

# NAT в VoIP

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Общие сведения](#)

[Статический NAT](#)

[Динамический NAT](#)

[Перегрузка NAT \(PAT\)](#)

[Параметры командной строки NAT](#)

[Крошечное отверстие NAT](#)

[ALG](#)

[Шлюзы](#)

[ЛОКАЛЬНЫЙ](#)

[Локальный для удаленного](#)

[Удаленный удаленный сотрудник](#)

[Удаленные телефоны с общественностью \(чтение: маршрутизуемый\) IP-адреса](#)

[Удаленные телефоны с закрытым IP - адресом](#)

[Удаленные SIP-телефоны](#)

[NAT SBC](#)

[Примечания дизайна](#)

[!--- конфигурацию](#)

[Поток вызовов с NAT SBC](#)

[Регистрация SIP](#)

[Признаки](#)

[Команды show и debug](#)

[Вещи проверить](#)

[Сценарии](#)

[Основной NAT](#)

[SIP ALG](#)

## Введение

Этот документ описывает NAT (Трансляция сетевых адресов) поведение в маршрутизаторах, работающих как CUBE (Cisco Unified Border Element), CME или CUCME (Cisco Unified Communication Manager Express), шлюзы и CUSP (Cisco Унифицированный прокси SIP).

## Предварительные условия

### Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- SIP (протокол инициации сеанса)
- Передача голоса по IP (протокол Интернета)
- Протоколы маршрутизации

## Используемые компоненты

Информация в данном документе основана на следующих положениях

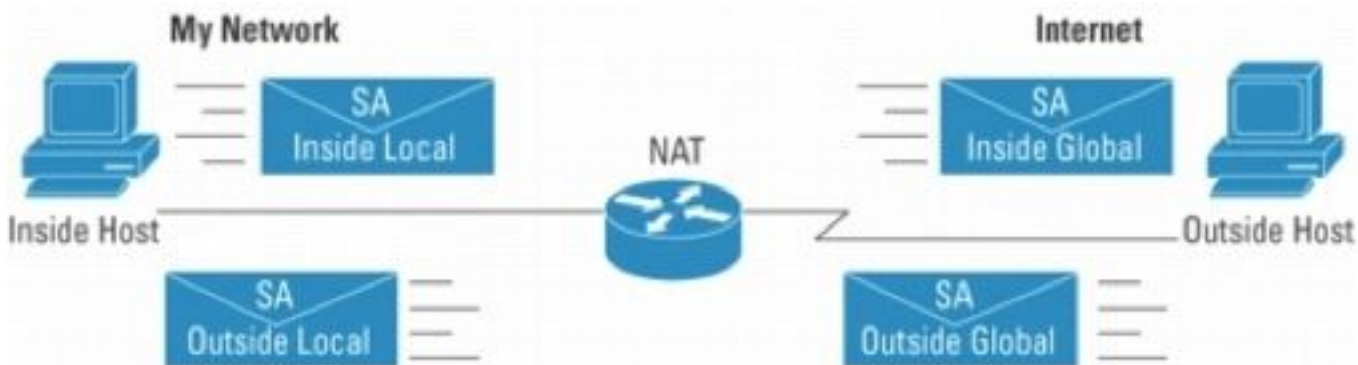
- Любая версия IOS 12.4T и выше.
- Любая версия CME

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.

## Общие сведения

Трансляция сетевых адресов является обычно используемым способом для перевода IP-адресов на пакетах, которые текут между сетями с помощью других адресных пространств. Цель этого документа не состоит в том, чтобы рассмотреть NAT. Скорее этот документ стремится предоставлять всеобъемлющий обзор NAT, поскольку это используется в Сетях VoIP Cisco. Кроме того, область ограничена компонентами, которые составляют Технологию передачи голосовых сообщений MS.

- NAT в основном заменяет IP-адрес в пакетах с другим IP-адресом
- Позволяет множественным хостам в частной подсети *совместно использовать* (т.е. появиться как) одиночный открытый IP - адрес, обратиться к Интернету.
- Как правило, конфигурации NAT изменяют только IP-адрес внутренних хостов
- NAT является двунаправленным - Если А будет преобразован в В на внутреннем интерфейсе, то В поступающий во внешний интерфейс будет преобразован в А!
- RFC 1631



An IP address is either local or global  
Local IP addresses are seen in the inside network  
Global IP addresses are seen in the Outside network

Рисунок 1

**Примечание:** Это может помочь думать о NAT как о помощи направить пакеты IP в и из сетей с помощью частного пространства адресов. Другими словами, NAT делает немаршрутизуемые адреса маршрутизуемыми

Рисунок 2 Показывает топологию, на которую ссылаются на рисунках, которые придерживаются.

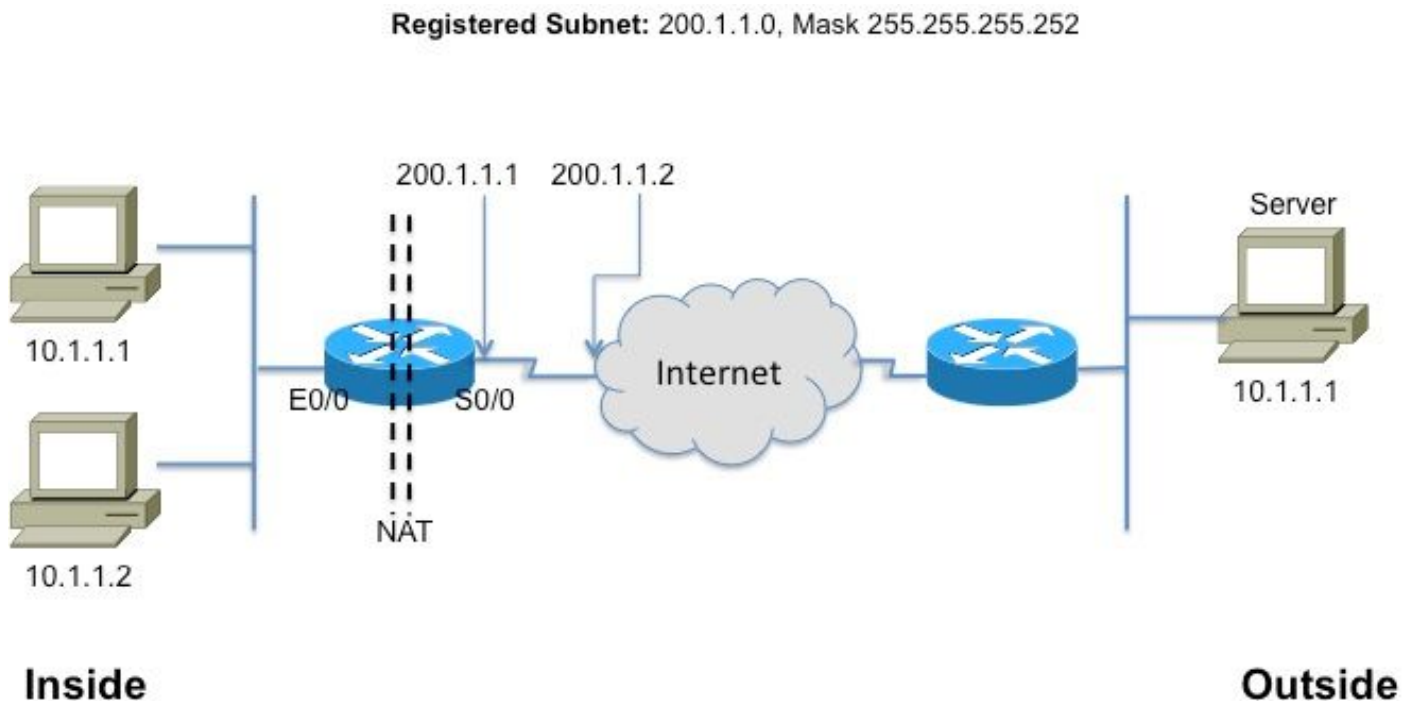


Рис. 2

Этот глоссарий является основным принципом, чтобы понять и описать NAT

- **Внутренний локальный адрес** – IP-адрес, назначенный хосту внутри сети. Как правило, адрес от частного пространства адресов.
- **Внутренний глобальный адрес** — маршрутизируемый IP - адрес, назначенный NIC или поставщиком услуг, который представляет один или больше в local ip address к внешнему миру.
- **Внешний локальный адрес** — IP-адрес внешнего хоста, как это появляется к внутренней сети. Этот адрес – необязательно допустимый – выделен из адресного пространства, маршрутизируемого внутри.
- **Внешний глобальный адрес** — IP-адрес, назначенный на хост на внешней сети владельцем хоста. Выделяемый из пространства глобальных маршрутизируемых сетевых адресов.

**Примечание:** Станьте довольными этими сроками. Любое примечание или doc на NAT, несомненно, обратятся к ним

## Статический NAT

Это - самая простая форма NAT, где в каждом внутреннем адресе статически преобразован во внешний адрес (и наоборот).

Inside Local	Inside Global
10.1.1.1	200.1.1.1
10.1.1.2	200.1.1.2

Рис. 3

CLI к конфигурации для вышеупомянутой трансляции следующие

```
interface Ethernet0/0
```

```
ip address 10.1.1.3 255.255.255.0
```

```
ip nat inside
```

```
!
```

```
interface Serial0/0
```

```
IP-адрес 200.1.1.251 255.255.255.252
```

```
ip nat снаружи <-Требуемый! [2]
```

```
ip nat inside source, статичный 10.1.1.2 200.1.1.2
```

```
ip nat inside source, статичный 10.1.1.1 200.1.1.1
```

## Динамический NAT

В динамическом NAT каждый внутренний хост сопоставлен с адресом от пула адресов.

- Выделяет IP-адрес от пула внутренних глобальных адресов.
- Если новый пакет поступает от еще одного внутреннего хоста, и этому нужна Запись NAT, но все объединенные IP-адреса используются, маршрутизатор просто сбрасывает от пакета.
- По существу пул внутренних глобальных адресов должен быть столь же большим как максимальное число параллельных хостов, которые должны использовать Интернет в то же время

Следующий CLI иллюстрирует настраивающий динамический NAT

```
ip nat pool fred 200.1.1.1 200.1.1.2 netmask 255.255.255.252
!
!
ip nat inside source list 1 pool fred
!
access-list 1 permit 10.1.1.2
access-list 1 permit 10.1.1.1
```

## Перегрузка NAT (PAT)

Когда пул (IP-адресов) меньше, чем набор адресов, которые должны быть преобразованы, эта функция пригождается.

- Несколько внутренних адресов, преобразованных посредством NAT только к одному или нескольким внешним адресам
- PAT (Преобразование адресов портов) использует уникальные номера исходного порта на Внутреннем **Глобальном IP-адресе** для различения трансляции. Поскольку номер порта закодирован в 16 битах, общее число могло теоретически быть целых 65,536 на IP-адрес. PAT попытается сохранить первый исходный порт, если этот исходный порт уже будет выделенным PAT, то попытается найти первый номер доступного порта
- Перегрузка NAT может использовать больше чем 65,000 портов, позволяя ему масштабироваться хорошо, не будучи нужен во многих зарегистрированных IP - адресах — во многих случаях, будучи нужен только в одном внешнем глобальном IP-адресе.

Рисунок 4 иллюстрирует PAT.

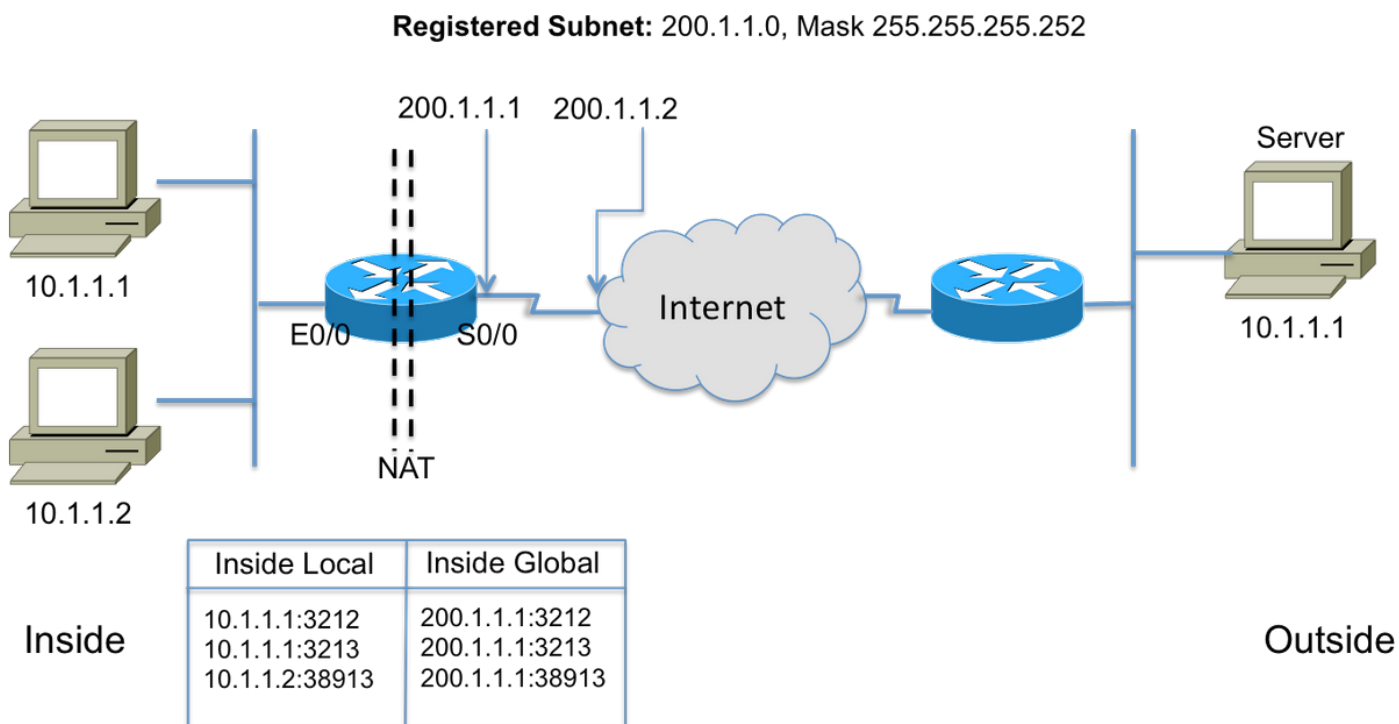


Рис. 4

## Параметры командной строки NAT

Реализация NAT Cisco очень универсальна с хостом опций. Некоторые упомянуты ниже, но см. [http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies\\_white\\_paper09186a0080091cb9.html](http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.html) для подробных данных о полном списке усовершенствований.

- Статические преобразования с портами – Входящие пакеты, адресованные определенному порту (например, порту 25, для сервера SMTP) передаваемый

определенному серверу.

- Поддержка Карт маршрутизации - Гибкость в настройке ФИЛЬТРОВ/ACL
- Более гибкие конфигурации пула - для разрешения прерывистых диапазонов адресов.
- Сохранение номера узла - Преобразовывает "сетевую" часть, сохраняет часть "хоста".

## Крошечное отверстие NAT

Крошечное отверстие в языке NAT обращается к сопоставлению между <IP - адрес хоста, порт> и <глобальный адрес, *глобальный* порт> кортежи. Это позволяет устройству NAT использовать номер порта назначения (который был бы *глобальным* портом) входящих сообщений для сопоставления назначения назад с IP - адресом хоста и портом, который инициировал сеанс. Следует отметить, что таймаут крошечных отверстий после периода неиспользования и общего адреса возвращен к пулу NAT.

## NAT в VoIP

Так, каковы проблемы и проблемы с NAT в Сетях VoIP? Ну, вспомните, что NAT, который мы обсудили до сих пор (*loosely referred to* как основной NAT) только, преобразовывает IP-адрес в *Заголовке IP - пакете* и повторно вычисляет контрольную сумму, конечно, но адреса переноса VoIP передача сигналов, встроенные в *тело* сообщений о передаче сигнала. Другими словами, на Уровне 5

Рисунок 5 иллюстрирует эффект отъезда необработанных встроенных IP - адресов. Передача вызовов завершает успешный, но прокси SIP в сбоях поставщика услуг, пытающихся направить среды (RTP) пакеты к адресу сред, передаваемому агентом вызовов!



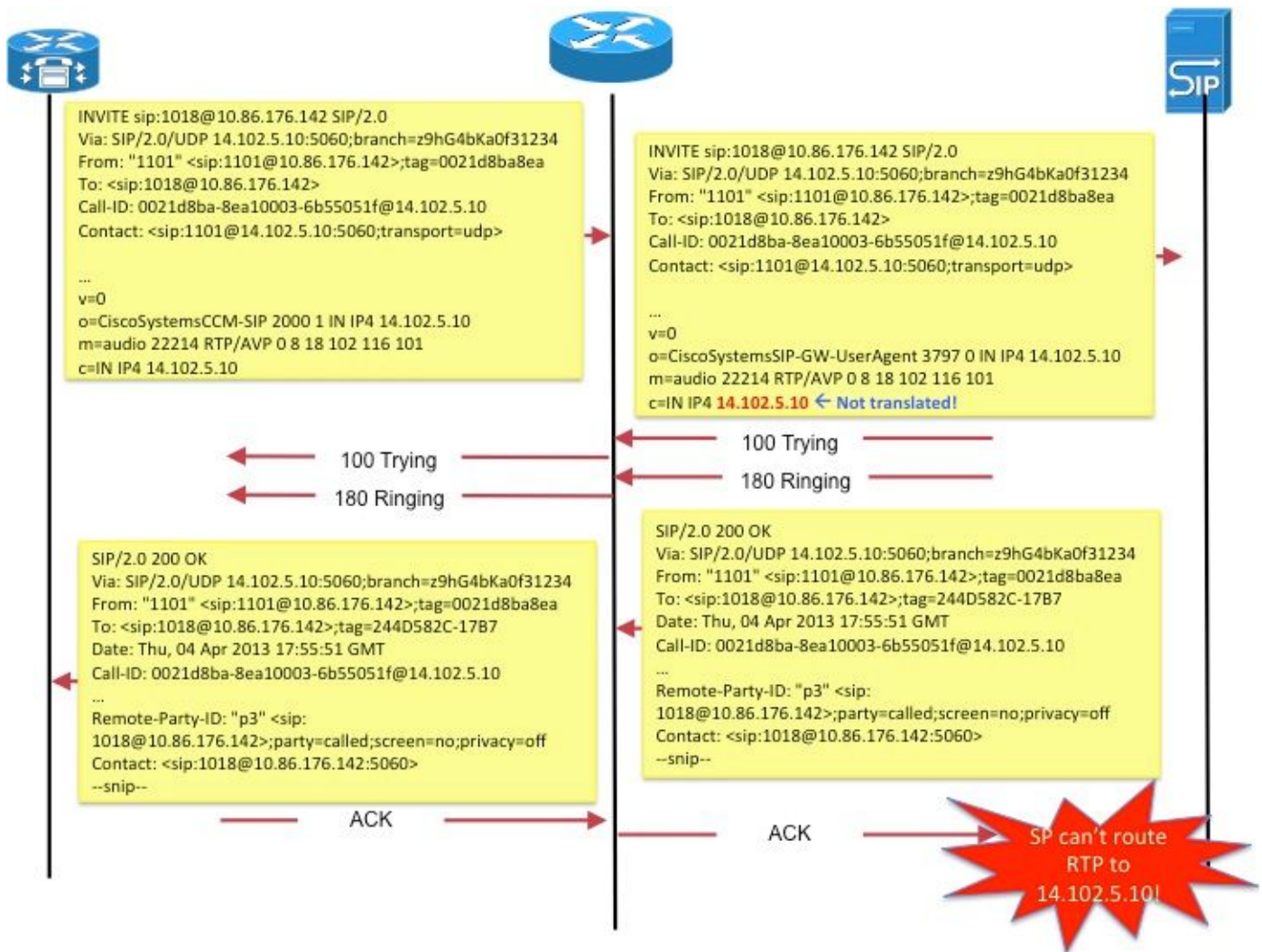


Рис. 5

Другим примером было бы использование конечной точки SIP **Контакта**: поле в SDP для передачи адреса, в котором конечная точка хотела бы получить сообщения о передаче сигнала для новых запросов.

Эти проблемы решены функцией под названием Шлюз уровня приложения (ALG).

## ALG

ALG понимает протокол, используемый определенными приложениями, что это поддерживает (например, SIP) и действительно протоколирует проверку пакетов и "устройство" трафика через него. Для хорошего описания того, как различные поля исправлены для сигнализации вызова SIP, обратитесь к <http://www.voip-info.org/wiki/view/Routers+SIP+ALG>.

На маршрутизаторах Cisco поддержка SIP ALG включена, по умолчанию, на стандартном порте TCP 5060. Возможно настроить ALG для поддержки нестандартных портов для сигнализации SIP. См. [http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr\\_nat/configuration/15-mt/nat-tcp-sip-alg.html](http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-tcp-sip-alg.html).

**Внимание.** : Остерегайтесь! Нет никакого RFC или другого стандарта, который обстоятельно объясняет, который встроил поля, должен быть преобразован для

различных протоколов VoIP. В результате реализации варьируются, среди поставщиков оборудования, приводящих к проблемам interop (и кэйсы TAC (Центра технической поддержки)).

## Шлюзы

Так как шлюзы, по определению, не являются устройствами от ip к ip, NAT не применим.

## СМЕ

Этот раздел сценариев вызова просмотра документации с СМЕ для понимания, почему должен использоваться NAT.

Сценарий 1. Местные телефоны

Сценарий 2. Удаленные телефоны (с открытыми IP - адресами)

Ситуация 3. Удаленный удаленный сотрудник

**Примечание:** Во всех случаях, для аудио для течения IP-адрес СМЕ должен быть маршрутизируемым

## ЛОКАЛЬНЫЙ

В этом сценарии (рисунок 6) два телефона, вовлеченные в вызов, являются телефонами подключенный по протоколу Skinny с закрытыми IP - адресами.



Рис. 6

**Примечание:** Помните, что телефон подключенный по протоколу Skinny, который связан в вызове с другим телефоном подключенный по протоколу Skinny в той же системе СМЕ, передает свои пакеты среды непосредственно к другому телефону; т.е. RTP для местного телефона к местному телефону НЕ течет через СМЕ.

Поэтому NAT не является применимым или требуемым в этом случае.



**Примечание:** СМЕ определяет, должны ли среды (RTP) непосредственно или не на основе того, и ли два телефона, вовлеченные в вызов, облежены и в тот же сегмент сети. В противном случае СМЕ вставляет себя в путь RTP.

## Локальный для удаленного

В этом сценарии (рисунок 7) СМЕ вставляет себя в поток RTP, таким образом, что RTP с телефонов будет завершен на СМЕ. СМЕ будет повторно инициировать потоки к другому телефону. Так как СМЕ находится и во внутренней (частной) сети и во внешней сети и передает свой внутренний адрес к внутреннему телефону и внешний (общий) адрес к внешнему телефону, NAT не требуется здесь также.

Обратите внимание, однако, что порты UDP/TCP (сигнализация, а также RTP) должны быть открыты между удаленным IP-телефоном и IP - адресом источника СМЕ. Это означает, что межсетевые экраны или другие фильтрующие устройства настроены для разрешения рассматриваемых портов.

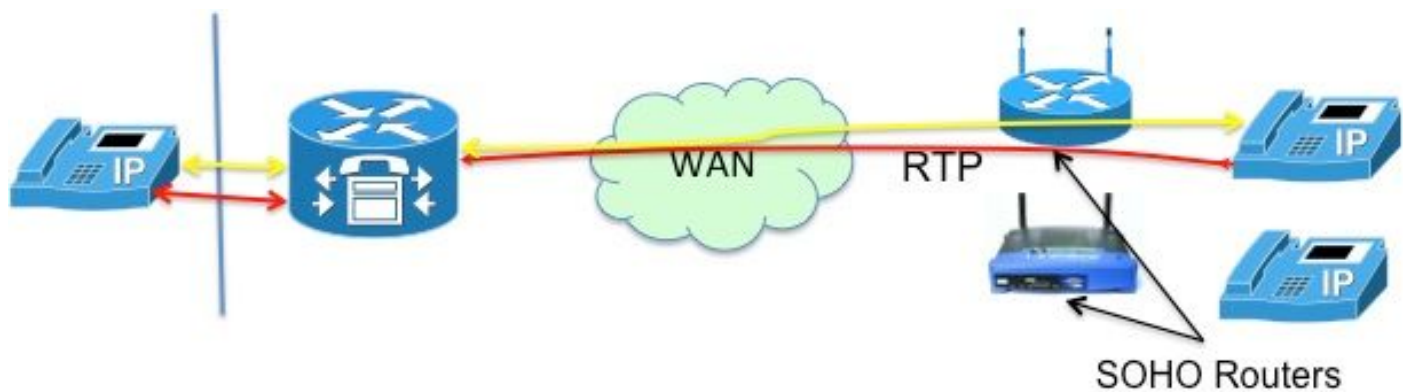


Рисунок 7

**Примечание:** Обратите внимание на то, что сигнальный [сообщения] всегда завершаются на СМ

## Удаленный удаленный сотрудник

Это обращается к IP-телефонам, соединяющимся с СМЕ по глобальной сети (WAN) для поддержки удаленных сотрудников, у которых есть офисы, которые удалены от маршрутизатора СМЕ. Наиболее распространенные дизайны - те, которые связали телефоны с маршрутизируемыми IP - адресами и телефоны с закрытыми IP - адресами.

### Удаленные телефоны с общественностью (чтение: маршрутизуемый) IP-адреса

Если оба, телефоны, вовлеченные в вызов, установлены настройки с общественностью, маршрутизируемыми IP - адресами, среды, могут течь между телефонами непосредственно (рисунок 8). Поэтому еще раз, никакая потребность в NAT!

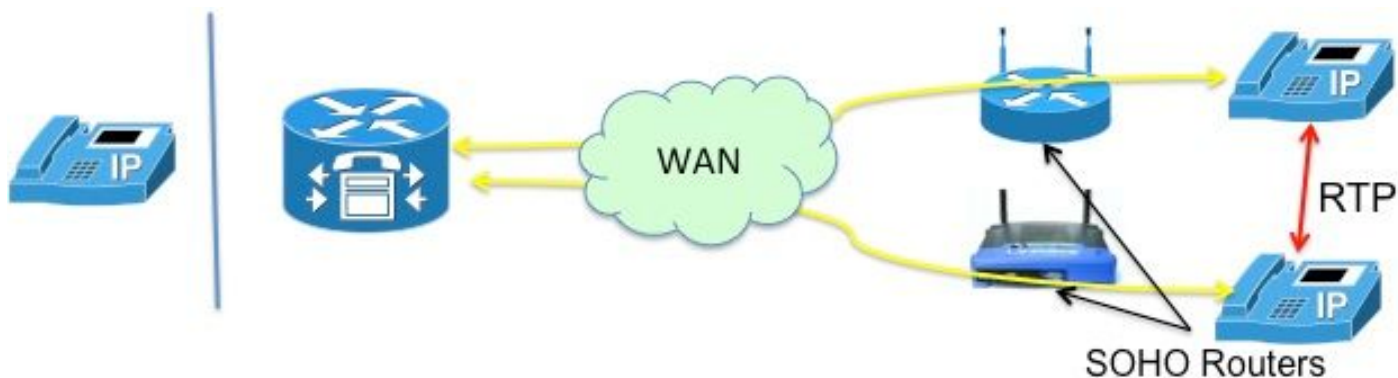


Рис. 8

## Удаленные телефоны с закрытым IP - адресом

В этом сценарии вызов сообщен между телефонами подключенный по протоколу Skinny, настроенными с закрытыми IP - адресами. Домашний офис (SOHO) маршрутизаторы, в целом, склонен не быть “знающим SCCP”. т.е. неспособный к переводу IP-адресов встроен в сообщения SCCP. Это означает, что, после вызова устанавливает завершение, телефоны заканчиваются с закрытым IP - адресом друг друга. Начиная с обоих телефоны являются частными, CME будет сигнализировать вызов между ними таким образом, что аудио течет непосредственно между телефонами. Это, однако, приведет к одностороннему или без звука аудио (так как закрытые IP - адреса, по определению, не могут маршрутизироваться к в Интернете!), пока один из следующих обходных путей не внедрен -

- Настройте статические маршруты на Маршрутизаторах Soho
- установите соединение IPSec VPN с телефонами

Лучший способ решить это состоял бы в том, чтобы настроить “mtp”. mtp команда гарантирует, что среды (RTP) пакеты от удаленных телефонов передают транзитом через маршрутизатор CME (рисунок 9).

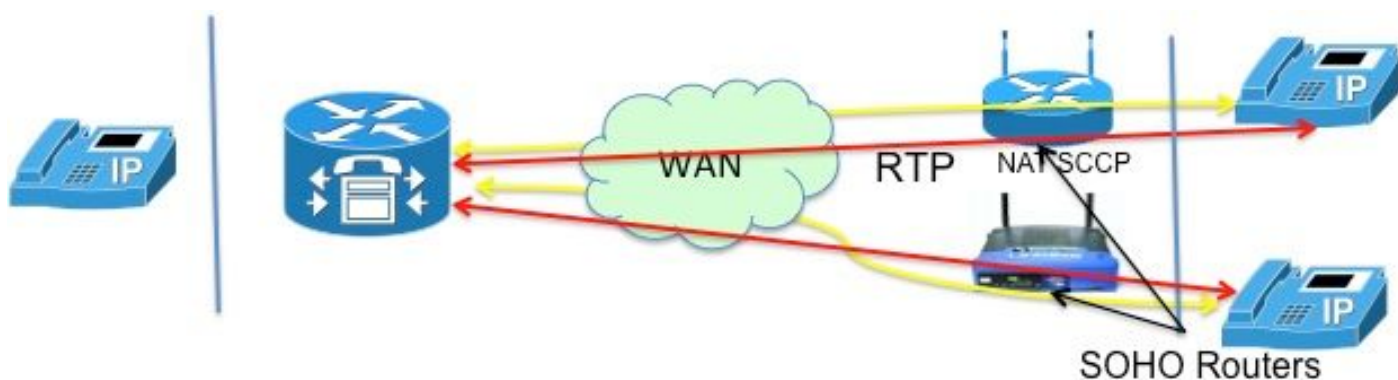


Рис. 9

“mtp” решение лучше из-за осложнений с открытием портов межсетевого экрана. Пакеты среды, текущие по глобальной сети (WAN), могут быть затруднены межсетевым экраном. Это означает, что вам нужно к открытым портам на межсетевом экране, но которые? С CME, передающим аудио, межсетевые экраны могут быть легко настроены для передачи пакетов RTP. Маршрутизатор CME использует **определенный** порт UDP (2000!) для пакетов среды. Так, просто позволив пакеты и от порта 2000, трафик RTP ALL можно передать.

Рисунок 10 иллюстрирует, как настроить mtp.

```
ephone 1  
  
Mac 1111.2222.3333  
  
тип 7965  
  
mtp  
  
кнопка 1:1
```

Рис. 10

Все не замечательно с mtp. Существуют ситуации, где mtp может не быть выбираемым

- MTP не нежен на загрузке ЦПУ
- МОН групповой адресации обычно не может передаваться по глобальной сети (WAN) - проверки функции МОН Групповой адресации, чтобы видеть, включен ли MTP для телефона и если это, не передает МОН к этому голосовому.

Таким образом, если у вас есть конфигурация глобальной сети (WAN), которая **может** передать пакеты групповой адресации, и можно позволить пакеты RTP через межсетевой экран, можно решить не использовать MTP.

## Удаленные SIP-телефоны

Обратите внимание на то, что SIP-телефоны не были упомянуты в вышеупомянутых сценариях. Это вызвано тем, что факта, что, если один из телефонов является SIP-телефоном, СМЕ вставляет себя в аудиопуть. Это тогда становится локальным-к-удаленному сценарием, описанным ранее, в чем NAT не требуется.

## CUBE

CUBE по сути выполняет NAT и функции PAT, как это завершает и повторно иницирует все сеансы. CUBE заменяет своим собственным адресом адрес любой оконечной точки, которую это передает с, таким образом эффективно скрываясь (перевод) адреса той оконечной точки.

Таким образом NAT не требуется с функцией CUBE. Существует сценарий Сервиса VoIP, в котором NAT требуется на CUBE, как описано в следующем разделе.

## Размещенное прохождение NAT

Краткие общие сведения на Размещенном сервисе телефонии помогут понимать объяснение для этой функции.

Размещенный сервис телефонии является новой формой Сервиса VoIP, в котором большая часть механизма находится в местоположении поставщика услуг. Они работают с домашними шлюзами (HGW), которые внедряют только основной NAT (т.е. NAT в L3/L4).

Например, Verizon устанавливает Терминал оптической сети (ONT), который предоставляет сервисы FiOS дома; голосовой вызов сообщен с помощью процесса SIP, встроенного в ОНТАРИО, которым сигнализация SIP сделана по частному IP - сети Verizon к новым программным коммутаторам, которые предоставляют сервис и контроль для установления голосовой связи другим клиентам Оцифрованной речи FiOS, или клиентам традиционного телефона.

Среди ключевых требований поставщика для размещенного сервиса телефонии включают,

- Удаленный обход NAT: способность предоставить услуги Класса 5 оконечным точкам, использующим NAT (который может только сделать уровень 3 NAT!) и устройства с функциями межсетевого экрана (путем выполнения "ALG" удаленно!)
  - Поддержка среды компании: способность передать среды между совместно-расположенными устройствами, где это не целесообразно направлять среды назад к IP - сети
  - Никакое добавленное оборудование, избавляя от необходимости добавить любой CPE.
- Данный вышеупомянутое, какие опции существуют для реализации такого сервиса?

- Замените HGW дорогим ALG,
- Используйте контроллер границы сеанса (SBC) для изменения встроенных заголовков SIP для пакетов. Это включает размещенный сетью, SIP поддержки продукта класса носителя в очень безопасной, отказоустойчивой конфигурации. Это решение отнесено в NAT SBC.

Опция NAT SBC удовлетворяет упомянутые выше требования поставщика.

## NAT SBC

NAT SBC работает следующим образом (рисунок 11)

1. Маршрутизатор доступа преобразовывает только IP-адрес L3/L4
2. IP-адрес в сообщении SIP, не преобразованном
3. SBC NAT перехватывает и преобразовывает встроенный IP - адрес. Момент SBC видит пакеты SIP, предназначенные к **200.200.200.10**, он ударяет туземный-sbc код.
4. Среда не преобразованы и идут непосредственно между телефонами [\[5\]](#)

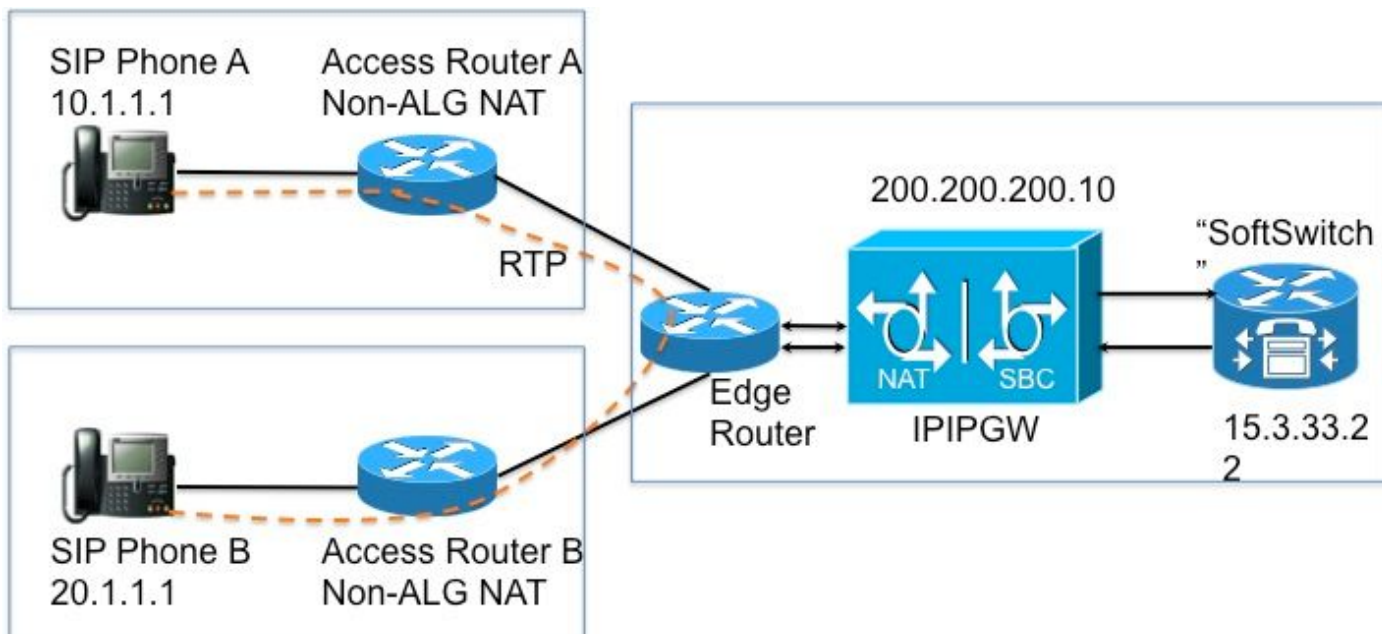


Рис. 1-1

## Примечания дизайна

- IP-адрес **200.200.200.10** (рисунок 12) не назначен ни на какой интерфейс на NAT SBC. Это настроено как адрес “прокси”, к которому SIP-телефон А и SIP-телефон В передают сообщения о передаче сигнала.
- Устройства Дом не преобразовывают определенный SIP/SDP поля *только для адреса* (например, CallId: O =, Предупреждение: заголовок и ответвление = параметр. maddr = и полученный = параметры обрабатывались в определенных сценариях только.). Эти поля обрабатываются NAT SBC, за исключением трансляции и авторизации авторизации прокси, потому что они сломают аутентификацию.
- Если домашние устройства настроены, чтобы сделать PAT, клиенты User Agent (телефоны и прокси) должны поддерживать симметричную сигнализацию [6] и симметричные и ранние среды. Необходимо настроить порт замены на NAT маршрутизатор SBC.
- В отсутствие поддержки симметричной сигнализации и симметричных и ранних сред, промежуточные маршрутизаторы должны быть настроены без PAT, и адрес замены должен быть настроен в NAT SBC.

## !--- конфигурацию

Пример конфигурации для типичного NAT SBC придерживается.

```
ip nat sip-sbc
    проксируйте 200.200.200.10 5060 15.3.33.22 5060 udr протокола
    пул идентификатора вызова пула идентификатора вызова
    session-timeout 300
    режим allow-flow-around
    порт замены
```

!

маска подсети sbc1 15.3.33.61 15.3.33.69 ip nat pool 255.255.0.0

маска подсети sbc2 15.3.33.91 15.3.33.99 ip nat pool 255.255.0.0

пул идентификатора вызова ip nat pool 1.1.1.1 1.1.255.254 масок подсети 255.255.0.0

внешний пул ip nat pool 200.200.200.100 200.200.200.200 маски подсети 255.255.255.0

список 1 ip nat inside source объединяет sbc1 перегрузку

список 2 ip nat inside source объединяет sbc2

список 3 ip nat outside source объединяет внешний пул add-route

список 4 ip nat inside source объединяет пул идентификатора вызова

!

разрешение access-list 1 10.1.1.0 0.0.0.255

разрешение access-list 1 171.1.1.0 0.0.0.255

разрешение на access-list 2 20.1.1.0 0.0.0.255

разрешение на access-list 2 172.1.1.0 0.0.0.255

разрешение на access-list 3 15.4.0.0 0.0.255.255

разрешение на access-list 3 15.5.0.0 0.0.255.255

разрешение на access-list 4 10.1.0.0 0.0.255.255

разрешение на access-list 4 20.1.0.0 0.0.255.255

## Поток вызовов с NAT SBC

Рисунок 13 и рисунок 14 иллюстрируют поток вызовов с точки зрения трансляций. На следующие моменты нужно обратить внимание -

- После регистрации программный коммутатор записывает два телефона как
  - SIP-телефон – 15.3.33.62 2001
  - SIP-телефон В – 15.3.33.62 2002
- В этом потоке вызовов SBC NAT эффективно оставляет IP-адрес сред необработанным.



## Call Flow – Media Flow-Around Phone A Calls Phone B

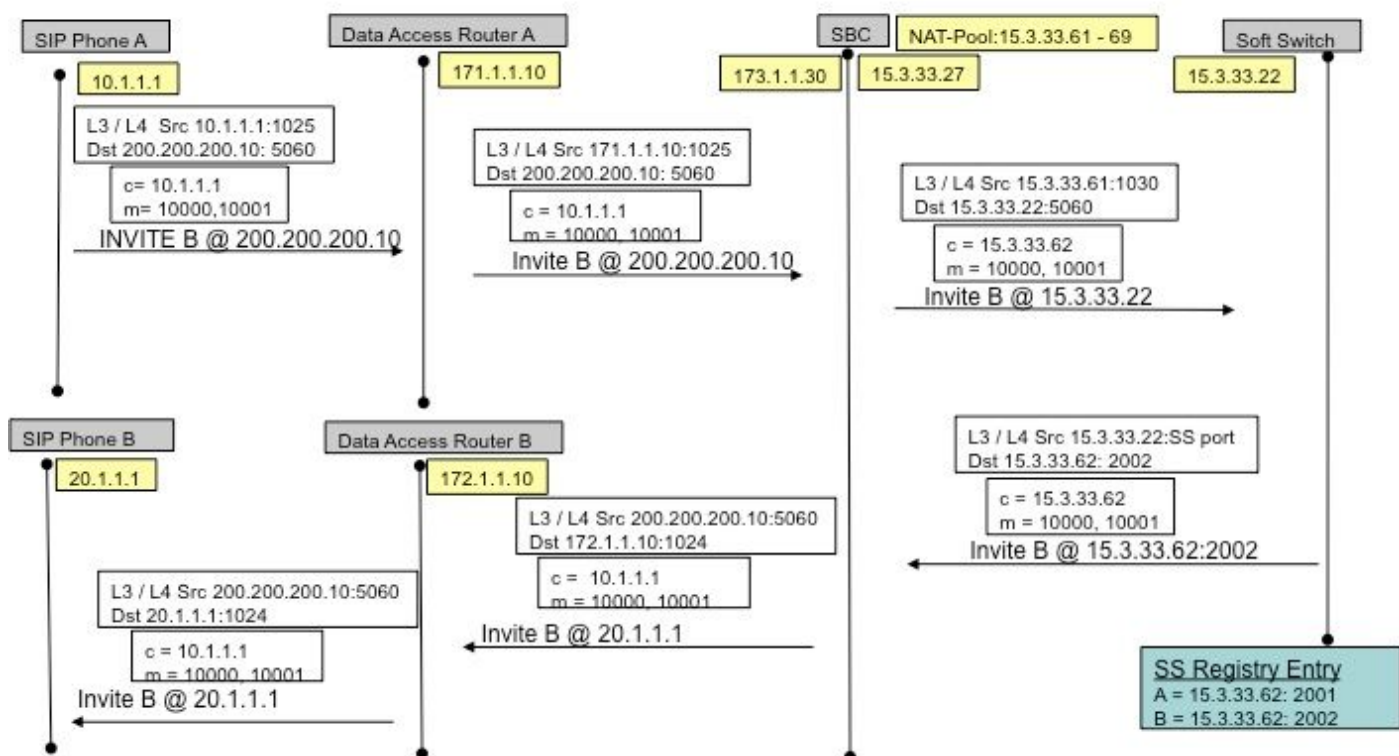


Рисунок 13

## Call Flow – Media Flow-Around (Cont' d) Phone A Calls Phone B

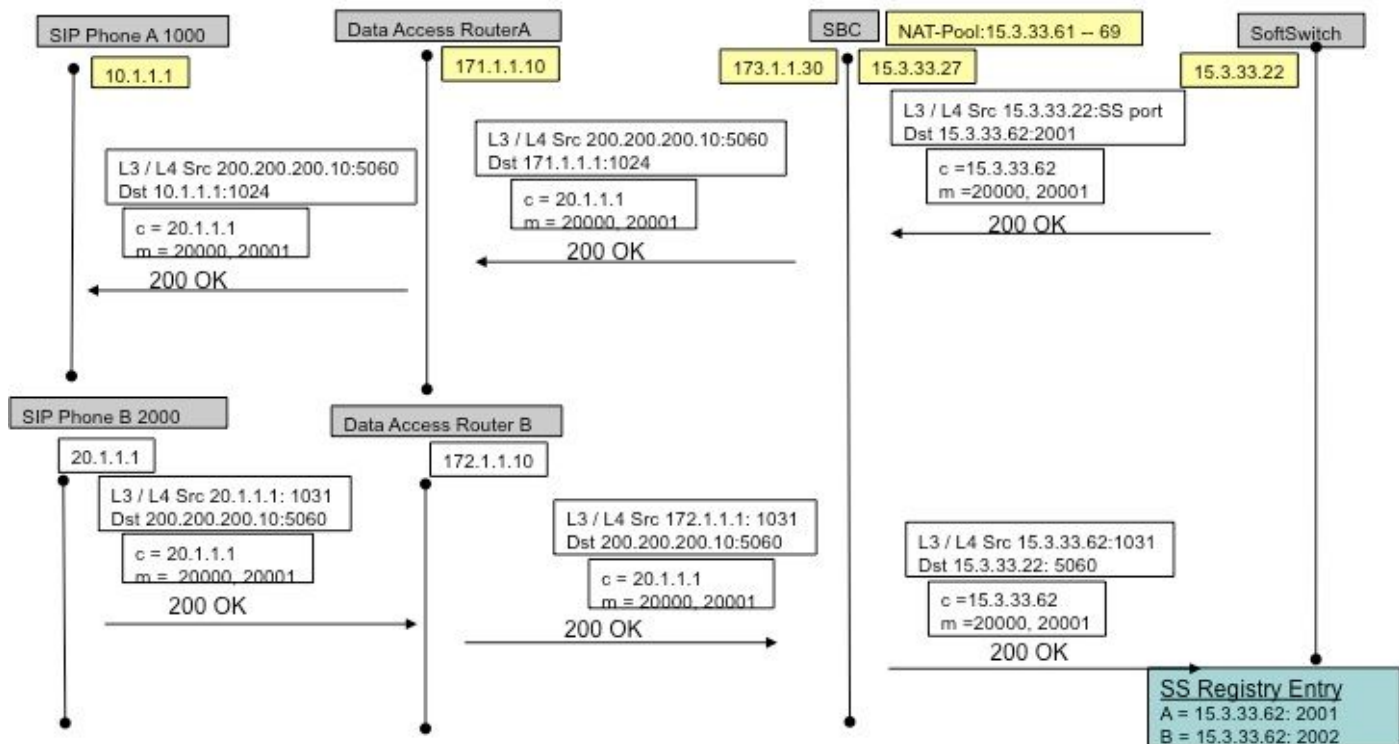


Рисунок 14

## Регистрация SIP

В более ранних версиях (NAT SBC), конечные точки SIP должны были передать *пакеты keep-alive* для хранения крошечного отверстия регистрации SIP открытым (для разрешения посещать-> в трафике для течения, например, входящие вызовы). *пакеты keep-alive* могли быть любым пакетом SIP, переданным конечной точкой или регистратором (программный коммутатор). Последние версии устраняют потребность в этом с NAT-SBC самом (в противоположность программным коммутаторам) то, чтобы вынуждать конечные точки повторно регистрировать часто для хранения крошечных отверстий открытыми.

**Примечание:** Признаки регистрационного крошечного отверстия с истекшим сроком могут быть неясными со случайными сбоями передачи вызовов.

## ОСТРЫЙ ВЫСТУП

CUSP имеет понятие логической сети, которая обращается к набору локальных интерфейсов, которые рассматриваются так же для (например, интерфейс, порт, транспорт для прослушивания) назначения маршрутизации. При настройке логической сети на CUSP можно настроить его для использования NAT. После того, как настроенный, SIP ALG автоматически включен. Это полезно когда определенные логические сети.

## Устранение неисправностей

### Признаки

Очевидный признак мог бы быть то, что вызов отказывает в одном или обоих направлениях. Меньше очевидных признаков могло бы включать,

- Односторонняя передача аудиоданных
- Односторонняя передача аудиоданных на передаче
- Без звука аудио
- Потеря регистрации SIP

### Команды show и debug

- `ip nat deb [потягивает | облегченный]`
- `show ip nat statistics`
- `show ip nat translations`

### Вещи проверить

- Гарантируйте, что конфигурация включает **ip nat** **внутри** или подкоманду **внешнего интерфейса ip nat**. Эти команды включают NAT на интерфейсах, и внутреннее/внешнее обозначение важно.

- Для статического NAT гарантируйте что **ip nat source статические** списки команд внутренней локальный адрес сначала и внутренней второй глобальный IP-адрес.
- Для динамического NAT гарантируйте, что ACL настроил для соответствия с пакетами, переданными соответствием внутреннего хоста, что пакеты хоста, прежде чем произошло любое преобразование NAT. Например, если внутренний локальный адрес 10.1.1.1 должен быть преобразован в 200.1.1.1, гарантировать, что ACL совпадает с адресом источника 10.1.1.1, не 200.1.1.1.
- Для динамического NAT без PAT гарантируйте, что пул имеет достаточно IP-адресов. Признаки не наличия достаточного количества адресов включают растущее значение во второй счетчик неудач в выходных данных **команды show ip nat statistics**, а также видящий все адреса в диапазоне, определенном в пуле NAT в списке динамических преобразований.
- Для PAT легко забыть добавлять опцию **перегрузки** на **команде ip nat inside source list**. Без него работает NAT, но PAT не делает, часто приводя к пакетам пользователей, не преобразовываемым и хостам, не бывшим способным добираться до Интернета.
- Возможно, NAT был настроен правильно, но ACL существует на одном из интерфейсов, сбрасывая от пакетов. Обратите внимание на то, что ACL процессов IOS перед NAT для пакетов, входящих интерфейс, и после перевода адресов для пакетов, выходящих из интерфейса.
- Не забывайте настраивать "ip nat снаружи" на взаимодействии через интерфейс, стоящем перед глобальной сетью (WAN) (даже если, не преобразовывая внешний адрес)!
- Как только NAT настроен, show ip nat translations ничего не показывает. Эхо-запрос однажды и затем проверяет снова.
- Захватите **Трассировки wireshark** на внутренних и внешних интерфейсах NAT-SBC

## Сценарии

Выходные данные отладки для нескольких сценариев показывают ниже. Они главным образом очевидны!

### Основной NAT

Конфигурацию и линии отладки для основного NAT показывают ниже.

```
interface Loopback0
 ip address 10.1.1.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
!
interface Serial0/1/0
 description **Line to FRS**
 ip address 100.10.10.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 encapsulation ppp
 ip nat inside source list 91 interface Serial0/1/0 overload
 access-list 91 permit 10.1.1.1
```

```
R1#show ip nat translations
Pro Inside global      Inside local          Outside local         Outside global
icmp 100.10.10.1:7    10.1.1.1:7           200.200.200.2:7     200.200.200.2:7
icmp 100.10.10.1:8    10.1.1.1:8           200.200.200.2:8     200.200.200.2:8
```

```
R1#ping 200.200.200.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 200.200.200.2, timeout is 2 seconds:
!!!!
R1# sho log
000044: *Apr 17 00:13:00.027: NAT: s=10.1.1.1->100.10.10.1, d=200.200.200.2
[40]
000045: *Apr 17 00:13:00.027: NAT*: s=200.200.200.2, d=100.10.10.1->10.1.1.1
[40]
```

Debug line for NAT on Incoming packet

## SIP ALG

Выходные линии от `show debug ip nat` показывают. В этом случае встроенный IP - адрес на исходящем пакете преобразован.

```
ip nat inside source static 10.1.1.1 20.1.1.1
```

```
-----  
Sent: INVITE sip:1018@10.86.176.142:5060 SIP/2.0  
Via: SIP/2.0/UDP 10.1.1.1:5060;branch=z9hG4bK23C1ED01  
Remote-Party-ID: "3196" <sip:3196@10.1.1.1>;party=calling;screen=no;privacy=off  
From: "3196" <sip:3196@10.1.1.1>;tag=A9F3DB34-EEE  
To: <sip:1018@10.86.176.142>  
Date: Tue, 23 Apr 2013 17:53:02 GMT  
Call-ID: 7A3AC014-AB7511E2-BE6BB2A0-B6AF1B2B@10.1.1.1  
--snip--  
Contact: <sip:3196@10.1.1.1:5060>  
--snip--  
v=0  
o=CiscoSystemsSIP-GW-UserAgent 9771 5845 IN IP4 10.1.1.1  
s=SIP Call  
c=IN IP4 10.1.1.1  
t=0 0  
m=audio 16384 RTP/AVP 18 100 101  
c=IN IP4 10.1.1.1  
--snip--
```

```
-----  
068441: Apr 23 13:53:02.477: NAT: SIP: [0] processing INVITE message  
068442: Apr 23 13:53:02.477: NAT: SIP: [0] register:0 door_created:0  
--snip--  
068447: Apr 23 13:53:02.477: NAT: SIP: [0] translated embedded address 10.1.1.1->20.1.1.1  
068448: Apr 23 13:53:02.477: NAT: SIP: [0] register:0 door_created:0  
068449: Apr 23 13:53:02.477: NAT: SIP: [0] register:0 door_created:0  
068450: Apr 23 13:53:02.477: NAT: SIP: Contact header found  
068451: Apr 23 13:53:02.477: NAT: SIP: Trying to find expires parameter  
068452: Apr 23 13:53:02.477: NAT: SIP: [0] translated embedded address 10.1.1.1->20.1.1.1  
068453: Apr 23 13:53:02.477: NAT: SIP: [0] register:0 door_created:0  
068454: Apr 23 13:53:02.477: NAT: SIP: [0] message body found  
068455: Apr 23 13:53:02.477: NAT: SIP: Media Lines present:1  
068456: Apr 23 13:53:02.477: NAT: SIP: Translated m= (10.1.1.1, 16384) -> (20.1.1.1, 16384)  
068457: Apr 23 13:53:02.477: NAT: SIP: old_sdp_len:307 new_sdp_len :307  
068458: Apr 23 13:53:02.477: //158107/79BF74A6BE66/SIP/Msg/ccsipDisplayMsg:
```

## Ссылки

### Обзор:

- [http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies\\_white\\_paper09186a0080091cb9.HTML](http://www.cisco.com/en/US/partner/technologies/tk648/tk361/tk438/technologies_white_paper09186a0080091cb9.HTML)
- **Анатомия:** [http://www.cisco.com/web/about/ac123/ac147/archived\\_issues/ipj\\_7-3/anatomy.html](http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-3/anatomy.html)
- [http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_tech\\_note09186a0080094831.shtml](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094831.shtml)

### VoiP и NAT

- <https://supportforums.cisco.com/docs/DOC-5406>
- <http://www.juniper.net/techpubs/software/junos-security/junos-security95/junos-security-swconfig-security/id-60290.HTML>

### Матрица характеристики NAT

- [http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_tech\\_note09186a0080b17919.shtml](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080b17919.shtml)
- [http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_tech\\_note09186a0080b17919.shtml](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080b17919.shtml)

[com/en/US/technologies/tk648/tk361/tk438/technologies\\_white\\_paper09186a00801af2b9.HTML](http://www.cisco.com/en/US/technologies/tk648/tk361/tk438/technologies_white_paper09186a00801af2b9.HTML)

- [http://www.cisco.com/en/US/tech/tk648/tk361/technologies\\_tech\\_note09186a0080b17919.shtml](http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080b17919.shtml)

#### Размещенный обход NAT:

- [www.tmcnet.com/it/0804/FKagoor.htm](http://www.tmcnet.com/it/0804/FKagoor.htm)

#### NAT SBC

- EDCS-611622
- EDCS-526070

#### ALG:

- [http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr\\_nat/configuration/15-0s/iadnat-applvlgw.html](http://www.cisco.com/en/US/docs/ios-xml/ios/ipaddr_nat/configuration/15-0s/iadnat-applvlgw.html)
- <http://www.voip-info.org/wiki/view/Routers+SIP+ALG>
- <http://www.commpartners.us/knowledge/attachments/voip-nat.pdf>
- [http://www.cisco.com/en/US/partner/docs/ios-xml/ios/ipaddr\\_nat/configuration/15-mt/nat-tcp-sip-alg.html](http://www.cisco.com/en/US/partner/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-tcp-sip-alg.html)

#### CME

- [http://www.cisco.com/en/US/docs/voice\\_ip\\_comm/cucme/srnd/design/guide/security.html#wp1077376](http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/srnd/design/guide/security.html#wp1077376)
- [http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/sbcu/sbc\\_cucm.html](http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/sbcu/sbc_cucm.html)