Путевые заметки: IETF 86

Очередная, 86-я конференция IETF (https://www.ietf.org/meeting/86/index.html) прошла с 10 по 15 марта в Орландо, Флорида, США. Это недельное совещание, которое проводится три раза в год и собирает более тысячи участников из полусотни стран, как обычно, было посвящено разработке новых стандартов и вопросам технического развития Интернета. Оговорюсь – хотя я и назвал IETF конференцией, это неправильно. IETF – это череда сессий более чем 120-ти Рабочих Групп, где участники совместно работают над конкретными предложениями новых протоколов и технологий. Также оговорюсь, – разработка и обсуждение стандартов в IETF проводится онлайн, в списках рассылки, а совещания помогают более широкому обмену мнениями, знакомству со смежными разработками и поиску общего мнения по сложным или спорным вопросам. В этот раз совещание IETF86 собрало 1071 участников из 51 страны мира.

Закат телефонной системы, какой мы ее знаем

Еще в 2009 Федеральное агентство по связи США (FCC) всерьез задумалось о будущем традиционных телефонных сетей и переходе на технологию IP, столь успешно работающую в Интернете. Четыре года спустя эти планы приобретают осязаемые черты и даже названы вехи - 2018 год, когда доминирующей технологией станет IP, а телефония превратится в приложение VoIP.

Причины здесь вполне практические.

Стоит посмотреть на телекоммуникационные услуги, приносящие сегодня прибыль, чтобы заметить, что все они связаны с Интернетом и используют технологию и инфраструктуру IP. В противоположность этому, прибыльность традиционных услуг фиксированной голосовой связи, использующих сети коммутации каналов, неуклонно снижается.

Согласно отчету «International Communications Market Report 2012» (www.cw.com/assets/content/services/ofcom/ofcom-uk-communications-report-2012.pdf), опубликованному британским телеком –регулятором Ofcom в конце прошлого года, прибыль от услуг фиксированной связи неуклонно падает, в среднем на 7% в год. В 2011 году наиболее быстро это происходило в Китае (17.8%), Индии (15.3%), Польше (13.3%) и Франции (13.1%). Интересно, что Россия явилась единственной среди стран, проанализированных в отчете, где в период 2006-2011 г.г. прибыльность медленно, но неуклонно росла в среднем на 2.9% в год.

Также практически во всех странах, упомянутых в отчете, объем телефонных разговоров (минут) неуклонно падает. Так в США за период 2006-2011 объем минут уменьшился почти вдвое, или в среднем на 11.2% в год.

Пользователи отказываются от услуг фиксированной связи в пользу альтернатив, предлагаемых мобильными и широкополосными сетями. В определенный момент число пользователей становится слишком мало и содержание инфраструктуры становится попросту невыгодным. Хотя многие ведущие телеоператоры уже переориентировались на IP-технологии, требование обмена трафиком с “устаревшими” традиционными сетями означает дополнительные затраты – сопровождение транкинговой инфраструктуры, преобразование IP-потоков в коммутируемые каналы и т.п.

Производители телекоммуникационного оборудования также переориентируются на IP, в результате сопровождение инфраструктуры становится все сложнее, не говоря о ее модернизации. Добавьте сюда вымывание квалифицированных специалистов - традиционных телефонистов - и причины стремления перейти на всеобщий IP становятся более чем очевидными.

Но существует еще один немаловажный аспект, побуждающий американских телеком-операторов требовать от FCC ускорения технологического перехода. Как известно, в противоположность сильно

зарегулированным услугам традиционной голосовой связи, для услуг Интернет регулирование минимально. Есть требования сетевой прозрачности (т.н. net neutrality), существуют попытки определить требования по параметрам качества предоставляемого доступа, но на этом список по-существу и заканчивается. Многие операторы рассчитывают, что переход к IP-технологии снимет многие дорогостоящие требования, связанные сегодня с передачей голосового трафика.

Одним из таких требований является обязательство обеспечения связности между коммутаторами различных операторов. Другим – государственное регулирование цен на обмен голосовым трафиком между операторами.

Следует заметить, что эти и ряд других требований из мира традиционной телефонии с большим трудом могут быть применены в контексте инфраструктуры IP и тем более Интернета. Вопросы обеспечения связности и договоренности об обмене трафиком в Интернете строятся на совершенно других принципах, основу которых составляют силы рыночной экономики. Попытки изменения этого баланса в пользу государственного регулирования, хотя бы изначально для голосового трафика, могут иметь существенные негативные последствия, как технологические, так и экономические, для развития Интернета в целом. Эта позиция достаточно четко отражена в петиции Comcast в адрес FCC (http://apps.fcc.gov/ecfs/document/view?id=7022113618).

Однако в отличие от своих американских коллег, европейские телеком-операторы, могут расценить такие попытки как благоприятные для собственного бизнеса. Несколько другая рыночная ситуация и конкуренция в Европейском Союзе побуждают некоторых крупных операторов обратиться за помощью к государству. Ярким примером этого является предложение Европейской ассоциации операторов телекоммуникационных сетей, поданное в рамках Всемирной конференции по международной электросвязи (ВКМЭ-12) по пересмотру Регламента международной электросвязи в прошлом году *(*www.etno.eu/datas/itu-matters/etno-ip-interconnection.pdf).

Была затронута тема перехода телефонии на технологии IP и на совещании IETF. Значительная часть технического пленарного заседания IETF86 была посвящена проблемам этого перехода. О планах и проблематике всеобщего перехода на технологию IP рассказал технический директор FCC Хеннинг Шульцрин (Henning Schulzrinne).

По-существу, по словам Хеннинга, мы имеем дело с тремя переходами:

- Переход от медных проводов к оптоволоконной связи. Основными побудительными мотивами являются увеличение пропускной способности, а также уменьшение затрат на сопровождение.

- Переход от фиксированной к беспроводной связи. Преимуществами этого перехода являются мобильность, а также уменьшение затрат на предоставление услуг в малонаселенных областях.

- Переход от сетей коммутации каналов к сетям пакетной коммутации IP. Данный переход обеспечивает значительную гибкость в предоставлении услуг (не только голос, а практически неограниченный спектр услуг передачи данных), но также и уменьшает затраты на передачу бита данных.

В своей презентации Хеннинг также определил 4 основные проблемные области, требующие решения при переходе на технологию IP:

- Качество и надежность

  Если качество и надежность в телефонных сетях достаточно хорошо и просто определены, само определение качества для IP представляет проблему. Какие метрики смогут адекватно отразить качество и надежность новой сети? Каким способом можно измерить эти параметры?

  Вопрос надежности в этом контексте встает необыкновенно остро. Речь здесь идет не о временной недоступности вэб-сайта или невозможности прочитать электронную почту, как это происходит с Интернетом. Сегодня в этом случае по крайней мере есть возможность позвонить в технический центр поддержки и заявить о проблеме. В будущем это будет означать недоступность единственной сети, обеспечивающей связь пользователя с внешним миром.

- Общественная безопасность

  Обеспечение безотказной работы номера вызова экстренных служб является важным требованием в обеспечении общественной безопасности. Это номера «911» в США и «112» во многих других странах, российские «01», «02», «03», «04» (Совет Федерации одобрил закон о введении единого телефонного номера для вызова экстренных служб «112»). Использование IP и Интернета

открывает громадные возможности для модернизации этой услуги, в настоящее время ограниченной голосовой связью. Передача фото, видео, текстовых сообщений являются новыми требованиями, предъявляемым к системам вызова экстренных служб. Технологии IP позволят удовлетворить этим требованиям, однако основными проблемами здесь являются точность определения местонахождения звонящего и надежность связи и доступа к центрам реагирования.

- Нумерация и надежные идентификаторы

  VoIP технологии снимают многие ограничения, традиционно накладываемые на телефонные номера. По-существу, номера становятся коммуникационными идентификаторами, равными среди множества других. Одной из серьёзных проблем в этой области является проблема подложных номеров вызывающего абонента (т.н. Caller ID spoofing). В мире VoIP такая подмена легко осуществима и в некоторых случаях вполне легальна. Помимо проблемы т.н. робоколлинга (Robocalling, http://en.wikipedia.org/wiki/Robocalling) – телефонной версии спама, многие услуги зависят от надежности и безопасности телефонных номеров. Например, некоторые банки используют телефон в качестве элемента многофакторной авторизации при совершении онлайн – транзакций.

- Универсальность услуги

  Универсальность коммуникационных услуг означает несколько вещей. Во-первых, глобальную связность – возможность установить связь с другим абонентом глобально. Во-вторых, доступность услуги независимо от географического положения, дохода, физических ограничений (например, ограничений по слуху или зрению). В-третьих – ценовая доступность. Требование обеспечения универсальности коммуникационных услуг записано в Кодекс США (http://ru.wikipedia.org/wiki/Кодекс_Соединённых_Штатов).

Хотя технология IP и интеграция услуг голосовой связи с другими услугами Интернета открывает поистине неограниченные возможности, удовлетворение требований в вышеперечисленных проблемных областях представляет сложную задачу как с технологической, экономической, так и правовой точек зрения.

Переход традиционных телефонных сетей на технологию IP означает гораздо больше, чем просто технологическая модернизация. Уже сегодня связность во многих случаях обеспечивается виртуальными сетями поверх Интернет-инфраструктуры. Обслуживание отдельной IP-инфраструктуры является слишком затратным для постоянно снижающегося объема голосового трафика.

Другими словами закат PSTN означает, что Интернет поглотит историческую услугу голосовой связи и станет по-существу единой крупнейшей коммуникационной средой, связывающей человечество.

Бесправный контент

Интернет дал новое значение понятию «публикация», будь то публикация текста, видео, аудио или какого-либо другого контента. Если «цифра» сделала копию неотличимой от оригинала, то благодаря Интернету распространение контента стало как никогда проще.

Копирование данных и обмен ими являются самой сутью Интернета. Артерии Сети наполнены копиями данных, оригиналы которых хранятся на компьютерных дисках, будь то веб-страница, музыкальный или видео – фрагмент.

Не секрет, что при этом авторские права создателей цифрового контента нередко нарушаются. И речь здесь идет не только и не столько о правах могущественного Голливуда или издательских домов. Сегодня почти каждый из нас является издателем и производителем контента, и все острее встает вопрос как сделать так, чтобы использование контента соответствовало желанию его создателя.

Различные системы и приложения, позволяющие пользователям публиковать и обмениваться контентом, например Facebook, предлагают возможность определить степень доступности контента - семья, друзья или «весь мир». Однако контент вне контекста этих приложений не содержит информации, которая позволила бы сказать что-либо о его создателе и его требованиях в отношении этого контента.

Понятная, на первый взгляд, задача порождает множество вопросов. Например, каким образом создатель может выразить свои авторские права и как эти права связаны с объектом данных? Помимо языка выражения этих прав, должны ли эти мета-данные быть частью объекта контента или, к примеру, сохранены на удаленном сервере и доступны по запросу? Другой аспект - каковы механизмы

удовлетворения требований создателя? Должны ли мы обратить свои взгляды к законодательству и правоохранительным органам, или предоставление возможности пользователю принять информированное правильное решение уже является серьезным шагом?

Этой теме был посвящен круглый стол, организованногый Internet Society в рамках IETF86 (http://www.internetsociety.org/events/community-calendar/ietf-86). В обсуждении приняли участие эксперты в области приложений, персональных данных и публикации контента: Leslie Daigle (модератор), Glenn Deen, Leif Johansson и Peter Saint-Andre. Основным вопросом обсуждения между участниками явился вопрос о возможных способах выражения требований создателя и их связи с объектом контента.

Участники во многом сошлись на том, что возможность идентификации объекта контента, идентификации создателя и, возможно, пользователя является ключевой в решении данной проблемы. Основной проблемой при этом является вопрос защиты персональных данных. В рамках IETF есть существенные наработки в этих областях, например результаты Рабочей Группы GEOPRIV, идентификаторы URC, стандарты по управлению идентификационной информацией.

Следует заметить, что целью возможной работы в этом направлении является создание благоприятных условий для использования контента, а не ограничения доступа к нему.

В этом заключается существенное отличие данного подхода от традиционного, принятого многими крупными производителями и правообладателями контента - путь ограничения распространения авторских произведений. Так называемые цифровые средства защиты авторских прав (DRM, Digital Right Management, http://ru.wikipedia.org/wiki/Технические_средства_защиты_авторских_прав) намеренно ограничивают, либо затрудняют какие-либо действия с данными в электронной форме (копирование, модификацию, просмотр и т. п.), либо позволяют отследить такие действия.

Очевидно, что обеспечение возможности воспроизведения и при этом запрещение копирования представляет собой крайне сложную задачу: воспроизведение — чтение информации, её обработка и запись на устройство вывода, копирование — чтение и запись информации на устройство хранения. То есть, если возможно воспроизведение (включающее промежуточный этап чтения информации), возможно и её последующее копирование. Поэтому эффективная техническая защита от копирования при разрешённом воспроизведении может быть достигнута только когда всё устройство (плеер или компьютер) находится целиком под контролем правообладателя. Это особенно актуально для цифровой информации, копирование которой не ведет к деградации качества.

Поскольку DRM малоэффективны сами по себе, для них установлена правовая защита. Законодатели многих стран, идя навстречу желанию крупнейших правообладателей, ввели ответственность за обход (преодоление, отключение, удаление) DRM. Например, в России IV часть Гражданского кодекса РФ (вступившая в силу 1 января 2008 г.) предусматривает ТСЗАП. Иногда такое законодательство идет вразрез с техническими и архитектурными принципами Интернета и приносит больше вреда, чем пользы. Примерами таких попыток явились печально известные SOPA (http://ru.wikipedia.org/wiki/Stop_Online_Piracy_Act) и ACTA (http://ru.wikipedia.org/wiki/ACTA).

Замечу, что направление, обсуждавшееся за круглым столом, хотя и не решает проблему пиратства, может явиться существенным шагом в направлении более «правильного» использования контента, при этом не нанося вреда Интернету в целом.

Вопросы автоматизации обслуживания DNSSEC

Решение проблемы замены корневого ключа «точки доверия», или TA (Trust Anchor), было стандартизовано в RFC5011 (http://datatracker.ietf.org/doc/rfc5011). Примером является замена ключа KSK (Key Signing Key, ключ для подписи ключей) корневой зоны – более подробно о DNSSEC и ключах я писал в статье «Как подписали корень» (http://www.ripn.net/articles/dnssec/). Суть решения заключается в возможности добавления нового SEP (или KSK) ключа, будущего ключа «точки доверия», к существующему набору ключей – DNSKEY RRSet. Если резолвер сможет удостовериться в подлинности этого ключа, используя существующий TA, новый ключ может быть добавлен к существующему набору TA резолвера.

Подобная проблема также существует при замене ключей KSK дочерней зоны, поскольку родительская зона должна отразить эту замену соответствующей модификацией записи DS.

При первоначальном подписании зоны открытые ключи (или сгенерированные записи DS) должны быть переданы администратору родительской зоны специальным образом, вне системы DNS (т.н. out-of band) для установления цепочки доверия от родительской к дочерней зоне. Процедура эта нестандартная и, как

правило, трудоемкая[1], зачастую требующая участия регистраторов и регистратур. Поэтому дочерние зоны предпочитают не менять ключи вообще из опасения неумышленного разрыва цепи доверия и, как следствие, невозможности удостоверения подлинности записей зоны. Очевидно, что с точки зрения безопасности такая ситуация далека от идеала.

В рамках заседания Рабочей Группы DNSOP (http://datatracker.ietf.org/wg/dnsop/) обсуждалось предложение решения этой проблемы.

Одной из возможностей автоматизации этого процесса является использование бита SEP в записи DNSKEY дочерней зоны, указывающего, что это ключ для подписи других ключей, который, соответственно, может быть использован для генерирования записи DS в родительской зоне. Недостатками этого метода является отсутствие контроля за алгоритмом дайджеста и ограничение, что запись DS может быть создана только для ключей, указанных в дочерней записи DNSKEY.

Другой подход, получивший положительную оценку группы, заключается в создании отдельной новой записи CDS – Child DS, являющейся копией записи DS, которая должна появиться в родительской зоне. Эта запись должна быть подписана ключом KSK, соответствующем текущей записи DS.

Предполагается, что оператор родительской зоны сможет периодически опрашивать дочерние зоны на предмет наличия и изменения записей DS, которые после проверки подписей могут быть включены в родительскую зону. Также, оператор дочерней зоны с помощью какого-либо автоматизированного процесса может сигнализировать оператору родительской зоны о необходимости замены текущей записи DS на новую, соответствующую CDS.

Реализация этого метода может облегчить автоматизацию взаимодействия между операторами дочерней и родительской зон. Более подробно об этом можно прочитать в соответствующем I-D: “Automating DNSSEC delegation trust maintenance (http://datatracker.ietf.org/doc/draft-kumari-ogud-dnsop-cds)

Новый Председатель IETF

После шести лет успешного председательства Расс Хаусли (Russ Housley) покинул этот пост. Новый выбранный председатель – Яри Арко (Jari Arko) – также хорошо известен в IETF. Он является автором трех десятков RFC и активно работает в области технологий IP, мобильного и беспроводного Интернета. Более подробно о Яри можно узнать на его собственном сайте http://www.arkko.com/.

Андрей Робачевский

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

[1] Типичная процедура включает авторизацию в онлайн-системе регистратора и ручное копирование записи DS с использованием соответствующей формы (в случае, конечно, если регистратор поддерживает DNSSEC). Тестирование с различными регистраторами показало, что в среднем этот процесс требует 12 шагов и занимает около 3 минут. Также существенна вероятность ошибок, поскольку процесс включает ручное копирование.