

IPv6: вчера, сегодня, завтра (Часть III)

Стратегия развития: сосуществование IPv4 и IPv6

Начав читать эту заключительную часть «трилогии» вы, возможно, с недоумением обнаружите, что в ней протоколу IPv4 уделено, пожалуй, больше места, чем его последователю – IPv6. Почему же в статье о завтрашнем дне протокола IPv6 и, как следствие, Интернета в целом, мы уделяем столько внимания его предшественнику? Не является ли внедрение IPv6 в инфраструктуре сервис-провайдера решением проблемы отсутствия свободного пула адресов IPv4?

Сложность в том, что эффективность этого внедрения зависит от степени глобального проникновения и использования IPv6. На сегодняшний день, степень эта весьма невелика, как мы увидели в предыдущей статье. Соответственно невысока и эффективность инвестиций в IPv6 поскольку, внедрение IPv6 не решит проблем недостатка IPv4, ибо большая часть Интернета по-прежнему доступна только через протокол IPv4. Размер этой части Интернета определяет значимость протокола IPv4 и, в обратной пропорции, протокола IPv6 для сервис-провайдеров. Действительно, как только все ресурсы Интернета будут доступны с помощью обоих протоколов, необходимость в протоколе IPv4 отпадет. На этом положении, кстати, и была основана изначальная схема перехода к IPv6, так называемая схема “двойного стека”.

Другим фактором, определяющим потребность в дополнительных адресах IPv4 является динамика роста самого сервис-провайдера. Ведь каждый новый подключенный клиент должен иметь возможность обмениваться данными с Интернетом IPv4, что требует предоставления этому клиента адреса IPv4. Скажем прямо, для растущих сервис-провайдеров возможно более приоритетным станет решение проблемы нехватки адресов IPv4, чем внедрение IPv6. В то же время важно отметить, что обсуждаемая стратегия и динамика сосуществования основана на предположении, что инфраструктура сервис-провайдера обеспечивает полноценную поддержку IPv6.

Динамика потребности в адресном пространстве IPv4 по мере глобального внедрения IPv6 показана на рисунке 1. На этом рисунке светло-зеленой линией обозначен рост глобального Интернета. По мере внедрения протокола IPv6 доля Интернета, доступного только по IPv4 будет неуклонно уменьшаться (темно-зеленая кривая). Синяя линия отображает размер сервис-провайдера, характеризуемый, например, числом подключенных пользователей. В данном случае представлен растущий провайдер. Наконец, потребность в адресах IPv4 показана кривой красного цвета.

По мере расширения клиентской базы провайдера пропорционально увеличивается потребность в дополнительных адресах IPv4. В то же время, все большая и большая часть Интернета становится доступной по протоколу IPv6, что выражается в обратной тенденции, когда все меньшее число пользовательских соединений основаны на протоколе IPv4. Соответственно, потребность в адресах IPv4 снижается. Наконец, когда подавляющее большинство ресурсов Интернета станет доступными по IPv6, потребность в IPv4 станет ничтожной. Таким образом завершится фаза перехода Интернета на протокол IPv6. Продолжительность этой фазы может занять несколько лет. Не исключена, правда, вероятность, что фаза эта не закончится никогда, но об этом – чуть позже.

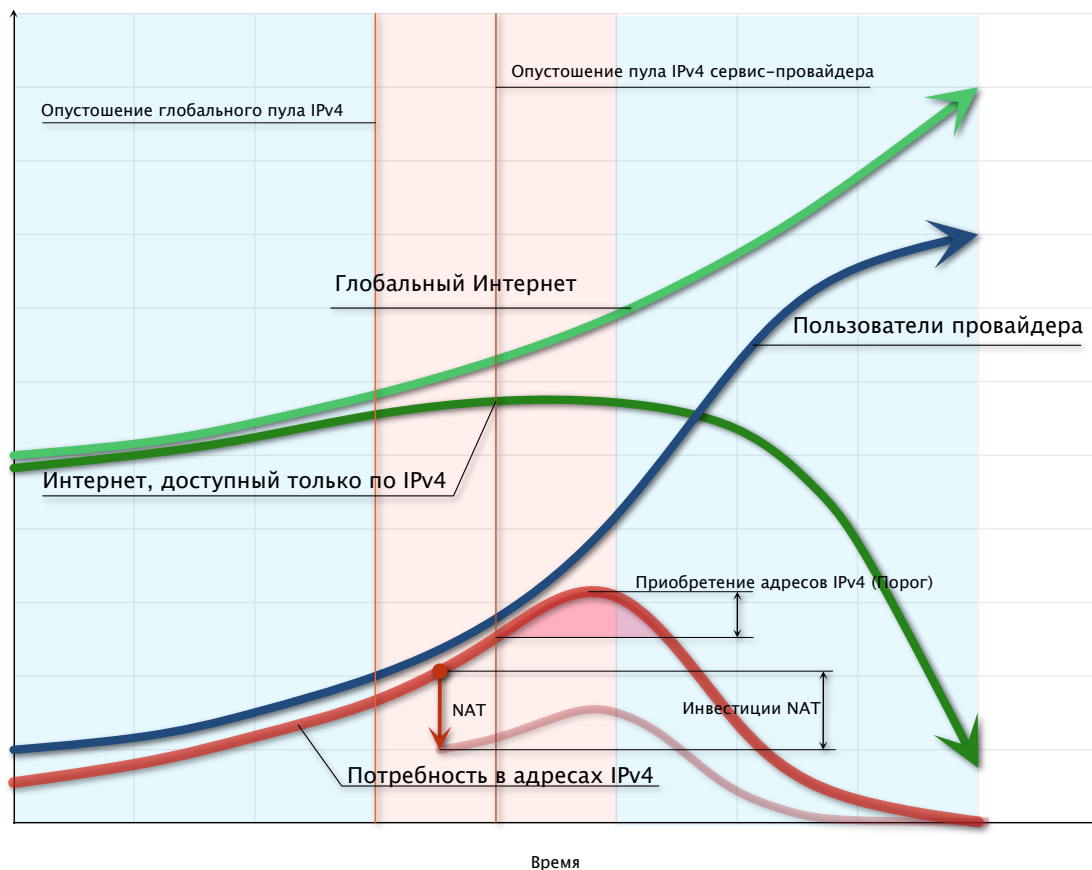


Рис. 1. Динамика сосуществования IPv4 и IPv6

Как видно из графика, наиболее критичной фазой для сервис провайдера является промежуток времени с момента опустошения глобального свободного пула IPv4 до момента, когда потребность в дополнительных адресах IPv4 начнет уменьшаться. Эта фаза отмечена на графике розовым цветом.

Надо заметить, что высота порога, образуемого красной кривой различна для разных провайдеров. Также различен момент завершения свободных адресов в собственном пуле провайдера (вторая вертикальная красная линия). Другими словами, умеренно растущий провайдер с достаточным запасом свободных адресов, имеет шансы "перезимовать" переходный период без особых ухищрений. Важно отметить, что и в этом случае необходимыми условиями являются полноценная поддержка IPv6 в инфраструктуре провайдера и неуклонное массовое проникновение IPv6 в глобальном Интернете.

Однако многим сервис-провайдерам придется столкнуться с проблемой нехватки IPv4 и задуматься над ее решением.

Существует два способа решения этой проблемы. Первый – это получение дополнительных адресов IPv4. Однако в недалеком будущем обращение к RIPE NCC или другой Региональной Регистратуре не даст желаемого результата ввиду отсутствия свободно распределяемого адресного пространства, и адреса будут перераспределяться между игроками путем купли-продажи, дарения, объединения и поглощения компаний и т.п. Трудно сказать, как будет развиваться этот сценарий и насколько объемным и ликвидным окажется рынок адресного пространства. В любом случае, второй способ – повышение эффективности использования адресного пространства с помощью технологии NAT (Network Address Translation), – является более реальной альтернативой или дополнительным решением. Этот сценарий показан на графике кривой розового цвета.

Но поскольку мы заговорили о технологии NAT, пожалуй стоит остановиться на ней поподробнее, поскольку эта технология является ключевой в моделях сосуществования IPv4 и IPv6.

Техническое отступление: как происходит передача данных в Интернете

Итак, прежде чем перейти непосредственно к разговору о будущем Интернета IPv6, давайте совершим краткий технический экскурс в техническую область и в общих чертах рассмотрим как же происходит передача данных в Интернете и какую роль играют адреса.

Работа Интернета основана на технологии пакетной коммутации без установления соединения. Структура пакета определена протоколом IP, и каждый пакет содержит IP-адрес отправителя и получателя. В задачу каждого узла сети (называемого также маршрутизатором) входит передача пакета, полученного от соседнего узла – к последующему. Выбор последующего узла происходит с помощью системы маршрутизации, благодаря которой маршрутизатор знает какому из своих соседей передать пакет с конкретным IP-адресом получателя.

Однако для пользователя передача данных происходит между его приложением и приложением получателя. Например, между вэб-браузером и вэб-сайтом. В этом случае можно представить, что существует виртуальное соединение между этими приложениями, по которому и происходит передача данных. Помимо IP-адресов отправителя (в данном случае – компьютера пользователя) и получателя (вэб-сервера) это соединение характеризуется дополнительными параметрами – так называемыми портами отправителя и получателя, которые можно рассматривать как локальные идентификаторы конкретных приложений на компьютере. Наконец, транспортный протокол (например, TCP или UDP) является пятым параметром, однозначно определяющим поток данных в Интернете в пределах ограниченного времени.

Эта особенность, а именно, что отправитель и получатель данных в действительности адресуются парой {IP-адрес, порт}, используется в технологии NAT (Network Address Translation), или более точно – NAT (Network Address & Port Translation). Другими словами, с помощью одного IP-адреса можно теоретически адресовать 65535 "соединений" – число, значительно превышающее потребности единичного пользователя. В этом случае устройство NAT для внешней сети будет выглядеть как компьютер с очень большим числом одновременно работающих приложений, в то время как на самом деле устройство NAT при передаче пакетов подставляет вместо порта и собственного IP-адреса (как адреса получателя с точки зрения внешних приложений) порт и локальный IP-адрес реального получателя. Обычно для адресации конечных устройств локальной сети, расположенной за устройством NAT используется специальное зарезервированное адресное пространство. Схема работы NAT показана на рисунке 2.

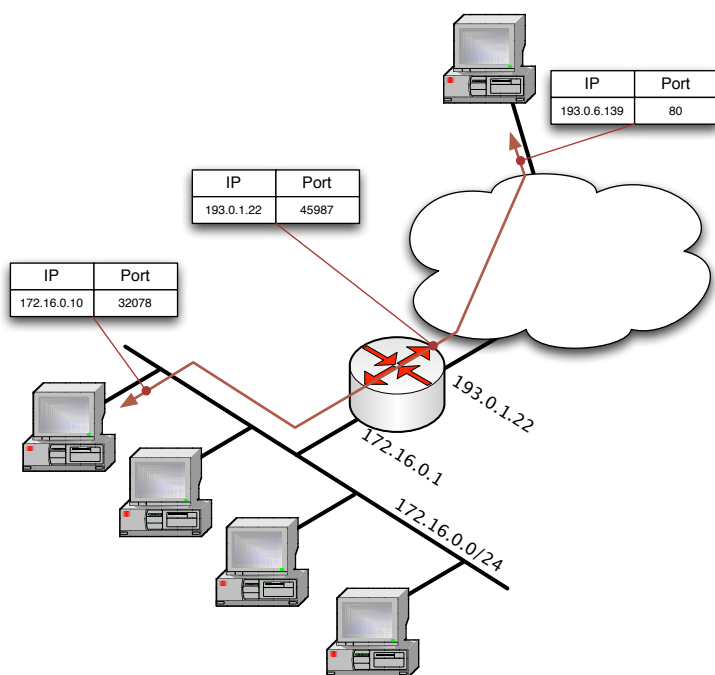


Рис. 2. Схема работы NAT

Насколько эффективен NAT? Это зависит от характера приложений, работающих на конечных устройствах и интенсивности их взаимодействия с глобальным Интернетом. На сегодня, компьютер обычного пользователя создает от 60 до 100 соединений с различными ресурсами глобального интернета. Дело в том, что многие приложения открывают более одного соединения. Это в большей степени относится к вэб-приложениям. Например Google Maps одновременно использует несколько десятков соединений. Но даже если эта цифра на порядок больше технология NAT позволяет более 60 пользователям совместно использовать один и тот же IP-адрес.

Звучит очень привлекательно. К сожалению, не все так радужно. Технология NAT содержит ряд серьезных недостатков, о которых мы поговорим позже. Здесь же отмечу, что NAT нарушает принцип "прозрачности" Интернета, о котором я говорил в предыдущих статьях. Помимо усложнения архитектуры сети, для полноценной работы некоторых приложений требуются дополнительные

средства, такие как STUN (RFC5389, <http://datatracker.ietf.org/doc/rfc5389/>), ICE (RFC5245, <http://datatracker.ietf.org/doc/rfc5245/>), TURN (http://ru.wikipedia.org/wiki/Traversal_Using_Relay_NAT, RFC5766, <http://datatracker.ietf.org/doc/rfc5766/>). Использование каскадов NAT, когда в сети за устройством NAT расположены также NAT со "вложенными" сетями, только усугубляет эти проблемы.

Переходные технологии сосуществования

Итак, технология NAT-мультиплексирования является одним из компонентов решения проблемы сосуществования двух протоколов, позволяя ослабить остроту нехватки адресов IPv4. Однако одной из основных проблем перехода к IPv6 является несовместимость его со своим предшественником – протоколом IPv4. Это означает, что устройство, поддерживающее только IPv6, не может непосредственно обмениваться данными с устройством IPv4. Виной этому является, скорее, протокол IPv4, который был изобретен для адресации нескольких десятков, может быть – сотен или тысяч, устройств Сети, и не предусматривал способа расширения.

План перехода «двойного стека» предполагал отсутствие устройств, «говорящих» только на одном из протоколов, другими словами – глобальное двуязычие. Плану этому не суждено было воплотиться в жизнь, поэтому для обмена данными между устройствами и сетями разных протоколов необходимо применение дополнительных технологий, точно также, как мы прибегаем к услугам переводчика для преодоления языкового барьера.

Давайте посмотрим, что же имеется в арсенале сервис-провайдеров.

Технологии туннелирования

Технологии туннелирования приходят на помощь, когда инфраструктура сервис-провайдера не поддерживает один из протоколов.

6to4

Технология 6to4 была стандартизована еще в 2001 году (RFC3056, <http://datatracker.ietf.org/doc/rfc3056/>) и с тех пор является наиболее распространенным методом для соединения изолированных островков IPv6 с другими такими же островами, а также глобальным Интернетом IPv6 через океан IPv4. Для этого используются автоматически создаваемые туннели.

Шлюз, или маршрутизатор 6to4, обеспечивает создание динамических туннелей путем инкапсуляции пакетов IPv6 в IPv4 для передачи через Интернет IPv4 к другому острову и декапсуляции входящего трафика. Для определения принимающего конца туннеля, шлюз извлекает адрес IPv4, который является адресом принимающего шлюза 6to4, из IPv6-адреса получателя.

Особенностью этого метода заключается в том, что все островки 6to4 совместно используют адресное пространство, определяемое префиксом 2002::/16. При этом, адресное пространство каждого островка определяется путем "присоединения" к 16 битам префикса 2002 32 бит IPv4-адреса шлюза 6to4. Например, если IPv4-адрес шлюза 193.0.7.5, то адресное пространство сети 6to4 определено префиксом 2002:c100:705::/48.

Для обеспечения связности с глобальным Интернетом IPv6 используются так называемые релеи 6to4. Это также шлюзы 6to4, однако они являются интерфейсом между сетями 6to4 и остальным Интернетом IPv6. Для избежания необходимости задания адресов релеев вручную, все они имеют один и тот же адрес – 192.88.99.1, который анонсируется с использованием технологии аникаст (anycast, <http://ru.wikipedia.org/wiki/Anycast>).

Схема работы системы 6to4 представлена на рисунке 3.

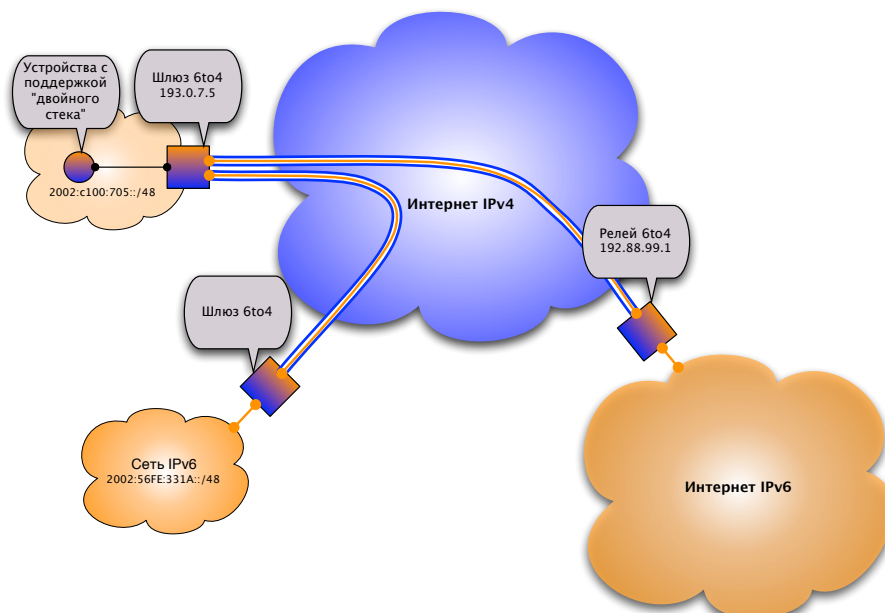


Рис. 3. Схема работы технологии 6to4

Хотя эта технология является наиболее популярной, намного опережающей подобные туннельные технологии как ISATAP и Teredo, ее применимость в основном ограничена пользователями-энтузиастами и небольшими корпоративными сетями. Для серьезных игроков больший интерес представляют технологии 6rd и DS-lite.

6rd

Одним из недостатков 6to4 является отсутствие контроля над релеем, обеспечивающим выход в глобальный IPv6. Поэтому невозможно гарантировать какие-либо параметры качества и связность, не говоря о том, что и выбор конкретного реля происходит автоматически, используя технологию аникаст.

На помощь здесь приходит метод 6rd (RFC5969, <http://datatracker.ietf.org/doc/rfc5969/>), о нем я немного писал в предыдущей статье. Эта технология решает проблему предоставления доступа к IPv6 пользователям провайдера широкополосного доступа без необходимости поддержки IPv6 в сети самого провайдера.

Во-первых, сеть 6rd использует собственное адресное пространство IPv6, полученное от Региональной Интернет Регистратуры. Это позволяет сервис-провайдеру анонсировать реальные IPv6-префиксы и, таким образом, более точно определять собственную политику маршрутизации.

Во-вторых, вся зона функционирования 6rd ограничена сетью сервис-провайдера. Используя терминологию 6to4, шлюзы 6rd встроены в оконечное оборудование пользователя, а релей также являются частью инфраструктуры сервис-провайдера.

Эти отличия показаны на рисунке 4.

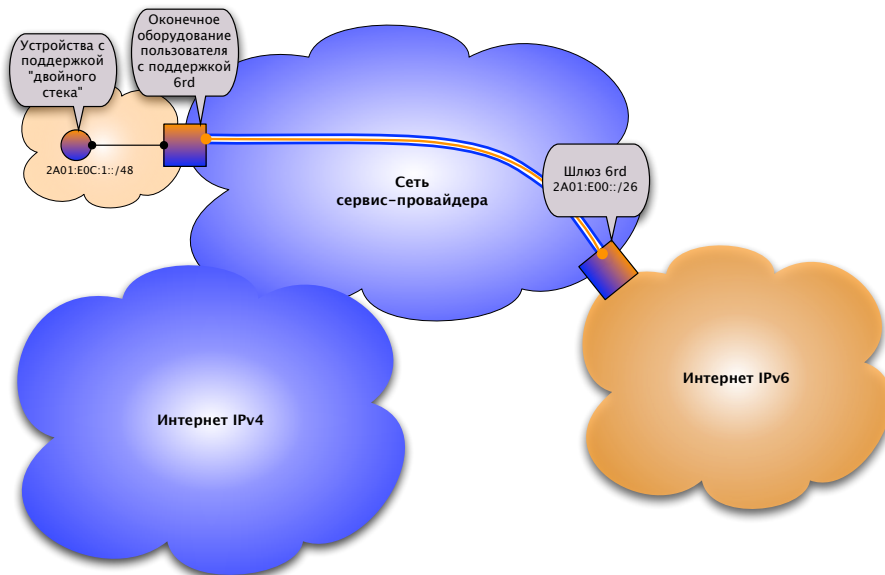


Рис. 4. Схема работы технологии 6rd

DS-lite

DS-lite (<http://datatracker.ietf.org/doc/draft-ietf-software-dual-stack-lite/>) в некотором смысле является зеркальной технологией по отношению к 6rd. DS-lite предполагает, что сеть провайдера полностью поддерживает IPv6, а туннели используются для передачи трафика IPv4 от сети пользователя к устройствам NAT сервис-провайдера. Также предполагается, что устройства сети пользователя поддерживают "двойной стек", а именно протокол IPv4 и IPv6.

Суть этого метода заключается в совместном использовании технологий туннелирования (инкапсуляция трафика IPv4 в пакеты IPv6) и централизованного NAT, или LSN (Large Scale NAT, также называемого CGN, Carrier Grade NAT), с целью обеспечения совместного использования ограниченного пула адресов IPv4 всеми пользователями сервис-провайдера. При этом обмен трафиком с ресурсами Интернет, доступными по протоколу IPv4, происходит с использованием этого протокола, а с ресурсами IPv6 – с использованием IPv6. Эта схема не предусматривает трансляции протоколов.

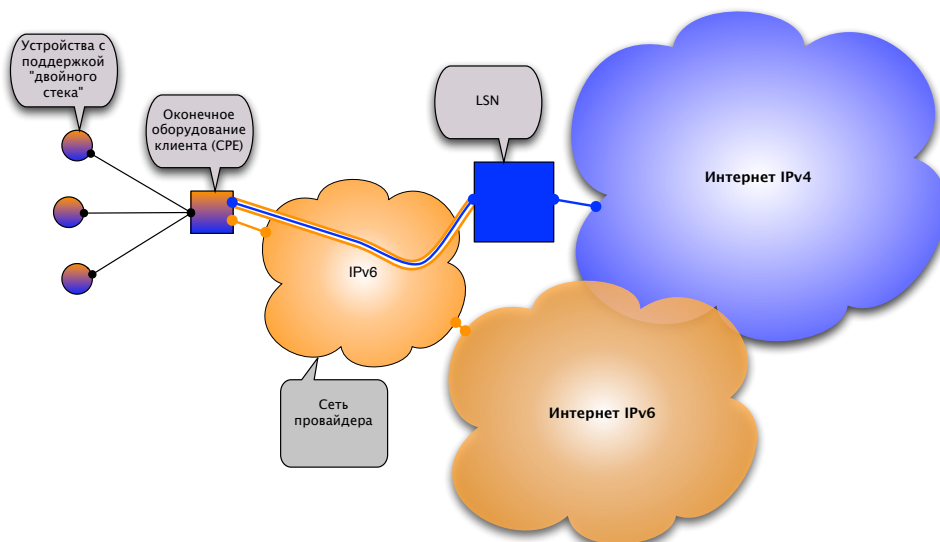


Рис. 5. Схема работы DS-lite

Как можно заметить из рисунка 5, на котором представлена схема работы DS-lite, обмен трафиком с ресурсами IPv6 происходит непосредственно, без использования каких-либо промежуточных технологий, например, туннелей.

В отношении IPv4 ситуация гораздо сложнее. Ввиду все более острой нехватки адресного пространства IPv4 в недалеком будущем, сегодняшняя широко используемая в сетях широкополосного доступа схема,

когда каждому пользователю сервис-провайдера предоставляется один публичный адрес IPv4, используемым устройством NAT пользователя для построения домашней локальной сети, не сможет быть эффективно применена.

Возможным решением этой проблемы (кстати, уже применяемым некоторыми сервис-провайдерами) является создание еще одного уровня NAT в сети сервис-провайдера. Хотя такая схема работает в общем случае, результатом ее применения являются существенные ограничения для многих сегодняшних и будущих приложений, а также сложность обслуживания.

Задачей DS-lite является исключение каскадирования устройств NAT, когда все устройства пользователей непосредственно взаимодействуют с центральным устройством NAT сервис-провайдера. В этом случае оконечное устройство пользователя не выполняет никаких функций NAT, а вместо этого обеспечивает создания туннелей к центральному NAT для каждого нового соединения между приложениями пользователя и сервисами Интернета.

В этом случае все пользовательские соединения, также как и в схеме каскадирования NAT, отображаются центральным LSN, но значительным преимуществом является большая прозрачность архитектуры и более высокая утилизация адресного пространства IPv4.

Говоря о прозрачности, одной из основных сложностей, связанных с применением NAT, является проблема контроля приложений за значениями порта и IP-адреса соединений, поскольку устройство NAT заменяет их на динамически присваиваемые. От этого зависит нормальное функционирование некоторых приложений, например, большинства мультимедийных интерактивных приложений. На сегодняшний день разработаны несколько механизмов решения этой проблемы, такие как STUN, ICE и TURN. Очевидно, что каскадирование устройств NAT усложняет ситуацию.

Отмечу, что технология DS-lite не предусматривает поддержку устройств, работающих только по протоколу IPv6. Для этого используются технологии трансляции.

Технология трансляции: NAT64 + DNS64

Логично предположить, что в недалеком будущем появятся устройства, поддерживающие только IPv6. Действительно, если мы говорим о масштабных мобильных, сенсорных или RFID сетях, необходимость поддержки двух протоколов усложнит и удорожит такие устройства.

Для взаимодействия таких сетей с Интернетом IPv4 необходимо применение трансляции адресов IPv6 в адреса IPv4 и обратно. Ввиду недостатка ресурсов IPv4, здесь, как и в случаях, рассмотренных выше, необходимо применение мультиплексирования потоков. По существу, в этой ситуации используются технологии централизованного NAT с внедрением дополнительной функции трансляции протоколов. Этот компонент еще называют NAT64 (<http://datatracker.ietf.org/doc/draft-ietf-behave-v6v4-xlate-stateful/>). Взаимодействие с другими сетями IPv6 происходит прозрачно. Эта архитектура показана на рисунке 6.

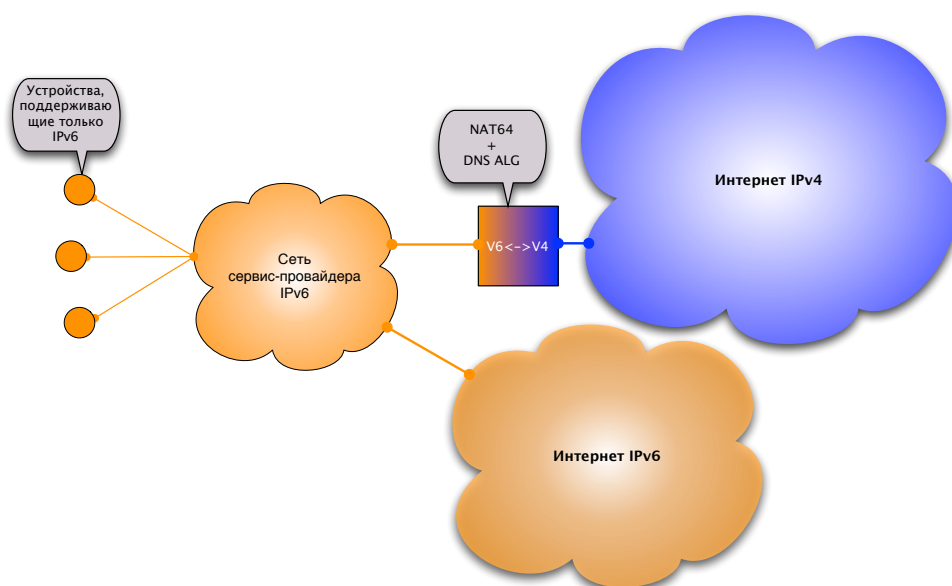


Рис. 6. Архитектура системы трансляции протоколов NAT64

Однако в данной схеме есть одна особенность, а именно необходимость дополнительной поддержки одного из наиболее критических приложений Интернета – системы доменных имен DNS.

Дело в том, что для большей части ресурсов Интернет запрос DNS вернет адрес IPv4. Поскольку сети, о которых идет речь, поддерживают только IPv6, такой ответ DNS вряд ли окажется полезным. Для решения этой проблемы используется дополнительный компонент – шлюз приложений (Application Layer Gateway, ALG). Суть его заключается в замещении адреса IPv4 в ответе DNS на синтезированный адрес IPv6, понятный клиенту, а также транслятору протоколов NAT64. Более подробно работу DNS ALG я рассмотрел в статье "Из жизни IP адресов. Перспективы протокола IPv4 и перехода к адресации IPv6".

Игроки и их потребности

Итак, до сих пор я употреблял общий термин "сервис-провайдер", различая их лишь по скорости роста и размеру. Однако проблемы и потребности, связанные с переходным периодом, в существенной степени зависят от конкретного вида деятельности провайдера. Например, стратегия транзитного оператора заметно отличается от стратегии провайдера широкополосного доступа, а корпоративную сеть нельзя сравнивать с сетью мобильного оператора. Давайте посмотрим на различные типы провайдеров, проанализируем проблемы, с которыми им возможно придется столкнуться, и оценим применимость существующих сегодня решений, о которых мы только что говорили.

Провайдеры транзита

Под провайдерами транзита я имею в виду сети, клиенты которых как правило самостоятельные сети со своим собственным адресным пространством. Услуги транзита, которые предоставляют такие операторы, обеспечивают этим клиентам глобальную связность.

Положение провайдеров транзита является наиболее выигрышным. Их собственные потребности в адресах IPv4 весьма скромны и в основном направлены на поддержку инфраструктуры. На сегодняшний день маршрутизация и передача трафика IPv6 является стандартной задачей, успешно решенной многими крупными и средними операторами.

Можно с уверенностью сказать, что проблемы переходного периода для операторов транзита не являются существенными.

Корпоративные сети

Многие корпоративные сети попадают в категорию сервис-провайдеров с умеренным ростом и достаточным запасом свободных адресов IPv4. То есть в категорию с довольно большими шансами переступить порог IPv4 (см. рис. 1) без особых дополнительных усилий. Даже если адресов IPv4 все же будет не хватать, в арсенале корпоративной сети имеется возможность реструктуризация сети и внедрения стандартного NAT-мультиплексирования.

Внедрение IPv6 хотя и является желательным, все же не является наиболее насущной задачей, поскольку в ближайшем будущем (и в течение многих последующих лет) IPv4 по-прежнему будет обеспечивать доступ к глобальным Интернет-ресурсам.

Необходимым является обеспечения IPv6-доступа к внешним ресурсам корпоративной сети, таким как, например, корпоративный веб-сайт. Но это задача ограниченная и достаточно тривиальная.

Провайдеры широкополосного доступа

Эти провайдеры обеспечивают широкополосный доступ к Интернету для "домашних" пользователей, с использованием кабельной или телефонной инфраструктуры доступа с помощью технологий DOCSIS и ADSL.

Для этой группы проблема нехватки адресов может встать достаточно остро. Провайдеры широкополосного доступа характеризуются очень большой пользовательской базой, порядок величины которой определяется числом домашних хозяйств в регионе обслуживания, а скорость роста во многих случаях является весьма значительной, особенно в регионах с большим потенциалом развития.

Для преодоления проблем переходного периода этим провайдерам скорее всего придется прибегнуть к уже обсуждавшимся технологиям централизованного NAT–мультиплексирования совместно с технологиями туннелирования DS–lite или 6rd. Это может потребовать достаточно значительного изменения инфраструктуры, включая системы обслуживания, мониторинга и биллинга. В большинстве случаев желательна также поддержка IPv6 пользовательскими оконечными устройствами (Customer Premise Equipment, CPE), например кабельными– или ADSL–модемами.

Все это говорит о том, что здесь требуется существенная подготовка и инвестиции. Несвоевременная модернизация инфраструктуры может существенно снизить эффективность инвестиций (например замена оконечного оборудования вне нормального цикла модернизации), ограничить возможность роста и снизить конкурентоспособность провайдера.

Дополнительным осложнением может явиться требование доступности отдельных услуг, предоставляемых в сети пользователя (т.н. домашний офис – SOHO), например вэб–сайтов, из глобального Интернета. Сегодня такая возможность обычно реализуется конфигурацией фиксированной трансляции определенных адресов и портов (т.н. port forwarding) на оконечном устройстве, которое находится под контролем самого пользователя. Новая архитектура потребует кооперации со стороны самого сервис–провайдера, обслуживающего LSN. Для автоматизации этого процесса в IETF в настоящее время разрабатывается протокол контроля распределения портов (Pinhole Control Protocol, PCP, <http://datatracker.ietf.org/doc/draft-ietf-pcp-base/>).

Мобильные операторы

Еще более серьезную проблему нехватка адресов IPv4 представляет для мобильных операторов. Это наиболее быстро растущая группа сервис–провайдеров и речь идет о десятках миллионов подписчиков. Если в случае широкополосного доступа размер клиентской базы пропорционален числу домашних хозяйств в регионе, то для мобильных операторов речь идет о населении региона или страны.

К тому же, по сравнению с широкополосным пользовательским доступом, услуга передачи данных менее насыщена. Например в развивающихся регионах, несмотря на значительное проникновение сотовой связи, мобильный Интернет только набирает обороты. Даже в развитых Европейских странах только 60% абонентов пользуются услугами передачи данных. Учитывая, что распространение услуги происходит по так называемой S–кривой, можно предположить, что скорость проникновения мобильного Интернета в сотовые сети будет только расти.

Во многих случаях технология двойного стека (например, используемая в DS–lite) является экономически нецелесообразной, поэтому наиболее перспективным является применение механизмов трансляции, когда мобильная сеть поддерживает исключительно IPv6, а для доступа к ресурсам, доступным только по IPv4, используется схема NAT64+DNS64.

Провайдеры распределенного контента и просто контент-провайдеры

Под "просто контент провайдерами" я имею в виду владельцев конкретного информационного ресурса, например вэб–сайта. Для существующих провайдеров проблемы нехватки адресов как таковой не существует, даже если развитие вэб–сайта потребует дополнительного адресного пространства, его достаточно легко "произвести" путем реструктуризации сети.

Проблемы же внедрения IPv6 во многом ограничиваются модернизацией (или просто конфигурацией) систем мониторинга, биллинга и т.п.

Наиболее целесообразным подходом для контент провайдеров является использование стандартной модели "двойного стека", когда ресурс доступен непосредственно как по протоколу IPv4, так и по протоколу IPv6.

Для провайдеров распределенного контента проблема переходного периода является более сложной.

Одной из причин является то, что потребность в дополнительном адресном пространстве для этих провайдеров по мере их развития будет оставаться актуальной. Несравненно менее острой, чем в случае с мобильными или операторами широкополосного доступа, но все же более значительной, чем для корпоративных сетей. Ведь для дополнительных кластеров, обеспечивающих доступ к контенту и расположенных в различных точках глобального Интернета, потребуется дополнительное адресное пространство.

Другая причина связана с доступом к контенту по протоколу IPv6, а именно пока что более низкая средняя производительность и параметры качества Интернета IPv6. Об этой проблеме я рассказывал в предыдущей статье на примере Google и Akamai.

Серьезность проблемы

Насколько серьезны проблемы переходного периода зависит не только от типа сервис-провайдеров, но также и от насыщенности и развитости рынка в регионе. Последнее определяет потенциальный рост сервис-провайдера, который является одним из факторов, определяющих потребность в дополнительных адресах IPv4.

Итак, давайте посмотрим на состояние дел в различных регионах земного шара. Для этого я обратился к статистическим данным на сайте <http://www.internetworldstats.com> и к статистическим источникам общего назначения.

Например в Германии с их 82 миллионами населения и 35 миллионами домашних хозяйств, уровень проникновения составляет 79%. Учитывая среднюю скорость роста за последние 10 лет (150%), потребность в дополнительном адресном пространстве IPv4 в год составит порядка $/12^1$ для провайдеров широкополосного доступа и $/12$ для мобильных операторов. Другими словами – $/11$ на всю страну. А с учетом мультиплексирования потоков с применением технологии NAT (принимая повышение эффективности в 64 раза) эта цифра окажется равной $/17$.

В то же время для России цифры еще менее радужны. Если верить статистике, в стране с населением в почти 140 миллионов насчитывается примерно 60 миллионов пользователей Интернета. При этом количество распределенных адресов IPv4 в этом регионе (<http://www.bgprexpert.com/addrspace2010.php>) составляет всего 35 миллионов. Это означает, что утилизация адресного пространства уже превышает 100% и использование технологий NAT носит масштабный характер. Это также означает, что получение дополнительных адресов, потребность в которых в год предположительно составляет порядка $/10$ для широкополосных операторов и $/13$ – для мобильных (с учетом текущего уровня использования передачи данных абонентами сотовой связи), практически невозможно путем реструктуризации внутренних или неиспользуемых ресурсов.

Еще более серьезной является ситуация в Китае и Индии, где потребность в адресном пространстве выражается цифрами $/6$ – $/7$! Даже с применением NAT-мультиплексирования цифра остается гигантской и выражается миллионами адресов IPv4.

Все это говорит о том, что, особенно для быстрорастущих экономических регионов, снижение остроты проблемы нехватки адресов IPv4 только с использованием NAT-мультиплексирования для повышения утилизации, является неэффективным даже на среднесрочном этапе. Более эффективной долгосрочной стратегией является снижение потребности за счет глобального внедрения IPv6 и, тем самым, уменьшение доли Интернета, доступного только по протоколу IPv4. Важным аспектом является то, что эта динамика является справедливой только для провайдеров, использующих переходные технологии сосуществования и обеспечивающих доступ как к ресурсам IPv4, так и IPv6.

Проблемы технологий сосуществования

Как мы увидели, все технологии сосуществования предусматривают применение NAT-мультиплексирования для IPv4, необходимое для того, чтобы "перешагнуть порог" дополнительного, но отсутствующего адресного пространства IPv4 (см. Рис. 1).

Однако масштабное использование NAT-мультиплексирования несет в себе существенное усложнение архитектуры и ряд серьезных проблем. О некоторых из них я уже писал в моей статье "Из жизни IP адресов. Перспективы протокола IPv4 и перехода к адресации IPv6", но здесь также остановлюсь на важных аспектах.

Приложения

Некоторые приложения не смогут нормально функционировать и потребуют дополнительных решений и поддержки (я уже упомянул это при обсуждении каскадирования NAT). К таким приложениям относятся протоколы предусматривающие инициацию входящих соединений, использующих predetermined порты (well known ports), фиксирующие значение адреса получателя или отправителя в передаваемых данных, а также предполагающие уникальность IP-адреса.

¹ Здесь и далее для обозначения размера адресного пространства IPv4 я буду использовать т.н. нотацию CIDR (Classless InterDomain Routing). Суть ее заключается в обозначении размера префикса и адресного пространства, которое он определяет с помощью знака / и числа битов. Например $/32$ обозначает один адрес IPv4, а $192.168.0.0/22$ соответствует блоку из 1024 адресов в диапазоне $192.168.0.0 - 192.168.3.255$. Количество адресов, соответствующее префиксу $/12$, определяется как $2^{32-12} = 2^{20}$, или порядка миллиона адресов.

Идентификация

Усложняется проблема идентификации пользователя. В новых условиях пользователь уже не может однозначно идентифицироваться IP адресом. Результатом может явиться необходимость модификации билинговых систем сервис провайдеров, изменение требований по хранению логов и т.п. Связанные с идентификацией пользователя системы профилирования, используемые провайдерами онлайн-рекламы, также не могут более рассчитывать на уникальность адреса IPv4.

Безопасность

Несколько факторов могут негативно влиять на безопасность. Например, ограничение возможного количества используемых портов отдельным пользователем или приложением может уменьшить степень случайности распределения портов, и, как следствие, увеличить вероятность атаки (например, атаки DNS Каминского). В дополнение, атака на отдельный адрес затронет также других пользователей. Верно и обратное – нежелательный трафик, источником которого является некоторый адрес, может быть атрибутирован нескольким пользователям.

Качество связи

Фрагментация пакетов возможно приведет к потере данных и ухудшению качества связи. Дополнительные устройства NAT могут являться причиной дополнительных задержек, а также представляют собой единую точку отказа.

Эти и другие проблемы тщательно анализируются в документе IETF «Issues with IP Address Sharing» <http://tools.ietf.org/html/draft-ietf-intarea-shared-addressing-issues>. Многие из этих проблем не новы, но масштабность их проявления в будущем потребует более сложных и дорогостоящих решений, чем сегодня.

Альтернативные сценарии развития

До сих пор мы рассматривали сценарий, когда основным протоколом Интернета будущего является IPv6. В этом сценарии движущими силами развития являются усложнение и удорожание инфраструктуры IPv4 и упрощение и удешевление поддержки IPv6. Последний фактор означает, в первую очередь, все большую доступность информационных ресурсов по протоколу IPv6 и, как следствие, уменьшение значимости IPv4. При достижении определенной критической массы развитие событий может приобрести характер цепной реакции, когда завершение перехода к протоколу IPv6 в глобальном масштабе произойдет очень быстро. Что является критической массой сказать трудно, но по оценкам некоторых экспертов 10% внедрения IPv6 может стать переломной точкой.

Однако данный сценарий работает только при условии, что сервис провайдеры внедрят и будут поддерживать IPv6 параллельно с существующей инфраструктурой IPv4, а значит будут готовы на эти дополнительные затраты переходного периода.

Тем не менее совсем не очевидно, что это условие будет выполнено. С момента опустошения пула адресов IPv4 основной проблемой, требующей решения, станет задача получения дополнительного адресного пространства для поддержки роста. Это возможно за счет покупки адресов, при достаточной ликвидности рынка купли-продажи адресов, практически несуществующего сегодня, или целых компаний, реструктуризации собственного адресного пространства и, наконец, повышение утилизации использования адресного пространства за счет внедрения технологий NAT-мультиплексирования. Любое решение будет стоить денег и дополнительные затраты, необходимые на внедрение IPv6 и не приносящие ни прибыли, ни уменьшения общих затрат в краткосрочном плане, могут быть просто неприемлемы для сервис-провайдера.

В то же время, для некоторых провайдеров, например для провайдеров широкополосного доступа, изменение архитектуры сети, необходимое для использования NAT-мультиплексирования, может быть воспринято как положительное развитие, обеспечивающее больший контроль за услугами, получаемыми клиентами, и, как следствие, возможность создания "новых" платных услуг. Например, открытие порта или расширение диапазона доступных портов может рассматриваться такими сервис-провайдерами как дополнительная услуга.

Если события будут развиваться по этому сценарию, шансы велики, что через некоторое время IPv6 уйдет в историю. А развитие, основанное на IPv4, будет ограничено, как размером адресного пространства, хотя и расширенного с помощью использования номеров портов, так и его текущим распределением. Поэтому, скорее всего, трансляция и мультиплексирование приобретут еще более сложный характер.

Сеть перестанет быть прозрачной, что существенно затруднит инновацию. Не думаю, что этот сценарий вселяет оптимизм.

Если возможность развития Интернета по этому сценарию во многом зависит от поведения провайдеров широкополосного доступа, то мобильные операторы могут обеспечить другой, диаметрально противоположный сценарий.

Вероятность развития второго сценария зависит от того, насколько быстро будет происходить проникновение услуги передачи данных в сотовых сетях. Напомню, что в отличие от широкополосного доступа, размер клиентской базы пропорционален населению региона, где степень проникновения сотовой связи на сегодняшний день во многих случаях близка или даже превышает 100% (несколько сотовых номеров на человека). И хотя в тех же регионах, и Россия находится среди них, процент использования услуги передачи данных по различным оценкам находится в диапазоне от 5 до 30%, эта цифра в короткий срок может подскочить до 60% (цифра, характерная для стран северной Европы) и выше. Инфраструктура в большинстве случаев готова, мобильные устройства поддерживают и все больше требуют (возьмите, например, современные смартфоны iPhone, Samsung, BlackBerry) наличие мобильного Интернета.

Абсолютные цифры такого роста впечатляют. Но также впечатляют сложность и дополнительные затраты на сопровождение систем адресной трансляции, основанных на технологии NAT64, о которой мы уже говорили. Другими словами, "порог" с рисунка 1, может оказаться для операторов слишком большим.

Но у мобильных операторов есть альтернатива. А именно, предоставлять только услуги, основанные на IPv6. Да, не все ресурсы будут доступны, но и затраты на предоставление мобильного Интернета изменятся незначительно. К тому же, для многих пользователей окажется приемлемой неполная функциональность Интернета, например доступность только Google и ресурсов, хранимых в его кэше, Facebook и Twitter. А возможность предоставления этих ресурсов по протоколу IPv6 при наличии спроса несомненна.

С другой стороны, стремительное появление пользователей, "разговаривающих" только на IPv6 послужит серьезным побудительным фактором поддержки IPv6 для провайдеров информационных ресурсов. Можно предположить, что и этот процесс будет носить лавинообразный характер.

Безусловно, такое развитие событий является наиболее предпочтительным. Данный сценарий позволит существенно сократить переходный период, упростить или по крайней мере не сильно усложнить архитектуру Сети.

Заключение

Какой из трех сценариев воплотится в будущем? Как изменится архитектура Интернета в результате этого перехода? На эти вопросы трудно дать однозначный ответ.

Однако очевидно, что переходный процесс потребует более сложных технологий и более "интеллектуальной" Сети и эти изменения вряд ли обратимы, даже если внедрение IPv6 закончится успешно. А это все больше отдаляет архитектуру Интернета от одного из фундаментальных принципов "прозрачности" и связанных с ним аспектов нейтральности Сети и ее инновационного потенциала. Но этот разговор – для следующей статьи.

Андрей Робачевский