Примечание: Ниже приведены материалы в переводе на русский язык, а их оригинал на английском языке размещен на icann.org. Англоязычная версия этих материалов размещена на сайте icann.org и является официальной версией.

RSSAC — вопросы и ответы

На этой странице приведены ответы на некоторые из самых популярных вопросов о консультативном комитете системы корневых серверов (RSSAC). Эта страница будет обновляться по мере изменения ответов или поступления новых часто задаваемых вопросов.

Если у вас есть вопрос, которого нет в этом списке, или же вы хотите уточнить ответ или получить дополнительную информацию, напишите непосредственно на адрес электронной почты ask-rssac@icann.org. Если вы хотите затронуть какой-то из вопросов, которые уже есть в этом списке, укажите его номер и заголовок.

Список тем

1. Количество операторов

1.1 Почему существует 13 идентификаторов корневых серверов?

В 1985 году корневых серверов было четыре. В период с 1987 года по 1991 год их было семь и все они были расположены в США. К 1993 году их стало восемь. На этом этапе возникла одна проблема. Документ RFC 1035 гласит, что «размер сообщений [DNS], передаваемых по протоколу UDP, ограничен 512 байтами». Введение дополнительных корневых серверов имен означало бы, что ответ на прайминг-запрос превысил бы 512 байт. В документе RFC 1035 не представлено обоснование этого ограничения в 512 байт, однако важно также отметить, что в те времена было распространено требование,

согласно которому IP-пакеты в Интернете не должны были превышать 576 байт.

Операторы корневых серверов поняли, что для того чтобы добавить еще дополнительные серверы, нужно было воспользоваться компрессией имен DNS. Поэтому было внесено предложение выделить корневым серверам имена в зоне домена root-servers.net. К 1995 году девять существовавших тогда корневых серверов были переименованы в a.root-servers.net, b.root-servers.net и т. д. В 1997 году было добавлено еще четыре сервера, таким образом, всего таких идентификаторов корневых серверов (RSI) стало 13.

До 1998 года операторов корневых серверов назначал д-р Джон Постел (Jon Postel), который выполнял функции администратора IANA. После его смерти в 1998 году количество операторов не изменилось, однако несколько из них за эти годы сменили своих владельцев.

Начиная с 1998 года ситуация поменялась в нескольких аспектах. Каждый корневой сервер обзавелся собственным IP-адресом по протоколу IPv6, а ICANN перешла к подписанию зоны с использованием т. н. расширений безопасности системы доменных имен DNS, или DNSSEC. Кроме того, размер сообщений, передаваемых по протоколу UDP, удалось увеличить за счет использования протокола механизмов расширения DNS (EDNS). Вместе эти изменения сделали проблему ограничения размера пакета UDP в 512 байт, а количества RSI в 13 менее актуальной.

В 2002 году консорциум Internet Software Consortium (сегодня он называется Internet Systems Consortium, или ISC) первым среди операторов корневых серверов выполнил развертывание технологии IP Anycast, эксперименты с которой в рамках проекта WIDE проводились и ранее. В дальнейшем его примеру последовали и другие операторы корневых серверов. Технология Anycast позволяет каждому оператору поддерживать работу своей службы с помощью множества отдельных экземпляров серверов. Собственно операторов, или RSI, и сейчас остается 13, но на самом деле по всему миру работает свыше 1000 зеркал Anycast их серверов.

Чтобы лучше понять историю системы корневых серверов (RSS), ознакомьтесь с документом RSSAC023: История системы корневых серверов. Если вас интересует дальнейшее развитие системы корневых серверов, ознакомьтесь с документом RSSAC037: Предлагаемая модель управления системой корневых серверов DNS.

1.2 Какие расчеты лежали в основе ограничения в 13 идентификаторов корневых серверов?

В 1997 году корневые серверы выполняли также роль авторитативных серверов для зон .COM, .NET и .ORG, и эта дополнительная функциональность накладывала важное ограничение на то, сколько таких идентификаторов RSI могло быть всего. Аналогично ограничению на размер прайминг-запроса в корневой зоне, запросы NS RRSET к зонам

.COM, .NET и .ORG не должны были превышать размер в 512 байт, а поскольку эти зоны обслуживались одними и теми же серверами, ко всем ним применялось одинаковое ограничение.

Пакет ответа на запрос DNS также содержит в себе полный текст запроса, на который он отвечает. Ответ на прайминг-запрос в корневой зоне всегда использует 5 байт для раздела запроса. 1 байт используется для параметра QNAME и по 2 для параметров QTYPE и QCLASS, то есть всего 5. Однако для прайминг-запроса для зоны .COM раздел запроса может быть значительно больше.

Назначение	**Байт**
Заголовок DNS	12
Первая запись NS	31
12 сжатых записей NS	(12 * 15) 180
13 записей A	(13 * 16) 208
Раздел запроса, QTYPE и QCLASS	4
Раздел запроса, QNAME	?
	=
	435

Таблица 1. Объяснение байт, используемых в ответе на прайминг-запрос в корневой зоне

435 байта используется, 77 остается для раздела запроса QNAME. В свое время было определено, что 64 байта должно быть достаточно для большинства запросов, отправляемых для доменов .COM, .NET и .ORG. Если добавить еще один сервер, понадобится еще 25 байт, а поскольку 435 + 64 + 25 > 512, было решено не добавлять еще один сервер.

2. Anycast

2.1 Почему у некоторых операторов много зеркал Anycast, а у других операторов всего несколько?

Операторы корневых серверов (RSO) — это независимые организации с разными задачами, моделями работы и источниками финансирования. Этими различиями может объясняться разное количество зеркал Anycast, а также разница в других аспектах работы. Операторы корневых серверов обладают значительной независимостью в том, каким образом они развертывают свои сети; см. документ RSSAC042: Заявление RSSAC

о независимости операторов корневых серверов. Все операторы корневых серверов привержены обязательствам предоставлять услуги DNS высокого качества.

2.2 Каким образом обеспечивается надлежащая репликация корневой зоны? Существует ли риск повреждения файлов корневой зоны какими-либо атаками или вредоносным ПО?

Передача файла корневой зоны от специалиста по обслуживанию корневой зоны (RZM) к отдельным операторам корневых серверов RSO осуществляется по протоколам передачи зоны DNS (протокол AXFR, определенный стандартом RFC 5936, и протокол IXFR, определенный стандартом RFC 1995). Эти сообщения передачи зоны защищаются посредством использования записей ресурсов TSIG согласно стандарту RFC 2845. Это надежный протокол, о каких бы то ни было случаях повреждения данных ничего не известно. Более того, поскольку корневая зона подписывается, неправильные или фальсифицированные ответы могут обнаруживаться валидаторами DNSSEC. Комитет RSSAC призывает использовать DNSSEC во всех случаях, когда это возможно.

2.3 Количество зеркал Anycast неограниченно или есть какой-то предел?

Работа технологии Anycast определена и описана в стандартах RFC 4786 «Работа служб Anycast» и RFC 7094 «Архитектурные соображения использования IP Anycast». Естественного предела количеству узлов в той или иной службе Anycast нет.

2.4 Корневые серверы выполняют репликацию и перепубликацию авторитативной корневой зоны, а затем полученные от них данные публикуют также зеркала Anycast. В чем разница между этими двумя видами перепубликации?

Операторы корневых серверов получают данные авторитативной зоны от специалиста по обслуживанию корневой зоны (RZM). Затем каждый оператор корневого сервера посредством собственной внутренней системы распространения передает данные зоны на все свои сайты и зеркала Anycast.

2.5 Мы обеспечиваем хостинг зеркала Anycast одного из корневых серверов в нашем городе. Мы видим, что оно отвечает на запросы, поступающие со всего мира. Как сделать так, чтобы оно отвечало только на запросы из нашего региона?

На самом деле это зависит от маршрутизации IP и от того, каким образом данный оператор корневого сервера управляет своей службой Anycast. Некоторые операторы корневых серверов настраивают свои маршрутизаторы и пиринговые сеансы таким образом, чтобы на зеркало Anycast поступал только локальный трафик. Другие же настраивают конфигурацию на работу с глобальным трафиком, когда выбор оптимального маршрута в сети отдается на усмотрение системе маршрутизации. Если вы сталкиваетесь с нежелательным поведением зеркала сервера, хостинг которого вы

обеспечиваете, вам следует обсудить эту проблему с оператором корневого сервера, который обеспечивает работу этой службы.

2.6 В 2016 году имела место масштабная атака на оператора Dyn. Может ли то же самое произойти со всеми anycast-зеркалами корневых серверов?

Да, по крайней мере теоретически. Это одна из причин, по которым в системе корневых серверов существует множество операторов и множество зеркал корневых серверов. Большое количество зеркал Anycast повышает пропускную способность системы корневых серверов RSS и однозначно помогает в случае атак.

2.7 Как можно подать запрос на размещение anycast-зеркала корневого сервера в нашей организации?

Обратитесь непосредственно к операторам корневых серверов по реквизитам, приведенным ниже. Как и в случае с вопросом 3.4, вы можете рассмотреть также вариант поддержания локальной копии корневой зоны, как описано в стандарте RFC 7706, в таком случае формально это не будет считаться частью anycast-системы корневых серверов.

Cogent Communications	
Министерство обороны США (NIC)	
ICANN	https://www.dns.icann.org/imrs/host/
Internet Systems Consortium, Inc.	https://www.isc.org/f-root/hosting-an-f-root-node/
NASA (Исследовательский центр им. Эймса)	
Netnod	https://www.netnod.se/i-root/i.root-servers.net
RIPE NCC	https://www.ripe.net/analyse/dns/k-root/hosting-a-k-root-node
Университет Мэриленда	
Университет Южной Калифорнии, Институт информатики	https://b.root-servers.org/
Армия США (исследовательская лаборатория)	
Verisign, Inc.	https://www.verisign.com/rirs
Проект WIDE	

3. DNS и сети

3.1 Каким образом рекурсивные серверы выбирают, к какому корневому серверу направить запрос, и какой идентификатор корневого сервера следует выбрать предпочтительным для моего рекурсивного сервера?

Это называется «алгоритм выбора сервера». В протоколе DNS не указано, каким образом рекурсивный сервер должен выбирать один из набора корневых серверов для того или иного запроса. Таким образом, каждый разработчик ПО для рекурсивного сервера определяет свой собственный алгоритм выбора сервера. В некоторых реализациях резолверы привязываются к серверу с минимальным временем отклика или же к одному из серверов со временем отклика, аналогичным минимальному. В некоторых реализациях резолверы каждый раз выбирают сервер случайным образом, а в некоторых — распределяют запросы между разными серверами на основе тех или иных сложных формул. В документе от 2012 года описан алгоритм, который был реализован в ПО, популярном в то время.

Пожалуй, самым надежным вариантом будет позволить вашему ПО рекурсивного сервера выполнять свои задачи так, как задумано разработчиками, а не пытаться повлиять на его выбор, чтобы отдавать предпочтение или, наоборот, избегать тех или иных серверов.

3.2 Нам известно, что DNS работает через порт 53 протокола UDP. Не могли бы вы объяснить, как DNS работает через порт 53 протокола TCP?

По умолчанию почти все клиенты DNS для всех запросов используют протокол передачи данных UDP. Однако в некоторых ситуациях вместо этого нужно использовать протокол TCP.

Чаще всего протокол TCP используется в случае, если ответы на запросы по протоколу UDP обрезаются. Урезание происходит тогда, когда ответ сервера слишком большой и не умещается в одно сообщение UDP. Это зависит от того, какой размер буфера UDP резервирует конкретный клиент, а также от любых возможных ограничений на размер ответа, которые может накладывать сам сервер. Когда клиент получает ответ с урезанным набором битов, протокол DNS определяет, что сервер должен повторить этот запрос по протоколу TCP, чтобы попытаться получить полный ответ.

Еще один вариант использования протокола TCP для целей DNS — это передача данных зоны. Поскольку целая зона обычно гораздо больше, чем может поместиться в сообщение UDP, имеет смысл передавать зону по протоколу TCP.

Кроме того, протокол TCP может использоваться в тех случаях, когда на сервер осуществляется атака. Сервер может отправлять клиентам урезанные ответы на запросы, чтобы определить, не имеет ли место фальсификация источника запроса. Клиенты, устанавливающие соединение по TCP, могут заноситься в белый список как нефальсифицированные источники. Кроме того, может использоваться методика, которая называется «ограничение скорости ответов» (RRL), когда урезанные ответы рассылаются время от времени специально. В таких случаях клиенты, генерирующие трафик атаки, не будут перепосылать запрос, а клиенты, не участвующие в атаке, будут иметь возможность получать ответы по протоколу TCP.

Возможность передачи запросов и ответов DNS по протоколу TCP является обязательной к реализации в любом ПО для работы с DNS. Дополнительные сведения см. в документе RFC 7766.

3.3 Каким образом можно сократить время отклика между моим рекурсивным сервером и корневым сервером?

Во-первых, следует тщательно проанализировать, обеспечит ли близость к большему количеству корневых серверов какие-либо реальные преимущества. Проанализируйте трафик запросов, посылаемых вашим рекурсивным сервером на корневые серверы имен. Если трафика больше, чем ожидается, возможно, вы сможете усовершенствовать конфигурацию ваших приложений или сетей таким образом, чтобы они не нуждались в столь частых запросах к корневым серверам. Чтобы измерить фактическое значение времени отклика, воспользуйтесь специальным ПО, например утилитой dig. Обычно достаточно, чтобы по меньшей мере два корневых сервера выдавали время отклика не более 100 миллисекунд.

Проанализируйте сетевой маршрут между вашим рекурсивным сервером и используемыми им корневыми серверами с помощью специальных инструментов, например traceroute. Если при этом обнаружатся какие-либо аномалии (например, маршрут через расположенные далеко узлы), попросите своего интернет-провайдера настроить оптимальную маршрутизацию.

Более подробные сведения об измерении качества обслуживания DNS можно получить из материалов проекта мониторинга качества предоставления услуг корневой зоны DNSMON, который осуществляется в рамках программы Atlas Организации европейских IP-сетей RIPE. Время отклика большинства серверов, измеряемое в сотых якорных пунктов RIPE Atlas, не превышает 60 мс.

Если корневых серверов в разумной близости нет, можно попробовать найти расположенную недалеко точку обмена трафика или дата-центр, в котором можно было бы разместить корневой сервер. Можно попросить одного или нескольких операторов корневых серверов расположить там свой сервер. При этом, правда, нужно иметь в виду, что если в том или ином месте уже расположен один корневой сервер, операторы обычно

не хотят размещать там еще один. Если вам нужна контактная информация оператора, посетите веб-сайт http://www.root-servers.org и воспользуйтесь кнопками Contact Email (Адрес электронной почты для связи) в разделе «Корневые серверы» внизу страницы.

3.4 Можно ли развернуть у себя корневой сервер самостоятельно, загрузив файл корневой зоны и выполнив валидацию подписи?

В документе RFC 7706 описывается соответствующий порядок действий, а также приводится список потенциальных проблем, связанных с этим. Нужно помнить, что такая конфигурация требует использования валидации DNSSEC. См. также проект LocalRoot.

3.5 Как долго рекурсивный сервер кэширует информацию?

У каждой записи DNS есть параметр времени существования (TTL), значение которого задается оператором зоны. Он определяет период, в течение которого рекурсивный сервер имен или другой клиент должен хранить данные в кэше для повторного использования. По истечении этого срока рекурсивный сервер имен должен обратиться к авторитативному серверу снова, чтобы обновить данные.

В случае корневой зоны некоторые записи получают время существования (TTL) продолжительностью 24 часа, а некоторые — 48 часов. Некоторые резолверы имеют ограничение на максимальную продолжительность хранения данных в кэше, обычно это 24 часа.

3.6 По прошествии времени данные в кэше становятся неактуальными, каким образом резолвер обновляется для отображения правильной информации DNS?

Если вы подозреваете, что данные в кэше рекурсивного сервера имен устарели, вы можете выполнить сброс кэша или перезапустить процесс сервера.

3.7 Что такое прайминг-запросы DNS и ответы на них?

Рекурсивные резолверы DNS нуждаются в предварительной подготовке своего кэша, чтобы он содержал конкретные данные из корневой зоны, прежде чем резолвер сможет отвечать на обычные запросы. В документе RFC 8109 описываются запросы, которые рекурсивные резолверы направляют на корневые серверы, а также ответы, которые они получают от корневых серверов.

4. DNSSEC

4.1 Могут ли расширения DNSSEC защитить от атак типа Fast Flux?

На самом деле нет. Технология DNSSEC предназначена для защиты от фальсификации данных, а не от атак типа Fast Flux.

4.2 Становится ли труднее при использовании DNSSEC передавать копию корневой зоны в локальной сети?

Нет, использование локальной копии корневой зоны означает просто то, что используются актуальные копии корневой зоны без каких бы то ни было изменений. Корневая зона поступает от специалиста по обслуживанию корневой зоны (RZM) со всеми необходимыми подписями DNSSEC.

Подробнее о том, как использовать локальные копии корневой зоны, см. в ответе на вопрос 3.4, а также в документе RFC 7706.

4.3 Кажется, передача данных DNS по протоколу UDP ограничивается размером блока в 512 байт, а DNS по TCP ограничивается размером блока в 4096 байт. Если моя зона будет подписана, возможно, размер блока будет превышать лимит. Значит ли это, что такие блоки будут отфильтровываться брандмауэром?

DNS по UDP больше не ограничивается размером блока в 512 байт. Механизмы расширения для DNS (EDNS), описанные в документе RFC 2671 с дальнейшими модификациями в документе RFC 6891, определяют то, каким образом клиенты и серверы могут указывать на поддержку размера блоков свыше 512 байт.

Размер блоков TCP никогда не ограничивался 4096 байтами. Этот протокол предназначен для передачи данных произвольного размера.

Озабоченность в отношении размера подписанных ответов не лишена оснований. Когда ответ на запрос DNS по UDP превышает максимальный размер передаваемого блока сети, он разбивается на фрагменты. Такая ситуация считается риском с точки зрения безопасности, поскольку представляет возможность использования т. н. отравления кэша. Некоторые брандмауэры блокируют такие фрагменты. По этой причине современные рекурсивные резолверы разрабатываются таким образом, чтобы использовать меньшие значения объема буфера EDNS и применять для повторно посылаемых запросов меньшие значения размера буфера. Когда размер буфера достигает приемлемого размера, рекурсивный сервер имен получает либо нефрагментированный ответ на запрос, либо ответ с урезанным набором битов, указывающим на необходимость повторного запроса по TCP.

5. RSSAC

5.1 Как соотносятся между собой комитеты RSSAC и RZERC? Является ли RZERC частью RSSAC?

Консультативный комитет системы корневых серверов (RSSAC) и комитет по анализу изменений корневой зоны (RZERC) — это два разных комитета в составе ICANN, однако

они обмениваются между собой представителями, а некоторые индивидуальные члены могут входить в состав обоих этих комитетов.

Устав RSSAC гласит, что этот комитет:
«...предоставляет Правлению и сообществу ICANN рекомендации по вопросам, касающимся функционирования, безопасности и целостности системы корневых серверов». Подробнее о роли RSSAC см. в документе RSSAC033: Заявление RSSAC о различиях между RSSAC и Root-Ops.

Устав RZERC гласит, что этот комитет:
«...занимается анализом предлагаемых архитектурных изменений корневой зоны DNS, систем (включая их аппаратное обеспечение и программные компоненты), используемых для изменения корневой зоны DNS, и механизмов, применяемых для распространения корневой зоны DNS».

На следующей схеме поясняется роль каждого из этих комитетов.
<СХЕМУ СМ. ЗДЕСЬ https://www.icann.org/groups/rssac/faq>

5.2 Есть ли какой-то срок, к которому мы сможем узнать, сколько корневых серверов необходимо по мнению RSSAC? Когда будет проведена оценка необходимости того или иного количества буквенных серверов?

У RSSAC нет никакого сложившегося мнения о том, сколько должно быть корневых серверов или их операторов. Нынешнее ограничение количества операторов обусловлено техническими, а не административными соображениями.

6. Группа подготовки RSSAC

6.1 Есть ли какое-либо ограничение на количество членов группы подготовки RSSAC?

Нет.

6.2 Каковы требования к времени, которое должны уделять члены группы подготовки RSSAC?

Ожидается, что члены группы подготовки RSSAC будут принимать участие в деятельности рабочих команд и в обсуждении в списке рассылки RSSAC. Некоторые члены смогут уделять больше времени, некоторые меньше, а какие-то рабочие команды и анализ тех или иных документов может требовать больше времени, чем какая-то другая деятельность. Однако, как правило, RSSAC ожидает, что члены группы подготовки RSSAC смогут уделять работе в ней по меньшей мере 4 часа в месяц.

7. Популярные заблуждения

Введение в работу DNS см. в материале Объяснение работы системы доменных имен Интернета для неспециалистов, автор Даниэль Карренберг (Daniel Karrenberg).

7.1 Определяют ли корневые серверы, куда будет направлен трафик Интернета?

Нет, маршрут, по которому по сетям от исходных к конечным адресам пересылаются пакеты, определяют маршрутизаторы и протокол BGP. DNS обеспечивает сопоставление имен, удобных для запоминания людьми, с соответствующими им IP-адресами, и именно такими IP-адресами оперируют в конечном итоге маршрутизаторы, определяющие, куда направится тот или иной пакет.

7.2 Большинство DNS-запросов обрабатываются корневыми серверами?

Нет, большинство запросов обрабатываются рекурсивными резолверами, которые не обращаются каждый раз к корневым серверам, а используют данные, сохраненные в кэше. Рекурсивный резолвер обращается к корневому серверу только тогда, когда у него в кэше отсутствует актуальная информация о доменах верхнего уровня или собственно корнях. В ответ на подавляющее большинство запросов, получаемых корневыми серверами, отправляется ответ с адресом, по которому рекурсивный сервер имен должен обратиться для получения ответа на свой запрос.

7.3 Есть ли какие-то отдельные идентификаторы корневых серверов, которые имеют какое-то особое значение?

Ни один из идентификаторов корневых серверов не является особенным.

7.4 Корневых серверов всего 13?

По всему миру расположено свыше 1000 серверов, которые соответствуют всего 13 идентификаторам корневых серверов (RSI), каждый из которых использует один адрес протокола IPv4 и один адрес протокола IPv6, а также anycast-маршрутизацию.

7.5 Операторы корневых серверов работают независимо друг от друга?

Да, операторы корневых серверов действительно независимы друг от друга, однако они тесно координируют работу между собой через комитет RSSAC и прочие форумы. Подробнее см. в документе RSSAC042: Заявление RSSAC о независимости операторов корневых серверов.

7.6 Корневые серверы получают только ту часть DNS-запроса, которая касается TLD?

В настоящее время корневые серверы (и на самом деле все серверы DNS) обычно получают в составе DNS-запроса полное запрашиваемое имя. Однако сейчас ведется новая работа над тем, чтобы передавать корневым серверам при необходимости только ту часть доменного имени, которая касается TLD.

В 2016 году Инженерная проектная группа Интернета (IETF) опубликовала документ RFC 7816, в котором описывается, каким образом рекурсивные серверы DNS могут передавать только минимально необходимую часть запрашиваемого имени. Это т. н. минимизация запрашиваемого имени, или QNAME Minimization. Технология QNAME Minimization сводится к тому, что рекурсивные серверы DNS будут передавать на запрашиваемые ими серверы только необходимые части доменного имени. Рекурсивные серверы DNS, использующие технологию QNAME Minimization, будут передавать корневым серверам только ту часть запроса, которая касается домена верхнего уровня. Это позволяет сократить объем передаваемой информации и тем самым обеспечить больший уровень конфиденциальности для пользователей, обращающихся к системе DNS. По состоянию на 2020 год технология QNAME Minimization является еще относительно новой и пока не развернута широко.