Корпорация Интернета по распределению имен и адресов

Комиссия по инновационному развитию технологий идентификации — проект отчета

21 февраля 2014 г.

Содержание

1. Введение ... 3
2. Стратегия комиссии ... 4
3. Перспективы развития ... 5
4. Эксплуатационные проблемы ... 8
   - 4.1. Защита корневой зоны ... 8
   - 4.2. Репликация ... 9
   - 4.3. Совместное управление зоной ... 11
   - 4.4. Деятельность реестров/регистраторов ... 12
   - 4.5. Какие данные должна публиковать ICANN? ... 12
     - 4.5.1. Параметры ICANN ... 12
     - 4.5.2. Дата рождения, деятельность и области использования домена ... 12
     - 4.5.3. Пример LISP ... 13
   - 4.6. Конфликты ... 13
5. Основы протокола DNS ... 14
   - 5.1. Общие принципы ... 15
   - 5.2. Модель данных ... 15
   - 5.3. Распространение ... 15
   - 5.4. Интерфейс программирования приложений (API) ... 16
   - 5.5. Протокол запросов ... 16
6. Выводы и рекомендации ... 18
7. Ссылки ... 19
8. Глоссарий ... 20
9. Дополнения членов комиссии ... 23
   - 9.1. Дополнение Джеймса Сенга ... 23
   - 9.2. Поведение приложений в отношении разрешения имен в DNS и списка поиска — Геофф Хьюстон ... 26
   - 9.3. Наблюдения относительно согласованности и тенденций — Геофф Хьюстон ... 28
   - 9.4. Дополнение Пола Викси ... 30
10. Приложения ... 33
    - 10.1. Материалы по LISP ... 33
    - 10.2. Материалы Хоффмана по API ... 33

1. Введение

Комиссия по инновационному развитию технологий идентификации (ИРТИ) была создана Корпорацией по распределению имен и номеров в Интернете (ICANN) со следующими целями:

1. Разработка стратегического плана технологического развития системы доменных имен (DNS) и других идентификаторов
2. Разработка рекомендаций по передовым практическим методам и эталонных систем
3. Управление технологиями в сфере оперативной 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 г., 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 Аркко (Jari Arkko) — председатель, Инженерный совет Интернета (IETF)
- Рик Бойви (Rick Boivie) — Научно-исследовательский центр IBM им. Томаса Дж. Уотсона
- Анн-Мари Эклунд-Лёвиндер (Anne-Marie Eklund-Löwinder) — руководитель службы безопасности, Фонд инфраструктуры Интернета
- Геофф Хьюстон (Geoff Huston) — главный научный сотрудник, Азиатско-тихоокеанский сетевой информационный центр
- Джеймс Сенг (James Seng) — генеральный директор, Zodiac Holdings
- Пол Викси (Paul Vixie) — генеральный директор, Farsight Security
- Лися Чжан (Lixia Zhang) — профессор информатики школы им. Постела, Калифорнийский университет в Лос-Анджелесе

Комиссия провела очные совещания в ванкуверском офисе IETF (ноябрь 2013 г.), в буэнос-айресском офисе ICANN (ноябрь 2013 г.), и в лос-анджелесском офисе ICANN (январь 2014 г.). Совещание в Буэнос-Айресе было открытым для общественности, а сводная информация о деятельности комиссии была также представлена на двух вебинарах в январе 2014 г. Дополнением к указанным совещаниям стало обсуждение с использованием электронной почты и других электронных средств. Отчет будет доступен для общественного обсуждения в феврале 2014 г. и окончательно доработан после мартовской конференции IETF в Лондоне.

Председатель хочет поблагодарить членов комиссии за все ценные выводы и идеи, а также ICANN за оказанную комиссии поддержку. Он также благодарит сотрудниц корпорации ICANN Элизу Герих (Elise Gerich) и Элис Янсен (Alice Jansen), которые делились своими мыслями 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 Интернета IPv4
- Адреса Интернета IPv6
- Адреса групповой рассылки
- Номера портов
- Номера протоколов
- Реестр унифицированных идентификаторов ресурсов (URI)
- База управляющей информации (MIB)
- База данных часовых поясов

Однако параллельно этому расширению временные рамки работы комиссии были сжаты с первоначального года 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 оригинальные 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 наиболее естественно отнести к сфере компетенции IETF или иной организации. Некоторые идеи поднимают политические вопросы, которые мы не решили, а только обозначили.

И наконец, учитывая огромное количество деятельности в указанной сфере, комиссия просто сделала выборку. Читатель не должен считать, что нам известно обо всей текущей деятельности, или что не рассмотренные здесь идеи являются менее важными.

3. Перспективы развития

Идентификаторы — тема, которая активно обсуждается в интернет-сообществе. В краткосрочном плане в Интернете появятся новые домены верхнего уровня (ДВУ). Ваша учетная запись Facebook вполне может стать единой учетной записью для входа в системы Интернета, аналогично вашей учетной записи Google. В долгосрочном плане у научного сообщества есть много различных проектов, в том числе сеть, ориентированная на контент (Content Centric Networking, CCN), сеть, ориентированная 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 своим 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 сплав ряда технологий, при котором 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, такими как IP-адреса). Когда мы анализируем перспективы развития идентификаторов, необходимо помнить о различиях между областью идентификаторов и функцией сопоставления, анализируя 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 борьба в большей степени носит дарвиновский характер, нежели основана на элегантности или других положительных качествах.

Действующие факторы расширения

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

- Новые ДВУ будут предпринимать попытки монетизации своих брендов. Хотя техническое сообщество проявляет большой скептицизм, более тысячи новых брендов будут бороться за процветание, и есть вероятность инноваций и некоторых сюрпризов.
- Возникающие 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 из членов комиссии отстаивал идею опубликования данных о «дате рождения» и «деятельности» домена в качестве основной информации, определяющей его репутацию. Другие предлагали использовать DNS в качестве реестра адресных блоков 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 на нескольких языках.

Действующие факторы сжатия

- DNS — давно существующий стандарт, который однако также 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. Реализации часто далеки от совершенства, актуальности или соответствия стандартам. Эти проблемы сдерживают внедрение DNSSEC и делают проблематичным внедрение любых новых видов данных или функций DNS. Это приводит к такой практике проектирования, когда все использование ограничивается адресными и текстовыми (TXT) записями. Такая консервативность присуща не только DNS.
- Существует коммерческий интерес управления («владения») 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 патентованных расширений, которая является 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 (ИИ) в строке браузера приводит к несовместимости продукции разных поставщиков. В качестве примера можно привести эксперимент Геоффа Хьюстона (см. дополнение), который проанализировал результаты

поиска по фразе «Geoff.Huston» в нескольких браузерах и сделал вывод о том, что среди поставщиков практически НЕТ согласованности. Отсутствие согласованности допустимо при браузерном поиске, когда ожидается, что пользователь проверит результаты, однако оно представляет опасность в случае файлов конфигурации систем — это одно из оснований для беспокойства в плане конфликтов.

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 то, 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 стремиться к возрождению или реструктуризации DNS разделились. Эта технология обсуждается в разделе «Основы DNS» настоящего отчета. Есть один политический вопрос: должна ли ICANN предпринять попытку сохранения и расширения системы DNS? Если это так, то как можно добиться согласованной архитектуры с учетом расхождения мнений в постоянной группе ICANN — IETF (где предположительно будет выполняться эта работа) и у остальных участников Интернета?

Долгосрочная перспектива

Одной из тем на долгосрочную перспективу является модель сети с именованными данными. Ее основные идеи: доступ к контенту по имени, повсеместная цифровая проверка подлинности, адаптируемое кеширование и схема потока, в которой запросы контента и ответы на них передаются по одному и тому же пути. Модель для запросов маршрутизации 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 из альтернатив модернизации существующей чистой внутрисхемной коммутации (ICN), аналогично большинству нынешних подходов [Фаязбахш, 2013 г.], 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 [Каминский, 2004 г.] и незаконного туннелирования доступа посредством DNS-запросов, которые выполняются до проверки подлинности в некоторых точках доступа WIFI. (По запросу «DNS tunneling» Google выдает 1 620 000 результатов.)

ICN использует совпадение наиболее длинного префикса и селекторы, что позволяет осуществлять транспортировку медиаданных. Ожидалось, что такие средства будут предусмотрены в разделе запросов первоначальной спецификации протокола DNS, но они так и не были разработаны.

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 переходный период, для завершения которого потребуются годы или десятилетия. Предпринимая любые попытки улучшения архитектуры DNS, следует без колебаний заимствовать элементы NDN.

ICN никоим образом не является единственной моделью для будущего, она всего лишь одна из наиболее проработанных моделей. Мы убеждены, что всегда имеет смысл постараться обобщить основные принципы, а затем изучить структуру. [Годси, 2011 г.] является хорошим примером, в том плане, что связывает воедино три составляющих: имя, физический идентификатор и инфраструктуру открытых ключей (PKI).

В последнее время был сделан акцент на распределении контроля [Newyorker, 2014 г.] и конфиденциальности: наиболее широко известным примером является система Namecoin. Существующая PKI представляет собой ресурс для крупномасштабного надзора и, следовательно, создает проблему для конфиденциальности. Решением может стать комбинация самосертифицирующихся объектов и используемой по согласию инфраструктуры открытых ключей или параллельное существование PKI и одноранговых (P2P) систем.

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 комиссии 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 проблемы безопасности аппаратных средств, которые могли упускаться из виду при проектировании

существующих систем, такие как инфицирование BIOS, шпионские модули на жестких дисках и так далее [Spiegel, 2014 г.].

4.2. Репликация

Система DNS всегда содержала два взаимодополняющих механизма распространения данных: запланированная репликация зон и запросы по требованию. 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, когда 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. Концептуально это распространение, как и распространение любой другой зоны в DNS, может быть выполнено посредством любого механизма: магнитные ленты и доставка курьерской почтой Федерал-Экспресс (FEDEX), пересылка файлов с помощью протокола передачи файлов (FTP) или Rsynch, или, что оптимальнее, путем инкрементной передачи зоны, когда передаются только данные об изменениях по сравнению с предыдущей версией, а не вся зона целиком. Копии могут либо принудительно отправляться посредством уведомлений DNS, либо извлекаться с использованием стратегии опроса, при которой осуществляется поиск изменений. Безопасность передачи зон может обеспечиваться через транзакционную подпись DNS (TSIG) и/или путем использования любого количества транспортных протоколов, например, защищенного интернет-протокола (IPSEC), протокола защищенной передачи гипертекстовой информации (HTTPS) и т. д. Существуют сотни экземпляров корневых серверов, на которых хранятся копии корневой зоны.

Когда пользователи хотят получить доступ к данным в корневой зоне, они отправляют запросы к корневой зоне. Маршрутизация этих запросов осуществляется при помощи двух механизмов: во-первых, по IP-адресу пункта назначения в запросе определяется совокупность корневых серверов, имеющих общий групповой адрес, и, во-вторых, система маршрутизации принимает решение о том, какой сервер в этой группе фактически получит данный запрос. Такая схема является результатом развития системы, вначале 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 только 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 имеются другие проблемы размера, связанные с добавлением адресов IPv6. На пути от корневого сервера к пользователю безопасность может дополнительно обеспечиваться посредством DNSSEC.

[1] В настоящее время двумя структурами корневых серверов управляет одна и та же организация — Verisign

В течение многих лет корневые серверы подвергались атакам, большая часть которых является разновидностями распределенной атаки типа «отказ в обслуживании» (DDOS). 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 приведет к снижению производительности, поскольку отправителю запросов придется 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 наблюдали как раз противоположное. Реакцией структур корневых серверов на недавнюю угрозу со стороны хакерской организации *Анонимус* стало расширение полосы пропускания и развертывание новых серверов с большой помпой.

Конечно, нет необходимости направлять атаку против комплекса корневых серверов, ее целью может быть соединение (соединения) пользователя с Интернетом. Хотя размер ущерба ограничен, при сравнении атакующей бот-сети и отдельного предприятия как правило значительный перевес сил на стороне атакующего, даже в случае крупных предприятий.

В своей практической деятельности некоторые члены комиссии рекомендовали предприятиям распространять во внутренней сети копии корневой зоны **и любых других критически важных 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, обретение внутренней самодостаточности в плане DNS, устраняющее угрозу отсутствия доступа к внешним серверам или ущерба от случайных или намеренных действий реестра, регистратора, оператора корневого сервера и т. д., является хорошей идеей для предприятия.

Учитывая факт наличия DNSSEC, у нас имеется способ распространения зоны, подлинность которой можно проверить с помощью встроенных цифровых подписей. Мы считаем, что этот принцип можно дополнительно расширить, например, защитив 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 описанная в предложении Пола Викси, включена в раздел «Дополнения» настоящего отчета.

Есть также 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.) Давайте просто устраним эту проблему.

Следует сообщить об отсутствии технической необходимости замены существующей системы корневых серверов тем лицам, которые предпочитают такой вариант; давайте просто упростим репликацию в корневой зоне и подадим пример для остальных зон.

4.3. Совместное управление зоной

В предыдущем разделе мы обсуждали 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.

Если описать простым языком, то корневая зона обновляется последовательно:

- ICANN получает от ДВУ 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, позволяющая задуматься о разделении контроля над корневой зоной? В этом направлении велись некоторые теоретические разработки. Одним из направлений научной мысли является использование нескольких (N) подписей для данных. Тогда для проверки подлинности данных потребуется M/N подписей. Конечно, ведутся споры относительно значений M и N и необходимости/желательности различных систем шифрования.

Мы не намерены высказываться в пользу конкретной системы в настоящем документе, но мы действительно считаем, что для начала качественной разработки можно использовать политический процесс принятия решения о способах совместного управления. Нашим замыслом является создание набора инструментов совместного управления зонами, не только для корневой зоны, но также 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 сведений о подписании DNSSEC, однако мы задаемся вопросом, не лучше ли создать общее средство вместо решения для этой точечной проблемы. Координация прямых и обратных адресов может быть еще одной прикладной областью.

Итак, что необходимо? Мы предполагаемой, что правильной моделью является такая, в которой у всех сторон, осуществляющих совместное управление, имеется ряд возможностей:

- Система инициализации общей зоны состоит из самой зоны, правил и индивидуальных журналов для регистрации каждым участником своих запросов и действий
- Запрос любого типа виден всем остальным участникам, которые могут его утвердить или отклонить, кроме того, возможен тайм-аут запроса
- Правила определяют, что происходит с запросом

- Одним из типов правил является голосование, которое определяет условия успешного выполнения запроса. Это может быть связано с задержкой из-за необходимости обсуждения запроса всеми сторонами.
    - Правила ВВУИО для нДВУ предписывают использование принципа 1 из N, таким образом каждый национальный домен верхнего уровня (нДВУ) может в одностороннем порядке менять собственные данные.
    - Другие домены могут использовать простое большинство голосов
- Указанные задержки могут быть важны, для того чтобы другие могли указать на операционные проблемы и дать возможность автору запроса пересмотреть его
- 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. Возможно, это кажется фантазией, однако византийские алгоритмы, такие как Bitcoin и Namecoin [Андреесен, 2014 г.] демонстрируют, что такие системы сегодня стали реальностью.

(Обратите внимание, что мы не предлагаем использовать эти правила, а предлагаем использовать распределенную систему для реализации любых правил, какие захочет ввести сообщество.)

4.4. Деятельность реестров/регистраторов

Некоторые члены комиссии утверждали, что ICANN в процессе своей деятельности должна давать гарантии относительно уровня обслуживания, однако комиссия не посчитала это проблемой, в решении которой она может добиться успеха.

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 программы ввода новых ДВУ 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 они могли напрямую использоваться любым участником интернет-сообщества.

4.5.2. Дата рождения, деятельность и области использования домена

Репутация DNS является ценным инструментом безопасности. Дата создания домена, вероятно, является единственной наиболее показательной информационной составляющей. Другая составляющая — частота обновления серверов имен и адресов домена. Новые домены и домены с высокой активностью обновления являются подозрительными. Желательно предоставлять эту информацию в режиме реального времени.

Информация об областях использования обсуждалась аналогичным образом, однако мы ожидаем результатов следующей конференции IETF в Лондоне, которая пройдет в марте 2014 г.

4.5.3. Пример LISP

На раннем этапе работы комиссии 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. Мы изыскали 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 контролировать политику и эксплуатацию?
- Кто должен этим заниматься: ICANN или региональные интернет-реестры (РИР)?
- Изменится ли ответ, если не охватывать IP-адреса?

Материалы по LISP содержатся в приложении. Никакие действия в рамках этого эксперимента не были предприняты.

По мнению некоторых членов комиссии: «LISP всего лишь единичный пример более общего класса технологий туннелирования транспортного уровня, и как таковой не ставит каких-либо 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 не является четко аргументированным».

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

4.6. Конфликты

Многие члены комиссии были знакомы с проблемой конфликтов в DNS, и хотя эта проблема широко обсуждалась, никакие новые содержательные направления не появились. У комиссии возникло ощущение, что физический прототип описанной в документе [ICANN, 2013 г.] системы настоятельно необходим.

5. Основы протокола DNS

Можно ли представить себе фундаментальный пересмотр, модернизацию или возрождение DNS? Многие, в том числе некоторые члены комиссии, считают, что установленная базовая система слишком невосприимчива к изменениям или что процесс нарушен, или что целесообразно начать все заново.

Удивительно, но комиссия оказалась единодушна во мнении, что усилия по описанию проблем и поиск решений оправданы; возможно, просто для того, чтобы поставить в этом вопросе точку. В настоящем разделе мы описываем некоторые проблемы, которые необходимо изучить в случае более широких 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, в противном случае они не будут получать электронную почту или веб-трафик. Однако из приблизительно 60 записей, которые были определены, широко используется меньше 10.

Усилия по созданию приложений натолкнулись на такие же трудности.

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, а также маршрутизации почты через границы организации — 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 к двум реализациям, использующим ресурсную запись TXT, и к спорам относительно целесообразности стандартизации новых типов когда бы то ни было.

Рекомендация по преобразованию телефонных номеров E.164 (ENUM), предназначенная 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 настоящей инновацией, разработчики ENUM проигнорировали необходимость маршрутизации информации, не являющейся телефонным номером вызываемого абонента, и производители оборудования предпочли хранить это значение в своих патентованных системах.

5.1. Общие принципы

Любая 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, невзирая на механизм расширения для DNS (EDNS0), большое количество аппаратного и программного обеспечения не будет передавать большие пакеты.
- Сохранять возможности подключения
- Стараться способствовать согласованным реализациям — если различные разработчики не следуют спецификациям, пользователь будет 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. Новые типы данных были определены, 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.

Мы утверждаем следующее: либо DNS следует определить свои собственные типы и форматы регистрационных записей в метаданных, переносимых в DNS, либо мы должны официально признать 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. Распространение

Зональная структура данных и кеширование по записи ресурса реализовано с отчасти неравномерными «улучшениями» до 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.

Мы также считаем, что можно улучшить безопасность за счет более частой репликации зон (возможно, имеющих меньший размер). Эти данные не обязательно должны быть защищены DNSSEC и, следовательно, могут повысить безопасность в тех местах, где система DNSSEC не внедрена.

5.4. Интерфейс программирования приложений (API)

API в системе DNS существует в двух видах: пользовательский интерфейс и имена на уровне API. В обоих случаях принес бы пользу стандартный синтаксис, который позволяет задать в явном виде полное доменное имя (FQDN). Качество обслуживания сообщества пользователей улучшилось бы при использовании согласованной совокупности политик для всех пользовательских интерфейсов, однако неясно, существует ли возможность уговорить поставщиков сделать это.

Интерфейс программирования API несколько раз пытались пересмотреть, в большинстве случаев неудачно. Недавно мы видели презентацию Пола Хоффмана (Paul Hoffman) на тему нового проектного решения, особенностями которого являются асинхронные интерфейсы и поддержка DNSSEC. См. приложение. Мы понимаем, что сейчас ведется работа в Verisign Labs и NLnet, но не смогли получить дополнительную информацию, хотя было сказано, что ее опубликование близится.

Однако независимо от API, есть сопутствующий вопрос: следует ли выполнять проверку подлинности DNSSEC и фильтрацию DNS (если такова предусмотрена). 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 морально устаревших 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 поставщику услуг Интернета или других услуг.

Политические и правовые ограничения могут потребовать иного.

Протокол запросов

5.5. Протокол запросов

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

Исконные проблемы транспортировки UDP начинаются с традиционного ограничения размера MTU 576 байтами. Ее 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 13 корневых серверов; впоследствии добавление подписей DNSSEC существенно расширило размер ответных пакетов. Считается, что механизм EDNS0 решил эту проблему, наряду с другими, с некоторым успехом. Однако есть и

другие ограничения, например, для размера кадра Ethernet — 1582, 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, которое блокирует доступ к порту 53 по протоколу TCP или ограничивает размер пакетов, или даже перехватывает 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 — 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 полезного трафика, чтобы отфильтровать трафик, используемый для атаки. Проверка адреса источника позволила бы решить существенную часть данной проблемы, как для DNS, так и для многих других протоколов. Комиссия это поддерживает, но такие меры 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 упрощенные механизмы проверки подлинности.

Одна из научных школ предлагает решить проблему транспорта путем переноса 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 (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. Однако как один, так и другой может не 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 какую-то схему контроля доступа к последующим меткам вместо NSEC.

Протоколы, разработанные в научно-исследовательской среде, такие как CCN, учитывают недостатки DNS и содержат все эти функциональные возможности. Проблема в большей степени состоит в поиске стимулов и путей модернизации существующей инфраструктуры с сохранением обратной совместимости, а не в новых научных открытиях в сфере протоколов.

6. Выводы и рекомендации

- Рост использования DNS в инфраструктуре продолжится; использование DNS в пользовательском интерфейсе (UI) ограничивается альтернативными поисковыми системами, интерфейсами мобильных устройств и т. п.
- ICANN должна публиковать больше подписанных DNSSEC данных для резервных меток и т. п.
- В сотрудничестве с IETF и другими организациями провести исследование для определения архитектурной концепции DNS в 2020 г.
- Спроектировать и создать прототип системы открытого опубликования данных корневой зоны.
- Спроектировать систему совместного управления корневой зоной.
- Выполнить практический анализ конфликтов для тестирования простоты реализации [ICANN, 2013 г.].

7. Ссылки

[Андреесен, 2014 г.] Андреесен, «В чем важность Биткойна?» (Andreesen, «Why Bitcoin Matters»), http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters

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

[Фаязбахш, 2013 г.] Фаязбахш с соавторами, «Меньше огорчений, максимум приобретений: постепенное развертывание ICN» (Fayazbakhsh et al, «Less Pain, Most of the Gain: Incrementally Deployable ICN»), Sigcomm, 2013 г.

[Годси, 2011 г.] Годси с соавторами «Присвоение имен в контентноориентированной архитектуре» (Ghodsi et al, «Naming in Content-Oriented Architecture»), Sigcomm, 2011 г.

[Хьюстон, 2013 г.] Исследование «DNS только по протоколу TCP».

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

[ICANN, 2013 г.] «Руководство для ИТ-специалистов по идентификации и смягчению конфликтов имен»,

https://www.icann.org/en/about/staff/security/ssr/name-collision-mitigation-05dec13-en.pdf

[Камински, 2004 г.] Д. Камински, «Туннелирование аудио, видео и SSH по DNS» (D. Kaminsky, «Tunneling Audio, Video, and SSH over DNS», BlackHat, 2004 г.

[Merit] Разделы, касающиеся доменов 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

[Мокапетрис, 1988 г.] П. Мокапетрис и К. Данлэп, «Разработка системы доменных имен» (P. Mockapetris and K. Dunlap, «Development of the Domain Name System»), SIGCOMM, 1988 г.

[Newyorker, 2013 г.]

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

[RFC 881] Дж. Постел, «План и график для доменных имен» (J. Postel, «The Domain Names Plan and Schedule»), ноябрь 1983 г.

[RFC 882] П. Мокапетрис, «Доменные имена — концепции и средства» (P. Mockapetris, «Domain Names — Concepts and Facilities»), ноябрь 1983 г.

[RFC 883] П. Мокапетрис, «Доменные имена — реализация и спецификация» (P. Mockapetris, «Domain Names – Implementation and Specification»), ноябрь 1983 г.

[RFC 1034] П. Мокапетрис, «Доменные имена — концепции и средства» (P. Mockapetris, «Domain Names — Concepts and Facilities»), ноябрь 1987 г.

[RFC 1035] П. Мокапетрис, «Доменные имена — реализация и спецификация» (P. Mockapetris, «Domain Names – Implementation and Specification»), ноябрь 1987 г.

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

8. Глоссарий

API Интерфейс программирования приложений

CCN Сеть, ориентированная на контент

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	Полное доменное имя
FTP	Протокол передачи файлов
HTTPS	Протокол защищенной передачи гипертекста
IANA	Агентство по распределению номеров Интернета
ICANN	Корпорация по распределению имен и номеров в Интернете
ICN	Сеть, ориентированная на информацию
IEEE	Институт инженеров по электротехнике и электронике
IETF	Инженерный совет Интернета
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 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 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
RR	Ресурсная запись — неделимая единица информации в DNS

Rsynch	Протокол дистанционной синхронизации — обеспечивает синхронизацию файлов и каталогов с минимизацией передачи данных благодаря использованию инкрементного кодирования.
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
ИИ	Искусственный интеллект
нДВУ	Национальный домен верхнего уровня — ДВУ, выделенный конкретной стране
рДВУ	Родовой домен верхнего уровня — ДВУ, который не соответствует коду какой-либо страны
РИР	Региональный интернет-реестр — одна из организаций, управляющих выделением и регистрацией номерных ресурсов Интернета в конкретном регионе мира. Например, ARIN — Американский реестр номеров Интернета, который действует в Канаде, США и на многих островах Карибского бассейна и северной части Атлантического океана.

9. Дополнения членов комиссии

Обратите внимание, что все дополнения приведены дословно, в том виде, как они были направлены отдельными лицами.

9.1. Дополнение Джеймса Сенга

Техническая архитектура

Являясь в душе хакером, я люблю децентрализованную архитектуру. Можно доказать, 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.

Однако мне неизвестна децентрализованная и одновременно скоординированная система идентификаторов, которая бы реально широко использовалась. Поэтому, хочешь не хочешь, система DNS все еще остается одной из наиболее распространенных систем идентификаторов. В IETF мы выбираем в качестве победителей «работающие коды», которые не обязательно лучше всего спроектированы.

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, но не решают ее. Обратите внимание, что я назвал это политической проблемой, поскольку вообще не думаю, что наличие нескольких корневых зон решает какую-либо техническую проблему; можно даже сказать, что это только повышает техническую сложность

ICANN

Система DNS и ее централизованный характер корневой зоны частично привели к тому, что выполнение первоначально простой функции IANA сегодня осуществляется огромной организацией под названием ICANN.

Моя работа в ICANN началась с первой конференции в 1999 году, и я присутствовал почти на всех последующих конференциях. В течение этих лет были 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 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 наиболее важно то, что, хотя могло бы быть и лучше, это работает. Предлагаемой альтернативе (МСЭ) присущи другие известные нам и более серьезные проблемы.

Поэтому я поддерживаю ICANN, так как это лучшая работающая система, которая у нас есть для координации идентификаторов DNS и корневой зоны.

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 интернационализированных доменных имен (IDN) 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 в случае создания IDN за рамками экосистемы DNS развертывание могло бы осуществляться намного быстрее (см., например, «Ключевые слова родного языка»), я говорю, что IDN лучше также и потому, что являются частью экосистемы DNS, где есть хорошо сформулированные открытые стандарты, открытые реализации, компании, которые действуют на основе официального статуса DNS, и адекватные средства защиты владельцев регистрации и конечных пользователей IDN.

По этой причине у меня нет сомнений и я поддерживаю изучение 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 такие идентификаторы предназначены для конечных пользователей. Они могут извлечь пару уроков из истории идентификаторов DNS и ICANN.

Политические аспекты корневой зоны

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

Ситуацию максимально ухудшает то, что 11 из 13 корневых серверов расположены в США в силу исторической случайности, 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 такой-то и такой-то стране, мы отклоняем это предложение, приводя исторические или технические доводы, доказывающие, что создать больше 13 корневых зон нельзя никоим образом.

Исторические факты я могу принять как довод.

Технические причины — нет. Это в большей степени отговорка, поскольку мне неизвестно о каких-либо серьезных усилиях IETF по поиску путей выхода за рамки 13 корневых зон. Вот почему я сказал на конференции в Буэнос-Айресе, что могу придумать пару технических решений, подходящих по крайней мере в качестве первоначального проекта. Мы не можем позволить корпорации ICANN по-прежнему использовать IETF / технические доводы для оправдания своего отказа от решения политических проблем, с которыми она столкнулась. 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 боле важно, управлять корневыми серверами не настолько приятно, как расхваливают.

Наличие у кого-либо корневой зоны не означает наличия прямого контроля над Интернетом. На самом деле, это такое же скучное занятие, как и эксплуатация экземпляра корневого сервера. Хотя, 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 то, что я сказал выше, однако большинство сотрудников ICANN не понимают.

Таким образом, при выборе оператора корневой зоны надо учитывать ряд соображений, потому что это крайне важно для стабильности идентификаторов Интернета, большая часть которой основана на Доверии. Однако Доверие, нравится вам это или нет, не является инженерной проблемой.

Джеймс Сенг

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

Почему DNSPod приносит пользу в Китае, несмотря на то, что «нарушает» работу DNS.

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

отсутствует — НЕ выполняет поиск в DNS

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

до — применяет список поиска, и если возвращен результат NXDOMAIN, то выполняет поиск базового имени

после — выполняет поиск базового имени, и если возвращен результат NXDOMAIN, то затем применяет список поиска

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

Поведение библиотеки DNS-преобразователя в базовых 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)	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 ДВУ и не выполняет поиск в DNS, когда имя не является ДВУ

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 распознает делегированные ДВУ и посылает запросы только тогда, когда последней меткой является ДВУ

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

9.3. Наблюдения относительно согласованности и тенденций — Геофф Хьюстон

Если вернуться к истокам системы доменных имен, то можно обнаружить так называемый «файл HOSTS» как древнюю 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. Не было принудительно обеспечиваемого единообразия среди всех этих многочисленных экземпляров файла HOSTS во всем множестве подключенных к ARPANET узлов, и 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), и 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, и в то же время дает возможность распределенного управления пространством имен. Если избегать конфликтов меток в рамках отдельно взятой зоны иерархии имен DNS, то можно избежать конфликтов 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. Подразумевается, что DNS — согласованная система в том отношении, что при введении записи одного и того же имени в DNS, запросы на разрешение этого имени будут возвращать 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, в противном случае будет возвращено сообщение о том, что совпадение не найдено.

Эта модель пространства имен DNS как пространство идентификационных имен, используемое для поддержки интерфейса человека с сетью, претерпела ряд изменений, главным образом под влиянием способов использования идентификаторов человеком в процессе общения. Мы стремимся использовать менее точные идентификаторы и такие, которые содержат элементы, отражающие местные условия, использующие местные языки и системы письменности, поэтому с течением времени роль DNS как формы человеческого интерфейса с сетевыми ресурсами и службами стала составной частью более широких 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 подразумевает использование локального списка поиска или суффиксов меток, позволяя пользователю указать начальную часть доменного имени и поручить локальному приложению или программе преобразования имен добавить 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.

Использование этих локальных операций преобразования имен дополнительно расширилось после возникновения необходимости сопоставления в DNS идентификаторов, для формирования которых используются символы не в американской кодировке ASCII (IDN: RFC5891). В этом документе четко определен процесс преобразования идентификатора, введенного пользователем, в закодированную строку метки, которая формирует запрос DNS. В этом случае алгоритм преобразования точно определен, чтобы многочисленные реализации стандарта IDN обеспечивали единообразное сопоставление идентификатора, введенного с использованием конкретного алфавита, и формы 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 попытается сделать это самостоятельно.

9.4. Дополнение Пола Викси

Универсальная адресация любому устройству для корневой зоны

Обзор

Мы предлагаем IANA создать несколько дополнительных вариантов корневой зоны DNS, чтобы обеспечить возможность универсальной адресации любому устройству и провести оперативный анализ. «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 рДВУ». При таком подходе служба имен корневой зоны не считается управляемой и рассматривается как неуправляемая утилита.

История вопроса

Систему универсальной адресации любому устройству для корневой зоны невозможно развернуть безопасным и надежным образом до наступления эпохи DNSSEC, поскольку в отсутствие DNSSEC любой отвечающий сервер можно настроить на произвольные данные корня DNS, включая новые ДВУ или повторно делегированные существующие ДВУ. При наличии DNSSEC операторы рекурсивных серверов имен могут настроить функцию подтверждения DNSSEC так, чтобы любая информация о рДВУ, поступающая от сервера имен системы с универсальной адресацией любому устройству, в обязательном порядке была заверена IANA, на что будут указывать подписи DNSSEC, выполненные при помощи ключа для подписания корневой зоны IANA (ZSK).

Современная система корневых серверов имен, как и существовавшая ранее, подвергается критике в том числе за отсутствие остойчивости к DDOS-атакам; при этом отмечается, что даже в условиях текущей широкомасштабной адресации любому устройству, используемой всеми операторами корневых серверов имен, в мире есть всего лишь несколько сотен серверов имен, которые являются полномочными отправителями ответов для корневой зоны DNS. Мы также обеспокоены в связи с необходимостью получения 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. Первый, базовая система универсальной адресации любому устройству, позволит любому оператору сервера имен перехватывать трафик, направляемый в систему корневых серверов имен, и отвечать на запросы локально. 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, чьи адреса не выделены ни одному конкретному оператору сервера имен корневой зоны (RNSO), а вместо этого остаются в ведении IANA для использования всеми без исключения заинтересованными сторонами. IANA обратится к РИР (например, ARIN или APNIC) с просьбой о выделении микроскопических инфраструктурных ресурсов, таких 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 рДВУ, в том числе тех, которые в ином случае не будут готовы к делегированию (например, .CORP и .HOME). Эти новые рДВУ будут делегированы на сервер имен, находящийся под управлением самой IANA в целях измерения. Каждому новому рДВУ будут присвоены подстановочные записи A и AAAA, адреса которых будут указывать на веб-серверы, находящиеся под управлением самой IANA в целях измерения.

Последствия

Учитывая иерархический характер маршрутизации в Интернете, адресные блоки для адресации любому устройству могут быть анонсированы на нескольких уровнях. Виртуальная машина (ВМ), запущенная на портативном персональном компьютере, может иметь собственный процесс сервера имен, который осуществляет прослушивание соответствующих общеизвестных адресов, таким образом ни один из запросов к службе имен корневой зоны не будет пропущен этой ВМ. Сам портативный персональный компьютер может также перехватывать исходящий трафик, направленный на эти общеизвестные адреса, чтобы обслуживать другие ВМ или процессы, запущенные на этом компьютере. Беспроводной маршрутизатор, находящийся за этим портативным компьютером может иметь серверы, прослушивающие эти адреса, таким образом ни один из запросов к службе имен корневой зоны не будет пропущен этой беспроводной ЛВС. Поставщик услуг Интернета может использовать серверы, прослушивающие эти общеизвестные адреса, чтобы обслуживать всех без исключения клиентов, не имеющих своих собственных серверов. И наконец, ожидается, что в мировом 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 этого 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 такого нежелательного перехвата. Мы хотим, чтобы последствием подобной атаки стало «жертва теряет службу корневых имен», а не «жертва 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 следует опубликовать в виде файла «корневых подсказок». Приведенные данные для iana-servers.net также должны присутствовать в реальной зоне iana-servers.net. Для этих примеров потребуются 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.

v6only-1 IN AAAA 2001:?:3::1

v6only-2 IN AAAA 2001:?:4::2

Вариант 3: универсальная адресация для изучения конфликтов рДВУ

. 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

gtldstudy-2 IN AAAA 2001:?:6::2

gtldstudy-2 IN A ?.?.6.2

10. Приложения

10.1. Материалы по LISP

10.2. Материалы Хоффмана по API