Министерство образования и науки Российской Федерации

Московский Государственный Технический Университет
им. Н.Э. Баумана

Факультет «Информатика и системы управления»
Кафедра «Компьютерные системы и сети»

Сурков Л.В.

Методические указания
к лабораторной работе по курсу
Корпоративные сети

Раздел
Построение защищенных сетей с использованием брандмауэров

Технология Network Address Translation.

2011

Технология Network Address Translation.

Теоретические основы.
Обзор трансляции адресов

Трансляция сетевых адресов – технология преобразования адресов и/или портов источника и/или получателя IP-пакета. Эти преобразования отслеживаются в соответствующих таблицах, что позволяет при получении ответного пакета выполнить обратную трансляцию адреса/порта. Технология NAT имеет два важных достоинства:

1. При NAT-адресации внутренние хосты могут совместно использовать один или несколько зарегистрированных внешних IP-адресов. При этом требуется относительно немного внешних адресов для поддержки большого числа внутренних хостов, что экономит IP-адреса.
2. NAT позволяет маскировать (скрыть) внутреннюю структуру локальной сети. За счёт выполнения трансляции адресов запросы компьютеров локальной сети к внешним хостам выглядят так, будто выполняются с одного и того же компьютера. Также можно с помощью трансляции адреса совместно с портом осуществлять сокрытие серверной инфраструктуры.

Важно отметить, что некоторые протоколы не поддерживают трансляцию адресов (например, PPTP), либо использование трансляции накладывает ограничения на использование некоторых служб. Для обхода таких проблем NAT-маршрутизатор должен иметь возможность разбирать пакеты, вносить изменения и собирать их снова;

Различают два способа трансляции адресов:

- Network Address Translation (NAT) – замена адреса источника на адрес маршрутизатора. При этом порт остаётся неизменным.
- Static Address Translation (SAT) – замена адрес источника или приёмника на некоторый адрес, при этом возможна одновременная замена порта.

  SAT подразделяется на два типа:
  - Source SAT – трансляция внутреннего адреса источника (*Inside local*) в зарегистрированный адрес источника (*Inside global*).
  - Destination SAT – трансляция внешнего адреса назначения (*Outside local)* в адрес назначения (*Outside global).*

Адресация NAT обычно функционирует на маршрутизаторе Cisco, соединяя две сети и транслируя частные локальные адреса внутренней сети в открытые зарегистрированные адреса внешней сети и обратно. Как показано на рисунке 1, внутреннему узлу требуется обменяться данными с внешним узлом (128.23.2.2).

NAT выполняет преобразование локального адреса (10.0.0.2) в глобальный (179.9.8.80) и сохраняет это в своей NAT-таблице. Аналогично внутренний адрес (10.0.0.3) преобразуется в глобальный (179.9.8.81).

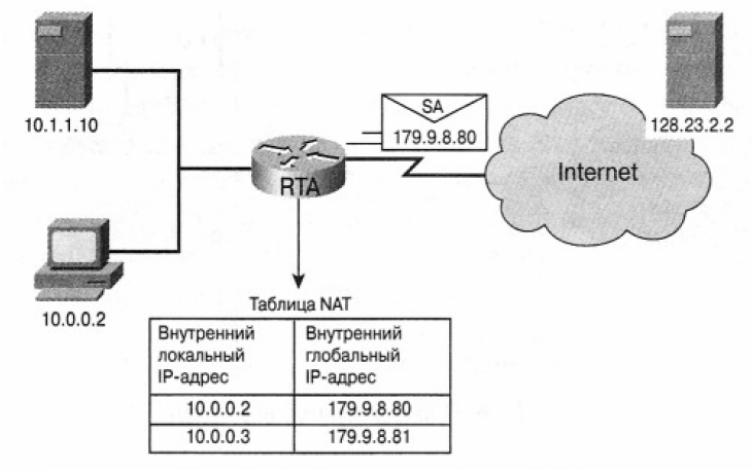


Рис.1. Адресная таблица NAT

NAT принимает ответный пакет, направленный из внешней сети во внутреннюю, просматривает свою адресную таблицу для нахождения преобразования данного глобального адреса в локальный. Такая статическая NAT-адресация взаимного однозначного преобразования локальных и глобальных адресов (адрес - адрес) обычно используется для внутренних IP-узлов, которые должны быть постоянно доступны из внешей сети (например, Internet), таких как сервер DNS или сервер электронной почты (e-mail server).

Адресация NAT может быть сконфигурирована для представления только одного внешнего адреса для всей внутренней сети с помощью однозначного преобразования номеров портов (много адресов – один адрес с назначенным портом). Эта функция адресации NAT называется PAT (Port Address Translation). Такой способ эффективно скрывает внутреннюю структуру сети от внешней сети и повышает уровень безопасности.

Использование адресации NAT позволяет выполнить трансляцию ряда внутренних адресов, в то время как PAT может транслировать лишь один или несколько внешних адресов. Как показано на рисунке 2, хосты 10.0.0.2 и 10.0.0.3 посылают пакеты во внешнюю сеть, используя один IP-адрес 179.9.8.80 и разные порты.

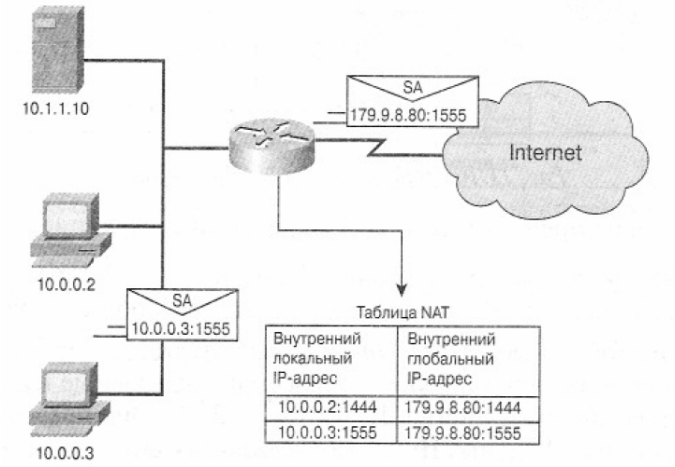


Рисунок 2. Таблица NAT/PAT

Поскольку номер порта записывается двумя байтами, общее количество внутренних адресов, которые могут быть транслированы в один внешний адрес, при использовании PAT теоретически может достигать 65 536 для каждого IP-адреса. PAT пытается сохранить первоначальный порт источника. Если порт источника уже присвоен, то адресация PAT пытается найти первый доступный номер порта в

соответствующей группе портов 0-511, 512-1023 или 1024-65535. Если в соответствующей группе нет доступных портов и конфигурируется более одного IP-адреса, то PAT переходит к следующему IP-адресу и пытается вновь найти первоначальный порт источника. Это процесс продолжается до тех пор, пока PAT не исчерпает доступные порты и внешние IP-адреса.

Cisco определила для NAT-адресации следующие термины.

- Внутренние локальные адреса *(Inside local address)* — IP-адреса, назначенные хосту во внутренней сети, соответствующие RFC 1918.
- Внутренние глобальные адреса *(Inside global address)* —зарегистрированные IP-адреса, назначаемые провайдером службы или выделяемые из регионального регистра Internet (Regional Internet Registries, RIR). Они предоставляют один или более внутренних локальных IP-адресов для связи с внешней сетевой средой.
- Внешние локальные адреса *(Outside local address)* — IP-адреса внешних узлов, в том виде как они известны узлам внутренней сети.
- Внешние глобальные адреса *(Outside global address)* — IP-адрес, назначаемый владельцем узла, этому узлу для использования во внешней сети.

Конфигурирование NAT и PAT

В настоящем разделе рассматриваются следующие вопросы конфигурирования.

- Статическая трансляция;
- Динамическая трансляция;
- Перезагрузка NAT (PAT).

Статическая трансляция

Под статической трансляцией понимается ручное конфигурирование адресов в просмотровой таблице. Для каждого внутреннего локального адреса при использовании статической NAT требуется внутренний глобальный адрес. Для того, чтобы сконфигурировать статическую трансляцию внутреннего адреса, требуется выполнить действия, описанные ниже.

1. Задать статическую трансляцию внутреннего локального адреса во внутренний глобальный адрес.

Router (config)#**ip nat inside source static** *local-ip global-ip*

2. Задать внутренний интерфейс и указать его, как принадлежащий к внутренней сети

Router (config)#**interface** *type number*
Router (config-if)#**ip nat inside**

3. Задать выходной интерфейс и указать его, как подсоединенный извне

Router (config)**#interface** *type number*
Router(config-if*)***#ip nat outside**

Пример статической NAT-адресации:

```
hostname GW
!
ip nat inside source static 10.1.1. 2 192.168.1.2
!
interface Ethernet0
ip address 10.1.1.1 255.255.255.0
ip nat inside
!
interface Serial0
ip address 192.168.1.1 255.255.255.0
ip nat outside
!
ip nat inside source static 10.1.1.2 192.168.1.2
```

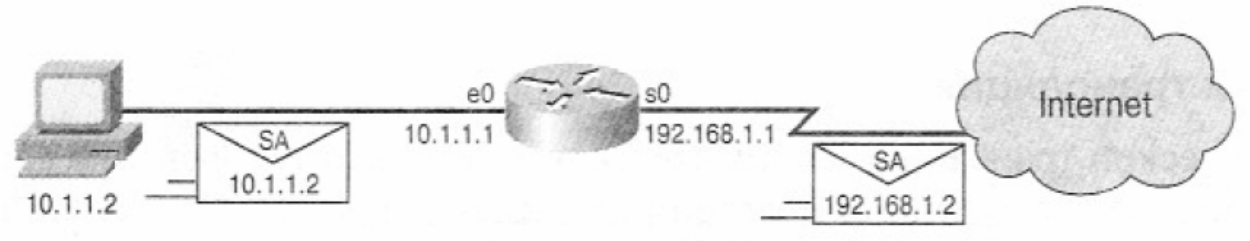


Рисунок 3. Статическая NAT-адресация:

Динамическая трансляция адресов

При использовании динамической трансляции адресов преобразования адресов не существуют в NAT-таблице до тех пор, пока маршрутизатор не получит данные, для которых такая трансляция требуется. Динамические преобразования адресов являются временными и в конечном итоге устаревают и удаляются. Для того, чтобы сконфигурировать трансляцию внутренних адресов, следует выполнить действия, описанные ниже.

1. Задать пул глобальных адресов, которые будут использоваться по мере необходимости.

Router (config)#**ip nat pool** *имя нач-ip конеч-ip* **{netmask** *маска* **| prefix-length** *длина-префикса***}**

2. Создать стандартный список доступа для идентификации тех адресов, которые нужно будет транслировать.

Router (config)#**access-list** *номер-списка* **permit** *источник* [шаблон-источник]

3. Сконфигурировать динамический NAT на основе адресов источника

Router (config)#**ip nat inside source list** *номер-списка-дост* **pool** *имя*

4.Указать внутренний интерфейс

Router (config)#**interface** *type number*
Router (config-if)#**ip nat inside**

5. Указать внешний интерфейс

Router (config)**#interface** *type number*

Router(config-if)**#ip nat outside**

Список доступа должен определять только те адреса, которые следует транслировать. Следует помнить о том, что неявная команда deny all присутствует в каждом списке доступа. Недостаточно строгий список доступа может привести к непредсказуемым результатам. Рекомендуется не конфигурировать списки доступа, на которые ссылаются команды NAT с **permit any** (т.е. разрешить трансляцию для всех). Использование permit any может привести к тому, что NAT будет потреблять слишком много ресурсов маршрутизатора, что может вызвать проблемы в сети.
Приведенные ниже команды конфигурируют соответствующие интерфейсы для выполнения внутренних и внешних функций.

Пример динамической NAT-адресации:

```
ip nat pool nat-pool1 179.9.8.80 179.9.8.95 netmask 255.255.255.0
ip nat inside source list 1 pool nat-pool1
!
interface fastethernet0/0
ip address 10.1.1.1 255.255.255.0
ip nat inside
!
interface Serial0/0
ip address 192.168.1.1 255.255.255.0
ip nat outside
!
```

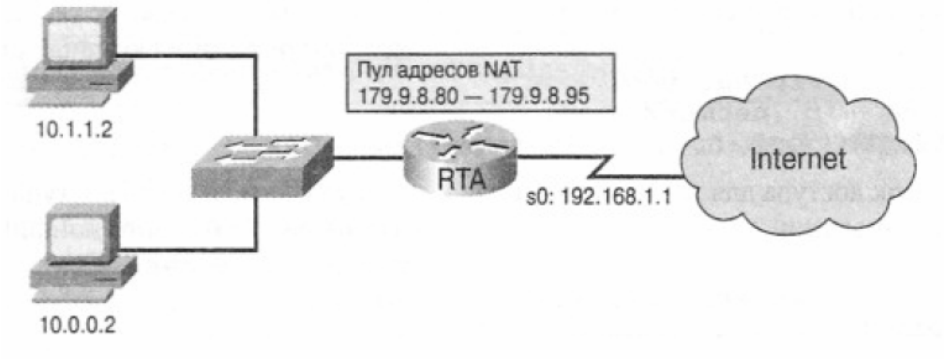


Рисунок 4.. Динамическая NAT-адресация.

В примере происходит трансляция всех адресов, проходящих через список доступа 1 (имеющие адрес источника от 10.0.0.0/16) в адрес из пула с именем *nat-pool.* Этот пул содержит адреса из диапазона от 179.9.8.80/28 до 179.9.8.95/28.

Перезагрузка NAT

Одной из наиболее мощных функций NAT является способность использовать PAT. Это иногда называется NAT-адресацией "много-в-один" или перегрузкой адреса. При использовании перегрузки *(overloading)* сотни узлов с частными адресами могут получать доступ к внешней сети (Internet), используя лишь один глобальный адрес. NAT-маршрутизатор отслеживает различные сеансы связи, устанавливая соответствие TCP и UDP номеров портов в таблице трансляции.

Для того, чтобы сконфигурировать перегрузку внутренних глобальных адресов, следует выполнить действия, описанные ниже.

1. Определить стандартный список доступа, разрешающий те адреса, которые должны транслирроваться

Router (config)#**access-list** *номер-списка* **permit** *источник* [шаблон-источник]

2. Сконфигурировать динамический NAT на основе адресов источников, указать список доступа, определенный на предыдущем этапе.

Router (config)#**ip nat inside source list** *номер-списка-дост* **interface** *интерфейс* **overload**

3. Задать набор глобальных адресов, которые будут использоваться для перезагрузки.

Router (config)#**ip nat pool** *имя ip-адрес* **{netmask** *маска* **| prefix-length** *длина-префикса***}**

4. Задать трансляцию с перезагрузкой.

Router (config)#**ip nat inside source list** *номер-списка-дост* **pool** *имя* **overload**

5.Указать внутренний интерфейс

Router (config)#**interface** *type number*
Router (config-if)#**ip nat inside**

6. Указать внешний интерфейс

Router (config)**#interface** *type number*
Router(config-if*)***#ip nat outside**

Пример перезагрузки NAT

1. Перезагрузка на интерфейсе.

```
Router(config)#access-list 1 permit 10.0.0.0 0.0.255.255
Router(config)#ip nat inside source list 1 interface serial0/0 overload
Router(config)#interface s0
Router(config-if)#ip nat outside
Router(config-if)#interface ethernet 0
Router(config-if)#ip nat inside
```

2. Перезагрузка с использованием пула.

```
Router(config)#access-list 1 permit 10.0.0.0 0.0.255.255
Router(config)#ip nat pool nat-pool2 179.9.8.20 netmask
255.255.255.240
Router(config)#ip nat inside source list 1pool nat-pool2 overload
Router(config)#interface s0
Router(config-if)#ip nat outside
Router(config-if)#interface ethernet 0
Router(config-if)#ip nat inside
```

Информация о трансляции.

show ip nat translation	Отображает активные сеансы трансляции адресов
show ip nat statistics	Отображает статистику трансляций

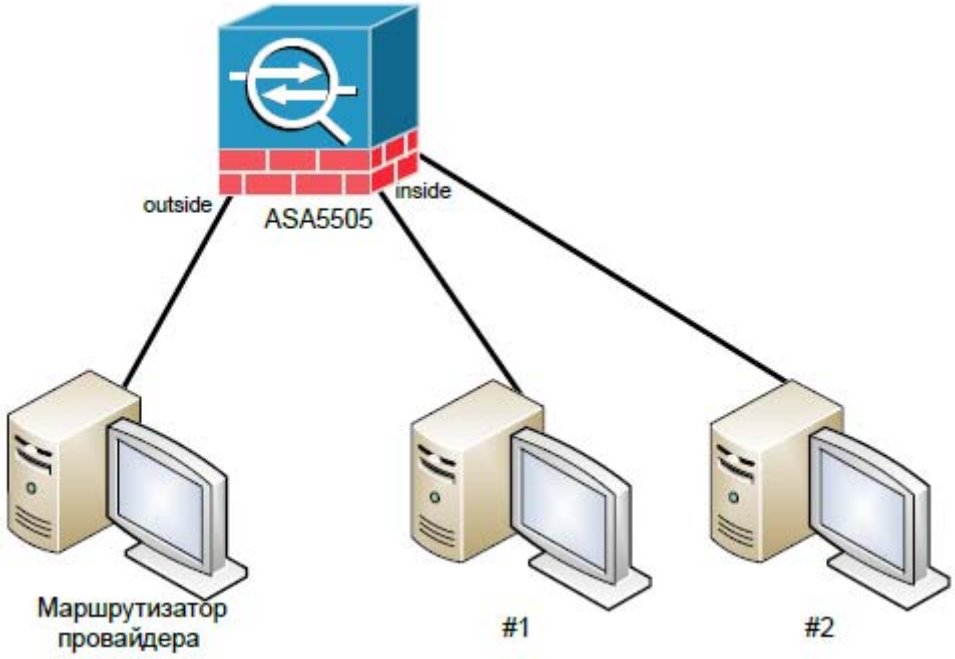
Поиск и устранение ошибок

Для тестирования функций NAT используется команда **debug ip nat,** которая отображает информацию обо всех пакетах, транслируемых маршрутизатором. По команде **debug ip nat** *detailed* выводится описание каждого пакета, для которого предполагается трансляция. При этом также выводится информация об определенных ошибках или исключительных условиях, таких, например, как невозможность выделить глобальный адрес. Команда **debug** сильно нагружает маршрутизатор – не злоупотребляйте ей и отключайте её, как только закончили поиск ошибок.

Практическая часть

Цель работы:

Изучение технологии NAT и способов её настройки на брандмауэре ASA5505.



Рисунок

Порядок выполнения работы:

1. Соберите топологию сети, представленную на рисунке

2. Настройте рабочие станции и брандмауэр таким образом, чтобы интерфейс outside ASA5505 и маршрутизатор провайдера принадлежали одной IP-подсети, а интерфейс inside ASA5505 и машины #1 и #2 – другой.

3. Настройте и запустите на маршрутизаторе провайдера веб-сервер.

4. Настройте NAT на ASA5505.

5. Одновременно осуществите обращение с машин #1 и #2 к веб-серверу провайдера.

6. Если попытка успешна (получена стартовая страница Apache), то запустите на машине провайдера утилиту *tcpdump* и снова осуществите запрос к веб-серверу с машин локальной сети.

7. Проанализируйте результаты, выдаваемые утилитой *tcpdump* и ответьте на вопрос:
какой IP-адрес и номер порта стоит в адресе отправителя запросов, получаемых веб- сервером.

Литература

1. James Boney, Cisco IOS in a Nutshell, 2-nd Ed., O`Reilly, 2008

2. Wendell Odom, Interconnecting Networking Devices Cisco, Part 2, Cisco Press, 2008

3. НПП «Учтех-Профи», ОС Arch Linux, Лабораторный практикум, Челябинск, 2010