Путевые заметки: RIPE 62

Наконец-то конференция RIPE опять проходила в Амстердаме. Хотя посещение новых мест является источником новых впечатлений, кажется все были рады встретиться опять в Краснопольском, который так и не дождался капитального ремонта.

Но сама конференция как всегда принесла новые впечатления. О них я и расскажу вкратце в этой статье.

Тема дня - IPv6

Вопросы внедрения и использования протокола IPv6 стали темой целого дня пленарных докладов. Неудивительно, ведь запас свободных адресов IPv4 подходит к концу, а уровень проникновения IPv6 по-прежнему мал.

На неискушенного участника некоторые выступления могли произвести двойственное впечатление. С одной стороны, да, долгосрочной альтернативы IPv6 вроде бы нет, а с другой стороны, здесь - ошибка, там - неполадка, тут - эксперименты и исследования. На самом деле не все так страшно и IPv6 в стандартных ситуациях вполне безобиден и готов к использованию. Но более сложные сети требуют больших усилий и осторожности. Например, топология связности в IPv6 и IPv4 могут существенно различаться вследствие применения туннелей, экспериментальных или запасных линков и т.п., что представляет проблему, например, в сетях распределения контента. В сетях широкополосного доступа трудностью является отсутствие или недостаточная поддержка требуемой функциональности IPv6 в пользовательских устройствах доступа. Наконец, в точках обмена трафика, где объем трафика IPv6 является существенным в абсолютных величинах, некоторые недоработки в оборудовании "вылезают" наружу. Но, в общем и целом, даже при наличии отдельных недочетов, лучше начинать внедрение сейчас, пока уровень трафика составляет от долей до пары процентов и даже серьезная неполадка не явится катастрофой, а будет, скорее, темой для презентации на следующей конференции RIPE.

IPv6 в глобальной системе маршрутизации

Итак, как же обстоят дела с IPv6 на сегодняшний день? Для ответа на этот вопрос Герт Дёринг (Gert Döring) представил анализ глобальной системы маршрутизации сетей IPv6. Доклады на эту тему Герт делает на конференциях RIPE уже на протяжении многих лет, рассматривая динамику внедрения iPv6 сквозь призму таблиц маршрутизации, и всегда находит интересные факты и особенности.

Тенденция роста числа префиксов IPv6, анонсируемых в Интернете, за последние 30 месяцев оставалась практически неизменной - устойчивый, хотя и слабый, экспоненциальный рост. Но начиная с этого года рост этот значительно усилился, как видно из графика на рисунке 1. Похоже, операторы осознали, что нехватка адресов IPv4 - не шутка. Еще одна приятная неожиданность - по числу анонсируемых префиксов IPv6 Россия стоит на четвертом месте в Европе после Германии, Великобритании и Нидерландов (рисунок 2).

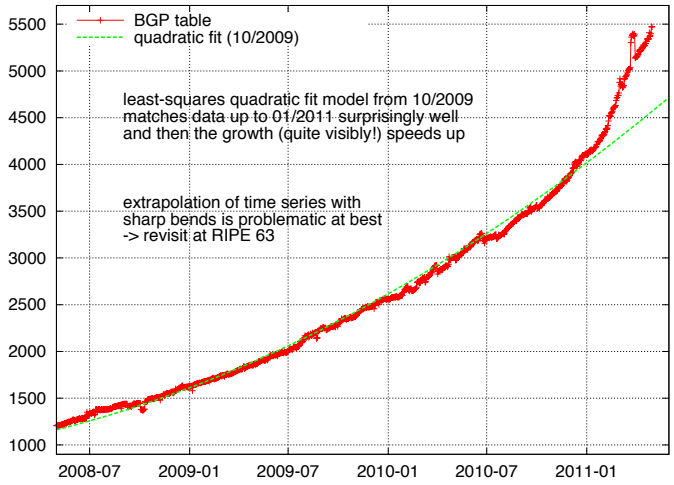

Рисунок 1. Динамика роста числа префиксов IPv6, анонсируемых в Интернете
(источник: презентация Герта Дёринга «IPv6 Routing Table Overview»,
http://ripe62.ripe.net/presentations/45-R62-v6-table.pdf)

Но все же, хотя динамика обнадеживает, степень внедрения IPv6 в сравнении с IPv4 очень мала – менее 10% сетей в Интернете используют IPv6.

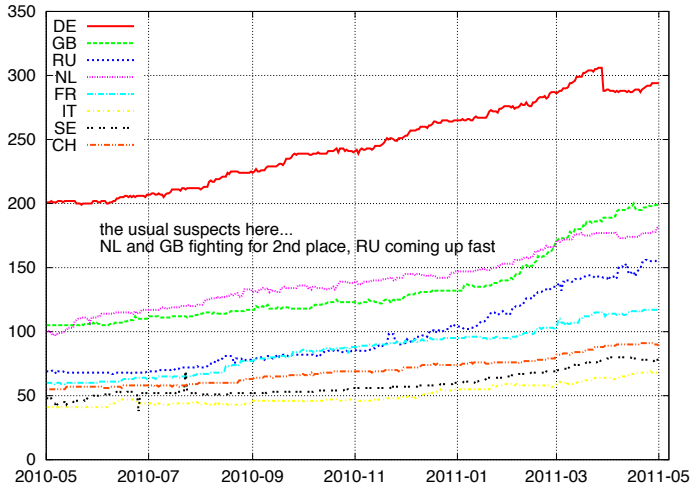

Рисунок 2. Ведущие страны по числу анонсируемых префиксов IPv6
(источник: презентация Герта Дёринга «IPv6 Routing Table Overview»,
http://ripe62.ripe.net/presentations/45-R62-v6-table.pdf)

IPv6 в оборудовании

Если ваша сеть не входит в эти 10%, будем надеяться, что поддержка IPv6 хотя бы является частью плана развития сети. В этом смысле очень полезным для вас может оказаться документ ripe-501 "Requirements For IPv6 in ICT Equipment "(http://www.ripe.net/ripe/docs/ripe-501), содержащий требования по поддержке IPv6 в ИТ-оборудовании. В основном рассчитанный на правительственные учреждения и крупные предприятия он также полезен для любой организации, осуществляющей закупку нового оборудования. Документ перечисляет обязательную и желательную функциональность со ссылкой на соответствующие стандарты (а стандартов – предостаточно, как видно из рисунка 3) для четырех классов оборудования: серверы и хосты, коммутаторы 2 уровня, маршрутизаторы и коммутаторы 3 уровня, а также устройства безопасности (экраны, устройства инспектирования трафика и т.п.).

Документ оказался очень полезным и уже переведен на несколько языков. В то же время, работа над документом продолжается. Причиной этому – появление новых стандартов, необходимость описания других сетевых элементов – мобильных устройств, оконечное пользовательское оборудование, программное обеспечение и т.п. О проблемах актуализации этого документа и его структуре шла речь в докладе Ян Жорж (Jan Žorž).

- RFC 2460, RFC 4291, RFC 3484(bis), RFC 4193, RFC 4443, RFC 3315, RFC 4862, RFC 1981, RFC 4861, RFC 4213, RFC 6214, RFC 3596, RFC 2671, RFC 3226, RFC 4605, RFC 2401, RFC 2406, RFC 2402, RFC 4306, RFC 4718, RFC 2407, RFC 2408, RFC 2409, RFC 3775, RFC 5555, RFC 4877, RFC 5095, RFC 4884, RFC 3971, RFC 4941, RFC 3736, RFC 2474, RFC 3140, RFC 3972, RFC 4301, RFC 4303, RFC 4302, RFC 3411, RFC 3412, RFC 3413, RFC 3414, RFC 3810, RFC 4821

Рисунок 3. "Tag cloud" стандартов IETF по IPv6
(Источник: презентация Яна Жоржа «RIPE-501bis", http://ripe62.ripe.net/presentations/48-ripe-501bis.pptx)

IPv6 не для всех

Наличие адресов и поддержки IPv6 в сети еще не означает, что IPv6-связность соответствует нормам качества сегодняшнего Интернета. Ошибки конфигурации маршрутизации, неоптимальная связность, использование экспериментальной инфраструктуры, – все это может привести к тому, что для пользователей применение протокола IPv6 выражается в низкой производительности или недоступности тех или иных ресурсов Интернета. Проблема осложняется тем, что в большинстве случаев при наличии поддержки IPv6 в пользовательской сети приложения выберают именно этот протокол для связи с ресурсами, доступными по IPv6. Для пользователя это может означать, например, что Google стал очень медленным, а то и вовсе недоступен. Такая ситуация также нежелательна для самого Google, поскольку она отрицательно сказывается на его конкурентоспособности.

Доклад Эрика Кляйна (Erik Kline), Google, был посвящен обсуждению технологий, позволяющих избежать подобных ситуаций.

В настоящее время Google использует т.н. технику "белых" листов. Суть ее заключается в том, что факт доступности Google по протоколу IPv6 (а именно – IPv6-адрес основного сайта www.google.com) является своего рода секретом для всех сетей, за исключением тех, которые находятся в специальном, "белом" списке. Достигается это следующим образом.

Как известно, для передачи данных между компьютерами в Интернете используются адреса (IPv4 или IPv6), а не имена. Глобальная система DNS обеспечивает трансляцию доменных имен в адреса и наоборот. Так вот, когда приложение запрашивает адрес www.google.com серверы, обслуживающие DNS-запросы Google, включат IPv6-адрес только в том случае, если сеть, откуда был сделан запрос, находится в "белом" списке. Ответы на запросы из других сетей будут содержать только адрес IPv4. Подробнее от об этом рассказывает сам Google: http://google.com/ipv6/

Однако создание и поддержание "белого" списка довольно трудоемкая операция, требующая дополнительных проверок со стороны Google – проверку аутентичности запроса на включение в список, проверку связности IPv6, ведение учета проблемных ситуаций, контакты с центром управления сети и т.п. Другими словами, такой подход масштабируется очень плохо.

Для автоматизации этого процесса Эрик предлагает использование DNS записей типа TXT (записи этого типа представляют собой просто текстовые строки) в обратных зонах – зонах, позволяющих отображать IP адреса обратно в имена. Записи эти будут содержать информацию о готовности или неготовности сети обеспечить доступ к ресурсам Google по протоколу IPv6. Например, запись

```
_aaaa.2.0.192.in-addr.arpa. 1W IN TXT "ok"
```

означает, что сеть 192.0.2/24 "сознательно" поддерживает IPv6 и может обеспечить качественный доступ своих пользователей к ресурсам IPv6.

При обработке DNS запроса Google может определить его источник и, соответственно, прочитать запись TXT и решить следует ли включить в ответ IPv6-адрес или ограничиться только адресом IPv4.

IPv6 в мире - World IPv6 Day

Страх перед "проблематичными" сетями IPv6 и возможностью потерять клиентов разделяют вместе с Google и другие крупнейшие провайдеры контента - Facebook, Yahoo!, Akamai и Limelight Networks. И поэтому, хотя все они уже поддерживают IPv6, доступ к их ресурсам в основном по-прежнему осуществляется по протоколу IPv4. И в то же время, именно эти провайдеры могут создать критическую массу контента, доступного по IPv6, которая, в свою очередь, подтолкнет пользовательские сети доступа к скорейшему внедрению IPv6. Об этой динамике я писал в своей статье "IPv6: вчера, сегодня, завтра (Часть III)".

В прошлом году в рамках серии совещаний, посвященных проблемам внедрения IPv6 проводимых ISOC, родилась идея - а что если все крупнейшие поставщики контента на один день одновременно откроют неограниченный доступ к своим основным сайтам по протоколу IPv6? Так возникла концепция Мирового Дня IPv6, World IPv6 Day, который состоится 8 июня 2011.

На сегодня, несколько сотен сервис-провайдеров контента и сетевого доступа выразили готовность принять участие в Дне.

С одной стороны, этот эксперимент позволит провайдерам контента реально определить процент "проблематичных" клиентов IPv6. Хочется надеяться, что для многих этот день укрепит уверенность в себе и в IPv6 и позволит продолжить предоставление IPv6-доступа в нормальном режиме.

С другой стороны, для сетевых операторов этот день открывает возможность "почувствовать" более значительные объемы трафика и, как следствие, выявить недоработки и ошибки в конфигурации и оборудовании, которые чрезвычайно трудно обнаружить при сегодняшнем нормальном уровне трафика IPv6. О том, к чему должен быть готов сетевой оператор и его центр технической поддержки рассказал в своей презентации Дэвид Фридман (David Freedman) (http://ripe62.ripe.net/presentations/198-RIPE-WIDACCESS.pdf). Эта презентация, кстати, вызвала довольно бурное обсуждение, в основном подогреваемая критическими замечаниям представителя одного из крупных сетевых операторов. Он, в частности, охарактеризовал World IPv6 Day как атаку на центры технической поддержки операторов со стороны провайдеров контента. Безусловно, это преувеличение, хотя провайдерам надо быть готовым к решению возможных проблем пользователей. Которые, кстати, придется решать раньше или позже. Но чем раньше, тем лучше.

Наконец, World IPv6 Day - это также возможность привлечь внимание мирового сообщества к вопросам внедрения IPv6 и необходимости дальнейшей стимулирования этого процесса.

Будет интересно проанализировать реакцию Интернета на этот микро-шок. Сегодня Интернет превратился в чрезвычайно сложную технико-социальную платформу и ее поведение в этот день может кое-что рассказать о перспективах IPv6.

Более подробную информацию о World IPv6 Day можно получить на сайте ISOC: http://isoc.org/wp/worldipv6day/.

Политики распределения адресного пространства пост-IPv4 эпохи

Итак, 31 января 2011 года в распоряжении IANA осталось только 5 блоков /8 адресного пространства IPv4, которые в соответствии с глобальной политикой были распределены между пятью Региональными Интернет-Регистратурами - RIPE NCC, ARIN, APNIC, LACNIC и AfriNIC. Пул свободных адресов IANA, таким образом, был исчерпан.

Два с половиной месяца спустя, 15 апреля, в распоряжении APNIC остался только один, последний блок /8, и в этом регионе распределение адресного пространства IPv4 теперь следует специальной политике, при которой каждый настоящий и будущий ЛИР может получить небольшой блок IPv4 - /22, но только один раз. Поскольку блок /8 можно "нарезать" на немногим более 16000 блочков /22 - процесс распределения оставшегося адресного пространства скорее всего займет не один год.

Кстати, подобная политика принята и в RIPE (http://www.ripe.net/ripe/docs/ripe-509 ----use-of-last----for-pa-allocations), хотя она и не приведена в действие, поскольку у RIPE NCC пока есть свободные адреса. На сколько хватит оставшихся 3.5 /8 до момента, когда вступит в силу политика распределения последнего блока /8, сказать трудно, но не исключено, что это может произойти уже в этом году.

Неудивительно, что многие новые предложения были сфокусированы на пост-IPv4 периоде.

Один из проектов, который также обсуждается и в других регионах для принятия в качестве глобальной политики, рассматривает вопрос распределения адресного пространства, возвращенного тем или иным способом обратно IANA. Название проета 2011-01 Global Policy for post exhaustion IPv4 allocation mechanisms by the IANA (http://www.ripe.net/ripe/policies/proposals/2011-01). Вопрос каким образом адресное пространство будет возвращено IANA выходит за рамки предложения.

Проект достаточно актуальный, хотя ввиду отсутствия автора проекта он не обсуждался на заседании, поскольку в настоящее время не определено, что делать с адресами IPv4, которые возвращены обратно в IANA. В проекте для этого предлагается создание специального пула возвращенного адресного пространства (Recovered IPv4 Pool), который будет периодически распределяться поровну между существующими РИРами. Если это предложение будет принято в качестве глобальной политики, каждому РИРу предстоит решить, что делать с дополнительным адресным пространством IPv4, полученным от IANA.

Другой проект, 2011-03 Post-depletion IPv4 address recycling - clarification of the "last /8" policy (http://www.ripe.net/ripe/policies/proposals/2011-03/), уточняет некоторые аспекты существующей политики по распределению последнего блока /8, о которой мы только что говорили. В частности, этот проект предлагает, что распределение любого возвращенного в RIPE NCC адресного пространства IPv4 (но не возвращенное далее в IANA) подчиняется тем же правилами, что и для последнего блока /8. Также уточняется, что при невозможности выделения непрерывного блока /22, запрос может быть удовлетворен частями.

Наконец, в ходе дискуссии на заседании рабочей группы по европейским точкам обмена трафиком - EIX, родилось новое предложение - о резервировании отдельного блока IPv4 для новых IX'ов. Дискуссия продолжилась на пленарном заседании, и идея была поддержана в целом, даже предлагалось расширить ее на другие элементы "критической инфраструктуры" - операторов доменов верхнего уровня, сетей anycast.

RPKI - спасение или напасть?

Хотя с начала этого года RIPE NCC начал предоставлять услуги сертификации адресных ресурсов (см. мою статью - "Сертификация Адресных Интернет-Ресурсов"), обсуждение сообществом этой новой услуги так и не достигло консенсуса. В результате - с 2008 года на повестке дня находится дремлющее в перерывах между конференциями RIPE предложение политики по сертификации, указывающее RIPE NCC обеспечить сертификацию ресурсов.

Вкратце, сертификация адресных ресурсов - адресных блоков и номеров автономных систем, - является фундаментом будущих систем безопасности маршрутизации (об этом я писал в статье "Путевые заметки: IETF80"). Хотя все вроде бы согласны, что безопасность маршрутизации - вещь хорошая, мнения разделились относительно негативных последствий решений, основанных на иерархической сертификации.

Основное опасение - не создаст ли такая система дополнительные точки контроля государства над Интернетом. Например, гипотетическая возможность отзыва (revocation) сертификата какой-либо сети и, как следствие, отключение ее от Интернета, по решению нидерландского суда, в юрисдикции которого находится RIPE NCC.

Эти опасения не беспочвенны - правительства ищут пути регламентирования работы Интернета, особенно в области борьбы с криминальными действиями. Известны попытки (некоторые - успешные) в ряд стран провести законодательство, предписывающее сервис провайдерам блокировать определенные ресурсы, например с использованием системы DNS. Хотя если присмотреться, эти попытки связаны с желанием "локализации" глобальных систем, таких как DNS или адресные ресурсы, для приведение их в соответствии с национальной политикой, а не использование этих систем для навязывания национальной политики какой-либо страны в глобальном масштабе. Интересно, что подобные страхи государственного контроля связывались с внедрением DNSSEC, однако именно необходимость внедрения этой технологии является одним из главных аргументов против упомянутых выше проектов законодательства (см. например, статью в CircleID: http://www.circleid.com/posts/20110525_experts_urge_congress_to_reject_proposed_dns_filtering_protect_ip/).

Дискуссия приобрела довольно эмоциональный характер, особенно в списках рассылки. Многие обсуждали страшные картины полицейского контроля за возможностью подключения к Интернету, и мало кто вспоминал про преимущества улучшения защищенности глобальной системы маршрутизации. Хотя случай с YouTube должен еще быть свеж в памяти, а более локализованные "атаки", в подавляющем большинстве своем ошибки конфигурации, происходят ежедневно. Возможно отчасти причиной является психология "это произойдет не со мной".

Как сделать конференции RIPE еще интереснее?

Конференции RIPE имеют богатую историю. За свое более чем двадцатилетнее существование было проведено 62 конференции, начиная с небольшой группы единомышленников, первопроходцев европейского Интернета и заканчивая представительным международным событием, собирающим более 400 участников, каким конференция RIPE является сегодня.

Однако времена меняются и мы меняемся вместе с ними. На прошлой конференции осенью 2010 года была сформирована специальная инициативная группа для разработки предложений по некоторым структурным улучшением в проведении совещаний RIPE.

Работу над этими предложениями группа начала с опроса, в котором приняло участие более 300 человек. Опрос собрал мнение участников относительно новых форм совещаний, таких как BOF (Brids of Feather - от поговорки Birds of a feather flock together, что-то вроде нашего "рыбак рыбака видит издалека" - неформальные встречи для предварительного обсуждения какого-либо вопроса), обучающие секции. Также создателей опроса интересовало что следует и чего не следует менять в проведении конференций.

В категорию "не следует менять" попали такие вещи как технический фокус, продолжительность и частота проведения, наличие (практически каждодневных) социальных событий. Взнос на участие в конференции был также расценен как справедливый и приемлемый.

В плане улучшений участники хотели бы видеть больше образовательного контента (87% участников посещают RIPE для самообразования), больше технических докладов, с фокусом на новейшие технологии и разработки, а также, наряду с пленарным заседанием и заседаниями рабочих групп, других форм встречи участников, как, например BOF. Также участники опроса выразили желание усилить вовлечение региональных операторских групп, таких как ENOG, MENOG, а также национальных групп в работу конференции.

Все это было принято на вооружение, а воплотить в жизнь эти пожелания предстоит новоизбранному программному комитету конференции. Надо заметить, что до сих пор работа над основной программой (не включая рабочие группы) велась достаточно неформально, в основном среди председателей рабочих групп. Более структурный подход к этому вопросы явился еще одним улучшением, предложенным инициативной группой.

Структура нового Программного Комитета выглядит следующим образом. Четыре представителя сообщества, назначенных для первого раза, а в дальнейшем - избранных демократическим путем. Представители региональных операторских форумов ENOG (здесь в программный комитет попал ваш покорный слуга) и MENOG. Один представитель от председателей рабочих групп. Региональный представитель принимающей стороны. Программный Комитет начнет свою работу уже в начале июня

для того, чтобы программа следующей конференции еще больше порадовала участников. Для связи с Программным Комитетом можно использовать адрес pc [at] ripe [dot] net.

До встречи в Вене!

Андрей Робачевский, Менеджер по программам ISOC

Мнения, представленные в статье, не обязательно отражают официальную позицию ISOC