Интернет: Камо Грядеши?

Картинка с кадром из культового ролика Apple стала слишком популярной. Слишком. И, собственно, роман "1984" стал слишком поминаем, как всуе, так и по делу. Настоящий текст - переклад текста Карла Ауэрбаха, известного тем, что будучи избранным президентом ICAAN, подал в суд на ICAAN. Впрочем, не только этим конечно же...



Итак, Карл Ауэрбах. Один из создателей Интернета. Член IETF со времен войн TCP/IP versus OSI, один из разработчиков SNMP, редактор сотен RFC, владелец компании Precept Software и, по сути, изобретатель IPTV (еще в 1995 году!). Потом компанию Precept Software он продал Cisco за $84M). Чувак настолько значимый в истории Интернета, что к каждой его статье нужно проявлять интерес просто потому что это Карл Ауэрбах.



Карл Ауэрбах

Пожалуй, круче него только Винт Серф, но Винт в последнее время примкнул к "Корпорации Добра", а это значит, что он немного выпадает из трендов в силу корпоративной культуры.

Впрочем, это всё предисловие.

А вот сказочка, которую и хочется пересказать на русском, была опубликована в блоге и перепечатана множеством издании. На русском не нашел

И называется статья "Интернет: куда ты идешь?". Причем, последняя фраза - это на латыни "Quo Vadis?" является крылатой. "Куда идешь ты, Господи?", - задал вопрос Апостол Петр Иисусу на Тайной

Вечере. И Иисус ответил: "За то, что ты оставил мой народ, я иду в Рим на второе распятие". По сути, фраза-вопрос является предложением задуматься, правильно ли человек живёт, туда ли идёт в своей жизни, верны ли его жизненные цели, ценности.

И действительно. Статья особенно интересна в свете последнего российского законотворческого дебоша, устроенного в завершении работы Думы шестого созыва.

Итак. Как же виделся Интернет (с большой буквы) в самом начале его разработки? Как-то вот так:



Пастораль. Золотые луга, ласковое солнышко, добрейшие люди пасут радужных единорогов. Очень много хороших и умных слов: "глобальный" и "открытый".

Интернет будущего описывался таким, что кажется, текст взят из утопического научно-фантастического романа конца шестидесятых прошлого века, написанного обкурившимся хиппи. Интернет рассматривался как инструмент разрушения никчемной конкуренции между странами и людьми, устранения социального неравенства, уравнивания богатства и бедности, введения всеобщей справедливости & равенства & братства.

Если верить такому будущему, то единственным препятствием, стоящим между текущим положением дел и "миром во всем мире", является то, что Интернет пока всё ещё не покрыл 100% поверхности Земного Шара. А еще то, что злые провайдеры до сих пор несправедливо относятся к различным видам трафика. Или что до сих пор IPv6 внедрён не везде. Или, вот еще некоторые злобные правительства возводят "великие стены" и осуществляют блокировки по IP. Кроме того, некоторые крупные корпорации (разумеется - злые) полюбили покупать домены первого уровня. Еще можно упомянуть, что шифрование трафика применяют не все...

И этот список можно продолжать бесконечно.

Я не согласен.

(Это Карл Ауэрбах не согласен!)

Вряд ли в будущем интернет будет утопическим местом, где честные веб-разработчики делают прекрасные приложения, а все интернет-провайдеры сплошь альтруисты. Справедливости, братства и равенства не существует.

Вместо этого мы наблюдаем очень мощные и, скорее всего, непреодолимые силы, которые разделяют и дробят Интернет на кусочки.

В будущем интернет будет состоять из "островов".

Эти "острова" будут иметь тенденцию совпадать своими границами со странами, культурами, или корпорациями. Между островами будет множество границ, барьеров и препон. Чтобы пересечь границы, мы будем вынуждены строить мосты.

А сетевой трафик, который перемещается по этим мостам, будет ограничиваться, мониториться, регулироваться, облагаться налогами.

В будущем Интернет станут использовать в качестве инструмента власти, контроля и обогащения.

И в значительной степени простых пользователей будущего Интернета, это не будет беспокоить.

Попробуем же описать это будущее - будущее, которое более вероятно, чем те химеры, фантазии и иллюзии, которые рисуются воображением идеалистов.

История повторяется

Кто не помнит своего прошлого, обречён пережить его вновь. (с) Джордж Сантаяна

При описании будущего, реальность всегда отличается деталях. Однако общие исторические закономерности, тем не менее, повторяются.

Даже в нашем современном мире - мире лёгких путешествий и глобальных корпораций - перемещение между странами, в основном, происходит через хорошо обустроенные порталы, и обычно совершается по заранее установленным путям.

В совсем недавнем прошлом этот узор мест-и-путей, или, по аналогии, карте островов-и-мостов, был ещё более четко обозначен. Вы не могли просто так взять и попасть в другую страну. А о путешествии на другой континент многие не могли и мечтать. Да и сейчас мимо таможни вам проскочить не удастся.

В то же время имеется исторический пример Римской Империи, где впервые были унифицированы дороги, но в конечном итоге это не защитило от набега варваров.

В этой статье мы попробуем доказать, что Интернет движется по той же самой исторической кривой - в конечном итоге мы придем к контролируемой изоляции или канализированным соединениям. И в течение следующих нескольких лет интернет будет медленно, но верно превращаться в острова, которые будут иметь границы, установленные национальными, корпоративными или культурными правительствами. И вместо открытой среды с прозрачными правилами управления, интернет-трафик между "островами" будет течь через узкие, четко определенные и строго контролируемые мосты.

Краткая история мира

Идея, что "планета - это в конечном итоге маленький и хрупкий шар", является достаточно новой.

На протяжении большей части истории человечества, мир был огромным и имел неверотяное количество разнообразнейших земель, разделённых границами. Путешествия и торговля являлись вопросом расстояний, которые необходимо было преодолеть, по пути пересекая моря и океаны, реки и пустыни.

Города и замки возводились в стратегически важных точках, где разветвлялись проезжие тракты или реки. Или, предположим, был мост через реку. Или там, где было удобно построить гавань. Вокруг городов всегда возводились стены и в этих стенах строилось всего лишь несколько ворот, через которые можно было попасть в город.



На наш современный взгляд, стены, окружающие города, являются военным атавизмом и реликтом давно закончившихся битв. Но была и другая причина строить каменные преграды, которая была значима не меньше военной причины для развития цивилизации: торговля. Или более конкретно - желание контролировать торговлю.

Если попытаться провести аналогию, в которой сравнить Интернет и средневековую Европу, то можно уловить схожесть между торговлей и потоками пакетов данных. Это может показаться слишком широким обобщением. Тем не менее, большую часть торговли и сегодня можно представить в виде потоков пакетов данных - контейнеров, танкеров, железнодорожных вагонов и целых составов. Стремление к всеобъемлющему контролю в равной степени можно отнести и к потоку пакетов, точно так же, как это делается для торговли.

Если мы оглянемся назад во глубину веков, то увидим, что мир - это географически обособленные "острова": баронства, графства, царства и империи. Эти "острова" сливались и распадались, они воевали, они боролись, и договаривались.

Несмотря на эту разобщенность, в мире существует по крайней мере одна константа: торговлю между островами во все времена старались как-то упорядочить, регулировать и облагать налогом.



Мытарь

Если вы контролировали мост через реку или проход через горы, то вы имели рычаг, с помощью которого могли бы получить силу, власть и богатство. Если вы контролировали город рядом с морским портом или расположенный на перекрестке торговых путей или на слиянии рек, или в месте, где проходили ярмарки - вы также имели власть.

Города, ярмарки, замки, как правило, строили там, где природные или искусственные коридоры движения сходились вместе. Город Нью-Йорк стал доминировать над своими соперниками Бостоном и Филадельфией, потому что Нью-Йорк Сити имеет удобную естественную гавань с видом на горы и свободный доступ в глубь Американского континента через реки Гудзон и Мохок, через которые легко попасть в бассейн реки Миссисипи и Великие Озера. Сейчас это целая транспортная система Нью-Йорк-Стейт-Бардж-канал.

Мы склонны рассматривать стены средневековых городов, как форму защиты. Но ворота в стенах были даже более важны, впрочем, как и мосты и каналы - вся торговля проходила через "дырочки", проделанные в искусственных или естественных барьерах. У каждых ворот денно и нощно находился специальный функционер, обязанностью которого было взимать налоги и сборы.

Города стали обменными пунктами, где народы обменивались товарами, где происходили экспортно-импортные сделки, где можно было купить всё, что было доступно в данной эпохе-времени. Товары, производимые в городе или в окрестных регионах, сначала аккумулировались в этом городе, а затем

экспортировались. Товары, создаваемые в других местах, сначала нужно было импортированы в город, где они потреблялись локально или распределялись по округе.

Эта модель существует и поныне: например, товары, произведенные в Китае, накапливаются сначала в китайских городах, где имеются крупные морские порты или аэропорты. Затем товары отгружаются и прибывают на западное побережье США в крупные города, такие как Лос-Анджелес или Сиэтл, где проходят обязательные таможенные процедуры, взимаются соответствующие пошлины. И только потом товары могут быть распространены в США.

Возможно, это станет неожиданностью для адептов "свободного обмена информацией", но Интернет сегодня представляет аналогичную картину. Интернет сервис-провайдеры (ISP) снабжают "связанностью" регионы, которые производят и потребляют товары и услуги, в то время как сами ISP получают эту "связанность" в точках пиринга / транзита, которые очень напоминают портовые города.

Это не "официальный" Интернет

Например, Hush-A-Phone:



Это оригинальное устройство, которым иногда снабжали телефонные аппараты в недавнем прошлом. Ну, как недавнем - до начала Второй мировой войны. Эта штука, сделанная из жести, надевалась на микрофон телефонного аппарата и имела специальную прорезь для губ. Вы должны были буквально вставить губы в эту прорезь и говорить. То есть, эдакая защита от подслушивания вашего разговора соседом по офису. Удобно. Однако в конце 1940-х годов ремонтная служба компании AT&T начала предупреждать клиентов, что применение таких приборов нежелательно и может привести к отключению от сети.

Интернет вырос из косного и негибкого мира телефонии, где каждое нововведение, каждое изменение должно было быть одобрено центральным бюрократическим аппаратом.

Интернет основан на другой идее: идее "пограничных инноваций", где базовая инфраструктурная сеть должна обеспечивать только минимальную функциональность. Но особо интересные вещи возникают, растут и развиваются не там, где провода и кабельная канализация.

Интернет основан на добровольности выбора пользователя.

В интернете нет Ma Bell ("крошек Белл" - так называли компании, оставшиеся после демонополизации AT&T). Не существует никакого "лорда интернета", который махал бы своим золотым скипетром и устанавливал бы свои официальные правила в каких-либо конкретных частях Интернета, обязательные и беспрекословные для исполнения.

В Интернете, по сути, нет и никакой официальной системы доменных имен. Нет никаких официальных установок даже по адресному IP-пространству. Более того, нет никаких официально установленных, утвержденных, подписанных и скрепленных печатью протоколов обмена данными или даже определений протоколов.

В то же время, существует некая доминирующая система доменных имен (DNS). Также имеется доминирующая система распределения IP-адресов и доминирующий набор протоколов, основных параметров и наборов правил обмена данными в Интернете.

Доминирование исходит из инерции истории и выбора большинства пользователей.

В то же время любой пользователь может выбрать, использовать, изменить или даже создать собственный DNS. Никто не запрещает иметь собственное, отделенное от основной сети, IP-адресное пространство. И никто не запрещает создать и использовать свои собственные протоколы обмена данными. Правда, в результате это может привести к изоляции от "большого Интернета".

Но некоторые люди жаждут изоляции. И если они готовы отключиться от "информационного океана" и принять последующую автономию - они свободны делать все эти вещи.

Другими словами, если человек или группа людей, или корпорация, или страна пожелает построить свой остров в Интернете - они вольны сделать это. Но если это произойдет (а это происходит), то придется строить мосты для соединения с общей частью Сети.



Кванмён. Интернет в Северной Корее

На самом деле, в Интернете уже давно существуют группы, которые пошли по этому пути. Существует система TOR с собственной "луковой" маршрутизацией. Существует "DarkNet". И, конечно же, существуют полностью изолированные сети, эксплуатируемые военными или государственными учреждениями.

Многие корпорации требуют от своих сотрудников использовать для работы отделенные виртуальные локальные сети (VLAN - Virtual Local Area Networks), когда они находятся вне офиса.

С появлением "облачных вычислений", виртуальных машин, а также "контейнеров" Software Defined Networking (SDN), количество частных сетей, работающих "поверх Интернет", стало расти в геометрической прогрессии. Вплоть до полной изоляции от "всех нас".

Системы Over-The-Top (OTT) по доставке контента конечным потребителям используют Интернет только как среду доставки цифровых продуктов.

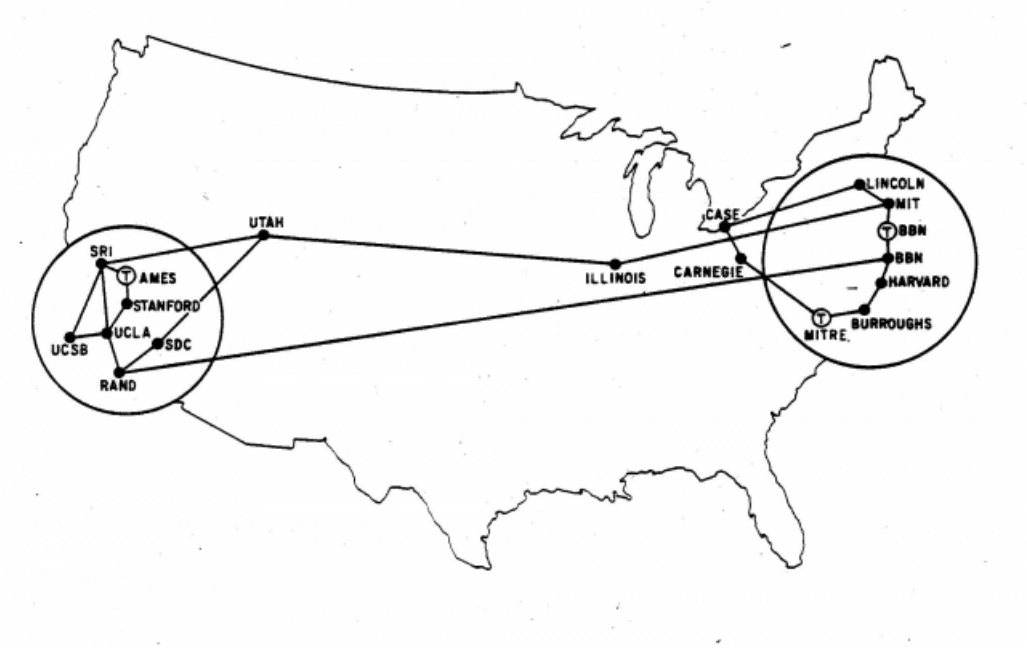
Всё вышеперечисленное совсем не обязательно изолированные "цифровые острова". Но они, по меньшей мере, полуострова с крепкими стенами, перегораживающими прямую дорогу в Интернет, низводя правила подключения "каждый-с-каждым" до уровня "особый случай".

Но что произойдет, если множество людей, корпораций и государств начнут задаваться вопросом: "А может быть необходим свой собственный остров в Интернет?". Ведь тогда они получат полный

контроль управления доступом, то есть некоторыми определёнными мостами. С целью получения силы, власти и богатства.

Сначала была сеть. А потом сетей стало много

1971 год. Карта ARPANET:



Каждый имеет право на собственное мнение.

Когда-то давно был Usenet. Еще был Bitnet. Был DECnet. И даже ESnet был. А потом сети стали объединяться. И появился ARPAnet.

ARPAnet стала единой сетью. Это была полно-связанная сеть с пакетной коммутацией под управлением Interface Message Processor (IMP). На хост-компьютерах, подключенных к IMP работали специальные программы-демоны, для которых был создан первый стандарт-протокол Network Control Protocol (NCP).

В то время в сетях было одно конкретное приложение, которое работало везде, на каждой машине: электронная почта. Между сетями были построены специальные "информационные мосты". Но для того чтобы навести эти мосты, потребовались некоторые очень странные вещи. Например, адреса отправителей, формат посланий и методы преобразования из одного формата в другой. Например, принцип работы электронной почты IBM Profs был полностью портирован с протокола BISYNC и всё выглядело так, как будто вы работаете с перфокартами на 80 столбцов. Адреса электронной почты Usenet выглядели как последовательность релейных компьютеров, через которые почта и должна была проходить для доставки адресату. Например, у автора (Карла Ауэрбаха) был такой адрес: decvax!ucbvax!asylum!karl

Было создано огромное количество различных инструментов преобразования сообщений, чтобы скрывать межсистемные различия. В конце концов индустрия остановились на форме адресации вида: "name@hostname". Впоследствии этот формат эволюционировал в текущий протокол SMTP.

Точно так же эволюционировали интернет-протоколы TCP и что более важно - IP, которые были разработаны для замены NCP. И собственно "Интернет" сначала назывался "catnet", а потом уже "internet", и идея заключалась в том, что большая сеть формируется на базе небольших сетей, используя Internet Protocol (собственно - IP) в качестве строительных блоков.

Эти небольшие сети могли в корне отличаться друг от друга архитектурой и используемыми протоколами "внутри", но ровно до тех пор, пока какой-либо из компьютеров не решится выйти "во внешнюю сеть". Тогда компьютер должен был раздробить пересылаемую информацию на множество IP-пакетов и каждый пакет должен был быть снабжен адресной информацией "отправитель" и "получатель". И блоки IP-адресов внутри одной сети должны были отличаться от блоков в другой - иначе возникала коллизия адресов и пакеты просто терялись в пути. Такие небольшие сети в последующем стали известны как "автономные системы" (AS), а блоки адресов стали называться "подсетями" (subnet) или "префиксами". Сейчас "автономные системы" и их адресные блоки образуют основу систем маршрутизации пакетов современного Интернета.

Поскольку новая система с открытым подключением сетей к сетям значительно облегчала

подключение все новых и новых "автономных сетей", а информация, содержащаяся в одних сетях интересовала пользователей в других "подсетях", то ARPANet стала расти экспоненциально. В итоге, большинство пользователей начали отказываться от собственных протоколов передачи данных в пользу TCP/IP и принялись разрабатывать собственные коммуникационные приложения. Сначала от проприетарных протоколов отказались научно-исследовательские организации и университеты, а затем, видя как быстро растет "сеть сетей", стали подключаться и крупные поставщики сетевых решений. К ARPANet присоединились DECNet, IPX/Netware, и даже "голубой гигант" IBM бросил заниматься собственной разработкой Systems Network Architecture (SNA) решив, что лучше подключиться, чем бороться.

Описание этой эволюции может показаться несколько абстрактным. Тем не менее, все эти преобразования и изменения в нашем образе мышления позволили Интернет расти и расширяться, поглощая и перемалывая все больше сетей и различных технологий - X.25, avian carrier, Frame Relay, Ethernet. И наконец - LTE.

Индивидуально управляемые сети, основанные на разнообразнейших технологиях и средах передачи данных, могут быть объединены в систему, в которой IP-пакеты могут путешествовать из сети в сеть и дальше - просто необходимо указать каждому пакету адрес и помочь найти путь от адресата к получателю и обратно.

Однако эта эволюция вовсе не закончена. В последние годы мобильные операторы связи - такие как Verizon или AT&T - начали стремительно изменяться из-за того, что пользователи, оплачивающие услуги связи, начали требовать не только и не столько привычную "телефонию", которая представляет собой "изолированный сад", но и связь с другими сетями. Они стали требовать "Интернет".

В ДНК-технологии Интернет содержится множество старых и глубоко внедренных в гены способов обработки множества сетевых методов для преодоления водоразделов. И это вовсе никого не должно удивлять: Интернет - это сеть сетей, а каждая сеть подключается к Интернет.

Грезы по универсальному Интернету

Способность легко транспортировать IP-пакеты друг другу из одной автономной сети в другую известна как принцип "end-to-end". Именно этот принцип позволил интернет развиваться как относительно "глупой среде" сети передачи пакетов, где на границах находятся очень умные маршрутизаторы. Такое положение вещей позволило инновационным изменениям совершаться "по краям", без изменения базовой сети сетей. Такая архитектура позволила внутренним частям - те автономным системам - меняться, развиваться и расти в сегодняшних сетевых провайдеров, не налагая обязательств для других "автономных систем" изменяться и соответствовать изменениям.

Сегодня, в 2016 году, мы наблюдаем, что такая архитектура имеет и собственные пределы. 32-разрядное адресное пространство IPv4 оказалось недостаточно ёмким, чтобы обеспечить достаточное количество адресов для Интернета, чтобы он мог расти и дальше. Впрочем, это было понятно уже в 1990-х годах, что адресов всем не хватит. По этому было создано несколько проектных альтернатив по расширению адресного пространства, в результате которого появилась новая версия протокола IP - IPv6. Многие надежды возлагаются на IPv6.

Грезы по универсальному Интернету не пропали. Но изменились.

Тем не менее интернет-мечта о ничем не ограниченных потоках IP-пакетов от IP-адреса адресата до IP-адреса назначения, никуда не исчезла.

Однако, эта мечта изменилась.

Изменённая мечта теперь заключается в том, чтобы вообще больше не заботиться о способах объединения IP-адресного пространства для ничем не ограниченных потоков пакетов.

Изменённая мечта теперь базируется на надежде "мое приложение работает везде, где я нахожусь, и на любом устройстве, которое я использую".

Старая мечта заключалась в заботах о пакетах. Изменённая мечта заботится о приложениях (Apps) и соединении HTTP/HTTPS на основе веб-браузеров и/или их кузенов - RESTFUL APIs.

Монетизация, монетизация и еще раз монетизация, или "Золото мостов".

Интернет был, есть и будет огромным золотоносным рудником.

В Интернете делают деньги на транспортировке данных.

В Интернете делают деньги на блокировке данных.

В Интернете делают деньги на регулировании данных.

В Интернете делают деньги на мониторинге данных.

В Интернете делают деньги на индексировании данных для поисковых систем. Причем, индексирование с различными целям - чтобы знать, кто с кем общается, или просто взимать больше денег для определенных видов трафика.

Но чтобы сделать действительно большие деньги, нужно найти место, где эти потоки данных сосредоточены. И существует ли лучшее места для контроля потока данных, чем мост между островами, где передаются огромные объемы трафика с одного острова на другой?

В теории - теория и практика одинаковы. Но на практике нет.

Грезы о "всемирной паутине" при воплощении столкнулись с суровой реальностью.

К сожалению, на уровне IP-пакетов протокол IPv6 является еще одной параллельной сетью, а не расширением существующей. Это означает, что IPv6, в большей степени замена существующей сети, чем плавное обновление и апгрейт. Поэтому, существующие ныне сети на IPv4, могут взаимодействовать с сетями, базирующимися только на IPv6, но с помощью нетривиальных ухищрений.

Сии ухищрения имеют множество названий - Teredo, инкапсуляция 6to4 и обратно 6rd, туннелирование ISATAP - и еще много страшных слов. Однако каждая технология и/или способ по-своему являются своеобразным мостом между миром IPv4 и миром IPv6.

"Проклятие унаследованных систем" - реальность, данная нам в ощущениях.

В предыдущие годы были сделаны колоссальные инвестиции в "мир IPv4" - закуплено оборудование, получены сертификаты, написана гора книг. Все это создает реальное сопротивление для массовой замены систем, работающих по протоколу IPv4.

Для крупных провайдеров и компаний, частичная, или даже полная замена оборудования станет всего лишь строчкой в бюджете на апгрейд программного обеспечения. Да даже и замена оборудования не представляет большой проблемы - в существующем зоопарке всегда находится нечто, что нужно срочно списывать, ибо оно сломалось, аммортизировалось или морально устарело. Именно таков жизненный цикл "основных средств" в крупных и долго живущих организациях.

Однако, для малого бизнеса и конечных потребителей, устаревшее оборудование должно быть полностью демонтировано и заменено новыми. Особенно это касается таких устройств, как принтеры, видеокамеры наблюдения, источники бесперебойного питания, файловые хранилища, телефонные коммутаторы, медиашлюзы и прочие машины, обеспечивающие работу бэк-офисов.

И, в большинстве случаев, основные затраты будут вовсе не на закуп железа или софта. В большинстве случаев главные финансовые потери придутся на переобучение пользователей и простои, связанные с модернизацией вполне себе функционирующих систем.

А еще существует фактор продавцов старых (и милых сердцу) систем и разработок на том же IPv4. И продавцы вовсе не горят желанием выбросить годы работы и миллионы инвестиций в мусорную корзину. Они, продавцы, хотят получать прибыль и не хотят вкладывать снова много денег в обучение, апгрейт и книгоиздательство. Money for nothing.

Элегантность архитектуры конфликтует с реальными инновациями

Шлюзы прикладного уровня (Application-level gateway, или ALG), более известные в технологической тусовке как "прокси", существовали с начала времен Интернет. Переадресация электронной почты является классическим примером, как ALG можно использовать для проведения электронных сообщений сквозь административные границы. Например, используя SMTP/SMTPS-пересылку, можно организовать "сборщик почты" на Gmail от Google и отправлять email на требуемые адреса частных, корпоративных и даже государственных систем электронной почты.

Трансляция сетевых адресов (Network Address Translation - NAT) система чуточку новее. При этом, NAT

самим своим существованием оскорбляет многих интернет-пуристов и радетелей за инженерную красоту сетевых решений. На самом деле, один из наиболее часто используемых аргументов в пользу IPv6: у IPv4 кончились адреса и IPv6 нужен для того, чтобы избавиться от NAT. Якобы, это позволит стать сетям более архитектурно эстетичными и технологичным.

Виртуальные частные сети (VLAN), по мнению технoперфекционистов, более красивы, поскольку они "частные" и "зашифрованные", и представляют собой как бы сегменты сети, которые накладываются на физические. Однако, по сути это прозаичный интернет-тоннель, когда трафик пробегает, очень похоже на телефонную коммутацию, но по "чужим проводам". Впрочем, VLAN вполне себе работающая конструкция, которая весьма востребована клиентами с некоторой долей паранойи.

А еще нас ждут массовые изменения в сознании и архитектуре сетей ввиду появления программно-конфигурируемых сетей (SDN). И SDN также принесёт некий новомодный способ или наложения одной сети поверх другой, или что-то более изощрённое.

NAT

Сервис NAT позволяет пользователям развернуть блок адресов на стыке двух сетей. С одной стороны, "операторский белый адрес", а с другой - "частный" отрезок адресного пространства IPv4. Уверен, что многие помнят "частные отрезки" IPv4-адресов наизусть.

И когда появилась эта технология, количество использованных NAT-систем росло взрывообразно. Сейчас NAT-сервисы встречаются везде. В каждом доме или на небольшом предприятии (да и в значительном числе крупных), где имеются бытовые и не очень бытовые маршрутизаторы, во всем мире используется NAT.

Сервис NAT делает очень простую вещь: он меняет содержимое IP-пакетов в части адресации "назначения" и "адресата", тем самым извращяя базовый интернет-принцип "прохождение неизменного пакета end-to-end". Разумеется, это вызывает определенные проблемы, потому что NAT должен сделать очень много манипуляций с каждым TCP или UDP пакетиком, изменив в нем 16 бит адреса и еще номер порта. При этом, количество портов в TCP|UDP-пространстве ограничено: всего 65536. И может показаться, что это достаточно большое число, но и для NAT, который может быть ограничен небольшим пулом доступных номеров портов, это является пределом того, насколько NAT - малый или "операторского класса" - можно масштабировать.

Кроме того, NAT может подпортить жизнь протоколам, в которых IP-адреса используются в качестве данных. Правда, эту проблему давно приземлили на несколько "старинных" до-натовских протоколов, таких как FTP, SDP и SIP. Более свежие протоколы, такие как HTTP/HTTPS не испытывают никаких трудностей.

Нет никаких сомнений, что NAT архитектурно кривая штука, которая нарушает принцип "end-to-end", и не очень хорошо масштабируется. Но наличие множества таких систем в эксплуатации также и не отрицает, что NAT часто оказываются полезными, надежными и адекватно эффективными.

Особо хочется отметить, что для многих приложений транспортными протоколами являются HTTP и HTTPS, а не TCP. И передача трафика, осуществляемая по протоколам HTTP/HTTPS легко проходит через адресное пространство прокси-серверов, трансляторы протокол-версии, или другие способы передать данные через интернет-границы. Другими словами, HTTP/HTTPS, а так же чудовищно огромное количество приложений, базирующихся на HTTP/HTTPS могут работать как прямо "end-to-end", так и легко проходить через "мосты между интернет-островами".

При этом, технически некрасивый NAT убедительно продемонстрировал, что Интернет может прекрасно работать, повторно используя адресные IP-пространства, и что большинство интернет-протоколов и приложений могут работать через NAT, с приемлемой производительностью.

Кроме того, NAT, хотя и не является полноценной системой безопасности, тем не менее, эта система соответствует базовым принципам безопасности, которая требует несколько преград между злодеем (не важно, кто это - "злобный кул-хацкер" или няшный "специалист по безопасности на белом коне") и защищаемым объектом.

NAT базово не может выстроить крепкие стены информационной защиты. Но NAT-системы добавляют лишние препятствия. При этом, NAT может быть препятствием, которое нетрудно преодолеть. А может быть, и достаточно сложным препятствием. NAT - это что-то типа рва вокруг замка. И "Большой Серый Волк" должен как-то преодолеть этот ров, чтобы полакомиться Ниф-Нифом и Наф-Нафом. Само собой, что поросята там еще прячутся в домике, но для того, чтоб до домика добраться, Волку придется тащить с собой лодку.

ALG

Существует еще одна технология, которая развивалась вместе с NAT. Эта технология не столь модная и не так распространена, но она существует: "шлюзы прикладного уровня" - Application-level gateway (ALG), которые чаще называют "Proxie". Или просто - "прокси", хотя это не совсем точное определение, поскольку "прокси" может выступать еще и в качестве кэширующего ресурса. ALG же чуточку проще.

Иногда ALG называют "middleboxes", потому что система работает как своего рода "man-in-the-middle"" ("человек-по-середине"). Техно-пуристы называют такие системы уничижительно - "посредники". Но на протяжении всей человеческой истории посредники иногда оказывались весьма ценны. А иные коммерсанты таки достигали богатства и славы, будучи банальными посредниками между, например, континентами.

ALG может быть совершенно прозрачным или достаточно "злым", но в любом случае система подставляет себя приложению пользователя вместо удаленного сетевого адреса.

ALG существуют на уровне приложений. ALG действует как эстафета между двумя различными транспортными доменами. Под этим подразумевается, что "прокси" выступает в роли сервера для клиента, и в качестве транспортного (TCP) клиента с точки зрения сервера.

Потенциально системы ALG/Proxies имеют возможности кэширования данных для эффективности передачи - зачем запрашивать один и тот же популярный файл у источника несколько раз, когда его можно просто сохранить где-то во внутренних хранилищах. А еще ALG может по заданным алгоритмам модифицировать передаваемые данные - эта функция весьма любима некоторыми коммерческими группами, но зачастую пользователи не жалуют такие "фичи".

Существует еще один аспект, который делает ALG особенно привлекательным для тех, кто заинтересован в безопасности или интеллектуальном анализе данных. Поскольку ALG существуют на уровне приложений, то они могут перехватывать, наблюдать, и даже изменять данные на уровне конкретных приложений. NAT так делать не умеет, поскольку оперирует на уровнях TCP-соединений. И даже механизму DPI (deep packet inspection - "глубокой инспекции пакетов") необходимо выполнить множество работы, чтобы выявить адресацию конкретного приложения так, чтобы не мешать фактически передаваемому трафику. А ALG это делает, поскольку имеется прямое разрешение пользовательской аппликации. Посему ожидается, что системы ALG более просты, более надежны и более эффективны, чем системы DPI.

Противодействие возможностям ALG, например, прочтение данных или их модификация в процессе передачи, обычно заключается в шифровании по типу "end-to’end". Это довольно эффективно.

Впрочем, природа ALG такова, что они могут представиться каким-то системам "как клиент" - напомню, что "proxy" переводится как "посредник". Следовательно, для ряда случаев возможна подмена не криптографических сертификатов, но собственно клиента. То есть, ALG, используя совершенно нормальный и легальный криптографический сертификат, соединятся с сервером, а потом уже используя свой сертификат, передает данные клиентскому приложению. Собственно, в этом и заключается механизм "человека-по-середине".

Но как насчет эффективности?

В профессиональных кругах достаточно много грязи было брошено в сторону NAT (включая "Carrier Grade NAT") и ALG.

Некоторые набросы довольно заслуженны: NAT (операторского класса или любые другие) не очень хорошо масштабируются.

И NAT, и ALG добавляют задержки при передаче данных. В случае NATa, эти задержки составляют всего несколько микросекунд, что, конечно же не очень заметно в единичном применении, но если таких "шлюзов" на пути пакета будет достаточно много, то для иных сетевых приложений это будет неприемлемо.

Использование ALG может, в своем худшем варианте, добавить куда большие временные задержки, хотя, в целом, это и не так смертельно.

С другой стороны, использование кэша ALG наоборот в некоторых случаях ускоряет передачу и экономит аплинки.

Для HTTP/HTTPS-трафика накладные расходы для установки TCP/TLS соединения часто является основным, и даже доминирующим фактором в восприятии пользователем времени отклика. И тот факт, что некоторые ALG позволяют повторное использование уже открытых соединений, использование этой технологии наоборот может фактически улучшить пользовательское восприятие ответной реакции в некоторых ситуациях.

В общем и целом, вопросы эффективности вычислительных мощностей и времени отклика NAT и ALG являются довольно сложными. Как правило, ответы на вопросы "эффективности" будут очень сильно зависеть от конкретных обстоятельств каждого отдельного случая.

Тем не менее, вопрос об эффективности несколько отвлеченный от практического применения. Никого, кажется, не беспокоит довольно значительные затраты вычислительных ресурсов на HTTPS по отношению к HTTP, или неэффективность наложенных сетей с использованием VLAN и SDN. Или вот, скажем, множественные счетчики web-аналитики, трекеры и "маяки", внедренные в код современных веб-сайтов так же влияют на общую производительность всей экосистемы интернета, но это так же никого не заботит. Просто вычислительных мощностей сегодня достаточно, чтобы обрабатывать этот трафик, а плюс-минус микросекунда не добавляет почти ничего на фоне других неэффективностей по причине своей исчезающей сравнительной малости.

Слабый клей

Центростремительные силы, удерживающие множество сетей в одном глобальном Интернете вместе, являются слабыми.

Основная сила, удерживающая Интернет от распада на множество сегментов - просто инерция. Люди не склонны менять работающие системы. И поэтому до сих пор Интернет работает очень хорошо.

И вот хочется заострить внимание на словах "до сих пор", которые имеют важное значение. Определенные группы, такие как отдельные государства, культурные и религиозные группы, некоторые коммерческие структуры начинают проявлять признаки недовольства. Риск того, что в скором времени появятся некие центры вокруг которых и начнут сливаться другие группы, чтобы отделиться от целого, совсем не иллюзорны.

Например, некоторые интернет-системы до сих пор работали великолепно. Вот те же операторы корневой системы доменных имен обеспечивали превосходный сервис, который делался в значительной степени без внешнего надзора. Но серверы доменных имен, а тем паче - корневая система, являются очень лакомым кусочком для тех, кто желает "навести свой порядок" и в режиме реального времени мониторить и/или регулировать все, что происходит в Интернете (см. выше - там рассказывалось уже про то, что вы легко можете создать свой собственный сервер DNS).

Очень уважаемые организации IETF, W3C и IEEE, где весьма квалифицированные инженеры и ученые пишут интернет-стандарты и протоколы на абсолютно добровольной основе. Основная сила, удерживающая людей в таких организациях - это то, что если "не они - то кто?". В том смысле, что, разумеется, никто не делает работы бесплатно - труд разработчиков стандартов и RFC оплачивается непосредственными работодателями. Как правило - производителями оборудования или крупными телеком-операторами. И это достаточно выгодные вложения - попытаться "протолкнуть" свой стандарт и первым реализовать его "в железе". Кроме того, экспериментальная база и получение новых идей из первых рук - также стоит немало.

Когда-то давно, было достаточно трудно построить сеть сетей, т.е. Интернет. Сегодня любой человек с достаточным количеством денег, может купить "составные части" - инженеров, оборудование и программное обеспечение, и построить свой собственный интернет ~~с блэк-джеком~~ - пригодную для коммерческого использования сеть, которая будет отличаться от "общего интернета". Собственно, такая вот частная сеть может даже использовать свою собственную версию IPv4 или IPv6 адресного пространства. И иметь свои собственные корневые сервисы доменных имен.

Пользователи такого частного интернета скорее всего будут чувствовать себя чуточку изолированными. Точнее - они будут совершенно точно изолированны, поскольку доступ до google.com или до fb.me будет осуществляться по желанию владельца "частного интернета". Но это не всегда будет являться отрицательным моментом. Потому что, повторимся, пользователи как раз могут желать самоизоляции. Пользователи будут чувствовать себя комфортно и счастливо от того, что никто не сможет достать их "снаружи". А все "проводящие пути" из "частного интернета" в "Интернет большой" или "мосты" контролируются, мониторятся и легко "разводятся" при любом выгодном владельцу "частной сети" случае.

И это вовсе не фантастика - "тёмные" и частные сети существуют, используются, а некоторые даже гордятся своей обособленностью.

IPv6 - клей или смазка?

Протокол IPv6 взаимодействует с IPv4 не напрямую. Основанный на IPv6 Интернет не является продолжением классического Интернета на IPv4. По сути, IPv6 - это почти полная замена Интернету IPv4.

Но нам никто не помашет флажком в тот день, когда весь Интернет станет IPv6.

Интернеты IPv4 / IPv6 будут достаточно долго сосуществовать и взаимодействовать.

Даже если Интернет не будет дальше фрагментироваться, то все равно - IPv4 и IPv6 образуют два разных острова.

Короче - Интернет уже фрагментирован вдоль границы между IPv4 и IPv6.

Разумеется, между устройствами IPv4 и IPv6 уже наведено множество мостов, мостиков и переправ, причем, таких, что пользователь, скорее всего, даже не заметит, каким из "интернетов" он пользуется в данную секунду времени. Предпринятые меры достаточно успешны в маскировке, но никто не исключает разрыва.

Сейчас выпускается множество новых устройств с "двойным стеком", а выбор между "островами" делается пользователем и поставщиком услуги. И даже больше - в любой момент можно сделать осознанный или автоматический выбор протокола для конкретного соединения.

Устройства с "двойным стеком" похожи на блоки питания, которые могут быть подключены в европейскую сеть 220 вольт или энергосеть США со 110 вольтами. Тот факт, что эти блоки питания могут работать либо с европейской, либо американской энергосетью совсем не означает, что европейская и американская энергосистемы слились и стали одной сетью. Точно так же устройства с одновременной поддержкой IPv4 и IPv6 не означает, что интернеты IPv4 и IPv6 слились и стали одним.

IPv6 был задуман для поддержки огромного, глобального и единого интернет-адресного пространства. Однако, существует факт, что внедрение IPv6 требует или развертывания "посредников" (proxy), или полную замену "устаревшего", но еще вполне работоспособного оборудования.

И вот, в объективной реальности мы уже имеем два интернет-острова и это считается совершенно нормальным, и где-то даже рутинным, явлением.

Распределение адресного пространства - бюрократия мешает

Если мы хотим забыть про архитектуру NAT, то имеется одна задачка, которая перечеркивает все преимущества огромного адресного пространства IPv6 - это необходимость получать адресные блоки. При этом, IP-адреса IPv4 совершенно объективно уже закончилось. Но это не отменяет ни процедуры распределения адресов, ни необходимости оплаты "услуг" регистратору, ни необходимости "защиты" адресного плана фактическим использованием адресов.

Эдакая мелкая задачка на "умственную полноценность" для оператора связи: "Хм, если большая часть трафика моих клиентов все равно должен пройти через прокси и множество других промежуточных устройств, то почему я должен беспокоиться о получении блока адресов? Может быть, было бы проще просто пропускать IPv6 из частной сетки через мой прокси в IPv4 (или наоборот) и все будет работать. И вот, кстати - тогда я могу самостоятельно назначать клиентам адреса IPv4 или IPv6, и избежать всей этой канители с оплатой и бюрократией при присвоение адреса".

Фрагментирующие силы

Появление единого и глобального Интернета в середине 1990-х годов было обязано одному сетевому приложению - WWW. Но сейчас этот стимул уже не столь актуален.

И дело вовсе не в том, что у пользователей пропало желание пользоваться бесшовным серфингом по веб-страничкам, нет. Просто, собственно WWW развивался таким образом, что "переходы по гиперссылкам" могут (и будут) адекватно поддерживаться даже при наличии границ и барьеров в Сети.

Такое восприятие очень важно: если Интернет может быть фрагментирован так, что восприятие целостности не нарушается или пренебрежительно мало, то аргументы в пользу "единого, глобального и открытого" адресного IP-пространства, становятся несущественными.

Тут можно, кстати, привести пример российского блэк-листа - большинство пользователей почти никогда (или очень редко) не встречаются с "экраном блокировки имени РКН", и пока это никого не напрягает. А как только начинает напрягать, в ход идут десятки способов обхода блокировок, и это опять никого не напрягает. Для 99,9% пользователей Интернет никак не изменился, хотя на самом деле это не так.

Гораздо больше "напрягает" то, что опять же подавляющее большинство пользователей не владеет иностранными языками, и, например, находя "смешной ролик" на Youtube на чужом языке,

обижаются, что не могут понять, в чем смысл шутки.

То есть, можно сделать вывод о том, что каких-либо "железобетонных" аргументов нет ни в пользу "глобальности" Сети, ни в пользу ее фрагментирования. Просто имеет место быть накопление доводов в обе стороны, что всё же не добавляет очков сторонникам глобальности, но и не не дает пока перевеса сторонникам ограничений. Но всё же, трещины в ткани "единого и неделимого" - накапливаются.

И что важно, небольшие трещинки являются предвестниками раскола, разлада и, в конечном итоге, слома всей системы.

И что же движет нас к фрагментации и появлению интернет-островов?

Никто не чувствует себя в безопасности

Почти каждый день мы получаем новости об еще одной удачной атаке злобных хакеров, репорты об утечке приватных данных или появлении оченердной уязвимости в системах безопасности.

Все (ну, многие - точно) чувствуют страх, что их системы как-то уязвимы.

Когда-то очень логичная централизация современной системы регистрации доменных имен, сегодня ставится под сомнение, поскольку является очень очевидной точкой отказа всей Интернет-экосистемы и является вожделенной целью для хакерской атаки. Все чаще проявляется интерес к децентрализации DNS или вообще замене системы, где единой точки отказа или управления не будет архитектурно.

Предполагается, что новые технологии (например DNSSec или что-то типа OpenDNS) будут более безопасными, что, в общем-то, верно и правильно. Тем не менее, с фронтов информационных войн продолжают приходить сводки, которые сообщают нам, что даже новейшее и самое распрекрасное программное обеспечение компьютеров и техники, содержащей компьютеры (мобильные телефоны, принтеры, маршрутизаторы и прочие IoT), являются уязвимыми к целенаправленным атакам.

Люди и организации начинают реагировать на такой шум тем, что для собственной безопасности они должны просто отключить, хотя бы частично, подключение к Интернету. А критически важные системы, по определению, не должны быть физически подключенными к Сети. Даже есть специальный термин: "air gapped" - "воздушный зазор". И вообще - важные системы, которые не просто "посмотреть котиков", а что-то серьезное - банк или управление атомной станцией - лучше капитально огородить DMZ. Или вообще сделать абсолютно автономными, выпуская "в мир" только что-то очень простое, что можно контролировать до байта.

Другими словами, операторы сетей и компьютерных систем начинают мыслить в терминах средневековых ленд-лордов: они хотят стену вокруг своей делянки.

Сетевые брандмауэры существуют уже достаточно давно. Но новая движуха все больше напоминает лозунг "будь самостоятелен", чем "будь ко всем подключен". Если брандмауэр это "ров с водой вокруг замка", над которым имеется подъемный мост, то свежая концепция больше напоминает "ров с водой вокруг замка, кишащий аллигаторами, который можно пересечь только на вот этой лодке со специальным надзирателем с алебардой". Не слишком образно?

Коммуникации в жизненно важных отраслях

Движение в сторону разграничения и изолированности сетей в пользу информационной безопасности становится еще более важным по мере того, как Сеть проникает в такие отрасли, где под угрозу ставится жизнь и здоровье человека. Это действительно важно и нужно в таких областях, как медицина или управление ЖКХ. И уж совершенно недопустим прямой коннект с глобальной сетью на объектах сверхповышенной опасности - ядерная энергетика, вооружение, управление транспортом и т.д., и т.п.

Управление рисками в области информационной безопасности также подталкивает к созданию дополнительных барьеров и границ в Интернете. И со временем эти барьеры будут становиться все выше, а рвы, разделяющие интернет-острова - все шире.

Возвышение приложений

В 2007 году, после появления iPhone, мы увидели новую волну интернет-инструментов: "мобильные приложения".

И что интересно - приложения могут быть совершенно равнодушны, и даже слепы к сетевым барьерам. Или наоборот - приложения могут очень чутко относиться к таковым, если разработчик

приложения понимает, что барьеры на пути IP-пакетов от приложения позволят добиться коммерческого успеха.

По гамбургскому счету, пользователю абсолютно до лампочки, как там всё внутри устроено, и какие магические силы заставляют работать любимых "покемонов". Для простого пользователя это магия и колдунство; никто не станет заботиться о протоколах, их красоте или уродстве, если шарики просто бросаются, при условии включения функции "мобильный интернет". Это просто водопроводная труба, и ничего больше.

Мобильная специфичность заключается в том, что пользователю не нужно вообще знать никаких веб-адресов - приложение устанавливается из "маркет-плеса" и просто работает. URL-адреса становятся ненужными. DNS и доменные имена становятся все менее и менее заметными для пользователей или превращаются в мнемонические короткие заклинания. Вплоть до голосового ввода.

Принцип "end-to-end" также становится не слишком очевидной необходимостью, ибо мобильное приложение просто знает куда, как и к кому обращаться. Нажал на иконку на мультитач-экране - и все. Приложение должно работать и отправлять байт информации, делая обладателю смартфона "хорошо" и "просто".

И подавляющее большинство мобильных приложений используют очень немногие интернет-протоколы. Строго говоря - один. HTTP/HTTPS. Некоторые еще могут SMTP/SMTPS/IMAP. Некоторым иногда нужен DNS. И совсем редко - SIP.

И каждый из этих протоколов легко проксируется.

Каждый из этих протоколов прекрасно может жить в условиях интернет-островов и быть "мостом" между хорошим, годным обособленным итернетиком, и большим, глобальным Интернетом.

Заплати и повинуйся: вы еще не утомились от арендных платежей?

Определенные интернет-активы, в частности это относится к адресному IP-пространству и системе доменных имен, находятся в ведении специальных регулирующих органов. Например, региональные реестры IP-адресации ведут RIR, а за домены отвечает ICANN. Эти активы можно получить только пройдя специальный бюрократический процесс, который включает в себя оплату прогрессирующих арендных ставок и подписание договора, ограничивающего вас в правах.

Медленно, но верно множество компаний начинают понимать, что эта ситуация несёт исключительно затраты и добавляет рисков. Если бизнес по какой-то причине пропускает шаг в бюрокартическом танце с регулятором, то внезапно может обнаружить, что он потерял какие-то интернет-активы от которых может многое зависеть. Случаев, когда организации просто пропускали дату платежа нескольких долларов за доменное имя - пруд пруди. Ситуация породила новый слой услуг, причем иногда довольно дорогих, с помощью которых корпорации и владельцы товарных знаков передавали в управление товарные знаки и доменные имена аутсорсерам. Просто потому, что кто-то же должен обрабатывать нескончаемый поток уведомлений о постоянно изменяющихся правилах ICANN, среди которых контактные проверки, обязательные периодические регистрации и продления аренды.

К примеру, вы не можете арендовать какое-то доменное имя на срок не более десяти лет - сколько не плати. С одной стороны это логично - за десять лет может многое случиться, включая смерть физического лица - владельца домена, или банкротство компании. И какое-то очень хорошее имя домена может просто зависнуть на долгий срок. Но имеется и обратная ситуация - корпорация процветает, но за десять лет ответственный за регистрацию домена сотрудник просто уволился, забыв передать пароль от "кабинета управления". И компании придется долго и нудно доказывать, что домен принадлежит именно вот ей, а не конкурентам или кибер-сквоттерам.

Стоимость за регистрацию и продление доменов также достаточно произвольно изменяется. Впрочем, не так быстро, как цены на нефть, но если у вас в управлении несколько сотен доменов, то можно легко "выйти из бюджета".

Все эти регуляторные политики по управлению интернет-активами стимулируют людей и организации изыскивать альтернативы, которые предложат непрерывность бизнеса и более уверенное завтра.

Так и получается, что в мире интернета, основанного на концепции "острова-и-мосты", совсем не обязательно придерживаться правил одной всемирной убер-регулирующей организации. Вместо этого, каждый "остров" просто примет свою собственную удобную для именно вот этого "острова" политику управления сетевыми активами, и будет чувствовать себя прекрасно.

Презентация нового курса управления использованием Интернета, или история про то, как будет выглядеть сбой

Изначально, ICANN была создана с целью сделать так, чтобы хвост вилял собакой. И в этом сия общественная организация преуспела, причем, за рамками всех ожиданий. Но сейчас этот регулирующий орган стоит слишком дорого, забюрократизирован сверх всякой меры и самое главное - у органа есть власть, с помощью которой определенные коммерческие или, что хуже, государственные органы, могут блокировать любые изменения в развитии Сети сетей.

(Есть мнение, что Чарльз Диккенс еще в 1857 году предсказал появление ICANN в "Крошке Доррит" - см. главу 10, "Содержит всю науку управления").

ICANN, по сути, захватила власть над большей частью Интернета, введя искусственную экономическую систему, где принцип "долго, дорого, некачественно" возведён в ранг абсолюта. Капризная и произвольная система "согласований", например, отсрочила введение новых доменных зон первого уровня на несколько лет. И это только надводная часть айсберга.

ICANN сохраняет свое понимание Интернет-системы, контролируя несколько ключевых функций, из которых наиболее значимое - торможение новых поколений корневых DNS зон.

Имеется ввиду, что иногда порядок нумерации доменных имен часто путают, и домены верхнего уровня называют нулевыми. На самом же деле, доменом нулевого уровня является "." (точка) и правильный порядок нумерации уровней доменов таков:

1. . (точка) — домен нулевого уровня,
2. .org — домен первого уровня, называемый также доменом верхнего уровня или зоной,
3. wikipedia.org — домен второго уровня,
4. ru.wikipedia.org — домен третьего уровня.

Изменения "точки" предлагают, и уже довольно давно, несколько потенциальных "конкурентов ICANN", что естественно в сей славной конторе спускается на тормозах.

А еще, ICANN многими странами воспринимается, как символ гегемонии Соединенных Штатов через Интернет.

Мы уже начали жить в фрагментированном Интернете

Наличие таких штук, как NAT и ALG наглядно демонстрирует, что есть совершенно жизнеспособная деятельность в "частных" адресных пространствах.

Иные корпорации просто заставляют своих сотрудников использовать зашифрованные виртуальные частные сети в то время, когда они работают вне офиса.

Существует множество решений, которые, используя концепции Software Defined Network, позволяют строить наложенные сети любых масштабов и степени сложности. И при этом, наложенная сеть выглядит совсем как внутренняя локальная сеть.

А еще существуют очень большие сетевые сообщества, в которых люди просто проводят все своё интернетное время. Для иных российских пользователей весь интернет ограничен "одноклассниками" и они просто не представляют себе, что существует еще что-то - им просто этого хватает, а остального они не понимают. Для юзеров из других стран, особенно с не очень развитой интернет-культурой, таким местом стал Facebook. Эти люди просто не могут понять, но они уже живут на острове. И только иногда появляются мосты, которые заботливо переадресуют их в "большой WEB", но при первом же замешательстве могут вернуть их в привычный и понятный мир демотиваторов и котиков.

Интернет пока не полностью фрагментирован - время еще не пришло. Но в монолитности уже полно трещин. И появляются люди, которые создают и используют эти трещины, чтобы извлечь из них собственную выгоду.

Создавая реальность

Скорее всего, вы уже устали читать этот длинный текст со множеством повторяющихся аргументов и камбэков (ох, Карл, как же я уже устал переводить это!). Но потерпите еще немного - сейчас мы дойдем до главного. Ну, например, совершенно логичный аргумент, которым вы можете возразить автору: "Это всё предположения, нет никаких предпосылок к тому, чтобы это стало реальностью."

Возможно, вы правы. Вполне может быть, что IPv6 после десятков попыток за двадцать лет

"перезагрузить интернет", внезапно ускорится в проникновении, и в какой-то момент рраз, да заменит весь существующий IPv4. И все технико-экономические причины, вынуждающие людей, корпорации и государства огородиться, изолироваться и защититься, будут волшебным образом устранены. Вполне возможно.

Но что, если не правы именно вы? Что вы станете делать, если стимулирование фрагментации интернетов продолжится? А что, если описываемое явление интернет-островов и мостов между ними, станет реальностью?

Острова

Мир интернет-островов и мостов между ними, скорее всего, будет развиваться и шириться из уже очевидных "закрытых садов" современного Интернета.

Первым может быть Китай.

Запросто может быть Россия.

КНДР уже остров, причем, мостов с миром там строить даже и не собираются.

Универсальные (мобильные+фиксированные) провайдеры, такие как Verizon и AT&T - уже в значительной степени ступили на путь строительства собственных островов.

Интернет-компании, которые занимаются развитием социальных сообществ и эксплуатируют идею user generated content, скорее всего, ранние строители собственных островов. Ну, вот тот же Facebook, Google, Linked-In. И, может быть, даже Microsoft.

Остров Netflix - звучит как название очередного шоу. Но вполне вероятно, что именно так будет называться один из первых островов.

И это мы не упомянули религиозные и культурные группы, которые уже долгое время поддерживают фрагментацию WEB, хотя бы тем, что никогда на религиозном сайте вы не увидите ссылки на сайт конкурирующей религии или на светский контент. Кстати, Ватикан уже получил домен верхнего уровня .church. И теперь сможет создать отдельные кластеры сайтов на практически любом известном языке, тем самым вырезав кусочек мирового Интернета. Мормоны, надо заметить, не отстают в активном строительстве интернета в интернете имени себя.

И Русская Православная Церковь так же пытается сделать что-то огороженное и православное, создавая собственные социальную сеть "Елицы" и мессенджер к ней.

Но скорее всего, множество островов будут появляться вокруг языка пользователей. Например, отчетливо виден интернет-остров, образованный вокруг арабского языка. Китайского. Японского. А что вы знаете об интернете в Бразилии? А ведь там проживает народу больше чем в России, хотя уровень проникновения чуточку меньше. Пока.

Самый очевидный строитель интернет-островов - это группы людей и корпорации, которые нуждаются в серьезных барьерах, в целях информационной безопасности. Очень просто - если существует возможность утечки критически важной информации, то лучше все же отключить сотрудникам возможность общаться с рабочего места с помощью всяческих он-лайн чатов и мессенджеров. Универсальный ответ на проблемы и угрозы инфобезопасности - "проще и надежнее отключиться от Интернета".

Мосты

Существуют подозрения, что немногие люди или организации будут осознанно идти по дороге с явной целью построения интернет-остров и мостов для них. Скорее всего, это явление будет приходить в нашу жизнь медленно и незаметно.

В начале на островах будут точно так же, как и вообще в интернете в целом, использовать те же IPv4 и IPv6 адресные пространства.

Но использование общего публичного адресного пространства приносит риск. Риск заключается в том, что те пакеты, которым ставят задачу, так или иначе пройти "брандмауэр", смогут бесконтрольно "бродить по острову" и таки нанести ущерб. То же самое про любой исходящий трафик: все, что может вытекать наружу через брандмауэр без ограничений - будет вытекать.

Так что, у сетевых администраторов будет соблазн сказать: "давайте сделаем больше, чем просто установить брандмауэр - давайте использовать отдельную IP-адресацию". Затем будут скрупулезно рассмотрены решения NAT, которые оставят желать лучшего. Это, в свою очередь, натолкнёт на идею создания технологии шлюза прикладного уровня.

Непрерывные требования со стороны правоохранительных органов и национальной безопасности в сочетании с разочарованием людей с "зашифрованным трафиком", будут стимулировать развертывание мостов на основе Application Level Gateway. И уже в нём различные потоки приложений будут в скором времени или заблокированы, или может быть введен "прозрачный шлюз" для некоторых конкретных протоколов и/или конкретных интернет-ресурсов где-то в недрах ALG.

Шаги

Изменения, которые приведут к концептуальным "интернет-островам и мостам между ними" будут очень плавными и эволюционными. Шажочек за шажочком. Не будет никаких революций с красными, черными и радужными флагами. Не будет никаких грандиозных и скоординированных действий "тёмных сил". Всё будет происходить по принципам, на которых, собственно, и строился интернет - инновационная деятельность "с краю". То есть, как раньше сети подключались к другим сетям, и что-то там внутри у себя подкручивали и довинчивали, точно так же будет происходить и сейчас. То есть, в различных государствах, или корпорациях, или сообществах, будут сначала медленно огораживаться за NAT. И это уже происходит.

Затем будут пытаться (нет - никто сразу не дёрнет за рубильник!) ограничивать какие-то движения пользователей, чутко реагируя на их реакции. Например, использовать различные механизмы "проводки данных через край" (Application Data Units или ADU - затрудняюсь с адекватным переводом, WF) по TCP или HTTP/HTTPS прокси и ALG.

Интернет не является особо хрупкой средой: крупные коммерческие операторы, особенно те, что работают в потребительском секторе (например, Comcast и Verizon) уже давно безнаказанно делают всяческие не очень корректные вещи с подменой трафика и, например, деградацией определенных видов трафика - это хорошо известно. Сервис Xfinity Comcast уже неоднократно был ловлен на том, что подменял некоторые элементы веб-страничек, запрашиваемых пользователями - подставлял какую-то рекламу поверх пользовательского контента.

Попробуем перечислить некоторые из шагов, которые скорее всего будут сделаны, чтобы продвигаться в сторону концепции "интернет-острова и мосты между ними". Эти шаги не обязательно будут происходить именно в такой последовательности:

- Возникновение новой системы имен DNS на базе таких известных систем анонимизации и сокрытия трафика, как .onion или .tor. Люди начнут понимать, что не только ICANN может выдавать доменные имена первого уровня. На самом деле, даже в текущей ситуации уже могут существовать не только канонический путь "с точкой" от нулевого домена. Нулевой домен вполне может начинаться, пусть и только логически, но с других уровней. Например, с .tor
- Появление новых корневых DNS-систем, которые начнут конкурируют или дополнять ICANN / NTIA / Verisign. И это начнётся с осознания того, что на самом деле в Интернете может существовать не одна, и не две корневых системы получения имен. Или даже можно будет отказаться вообще от имен, которые существуют только для того, чтобы пользователь вводил имя сайта на понятном языке, не запоминая цифр. Согласитесь, что мобильным приложениям, чаще всего, DNS просто не нужны.
- Множество компаний, корпораций или просто групп людей, которые в настоящее время находятся за NAT, будут последовательно модернизировать свои системы и со временем с "простого NAT" перейдут к более умным и совершенным ALG. Возможно, появится что-то новое или хорошо забытое старое, и эти системы начнут называть как-то более звучно - "брандмауэр", "регулировщик нагрузки", "контроллер пограничного шлюза". Но, скорее всего, просто "прокси".
- Виртуальных частных сетей, которые пронизывают сети "физических провайдеров", станет очень много. Эти сети нужны будут для "наведения мостов" или для связи удалённых географически мест в свой собственный "логический остров".
- Следующий возможный шаг - наложенные сети на базе Software Defined Network (SDN) с собственным адресными пространствами и "потоками". По сути, это те же самые виртуальные частные сети, только лучше, поскольку более управляемы и понятны конечным пользователям на уровне логики восприятия. И при этом, не нужно будет знать функций TCP/IP.
- CDN для OTT. Поставщики контента уже строят и/или используют CDN для улучшения качества сервиса. Но особый интерес будет представлять использование наложенных сетей из предыдущего "шага" - VPN и SDN. По сути, это база для развития OTT по наложенным сетям, куда провайдер, скорее всего, вмешиваться не сможет физически.

Все эти изменения будут происходить в частном порядке, медленно и спокойно. Просто в один прекрасный день мы проснёмся с пониманием того, что Интернет уже нынче не тот.

А что там с "Сетевым Нейтралитетом"?

Суть сетевого нейтралитета заключается в попытке предотвратить желание операторов дискриминировать некоторых своих клиентов на основании типа трафика, источника трафика или назначения трафика. Исключительно в экономических целях, конечно.

Сетевой нейтралитет представляет собой попытку создать своего рода "единого мирового провайдера", где для всех игроков формируются одинаковые правила. В некотором смысле, NN - это очередная попытка вдохнуть жизнь в принцип "end-to-end".

В данной статье утверждается, что на уровне IP-пакетов, принцип "end-to-end" умирает, если уже не умер. При этом, нет явного понимания, что усилия по установлению NN - это хорошо для рынка. В лучшем случае, Сетевой Нейтралитет может предотвратить и как-то сгладить наихудшие последствия отмены NN - это шантаж операторов и попытки собрать деньги "с двух концов трубы".

С одной стороны, автор (Крал Ауэрбах, напомню) сторонник недискриминационной передачи пакетов IP-провайдерами. Но также автор признает, что не все виды трафика равны по чисто потребительским качествам и средствам обеспечения надлежащего качества: голосовому Voice-Over-IP (VoIP) трафику необходим низкий уровень потери пакетов, низкая задержка транзита, а также низкое изменение этой транзитной задержки (т.е. небольшой джиттер) для относительно легкого (50 пакетов в секунду) потока равномерно распределённых пакетов. Асинхронной передаче больших файлов нужна сетевая услуга, которая позволяет использовать пакеты большого размера, часто сгруппированных в пачки. А потоковому видео требуется такой способ передачи, который сможет обеспечить низкие потери, низкий уровень джиттера для потоков, и который сможет обеспечить периодические всплески больших пакетов. Разумеется, для провайдеров имеет смысл научиться распознавать и учитывать эти различные виды потребностей.

И вот тут-то концепция "интернет-острова и мост между ними" очевидно, намеренно и отчетливо НЕ нейтральна. Островная изоляция является полной противоположностью свободного и открытого мира с сетевым нейтралитетом. Как остров решит поступать с данными видом трафика - так тому и быть. При этом, пропаганда сетевого нейтралитета, кажется, совсем не отбивает у множества людей, корпораций, правительств, религий, культурных групп и целых государств желания создавать стены, в которых имеется лишь несколько хорошо контролируемых порталов.

Вывод

"Интернет-острова и мосты между ними" будут вне зависимости от наших желаний или предпочтений.

Приход островов не примет вид цунами. Скорее всего, это будет выглядеть как медленный прилив.

Пользователи приложений не будут особенно обеспокоены тем, что операторы, разработчики и поставщики, создающие "острова и мосты" имеют собственный. В конце концов, зарабатывать деньги - это нормально. Но беспокойство будет вызывать только то, что будет ухудшать их положение "клиента оператора связи". Никто не заметит умного прокиска до тех пор, пока он не перекроет доступ к нужному телекоммуникационному приложению. И пока пользователь не замечает своей "жизни на острове" - всё будет хорошо.

Впрочем, обратное утверждение тоже работает - если пользователю на каком-то острове станет некомфортно, он просто уйдет к конкурирующему оператору.