DNS

DNS	
Название:	Domain Name System
Уровень (по модели OSI):	Прикладной
Семейство:	TCP/IP
Порт/ID:	53/TCP, 53/UDP
Назначение протокола:	Разрешение доменных имён
Спецификация:	RFC 1034, RFC 1035 / STD 13
Основные реализации (клиенты):	DNS-модуль Microsoft Windows и Linux
Основные реализации (серверы):	BIND

DNS (англ. *Domain Name System* — система доменных имён) — распределённая система преобразования имени хоста (компьютера или другого сетевого устройства) в IP адрес. DNS работает в сетях TCP/IP. Как частный случай, DNS может хранить и обрабатывать и обратные запросы, определения имени хоста по его IP (PTR-записи).

Ключевые характеристики DNS

DNS обладает следующими характеристиками:

- *распределённость хранения информации*. Каждый узел сети в обязательном порядке должен хранить только те данные, которые входят в его *зону ответственности* и (возможно) адреса *корневых DNS-серверов*.
- *Кеширование информации*. Узел *может* хранить некоторое количество данных не из своей зоны ответственности для уменьшения нагрузки на сеть.
- *Иерархическая структура*, в которой все узлы объеденены в дерево, и каждый узел может или самостоятельно определять работу нижестоящих узлов, или *делегировать* (передавать) их другим узлам.
- *Резервирование* За хранение и обслуживание своих узлов (зон) отвечают (обычно) несколько серверов, разделённые как физически, так и логически, что обеспечивает сохранность данных и продолжение работы даже в случае сбоя одного из узлов.

DNS важна для работы Интернета, ибо для соединения с узлом необходима информация о его IP-адресе, а для людей проще запоминать буквенные (обычно осмысленные) адреса, чем последовательность цифр IP-адреса. В некоторых случаях это позволяет использовать виртуальные серверы, например, HTTP-сервера, различая их по имени запроса. Первоначально преобразование между доменными и IP-адресами производилось с использованием специального текстового файла HOSTS.TXT, который составлялся централизованно и обновлялся на каждой из машин сети вручную. С ростом Сети возникла необходимость в эффективном, автоматизированном механизме, которым и стала DNS.

DNS была разработана Полом Мокапетрисом в 1983 году; оригинальное описание механизмов работы описано в RFC 882. В 1987 публикация RFC 1034 и RFC 1035 изменили спецификацию DNS и отменили RFC 882 и RFC 883 как устаревшие. Некоторые новые RFC дополнили и расширили возможности базовых протоколов.

Дополнительные возможности

- поддержка динамических обновлений
- безопасные соединения (DNSsec)
- поддержка различных типов информации (srv записи)

Терминология и принципы работы

Ключевыми понятиями DNS являются:

- **Зона** — логический узел в дереве имён. Право администрировать зону может быть передано третьим лицам, за счёт чего обеспечивается распределённость базы данных. При этом персона, передавшая право на управление в своей базе данных хранит информацию только о существовании зоны (но не подзон!), информацию о персоне (организации), управляющей зоной и адрес серверов, которые отвечают за зону. Вся дальнейшая информация хранится уже на серверах, ответственных за зону.
- **Домéн** — название зоны в системе доменных имён (DNS) Интернета, выделенной какой-либо стране, организации или для иных целей. Структура доменного имени отражает порядок следования зон в иерархическом виде; доменное имя читается справа налево (в порядке убывания значимости), корневым доменом всей системы является точка ('.'), следом следуют домены первого уровня (географические или тематические), следом - домены второго уровня, третьего и т.д. (например, для адреса `ru.wikipedia.org` домен первого уровня — `org`, втрого `wikipedia`, третьего `ru`). На практике точку в конце имени часто опускают, но она бывает важна в случаях разделения между относительными доменами и FQDN (англ. *Fully Qualifed Domian Name*, полностью определённое имя домена).
- **Поддомен** — имя подчинённой зоны. (например, `wikipedia.org` — поддомен домена `org`, а `ru.wikipedia.org` — домена `wikipedia.org`). Теоретически такое деление может достигать глубины 127 уровней, а каждая метка может содержать до 63 символов, пока общая длина вместе с точками не достигнет 254 символов. Но на практике регистраторы доменных имён используют более строгие ограничения.
- **DNS-сервер** — специализированное ПО для обслуживания DNS. DNS-сервер может быть ответственным за некоторые зоны и/или может перенаправлять запросы вышестоящим серверам.
- **DNS-клиент** — специализированная библиотека (или программа) для работы с DNS. В ряде случаев DNS-сервер выступает в роли DNS-клиента.
- **ответственность** (англ. *authoritative*) — признак размещения зоны на DNS-сервере. Ответы DNS-сервера могут быть двух типов: *ответственные* (когда сервер заявляет, что сам отвечает за зону) и *не ответственные* (англ. *Non-authoritative*), когда сервер обрабатывает запрос, и возвращает ответ других серверов. В некоторых случаях вместо передачи запроса дальше DNS-сервер может вернуть уже известное ему (по запросам ранее) значение (режим кеширования).
- **DNS-запрос** англ. *DNS query* — запрос от клиента (или сервера) серверу. Запрос может быть *рекурсивным* или *нерекурсивным*. Нерекурсивный запрос либо возвращает данные о зоне, которая находится в зоне ответственности DNS-сервера (который получил запрос) или возвращает адреса корневых серверов (точнее, адрес любого сервера, который обладает большим объёмом информации о запрошенной зоне, чем отвечающий сервер). В случае рекурсивного запроса сервер опрашивает сервера (в порядке убывания уровня зон в имени), пока не найдёт ответ или не обнаружит, что домен не существует. На практике поиск начинается с наиболее близких к искомому DNS-серверов, если информация о них есть в кеше и не устарела, сервер может не запрашивать DNS-сервера). Рекурсивные запросы требуют больше ресурсов от сервера (и создают больше трафика), так что обычно принимаются от "известных" владельцу сервера узлов (например, провайдер предоставляет возможность делать рекурсивные запросы только своим клиентам, в корпоративной сети рекурсивные запросы принимаются только из локального сегмента). Нерекурсивные запросы обычно принимаются ото всех узлов сети (и осмысленный ответ даётся только на запросы о зоне, которая размещена на узле, на DNS-запрос о других зонах обычно возвращаются адреса корневых серверов).

Система DNS содержит иерархию *серверов DNS*. Каждый домен или поддомен поддерживается как минимум одним *авторитетным сервером DNS* (от англ. *authoritative — авторитетный,*

заслуживающий доверия; в Рунете применительно к DNS и серверам имен часто употребляют и другие варианты перевода: авторизированный, авторитативный), на котором расположена информация о домене. Иерархия серверов DNS совпадает с иерархией доменов.

Имя хоста и IP-адрес не тождественны — хост с одним IP-адресом может иметь множество имён, что позволяет поддерживать на одном компьютере множество веб-сайтов (это называется виртуальный хостинг). Обратное тоже справедливо — одному имени может быть сопоставлено множество хостов: это позволяет создавать балансировку нагрузки. С третьей стороны, бывают реально работающие IP-адреса, которым не соответствует никакое имя.

Для повышения устойчивости системы используется множество серверов, содержащих идентичную информацию. Существует 13 корневых серверов, расположенных по всему миру и привязанных к своему региону, их адреса никогда не меняются, а информация о них есть в любой операционной системе.

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 в случае, если ответ больше 512 байт, или в случае AXFR-запроса.

Рекурсия

Рассмотрим на примере работу всей системы.

Предположим, мы набрали в браузере адрес `ru.wikipedia.org`. Браузер спрашивает у сервера DNS: «какой IP-адрес у `ru.wikipedia.org`»? Однако, сервер DNS может ничего не знать не только о запрошенном имени, но даже обо всём домене `wikipedia.org`. В этом случае имеет место *рекурсия*: 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 поддерживает доменную зону `org`.» 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 поддерживает доменную зону `wikipedia.org`.» Наконец, тот же запрос отправляется к третьему DNS-серверу (который является авторитетным сервером для зоны wikipedia.org), и получает ответ — IP-адрес, который и возвращает клиенту — браузеру.

В данном случае при разрешении имени, то есть в процессе поиска IP по имени:

- браузер отправил известному ему DNS-серверу т.н. *рекурсивный запрос* — в ответ на такой тип запроса сервер обязан вернуть «готовый результат», то есть IP-адрес, либо сообщить об ошибке;
- а сам DNS-сервер, получивший запрос от клиента, последовательно отправлял *итеративные запросы*, на которые получал от других DNS-серверов уточняющие ответы, пока не получил авторитетный ответ от сервера, ответственного за запрошенную зону

В принципе, запрошенный сервер, будучи лентяем, мог бы передать рекурсивный запрос «вышестоящему» DNS-серверу и дождаться готового ответа, но в данном примере он добросовестно выполнил свою задачу.

Запрос на определение имени обычно не идёт дальше *кеша DNS*, который помнит (ограниченное время) ответы на запросы, проходившие через него ранее. Организации или провайдеры могут по своему усмотрению организовывать кэш DNS. Вместе с ответом приходит информация о том, сколько времени следует хранить эту запись в кэше.

Обратный DNS-запрос

DNS используется в первую очередь для преобразования символьных имён в IP-адреса, но он также может выполнять обратный процесс. Для этого используются уже имеющиеся средства DNS. Дело в том, что с записью DNS могут быть сопоставлены различные данные, в том числе и какое-либо символьное имя. Существует специальный домен `in-addr.arpa`, записи в котором используются для

преобразования IP-адресов в символьные имена. Например, для получения DNS-имени для адреса `11.22.33.44` можно запросить у DNS-сервера запись `44.33.22.11.in-addr.arpa`, и тот вернёт соответствующее символьное имя. Обратный порядок записи частей IP-адреса объясняется тем, что в IP-адресах старшие биты расположены в начале, а в символьных DNS-именах старшие (находящиеся ближе к корню) части расположены в конце.

Записи DNS

Наиболее важные категории DNS записей:

- **Запись A** (*address record*) или **запись адреса** связывает имя хоста с адресом IP. Например, запрос A-записи на имя `referrals.icann.org` вернет его IP адрес — `192.0.34.164`
- **Запись CNAME** (*canonical name record*) или **каноническая запись имени** (псевдоним) используется для перенаправления на другое имя
- **Запись MX** (*mail exchange*) или **почтовый обменник** указывает сервер(а) обмена почтой для данного домена.
- **Запись PTR** (*pointer*) или **запись указателя** связывает IP хоста с его каноническим именем. Запрос в домене `in-addr.arpa` на IP хоста в reverse форме вернёт имя (FQDN) данного хоста (см. Обратный DNS-запрос). Например, (на момент написания), для IP адреса `192.0.34.164`: запрос записи PTR `164.34.0.192.in-addr.arpa` вернет его каноническое имя `referrals.icann.org`.
- **Запись NS** (*name server*) указывает на DNS-серверы для данного домена.
- **Запись SOA** (*Start of Authority*) указывает, на каком сервере хранится эталонная информация о данном домене.

Зарезервированные доменные имена

Документ RFC 2606 (Reserved Top Level DNS Names — Зарезервированные имена доменов верхнего уровня) определяет названия доменов, которые следует использовать в качестве примеров (например, в документации), а также для тестирования. Кроме `example.com`, `example.org` и `example.net`, в эту группу также входят `test`, `invalid` и др.

Интернациональные доменные имена

Доменное имя может состоять только из ограниченного набора ASCII символов, позволяя набрать адрес домена независимо от языка пользователя. ICANN утвердил основанную на Punycode систему IDNA, преобразующую любую строку в кодировке Unicode в допустимый DNS набор символов.

Программное обеспечение DNS

Отдельные алгоритмы работы DNS используются в:

- BIND (Berkeley Internet Name Domain)
- djbdns (Daniel J. Bernstein's DNS)
- MaraDNS
- NSD (Name Server Daemon)
- PowerDNS
- Microsoft DNS Server (в серверных версиях операционных систем Windows NT)

Информация о домене

Многие домены верхнего уровня поддерживают сервис whois, который позволяет узнать кому делегирован домен, и другую техническую информацию.

Регистрация домена

Регистрация домена - процедура получения доменного имени. Заключается в создании записей, указывающих на администратора домена, в базе данных DNS. Порядок регистрации и требования зависят от выбранной доменной зоны. Регистрация домена может быть выполнена как организацией-регистратором, так и частным лицом, если это позволяют правила выбранной доменной зоны.

Корневые серверы DNS

Корневы́е се́рверы DNS — это серверы DNS, содержащие информацию о Доменах верхнего уровня, конкретнее — указатели на серверы DNS, поддерживающие работу каждого из этих доменов. Основные корневые серверы DNS обозначаются латинскими буквами от A до M. Они управляются различными организациями, действующими по согласованию с ICANN.

У многих корневых серверов DNS существуют зеркала. В частности, российское зеркало сервера F расположено в РосНИИРОС.

Буква	IP адрес	Старое имя	Оператор	Местоположение	Програмное обеспечение
A	198.41.0.4	ns.internic.net	VeriSign	Dulles, Virginia, U.S.	BIND
B	192.228.79.201	ns1.isi.edu	USC-ISI	Marina Del Rey, California, U.S.	BIND
C	192.33.4.12	c.psi.net	Cogent Communications	distributed using anycast	BIND
D	128.8.10.90	terp.umd.edu	University of Maryland	College Park, Maryland, U.S.	BIND
E	192.203.230.10	ns.nasa.gov	NASA	Mountain View, California, U.S.	BIND
F	192.5.5.241	ns.isc.org	ISC	distributed using anycast	BIND
G	192.112.36.4	ns.nic.ddn.mil	Defense Information Systems Agency	Columbus, Ohio, U.S.	BIND
H	128.63.2.53	aos.arl.army.mil	U.S. Army Research Lab	Aberdeen Proving Ground, Maryland, U.S.	NSD
I	192.36.148.17	nic.nordu.net	Autonomica	distributed using anycast	BIND
J	192.58.128.30		VeriSign	distributed using anycast	BIND
K	193.0.14.129		RIPE NCC	distributed using anycast	NSD
L	199.7.83.42		ICANN	distributed using anycast	NSD
M	202.12.27.33		WIDE Project	distributed using anycast	BIND

Зеркало (в сети)

Зе́ркало — точная копия данных одного сервера на другом. В интернете **зеркалом сайта** называют точную копию другого сайта. Наиболее часто зеркала сайтов используются для предоставления нескольких источников одной и той же информации. Часто большие или популярные файлы располагают на нескольких зеркалах для ускорения скачивания и распределения нагрузки.

Причины

Причины зеркалирования сайтов следующие:

- Защита данных от повреждения, обычно при сбое жестких дисков.
- Сохранение копии веб-сайта, особенно когда он закрыт или собирается закрыться.
- Обеспечение доступа к недоступной информации. К примеру, когда в 2002 году властями Китая был заблокирован доступ к популярному интернет-поисковику Google, его **зеркало** elgooG использовалось, чтобы обойти блокировку.
- В случаях когда внешний трафик значительно дороже внутреннего целесообразно создавать зеркала популярнх внешних ресурсов в собственной зоне Интернет.zi

Примеры

Хороший пример зеркалирования — широко известный веб-сайт SourceForge.net. Он занимается хостингом программ с открытым исходным кодом. SourceForge.net использует множество различных серверов для достижения одной цели: предоставить возможность скачивания файлов пользователями. Много инновационных компьютерных проектов хранят свои сайты и файлы на SourceForge.net, у которого есть зеркала во множестве стран мира. Официальными зеркалами в России являются:

- CitKit
- PeterHost
- CitForum

Большие сети зеркал используют также проекты Debian, FreeBSD, OpenSUSE, Fedora, и другие. Википедия также имеет несколько зеркал в различных местах.

Программы для зеркалирования

- ftpmirror
- wget
- rsync
- CVSup