Как работает преобразование NAT

Данный документ содержит флэш-анимацию.

Содержание

Общие сведения

Если вы читаете данный документ, то, скорее всего, вы подключены к Интернету и весьма велика вероятность того, что вы используете **преобразование сетевых адресов (NAT)** непосредственно сейчас.

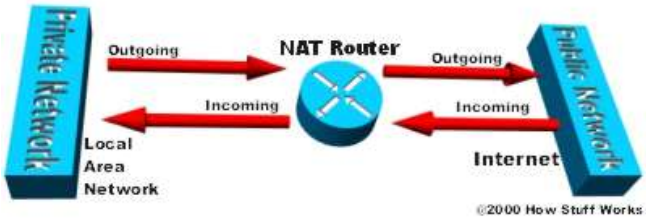
Интернет разросся до таких размеров, о которых никто и не предполагал. Несмотря на то, что точный размер его неизвестен, согласно текущим оценкам в Интернете в активном состоянии находится около 100 миллионов хостов и более 350 миллионов пользователей. Это больше, чем все население США! Фактически скорость расширения такова, что ежегодно размер Интернета удваивается.

А какое отношение NAT имеет к размеру Интернет? Самое непосредственное! Чтобы компьютер мог обмениваться информацией с другими компьютерами и веб-серверами в Интернет, у него должен быть **IP-адрес**. IP-адрес (IP расшифровывается как "протокол Интернета", англ. - "Internet Protocol") представляет собой уникальное 32-битовое число, которое указывает на расположение вашего компьютера в сети. В основном он используется так же, как адрес вашей улицы: это способ определения вашего точного местоположения для отправки вам данных.

Когда IP-адреса только появились, то все думали, что адресов достаточно для удовлетворения любых потребностей. Теоретически можно использовать 4 294 967 296 уникальных адресов (2^{32}). Реально доступно меньше адресов (в диапазоне от 3,2 до 3,3 миллиардов). Их число ограничивается следующими факторами: способом разделения адресов на классы и необходимостью резервировать некоторые адреса для многоадресной передачи, тестирования или иных целей.

Из-за стремительного расширения использования Интернета и увеличением домашних и коммерческих сетей, количества доступных IP-адресов стало просто не хватать. Очевидное решение – переделать формат адреса так, чтобы появилась возможность использования большего количества адресов. Работа над этой проблемой идет (**IPv6**), но реализация решения займет как минимум несколько лет, поскольку для этого требуется изменить всю инфраструктуру Интернета.

Маршрутизатор NAT преобразует трафик, входящий в частную сеть и покидающий ее.



Вот где большую пользу оказывает преобразование NAT (RFC 1631). В основном преобразование сетевых адресов позволяет одному устройству, например, маршрутизатору, выступать в качестве агента между Интернетом ("сетью общего пользования") и локальной (или "частной") сетью. Это означает, что для представления всей группы компьютеров кому-либо находящемуся за пределами этой сети требуется только один уникальный IP-адрес.

Нехватка IP-адресов является только одной из причин для использования NAT. Есть еще две веских причины:

- Безопасность;
- Администрирование.

Вы узнаете больше о том, как получить преимущества от использования NAT, но сначала давайте рассмотрим NAT и его возможности ближе…

Предварительные условия

Требования

Для понимания данного документа требуется наличие следующих знаний:

- Принципы IP-адресации и маршрутизации.

Используемые компоненты

Данный документ не ограничен отдельными версиями программного и аппаратного обеспечения.

Условные обозначения

Дополнительные сведения об условных обозначениях в документах см. в документе "Технические рекомендации Cisco. Условные обозначения".

Что скрывается за маской

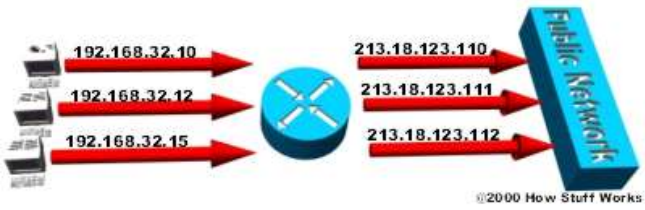
NAT похоже на секретаря в большом офисе. Предположим, секретарь получил указания переадресовать вам звонки только по вашему требованию. Позже вы звоните потенциальному клиенту и оставляете ему сообщение о том, чтобы он вам перезвонил. Вы сообщаете секретарю, что ожидается звонок от данного клиента, с которым вас следует соединить.

Клиент набирает общий номер офиса, поскольку клиент знает только этот номер. Когда клиент сообщает секретарю имя разыскиваемого человека, секретарь просматривает таблицу поиска, которая содержит имя человека и дополнительный номер. Секретарь знает, что этот вызов был запрошен, поэтому он переадресует звонящего на ваш дополнительный номер.

Технология преобразования сетевых адресов, разработанная Cisco, используется в устройстве (брандмауэре, маршрутизаторе или компьютере), который находится между внутренней сетью и остальным миром. Механизм преобразования NAT представлен в различных формах и может работать несколькими способами:

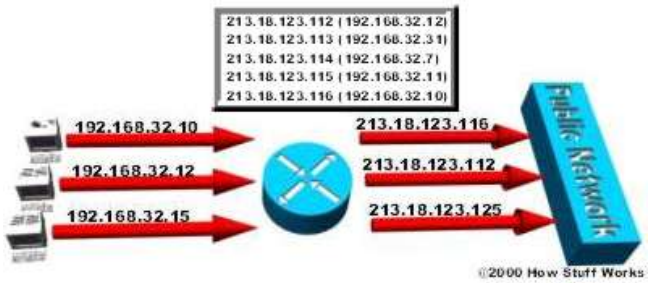
- **Статическое NAT** – сопоставление незарегистрированного IP-адреса зарегистрированному IP-адресу как один к одному. Это особенно полезно, когда необходимо предоставить доступ к устройству из-за пределов сети.

  В статическом NAT IP-адрес 192.168.32.10 компьютера всегда будет преобразовываться в 213.18.123.110:



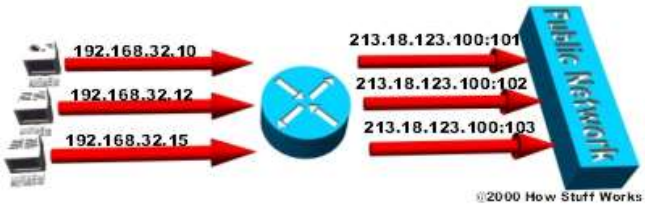
- **Динамическое NAT** – сопоставление незарегистрированного IP-адреса зарегистрированному IP-адресу из группы зарегистрированных адресов. Динамическое NAT также устанавливает соответствие "один к одному" между незарегистрированным и зарегистрированным IP-адресами, однако сопоставление может меняться в зависимости от доступности зарегистрированных адресов в пуле во время обмена информацией.

  В динамическом NAT IP-адрес 192.168.32.10 будет преобразовываться в первый доступный адрес из диапазона от 213.18.123.100 до 213.18.123.150:



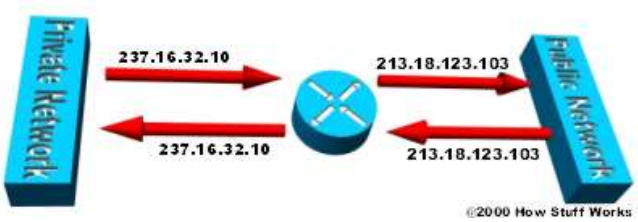
- **Перегрузка** – форма динамического NAT, когда несколько незарегистрированных IP-адресов сопоставляются одному IP-адресу посредством использования различных портов. Также известно как PAT (преобразование портов в адреса), одноадресное NAT или NAT с мультиплексированием по портам.

  При перегрузке адрес каждого компьютера частной сети преобразуется в один и тот же IP-адрес (213.18.123.100), но с назначением различных номеров портов:



- **Наложение** – когда IP-адреса, используемые во внутренней сети, являются зарегистрированными IP-адресами, используемыми в другой сети, маршрутизатор должен хранить таблицу подстановки этих адресов, чтобы он мог их перехватывать и заменять на зарегистрированные уникальные IP-адреса. Важно отметить, что маршрутизатор NAT должен преобразовывать "внутренние" адреса в зарегистрированные уникальные адреса, а также должен преобразовывать "внешние" зарегистрированные адреса в адреса, уникальные для частной сети. Это можно сделать либо с использованием статического NAT, либо с использованием DNS и реализацией динамического NAT.

  Внутренний диапазон IP-адресов (237.16.32.xx) также является зарегистрированным диапазоном, используемым другой сетью. Поэтому маршрутизаторы преобразуют адреса во избежание потенциальных конфликтов с другой сетью. Когда информация передается во внутреннюю сеть, он также преобразует зарегистрированные глобальные IP-адреса обратно в незарегистрированные локальные IP-адреса.

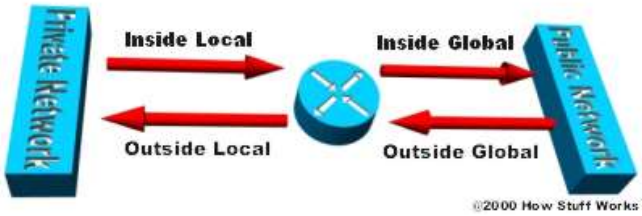


Обычно внутренней сетью является **ЛВС (локальная вычислительная сеть)**, часто называемая **тупиковым доменом**. Тупиковый домен представляет собой ЛВС, IP-адреса внутри которой используются внутренним образом. Большинство сетевого трафика тупикового домена является локальным, он не выходит за пределы внутренней сети. Тупиковый домен может содержать как зарегистрированные, так и незарегистрированные IP-адреса. Естественно, для связи с остальным миром все компьютеры, использующие незарегистрированные IP-адреса, должны использовать преобразование сетевых адресов.

Преобразование NAT можно настроить различными способами. В примере ниже маршрутизатор NAT настроен на преобразование незарегистрированных IP-адресов (среди локальных адресов), которые находятся в частной (внутренней) сети, в зарегистрированные IP-адреса. Это происходит всякий раз, когда устройству с незарегистрированным адресом, находящемуся внутри, необходимо осуществить обмен информацией с сетью (внешней) общего пользования.

- ISP назначает вашей компании диапазон IP-адресов. Назначенный блок адресов представляет собой зарегистрированные уникальные IP-адреса и называется **внутренними глобальными адресами**. Незарегистрированные частные IP-адреса разбиты на две группы: маленькая группа (**внешние локальные адреса**), которая будет использоваться маршрутизаторами NAT, и большая группа, которая будет использоваться в тупиковом домене, известная как **внутренние локальные адреса**. Внешние локальные адреса используются для преобразования уникальных IP-адресов, известных как **внешние глобальные адреса**, устройств сети общего пользования. Дополнительные сведения по определениям глобальных и локальных адресов см. в документе NAT: определения терминов локальный и глобальный. NAT преобразует только трафик, который проходит между внутренней и внешней сетью и указывается как подлежащий преобразованию. Любой трафик, не соответствующий критериям преобразования или трафик, пересылаемый между другими интерфейсами маршрутизатора, никогда не преобразуется, поскольку он и так пересылается.

  IP-адреса обозначаются по-разному. Это зависит от того, находятся они в частной сети (в тупиковом домене) или в сети общего пользования (Интернет), а также от типа трафика, входящего или исходящего:



- Большинство компьютеров тупикового домена обмениваются друг с другом информацией при помощи локальных адресов.
- Некоторые из компьютеров тупикового домена обмениваются большим количеством информации с внешней сетью. Эти компьютеры имеют внутренние глобальные адреса, поэтому им преобразование не требуется.
- Когда компьютеру в домене частной сети, имеющий внутренний локальный адрес, необходим обмен данными с компьютером, находящимся за пределами сети, пакеты передаются маршрутизаторам NAT посредством обычной маршрутизации к шлюзу по умолчанию.
- Маршрутизатор NAT проверяет, есть ли в таблице маршрутизации запись для адреса места назначения. Если адрес места назначения отсутствует в таблице маршрутизации, пакет сбрасывается. Если запись есть, маршрутизатор проверяет, идет ли пакет из внутренней сети во внешнюю, а также проверяет, соответствует ли пакет критериям, заданным для преобразования. Затем маршрутизатор проверяет таблицу преобразования адресов, чтобы проверить наличие записи для внутреннего локального адреса со связанным внутренним глобальным адресом. Если запись найдена, он преобразует пакет с использованием внутреннего глобального адреса. Если настроена только статическое NAT и запись не найдена, оно пересылает пакет без преобразования.
- Используя внутренний глобальный адрес, маршрутизатор посылает пакет на адрес места назначения.
- Компьютер сети общего пользования посылает пакет в частную сеть. Адрес источника пакета является внешним глобальным адресом. Адрес места назначения является внутренним глобальным адресом.
- Когда пакет поступает во внешнюю сеть, маршрутизатор NAT по таблице преобразования адресов определяет наличие адреса места назначения, сопоставленного с компьютером тупикового домена.
- Маршрутизатор NAT преобразует внутренний глобальный адрес пакета во внутренний локальный адрес, после чего проверяет таблицу маршрутизации перед тем, как отправить пакет на компьютер места назначения. Когда запись для адреса не найдена в таблице преобразования, он не преобразуется, а выполняется проверка наличия адреса места назначения в таблице маршрутизации. Пакет сбрасывается, если в таблице маршрутизации не удалось найти маршрут до адреса места назначения.

Дополнительную информацию по порядку обработки транзакций при помощи NAT см. в документе Порядок работы NAT.

При перегрузке NAT используется функция стека протоколов TCP/IP, которая называется мультиплексированием. Она позволяет компьютеру одновременно поддерживать несколько соединений с удаленными компьютерами при помощи разных портов TCP или UDP. Заголовок IP-пакета содержит следующую информацию:

- Адрес источника — IP-адрес компьютера-источника, например, 201.3.83.132;
- Порт источника — номер порта TCP или UDP, назначенный компьютером, создавшим данный пакет, например, порт 1080;
- Адрес места назначения — IP-адрес компьютера-получателя, например, 145.51.18.223;
- Порт места назначения — номер порта TCP или UDP, открытие которого на компьютере-получателе запрашивает компьютер-источник, например, порт 3021.

С помощью этих адресов указываются оба компьютера, участвующих в соединении, в то время как номера портов обеспечивают уникальность идентификатора для соединения между двумя компьютерами. Комбинация этих четырех цифр определяет одно TCP/IP-соединение. Для каждого номера порта используется 16 битов, что означает 65 536 (2^{16}) возможных значений. В действительности, поскольку разные производители распределяют порты различными способами, можно ожидать наличия около 4 000 доступных портов.

Динамическое преобразование сетевых адресов и примеры перегрузки

Флэш-анимация: динамическое преобразование сетевых адресов (NAT)

Принцип работы динамического NAT:

Перейдите к  флэш-анимации динамического NAT и нажмите на одну из зеленых кнопок, чтобы успешно отправить пакет в тупиковый домен или из него. Чтобы отправить пакет, который маршрутизатор сбросит вследствие неправильного адреса, нажмите одну из красных кнопок.

- Внутренняя сеть (тупиковый домен) настроен с использованием IP-адресов, которые не были специально выделены этой компании **IANA (Организация по назначению номеров Интернет)**, глобальной организацией, назначающей IP-адреса. Эти адреса должны считаться **немаршрутизируемыми**, поскольку они не являются уникальными. Они являются внутренними локальными адресами.
- Компания устанавливает маршрутизатор с включенным преобразованием сетевых адресов. Маршрутизатор использует диапазон уникальных IP-адресов, которые IANA назначает компании. Эти адреса являются внутренними глобальными.
- Компьютер тупикового домена предпринимает попытку подключения к компьютеру, находящемуся за пределами сети, например, к веб-серверу.
- Маршрутизатор получает пакет от компьютера тупикового домена.
- После проверки таблицы маршрутизации и процесса проверки для выполнения преобразования, маршрутизатор сохраняет немаршрутизируемый IP-адрес компьютера в **таблице преобразования адресов**. Маршрутизатор заменяет немаршрутизируемый IP-адрес компьютера-отправителя первым доступным IP-адресом, из диапазона уникальных IP-адресов. Теперь в таблице преобразования содержится запись, устанавливающая соответствие немаршрутизируемого IP-адреса компьютера и одного из уникальных IP-адресов.
- После возвращения пакета от компьютера-адресата маршрутизатор проверяет адрес места назначения в пакете. После он проверяет таблицу преобразования адресов, чтобы узнать, какому компьютеру тупикового домена принадлежит пакет. Он заменяет адрес назначения на адрес, хранящийся в таблице преобразования адресов, и отправляет пакет этому компьютеру. Если соответствующий адрес в таблице отсутствует, маршрутизатор сбрасывает пакет.
- Компьютер получает пакет от маршрутизатора, и процесс повторяется, пока компьютер обменивается данными с внешней системой.

Принцип работы перегрузки:

- Внутренняя сеть (тупиковый домен) был настроен с использованием немаршрутизируемых IP-адресов, которые не были специально назначены IANA этой компании.
- Компания устанавливает маршрутизатор с включенным преобразованием сетевых адресов. Маршрутизатор использует уникальный IP-адрес, который IANA назначает компании.
- Компьютер тупикового домена предпринимает попытку подключения к компьютеру, находящемуся за пределами сети, например, к веб-серверу.
- Маршрутизатор получает пакет от компьютера тупикового домена.
- После маршрутизации и процесса проверки для выполнения преобразования, маршрутизатор сохраняет немаршрутизируемый IP-адрес компьютера и номер порта в таблице преобразования адресов. Маршрутизатор заменяет немаршрутизируемый IP-адрес компьютера-отправителя IP-адресом маршрутизатора. Маршрутизатор заменяет исходный порт отправителя на номер порта, который совпадает с записью, в которой маршрутизатор сохранил адресную информацию отправителя в таблице преобразования адресов. Теперь в таблице преобразования содержится запись, устанавливающая соответствие немаршрутизируемого IP-адреса компьютера и номера порта с IP-адресом маршрутизатора.
- После возвращения пакета от компьютера-адресата маршрутизатор проверяет порт места назначения в пакете. После он проверяет таблицу преобразования адресов, чтобы узнать, какому компьютеру тупикового домена принадлежит пакет. Он заменяет адрес назначения и порт назначения на адрес и порт, хранящиеся в таблице преобразования адресов, и отправляет пакет этому компьютеру.
- Компьютер получает пакет от маршрутизатора, и процесс повторяется, пока компьютер обменивается данными с внешней системой.
- Поскольку теперь у маршрутизатора NAT исходный адрес компьютера и исходный порт сохранен в таблице преобразования адресов, маршрутизатор будет продолжать использовать этот самый номер порта в течение времени подключения. Таймер сбрасывается при каждом доступе маршрутизатора к записи в таблице. Если до истечения таймера доступ к записи не осуществляется, запись удаляется из таблицы.

В следующей таблице приведено описание того, как компьютер из тупикового домена может быть представлен для внешних сетей:

Исходный компьютер	**IP-адрес исходного компьютера**	**Порт исходного компьютера**	**IP-адрес маршрутизатора NAT**	**Назначенный номер порта маршрутизатора NAT**
A	192.168.32.10	400	215.37.32.203	1
B	192.168.32.13	50	215.37.32.203	2
C	192.168.32.15	3750	215.37.32.203	3
D	192.168.32.18	206	215.37.32.203	4

Как можно видеть, маршрутизатор NAT сохраняет IP-адрес и номер порта каждого из компьютеров в таблице преобразования адресов. После он заменяет IP-адрес на собственный зарегистрированный IP-адрес и номер порта, соответствующий расположению записи для исходного компьютера пакета в таблице. Поэтому из любой внешней сети виден IP-адрес и номер порта маршрутизатора NAT, назначенный маршрутизатором в качестве сведений о компьютере-источнике, содержащихся в каждом пакете.

При этом в домене тупиковой сети может находиться несколько компьютеров, использующих выделенные IP-адреса. Можно создать список доступа IP-адресов, из которого маршрутизатор будет узнавать, каким компьютерам сети требуется NAT. Все другие IP-адреса будут проходить без преобразования.

Количество одновременных преобразований, которое может поддерживать маршрутизатор, зависит в основном от количества доступной ему **DRAM (динамической оперативной памяти)**. Однако поскольку обычно запись в таблице преобразования занимает

всего около 160 байтов, маршрутизатор с 4 Мб DRAM теоретически может одновременно обрабатывать 26 214 преобразований. Этого более чем достаточно для большинства приложений.

IANA выделила специальные диапазоны IP-адресов для использования в качестве немаршрутизируемых внутренних сетевых адресов. Эти адреса считаются незарегистрированными (дополнительную информацию см. в RFC 1918: выделение адресов для частных подсетей Интернета , в котором приведены эти диапазоны адресов), а это означает, что ни одна компания или агентство не может заявить свои права на них и использовать их на общедоступных компьютерах. Маршрутизаторы не переадресуют пакеты на незарегистрированные адреса, поскольку такие сети являются частными и не предполагают распространения данных о себе во внешнем мире. Это означает, что пакет с компьютера с незарегистрированным адресом может попасть на зарегистрированный компьютер-получатель, но ответ будет отклонен первым маршрутизатором, через который он проходит.

Существует диапазон для каждого из трех классов IP-адресов, используемых для организации сетей:

- Диапазон 1 предназначен для класса A: от 10.0.0.0 до 10.255.255.255
- Диапазон 2 предназначен для класса B: от 172.16.0.0 до 172.31.255.255
- Диапазон 3 предназначен для класса C: от 192.168.0.0 до 192.168.255.255

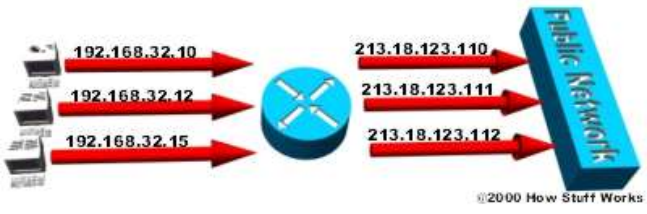
Несмотря на то, что каждый из диапазонов относится к отдельному классу, требования по использованию конкретных диапазонов для внутренних сетей отсутствуют. Однако использование этих диапазонов является более правильным, поскольку это существенно снижает вероятность возникновения конфликтов IP-адресов.

Безопасность и администрирование

Реализация динамического NAT автоматически создает брандмауэр между внутренней сетью и внешней сетью или Интернетом. Динамический NAT позволяет существовать только тем соединениям, которые инициируются из тупикового домена. Естественно, это означает, что компьютер из внешней сети не может подключиться к одному из компьютеров внутренней сети до тех пор, пока последний не инициирует соединение. Поэтому можно просматривать Интернет-страницы, подключаться к сайтам и даже загружать файлы. Однако кто-либо посторонний не может просто зафиксировать ваш IP-адрес и использовать его для подключения к порту вашего компьютера.

Статическое NAT (которое также называется **сопоставлением на входе**) в определенных ситуациях позволяет устанавливать соединения, инициируемые внешними устройствами для связи с компьютерами в тупиковом домене. Например, может возникнуть необходимость в установлении соответствия внутреннего глобального адреса с определенным внутренним локальным адресом, назначенным вашему веб-серверу.

Статическое NAT (сопоставление на входе) позволяет компьютеру тупикового домена сохранять определенный адрес при взаимодействии с устройствами за пределами сети.

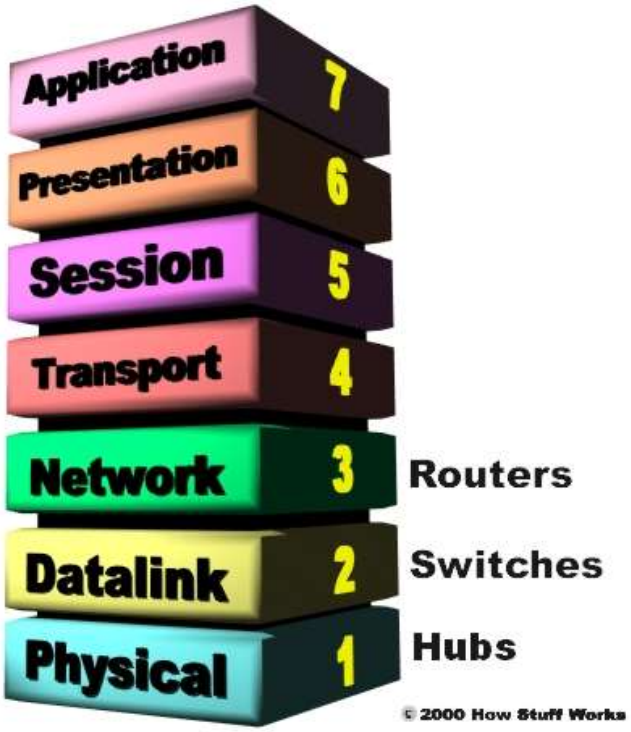


Некоторые маршрутизаторы NAT предусматривают обширное фильтрование и регистрацию трафика. Фильтрование позволяет компании контролировать типы сайтов, которые сотрудники посещают во всемирной паутине, не позволяя им просматривать материалы сомнительного характера. Можно использовать регистрацию трафика для создания файла журнала с информацией о посещаемых сайтах и создавать на его основе различные отчеты.

Иногда преобразование сетевых адресов путают с **прокси-серверами**, но они определенным образом различаются. Преобразование NAT является прозрачным для исходного компьютера и компьютера получателя. Ни один из них не подозревает о посредничестве третьего устройства. Прокси-сервер не является прозрачным. Исходному компьютеру известно, что он выполняет запрос к прокси-серверу, и он должен быть для этого настроен. Компьютер места назначения считает, что прокси-сервер **ЯВЛЯЕТСЯ** исходным компьютером и работает с ним напрямую. Кроме того, прокси-серверы обычно работают на уровне 4 (транспортном) базовой модели OSI или более высоком, в то время как NAT является протоколом уровня 3 (сетевого). Работая на более высоком уровне, прокси-

серверы в большинстве случаев действуют медленнее, чем устройства NAT.

NAT работает на сетевом уровне (уровне 3) базовой модели OSI, что является необходимостью, поскольку на этом уровне работают маршрутизаторы:



Несомненным преимуществом NAT является прямое управление сетью. Например, можно переместить веб-сервер или FTP-сервер на другой компьютер и не волноваться о неработающих ссылках. Просто измените сопоставление на входе по новому внутреннему локальному адресу на маршрутизаторе, чтобы учесть новый узел. Кроме того, можно производить изменения во внутренней сети, поскольку только один внешний IP-адрес либо принадлежит маршрутизатору, либо берется из пула глобальных адресов.

NAT и DHCP сочетаются естественным образом, поэтому можно выбирать для тупикового домена диапазон незарегистрированных IP-адресов и по необходимости выделять их при помощи DHCP-сервера. Это также упрощает расширение сети при росте потребностей. Отсутствует необходимость запрашивать у IANA дополнительные IP-адреса. Можно расширить диапазон доступных IP-адресов, настроенных в DHCP, и немедленно получить пространство для дополнительных компьютеров в сети.

Многоканальное подключение

Поскольку организации все больше и больше полагаются на Интернет, наличие нескольких точек подключения к Интернету быстро становится неотъемлемой частью их сетевой стратегии. Наличие нескольких подключений, что также называется **многоканальным подключением**, снижает риск потенциального нарушения деятельности при сбое одного из подключений.

Кроме обеспечения надежного подключения многоканальное подключение позволяет компании выполнять распределение нагрузки, уменьшая количество компьютеров, подключенных к Интернету через одно соединение. Распределение нагрузки между несколькими подключениями оптимизирует производительность и может существенно уменьшить время ожидания.

Сети с многоканальными подключениями часто подключены к нескольким различным **ISP (поставщики услуг Интернет)**. Каждый ISP назначает компании IP-адрес (или диапазон IP-адресов). Для организации маршрутизации между сетями, использующими различные протоколы, маршрутизаторы используют **BGP (протокол пограничных шлюзов)**, входящий в состав семейства протоколов TCP/IP. В сетях с многоканальным подключением маршрутизатор со стороны тупикового домена использует **IBGP (внутренний протокол пограничных шлюзов)** и **EBGP (внешний протокол пограничных шлюзов)** для связи с другими маршрутизаторами. При использовании NAT совместно с многоканальным подключением на маршрутизаторе NAT настраивается несколько пулов внутренних глобальных адресов, выделяемых различными ISP. Один внутренний локальный адрес должен быть сопоставлен более чем одному внутреннему глобальному адресу из настроенных пулов в зависимости от поставщика, через которого трафик направляется по адресу назначения. Это известно как NAT по месту назначения. Дополнительные сведения см. в документе NAT – возможность использовать карты маршрутов со статическим преобразованием.

Многоканальное подключение играет важную роль при нарушении подключения к одному из ISP. Как только маршрутизатор,

отвечающий за подключение к этому ISP определяет, что соединение потеряно, он перенаправляет все данные через один из других маршрутизаторов.

NAT можно использовать для обеспечения масштабируемой маршрутизации для многоканального подключения к нескольким поставщикам.

Дополнительные сведения

- **Настройка преобразования сетевых адресов: начало работы**
- **Преобразование сетевых адресов в Cisco IOS**
- **Обзор преобразования сетевых адресов в Cisco IOS**
- **Настройка IP-адресации**
- **Использование NAT в перекрывающихся сетях**
- **Преобразование сетевых адресов: порядок работы**
- **Журнал Интернет-протокола: неполадки NAT**
- **RFC 1631: преобразователь сетевых IP-адресов (NAT)**
- **RFC 1918: выделение адресов для частных подсетей Интернета**
- **База знаний - техническая документация: вопросы и ответы по преобразованию сетевых адресов**
- **Обсуждение технических вопросов NAT**
- **Страница поддержки NAT**
- **Техническая поддержка - Cisco Systems**

Дата генерации PDF файла: Jan 05, 2010

http://www.cisco.com/support/RU/customer/content/9/92048/nat-cisco.shtml