

IPv6: вчера, сегодня, завтра

(Часть I)

Интернет - поистине удивительный феномен! Трудно переоценить его инновационный потенциал, и в то же время Интернет крайне консервативен и с большой неохотой реагирует на изменения. Работа Сети основана на взаимодействии и кооперации между сервис-провайдерами, и, тем не менее, Интернет демонстрирует яркий индивидуализм, когда дело доходит до усилий на благо всего сообщества.

Парадоксы этой уникальной экосистемы можно отчетливо увидеть в истории протокола, который должен стать протоколом будущего Интернета - IP версии 6. О нем и пойдет речь в этой статье.

На самом деле - это три статьи под общим названием "IPv6: вчера, сегодня, завтра", каждая из которых посвящена определенному периоду, связанному с IPv6. В первой статье, "вчера", мы обернемся назад, чтобы увидеть истоки IPv6, его возможности и связанные с ним надежды, а также проанализируем, почему спустя десятилетие уровень проникновения IPv6 очень мал.

В следующей статье, "сегодня", я хотел бы предложить вам взглянуть на процесс внедрения IPv6 более позитивно. Неизбежное опустошение пула свободных адресов IPv4 является стимулом многих успешных программ реального использования IPv6. Мы остановимся на нескольких примерах того, как операторы планируют переход к протоколу IPv6.

Наконец, в статье "завтра" я попробую заглянуть в будущее, хотя хочу сразу предупредить, что даром ясновидения не обладаю. Несмотря на то, что внедрение протокола IPv6 является необходимым условием долгосрочного развития открытого Интернета, в непосредственном будущем основной проблемой многих сервис-провайдеров может стать продолжающаяся потребность в дополнительных адресах IPv4. Победит ли IPv6 в этих условиях или станет жертвой корпоративного эгоизма?

И.А.Бродский когда-то сказал: "Настоящему, чтобы обернуться будущим, требуется вчера". С этого вчера мы и начнем.

Истоки

Если вы думаете, что протокол IPv6 является "новым" - это не совсем так. Базовая спецификация этого протокола была опубликована 12 лет назад (RFC2460, <http://datatracker.ietf.org/doc/rfc2460/>), а работа над его созданием началась в начале девяностых годов прошлого столетия.

Работа эта, как это ни покажется странным, была вызвана проблемой нехватки адресного пространства. И это почти 20 лет назад! Тогда эта проблема была на время решена изменениями архитектуры маршрутизации - CIDR (Classless Inter-Domain Routing, RFC 1518, <http://datatracker.ietf.org/doc/rfc1518/>) и соответствующими изменениями в распределении адресного пространства (RFC1519, <http://datatracker.ietf.org/doc/rfc1519/>), обеспечившие значительно более эффективное его использование.

Также интересно отметить, что начало этой работы ознаменовалось конфликтом, который привел к ревизии процесса принятия решений в IETF, что в то время означало - в Интернете. То, что сегодня называется размытым термином Internet Governance.

Итак, в 1991-92 годах IETF и все техническое сообщество было серьезно озабочено проблемами нехватки адресного пространства с одной стороны и неудержимого роста таблиц маршрутизации - с другой. Для анализа этих проблем и выработки решений была специально сформирована группа ROAD (ROuting and ADressing, Маршрутизация и Адресация). Группа выработала конкретные краткосрочные рекомендации (такие как, например, CIDR), однако достичь консенсуса относительно долгосрочных решений, в частности в области увеличения адресного пространства, группе не удалось.

В июне 1992 года комитет IESG (IETF Engineering Steering Group) рассмотрел эти предложения и рекомендовал более глубокое обсуждение возможных решений с целью лучшего понимания последствий и модели переходного периода (RFC 1380, <http://datatracker.ietf.org/doc/rfc1380/>). В то же время, новые предложения как решить проблему большего адресного пространства, продолжали поступать.

Двумя неделями позже IAB провел рабочее совещание в рамках которого выработал собственные рекомендации (<http://www.ripe.net/ripe/maillists/archives/ripe-list/1992/msg00001.html>). В отличие от IESG, IAB считал, что опасность исчерпания адресных ресурсов слишком велика, чтобы позволить длительный эволюционный процесс выбора лучшего решения. По мнению IAB IETF должен был начать активно работать над одним из рассматривавшихся решений, а именно IPv7 (так IAB назвал новый протокол), основанный на протоколе CLNP - межсетевой протокол модели OSI, который использует 160-битную адресацию, описанный в стандарте ISO 8473 Международной Организации по Стандартизации (ISO, International Organization for Standardization).

Эти рекомендации вызвали бурю протеста. Критике подверглись как технические качества предложения, так и сам поступок, который был воспринят как волюнтаристское решение IAB и грубое нарушение процесса принятия решений в IETF. Отягощающим обстоятельством явился также факт, что предложение было основано на одном из протоколов конкурирующего семейства OSI, активно поддерживаемого в то время многими государствами и крупными традиционными телекоммуникационными компаниями. Предложение IAB рассматривалось как передача контроля над одним из фундаментальных протоколов Интернета - IP в руки ISO.

Одним из последствий этого инцидента явилось уменьшение роли IAB в процессе стандартизации и полный пересмотр процесса выбора членов IAB и IESG. Этот процесс, который существует и по сегодняшний день, предусматривает номинацию кандидатов из международного технического сообщества независимым Номинационным Комитетом, члены которого случайно выбираются из добровольцев - участников IETF.

Другим последствием стал выбор нового протокола, IP следующего поколения, или IPng, следуя традиционному процессу IETF "снизу-вверх". За основу было взято одно из многочисленных предложений - SIP (Simple Internet Protocol). Впоследствии ему был присвоен номер "6".

Архитектура

С разработкой и внедрением IPv6 связывали большие надежды. И хотя изначально IPv6 был призван решить проблему нехватки адресного пространства протокола IP, в конце девяностых - начале этого века эта проблема не стояла так остро. Изменения в системе маршрутизации и более рациональная политика распределения адресного пространства, воплощенная Региональными Интернет-Регистратурами (Regional Internet Registries, RIR), способствовали существенному замедлению потребления адресов IPv4.

В то же время IPv6 по-прежнему рассматривался многими как возможность обновить архитектуру Интернета, вернуть утраченную простоту и начинавший размываться принцип прозрачности (end-to-end principle). Этот один из ключевых архитектурных принципов стоит рассмотреть немного подробнее.

Суть принципа прозрачности состоит в том, что "интеллект" сосредоточен в оконечных

устройствах, которые используют прозрачную сеть для обмена данными. Прозрачность сети заключается в отсутствии фильтрации или модификации данных, в том числе и контрольной информации, например заголовков пакетов. Такая архитектура, в корне отличавшаяся от традиционных телефонных сетей, в которых "интеллектуальная" сеть передает данные между простыми устройствами, в многом определила инновационный потенциал Интернета и его бурное развитие.

В самом деле, при таком подходе создание новых приложений и услуг не требует модификации сети или каких-либо согласований с сервис провайдером и находится полностью в руках разработчика. Внедрение новых приложений и, соответственно, новой функциональности Интернета, не требует модификации самой Сети, ее фундаментальных технологий, таких как сетевые и транспортные протоколы, и может быть произведено независимо с минимальными затратами. В этом суть инновации Интернета.

Однако некоторые решения, призванные отдалить проблему нехватки адресов IPv4, существенным образом исказили эту элегантную архитектурную концепцию. Наряду с долгосрочным планом решения проблемы - разработкой нового протокола на смену IPv4 и уже упоминавшимся изменением в системе маршрутизации CIDR, в 1993 году было предложено еще одно решение, призванное существенно увеличить эффективность использования глобальных адресов IP - трансляция адресов, или NAT (Network Address Translation).

Решение это, впервые описанное в RFC1631 (<http://datatracker.ietf.org/doc/rfc1631/>), являлось простым и одновременно эффективным. Оно было основано на наблюдении, что в пользовательской сети (например, в сети организации) интенсивность обмена трафиком между компьютерами внутри сети значительно превышает обмен трафиком с глобальными внешними ресурсами. Соответственно, в каждый момент времени только часть компьютеров сети обменивается данными с глобальным Интернетом и требует меньше глобальных IP адресов, чем общее число компьютеров в сети. В дальнейшем это решение было доработано и включило также трансляцию номеров портов (своего рода адресов приложений на конкретном компьютере), что позволило повысить эффективность использования глобальных адресов в десятки, а то и в сотни раз.

К сожалению, у этого решения есть одна большая проблема - оно нарушает принцип прозрачности сети. В частности, приложения больше не знают свой глобальный IP адрес и порт, так как это решение теперь принимает сеть, а точнее устройство NAT.

Некоторые приложения не могли работать в условиях NAT и требовали разработки дополнительных средств. Но для большинства приложений NAT не представлял проблем. Более того, помимо более рационального использования адресного пространства, NAT предоставлял сетевым администраторам ряд полезных функций: простота адресного плана сети, его независимость от сервис-провайдера, большая защищенность сети ввиду экранирования реальной топологии и доступа к конкретным компьютерам. Все это обеспечило успех этой технологии и ее широкое распространение.

Это, однако, не вызывало особого энтузиазма в IETF, - "запятнанный" нарушением принципа прозрачности, NAT надолго остался "золушкой" в мире Интернет-технологий. Наряду с решением проблемы нехватки адресного пространства раз и навсегда, протокол IPv6 был призван восстановить чистоту и простоту архитектуры Сети и обеспечить ее дальнейшее развитие.

К светлому будущему

Помимо этих "идейных" соображений, предполагалось, что ряд полезных функций, отсутствующих у IPv4, сделают протокол IPv6 привлекательным для сетевых операторов и обеспечат его повсеместное внедрение. Более подробно я рассказал об этих функциях в статье "Из жизни IP адресов".

Конечно, самым очевидным преимуществом IPv6 является существенно увеличенный размер адресного пространства. Размер адреса IPv6 составляет 128 бит, в четыре раза больше, чем у его предшественника, что экспоненциально увеличивает количество адресуемых устройств. Согласно Википедии, если все адреса IPv6 разделить поровну между всеми жителями Земли сегодня, то каждый из нас получит столько же адресов, сколько атомов в тонне угля! Поистине неограниченное количество, хотя это когда-то считалось справедливым и для IPv4.

Протокол IPv6 полностью интегрирован с протоколом IPsec, обеспечивающим защищенность данных на уровне IP, то есть "сквозную" защищенность между оконечными устройствами.

Также в протокол были интегрированы такие функции как автоконфигурация, оптимизация контрольной информации и поддержка мобильной связи.

Государственная поддержка

Протокол IPv6 был взят за основу при разработке нескольких государственных программ в Японии, Южной Корее, Европейском Союзе, а также в Индии и Китае. Все эти программы ставили целью создание масштабной информационной инфраструктуры на основе Интернета и, таким образом, занятие передовых позиций в глобальном информационном обществе и повышение конкурентоспособности. Протокол Интернета нового поколения - IPv6 - как нельзя лучше подходил для этих целей. Создание опорной инфраструктуры на основе IPv6 предлагало практически неограниченные возможности для повсеместного проникновения Интернета в дома конечных пользователей, бизнес и государственные учреждения.

Так, например, IPv6 стал частью национальной стратегии Японии в области информационных технологий и Интернета, так называемой стратегии e-Japan. В частности, стратегия предполагала полный переход на протокол IPv6 к 2005 году. Для достижения этой цели государство использовало различные средства - от значительного финансирования разработок и исследований в области IPv6, до специальных налоговых льгот и масштабных образовательных программ, стимулирующих переход на новую технологию.

Примерно в то же время, переход на IPv6 был обозначен как один из приоритетов в построении единого информационного пространства Европейского Союза. Основной упор делался на развитие мобильной связи на основе технологии 3G и IPv6 с его колоссальным объемом адресного пространства подходил как нельзя более кстати. В послании Еврокомиссии Совету Европы и Европарламенту в 2002 году, в частности говорилось, что внедрение 3G на основе IPv4 представляет серьезный риск ввиду ограниченности числа адресов, недостаток которых станет критичным уже к 2005 году (http://www.ec.ipv6tf.org/PublicDocuments/com2002_0096en01.pdf).

Участие государства в процессе внедрения IPv6 в США было отчасти связано с объявленной США войной с терроризмом и кибер-терроризмом в частности. Дело в том, что одной из особенностей IPv6 считалась более высокая защищенность передачи данных. Хотя в реальности IPv6 не многим более защищен, чем IPv4, факт более интегрированной поддержки протокола IPsec, явился одним из ключевых в принятии Министерством Обороны США в 2003 году программы перехода к IPv6 к 2008 году (<http://www.defense.gov/news/Jun2003/d20030609nii.pdf>).

Утраченные иллюзии

На фоне пропагандистских усилий Региональных Интернет Регистратур и других "I*-организаций" (IETF, ISOC, ICANN и т.д), государственной поддержки и угрозы опустошения пула свободных адресов IPv4, пожалуй самой острой несбывшейся надеждой оказались темпы внедрения IPv6. Спустя десятилетие с момента создания

протокола уровень его распространения не превышает нескольких процентов. (<http://labs.ripe.net/Members/mirjam/content-ipv6-measurements-compilation-part-2/>, <http://www.potaroo.net/ispcol/2010-04/ipv6-measure.html>).

Давайте попытаемся понять причины такой ситуации.

Начнем с того, что само нововведение не было таким уж революционным. Изменение ограничивалось протоколом IP, не затрагивая все остальные уровни протоколов - транспортные (TCP, UDP) и протоколы приложений. Электронная почта осталась электронной почтой, а веб-страница отображается одинаково, независимо от того доступен ли сайт по протоколу IPv4 или IPv6. По-существу, основным изменением было увеличение длины адреса в четыре раза и соответствующее колоссальное увеличение адресного пространства.

Слухи о повышенной безопасности IPv6 оказались явно преувеличенными. На практике, технология IPsec, создавшая этот своего рода миф, может также быть использована для протокола IPv4. Более того, ввиду незначительного внедрения IPv6, свое основное приложение IPsec нашел в протоколе IPv4, ни в чем не уступающему в этом отношении IPv6!

Полезность других функций, таких как автоконфигурация и поддержка мобильности во многих случаях не смогли перевесить прагматичный консерватизм сетевых архитекторов и операторов. 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, почти так же, как в IPv4. Задача поддержки multihoming (подключение клиента к нескольким сервис-провайдерам для увеличения надежности) в IPv6 потребовало отдельного решения и существенно усложнила элегантную структуру эффективной маршрутизации, считающейся одним из преимуществ IPv6. В результате на практике multihoming реализуется аналогично IPv4, путем анонсирования собственных префиксов обоим сервис провайдерам, что, конечно, приводит к неоправданному росту таблиц маршрутизации.

Отражение этих несбывшихся надежд относительно IPv6 видно в краткой сравнительной характеристике двух протоколов, сделанной как-то одним из сетевых инженеров - "на 92 битов больше и никаких чудес".

Но при этом три фактора оказались критическими для IPv6.

Во-первых, IPv6 несовместим с IPv4. Это означает, что устройство, поддерживающее только IPv4, не может непосредственно обмениваться данными с устройством IPv6. Это, скорее, недостаток IPv4, который не предусматривает расширяемости, но потерпевшим стал IPv6. Отсутствие совместимости означает невозможность постепенного внедрения, когда сети переходят на новый протокол, примерно так же, как мы обновляем программное обеспечение на нашем компьютере. Может показаться, что так и происходит и постепенно все больше сетей поддерживают IPv6, но это не так. Внедрение IPv6 требует построение параллельной инфраструктуры и сети, даже если обе реализуются теми же устройствами. Эта параллельная сеть требует затрат, но, увы, пока что не дает никаких дополнительных преимуществ.

Во-вторых, протокол IPv6 является протоколом низкого уровня (уровень Интернет в модели TCP/IP, двумя уровнями ниже протоколов Приложений). Согласно самой архитектуре протоколов, приложениям должно быть безразлично, какой именно протокол выполняет функции этого уровня. Соответственно и рядовой пользователь, движущая сила рынка, абсолютно безразличен к проблеме внедрения IPv6. По большому счету, протокол IPv6 как таковой не обеспечивает ни большей скорости, ни качества или защищенности передачи данных, что делает предоставление IPv6 как дополнительной услуги коммерчески неоправданным. В результате и сервис-провайдеры до настоящего времени не демонстрируют особого энтузиазма в отношении IPv6.

Наконец, IPv6 является относительно новой и менее отлаженной технологией, поэтому начальные затраты на сопровождение инфраструктуры IPv6 могут оказаться существенным. Это и потребность в более опытном персонале, и покупка более дорогостоящего оборудования. В то же время на начальном этапе внедрения инфраструктура может обладать худшими показателями как в отношении связности и пропускной способности ввиду неоптимальной глобальной связности IPv6, так и, как ни парадоксально, в вопросах безопасности ввиду большего количества недоработок в программном обеспечении. В результате наиболее прагматичным решением является как можно более позднее начало внедрения IPv6, когда и затраты ниже, и опыта больше, что мы и наблюдаем сегодня.

Уровень внедрения IPv6 в сегодняшнем Интернете не превышает нескольких процентов. Однако динамика его распространения за последние несколько месяцев вселяет определенную надежду. Успеет ли IPv6 достичь критической массы или станет жертвой коллективного эгоизма? Об этом мы поговорим в следующих статьях.

Андрей Робачевский, Технический директор RIPE NCC

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