

DNS. Схема работы DNS

Иерархия символьных имен

DNS. Схема работы DNS

В сетях TCP/IP соответствие между доменными именами и IP-адресами может устанавливаться средствами как локального хоста, так и централизованной службы.

На раннем этапе развития Интернета на каждом хосте вручную создавался текстовый файл с известным именем `hosts`. Этот файл состоял из некоторого количества строк, каждая из которых содержала одну пару «доменное имя — IP-адрес».

По мере роста Интернета файлы hosts также увеличивались в объеме, и создание масштабируемого решения для разрешения имен стало необходимостью.

Решением стала централизованная служба **DNS (Domain Name System — система доменных имен)**, основанная на распределенной базе отображений «доменное имя — IP-адрес».

Служба DNS использует в своей работе DNS-серверы и DNS-клиенты. **DNS-серверы поддерживают распределенную базу отображений, а DNS-клиенты обращаются к серверам с запросами об отображении разрешения доменного имени на IP-адрес.**

Служба DNS использует текстовые файлы почти такого же формата, как и файл hosts, и эти файлы администратор также подготавливает вручную.

Служба DNS опирается на иерархию доменов, и каждый DNS-сервер хранит только часть имен сети

При росте количества узлов в сети проблема масштабирования решается созданием новых доменов и поддоменов имен и добавлением в службу DNS новых серверов.

Для каждого домена имен создается свой DNS-сервер.

На серверах применяют два подхода к распределению имен.

Подход 1: сервер может хранить отображения «доменное имя — IP-адрес» для всего домена, включая все его поддомены. Однако такое решение оказывается плохо масштабируемым, так как при добавлении новых поддоменов нагрузка на этот сервер может превысить его возможности.

Подход 2: сервер домена хранит только имена, которые заканчиваются на следующем ниже уровне иерархии по сравнению с именем домена. (Аналогично каталогу файловой системы, который содержит записи о файлах и подкаталогах, непосредственно в него «входящих».) Именно при такой организации службы DNS нагрузка по разрешению имен распределяется более-менее равномерно между всеми DNS-серверами сети.

Например, в первом случае DNS-сервер домена mmt.ru будет хранить отображения для всех имен, заканчивающихся на mmt.ru (www.zil.mmt.ru, ftp.zil.mmt.ru, mail.mmt.ru и т. д.).

Во втором случае этот сервер хранит отображения только имен типа mail.mmt.ru, www.mmt.ru, а все остальные отображения должны храниться на DNS-сервере поддомена zil.

Каждый DNS-сервер помимо таблицы отображений имен содержит ссылки на DNS-серверы своих поддоменов.

Ссылки связывают отдельные DNS-серверы в единую службу DNS. Ссылки представляют собой IP-адреса соответствующих серверов.

Для обслуживания корневого домена выделено несколько дублирующих друг друга DNS-серверов, IP-адреса которых широко известны (их можно узнать, например, в InterNIC).

Существует две основные схемы разрешения DNS-имен. В первом варианте работу по поиску IP-адреса координирует DNS-клиент:

1. DNS-клиент обращается к корневому DNS-серверу с указанием полного доменного имени.

2. DNS-сервер отвечает клиенту, указывая адрес следующего DNS-сервера, обслуживающего домен верхнего уровня, заданный в следующей старшей части запрошенного имени.

3. DNS-клиент делает запрос следующего DNS-сервера, который отсылает его к DNS-серверу нужного поддомена и т. д., пока не будет найден DNS-сервер, в котором хранится соответствие запрошенного имени IP-адресу. Этот сервер дает окончательный ответ клиенту.

Такая процедура разрешения имени называется не рекурсивной, когда клиент сам итеративно выполняет последовательность запросов к разным серверам имен. Эта схема загружает клиента достаточно сложной работой, и она применяется редко.

Во втором варианте реализуется рекурсивная процедура:

1. DNS-клиент запрашивает локальный DNS-сервер, то есть тот сервер, обслуживающий поддомен, которому принадлежит имя клиента.
2. Далее возможны два варианта действий:

- **если локальный DNS-сервер знает ответ, то он сразу же возвращает его клиенту** (это может произойти, когда запрошенное имя входит в тот же поддомен, что и имя клиента, или когда сервер уже узнавал данное соответствие для другого клиента и сохранил его в своем кэше);
- **если локальный сервер не знает ответ, то он выполняет итеративные запросы к корневому серверу и т. д. точно так же, как это делал клиент в предыдущем варианте, а получив ответ, передает его клиенту, который все это время просто ждет его от своего локального DNS-сервера.**

- В этой схеме клиент перепоручает работу своему серверу, именно поэтому схема называется рекурсивной, или косвенной. **Практически все DNS-клиенты используют рекурсивную процедуру.**
- **Для ускорения поиска IP-адресов DNS-серверы широко применяют кэширование проходящих через них ответов.** Чтобы служба DNS могла оперативно обрабатывать изменения, происходящие в сети, ответы кэшируются на относительно короткое время — обычно от нескольких часов до нескольких дней.

Обратная зона

Служба DNS предназначена также для нахождения DNS-имени по известному IP-адресу.

- Обратная запись не всегда существует даже для тех адресов, для которых есть прямые записи. Ее могут просто забыть создать или же ее создание требует дополнительной оплаты. Обратная задача решается в Интернете путем организации так называемых обратных зон.

Обратная зона — это система таблиц, которая хранит соответствие между IP-адресами и DNS-имена хостов некоторой сети. Для организации распределенной службы и использования для поиска имен того же программного обеспечения, что и для поиска адресов, применяется оригинальный подход, связанный с представлением IP-адреса в виде DNS-имени.

Первый этап преобразования заключается в том, что составляющие IP-адреса интерпретируются как составляющие DNS-имени. Например, адрес 192.31.106.0 рассматривается как состоящий из старшей части, соответствующей домену 192, затем идет домен 31, в который входит домен 106.

Далее, учитывая, что при записи IP-адреса старшая часть является самой левой частью адреса, а при записи DNS-имени — самой правой, то составляющие в преобразованном адресе указываются в обратном порядке, то есть для данного примера — 106.31.192.

Для хранения соответствия всех адресов, начинающихся, например, с числа 192, заводится зона 192 со своими серверами имен. Для записей о серверах, поддерживающих старшие в иерархии обратные зоны, создана специальная зона in-addr.arpa, поэтому полная запись для использованного в примере адреса выглядит так:

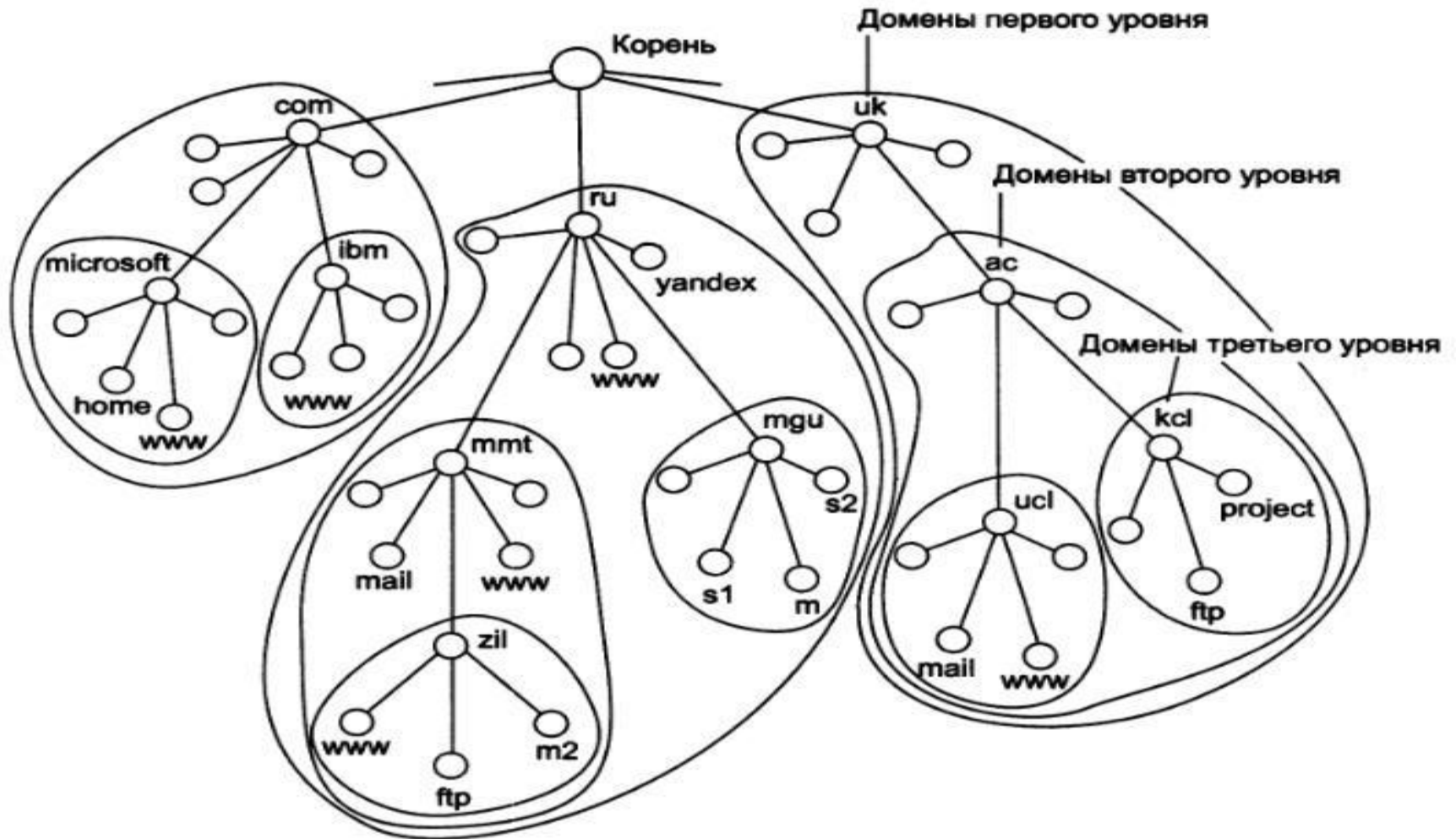
106.31.192.in-addr.arpa.

Серверы для обратных зон используют файлы баз данных, не зависящие от файлов основных зон, в которых имеются записи о прямом соответствии тех же имен и адресов. Такая организация данных может приводить к несогласованности, так как одно и то же соответствие вводится в файлы дважды.

Иерархия символьных имен

В стеке TCP/IP применяется доменная система имен, которая имеет иерархическую древовидную структуру, допускающую наличие в имени произвольного количества составных частей

Пространство доменных имен



Дерево имен начинается с корня, обозначаемого здесь точкой (.). Затем следует старшая символьная часть имени, вторая по старшинству символьная часть имени и т. д. Младшая часть имени соответствует конечному узлу сети.

Составные части доменного имени отделяются друг от друга точкой. Например, в имени `home.microsoft.com` составляющая `home` является именем одного из компьютеров в домене `microsoft.com`.

Краткое доменное имя — это имя конечного узла сети: хоста или порта маршрутизатора. Краткое имя — это лист дерева имен.

Относительное доменное имя — это составное имя, начинающееся с некоторого уровня иерархии, но не самого верхнего. Например, [www.zil](#) — это относительное имя. Полное доменное имя (Fully Qualified Domain Name, FQDN) включает составляющие всех уровней иерархии, начиная от краткого имени и кончая корневой точкой: [www.zil.mmt.ru.](#)

**Корневой домен управляется
центральными органами Интернета, в
частности ICANN.** Домены верхнего уровня
назначаются для каждой страны, а также
для различных типов организаций. Имена
этих доменов должны следовать
международному стандарту ISO 3166.

- **ICANN** - «Корпорация по управлению доменными именами и IP-адресами» (*Internet Corporation for Assigned Names and Numbers*), сокращённо **ICANN** (читается *айкэн*^[1]) — международная некоммерческая организация, созданная 18 сентября 1998 года при участии правительства США для регулирования вопросов, связанных с доменными именами, IP-адресами и прочими аспектами функционирования Интернета.

Корпорация ICANN начала использовать распределённую систему регистрации доменов, которая основана на принципе свободного доступа аккредитованных регистраторов к реестрам доменных имен. Этот шаг положил начало формированию конкурентного доменного рынка. Сегодня в доменных зонах общего пользования работает более 900 аккредитованных регистраторов, благодаря чему количество зарегистрированных доменов значительно возросло и уже превышает 270 миллионов^[2].

- com — коммерческие организации (например, microsoft.com);
- edu — образовательные организации (например, mit.edu);
- gov — правительственные организации (например, nsf.gov);
- org — некоммерческие организации (например, fidonet.org);
- net — сетевые организации (например, nsf.net).

Каждый домен администрирует отдельная организация, которая обычно разбивает свой домен на поддомены и передает функции администрирования этих поддоменов другим организациям. Чтобы получить доменное имя, необходимо зарегистрироваться в какой-либо организации, которой делегированы полномочия по распределению имен доменов.

- Доменная система имен реализована в Интернете, но она может работать и как автономная система имен в любой крупной корпоративной сети, которая хотя и использует стек TCP/IP, никак не связана с Интернетом.

InterNIC

В течении долгого времени за предоставление сетевых информационных услуг в масштабах всего мирового сообщества (всей "*Ceru Internet*") не отвечал никто. В начале 90-х годов для решения этой проблемы был создан центр сетевой информации *InterNIC* (*NIC Internet -- Network Informational Center Internet*), финансируемый NSF (Национальным научным фондом США). Услуги *InterNIC* предоставляются всем пользователям "*Ceru Internet*", включая живущих за пределами США.

InterNIC состоит из трех отделений:

- Служба регистрации
- Служба баз данных
- Служба информации

Кроме центрального ***InterNIC*** существуют и постоянно увеличивается региональные центры. В Европе Европейское отделение NIC расположено в Амстердаме.

Служба регистрации

Служба регистрации отвечает за выделение сетевых адресов и доменных имен **верхнего уровня**. Как правило, регистрацией и выделением соответствующих адресов занимается поставщик услуг Internet (IP-провайдер), хотя если Вы работаете в достаточно большой организации, содержащей где-то около 500 компьютеров, это можно делать и самостоятельно.

Служба регистрации может быть полезной, если Вам необходимо отыскать данные о какой-либо удаленной сети. При обращении к ней можно получить адреса поставщиков сетевых услуг для интересующей вас сети.

Служба баз данных

Служба баз данных предназначена для создания баз данных по обслуживанию пользователей сети Internet.

Основная работа заключается в создании глобального адресного справочника абонентов Сети. В настоящее время пока отсутствует полный справочник абонентов Сети, и поиск абонентов осуществляется при помощи различных поисковых систем ([whois запросы](#)). Но в ближайшее время, по всей видимости, задача поиска абонентов будет решена.

Создается и уже работает справочник услуг с разбивкой по типу услуги, которую предоставляет абонент, а не по названию

Служба информации

Служба информации различными способами распространяет информацию об Internet. В нее может обратиться любой интересующийся (по телефону, факсу, электронной почте и по прямому соединению - telnet). Информация предоставляется бесплатно средствами [Gopher](#), [WAIS](#), [World Wide Web](#) и анонимного [FTP](#).