

Часто задаваемые вопросы технологии NAT

Содержание

[Введение](#)

[NAT общего назначения](#)

[Речевой NAT](#)

[NAT с VRF/MPLS](#)

[NAT NVI](#)

[SNAT](#)

[NAT-PT \(v6 к v4\)](#)

[Зависимая от платформы Cisco 7300/7600/6k](#)

[Зависимая от платформы Cisco 850](#)

[Развертывания NAT](#)

[Оптимальные методы NAT](#)

[Дополнительные сведения](#)

Введение

Этот документ предоставляет ответы на часто задаваемые вопросы о Технологии NAT.

NAT общего назначения

Вопрос. . Что такое NAT?

О. Технология NAT разработана для Сохранения IP-адреса. Это включает частные IP сети, которые используют незарегистрированные IP - адреса для соединения с Интернетом. NAT воздействует на маршрутизатор, обычно подключая две сети вместе, и преобразовывает частное (не глобально уникальный) адреса во внутренней сети в юридические адреса, прежде чем пакеты будут переданы к другой сети.

Как часть этой возможности, NAT может быть настроен для объявления только одного адреса для всей сети к внешнему миру. Это предоставляет дополнительные меры безопасности путем эффективного сокрытия всей внутренней сети позади того адреса. NAT предлагает двойные функции безопасности и сохранения адреса и, как правило, внедряется в средах удаленного доступа.

Вопрос. . Как работает NAT?

О. В основном NAT позволяет одиночное устройство, такое как маршрутизатор, для действия как агент между Интернетом (или открытая сеть) и локальной сетью (или частная сеть), что означает, что только одиночный уникальный IP - адрес требуется, чтобы представлять всю группу компьютеров к чему-либо вне их сети.

Вопрос. . Как я настраиваю NAT?

О. Для настройки традиционного NAT необходимо сделать по крайней мере один интерфейс на маршрутизаторе (NAT снаружи) и другой интерфейс на маршрутизаторе (NAT внутри), и ряд правил для перевода IP-адресов в заголовках пакета (и информационные наполнения при желании) должен быть настроен. Для настройки виртуального интерфейса NAT (NVI) вам нужен по крайней мере один интерфейс, настроенный с поддержкой NAT наряду с тем же рядом правил, как упомянуто выше.

Для получения дополнительной информации обратитесь к [Руководству по конфигурации Сервисов IP-адресации Cisco IOS](#) или [Настройке виртуальный интерфейс NAT](#).

Вопрос. . Каковы основные различия между реализациями NAT Cisco PIX Security Appliance и программным обеспечением Cisco IOS?

О. NAT на основе ПО Cisco IOS не существенно отличается от функции NAT в Cisco PIX Security Appliance. Основные различия включают другие типы трафика, поддерживаемые в реализации. См. [устройства защиты Cisco PIX серии 500](#) и [Примеры Конфигурации NAT](#) для получения дополнительной информации о конфигурации NAT на устройствах PIX Cisco (включает поддерживаемые типы трафика).

Вопрос. . На которых аппаратных средствах для маршрутизации Cisco ПРЕОБРАЗОВАНИЕ СЕТЕВЫХ АДРЕСОВ В CISCO IOS доступно? Как могут быть упорядочены аппаратные средства?

О. Программное средство Cisco Feature Navigator позволяет клиентам определять функцию (NAT) и находить, на котором выпуске и версии аппаратного обеспечения эта функция ПО Cisco IOS доступна. См. [Cisco Feature Navigator](#) для использования этого программного средства.

Вопрос. . NAT появляется до или после маршрутизации?

О. Заказ, в котором транзакции обработаны с помощью NAT, основывается, идет ли пакет от внутренней сети до внешней сети или от внешней сети до внутренней сети. Внутри к внешней трансляции происходит после того, как маршрутизация, и снаружи к внутренней трансляции происходит перед маршрутизацией. [Дополнительная информация содержится в документе "Порядок работы NAT"](#).

Вопрос. . NAT может быть развернут в общей среде беспроводной локальной сети?

О. Да. NAT - Статическая ip Функция поддержки оказывает поддержку для пользователей со статическими IP - адресами, позволяя тем пользователям установить сеанс IP в общей среде беспроводной локальной сети.

Вопрос. . NAT делает распределение нагрузки TCP для Серверов на внутренней сети?

О. Да. Использование NAT, можно установить действительный хост на внутренней сети,

которая координирует распределение нагрузки среди реальных хостов. См. [Предотвращение Перегрузки Сервера Использование TCP, Балансирующего нагрузку](#) для получения дополнительной информации.

Вопрос. . Я могу ограничить количество преобразований NAT?

О. Да. Функция Преобразования NAT Ограничения скорости предоставляет способность ограничить максимальное число параллельных операций NAT на маршрутизаторе. В дополнение к предоставлению пользователям большего контроля над тем, как адреса NAT используются, функция Преобразования NAT Ограничения скорости может быть использована для ограничения эффектов вирусов, червей и атак отказ в обслуживании.

Вопрос. . Как направляет изученный или распространившийся для IP-подсетей или адресов, которые используются NAT?

О. Маршрутизация для IP-адресов, созданных NAT, изучена если:

- Внутренний пул глобальных адресов формируется в подсети маршрутизатора следующего узла.
- Статический вход маршрутизатора настроен в маршрутизаторе следующего перехода и перераспределен в сети маршрутизации.

Когда с внутренним глобальным адресом совпадают с локальным интерфейсом, NAT устанавливает псевдоним IP и Запись ARP, в этом случае маршрутизатор будет **Proxy-arp** для этих адресов. Если это поведение не требуется, используйте ключевое слово *no-alias*.

Когда пул NAT настроен, опция *add-route* может использоваться для автоматического внесения маршрута.

Вопрос. . Сколько текущих сеансов NAT поддерживаются в Cisco IOS NAT?

О. Предел сеанса NAT ограничен суммой доступного DRAM в маршрутизаторе. Каждое преобразование NAT использует приблизительно 312 байтов в DRAM. В результате 10,000 трансляций (больше, чем обычно обрабатывались бы на одиночном маршрутизаторе) используют приблизительно 3 МБ. Поэтому типичные аппаратные средства для маршрутизации имеют более чем достаточно памяти для поддержки тысяч преобразований NAT.

Вопрос. . Какая направляющая производительность может ожидаться при использовании ПРЕОБРАЗОВАНИЯ СЕТЕВЫХ АДРЕСОВ В CISCO IOS?

О. ПРЕОБРАЗОВАНИЕ СЕТЕВЫХ АДРЕСОВ В CISCO IOS поддерживает Быстрое переключение ретрансляций CISCO, быструю коммутацию и коммутацию в контексте процесса. Для 12.4T выпуск и позже, больше не поддерживается путь быстрой коммутации. Для платформы Cat6k переключающимся заказом является Netflow (коммутируемый путь HW), CEF, путь обработки.

Производительность зависит от нескольких факторов:

- Тип приложения и его типа трафика
- Встроены ли IP-адреса

- Exchange и контроль нескольких сообщений
- Исходный порт требуется
- Количество преобразований
- Другие приложения, работающие в это время
- Тип аппаратных средств и процессора

Вопрос. . Можно ли применить Cisco IOS NAT к субинтерфейсам?

О. Да. Источник и/или трансляции преобразования сетевых адресов назначения могут быть применены к любому интерфейсу или подинтерфейсам, имеющим IP-адрес (включая интерфейсы номеронабирателя). NAT не может быть настроен с беспроводным Виртуальным интерфейсом. Беспроводной Виртуальный интерфейс не существует во время записи в NVRAM. Таким образом, после перезагрузки, маршрутизатор высвобождает конфигурацию NAT на беспроводном Виртуальном интерфейсе.

Вопрос. . ПРЕОБРАЗОВАНИЕ СЕТЕВЫХ АДРЕСОВ В CISCO IOS может использоваться с Протоколом HSRP для обеспечения избыточных соединений интернет-провайдеру?

О. Да. NAT действительно предоставляет избыточный HSRP. Однако это отличается от SNAT (преобразование Stateful NAT). NAT с HSRP является системой не сохраняющей состояние. Когда сбой имеет место, текущий сеанс не поддержан. Во время статической конфигурации NAT (когда пакет не совпадает ни с какой СТАТИЧЕСКОЙ конфигурацией правила), пакет передан через без любой трансляции.

Вопрос. . ПРЕОБРАЗОВАНИЕ СЕТЕВЫХ АДРЕСОВ В CISCO IOS поддерживает входные преобразования на Интерфейсе Frame Relay? Он поддерживает исходящую трансляцию на стороне Ethernet?

О. Да. Инкапсуляция не имеет значения для NAT. NAT может быть сделан, где существует IP-адрес на интерфейсе, и интерфейсом является NAT внутри или NAT снаружи. Должна быть внутренняя часть и внешняя сторона для NAT для функционирования. При использовании NVI должен быть по крайней мере один включенный интерфейс NAT. Посмотрите, [Как я настраиваю NAT?](#) дополнительные сведения.

Вопрос. . Одиночный Маршрутизатор с NAT может позволить некоторым пользователям использовать NAT и других пользователей на том же Интерфейсе Ethernet, чтобы продолжить использовать их собственные IP-адреса?

О. Да. Это может быть выполнено с помощью списка доступа, описывающего набор хостов или сетей, которые требуют NAT. Все сеансы на том же хосте будут или преобразованы или пройдут через маршрутизатор и не будут преобразованы.

Списки доступа, расширенные списки доступа и Карты маршрутизации могут использоваться для определения *правил*, по которым преобразованы IP - устройства. Сетевой адрес и соответствующая маска подсети должны всегда задаваться. Ключевое слово *любой* не должен использоваться вместо сетевого адреса или маски подсети (см. [часто задаваемые вопросы NAT, Оптимальные методы и Руководство по развертыванию](#)

для большего количества подробности). Со Статической конфигурацией NAT, когда пакет не сделает совпавший ни с какой СТАТИЧЕСКОЙ конфигурацией правила, пакет будет передан через без любой трансляции.

Вопрос. . При настройке для PAT (перегрузка), каково максимальное число трансляций, которые могут быть созданы на внутренний глобальный IP-адрес?

О. PAT (перегрузка) делит доступные порты на глобальный IP-адрес в три диапазона: 0-511, 512-1023, и 1024-65535. PAT назначает уникальный исходный порт для каждого UDP или сеанса TCP. Это пытается назначить значение того же порта исходного запроса, но если первый исходный порт уже использовался, это начинает просматривать с начала определенного диапазона портов найти первый доступный порт и назначает его на диалог. Существует исключение для 12.2S основание кода. 12.2S основание кода использует другую логику порта, и нет никакого резервирования порта.

Вопрос. . Принципы работы трансляции адресов портов?

О. PAT работает или с одним глобальным IP-адресом или со множественными адресами.

PAT с одним IP-адресом

Условие	Описание
1	NAT/PAT осматривает трафик и совпадает с ним к правилу трансляции.
2	Правило совпадает к конфигурации PAT.
3	Если PAT знает о типе трафика и если тот тип трафика имеет "ряд определенных портов или портов, это выполняет согласование", который это будет использовать, PAT откладывает их и не выделяет их как уникальные идентификаторы.
4	Если сеанс без специальных требований порта пытается соединиться, PAT преобразовывает IP - адрес источника и проверяет наличие исходного вызывающего порт (433, например). Примечание: Для Протокола TCP и Протокола UDP, диапазоны: 1-511, 512-1023, 1024-65535. Для Протокола ICMP первая группа запускается в 0.
5	Если запрошенный порт источника доступен, PAT назначает исходный порт, и сеанс продолжается.
6	Если запрошенный порт источника не доступен, PAT начинает искать с начала соответствующей группы (запускающийся в 1 для TCP или приложений UDP, и от 0 для ICMP).
7	При наличии доступного порта выполняется назначение, и сеанс продолжается.

8	Если нет доступных портов, пакет отбрасывается.
---	---

ПАТ с несколькими IP-адресами

Условие	Описание
1-7	Первые семь условий совпадают с с одним IP-адресом.
8	Если никакие порты не доступны в соответствующей группе на первом IP-адресе, NAT переходит к следующему IP-адресу в пуле и пытается выделить первый исходный порт, который запрашивают.
9	Если запрошенный порт источника доступен, NAT назначает исходный порт, и сеанс продолжается.
10	Если запрошенный порт источника не доступен, NAT начинает искать с начала соответствующей группы (запускающийся в 1 для TCP или приложений UDP, и от 0 для ICMP).
11	При наличии доступного порта выполняется назначение, и сеанс продолжается.
12	Если никакие порты не доступны, пакет отброшен, пока другой IP-адрес не доступен в пуле.

Вопрос. . Что такое пулы IP NAT?

О. Пулы IP NAT являются диапазоном IP-адресов, которые выделены для преобразования NAT по мере необходимости. Для определения пула команда настройки используется:

```
ip nat pool <name> <start-ip> <end-ip> {netmask <netmask> | prefix-length <prefix-length>} [type {rotary}]
```

Пример 1

Следующий пример преобразовывает между внутренними хостами, обращенными или от 192.168.1.0 или от 192.168.2.0 сетей до глобально уникальной 10.69.233.208/28 сети:

```
ip nat pool net-208 10.69.233.208 10.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
ip address 10.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet 1
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
```

```
access-list 1 permit 192.168.2.0 0.0.0.255
```

Пример 2

В следующем примере цель состоит в том, чтобы определить виртуальный адрес, соединения, которым распределены среди ряда реальных хостов. Пул определяет адреса реальных хостов. Список доступа определяет виртуальный адрес. Если трансляция уже не существует, пакеты TCP от последовательного интерфейса 0 (внешний интерфейс), чье назначение совпадает, список доступа преобразованы в адрес от 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
```

Вопрос. . Каково максимальное число конфигурируемых пулов IP NAT (ip nat pool "название")?

О. В практическом применении максимальное число конфигурируемых пулов IP ограничено суммой доступного DRAM в конкретном маршрутизаторе. (Cisco рекомендует настроить размер пула 255.) Каждый пул должен быть не больше, чем 16 битов. В 12.4 (11) T и позже, IOS представляют CCE (Механизм Общей классификации). Это ограничило NAT, чтобы только иметь максимум 255 пулов. В 12.2S основание кода, нет никакого максимального ограничения пулов.

Вопрос. . Каково преимущество использования route-map по сравнению с ACL на пуле NAT?

О. Route-map защищает нежелательных внешних пользователей для достижения внутренним пользователям/серверам. Это также имеет возможность сопоставить одиночный внутренний IP-адрес с другими Внутренними глобальными адресами на основе правила. См. [Поддержку NAT Множественных пулов Использование Карт маршрутизации](#) для получения дополнительной информации.

Вопрос. . На что IP-адрес "накладывается" в контексте NAT?

О. Наложение IP-адреса обращается к ситуации, где два местоположения, которые хотят соединить, оба используют ту же схему IP-адреса. Это не редкий случай; когда компании объединяются или получены, это часто происходит. Без специальной поддержки установка связи и сеансов между двумя расположениями невозможна. Перекрытый IP-адрес может быть общим адресом, назначенным на другую компанию, частный адрес, назначенный на другую компанию, или может прибыть из диапазона частных адресов, как определено в [RFC 1918](#).

Закрытые IP - адреса немаршрутизуемы и требуют, чтобы преобразования NAT позволили соединения с внешним миром. Решение включает ответы запроса имени Системы доменных имен (DNS) прерывания от внешней стороны до внутренней части,

устанавливание трансляции для внешнего адреса и договаривания DNS - ответ прежде, чем передать его внутреннему хосту. Сервер DNS требуется, чтобы быть включенным с обеих сторон устройства NAT для решения пользователей, желающих иметь соединение между обеими сетями.

NAT в состоянии осмотреть и выполнить переадресацию на содержании DNS A и записи PTR, как показано в [Использовании NAT в Наложениях сети](#).

Вопрос. . Что такое статические преобразования NAT?

О. Статические преобразования NAT имеют однозначное сопоставление между локальной переменной и глобальными адресами. Пользователи могут также настроить преобразования статических адресов к уровню порта и использовать остаток от IP-адреса для других трансляций. Это, как правило, происходит, где вы выполняете Преобразование адресов портов (PAT).

Следующий пример показывает, как настроить routemap для разрешения трансляции снаружи внутрь для статического NAT:

```
ip nat inside source static 1.1.1.1 2.2.2.2 route-map R1 reversible
!
ip access-list extended ACL-A
permit ip any 30.1.10.128 0.0.0.127
route-map R1 permit 10 match ip address ACL-A
```

Вопрос. . Что предназначается термином *Перегрузка трансляции сетевых адресов*; этот PAT?

О. Да. Перегрузка трансляции сетевых адресов является PAT, который связал использование пула с диапазоном одного или более адресов или использования IP-адреса интерфейса в сочетании с портом. Когда вы перегружаетесь, вы создаете полностью расширенную трансляцию. Это - запись в таблице трансляции, содержащая IP-адрес и информацию об источнике/порте назначения, которую обычно называют PAT или перегрузкой.

PAT (или перегружающийся) является функцией ПРЕОБРАЗОВАНИЯ СЕТЕВЫХ АДРЕСОВ В CISCO IOS, которое используется для перевода *внутренний* (внутри локальный) частные адреса к один или больше *снаружи* (в глобальном, обычно регистрируемом) IP-адреса. Уникальные номера портов источника для каждого преобразования позволяют отличать один диалог от другого.

Вопрос. . Что такое динамические преобразования NAT?

О. В динамических преобразованиях NAT пользователи могут установить динамическое отображение (сопоставление) между локальной переменной и глобальными адресами. Динамическое отображение (сопоставление) выполнено путем определения локальных адресов, которые будут преобразованы и пул адресов или IP-адреса интерфейса, от которого можно выделить глобальные адреса и привязав два.

Вопрос. . Что такое ALG?

О. ALG является Шлюз уровня приложения (ALG). NAT выполняет услуги по переводу на любом Протоколе управления передачей / Протокол датаграммы пользователя (TCP/UDP)

трафик, который не несет источник и/или IP - адреса назначения в потоке данных прикладной программы.

Эти протоколы включают FTP, HTTP, SKINNY, H232, DNS, RAS, SIP, TFTP, telnet, система отслеживания FTP-архивов, finger, NTP, NFS, rlogin, rsh, rcp. Определенные протоколы, которые встраивают информацию о IP-адресе в информационном наполнении, требуют поддержки Шлюза прикладного уровня (ALG).

См. [Использование Шлюзов прикладного уровня с NAT](#) для получения дополнительной информации.

Вопрос. . Можно ли создать конфигурацию с динамической и статической трансляцией сетевых адресов?

О. Да. Однако тот же IP-адрес не может использоваться для конфигурации NAT static или в пуле для конфигурации NAT dynamic. Все открытые IP - адреса должны быть уникальными. Обратите внимание на то, что глобальные адреса, используемые в статических преобразованиях, автоматически не исключены с динамическими пулами, содержащими те же глобальные адреса. Динамические пулы должны быть созданы для исключения адресов, назначенных статическими записями. Для получения дополнительной информации обратитесь к [Настройке, Статической и динамической NAT Одновременно](#).

Вопрос. . Когда traceroute сделан через маршрутизатор NAT, traceroute должен показать Глобальный адрес NAT, или это должно пропустить Локальный адрес NAT?

О. Traceroute снаружи должен всегда возвращать глобальный адрес.

Вопрос. . Как PAT выделяет порт?

О. NAT представляет дополнительные функции порта: полный диапазон и схема порта.

- Полный диапазон позволяет NAT использовать все порты независимо от своего диапазона порта по умолчанию.
- Схема порта позволяет, что NAT для резервирования пользователя определяет диапазон портов для определенного приложения.

См. [Определяемые пользователем Диапазоны Исходного порта для PAT](#) для получения дополнительной информации.

В 12.4 (20) T2 вперед, NAT представляет рандомизацию порта для L3/L4 и симметричного порта.

- Рандомизация порта позволяет NAT случайным образом выбирать любой глобальный порт для запроса исходного порта.
- Симметричный порт позволяет NAT поддерживать *независимую окончечную точку*.

См. [Анатомия: Внутренняя сеть Взгляда Преобразователя адресов](#) для получения дополнительной информации.

Вопрос. . Каково различие между сегментацией TCP и Фрагментацией ip?

О. Фрагментация ip происходит на Уровне 3 (IP); сегментация TCP происходит на Уровне 4 (TCP). Фрагментация ip имеет место, когда пакеты, которые больше, чем Максимальный размер передаваемого блока данных (MTU) интерфейса, переданы из этого интерфейса. Эти пакеты должны будут быть или фрагментированы или сброшены, когда они отосланы интерфейс. Если бит "Не фрагментировать" (DF) будет "not set" в IP-заголовке пакета, то пакет будет фрагментирован. Если бит DF установлен в IP-заголовке пакета, пакет отброшен и сообщение об ошибках ICMP, указывающее, что MTU следующего перехода value будет возвращен к отправителю. Все фрагменты пакета IP несут тот же Идентификатор в IP - заголовке, который позволяет заключительному получателю повторно собирать фрагменты в исходный пакет IP. См. [Фрагментацию ip Решения, MTU, MSS и Проблемы PMTUD с GRE и IPsec](#) для получения дополнительной информации.

Когда приложение на конечной станции передает данные, сегментация TCP имеет место. Данные прикладной программы разделяются на то, что TCP считает блоками оптимального размера для передачи. Эту единицу информации, которую передают от TCP до IP, называют сегментом. Сегменты TCP передаются в дейтаграммах IP. Эти дейтаграммы IP могут тогда стать IP - фрагментами, поскольку они проходят через сеть и встречают ссылки более низкого MTU, чем они могут пройти.

TCP сначала сегментирует эти данные в сегменты TCP (на основе значения TCP MSS) и добавит заголовок TCP и передаст этот сегмент TCP к IP. Затем IP добавит IP - заголовок для передачи пакета к хосту удаленного конца. Если пакет IP с сегментом TCP будет больше, чем IP MTU на исходящем интерфейсе на пути между хостами TCP тогда, то IP фрагментирует пакет IP/TCP для адаптации. Эти фрагменты пакета IP будут повторно собраны на удаленном хосте IP - уровнем и завершены сегментом TCP (который первоначально передавался), будет вручен уровню TCP. Уровень TCP понятия не имеет, что IP фрагментировал пакет во время транзита.

NAT поддерживает IP - фрагменты, но он не поддерживает сегменты TCP.

Вопрос. . NAT поддерживает не в порядке для сегментации TCP и Фрагментации ip?

О. NAT поддерживает только неисправные IP - фрагменты из-за ip virtual-reassembly.

Вопрос. . Как отладить сегментация TCP и Фрагментация ip?

О. NAT использует тот же CLI отладки и для Фрагментации ip и для сегментации TCP: `debug ip nat frag`.

Вопрос. . Существует ли поддерживаемый MIB NAT?

О. Нет. Там в не поддерживаемом MIB NAT, включая CISCO-IETF-NAT-MIB.

Вопрос. . Что такое таймаут TCP, и как он касается таймера TCP NAT?

О. Если трехэтапное установление связи не будет завершено, и NAT видит пакет TCP, то NAT запустит 60-секундный таймер. Когда трехэтапное установление связи завершено, NAT использует 24-часовой таймер для Записи NAT по умолчанию. Если конечный хост передает СБРОС, NAT изменяет таймер по умолчанию от 24 часов до 60 секунд. В случае FIN NAT изменяет таймер по умолчанию от 24 часов до 60 секунд, когда это получает FIN и

ACK FIN.

Вопрос. . Я могу изменить количество времени, которое это занимает для NAT translation для таймаута от NAT translation таблицы?

О. Да. Можно изменить значения таймаута NAT для всех записей или для различных типов NAT translations (таких как таймаут udp, dns-timeout, таймаут tcp, first-таймаут, таймаут icmp, таймаут pptp, syn-таймаут, таймаут порта и время ожидания эхо-ответа arp).

Вопрос. . Как я останавливаю Протокол LDAP от присоединения дополнительных байтов к каждому пакету ответа LDAP?

О. Параметры LDAP добавляют дополнительные байты (результаты поиска LDAP) при обработке сообщений типа Search-Res-Entry. LDAP подключает 10 байтов результатов поиска к каждому пакету ответа LDAP. Если это 10 дополнительных байтов результата данных в пакете, превышающем Максимальный размер передаваемого блока данных (MTU) в сети, пакет, отброшено. В этом случае Cisco рекомендует выключить это поведение LDAP с помощью команды `no ip nat service append-ldap-search-res` CLI для пакетов, которые будут переданы и получены.

Вопрос. . Какова рекомендация маршрута для внутреннего глобального/внешнего local IP address на коробке NAT?

О. Маршрут должен быть задан на настроенной коробке NAT для внутреннего глобального IP-адреса для функций, таких как NAT-NVI. Точно так же маршрут должен также быть задан на коробке NAT для внешнего local IP address. В этом случае любой пакет от в к направлению с помощью внешнего статического правила потребует этого вида маршрута. В таких сценариях, при обеспечении маршрута для IG/OL, должен также быть настроен IP-адрес следующего перехода. Если конфигурация следующего перехода отсутствует, это считают ошибкой конфигурации и приведет к неопределенному поведению.

NVI-NAT присутствует в пути функции обработки исходящих данных только. Если у вас есть напрямую подключенная подсеть с NAT-NVI или внешним правилом преобразования NAT, настроенным на коробке, то в тех сценариях, необходимо предоставить фиктивный IP-адрес следующего перехода и также связанный ARP для Следующего перехода. Это необходимо для базовой инфраструктуры для вручения пакета NAT для трансляции.

Вопрос. . ПРЕОБРАЗОВАНИЕ СЕТЕВЫХ АДРЕСОВ В CISCO IOS поддерживает ACL с "регистрационным" ключевым словом?

О. При настройке ПРЕОБРАЗОВАНИЯ СЕТЕВЫХ АДРЕСОВ В CISCO IOS для динамического преобразования NAT ACL используется для определения пакетов, которые могут быть преобразованы. Текущая архитектура NAT не поддерживает ACL с "регистрационным" ключевым словом.

Речевой NAT

Вопрос. . NAT поддерживает Skinny Client Control Protocol (SCCP) v17, который поставлен с Cisco Unified Communications Manager (CUCM) V7?

О. CUCM 7 и все нагрузки телефона по умолчанию для CUCM 7 поддерживают SCCPv17. Когда телефон регистрируется, используемая версия SCCP определена самой высокой общей версией между CUCM и телефоном.

NAT еще не поддерживает SCCP v17. Пока поддержка NAT SCCP v17 не внедрена, микропрограммное обеспечение должно быть понижено до версии 8-3-5 или ниже так, чтобы о SCCP v16 выполнили согласование. CUCM6 не встретится с проблемой NAT ни с какой нагрузкой телефона, пока это использует SCCP v16. Cisco IOS в настоящее время не поддерживает версию 17 SCCP.

Вопрос. . Какие CUCM/SCCP/firmware версии загрузки поддерживаются NAT?

О. NAT поддерживает версию 6.x CUCM и более ранние релизы. Эти версии CUCM освобождены с по умолчанию 8.3.x (или ранее) телефонная загрузка ПО, которые поддерживают SCCP v15 (или ранее).

NAT не поддерживает версии CUCM 7.x или более поздние версии. Они версия CUCM освобождена с по умолчанию 8.4.x телефонная загрузка ПО, которая поддерживает SCCP v17 (или позже).

Если CUCM 7.x или позже используется, более старая загрузка ПО должна быть установлена на сервере TFTP CUCM так, чтобы телефоны использовали загрузку ПО с SCCP v15 или ранее чтобы поддерживаться NAT.

Ссылка ниже подтверждает, что загрузка ПО 8.3.x содержит SCCP v15 или ранее и будет работать с NAT и что загрузка ПО 8.4.x содержит SCCP v17 и НЕ будет работать с NAT.

<http://third-gen-phones.gforge.cisco.com/twiki/prod/bin/view/Thirdgenphones/CCMLoadNumberAndCodeNameDecoderRing>

Вопрос. . Что такое Усовершенствование Распределения портов PAT Поставщика услуг для RTP и RTCP?

О. Усовершенствование Распределения портов PAT Поставщика услуг для RTP и функции RTCP гарантирует это для SIP, H.323 и Skinny голосовых вызовов. Номера портов, используемые для потоков RTP, являются даже номерами портов, и потоки RTCP являются следующим последующим номером нечетного порта. Номер порта преобразован в номер в диапазоне, заданном, приспособив RFC 1889. Вызов с номером порта в диапазоне приведет к трансляции PAT на другой номер порта в этом диапазоне. Аналогично, трансляция PAT для номера порта вне этого диапазона не приведет к трансляции на номер в данном диапазоне.

См. [Усовершенствование Распределения портов PAT Поставщика услуг для RTP и RTCP](#) для получения дополнительной информации.

Вопрос. . Что такое Протокол SIP, и пакеты SIP могут быть преобразованы посредством NAT?

О. Протокол SIP является основанным на ASCII, протоколом прикладного уровня, который может использоваться для установления, поддержать, и завершить вызовы между двумя или больше конечными точками. SIP является альтернативным протоколом,

разработанным инженерной группой по развитию Интернета (IETF) для мультимедийной конференц-связи по IP. Реализация Cisco SIP позволяет поддерживаемым Платформам cisco сигнализировать настройку голосовых и мультимедийных вызовов по IP - сетям.

Пакеты SIP могут быть преобразованы посредством NAT.

Вопрос. . Что такое Размещенная поддержка прохождения NAT Контроллера границы сеанса (SBC)?

О. Размещенное прохождение NAT Cisco IOS для функции SBC позволяет маршрутизатору Уровня приложения шлюза (ALG) SIP ПРЕОБРАЗОВАНИЯ СЕТЕВЫХ АДРЕСОВ В CISCO IOS действовать как SBC на Мультисервисном IP-to-IP Cisco шлюз, который помогает гарантировать плавную доставку передачи голоса по IP (VoIP) сервисы.

См. [Cisco IOS Настройки Размещенное прохождение NAT для Контроллера Границы Сеанса](#) и [SP Размещенное прохождение NAT для вызовов SIP Использование Контроллера Границы Сеанса Cisco IOS](#) для получения дополнительной информации.

Вопрос. . Сколько SIP, Skinny, и H323 вызовов может память маршрутизаторов и ЦПУ обработать через NAT?

О. Количество вызовов, обрабатываемых маршрутизатором NAT, зависит от количества памяти, доступного на коробке и питании для обработки ЦП.

Вопрос. . Маршрутизатор NAT поддерживает сегментацию TCP пакетов H323 и Skinny?

О. Сегментация TCP поддержки NAT IOS для H323 в 12.4 Магистралах и сегментация TCP поддерживают для SKINNY от 12.4 (6) Т вперед.

Вопрос. . Там какие-либо предупреждения состоят в том, чтобы не упустить при использовании конфигурации перегрузки NAT в речевых развертываниях?

О. Да. Когда у вас есть конфигурации перегрузки NAT и речевые развертывания, вам нужно сообщение о регистрации, чтобы пройти NAT и создать ассоциацию для-> в достигнуть этого внутреннего устройства. Внутреннее устройство передает эту регистрацию периодической формой, и NAT обновляет этот pin-hole/association от информации как в сигнальном сообщении.

Вопрос. . Там какие-либо известные неполадки вызваны путем выдачи команды `clear ip nat trans *` или команды `clear ip nat trans forced` в речевых развертываниях?

О. В речевых развертываниях, когда вы выполните команду `clear ip nat trans *` или команду `clear ip nat trans forced` и иметь динамический NAT, вы вытрете pin-hole/association и должны ждать следующего регистрационного цикла от внутреннего устройства до re-establish это. Cisco рекомендует не использовать эти команды clear в речевых развертываниях.

Вопрос. . NAT поддерживает голос совместно-расположенное решение?

О. Нет. Совместно-расположенное решение в настоящее время не поддерживается. Следующие развертывания с NAT (на той же коробке) считают совместно-расположенным решением: CME/DSP-Farm/SCCP/H323.

Вопрос. . NVI поддерживает Skinny ALG, H323 ALG и SIP TCP ALG?

О. Нет. Обратите внимание на то, что на SIP UDP ALG (используемый большинством развертываний) не затронут.

NAT с VRF/MPLS

Вопрос. . Маршрутизатор NAT будет когда-либо поддерживать преобразование посредством NAT того же адресного пространства в VRF, как преобразовывается посредством NAT в пространстве глобального адреса? В настоящее время я получаю это предупреждение: "%, подобная статическая запись (1.1.1.1---> 22.2.2.2) уже существует", когда я пытаюсь настроить

придерживающееся: `72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2`
`72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf RED`

О. Устаревший NAT поддерживает config адреса overloapping по другим VRF. Необходимо было бы настроить наложение в правиле с опцией *match-in-vrf* и установить **внутреннюю часть/внешнюю сторону ip nat** в том же VRF для трафика по тому определенному VRF. Перекрывающаяся поддержка не включает таблицу глобальной маршрутизации.

Необходимо добавить ключевое слово *match-in-vrf* для перекрывающихся статических записей NAT VRF для других VRF. Однако не возможно наложиться на глобальный и VRF адреса NAT.

```
72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf RED match-in-vrf 72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf BLUE match-in-vrf
```

Вопрос. . Устаревший NAT поддерживает Облегченный VRF (Преобразовывающий посредством NAT от VRF до другого VRF)?

О. Нет. Необходимо использовать NVI для того, чтобы преобразовать посредством NAT между другими VRF. Можно использовать устаревший NAT, чтобы сделать NAT от VRF до глобального или скручивания жгутов NAT тот же VRF.

NAT NVI

Вопрос. . Что такое NAT NVI?

О. NVI обозначает виртуальный интерфейс NAT. Это позволяет NAT преобразовывать между двумя другими VRF. Это решение должно использоваться вместо [Трансляции сетевых адресов на каскад](#).

Вопрос. . Должен NAT NVI использоваться при преобразовывании посредством NAT между интерфейсом в глобальном и интерфейсом в VRF?

О. Cisco рекомендует использовать устаревший NAT для VRF к глобальному NAT (ip nat внутри/) и между интерфейсами в том же VRF. NVI используется для NAT между другими VRF.

Вопрос. . Сегментация TCP для NAT-NVI, поддержал?

О. Нет никакой поддержки сегментации TCP для NAT-NVI.

Вопрос. . NVI поддерживает Skinny ALG, H323 ALG и SIP TCP ALG?

О. Нет. Обратите внимание на то, что на SIP UDP ALG (используемый большинством развертываний) не затронут.

Вопрос. . Сегментация TCP, поддерживаемая с SNAT?

О. SNAT не поддерживает TCP ALGs (такой как, SIP, SKINNY, H323 или DNS). Поэтому сегментация TCP не поддерживается. Однако SIP UDP и DNS поддерживаются.

SNAT

Вопрос. . Что такое преобразование Stateful NAT (SNAT)?

О. SNAT позволяет двум или больше преобразователям сетевых адресов функционировать как группа трансляции. Один участник группы трансляции обрабатывает трансляцию требования трафика информации о IP-адресе. Кроме того, это сообщает резервному переводчику активных потоков, как они происходят. Резервный переводчик может тогда использовать информацию от активного переводчика для подготовки двойных записей в таблице трансляции. Поэтому, если активному переводчику препятствует критический опасный отказ, трафик может быстро быть коммутирован к резервной копии. Трафик продолжается, так как те же трансляции сетевых адресов используются, и состояние тех трансляций было ранее определено. См. [Упругость Улучшенного IP Использование преобразования Stateful NAT Cisco](#) для получения дополнительной информации.

Вопрос. . Сегментация TCP поддерживается с SNAT?

О. SNAT не поддерживает TCP ALGs (такой как, SIP, SKINNY, H323 или DNS). Поэтому сегментация TCP не поддерживается. Однако SIP UDP и DNS поддерживаются.

Вопрос. . Поддержка SNAT асимметричной маршрутизации?

О. Асимметричные поддержки маршрутизации NAT путем включения как организация очереди. По умолчанию поскольку-организация-очереди, включают. Однако от 12.4 (24) T, прогрессивный, как помещающий в очередь, больше не поддерживается. Клиенты должны удостовериться, что пакеты маршрутизируются должным образом, и надлежащая задержка добавлена для асимметричной маршрутизации для работы правильно.

NAT-PT (v6 к v4)

Вопрос. . Что такое NAT-PT?

О. NAT-PT является v4 к v6 трансляции для NAT. Трансляция протоколов (NAT-PT) является механизмом трансляции IPv4 IPv6, как определено в [RFC 2765](#) и [RFC 2766](#), позволяя устройствам только для IPv6 связаться с устройствами только для IPv4 и наоборот. См. [Реализацию NAT-PT для IPv6](#) для получения дополнительной информации об этой функции

Вопрос. . NAT-PT поддерживается в пути технологии CEF?

О. NAT-PT не поддерживается в пути CEF.

Вопрос. . Какие ALGs поддерживаются в NAT-PT?

О. NAT-PT поддерживает TFTP/FTP и DNS. Нет никакой поддержки голоса и SNAT в NAT-PT.

Вопрос. . ASR 1004 поддерживает NAT-PT?

О. Маршрутизаторы агрегации (ASR) используют NAT64. Для получения дополнительной информации о настройке NAT64 обратитесь к [Настройке Сеть Маршрутизации для NAT64 Не сохраняющего состояние](#).

Зависимая от платформы Cisco 7300/7600/6k

Вопрос. . Действительно ли преобразование Stateful NAT (SNAT) доступно на Catalyst 6500 на серии SX?

О. SNAT не доступен на Catalyst 6500 на серии SX.

Вопрос. . Осведомленный о VRF NAT поддерживается в аппаратных средствах на 6k?

О. Осведомленный о VRF NAT не поддерживается в аппаратных средствах на этой платформе.

Вопрос. . 7600 и Cat6000 поддерживают осведомленный о VRF NAT?

О. На 65xx/76xx платформе не поддерживается осведомленный о VRF NAT, и CLI заблокированы.

Примечание: Можно внедрить дизайн путем усиления FWASM, который выполняется в действительном прозрачном режиме контекста.

Зависимая от платформы Cisco 850

Вопрос. . Cisco 850 поддерживает Skinny NAT ALG в выпуске 12.4T?

О. Нет. Нет никакой поддержки Skinny NAT ALG в 12.4Т на серии 850.

Развертывания NAT

Вопрос. . Как я внедряю NAT?

О. NAT включает частные IP объединения нескольких локальных сетей, которые используют незарегистрированные IP-адреса для соединения с Интернетом. NAT преобразовывает частное (RFC1918) адрес во внутренней сети в юридические маршрутизируемые адреса, прежде чем пакеты будут переданы на другую сеть.

Для получения дополнительной информации о реализации NAT, обратитесь к [Настройке NAT для Сохранения IP-адреса](#).

Вопрос. . Как я внедряю NAT с голосом?

О. Поддержка NAT голосовой характеристики позволяет, что SIP встроил сообщения, проходящие через маршрутизатор, настроенный с Технологией NAT, которая будет преобразована назад в пакет. Шлюз уровня приложения (ALG) используется с NAT для перевода голосовых пакетов.

Для получения дополнительной информации о реализации NAT с голосом, обратитесь к [Поддержке NAT ALGs](#).

Вопрос. . Как делают меня интеграция NAT с MPLS VPN?

О. Интеграция NAT с функцией MPLS VPN позволяет множественным MPLS VPN быть настроенными на одиночном устройстве для сотрудничества. NAT может дифференцироваться, от которого MPLS VPN он получает IP - трафик даже если MPLS VPN все использование та же схема IP-адресации. Это усовершенствование позволяет множественным клиентам MPLS VPN совместно использовать сервисы при обеспечении, что каждый MPLS VPN является абсолютно отдельным от другого.

Вопрос. . Сопоставление NAT static поддерживает HSRP для высокой доступности?

О. Когда запрос Протокола ARP инициирован для адреса, который настроен со статическим отображением Технологии NAT и принадлежит маршрутизатору, NAT отвечает MAC-адресом BIA на интерфейсе, к которому указывает ARP. Два маршрутизатора действуют как HSRP, активный и резервный. Их внутренние интерфейсы NAT должны быть включены и настроены для принадлежности группе.

Вопрос. . Как я внедряю NAT NVI?

О. Функция виртуального интерфейса NAT (NVI) удаляет требование для настройки интерфейса или как NAT внутри или как NAT снаружи. Для получения дополнительной информации о NAT NVI, обратитесь к [Настройке виртуальный интерфейс NAT](#).

Вопрос. . Как я внедряю распределение нагрузки с NAT?

О. Существует два вида распределения нагрузки, которое может быть сделано с NAT: можно сбалансировать нагрузку входящий к ряду серверов для распределения загрузки на серверах, и можно сбалансировать нагрузку трафика пользователя к Интернету более чем два или больше интернет-провайдера.

Для получения дополнительной информации о входящем распределении нагрузки, обратитесь к [Предотвращению Перегрузки Сервера Использование Распределения нагрузки TCP](#).

Для получения дополнительной информации о балансировке исходящей нагрузки, обратитесь к [IOS NAT, Распределяющий нагрузку для Двух Подключений ISP](#).

Вопрос. . Как я внедряю NAT в соединении с IPSec?

О. Существует поддержка IP-безопасности (IPSec) Безопасное закрытие полезной нагрузки (ESP) через NAT и Прозрачность NAT IPSec.

IPSec ESP через Характеристику NAT предоставляет способность поддерживать множественный параллельный IPSec, ESP туннелирует или соединения через устройство ПРЕОБРАЗОВАНИЯ СЕТЕВЫХ АДРЕСОВ В CISCO IOS, настроенное на перегрузке или режиме преобразования адресов портов (PAT).

Функция прозрачности NAT IPSec представляет поддержку Трафика IPSec для перемещения через NAT или точки PAT в сети путем адресации ко многим известный incompatibilities между NAT и IPSec.

Вопрос. . Как я внедряю NAT-PT?

О. NAT-PT (Трансляция сетевых адресов — Трансляция протоколов) является механизмом трансляции IPv4 IPv6, как определено в [RFC 2765](#) и [RFC 2766](#), который позволяет устройствам только для IPv6 связываться с устройствами только для IPv4 и наоборот.

Для получения дополнительной информации о реализации и настройке NAT-PT, обратитесь к [Реализации NAT-PT для IPv6](#).

Вопрос. . Как я внедряю, передает NAT в многоадресном режиме?

О. Это возможно к NAT source IP для многоадресной рассылки. Route-map не может использоваться при выполнении динамического NAT для групповой адресации, только список доступа поддерживается для этого.

Для получения дополнительной информации обратитесь к тому, [Как Действительно Передает NAT в многоадресном режиме, Работают на маршрутизаторы Cisco](#). Целевая группа многоадресной рассылки преобразована посредством NAT с помощью решения [для Отражения Сервиса групповой адресации](#).

Вопрос. . Как я внедряю преобразование Stateful NAT (SNAT)?

О. SNAT включает непрерывное обслуживание для динамично сопоставленных сеансов NAT. Сеансы, которые статически определены, получают преимущество резервирования без потребности в SNAT. В отсутствие SNAT сеансы, которые используют динамические

сопоставления NAT, были бы разъединены в случае критического опасного отказа и должны будут быть восстановлены. Только минимальная конфигурация SNAT поддерживается. Будущие развертывания должны быть выполнены только после говораций с вашей Группой Cisco Account для проверки дизайна относительно текущих ограничений.

SNAT рекомендуется для следующих сценариев:

- Режим HSRP, как описано в отчете SNAT: [Упругость Улучшенного IP Использование преобразования Stateful NAT Cisco](#).
- Основной/резервный не рекомендуемый режим, так как существуют некоторые функции, отсутствующие по сравнению с HSRP.
- Для переключаются сценарии и для 2 настроек маршрутизатора. Т.е. если отказы маршрутизатора, другой маршрутизатор вступает во владение эффективно. (Архитектура SNAT не разработана для обработки Интерфейсных откидных створок.)
- Сценарий неасимметричной маршрутизации поддерживается. Асимметричная маршрутизация может быть обработана, только если задержка в пакете ответа выше, чем это между 2 маршрутизаторами SNAT для обмениваний сообщениями SNAT.

В настоящее время архитектура SNAT не разработана для обработки устойчивости; поэтому, эти тесты, как ожидают, не успешно выполняются:

- Очистка Записей NAT, в то время как существует трафик.
- Изменяя интерфейсные параметры (как изменение IP-адреса, shut/no-shut, и т.д.), в то время как существует трафик.
- SNAT, определенный **ясный** или **команды показа**, как ожидают, не выполнится должным образом и не рекомендован. Некоторые относящиеся к SNAT **ясные** и **команды показа** следующие:

```
clear ip snat sessions * clear ip snat sessions <ip address of the peer> clear ip snat translation distributed * clear ip snat translation peer < IP address of SNAT peer> sh ip snat distributed verbose sh ip snat peer < IP address of peer>
```
- Если пользователь хочет к clear entry, **clear ip nat trans forced** или команды **clear ip nat trans *** могут использоваться. Если пользователь хочет просмотреть записи, **show ip nat translation**, **show ip nat translations verbose**, и команды **show ip nat stats** могут использоваться. Если *внутренний сервис* будет настроен, то он покажет SNAT определенную информацию также.
- При очистке преобразований NAT сзади не рекомендуется маршрутизатор. Всегда очищайте Записи NAT на основном маршрутизаторе SNAT.
- SNAT не является HA; поэтому, конфигурации на обоих маршрутизаторах должны быть тем же. Оба маршрутизатора должны иметь то же выполнение образа. Также удостоверьтесь, что базовая платформа, используемая для обоих маршрутизаторы SNAT, является тем же.

Оптимальные методы NAT

Вопрос. . Есть ли какие-либо оптимальные методы NAT?

О. Да. Это оптимальные методы NAT:

1. И при использовании динамического и при использовании статического NAT, ACL, который устанавливает правило для динамического NAT, должен исключить

статические локальные хосты, таким образом, нет никакого наложения.

2. Остерегайтесь использования ACL для NAT с **permit ip any any**, поскольку можно получить непредсказуемые результаты. После 12.4 (20) NAT T преобразует локально генерируемый HSRP и пакеты протокола маршрутизации, если они будут отосланы внешний интерфейс, а также локально зашифрованные пакеты, совпадающие с правилом NAT.
3. Когда у вас будут наложения сети для NAT, используйте ключевое слово **match-in-vrf**. Необходимо добавить ключевое слово **match-in-vrf** для перекрывающихся статических записей NAT VRF для других VRF, но не возможно наложиться на глобальный и VRF адреса NAT.

```
Router(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf RED match-in-vrf Router(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf BLUE match-in-vrf
```
4. Пулы NAT с тем же диапазоном адресов не могут использоваться в других VRF, пока не используется ключевое слово **match-in-vrf**. Пример:

```
ip nat pool poolA 171.1.1.1 171.1.1.10 prefix-length 24 ip nat pool poolB 171.1.1.1 171.1.1.10 prefix-length 24 ip nat inside source list 1 poolA vrf A match-in-vrf ip nat inside source list 2 poolB vrf B match-in-vrf
```

Примечание: Wven, хотя конфигурация интерфейса командой строки допустима без ключевого слова **match-in-vrf** конфигурация, не поддерживается.
5. При развертывании распределения нагрузки интернет-провайдеров с перегрузкой интерфейса NAT оптимальный метод должен использовать route-map с интерфейсным соответствием по соответствию ACL.
6. При использовании сопоставления пула вы не должны использовать два других сопоставления (ACL или route-map) для совместного использования того же адреса пула NAT.
7. Когда развертывание того же NAT управляет на двух других маршрутизаторах в сценарии аварийного переключения, необходимо использовать резервирование HSRP.
8. Не определяйте тот же внутренний глобальный адрес в Статическом NAT и Динамическом пуле. Это действие может привести к нежелательным результатам.

[Дополнительные сведения](#)

- [Поддержка технологии IP-маршрутизации](#)
- [Cisco Systems – техническая поддержка и документация](#)