САН-ХУАН – Принципы работы: функционирование корневых серверов
Понедельник, 12 марта 2018 года, 10:30 – 12:00 по AST
ICANN61 | Сан-Хуан, Пуэрто-Рико

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Доброе утро! ICANN61, семинар «Принципы работы: функционирование корневых серверов», 12 марта

КАТИ ПЕТЕРСЕН (CATHY PETERSEN): Всем доброе утро. Добро пожаловать на семинар «Принципы работы». Мы немного отстаем от графика после этой замечательной церемонии открытия, поэтому, пожалуйста, будьте терпеливы. Мы скоро начнем. Спасибо.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Уважаемые! Мы приступим к работе через две-три минуты. Мы начинаем на 15 минут позже из-за затянувшейся церемонии открытия. Но если вы будете готовы начать через две-три минуты, это было бы здорово.

КАТИ ПЕТЕРСЕН: И снова доброе утро всем присутствующим. Добро пожаловать на семинар «Принципы работы». На этом заседании мы поговорим о функционировании корневых серверов. Снова благодарим вас за терпение. Первую презентацию нам представит Эндрю Макконахи. Эндрю?

ЭНДРЮ МАККОНАХИ (ANDREW MCCONACHIE): Спасибо. Здравствуйте, меня зовут Эндрю Макконахи. Я работаю в поддержке политики ICANN, в области поддержки Консультативного комитета системы корневых серверов (RSSAC). Я буду говорить о системе корневых серверов.

Во-первых, немного о повестке дня. Сегодня у нас четыре раздела: обзор системы доменных имен, современная система корневых серверов и ее особенности. Затем я передам слово своему коллеге Стиву Шенгу, который объяснит, что такое Anycast, а затем расскажет о RSSAC и некоторых последних мероприятиях RSSAC.

После этого у нас будет период вопросов и ответов, когда некоторые из находящихся здесь операторов корневых серверов ответят на ваши вопросы. Поэтому прошу приберечь ваши вопросы на самый конец.

Давайте начнем с обзора системы доменных имен и корневых серверов. Вкратце повторим: что такое IP-адреса и как они работают в качестве идентификаторов в интернете? IP-адреса являются фундаментальными идентификаторами в интернете, и все узлы подключенные к интернету должны иметь IP-адреса.

Независимо от версии IPv4 или IPv6, или при работе через NAT, вы все равно должны иметь IP-адрес. IP-адреса являются числовыми метками. Они совершенно неудобны для восприятия человеком. Это просто числа.

Зачем нам нужна система доменных имен (DNS)? Что ж, основная проблема в том, как я указал на предыдущем слайде, IP-адреса трудно запомнить и они изменяются в множестве. Поэтому первоначальной задачей DNS было просто получить легко запоминающиеся имена, которые можно сопоставить с IP-адресами, чтобы запоминать IP-адреса.

Эти задачи остаются, но также существует еще множество современных задач, таких как совместное использование IP-адресов и сопоставление нескольких IP-адресов с одним сервисом. Теперь к первоначальной проблеме сложного запоминания IP-адресов добавилась современная проблема сопоставления нескольких к одному и одного к нескольким.

Сегодня система доменных имен является иерархической. Как видно на схеме, вверху находится корневой сервер. Под ним мы имеем так называемые домены верхнего уровня или TLD. Можно привести несколько примеров, включая .edu, .mil, .uk. За тем под ними находится, как некоторые называют, второй уровень, затем третий уровень и так далее. Они имеют сопоставленные IP-адресам имена. Это то, с чем мы хорошо знакомы, но существуют и другие сопоставления, такие как записи mx для почтовых серверов, обратные записи, иногда называемые записями PTR, которые позволяют от имен перейти обратно к IP-адресам.

Этот слайд довольно объемный. Я работал над ним довольно долго. Целью этого слайда является показать процесс разрешения имен DNS, как пользователь работает с DNS, через что он проходит, различные этапы, как протекает взаимодействие с DNS, чтобы пользователь смог преобразовать доменное имя в IP-адрес и, наконец, перейти на сайт.

Пользователь находится здесь справа. Ему необходимо перейти на веб-сервер www.example.com. Первое, что он делает, открывает браузер. Это приводит к выдаче запроса DNS, и этот запрос DNS направляется к так называемому рекурсивному серверу имен. Предположим, что в кэше рекурсивного сервера имен ничего нет, и для примера предположим, что этот рекурсивный сервер имен только что включили, его кэш пуст и ему ничего не известно. Что он делает?

Он просто получил запрос на www.example.com. Ему потребуется выполнить массу работы перед тем как он сможет ответить пользователю. Первое что он делает, это дает запрос корневому серверу и спрашивает, «Где www.example.com. Где он?» Корневой сервер отвечает, «Я не знаю, где находится это все целиком, но я знаю, где находится .com.» Поэтому он возвращает рекурсивному серверу имен адрес DNS-серверов .com.

Затем рекурсивный сервер имен отправляется к DNS-серверам .com и спрашивает, «Где находится www.example.com?» DNS-сервер .com отвечает, «Я не знаю, где находится это все целиком, но я знаю, где находится DNS-сервер example.com. Он здесь.»

Затем рекурсивный сервер имен отправляется к DNS-серверам example.com и спрашивает, «Где находится www.example.com?» Наконец, он получает в ответ то что искал и теперь рекурсивный сервер имен в состоянии сообщить пользователю адрес www.example.com.

Вот как пользователь проходит все этапы разрешения этого доменного имени в IP-адрес и, наконец, получает возможность посетить этот сайт.

На этом слайде я еще не говорил о другом аспекте, таком как безопасность. Это DNSSEC или аспект безопасности DNS, как его иногда называют, который присутствует в каждым из этих вопросов между рекурсивным сервером имен и каждым из этих полномочных DNS-серверов – корневой сервер имен, DNS-сервер .com и DNS-сервер example.com – ответы, которые поступают обратно в рекурсивный сервер имен от этих полномочных серверов, подписаны, и рекурсивный сервер имен способен проверить правильность ответа. Что этот ответ не был подделан. Что он не был предоставлен неверным полномочным DNS-сервером. Это правильный ответ, и это стало возможным благодаря DNSSEC.

Таков процесс разрешения системы доменных имен. Как видно из предыдущего слайда, корневым серверам известно только кого необходимо спросить следующим. У них имеются только адреса таких серверов имен доменов верхнего уровня, как .com, .net и .org. Однако, как правило, у них нечасто спрашивают это.

В предыдущем приведенном мной примере имелась гипотетическая ситуация, когда рекурсивный сервер имен был только что включен и его кэш был пуст. На самом деле, это случается очень редко. Рекурсивные сервера имен характеризуются весьма интенсивным кэшированием, и ответы на огромное большинство запросов к рекурсивным сервера имен поступают из кэша. Это означает, что к корню поступает намного меньше запросов, чем можно сначала предположить.

Современные DNS имеют некоторые усовершенствования. Я уже говорил о DNSSEC, иногда говорят DNS безопасность или расширения безопасности. Смысл DNSSEC заключается в добавлении подписи к ответам, поступающим в рекурсивные сервера имен, чтобы рекурсивный сервер имен мог проверить их подлинность. Под проверкой подлинности я подразумеваю, что он может убедиться в правильности ответа, поскольку он был подписан криптографическим ключом, поэтому ответ является правильным.

Также была повышена защита персональных данных и Инженерная проектная группа Интернета все еще продолжает серьезную работу в этом направлении. Что-то наподобие безопасности DNS поверх транспортного уровня, для защиты передачи запроса по проводу, гарантирующей недоступность для посторонних глаз. Это все еще находится в состоянии активной разработки.

Другим современным усовершенствованием DNS является метод Anycast. Метод Anycast активно используется операторами корневых серверов. В основном, Anycast выполняет две важных функции. Он позволяет нескольким серверам совместно использовать один IP-адрес и защищает от атак DDoS. Мой коллега Стив Шенг позже более подробно расскажет об Anycast и как он работает.

Корневая зона в сравнении с корневыми серверами. Корневая зона это данные, которые предоставляет корневой сервер. Можно рассматривать корневую зону как отправную точку. Это перечень TLD и DNS-серверов. Это вершина иерархии или древовидной структуры. Управление осуществляет ICANN на основании политики сообщества. Составление и рассылку всем операторам корневых серверов осуществляет специалист по обслуживанию корневой зоны. Повторю, это содержание базы данных операторов корневых серверов. Это данные, которые обслуживают корневые серверы.

С другой стороны, в ответе корневых серверов содержатся данные из корневой зоны. В настоящее время имеется 13 идентификаторов и свыше 900 зеркал во множестве различных физических местоположений по всему миру. Корневые сервера играют чисто техническую роль. Они обслуживают данные корневой зоны. Каждое из этих облаков Anycast, работу которых обеспечивают операторы корневых серверов, является их собственной ответственностью.

Рассмотрим немного подробнее работу оператора корневого сервера. Существует 12 различных групп профессиональных инженеров, которые сосредоточены на надежности и стабильности сервиса, доступности для всех интернет-пользователей. Они являются профессионалами и они сотрудничают друг с другом, а также работают независимо. Это группа различных организаций. Под этим я подразумеваю, что они технически, организационно и географически различны.

Однако операторы не вовлечены в формирование политики и они не участвуют в модификации данных. Они просто обслуживают данные корневой зоны. Они обеспечивают надежную работу сервиса, обслуживают эти данные и оценивают и внедряют новые технические модификации – те новые стандарты, которые могут поступать от Инженерной проектной группы Интернета – обеспечивают поддержание устойчивого, надежного и доступного всем пользователям интернета как сервиса.

Таковы вкратце основы DNS, немного технические, но, возможно, не слишком технические. Теперь давайте перейдем к современной системе корневых серверов и некоторым ее особенностям.

Рост системы корневых серверов. На этом слайде показана краткая история роста численности корневых серверов, идентификаторов корневых серверов за последние годы, начиная с 1980-х годов. Можно видеть определенный прогресс.

Сейчас, начиная с 1998 года имеется 13 различных идентификаторов. Эти изменения главным образом произошли в ответ на технические требования, а также в связи с проблемами масштабирования. Сегодня проблемы масштабирования фактически решены посредством Anycast. Anycast это просто замечательный инструмент в инструментарии операторов корневых серверов для решения проблем масштабирования.

Сегодня все корневые сервера работают с IPv6 и IPv4, поэтому имеется 13 пар адресов IPv4 и IPv6. Повторю, что имеется более 900 отдельных зеркал.

Существует ряд фундаментальных принципов системы корневых серверов. Их пять. Важно, чтобы эта система корневых серверов обеспечивала устойчивую, надежную и гибкую платформу для DNS, чтобы она работала для общего блага всего интернета, чтобы IANA являлась источником данных корневых DNS – этих данных корневой зоны, и чтобы архитектурные изменения делались на основании результатов технической оценки и обоснованных технических потребностей, и что техническая деятельность и ожидания DNS определялись Инженерной проектной группой интернета.

Если вас заинтересует более подробная история системы корневых серверов, можно загрузить и прочитать RSSAC023, историю системы корневых серверов, с сайта RSSAC.

Это современные операторы корневых серверов. Как видно, существует 13 идентификаторов. Их имена узлов перечислены слева. В средней колонке показаны IP-адреса. Как IPv4, так и IPv6 для всех из них. Каждый из этих IPv4 и IPv6 адресов, а также, как минимум IPv4 адреса, размещены в облаке Anycast. Поэтому за этими IP-адресами находится много, много серверов – свыше 900 на данный момент, но их число растет все время. На последней конференции ICANN, когда я проводил эту презентацию, я говорил, что имеется 800 зеркал, а сейчас я говорю, что здесь свыше 900 зеркал. Так что в наличии постоянный рост.

Существует много точек зрения на современные корневые сервера. Это с сайта root-servers.org. Это просто обзор где расположены корневые сервера. Он не является особенно точным. Он не укажет, например, где точно находятся семь зеркал корневого сервера в Мадагаскаре. Это графическое представление. Это может быть интересным. Можно углубиться в подробности, если зайти на сайт. Даже можно увидеть конкретные города, где находятся зеркала каждого из операторов. Это очень широкий и общий обзор, но если зайти на сайт, можно действительно углубиться в детали и получить некоторую интересную информацию об этом.

Это схема управления корневой зоной. Это то, как данные корневой зоны, корневая зона, попадает на корневые сервера. Давайте предположим, что вы оператор TLD и вам необходимо сделать изменения в корневой зоне. Возможно, изменить ваши записи NS. Возможно, изменить ваши связующие записи. Вам необходимо изменить некоторую информацию, связанную с некоторыми записями в вашем TLD.

Итак, вы идете в IANA и делаете изменение, а затем это изменение будет передано специалисту по обслуживанию корневой зоны, которым в настоящее время является Verisign. Затем, я полагаю, дважды в день они будут рассылать это изменение, они будут рассылать корневую зону целиком операторам корневых серверов. Затем операторы корневых серверов отвечают за то, чтобы это изменение поступило во все их облако Anycast и затем обслуживало или отвечало на запросы, приходящие от всех рекурсивных сопоставителей.

Она из особенностей операторов корневых серверов: имеется разнообразие организационной структуры, история их деятельности иногда различна, они используют различное аппаратное и программное обеспечение. Они используют разные аппаратные платформы, а также разные программные платформы. Это помогает в смысле безопасности благодаря сильной корреляции между лучшей безопасностью и повышенным разнообразием. Они также имеют различного типа модели финансирования. Это организации различного типа и они получают финансирование различными путями.

Они, однако, совместно используют передовые методы работы: сильную физическую безопасность, они с избытком резервируют свою производительность для борьбы с атаками DDoS, а также чтобы справляться с пиковым трафиком, и они все имеют профессиональные и доверенные кадры.

Они сотрудничают посредством различных отраслевых мероприятий в сообществе. ICANN является одной из них, а также Инженерная проектная группа интернета, NOG, такие как NANOG или RIPE, DNS-OARC, которые являются операционными и исследовательскими группами. Они также используют основанные на интернете инструменты сотрудничества, и их деятельность является транспарентной.

Они также координируют подготовку к внештатным ситуациям, чтобы защитить инфраструктуру в случае катастрофических или другого рода аварийных ситуаций. Они проводят периодические мероприятия для поддержке мероприятий по ликвидации аварийных ситуаций. Я не могу прочитать этот последний пункт, поскольку он обрезан.

Реакция на развитие интернета. По мере развития интернета, в систему DNS вводятся новые требования. Со временем операторы корневых серверов должны принять IPv6, Anycast, DNSSEC. IDN здесь упомянуты также потому, что множество IDN находятся в корневой зоне. Важно повысить надежность, время реагирования и отказоустойчивость. Повторю, что имеется более 900 зеркало Anycast.

Некоторые мифы, которые могут существовать, некоторые ошибочные толкования в отношении системы корневых серверов. Миф первый, корневые сервера управляют направлением сетевого трафика. Это совершенно не так. Фактически это совсем и полностью не так, поскольку это миф. На самом деле направление сетевого трафика определяют маршрутизаторы. Я считаю, что этот миф появился вследствие того, что DNS сопоставляет имена с IP-адресами, но в конечном итоге это маршрутизаторы на основании IP-адресов определяют куда идет пакет.

Другой миф в том, что большинство запросов DNS обрабатывает корневой сервер. Как видно из примера, это может быть так, если кэш рекурсивного сервера DNS пуст, но это так очень редко. Поэтому большинство серверов DNS не обслуживаются корневым сервером. Большинство из них обслуживается кэшем рекурсивного сервера.

Что администрация корневой зоны и предоставление услуги это одно и тоже является еще одним мифом. Это не так. На схеме, которую думаю я показывал ранее, по поводу разделения обязанностей и как изменение проходит по своему пути от корневых серверов, видно, что здесь задействованы разные стороны.

Другой миф заключается в том, что идентификаторы корневых серверов имеют специальное значение. На самом деле, нет. Или, что имеется только 13 корневых серверов. Из свыше 900.

Другой миф о том, что операторы корневых серверов осуществляют деятельность независимо. Хотя они являются независимыми организациями, они тесно координируют деятельность и сотрудничают чтобы обеспечить стабильное обслуживание системы корневых серверов в целом.

Последний миф состоит в том, что операторы корневых серверов получают только часть запроса TLD, что ж, это на самом деле не так. Они получают весь запрос целиком. Просто именно так работает DNS. В инженерной проектной группе интернета ведется работа, чтобы это изменить. Если интересно, ключевым словом здесь является минимизация QNAME и можно прочитать об этой работе, чтобы корневые сервера могли получать только верхнюю часть запроса.

Теперь я передаю слово моему коллеге Стиву Шенгу, который ознакомит с последними двумя разделами, начиная с Anycast.

СТИВ ШЕНГ (STEVE SHENG): Спасибо, Эндрю. Меня зовут Стив Шенг. Я тоже работаю в отделе оказания помощи при формировании политики RSSAC. Я объясню, что такое Anycast, а также расскажу о RSSAC и ее мероприятиях.

Anycast является термином маршрутизации и адресации. Существует два термина: Unicast и Anycast. Здесь содержатся важные различия. В Unicast пакеты или датаграммы от источников все направляются в одно место назначения и одно зеркало обслуживает все источники. Поэтому в случае атаки отказа в обслуживании весь трафик атаки идет в направлении единственного зеркала. Это Unicast.

В свою очередь, в Anycast множество зеркал предоставляют одни данные всем источникам. Это множество зеркал имеет один IP-адрес, и промежуточные политики маршрутизации определяют место назначения на основании источника. Это значит, что источник получает данные быстрее, место назначения находится ближе, и трафик атаки DDoS направляется к ближайшему зеркалу.

Позвольте показать это на схеме. Вот иллюстрация Unicast, показаны обозначения источника и места назначения. Место назначения является единственным зеркалом, и трафик направляется по кратчайшему маршруту к единственному месту назначения.

Здесь, в Anycast, показаны три места назначения синим цветом. Все эти места назначения представлены одним IP-адресом и политики маршрутизации определяют самое ближнее, от этого источника к месту назначения. Это значит, что путь от источника к месту назначения является кратчайшим и данные доставляются быстро.

Как это помогает при атаках типа отказа в обслуживании? Во время атаки типа «отказ в обслуживании», злоумышленник атакует место назначения. Но поскольку это Anycast, трафик следует только к ближайшей ссылке. Из этого следует, что, возможно, одна из ссылок на место назначение является перегруженной, но другие места назначения продолжают обслуживать трафик.

Одним из вопросов, полученных нами на этих семинарах, касается системы корневых серверов и ваших сетей. Некоторые из вас являются сетевыми операторами, некоторые, возможно, операторами рекурсивных зеркал. Если вы сетевой оператор, вы захотите иметь поблизости три или четыре зеркала. Это приблизит зеркала к вам и в некоторых зеркалах поможет снизить время циклического прохождения пакета.

Полагаю, дополнительно, вы также захотите увеличить свои пиринговые соединения и пиринговые взаимодействия. Иногда вблизи от вас находится корневое зеркало, но трафик продолжает, чтобы достичь вас, обходить половину земного шара. Причиной являются пиринговые соединения и пиринговые взаимодействия. Это также важный фактор.

Если вы являетесь оператором рекурсивного сопоставителя, чтобы увеличить кэш, необходимо подумать о внедрении технологии RFC7706. Она заключается в создании копии корневой зоны с адресом обратной связи. Выгода в том, что иногда это снижает опасность доступности для посторонних глаз конфиденциальных данных, идущих от рекурсивного сопоставителя к корневому серверу.

Очевидна важность включения проверки подлинности DNSSEC в сопоставителях. Это обеспечит невозможность получения сфальсифицированных данных IANA, как сказал Эндрю, вместе с верными данными.

И наконец, я считаю, поскольку мы в ICANN, мы пригласим группу технических и других экспертов для участия и содействия в группу подготовки RSSAC. Именно в ней разрабатываются и создаются технические рекомендации RSSAC.

Теперь, позвольте мне сделать краткий анонс или обзор RSSAC и последних мероприятий RSSAC. RSSAC это Консультативный комитет системы корневых серверов. Согласно уставу он дает сообществу и Правлению ICANN рекомендации в отношении работы, безопасности и целостности системы корневых серверов интернета и управления ею. Обратите внимание, это весьма небольшой объем работ для этого консультативный комитет.

Одно важное отличие часто смешивают, особенно в ICANN, что RSSAC это комитет, который дает рекомендации в первую очередь правлению, но также другим членам и организациям ICANN, вовлеченным в общую работу DNS.

Тем не менее, операторы корневых серверов представлены в RSSAC. Но очень важно отметить, что сам RSSAC не вмешивается в оперативные вопросы. Поэтому, я считаю, это очень важное различие, не следует смешивать эти две сущности.

В общей структуре управления ICANN это один из четырех консультативных комитетов, и он находится здесь, в экосистеме ICANN.

Внутри организации RSSAC состоит из назначенных представителей или операторов корневых серверов, и каждый из них может назначить заместителя представителя в RSSAC. Он также имеет представителей среди партнеров управления корневой зоной и ключевых технических организаций.

Группа подготовки RSSAC, о которой я упоминал ранее, является органом волонтеров, состоящим из экспертов в предметной области. Ее члены утверждаются RSSAC на основании выражения заинтересованности.

Текущими председателями RSSAC являются Брэд из Verisign и Трипти из Мадридского университета. Брэд и Трипти, вы в зале? Поднимите руку. Это Брэд. Я знаю Трипти, но она просто отошла на минутку.

В RSSAC имеется несколько представителей. Один из представителей от оператора функций IANA, специалист по обслуживанию корневой зоны. Эндрю показывал эту схему, порядок управления корневой зоной, вот IANA и специалист по обслуживанию корневой зоны. Они являются здесь двумя критически важными сущностями.

RSSAC также имеет представителя Совета по архитектуре интернета. Это обеспечивает архитектурные рекомендации ISOC и IETF по архитектурным вопросам интернета.

Внутри ICANN, RSSAC имеет представителей в Консультативном комитете по безопасности и стабильности, правлении ICANN, Номинационном комитете, Постоянном комитете потребителей, который является комитетом, призванным наблюдать за выполнением функции IANA, в настоящее время выполняемой PTI.

И, наконец, Комитет по анализу изменений корневой зоны, это комитет, созданный как часть передача координирующей роли IANA, чтобы наблюдать за архитектурными вопросами для развития корневой зоны.

Группа подготовки RSSAC в настоящее время имеет 88 технических экспертов. Их выражения заинтересованности опубликованы. Во всех публикациях RSSAC по любому из членов группы подготовки, участвующих или руководящих этой работой, их подтверждение находится в конце каждого отчета. Существует общественное доверие к индивидуальной работе.

Они публикуют различные важные рекомендации. И группа подготовки является транспарентной для тех, кто выполняет эту работу. Лист рассылки открыт, поэтому вы можете просмотреть архивы. Здесь также находятся концепции, определяющие ход работ.

Если вы заинтересованы присоединится к Группа подготовки RSSAC, направьте электронное письмо с заявкой на адрес rssac-membership@icann.org.

Вот некоторые из последних публикаций RSSAC. RSSAC имеет серии публикаций. Они пронумерованы. Последняя под номером 31. Последняя [бесплатная] публикация RSSAC029, в которой описаны результаты их семинара в октябре 2017 года. RSSAC030 это заявление о записях в источниках информации для корневых серверов DNS. А RSSAC031 это ответ на последующие процедуры GNSO PDP. Это о последующих процедурах для создания новых TLD. Ответ RSSAC касается темы масштабирования корневого сервера.

RSSAC проведет открытое заседание на этой неделе. Приглашаю посетить его, чтобы услышать в более подробных деталях об этих публикациях.

О текущих работах, из две: Упорядочение процедур деперсонализации при сборе данных. RSSAC выпустила публикацию RSSAC002, и операторы корневых серверов реализовали это, опубликовав статистику по корневым серверам и системе корневых серверов. Здесь [работы продолжаются] можно видеть процедуру деперсонализации некоторых из этих данных. Другая часть работ — это размеры пакетов и DNS.

Вследствие реструктуризации RSSAC в 2013 году, транспарентность, которую пытаются улучшить, является одной из важных целей, и в этом достигнут значительный прогресс благодаря организации группы подготовки, публикации протоколов совещаний и отчетов семинаров, чтобы сообщество ICANN могло понять текущее состояние работ, отчетов и семинаров.

Опубликован календарь RSSAC и группы подготовки со всеми различными рабочими совещаниями. На каждом совещании ICANN, RSSAC проводит открытые заседания. У нас есть учебные руководства, и взаимодействие с представителями обеспечивает передачу информации ключевым организациям.

Наконец, RSSAC имеет [кодированные] операционные процедуры, определяющие порядок работы RSSAC. Они также опубликованы на сайте. Полагаю, это третья редакция.

Операторы корневых серверов также предпринимают шаги по улучшению транспарентности. Опубликованы повестки дня операторов корневых серверов для мероприятий IETF. Каждый оператор опубликовал статистику RSSAC002. Они принимают участие в работе RSSAC. Имеется общедоступный сайт, один сайт, и с этого сайта можно перейти к сайтам отдельного оператора. Они совместно работают над отчетами и крупными мероприятиями. Например, относительно атаки DDoS в прошлом году. А RSSAC выступает в качестве шлюза, направляя эти вопросы операторам корневых серверов, и они отвечают на эти вопросы.

Для получения подробной информации вот ссылка на сайт RSSAC. Все общие вопросы вы можете направлять электронной почтой по этому адресу. Ссылка на группу подготовки и членство указаны здесь.

Наконец, я хочу обратить ваше внимание на то, что RSSAC недавно опубликовала на своем сайте часто задаваемые вопросы и ответы. Полагаю, вот список 25 часто задаваемых вопросов. Некоторые из них составлены по результатам этих заседаний. Поэтому они очень полезны для понимания RSSAC.

На этом, думаю, мы подошли к концу презентации. В зале присутствуют некоторые члены RSSAC. Я приглашаю их выйти сюда на сцену и представится, а также я буду руководить ходом ответов на вопросы. Тогда, наверное, я представлю членов RSSAC, вышедших на эту сцену.

Если у вас есть вопросы, пожалуйста, поднимайте руку и я вас увижу. Так что давайте это сделаем. Позвольте попросить членов RSSAC представиться, начиная с Фреда?

ФРЕД БЕЙКЕР (FRED BAKER): Фред Бейкер, ISC.

ДЖОН КРЕЙН (JOHN CRAIN): Джон Крейн, ICANN.

КАВЕ РАНДЖБАР (KAVEH RANJBAR): Каве Ранджбар, RIPE NCC.

БРЭД ВЕРД (BRAD VERD): Брэд Верд, Verisign

ЛАРС-ЙОХАН ЛИМАН (LARS-JOHAN LIMAN): Ларс-Йохан Лиман, Netnod.

СТИВ ШЕНГ: Спасибо. Мы начнем с вопросов онлайн. Кати?

КАТИ ПЕТЕРСЕН: У нас онлайн-вопрос от Хосе де ла Круз. Вопрос: «Планируется увеличить количество идентификаторов сверх 13?»

СТИВ ШЕНГ: «Планируется увеличить количество идентификаторов сверх 13?» Кто хотел бы ответить?

КАВЕ РАНДЖБАР: Я могу начать. Во-первых, технически расширение возможно. Это мое личное мнение. Но я думаю, что главный вопрос в том, должны ли мы увеличивать количество идентификаторов? Поскольку эти буквы, фактически, являются идентификаторами. Но с технологической точки зрения, если посмотреть на текущую ситуацию, добавление узлов или добавление букв не делает значительного или видимого технического различия. Поэтому первый вопрос заключается в том, какую проблему вы пытаетесь решить, добавляя новые идентификаторы? Таково мое мнение.

БРЭД ВЕРД: Думаю могу добавить следующее к текущему вопросу. Мы получаем его достаточно часто, и я считаю ответ в том, что RSSAC размышляет не только над тем, чтобы добавит, но, возможно, удалить некоторые из них. Возможно, 13 неверное число. Возможно меньше, возможно больше. Мы не знаем. Это один из пунктов в списке, над решением которых мы работаем. Но как сказал Каве, нашей целью является поиск решения технического ответа на этот вопрос. Спасибо.

СТИВ ШЕНГ: Спасибо, Каве и Брэд. Теперь я перехожу к вопросам из зала. Прошу вас, участник впереди.

КАТИ ПЕТЕРСЕН: Если позволите – просто напомню – прошу называть себя и свою принадлежность, если имеется. Спасибо.

АБДУЛКАРИМ ОЛОЙЕДЕ (ABDULKARIM OLOYEDE): Большое спасибо. Меня зовут Абдулкарим, и я из Нигерии. Я впервые в ICANN. Мой вопрос относительно корневых серверов, поскольку каждый из 13 корневых серверов, вероятно, дублируется где-то на планете с тем-же IP-адресом. Так, если возникла проблема с одним из дубликатов, как их можно отличить, если у них одинаковый IP-адрес? Как определить его местоположение? Спасибо.

ФРЕД БЕЙКЕР: Это вопрос о том, как фактически работает Anycast, что немного обсуждалось в предыдущих презентациях. Фундаментальной вещью здесь является маршрутизация. Каждый из этих серверов не только выполняет обслуживание, отвечая на запросы и осуществляя преобразование, чем бы оно ни было, но также участвует в BGP с ISP или IXP, в анонсировании своих адресов.

Поэтому, когда приходит запрос откуда-либо на этот адрес, маршрутизация направляет его на ближайшее топологически зеркало сервера. Если один из серверов не работает, маршрутизация прекращается, по каким-либо неблагоприятным причинам, то адрес этого местоположения удаляется из BGP. BGP больше не выполняет маршрутизацию в этом направлении, но рядом должны быть другие идентификаторы с таким же адресом. Поэтому теперь маршрутизация пакетов осуществляется в какое-то другое место. Это просто стандарт, по которому работает маршрутизация.

В наихудшем случае, давайте представим – и я не знаю причину по которой это может произойти – но представим, что адрес больше не доступен для маршрутизации. Он просто не существует. Одна из причин, почему у нас есть 13 операторов корневых серверов заключается в том, что приложение, сопоставитель в чьем-либо компьютере, может выбрать один из других адресов и направить запрос кому-нибудь еще. Таким образом имеется два уровня резервирования.

СТИВ ШЕНГ: Спасибо. Лиман?

ЛАРС-ЙОХАН ЛИМАН: Хочу добавить, что когда вы используете Anycast, каждый сервер имеет два IP-адреса. Один IP-адрес одинаковый для всех компьютеров, и именно он используется для трафика DNS. Кроме этого, каждый сервер имеет уникальный отдельный адрес. Он используется операторами для внутреннего доступа, так сказать, для обслуживания и администрирования.

СТИВ ШЕНГ: Спасибо. Джон?

ДЖОН КРЕЙН: Спасибо. Я думаю, вы также спрашивали, как вы можете узнать, к какому из них вы обращаетесь. Это, на самом деле, запрос DNS на зарос TXT. Вы должны набрать CHAOS HOSTNAME.BIND и имеется пара других вариантов, где каждое зеркало фактически имеет имя, которое вы можете запросить в DNS, и получить ответ, к кому конкретно вы обратились. Я могу показать вам позже на компьютере, если вы хотите это знать.

СТИВ ШЕНГ: Спасибо за ваш вопрос и исчерпывающий ответ. Участник позади?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: [неразборчиво] из Индии. [неразборчиво] безопасность [неразборчиво] DNSSEC. Можете просто сказать нам, в каких странах (DNSSEC) полностью реализована и какие проблемы возникли во время реализации.

СТИВ ШЕНГ: Вопрос по развертыванию DNSSEC. Есть желающие? Полагаю, в среду семинар DNSSEC. В начале семинара они покажут цифры развертывания по всему миру. Это будет заседание, где вы сможете найти эти цифры.

БРЭД ВЕРД: Это немного не по теме RSSAC. Если по другому перефразировать ваш вопрос и связать его с корневыми серверами, возможно мы попытаемся на него ответить.

КАВЕ РАНДЖБАР: Главное, просто разъясните что мы опубликовали как операторы корневых серверов, мы получили подписанный файл зоны. Это подписанная корневая зона. Это в прошлом, работа RSSAC или операторов корневых серверов фактически началась после того, как появился подписанный файл корневой зоны и мы просто разослали этот файл. Так с нашей точки зрения, мы просто разослали подписанную корневую зону. Мы обеспечили сохранение целостности полученного файла, и мы гарантировали его сохранность во время рассылки файла или его содержания.

СТИВ ШЕНГ: Благодарю вас. Другие вопросы? Участник вон там?

ТАРАУ БАУИА (TARAU BAUIA): Тарау Бауиа, Кирибати. У меня один вопрос. При развертывании DNSSEC возникали ли проблемы с поддоменами [или скажем] с доменом .com, которые не имеет ключей или еще не изменен в DNSSEC? Будет это проблемой?

СТИВ ШЕНГ: Повторю, это также касается DNSSEC и, возможно, лучше подойдет к семинару в среду. Таково мое мнение. Я приглашаю вас посетить этот семинар. Прошу подойти ко мне, и я расскажу вам подробнее об этом семинаре. Теперь я перехожу к онлайн-вопросу, а затем вы следующий.

КАТИ ПЕТЕРСЕН: У нас еще один вопрос от Хосе де ла Круз. Вопрос: «Кто может принимать участие в RSSAC?»

СТИВ ШЕНГ: Спасибо.

БРЭД ВЕРД: В RSSAC имеется группа подготовки, членами которой в настоящее время является свыше 80 экспертов в предметной области. Все наши рабочие комитеты сформированы из группы подготовки, и спонсируются группой подготовки. Чтобы – я полагаю это есть на экране – стать членом группы подготовки, если это вас интересует, можно направив электронное письмо по этому адресу. Заявление рассматривает наш комитет по членству. Вам необходимо предоставить SOI, то есть, выражение заинтересованности. После этого вы становитесь членом группы подготовки и принимаете участие в подготовке решений.

СТИВ ШЕНГ: Спасибо, Брэд, и спасибо вам, Хосе, за этот вопрос. Прошу вас, участник впереди?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Стив? Вы позволите?

СТИВ ШЕНГ: Да, говорите.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Просто добавлю, повторю, большая часть фактической технической работы RSSAC выполняется группой подготовки. Поэтому, если вы член группы подготовки, именно вы выполняете фактическую работу. Итак RSSAC, как показано на слайдах, это 12 организаций, 13 операторов, фактически выполняющих большую часть административной работы.

Когда мы получаем вопрос или когда требуется совет, мы формируем рабочий комитет в группе подготовки. И все мы – члены комитета RSSAC – также являемся частью Группы подготовки RSSAC. Поэтому если мы также хотим принимать участие в подготовке решения, мы также присоединяемся к рабочему комитету. И для каждого полученного вопроса или рекомендации, мы формируем рабочий комитет и основная работа выполняется в группе подготовки, поэтому вы будете частью RSSAC.

БРЭД ВЕРД: Если вы добавите, что работа также связана с людьми в группе подготовки, которые выполняют эту работу. Так не бывает, что группа подготовки выполняет работу, составляет документы, а другие люди приписывают заслуги себе. Если вы участник, вы принимаете непосредственное участие.

СТИВ ШЕНГ: Спасибо. Прошу вас.

АБДУЛКАРИМ ОЛОЙЕДЕ: Хорошо, спасибо. Я хочу знать, как часто происходят заседания RSSAC, и как часто заседания группы подготовки?

БРЭД ВЕРД: RSSAC заседает ежемесячно. Мы проводим ежемесячные телеконференции, готовим протоколы и освещаем вопросы. Эти телеконференции открытые не так-ли?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Протоколы — да.

БРЭД ВЕРД: Протоколы публикуются. Извините меня. Протоколы публикуются. Кроме этого, RSSAC проводит совещания здесь на заседаниях ICANN, также RSSAC пару последних лет проводит два семинара в год в связи с работой над развитием, о чем вы могли слышать, если посетили здесь открытое совещание RSSAC.

Работа группы подготовки всегда проводится онлайн. Все время собираются рабочие комитеты. Работа в рабочих комитетах проводится в зависимости от их собственного распорядка. Это могут быть еженедельные телеконференции или раз в две недели. Фактически их периодичность зависит только от рабочей нагрузки.

Совещания самой группы подготовки проводятся здесь в AGM. Между прочим, и это определила сама группа подготовки. Так что группа подготовки поставила вопрос где проводить совещания, и пришла к соглашению, что проводит совещания в AGM на заседаниях ICANN, и мы теперь собираемся на каждом втором заседании IETF. Думаю, проще сказать, группа подготовки проводит свои совещания по четным заседанием IETF.

СТИВ ШЕНГ: Спасибо. И следующее заседание группы поддержки на 102 IETF в Монреале. Спасибо. Другие вопросы? Прошу вас, участник слева?

БОННИ МТЕНГВА (BONNIE MTENGWA): Хорошо, спасибо. Я Бонни Мтенгва, нормативное регулирование в сфере телекоммуникаций Зимбабве. У меня вопрос. Мы собираемся разместить один из корневых серверов в Зимбабве, заинтересована ли ICANN помочь разместить корневой сервер или, возможно, это зависит только от переговоров страны с операторами корневых серверов или, возможно получить помощь от ICANN либо, возможно, сначала необходимо выполнить некоторые требования?

СТИВ ШЕНГ: Спасибо за вопрос и интерес к размещению зеркала корневого сервера. Лиман?

ЛАРС-ЙОХАН ЛИМАН: Многие, если не все, то большинство операторов корневых серверов имеют облака Anycast и склонные вступать в дискуссии относительно того, где их размещать и где их устанавливать. Это не обсуждается между страной и оператором корневого сервера. Это между конкретным узлом, организацией, предоставляющей аренду серверов. В большинстве случаев точкой обмена трафиком интернет является крупный интернет-провайдер или аналогичная компания.

Вы правы, что необходимо выполнить определенные требования, главным образом технические и финансовые требования. Мы работаем над составлением списка контактов, но я скажу, идите и поговорите с любым оператором корневого сервера и мы постараемся объяснить, как мы видим эти взаимоотношения и какие наши и других сторон требования будут видны также с их стороны. Вопрос размещения корневого сервера [имен] в вашем региона определенно является открытым, если мы сможем найти способ удовлетворить эти требования, поскольку потребуется поработать, имеются требования, да.

СТИВ ШЕНГ: Спасибо, Лиман. Другие вопросы? Снова участник спереди.

АБДУЛКАРИМ ОЛОЙЕДЕ: Я просто подумал, да, корневой сервер DNS является важной частью интернета и работа RSSAC и деятельность операторов корневых серверов выглядит достаточно открытой. Мы говорили о злоумышленниках, пытающихся атаковать корневые сервера. Как вы будете защищаться от этого? Если такое лицо имеет внутренний мотив, поскольку любой может принять участие, прийти на заседание, любой может принять участие в работе. Так как вы будете защищаться от этого? Спасибо.

СТИВ ШЕНГ: Вопрос о том, как оградить злоумышленников (от работы с RSSAC).

КАВЕ РАНДЖБАР: Это хороший вопрос, сложный вопрос [также], поскольку здесь имеется множество аспектов. Но я думаю об одной вещи, и я говорю только от RIPE NCC, но думаю большинство, если не все, операторы корневых серверов разделяют это мнение, что мы не можем гарантировать безопасность корневых серверов путем затемнения. Мы полностью открыты не столько потому, что мы так работаем, но потому, что сам принцип работы DNS является открытым. Вы можете получить множество информации о зеркалах, где они размещены и все остальное. Во многих случаях мы публикуем это, но даже если мы этого не сделаем, посредством DNS при наличии незначительных основных знаний это легко узнать.

Поэтому система открыта. Со всей имеющейся производительностью, которой мы располагаем с технической точки зрения, главной нашей задачей является старание гарантировать способность ответить на каждый отдельный запрос. И да, как операторы корневых серверов, мы также позволяем направлять им злонамеренные запросы независимо от того, атака это или нет. Но в целом, мы располагаем достаточной производительностью, чтобы обеспечить [устойчивое] и постоянное обслуживание правильных и хороших запросов.

СТИВ ШЕНГ: Джон?

ДЖОН КРЕЙН: В сети работают профессионалы, поэтому все операторы имеют опытных инженеров и службы безопасности, и мы очень серьезно заботимся о надежности наших систем. Вот почему, если вы разместили зеркало, например, существуют требования и некоторые из них определяют, кто и как имеет доступ к машинам и прочее. Так что мы очень серьезно относимся к безопасности. Но как Каве только что сказал, по своей сути и цели DNS является совершенно открытой. Если хотите, это природа самого протокола.

СТИВ ШЕНГ: Спасибо. Брэд?

БРЭД ВЕРД: Хочу более подробно остановиться на вашем вопросе. Я понял, что Группа подготовки RSSAC является открытой и все имеют возможность присоединиться, что помешает злоумышленнику вступить и попытаться сделать что-либо вредоносное. Это вы имели в виду, задавая вопрос?

Я считаю, да, риск есть. Мы хотим быть открытыми. Мы хотим быть транспарентными, и мы хотим учитывать различные точки зрения многих людей, чтобы приходить к наилучшим возможным решениям по всем техническим проблемам, встающим перед нами. Как сопредседатель, я надеюсь, что существующие проверки и преобладание людей с хорошими намерениями позволит выявить людей с злыми намерениями и работа с ними позволит определить что происходит. Но пока, мне не известно о том, что такое случалось, но это риск.

СТИВ ШЕНГ: Спасибо. Следующий вопрос? Участник позади?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Здравствуйте. Меня зовут [неразборчиво] и я из Индии. Я вернусь к вопросу, который вы затронули ранее в своей презентации, что маршрут трафика определяется не коневым сервером, а маршрутизаторами. Я хочу спросить у вас, особенно в связи с тем, что вы указали на требования RSSAC002, чтобы операторы корневых серверов публиковали статистику своих корневых серверов. Теперь, если я захочу определить, какой общий сетевой трафик поступил из конкретного места или конкретной страны, то как я могу это экстраполировать или как я могу измерить это исходя из определенной статистки, которая уже доступна онлайн, которая доступна из открытого источника? Спасибо.

СТИВ ШЕНГ: [Благодарю за вопрос].

БРЭД ВЕРД: Постараюсь дать самый краткий ответ. Трафик корневого DNS не должен использоваться для измерения общего сетевого трафика.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Нет, извините, что прерываю вас, но еще я хочу у вас спросить, как я могу сделать [неразборчиво] определенную оценку или некоторую приблизительную оценку, положим близкую к точной оценку, как мне использовать трафик DNS для измерения поступившего [неразборчиво]?

НЕНАЗВАВШИЙСЯ МУЖЧИНА: В общем, как сказал Брэд, фактически, чтобы получить просто полезную оценку, вы не должны использовать для этого DNS. Платформа DNS не для этого, а существуют другие методы измерений. Например, если хотите, взгляните на Google MLAP. На основании показываемого ими [потока] трафика, они пытаются оценить [остальной] трафик страны или региона.

Также имеются другие [продукты], но DNS по-правде не подходящая для этого платформа. Основной причиной является во-первых то, что не весь контент проходит через DNS. А во-вторых, то что вы получите от DNS на любом уровне, особенно на корневом, большинство поступает из кэша сопоставителей, а эффективность кэша для нас не видна. Поэтому, фактически, невозможно получить даже полезную оценку на основании трафика DNS.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Позвольте добавить к этому еще одно. Когда вы заходите в корневую систему и статистика RSSAC002 показывает получение большого числа запросов IPv6, множества UDP, множества прочего, это запросы к корню. Что люди пытаются найти домены .com и .net и прочие по всему миру. Они не ищут конкретные сайты в каком-либо смысле или даже отдельные компании. Они ищут регистратуры. Так что это просто неверные данные.

СТИВ ШЕНГ: Спасибо. Другие вопросы? Есть ли еще онлайн-вопросы?

КАТИ ПЕТЕРСЕН: Вопросов онлайн нет.

АБДУЛКАРИМ ОЛОЙЕДЕ: В смысле RSSAC и наращивания организационного потенциала, делается ли вами что-либо подобное? Наращивание потенциала для, возможно, развивающихся стран или заинтересованных лиц? Поскольку неоднократно, если, например, я заинтересован, я никогда в своей жизни не буду работать на коневом сервере, или я могу быть заинтересован в области, которая слишком техническая для меня, поскольку я не делал этого в своей повседневной жизни, но я хочу знать больше. Спасибо.

КАВЕ РАНДЖБАР: Я задам вопрос по своему, не знаю, правильно ли я его понял. Прежде всего, давайте представим, что вы первый раз присутствуете и являетесь участником. Поэтому большое спасибо, что принимаете активное участие. Это весьма приветствуется.

В отношении наращивания потенциала, фактически каждый отдельный оператор корневого сервера имеет или может иметь свой собственный план. Например, я расскажу о RIPE NCC. Мы в RIR, региональной интернет-регистратуре, для Европы, Среднего Востока и Центральной Азии. Вот что мы делаем, не только в нашем регионе, но также для остального мира, включая Африку и регион AP, мы работаем с другими RIR. Например, [неразборчиво] у нас есть Меморандум о взаимопонимании с AfriNIC для Африки или APNIC для Азиатско-Тихоокеанского региона, и в частности позвольте мене использовать пример из Африки.

Что мы сделали в Африке это сформировали AfriNIC совместно с ISOC Африки, они фактически обеспечили финансирование и переговоры с операторами и заинтересованными сторонами, а мы фактически разместили несколько узлов на основе этого финансирования и этого потенциала, созданного посредством ISOC Африки и (нашего RIR).

Такой метод мы выбрали в RIPE NCC. Другие имеют другие методы и другие подходы к развитию регионов. Так что вам надо проверить каждого отдельного оператора корневого сервера.

Просто отмечу, поскольку также был вопрос о том, как получить зеркала корневых серверов, на сайте root-servers.org имеется список каждого оператора и здесь также находятся их сайты для услуг корневой зоны. Так что вы можете проверить сайт RIPE NCC на услуги корневой зоны, сайт Verisign на услуги корневой зоны. И здесь вы найдете всю информацию. Например, здесь перечислены наши соглашения с другими RIR и здесь написано и указано как вы можете перейти сюда либо прямо либо косвенно через [вашу] региональную интернет-регистратуру.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Могу я добавить, большинство этих вопросов операционные по характеру, и здесь также присутствует много операторов корневых серверов. Но я снова спрошу вас об обязанности RSSAC давать рекомендации о системе корневых серверов правлению и сообществу. Было много вопросов напрямую не относящихся к RSSAC, и я считаю, что находящаяся здесь группа готова ответить на них и мы хотим быть транспарентными насколько это возможно, но мы хотим продолжить – существует разделение между операторами корневых серверов и RSSAC. Таким образом, я просто хочу это подчеркнуть.

СТИВ ШЕНГ: Благодарю вас. Другие вопросы? Один? А, Лиман.

ЛАРС-ЙОХАН ЛИМАН: Просто заключительное замечание. Если у вас возникнут вопросы после заседания, можете подойти и поговорить, как минимум, со мной лично. Я имею ввиду всех нас. Мы здесь для этого. Мы хотим поговорить с вами, и я готов ответить на любые вопросы, насколько смогу.

НЕНАЗВАВШИЙСЯ МУЖЧИНА: Еще раз, хочу сделать замечание к часто задаваемым вопросам, недавно добавленным на сайте RSSAC. Хотя, как я сказал ранее, множество полученных вопросов операционные по характеру, мы постарались собрать все эти вопросы, поступившие на множестве этих различных презентаций, а также вопросы, которые мы просто получили обычным путем. Часто задаваемые вопросы постоянно дополняются, поэтому, если здесь нет интересующего вас вопроса, я уверен кто-нибудь еще его задаст, просим поделиться им с нами и мы добавим его и сделаем часто задаваемые вопросы еще полнее. Спасибо.

СТИВ ШЕНГ: Теперь, разрешите мне показать на экране сайт RSSAC, здесь у нас совещания, группа подготовки, публикации и часто задаваемые вопросы. Если щелкнуть по ссылке, здесь множество информации о протоколах заседаний, членах группы подготовки, все публикации RSSAC и часто задаваемые вопросы.

Сайт root-servers.org о котором говорил Каве является шлюзом к отдельным корневым серверам. Если у вас есть конкретные [дополнительные] вопросы, здесь имеется контактная информация. Также отсюда мы взяли карту Anycast для презентации. Вы также можете более глубоко погрузится в сайт для получения дополнительной информации.

На этом, если больше нет вопросов, я благодарю вас за участие и членов RSSAC за ответы на ваши вопросы. Спасибо. Объявляю заседание закрытым.

КАТИ ПЕТЕРСЕН: Спасибо всем.

[КОНЕЦ СТЕНОГРАММЫ]