Интернет-корпорация по присвоению имен и номеров

Отчет Комиссии по инновационному развитию технологий идентификации

15 мая 2014 года – окончательная версия

Содержание

1. Вступление

Комиссия по инновационному развитию технологий идентификации (ITI) была создана Интернет-корпорацией по присвоению имен и номеров (ICANN) со следующими целями:

1. Разработка дорожной карты технологического развития системы доменных имен (DNS) и других идентификаторов

2. Разработка рекомендаций о передовых практических методах и эталонных системах

3. Управление технологиями в сфере операционной деятельности, безопасности, политики и технических функций ICANN

4. Сотрудничество с сообществом ICANN и общественностью по вопросам технологий

Состав комиссии был выбран в течение сентября и октября 2013 года, а ее председателем стал Пол Мокапетрис (Paul Mockapetris). Члены комиссии действуют от своего имени, а их принадлежность к организациям используется только в целях идентификации.

- Яри Арко (Jari Arkko) — председатель, Инженерная проектная группа Интернета (IETF)
- Рик Буави (Rick Boivie) — научно-исследовательский центр IBM им. Томаса Дж. Уотсона (Thomas J. Watson Research Center)
- Анн-Мари Эклюнд-Лоуиндер (Anne-Marie Eklund-Löwinder) — менеджер по безопасности, Фонд инфраструктуры интернета
- Геофф Хьюстон (Geoff Huston) — главный научный сотрудник, Азиатско-тихоокеанский сетевой информационный центр
- Джеймс Сенг (James Seng) — генеральный директор, компания Zodiac Holdings
- Пол Викси (Paul Vixie) — генеральный директор, компания Farsight Security
- Лиция Чанг — лауреат фонда им. Постеля, профессор кафедры программирования, Калифорнийский университет в Лос-Анджелесе

Были проведены встречи в рамках IETF-Ванкувер (ноябрь 2013 года), на конференции ICANN в Буэнос-Айресе (ноябрь 2013 года) и в офисе ICANN в Лос-Анджелесе (в январе 2014 года). Совещание в Буэнос-Айресе было открытым для общественности, а сводная информация о деятельности комиссии была также представлена на двух вебинарах в январе 2014 года. В дополнение к указанным совещаниям, обсуждения продолжались по электронной почте и

другими подобными способами. По проектам отчетов проходит сбор комментариев с февраля 2014 года.

Председатель хотел бы поблагодарить членов комиссии за все ценные выводы и идеи, а также ICANN за оказанную комиссии поддержку. Он также благодарит сотрудниц корпорации ICANN Элизу Герич (Elise Gerich) и Алис Джансен (Alice Jansen), которые делились своими идеями и обеспечивали поддержку всей работы комиссии.

2. Стратегия комиссии

Название комиссии выбрано не случайно. Рамки работы были расширены за пределы DNS как таковой из-за признания растущей важности идентификаторов всех видов для интернета, а также роли ICANN в управлении другими идентификаторами. Неполный список текущего портфеля работ ICANN включает:

- Доменные имена
- Номера автономных систем (AC)
- Адреса IPv4
- Адреса IPv6
- Адреса групповой рассылки
- Номера портов
- Номера протоколов
- Реестр унифицированных идентификаторов ресурсов (URI)
- База управляющей информации (MIB)
- База данных часовых поясов

Однако параллельно с этим расширением временные рамки работы комиссии были сжаты с года, как было определено первоначально, до приблизительно шести месяцев. Это привело к ориентации на DNS в большей степени, чем мы надеялись.

Чтобы компенсировать это, комиссия взяла на вооружение следующие принципы:

- Стремиться записывать все обсуждаемые идеи, но сосредоточить внимание на новых
- Искать конкретные мощные тенденции (например, расширение интернета, тенденции в архитектуре процессоров)
- Искать «острые» проблемы
- Избегать сосредоточения усилий на «хорошо вспаханных полях» (например, на развертывании DNSSEC, существующих стратегиях устранения конфликтов) и искать новаторские идеи

Центральная задача комиссии — представить ICANN информацию для процесса стратегического планирования. Хотя комиссия не обсуждала идеи, близкие к оперативным потребностям ICANN, она не ограничивала себя идеями, которые могли бы быть реализованы непосредственно ICANN. Реализацию многих рассматриваемых в настоящем документе идей было бы наиболее естественно отнести к сфере компетенции IETF или иной организации. Некоторые идеи поднимают политические вопросы, которые мы не решили, а только обозначили.

И наконец, в связи с огромным объемом деятельности в области идентификаторов распределенных систем, комиссия провела выборку по пространству. Читателю не следует из

этого заключать, что комиссия была осведомлена о всей происходящей деятельности или что идеи, не отраженные в этом отчете менее важны, чем отраженные здесь идеи.

3. Дорожная карта

Идентификаторы продолжают оставаться болезненной темой в сообществе интернета. В краткосрочном плане в интернете появятся новые домены верхнего уровня (TLD). Facebook, как и Google, старается сделать так, чтобы вход с помощью учетной записи их сайта стал единым путем выхода в интернет. В долгосрочном плане у научного сообщества есть много различных проектов, в том числе сеть, ориентированнаю на контент (Content Centric Networking, CCN), сеть, ориентированнаю на информацию (Information Centric Networking, ICN), сеть с именованными данными (Named Data Networking, NDN) и многие другие варианты. Хотя специалисты не могут достичь согласия относительно наименования этой области, все они едины во мнении, что контент должен определяться собственным именем, а не местоположением, и должно осуществляться адаптируемое кеширование. Авторы других предложений настаивают, что гениальной идеей будущего являются одноуровневые имена, и самосертифицирующиеся имена должны лечь в основу любой новой системы.

Идентификаторы — основа любой сети в плане необходимости уникального определения компонентов сети для других компонентов этой сети. Кроме того, современные сети не являются единым однородным доменом, и представляют собой сочетание ряда технологий, в связи с чем возникает необходимость сопоставления между областями идентификации. Эта функция сопоставления выполняется несколькими способами. В контексте интернета одна из наиболее заметных областей идентификации — это область доменных имен, которая является иерархически структурированным пространством имен. С этим пространством имен связана функция сопоставления, позволяющая сопоставить доменные имена с другими идентификаторами (например с IP-адресами). При рассмотрении перспектив развития идентификаторов, необходимо помнить о различиях между областью идентификаторов и функцией сопоставления и анализировать перспективы развития каждой из них.

В современном интернете комиссия обнаружила несколько факторов, которые будут обеспечивать расширение использования DNS, а также несколько факторов, которые будут оказывать противоположное воздействие. Не все эти факторы являются техническими, и это противостояние основано скорее на дарвиновском подходе, чем на элегантности или других положительных свойствах.

<u>Действующие факторы расширения</u>

- Система DNS пользуется преимуществом как более старая система, которая встроена почти в каждое устройство, выходящее в интернет. Простой рост существующей базы будет расширять объем ее использования. Например, приложению, которому необходимо передавать данные через брандмауэры и обеспечивать их кеширование по всему интернету, DNS доступна в качестве уже существующей базы.

- Новые TLD будут предпринимать попытки монетизации своих брендов. Хотя техническое сообщество к ним относится с большим скептицизмом, более тысячи новых брендов будут бороться за процветание, и есть вероятность инноваций и некоторых сюрпризов.
- Новые возможности, например возможности обеспечения безопасности благодаря расширениям безопасности системы доменных имен (DNSSEC) или аутентификация именованных объектов на базе DNS (DANE), могут стимулировать более широкое использование.
- Новые данные в DNS способны расширить ее использование, особенно в сочетании с DNSSEC для гарантии подлинности. Один член комиссии выступает за публикацию «дня рождения», информацию о регистраторах и «времени, истекшем с момента делегирования" доменов в качестве базовой информации о репутации. Другие предлагали использовать DNS в качестве реестра адресных блоков, автономных систем и т. п. ICANN ограничила применение некоторых меток в доменных именах, и реестр таких данных в режиме реального времени может оказаться целесообразным решением, особенно когда бумажные спецификации оформляются разными алфавитами. На практике эти базы данных могут быть общедоступными или конфиденциальными.
- Для разных людей интернет вещей значит разное, но обычно это значит в частности огромное количество предметов в одной или более огромных распределенных баз данных. DNS была предложена в качестве строительного блока в нескольких типах архитектур интернета вещей и прототипов, как часть общедоступной DNS и в качестве одной или более частных баз данных DNS. Комиссия хотела бы иметь больше времени для более полного изучения этого вопроса, рекомендует его изучить далее и считает, что DNS также может иметь определенную роль.

Действующие факторы сжатия

- DNS — давно существующий стандарт, который одновременно является и препятствием, поскольку логическая схема DNS, встроенная в точки доступа WIFI, кабельные модемы и модемы цифровых абонентских линий связи (DSL), брандмауэры, маршрутизаторы и программную базу интернета, часто ограничивает рамки использования и сдерживает инновационное развитие. Реализация DNS далека от совершенства, не всегда актуальна и не всегда соответствует стандартам. Эти проблемы сдерживают внедрение DNSSEC и делают проблематичным внедрение любых новых видов данных или функций DNS. Это в свою очередь приводит к такой практике проектирования, когда все использование ограничивается адресными и текстовыми (TXT) записями. Такое окостенение присуще не только DNS.
- Существует коммерческая заинтересованность в управлении («владении») окном поиска и/или пространством идентификаторов. Интерес здесь заключается в том, чтобы отслеживать намерения пользователя в произвольной форме и скрывать от него общедоступные ресурсы интернета. Мы заметили тенденцию жесткого кодирования устройств на использование конкретной службы DNS, а также расширений собственной разработки, которые являются путем к раздробленности.

- Пользователи отдают предпочтение интерфейсу с более широкими возможностями. Вместо ввода имен DNS пользователи и приложения часто применяют поисковые и другие механизмы для доступа к конкретной информации. К примеру, строка унифицированного адреса ресурса (URL) в браузерах сегодня во многом является инструментом поиска. Современный пользовательский интерфейс — мобильное устройство, которое не благоприятствует клавиатурному вводу. Использование модулей распознавания речи и других видов искусственного интеллекта в строке браузера приводит к несовместимости продукции разных поставщиков. Например, член комиссии Джеофф Хьюстон (см. замечание) провел эксперимент с поиском слов «Geoff.Huston» в разных браузерах и не заметил практически никакой схожести в результатах поиска при использовании продуктов разных поставщиков. Отсутствие схожести допустимо при браузерном поиске, когда ожидается, что пользователь проверит результаты, однако оно представляет опасность в отношении файлов конфигурации систем — это одно из оснований для беспокойства в плане совпадений.

У комиссии возникло ощущение, что хотя использование системы DNS может сократиться за счет пользовательского интерфейса, она скорее всего останется инфраструктурным инструментом. Одной из аналогий является тот факт, что DNS не бумажная книга, которую могут вытеснить электронные книги, а набор компьютерных команд, для доступа к которым используются языки более высокого уровня.

Мнения относительно возможности или целесообразности стремления к возрождению или реструктуризации DNS разделились. Эта технология обсуждается в разделе «Основы DNS» настоящего отчета. Также существует вопрос определения политики в отношении того следует ли ICANN попытаться сохранить и продлить действие системы DNS. Если это так, то следует понять как обеспечить существование согласованной архитектуры с учетом расхождения мнений в постоянной группе ICANN — IETF (где предположительно и будет выполняться эта работа) и у остальных участников интернета.

Долгосрочная перспектива

Одной из тем на долгосрочную перспективу является модель сети с именованными данными. Эти ключевые идеи включают доступ к контенту по названиям, повсеместной цифровой идентификации, адаптируемому кешированию и схеме прохождения поиска, в рамках которой запросы и ответы проходят по одному и тому же пути. Модель для маршрутизации запросов иногда определяется просто как использование иерархии имен для принятия решений о маршрутизации на основе совпадения наиболее длинного префикса, которое скептики считают не поддающимся расширению. Так или иначе, создано программное обеспечение, оборудование и несколько испытательных стендов для проверки сетевых характеристик. Наиболее очевидными областями применения является распространение контента, но сторонники этой модели заявляют о ее пригодности для управления процессами, автомобильных сетей и т. д.

В известном смысле, DNS стала первой альтернативой модернизации существующей чистой внутрисхемной коммутации (ICN), аналогично большинству нынешних подходов [Fayazbakhsh 2013], в которых предпринимаются попытки сохранить наиболее важные компоненты модели ICN. У каждого свое мнение о важности этого.

Система DNS извлекает данные по имени. Она не пытается осуществлять маршрутизацию по имени, а вместо этого использует уровень адресации интернета; такая схема исправляет то, что некоторые считают основной проблемой расширения ICN. Отчасти DNS заслужила плохую репутацию как средство туннелирования видео [Kaminsky 2004] и незаконного туннелирования доступа посредством DNS-запросов, которые выполняются до проверки подлинности в некоторых точках доступа WIFI. (Поиск термина «DNS-туннелирование» при помощи Google выдает приблизительно 1 620 000 результатов.)

У ICN совпадение наиболее длинного префикса и селекторы, позволяющие передавать медийные данные, то есть возможности, которые хоть и предполагались в части, касающейся запросов в первоначальной технической спецификации протокола DNS, но не были развиты.

Во всяком случае, если допустить возможность увеличения пакетов DNS и добавления некоторых дополнительных полей запросов, контентные услуги могут быть реплицированы в DNS. Сопоставление в ICN запросов и ответов, прошедших проверку подлинности, может стать наилучшим способом предотвращения атак на DNS с усилением.

Наконец, можно представить замещающую DNS схему NDN, которая по всей вероятности вначале будет расширенным набором средств DNS в течение переходного периода, который продлится годы или десятилетия. Все попытки улучшения архитектуры DNS должны без колебаний заимствовать элементы NDN.

ICN никоим образом не является единственной моделью для будущего, она всего лишь одна из наиболее проработанных моделей. Комиссия убеждена в том, что всегда имеет смысл постараться обобщить основные принципы, а затем изучить структуру. [Ghodsi2011] хороший пример соотношения троицы имени, данных о реальной физической личности и инфраструктуры открытых ключей (PKI).

Совсем недавно стало уделяться отдельное внимание распределению управления [Newyorker 2014] и защите персональных данных, чему система Namecoin наиболее известный пример. Существующая PKI представляет собой ресурс для крупномасштабного надзора и, следовательно, создает трудности с точки зрения защиты персональных данных. Решением может стать комбинация самосертифицирующихся объектов и используемой по согласию инфраструктуры открытых ключей или параллельное существование PKI и одноранговых (P2P) систем. Комиссия по инновационному развитию технологий идентификации (ITI) не изучала этот вопрос, но находит его очень интересным.

4. Эксплуатационные проблемы

В процессе повседневной деятельности ICANN возникает несколько проблем. По большей части они связаны с корневой зоной.

4.1.Защита корневой зоны

С учетом того, что инфраструктура корневой зоны имеет первоочередную важность, поступило несколько внешних предложений о том, что комиссии следует проанализировать технологию высоконадежных вычислений. Комиссия пришла к мнению, что могут быть основания для применения технологии этого вида в системах, используемых для изменения и подписания корневой зоны, однако анализ способов улучшения распространения подписанных данных по аппаратным средствам общего назначения являлся для комиссии более подходящим приоритетом. Разоблачения Сноудена подняли некоторые вопросы с точки зрения обеспечения безопасности материальной части, которые возможно не рассматривались при разработке существующих систем, такие как заражение BIOS, шпионское ПО, поражающее жесткий диск и т.д. [Spiegel 2014].

4.2.Репликация

У DNS всегда было два дополнительных механизма для распределения данных: заранее запланированная репликация зон и специальные запросы. С точки зрения отдельной порции данных DNS, записи ресурса (RR), она берет начало в своем первичном источнике как часть зоны, перемещается с этой зоной в результате одной или нескольких операций передачи зоны, а затем заканчивает свое движение в конечный пункт назначения, где она извлекается по запросу.

Например, корневая зона создается ICANN в партнерстве с Verisign и министерством торговли США, а затем распространяется по всем корневым серверам посредством операций передачи зоны. С концептуальной точки зрения это распределение, как и распределение любой другой зоны в DNS, может исполняться любым механизмом: при помощи магнитных лент и доставки службой Federal Express (FEDEX), по протоколу передачи данных (FTP) или Rsynch или более оптимальным образом — посредством метода инкрементального переноса зоны, при котором отправляются изменения, произошедшие со времени реализации предыдущей версии, а не вся зона. Копии могут либо принудительно отправляться посредством уведомлений DNS, либо извлекаться с использованием стратегии опроса, при которой осуществляется поиск изменений. Перенос зон безопасности может осуществляться при помощи транзакционной подписи (TSIG) и/или любого другого протокола переноса, таких как безопасность интернет-протокола (IPSEC), протокол защищенной передачи гипертекста (HTTPS) и т.д. Существуют сотни корневых серверов с копиями корневой зоны.

При необходимости получить доступ к корневой зоне пользователи направляют к ней запрос. Маршрутизация этих запросов осуществляется при помощи двух механизмов: сначала по IP-адресу пункта назначения в запросе определяется совокупность корневых серверов, имеющих общий групповой адрес, а затем система маршрутизации принимает решение о том, какой сервер в этой группе фактически получит данный запрос. Такая схема является результатом развития системы, изначально имевшей 3 корневых сервера с одноадресной передачей, впоследствии расширенной до 13 структур корневых серверов, использующих кластеры с распределенной нагрузкой, и затем эволюционировавшей до нынешней схемы (при множестве менее значительных промежуточных этапов). В упрощенном виде, «13 корневых серверов» на самом деле представляют собой «13 структур корневых серверов», которые в конечном итоге доставляют зону на сотни или тысячи отдельных серверов[1]. Причина использования всего 13 структур корневых серверов и адресации любому устройству состоит в том, что это сделать гораздо проще, чем смягчить ограничения на размер пакетов протокола пользовательских дейтаграмм DNS (UDP). Также сущестуют и другие проблемы в отношении к размеру, связанные с добавлением адресов IPv6. По пути от корневого сервера к пользователю безопасность может дополнительно обеспечиваться посредством DNSSEC.

В течение многих лет корневые серверы подвергались атакам, большая часть которых является разновидностями распределенной атаки типа «отказ в обслуживании» (DDOS). Для того, чтобы такая атака на конкретного пользователя была успешной, она должна нарушить обработку запросов по всем адресам произвольной рассылки, имеющимся в 13 различных структурах корневых серверов. Нарушение нормальной обработки запросов для части структур приводит к снижению производительности, поскольку отправителю запросов приходится выяснять, каких корневых серверов следует избегать. Это нарушение может привести к выведению из строя сервера или сетевого пути к серверу, как правило из-за перегрузки. Так, например, в ходе одной из подобных атак пользователи в Калифорнии считали, что корневой сервер в Стокгольме вышел из строя, в то время как пользователи в Стокгольме видели прямо противоположную ситуацию. Реакцией структур корневых серверов на недавнюю угрозу со стороны хакерской организации *Анонимус* стало расширение полосы пропускания и развертывание новых серверов с большой помпой.

Атака, конечно, не обязательно должна быть направлена на комплекс корневых серверов, ее объектом может быть соединение (соединения) пользователя с интернетом. Хотя размер ущерба ограничен, соотношение сил атакующей бот-сети и отдельного предприятия как правило оказывается в пользу атакующего, даже когда речь идет о крупных организациях.

В своей практической деятельности некоторые члены комиссии рекомендовали организациям распространять во внутренней сети копии корневой зоны **и любых других критически важных**

[1] В настоящее время двумя структурами корневых серверов управляет одна организация — Verisign.

зон, чтобы во время атаки можно было продолжать нормальную деятельность, по крайней мере в части DNS. ICANN обеспечивает простоту получения любой организацией копии корневой зоны, которая после небольшой дополнительной работы может стать экземпляром корневого сервера в структуре корневых серверов ICANN. Кроме того, организациям было бы полезно быть внутренне самодостаточными в плане DNS и устранять угрозу отсутствия доступа к внешним серверам или ущерба от случайных или намеренных действий регистратуры, регистратора, оператора корневого сервера и т. д.

DNSSEC обеспечивает способ распространения зоны, подлинность которой можно проверить при помощи встроенных цифровых подписей. Комиссия считает, что этот принцип можно расширить, защитив, например, данные о делегировании и связующие записи. Возможно, также удастся исключить или сократить данные об организации, управляющей корневым сервером, и адресные данные. Одна из подобных схем подробно описана в предложении Пола Викси и включена в раздел «Замечания» настоящего отчета.

Есть также и важные политические аспекты. Существует 13 структур корневых серверов, но некоторые страны чувствуют себя обделенными, несмотря на возможность иметь в своей стране столько экземпляров корневого сервера ICANN, сколько они пожелают установить. (Не говоря уже о том, что несколько других организаций, управляющих корневыми серверами, желают расширить свои группы с адресацией любому устройству.) Предлагаем просто устранить эту проблему.

Следует отметить, что нет технической необходимости заменять существующую систему корневых серверов тем лицам, которые ее предпочитают; предлагаем просто упростить метод репликации в корневой зоне и подать пример для остальных зон.

4.3.Совместное управление зоной

В предыдущем разделе мы обсудили политические настроения, которые стимулируют стремление стран создавать собственную структуру корневых серверов. Эти опасения могут быть обоснованными или необоснованными, однако нет сомнения в том, что текущая деятельность корневой зоны базируется в США и подпадает под юрисдикцию США.

Приведем общую схему последовательности действий при обновлении корневой зоны:

- ICANN получает от доменов верхнего уровня запросы на обновление и проверяет их на предмет наличия ошибок
- ICANN сообщает об изменениях министерству торговли
- ICANN отправляет утвержденные изменения компании Verisign
- Verisign создает подписанную корневую зону и распространяет ее

Есть ли техническая возможность разделения контроля над корневой зоной? В этом направлении были предложены некоторые теории. Одним из направлений научной мысли является

использование нескольких (N) подписей для данных. В таком случае для проверки подлинности данных потребуется M/N подписей. Конечно, ведутся споры относительно значений M и N и необходимости/желательности различных систем шифрования.

В настоящем документе мы не намерены высказываться в пользу той или иной конкретной системы, но действительно считаем, что качественная разработка может положить начало политическому процессу принятия решения о способах совместного управления конкретной зоны. Наше видение — создание набора инструментов совместного управления зонами, не только для корневой зоны, но и для решения других проблем координации зон. Мы обращаем внимание на то, что у рабочей группы по вопросам эксплуатации DNS (DNSOPS) в IETF есть два предложения относительно координации информации о подписании DNSSEC, однако хотели бы понять не лучше ли создать общее средство, а не решения этой одной точечной проблемы. Координация прямых и обратных адресов может быть еще одной областью применения этих решений.

Итак, что необходимо? Мы предполагаем, что правильная модель -- это такая модель, в которой все стороны, осуществляющие совместное управление, имеют ряд возможностей:

- Систему инициализации общей зоны, состоящей из самой зоны, правил и индивидуальных журналов регистрации каждым участником своих запросов и действий
- Выполнения автоматических технических проверок необходимых для конкретных зон
- Обеспечение видимости запросов любого типа всем остальным участникам, которые могут его утвердить или отклонить; кроме того, должен быть возможен тайм-аут запроса
- Правила, определяющие, что происходит с запросом
    - Один из типов правил — голосование, определяющее условия успешного выполнения запроса. Сюда может войти определение длительности задержки для предоставления всем сторонам времени обсудить запрос.
        - Для национальных доменов верхнего уровня, правилами ВВУИО предписано использование принципа 1 из N, предоставляя каждому национальному домену верхнего уровня (ccTLD) возможность менять собственные данные в одностороннем порядке.
        - Другие домены могут использовать метод простого большинства голосов
    - Указанные задержки могут быть важны для того, чтобы другие могли указать на операционные проблемы и дать возможность автору запроса пересмотреть свои запросы
    - Для разных операций могут применяться разные условия, например, для создания новых элементов, редактирования старых и т. д.

Затем каждый из участников может соблюдать стандартный алгоритм для обеспечения единообразия. Это решение может показаться утопическим, но излишне сложные алгоритмы, такие как Bitcoin и Namecoin [Andreesen 2014] демонстрируют, что подобные системы сегодня являются реальностью.

(Обратите внимание на то, что Комиссия предлагает не правила, а просто распределенную систему для реализации любых правил, которые захочет ввести сообщество.)

4.4.Деятельность регистратур/регистраторов

Некоторые члены комиссии утверждали, что ICANN в процессе своей деятельности должна давать гарантии относительно уровня обслуживания, но комиссия посчитала, что не сможет продвинуться в решении этой проблемы.

4.5.Какие данные должна публиковать ICANN?

4.5.1. Параметры ICANN

У корпорации ICANN есть много совокупностей параметров, которыми она управляет в процессе выполнения функций Агентства по распределению номеров интернета (IANA), реализации процессов ввода новых доменов верхнего уровня и другой деятельности, например резервирования меток на нескольких языках. Все они должны быть доступны в интернете, возможно, в DNS, и, безусловно, в защищенном виде, чтобы все члены сообщества интернета могли ими пользоваться напрямую. В других решениях предлагается использовать DNS в качестве реестра блоков адресов, автономных систем и т.д.

4.5.2. Дата рождения, деятельность и области использования домена

Репутация DNS является ценным инструментом обеспечения безопасности. На настоящий момент дата создания домена является единственным индикатором информации о репутации домена. Другая составляющая — частота обновления серверов имен и адресов домена. Иногда важно знать который регистратор создал и управляет доменным именем. Подозрения вызывают новые домены, частые уточнения и некоторые регистраторы. Желательно предоставлять эту информацию в режиме реального времени.

Информация об областях использования обсуждалась аналогичным образом, но была принята на рассмотрение в ходе следующей конференции IETF в Лондоне, которая пройдет в марте 2014 г.

4.5.3. Пример LISP

На раннем этапе работы комиссии ей было предложено рассмотреть целесообразность поддержки корпорацией ICANN надкорневой службы для протокола разделения указателей/идентификаторов (LISP) [RFC 6830]. Как разъяснил нам Дино Фариначчи (Dino Farinacci) и его коллеги, ICANN хотела бы ввести в эксплуатацию серверы LISP в качестве экспериментальной службы, чтобы направлять на них запросы к существующим серверам LISP, не обеспечивающим в настоящее время универсальных возможностей подключения. ICANN нашла

ресурсы для четырех серверов, однако проект так и не начался из-за нескольких нерешенных проблем:

- Каковы будут масштабы (продолжительность и т. д.) эксперимента? Каковы критерии успеха?
- Какое программное обеспечение будет использоваться, и кто будет обеспечивать его поддержку? Были доступны два специализированных варианта.
- Кто будет определять политику и контролировать эксплуатацию?
- Кто должен этим заниматься: ICANN или региональные интернет-регистратуры (RIR)?
- Изменится ли ответ, если не охватывать IP-адреса?

Никакие действия в рамках этого эксперимента не предпринимались.

По мнению некоторых членов комиссии «LISP — всего лишь единичный пример более общего класса технологий туннелирования транспортного уровня, и являясь таковым, не ставит никаких принципиально новых задач управления идентификаторами, выходящих за рамки текущей эксплуатационной практики управления. Поэтому утверждение о том, что эта форма туннелирования требует особого внимания и поддержки со стороны ICANN четких обоснований под собой не имеет».

Корпорации ICANN следует ожидать, что политические и технические вопросы, касающиеся новых идентификаторов, возникнут снова, и планировать деятельность соответствующим образом.

4.6. Совпадения

Многие члены комиссии были знакомы с проблемой совпадения имен в DNS и хотя эта проблема широко обсуждалась, никакие новые содержательные направления не возникли. Комиссия решила, что существует настоятельная потребность в создании физического прототипа системы, описанного в документе [ICANN 2013].

5. Основы протокола DNS

Можно ли представить себе фундаментальный пересмотр, модернизацию или возрождение DNS? Многие, включая некоторых членов комиссии, считают, что установленная базовая система слишком невосприимчива к изменениям или что процесс нарушен[2] или что целесообразно начать все заново.

[2] Здесь мнения разделились. Некоторые утверждают, что в некоторых конкретных рабочих группах (особенно в прошлом) процесс IETF просто «сломан". Другие считают, что необходимо использовать интерфейс программирования приложений (API), а IETF их не использует, но кто их вообще использует? Третьи читают, что разнообразие рабочих групп по DNS повышает темп изменений и новаторства лучше, чем наличие общего видения.

Удивительно, но комиссия оказалась единодушна во мнении, что усилия по описанию проблем и поиск решений оправданы; возможно, так произошло просто потому что в этом вопросе было необходимо поставить точку. В настоящем разделе мы описываем некоторые проблемы, которые необходимо изучить в случае развертывания более расширенных усилий в данном направлении.

В истории инновационного развития DNS есть свои успехи и неудачи. Одним из основных уроков является то, что технология получает широкое признание только в том случае, если приносит конкретную пользу. Администраторы заботятся о сохранении подключения своих зон к глобальной DNS и об актуальности своих записей A и MX, так как в противном случае они не будут получать электронную почту или веб-трафик. Однако из приблизительно 60 типов записей, которые имеют определения, широко используется менее 10.

Работа по созданию приложений на основании DNS столкнулась с такими же трудностями.

В первой группе стандартов RFC для DNS предлагался метод маршрутизации почты в конкретные почтовые ящики, но он нигде не был реализован. Вторая схема, ресурсная запись MX, решала проблему создания резервных почтовых серверов и маршрутизации почты через границы организации — и сегодня она является основой почтовой маршрутизации. Базы данных для борьбы со спамом были широко внедрены без стандартизации. Конкуренция при разработке стандартов проверки подлинности почты привела созданию двух способов реализации, использующих ресурсную запись TXT, и к спорам относительно целесообразности стандартизации новых типов в принципе.

Работа по преобразованию телефонных номеров E.164 (ENUM) для стандартизации маршрутизации телефонных и других медийных данных при помощи DNS также имела крайне ограниченный успех. Хотя технология использования указателя на авторитетный узел именования (NAPTR) считается по-настоящему новаторским подходом, разработчики ENUM проигнорировали необходимость маршрутизации информации, не являющейся телефонным номером вызываемого абонента, и производители оборудования предпочли хранить это значение в системах собственной разработки.

5.1.Общие принципы

Любое новое проектное решение должно:

- Устранять ограничения размера — максимальный размер передаваемого блока (MTU) 576 байт, вероятно, сделал больше для сдерживания развития DNS, чем любой другой отдельно взятый фактор; DNSSEC не вписывается в это ограничение, и несмотря на существование механизма расширения для DNS (EDNS0), большое количество аппаратного и программного обеспечения не передает большие пакеты.
- Сохранять возможности подключения ко всем существующим именам и данным DNS

- Стараться способствовать согласованным решениям — если разработчики не будут следовать спецификациям, пользователь оказывается зажат в рамки существующей общей области перекрытия
- Допускать возможность будущего расширения
- Создавать стимулы для внедрения

5.2.Модель данных

В первых стандартах RFC для DNS предусматривались параллельные пространства имен для различных «классов» информации и создание новых типов данных из простых компонентов. Понятие классов никогда не прорабатывалось. Были определены новые типы данных , но впоследствии многие стали выступать за использование для переноса данных общей записи TXT, предназначенной для произвольных текстовых строк, вместе с другим уровнем меток в качестве заменителя этого типа регистрационных записей.

Комиссия считает, что либо DNS следует определить свои собственные типы и форматы регистрационных записей в метаданных в DNS, либо DNS должна признавать дочерние метки последним типом данных и расширить запросы для обеспечения более гибкого сопоставления.

И наконец, нам необходимо изучить самоподписанные объекты данных, которые могут существовать независимо от доменного имени.

5.3. Распределение

Зональная структура данных и кеширование по записи ресурса реализовано при помощи отчасти неравномерных «улучшений» стандарта времени существования (TTL) и упреждающей выборки информации с истекающим сроком. Возможно, имеет смысл обсудить новые способы группировки данных с порядковыми номерами, которые позволяли бы обновлять группы кешированных данных без фактической передачи данных.

Комиссия также считает, что можно улучшить безопасность за счет более частой репликации зон (возможно, меньшего размера) при помощи существующих механизмов перевода зоны и т.д. Эти данные не обязательно должны защищаться DNSSEC и, следовательно, могут повысить безопасность в тех местах, где система DNSSEC не внедрена.

5.4. Интерфейс программирования приложений (API)

Существует два варианта API DNS: пользовательский интерфейс и имена на уровне API. В обоих случаях был бы полезен стандартный синтаксис, который позволяет задавать в явном виде полностью определенное доменное имя (FQDN). Качество обслуживания сообщества пользователей улучшилось бы при использовании согласованной совокупности правил для всех пользовательских интерфейсов, однако неясно, возможно ли уговорить на это поставщиков.

Интерфейс программирования API несколько раз пытались пересмотреть, в большинстве случаев неудачно. Комиссия недавно выслушала доклад Пола Хоффмана (Paul Hoffman) на тему нового проектного решения, особенностями которого являются асинхронные интерфейсы и поддержка

DNSSEC. Работа была впоследствии выпущена на встрече IETF в Лондоне в марте 2014. См. http://vpnc.org/getdns-api/

Однако отдельно от API, существует сопутствующий вопрос: следует ли выполнять проверку подлинности DNSSEC и фильтрацию DNS (в соответствующих случаях). Комиссия пришла к единогласному мнению, что технически следует разрешить использование в качестве оконечного элемента DNSSEC оконечную систему (которой может быть виртуальная машина, ноутбук, сервер в среде пользователя и т. д., в зависимости от предпочтений пользователя), несмотря на тот факт, что это может оказаться невозможным из-за маршрутизатора, брандмауэра или других исторически существующих ограничений. Аналогичным образом, хотя фильтрацию DNS используют не все, она должна находиться под контролем пользователя.

Ничто из сказанного не должно означать, что пользователю запрещено поручить выполнение этих задач своему интернет-провайдеру или другим специалистам.

Ограничения, возникающие в связи с существующими правилами и законами могут потребовать иного.

5.5. Протокол запросов

Протоколу запросов DNS присущи два типа проблем: проблемы, связанные с транспортировкой запросов/ответов от отправителя к серверу, и проблемы, связанные с увеличением возможностей запроса.

Исконные проблемы транспортировки UDP начинаются с традиционного ограничения размера MTU 576 байтами. Первоначальным решением был возврат к TCP для передачи данных большего объема. Размер данных корневой зоны стал, вероятно, первым местом, где ограничения MTU имели очень широкие последствия и привели к ограничению в 13 корневых серверов; впоследствии добавление подписей DNSSEC существенно расширило размер ответных пакетов. Механизм EDNS0 был разработан для того, чтобы решить эту проблему, наряду с другими, что в некоторой степени и произошло. Однако есть и другие ограничения, такие как размер кадра Ethernet или для IPv6 — 1280 и т. д., которые принципиально ограничивают UDP.

Кроме того, EDNS0 не может решить проблему точек доступа, маршрутизаторов, брандмауэров и другого оборудования, которые блокируют доступ к порту 53 по протоколу TCP или ограничивают размер пакетов или даже перехватывают запросы DNS в прозрачных прокси, часто в ущерб обслуживанию. Аналогичные проблемы могут существовать в кеширующих серверах имен, которые не поддерживают большие пакеты, все типы данных DNS, EDNS0 и т. д. Некоторые проблемы могут быть достаточно малозаметными. Можно привести один пример: прохождение пакетов DNSSEC осуществляется без проблем, но не во время смены ключей DNSSEC, то есть стандартной процедуры обслуживания, во время которой пакеты становятся немного больше.

Сопутствующей проблемой являются DDOS-атаки на DNS, особенно с использованием отражения и усиления. В этих случаях желательно иметь какой-то способ идентификации настоящего трафика, чтобы фильтровать трафик, используемый для атаки. Проверка адреса источника [BCP

38] позволила бы в значительной степени разрешить данную проблему, как для DNS, так и для многих других протоколов. Комиссия поддерживает эти меры[3], но они не получили широкого распространения. Формирование скорости передачи и различные эвристические алгоритмы способны помочь, но они вряд ли являются оптимальным решением. Возможными средствами были и остаются разнообразные легкие механизмы проверки подлинности.

Один из подходов к решению проблемы транспорта является перенос всего трафика DNS в https:. Логика здесь заключается в том, что у всех есть кровная заинтересованность в использовании защищенного потока веб-трафика, и значит это надежный путь (а по мнению некоторых — ЕДИНСТВЕННЫЙ надежный путь). Платой является состояние подключения и сопутствующие накладные расходы. К альтернативам относится некий новый транзакционный протокол или способ использования UDP, но существует вероятность того, что оба решения окажутся неспособны функционировать в некоторых частях установленной базовой системы. В любом случае существует проблема того, какой формат использовать в транзакциях DNS: традиционный или новый.

Независимо от транспорта, протокол запросов DNS следует расширить для повышения гибкости запросов. Сюда можно отнести некоторую схему контроля доступа к последующим меткам вместо NSEC и NSEC3.

Протоколы, разработанные в научно-исследовательской среде, такие как CCN, учитывают недостатки DNS и содержат все эти функциональные возможности. В отношении этих новых протоколов сложность состоит в большей степени в наличии стимулов и путей модернизации существующей инфраструктуры с сохранением обратной совместимости, вместо создания совершенно новых разработок в науке о протоколах.

6. Выводы и рекомендации

- Использование DNS в рамках инфраструктуры будет продолжать расти; использование DNS в пользовательском интерфейсе испытывает конкуренцию со стороны альтернатив, основанных на принципах поиска, мобильных интерфейсов и т.д.
- ICANN следует опубликовать дополнительные данные, подписанные ключом DNSSEC для зарезервированных меток и т.д.
- Совместно с Инженерной проектной группой интернета (IETF), среди прочих, следует провести исследование для создания определения архитектурного видения DNS в 2020 году.
- Разработать и создать прототип публикации открытой корневой зоны.

[3] Вариант [BCP 38] поддерживают все члены комиссии, при чем некоторые считают, что его поддержка должна войти в ряд основных рекомендаций комиссии. При этом большинство отмечает, что со времени публикации BCP в 2000-м году, вариант этот применяется очень мало.

- Разработать систему совместного управления зонами для корневой зоны.
- Провести упражнения по совпадению имен для проверки легкости реализации [ICANN 2013].

7. Ссылки

[Andreesen 2014] Andreesen, “Why Bitcoin Matters”, http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters

[BCP 38] Ferguson el al, “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing”, RFC 2827, май 2000

[DNS/TCP] https://lists.dns-oarc.net/mailman/listinfo/tcp-testing

[Fayazbakhsh 2013] Fayazbakhsh et al, “Less Pain, Most of the Gain: Incrementally Deployable ICN”, Sigcomm 2013

[Ghodsi 2011] Ghodsi et al, “Naming in Content-Oriented Architecture”, Sigcomm 2011

[Huston 2013] DNS-over-TCP-only study.

http://www.circleid.com/posts/20130820_a_question_of_dns_protocols/ и последующая ветка обсуждения функционирования DNS

[ICANN 2013] “Guide to Name Collision Identification and Mitigation for IT Professionals”, https://www.icann.org/en/about/staff/security/ssr/name-collision-mitigation-05dec13-en.pdf

[Kaminsky 2004] D. Kaminsky, “Tunneling Audio, Video, and SSH over DNS”, BlackHat 2004

[Merit] Разделы о доменах и DNS

http://www.afnic.fr/en/about-afnic/news/general-news/6391/show/the-internet-in-10-years-professionals-answer-the-afnic-survey.html

[Mockapetris 88] P. Mockapetris and K. Dunlap, “Development of the Domain Name System”, SIGCOMM 88

[Newyorker 2013]

http://www.newyorker.com/online/blogs/elements/2013/12/the-mission-to-decentralize-the-internet.html?goback=%2Egde_1430_member_5817512945197801473#%21

[RFC 881] J. Postel, “The Domain Names Plan and Schedule”, ноябрь 1983 года

[RFC 882] P. Mockapetris, “Domain Names – Concepts and Facilities”, ноябрь 1983 года

[RFC 883] P. Mockapetris, “Domain Names – Implementation and Specification”, ноябрь 1983 года

[RFC 1034] P. Mockapetris, “Domain Names – Concepts and Facilities”, ноябрь 1987 года

[RFC 1035] P. Mockapetris, “Domain Names – Implementation and Specification”, ноябрь 1987 года

[Spiegel 2014] http://www.spiegel.de/international/world/nsa-secret-toolbox-ant-unit-offers-spy-gadgets-for-every-need-a-941006.html

8. Глоссарий

A	Вид записи DNS, использующийся для адресов IPv4
AAAA	Вид записи DNS, использующийся для адресов IPv6. Также известен под названием «quad A»
AI	Искусственный интеллект
API	Интерфейс программирования приложений
BCP	Передовые методы – выборка RFC
CCN	Сеть, ориентированная на контент
ccTLD	Национальный домен верхнего уровня – домен верхнего уровня, присвоенный конкретной стране. Иногда управляется сторонней организацией.
DANE	Аутентификация именованных объектов на базе DNS
DDOS	Распределенная атака типа «отказ в обслуживании»
DNS	Система доменных имен — система присвоения имен в интернете
DNSOPS	Рабочая группа IETF, занимающаяся в том числе вопросами эксплуатации DNS
DNSSEC	Расширения безопасности системы доменных имен
DSL	Цифровая абонентская линия связи
E.164	Рекомендация сектора стандартизации электросвязи МСЭ (ITU-T) под названием «Международный телекоммуникационный план нумерации для сетей общего пользования», которая определяет план нумерации для мировой коммутируемой телефонной сети общего пользования (PSTN) и некоторых других сетей передачи данных
EDNS0	Механизм расширения DNS [RFC 2671] — стандарт расширения размера и полей в первоначальной спецификации DNS
ENUM	Рекомендация по преобразованию телефонных номеров E.164 — принципы объединения международной системы нумерации телефонов в коммутируемой телефонной сети общего пользования с пространством адресов и идентификационных имен интернета, например для маршрутизации телефонного вызова

FEDEX Курьерская служба «Федерал-Экспресс»

FQDN Полностью определенное доменное имя

FTP Протокол передачи файлов

gTLD Домен общего пользования – домен верхнего уровня, который не соответствует никакому страновому соду

HTTPS Протокол защищенной передачи гипертекста

IANA Администрация адресного пространства Интернет (IANA)

ICANN Интернет-корпорация по присвоению имен и номеров

ICN Сеть, ориентированная на информацию

IEEE Институт инженеров по электротехнике и электронике

IETF Инженерная проектная группа Интернета

IOT Интернет вещей

IP Интернет-протокол

IPSEC Безопасность интернет-протокола

IPv4 Версия 4 интернет-протокола

IPv6 Версия 6 интернет-протокола

ITI Комиссия ICANN по стратегии инновационного развития технологий идентификации

LISP Протокол разделения указателей/идентификаторов [RFC 6830]

MIB База управляющей информации

MTU Максимальный размер передаваемого блока — размер максимального блока данных, который можно передать в принципе или передать без фрагментации

MX Обмен почтой — тип данных DNS, который определяет адрес почтового шлюза, осуществляющего обработку электронной почты для конкретного домена

NAPTR Указатель на авторитетный узел именования — тип данных DNS, который наиболее широко используется в интернет-телефонии

NDN Сеть с именованными данными

P2P Одноранговая сеть

PKI Инфраструктура открытых ключей

RFC Запрос комментариев — пояснительные записки, в которых задокументированы технические и эксплуатационные стандарты Интернета

RIR Региональная интернет-регистратура – одна из организаций, управляющих присвоением и регистрацией номерных ресурсов интернета в пределах одной конкретной части мира. Например, ARIN, Американский регистратор интернет-номеров, работает с Канадой, США и многими Карибскими и Североатлантическими островами.

Rsynch Протокол дистанционной синхронизации — обеспечивает синхронизацию файлов и каталогов с минимизацией передачи данных благодаря использованию инкрементного кодирования.

RR Ресурсная запись — неделимая единица информации в DNS

TSIG Транзакционная подпись

TTL Время существования

TXT Ресурсная запись текстового типа в DNS, которая позволяет использовать текстовые поля произвольного формата

UDP Протокол пользовательских дейтаграмм — протокол интернета для передачи дейтаграмм без организации соединения

UI Пользовательский интерфейс

URI Унифицированный идентификатор ресурса

URL Унифицированный адрес ресурса

WIFI «Wireless Fidelity» — стандарт беспроводной сети, входящий в семейство стандартов IEEE 802.11

9. Замечания членов комиссии

Обратите внимание на то, что все замечания приведены дословно, в том виде, в каком они были направлены автором.

9.1. Замечания Джеймса Сенга

Техническая архитектура

Я в душе хакер и поэтому люблю децентрализованную архитектуру. Можно утверждать, что причиной большей части наших сегодняшних «политических проблем» является централизованный характер DNS, имеющей корневую зону.

Поэтому мне нравятся такие технологии, как Namecoins или другие системы децентрализованных идентификаторов.

При этом мне неизвестно о существовании децентрализованной и одновременно скоординированной системы идентификаторов, которая бы реально широко использовалась. Поэтому, хочешь не хочешь, система DNS продолжает оставаться одной из наиболее распространенных систем идентификаторов. В IETF мы выбираем в качестве победителей «работающие коды», которые не всегда спроектированы наилучшим образом.

Я не верю в многокорневую систему или в альтернативную корневую зону. Как я говорил в Буэнос-Айресе, я поддерживаю RFC 2826. Многокорневая система, альтернативная корневая зона и все соответствующие предложения только переводят принципиальную политическую проблему на другой уровень, не решая ее. Прошу обратить внимание на то, что я назвал это политической проблемой, поскольку вообще не считаю, что наличие нескольких корневых зон решает какие-либо технические проблемы; можно даже сказать, что они только повышают техническую сложность.

ICANN

Существование системы DNS и ее централизованной корневой зоны частично привело к тому, что выполнение изначально простой функции IANA сегодня осуществляется огромной организацией под названием ICANN.

Я начал работать в ICANN на ее первой конференции в 1999 году и присутствовал почти на всех последующих конференциях. В течение этих лет возникали ситуации, когда мне хотелось, чтобы ICANN поступила по-другому, то есть наши мнения не всегда совпадали.

Однако ICANN — «работающий код» координации идентификаторов DNS. Возможно, есть и другие, лучшие проекты, может быть более простые и элегантные (например, многие в сообществе IETF хотели бы вернуться в прошлое, во времена Джона Постела), но ситуация такова, какова она есть сейчас, и самое важное, что она действительно работает, хотя и она могла бы работать лучше. Предлагаемой альтернативе (МСЭ) присущи другие известные нам и более серьезные проблемы.

Поэтому я поддерживаю ICANN, лучшей функционирующей системы для координации идентификаторов DNS и корневой зоны у нас нет.

Расширение DNS и ее систем в другие области

Отсюда вытекает, что я мало заинтересован в переработке DNS или в использовании альтернативных предложений по используемым для имен идентификаторам. В конечном итоге, кто-то, какая-то организация должна существовать, чтобы заниматься координацией, и мы везде столкнемся с теми же самыми политическими проблемами.

Я поддерживаю имеющуюся у нас экосистему DNS (стандарты DNS, функционирование корневой зоны, ICANN, ...), которая мне нравится. Первоначально она предназначалась только для DNS, но развилась и расширилась в другие области (например, RFID), охватывая более значительную часть сообщества. Проделанная нами работа в сфере IDN-доменов в определенном смысле включает группы пользователей сообщества, которые нуждаются в использовании своего родного языка, в экосистему DNS вместо того, чтобы допустить создание ими собственных систем.

Хотя некоторые спорят со мной, доказывая, что если бы мы создали IDN-домены за рамками экосистемы DNS, развертывание могло бы осуществляться намного быстрее (см., например, «Ключевые слова родного языка»), я утверждаю, что IDN-домены лучше также и потому, что являются частью экосистемы DNS, где уже существуют хорошо сформулированные открытые стандарты, открытая реализация, компании, которые выстраивают свою деятельность на основании легитимности DNS, и аналогичные средства защиты владельцев доменов и конечных пользователей IDN-доменов.

Поэтому я без всяких сомнений поддерживаю вариант изучения возможностей расширения DNS в область идентификаторов, для которых эта система изначально не предназначалась. Инженеры, разрабатывающие идентификаторы, часто проявляют наивность в отношении политических аспектов, связанных с идентификаторами, особенно если эти идентификаторы предназначены для конечных пользователей. Они могли бы извлечь уроки из истории идентификаторов DNS и ICANN.

Политические аспекты корневой зоны

Политика ICANN и количество людей, считающих ICANN частью системы «управления интернетом», связана с ролью этой корпорации в плане координации работы корневых серверов.

Ситуацию максимально ухудшает тот факт, что по исторической случайности 11 из 13 корневых серверов расположены в США, однако это все равно усугубляет ощущение, что ICANN находится под контролем США, особенно в наши дни, после разоблачений Сноудена.

Когда появляется кто-то и говорит о необходимости наличия корневого сервера в той или иной стране, мы отклоняем это предложение, приводя исторические или технические доводы о невозможности создания более 13 корневых зон.

Я могу принять как довод исторические факты.

Технические причины — нет. Это в большей степени отговорка, поскольку мне неизвестно о какой-либо серьезной работе IETF по поиску путей выхода за рамки 13 корневых зон. Именно поэтому на конференции в Буэнос-Айресе я говорил о том, что могу придумать пару технических решений, подходящих по крайней мере в качестве первоначального проекта. Мы не можем позволить ICANN продолжать использовать IETF / технические доводы для оправдания своего отказа от решения возникающих перед корпорацией политических проблем. Мы должны иметь возможность сказать ICANN: да, это можно сделать, но политическое решение относительно того, делать это или нет, должны принять вы.

Вдобавок, что еще более важно, управлять корневыми серверами не настолько приятно, как это расхваливают.

Наличие корневой зоны не означает наличие прямого контроля над интернетом. На самом деле, это такое же скучное занятие, как и эксплуатация корневого сервера с адресацией любому устройству. При этом, если оператор корневой зоны не следует передовым методам эксплуатации корневой зоны (например, стандартам RFC 2010 и RFC 2870), он может причинить большой ущерб интернету.

Большинство технических специалистов вероятно поняли о чем я говорил выше, но большинство других участников в жизни ICANN — нет.

То есть при выборе оператора корневой зоны следует учитывать ряд соображений, потому это то, что определяет стабильность идентификаторов интернета, которая в большой мере основана на Доверии. Однако как бы то ни было, Доверие — не инженерная проблема.

- Джеймс Сенг

http://chineseseoshifu.com/blog/dnspod-in-china.html

Почему DNSPod приносит пользу в Китае, несмотря на то, что он «сломал» DNS.

9.2.Поведение приложений в отношении разрешения имен в DNS и списка поиска — Джефф Хьюстон

отсутствует — НЕ выполняет поиск в DNS

никогда — выполняет поиск базового имени, но не применяет список поиска

до — применяет список поиска и при возвращении результата NXDOMAIN выполняет поиск базового имени

после — выполняет поиск базового имени, и при возвращении результата NXDOMAIN затем применяет список поиска

всегда — НЕ выполняет поиск базового имени, применяет только список поиска

Поведение библиотеки DNS-преобразователя в основных операционных системах

Система	**Абсолютный** *сервер.*	**Относительный с одной меткой** *сервер*	**Относительный с несколькими метками** *www.сервер*
MAC OSX 10.9	никогда	всегда	никогда
Windows XP	никогда	всегда	после
Windows Vista	никогда	всегда	никогда
Windows 7	никогда	всегда	никогда
Windows 8	никогда	всегда	никогда
FreeBSD 9.1	никогда	до	после
Ubuntu 13.04	никогда	до	после

Поведение браузеров на платформах MAC и Windows

MAC OSX 10.9

	сервер.	*сервер*	*www.сервер*

Chrome (31.0.1650.39 beta-версия)	никогда	всегда	до
Opera (12.16)	никогда	всегда	никогда
Firefox (25.0)	после*	всегда	после*
Safari (7.0 9537.71)	отсутствует**	отсутствует**	отсутствует**

* Добавляется префикс «www.», затем предпринимается попытка использования префикса «www.» с добавлением списка поиска

** По-видимому, Safari распознает домен верхнего уровня и не выполняет поиск в DNS, когда имя не является доменом верхнего уровня

Windows 8.1

	сервер.	*сервер*	*www.сервер*
Explorer (11.0.900.16384)	отсутствует	отсутствует	никогда
Firefox (25.0)	никогда*	всегда	никогда
Opera (17.0)	отсутствует	отсутствует	отсутствует**
Safari (5.1.7 7534.57.2)	никогда*	всегда***	никогда

* Добавляется префикс «www»

** OPERA знает о делегированных доменах верхнего уровня и посылает запросы только тогда, когда последней меткой является домен верхнего уровня

*** Добавляется префикс «www» и суффикс «.com»

9.3. Наблюдения относительно согласованности и тенденций — Джефф Хьюстон

Если вернуться к истокам системы доменных имен, то можно обнаружить так называемый «файл HOSTS» как раннюю попытку внедрить имена, удобные для человека, в среду компьютерных сетей. В сети ARPANET использовалась такая модель именования сетевых узлов, в которой каждый подключенный узел имел локальный файл конфигурации, файл HOSTS, содержащий имена всех остальных узлов ARPANET и адреса каждого узла согласно протоколу. Среди всех этих многочисленных экземпляров файла HOSTS во всем множестве подключенных к ARPANET узлов не было принудительно обеспечиваемого единообразия , как не было в то время никакого метода распространения копии файла HOSTS по всей сети. Практическая ценность этого файла HOSTS заключалась в возможности использования понятных человеку имен вместо более непонятных адресов уровня протокола. Пользователи могли определять сетевые узлы по их условному имени, которое затем преобразовывалось в двоичные адреса конкретного протокола через операции поиска в файле hosts. По мере роста ARPANET, рос размер и частота обновления файла HOSTS, а также росли накладные расходы на поддержание точности локальных файлов HOSTS. Формат файлов HOSTS был стандартизован (RFC952), была определена центральная служба файлов HOSTS (RFC953), которая могла заменить множество локальных копий файла HOSTS.

Затем на замену этой системе пришла система доменных имен (DNS), технические требования к которой первоначально были определены в 1983 году в стандартах RFC 882 и RFC 883. Механизм преобразования имени, выраженного понятной для человека строкой, в служебный адрес конкретного протокола сохранялся при переходе от файла HOSTS к DNS.

Это пространство идентификаторов обладало рядом свойств, включая то, что система DNS охватила пространство имен, удобных для использования в человеческой речи, и одновременно сделала возможным создание достаточно формальной структуры, позволяющей компьютерным приложениям манипулировать доменными именами детерминированным образом. Пространство имен DNS имеет иерархическую структуру, которая позволяет эффективно осуществлять поиск точных совпадений, одновременно обеспечивая возможность распределенного управления пространством имен. Если избегать совпадения меток в рамках отдельно взятой зоны иерархии имен DNS, то можно избежать совпадения имен в рамках всего пространства имен DNS, что позволяет легко управлять уникальностью имен а контексте DNS. Система DNS является гибкой в плане своей функции сопоставления и может использоваться для создания соответствий между структурированным пространством имен и любой другой формой именованных ресурсов нашей точки обслуживания. DNS создавалась как согласованная система в том отношении, что при введении записи одного и того же имени в DNS, запросы на разрешение этого имени возвращают одинаковые ответы при отправке запросов из любого места и в любое время. Это позволяет обеспечить ссылочную согласованность в том смысле, что имя DNS можно передавать от одного лица к другому, и при этом оно будет ссылаться на одно и то же местонахождение ресурса или службы. DNS не предназначена для замены системы каталогов или системы поиска. Если в DNS существует полное совпадение с указанным в запросе именем, то в ответ на такой запрос будет возвращено сопоставленное этому имени значение, а в противном случае будет возвращено сообщение о том, что совпадение не найдено.

Эта модель пространства имен DNS как пространство идентификационных имен, используемое для поддержки взаимодействия человека с сетью, претерпела ряд изменений, главным образом под влиянием способов использования идентификаторов человеком в процессе общения. У нас тенденция использовать идентификаторы менее точным образом, при чем это происходит методами, в рамках которых включаются элементы, отражающие местные условия — местные языки и наборы символов — и поэтому с течением времени роль DNS как способа взаимодействия человека с сетевыми ресурсами и службами стала составной частью более общего направления усилий по поддержке интерфейсов, функционирующих более «естественным» для человека образом.

В стандарте RFC1034 было предложено использовать сокращение в спецификации имен DNS, когда имена, не заканчивающиеся на «.», стали называться «относительными именами», и, как отмечается в стандарте RFC1034, «относительные имена главным образом используются в интерфейсе пользователя, где их интерпретация меняется в зависимости от реализации». Как правило, такая локальная интерпретация подразумевала использование локального списка поиска или суффиксов меток, позволяя пользователю указать начальную часть доменного имени и передать при помощи локального приложения или программы преобразования имен процедуру, по которой добавляется определенный в локальной системе суффикс для формирования полного имени DNS.

Такая форма избирательного заполнения пространства идентификаторов DNS путем использования суффиксов имен получила дополнительное развитие в пользовательском интерфейсе веб-браузеров, где распространенной практикой стало преобразование компонента URL идентификатора DNS путем добавления префиксной строки «www.» и определенного в локальной системе суффикса (как правило «.com»). Таким образом, указанный пользователем идентификатор и идентификационное имя, используемое в последующем запросе DNS, становились связанными, но не обязательно одинаковыми.

Подобное использование локальных операций преобразования имен было расширено далее методом, в рамках которого идентификаторы, сформированные из наборов не латинских символов — не американской ASCII — сопоставлялись в DNS (IDN-домены: RFC5891). В этом документе четко определен процесс преобразования идентификатора, введенного пользователем, в закодированную строку метки, которая формирует запрос DNS. В этом случае алгоритм преобразования имеет точное определение, чтобы многочисленные виды реализации стандарта IDN обеспечивали единообразное сопоставление идентификатора, введенного с использованием конкретного алфавита в форму закодированного имени DNS.

Следующим этапом развития и совершенствования модели взаимодействия с человеком стала унификация критериев поиска и URL при вводе в браузеры. При этом, если при вводе данных в браузер пользователь не использовал полную спецификацию URL, современный браузер пытается сделать это самостоятельно.

9.4.Некоторые проблемы существующих технологий идентификаторов – Рик Буави (Rick Boivie)

1. Отказоустойчивость корневой зоны

Сегодня система DNS в очень большой степени зависит от наличия, пропускной способности и достижимости корневых серверов. Если бы организации, интернет-провайдеры, страны или пользователи обслуживали собственную копию (или копии) корневой зоны и использовали эти копии для разрешения доменных имен вместо того, чтобы всегда обращаться к «реальным» корневым серверам, то организации, интернет-провайдеры, страны или пользователи были бы лучше защищены от атак на корневые зоны и могли бы продолжать функционировать даже при отсоединении от реальных корневых серверов и в случаях отсутствия, перегруженности и нарушения работы реальных корневых серверов.

2. Мошенническое использование IP-адресов

Одним из важнейших инструментов, при помощи которых нарушители не позволяют своим жертвам использовать интернет, являются IP-пакеты с поддельными адресами источника. Отправляя пакеты таким образом, что создается впечатление, что они поступают от объекта атаки и делая это с большого количества компьютеров, атакующий может использовать большое количество «ответного» трафика, который заполнит или переполнит то, что позволяет сети вернуться к объекту атаки.

3. Сопоставление имен с адресом в DNS при помощи метода Fast Flux

Сегодня нарушители зачастую неправильно используют систему DNS способом, который позволяет им избежать попытки законных властей отслеживать и прекращать их незаконную деятельность. Сегодня «бот-мастер» может использовать целый ряд захваченных компьютеров («ботнет») для осуществления разных видов незаконной деятельности, включая отправку спама, проведение DDOS-атак и заражение других компьютеров различными видами вредоносного ПО. Бот-мастера способны быстро переводить свою незаконную деятельность с одного набора захваченных компьютеров на другой посредством быстрого изменения сопоставленных имен и адресов в системе DNS для того, чтобы прятаться от попыток законных властей отследить и остановить их незаконную деятельность.

Мы рекомендуем ICANN в сотрудничестве с другими членами сообщества интернета предпринять следующие действия:

(1) улучшить отказоустойчивость корневой зоны,

(2) решить проблему мошеннического использования IP-адресов

(3) решить проблему, возникающую при сопоставлении имен и адресов при помощи метода fast-flux.

9.5.Универсальная адресация любому устройству для корневой зоны — Пол Викси (Paul Vixie)

Обзор

Мы предлагаем IANA создать несколько дополнительных вариантов корневой зоны DNS, чтобы обеспечить возможность универсальной адресации любому устройству и проведения оперативного анализа. «Универсальная адресация любому устройству» в этом контексте означает корневую зону, в вершине которой список записей NS содержит только два сервера имен, чьи соответствующие «общеизвестные» адреса (определяемые записями A и AAAA) могут размещаться на любом узле. «Оперативный анализ» в этом контексте предусматривает широкомасштабное открытое тестирование службы имен корневой зоны, поддерживающей только протокол IPv6, и широкомасштабное открытое тестирование последствий конфликтов «новых доменов общего пользования». При таком подходе к службе имен корневой зоны она рассматривается как неуправляемая утилита.

История вопроса

Систему универсальной адресации любому устройству для корневой зоны было невозможно развернуть безопасным и надежным образом до наступления эпохи DNSSEC, поскольку в отсутствие DNSSEC любой отвечающий сервер можно было настроить на произвольные данные корня DNS, включая новые домены верхнего уровня или повторно делегированные существующие домены верхнего уровня. Благодаря DNSSEC, у операторов рекурсивных серверов имен появилась возможность настроить функцию подтверждения DNSSEC так, чтобы любая информация о домене общего пользования, поступающая от сервера имен системы с универсальной адресацией любому устройству, в обязательном порядке заверялась IANA, на что указывают подписи DNSSEC, выполненные при помощи ключа для подписания корневой зоны IANA (ZSK).

Как текущая, так и и существовавшая ранее система корневых серверов имен подвергалась критике в частности из-за отсутствия отказоустойчивости к DDOS-атакам; при этом отмечается, что даже в условиях существующего объема широкомасштабной адресации любому устройству, используемой всеми операторами корневых серверов имен, в мире все еще существует несколько сотен серверов имен, которые являются полномочными отправителями ответов для корневой зоны DNS. У нас также вызывает обеспокоенность необходимость наличия доступа к системе корневых серверов имен даже для установления соединений, имеющих исключительно локальный характер, поскольку в ином случае локальные клиенты не имеют никакой возможности обнаружить локальные службы. В распределенных системах мирового масштаба, к которым относится интернет, критически важные службы должны иметь в высшей степени распределенный характер.

Подробные сведения

Следует создать несколько полезных вариантов. Во-первых, базовая система универсальной адресации любому устройству позволит любому оператору сервера имен перехватывать трафик, направляемый в систему корневых серверов имен и отвечать на запросы локально. При этом IANA создаст и подпишет цифровой подписью (при помощи DNSSEC) дополнительный вариант корневой зоны, имеющей в своей вершине другой набор записей NS. Эти записи NS будут обозначать серверы имен с адресами, не присвоенными ни одному конкретному оператору сервера имен корневой зоны (RNSO), а остающимися в ведении IANA для использования всеми без исключения заинтересованными сторонами. IANA обратится в региональную интернет-регистратуру (например, ARIN или APNIC) с просьбой выделить микроскопические инфраструктурные ресурсы, такие как несколько 24-разрядных префиксов в формате IPv4 и несколько 48-разрядных префиксов в формате IPv6, для использования в системе универсальной адресации любому устройству корневой зоны.

Второй вариант существующей корневой зоны предусматривает универсальную адресацию любому устройству, как описано выше, но с указанием только таких серверов имен, которые обеспечивают возможность подключения исключительно по протоколу IPv6 (определяется наличием записей AAAA) и не обеспечивают подключение по протоколу IPv4 (определяется отсутствием записей A). Этот вариант упростит оперативный анализ сети, где используется только IPv6.

Третий вариант существующей корневой зоны предусматривает универсальную адресацию любому устройству, как описано выше, но будет содержать записи о делегировании всех известных новых доменов общего пользования, в том числе тех, которые в ином случае не будут готовы к делегированию (например, .CORP и .HOME). Эти новые домены общего пользования будут делегированы на сервер имен, находящийся под управлением самой IANA в целях измерения показателей работы. Каждому новому домену общего пользования будут присвоены подстановочные записи A и AAAA, адреса которых будут указывать на веб-серверы, находящиеся под управлением самой IANA в целях измерения показателей работы.

Последствия

Учитывая иерархический характер маршрутизации в интернете, адресные блоки для адресации любому устройству анонсироваться на нескольких уровнях. Виртуальная машина (ВМ), запущенная на портативном персональном компьютере, может иметь собственный процесс сервера имен, который осуществляет прослушивание соответствующих общеизвестных адресов, благодаря чему эта ВМ не пропускает ни один запрос к службе имен корневой зоны. Сам ноутбук может также перехватывать исходящий трафик, направленный на эти общеизвестные адреса, чтобы обслуживать другие ВМ или процессы, запущенные на этом компьютере. Беспроводный маршрутизатор, находящийся за этим ноутбуком, может иметь серверы, прослушивающие эти адреса, благодаря чему эта беспроводная локальная сеть не пропускает ни один запрос к службе имен корневой зоны. Интернет-провайдер может использовать серверы, прослушивающие эти общеизвестные адреса, чтобы обслуживать всех без исключения клиентов, не имеющих своих собственных серверов. И наконец, ожидается, что в глобальном интернете будет много

операторов, анонсирующих маршруты к этим хорошо известным адресным блокам, в списке которых не последними будут двенадцать существующих операторов корневых серверов имен.

Положительными последствиями этого могут стать более высокая потенциальная отказоустойчивость и сокращение времени задержки в службе имен корневой зоны. Отрицательными последствиями могут стать уменьшение диагностических возможностей и повышенная уязвимость к «отравлению маршрута» или «перехвату» трафика службы имен корневой зоны. В любом случае жизненно важно, чтобы проверка DNSSEC стала повсеместной, чтобы уменьшить последствия подобного перехвата. Мы хотим, чтобы последствием подобной атаки стало «объект нападения теряет службу корневых имен», а не «объект нападения видит другое пространство имен DNS».

Примеры

В приведенных ниже примерах показана совокупность записей NS для вершины каждого варианта корневой зоны, включая связующую адресную запись. Эти данные следует включить в вариант корневой зоны до подписания DNSSEC, а также опубликовать в виде файла «корневых подсказок». Приведенные данные для iana-servers.net также должны присутствовать в реальной зоне iana-servers.net. Для этих примеров потребуется четыре выделенных микроресурса IPv4 и шесть выделенных микроресурсов IPv6.

Вариант 1: универсальная адресация любому устройству

```
. IN NS anycast-1.iana-servers.net.
. IN NS anycast-2.iana-servers.net.
$ORIGIN iana-servers.net.
anycast-1 IN AAAA 2001:?:1::1
anycast-1 IN A ?.?.1.1
anycast-2 IN AAAA 2001:?:2::2
anycast-2 IN A ?.?.2.2
```

Вариант 2: универсальная адресация любому устройству только по протоколу IPv6

```
. IN NS v6only-1.iana-servers.net.
. IN NS v6only-2.iana-servers.net.
$ORIGIN iana-servers.net.
anycast-1 IN AAAA 2001:?:3::1
anycast-1 IN AAAA 2001:?:4::2
```

Вариант 3: универсальная адресация для изучения случаев совпадений имен доменов общего пользования

```
. IN NS gtldstudy-1.iana-servers.net.
. IN NS gtldstudy-2.iana-servers.net.
$ORIGIN iana-servers.net.
gtldstudy-1 IN AAAA 2001:?:5::1
```

gtldstudy-1 IN A ?.?.5.1