Путевые заметки: RIPE59

В начале октября, точнее с 5-го по 9-е, в Лиссабоне прошла очередная конференция RIPE. Более 330 участников из 33 стран в течение недели обсуждали вопросы, связанные с развитием Интернета. Не претендуя на исчерпывающий отчет о конференции, я предлагаю читателю несколько тем RIPE59, интересных с моей точки зрения.

RIPE Labs

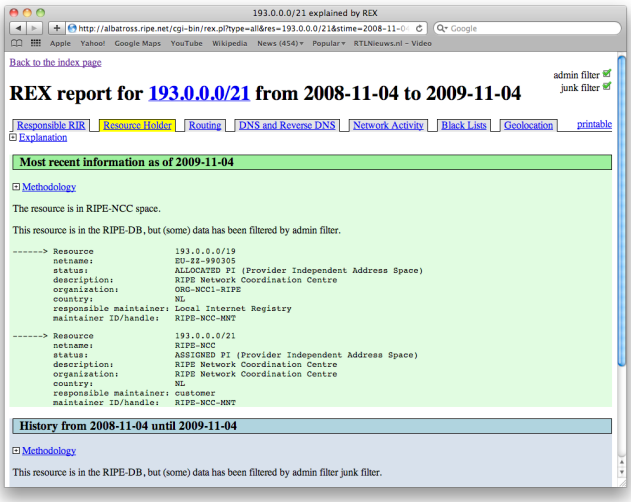
RIPE NCC в лице Mirjam Kuehne представил участникам новую концепцию - RIPE Labs (http://labs.ripe.net/). Концепция похожа на существующие лаборатории, например Google Labs, и заключается в создании форума и платформы для обкатки новых идей, приложений и услуг. RIPE Labs открыты для всего сообщества RIPE - зарегистрированные пользователи имеют возможность не только обсуждать, но и демонстрировать собственные приложения и идеи.

Для RIPE NCC Labs предоставляют возможность показа и обсуждения новых приложений и услуг на раннем этапе их создания. Это позволит нам создать продукты, которые более точно соответствуют нуждам наших пользователей и не тратить силы на разработку приложений, которые являются с их точки зрения малоинтересными.

В рамках Labs были представлены несколько таких приложений, которые в будущем могут занять место в портфеле услуг RIPE NCC.

REX - Resource Explainer

Хотите узнать какая Интернет Регистратура отвечает за адресный ресурс? Какие из подсетей были активны в Интернете за последний месяц? Какие автономные системы анонсировали данное адресное пространство последние 10 лет? Для ответа на подобные вопросы достаточно задать адресный префикс и REX предоставит информацию, собранную из различных источников. REX может стать основой возможных будущих "репутационных" услуг, предоставляемых RIPE NCC. Вы можете сами оценить возможности прототипа: http://albatross.ripe.net/cgi-bin/rex.pl.

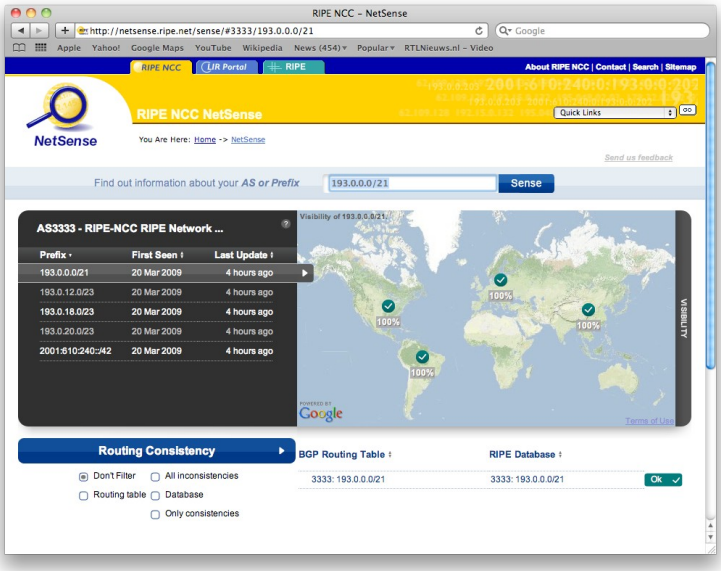


Netsense

Netsense (http://netsense.ripe.net/) является прототипом нового портала Информационных Услуг (ИУ) RIPE NCC. Вы, наверное, знакомы с традиционными системами ИУ. Эти услуги предоставляют доступ к данным о функционировании Интернета, которые RIPE NCC собирает уже на протяжении

более 10 лет, используя обширную измерительную сеть. Точнее, несколько сетей. Традиционно мы делим все измерения на активные, когда пробы генерируют трафик и по реакции сети определяют параметры связности (задержка, потери пакетов и т.п.), и пассивные, когда система наблюдает за изменениями в системе маршрутизации Интернета. За первую категорию измерений отвечает сеть TTM, а вторую группу измерений обеспечивает RIS. Обе сети имеют глобальный характер и насчитывают несколько десятков пробов, размещенных на всех континентах.

Однако пользовательский интерфейс доступа к этим данным для решения практических задач - от диагностики и мониторинга сети, до оптимизации маршрутизации и планирования, - оставлял желать лучшего. Предполагалось, что наш пользователь уже довольно хорошо знаком с общим пакетом и сможет выбрать нужный инструмент. Однако, как оказалось, для большинства это



непростая задача.

Основная идея нового подхода, который воплощен в прототипе Netsense, заключается в том, что все, что необходимо для входа в портал и начала путешествия - это ваша сеть - автономная система или префикс. Мы расскажем вам все, что наши системы знают и ней, о ее состоянии в глобальном Интернете. Отсюда вы можете начать диагностику проблем, если таковые имеются, например проблемы со стабильностью префикса, или задать параметры для мониторинга.

Пользователи также получат возможность взглянуть на Интернет с различной степенью детализации. Начиная от, так сказать, глобальных погодных условий в Интернете, континенте, стране, регионе и заканчивая функционированием отдельной сети.

DNS

В этот раз основной темой обсуждений в области DNS явилась корневая зона. Неудивительно, поскольку в недалеком будущем эта зона может претерпеть серьезные изменения.

Во-первых - цифровая подпись содержимого зоны с помощью технологии DNSSEC. Годы велись дискуссии - когда же будет подписана зона, кто будет контролировать ключи, как это отразится на системе DNS и Интернете в целом. Осенью прошлого года подразделение министерства торговли США, Национальная Администрация по Телекоммуникации и Информации (NTIA), опубликовала возможные схемы подписания корневой зоны. Среди представленных сценариев были также предложение ICANN и предложение VeriSign. Спустя почти год публичных комментариев и, очевидно, внутренних дискуссий, ICANN, VeriSign и NTIA договорились о прагматичной схеме, при которой существующий процесс внесения изменений в зону остается прежним, а основные игроки получают дополнительные роли: ICANN контролирует т.н. Trust Anchor - ключ для подписания ключей (Key Signing Key, KSK), NTIA по-прежнему утверждает изменения, а VeriSign владеет ключом подписания зоны (Zone Signing Key, ZSK), который используется для генерирования подписанной корневой зоны, и осуществляет ее публикацию на

скрытом мастер-сервере. Далее, зона публикуется операторами корневой зоны (RIPE NCC является одним из них, отвечая за корневой сервер k.root-servers.net). Надо отметить, что в соответствии с технологией DNSSEC, ключ KSK подписывает ключ(и) ZSK. Другими словами, контроль за подписанием зоны в конечном итоге остается за ICANN.

Когда политические страсти вокруг подписания корневой зоны постепенно улеглись, настало время взглянуть на технические аспекты этого изменения. А их немало. Помимо внутренней защищенной архитектуры хранения и использования ключей, защищенного взаимодействия между игроками, сама публикация подписанной зоны представляет серьезную задачу. Это, в первую очередь, связано с масштабом последствий, которые изменения в корневой зоне могут иметь для глобального сообщества пользователей Интернета.

Matt Larson (VeriSign) и Joe Abley (ICANN) в своей презентации "Status Update: Implementing DNSSEC at the Root" (http://www.ripe.net/ripe/meetings/ripe-59/presentations/abley-dnssec-root-zone.pdf) рассказали о предлагаемом ими подходе постепенного внедрения DNSSEC в корневой зоне с целью более точного контроля изменений в работе корневого DNS и минимизации возможных негативных последствий.

Суть предложения заключается в следующем. Подписанная зона сначала публикуется только на одном корневом сервере, через некоторое время (недели) - на следующем и т.д. пока все корневые серверы не станут обслуживать подписанную зону. Идея в том, что в случае, если резолвер (сервер DNS, который осуществляет полную трансляцию имен для группы пользователей - например, сети или организации) не может работать с подписанным ответом от корневого сервера, у него все еще есть выбор - обратиться к следующему серверу, который публикует неподписанную зону. Анализируя изменения трафика между серверами, можно оценить масштаб проблем. Однако такой подход приведет к тому, что пользователи будут получать то подписанные ответы, которые они должны валидировать, то неподписанные, в зависимости от того, какой сервер отвечает на запрос. Такая ситуация, конечно, весьма нежелательна.

Однако, если присмотреться к возможным негативным последствиям подписания зоны, значительное увеличение размера ответов, во многих случаях превышающее заветные 512 байт, является основным. Хотя предполагается, что клиенты, запрашивающие подписанный ответ (а на сегодняшний день, это является установкой по умолчанию для большинства программного обеспечения DNS), поддерживают расширения EDNS0 и способны обрабатывать большие пакеты, существует ряд других обстоятельств, которые могут привести к ошибке. Например, превышение размера MTU (максимальный размер датаграммы, который может быть передан между конечными устройствами, зависящий от конкретного пути следования пакета), а также фильтрация сетевыми экранами.

Именно поэтому авторы предлагают подписать зону заведомо неправильным ключом, необходимым только для увеличения размера ответов. Они назвали такую зону - Deliberately Unvalidatable Root Zone (DURZ) - зона, которая заведомо не може быть криптографически валидирована.

```
.  DURZ 3600    IN          DNSKEY 256 3 5 (
                            AwEAAa++++++++++++++++++++++
                            ++++++++
                            ++THIS/KEY/AN/INVALID/KEY/AND/SHOULD
                            /NOT/BE/USED/CONTACT/ROOTSIGN/AT/ICA
                            NN/DOT/ORG/FOR/MORE/INFORMATION++++
                            +
                            ++++++++++++++++++++++++++++
                            ++++++++
                            ++++++++++++++++++++++++++++
                            ++++++++
                            ++++++++++++++++++++++++++++
                            ++++++++
                            ++++++++++++++++++++++++++++
                            ++++++++
                            ++++++++++++++++++++++++++++
                            ++++++++
                            ++++++++++++++++++++/=
                            ) ; Key ID = 6477
```

«Неправильный» ключ корневой зоны DURZ

После того, как зона DURZ будет полностью внедрена - обслуживаться всеми корневыми серверами, можно будет заменить неправильные ключи на настоящими и объявить задачу выполненной.

На временной оси это выглядит следующим образом:

- 1 декабря 2009 - начало подписания зоны для внутреннего пользования. Все процессы задействованы, зона публикуется на специальном скрытом мастере, но не публикуется корневыми серверами.
- Январь-июль 2010 - постепенное внедрение зоны DURZ на корневых серверах
- Июль 2010 - ключ KSK заменен на настоящий и Trust Anchor опубликован. Корневая зона подписана!

Во-вторых, помимо DNSSEC ряд других нововведений планируется к внедрению. Среди них создание в больших количествах новых доменов общего пользования (gTLD), введение международных доменных имен и поддержка IPv6 всеми корневыми серверами. Все это увеличивает как размер самой зоны и ответов, так и увеличивает частоту изменений зоны. Все это, в свою очередь, увеличивает риск для глобальной распределенной системы DNS. Для определения комплексного эффекта, который эти изменения могут иметь на корневую зону и глобальную DNS в целом, Совет ICANN запросил комитеты RSSAC и SSAC провести исследование этого вопроса.

Первые результаты этого исследования были представлены участникам конференции председателем исследовательской группы Lyman Chapin. Полный отчет можно прочитать http://www.icann.org/en/committees/dns-root/root- scaling-study-report-31aug09-en.pdf. Приведу основные результаты:

- В области управления корневой зоной (внесение и авторизация новых записей, генерирование зоны и т.п.) основным сдерживающим фактором масштабирования является человеческий фактор. Другими словами, этот процесс слабо автоматизирован.
- В области публикации увеличение зоны в основном затрагивает географические области с недостаточной связностью. Одной из задач внедрения anycast-копий серверов, являлось улучшить параметры доступа к корневой зоне именно для таких регионов. При значительном увеличении размера зоны и частоты изменений, пропускная способность сети, необходимая для синхронизации всех копий, может явиться сдерживающим фактором в областях, где сетевая инфраструктура недостаточно развита.
- Управление рисками, связанными с годовым увеличением числа записей в корневой зоне порядка сотен, может осуществляться текущими участниками системы без каких-либо изменений.
- Управление рисками, связанными с годовым увеличением числа записей в корневой зоне порядка тысяч, может осуществляться только при изменении условий для одного или более участников.

Другими словами - двигаться можно, но осторожно. В этом смысле группа предложила разработку "системы раннего оповещения", которая обеспечит условия, при которых, возможные негативные последствия будут всегда находятся в зоне контроля участников системы, а также могут быть приняты своевременные меры для их устранения. Эту концепцию иллюстрирует аналогия автомобиля, двигающегося по неосвещенной дороге. Водитель вряд ли может предугадать все возможные препятствия на своем пути, однако необходимо, чтобы скорость его движения и зона освещения фарами соответствовали времени реакции водителя.

Адресные политики

Как и следовало ожидать, основными вопросами (и соответствующими проектами политик) являлись проблемы распределения оставшегося адресного пространства: распределение последнего блока /8 и справедливое распределение оставшегося адресного пространства Ipv4.

В соответствии с глобальной политикой распределения оставшегося адресного пространства IPv4

"Global Policy for the Allocation of the Remaining IPv4 Address Space" (ripe-436) IANA зарезервировала блок /8 для каждой РИР. Политика распределения этого последнего блока определяется в каждом регионе независимо. В регионе RIPE в настоящее время существуют два проекта:

Первый (http://www.ripe.net/ripe/policies/proposals/2008-06.html) предоставляет возможность текущим и будущим ЛИРам получить один и только один блок адресов IPv4 максимальным размером равным минимальному размеру распределяемого пространства на момент исполнения данной политики (сегодня это /21).

Второе предложение также направлено на поддержку сервис-провайдеров в переходный период исчерпания, но содержит дополнительные механизмы для стимуляции внедрения протокола IPv6 - “IPv4 Allocation and Assignments to Facilitate IPv6 Deployment (http://www.ripe.net/ripe/policies/proposals/2009-04.html)”. Это предложение также предусматривает "масштабирование" запросов, учитывая возможности повышенной утилизации использования адресов с помощью технологий мультиплексирования (например, трансляторов NAT).

Эти предложения были представлены на прошлой конференции RIPE, но несколько месяцев обсуждений в списках рассылки так и не привели к консенсусу в каком направлении двигаться.

На заседании рабочей группы Адресной Политики Remco van Mook сделал попытку примирить противоречия и выступил с альтернативным предложением. Суть его заключается в следующем:

1. зарезервировать /10 для будущего использования
2. распределять адреса только единым блоком (например, если запрос был на /17, а самый большой единый блок /19, только этот блок и будет выделен)
3. увеличить требования утилизации с 80% до 95%

Последующее обсуждение выявило несколько слабых сторон предложения, возможно они будут учтены в формальном проекте. Будущее покажет, сможет ли этот проект достичь консенсуса. Пока что большинство согласно с одним - ничего не предпринимать в данной ситуации - не лучшая позиция.

Сертификация

Проекту политики сертификации адресных ресурсов (http://www.ripe.net/ripe/policies/proposals/2008-08.html) исполнился год. Год назад, на конференции в Дубае, некоторые участники выразили озабоченность возможными последствиями данной политики (и собственно сертификации), но серьезного обсуждения за это время не произошло. Поэтому, чтобы сдвинуть процесс с мертвой точки, председатель исполкома RIPE NCC Nigel Titley постарался четко обозначить основные проблемы и возможные пути их решения (http://www.ripe.net/ripe/meetings/ripe-59/presentations/titley-2008-08.pdf).

А возможных проблем и методов их решения несколько:

Контрактные отношения. Согласно проекта политики, период действия сертификата связан с продолжительностью контрактных отношений с RIPE NCC. Организации, прекращающие контрактные отношения с RIPE NCC и перестающие быть ЛИРами (в основном в силу неуплаты взносов), по-крайней мере лишатся возможности обновления своих сертификатов. Правда, уже в настоящее время ресурсы «закрывшихся» ЛИРов подлежат возврату.

Юридические аспекты. Теоретически, в целях пресечения преступной деятельности правоохранительные органы могут потребовать удалить определенные сети из базы данных RIPE. Сегодня такие действия не будут иметь значительного эффекта, но в случае, если технология сертификации будет внедрена на уровне протоколов маршрутизации - последствия могут быть более серьезными. Надо оговориться, что правоохранительные органы могут запросить нечто подобное только через суд, а суд должен решить правомерность подобного запроса. Вопрос применимости существующей законодательной базы в данной ситуации требует дополнительного исследования. Далее, документами, регламентирующими сертификацию ресурсов, являются сертификационная политика (RPKI Certificate Policy – не путать с политикой сертификации, обсуждаемой в RIPE) и установленная практика сертификации (Certificate Practice Statement). Оба эти документа находятся в руках сообщества и могут содержать элементы, препятствующие использование сертификации в качестве "красной кнопки". Наконец, как продемонстрировал в свой презентации "RPKI Local Processing Model" Stephen Kent (http://www.ripe.net/ripe/meetings/ripe-

59/presentations/kent-rpki.pdf), сертификация лишь предоставляет данные для принятия решений, сами же решения принимаются в соответствии с локальной политикой. Даже, если эти решения внедрены на уровне BGP, как предлагается в проектах IETF, проверка подлинности пути (или анонсирующей автономной системы) - всего лишь один из критериев в процессе выбора лучшего пути. Другими словами, среди нескольких возможных путей, подлинный путь получит предпочтение, но если путь единственный, то скорее всего он будет выбран в любом случае. Плюс, провайдер сможет установить "белые списки", отменив проверку подлинности для определенных сетей.

Споры и разногласия в отношении ресурсов. Какую роль здесь играет сертификация? Или в этом случае процесс мало отличается от стандартной процедуры решения споров?

Наконец, ошибки. Очевидно, что критичность сертификации для глобальной системы маршрутизации будет возрастать по мере более широкого ее внедрения. Но это вряд ли произойдет внезапно, а последовательное развитие позволит адаптировать и обкатать систему.

Способность меняться

На этой неделе сообщество RIPE в очередной раз продемонстрировало свою возможность изменяться в соответствии с новыми требованиями и задачами. На повестке дня двух рабочих групп - IPv6-WG и TT-WG - стоял вопрос изменения чартера.

В Рабочей Группе по IPv6, Shane Kerr выступил с радикальным предложением распустить группу и использовать это время на решение более насущных проблем. Не то что бы IPv6 не является насущной проблемой, как раз наоборот. Но по мнению Shane задачи Группы не соответствуют текущему моменту, учитывая, что до исчерпания свободного пула адресов IPv4 осталось 3-4 конференции RIPE (и соответственно заседаний Рабочей Группы).

Большинство не согласилось с идеей роспуска группы, но поддержало предложение радикально переработать чартер. Дальнейшее обсуждение обозначило и основные задачи - максимально способствовать внедрению IPv6 и решению проблем сосуществования двух протоколов - ситуация, которая по мнению экспертов продлится несколько лет (если не десятков лет). Новый чартер в настоящее время обсуждается в списке рассылки ipv6-wg@ripe.net.

Вторая Группа, в которой также поступило предложение об изменении чартера, была TT-WG (Рабочая Группа по Тест-Трафику). Исторически работа группы была посвящена обсуждению системы TTM, созданной и обслуживаемой RIPE NCC. Измерения производительности Интернета являлись регулярными темами обсуждений, но в основном в рамках TTM. Однако в последние годы на повестку дня все чаше стали выноситься темы, выходящие за эти рамки. Речь идет о различных измерительных проектах и системах, интересных аналитических докладах, основанных на собранных данных, инструментарии, который помогает сервис-провайдерам лучше понять, что происходит в Интернете и как он работает. Одним из примеров, конечно, является новая концепция Информационных Услуг RIPE NCC - Netsense. А форум RIPE Labs мог бы найти в Рабочей Группе отражение совего виртуального сообщества. На заседании Рабочей Группы было предложено расширить круг вопросов с особым упором на мониторинг, диагностирование, анализ тенденций развития и функционирования сетей и Интернета в целом.

Лиссабон

В заключение – пару слов о месте проведения конференции. Лиссабон - очень красивый город, хотя в основном мое знакомство с ним ограничилось отелем Corinthia. Говорят, что еще финикийцы присмотрели это место а название города берет свое начало от финикийского «Alis Ubbo» (благословенная бухта). Во втором веке до н.э. он впервые упоминается в древних летописях, потом с десяток веков он переходил из одних рук в другие, пока, наконец не стал столицей Португалии в 1256 году. Несмотря на свою многовековую историю, Лиссабон выглядит довольно молодо - в 1755 году он был разрушен до основания сильным землетрясением. В восстановленом Лиссабоне доминирует свет – от белых каменных мостовых, до яркого теплого солнца.

Технический директор RIPE NCC Андрей Робачевский

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