№7
ноябрь 2017

MSK IX

Интернет изнутри

Пиринг и транзит

Безопасный пиринг

Защищенность конкретной сети зависит от усилий других сетевых операторов. Как защитить себя и глобальную систему маршрутизации

Содержание:

Журнал «Интернет изнутри»
По всем вопросам пишите на info@internetinside.ru

Порядковый номер выпуска и дата его выхода в свет:
Выпуск №7, дата выхода: ноябрь 2017 г.

Свидетельство о регистрации СМИ в Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций.
Регистрационный номер:
ПИ № ФС77-71202 от 27.09.2017

Публикуется при поддержке АНО «ЦВКС «МСК-IX»

Главный редактор:
Андрей Робачевский

Зам. главного редактора:
Новикова Татьяна

Редакционная коллегия:
Воронина Елена
Платонов Алексей

Дизайн:
Чернега Наталья

Корректор:
Рябова Наталья

Связность = пиринг + транзит

главный редактор,
Андрей Робачевский

Дорогой читатель!

В одном из предыдущих номеров журнала, посвященном проблемам связности, мы задались вопросом, каким образом связность Интернета остается такой стабильной и всеобъемлющей, учитывая, что этот результат зависит от взаимодействия десятков тысяч сетей без какой-либо централизованной координации. Удивительно, но за исключением аномалий, которые детально исследовал Джефф Хьюстон в своей статье «В Интернете каждый соединен с каждым – верно?», этот исход в значительной степени удовлетворяет потребности рынка, его участников и пользователей Интернета.

Движущими силами достижения этого результата являются две основные формы взаимодействия между сетями — пиринг и транзит. Пиринг подразумевает общение на равных и в большинстве случаев означает обмен трафиком между сетями участников на безвозмездной основе. Транзит обеспечивает то, что сети не смогли достичь путем пиринга – глобальную связность каждого с каждым. И за это приходится, как правило, платить.

Однако похоже, что структура Интернета меняется, и все больше связности, и главное – важной связности, можно обеспечить пирингом. В первую очередь, это связано с консолидацией провайдеров контента и облачных услуг и их желанием находиться как можно ближе к потребителю. Посредничество провайдеров транзита становится менее необходимым. Это хорошая новость для точек обмена трафиком IXP, но и им не стоит забывать, что они сами являются посредниками. Эту эволюцию Сети анализирует в статье «Смерть транзита» Джефф Хьюстон.

О том, как развивался пиринг в России, так сказать, историческую перспективу его эволюции предлагает в своей статье технический директор MSK-IX Александр Ильин.

Не обошли мы вниманием такие важные аспекты пиринга, как оптимизация – от его технической оптимизации до оптимизации правового регулирования.

Этим номером журнала мы открываем новую рубрику «Новости интернет-индустрии» с выборкой интересных событий отрасли. Изначальный акцент на доменную индустрию, но в дальнейшем мы планируем включить и другие аспекты.

Наконец, по многочисленным просьбам читателей, мы ввели некоторые технологические усовершенствования и начиная с этого номера будем также предоставлять журнал в формате EPUB. Так что читайте на здоровье на планшетах и смартфонах!

Как всегда, нам очень интересно и важно знать ваше мнение. Что понравилось и что можно улучшить? Какие темы вы хотели бы увидеть в следующих выпусках?

Пишите нам по адресу info@internetinside.ru.

Смерть транзита?

Джефф Хьюстон (Geoff Huston)

На недавнем совещании NANOG я был поражен, как мало презентаций было посвящено интернет-сервис-провайдерам (ISP) и проблемам, связанным с их работой, и одновременно – как много было презентаций, рассматривающих различные аспекты дата-центров. Если судить по темам разговоров в кулуарах, сегодня в этой области доминируют вопросы проектирования дата-центров и эксплуатации сетей дистрибуции контента (Content Distribution Network, CDN). А функция ISP, в особенности транзитных ISP, как будто сокращается. Сейчас мы уже не предоставляем пользователю доступ к контенту, а доставляем контент пользователю. Значит ли это, что роль транзита для пользователей Интернета отмерла? Посмотрим на этот вопрос повнимательнее.

Интернет состоит из многих десятков тысяч отдельных сетей, каждая из которых выполняет определенную роль. Если за основу брать систему маршрутизации Интернета, то в ней примерно 55400 дискретных сетей (или «автономных систем», как называют их в маршрутизации). Большинство этих сетей находится на периферии и практически не осуществляет услугу транзитной передачи пакетов в другие сети, таких сетей сейчас около 47700. Оставшиеся 7700 сетей функционируют немного в другом качестве. Они не только анонсируют набор собственных адресов в Интернет, но и транслируют анонсы других сетей – иными словами, выполняют роль «транзитного» провайдера.

Почему это различие было так важно в прошлом? Что такого особенного в «транзите»?

В значительной мере этот вопрос был связан с финансовыми расчетами между провайдерами. Во многих областях деятельности, если предоставление той или иной услуги потребителю требует усилий нескольких поставщиков, часто встречается следующая система: тот поставщик, который получает от заказчика деньги, оплачивает остальным их вклад в предоставление услуги. Вроде бы звучит логично и правильно, но Интернет не очень приспособлен для таких соглашений. Нет четкой модели того, какими могут быть «компоненты услуг», нет и общепринятого соглашения о том, как вести учет услуг согласованно с любыми финансовыми расчетами между провайдерами. В общем и целом, Интернет отверг такие соглашения и принял более простую модель, основанную всего на двух типах соединений. В модели соединений один поставщик стано-

Рис. 1. Модель «поставщик-потребитель» и пиринговая модель в мире ISP.

вится поставщиком другого, который становится потребителем, и потребитель оплачивает услугу поставщику. Во второй модели оба поставщика оказываются примерно в эквивалентном положении, и в этом случае они могут найти взаимоприемлемый выход в том, чтобы обмениваться трафиком бесплатно (т.н. пиринг, см. рис. 1).

В этой среде выяснить, кто чей поставщик и кто чей потребитель, иногда бывает затруднительно. Не менее сложно бывает установить, выгодны ли вам пиринговые отношения с другим поставщиком или нет. Но существует один критерий, который, казалось бы, самоочевиден: провайдеры доступа платят транзитным провайдерам за трафик. Результатом повсеместного применения такого подхода стал целый набор «уровней», где игроки, занимающие один уровень, как правило, взаимодействовали по пиринговой системе, в то время как при взаимодействии разных уровней нижележащая сеть становилась потребителем, а верхняя – поставщиком. Уровни эти не были формально определены, и «включение» в состав уровня тоже не было однозначным. Можно сказать, что, по сути, эта многоуровневая модель отражала результат процесса переговоров, согласно которому место каждого ISP определялось, главным образом, тем, с кем он находился в равных отношениях, для кого был поставщиком, а для кого потребителем.

Понятно к чему это привело: наверху этой иерархии оказались доминирующие поставщики услуг транзита. Занимающие верхний уровень так называемые интернет-провайдеры первого уровня (Tier One) образовали неформальную олигархию Интернета.

Чтобы понять, почему транзит так важен, достаточно взглянуть на отдаленные уголки земного шара, где стоимость доступа в Интернет – это по большей части стоимость транзита. Примерно десятилетие назад в Австралии около 75% всех данных, передававшихся конечным пользователям, пересекали Тихий океан, и оплачивали это удовольствие австралийские ISP. В результате стоимость доступа в Интернет для конечных пользователей была очень высока, практиковались ограничения трафика и всевозможные ухищрения по локальному кэшированию данных.

Даже на тех рынках, где стоимость транзита не настолько доминировала, существовало четкое различие между уровнями, а позиция каждого конкретного ISP на одном и том же рынке определялась совокупностью инфраструктурных активов, общего числа прямых и косвенных абонентов (т.е. совокупной доли рынка) и способностей переговорщиков. Но даже на таких рынках транзит имел большое значение в плане инфраструктурных активов, включая размер и охват. Например, региональному или местному ISP стоило бы гигантских усилий договориться о пиринге с провайдером национального уровня.

Но это было в давние времена, а сейчас в этой модели Интернета многое изменилось. Первоначальная модель Интернета была построена на функции передачи (carriage function), и ее ролью была передача трафика от клиента к серверу и обратно, где бы этот сервер ни находился. Тут можно даже согласиться с сенатором Тедом Стивенсом (Ted Stevens, престарелый американский сенатор, «прославившийся» в 2006 г. сказанными с трибуны Сената фразами типа «мне тут прислали Интернет» и «Интернет – это не большой грузовик, это серия труб, и они могут засориться». Множество фраз из той эпохальной речи стало мемами – перев.): такая модель Интернета действительно «серия труб». Сервисы населяли

Рис. 2. Уровни в среде ISP.

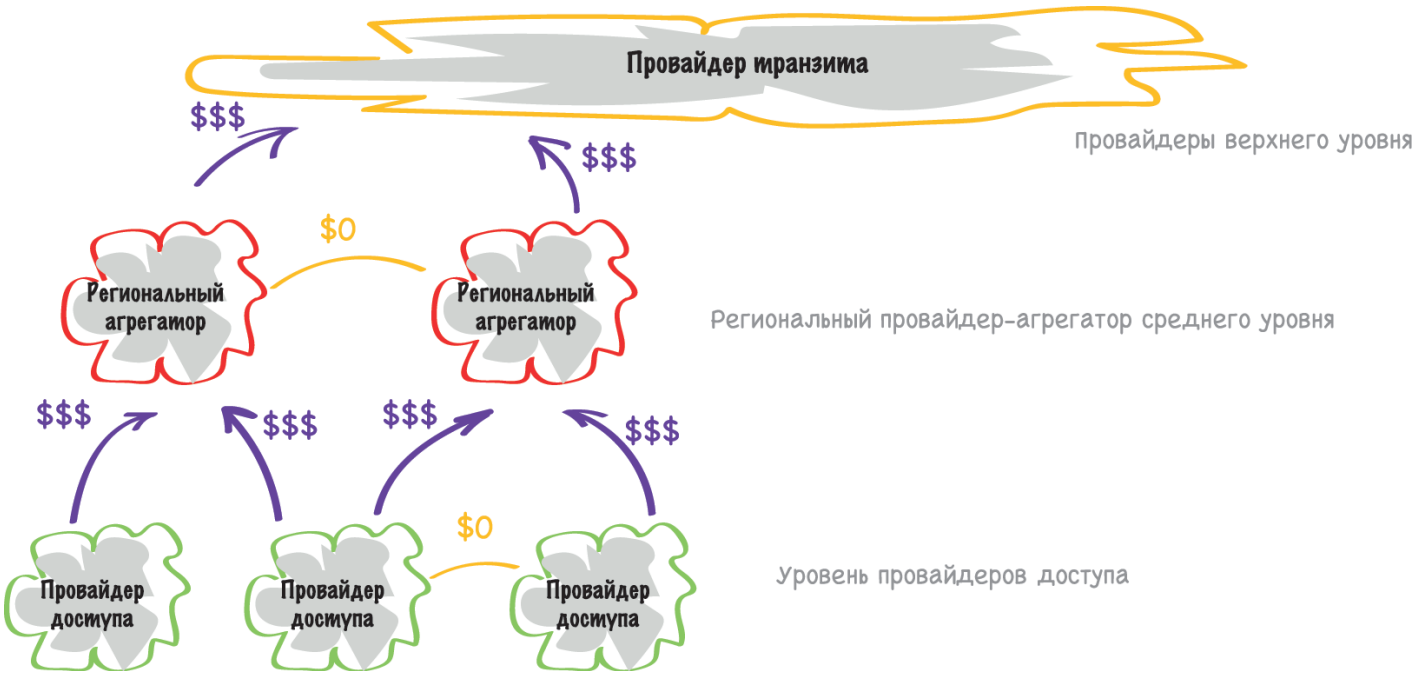
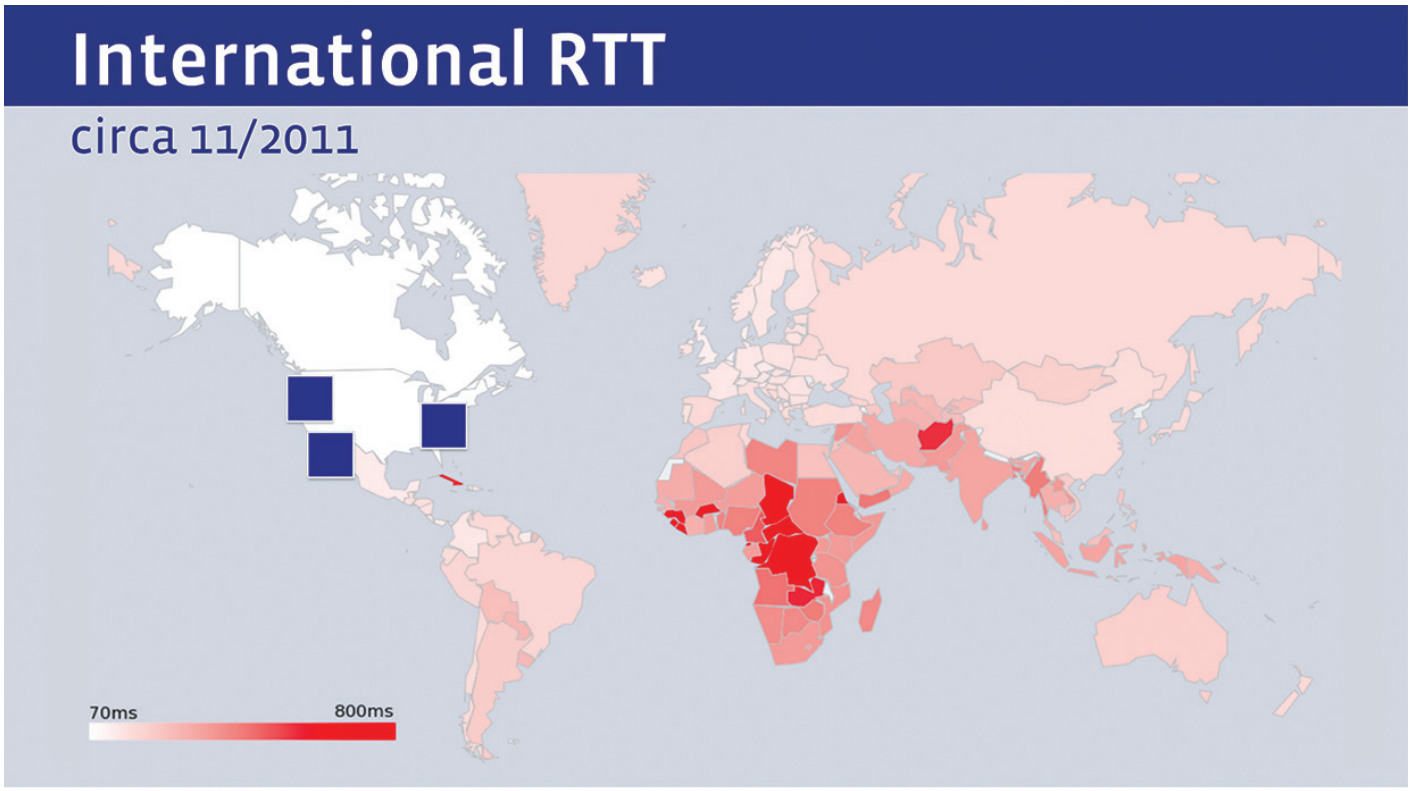


Рис. 3. Быстродействие сервисов в Интернете, ок. 2011 г.



край сети, а сеть была единообразно способна соединять пользователя с сервисами, где бы они ни находились. Но не стоит путать способность с быстродействием. Хотя эта модель позволяла любому пользователю подключиться к любому сервису, маршруты передачи в Интернете для разных пользователей при обращении к одному и тому же сервису могли радикально отличаться. Часто это приводило к аномалиям быстродействия: чем дальше пользователь находился от контента, тем медленнее была услуга. Возьмем, например, следующий слайд, взятый из презентации на Facebook для NANOG 68 (рис. 3).

Участки, обслуживаемые геостационарными спутниками, и особо удаленные регионы (в плане километража проводки) демонстрируют огромные значения круговой задержки (RTT) при обмене данными между пользователем и точкой предоставления услуги. Разумеется, эта RTT – еще не все. Добавим сюда еще и длительную транзакцию DNS, потом установку сеанса TCP, а потом, возможно, и рукопожатие TLS, потом запрос транзакции, потом доставку запрошенного контента по TCP с медленным стартом – и получится, что для пользователя задержка составит не менее трех RTT, а зачастую и еще вдвое больше. То, что для пользователя, находящегося в одном городе с сервером, отняло бы десятую долю секунды, в отдаленном районе превращается в 6 секунд. Такие задержки не всегда вызваны плохим выбором маршрута в системе маршрутизации Интернета или плохой связностью физической сети, хотя то и другое вносит в них ощутимый вклад. В значительной мере проблема обусловлена такими физическими банальностями, как скорость света и размеры Земли. Отправка пакета на геостационарный спутник и возврат его на Землю занимает треть секунды. Задержка при обмене данными со спутником определяется скоростью света и высотой геостационарной орбиты. Подводный кабель быстрее, но ненамного. В оптоволоконном кабеле сигнал распространяется со скоростью, равной 2/3 скорости света, поэтому сигнал идет через Тихий океан и обратно за 160 миллисекунд. Поэтому в определенном плане есть границы того, чего можно достичь, пытаясь организовать оптимальную топологию для Интернета, а потом варианты будут исчерпаны – конечно, если не ждать, пока континентальный дрейф не подгонит материки друг к другу! Если вам действительно нужно повысить быстродействие своего сервиса, то, очевидно, следующим шагом будет полный отказ от транзита – разместите копию контента ближе к пользователю.

Именно это сегодня и происходит. Сегодня мы видим проекты по прокладке подводных кабелей для того, чтобы связать между собой дата-центры крупнейших провайдеров, вместо того, чтобы гонять пользовательский трафик в удаленные дата-центры. Компания Google всерьез занялась приобретением доли в подводных кабелях в 2008 году и сейчас участвует в шести таких кабелях (в качестве иллюстрации приведем вырезку из недавнего объявления о прокладке нового кабеля: рис. 4).

Как пишет Wired, Тим Стронг (Tim Stronge), вице-президент TeleGeography, заявляет, что прокладка нового кабеля – продолжение нынешнего тренда. «У крупных поставщиков контента гигантские и часто непредсказуемые требования к трафику, особенно в собственных дата-центрах, – говорит он. – Их потребности столь велики, что на самых крупных маршрутах им выгоднее строить свое, чем платить

за чужое. Владение подводными оптоволоконными кабелями также дает им достаточную гибкость для того, чтобы наращивать мощности по потребностям, а не зависеть от эксплуатантов подводного кабеля» (http://www.wired.co.uk/article/google-facebook-plcn-internet-cable).

Смена парадигмы в способе доступа к контенту также влечет за собой смену ролей в различных точках обмена интернет-трафиком. Первоначальным мотивом для организации точек обмена было то, что группа местных провайдеров доступа заключала соглашение о прямом пиринге. Благодаря этому можно было не платить провайдерам транзита, а до тех пор, пока имелась значительная пропорция обмена местным трафиком, точки обмена закрывали реальную потребность, заменяя часть роли транзитного провайдера местной коммутацией. Однако операторы обмена быстро поняли, что если добавить к точке обмена еще и услуги дата-центра, то участники ощутят рост пользовательского трафика на точке обмена, а следовательно, повысится ее относительная значимость.

Существует еще один фактор, который выдавливает контент и сервисы в специализированные системы доставки контента, - это угроза злонамеренной атаки. Индивидуальные участники рынка, особенно те, для кого предоставление онлайн-сервисов не является основным бизнесом, с трудом могут инвестировать в инфраструктуру и квалифицированный персонал для того, чтобы противостоять атакам отказа в обслуживании (Denial of Service, DoS). Такое желание повысить устойчивость сервисов перед лицом атаки, вместе с потребностью пользователей в быстром доступе, приводит к потребности в своего рода аникаст-услуге, которая бы распределяла сервисы по многочисленным точкам доступа, близким к различным группам пользователей. Неудивительно, что дистрибуторы контента, такие как Akamai, Cloudflare и многие другие, столкнулись с таким высоким спросом на свои услуги.

Так если контент перемещается в дата-центры, а мы размещаем эти центры как можно ближе к пользователям, что это означает для транзитных ISP?

Ничего хорошего, и, хотя я, возможно, рано бью тревогу, мне кажется, что новых проектов по прокладке магистральных кабелей, финансируемых транзитными ISP, не будет, по крайней мере, сейчас. На многих развитых потребительских рынках Интернета просто нет потребности в столь массовом доступе конечных пользователей к удаленным сервисам. Вместо этого поставщики контента перемещают свой основной контент как можно ближе к потребителю, и ведущую роль в финансировании дальнейшего развития магистральной инфраструктуры Интернета берут на себя системы дистрибуции контента. Для пользователя это означает повышение быстродействия и, возможно, снижение цен, особенно если учесть исчезновение ценового компонента транзитной передачи. Потребность в дальней транзитной инфраструктуре никуда не делась, но сейчас основная масса этой потребности приходится на поставщиков контента, а пользовательский компонент становится эзотерической нишевой активностью, которая выходит за пределы мэйнстримовой передачи данных.

В результате изменяется и общая архитектура Интернета. Из плоской полносвязной сети начала 90-х годов, где каждый мог подключиться к каждому и все были равноправны, мы в значительной степени превратили Интернет в клиент-серверную систему, в которой большая часть данных передается между клиентами

Рис. 4. Объявление о прокладке кабеля CDN-провайдером.

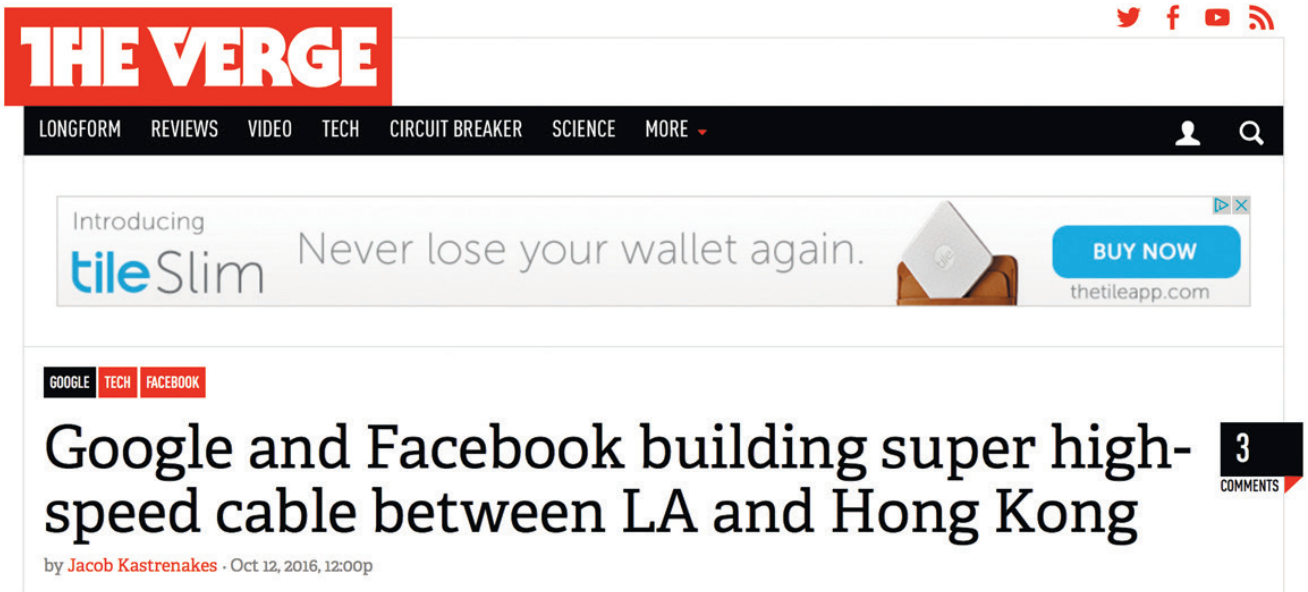
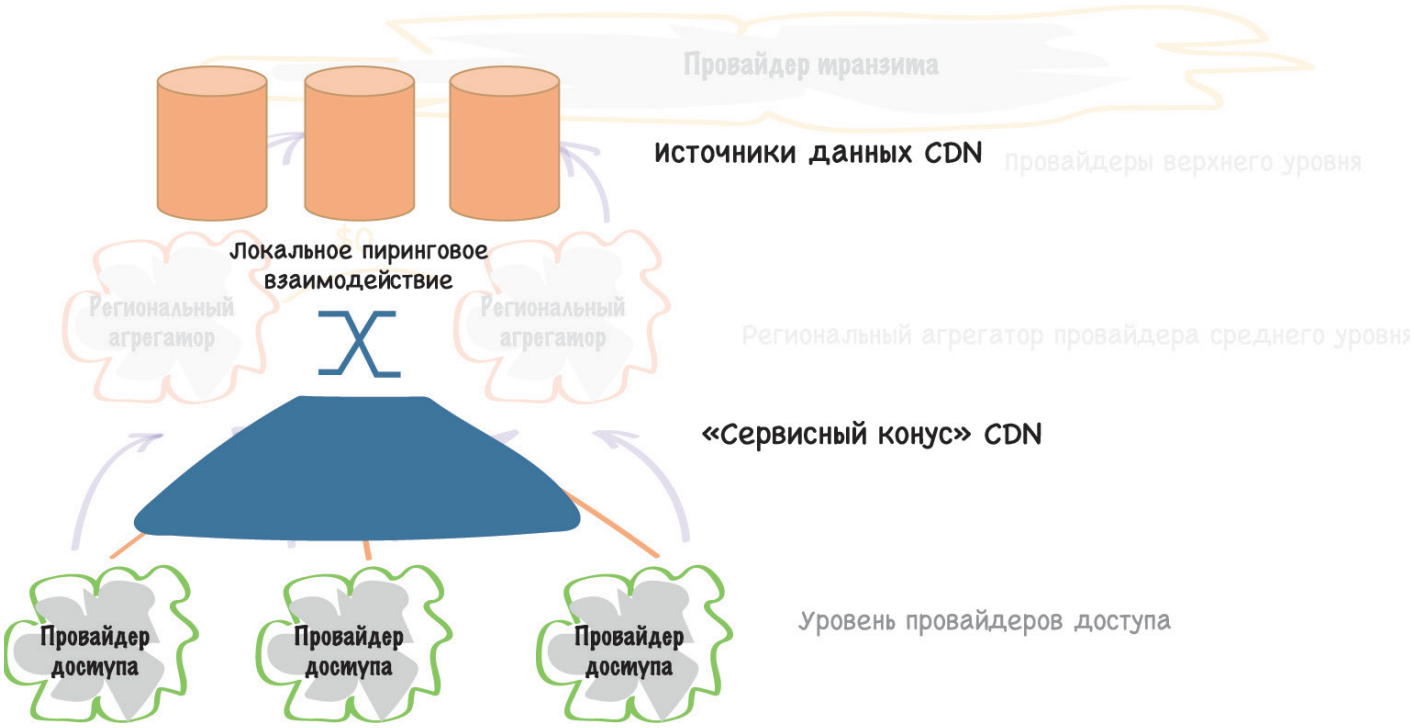


Рис. 5. «Сервисные конусы» CDN.



и серверами, а трафик «клиент-клиент» практически исчез. Этому во многом содействовали устройства NAT (Network Address Translation), фактически скрывая клиентов до тех пор, пока те не инициировали соединение с сервером. Возможно, именно из-за NAT опустошение пула адресов IPv4 не стало катастрофой, как мы тогда ожидали. К тому моменту, когда новых адресов практически не осталось, мы во многом отошли от пиринговой модели сетевых соединений, а основанная на NAT модель сетей доступа была полностью совместима с клиент-серверной. Когда мы начали крупномасштабно развертывать NAT, клиент-серверная модель доступа уже закрепилась, и два подхода прекрасно дополнили друг друга.

Возможно, что сейчас мы дробим клиент-серверную модель на более мелкие кусочки, фактически загоняя каждого клиента в сервисные «конусы», определяемые группой местных дата-центров (рис. 5).

Если мир интернет-сервисов действительно определяется небольшой группой CDN-провайдеров, таких как Google, Facebook, Amazon, Akamai, Microsoft, Apple, Netflix, Cloudflare и еще парочка других, а все остальные поставщики услуг, по сути, просто помещают свои услуги в эти большие облака контента, то зачем нам вообще нужно выталкивать клиентский трафик в далекие дата-центры? Какова оставшаяся потребность в транзите на дальние расстояния? Есть ли вообще будущее у провайдеров транзита?

Возможно, я бью тревогу преждевременно – перефразируя Марка Твена, можно сказать, что слухи о смерти транзитных ISP сильно преувеличены. Но не следует забывать, что на свете не существует никаких правовых норм, которые гарантировали бы полную связность Интернета, и никаких правовых требований, которые бы навязывали Интернету какую-то одну определенную сервисную модель. В мире частных инвестиций и частнопредпринимательской деятельности нередко бывает, что провайдеры решают те проблемы, которые считают нужным решать, и делают это так, как им нравится, игнорируя то, что кажется им обузой – а поскольку их время и силы конечны, они игнорируют то, что не приносит им прибыли. Поэтому, хотя «всемирный охват» и «полная связность соединений» и имели большой смысл в старом, регулируемом госструктурами мире телефонной связи (и в явном социальном договоре, который лег в основу этой системы), для Интернета такие концепции социальных обязательств неважны. Если пользователи не ценят что-то настолько, что готовы за это платить, то у провайдеров нет стимула предоставлять это «что-то»!

Если транзит становится малопопулярной и редко используемой услугой, то можно ли представить себе архитектуру Интернета вообще без транзита? Вполне можно представить себе эволюцию Интернета в набор пользовательских «конусов», отходящих от местных точек дистрибуции данных, а для передачи или синхронизации данных между центрами можно выбрать и совершенно другие механизмы. Единый Интернет превратится в распределенную структуру, очень похожую на сегодняшние клиент-серверные среды, но с неким уровнем неявной сегментации между различными «облаками» сервисов. Да, я сейчас весьма утрирую, но все равно такая картина не выходит за пределы возможного.

Если же такая структура станет реальностью, то будет ли вообще

какой-то смысл сохранять единое адресное пространство во всемирном масштабе? Если все потоки трафика ограничены каждый своим сервисным конусом, то оставшаяся потребность в адресации в лучшем случае выродится в потребность уникальных идентификаторов для конечных точек конусов, а уникальностью в масштабе всей сети (что бы выражение «вся сеть» ни значило в подобной системе) можно и пожертвовать. Если кто-то еще помнит работу IETF над региональными IP (RSIP – Realm-Specific IP, RFC 3102), они поймут, что я имею в виду.

Но такое будущее, если оно вообще наступит, наступит как минимум через несколько лет.

Сегодня все, что мы наблюдаем, – это дальнейшие изменения в непрекращающихся трениях между передачей и контентом. Мы видим постепенный отход от модели, в которой инвестиции делаются, главным образом, в передачу (в которой пользователя «перемещают» к двери «бункера» с контентом). Ее заменяет модель, которая перемещает копию контента поближе к пользователю, обходя значительную часть старой функции передачи. Иными словами, сейчас похоже, что контент на подъеме, а передача и те, кто ею занимается – особенно в части дальнего транзита, – столкнулись с падением ценности своих услуг для клиентов.

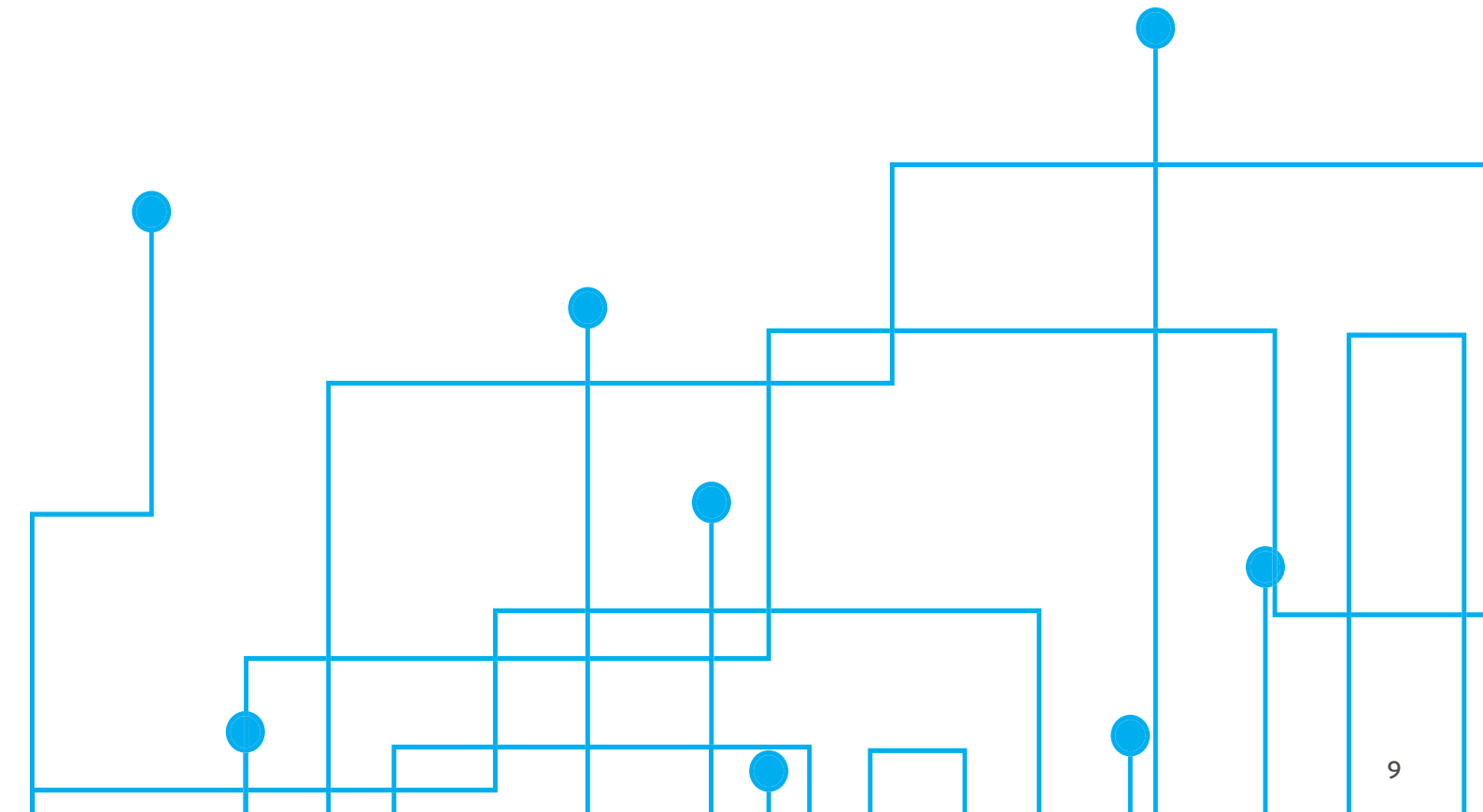
Но эта новая модель поднимает также ряд интересных вопросов об однородности Интернета. Не все сервисы одинаковы, и не весь контент доставляется одинаково. CDN вполне может по своему усмотрению выбирать язык для пользователей или соблюдать региональные лицензии на контент. Например, у Netflix разные каталоги для разных стран. Сервис в разных частях света получается неодинаковым. На более общем уровне мы видим определенный уровень сегментации, или фрагментации, архитектуры Интернета в результате специализации доставки сервисов. В такой среде, сегментированной на практически самозамкнутые сервисные конусы, какая рыночная движущая сила заставит реализовать все мыслимые сервисы в каждой точке их дистрибуции? И кто заплатит за такие излишества? А если никто не готов поддерживать эту модель «универсального» контента, то насколько разным будет «Интернет» в зависимости от того, где вы находитесь? Будут ли везде доступны все доменные имена, будут ли они правильно преобразовываться в такой сегментированной среде? Очевидно, мысли о кастомизации локальных сервисов в каждом регионе быстро скатываются на путь к страшилкам о «распаде Интернета на несвязанные кусочки», поэтому, пожалуй, здесь стоит остановиться и оставить открытыми вопросы, которые могут возникнуть вследствие возможного упадка транзита и бума контент-сетей.

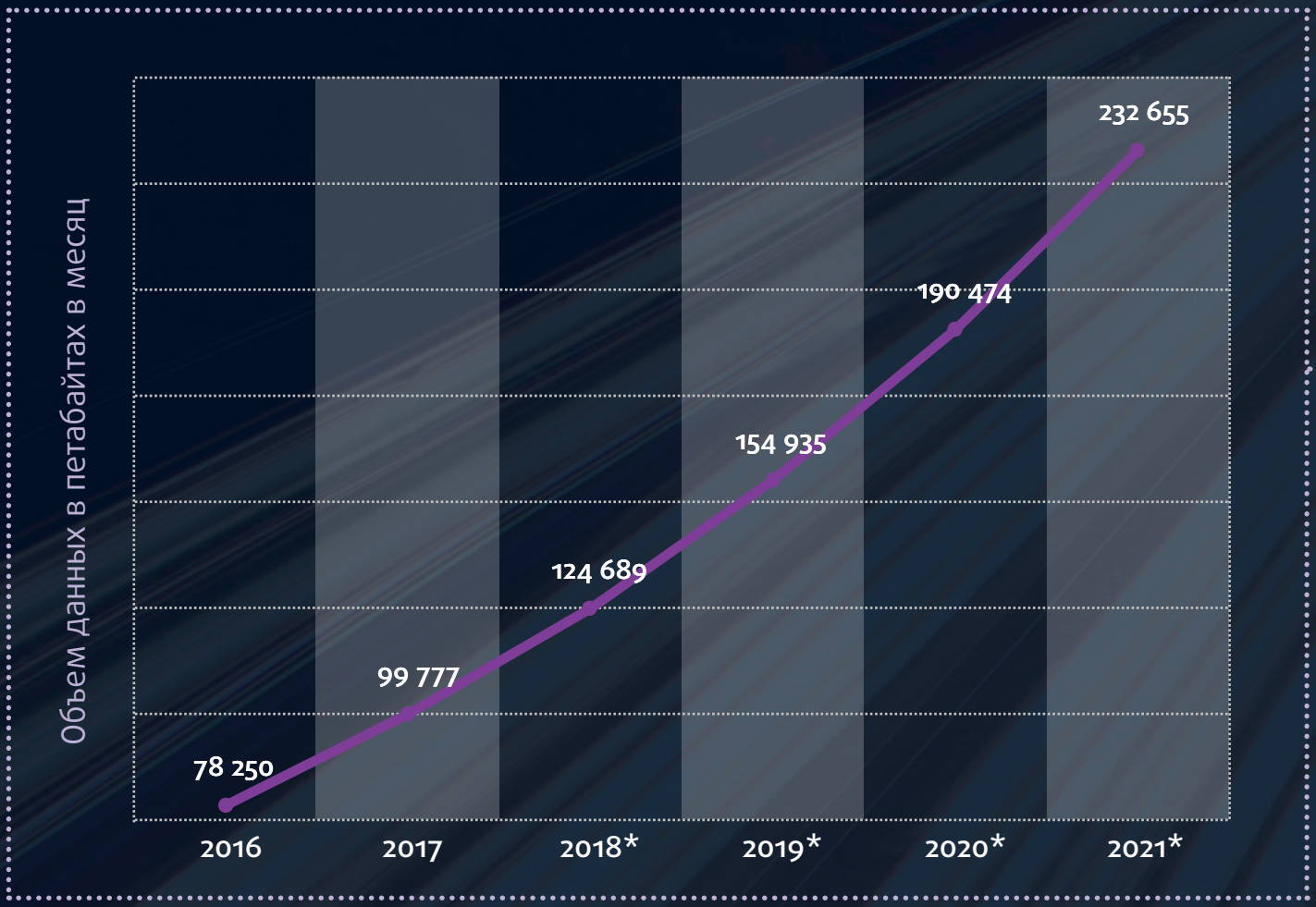
Сколько продержится эта модель, никому не ведомо. Вполне возможно, это лишь переходная фаза, а сегодняшний упор на дата-центры – только отражение нынешней ситуации, а не тенденции. Так что, быть может, еще не пора совсем отказываться от традиционных принципов универсальной связности и транзитных сервисов, хотя сейчас похоже, что Интернет делает очень большой шаг в этом направлении!

Оговорка

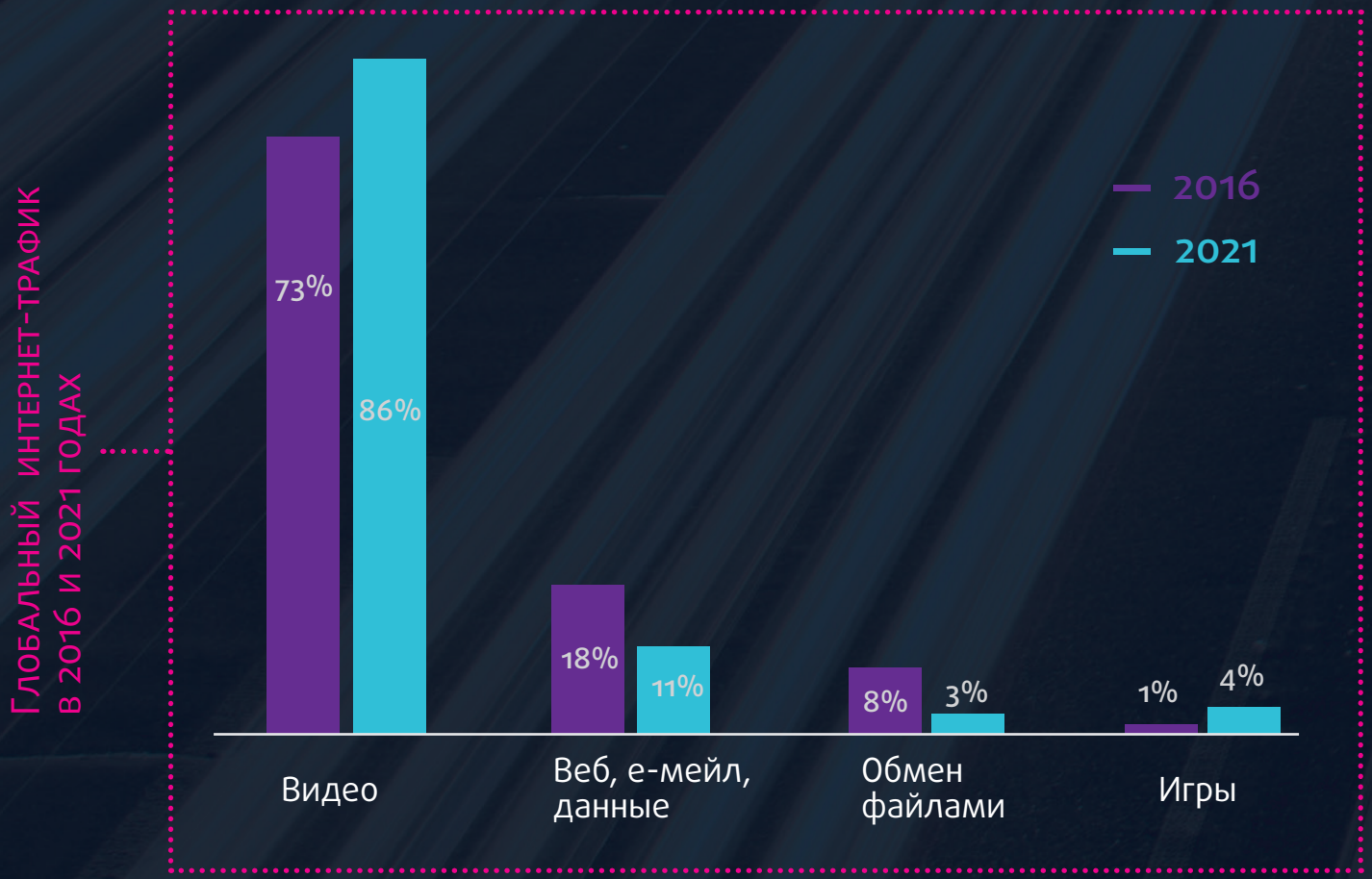
Изложенные выше воззрения могут не совпадать с позицией Asia Pacific Network Information Centre.

Источник: The Death of Transit?, www.potaroo.net/ispcol/2016-10/xtransit.html





Источник:
TeleGeography, https://www.theatlas.com/charts/HJV4pWDz-

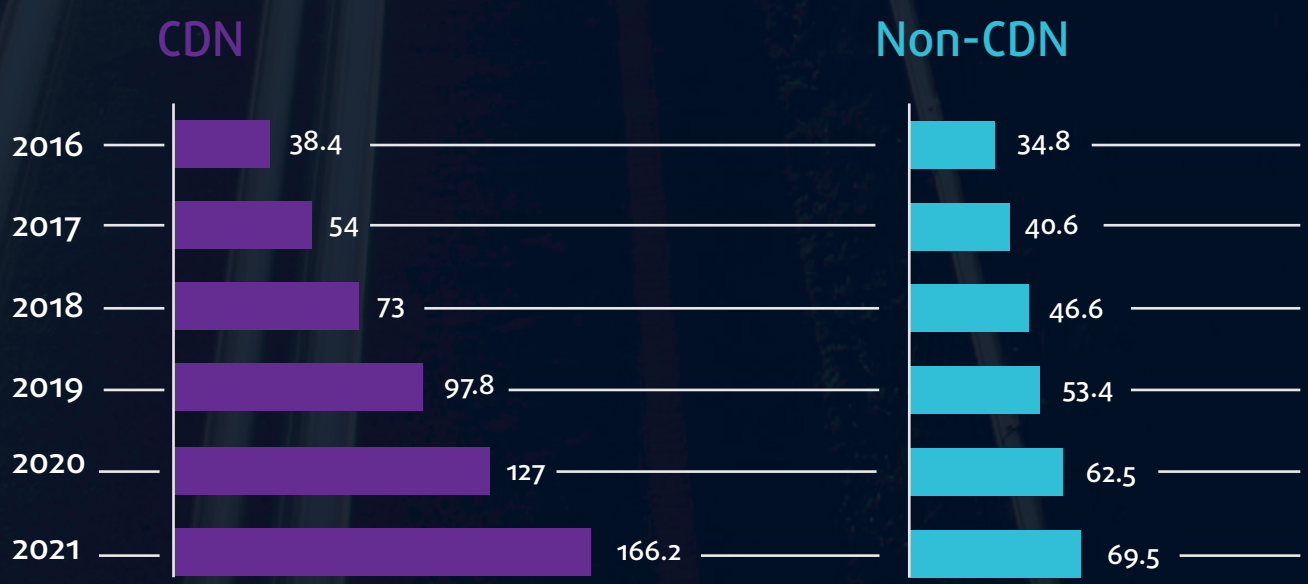


ОБЪЕМ ДАННЫХ ГЛОБАЛЬНОГО ПОТРЕБИТЕЛЬСКОГО IP-ТРАФИКА С 2015 ДО 2021 (В ПЕТАБАЙТАХ В МЕСЯЦ)

График показывает прогноз роста объема данных международного IP-трафика до 2021. В 2021 глобальное потребление IP-трафика, как ожидают, достигнет 232 655 петабайтов при 24-процентном среднегодовом темпе роста.

Источник:
Statista, https://www.statista.com/statistics/267202/global-data-volume-of-consumer-ip-traffic/

БОЛЬШАЯ ЧАСТЬ ИНТЕРНЕТ-ТРАФИКА БУДЕТ ПЕРЕДАВАТЬСЯ ПО СЕТЯМ ДОСТАВКИ КОНТЕНТА (CDNS) (В ЭКСАБАЙТАХ)



Источник:
TeleGeography, https://www.theatlas.com/charts/S1kIUTIMW

Эволюция пиринга

Александр Ильин

Интернет развивается органически. Не существует общего плана развития Сети, центрального управляющего пункта. Даже протоколы, используемые в Интернете, не являются обязательными, а лишь итогом консенсуса, достигнутого техническим сообществом. В Интернете отсутствует сквозная гарантия качества и маршрута, по которому будет передаваться трафик из точки А в точку Б. И тем не менее, Интернет обеспечивает глобальную связность, открывая все новые возможности и приложения. В основе этого чуда лежит взаимодействие между независимыми операторами по обмену трафиком – так называемый пиринг. О его прошлом, настоящем и будущем я поговорю в этой статье.

Интернет развивается органически. Не существует общего плана развития Сети, центрального управляющего пункта. Даже протоколы, используемые в Интернете, не являются обязательными, а лишь итогом консенсуса, достигнутого техническим сообществом. В Интернете отсутствует сквозная гарантия качества и маршрута, по которому будет передаваться трафик из точки А в точку Б. И тем не менее, Интернет обеспечивает глобальную связность, открывая все новые возможности и приложения. В основе этого чуда лежит взаимодействие между независимыми операторами по обмену трафиком – так называемый пиринг. О его прошлом, настоящем и будущем я поговорю в этой статье.

Немного истории

Предоставление возможности пирингового взаимодействия на Московской точке обмена трафиком появилось как альтернатива дорогому и неэффективному (на тот момент) IP-транзиту. В начале 1990-х международный транзит практически отсутствовал. У крупнейших на то время сетей «Релкома» и «Демоса», например, это были каналы, не превышающие 1 Мбит/с. Рост трафика и желание максимально сократить издержки дали толчок к появлению точки обмена трафиком. При этом было крайне важно определить нейтральную организационную структуру для управления этой точкой, чтобы были максимально учтены интересы всех участников, подписавших первое соглашение о точке обмена трафиком. Таким связующим звеном коллегиально выбрали Российский НИИ развития общественных сетей (РосНИИРОС), и уже в 1995 году был установлен первый коммутатор в Москве на площадке ММТС-9 (М9), способный «переварить» стыки с операторами на скоростях 10 Мбит/с. По тем временам это казалось более чем достаточно. Однако с момента появления точки обмена трафиком стало ясно, что организация качественного межоператорского обмена является прежде всего технической задачей. Поначалу это даже выглядело как закрытый клуб по интересам (некоторые международные точки обмена трафиком до сих пор сохраняют похожую модель), ведь чтобы попасть на точку обмена трафиком, было важно не только наличие автономной системы, но и рекомендации как минимум трех участников на вступление нового члена «клуба». Поскольку решение принималось, как правило, на уровне технического директора компании, то по замыслу организаторов, это должно было обеспечить отбор только тех участников, которые имели достаточно высокую техническую квалификацию.

Одновременно с развитием взаимного обмена трафиком велась работа по активному поиску оптимальный среды передачи данных. С этой целью применялись самые разнообразные технологии. Например, в некоторых городах обмен трафиком обеспечивался на основе технологии Frame-Relay, а в Москве помимо устоявшегося Ethernet пытались применить даже решение на базе теперь уже подзабытого ATM (Asynchronous Transfer Mode).

«Клуб» рос и развивался, первых участников было так немного, что они знали друг друга буквально поименно и никому не составляло особого труда настроить пиринг между своими сетями. Однако с появлением каждого нового игрока на арене площадки обмена трафиком становилось понятно, что сложность настройки растет, да и вероятность ошибки тоже. Список участников существенно вырос и входить в «клуб» для новых игроков становилось все проще, поэтому правило трех рекомендаций вскоре отменили совсем. Однако технически становилось понятно, что простого межоператорского взаимодействия уже мало, нужно было быстрее вырабатывать правила и систематизировать эту систему. В то время отличие нашей Московской точки обмена трафиком от соответствующих международных систем было существенным. Международная сеть была построена на основе крупных мировых операторов, так называемых Tier1 (https://ru.wikipedia.org/wiki/Tier-1-операторы), предоставляющих глобальную связность, что существенно отличалось от России, где на тот момент этих операторов не было. У нас росло количество небольших и средних сетей, которые хотели сэкономить на международной канальной емкости и активно вступали в

«клуб» MSK-IX, в то время как в Европе крупнейшие точки росли на основе консолидации трафика, а не по количеству участников.

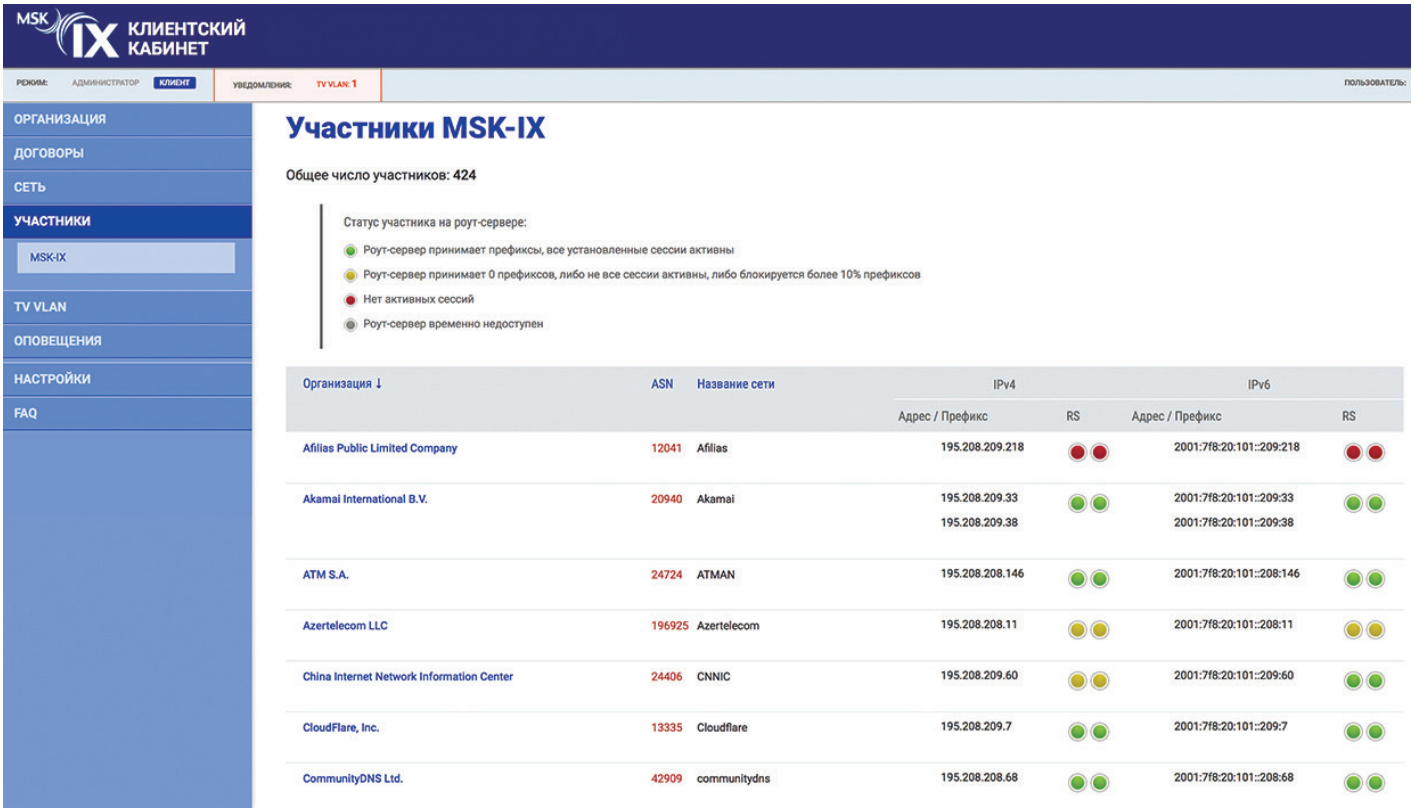
Сервер маршрутов

Разные подходы к формированию точек обмена порождали разные технические требования и методы решения задач. В частности, на MSK-IX появился инструмент Сервер маршрутов (Route Server) - одна из самых первых реализаций среди точек обмена трафиком. Основной его задачей на этапе запуска было минимизировать количество пиринговых попарных взаимодействий «каждый с каждым» и упростить настройки маршрутизации между всеми участниками. Эта система позволяла передавать маршруты с применением транзитного звена – «арбитра», в то время как основной трафик продолжал передаваться напрямую между участниками. Это существенно сократило сроки переконфигурации при любых изменениях состава участников в точке обмена и позволило быстро включаться новым сетям, ведь теперь не нужно было разыскивать всех своих коллег по пирингу и вести переговоры с каждым из них в отдельности.

Отметим, что модель Route Server оказалась настолько эффективна, что в какой-то момент она стала играть решающую роль в пиринговом обмене. Безусловно, требования к ее надежности были очень высоки, поэтому нами было запущено сразу два таких устройства в разных ЦОДах. С каждым годом по мере развития новых сетей все больше игроков рынка осознавали необходимость резервирования инфраструктуры. В то время активно появлялись запросы на создание резервных стыков с IX. Это было обусловлено сравнительно более низкой надежностью линий связи в отличие от оборудования, а кроме того, маршрутизаторы стоили немалых денег и, пытаясь сэкономить, участники MSK-IX старались зарезервировать хотя бы линии связи. Это привело тогда к очередной насущной технической задаче - необходимости выделения второй IP-сети на платформе IX, ведь один маршрутизатор участника не позволял сделать сразу два стыка с единым пространством MSK-IX (нельзя было применить IP-адреса из одной сети на разных портах маршрутизатора). Особую роль в развитии услуг резервирования в то время сыграл также знаменитый Московский «блэкаут» (25 мая 2005 года)(https://ru.wikipedia.org/wiki/Авария_в_энергосистеме_в_Москве_(2005)), обесточивший половину Москвы, когда частичная связность сохранилась только для тех сетей-участников MSK-IX, кто своевременно озаботился соответствующим резервом.

Существующая на тот момент модель системы Route Server добавляла свою автономную систему в маршрут BGP и со временем стала казаться не очень удобной. Участникам уже было недостаточно просто установить обмен маршрутами, но и хотелось видеть максимально короткий маршрут до своего соседа, исключив необходимость в прямых пирингах. Вообще борьба за «лучший» маршрут развернулась нешуточная, каждая сеть хотела развернуть трафик клиентов именно на себя и оттянуть тем самым трафик от других участников. В таких условиях формулировались и развивались наши правила и технические требования услуги. Совместно с разработчиками нам удалось модернизировать систему Route Server и научиться убирать «лишнюю» автономную систему из пути маршрутизации. Route Server по сути стал прозрачным, что позволило нам выйти на новый уровень взаимодействия,

Рис. 1. Система светофора, применяемая в MSK-IX.



создав для участников полную иллюзию прямого стыка друг с другом. Route Server уже полноценно работал в роли арбитра, помогая не только наладить пиринг, но и отслеживал и блокировал возможные ошибки в построении фильтров операторов (проверяя корректность маршрутов по IRR базам данных). Тут, кстати, тоже было наше отличие от зарубежных точек обмена трафиком. Там Route Server появился как вспомогательный инструмент и отдавал все маршруты, которые ему транслировали участники, без фильтрации, «as is». К сожалению, весьма распространенной была картина, когда администратор сети недолго думая настраивал BGP по базовой литературе (одной из самых лучших книг по протоколу BGP была книга Sam Halabi, Internet Routing Architectures (https://www.amazon.com/Internet-Routing-Architectures-2nd-Halabi/dp/157870233X), максимально просто и без фильтров. Это приводило к взаимной передаче маршрутов от одного участника другому, и лишь бдительное «око» Route Server позволяло отловить подобную ситуацию еще на самом раннем этапе, что помогло нам с годами и набранным опытом выработать доверие к этому инструменту.

Кто бросил валенок на пульт?

Однако одним лишь сервером маршрутов вопросы пиринга не ограничивались, и перед нами регулярно вставали новые интересные задачи. С ростом количества участников наша платформа все больше выступала в роли агрессивной среды передачи данных. Это было обусловлено тем, что обмен трафиком осуществлялся в одной IP-сети, где каждый участник подключался своим оборудованием, зачастую со своими настройками и нестандартными параметрами. Нам требовались новые подходы к контролю нежелательного трафика с целью поддержания стабильности.

С точки зрения производителей (вендоров) оборудования, мы представляли нечто среднее между ЦОДом и корпоративной сетью со множеством участников. Следует отметить, что яркое отличие IX от других проектов заключается в том, что до конца неизвестно, что прячется за портом участника. Это может быть как порт роутера, так и целая сетевая инфраструктура с разнородным оборудованием. Действия одного участника могли в мгновение разрушить пиринг на всей сети. Сеть стала попадать под «штормы», которые порождались самими участниками. Ряд нарушений касался и самой IP-сети IX, которую нельзя анонсировать «в мир». Знаменитая шутка тех лет – «Кто сегодня бросил валенок на пульт?» – именно об этом нарушении.

Схожие задачи вставали и перед зарубежными крупнейшими точками обмена трафиком. Все это подталкивало сообщество к консолидации и обмену опытом. Возникла ассоциация Euro-IX, объединившая деятельность точек обмена трафиком и позволившая оперативно решать целый ряд совместных задач. В результате этой совместной активности, например, появился список требований к вендорам, и они обратили, наконец, внимание на точки обмена. Стали появляться различные механизмы защиты инфраструктуры, которые снимали растущее давление со стороны новых ошибок участников и защищали сеть.

Технологии пирингового обмена не стояли на месте. Участникам хотелось эффективнее управлять своими маршрутами для получения экономической выгоды. Начались различные пиринговые войны и разрывы пирингов, нацеленные на попытки заработать операторами, имеющими значимое присутствие на точке обмена. Появлялись и множились специфические задачи у контент-операторов, требовалась все большая гибкость управления маршрутами. Разработчики придумали, как строить индивидуальные BGP-таблицы Route Server для каждого участника с учетом его потребностей. Так появился полезный функционал MultiRIB для Route Server. Для управления таблицей весьма активно применялись управляющие BGP community. Стало ясно, что без возможности оперативного анализа таблиц работать неудобно, и появился инструмент Looking Glass. Теперь уже многое можно было увидеть быстро, оперативно. В случае проблем со связностью оператору успешно удавалось самому принимать решение. Свод наших технических правил продолжал пополняться на основе анализа очередных случаев из практики и опыта инженеров. С ростом количества сетей, участвующих в пиринге, росла и сложность возникающих ошибок. Например, мы сталкивались с блокировками части трафика на выдаваемые маршруты в сторону RS. Это приводило к «черным дырам» в прохождении трафика и негативно сказывалось на пиринге. Безусловно, инструменты, такие как BGP community, позволяли это исправлять, хотя зачастую требовалось немало времени для выяснения причин. Стандартные средства сетевой диагностики не позволяли быстро выявлять эти ошибки, поскольку они были специфичны для конкретной сети определенного оператора.

Рост числа участников стал также приводить к очень частым и типичным ошибкам, таким как «забывчивость» системных администраторов передавать маршруты в сторону IX и ошибками в настройках при смене оборудования. Мы продолжали искать способы выхода из этих ситуаций и повышения качества пиринга. В конечном итоге удалось реализовать целую систему контроля подобных ситуаций с уведомлениями клиентов. Была поставлена задача балансировать на разумном уровне количества уведомлений, чтобы, с одной стороны, не надоедать системным администраторам, а с другой, напомнить им о необходимости исправления ошибок. Таким образом, у нас появилась система уведомлений об ошибках сетевых администраторов, куда впоследствии добавились ошибки на линиях связи, проблемы с фильтрами и другие. Мы придумали весьма наглядную систему светофора (рис. 1). Каждый участник мог видеть не только свой статус подключения к Route Server, но и статус всех соседей по пирингу, причем в яркой наглядной форме («зеленый», «желтый», «красный»), что безусловно многим стало помогать при поиске истинных причин проблем пиринга.

Развитие пиринговых платформ

Семимильными шагами шло не только развитие московской платформы обмена трафиком, но и других региональных точек обмена. В нашей статистике мы фиксировали рост трафика свыше 200% в год, что существенно влияло на рост всей сетевой инфраструктуры. В начале

2000-х годов стартовал проект создания сетей обмена трафиком от Москвы до Владивостока на базе РосНИИРОС. Однако возникли достаточно большие сложности по внедрению стабильных организационно-технических решений в городах. Было проблематично найти площадки, отвечающие требованиям надежности, доступности для участников и нейтральности по отношению к игрокам рынка. Точки обмена трафиком в первую очередь шли за рынком и вставали на тех площадках, где было возможно объединить максимальное число участников. Однако помимо физического присутствия на площадке требовалось немало работы на этапе взаимодействия с операторами. Нужно было донести до потенциальных участников преимущества модели обмена трафиком и объяснить специфику работы IX'а. Поначалу это давалось нелегко - и тут внесли свою активную лепту растущие контент-проекты. Эти участники особенно остро ощущали необходимость продвижения ближе к конечному пользователю и наглядно показывали выгоду от прямого пирингового взаимодействия через IX по сравнению с транзитом.

Рост количества точек обмена трафиком в общемировом пространстве и конкуренция на этом поле вынудили искать новые модели поведения и схемы сети в рамках новых проектов. Одной из таких идей явилась попытка изменить подход к нейтральности точек обмена трафиком, например, разделить участников по какому-либо принципу и компенсировать стоимость сетевой инфраструктуры одних за счет других. Таким образом, появились «контентные» точки обмена трафиком, где предоставлялись максимально удобные условия для поставщиков контента и предпринимались попытки скомпенсировать расходы на инфраструктуру за счет стоимости услуг, предоставляемых потребителям контента.

Интернет-сообщество в определенный момент стало осознавать явную выгоду проектов, объединяемых общей идеей пиринга между сетями, и уже никому не требовалось объяснять преимущества межсетевого обмена трафиком. Это в свою очередь послужило поводом создания еще одной модели, названной PIPEX (от «pipe» – труба) или IXN (Internet Exchange Network). Идея в первую очередь заключалась в том, чтобы выйти за пределы классической модели и соединить географически разделенные сетевые сегменты в единое пространство, сохранив тем не менее название «точка обмена трафиком». Преимущества данной модели выглядят очевидно – не нужно никому объяснять, что такое обмен трафиком, нет необходимости предоставлять участникам полный IP-транзит, а подключение каждого нового города увеличивает размерность сети и расширяет ее географию. Данный подход формирует нечто среднее между классической точкой обмена трафиком и провайдером IP-транзита, хотя по сути своей является упрощенной моделью IP-транзита с неполной связностью,

Рис. 2. Инструментарий Looking Glass.

Network	Next Hop	Metric	LocPrf	AS_Path	Origin	Reject Reason
77.244.112.224/27	195.208.208.11		100	196925 42779	i	Wrong prefix length
81.21.86.117/32	195.208.208.11		100	196925	?	Wrong prefix length
93.184.224.0/20	195.208.208.11		100	196925 39280 39280 39280 39280	?	IRR route is
109.235.193.32/29	195.208.208.11		100	196925	?	Wrong prefix
109.235.193.48/29	195.208.208.11		100	196925	?	Wrong prefix
109.235.197.128/29	195.208.208.11		100	196925	?	Wrong prefix
109.235.197.136/29	195.208.208.11		100	196925	?	Wrong prefix
109.235.198.136/29	195.208.208.11		100	196925	?	Wrong prefix
134.19.212.0/25	195.208.208.11		100	196925	?	Wrong prefix
134.19.212.128/25	195.208.208.11		100	196925	?	Wrong prefix
134.19.214.32/28	195.208.208.11		100	196925	?	Wrong prefix
134.19.214.208/28	195.208.208.11		100	196925	?	Wrong prefix
134.19.215.192/29	195.208.208.11		100	196925	?	Wrong prefix length
134.19.217.0/25	195.208.208.11		100	196925	?	Wrong prefix length
134.19.217.128/25	195.208.208.11		100	196925	?	Wrong prefix length
134.19.218.192/27	195.208.208.11		100	196925	?	Wrong prefix length
185.41.200.0/22	195.208.208.11		100	196925 39280 39280 39280 39280	?	IRR route is absent
185.129.92.0/22	195.208.208.11		100	196925 57786	i	IRR route is absent
185.146.112.0/22	195.208.208.11		100	196925 57293	i	IRR route is absent

407 - Wrong prefix length

Размер префикса данного маршрута меньше общепринятого размера в Интернете (RFC 7454), поэтому многие участники IX могут отфильтровать такие маршруты на приеме от роут-сервера на своей стороне.

Рекомендации:

- Если вы хотели создать blackhole-анонс, убедитесь, что в конфигурации вашего оборудования указано корректное значение blackhole-community.
- В других случаях:
  - создайте route-объект в базе RIPE (или ином IRR) для приема данного маршрута роут-сервером;
  - анонсируйте (согласно RFC 7454) по EBGP маршруты блоками от /24 и крупнее для IPv4, блоками от /48 и крупнее для IPv6.

Время последней проверки: 23-10-2017 14:05:13 MSK

за меньшие (нежели чем транзит) деньги. Для реализации модели потребовалось внедрить прозрачную сетевую инфраструктуру с точки зрения протокола классической маршрутизации BGP4, что стало возможно благодаря наличию функционала «прозрачный Route Server» у большинства крупных вендоров. Это позволило не только построить географически распределенную сеть, но и уйти от broadcast-доменов, включающих все сетевое оборудование, а также применить обычные маршрутизаторы для реализации проекта. Однако, как говорится, дьявол кроется в деталях. Хорошо известно, что отработанный за многие годы протокол BGP4 хотя и не лишен ряда недостатков, но показывает существенную стабильность и устойчивость для организации сетевого взаимодействия. В данном случае в проектах, по сути, использовался «поломанный» BGP, в результате чего пострадал целый ряд сетей, для которых маршрутизация строилась неоптимальным образом, и самое главное, что они были не в силах на это повлиять. У сетей, взаимодействующих с PIPEX, фактически стало меньше возможностей влиять на выбор сетевого маршрута, так как длина маршрута сократилась и зачастую стали выбираться неоптимальные пути. Очень сильно участники PIPEX зависели от каналов – связующих звеньев системы. В отличие от классической модели, они имели большую длину, что в условиях отсутствия качественной канальной емкости часто приводило к потерям трафика, а также задержке и её вариации в передаче данных. В качестве примера реальной проблемы можно привести забавную историю про взаимодействие двух участников IX'а в Екатеринбурге через Амстердам, которое обнаружилось не сразу, так как один из PIPEX'ов выдал маршрут с одной классической точки обмена трафиком на другую. К сожалению, подобные проекты, помимо некорректного взаимодействия между сетями, стали приводить к еще более необычным эффектам, таким как асимметричность прохождения маршрутов и связанные с этим возможные блокировки на стороне некоторых операторов. В то же время «классические» точки обмена трафиком тоже расширяли географию, но за счет внедрения схем с привлечением партнеров и расширением возможной территории подключения. Это позволяло операторам тонко управлять своим сетевым взаимодействием, более детально относиться к качеству взаимодействия и давало свободу действия участникам, подключенным географически удаленно на конкурентном рынке.

Инструментарий

Развитие платформы точек обмена трафиком находится в постоянном движении. Модель протокола BGP4, активно применяемая для межоператорского обмена, постоянно обрастает все более новыми возможностями. Об этом регулярно идут дискуссии на IETF, где сообщество ищет реализацию новых идей и усовершенствований. Увы, в последние годы широкое развитие сетей при одновременном отставании учебного процесса привело к снижению качества знаний сетевых специалистов, допущенных к управлению глобальной маршрутизацией. Это сказалось, в том числе, и на модели потребления услуг точек обмена трафиком. Зачастую участник сети просто хочет, чтобы все работало сразу и при его минимальном участии. Понимая, что это – объективная реальность, мы попытались сделать среду работы системного администратора максимально комфортной. Для этого мы в числе первых внедрили усовершенствованный механизм Looking Glass на Route Server, который позволяет не только видеть отвергаемые сетевые маршруты участника, но и самостоятельно анализирует причины и подробно расписывает ошибки по каждому отвергаемому маршруту. Помимо этого возможна отсылка автоматизированных уведомлений участнику о замеченных критичных ошибках. Интерфейс этого инструментария показан на рис. 2.

Уязвимый BGP

Отдельно хотелось бы отметить целый ряд проблем, обобщающихся терминами BGP Route Leak и BGP Hijacking. По сути, это целый комплекс ошибок и упущений настроек протокола, приводящих к самым тяжелым последствиям.

Route Leak заключается в том, что один из участников ошибочно (как правило, без всякого умысла) выдает маршруты на «чужие» сети. Согласно правилам взаимодействия, каждый участник должен анонсировать на точке обмена трафиком только свои сети и сети своих клиентов. Нарушение этого принципа приводит к тому, что сеть из равноправного пира превращается в провайдера транзита, вовлекая в передачу транзитного трафика и саму точку обмена трафиком. Результатом может быть изменение времени отклика сетевых ресурсов, увеличение задержки и потеря трафика. Негативный эффект зачастую выходит за рамки IXP и может поразить систему маршрутизации в глобальном масштабе.

Нами отдельно были внедрены механизмы борьбы с этими неприятными явлениями. С целью защиты от возможных ошибок на сети MSK-IX применяются глубокие механизмы фильтрации, позволяющие анализировать базы данных IRR (Internet Routing Registry) и строить сетевые фильтры по IP-сетям и автономным системам для каждого участника. Мы контролируем дополнительно количество анонсируемых маршрутов каждым участником, фиксируем граничные значения взаимодействия и общей таблицы в целом и оперативно сигнализируем в случае существенного изменения.

BGP Hijacking – значительно более разрушительная ошибка маршрутизации. В результате действия оператора создается новый маршрут в таблице маршрутизации с измененным атрибутом Origin. Как правило, использование этого маршрута приводит к блокировке передающихся данных и фактически - к нарушению сетевого взаимодействия для пострадавших сетей. В последнее время эта ошибка стала все чаще возникать в результате внедрения механизмов фильтрации контента или же организации защиты от DDoS-атак. К счастью, вовремя появились механизмы RPKI, позволяющие проводить проверку («валидацию») подобных маршрутов и избегать возникающих вследствие этого проблем, однако внедрение этих механизмов требует серьезных усилий у валидирующего оператора и поддержки компонентов системы валидации различными производителями оборудования, так что этот этап еще впереди.

Создание «прозрачной» модели передачи маршрутной информации в BGP производителями оборудования изначально было нацелено на задачи создания Route Server и аналогичные проекты. Однако простота модификации BGP-маршрутов стала создавать потенциальную уязвимость для стабильности. Появилась угроза изменения атрибута AS_PATH маршрута с сохранением ASN сети, являющейся его источником. Изначально идея существования атрибута AS_PATH в BGP была нацелена на защиту от петель маршрутизации. Именно поэтому маршрутизатор не принимает от внешней сети маршруты, прошедшие через собственную автономную систему. «Прозрачная» модель BGP на распределенной инфраструктуре, модифицируя AS_PATH и убирая собственную AS из него, несет существенную угрозу маршрутных петель.

К сожалению, до сих пор отсутствует защита от изменений и валидация AS_PATH, хотя регулярно предпринимаются попытки эту ситуацию изменить. Например, в 2004 году компания Cisco вносила в IETF Internet Draft с описанием механизма Secure Origin BGP (soBGP)(https://tools.ietf.org/html/draft-ng-sobgp-bgp-extensions-02). Суть драфта заключалась в том, чтобы помимо валидации с помощью цифровых подписей автономных систем внедрить валидацию маршрута с помощью построения сетевого графа связности. Предложенный авторами механизм валидации, по сути, предлагал простой алгоритм, где две автономные системы описывали свое взаимодействие друг с другом – и его можно было проверить с помощью цифровой подписи. Если на пути следования между ними появлялась третья автономная система, у которой такой подписи не было, то этому маршруту можно было снизить приоритет или же отбросить. Однако в то время подобные изменения казались слишком сложными, требующими дополнительной памяти и ресурсов маршрутизаторов, поэтому дальше BGP-драфта дело не пошло. Одну из идей, способную частично локализовать проблему утечки маршрутов, предложили коллеги из компании Qrator (https://datatracker.ietf.org/doc/draft-ietf-idr-bgp-open-policy/). Суть предлагаемого метода заключается в том, чтобы прописать характер взаимодействия автономных систем на уровне настройки BGP, разбив их на три типа: клиент/провайдер/пиринг. Таким образом, необходимо, чтобы клиент не принимал маршрут от клиента, на пиринге были только пиринги и т.д.

Похожая идея нашла реализацию в виде очередного RFC8212 (https://tools.ietf.org/html/rfc8212). В результате анализа ошибок (утечек) маршрутов последнего времени было обнаружено, что они могут возникать в момент первичной настройки (перенастройки) оборудования, когда участник просто забывает прописать фильтры протокола. Предлагаемый механизм не допускает приема и передачи маршрутов без настроенных на оборудовании фильтров и отчасти помог бы уберечь от ошибок конфигурации такого рода.

На последней конференции NANOG71 в Сан-Хосе в 2017 году Cisco представила свой доклад на тему борьбы с утечкой маршрутов (https://pc.nanog.org/static/published/meetings/NANOG71/1430/20171003_Heitz_Bgp_Large_Community_v2.pdf). Суть предлагаемого метода заключается в том, чтобы проводить маркировку с помощью механизма BGP community и последующую валидацию маршрутов на пути следования.

Очередная идея защиты атрибута AS_PATH была недавно стандартизована в IETF. Расширения протокола BGP под общим названием BGPSEC документированы в 4 RFC (https://www.rfc-editor.org/info/rfc8205, https://www.rfc-editor.org/info/rfc8206, https://www.rfc-editor.org/info/rfc8207, https://www.rfc-editor.org/info/rfc8208). Суть решения заключается в выстраивании цепочки доверия всего маршрута на пути его следования от источника к получателю и позволяет не только валидировать origin маршрута, но и AS_PATH. В перечисленных RFC подробно описан механизм передачи отдельного атрибута с цифровой подписью.

Однако очень часто предлагаемые механизмы защиты наталкиваются на серьезное препятствие в виде уже годами работающих алгоритмов и оборудования, которое не в состоянии поддерживать подобный функционал. Более того, внедрение новых механизмов криптографии в основу сети – ее основной мозг (маршрутизатор) – может сказаться критическим образом на выделяемых ресурсах и потребует существенной перестройки всей глобальной сетевой инфраструктуры, что вряд ли реализуемо без веских на то причин, поскольку связано с очень серьезными трудозатратами.

Взгляд в будущее

Активно продолжается внедрение механизмов, нацеленных на оптимизацию времени сходимости протокола BGP. С этой целью многими точками обмена уже давно и успешно применяется протокол BFD, позволяющий оперативно реагировать на изменение в физической инфраструктуре сети.

Рабочие группы IETF продолжают работу над стандартами и ищут применение все новым глобальным идеям, в том числе, и в механизмах сетевой сигнализации. Есть целый набор нововведений, касающийся задач минимизации обрывов связи в результате подготовки и проведения плановых работ на сети. Не так давно, в июле этого года, в Лондоне ассоциацией Euro-IX проводился Route Server Workshop, где, в том числе, велась работа над стандартизацией набора управляющих BGP community на всех доступных точках обмена трафиком. Это достаточно важно во время консолидации платформ обмена трафиком и в связи с наличием ряда международных проектов сразу на нескольких глобальных точках обмена трафиком.

В заключение хотелось бы отметить, что экосистема точек обмена трафиком – это постоянно растущий организм, который активно взаимодействует с глобальной интернет-средой, изменяя ее и, в свою очередь, изменяясь сам. Разрабатываемые и применяемые на точках обмена трафиком инструментарии и методики вносят существенный вклад в развитие общемирового пирингового обмена. Ну а впереди на техническом фронте уже просматривается эпоха автоматизации и упрощения сложных процессов, что усилит интерес к использованию подобных проектов большинством участников рынка.

Оптимизация пиринга BGP

Ченгиз Алаэттиноглу (Cengiz Alaettinoglu), Packet Design

Оптимизация пиринга BGP для снижения затрат и повышения качества обслуживания: Качество обслуживания и прибыльность интернет-сервис-провайдеров сегодня во многом зависит от правильной оптимизации трафика и взаимодействия с другими сетями. Недостаток данных и инструментария не позволял провайдерам принимать информированные и оптимальные решения в этой области. Сегодня же имеется целый ряд способов оптимизации пиринга, позволяющих сократить затраты на транзит, не снизив, а возможно, и повысив качество услуг.

Принятие информированных пиринговых решений повышает качество обслуживания и прибыльность работы всех провайдеров услуг – от крупнейших до региональных и более мелких. Например, когда транзитная пропускная способность провайдера подходит к концу, он должен решить, стоит ли наращивать мощность существующих каналов, добавить новый канал к тому же провайдеру в другом месте или использовать пиринг с совершенно новым провайдером.

Исторически у провайдеров не было сетевых данных, необходимых для принятия таких решений. Сегодня же имеется целый ряд способов оптимизации пиринга BGP (Border Gateway Protocol), позволяющих сократить затраты на транзит, не снизив, а возможно, и повысив качество обслуживания.

В настоящей статье мы рассмотрим распространенные типы политик и операционных ограничений, влияющих на деловые связи между провайдерами, а также то, как традиционные сетевые инструменты мешают принимать информированные пиринговые решения. Затем мы обсудим две задачи, необходимые для оптимизации пиринга и ставшие возможными благодаря развитию технологий анализа маршрутов.

Как работает пиринг BGP

Пиринг в сфере интернет-маршрутизации весьма сложен. И для создания пиринга, и для пиринговых отношений

Рис. 1. Маршруты BGP по соседним и исходным AS.

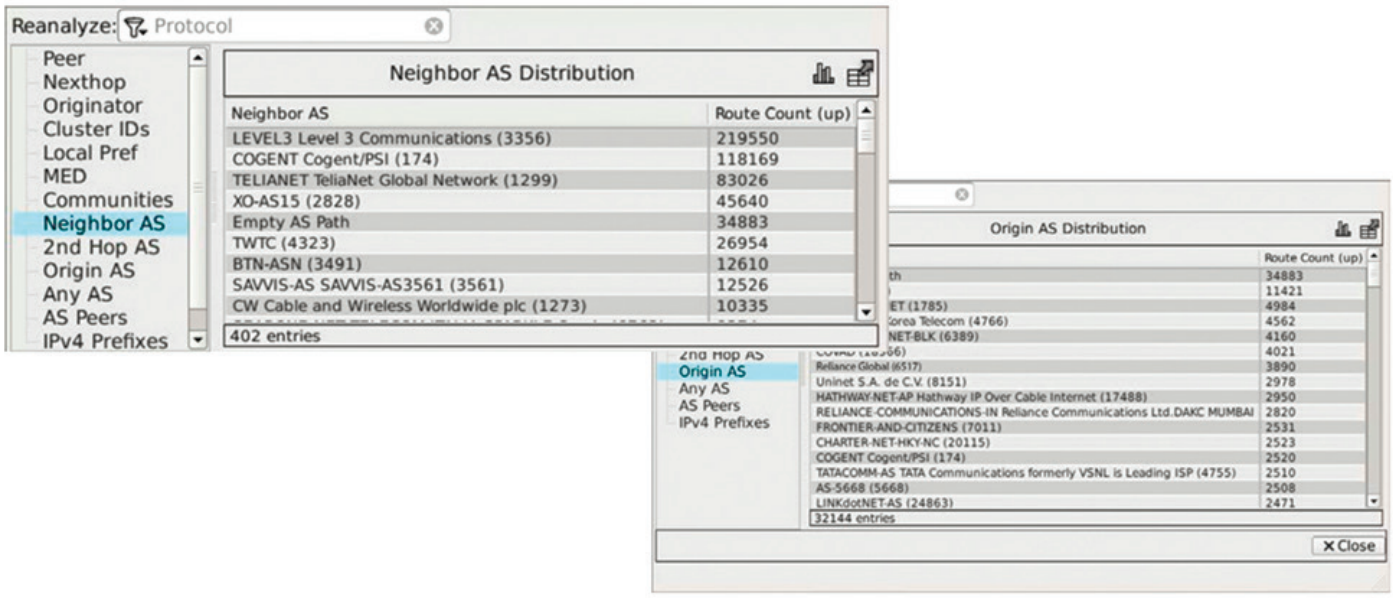
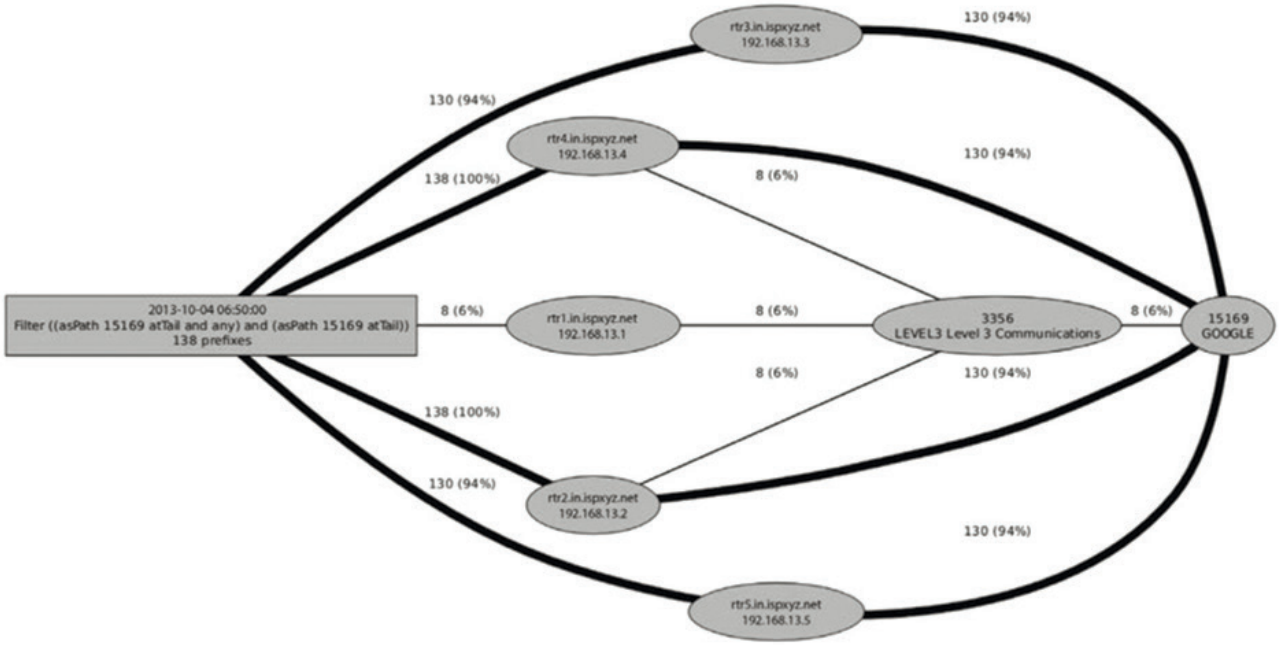


Рис. 2. Маршруты BGP по соседним и исходным AS.



между провайдерами аналогичного уровня используется протокол BGP. Он соединяет друг с другом автономные системы (AS). С помощью BGP пограничный маршрутизатор одной AS устанавливает пиринг с пограничным маршрутизатором другой AS, а затем эти маршрутизаторы обмениваются друг с другом известными маршрутами. Если маршрутизатор сообщает пиру о том или ином маршруте, то пир может пересылать по этому маршруту пакеты в его точку назначения. Пакеты транзитом передаются в следующую AS, откуда либо доставляются до точки назначения (если она локальная), либо пересылаются в следующую AS. Объявляя маршрут, AS разрешает другой AS использовать свои ресурсы для транзитной пересылки пакетов. То, какие именно маршруты будут объявлены, регулируется ограничениями политик, и они же определяют характер деловых связей между AS.

Между различными AS обычно применяются ограничения политик двух типов, соответствующие двум бизнес-моделям:

Провайдер – клиент

Отношения вида «провайдер – клиент», как правило, используются между провайдерами и обслуживаемыми ими предприятиями, либо между провайдерами регионального и глобального уровня. Клиент платит провайдеру за транзит пакетов до места назначения (и обратно). Обычно сумма оплаты пропорциональна объему пересылаемого трафика. В этом случае провайдер объявляет клиентам все известные ему маршруты.

Равноправные узлы (пиринг)

При пиринге, как правило, пересылка трафика друг друга осуществляется бесплатно. Преимущество каждого провайдера в том, что для пользователя качество услуги повышается, так как сокращается задержка при обращении к сервисам другого провайдера. Каждая AS объявляет другим AS только свои собственные маршруты (включая маршруты клиентов). В этом случае AS может использовать ресурсы следующей AS только для транзита трафика, адресованного внутри этой AS, или ее клиентов. Иными словами, следующая AS не выполняет передачу пакетов третьим сторонам.

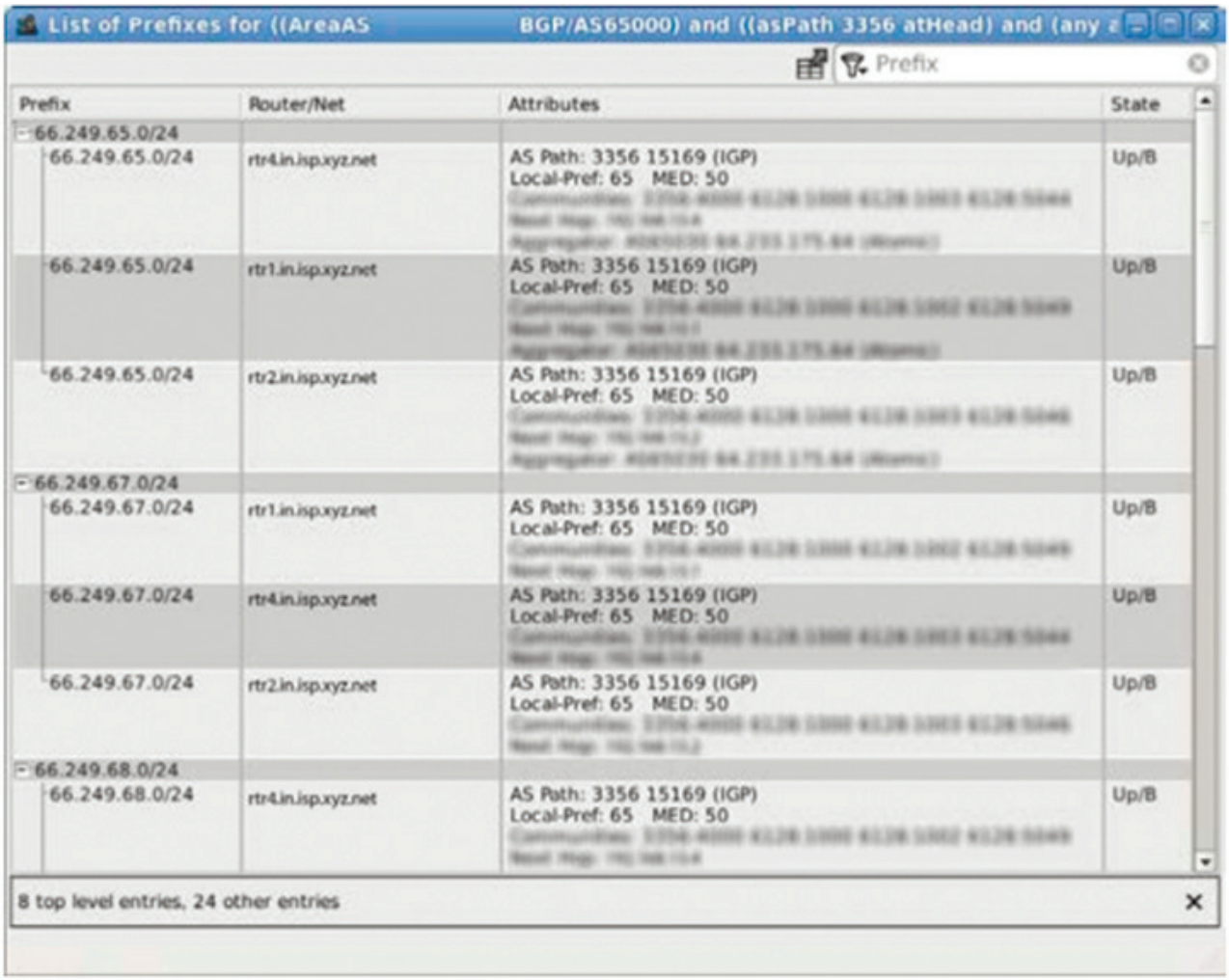
Крупные провайдеры с глобальным охватом – так называемые провайдеры высшего уровня (также называемые Tier-1 - прим. ред.) – как правило, заключают пиринговые соглашения друг с другом. Любой провайдер значительно сэкономил бы на транзите, если бы смог организовать пиринг на этих условиях с провайдерами высшего уровня. Но для пиринга AS высшего уровня обычно требуют от потенциальных партнеров:

- географического охвата, дополняющего охват самого провайдера;
- возможности и желания осуществлять пиринг в нескольких географически разнесенных местах;
- обмена трафиком между собой и потенциальным партнером примерно в равной пропорции;
- и ряд других операционных требований.

В результате большинство AS, включая региональных провайдеров, вынуждено платить за транзит. Аналогично большинство предприятий покупают транзит у региональных провайдеров или провайдеров высшего уровня.

Однако даже у самых маленьких провайдеров есть возможность пиринга. Они могут объединяться с другими мелкими провайдерами в своем регионе или же с провайдерами контента (которым это также принесет снижение затрат и повышение качества для пользователей). Но такое сотрудничество имеет смысл, только если две AS обмениваются значительными объемами трафика. Экономия на транзите должна

Рис. 3. Восемь префиксов доступны только через Level 3 Communications.



оправдывать затраты на прямой канал между двумя AS (и остальную инфраструктуру, например, оптические порты и кросс-соединения). Выгодный вариант пиринга между AS предоставляют точки обмена трафиком IXP (Internet Exchange Point: такая точка представляет собой т.н. колокацию, где несколько AS держат свои маршрутизаторы, устанавливают пиринг BGP и обмениваются трафиком друг с другом через локальную сеть точки обмена).

Заметим, что и для провайдеров высшего уровня решения о пиринге непросты. Пусть, например, провайдер A – вымышленный провайдер высшего уровня, имеющий очень развитую сеть в России, – получает запрос о пиринге в Москве от провайдера B – другого провайдера высшего уровня, который в России представлен хуже. Если провайдер A одобрит этот запрос, не разобравшись в последствиях, он может потерять конкурентное преимущество.

Провайдеру A важно знать, будет ли московский трафик симметричным в обоих направлениях. Если провайдер B будет передавать транзитом больше трафика, чем провайдер A, тот окажется в невыгодном положении, так как за транзит ни один из участников денег не берет. А провайдер B при этом еще и улучшит обслуживание своих пользователей, для которых снизится задержка при обмене данными с другими точками в России.

Принятие информированных решений о пиринге

Принятие информированных пиринговых решений важно для всех провайдеров – от крупнейших до региональных и более мелких. Оно влияет на прибыль каждого из них. Для принятия информированных решений о пиринге провайдерам нужно две вещи.

Добиться информированности о трафике

Во-первых, и это главное: провайдеру необходимо знать все о трафике, включая следующие аспекты:

1. Сколько трафика принимается от его провайдеров, пиров и клиентов (например, соседних AS) и сколько передается к ним.
2. Куда идет этот трафик или откуда он исходит (исходные и целевые AS).
3. Через какие еще AS этот трафик проходит по пути (транзитные AS).

Добившись такой информированности о трафике, провайдер может

оптимизировать пиринг BGP так, чтобы снизить затраты на транзит. Вот пример такой ситуации: образовательная сеть в США обнаружила, что значительная часть ее трафика направляется к местному провайдеру кабельного Интернета. Ничего удивительного в этом не было: ученики и учителя обращались к школьным ресурсам из дома. Образовательная сеть организовала пиринг с кабельным провайдером, и обе стороны снизили затраты на транзит.

Смоделировать эффект изменений пиринга

Во-вторых, провайдеру необходимо смоделировать эффект изменений пиринга. Например, обдумывая изменение пиринга, провайдер должен решить, следует ли ему:

1. Нарастить пропускную способность существующих каналов.
2. Добавить новый канал к тому же провайдеру в другом месте; или
3. Использовать пиринг с совершенно новым провайдером.

Чтобы выяснить, что будет выгоднее, инженерам нужно смоделировать изменения в рабочей сети и проверить, как именно они повлияют на состояние маршрутизации и трафик, чтобы избежать неожиданностей.

Недостатки традиционных инструментов управления пирингом

Создание выгодных пиринговых отношений и постоянный их мониторинг – дело сложное и трудоемкое. Инженерам по пирингу приходится непрерывно отслеживать входящий и исходящий трафик, чтобы решить, имеет ли смысл пиринг с другими автономными системами, а если да, то с какими именно.

Без непрерывного мониторинга переключение прямого пира на пиринг выше по потоку может вызвать непредвиденные изменения. При всплеске внешнего трафика важно быстро определить его источник и точку назначения, а также то, пиринговая ли это проблема или последствия изменений маршрутизации IGP (внутренний протокол маршрутизации - прим. ред.). При наплыве или спаде префиксов, а также тогда, когда AS сообщает об аномальных префиксах, необходимо тут же оповестить операционные команды, чтобы выполнить триаж инцидента и избежать прерывания обслуживания или угрозы безопасности.

В прошлом у сетевых инженеров не было полной информации и инструментов для управления интернет-пирингом. Им мешали неполные данные о трафике и маршрутизации, изолированный анализ данных и статические инструменты моделирования. Хотя и возможно получить информацию о трафике, используя технологии аналитики потока, у анализа данных о трафике, собранных с отдельных маршрутизаторов, есть свои пределы.

Например, инструменты анализа трафика работают, анализируя данные о потоке, экспортируемые маршрутизаторами по технологиям IPFIX, NetFlow, J-Flow, NetStream и пр. Эти данные собираются по интерфейсам и, как правило, содержат метки MPLS, исходные и целевые IP-адреса, класс

Рис. 4. Общий трафик сети.

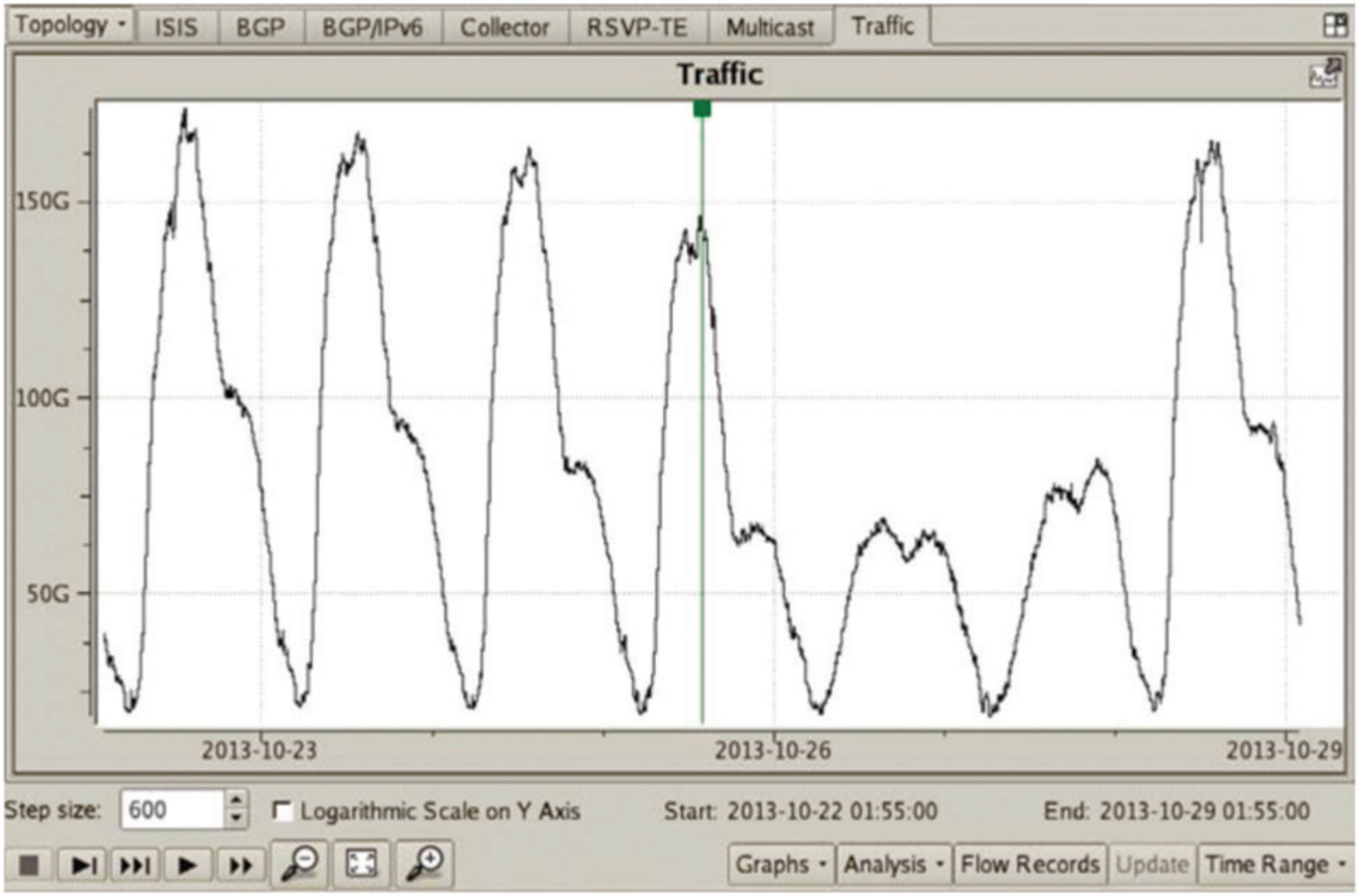
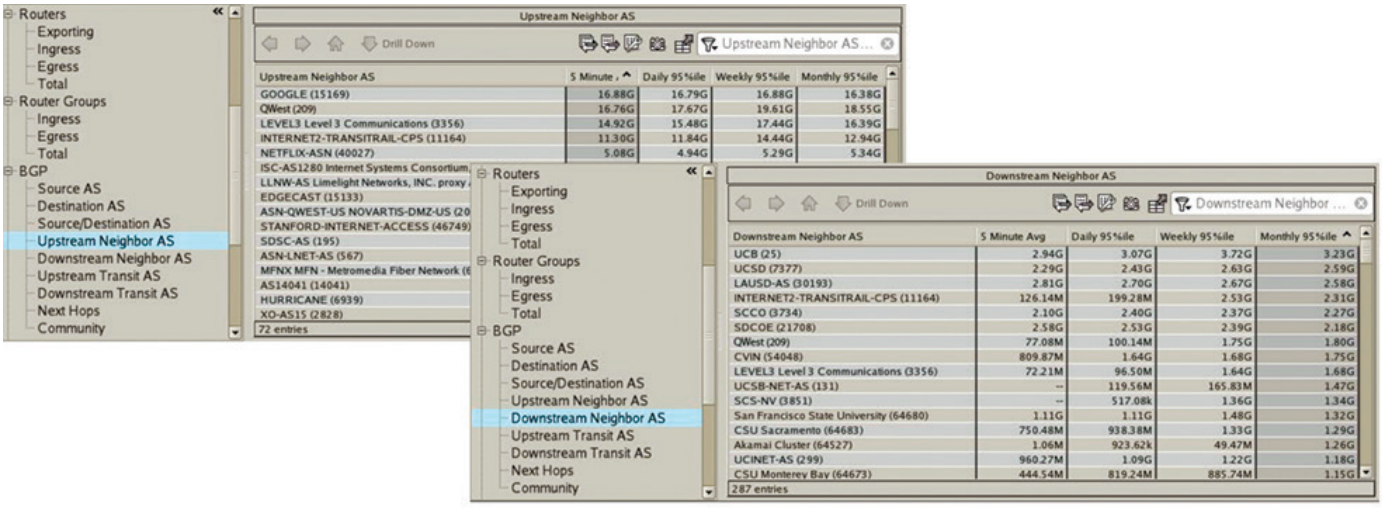


Рис. 5. Трафик исходных и целевых AS.



обслуживания и протокол IP, номера портов транспортного уровня, время старта и длительность потока, а также количество переданных байтов. В некоторых вариантах указываются также ограниченные данные о номерах исходных и целевых AS. Большинство инструментов анализа потока могут суммировать объемы трафика по этим потокам для каждого исходного и целевого IP-адреса, порта и номера AS, генерируя отчеты по N крупнейших источников/получателей для каждого интерфейса, откуда экспортируются данные потока.

Однако обычные инструменты анализа трафика не умеют определять каждый путь, от источника до цели, для каждого потока в сети. А эти данные жизненно важны для управления и мониторинга сетей, использующих пиринг. Провайдерам необходимо легко и просто понимать, как входящий пиринговый трафик влияет на маршрутизацию в собственной сети провайдера. Например, всплеск трафика может перегрузить те или иные каналы и вызвать изменение маршрутов IGP. Но этой важной информации о трафике и его поведении просто нет.

Нечего и говорить, что для оценки требований пиринга, отслеживания внешнего трафика и устранения неполадок необходимы телеметрия в реальном времени и мощные аналитические инструменты. Добившись полной видимости трафика по путям маршрутизации, провайдеры могут принимать информированные решения и затем оптимизировать свой пиринг BGP. Последние инновации в области аналитики маршрутизации и трафика дают гораздо более цельную картину пиринговых отношений, а также позволяют моделировать изменения пиринга и точно прогнозировать их эффект.

Аналитика маршрутизации и трафика, помогающая принимать решения о пиринге

Чтобы «видеть» трафик и моделировать эффект изменений пиринга, сетевым инженерам нужно уметь анализировать и моделировать маршруты и политики BGP, а также маршруты IGP и топологию сети провайдера. Новые технологии аналитики маршрутов показывают

Рис. 6. Недельный трафик по шести крупнейшим исходным AS.

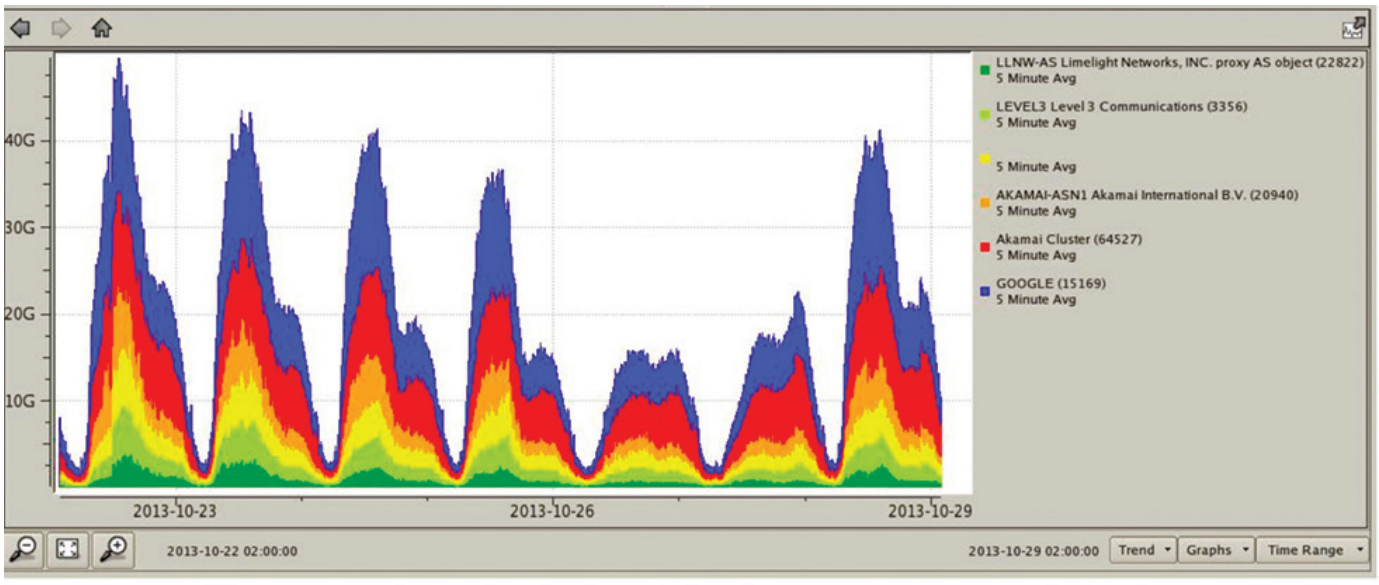
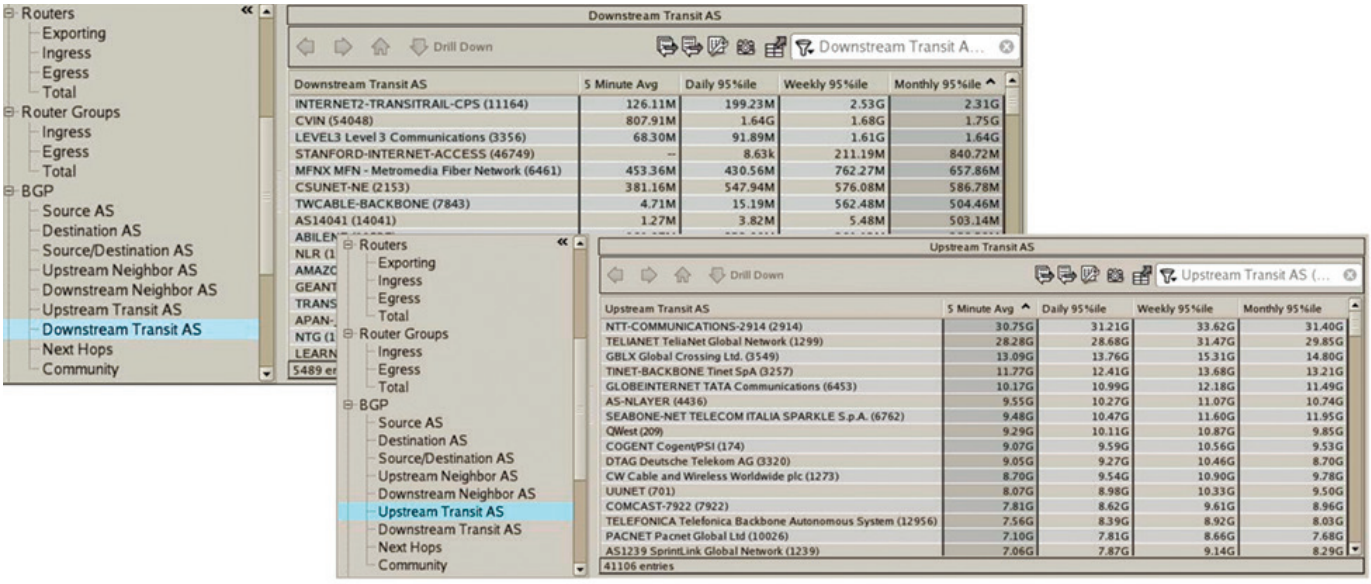


Рис. 7. Отчеты по трафику AS выше и ниже по течению.



путь для каждого потока – точно и экономично.

Объединив анализ маршрутизации и анализ трафика для записей обо всех принимаемых потоках, можно вычислить полный путь – как вперед, к точке назначения, так и назад, к источнику потока. Этот путь будет включать каналы и маршруты в сети, а также внешние каналы, соседние AS выше и ниже по потоку, транзитные AS, исходную и целевую AS.

Этот подход имеет целый ряд преимуществ. Во-первых, трафик становится гораздо лучше видим. Во-вторых, становится виден трафик даже для каналов, из которых данные потока не экспортируются. Например, региональный провайдер, имеющий дело, главным образом, с интернет-трафиком, сможет отслеживать только свои внешние каналы, а аналитика маршрутизации рассчитает потоки трафика по внутренним каналам и построит их карту. И в-третьих, упрощается обнаружение дублированных потоков, благодаря чему один и тот же поток, экспортированный на нескольких каналах, будет учтен только один раз в каждом отчете (это часто называется дедупликацией потоков – англ. flow de-duplication).

Видимость политик BGP

Как мы уже отмечали, политики BGP напрямую влияют на объемы пирингового трафика. Аналитика маршрутизации покажет, правильно ли текущие конфигурации маршрутизаторов реализуют политики BGP, путем проверки динамического набора маршрутов BGP. Инженеры могут просматривать результаты по пирам и маршрутизаторам следующего шага, соседним, транзитным, исходным и целевым AS, метрикам local preference и значениям MED, а также по сообществам BGP. На рис. 1 показано число маршрутов, объявленных каждой соседней AS, плюс число маршрутов, исходящих из каждой исходной AS.

Из таких записей можно визуализировать или перечислить соответствующий набор маршрутов. На рис. 2 визуализируются маршруты,

Рис. 8. Проекция потока на его путь.

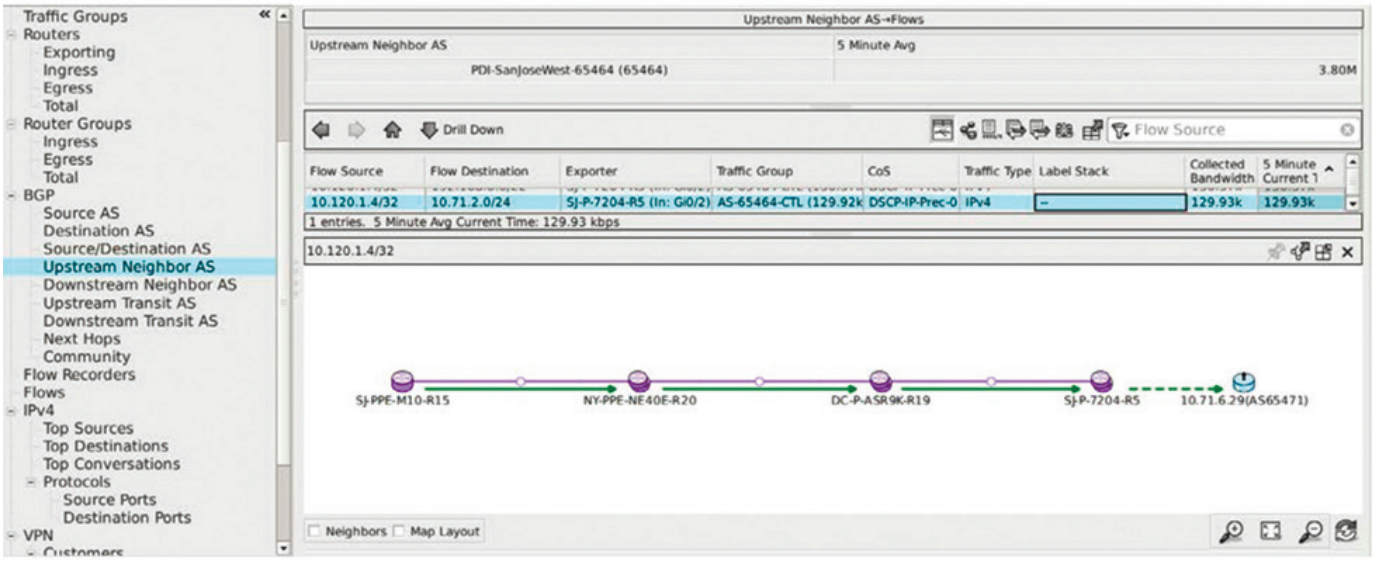
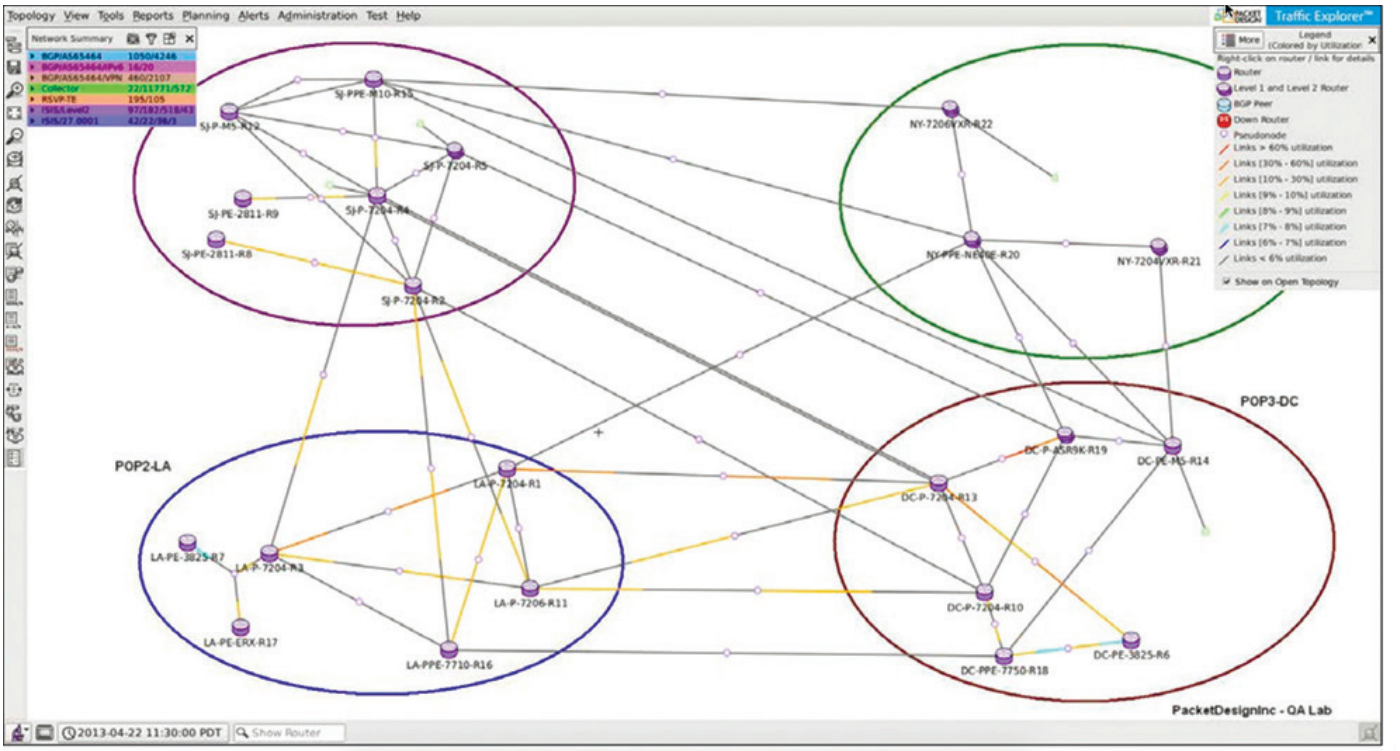


Рис. 9. Уровни трафика по внутренним каналам.



для которых исходной AS служит AS 15169, принадлежащая Google. Т.е. показано, как от данного провайдера добраться до Google. Граничных маршрутизаторов пять, они промаркированы rtr1–rtr5. Все граничные маршрутизаторы, кроме rtr1, осуществляют прямой пиринг с Google. Кроме того, rtr1, rtr2 и rtr4 могут обмениваться трафиком с Google через компанию Level 3 Communications. BGP предпочитает маршруты с более короткими путями AS, поэтому он требует использовать маршрутизаторы с прямым пирингом. Эти маршруты показаны жирными линиями. Чем жирнее линия, тем больше предпочтительных маршрутов идет по этому соединению.

Обратите внимание, что из 138 префиксов Google восемь доступны только через Level 3 Communications. Эти префиксы перечислены на рис. 3. Тут же возникает ряд вопросов: это сознательная политика или результат неправильной конфигурации? И за какой объем трафика отвечают эти префиксы (т.е. за какой объем транзита провайдер платит Level 3 Communications)?

Данные о трафике

На рис. 4 показан весь трафик в сети регионального провайдера за неделю. Видны типичные суточные колебания: каждый день около полудня наблюдается пик, а по выходным объем трафика гораздо ниже, чем в рабочие дни.

Отчеты о трафике по исходным и целевым AS показывают, откуда поступает трафик и куда он следует – см. рис. 5. Здесь имеется множество настраиваемых статистических показателей, но на скриншоте показаны среднее значение за 5 минут и объемы для 95-й перцентили: суточные, недельные и месячные. Для шести первых исходных AS на рисунке 6 показана вариация трафика для той же самой недели.

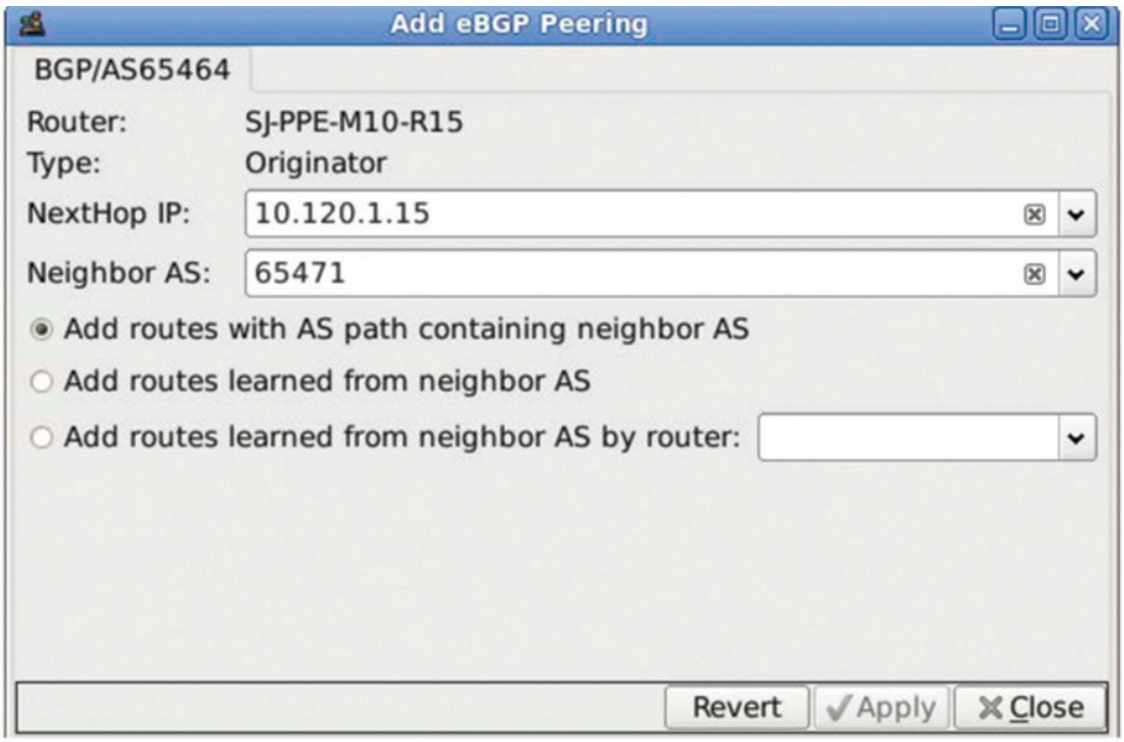
Для этой сети крупнейшей исходной AS является Google. Можно ли установить прямой пиринг с Google? Провайдер из примера действительно находится в пиринге с Google, т.е. экономит на транзите трафика Google – 13 Гбит/с. Кстати, отчет о трафике по исходным AS не ограничивается N первых строчек. Хотя пиринг с несколькими крупнейшими AS и дал бы самый значительный выигрыш в стоимости транзита, это не всегда возможно из-за географических расстояний. Более практичным может оказаться пиринг с AS ниже по списку. Или, возможно, найдется другая AS, которая может взять на себя транзит (платный или бесплатный на взаимовыгодной основе) трафика многих исходных AS из списка. Эти возможности представлены в отчетах по трафику AS выше и ниже по течению, как показано на рис. 7.

Для регионального провайдера, где большая часть трафика поступает из Интернета, в принятии решений о пиринге главную роль играет отчет о трафике выше по течению. Отметим, что несмотря на то, что технология маршрутизации однозначно определяет исходную AS потока, путь, проходимый этим трафиком, зависит от политик исходной AS и транзитных AS по пути следования.

Эта информация не распространяется непосредственно в BGP, поэтому обычная аналитика маршрутизации тут не поможет. Новые технологии анализа маршрутизации используют комбинаторную разведку путей AS, происходящую во время сходимости BGP, и создают граф AS в Интернете, учитывающий политики. Таким образом, становится возможным узнать, через какие транзитные AS может проходить трафик каждой исходной AS при прямом пиринге.

Сочетание аналитики маршрутов и трафика также выявляет соседние AS выше и ниже по течению (т.е. прямых

Рис. 10. Добавление нового пира BGP.



пиров), с разбивкой на отдельные внешние каналы и сообщества BGP. Чтобы добиться еще большей детализации, можно определить группы трафика на основе исходного и целевого IP-адресов. Такие отчеты помогут понять, пришла ли пора увеличить пропускную способность пиринговых каналов.

Даже если данные потока экспортируются только для пиринговых каналов, аналитика маршрутизации может проецировать эти потоки по внутренним каналам в сети. Иллюстрация приведена на рис. 8. После проекции всех потоков высчитываются итоговые данные использования всех внутренних каналов – на рис. 9 они показаны с цветовыми кодами по загруженности каналов на топологической карте.

Моделирование трафика

При принятии решений о пиринге нужен инструмент планирования, чтобы моделировать изменения маршрутизации, например, добавлять

Рис. 11. Тонкая настройка политик BGP путем изменения значений атрибута BGP Local-Pref.

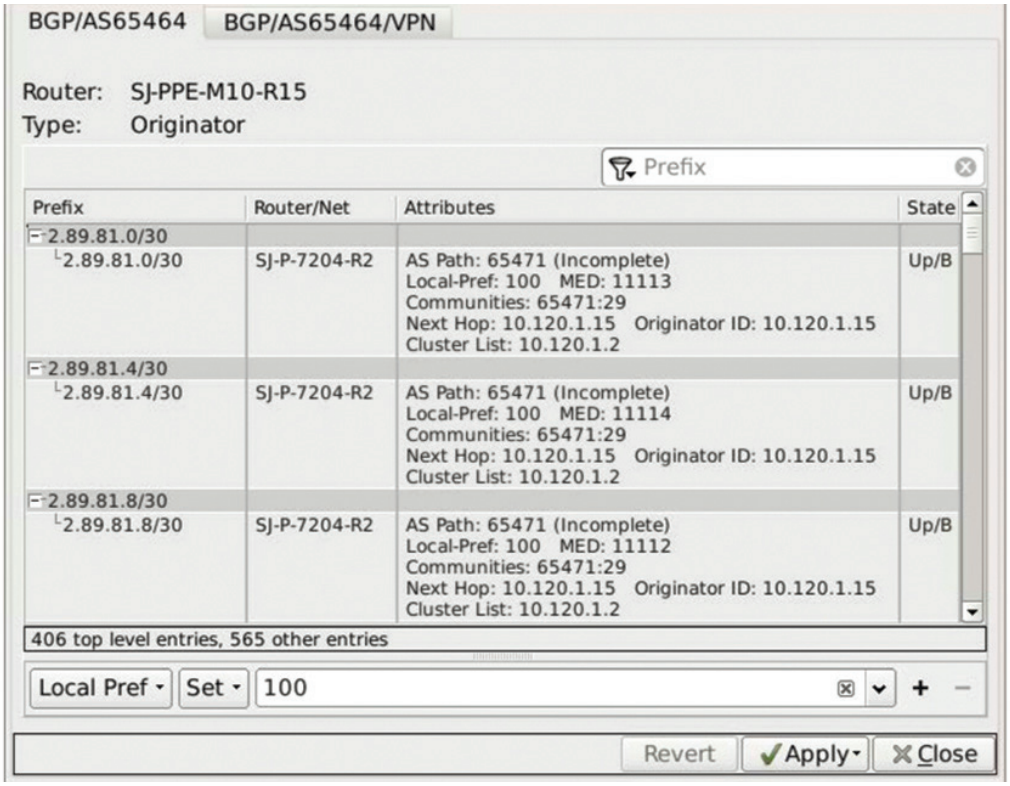
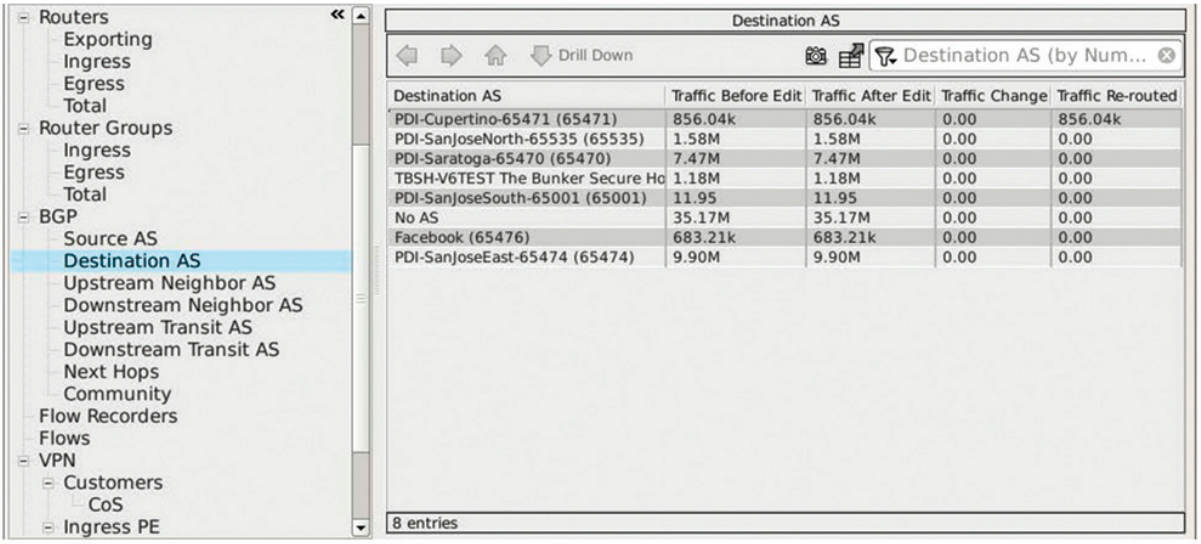


Рис. 12. Объемы трафика по целевым AS до и после изменения.



пиринг BGP. Моделирование трафика на базе аналитики маршрутизации очень облегчает такое планирование, так как модель в его основе включает пути потоков. При изменении путей в модели аналитика маршрутизации может вычислить сравнительные объемы трафика до и после изменения на внутренних и внешних каналах и AS.

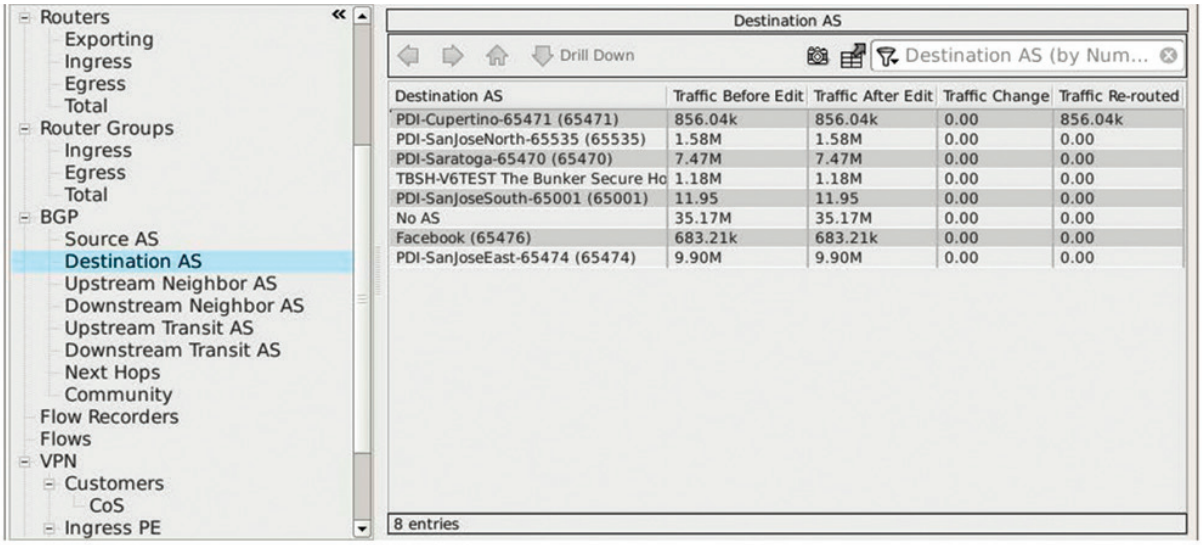
Такое моделирование осуществляется практически мгновенно, в отличие от обычных инструментов планирования, требующих нескольких часов или дней для того, чтобы построить точную модель сети. Эта модель основана на событиях маршрутизации IGP и BGP, а потому всегда точна и доступна в реальном времени. Помимо добавления и отказов каналов, префиксов и маршрутизаторов, технология аналитики маршрутизации позволяет моделировать добавление и отказы пирингов BGP.

Диалоговое окно на рис. 10 иллюстрирует вышесказанное. Добавляя пира BGP, можно автоматически выбрать маршруты, которые будут объявляться новым пиром, например, все маршруты, у которых номер AS этого пира значится в атрибуте BGP AS-path. Как видно на рис. 11, политики можно детализировать и дальше.

Впоследствии для каждого отчета о трафике выдается сравнительное представление «до» и «после». Напри-

Благодаря недавним инновациям стало возможно регистрировать и сохранять все события маршрутизации и рассчитанные пути трафика в высокопроизводительной базе данных. Поэтому стало возможно воспроизводить события маршрутизации и трафика для диагностики первопричин проблем. Например, можно «перемотать назад» время в сети до момента, когда канал стал перегружен, и проанализировать трафик в канале. Можно увидеть, откуда и куда шел этот трафик, какой путь он использовал, а главное – какие политики нужно применить, чтобы избежать подобных перегрузок.

Рис. 13. Матрица трафика: интернет-трафик и трафик VPN уровней 2 и 3.



мер, на рисунке 12 приведен отчет по целевым AS после моделирования изменений, приведенных на рисунке 10 (в топологии малой лаборатории). Объемы трафика не изменились, но весь трафик перенаправлен в новое пиринговое расположение, как видно в последнем столбце отчета.

Другие преимущества анализа трафика и маршрутизации

Применение этой технологии не ограничивается анализом пирингового трафика BGP. Новые технологии понимают VPN BGP/MPLS IP уровня 3, а также псевдопроводные VPN уровня 2 типа Martini. Для каждого VPN-сервиса и каждого заказчика дается полная информация о том, где трафик входит в сеть, по каким путям он следует и где выходит из сети. На основе этой информации можно генерировать матрицы трафика. Пример такой матрицы, сочетающий в себе интернет-трафик и трафик VPN уровней 2 и 3, приведен на рис. 13.

Можно также отслеживать туннели RSVP-TE, вместе с их путями и объемом передаваемого по ним трафика. Можно выполнять анализ отказов и выяснять, достаточна ли пропускная способность маршрутов быстрой перемаршрутизации или вторичных маршрутов для того, чтобы справиться с дополнительным трафиком при отказе. Отчеты для туннелей показывают минимальные, средние, максимальные значения и значения 95-й перцентили по дням, неделям и месяцам. Эти данные можно использовать в конфигурациях маршрутизаторов для более точного резервирования пропускной способности туннелей.

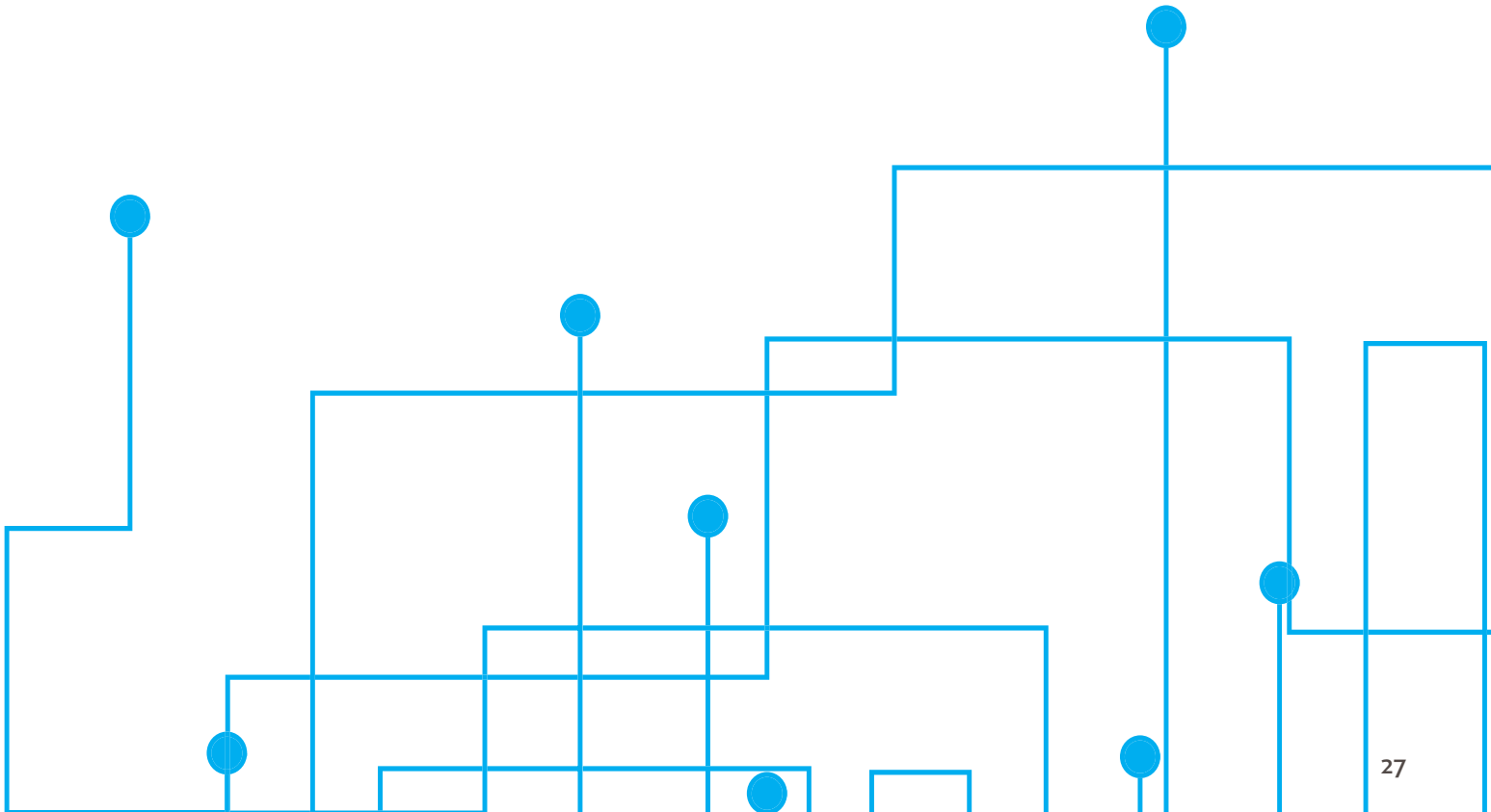
Для многоадресной (multicast) маршрутизации можно отслеживать все деревья PIM (Protocol Independent Multicast) в сети. Также можно проецировать многоадресный трафик по сетевым каналам, чтобы понять его поведение. IPTV и подобные приложения вносят в сеть большой объем многоадресного трафика. Планирование трафика без учета многоадресных пакетов теперь уже нельзя назвать ни реалистичным, ни приемлемым.

Благодаря недавним инновациям стало возможно регистрировать и сохранять все события маршрутизации и рассчитанные пути трафика в высокопроизводительной базе данных. Поэтому стало возможно воспроизводить события маршрутизации и трафика для диагностики первопричин проблем. Например, можно «перемотать назад» время в сети до момента, когда канал стал перегружен, и проанализировать трафик в канале. Можно увидеть, откуда и куда шел этот трафик, какой путь он использовал, а главное – какие политики нужно применить, чтобы избежать подобных перегрузок.

Правильный анализ пиринга

Благодаря развитию технологий аналитики трафика и маршрутизации провайдеры могут устанавливать и поддерживать такие пиринговые отношения, которые им наиболее выгодны. Полная информированность о трафике – в том числе и о точных путях каждого потока в сети – и интерактивное моделирование изменений помогают снизить затраты на транзит и повысить качество обслуживания. Инженеры и планировщики могут увидеть объемы трафика BGP по каждому пиру, его источники и пункты назначения, точки входа и выхода, транзитные AS в реальном времени и в каждый прошедший момент. Операционный мониторинг в реальном времени и исторический анализ помогают NOC своевременно управлять доставкой сервисов, профилактически решая проблемы. Возможности моделирования позволяют точно прогнозировать эффект предлагаемых изменений на трафик, снижая вероятность ошибок планирования и конфигурации.

Источник: PacketDesign



Применение Multipath TCP

Оливер Бонавентуре, Сунгхун Сео
(Olivier Bonaventure, SungHoon Seo)

Протокол MPTCP (Multipath Transmission Control Protocol), описанный в RFC 6824 (https://datatracker.ietf.org/doc/rfc6824/), стал новейшим расширением заслуженного протокола TCP. TCP был создан тогда, когда у хостов был один сетевой интерфейс и один IP-адрес. Каждое соединение TCP идентифицируется четверкой данных (исходный и целевой адреса, исходный и целевой порты), и каждый пакет, относящийся к этому соединению, содержит эту четверку. Несмотря на юный возраст, Multipath TCP уже массово используется в коммерческих сервисах. На смартфонах он комбинирует сотовые сети и сети Wi-Fi, повышая пропускную способность и ускоряя работу приложений, чувствительных к задержке.

Протокол MPTCP (Multipath Transmission Control Protocol), описанный в RFC 6824 (https://datatracker.ietf.org/doc/rfc6824/), стал новейшим расширением заслуженного протокола TCP. TCP был создан тогда, когда у хостов был один сетевой интерфейс и один IP-адрес. Каждое соединение TCP идентифицируется четверкой данных (исходный и целевой адреса, исходный и целевой порты), и каждый пакет, относящийся к этому соединению, содержит эту четверку. После установки соединения TCP невозможно изменить ни один из элементов четверки, не разорвав соединение, а в современных сетях это обстоятельство превращается в существенное ограничение по следующим причинам:

Многие хосты поддерживают одновременно IPv4 и IPv6. Даже если интерфейс у них один, адресов оказывается два и более, и между каждой парой обменивающихся данными хостов есть несколько сетевых маршрутов.

У многих хостов по нескольку интерфейсов (смартфоны, планшеты и пр.).

Сегодня в Интернете все возрастает количество мобильных хостов, чьи адреса могут изменяться при переходе из одной беспроводной сети в другую.

Multipath TCP решает эти проблемы, дополняя TCP таким образом, что обмен данными, относящимися к одному соединению, становится возможен по различным маршрутам. Для этой цели Multipath TCP комбинирует несколько соединений TCP (названных в RFC 6824 субпотоками – subflow) в одно соединение Multipath TCP. Первый субпоток начинается с тройственного рукопожатия, как и обычное соединение TCwP. Основное отличие в том, что пакет SYN содержит опцию MP_CAPABLE, которая задает использование Multipath TCP и случайных ключей.

Как только первый субпоток установлен, любой из хостов, участвующих в коммуникации, может создать дополнительный субпоток с любого из своих адресов на любой адрес удаленного хоста, отправив новый SYN с опцией MP_JOIN. Такие субпотоки могут создаваться и закрываться в любой момент, что очень важно для мобильных хостов. Данные можно передавать по любому из субпотоков, входящих в соединение Multipath TCP в данный конкретный момент. Если субпоток перестал работать, то все данные, которые передавались по нему и до сих пор не подтверждены, будут повторно переданы по другим субпотокам. (Для получения дополнительных сведений о Multipath TCP см. RFC 6824 или NSDI '12.[1])

Сегодня существует несколько независимых реализаций Multipath TCP, совместимых друг с другом. Самые распространенные – iOS/macOS и Linux (https://www.multipath-tcp.org). Multipath TCP поддерживается балансировщиками нагрузки, а также ведутся работы по внедрению протокола на FreeBSD и Solaris. В настоящей статье описан ряд коммерческих сервисов, использующих уникальные возможности Multipath TCP.

Смартфоны

Самая масштабная реализация Multipath TCP – для смартфонов.

Сквозная реализация Multipath TCP

Смартфоны часто подключены сразу и к точке доступа Wi-Fi, и к сотовой сети. Если пользователь подключен к Интернету по Wi-Fi и выходит из зоны досягаемости точки доступа Wi-Fi, то смартфон теряет подключение, а значит, TCP-соединение по Wi-Fi тоже «отваливается». Одним из преимуществ Multipath TCP является способность без труда переключаться с одного интерфейса на другой, это делает его лучшим кандидатом на решение подобных проблем со связью (рис. 1).

Siri – электронный помощник в операционных системах Apple iOS и macOS. Поскольку распознавание речи требует огромной вычислительной мощности, Siri передает голосовые команды потоком в центр данных Apple для распознавания, а потом получает от него результат. Хотя длительность взаимодействия пользователя с Siri относительно невелика, паттерн использования помощника делает Siri идеальным клиентом для MPTCP.

Многие используют Siri на ходу или в машине. По мере того как пользователь удаляется от точки доступа Wi-Fi, TCP-соединение, по которому Siri передает голосовую команду, в конце концов, разрывается, и вместо ожидаемого результата хозяин смартфона получает сообщение об ошибке.

Чтобы решить эту проблему, Apple использует MPTCP, начиная с версии iOS 7. Когда пользователь отдает голосовую команду Siri, iOS устанавливает MPTCP-соединение по Wi-Fi и сотовой связи. Если телефон теряет соединение с точкой доступа Wi-Fi, трафик перенаправляется по сотовому интерфейсу. Бывает так, что Wi-Fi-соединение, не разрываясь, теряет качество настолько, что по нему практически ничего нельзя передать. В этом случае происходит еще один тайм-аут повторной передачи, и iOS перенаправляет трафик по сотовому каналу.

Чтобы еще больше снизить задержку, iOS измеряет значения круговой задержки (RTT) на двух интерфейсах. Чудовищная задержка часто образуется в случае излишней буферизации (bufferbloat). У канала Wi-Fi значение RTT может быть гораздо выше, чем у сотового канала. Когда iOS обнаруживает, что RTT у Wi-Fi значительно выше, чем у сотового канала, она направляет голосовой поток через сотовый интерфейс.

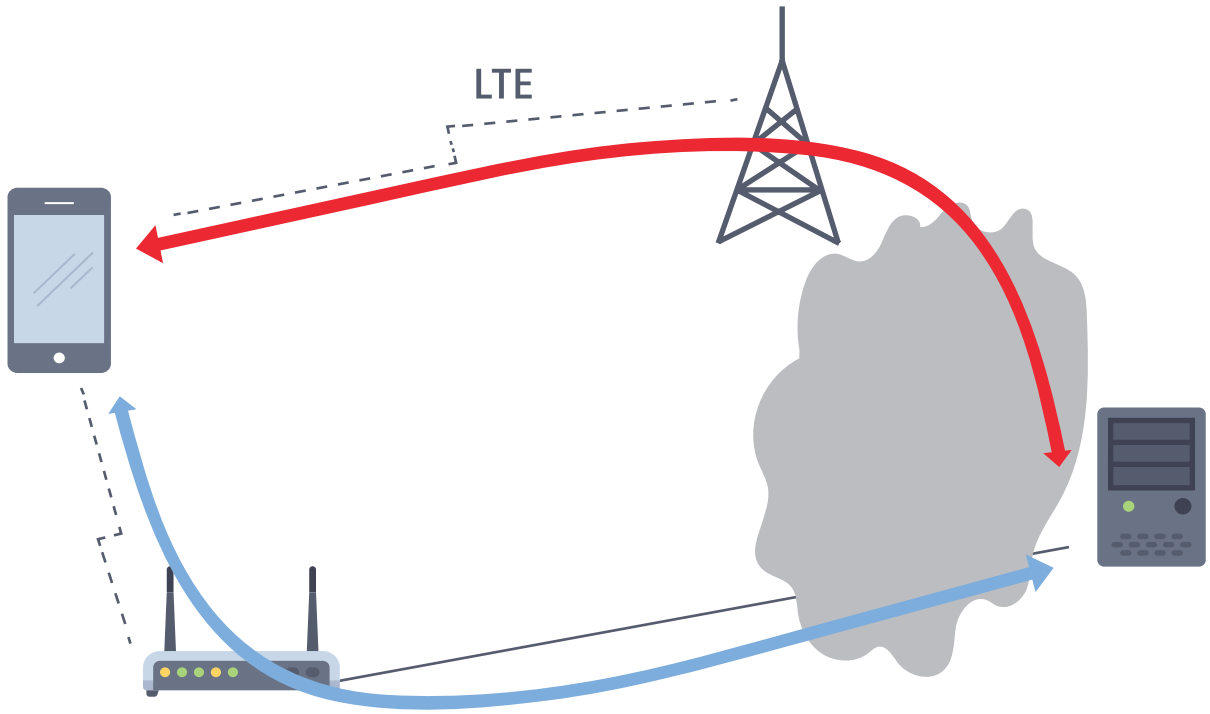
И, наконец, используется ввод Wi-Fi Assist (https://support.apple.com/en-us/HT205296) и триггер для переключения на сотовый интерфейс. Для пользователей Siri внедрение MPTCP обернулось значительным сокращением числа сетевых ошибок. После создания двух субпотоков (один – по Wi-Fi, второй – по сотовой сети) количество сетевых ошибок сократилось на 80%.

Благодаря измерению RTT и смене субпотока по его результатам Siri также стал быстрее реагировать на команды пользователя. Теперь Siri может обрабатывать команды пользователя на 20% больше в 95-й перцентили и на 30% больше в 99-й перцентили.

Развертывание MPTCP в Интернете произошло практически безболезненно. Способность MPTCP справляться с помехами от промежуточных устройств и потом возвращаться к обычному TCP оказалась полезной и не обнаружила крупных проблем. Однако примерно 5% соединений по-прежнему возвращаются к обычному TCP, вследствие внедрения прозрачных TCP-прокси в сотовых сетях и убирания опций MPTCP брандмауэрами.

Одна из проблем MPTCP – это трудность отладки. Обработка субпотоков связана со значительной сложностью кода: интерфейсы Wi-Fi появляются и пропадают. В некоторых сетях имеются промежуточные устройства, которые вмешиваются в работу MPTCP, что делает невозможным создание субпотоков. Пограничные сценарии, которые трудно воспроизвести и которые реализуются только тогда,

Рис. 1. Иллюстрация пользования несколькими интерфейсами одновременно.



когда продукты развертываются в огромных количествах, требуют основательного механизма журналирования для того, чтобы отследить поведение MPTCP-соединения.

Из-за неопределенностей, вносимых в сеть промежуточными устройствами, крайне трудно выявить истинные причины проблем. В результате не всегда можно разграничить программные ошибки и вмешательство промежуточного устройства.

Multipath TCP поверх прокси SOCKS

Помимо серверов, развертываемых именно для предыдущего сценария, очень немного серверов уже поддерживают Multipath TCP. Несмотря на это, ряд сетевых операторов стремится повысить быстродействие для пользователей смартфонов, комбинируя существующие сотовые и Wi-Fi-сети. Сетевые операторы в нескольких странах полагаются на SOCKS (RFC 1928, https://datatracker.ietf.org/doc/rfc1928/), чтобы одновременно использовать Wi-Fi-сети и сотовые сети. С точки зрения оператора, основным преимуществом совмещения SOCKS и MPTCP является легкость в развертывании, поскольку в существующей основной инфраструктуре сотовых сетей и Wi-Fi практически не существует зависимостей (https://www.ietf.org/proceedings/93/slides/slides-93-mptcp-3.pdf).

Ряд моделей коммерческих смартфонов на платформе Android содержат реализацию Multipath TCP в ядре Linux и в клиенте SOCKS. Клиент SOCKS, выполняемый на смартфоне, перехватывает любые попытки подключения по TCP к далеким серверам. Затем он создает подключение к серверу SOCKS, управляемому сетевым оператором.

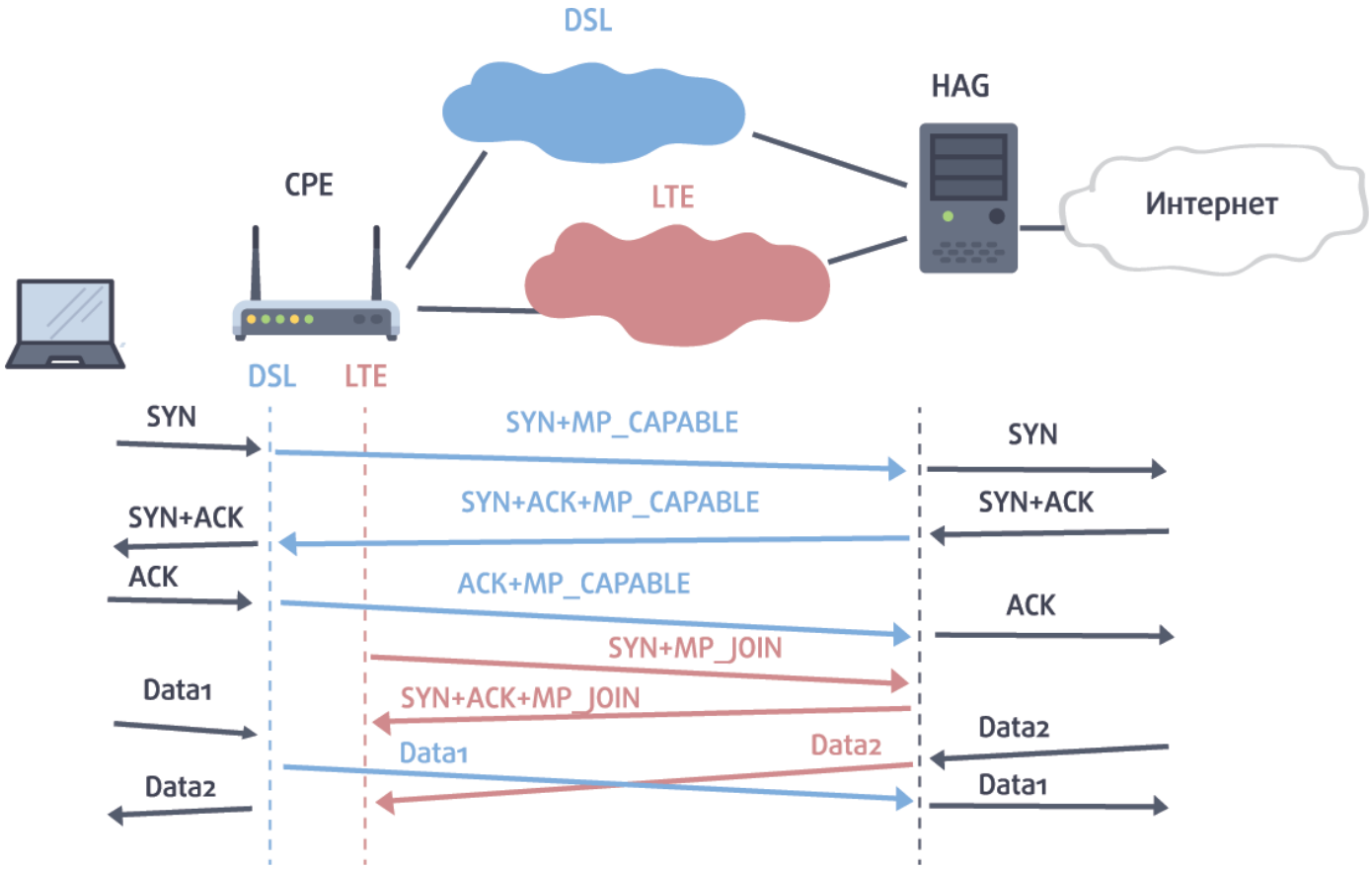
После аутентификации пользователя клиент SOCKS отправляет команду на сервер SOCKS, который создает подключение TCP с удаленным сервером. В этот момент существует соединение Multipath TCP между смартфоном и сервером SOCKS и соединение TCP между сервером SOCKS и удаленным сервером. Сервер SOCKS пересылает все данные, отправленные по соединению Multipath TCP, по соединению TCP и наоборот. Смартфоны создают дополнительные субпотоки в направлении сервера SOCKS через другие доступные интерфейсы. Результатом становится большее удобство для пользователя, за счет агрегирования пропускной способности и гладкого переключения субпотоков.

Гибридные сети доступа

Еще один важный сценарий использования Multipath TCP – это сети доступа. Во многих регионах мира имеющиеся сети доступа ограничивают полосу пропускания. Типичный пример – сельская местность, где для сетевых операторов очень затратно развертывать сети доступа с большой полосой пропускания. Даже если полоса пропускания сети доступа ограничена, часто можно подписаться на другие сетевые сервисы, которые в комплексе дают большую полосу пропускания и надежность.

Несколько компаний развернули решения, которые используют уникальные возможности Multipath TCP. Одна использует прокси SOCKS и позволяет конечным

Рис. 2. Установка сеанса Multipath TCP.



пользователям эффективно комбинировать сетевые сервисы различных провайдеров. Вторая нацелена на сетевых операторов, которые хотят объединить проводные (например, xDSL) и беспроводные (например, LTE) сети, чтобы предоставить потребителям большую пропускную способность (https://www.broadband-forum.org/technical/download/TR-348.pdf).

Комбинирование сетей доступа с помощью SOCKS

SOCKS также используется совместно с Multipath TCP для комбинирования различных сетей доступа. В этой инсталляции конечными пользователями являются обычные хосты, не поддерживающие Multipath TCP. Чтобы можно было воспользоваться возможностями Multipath TCP, в LAN конечного пользователя устанавливается промежуточное оборудование. Оно выступает в роли клиента SOCKS и взаимодействует с сервером в облаке. И промежуточное оборудование, и облачный сервер используют Multipath TCP, а следовательно, могут работать с любыми доступными сетями доступа, если промежуточному оборудованию присвоен IP-адрес в каждой из сетей доступа.

Как правило, промежуточное оборудование выступает в роли шлюза по умолчанию для LAN конечного пользователя. Оно перехватывает все пакеты TCP, которые хосты в LAN отправляют вовне, и затем по прокси передает их по каналам Multipath TCP на сервер SOCKS, находящийся в облаке. Этот сервер закрывает соединения Multipath TCP и открывает обычные соединения TCP с конечными точками пакетов.

Это решение уже находится в коммерческой эксплуатации в двух странах. Пользователи сообщают об успешном комбинировании различных типов ссылок доступа, включая xDSL (от ADSL до VDSL), DOCSIS, 3G, 4G и спутниковые каналы.

Multipath TCP в гибридных сетях доступа

Некоторые сетевые операторы развернули как проводные (например, xDSL), так и беспроводные (например, LTE) сети и желают комбинировать их, чтобы предлагать большую пропускную способность. Multipath TCP также может использоваться для оказания таких услуг (рис. 2).

В этой инсталляции Multipath TCP не поддерживается ни клиентом, ни сервером. Multipath TCP используется на конечном пользовательском оборудовании (Customer Premise Equipment, CPE) и гибридном агрегирующем шлюзе (Hybrid Aggregation Gateway, HAG), находящемся в центре данных сетевого оператора, который управляет обеими сетями доступа (https://datatracker.ietf.org/doc/draft-peirens-mptcp-transparent/).

Когда клиент открывает TCP-соединение с удаленным сервером, он отправляет пакет SYN. Этот пакет перехватывается CPE, который виртуально терминирует соединение TCP и затем добавляет опцию MP_CAPABLE в TCP-пакет, перед тем как переслать его по сети xDSL. HAG, находящийся на пути, по которому проходят все пакеты, отправляемые клиентом по сети xDSL, перехватывает пакет SYN. Он виртуально терминирует соединение Multipath TCP и затем пересылает SYN серверу, удалив опцию MP_CAPABLE. После этого сервер подтверждает установку соединения, отправив SYN+ACK. HAG перехватывает и этот пакет, обновляет его статус для этого соединения и добавляет опцию MP_CAPABLE, а затем пересылает его на CPE. CPE действует аналогично. Он обновляет состояние пакета и пересылает SYN+ACK на клиента (отрезав опцию MP_CAPABLE), чтобы подтвердить установку соединения. В этот момент открыто три соединения TCP. Первое – обычное соединение TCP. Оно начинается на клиенте и виртуально терминируется на CPE. Второе – соединение Multipath TCP, которое виртуально терминируется на CPE и HAG. Третье – опять же обычное соединение TCP между HAG и удаленным сервером. С операционной точки зрения важно отметить, что при использовании IPv6 ни CPE, ни HAG не нужно транслировать адреса исходного и целевого хостов в пересылаемых TCP-пакетах. IP-адрес клиента остается виден целевому серверу. Это важное преимущество по сравнению с решениями на базе SOCKS.

Кроме того, в этой структуре соединение между клиентом и сервером можно создать в рамках времени приема-передачи (round trip time).

Выводы

Несмотря на юный возраст, Multipath TCP уже массово используется в коммерческих сервисах. На смартфонах он комбинирует сотовые сети и сети Wi-Fi, повышая пропускную способность и ускоряя работу приложений, чувствительных к задержке. В сетях доступа он поддерживает гибридные сети доступа, которые повышают удобство для пользователя, эффективно комбинируя существующие проводные и беспроводные сети.

Ссылки

1. Raiciu, C., Paasch, C., Barré, S., Ford, A., Honda, M., Duchêne, F., Bonaventure, O., Handley, M., “How Hard Can It Be? Designing and Implementing a Deployable Multipath TCP”, USENIX Symposium of Networked Systems Design and Implementation (NSDI ’12), апрель 2012 г.

БЛАГОДАРНОСТИ

Авторы благодарят Кристофа Пааша (Christoph Paasch) и Саймона Леливра (Simon Lelievre).

Источник: Multipath TCP Deployments

Оптимизация маршрутизации трафика

Елена Воронина, Мадина Касенова

Оптимизация маршрутизации трафика – «оптимизация» правового регулирования: Динамика развития любых общественных отношений всегда опережает их правовое регулирование, а достижение полного соответствия регулирования содержанию «опосредуемых правом» отношений, по сути, недостижимо. Законодатель практически всегда решает вопрос о том, необходимо ли регулировать те или иные общественные отношения с помощью права, и, исходя из содержания конкретных отношений, как правило, стоит перед выбором правовых форм и методов, которые будут адекватно и эффективно их регулировать.

Динамика развития любых общественных отношений всегда опережает их правовое регулирование, а достижение полного соответствия регулирования содержанию «опосредуемых правом» отношений, по сути, недостижимо. Законодатель практически всегда решает вопрос о том, необходимо ли регулировать те или иные общественные отношения с помощью права, и, исходя из содержания конкретных отношений, как правило, стоит перед выбором правовых форм и методов, которые будут адекватно и эффективно их регулировать.

Происходящий объективный процесс «интернетизации» государств обусловлен стремительным развитием интернет-технологий, которые изменяют географию распространения Интернета и аудиторию интернет-пользователей, расширяя тем самым социальные сферы применения Интернета. В свою очередь этот процесс, с одной стороны, диверсифицирует правовое регулирование значительного числа существующих отношений и на национальном, и на международном уровне. С другой стороны, расширение социальных сфер применения Интернета актуализирует необходимость решения вопроса о том, какие «новые» общественные отношения, возникающие в сфере функционирования и использования Интернета, следует регулировать, и каковы должны быть формы и методы такого регулирования.

Сложность правового регулирования отношений, связанных с Интернетом, заключается в том, что Интернет не представляет собой «единый и целостный» объект регулирования. Фундаментальным свойством проектирования технологической инфраструктуры Интернета является многоуровневая структурированность, которая позволяет объединять в рамках одной сети – Интернета – множество разных сетей, соединение которых, в свою очередь, и образует трансграничную глобальную сеть Интернет, позволяя пользователям различных сетей взаимодействовать и обмениваться данными/контентом. По сути, Интернет – это «сеть сетей», т.е. глобальная сеть объединенных «автономных/независимых» сетей.

Многообразие и разность сетей определяется тем, что все они создавались в разное время, спроектированы и функционируют на различных технологических принципах, их назначение и внутрисистемные связи «не совпадают», они располагаются в разных географических точках, отличаются масштабом (местные, локальные, региональные, трансграничные) и т.д. В итоге, пользователи одной сети не могут взаимодействовать с пользователями другой сети, если эта сеть не установит соединения с глобальной сетью и не будет при этом соблюдать технологические «правила игры».

Интернет спроектирован и обладает такой технологической инфраструктурой, которая «создает единое поле» взаимосвязанности и взаимодействия, к примеру, магистральных сетей (backbones); сетей доставки контента (Content Delivery Networks, CDN), мобильных широкополосных сетей (broadband networks) и т.д. В этом смысле способы установления связанности разных сетей имеют фундаментальное значение.

Множество и разность составляющих Интернет сетей определяет разнообразие круга сетевых операторов, к которым относятся, в частности, провайдеры сетей доставки контента (CDN Provider); провайдеры интернет-услуг (Internet Service Provider, ISP); контент-провайдеры (Content Providers); региональные провайдеры транзитных услуг (Regional Transit Providers, RTP) и т.д. При этом сетевыми операторами выступают организации, созданные в разных организационно-правовых формах, относящиеся, в том числе, к различным правопорядкам, действующие как в одной, так и в нескольких юрисдикциях, как являющиеся собственниками автономных сетей, так и не являющиеся таковыми.

Исключительно в рамках глобальной сети Интернет разнообразные сети могут взаимодействовать между собой

и обеспечивать передачу контента/данных пользователей/пользователям таких сетей. Возможность взаимодействия разных сетей в Интернете обеспечивает технологическая инфраструктура Интернета, функционирование которой обеспечивают уникальные идентификаторы Интернета и стек протоколов TCP/IP (и их последующее расширение). Технологическая инфраструктура Интернета является многоуровневой и зиждется на фундаментальных принципах, отражающих сущность проектирования сети Интернет: это архитектурные принципы Интернета (Architectural Principles of the Internet) и «принцип уровней» (Layer Principle).

Архитектурные принципы Интернета закреплены в документе RFC1958 Architectural Principles of the Internet. В соответствии с нормативными положениями RFC 1958, «Конечный результат функционирования сети Интернет является главным. Задача сети заключается в наиболее эффективной и гибкой передаче дейтаграмм. Все остальное должно осуществляться оконечными устройствами». В ряду основных архитектурных принципов технического проектирования Интернета принцип сквозной связи (end-to-end principle, e2e) является основополагающим, поскольку цель – обеспечение передачи контента/данных от отправителя к получателю.

Отражением фундаментальных основ проектирования технологической инфраструктуры Интернета выступает принцип уровней (Layer Principle). Технологическая инфраструктура Интернета охватывает физические каналы связи и компьютерное оборудование; программные и технические средства, обеспечивающие взаимодействие базовых компонентов Интернета, маршрутизирующих передачу данных; собственно сами интернет-ресурсы в виде веб-сайтов, социальных сетей, служб электронной почты, систем поиска и передачи информации и т.д. Уровни технологической инфраструктуры Интернета функционально связаны и иерархически «вертикально» структурированы. С точки зрения системных связей между инфраструктурными уровнями, выделяют несколько уровней, которые представлены в двух архитектурных типах, а именно: эталонной модели OSI и эталонной модели TCP/IP. Вместе с тем, в обеих моделях транспортный уровень (Transport Layer), на котором обеспечивается передача контента/данных между оконечными устройствами (End Systems), рассматривается в качестве ключевого .

Установление функциональных связей разнообразных сетей в рамках единой, глобальной сети – сети Интернет – обеспечивают уникальные идентификаторы технологической инфраструктуры Интернета, к числу которых относятся номерные ресурсы Интернета и система доменных имен. Номерные ресурсы Интернета, как уникальные идентификаторы, охватывают адреса интернет-протокола (IP-address), номера автономных систем (Autonomous System Numbers ASN), номера портов протоколов и значения параметров.

Пиринг происходит от английского слова «Peer», наиболее адекватный контекстный перевод которого – «пользователь, равный по положению и уровню», одновременно передающий и получающий данные/контент; кроме того, «Peer» также означает одноранговую сеть/одноранговый узел. Понятие «пиринг» терминологически используется достаточно широко, однако оно содержательно не определено. Нет определения понятия «пиринг», в том числе и в документах организации Internet Engineering Task Force (IETF), например, в RFC 1983 Internet User's Glossary , который содержит понятийно-категориальный аппарат ключевых терминов Интернета.

Сетевые операторы самостоятельно определяют технические способы и условия установления межсетевого взаимодействия друг с другом с тем, чтобы обеспечить связь между конечными пользователями таких сетей, а также для доставки данных/контента. Тип сети, возможности технологической инфраструктуры сети, ее масштаб, правовой статус сетевого оператора и т.д. выступают для сетевого оператора определяющими факторами выбора технических, коммерческих, организационно-правовых «стратегий присоединения» и взаимодействия с другими сетями, оптимизирующих маршрутизацию трафика для обмена данными/контентом пользователей таких сетей. Межсетевое взаимодействие и связанность разных сетей обеспечивается посредством двух основных механизмов: «пиринг» (Peering) и «транзит» (Transit).

В настоящее время в условиях усложнения интернет-отношений, разнообразия связей между сетевыми операторами (двусторонние и многосторонние, локальные, региональные, трансграничные и т.д.) актуализируется вопрос о так называемом пиринге для контента (Peering for Content) между интернет-провайдерами (ISP), поскольку оптимизация стоимости связи доставки контента становится

если не первоочередной, то ключевой. Вместе с тем, в формате статьи целесообразно остановиться на пиринге как таковом.

Что такое пиринг (peering).

Пиринг происходит от английского слова «Peer», наиболее адекватный контекстный перевод которого – «пользователь, равный по положению и уровню», одновременно передающий и получающий данные/контент; кроме того, «Peer» также означает одноранговую сеть/одноранговый узел. Понятие «пиринг» терминологически используется достаточно широко, однако оно содержательно не определено. Нет определения понятия «пиринг», в том числе и в документах организации Internet Engineering Task Force (IETF), например, в RFC 1983 Internet User's Glossary , который содержит понятийно-категориальный аппарат ключевых терминов Интернета.

Wikipedia, например, предлагает следующее определение этого понятия: «при использовании компьютерных сетей для передачи данных, пиринг – это добровольное (безвозмездное) взаимное соединение в Интернете административно независимых сетей для целей обмена трафиком между пользователями каждой сети» . Кембриджский словарь бизнес-лексики определяет пиринг как «способ межсетевого подключения отдельных сетей друг к другу для того, чтобы пользователи разных сетей могли свободно взаимодействовать друг с другом для обмена контентом. Пиринг осуществляется между владельцами сетей на добровольной основе и предоставляется бесплатно пользователям». Представляется, что такое определение понятия «пиринга» точнее отражает его содержание как технического термина.

Эволюция Интернета, несомненно, повлияла на понятийно-терминологическое использование пиринга, который приобрел множество оттенков и в настоящее время аккумулирует технические, финансовые аспекты, включая «пиринговые политики» провайдеров сетей.

Для осуществления межсистемного взаимодействия различных сетей в практическом плане в рамках пирингового соединения необходимо установление «физического» местонахождения конкретного оборудования, обеспечивающего техническое подключение отдельных сетей друг к другу для обмена трафиком. За последнее десятилетие различные сетевые операторы почти во всех регионах развернули множество центров размещения сетевого оборудования, которые обеспечивают сетевые соединения - так называемые точки обмена интернет-трафиком (Internet eXchange Point, IXP).

При этом пиринговое соединение сетей (двух и более) осуществляется посредством их «физического» соединения, а маршрутизация данных осуществляется с использованием протокола BGP .

Следует заметить, что выражение «обмен трафиком» носит скорее образный характер. По сути, сети организуют технологическую «общую точку», которая дает возможность маршрутизирующим устройствам выбрать наиболее короткий, оптимальный путь. Как правило, пиринговые стыки организуют с избыточной пропускной способностью, что позволяет эффективно бороться с сетевыми задержками и оперативно наращивать емкость сети. В этом контексте, сетевые соединения – IXP – являются важным инфраструктурным элементом Интернета, способствующим улучшению локальной связанности и скорости доступа к информационным ресурсам сети.

Интернет, как «сеть сетей», объединяет тысячи разных сетей (локальных, региональных, трансграничных и т.д.), в том числе взаимодействующих между собой посредством пиринга.

Пиринговое межсетевое взаимодействие (Peering Arrangement) и пиринговые соглашения (Peering Agreement)

Пиринг – как взаимное соединение и взаимодействие двух и более сетей – имеет определенные преимущества. Наиболее очевидными преимуществами использования пиринга является, в частности, возможность прямого подключения сетей между собой, что оптимизирует маршруты трафика, способствуя улучшению локальной связанности и оптимизации расходов операторов.

Пиринговое межсетевое взаимодействие (Peering Arrangement) вариативно. Но вариативность использования пиринга определяется такими факторами, как согласие на взаимное подключение другой сети (нескольких сетей), размер сети и объем трафика в рамках сети, масштаб клиентской базы, технические возможности и наличие соответствующей инфраструктуры подключения и проч. Помимо этих факторов, на вариативность использования пиринга влияет существование нескольких типов пиринговых соединений, а именно: публичный пиринг (Public Peering) и частный пиринг (Private Peering).

Публичный пиринг – межсетевое взаимодействие, осуществляемое посредством IXP, при котором сети-пиры, используя одно или несколько физических соединений, подключаются друг к другу. Публичный пиринг позволяет сетям-пирам обмениваться трафиком между собой с использованием одного соединения, что увеличивает производительность сети и оптимизирует расходы.

Частный пиринг (Private Peering) – межсетевое взаимодействие, осуществляемое посредством прямого физического соединения между двумя сетями без подключения «к оборудованию точки обмена». При частном пиринге, как правило, одна сеть подключается к другой в одном и том же здании, для маршрутизации трафика. В рамках частного пиринга выделяют «частичный пиринг» (Partial Peering), именуемый также «региональным пирингом» (Regional Peering).

Частичный пиринг является вариантом пирингового обмена, при котором автономные сети обмениваются трафиком только между конкретным кругом пользователей в определенном регионе. Поскольку при пиринге автономные сети обеспечивают обмен всем трафиком с любым из своих пользователей, независимо от его местонахождения в сети, глобальный сетевой узел, охватывающий, например, локальные сети в Швеции, может посредством пирингового соединения обеспечить трафик только для «своих шведских» пользователей. Частичный пиринг, таким образом, позволяет оптимизировать затраты, т.к. обеспечивает трафиком только «шведскую сеть», а также создает условия для оптимальной передачи локального трафика между региональными пользователями.

Разнообразие типов пиринговых соединений обусловливает и различия в договорах/соглашениях, которые регулируют взаимодействия субъектов пиринговых отношений. Сложность анализа договоров, предметом которых выступает пиринг, является то, что они заключаются между организациями, являются субъектами частного права, носят конфиденциальный характер и, как правило, содержат «оговорку о неразглашении». Некоторые подробности договорных условий обнаруживаются при возникновении судебных разбирательств или, к примеру, если в годовые отчеты компаний включена соответствующая информация. Стоит также отметить, что согласно обзору пиринговых отношений, подготовленному компанией PCH в 2016 году, большинство соглашений носит неформальный характер.

Сетевые операторы заключают пиринговые соглашения (Peering Agreement) главным образом в целях экономии затрат на «достаточность трафика», а также в целях улучшения связанности сети, т.е. «связанность» выступает одним из ключевых показателей качества услуг, предоставляемых сетевым оператором. При этом для пользователей пиринг, по сути, «остается за кадром», т.к. не является некой отдельной/самостоятельной услугой, а инкорпорирован в состав услуг, предоставляемых сетевым оператором своим пользователям.

Пиринговые соглашения, как правило, квалифицируются как безвозмездные , однако такая оценка носит достаточно «обобщенный» характер, в том числе потому, что условия и обязательства таких соглашений сформулированы по-разному.

Общедоступная российская правовая база «Консультант» (СПС «Консультант Плюс») предлагает следующую «типовую договорную форму», названную «Договор обмена интернет-трафиком» . Сторонами этого договора обозначены «Оператор 1» и «Оператор 2», которые «одновременно являются участниками обменного узла (_xxx_) пиринговой сети». При этом указанный обменный узел является для сторон такого договора «точкой взаимного обмена трафика между собственными сетями».

Предмет договора обмена интернет-трафиком сформулирован достаточно неоднозначно:

- стороны обеспечивают взаимодействие сетей на технических условиях с возможностью прямой передачи трафика от одного адресного пространства, принадлежащего Оператору 1, в адресное пространство, принадлежащее Оператору 2, а также от адресного пространства Оператора 2 в адресное пространство Оператора 1 через обменный узел (_xxx_) пиринговой сети с применением статической маршрутизации IP-пакетов;
- стороны устанавливают необходимые статические маршруты на своих маршрутизаторах, включенных в обменный узел (_xxx_) пиринговой сети;
- Оператор 1 устанавливает в сторону Оператора 2 статические маршруты на следующие префиксы IP-сетей: (_xxx_), через шлюз (_xxxx_);

- Оператор 2 устанавливает в сторону Оператора 1 статические маршруты на следующие префиксы IP-сетей: (_xxx_), через шлюз (_xxx_);

- стороны поддерживают статические маршруты, указанные в п.п. 1.4-1.5, со своей стороны в полном объеме и постоянно, пока действует данный договор;

- обмен трафиком между сетями сторон происходит только через обменный узел (_xxx__) пиринговой сети. Стороны договорились установить соответствующие фильтры на своих маршрутизаторах для исключения возможности пропуска трафика по иным путям, кроме указанного в настоящем договоре».

Несколько иначе сформулированы условия «Типового пирингового соглашения» Компьютерного центра Венского Университета. Так, соглашение заключается «в целях взаимосвязи между сетями сторон в Интернете («интернет-пиринг»)», которая осуществляется посредством точки обмена трафиком (Vienna Internet Exchange, VIX), расположенной по адресу (_xxx_).

Предметом пирингового соглашения является обмен трафиком между сетью (_xxx_) и его членами (_xxx_), а также их клиентами или связанными с ними компаниями. В рассматриваемом типовом пиринговом соглашении сформулирован целый ряд технических условий взаимосвязи между сетями. В числе которых отметим следующие:

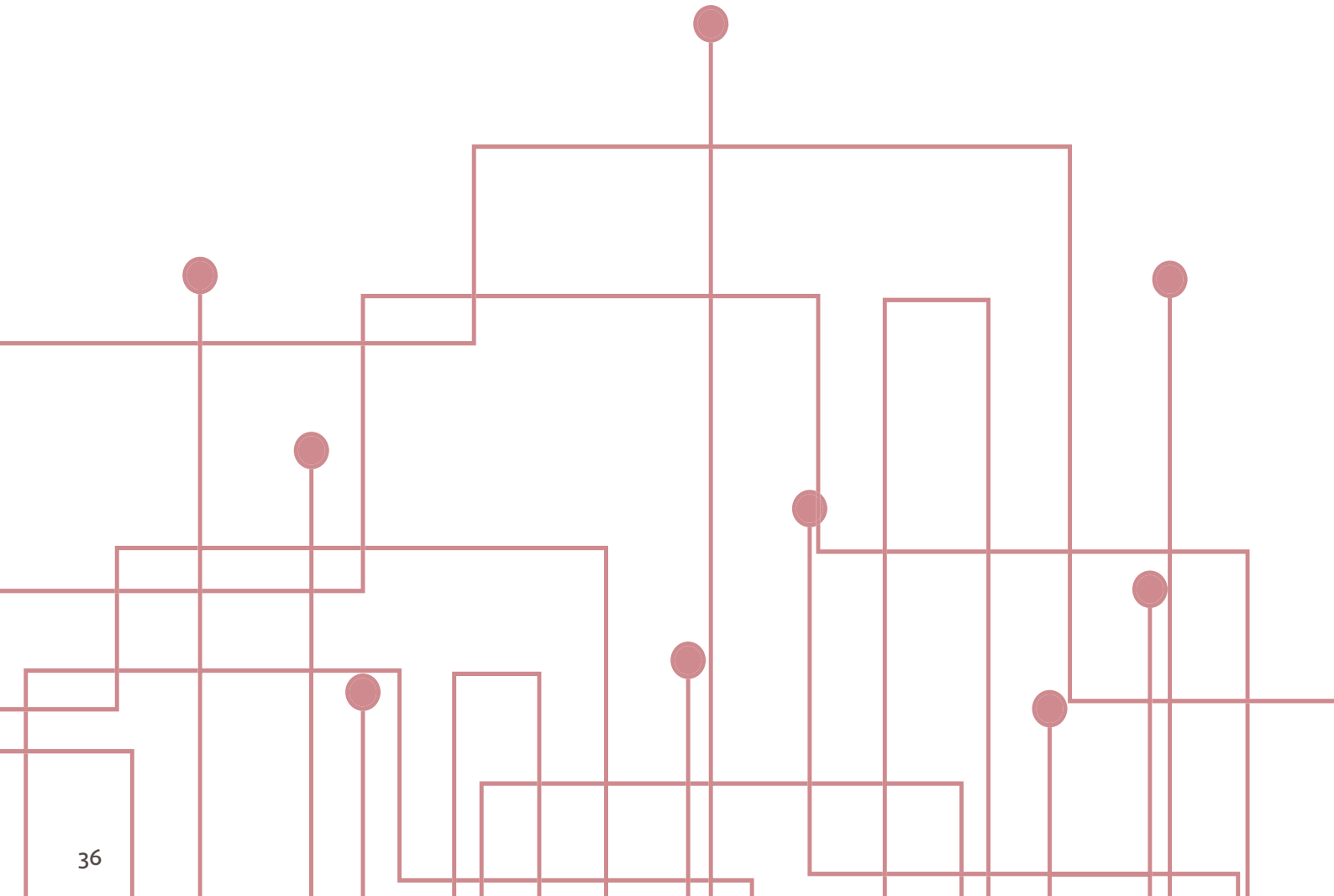
- каждая сторона оплачивает свои собственные расходы по обеспечению пропускной способности маршрутизации и аппаратных систем на своих оконечных устройствах/линиях связи;

- расходы на подключение каждой из сторон к точке обмена (VIX), включая расходы на установку (расходы на монтаж) и текущие эксплуатационные издержки, оплачиваются каждой стороной индивидуально;

- пиринговое соединение между двумя сетями осуществляется через протокол пограничных шлюзов (BGP);

- вся маршрутизация и обмен данными, а также регулирующая политика маршрутизации регистрируются в реестре RIPE.

Пиринговые межсетевые соединения так или иначе нуждаются в определенной инфраструктуре, а подключение (соединение) к конкретной сети может потребовать расходов сетевого оператора. При заключении пирингового соглашения такие расходы, как правило, возлагаются на стороны (сетевых операторов) заключаемого соглашения.



Некоторые выводы вместо заключения

Интернет, как «сеть сетей», обладает такой технологической инфраструктурой, которая позволяет осуществлять взаимодействие разных сетей. Соответственно, правовое регулирование, игнорирующее тот факт, что Интернет не может быть неким «целостным, единым» объектом регулирования, – рискует быть неадекватным и неэффективным.

Объективные свойства многоуровневой технологической инфраструктуры Интернета, включая функциональную целостность и взаимосвязанность инфраструктурных уровней, радикально отличаются от технологии телефонных и телеграфных сетей. Этот факт целесообразно рассматривать ключевым и определяющим для правового регулирования общественных отношений, связанных со сферой функционирования и использования Интернета, которое не может совпадать и развиваться в контексте и логике архитектуры и эксплуатации телефонных и телеграфных сетей. Иной подход негативно отразится на эффективности правового регулирования отношений в сфере использования Интернета и, следовательно, будет экономически затратным.

Интернет, будучи глобальной (трансграничной) сетью, обеспечивающей взаимодействие разнообразных сетей, основывается на различных коммуникативных механизмах межсетевых соединений. Сетевыми операторами выступают различные организации, созданные в разных организационно-правовых формах, в том числе относящиеся к разным правопорядкам и действующие в разных юрисдикциях. Соответственно, разность механизмов межсетевых соединений, разность круга субъектов (сетевых операторов) порождает возникновение многообразных отношений, основным правовым средством регулирования которых выступает договор. Именно с помощью договора достигается оптимальное сочетание публичных и частных методов регулирования отношений в сфере использования Интернета.

В отличие от телефонной сети со сложившейся общепризнанной моделью отношений (оплата за исходящий трафик), в Интернете направление трафика не позволяет однозначно определить поставщика и потребителя услуги. Это обусловлено многообразием целей и способов передачи информации в Интернете. Пиринг является одной из самых сложных форм таких взаимоотношений, как с экономической точки зрения, так и с точки зрения правового регулирования, не имеющего прямых аналогий с телефонными сетями. В общественных интересах важно, чтобы недостатки в разработанности понятийно-категориального аппарата и инерция «традиционного» мышления законодателей, нередко приводящая к «избыточности правового регулирования», не приводили бы к использованию ненужных ограничений применения Интернета как важнейшего сегмента развития цифровой экономики государства.

Безопасный пиринг

Андрей Робачевский

Известно, что система маршрутизации Интернета уязвима. Любая из порядка 60 ооо участвующих в маршрутизации сетей может попытаться внедрить в систему ложный маршрут, и шансы велики, что он будет принят другими сетями, порой со значительными последствиями. Защищенность конкретной сети зависит от усилий других сетевых операторов. Технологические решения и инструментарий играют существенную роль, но повсеместное внедрение этих практик и технологий в сетях определяет конечный результат. Как защитить себя и глобальную систему маршрутизации – этот вопрос мы рассмотрим в данной статье.

Современная система маршрутизации Интернета сформировалась более 25 лет назад. Результатом перехода от топологии с центральной, ядровой сетью (NSFNET) и подключенных к ней региональных сетей стала многосвязная система независимых равноправных сетей без какого бы ни было центрального контроля. Параллельно произошел переход от изначального протокола маршрутизации EGP к протоколу BGP. Суть его работы была достаточно проста - каждая из сетей сообщала другой сети – пиру – о сетях, которые через нее доступны, путем анонсирования адресного пространства (адресных префиксов) этих сетей. Удивительно, но ни система маршрутизации, ни сам протокол за прошедшее время существенно не изменились.

Однако в 1995 году, когда была стандартизована сегодняшняя версия протокола BGP – BGP-4 (RFC1771, https://datatracker.ietf.org/doc/rfc1771/), Интернет во многом являлся научно-исследовательским проектом, а не глобальной коммуникационной системой, поддерживающей мультимиллиардную цифровую индустрию. Гибкость, простота и производительность, а отнюдь не защищенность и безопасность являлись основными требованиями.

Другими словами, несмотря на свою фундаментальную значимость, протокол BGP основан на доверии между соединенными сетями, принимая полученную от них информацию за чистую монету. Более того, доверие это обладает транзитивным свойством - пиры доверяют своим соседям, те, в свою очередь, - своим, и в итоге все доверяют всем.

Незащищенный BGP

Десять лет спустя, в 2006 году, в IETF были опубликованы два документа: RFC4593 (http://datatracker.ietf.org/doc/rfc4593/), в котором обсуждаются потенциальные угрозы системы маршрутизации, и RFC4272 (http://datatracker.ietf.org/doc/rfc4272/), в котором подробно рассматриваются уязвимые места протокола BGP – основного протокола глобальной системы маршрутизации Интернета.

Суть их сводится к следующему:

- Отсутствие внутреннего механизма, обеспечивающего защиту целостности, свежести и аутентичности сообщений BGP, которыми обмениваются сети-пиры друг с другом. Эта проблема имеет отношение к защите канала между пирами и часто решается локальными средствами.
- Отсутствие механизма для проверки прав автономной системы, или сети, анонсировать префикс.
- Отсутствие механизма для проверки подлинности атрибутов пути, анонсированных сетью-пиром.

Другими словами, несмотря на свою фундаментальную значимость, протокол BGP основан на доверии между соединенными сетями, принимая полученную от них информацию за чистую монету. Более того, доверие это обладает транзитивным свойством – пиры доверяют своим соседям, те, в свою очередь, – своим, и в итоге все доверяют всем.

Поэтому маршруты, полученные от пира, нуждаются в дополнительной проверке, которая не обеспечивается самим протоколом. Проблема усложняется тем, что эти проверки не являются обязательными – они не влияют на функционирование самого протокола. И как следствие – эти проверки используются далеко не повсеместно, делая глобальную систему уязвимой для атак.

Атаки

Уязвимость глобальной системы маршрутизации не обязательно используется с преступной целью. На самом деле большинство случаев искажения желаемой маршрутизации связаны с ошибками конфигурации. Однако эффект от таких ошибок не меньше, а зачастую значительно больше, чем от спланированной атаки.

Несмотря на различие целей и конечного эффекта, механизм атаки принципиально строится на возможности создания искаженной картины топологии Интернета атакуемой сетью, которая затем транзитивно распространяется по всей Сети.

Приведу несколько примеров таких атак и их последствий:

Создание «черных дыр». Целью этой атаки является недоступность сети для всего или части Интернета, другими словами – совершение атаки отказа в обслуживании (Denial of Service, DoS). Атакующая сеть анонсирует адресное пространство других сетей. Весь трафик, имеющий отношение к атакуемой сети, направляется в эту сеть и затем отбрасывается. В результате все сервисы, предлагаемые сетью, становятся недоступными для пользователей. Хрестоматийным примером такой атаки является случай недоступности YouTube (https://www.cnet.com/news/how-pakistan-knocked-youtube-offline-and-how-to-make-sure-it-never-happens-again/).

Захват. По сути не отличается от создания «черных дыр», хотя цели злоумышленников отличаются. Злоумышленники маскируются под атакуемую сеть для проведения краткосрочных акций, например, рассылки спама. После этого такая сеть, или ее фантом, разумеется, исчезает. Часто злоумышленниками используется нераспределенное или давно неиспользуемой адресное пространство.

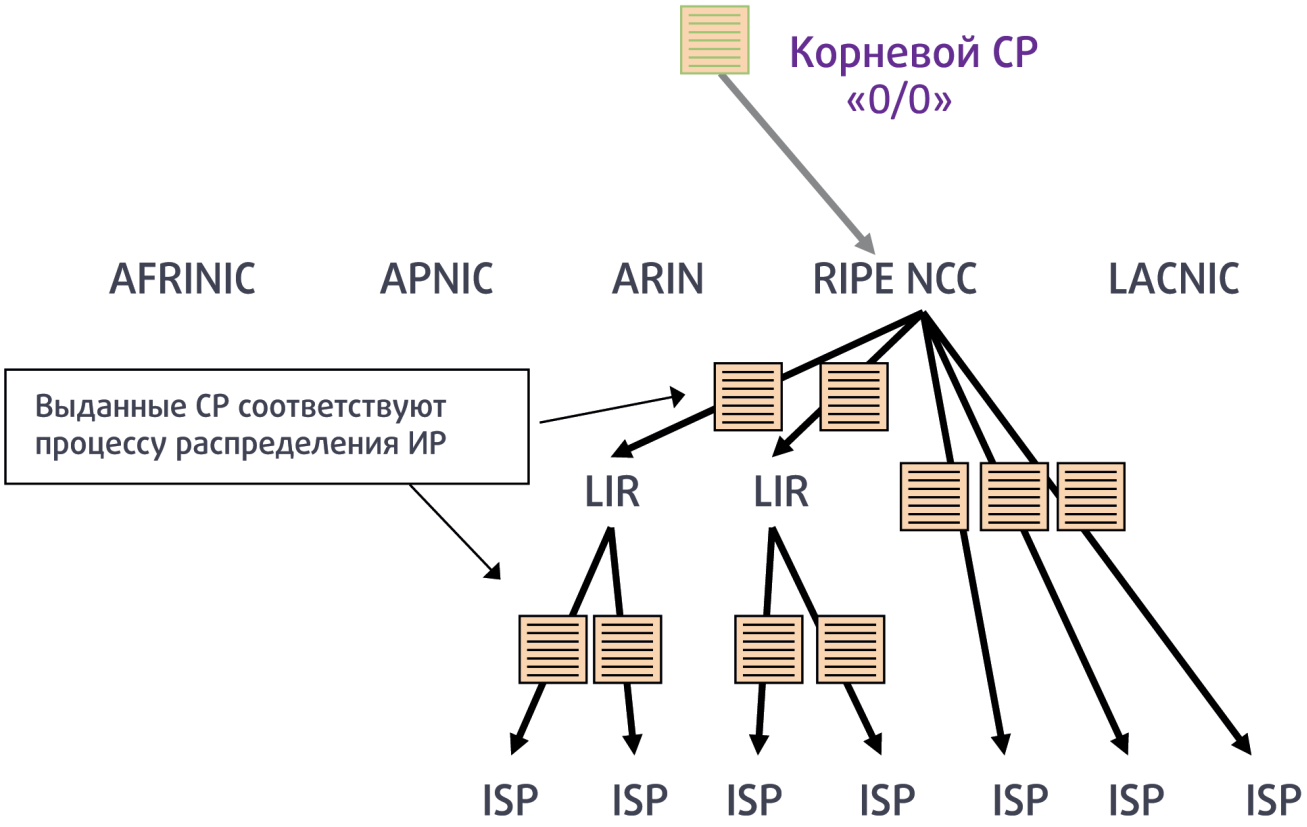
Перенаправление. Эта атака похожа на предыдущие, только после прохождения по сети-перехватчику трафик возвращается в нормальное русло и попадает к получателю. Из-за этого такую атаку труднее обнаружить. Целью обычно является «подслушивание» или модификация передаваемых данных. Злоумышленники часто используют такой вид атаки для пассивной разведки ресурсов и потенциально слабых мест сети организации. Примером такой атаки является атака Пилосова-Капеллы (https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf)

«Утечка маршрутов» (route leaks). Очень похожа на атаку «перенаправления», однако не использует сфабрикованные анонсы, а является нарушением стандартной политики маршрутизации. Стандартная политика связана с ролями, которые сети играют в плане межсетевого соединения: клиент, провайдер и равный партнер, или пир. Примером такого нарушения является ситуация, когда сеть-клиент начинает реанонсировать маршруты, полученные от одного провайдера, другому провайдеру. Таким образом сеть-клиент сама становится провайдером услуги транзита, часто с печальными для себя последствиями – объем перенаправленного трафика намного превышает ресурсы сети. Об «утечках маршрутов» подробно рассказано в статье Джеффа Хьюстона в №2 «Интернета Изнутри».

Нестабильность. Нестабильность в глобальной системе маршрутизации может быть вызвана частыми изменениями в анонсировании конкретной сети (попеременное анонсирование и аннулирование), с целью «демпфирования» маршрутов данной сети провайдерами и, как следствие, блокирования связности.

Фабрикация адреса источника трафика. Хотя в этом случае система маршрутизации как таковая не подвергается

Рис. 1. Общая схема RPKI.



атаке, данный метод широко используется в так называемых атаках на отражение. В этом случае обратный трафик, например, ответы на изначальные запросы, направляется не к истинному источнику, а к получателю, чей адрес был сфабрикован. Как правило, такие атаки используют протокол без установления соединения UDP (User Datagram Protocol, http://ru.wikipedia.org/wiki/Udp) и основаны на эффекте усиления, когда небольшие запросы от многих источников порождают ответы значительно большего размера. Одна из критических систем, в основном использующая UDP и подверженная атакам такого рода, является DNS.

Отсутствие механизмов проверки подлинности полученной информации позволяет атакующему повлиять на маршрутизацию трафика, относящегося к той или иной сети, в глобальном масштабе. Эти атаки, многие из которых являются попросту ошибками конфигурации, быстро распространяются, захватывая значительное число сетей с серьезными последствиями. Как правило, продолжительность таких атак не превышает нескольких часов, что не уменьшает их разрушительного действия.

Инструментарий

Безопасность и надежность системы маршрутизации во многом зависит от возможности правильного ответа на вопросы:

Является ли префикс, полученный в сообщении BGP, правомерным (т.е. представляющим законно распределенное адресное пространство и право на его использование)?

Является ли автономная система-источник маршрута правомочным владельцем префикса?

Соответствует ли атрибут AS_PATH, полученный в сообщении BGP, действительному пути, который прошло данное сообщение в сети Интернет?

Если сам протокол BGP не позволяет осуществить проверку подлинности маршрутов, полученных от другой сети, какими средствами располагает оператор для решения этой задачи? Основу решения составляют источники достоверной информации о распределенном адресном пространстве, о маршрутах и их правомочных сетях-источниках.

Таких источников, по существу, три: базы данных распределенных номерных ресурсов региональных интернет-регистратур (РИР, Regional Internet Registry, RIR) whois, интернет-регистратуры маршрутизации IRR (Internet Routing Registry) и репозитории системы RPKI (Resource PKI).

Базы данных номерных ресурсов

Для тех, кто хочет хотя бы защитится от нераспределенного адресного пространства (которого, впрочем, становится все меньше в мире IPv4) и так называемых богонов, основным источником информации являются базы данных распределенных номерных ресурсов, обслуживаемые соответствующими РИРами.

Хотя эту информацию можно получить через соответствующий whois-сервер регистратуры, иногда более практичным способом является использование так называемых файлов статистики, доступных на сайте ftp (ftp://ftp.ripe.net/pub/stats). Например, интернет ресурсы, распределенные RIPE NCC, представлены в следующем файле: ftp://ftp.ripe.net/pub/stats/ripencc/delegated-ripencc-latest.

Как вы можете заметить, число записей весьма внушительно, также внушительным будет список префиксов в конфигурации ваших граничных маршрутизаторов.

База данных IANA (Internet Assigned Number Authority, www.iana.org), например, http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml для ресурсов IPv4, является более компактной, хотя и не содержит деталей - каждая запись имеет размер /8 в случае IPv4, а детализация для адресного пространства IPv6 и того меньше. Однако данный подход позволяет по крайней мере блокировать сети, использующие нераспределенные адресные ресурсы.

Организация Team Cymru, специализирующаяся на вопросах инфраструктурной безопасности, каждые четыре часа генерирует полный список неиспользуемого адресного пространства IPv4 и IPv6. Эти списки доступны как в виде текстового файла, так и путем настройки BGP-пиринга с их сервером маршрутов (route server, RS). См. http://www.team-cymru.org/bogon-reference.html.

Интернет-регистратуры маршрутизации (IRR)

Частичную помощь в решении данной проблемы оказывают интернет-регистратуры маршрутизации (Internet Routing Registry, IRR). Суть их заключается в следующем: сетевые операторы регистрируют в базе данных свою политику маршрутизации, а именно с кем и как сеть взаимодействует, и префиксы, которые сеть использует и анонсирует в Интернет. Для описания политик используется язык RPSL, о котором мы уже говорили. Также существует инструментарий, наиболее известный из которых IRRToolset (http://irrtoolset.isc.org/), который позволяет автоматизировать конфигурацию маршрутизации провайдера по данным IRR.

IRR отображают весьма неполную картину, так как регистрация данных в этих базах данных сугубо добровольная. Многие операторы не хотят себе морочить голову какими-то IRR, часть операторов не регистрирует по причине нежелания разглашать свою политику. Те же, кто все же зарегистрировал свою политику, не всегда поддерживают актуальность данных. Проблема в том, что хотя эта деятельность служит на благо общего дела – безопасной системы маршрутизации, польза для самого провайдера не всегда ощутима.

Неполнота и ненадежное качество данных, а также плохая масштабируемость подхода - попробуйте-ка создать фильтры для всех префиксов, зарегистрированных в IRR! – делает IRR

малопригодными для проверки достоверности всех маршрутов в глобальном масштабе. В то же время IRR являются весьма удобным инструментом для автоматизации построения фильтров для подключенных клиентов.

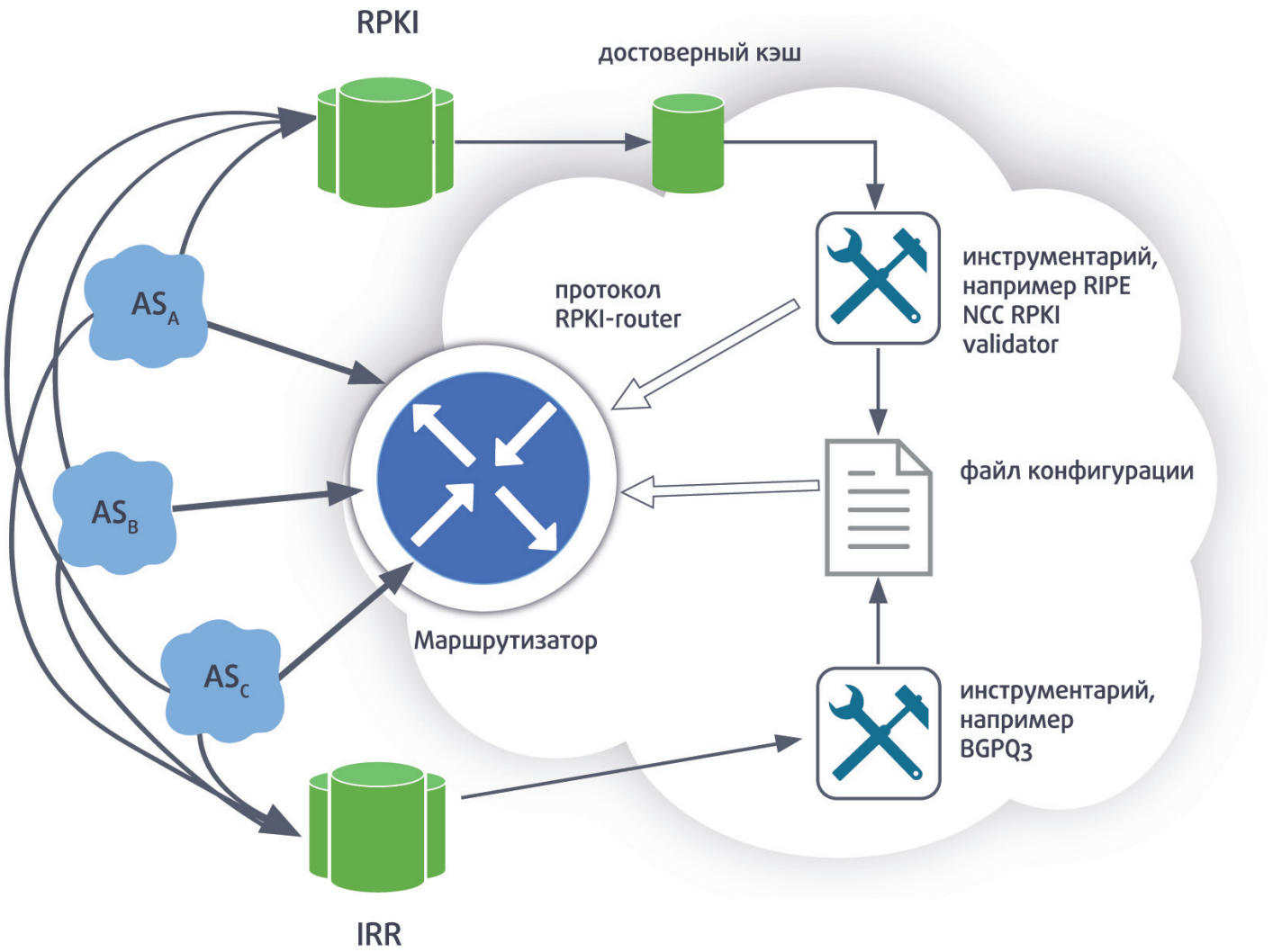
Репозитории RPKI

Учитывая недостатки IRR, уже в конце 90-х техническое сообщество начало работать над созданием более надежной информационной системы, основанной на цифровой сертификации номерных ресурсов. Система получила название RPKI. Фундаментом RPKI является система открытых ключей (Public Key Infrastructure, PKI), элементами которой являются сертификаты интернет-ресурсов. На основе этих сертификатов держатели ресурсов могут создавать криптографически заверенные объекты, например, ROA (Route Origin Authorization), указывающие на автономные системы, которые могут являться источником определенного маршрута.

Как и любая система PKI, RPKI имеет иерархическую структуру с корневым сертификатом во главе. Корневой сертификат в качестве списка номерных ресурсов охватывает все адресное пространство IPv4, IPv6 и автономных систем. С помощью этого сертификата могут быть сгенерированы сертификаты РИР в соответствии с фактически распределенным адресным пространством. Замечу, что в настоящее время РИР обеспечивают собственные корневые сертификаты, таким образом мы имеем не одну, а пять иерархических структур RPKI.

РИРы осуществляют сертификацию ресурсов, которые они распределяют локальным регистратурам (Local Internet Registry, LIR). Локальные регистратуры могут осуществлять последующее распределение и соответствующую сертификацию. Наконец, сетевые операторы, многие из которых являются локальными регистратурами, фактически использующие адресное пространство, также должны иметь возможность генерирования временных сертификатов для подписания вторичных объектов RPKI, например, ROA.

Рис. 2. Использование различных механизмов для валидации анонсов.



Общая схема RPKI проиллюстрирована на рис. 1.

В плане обеспечения безопасности маршрутизации, ROA – это ключевой элемент RPKI. Как следует из названия, ROA является разрешением, выданным сетью-владельцем прав на использование адресного пространства на анонсирование данных ресурсов автономной системой (АС), указанной в ROA. В соответствии со спецификацией, ROA содержит номер авторизованной АС и список IP-префиксов, которые эта АС имеет разрешение анонсировать. К этому "заявлению" прилагается сертификат, описывающий соответствующие АИР, и весь объект подписан с использованием ключа, указанного в сертификате.

По сравнению с IRR система обладает несколькими существенными преимуществами. Во-первых, данные о распределенных номерных ресурсах предоставляются в стандартной форме цифровых сертификатов со стандартными расширениями (расширения X.509 собственно и содержат список ресурсов, привязанных к открытому ключу сертификата). Во-вторых, достоверность и свежесть данных может быть проверена с использованием криптографических средств третьими лицами. Как и в стандартном PKI, для проверки необходима конфигурация доверия только к одному сертификату – т.н. точка доверия (Trust Anchor, TA). В-третьих, сертификаты ресурсов могут использоваться их владельцами (держателями адресного пространства) для, например, электронной авторизации определенных автономных систем для анонсирования этого адресного пространства, выполняя, таким образом, функцию объектов route традиционных IRR.

Использование ROA возможно как для построения фильтров, так и в качестве дополнительного правила в процессе выбора пути BGP. Логично предположить, что интеграция информации, полученной от системы RPKI в процесс BGP, является более масштабируемым решением.

Возможное применение IRR и RPKI для валидации анонсов, полученных от соседних сетей, представлено на рис. 2. В случае использования RPKI предполагается, что сервис-провайдер хранит собственную копию всех объектов глобальной системы RPKI, проверяет их достоверность и периодически обновляет. Результирующая база данных содержит только достоверную информацию (достоверный кэш, validated cache) и может быть непосредственно использована процессом BGP маршрутизатора с применением протокола RPKI-маршрутизатор (https://datatracker.ietf.org/doc/rfc8210/). Другим вариантом является использование этой базы данных для построения фильтром, так же, как и в случае с IRR.

Вопросы внедрения

Рассмотренный инструментарий может реально решить проблему безопасности системы маршрутизации только при достаточном уровне внедрения. Дело в том, что усилия отдельного провайдера вносят несущественный вклад в улучшение глобальной системы и, как ни парадоксально, еще менее существенный - в улучшение собственной безопасности.

Например, валидация анонсов маршрутов, полученных от клиентов, безусловно предотвращает атаки захвата префиксов этими клиентами, но не является защитой от захвата их адресного пространства в другой части Интернета.

При рассмотрении проблематики безопасности глобальной системы маршрутизации мы сталкиваемся со своего рода феноменом трагедии общин (http://ru.wikipedia.org/wiki/Трагедия_общин). Общие усилия могут значительно уменьшить проблему, но тенденция перекладывания этого бремени на других не позволяет добиться существенных результатов. Осуществляя фильтрацию анонсов или ограничивая распространение ошибок и умышленных захватов, оператор фактически защищает чужие сети, на безопасность же собственной его действия не влияют. В то же время, если все действуют в собственных краткосрочных интересах, улучшения в этой области так и не произойдет.

Хорошие манеры

Одним из путей решения проблемы трагедии общин, которая по сути представляет собой неспособность рыночных сил исправить ситуацию, является государственное регулирование. Существует много примеров, особенно в области безопасности, когда регулирование в форме требования соответствия определенным стандартам приносило желаемые результаты.

Классическим примером является введение в США закона, предписывающего обязательное оборудование автомобилей ремнями безопасности. На принятие этого закона существенно повлияла книга Ральфа Нейдера «Опасен на любой скорости» (https://ru.wikipedia.org/wiki/Опасен_на_любой_скорости).

Однако регулирование имеет ряд недостатков, делающих этот подход малоэффективным, по крайней мере, как единственное решение:

- регулирование предполагает наличие стандартов, определяющих требования по безопасности; часто используемые международные стандарты серии ISO 27000 являются очень общими, дорогостоящими в воплощении и сертификации и нацелены на требование соответствия определенным процессам, а не конечным результатам;
- регулирование может стать непропорциональным бременем для отрасли в решении проблемы;
- наконец, регулирование в государственном масштабе малоэффективно для решения глобальных задач, таких как защищенность глобальной системы маршрутизации.

Другой подход, который, впрочем, также вряд ли является полным решением, использует социальные связи сообщества взаимозависимых игроков. В традиционном случае трагедии общин таким сообществом являются фермеры, обеспокоенные истощением совместно используемых пастбищных лугов, в нашем же случае – это сетевые операторы, пиры, обеспокоенные целостностью и достоверностью совместно создаваемой маршрутизационной информации.

Примером использования такого подхода является инициатива MANRS (Mutually Agreed Norms for Routing Security, https://www.manrs.org), поддерживаемая растущим сообществом сетевых операторов.

MANRS определяет ряд требований и связанных с ними конкретных мер (Actions), которые являются наиболее элементарными практиками защиты системы маршрутизации. Несмотря на относительную простоту, по мере широкого внедрения эти меры смогут существенно усилить защищенность системы.

Требования эти следующие:

Предотвращение распространения неправильной маршрутизационной информации. Сетевой оператор обеспечивает правильность собственных анонсов и анонсов от своих клиентов со степенью детализации на уровне отдельных префиксов и AS-PATH.

Предотвращение трафика с подложными IP-адресами. Оператор осуществляет проверку адреса-источника для, по крайней мере, клиентских сетей с одним подключением, своих собственных конечных пользователей и инфраструктуры.

Улучшение информационного обмена и координации между сетевыми операторами в глобальном масштабе. Оператор публикует актуальную контактную информацию.

Поддержка проверки достоверности маршрутизационной информации в глобальном масштабе.

Оператор публикует собственную политику маршрутизации и данные о префиксах, анонсируемых сетью. Эти данные могут использоваться другими операторами для проверки достоверности анонсов.

Особенностью MANRS является то, что перечисленные требования имеют узкую область применения, делая их максимально конкретными и оптимальными с точки зрения стоимости внедрения и связанных дополнительных операционных рисков. Так, например, требование предотвращения распространения ложной маршрутизационной информации распространяется только на клиентов провайдера и его собственную инфраструктуру – где проверка достоверности этой информации достаточно тривиальна. То же относится и к другим требованиям.

Этот базовый уровень безопасности составляет основу формирования сообщества операторов с общей целью обеспечения большей защищенности системы.

Эта инициатива также открывает перспективы использования экономических факторов для решения задачи безопасности. Из выводов недавно проведенного исследования аналитической компании 451 Research (http://www.routingmanifesto.org/resources/research/) очевидно, что организации, пользующиеся услугами сетевых операторов, весьма обеспокоены теми же проблемами, которые являются целевыми для MANRS. Более того, многие из них видят в MANRS эффективное средство решения этих проблем и готовы на дополнительные затраты ради партнерства с оператором-участником инициативы.

Роль точек обмена трафиком

Многие точки обмена трафиком сами в определенной степени являются сетевыми операторами – возьмите, например, внутреннюю сеть обслуживания. Внедрение общепринятых норм маршрутизационной гигиены в сети IXP безусловно необходимо. Однако в плане вклада в улучшения защищенности системы маршрутизации и пиринга IXP могут внести гораздо более значительный вклад.

IXP могут и уже играют очень важную роль в создании более безопасной инфраструктуры Интернета. Многие из них представляют собой активные сообщества операторов с общими оперативными целями. IXP являются платформой для обсуждения оперативных проблем, включая проблемы небезопасного пиринга, борьбы с вредоносным трафиком атак и аномалии маршрутизации. MANRS в этом отношении может служить хорошей отправной точкой таких обсуждений и стимулировать конкретные результаты.

Для IXP MANRS может предоставить возможность построить «безопасное сообщество операторов», используя общий доказанный уровень безопасности, предоставляемый MANRS. Это также способ продемонстрировать внешнему миру внимание IXP к безопасности и устойчивости экосистемы Интернета и, следовательно, к высококачественным услугам.

Каков же может быть конкретный вклад IXP?

Содействие предотвращению распространения неверной информации о маршрутах.

Многие IXP используют сервер маршрутов для облегчения многостороннего пиринга – при этом оператору необходимо установить лишь одну сессию с RS, чтобы получить все анонсы участников. Сервер маршрутов также может осуществлять дополнительные функции – например, проверять полученные анонсы.

Проверка выполняется путем проверки анонсов BGP с использованием IRR или репозитория RPKI. Также разумно проверять анонсы на предмет «богонов» или «марсиан» (префиксы IP, как определено в RFC1918, RFC5735 и RFC6598; ASN в AS-PATH, как определено RFC5398, RFC6793, RFC6996, RFC7300, RFC7607).

Основываясь на результатах процесса проверки, анонс может быть помечен как VALID, INVALID или UNKNOWN с использованием предопределенных сообществ или отфильтрован в зависимости от политики RS, принятой членами IXP.

Защита пиринговой платформы.

Хотя, строго говоря, это не относится к маршрутизации, применение гигиены на уровне 2 может обеспечить плавную работу платформы и способствовать стабильности инфраструктуры и маршрутизации IXP.

Обычно фильтрация применяется к:

- пактам Ethernet с неразрешенными форматами;
- пакетам с недопустимыми Ethertypes;
- трафику, относящемуся к внутренним протоколам, как IRDP, переадресация ICMP, протоколы обнаружения (CDP, EDP), протоколы VLAN/транкинга (VTP, DTP), BOOTP/DHCP и т.п.;
- трафику, ограниченному конфигурацией безопасности порта MAC.

Помощь в предотвращении нежелательного трафика.

Предлагая телеметрические данные на основе потоков Netflow / Jflow / Sflow / IPFIX для L2-L4 для своих членов, IXP может помочь операторам в предотвращении нежелательного трафика (например, трафик с поддельными исходными IP-адресами) или смягчить атаку DDoS.

Поддержка глобальной оперативной связи и координации между сетевыми операторами.

Эффективная коммуникация между членами IXP имеет важное значение для смягчения сетевых инцидентов, таких как неправильные конфигурации, сбои или атаки DoS. Ключевую роль играют списки рассылки или другие средства связи и каталог участников, доступный всем членам биржи, содержащей обновленную контактную информацию.

Такие простые меры, как предоставление необходимых списков рассылки и директориев участников может иметь большое значение для быстрого разрешения случаев злоупотреблений, безопасности и операционных инцидентов.

Предоставление участникам средств мониторинга и отладки.

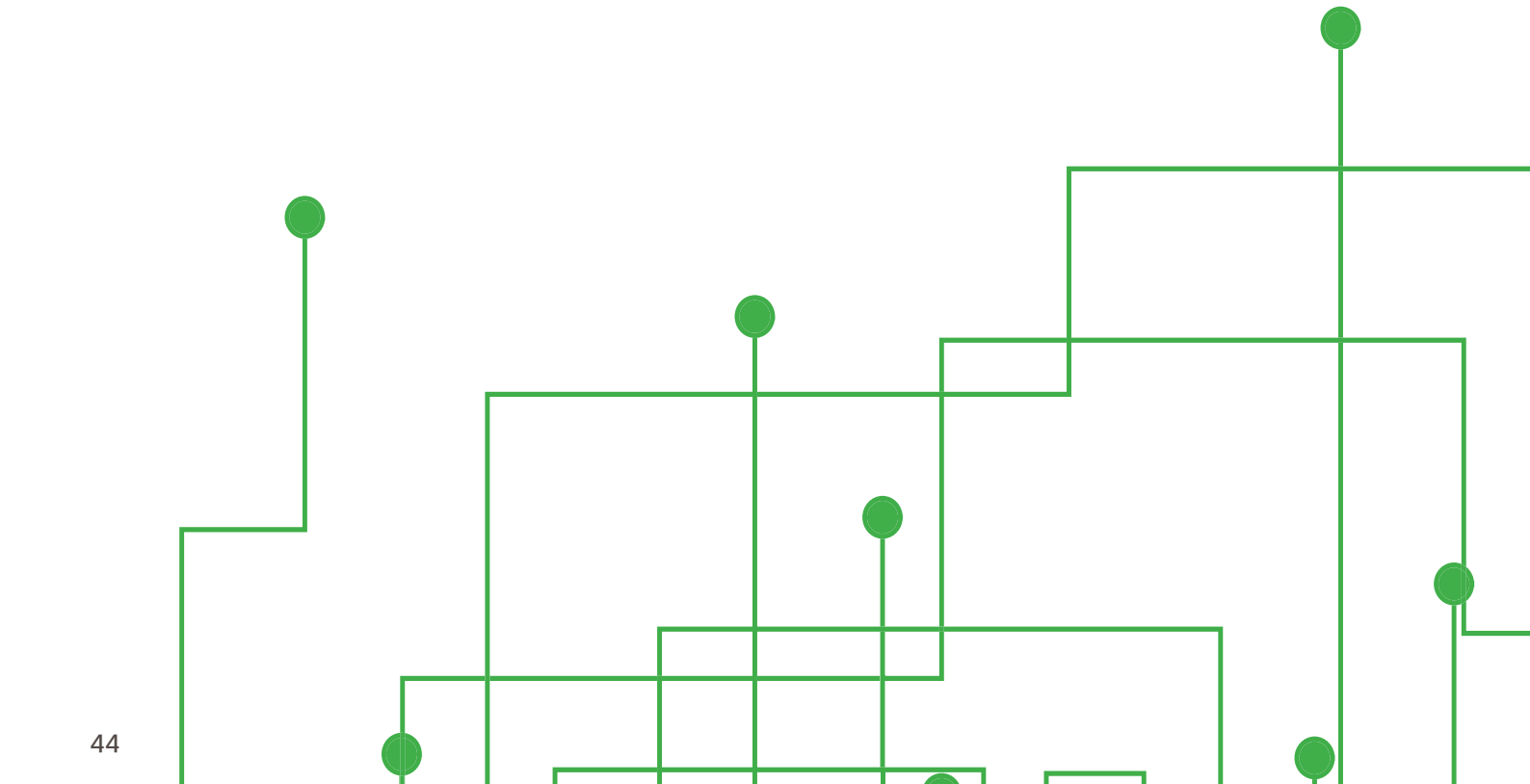
Смотровое стекло (Looking Glass) сервера маршрутов является важным средством, которое может помочь отладить инциденты или аномалии маршрутизации и предотвратить или сократить негативные последствия таких инцидентов.

Содействие в смягчении атаки отказа в обслуживании (Denial of Service, DoS).

Чтобы помочь сетям смягчить влияние атаки DDoS на их сети, IXP может предложить один из двух основных механизмов для прекращения нежелательного трафика без перегрузки пиринговой платформы или инфраструктуры участников: «сток» (sink hole) и «черная дыра» (blackhole).

При использовании «стока» IXP настраивает конкретный MAC-адрес и соответствующий IP-адрес. Весь трафик, предназначенный для этого IP-адреса, удаляется платформой IXP. Оператор-участник, испытывающий объемную DoS-атаку на определенные префиксы своей сети, может объявить эти префиксы с настройкой next hop, указывающей на IP-адрес «стока». Это можно сделать через сервер маршрута или двусторонний пиринг.

При использовании подхода «черной дыры» оператор, испытывающий объемную DoS-атаку, «включает» черную дыру на сервере маршрутов, используя стандартное BGP-сообщество BLACKHOLE (RFC 7999). В результате весь трафик, предназначенный для этих префиксов, будет удален на платформе IXP.



Заключение

Защищенность системы маршрутизации Интернета зависит от усилий многих участников. Технологические решения и инструментарий играют существенную роль, но внедрение этих практик и технологий в сетях определяет конечный результат. Сегодняшний Интернет насчитывает почти 60 000 автономных систем, которые используют BGP для обмена маршрутами. Однако большинство этих сетей являются конечными клиентами сетей следующего ранга, которые предоставляют услуги транзита и играют более существенную роль в глобальной маршрутизации (см. http://bgp.potaroo.net/as2.0/bgp-transitas.txt). Таких сетей около восьми тысяч. Если большинство из них станут применять базовые практики маршрутизационной гигиены, о которой я писал в этой статье, маршрутизация в Интернете станет гораздо более защищенной и стабильной.

ICANN отложила ротацию ключей KSK (Key Signed Key) для корневой зоны

Павел Храмцов

ICANN отложила начало процедуры ротации ключей (KSK) для корневой зоны 27 сентября. Таким образом, событие, которое планировалось с 2010 года после подписания корня, откладывается на неопределенный срок. А должно было оно произойти 11 октября 2017.

Возникает резонный вопрос: что понудило ICANN изменить свои планы?

В своем сообщении ICANN[1] указала, что «Изменение ключа подразумевает создание новой пары криптографических ключей и распространение нового открытого компонента ключа среди резолверов, осуществляющих валидацию DNSSEC (DNSSEC - расширения безопасности системы доменных имен). Если посмотреть на предполагаемое количество интернет-пользователей, которые используют резолверы, осуществляющие валидацию DNSSEC, изменение KSK может затронуть приблизительно четверть интернет-пользователей мира или 750 миллионов человек».

Мягкое «изменение KSK может затронуть» означает то, что эти сотни миллионов пользователей потеряют возможность доступа к информационным ресурсам Сети по доменному имени. Получить информацию, используя IP-адреса ресурсов, будет можно, но кто же знает, а если даже и знает, то помнит ли адреса yandex, google и facebook. Кроме того, для этих пользователей прекратится доступ не только в web, но они потеряют возможность переписываться со своими друзьями и коллегами посредством электронной почты.

Так что решение ICANN скорее всего оправданно. Тем не менее, следует обратить внимание на два момента: что заставило внедрить технологию DNSSEC в систему DNS, как ICANN обнаружила возможность возникновения проблемы и оценила возможный ущерб.

Для чего нужен DNSSEC

В 2008 году на конференции BlackHat 2008 Дэн Камински обратил внимание сетевой общественности на фундаментальную проблему реализации протокола DNS – возможность подмены содержания ответов авторитетных DNS-серверов и кэширование подменных ответов резолверами.

Подменить адрес источника позволяет транспорт UDP – это фундаментальная уязвимость этого транспортного протокола. А вторая фундаментальная проблема – это кэширование, которое является неотъемлемой частью работы системы DNS. Кэширующие серверы обслуживают конечных пользователей. У крупного ISP (Internet Service Provider) один кэширующий сервер может обслуживать тысячи клиентов. «Отравление» кэша, таким образом, представляет серьезную проблему.

Подменить можно не только соответствие между, скажем, именем yandex.ru и адресом 77.88.55.55 (один из списков адресов, которые связаны с этим именем), но адрес сервера, который обслуживает корень системы DNS, скажем, a.root-servers.net (198.41.0.4). А вот это уже позволяет построить параллельный Интернет для клиентов кэширующего сервера.

Кэши «отравляли» и до сообщения Камински. На программное обеспечение ставили заплатки - и проблема на некоторое время «уходила» до повторения атаки в новых условиях. Но тут за дело, т.е. ликвидацию угрозы, взялись всерьез. Рандомизацией портов и других полей заголовка UDP и DNS-пакетов дело не ограничилось.

В 2005 году появились спецификации расширения безопасности DNS[2] - DNSSEC. Идея состояла в том, чтобы обеспечить независимый способ проверки достоверности DNS-ответов, основанный на анализе информации самих ответов.

В заголовок DNS-пакета добавили несколько флагов, в список записей описания ресурсов добавили записи, которые позволяли передавать ключи и подписи. Главная идея состояла в эксплуатации административной процедуры делегирования права управления файлом зоны домена. Все ответы в DNSSEC удостоверены цифровой подписью администратора зоны, которая, в свою очередь, удостоверена цифровой подписью администратора старшей зоны.

В иерархии DNS администратор старшей зоны делегирует администратору младшей зоны право вести файл зоны

ОБЩИЙ ГРАФИК РОТАЦИИ ПАРЫ KSK

22 июня 2016 — Был опубликован план ротации ключа. Опубликован он был для широкого обсуждения

27 октября 2016 — Должна была начаться процедура ротации ключа. В этот день была сгенерирована новая пара ключей KSK (открытый и секретный)

февраль 2017 — Ключи были скопированы в резервное хранилище

13 марта 2017 — Появилась возможность протестировать программное обеспечение на предмет возможности получения нового ключа и работы с ним. Это можно было сделать либо вручную (скопировать ключ с https://www.iana.org/dnssec/files), либо проверить возможность поддержки резолвером RFC-5011

11 июля 2017 — Новый публичный KSK был опубликован в DNS. С этого момента можно было проверить, копирует ли резолвер новый ключ согласно RFC-5011 или требуется ручное вмешательство

19 сентября 2017 — Все корневые серверы увеличили размер ответа DNSKEY

11 октября 2017 — Новый ключ должен был начать использоваться для удостоверения на равных со старым ключом

февраль 2018 — Ожидался отзыв старого ключа

своего домена на свое усмотрение. Это означает, что между администраторами есть независимый канал взаимодействия, который позволяет обмениваться информацией. Соответственно, администратор младшей зоны может передать администратору старшей зоны информацию для размещения в его файле зоны, которую потом можно будет сравнить непосредственно или путем вычислений с тем, что он разместил у себя в файле зоны.

Пакет RFC про DNSSEC определяет различные варианты удостоверения подписей данных из файла зоны домена. В том числе, например, и «острова» доверия. Однако в полной версии цепочка доверия всегда выстраивается до ключей корневой зоны. В данном случае пара ключей KSK корня фактически и являются тем якорем доверия, который необходим для удостоверения правильности ответов резолверов.

Учитывая тот факт, что при первичном рекурсивном поиске любого соответствия имени адресу мы должны обратиться к корню, неточности или шероховатости в получении KSK могут вылиться в большую проблему.

Новый ключ и валидирующие резолверы

Общий график ротации пары KSK выглядел следующим образом:

22 июня был опубликован план ротации ключа. Опубликован он был для широкого обсуждения.

27 октября 2016 года должна была начаться процедура ротации ключа. В этот день была сгенерирована новая пара ключей KSK (открытый и секретный).

В феврале 2017 года ключи были скопированы в резервное хранилище.

13 марта 2017 года появилась возможность протестировать программное обеспечение на предмет возможности получения нового ключа и работы с ним. Это можно было сделать либо вручную (скопировать ключ с https://www.iana.org/dnssec/files), либо проверить возможность поддержки резолвером RFC-5011.[3]

11 июля 2017 новый публичный KSK был опубликован в DNS. С этого момента можно было проверить, копирует ли резолвер новый ключ согласно RFC-5011 или требуется ручное вмешательство.

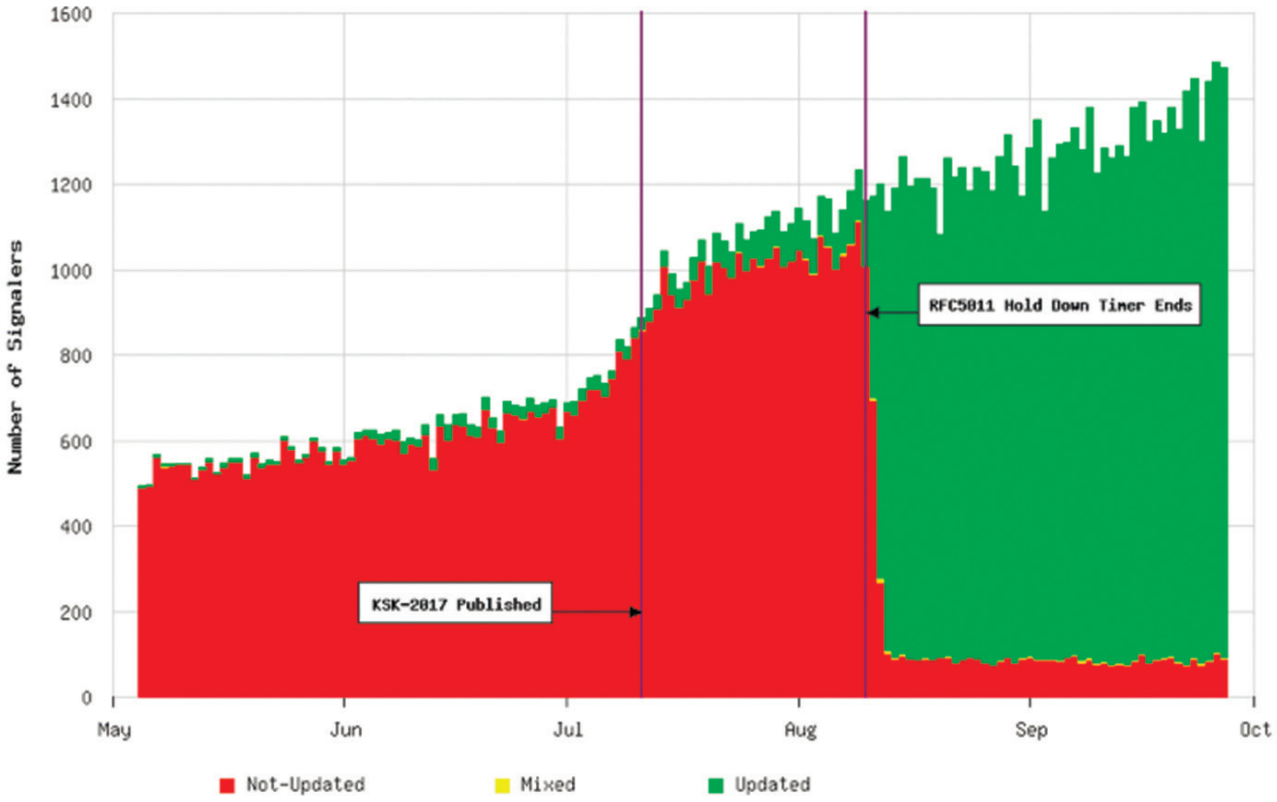
19 сентября 2017 все корневые серверы увеличили размер ответа DNSKEY.

11 октября новый ключ должен был начать использоваться для удостоверения на равных со старым ключом.

В феврале 2018 года ожидался отзыв старого ключа.

Считалось, что с весны до осени 2017 года времени достаточно, чтобы провайдеры DNS-резолверов убедились в правильности работы с DNSSEC.

Рис. 1. Статистика получения данных о поддерживаемых KSK.



Здесь следует особо отметить, что ротация ключа корневой зоны касается только провайдеров кэширующих резолверов, т.к. именно они (резолверы) осуществляют валидацию DNS-ответов согласно стандартам DNSSEC. Теоретически такую валидацию можно осуществлять и на стороне конечного клиента. Но вероятность такого варианта исчезающе мала.

Операторам валидирующих резолверов необходимо было провести следующие мероприятия:

Определить, поддерживает ли их резолвер ротацию ключей согласно RFC 5011. Если такая поддержка есть, то убедиться в том, что она включена.

Проверить, что резолвер, поддерживающий RFC 5011, смог получить KSK-2017 (уже опубликован) и корректно включил этот ключ в список доверенных.

Для резолверов, не поддерживающих RFC 5011, заблаговременно получить достоверную копию KSK-2017 и включить его в список доверенных ключей.

Например, валидирующие рекурсивные резолверы АО «ЦВКС «МСК-IX», входящие в облака:

- dns.ix.ru (IPv4: 62.76.76.62 / IPv6: 2001:6d0:6d0::2001);
- dns2.ix.ru (IPv4: 62.76.62.76 / IPv6: 2001:6d0:6d::2001),

поддерживают стандарт RFC 5011.

Все необходимые опции программного обеспечения на валидирующих рекурсивных серверах АО «ЦВКС «МСК-IX» для возможности автоматической ротации KSK корневой зоны DNS были активированы. Соответственно, ключи были вовремя получены.

Однако у корпорации ICANN не было уверенности, что операторы валидирующих резолверов правильно понимают грозящие им перемены. По этой причине за подписью президента ICANN Йорана Марби (Göran Marby) национальным администраторам связи в сентябре было разослано информационное письмо с настоятельными рекомендациями и разъяснениями по поводу ротации ключа KSK.

«ЦВКС «МСК-IX» в качестве оператора системы DNS национальных доменов ru/рф провел исследование статистики обращений резолверов к авторитетным серверам зон ru/рф. В результате этого исследования выяснилось, что 75,79% российских резолверов готовы принимать DNSSEC. А вот среди зарубежных резолверов таких оказалось больше - 86,01%. Если бы все они реально валидировали ответы и не поддерживали новый ключ, то проблема была бы серьезной.

Но всегда полезно руководствоваться принципом «доверяй, но проверяй». В апреле 2017 года в протокол DNS были внесены изменения[4], которые позволяли получать информацию о том, какой из KSK поддерживает резолвер. ISC в bind и NLnet Labs в unbound реализовали эту спецификацию. Это позволило VeriSign получить соответствующую статистику[5] (рис. 1).

Согласно этим данным, от 6% до 8% резолверов продолжают поддерживать только старый KSK.

Результаты исследования были переданы в ICANN - и корпорация решила заморозить на неопределенное время процедуру ротации ключа. В конце концов, семь лет не меняли, можно еще несколько месяцев потерпеть, пока окончательно не определится тенденция с получением нового ключа, и пока не станет ясно, что администраторы этих серверов не намерены что-либо предпринимать.

Ссылки

1. https://www.icann.org/news/announcement-2017-09-27-ru

2. https://www.ietf.org/rfc/rfc4035.txt, https://www.ietf.org/rfc/rfc4034.txt, https://www.ietf.org/rfc/rfc4033.txt

3. https://tools.ietf.org/html/rfc5011

4. https://tools.ietf.org/html/rfc8145

5. https://blog.verisign.com/domain-names/root-zone-ksk-rollover-postponed/

Новости Доменной индустрии

Важные события 2017

КООРДИНАЦИОННЫЙ ЦЕНТР ДОМЕНОВ .RU/.РФ И CNNIC СОВМЕСТНО РАЗВИВАЮТ ИНТЕРНЕТ

Директор Координационного центра доменов .ru/.рф Андрей Воробьев принял участие в российско-китайском форуме «Москва – Пекин: торгово-экономическое и культурное сотрудничество на Шелковом пути», который состоялся 18 сентября в МИА «Россия сегодня».

На секции «Экономическое сотрудничество стран в эпоху диджитал» Андрей Воробьев рассказал о важности совместной работы для обеспечения стабильности критической информационной инфраструктуры и установления прозрачных договоренностей в сфере интеллектуальной собственности в эпоху цифровой экономики. Также Андрей рассказал о сотрудничестве Координационного центра доменов .ru/.рф и китайской регистратуры CNNIC и участии КЦ в подготовке российско-китайского торгового соглашения в области защиты доменов и товарных знаков.

РЕГИСТРАТОРЫ ПОЛУЧИЛИ 750 ОБРАЩЕНИЙ О СНЯТИИ С ДЕЛЕГИРОВАНИЯ ДОМЕННЫХ ИМЕН

В августе 2017 года компетентными организациями в адрес регистраторов было направлено в общей сложности 750 обращений о снятии с делегирования доменных имен. Анализ доменов-нарушителей по типу выявленной вредоносной активности в отчетном периоде показал, что распределение доменов-нарушителей по типам вредоносной активности по сравнению с июлем 2017 года осталось неизменным. Лидируют вновь доменные имена, связанные с распространением вредоносного программного обеспечения (477 обращений). Далее следуют фишинговые ресурсы (268 обращений) и контроллеры бот-сетей (пять обращений).

За отчетный период по обращениям компетентных организаций были сняты с делегирования 734 доменных имени. 16 доменных имен не были заблокированы, т.к. администраторы оперативно устранили причины блокировки или же ресурс был ранее заблокирован хостинг-провайдером. В 12 случаях делегирование было восстановлено по ходатайству соответствующей компетентной организации после устранения причины блокировки. В настоящее время остаются заблокированными 722 доменных имени.

УЧРЕДИТЕЛИ КООРДИНАЦИОННОГО ЦЕНТРА ДОМЕНОВ .RU/.РФ УТВЕРДИЛИ ПРИОРИТЕТНЫЕ НАПРАВЛЕНИЯ РАБОТЫ НА 2017-2019 ГОДЫ

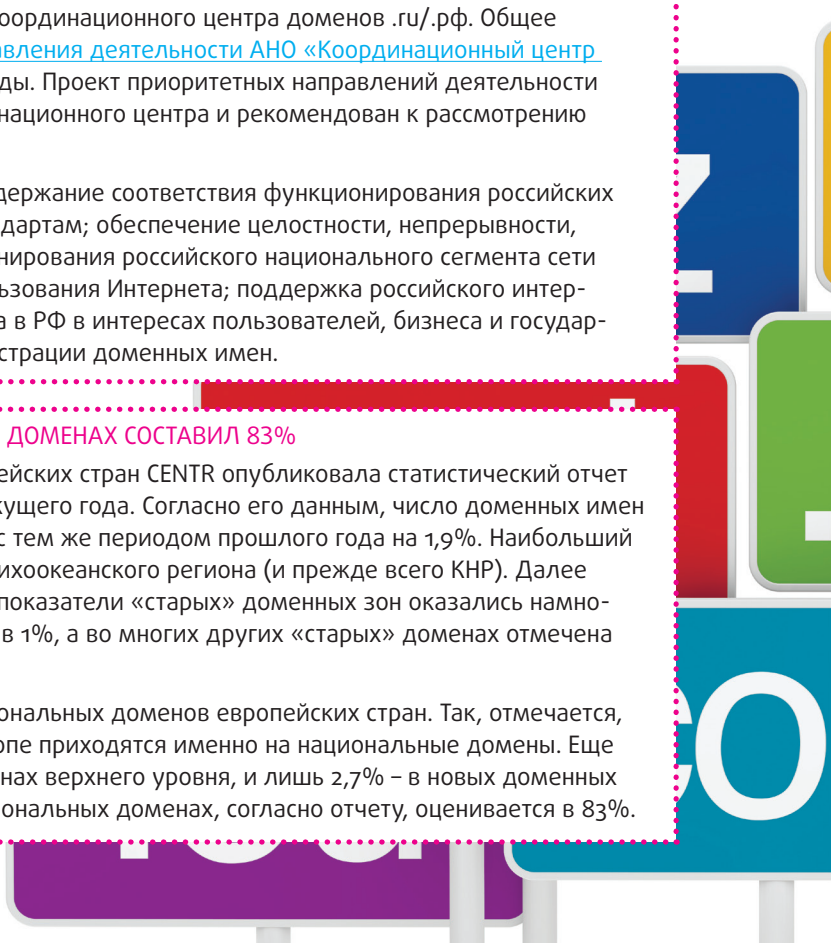
4 сентября состоялось общее собрание учредителей Координационного центра доменов .ru/.рф. Общее собрание учредителей утвердило приоритетные направления деятельности АНО «Координационный центр национального домена сети Интернет» на 2017–2019 годы. Проект приоритетных направлений деятельности КЦ ранее был рассмотрен на заседании совета Координационного центра и рекомендован к рассмотрению общим собранием учредителей КЦ.

Среди приоритетных направлений деятельности – поддержание соответствия функционирования российских национальных доменов .ru и .рф международным стандартам; обеспечение целостности, непрерывности, стабильности, устойчивости и защищенности функционирования российского национального сегмента сети Интернет; содействие повышению безопасности использования Интернета; поддержка российского интернет-сообщества, расширение использования интернета в РФ в интересах пользователей, бизнеса и государства и обеспечение качества и доступности услуг регистрации доменных имен.

УРОВЕНЬ ПРОДЛЕНИЯ РЕГИСТРАЦИЙ В НАЦИОНАЛЬНЫХ ДОМЕНАХ СОСТАВИЛ 83%

Ассоциация регистратур национальных доменов европейских стран CENTR опубликовала статистический отчет DomainWire Global TLD Stat Report за второй квартал текущего года. Согласно его данным, число доменных имен достигло 312 миллионов, увеличившись по сравнению с тем же периодом прошлого года на 1,9%. Наибольший рост показали национальные домены стран Азиатско-Тихоокеанского региона (и прежде всего КНР). Далее идут новые общие домены верхнего уровня. При этом показатели «старых» доменных зон оказались намного скромнее. Так, домен .com продемонстрировал рост в 1%, а во многих других «старых» доменах отмечена тенденция к снижению числа имен.

В отчете акцентируется внимание на показателях национальных доменов европейских стран. Так, отмечается, что почти 58% всех регистраций доменных имен в Европе приходятся именно на национальные домены. Еще 39,5% составляют регистрации в «старых» общих доменах верхнего уровня, и лишь 2,7% – в новых доменных зонах. Средний уровень продления регистраций в национальных доменах, согласно отчету, оценивается в 83%.



В ЗОНАХ .RU И .РФ ЗАРАБОТАЛ РЕЗЕРВНЫЙ РЕЕСТР

6 сентября в Алматы открылась юбилейная 10-я Международная конференция администраторов и регистраторов национальных доменов верхнего уровня стран СНГ, Центральной и Восточной Европы (TLDCON 2017). Для участия в ней зарегистрировались 140 человек из 17 стран мира.

Во время конференции генеральный директор MSK-IX Елена Воронина представила участникам конференции TLDCON 2017 резервный реестр национальных российских доменов, разработанный MSK-IX и начавший свою работу 1 сентября. Резервный реестр снижает последствия рисков для стабильности и безопасности системы доменных имен в случае отказа в работе основного реестра доменов .ru и .рф и позволяет сохранить копию файла зоны .ru и .рф в любой критической ситуации. «Резервный реестр – это наш совместный проект с Координационным центром доменов .ru/.рф, он делает систему DNS еще более устойчивой к разного рода воздействиям. Но это не единственный наш проект, связанный с доменным бизнесом. Наша DNS-сеть состоит сегодня из 32 узлов, распределенных по всему миру. Мы собираем статистику со всех узлов сети и на основе разностороннего анализа делаем выводы о том, где расположить следующий узел. Сегодня тенденция такова, что примерно 50% запросов приходит с территории России, а другие 50% - из разных стран, причем большинство из них из стран бывшего СССР. Вместе с Координационным центром мы выявляем точки наибольшей концентрации запросов в этих странах и размещаем там наши узлы DNS. Не так давно новый узел DNS был размещен в Казахстане», - рассказала Елена Воронина.

ЗАБЛОКИРОВАНЫ СОТНИ ДОМЕНОВ, СПОСОБСТВОВАВШИХ НЕЛЕГАЛЬНОЙ ТОРГОВЛЕ ЛЕКАРСТВАМИ

Завершилась масштабная международная операция Pangea X, инициированная сотрудниками Интерпола совместно с Европолом и Управлением по санитарному надзору за качеством пищевых продуктов и медикаментов США (Food and Drug Administration – FDA). Она проходила с 12 по 19 сентября и стала самой крупной в истории борьбы с нелегальной онлайн-торговлей фальшивыми и контрафактными медикаментами и медицинским оборудованием. Операция проводится уже в десятый раз, и если в 2008 году в ней участвовали лишь семь стран, на сей раз она объединила усилия правоохранителей, таможенных служб и органов по надзору за оборотом наркотических и лекарственных средств из 123 государств.

Точное число заблокированных в ходе операции доменных имен пока неизвестно. Однако только в США их число превысило 100, сообщает DomainPulse, ссылаясь на данные FDA. Что касается количества заблокированных по всему миру веб-сайтов, то оно составило 3584. Также была пресечена деятельность ряда доменных регистраторов, платежных систем и курьерских сервисов доставки, участвовавших в цепочках нелегальной онлайн-торговли.

СТАРТОВАЛА ПИЛОТНАЯ ПРОГРАММА ВНЕДРЕНИЯ «НАСЛЕДНИКА» WHOIS

Корпорация ICANN объявила о запуске пилотной программы по внедрению протокола Registration Data Access Protocol (RDAP). Протокол RDAP принят в качестве стандарта IETF в 2015 году и должен прийти на смену Whois. RDAP исполняет те же функции, что и Whois, но базируется на протоколе HTTP/S и формате JSON, что позволяет облегчить обработку данных. Кроме того, протокол упрощает использование нелатинских символов и, соответственно, расширяет возможности работы с регистрационными данными интернационализированных доменов.

Участие в программе является добровольным для регистратур и регистраторов. Они вольны выбрать собственные способы реализации RDAP и отображения регистрационных данных. Корпорация ICANN намерена ограничиться ролью координатора программы с тем, чтобы впоследствии обобщить полученный опыт и выбрать оптимальные формы использования RDAP. Пилотная программа по внедрению RDAP продлится до 31 июля 2018 года. Некоторые наблюдатели выказывают обеспокоенность тем, что RDAP позволяет дифференцировать уровень доступа к регистрационным данным. И нельзя исключать того, что многие пользователи Whois в будущем столкнутся с тем, что в их распоряжении окажется меньше регистрационных сведений, чем сегодня.

Календарь событий: 2017-2018 год

Международные события

18-21 декабря
IGF 2017,
Женева, Швейцария

В декабре состоится ежегодный Форум по управлению Интернетом (Internet Governance Forum, IGF). Целью Форума является вовлечение представителей различных групп - государственных органов, профессионального телекоммуникационного сообщества, бизнеса и гражданского общества, - в обсуждение вопросов, связанных с развитием и управлением Интернетом.
https://igf2017.swiss/#about-igf

19-21 февраля 2018
NANOG 72,
Атланта, США

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: система глобальной маршрутизации, DNS, пиринг и связность.
https://nanog.org/meetings/nanog72/home

18-21 февраля 2018
NDSS 2018,
Сан-Диего, США

Симпозиум NDSS - это ежегодная конференция, организуемая ISOC с целью способствования обмену информацией между исследователями и практиками по безопасности сетей и распределенных систем. Целевая аудитория включает в себя тех, кто заинтересован в практических аспектах компьютерной безопасности, с акцентом на реальные разработки и внедрения. К докладам принимаются исследовательские и практические проекты. Все доклады проходят тщательный отбор, поэтому сроки подачи очень ранние - прием докладов закончился еще в августе этого года. Так что если вы планируете подать доклад, следите за объявлениями к симпозиуму 2019 года!
https://www.ndss-symposium.org/

19-28 февраля 2018
APRICOT 2018,
Катманду, Непал

APRICOT - крупнейшая ежегодная конференция по интернет-технологиям, собирающая более 800 участников азиатского региона и Океании. Здесь обсуждаются вопросы внедрения и использования интернет-технологий, технического администрирования сетей и инфраструктурных услуг Интернета.
https://2018.apricot.net/

10-15 марта 2018
ICANN 61,
Сан-Хуан, Пуэрто-Рико

Встречи ICANN проводятся три раза в год в различных регионах земного шара, чтобы предоставить возможность активным членам сообщества ICANN лично поучаствовать в обсуждении насущных проблем. Общей темой, конечно, является DNS - глобальная система трансляции имен. Здесь обсуждаются как технические вопросы обслуживания услуг DNS, так и юридические и бизнес-аспекты предоставления регистрационных услуг. Участие во встречах ICANN бесплатно.
https://meetings.icann.org/en/sanjuan61

17-23 марта 2018
IETF 101,
Лондон, Великобритания

IETF (Internet Engineering Task Force) является одной из основных организаций по разработке стандартов в области Интернета. В основном работа в IETF проходит в многочисленных 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 (в среднем около 1200 участников из более 50 стран мира). Совещания IETF – это хорошая возможность познакомиться с новейшими тенденциями в области сетевых технологий и принять участие в их разработке.
https://www.ietf.org/meeting/upcoming.html

14-18 мая 2018
RIPE 76,
Марсель, Франция

Встречи RIPE проводятся два раза в год и собирают более 500 участников для обсуждения вопросов политики распределения номерных ресурсов (IP-адресов и номеров автономных систем) в зоне обслуживания RIPE NCC, сотрудничества, а также технических вопросов, связанных с маршрутизацией, DNS, связностью, измерениями и инструментарием.
https://ripe76.ripe.net/

В России

23 ноября 2017, Казань

BIT-2017

Международный Гранд Форум BIT-2017: облачные технологии, дата-центры, корпоративные коммуникации, Интернет вещей, аудио-/видеорешения, информационные сервисы для бизнеса. Мероприятие покрывает все вопросы, связанные с центрами обработки данных, современными коммуникационными сервисами, облачными вычислениями, Интернетом вещей, корпоративными аудио- и видеотехнологиями. https://kazan-2017.ciseventsgroup.com/

14 декабря 2017, Чебоксары

IT-LINK 2017

5-й межрегиональный форум об IT-технологиях и телекоммуникациях в бизнесе, главное событие для IT-сообщества региона, способствующее консолидации мнений и усилий государства, IT и бизнеса в создании благоприятной среды для развития информационных технологий в Чувашской Республике. http://forum-it.link/

21 февраля 2018, Санкт-Петербург

V Бизнес-форум «Телеком двух столиц: Эффективные пути повышения конкурентоспособности операторов связи в мегаполисах»

Главное общественное событие ИКТ-рынка Северо-Западного региона соберет на своей площадке более 200 ведущих экспертов отрасли, включая представителей региональных и федеральных операторов связи, вендоров и интеграторов телекоммуникационных решений, представителей регулирующих органов и отраслевых СМИ. http://www.comnews-conferences.ru/

В Москве

23-24 ноября 2017, «Холидей Инн Лесная»

VII Международный бизнес-форум «Broadband Russia Forum 2017 - Инфраструктура для цифровой трансформации»

Государственная политика развития национальной цифровой инфраструктуры и ликвидации цифрового неравенства, новые требования к сетям ШПД, инновации в архитектуре, технологиях и бизнес-моделях, умные сети и интеллектуальное управление трафиком, NFV, SDN, применение технологий IoT – эти и другие темы станут основой деловой программы Broadband 2017. http://www.comnews-conferences.ru/ru/conference/tn2018

7 декабря 2017, Конгресс-зал Центра международной торговли

XIII Пиринговый форум MSK-IX 2017

Крупнейшая ежегодная встреча участников интернет- и телеком-рынка. Форум проводится с 2005 года, с каждым годом собирая все большее число профессионалов. За это время из внутрисетевого мероприятия среди участников MSK-IX форум превратился в открытую деловую площадку, на которой обсуждаются самые актуальные вопросы развития сети и обмена трафиком. https://peering-forum.ru/

30 января – 1 февраля 2018, МВЦ «Крокус Экспо»

XX Международная выставка-форум CSTB. Telecom&Media 2018

Цифровая трансформация – можно ли к ней подготовиться, сколько нужно ЦОД, чтобы Россия могла идти в ногу с цифровой революцией, инициативы по импортозамещению IT-технологий, где и в какие сроки будут строить новые дата-центры, варианты трансформации IT для дата-центров. www.cstb.ru

1-2 февраля 2018, Здание правительства

XX Большой Национальный форум информационной безопасности «Инфофорум-2018»

Более 10 лет усилия Инфофорума направлены на создание условий для взаимодействия специалистов в области обеспечения информационной безопасности в Российской Федерации. Более 1500 участников из 60 субъектов РФ. Соорганизаторами выступят: Комитет Государственной Думы ФС РФ по безопасности и противодействию коррупции, Аппарат Совета Безопасности РФ и Торгово-промышленная палата РФ.
https://infoforum.ru/

22-23 марта 2018, «Холидей Инн Лесная»

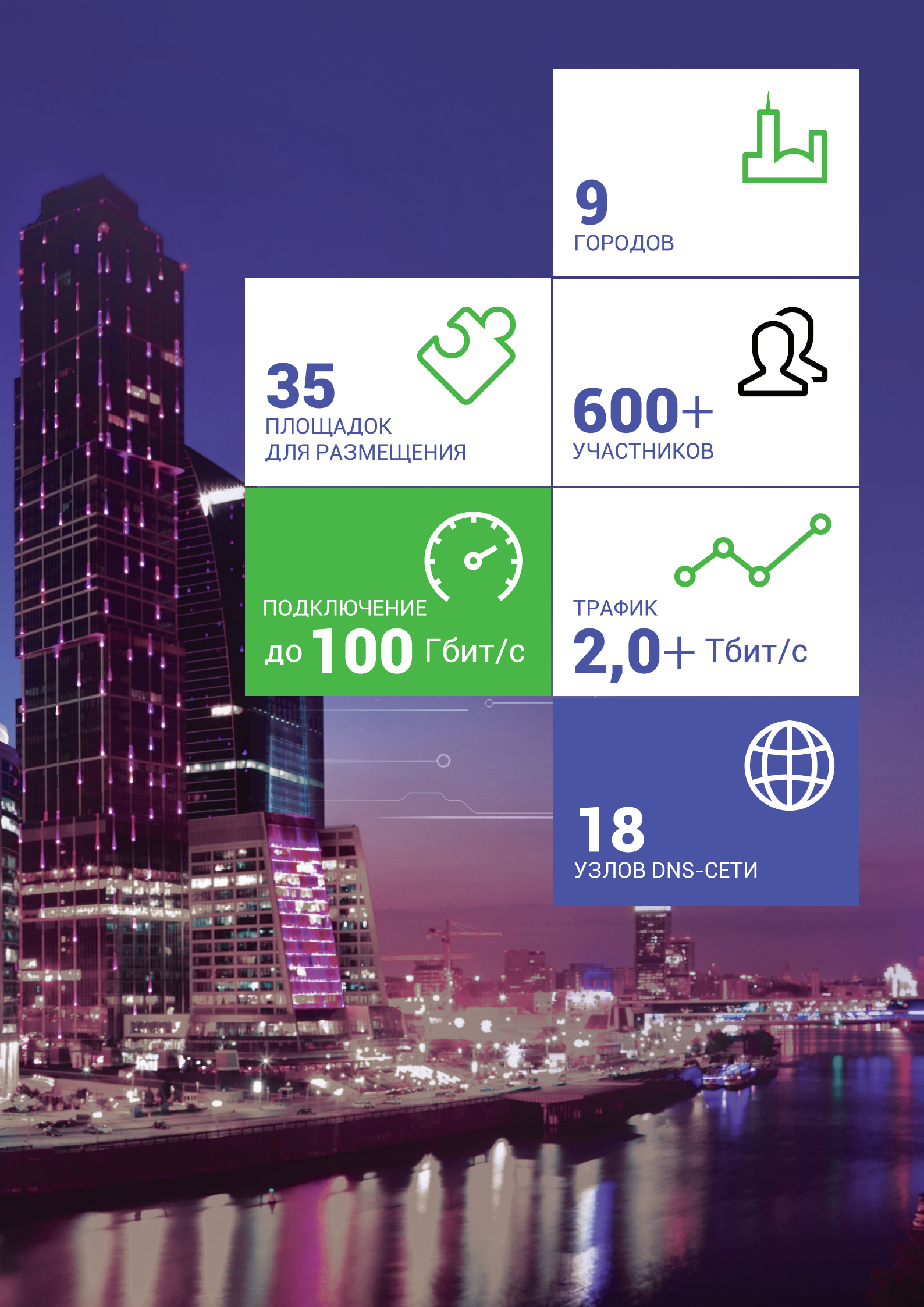
IX Международная конференция «Transport Networks Russia 2018 - Развитие телекоммуникационных транспортных сетей в России и СНГ»

Крупнейшее ежегодное мероприятие, посвященное развитию рынка телекоммуникационных транспортных сетей в России и СНГ, за последние восемь лет стало основным местом встреч регуляторов и первых лиц операторского бизнеса.
http://www.comnews-conferences.ru/ru/conference/tn2018

MSK IX

WWW.MSK-IX.RU

+7 (495) 737-9295



9
ГОРОДОВ

35
ПЛОЩАДОК
ДЛЯ РАЗМЕЩЕНИЯ

600+
УЧАСТНИКОВ

ПОДКЛЮЧЕНИЕ
до **100** Гбит/с

ТРАФИК
2,0+ Тбит/с

18
УЗЛОВ DNS-СЕТИ

Интернет изнутри

2017