

Измерение DNS поверх IPv6

Джефф Хьюстон

Аннотация

В статье рассматривается готовность системы DNS к работе с протоколом IPv6 – в частности, возможность разрешения доменных имён через авторитетные DNS-серверы, доступные исключительно по IPv6. Опираясь на данные измерений APNIC, Джефф Хьюстон предлагает метод тестирования, ориентированный именно на DNS и дополняющий измерения, проводимые через веб-среду.

Результаты показывают, что около 75% пользователей Интернета способны выполнять DNS-запросы по протоколу IPv6. При этом расхождения в данных, полученных с помощью разных методов измерения, подчёркивают сложность оценки готовности к IPv6, а также трудности, связанные с переходом на DNS-инфраструктуру, функционирующую исключительно на базе IPv6.

Ключевые слова:

DNS, IPv6, резолвер

Теоретически, архитектура IPv6 была спроектирована так, что транспортные протоколы сквозной передачи данных верхнего уровня, а именно TCP и UDP, не должны были знать о том, какой IP-протокол используется на сетевом уровне. Ведь мы должны иметь возможность использовать IPv4 и IPv6 в системе DNS взаимозаменяемо, верно?

Эта тема рассматривалась в документе серии BCP (Best Common Practice, «лучшая современная практика»), опубликованном в 2004 году под номером RFC 3901, «DNS IPv6 Transport Operational Guidelines» («Рекомендации по использованию транспорта IPv6 для DNS»). В документе содержались две основные рекомендации:

- во-первых, каждый рекурсивный сервер имён должен быть либо с поддержкой только IPv4, либо с двойным стеком (dual-stack);
- во-вторых, каждая зона DNS должна обслуживаться как минимум одним доступным сервером имён, использующим IPv4.

По сути, это был призыв «Пока не отказывайтесь от IPv4!», что на то время было вполне разумным советом.

В начале 2026 года планируется опубликовать обновлённую версию этого документа под названием RFC 3901bis, в которой предлагается несколько иной набор рекомендаций (прим. редакции – эта версия была опубликована в августе 2026 года под номером RFC10001). Согласно этому документу, как минимум два сервера имён для каждой зоны должны поддерживать двойной стек, то есть каждый сервер имён будет доступен по IPv6. Этот документ даёт следующую практическую рекомендацию по поддержке IPv6 в DNS: «Пришло время отнестись к IPv6 всерьез!» Предположение, лежащее в основе документа RFC 3901bis, заключается в том, что IPv6 теперь является зрелой и хорошо изученной технологией, а использование IPv6 в качестве транспорта для DNS столь же эффективно и быстро, как и использование IPv4.

Но можно ли считать этот совет разумным? Основная проблема, связанная с отказами в обслуживании DNS, заключалась в адаптации к нагрузкам при передаче больших объёмов данных через сети с ограничением размера паке-

тов. IPv6 лишил маршрутизаторы возможности выполнять «фрагментацию на лету», и это повлияло на работу DNS при больших нагрузках с использованием UDP поверх IPv6.

За последние несколько лет я неоднократно рассматривал этот сценарий, в том числе в статьях «Adding IPv6-only to DNS and Truncation in UDP», «IPv6, the DNS and Happy Eyeballs», «IPv6 and the DNS». При попытке передать по протоколу IPv6 большие ответы, требующие фрагментации пакетов, DNS сталкивается с примерно 40% отказов.

Что, если мы ограничим рассмотрение типичным случаем DNS, когда запросы и ответы свободно помещаются в размере максимального нефрагментированного пакета IPv6 в 1280 байт? Какая часть пользователей Интернета сможет получить надёжный доступ к DNS-серверу, доступ к которому возможен только по протоколу IPv6?

Чтобы ответить на такой вопрос, нам нужно было бы провести широкомасштабное исследование среди пользователей Интернета и проверить их способность «резолвить» (разрешать в адрес IP) DNS-имя, доступ к которому возможен только по IPv6. Эта тема степени готовности конечных пользователей использовать IPv6 для доступа ко всем формам интернет-сервисов уже много лет вызывала значительный интерес в рамках более масштабной задачи перевода всего Интернета на IPv6.

Вопрос, который я хотел бы здесь рассмотреть, касается степени поддержки пользовательскими DNS-резолверами протокола DNS поверх IPv6. Другими словами, если бы мы разместили авторитетный сервер на платформе, поддерживающей только IPv6, какая часть пользователей Интернета смогла бы разрезолвить имя, доступное таким образом?

Измерение DNS

Во-первых, несколько слов предостережения. При измерении DNS всё не так просто, как кажется. Когда мы говорим о DNS в этом контексте, мы на самом деле говорим о функции резолвинга имён. И центральным в этом является концепция «DNS-резолвера».

Резолверы

Итак, давайте зададим вопрос: «Что такое DNS-резолвер?»

Как ни странно, прямого ответа не существует. Мы на самом деле не до конца понимаем, что такое «DNS-резолвер». Это может быть единая платформа, на которой запущен экземпляр кода DNS-резолвера, или это может быть набор серверных DNS-систем с каким-либо фронтенд-распределителем нагрузки, или это может быть гибридная совокупность серверов с набором частично синхронизированных кешей, чтобы они эмулировали общий кеш и использовали этот общий кеш в работе каждого серверного движка.

Мы грубо классифицировали DNS-резолверы на stub-резолверы (локальные резолверы), которые находятся близко к конечному пользователю на его устройстве, рекурсивные резолверы, которые предназначены для навигации по распределённой базе данных DNS для резолвинга запрашиваемых имён, и перенаправляющие (forwarding) резолверы, которые передают свои запросы другим резолверам, а не отвечают на них сами. Существуют и более сложные формы гибридного поведения, которые могут быть распределены между множеством различных систем резолвинга. Все они называются резолверами.

Не все резолверы одинаковы и не все одинаково важны. У резолвера может быть всего один клиент, как у DNS-резолвера в моей локальной сети, а может быть и несколько миллионов, если не сотен миллионов клиентов, как в случае с некоторыми крупными открытыми DNS-резолверами, или любое промежуточное значение. Поэтому, когда мы говорим о DNS-резолверах, на самом деле довольно сложно понять, о чём именно идёт речь. Получение статистического показателя в виде некоторого процента DNS-резолверов, поддерживающих запросы по IPv6, не имеет смысла с точки зрения оценки полезности IPv6 в DNS. Вот почему, когда мы говорим об уровне поддержки IPv6 в DNS-резолвинге, метрикой, которую мы будем использовать, будет не количество самих DNS-резолверов, а количество пользователей в процентном соотношении от общего числа пользователей.

Запросы

Конечно, если вы думали, что это был сложный вопрос о DNS, то вот вам еще один: «Что такое запрос?»

Вопрос может показаться глупым, но в нём есть смысл. Процесс резолвинга, используемый DNS для навигации по структурам данных DNS, вызывает веерный (fan-out) запрос, где один начальный запрос к рекурсивному резолверу заставляет этот резолвер запускать последовательность поисковых запросов, в попытках понять, где может находиться запрашиваемая информация в рамках распределённой базы данных DNS.

Связанная с этим проблема заключается в том, что по умолчанию DNS использует UDP в качестве транспорта. UDP не обеспечивает никаких гарантий доставки, поэтому отправитель должен некоторое время ждать ответа, и если ответ не поступает за это время, у него нет другого выхода, кроме как повторить запрос. Резолверы не ведут себя единообразно, в разных реализациях используются разные значения таймеров для определения времени повторного запроса. Выбор таймера представляет собой компромисс между стремлением ответить как можно быстрее на исходный DNS-запрос и предотвращением флуда(перегрузки) DNS излишними запросами.

DNS-запросы не имеют счётчика переходов – «хопов» (hop count), поэтому, если запрос перенаправляется от одного резолвера к другому, к нему не прикрепляется история того, откуда пришёл запрос, и нет кода причины, почему запрос был перенаправлен. В DNS нет контекста, который позволил бы нам определить причину любого конкретного запроса,

нет счётчика хопов для выявления зацикливания и нет TTL (time-to-live) – «времени жизни» для обнаружения и удаления «устаревших» запросов. В результате DNS-резолвинг склонен грешить избыточностью в генерации запросов. Наши измерения, проведённые на авторитетном DNS-сервере, показывают, что от 25% до 30% отдельных запросов повторяются внутри DNS (рисунок 1).

Я подозреваю, что одна из причин такого расточительного повторения запросов внутри DNS кроется в выборе UDP в качестве транспортного протокола по умолчанию. Резолвер не знает, когда запрос был отброшен, и лучшая стратегия для резолвера – разослать поток запросов на другие авторитетные серверы, а в случае локального резолвера – на другие рекурсивные резолверы, чтобы компенсировать непредсказуемое время отклика UDP.

Измерения APNIC

Наконец, давайте посмотрим на собственную измерительную установку APNIC, которая используется для проведения подобных измерений.

Мы используем рекламную сеть Google для генерации DNS-запросов внутри рекламных онлайн-кампаний и используем параметры в рекламной кампании, чтобы получить как можно более широкое распространение рекламы. Каждое объявление содержит список URL-адресов и управляющий скрипт, который ставит браузеру задачу запрашивать каждый URL-адрес, а затем сообщает об успешном (или неуспешном) выполнении каждой попытки запроса. DNS-имена, входящие в состав каждого URL, содержат компонент имени, уникальный для каждого отдельного пользователя, получившего рекламу. Таким образом, рекурсивные DNS-резолверы не имеют кешированных данных и вынуждены отправлять запросы авторитетному DNS-серверу для резолвинга предоставленного имени. Мы отслеживаем эти запросы от рекурсивных к авторитетным серверам инструментами нашего авторитетного сервера и сопоставляем эти запросы с записями о размещении рекламы на экспериментальной платформе.

Измерение DNS поверх IPv6 с помощью Web Fetch

Для выполнения этого измерения мы написали скрипт для рекламы, который включает URL, использующий уникальное DNS-имя, и настроили авторитетный сервер для этого DNS-имени так, чтобы он был доступен только по IPv6.

Пользователь может резолвить DNS-имя и, следовательно, загрузить веб-объект, только если его настройка резолвера имён поддерживает DNS-запросы по IPv6. Хотя резолвинг

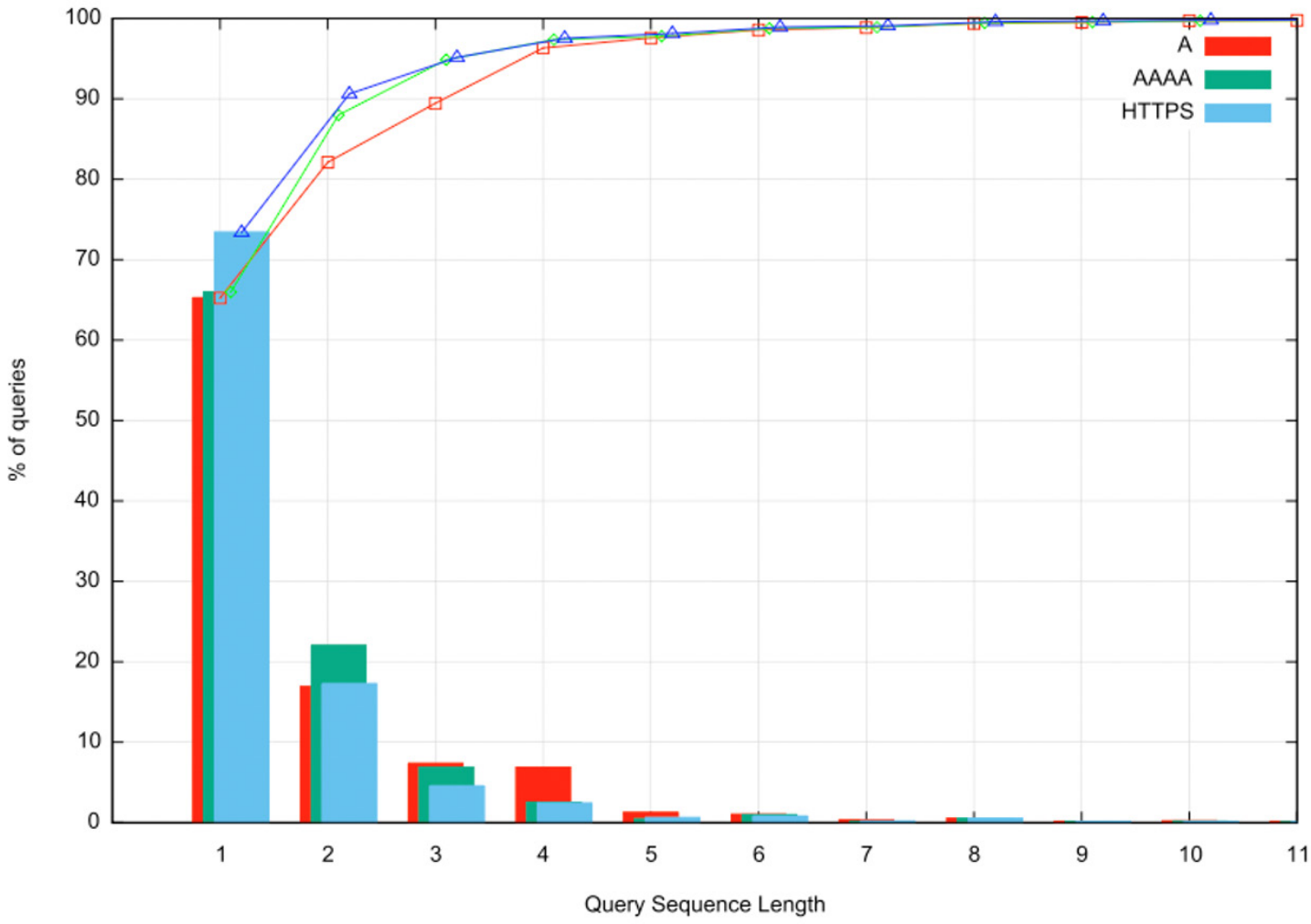

Рис. 1. Профиль повторения DNS-запросов.

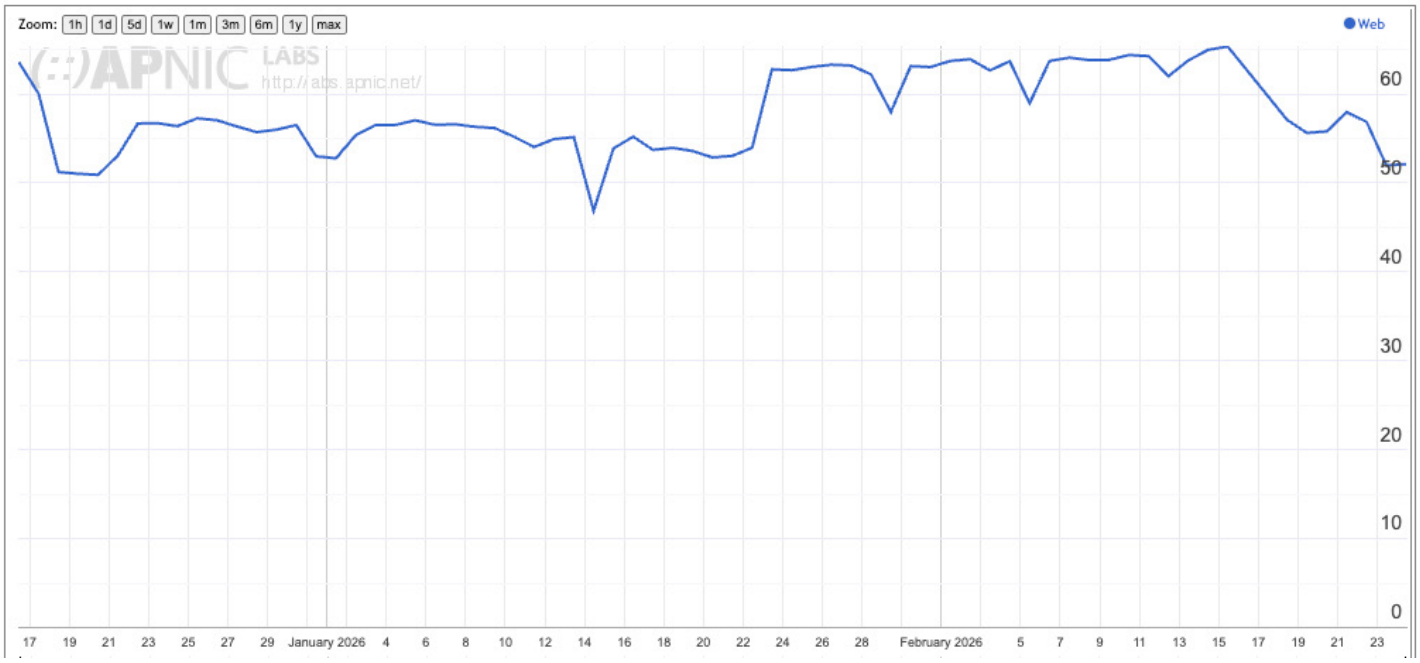

Рис. 2. Веб-измерение способности DNS-резолвинга с использованием IPv6.

DNS-имени опирается на IPv6, само имя может быть преобразовано как в IPv4 (A), так и в IPv6 (AAAA) записи.

Таким образом, провести измерение довольно просто. Мы считаем записи о размещении рекламы и долю тех записей, где пользователь успешно выполняет загрузку веб-объекта DNS поверх IPv6. Таким образом, доля успешных обращений – это показатель способности пользователей по всему Интернету выполнять резолвинг DNS с использованием IPv6. Эти данные показаны на рисунке 2.

Кажется, это разумное измерение. Результат, а именно то, что от 50% до 65% пользователей демонстрируют свою способность резолвить DNS-имя, требующее использования DNS поверх IPv6.

Мы закончили, да?

Ну, возможно, нет. Видите ли, внутри браузера пользователя происходит пара действий, о которых нам нужно знать. Браузер получает задачу загрузить веб-объект. Ему сообщают его имя, DNS-имя, которое он сначала должен резолвить. Только когда DNS разрезолвит это имя, браузер сможет выполнить загрузку. Но что, если выполнение скрипта рекламы будет прервано до завершения скрипта? Задача DNS, которая, возможно, уже была передана резолверу, будет выполняться до завершения, но когда результат будет передан обратно в браузер, последующей веб-загрузки не произойдёт. Возможно, этот результат не будет учтён.

Есть ли другой способ выполнить это измерение способности IPv6 в DNS, используя только DNS? Если бы это было возможно, то после передачи задачи в DNS процесс резолвинга имени продолжался бы до завершения и не прерывался бы досрочно, если бы управляющий скрипт рекламы был завершён.

Измерение DNS поверх IPv6 с помощью DNS

Ответ на этот вопрос заключается в том, что такое измерение можно провести полностью в рамках DNS. Мы используем метод «делегирования без привязки» (glueless delegation) в DNS.

Когда рекурсивный резолвер спрашивает авторитетный сервер об имени, которое не существует в обслуживаемой зоне, но находится в делегированной зоне, сервер вернёт ответ с перенаправлением (referral response).

При делегировании в DNS указывается имя делегированной зоны и имена серверов, которые являются авторитетными для этой зоны. Когда авторитетный сервер запрашивают об имени, которое находится в делегированной зоне, он генерирует ответ с перенаправлением, в секции Authority которого содержатся записи о серверах DNS, а в секции Additional – IP-адреса этих серверов («склеивающие записи», glue records). Если эти имена серверов указаны в делегированной зоне, то эти склеивающие записи необходимы, так как нет другого способа для рекурсивного резолвера преобразовать эти имена в их IP-адреса. Однако когда имена определены в другой зоне, не связанной с запрашиваемой зоной, эти склеивающие записи не являются необходимыми для резолвинга. Если склеивающие записи отсутствуют в ответе-перенаправлении, то рекурсивному резолверу потребуется приостановить основную задачу преобразования исходного имени и поработать над подзадачей резолвинга имени сервера DNS. После этого он сможет использовать полученные IP-адреса для возобновления резолвинга исходного имени.

Таким образом, это даёт основу для проверки поддержки IPv6 в DNS, как показано на рисунке 3.

```
Zone: example.com
...
a IN NS ns1.some.other.zone.
...


Zone: some.other.zone
...
. IN NS nso.some.other.zone.
nso IN AAAA 2001:db8::1
...
ns1 IN AAAA 2001:db8::2
...


Zone: a.example.com
...
. IN NS ns1.some.other.zone.
. IN A 192.0.2.3
IN AAAA 2001:db8::3
```

Рис. 3. Пример делегирования без склеивающих записей.

В этом случае рекурсивный резолвер, пытающийся преобразовать имя a.example.com, получит ответ с перенаправлением на имя сервера ns1.some.other.zone без склеивающих записей. После этого ему нужно будет приостановить процесс резолвинга a.example.com и начать процесс резолвинга имени сервера ns1.some.other.zone. После завершения этого процесса (с получением IPv6-адреса 2001:db8::2) он сможет вернуться к исходной задаче и запросить у этого IPv6-адреса IP-адреса a.example.com. Однако, поскольку сервер some.other.zone поддерживает только IPv6, рекурсивный резолвер может отправить этот запрос только в том случае, если он поддерживает DNS-запросы по протоколу IPv6 и может получить DNS-ответ только по протоколу IPv6.

Мы можем провести оба измерения с использованием DNS по IPv6 в рамках одного рекламного скрипта, протестировав DNS-среду пользователя обоими способами. Мы ожидаем, что результаты измерений будут достаточно хорошо коррелировать, при этом измерение с использованием DNS даст чуть более высокий результат. Именно это мы и наблюдаем (см. рисунок 4). Приблизительно на 10% более низкий результат при использовании веб-запроса можно объяснить «потерями» при переходе от резолвинга DNS к завершению веб-запроса.

Есть ли у нас основания для такого предположения?

Аномалии измерений

В ряде африканских стран наблюдается стабильное, хотя и аномальное поведение при измерении этого показателя, когда значение, полученное с помощью веб-измерений, значительно выше значения, полученного с помощью DNS. Хороший пример — Алжир (рисунок 5), хотя аналогичная ситуация наблюдается в Ливии, Египте, Мавритании, Либерии и ряде других преимущественно африканских стран (см. https://stats.labs.apnic.net/v6odns).

Есть и страны с противоположным аномальным результатом: в них показатель DNS выше веб-показателя значительно больше, чем на 10%. Хорошим примером такого противоположного аномального результата является Эфиопия (рисунок 6).

Стоит отметить ещё один результат, который можно увидеть на примере Германии, где ежедневные измерения на основе веб-запросов и DNS-запросов очень хорошо коррелируют друг с другом. Уровень «потери веб-трафика», когда DNS-запрос не преобразуется в видимый веб-запрос, крайне низок для всей выборки в этой стране (рисунок 7).

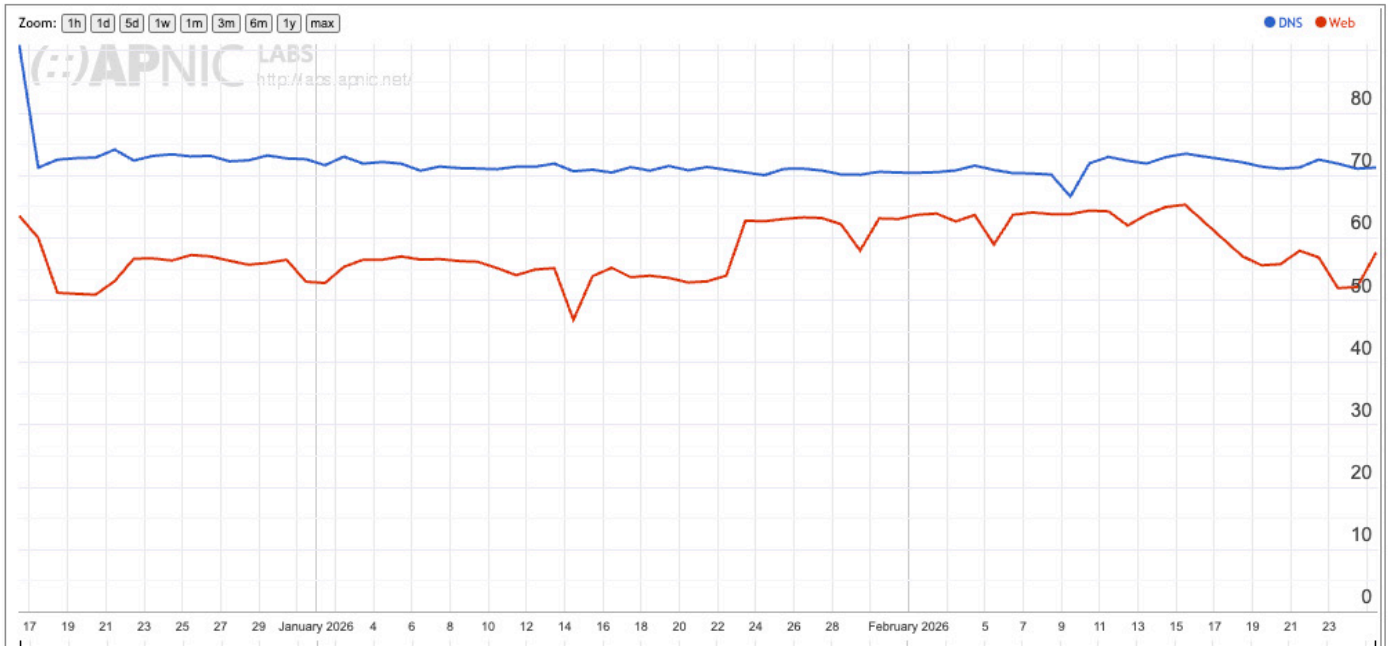

Рис. 4. Измерение способности резолвинга DNS поверх IPv6 с помощью DNS и веб-измерений.

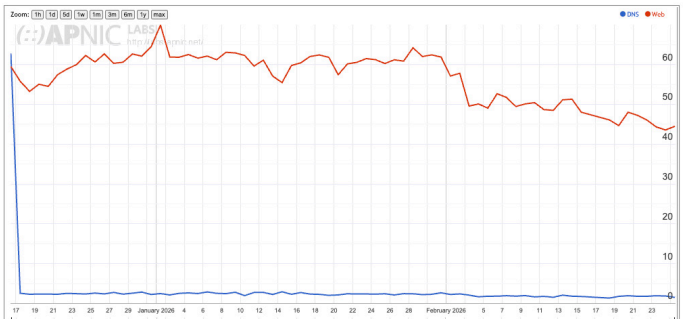

Рис. 5. Измерение способности резолвинга DNS поверх IPv6 на основе данных DNS и веб-измерений в Алжире.

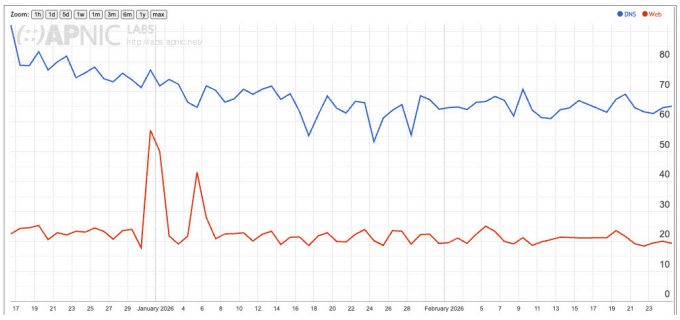

Рис. 6. Измерение способности резолвинга DNS поверх IPv6 на основе измерений DNS и веб-трафика в Эфиопии.

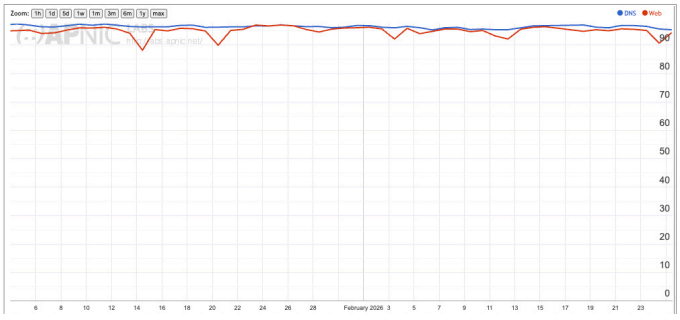

Рис. 7. Измерение способности резолвинга DNS поверх IPv6 на основе данных DNS и веб-измерений в Германии.

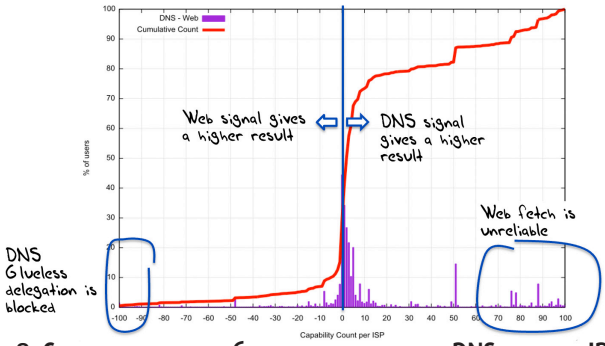

Рис. 8. Сравнение способности резолвинга DNS поверх IPv6, DNS и веб.

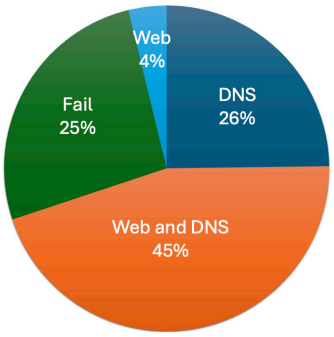

Рис. 9. Разбивка результатов измерений веб-трафика и DNS.

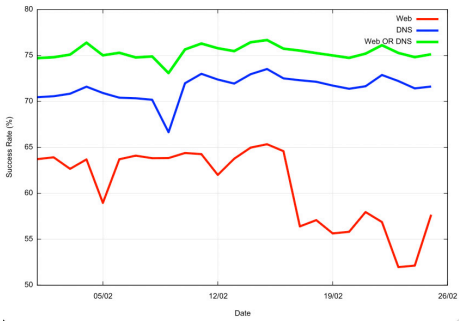

Рис. 10. Серия результатов по дням.

Эти результаты сложно объяснить в рамках традиционной модели инфраструктуры DNS, поскольку в обоих случаях измеряется одно и то же поведение одних и тех же пользователей, тестирующих одни и те же DNS-резолверы.

Один из способов сравнить эти два подхода — проанализировать каждую сеть и сопоставить результаты измерений DNS- и веб-трафика. Такое сравнение показано на рисунке 8.

Менее чем для 8% измеренных конечных точек значение, полученное при измерении с помощью DNS, было более чем на 10% меньше значения, полученного при измерении с помощью интернет-трафика, в то время как для 30% измеренных конечных точек наблюдалась обратная ситуация. Для оставшихся 62% измерений разница между двумя показателями не превышала 10%.

На рисунке 9 представлена разбивка результатов измерений с помощью трафика Интернет и с помощью DNS по дням. В 4% случаев при измерении с помощью трафика Интернет был получен положительный результат, указывающий на поддержку DNS поверх IPv6, в то время как при измерении с помощью DNS результат был отрицательным. В 26% случаев при измерении через DNS был получен положительный результат, а при измерении с помощью трафика Интернет — отрицательный. В 45% случаев и при измерении с помощью трафика Интернет, и при измерении с помощью DNS результат был положительным.

Результаты, безусловно, интересны. Измерение только с помощью DNS более показательно, поскольку мы видим, что DNS работает через делегирование без «склеивания» более надёжным образом. Однако есть сети, в которых происходит блокировка резолвинга доменных имён при отсутствии «склеивающих» записей (в основном в Северной Африке), и эта блокировка затрагивает около 3% от общего числа пользователей.

Таким образом, мы видим, что около 75% пользователей могут использовать DNS через IPv6.

Примечание

Приведённые выше взгляды не обязательно отражают точку зрения Азиатско-Тихоокеанского сетевого информационного центра.

Об авторе:

Джефф Хьюстон (Geoff Huston), AM B.Sc., M.Sc., является главным научным сотрудником Азиатско-Тихоокеанского сетевого информационного центра (APNIC), регионального интернет-регистратора, обслуживающего Азиатско-Тихоокеанский регион.

Контроль качества инфраструктуры Интернета – ICANN SLAM

Дмитрий Коваленко

Аннотация

Как ICANN контролирует стабильность Интернета в миллисекундах? Разбираем устройство системы SLAM (Service Level Agreement Monitoring) — невидимого арбитра, который непрерывно тестирует сотни доменных зон верхнего уровня через сеть из 40 глобальных пробников. Внутри статьи — технические критерии Спецификации № 10 для gTLD, особенности добровольного мониторинга для национальных доменов (ccTLD) и принципы получения данных через API (MoSAPI).

Ключевые слова:

ICANN SLAM, MosAPI, распределённая сеть мониторинга, gTLD, ccTLD, DNS, RDAP, SRS

Введение

Доменная индустрия является важной частью цифровой инфраструктуры и влияет на развитие технологий, бизнеса и общества в целом. ICANN (Internet Corporation for Assigned Name and Numbers) является ключевой некоммерческой организацией в доменной индустрии на глобальном уровне. Одной из важнейших задач в обеспечении бесперебойного функционирования доменов верхнего уровня (TLD) является контроль за соблюдением технических требований к инфраструктуре, обеспечивающей работоспособность TLD. Важными частями этой инфраструктуры являются несколько сервисов: широко известный сервис DNS и менее известные сервисы SRS и RDAP. В частности, при регистрации домена второго уровня регистратор отправляет команду по протоколу EPP в систему регистрации доменов (SRS) реестра TLD. Впоследствии информация о домене из реестра попадает в DNS — домен делегируется на соответствующие серверы имён, а данные о владельце домена становятся доступны через RDAP, являющимся преемником устаревшего протокола WHOIS. Главным инструментом контроля работы основных сервисов TLD выступает система SLAM (Service Level Agreement Monitoring) [1].

В этой статье мы разберём, как устроена система SLAM, из каких географических точек планеты производятся замеры и как эту систему можно использовать для мониторинга сервисов национальных доменов верхнего уровня (ccTLD).

Зачем ICANN контролирует регистратуры TLD

Когда ICANN делегирует новую доменную зону верхнего уровня (например, .tech, .online или .tatar), она подписывает с регистратурой — организацией, которая отвечает за функционирование TLD — базовое соглашение (Base gTLD Registry

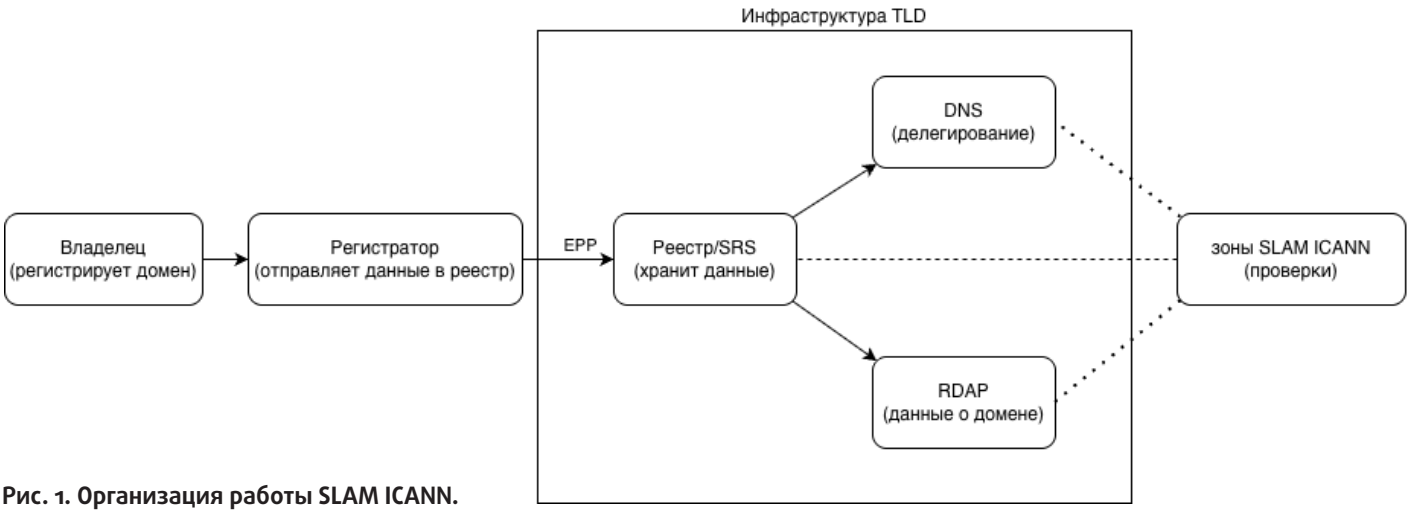

Рис. 1. Организация работы SLAM ICANN.

Agreement). В Спецификации № 10 (Specification 10) этого соглашения прописаны требования к качеству, доступности и скорости работы критически важных сервисов. Система SLAM создана именно для того, чтобы проверять, выполняют ли регистратуры эти обязательства.

При этом важно понимать, что зона юридической ответственности разделена в зависимости от типа регистратуры.

- Регистратуры gTLD (такие как .shop, .tech, .moscow) связаны с ICANN договорами. Они обязаны строго соблюдать все параметры Спецификации № 10, иначе рискуют потерять право на управление зоной.

- Регистратуры исторических gTLD (legacy gTLDs — таких как .com, .net или .org) имеют свои индивидуальные контракты с ICANN, в которые изначально не входила Спецификация № 10. Однако в процессе продления договоров ICANN планомерно унифицирует технические требования, например, на базовое соглашение перешли .org, .info и .biz. Исключение составляют лишь домены верхнего уровня .gov, .edu, .mil, которые регулируются отдельными внутренними регламентами США.

- Регистратуры страновых доменов ccTLD (такие как .uk, .de, .jp или .ru) находятся в совершенно иных условиях. Они представляют собой национальные структуры, работают по национальным правилам и не подпадают под прямое административное регулирование со стороны ICANN. Соответственно, они не обязаны выполнять требования Спецификации № 10. Тем не менее, ccTLD могут добровольно подключаться к системе SLAM, чтобы использовать её инструменты для анализа собственных сервисов.

Что именно измеряет SLAM: критерии Спецификации № 10

В Спецификации № 10 описаны проверки конкретных технических параметров по трём главным китам доменной инфраструктуры: DNS, RDDS/RDAP и SRS/EPP. Но в настоящее время мониторинг проводится только для служб DNS и RDDS/RDAP, а для SRS/EPP не проводится [2]. Замеры контролируют две ключевые метрики: доступность (availability) — процент времени стабильной работы — и время ответа (Round-Trip Time, RTT) — скорость реакции сервиса. Если показатели падают ниже требуемых значений, SLAM автоматически открывает инцидент.

Критерии проверки DNS

- Доступность DNS-сервиса: 100% (0 минут простоя в месяц). Сервис считается доступным, если в конкретный момент времени хотя бы два делегированных DNS-сервера из всех прописанных для зоны IP-адресов успешно отвечают на запросы зондов SLAM. Это самый критичный компонент инфраструктуры. Сбой в доступности DNS-сервиса означает, что домены в зоне по истечении TTL закешированных записей станут недоступны по всему миру. Поэтому здесь самое строгое требование к доступности, и падение сервиса — это триггер для немедленного вмешательства ICANN.

- Валидация DNSSEC: SLAM проверяет корректность цепочки доверия и правильность отдачи DNSSEC-записей. Любая техническая ошибка в подписях зон приравнивается к падению DNS.

- Доступность конкретного DNS-сервера: ≥ 99% (допускается не более 432 минут простоя в месяц для каждого отдельного IP-адреса). SLAM индивидуально проверяет каждый зарегистрированный IPv4- и IPv6-адрес каждого DNS-сервера зоны. Здесь требования мягче, что позволяет проводить техническое обслуживание инфраструктуры отдельных DNS-серверов без инцидентов в SLAM.

- Время ответа (RTT) для UDP: ≤ 500 мс для не менее 95% запросов. Тестовые пакеты DNS из сети зондов SLAM должны получить ответы по протоколу UDP от DNS-сервера быстрее, чем за полсекунды, а 5% ответов, превышающих порог, SLAM проигнорирует при подсчёте.

- Время ответа (RTT) для TCP: ≤ 1500 мс для не менее 95% запросов. Для тестовых пакетов DNS из сети зондов SLAM по протоколу TCP порог выше, так как необходимо дополнительное время для установки TCP-сессии.

- Время обновления DNS: ≤ 60 минут для не менее 95% зондов. Эта метрика считает время с момента, когда регистратор получил от системы регистрации (SRS) подтверждение об изменении данных по домену (например, смена NS-записей или добавление новых), до момента, когда зонды SLAM начнут получать от DNS-серверов новые данные. По сути, это жёсткий лимит на генерацию и дистрибуцию файлов доменной зоны, но на момент написания статьи эта метрика не контролировалась SLAM.

Критерии проверки RDDS/RDAP

- Доступность RDDS-сервиса: 98% (допускается не более 864 минут простоя в месяц). Сервисы WHOIS, классический — Port 43 и Web-WHOIS, предоставляющие информацию о владельцах доменов. Хотя они напрямую не влияют на открытие сайтов, ICANN считает их критически важными для безопасности и борьбы с фишингом.

- Время ответа RDDS (RTT): ≤ 2000 мс для не менее 95% запросов. Для запроса, отправленного на конкретный IP-адрес одного из серверов одной из служб RDDS, считается время от момента начала TCP-соединения и до его завершения. В зависимости от выбранной службы анализируется либо ответ WHOIS (для Port 43), либо HTTP-ответ (для Web-WHOIS).

- Время обновления RDDS: ≤ 60 минут для не менее 95% зондов. Эта метрика считает время с момента, когда регистратор получил от системы регистрации (SRS) подтверждение об изменении данных по домену (например, смена контакта), до момента, когда зонды SLAM начинают получать от RDDS-серверов новые данные. По сути, это лимит на синхронизацию данных между базой данных реестра и

её внешними публичными сервисами RDDS, но на момент написания статьи эта метрика не контролировалась SLAM.

С января 2025 года RDAP стал основным источником информации о регистрации доменных имен в gTLD, и ICANN перешла к полноценному контролю RDAP через систему SLAM. С этого момента проблемы с RDAP подлежат таким же процедурам эскалации, как и у старого протокола WHOIS [3]:

- доступность RDAP-сервиса: 98% (допускается не более 864 минут простоя в месяц);
- время ответа (RTT) для RDAP: ≤ 2000 мс для не менее 95% запросов. Для этой проверки появляется обязательное требование – использование протокола HTTPS;
- время обновления RDAP: ≤ 60 минут для не менее 95% зондов.

Критерии проверки SRS

- Доступность EPP-сервиса: 98% (допускается не более 864 минут простоя в месяц). Служба считается доступной, если зонды SLAM успешно устанавливают TCP-соединения со службой и получают корректные ответы на базовые команды. SRS/EPP — важная часть распределённой системы регистрации, через которую аккредитованные регистраторы отправляют XML-команды по протоколу EPP на регистрацию, продление или изменение доменов. Сбои этой системы не ломают текущий DNS, но полностью парализуют продажи и управление доменами.

SLAM разделяет команды EPP на три категории по уровню нагрузки и замеряет их RTT раздельно:

- команды EPP-сессии (RTT): ≤ 2000 мс для не менее 95% транзакций. Сюда входят служебные команды управления сессией: <login> (авторизация) и <logout> (завершение сессии). Зонды имитируют реальное поведение регистратора: устанавливают защищённое TLS-соединение, проходят авторизацию, выполняют серию тестовых запросов/изменений и корректно закрывают сессию. Если на этапе «рукопожатия» или логина происходят задержки — это сразу отразится на данной метрике;
- EPP-команды чтения (RTT): ≤ 2000 мс для не менее 95% транзакций. К этой категории относятся команды чтения данных, такие как <check> (проверить доступность домена) и <info> (получить данные объекта);
- EPP-команды записи (RTT): ≤ 4000 мс для не менее 95% транзакций. Это команды, которые меняют состояние базы данных реестра: <create> (регистрация), <update> (обновление данных), <delete> (удаление) и <renew> (продление).

Задекларировано, что метрики времени ответа для EPP-команд чтения и записи выполняются только над реально существующими в реестре объектами и учитывают интервал между отправкой одной команды и получением ответа на неё. Накладные расходы, такие как открытие/закрытие TCP- и EPP-сессий, из этих замеров исключены, но на момент написания статьи эти метрики SRS/EPP не контролировались SLAM.



Рис. 2. География размещения зондов ICANN.

При взгляде на метрики RTT невольно появляется вопрос, почему используются такие высокие пороги. Для сетевого инженера задержка в 500 миллисекунд на DNS-ответ кажется огромной, ведь в пределах одной небольшой страны или города DNS-сервер отвечает за 2—10 мс. Ответ на этот вопрос раскрою в следующем разделе.

Географическая архитектура SLAM: глобальная сеть зондов

Чтобы круглосуточно контролировать «пульс» инфраструктуры доменов верхнего уровня, ICANN развернула глобальную сеть из 40 измерительных зондов, охватывающих все регионы. Списки IP-адресов этих зондов периодически обновляются и доступны регистратурам через RRI (Registration Reporting Interfaces).

Для обеспечения максимальной объективности ICANN арендует мощности в крупнейших дата-центрах мировых магистральных провайдеров и облачных гигантов. Зонды не сконцентрированы в одной локации, а буквально «опоясывают» земной шар.

География SLAM заставляет ICANN закладывать огромный буфер на физические ограничения сети:

- скорость света в оптоволокне конечна: запрос от зонда из Австралии или Южной Африки до узла в Европе, проходя через трансокеанские подводные кабели и десятки стыков, в идеальных условиях тратит 150—250 мс только на путь туда и обратно;
- магистральный Интернет постоянно «дышит»: перестроение таблиц маршрутизации и временные перегрузки на стыках операторов связи могут поднять RTT.

Высокие пороги гарантируют, что SLAM зафиксирует реальную деградацию важных инфраструктурных сервисов, а не зафиксирует нарушение SLA из-за того, что где-то посреди Атлантического океана оператор связи перенаправил трафик по резервному маршруту. Кроме этого, зонды не размещают за каналами связи с большой задержкой распространения сигнала, такими как спутниковые каналы.

Как SLAM проверяет аварии: правило консенсуса 51%

Система SLAM спроектирована так, чтобы исключить ложные срабатывания, вызванные проблемами с Интернетом у самого измерительного зонда. Система работает по следующему алгоритму консенсуса:

- цикл проверок: тесты запускаются каждую минуту для DNS и каждые пять минут — для RDDS/RDAP;
- консенсус (51%): чтобы зафиксировать сбой службы (например, падение DNS), система должна получить подтверждение как минимум от 51% всех активных зондов в рамках цикла проверки. Если только один зонд в Лондоне не получает ответа от сервера, а остальные 39 успешно получают ответы — инцидент не откроется, проблема признается локальной для сети этого зонда;
- правило нескольких циклов: инцидент в SLAM откроется только тогда, когда сбой, подтверждённый 51% зондов, держится три цикла подряд для DNS и два цикла — для RDDS/RDAP, и закроется, если восстановление подтверждено аналогичным образом. Такая логика делает SLAM надёжным арбитром: если была зафиксирована авария, значит, у регистратуры действительно начались серьёзные проблемы на инфраструктуре.

Что происходит при нарушении SLA: механизм эскалации и запуск EBERO

Система SLAM это не просто пассивный счётчик миллисекунд. Как только фиксируется, что показатели доступности или времени ответа вышли за рамки Спецификации № 10, ICANN запускает регламентированный процесс. В зависимости от характера сбоя события развиваются по двум сценариям: юридическому (Compliance Escalation) или экстренному техническому (программа Emergency Back-end Registry Operator — EBERO), где бюрократические процедуры откладываются.

Сценарий 1. Юридический

Этот путь активируется, если регистратура систематически нарушает взятые на себя обязательства. За дело берётся департамент ICANN Contractual Compliance, который осуществляет проактивный мониторинг для обеспечения соблюдения договорными сторонами условий соглашений и публикует отчёты о своей работе на ежемесячной основе [4], касательно регистратуры этот сценарий можно структурировать следующим образом:

- запрос разъяснений (Inquiry Notice): регистратуре высылается запрос, на который она обязана оперативно отреагировать, объяснить причины деградации критического сервиса и отчитаться о принятых мерах. Здесь может быть несколько итераций, в зависимости от качества ответов регистратуры;
- уведомление о нарушении (Notice of Breach): если сбои повторяются или регистратура не может исправить ситуацию, ICANN выносит официальное предупреждение. С этого момента регистратуре даётся ограниченный временной лимит на исправление проблем. Статус этих уведомлений является публичным. С текущим списком можно ознакомиться на сайте ICANN [5];
- расторжение контракта (Termination): ICANN запускает процесс расторжения контракта (Termination by ICANN), на завершающем этапе этого процесса ICANN официально уведомляет о расторжении контракта, тем самым аннулируя права регистратуры на gTLD.

Сценарий 2. Экстренное спасение — EBERO

Если инфраструктурный сбой носит необратимый характер и влияет на работу владельцев доменов в этом gTLD, например, технический бэкенд-оператор расторг контракт с регистратурой и отключил критические сервисы, отвечающие за gTLD, как это было с gTLD .nowruz, то ICANN официально инициирует экстренную процедуру спасения gTLD.

Как это работает: ICANN имеет долгосрочные контракты с опытными бэкенд-операторами (такими как CIRA, Nominet и CNNIC), которые действуют в соответствии с детально проработанной процедурой реагирования на чрезвычайные ситуации, называемой «Общий порядок перехода» (Common Transition Process — CTP).

Час «X»: если регистратура не может обеспечить работу критически важных сервисов, управление зоной в принудительном порядке переключается на одного из операторов EBERO.

Что спасают: перехватив управление, EBERO поднимает пять критических сервисов: DNS, DNSSEC, WHOIS/RDAP, SRS/EPP и выгрузку данных реестра в Escrow.

Что не спасают: бэкенд-оператор EBERO не предоставляет никаких дополнительных услуг, которые регистратура gTLD могла предоставлять своим пользователям, например, услуги хостинга.

Реальные прецеденты уже были; например, в 2024 году из-за критических проблем с WHOIS/RDAP под экстренное управление EBERO были принудительно переведены gTLD .nowruz, .pars, .shia, .tci и .xn--mgbt3dhd, за которые отвечала регистратура AGIT. В декабре 2024 ICANN расторгла с AGIT контракты на поддержку этих gTLD [6]. На текущий момент число gTLD, которые поддерживаются по программе EBERO, равно семи. Все эти домены поддерживаются бэкенд-оператором Nominet [7] и ждут своей дальнейшей участи.

Как устроен сбор данных: Архитектура MoSAPI

Все метрики, которые собирает распределённая сеть зондов SLAM, не остаются вещью в себе. ICANN предоставляет регистраторам gTLD, аккредитованным регистраторам и участвующим регистратурам ccTLD доступ к специальному программному интерфейсу — MoSAPI (Monitoring System API). Это защищённый REST API, работающий по протоколу HTTPS. Взаимодействие с MoSAPI подчиняется нескольким правилам:

- на транспортном уровне: поддерживается только протокол TLS версии 1.3, а также осуществляется фильтрация по IP;
- на сессионном уровне: для одного аккаунта разрешена только одна активная сессия, срок действия сессии не более 15 минут, кроме этого, разрешено открывать только одну сессию на один аккаунт не чаще чем раз в 5 минут, и новая сессия автоматически закроет старую.

Ключевые возможности

Через запросы к API можно собирать следующие сущности:

- текущий статус сервисов: общий статус сервисов (DNS, DNSSEC, RDDS, RDAP) по домену верхнего уровня;
- статус оповещений: информация о том, есть ли в данный момент предупреждение по какому-либо сервису;
- счётчик downtime: возвращает общее количество минут простоя сервиса за скользящую неделю (rolling week), что позволяет видеть, насколько близко сервис подошёл к критической отметке;
- логи инцидентов: полная выгрузка истории открытых и закрытых инцидентов по конкретной службе;
- логи измерений: детализация конкретных тестов, привязанная к временным меткам;
- сетевая диагностика: детализация сетевой связности для исследования сетевых инцидентов — когда зонд фиксирует ошибку подключения к anycast IP-адресу, то с помощью сохранённой диагностики утилиты MTR можно понять, на каком участке сети произошёл сбой.

Для технических специалистов работа системы SLAM приносит несколько ключевых особенностей:

- прозрачность: благодаря интерфейсу MoSAPI ICANN предоставляет сторонний взгляд на ключевую инфраструктуру TLD. Выгрузка сырых логов из распределённой сети 40 глобальных зондов позволяет объективно оценить, как критически важные сервисы выглядят в глазах пользователей из Москвы, Сан-Паулу или Токио;
- необходимость локальной аналитики: ограниченное хранение исторических данных (365 дней) в MoSAPI и отсутствие интерфейса для аналитиков заставляют строить собственные отказоустойчивые системы сбора и визуализации данных, которые позволяют сохранять многолетнюю историю системы SLAM для глубокого ретроспективного анализа.

Интерфейс MoSAPI не является статичным, с момента выпуска первой публичной версии 2.5 в 2017 году спецификация прошла через более чем 15 крупных итераций и дополнений. А внедрение тестового полигона на базе домена .test для отладки создаваемых интеграций информационных систем регистратур с MoSAPI говорит о высокой востребованности интерфейса.

Заключение

Система мониторинга ICANN SLAM — это важный элемент обеспечения стабильности современного Интернета. С её помощью ICANN поддерживает стабильность, предсказуемость и безопасность работы глобальной адресной системы для миллионов пользователей по всему миру. Для доменной индустрии существование такой независимой системы мониторинга даёт несколько важных преимуществ:

- глобальный стандарт качества;
- прозрачность взаимодействия;
- приоритет интересов пользователей.

SLAM демонстрирует, как автоматизированный аудит и чёткие правила игры помогают координировать сложнейшую распределённую инфраструктуру и сохранять Интернет единым и связанным пространством.

Для регистратуры ccTLD лучшей практикой для контроля инфраструктуры является гибридный подход:

- использование внешнего мониторинга ICANN SLAM через добровольное подключение позволяет получать объективный трансграничный взгляд на доступность важных сервисов ccTLD;
- развёртывание собственной распределённой системы мониторинга, спроектированной и построенной с учётом лучшего международного опыта эксплуатации критических систем. Собственная сеть измерительных зондов позволяет контролировать внутреннюю связность, гибко настраивать уведомления под локальную специфику и повышать суверенитет и отказоустойчивость национальной доменной зоны в любых условиях.

Глоссарий:

DNS (Domain Name System) — система доменных имён.

DNSSEC (Domain Name System Security Extensions) — набор расширений к протоколу DNS, который повышает его безопасность за счёт криптографической проверки подлинности и целостности данных, передаваемых через систему доменных имён.

EBERO (Emergency Back-end Registry Operator) — комплекс мер по поддержке работоспособности доменов в случаях нарушения регистратором правил функционирования в соответствии с контрактом ICANN.

Escrow — депозит данных реестра TLD.

gTLD (generic Top-Level Domain) — общий домен верхнего уровня.

ccTLD (Country Code Top Level Domain) — страновой домен верхнего уровня.

MosAPI — Monitoring System API в ICANN.

NS-запись (Name Server) — тип ресурсной записи в системе DNS, который указывает, какие DNS-серверы являются авторитетными для конкретного домена.

REST API (Representational State Transfer Application Programming Interface) — архитектурный стиль взаимодействия между клиентом и сервером.

RDDS/RDAP (Registration Data Access Protocol) — сервис, позволяющий третьим лицам получать доступ к данным регистрации доменных имён.

RTT (Round-Trip Time, RTT) — скорость ответа сервиса.

RRI (Registration Reporting Interfaces) — набор интерфейсов, предоставляемых организацией ICANN регистратурам и аккредитованным регистраторам для предоставления необходимой отчётности.

SRS (Shared Registration System) — распределённая система регистрации доменов.

SRS/EPP (Extensible Provisioning Protocol) — протокол, который работает внутри SRS и задаёт правила обмена данными.

TTL (Time to Live) — механизм, который ограничивает время жизни данных.

WHOIS (от англ. who is — «кто это») — сетевой протокол прикладного уровня, базирующийся на протоколе TCP (порт 43). Основное применение — получение регистрационных данных о владельцах доменных имён. В настоящее время заменен на RDAP.

Список литературы:

[1] https://www.icann.org/en/system/files/files/presentation-slam-13may17-en.pdf

[2] https://www.icann.org/en/system/files/files/mosapi-specification-26may26-en.pdf, page 7

[3] https://itp.cdn.icann.org/en/files/contracted-parties-communications/escalations-sla-failures-rdap-15jan25-en.pdf

[4] https://www.icann.org/resources/pages/contractual-compliance-monthly-reports-2025-09-15-en

[5] https://www.icann.org/compliance/notices

[6] https://www.icann.org/en/contracted-parties/registry-operators/services/registry-agreement-termination-service

[7] https://nominet.uk/blog/emergency-rescue-whats-an-ebero/

Об авторе:

Дмитрий Юрьевич Коваленко, архитектор DNS-решений — начальник отдела в MSK-IX.