. Узлы с IPv4-адресами источника (192.168.10.10 (PC1) и 192.168.11.10 (PC2)) отправляют пакеты, запрашивающие подключение к серверу на публичный IPv4-адрес (20165.200.254).
2. Маршрутизатор R2 получает первый пакет от узла 192.168.10.10. Поскольку этот пакет был получен на интерфейс, настроенный как внутренний интерфейс NAT, R2 проверяет конфигурацию NAT, чтобы определить, следует ли выполнять преобразование для данного пакета. ACL разрешает этот пакет, поэтому R2 выполняет его преобразование. Маршрутизатор R2 проверяет свою таблицу NAT. Поскольку для данного IPv4-адреса нет записей преобразования, R2 решает, что для адреса источника 192.168.10.10 требуется динамическое преобразование. Маршрутизатор R2 выбирает доступный глобальный адрес из динамического пула адресов и создает запись преобразования — 20165.200.226. Первоначальный IPv4-адрес источника (192.168.10.10) — это внутренний локальный адрес, а используемый для преобразования адрес — это внутренний глобальный адрес (20165.200.226) в таблице NAT.

R2 повторяет процедуру для второго узла, 192.168.11.10, выбирая следующий доступный глобальный адрес из динамического пула адресов и создавая вторую запись преобразования, 20165.200.227.

1. R2 заменяет внутренний локальный адрес источника ПК 1 (192.168.10.10) используемым для преобразования внутренним глобальным адресом (20165.200.226) и пересылает пакет. Те же действия выполняются для пакета, отправленного ПК 2, с использованием для преобразования адреса, соответствующего ПК 2 (20165.200.227).

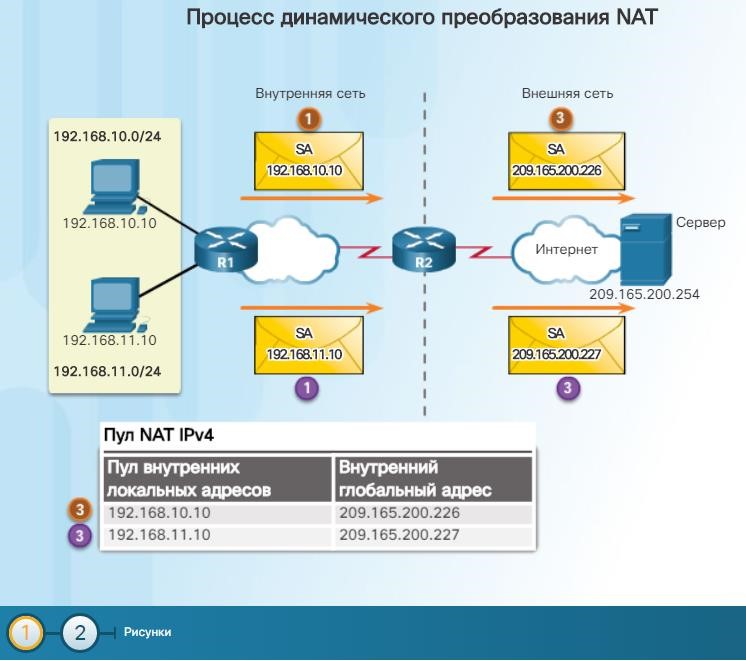
На рис. 2 показан поток трафика снаружи вовнутрь.

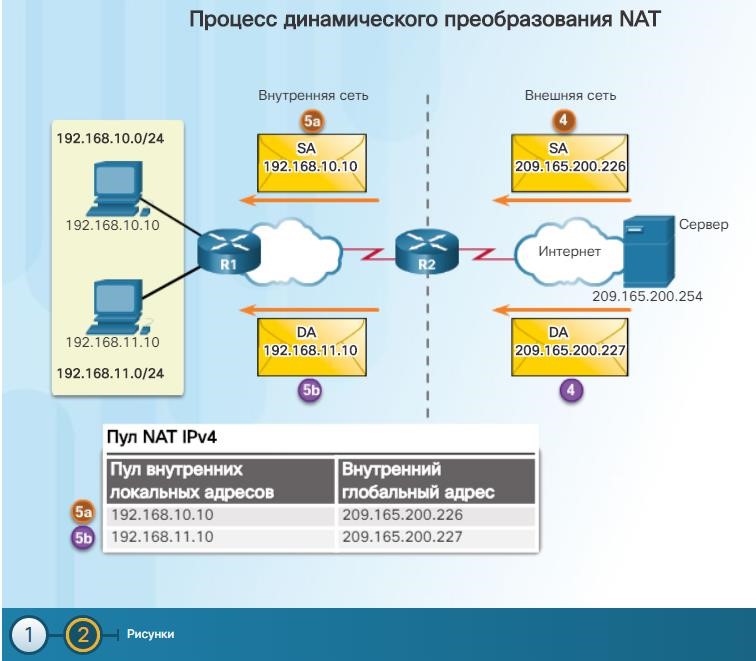
1. Сервер получает пакет от ПК 1 и отвечает, используя IPv4-адрес назначения 20165.200.226. Получив второй пакет, сервер отвечает ПК 2, используя IPv4-адрес назначения 20165.200.227.

5a. Получив пакет с IPv4-адресом назначения 20165.200.226, маршрутизатор R2 выполняет поиск в таблице NAT. С помощью сопоставления из таблицы маршрутизатор R2 выполняет преобразование адреса обратно во внутренний локальный адрес (192.168.10.10) и пересылает пакет ПК 1.

5b. Получив пакет с IPv4-адресом назначения 20165.200.227, маршрутизатор R2 выполняет поиск в таблице NAT. С помощью сопоставления из таблицы маршрутизатор R2 выполняет преобразование адреса обратно во внутренний локальный адрес (192.168.11.10) и пересылает пакет ПК 2.

6. ПК 1 с адресом 192.168.10.10 и ПК 2 с адресом 192.168.11.10 получают пакеты и продолжают диалог. Маршрутизатор NAT выполняет шаги 2-5 для каждого пакета (шаг 6 не приводится на рисунках).





### 2.2.4 Проверка динамического NAT

В выходных данных команды **show ip nat translations**, представленных на рис. 1, показаны сведения о двух предыдущих назначениях NAT. Команда отображает все настроенные статические преобразования адресов и все динамические преобразования, созданные в результате обработки трафика.

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

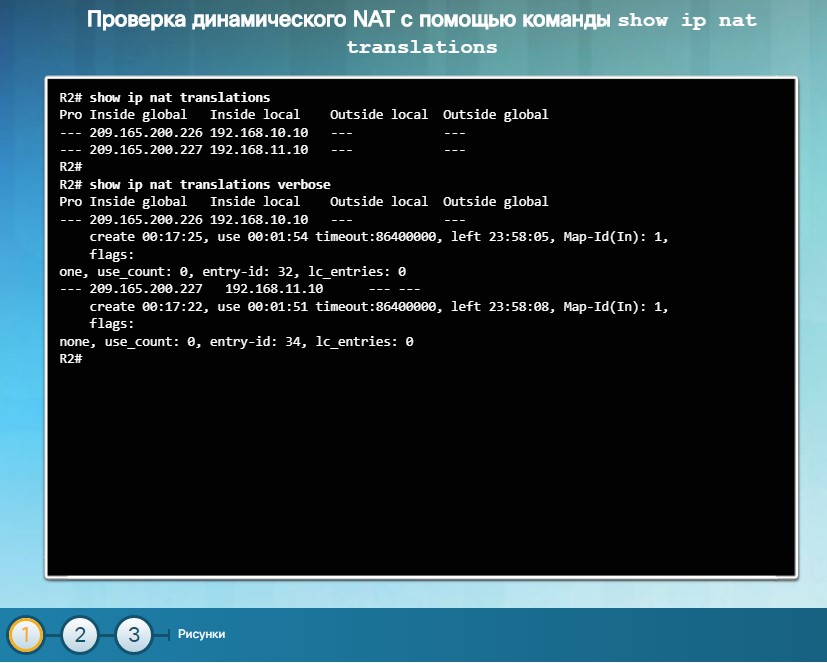
По умолчанию срок действия записей преобразования истекает через 24 часа, если настройка таймеров не была изменена с помощью команды **ip nat translation timeout** *timeout-seconds* в режиме глобальной конфигурации.

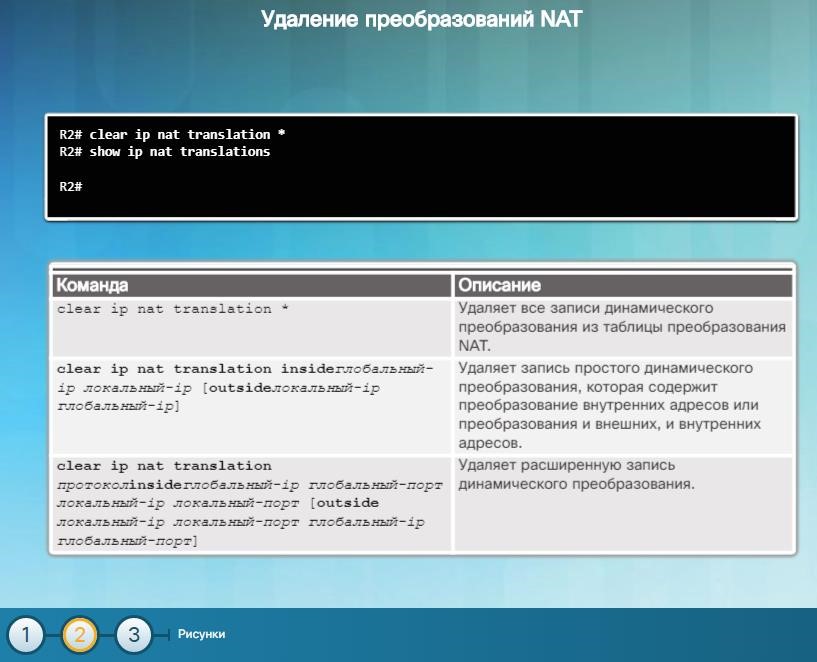
Для удаления динамических записей до истечения их времени действия используйте команду привилегированного режима EXEC **clear ip nat translation** (рис. 2). При проведении проверки настройки NAT рекомендуется удалять динамические записи. Как показано в таблице, эту команду можно использовать с ключевыми словами и переменными, чтобы определить удаляемые записи. Удаление конкретных записей нужно для того, чтобы не нарушить работу активных сеансов. Для удаления всех преобразований из таблицы используйте команду привилегированного режима EXEC **clear ip nat translation**\*.

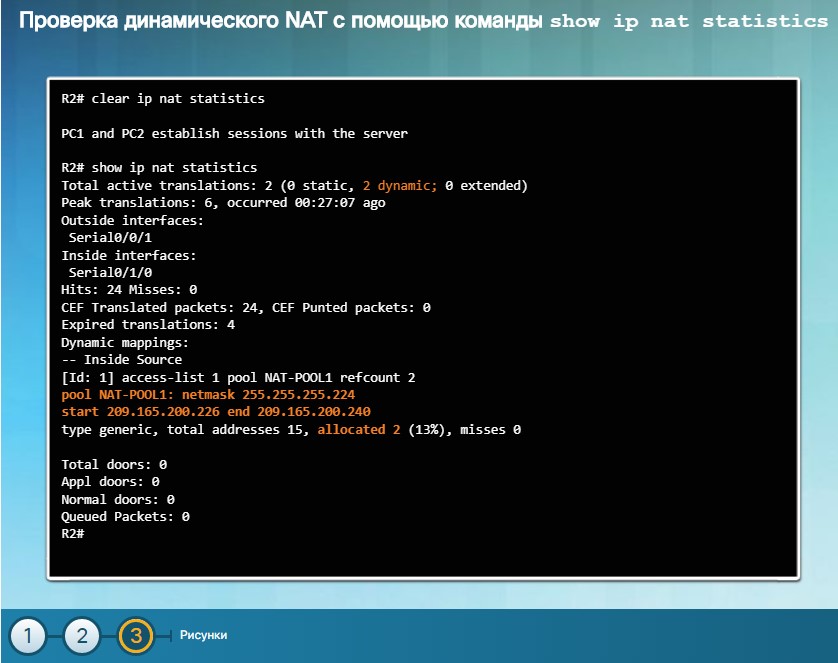
**Примечание**. Из таблицы удаляются только динамические преобразования. Статические адреса нельзя убрать из таблицы преобразований.

Как показано на рис. 3, команда **show ip nat statistics** выводит сведения о суммарном количестве активных преобразований, параметрах настройки NAT, числе адресов в пуле и числе выделенных адресов.

В качестве альтернативы можно воспользоваться командой **show running-config** и найти команды NAT, ACL, интерфейса или пула с нужными значениями. Внимательно изучите результаты и исправьте все обнаруженные ошибки.







### 2.2.5 Packet Tracer. Настройка динамического NAT

**В рамках данного упражнения Packet Tracer необходимо решить следующие задачи:**

* Часть 1. Настройка динамического преобразования NAT
* Часть 2. Проверка реализации NAT

[Практическая работа NAT-3. Настройка динамического NAT. Инструкции](files/Практическая%20работа%20NAT-3_Настройка%20динамического%20NAT.docx)

[Packet Tracer NAT-3. Настройка динамического NAT. PKA](files/Практическая%20работа%20NAT-3_Настройка%20динамического%20NAT.pka)

### 2.2.6 Лабораторная работа. Настройка динамического и статического NAT

**В этой лабораторной работе вы выполните следующие задачи:**

* Часть 1. Построение сети и проверка соединения
* Часть 2. Настройка и проверка статического NAT
* Часть 3. Настройка и проверка динамического NAT

[Лабораторная работа NAT-4. Настройка динамического и статического NAT](files/Лабораторная%20работа%20NAT-4_Настройка%20динамического%20и%20статического%20NAT.docx)

## 2.3 настройка РАТ

### 2.3.1 Настройка РАТ. Пул адресов

Преобразование адреса и номера порта PAT (также называемое NAT с перегрузкой) экономит адреса во внутреннем пуле глобальных адресов, разрешая маршрутизатору использовать один внутренний глобальный адрес для нескольких внутренних локальных адресов. Другими словами, один публичный IPv4-адрес может использоваться для сотен или даже тысяч внутренних частных IPv4-адресов. Если настроен данный тип преобразования, маршрутизатор хранит достаточный объем информации протоколов более высоких уровней, например, номера портов TCP или UDP, для обратного преобразования внутреннего глобального адреса в нужный внутренний локальный адрес. При привязке нескольких внутренних локальных адресов одному внутреннему глобальному адресу для различения локальных адресов используются номера портов TCP или UDP.

**Примечание.** Суммарное количество внутренних адресов, которые могут быть преобразованы в один внешний адрес, теоретически может достигать 65 536 на один IPv4-адрес. Но число внутренних адресов, которым можно назначить один IPv4-адрес, приблизительно составляет 4000.

В зависимости от способа выделения публичных IPv4-адресов интернет-провайдером существуют два способа настройки PAT. В первом случае интернет-провайдер выделяет организации несколько публичных IPv4-адресов, а во втором случае выделяется единственный публичный IPv4-адрес, необходимый организации для подключения к сети интернетпровайдера.

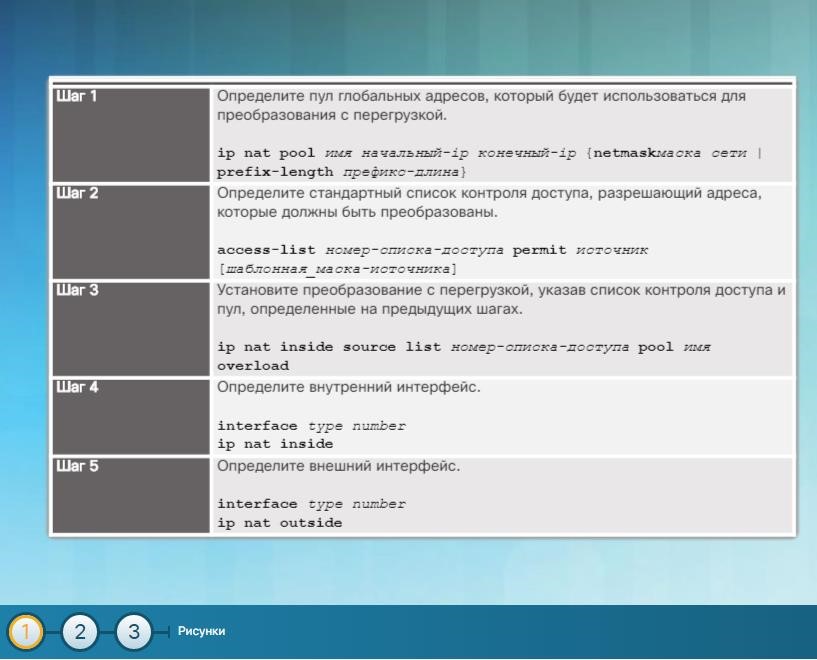
#### Настройка PAT для пула общедоступных IPv4-адресов

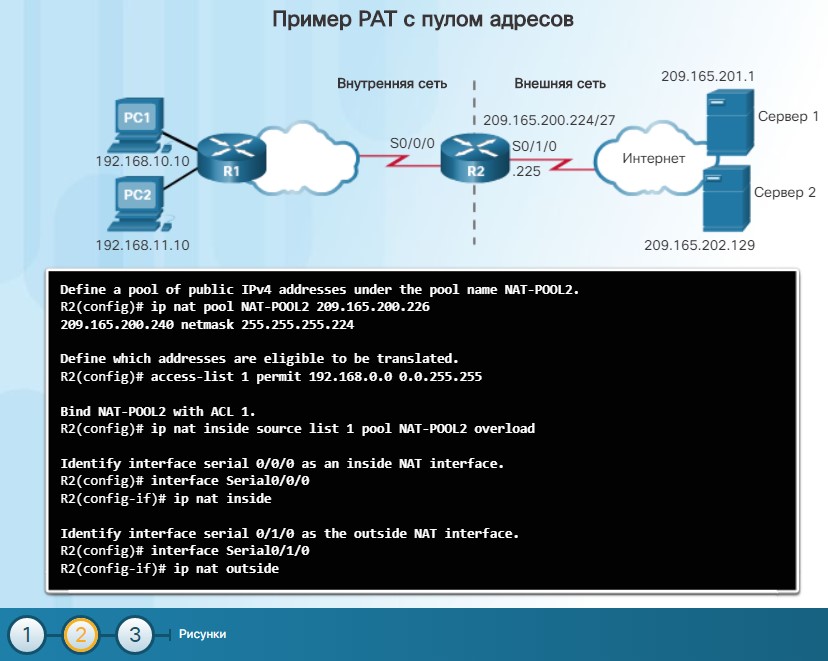
Если объекту было выделено несколько публичных IPv4-адресов, то эти адреса могут быть частью пула, используемого PAT. Это аналогично динамическому NAT, за исключением того, что публичных адресов недостаточно для создания взаимно-однозначных соответствий внутренних и внешних адресов. Небольшой пул адресов совместно используется большим числом устройств.

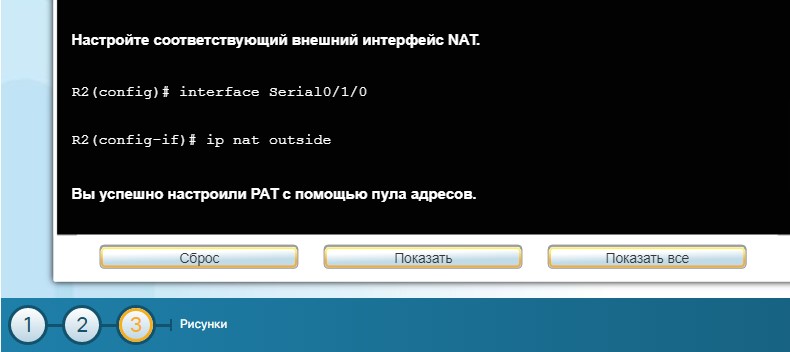
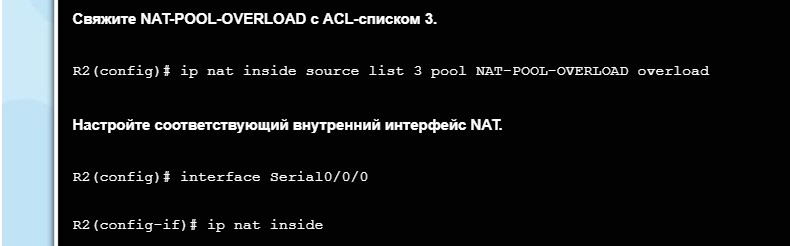
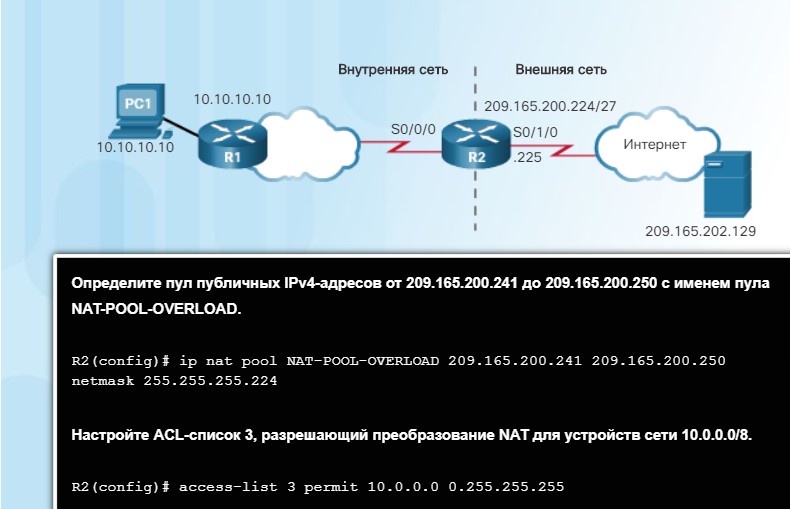
На рис. 1 показаны действия по настройке PAT для использования пула адресов. Основное различие между данной настройкой и настройкой для динамического взаимно-однозначного NAT состоит в использовании ключевого слова **overload**. Ключевое слово **overload** включает PAT.

В примере настройки, показанном на рис. 2, создается преобразование с перегрузкой для пула NAT с именем NATPOOL2. NAT-POOL2 содержит адреса с 20165.200.226 по 20165.200.240. Объектами преобразования являются узлы сети 192.168.0.0/16. В качестве внутреннего интерфейса определен интерфейс S0/0/0, а в качестве внешнего интерфейса — интерфейс S0/1/0.

Используйте средство проверки синтаксиса на рис. 3, чтобы настроить PAT на маршрутизаторе R2, используя пул адресов.







### 2.3.2 Настройка РАТ. Единый адрес

#### Настройка PAT для одного публичного IPv4-адреса

На рис. 1 показана топология реализации PAT для преобразования одного публичного IPv4-адреса. 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 20165.200.225 (IPv4-адрес интерфейса S0/1/0). Потоки трафика будут определяться номерами портов в таблице NAT, поскольку было использовано ключевое слово **overload**.

На рис. 2 показаны шаги, необходимые для настройки PAT с одним IPv4-адресом. Если доступен только один публичный IPv4-адрес, для настройки с перегрузкой обычно назначается публичный адрес внешнего интерфейса, подключаемого к интернет-провайдеру. Все внутренние адреса в пакетах, выходящих из внешнего интерфейса, преобразуются в один IPv4-адрес.

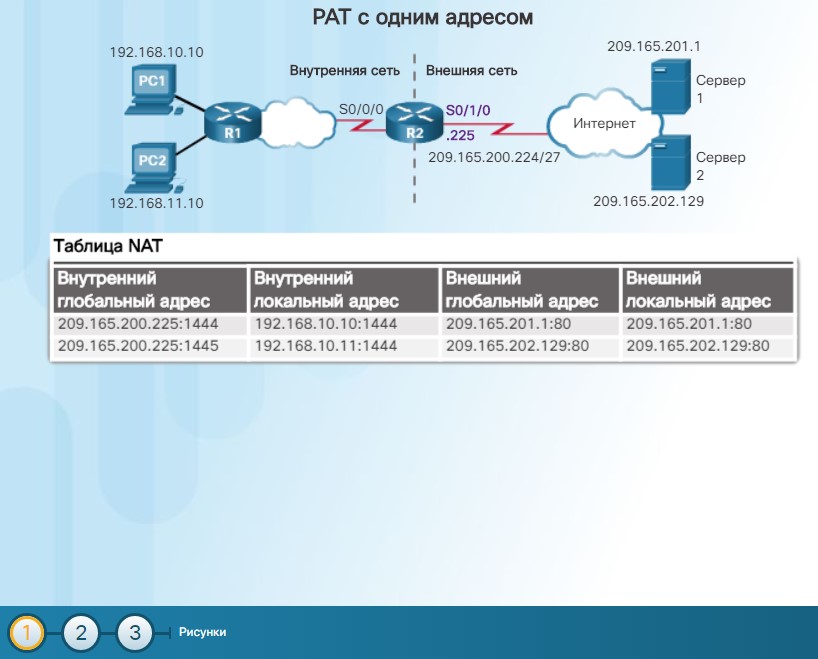
**Шаг 1.** Определите ACL, разрешающий преобразование трафика.

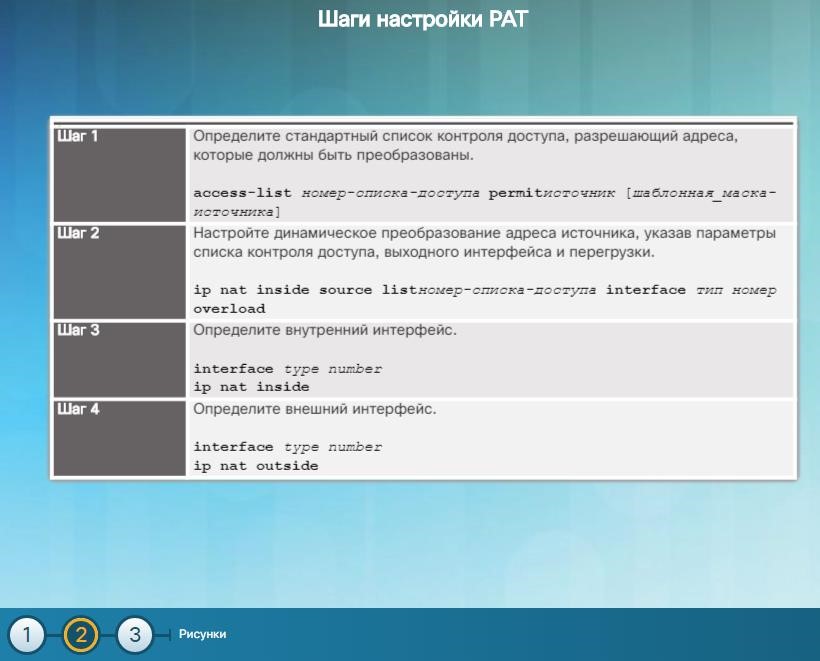
**Шаг 2.** Настройте преобразование адреса источника, используя ключевые слова **interface** и **overload**. Ключевое слово **interface** определяет IPv4-адрес интерфейса, который будет использоваться при преобразовании внутренних адресов. Ключевое слово **overload** указывает маршрутизатору отслеживать номера портов для каждой записи NAT. **Шаг 3.** Укажите интерфейсы, являющиеся внутренними по отношению к NAT. Это любой интерфейс, подключенный к внутренней сети.

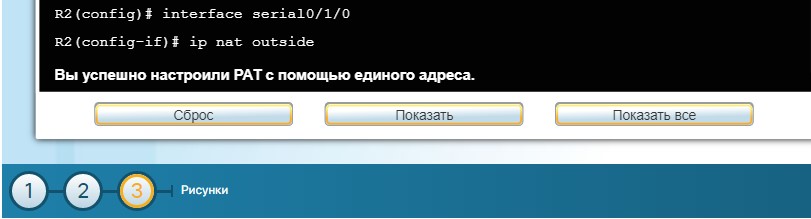
**Шаг 4.** Укажите интерфейс, являющийся внешним по отношению к NAT. Это должен быть тот же интерфейс, что указан в записи преобразования источника на шаге 2.

Эта настройка аналогична динамическому NAT, за исключением использования ключевого слова **interface** вместо пула адресов для определения внешнего IPv4-адреса. Таким образом, пул NAT не определяется.

Используйте средство проверки синтаксиса на рис. 3, чтобы настроить PAT на маршрутизаторе R2 с использованием одного адреса.







### 2.3.3 Анализ РАТ

Процесс преобразования NAT с перегрузкой является одинаковым как при использовании пула адресов, так и при использовании одного адреса. Продолжим предыдущий пример PAT с использованием одного публичного IPv4-адреса. Компьютеру ПК1 требуется подключение к веб-серверу Сервер 1. Одновременно другому клиенту, ПК 2, нужно установить аналогичный сеанс с веб-сервером Сервер 2. И для ПК 1, и для ПК 2 настроены частные IPv4-адреса, а на маршрутизаторе R2 включено преобразование PAT.

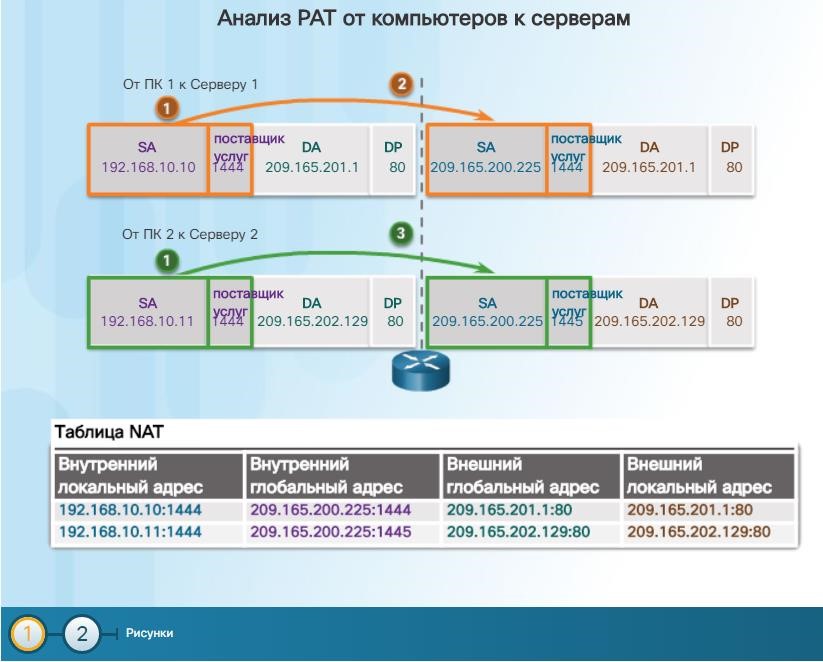
#### Процесс передачи пакетов от компьютеров к серверам

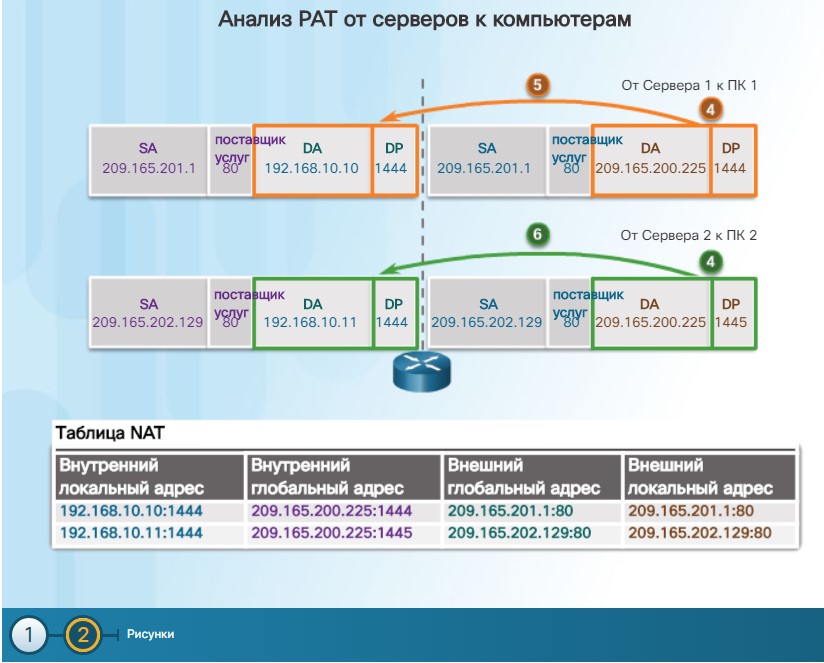
1. На рис. 1 показаны компьютеры ПК 1 и ПК 2, отправляющие пакеты серверам Сервер 1 и Сервер 2 соответственно. ПК 1 использует IPv4-адрес 192.168.10.10 и порт TCP источника 1444. ПК 2 использует IPv4-адрес 192.168.10.11 источника и, по случайному совпадению, тот же порт TCP источника — 1444.
2. Пакет компьютера ПК 1 первым достигает маршрутизатора R2. Используя PAT, R2 изменяет IPv4-адрес источника на 20165.200.225 (внутренний глобальный адрес). В таблице NAT отсутствуют другие устройства, использующие порт 1444, поэтому PAT сохраняет этот же номер порта. Затем пакет пересылается серверу Сервер 1 по адресу 20165.201.1.
3. Далее на маршрутизатор R2 приходит пакет с ПК 2. Настройка PAT обеспечивает использование для всех преобразований одного внутреннего глобального IPv4-адреса — 20165.200.225. Аналогично процессу преобразования для ПК 1, PAT изменяет IPv4-адрес источника ПК 2 на внутренний глобальный адрес 20165.200.225. Однако в этом пакете ПК 2 используется номер порта источника, уже содержащийся в текущей записи PAT, обеспечивающей преобразование для ПК 1. PAT увеличивает номер порта источника, пока его значение не окажется уникальным для данной таблицы. В данном случае записи порта источника в таблице NAT и пакету от ПК 2 назначается номер 1445.

Хотя ПК 1 и ПК 2 используют одинаковый преобразованный адрес - внутренний глобальный адрес 20165.200.225, и одинаковый номер порта источника — 1444, измененный номер порта для ПК 2 (1445) делает уникальной каждую запись в таблице NAT. Это становится очевидным при отправке серверами ответных пакетов клиентам.

#### Процесс передачи пакетов от серверов к компьютерам

1. Как показано на рис. 2, при типовом обмене «клиент-сервер» серверы Сервер 1 и Сервер 2 отвечают на запросы, полученные от компьютеров ПК 1 и ПК 2 соответственно. Серверы используют для обратного трафика порт источника из полученного пакета в качестве порта назначения и адрес источника — в качестве адреса назначения. Серверы ведут себя так, как если бы они взаимодействовали с одним узлом 20165.200.225, однако это не так.
2. Получив пакеты, маршрутизатор R2 находит уникальную запись в таблице NAT, используя адрес назначения и порт назначения каждого пакета. В случае получения пакета от сервера Сервер 1 адресу назначения IPv4 20165.200.225 соответствует несколько записей, но только одна из них содержит порт назначения 1444. Используя эту запись таблицы, маршрутизатор R2 изменяет IPv4-адрес назначения пакета на 192.168.10.10. Изменение порта назначения в данном случае не требуется. Затем пакет пересылается компьютеру ПК 1.
3. Получив пакет от сервера Сервер 2, маршрутизатор R2 выполняет аналогичное преобразование. Маршрутизатор снова находит адрес назначения IPv4 20165.200.225 с несколькими записями. Однако, используя порт назначения 1445, R2 может уникально идентифицировать запись преобразования. IPv4-адрес назначения меняется на 192.168.10.11. В этом случае порт назначения также необходимо изменить обратно на первоначальное значение 1444, сохраненное в таблице NAT. Затем пакет пересылается компьютеру ПК 2.

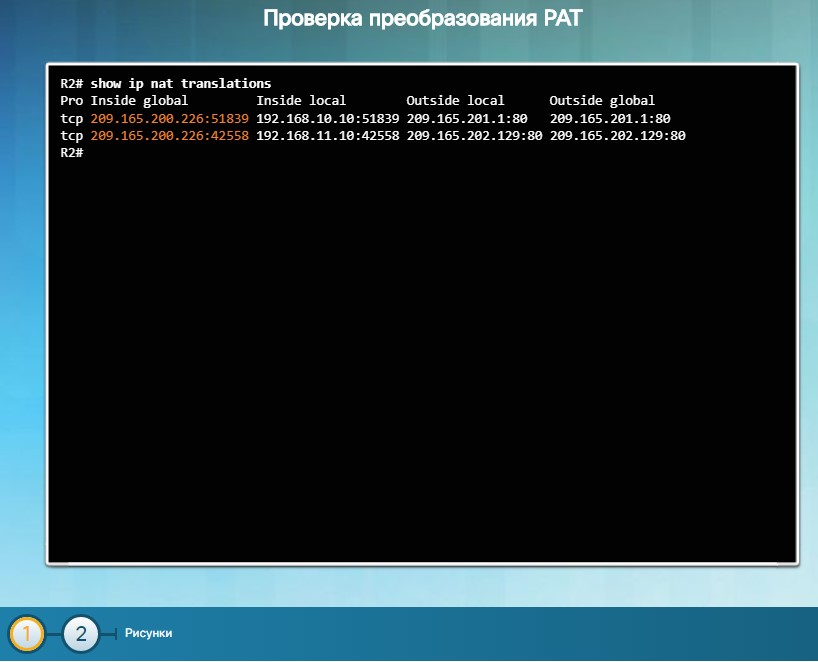


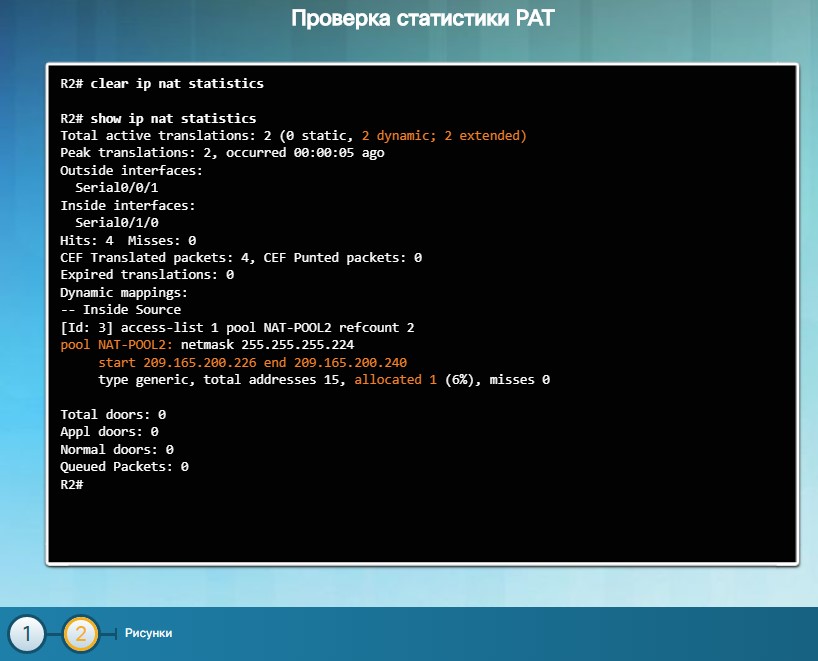


### 2.3.4 Проверка РАТ

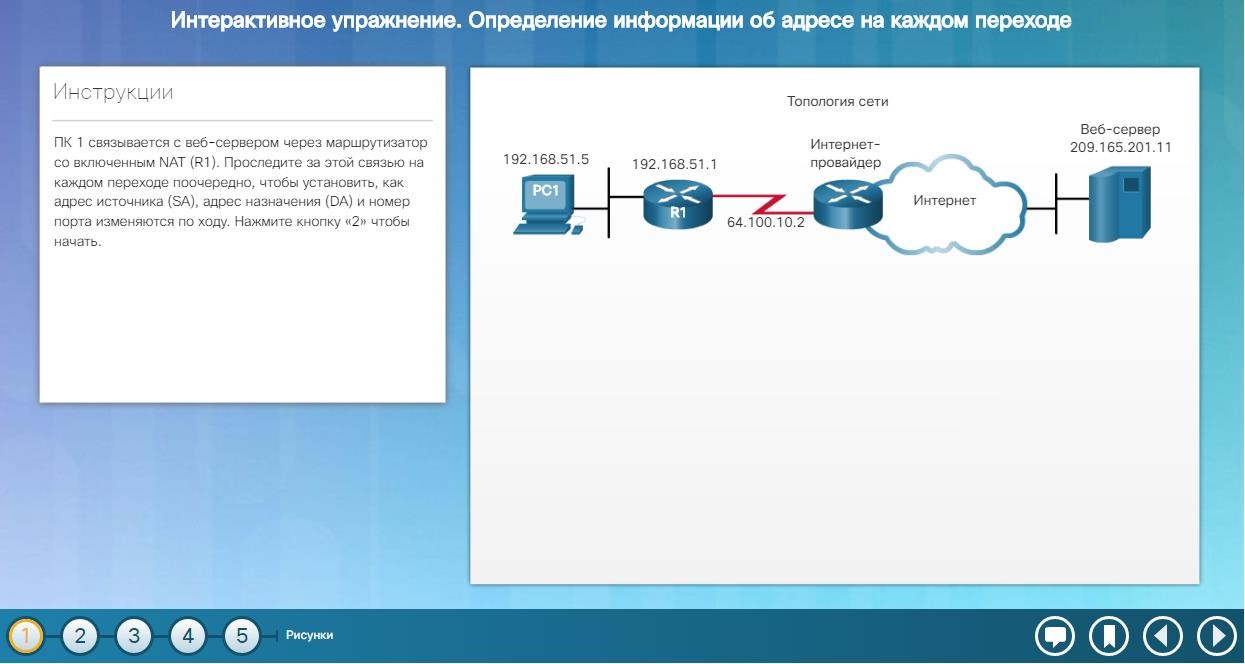
Маршрутизатор R2 настроен на предоставление PAT клиентам из сети 192.168.0.0/16. Когда внутренние узлы выходят через маршрутизатор R2 в Интернет, выполняется преобразование их адресов в IPv4-адрес из пула PAT с уникальным номером порта источника. Для проверки PAT используются те же команды, что и для проверки статического и динамического NAT, как показано на рис. 1. 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 20165.200.226 (внутренний глобальный адрес). Для различения этих двух транзакций в таблице NAT используются номера портов источников.

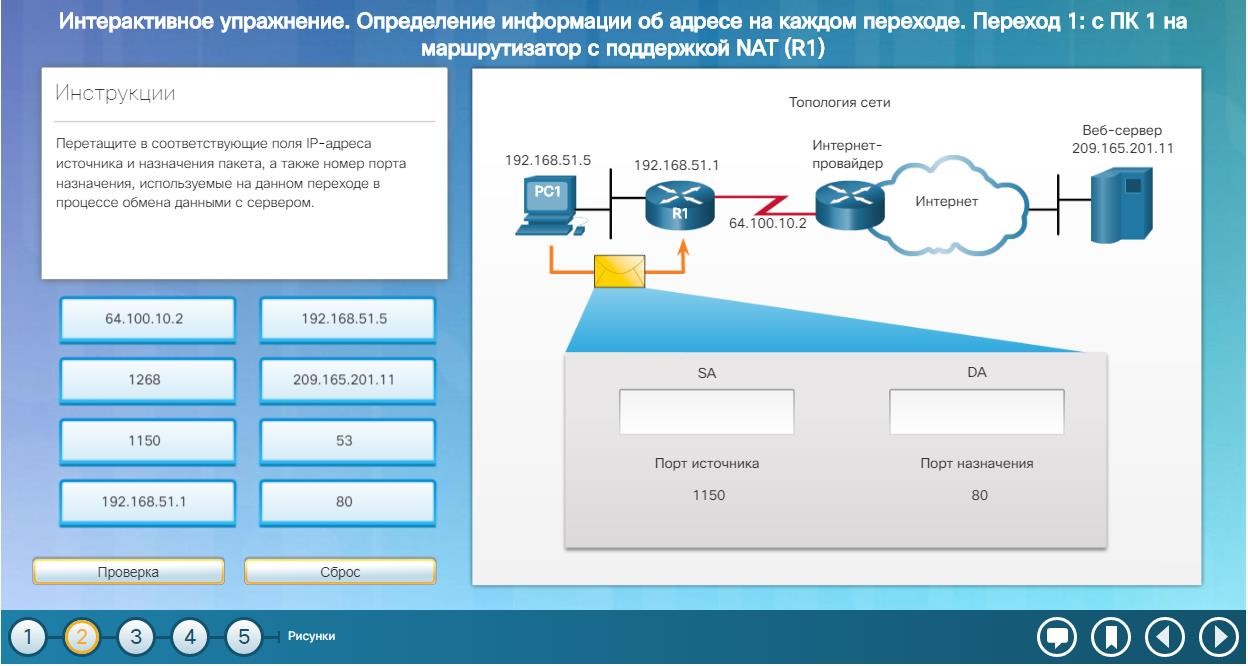
Как показано на рис. 2, команда **show ip nat statistics** позволяет проверить, что в пуле NAT-POOL2 выделен один адрес для обоих преобразований. В выходных данных команды содержатся сведения о количестве и типе активных преобразований, параметрах настройки NAT, количестве адресов в пуле и количестве выделенных адресов.

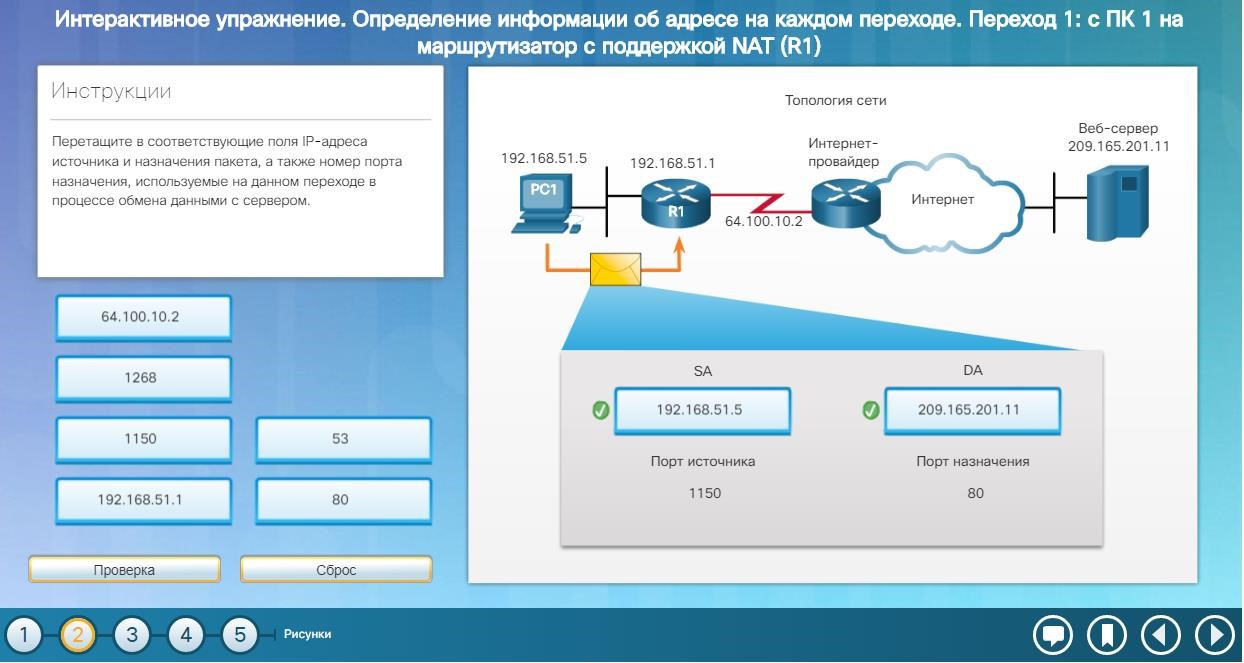


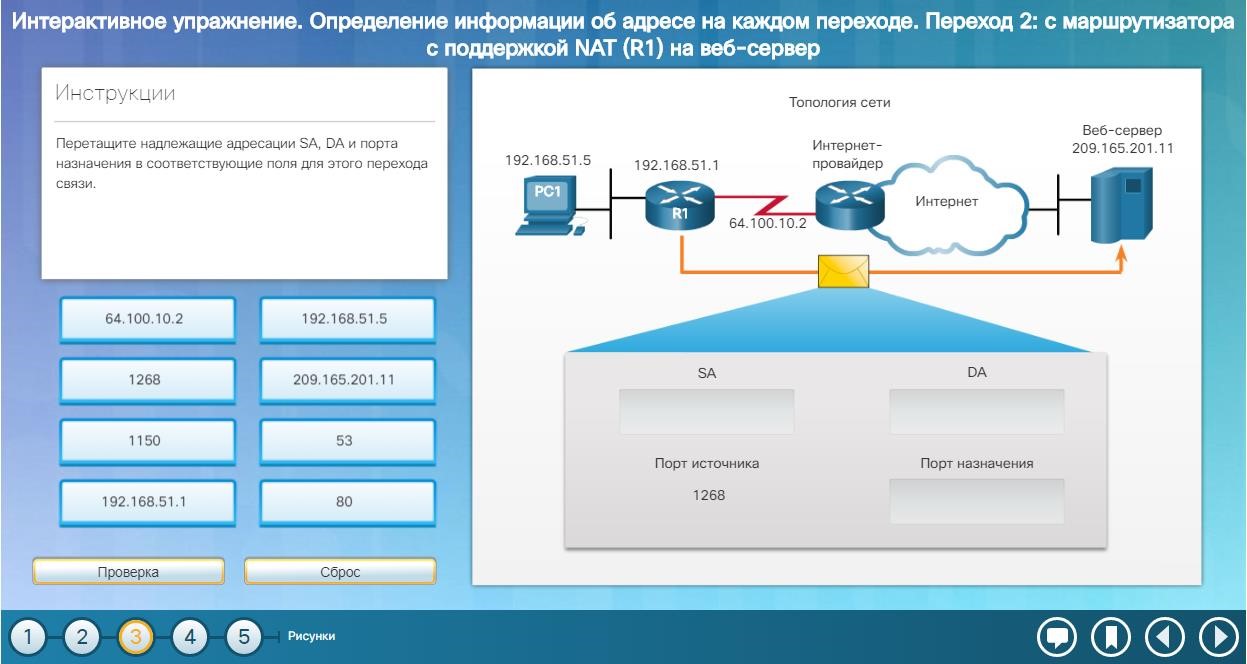


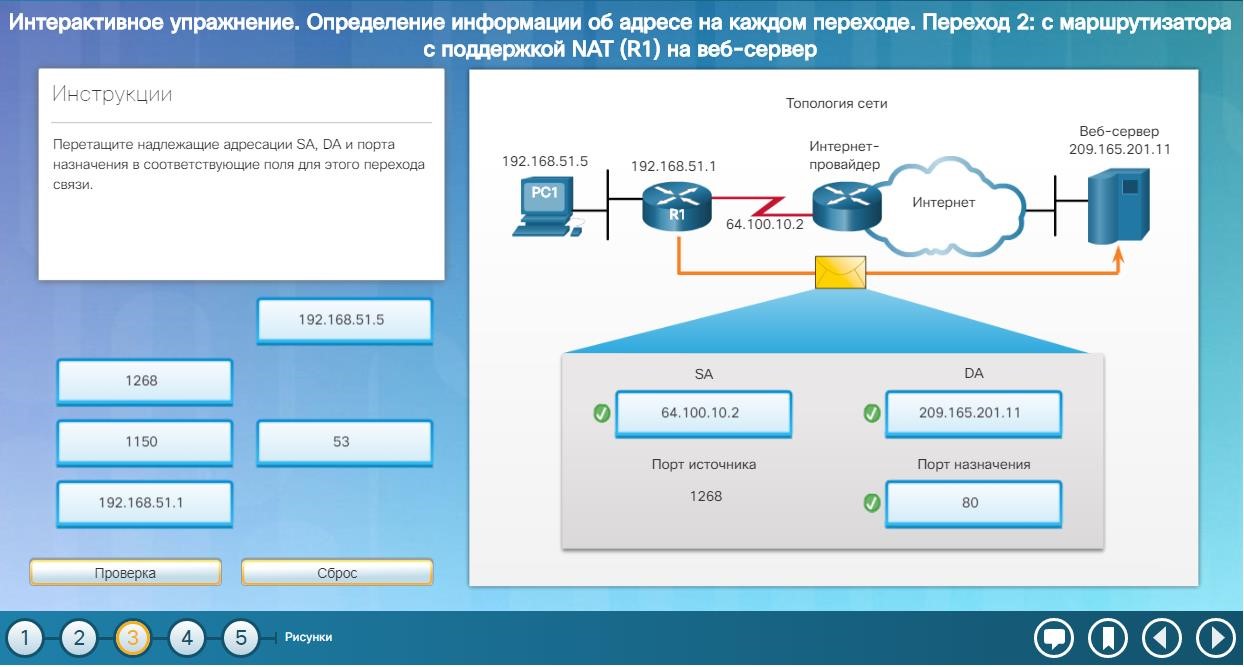
### 2.3.5 Интерактивное задание. Определение информации об адресе на каждом переходе

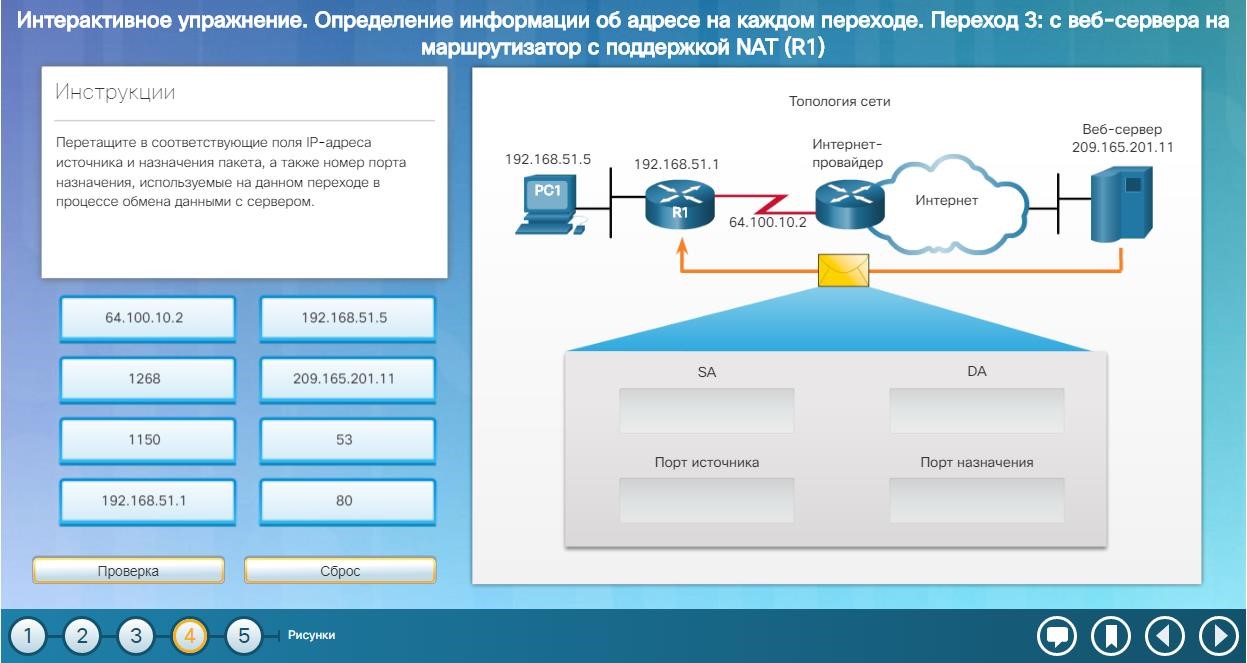


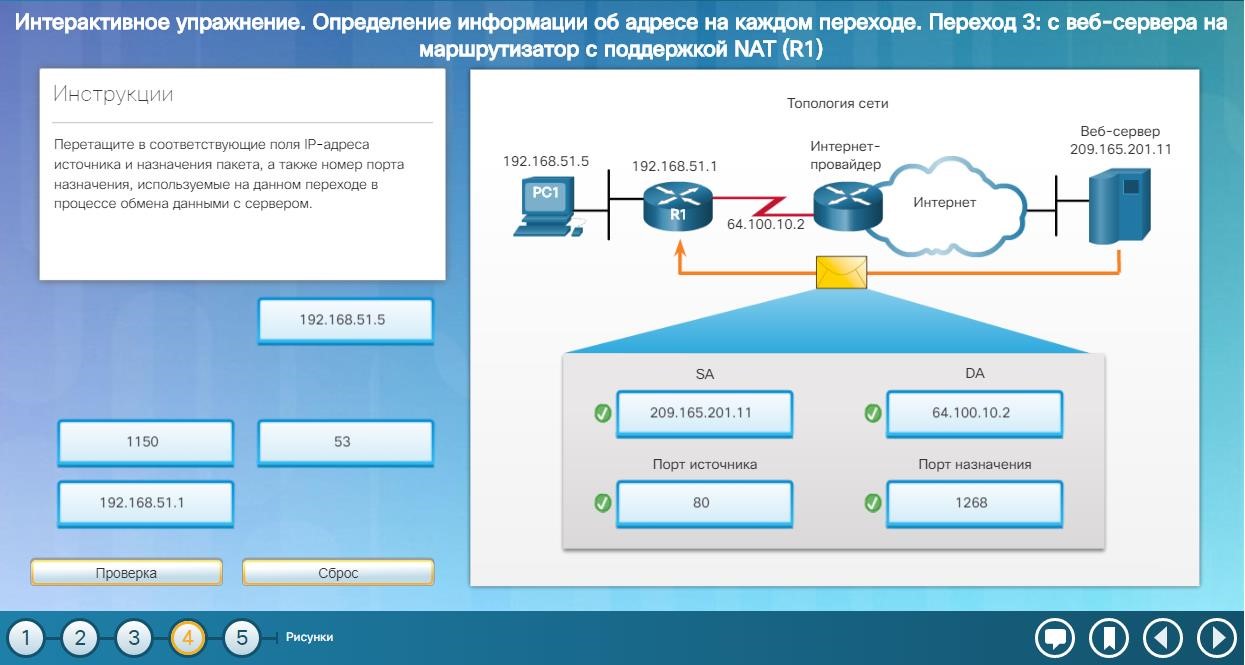


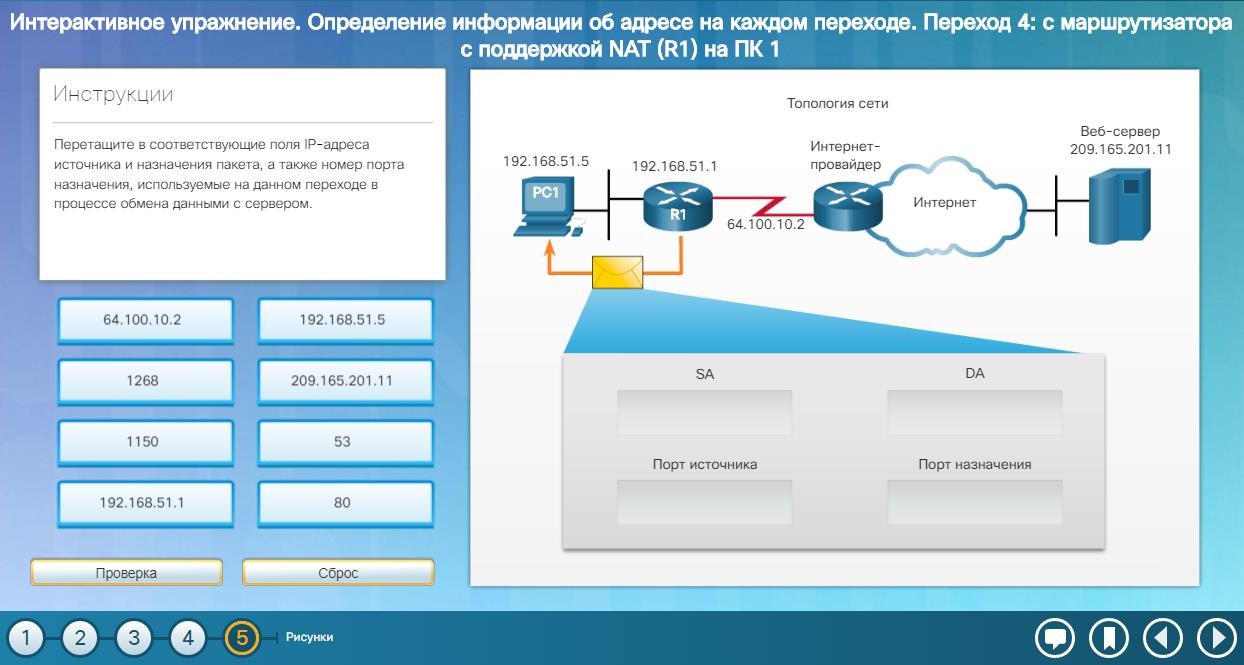


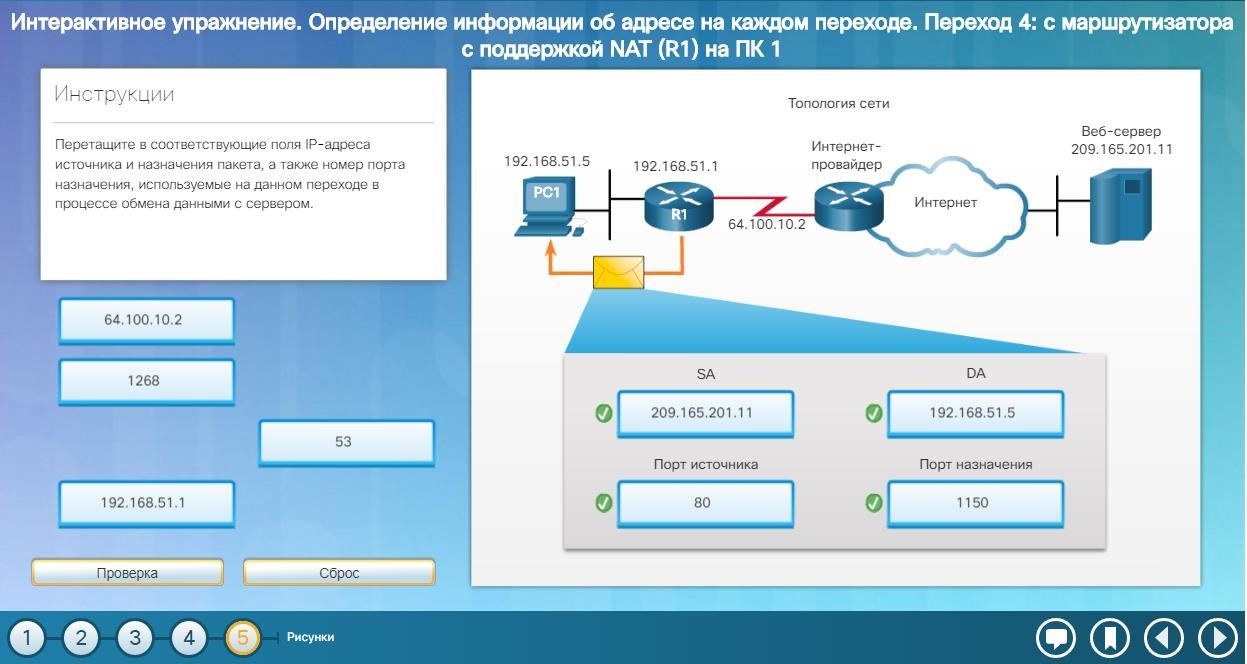












### 2.3.6 Packet Tracer. Реализация статического и динамического NAT

**В рамках данного упражнения Packet Tracer необходимо решить следующие задачи:**

* Часть 1. Настройка динамического NAT с использованием PAT
* Часть 2. Настройка статического преобразования (NAT)
* Часть 3. Проверка реализации NAT

[Практическая работа NAT-5. Реализация статического и динамического NAT. Инструкции](files/Практическая%20работа%20NAT-5_Реализация%20статического%20и%20динамического%20NAT.docx)

[Packet Tracer NAT-5. Реализация статического и динамического NAT. PKA](files/Практическая%20работа%20NAT-5_Реализация%20статического%20и%20динамического%20NAT.pka)

2.3.7 Лабораторная работа. Настройка преобразования адреса и номера порта

# (РАТ)

**В этой лабораторной работе вы выполните следующие задачи:**

* Часть 1. Построение сети и проверка соединения
* Часть 2. Настройка и проверка пула NAT с перегрузкой
* Часть 3. Настройка и проверка PAT

[Лабораторная работа NAT-6. Настройка преобразования адреса и номера порта (PAT)](files/Лабораторная%20работа%20NAT-6_Настройка%20преобразования%20адреса%20и%20номера%20порта%20_PAT.docx)

## 2.4 Настройка перенаправления портов

### 2.4.1 Перенаправление портов

Перенаправление портов — это перенаправление трафика, адресованного определенному сетевому порту, от одного узла сети на другой узел. Данный метод позволяет внешним пользователям снаружи достигать порта для частного IPv4адреса (в локальной сети), используя маршрутизатор с поддержкой NAT.

Как правило, для работы пиринговых программ обмена файлами и выполнения таких операций, как работа веб-сервера или исходящий FTP, требуется, чтобы порты маршрутизатора были перенаправлены или открыты, как показано на рис. 1. Поскольку NAT скрывает внутренние адреса, пиринговые приложения работают только изнутри — в этом случае NAT может сопоставить исходящие запросы и входящие ответы.

Проблема заключается в том, что NAT не разрешает инициировать запросы снаружи. Эту ситуацию можно разрешить с помощью изменений, внесенных вручную. Можно настроить перенаправление портов, чтобы определить конкретные порты, которые могут быть переадресованы на внутренние узлы.

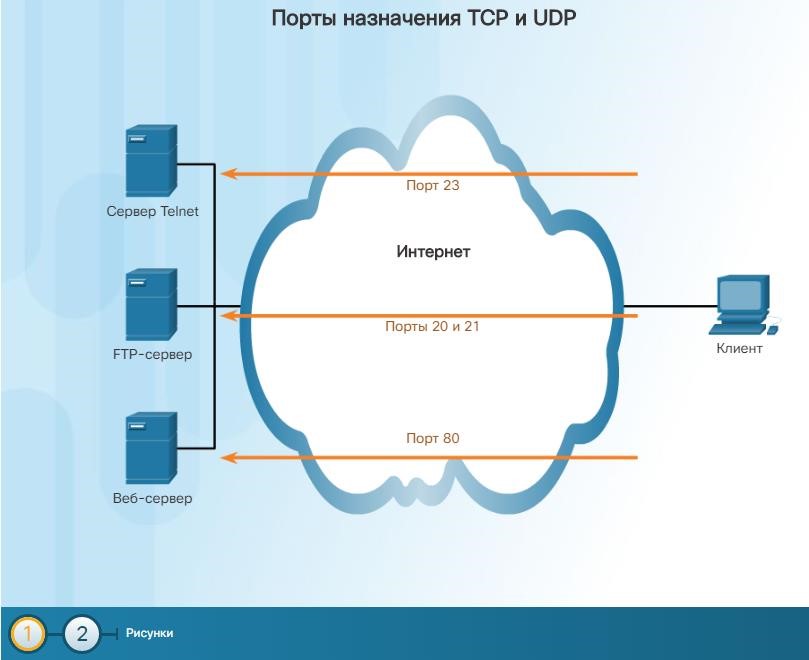
Помните, что программные приложения для Интернета работают с пользовательскими портами, которые должны быть открыты или доступны этим приложениям. Различные приложения используют разные порты. Это позволяет приложениям и маршрутизаторам определять сетевые сервисы. Например, HTTP работает через общеизвестный порт 80. Когда кто-то вводит адрес **http://cisco.com**, в веб-браузере отображается веб-сайт Cisco Systems, Inc. Обратите внимание, что пользователю не нужно указывать номер порта HTTP для запроса страницы, поскольку приложение предполагает, что будет использоваться порт 80.

Если требуется другой номер порта, его можно добавить к URL-адресу, отделив двоеточием (:). Например, если вебсервер прослушивает порт 8080, пользователь должен ввести **http://www.example.com:8080**.

Перенаправление портов позволяет пользователям достигать внутренних серверов из Интернета, используя адрес WANмаршрутизатора и соответствующий номер внешнего порта. Внутренние серверы обычно настраиваются с

использованием частных IPv4-адресов, соответствующих RFC 1918. Когда запрос отправляется по IPv4-адресу порта WAN через Интернет, маршрутизатор переадресует запрос соответствующему серверу в локальной сети. Из соображений безопасности широкополосные маршрутизаторы по умолчанию не разрешают перенаправление внешних веб-запросов узлам внутренней сети.

На рис. 2 изображен владелец небольшого предприятия, использующий сервер PoS (пункт продаж) для отслеживания продаж и запасов на складе. Сервер доступен внутри склада, но поскольку ему назначен частный адрес IPv4, публичный доступ к этому серверу из Интернета невозможен. Включение на локальном маршрутизаторе перенаправления портов предоставляет владельцу доступ к серверу пункта продаж из Интернета. Перенаправление портов на маршрутизаторе настраивается с помощью номера порта назначения и частного IPv4-адреса сервера пункта продаж. Для доступа к серверу клиентское ПО должно использовать публичный IPv4-адрес маршрутизатора и порта назначения сервера.





### 2.4.2 Пример маршрутизатора беспроводной связи

На рисунке показано окно настройки перенаправления на один порт для маршрутизатора беспроводной связи Packet Tracer. По умолчанию перенаправление портов на маршрутизаторе не включено.

Перенаправление портов для приложений можно включить, указав внутренний локальный адрес, на который должны перенаправляться запросы. На рисунке запросы к службе HTTP, поступающие на маршрутизатор беспроводной связи, перенаправляются на веб-сервер с внутренним локальным адресом 192.168.1.254. Если внешний WAN IPv4-адрес маршрутизатора беспроводной связи — 20165.200.225, то внешний пользователь может ввести **http://www.example.com**, и этот маршрутизатор перенаправит запрос HTTP внутреннему веб-серверу по IPv4-адресу 192.168.1.254, используя номер порта по умолчанию — 80.

Можно также указать номер порта, отличающегося от номера порта по умолчанию, соответствующего 80. Однако внешний пользователь должен знать конкретный используемый номер порта. Чтобы определить другой порт, необходимо изменить значение внешнего порта (External Port) в окне перенаправления на один порт (Single Port Forwarding).

Подход при настройке перенаправления портов зависит от производителя и модели широкополосного маршрутизатора в сети. Однако некоторые действия являются общими для всех моделей. Если в инструкциях, предоставленных интернетпровайдером, или в инструкциях, прилагаемых к маршрутизатору, нет четких указаний, перейдите на вебсайт [http://www.portforward.com,](http://www.portforward.com/) где можно найти руководства для некоторых широкополосных маршрутизаторов. Следуйте инструкциям, чтобы при необходимости добавить или удалить порты в соответствии с потребностями любых приложений, которые нужно разрешить или отклонить.



### 2.4.3 Настройка перенаправления портов с помощью IOS

Реализация перенаправления портов с помощью команд IOS аналогична применению команд настройки статического NAT. Перенаправление портов фактически является статическим преобразованием NAT с указанным номером порта TCP или UDP.

На рис. 1 показана команда статического NAT, используемая для настройки перенаправления портов с помощью IOS. На рис. 2 приведен пример настройки перенаправления портов с помощью команд IOS на маршрутизаторе R2.

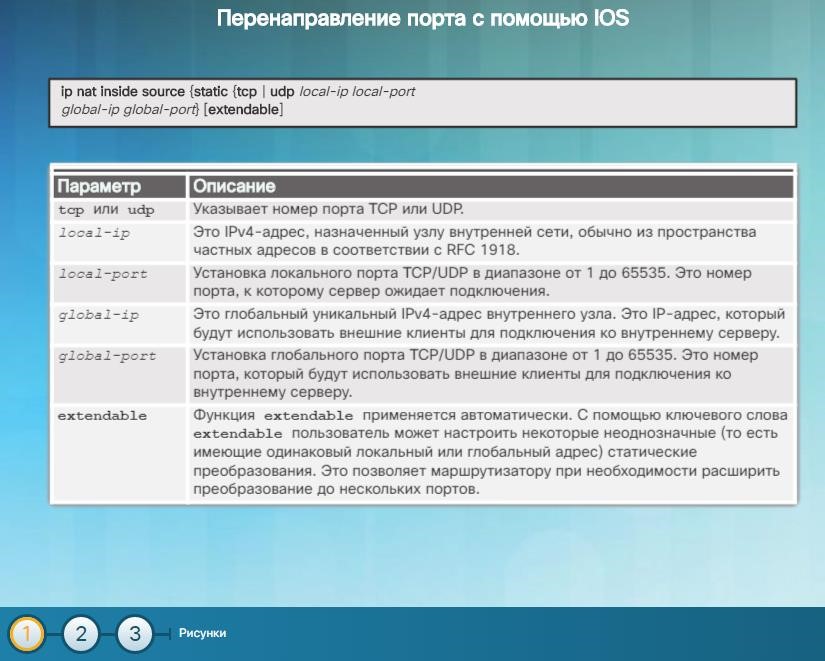
192.168.10.254 — это внутренний локальный IPv4-адрес веб-сервера, прослушивающего порт 80. Пользователи получат доступ к этому внутреннему веб-серверу с помощью глобального IPv4-адреса 20165.200.225, который является глобальным уникальным общедоступным IPv4-адресом. В данном случае это адрес интерфейса Serial 0/1/0 маршрутизатора R2. В качестве глобального порта настроен порт 8080. Он будет портом назначения, используемым вместе с глобальным IPv4-адресом 20165.200.225 для доступа к внутреннему веб-серверу. В настройке NAT обратите внимание на следующие параметры команды:

* *local-ip* = 192.168.10.254
* *local-port* = 80
* *global-ip* = 20165.200.225
* *global-port* = 8080

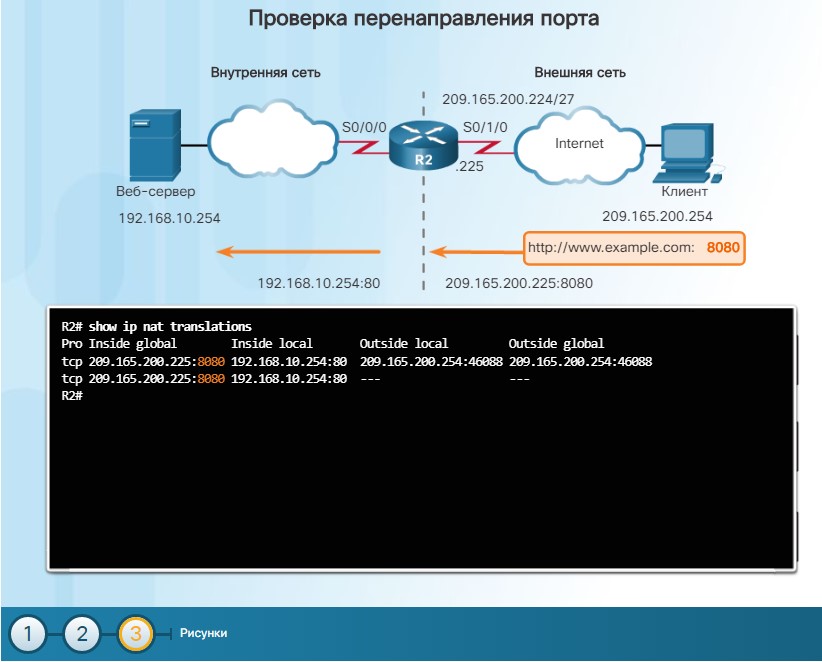
Если не используется стандартный номер порта, клиент должен указать номер порта в приложении. Как и для других типов NAT, для перенаправления портов необходимо настроить как внутренний, так и внешний интерфейсы NAT.

Аналогично статическому NAT, для проверки перенаправления портов можно использовать команду **show ip nat translations**, как показано на рис. 3.

В рассматриваемом примере, когда маршрутизатор получает пакет с внутренним глобальным IPv4-адресом 20165.200.225 и TCP-портом назначения 8080, он выполняет поиск в таблице NAT, используя в качестве ключа IPv4адрес назначения и порт назначения. Затем маршрутизатор преобразует адрес во внутренний локальный адрес узла 192.168.10.254 и порт назначения 80. Затем R2 пересылает пакет веб-серверу. Для обратных пакетов, идущих от вебсервера к клиенту, этот процесс инвертируется.







### 2.4.4 Packet Tracer. Настройка перенаправления портов на маршрутизаторе беспроводной связи

#### Сценарий

Ваш друг хочет играть с вами в игры на вашем сервере. Каждый из вас находится у себя дома, у каждого настроен выход в Интернет. Необходимо настроить маршрутизатор беспроводной связи для перенаправления портов в запросах HTTP к вашему серверу таким образом, чтобы ваш друг получил доступ к главной веб-странице игры.

[Практическая работа NAT-7. Настройка перенаправления портов на маршрутизаторе беспроводной связи. Инструкции](files/Практическая%20работа%20NAT-7_Настройка%20перенаправления%20портов%20на%20маршрутизаторе%20беспроводной%20связи.docx)

[Packet Tracer NAT-7. Настройка перенаправления портов на маршрутизаторе беспроводной связи. РКА](files/Практическая%20работа%20NAT-7_Настройка%20перенаправления%20портов%20на%20маршрутизаторе%20беспроводной%20связи.pka)

2.5 NAT и IPv6 2.5.1 NAT для IPv6?

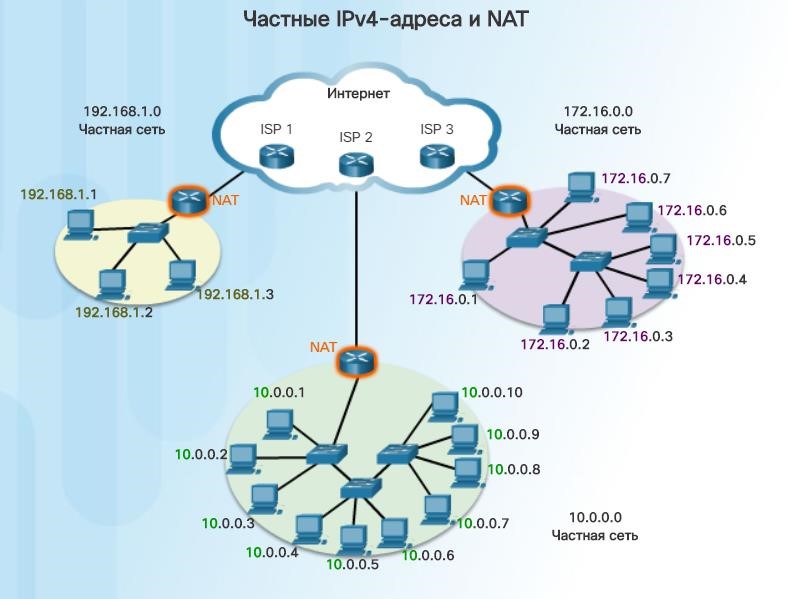
С начала 90-х гг. прошлого века приоритетной задачей для IETF стало решение проблемы исчерпания адресного пространства IPv4. Сочетание частных IPv4-адресов RFC 1918 и NAT стало средством замедления процесса исчерпания. NAT обладает заметными недостатками, и в январе 2011 г. Администрация адресного пространства Интернет (IANA) выделила для региональных регистраторов Интернета свои последние IPv4-адреса.

Одним из «ненамеренных» преимуществ NAT для IPv4 стало то, что эта технология скрывает частные сети от публичного Интернета. Преимуществом NAT является обеспечение кажущейся безопасности путем запрета компьютерам из публичного Интернета доступа к внутренним узлам. Но эту технологию нельзя считать заменой полноценной сетевой безопасности, например, обеспечиваемой межсетевым экраном.

Комиссия по архитектуре Интернета (IAB) включила в RFC 5902 следующее положение, касающееся преобразования IPv6:

«Обычно считается, что устройство NAT обеспечивает один уровень защиты, поскольку внешние узлы не могут напрямую начать взаимодействие с узлами, находящимися за устройством NAT. Но не следует путать устройства NAT с межсетевыми экранами. Как оговорено в разделе 2.2 RFC4864, само по себе преобразование не обеспечивает безопасность. Функция фильтрации с отслеживанием состояния (stateful filtering) обеспечивает тот же уровень защиты, не требуя функции преобразования».

Протокол IPv6 с 128-битовым адресом предоставляет 340 ундециллионов адресов. Таким образом, адресное пространство не является проблемой. Протокол IPv6 был разработан, чтобы устранить необходимость в NAT для IPv4 с его преобразованием между публичными и частными IPv4-адресами. Тем не менее, IPv6 действительно реализует определенную форму NAT. IPv6 включает и собственное пространство частных IPv6-адресов, и преобразования NAT, реализованные иначе, чем для IPv4.



### 2.5.2 Уникальные локальные IPv6-адреса

Уникальные локальные IPv6-адреса (unique local addresses, ULA) похожи на частные адреса RFC 1918 в IPv4, но при этом существенно отличаются от них. Цель unique local адресов — обеспечить пространство IPv6-адресов для взаимодействия в пределах локального объекта. Это не означает ни предоставления дополнительного пространства IPv6-адресов, ни обеспечения уровня безопасности.

Как показано на рисунке, unique local адрес использует префикс FC00::/7, и поэтому первая 16-битовая группа находится в диапазоне от FC00 до FDFF. Если префикс назначается локально, следующий один бит установлен равным 1. Возможность использования значения 0 может быть определена позже. Следующие 40 битов — это глобальный идентификатор, за которым следует 16-битовый идентификатор подсети. Эти первые 64 бита объединяются для создания префикса уникального локального адреса. Это оставляет 64 бита для идентификатора интерфейса или, согласно терминологии IPv4 — узловой части адреса.

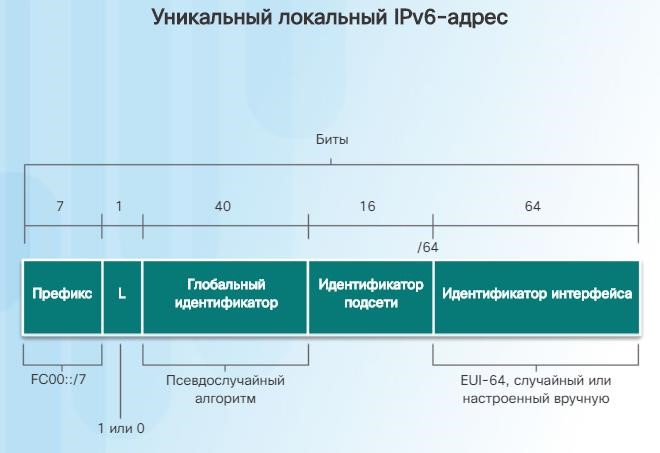
Уникальные локальные адреса определены в RFC 4193. Unique local адреса также называются локальными IPv6адресами (не следует путать с IPv6-адресами типа link-local) и обладают рядом характеристик, в том числе перечисленными ниже:

* Возможность объединять или частным образом соединять узлы без каких-либо конфликтов адресов или необходимости в перенумерации интерфейсов, использующих эти префиксы.
* Независимость от интернет-провайдера и возможность применения с целью взаимодействия внутри площадки без подключения к Интернету.
* Невозможность маршрутизации через Интернет, и даже при случайной «утечке» такого адреса из-за маршрутизации или DNS конфликт с другими адресами отсутствует.

Unique local адреса не настолько просты, как адреса RFC 1918. В отличие от частных IPv4-адресов, IETF не стремилась использовать разновидность NAT для преобразования между уникальными локальными адресами и глобальными индивидуальными адресами IPv6.

Реализация и потенциальные сферы применения уникальных локальных IPv6-адресов все еще изучается интернетсообществом. Например, организация IETF рассматривает возможность использования 40-разрядного глобального идентификатора, который назначается централизовано при использовании префикса уникального локального адреса FC00::/8. 40-разрядный глобальный идентификатор генерируется случайным образом либо может быть задан вручную при использовании префикса уникального локального адреса FD00::/8. Остальные адреса остаются неизменны. Мы все еще используем 16 битов для идентификатора подсети и 64 бита для идентификатора интерфейса.

**Примечание**. В исходной спецификации IPv6 было выделено адресное пространство для site-local адресов (с областью видимости в рамках одной площадки), определенных в RFC 3513. IETF признала в RFC 3879 site-local адреса устаревшими, поскольку термин «площадка» (site) был признан неоднозначным. Для адресов типа site-local использовался диапазон префиксов FEC0::/10, их по-прежнему можно найти в ряде устаревших документов IPv6.



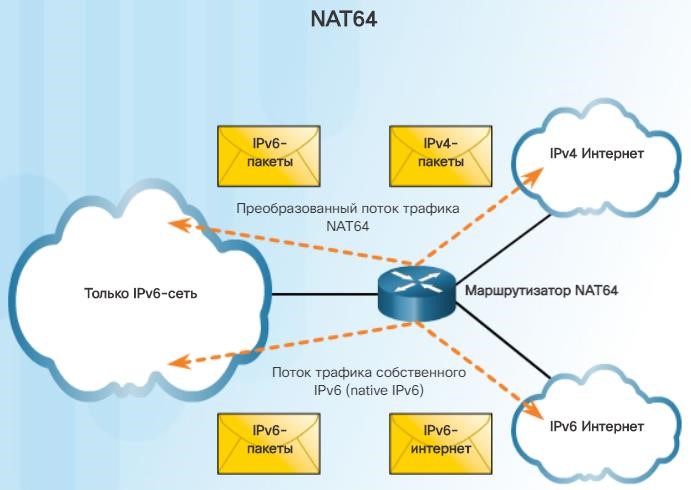
### 2.5.3 Протокол NAT для IPv6

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 IPv6адресов в глобальные IPv6-адреса.

В идеале, IPv6 должен по возможности использоваться в чистом виде. То есть когда устройства IPv6 взаимодействуют друг с другом по сетям IPv6. Организация IETF разработала несколько методов перехода для различных сценариев перехода от IPv4 к IPv6, включая использование двойного стека, туннелирование и трансляцию адресов.

Двойной стек применяется, когда устройства запускают набор протоколов и для IPv4, и для IPv6. Туннелирование для IPv6 — это процесс инкапсуляции пакетов IPv6 в пакеты IPv4. Данный метод позволяет передавать пакет IPv6 по сети, в которой используется только протокол IPv4.

NAT для IPv6 следует использовать не как долгосрочную стратегию, а лишь как временный механизм, помогающий перейти с IPv4 на IPv6. Со временем появилось несколько типов NAT для IPv6, включая NAT-PT (Network Address Translation-Protocol Translation, преобразование сетевых адресов — преобразование протоколов). Организация IETF признала технологию NAT-PT устаревшей и порекомендовала использовать ее замену — NAT64. NAT64 не рассматривается в рамках настоящего учебного курса.



# 3 Поиск и устранение неполадок NAT

## 3.1 Команды поиска и устранения неполадок, связанных с NAT

### 3.1.1 Команды " show ip nat"

На рис. 1 показан маршрутизатор R2 с включенной поддержкой PAT, использующий диапазон адресов от 20165.200.226 до 20165.200.240.

Если в среде NAT возникают проблемы подключения IPv4, поиск причин неполадок часто оказывается сложной задачей. Первое действие при устранении проблемы — исключить NAT как причину. Выполните следующие действия, чтобы убедиться, что NAT работает должным образом.

**Шаг 1.** В зависимости от конфигурации четко определите цели и задачи NAT. На данном этапе можно выявить проблему с настройкой.

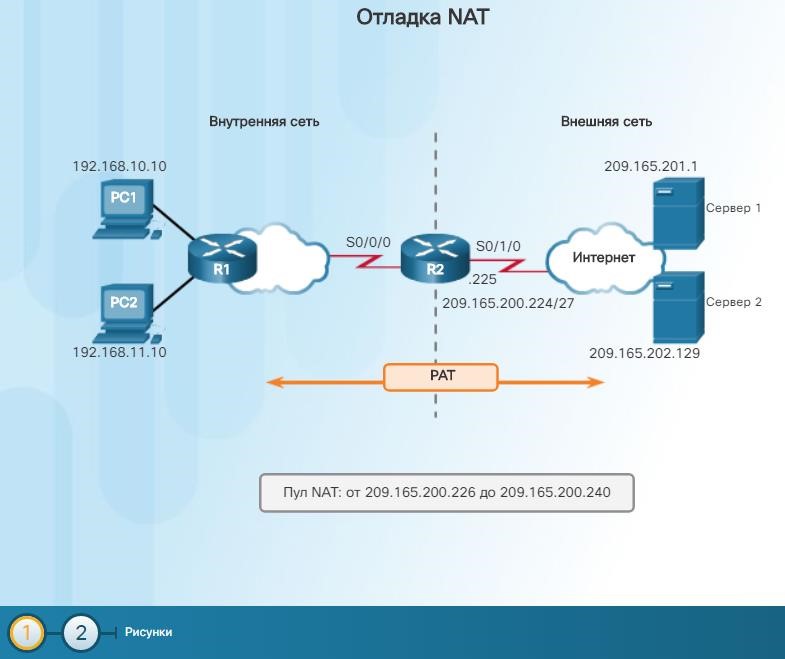
**Шаг 2.** С помощью команды **show ip nat translations** убедитесь, что таблица преобразований содержит правильные преобразования.

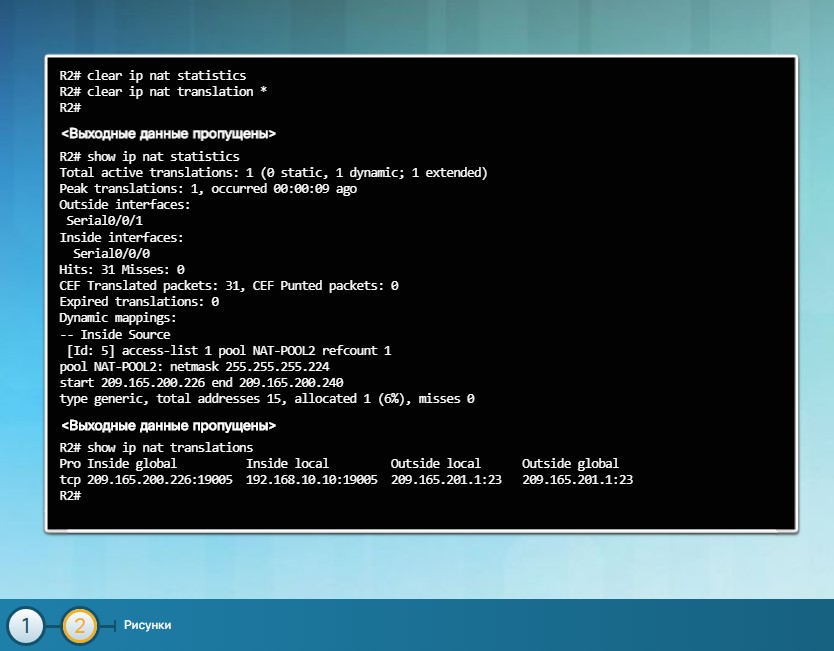
**Шаг 3.** Используйте команды **clear** и **debug**, чтобы убедиться, что NAT работает должным образом. Проверьте, создаются ли динамические записи снова после их удаления.

**Шаг 4.** Подробно изучите, что происходит с преобразованным пакетом, и убедитесь, что маршрутизаторы используют правильные данные маршрутизации для передачи пакета.

На рис. 2 показаны результаты выполнения команд **show ip nat statistics** и **show ip nat translations**. Перед использованием команд **show** статистика и записи NAT в таблице NAT удаляются с помощью команд **clear ip nat statistics** и **clear ip nat translation \***. После того, как узел 192.168.10.10 обратится к серверу в 20165.201.1 по протоколу telnet, будут отображены статистика NAT и таблица NAT, которые также помогают убедиться в корректной работе NAT.

В простой сети может быть целесообразно отслеживать статистику NAT с помощью команды **show ip nat statistics**. С помощью команды **show ip nat statistics** отображаются сведения об общем количестве активных преобразований, параметрах настройки NAT, количестве адресов в пуле и количестве выделенных адресов. Однако в более сложной среде NAT, в случае нескольких преобразований, эта команда не позволяет четко определить проблему. В подобных случаях может потребоваться выполнить команду **debug** на маршрутизаторе.





### 3.1.2 Команда " debug ip nat"

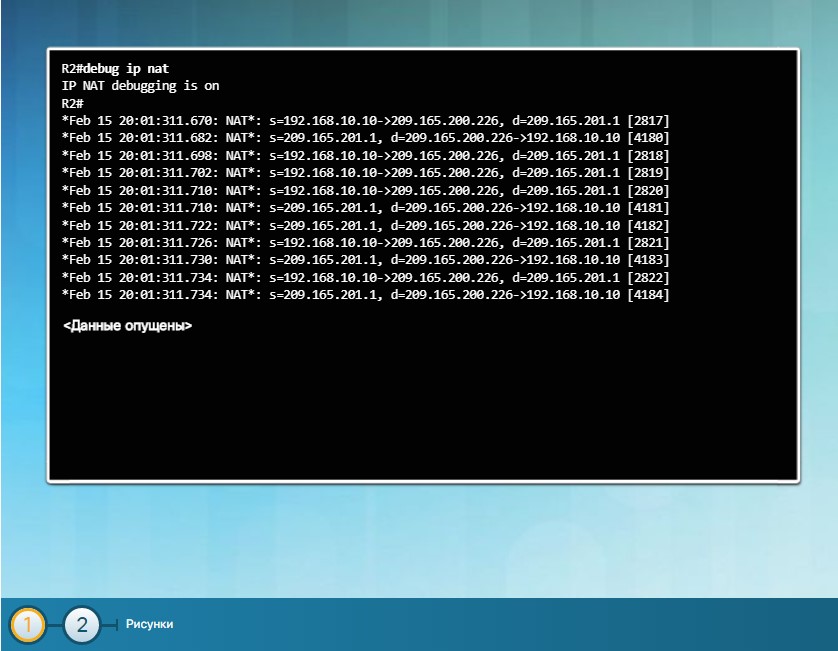
Используйте команду **debug ip nat** для проверки работы NAT путем вывода сведений о каждом пакете, преобразованном маршрутизатором. Команда **debug ip nat detailed** выводит описание каждого пакета, рассматриваемого в качестве кандидата на преобразование. Кроме того, эта команда выводит сведения о конкретных ошибках и исключениях, таких как невозможность выделить глобальный адрес. Команда **debug ip nat detailed** выдает больше служебных данных, чем команда **debug ip nat**, но она может предоставить подробные сведения, которые могут быть необходимы для отладки NAT. Устранив неполадки, всегда отключайте режим отладки.

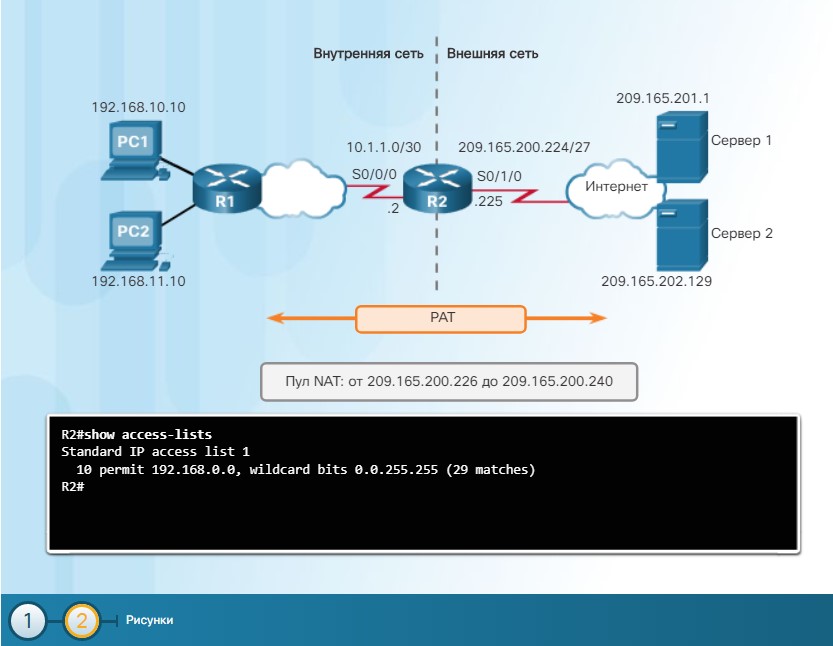
На рис. 1 показан результат выполнения **debug ip nat**. Результат показывает, что внутренний узел (192.168.10.10) создал трафик к внешнему узлу (20165.201.1), и адрес источника был преобразован в адрес 20165.200.226.

При расшифровке результатов отладки учитывайте значение перечисленных ниже символов:

* **\* (звездочка)** — символ звездочки рядом с NAT показывает, что преобразование выполняется по пути с быстрой коммутацией. Коммутация первого пакета диалога всегда является программным процессом и поэтому выполняется медленнее. Оставшиеся пакеты проходят по пути с быстрой коммутацией если существует запись кэша.
* **s=** — этот символ обозначает IPv4-адрес источника.
* **a.b.c.d**--->**w.x.y.z** — это значение показывает, что адрес источника a.b.c.d преобразуется в w.x.y.z.
* **d=** — этот символ обозначает IPv4-адрес назначения.
* **[xxxx]** — значение в скобках является идентификационным номером IPv4. Приведенная выше информация может быть полезна для отладки, так как она позволяет осуществить корреляцию с другими данными трассировки от анализаторов протоколов.

**Примечание.** Убедитесь, что список контроля доступа (ACL), указанный в команде для настройки NAT, разрешает все необходимые сети. На рис. 2 преобразование разрешается только для адресов 192.168.0.0/16. Маршрутизатор R2 не выполняет преобразование для пакетов из внутренней сети, адресованных в Интернет, если адреса их источников прямо не разрешены ACL-списком 1.





### 3.1.3 Сценарий поиска и устранения неполадок, связанных с NAT

#### Пример внедрения

На рис. 1 показано, что узлы локальной сети 192.168.0.0/16, ПК 1 и ПК 2 не могут отправлять эхо-запросы ping к серверам во внешних сетях, Сервер 1 и Сервер 2.

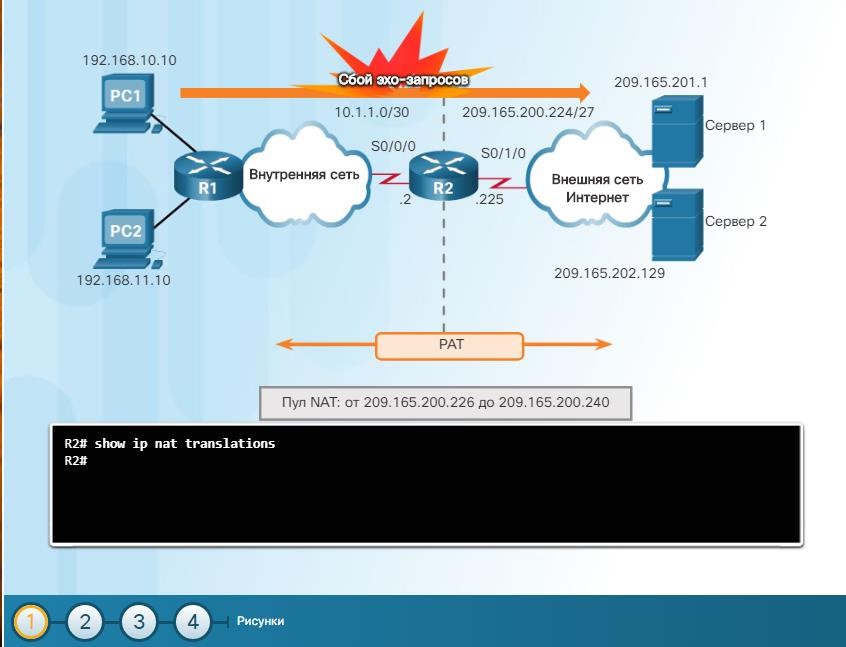
Чтобы приступить к устранению этой проблемы, используйте команду **show ip nat translations**, позволяющую определить, содержатся ли в таблице NAT записи преобразования. Результат на рис. 1 показывает, что преобразования в таблице отсутствуют.

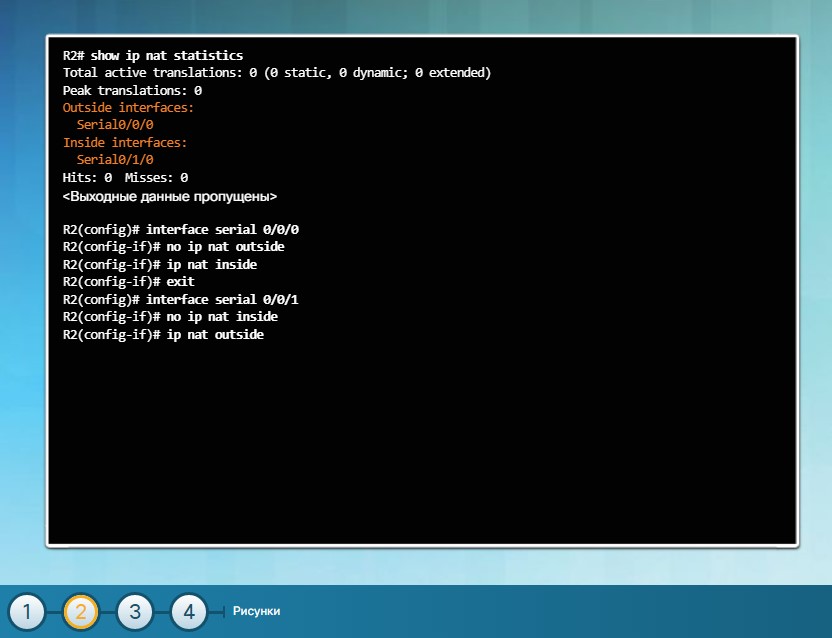
Чтобы определить, выполнялись ли какие-либо преобразования, используется команда **show ip nat statistics**. Данная команда также определяет интерфейсы, между которыми должно выполняться преобразование. В выходных данных, приведенных на рис. 2, счетчики NAT равны 0, что говорит о том, что преобразование не выполнялось. Сравнивая выходные данные с топологией на рис. 1, обратите внимание, что интерфейсы маршрутизатора NAT неправильно определены как внутренние и внешние относительно NAT. Неправильность настройки также можно проверить с помощью команды **show running-config**.

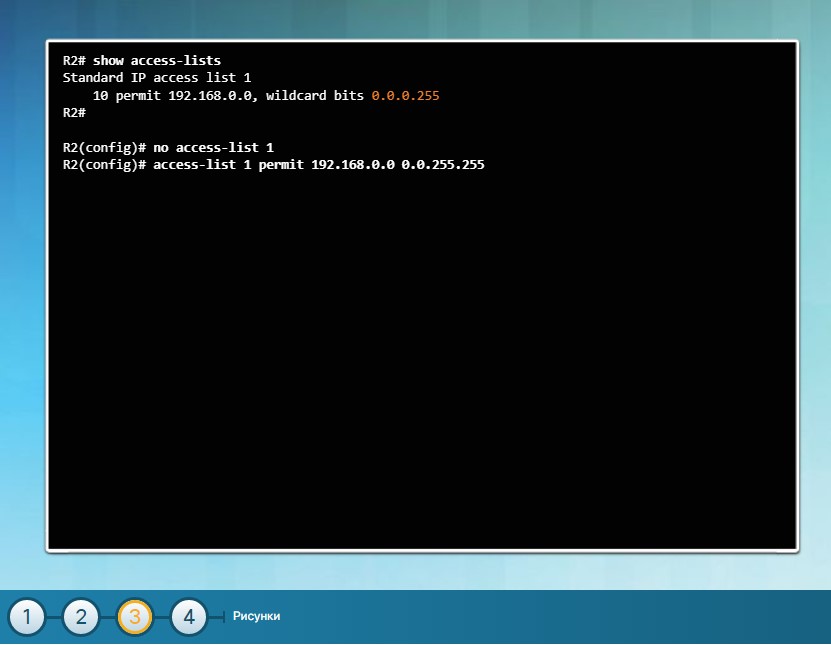
Перед применением правильной настройки необходимо удалить текущую настройку интерфейсов NAT.

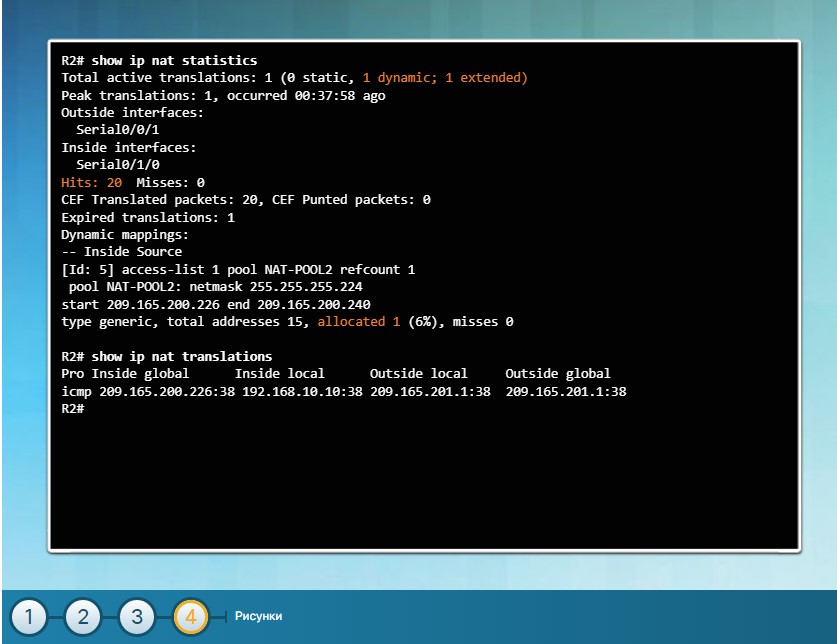
После правильного определения внутренних и внешних интерфейсов NAT отправка еще одного эхо-запроса ping от ПК 1 на Сервер 1 заканчивается неудачей. С помощью команд **show ip nat translations** и **show ip nat statistics** еще раз убедитесь, что преобразование все еще не выполняется.

На рис. 3 используется команда **show access-lists**, позволяющая определить, разрешает ли ACL-список, указываемый в командах NAT, все необходимые сети. Изучение выходных данных команды показывает, что в ACL, определяющем адреса для преобразования, использована неправильная шаблонная маска. Шаблонная маска разрешает использование только подсети 192.168.0.0/24. Список контроля доступа нужно сначала удалить, а затем настроить заново, используя правильную шаблонную маску. После исправления настроек с ПК 1 на Сервер 1 отправляется еще один эхо-запрос, и в этот раз запрос выполняется успешно. Как показано на рис. 4, чтобы убедиться в выполнении преобразования NAT, используются команды **show ip nat translations** и **show ip nat statistics**.









### 3.1.4 Packet Tracer. Проверка и отладка настроек NAT

Подрядчик восстановил старую настройку на новом маршрутизаторе с работающим преобразованием NAT. Однако после создания резервной копии старой настройки сеть изменилась, и в нее была добавлена новая подсеть. Ваша задача — восстановить работу сети.

[Практическая работа NAT-8. Проверка и отладка настроек NAT. Инструкции](files/Практическая%20работа%20NAT-8.%20Проверка%20и%20отладка%20настроек%20NAT.docx)

[Packet Tracer NAT-8. Проверка и отладка настроек NAT. РКА](files/Практическая%20работа%20NAT-8.%20Проверка%20и%20отладка%20настроек%20NAT.pka)

### 3.1.5 Лабораторная работа. Отладка настроек NAT

**В этой лабораторной работе вы выполните следующие задачи:**

* Часть 1. Создание сети и настройка основных параметров устройства
* Часть 2. Отладка статического преобразования (NAT)
* Часть 3. Отладка динамического преобразования NAT

[Лабораторная работа NAT-9. Отладка настроек NAT](files/Лабораторная%20работа%20NAT-9.%20Отладка%20настроек%20NAT.docx)

# 4 Обзор

## 4.1 Заключение

### 4.1.1 Проверка NAT

**Проверка NAT**

#### Сценарий

В схеме сети вашей компании в данный момент преобразование не используется. Принято решение настроить на некоторых устройствах использование служб NAT для подключения к почтовому серверу.

Прежде чем разворачивать NAT в действующей сети, создается прототип NAT с использованием программы-симулятора.

Дополнительные инструкции см. в PDF-файле, прилагаемом к заданию.

[Лабораторная работа NAT-10. Проверка NAT. Инструкции](files/Лабораторная%20работа%20NAT-10.%20Проверка%20NAT.docx)

### 4.1.2 Packet Tracer. Отработка комплексных практических навыков

#### Сценарий

Данное заключительное упражнение поможет отработать многие навыки, полученные в процессе освоения учебного материала. Во-первых, нужно выполнить документирование сети. Убедитесь, что у вас имеется распечатанный вариант инструкций. На этапе реализации вы будете настраивать на коммутаторе виртуальные сети VLAN, транки, защиту портов и удаленный доступ по протоколу SSH. Затем вы реализуете на маршрутизаторе маршрутизацию между сетями VLAN и преобразование NAT. Наконец, опираясь на документацию, вы проведете проверку этой маршрутизации путем тестирования связи между конечными устройствами.

[Практическая работа NAT-11. Отработка комплексных практических навыков (инструкции)](files/Практическая%20работа%20NAT-11_Отработка%20комплексных%20практических%20навыков.docx)

[Packet Tracer NAT-11. Отработка комплексных практических навыков (PKA)](files/Практическая%20работа%20NAT-11_Отработка%20комплексных%20практических%20навыков.pka)

### 4.1.3 NAT для IPv4

В материале данной главы рассматривается использование NAT для смягчения исчерпания адресного пространства IPv4. NAT для IPv4 позволяет сетевым администраторам использовать пространство частных адресов RFC 1918, одновременно предоставляя подключение к Интернету с использованием одного публичного адреса или ограниченного числа публичных адресов.

NAT экономит пространство публичных адресов и значительно сокращает административные издержки при добавлении, перемещении и смене адресов. NAT и PAT могут использоваться для экономии пространства общедоступных адресов, не влияя на подключения к сети интернет-провайдера. Однако NAT имеет определенные недостатки — данная технология отрицательно влияет на производительность, мобильность устройств, а также на возможность сквозного соединения. Поэтому NAT следует использовать в качестве кратковременного решения проблемы исчерпания адресов до внедрения долговременного решения, которым является IPv6.

В главе рассмотрено использование преобразования (NAT) для протокола IPv4, а именно:

* характеристики, терминология и общие принципы работы NAT;
* различные типы NAT, включая статический NAT, динамический NAT и NAT с перегрузкой;
* преимущества и недостатки NAT;
* настройка, проверка и анализ статического NAT, динамического NAT и NAT с перегрузкой;
* использование перенаправления портов для доступа к внутренним устройствам из сети Интернет;
* почему преобразование NAT доступно, но не интегрировано в сетях IPv6;
* отладка NAT с помощью команд **show** и **debug**.