RFC 3022 — Традиционная трансляция сетевых адресов IP (NAT)

Статус документа

Этот документ содержит информацию для сообщества Internet и не определяет каких-либо стандартов. Документ может распространяться свободно.

Тезисы

Базовая трансляция сетевых адресов или Basic NAT представляет собой метод отображения адресов IP из одной группы в другую, прозрачного для конечных пользователей. Трансляция сетевых адресов и номеров портов или NAPT — метод, с помощью которого множество сетевых адресов и соответствующих портов TCP/UDP (Transmission Control Protocol/User Datagram Protocol) преобразуется в один сетевой адрес и номер порта TCP/UDP. Оба метода вместе называют традиционной трансляцией адресов (traditional NAT). NAT обеспечивает механизм подключения областей с приватными адресами к внешним областям, в которых используются уникальные в глобальном масштабе зарегистрированные адреса.

Предисловие

Описанная в этом документе работа NAT расширяет возможности трансляции адресов, описанные в RFC 1631 и включает новый тип адресов, а также трансляцию портов TCP/UDP. Кроме того, документ вносит исправления в алгоритм корректировки контрольных сумм (Checksum adjustment), опубликованный в RFC 1631, а также включает обсуждение работы NAT и возможные ограничения.

1. Введение

Необходимость преобразования (трансляции) адресов IP возникает в тех случаях, когда используемые внутри сети адреса IP невозможно использовать за пределами сети из соображений сохранения тайны или по той причине, что эти адреса корректны только внутри сети.

Сетевая топология за пределами локального домена может изменяться по разным причинам. Абоненты могут менять провайдеров, опорные сети компаний могут реорганизоваться, а провайдеры могут делиться или объединяться. Всякий раз при изменении внешней топологии выделение адресов внутри локального домена также требуется соответствующим образом изменять. Эти изменения могут оставаться незаметными для пользователей внутри домена при централизованном изменении на одном маршрутизаторе, обеспечивающем трансляцию адресов.

Базовая трансляция во многих случаях (за исключением ситуаций, указанных в [NAT-TERM] и главе 6 данного документа) может обеспечивать доступ пользователей из частной сети во внешние сети, а также доступ извне к некоторым локальным хостам. Организациям, в которых сеть используется для решения внутренних задач, а доступ во внешние сети требуется нерегулярно, такая схема будет весьма удобна.

Многие пользователи SOHO и удаленные сотрудники используют в своих офисах множество узлов с приложениями TCP/UDP, но имеют лишь один адрес IP, выделенный их маршрутизатору провайдером для доступа во внешнюю сеть. Эта постоянно растущая группа

удаленных пользователей может применить метод трансляции NAPT, который позволяет множеству узлов из локальной сети одновременно получить доступ во внешние сети с использованием единственного адреса IP, выделенного для их маршрутизатора.

Существуют ограничения на использование метода трансляции. Обязательно, чтобы все запросы и отклики, относящиеся к одной сессии, маршрутизировались одним NAT-маршрутизатором. Одним из вариантов решения задачи является организация NAT на граничном маршрутизаторе, который является единственным для краевого домена и все пакеты IP, адресованные в домен или исходящие из него, проходят через этот маршрутизатор. Существуют также варианты решения задачи при использовании множества устройств NAT. Например, частная сеть может иметь две разных точки выхода в сети различных провайдеров и поток пакетов той или иной сессии внутреннего хоста может проходить через любое устройств NAT, которое будет обеспечивать лучшую метрику для внешнего хоста. При отказе одного из маршрутизаторов NAT оставшийся маршрутизатор сможет обслуживать трафик для всех соединений. Однако в этой модели при смене маршрутизации во время организованной сессии и переключении на другой маршрутизатор NAT соединение данной сессии будет разорвано. В качестве варианта решения этой проблемы можно использовать одинаковую конфигурацию NAT на обоих маршрутизаторах и обмен информацией о состоянии соединений для обеспечения безопасного переключения трафика между маршрутизаторами.

Трансляция адресов не зависит от приложений и часто сопровождается специализированными шлюзами (ALG для мониторинга и изменения передаваемой информации. FTP является наиболее популярным представителем ALG на устройствах NAT. Приложениям, которым требуется наличие ALG, недопустимо передавать свои данные в шифрованном виде, поскольку это будет нарушать работу ALG, если последний не имеет ключа для расшифровки информации.

Недостатком этого решения является сквозная значимость адресов IP и рост числа хранимых состояний. В результате сквозная защита IP на сетевом уровне, обеспечиваемая IPSec, не может использоваться конечными станциями при наличии в пути устройств NAT. Преимуществами этого варианта является то, что его можно реализовать без внесения изменений в настройки хостов и маршрутизаторов.

Определения терминов "Address Realm", "Transparent Routing", "TU Ports", "ALG" и др., используемые в данном документе, можно найти в [NAT-TERM].

2. Обзор традиционной трансляции NAT

Описанная в этом документе работа системы трансляции адресов относится к Traditional NAT. Существуют и другие варианты NAT, которые в этом документе не рассматриваются. Traditional NAT обеспечивает в большинстве случаев внутренним хостам частных сетей прозрачный доступ во внешнюю сеть. При традиционной трансляции сессии являются односторонними и направлены наружу из частной сети. Организация сессий в противоположном направлении может быть разрешена в качестве исключения с использованием статического отображения адресов для избранных хостов. Традиционная трансляция имеет два варианта — Basic NAT и NAPT. Basic NAT обеспечивает преобразование только для адресов, а NAPT позволяет транслировать адреса IP и идентификаторы транспортного уровня (такие, как номера портов TCP/UDP или ICMP query ID).

Если явно не указано иное, термины NAT и трансляция адресов в этом документе относятся к традиционной трансляции, а именно NAPT и Basic NAT. Для выполнения трансляции могут использоваться только оконечные маршрутизаторы, как показано на рисунке 1.

```
     \ | /                 .                                /
+---------------+  WAN     .           +-----------------+/
|Regional Router|----------------------|Stub Router w/NAT|---
```

```
+---------------+          .           +-----------------+\
                           .                       |         \
                           .                       |  LAN
                           .               ---------------
                      Stub border
```

??????? 1: ??????????? ??????????? NAT

2.1 Обзор Basic NAT

В этом параграфе описана работа Basic NAT. Оконечный домен с набором приватных сетевых адресов может взаимодействовать с внешними сетями, используя динамическое отображение набора приватных адресов на некое множество публичных адресов IP. Если число локальных узлов не превышает число имеющихся публичных адресов, каждому локальному адресу можно гарантированно поставить в соответствие публичный адрес. В противном случае число узлов, которые могут одновременно получить доступ во внешние сети, будет ограничено количеством публичных адресов. Отдельные локальные адреса могут статически отображаться на конкретные публичные адреса для обеспечения доступа к локальным хостам извне с использованием фиксированных адресов. С одного локального узла может быть организовано множество одновременных сессий, использующих одно адресное отображение.

Адреса внутри оконечного домена являются локальными для этого домена и некорректны за его пределами. Таким образом, эти адреса могут использоваться одновременно во множестве оконечных доменов.

Например, один блок адресов класса A может применяться во многих оконечных доменах сразу. В каждой точке выхода из оконечного домена во внешнюю сеть используется NAT. Если в домене используется несколько точек выхода, важное значение приобретает использование во всех таких точках одинаковых таблиц трансляции NAT.

В примере, показанном на рисунке 2, оконечные домены A и B используют блок приватных адресов класса A 10.0.0.0/8 [RFC 1918 (Распределение адресов в частных IP-сетях) [1]].

Системе NAT домена A выделен блок адресов класса C 198.76.29.0/24, а в домене B — блок 198.76.28.0/24. Адреса блоков класса C являются уникальными в глобальном масштабе и другие устройства NAT не могут их использовать.

```
                        \ | /
                      +---------------+
                      |Regional Router|
                      +---------------+
                    WAN |            | WAN
                        |            |
    Stub A .............|....   ....|............ Stub B
                        |            |
      {s=198.76.29.7,^  |            |  v{s=198.76.29.7,
       d=198.76.28.4}^  |            |  v d=198.76.28.4}
        +-----------------+       +-----------------+
        |Stub Router w/NAT|       |Stub Router w/NAT|
        +-----------------+       +-----------------+
              |                         |
              |  LAN                LAN  |
        -------------             -------------
                   |                  |
{s=10.33.96.5, ^  |                  |  v{s=198.76.29.7,
 d=198.76.28.4}^ +--+             +--+ v d=10.81.13.22}
                 |--|             |--|
```

```
                /____\          /____\
              10.33.96.5      10.81.13.22

??????? 2: ?????? ?????? Basic NAT
```

Когда хост домена A с адресом 10.33.96.5 хочет передать пакет хосту домена B с адресом 10.81.13.22, он использует в качестве адреса получателя уникальное в глобальном масштабе значение 198.76.28.4 и передает пакет своему основному маршрутизатору. Этот маршрутизатор имеет статический маршрут в сеть 198.76.0.0 и пакет пересылается в WAN-канал. Однако до того, как пакет будет передан, NAT преобразует адрес отправителя 10.33.96.5 в заголовке IP в уникальный адрес 198.76.29.7. Аналогично происходит преобразование адресов для пакетов IP, передаваемых в обратном направлении.

Отметим, что трансляция не требует внесения изменений на хостах или маршрутизаторах. Например, при для хоста домена A хостом из домена B будет использоваться адрес 198.76.28.4. Трансляция адресов в большинстве случаев прозрачна для конечных хостов. Естественно, что приведенный пример очень прост. Эта схема трансляции имеет множество спорных моментов, которые требуется исследовать.

2.2. Обзор NAPT

Предположим, что организация имеет частную сеть IP и WAN-канал к провайдеру. Краевому маршрутизатору оконечной сети присвоен уникальный адрес для интерфейса канала WAN, а узлы внутри сети организации используют приватные адреса, значимость которых ограничена данной сетью. В этом случае узлы внутренней сети могут получить одновременный доступ во внешние сети с использованием единственного зарегистрированного адреса IP и трансляции NAPT. Этот вариант трансляции позволяет отображать пары типа (локальный адрес, локальный номер порта TU) в пары типа (зарегистрированный адрес, присвоенный номер порта TU).

Эта модель отвечает требованиям большинства групп SOHO для организации доступа во внешние сети с использованием единственного адреса IP, выделенного провайдером. Модель можно расширить для того, чтобы обеспечить доступ извне к локальному узлу за счет статического отображения локального узла на каждый номер порта TU для зарегистрированного адреса IP.

В показанном на рисунке 3 примере внутри оконечной сети A используется блок адресов класса A 10.0.0.0/8. WAN-интерфейсу граничного маршрутизатора сети провайдером присвоен IP-адрес 138.76.28.4.

```
                                  \ | /
                                +-----------------------+
                                |Service Provider Router|
                                +-----------------------+
                              WAN |
                                  |
            Stub A .............|....
                                  |
    ^{s=138.76.28.4,sport=1024, |  v{s=138.76.29.7, sport = 23,
    ^ d=138.76.29.7,dport=23}   |  v d=138.76.28.4, dport = 1024}
                     +------------------+
                     |Stub Router w/NAPT|
                     +------------------+
                       |
                       |  LAN
---------------------------------------------
   |        ^{s=10.0.0.10,sport=3017, |  v{s=138.76.29.7, sport=23,
```

```
   |        ^ d=138.76.29.7,dport=23} |  v d=10.0.0.10, dport=3017}
   |                                  |
  +--+      +--+                    +--+
  |--|      |--|                    |--|
 /____\    /____\                  /____\
10.0.0.1  10.0.0.2   .....        10.0.0.10

??????? 3: ?????? NAPT
```

Когда хост сети A с адресом 10.0.0.10 передает пакет telnet хосту 138.76.29.7, он указывает публичный адрес получателя 138.76.29.7 и отправляет пакет основному маршрутизатору. Маршрутизатор имеет статический маршрут в сеть 138.76.0.0/16 и пересылает пакет в канал WAN. Однако до пересылки пакета NAPT транслирует адрес отправителя 10.0.0.10 и номер порта TCP 3017 в заголовках IP и TCP, используя публичный адрес 138.76.28.4 и уникальное значение номера порта TCP (скажем, 1024). Для обратных пакетов происходит похожее преобразование адреса и номера порта TCP в IP-адрес локального хоста и номер целевого порта TCP.

Отметим снова, что не требуется вносить какие-либо изменения на хостах или маршрутизаторах. Трансляция совершенно прозрачна.

В описанном варианте поддерживаются только сеансы TCP/UDP, организованные из локальной сети. Однако для некоторых служб (таких, как DNS) требуется обеспечить доступ извне. Могут существовать также иные службы, к которым организация хочет предоставить внешний доступ. Можно статически настроить на граничном маршрутизаторе отображение общеизвестных номеров портов TU [RFC 1700] на адреса конкретных хостов локальной сети.

В дополнение к сессиям TCP/UDP маршрутизатор NAPT может также обеспечивать мониторинг сообщений ICMP, за исключением типа REDIRECT. Запросы ICMP транслируются подобно пакетам TCP/UDP и поле идентификатора в заголовке сообщения ICMP будет уникально отображаться в идентификатор запроса для зарегистрированного адреса IP. Поле идентификатора в заголовках сообщений ICMP устанавливается отправителем и возвращается неизменным в отклике на запрос. Следовательно, пара (локальный адрес IP, локальный идентификатор ICMP) отображается в пару (публичный адрес IP, выделенное значение идентификатора ICMP) маршрутизатором NAPT и обеспечивает уникальную идентификацию всех типов сообщений ICMP от любого из локальных хостов. Изменение сообщений ICMP об ошибках рассматриваемое ниже, включает модификацию данных ICMP, а также заголовков IP и ICMP.

В конфигурациях NAPT, где зарегистрированный адрес IP совпадает с IP-адресом WAN-интерфейса оконечного маршрутизатора, этот маршрутизатор должен различать сессии TCP, UDP или ICMP, организованные им самим от сессий, организованных узлами внутренней сети. Все входящие сессии (включая TCP, UDP и ICMP) предполагаются адресованными маршрутизатору NAT, как конечной точке, если целевой порт не отображен статически на адрес того или иного узла локальной сети.

Сессии, отличные от TCP, UDP и ICMP, просто не поддерживаются для локальных узлов, обслуживаемых маршрутизатором NAPT.

3. Фазы трансляции для сеанса

Фазы традиционной трансляции NAT совпадают с описанными в [NAT-TERM]. В следующих параграфах рассматриваются специфические аспекты традиционной трансляции.

3.1. Привязка адреса

При использовании Basic NAT приватный адрес связывается с внешним адресом при

организации первой исходящей сессии со стороны хоста локальной сети. Все последующие сессии, организованные этим хостом, будут использовать тот же адрес для трансляции пакетов.

В случае NAPT множество приватных адресов отображается на один публичный адрес и привязка будет осуществляться между парами (приватный адрес, приватный порт TU) и парами (публичный адрес, выделенный порт TU). Как и для Basic NAT эта привязка определяется при организации первой исходящей сессии для пары (приватный адрес, приватный порт TU) со стороны хоста локальной сети. Хотя это и не является общепринятым, возможна организация приложением на хосте локальной сети множества одновременных сессий для одной пары (приватный адрес, приватный порт TU). В таких случаях для этой пары (приватный адрес, приватный порт TU) может использоваться одна привязка для всех пакетов, относящихся к сессиям для данной пары с этого хоста.

3.2. Просмотр и трансляция адреса

После привязки адреса или пары (адрес, порт TU)в случае использования NAPT может на программном уровне поддерживаться информация о состоянии каждого соединения, использующего данную привязку. Пакеты, относящиеся к одной сессии транслируются с учетом данной сессии. Точное поведение трансляции рассматривается ниже.

3.3. Удаление привязки адреса

Когда последняя сессия для адреса или пары (адрес, порт TU) завершается, привязка может быть ликвидирована.

4. Преобразование пакетов

Пакеты, относящиеся к сессиям NAT, подвергаются трансляции для обоих направлений. Детальное описание преобразований, выполняемых для отдельных пакетов рассматривается ниже.

4.1. Манипуляции с заголовками IP, TCP, UDP и ICMP

В модели Basic NAT требуется изменять заголовок IP в каждом пакете. Модификация включает адрес IP (адрес отправителя для исходящих пакетов и адрес получателя для входящих) и контрольную сумму IP.

Для сессий TCP ([TCP]) и UDP ([UDP]) также требуется изменять контрольную сумму в заголовках TCP/UDP. Это связано с тем, что контрольная сумма TCP/UDP учитывает также псевдозаголовок, содержащий IP-адреса отправителя и получателя. Исключением являются случаи когда контрольная сумма заголовка UDP имеет значение 0 — в этом случае поле контрольной суммы не меняется. Для пакетов ICMP Query ([ICMP]) не требуется вносить изменений в заголовок ICMP, поскольку контрольная сумма в заголовке ICMP не учитывает адресов IP.

В модели NAPT изменение заголовка IP похоже на случай Basic NAT. Для сессий TCP/UDP изменяется также номер порта TU (порт отправителя для исходящих пакетов и порт получателя для входящих) в заголовке TCP/UDP. Заголовок ICMP в пакетах ICMP также требуется изменять для корректировки значения идентификатора запроса и контрольной суммы заголовка ICMP. Идентификатор запроса хоста внутренней сети в исходящих пакетах должен заменяться на присвоенный при трансляции идентификатор, а для входящих откликов должно выполняться обратное преобразование. Контрольная сумма заголовка ICMP должна корректироваться с учетом трансляции Query ID.

4.2. Корректировка контрольной суммы

Преобразования NAT выполняются для каждого пакета и могут приводить к значительным расходам вычислительных ресурсов при необходимости корректировки одной или нескольких контрольных сумм в дополнение к простой замене полей. К счастью существует приведенный ниже алгоритм, делающий корректировку контрольных сумм заголовков IP, TCP, UDP и ICMP очень простой и эффективной. Поскольку все эти заголовки используют арифметику дополнения до 1, достаточно рассчитать разность между адресами до и после трансляции и добавить полученное значение к контрольной сумме. Приведенный ниже алгоритм применим только для случаев четного смещения (т. е., поле optr должно начинаться с четного октета от начала заголовка) и четной длины (т. е., поля olen и nlen должны иметь четные значения). Ниже приведен вариант реализации алгоритма на языке C.

```
void checksumadjust(unsigned char *chksum, unsigned char *optr,
int olen, unsigned char *nptr, int nlen)

/* ?????????: unsigned char ????? ?????? 8 ?????, long - 32 ????.
  - chksum ????????? ?????????? ????? ??????
  - optr ????????? ?????? ?????? ? ??????
  - nptr ????????? ????? ?????? ? ??????
*/
{
  long x, old, new;
  x=chksum[0]*256+chksum[1];
  x=~x & 0xFFFF;
  while (olen)
  {
      old=optr[0]*256+optr[1]; optr+=2;
      x-=old & 0xffff;
      if (x<=0) { x--; x&=0xffff; }
      olen-=2;
  }
  while (nlen)
  {
      new=nptr[0]*256+nptr[1]; nptr+=2;
      x+=new & 0xffff;
      if (x & 0x10000) { x++; x&=0xffff; }
      nlen-=2;
  }
  x=~x & 0xFFFF;
  chksum[0]=x/256; chksum[1]=x & 0xff;
}
```

4.3. Изменение сообщений ICMP об ошибках

Изменения для сообщений ICMP об ошибках ([ICMP]) будут включать модификацию заголовков IP и ICMP, а также модификацию заголовков пакета, вложенного в поле данных сообщения ICMP.

Чтобы трансляция NAT была прозрачной для конечных хостов, адрес IP в заголовке IP, вложенном в поле данных сообщения ICMP, а также контрольная сумма вложенного заголовка IP должны быть изменены. Требуется также изменить значение контрольной суммы заголовка ICMP с учетом изменений, внесенных в данные.

Для случая NAPT, если пакет IP, вложенный в сообщение ICMP, является пакетом TCP, UDP или ICMP Query, потребуется также изменить номер порта TU в заголовке TCP/UDP или поле Query Identifier в заголовке ICMP Query.

В заключение нужно изменить заголовок IP пакета, содержащего сообщение ICMP.

4.4. Поддержка FTP

Одно из наиболее популярных приложений FTP ([FTP]) будет требовать наличия ALG для мониторинга управляющей сессии, чтобы определить параметры соответствующего сеанса передачи данных. FTP ALG является встроенной компонентой большинства реализаций NAT.

FTP ALG требует специальной таблицы для корректировки порядковых номеров и номеров подтверждений с учетом номера порта FTP для отправителя или получателя. В записи таблицы следует включать адреса и номера портов для отправителя и получателя, приращения (delta) для порядковых номеров, а также временные метки. Новые записи включаются в таблицу только в результате наблюдения команд FTP PORT и откликов PASV. Приращение порядкового номера может увеличиваться или уменьшаться для каждой команды FTP PORT и отклика PASV. Порядковые номера инкрементируются для исходящих пакетов, а номера подтверждений декрементируются для входящих пакетов на величину приращения (delta).

Для случая Basic NAT преобразование данных FTP ограничивается трансляцией между приватными и публичными адресами (кодируются пооктетно в ASCII). Для случая NAPT требуется также трансляция октетов, задающих номер порта TCP (в коде ASCII) и следующих за октетами адреса.

4.5 Поддержка DNS

Исходя из того, что при традиционной трансляции NAT сессии преимущественно инициируются из внутренней сети, можно избежать применения DNS ALG в связке с традиционной трансляцией NAT. Внутренние серверы DNS приватного домена обеспечивают преобразование имен в адреса IP для внутренних хостов и возможно для некоторых внешних хостов. Внешние серверы DNS поддерживают преобразование имен для внешних хостов, но не поддерживают для внутренних. Если в частной сети нет внутренних серверов DNS, все запросы DNS могут направляться к внешним серверам DNS для поиска отображения имен внешних хостов.

4.6. Обработка опций IP

Дейтаграммы IP с любыми из опций Record Route, Strict Source Route и Loose Source Route будут включать запись использования адресов IP промежуточных маршрутизаторов. Промежуточный маршрутизатор NAT может отказаться от поддержки таких опций или оставлять нетранслированные адреса при обработке опций. Результатом сохранения нетранслированных адресов в опциях будет раскрытие внутренних адресов сети в пакетах с опциями заданной отправителем маршрутизации. Это не создает, по сути, дополнительного риска, поскольку предполагается, что каждый маршрутизатор просматривается только маршрутизатором следующего интервала (next hop router).

5. Разное

5.1. Деление адресов на приватные и публичные

Для описанной в документе работы NAT необходимо разделить пространство адресов IP на две части — приватные адреса, используемые внутри оконечного домена, и публичные адреса с глобальной доступностью. Любой конкретный адрес должен относится к числу приватных или публичных. Области приватных и публичных адресов не перекрываются.

Проблема перекрытия приватных и публичных адресов заключается в следующем — предположим, что хост оконечного домена A хочет передать пакет хосту оконечного домена

B, но публичные адреса домена B перекрываются с приватными адресами домена A. В таком случае маршрутизаторы домена A не смогут отличить публичный адрес хоста из домена B от приватного адреса в своем домене.

5.2. Рекомендации по выбору приватных адресов

[RFC 1918 [1]] содержит рекомендации по выделению адресного пространства для частных сетей. Агентство IANA выделило для этих целей 3 блока адресов IP — 10.0.0.0/8, 172.16.0.0/12, и 192.168.0.0/16. В нотации без использования CIDR первый блок представляет собой одну сеть класса A, второй — 16 последовательных сетей класса B, а третий — 256 последовательных сетей класса C.

Организации, которые решили использовать адреса из указанных блоков, могут делать это без какого-либо согласования с IANA или реестром Internet. Адресное пространство может, таким образом, использоваться одновременно во множестве организаций с трансляцией NAT на граничных маршрутизаторах.

5.3. Маршрутизация через NAT

Маршрутизаторам, обеспечивающим NAT, не следует анонсировать наружу префиксы частных сетей. За пределами оконечного домена могут быть известны только публичные адреса. Однако глобальная информация, получаемая NAT от оконечного маршрутизатора может обычным путем анонсироваться во внутреннюю сеть.

Обычно оконечный маршрутизатор NAT имеет статический маршрут для пересылки всего направленного наружу трафика маршрутизатору сервис-провайдера через канал WAN, а маршрутизатор провайдера имеет статический маршрут для пересылки пакетов NAT (т. е., пакетов, в которых IP-адрес получателя относится к используемому NAT блоку публичных адресов) маршрутизатору NAT через канал WAN.

5.4. Переключение с Basic NAT на NAPT

В Basic NAT, когда число узлов внутренней сети превышает число доступных для трансляции публичных адресов (например, внутренняя сеть класса B отображается в публичный блок класса C) внешний доступ к некоторым хостам внутренней сети может быть внезапно нарушен после того, как будет использован весь доступный блок публичных адресов. Это очень неудобно и вносит существенные ограничения. Таких ситуаций можно избежать, разрешая маршрутизатору с Basic NAT переключаться в режим NAPT после того, как будет исчерпан весь блок публичных адресов. Это обеспечит постоянный доступ извне к хостам внутренней сети, сохраняя возможность доступа из частной сети ко внешним ресурсам для большинства приложений. Отметим, однако, что некоторые приложения, работающие через Basic NAT, могут быть прерваны в результате переключения на трансляцию NAPT.

6. Ограничения NAT

[NAT-TERM] описывает ограничения, присущие всем вариантам NAT без особой детализации. Ниже приводится более подробное описание ограничений, присущий традиционной трансляции NAT.

6.1. Безопасность и сохранность тайны

Традиционная трансляция NAT может рассматриваться как средство сокрытия внутренней структуры сети, поскольку сеансы организуются со стороны внутренних хостов и реальные адреса этих хостов недоступны извне.

Однако в силу тех же причин могут осложниться вопросы отладки (включая случаи нарушения безопасности). Если хост частной сети совершает какие-либо некорректные действия в Internet (например, атака другого хоста или рассылка спама), существенно сложней отследить реальный источник проблем, поскольку IP-адрес хоста скрыт маршрутизатором NAT.

6.2. Отклики ARP на транслированные публичные адреса интерфейсов ЛВС

Трансляция NAT должна использоваться только на граничных маршрутизаторах оконечных доменов. В примерах, иллюстрирующих Basic NAT и NAPT, поддерживался WAN-канал к внешнему маршрутизатору (т. е., к маршрутизатору сервис-провайдера) от маршрутизатора NAT. Однако, если канал WAN заменить соединением через ЛВС и часть или все публичные адреса, используемые для отображения NAT будут относиться к той же подсети IP, что и сегмент ЛВС, ожидается, что маршрутизатор NAT будет поддерживать ARP для диапазона адресов, относящегося к той же подсети. В варианте Basic NAT маршрутизатор должен отвечать на запросы ARP для отображенных с помощью NAT публичных адресов своим адресом MAC. Если маршрутизатор NAT не отвечает на такие запросы, они останутся безответными, поскольку в сети нет других узлов, которые могли бы на них ответить.

Такой случай маловероятен для NAPT, за исключением ситуаций, когда единственный адрес, используемый для отображения NAPT, не совпадает с адресом интерфейса NAT-маршрутизатора (как в описанном в параграфе 5.4 случае переключения в Basic NAT на NAPT).

Использование для трансляции NAT диапазона адресов из непосредственно подключенной подсети избавляет от необходимости задания статического маршрута на маршрутизаторе сервис-провайдера.

Авторы считают, что подключения к сервис-провайдеру через ЛВС не являются широко распространенными. Однако производители могут быть заинтересованы в поддержке для таких случаев функций proxy ARP.

6.3. Трансляция исходящих фрагментов TCP/UDP в NAPT

Трансляция исходящих (т. е., переданных внутренними хостами) фрагментов TCP/UDP в случае NAPT обречена на неудачу. Причина этого заключается в том, что лишь первый фрагмент содержит заголовок TCP/UDP, который позволяет связать пакет с конкретной сессией для преобразования адресов. Последующие фрагменты не содержат информации о номере порта TCP/UDP, а просто включает некий идентификатор фрагментации, заданный в первом фрагменте. Предположим, что два приватных хоста передают фрагментированные пакеты TCP/UDP одному получателю. Может случиться так, что оба эти хоста используют одинаковый идентификатор фрагментации. Когда адресат получит эти два несвязанных фрагмента, содержащих один идентификатор фрагментации и адрес отправителя, он не сможет определить к какой из сессий относится каждый из фрагментов.

В результате обе сессии окажутся поврежденными.

7. Современные реализации

Доступно множество коммерческих реализаций трансляции адресов, которые соответствуют описанию NAT в данном документе. Открытая ОС Linux содержит реализацию NAT, называемую "IP masquerade". Открытая ОС FreeBSD содержит реализацию NAPT, работающую как демон.

Отметим, что исходный код Linux распространяется по лицензии GNU, а программы FreeBSD —

по лицензии UC Berkeley.

Программы для Linux и FreeBSD являются бесплатными и вы можете купить компакт-диск с любой из этих программ за весьма разумную цену. Можно также просто загрузить последний вариант программы со множества серверов FTP.

8. Вопросы безопасности

Вопросы безопасности, рассмотренные в [NAT-TERM] для всех вариантов NAT, применимы к традиционной трансляции NAT.

Литература

1. [NAT-TERM] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.
2. [RFC 1918] Rekhter, Y., Moskowitz, B., Karrenberg, D., de Groot, G. and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996. [1]
3. [RFC 1700] Reynolds, J. and J. Postel, "Assigned Numbers", STD 2, RFC 1700, October 1994.
4. [RFC 1122] Braden, R., "Requirements for Internet Hosts — Communication Layers", STD 3, RFC 1122, October 1989 [2]
5. [RFC 1123] Braden, R., "Requirements for Internet Hosts — Application and Support", STD 3, RFC 1123, October 1989 [3]
6. [RFC 1812] Baker, F., "Requirements for IP Version 4 Routers", RFC 1812, June 1995.
7. [FTP] Postel, J. and J. Reynolds, "FILE TRANSFER PROTOCOL (FTP)", STD 9, RFC 959, October 1985.
8. [TCP] Defense Advanced Research Projects Agency Information Processing Techniques Office, "TRANSMISSION CONTROL PROTOCOL (TCP) SPECIFICATION", STD 7, RFC 793, September 1981. [4]
9. [ICMP] Postel, J., "INTERNET CONTROL MESSAGE (ICMP) SPECIFICATION", STD 5, RFC 792, September 1981. [5]
10. [UDP] Postel, J., "User Datagram Protocol (UDP)", STD 6, RFC 768, August 1980. [6]
11. [RFC 2101] Carpenter, B., Crowcroft, J. and Y. Rekhter, "IPv4 Address Behaviour Today", RFC 2101, February 1997.

Адреса авторов

Pyda Srisuresh
Jasmine Networks, Inc.
3061 Zanker Road, Suite B
San Jose, CA 95134 U.S.A.
Phone: (408) 895-5032
EMail: moc.oohay@hserusirs

Kjeld Borch Egevang
Intel Denmark ApS
Phone: +45 44886556
Fax: +45 44886051
EMail: moc [dot] letni [at] gnavege [dot] dlejk
http://www.freeyellow.com/members/kbe [7]

Перевод на русский язык

Николай Малых, moc.milib@hkylamn

Источник (получено *2025-12-11 22:48*):
http://muff.kiev.ua/content/rfc-3022-traditsionnaya-translyatsiya-setevykh-adresov-ip-nat

Ссылки:

[1] http://rfc2.ru/1918.rfc
[2] http://rfc2.ru/1122.rfc
[3] http://rfc2.ru/1123.rfc
[4] http://rfc2.ru/793.rfc
[5] http://rfc2.ru/792.rfc
[6] http://rfc2.ru/768.rfc
[7] http://www.freeyellow.com/members/kbe