Как работает NAT

Автор: HunSolo от 1-07-2013, 15:35, посмотрело: 25028

Если Вы читаете этот документ, то скорее всего вы подсоединены к Интернету, и используете трансляцию сетевых адресов (**Network Address Translation, NAT**) прямо сейчас! Интернет стал настолько огромным, чем кто-либо мог себе представить. Хотя точный размер неизвестен, текущая оценка это приблизительно 100 миллионов хостов и более чем 350 миллионов пользователей, активно работающих в Интернете. Фактически, норма роста такова, что Интернет эффективно удваивается в размере каждый год.

Введение

Для компьютера, чтобы общаться с другими компьютерами и Web-серверами в Интернете, он должен иметь IP адрес. IP адрес (IP означает Интернет Протокол) - это уникальное 32-битовое число, которое идентифицирует местоположение вашего компьютера на сети. В основном это работает точно так же как ваш уличный адрес: способ точно выяснить, где вы находитесь и доставить вам информацию. Теоретически, можно иметь 4,294,967,296 уникальных адресов (2^32). Фактическое число доступных адресов является меньшим (где-нибудь между 3.2 и 3.3 миллиарда) из-за способа, которым адреса разделены на классы и потребности отвести некоторые из адресов для мультивещания, тестирования или других определенных нужд. С увеличением домашних сетей и деловых сетей, число доступных IP адресов уже не достаточно. Очевидное решение состоит в том, чтобы перепроектировать формат адреса, чтобы учесть больше возможных адресов. Таким образом, развивается протокол IPv6, но, это развитие займет несколько лет, потому что требует модификации всей инфраструктуры Интернета.

Вот где приходит NAT нам во спасение. В основном, Сетевая Трансляция Адресов, позволяет единственному устройству, типа маршрутизатора, действовать как агент между Интернетом (или "публичной сетью") и локальной (или "частной") сетью. Это означает, что требуется только единственный уникальный IP адрес, чтобы представлять всю группу компьютеров чему-либо вне их сети. Нехватка IP адресов - только одна причина использовать NAT. Два других серьезных основания это безопасность и администрирование

Вы узнаете о том, как можно извлечь выгоду из NAT, но сначала, давайте познакомимся с NAT чуть ближе и посмотрим, что он может делать.

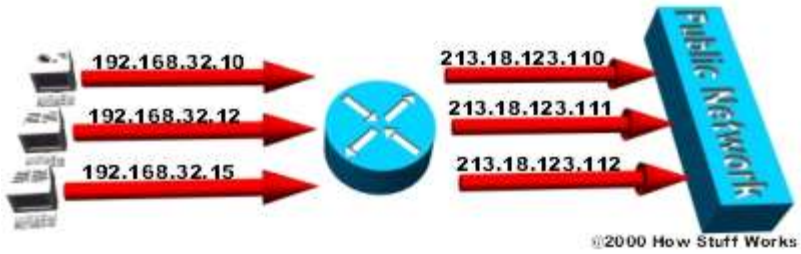
Маскировка

NAT похож на секретаря большого офиса. Скажем, вы оставили инструкции секретарю, чтобы не перенаправлять вам никакие звонки, до тех пор, пока вы не попросите об этом. Позже, вы звоните потенциальному клиенту и оставляете сообщение для него, чтобы он перезвонил вам. Вы говорите секретарю, что ожидаете звонок от этого клиента и звонок нужно перевести. Клиент звонит на основной номер вашего офиса, являющийся единственным номером, который он знает. Когда клиент говорит секретарю, кого он ищет, секретарь проверяет свой список сотрудников, чтобы найти соответствие имени и его номера расширения. Секретарь знает, что вы запрашивали этот звонок, поэтому он переводит звонившего на ваш телефон.

Разработанная технология Cisco, Трансляция Сетевых Адресов используется устройством (межсетевым экраном, маршрутизатором или компьютером), которое находиться между внутренней сетью и остальной частью мира. NAT имеет много форм и может работать несколькими способами:

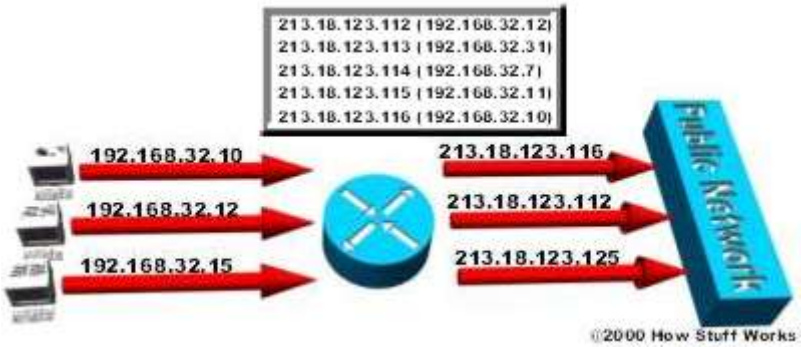
Статический NAT - Отображение незарегистрированного IP адреса на зарегистрированный IP адрес на основании один к одному. Особенно полезно, когда устройство должно быть доступным снаружи сети.

В статическом NAT, компьютер с адресом 192.168.32.10 будет всегда транслироваться в адрес 213.18.123.110:



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.

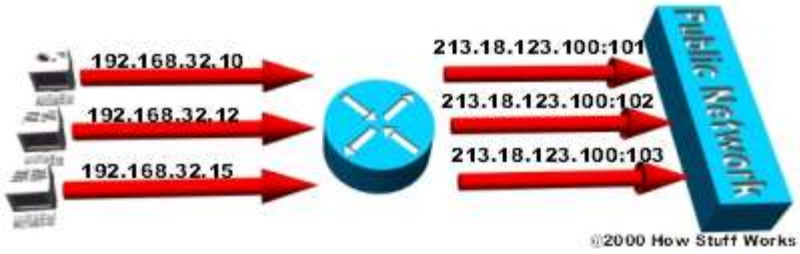
В динамическом NAT, компьютер с адресом 192.168.32.10 транслируется в первый доступномый адрес в диапазоне от 213.18.123.100 до 213.18.123.150



Перегрузка(Overload) - форма динамического NAT, который отображает несколько

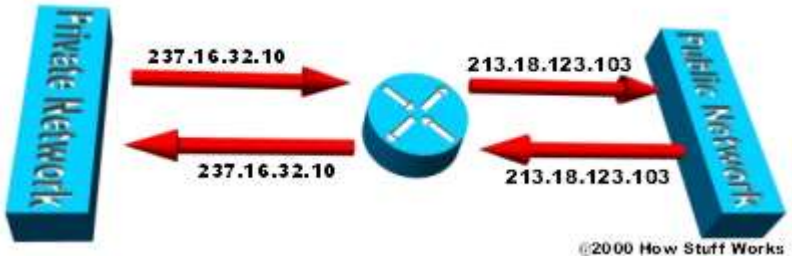
незарегистрированных адресов в единственный зарегистрированный IP адрес, используя различные порты. Известен также как PAT (Port Address Translation)

При перегрузке, каждый компьютер в частной сети транслируется в тот же самый адрес (213.18.123.100), но с различным номером порта



Перекрытие - Когда IP адреса, используемые в вашей внутренней сети, также используются в другой сети, маршрутизатор должен держать таблицу поиска этих адресов так, чтобы он мог перехватить и заменить их зарегистрированными уникальными IP адресами. Важно отметить, что NAT маршрутизатор должен транслировать "внутренние" адреса в зарегистрированные уникальные адреса, а также должен транслировать "внешние" зарегистрированные адреса в адреса, которые являются уникальными для частной сети. Это может быть сделано либо через статический NAT, либо вы можете использовать DNS и реализовать динамический NAT.

Пример:
Внутренний диапазон IP (237.16.32.xx) является также зарегистрированный диапазоном, используемым другой сетью. Поэтому, маршрутизатор транслирует адреса, чтобы избежать потенциального конфликта . Он также будет транслировать зарегистрированные глобальные IP адреса обратно к незарегистрированным локальным адресам , когда пакеты посылаются во внутреннюю сеть

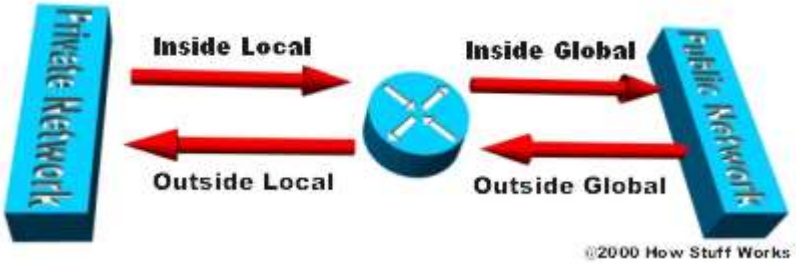


Внутренняя сеть – это обычно LAN (Локальная сеть), чаще всего, называемая, *тупиковым доменом*. Тупиковый домен это LAN, которая использует внутренние IP адреса. Большинство сетевого трафика в таком домене является локальным, он не покидает пределов внутренней сети. Домен может включать как зарегистрированные так и незарегистрированные IP адреса. Конечно, любые компьютеры, которые используют незарегистрированные IP адреса, должны использовать NAT, чтобы общаться с остальной частью мира.

NAT может быть сконфигурирован различными способами. В примере ниже NAT-маршрутизатор сконфигурирован так, чтобы транслировать незарегистрированные IP адреса (локальные внутренние адреса), которые постоянно находятся в приватной (внутренней) сети в зарегистрированные IP адреса. Это случается всякий раз, когда устройство на внутренней части с незарегистрированным адресом должно общаться с внешней сетью.

ISP назначает диапазон адресов IP вашей компании. Назначенный блок адресов - это уникальные зарегистрированные IP адреса и называются **внутренними глобальными адресами (inside global)**. Незарегистрированные частные IP адреса разбиты на две группы, маленькая группа, **внешние локальные адреса (outside local)**, будет использоваться NAT маршрутизаторами и основная, которая будет использоваться в домене, известна как **внутренние локальные адреса (inside local)**. Внешние локальные адреса используются, чтобы транслировать уникальные IP адреса, известные как **внешние глобальные адреса(outside global)**, устройств на общественной сети.
NAT транслирует только тот трафик, который проходит между внутренней и внешней сетью и определен для трансляции. Любой трафик, не соответствующий критериям трансляции или тот, который проходит между другими интерфейсами на маршрутизаторе, никогда не транслируется, и пересылается как есть.

IP адреса имеют различные обозначения, основанные на том, находятся ли они на частной сети (домен) или на общественной сети (Интернет) и является ли трафик входящим или исходящим:



- Большинство компьютеров в домене общается друг с другом, используя внутренние локальные адреса.
- Некоторые компьютеры в домене взаимодействуют с внешней сетью. Эти компьютеры имеют внутренние глобальные адреса, что означает, что они не требуют трансляции.
- Когда компьютер в домене, который имеет внутренний локальный адрес, хочет взаимодействовать с внешней сетью, пакет идет в один из NAT-маршрутизаторов посредством обычной маршрутизации.
- NAT- маршрутизатор проверяет таблицу маршрутизации, чтобы посмотреть, имеется ли у него запись для конечного адреса. Если адрес приемника не находится в таблице маршрутизации, пакет отбрасывается. Если запись доступна, роутер проверяет, идет ли пакет из внутренней сети во внешнюю, а также, соответствует ли пакет критериям, определенным для трансляции. Затем маршрутизатор проверяет таблицу трансляции адресов, чтобы выяснить, существует ли запись для внутреннего локального адреса и соответствующего ему внутреннего глобального адреса. Если запись найдена, он транслирует пакет, используя внутренний глобальный адрес. Если сконфигурирован только статический NAT, и никакой записи не найдено, то роутер посылает пакет без трансляции.
- Используя внутренний глобальный адрес, маршрутизатор пересылает пакет его адресату.

- компьютер на общественной сети посылает пакет в частную сеть. Адрес источника в пакете – это внешний глобальный адрес. Адрес приемника - внутренний глобальный адрес.
- Когда пакет прибывает во внешнюю сеть, NAT-маршрутизатор смотрит в таблицу трансляций и определяет адрес приемника, отображенный на компьютер в домене.
- NAT-маршрутизатор транслирует внутренний глобальный адрес пакета на внутренний локальный адрес и затем проверяет таблицу маршрутизации прежде, чем пошлет пакет конечному компьютеру. Всякий раз, когда запись не найден для адреса в таблице трансляций, пакет не транслируется и роутер продолжает поверку таблицы маршрутизации на поиск адреса приемника.

NAT-перегрузка (overloading) использует особенность стека протокола TCP/IP, такую как мультиплексирование, которое позволяет компьютеру поддерживать несколько параллельных подключений с удаленным компьютером, используя различные TCP или UDP порты. Пакет IP имеет заголовок, который содержит следующую информацию:

- Исходный адрес – IP адрес компьютера источника, например, 201.3.83.132.
- Исходный порт – номер TCP или UDP порта, назначенное компьютером источником для этого пакета, например, Порт 1080.
- Адрес назначения – IP адрес компьютера приемника. Например, 145.51.18.223.
- Порт назначения – номер TCP или UDP порта, который просит открыть компьютер источник на приемнике, например, порт 3021.

IP адреса определяют две машины с каждой стороны, в то время как номера портов гарантируют, что соединение между этими двумя компьютерами имеет уникальный идентификатор. Комбинация этих четырех чисел определяет единственное соединение TCP/IP. Каждый номер порта использует 16 битов, что означает, что сушествует 65 536 (2^16) возможных значения. В действительности, так как различные изготовители отображают порты немного различными способами, вы можете ожидать приблизительно 4 000 доступных портов.

Примеры динамического NAT и NAT с перегрузкой