DNS

JSP & Servlets
8 уровень, 3 лекция

ОТКРЫТА

История появления DNS

Еще в 70-е годы люди устали запоминать IP-адреса серверов, к которым хотели обратиться. Тогда же появилась идея использовать более простое и запоминающееся имя вместо числового адреса хоста.

Работники Стэнфордского исследовательского института придумали текстовый файл **HOSTS.TXT**, который содержал список строковых имен и соответствующие им числовые адреса компьютеров в ARPANET.

Адреса назначались вручную. Чтобы запросить имя хоста и адрес или добавить компьютер в главный файл, пользователи связывались с сетевым информационным центром Стэнфорда по телефону в рабочее время.

К началу 1980-х годов поддержание единой централизованной таблицы хостов стало медленным и громоздким, а развивающейся сети требовалась автоматическая система именования для решения технических и кадровых вопросов.

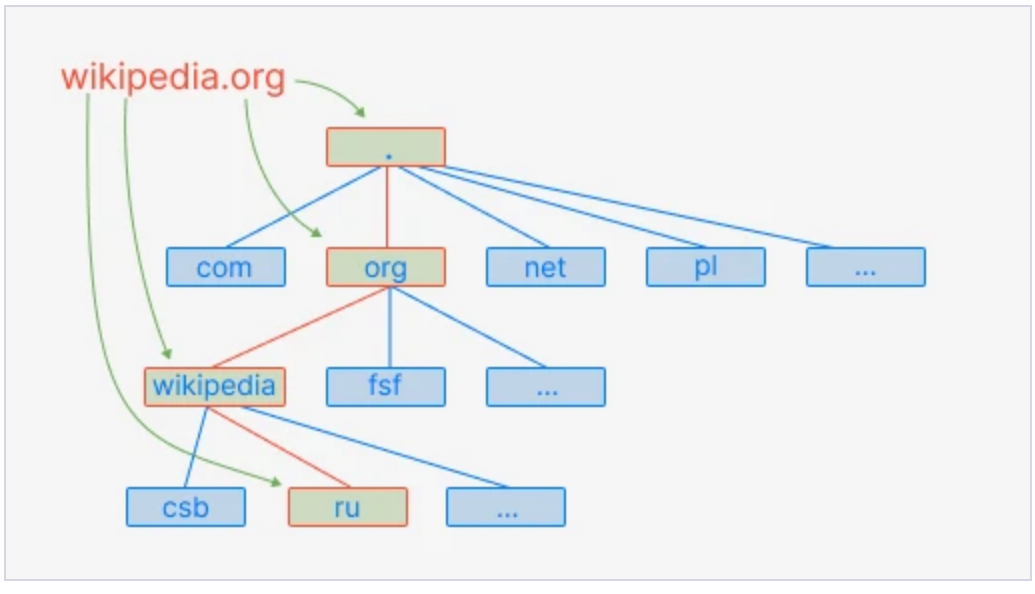
В 1984 году четыре студента университета Беркли написали первую версию иерархической системы доменных имен. В настоящее время она широко распространена, особенно в Unix-системах, и по-прежнему является наиболее широко используемым программным обеспечением DNS в Интернете.

Знакомство с DNS

Domain Name System (DNS) — это распределительная система для хранения и получения информации о доменах. Она чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты и/или обслуживающих узлах для протоколов в домене.

Система организована в виде некой иерархии DNS-серверов, взаимодействующих по определенному протоколу. Основой понимания DNS является представление об иерархической структуре имени и зонах.

Каждый сервер, отвечающий за доменную зону, может передать ответственность за дальнейшую часть домена другому серверу, что позволяет возложить ответственность за актуальность информации на серверы различных организаций, отвечающих только за «свою» часть доменного имени.



Система DNS содержит **иерархию DNS-серверов**, соответствующую иерархии зон. Каждая зона поддерживается как минимум одним авторитетным сервером DNS, на котором расположена информация о домене.

Важно! Имя и IP-адрес не обязательно относятся друг к другу как один к одному. Один IP-адрес может иметь множество доменных имен, что позволяет поддерживать на одном компьютере множество веб-сайтов (это называется **виртуальный хостинг**).

Может быть и наоборот — одному доменному имени может быть сопоставлено множество IP-адресов: это позволяет создавать **балансировку нагрузки и активно используется в CDN-сетях**.

Для повышения устойчивости системы используется множество серверов, содержащих идентичную информацию, а в протоколе есть средства, позволяющие поддерживать синхронность информации, расположенной на разных серверах. Существует 13 корневых серверов, их адреса практически не изменяются.

Интересно! Протокол DNS использует для работы TCP- или UDP-порт 53 для ответов на запросы. Традиционно запросы и ответы отправляются в виде одной UDP-датаграммы. TCP используется, когда размер данных ответа превышает 512 байт.

Записи DNS

DNS сервер хранит набор параметров для каждого доменного имени. Это записи об имени домена, его IP-адресе, а также различная служебная информация.

Всего таких записей несколько десятков, так что мы рассмотрим только самые популярные из них:

A	Address	IP-адресс
AAAA	Address IPv6	Адрес в формате IPv6
CNAME	Canonical name	Каноническое имя для псевдонима
MX	Mail Exchanger	Адрес почтового шлюза для домена
NS	name server	Адрес узла, отвечающего за доменную зону
SOA	Start of authority	Указание на авторитетность информации
SRV	Server selection	Указание на местоположение серверов для сервисов
PTR	pointer	Соответствие адреса имени — обратное соответствие для A и AAAA
TXT	Text string	Запись произвольных двоичных данных, до 255 байт

Самые интересные тут такие:

- **A**-запись позволяет задать IP-адрес, который соответствует домену.
- **CNAME** позволяет задать синоним имени, например, www.javarush.ru == javarush.ru.
- **MX** запись содержит информацию о почтовом сервере: что делать, если на xxx@javarush.ru придет письмо.
- **NS** — указывает на адрес DNS-сервера, который содержит информацию по данному домену. Полезно, когда записи кэшируются и хранятся не на родных узлах.

Поиск IP адреса

Давайте разберемся как работает DNS-система.

Допустим, ты набрал в браузере адрес api.javarush.ru. Браузер обратится к локальному DNS-сервису и попросит дать ему IP-адрес для домена api.javarush.ru. Дальше будет происходить вот что…

Сначала DNS-сервис смотрит, есть ли этот домен в локальном файле hosts на твоем компьютере. Если есть, то берет IP-адрес из него. Если нет, то отправляет запрос к известному ему DNS-серверу: “Какой там IP-адрес у api.javarush.ru?”.

Однако, сервер DNS может ничего не знать не только о запрошенном имени, но и даже обо всем домене javarush.ru. В этом случае сервер обращается к корневому серверу — например, 198.41.0.4. Этот сервер сообщает: “У меня нет информации о данном адресе, но я знаю, что 204.74.112.1 является ответственным за зону ru.”.

Тогда сервер DNS направляет свой запрос к 204.74.112.1, но тот отвечает: “У меня нет информации о данном сервере, но я знаю, что 207.142.131.234 является ответственным за зону javarush.ru.”. Наконец, тот же запрос отправляется к третьему DNS-серверу и получает ответ — IP-адрес, который и передается клиенту, то есть браузеру.

В данном случае в процессе поиска IP по имени сработали такие правила:

- Браузер отправил известному ему DNS-серверу **рекурсивный запрос** (в ответ на такой тип запроса сервер обязан вернуть IP-адрес, либо пустой ответ и код ошибки NXDOMAIN).
- DNS-сервер, получивший запрос от браузера, последовательно отправлял нерекурсивные запросы, на которые получал от других DNS-серверов ответы, пока не получил ответ от сервера, ответственного за запрошенную зону.
- Остальные упоминавшиеся DNS-серверы обрабатывали запросы нерекурсивно (и, скорее всего, не стали бы обрабатывать запросы рекурсивно, даже если бы такое требование стояло в запросе).

Иногда допускается, чтобы запрошенный сервер передавал рекурсивный запрос “вышестоящему” DNS-серверу и дожидался готового ответа.

Важно! При рекурсивной обработке запросов все ответы проходят через DNS-сервер, и он получает возможность кэшировать их. Повторный запрос тех же доменных имен обычно не идет дальше кэша сервера, обращения к другим серверам не происходит вообще.

Допустимое время хранения ответов в кэше приходит вместе с ответами (поле TTL ресурсной записи).

Файл hosts

Обратили внимание, что сначала поиск идет в локалном файле hosts. Это наследник того файла HOSTS.TXT, который был придуман еще во времена ARPANET. Да, он до сих пор существует и до сих пор используется.

Он расположен по пути:

- **/etc/hosts** в Linux.
- **%SystemRoot%\system32\drivers\etc\hosts** в Windows.
- **/system/etc/hosts** в Android.

Обычно файл включает в себя определение расположения узла localhost:

```
127.0.0.1       localhost
```

Структура его очень проста: сначала идет IP-адрес, затем доменное имя.

Полезное

С помощью файла hosts возможно осуществлять фильтрацию рекламы путем перенаправления доменных адресов баннеров на адрес 127.0.0.0, 127.0.0.1 или 0.0.0.0.

Использование 127.0.0.1 обычно не рекомендуется, так как приводит к ожиданию ответа и сопутствующим задержкам, если сервер не существует или неправильно настроен. А если замапить какой-нибудь рекламный домен на IP-адресс 0.0.0.0, то все запросы к нему сразу будут отваливаться).

Публичные DNS-сервера

Обычно ты получаешь DNS-сервер вместе с услугой интернета, когда его подключаешь. Но такой бесплатный DNS-сервер — не всегда лучший вариант. Более того, возможно ты бы не хотел, чтобы каждый раз, когда заходишь на какой-то сайт к DNS-серверу твоего провайдера, отправлялся запрос с именем домена.

Поэтому многие предпочитают переходить на публичные бесплатные DNS-сервера. Во-первых, они очень быстрые и у них большой кэш доменных имен. Ты получишь ускоренную загрузку сайтов и безотказную работу с минимальной вероятностью технических неполадок.

Во-вторых — безопасность. Некоторые DNS-сервисы могут блокировать доступ к фишинговым и вредоносным сайтам и предлагают фильтрацию контента, чтобы защитить детей от нежелательного контента в интернете.

Такие DNS-сервера могут даже бороться с мошенниками. Например, ты заходишь на поддельный сайт банка, а DNS-сервер отдаст тебе не IP-адрес мошенников, а своей службы безопасности.

Список таких серверов

Cloudflare	1.1.1.1 1.0.0.1	Cloudflare обещает, что не будет использовать данные посещений для показа рекламы и обязуется никогда не записывать IP-адреса источника запросов на диск
Google Public DNS	8.8.8.8 8.8.4.4	Сохраняет полную информацию об IP-адресе запрашивающего устройства в течение примерно 24-48 часов для устранения неполадок и диагностики
Comodo Secure DNS	8.26.56.26 8.20.247.20	Блокирует фишинговые сайты, но и предупреждает, если вы пытаетесь посетить сайты с вредоносными, шпионскими программами
Яндекс.DNS	77.88.8.8 77.88.8.1	Бесплатный DNS-сервис от популярной российской поисковой системы

‹ Предыдущая лекция

Следующая лекция ›