# Типы трансляции сетевых адресов (NAT) и SIP

Перейти к: навигация, поиск

***Приглашаем принять участие в тестировании виртуальной АТС от SIPNET!***

**Содержание**

[убрать]



# ВВЕДЕНИЕ

Трансляция сетевых адресов (NAT) используется многими сервис провайдерами и частными пользователями для решения проблемы нехватки реальных IP-адресов и обеспечения безопасности локальных сетей подключенных к Интернету. Например. Предприятие может иметь выделенный диапазон реальных IP-адресов, но гораздо большее количество компьютеров имеющих локальные IP-адреса которым необходим доступ в Интернет. Для решения этой проблемы используется технология трансляции адресов, которая позволяет компьютерам локальной сети взаимодействовать с сетью Интернет, используя всего один внешний реальный IP-адрес. NAT решает эту проблему с помощью подмены локального IP-адреса на наружный общедоступный адрес. Заменяя внутренний IP-адрес и порт на внешний IP-адрес и порт, NAT сохраняет таблицу соответствия, затем при получении ответного пакета производится обратное преобразование.
К локальным IP-адресам относятся следующие диапазоны адресов: 10.xxx.xxx.xxx, 192.168.xxx.xxx, 172.16.xxx.xxx - 172.32.xxx.xxx.

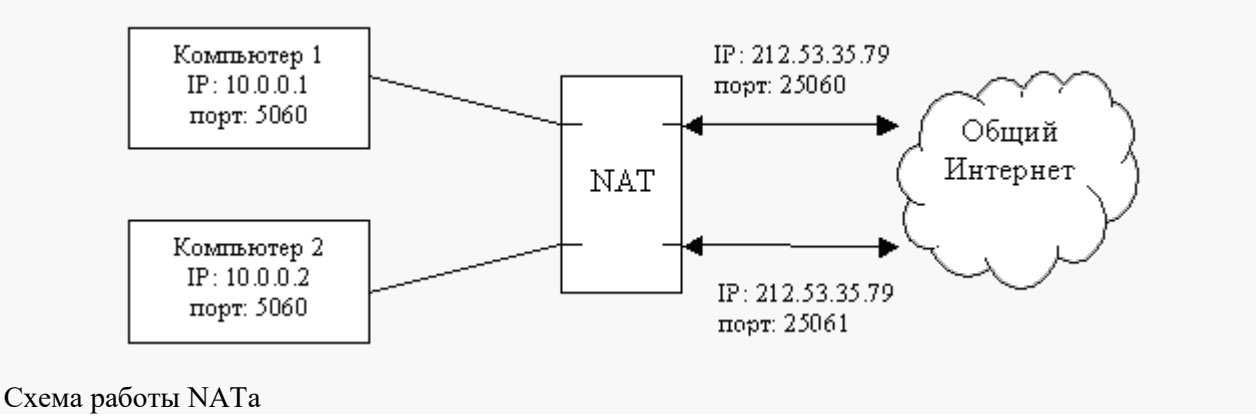


Схема работы NATa

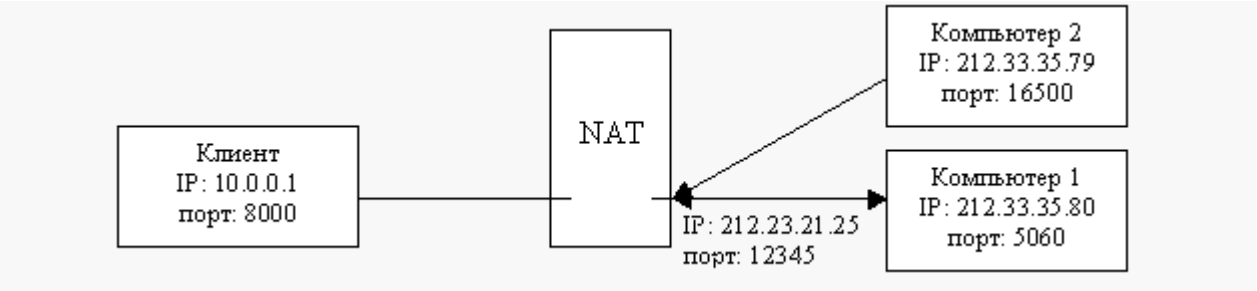
# Типы трансляторов сетевых адресов (NAT)

Трансляторы адресов подразделяются на 4 типа:
1. Полный конус (Full Cone)
2. Ограниченный конус (Restricted Cone)
3. Порт ограниченного конуса (Port Restricted Cone)
4. Симметричный (Symmetric)

В первых трех типах NATa разные IP-адреса внешней сети могут взаимодействовать с адресом из локальной сети используя один и тот же внешний порт. Четвертый типа, для каждого адреса и порта использует отдельный внешний порт.
NATы не имеют статической таблицы соответствия адресов и портов. Отображение открывается, когда первый пакет посылается из локальной сети наружу через NAT и действует определенный промежуток времени (как правило, 1-3 минуты), если пакеты через этот порт не проходят, то порт удаляется из таблицы соответствия. Обычно NAT распределяют внешние порты динамически, используется диапазон выше 1024.

# Полный конус (Full Cone)

При использовании NATa работающего по типу полного конуса внешний отображаемый порт открыт для пакетов приходящих с любых адресов. Если кто-то из внешнего Интернета хочет в этот момент отправить пакет клиенту, расположенному за НАТом, то ему нужно знать только внешний порт через который установлено соединение. Например, компьютер за NATом с IP-адресом 10.0.0.1 посылает и получает пакеты через порт 8000, отображающийся на внешний IP-адрес и порт 212.23.21.25:12345, то любой в Интернете может послать пакеты на этот 212.23.21.25:12345, и эти пакеты попадут на клиентский компьютер 10.0.0.1:8000.



NAT работающий по типу полного конуса

# Ограниченный конус (Restricted Cone)

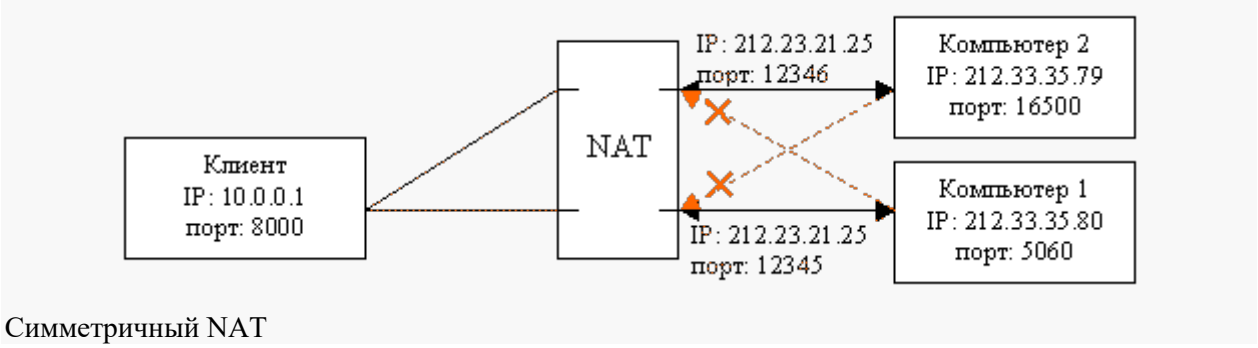
NAT, с ограниченным конусом, открывает внешний порт сразу после того как локальный компьютер отправит данные на определенный внешний IP-адрес. Например, если клиент посылает наружу пакет внешнему компьютеру 1, NAT отображает клиента 10.0.0.1:8000 на 212.23.21.25:12345, и внешний компьютер 1 может посылать пакеты назад по этому назначению. Однако, NAT будет блокировать пакеты идущие от компьютера 2, до тех пор пока клиент не пошлет пакет на IP-адрес этого компьютера. Когда он это сделает, то оба внешних компьютера 1 и 2 смогут посылать пакеты назад клиенту, и оба будут иметь одно и то же отображение через НАТ.

# Порт ограниченного конуса (Port Restricted Cone)

NAT с портом ограниченного конуса почти идентичен NATу с ограниченным конусом. Только в этом случае, NAT блокирует все пакеты, если клиент предварительно не послал наружу пакет на IP-адрес и порт того компьютера, который посылает пакеты клиенту. Поэтому, если клиент посылает внешнему компьютеру 1 на порт 5060, то NAT только тогда пропустит пакет к клиенту, когда он идет с 212.33.35.80:5060. Если клиент послал наружу пакеты к нескольким IP-адресам и портам, то они могут ответить клиенту на один и тот же отображенный IP-адрес и порт.

# Симметричный (Symmetric)

Симметричный NAT кардинально отличается от первых трех в способе отображения внутреннего IP-адреса и порта на внешний адрес и порт. Это отображение зависит от IP-адреса и порта компьютера, которому предназначен посланный пакет. Например, если клиент посылает с адреса 10.0.0.1:8000 компьютеру 1, то он может быть отображен как 212.23.21.25:12345, в тоже время, если он посылает с того же самого порта (10.0.0.1:8000) на другой IP-адрес, он отображается по-другому (212.23.21.25:12346).




Симметричный NAT

Компьютер 1 может отправить ответ только на 212.23.21.25:12345, а компьютер 2 может ответить только на 212.23.21.25:12346. Если любой из них попытается послать пакеты на порт с которого он не получал пакеты, то эти пакеты будут игнорированы. Внешний IP-адрес и порт открывается только тогда, когда внутренний компьютер посылает данные наружу по определенному адресу.

# NAT и Интернет телефония с использованием SIP протокола

Существует три основных проблемы прохождения через NAT звонков с использованием SIP протокола.
1. Наличие локальных адресов в SIP сигнализации.

INVITE sip:81070957877777@212.53.35.244 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.201:5060
From: sip:1234567@tario.ru
To: sip:81070957877777@tario.ru
Contact: sip: 1234567@192.168.1.201:5060
Call-ID: ED9650AC-8054-CF8CCC22FDAD@192.168.1.201
CSeq: 43 INVITE
Content-Type: application/sdp
Content-Length: 228

v=0
o=562003 819348 819348 IN IP4 192.168.1.201
s=X-Lite
c=IN IP4 192.168.1.201
t=0 0
m=audio 8090 RTP/AVP 4 101
a=rtpmap:4 G723/8000
a=rtpmap:101 telephone-event/8000

В приведенном примере сигнализации красным цветом выделены поля, в которых указан локальный адрес. Как следствие этого сервер сети Интернет-телефонии (SoftSwitch) обработав такой запрос, с локальными адресами, не может отправить абоненту ответ, поскольку в поле "Via" указан адрес, который не маршрутизируется в Интернете.

2. Прохождение голосового потока (RTP). Вызываемый абонент, получив вызов от сервера сети Интернет-телефонии, с указанием локального адреса получателя голосового потока не может отправить речевую информацию по назначению, поскольку указанный адрес не маршрутизируется в Интернете. Вследствие этого возникает, одностороння слышимость абонентов или ее полное отсутствие.

3. Абонент, подключенный через NAT, практически не может принимать входящие звонки. Это связанно с тем, что NAT резервирует внешний порт на небольшой промежуток времени (от 1 до 3 мин.), поле чего освобождает его.
Полученный после этого входящий вызов от сервера сети Интернет-телефонии просто игнорируется и как следствие этого абонент расположенный за NATом не может получить информацию о входящем звонке.

# Возможные методы прохождения через NAT

Разные производители предусматривают в своем оборудовании разные способы решения проблемы с прохождения через NAT. Однако все этим методы можно разделить на четыре группы.

# 1. Использование предоставленного IP адреса (Shared IP)

Суть данного метода заключается в том, что на NAT сервере прописывается безусловное перенаправление пакетов приходящих на определенный внешний порт NATa внутреннему IP адресу VoIP устройства. На VoIP устройстве указывается внешний IP адрес NATa, который используется в сигнализации в качестве оригинирующего. Данный метод приемлем для небольших локальных сетей с постоянным внешним IP адресом, использующих небольшое количество VoIP устройств. Его можно использовать вне зависимости от типа NATa. Использование данного метода в больших сетях использующих динамические адреса практически невозможно.
Примеры устройств поддерживающих данный метод.
- Cisco ATA-186
- Grandstream BudgeTone 100
- Asotel Dynamix DW-02 (DW-04)

# 2.UPnP

Данная технология была разработана компанией Microsoft для решения проблем прохождения через NAT. Суть ее заключается в возможности автоматического управления работой NATa. Для подключения с использованием этого необходима поддержка UPnP как VoIP устройством так и самим NATом. Одной из основных проблем при использовании данного подхода является очень ограниченное количество NATов и VoIP устройств поддерживающих данный протокол.
Примеры устройств поддерживающих данный метод.
- PC Phoneline
- Asotel Dynamix
- WellTech
- Windows Messenger 5.0

Примеры NATов поддерживающих UPnP
- Windows XP NAT
- Winroute Pro 5.0

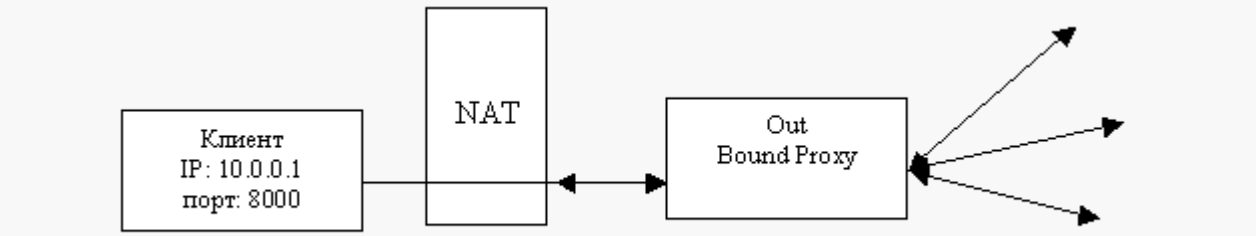
# 3.STUN

Данная технология позволяет обеспечить работу VoIP устройств, которые подключены через конусные NATы. Суть данного метода заключается в том, что VoIP устройство вначале отправляет запрос на STUN сервер, который сообщает текущий внешний адрес и порт, который потом используется в качестве принимающего.
Для обеспечения прохождения входящих звонков VoIP устройство периодически посылает пустые пакеты на адрес сервера маршрутизации сети Интернет телефонии, поддерживая, таким образом, резервирование внешнего порта. Подключение с использованием STUN может использоваться в крупных сетях с использованием динамического распределения адресов.

Примеры устройств поддерживающих данный метод.
- Cisco ATA-186 v3.0 и выше
- Grandstream BudgeTone 100
- SIPURA SPA-2000

# 4. Проксирование на оригинирующий адрес

Данный метод позволяет подключать через NAT практически любое SIP устройство, даже не предусматривающее подключение через NAT. Его можно использовать с любым типом NATa. Суть данного метода заключается в использовании специального пограничного контролера (OutBoundProxy) производящего коррекцию сигнализации и проксирование голосового трафика на оригинирующий адрес. Основным недостатком данного метода является проксирование голосового трафика, что может приводить к дополнительной задержке, если OutBoundProxy находится на значительном расстоянии от клиента.
Для обеспечения прохождения входящих звонков VoIP устройству переодически отсылаются пустые пакеты для поддержки резервирования внешнего порта.
Простейшим примером пограничного контролера может являться SIPOffice.




Проксирование на оригинирующий адрес

# Использованные материалы

1. NAT Traversal in SIP, Baruch Sterman, Ph.D.
2. [1]
3. [2]
4. Network Convergence and the NAT/Firewall Problems, Victor Paulsamy