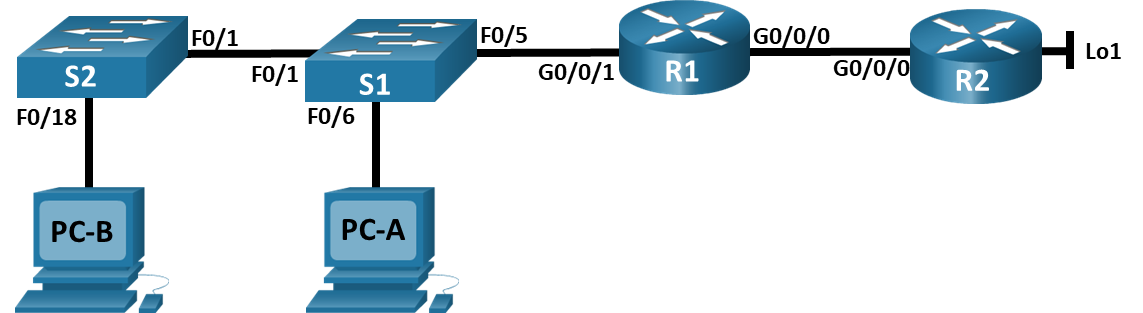
Лабораторная работа - Настройка NAT для IPv4

# Топология



# Таблица адресации

|  |  |  |  |
| --- | --- | --- | --- |
| Устройство | Интерфейс | IP-адрес | Маска подсети |
| R1 | G0/0/0 | 209.165.200.230 | 255.255.255.248 |
| R1 | G0/0/1 | 192.168.1.1 | 255.255.255.0 |
| R2 | G0/0/0 | 209.165.200.225 | 255.255.255.248 |
| R2 | Lo1 | 209.165.200.1 | 255.255.255.224 |
| S1 | VLAN 1 | 192.168.1.11 | 255.255.255.0 |
| S2 | VLAN 1 | 192.168.1.12 | 255.255.255.0 |
| PC-A | NIC | 192.168.1.2 | 255.255.255.0 |
| PC-B | NIC | 192.168.1.3 | 255.255.255.0 |

# Цели

Часть 1. Создание сети и настройка основных параметров устройства

Часть 2. Настройка и проверка NAT для IPv4

Часть 3. Настройка и проверка PAT для IPv4

Часть 4. Настройка и проверка статического NAT для IPv4.

# Общие сведения/сценарий

Преобразование (NAT) — это процесс, при котором сетевое устройство, например маршрутизатор Cisco, назначает публичный адрес узлам в пределах частной сети. NAT используют для сокращения количества публичных IP-адресов, используемых организацией, поскольку количество доступных публичных IPv4-адресов ограничено.

Интернет-провайдер выделил компании общедоступное пространство IP-адресов 209.165.200.224/29. Эта сеть используется для обращения к каналу между маршрутизатором ISP (R2) и шлюзом компании (R1). Первый адрес (209.165.200.225) назначается интерфейсу g0/0 на R2, а последний адрес (209.165.200.230) назначается интерфейсу g0/0/0 на R1. Остальные адреса (209.165.200.226-209.165.200.229) будут использоваться для предоставления доступа в Интернет хостам компании. Маршрут по умолчанию используется от R1 до R2. Подключение интернет-провайдера к Интернету смоделировано loopback-адресом на маршрутизаторе интернет-провайдера.

В этой лабораторной работе вы будете настраивать различные типы NAT. Вы выполните тестирование, отображение и проверку осуществления всех преобразований и проанализируете статистику NAT/PAT для контроля процесса.

**Примечание**: Маршрутизаторы, используемые в практических лабораторных работах CCNA, - это Cisco 4221 с Cisco IOS XE Release 16.9.3 (образ universalk9). В лабораторных работах используются коммутаторы Cisco Catalyst 2960 с Cisco IOS версии 15.2(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и результаты их выполнения могут отличаться от тех, которые показаны в лабораторных работах. Правильные идентификаторы интерфейса см. в сводной таблице по интерфейсам маршрутизаторов в конце лабораторной работы.

**Примечание.** Убедитесь, что у всех маршрутизаторов и коммутаторов была удалена начальная конфигурация. Если вы не уверены в этом, обратитесь к инструктору.

# Необходимые ресурсы

* 2 маршрутизатора (Cisco 4221 с универсальным образом Cisco IOS XE версии 16.9.4 или аналогичным)
* 2 коммутатора (Cisco 2960 с операционной системой Cisco IOS 15.2(2) (образ lanbasek9) или аналогичная модель)
* 2 ПК (ОС Windows с программой эмуляции терминалов, такой как Tera Term)
* Консольные кабели для настройки устройств Cisco IOS через консольные порты.
* Кабели Ethernet, расположенные в соответствии с топологией

# Инструкции

## Создание сети и настройка основных параметров устройства

В первой части лабораторной работы вам предстоит создать топологию сети и настроить базовые параметры для узлов ПК и коммутаторов.

### Подключите кабели сети согласно приведенной топологии.

Подключите устройства в соответствии с топологией и подсоедините соответствующие кабели.

### Произведите базовую настройку маршрутизаторов.

Откройте окно конфигурации

* + - 1. Назначьте маршрутизатору имя устройства.
      2. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
      3. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
      4. Назначьте **cisco** в качестве пароля консоли и включите вход в систему по паролю.
      5. Назначьте **cisco** в качестве пароля VTY и включите вход в систему по паролю.
      6. Зашифруйте открытые пароли.
      7. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.
      8. Настройте IP-адресации интерфейса, как указано в таблице выше.
      9. Настройте маршрут по умолчанию. от R2 до R1.
      10. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Закройте окно настройки.

### Настройте базовые параметры каждого коммутатора.

Откройте окно конфигурации

* + - 1. Присвойте коммутатору имя устройства.
      2. Отключите поиск DNS, чтобы предотвратить попытки маршрутизатора неверно преобразовывать введенные команды таким образом, как будто они являются именами узлов.
      3. Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
      4. Назначьте **cisco** в качестве пароля консоли и включите вход в систему по паролю.
      5. Назначьте **cisco** в качестве пароля VTY и включите вход в систему по паролю.
      6. Зашифруйте открытые пароли.
      7. Создайте баннер с предупреждением о запрете несанкционированного доступа к устройству.
      8. Выключите все интерфейсы, которые не будут использоваться.
      9. Настройте IP-адресации интерфейса, как указано в таблице выше.
      10. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Закройте окно настройки.

## Настройка и проверка NAT для IPv4.

В части 2 необходимо настроить и проверить NAT для IPv4.

### Настройте NAT на R1, используя пул из трех адресов 209.165.200.226-209.165.200.228.

Откройте окно конфигурации

* + - 1. Настройте простой список доступа, который определяет, какие хосты будут разрешены для трансляции. В этом случае все устройства в локальной сети R1 имеют право на трансляцию.

R1(config)# **access-list 1 permit 192.168.1.0 0.0.0.255**

* + - 1. Создайте пул NAT и укажите ему имя и диапазон используемых адресов.

R1(config)# **ip nat pool PUBLIC\_ACCESS 209.165.200.226 209.165.200.228 netmask 255.255.255.248**

**Примечание.** Параметр маски сети не является разделителем IP-адресов. Это должна быть правильная маска подсети для назначенных адресов, даже если вы используете не все адреса подсети в пуле.

* + - 1. Настройте перевод, связывая ACL и пул с процессом преобразования.

R1(config)# **ip nat inside source list 1 pool PUBLIC\_ACCESS**

**Примечание**: Три очень важных момента. Во-первых, слово «inside» имеет решающее значение для работы такого рода NAT. Если вы опустить его, NAT не будет работать. Во-вторых, номер списка — это номер ACL, настроенный на предыдущем шаге. В-третьих, имя пула чувствительно к регистру.

* + - 1. Задайте внутренний (inside) интерфейс.

R1(config)# **interface g0/0/1**

R1(config-if)# **ip nat inside**

* + - 1. Определите внешний (outside) интерфейс.

R1(config)# **interface g0/0/0**

R1(config-if)# **ip nat outside**

### Проверьте и проверьте конфигурацию.

* + - 1. С PC-B, запустите эхо-запрос интерфейса Lo1 (209.165.200.1) на R2. Если эхо-запрос не прошел, выполните процес поиска и устранения неполадок. На R1 отобразите таблицу NAT на R1 с помощью команды **show ip nat translations**.

R1# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

--- 209.165.200.226 192.168.1.3 --- ---

226:1 192.168.1. 3:1 209.165.200. 1:1 209.165.200. 1:1

Total number of translations: 2

#### Вопросы:

Во что был транслирован внутренний локальный адрес PC-B?

Введите ваш ответ здесь.

Какой тип адреса NAT является переведенным адресом?

* + - 1. С PC-A, запустите эхо-запрос интерфейса Lo1 (**209.165.200.1**) на R2. Если эхо-запрос не прошел, выполните отладку. На R1 отобразите таблицу NAT на R1 с помощью команды **show ip nat translations**.

R1# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

--- 209.165.200.227 192.168.1.2 --- ---

--- 209.165.200.226 192.168.1.3 --- ---

227:1 192.168.1. 2:1 209.165.200. 1:1 209.165.200. 1:1

226:1 192.168.1. 3:1 209.165.200. 1:1 209.165.200. 1:1

Total number of translations: 4

* + - 1. Обратите внимание, что предыдущая трансляция для PC-B все еще находится в таблице. Из S1, эхо-запрос интерфейса Lo1 (**209.165.200.1**) на R2. Если эхо-запрос не прошел, выполните отладку. На R1 отобразите таблицу NAT на R1 с помощью команды **show ip nat translations**.

R1# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

--- 209.165.200.227 192.168.1.2 --- ---

--- 209.165.200.226 192.168.1.3 --- ---

--- 209.165.200.228 192.168.1.11 --- ---

226:1 192.168.1. 3:1 209.165.200. 1:1 209.165.200. 1:1

228:0 192.168.1. 11:0 209.165.200. 1:0 209.165.200. 1:0 209.165.200. 1:0

Total number of translations: 5

* + - 1. Теперь запускаем пинг R2 Lo1 из S2. На этот раз перевод завершается неудачей, и вы получаете эти сообщения (или аналогичные) на консоли R1:

Sep 23 15:43:55.562: %IOSXE-6-PLATFORM: R0/0: cpp\_cp: QFP:0.0 Thread:000 TS:00000001473688385900 %NAT-6-ADDR\_ALLOC\_FAILURE: Address allocation failed; pool 1 may be exhausted [2]

* + - 1. Это ожидаемый результат, потому что выделено только 3 адреса, и мы попытались ping Lo1 с четырех устройств. Напомним, что NAT — это трансляция «один-в-один». Как много выделено трансляций? Введите команду **show ip nat translations verbose** , и вы увидите, что ответ будет 24 часа.

R1# **show ip nat translations verbose**

Pro Inside global Inside local Outside local Outside global

--- 209.165.200.226 192.168.1.3 --- ---

create: 09/23/19 15:35:27, use: 09/23/19 15:35:27, timeout: 23:56:42

Map-Id(In): 1

<output omitted>

* + - 1. Учитывая, что пул ограничен тремя адресами, NAT для пула адресов недостаточно для нашего приложения. Очистите преобразование NAT и статистику, и мы перейдем к PAT.

R1# **clear ip nat translations \***

R1# **clear ip nat statistics**

Закройте окно настройки.

## Настройка и проверка PAT для IPv4.

В части 3 необходимо настроить замену NAT на PAT в пул адресов, а затем на PAT с помощью интерфейса.

### Удалите команду преобразования на R1.

Откройте окно конфигурации

Компоненты конфигурации преобразования адресов в основном одинаковы; что-то (список доступа) для идентификации адресов, пригодных для перевода, дополнительно настроенный пул адресов для их преобразования и команды, необходимые для идентификации внутреннего и внешнего интерфейсов. Из части 1 наш список доступа (список доступа 1) по-прежнему корректен для сетевого сценария, поэтому нет необходимости воссоздавать его. Мы будем использовать один и тот же пул адресов, поэтому нет необходимости воссоздавать эту конфигурацию. Кроме того, внутренний и внешний интерфейсы не меняются. Чтобы начать работу в части 3, удалите команду, связывающую ACL и пул вместе.

R1(config)# **no ip nat inside source list 1 pool PUBLIC\_ACCESS**

### Добавьте команду PAT на R1.

Теперь настройте преобразование PAT в пул адресов (помните, что ACL и Pool уже настроены, так что это единственная команда, которую нам нужно изменить с NAT на PAT).

R1(config)# **ip nat inside source list 1 pool PUBLIC\_ACCESS overload**

### Протестируйте и проверьте конфигурацию.

* + - 1. Давайте проверим, что PAT работает. С PC-B, запустите эхо-запрос интерфейса Lo1 (209.165.200.1) на R2. Если эхо-запрос не прошел, выполните отладку. На R1 отобразите таблицу NAT на R1 с помощью команды **show ip nat translations**.

R1# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

226:1 192.168.1. 3:1 209.165.200. 1:1 209.165.200. 1:1

Total number of translations: 1#

#### Вопросы:

Во что был транслирован внутренний локальный адрес PC-B?

Какой тип адреса NAT является переведенным адресом?

Чем отличаются выходные данные команды **show ip nat translations** из упражнения NAT?

Введите ваш ответ здесь.

* + - 1. С PC-A, запустите эхо-запрос интерфейса Lo1 (209.165.200.1) на R2. Если эхо-запрос не прошел, выполните отладку. На R1 отобразите таблицу NAT на R1 с помощью команды **show ip nat translations**.

R1# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

226:1 192.168.1. 2:1 209.165.200. 1:1 209.165.200. 1:1

Total number of translations: 1

Обратите внимание, что есть только одна трансляция. Отправьте ping еще раз, и быстро вернитесь к маршрутизатору и введите команду **show ip nat translations verbose** , и вы увидите, что произошло.

R1# **show ip nat translations verbose**

Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.226:1 192.168.1.2:1 209.165.200.1:1 209.165.200.1:1

create: 09/23/19 16:57:22, use: 09/23/19 16:57:25, timeout: 00:01:00

<output omitted>

Как вы можете видеть, время ожидания перевода было отменено с 24 часов до 1 минуты.

* + - 1. Генерирует трафик с нескольких устройств для наблюдения PAT. На PC-A и PC-B используйте параметр -t с командой ping, чтобы отправить безостановочный ping на интерфейс Lo1 R2 (**ping -t 209.165.200.1**), затем вернитесь к R1 и выполните команду **show ip nat translations**:

R1# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.226:1 192.168.1.2:1 209.165.200.1:1 209.165.200.1:1

226:2 192.168.1. 3:1 209.165.200. 1:1 209.165.200. 1:2

Total number of translations: 2

Обратите внимание, что внутренний глобальный адрес одинаков для обоих сеансов.

#### Вопрос:

Как маршрутизатор отслеживает, куда идут ответы?

* + - 1. PAT в пул является очень эффективным решением для малых и средних организаций. Тем не менее есть неиспользуемые адреса IPv4, задействованные в этом сценарии. Мы перейдем к PAT с перегрузкой интерфейса, чтобы устранить эту трату IPv4 адресов. Остановите ping на PC-A и PC-B с помощью комбинации клавиш Control-C, затем очистите трансляции и статистику:

R1# **clear ip nat translations \***

R1# **clear ip nat statistics**

### На R1 удалите команды преобразования nat pool.

Опять же, наш список доступа (список доступа 1) по-прежнему корректен для сетевого сценария, поэтому нет необходимости воссоздавать его. Кроме того, внутренний и внешний интерфейсы не меняются. Чтобы начать работу с PAT к интерфейсу, очистите конфигурацию, удалив пул NAT и команду, связывающую ACL и пул вместе.

R1(config)# **no ip nat inside source list 1 pool PUBLIC\_ACCESS overload**

R1(config)# **no ip nat pool PUBLIC\_ACCESS**

### Добавьте команду PAT overload, указав внешний интерфейс.

Добавьте команду PAT, которая вызовет перегрузку внешнего интерфейса.

R1(config)# **ip nat inside source list 1 interface g0/0/0 overload**

### Протестируйте и проверьте конфигурацию.

* + - 1. Давайте проверим PAT, чтобы интерфейс работал. С PC-B, запустите эхо-запрос интерфейса Lo1 (209.165.200.1) на R2. Если эхо-запрос не прошел, выполните отладку. На R1 отобразите таблицу NAT на R1 с помощью команды **show ip nat translations**.

R1# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

209.165.200. 230:1 192.168.1. 3:1 209.165.200. 1:1 209.165.200. 1:1

Total number of translations: 1

* + - 1. Сделайте трафик с нескольких устройств для наблюдения PAT. На PC-A и PC-B используйте параметр -t с командой ping для отправки безостановочного ping на интерфейс Lo1 R2 **(ping -t 209.165.200.1**). На S1 и S2 выполните привилегированную команду exec ping 209.165.200.1 повторить 2000. Затем вернитесь к R1 и выполните команду **show ip nat translations**.

R1# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

209.165.200. 230:3 192.168.1. 11:1 209.165.200. 1:1 209.165.200. 1:3

209.165.200. 230:2 192.168.1. 2:1 209.165.200. 1:1 209.165.200. 1:2

209.165.200. 230:4 192.168.1. 3:1 209.165.200. 1:1 209.165.200. 1:4

209.165.200. 230:1 192.168.1. 12:1 209.165.200. 1:1 209.165.200. 1:1

Total number of translations: 4

Теперь все внутренние глобальные адреса сопоставляются с IP-адресом интерфейса g0/0/0.

Остановите все пинги. На PC-A и PC-B, используя комбинацию клавиш CTRL-C.

Закройте окно настройки.

## Настройка и проверка статического NAT для IPv4.

В части 4 будет настроена статическая NAT таким образом, чтобы PC-A был доступен напрямую из Интернета. PC-A будет доступен из R2 по адресу 209.165.200.229.

**Примечание.** Конфигурация, которую вы собираетесь завершить, не соответствует рекомендуемым практикам для шлюзов, подключенных к Интернету. Эта лаборатория полностью опускает стандартные методы безопасности, чтобы сосредоточиться на успешной конфигурации статического NAT. В производственной среде решающее значение для удовлетворения этого требования будет иметь тщательная координация между сетевой инфраструктурой и группами безопасности.

### На R1 очистите текущие трансляции и статистику.

Откройте окно конфигурации

R1# **clear ip nat translations \***

R1# **clear ip nat statistics**

### На R1 настройте команду NAT, необходимую для статического сопоставления внутреннего адреса с внешним адресом.

Для этого шага настройте статическое сопоставление между 192.168.1.11 и 209.165.200.1 с помощью следующей команды:

R1(config)# **ip nat inside source static 192.168.1.2 209.165.200.229**

### Протестируйте и проверьте конфигурацию.

* + - 1. Давайте проверим, что статический NAT работает. На R1 отобразите таблицу NAT на R1 с помощью команды **show ip nat translations**, и вы увидите статическое сопоставление.

R1# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

--- 209.165.200.229 192.168.1.2 --- ---

Total number of translations: 1

* + - 1. Таблица перевода показывает, что статическое преобразование действует. Проверьте это, запустив ping с R2 на 209.165.200.229. Плинги должны работать.

Примечание. Возможно, вам придется отключить брандмауэр ПК для работы pings.

* + - 1. На R1 отобразите таблицу NAT на R1 с помощью команды **show ip nat translations**, и вы увидите статическое сопоставление и преобразование на уровне порта для входящих pings.

R1# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

--- 209.165.200.229 192.168.1.2 --- ---

229:3 192.168.1. 2:3 209.165.200. 225:3 209.165.200. 225:3 209.165.200.

Total number of translations: 2

Это подтверждает, что статический NAT работает.

Закройте окно настройки.

# Сводная таблица по интерфейсам маршрутизаторов

| Модель маршрутизатора | Интерфейс Ethernet № 1 | Интерфейс Ethernet № 2 | Последовательный интерфейс № 1 | Последовательный интерфейс № 2 |
| --- | --- | --- | --- | --- |
| 1 800 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 1900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2801 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 4221 | Gigabit Ethernet 0/0/0 (G0/0/0) | Gigabit Ethernet 0/0/1 (G0/0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 4300 | Gigabit Ethernet 0/0/0 (G0/0/0) | Gigabit Ethernet 0/0/1 (G0/0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |

**Примечание**. Чтобы определить конфигурацию маршрутизатора, можно посмотреть на интерфейсы и установить тип маршрутизатора и количество его интерфейсов. Перечислить все комбинации конфигураций для каждого класса маршрутизаторов невозможно. Эта таблица содержит идентификаторы для возможных комбинаций интерфейсов Ethernet и последовательных интерфейсов на устройстве. Другие типы интерфейсов в таблице не представлены, хотя они могут присутствовать в данном конкретном маршрутизаторе. В качестве примера можно привести интерфейс ISDN BRI. Строка в скобках — это официальное сокращение, которое можно использовать в командах Cisco IOS для обозначения интерфейса.

Конец документа