

Настройка трансляции сетевых адресов и преобразование адреса статического порта для поддержки внутреннего веб-сервера

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Общие сведения](#)

[Настройка](#)

[Схема сети](#)

[!--- конфигурацию](#)

[Проверка](#)

[Устранение неполадок](#)

[Дополнительные сведения](#)

Введение

Cisco IOS® Network Address Translation (NAT) разработан для упрощения и защиты IP-адресов. Эта технология позволяет объединенным сетям с частными (незарегистрированными) IP-адресами подключаться к Интернету. NAT действует на маршрутизаторе Cisco, соединяющем друг с другом две сети, и преобразует частные (внутренние локальные) адреса, применяемые во внутренней сети, в публичные адреса (действующие за пределами локальной сети) до передачи пакетов в другую сеть. Как часть этой функциональной возможности, вы можете настроить NAT так, что только один адрес для всей сети будет афишироваться во внешнем мире. Тем самым внутренняя сеть фактически скрывается от остального мира. Поэтому дополнительным преимуществом NAT является укрепление безопасности.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям

программного обеспечения и оборудования.

Условные обозначения

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

Общие сведения

Одна из основных характеристик NAT является преобразованием адреса статического порта (PAT), который также упоминается как "перегрузка" в Конфигурации Cisco IOS. Статический PAT разработан для разрешения однозначного сопоставления между локальной переменной и глобальными адресами. Стандартное назначение статичного PAT - это разрешить пользователям Интернета из общедоступной сети иметь доступ к веб-серверу, расположенному в частной сети.

[Чтобы получить дополнительную информацию о NAT, см. Страницы технической поддержки NAT.](#)

Эта таблица показывает три блока пространства IP-адресов, доступного для частных сетей. Консультируйтесь [с RFC 1918](#) для получения дополнительной информации об этих специальных сетях.

Пространство IP-адресов	Класс
10.0.0.0 - 10.255.255.255 (префикс 10/8)	Класс А
172.16.0.0 - 172.31.255.255 (префикс 172.16/12)	Класс В
192.168.0.0 - 192.168.255.255 (префикс 192.168/16)	Класс С

Примечание: Первый блок является только единым классом номер сети, в то время как второй блок является рядом 16 чисел смежных сетей класса В, и третий блок является рядом 256 чисел смежных сетей класса С.

В этом примере Internet Service Provider (ISP) назначает на пользователя DSL только один IP-адрес, 171.68.1.1/24. Назначенный IP - адрес является зарегистрированным уникальным IP - адресом и назван внутренним глобальным адресом. Этот зарегистрированный IP - адрес используется всей частной сетью для просмотра Интернета и также интернет-пользователями, которые происходят из открытой сети для достижения Web-сервера в частной сети.

Частная локальная сеть (LAN), 192.168.0.0/24, связана с Интерфейсом Ethernet маршрутизатора NAT. Эта частная локальная сеть (LAN) содержит несколько PC и Web-сервер. Маршрутизатор NAT настроен для перевода незарегистрированных IP - адресов (внутренние локальные адреса), которые прибывают от этих PC до одиночного открытого IP - адреса (в глобальном - 171.68.1.1) для просмотра Интернета.

IP-адрес 192.168.0.5 (Web-сервер) является адресом в частном пространстве адресов, которое не может маршрутизироваться к Интернету. Единственный видимый IP - адрес для пользователей общедоступного Интернета для достижения Web-сервера 171.68.1.1. Поэтому маршрутизатор NAT настроен для выполнения однозначного сопоставления между

IP-адресом 171.68.1.1 порта 80 (порт 80 используется для просмотра Интернета), и 192.168.0.5 порта 80. Это сопоставление позволяет интернет-пользователям на общедоступной стороне иметь доступ к внутреннему веб-серверу.

Эта топология сети и пример конфигурации могут использоваться для Cisco 827, 1417, SOHO77 и 1700/2600/3600 ADSL WIC. В качестве примера в этом документе используется Cisco 827.

Настройка

В этом разделе вам предоставляется информация для того, чтобы настроить функциональные возможности, описанные в этом документе.

Примечание: Чтобы найти, что дополнительные сведения о командах, используемых в этом документе, обращаются к [Средству поиска команд IOS Command Lookup Tool \(только зарегистрированные клиенты\)](#).

Схема сети

В настоящем документе используется следующая схема сети.

!--- конфигурацию

Cisco 827

```
Current Configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
!
hostname 827
!
ip subnet-zero
no ip domain-lookup
!
bridge irb
!
interface Ethernet0
ip address 192.168.0.254 255.255.255.0
ip nat inside !--- This is the inside local IP address
and it is a private IP address. ! interface ATM0 no ip
address no atm ilmi-keepalive pvc 0/35 encapsulation
aal5snap ! bundle-enable dsl operating-mode auto bridge-
group 1 ! interface BVI1 ip address 171.68.1.1
255.255.255.240 ip nat outside !--- This is the inside
global IP address. !--- This is your public IP address
and it is provided to you by your ISP. ! ip nat inside
source list 1 interface BVI1 overload !--- This
statement makes the router perform PAT for all the !---
End Stations behind the Ethernet interface that uses !--
- private IP addresses defined in access list #1. ip nat
inside source static tcp 192.168.0.5 80 171.68.1.1 80
extendable !--- This statement performs the static
address translation for the Web server. !--- With this
statement, users that try to reach 171.68.1.1 port 80
(www) are !--- automatically redirected to 192.168.0.5
```

```
port 80 (www). In this case !--- it is the Web server.
ip classless ip route 0.0.0.0 0.0.0.0 171.68.1.254 !---
IP address 171.68.1.254 is the next hop IP address, also
!--- called the default gateway. !--- Your ISP can tell
you what IP address to configure as the next hop
address. ! access-list 1 permit 192.168.0.0 0.0.0.255 !-
-- This access list defines the private network !---
that is network address translated. bridge 1 protocol
ieee bridge 1 route ip ! end
```

Проверка

От выходных данных команды **show ip nat translation** локальная Внутренняя часть является настроенным IP - адресом, назначенным на Web-сервер на внутренней сети. Заметьте, что 192.168.0.5 адрес в частном пространстве адресов, которое не может маршрутизироваться к Интернету. Внутренним глобальным является IP-адрес внутреннего хоста, который является Web-сервером, как это появляется к внешней сети. Этот адрес является одним известным людям, которые пытаются обратиться к Web-серверу из Интернета.

The `Outside local` является IP-адрес внешнего хоста, как это появляется к внутренней сети. Это - не обязательно допустимый адрес. Но, это выделено от адресного пространства, которое может маршрутизироваться на внутренней части.

Адресом `Outside global` является IP-адрес, назначенный на хост на внешней сети владельцем хоста. Адрес выделен от адреса или сетевого пространства, которое может глобально маршрутизироваться.

Заметьте, что адрес 171.68.1.1 с номером порта 80 (HTTP) преобразовывает в 192.168.0.5 порта 80, и наоборот. Поэтому интернет-пользователи могут просмотреть веб-сайты сервер даже при том, что Web-сервер находится на частной сети с закрытым IP - адресом.

Для получения дополнительных сведений о том, как устранить неполадки NAT, обратитесь к [Операции NAT Проверки и Основному Устранению проблем трансляции сетевых адресов](#).

```
827#
827#show ip nat translation Pro Inside global Inside local Outside local Outside global tcp
171.68.1.1:80 192.168.0.5:80 --- --- tcp 171.68.1.1:80 192.168.0.5:80 198.133.219.1:11000
198.133.219.1:11000 827#
```

Устранение неполадок

Для устранения проблем переадресации можно выполнить **команды понедельник условия и debug ip nat detailed** на маршрутизаторе, чтобы видеть, преобразовывает ли адрес правильно. Видимый IP - адрес для внешних пользователей для достижения Web-сервера 171.68.1.1. Например, потребители от общедоступной стороны интернета которые пробуют достигнуть порт 80 171.68.1.1 (www) автоматически перенаправлены к порту 80 192.168.0.5 (www), который в этом случае веб-сервер.

```
827#term mon 827#debug ip nat detailed IP NAT detailed debugging is on 827# 03:29:49: NAT:
creating portlist proto 6 globaladdr 171.68.1.1 03:29:49: NAT: Allocated Port for 192.168.0.5 ->
171.68.1.1: wanted 80 got 80 03:29:49: NAT: o: tcp (198.133.219.1, 11000) -> (171.68.1.1, 80)
[0] <... snipped ...>
```

Дополнительные сведения

- [Сведения о поддержке технологии DSL Cisco](#)
- [Дополнительная информация о продукте](#)
- [Cisco Systems – техническая поддержка и документация](#)