Система доменных имён (Domain Name System, DNS)

Кулябов Д. С., Королькова А. В.

Российский университет дружбы народов

Содержание

Основные понятия DNS

Система доменных имён (Domain Name System, DNS)

распределённая система (распределённая база данных), ставящая в соответствие доменному имени хоста (компьютера или другого сетевого устройства) IP адрес и наоборот.

Зона

логический узел в дереве имён

Домен

название зоны в системе доменных имён (DNS) Интернет, выделенной какой-либо стране, организации или для иных целей

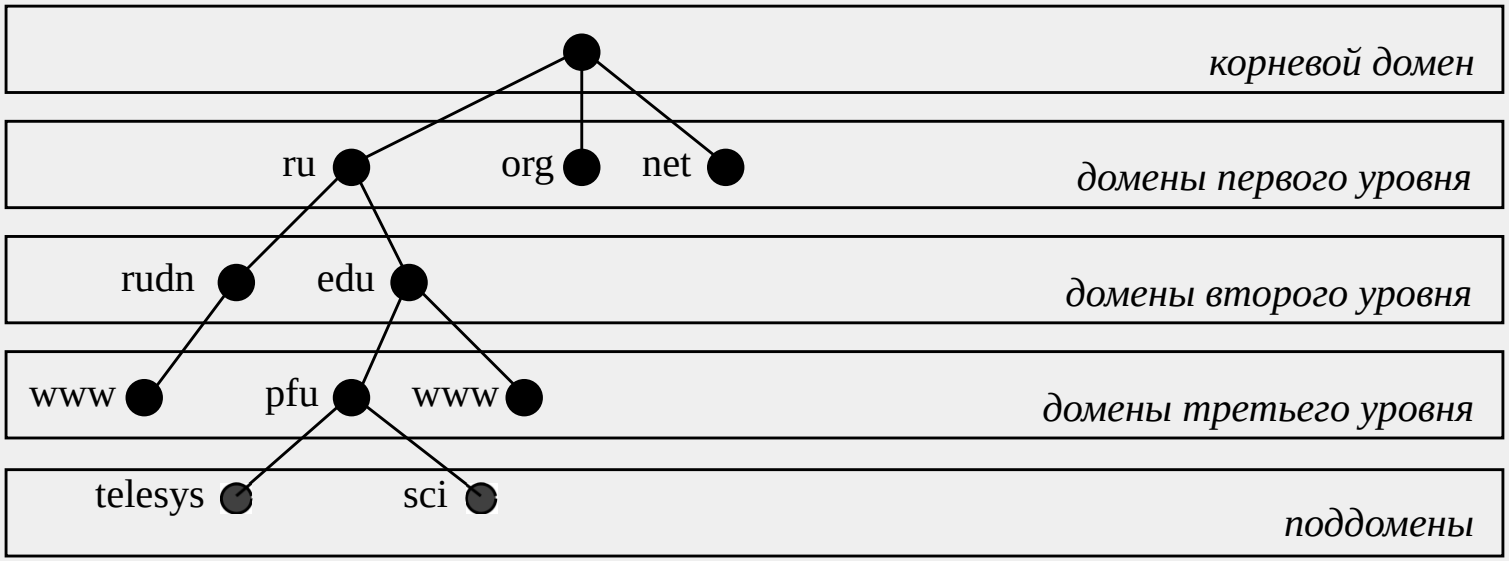
Поддомен (subdomain)

имя подчинённой зоны

Структура доменного имени отражает порядок следования зон в иерархическом виде.

Пример

Иерархическая структура DNS



DNS-сервер

специализированное ПО для обслуживания DNS

В качестве серверов доменных имён чаще всего используются различные версии BIND (Berkeley Internet Name Domain).

DNS-клиент

специализированная библиотека (или программа) для работы с DNS

Задачи клиента:

- опрос DNS-серверов
- интерпретация полученных ответов (RR-записей или сообщений об ошибках)
- возврат информации в программу, которая её запросила

Ответственность или авторитативность (authoritative)

признак размещения зоны на DNS-сервере

Типы DNS-серверов:

- **первичный мастер-сервер (primary master)**: производит загрузку данных для зоны из файла на машине-сервере
- **вторичный мастер-сервер (secondary master)**: получает данные зоны от авторитативного (authoritative) мастер-сервера этой зоны
- **кэширующий сервер**: неавторитативный (non-authoritative) DNS-сервер, предназначенный для хранения в памяти (кэше) ответов на предыдущие запросы от DNS-клиентов

Трансфер зоны (zone transfer)

передача данных зоны от первичного к вторичному DNS-серверу

Делегирование поддоменов

передача ответственности за часть домена другой организации (различные DNS-сервера назначаются авторитативными в делегируемых поддоменах)

DNS-запрос (DNS query)

запрос от клиента (или сервера) серверу

Типы запросов:

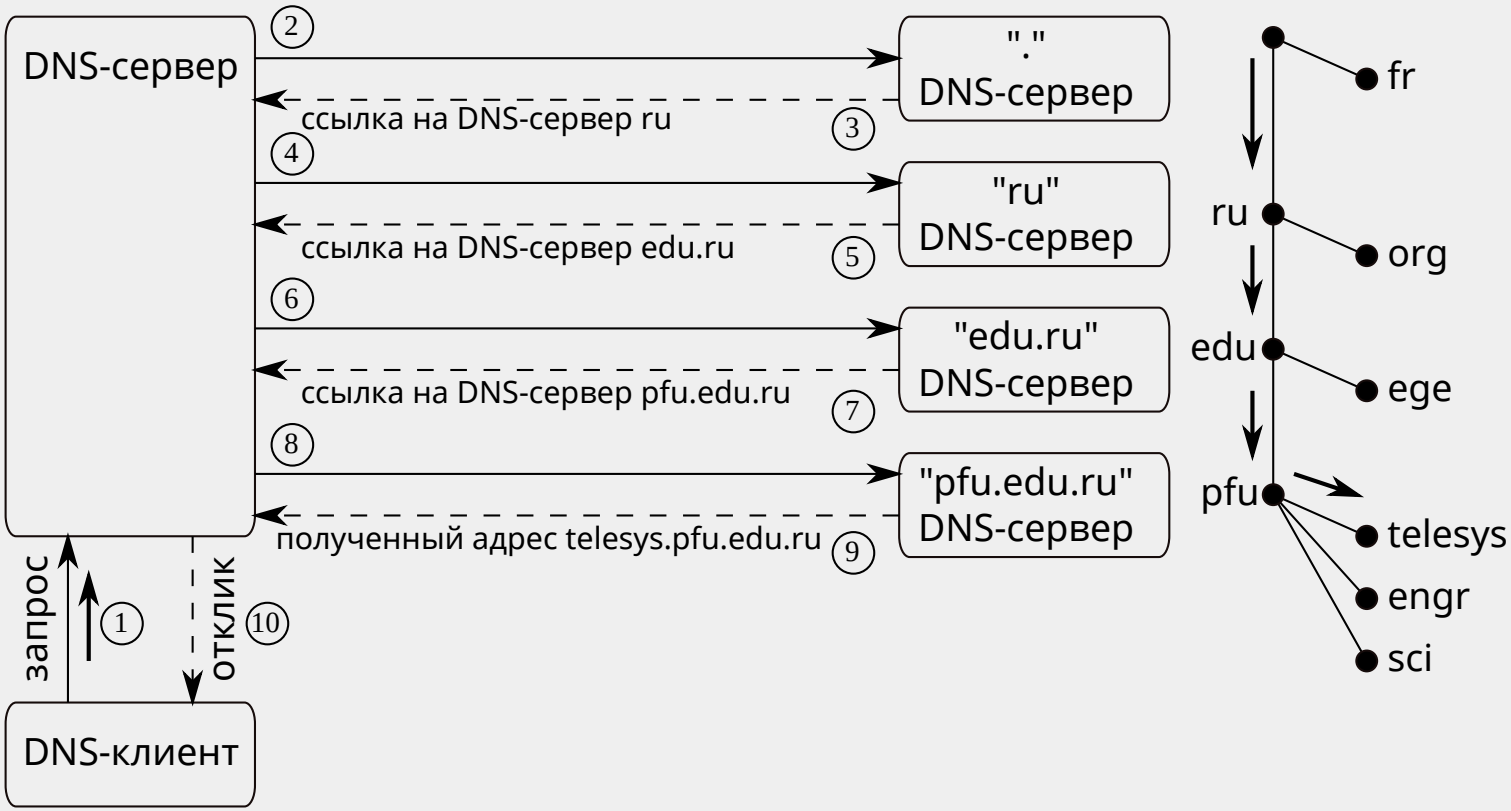
- **рекурсивный**: опрос DNS-серверов идёт в порядке убывания уровня зон в имени до получения ответа на запрос или до обнаружения отсутствия записи о домене на корневом сервере
- **нерекурсивный**: запрос идёт к авторитативному серверу зоны, который возвращает адреса корневых серверов

Типы ответов DNS-сервера:

- **авторитативные (authoritative)**: сервер заявляет, что сам отвечает за зону
- **неавторитативные (Non-authoritative)**: сервер обрабатывает запрос и возвращает ответ от других серверов

Пример

Рекурсивный запрос



Характеристики DNS

Характеристики DNS

- **Распределённость хранения информации.** Каждый узел сети хранит 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.** Все узлы объединены в дерево, каждый узел может самостоятельно определять работу нижестоящих узлов или делегировать их другим узлам.
- **Резервирование.** Несколько серверов (разделённые физически и логически) отвечают за хранение и обслуживание своих узлов (зон), что обеспечивает сохранность данных и продолжение работы даже в случае сбоя одного из узлов.

Файлы данных зоны

Файлы данных зоны

файлы, из которых первичные DNS-серверы производят чтение зональных данных

В файле описания зоны используются:

- *директивы управления (control entries)*
- *записи описания ресурсов (resource records, RR)*

Директивы управления:

- `$ORIGIN`: определяет текущее имя домена (например, в случае, когда в описание зоны требуется включить запись описания хоста из другой зоны);
- `$INCLUDE`: используется для того, чтобы в файл описания зоны можно было включить содержание другого файла (рекомендуется при описании больших зон, разбивая их на небольшие фрагменты).

Синтаксис:

```
[<comment>]
$ORIGIN [<comment>]
$INCLUDE [] [<comment>]
```

В квадратные скобки [ ] заключены необязательные параметры, а в угловые скобки < > — сущности.

RR-записи

описывают все узлы сети в зоне и помечают делегирование поддоменов

Типы записи описания ресурсов:

- SOA-запись — указывает на авторитативность для зоны
- NS-запись — перечисляет DNS-серверы зоны
- A — отображение имён узлов в адреса
- PTR — отображение адресов в имена узлов
- CNAME — каноническое имя (для псевдонимов)
- MX — отображение имён почтовых серверов

Формат записи SOA:

```
[zone] [ttl] IN SOA origin contact (
                    serial refresh retry expire minimum)
```

- *zone* — имя зоны;
- *ttl* — время кэширования (в SOA всегда пустое, определяется директивой управления `$TTL`);
- IN — класс данных Internet;
- *origin* — доменное имя primary master сервера зоны;
- *contact* — почтовый адрес лица, осуществляющего администрирование зоны (т.к. символ `@` имеет особый смысл при описании зоны, то вместо него в почтовом адресе используется символ «.»);

- *serial* — серийный номер файла зоны в нотации ГГГГММДДВВ (учёт изменений файла описания зоны);
- *refresh* — интервал времени, после которого slave сервер обязан обратиться к master серверу с запросом на верификацию своего описания зоны;
- *retry* — интервал времени, после которого slave сервер должен повторить попытку синхронизировать описание зоны с master сервером;
- *expire* — интервал времени, после которого slave сервер должен прекратить обслуживание запросов к зоне, если он не смог в течение этого времени верифицировать описание зоны, используя информацию с master сервера;
- *minimum* — время негативного кэширования (negative caching), т.е. время кэширования ответов, которые утверждают, что установить соответствие между доменным именем и IP-адресом нельзя.

NS-записи обычно следуют сразу за записью SOA в файле описания зоны и указывают на серверы, которые ответственны за эту зону.

Формат записи NS:

```
[domain][ttl] IN NS [server]
```

- *domain* — имя домена, для которого сервер, указанный последним аргументом записи NS, поддерживает описание зоны;
- *server* — доменное имя сервера.

Записи NS указывают как на master, так и на slave серверы. Обычно primary master записывают первым, а резервные серверы указывают вслед за ним.

Основное назначение **адресной записи** — установить соответствие между доменным именем машины и IP-адресом.

Формат адресной записи:

```
[host][ttl] IN A [address]
```

- *host* — доменное имя хоста;
- *address* — IP-адрес машины.

Запись **Mail eXchanger (MX)** определяет хост, который отвечает за доставку почты в определённый домен.

Формат MX-записи:

```
[name] [ttl] IN MX [preference] [host]
```

- *name* — имя машины или домена, на который может отправляться почта;
- *preference* — приоритет почтового сервера, имя которого (поле *host*) указано последним аргументом в поле данных MX-записи.

Запись **CNAME** определяет синонимы для реального (канонического) доменного имени машины, которое определено в записи типа A (Address).

Формат записи CNAME:

```
[nickname] [ttl] IN      CNAME    [host]
```

Поле *nickname* определяет синоним для канонического имени, которое задается в поле *host*.

Пример

```
$ORIGIN user.net.
olga     IN       A        144.206.192.2
www      IN       CNAME    olga.user.net.
gopher   IN       CNAME    olga.user.net.
```

Задача поиска доменного имени по IP-адресу является обратной к прямой задаче — поиску IP-адреса по доменному имени.

- Прямая задача решается в DNS при помощи записей типа *A (Address)*.
- Обратная же задача решается при помощи записей-указателей типа *PTR (Pointer)*, которые совместно с записями SOA и NS составляют описание так называемой **«обратной» зоны**.

Формат PTR-записи:

```
[name][ttl] IN PTR [host]
```

- *name* — номер (не реальный IP-адрес машины, а имя в специальном домене in-addr.arpa или в одной из его зон);
- *host* — доменное имя хоста.

Домен IN-ADDR.ARPA (Address and Routing Parameter Area Domain)

обеспечивает отображение численных величин, определяемых протоколами межсетевого обмена, в пространство имён

Поддомены ARPA:

- in-addr.arpa — для отображения IP-адресов IPv4 в пространство доменных имен
- ip6.arpa — для отображения IP-адресов IPv6 в пространство доменных имен
- e164.arpa — для отображения телефонных номеров формата E.164

Пример

Запись информации об узле с адресом 194.226.43.1 в домене IN-ADDR.ARPA:

```
1.43.226.194.in-addr.arpa
```

Пример

Описание **прямой зоны**:

```
zone "sci.pfu.edu.ru" in {
        type master;
        file "user.net";
};
```

Пример

Описание **обратной зоны**:

```
zone "0.0.127.IN-ADDR.ARPA" {
        type master;
        file "localhost.rev";
};
```

Пример

Фрагмент файла `user.net` описания зоны:

```
@    IN      SOA   @   ns.user.net. user.user.net. (
                    1    ;Порядковый номер
                    3h   ;Обновление через 3 часа
                    1h   ;Повторение попытки через 1 час
                    1w   ;Устаревание через 1 неделю
                    1h );Отрицательное TTL в 1 час
      IN      NS        ns.user.net.
ns    IN      A         192.168.1.1
$ORIGIN user.net.
; Zone user.net
ns    IN      A         192.168.1.1 ; name server
www   IN      A         192.168.1.2 ; web server
```

Символ `@` в записи SOA указывает на то, что текущим *именем домена* является `user.net`.

Первое имя после SOA — имя первичного мастер-сервера DNS зоны. Второе имя — адрес электронной почты человека, управляющего зоной.

Запись *описания сервера доменных имен (NS)* относится к домену user.net, т.е. *авторитативным сервером* для домена user.net будет ns.user.net.

Далее определяется *адрес хоста с именем* ns.user.net (не обязательно указывать имя целиком).

`$ORIGIN` определяет имя текущей зоны.