Настройка динамического и статического NAT

Топология

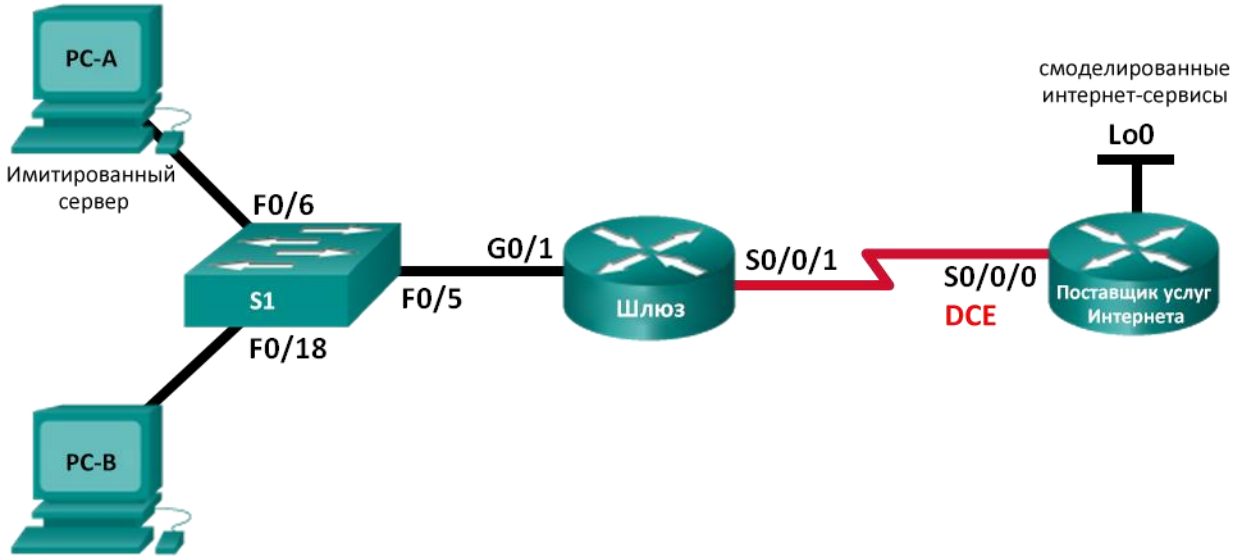

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
Шлюз_ФАМИЛИЯ	G0/1	192.168.1.1	255.255.255.0	—
	S0/0/1	209.165.201.18	255.255.255.252	—
ISP	S0/0/0 (DCE)	209.165.201.17	255.255.255.252	—
	Lo0	192.31.7.1	255.255.255.255	—
PC-A (смоделированный сервер)	NIC	192.168.1.20	255.255.255.0	192.168.1.1
PC-B	NIC	192.168.1.21	255.255.255.0	192.168.1.1

Задачи

Часть 1. Построение сети и проверка соединения

Часть 2. Настройка и проверка статического NAT

Часть 3. Настройка и проверка динамического NAT

Необходимые ресурсы

- 2 маршрутизатора Cisco
- 1 коммутатор Cisco
- 2 ПК (под управлением Windows 7 или 8 с программой эмуляции терминала Tera Term или Putty)

- Консольные кабели для настройки устройств Cisco IOS через консольные порты
- Кабели Ethernet и последовательные кабели согласно топологии.

Часть 1: Построение сети и проверка связи

В первой части вам предстоит настроить топологию сети и выполнить базовую настройку, например, IP-адреса интерфейсов, статическую маршрутизацию, доступ к устройствам и пароли.

Шаг 1: Создайте сеть согласно топологии.

Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.

Шаг 2: Настройте узлы ПК.

Шаг 3: Выполните инициализацию и перезагрузку маршрутизатора и коммутаторов.

Шаг 4: Произведите базовую настройку маршрутизаторов.

a. Подключитесь к маршрутизатору с помощью консоли и перейдите в режим глобальной настройки.

b. Скопируйте приведенную ниже базовую конфигурацию и вставьте ее в текущую конфигурацию на маршрутизаторе.

```
no ip domain-lookup
service password-encryption
enable secret class
banner motd #
Unauthorized access is strictly prohibited. #
line con 0
password cisco
login
logging synchronous
line vty 0 4
password cisco
login
```

c. Настройте имена хостов в соответствии с топологией. Используйте имя Gateway_ФАМИЛИЯ, укажите вашу фамилию на английском языке.

d. Скопируйте текущую конфигурацию в файл загрузочной конфигурации.

Шаг 5: Для симуляции создайте веб-сервер на ISP.

a. Создайте локального пользователя с именем **webuser** с зашифрованным паролем **webpass,** уровень привилегий – 15.

b. Включите службу HTTP-сервера на маршрутизаторе ISP с помощью команды **ip http server**. Учтите, что данная команда может не работать в вашей версии Packet Tracer.

c. Настройте сервис HTTP таким образом, чтобы он использовал локальную базу данных пользователей. Используйте команду **ip http authentication local**. Учтите, что данная команда может не работать в вашей версии Packet Tracer.

Шаг 6: Настройте статическую маршрутизацию.

a. Создайте статический маршрут на маршрутизаторе ISP до диапазона назначенных публичных сетевых адресов 209.165.200.224/27 маршрутизатора Gateway_ФАМИЛИЯ, используя адрес следующего перехода.

b. Создайте маршрут по умолчанию от маршрутизатора Gateway_ФАМИЛИЯ к маршрутизатору ISP, используя адрес следующего перехода.

Шаг 7: Сохранение текущей конфигурации в качестве загрузочной.

Шаг 8: Проверьте подключение к сети.

a. С компьютеров отправьте эхо-запросы на интерфейс G0/1 маршрутизатора Gateway_ФАМИЛИЯ. Выполните отладку, если эхо-запрос не проходит.

b. Отобразите таблицы маршрутизации на обоих маршрутизаторах, чтобы убедиться, что статические маршруты содержатся в таблице маршрутизации и правильно настроены на обоих маршрутизаторах.

Часть 2: Настройка и проверка статического преобразования NAT

В статическом NAT используется сопоставление локальных и глобальных адресов по схеме «один к одному». Метод статического преобразования особенно полезен для веб-серверов или устройств, которые должны иметь постоянный адрес и быть доступными из Интернета.

Шаг 1: Настройте статическое сопоставление.

Статическая привязка должна быть настроена для преобразования маршрутизатором частного внутреннего адреса сервера 192.168.1.20 в публичный адрес 209.165.200.225 и обратно. Это позволит пользователю из Интернета получить доступ к компьютеру PC-A. Компьютер PC-A моделирует сервер или устройство с постоянным адресом, к которому можно получить доступ из Интернета.

Шаг 2: Задайте интерфейсы.

Выполните на соответствующих интерфейсах маршрутизатора Gateway_ФАМИЛИЯ команды для того, что, чтобы обозначить внутренний и внешний интерфейсы для преобразования.

Шаг 3: Протестируйте настройку.

a. Отобразите таблицу статических **преобразований** NAT.

Во что был преобразован внутренний адрес локального узла?

192.168.1.20 = _____

Кем назначен внутренний глобальный адрес?

_____

Кем назначен внутренний локальный адрес?

_____

b. На компьютере ПК A отправьте эхо-запрос на интерфейс Lo0 (192.31.7.1) маршрутизатора ISP. Если эхо-запрос не прошел, выполните отладку. На маршрутизаторе Gateway_ФАМИЛИЯ просмотрите таблицу преобразований NAT.

Когда компьютер ПК A отправил ICMP-запрос (эхо-запрос) на адрес ISP 192.31.7.1, в таблицу была добавлена запись NAT, где ICMP указан в виде протокола.

Какой номер порта использовался в данном обмене пакетами ICMP? _____

c. С компьютера ПК A подключитесь по Telnet к интерфейсу Lo0 ISP и отобразите таблицу преобразований NAT.

Примечание. NAT для запроса ICMP может устареть, из-за чего он будет удален из таблицы NAT.

Какой протокол использовался для этого преобразования? _____

Укажите номера используемых портов.

Внутренний глобальный/локальный: _____

Внешний глобальный/локальный: _____

d. Поскольку статический NAT настроен для ПК A, убедитесь в успешном прохождении эхо-запроса от ISP до ПК A по публичному адресу через статический NAT (209.165.200.225).

e. На маршрутизаторе Gateway_ФАМИЛИЯ отобразите таблицу NAT, чтобы проверить преобразование.

Обратите внимание, что внешний локальный и внешний глобальный адреса совпадают. Этот адрес — адрес источника в удаленной сети ISP. Для успешной отправки эхо-запроса от ISP, внутренний глобальный адрес статического NAT 209.165.200.225 был преобразован во внутренний локальный адрес компьютера ПК A (192.168.1.20).

f. Проверьте статистику NAT, выполнив соответствующую команду на маршрутизаторе, являющемся шлюзом.

Часть 3: Настройка и проверка динамического преобразования (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. Динамическое преобразование NAT представляет собой сопоставление адресов по схеме «многие ко многим» между локальными и глобальными адресами.

Шаг 1: Очистите данные NAT.

Перед добавлением динамических преобразований очистите все NAT и удалите статистику из части 2 с помощью команд **clear ip nat translation *** и **clear ip nat statistics**.

Шаг 2: Создайте список контроля доступа (ACL-список), соответствующий диапазону частных IP-адресов локальной сети.

ACL-список 1 используется для обеспечения возможности преобразования сети 192.168.1.0/24 (необходимо разрешить эту сеть, используя стандартный ACL-список). Добавьте ACL 1 на Gateway_ФАМИЛИЯ.

Шаг 3: Убедитесь, что настройки интерфейсов NAT все еще действительны.

Проверьте настройки NAT (статистику преобразований) на маршрутизаторе Gateway_ФАМИЛИЯ.

Шаг 4: Определите пул пригодных к использованию публичных IP-адресов.

Создайте NAT-пул на маршрутизаторе Gateway_ФАМИЛИЯ с именем **public_access**. Диапазон адресов в пуле – от **209.165.200.242** до **209.165.200.254**. Маска подсети – 255.255.255.224.

Шаг 5: Определите NAT из внутреннего списка адресов источника на пул внешних адресов.

Примечание. Помните, что имена пула NAT регистрозависимы, а имя пула, вводимое здесь, должно совпадать с именем, использованным на предыдущем шаге.

Вам необходимо на маршрутизаторе Gateway_ФАМИЛИЯ привязать ACL-список с номером 1 к NAT-пулу **public_access**.

Шаг 6: Протестируйте настройку.

a. С ПК B отправьте эхо-запрос на интерфейс Lo0 (192.31.7.1) маршрутизатора ISP. Если эхо-запрос не прошел, выполните отладку. На маршрутизаторе Gateway_ФАМИЛИЯ просмотрите таблицу преобразований NAT.

   Как выглядит преобразованный внутренний адрес локального узла для ПК B?

   192.168.1.21 = _____

   Когда ПК B отправил сообщение ICMP на адрес ISP 192.31.7.1, в таблицу была добавлена динамическая запись NAT с указанным протоколом ICMP.

   Какой номер порта использовался в данном обмене пакетами ICMP? _____

b. На компьютере ПК B откройте веб-браузер и введите IP-адрес имитируемого на ISP веб-сервера (интерфейс Lo0). При запросе войдите в систему под именем **webuser** и с паролем **webpass**. Учтите, что данное действие может не сработать в вашей версии Packet Tracer.

c. Выведите на экран таблицу преобразований NAT.

   Какой протокол использовался для этого преобразования? _____

   Укажите номера используемых портов.

   Внутренний: _____

   Внешний: _____

   Какие общеизвестные номер порта и сервис использовались? _____

d. Проверьте статистику NAT на маршрутизаторе, являющемся шлюзом.

Шаг 7: Удалите запись статического NAT.

На шаге 7 запись статического NAT удаляется, и можно просмотреть запись NAT.

a. Удалите запись для статического NAT из части 2. При запросе об удалении дочерних записей введите **yes** (да).

b. Очистите трансляции NAT и статистику.

c. Отправьте эхо-запрос к ISP (192.31.7.1) с обоих узлов.

d. Отобразите таблицу преобразований и статистику NAT.

Контрольные вопросы

1. Зачем нужно использовать NAT в сети?

   _____

   _____

   _____

2. В чем заключаются ограничения NAT?

   _____

   _____

   _____