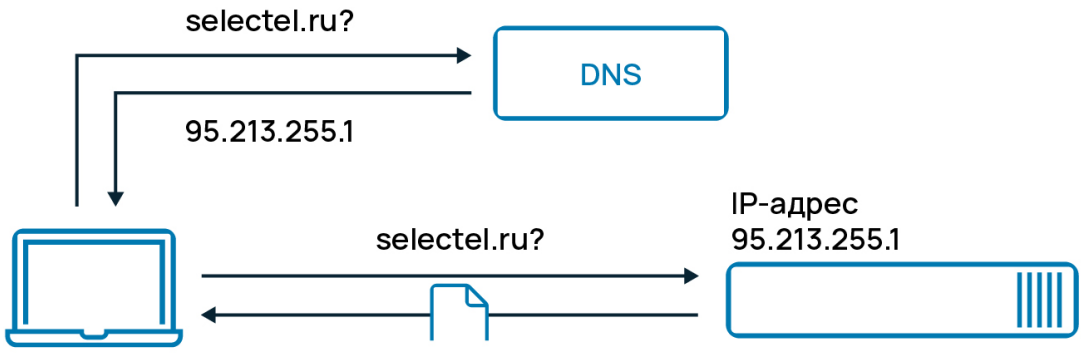
DNS-сервер Bind9

DNS (Domain Name System, система доменных имен) — технология, которая предоставляет браузеру возможность находить конкретный сайт по его имени с помощью DNS-серверов.

Принцип работы DNS похож на поиск и вызов контактов из телефонной книги смартфона. Ищем имя, нажимаем «позвонить», и телефон соединяет нас с нужным абонентом. Понятно, что смартфон в ходе звонка не использует само имя человека, вызов возможен только по номеру телефона. Если вы внесете имя без номера телефона, позвонить человеку не сможете.

Так и с сайтом. Каждому имени сайта соответствует набор цифр формата 000.000.000.000. Этот набор называется IP-адресом, примером реального IP-адреса является 192.168.0.154 или 203.113.89.134. Когда пользователь вводит в адресной строке браузера имя сайта, например google.com, компьютер запрашивает IP-адрес этого сайта на специальном DNS-сервере и после получения корректного ответа открывает сам сайт.



Selectel

Терминология

Основными компонентами DNS являются:

Домен (доменное имя) — символьное имя для обозначения сервера в сети интернет. Доменные имена являются иерархической структурой, в которой каждый уровень отделяется точкой. Основными уровнями являются:

- Корневой домен. В урле он не используется, но всегда подразумевается. От него начинается построение всех урлов в сети интернет
- Домены верхнего уровня. К ним относятся домены .ru, .com, .net, .su и так далее. Также этот домен называют доменом первого уровня.
- Домен второго уровня (или основной домен). Это основное имя вашего сайта
- Поддомены (домены третьего, четвёртого, пятого и т.д. уровня). Сюда входят все поддомены основного домена.

DNS-сервер — система, ответственная за хранение и поддержание в актуальном состоянии записей о своих дочерних доменах. Каждый DNS-сервер ответственен только за свою зону, то есть DNS-сервер домена .io знает о том, где расположен домен hexlet, DNS-сервер которого знает о расположении своих поддоменов.

Корневой DNS-сервер — система, знающая расположение (IP-адреса) DNS-серверов доменов верхнего уровня.

Ресурсная запись — единица информации DNS-сервера. Каждая ресурсная запись имеет несколько полей:

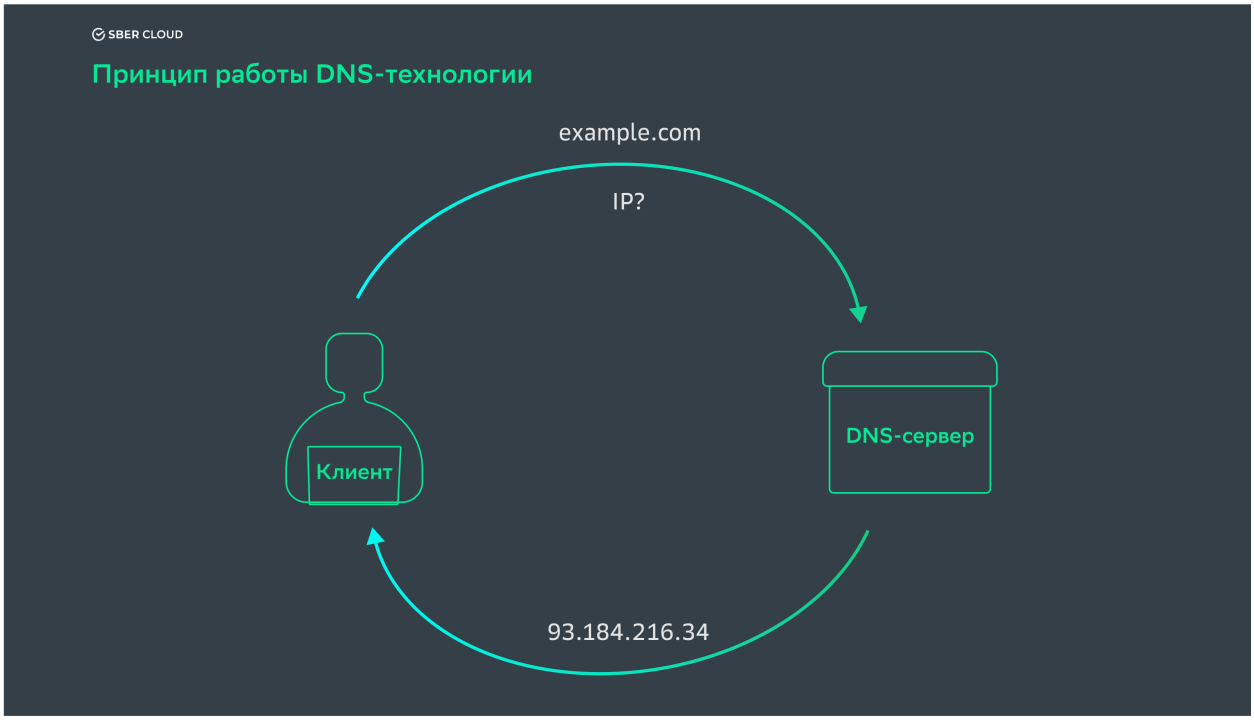
- Имя (домен, к которому относится запись)
- Тип
- Параметры
- Значение

Что такое DNS-сервер?

Это как раз и есть «книга контактов» интернета. DNS-сервер — это специализированный компьютер (или группа), который хранит IP-адреса сайтов. Последние, в свою очередь, привязаны к именам сайтов и

обрабатывает запросы пользователя. В интернете много DNS-серверов, они есть у каждого провайдера и обслуживают их пользователей.

Система доменных имен работает не в виртуальном пространстве, а на определенных физических устройствах. Все данные о доменах хранятся в формате записей на компьютерах, оснащенных соответствующим программным обеспечением.



Зачем нужны DNS-серверы и какие они бывают?

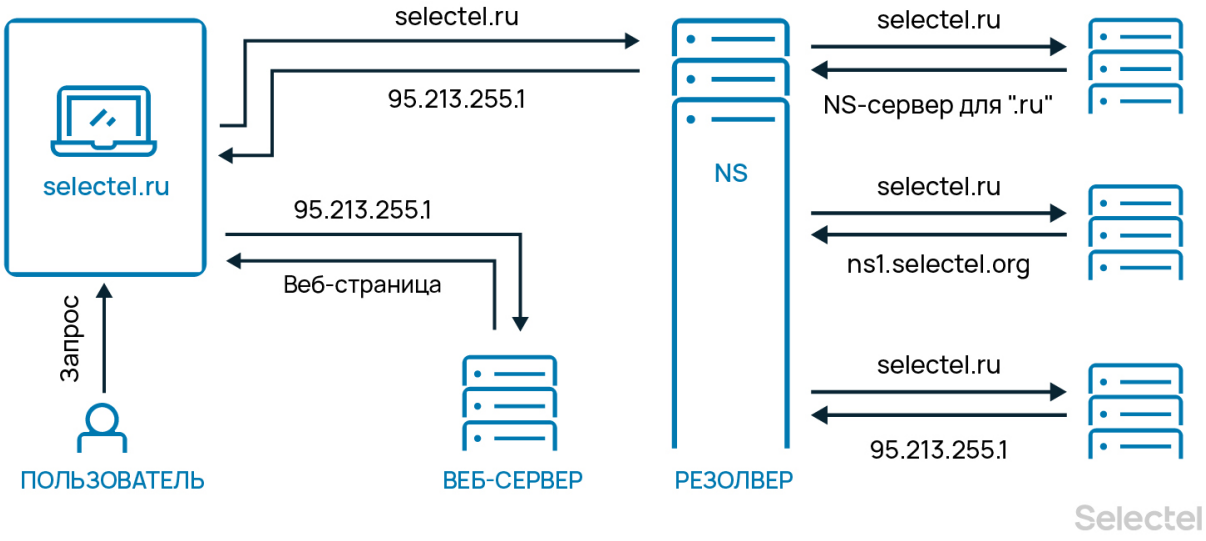
Основное предназначение DNS-серверов — хранение информации о доменах и ее предоставление по запросу пользователей, а также кэширование DNS-записей других серверов. Это как раз «книга контактов», о которой мы писали выше.

В случае кэширования все несколько сложнее. Дело в том, что отдельно взятый DNS-сервер не может хранить вообще всю информацию об адресах сайтов и связанных с ними IP-адресами. Есть исключения — корневые DNS-серверы, но о них позже. При обращении к сайту компьютера пользователя браузер первым делом проверяет локальный файл настроек DNS, файл hosts. Если там нет нужного адреса, запрос направляется дальше — на локальный DNS-сервер интернет-провайдера пользователя.

Локальный DNS-сервер в большинстве случаев взаимодействует с другими DNS-серверами из региона, в котором находится запрошенный сайт. После нескольких обращений к таким серверам локальный DNS-сервер получает искомое и отправляет эти данные в браузер — запрошенный сайт открывается. Полученные данные сохраняются на локальном сервере, что значительно ускоряет его работу. Поскольку, единожды «узнав» IP-адрес сайта, запрошенного пользователем, локальный DNS сохраняет эту информацию. Процесс сохранения полученных ранее данных и называется кэшированием.

Если пользователь обратится к ранее запрошенному сайту еще раз, то сайт откроется быстрее, поскольку используется сохраненная информация. Правда, хранится кэш не вечно, время хранения зависит от настроек самого сервера.

IP-адрес сайта может измениться — например, при переезде на другой хостинг или сервер в рамках прежнего хостинга. Что происходит в этом случае? В этом случае обращения пользователей к сайту, чей IP-адрес поменялся, некоторое время обрабатываются по-старому, то есть перенаправление идет на прежний «айпишник». И лишь через определенное время (например, сутки) кэш локальных серверов обновляется, после чего обращение к сайту идет уже по новому IP-адресу.



де 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.

Что такое DNS-зоны?

В этой статье мы рассматриваем лишь вариант «один домен — один IP-адрес». На самом деле, ситуация может быть и сложнее. Так, с определенным доменным именем может быть связано несколько ресурсов — сайт и почтовый сервер. У этих ресурсов вполне могут быть разные IP-адреса, что дает возможность повысить надежность и эффективность работы сайта или почтовой системы. Есть у сайтов и поддомены, IP-адреса которых тоже могут быть разными.

Вся эта информация о связи сайта, поддоменов, почтовой системы хранится в специальном файле на DNS-сервере. Его содержимое называется DNS-зона. Файл содержит следующие типы записей:

- A — адрес веб-ресурса, который привязан к конкретному имени домена.
- MX — адрес почтового сервера.
- CNAME — чаще всего этот тип записи используется для подключения поддомена.
- NS — адрес DNS-сервера, который отвечает за содержимое других ресурсных записей.
- TXT — любая текстовая информация о доменном имени.
- SPF — данные с указанием списка серверов, которые входят в список доверенных для отправки писем от имени указанного домена.
- SOA — исходная запись зоны, в которой указаны сведения о сервере и которая содержит шаблонную информацию о доменном имени.

А что с новыми доменами?

После регистрации доменного имени нужно «рассказать» о нем DNS-серверам. Для этого нужно прописать ресурсные записи, что обычно делается в админке хостинг-провайдера или доменного провайдера. Примерно через сутки DNS-записи пропишутся в локальном сервере, также они попадут и в реестры всех прочих DNS-серверов. Как только это произойдет, новый домен станет нормально открываться браузером. «DNS сайта», как иногда ошибочно называют доменное имя, активируется.

Ниже список самых популярных и общедоступных DNS-серверов (актуально на октябрь 2021):

- Google: 8.8. 8.8 & 8.8. 4.4.
- Quad9: 9.9. 9.9 & 149.112. 112.112.
- OpenDNS: 208.67. 222.222 & 208.67. 220.220.
- Cloudflare: 1.1. 1.1 & 1.0. 0.1.
- CleanBrowsing: 185.228. 168.9 & 185.228. 169.9.
- Alternate DNS: 76.76. 19.19 & 76.223. 122.150.
- AdGuard DNS: 94.140. 14.14 & 94.140.

Как зарегистрировать домен для сайта?

https://help.reg.ru/hc/ru/articles/4408054420753-Как-зарегистрировать-домен

DNS-сервер Bind9

Bind9 - открытая и наиболее распространённая реализация DNS-сервера, обеспечивающая выполнение преобразования DNS-имени в IP-адрес и наоборот. Исполняемый файл-демон сервера BIND называется named.

Устанавливается на сервера под управлением UNIX, но имеет также сборку под Windows. Расшифровывается как Berkeley Internet Name Domain.

Инсталляция сервера bind, как правило, выполняется из репозитория Linux (Debian, Ubuntu, CentOS и так далее) или портов (FreeBSD, Gentoo, ...). Также можно скачать пакет для установки с официального сайта.

Установка и настройка Bind9 на ОС Linux (Ubuntu 20.04)

Для начала посмотрим, как вообще работает DNS.

Команда *nslookup* — инструмент сетевого администрирования для запросов в доменной системе имен (DNS) с целью получения доменного имени, IP-адреса или другой информации из записей DNS. Кроме того, эта команда используется для поиска и устранения проблем с DNS. Синтаксис: `nslookup [ОПЦИИ] [ИМЯ/АДРЕС] [СЕРВЕР ИМЕН]`

Например, `nslookup google.com` выведет:

```
nslookup google.com
╤хЁтхЁ:  ns1.lipetsk.ru
Address:  195.34.224.1

╚ь :    google.com
Addresses:  2a00:1450:4010:c0e::8a
          2a00:1450:4010:c0e::8b
          2a00:1450:4010:c0e::65
          2a00:1450:4010:c0e::66
          74.125.131.102
          74.125.131.113
          74.125.131.101
          74.125.131.138
```

```
          74.125.131.139
          74.125.131.100
```

Заметим, если для команды nslookup не указать DNS сервер, он будет использовать DNS сервер компьютера по умолчанию:

```
ipconfig /all

Срок аренды истекает. . . . . . . . . . : 16 февраля 2022 г. 4:48:40
   Основной шлюз. . . . . . . . . : fe80::9294:e4ff:feed:e27c%9
                                     192.168.0.1
   DHCP-сервер. . . . . . . . . . . : 192.168.0.1
   IAID DHCPv6 . . . . . . . . . . . : 114839782
   DUID клиента DHCPv6 . . . . . . . : 00-01-00-01-27-B1-66-88-D8-50-E6-B9-B7-C2
   DNS-серверы. . . . . . . . . . . : 195.34.224.1
                                     195.34.224.2
   NetBios через TCP/IP. . . . . . . . : Включен
```

Наша цель настроить DNS сервер Bind9 на виртуальной машине под управлением ОС Linux и посмотреть IP-адреса популярных сайтов, указав для команды nslookup в качестве DNS сервера IP-адрес Linux машины с установленным и настроенным Bind9.

Установка DNS-сервера bind9:

```
sudo apt install bind9 bind9utils bind9-doc
```

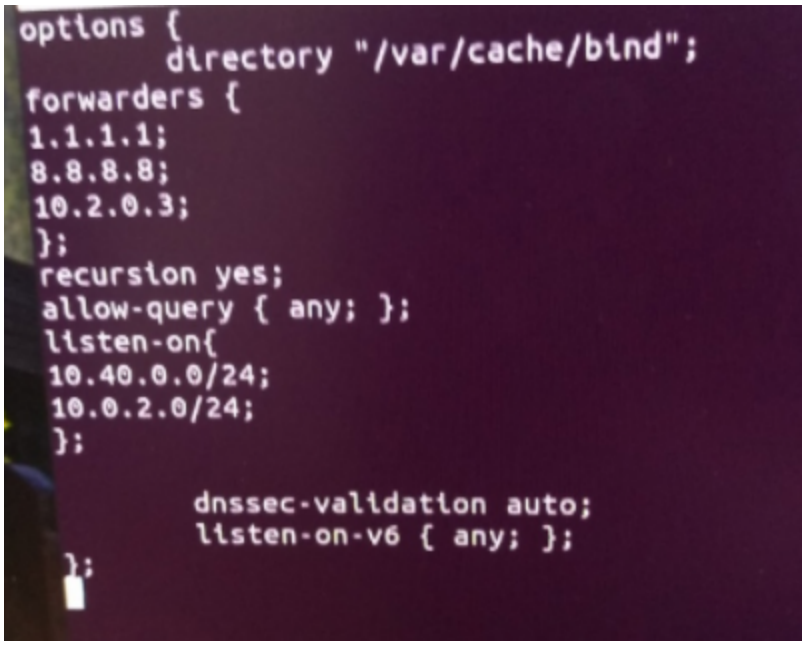
Проверяем статус и работоспособность:

```
sudo systemctl status bind9
```

Настройка BIND9
Откроем основной файл конфигурации:

```
sudo nano /etc/bind/named.conf.options
```

Должен получиться файл конфигурации со следующим содежимым:



Файл /etc/bind/named.conf.options

```
options {
        directory "/var/cache/bind";
        forwarders{
        1.1.1.1;
        8.8.8.8;
        195.34.224.1;
        };
        recursion yes;
        allow-query {any;};
        listen-on{
        192.168.56.0/24;
        };
        dnssec-validation auto;
        listen-on-v6 { any; };
        auth-nxdomain no;
        querylog yes;
};
```

> В конце файла обязательно должна быть 1 пустая строка!!!!!!!!!!!!!!

Здесь директива ***listen-on*** позволяет указать сети, которые будет обслуживать DNS-сервер.

BIND9 по умолчанию разрешает только локальные запросы. Добавьте необходимые IP-адреса в директиву ***«allow-query»*** или «any;» чтобы разрешить все запросы.

Перенаправители (***forwarders***) содержат IP-адреса DNS-серверов, на которые перенаправляется запрос, если наш сервер не содержит необходимых данных: 8.8.8.8, 8.8.4.4 стандартные DNS-сервера Google и 10.2.0.3 - DNS-сервер сети ЕГУ.

Сохраним файл. Проверим конфигурацию:

```
sudo named-checkconf
```

Перезапустим службу сервера:

```
sudo systemctl restart bind9
```

Проверим статус:

```
sudo systemctl status bind9
```

Добавим bind в исключение фаерволла:

```
sudo ufw allow Bind9
```

Протестируем bind9. С другого компьютера в сети (например с Windows, сеть 10.40.0.0, хост 10.40.0.1):

```
nslookup google.com ip-нашего-dns-сервера
```

То есть, в нашем случае ip-адрес виртулаьной машины:

```
nslookup google.com 192.168.0.7
```

```
╤xËтxË:  UnKnown
Address:  192.168.0.7

Не заслуживающий доверия ответ:
╚ь :     google.com
Addresses:  2a00:1450:4010:c0f::64
          2a00:1450:4010:c0f::8b
          2a00:1450:4010:c0f::71
          2a00:1450:4010:c0f::65
          216.58.210.174
```

Если необходимо, чтобы bind разрешал записи для собственного домена, необходимо создать соответствующую зону.

Заключение

Теперь вы можете обращаться к интерфейсам серверов вашей частной сети по имени, а не по IP-адресу. Это упрощает настройку служб и приложений, поскольку вам больше не нужно запоминать частные IP-адреса, а файлы будет легче читать и понимать. Кроме того, теперь вы можете изменять свои конфигурации для работы с новыми серверами в одном месте, на вашем основном DNS-сервере, вместо того чтобы редактировать целых набор самых разных файлов.

Списое использованных источников

https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-a-private-network-dns-server-on-ubuntu-18-04-ru

https://selectel.ru/blog/dns-server/

https://mcs.mail.ru/blog/chto-takoe-dns-tri-bukvy-na-kotoryh-derzhitsya-internet

https://obu4alka.ru/settings-dns-bind9-ubuntu-20-04.html