Краткий обзор системы корневых серверов

Офис технического директора ICANN

Давид Конрад (David Conrad)
OCTO-010
06.05.2020

ICANN

СОДЕРЖАНИЕ

Этот документ входит в состав серии документов OCTO. См. страницу публикаций OCTO - здесь приведен список документов по порядку. Вопросы или предложения по любому из этих документов отправляйте на адрес octo@icann.org.

Корневой сервер отвечает на самые первые вопросы в цепочке операций, конечной целью которой является преобразование доменных имен в адреса интернет-протокола (IP) или другие данные, которые используются для работы Интернета.

1 Процесс разрешения системы доменных имен.

Людям удобнее называть друг друга по именам, однако в компьютерах обычно используются числа. Когда вы смотрите страницы в Интернете, вашему браузеру нужно знать IP-адреса, то есть уникальные в глобальных масштабах номера веб-серверов, на которых расположены интересующие вас веб-сайты. Когда вы вводите доменное имя веб-сайта или переходите по ссылке на тот или иной URL-адрес, ваш браузер пытается узнать соответствующий IP-адрес и для этого запускает процесс, который называется *разрешение DNS*.

Браузер направляет запрос на т. н. «резолвер», то есть специальное ПО, посредством которого реализуется процесс разрешения DNS. Резолверы хранят локальные копии ответов на ранее поступавшие запросы. Это т. н. *кэш*, с помощью которого резолвер может сразу же отвечать на какие-то запросы браузера, не выполняя для этого никаких других действий. Однако когда в таком локальном кэше резолвера ответа на поступивший запрос нет, происходит то, что лучше всего демонстрирует весь процесс разрешения DNS в целом. На первом этапе,[1] чтобы узнать IP-адрес требуемого веб-сайта, запрос с его доменным именем[2] направляется на один из 13 корневых серверов.[3] Однако корневые серверы содержат только информацию о доменах верхнего уровня (TLD), в частности, список таких доменов и соответствующих серверов имен, располагающих информацией о доменах второго уровня в таких TLD. Корневой сервер, на который поступил запрос, в ответ направляет список серверов имен для домена верхнего уровня, к которому относится имя запрашиваемого веб-сайта. К примеру, если вы пытаетесь посетить веб-сайт по адресу www.example.com, ваш резолвер направит на один из корневых серверов запрос IP-адреса, соответствующего этому доменному имени, а корневой сервер в ответ укажет список всех серверов имен для домена верхнего уровня, к которому оно относится, т. е. в данном случае для домена .com.

1 С технической точки зрения, если быть точными, в большинстве случаев этому предшествует еще один этап. Резолвер при запуске обычно считывает заранее определенный файл (т. н. «файл корневых ссылок»), который содержит 26 IP-адресов всех 13 корневых серверов (по 13 для протоколов IPv4 и IPv6). Прочитав этот файл, резолвер направляет запрос по одному из этих адресов, чтобы узнать, не изменились ли адреса корневых серверов. Этот этап называется «прайминг-запрос», он позволяет поддерживать актуальность информации резолверов о корневых серверах.

2 В недавнем стандарте «Минимизация имен запросов (см. Query Name Minimization, RFC 7816) рекомендуется, чтобы для обеспечения конфиденциальности резолвер передавал только ту часть имени, которая относится к серверу имен, на который передается запрос, то есть чтобы на корневые серверы отправлялись только запросы серверов имен TLD, на серверы имен TLD — только запросы имен второго уровня (вместе с TLD) и т. п. Подробное описание этого стандарта и его последствий выходят за рамки настоящего документа.

3 Сервер имен — это специальное программное обеспечение на компьютере, отвечающем на запросы DNS. Зачастую корневые серверы имен называются просто корневыми серверами, хотя на самом деле «корневой сервер» — это не один компьютер (мы рассмотрим это позже). Может вносить небольшую путаницу еще и то, что резолверы тоже иногда называются серверами имен, в особенности в домашних маршрутизаторах и различных конфигурационных файлах, однако в настоящем документе мы будем всегда называть их резолверами.

На следующем этапе процесса разрешения этот же запрос направляется на один из серверов имен TLD, список которых был прислан в ответ на предыдущий запрос. Серверы имен TLD, как и корневые серверы, обычно содержат информацию о серверах имен только тех доменов, за которые они отвечают. Для серверов имен TLD это домены второго уровня в соответствующем TLD. Аналогичным образом, как и в случае с запросами, отправляемыми на корневые серверы, в ответ на запрос, направленный на сервер имен TLD, выдается список серверов имен для соответствующего домена второго уровня. Возвращаясь к нашему примеру, чтобы узнать IP-адрес для имени www.example.com, резолвер направит запрос на один из серверов имен домена .com, а сервер имен домена .com в ответ пришлет список всех серверов имен для домена example.com.

Таким образом процесс разрешения будет продолжаться до тех пор, пока запрос не поступит на сервер имен, который либо сможет на него ответить — то есть выдать IP-адрес соответствующего веб-сервера, — либо же сможет авторитетно заявить, что запрашиваемое имя не существует. В нашем примере резолвер направит запрос адреса для имени www.example.com одному из серверов имен домена example.com, который, как можно предположить, будет знать IP-адрес компьютера, на котором расположен сайт с именем www.example.com, и сможет сообщить этот адрес в ответ на запрос.

Разумеется, выполнение всех этих действий занимает какое-то время, однако ускорить выполнение запроса помогает описанный выше локальный кэш: прежде чем отправлять запрос на сервер имен, резолвер сначала проверит, не задавался ли этот вопрос ранее, потому что в таком случае ответ на него уже содержится в локальном кэше резолвера. В таком случае будет выдан ответ, полученный от сервера имен в прошлый раз. Если же таких данных в кэше нет, тогда запрос будет направлен на сервер имен, а ответ на него будет сохранен в локальный кэш, чтобы его можно было использовать в следующий раз, уже не обращаясь к серверу имен. Такое кэширование является важнейшим фактором масштабирования всей системы DNS. При включенных расширениях безопасности DNS (DNSSEC) эта последовательность операций несколько усложняется — резолвер дополнительно проверяет криптографические подписи получаемых данных, чтобы убедиться, что в них не были внесены изменения злоумышленниками.

2 Система корневых серверов

Как можно видеть из описанного выше, корневые серверы играют довольно ограниченную роль, которая сводится в основном к тому, чтобы отвечать на запросы, присылаемые им на первом этапе процесса разрешения. При этом, несмотря на такую ограниченную роль, корневые серверы являются важнейшим компонентом Интернета, без которого была бы невозможна его работа. Если бы не возможность получить первичный список серверов имен, который выдают корневые серверы, нельзя было бы узнать адрес ни одного из доменных имен в Интернете[4].

Система корневых серверов состоит из более чем 1000 отдельных компьютеров (т. н. «зеркал» корневых серверов), содержащих данные о корне DNS. Эти зеркала отвечают

[4] Некоторые операторы сетей используют специальные приемы, например, описанные в стандарте RFC 7706 (https://tools.ietf.org/html/rfc7706) или аналогичные им, чтобы поддерживать локальную копию корня DNS, благодаря чему их резолверы могут не обращаться с запросами к корневым серверам. Однако такие приемы применяются все же относительно редко и выходят за рамки настоящего документа.

на запросы резолверов Интернета, перенаправляя их, как уже было сказано, на серверы имен соответствующих доменов верхнего уровня.

Двенадцать организаций — т. н. «операторов корневых серверов» — обслуживают 13 корневых серверов[5], именуемых по буквам английского алфавита, от a до m, в домене root-server.net, то есть от a.root-servers.net до m.root-servers.net. Каждому из этих корневых серверов, или корневых служб, присвоено по два уникальных IP-адреса, один по протоколу IPv4, а другой — по протоколу IPv6. Эти IP-адреса изначально указаны в конфигурации всех резолверов Интернета, что позволяет таким резолверам обращаться к корневым службам с запросами. А таких запросов к корневым серверам поступает немало — свыше 70 миллиардов каждый день.

13 корневых служб отвечают на присылаемые им запросы, отправляя в ответ информацию из корневой зоны в том виде, в котором она находится в управлении оператора функций IANA, роль которого выполняет ICANN, или же, если запрашиваемый TLD не был делегирован, сообщение о том, что запрашиваемое имя не существует. Эта информация защищена с помощью DNSSEC: если в эти данные будут внесены кем бы то ни было какие-либо изменения, резолверы, на которых включены расширения DNSSEC, будут игнорировать такие ответы, что позволяет не допустить внесения изменений в данные корневой зоны или осуществления атак, направленных на добавление к ответу несанкционированной информации.

Крайне важно обеспечить отказоустойчивость системы корневых серверов, потому что она должна сохранять способность отвечать на непрерывный поток огромного количества запросов, оставаясь при этом устойчивой к различным кибератакам. Для соблюдения таких требований к отказоустойчивости операторы корневых серверов распределяют зеркала корневых серверов по всему миру, используя для этого технологию маршрутизации, которая называется *Anycast.* Маршрутизация по технологии Anycast позволяет компьютерам, разбросанным по всему Интернету, использовать одни и те же IP-адреса и выдавать одинаковые ответы на запросы, что делает возможным размещать зеркала корневых серверов в сотнях самых разных городов и стран. В настоящее время система корневых серверов благодаря большому количеству зеркал по всему миру отличается крайне высокой отказоустойчивостью. Подробнее о распределении зеркал корневых серверов см. здесь https://root-servers.org.

3 Участие сообщества ICANN

В состав одного из консультативных комитетов ICANN, консультативного комитета системы корневых серверов (RSSAC), входят, наряду с другими членами, и собственно операторы корневых серверов. Комитет RSSAC предоставляет Правлению и сообществу ICANN рекомендации по вопросам, касающимся функционирования, безопасности и целостности системы корневых серверов Интернета, а также управления ею. Кроме того, RSSAC назначает заинтересованных в этом отраслевых экспертов в группу подготовки RSSAC, которая занимается подготовкой документов RSSAC, в т. ч. отчетов и рекомендаций. Подробнее о комитете RSSAC и группе подготовки RSSAC см. здесь: https://www.icann.org/groups/rssac, а список документов, подготовленных RSSAC, находится здесь: https://www.icann.org/groups/rssac/documents.

[5] Исторически так сложилось, что одна организация управляет двумя корневыми серверами.

4 Может ли наша организация разместить у себя зеркало Anycast корневого сервера?

У многих операторов корневых серверов есть программы, в рамках которых вы можете разместить у себя локальное зеркало корневого сервера. Список операторов корневых серверов см. здесь: https://root-servers.org.

Разместить у себя зеркало корневого сервера может быть полезно пользователям больших сетей, например, интернет-провайдеров или крупных корпоративных сетей. Кроме того, это способствует повышению безопасности, стабильности и отказоустойчивости инфраструктуры DNS Интернета в отдельной стране или регионе. Одним из преимуществ размещения зеркала корневого сервера является то, что благодаря этому сокращается время отклика на запросы DNS, отправляемые из ваших сетей, в особенности для несуществующих имен, а также уменьшается использование полосы пропускания сети за счет запросов DNS, которые в таком случае больше не нужно отправлять на зеркала корневых серверов за пределами вашей сети.

5 Роль корпорации ICANN

Если говорить о выполнении тех или иных операций, то, помимо роли оператора функций IANA, который, наряду с другой деятельностью, также вносит изменения в данные корневой зоны, распределяемые затем по 13 корневым серверам, корпорация ICANN выступает администратором одного из таких 13 корневых серверов (а именно сервера L по адресу l.root-servers.net, известного как корневой сервер под управлением ICANN, или IMRS), а также участвует в дискуссиях вместе с другими операторами корневых серверов. Кроме того, корпорация ICANN поддерживает RSSAC в его дискуссиях, посвященных вопросам политик, а также в прочей его деятельности, и группу подготовки RSSAC в ее работе.

Для поддержания безопасности, стабильности и отказоустойчивости инфраструктуры DNS корпорация ICANN приглашает организации, отвечающие определенным критериям операционных возможностей, размещать у себя зеркала корневого сервера, находящегося в управлении ICANN. Более подробные сведения о размещении зеркала Anycast корневого сервера под управлением ICANN (IMRS) см. здесь: https://www.dns.icann.org/imrs/faq/
.