Из жизни IP адресов. Перспективы протокола IPv4 и перехода к адресации IPv6

Андрей Робачевский

Технический директор RIPE NCC

Тридцать лет назад трудно было себе представить, что четырех миллиардов адресов будет недостаточно для сети Интернет. Сегодня же прогнозы показывают, что пул свободных адресов IPv4 будет исчерпан к середине 2012, всего через три года. А ведь каждое устройство в глобальной сети имеет свой уникальный IP адрес. Как это скажется на развитии Интернета, который сегодня в подавляющем большинстве базируется на адресах IPv4? К каким изменениям архитектуры Сети это приведет?

Последующая версия Интернет-протокола, IPv6, была призвана решить эти и ряд других проблем. «Была призвана», потому что по плану сегодня IPv6 уже должен был полностью заместить IPv4. По ряду технических и экономических причин этого не произошло. Но IPv6 по-прежнему рассматривается как основной протокол будущего Интернета, а переход к IPv6 - как основной фактор дальнейшего развития глобальной сети.

Однако, скорее всего этот процесс займет годы, в течение которых Интернет будет развиваться на фоне сосуществования двух протоколов.

Шестая версия протокола IP

История и стандарты

Текущая версия Интернет- или IP-протокола - фундаментального сетевого протокола Интернета, - IPv4 была разработана в 70-х годах прошлого столетия. Спецификация IPv4 была впервые опубликована в качестве стандарта IETF RFC791 в 1981 году. В то время Интернет назывался ARPANET, насчитывал несколько сотен хостов и находился под контролем Министерства Обороны США. С тех пор многое изменилось, но большая часть Интернет по-прежнему использует протокол и адресацию IPv4.

В 1981 году трудно было представить, что 32 бита адреса IPv4, позволяющие присвоить уникальный номер 4 миллиардам систем (компьютеров, маршрутизаторов и т.п.), является реальным ограничением. Однако уже к 1992 году масштабируемость и ограниченность адресного пространства IPv4 встала на повестку дня. Изменения в архитектуре маршрутизации и распределении адресного пространства под названием CIDR (Classless Inter-Domain Routing, Бесклассовая Междоменная Маршрутизация), которые были стандартизованы в 1993 году (RFC1518, RFC 1519), позволили существенно замедлить потребление адресов.

Однако предупреждение было принято к сведению и уже в начале 1994 года IETF начал работу над созданием новой версии протокола IP, позднее получившей название IPv6. Базовая спецификация было опубликована в 1998 году (RFC2460), окончательная версия структуры адресации IPv6 - в 2006 году (RFC4291).

Основные отличия IPv6

Размер адресного пространства

Размер адреса IPv6 128 бит. Чтобы лучше представить, насколько больше адресного пространства у IPv6, представьте следующую аналогию: если бы все адреса IPv4 уместились в iPod'е, то для IPv6 потребовался бы весь земной шар (http://blog.icann.org/2007/06/ipv6-the-ipod-and-the-earth)!

Помимо значительного увеличения адресного пространства предполагается, что IPv6 сможет поддерживать большее число уровней сетевой иерархии и более оптимальное с точки зрения маршрутизации и конфигурации распределение адресного пространства.

Оптимизация обработки

При разработке протокола IPv6, особое внимание было уделено оптимизации обработки пакетов на сетевом уровне. IPv6 предполагает наличие вложенных заголовков для различных расширений, например, для криптографической защиты данных. В то же время базовый заголовок IPv6 содержит минимальное число полей и имеет фиксированный размер.

Другой особенностью и отличием от IPv4 является отсутствие поддержки так называемой фрагментации пакетов. В случае IPv4 если маршрутизатор получает пакет, размер которого слишком большой для передачи через интерфейс, маршрутизатор производит фрагментацию - дробление пакета на более мелкие, в дальнейшем консолидируемые в исходный пакет получателем. Заголовок пакета IPv4 имеет соответствующие поля, поддерживающие эту функциональность.

В IPv6 фрагментация промежуточными устройствами запрещена. Если пакет IPv6 превышает допустимый размер для последующей передачи, маршрутизатор генерирует сообщение ICMP "Packet too big" (Слишком большой пакет) и посылает его обратно отправителю. В зависимости от приложения отправитель либо выбирает размер пакета, который позволит передачу на всем пути следования без фрагментации, либо дробит пакет самостоятельно. Как и в случае IPv4 консолидация фрагментированных пакетов входит в задачу получателя. Как следствие, передача пакетов IPv6 требует меньших затрат от промежуточного сетевого оборудования.

Автоконфигурация

Для протокола IPv6 была разработана так называемая система автоконфигурации без сохранения состояния (Stateless Autoconfiguration). Данный протокол позволяет различным устройствам, присоединенным к сети IPv6, получить доступ в Интернет без дополнительных средств - например, DHCP (Dynamic Host Configuration Protocol). Суть подхода заключается в том, что устройство получает адрес, состоящий из префикса сети и идентификатора устройства, автоматически сгенерированного с использованием MAC-адреса.

Защита данных

В протокол IPv6 изначально включена система безопасности, основанная на технологии IPsec. IPsec предусматривает два режима работы: транспортный режим и туннельный режим. В транспортном режиме производится защита (шифрование) данных пакета, но не заголовка. С точки зрения маршрутизации такой IP-пакет выглядит вполне обычно, а в задачу получателя входит декодирование содержимого пакета. При использовании туннельного режима данные всего пакета, включая заголовок, шифруются и инкапсулируются в новый пакет. Получатель, указанный в этом новом пакете, является окончанием защищенного канала, или туннеля, и в его задачу входит извлечение изначального пакета и последующая доставка. Дополнительно, пакет IPv6 содержит заголовок аутентификации для определения подлинности и отсутствия модификации данных пакета.

Мобильность

Поддержка мобильности в IP означает, что оконечное устройство может изменить свое местоположение в сети и IP адрес без потери существующих связей, соответствующих потокам передачи данных. Для обеспечения этой функциональности, мобильные устройства используют отдельные IP адреса, по которым устройства всегда доступны при передаче данных. За авторизацию мобильного устройства в сети и обеспечение соответствия между реальным и мобильным IP адресами отвечает т.н. Домашний Агент - устройство, расположенное в "домашней" сети мобильного пользователя. Основным отличием реализации мобильности между IPv4 и IPv6 является то, что в случае IPv4 передача данных также производится (туннелируется) через Домашнего Агента, в то время как в IPv6 Домашний Агент обеспечивает только контролирующие функции (авторизацию и обеспечение соответствия между реальным и мобильным адресами), а передача данных производится между отправителем и получателем напрямую. Такой подход обеспечивает более оптимальную маршрутизацию данных и, как следствие, повышение качества передачи.

Приведенные особенности протокола IPv6 призваны улучшить производительность, качество и защиту передачи данных. Однако опыт практического внедрения протокола IPv6 показывает, что указанные улучшения весьма незначительны и во многих случаях не используются. Напротив, операторы зачастую прибегают к проверенным практикой методам, разработанным для сетей IPv4. Так, например, для

конфигурации подключенных устройств используется система DHCP, а в области защиты данных технология IPsec может быть использована в IPv4 почти также эффективно, как и в IPv6. Эффективная поддержка multihoming (подключение клиента к нескольким сервис-провайдерам для увеличения надежности) в IPv6 потребовала отдельного решения и существенно усложнила элегантную структуру эффективной маршрутизации, считающейся одним из преимуществ IPv6. В результате на практике multihoming реализуется аналогично IPv4, что, конечно, приводит к неоправданному росту таблиц маршрутизации.

В среде сетевых операторов существует мнение, что единственное преимущество IPv6 – это расширение доступного адресного пространства.

Ограниченность ресурсов IPv4

Сегодня стремительное развитие Интернет достигло точки, когда большая часть адресов IPv4 уже распределена. Это трудно было себе представить двадцать лет назад и тогда адресные ресурсы щедро распределялись блоками по 16 миллионов адресов, т.н. сетями класса A. Ситуация изменилась к середине 90-х, когда была внедрена технология CIDR, позволившая выделять блоки адресов, соответствующие реальным потребностям. В это же время были образованы Региональные Интернет Регистратуры (РИР, RIR, Regional Internet Registries), ответственные за распределение адресов и номеров автономных сетей в соответствии с правилами, разработанными региональным Интернет-сообществом. Сначала был образован RIPE NCC (1992) и APNIC (1993), и далее ARIN (1995), LACNIC (2002) и AfriNIC(2005). Зона обслуживания Регистратур показана на рисунке 1. За обслуживание центральной регистратуры отвечает организация IANA.

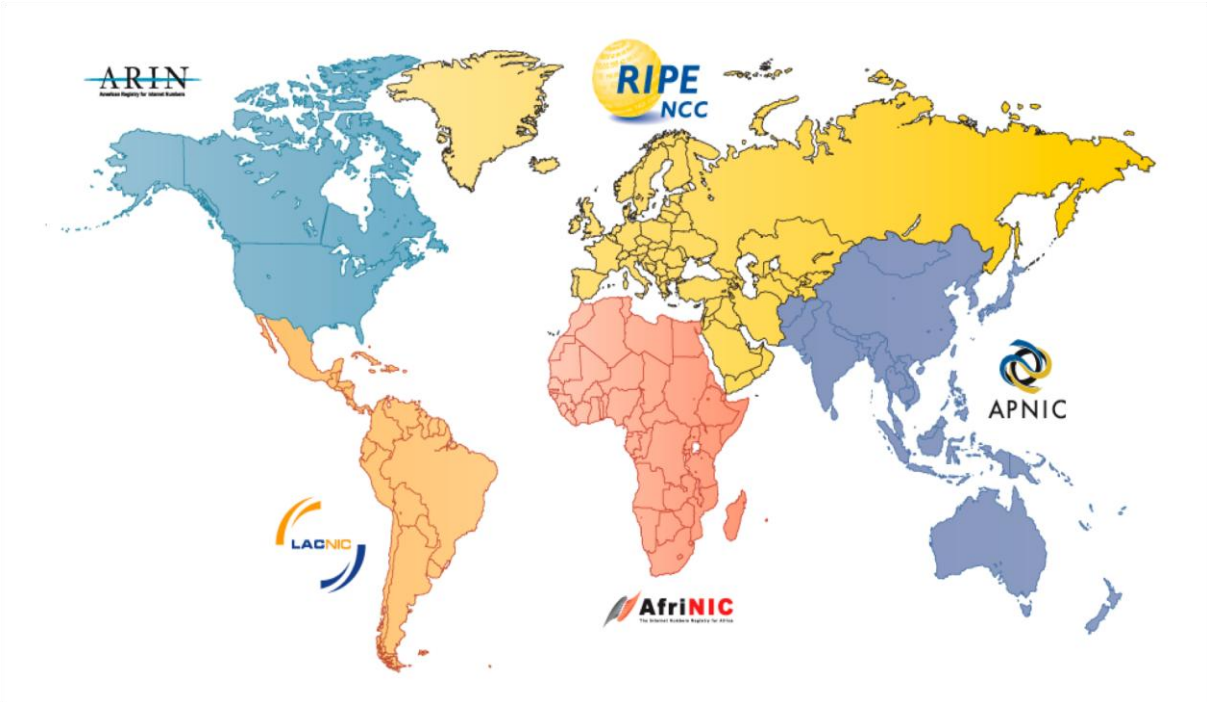

Рис 1. Региональные Интернет Регистратуры и зоны их обслуживания

Все это позволило увеличить эффективность распределения адресного пространства и отдалить сроки, когда все свободные адреса IPv4 будут распределены. Сегодня прогнозы показывают, что этот момент наступит уже через несколько лет.

Опустошение пула свободных адресов IPv4 не произойдет внезапно. Можно выделить как минимум три фазы этого процесса:

1. Сначала закончатся свободные адреса, которые IANA распределяет РИРам
2. Далее подойдут к концу адреса, которые РИРы распределяют своим членам - Локальным Интернет Регистратурам и сервис-провайдерам
3. Наконец на уровне ЛИРа все свободные адреса будут также распределены между подключенными клиентами.

Динамика уменьшения свободного адресного пространства IPv4 анализируется многими организациями и экспертами. Большинство сходится во мнении, что пул свободных адресов на уровне IANA закончится приблизительно в 2011 году. Джеф Хьюстон (APNIC) разрабатывает модели динамики распределения и ежедневно обновляет прогноз опустошения свободного пула на вэб-сайте http://www.potaroo.net/tools/ipv4/index.html.

Вопросы внедрения IPv6

Как уже отмечалось, наиболее важным фактором внедрения протокола IPv6 является преодоление ограниченности адресных ресурсов IPv4. IPv6 предлагает практически неограниченный с сегодняшней точки зрения запас адресов, что рассматривается как один из критических факторов развития приложений будущего - повсеместное распространение мобильного Интернета, пиринговых приложений (например bittorrent, игровых приложений) и т.п.

В то же время протокол IPv6 не является совместимым с протоколом IPv4. Это означает, что устройство, поддерживающее только IPv6, не может взаимодействовать с устройством IPv4 напрямую. Этот факт существенно усложняет процесс перехода к IPv6.

Другим фактором, объясняющим недостаточные темпы внедрения IPv6, является отсутствие сильных побудительных факторов. Проблема, свойственная многим технологическим изменениям, заключается в том, что на начальных стадиях внедрения, пока не достигнут массовый уровень, преимущества (как технические, так и экономические) технологии проявляются лишь в незначительной степени. После достижения "критической массы" ситуация радикально меняется в пользу новой технологии и ее внедрение форсируется ясными и более естественными факторами. Такой критической точкой можно будет считать момент, когда подсоединение нового IPv6 устройства будет дешевле, чем устройства, поддерживающего протокол IPv4. Однако в настоящее время внедрение IPv6 означает инвестиции, которые не являются краткосрочно прибыльными.

Незначительный уровень внедрения также отрицательно влияет на общую осведомленность относительно IPv6, на отсутствие необходимого уровня квалификации и знаний в этой области, а также на недостаточно эффективный процесс разработки и улучшения оборудования через цикл реального использования и поддержки.

Побудительные факторы

Долгосрочная потребность в адресных ресурсах

IPv4 не может удовлетворить долгосрочную потребность в адресных ресурсах в том виде, к которому мы привыкли сегодня. Прогнозы показывают, что пул свободных адресов будет исчерпан на уровне Региональных Интернет Регистратур уже в 2012 году. Однако новые и будущие приложения и устройства, требующие постоянной связи с Интернет - мобильные устройства, сенсорные и RFID сети, распределенный компьютинг и игровые приложения – только увеличивают потребность в адресных ресурсах.

Следует ожидать, что получат развитие механизмы (некоторые существуют уже сегодня), которые позволят Интернету развиваться в условиях недостатка адресов IPv4, и в то же время с использованием IPv4. Например, более эффективное использование адресного пространства с использованием технологии NAT. Процессы перераспределения ресурсов, например, посредством купли-продажи адресов, также позволят продлить жизнеспособность IPv4. Однако эти механизмы не являются решением проблемы, а только предлагают некоторую отсрочку. В то же время эти изменения приведут к усложнению архитектуры сети, ограничениям на возможные сетевые приложения и как следствие - увеличение затрат на сопровождение и уменьшение динамики и инноваций в развитии Интернета. Результатом этих изменений может явиться увеличение стоимости и одновременно уменьшение ценности интернет-услуг для пользователей.

Требования соответствия

В некоторых случаях решения о внедрении IPv6 в общественном секторе экономики (например, требование для правительственных учреждений) является сильным побудительным факторам внедрения IPv6 для поставщиков услуг и оборудования, работающими с этими учреждениями.

Примерами таких инициатив может служить разработанный правительством США т.н. IPv6 profile – требования к сетевому оборудованию в плане поддержки IPv6, предназначенного для использования в IT инфраструктуре правительства США, а также требование к федеральным агентствам США продемонстрировать возможность поддержки IPv6 до 30 июня 2008 года. Министерство по связи и Интернет Японии издало рекомендации по поддержке IPv6 в государственных онлайн системах для обеспечения внедрения IPv6 в информационных системах различных министерств. Европейский Союз разработал программу i2010, содержащую план по широкому внедрению IPv6 в Европе к 2010 году.

Конечно, не все из существующих программ и инициатив одинаково эффективны в стимулировании индустрии по внедрению IPv6, но они могут являться одним из сильнейших мотивов, особенно, когда непосредственные экономические преимущества не очевидны.

Уменьшение долгосрочных операционных затрат

Благодаря гораздо большему размеру доступного адресного пространства сервис-провайдеры могут упростить структуру сетей и исключить использование технологий NAT. В результате пользовательские приложения будут иметь возможность установления непосредственной связи друг с другом (так называемый принцип end-to-end). Это, в первую очередь, важно для поддержки пиринговых приложений, таких как Bittorrent и Skype.

Поддержка мобильных приложений

Помимо более эффективной поддержки мобильных приложений, IPv6 практически не накладывает ограничений на размер сети. Это может являться критическим фактором, учитывая, что требование быть всегда подключенным к сети передачи данных для мобильных устройств означает постоянно присвоенный IP адрес.

Сценарии развития сетей

В условиях существенного недостатка адресных ресурсов IPv4 и отсутствия критической массы внедрения IPv6, долгосрочное развитие сетей потребует нового архитектурного подхода.

Очевидно, что основной услугой сервис-провайдеров является предоставление клиентам доступа к информационным ресурсам Интернет. В то же время с большой вероятностью можно предположить, что к моменту исчерпания свободных адресов IPv4 значительная часть ресурсов будет все же доступна только по протоколу IPv4. Это означает, что реальным требованием по-прежнему остается связность с Интернетом IPv4. В условиях нехватки или отсутствия свободных адресов IPv4 это является достаточно серьезной проблемой.

Традиционный подход

Основной проблемой перехода от IPv4 к IPv6 является несовместимость двух протоколов. Клиент IPv6 не может общаться с клиентом, поддерживающим только IPv4, напрямую.

В недалеком прошлом представлялось, что решением этой проблемы является внедрение т.н. "двойного стека", когда компьютеры сети поддерживают оба протокола и являются подключенными как к сети IPv4, так и к сети IPv6. Данное разделение является логическими и

физически используется одна и та же сетевая инфраструктура. Для доступа к ресурсам IPv4 используется протокол IPv4, а к ресурсам IPv6 - IPv6. Все достаточно просто, но...

Темпы внедрения IPv6 оказались незначительными. План "двойного стека" сработал бы, если бы в ближайшем будущем можно было бы констатировать, что подавляющее большинство компьютеров Интернета имеют доступ как к IPv4, так и к IPv6. В этом случае можно было бы просто отключить поддержку IPv4 и - чудо! - Интернет перешел бы на новый протокол. Этого не случилось. И вряд ли случится ввиду нехватки в недалеком будущем адресов IPv4, необходимых для обеспечения перехода по схеме "двойного стека".

Итак, сетевые операторы не спешат с внедрением IPv6, поскольку пока есть в наличие адреса IPv4. А к моменту отсутствия свободных адресов IPv4 "двойной стек" для новых подключений станет невозможен. Конечно, Интернет будет продолжать работать и развиваться. Но для долгосрочного развития необходимо решение двух основных задач - предоставление доступа к ресурсам IPv4 для новых пользователей и параллельное внедрение IPv6 как реальное решение проблемы роста.

Тут есть несколько вариантов. Общим среди них является увеличение эффективности использования адресов IPv4.

Мультиплексирование

Одним из хорошо известных способов борьбы с нехваткой адресных ресурсов является технология мультиплексирования потоков IP путем задействования дополнительных 16 бит поля порта заголовка IP. Наиболее распространенным вариантом данной технологии является трансляции сетевого адреса и порта (NAPT или просто NAT, Network Address and Port Translation).

Дело в том, что потоки данных в Интернете уникально идентифицируются 4 параметрами: IP адресом и портом получателя и IP адресом и портом отправителя. В традиционном исполнении внутренняя сеть за устройством NAT использует расширенное адресное пространства (обычно используются т.н. "частные адреса") и исходящие IP-потоки транслируются в потоки с использованием ограниченного числа "глобальных" адресов и номеров портов. Такая же трансляция происходит и в обратном направлении. Таким образом, теоретически с помощью одного глобального IP адреса можно идентифицировать около 65 тысячи различных потоков. В среднем, однако, один пользователь одновременно использует только около 70-100 различных потоков (например, приложение Google Maps открывает около 20-30 различных потоков с компьютером пользователя) - незначительную часть теоретического предела. Незадействованные номера портов могут быть использованы для мультиплексирования.

Примером применения технологии NAT является расширение домашней сети пользователей кабельного сетевого провайдера. Сегодня типичной является ситуация, когда каждый клиент получает как минимум один IPv4 адрес. За этим адресом он волен строить свою собственную сеть

(домашнюю или офисную) с использованием NAT. Вероятнее всего, что эта ситуация изменится в будущем и несколько клиентов будут совместно использовать один адрес IPv4.

Для реализации новой архитектуры, схематически представленной на рисунке 2, предполагается использовать два новых типа устройств:

- Широкомасштабный NAT (LSN, Large Scale NAT) и
- Маршрутизатор с распределением портов (PRR, Port Reduction Router).

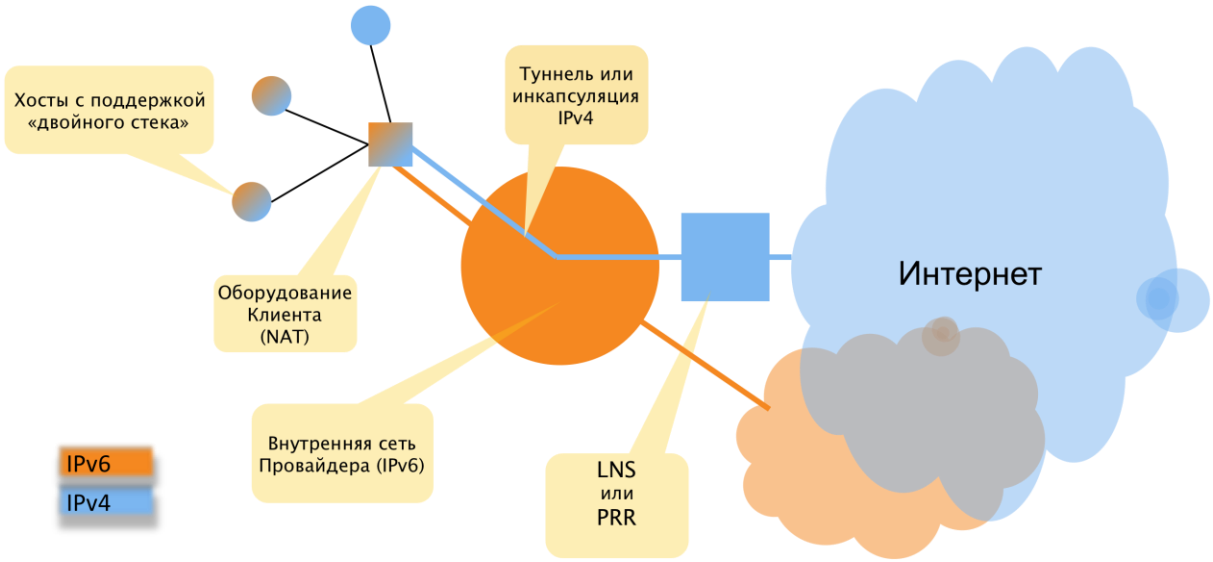

Рис. 2. Предоставление доступа с использованием мультиплексирования потоков

Устройство LSN отличается от традиционного NAT возможностью поддержки очень большого числа потоков и производительностью трансляции портов и адресов. LSN призван также следить за распределением адресов и портов, не позволяя отдельным клиентам узурпировать этот ресурс или отрицательно влиять на работу других клиентов. Процесс трансляции адресов в сетях этой архитектуры показан на рисунке 3.

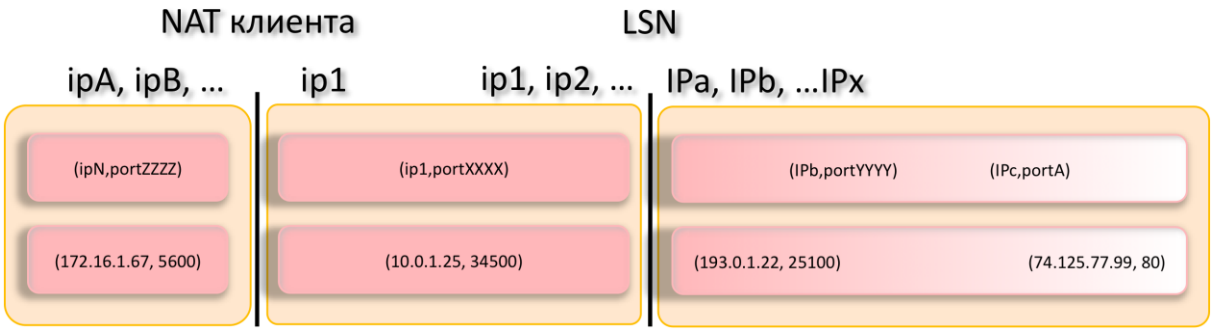

Рис. 3. Адресная трансляция с применением LSN

Другим решением совместного использования адресных ресурсов является выделение клиентам фиксированного адреса IPv4 и определенного диапазона номеров портов. Данный поход является основой новой архитектуры, реализуемой с помощью PRR и нового поколения маршрутизаторов клиента, способного обмениваться информацией с PRR относительно выделенных номеров портов. Преимуществом данного

подхода является больший контроль за доступными адресами и портами со стороны клиента и возможность прозрачного обмена данными между конечными приложениями. Схема мультиплексирования PRR показана на рисунке 4.

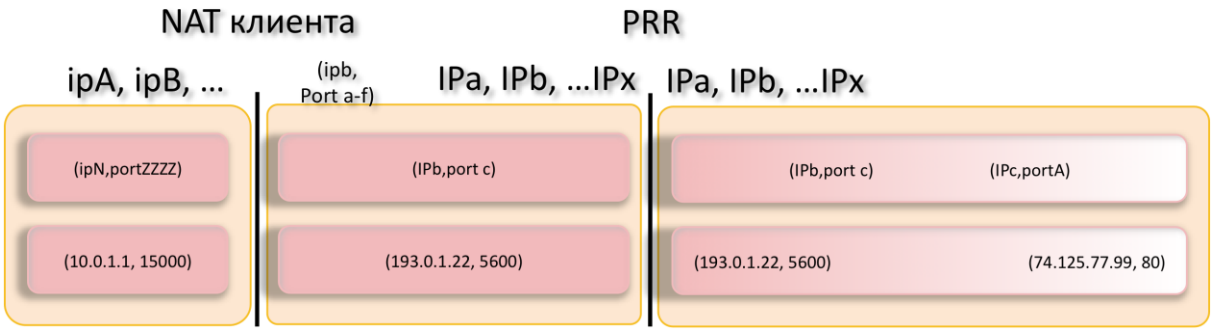

Рис. 4. Адресная трансляция с применением PRR

Внедрение IPv6

Казалось бы, рассмотренная архитектура делает внедрение IPv6, строго говоря, необязательным. В конце концов, сегодня 99% ресурсов Интернет доступны только по протоколу IPv4. Однако следует отдавать себе отчет, что предложенная архитектура является только временным решением и не столь отдаленном будущем приведет к тем же проблемам, которые мы решаем сегодня. Поэтому внедрение IPv6 является критическим фактором успешного долгосрочного развития Интернет.

В рассмотренных выше сценариях предполагается, что параллельно с обеспечением доступа к Интернету IPv4 усиленными темпами продолжается внедрение IPv6 в сетях и конечных устройствах клиентов. Таким образом, большая часть конечных устройств поддерживает как IPv4, так и IPv6 – или "двойной стек". При этом в условиях нехватки IPv4 ситуация меняется в лучшую сторону для IPv6, усиливая побудительные факторы внедрения этого протокола. Точнее говоря, ситуация меняется в худшую сторону для IPv4 вследствие усложнения архитектуры системы доступа по протоколу IPv4 и связанных с этим проблем.

Рассмотрим эти проблемы подробнее.

Проблемы

Многие приложения, которые прозрачно работают сегодня, потребуют дополнительных решений и поддержки. Хотя накоплен значительный опыт взаимодействия различных приложений с NAT, не все сегодняшние решения будут успешно работать в новых условиях. Примерами являются приложения, зависящие от предопределенных номеров портов (well known ports) и получающее все более широкое распространения приложения UPnP.

Увеличение числа уровней трансляции, более динамичное и краткосрочное выделение ресурсов (IP адресов и номеров портов), большее число приложений, где как клиент, так и сервер расположены за устройствами типа NAT, все это может отрицательно влиять на качество предоставляемых услуг и вероятнее всего увеличит стоимость их сопровождения для сервис-провайдера.

Такие вопросы как безопасность и надежность потребуют более сложных и дорогостоящих решений, чем сегодня.

Также 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.

При этом сети IPv6 во многом лишены этих проблем. Для сервис-провайдера использование клиентом инфраструктуры IPv6 будет означать меньшую нагрузку на мультиплексирующие компоненты IPv4, а для клиента большая гибкость, контроль и качество услуг.

Трансляция протоколов

До сих пор предполагалось, что устройства поддерживают протокол IPv4. Однако 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. При условии, конечно, что при необходимости эти устройства смогут общаться с Интернетом IPv4.

Для взаимодействия таких сетей с Интернетом IPv4 предполагается 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 будут использованы технологии, рассмотренные в предыдущих секциях - LSN и RPP, с внедрением дополнительной функции трансляции протоколов. Этот компонент еще называют NAT64. Взаимодействие с другими сетями IPv6 будет происходить прозрачно. Эта архитектура показана на рисунке 5.

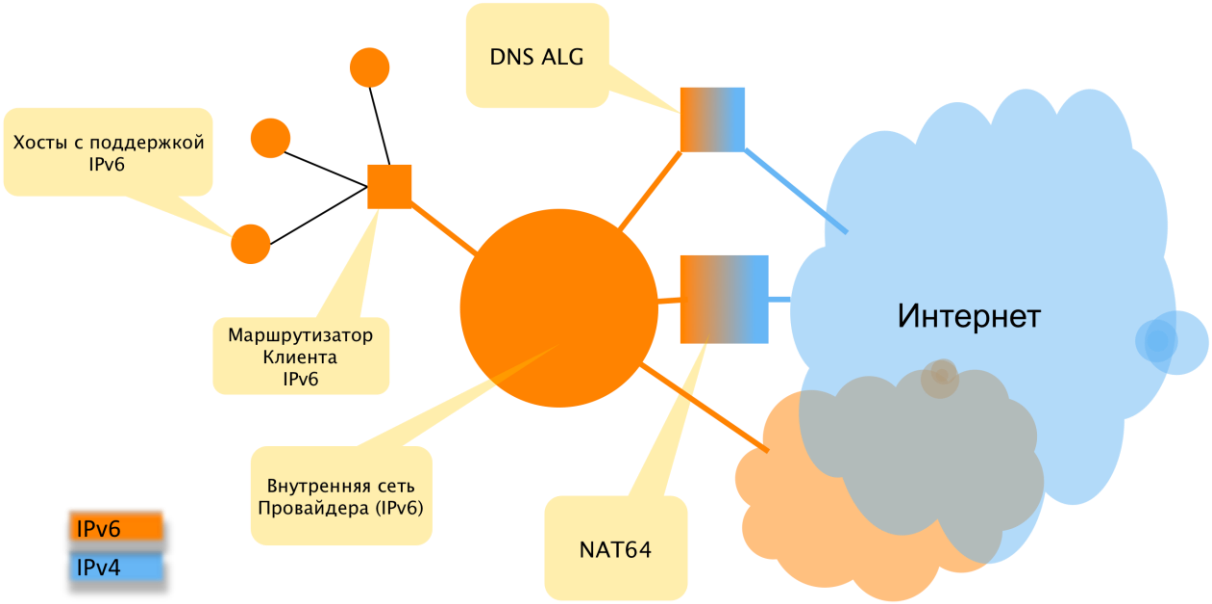

Рис. 5. Архитектура сети с трансляцией протоколов

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

Действительно, нормальная работа в Интернет немыслима без DNS. Всякий раз, когда мы набираем имя веб-сайта или посылаем электронную почту, эта система берет на себя задачу трансляции имени в цифровой адрес протокола IP (IPv4 или IPv6), необходимый для осуществления связи между компьютерами в сети.

В то же время для большей части ресурсов Интернет запрос DNS вернет адрес IPv4. Хотя механизм трансляции протоколов позволит клиенту получить доступ к ресурсам IPv4, учитывая, что клиент не поддерживает IPv4, такой ответ DNS вряд ли окажется полезным.

Для решения этой проблемы используется дополнительный компонент - шлюз приложений (Application Layer Gateway, ALG). Вообще говоря, этим термином называют широкий набор устройств и решений, позволяющих различным приложениям преодолеть ограничения, накладываемые устройствами типа NAT. Здесь же мы рассмотрим решение для приложений DNS.

Суть его заключается в замещении адреса IPv4 в ответе DNS на синтезированный адрес IPv6, понятный клиенту и, как мы увидим далее, транслятору протоколов NAT64.

Как обычно, перед началом связи, клиент посылает запрос локальному DNS серверу. В нашем случае его роль выполняет ALG. ALG производит разрешение запроса, и, допустим, получает IPv4 адрес искомого ресурса. Но в ответе клиенту ALG подставляет синтезированный адрес IPv6. По существу, этот адрес состоит из предустановленного префикса, известного как ALG, так и NAT64, и IPv4 адреса ресурса. Теперь, когда клиент попытается установить связь с ресурсом, NAT64 поймет, что клиент использует синтезированный адрес и преобразует

его в исходный IPv4 адрес получателя. Схема работы ALG показана на рисунке 6.

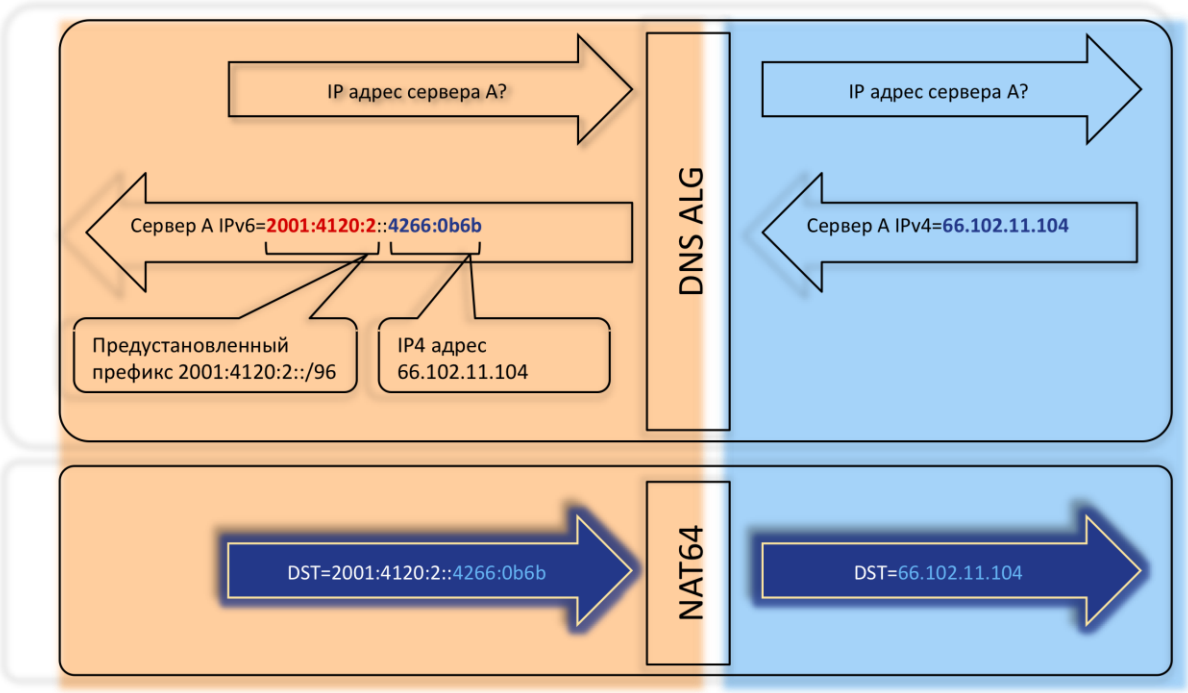

Рис. 6. Схема работы DNS ALG

Текущие решения и разработки IETF

Архитектурные решения, рассмотренные в этой статье, являются основным фокусом обсуждения ряда рабочих групп IETF. Наиболее значительными являются группы BEHAVE и SOFTWIRES. Вопросы сосуществования двух протоколов и эффективного внедрения IPv6 также обсуждаются в рабочей группе V6OPS, а также промежуточных встречах IETF, посвященных данной теме.

Рабочая группа SOFTWIRES занята стандартизацией методов обнаружения, управления и инкапсуляции для соединения сетей IPv4 с использованием сетей IPv6 и наоборот. Такие соединения-туннели получили название softwires. Группой рассматриваются две основные архитектуры – звездообразные и сетевые. В первом случае сети или отдельные клиенты осуществляют соединения точка-точка через сети другого протокола (например, сети IPv4 через транзитную сеть IPv6) с концентратором. Во втором случае связь осуществляется между несколькими островными сетями одного протокола в пространстве сети другого.

Рабочая группа BEHAVE документирует различные схемы использования и режимы работы устройств NAT, при которых поведение таких устройств не зависит от конкретного приложения и является, таким образом, максимально предсказуемым. Конечной целью этой работы является поддержка архитектуры, обеспечивающей переход к протоколу IPv6.

Заключение

Быстрое уменьшение свободного пула адресов IPv4 и незначительные темпы внедрения IPv6 не оставляют надежды на переход к новому протоколу с помощью стандартного "двойного стека", как изначально предполагалось. Это означает, что к моменту исчерпания свободного пула, IPv6 не сможет представлять рабочей альтернативы для дальнейшего развития Интернет.

Тем не менее, Интернет будет продолжать работать и развиваться. Источником уверенности является факт, что утилизация распределенных ресурсов IPv4 невысока, как с точки зрения неиспользуемого адресного пространства, так и с точки зрения возможностей расширения адресного пространства за счет номеров портов на основе технологий мультиплексирования потоков данных.

Однако это всего лишь дополнительное время и будем надеяться, что оно будет использовано для создания реальной альтернативы - повсеместного внедрения IPv6. Основные решения уже существуют, часть из них в стадии обсуждения, часть уже реализуется в оборудовании и внедряется в сетях.

Мнения, представленные в статье, не обязательно отражают официальную позицию RIPE NCC