Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное
учреждение высшего профессионального образования
«Севастопольский государственный университет»

ИССЛЕДОВАНИЕ СПОСОБОВ ТРАНСЛЯЦИИ СЕТЕВЫХ АДРЕСОВ

Методические указания

к выполнению лабораторной работы
по дисциплине **«Инфокоммуникационные системы и сети»**
Для студентов, обучающихся по направлению 09.03.02
«Информационные системы и технологии»
И 09.03.03 «Прикладная информатика»
по учебному плану подготовки бакалавров
дневной и заочной форм обучения

Севастополь
2021

УДК 004.732

Исследование способов трансляции сетевых адресов. Методические указания к лабораторным занятиям по дисциплине «Инфокоммуникационные системы и сети» / Сост. В.С. Чернега – Севастополь: Изд-во СевГУ, 2021 – 17 с.

Методические указания предназначены для проведения лабораторных работ по дисциплине «Инфокоммуникационные системы и сети». Целью методических указаний является помощь студентам в изучении способов преобразования частных сетевых адресов в публичные. Излагаются теоретические и практические сведения необходимые для выполнения лабораторной работы, требования к содержанию отчета.

Методические указания рассмотрены и утверждены на методическом семинаре и заседании кафедры информационных систем
(протокол № ____ от «_____» _____ 2021 г.)

Рецензент: Моисеев Д.В., д-р. техн. наук, профессор кафедры ИТиКС

Лабораторная работа

Исследование способов трансляции сетевых адресов

1 Цель работы

Углубление теоретических знаний в области архитектуры компьютерных сетей и сетевых операционных систем, исследование способов трансляции сетевых адресов и приобретение навыков в построении и исследовании связи локальных сетей с глобальной средствами симулятора Cisco Packet Tracer.

2 Краткие теоретические сведения

Трансляция сетевых адресов NAT (Network Address Translation) предназначена для преобразования одних IP-адресов в другие, в частности замены внутренних частных адресов локальных сетей, которые не маршрутизируются в глобальной сети Internet, в глобальные (публичные) адреса. Это даёт возможность выхода в Internet для пользователей корпоративных локальных IP сетей, использующих частные IP адреса. NAT применяется также для связи территориально распределённых подразделений организации через Internet. Технология NAT дополнительно повышает безопасность сети, скрывая структуру внутренней сети, благодаря тому, что из внешней сети не видны внутренние IP-адреса ее пользователей.

Для внутренних сетей международным стандартом выделены частные адреса для использования их только во внутренних сетях. Для классов A, B и C выделены соответствующие частные адреса (Таблица 2.1).

Таблица 2.1 – Частные IPv.4-адреса сетей

Класс	Адреса		Маска сети	Число сетей
	Начальный	Конечный		
A	10.0.0.0	10.255.255.255	255.0.0.0	1
B	172.16.0.0	172.16.31.255	255.255.0.0	15
C	192.168.0.0	192.168.255.255	255.255.255.0	255

Преобразование адресов осуществляется маршрутизатором (NAT-Router), соединяющим внутреннюю локальную сеть организации с глобальной (внешней) сетью Internet (рисунок 2.1). Следует заметить, что основной задачей домашних маршрутизаторов является трансляция сетевых адресов, т.е преобразо-

вания частных адресов одного из компьютера домашней сети в публичный адрес, полученный от интернет-провайдера.

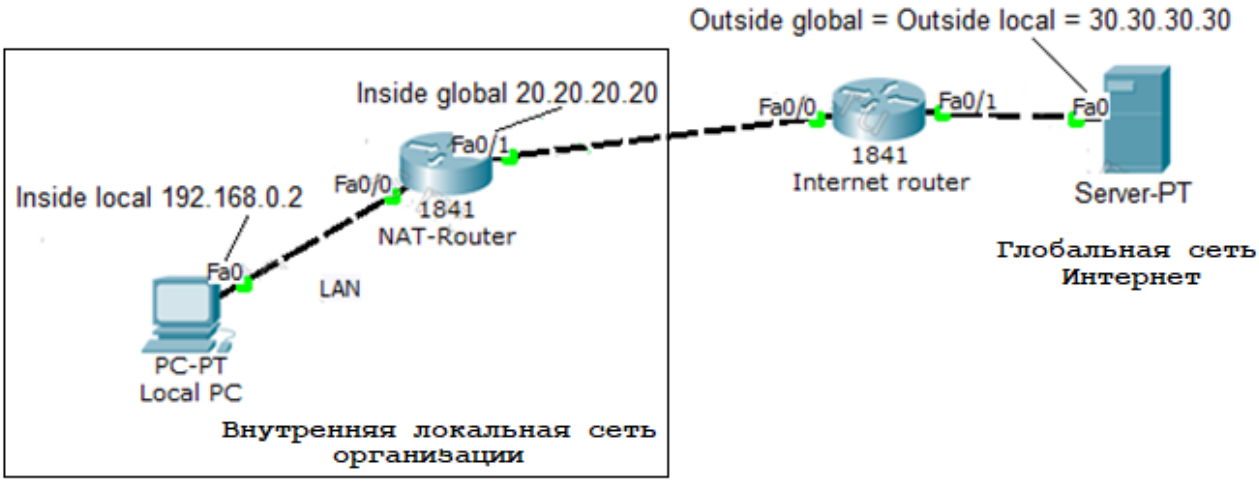

Рисунок 2.1– Общая схема трансляции адресов

Когда маршрутизатор, на котором активирована процедура NAT, получает пакет из внутренней сети, он изменяет в нём адрес источника, пересчитывает контрольную сумму и отправляет его в глобальную сеть Internet. При приёме ответного пакета модуль NAT заменяет в нём глобальный адрес собственного приёмника (адрес внешнего интерфейса локального маршрутизатора) на адрес интерфейса внутреннего хоста. Для такой замены маршрутизатор поддерживает специальные таблицы преобразований адресов, которые постоянно обновляются. Корпорацией Cisco в процедуре трансляции адресов введены четыре типа адресов.

1. **Внутренний** (**inside**) адрес – адрес компьютерной сети, используемый в организации. Разные организации могут иметь одинаковые внутренние адреса.
2. **Внешний**, по отношению к внутренней сети организации, адрес (**outside**). Под ним понимается адрес другой сети (либо сервера), принадлежащей иной организации. Этот внешний адрес может совпадать с внутренним адресом другой организации.
3. **Глобальный** адрес (**global**) – уникальный публичный IP адрес глобальной сети Internet.
4. **Локальный** адрес (**local**) – IP-адрес, используемый внутри локальной сети организации, называемой Intranet. Эти адреса не адресуются в сети Internet и поэтому могут использоваться лишь как локальные.

Исходя из этого деления адресов, различают следующую комбинацию рассмотренных типов адресов.

Внутренний локальный адрес (**inside local**) — частный адрес локальной сети организации, не воспринимаемый маршрутизатором глобальной сети Internet.

Внутренний глобальный адрес (**inside global**) — адрес, выделенный организации провайдером глобальной сети, являющийся публичным Internet-адресом.

Внешний локальный адрес (**outside local**) — частный адрес локальной сети другой организации (или сервера).

Внешний глобальный адрес (**outside global**) — публичный (глобальный) уникальный адрес другой организации, принадлежащий пространству Internet-адресов. Внешний глобальный адрес другой организации может совпадать с внутренним адресом данной организации (см. рисунок 2.2).

Следует отметить, что эмулятор Cisco packet Tracer всегда показывает, что внешний локальный адрес (outside local) всегда равен внешнему глобальному адресу (outside global).

Различают три способа трансляции адресов: *статический, динамический* и *перегрузка* (**overload**). При статическом NAT в явном виде с помощью команд IOS задаются пары «внутренний адрес – глобальный адрес». При динамическом преобразовании глобальные адреса берутся из определённого набора (пула) внешних адресов. При перегрузке все внутренние адреса, подлежащие преобразованию, заменяются на единственный глобальный адрес внешнего интерфейса маршрутизатора.

Для конфигурирования NAT следует указать маршрутизатору внутренние и внешние сети с помощью основных команд **`ip nat inside | outside`**. Эти команды определяются на уровне интерфейсов, то есть в строке команды **`interface`**. Дополнительные команды зависят от используемого типа NAT. Это либо задание статической NAT, либо определение пула внешних адресов, или задание команды для перегрузки. Кроме этого следует также задать список управления доступом ACL для определения внутреннего трафика, адреса которого будет транслироваться. Сам по себе ACL не осуществляет преобразования адресов.

Процесс NAT прозрачен для внутренних адресов. Так компьютер локальной сети с некоторым внутренним адресом, отправивший пакет во внешнюю сеть и получивший ответ «не догадывается», что пакет прошел NAT преобразование на маршрутизаторе, как при отправке, так и при приёме. Внутреннему хосту представляется, что он имеет непосредственный выход во внешний мир.

2.1 Конфигурация статической трансляции

Конфигурирование процедуры NAT при любом способе трансляции следует осуществлять в режиме глобальной конфигурации маршрутизатора!

При статической трансляции, как отмечалось выше, один внутренний адрес преобразуется в один внешний. При этом все запросы, приходящие из глобальной сети на внешний адрес маршрутизатора, будут транслироваться на компьютер (хост) внутренней сети. Словно бы данный хост и является обладателем этого публичного IP-адреса.

Для задания статической трансляции необходимо выполнить следующие действия:

1. Установить режим статической трансляции между внутренним локальным (частным) адресом и внутренним глобальным (публичным) адресом:

ip nat inside source static <локальный адрес> <глобальный адрес>

2. Указать внутренний интерфейс: **interface** <тип> <номер>

3. Пометить этот интерфейс, как принадлежащий внутренней сети: **ip nat** inside

5. Указать внешний интерфейс: interface <тип> <номер>

6. Пометить этот интерфейс, как принадлежащий внешней сети: **ip nat** outside

Использование статической трансляции целесообразно при наличии внутри сети сервера, к которому необходим полный доступ извне. Очевидно, этот вариант нельзя применять, если в Internet необходимо выпустить 2 и более хостов через один адрес.

2.2 Конфигурация динамической трансляции

Динамическая трансляция адресов применяется, если организации предоставлена группа (пул) публичных адресов, например, провайдер выделил сеть 198.51.100.0/28 с 16-ю адресами. Два из них (первый и последний) – адрес сети (0000) и широковещательный (1111), ещё два адреса назначаются на оборудование для обеспечения маршрутизации. 12 оставшихся адресов можно применять для процедуры NAT и использовать их для работы с Интернет остальным пользователям локальной сети. Ситуация похожа на статический способ NAT, когда один частный адрес преобразуется в один внешний, но теперь внешний адрес не жестко зафиксирован, а будет выбираться динамически из заданного диапазона (пула).

Для конфигурации динамической трансляции необходимо выполнить следующие действия:

1. Определить пул (диапазон) глобальных адресов:

Router(config)#**ip nat pool** <имя> <первый адрес> <последний адрес> [netmask <маска подсети> или prefix-length <длина префикса>]

Примечание: В дальнейшем для сокращения записи приглашение в режиме глобальной конфигурации Router(config)# не приводится.

2. Определить стандартный список доступа, регламентирующий адреса, подлежащие трансляции:

access-list <номер> permit <адрес или блок адресов>

3. Установить динамическую трансляцию на основе списка доступа, определенного на предыдущем шаге:

ip nat inside source list <номер списка доступа> pool <имя>

4. Указать внутренний интерфейс: **interface** <тип> <номер>

5. Пометить этот интерфейс, как принадлежащий внутренней сети: **ip nat** inside

6. Указать внешний интерфейс: **interface** <тип> <номер>

7. Пометить этот интерфейс, как принадлежащий внешней сети: **ip nat** outside

2.3 Использование одного внутреннего глобального адреса

Этот способ имеет несколько названий: NAT Overload (перегрузка), адресация портов – Port Address Translation (PAT), Many-to-One NAT (замена многих одним). Суть способа состоит в том, что через один внешний адрес могут выходить в глобальную сеть любое количество компьютеров локальной сети, обладающих только частными адресами. Этот способ позволяет решить проблему с нехваткой внешних IP-адресов.

Служба PAT транслирует частные адреса локальных хостов в один публичный. Чтобы правильно пересылать IP-пакеты ответов, поступивших с единственным адресом на вход маршрутизатора локальной сети, на нужный компьютер внутренней сети, маршрутизатор должен помечать каждый локальный хост некоторой меткой. В качестве такой метки используется номер порта из диапазона динамических портов (номера от 1025 до 65535).

При выходе с локального компьютера-источника в глобальную сеть транслятор PAT в маршрутизаторе дополняет частный IP-адрес локального источника одним из номеров порта из разрешенного диапазона и заменяет его на комплексный публичный адрес с тем же номером порта: **IP-адрес: номер порта.** Связка «IP-адрес + номер порта» называется сетевым **сокетом**, который является программным интерфейсом при обмене данными между процессорами. Когда ответ возвращается с сервера, выделенный номер порта локального компьютера, который на обратном пути становится номером порта назначения, определяет, какому локальному компьютеру маршрутизатор должен направить пакеты.

Адреса (сокеты) локальных компьютеров	Адрес (сокеты) маршрутизатора локальной сети
Inside local	Inside global
10.10.1.2:1025	175.10.1.1:1025
10.10.1.3:1026	175.10.1.1:1026
10.10.1.4:1027	175.10.1.1:1027
10.10.1.5:1028	175.10.1.1:1028
10.10.1.6:1029	175.10.1.1:1029

Рисунок 2.2 – Пример таблицы динамической трансляции адресов PAT

На рисунке 2.2 показан пример таблицы трансляции компьютеров локальной сети 10.10.1.0 в единственный публичный адрес 175.10.1.1 маршрутизатора локальной сети.

Для конфигурирования способа использования одного внутреннего глобального адреса необходимо выполнить следующие шаги:

1. Определить стандартный список доступа:

```
Router(config)#access-list <номер> permit <внутренний адрес
                    или блок адресов>
```

2. Установить способ динамической трансляции адресов, разрешенных в списке доступа, определенном на предыдущем шаге:

```
Router(config)#ip nat inside source list <номер списка доступа>
              interface <тип> <номер> overload
```

3. Указать внутренний интерфейс:

```
Router(config)#interface <тип> <номер>
```

4. Пометить этот интерфейс, как принадлежащий внутренней сети:

```
ip nat inside
```

5. Указать внешний интерфейс: **interface** <тип> <номер>

6. Пометить этот интерфейс, как принадлежащий внешней сети: **ip nat** outside

2.4 Процедура проброса портов

Служба NAT осуществляет маскировку адресов компьютеров внутренней сети и пропускает только ответные пакеты из внешней сети на посланный запрос с внутреннего компьютера. Однако в ряде случаев возникает необходимость получить «извне» доступ к какому-нибудь конкретному устройству в локальной сети. Например, если требуется развернуть на локальном компьютере сервер с доступом из Интернета или осуществить подключение к IP-видеокамере, находящейся во внутренней сети, либо при участии владельцев домашней сети в многопользовательских играх и проч.

Для осуществления такого доступа применяется специальная процедура, называемая «**Проброс (перенаправление) порта**» (*англ*. Port Forwarding), которая является частным случаем реализации механизма трансляции адресов PAT**.** При осуществлении проброса порта формируется специальное правило, установленное в маршрутизаторе локальной сети, в соответствии с которым разрешаются все обращения извне к определенному порту сети и затем передаются на конкретное устройство во внутренней сети. Чтобы из внешней сети можно было выполнить доступ к некоторому приложению нужно открыть соответствующий порт. Не забывайте, что понятие «открыть порт» означает, что

пакеты, адресованные на данный порт, будут приниматься на обработку соответствующим приложением.

«Пробросить» порт — это дать команду маршрутизатору зарезервировать один порт и все приходящие на него данные направлять на определенный порт компьютера внутренней сети. Другими словами, сделать исключение из правила отклонения неинициированных внешних запросов и принимать их при заданных условиях. Процедура проброса портов позволяет сделать доступным локальное устройство из публичной сети. После перенаправления портов, TCP и (или) UDP пакеты, пришедшие на заданный порт роутера, будут перенаправлены на нужный порт устройства, находящегося в локальной сети**.**

Так как в случае проброса портов будет открыт доступ к устройствам, находящимся внутри вашей локальной сети, особое внимание следует уделить безопасности, в частности, следует:

- для подключения к устройству должен использоваться надежный пароль;
- если передается конфиденциальная информация, то она должна быть в шифрованном виде.

Для того чтобы задать перенаправление всех запросов, поступающих на публичный адрес маршрутизатора локальной сети, на соответствующий порт нужного внутреннего адреса, можно воспользоваться следующей директивой:

```
Router(config)#ip nat inside source static tcp|udp
<local address> <local port> <global address> <global port>
```

Применение данной команды означает, что TCP либо - UDP запрос, пришедший из Интернета на адрес <global address> по номеру порта <global port>, будет перенаправлен на внутренний адрес <local address> на порт <local port>.

3 Описание лабораторного стенда

В качестве лабораторной установки используется персональный компьютер с инсталлированной программой Packet Tracer, позволяющей осуществлять моделирования компьютерных сетей, построенных на оборудовании корпорации Cisco. Подробно описание пакета моделирования и работы с ним изучалось ранее и приведено в лабораторной работе №1.

Объектом исследования является сеть, схема которой изображена на рисунке 3.1. Лабораторная установка состоит из локальной сети, подключенной к глобальной сети. Локальная сеть состоит их двух персональных компьютеров PC0 и PC1, объединенных коммутатором второго уровня Switch0. Для выхода в глобальную сеть служит маршрутизатор Router0. Адрес локальной сети лабораторной установки определяется номером варианта и равен 192.168.X.0. Здесь X – две последних цифры зачетной книжки.

Глобальная сеть представлена маршрутизатором провайдера Router1, компьютером PC2, коммутатором Switch1и сервером Server0. Адрес шлюза по

умолчанию сети провайдера определяется номером варианта и равен X.0.0.1/8, а адрес сервера - X.0.0.100+X, где X – две последние цифры зачетной книжки.

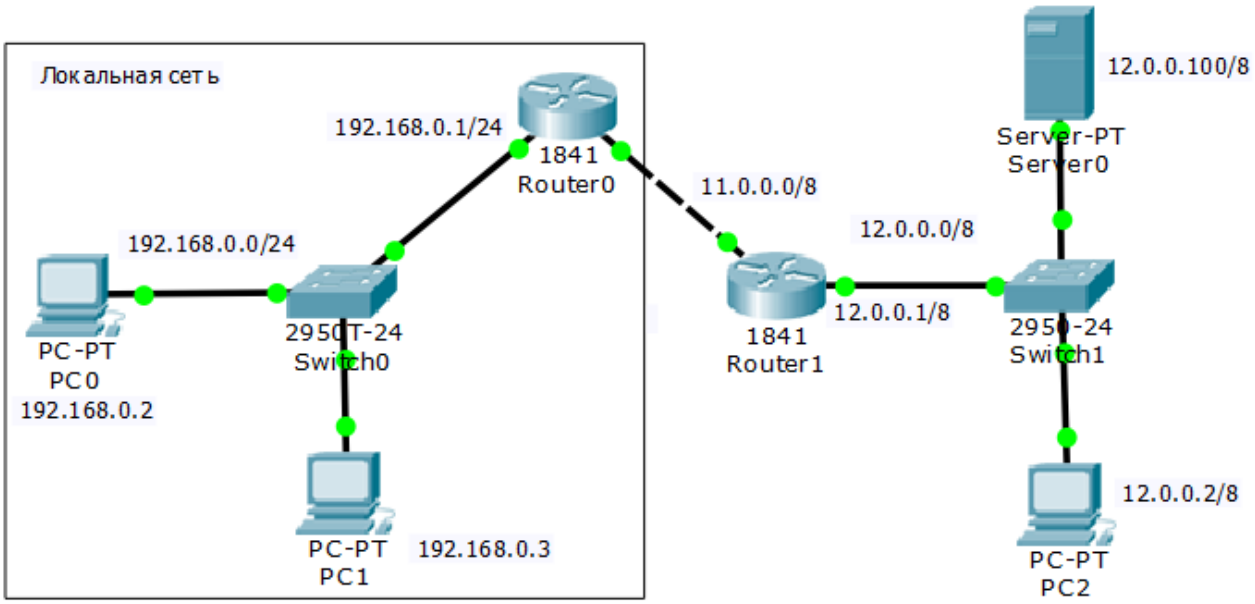

Рисунок 3.1 - Схема лабораторной установки

4 Программа и методика выполнения работы

4.1 Изучить теоретический материал, относящийся к разделу «Локальные компьютерные сети». Особое внимание следует уделить подразделам «Списки доступа» и «Трансляция сетевых адресов», устройству и конфигурации маршрутизаторов. (Выполняется в процессе домашней подготовки).

4.2 Построить в окне эмулятора Packet Tracer локальную сеть, подключенную к глобальной сети (рисунок 3.1). Задать сетевым интерфейсам IP-адреса согласно индивидуальному варианту.

4.3 Настроить статическую маршрутизацию на обоих маршрутизаторах.

4.4 Исследовать достижимость сетевых узлов путем их пингования. Результаты пингования сохранить для отчета.

4.5 Исследовать в режиме эмуляции Packet Tracer содержимое заголовков кадров и пакетов при отсутствии процедуры трансляции адресов.

4.6 Выполнить настройку маршрутизатора локальной сети на трансляцию адресов локальных компьютеров по способу PAT.

4.7 Выполнить пингование сервера и компьютера провайдера при наличии трансляции адресов и исследовать заголовки кадров и пакетов в режиме эмуляции Packet Tracer.

4.8 Проверить таблицу трансляции адресов на маршрутизаторе локальной сети с помощью команды `show ip nat translations`.

Для анализа заголовков кадров на 2-м (канальном) и 3-м (сетевом) уровнях эталонной модели OSI следует переключить Packet Tracer в режим симуля-

ции и выполнить пересылку пакетов с локального компьютера на сервер. На рисунке 4.1 приведен вид окна с информацией о заголовках кадров и пакетов на внутреннем и внешнем интерфейсах маршрутизатора локальной сети.

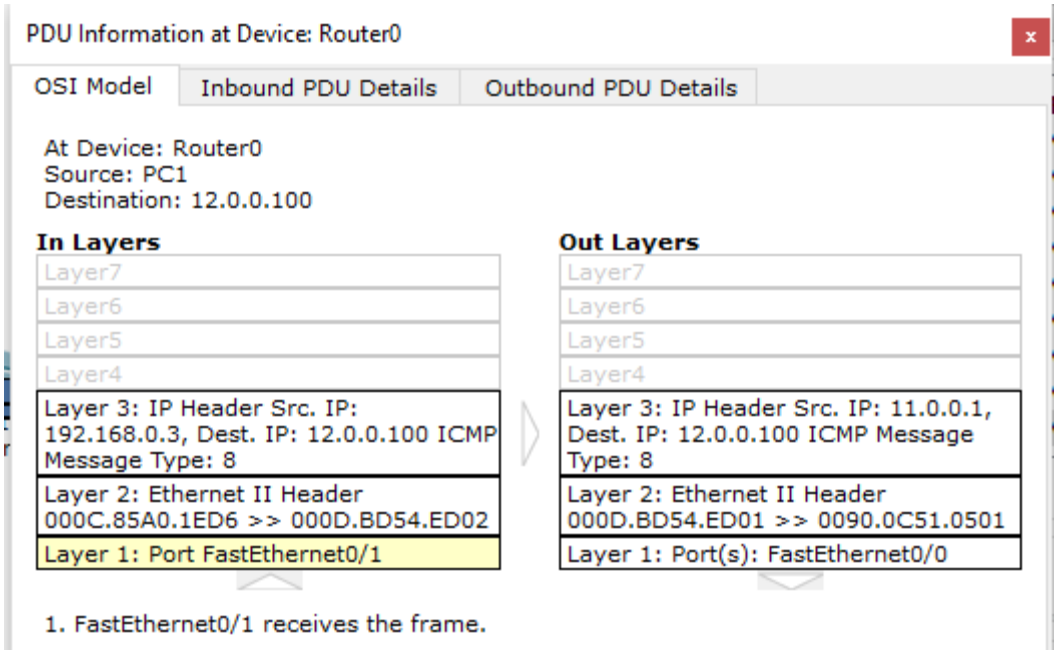

Рисунок 4.1 – Содержание заголовков пакетов на внутренним и внешним интерфейсах маршрутизатора

Как видно из рисунка, на входной порт маршрутизатора FastEthernet 0/1 поступил пакет от компьютера-источника с частным адресом 192.168.0.3 на публичный адрес сервера 12.0.0.100. На выходе портаFa 0/0 маршрутизатора частный адрес отправителя сменился на публичный адрес 11.0.0.1, а адрес получателя остается прежним. Отсюда следует, что процедура NAT функционирует правильно.

Полную таблицу NAT можно посмотреть с помощью команды show ip nat translations:

```
Router#sh ip nat translations
Pro  Inside global     Inside local       Outside local      Outside global
icmp 11.0.0.1:1        192.168.0.3:1      12.0.0.2:1         12.0.0.2:1
icmp 11.0.0.1:3        192.168.0.2:3      12.0.0.100:3       12.0.0.100:3
```

Для настройки NAT на роутере необходимо выполнить следующие шаги:

1. Зайти в настройки Router0, во вкладку интерфейса командной строки CLI

2. Для входа в режим администратора ввести команду enable (en): Router>en, а для входа в режим настройки ввести команду config t: Router#config t

3. Интерфейс FastEthernet 0/1 является внутренним интерфейсом локальной сети, к которому подключены рабочие станции PC. Для настройки NAT на маршрутизаторе необходимо это указать в настройках. Такая настройка осуществляется при помощи следующих команд:

Зайти в настройки интерфейса:

Router(config)#int FastEthernet 0/0

и объявить интерфейс внутренним интерфейсом:

Router(config-if)#ip nat inside

Сохранить и выйти из настроек интерфейса

Router(config-if)#exit

4. Аналогично нужно настроить интерфейс FastEthernet 0/0, который подключен к сети провайдера. Отличие состоит в том, что Fa0/0 должен быть инициирован как внешний интерфейс NAT:

зайти в настройки интерфейса:

Router(config)#int FastEthernet 0/1

объявить интерфейс внешним интерфейсом NAT:

Router(config-if)#ip nat outside

Сохранить и выйти из настроек интерфейса:

Router(config-if)#exit

5. Задать пул внешних адресов, в которые будут транслироваться внутренние адреса.

При задании пула адресов необходимо указать первый и последний адреса из входящей в пул последовательности адресов. Если в пуле всего один адрес (как в данном примере) необходимо указать его 2 раза.

Router(config)#ip nat pool natpool 11.0.0.1 11.0.0.1 netmask 255.0.0.0

6. Задать список доступа:

Router(config)#access-list 1 permit any

Any – ключевое слово, означает, что список доступа будет разрешать пакеты с любым адресом отправителя.

7. Включить процедуру NAT на Router0.

Router(config)#ip nat inside source list 34 pool natpool overload

Данная команда предписывает маршрутизатору трансляцию всех частных пакетов, поступивших на внутренний интерфейс и разрешенных списком доступа номер 1, в один и тот же публичный адрес из NAT пула “natpool”. Ключ overload указывает, что трансляции будут осуществляться способом «перегрузка», позволяя нескольким внутренним адресам транслироваться на один IP-адрес.

```
Router>en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa0/1
Router(config-if)#ip nat inside
Router(config-if)#exit
Router(config)#int fa0/0
Router(config-if)#ip nat outside
Router(config-if)#exit
Router(config)#ip nat pool natpool 11.0.0.1 11.0.0.1 netmask 255.0.0.0
Router(config)#access-list 1 permit any
Router(config)#ip nat inside source list 1 pool natpool overload
Router(config)#exit
Router#
```