Лабораторная работа № 6
Трансляция сетевых адресов

6.1. Цель работы

Лабораторная работа № 6 предназначена для изучения технологий и протоколов трансляции IP-адресов и представляет собой сценарий для Cisco Packet Tracer. Для успешного выполнения лабораторной работы студентам необходимо выполнить задание сценария и подготовить отчет (по своему варианту), а также защитить его в форме собеседования.

6.2. Теоретическая часть

6.2.1. Дефицит IPv4-адресов

Несмотря на значительный объем пространства IPv4 адресов (2^{32} адресов, т.е. около 4,22 млрд.), его исчерпание уже несколько десятилетий считается серьезной проблемой.

Напомним, что адресное пространство сети Интернет (как и другие пространства числовых и символьных идентификаторов) регулируются американской некоммерческой организацией IANA (англ. Internet Assigned Numbers Authority), а также пятью региональными интернет-регистраторами (Regional Internet Registry, RIR), и локальными интернет-регистраторами, такими как интернет-провайдеры.

Региональные регистраторы занимаются технической стороной функционирования Интернета: выделением IP-адресов, номеров автономных систем, регистрацией обратных зон DNS и другими техническими проектами. Часто региональные регистраторы занимаются статистическим анализом сетей, мониторингом точек обмена трафиком и поддержкой корневых зон DNS. IANA делегирует RIR большие объёмы Интернет-ресурсов, которые RIR делегируют своим членам в соответствии со своими правилами.

На данный момент существуют пять RIR:

- American Registry for Internet Numbers (ARIN) — для Северной Америки;
- RIPE Network Coordination Centre (RIPE NCC) — для Европы, Ближнего Востока и Центральной Азии;
- Asia-Pacific Network Information Centre (APNIC) — для Азии и Тихоокеанского региона;
- Latin American and Caribbean Internet Addresses Registry (LACNIC) — для Латинской Америки и Карибского региона;

– African Network Information Centre (AfriNIC) — для Африки и региона Индийского океана.

Уже в сентябре 2015 года об исчерпании общего запаса свободных IPv4 адресов и ограничениях на выдачу новых адресов объявили все региональные регистраторы, кроме AfriNIC. Исчерпание последнего блока AfriNIC ожидается в первой половине 2018 года.

Исчерпание адресов стало причиной, давшей толчок развитию ряда новых сетевых технологий, включая бесклассовую адресацию (Classless Inter-Domain Routing, CIDR), трансляцию адресов (Network Address Translation, NAT) и новую версию протокола IP – IPv6. Технология CIDR была подробно рассмотрена ранее (см. методические указания к лабораторной работе № 1). Технология IPv6 не входит в программу настоящего курса. Рассмотрим технологию NAT.

6.2.2. Типы адресов NAT

Итак, IPv4-адресов недостаточно, чтобы назначить уникальные адреса всем устройствам, подключённым к сети Интернет. В большинстве случаев сети реализуются с использованием т.н. частных IPv4-адресов. Эти частные адреса используются в рамках организации или объекта с целью обеспечения взаимодействия устройств внутри сети. Для такой сети адреса могут быть выбраны администратором из специально зарезервированных блоков адресов:

– 192.168.0.0/16
– 172.16.0.0/12
– 10.0.0.0/8).

Но поскольку эти адреса не уникальны и не позволяют определить конкретную компанию или организацию, частные IPv4-адреса нельзя использовать для маршрутизации через Интернет. Для того, чтобы разрешить устройству с частным IPv4-адресом доступ к устройствам и ресурсам вне локальной сети, частный адрес сначала необходимо преобразовать в публичный адрес.

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, расположенные в сети Интернет. 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.

В терминологии NAT под «внутренней сетью» подразумевается набор сетей, задействованных в преобразовании. Термин «внешняя сеть» относится ко всем остальным сетям.

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

При определении используемого типа адреса важно помнить, что терминология NAT всегда применяется с точки зрения устройства с преобразуемым адресом (Рис 6.1). Внутренний адрес — это адрес устройства, преобразуемый устройством NAT. Внешний адрес — это адрес устройства назначения.

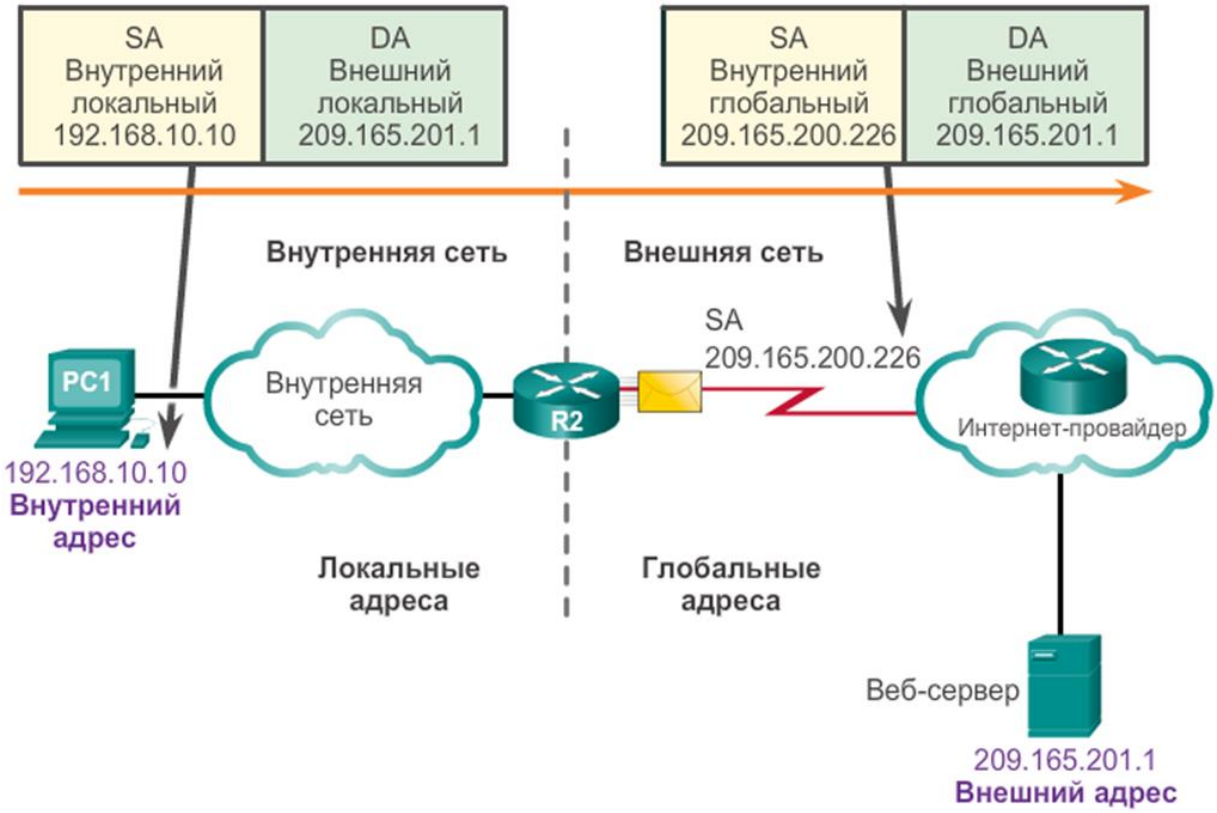

Рис. 6.1. Типы адресов NAT

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.

Термины «внутренний» и «внешний» используются в сочетании с терминами «локальный» и «глобальный», когда речь идёт о конкретных адресах. Внутренний локальный адрес — это адрес источника, видимый из

внутренней сети. Внутренний глобальный адрес — это адрес источника, видимый из внешней сети. Внешний глобальный адрес — это адрес назначения, видимый из внешней сети. Внешний локальный адрес — это адрес назначения, видимый из внутренней сети.

6.2.3. Принцип работы NAT

Задача процесса NAT – выполнить трансляцию адресов на границе внутренней и внешней сетей, т.е. изменить в проходящих пакетах IP-адрес источника или назначения. Процесс NAT использует для работы специальную таблицу отображений. Записи в таблице создаются при чтении конфигурационного файла (статические) или при срабатывании определенных правил (динамические).

Для работы процесса NAT необходимо, чтобы интерфейсы маршрутизатора были помечены как внутренние – inside или внешние – outside. Тогда у пакета, пришедшего на inside интерфейс меняется source IP. Это называется **прямой** трансляцией.

Для того, чтобы ответный пакет мог достичь получателя, расположенного во внутренней сети, у пакета, пришедшего на outside интерфейс меняется destination IP. Это называется **обратной** трансляцией.

Рассмотрим прямую трансляцию подробнее.

ПРИМЕЧАНИЕ. Здесь и далее рассмотрен самый распространенный вариант применения сетевой трансляции – Inside Source NAT. В других вариантах, например, Inside Destination NAT, принцип работы несколько иной, однако данные варианты NAT не рассматриваются в настоящем курсе.

Сетевой пакет, поступивший на inside интерфейс и соответствующий критериям трансляции, маркируется как «возможно транслируемый». Затем пакет подвергается маршрутизации. Если при этом пакет направлен на интерфейс, помеченный как outside, происходит трансляция. Если трансляция динамическая, маршрутизатор проверяет ее наличие в таблице трансляций. Если ее там нет — создает, если уже есть — обнуляет счетчик неактивности. Если же пакет попадает на выход на интерфейс, не помеченный как outside — трансляция НЕ происходит.

Рассмотрим обратную трансляцию.

Сетевой пакет, попадая на outside интерфейс, в противовес прямой трансляции, сначала подвергается NAT. Если трансляция существует (неважно, динамическая или статическая), у пакета меняется IP-адрес назначения. И только после этого пакет подвергается маршрутизации и перенаправляется по назначению.

Для обратной трансляции не обязательно наличие метки inside на каком-либо интерфейсе. Все равно, если прямая трансляция существует, обратная трансляция сработает до маршрутизации. Однако такая ситуация возможна только тогда, когда трафик не проходил через inside интерфейс, а значит был сгенерирован самим маршрутизатором.

Следовательно, трафик самого роутера может подвергаться трансляции, если он попадает на интерфейс, помеченный как outside, и удовлетворяет критериям NAT. Следует аккуратно создавать критерии отбора, чтобы не включить в трансляцию, например, трафик протоколов маршрутизации.

Виртуальные интерфейсы маршрутизатора (саб-интерфейсы и loopback) трактуются, как и любые другие. Они могут быть помечены как inside или outside и участвовать в трансляции адресов.

Приведенные выше особенности необходимо учитывать при маркировке интерфейсов как inside и outside.

6.2.4. Режимы работы NAT

Существуют три режима преобразования сетевых адресов.

Статическое преобразование сетевых адресов (**статический NAT**) — это взаимно-однозначное соответствие между локальным и глобальным адресами. Пример статического NAT, сопоставляющего локальный адрес 192.168.1.1 с глобальным 82.179.84.1 (вводится в режиме глобальной конфигурации):

```
ip nat inside source static 192.168.1.1 82.179.84.1
```

Такая команда создает постоянную двустороннюю трансляцию. Так что наш хост всегда будет доступен по одному внешнему адресу и эта трансляция никогда не вылетит из таблицы трансляций по таймауту. Это удобно, например, для присвоения глобальных адресов серверам, расположенным во внутренней сети.

Часто бывает, что нужно выставить наружу не целый адрес, а только один порт (например, TCP 80 для веб-сервера). Для этого создается постоянная статическая трансляция для некоторых выборочных портов, например:

```
ip nat inside source static tcp 10.0.1.1 80 11.1.1.21 80
ip nat inside source static udp 10.0.1.1 5060 11.1.1.21 7877
```

Динамическое преобразование сетевых адресов (**динамический NAT**) — это сопоставление адресов по схеме «многие ко многим» между локальными и глобальными адресами. Для использования данного режима необходимо определить, какой именно трафик (с каких внутренних адресов)

должен быть подвергнут процедуре трансляции, и какие глобальные адреса необходимо использовать при выполнении такой трансляции.

Для решения первой задачи необходимо настроить стандартный список контроля доступа (ACL), разрешающий адреса, которые должны быть преобразованы. *Более подробно о списках контроля доступа и их настройке см. методические указания к лабораторной работе № 5.* Указанный ACL не следует применять к интерфейсу: он предназначен не для фильтрации трафика, а для отбора тех пакетов, для которых следует выполнить преобразование адресов. Допускается использование расширенного ACL вместо стандартного.

ПРИМЕЧАНИЕ. В данном ACL могут встречаться строки с командой deny. Трафик, удовлетворяющий таким строкам, не блокируется, а просто не подвеграется трансляции.

Для решения второй задачи необходимо создать пул внешних адресов, которые будут использованы при выполнении преобразования.

Пример динамического NAT, выполняющего трансляцию адресов для всех пакетов, удовлетворяющих критериям стандартного списка контроля доступа (номер 100), с использованием глобальных адресов из пула mypool 82.179.84.100 – 82.179.84.200 (команды вводятся в режиме глобальной конфигурации):

```
ip access-list 100 permit 10.0.1.0 0.0.0.255
ip nat pool mypool 11.1.1.100 11.1.1.200 netmask 255.255.255.0
ip nat inside source list 100 pool mypool
```

В случае динамического NAT трансляция создается (добавляется запись в таблицу NAT) динамически при передаче первого исходящего пакета, удовлетворяющего правилам трансляции. При этом трансляция создается целиком для адреса (не для отдельных портов, хотя в таблицу и записывается с указанием номеров портов). Запись о трансляции хранится некоторое время (настраиваемый параметр, по умолчанию равен 86400 секунд – 24 часа), чтобы ответные пакеты могли быть доставлены адресату. В течение времени жизни записи в таблице трансляций пакеты снаружи могут проходить на транслируемый хост по внешнему (inside global) адресу. Если в течение некоторого времени трафик по этой трансляции отсутствует, трансляция удаляется и адрес возвращается в пул.

Если требуется создать трансляцию, а свободных адресов в пуле нет, то пакет отбрасывается. Следовательно, динамический NAT без перегрузки пригоден только для таких сетей, где количество глобальных адресов в пуле

сопоставимо с количеством транслируемых узлов, иначе высока вероятность проблем с доступом наружу.

Перегруженный NAT — это сопоставление адресов по схеме «многие к немногим» (или даже «многие-к одному») между локальными и глобальным адресами. Данный метод также называется динамическим NAT с перегрузкой или PAT – Port Address Translation, т.к. в этом режиме для обеспечения однозначности отображения маршрутизатор использует не только IP-адреса, но еще и TCP/UDP порты.

Перегруженный режим во многом схож с динамическим, но требует добавления к команде создания отображения ключевого слова overload.

```
ip nat inside source list 100 pool mypool overload
```

Также вместо создания пула адресов может быть указан внешний интерфейс маршрутизатора. Тогда именно адрес внешнего интерфейса и будет использоваться в качестве глобального для всех исходящих пакетов, удовлетворяющих критериям отбора. Пример перегруженного NAT, использующего в качестве глобального адрес внешнего интерфейса FastEthernet 0/1:

```
ip nat inside source list 100 interface fa0/1 overload
```

Поведение перегруженной трансляции отличается от поведения обычного динамического NAT еще и тем, что доступ снаружи на inside global адрес невозможен. Именно это позволяет говорить о некоторой повышенной безопасности при использовании PAT, т.к. фактически все соединения инициируются изнутри корпоративной сети, а снаружи могут приходить только ответы на них – внутренняя сеть скрыта и защищена. Для обеспечения выборочного доступа обычно создают в дополнение к перегруженному NAT отдельные статические отображения.

ВНИМАНИЕ! Независимо от выбранного режима работы NAT, для его корректной работы необходимо отметить на маршрутизаторе интерфейсы, подключенные к внешней и внутренним сетям соответственно. В противном случае трансляция осуществляться не будет! Для этого используется специальная команда в режиме конфигурирования интерфейса:

```
ip nat inside
ip nat outside
```

6.2.5. Протокол DHCP

Протокол динамической настройки узлов (англ. Dynamic Host Configuration Protocol, DHCP) предназначен для автоматизации присвоения устройствам различных сетевых настроек. DCHP позволяет автоматически настраивать на клиентских устройствах следующие основные параметры:

- IP адрес;
- основной шлюз;
- маска подсети;
- DNS сервер.

Это наиболее частое использование DHCP, но можно передавать и огромное количество других параметров. Например, можно передавать дополнительные маршруты, чтобы в разные сети компьютер ходил через разные шлюзы. Или, с помощью DHCP можно организовывать загрузку устройств по сети. В этом случае клиент получает помимо основных параметров, адрес TFTP сервера и имя файла-загрузчика на нём.

Когда клиент, например, обычный компьютер, запускается, операционная система видит, что для некоторого сетевого интерфейса включена опция «получить адрес автоматически». Процедура получения адреса по DHCP состоит из четырех этапов. Параметры процедуры несколько отличаются в зависимости от используемого режима работы DHCP (ручной, автоматический, динамический).

При использовании ручного режима на сервере должна быть заранее создана таблица соответствия MAC-адресов клиентов и зарезервированных за ними IP-адресов. Обычно такой режим используется в сочетании с динамическим, когда необходимо обеспечить отдельным клиентам (например, серверам или сетевым устройствам) постоянные IP-адреса и нет возможности присвоить их статически. Такое соответствие создается единожды и действует постоянно.

В автоматическом режиме работы аналогичное постоянное соответствие создается автоматически. Этот режим работы схож с ручным, но не требует настройки таблицы соответствия: она заполняется автоматически по мере поступления запросов клиентов. Необходимо контролировать наличие свободных адресов в пуле, т.к. созданные соответствия действуют постоянно, как и в ручном режиме.

Наиболее часто применяется третий – динамический режим работы DHCP, в котором таблица формируется автоматически, но каждая запись в ней имеет срок действия, по истечение которого адрес освобождается и возвращается в пул.

Рассмотрим последовательность работы DHCP при использовании наиболее часто используемого **динамического** режима работы.

1. Компьютер отправляет широковещательный запрос «DHCP discover» (от англ. discover – открытие). В заголовках канального уровня такого запроса указывается MAC-адрес клиента в качестве адреса отправителя и широковещательный MAC-адрес ffff.ffff.ffff в качестве адреса получателя. На третьем уровне адрес отправителя отсутствует, адрес получателя равен 255.255.255.255.

2. Все устройства в домашней сети получают это широковещательное сообщение. DHCP сервера (а их теоретически может быть несколько) отвечают клиенту. Сервер резервирует в своём пуле адресов какой-то адрес (если не было резервации до этого для данного MAC-адреса клиента) и выделяет этот IP клиенту на какое-то время (lease time). Этот адрес высылается клиенту вместе с остальными параметрами, настраиваемыми по DHCP. При этом в качестве адресов получателя используется уже новый выделенный клиентский IP-адрес и клиентский MAC. Такое сообщение называется «DHCP offer» (от англ. offer – предложение).

3. Из полученных предложений клиент выбирает одно (обычно оно всего одно, либо выбирается полученное первым) и отправляет со своего MAC и нового IP на MAC и IP уже конкретного сервера сообщение «DHCP request» (англ. request – запрос) – согласие с полученными параметрами.

4. Сервер резервирует за клиентом выделенный адрес на какое-то время (lease time – срок аренды). До этого момента адрес был выделен, но не зарезервирован. Теперь же он окончательно закреплён за клиентом. Сервер вносит запись о соответствии IP- и MAC-адресов клиента в свою ARP-таблицу и высылает клиенту сообщение, что тот успешно зарегистрирован – «DCHP Acknowledge» (от англ. acknowledge – подтверждение).

Клиент начинает работать.

6.2.6. Команды IOS

Рассмотрим список новых команд IOS, необходимых и достаточных для настройки NAT. Более простые и ранее изученные команды см. в описании лабораторных работ №№ 1-5, а также в контекстной справке Cisco IOS (команда «?»).

Команды привилегированного режима

`router#`

```
show ip nat translations
```

Отображает список активных трансляций IP-адресов.

Команды режима глобального конфигурирования

`router(config)#`

```
ip nat inside source static <Локальный IP-адрес> <Глобальный
IP-адрес>
```

Создает статическое NAT-отображение указанного локального адреса в указанный глобальный.

ПРИМЕЧАНИЕ. Для включения указанного отображения необходима активация NAT хотя бы на одном внутреннем и одном внешнем интерфейсах.

```
ip nat pool <Имя пула> <Начальный IP-адрес пула> <Конечный IP-
адрес пула> netmask <маска>
```

Создает пул глобальных IP-адресов для последующего использования в динамическом NAT-преобразовании; границами пула являются заданные начальный и конечный IP-адреса (могут совпадать, тогда трансляция будет в 1 адрес); опция netmask позволяет вырезать из диапазона адресов в пуле те адреса, которые являются адресами SUBNET или BROADCAST при данной маске.

ПРИМЕЧАНИЕ. Для включения отображения необходима активация NAT хотя бы на одном внутреннем и одном внешнем интерфейсах, а также создание самого преобразования – связь пула со списком контроля доступа.

```
ip nat inside source list <ACL> pool <Имя пула>
```

Создает динамическое NAT-отображение для трафика, отбираемого с помощью заданного ACL, в указанный пул глобальных адресов.

ПРИМЕЧАНИЕ. Для включения указанного отображения необходима активация NAT хотя бы на одном внутреннем и одном внешнем интерфейсах.

```
ip nat inside source list <ACL> interface <Имя интерфейса>
overload
```

Создает перегруженное динамическое NAT-отображение для трафика, отбираемого с помощью заданного ACL, в (глобальный) адрес указанного внешнего интерфейса.

ПРИМЕЧАНИЕ. Для включения указанного отображения необходима активация NAT хотя бы на одном внутреннем интерфейсе, а также на интерфейсе отображения (как на внешнем).

```
ip dhcp pool <имя пула>
```

Создает на маршрутизаторе dhcp-пул с указанным именем и переводит маршрутизатор в режим конфигурирования dhcp;

```
ip dhcp excluded address <начальный (или единственный) IP-адрес> [конечный IP-адрес]
```

Исключает из пула dhcp-адресов один (или несколько) адресов, например, если они присвоены каким-то устройствам статически. Среди исключаемых обязательно должен быть адрес основного шлюза!

Команды конфигурирования интерфейса

`router(config-if)#`

```
ip nat {inside | outside}
```

Активирует на текущем интерфейсе функцию NAT-преобразования и помечает данный интерфейс как внутренний или внешний.

```
ip helper-address <ip-адрес>
```

Включает пересылку dhcp-запросов на удаленный интерфейс (используется на интерфейсе – основном шлюзе, если dhcp-сервер не является основным шлюзом для клиентских устройств в сети).

Команды конфигурирования dhcp

`router(dhcp-config)#`

```
network <IP-адрес сети> <сетевая маска>
```

Задает диапазон адресов пула, которые будут раздаваться клиентам, а также маску подсети.

```
Router(dhcp-config)#dns-server <IP-адрес основоного DNS-сервера> [IP-адреса других DNS-серверов]
```

Задает адрес DNS-сервера для клиентов.

```
Router(dhcp-config)#default-router 192.168.100.1
```

Задает адрес основного шлюза.

ПРИМЕЧАНИЕ. Протокол DHCP позволяет настраивать массу различных сетевых параметров. Здесь рассмотрен минимальный перечень опций, необходимый и достаточный для выполнения задания лабораторной работы.

6.3. Задание на лабораторную работу

Лабораторная работа выполняется в среде Cisco Packet Tracer в предложенном Вам файле-сценарии формата pka. Сценарий содержит созданную заранее топологию в виде составной сети, моделирующей корпоративную сеть условного предприятия, подключенную к сети Интернет (рис. 6.2). Устройства частично настроены.

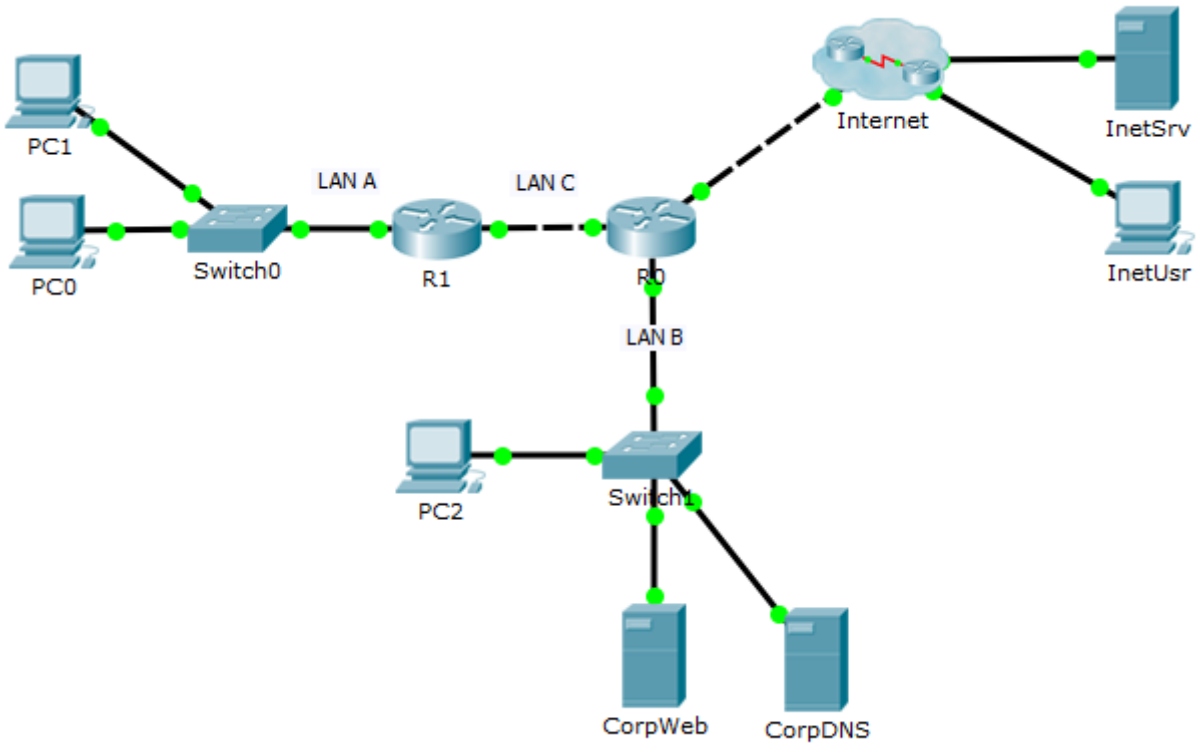

Рисунок 6.2. Топология сети

6.3.1. Расчёт и настройка IP-адресов

Необходимо выполнить расчет IP-адресов локальных сетей и устройств, настроить все устройства (компьютеры и маршрутизаторы), маршрутизацию и NAT-трансляцию IP-адресов.

Представленная топология состоит из трех областей: левой (LAN A – подключена к R1, не настроена), средней (LAN C – между R0 и R1, не настроена), нижней (LAN B – подключена к R0, не настроена) и правой (сеть Интернет, настроена).

Необходимо рассчитать адреса устройств в сетях LAN A и LAN B, исходя из известных диапазонов адресов (где X – номер Вашего варианта):

- для сети LAN A – 192.168.X.0/24;
- для сети LAN B – 172.17.X.0/24.

Для служебной сети, соединяющих между собой маршрутизаторы R0 и R1, использовать адреса LAN C:

- для сети LAN C – 172.16.X.0/24.

Для настройки компьютеров в сети LAN A использовать протокол DHCP. Для этого необходимо на маршрутизаторе R1 создать пул DHCP-адресов из заданного диапазона и выполнить его настройку (назначить раздачу адресов, шлюза, корпоративного DNS-сервера). На компьютерах необходимо активировать DHCP-клиент – включить автоматическое получение IP-адресов.

Выполнить настройку компьютеров и серверов в LAN B (настроить IP-адрес, маску подсети, шлюз по умолчанию и DNS-сервер). Задать компьютерам и серверам IP-адреса из соответствующих диапазонов. Как и ранее, использовать для конечных устройств **максимальные** IP-адреса из доступных.

Настроить интерфейсы маршрутизаторов R0 и R1, используя **минимальные** IP-адреса из доступных. Использовать меньший адрес для маршрутизатора с меньшим порядковым номером.

ПРИМЕЧАНИЕ. IP-адрес на внешнем интерфейсе маршрутизатора R0 настраивать не нужно: он уже настроен.

Отредактировать содержимое веб-страницы на корпоративном веб-сервере, добавив следующие сведения: ФИО, номер группы, номер варианта.

Выполнить первоначальную настройку маршрутизаторов (присвоить символьные имена, задать пароли для доступа к консоли, привилегированному режиму и виртуальному терминалу, включить шифрование всех паролей и добавить баннер). *Подробнее о первоначальной настройке устройств см. методические рекомендации к лабораторной работе №1.*

Используя команды проверки конфигурации (show), убедиться в правильности введенных настроек. Адреса устройств занести в отчет.

6.3.2. Настройка маршрутизации

Настройка маршрутизации в данном сценарии выполняется статическими методами. *Подробнее о настройке статической маршрутизации см. методические рекомендации к лабораторной работе №3*.

Поскольку сеть LAN A является тупиковой, маршрутизатор R1 имеет единственный выход во внешние сети через R0. Следовательно, на R1 необходимо настроить статический маршрут по умолчанию, указывающий в направлении R0.

Аналогично, ветви сетей B и C являются тупиковыми, и маршрутизатор R0 имеет единственный выход и Интернет через маршрутизатор ISP (расположен в кластере Internet). Следовательно, на R0 необходимо также настроить статический маршрут по умолчанию, указывающий в направлении ISP.

ПРИМЕЧАНИЕ. Маршрут до LAN A на маршрутизаторе R0 добавлять не нужно. Проблема доступности устройств LAN A с маршрутизатора R0 будет решена иначе – с помощью NAT.

Используя команды проверки конфигурации (show), убедиться в правильности введенных настроек. TCP echo запросы (ping) для диагностики использовать не следует: до настройки трансляции адресов они проходить не будут.

6.3.3. Настройка NAT

Устройства LAN A имеют адреса из диапазона 192.168.0.0/16. Эти адреса являются внутренними. По сценарию лабораторной работы они используются только внутри сети LAN A и не маршрутизируются даже внутри моделируемой корпоративной сети. Для их выхода за пределы домашней сети необходимо настроить на R1 динамическое отображение этих (внутренних для LAN A) адресов в адреса корпоративной сети. Корпоративная сеть имеет адресацию в диапазоне 172.16.0.0/12 (см. LAN B, LAN C) – это следует учесть при настройке преобразования. *Будьте внимательны при выборе глобальных адресов для трансляции!*

Пошаговая инструкция по настройке:

1) Создать ACL для отбора сетевых пакетов, подлежащих трансляции.
2) Создать пул адресов, которые будут являться глобальными.
3) Создать NAT-отображение, связав созданные ACL и пул адресов.
4) Пометить внешний и внутренний интерфейсы директивами NAT.

Используя команды проверки конфигурации (show), tcp echo запросы и веб-браузеры компьютеров, убедиться в правильности введенных настроек.

На данном этапе должна работать связь между устройствами в пределах корпоративной сети (LAN A, LAN B, LAN C). Проследить этапы обработки пакетов в режиме симуляции. *Обратите внимание на преобразование адресов!* Полученные результаты занести в отчет.

Осталось настроить доступ в Интернет и обратно.

R0 является внешним шлюзом для моделируемой корпоративной сети. Поскольку в сети Интернет внутренние адреса корпоративной сети из диапазона 172.16.0.0/12 не маршрутизируются, необходимо настроить на R0 NAT-отображение для таких адресов. Используем PAT – перегруженный динамический NAT.

Пошаговая инструкция по настройке:

1) Создать ACL для отбора сетевых пакетов, подлежащих трансляции.
2) Создать NAT-отображение, связав созданный ACL и внешний интерфейс.
3) Пометить интерфейсы директивами NAT.

Заметим, что в сети LAN B расположены два сервера, к которым необходимо разрешить внешний доступ из сети Интернет (в противном случае сайт организации не будет виден из Интернета). Для этого необходимо обеспечить указанным серверам постоянные уникальные внешние (глобальные) IP-адреса. Перегруженный режим NAT не позволяет решить эту проблему. Для ее решения воспользуемся статическим NAT и создадим соответствующие отображения для каждого из серверов. *Глобальные адреса серверов неизвестны! Узнайте их самостоятельно по известным доменным именам:www.corp.com, ns.corp.com.*

ПРИМЕЧАНИЕ. Основной инструмент диагностики системы доменных имен – утилита nslookup. Для ее запуска необходимо выполнить одноименную команду в командной строке операционной системы (для Windows и в Packet Tracer – в приложении Command Prompt).

Заметим, что для доступа к указанным серверам с устройств, расположенных в пределах корпоративной сети, необходимо использовать внутренние адреса серверов. Занесите их в базу данных корпоративного DNS-сервера.

Настойка завершена. Используя команды проверки конфигурации (show), tcp echo запросы (ping) и веб-браузеры компьютеров, убедиться в правильности введенных настроек. На данном этапе должна работать связь между всеми устройствами корпоративной сети и сети Интернет, за исключением отдельных tcp echo запросов. *Каких именно и почему?* Сайты

www.corp.com и internet.com должны быть доступны из Интернета и из корпоративной сети.

6.3.4. Анализ пакета в режиме симуляции

Перейти в режим simulation и настроить фильтр пакетов.

С помощью веб-браузера на компьютере PC0 открыть сайты www.corp.com и internet.com и проследить за прохождением пакетов по сети, изменением адресов в заголовках сетевого уровня. Полученные данные и выводы занести в отчет.

ПРИМЕЧАНИЯ.

1. При анализе прохождения пакета через маршрутизатор следует добавлять в таблицу по две строки: для входного и выходного интерфейсов.

2. Поскольку в задании требуется провести анализ пакетов на сетевом уровне, коммутаторы можно пропустить.

3. Столбец «Тип NAT» необходимо заполнять только в тех строках, где происходит преобразование адресов.

Повторить анализ для пакетов, возникающих при обращении к указанным серверам с узлов PC2 и InetUsr. Полученные данные и выводы занести в отчет.

6.4. Контрольные вопросы

1. Как и кем регулируется пространство IPv4-адресов?
2. Чем обусловлена нехватка IPv4-адресов?
3. Какие технологии позволяют снизить остроту нехватки IPv4-адресов?
4. Какие IP-адреса называют частными? Для чего они предназначены?
5. Что такое трансляция сетевых адресов? Для чего она используется?
6. Какие сведения хранятся в таблице NAT?
7. Какие типы адресов существуют в контексте трансляции? Чем они отличаются?
8. Как работает трансляция адресов? Каков порядок обработки пакета NAT-маршрутизатором?
9. Какие существуют режимы работы NAT? Чем они отличаются? Какова область применения каждого из них?
10. Что такое пул адресов в контексте NAT? В чем отличие от пула адресов DHCP?
11. Для чего предназначены ACL в контексте NAT? Как следует понимать правила permit и deny в таких ACL?

12. Почему необходимо маркировать интерфейсы NAT-маршрутизатора как внешние и внутренние?
13. Как обеспечить доступность устройств, использующих частные IP-адреса, извне домашней сети? Какие режимы NAT для этого подходят?
14. Для чего предназначен протокол DHCP? Каков его принцип работы?

6.5. Варианты индивидуальных заданий

Варианты индивидуальных заданий указаны в разделе 6.3.1.

6.6. Форма отчета

Отчет о выполнении лабораторной работы оформляется в соответствии с индивидуальным вариантом задания и является обязательным требованием для допуска к защите наряду с правильно настроенным сценарием работы в программе Packet Tracer.

Отчет должен включать титульный лист, схему сети, а также заполненные таблицы, приведенные ниже.

6.6.1. Сведения о конфигурации устройств

Устр-во	Интерфейс	IP-адрес	Маска подсети	Шлюз
R1				
R0				
PC 0	NIC			
PC 1	NIC			
PC 2	NIC			
CorpWeb	NIC			
CorpDNS	NIC			
InetUsr	NIC			
InetSrv	NIC			

6.6.2. Сведения о настроенных NAT

Устр-во	Интер-фейс inside	Интер-фейс outside	Команды конфигурирования NAT (включая пул и ACL)
R1			

R0			

6.6.3. Анализ пакетов в режиме симуляции

PC0 – www.corp.com

На устройстве	Source IP	Destination IP	Тип NAT

PC0 – internet.com

На устройстве	Source IP	Destination IP	Тип NAT

PC2 – www.corp.com

На устройстве	Source IP	Destination IP	Тип NAT

PC2 – internet.com

На устройстве	Source IP	Destination IP	Тип NAT

InetUsr – www.corp.com

На устройстве	Source IP	Destination IP	Тип NAT

InetUsr – internet.com

На устройстве	Source IP	Destination IP	Тип NAT