№1
осень 2015

MSK IX

Интернет изнутри

Эволюция

Мобильный интернет, Джефф Хьюстон
Похоже, что мы на самом деле наблюдаем как интернет и даже компьютеры, населяющие интернет, постепенно пропадают из общественного фокуса

с.4

Содержание:

Иформационный сборник «Интернет изнутри»

По всем вопросам пишите на info@internetinside.ru

Порядковый номер выпуска и дата его выхода в свет:
Выпуск №1, дата выхода: сентябрь 2015г.

Публикуется при поддержке АНО «ЦВКС «МСК-IX»

Главный редактор:
Андрей Робачевский

Зам. главного редактора:
Новикова Татьяна

Дизайн:
Чернега Наталья

Вчера, сегодня, завтра...

главный редактор,
Андрей Робачевский

Дорогой читатель!

Перед Вами первый номер журнала «Интернет изнутри». Цель этого издания – познакомить Вас с технологиями, протоколами и архитектурой, а также экономическими и социальными аспектами функционирования и развития Сети. Другими словами – посмотреть на «устройство» Интернета изнутри.

Ключевой темой сегодняшнего номера является Эволюция. История Интернета коротка, и тем отчетливее видна траектория развития этой уникальной коммуникационной системы. Уникальность ее не только и, возможно, не столько в используемых технологиях, сколько в ее способности к самоорганизации и самоадаптации. «Само-», поскольку в Интернете нет видимого плана развития, его топология понятна только в общих чертах и не существует организации, управляющей и координирующей развитие глобальной Сети.

Вместо этого мы наблюдаем десятки тысяч независимых сетей, принимающих независимые решения по архитектуре, связности и предлагаемым услугам, и тем не менее – о чудо! – объединенные невидимой силой в единую глобальную коммуникационную среду.

У этой «невидимой силы» несколько составляющих – это, конечно, экономические факторы, силы рынка, это также сотрудничество и координация в области разработки стандартов, распределение адресного пространства, координация пространства доменных имен верхнего уровня.

Интернет – это своего рода организм, экосистема, и поэтому термин «эволюция» так подходит для описания траектории развития этой глобальной системы.

В этом номере мы предлагаем вашему вниманию два примера эволюционного развития Интернета. Мы поговорим об эволюции технологической (об этом статья Джеффа Хьюстона «Мобильный Интернет») и об истоках некоторых координационных функций – в статье «Эволюция IANA».

Я надеюсь, что журнал Вам понравится и мы Вы будете ожидать следующего номера. Чтобы сделать его более интересным, Ваше мнение нам очень важно. Можно сказать, что эволюция этого издания отчасти в Ваших руках! Ваши отзывы и предложения мы ждем по адресу info@internetinside.ru.

генеральный директор АО «ЦВКС «МСК-IX», Елена Воронина

Нам электричество ночную мглу разбудит.
Нам электричество пахать и сеять будет.
Нам электричество любой заменит труд.
Нажал на кнопку – чик-чирик – все будет тут, как тут.
(Студенческий фольклор)

Введение

Уважаемые друзья,

Интернет сегодня – это яркое творение совокупной мысли людей многих профессий: инженеров, физиков, лингвистов, математиков, юристов, строителей и простых обывателей.

Публичные интернет-интерфейсы очень дружелюбны, что позволяет широкому кругу пользователей использовать возможности сети вне зависимости от профессии и образования. Действительно, «нажал на кнопку – чик-чирик – все будет тут, как тут».

Наличие предмета и метода computer science, как самостоятельной науки, оспаривается многочисленными оппонентами. Тем не менее, стремительное развитие сети и все возрастающее значение сетевых технологий в различных областях бизнеса, диктует необходимость «научного» подхода в вопросах развития и разработки, внедрения новых технологий, доступности знаний о новациях и трендах компьютерной науки. Высокий уровень развития компьютерных технологий становится стратегическим преимуществом.

Сегодня мы представляем Вашему вниманию первый пилотный выпуск журнала «Интернет изнутри».

Идея журнала возникла на волне успеха книги А. Робачевского «Интернет изнутри», которая была создана специально к 10 Пиринговому форуму MSK-IX.

Миссия журнала – акцентировать внимание читателя на основных направлениях computer science, новых технологиях и разработках, ключевых событиях жизни Глобальной сети. Что из этого получится, покажет время и Ваши отзывы.

Мобильный Интернет

Джефф Хьюстон (Geoff Huston)

Откуда берет свое начало мобильный Интернет и куда направляется индустрия мобильной связи? Станет ли смартфон долгосрочным феноменом или его в свою очередь заменят мириады все более мелких встраиваемых устройств? Становится ли Интернет в целом неосязаем и подобно воде из водопроводного крана, мы будем реально замечать его присутствие только в те редкие моменты, когда его не будет с нами! Джефф Хьюстон обращается к истории компьютеров и Интернета в поиске ответов на эти вопросы.

Отмечено, что наиболее совершенными технологиями являются те, которые исчезают (Марк Вейзер (Mark Weiser), 1991). Они все сильнее вплетаются в ткань ежедневной жизни до тех пор, пока не становятся неотличимы от нее, и мы вспоминаем о них только тогда, когда эти технологии отсутствуют.

Достижение, которое заключается в подаче чистой водопроводной питьевой воды в каждый дом, где она становится доступной по одному повороту крана, является отличным примером результата крупномасштабного гражданского строительного проекта, объединяющего отрасли металлургии, гидрологии, химии и физики. Однако мы не замечаем этого до тех пор, пока это достижение не исчезнет. То же самое можно сказать в отношении внедрения такой бытовой техники, как холодильник, стиральная машина и плита. И конечно, давайте не будет забывать домашнюю электрическую сеть. До строительства общенациональных сетевых систем, заказчиками электроэнергии выступали целые общины, а обслуживание заключалось в освещении общественных мест города по ночам. Потребление электричества дома было недоступной роскошью для большинства домовладений. Сегодня же мы воспринимаем это как нечто само собой разумеющееся.

Компьютеры также исчезают. Современный автомобиль обрабатывает более 100 миллионов строк программного кода в более чем 100 микропроцессорных модулях управления. То, что мы видим в автомобиле – это не все эти устройства, а антиблокировочную тормозную систему, систему регулировки тяги, круиз-контроль, автоматические дворники и предупреждение о не застегнутом ремне безопасности. Каждая из имеющихся в автомобиле базовых систем управления фактически остается невидимой, а все, что мы видим – это интерфейс взаимодействия с человеком. Эта видимая интерфейсная система, по существу контроллер развлекательных устройств и навигационный сервис, является в настоящее время пространством, в котором компании Apple и Google борются за приоритетное положение у производителей автомобилей, в то время как все прочие микропроцессорные системы автомобиля остаются незамеченными.

Так как же мы должны относиться к Интернету? Похож он на крупные электрогенераторы: технологическое достижение, которое воспринимают как нечто само собой разумеющееся и в основном не замечают? Смотрим ли мы все больше на Интернет в свете приложений и сервисов, которые в нем располагаются, и просто игнорируем, каким образом построены базовые системы?

Как насчет последней Интернет-революции – массового роста популярности мобильных смартфонов? Будет ли мобильное персональное вычислительное устройство длительным феноменом или его в свою очередь заменят мириады все более мелких встраиваемых устройств?

Что мы можем сказать об индустрии мобильных смартфонов? Направляются ли эти устройства, построенные по принципу «все в одном», по тому же пути технологического забвения, что и мейнфреймы, ноутбуки и даже браузеры?

Или эти устройства останутся с нами?

Как мы здесь оказались?

Один из способов ответить на этот вопрос заключается во взгляде на эволюцию самого компьютера. Компьютеры – это одна из новейших отраслей экономики. Безусловно, в 19-м веке существовала аналитическая машина Бэббиджа (Charles Babbadge), однако первыми компьютерами, которые появились в середине 20-го столетия, были программируемые вычислители. Они были шедевром электротехники стоимостью, которую могло себе позволить лишь государство, а их размер и хрупкость требовали для них собственного здания, электропитания и регулируемых условий внешней среды. Электронные лампы были большими, требовали высокого уровня напряжения и были весьма хрупкими. Для таких первых компьютеров, как ENIAC, небольшую группу людей специально обучали их программированию, а более крупные команды специалистов занимались обслуживанием этих «бегемотов». Такая модель компьютерных вычислений была доступна для очень немногих, а их стоимость была абсолютно неподъемной для большинства людей.

Все изменило изобретение транзистора. Транзисторы были значительно более надежными, потребляли гораздо меньше электроэнергии, а их производство было намного более дешевым, что привело к появлению в 1960 г. коммерческого компьютера. Эти системы, такие как широко распро-

страненные мейнфреймы IBM System 360, использовались крупными корпорациями, университетами и исследовательскими институтами, а также государственными учреждениями. Для них по прежнему требовались специальные помещения и сооружения, а также команда операторов, которая поддерживала их работу, однако теперь они перешли из разряда числовых вычислителей в категорию устройств для хранения и обработки информации. Эти компьютеры могли хранить и обрабатывать текст, а также числовые данные. В то время компьютеры рассматривались как самостоятельное устройство, а гигантами отрасли были производители, чей логотип красовался на аппаратном обеспечении. Стоимость системы состояла из стоимости аппаратного обеспечения: тогда как остаточная стоимость, приходящаяся на программное обеспечение, была несущественной.

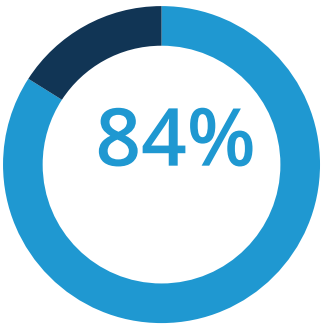
Эволюция транзистора и его превращение в интегральную схему сначала позволили повысить мощность мейнфреймов. Эти системы стали более быстрыми, они хранили больше информации, но по прежнему размещались в специальных помещениях и обслуживались группой специалистов. Но интегральная схема также позволила втиснуть процессор в отдельный чип (микросхему), и компьютерная индустрия была потрясена наступлением эры персонального компьютера. Лишь некоторые из гигантов эры мейнфреймов сумели переключиться на новую продукцию, и некогда знаменитые брэнды Univac, Digital и Burroughs тихо канули в небытие. Наступление эры компьютеров как потребительского товара изменило отрасль и превратило ее в индустрию, зависящую от объемом выпускаемой продукции, что привело к появлению новых «мастодонтов», самым заметным из которых стала корпорация Microsoft. Компания Microsoft не производила аппаратное обеспечение. Она стала разработчиком и поставщиком всех продуктов для ПК. В то время как компании, производящие компьютеры, вели между собой ценовые войны, сводя к минимуму свою маржу из-за безжалостного давления конкурентов, корпорация Microsoft сумела создать фактическую монополию на пакеты программного обеспечения, которые обеспечивали превращение этих устройств в жизненно важные компоненты практически каждого офиса на планете.

Последующая эволюция интегральных схем привела к непрерывному уменьшению их размеров и снижению требований к теплоотводу, что позволило уменьшить размер компьютера до величины человеческой ладони. Первое массовое рыночное предложение в этом сегменте – Apple iPhone – стало во многих аспектах революционным. Оно уменьшило компьютер общего назначения до устройства, имеющего в своем составе всего 5 кнопок, а не 101. Этот продукт располагал искусно изготовленным цветным экраном такого высокого разрешения, что он перестал быть громоздким компьютерным монитором, предоставив в распоряжение пользователя интерфейс, естественный для человеческого глаза. Хотя мир телефонов и компьютерная индустрия взаимодействовали уже в течение многих лет, телефонный мир ревниво охранял свою территорию. Несмотря на то, что цифровые технологии широко применялись в телефонии для передачи сигнала и коммутации, сама телефонная трубка очень медленно уходила от своих базовых разговорных функций. Казалось, что единственной инновационной технологией, появившейся в телефонном мире более чем за столетие, был факс. Появление iPhone стало прямой атакой на этот уравновешенный, консервативный мир телефонии. Одно из мнений заключается в том, что iPhone стал мобильным телефоном, который делал гораздо больше чем отправка и прием звонков. Возможно более реалистичным взглядом является то, что iPhone стал полнофункциональным мобильным карманным компьютером, который время от времени мог также быть мобильным телефоном.

Как это часто случается, путь, по которому следовали компьютерные технологии, стал дорогой непрерывных разрывов и инноваций. Каждая технологическая волна создавала благоприятные возможности для смелых предпринимателей, позволяя им сместить установившихся участников рынка, а сами устоявшееся участники рынка оказались неспособны удержать под контролем дальнейшую эволюцию той же самой технологии, создавая окна возможностей для последующих инноваций и разрывов. Представляется, что изменение является постоянным фактором в этой среде.

На протяжении последних десяти лет изменения, которые были введены этими мобильными «умными» устройствами, стали поистине феноменальными. Компьютер больше не размещается в специально выделенном здании, он даже перестал быть центром святилища на рабочем месте. То, что мы видим – это небольшое удобное устройство, которое можно носить в кармане или даже на запястье. Мы ожидаем, что Интернет будет всегда с нами, где бы мы не находились и что бы мы не делали. Бумажные карты? Кому они нужны, когда в моем смартфоне есть навигационное приложение! Книги? Нет, пользуйтесь своим приложением для чтения! Обмен сообщениями, разговоры, общение, работа. Все это в вашем смартфоне. Произошли огромные социальные изменения. Интернет больше не является местом назначения. Вам больше не нужно идти к своему настольному компьютеру, который с помощью проводов подключен к некоей эфемерной сети. Компьютер с вами всегда, где бы вы не находились и что бы вы не делали. Сегодня Интернет используется эпизодически, но, одновременно, он является постоянным фоном во всех наших делах.

Глубину этих изменений можно увидеть с помощью некоторой отраслевой статистики.



Сегодня в развитых странах количество мобильных «умных» устройств составляет 84% от численности населения, тогда как в развивающихся странах такие устройства все еще во многом являются роскошью, при этом показатель проникновения равен 21%, однако общее количество пользователей этих мобильных устройств и мобильного Интернета в настоящее время составляет 2,3 миллиарда.

Цифры, цифры, цифры

Согласно статистике, публикуемой Сектором развития Международного союза электросвязи (МСЭ), доступ в Интернет в настоящее время имеют 2,9 миллиарда пользователей или в среднем 40 человек из 100 по всему миру.

Несмотря на то, что эта цифра кажется очень большой, она меркнет перед количеством пользователей мобильных телефонных услуг, которое сегодня составляет 7 миллиардов. В настоящее время в развитых странах уровень проникновения услуг на основе SIM на 20% превышает численность населения. Многие люди теперь имеют мобильный

телефон, мобильный планшет, возможно модуль SIM в своем автомобиле, и, потенциально, они используют разные мобильные устройства в своей личной и профессиональной жизни.

Сегодня в развитых странах количество мобильных «умных» устройств составляет 84% от численности населения, тогда как в развивающихся странах такие устройства все еще во многом являются роскошью, при этом показатель проникновения равен 21%, однако общее количество пользователей этих мобильных устройств и мобильного Интернета в настоявшее время составляет 2,3 миллиарда. Весь этот рост произошел за последние восемь лет, при этом ежегодный прирост количества активируемых «умных» устройств равнялся 400 миллионам в год или 13 активаций новых устройств в секунду. Сегодня эти мобильные устройства составляют 40% «видимых» устройств, подключенных к Интернету, тогда как доля настольных компьютеров и ноутбуков уменьшилась до 60%.

Индустрия по производству компьютерных устройств также «переключила передачу»: производство процессоров для настольных компьютеров и ноутбуков уменьшается перед лицом натиска мобильных систем. В 2014 году было отгружено примерно 1,5 миллиарда мобильных смартфонов, и это количество оказало колоссальное влияние на стоимость единицы продукции для собранных устройств и их микросхемных компонентов. В настоящее время стоимость смартфона в сборе в среднем упала ниже $100 за единицу в точке изготовления. Кроме того, стоимость устройств сдерживается благодаря использованию программного обеспечения с открытым исходным кодом для управления платформой и, конечно, благодаря использованию существующей вселенной веб-контента для загрузки на эти устройства. Это означает, что дополнительные издержки по предоставлению услуг для этих устройств так малы, что являются несущественными.

Кто является поставщиком этой индустрии? В 2014 году операционная система Google Android использовалась в 84% от общего количества отгруженных смартфонов и планшетов, тогда как операционная система Apple iOS использовалась для 12% всех устройств, а оставшаяся часть пришлась в основном на ОС Windows for Mobiles, которая в большинстве своем устанавливалась на платформы Nokia Lumina.

Эти пропорции долей рынка не обязательно трансформировались в эквивалентные соотношения доходов и стоимости корпораций. Если смотреть на стоимость компаний, то на конец февраля 2014 года рыночная капитализация Google составил примерно $368 миллиардов, что сравнимо с рыночной капитализацией Microsoft, составившей $359 миллиардов. Хотя в 2014 году на компанию Apple приходилось всего 12% отгруженных устройств, рыночная капитализация Apple в настоящее время равняется $755 миллиардам.

Причина, по которой эти доли рынка и уровни капитализации так отличаются, заключается в показателях доходов этих компаний.

Подход, основанный на программном обеспечении с открытым исходным кодом, который компания Google использует для своей платформы Android, не генерирует для Google тот же уровень дохода в пересчете на одно устройство. Компания Google по прежнему сильно зависит от своей рекламной деятельности, которая, согласно отчетам, принесла примерно 90% из общего объема поступлений в $66 миллиардов. Это приносит очень мало в смысле маржи от продажи аппаратных и программных платформ на мобильном рынке, а обоснование открытого распространения платформы Android возможно заключается в том, что получившаяся в результате среда с открытым доступом становится удобным полем для операций Google по размещению рекламы.

Выручка Microsoft в размере $86 миллиардов в основном складывается из поступлений от продажи коммерческих лицензий, что, по-видимому, являются наследием исторически доминирующего положения корпорации в сфере офисной ИТ-среды. Выручка от продаж операционной системы Windows Phone составила $2 миллиарда с маржой всего $54 миллиона.

Компания Apple является совершенно другим случаем. Мобильные продукты Apple принесли выручку в размере $150 миллиардов. Необходимо отметить, что компания Apple сохраняет очень жесткий уровень контроля как над своими аппаратными платформами, операционной системой iOS, программными приложениями, которые работают под управлением этой ОС, так и формами взаимодействия, которые эти приложения предлагают пользователям. Такая форма жесткой вертикальной привязки – от базовой аппаратной платформы и до розничной продажи услуг через магазин Apple Shop – означает, что компания Apple оказалась чрезвычайно эффективной в деле сохранения очень высокого уровня маржи от продажи продуктов iPhone. Легендарная одержимость Apple дизайном в этой области означает, что компания оказалась способна сохранить свое положение в глазах потребителей как производителя премиум-продуктов. В то же самое время, высокий уровень контроля над платформой привел к тому, что компания Apple смогла эффективно реализовать эту премиум-стоимость, направив поток выручки в сторону Apple. При этом Apple оставляет другим участникам, включая операторов мобильных сетей, лишь незначительную долю общей выручки.

Технологии мобильной связи

За последнее десятилетие услуги передачи данных в мобильном мире практически пережили революцию. В рамках исходной модели услуг передачи данных в архитектуре GSM для передачи данных использовался голосовой канал, при этом доступная скорость передачи обычно составляла 16 – 32 Кбит/с, а наложенная задержка равнялась 0,5 секунды.

Последующее внедрение стандартов 3G позволило двигаться в совершенно ином направлении, адаптируя модель W-CDMA с совместно используемыми каналами. Более короткие интервалы передачи, модифицированный алгоритм разрешения конфликтов и использование методов амплитудной и фазовой модуляции в несущем сигнале были объединены с технологией уступающего захвата канала. Результатом стала теоретическая скорость передачи данных 20 Мбит/с в нисходящем и 5,87 Мбит/с в восходящем направлении, однако этой теоретически возможной скорости редко удается добиться на практике. Более типичные скорости, с которыми сталкивается пользователь 3G-сетей, составляют 1 Мбит/с.

3G-сети используют модель каналов между шлюзом и устройством, а также используют протокол PPP для создания IP-соединения. Одним из побочных эффектов этой модели является то, что каждая ассоциация устройства привязана к IP адресу. Это означает, что для поддержки обоих протоколов IPv4 и IPv6 оператор должен выделить 2 канала для устройства с 2 стеками. Модель 4G LTE избавляется от PPP-канала и шлюза и использует внутреннюю инфраструктуру, полностью замкнутую на IP. В настоящее время устройство 4G способно работать в

режиме с двойным стеком и с двумя ассоциациями IPv4 и IPv6 с сетью без удвоения издержек на поддержание соединения. Кроме того, 4G использует преимущества более чувствительных цифровых сигнальных процессоров, устанавливаемых в телефонной трубке и в шлюзе, обеспечивая поддержку 64 QAM, а также использует несколько антенн MIMO для того, чтобы периодически получать более крупные сегменты спектра, если они доступны. В хороший день, когда ветер дует в спину и вы находитесь вблизи от незагруженной базовой станции, при отсутствии помех скорость 4G-соединения может даже превысить 100 Мбит/с. На практике большинство 4G-соединений характеризуются гораздо более низкой скоростью, однако большинство пользователей все равно замечают значительное улучшение по сравнению с 3G.

В то время как операторы мобильной связи участвуют в проектах по выбору конкретного варианта семейства (естественно) взаимно несовместимых 4G-услуг, которые они будут использовать для модернизации своей инфраструктуры базовых станций, технологии не стоят на месте. В начале 2015 г. компания Ericsson заявила права на лейбл 5G, утверждая, что провела лабораторные испытания канала 15 ГГц, используя модуляцию QAM и методы MIMO для того, чтобы добиться от радиосоединения скорости 5 Гбит/с. Компания Ericsson утверждает, что эта технология не будет доступна для широкого использования до 2020 г., хотя, как я подозреваю, за этим растянутым сроком реализации скрываются дополнительные проблемы. Среда городской застройки в основном прозрачна для радиочастот в диапазоне 100 МГц, однако по мере увеличения частоты сигнал сталкивается с возрастающими трудностями, связанными с поглощением и отражением, и к моменту, когда он достигает частот в диапазоне Ku, для распространения такого сигнала сегодня обычно требуется прямая линия видимости. Некоторые специалисты подозревают, что одной из крупных проблем, с которой столкнется Ericsson и программа 5G, станет изготовление сигнальных процессоров, способных справляться с трудностями, связанными с управлением высокочастотными сигналами в условиях городской застройки.

Будущее

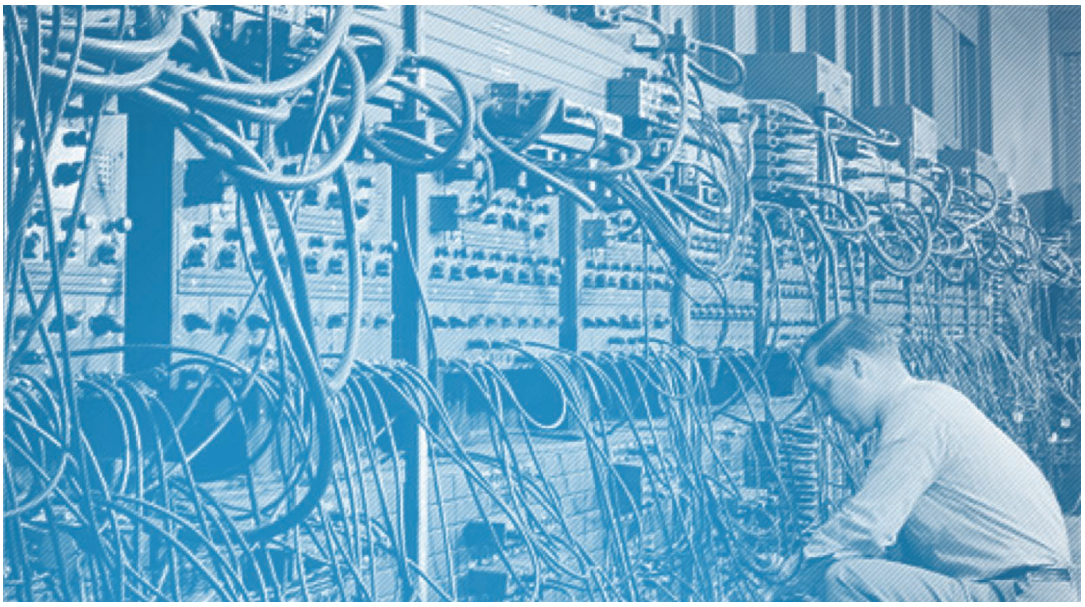
Куда направляется индустрия мобильной связи?

Рынок мобильных телефонов уже достиг уровней «супернасыщения», при этом в развитых странах использование мобильных SIM-карт превышает численность населения. Все выглядит так, что рынок смартфонов движется в точно таком же направлении. Однако существует несколько трещин, которые портят этот благодушный взгляд на будущее индустрии мобильной связи.

Базовым топливом для индустрии мобильной связи является спектр радиочастот. Существуют два типа спектра. Первый – это традиционная среда исключительных лицензий на использование спектра, при котором операторы мобильной связи платят государству лицензионный сбор за исключительный доступ к определенному диапазону спектра в определенной географической области. Модель распределения такого спектра менялась от административного распределения к открытым аукционам, а аукционная цена этих лицензий время от времени отражала иррациональный прилив крови в головы операторов мобильной связи. Высокая стоимость доступа к спектру означает, что оператор мобильной связи начинает свою деятельность с учетом нетривиального элемента затрат, а, помимо этого, оператор должен также инвестировать средства в создание физической установки и в операции по управлению бизнесом. Обычно аукционы на спектр частот проводятся таким образом, чтобы отдельный оператор не мог получить монопольное положение, и большинство правительственных органов добиваются того, чтобы в большинстве густонаселенных районов было от двух до четырех разных владельцев частот. Иногда такой уровень конкуренции достаточен для того, чтобы сформировать эффективный рынок без ценовых искажений, однако в других случаях небольшое число конкурентов и входные барьеры для новых участников ведут к различным формам искажений ценообразования на рынке мобильной связи, при которых розничная цена услуги не имеет прямой связи с базовыми издержками.

Однако конкурентное давление со стороны других операторов мобильной связи не является единственным источником конкуренции. Одним из важных факторов также является другая форма спектра частот. Системы WiFi используют два неуправляемых, совместно используемых диапазона – один на частотах 2,4 ГГц и второй 5 ГГц. Обычно существуют ограничения на максимальную мощность передачи сигнала, которая используется устройствами, работающими в этих диапазонах частот, но во всех других отношениях они открыты для доступа. В те-

Сохранится ли в будущем модель компьютера общего назначения или мы увидим усиление специализации по мере того, как компьютерная индустрия оставляет в прошлом универсальные модели и, вместо этого, все больше специализируется и старается «встроить» себя в каждый аспект нашей жизни?

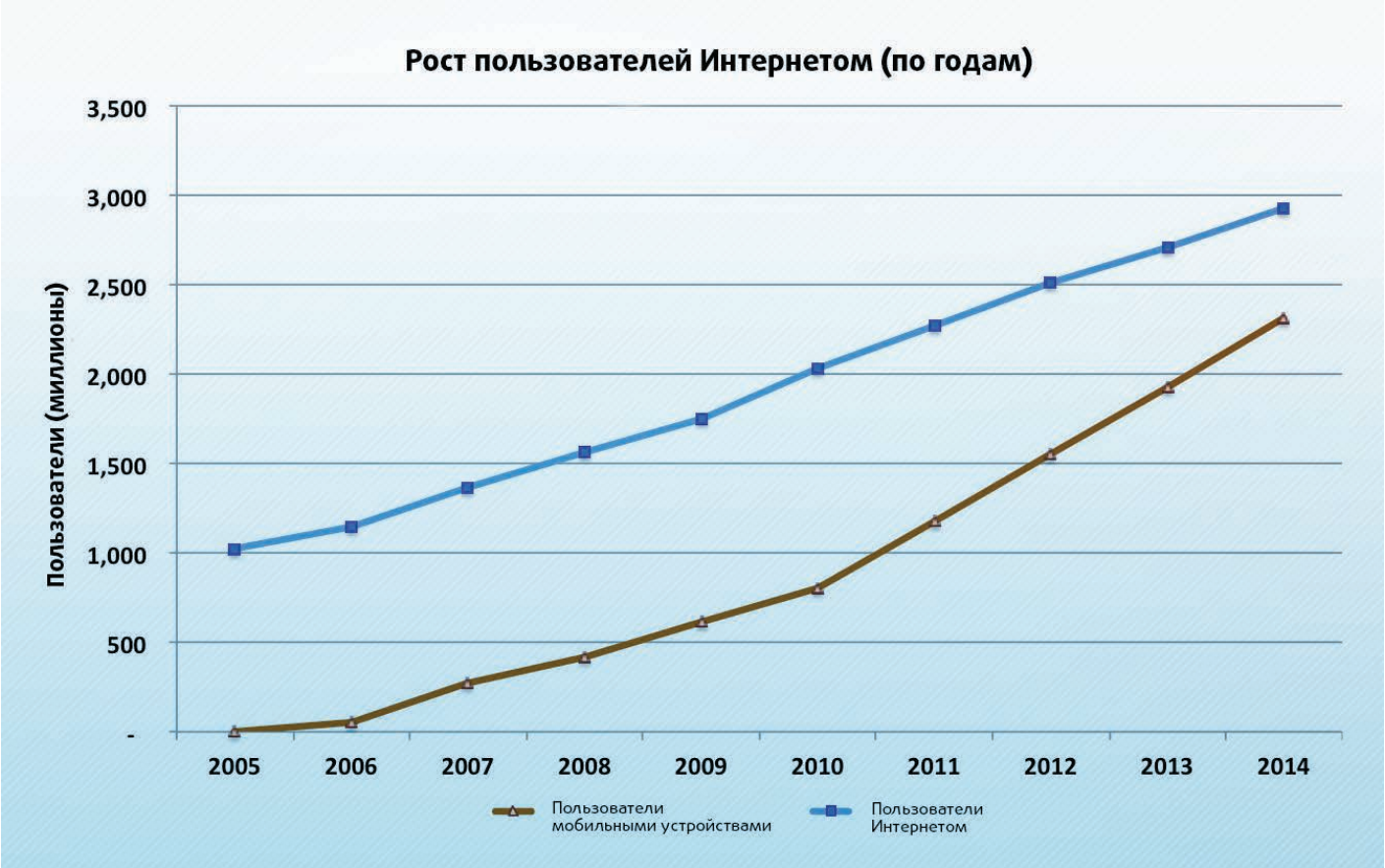


чение многих лет WiFi использовался для поддержки домашнего и корпоративного беспроводного доступа. Системы WiFi обычно работают на расстоянии до 70 м внутри здания и до 250 м на улице. Такой небольшой радиус действия WiFi-систем, который стал результатом ограничения на мощность передачи, к счастью позволил этим системам работать с чрезвычайно высокой пропускной способностью. Они работают на скоростях от 10-50 Мбит/с (спецификация 802.11b) и до 1,3 Гбит/с (спецификация 802.11ac). Ожидается, что в недалеком будущем эти скорости могут быть еще больше повышены.

В течение некоторого времени эти две модели использования спектра обеспечили разделение на два отдельных рынка. Спектр исключительного использования для «традиционных» операторов мобильной связи и совместно используемый спектр частот для самостоятельно установленных домашних и офисных приложений. Однако в настоящее время некоторые операторы инфраструктуры проводного доступа вступили в прямую конкуренцию с операторами сотовой связи в сфере предоставления услуг мобильной связи. Услуга Xfinity от компании Comcast в США является хорошим примером такого подхода. Компания сообщает о миллионах точек доступа WiFi, которые могут использоваться существующими клиентами Comcast без взимания дополнительной платы. Возможно это покажется удивительно, но некоторые крупнейшие операторы мобильной связи последовали этому примеру и также предлагают своим заказчикам услуги бесплатного WiFi-доступа. Например, компания AT&T имеет в США предложение WiFi-доступа. Частично это можно объяснить защитой своей доли рынка. Однако здесь также присутствует постоянная проблема «перенаселенности» в лицензируемых диапазонах радиочастот. Услуги передачи данных 3G и 4G являются адаптивными, они пытаются использовать все незадействованные мощности доступа. Однако в местах интенсивного использования, например в густонаселенных городских центрах, проблема предоставления услуг по высокоскоростной передаче данных в лицензируемом спектре частот становится весьма острой. Один из подходов заключается в использовании точек доступа WiFi в качестве разгрузочного механизма для таких районов с сильной перегрузкой. Наблюдение о том, что это приводит к столкновению с бизнес-целями WiFi-конкуренции операторов мобильной связи, возможно является дополнительным бонусом такого сценария!

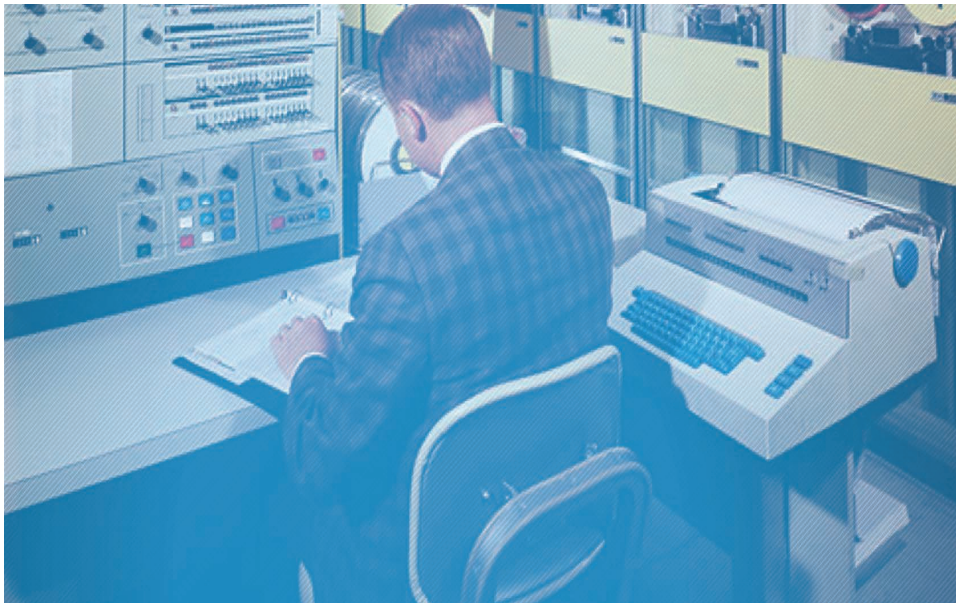
Однако с WiFi связаны некоторые проблемы, которые не столь очевидны в рамках традиционных услуг мобильной связи. Индустрия мобильной связи поддерживала хэндовер базовых станций с момента своего возникновения, что позволяло поддерживать активный поток данных на устройство даже при движении, при этом устройство «передавалось» от одной точки доступа другой. Передача обслуживания в рамках WiFi не так четко поддерживается. Проблема проявляется в тех случаях, когда точки доступа WiFi располагаются в разных IP-сетях, при этом передача обслуживания от одной точки доступа WiFi к другой подразумевает изменение IP-адреса устройства. Обычно изменение IP-адреса эквивалентно прерыванию всех активных соединений устройства. Однако возможно создать приложение, которое использует некоторую форму постоянства сеансовых ключей для того, чтобы позволить одной из конечных точек сеанса изменять IP-адрес при сохранении сеанса открытым и без потери состояния. Кроме того, уже имеются мобильные приложения, использующие протокол Multi-Path TCP, в которых логический сеанс разделялся между несколькими интерфейсами, потенциально по-

Рис.1. Рост числа пользователей Интернетом



зволяя добавлять и удалять интерфейсы из набора интерфейсов, поддерживающих этот логический сеанс TCP. По сути, устройство и его приложения теперь способны использовать преимущества среды с большим числом соединений, в которой все интерфейсы мобильного устройства можно соответствующим образом задействовать.

Что это означает для индустрии мобильной связи?



То, что мы наблюдаем, означает, что мобильнее устройство больше не привязано к оператору мобильной связи, и само устройство способно адаптивно реагировать на использование «наилучшей» сети вне зависимости от того, является ли решающим фактором наибольшая доступная пропускная способность или наименьшие предельные издержки для потребителя. С точки зрения устройства, сотовая сеть является просто одним из возможных поставщиков услуг передачи данных, и при этом можно использовать другие опции, такие, как WiFi, Bluetooth и USB-порты, а устройство способно сделать независимый выбор на основе собственных предпочтений.

Это имеет глубокие последствия. В то время как устройство было привязано к сотовой сети, эта сеть могла позиционировать себя как дорогую премиум-услугу с сопутствующими высокими ценами и большой маржой. Единственной формой конкуренции в рамках этой модели было предоставление услуг аналогично позиционирующими себя другими операторами мобильной связи. Ограниченное число лицензий на диапазоны частот часто означало, что игроки образовывали неформальные картели, а цены оставались высокими. После того, как устройство само становится способно использовать другие услуги доступа, операторы мобильной связи сталкиваются с серьезными трудностями при попытке сохранить премиальную надбавку к цене за свои услуги. В результате, сектор услуг мобильной связи неумолимо переходит к модели услуг, характерной для сырьевых товаров. Премиум-продукт мобильной голосовой связи теперь превращается в еще один неразличимый поток цифровых данных, а маржа операторов мобильной связи подвергается постоянному разъедающему давлению. Операторы, использующие открытые нелицензируемые WiFi-частоты, способны оказать значительное коммерческое давление на установившихся участников рынка мобильной связи. Это означает, что премиальная надбавка к цене, уплачиваемая за исключительное использование спектра частот, давит на маржу операторов, чьи доходы все в большей степени поступают от услуг, связанных с «товарной» передачей данных.

Возможно на этом пути встретится большее число изменений. «Улучшения», которые превратили мобильный телефон в смартфон, не были мотивированы предоставлением более качественной голосовой связи. Нисколько. Изменения заключались в том, что устройство добавило удобные для глаз дисплеи, камеры, средства сенсорного управления, локальное хранилище данных, средства позиционирования и доступ ко всем онлайновым услугам, к которыми мы привыкли, работая за настольным компьютером. То, что мы имеем сегодня, это эквивалент вчерашнего универсального мейнфрейма в вашем кармане. Направление изменений в рамках этой модели, заключается в увеличении памяти, повышении разрешения дисплея, снижении энергопотребления, повышении процессорной мощности. Другими словами, незначительные улучшения той же самой базовой модели. Однако мы также наблюдаем появление нового спектра специализированных продуктов, которые также используют мобильность, но не являются универсальными компьютерами, а превратились в специальные устройства, предназначенные для предоставления конкретных услуг. Хорошим примером такого вида специализации является «Fitbit» (фитнес-трекер), который представляет собой специализированное устройство, измеряющее физическую активность носителя. Кредитные карты, а также множество муниципальных карт для проезда в метро теперь включают встроенные процессоры, которые хранят данные о стоимости в самой карте. Сегодня многие страны выдают паспорта со встроенными электронными чипами.

Сохранится ли в будущем модель компьютера общего назначения или мы увидим усиление специализации по мере того, как компьютерная индустрия оставляет в прошлом универсальные модели и, вместо этого, все больше специализируется и старается «встроить» себя в каждый аспект нашей жизни?

Похоже, что мы на самом деле наблюдаем как Интернет и даже компьютеры, населяющие Интернет, постепенно пропадают из общественного фокуса. По-видимому, эти технологии стали такой неотъемлемой частью нашей жизни, что мы больше не распознаем их как что-то специальное или особенное. Они неотвратимо вплетают себя в ткань нашей жизни. И важнейшим элементом этого преобразующего изменения стало «отвязывание» Интернета с помощью мобильности, принятой с таким энтузиазмом. Интернет, который теперь присутствует постоянно и всегда доступен, больше неосязаем. Подобно воде из водопроводного крана, мы будем реально замечать ту роль, которую играет вездесущий Интернет, только в те редкие моменты, когда его не будет с нами!

Источник: The Mobile Internet. Geoff Huston. The ISP Column

Временная шкала развития Мобильного Интернета*

2015

Октябрь — Продано больше планшетов, чем ПК

Октябрь — 3 млрд. пользователей

Май — В США более половины времени, проводимого онлайн, приходится на мобильные приложения

Май — 75 млрд. загрузок iOS

Июнь — Больше было продано смартфонов, чем других, в развивающихся странах

2014

Сентябрь — Смартфонов продано больше, чем обычных телефонов в мире

Сентябрь — Больше продано планшетов, чем ноутбуков

Август — 50 млрд. загрузок с Google Play

Июль — Появление Firefox OC

2013

Апрель — Более 50% времени, проводимого онлайн с использованием смартфона, приходится на приложения

Май — Появление Windows phone

2012

Декабрь — Больше 50% пользователей в развивающихся странах используют широкополосный доступ

2010

Октябрь — Запуск 4G

2009

Декабрь — Появление Blackberry App Store

Апрель — Появление Android Market

Октябрь — Появление Apple Store

2008

Июль — Появление iPhone

2007

Июнь — Запуск 3G

2001

Октябрь — Появление GPRS

2000

*Источник: Timeline of Milestones in the Development of the Mobile Internet. Internet Society Global Internet Report 2015. Michael Kende

Гигабитный Ethernet: от 1 до 100 Гбит/с и быстрее

Уильям Сталлингс (William Stallings)

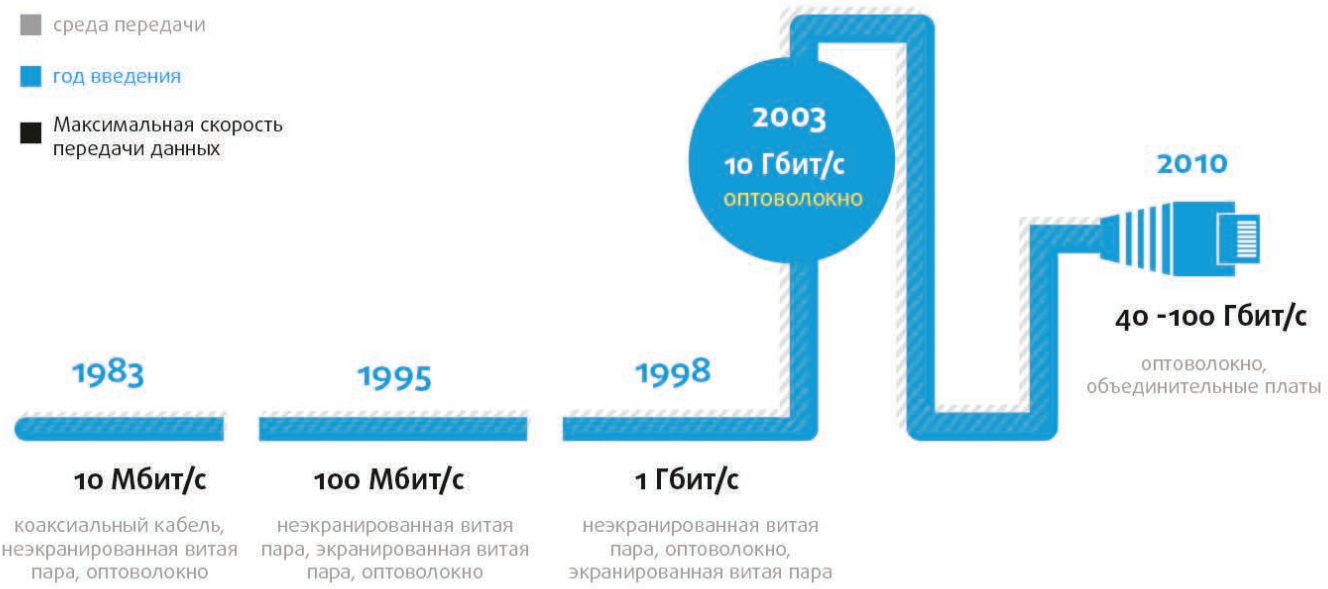
Ethernet является широко распространенной и доминирующей технологией для проводных локальных сетей. Преимущественно используется в корпоративных ЛВС, для обеспечения ШПД, в ЦОДах, а также для связи между сетями MAN и даже WAN. Рынок решений на основе Ethernet достиг достаточных размеров для того, чтоб ускорить увеличение скоростей для конкретных видов использования. Залог популярности технологии Ethernet кроется в наличии недорогих, надежных и совместимых сетевых решений от целого ряда поставщиков. Успешность гигабитного и 10-гигабитного Ethernet подтверждает важность выбора технологий, связанных с управлением сети.

Технология Ethernet появилась в начале 1980-х годов и с тех пор стала основным решением для развертывания локальных вычислительных сетей (ЛВС) в офисном пространстве. Требования к пропускной способности ЛВС стремительно росли из года в год. К счастью, росла и пропускная способность Ethernet. Сейчас на дворе эпоха гигабитного Ethernet.

Изначально Ethernet представлял собой систему на базе шинной топологии со скоростью передачи данных 2.94 Мбит/с по коаксиальному кабелю. В топологии типа «общая шина» все рабочие станции подключены к одному кабелю, при этом станции не могут передавать одновременно, а только последовательно. Использование шины регулируется с помощью протокола управления доступом к среде (Medium Access Control – MAC), в основе которого лежит принцип обнаружения конфликтов. По сути, каждая рабочая станция может свободно передавать MAC-кадры по шине. Если станция обнаруживает конфликт при передаче, она приостанавливает передачу и через некоторое время предпринимает новую попытку.

Первым поступившим в продажу оборудованием на основе Ethernet стали системы на базе шинной топологии со скоростью 10 Мбит/с. Их появление совпало с разработкой единого стандар-

Рис.1. Стандарты физического уровня IEEE 802.3



та Ethernet комитетом IEEE 802.3. Также, не меняя MAC-протокол или формат MAC-кадров, можно было использовать конфигурацию на базе топологии «звезда», при которой трафик идет через центральный узел, а пересылка данных через узел возможна в определенный момент времени только одной станцией. Для повышения пропускной способности вместо узла используется коммутатор, что позволяет работать в полнодуплексном режиме. При использовании коммутатора применяются тот же формат и протокол MAC, однако обнаружения конфликтов больше не требуется. По мере роста спроса и требований к пропускной способности был усовершенствован MAC-уровень. В частности, были увеличены кадры MAC-уровня.

В настоящее время скорость систем Ethernet достигает 100 Гбит/с. На рис.1 обобщена информация об этапах развития стандартов IEEE 802.3.

Технология Ethernet быстро завоевала всеобщее признание и стала основной технологией для ЛВС, со временем также распространившись на региональные вычислительные сети. Она применяется в различных целях и средах.

Ошеломляющий успех технологии Ethernet обусловлен ее чрезвычайно высокой адаптивностью. При любой пропускной способности используется один и тот же протокол и формат кадров MAC. Различия наблюдаются на физическом уровне, в определении метода сигнализации и средствах передачи.

Теперь рассмотрим характеристики Ethernet с гигабитными скоростями передачи данных.

Гигабитный Ethernet (1 Гбит/с)

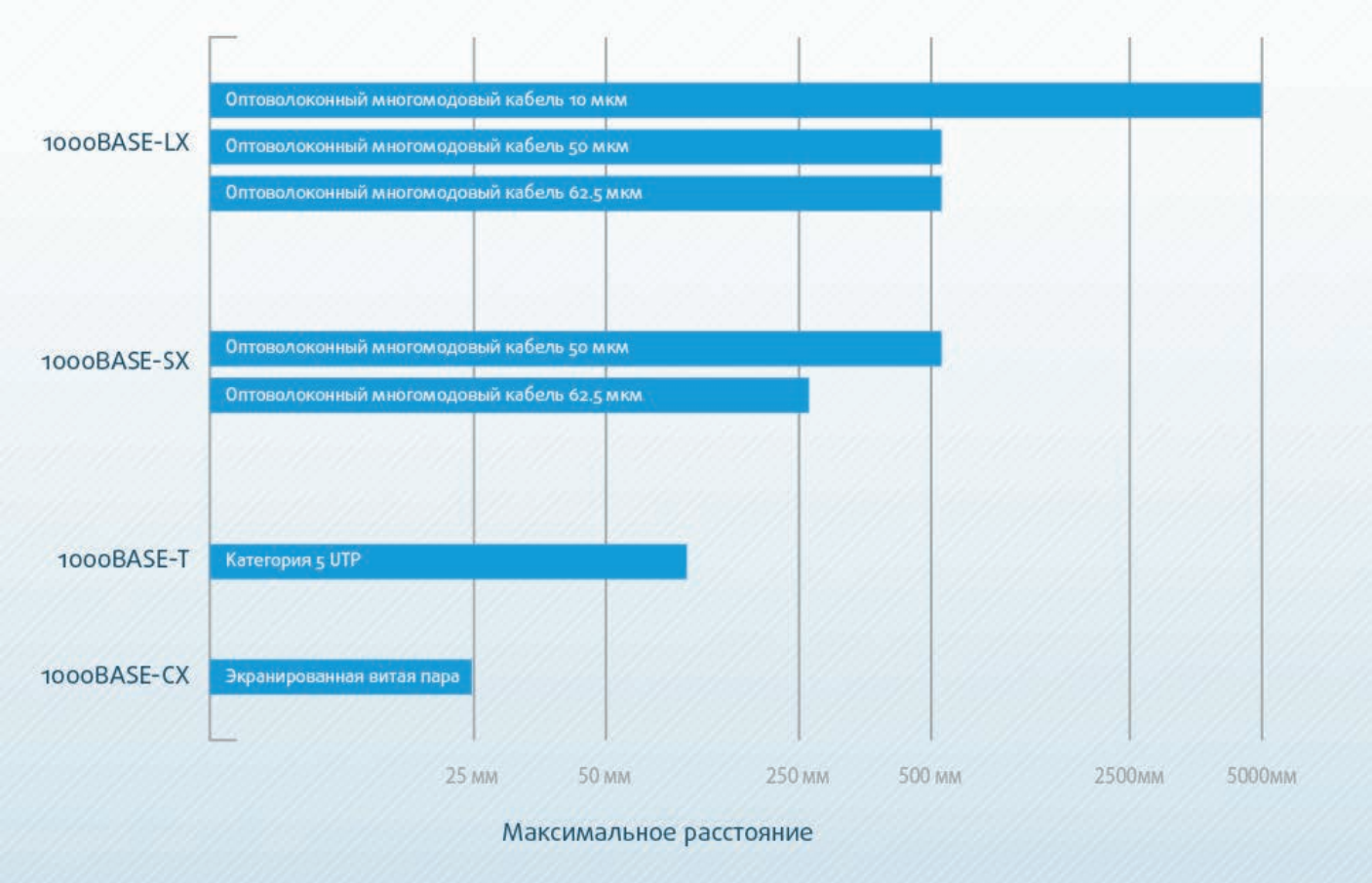
На протяжении многих лет первоначальной мощности Ethernet (10 Мбит/с) было достаточно для удовлетворения нужд большинства офисов. Однако к началу 1990-х годов стала очевидна необходимость повышения скорости передачи дынных для поддержки растущей нагрузки трафика в типичной локальной сети.

Основными движущими силами процесса повышения скорости Ethernet стали:

- Централизованные серверные фермы: во многих мультимедийных приложениях требуется, чтобы клиентская система могла получать большие объемы данных от множества централизованных серверов, которые называются «серверные фермы». С ростом производительности серверов пропускная способность сети стала недостаточной.

- Рабочие группы, потребляющие большие объемы данных: как правило, такие группы состоят из небольшого количества пользователей, которым требуется обмениваться по сети большими файлами. Например, разработчики программного обеспечения и специалисты по компьютерному моделированию.

Рис.2. Вариант сред для гигабитного Ethernet (сопоставление)



- Высокоскоростные магистральные сети: по мере роста требований к производительности компьютеров, компании стали создавать системы ЛВС, связанные высокоскоростными магистральными линиями.

Для удовлетворения таких потребностей комитет IEEE 802.3 разработал ряд спецификаций для повышения пропускной способности Ethernet до 100 Мбит/с, а еще через несколько лет были созданы стандарты для гигабитного Ethernet. В каждой новой спецификации новые средства передачи и схемы кодировки строились на основе уже известной технологии Ethernet, что делало переход на новые стандарты проще, чем если бы каждый раз спецификации создавались с нуля.

Гигабитный стандарт включает ряд вариантов передачи данных (Рис. 2):

- 1000BASE-SX: Коротковолновый вариант. Оптоволоконный многомодовый кабель диаметром 62,5 мкм и длиной до 275 м или диаметром 50 мкм и длиной до 550 м, поддерживающий дуплексные линии. Используемые длины волн находятся в диапазоне от 770 до 860 нм.

- 1000BASE-LX: Длинноволновый вариант. Оптоволоконный многомодовый кабель диаметром 62,5 мкм или 50 мкм, поддерживающий дуплексные линии длиной до 550 м или одномодовый кабель диаметром 10 мкм длиной до 5 км. Используемые длины волн находятся в диапазоне от 1270 до 1355 нм.

- 1000BASE-CX: Этот вариант поддерживает гигабитные линии связи между устройствами, расположенными в одном помещении или в одной аппаратной стойке, для которых используются медные перемычки (специализированные экранированные кабели из витых пар протяженностью не более 25 м). Каждая линия состоит из отдельной экранированной витой пары, данные по которой передаются в обе стороны.

- 1000BASE-T: Этот вариант использует четыре неэкранированных витых пары категории 5 для связи с устройствами на расстоянии до 100 м, передавая и получая данные на все четыре пары одновременно с эхокомпенсацией.

В первых трех из вышеприведенных вариантов гигабитного Ethernet используется система кодирования 8B/10B, в которой 8-битные символы при передаче кодируются 10 битами. Добавление битов выполняет две функции. Во-первых, в результате код обеспечивает стабильное соотношение нолей и единиц по сравнению с некодированным потоком и позволяет ограничить число подряд идущих нолей и единиц, которые иначе бы замедляли синхронизацию между отправляющим и получающим устройствами. Во-вторых, код позволяет выявлять ошибки.

Для 1000BASE-T используется кодирование 4D-PAM5, сложная система, описание которой не входит в задачи данной статьи.

Как правило, при использовании гигабитного Ethernet, опорный коммутатор ЛВС со скоростью 1 Гбит/с обеспечивает связь по магистральной линии с центральными серверами и коммутаторами Ethernet высокоскоростных рабочих групп. Каждый коммутатор рабочей группы поддерживает как связь со скоростью 1 Гбит/с для соединения с опорным коммутатором ЛВС и поддержки высокопроизводительных серверов рабочих групп, так и связь со скоростью 100 Мбит/с для работы с высокопроизводительными рабочими станциями, серверами и коммутаторами ЛВС со скоростью 100 Мбит/с.

10-гигабитный Ethernet

Еще не высохли чернила на спецификациях гигабитного Ethernet, когда стало ясно, что по мере роста трафика эта технология не сможет удовлетворить растущие потребности даже в краткосрочной перспективе. В связи с этим комитет IEEE 802.3 вскоре принял стандарт 10-гигабитного Ethernet. Основным требованием для нового стандарта было повышение внутрисетевого трафика (локальные взаимосвязанные сети) и интернет-трафика.

Стремительный рост внутрисетевого и интернет-трафика стал результатом целого ряда факторов:

- Рост количества сетевых подключений.

- Рост скорости соединения каждой рабочей станции (например, пользователи с подключением 10 Мбит/с стали переходить на 100 Мбит/с, а те, кто пользовался аналоговыми модемами 56K стали переходить на DSL или кабельные модемы).

- Распространение приложений, требующих большой пропускной способности сети, например, высококачественного видеоконтента.

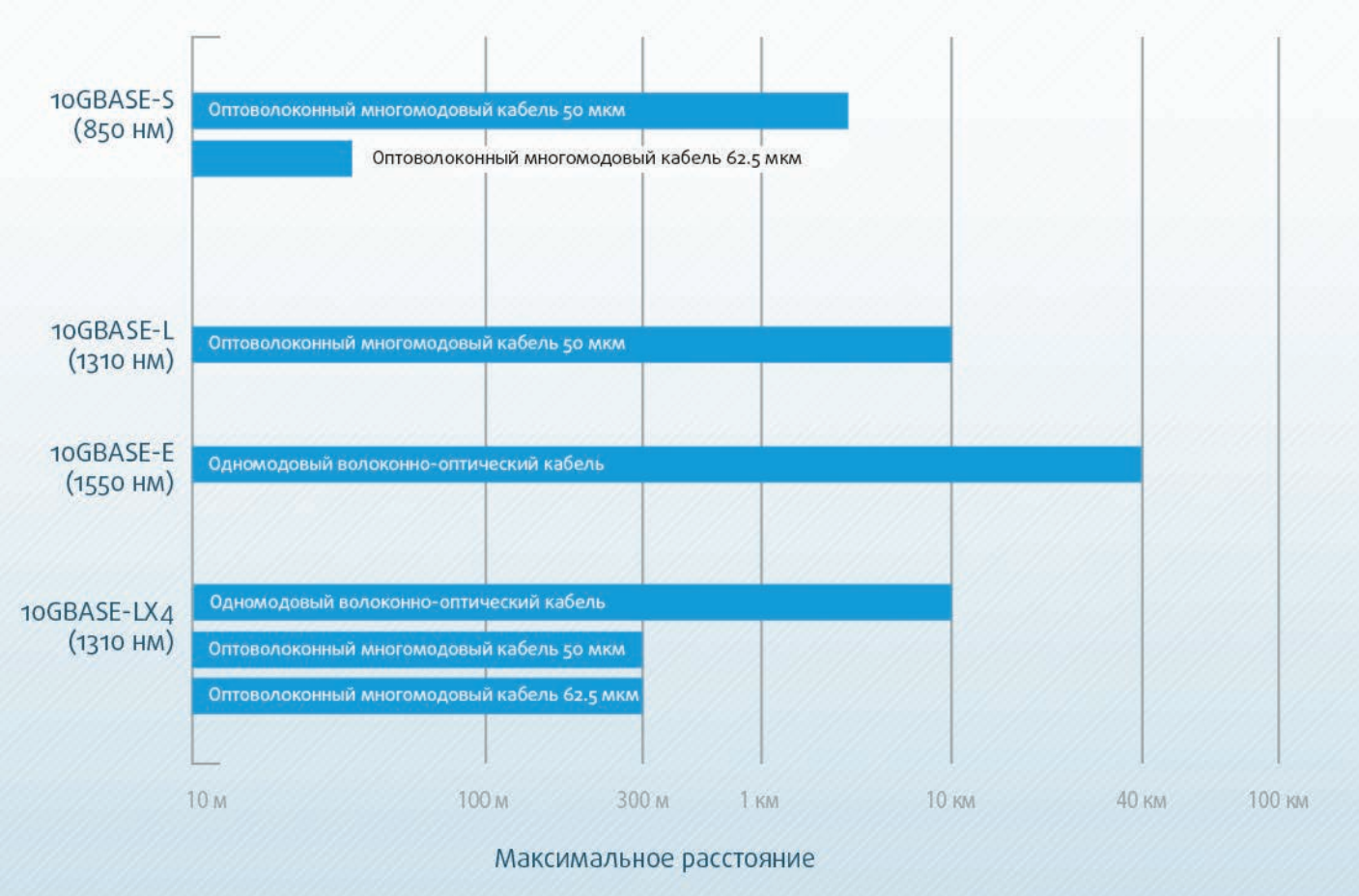
- Рост трафика по интернет-хостингу и хостингу приложений.

Изначально 10-гигабитный Ethernet использовался на высокоскоростных локальных магистральных линиях, соединяющих мощные коммутаторы. По мере повышения требований к пропускной способности, 10-гигабитный Ethernet стали применять и в других сегментах сети, включая серверные фермы, опорные и локальные сети. Эта технология позволяет интернет-провайдерам и поставщикам услуг сетевого доступа обеспечивать высокую скорость связи при минимальных издержках между коммутаторами операторского класса и маршрутизаторами.

Данная технология также позволяет строить сети MAN и WAN, соединяющие географически удаленные друг от друга ЛВС между кампусами или точками присутствия (PoP). Таким образом, Ethernet стал конкурировать с протоколом ATM (асинхронный режим передачи) и другими географически распределенными системами и сетевыми технологиями передачи данных. В большинстве случаев, когда требования заказчика сводятся к передаче данных и использованию TCP/IP, 10-гигабитный Ethernet обладает существенными преимуществами по сравнению с протоколом ATM как для конечных пользователей, так и для провайдеров. К таким преимуществам относятся следующие:

- Не требуется осуществлять дорогостоящую конвертацию пакетов Ethernet в ячейки ATM, существенно снижающую пропускную способность; вся сеть работает по технологии Ethernet.

Рис.3. Диапазон работы 10-гигабитного Ethernet



- Сочетание IP и Ethernet обеспечивает возможность отслеживать качество и класс предоставляемых услуг передачи данных на сопоставимом с ATM уровне, то есть продвинутые технологии управления трафиком доступны как пользователям, так и провайдерам.

- В спецификациях 10-гигабитного Ethernet представлено большое разнообразие стандартных оптических интерфейсов (длина волны и расстояние), что способствует оптимизации функционирования самой технологии и делает использование LAN, MAN и WAN менее затратным.

Максимальное расстояние колеблется от 300 метров до 40 километров. Связь работает исключительно в полнодуплексном режиме на различном оптоволоконном оборудовании.

Для 10-гигабитного Ethernet предусмотрены четыре стандарта физической среды (Рис. 3). Первые три имеют по два подвида: R и W. Буквой R обозначаются виды физической среды, в которых применяется технология кодирования 64B/66B (66 бит линейного кода на 64 бита данных), обладающая теми же преимуществами, что и 8B/10B при более низких накладных расходах. Стандарты R предназначены для так называемого темного волокна, то есть для не работающих в данный момент каналов волоконно-оптического кабеля, которые не соединены с каким-либо оборудованием. Буквой W обозначаются виды физической среды, в которых также используется код 64B/66B, и имеется возможность подсоединения к оборудованию синхронных оптических сетей.

Ниже приведены описания четырех стандартов физической среды:

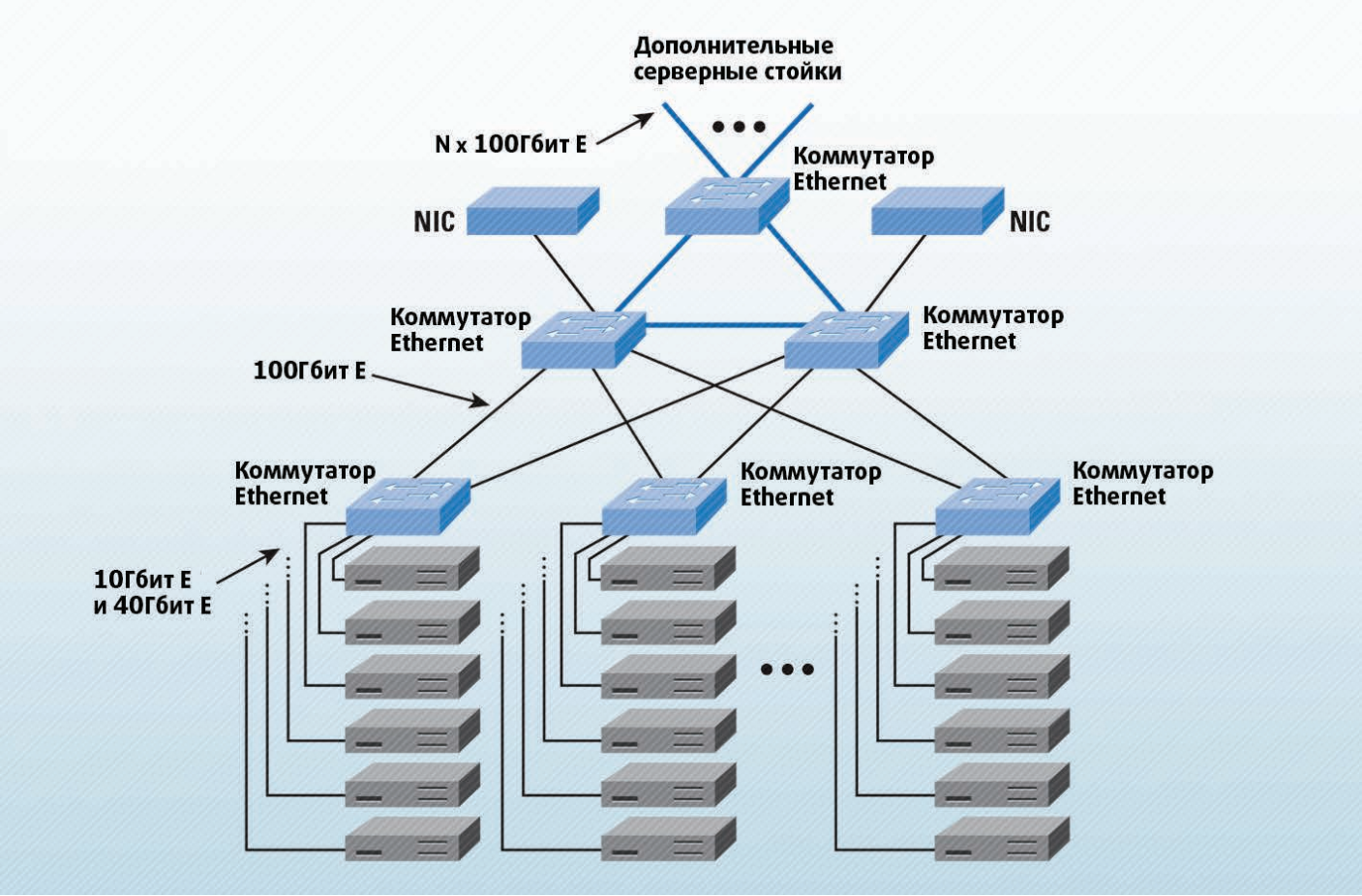
- 10GBASE-S (для коротких расстояний): 850 нм по многомодовому волокну с поддержкой расстояний до 300 метров. Существуют версии 10GBASE-SR и 10GBASE-SW.

- 10GBASE-L (для дальних расстояний): 1310 по одномодовому волоконно-оптическому кабелю с поддержкой расстояний до 10 км. Существуют версии 10GBASE-LR и 10GBASE-LW.

- 10GBASE-E (расширенный): 1550 нм по одномодовому волоконно-оптическому кабелю при поддержке расстояний до 40 км. Существуют версии 10GBASE-ER и 10GBASE-EW.

- 10GBASE-LX4: 1310 нм по одномодовому волоконно-оптическому кабелю при поддержке расстояний до 10 км. В данной среде используется технология оптического мультиплексирования WDM для мультиплексирования четырех несущих волн.

Рис.4. Пример конфигурации 100-гигабитного Ethernet для крупного объекта с множеством сверхкомпактных серверов



40-гигабитный и 100-гигабитный Ethernet

Ethernet – оптимальная и наиболее распространенная технология для проводных локальных сетей. Именно ей отдается предпочтение при развертывании корпоративных ЛВС, обеспечении работы широкополосного доступа и центров обработки и хранения данных (ЦОДов). Ethernet также пользуется популярностью в рамках сетей MAN и даже WAN.

Кроме того, Ethernet на данный момент является наиболее популярным средством предоставления проводного сигнала для обеспечения работы таких беспроводных технологий как Wi-Fi and WiMAX в локальных сетях Ethernet.

Популярность технологии Ethernet обусловлена наличием недорогих, надежных и совместимых сетевых продуктов от различных поставщиков. По мере сближения и объединения различных средств связи, разрастания серверных ферм, популяризации IP-телефонии, IP-телевидения и приложений Web 2.0 появился спрос на коммутаторы Ethernet с еще большей пропускной способностью. Появлению 100-гигабитного Ethernet способствовало следующее:

- ЦОДы и поставщики мультимедийных интернет-ресурсов: по мере увеличения объема мультимедийного контента в интернете и роста популярности интернет-приложений, поставщики контента расширяют ЦОДы, максимально используя возможности 10-гигабитного Ethernet. Такие компании, скорее всего, первыми перейдут на 100-гигабитный Ethernet в силу необходимости обеспечения высокой пропускной способности.

- Городские сетевые операторы и поставщики видеоконтента: развитие сегмента видео по запросу сыграло определяющую роль в развитии нового поколения городских сетей на основе 10-гигабитного Ethernet. В среднесрочной перспективе таким провайдерам наверняка тоже потребуется высокая пропускная способность.

- Корпоративные ЛВС: продолжение сближения голосовой связи, видеосервисов и услуг по хранению данных ведет к повышению требований к коммутаторам. Однако большинство компаний до сих пор располагают лишь гигабитным или 10-гигабитным Ethernet, а переход на 100-гигабитный Ethernet вряд ли будет быстрым.

- Точки обмена интернет-трафиком и опорные сети крупных провайдеров: через эти узлы проходят огромные потоки информации, что не может не способствовать переходу на 100-гигабитный Ethernet.

В 2007 году рабочая группа IEEE 802.3 разрешила создать проектное подразделение IEEE P802.3ba по разработке 40-гигабитного и 100-гигабитного Ethernet. В запросе на создание проекта 802.3ba приводилось множество примеров ситуаций, в которых необходимая пропускная способность выше, чем 10 Гбит/с. Речь шла о точках обмена интернет-трафиком, высокопроизводительных вычислениях и доставке видео по запросу. В запросе также приводилось обоснование наличия в новом стандарте двух скоростей передачи данных (40 и 100 Гбит/с), согласно которому темпы роста потребностей сетей и конечных станций неодинаковы.

На Рис. 4 показаны примеры использования 100-гигабитного Ethernet. В крупных ЦОДах с большим количеством сверхкомпактных серверов наблюдается тенденция по оснащению отдельных серверов 10-гигабитными портами, чтобы они могли справляться с большими объемами проходящего через них трафика. Обычно в одной стойке несколько серверов и один или два 10-гигабитных коммутаторов для соединения всех серверов и взаимодействия с другими стойками. Коммутаторы обычно встроены в стойку и называются ToR (Top-of-Rack)-коммутаторами. Термин ToR считается синонимом понятия «коммутатор доступа», даже если он не расположен на верхнем этаже стойки (top of rack). Обеспечение связи между множеством стоек сверхкомпактных серверов за счет установки в них дополнительных 10-гигабитных коммутаторов представляется все менее целесообразным для крупных ЦОДов, предоставляющих, например, услуги по хранению и обработке облачных данных. Для обработки все большего объема данных требуются коммутаторы с пропускной способностью более 10 Гбит/с. С их помощью можно не только обеспечить связь между серверными стойками, но и соединение с внешними устройствами посредством контроллеров сетевого интерфейса (NICs).

Первые устройства этого уровня появились в 2009 году, а создание стандарта IEEE 802.3ba завершилось в 2010 году. Пока большинство компаний отдает предпочтение 40-гигабитным коммутаторам, однако, ожидается, в ближайшие годы рыночная доля 40-гигабитного и 100-гигабитного Ethernet существенно вырастет.

Стандартом IEEE 802.3ba предусмотрено три типа среды

Таблица 1. Варианты физической среды для 40-гигабитного и 100-гигабитного Ethernet

	40 Гбит/с	100 Гбит/с
1 метр по объединительной плате	40GBASE-KR4	40GBASE-KR4
10 метров по медному кабелю	40GBASE-CR4	100GBASE-CR10
100 метров по многомодовому волокну	40GBASE-SR4	100GBASE-SR10
100 метров по многомодовому волокну	40GBASE-KR4	40GBASE-KR4
10 км по одномодовому волокну	40GBASE-LR4	100GBASE-LR4
40 км по одномодовому волокну		100GBASE-ER4

Обозначения:

Медь: K = объединительная плата; C = соединение кабелей

Оптоволокно: S = короткий (100 м); L - длинный (10 км);

E = расширенный диапазон (40 км)

Система кодирования: R = блочное кодирование 64B/66B

Последняя цифра: кол-во линий (медный кабель или длина волн для оптоволокна)

(Таблица 1): медная плата, твин-аксиальный кабель (что-то вроде коаксиального кабеля) и оптоволокно. Для меди предусмотрено четыре отдельные физические линии. Для оптоволокна предусмотрены либо 4, либо 10 длин волн в зависимости от расстояния и пропускной способности.

Метод многополосного распределения (Multilane Distribution, MLD)

В основе стандарта 802.3ba лежит технология MLD, позволяющая достигать требуемых скоростей. В этой связи необходимо рассказать о двух концепциях: собственно об MLD и о виртуальных полосах.

В целом, метод MLD заключается в том, что для обеспечения скорости в 40 Гбит/с или 100 Гбит/с можно соединить конечную станцию с Ethernet коммутатором или два коммутатора по нескольким параллельным полосам (каналам). Эти полосы могут быть отдельными проводами, например, соединение узлов четырьмя параллельными витыми парами. Другой вариант заключается в разделении полос по частоте, как это делается с помощью технологии WDM по оптоволоконному кабелю.

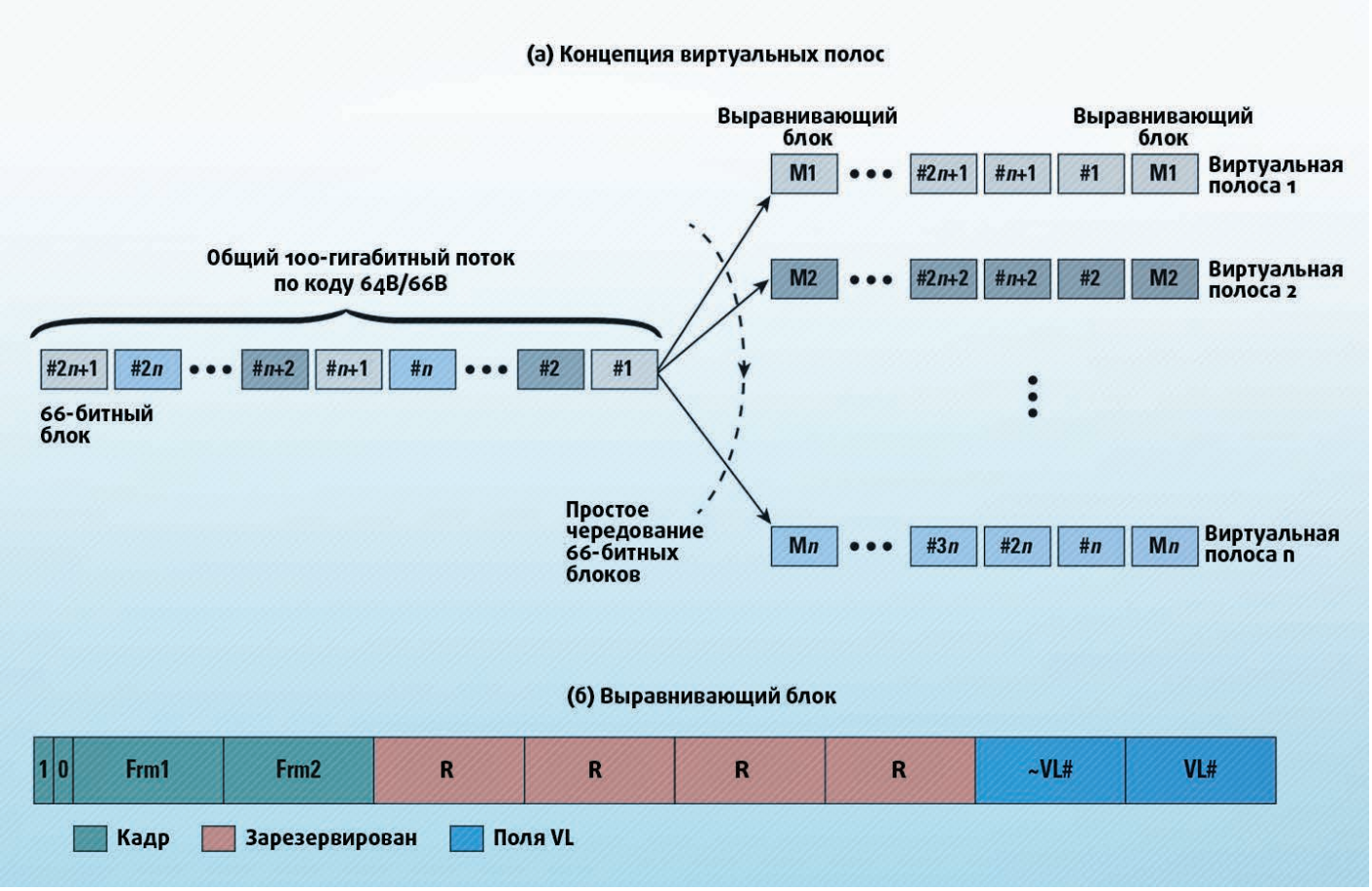
Для наглядности, остановимся на конкретном примере многополосной структуры физического подуровня PMA (Physical Medium Attachment, модуль доступа к физической среде). Создаваемые полосы называются виртуальными полосами. Если количество полос в электрическом или оптическом канале не совпадает, виртуальные полосы принимаются соответствующим количеством физических полос подуровня PMD (Physical Medium Dependent, зависимый от физической среды модуль). Это вид обратного мультиплексирования.

На Рис. 5(a) показана схема виртуальных полос. Поток данных пользователя кодируется по системе 64B/66B, которая также применяется в 10-гигабитном Ethernet. Данные поступают в виртуальные полосы путем чередования 66-битных блоков (первое слово – первая полоса, второе слово – вторая полоса и т. п.) В каждую виртуальную полосу периодически добавляется уникальный «выравнивающий» 66-битный блок. Эти блоки используются для выявления и упорядочивания виртуальных полос и восстановления общего потока данных.

Затем виртуальные полосы передаются по физическим полосам. Если физических полос меньше, чем виртуальных, используется мультиплексирование на уровне битов. Количество виртуальных полос должно быть кратно (1 или более) количеству физически полос.

На Рис. 5(b) показан формат выравнивающих блоков. Блок состоит из восьми однобайтовых ячеек, перед которыми идет двухбитное поле синхронизации со значением 10. Ячейки Кадр содержат последовательность кадров, присущую всем виртуальным полосам и ис-

Рис.5. Функционирование 100-гигабитного Ethernet по MLD методике



пользуемую получателем для выстраивания блоков. Поля VL# содержат информацию об уникальных характеристиках виртуальных полос: одна ячейка содержит двоичный код, обратный содержанию второй ячейки.

25-гигабитный и 50-гигабитный Ethernet

Одним из вариантов внедрения 100-гигабитного Ethernet является создание четырех 25-гигабитных полос. Таким образом, разработка стандартов 25-гигабитного и 50-гигабитного Ethernet на основе одной или двух полос не представляет особой трудности. Наличие двух альтернативных решений, основанных на технологии 100-гигабитного Ethernet, позволило бы пользователям более гибко реагировать на текущие и будущие запросы, поскольку такое решение позволяет без особых усилий повысить пропускную способность.

Такие рассуждения привели к образованию консорциума 25-гигабитного Ethernet силами ведущих провайдеров облачных услуг, включая Google и Microsoft. Цель этого консорциума заключается в поддержке совместимости в рамках отраслевого стандарта Ethernet для повышения производительности и снижения издержек в расчете на Гбит/с соединения между сетевой картой сервера и ToR коммутатора. Принятая консорциумом спецификация предусматривает однополосный 25-гигабитный Ethernet протокол и двухполосный 50-гигабитный Ethernet протокол. Пропускная способность этих решений превышает мощность физических полос по твинаксиальному медному кабелю от стойки до коммутатора до 2,5 раз по сравнению с 10-гигабитным и 40-гигабитным Ethernet. В настоящее время в рамках комитета IEEE 802.3 ведется разработка необходимых стандартов для 25-гигабитного Ethernet, которые также могут включать 50-гигабитный Ethernet.

Пока сложно сказать какой из этих вариантов (25, 40, 50 или 100 Гбит/с) завоюет рынок. В среднесрочной перспективе, скорее всего, 100-гигабитные коммутаторы будут преимущественно востребованы на крупных объектах, тогда как возможность использовать менее дорогие и не такие быстрые альтернативы дает компаниям различные варианты по наращиванию пропускной способности по мере роста спроса.

400-гигабитный Ethernet

Со временем запросы увеличиваются. Комитет IEEE 802.3 в настоящее время изучает возможность создания 400-гигабитного стандарта Ethernet. Пока о каких-либо конкретных сроках не сообщалось. А если заглянуть еще дальше в будущее, мало кто спорит с тем, что когда-нибудь будет и стандарт для терабитного Ethernet (один терабит – триллион бит в секунду).

2,5-гигабитный и 5-гигабитный Ethernet

В силу универсальности и вездесущности Ethernet, а также по мере разработки стандартов для все более высоких скоростей, появилось предложение о стандартизации 2,5-гигабитного и 5-гигабитного варианта Ethernet. Это предложение пользуется всеобщей поддержкой. Эти стандарты имеют сравнительно небольшую скорость. Их называют Multirate Gigabit BASE-T (MGBASE-T). В настоящее время Альянс MGBASE-T занимается координацией разработки стандартов без участия IEEE. Не исключено, что в конечном счете комитет IEEE 802.3 подготовит стандарты, в основу которых ляжет проделанная в отрасли работа.

Эти два варианта в первую очередь предназначены для доставки беспроводного трафика IEEE 802.11ac в проводные сети. IEEE 802.11ac – это 3,2-гигабитный стандарт для Wi-Fi, который пользуется все большей популярностью там, где требуются скорости выше 1 Гбит/с. Например, речь может идти о беспроводной связи в офисном пространстве. Новый беспроводной стандарт предоставляет больше возможностей по сравнению с гигабитным Ethernet, при этом не требуя перехода на 10-гигабитный Ethernet, что на ступень выше. Если бы 2,5-гигабитный и 5-гигабитный Ethernet мог работать на кабеле для гигабитного Ethernet, такой стандарт обеспечил бы повышение скорости для точек доступа, поддерживающих беспроводные сети 802.11ac с высокой пропускной способностью.

Залог популярности технологии Ethernet кроется в наличии недорогих, надежных и совместимых сетевых решений от целого ряда поставщиков. Различные виды связи сливаются в одно целое, разрастаются огромные серверные фермы, растет использование IP-телефонии, IP-телевидения и приложений Web 2.0. Все это делает потребность в повышении скорости коммутаторов Ethernet еще более насущной.

Заключение

Ethernet является широко распространенной и доминирующей технологией для проводных локальных сетей. Преимущественно используется в корпоративных ЛВС, для обеспечения ШПД, в ЦОДах, а также для связи между сетями MAN и даже WAN. Кроме того, в настоящее время Ethernet является основным средством подсоединения таких беспроводных технологий как Wi-Fi и WiMAX к сетям Ethernet. Рынок решений на основе Ethernet достиг достаточных размеров для того, чтоб ускорить увеличение скоростей для конкретных видов использования. Например, речь идет о 25-гигибитном и 50-гигабитном Ethernet для ЦОДов и о 2,5-гигабитном и 5-гигабитном Ethernet для обеспечения работы беспроводных сетей. Доступность широкого спектра стандартизированных Ethernet решений позволяет операторам сетей предлагать индивидуальные решения, позволяющие оптимизировать деятельность, снизить расходы и потребление энергии.

Залог популярности технологии Ethernet кроется в наличии недорогих, надежных и совместимых сетевых решений от целого ряда поставщиков. Различные виды связи сливаются в одно целое, разрастаются огромные серверные фермы, растет использование IP-телефонии, IP-телевидения и приложений Web 2.0. Все это делает потребность в повышении скорости коммутаторов Ethernet еще более насущной.

Успешность гигабитного и 10-гигабитного Ethernet подтверждает важность выбора технологий, связанных с управлением сети. 40-гигабитный и 100-гигабитный Ethernet совместимы с существующими ЛВС, программным обеспечением по управлению сетью и приложениями. Именно совместимостью объясняется долголетие технологии, которая появилась 30 лет назад и остается востребованной в современном быстроменяющемся мире.

Источник: Gigabit Ethernet: From 1 to 100 Gbps and Beyond. William Stallings. The Internet Protocol Journal, Volume 18, Number 1

Открытые стандарты:

Открытый исходный код, Открытый контур

Дэвид Уорд (David Ward)

В Интернете по большей части доминирует программное обеспечение; и в последние несколько лет в рамках методологии гибкой разработки (agile development) резко возросли темпы инноваций – инноваций, которые требуют стандартизации. Код не является нормативом, хотя именно он является определяющим фактором в открытом программном обеспечении (ОПО). ОРС и согласованные стандарты необходимы. При этом ОРС должны учитывать, что цикл открытого ПО способен создать условия для достижения консенсуса между участниками рынка в отношении заполнения пробела в стандартах, и понимание этого может играть ключевую роль в нашем общем будущем.

Перед членами сообщества (сообщества IETF, прим. ред.) и сторонними наблюдателями стоит насущный вопрос: Нужны ли в мире растущего числа проектов в сфере открытого программного обеспечения (ОПО) организации по разработке стандартов (ОРС), такие как Инженерный совет Интернета (IETF).

Для тех, кто только что присоединился к этой дискуссии, поясним, что суть вопроса не в том, должны ли существовать ОРС. Они – реальность, связанная с торговой политикой и международными отношениями. Их основная задача состоит в том, чтобы не допустить появления коммуникационной «вавилонской башни» и установить контроль над использованием глобальной коммерческой и информационной инфраструктуры. Вопрос в том, играют ли эти организации роль в создании условий для инновации.

В Интернете по большей части доминирует программное обеспечение; и в последние несколько лет в рамках методологии гибкой разработки (agile development) резко возросли темпы инноваций – инноваций, которые требуют стандартизации.

Проблемы ОРС

Чтобы идти в ногу с технологическим прогрессом гарантировать, что собственные процессы разработки остаются актуальными, ОРС, такие как IETF, должны изменить свои процессы.

В Интернете по большей части доминирует программное обеспечение; и в последние несколько лет в рамках методологии гибкой разработки (agile development) резко возросли темпы инноваций – инноваций, которые требуют стандартизации. Код не является нормативом, хотя именно он является определяющим фактором в открытом программном обеспечении (ОПО).

ОРС и согласованные стандарты необходимы. При этом ОРС должны учитывать, что цикл открытого ПО способен создать условия для достижения консенсуса между участниками рынка в отношении заполнения пробела в стандартах, и понимание этого может играть ключевую роль в нашем общем будущем.

Для стороннего наблюдателя (и даже для некоторых инсайдеров), недавняя реорганизация рабочих групп (рабочих групп IETF, прим. ред.) напоминает простую перестановку стульев, то есть в принципе ничего не меняет.

Темпы реализации проектов ОРС и ОПО соотносятся как минимум 2:1 (два года на бумажный стандарт против одного года на продукт, который создает фактический стандарт).

Создается впечатление, что многие ОРС в разных странах мира не могут определить сферу своей деятельности и держаться в этих границах. Напротив, на их «территориях» бурно произрастают новые группы по изучению новых технологий. Каждая организация потенциально (и рискованно) считает себя вечной. Незначительное число ОРС имеют план собственного жизненного цикла, предусматривающий ограничение полномочий и сферы деятельности применительно к новым технологиям.

Реальной согласованности действий между ОРС практически не существует. Это ослабляет усилия и ресурсы участвующих компаний и физических лиц, создает путаницу для потребителей этих технологий.

Внутри IETF мы сталкиваемся с многочисленными проблемами, связанными с собственным жизненным циклом. Сколько времени тратится на дальнейшую стандартизацию уже зарекомендовавшей себя технологии за счет более актуальных рабочих групп? Как мы справляемся с проблемами, технологиями и новой архитектурой, которые проходят сквозь всю нашу существующую структуру (например, недавний бум модели YANG во многих рабочих группах)? В сравнении с популярными сетевыми проектами ОПО, в чем проигрывает IETF?

А главное, как мы можем убедить компании-стартапы, новых разработчиков, новых потребителей в том, что мы готовы прислушаться к их мнению? И при этом не демонстрировать превосходство, а проявлять демократизм, где ценятся реальные качества и заслуги?

Для стороннего наблюдателя (и даже для некоторых инсайдеров), недавняя реорганизация рабочих групп напоминает простую перестановку стульев, то есть в принципе ничего не меняет. Здесь действует Закон Конвея.

Закон Конвея: организации, разрабатывающие системы, создают модели, которые неизбежно копируют коммуникационную структуру этих организаций

Без фундаментальных структурных изменений ничего другого ожидать не следует. Мир не должен ждать два года, чтобы получить стандарт Цепи Функции Обслуживания (Service Function Chaining), и еще дольше, чтобы получить стандарт для Оверлеев Сетевой Виртуализации (Network Virtualization Overlay) (или виртуализации сетевых функций в целом, что больше является проблемой Европейского института телекоммуникационных стандартов).

Открытый код

Помимо проблем глобального сообщества ОРС и IETF, существует потенциальный риск того, что ОПО решит взять на себя функции по стандартизации.

Проще говоря, существует опасность кооптирования открытого кода в силу неэффективного управления. Судьба плохо руководимых проектов разработки ОПО может различаться, но всегда печальна.

Как и в случае неконтролируемого наложения стандартов от многочисленных ОРС, путаница может стать результатом осуществления проектов ОПО. Соперничество может быть как непреднамеренное (например, различия в технических подходах) и умышленное (например, бесплатное ПО, которое предлагается как открытое при отсутствии реального многообразия и альтернативы в плане поддержки, бесплатные продукты или добавочные блоки к другим проектам). В результате мы получаем множество маленьких сообществ, которым не хватает финансирования или сотрудников, и в этих монокультурах доминирует одна сторона.

- Эффективное и беспристрастное управление третьими лицами помогает избежать пересекающихся, однобоких и создающих путаницу проектов.

Осуществление проектов ОПО, не увязанных в более крупную архитектуру, может привести к фрагментации. Фрагментация происходит, когда каждый из множества проектов привносит часть общего решения, которые, тем не менее, не могут быть использованы в комплексе, отсюда – отсутствие прогресса и вмешательство в инновации более высокого уровня.

- Эффективное управление позволяет сформировать сообщество, которое учитывает связность проекта по восходящей и нисходящей.

Эффективное и беспристрастное управление третьими лицами помогает избежать пересекающихся, однобоких и создающих путаницу проектов.

Дефекты защиты возникают в результате недостаточного внимания проекта к вопросам безопасности, недостаточного количества рецензентов и специалистов по обслуживанию. Так случилось недавно с OpenSSL (HeartBleed), и сейчас эту проблему решает Инициатива Корневой Инфраструктуры (Core Infrastructure Initiative) консорциума Linux Foundation (для OpenSSL, OpenSSH и NTPd).

- Эффективное управление обеспечивает оптимальный процесс разработки не только для новых продуктов, но и для обслуживания существующих программ, их обновления и публикации.

Кроме того, надлежащее управление может обеспечить необходимые юридические, управленческие, стратегические и бизнес-процессы для адекватного осуществления прав собственности и лицензирования разработок, управления релизами, вовлечения открытого сообщества. Есть отличные примеры этому в консорциумах Linux Foundation, Apache Foundation и OpenStack Foundation.

Альтернативная модель ОРС

ОРС выдвинули несколько предложений включить в свою деятельность и стандартизировать сетевые архитектуры, которые были разработаны в открытом ПО путем определения программного интерфейса на уровне конечной точки, интерфейса или приложения (Application Program Interface, API). Консорциум Open Networking Foundation (ONF) – отличный пример ранних попыток создать другую гибридную модель: пытаясь связать оба мира, он использовал слово «стандарт», чтобы описать протокол обмена данными, и слово «открытый» для описания архитектуры.

Протокол разрабатывался на основе множества зачастую несовместимых с предыдущими версиями стандартов. Организация очень быстро перешла к активной поддержке и развитию рынка для протокола, архитектуры и контроллера OpenFlow (последний вид деятельности обычно не ассоциируется с традиционной ОРС).

Несмотря на доступность контроллеров и сетевых коммутаторов с открытым кодом, большинство разработок были осуществлены за пределами ONF отдельными заинтересованными группами. ONF не предоставил собственной эталонной реализации..

Наиболее важный урок, который ОРС и ОПО могут извлечь из опыта ONF, состоит в следующем: действительно успешные экосистемы и сообщества создаются на основе открытости решений и сотрудничества, а не через посредство осуществления права собственности, и только таким образом удастся избежать фрагментации и путаницы. В отличие от ОРС, в проектах ОПО есть место маркетингу, однако главное внимание должно уделяться формированию сообщества и привлечению к работе заинтересованных лиц.

Почему важны открытые API и концептуальные стандарты

Многие из новых проектов ОПО предлагают широкомасштабные и связанные между собой архитектуры решений. Важно рассмотреть роль таких ОРС, как IETF, в создании нормативной соединительной ткани этих новых архитектур, чтобы обеспечить в этой среде необходимую функциональную совместимость (См. https://tools.ietf.org/html/draft-opsawgoperators-ietf-00, опубликованную членами Internet Society).

Будущие стандарты в программно-конфигурируемых сетях будут появляться в форме API и рамочных концепций приложений и сервисов. Те же причины, по которым стандартизируются базовые Интернет-протоколы, применимы и к этим концепциям более высокого уровня: совместимость, выбор и дизайн системы.

Стандартизация необходима для развенчания мифа о том, что будущее, объединяющее огромное количество ОПО, это будущее, в котором все ПО и все решения являются бесплатными, и единственно возможная экономическая модель для производителя – исключительно поддерживать ОПО.

Напротив, правильно спроектированные, открытые и стандартизированные кнцепции, протоколы, конечные автоматы и иже с ними позволяют разработчикам предоставлять интеллектуальную собственность в виде модулей, которые, при необходимости, можно легко заменить. Безусловно в рамках разрабатываемых решений останется место компонентам ОПО, поддерживаемым сообществом, однако посредством стандартизации стимулы к инновациям у ведущих разработчиков и стартапов будут сохранены.

Стандартизация необходима для развенчания мифа о том, что будущее, объединяющее огромное количество ОПО, это будущее, в котором все ПО и все решения являются бесплатными, и единственно возможная экономическая модель для производителя – исключительно поддерживать ОПО.

Таким образом, поддержка производителем ОПО становится рациональной и понятной, как и ее использование в сообществе операторов.

Открытый контур

Несмотря на политические или экономические права на существование, право любой ОРС пользоваться авторитетом нужно заслужить. IETF является, пожалуй, наиболее подходящей ОРС для решения задачи по стандартизации программно-конфигурируемых сетей. Сфера деятельности IETF одновременно не слишком широкая (например, IETF не занимается вопросами здравоохранения и безопасности или защиты окружающей среды и изменения климата), но и не слишком узкая (например, не какая-то определенная услуга или сетевая область сервисный). Опыт IETF в определении архитектуры, разработке протокола, моделировании информации и данных (YANG) может быть полезен для реализации сетевых проектов ОПО.

Как добиться значимости IETF в данной среде

Чтобы утвердить IETF в качестве авторитета в области новых разработок, необходимых профессионалам и операторам в сфере IT, я предлагаю IETF сделать следующее:

- Подумать о реформировании и реструктурировании для поддержки более гибкого процесса. Отбросить всё мертвое и освободить место для новой работы. В частности, нужно быстро осознать неудачу, чтобы быстрее преуспеть с меньшим набором актуальных идей, но лучшего качества, чтобы двигаться со скоростью развития рынка. Больше встреч в формате BoF (Birds of Feather), больше успешных и нужных рабочих групп с более коротким сроком работы, меньше бумажной волокиты, больше ощутимых результатов. Позвольте новым рабочим группам выполнять техническую работу параллельно с разработкой концепции, архитектуры, требований и сценариев использования, в которых мы увязли. Сократите продолжительность цикла для всего (чтобы прийти к какому-то консенсусу, два года вполне достаточный срок).

Принудительная интеграция навыков и целей может изменить сообщество в худшую сторону. Сотрудничество, взаимодействие и обмен идеями подходят нам гораздо больше.

- Уделить больше внимания разработке ПО в структуре IETF. Необходимо поощрять эксплуатационную совместимости и демонстрацию функций на протяжении всего цикла разработки. Работающий код когда-то был одним из принципов IETF, но запоздалый работающий код ведет к потере гибкости. Подумайте о «хакатонах» применительно к процессу разработки стандартов. По моему опыту, наиболее удачные стандарты были созданы параллельно с написанием кода.

Закон открытого ПО: качество и успех проекта на 100% зависят от заинтересованности, энергии и способностей сообщества разработчиков. Закон открытых стандартов: важность, применимость и своевременность соответствующего стандарта на 100% зависит от заинтересованности, энергии и готовности идти на компромисс тех, кто имеет полномочия управлять, организовывать и обеспечивать завершение работы ОРС.

- Расширить проведение исследовательских работ (это уже хорошо получается), тем самым вовлекая больше участников.

- Исправить, изменить и перестроить процесс взаимодействия с другими организациями, потому что это крайне важно для сотрудничества с проектами ОПО. На самом деле, даже не используйте существующий процесс как модель.

- Принять во внимание проекты открытого ПО. Прежде всего, это потребует организации открытого взаимодействия между исполнительным комитетом IETF (Internet Engineering Steering Group, IESG) и авторитетными консорциумами ОПО в работе над совместными проектами. Хороший пример такого совместимого и надлежащим образом управляемого проекта – проект OpenDaylight (Linux Foundation), который продвигает использование моделей YANG в IETF, а также другие проекты открытого ПО.

Активное исследование и мониторинг проектов ОПО позволяет активно вкладывать наши ресурсы в новые технологии вместо того, чтобы ждать, когда они сами придут к нам.

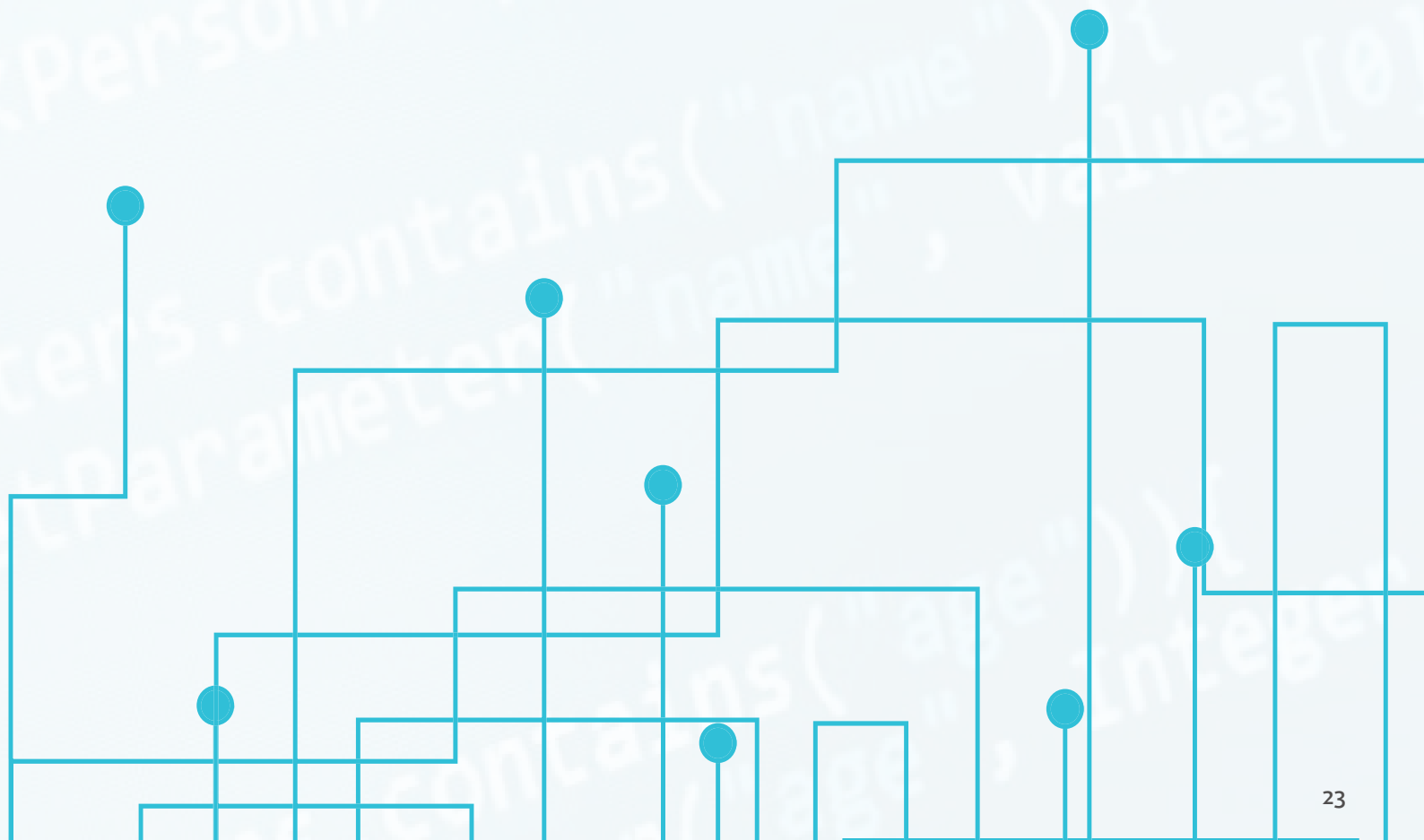
Обратная связь между сторонами поможет определить области новых и существующих проектов, которые необходимо стандартизировать, которые должны подчиняться существующим стандартам, либо не соответствуют стандартам. Исходя из опыта, написание кода до стандартизации обеспечивает наиболее полное и простое определение протоколов.

Часть этого процесса потребует, чтобы IETF постаралась не копировать всё в рабочие группы IETF. Специалисты ОРС и специалисты по ОПО – это не одно и то же. Парадоксально, но для наших целей, код не является нормативом. Однако также сложно определить и стандартизировать API, без написания кода. Принудительная интеграция навыков и целей может изменить сообщество в худшую сторону. Сотрудничество, взаимодействие и обмен идеями подходят нам гораздо больше. (Обратите внимание, что сотрудничество не удастся, если цикл ОРС будет замедлять работу партнера по ОПО. Справедливо и обратное: пассивное сообщество открытого ПО не сможет взаимодействовать ни с одной ОРС).

И наконец, мы должны (1) адаптировать и принять новые законы, и (2) постараться избежать Закона Конвея.

Если мы признаем существование этих законов, мы должны также понимать, что роли ОПО и ОРС должны измениться. Мы должны проложить новую траекторию, двигаться быстрее и сконцентрироваться на задаче создания более масштабного и более совершенного Интернета.

Источник: Open Standards, Open Source, Open Loop. David Ward. IETF Journal, Volume 10, Issue 3



Эволюция IANA: от записной книжки Джона Постела до ICANN

Андрей Робачевский

В начале 2000 года, между NTIA и ICANN был заключен договор на предоставление функций IANA, постфактум легитимирующим поглощение ICANN IANA, но также восстанавливающий контроль правительства США за этими ключевыми функциями. Этот договор перезаключался 4 раза и пережил значительное число различных поправок. Именно этот договор подразумевается в заявления NTIA, когда речь идет о роли правительства США в координации глобальной системы DNS. Прекращение действия этого договора и его замена моделью самоуправления является сутью процесса передачи.

Национальная администрация по телекоммуникациям и информации США - NTIA (National Telecommunications and Information Administration) 14 марта 2014 года опубликовала заявление о намерении передать ключевые функции глобальной системы имен DNS в руки мирового сообщества. Сам заголовок заявления обозначил главную проблему, которую NTIA предполагало решить – исключение явного ассиметричного присутствия правительства США в процессе принятия решений в отношении корневой зоны глобальной DNS. Однако проблема оказалась больше, поскольку по исторической случайности правительство США помимо уникальных имен корневой зоны DNS оказалось формально вовлечено в администрирование других уникальных параметров Интернета: протоколов и адресов.

Причина – администрацией всех трех классов уникальных параметров занимается организация под именем IANA (Internet Assigned Numbers Authority, в дословном переводе - Администрация присвоенных идентификаторов Интернета), а ее функции в настоящее время выполняет ICANN в рамках контракта с NTIA. Действие этого контракта истекает 30 сентября этого года.

Это заявление дало начало созданию различных групп и дискуссионных форумов сообщества для разработки возможных моделей IANA без правительства США. Но для того, чтобы лучше понять, что же такое IANA и значимость грядущих перемен, нужно обратиться к истории создания и эволюции этой необычной структуры.

Этой статьей мы начинаем серию публикаций, посвященных эволюции IANA. Первая из них – взгляд в прошлое.

Ранние годы

Как набор функций IANA существовала с начала 70-х прошлого столетия в рамках проекта ARPANET, который являлся предтечей Интернета. Этот проект *«дал начало процессу формирования сетей, впоследствии соединенных друг с другом, чтобы превратиться в Интернет. Кто-то должен был следить за всеми протоколами, идентификаторами, сетями и адресами и, в конечном счете, за именами всех вещей в сетевой вселенной»* - писал в некрологе на смерть научного сотрудника Института Информатики (ISI) Университета Южной Калифорнии (USC) и одной из выдающихся фигур сетевого сообщества Джона Постела (Jon Postel) другой корифей Интернета Винт Серф («I REMEMBER IANA»).

IANA не являлась организацией – она была не более чем каталогом уникальных идентификаторов протоколов и блоков адресов. Фактически, этот акроним был тождественен Джону Постелу – он придумал имя и выполнял ее функции.

Первые записи этих идентификаторов Постел вел в легендарной записной книжке. Эту работу Постел выполнял в ISI в рамках грантов агентства по перспективным оборонным научно-исследовательским разработкам США DARPA. Назначение грантов было достаточно общим, объединяя в своем финансировании помимо функций IANA, работу редактора серий RFC и другие проекты. Сам термин IANA до 1993 года вообще не фигурировал в описании работ, да и потом он появился в глубинах договора на исполнение проекта высокопроизводительных вычислений Teranode.

В ноябре 1983 году научный сотрудник ISI Пол Мокапетрис (Paul Mockapetris) завершил работу над спецификацией и испытаниями нового протокола и системы, призванной прийти на смену файлу hosts.txt, который использовался для именования хостов сети ARPANET. Система являлась распределенной и называлась системой доменных имен или DNS (Domain Name System). Она выполняла те же функции, что и hosts.txt – позволяла транслировать более легкие для использования имена в адреса компьютеров. В том же ноябре Постел опубликовал план перехода к новой системе.

Особенностью системы являлось то, что она была иерархической, беря свое начало с так называемой корневой зоны, содержащей список доменов верхнего уровня. Осенью 1984 года Постел предложил 5 доменов верхнего уровня .gov, .mil, .edu, .com, и .org. Не желая вдаваться в дискуссию о семантике этих имен, которая уже началась, он опубликовал это предложение как «Официальную политику, утвержденную IAB и DARPA». В этом же документе была определена политика относительно национальных доменов – их регистрация проводилась в соответ-

ствии с двухбуквенным кодом (т.н. alpha-2) таблицы ISO 3166-1. В результате, начиная с 1985 года ответственность за администрирования корневой зоны также легла на Джона Постела. Услуги регистрации и сопровождения стал выполнять информационный центр DDN-NIC исследовательским институтом SRI International.

Процесс регистрации и сопровождения таких критических ресурсов как адресное пространство и других идентификаторов тоже требовал больших ресурсов, чем записная книжка. В 1987 году функция регистрации и сопровождения базы данных распределения адресных блоков также перешла к информационному центру SRI. Таким образом к конце 1980-х DDN-NIC стал де-факто IANA. Руководил этой деятельностью по-прежнему Джон Постел.

Поскольку SRI в целом финансировалась министерством обороны США постоянно поднимался вопрос субсидирования «гражданской» части регистратуры. Решением стал грант NSF, который стал финансировать “гражданскую” часть. В то же время стремительными темпами развивался Интернет в Западной Европе и делегирование адресных блоков уже происходило не только «гражданским» сетям, но и сетям в других государствах. Началась делегация национальных доменов. Структура информационного центра DDN-NIC все меньше подходила для этой роли.

Таким образом к началу 1990-х встал вопрос о физическом разделении информационного центра.

Гражданский Интернет

На выполнение функций IANA для «гражданского» Интернета был объявлен тендер, который был выигран в то время неизвестной небольшой компанией NSI (Network Solutions, Inc.). Это стало неожиданностью. Передача функций обслуживания корневой зоны DNS и регистратуры адресных блоков от «ветерана» Интернета SRI International к незнакомому игроку явилась значительным событием.

Собственно процесс передачи оказался болезненным, с ошибками и сюрпризами, вызвавшими недовольство технического сообщества IETF. К концу 1991 года этот процесс был завершен и IANA обосновалась в Вирджинии. В 1992 году в ходе нового проекта NSF родилась концепция инфоцентра InterNIC, полностью ориентированного на «гражданский» Интернет. В 1993 году NSF объявила тендер на осуществление регистрационных услуг InterNIC, победителем которого стала все та же компания NSI. Кооперативное соглашение – форма контрактов NSF - предоставил NSI монопольные права на регистрацию доменов второго уровня в .com, .org и .net в порядке очередности получения заявок. Хотя контракт был между NSF и NSI, регистрационные услуги однозначно подразумевали IANA.

Изначально регистрация производилась бесплатно, за счет финансирования NSF. Однако по мере роста числа регистраций и, соответственно расходов на их сопровождение, вопросы финансирования встали на повестку дня. На повестку для встал вопрос возможности платной регистрации.

В марте 1995 год компания NSI была куплена контрактором минобороны компанией SAIC в совет директоров которой входили бывшие сотрудники силовых министерств и ведомств США. Через несколько месяцев после этого в мире доменных имен произошли существенные изменения, напрямую связанные со стратегией приватизации Интернета, проводимой NSF.

Приватизация

В сентябре того же 1995 года к Кооперативному Соглашениию между NSF и NSI была принята поправка №4, позволившая последней взимать взносы за регистрацию имен в доменах верхнего уровня .org, .net и .com. Это решение не только избавило NSF от всё растущих субсидий на поддержку регистраций, поправило плачевное состояние бюджета NSI, но и предоставило NSI доступ к поистине золотой жиле.

Хотя за Постелом оставалось последнее слово в вопросах изменения корневой зоны, коммерциализация доменов верхнего уровня и в особенности .com дала начало дискуссиям о вопросах администрирования и управления Интернетом, которые не прекращаются и сегодня.

Вопросы администрирования корневой зоны затрагивали интересы растущего числа разнообразных групп – начиная от новообразованных компаний, которым нужно было значащее имя в Интернете, до правообладателей торговых марок, видевших в DNS как возможности, так и опасности, до правительств государств, постепенно понимающих, что эти вопросы граничат с их суверенными интересами.

Формально NSI не имела права вносить изменений в корневую зону, но компания по-существу монопольно контролировала корневой уровень и чрезвычайно прибыльный бизнес доменов второго уровня. Это положение вещей вносило серьезный дискомфорт. Одним из путей изменения монополистической позиции в корне являлось возможность создания дополнительных доменов верхнего уровня. Но политика создания новый доменов отсутствовала и было непонятно, кто же de jure контролирует корень DNS.

Ситуация осложнялась фактом, что пятилетний договор между NSI и NSF истекал в 1998 году. В отсутствие NSF будущее управление корневой зоной было по меньшей мере непонятным.

При участии Джона Постела несколько инициативных групп начали активное обсуждение возможных моделей управления корневой зоной DNS. Одна из таких моделей была разработана группой под названием International Ad Hoc Committee (IAHC), специально для этого созданной под эгидой ISOC, IAB, IANA, МСЭ (Международного союза электросвязи), INTA (Международной ассоциации торговых марок) и WIPO (Всемирной организаций интеллектуальной собственности, ВОИС).

Структура управления корневым уровнем DNS в предложении IAHC и связанным с ним Протоколом о взаимопонимании gTLD-MOU выглядела следующим образом. Вместо создания множества новых доменов верхнего уровня и связанных с ними регистратур-регистраторов, работающих по модели NSI, но конкурирующим между собой, как это было предложено Постелом в его Проекте, комитет IAHC предлагал разделить функции регистратуры и регистратора, и стимулировать конкуренцию на уровне последних.

В рамках предложения предполагалось создание всего нескольких дополнительных доменов верхнего уровня, свободных от монополии NSI. Как было сказано в предложении «пространство имен верхнего уровня обеспечивает перераспределение избытка имен через структуру национальных доменов» и что создание новых до-

менов верхнего уровня «неизбежно приведет к дублированию регистрации, делая существующие проблемы, связанные с полезностью и жизнеспособностью структуры DNS Интернета только более сложными». В отношении национальных доменов предложение признавало суверенитет государств в определении политики.

Регистраторы получали равноправный доступ ко все доменам верхнего уровня. Они могли устанавливать собственные расценки за свои услуги, конкурируя между собой. Все Регистраторы являлись членами ассоциации регистраторов CORE (Council of Registrars, Совет Регистраторов), отвечающей за разработку правил, обеспечение необходимой координации, а также организационной и юридической поддержки. По замыслу IAHC, CORE должна была быть зарегистрирована как швейцарская некоммерческая организация в Женеве.

Вопросы разногласий в отношении доменных имен были решены путем установления 60-дневного периода ожидания во время которого возможные споры должны были быть урегулированы специальными комитетами Всемирной Организации по Интеллектуальной Собственности (ВОИС, WIPO), т.н. Administrative Challenge Panels.

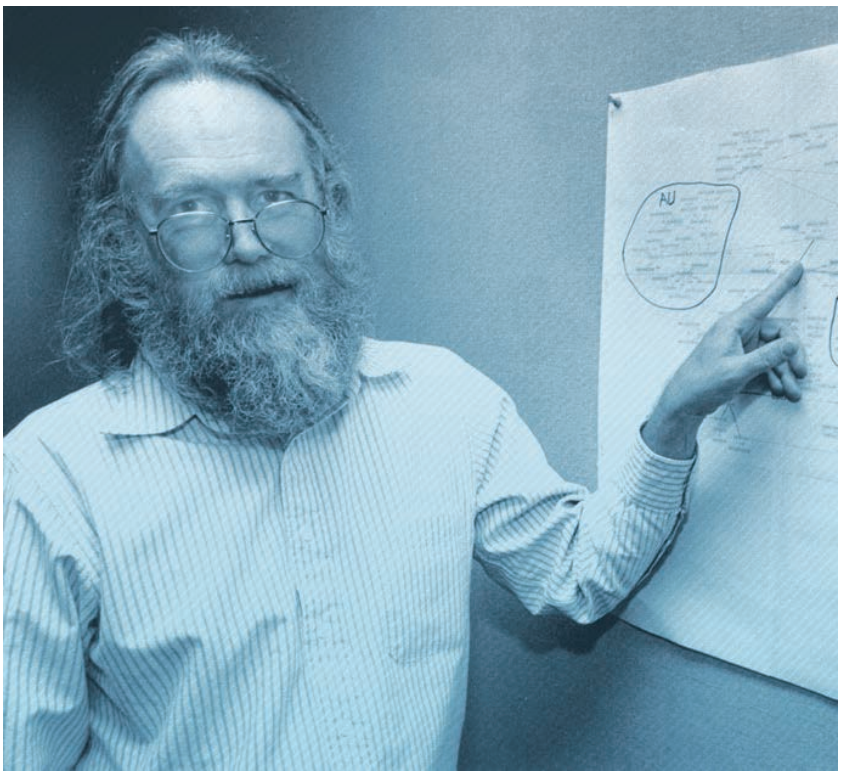
Официальная церемония подписания Протокола gTLD-MOU состоялась в мае 1997 года в Женеве. Более 200 организации подписали протокол, включая Международный Союз Электросвязи (МСЭ), уже упомянутый мной ВОИС и Всемирный Почтовый Союз (ВПС).

Тем не менее, протокол вызвал критику ряда организаций, которые видели в нем угрозу своим интересам. В первую очередь это была NSI, которая после окончания договора с NSF могла быть сведена до уровня регистратора с полной потерей своей монопольной позиции.

Протокол вызвал и серьезную озабоченность правительства США, которое видело в нем возможность передачи контроля над глобальной DNS межгосударственным организациям, например к МСЭ. Советник президента Клинтона Ира Магазинер (Ira Magaziner) вынужден был вмешаться. В июле 1997 года телекоммуникационное агентство NTIA министерства торговли США опубликовало проект приватизации DNS для публичного обсуждения. Этот проект призван был напомнить о de jure контроле правительства США за корневым уровнем и IANA, а также взять инициативу создания новой модели управления Интернетом в свои руки.

Проект во многом основывался на модели IAHC и содержал эскиз будущей некоммерческой организации, которой правительство США предполагало передать функции IANA, и которая была призвана обеспечивать координацию распределение имен, номеров и адресов. Также был предложен план демонополизации NSI, начиная с предоставления доступа к доменам .com, .org, .net другим регистраторам на равной основе и заканчивая передачу контроля за корневой зоной и ее мастер-сервером a.root-servers.net (Сегодня a.root-servers.net всего лишь один из 13 вторичных авторитетных серверов, обслуживающих корневую зону. Содержимое этой зоны все серверы получают от так называемого «спрятанного» мастер-сервера, обслуживаемого Verisign, после приобретения NSI в 2000 г.)

Значение этого проекта, как и последующего «Зеленого документа» (Green Paper - временный консультационный отчет для последующего (публичного) обсуждения, но без каких-либо обязательств к последующим действиям. Это, как правило, первый шаг на пути изменения законодательства или государственной политики. За «Зеленой Книгой» может последовать так называемая «Белая Книга» (White Paper) - официальный документ, разъясняющий цели и суть предполагаемого изменения или новой политики и предусматривающий в то же время опрос общественного мнения.) не всеми было понято однозначно. Комитет IAHC продолжал действовать согласно изначальному плану и в октябре 1997 года была создана ассоциация CORE.



Джон Постел создал и сопровождал IANA вплоть до своей смерти в 1998 году. Он, собственно, и являлся IANA. (Фотография Irene Fertik, USC News Service. Copyright 1994, USC.)

За несколько месяцев до окончания договора между NSF и NSI, Джон Постел решил сделать «небольшой шаг в направлении» новой управляющей модели Интернета, когда «редакция и публикация корневой зоны будет осуществляться непосредственно IANA (см. письмо Постела операторам корневых серверов). Этот «тест» не вызвал энтузиазма в правительстве США и Магазинер убедительно попросил Постела прекратить его.

После этого события развивались также стремительно, но уже под контролем правительства США. За «Зеленой книгой» последовала «Белая книга», организация различных комитетов и форумов по разработке новой модели управления. Наиболее выдающимися из которых были IANA Transition Advisors Group ITAG (Группа советников по трансформации IANA) под предводительством Постела и анти-IAHC группа, под координацией которой прошла серия так называемых International Forum on the White Paper, IFWP (Международный Форум по Белой Книге). Но в то время как Форум организовывал встречи в различных точках земного шара и стимулировал обсуждение вопросов новой модели управления между членами

Интернет-сообщества, ключевыми в процессе становления новой компании, которая получила название ICANN (Internet Corporation for Assigned Names and Numbers - Корпорация Интернета по распределению адресов и номеров), были коалиция IAHC во главе с Джоном Постелом и NTIA.

В сентябре 1998 года ICANN была зарегистрирована как некоммерческая корпорация в штате Калифорния, США. Функции IANA естественным образом перешли в ICANN.

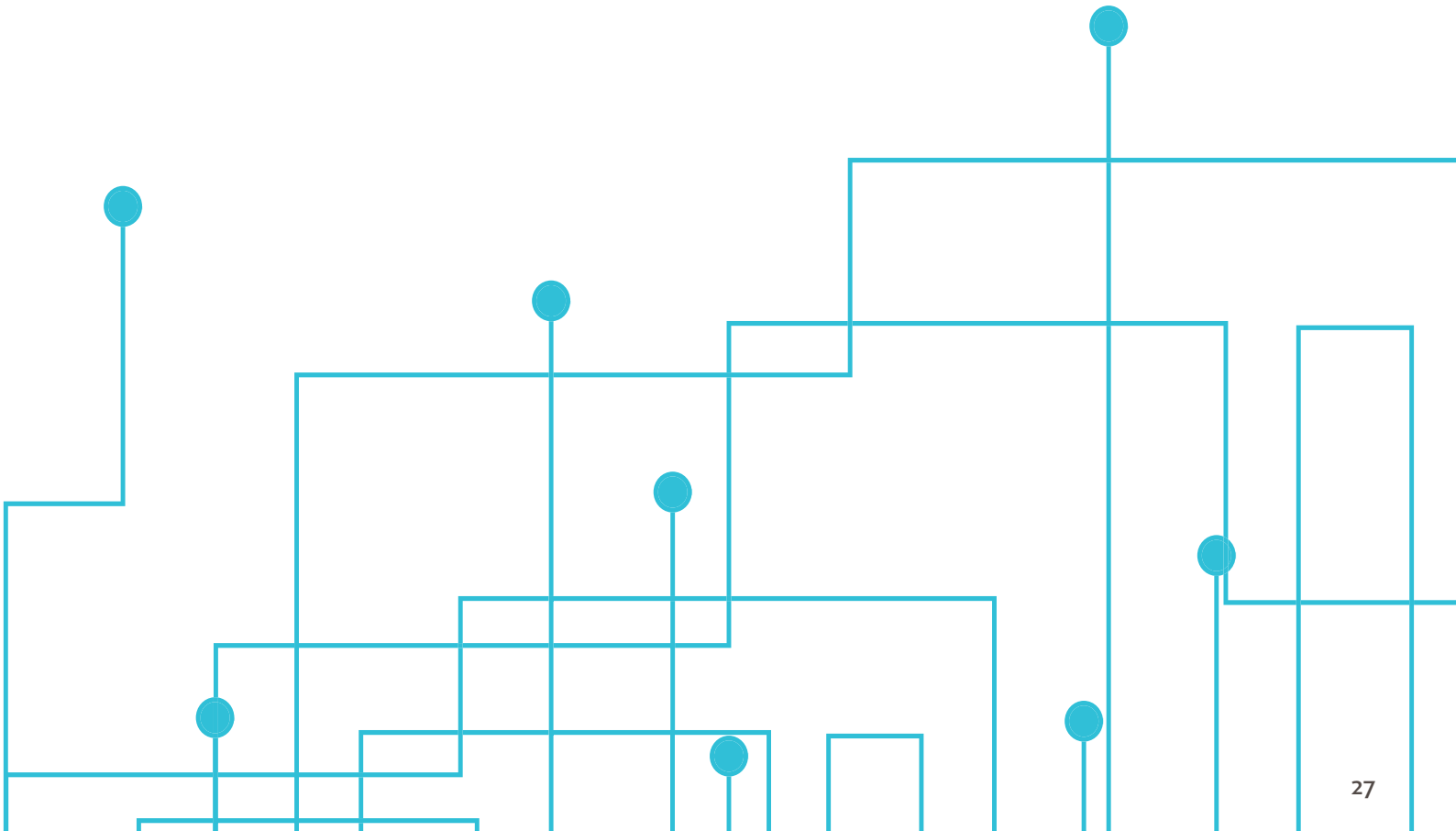
IANA сегодня

За время своего существования IANA превратилась в центральную регистратуру различных параметров Интернета в трех областях:

- Протоколы Интернета, где IANA отвечает за присвоение различных параметров (операционных кодов, номеров портов и протоколов, идентификаторов объектов), которые используются разнообразными протоколами Интернета, в подавляющем большинстве разработанными IETF.
- Система доменных имен DNS, где IANA отвечает за содержимое корневой зоны и обслуживание запросов на ее изменение.
- Адресное пространство IP, где IANA обслуживает глобальный пул, часть которого распределяется между Региональными Интернет-Регистратурами (РИР), часть предназначается для системы мультикаст, а часть зарезервирована IETF для будущего использования.

То есть в независимой децентрализованной культуре Интернета IANA отвечает за три централизованные, иерархические и чрезвычайно важные базы данных и связанные с ними услуги.

В начале 2000 года, между NTIA и ICANN был заключен договор на предоставление функций IANA, постфактум легитимирующим поглощение ICANN IANA, но также восстанавливающий контроль правительства США за этими ключевыми функциями. Этот договор перезаключался 4 раза и пережил значительное число различных поправок. Именно этот договор подразумевается в заявления NTIA, когда речь идет о роли правительства США в координации глобальной системы DNS. Прекращение действия этого договора и его замена моделью самоуправления является сутью процесса передачи. Но о нем мы поговорим в следующей статье.



Цена DNSSEC

Джефф Хьюстон

Преимущества использования расширений безопасности DNS - DNSSEC очевидны. Но какова стоимость внедрения этого протокола? Исследования Джеффа Хьюстона показывают, что если принять в расчет кэширование, то увеличение затрат на стороне клиента-резолвера практически незаметно. Для администраторов авторитетных серверов ситуация несколько иная. Сегодня подписание доменного имени по DNSSEC увеличит общую нагрузку по количеству запросов на авторитетные серверы имен примерно в 1,5 раза, а исходящий трафик — приблизительно в 8 раз. Ошибки DNSSEC — просроченные ключи, неправильные подписи, разорванная цепь доверия между родительской и дочерней зонами — приводят как минимум к удвоению числа запросов по сравнению с правильно подписанным именем и аналогичному удвоению объема трафика.

Если вы занимаетесь DNS, самое время озаботиться повышением ее безопасности DNS, активировав DNSSEC, если вы еще этого не сделали. Множество атак начинается с фальсификации данных DNS, а заканчивается тем, что заводит ничего не подозревающего пользователя в ловушку. DNSSEC надежно защищает DNS-клиента от такого обмана. Но, как известно, бесплатный сыр бывает только в мышеловке, а потому активация DNSSEC имеет свою цену в плане трафика и производительности. В этой статье я опишу наши наблюдения, полученные в ходе эксперимента по количественной оценке развертывания DNSSEC в крупной сети, и постараюсь с их помощью ответить на вопрос: какова дополнительная цена включения DNSSEC?

Разумеется, при обсуждении DNS есть две перспективы, клиента (или резолвера) и авторитетного сервера имен. Мы рассмотрим обе по очереди.

DNSSEC на стороне клиента

Начнем с DNS-клиента. Какова цена включения проверки DNSSEC для ответов DNS?

Интуитивно можно предположить, что для имен из зон, подписанных DNSEC, клиент будет тратить чуть больше времени на трансляцию имен, а также генерировать дополнительные запросы для обеспечения валидации. Поступающие к клиенту ответы тоже, по идее, должны увеличиться в объеме, поскольку будут содержать данные подписи DNSSEC.

Можем ли мы оценить эту разницу количественно?

Рассмотрим поведение клиента и сравним ситуации с DNSSEC и без.

Для начала рассмотрим процесс трансляции DNS при разборе 5-доменного имени (z.00001.z.dashnxdomain.net.) в случае, если у клиента нет кэшированного состояния и проверка DNSSEC клиентом не выполняется. В нашем эксперименте весь процесс трансляции имени потребовал 4 запросов DNS и занял 0,535 секунды. В терминах трафика DNS в ходе обработки запроса было создано 292 байта трафика исходящих запросов и в общей сложности 1622 байта полученных ответов DNS. Однако запросы к корневому серверу имен и серверу имен .net в какой-то степени работали на заполнение локального кэша DNS. Если мы попробуем отправить с того же самого клиента второй запрос через несколько секунд после первого, изменив только самый младший поддомен, то процесс трансляции имен DNS пойдет гораздо быстрее и эффективнее, потребовав всего одного запроса и одного ответа: общее время будет составлять 191 мс, объем запросов - 83 байта, ответов - 134 байта.

Теперь для сравнения посмотрим, как будет выглядеть DNS-трансляция похожего имени, если локальный клиент настроен на выполнение проверки DNSSEC, а запрашиваемое имя подписано по DNSSEC. С учетом запросов для заполнения корневого ключа, если кэш имен клиента был первоначально совершенно пуст, то процесс потребовал 20 запросов DNS и занял 2,102 секунды. При этом было отправлено всего 1446 байт, получено в виде ответов 13 026 байт. Это вчетверо больше по времени и в 8 раз больше по трафику, чем без DNSSEC. Разумеется, при заполненном кэше нагрузка DNSSEC гораздо меньше, и для трансляции имени, которое отличается лишь младшим поддоменом, потребовался всего один запрос. Даже в этом случае объем ответов DNS примерно в 8 раз больше при наличии подписи. Кэширование на клиентской стороне - очень мощный инструмент в DNS, заметно повышающий быстродействие DNS. При использовании DNSSEC его эффект становится даже более выражен. Сравнительные данные по описанным сценариям сведены в таблицу 1.

Последовательный и параллельный подходы в запросах на проверку

Показатели работы резолвера Bind 9.9, который мы использовали для проведения экспериментов, можно значительно улучшить, сменив последовательный метод проверки подписей DNSSEC на параллельную процедуру клиентом DNS. В этом случае для проверки подписи DNSSEC потребуется 14

Таблица 1. Трансляция имени DNS из 5 частей с проверкой DNSSEC и без

	Запросы	Время	Отправлено (байт)	Получено (байт)
Без подписи	4	0,535	292	1 622
Без подписи, с кэшированием	1	0,191	83	134
С подписью	20	2,102	1 446	13 026
С подписью, с кэшированием	1	0,191	82	1 123

последовательных запросов, которые займут 12 различных интервалов запрос-ответ. Все вопросы, за исключением двух, выстраиваются в последовательную очередь, где каждый из них ожидает завершения предыдущего запроса и лишь затем передается в сеть.

Однако, как показали отдельные эксперименты с различными перестановками намеренно искаженных конфигураций проверки подписей, используемый клиентом процесс проверки путем сопоставления ключа не будет начат до тех пор, пока не завершится весь процесс опроса DNS для DNSKEY и ресурсных записей DS. Быстрее было бы запустить значительную часть этих запросов на параллельное выполнение. Если бы Bind смог распараллелить этот процесс и обрабатывать, скажем, по 20 запросов в любой момент времени, то задача заполнения кэша для резолвера с проверкой сократилась бы с 2,102 с до 0,725 с, что всего на один интервал «вопрос-ответ» (190 мс) больше, чем для случая без подписи и без проверки.

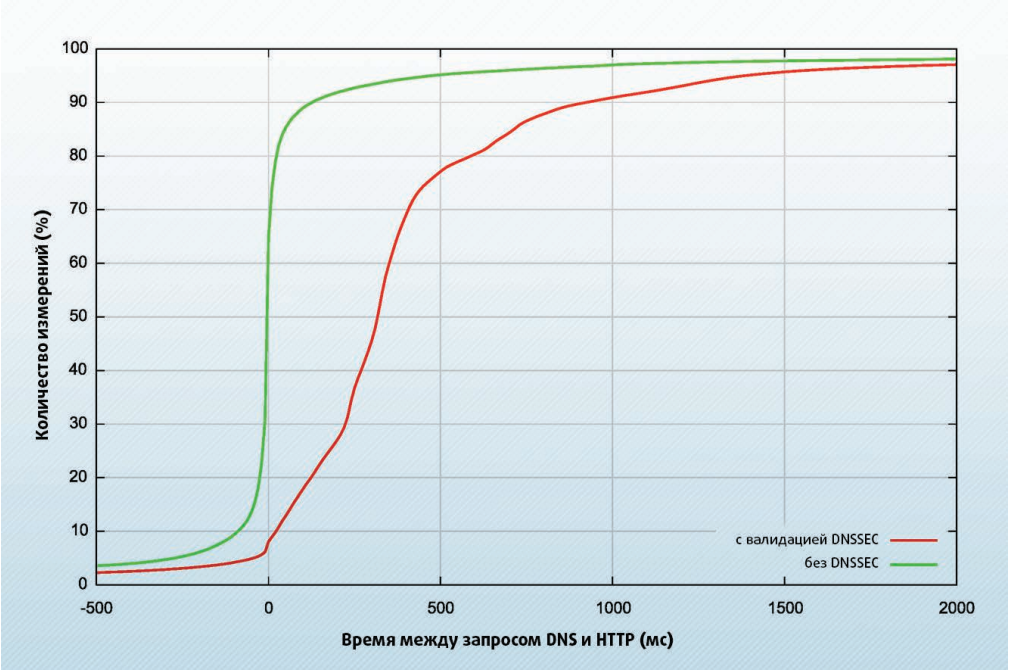
Также неясно, почему клиент Bind 9.9 направляет запросы о записи DS зоны родителю родителя до того, как повторно опросить родительскую зону. Такие запросы к «дедовской» зоне заканчиваются провалом, так как в нашем случае эта зона является авторитетной службой, не имеющей никакой информации о записях DS зоны-«внучки». Если это попытка оптимизировать запросы DNS, то мы не в состоянии понять, что такое поведение вообще может оптимизировать.

Можно ли сравнить эти тесты с наблюдаемой работой? В рамках программы измерения показателей развертывания DNSSEC в Интернете мы просили конечных пользователей выбрать два уникальных (не кэшированных) URL. Одно из них должно было быть именем с подписью DNSSEC, второе - не подписанным DNSSEC.

Насколько дольше для клиента окажется трансляция некэшированного DNSSEC-имени по DNSSEC по сравнению с трансляцией неподписанного имени резолвером без DNSSEC?

Мы используем измерения на серверной стороне, измеряя время, прошедшее с получения первого запроса DNS для конкретного имени до поступления команды HTTP GET. Когда мы измеряем данные клиентов, использующих резолверы без поддержки DNSSEC, и сравниваем относительное время выборки для трансляции неподписанного и некэшированного имени DNS с подписанным некэшированным именем DNS, мы видим кумулятивное распределение, изображенное на рис. 1 линией «No DNSSEC». Примерно для 20% конечных пользователей имя с подписью DNSSEC транслируется быстрее неподписанного. Это, похоже, часть экспериментальной вариации, обнаруженной в системе скриптов

Рис.2. Сравнительное время трансляции имен DNS

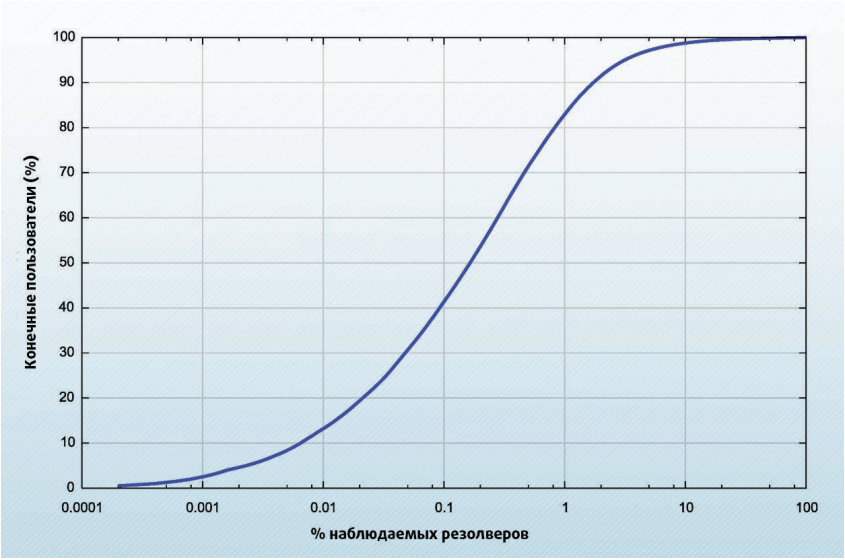


Концентрация резолверов DNS в Интернете

Кэширование DNS в Интернете исключительно эффективно, и можно утверждать, что DNS отличается особой эффективностью кэширования по сравнению с любыми другими интернет-приложениями или службами. Частично это обусловлено концентрацией: небольшой набор резолверов DNS используется огромным количеством конечных клиентов.

За прошедшие полгода в ходе нашего эксперимента мы выполнили около 40 млн. индивидуальных измерений DNS и обнаружили, что 20% этих конечных пользователей используют всего 100 резолверов, а 82% конечных пользователей используют лишь 1% из 500 000 видимых резолверов. Отсюда следует, что как только один из таких популярных резолверов кэширует ответ, значительная часть конечных клиентских устройств получает облегченный доступ к попавшей в кэш информации.

Распределение резолверов DNS по клиентам

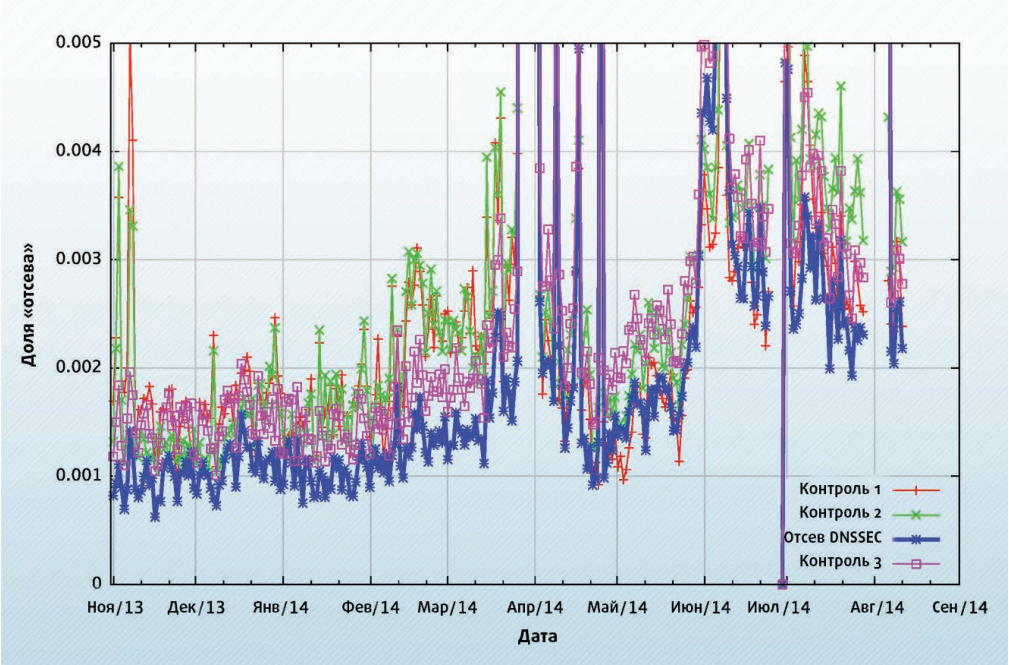


Flash, которая использовалась в процессе эксперимента: для нее процесс трансляции DNS не обнаруживает тесной связи с подсистемой получения URL. Аналогично еще примерно для 20% пользователей обработка подписанного DNSSEC доменного имени оказывается дольше альтернативы, несмотря на то, что используемые резолверы не выполняют никаких запросов RR, связанных с DNSSEC. Таким образом, серия данных «No DNSSEC» в эксперименте является «контрольным» профилем. Серия данных «DNSSEC-Validating» отражает то же самое измерение, но для пользователей, использующих резолверы DNS для проверки DNSSEC. В этом случае медиана распределения для второй серии данных отражает дополнительный 300-миллисекундный компонент для трансляции имени с подписью DNSSEC. Это согласуется с наблюдением, что в данном случае выполняются следующие дополнительные запросы DNS: запрос DNSKEY RR для конечной зоны и запрос DS RR для ключей KSK и ZSK, отрабатываемый родительской зоной. Похоже, что большинство клиентов выполняют эти дополнительные запросы последовательно. Хотя для проверки необходимо собрать всю цепочку данных ключа DNSSEC вплоть до корневого ключа, большая часть этих данных кэшируется резолверами, так как уровень запросов на ключи для обычных родительских зон гораздо ниже, чем уровень запросов для уникальных конечных зон.

Похоже, что главным «затратным» компонентом DNSSEC для клиента является дополнительное время на получение данных DNSSEC и что эти затраты еще более увеличиваются за счет последовательной обработки запросов, которую применяет большинство резолверов. Однако эти затраты практически нивелируются кэшированием, и дополнительные затраты на трансляцию популярных имен DNS для подавляющего большинства конечных пользователей минимальны благодаря сочетанию двух факторов: концентрации рекурсивных резолверов и кэширования. Если конечный клиент полагается на локальный резолвер для проверок DNSSEC, то кэширование полностью уничтожает описанные дополнительные затраты для клиента. Если клиент сам выполняет проверку ответов DNS, то проверочный компонент добавляет дополнительный цикл запросов к локальному резолверу - чтобы получить данные подписи DNSSEC, если их еще нет в локальном кэше резолвера.

По нашим наблюдениям, если клиент может транслировать неподписанное имя DNS за один запрос (это примерно 80-90% всех клиентов), то дополнительное время на проверку DNSSEC не превосходит 500 мс для некэшированного имени DNS. Подчеркну, что приведенные выше данные относятся именно к некэшированным именам DNS.

Рис.3. Доля «отсева» для имен DNS с подписями DNSSEC



Кэширование DNS практически устраняет дополнительную задержку, так что результирующие данные не хуже указанных, а в большинстве случаев и лучше.

Есть еще один потенциальный аспект для клиента, который необходимо учесть. При использовании подписей DNSSEC запросы DNS сильно разбухают в объеме. В то же время существует подозрение, что некоторая часть Интернета все еще находится за отставшим от жизни промежуточным ПО, которое считает, что протокол UDP, используемый DNS, ограничивает размеры и запроса, и ответа 512 байтами. Если это так, то должно существовать заметное подмножество конечных пользователей, которые не смогут транслировать имя с подписью DNSSEC. Проявляется ли это в данных эксперимента?

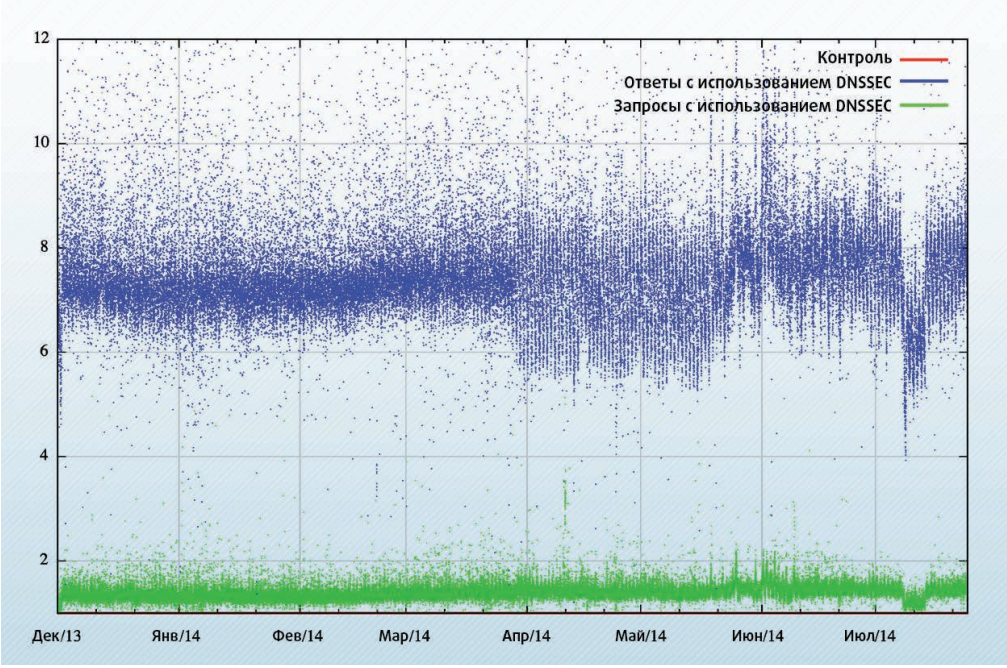
Чтобы выявить такие аномалии, можно попытаться разобрать на части эксперимент DNSSEC и попробовать найти данные, коррелирующие с неспособностью клиента транслировать имя с подписью DNSSEC. В этом эксперименте мы используем три URL. Один не подписан, второй подписан действительной подписью DNSSEC, третий тоже подписан - но для него цепочка проверки подписи намеренно разорвана. Если конечный пользователь не может транслировать DNSSEC-имена вообще, то в результатах эксперимента мы увидим попытки трансляции DNS для всех трех уникальных URL, но получение адреса будет присутствовать только для URL с неподписанным именем DNS. Если эти конечные пользователи не могут транслировать имя с подписью DNSSEC, то следует также ожидать, что все запросы DNS касательно подписанного имени будут содержать расширение EDNS0 с набором флагов DNSSEC_OK. Иными словами, все запросы о подписанных именах должны вызывать длинный подписанный ответ.

В контексте данного конкретного эксперимента, который мы использовали для сбора данных DNS, возникает следующая проблема: нельзя быть уверенными, что все пользователи завершат все три запроса URL. Эксперимент завершится преждевременно, если пользователь уйдет с веб-страницы, на которой эксперимент проводился, а управляющий скрипт эксперимента, Adobe Flash, судя по всему, выполняет три запроса в относительно случайном порядке. Поэтому можно ожидать небольшого «отсева» для каждого из трех URL. Если есть признаки неспособности транслировать имена с подписями DNSSEC, то следовало бы ожидать, что уровень отсева для описанных выше условий будет больше, чем для других комбинаций. Нам требуется пара контрольных экспериментов, чтобы описать «случайный» фоновый отсев. Первый контрольный показатель - это количество пользователей, которые получают имена, подписанные DNSSEC, но не получают неподписанные. Второй контрольный показатель - количество пользователей, которые получают неподписанный URL и плохо подписанный URL, но не правильно подписанный URL. Третий контрольный показатель - количество пользователей, которые получают неподписанный URL, но не подписанный DNSSEC URL, а при этом не обязательно все содержат установленный бит DNSSEC-OK в своих запросах. На рис. 2 показаны результаты этого измерения на 56 млн. образцов в течение 9 месяцев. Три контрольных показателя отсева более-менее коррелируют друг с другом, составляя примерно от 0,1% до 0,3% пользователей, при этом показатель отсева для трансляции DNSSEC на 0,02% ниже всех трех контрольных показателей и никогда не превосходит их. На основе этих данных можно сделать наблюдение, что на таком уровне детализации нет заметных сигналов, которые бы указывали на существование популяции пользователей, неспособных транслировать имя DNS с подписью DNSSEC. Эти данные не обнаруживают сколько-нибудь значительного отсева по DNSSEC в современном Интернете.

Следует сделать оговорку относительно ограничений данного конкретного эксперимента. Ни один из подписанных DNSSEC ответов на запросы не превосходил 1280 октетов, не говоря уже об 1500 октетах. Это означает, что мы не вызываем фрагментации пакетов UDP ни в IPv4, ни в IPv6. Поэтому конкретной точкой отказа для этого эксперимента являются резолверы клиентов, накладывающие ограничение в 512 байт на максимальный размер ответа DNS, но при условии, что резолвер разрешил использование EDNS0 в своих запросах. Имело бы смысл повторить эксперимент, используя размер ответа DNSSEC более 1500 октетов, чтобы проверить, вызывает ли фрагментация UDP в IPv4 или IPv6 повышение отсева из-за невозможности выполнить трансляцию DNS для таких длинных ответов. Возможно, мы обнаружим это, повторив эксперимент в дальнейшем.

Каковы затраты для клиентов резолвера, когда последний включает проверку DNSSEC? Если принять в расчет кэширование, то увеличение затрат практически незаметно. Обновление кэша отнимает дополнительные циклы, а время обновления зависит от глубины доменного имени, состояния локальных кэшей и сетевого пути между резолвером и авторитетными серверами имен.

Рис.4. Соотношение трафика запросов и ответов с подписью к трафику без использования DNSSEC



DNSSEC на стороне сервера

А как обстоят дела с ценой DNSSEC для авторитетных серверов имен? Насколько раз-

личается нагрузка при обслуживании подписанной зоны от неподписанной? И какие прогнозы можно сделать для той гипотетической ситуации, когда каждый резолвер DNS выполняет проверку DNSSEC?

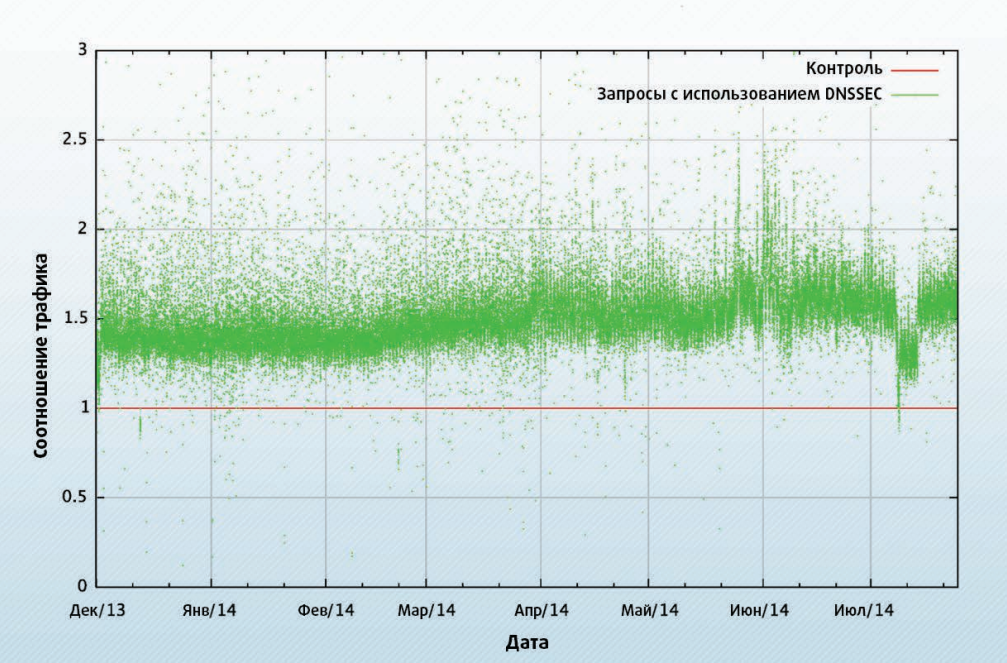
В этом эксперименте мы будем использовать имя из 5 частей. 5-я часть соответствует wildcard в конечной зоне, а 4-я часть намеренно сделана уникальной. Нас интересует нагрузка на авторитетный сервер имен для этих подписанных зон с уникальными именами. Делегирование имен и информация о ключах для первых трех частей ожидаются кэшированными, поэтому нагрузка из запросов, в сущности, вся падает на 4-ю зону. Для неподписанной зоны мы видим один запрос на авторитетном сервере имен: 128-байтовый запрос A-записи и 179-байтовый ответ.

Когда зона подписана DNSSEC и резолвер умеет работать с DNSSEC, обычно присутствуют 2 дополнительных запроса: один для ключа подписи зоны в самой зоне (запись DNSKEY Resource Record, RR), а второй - для ключей подписания ключа и ключей подписания зоны, где запрос направлен серверу имен родительской зоны (DS RR). В этом случае, поскольку авторитетный сервер имен является авторитетным и для подписанной зоны, и для ее подписанного родителя, оба запроса видны на авторитетном сервере имен. В результате авторитетный сервер имен получает 3 запроса: для нашего эксперимента это 287 байт запросов и 2251 байт ответов. Можно сделать вывод, что ценой обслуживания зоны, подписанной DNSSEC, является увеличение нагрузки по запросам вдвое (или втрое, если авторитетный сервер обслуживает и родительскую зону), а нагрузки по ответам - в 11 раз (или в 12, если обслуживается и родительская зона) при ответах на запросы резолвера, поддерживающего DNSSEC.

Что мы видим в этом эксперименте?

В этом эксперименте авторитетный сервер имен был авторитетным и для последних подписанных зон, и для их общей родительской зоны, поэтому следовало бы ожидать, что сервер получит и запрос DNSKEY RR для последней подписанной зоны, и запрос DS RR для той же зоны, адресованный родительской зоне. Результаты за 8-месячный период - с декабря 2013 г. по июль 2014 г. - показаны на рис. 3.

Рис.5. Соотношение трафика запросов с подписью к трафику без использования DNSSEC



Трафик ответов на запросы для подписанной зоны вырос примерно с 7-кратного объема трафика для неподписанной зоны в декабре 2013 г. до примерно 8-кратного в июле 2014 г. Этот рост, скорее всего, вызван увеличением количества резолверов DNSSEC, выполняющих проверку DNSSEC за тот же период времени, а не изменениями поведения отдельных резолверов. Из этих данных следует, что если взять неподписанную зону DNS и подписать ее, то для авторитетного сервера имен исходящий трафик ответов на запросы DNS вырастет примерно в 8 раз. Сегодня резолверы DNS, выполняющие проверку DNSSEC, используют примерно 20% всей базы Интернет-клиентов. Если все резолверы станут выполнять проверку DNSSEC, увеличится ли трафик ответов DNS в 40 раз по сравнению с нагрузкой для неподписанного имени? А если так и будет, как это согласуется с теоретическим предсказанием 12-кратного трафика?

Ответ заключается в использовании механизма расширения EDNS0 и флага DNSSEC-OK в рамках этого расширения. В то время как около 80% клиентов в Интернете используют резолверы DNS, не выполняющие никаких проверок подписей DNSSEC, примерно 85% клиентов используют резолверы DNS, которые включают в свой запрос расширение EDNS0 и устанавливают бит DNSSEC-OK для этого расширения. Иными словами, приблизительно 2/3 пользователей Интернета работают с резолверами DNS, которые требуют включать данные подписи DNSSEC в ответы на свои запросы, но проверять эти данные не удосуживаются! Поэтому сегодня лишь 20% клиентов используют резолверы DNS, которые выполняют проверку подписей DNSSEC в той или иной форме, но из-за повального распространения EDNS0 трафик ответов на запросы уже раздут в 7-8 раз. Если эти 20% превратятся в 100%, т.е. каждый резолвер будет выполнять проверку DNSSEC, то увеличение трафика на авторитетном сервере имен возрастет не в 40 раз, а гораздо более скромно - в 11-12 раз, что согласуется с исходным теоретическим предсказанием.

Если игнорировать фактор размера и смотреть только на количество запросов, то зона с подписью DNSSEC дает где-то от 1,4 до 1,6-кратного количества запросов по сравнению с неподписанной (рис. 4). Теория утверждает, что зона с подписью DNSSEC должна генерировать 3 запроса от резолверов с проверкой DNSSEC, поэтому если 20% клиентов используют резолверы DNSSEC, то нагрузка на авторитетный сервер имен по числу запросов увеличится в 1,4 раза. Рост нагрузки по запросам до 1,6 раза коррелирует с тем, что зона, подписанная по DNSSEC, получает в 4 раза больше запросов по сравнению с неподписанной. Частично расхождение обусловлено медленным ростом количества дублирующихся запросов, который мы наблюдали на авторитетном сервере имен, т.е. запросов, в которых связанные резолверы DNS отправляли серверу

один и тот же запрос практически параллельно. Это явление наблюдается в решениях, где резолверы объединены в фермы,а исходный запрос направляется на несколько резолверов одновременно с тем, чтобы повысить надежность и улучшить кэширование системы.

В этом случае эффект кэширования имени не обязательно влияет на расчеты. Пусть наш эксперимент и использует уникальные имена, которые нельзя найти в кэше резолвера DNS, но эта ситуация аналогична обращению к часто используемому имени, когда отдельные резолверы периодически обновляют свой кэш ответами с авторитетного сервера имен. Здесь нас интересует не абсолютное число запросов и не абсолютное количество байтов, а пропорция этих значений для имени, подписанного DNSSEC, и неподписанного имени.

Сегодня подписание доменного имени по DNSSEC увеличит общую нагрузку по количеству запросов на авторитетные серверы имен примерно в 1,5 раза, а исходящий трафик - приблизительно в 8 раз. Также можно предсказать, что если весь Интернет перейдет на резолверы, проверяющие подписи DNSSEC, то подписание имени для авторитетного сервера имен увеличит нагрузку по числу запросов примерно в 4 раза, а по трафику ответов - в 12 раз.

Плюсы и минусы

До этого момента мы сравнивали DNS-трансляцию неподписанного имени с подписанным по DNSSEC. Но, несмотря на все усилия, бывают случаи, когда подпись DNSSEC не удается проверить. Разумеется, тому есть множество причин. Ключи подписания могут быть просрочены, либо может быть нарушена связь ключей родительского и дочернего доменов, либо зона может быть так или иначе повреждена. Кроме того, проблема вообще может не иметь отношения к файлу зоны и ее авторитетным серверам имен. Резолвер может не поддерживать используемый алгоритм подписания, или же первоначальный комплект корневых ключей может быть просрочен (см., например, статью Rollover and Die).

Что происходит при неудачной попытке проверки?

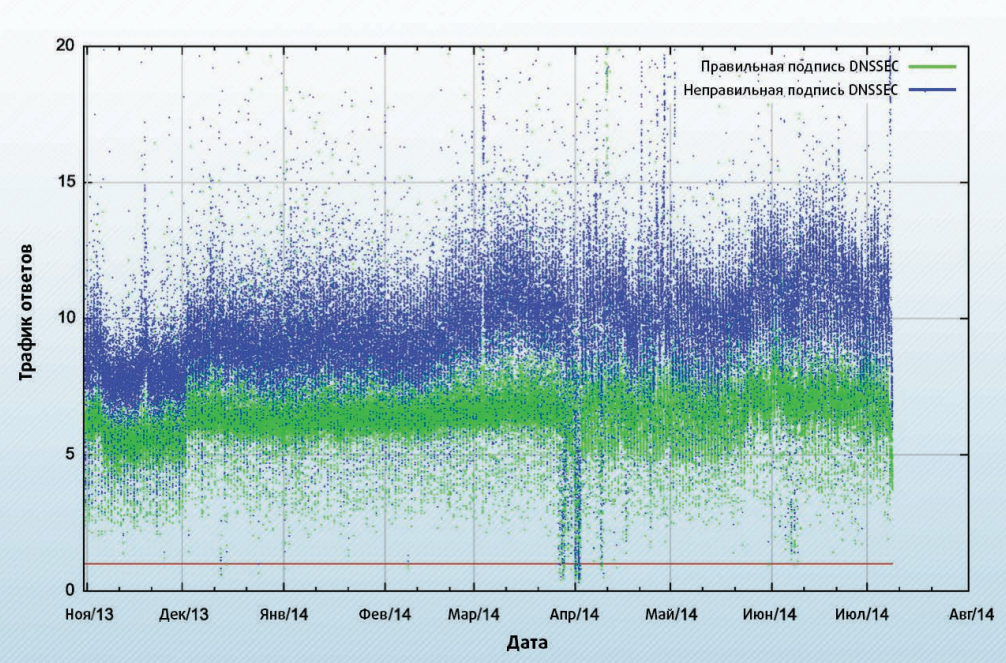
С точки зрения конечного клиента видно, что есть проблема, но непонятно, в чем она заключается. Резолвер, поддерживающий DNSSEC, при возникновении проблемы с проверкой DNSSEC возвращает ответ на исходный запрос с кодом ответа, который туманно сообщает об «ошибке сервера». Авторы этого кода ошибки первоначально имели в виду, что, возможно, само транслируемое имя в полном порядке, но сервер почему-то не смог его транслировать. Кстати, многие конечные клиенты используют несколько резолверов DNS именно на этот случай. Если запрос к одному резолверу не дает результата, следующим шагом будет повторный запрос к другому резолверу. Даже если он тоже окончится неудачей с тем же кодом ошибки, не все потеряно. Запрос можно повторить, установив размер EDNS0 в 512. Поэтому, если клиенты используют резолверы с проверкой DNSSEC и если подпись DNSSEC неправильна, возникают повторные запросы.

Повторяют запросы не только конечные клиенты. Как показано в статье Rollover and Die, некоторые старые версии кода трансляции DNS прослеживают иерархию делегирования имен назад и вверх и пытаются проверить подпись DNSSEC, используя все возможные векторы серверов имен зоны в последовательности запросов подписи. Только если такой всеобъемлющий запрос не дает результата, резолвер возвращает код «Ошибка сервера».

Влияние такого прилежания резолверов, стремящихся во что бы то ни стало найти хороший путь для проверки цифровой подписи, изображено на рис. 5. Четверть всех конечных клиентов, выполняющих проверку DNSSEC, используют DNSSEC-резолверы, которые продолжают рассылать запросы о плохо подписанном имени DNSSEC в течение более 6 секунд. Шестая часть клиентов работает с DNSSEC-резолверами, которые не бросают попыток найти хороший путь проверки в течение 20 секунд и более. Поэтому для клиента, использующего DNSSEC-резолверы при попытке транслировать плохо подписанное имя, ситуация выглядит так: разумеется, DNSSEC-резолвер не может транслировать имя, но ждать плохих новостей части клиентов приходится очень долго.

Можем ли мы дать количественную оценку фактору роста запросов на авторитетном сервере имен для случая, если подпись DNSSEC не удается транслировать? На рис. 6 изображен относительный профиль трафика при обработке правильно подписанного имени и плохо подписанного имени. Для плохо подписанного имени трафик ответов втрое больше, чем для правильно подписанного. Из этого можно сделать вывод, что если каждый резолвер DNS будет поддерживать DNSSEC, то авторитетный сервер имен будет испытывать 24-кратное увеличение трафика по сравнению с обработкой неподписанного имени. Однако, поскольку только 22% резолверов производят валидацию и, соответственно, реагируют на неправильную подпись, разница между правильно и плохо подписанными именами

Рис.6. Трафик ответов DNS для плохо подписанного имени

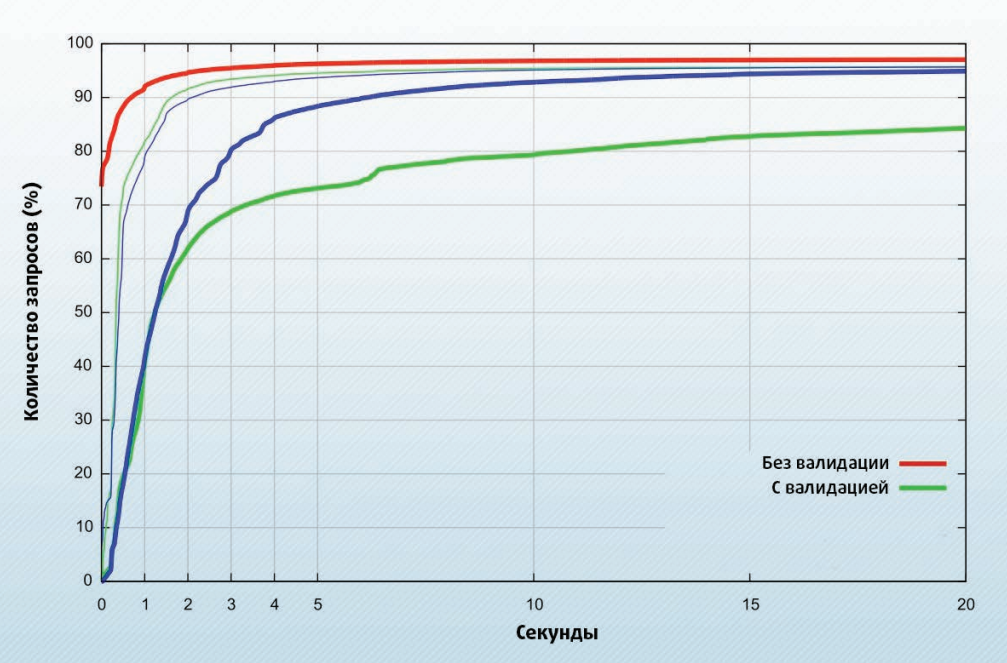


не столь велика, и наблюдаемое воздействие плохой подписи составляет около 3-кратного по сравнению с правильно подписанным именем.

Но это нижняя граница, а не реалистичный индикатор ожидаемого воздействия. Когда мы изучали соотношение трафика для неподписанного имени и правильно подписанного имени на рис. 4, прозвучал комментарий, что это соотношение не изменится, если имя станет кэшируемым, до тех пор, пока параметры кэширования одинаковы для обоих имен. В качестве входящих запросов на авторитетный сервер имен попадают те запросы, которые вызвали непопадание в кэш на локальном резолвере.

Однако если имя подписано плохо, резолверы с поддержкой DNSSEC не должны кэшировать ответ, т.к. результат попытки трансляции имени ненадежен. Значит, наблюдаемый 3-кратный относительный коэффициент нагрузки относится только к сравнению трансляции некэшированных имен. Если же имя кэшируемое, а подпись DNSSEC неправильная, то рост нагрузки по количеству запросов и объему трафика на авторитетном сервере имен будет более ощутим, т.е. каждый DNSSEC-резолвер будет давать промах мимо кэша при каждой попытке трансляции.

Рис.7. Время выполнения запроса DNS для плохо подписанного имени



Повышение объема трафика в результате искажения подписи DNSSEC зависит от исходных параметров кэширования и исходного уровня попаданий в кэш. Рост относительной нагрузки на авторитетный сервер имен в результате неправильной подписи DNSSEC может быть произвольно большим, поскольку результатом является произведение базового коэффициента пропорциональности 3 на уровень попаданий в кэш для эквивалентного корректно подписанного имени.

Цена DNSSEC

Эффективная работа DNS зависит от эффективного кэширование, и появление DNSSEC ничего не меняет в этой ситуации. Цена добавления подписи DNSSEC для клиента практически нивелируется кэшированием DNS.

Для серверов имен цена несколько больше, поскольку увеличение длины ответов DNSSEC означает и увеличение объема трафика. Сегодня подписание имени означает возрастание нагрузки по запросам в 1,5 раза, а исходящего трафика - в 8 раз. Если весь Интернет перейдет на резолверы, проверяющие подписи DNSSEC, то подписание имени для авторитетного сервера имен увеличит нагрузку по числу запросов примерно в 4 раза, а по трафику ответов - в 12 раз.

Крайне важно поддерживать подписи DNSSEC в должном порядке. Для неправильных подписей количество запросов возрастает лавинообразно. Можно ожидать как минимум удвоения числа запросов по сравнению с правильно подписанным именем и аналогичного удвоения объема трафика. Но, подчеркиваем - это как минимум. Скорее всего, рост будет гораздо больше. И эта нагрузка на сервер не будет приносить абсолютно никакой пользы. Если подпись неверна, то DNSSEC-резолверы и их клиенты будут не в состоянии транслировать имя.

Оговорка

Изложенные выше воззрения могут не совпадать с позицией Asia Pacific Network Information Centre.

Об авторе

ДЖЕФФ ХЬЮСТОН (Geoff Huston) - главный исследователь APNIC, регионального интернет-регистратора, обслуживающего Азиатско-Тихоокеанский регион.

Источник: The Cost of DNSSEC. Geoff Huston. The ISP Column

IT-конференции

Ольга Александрова-Мясина

Привет. Меня зовут Ольга. Я буду рассказывать вам о мероприятиях в сфере IT и интернета, на которых бываю. Начну с того, что конференции в сфере IT и интернета - это большая часть моей жизни. На одних я работаю как организатор, на других - участник деловой программы или слушатель. Поэтому могу поделиться своими впечатлениями о двух сторонах мероприятия: той, которую видят все, и той, с которой знакомы лишь те, кто мероприятия делает.

На самом деле это очень интересно, когда на «чужом» мероприятии ты почти автоматически отмечаешь все достоинства и недостатки, понимаешь, что стоит за небольшой заминкой с микрофоном для спикера и думаешь, кто даст тебе контакты отличной кейтеринговой службы, которая настолько быстро и эффективно накормила 500 человек сразу.

Вообще о мероприятиях, которые проводишь не ты, писать гораздо проще. Тут можно и порассуждать о том, что можно было бы сделать еще, и пожурить коллег за нерасторопность, и дать несколько полезных советов. Но, с другой стороны, любое мероприятие, которое делает наша команда, тоже можно вот так разобрать по косточкам и найти в нем как множество достоинств, так и немало недостатков, видимых стороннему профессиональному глазу. Поэтому будет лучше, если для начала я попробую беспристрастно взглянуть на одно из самых крупных мероприятий, которое мы с коллегами из Координационного центра доменов .RU и .РФ (КЦ) подготовили и провели. Это был Российский форум по управлению Интернетом RIGF-2015.

Проводили мы его уже в шестой раз, поэтому, конечно, у нас есть некоторый опыт и понимание того, как это мероприятие нужно делать. С прошлого года мы решили объединить этот форум с празднованием дня рождения точки RU и оба мероприятия провести 7 апреля. Несмотря на то, что проводить два ивента в один день всегда сложно, мы решили так сделать из-за большого количества зарубежных гостей. Понятно, что раз уж они получили визу и купили билет, то надо показать им все, что возможно за короткий период времени. А возможно немало. Во-первых, сама по себе Москва фантастически красива весной, распускается зелень, первые цветы и первое солнышко. Во-вторых, можно посетить другие форумы и конференции, которые проходят «рядом» с нашим событием.

Я приехала в Лотте отель (именно там был форум) рано утром для того, чтобы проверить полную готовность. В зале наносились последние штрихи, команда на регистрации разворачивала компьютерную систему для регистрации гостей форума и печати бейджей, официанты расставляли столы и посуду для кофе-брейка. Ведущий форума, мой коллега Леонид Тодоров был, как всегда, идеален – в костюме с прекрасно подобранным галстуком, благоухающий хорошим парфюмом.

Я всегда страшно волнуюсь перед началом всех наших мероприятий. Конечно же, понимаю, что если все запланировать и предусмотреть, то ничего не случится, но эмоции всегда берут вверх над разумом.

Вот уже стали подходить другие сотрудники, обслуживающий персонал и даже первые участники. Как хорошо, что есть люди, приходящие на мероприятия заранее! Если бы не эти достойные посетители, я бы ровно в 9 умирала бы от мысли о том, что никто не придет, но первые посетители всегда меня успокаивают.

Потом еще немного и вот оно – торжественное открытие! Форум открывался небольшим фильмом про Интернет с цифрами и данными о кибермошенниках. Такие фильмы всегда очень хорошо принимаются аудиторией, а вся наша команда чувствует невероятную гордость за некоторую причастность к тому, о чем речь.

После официального открытия можно немного вздохнуть. Для меня это практически полдела. Почему-то в этот момент кажется, что дальше всё пойдет само собой. Поэтому я спокойно устроилась в кресле возле стойки регистрации и собралась проверить почту. Вдруг мне пришло sms-сообщение от директора Андрея Колесникова: «Перешли к награждению орденом, неси его в зал».

Небольшое отступление – надо рассказать о том, что это за орден.

Идея награждать выдающихся деятелей интернета пришла нам в голову еще при подготовке к самому первому RIGF в 2010 году. Мы изготовили специальные ордена со знаком @ Virtuti Interneti («За заслуги в сфере интернета»), и с тех пор традиционно награждаем лучшего из лучших интернетчиков во время форума по управлению интернетом.

В этот раз решено было наградить Пола Викси.

Пол Викси – один из создателей современного интернета, разработчиком и автором современных интернет-протоколов и систем, на которых работает современная сеть. Он является основателем Консультативного совета по системам корневых серверов ICANN (RSSAC) и Консультативного совета по безопасности и стабильности ICANN (SSAC), много лет занимался управлением корневым сервером F-root. Теперь он входит в команду поддержки корневого сервера C-root и является системным администратором Op Sec Trust.

И вот читаю я смс и осознаю, что орден благополучно лежит в офисе на столе, так как достать-то я его достала, а вот с собой на форум по какой-то причине не взяла. В тот момент я физически ощутила, что испыта-

ют люди во время землетрясения: мне захотелось убежать, куда глаза глядят. Я стала судорожно думать, что предпринять. Вернее так: как сделать, чтобы я закрыла глаза, а когда их открыла, то еще было бы вчера. Но чудес не бывает, пришлось звонить в офис и организовывать эстафету, где мне пришлось исполнить роль ведущего бегуна. Орден был доставлен вовремя, ноги стерты. Потом вечером, когда я сняла туфли, то почувствовала невероятное счастье! Пожалуй, по-настоящему счастливым человеком я до этого момента и вовсе и не была!

Отмечу две секции, которые мне особенно запомнились: «Снизу вверх и наискосок» и «Ваш звонок очень важен для нас».

На первой обсуждались проблемы управления интернетом и роль, которую в этом процессе могут играть страны БРИКС (группа из 5 стран: Бразилия, Россия, Индия, Китай и Южная Африка). Эксперты акцентировали внимание на актуальных вопросах в различных аспектах. Особое внимание было уделено опасности дробления глобальной сети и площадок, на которых обсуждаются вопросы управления ею. Модератором секции была Мадина Касенова, в дискуссии приняли участие Олег Демидов (Россия), Лаки Мазилела (ЮАР), Марилия Масиел (Бразилия), Марина Никерова (Россия), Парминдерджит Сингх (Индия) и Люнь Хань (Китай). Интересно, что на этой секции были представлены все страны, входящие в БРИКС. И хотя, с одной стороны, представители всех этих пяти стран говорили о гегемонии США в интернете и давлении американского правительства на сеть, с другой - все они высказывали озабоченность возможностью раздробления интернета на отдельные сегменты. Так, Парминдерджит Сингх (IT for Change, Индия) подчеркнул, что политический вакуум в сфере управления интернетом сформировался уже достаточно давно, но, с его точки зрения, управление интернетом не может быть «растворено» в техническом сообществе, и та или иная политическая структура в данной сфере в любом случае необходима. Еще больше опасений из-за возможного дробления сети выразила Марилия Масиел (Center for Technology and Society of the Getulio Vargas Foundation, Бразилия), которая расценила сегодняшний момент как критический для создания устойчивой основы и новых принципов управления глобальной сетью. За объединение усилий всех стран и сторон выступил и Лаки Масилела (ZACR, ЮАР), который весьма образно описал сегодняшние попытки выработать новые принципы управления интернетом как попытки дюжины слепцов описать слона, ощупывая его с разных сторон. Он подчеркнул, что лишь стремление всех стран и сообществ к сотрудничеству позволит решить задачу, стоящую перед интернет-сообществом.

На секции «Ваш звонок очень важен для нас» обсуждалось взаимодействие интернет-бизнеса и органов государственной власти. Эксперты, участвовавшие в дискуссии, высказались на темы локализации и хранения персональных данных пользователей, проблем налогообложения международных интернет-компаний и концепции сетевого нейтралитета. В обсуждении этих вопросов приняли участие Вартан Хачатуров, Александр Шепилов, Михаил Якушев, Дмитрий Мариничев, а также Фредерик Донк (Бельгия) и Жюльен Носетти (Франция). Член Совета Федерации РФ Александр Шепилов на примере недавних отключений пользователей Крыма от ряда интернет-сервисов констатировал, что декларации об отсутствии границ в глобальной сети остаются скорее словами, и государства вынуждены реагировать на подобные прецеденты. Интернет-омбудсмен Дмитрий Мариничев высказался против дробления и излишнего регулирования интернета, за смягчение требований по хранению персональных данных, а также за то, чтобы любая технология контролировалась, прежде всего, техническим сообществом. Фредерик Донк (ISOC, Бельгия) призвал представителей государственной власти мыслить более глобально, оценивая долгосрочные последствия принимаемых решений. Он также охарактеризовал проблему локализации и хранения персональных данных как стремление решить политические цели техническими средствами.

Второе весеннее мероприятие, на котором я побывала, был **РИФ (Российский Интернет Форум)** – и здесь я уже была слушателем и немного участником программы. Я люблю это мероприятие с тех самых пор, когда оно проходил только в Лесных далях, а все участники и выступающие помещались в 6 корпусах пансионата, еще и свободные номера оставались. Тогда приезжали только те, кто напрямую относился к интернет-рынку, здесь не было продавцов пластиковых окон и представителей маленьких интернет-магазинов. Теперь все изменилось, и вот уже толпы людей на регистрации, шатры для докладов, все соседние пансионаты заняты участниками, и столько новых лиц, что кажется, конференция совсем на другую тему, а ты тут так...случайно.

Множество интересных секций, в параллелях, докладчики рекламируют свои компании, как будто они попали на сцену перед целевой аудиторией в последний раз и надо успеть рассказать обо всех сервисах, иначе командировку не засчитают.

Тем не менее, интересно было послушать секцию под названием «Антипиратский закон. Что ждет Рунет?»

Вернее это была не секция, а панельная дискуссия, в ходе которой обсуждали тему поправок к антипиратскому закону, вступивших в силу с 1 мая 2015 года.

Эти поправки ужесточили законодательство в области защиты интересов правообладателей. Теперь действие закона распространяется на музыку, книги и программное обеспечение. Вводится механизм досудебного урегулирования споров между правообладателями и владельцами сайтов. Последние обязаны публиковать свои контакты, чтобы правообладатели имели возможность направить требование об удалении незаконно размещенного контента. Неисполнение требования правообладателя влечёт блокировку ресурса, а за повторное нарушение интернет-площадки будут блокироваться навсегда. Реестр заблокированных таким образом сайтов будет вести Роскомнадзор.

В дискуссии участвовали представители бизнеса, правообладателей и государства, которые обсудили особенности поправок к антипиратскому закону для всех заинтересованных сторон и возможности для интернет-площадок по минимизации возможных рисков в связи с вступлением в силу расширенного «антипиратского» закона. В центре внимания оказались вопросы эффективного использования закона для борьбы с пиратами и монетизации легального контента как правообладателями, так и интернет-площадками. Надеюсь, что информация была услышана всеми сторонами и будут приняты необходимые решения.

Потом наступил май и я начала подготовку посещения Санкт-Петербурга. Там меня ждал **IPV6 Day** и знаковое отраслевое мероприятие **ХостОбзор**, что ежегодно проходит в 100 км от города.

Музей связи ждал участников дня IPV6, и уже во второй раз я напросилась на экскурсию по этому легендарному месту. Помимо прекрасного зала с колоннами, там есть и действует музей с различными экспонатами, которые хоть как-то относятся к сфере радио. Внизу, в большом зале со стеклянной

крышей стоял настоящий спутник и все с ним фотографировались.

Открыли мероприятие **Елена Воронина**, генеральный директор MSK-IX, и **Алексей Платонов**, генеральный директор Технического центра Интернет. Они поздравили участников с юбилеем и отметили, что успех компании стал возможен благодаря ее сильному академическому фундаменту и совместной работе с партнерами.

Елена Воронина также напомнила, что переход на IPv6, по прогнозам, займет 20-25 лет.

Сергей Киселев, руководитель проектов развития MSK-IX, рассказал, что в настоящее время MSK-IX занимает четвертое место в мировом рейтинге точек обмена трафиком и лидирует по числу уникальных подключенных сетей. Точки присутствия MSK-IX расположены во всех федеральных округах России, услугами компании пользуются более 500 клиентов, а суммарный объем трафика уже вплотную приблизился к 1,5 Тбит/с. Оказывается, что в настоящее время все сети компании полностью поддерживают IPv6 и предоставляют своим клиентам подключение и обмен трафиком по этому протоколу. Потом выступил представитель RIPE NCC **Максим Буртиков** и рассказал, какие компании уже внедрили IPV6 и где они находятся. По его словам, большинство компаний, поддерживающих работу с IPv6, расположены в крупных российских городах, и в регионах распространение IPv6 не так велико. Тем не менее, уже более 75% всех локальных интернет-регистратур (LIR) получили блоки IPv6 адресов и постепенно адаптируют свою инфраструктуру для работы с ними. Также Максим отметил, что в настоящее время в мире сложно выделить лидера по темпам внедрения протокола, все страны находятся примерно на одном уровне и отличаются только динамикой работы с существующими сетями. По его словам, работа крупных технологических компаний с регионами будет способствовать его скорейшему внедрению.

Во время завершающего фуршета я уже катила свой боевой чемодан по ковровым дорожкам музея, чтобы успеть на автобус до пансионата Raivola.

Ехали мы по пробкам часа два, не меньше, зато потом меня практически свалил с ног невероятный запах хвойного леса, на контрасте с городским смогом он действовал вдохновляюще.

Вечер первого дня на ХостОбзоре – это время для общения с коллегами, старыми и новыми. Ведь сюда приезжают даже те, кто ушел с рынка, но рынок их не отпускает. Все собираются в баре «За спичками», занимают большие столы для тех, кто подтянется позже, и разговаривают...

Здесь придумываются новые проекты, заключаются новые сделки и договоры. Думаю, что многие хостинговые и регистраторские компании в России обязаны этому культовому месту за всё то, что сейчас у нас есть. За то хорошее и плохое, что окружает нас каждый день в нашей работе. За ту часть интернета, что была создана на ХостОбзоре, на неформальной части общения.

Потом был первый день – он самый насыщенный. Там, во время оживленной дискуссию с представителями Минкомсвязи, хостинг-провайдеры обратились к интернет-омбудсмену Дмитрию Мариничеву с просьбой о налаживании конструктивного диалога с органами власти.

Было составлено письмо с просьбой о содействии. Также от имени «ХостОбзора» было составлено и опубликовано открытое письмо к хостинг-провайдерам с призывом присоединится к инициативе.

В результате совместной работы отрасли и интернет-омбудсмена предполагается решить две наиболее актуальные проблемы в индустрии хостинга: первая – это правовая неопределенность в работе хостинговых компаний, вызванная отсутствием внятного лицензирования услуг связи; вторая – это отсутствие возможности для хостинг-провайдеров предпринимать активные действия в случае блокировки ресурсов, расположенных на их мощностях.

В дальнейшем взаимодействие между хостинг-провайдерами и интернет-омбудсменом будет идти напрямую. Предполагается, что в результате совместной работы эксперты в области хостинга смогут сформировать предложения по изменению регулирующих документов, которые затем будут рассматриваться органами государственной власти.

Второй день был для меня коротким, он выпадал на субботу и чтобы успеть на «Сапсан», мне надо было покинуть конференцию в середине дня.

Тем не менее, удалось послушать Марину Никерову из Технического центра Интернет, которая рассказала о новой маркетинговой программе для регистраторов. Эта программа затрагивает технические решения, вопросы маркетинга, работы с регистраторами и конечными пользователями. В ее основе лежит идея более тесного сотрудничества с регистраторами и поддержки их бизнес-инициатив.

Среди самых важных изменений, которые вступят в силу в ближайшее время — запуск процедуры безбумажного переноса доменного имени между регистраторами, введение рейтинга регистраторов, новые скидочные программы и услуги для конечных пользователей.

Новая система рейтинга регистраторов позволит выявить самых активных и эффективных игроков рынка. Регистраторы, которые успешнее всего ведут бизнес, получат дополнительное освещение в СМИ и на сайтах КЦ и ТЦИ, а в перспективе – дополнительные привилегии от Технического центра Интернет. При составлении рейтинга будут учитываться разнообразные факторы: динамика прироста количества зарегистрированных доменных имен, участие в маркетинговых акциях, обеспечение кибербезопасности и многое другое.

Такая у меня была весна.

А потом настало лето и началось оно с конференции **ENOG в Казани**. Сначала про город. Он мне понравился - широкие улицы, добрые люди. Кажется, что небо там так высоко, что даже на самолете до него не добраться, а облака хочется потрогать. Они там как из детства; кудрявые, белые и можно разглядывать фигурки зверей и птиц. Еще в Казани удивительной красоты набережная, открывающая вид на красавицу-Волгу. И потрясающе вкусная местная кухня!

Для меня этот город – город простора и воздуха. Так легко там дышать и передвигаться. Кстати, о передвижении. Такси в городе стоит очень дешево. Самая дорогая наша поездка была из аэропорта в город -1000 р., а самая дешевая по городу – 59 р. Зачем при таких ценах местные жители перемещаются на собственных автомобилях, мне не понятно.

За день до открытия ENOG мне удалось побывать на партнерском завтраке MSK-IX. Так как текущий год юбилейный для компании, то было запланировано провести серию мероприятий для региональных партнеров и для тех, кому близка тема Internet Exchange.

В небольшом зале отеля Holiday Inn был накрыт приятный кофе-брейк с разноцветными чашками. Хорошее решение, которое сразу бросилось в глаза, и я записала идею в свой «волшебный» блокнот.

Открыл мероприятие директор по продажам MSK-IX **Евгений Морозов**, он рассказал об истории развития точек обмена трафиком в России и мире, привел статистику по ним, а также остановился на особенностях работы с европейскими IX. По его словам, московская точка обмена трафиком имеет наибольшее количество уникальных клиентов, что дает компании серьезные преимущества. Также Евгений рассказал об истории развития связи в Казани и Татарстане в целом, и о планах MSK-IX в этом регионе.

Александр Ильин, технический директор MSK-IX, в своем докладе уделил внимание техническим особенностям работы точки обмена трафиком. Он подчеркнул, что в Казани расположена не только точка присутствия, но и DNS-узел, поддерживающий основные российские доменные зоны .RU, .РФ, .SU и многие другие.

«Мы не стоим на месте и постоянно развиваем свою инфраструктуру. Сейчас идет миграция на новую платформу, мы укрупняем узлы и расширяем каналы. Все работы сопровождаются тщательным анализом и экспертизой, поэтому переезд пройдет незаметно для наших пользователей. В свою очередь мы призываем всех принять более активное участие в развитии российского рынка пиринга и открыты для всех предложений по организации точек доступа,» – сказал Александр.

Потом начался ENOG, и я практически все эти два дня провела в зале конференции: наша команда вела твиттер на двух языках, фотографировала участников и писала новости, а это, должна я вам сказать, нелегко, даже в 6 рук.

Конференция проходила в девятый раз. Каждый год ENOG собирает представительную аудиторию международных и региональных экспертов из разных стран мира, представителей операторов связи и сервис-провайдеров.

Участников конференции приветствовал заместитель министра информатизации и связи Республики Татарстан Тимур Зарипов. Он напомнил, что одним из знаковых событий в сфере интернета в 2014 году стал запуск первого российского регионального домена верхнего уровня .TATAR.

В первый день конференции обсуждались вопросы глобального управления интернетом, роли государств и международных организаций в этом процессе, локализации трафика, перспективы процедуры NTIA Transition, которая должна завершиться в сентябре этого года. Председатель RIPE Ганс Холен рассказал , в какой стадии находится процесс передачи прав подписи корневой доменной зоны, Евгений Усков из HLL представил анализ маршрутизации трафика в волжском регионе, а Алексей Семеняка в своем докладе коснулся темы передачи IP-адресов в России. Кроме того, представители RIPE NCC провели несколько практических занятий по использованию различных инструментов RIPE NCC для мониторинга и анализа сетевой инфраструктуры.

Второй день региональной конференции ENOG 9 в Казани был посвящен обсуждению перспектив развития IX, изменений в пиринговой политике и локализации трафика. Эти вопросы обсуждались на круглом столе «Многоликий распределенный пиринг и российская экосистема IXP» с участием операторов связи и региональных точек обмена трафиком. Круглый стол провела генеральный директор MSK-IX Елена Воронина.

Участники круглого стола поделились со слушателями своими взглядами на перспективы развития рынка обмена трафиком и рассказали о том, с какими основными вызовами приходится сталкиваться игрокам. Большое внимание было уделено и критериям качества работы с региональными IX. По мнению Алексея Рогдеева из компании Ростелеком, задача по локализации трафика в регионах является одной из самых важных: «Я считаю, что точки обмена трафиком должны стоять в каждом субъекте федерации. Это помогает улучшить сервис для конечных клиентов и способствует развитию широкополосного доступа». Он так же отметил, что не видит конкуренции между точками обмена трафиком и магистральными операторами.

В завершение конференции управляющий директор RIPE NCC **Аксель Павлик** наградил программный комитет за работу над формированием программы форума, а народ перебрался в фойе пить вино, чай, кофе и разговаривать про бизнес.

Уезжала я и еще несколько коллег на следующий день. До аэропорта мы очень быстро доехали всего за 400 рублей. Слоняясь внутри здания после досмотра и ожидая вылета, мне удалось обнаружить магазин, где продавались меховые игрушки. Не выдержала и усадила в рюкзак белоснежного мехового зайца, который очень просил забрать его в Москву.

Календарь событий: 2015 год

Международные события

5-7 октября 2015
NANOG65,
Монреаль, Канада

Североамериканская группа сетевых операторов (The North American Network Operators Group, NANOG), является одной из самых активных профессиональных ассоциаций в области сетевой архитектуры, конфигурации и технического администрирования сетей в Интернете. Основной фокус NANOG на технологиях и системах, обеспечивающих работу Интернета: систему глобальной маршрутизации, DNS, пиринг и связность. https://www.nanog.org/meetings/NANOG65/home

13-14 октября 2015
ENOG10,
Одесса, Украина

ENOG (Евро-азиатская группа сетевых операторов) представляет собой региональный форум интернет-специалистов, занимающихся важнейшими аспектами работы Интернета. В рамках форума они имеют возможность обмениваться опытом и знаниями по вопросам, присущим Российской Федерации, странам СНГ и Восточной Европы. http://www.enog.org/meetings/enog-10/

1-6 ноября 2015
IETF94,
Йокохама, Япония

IETF (Internet Engineering Task Force) является одной из основных организаций по разработке стандартов в области Интернета. В основном работа в IETF производится в могочисленных списках рассылки, соответствующих различным рабочим группам (этих групп более 100). Три раза в год IETF проводит недельные совещания на которые приезжают разработчики протоколов, инженеры и операторы со всего мира. https://www.ietf.org/meeting/94/

16-20 ноября 2015
RIPE71,
Бухарест, Румыния

Встреча RIPE проводятся два раза в год и собирают около полутысячи участников для обсуждения вопросов политики распределения номерных ресурсов (IP адресов и номеров автономных систем) в зоне обслуживания RIPE NCC, сотрудничества, а также технические вопросы связанные с маршрутизацией, DNS, связностью, измерениями и инструментарием. https://ripe71.ripe.net/

В России

14 октября, Россия, Новосибирск

Партнерский завтрак - завершающее мероприятие цикла семинаров MSK-IX
В честь 20-летия MSK-IX в течение 2015 года проводит серию мероприятий в городах России. Топ-менеджеры компании встречаются с представителями телеком-сообщества, чтобы обсудить актуальные темы пиринга, развития и обеспечения безопасности сетей передачи данных. http://www.msk-ix.ru/events/mskix-20years/

с 15 по 17 октября, Россия, Красноярск

Специализированная выставка «Информационные технологии. Телекоммуникации» itCOM 2015
Экспонируемые продукты: сети, телекоммуникационные технологии, сетевые компоненты и обеспечение, приложения и сервисы, информационные системы и др. http://www.krasfair.ru/events/itCOM/

с 10 по 12 ноября Россия, Якутск

Межрегиональная выставка «Информационные технологии. Телекоммуникации. Связь 2015»
Экспонируемые продукты: оборудование и системы связи, телерадиовещание, кабели связи и антенны, мобильная, спутниковая связь, телекоммуникационные системы, мобильное телевидение, беспроводные сети, интернет-провайдеры, IT-системы и оборудование, IT-консалтинг и др.

24-26 ноября 2015, Россия, Екатеринбург

Специализированная выставка техники и технологий для защиты информации. DISCOVER ICT 2015
«DISCOVER ICT» - открытие комплекса информационных и коммуникационных технологий с учетом тесной взаимосвязи этих технологий для потребителей. Основные тематические разделы: связь, интернет, аппаратные средства, программное обеспечение, инвестиции и государственная поддержка. http://discover-ict.com/index.php/ru/

В Москве

с 1 по 2 октября 2015, гостиница «Метрополь»	9-й Международный Форум и выставка «ПРОФЕССИОНАЛЬНАЯ РАДИОСВЯЗЬ И НАВИГАЦИЯ» Организатор: infor-media Russia
6 октября 2015, event-холл «ИнфоПространство»	«Ethernet-форум – 2015» Организатор: «Журнал сетевых решений/LAN» и Агентство OSP-Con http://www.ospcon.ru/event/ethernet-forum-2015_125.html
15 октября 2015, отель «Radisson Blu Belorusskaya»	Пятый Международный Форум «TELECOM NETWORKS: F&M Infrastructure. Sharing, Engineering, Development, Outsourcing & Metering» Организатор: Connectica Lab http://www.telconetworks-forum.com/
11 ноября 2015, отель «Radisson Blu Belorusskaya»	Шестая Всероссийская Конференция «Revenue Assurance, Fraud, InfoSecurity & Risk Management» Организатор: Connectica Lab http://www.revassurance-forum.ru/
12 ноября 2015, отель «Рэдиссон Славянская»	CNews Forum 2015: Информационные технологии завтра Организатор: CNews Conferences http://www.forum.cnews.ru/
19 ноября 2015, отель «Radisson Blu Belorusskaya»	III Международный Форум «SMART ENERGY & SMART GRID. Проектирование и развитие интеллектуальных энергетических систем и сетей» Организатор: Connectica Lab http://www.smartgrid-forum.com/
25 ноября 2015, event-холл «ИнфоПространство»	Форум «Data Cloud World 2015» Организатор: издательство «Открытые системы» http://www.ospcon.ru/event/forum-data-cloud-world-2015_129.html
с 26 по 27 ноября 2015, отель «Холидей Инн Лесная»	V международный форум «Broadband Russia Forum 2015 – Развитие широкополосных сетей нового поколения в России» Организатор: ComNews Conferences http://www.comnews-conferences.ru/bb2015
3 декабря 2015, бизнес-центр «Японский дом»	Международный Форум «PROмобильность: бизнес, инфраструктура, приложения» (PROмобильность-2015) Организатор: CIS Events Group http://www.moscow-promobility-2015.ciseventsgroup.com
9 декабря 2015, отель «Radisson Blu Belorusskaya»	Шестой Форум «Loyalty in Telecom & Media. Удержание клиентов и маркетинговая аналитика для телеком, медиа и интернет бизнеса» Организатор: Connectica Lab http://www.telcoloyalty-forum.com/
10 декабря 2015, здание Правительства Москвы	Пиринговый форум MSK-IX 2015 Форум дает возможность специалистам обменяться опытом, узнать о последних технологических решениях. Организатор: MSK-IX http://peering-forum.ru/