Преобразование сетевых адресов на одном интерфейсе

Содержание

Введение

Что подразумевается под преобразованием сетевого адреса на одном интерфейсе? Термин "на одном интерфейсе" обычно подразумевает использование единого физического интерфейса маршрутизатора для выполнения задач. Так как можно использовать субинтерфейсы одного и того же физического интерфейса для выполнения магистрали межкоммутаторного соединения (ISL), мы можем использовать единственный физический интерфейс на маршрутизаторе для того, чтобы выполнить NAT.

Примечание. Маршрутизатору необходимо направлять каждый пакет посредством интерфейса обратной связи. Это ухудшает производительность маршрутизатора.

Предварительные условия

Требования

Для данного документа отсутствуют особые требования.

Используемые компоненты

Для данной функции необходимо использование версии ПО Cisco IOS®, которая поддерживает NAT. Используйте Навигатор по функциям Cisco II (только для зарегистрированных клиентов), чтобы определить, какие версии IOS совместимы с данной функцией.

Базовые сведения

Для преобразования сетевых адресов пакету необходимо переключаться с внутреннего на внешний интерфейс NAT и обратно. Это требование для NAT не изменилось, но в этом документе показано, как можно использовать виртуальный интерфейс, также известный как интерфейс обратной связи, и основанную на политиках маршрутизацию, чтобы наладить работу NAT в маршрутизаторе с единым физическим интерфейсом.

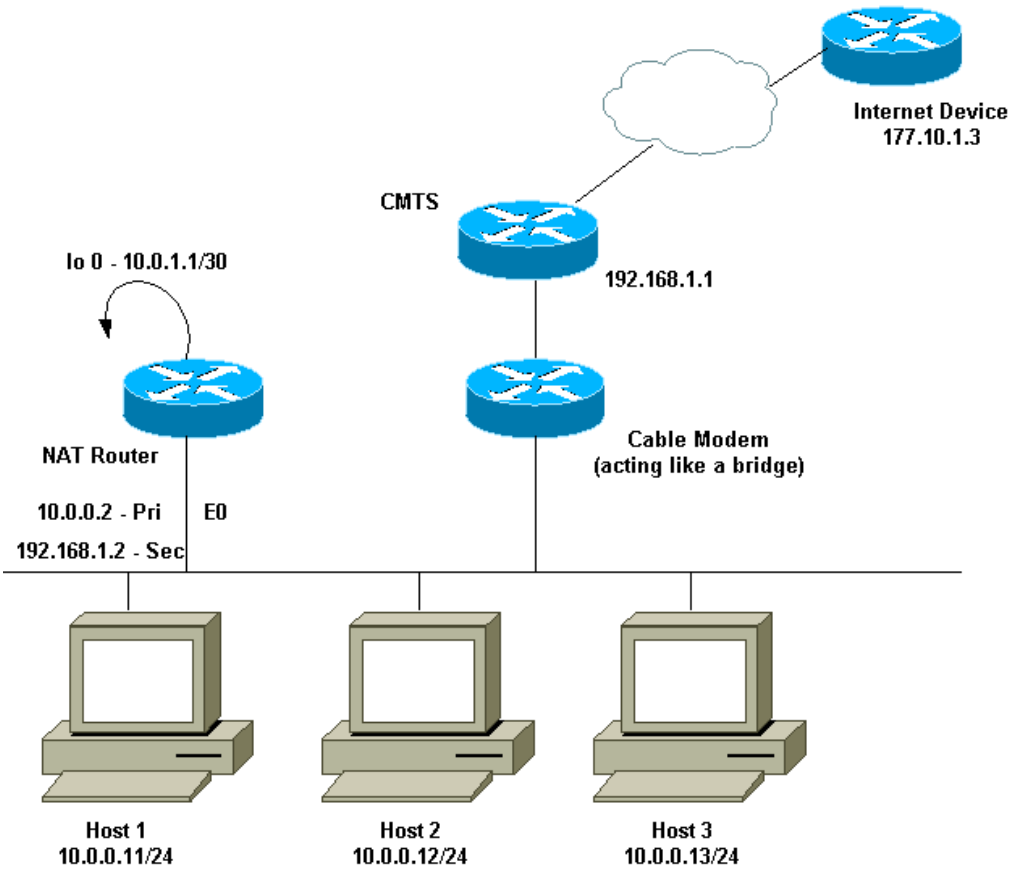
Такие требования для NAT на одном интерфейсе являются редкими. Фактически, примеры, приведенные в этом документе, могут быть единственными примерами ситуаций, в которых необходима конфигурация. Однако другие случаи, когда пользователи применяют маршрутизацию, основанную на политиках, в связке с NAT, мы не рассматриваем как преобразование сетевых адресов (NAT) на одном интерфейсе, потому что в этих случаях используется несколько физических интерфейсов.

Условные обозначения

Дополнительные сведения об условных обозначениях, используемых в данном документе, см. в разделе Условные обозначения, используемые в технической документации Cisco.

Пример 1. Схема и конфигурация сети

Схема сети



Представленная выше схема сети часто встречается в конфигурации кабельного модема. Система кабельных модемов (CMTS) является устройством, включающем маршрутизатор, а также кабельный модем (CM) и работающем в качестве моста. Рассматриваемая проблема заключается в том, что поставщик Интернет-услуг (ISP) не предоставил нам достаточно действительных адресов для всех хостов, которым требуется подключение к Интернету. Поставщик Интернет-услуг выдал адрес 192.168.1.2, который может быть использован для устройства. По следующему запросу были предоставлены три дополнительных адреса – от 192.168.2.1 до 192.168.2.3, – в которые NAT преобразовывает хосты диапазона 10.0.0.0/24.

Требования

Наши требования:

-

- Все хосты в сети необходимо подключить к Интернету.
- Хост 2 должен быть доступен в Интернете и иметь IP-адрес 192.168.2.1.
- Так как мы располагаем большим количеством хостов, чем легальные адреса, мы используем подсеть 10.0.0.0/24 для осуществления внутренней адресации.

В данном документе рассматривается только конфигурация маршрутизатора NAT. Однако мы сделаем несколько важных замечаний в отношении конфигурации хостов.

Конфигурацию маршрутизатора NAT

Конфигурацию маршрутизатора NAT

```
interface Loopback0
ip address 10.0.1.1 255.255.255.252
ip nat outside
!--- Создание виртуального интерфейса, называемого Loopback 0, и назначение ему
!--- IP-адреса 10.0.1.1. Определение интерфейса Loopback 0 в качестве
!--- внешнего интерфейса NAT.

!
!
interface Ethernet0
ip address 192.168.1.2 255.255.255.0 secondary
ip address 10.0.0.2 255.255.255.0
ip Nat inside
!--- Назначение первичного IP-адреса 10.0.0.2 и вторичного IP-адреса
!--- 192.168.1.2 интерфейсу Ethernet 0. Определение интерфейса Ethernet 0
!--- в качестве внутреннего интерфейса NAT. Адрес 192.168.1.2 будет использоваться для связи
!--- с CMTS и Интернетом через CM.  Адрес 10.0.0.2
!--- будет использоваться для связи с локальными хостами.


ip policy route-map Nat-loop
!--- Назначение интерфейсу Ethernet 0 карты маршрутов "Nat-loop" для маршрутизации, основанной на политиках.

!
ip Nat pool external 192.168.2.2 192.168.2.3 prefix-length 29
ip Nat inside source list 10 pool external overload
ip Nat inside source static 10.0.0.12 192.168.2.1
!--- Функция NAT определена: пакеты, соответствующие списку access-list 10, будут
!--- преобразовываться в адрес из пула, называемого "external".
!--- Статическое преобразование NAT определено таким образом, чтобы адрес 10.0.0.12
!--- преобразовывался в 192.168.2.1 (это необходимо для хоста 2, к которому требуется
!--- осуществлять доступ из Интернета).


ip classless
!
!
ip route 0.0.0.0 0.0.0.0 192.168.1.1
ip route 192.168.2.0 255.255.255.0 Ethernet0
!--- Для статического маршрута по умолчанию установлен адрес 192.168.1.1, кроме того, статический маршрут
!--- для сети 192.168.2.0/24 непосредственно подключен к интерфейсу
!--- Ethernet 0

!
!
access-list 10 permit 10.0.0.0 0.0.0.255
!--- Access-list 10 определен для использования выше с помощью инструкции NAT.


access-list 102 permit ip any 192.168.2.0 0.0.0.255
access-list 102 permit ip 10.0.0.0 0.0.0.255 any
!--- Access-list 102 определен и используется картой маршрутов "Nat-loop",
!--- которая применяется для маршрутизации, основанной на политиках.

!
Access-list 177 permit icmp any any
!--- Access-list 177 используется для команды debug.

!
route-map Nat-loop permit 10
match ip address 102
set ip next-hop 10.0.1.2
```

```
!--- Создание карты маршрутов "Nat-loop", используемой для маршрутизации, основанной на политиках.
!--- С помощью карты маршрутов задается режим, при котором любые пакеты, удовлетворяющие списку access-list 102,
!--- передаются на следующий участок тракта по адресу 10.0.1.2 и маршрутизируются по направлению "из"
!--- интерфейса loopback. Маршрутизация всех остальных пакетов выполняется обычным образом.
!--- Адрес 10.0.1.2 используется, поскольку этот следующий участок тракта определяется
!--- как расположенный на интерфейсе loopback, в результате чего маршрутизация, основанная на политиках, выполняется на
!--- loopback0. С другой стороны, для получения таких же результатов можно было бы использовать инструкцию "set interfac
!--- loopback0".

!
end
NAT-router#
```

Примечание. Для всех хостов шлюз по умолчанию настроен на адрес 10.0.0.2, который является NAT-маршрутизатором. Поставщик Интернет-услуг, также как CMTS, должен иметь маршрут по адресу 192.168.2.0/29, который указывает путь к NAT-маршрутизатору для возвращения данных к работе, так как трафик с внутреннего хоста определяется как полученный из подсети. В следующем примере CMTS направляет трафик для адреса 192.168.2.0/29 по адресу 192.168.1.2, который настроен на NAT маршрутизаторе.

Пример 1. Выходные данные команд show и debug

Если вы хотите убедиться, что ваша конфигурация работает правильно, прочитайте этот раздел.

Чтобы показать, что вышеупомянутая конфигурация работает, были проведены несколько **ping**-тестов, в то время как NAT-маршрутизатор контролировал выходные данные команды **debug**. Теперь видно, что команды **ping** успешно выполняются, а выходные данные команд **debug** показывает как раз сам текущий процесс.

Примечание. Перед использованием команд **debug** ознакомьтесь с документом Важные сведения о командах debug.

Тест 1

В первом тесте мы выполняем команду **ping** от устройства в Интернете к хосту 2. Запомните, что одним из требований было то, что устройства в Интернете должны иметь возможность взаимодействовать с хостом 2 по адресу 192.168.2.1. Следующим является выходные данные команды **debug**, как показывает NAT-маршрутизатор. Командами **debug**, запущенными в NAT-маршрутизаторе, были **debug ip packet 177 detail** , которая использует заданный лист доступа **access-list 177**, **debug ip Nat** и **debug ip policy**, которая выводит пакеты, маршрутизированные политикой.

Ниже представлены выходные данные команды **show ip Nat translation**, выполненной NAT-маршрутизатором.

```
NAT-router# show ip Nat translation
Pro Inside global      Inside local       Outside local      Outside global
--- 192.168.2.1        10.0.0.12          ---                ---
NAT-router#
```

От устройства в Интернете, в данном случае маршрутизатора, мы, как показано ниже, успешно выполняем команду **ping** относительно адреса 192.168.2.1.

```
Internet-device# ping 192.168.2.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/92/92 ms
Internet-device#
```

Чтобы узнать, что происходит в маршрутизаторе, см. выходные данные и комментарии к командам **debug**.

```
IP: s=177.10.1.3 (Ethernet0), d=192.168.2.1, len 100, policy match
   ICMP type=8, code=0
IP: route map Nat-loop, item 10, permit
IP: s=177.10.1.3 (Ethernet0), d=192.168.2.1 (Loopback0), Len 100, policy routed
   ICMP type=8, code=0
!--- Из приведенных выше выходных данных команды debug следует, что пакет с источником 177.10.1.3 направляется
!--- по адресу 192.168.2.1. Пакет соответствует инструкциям в карте "Nat-loop" для
!--- маршрутов, основанных на политиках, и разрешен и маршрутизируется в соответствии с политикой. Параметры type 8,
!--- протокола управляющих сообщений сети Интернет (ICMP) указывает, что этот
!--- пакет является пакетом запроса "ICMP-эхо".


IP: Ethernet0 to Loopback0 10.0.1.2
IP: s=177.10.1.3 (Ethernet0), d=192.168.2.1 (Loopback0), g=10.0.1.2, Len 100,
forward
   ICMP type=8, code=0
!--- Пакет теперь направляется на следующий участок тракта по адресу 10.0.1.2
!--- (см. выше).


IP: NAT enab = 1 trans = 0 flags = 0
NAT: s=177.10.1.3, d=192.168.2.1->10.0.0.12 [52]
IP: s=177.10.1.3 (Loopback0), d=10.0.0.12 (Ethernet0), g=10.0.0.12, Len 100,
forward
   ICMP type=8, code=0
IP: NAT enab = 1 trans = 0 flags = 0
!--- Теперь после принятия решения о маршрутизации выполняется NAT. Из приведенной выше
!--- информации следует, что адрес 192.168.2.1 преобразуется в 10.0.0.12, и
!--- этот пакет передается из интерфейса Ethernet 0 в локальный хост.
!--- Примечание. При передаче пакета из внутреннего интерфейса во внешний он маршрутизируется и
!--- затем преобразуется (NAT). При передаче в противоположном направлении (из внешнего интерфейса во внутренний)
!--- вначале выполняется NAT.


IP: s=10.0.0.12 (Ethernet0), d=177.10.1.3, Len 100, policy match
   ICMP type=0, code=0
IP: route map Nat-loop, item 10, permit
IP: s=10.0.0.12 (Ethernet0), d=177.10.1.3 (Loopback0), Len 100, policy routed
   ICMP type=0, code=0
IP: Ethernet0 to Loopback0 10.0.1.2
!--- Хост 2 теперь передает отклик на "ICMP-эхо", который определяется с помощью параметров type 0, code 0 протокола
!--- Этот пакет также соответствует инструкциям маршрутизации, основанной на политиках, и
!--- разрешен для выполнения такой машрутизации.


NAT: s=10.0.0.12->192.168.2.1, d=177.10.1.3 [52]
IP: s=192.168.2.1 (Ethernet0), d=177.10.1.3 (Loopback0), g=10.0.1.2, Len 100,
forward
   ICMP type=0, code=0
IP: s=192.168.2.1 (Loopback0), d=177.10.1.3 (Ethernet0), g=192.168.1.1, Len 100,
forward
   ICMP type=0, code=0
IP: NAT enab = 1 trans = 0 flags = 0
!--- Из приведенных выше выходных данных видно, что IP-адрес хоста 2 преобразуется в
!--- 192.168.2.1, и результирующий пакет передается из интерфейса loopback 0
!--- в соответствии с маршрутизацией, основанной на политике, и, наконец, направляется из интерфейса
!--- Ethernet 0 в Интернет-устройство.

!--- Оставшиеся выходные данные команды debug повторяют предыдущие
!--- для каждой из четырех дополнительных операций обмена пакетами ICMP (по умолчанию
!--- при выдаче запросов "ICMP-эхо" из маршрутизаторов Cisco посылается пять ICMP-пакетов). Большая часть
!--- выходной информации здесь не приводится, поскольку она является избыточной.


IP: s=177.10.1.3 (Ethernet0), d=192.168.2.1, Len 100, policy match
   ICMP type=8, code=0
IP: route map Nat-loop, item 10, permit
IP: s=177.10.1.3 (Ethernet0), d=192.168.2.1 (Loopback0), Len 100, policy routed
   ICMP type=8, code=0
IP: Ethernet0 to Loopback0 10.0.1.2
IP: s=177.10.1.3 (Ethernet0), d=192.168.2.1 (Loopback0), g=10.0.1.2, Len 100,
forward
   ICMP type=8, code=0
IP: NAT enab = 1 trans = 0 flags = 0
NAT: s=177.10.1.3, d=192.168.2.1->10.0.0.12 [53]
IP: s=177.10.1.3 (Loopback0), d=10.0.0.12 (Ethernet0), g=10.0.0.12, Len 100,
forward
   ICMP type=8, code=0
IP: NAT enab = 1 trans = 0 flags = 0
IP: s=10.0.0.12 (Ethernet0), d=177.10.1.3, Len 100, policy match
   ICMP type=0, code=0
IP: route map Nat-loop, item 10, permit
IP: s=10.0.0.12 (Ethernet0), d=177.10.1.3 (Loopback0), Len 100, policy routed
   ICMP type=0, code=0
IP: Ethernet0 to Loopback0 10.0.1.2
```

```
NAT: s=10.0.0.12->192.168.2.1, d=177.10.1.3 [53]
IP: s=192.168.2.1 (Ethernet0), d=177.10.1.3 (Loopback0), g=10.0.1.2, Len 100,
forward
   ICMP type=0, code=0
IP: s=192.168.2.1 (Loopback0), d=177.10.1.3 (Ethernet0), g=192.168.1.1, Len 100,
forward
   ICMP type=0, code=0
IP: NAT enab = 1 trans = 0 flags = 0
```

Тест 2

Другое требование – разрешить хостам устанавливать связь с Интернетом. В этом тесте выполняем команду **ping** от Хоста 1 в Интернет. Ниже показан результат выполнения команд **show** и **debug**.

В исходном положении таблица NAT-преобразования в NAT-маршрутизаторе выглядит следующим образом:

```
NAT-router# show ip Nat translation
Pro Inside global      Inside local       Outside local      Outside global
--- 192.168.2.1        10.0.0.12          ---                ---
NAT-router#
```

Выполняя команду **ping** в Хосте 1, мы видим:

```
Host-1# ping 177.10.1.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 177.10.1.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/92/96 ms
Host-1#
```

Как видно выше, команда **ping** был успешно выполнена. Таблица NAT в маршрутизаторе теперь выглядит следующим образом:

```
NAT-router# show ip Nat translation
Pro Inside global      Inside local       Outside local      Outside global
icmp 192.168.2.2:434   10.0.0.11:434      177.10.1.3:434     177.10.1.3:434
icmp 192.168.2.2:435   10.0.0.11:435      177.10.1.3:435     177.10.1.3:435
icmp 192.168.2.2:436   10.0.0.11:436      177.10.1.3:436     177.10.1.3:436
icmp 192.168.2.2:437   10.0.0.11:437      177.10.1.3:437     177.10.1.3:437
icmp 192.168.2.2:438   10.0.0.11:438      177.10.1.3:438     177.10.1.3:438
--- 192.168.2.1        10.0.0.12          ---                ---
NAT-router#
```

В приведенной выше таблице преобразования NAT отображены дополнительные преобразования, являющиеся результатом динамической конфигурации NAT (в отличие от статической конфигурации NAT).

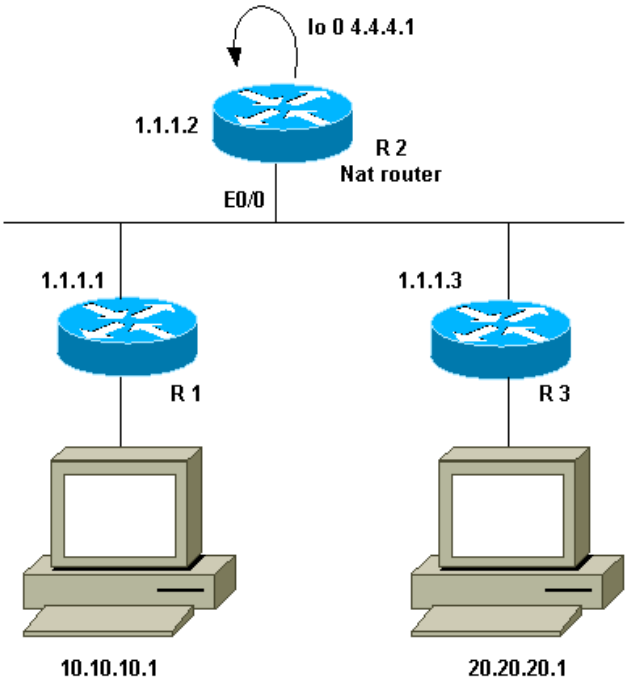
Результат выполнения команды **debug** показывает процессы, происходящие в NAT-маршрутизаторе.

```
IP: NAT enab = 1 trans = 0 flags = 0
IP: s=10.0.0.11 (Ethernet0), d=177.10.1.3, Len 100, policy match
   ICMP type=8, code=0
IP: route map Nat-loop, item 10, permit
IP: s=10.0.0.11 (Ethernet0), d=177.10.1.3 (Loopback0), Len 100, policy routed
   ICMP type=8, code=0
IP: Ethernet0 to Loopback0 10.0.1.2
!--- Из приведенной выше выходной информации следует, что пакет запроса "ICMP-эхо", инициированный
!--- хостом 1, направляется в соответствии с политиками из интерфейса loopback.

NAT: s=10.0.0.11->192.168.2.2, d=177.10.1.3 [8]
```

```
IP: s=192.168.2.2 (Ethernet0), d=177.10.1.3 (Loopback0), g=10.0.1.2, Len 100,
forward
   ICMP type=8, code=0
IP: s=192.168.2.2 (Loopback0), d=177.10.1.3 (Ethernet0), g=192.168.1.1, Len 100,
forward
   ICMP type=8, code=0
IP: NAT enab = 1 trans = 0 flags = 0
!--- После принятия решения о маршрутизации средствами маршрутизации, основанной на политиках,
!--- выполняется преобразование, в результате которого IP-адрес хоста 1 (10.0.0.11)
!--- преобразуется, как показано выше, в адрес из пула "external" (192.168.2.2).
!--- Затем пакет передается из интерфейса loopback 0 и, наконец, из интерфейса Ethernet 0 -
!--- в Интернет-устройство.


IP: s=177.10.1.3 (Ethernet0), d=192.168.2.2, Len 100, policy match
   ICMP type=0, code=0
IP: route map Nat-loop, item 10, permit
IP: s=177.10.1.3 (Ethernet0), d=192.168.2.2 (Loopback0), Len 100, policy routed
   ICMP type=0, code=0
IP: Ethernet0 to Loopback0 10.0.1.2
IP: s=177.10.1.3 (Ethernet0), d=192.168.2.2 (Loopback0), g=10.0.1.2, Len 100,
forward
   ICMP type=0, code=0
!--- Интернет-устройство посылает отклик "ICMP-эхо", который соответствует
!--- политике; пакет маршрутизируется на основе политики и передается из интерфейса Loopback 0.


IP: NAT enab = 1 trans = 0 flags = 0
NAT: s=177.10.1.3, d=192.168.2.2->10.0.0.11 [8]
IP: s=177.10.1.3 (Loopback0), d=10.0.0.11 (Ethernet0), g=10.0.0.11, Len 100,
forward
   ICMP type=0, code=0
!--- Пакет возвращается на интерфейс loopback, на котором
!--- блок адреса, связанный с пунктом назначения, преобразуется из 192.168.2.2
!--- в 10.0.0.11, после чего пакет передается из интерфейса Ethernet 0 на локальный хост.

!--- Обмен по протоколу ICMP повторяется для оставшихся ICMP-пакетов, информация о некоторых из которых
!--- приведена выше.


IP: NAT enab = 1 trans = 0 flags = 0
IP: s=10.0.0.11 (Ethernet0), d=177.10.1.3, Len 100, policy match
   ICMP type=8, code=0
IP: route map Nat-loop, item 10, permit
IP: s=10.0.0.11 (Ethernet0), d=177.10.1.3 (Loopback0), Len 100, policy routed
   ICMP type=8, code=0
IP: Ethernet0 to Loopback0 10.0.1.2
NAT: s=10.0.0.11->192.168.2.2, d=177.10.1.3 [9]
IP: s=192.168.2.2 (Ethernet0), d=177.10.1.3 (Loopback0), g=10.0.1.2, Len 100,
forward
   ICMP type=8, code=0
IP: s=192.168.2.2 (Loopback0), d=177.10.1.3 (Ethernet0), g=192.168.1.1, Len 100,
forward
   ICMP type=8, code=0
IP: NAT enab = 1 trans = 0 flags = 0
IP: s=177.10.1.3 (Ethernet0), d=192.168.2.2, Len 100, policy match
   ICMP type=0, code=0
IP: route map Nat-loop, item 10, permit
IP: s=177.10.1.3 (Ethernet0), d=192.168.2.2 (Loopback0), Len 100, policy routed
   ICMP type=0, code=0
IP: Ethernet0 to Loopback0 10.0.1.2
IP: s=177.10.1.3 (Ethernet0), d=192.168.2.2 (Loopback0), g=10.0.1.2, Len 100,
forward
   ICMP type=0, code=0
IP: NAT enab = 1 trans = 0 flags = 0
NAT: s=177.10.1.3, d=192.168.2.2->10.0.0.11 [9]
IP: s=177.10.1.3 (Loopback0), d=10.0.0.11 (Ethernet0), g=10.0.0.11, Len 100,
forward
   ICMP type=0, code=0
```

Пример 2. Схема и конфигурация сети

Схема сети



Требования

Для взаимодействия необходимы определенные устройства двух узлов (R1 и R3). Оба узла используют незарегистрированные IP-адреса, значит необходимо преобразовать их во время взаимодействия узлов. В данном случае хост 10.10.10.1 изменяется на 100.100.100.1, а хост 20.20.20.1 – на 200.200.200.1. Поэтому необходимо, чтобы преобразование выполнялось в обоих направлениях. Трафик между этими двумя узлами в целях учета должен проходить через R2. В итоге наши требования выглядят следующим образом:

- Хостам 10.10.10.1 узла R1 и 20.20.20.1 узла R3 необходимо взаимодействовать, используя их сетевые адреса.
- Трафик между этими узлами должен пересылаться по R2.
- В нашем случае нам нужно настроить трансляции статических адресов, как показано в конфигурации ниже.

Конфигурацию маршрутизатора NAT

Конфигурацию маршрутизатора NAT

```
interface Loopback0
ip address 4.4.4.1 255.255.255.0
ip Nat inside
!--- Создание виртуального интерфейса, называемого Loopback 0, и назначение ему IP-адреса
!--- 4.4.4.1. Кроме того, для него определяется внутренний интерфейс NAT.

!
Interface Ethernet0/0
ip address 1.1.1.2 255.255.255.0
no ip redirects
ip Nat outside
ip policy route-map Nat
!--- Назначение IP-адреса 1.1.1.1/24 для e0/0. Отмена перенаправления для того, чтобы пакеты,
!--- поступающие из R1 и предназначенные для R3, не перенаправлялись в R3 и
!--- наоборот. Определяет интерфейс в качестве внешнего интерфейса NAT. Назначает
!--- карту маршрутизации "Nat", используемую для маршрутизации, основанной на политиках.

!
ip Nat inside source static 10.10.10.1 200.200.200.1
!--- Создает статическое преобразование таким образом, чтобы для пакетов, принятых на внутреннем интерфейсе
!--- и имеющих адрес источника 10.10.10.1, выполнялось преобразование их адреса источника
!--- в 200.200.200.1. Примечание. Это предполагает, что для пакетов, принятых
!--- на внешнем интерфейсе с адресом назначения 200.200.200.1,
!--- будет выполняться преобразование адреса в 10.10.10.1.
```

```
ip Nat outside source static 20.20.20.1 100.100.100.1
!--- Создает статическое преобразование таким образом, чтобы для пакетов, принятых на внешнем интерфейсе
!--- и имеющих адрес источника 20.20.20.1, выполнялось преобразование их адреса источника
!--- в 100.100.100.1. Примечание. Это предполагает, что для пакетов, принятых на
!--- внутреннем интерфейсе и имеющих адрес назначения 100.100.100.1, будет
!--- выполняться преобразование адреса назначения в 20.20.20.1.


ip route 10.10.10.0 255.255.255.0 1.1.1.1
ip route 20.20.20.0 255.255.255.0 1.1.1.3
ip route 100.100.100.0 255.255.255.0 1.1.1.3
!
access-list 101 permit ip host 10.10.10.1 host 100.100.100.1
route-map Nat permit 10
match ip address 101
set ip next-hop 4.4.4.2
```

Пример 2. Выходные данные команд show и debug

Примечание. Интерпретатор выходных данных поддерживает некоторые команды show, что позволяет выполнять анализ выходных данных команд show. Перед использованием команд **debug** ознакомьтесь с документом Важные сведения о командах debug.

Тест 1

Как показано в конфигурации выше, есть два статических преобразования NAT, которые можно увидеть на R2 с помощью команды **show ip Nat translation**.

Ниже представлены выходные данные команды **show ip Nat translation**, выполненной NAT-маршрутизатором.

```
NAT-router# show ip Nat translation
Pro Inside global      Inside local       Outside local      Outside global
--- ---                ---                100.100.100.1      20.20.20.1
--- 200.200.200.1      10.10.10.1         ---                ---
R2#
```

В этом тесте мы получили результат команды **ping** от устройства (10.10.10.1) узла R1, предназначенного для сетевого адреса устройства (100.100.100.1) узла R3. Результат выходных данных команды **debug ip Nat** и **debug ip packet** на узле R2.

```
IP: NAT enab = 1 trans = 0 flags = 0
IP: s=10.10.10.1 (Ethernet0/0), d=100.100.100.1, Len 100, policy match
   ICMP type=8, code=0
IP: route map Nat, item 10, permit
IP: s=10.10.10.1 (Ethernet0/0), d=100.100.100.1 (Loopback0), Len 100, policy
routed
   ICMP type=8, code=0
IP: Ethernet0/0 to Loopback0 4.4.4.2
!--- Приведенные выше выходные данные указывают, что пакет, источник которого находится по адресу 10.10.10.1, а пунк
!--- по адресу 100.100.100.1, поступает на интерфейс E0/0, который определен в качестве внешнего
!--- интерфейса NAT. В этот момент выполнение каких-либо функций NAT не требуется,
!--- однако для маршрутизатора также активирована функция маршрутизации, основанной на политиках для
!--- E0/0. Из выходных данных следует, что пакет соответствует политике, которая
!--- определена в инструкциях, описывающих маршрутизацию, основанную на политиках.


IP: s=10.10.10.1 (Ethernet0/0), d=100.100.100.1 (Loopback0), g=4.4.4.2, Len 100,
forward
   ICMP type=8, code=0
IP: NAT enab = 1 trans = 0 flags = 0
!--- Теперь приведенные выше данные указывают на то, что пакет маршрутизируется на основе политики из интерфейса
!--- loopback0. Следует помнить, что интерфейс loopback определен в качестве внутреннего интерфейса NAT.


NAT: s=10.10.10.1->200.200.200.1, d=100.100.100.1 [26]
NAT: s=200.200.200.1, d=100.100.100.1->20.20.20.1 [26]
!--- Приведенные выше выходные данные указывают на то, что пакет теперь поступает на интерфейс
!--- loopback0. Поскольку это внутренний интерфейс NAT, важно
```

```
!--- отметить, что перед выполнением преобразования (информация о котором приведена выше) маршрутизатор
!--- ищет в таблице маршрутизации маршрут к пункту назначения, которому
!--- перед преобразованием все еще назначен адрес 100.100.100.1. По окончании операции
!--- поиска маршрутизатор продолжает выполнять преобразование в соответствии с указанной выше информацией.
!--- Сведения о поиске маршрут не отображаются в выходных данных команды debug.


IP: s=200.200.200.1 (Loopback0), d=20.20.20.1 (Ethernet0/0), g=1.1.1.3, Len 100,
forward
   ICMP type=8, code=0
IP: NAT enab = 1 trans = 0 flags = 0
!--- Выше приводится информация о передаче результирующего преобразованного пакета
!--- из интерфейса E0/0.
```

Здесь представлен ответный пакет полученный от устройства узла R3, предназначенный для устройства узла R1.

```
NAT: s=20.20.20.1->100.100.100.1, d=200.200.200.1 [26]
NAT: s=100.100.100.1, d=200.200.200.1->10.10.10.1 [26]
!--- Ответный пакет поступает на интерфейс e0/0, который является внешним
!--- интерфейсом NAT. В этом направлении (от внешнего к внутреннему интерфейсу) преобразование
!--- выполняется перед маршрутизацией. Приведенные выше выходные данные указывают на выполнение преобразования.


IP: s=100.100.100.1 (Ethernet0/0), d=10.10.10.1 (Ethernet0/0), Len 100, policy
rejected -- normal forwarding
   ICMP type=0, code=0
IP: s=100.100.100.1 (Ethernet0/0), d=10.10.10.1 (Ethernet0/0), g=1.1.1.1,
Len 100, forward
   ICMP type=0, code=0
!--- На интерфейсе E0/0 по-прежнему активирована функция маршрутизации, основанной на политиках, поэтому пакет
!--- проверяется на соответствие политике (см. выше). Пакет не соответствует
!--- политике и передается обычным образом.
```

Обзор

В данном документе рассматривается маршрутизация, основанная на политике и преобразовании сетевых адресов (NAT) для создания сценария NAT в одном интерфейсе. Важно помнить, что данная конфигурация может уменьшить производительность маршрутизатора, использующего NAT, так как пакеты могут быть направлены через маршрутизатор.

Дополнительные сведения

- **Страница поддержки NAT**
- **Техническая поддержка — Cisco Systems**

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/10/107579/nat-on-stick.shtml