23.2 DNS

DNS (Domain name system) — это система, преобразующая человекочитаемые доменные имена в IP-адреса, понимаемые машиной. Однако в DNS, как и во всем современном вебе есть множество нюансов. Причина тому многократно увеличившееся число устройств, которые могут выходить в Интернет, во много раз усложнившаяся схема сетевой связанности и сами Интернет-технологии, которые развивались далеко не по заданной их разработчиками траектории.

DNS, одна их тех технологий, которая, по мнению отца WWW — Бернерс-Ли Тима «свернула не туда в своём развитии». Давайте, разбираться, что же не так с DNS, когда оно свернуло не туда, и как вообще DNS устроен и работает?

Разберемся сразу в понятиях, что такое WWW (Web) и Internet. WWW (Web) или World Wide Web — это распределенная система, предоставляющая возможность доступа к связанным документам на компьютерах, подключенных к общей сети.

WWW состоит из миллионов веб-серверов, которые обслуживают гипертекстовые документы — html-страницы и статические файлы. Группа веб-страниц объединенная общей тематикой, дизайном и связанная между собой ссылками называется сайтом. Именно Web, как комплекс технологий, куда входит и DNS дал толчок развитию Интернета.

Internet — это глобальная всемирная компьютерная сеть, объединяющая миллионы других сетей и устройств. Internet — это компьютерная сеть, устройства в которой обмениваются информацией с помощью IP-адресов и стека протоколов TCP/IP.

Итак, WWW — это система доступа к web-ресурсам, набор технологий, делающих возможным доступ к различной информации хранящейся на компьютерах, объединенных глобальной мировой сетью под названием Internet.

DNS — это технология относящаяся к WWW. Концепция и принципы DNS были описаны в Книге Бернерс-Ли Тима «Плетя паутину: истоки и будущее Всемирной паутины» (англ. Weaving the Web: Origins and Future of the World Wide Web). По задумке праотца WWW, DNS как система должна быть распределенной, но что-то пошло не так.

Теперь, когда мы точно понимает, что такое WWW и Internet, и куда относится DNS — давайте вплотную им и займемся. Начнём с простого, поймем, что такое DNS и как он работает.

В двух словах и без расшифровки аббревиатур и ссылок на Wiki, DNS — это технология, которая позволяет вам писать человекопонятным языком названия сайтов в поисковую строку браузера, а браузеру находить нужный сайт и отображать его.

DNS занимается тем, что преобразует названия сайтов — доменные имена, которые вводят в поисковую строку браузера в IP-адреса конкретных серверов. Если бы не было DNS, вам бы пришлось запоминать IP-адреса нужных вам ресурсов и вводить их вручную в браузер.

Хорошо, с общим принципом работы разобрались, но возникает вопрос: откуда DNS берёт информацию? Сайтов же миллионы, где эта вся информация хранится?

Сведения о доменах и их связи с IP-адресами находятся в распределенной базе данных, которая хранится на DNS-серверах, образующих иерархию. Для работы

DNS использует TCP/IP стек, TCP- или UDP-порт 53. DNS-сервер — это комбинированное понятие подразумевающие под собой ПО, которое отвечает за обработку DNS-запроса и сам «железный сервер». О них поговорим позже, сейчас давайте разберёмся с иерархией DNS и механикой запросов браузера к DNS.

Когда вы вводите запрос в поисковую строку браузера, например, myfreedom.by — браузер сначала проверит наличие DNS-записи на вашем локальном компьютере в файле hosts, если там нет нужного адреса, запрос направляется дальше — на локальный DNS-сервер интернет-провайдера пользователя, если и там записи нет, запрос уходит выше на сервера географических зон.

Получается, что DNS-запрос поднимается от локальных хранилищ данных до самого верхнего уровня, это быстрее, чем делать запрос сначала к корневому DNS-серверу и идти вниз. К тому же, есть нюанс — опрашивает DNS-сервера второго, верхнего и корневого уровней не браузер, а локальный DNS-сервер — resolver.

Resolver находит сведения о домене, возвращает их браузеру и записывает данные в кеш на 24 часа. Именно отсюда время обновления DNS-записей может занять до 24 часов. Но это очень полезное действие, так как при следующем обращении к этому сайту, resolver просто вернет данные из кеша и сайт загрузится быстрее.

Кстати, история hosts-файла довольно занятная. Ранее это было единственным способом не запоминать IP-адреса. Сейчас же hosts-файл — это по большей части исторический рудимент, который используют, пожалуй, только с целью тестирования и разработки.

Выглядит это примерно так: вы купили виртуальный сервер, запустили на нём какой-то сервис, а доменное имя ещё не приобрели, а тестировать сервисы нужно. Вы вносите запись следующего вида в hosts-файл: 93.159.221.110 my_test_site.ru, сохраняете и обращаетесь по имени к своему сайту через браузер.

Пути расположения hosts-файла:

- Windows XP, 2003, Vista, 7, 8, 10 — c:\windows\system32\drivers\etc\hosts;
- Linux, Ubuntu, Unix, BSD — /etc/hosts;
- macOS — /private/etc/hosts.

С помощью hosts-файла можно делать и другие полезные штуки, например, ограничить доступ к определенным Интернет-ресурсам на локальной машине.

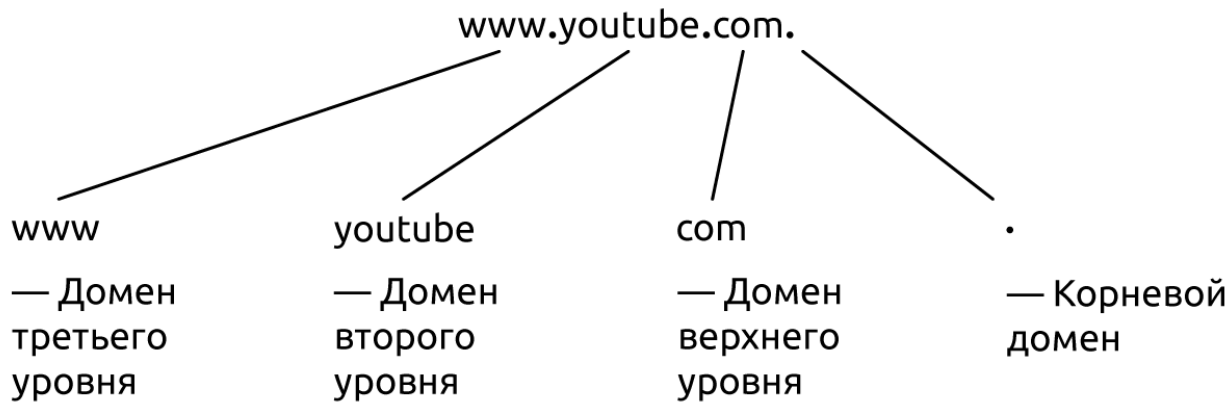
С тем, как происходит DNS-запрос разобрались, давайте теперь немного поговорим, что такое DNS-серверы и, что они хранят.

Что такое DNS-сервер и DNS-записи?

Как мы упомянули ранее DNS-сервер — это с одной стороны ПО, как правило, это BIND, NSD, PowerDNS или Microsoft DNS Server, а с другой стороны — «железный сервер». DNS-серверы бывают корневыми, они отвечают за самый верхний уровень — «.», отвечающими за геозоны — .ru,.com,.io,.by,.kz и локальные DNS-серверы.

Доменное имя отражает иерархию DNS-серверов, если читать его справа налево. Сначала идёт точка — это обращение к корневому серверу, она не отражается, но автоматически всегда подставляется, затем идёт домен верхнего уровня — .com, .ru, .kz и т.д., далее домен второго уровня — собственно само название сайта, далее может быть указан домен третьего уровня, как правило, это www или какой-то технический поддомен: api, panel, slack и т.д.

Вот как графически выглядит расшифровка доменного имени, хорошо нам всем известного ресурса:



Исторически все корневые DNS-серверы находились в Северной Америке, но с ростом популярности Интернета, они появились и в других странах. Сейчас их около 123, часть из них находится и в России:

- F.root (Москва);
- I.root (Санкт-Петербург);
- J.root (Москва, Санкт-Петербург);
- K.root (Москва, Санкт-Петербург, Новосибирск);
- L.root (Москва, Ростов-на-Дону, Екатеринбург).

Хорошо, DNS-серверы (с точки зрения железа) — это мощные серверы, которые принадлежат крупным организациям и хранят данные о DNS-зонах. Поговорим о них подробнее.

Самая простая ситуация — это когда DNS-запись содержит лишь сведения о соотношении IP-адреса сервера с доменным именем, но данных может быть куда больше. Например, у сайта, поддоменов и почтового сервера могут быть разные IP-адреса и вся эта информация должна хранится в одном месте — специальном файле на DNS-сервере, его содержимое называется DNS-зона.

Файл содержит следующие типы записей:

- A-запись — привязка IP-адреса веб-ресурса к конкретному имени домена. DNS-зона может содержать несколько A-записей;
- AAAA-запись — преобразование имени хоста в IPV6-адрес;
- MX-запись — адрес почтового сервера в текущем домене;
- CNAME-запись — запись для подключения поддомена или перенаправления на основной домен;
- NS-запись — адрес DNS-сервера, обслуживающего данный домен;
- TXT-запись — произвольная текстовая информация о доменном имени;
- SRV-запись — позволяет получить имя хоста и номер порта серверов для определенных служб;
- SPF-запись — содержит список доверенных серверов, с которых может отправляться почта данного домена, и сведения о механизме обработки писем, отправленных с других серверов;
- SOA — начальная запись зоны, которая указывает местоположение эталонной записи о домене;
- SSHFP-запись — хранит слепок ключей SSH в DNS.
-

С течением времени значение некоторых DNS-записей расширилось. Например, для подключения CDN используется A-запись, а в некоторых случаях ещё и NS-записи. В A-записи указывается IP-адрес CDN-сервера провайдера, а в NS — NS-сервера провайдера. Это делается для перенаправления трафика и использования DNS-серверов провайдера.

Такая схема подключения CDN используется в 1cloud. Это позволяет в среднем на 30% увеличить скорость загрузки сайта за счёт использования быстрых DNS-серверов, а нагрузка на сайт уходит полностью.

TXT-запись чаще всего используется для подтверждения владения доменом. Обычно это нужно при установке yandex и google счётчиков и запуска рекламы на этих же ресурсах.

Итак, мы затронули множество аспектов работы DNS: начиная от исходной идеи до современного применения. Настало время собрать все воедино и подвести итог.

DNS: что в итоге?

Собираем все новые знания о DNS воедино и раскладываем всё по полочкам.

1. DNS — это система, которая позволяет пользователям вводить человекопонятные названия сайтов в поисковую строку, а браузеру получать IP-адрес ресурса, к которому нужно обратиться;
2. Система хранения DNS-данных (зон) распределённая, а вот серверы, на которых хранятся данные выстроены иерархически. На верхнем уровне находятся корневые DNS-серверы, ниже — DNS серверы географических зон, ещё на уровень ниже — локальные DNS-серверы;
3. DNS-запрос браузером посылается сначала на локальные DNS-серверы (resolve), а затем уже они ищут нужную DNS-запись по иерархии выше;
4. DNS-данные для каждого домена называются DNS-зонами и хранят DNS-записи различных типов;
5. DNS-зонами можно управлять с помощью платных и бесплатных сервисов.