Основы DNS

Первоначально DNS была рассчитана на поддержку 50 млн. записей и допускала безопасное расширение до нескольких сотен миллионов записей. По оценкам **Мокапетриса**, сейчас насчитывается около 1 млрд. имен DNS, в том числе почти 20 млн. общедоступных имен. Остальные принадлежат системам, расположенным за межсетевыми экранами.

Их имена неизвестны обычным Internet-пользователям. Управлением DNS-серверов занимается международная некоммерческая организация ICANN, расположенная в США.

Использование локального файла hosts и системы доменных имен DNS для разрешения имен сетевых узлов

Если люди в своих операциях с сетевыми ресурсами будут использовать имена узлов, а не IP-адреса, тогда должен существовать механизм, сопоставляющий именам узлов их IP-адреса.

- Есть два таких механизма - локальный для каждого компьютера файл **hosts** и централизованная иерархическая **служба имен DNS.**

С ростом сетей поддерживать актуальность и точность информации в файле hosts становится все труднее. Появилась необходимость в централизованной базе данных имен, позволяющей производить преобразование имен в IP-адреса без хранения списка соответствия на каждом компьютере. Такой базой стала DNS (Domain Name System) - система именования доменов, которая начала массовую работу в 1987 году.

DNS - это *иерархическая база данных*, сопоставляющая имена сетевых узлов и их сетевых служб IP-адресам узлов.

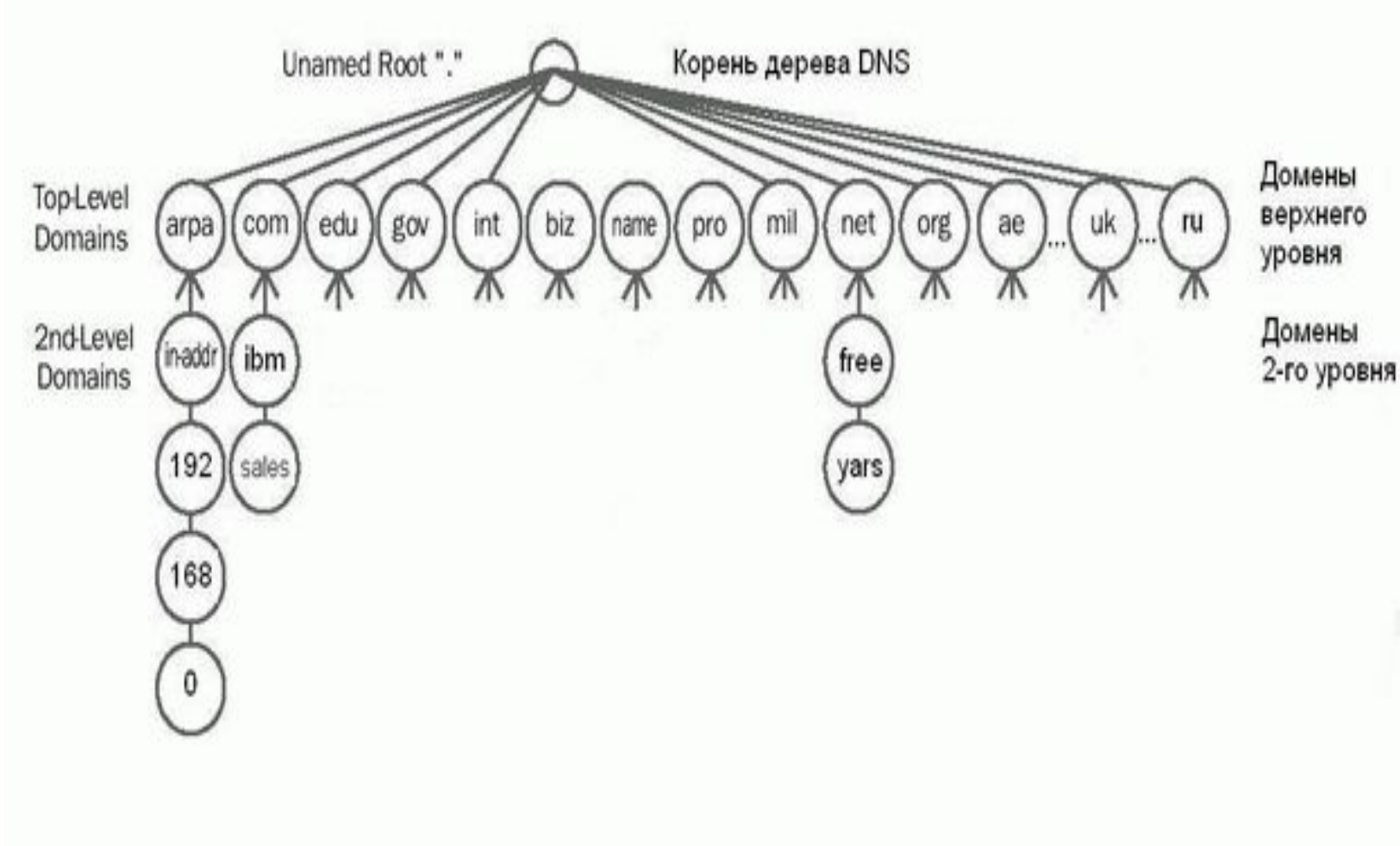
В основе *иерархической структуры базы данных* DNS лежит доменное пространство имен (domain namespace), основной структурной единицей которого является домен, объединяющий сетевые узлы (хосты), а также поддомены. Процесс поиска в БД службы DNS имени некоего сетевого узла и сопоставления этому имени IP-адреса называется "**разрешением имени узла в пространстве имен DNS**".

Служба DNS состоит из трех основных компонент:

- **Пространство имен DNS и соответствующие ресурсные записи (RR, resource record)** - это сама распределенная база данных DNS;
- **Серверы имен DNS** - компьютеры, хранящие базу данных DNS и отвечающие на запросы DNS-клиентов;
- **DNS-клиенты (DNS-clients, DNS-resolvers)** -компьютеры, посылающие запросы серверам DNS для получения ресурсных записей.

Пространство имен.

Пространство имен DNS - иерархическая древовидная структура, начинающаяся с корня, не имеющего имени и обозначаемого точкой ".".



Где находятся главные DNS-серверы?

DNS-серверы верхнего уровня, которые содержат информацию о корневой DNS-зоне, называются **корневыми.** Этими серверами управляют разные операторы. Изначально корневые серверы находились в Северной Америке, но затем они появились и в других странах. Основных серверов — 13. Но, чтобы повысить устойчивость интернета в случае сбоев, были созданы запасные копии, реплики корневых серверов. Так, количество корневых серверов увеличилось с 13 до 123.

В Северной Америке находятся 40 серверов (32,5%), в Европе – 35 (28,5%), еще 6 серверов располагаются в Южной Америке (4,9%) и 3 – в Африке (2,4%). Если взглянуть на карту, то DNS-серверы расположены согласно интенсивности использования интернет-инфраструктуры. Есть сервера в Австралии, Китае, Бразилии, ОАЭ и других странах, включая Исландию.

В России тоже есть несколько реплик корневых серверов DNS, среди которых:

- 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).
- Один из узлов корневого DNS-сервера K-root размещен в Selectel.

Для доменов 1-го уровня различают 3 категории имен:

- **ARPA** - специальное имя, используемое для обратного разрешения DNS (из IP-адреса в полное имя узла);
- **Общие (generic) имена 1-го уровня** - 16 (на данный момент) имен, назначение которых приведено в табл. 1;
- **Двухбуквенные имена для стран** - имена для доменов, зарегистрированных в соответствующих странах (например, ru - для России, ua - для Украины, uk - для Великобритании и т.д.).

Имя домена	Назначение
aero	Сообщества авиаторов
biz	Компании (без привязки к стране)
com	Коммерческие организации, преимущественно в США (например, домен microsoft.com для корпорации Microsoft)
coop	Кооперативы
edu	Образовательные учреждения в США
gov	Правительственные учреждения США
info	Домен для организаций, предоставляющих любую информацию для потребителей
int	международные организации (например, домен nato.int для НАТО)
mil	Военные ведомства США
museum	Музеи
name	Глобальный домен для частных лиц
net	Домен для Интернет-провайдеров и других организаций, управляющих структурой сети Интернет
org	Некоммерческие и неправительственные организации, преимущественно в США
pro	Домен для профессиональных объединений (врачей, юристов, бухгалтеров и др.)
job	Кадровые агентства
travel	Туроператоры

Каждая страна (государство) имеет свой географический домен из двух букв:

ae	United Arab Emirates (Объединенные Арабские Эмираты)	au	Australia (Австралия)
be	Belgium (Бельгия)	br	Brazil (Бразилия)
by	Belarus (Белоруссия)	ca	Canada (Канада)
ch	Switzerland (Швейцария)	cz	Czech Republic (Чехия)
de	Germany (Германия)	dk	Denmark
do	Dominican Republic (Доминиканская республика)	ee	Estonia (Эстония)
es	Spain (Испания)	fi	Finland (Финляндия)
fr	France (Франция)	hu	Hungary (Венгрия)
il	Israel (Израиль)	in	India (Индия)
jp	Japan (Япония)	kg	Kyrgyzstan (Кыргызстан)
kr	South Korea (Южная Корея)	kz	Kazakhstan (Казахстан)
lt	Lithuania (Литва)	lv	Latvia (Латвия)
mx	Mexico (Мексика)	nl	Netherlands (Нидерланды)
no	Norway (Норвегия)	nz	New Zealand (Новая Зеландия)
pl	Poland (Польша)	ro	Romania (Румыния)
ru	Russia (Россия)	si	Slovenia (Словения)
sk	Slovak Republic (Словакия)	su	Soviet Union (Советский Союз - поддерживается, но не распределяется)
ua	Ukraine (Украина)	uk	United Kingdom (Соединенное Королевство Великобритании и Северной Ирландии)
yu	Yugoslavia (Югославия)	za	South Africa (Южная Африка)

Служба DNS: домены и зоны

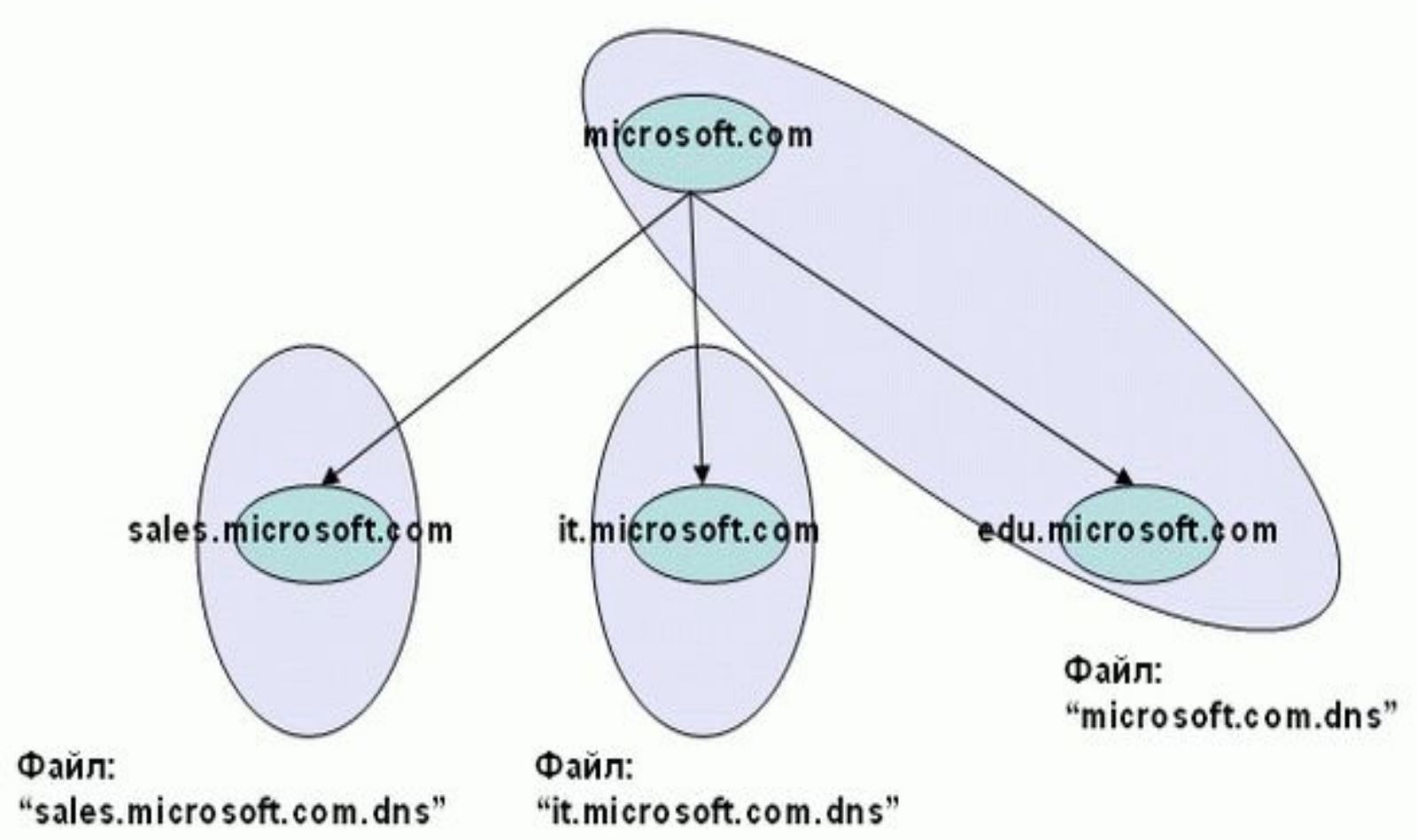
Каждый DNS-сервер отвечает за обслуживание определенной части пространства имен DNS. Информация о доменах, хранящаяся в БД сервера DNS, организуется в особые единицы, называемые **зонами** (zones).

Зона - это способ представления информации о домене и его поддоменах в хранилище тех серверов DNS, которые отвечают за данный домен и поддомены.

Системы семейства Windows Server поддерживают следующие типы зон:

- **Стандартная основная (standard primary)** - главная копия стандартной зоны; только в данном экземпляре зоны допускается производить какие-либо изменения, которые затем реплицируются на серверы, хранящие дополнительные зоны;
- **Стандартная дополнительная (standard secondary)** - копия основной зоны, доступная в режиме "только-чтение", предназначена для повышения отказоустойчивости и распределения нагрузки между серверами, отвечающими за определенную зону; процесс репликации изменений в записях зон называется "передачей зоны" (*zone transfer*) (информация в стандартных зонах хранится в текстовых файлах, файлы создаются в папке "%system root%\system32\dns", имя файла, как правило, образуется из имени зоны с добавлением расширения файла ".dns"; термин "стандартная" используется только в системах семейства Windows);
- **Интегрированная в Active Directory (Active Directory–integrated)** - вся информация о зоне хранится в виде одной записи в базе данных Active Directory (такие типы зон могут существовать только на серверах Windows, являющихся контроллерами доменов Active Directory; в интегрированных зонах можно более жестко управлять правами доступа к записям зоны; изменения в записях зоны между разными экземплярами интегрированной зоны производятся не по технологии передачи зоны службой DNS, а механизмами репликации службы Active Directory);
- **Зона-заглушка** (**stub** ; только в Windows 2003) - особый тип зоны, которая для данной части пространства имен DNS содержит самый минимальный набор ресурсных записей (начальная запись зоны SOA, список серверов имен, отвечающих за данную зону, и несколько записей типа A для ссылок на серверы имен для данной зоны).

пример соотношения между понятиями домена и зоны.



В данном примере пространство имен DNS начинается с домена microsoft.com, который содержит:

3поддомена: sales.microsoft.com, it.microsoft.com и edu.microsoft.com (домены на рисунке обозначены маленькими горизонтальными овалами).

Домен - понятие чисто логическое, относящееся только к распределению имен. Понятие домена никак не связано с технологией хранения информации о *домене.*

Зона - это способ представления информации о домене и его поддоменах в хранилище тех серверов DNS, которые отвечают за данный домен и поддомены.

В данной ситуации, если для хранения выбрана технология стандартных зон, то размещение информации о доменах может быть реализовано следующим образом:

записи, относящиеся к доменам microsoft.com и edu.microsoft.com, хранятся в одной зоне в файле "microsoft.com.dns" (на рисунке зона обозначена большим наклонным овалом);

управление доменами sales.microsoft.com и it.microsoft.com делегировано другим серверам DNS, для этих доменов на других серверах созданы соответствующие файлы "sales.microsoft.com.dns" и "it.microsoft.com.dns" (данные зоны обозначены большими вертикальными овалами).

Делегирование управления - передача ответственности за часть пространства имен другим серверам DNS.

Все запросы, отправляемые DNS-клиентом DNS-серверу для разрешения имен, делятся на два типа:

- ***итеративные запросы*** (клиент посылает серверу DNS запрос, в котором требует дать наилучший ответ без обращений к другим DNS-серверам);
- ***рекурсивные запросы*** (клиент посылает серверу DNS запрос, в котором требует дать окончательный ответ даже если DNS-серверу придется отправить запросы другим DNS-серверам; посылаемые в этом случае другим DNS-серверам запросы будут **итеративными**).
- Обычные DNS-клиенты (например, рабочие станции пользователей), как правило, посылают **рекурсивные запросы.**

Различают **локальные, корневые и авторитетные серверы имен**.

Для непосредственного отображения пространства имен в пространство IP-адресов служат т.н. **ресурсные записи** (RR, resource record).

Каждый сервер DNS содержит ресурсные записи для той части пространства имен, за которую он несет ответственность (*authoritative*).

Табл. 3 содержит описание наиболее часто используемых типов ресурсных записей.

Тип ресурсной записи	Функция записи	Описание использования
A	Host Address Адрес хоста, или узла	Отображает имя узла на IP-адрес (например, для домена microsoft.com узлу с именем www.microsoft.com сопоставляется IP-адрес с помощью такой записи: www A 207.46.199.60)
CNAME	Canonical Name (alias) Каноническое имя (псевдоним)	Отображает одно имя на другое
MX	Mail Exchanger Обмен почтой	Управляет маршрутизацией почтовых сообщений для протокола SMTP
NS	Name Server Сервер имен	Указывает на серверы DNS, ответственные за конкретный домен и его поддомены
PTR	Pointer Указатель	Используется для обратного разрешения IP-адресов в имена узлов в домене in-addr.arpa
SOA	Start of Authority Начальная запись зоны	Используется для указания основного сервера для данной зоны и описания свойств зоны
SRV	Service Locator Указатель на службу	Используется для поиска серверов, на которых функционируют определенные службы (например, контроллеры доменов Active Directory или серверы глобального каталога)

Ресурсные записи

Формат ресурсных записей в DNS (RR)

Ресурсные записи

- **Имя домена** в такой записи может иметь произвольную длину.
- Поля ***тип*** и ***класс*** характеризуют **тип и класс данных**, включенных в запись (аналогичны используемым в запросах).
- Поле ***время жизни*** (TTL) содержит время (в секундах), в течение которого запись о ресурсах может храниться в буферной памяти (в кэше). Обычно это время соответствует **двум дням**.
- **Формат информации о ресурсах** зависит от кода в поле ***тип***, так для тип=1 - это 4 байта IP-адреса.
- **Сервер имен** может обслуживать и другие запросы, например, по IP-адресу определять символьное имя домена или преобразовать имя домена в адрес почтового сервера.
- Когда организация присоединяется к Интернет, она получает в свое распоряжение не только определенную DNS-область, но и часть пространства в **in-addr.arpa**, соответствующую ее IP-адресам.
- **Домен in-addr.arpa** предназначен для определения имен по их IP-адресам. Такая схема исключает процесс перебора серверов при подобном преобразовании.

Зоны прямого и обратного просмотра

- Зоны служащие для разрешения имен узлов в IP-адреса называются зонами прямого просмотра. Наиболее часто используемые для этого типы записей: **A, CNAME, SRV.**
- Для определения имени узла по его IP-адресу служат ***зоны обратного просмотра*** (*reverse lookup* zones), основной тип записи в "обратных" зонах - **PTR.**