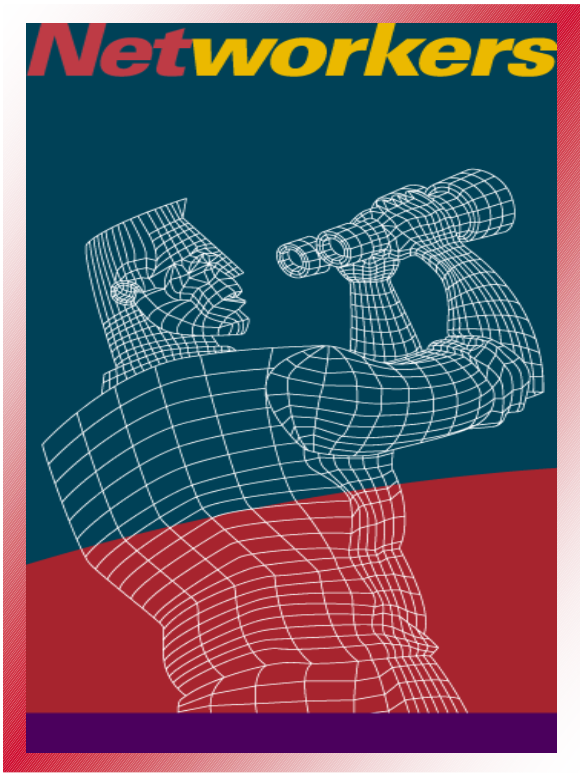
PLUS COMMUNICATIONS

Cisco Systems Russia
113054, Москва, Россия,
Космодамианская наб., 52
тел.: +7(095)961-1410
факс: +7(095)961-1469
http://www.cisco.com

PLUS Communications
109180, Москва, Россия,
1-й Хвостов пер., 11-А
тел.: +7 (095) 238-3711
факс: +7 (095) 238-3777
http://www.pluscom.ru

Cisco IOS
Конфигурирование функций
Network Address Translation



МОСКВА, 1999

Содержание

Введение 4
Применение NAT в современных бизнес-сетях 4
Преимущества NAT 4
Терминология NAT 5
Действия, выполняемые при настройке NAT 5
Трансляция внутренних адресов Source 6
  Конфигурация статической трансляции 7
  Конфигурация динамической трансляции 7
Использование одного внутреннего глобального адреса 8
Трансляция перекрывающихся адресов 9
  Конфигурирование статической трансляции 10
  Конфигурирование динамической трансляции 11
Обеспечение распределения нагрузки TCP 11
Изменение тайм-аутов трансляции 13
Мониторинг и сопровождение NAT 14

Введение

Двумя основными проблемами, стоящими сегодня перед глобальной сетью Интернет, является ограниченность адресного пространства протокола IP и масштабирование маршрутизации. Функции NAT (Network Address Translation), о которых пойдет речь в настоящей статье, появились в программном обеспечении Cisco IOS не случайно. Это было связано идеей предоставления организациям возможности использования внутри корпоративных и частных сетей адресного пространства, отличного от того, которого от них требуют поставщики услуг Интернет. Так, например, функции NAT позволяют организациям, использующим во внутренних корпоративных сетях маршрутизируемое частное адресное пространство (Private Subnets), получать доступ к узлам и ресурсам Интернет, имеющим «настоящие» адреса IP. Другой сферой применения NAT можно считать создание более гибкого решения по переадресации узлов для организаций, либо меняющих поставщика услуг Интернет, либо переадресующих блоки CIDR (Classless Interdomain Routing). Полное описание функций NAT можно найти в документе RFC 1631.

Применение NAT в современных бизнес-сетях

Функции NAT для решения следующих проблем и задач:

- При необходимости подключения к Интернет, когда количество внутренних узлов сети превышает выданное поставщиком услуг Интернет количество реальных адресов IP. NAT позволяет частным сетям IP, использующим незарегистрированные адреса, получать доступ к ресурсам Интернет. Функции NAT конфигурируются на пограничном маршрутизаторе, разграничивающем частную (внутреннюю) сеть и сеть общего пользования (например, Интернет). Далее сеть общего пользования мы будем называть *внешней сетью*, а частную сеть – *внутренней сетью*. Функции NAT перед отправкой пакетов во внешнюю сеть осуществляют трансляцию внутренних локальных адресов в уникальные внешние адреса IP.
- При необходимости изменения внутренней системы адресов. Вместо того, чтобы производить полное изменение всех адресов всех узлов внутренней сети, что представляет собой достаточно трудоемкую процедуру, функции NAT позволят производить их трансляцию в соответствии с новым адресным планом.
- При необходимости организации простого разделения трафика на основе портов TCP. Функции NAT предоставляют возможность установления соответствия (mapping) множества локальных адресов одному внешнему адресу, используя функции распределения нагрузки TCP.

Являясь решением проблем организации связи между различными узлами и подсетями (connectivity problems), на практике функции NAT в данный момент времени обслуживают работу лишь небольшого числа узлов во внутреннем домене. Это связано с тем, что ситуация, при которой всем узлам внутренней сети одновременно необходимо взаимодействовать с некоторыми внешними узлами, является маловероятной. Тогда в этом случае только сравнительно небольшое количество внутренних адресов по мере необходимости должны транслироваться во внешние адреса. В том случае, если какой-либо внешний адрес больше не используется каким-либо внутренним узлом, то он отдается в распоряжение другому внутреннему узлу.

Преимущества NAT

Одним из важнейших преимуществ NAT является то, что нет необходимости вносить изменения в конфигурацию конечных узлов и маршрутизаторов внутренней сети, за исключением тех устройств, на которых собственно и выполняются эти функции. Как уже отмечалось выше, функции NAT не имеют практического применения в тех сетях, где с внешней сетью одновременно работает большое количество внутренних узлов. К тому же некоторые приложения используют встроенные адреса IP, что ставит под вопрос использование NAT. Такие приложения либо не могут работать прозрачно в сетях с использованием NAT, либо их трафик вообще не будет проходить через устройства, реализующие функции NAT. Также отметим, что функции NAT скрывают внутреннее расположение узлов, что в зависимости от конкретных условий может быть как преимуществом, так и недостатком.

Маршрутизатор, выполняющий функции NAT, должен иметь, по крайней мере, один внутренний и один внешний интерфейсы. При обычном использовании NAT конфигурируется на выходном маршрутизаторе, разделяющем локальный домен и сеть общего пользования. Когда пакет покидает пределы локального домена, функции NAT транслируют содержимое поля Source (локальный адрес отправителя пакета) в значение уникального внешнего адреса. Когда же пакет

входит в локальный домен, производится трансляция уникального внешнего адреса в локальный адрес. Если локальный домен имеет более одного выхода во внешнюю сеть, то все маршрутизаторы NAT должны иметь одинаковые таблицы соответствия внутренних и внешних адресов. Если программное обеспечение не в состоянии занять адрес для текущего пакета, то такой пакет будет уничтожен. Одновременно в обратном направлении будет отправлен пакет ICMP, содержащий извещение об уничтожении этого пакета (Host Unreachable).
Маршрутизатор, выполняющий функции NAT, не должен распространять во внешнюю сеть информацию о внутренних подсетях. Тем не менее, маршрутная информация, получаемая маршрутизатором NAT из внешней сети, обычно распространяется по внутренней сети.

Терминология NAT

Как уже рассматривалось выше, термин *внутренняя сеть* применяется для тех сетей, которые находятся внутри организаций и используют адреса, нуждающиеся в трансляции. Внутри такого сетевого домена узлы используют одно адресное пространство, в то время как снаружи они доступны по адресам из другого адресного пространства, определяемого настройками функций NAT. Первое адресное пространство принято называть *локальным*, а второе – *глобальным адресным пространством*.
Аналогичным образом термин *внешняя сеть* относится к тем сетям, к которым подключаются внутренние сетевые домены. Эти сети не находятся под контролем организаций. Как будет описано далее, узлы внешней сети также могут быть объектами трансляции. Они могут использовать как локальные, так и глобальные адреса.
Приведем список определений и терминов, используемых функциями NAT:

- *Внутренний локальный адрес (Inside local address)*. Это адреса IP, присвоенные узлам внутренней сети. Как правило, эти адреса не являются зарегистрированными NIC (Network Information Center) или поставщиком услуг.
- *Внутренний глобальный адрес (Inside global address)*. Этот адрес выдается организации центром NIC или поставщиком услуг Интернет. Он представляет один или более внутренних узлов во внешней сети.
- *Внешний локальный адрес (Outside local address)*. Это адрес IP, присвоенный внешнему узлу и означающий, что внешний узел принадлежит внутренней сети. Этот адрес не нуждается в регистрации. Этот адрес должен принадлежать такому адресному пространству, которое имеет возможность маршрутизироваться во внутреннюю сеть.
- *Внешний глобальный адрес (Outside global address)*. Это адрес IP, присвоенный узлу внешней сети владельцем данного узла. Этот адрес принадлежит глобальному адресному или сетевому пространству.

Действия, выполняемые при настройке NAT

Прежде, чем приступить к конфигурированию функций NAT, необходимо проанализировать имеющуюся информацию о локальных и глобальных внутренних адресах. Следующие разделы статьи будут посвящены обсуждению того, каким образом можно использовать NAT в зависимости от потребностей в каждом конкретном случае.

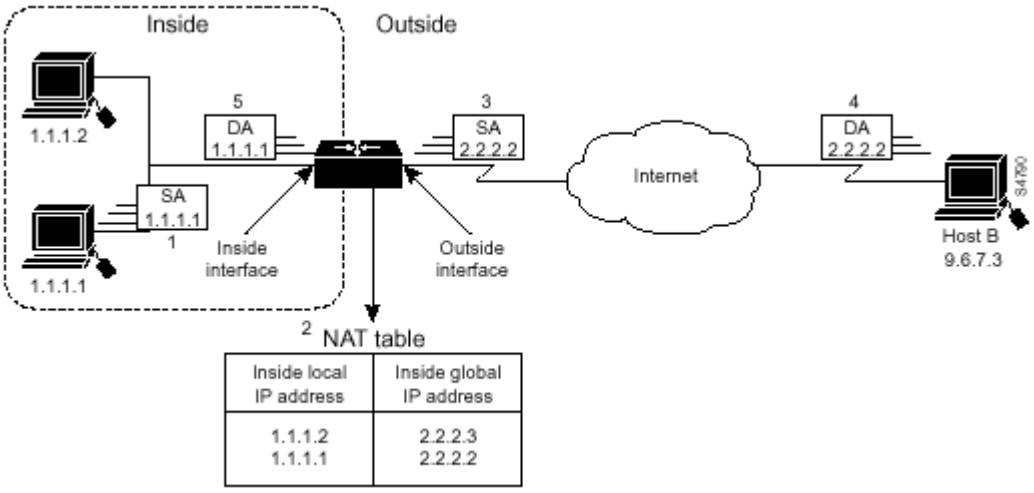
Трансляция внутренних адресов Source

Эта функция NAT позволяет транслировать имеющиеся внутренние адреса IP в уникальные адреса, принадлежащие глобальному адресному пространству, при необходимости обеспечения взаимодействия внутренней сети с внешней сетью. Имеется возможность использования статической или динамической трансляции:

- *Статическая трансляция* устанавливает соответствие адресов по типу «один к одному», т.е. один глобальный внутренний адрес соответствует одному локальному внутреннему адресу. Статическая трансляция применяется в тех случаях, когда некий внутренний узел должен быть доступен извне по постоянному адресу (например, сервер WWW).
- *Динамическая трансляция* устанавливает соответствие между внутренним локальным адресом и пулом глобальных адресов.

На рис. 1 показан маршрутизатор, транслирующий адреса узлов, содержащихся в поле Source заголовков пакетов IP из внутренних во внешние.

Рис. 1. Трансляция внутренних адресов Source



Приведенный ниже процесс описывает трансляцию локальных адресов Source, показанную на рис. 1:

1. Пользователь узла 1.1.1.1 открывает соединение с узлом B.
2. Первый пакет, полученный маршрутизатором от узла 1.1.1.1 приводит к тому, что маршрутизатор начинает проверять таблицу NAT.
   - Если имеется статическая запись в таблице трансляции, то маршрутизатор переходит к пункту 3.
   - Если статической записи в таблице трансляции нет, то маршрутизатор определяет, что адрес узла-источника пакета (SA, Source Address) 1.1.1.1 должен транслироваться динамически. Далее маршрутизатор выбирает свободный глобальный адрес из пула адресов и создает в таблице запись о трансляции. Тип такой записи называется *простая запись (Simple Entry)*.
3. Маршрутизатор заменяет внутренний локальный адрес узла 1.1.1.1 на указанный в таблице трансляции глобальный адрес (2.2.2.2), а затем передает пакет во внешнюю сеть.
4. Узел B получает пакет и отвечает узлу 1.1.1.1 используя внутренний глобальный адрес назначения (DA, Destination Address) 2.2.2.2.
5. Когда маршрутизатор получает пакет с внутренним глобальным адресом, он сверяется с таблицей NAT, используя внутренний глобальный адрес в качестве ключа поиска. Далее происходит трансляция внутреннего глобального адреса во внутренний локальный адрес узла 1.1.1.1, и пакет передается узлу 1.1.1.1.
6. Узел 1.1.1.1 получает этот пакет и продолжает взаимодействие с узлом B. Маршрутизатор осуществляет действия, описанные в пунктах 2 – 5, по отношению к каждому пакету.

Конфигурация статической трансляции

Для конфигурации статической трансляции необходимо выполнить следующие действия:

Действие	Команда
Установить режим статической трансляции между внутренним локальным адресом и внутренним глобальным адресом	`ip nat inside source static <локальный адрес> <глобальный адрес>`
Указать внутренний интерфейс	`interface <тип> <номер>`
Пометить данный интерфейс, как принадлежащий внутренней сети	`ip nat inside`
Указать внешний интерфейс	`interface <тип> <номер>`
Пометить данный интерфейс, как принадлежащий внешней сети	`ip nat outside`

Показанный пример содержит лишь минимальные изменения в конфигурации маршрутизатора. При использовании нескольких внутренних и внешних интерфейсов необходимо аналогичные действия произвести и в отношении остальных интерфейсов.

Конфигурация динамической трансляции

Для конфигурации динамической трансляции необходимо выполнить следующие действия:

Действие	Команда
Определить пул глобальных адресов	`ip nat pool <имя> <первый адрес> <последний адрес> [netmask <маска подсети> или prefix-length <длина префикса>]`
Определить стандартный список доступа, регламентирующий адреса, подлежащие трансляции	`access-list <номер> permit <адрес или блок адресов>`
Установить динамическую трансляцию на основе списка доступа, определенного на предыдущем шаге	`ip nat inside source list <номер списка доступа> pool <имя>`
Указать внутренний интерфейс	`interface <тип> <номер>`
Пометить данный интерфейс, как принадлежащий внутренней сети	`ip nat inside`
Указать внешний интерфейс	`interface <тип> <номер>`
Пометить данный интерфейс, как принадлежащий внешней сети	`ip nat outside`

Замечание. Список доступа должен разрешать только те адреса, которые действительно необходимо транслировать (Необходимо помнить, что последней строкой любого списка доступа является **deny all**). Список доступа, разрешающий более широкий блок адресов может привести к непредсказуемым результатам.

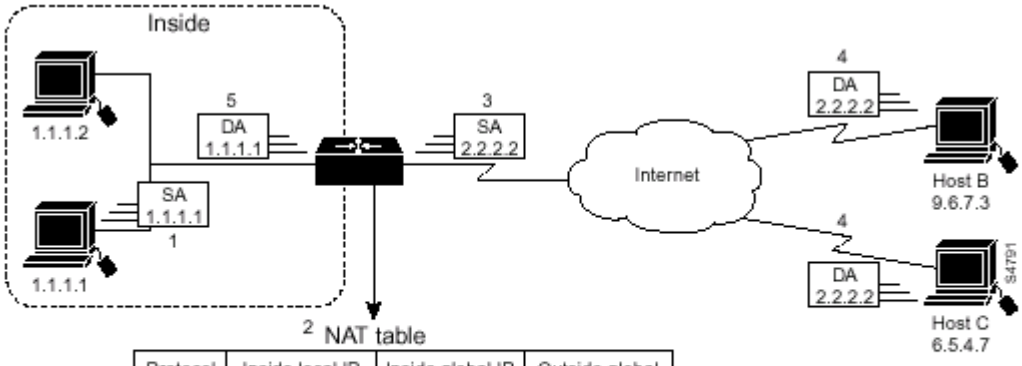
Представленный ниже пример транслирует все адреса узлов-источников, определенных списком доступа 1 (разрешены адреса от 192.168.1.0/24), в пул адресов, названный net-208. Этот пул содержит адреса с 171.69.233.208 по 171.69.233.233.

```
ip nat pool net-208 171.69.233.208 171.69.233.233 netmask
255.255.255.240
ip nat inside source list 1 pool net-208
!
interface serial 0
ip address 171.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet 0
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
```

Использование одного внутреннего глобального адреса

Существует возможность экономии пула внутренних глобальных адресов путем разрешения маршрутизатору использовать один глобальный адрес для трансляции нескольких локальных адресов. Если используется такой вариант конфигурации, то маршрутизатор использует информацию протоколов более высокого уровня (например, TCP и UDP) для обратной трансляции глобального адреса в корректные локальные адреса. При использовании соответствия нескольких локальных адресов одному глобальному адресу номера портов TCP или UDP каждого внутреннего узла указывают на локальные адреса этих узлов.
На рис. 2 показан принцип работы NAT, когда один внутренний глобальный адрес представляет несколько внутренних локальных адресов. Порты TCP используются в качестве критерия принадлежности пакетов тому или иному локальному адресу.

Рис. 2. Использование одного внутреннего глобального адреса



Protocol	Inside local IP address:port	Inside global IP address:port	Outside global IP address:port
TCP	1.1.1.2:1723	2.2.2.2:1723	6.5.4.7:23
TCP	1.1.1.1:1024	2.2.2.2:1024	9.6.7.3:23

Ниже показан процесс, выполняемый маршрутизатором в сети на рис. 2. Узлы B и C обращаются к одному узлу 2.2.2.2. На самом же деле они общаются с разными узлами во внутренней сети. Разделителем адресов этих узлов служит номер порта TCP. Фактически получается, что довольно большое количество внутренних узлов могут разделять один внутренний глобальный адрес IP, используя для этого разные порты TCP.

1. Пользователь узла 1.1.1.1 открывает соединение с узлом B.
2. Первый пакет, получаемый маршрутизатором от узла 1.1.1.1 приводит к тому, что маршрутизатор начинает проверку таблицы NAT.
   Если в таблице нет записей о трансляции, то маршрутизатор определяет, что адрес 1.1.1.1 должен быть транслирован, и устанавливает трансляцию внутреннего локального адреса 1.1.1.1 в имеющийся глобальный адрес. Если включен режим использования одного внутреннего глобального адреса и в настоящий момент работает другая процедура трансляции, то маршрутизатор забирает у этой процедуры данный глобальный адрес, обеспечивая при этом сохранение всей необходимой для обратной трансляции информации. Такой тип записи называется *расширенной записью (Extended Entry)*.
3. Маршрутизатор заменяет внутренний локальный адрес 1.1.1.1 выбранным глобальным адресом и осуществляет передачу пакета во внешнюю сеть.
4. Узел B получается этот пакет и отвечает узлу 1.1.1.1, используя внутренний глобальный адрес 2.2.2.2.
5. При получении из внешней сети пакета с внутренним глобальным адресом 2.2.2.2 маршрутизатор производит просмотр таблицы NAT, используя тип протокола, внутренний глобальный адрес и порт, а также внешний адрес и порт в качестве ключа поиска. После этого производится обратная трансляция адреса в локальный адрес 1.1.1.1, и пакет передается узлу 1.1.1.1.
6. Узел 1.1.1.1 получает этот пакет и продолжает взаимодействие. Маршрутизатор производит действия, описанные в пунктах 2 – 5 для каждого проходящего пакета.

Для конфигурирования режима использования одного внутреннего глобального адреса необходимо выполнить следующие шаги:

Действие	Команда
Определить пул глобальных адресов	`ip nat pool <имя> <первый адрес> <последний адрес> [netmask <маска подсети> или prefix-length <длина префикса>]`
Определить стандартный список доступа	`access-list <номер> permit <внутренний адрес или блок адресов>`
Установить режим динамической трансляции адресов, разрешенных в списке доступа, определенном на предыдущем шаге	`ip nat inside source list <номер списка доступа> pool <имя> overload`
Указать внутренний интерфейс	`interface <тип> <номер>`
Пометить данный интерфейс, как принадлежащий внутренней сети	`ip nat inside`
Указать внешний интерфейс	`interface <тип> <номер>`
Пометить данный интерфейс, как принадлежащий внешней сети	`ip nat outside`

Замечание. Список доступа должен разрешать только те адреса, которые действительно необходимо транслировать (Необходимо помнить, что последней строкой любого списка доступа является **deny all**). Список доступа, разрешающий более широкий блок адресов может привести к непредсказуемым результатам.

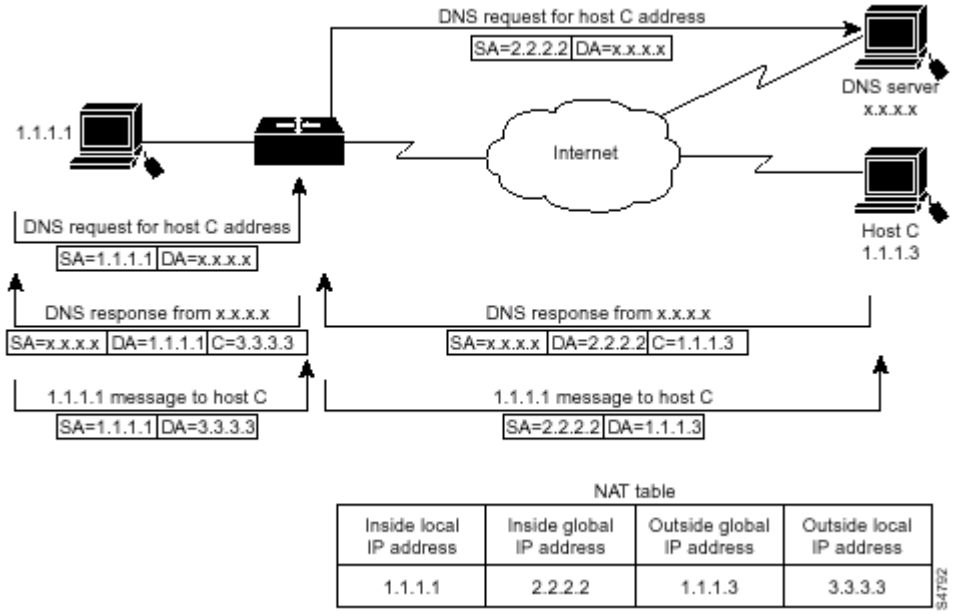
Приведенный ниже пример создает пул адресов, названный net-208. Данный пул содержит адреса с 171.69.233.208 по 171.69.233.233. Список доступа 1 разрешает пакеты, имеющие адрес отправителя с 192.168.1.0 по 192.168.1.255. Если в данный момент не производится процедур трансляции, то адреса в пакетах, соответствующих условиям списка доступа 1, транслируются в адрес из указанного пула. Маршрутизатор позволяет нескольким внутренним адресам (с 192.168.1.0 по 192.168.1.255) использовать один глобальный адрес. Для определения того или иного соединения маршрутизатор использует номера портов.

```
ip nat pool net-208 171.69.233.208 171.69.233.233 netmask
255.255.255.240
ip nat inside source list 1 pool net-208 overload
!
interface serial0
ip address 171.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet0
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
```

Трансляция перекрывающихся адресов

В описании NAT говориться, что данные функции используются для трансляции адресов IP, которые не являются официально зарегистрированными или закрепленными за определенными узлами или подсетями. Однако, может сложиться такая ситуация, при которой внутри корпоративной сети будет использоваться пространство адресов, официально закрепленное за другой сетью. Ситуация, при которой один и тот же адрес используется как легальный и как нелегальный одновременно, называют *перекрыванием (Overlapping)*. Функции NAT можно использовать с целью трансляции внутренних адресов, перекрывающихся с внешними адресами. Этот режим NAT используется в случаях, когда одна сеть использует адресное пространство другой, и в то же время необходимо организовать взаимодействие этих двух сетей.
На рис. 3 показана работа NAT в режиме трансляции перекрывающихся адресов.

Рис. 3. Трансляция перекрывающихся адресов



При таком режиме маршрутизатор выполняет действия, показанные ниже:

1. Пользователь узла 1.1.1.1 открывает соединение с узлом C по имени, полученном от сервера DNS.
2. Маршрутизатор перехватывает ответ сервера DNS и транслирует возвращаемый адрес, если имеет место перекрывание (это приводит к тому, что легальный адрес становится нелегальным во внутренней сети). Для обеспечения трансляции маршрутизатор создает простую запись трансляции, которая устанавливает соответствие между перекрывающимся адресом 1.1.1.3 и адресом из предварительно сконфигурированного пула внешних локальных адресов.
   Маршрутизатор отслеживает все ответы сервера DNS, обеспечивая таким образом отсутствие внешнего локального адреса во внутренней сети. Если такая ситуация имеет место быть, то маршрутизатор транслирует данный адрес.
3. Узел 1.1.1.1 открывает соединение с узлом 3.3.3.3.
4. Маршрутизатор настраивает соответствие внутренних локальных и глобальных адресов, а также внешних локальных и глобальных адресов.
5. Маршрутизатор заменяет адрес источника на внутренний глобальный адрес и адрес получателя на внешний глобальный адрес.
6. Узел C получает пакет и продолжает взаимодействие.
7. Маршрутизатор производит определение и замену адреса получателя на внутренний локальный адрес и адреса отправителя на внешний локальный адрес.
8. Узел 1.1.1.1 получает пакет и продолжает взаимодействие, используя процесс трансляции адресов.

Конфигурирование статической трансляции

Для конфигурирования статической трансляции внешних адресов узлов-отправителей, необходимо выполнить следующие шаги:

Действие	Команда
Установить статическую трансляцию между внешним локальным адресом и внешним глобальным адресом	`ip nat outside source static <глобальный адрес> <локальный адрес>`
Указать внутренний интерфейс	`interface <тип> <номер>`
Пометить данный интерфейс, как принадлежащий внутренней сети	`ip nat inside`
Указать внешний интерфейс	`interface <тип> <номер>`
Пометить данный интерфейс, как принадлежащий внешней сети	`ip nat outside`

Конфигурирование динамической трансляции

Для конфигурирования динамической трансляции внешних адресов узлов-отправителей, необходимо выполнить следующие шаги:

Действие	Команда
Определить пул локальных адресов	`ip nat pool <имя> <начальный адрес> <конечный адрес> [netmask <маска подсети> или prefix-length <длина префикса>]`
Определить стандартный список доступа	`access-list <номер> permit <локальный адрес или блок адресов>`
Установить динамическую трансляцию внешних адресов узлов-отправителей, основанную на списке доступа, определенном на предыдущем шаге	`ip nat outside source list <номер списка доступа> pool <имя>`
Указать внутренний интерфейс	`interface <тип> <номер>`
Пометить данный интерфейс, как принадлежащий внутренней сети	`ip nat inside`
Указать внешний интерфейс	`interface <тип> <номер>`
Пометить данный интерфейс, как принадлежащий внешней сети	`ip nat outside`

Замечание. Список доступа должен разрешать только те адреса, которые действительно необходимо транслировать (Необходимо помнить, что последней строкой любого списка доступа является **deny all**). Список доступа, разрешающий более широкий блок адресов может привести к непредсказуемым результатам.

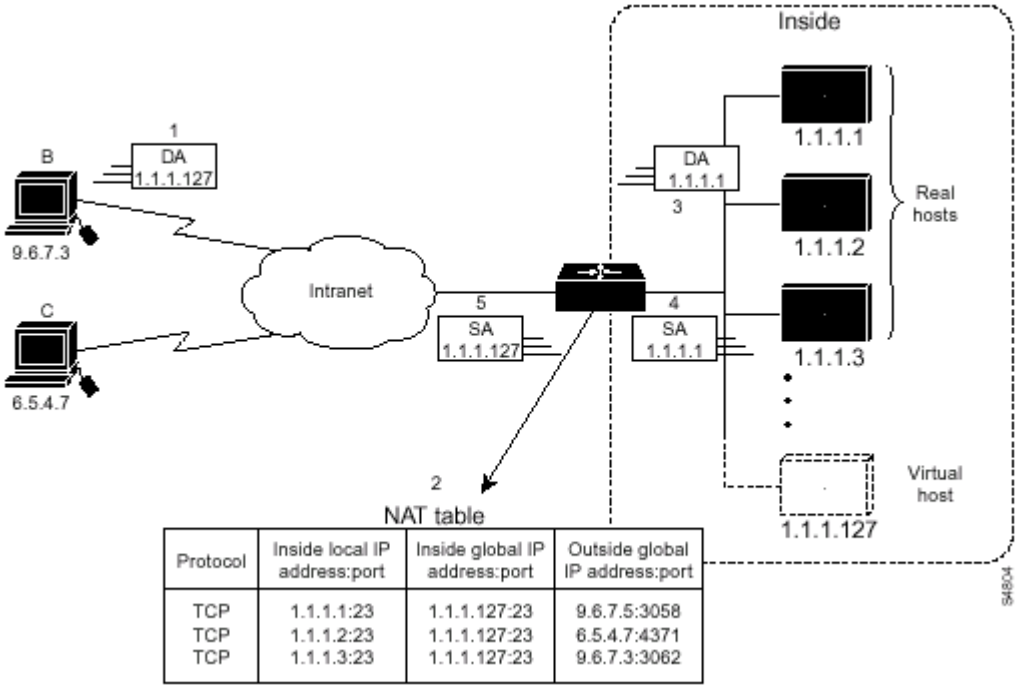
В приведенном ниже примере адреса в локальной сети используются кем-то еще в качестве легальных адресов Интернет. Во внешней сети необходимо производить дополнительную трансляцию. Пул net-10 является пулом внешних локальных адресов IP. Выражение *ip nat outside source list 1 pool net-10* транслирует адреса узлов из внешней перекрывающейся сети в адреса данного пула.

```
ip nat pool net-208 171.69.233.208 171.69.233.223 prefix-length 28
ip nat pool net-10 10.0.1.0 10.0.1.255 prefix-length 24
ip nat inside source list 1 pool net-208
ip nat outside source list 1 pool net-10
!
interface serial 0
ip address 171.69.232.192 255.255.255.240
ip nat outside
!
interface ethernet0
ip address 192.168.1.94 255.255.255.0
ip nat inside
access-list 1 permit 192.168.1.0 0.0.0.255
```

Обеспечение распределения нагрузки TCP

Другая сфера применения NAT не относится к использованию адресов Интернет. Допустим, что организация имеет множество узлов, которые должны подключаться к одному узлу, характеризующемуся высокой степенью загрузки запросами пользователей. Используя NAT можно организовать виртуальный узел во внутренней сети, который будет координировать разделение нагрузки между реальными узлами сети. Адреса узлов назначения, совпадающие с условиями списка доступа, заменяются на адреса из постоянно перебираемого пула. Выбор адреса осуществляется по механизму round-robin, причем такой выбор производится только при установлении нового соединения из внешней сети во внутреннюю. Трафик «не-TCP» передается без изменений. Эта функция показана на рис. 4.

Рис. 4. Распределение нагрузки TCP



Protocol	Inside local IP address:port	Inside global IP address:port	Outside global IP address:port
TCP	1.1.1.1:23	1.1.1.127:23	9.6.7.5:3058
TCP	1.1.1.2:23	1.1.1.127:23	6.5.4.7:4371
TCP	1.1.1.3:23	1.1.1.127:23	9.6.7.3:3062

Маршрутизатор выполняет следующие действия при переборе адресов:

1. Пользователь узла B (9.6.7.3) открывает соединение с виртуальным узлом 1.1.1.127.
2. Маршрутизатор получает пакет с запросом на подключение и создает новую запись трансляции, выбирая для нее новый реальный узел (1.1.1.1) в качестве внутреннего локального адреса IP.
3. Маршрутизатор заменяет адрес назначения выбранным адресом реального узла и передает пакет.
4. Узел 1.1.1.1 получает пакет и формирует ответ на него.
5. Маршрутизатор получает ответный пакет и просматривает таблицу NAT, используя в качестве ключа поиска внутренний локальный адрес и номер порта. Маршрутизатор транслирует адрес источника в адрес виртуального узла и передает пакет по сети.

Следующий запрос на соединение вынуждает маршрутизатор выбирать адрес 1.1.1.2 в качестве внутреннего локального адреса.

Для конфигурирования этого режима использования функций NAT необходимо произвести приведенные ниже шаги. Эта функция NAT позволяет устанавливать соответствие между одним виртуальным узлом и множеством реальных узлов сети. Каждая новая сессия TCP открывает новый виртуальный узел. Эта сессия будет транслироваться как сессия с другим реальным узлом.

Действие	**Команда**
Определить пул адресов, состоящий из адресов реальных узлов	`ip nat pool <имя> <начальный адрес> <конечный адрес> [netmask <маска подсети> или prefix-length <длина префикса>]`
Определить список доступа, разрешающий адрес виртуального узла	`access-list <номер> permit <адрес назначения или группа адресов>`
Установить динамическую внутреннюю трансляцию адресов назначения на основе вписка доступа, определенного на предыдущем шаге	`ip nat inside destination list <номер списка доступа> pool <имя>`
Указать внутренний интерфейс	`interface <тип> <номер>`
Пометить данный интерфейс, как принадлежащий внутренней сети	`ip nat inside`
Указать внешний интерфейс	`interface <тип> <номер>`
Пометить данный интерфейс, как принадлежащий внешней сети	`ip nat outside`

Замечание. Список доступа должен разрешать только те адреса, которые действительно необходимо транслировать (Необходимо помнить, что последней строкой любого списка доступа является **deny all**). Список доступа, разрешающий более широкий блок адресов может привести к непредсказуемым результатам.

В приведенном ниже примере основной целью определения виртуального адреса является то, что все соединения распределяются между несколькими реальными узлами. Пул адресов определяет эти узлы. Список доступа определяет виртуальный адрес. Если в данный момент нет процедуры трансляции, то пакет TCP с интерфейса Serial 0 (внешний интерфейс), адрес назначения которого удовлетворяет условиям списка доступа, транслируется в один из адресов адресного пула.

```
ip nat pool real-hosts 192.168.15.2 192.168.15.15 prefix-length 28
type rotary
ip nat inside destination list 2 pool real-hosts
!
interface serial 0
ip address 192.168.15.129 255.255.255.240
ip nat outside
!
interface ethernet 0
ip address 192.168.15.17 255.255.255.240
ip nat inside
!
access-list 2 permit 192.168.15.1
```

Изменение тайм-аутов трансляции

По умолчанию динамическая трансляция адресов периодически не используется. При необходимости можно изменить значение тайм-аута, после которого используемые адреса трансляции будут освобождаться для других нужд. Если не сконфигурирован режим использования одного глобального адреса для нескольких локальных адресов (overloading), то время действия простых записей трансляции составляет 24 часа. Для изменения значения тайм-аута необходимо выполнить следующие шаги:

Действие	Команда
Изменить значение тайм-аута для динамической трансляции адресов. Режим overloading не используется.	`ip nat translation timeout <значение в секундах>`

Если используется режим overloading, то управление тайм-аутами производится более тонко в связи с тем, что каждая запись трансляции определяет тип трафика, используемый указанными в записи узлами. Команды по изменению значений тайм-аутов выглядят следующим образом:

Действие	Команда
Изменение значения тайм-аута UDP (по умолчанию 5 минут)	`ip nat translation udp-timeout <значение в секундах>`
Изменение значения тайм-аута DNS (по умолчанию 1 минута)	`ip nat translation dns-timeout <значение в секундах>`
Изменение значения тайм-аута TCP (по умолчанию 24 часа)	`ip nat translation tcp-timeout <значение в секундах>`
Изменение значения тайм-аута Finish и Reset (по умолчанию 1 минута)	`ip nat translation finrst-timeout <значение в секундах>`

Мониторинг и сопровождение NAT

По умолчанию таблица динамической трансляции адресов со временем очищается автоматически. Однако, имеется возможность проведения работ по мониторингу и сопровождению NAT с консоли управления маршрутизатором:

Действие	Команда
Очистить все записи динамической трансляции адресов из таблицы NAT	`clear ip nat translation *`
Очистить простую запись динамической трансляции, содержащей информацию либо о внутренней трансляции, либо о внутренней и внешней трансляции	`clear ip nat translation inside <глобальный адрес> <локальный адрес> [outside <локальный адрес> <глобальный адрес>]`
Очистить простую запись динамической трансляции, содержащую информацию о внешней трансляции	`clear ip nat translation outside <локальный адрес> <глобальный адрес>`
Очистить расширенную запись динамической трансляции	`clear ip nat translation <протокол> inside <глобальный адрес> <глобальный порт> <локальный адрес> <локальный порт> [outside <локальный адрес> <локальный порт> <глобальный адрес> <глобальный порт>]`

Просмотреть текущее состояние NAT можно при помощи следующих команд:

Действие	Команда
Показать активные трансляции	`show ip nat translations [verbose]`
Показать статистику трансляций	`show ip nat statistics`

