Практическая работа № 6.

Трансляция адресов (NAT) в Cisco Packet Tracer.

Цель работы:

Закрепить понимание принципов работы NAT, а также сформировать начальные навыки в конфигурировании NAT и Firewall в Cisco Packet Tracer.

Краткие теоретические сведения.

NAT (Network Address Translation) – технология стека TCP\IP. Она позволяет модифицировать заголовки пересылаемых через NAT IP-пакетов и TCP\UDP сообщений.

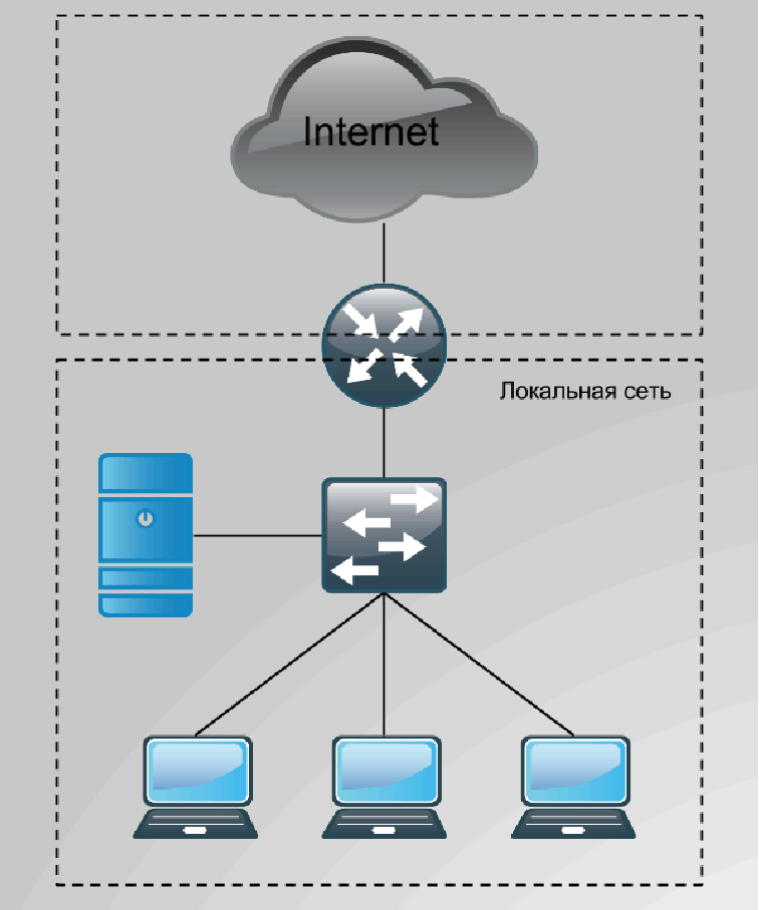
NAT в общем случае представляет собой компьютер или аппаратный маршрутизатор, подключенный одним интерфейсом к внешней сети, а другими к внутренней. Оба интерфейса имеют IP адреса в каждой из сетей. Типичным применением NAT является обеспечение доступа из локальной сети с приватными IP-адресами к ресурсам внешней сети с IP-адресами интернет. При передаче запроса от локального клиента к внешнему ресурсу подменяется сокет отправителя: IP адрес меняется на внешний IP адрес NAT, а порт на свободный порт на внешнем интерфейсе NAT. Когда приходит ответ от внешнего ресурса, происходит обратная замена сокета и пакет передается в локальную сеть получателю. Так же с помощью NAT можно публиковать локальные сокеты на реальном IP адресе и реальном порту. Например, для обеспечения доступа извне к Web серверу, расположенному в локальной сети. В этом случае на NAT делается статическое отображение внешнего сокета на внутренний.

Публичный IP адрес (Белый IP) - адрес-это глобально маршрутизируемый одноадресный IP-адрес, что означает, что этот адрес не является адресом, зарезервированным для использования в частных сетях, таких как сети, зарезервированные RFC 1918, или различные форматы адресов IPv6 локальной области или локальной области сайта, например для локальной адресации канала

Частный IP адрес (Серый IP) -

- От 10.0.0.0 до 10.255.255.255 с маской 255.0.0.0.0 (сеть класса A - около 16 млн. адресов)
- От 172.16.0.0 до 172.31.255.255 с маской 255.240.0.0 (сеть класса B - около 65 тыс. адресов)
- От 192.168.0.0 до 192.168.255.255 с маской 255.255.255.0 (сеть класса C - около 256 адресов)

.



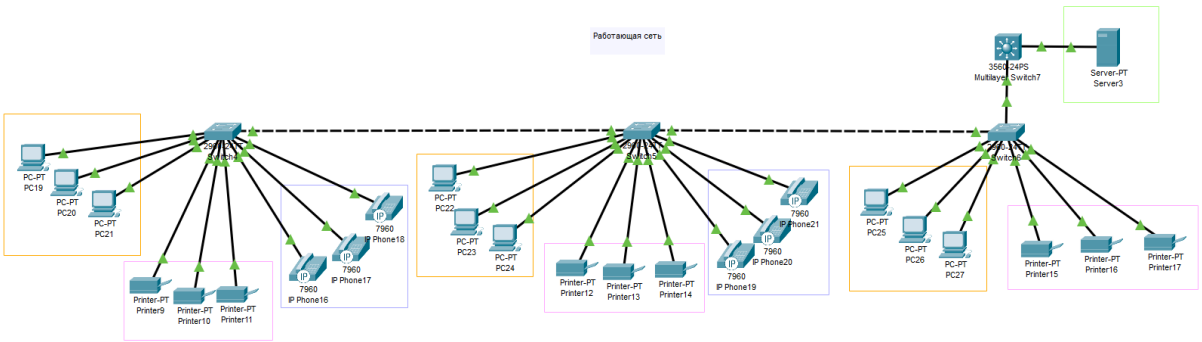
Требования:

для выполнения работы необходима установка симулятора CISCO PacketTracer.

Задание к лабораторной работе

1. Добавление эмуляции сервера в сети Интернет к существующей сети.

1. Запустите лабораторную работу 3.

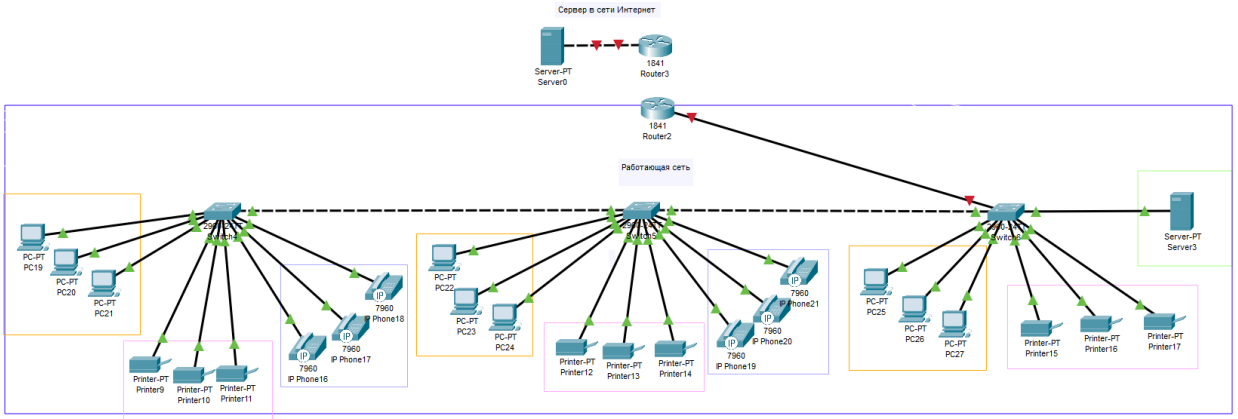


2. Добавьте в неё:

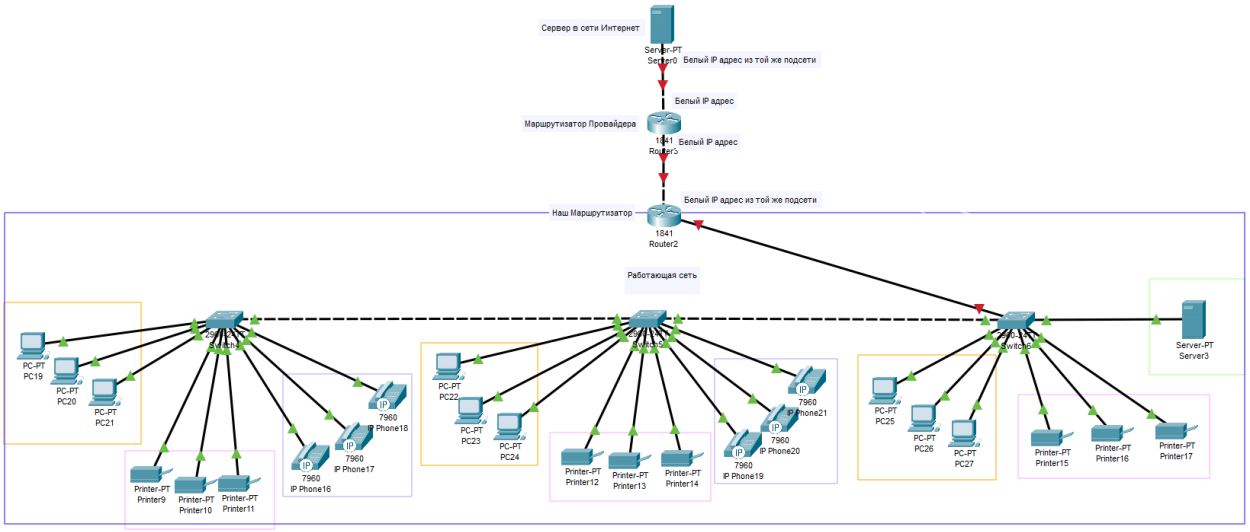
- Маршрутизатор, который маршрутизирует трафик из существующей сети наружу
- Сервер, эмулирующий сервер в сети Интернет

- Маршрутизатор, который эмулирует провайдера.

3. При желании удалите коммутатор 3 уровня, поскольку он не нужен, ведь теперь трафик может маршрутизироваться маршрутизатором. В таком случае VLAN'ы будут приземляться на машртутизаторе, поэтому порт коммутатора L2, который подсоединяется к маршрутизатору, будет trunk. И в таком случае на маршрутизаторе нужно создавать сабинтерфейсы для соответствующих VLAN.



4. Промоделируйте подключение к сети Интернет: обратитесь к провайдеру и он вам прокинет линк и выдаст белый статический IP адрес. Мы эмулируем интернет посредством роутера и сервера, у которых будут публичные белые IP адреса (любой, префикс маски может быть /30). У провайдера к нам будет белый IP адрес, к серверу будет другой белый IP адрес и у сервера будет белый IP адрес из той же подсети, что и к серверу. Пропишите на порте вашего маршрутизатора белый IP адрес, который вам выделил провайдер, из той же сети провайдера. Настройте шлюз по умолчанию на нашем маршрутизаторе – это будет адрес провайдера.



2. Настройка PAT

1. Если мы пропингуем Интернет сервер из компьютера нашей сети, то он не пропингуется, потому что компьютеры нашей сети используют серые адреса и маршрутизатор

провайдера не знает про наши сети. С помощью NAT обеспечим доступ нашим компьютерам в сеть Интернет (к серверу).

2. Сначала нужно определиться, какой интерфейс маршрутизатора провайдера будет являться внешним, а какой внутренним. К внешнему интерфейсу нужно применить команду ip nat outside, а к внутреннему ip nat inside. Необходимо учесть, что внутренних интерфейсов несколько, по количеству VLAN, но доступ в Интернет нужен только компьютерам, ноутбукам и серверу.
3. Необходимо создать access list'ы, чтобы определить, какой трафик должны пропускать через NAT, с помощью команды ip accesslist standard <ИМЯ_ЛИСТА>, permit (IP адрес VLAN сети 1, wildcard маска VLAN сети 1), permit (IP адрес VLAN сети 2, wildcard маска VLAN сети 2) и т.д.
4. Настраивайте NAT с помощью команды ip nat inside source list <ИМЯ_ЛИСТА> interface <ИМЯ_ИНТЕРФЕЙСА_OUTSIDE> overload;
5. Проверьте работу NAT с помощью команды show ip nat translations

3. Статический NAT

1. Необходимо обеспечить доступ из Интернет в наш локальный сервер.
2. Настройте уникальный внешний вид страницы HTTP сервера, для создания уникальности лабораторной работы.
3. Настройте ваш маршрутизатор для обеспечения доступа из Интернет в наш локальный сервер. Настройте статический NAT командой ip nat inside source static tcp <внутренний адрес нашего сервера> <80 – порт HTTP> <внешний IP адрес, который на маршрутизаторе> <80 – порт HTTP>;
4. Сохраните настройки командой wr mem.
5. Проверьте работоспособность.

Содержание отчета

Требуется подготовить отчет в формате DOC\DOCX или PDF, а также файл модели CPT. Отчет содержит

1. Титульный лист
2. Задание на лабораторную работу
3. Пункты выполнения работы, в соответствии с заданием с подробными пояснениями и комментариями.
4. Карта сети и конфигурационных файлов устройств (скриншоты).
5. Работоспособность Вашей сети необходимо продемонстрировать преподавателю на

компьютере.

Отчет выслать в течение 4-х недель (минус 1 день) на адрес akharitonov@itmo.ru. Если отчет будет выслан позже, то защита будет с понижением оценки.

В теме письма: №группы ФИО (латинскими буквами) №работы (например: 5555 Fedor Sumkin 6)

Понятийный минимум по работе

1. NAT - Network Address Translation
2. Публичный IP адрес
3. Частный IP адрес
4. Статический NAT
5. Динамический NAT
6. Перегруженный NAT

Материалы для работы

https://youtu.be/6d2kvuWuyI0?feature=shared

Курс молодого бойца, раздел NAT

https://youtu.be/4tDCKgJWr-I?feature=shared

Configuring DHCP and NAT

https://habr.com/ru/articles/583172/

NAT (Network Address Translation) для новичков