

# Настройка трансляции сетевых адресов: Начало работы

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Краткое руководство по началу конфигурации и развертыванию NAT](#)

[Определение трансляции сетевых адресов внутри и вне интерфейсов](#)

[Пример: Разрешение доступа в Интернет внутренним пользователям](#)

[Конфигурация NAT для разрешения доступа в Интернет внутренним пользователям](#)

[Конфигурация NAT для разрешения доступа в Интернет внутренним пользователям с использованием перегрузки](#)

[Пример: Разрешение доступа к внутренним устройствам из Интернета](#)

[Настройка преобразования сетевых адресов \(NAT\), чтобы разрешить доступ из Интернета к внутренним устройствам](#)

[Пример: Переадресация трафика TCP на другой TCP-порт или адрес](#)

[Конфигурирование трансляции сетевых адресов 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](#)

[Различие между однозначным сопоставлением и многие ко многим](#)

[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**

Этот документ требует базовых знаний о терминах, использованных в связи с NAT. Некоторые определения могут быть найдены в [NAT: Локальные и глобальные определения](#).

## Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

Маршрутизаторы Cisco серии 2500

ПО Cisco IOS® версии 12.2 (10b)

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

## Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.](#)

## Краткое руководство по началу конфигурации и развертыванию NAT

При настройке NAT иногда трудно знать, где начать, особенно если вы плохо знакомы с NAT. Эти шаги ведут вас для определения то, что вы хотите, чтобы NAT сделал и как настроить его:

[Определите NAT внутри и вне интерфейсов.](#)

Доступны ли пользователи на нескольких интерфейсах?

Имеют ли несколько интерфейсов выход в Интернет?

Определите, чего вы пытаетесь достичь с помощью NAT.

[Вы пытаетесь разрешить доступа в Интернет внутренним пользователям?](#)

[Вы пытаетесь разрешить доступ Интернет к внутренним устройствам \(например, почтовому серверу или веб-серверу\)?](#)

[Предпринимается попытка 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 перекрывающимся сетям связываться друг с другом?](#)

Чтобы закончить сделанное выше, настройте NAT. На основании изменений на этапе 2 необходимо определить, какие функции использовать из представленных далее:

Статический NAT

Динамический NAT

Перегрузка

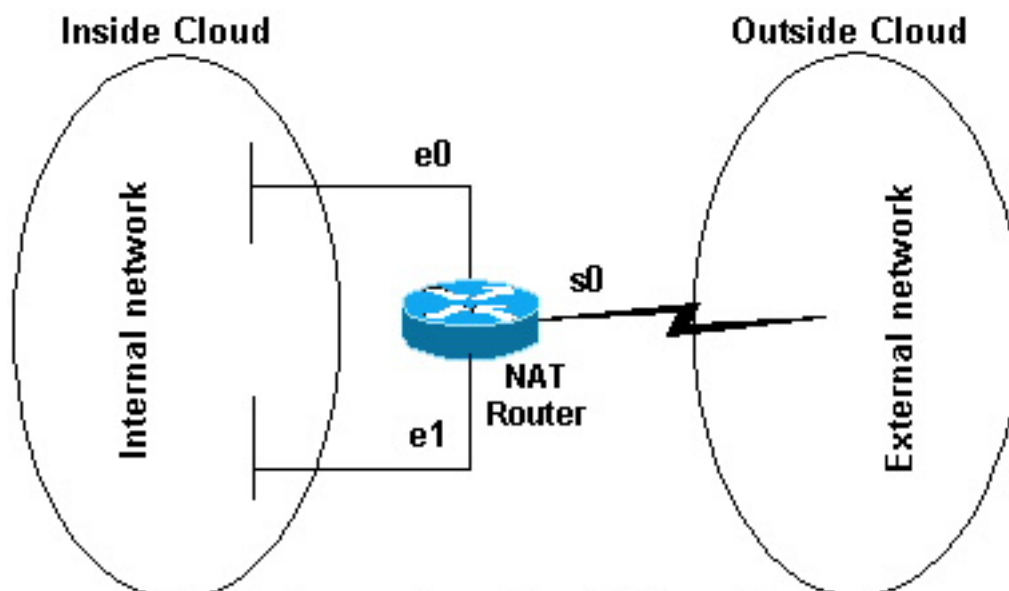
Любая комбинация вышеупомянутого

Проверьте работу NAT.

Каждый из этих примеров преобразования NAT ведет вас посредством шагов 1 - 3 Пунктов Краткого руководства по началу работы выше. В этих примерах описаны некоторые стандартные сценарии, по которым Cisco рекомендует развертывание NAT.

## [Определение трансляции сетевых адресов внутри и вне интерфейсов](#)

Первый шаг для развертывания NAT должен определить Внутренние и внешние интерфейсы 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. Эти данные показывают пример этого.

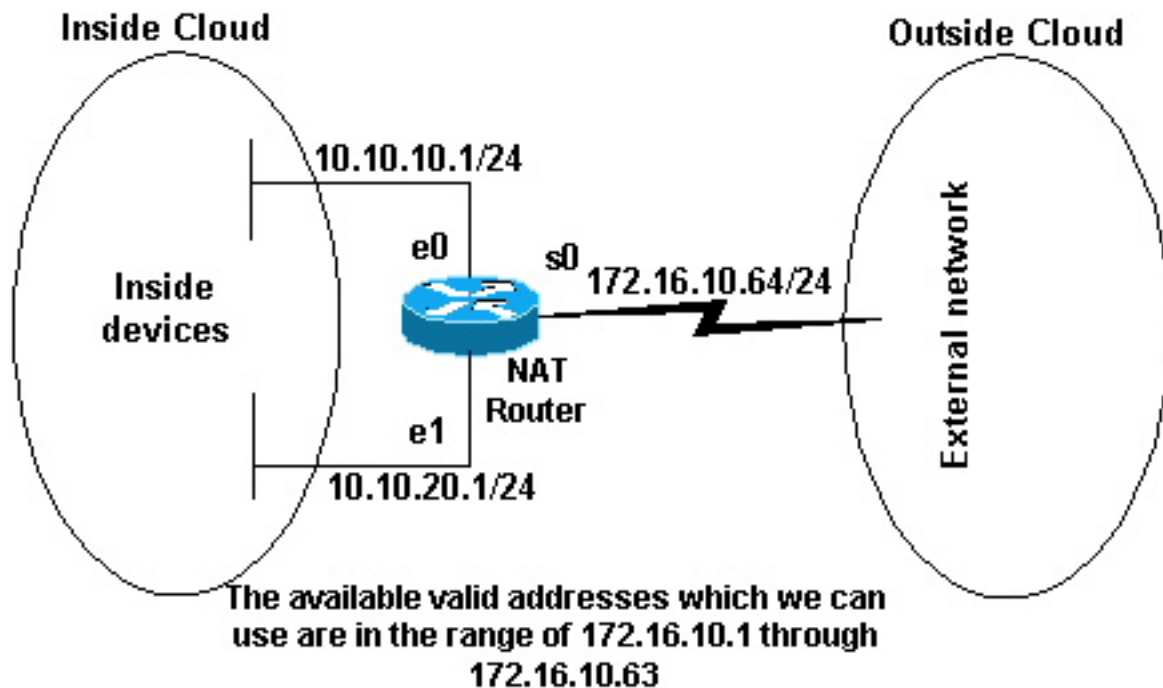


**In this figure, ethernet 0 and ethernet 1 will be defined as NAT inside interfaces and serial 0 will be defined as a NAT outside interface.**

## [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 вся связь с устройствами в Интернете происходит из внутренних устройств, вам нужны одиночный допустимый адрес или пул допустимых адресов.

Эти данные показывают схему простой сети с интерфейсами маршрутизатора, определенными как внутри и снаружи:



В данном примере вы хотите, чтобы NAT позволил определенным устройствам (первые 31 от каждой подсети) на внутренней части инициировать связь с устройствами на внешней стороне путем перевода их недопустимого адреса 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 данном примере можно настроить NAT, чтобы преобразовать каждое из внутренних устройств к уникальному действительному адресу или преобразовать каждое из внутренних устройств к тому же допустимому адресу. Второй метод известен как перегрузка. Пример того, как настроить каждый метод, дан здесь.

## [Конфигурация 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
 !--- Defines Ethernet 0 with an IP address and as a NAT
 inside interface. interface ethernet 1 ip address
 10.10.20.1 255.255.255.0 ip nat inside !--- Defines
 Ethernet 1 with an IP address and as a NAT inside
 interface. interface serial 0 ip address 172.16.10.64
 255.255.255.0 ip nat outside !--- Defines serial 0 with
 an IP address and as a NAT outside interface. ip nat
 pool no-overload 172.16.10.1 172.16.10.63 prefix 24 ! -
 -- Defines a NAT pool named no-overload with a range of
 addresses !--- 172.16.10.1 - 172.16.10.63. ip nat inside
```

```
source list 7 pool no-overload ! ! !--- Indicates that
any packets received on the inside interface that !---
are permitted by access-list 7 has !--- the source
address translated to an address out of the !--- NAT
pool "no-overload". access-list 7 permit 10.10.10.0
0.0.0.31 access-list 7 permit 10.10.20.0 0.0.0.31 !---
Access-list 7 permits packets with source addresses
ranging from !--- 10.10.10.0 through 10.10.10.31 and
10.10.20.0 through 10.10.20.31.
```

**Примечание:** Cisco настоятельно рекомендует, чтобы вы не настраивали списки доступа, на которые ссылаются команды NAT с разрешением никто. Использование команды permit any может привести к тому, что NAT будет потреблять слишком большое количество ресурсов маршрутизатора, что вызовет проблемы с сетью.

Заметьте в предыдущей конфигурации, что только первые 32 адреса от подсети 10.10.10.0 и первые 32 адреса от подсети 10.10.20.0 разрешены access-list 7. Таким образом, выполняется преобразование только этих исходных адресов. Могут быть другие устройства с другими адресами на внутренней сети, но они не преобразованы.

[Последним действием является проверка работы NAT в должном порядке.](#)

## Конфигурация NAT для разрешения доступа в Интернет внутренним пользователям с использованием перегрузки

### Маршрутизатор NAT

```
interface ethernet 0
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 !--- Defines Ethernet 0 with an IP address and as a NAT
 inside interface. interface ethernet 1 ip address
 10.10.20.1 255.255.255.0 ip nat inside !--- Defines
 Ethernet 1 with an IP address and as a NAT inside
 interface. interface serial 0 ip address 172.16.10.64
 255.255.255.0 ip nat outside !--- Defines serial 0 with
 an IP address and as a NAT outside interface. ip nat
 pool ovrlld 172.16.10.1 172.16.10.1 prefix 24 ! !---
 Defines a NAT pool named ovrlld with a range of a single
 IP !--- address, 172.16.10.1. ip nat inside source list
 7 pool ovrlld overload ! ! ! ! !--- Indicates that any
 packets received on the inside interface that !--- are
 permitted by access-list 7 has the source address !---
 translated to an address out of the NAT pool named
 ovrlld. !--- Translations are overloaded, which allows
 multiple inside !--- devices to be translated to the
 same valid IP address. access-list 7 permit 10.10.10.0
 0.0.0.31 access-list 7 permit 10.10.20.0 0.0.0.31 !---
 Access-list 7 permits packets with source addresses
 ranging from !--- 10.10.10.0 through 10.10.10.31 and
 10.10.20.0 through 10.10.20.31.
```

Обратите внимание в предыдущей второй конфигурации, пул NAT "ovrlld" только имеет диапазон одного адреса. Ключевое слово overload, используемое в команде ip nat inside source list 7 pool ovrlld overload, позволяет NAT транслировать несколько внутренних устройств на один адрес в пуле.

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

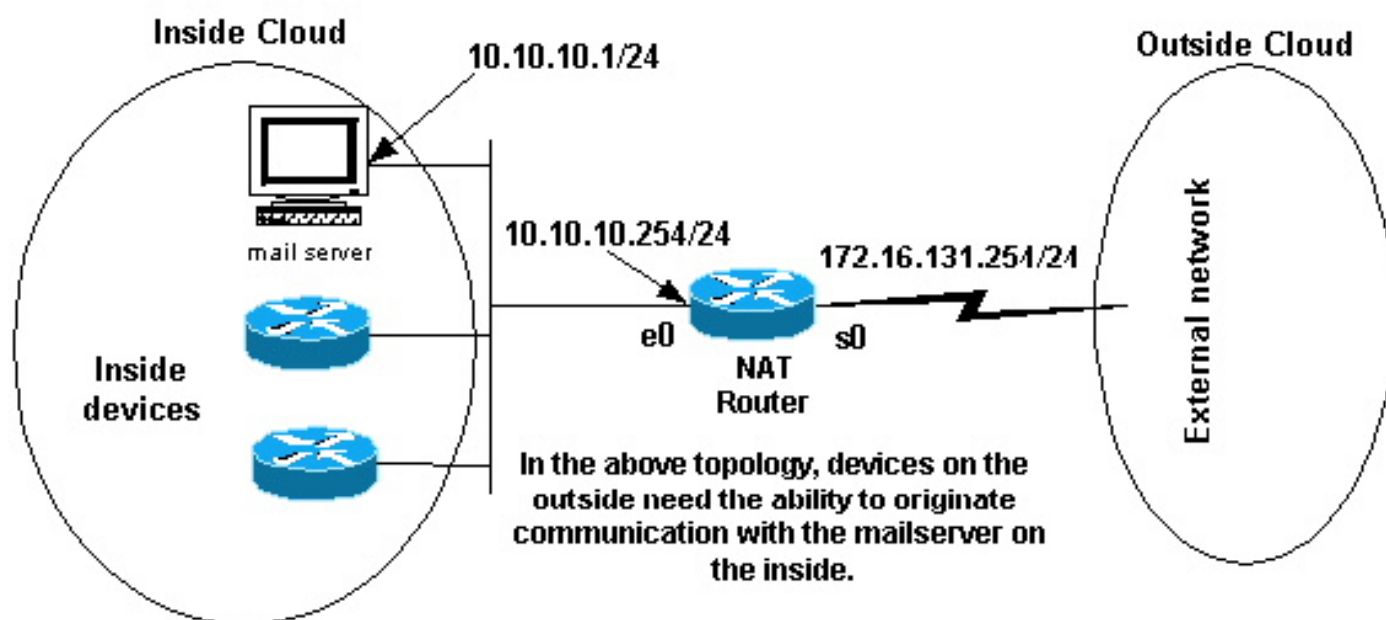
последовательному интерфейсу 0.

После настройки перезагрузки 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. Это типично для устройств в Интернете для отправки электронного письма почтовому серверу, который находится на внутренней сети.



## Настройка преобразования сетевых адресов (NAT), чтобы разрешить доступ из Интернета к внутренним устройствам

В данном примере вы сначала определяете Внутренние и внешние интерфейсы NAT, как показано в предыдущей схеме сети.

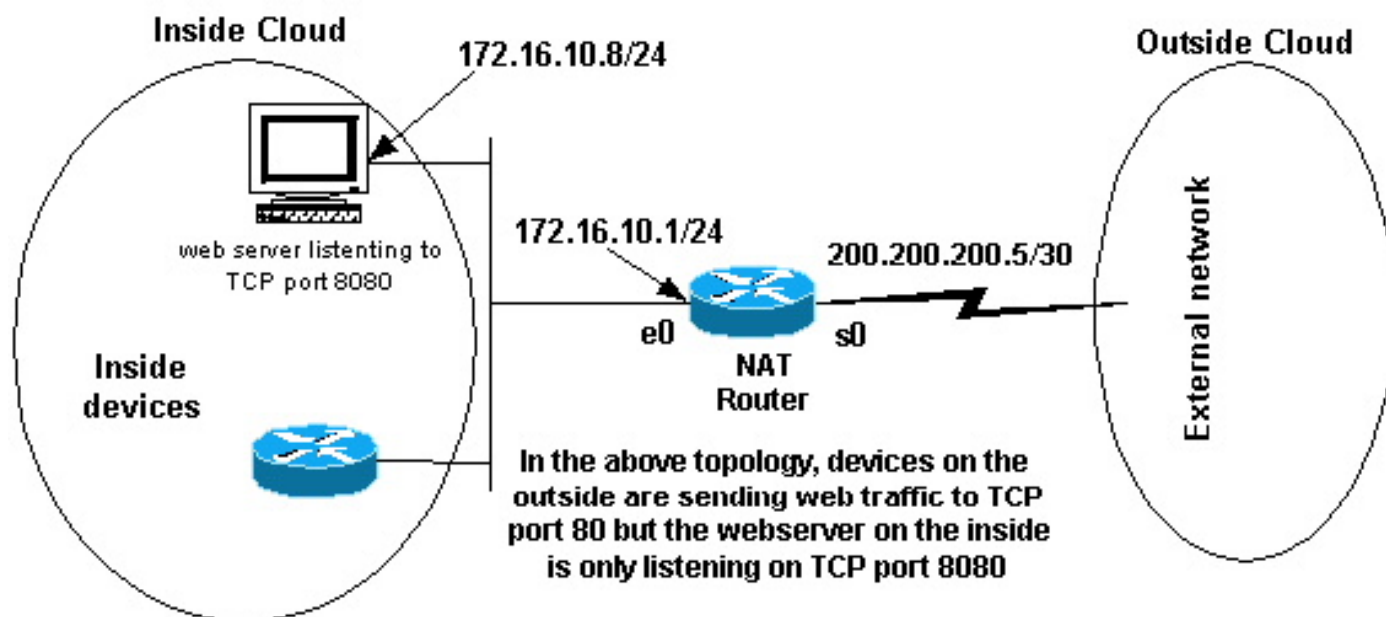
Во-вторых, вы определяете это, вы хотите, чтобы пользователи на внутренней части были в состоянии инициировать связь с внешней стороной. Необходимо, чтобы внешние устройства могли устанавливать связь только с внутренним почтовым сервером.

Шаг третий должен настроить NAT. Для выполнения, что вы определили 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 в предыдущей схеме сети можно решить, что вы хотите, чтобы NAT перенаправил пакеты с внешней стороны, предназначенной для 172.16.10.8:80 к 172.16.10.8:8080. Можно использовать команду статической трансляции сетевых адресов для перевода номера порта TCP для достижения этого. Пример конфигурации показывают здесь.

## Конфигурирование трансляции сетевых адресов 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
 !--- Defines Ethernet 0 with an IP address and as a NAT
 inside interface. interface serial 0 ip address
 200.200.200.5 255.255.255.252 ip nat outside !---
 Defines serial 0 with an IP address and as a NAT outside
 interface. ip nat inside source static tcp 172.16.10.8
 8080 172.16.10.8 80 !--- Static NAT command that states
 any packet received in the inside !--- interface with a
 source IP address of 172.16.10.8:8080 is !--- translated
 to 172.16.10.8:80.
```

Обратите внимание на то, что описание конфигурации для команды статической трансляции сетевых адресов указывает, что любой пакет, полученный во внутреннем



интерфейсе с адресом источника 172.16.10.8:8080, преобразован в 172.16.10.8:80. Это также подразумевает, что любому пакету, полученному на внешнем интерфейсе с адресом назначения (DA) 172.16.10.8:80, преобразовали назначение в 172.16.10.8:8080.

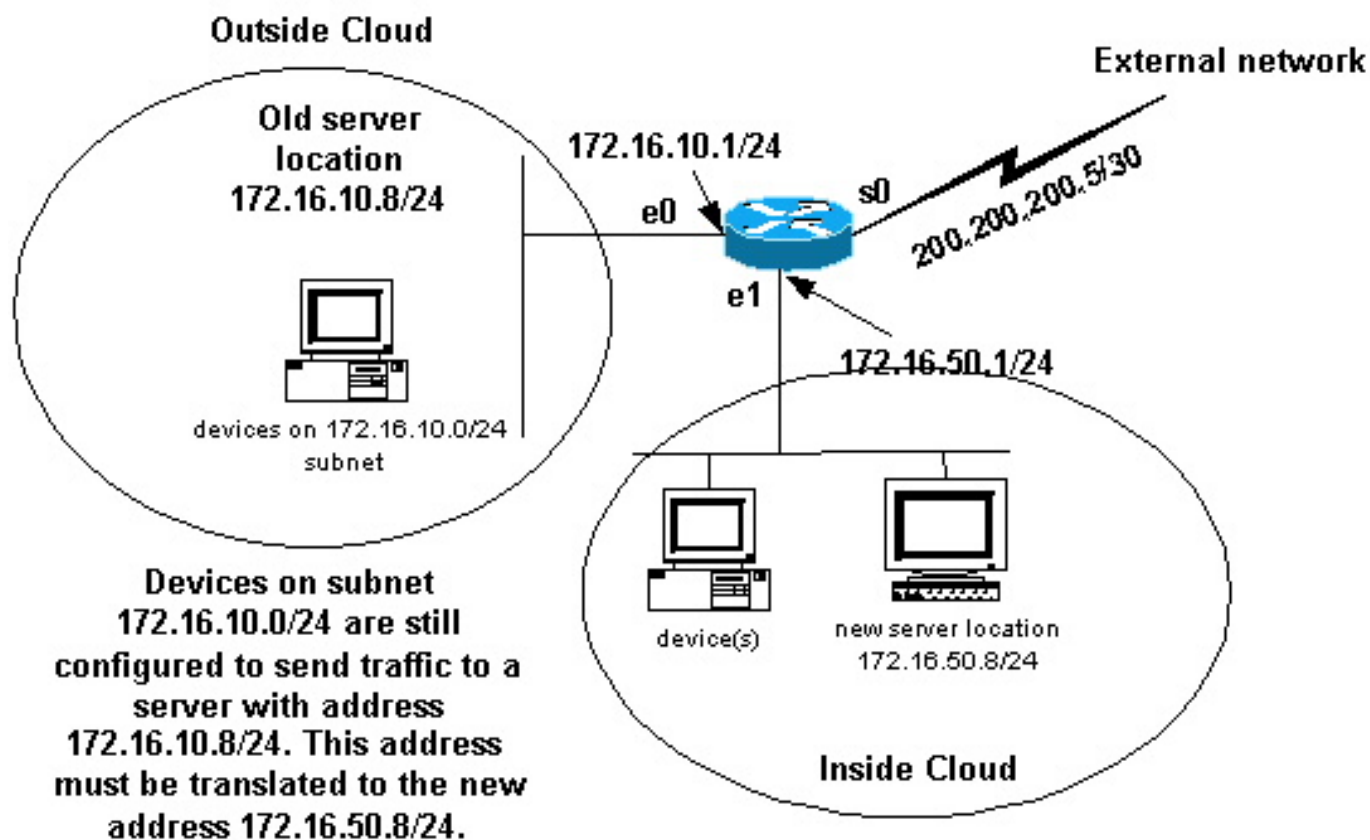
[Последним действием является проверка работы NAT в должном порядке.](#)

```
show ip nat translations
```

```
Pro Inside global      Inside local      Outside local     Outside global
tcp 172.16.10.8:80     172.16.10.8:8080 ---               ---
```

## [Пример: Использование NAT во время сетевых переходов](#)

Развертывание NAT полезно, когда необходимо переадресовать устройства в сети или когда вы заменяете одно устройство другим. Например, если все устройства в использовании сети, индивидуальный сервер и этот сервер должны быть заменены новым, который имеет новый IP-адрес, изменение конфигурации всех сетевых устройств для использования нового адреса сервера, занимают время. Тем временем можно использовать NAT для настройки устройств со старым адресом для перевода их пакетов для передачи 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 использование (по возможности) IP-адреса нового сервера.

Для этого можно использовать статическое преобразование сетевых адресов (NAT). Вот примерная конфигурация.

## 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
 !--- Defines Ethernet 0 with an IP address and as a NAT
 outside interface. interface ethernet 1 ip address
 172.16.50.1 255.255.255.0 ip nat inside !--- Defines
 Ethernet 1 with an IP address and as a NAT inside
 interface. interface serial 0 ip address 200.200.200.5
 255.255.255.252 !--- Defines serial 0 with an IP
 address. This interface is not !--- participating in
 NAT. ip nat inside source static 172.16.50.8 172.16.10.8
 !--- States that any packet received on the inside
 interface with a !--- source IP address of 172.16.50.8
 is translated to 172.16.10.8.
```

Обратите внимание на то, что внутренняя исходная команда NAT в данном примере также подразумевает, что пакетам, полученным на внешнем интерфейсе с адресом назначения (DA) 172.16.10.8, преобразовали адрес назначения (DA) в 172.16.50.8.

[Последним действием является проверка работы NAT в должном порядке.](#)

## Пример: Использование NAT в перекрывающихся сетях

Перекрывание сетей с возникает, когда внутренним устройствам присваиваются IP-адреса, уже используемым другими устройствами в Интернете. [Перекрывающиеся сети также возникают, когда две компании, обе из которых в своих сетях используют RFC 1918 IP-адреса, сливаются.](#) Эти две сети должны общаться, желательно без необходимости переадресации своих устройств. См. [Использование NAT в Наложениях сети](#) для получения дополнительной информации о конфигурации NAT для этой цели.

## Различие между однозначным сопоставлением и многие ко многим

Конфигурация статического NAT создает сопоставление "один к одному" и преобразует определенный адрес в другой адрес. Данный тип конфигурации создает в таблице NAT постоянную запись, существующую до тех пор, пока существует конфигурация, и разрешает инициировать соединения как внутренним, так и внешним хостам. Это главным образом полезно для хостов, которые предоставляют сервисы приложения как почта, сеть, FTP и т.д. Пример:

```
Router(config)#ip nat inside source static 10.3.2.11 10.41.10.12 Router(config)#ip nat inside
source static 10.3.2.12 10.41.10.13
```

Динамический NAT полезен, когда меньше адресов доступно, чем фактическое количество хостов, которые будут преобразованы. Когда хост инициирует соединение и устанавливает однозначное сопоставление между адресами, это создает запись в таблице NAT. Но, сопоставление может варьироваться, и оно зависит от зарегистрированного адреса, доступного в пуле во время связи. Динамический NAT позволяет сеансам инициироваться только изнутри или внешние сети, для которых он настроен. Динамические Записи NAT удалены из таблицы преобразования, если хост не связывается для определенного периода времени, который конфигурируем. Адрес тогда возвращен к пулу для

использования другим хостом.

Например, выполните эти шаги подробной конфигурации:

Создайте пул адресов

```
Router(config)#ip nat pool MYPOOLEXAMPLE 10.41.10.1 10.41.10.41 netmask 255.255.255.0
```

Создайте access-list для внутренних сетей, который должен быть сопоставлен

```
Router(config)#access-list 100 permit ip 10.3.2.0 0.0.0.255 any
```

Привяжите access-list 100, который выбирает внутреннюю сеть 10.3.2.0 0.0.0.255, чтобы быть преобразованным посредством NAT к пулу MYPOOLEXAMPLE и затем перегрузить адреса.

```
Router(config)#ip nat inside source list 100 pool MYPOOLEXAMPLE overload
```

## 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:

Определение трансляции сетевых адресов внутри и вне интерфейсов.

Определение, чего вы пытаетесь достичь с помощью NAT.

Настройка NAT для выполнения задачи, сформулированной на этапе 2.

Проверка работы NAT.

В каждом из предыдущих примеров использовались различные формы команды `ip nat inside`. Можно также использовать команду `ip nat outside`, чтобы выполнить те же цели, но иметь в виду заказ NAT операций. Для примеров конфигурации, которые используют команды `ip nat outside`, обратитесь к [Примеру конфигурации Использование Команды ip nat outside source list](#) и [Примера конфигурации Использование Команды ip nat outside source static](#).

Предыдущие примеры также продемонстрировали эти действия:

Команда	Действие
<code>ip nat</code>	<ul style="list-style-type: none"><li>• Преобразует источник пакетов IP,</li></ul>

<b>inside source</b>	перемещающихся изнутри наружу. • Преобразует место назначения пакетов IP, перемещающихся снаружи внутрь.
<b>ip nat outside source</b>	• Транслирует источник пакетов IP, перемещающихся снаружи внутрь. • Транслирует конечные адреса исходящих IP-пакетов.

## [Дополнительные сведения](#)

- [Страница поддержки NAT](#)
- [Протоколы маршрутизируемые по IP](#)
- [Страница поддержки IP-маршрутизации](#)
- [Работа NAT](#)
- [Преобразование сетевых адресов: порядок работы](#)
- [Часто задаваемые вопросы о ПРЕОБРАЗОВАНИИ СЕТЕВЫХ АДРЕСОВ В CISCO IOS](#)
- [Cisco Systems – техническая поддержка и документация](#)