NAT

NAT (от англ. *Network Address Translation* — «преобразование сетевых адресов») — это механизм в сетях TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов. Также имеет названия *IP Masquerading*, *Network Masquerading* и *Native Address Translation*.

Функционирование

Преобразование адресов методом NAT может производиться почти любым маршрутизирующим устройством — маршрутизатором, сервером доступа, межсетевым экраном. Наиболее популярным является SNAT, суть механизма которого состоит в замене адреса источника (англ. *source*) при прохождении пакета в одну сторону и обратной замене адреса назначения (англ. *destination*) в ответном пакете. Наряду с адресами источник/назначение могут также заменяться номера портов источника и назначения.

Принимая пакет от локального компьютера, роутер смотрит на IP-адрес назначения. Если это локальный адрес, то пакет пересылается другому локальному компьютеру. Если нет, то пакет надо переслать наружу в интернет. Но ведь обратным адресом в пакете указан локальный адрес компьютера, который из интернета будет недоступен. Поэтому роутер «на лету» производит трансляцию IP-адреса и порта и запоминает эту трансляцию у себя во временной таблице. Через некоторое время после того, как клиент и сервер закончат обмениваться пакетами, роутер смотрит у себя в таблице запись о n-ом порте за сроком давности.

Помимо source NAT (предоставления пользователям локальной сети с внутренними адресами доступа к сети Интернет) часто применяется также destination NAT, когда обращения извне транслируются межсетевым экраном на компьютер пользователя в локальной сети, имеющий внутренний адрес и потому недоступный извне сети непосредственно (без NAT).

Существует 3 базовых концепции трансляции адресов: статическая (Static Network Address Translation), динамическая (Dynamic Address Translation), маскарадная (NAPT, NAT Overload, PAT).

Статический NAT — Отображение незарегистрированного IP-адреса на зарегистрированный IP-адрес на основании один к одному. Особенно полезно, когда устройство должно быть доступным снаружи сети.

Динамический NAT — Отображает незарегистрированный IP-адрес на зарегистрированный адрес от группы зарегистрированных IP-адресов. Динамический NAT также устанавливает непосредственное отображение между незарегистрированным и зарегистрированным адресом, но отображение может меняться в зависимости от зарегистрированного адреса, доступного в пуле адресов, во время коммуникации.

Перегруженный NAT (NAPT, NAT Overload, PAT, маскарадинг) — форма динамического NAT, который отображает несколько незарегистрированных адресов в единственный зарегистрированный IP-адрес, используя различные порты. Известен также как PAT (Port Address Translation). При перегрузке каждый компьютер в частной сети транслируется в тот же самый адрес, но с различным номером порта.

Механизм NAT определён в RFC 1631, RFC 3022.

Преимущества

NAT выполняет три важных функции.

1. **Позволяет сэкономить IP-адреса** (только в случае использования NAT в режиме PAT), транслируя несколько внутренних IP-адресов в один внешний публичный IP-адрес (или в несколько, но меньшим количеством, чем внутренних). По такому принципу построено большинство сетей в мире: на небольшой район домашней сети местного провайдера или на офис выделяется 1 публичный (внешний) IP-адрес, за которым работают и получают доступ интерфейсы с приватными (внутренними) IP-адресами.

2. Позволяет предотвратить или ограничить обращение снаружи ко внутренним хостам, оставляя возможность обращения изнутри наружу. При инициации соединения изнутри сети создаётся трансляция. Ответные пакеты, поступающие снаружи, соответствуют созданной трансляции и поэтому пропускаются. Если для пакетов, поступающих снаружи, соответствующей трансляции не существует (а она может быть созданной при инициации соединения или статической), они не пропускаются.
3. Позволяет скрыть определённые внутренние сервисы внутренних хостов/серверов. По сути, выполняется та же указанная выше трансляция на определённый порт, но возможно подменить внутренний порт официально зарегистрированной службы (например, 80-й порт TCP (HTTP-сервер) на внешний 54055-й). Тем самым, снаружи, на внешнем IP-адресе после трансляции адресов на сайт (или форум) для осведомлённых посетителей можно будет попасть по адресу http://example.org:54055, но на внутреннем сервере, находящемся за NAT, он будет работать на обычном 80-м порту. Повышение безопасности и скрытие «непубличных» ресурсов.

Недостатки

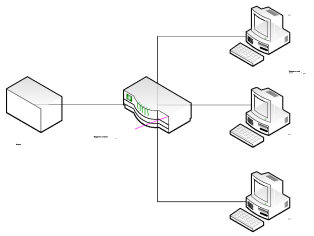
1. Не все протоколы могут «преодолеть» NAT. Некоторые не в состоянии работать, если на пути между взаимодействующими хостами есть трансляция адресов. Некоторые межсетевые экраны, осуществляющие трансляцию IP-адресов, могут исправить этот недостаток, соответствующим образом заменяя IP-адреса не только в заголовках IP, но и на более высоких уровнях (например, в командах протокола FTP). См. Application-level gateway.
2. Из-за трансляции адресов «много в один» появляются дополнительные сложности с идентификацией пользователей и необходимость хранить полные логи трансляций.
3. DoS со стороны узла, осуществляющего NAT — если NAT используется для подключения многих пользователей к одному и тому же сервису, это может вызвать иллюзию DoS-атаки на сервис (множество успешных и неуспешных попыток). Например, избыточное количество пользователей ICQ за NAT приводит к проблеме с подключением к серверу некоторых пользователей из-за превышения допустимой скорости подключений. Частичным решением проблемы является использование *пула адресов* (группы адресов), для которых осуществляется трансляция.
4. В некоторых случаях, необходимость в дополнительной настройке (см. Трансляция порт-адрес) при работе с пиринговыми сетями и некоторыми другими программами, в которых необходимо не только инициировать исходящие соединения, но также принимать входящие. Однако, если NAT-устройство и ПО, требующее дополнительной настройки, поддерживают технологию Universal Plug & Play, то в этом случае настройка произойдет полностью автоматически и прозрачно для пользователя.

Пример

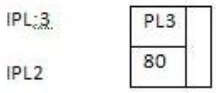
Трансляция локальной сети с диапазоном адресов 172.17.14.0/24 в глобальную сеть будет осуществляться через один внешний IP-адрес (адрес маршрутизатора, выполняющего трансляцию).

Применение

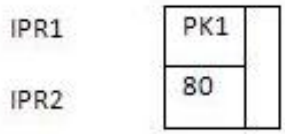
- Для обеспечения доступа множества узлов во внешнюю IP сеть через единственный IP-адрес

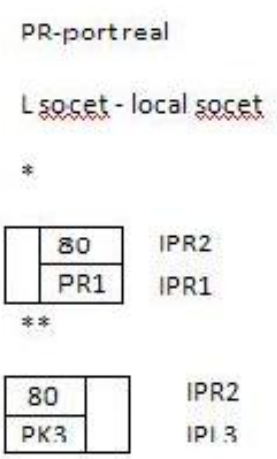


- На рабочих станциях указанный шлюз по умолчанию или gateway



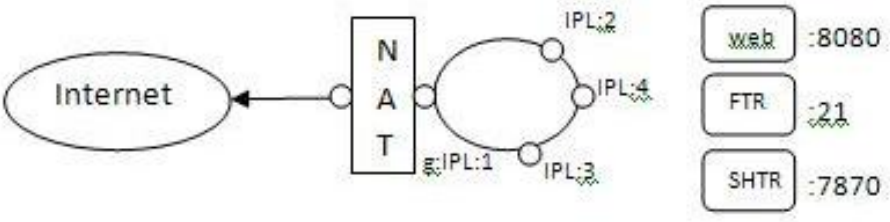
- Преобразует служебные заголовки, формирует идентичный IP-пакет

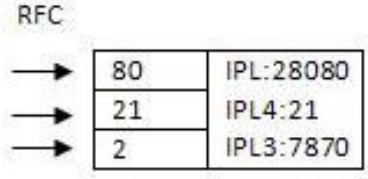




Если подменим Socet, то знаем кому отвечать, а если подменим только IP, то не знаем кому

- Публикация локальных ресурсов во внешней IP-сети





только

не FTR, а FTP и не SHTR а SHTP

• Экономическая выгода вследствие приобретения единственного IP-подключения, а не IP-сети.

• Сокрытие от внешнего наблюдателя структуры внутренней IP-сети.

• Организация системы с распределенной нагрузкой.

• При общем доступе через NAT прозрачно открывается доступ к внутренней структуре с защитой без использования межсетевого экрана и т. п.

• Через NAT корректно работают многие сетевые протоколы. Конструктивные реализации (общий доступ — это и есть подключение NAT) есть аппаратная реализация NAT (интегрированы межсетевые экраны).

NAT Traversal

NAT Traversal (прохождение или автонастройка NAT) — это набор возможностей, позволяющих сетевым приложениям определять, что они находятся за устройством, обеспечивающим NAT, узнавать внешний IP-адрес этого устройства и выполнять сопоставление портов для пересылки пакетов из внешнего порта NAT на внутренний порт, используемый приложением; все это выполняется автоматически, пользователю нет необходимости вручную настраивать сопоставления портов или вносить изменения в какие-либо другие параметры. Однако существуют меры предосторожности в доверии к таким приложениям — они получают обширный контроль над устройством, появляются потенциальные уязвимости.

Операционные системы с поддержкой NAT

При недостаточном финансировании, либо при наличии уже существующего сервера под управлением серверной ОС возможно организовать трансляцию адресов без необходимости закупки дополнительных устройств. В таком случае, оптимальным будет наличие по крайней мере двух сетевых адаптеров в сервере (возможны варианты с одним, но при наличии trunk-VLAN).

Все существующие и использующиеся серверные ОС поддерживают простейшую трансляцию адресов.

С точки зрения же отказоустойчивости, гибкости и производительности, используются операционные системы UNIX (большинство GNU/Linux, *BSD-системы, а также OpenSolaris и др.). Во многих из них NAT доступен «из коробки», в других возможна реализация за счёт добавления модулей в сочетании с межсетевыми экранами с функциями трансляции адресов (IPFW, IPtables и др.). 00

Ссылки

- Типы Network Address Translation (NAT) [1]

Примечания

[1] http://aoz.com.ua/2009/01/26/nat-types/

Источники и основные авторы

NAT *Источник*: http://ru.wikipedia.org/w/index.php?oldid=49565599 *Редакторы*: APTEM, Alex Smotrov, Alex.ryazantsev, Ambience8, AndrewZhukov, Andrey Olegovich, Dagon, Exlex, George Shuklin, Grain, Gromolyak, Gul, Imaginary, Inity, Kaputt, Kink, KleverI, Knyf, MaGIc2laNTern, Maickellz, Mashiah Davidson, Mercury, Nikolay Nikolaevich Fedotov, Omerta13, Pupkinson, Roxis, Roygbiv, SPKirsch, Shotik, Skor, Snch, Softy, Transgressor, Tucvbif, Vadim68 ferenets, Vanderpool, Vasiliy Faronov, Vlad2000Plus, Voidus, WikiCle, Winterheart, Zul, ~obsidian, Алексей Шиянов, Басманов Даниил, Менязовут, Нирваньчик, Сергей Прохоренко, 99 анонимных правок

Источники, лицензии и редакторы изображений

Файл:NAT.svg *Источник*: http://ru.wikipedia.org/w/index.php?title=Файл:NAT.svg *Лицензия*: Creative Commons Attribution-Sharealike 3.0 *Редакторы*: Алексей Шиянов

Файл:Gateway.JPG *Источник*: http://ru.wikipedia.org/w/index.php?title=Файл:Gateway.JPG *Лицензия*: Public Domain *Редакторы*: Shotik, 1 анонимных правок

Файл:Ip-paket.JPG *Источник*: http://ru.wikipedia.org/w/index.php?title=Файл:Ip-paket.JPG *Лицензия*: Public Domain *Редакторы*: Shotik, 1 анонимных правок

Файл:Ip-set.JPG *Источник*: http://ru.wikipedia.org/w/index.php?title=Файл:Ip-set.JPG *Лицензия*: Public Domain *Редакторы*: Shotik, 1 анонимных правок

Лицензия