**ЛАБОРАТОРНАЯ РАБОТА №9**

Тема: Использование NAT

Цель работы: изучить особенности трансляции сетевых адресов с помощью технологии NAT

Ход работы

Задание 1

Расположены и соединены оборудования (Рисунок 1.1).

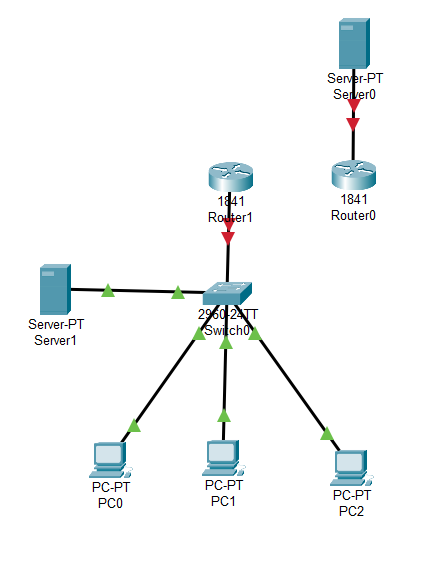


Рисунок 1.1 – Построенная схема сети

Созданы 2 VLAN с именами users и server (Рисунок 1.2).

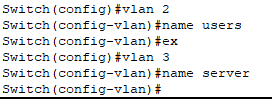


Рисунок 1.2 – Создание VLAN-ов

Присвоены каждому узлу сети отдельный VLAN (Рисунок 1.3).

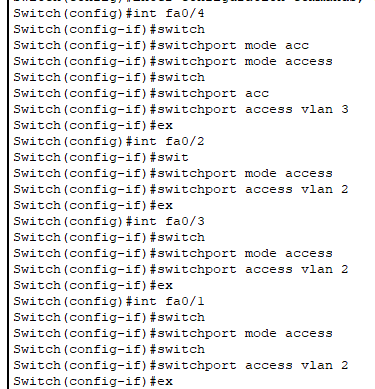


Рисунок 1.3 – Присвоение VLAN интерфейсам

Проверена правильность присвоения командой show run (Рисунок 1.4).

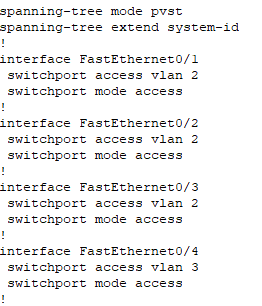


Рисунок 1.4 – Проверка правильности присвоения

Настроен интерфейс, ведущий к маршрутизатору как тегированный и включены в него созданные VLAN (Рисунок 1.5).

Рисунок 1.5 – Настроенный интерфейс Fa0/5 коммутатора

Включен интерфейс в маршрутизатора командой no shutdown (Рисунок 1.6).

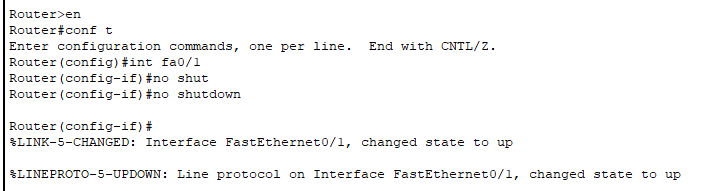


Рисунок 1.6 – Включение интерфейса

Включен субинтерфейс (Рисунок 1.7).

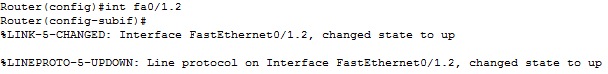


Рисунок 1.7 – Включение субинтерфейса

Применена для каждого субинтерфейса инкапсуляция и заданы ip-адреса (Рисунок 1.8).

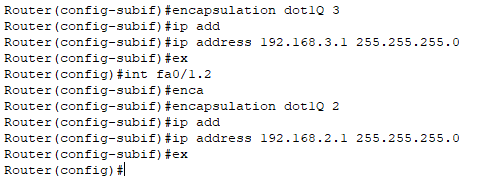


Рисунок 1.8 – Применение инкапсуляции и задание ip-адресов

Проверена правильность настроек командой show run (Рисунок 1.9).

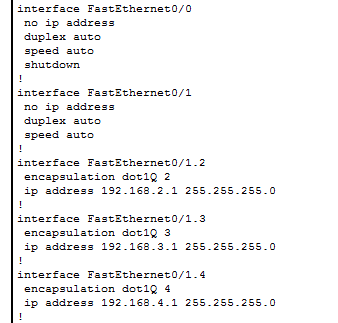


Рисунок 1.9 – Проверка правильности настроек

Заданы ПК ip-адреса, маски и основные шлюза.

Проверена работоспособность с помощью утилиты ping (Рисунок 1.10).

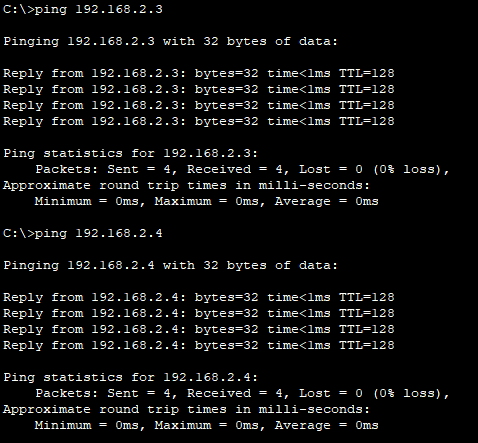


Рисунок 1.10 – Проверка работоспособности

Задание 2: Построена сеть с использованием маршрутизатора (Рисунок 2.1).

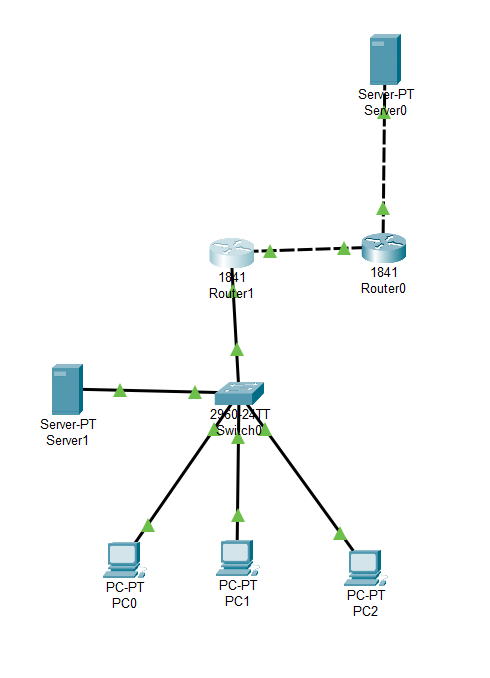


Рисунок 2.1 – Построенная схема сети

В маршрутизаторе провайдера заданы ip-адрес для интерфейсов (Рисунок 2.2).

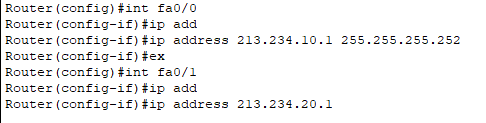


Рисунок 2.2 – Настройка интерфейсов маршрутизатора

Заданы соответствующие настройки и на самом сервере (Рисунок 2.3).

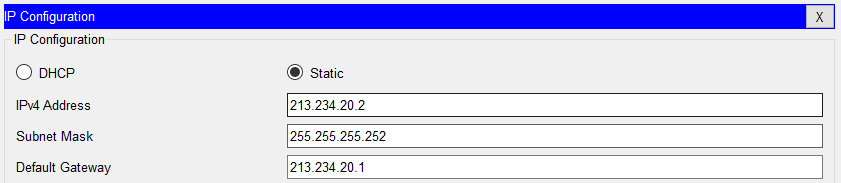


Рисунок 2.3 – Настройка сервера

Задан маршрутизатору в локальной сети тот же адрес и прописан маршрут по умолчанию к провайдеру (Рисунок 2.4).

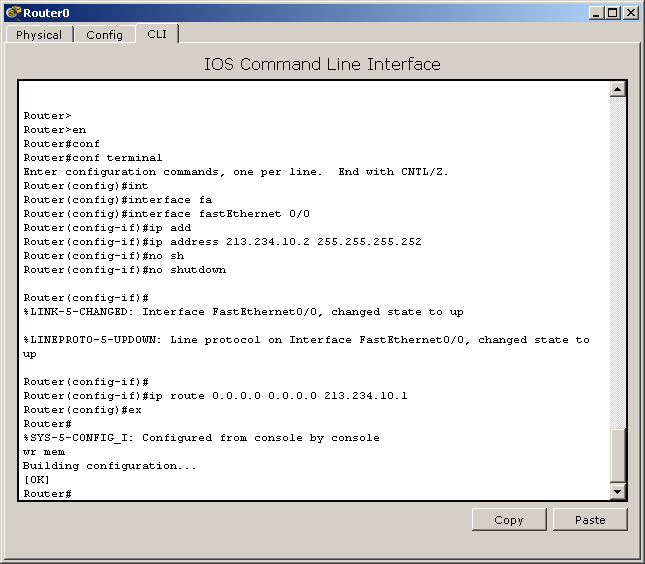


Рисунок 2.4 – Настройка маршрутизатора

Проверена доступность шлюза по умолчанию и сервера в интернете при помощи утилиты ping (Рисунок 2.5).

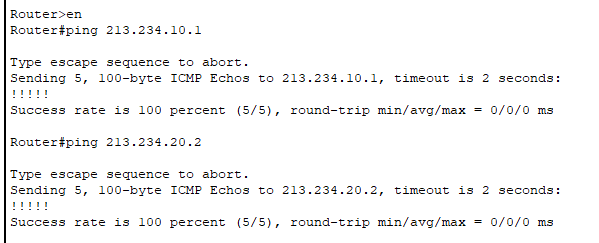


Рисунок 2.5 – Проверка работоспособности

Заданы параметры inside и outside соотвествующим интерфейсам с помощью команды ip nat (Рисунок 2.6).

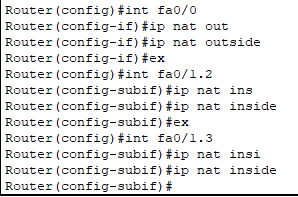


Рисунок 2.6 – Определение внешних и внутренних адресов

Создан Access-лист с именем FOR-NAT и заданы подсети для натирования (Рисунок 2.7).

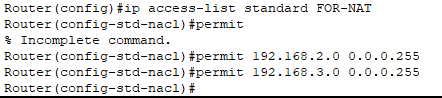


Рисунок 2.7 – Задание натируемых подсетей

Реализовано натирование изнутри локальной сети, а также определен PAT (Рисунок 2.8).

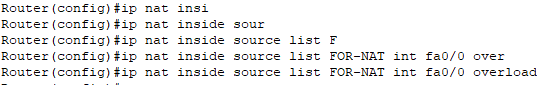


Рисунок 2.8 – Задание PAT

Проверена работоспобность NAT при помощи утилиты ping (Рисунок 2.9).

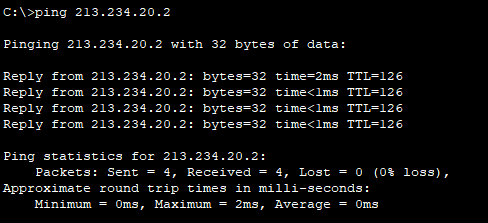


Рисунок 2.9 – Проверка работоспобности

Задание 3: Обеспечен доступ к локальному веб-серверу из глобальной сети с использованием Static NAT.

Изменен HTML-текст сайта, указав свою фамилию и группу (Рисунок 3.1).

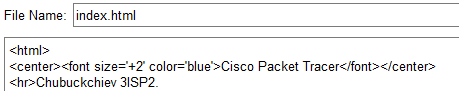


Рисунок 3.1 – Изменение HTML-текста сайта

Указан параметр static, записан протокол передачи, адрес и порт веб-сервера в локальной сети и адрес и порт интерфейса, ведущего во внешнюю сеть (Рисунок 3.2).

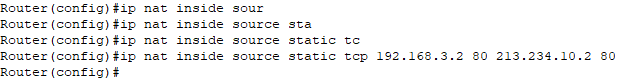


Рисунок 3.2 – Задание Static NAT

Получен сайт, внутри которого указанные ранее фамилия и группа (Рисунок 3.3).

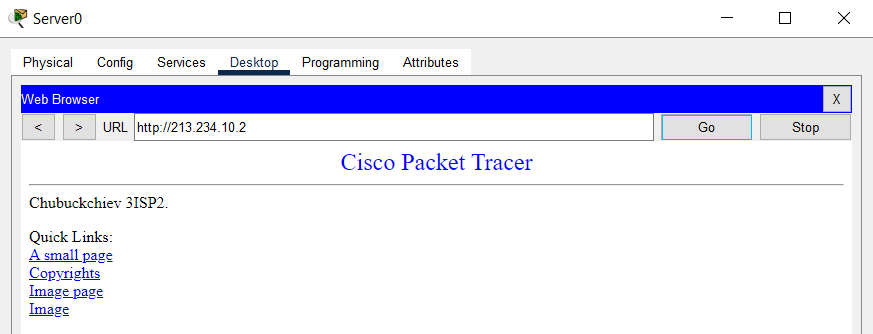


Рисунок 3.3 – Тест работоспобности веб-сервера

Задание 4

1. Какие устройства позволяют применять NAT?

Устройства, которые могут выполнять функции маршрутизации и имеют возможность изменять адреса в IP-пакетах, могут применять NAT. Это могут быть маршрутизаторы, межсетевые экраны (firewalls), прокси-серверы и другие сетевые устройства.

2. В чем суть технологии NAT?

Network Address Translation (NAT) — это технология, используемая для перевода IP-адресов из одной сети в другую. Основная цель NAT заключается в том, чтобы скрыть внутренние IP-адреса компьютеров в локальной сети за одним или несколькими общедоступными IP-адресами, которые используются для взаимодействия с внешними сетями, такими как Интернет.

3. Перечислите основные виды NAT:

– Static NAT (SNAT или 1:1 NAT): Происходит однозначное соответствие между внутренним и внешним IP-адресом, каждому внутреннему IP-адресу назначается свой уникальный внешний IP-адрес.

– Dynamic NAT: Внутренним устройствам назначаются внешние IP-адреса из пула доступных адресов при необходимости, и эти адреса освобождаются обратно в пул после завершения сеанса связи.

– PAT (Port Address Translation): Вид NAT, который позволяет использовать один общий внешний IP-адрес для нескольких внутренних устройств, используя уникальные комбинации IP-адреса и порта.

4. В каких случаях целесообразно использование статического NAT?

Статический NAT часто используется, когда необходимо обеспечить доступ к внутренним серверам или устройствам из внешней сети. Это может включать в себя сервера веб-сайтов, почтовые сервера или другие ресурсы, которые должны быть доступны из интернета по постоянным IP-адресам. Также статический NAT обеспечивает более предсказуемое и управляемое соответствие между внутренними и внешними адресами, что может быть полезно для некоторых видов сетевой конфигурации, таких как виртуальные частные сети (VPN) или сети с высокими требованиями к безопасности.

5. В чем преимущества PAT перед другими видами NAT?

Преимущества PAT (Port Address Translation) включают в себя эффективное использование доступных внешних IP-адресов путем назначения уникальных комбинаций IP-адресов и портов для внутренних устройств. Это позволяет обеспечить доступ к интернету для множества устройств, используя только один внешний IP-адрес. Также PAT обеспечивает повышенную безопасность, поскольку исходный IP-адрес в пакете скрыт, что затрудняет прямые атаки извне.

6. Перечислите преимущества и недостатки NAT:

Преимущества NAT:

– Скрытие внутренних IP-адресов для повышения безопасности сети.

– Экономия IP-адресов, так как несколько внутренних устройств могут использовать один общий внешний IP-адрес.

– Возможность использования частных IP-адресов внутри локальной сети.

Недостатки NAT:

– Увеличение сложности конфигурации и управления сетью.

– Возможные проблемы с поддержкой некоторых протоколов или услуг, таких как VoIP.

– Возможное ухудшение производительности из-за дополнительной обработки пакетов в сетевых устройствах.

7. В чем смысл NAT Loopback?

NAT Loopback (или NAT Reflection) - это технология, позволяющая устройствам внутри локальной сети обращаться к ресурсам по их внешнему IP-адресу, даже если они находятся внутри этой же сети. Это полезно, когда требуется доступ к ресурсам, которые обычно доступны только извне сети, например, к веб-серверу на маршрутизаторе.

8. Почему нецелесообразно использование динамического NAT?

Использование динамического NAT не всегда нецелесообразно, но в некоторых сценариях может возникнуть необходимость в управлении исходящими соединениями и ведении журнала соединений. Динамический NAT может также создать проблемы с доступом к определенным ресурсам из внешней сети, если устройство находится за NAT и использует динамический адрес.

9. Что такое destination NAT и в чем его отличия от Source NAT?

Destination NAT (DNAT) изменяет адрес назначения входящих пакетов, перенаправляя их на другие устройства или службы внутри сети. Source NAT (SNAT), с другой стороны, изменяет адрес отправителя в исходящих пакетах, обычно для того чтобы скрыть источник соединения. Таким образом, DNAT изменяет адрес назначения, а SNAT изменяет адрес отправителя.