



Настройка трансляции сетевых адресов: Начало работы

Содержание

Введение

Предварительные условия

Требования

Используемые компоненты

Условные обозначения

Краткое описание работ по конфигурации и развертыванию NAT

Определение трансляции сетевых адресов внутри и вне интерфейсов

Пример: Разрешение доступа в Интернет внутренним пользователям

Настройка NAT для разрешения доступа в Интернет внутренним пользователям

Настройка NAT для разрешения доступа в Интернет внутренним пользователям с помощью функции перегрузки

Пример: Разрешение доступа к внутренним устройствам из Интернета

Настройка NAT, разрешающая доступ из Интернета к внутренним устройствам

Пример: Переадресация трафика TCP на другой TCP-порт или адрес

Настройка NAT для того, чтобы перенаправить трафик TCP на другой порт или адрес TCP

Пример: Использование NAT во время сетевых переходов

Настройка NAT для использования при сетевых переходах

Пример: Использование NAT в перекрывающихся сетях

Проверка работы NAT

Заключение

Дополнительные сведения

Введение

В данном документе описывается настройка трансляции сетевых адресов (NAT) в маршрутизаторах Cisco для использования в стандартных сетевых сценариях. Целевая группа данного документа – это пользователи, только начавшие работу с NAT.

Примечание. В данном документе под Интернет-устройством понимается устройство в любой внешней сети.

Предварительные условия

Требования

Чтобы использовать данный документ, необходимо знание терминов, используемых в связи с NAT. Некоторые определения можно найти в документе NAT: Локальные и глобальные определения.

Используемые компоненты

Сведения, содержащиеся в данном документе, относятся к следующим версиям программного и аппаратного обеспечения:

- Маршрутизаторы Cisco серии 2500
- ПО Cisco IOS® версия 12.2 (10b)

Сведения, представленные в данном документе, были получены на тестовом оборудовании в специально созданных лабораторных

условиях. При написании данного документа использовались только данные, полученные от устройств с конфигурацией по умолчанию. При работе с реально функционирующей сетью необходимо полностью осознавать возможные последствия выполнения команд до их применения.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в разделе Технические советы Cisco. Условные обозначения.

Краткое описание работ по конфигурации и развертыванию NAT

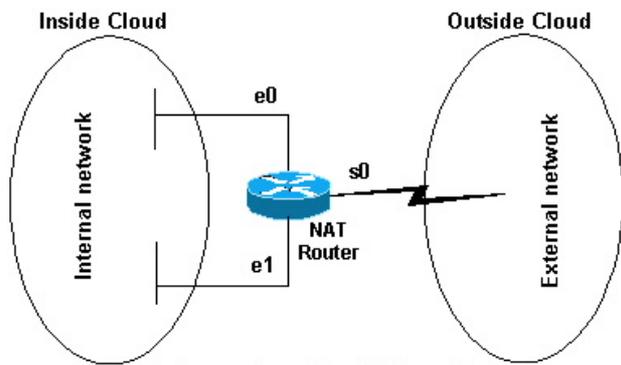
При настройке NAT иногда сложно определить, с чего начать, особенно если пользователь только начал работу с NAT. Данное руководство поможет определить, чего ждать от NAT и каким образом провести его настройку.

1. Определите NAT внутри и вне интерфейсов.
 - Доступны ли пользователи на нескольких интерфейсах?
 - Имеют ли несколько интерфейсов выход в Интернет?
2. Определите, чего вы пытаетесь достичь с помощью NAT.
 - Вы пытаетесь разрешить доступа в Интернет внутренним пользователям?
 - Вы пытаетесь разрешить доступ из Интернета к внутренним устройствам (например почтовому серверу или веб-серверу)?
 - Вы пытаетесь перенаправить трафик TCP на другой порт или адрес TCP?
 - Вы используете NAT во время сетевых переходов (к примеру, после изменения IP-адреса сервера и до обновления всех клиентов необходимо, чтобы все необновленные клиенты могли получать доступ к серверу через исходный IP-адрес, а обновленные клиенты получали доступ к серверу через новый адрес)?
 - Вы используете NAT, чтобы позволить переключаящимся сетям связываться друг с другом?
3. Чтобы выполнить описанные выше действия, настройте NAT. На основании изменений на этапе 2 необходимо определить, какие функции использовать из представленных далее:
 - Static NAT
 - Dynamic NAT
 - Overloading
 - Любая комбинация данных функций
4. Проверка работы NAT.

В каждом из следующих примеров настройки NAT выполняются этапы 1-3 данного краткого руководства. В этих примерах описаны некоторые стандартные сценарии, по которым Cisco рекомендует развертывание NAT.

Определение трансляции сетевых адресов внутри и вне интерфейсов

Первый этап развертывания NAT - определение внутренних и внешних интерфейсов NAT. Самым простым способом будет определить внутреннюю сеть как "inside", а внешнюю – как "outside". В то же время термины "внутренний" и "внешний" также являются условными. На следующем рисунке показан пример.

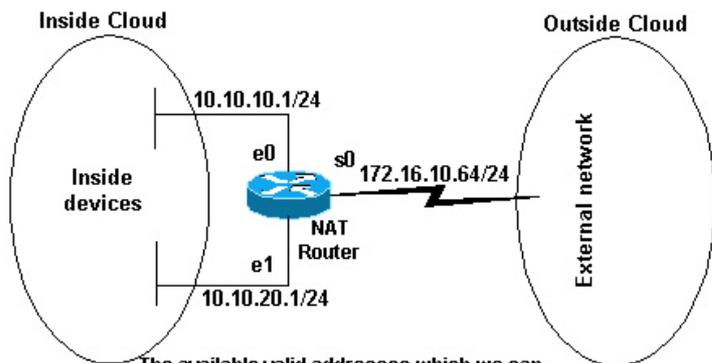


In this figure, ethernet 0 and ethernet 1 will be defined as NAT inside interfaces and serial 0 will be defined as a NAT outside interface.

Пример: Разрешение доступа в Интернет внутренним пользователям

Возможно, вы хотите предоставить доступ в Интернет внутренним пользователям, но у вас нет достаточного количества допустимых адресов. Если все взаимодействия с Интернет-устройствами возникают из внутренних устройств, то нужен один допустимый адрес или пул допустимых адресов.

На следующем рисунке показана схема простой сети с внутренним и внешним интерфейсами маршрутизатора:



The available valid addresses which we can use are in the range of 172.16.10.1 through 172.16.10.63

В этом примере NAT нужен затем, чтобы разрешить определенным внутренним устройствам (первым 31 из каждой подсети) создать связь с устройствами снаружи, преобразуя их недопустимый адрес в допустимый адрес или пул адресов. Пул задан как диапазон адресов от 172.16.10.1 до 172.16.10.63.

Теперь можно приступить к настройке NAT. Для выполнения описанных выше действий используйте функцию динамического NAT. При динамической трансляции сетевых адресов таблица трансляции в маршрутизаторе исходно является пустой и начинает заполняться после того, как трафик для трансляции проходит через маршрутизатор. (В отличие от функции статического NAT, где трансляция настраивается статически и помещается в таблицу трансляции без присутствия трафика).

В этом примере можно настроить NAT для трансляции каждого внутреннего устройства на уникальный допустимый адрес или для трансляции всех внутренних устройств на один допустимый адрес. Второй метод известен как перегрузка. Пример настройки каждого метода приведен ниже.

Настройка NAT для разрешения доступа в Интернет внутренним пользователям

Маршрутизатор NAT

```
interface ethernet 0
ip address 10.10.10.1 255.255.255.0
```

```

ip nat inside

!--- Определяет Ethernet 0 с помощью IP-адреса в качестве внутреннего интерфейса NAT.

interface ethernet 1
ip address 10.10.20.1 255.255.255.0
ip nat inside

!--- Определяет Ethernet 1 с помощью IP-адреса в качестве внутреннего интерфейса NAT.

interface serial 0
ip address 172.16.10.64 255.255.255.0
ip nat outside

!--- Определяет serial 0 с помощью IP-адреса в качестве внешнего интерфейса NAT.

ip nat pool no-overload 172.16.10.1 172.16.10.63 prefix 24
!

!--- Определяет пул NAT под названием "no-overload" с помощью ряда адресов
!--- 172.16.10.1 - 172.16.10.63.

ip nat inside source list 7 pool no-overload
!
!

!--- Указывает на то, что адреса источников любых пакетов, полученных на внутреннем интерфейсе,
!--- допускаемых в списке доступа 7,
!--- преобразованы в адрес "no-overload"
!--- вне пула NAT.

access-list 7 permit 10.10.10.0 0.0.0.31
access-list 7 permit 10.10.20.0 0.0.0.31

!--- Список доступа 7 открывает доступ пакетам с адресами источника от
!--- 10.10.10.0 до 10.10.10.31 и от 10.10.20.0 до 10.10.20.31.

```

Примечание. Cisco настоятельно рекомендует не настраивать списки доступа, упоминаемые в командах NAT, с помощью команды **permit any**. Использование команды **permit any** может привести к тому, что NAT будет потреблять слишком большое количество ресурсов маршрутизатора, что вызовет проблемы с сетью.

В приведенной выше конфигурации следует отметить, что только первые 32 адреса из подсети 10.10.10.0 и первые 32 адреса из подсети 10.10.20.0 разрешены **списком доступа 7**. Таким образом, выполняется преобразование только этих исходных адресов. Внутренняя сеть может содержать другие устройства с другими адресами, которые не транслируются.

Последнее, что нужно сделать — это убедиться в надлежащей работе NAT.

Настройка NAT для разрешения доступа в Интернет внутренним пользователям с помощью функции перегрузки

Маршрутизатор NAT

```

interface ethernet 0
ip address 10.10.10.1 255.255.255.0
ip nat inside

!--- Определяет Ethernet 0 с помощью IP-адреса в качестве внутреннего интерфейса NAT.

interface ethernet 1
ip address 10.10.20.1 255.255.255.0
ip nat inside

!--- Определяет Ethernet 1 с помощью IP-адреса в качестве внутреннего интерфейса NAT.

interface serial 0
ip address 172.16.10.64 255.255.255.0
ip nat outside

```

```
!--- Определяет serial 0 с помощью IP-адреса в качестве внешнего интерфейса NAT.

ip nat pool ovrld 172.16.10.1 172.16.10.1 prefix 24
!

!--- Определяет пул NAT под названием "ovrld" с помощью одиночного IP-адреса
!--- 172.16.10.1.

ip nat inside source list 7 pool ovrld overload
!
!
!
!

!--- Указывает на то, что адреса источников любых пакетов, полученных на внутреннем интерфейсе,
!--- допускаемых в списке доступа 7, будут транслированы в
!--- адреса, вне пула NAT под названием "ovrld".
!--- Трансляции будут перегружены, что позволит нескольким внутренним устройствам
!--- транслироваться на один и тот же допустимый IP-адрес.

access-list 7 permit 10.10.10.0 0.0.0.31
access-list 7 permit 10.10.20.0 0.0.0.31

!--- Список доступа 7 открывает доступ пакетам с адресами источника от
!--- 10.10.10.0 до 10.10.10.31 и от 10.10.20.0 до 10.10.20.31.
```

Заметьте, что выше во второй конфигурации пул NAT "ovrld" имеет диапазон только из одного адреса. Ключевое слово **overload**, используемое в команде **ip nat inside source list 7 pool ovrld overload**, позволяет NAT транслировать несколько внутренних устройств на один адрес в пуле.

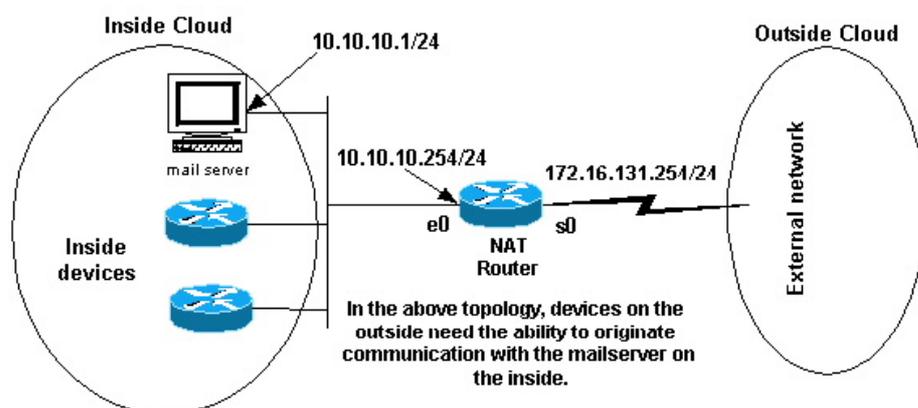
Еще одной формой данной команды является команда **ip nat inside source list 7 interface serial 0 overload**, которая настраивает NAT для перегрузки по адресу, присвоенному последовательному интерфейсу 0.

После настройки перегрузки в маршрутизаторе накапливается достаточное количество данных протоколов высокого уровня (к примеру, номера портов TCP или UDP) для обратной трансляции глобального адреса на правильный локальный адрес. Определения глобального и локального адреса см. в NAT: Локальные и глобальные определения.

Последним действием является проверка работы NAT в должном порядке.

Пример: Разрешение доступа к внутренним устройствам из Интернета

Может понадобиться обеспечить информационный обмен между устройствами внутренней сети и устройствами в Интернете, при котором соединение инициируется внешним устройством, например обмен сообщениями электронной почты. Для устройств в Интернете типично отправлять почту на почтовый сервер, находящийся во внутренней сети.



Настройка NAT, разрешающая доступ из Интернета к внутренним устройствам

В этом примере в первую очередь происходит определение внутренних и внешних интерфейсов NAT, как показано на сетевой диаграмме выше.

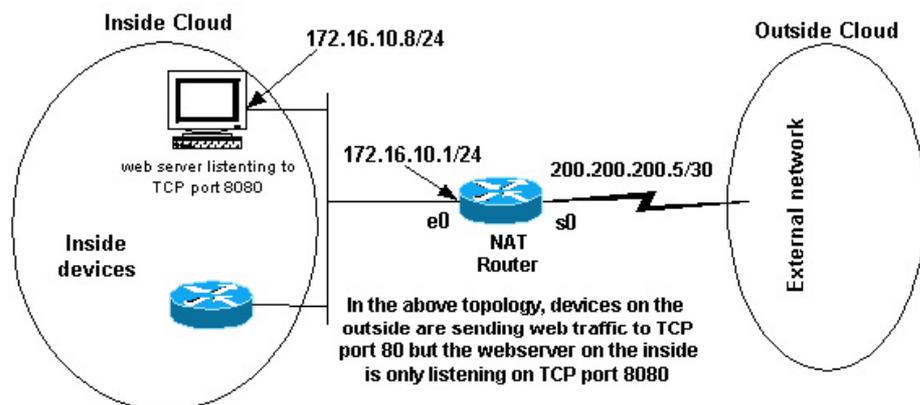
Во-вторых, определяется, что внутренние пользователи могут создавать связь с внешними устройствами. Необходимо, чтобы внешние устройства могли устанавливать связь только с внутренним почтовым сервером.

Третий этап — настройка NAT. Чтобы завершить начатый процесс, можно настроить статический и динамический NAT вместе. Дополнительная информация о настройке, описанной в данном примере, содержится в документе Одновременная настройка статического и динамического NAT.

Последним действием является проверка работы NAT в должном порядке.

Пример: Переадресация трафика TCP на другой TCP-порт или адрес

Наличие веб-сервера во внутренней сети — это еще один пример, когда для устройств в Интернете может оказаться необходимым инициировать взаимодействие с внутренними устройствами. В некоторых случаях внутренний веб-сервер может быть настроен для взаимодействия с веб-трафиком через порт TCP, а не порт 80. К примеру, внутренний веб-сервер может устанавливать соединение через порт TCP 8080; в этом случае можно использовать NAT для перенаправления трафика, предназначенного для порта TCP 80 к порту TCP 8080.



После определения интерфейсов, как показано на схеме сети выше, NAT может перенаправлять внешние пакеты, предназначенные для адресов от 172.16.10.8:80 до 172.16.10.8:8080. Для этого можно транслировать номер порта TCP с помощью команды "static nat". Пример конфигурации приведен ниже.

Настройка NAT для того, чтобы перенаправить трафик TCP на другой порт или адрес TCP

Маршрутизатор NAT

```
interface ethernet 0
ip address 172.16.10.1 255.255.255.0
ip nat inside
```

!--- Определяет Ethernet 0 с помощью IP-адреса в качестве внутреннего интерфейса NAT.

```
interface serial 0
ip address 200.200.200.5 255.255.255.252
ip nat outside
```

!--- Определяет serial 0 с помощью IP-адреса в качестве внешнего интерфейса NAT.

```
ip nat inside source static tcp 172.16.10.8 8080 172.16.10.8 80
```

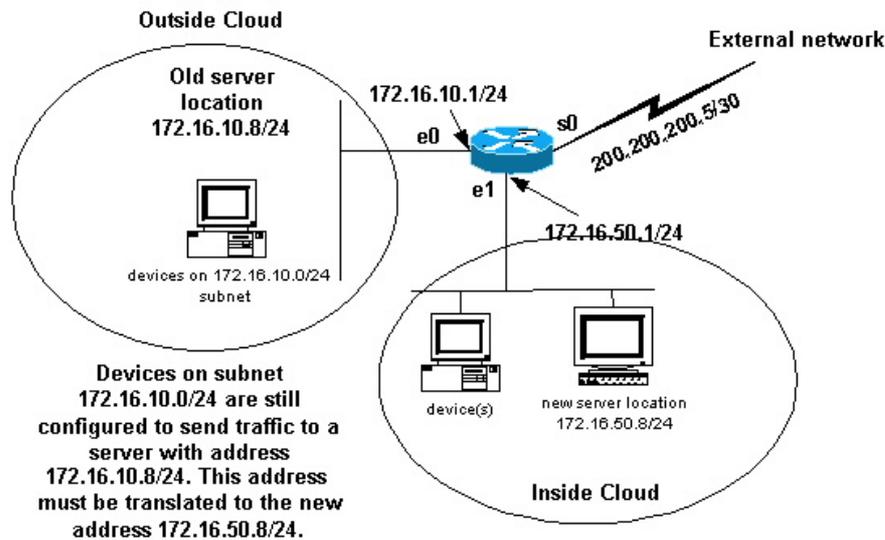
!--- Команда статического NAT, которая задает, чтобы все пакеты, полученные внутренним интерфейсом с IP-адресом источника 172.16.10.8:8080, были преобразованы в 172.16.10.8:80.

Учтите, что описание настройки статической команды NAT указывает, что все пакеты, полученные внутренним интерфейсом с адресом источника 172.16.10.8:8080, будут преобразованы в 172.16.10.8:80. Это также подразумевает, что все пакеты, полученные внешним интерфейсом с адресом назначения 172.16.10.8:80, будут преобразованы в 172.16.10.8:8080.

Последним действием является проверка работы NAT в должном порядке.

Пример: Использование NAT во время сетевых переходов

Развертывание NAT может потребоваться для переадресования устройств сети или при замене одного устройства другим. Например, если все устройства в сети используют определенный сервер и этот сервер необходимо заменить новым сервером с новым IP-адресом, то перенастройка всех сетевых устройств, использующих новый адрес сервера, займет определенное время. Однако можно использовать NAT для настройки устройств, использующих старые адреса, чтобы транслировать их пакеты для связи с новым сервером.



После определения интерфейсов NAT, как показано выше, NAT может транслировать внешние пакеты, направленные на адреса старого сервера (172.16.10.8), и направлять их на новый адрес сервера. Обратите внимание, что новый сервер относится к другой сети LAN и устройства, находящиеся в этой сети или достижимые через нее (устройства из внутренней части сети), следует настроить на (по возможности) IP-адрес нового сервера.

Для этого можно использовать статическое преобразование сетевых адресов (NAT). Пример конфигурации приведен ниже.

Настройка NAT для использования при сетевых переходах

Маршрутизатор NAT

```
interface ethernet 0
ip address 172.16.10.1 255.255.255.0
ip nat outside
```

!--- Определяет Ethernet 0 с помощью IP-адреса в качестве внешнего интерфейса NAT.

```
interface ethernet 1
ip address 172.16.10.64 255.255.255.0
ip nat inside
```

!--- Определяет Ethernet 1 с помощью IP-адреса в качестве внутреннего интерфейса NAT.

```
interface serial 0
ip address 200.200.200.5 255.255.255.252
```

!--- Определяет интерфейс serial 0 с помощью IP-адреса. Этот интерфейс

```
!--- не участвует в NAT.
```

```
ip nat inside source static 172.16.50.8 172.16.10.8
```

```
!--- Указывает на то, что IP-адреса источников 172.16.50.8 любых пакетов, полученных на внутреннем интерфейсе,  
!--- будут преобразованы в 172.16.10.8.
```

Обратите внимание на то, что команда внутреннего источника NAT в данном примере также подразумевает, что адрес назначения пакетов, полученных на внешнем интерфейсе, 172.16.10.8, будет преобразован в адрес 172.16.50.8.

Последним действием является проверка работы NAT в должном порядке.

Пример: Использование NAT в перекрывающихся сетях

Перекрывание сетей возникает, когда внутренним устройствам присваиваются IP-адреса, уже используемые другими устройствами в Интернете. Также перекрывание происходит, когда сливаются две компании, использующие в своих сетях IP-адреса RFC 1918. Эти две сети должны общаться, желательно без необходимости переадресации своих устройств. Дополнительная информация о настройке NAT для этой цели содержится в документе [Использование NAT в перекрывающихся сетях](#).

Проверка работы NAT

После настройки NAT убедитесь, что он работает, как нужно. Это можно сделать несколькими способами: с помощью сетевого анализатора, команд **show** или **debug**. Подробный пример проверки NAT содержится в документе [Проверка работы и устранение основных неисправностей NAT](#).

Заключение

В примерах в данном документе содержится краткое руководство, которое поможет настроить и развернуть NAT. К действиям, описанным в руководстве, относится следующее:

1. Определение NAT внутри интерфейсов и за их пределами.
2. Определение, чего вы пытаетесь достичь с помощью NAT.
3. Настройка NAT для выполнения задачи, сформулированной на этапе 2.
4. Проверка работы NAT.

В каждом из вышеуказанных примеров были использованы различные формы команды **ip nat inside**. Для этого также можно использовать команду **ip nat outside**, не забывая о порядке работы NAT. Примеры настройки с помощью команд **ip nat outside** содержатся в документе [Пример настройки с использованием команды ip nat outside source list и ip nat outside source static](#).

Также в примерах выше представлено следующее:

Действие	команды
<code>ip nat inside source</code>	<ul style="list-style-type: none">• Преобразует источник IP-пакетов, перемещающихся изнутри наружу.• Транслирует конечную точку IP-пакетов, проходящих снаружи внутрь.

<p>Команда <code>ip nat outside source</code></p>	<ul style="list-style-type: none">• Транслирует источник IP-пакетов, перемещающихся снаружи внутрь.• Преобразует назначения IP-пакетов, перемещающихся изнутри наружу.
---	---

Дополнительные сведения

- [Страница поддержки NAT](#)
- [Страница поддержки маршрутизируемых IP-протоколов](#)
- [Страница поддержки IP-маршрутизации](#)
- [Как работает NAT](#)
- [Порядок работы NAT](#)
- [Часто задаваемые вопросы о ПО Cisco IOS NAT](#)
- [Техническая поддержка - Cisco Systems](#)

© 1992-2010 Cisco Systems, Inc. Все права защищены.

Дата генерации PDF файла: Jan 05, 2010

<http://www.cisco.com/support/RU/customer/content/9/92026/12.shtml>
