Типы трансляции сетевых адресов (NAT) и SIP

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.

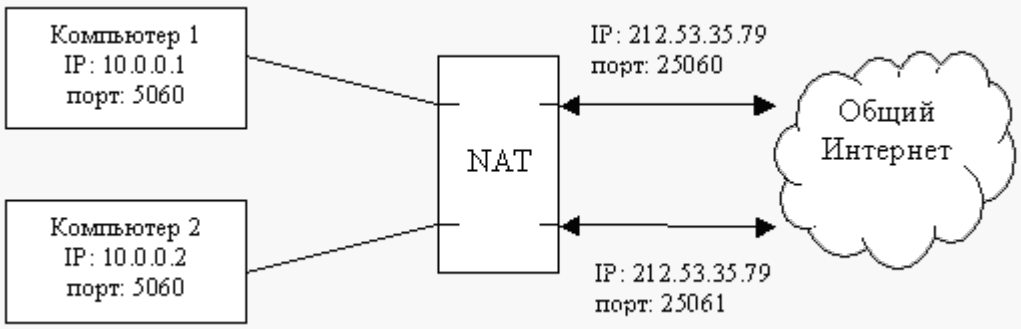


Схема работы NATa

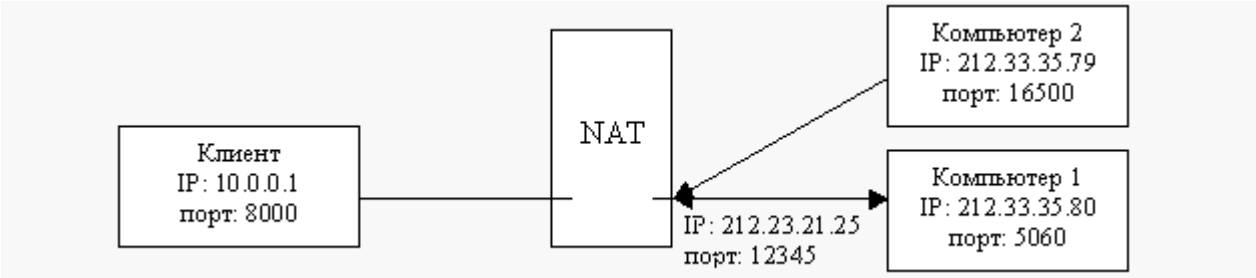
Типы трансляторов сетевых адресов (NAT)

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 NATа 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 NATа 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)

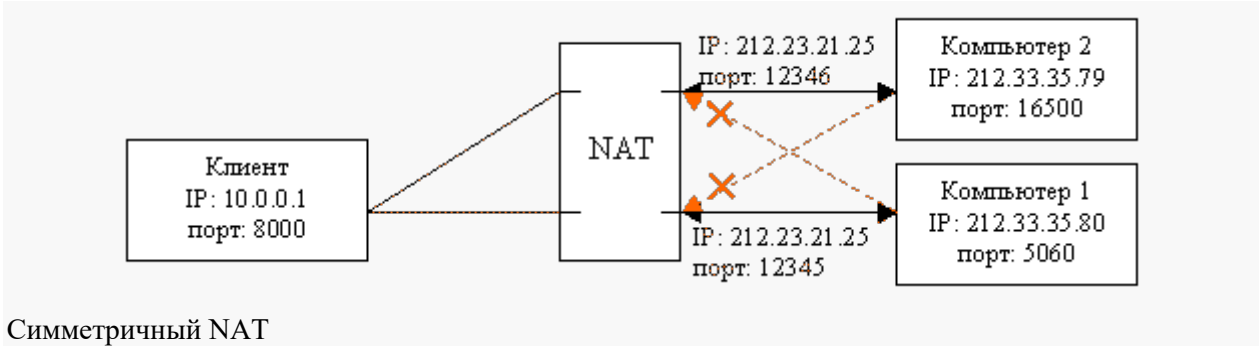
NAT, с ограниченным конусом, открывает внешний порт сразу после того как локальный компьютер отправит данные на определенный внешний IP-адрес. Например, если клиент посылает наружу пакет внешнему компьютеру 1, NAT отображает клиента 10.0.0.1:8000 на 212.23.21.25:12345, и внешний компьютер 1 может посылать 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 ограниченный конус (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.