RU

ICANN81 | Ежегодное общее собрание — Принципы работы — Работа корневых серверов
10 ноября 2024 года (воскресенье), 13:15 – 14:30 по TRT

УЛЬРИХ ВИССЕР (ULRICH WISSER):

Здравствуйте и добро пожаловать на ознакомительный вебинар из цикла «Принципы работы», который будет посвящен работе корневых серверов. Меня зовут Ульрих Виссер, на этом заседании я буду исполнять обязанности координатора участия. Пожалуйста, помните о том, что это заседание записывается, придерживайтесь стандартов ожидаемого поведения ICANN и политики сообщества ICANN по предупреждению домогательств. Во время заседания будут зачитываться только те вопросы и комментарии, которые отправлены с помощью функции вебинара Q&A. Если вы захотите выступить в ходе этого заседания, поднимите руку в Zoom. Когда вам предоставится слово, если вы участвуете в виртуальном формате, вы получите возможность включить свой микрофон в Zoom. Участники на месте будут пользоваться своими физическими микрофонами. Называйте для протокола свое имя и говорите не слишком быстро. Приглашаем всех пользоваться чатом. Обратите также внимание, что в формате вебинара Zoom закрытые чаты возможны только между участниками группы. Любое сообщение, отправленное участником дискуссии или обычным участником

другому обычному участнику, будет видно всем организаторам заседания, со-организаторам и другим участникам панельной дискуссии. А теперь я передаю слово Кену Ренарду.

КЕН РЕНАРД (KEN RENARD): Спасибо. Добрый день! Меня зовут Кен Ренард. Я представляю одного из операторов корневых серверов — Исследовательскую лабораторию сухопутных войск. Сегодня мы проведем презентацию и пригласим всех желающих задавать вопросы по ней. Она будет очень интерактивной. Мы рады видеть вас здесь. И мы рады, что можем поделиться с вами этой информацией об основах работы. Да, у меня есть пульт. Итак, в двух словах, сегодня мы будем говорить о некоторых аспектах работы DNS, потому что это поможет нам объяснить, какое место занимает во всем этом система корневых серверов. Это своего рода положение дел, отражающее то, как выглядит система корневых серверов на сегодняшний день. Краткое объяснение Anycast, затем мы расскажем о (неразборчиво) и немного о том, как осуществляется управление ими.

Итак, начнем мы с того, что IP-адрес в Интернете — это на самом деле такой фундаментальный идентификатор, который можно представить в виде таких цифр или в виде строки из ноликов и единичек, которая представляет собой такой адрес. То есть когда вы подключаетесь к Интернету, вам присваивается IP-адрес. Проблема здесь в том, что мы, люди, не очень хорошо запоминаем

такие цифры. А это могут быть очень разные цифры. И это хорошо. То есть это та причина, по которой изначально разрабатывалась система DNS — чтобы было удобно работать с этими цифрами, учитывая то, что они могут быть разными. Более современный аспект этой технологии заключается в том, что один и тот же IP-адрес может иногда использоваться совместно разными сайтами. И дополняет это тот факт, что один и тот же адрес, как и один и тот же сайт, может на самом деле располагаться по нескольким IP-адресам. Так что система DNS — наш друг. Она значительно все упрощает для нас, так что она используется все время. Здесь у нас пространство имен. Мы на самом деле используем DNS, чтобы сопоставлять имена с этими IP-адресами. Так что у нас есть это иерархическое пространство имен, которое начинается здесь, на верхнем уровне, с корневой системы. А под этим располагаются все наши TLD-домены, то есть домены верхнего уровня. Это национальные домены. Это т. н. домены gTLD. Ниже располагается второй уровень, под ним третий и т. д. Чаще всего, пожалуй, DNS используется для того, чтобы сопоставить с именем соответствующий ему IP-адрес. Но аналогичным образом сопоставляются также и другие ресурсы, например, почтовые сервера для того или иного домена. Вот так работает почта. Зачастую это адреса, когда IP-адрес используется для поиска какого-то существующего имени. Кроме того, в DNS хранится много информации, связанной с безопасностью, что помогает нам поддерживать безопасность в Интернете. Если посмотреть на DNS, здесь внизу прекрасные слова. DNS — это распределенная по

всему миру масштабируемая динамическая база данных с нежесткой связностью. То есть это можно представить себе как телефонный справочник. Посвятим этому некоторое время. Это процесс поиска имени в DNS. Это классическая схема, которую можно увидеть в практически каждом учебнике. С ее помощью удобно описать какие-то базовые вещи. Когда мы закончим, я добавлю поверх нее еще один уровень.

Итак, если посмотреть на этот процесс, вот здесь, слева, вот ваше мобильное устройство, ваш браузер, ваш компьютер, ваш холодильник, тостер, электрический выключатель — все, что угодно, что подключено к Интернету, будет выступать в этой роли и запрашивать IP-адреса для тех или иных имен. Чтобы узнать адреса этих имен, ваше устройство обращается к рекурсивному резолверу. Это этот прямоугольник в центре. Такие рекурсивные резолверы — это рабочие лошадки глобальной системы DNS. Именно здесь происходит самое интересное. Основной объем работы выполняется здесь, на рекурсивном резолвере. То есть ваше устройство обращается к локальному рекурсивному резолверу и запрашивает адрес сайта, здесь у нас для примера www.example.com. А рекурсивный резолвер должен выяснить, какой адрес соответствует этому имени. Здесь мы описываем схему этого процесса. На первом этапе выясняется, где расположен домен .com. То есть система корневых серверов — это только этот прямоугольник в правом верхнем углу. Он будет подавать запрос. Система корневых серверов скажет, к примеру, я

не знаю адрес сайта www.example.com, но я знаю, где находится база данных для домена .com. И эта информация будет выдана рекурсивному резолверу. Рекурсивный резолвер скажет: «Ага! Раз я теперь знаю, где находится база данных домена .com, обращусь-ка я к ней и задам ей тот же вопрос». А домен .com даст свой ответ, практически таким же образом. Я не знаю адрес для этого полного имени, но я знаю, где находится example.com. Эта информация возвращается на резолвер, и тогда этот рекурсивный резолвер может обратиться с запросом к базе данных для домена example.com и получить ответ на него.

Еще одна действительно важная составляющая всего этого — это то, что в процессе этого такой рекурсивный резолвер запоминает каждый из ответов, возвращаемых на его запросы. Ваше устройство еще раз подает запрос адреса для имени www.example.com. Оно уже знает ответ, поэтому ему больше не нужно проходить все три этапа этого процесса. Если ваше устройство запрашивает адрес для имени q.example.com, оно может пропустить первый этап, то есть обращение к системе корневых серверов. Оно может пропустить второй этап, то есть запрос сервера для домена .com, и перейти сразу к последнему этапу. То есть такая оптимизация является встроенной в сам этот процесс. Эта информация кэшируется или запоминается на определенный период времени. Для корневой системы, в частности, этот период составляет 48 часов. То есть каждый раз, когда будет подаваться какой-то запрос к домену .com, ваш

рекурсивный резолвер должен будет обратиться не более чем... Еще один элемент оптимизации — это то, что вы не единственный, кто использует этот рекурсивный резолвер. Вы и еще десятки или сотни или тысячи других пользователей Интернета, находящихся рядом, используете один и тот же рекурсивный резолвер, который таким образом может запоминать все, что уже запрашивал кто-то из других пользователей. То есть ваше устройство может отправлять тысячи запросов к DNS, но ни один из них не будет направляться непосредственно к системе корневых серверов, потому что вся эта информация может уже быть в памяти. То есть это невероятная оптимизация эффективности, и вы можете видеть здесь, что система корневых серверов, вот этот авторитарный корневой сервер — это очень важный элемент, потому что с него все начинается, но он так не так уж и часто используется. Перейдем к следующему.

Немного подробнее о кэшировании и разрешении имен. Итак, у каждой записи DNS есть параметр времени существования, т. н. time to live, или TTL. Это срок, на который такой рекурсивный резолвер может запоминать полученный ответ, прежде чем эти данные будут признаны устаревшими и их необходимо будет запрашивать заново. Важный момент — корневые сервера выдают информацию только о доменах верхнего уровня. Они знают только то, где расположен домен .com. Где расположен домен example.com, они уже не знают. Только домены верхнего уровня.

На данный момент существует всего 1450 доменов верхнего уровня. То есть у нас очень небольшая база данных.

Теперь о некоторых современных усовершенствованиях DNS. Это, по сути... они относятся не непосредственно к системе корневых серверов, просто это усовершенствования, которые довольно сильно помогают в работе DNS. Это безопасность DNS, то есть расширения безопасности системы доменных имен, или DNSSEC, благодаря которым мы можем обеспечивать для данных DNS защиту с подписью криптографическим ключом. Это устраняет, или, вернее, как говорят специалисты в области безопасности, снижает риск подделки адресов. И этот промежуточный сервер, этот резолвер, рекурсивный резолвер, который находится между подателем запросов и серверами, выдающими ответы, имеет возможность проверять контрольные суммы криптографической защиты, чтобы удостовериться в подлинности получаемых данных. Так что на самом деле не важно, откуда к вам приходит информация из DNS, потому что вы можете убедиться в том, что она достоверна и не была никем изменена. Есть также усовершенствования, касающиеся защиты конфиденциальности. Это касается того, что в этом примере, когда вы запрашиваете адрес для имени www.example.com, мы видели, что этот запрос отправляется в корневую зону, он также отправляется на сервера .com и на этот рекурсивный резолвер. А там на самом деле может быть какая-то конфиденциальная информация. С точки зрения системы корневых серверов мы не видим адрес вашего

устройства, мы видим адрес только этого рекурсивного резолвера. Так что мы не [неразборчиво] на конкретный компьютер или устройство, а только на используемый им рекурсивный резолвер. Есть и другие протоколы, такие как DOT, или DNS по TLS, есть DNS по HTTS, есть DOQ, то есть DNS по QUIC, с помощью которых передаваемые таким образом запросы шифруются. И они на данном этапе работают между вашим устройством, которое показано слева, и этим промежуточным сервером, то есть рекурсивным резолвером. Нам еще предстоит узнать, как они используются на этом втором этапе.

Хорошо, немного о системе корневых серверов на сегодня. Здесь кое-какие определения. Корневая зона. Это на самом деле список доменов верхнего уровня и адресов их серверов имен, то есть DNS-серверов. То есть это то, что находится в корневой зоне. Мы, то есть система корневых серверов, работаем поверх этого. Скоро мы и это рассмотрим. Система корневых серверов — это в совокупности набор операторов корневых серверов плюс вся та инфраструктура, которая развернута у каждого из таких операторов, то есть это компьютеры, которые отвечают на запросы из Интернета. Оператор корневого сервера, а вы часто будете слышать это словосочетание или сокращение RSO, — это организация, которая поддерживает работу каждого из таких корневых серверов, а мы сейчас рассмотрим это чуть подробнее. Зеркало Anycast корневого сервера — это на самом деле одно место в сети. У нас есть 12 операторов корневых серверов, 13

корневых серверов и свыше, кажется, 1800 зеркал Anycast. То есть у каждого оператора на их IP-адресах работает множество компьютеров по всему миру.

Консультативный комитет системы корневых серверов — это консультативный комитет ICANN, в который входят члены, назначаемые операторами корневых серверов, а также некоторые представители. Мы консультируем Правление и сообщество ICANN по вопросам работы корневых серверов. Давайте рассмотрим это немного подробнее и, так сказать, разделим понятия корневой зоны и системы корневых серверов. Скажу еще раз, корневая зона — это данные. Система корневых серверов — это компьютеры, которые работают в Интернете и к которым вы можете направлять запросы, а они будут возвращать вам ответы на эти запросы. То есть это очень небольшая часть всей системы. Опять же, это очень важно, но такое разделение делается на самом деле в целях обеспечения безопасности, это разделение обязанностей, то есть чтобы роли и обязанности были четко определены.

Здесь немного подробнее описывается администрирование корневой зоны. То есть если вы оператор домена верхнего уровня [неразборчиво] запрос, возможно, вам нужно изменить адрес вашего сервера DNS. Тогда этот запрос направляется в IANA. Именно там вносятся такие изменения. Изменения вносятся в фактическую базу данных. Этот файл защищается всеми подписями, и именно здесь начинается система корневых серверов. Мы получаем эту таблицу, которая уже подписана, уже

зафиксирована, а мы просто работаем с ней. Мы рассылаем этот файл по всем нашим компьютерам, на все наши резолверы, которые показаны в правой части и которые обрабатывают запросы к нашей системе. То есть на нас приходится лишь малая часть всего администрирования корневой зоны.

Если оглянуться назад, на 1984 год, то есть 40 лет назад, когда была создана система DNS, тогда было четыре корневых сервера. А по мере роста Интернета в США и в некоторых других странах возникла необходимость увеличить их количество. У нас было семь корневых серверов. Мы видим, что значительная часть этого роста пришлась на 80 и 90 годы. У нас есть корневые сервера, не только операторы корневых серверов, которые расположены по всему миру. У каждого из этих операторов есть компьютеры, расположенные по всему миру. С течением времени мы реагируем на технические потребности. Это техническая служба и мы придерживаемся некоторых принципов, которые очень важны для работы этой системы. Она должна работать всегда. То есть мы реагируем на технические потребности, потому что со временем развиваются технологии и растет количество запросов. Проблемы с масштабированием. Когда-то давно 13 корневых серверов означало 13 физических компьютеров. Сейчас 13 корневых серверов — это свыше 1800 компьютеров. То есть использование технологии Anycast позволило нам масштабировать эту систему в новое измерение, чтобы она могла обслуживать гораздо большее сообщество. Если вас действительно интересуют подробности

истории этих технологий, то кое-какие интересные детали приведены в документе RSSAC023.

Итак, идентификаторы корневых серверов и их операторы. Все эти адреса публичные. Мы все работаем на адресах IPv4 и IPv6, то есть мы уже долгое время этим занимаемся. Есть такой сайт, на который вы можете перейти, root-servers.org, там есть такая удобная маленькая карта, на которой можно менять масштаб, смотреть и находить эти 1800 реплик, где каждая из них находится. Правда, это не обязательно именно их местоположение в смысле топографии, потому что Интернет и география — это не совсем одно и то же, но там действительно очень широко эти сервера распределены. Необязательно находить именно тот, который близко к вам физически, потому что это Интернет. Вы можете связаться с любым из них. Отсюда, из Стамбула, вы можете обратиться к любому из корневых серверов, а они обработают ваш запрос совместно. Маршрутизация может направить вас на тот из них, который ближе к вам. Маршрутизация может направить вас на сервер, расположенный за тысячи километров от вас, но на ваш запрос в любом случае будет дан ответ.

В RSSAC был разработан набор базовых принципов работы. Это, пожалуй, долго читать. Вы, конечно же, можете ознакомиться с этим набором слайдов онлайн. Я отмечу только несколько из них. Это все такие вещи, которые нам очень дороги и близки, назовем наш принцип номер два, в соответствии с которым источником данных корневой системы DNS является IANA. То есть это то,

откуда мы получаем наши данные, из IANA через корневую зону, принцип «Один Интернет — одна корневая зона». Если вы обратитесь к любому из этих 1800 серверов в Интернете, то они будут выбирать данные из одной и той же базы.

Сила системы корневых серверов в целом заключается в ее разнообразии. У нас разнообразное аппаратное и программное обеспечение, у нас есть самые разные организации. Если даже случится сбой в оборудовании какого-то конкретного поставщика, то на всей системе это не скажется. То же самое и с программным обеспечением. Если в каком-то конкретном программном обеспечении будет ошибка, она затронет только лишь малую часть всей системы. То же самое и с отраслями, которые у нас представлены. У нас есть государственные органы, у нас есть коммерческие и некоммерческие организации, образовательные учреждения. То есть проблемы в какой-то одной конкретной отрасли не затронут работу корневых серверов. Как операторы корневых серверов мы тесно сотрудничаем и взаимодействуем друг с другом и с сообществом заинтересованных сторон. Поэтому мы здесь. Мы довольно тесно сотрудничаем в работе над некоторыми техническими проблемами, что помогает нам развиваться и поддерживать систему корневых серверов. Но мы также поддерживаем анонимность, автономность и независимость, то есть мы не контролируем друг друга. Никто из нас не главнее других, просто мы коллективно выполняем эту работу.

Существуют определенные мифы, касающиеся системы корневых серверов, которые мы довольно часто слышим, например, о том, что мы контролируем то, куда направляется сетевой трафик. Это совершенно точно не так. Этим занимаются маршрутизаторы. Мы обеспечиваем работу одной части процесса разрешения имен. Корневые сервера обрабатывают запросы. Мы видели чуть раньше слайд, на котором речь шла о рекурсивных резолверах и кэшировании данных. На самом деле очень немногие DNS-запросы заканчиваются обращением к системе корневых серверов. Содержанием этих данных управляет IANA. Мы просто операторы компьютеров. Мы просто такой отдел ИТ корневой зоны. Все эти буквы, а серверам назначены буквы от A до M, но никакого особого значения они не несут. По сути, они были назначены просто случайным образом. На предыдущем слайде, там был этот последний миф о том, что реплики корневых серверов получают полный запрос DNS. Если подается запрос адреса для имени www.example.com, обычно к нам поступает весь этот запрос. Мы видим, что рекурсивный резолвер запрашивает адрес для имени www.example.com. Мы знаем, что мы выдадим ответ только для домена .com. На самом деле существует такая технология, которая называется QNAME Minimization, она позволяет рекурсивному резолверу сокращать этот запрос, так что мы, то есть система корневых серверов, мы видим это не как запрос адреса для имени www.example.com. То есть у нас есть такая технология, которая может быть реализована на вашем рекурсивном резолвере и

которая позволяет обеспечивать чуть большую конфиденциальность.

Некоторые рекомендации по использованию системы корневых серверов. Если вы являетесь оператором рекурсивного резолвера, вы можете проверять маршрут к вашим репликам корневых серверов. То есть вы можете выполнить команду отслеживания маршрута, trace route или что-то в этом роде, чтобы посмотреть, где находится каждая реплика. Обычно вас интересуют три или четыре реплики, которые расположены не очень далеко. У нас нет точного определения того, что такое «не очень далеко». Обычно это измеряется по скорости отклика. Мы рекомендуем использовать резолвер с проверкой подлинности DNSSEC, просто на случай, если кто-то еще [неразборчиво] у вас будет возможность удостовериться в подлинности этой информации. Мы рекомендуем участвовать в работе технических сообществ DNS. Членство RSSAC довольно сильно ограничено операторами корневых серверов, но у нас есть еще группа подготовки RSSAC, открытая для специалистов в области DNS. Значительная часть нашей работы в RSSAC выполняется именно в этой группе подготовки. Если вы хотите участвовать в ее работе, зайдите на сайт и поищите группу подготовки. Там есть информация о том, как подать заявку на членство в ней. А некоторые операторы корневых серверов на самом деле попросят вас дать им возможность разместить реплику их корневого сервера где-нибудь у вас в сети. Чтобы это сделать, нужно связаться с кем-то из

членов RSSAC здесь или с кем-то из операторов корневых серверов здесь и написать по электронной почте на адрес ask-RSSAC@ICANN.org. Такое письмо дойдет и до нас. Взглянем кратко на это. [неразборчиво] множество статистических показателей, касающихся использования системы корневых серверов. Это просто как если бы мы рассматривали запросы в целом, по сути, это среднее количество запросов в день. Речь идет о приблизительно 100 миллиардах запросов в день, которые мы все наблюдаем в совокупности. Звучит впечатляюще. Большинство из них мусор и ошибки конфигурации, но мы однозначно видим выделение ресурсов с избыточностью. Потенциал по ресурсам там очень большой. Хорошо, на этом я передаю слово Лиману, который расскажет о технологии Anycast.

ЛАРС-ЙОХАН ЛИМАН: Здравствуйте, меня зовут Ларс Лиман (Lars Liman). Я работаю в компании Netnod, которая поддерживает работу одного из наборов корневых серверов. Я попробую поговорить немного о технологии Anycast. Итак, технология Anycast на самом деле не относится непосредственно к DNS. Это такой прием, который мы используем в сети, чтобы иметь возможность распределять нагрузку между различными серверами для каждого оператора в системе корневых серверов. То есть все эти 1800 серверов, о которых говорил Кен, они разбиты на разных размеров группы между разными операторами. Компания Netnod поддерживает работу приблизительно 75 или 80 из этих в общей сложности 1800

узлов. И все сервера, находящиеся в управлении одного и того же оператора, имеют один и тот же IP-адрес. То есть два, один протокола IPv4 и один — IPv6. Обычно нельзя, чтобы у двух компьютеров в сети был один и тот же IP-адрес. Но Anycast — это такая уловка, которая позволяет делать это таким образом, что у нас получаются идентичные копии.

Я в данном случае воспользуюсь такой аналогией. Если вы путешествуете по Европе с мобильным телефоном, вы можете набрать... Если так случится, что вы попадете в какую-то чрезвычайную ситуацию, когда вам понадобится скорая помощь, вы сможете набрать на своем телефоне номер 112. Вас свяжут с центром реагирования на аварийные ситуации, который поможет направить скорую помощь в то место, где вы находитесь. Если вы находитесь в Нидерландах, в Амстердаме, и наберете номер 112, то вас свяжут с центром реагирования на аварийные ситуации, который расположен рядом с Амстердамом. Если вы поедете в Италию, в Рим, и наберете номер 112 там, то ваш звонок не будет направлен в Амстердам. Он будет направлен в диспетчерский центр в Риме или недалеко от Рима. Это тот же прием, который используем и мы, только уже в контексте Интернета. Таким образом, если ваш резолвер, то есть компьютер, который помогает находить адреса в Интернете, если ваш резолвер расположен в Амстердаме и при этом пытается обратиться к корневому серверу имен по определенному IP-адресу, то его запрос будет направлен на корневой сервер имен рядом с

Амстердамом или в самом Амстердаме. Если ваш сервер имеет тот же IP-адрес, но расположен в Риме, то ваш запрос будет передан на сервер в Риме или рядом с Римом. И это всего два примера. Сейчас у нас есть сервера в 75 разных местах, а у других операторов они могут быть в 50 или в 200 разных местах по всему миру. Иногда они у нас располагаются в одних и тех же местах, но в большинстве случаев в разных. То есть существует целая сеть таких серверов, и всегда найдется такой сервер, который расположен недалеко от вас. Так что, используя эти конкретные цифры адреса для обращения к корневому серверу, можно всегда связаться с сервером, расположенным недалеко.

Я попытаюсь проиллюстрировать это с помощью слайдов. Но прежде чем это сделать, я хочу подчеркнуть, что это дает нам несколько интересных особенностей. Нет, на самом деле я сначала пройдусь по слайдам. Следующий слайд, пожалуйста. Спасибо. Маршрутизация в Интернете работает так, чтобы по возможности направлять пакеты по кратчайшему маршруту между двумя компьютерами. Обычно они проходят через несколько маршрутизаторов, или я бы... Я тут немного неправильно использую термин «сетевой коммутатор», который как бы направляет трафик между различными звеньями и пытается направлять пакеты все ближе и ближе к конечному пункту их маршрута. В обычном случае, когда не используется технология Anycast, передача осуществляется между двумя уникальными IP-адресами. Это адрес отправителя и адрес получателя, то есть

пакет передается в направлении адреса получателя. То есть все эти маршрутизаторы работают совместно для того, чтобы направить ваши пакеты к конечной точке, к точке назначения, к тому серверу, к которому вы пытаетесь обратиться. А DNS-запросы в Интернете — это обычный сетевой трафик. DNS-пакеты ничем особым не выделяются. То есть для них используется тот же принцип. Если вы отправляете запрос DNS с резолвера, показанного слева, на DNS-сервер, показанный справа, то он передается по сети. Следующий слайд, пожалуйста.

Теперь представьте себе, что у вас есть три идентичных точки назначения. Они на самом деле работают одинаково. У них один и тот же IP-адрес. У них одно и то же содержание базы данных. Это очень важно. Они используют одну и ту же сеть и один и тот же способ подключения к этой сети. Пакет, отправленный с исходного адреса, будет пытаться попасть в ближайшую точку назначения. И это на самом деле работает, потому что эти точки назначения объявляют в сети, мол, вот я здесь, вот же я, вот мой IP-адрес. Так что вы попадете в ближайшую к вам точку, голос которой, так сказать, будет звучать громче всего. Положительный момент здесь в том, что пакеты с разных исходных адресов будут попадать в разные конечные точки назначения. Следующий слайд, пожалуйста.

То есть пакеты с исходного адреса слева попадут на сервер в левом нижнем углу, потому что он ближе всего к этому исходному адресу. А пакеты с исходного адреса в правом верхнем углу попадут на

сервер в правом нижнем углу, потому что к этому исходному адресу ближе всего этот сервер. То есть в зависимости от того, где именно в сети вы находитесь, ваши DNS-запросы будут всегда попадать в ближайшую точку назначения, или же это можно использовать также и в других ситуациях. Это не обязательно должна быть система DNS. Конечно, очень важно, чтобы эти синие точки назначения были синхронизированы. Чтобы ответ на ваш запрос был одинаковым независимо от того, на какой конечный сервер он попадет. И это задача операторов корневых серверов — сделать так, чтобы все эти конечные сервера были должным образом синхронизированы и располагали обновленными и достоверными данными.

Здесь есть ряд интересных особенностей, которые могут быть не сразу очевидны. Одна из них — это то, что при атаках большими объемами трафика, это т. н. распределенные атаки типа «отказ в обслуживании», или DDOS, когда создаются очень большие, просто огромные группы из, возможно, небольших компьютеров, это могут быть веб-камеры у вас дома, это может быть ваш ноутбук, это может быть ваша приставка к телевизору, подключенная к Интернету, которая в какой-то момент была заражена вирусом и теперь будет отправлять трафик в определенную точку. При использовании старой модели, т. н. технологии Unicast, весь этот трафик пойдет к одному и тому же адресату, потому что он и есть только один. А это значит, что вся такая атака может быть направлена на определенную систему-жертву, которая будет

перегружена и не сможет должным образом отвечать на запросы. Если использовать технологию Unicast в рамках такой модели, то трафик со всех этих приставок в красной области будет доставлен в эту красную конечную точку, извините, в эту конечную точку в правом верхнем углу, а эти камеры в левом нижнем углу будут атаковать сервер в левом нижнем углу. То есть трафик распределяется между всеми этими узлами. А если вам нужно атаковать 1800 узлов, то, чтобы их атаковать, чтобы перегрузить их, вам понадобится очень уж большая сеть из веб-камер, приставок и ноутбуков. И такая система перестанет работать, только когда будет перегружена вся полностью. То есть такой способ масштабирования до тысяч серверов обеспечивает неплохую устойчивость против такого рода атак.

Еще одна особенность, которая может быть не сразу очевидна, это то, что если мы возьмем сервер в правом верхнем углу и уберем его полностью из сети, то все маршрутизаторы на пути к нему будут уведомлены об этом. Сервера в правом верхнем углу больше нет. То есть трафик в таком случае будет направляться на следующий ближайший узел, то есть этот узел в правом нижнем углу. И это все происходит автоматически, когда прекращают приходить уведомления по протоколу граничного шлюза, или BGP, это говорит о том, что этого узла больше нет, и тогда вся сеть маршрутизаторов автоматически переключается, мол, давайте тогда посылать трафик по этому маршруту. И все просто незаметно продолжает работать. Разумеется, на сервер в правом

нижнем углу будет поступать больший объем трафика, но это не проблема, потому что для каждого из них обеспечивается избыточное резервирование. Каждый сервер способен обрабатывать в разы больше трафика, чем тот объем, который поступает на него обычно. Так что это не проблема. И здесь есть такая особенность, что я как оператор корневого сервера могу вывести из эксплуатации наш узел в Англии, в Лондоне, а вы этого даже и не заметите. Все будет по-прежнему нормально работать, а мы сможем провести техническое обслуживание. Мы можем установить новую операционную систему, или поменять отказавший жесткий диск, или еще что-то сделать с нашим сервером, а потом просто включить его снова, когда все будет налажено. И вот этот узел снова работает. Появляется более короткий маршрут и трафик начинает снова направляться на сервер, который возобновил свою работу. То есть это дает нам очень гибкие возможности в том, что касается технического обслуживания таких серверов. Если вернуться на 25 лет назад в прошлое, когда серверов было всего 13, если бы мы тогда отключили всего один наш сервер, то это немного снизило бы отказоустойчивость системы корневых серверов в целом, и это можно было бы заметить, если внимательно смотреть, но сегодня обеспечивается гораздо большая гибкость, так что все это делать гораздо удобнее. Нам даже не нужно информировать друг друга о том, что мы проводим техническое обслуживание, потому что все автоматически возвращается в систему маршрутизации и просто продолжает работать. Пожалуй, на этом я передам слово Уэсу,

который расскажет нам немного о консультативном комитете системы корневых серверов и о его группе подготовки. Спасибо.

УЭС ХАРДАКЕР (WES HARDAKER): Больш

ое спасибо, Лиман. Меня зовут Уэс Хардакер. Я представляю оператора корневого сервера в Институте информатики Университета Южной Калифорнии, кроме того, я выступаю еще в нескольких других ролях, о которых я вам расскажу через минутку, когда мы подойдем к соответствующему слайду, но сейчас мы поговорим о том, что собой представляют RSSAC и группа подготовки RSSAC. То есть мы немного оставим технические темы и перейдем к административным вопросам.

Итак, что такое RSSAC? Его роль состоит в консультировании сообщества и Правления ICANN по вопросам, связанным с функционированием, администрированием, безопасностью и целостностью системы корневых серверов Интернета. Это очень аккуратная формулировка и, если задуматься, очень узкая. Мы не консультируем по вопросам, связанным с DNS. Мы не даем рекомендаций в отношении еще чего-то, связанного с ICANN. Мы консультируем только по вопросам, касающимся системы корневых серверов, и все. Ни IANA, ни каких бы то ни было еще частей ICANN.

С учетом этого, чем RSSAC занимается, а чем нет? Во-первых, так сказать, мы стремимся выдавать рекомендации, как я только что упомянул, в первую очередь Правлению. Почти все наши рекомендации как бы предназначены для Правления, хотя в общем мы можем давать рекомендации и сообществу. У нас были, к примеру, какие-то документы, в которых сообществу рекомендовалось заняться какими-то последующими исследованиями или продолжить изучение каких-то вопросов. Операторы корневых серверов в RSSAC представлены, но сам RSSAC как таковой никакой операционной деятельностью не занимается. Мы на самом деле не обсуждаем ничего из того, о чем только что говорил Лиман, ничего, что касалось бы технологии Anycast или того, например, как мы организовываем хостинг наших служб. Это не касается RSSAC. RSSAC — это на самом деле просто та часть системы корневых серверов, которая занимается политиками.

Наше руководство состоит из Джеффа Осборна (Jeff Osborn), который занимает должность председателя RSSAC и который сидит напротив меня, и заместителя председателя RSSAC, которого вы уже слышали, это Кен Ренард. А сам комитет состоит из основных представителей от всех операторов корневых серверов, по одному представителю и по одному дублеру представителя. Так что, как, кажется, уже сказал Кен, есть 13 операторов корневых серверов или 12 организаций-операторов корневых серверов, что дает нам в общей сложности 24

представителя от операторов корневых серверов в RSSAC. Кроме того, у нас есть представители при комитете от других органов. Я подробнее расскажу об этом на следующем слайде.

И еще есть группа подготовки RSSAC, о которой я расскажу подробно, кажется, Лиман уже о ней немного говорил, или это был на самом деле Кен, извините. Но это группа волонтеров из числа экспертов в предметной области, и именно в этой группе у нас выполняется большая часть нашей работы. Сам RSSAC на самом деле не готовит много [документов в последнее время]. Мы перенесли почти всю эту работу, чтобы привлечь больше людей в помощь нам. Через минуту я еще к этому вернусь. Членов группы подготовки RSSAC утверждает RSSAC на основе подаваемых ими заявлений о заинтересованности. То есть они подают заявления о заинтересованности [неразборчиво] еще на следующем слайде.

Итак, мы поддерживаем взаимоотношения с рядом других организаций, которые назначают к нам своих представителей. У нас есть такие представители от других организаций, это люди, которые помогают нам непосредственно в RSSAC. Один представитель от оператора функций IANA, то есть PTI. Один от специалиста по обслуживанию корневой зоны, то есть компании Verisign, которая, конечно же, также сама является оператором корневого сервера. То есть в RSSAC у нее две роли. У нас есть представитель от Совета по архитектуре Интернета, от IETF. И еще у нас есть представитель от консультативного комитета по безопасности и стабильности, или SSAC. У нас есть также наши

представители в других органах. У нас есть представитель от нашего комитета в Правлении ICANN. На самом деле эту роль сейчас выполняю я. То есть я являюсь представителем в Правлении ICANN. Еще у нас есть наши представители в номинационном комитете ICANN, в постоянном комитете потребителей и в комитете по анализу изменений корневой зоны. Для последнего из перечисленных комитетов используется аббревиатура RZERC, это еще один комитет, который занимается рассмотрением того, как могут работать изменения системы корневых серверов. Он отличается от RSSAC, который занимается скорее тем, как работает система. RZERC отвечает за рассмотрение того, каким образом могут вноситься технические изменения, если нам потребуется их вносить.

Итак, что из себя представляет группа подготовки RSSAC? Я уже говорил об этом. В нее на данный момент входит свыше 100 человек, и все они — специалисты в области DNS. Это люди, которые хорошо понимают эту технологию. Именно к ним мы обращаемся, когда нам нужно какое-то глубокое понимание того, как мы можем усовершенствовать DNS или как мы можем лучше ее понять в том, что касается системы корневых серверов. Все они в свое время подали публичные выражения заинтересованности, в которых указали свой опыт, имеющий отношение к DNS, а также причины, по которым они хотят принять участие в работе группы подготовки RSSAC, и уровень своей квалификации. И, что самое главное, работа каждого из них получает общественное

признание. То есть во всех наших документах RSSAC, если вы посмотрите, там внизу у нас есть раздел, в котором указаны авторы, это, по сути, все члены группы подготовки RSSAC, которые внесли свой вклад в работу над этим документом. И вы увидите, что тех, кто внес свой вклад в работу над тем или иным конкретным документом, зачастую очень много, потому что нам очень многие помогают, а мы очень ценим их мнения.

Цель этой группы подготовки, на самом деле... как я уже сказал, это такая группа специалистов по DNS, которые свой разносторонний опыт привносят в работу над теми документами, которые мы публикуем, что позволяет нам гарантировать, что все будет продумано глубоко и в полном объеме, а не в каких-то узких пределах, потому что, к примеру, если взять всего несколько авторов, то они не смогут обеспечить такое разнообразие. Мы также обеспечиваем транспарентность в том, кто выполняет эту работу. Обычно вся работа в группе подготовки ведется в открытом режиме. Это действительно концептуальная основа того, как осуществляется работа в RSSAC.

Далее я расскажу вам об эволюции управления системой корневых серверов. То есть это в меньшей мере касается RSSAC, за исключением того, что RSSAC как бы начал это. Произошло следующее — когда мы назначили оператора 12-го корневого сервера, это было очень давно, более 20 лет назад, тогда не было никакой процедуры для добавления или удаления операторов, когда это может понадобиться. Так как же нам изменить это, кто

этим будет заниматься? И в июне 2018 года RSSAC решил как бы возобновить эту работу, чтобы выяснить, как нам поступать в таких случаях в будущем? Как мы будем решать эту проблему? И мы подготовили документ RSSAC37, в котором описывался подход к управлению системой корневых серверов, в том числе возможность добавлять или удалять из этой системы операторов корневых серверов. Мы также подготовили набор принципов, о котором, кажется кто-то уже говорил и который касался нашей работы и правил, которые мы применяем к системе корневых серверов, например, мы не фильтруем трафик, мы отвечаем на все поступающие запросы.

После того, как этот документ был опубликован, Правление ICANN приняло в отношении него решение, руководствуясь рекомендациями, которые были изложены в документе RSSAC38, и корпорации было поручено создать рабочую группу по управлению системой корневых серверов. Эта работа сейчас выполняется. Позже на этой неделе состоится пять заседаний, они будут проводиться в открытом формате, если вас они заинтересуют, и на этих заседаниях мы разрабатываем модель управления, которая позволяла бы сохранить эти 11 руководящих принципов, которые мы сформулировали в документе RSSAC37, в т. ч. в том, что касается разнообразия, сотрудничества и независимости, и в этом участвуют представители не только заинтересованных сторон из системы корневых серверов, но также и других организаций, о которых мы расскажем на другом

слайде через минутку. И по итогам этой работы будет подготовлен документ ICANN, который также будет вынесен на общественное обсуждение ICANN, то есть после того, как будут документально оформлены результаты работы группы по управлению, сообществу также будет предоставлена возможность прокомментировать результаты этой работы.

Так что заинтересованные стороны системы корневых серверов, мы на самом деле определили это в документе RSSAC37, и, конечно же, все сообщество ICANN, все очень заинтересованы в надлежащей работе системы корневых серверов, как и собственно операторы корневых серверов. Мы поддерживаем работу этой службы, так что очевидно, что мы заинтересованы в том, чтобы она продолжала работать, а также в этом заинтересованы и Инженерная проектная группа Интернета, или IETF, и Совет по архитектуре Интернета, потому что именно IETF на самом деле занимается разработкой, подготовкой и поддержанием спецификаций DNS и изменений в них. На прошлой неделе состоялась встреча в Дублине. Многие участники IETF присутствуют здесь на этой неделе, и они явным образом очень заинтересованы в успешной работе системы корневых серверов, поскольку именно они обеспечивают поддержку DNS в целом. В рабочую группу по управлению системой корневых серверов входит множество разных людей, которые представляют разные организации, то есть по одному члену от каждого из операторов корневых серверов, есть два члена от группы заинтересованных

сторон-регистратур, два члена от ccNSO и два члена от Совета по архитектуре Интернета, который я упоминал минуту назад, кроме того, у нас есть еще несколько представителей. Эти синие кружки справа, три синих кружка, это два представителя от Правления ICANN, один представитель от специалиста по обслуживанию корневой зоны и один представитель от IANA.

И на этом мы на самом деле подходим к завершению всей этой презентации. Через минуту мы ответим на вопросы, а вот для вас несколько ресурсов. Более подробную информацию о самом комитете RSSAC можно посмотреть на нашей странице, которая у нас расположена на сайте ICANN, конечно же, и на этой странице у нас есть список часто задаваемых вопросов. Он составлен так, чтобы его было легко читать, так что если вы хотите узнать больше о системе корневых серверов, то там на самом деле полезная информация, с которой следует ознакомиться от начала до конца, потому что она поможет избежать некоторых распространенных неправильных представлений. У нас также есть список рассылки ask-RSSAC@ICANN.org, если у вас есть вопросы о системе корневых серверов или если вы хотите узнать подробнее о ресурсах, или еще нам иногда пишут и задают вопросы о том, как выполнить развертывание системы корневых серверов ближе к той или иной стране или региону, и обычно мы рекомендуем почитать список часто задаваемых вопросов по этой теме, потому что это один из [неразборчиво]. Если вас интересует более подробная информация о группе подготовки, особенно если вы хотите

присоединиться к работе группы подготовки, то у нас есть страница и для этого, а также адрес электронной почты RSSAC-membership@ICANN.org. Если вас интересует возможность стать членом группы подготовки, то мы попросим вас прислать выражение заинтересованности, которое затем будет направлено на рассмотрение в комитет по членству в группе подготовки. Как я уже говорил, обычно мы ищем специалистов в области DNS или в какой-то еще предметной области, чтобы вы могли принести пользу группе подготовки в работе над нашими документами. На этом хочу спросить, есть ли у кого-то какие-то вопросы? Иногда мы делаем перерыв посреди презентации, а сейчас не сделали. Вопросы по поводу чего-то из того, о чем шла речь, по поводу каких-либо технических или административных моментов.

УЛЬРИХ ВИССЕР: В модуле Q&A вопросов сейчас нет. Хочу только напомнить, поднимайте руки в зале Zoom или пишите свои вопросы в модуле Q&A. Я буду их зачитывать. А если вы здесь, в аудитории, выходите к микрофону и... да, прошу вас. Доброе утро.

ОМАР ШУРАН: У меня только вопрос, который касается той информации о технологии Anycast. Это то же самое, что корневые сервера под управлением ICANN, то есть IMRS, или нет?

УЭС ХАРДАКЕР: Anycast — это название общей технологии маршрутизации, которую используют все операторы корневых серверов. Резолвер все равно скажет, что ему нужен адрес IMRS или адрес сервера Института информатики Университета Южной Калифорнии, и тогда, когда вы попытаетесь обратиться к инфраструктуре этого конкретного оператора корневого сервера, вас перенаправят куда-то в зависимости от того, где вы находитесь. То есть все эти 12 операторов... были такие периоды времени, когда эту технологию использовали только некоторые операторы корневых серверов. Я вам честно признаюсь, что мы были последним оператором, перешедшим на использование технологии Anycast. Мой предшественник считал, что будет лучше отложить такой переход на очень долгое время, чтобы убедиться в стабильности такого механизма, и сейчас мы знаем, что он очень стабилен. Его использует не только система корневых серверов.

УЛЬРИХ ВИССЕР: В модуле Q&A вопросов нет. Будут еще вопросы из зала?

УОРРЕН КУМАРИ (WARREN KUMARI): Почем

у операторы корневых серверов занимаются тем, чем они занимаются? Я хочу сказать, что это, кажется, довольно большие затраты и все такое. Почему вы тратите на эту работу свои деньги и время?

УЭС ХАРДАКЕР: Это прекрасный вопрос от Уоррена, который, кстати, является членом группы подготовки RSSAC и знает ответ на него. Но спасибо за вопрос. Реальность такова, что мы занимаемся этим уже долгое время и мы делаем это исключительно во благо Интернета. Точка. Это недешево. Нам за это не платят. В моей организации у меня каждый год проходит битва за бюджет, когда решается, сколько мы можем выделить на закупку новой инфраструктуры и все такое. Это недешевый процесс. Итак, Лиман

ЛАРС-ЙОХАН ЛИМАН: Если можно, я продолжу дальше. Это началось еще тогда, когда Интернет был совсем другим. Сегодня в Интернете ведется большой бизнес и передается много трафика. Но когда создавалась система DNS и возникла необходимость в корневых серверах, когда была создана DNS, мы стали нуждаться в корневых серверах, которые обслуживали бы верхний уровень, самый высокий и очень маленький уровень DNS. И я должен признаться, как только что сделал Уэс, что когда компания Netnod начиналась как оператор корневого сервера, то есть не Netnod, потому что она возникла уже позже на основе того первого оператора, а это был Королевский технологический институт в Стокгольме, это была рабочая станция, вот такого размера компьютер, который стоял на столе в офисе. Настолько это все было тогда незначительным. Наши сегодняшние системы совершенно не такие. Поддержание

их работы — абсолютно профессиональная деятельность. У нас этим занимаются десятки сотрудников, за 30 лет это выросло до таких масштабов, и мы постепенно следовали за этим ростом. Но начиналось все с простой просьбы со стороны IANA, мол, не могли бы вы для нас это сделать? Конечно. И мы поняли, что это продолжается уже как очень важная услуга для сообщества Интернета, и мы хотим ее предоставлять.

Пользу приносит то, если вернуться к той части презентации, которую провел Кен, что у нас есть самые разные организации. Как вы сказали, Кен, у нас есть государственные органы, у нас есть коммерческие и некоммерческие организации, учреждения сектора науки и образования. У каждого из нас своя разная финансовая основа для такой работы. То есть оператор Netnod находит деньги для того, чтобы предоставлять эту услугу, по-своему, а Университет Южной Калифорнии — как-то иначе, а агентство [неразборчиво] — как-то еще, а у коммерческих компаний еще какие-то варианты. Так что даже если бы финансовые системы претерпели бы какие-то радикальные изменения, то это затронуло бы не всех операторов корневых серверов, не сразу и не одинаково. То есть это такого рода разнообразие, которое очень важно для жизнестойкости, для возможности поддерживать эту услугу в течение очень длительного времени. Спасибо.

УЭС ХАРДАКЕР: Есть еще вопросы?

КЕН РЕНАРД: Я просто считаю необходимым добавить еще один ответ к тому, который уже был дан, потому что Уэс работает в университете, а я президент некоммерческой компании, а все дошло уже до того, что когда вы в Интернете говорите, что делаете что-то бесплатно, то люди буквально мне в лицо этим швыряют и говорят, мол, Facebook тоже денег не берет. Я просто хочу заявить совершенно однозначно. Наша организация разрабатывает программное обеспечение, необходимое для работы Интернета, и раздает его. Все наши расходы покрываются за счет тех клиентов, которые приходят к нам за помощью и оплачивают услуги поддержки, что помогает оплачивать разработку бесплатного программного обеспечения, за которое никто не платит. У нас по всему миру насчитывается по разным оценкам около полутора миллиона пользователей программного обеспечения BIND. Около 100 из них платят нам какие-то деньги за поддержку. Кроме того, мы берем 20% тех денег, которые мы зарабатываем на поддержке BIND и другого программного обеспечения с открытым кодом, и тратим их на поддержание работы системы корневых серверов. Так что когда мы говорим, что мы не берем за это денег, я не имею в виду, что мы потом зарабатываем на продаже всей вашей конфиденциальной информации. Никакая конфиденциальная информация из рук в руки не переходит. Никакая вообще информация из рук в руки не переходит. Никакой контент из рук в

руки не переходит. Все, что мы делаем, это выдаем адрес авторитативного сервера, которые знает, по каким адресам расположены домены верхнего уровня. То есть когда мы говорим, что мы некоммерческая организация, которая не зарабатывает деньги, то это самое честное заявление, которое вы когда-либо услышите. Мы действительно некоммерческая организация и действительно не зарабатываем деньги. Мы буквально так и работаем, а если ваш цинизм мешает вам верить, то не слушайте. Мы буквально так и работаем, у меня работает компания из 19 сотрудников из 19 разных стран, и все они искренне верят в то, что Интернет с единым источником имен — это достаточная ценность, чтобы зарабатывать меньше денег в некоммерческой организации. Мы действительно преданы нашей миссии.

ХАНС ПЕТТЕР ХОЛЕН: Если вопросов больше нет, то я могу дать еще один ответ, потому что нас 12 операторов и у всех у нас разные ответы, не так ли? Я, то есть моя организация, мы являемся оператором корневого сервера K. Давайте чтобы я больше не играл с этой службой. Мы организация, основанная на членстве. У нас около 20 000 членов, которые платят за работу корневого сервера K наряду с другими службами. Если вам интересно, сколько это стоит, вы можете взглянуть на наши ежегодные финансовые отчеты или на план деятельности и бюджет, и посмотреть, какие там указаны затраты. Если разделить их на количество членов, то можно увидеть, что получается что-то около 50 евро в год. Есть множество разных

способов финансирования таких затрат, что является одной из сильных сторон той системы, в которой все мы по-разному участвуем. Было бы очень необычно, если бы все столкнулись с каким-то финансовым кризисом в одно и то же время.

УЛЬРИХ ВИССЕР: У нас есть вопрос в модуле Q&A. Какие отношения RSSAC поддерживает с другими группами, если позволите, в особенности с некоммерческими сторонами?

УЭС ХАРДАКЕР: RSSAC проводит встречи с другими группами интересов, которые с нами как бы непосредственно связаны, потому что, как, кажется, уже сказал Кен, мы обслуживаем корневую зону IANA, не так ли? Мы обязуемся в качестве источника данных использовать IANA. Большинство групп интересов ICANN, которые представляют домены верхнего уровня, например, будь то домены ccNSO или GNSO, когда им нужно реализовать какие-то изменения функциональности доменов верхнего уровня, они работают непосредственно с ICANN. Мы работаем с IANA. Это то, чему мы уделяем больше всего внимания в делах, касающихся действительно операционных вопросов. Мы регулярно проводим встречи с консультативным комитетом по безопасности и стабильности. Мы регулярно проводим встречи с Правлением ICANN. На этой неделе у нас состоялась встреча с Организацией поддержки адресов. Мы проводим встречи по мере

необходимости. Кроме того, некоторое время назад у нас состоялась также встреча с ALAC. Сегодня утром у нас была встреча с GAC. То есть по мере необходимости. Обычно мы не любим проводить встречи, если нет реальной необходимости. То есть в этот раз мы не будем проводить встречу с Правлением ICANN. Это то, что мы делали последние три или четыре раза. Никакой непосредственной, срочной необходимости проводить встречу между нашими двумя организациями сейчас нет. Мы не хотим, так сказать, впустую тратить чье-то время и просиживать бессодержательные заседания.

ЛАРС-ЙОХАН ЛИМАН: Но я хочу подчеркнуть, что мы всегда приветствуем любое взаимодействие. Если возникают какие-то проблемы, которые, по вашему мнению, касаются операторов корневых серверов. Пожалуйста, приходите к нам, мы будем рады обсудить это. И если при этом возникнет необходимость провести встречу, то мы будем рады ее организовать. Но мы не проводим встречи на регулярной основе, если у нас нет на столе проблем, которые необходимо обсудить. Как сказал Уэс, в этом контексте встреч проводится достаточно. Нам не нужно прибавлять к этому какие-то заседания просто ради заседаний. Но мы действительно очень приветствуем любое взаимодействие с другими группами и частными лицами. Если у вас есть какие-то вопросы, касающиеся системы корневых серверов, остановите меня в коридоре и спросите. Вы найдете меня. Я ростом два метра. Меня легко найти.

КЕН РЕНАРД: Операторов корневых серверов, то есть организаций, которые выполняют функции операторов корневых серверов, всего 12. Семь из них присутствуют сейчас в этом зале, так что мы можем поднять руки. Мы здесь.

УЛЬРИХ ВИССЕР: У нас есть еще один вопрос в модуле Q&A. Не могли бы вы рассказать подробнее об операторах Anycast и о их взаимоотношениях с RSSAC, если таковые взаимоотношения существуют?

ЛАРС-ЙОХАН ЛИМАН: Операторы Anycast. Это мы. Мы являемся операторами сети, в которой используется технология Anycast. Только учтите, что нам не нужно ничего особенного делать с маршрутизаторами в Интернете. Итак. В случае с оператором Netnod мы поддерживаем работу 75 серверов в разных точках, это наши сервера. Мы являемся их операторами. Мы доставляем их в точку установки. У нас есть специалисты, которые помогают нам монтировать их в стойки и подключать все необходимые кабели — сетевые, питания, что там еще. А затем мы входим в систему на сервере и выполняем нужные операции, и сервер объявляет об установлении отношений... сначала выполняется согласование отношений, а потом он объявляет об этом ближайшему маршрутизатору перед

ним в сети. Он объявит о том, что теперь корневой сервер Netnod в сети и у него такой-то IP-адрес. Пожалуйста, присылайте мне трафик. Так что в каком-то специальном операторе Anycast нет необходимости. Различные операторы корневых серверов поддерживают работу каждый своего собственного подмножества из этих 1800 серверов. И каждый из таких установленных серверов может представлять собой больше, чем один физический корпус. Это может быть несколько серверов и локальный маршрутизатор для этого оператора корневого сервера. Такой кластер, то есть такое сочетание серверов, объявит о своем присутствии ближайшему маршрутизатору. Присылайте мне трафик. И больше ничего нужно. Спасибо.

УЛЬРИХ ВИССЕР: Есть ли какие-то правовые или технические требования, которые операторы корневых серверов должны выполнять постоянно, помимо поддержания непрерывной готовности?

[ХАНС ПЕТТЕР ХОЛЕН:] Знаете, мы часто говорим,, что на Интернет не распространяется регулирование или юрисдикция какого-либо правительства. И это действительно так, если говорить о процессах разработки политик в ICANN или в региональных интернет-регистратурах или каких-то еще органах. Но абсолютно каждый оператор является организацией той или иной правовой формы в какой-то стране и на него распространяются законы этой страны. RIPE NCC

находится в Европе, поэтому мы обязаны соблюдать европейское законодательство. Мои коллеги, присутствующие здесь, находятся в США. Они обязаны соблюдать законодательство США. В этом законодательстве наша работа не регулируется в деталях. Но принимаются новые законы, которыми вводятся новые требования в отношении работы критической инфраструктуры. Это происходит разными темпами в разных странах. Так что сейчас мы живем в интересное времена.

ЛАРС-ЙОХАН ЛИМАН: Я хотел бы добавить к этому, потому что вопрос также касался технических спецификаций. И да, несколько технических спецификаций есть. Мы, к примеру, обязаны использовать протокол DNS, который был указан в определенном техническом стандарте инженерной проектной группой Интернета, то есть IETF. Кроме того, существует документ, в котором описывается, как корневые сервера должны отвечать на входящие запросы DNS. Этот документ был опубликован Советом по архитектуре Интернета в сотрудничестве с операторами корневых серверов. А группа подготовки RSSAC, о которой мы уже говорили, разработала документ, в котором описываются ожидания в отношении уровня обслуживания и который был опубликован только что или будет опубликован в самое ближайшее время. Если он еще не был опубликован, то будет опубликован совсем скоро, и в нем описываются условия, которые, как ожидается, операторы корневых серверов должны выполнять, то есть мы должны

выдавать ответы в соответствии с определенными техническими требованиями в том, что касается времени отклика. А также сколько времени должно проходить с момента выхода новых данных до обновления их на конечных узлах и тому подобные вещи. Так что да, какие-то технические ожидания существуют.

УЭС ХАРДАКЕР: Документ, который вы имеете в виду, кажется, называется RSSAC047. Я бы только добавил еще немного и сказал, что мы не можем просто вести мониторинг готовности наших устройств к работе. Я думаю, вы были бы очень впечатлены, если бы узнали, что нужно делать для управления любой сетью, будь то корневой сервер, или сервер DNS, или файловый сервер, или веб-сервер . Сколько всяких графиков мы вынуждены создавать, сколько всяких уведомлений должны отслеживать, работает ли что-то или не работает, или работает слишком медленно, или же какое-то оборудование перегружено по объемам трафика. Это все те вещи, от которых я моментально просыпаюсь. Заканчивается ли место на диске? Есть множество мелочей, которые важны в поддержании работы инфраструктуры, и если что-то вдруг отказывает, то об этом необходимо узнавать сразу же. И когда возникает что-то новое, что мы не могли предвидеть заранее и для чего не предусмотрели мониторинг, то это первое, что я делаю, я записываю новый параметр, который необходимо отслеживать, а у меня есть коллега, который гениально составляет очень интересные графики, и я весь день их разглядываю.

ЛАРС-ЙОХАН ЛИМАН: Есть очень много разного опыта. Я уже говорил, что у нас поддержанием этой работы занимается где-то с 10 человек, и у каждого оператора корневого сервера есть множество таких специалистов. Это не только те несколько человек, которые присутствуют здесь, в этом зале, мы те люди, которые занимаются всем этим, опять же, я очень редко прикасаюсь к каким-то техническим деталям работы корневых серверов. Но опыт, накопленный операторами корневых серверов в управлении серверами DNS, можно измерять, наверное, человеко-столетиями. Если взять весь тот опыт, который накоплен в обеспечение работы DNS, в анализе содержимого DNS и потоков трафика DNS, в анализе содержания пакетов, в процедурах обновления и мониторинга, а также управления трафиком в сети, то весь этот опыт сейчас используется для обеспечения работы корневых серверов. И во всех наших организациях накоплен такой опыт и такие знания, так что это не просто несколько человек, которые собрались за этим столом.

[ЮСУФ:] Меня зовут Юсуф, я из [Университета Мармара] в Стамбуле. У меня такой вопрос: как вы видите, что в том или ином регионе есть достаточно реплик? Например, в Стамбуле есть семь реплик. Как вы определяете, достаточно ли этого, кто это определяет?

ХАНС ПЕТТЕР ХОЛЕН: Несмотря на то, что я могу говорить только с позиции одного оператора корневого сервера, а именно корневого сервера K, но центр RIPE NCC также поддерживает работу глобальных измерительных сетей, которые насчитывают свыше 13000 единиц измерительного оборудования. И мы используем данные этих измерительных сетей, а также данные из других источников, чтобы анализировать время отклика из разных мест, в которых расположено такое измерительное оборудование в этих сетях, чтобы контролировать качество обслуживания по всей топографии наших сетей. И эти данные могут использовать все операторы корневых серверов, некоторые используют данные других измерений, чтобы видеть, находится ли уровень предоставляемых ими услуг на том уровне, который им нужен. Если у вас есть особый интерес к этой теме, тот центр RIPE NCC также принимает открытые заявки на хостинг узлов, так что вы можете связаться с нами, чтобы установить один из них, например, у своего локального интернет-провайдера. Если вы считаете, что их должно быть больше, вы можете связаться с нами, чтобы обсудить это. У других операторов корневых серверов для этого могут использоваться другие процедуры, и это тоже часть этого замечательного разнообразия. У нас нет какого-то единого подхода, у нас есть 12 разных подходов к решению таких задач, так что даже если мой подход неправильный, значит, возможно, кто-то другой сделает это лучше.

УЭС ХАРДАКЕР: Следует отметить, что до технологии Anycast Интернет тоже нормально работал, и серверов было 13. То есть на самом деле не так уж и обязательно, чтобы один из них располагался рядом с вами. Как мы уже говорили до этого, DNS-сервер у вашего интернет провайдера работает быстро благодаря кэшированию. Это не потому, что корневой сервер расположен близко к вам, потому что на самом деле до корневой зоны доходит очень небольшое количество запросов, так что возможность связаться именно с корневой зоной не является критически важной.

[ТАХИР:] Здравствуйте, это Тахир из Технического университета Стамбула. Я хотел бы задать один вопрос — при использовании Anycast у нас по всему миру распределены эквивалентные друг другу сервера. А какими данными или какой информацией они располагают? Возникают ли у вас какие-либо проблемы с синхронизацией и как часто необходимо все синхронизировать? У вас есть для этого какие-то онлайн или офлайн процедуры?

КЕН РЕНАРД: Да, все эти сервера нужно время от времени синхронизировать. Обычно корневая зона обновляется где-то от одного до трех раз в день. Мы действительно измеряем, насколько быстро это происходит, и публикуем результаты этих измерений в документе RSSAC002. То есть обычно корневая зона публикуется и сразу же распространяется по всей инфраструктуре. Рассылка всех этих

данных занимает секунды. Но это может быть по-разному, если та или иная реплика сервера находится в каком-то удаленном месте, с которым не очень хорошая связь, то может пройти какое-то время, прежде чем эти данные туда попадут. То есть у нас редко бывают какие-то проблемы с такой синхронизацией. Так бывает. Но есть параметры протокола DNS, которые определяют, что, если ваша версия этой зоны слишком устарела, она исключается из обслуживания. То есть мы хотим не допустить ситуации, в которой данные могли бы оказаться слишком старыми, особенно если недействительными станут подписи DNS, потому что у них тоже есть срок действия.

УЭС ХАРДАКЕР: Следует отметить, что каждую запись в корневой зоне разрешается сохранять в памяти в течение двух дней, прежде чем необходимо будет запрашивать ее снова. Так что нужно помнить, что, по сути, для всех записей гарантируется действительность в течение двух дней.

ЛАРС-ЙОХАН ЛИМАН: Опять же, здесь играет свою роль технология Anycast, потому что мы следим за всеми системами с помощью наших средств мониторинга, и один из тех параметров, которые мы контролируем, это были ли данные должным образом обновлены. Если мы замечаем, что они не были обновлены должным образом и мы не можем быстро это исправить, тогда мы их просто

отключаем. Мы отключаем этот узел и трафик на него больше не передается. Они будут передаваться на другой узел, на котором данные обновлены, а на этом мы сможем исправить проблему, пока он будет отключен. И когда мы все исправим, тогда мы снова включим его в систему. Так что и здесь технология Anycast работает на вашу и нашу пользу.

[ДЖУНАИД МИЯДЖИ (JUNAID MIYAJI):]

Здравс

твуйте, меня зовут Джунаид Мияджи, я из Бангладеш, я впервые участвую в конференции ICANN на месте. И у меня вопрос. Несколько дней назад мы столкнулись с проблемой в нашей стране, когда у нас не работал Интернет. И тогда я обнаружил, что мы от всего Интернета были отключены, но наша сеть IX работала нормально. Однако разрешение DNS у нас тогда не работало, потому что без подключения DNS к Интернету невозможно выполнять разрешение доменных имен. Есть ли у вас какие-то варианты или какие-то возможности сделать так, чтобы корневая зона работала с сетями IX, я имею в виду локальный Интернет, или какие-то еще способы, возможно, чтобы индивидуальный пользователь, такой как я, мог кэшировать записи корневой зоны, особенно для таких стран, как наша? Спасибо.

ЛАРС-ЙОХАН ЛИМАН: Да, да и да. Чтобы выполнить разрешение DNS для обычного имени, нужен не только корневой сервер, но и все остальные уровни под ним. А там дальше идет взрывной рост количества имен, так что вам пришлось бы кэшировать очень большие объемы данных. При этом сама корневая зона представляет собой открытую информацию, которую вы можете загрузить. Я могу позже показать вам, как это сделать. И есть документ IETF, в котором описывается, как работать с такой зоной на вашем локальном резолвере. Вы можете поднять эту корневую зону на своем резолвере, так что ему не придется обращаться к корневому DNS-серверу. Тогда вы будете делать все самостоятельно. Вы сможете регулярно копировать эту зону и выполнять т. н. передачу зоны с каких-то открытых узлов. У операторов есть такие узлы, которые позволяют вам копировать эту зону автоматически. И тогда, если ваша сеть не будет работать и вы не сможете скопировать новую версию, старая версия продолжит использоваться еще, кажется, неделю или около того. Так что да, способы обойти эту проблему существуют. Однако мне кажется, что во время этого отключения Интернета корневые сервера в Бангладеш, возможно, продолжали работать, просто следующее звено в сети, возможно сервер com или... Извините, я не помню, какой домен верхнего уровня у Бангладеш. Но, я повторюсь, может не работать какой-то из уровней ниже, то есть это те серверы, которые расположены за пределами Бангладеш, и тогда мы не сможем вам с этим помочь.

УЭС ХАРДАКЕР: В Бангладеш на самом деле шесть корневых серверов, так что, скорее всего, они должны были продолжать работать.

[ДЖУНАИД МИЯДЖИ:] Извините, но, к сожалению, я все перепробовал, и то, как вы сказали, чтобы поднять собственные сервера DNS и кэшировать записи корневой зоны, и чтобы обеспечить разрешение имен для них. К сожалению, у меня ничего не получилось, и именно поэтому я задал этот вопрос. Кроме того, во время этого отключения Интернета у нас... Я перепробовал тысячу способов, чтобы придумать, как сделать так, чтобы это заработало через Anycast, но оно все равно не заработало. Кроме того, тот способ разрешения записей, о котором вы говорите, это у меня тоже не заработало. Так что я думаю, что я, возможно, допустил какие-то технические ошибки или что-то такое. Так что если есть какая-то возможность связаться с какими-то техническими специалистами, чтобы решить эти проблемы с...

УЭС ХАРДАКЕР: То, о чем вы говорите, это разные вещи. То есть тут есть две составляющие, понимаете? Давайте представим, что вы пытаетесь узнать адрес по имени сайта, например, и что этот сайт работает... давайте я выберу не страну, а, например, Антарктику, хорошо? Если тот или иной регион отключен от Интернета, возможно, в

результате какого-то стихийного бедствия, например, урагана или еще чего-то, возможно, по политическим или каким-то еще причинам, то связаться с ним не получится никак, понимаете? Этот сервер находится в Антарктике, так что если даже у вас и получилось бы узнать его адрес, то он все равно не работает, понимаете? А другой аспект — это то, что если сервер DNS... скажем, вы посылаете запрос для имени example.com, и если сервер DNS для имени example.com расположен в Антарктике и у вас нет с ним связи по какой-то причине, неважно, там, кабель поврежден. Ваш интернет-провайдер начнет с корневой зоны, и оттуда вы ответ получите, потому что там все работает, но корневой сервер не может помочь вам с проблемами доступа где-то еще. Корневой сервер не сможет решить для вас эту проблему.

[ДЖУНАИД МИЯДЖИ:] Спасибо, но я, кажется, что-то пропустил. Это я понимаю. Когда я говорю о сетях IX, я имею в виду, что у нас есть какие-то серверы в наших локальных сетях, вот как у меня есть серверы в Бангладеш, в Даке. То есть разрешение имен должно работать для сайтов, расположенных в Даке, не за пределами Бангладеш, но мне нужно, чтобы работало разрешение для доменных имен, расположенных в Бангладеш. И конкретно эти сайты работали с сетями IX, то есть у нас получалось обращаться к ним непосредственно по IP-адресам, но не по доменным именам, и нам хотелось бы иметь возможность выполнять разрешение с помощью корневой зоны. Вот о чем я спрашивал.

КАРЛ РЕУСС (KARL REUSS): Мы работаем в партнерстве с организацией Packet Clearing House, или PCH, чтобы поддерживать работу многих из наших узлов Anycast. Мы работаем в партнерстве с ними, наши сервера работают на их инфраструктуре, они помогают многим странам организовывать точки обмена трафиком и свои собственные, внутренние DNS-сервера для своих доменов верхнего уровня. Это такого рода задача, когда нужно много всего настроить, чтобы все работало так, как надо, и это сложно тестировать, кроме как в ситуациях, когда ничего не работает. Чтобы все было организовано правильно, нужно будет настраивать множество разных аспектов этих систем. Мы можем поработать с вами. Я знаю, что мы присутствуем в Бангладеш. Мы можем посмотреть на что-то из того, о чем вы говорили, чтобы выяснить, возможно, там что-то не так настроено. Здесь есть несколько разных составляющих, и корневой сервер — только одна из них. Корневой сервер может работать как надо, но там есть еще много чего, с чем могут быть проблемы.

[ХАНС ПЕТТЕР ХОЛЕН:] Если позволите, я только добавлю, что это, на мой взгляд, очень интересная проблема, с которой на практике сталкивались очень немногие страны. Как обеспечить работу инфраструктуры внутри страны, когда нет связи с внешним миром? Некоторые страны тестировали такие ситуации, и высказывались разные подозрения

в отношении причин, по которым они это делали. Кто-то говорит, что это для того, чтобы отрезать свои страны от внешнего мира. Кто-то говорит, что это для защиты своего суверенитета. Само по себе такое тестирование выглядит неоднозначно. Я считаю, что мы как техническое сообщество должны объединить наши усилия и рассмотреть эту проблему, чтобы выяснить, каким образом можно обеспечить работу максимально возможного подмножества сети в условиях кризиса. Потому что в мире есть страны, в которых идут вооруженные конфликты, у нас бывают стихийные бедствия и чего только не бывает. Все, что в наших силах, что мы можем сделать, чтобы понять эту проблему и обеспечить отказоустойчивость Интернета, — я думаю, это стоит сделать. Но, как я уже сказал, корневые сервера — это лишь небольшая часть этой проблемы. Я считаю, что эта задача больше для тех из нас, кто также участвует в другой работе, имеющей отношение к DNS.

КАРЛ РЕУСС: Кажется, у нас действительно многие службы работают через PCH в Бангладеш. Так что создается впечатление, что там уже есть многое из того, что там должно быть, просто, возможно, не до конца настроена конфигурация так, как это должно быть.

УЭС ХАРДАКЕР: К сожалению, ваша проблема заключается не в корневом сервере. Скорее, это что-то в домене .bd или еще где-то в инфраструктуре. Но нужен анализ, чтобы понять где. Есть еще вопросы?

УЛЬРИХ ВИССЕР: Кажется, мы уже превысили наше время. Спасибо всем за участие.

[КОНЕЦ СТЕНОГРАММЫ]