Протокол DNS

DNS (англ. Domain Name System) — система доменных имѐн, способная по запросу, содержащему доменное имя хоста (компьютера или другого сетевого устройства), сообщить IP адрес или (в зависимости от запроса) другую информацию.

DNS может хранить и обрабатывать и обратные запросы, определения имени хоста по его IP адресу:
IP адрес по определѐнному правилу преобразуется в доменное имя, и посылается запрос на информацию типа "PTR".

Ключевые характеристики

- **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 объединены 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, разделѐнные как физически, так и логически, что обеспечивает сохранность данных и продолжение работы даже в случае сбоя одного из узлов.

Стандарты на работу DNS

RFC 1034 — Domain Names — Concepts and Facilities: http://tools.ietf.org/html/rfc1034

RFC 1035 — Domain Names — Implementation and Specification: http://tools.ietf.org/html/rfc1035

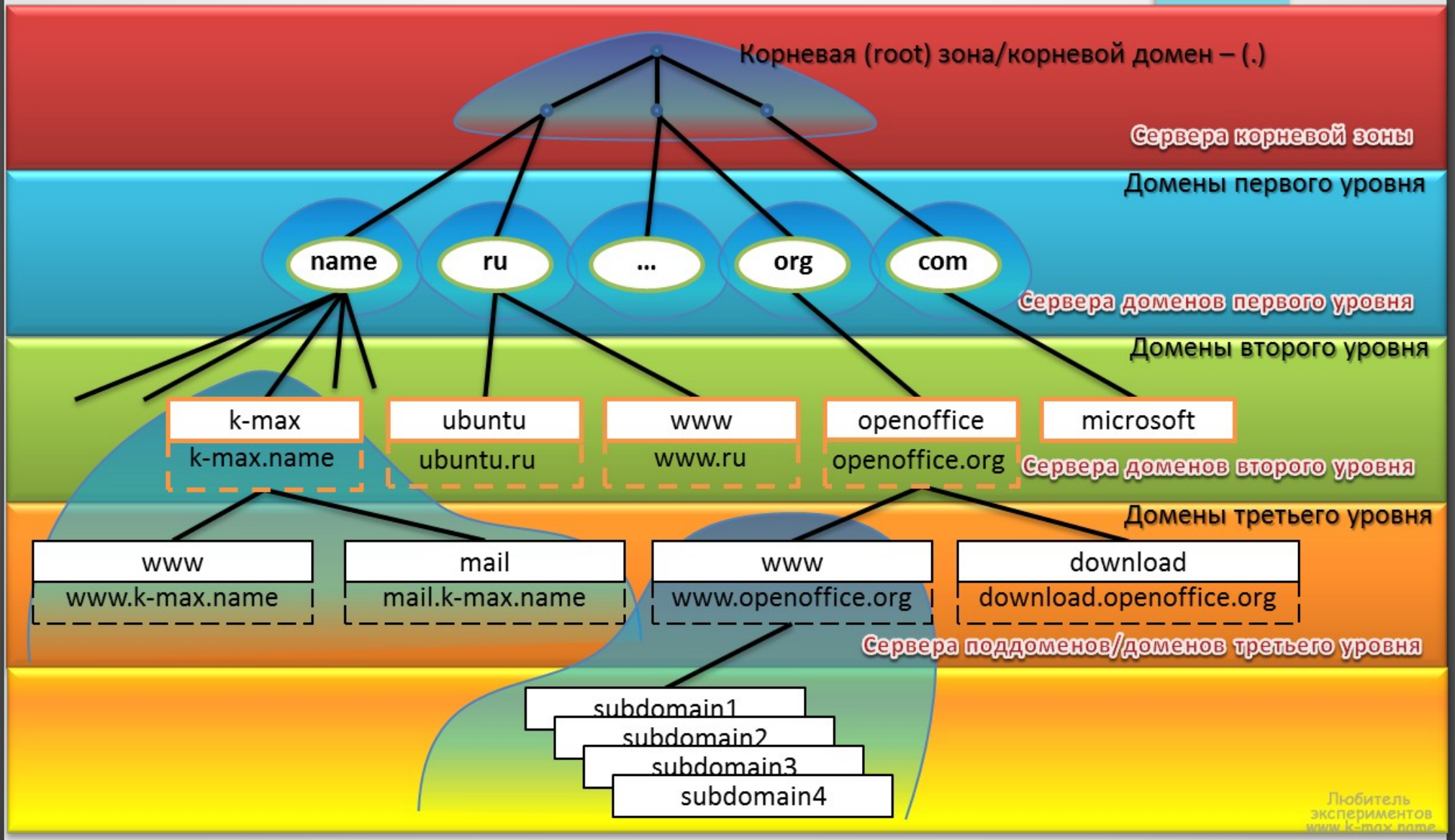
RFC 1537 — Common DNS Data File Configuration Errors: http://tools.ietf.org/html/rfc1537

RFC 1591 — Domain Name System Structure and Delegation: http://tools.ietf.org/html/rfc1591

RFC 1713 — Tools for DNS Debugging: http://tools.ietf.org/html/rfc1713

RFC 2606 — Reserved Top Level DNS Names: http://tools.ietf.org/html/rfc2606

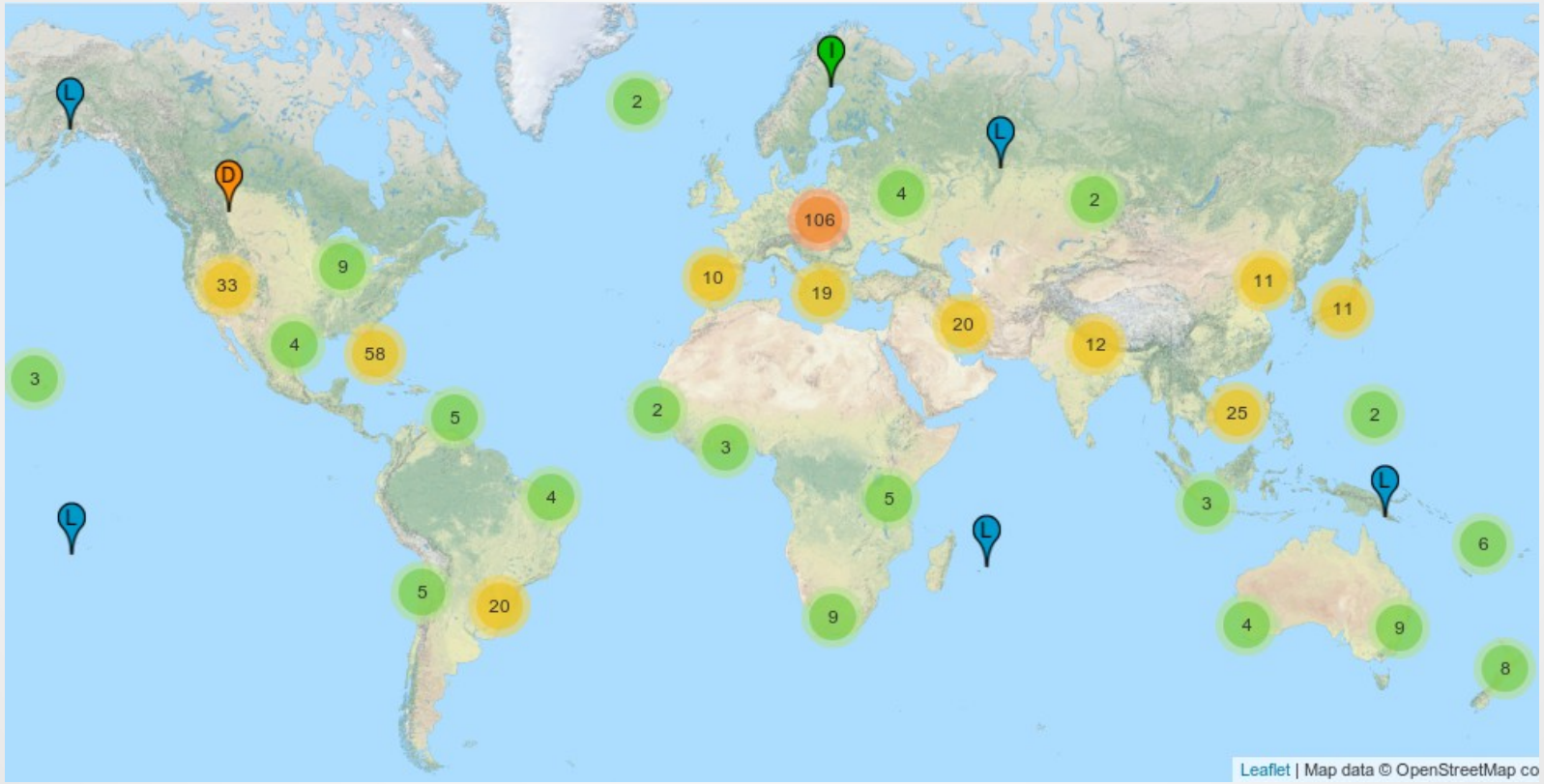
Структура DNS



Структура DNS

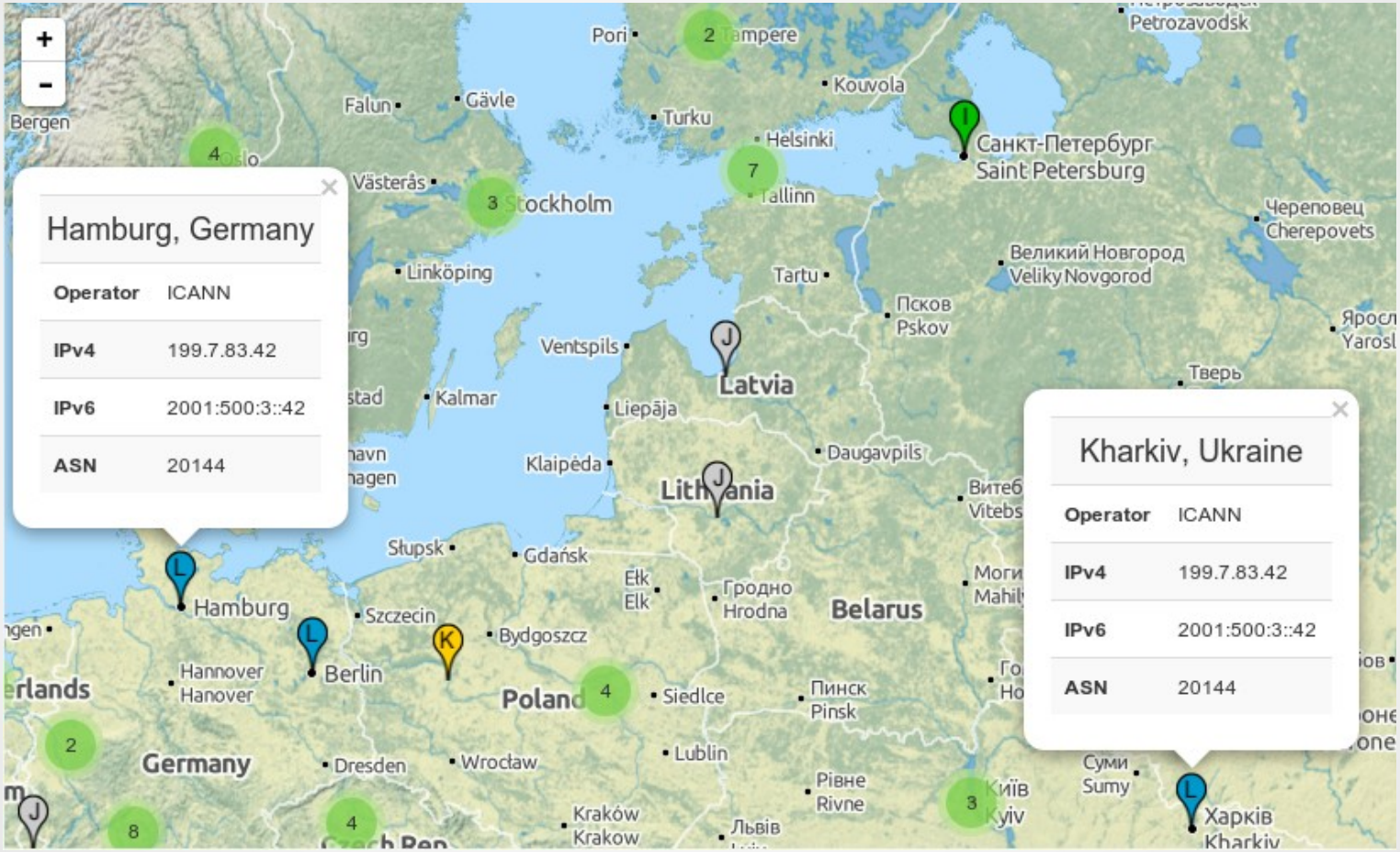
- Доменная структура DNS представляет собой древовидную иерархию, состоящую из **узлов**, **зон**, **доменов** и поддоменов.
- "Вершиной" доменной структуры является **корневая зона**.
- Настройки корневой зоны расположены на множестве серверов/зеркал, размещенных по всему миру и содержат информацию о всех серверах корневой зоны, а так же отвечающих за домены первого уровня (ru, net, org и др).

Структура DNS



http://www.root-servers.org/

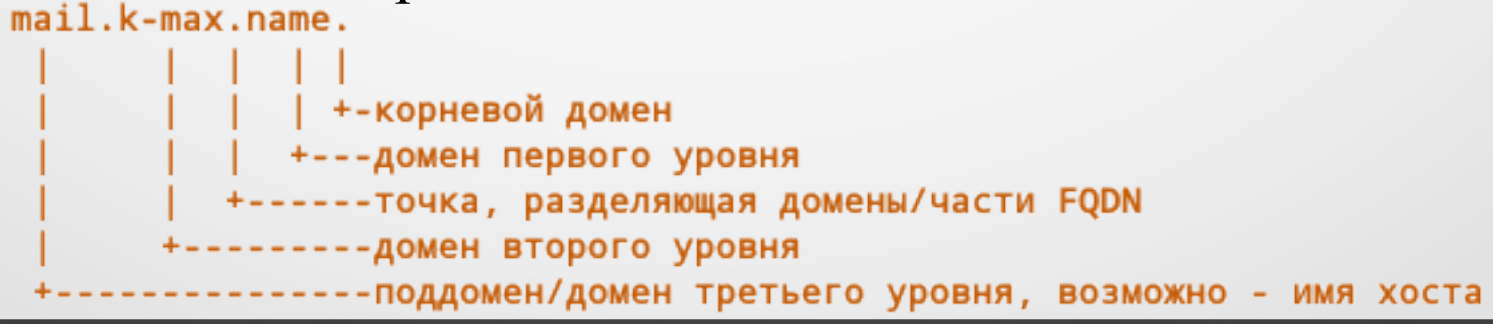
Структура DNS



http://www.root-servers.org/

Структура DNS

- **Домéн** (англ. domain — область) — узел в дереве имён, вместе со всеми подчинёнными ему узлами (если таковые имеются), то есть именованная ветвь или поддерево в дереве имен.
- **Зона** — часть дерева доменных имен, размещаемая как единое целое на некотором сервере доменных имен (DNS-сервере). Целью выделения части дерева в отдельную зону является передача ответственности за соответствующий домен другому лицу или организации. Это называется **делегированием.**
- **FQDN** (англ. Fully Qualifed Domain Name, полностью определённое имя домена) - это имя домена, однозначно определяющее доменное имя и включающее в себя имена всех родительских доменов иерархии DNS, в том числе и корневого.



Ресурсная запись DNS

- **Ресурсная запись** - это единица хранения и передачи информации в DNS. Каждая такая запись несет в себе информацию соответствия какого-то имени и служебной информации в DNS, например соответствие имени домена - IP адреса.

Запись ресурса состоит из следующих полей:

```
name.                TTL    CLASS      TYPE       DATA
```

- **имя (NAME)** — доменное имя, к которому привязана или которому «принадлежит» данная ресурсная запись, либо IP адрес. При отсутствии данного поля, запись ресурса наследуется от предыдущей записи.
- **Time To Live (TTL)** — дословно "время жизни" записи, время хранения записи в кэше DNS (после указанного времени запись удаляется)
- **класс (CLASS)** - определяет тип сети, (в 99,99% случаях используется IN что обозначает - Internet)
- **тип (TYPE)** — тип записи синтаксис и назначение записи
- **данные (DATA)** - различная информация, формат и синтаксис которой определяется типом.

При этом, возможно использовать следующие символы:

- **;** - Вводит комментарий
- **#** - Также вводит комментарии (только в версии BIND 4.9)
- **@** - Имя текущего домена
- **( )** - Позволяют данным занимать несколько строк
- ***** - Метасимвол (только в поле имя)

Основные типы ресурсных записей

- **A** - (address record/запись адреса) отображают имя хоста (доменное имя) на адрес IPv4т(поле NAME - k-max.name., поле TTL - 86400, поле CLASS - IN, поле DATA - 81.177.139.65):

```
k-max.name.             86400   IN      A       81.177.139.65
```

- **AAAA** (IPv6 address record) аналогична записи A, но для IPv6.
- **CNAME** (canonical name record/каноническая запись имени (псевдоним)) - отображает алиас на реальное имя (для перенаправления на другое имя):

```
ftp             86400   IN      CNAME       www.k-max.name.
```

- **PTR** (pointer) - отображает IP-адрес в доменное имя (в специальном домене IN-ADDR.ARPA).

```
50.0.87.194 IN PTR www.ru.
```

Основные типы ресурсных записей

- **MX** (mail exchange) - указывает хосты для доставки почты, адресованной домену. При этом поле **NAME** указывает домен назначения, поля **TTL, CLASS** - стандартное значение, поле **TYPE** принимает значение **MX**, а поле **DATA** указывает приоритет и через пробел - доменное имя хоста, ответственного за прием почты. Например, следующая запись показывает, что для домена k-max.name направлять почту сначала на mx.k-max.name, затем на mx2.k-max.name, если с mx.k-max.name возникли какие-то проблемы. При этом, для обоих MX хостов должны быть соответствующие A-записи:

```
  k-max.name.             17790   IN      MX      10 mx.k-max.name.
k-max.name.             17790   IN      MX      20 mx2.k-max.name.
```

Основные типы ресурсных записей

- **NS** (name server/сервер имён) указывает на DNS-сервер, обслуживающий данный домен. Вернее будет сказать - указвают сервера, на которые делегирован данный домен.

```
k-max.name.             1577    IN      NS      ns2.jino.ru.
k-max.name.             1577    IN      NS      ns1.jino.ru.
```

- **SRV** (server selection) - указывают на сервера, обеспечивающие работу тех или иных служб в данном домене (например Jabber и Active Directory).

Основные типы ресурсных записей

- **SOA** (Start of Authority/начальная запись зоны) - описывает основные/начальные настройки зоны, можно сказать, определяет зону ответственности данного сервера. Поле **Name** содержит имя домена/зоны, поля **TTL, CLASS** - стандартное значение, поле **TYPE** принимает значение SOA, а поле **DATA** состоит из нескольких значений, разделенных пробелами:
  имя главного DNS (Primary Name Server), **адрес администратора зоны**, далее в скобках **- серийный номер файла зоны** (Serial number). *При каждом внесении изменений в файл зоны данное значение необходимо увеличивать*, это указывает вторичным серверам, что зона изменена, и что им необходимо обновить у себя зону. Далее - значения таймеров (**Refresh** - указывает, как часто вторичные серверы должны опрашивать первичный, чтобы узнать, не увеличился ли серийный номер зоны, **Retry** - время ожидания после неудачной попытки опроса, **Expire** - максимальное время, в течение которого вторичный сервер может использовать информацию о полученной зоне, **Minimum TTL** - минимальное время, в течение которого данные остаются в кэше вторичного сервера).

```
k-max.name.             86400   IN      SOA     ns1.jino.ru. hostmaster.jino.ru. (
                                                 2011032003 ; serial (серийный номер)
                                                 28800 ; refresh (обновление)
                                                 7200 ; retry (повторная попытка)
                                                 604800 ; expire (срок годности)
                                                 86400) ; minimum TTL (минимум)
```

Инструменты работы с DNS

- Для разрешения имен и IP адресов клиентскими приложениями используется библиотека Resolver.
- Это функциональность системы (ядра). Приложения посылают системные вызовы gethostbyname(2) и gethostbyaddr(2), а ядро уже на основании настроек в файле /etc/nsswitch.conf определяет по какому пути ему далее действовать

```
root@DNS:~# cat /etc/nsswitch.conf
......
hosts:          files dns
networks:       files
```

- Преобразование имен хостов в IP (строка **hosts: files dns**) сначала из файла /etc/hosts, затем силами DNS
- преобразование имен сетей в IP (строка networks: files) с помощью файла /etc/network.

Инструменты работы с DNS

- Настройка используемых DSN-серверов производится в файле /etc/resolv.conf

```
root@DNS:~# cat /etc/resolv.conf
nameserver 192.168.1.1
nameserver 192.168.1.2
domain  examle.com
```

- Параметр **domain** определяет заданное по умолчанию имя домена, которое будет подставлено, когда DNS не удастся найти имя хоста.
- Существует так же опция **search**, которая задает дополнительные домены, в которых необходимо произвести поиск и разрешение имени хоста.
- Опции search и domain нельзя использовать совместно.

Инструменты работы с DNS

Ответы DNS бывают следующего типа:

- **Авторитативный ответ** (authoritative response) приходит от серверов, являющихся ответственными за зону.
- **Неавторитативный ответ** (non authoritative response) приходит от серверов, которые не отвечают за зону (от кэширующих).

Ответ DNS обычно содержит следующую информацию:

- **Запись заголовка** - служебную информацию о запросе.
- **Запись запроса** - повторяет отправленный запрос.
- **Запись ответа** - собственно, сам ответ.
- **Записи авторитетных серверов** - информацию об авторитетных серверах, хранящих информацию по текущему запросу.
- **Дополнительную информацию** - дополнительные записи, например адреса NS-серверов.

Инструменты работы с DNS

- Утилита dig

```
root@DNS:~# dig ya.ru

; <<>> DiG 9.7.3 <<>> ya.ru (раздел заголовка)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53499
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 2, ADDITIONAL: 3

;; QUESTION SECTION: (раздел запроса)
;ya.ru.                         IN      A

;; ANSWER SECTION: (раздел ответа)
ya.ru.                  4813    IN      A       87.250.250.203
ya.ru.                  4813    IN      A       87.250.251.3
ya.ru.                  4813    IN      A       93.158.134.3
ya.ru.                  4813    IN      A       93.158.134.203
ya.ru.                  4813    IN      A       213.180.204.3
ya.ru.                  4813    IN      A       77.88.21.3
ya.ru.                  4813    IN      A       87.250.250.3

;; AUTHORITY SECTION: (авторитативные сервера)
ya.ru.                  4813    IN      NS      ns1.yandex.ru.
ya.ru.                  4813    IN      NS      ns5.yandex.ru.

;; ADDITIONAL SECTION: (дополнительная информация - адреса авторитативных name servers)
ns5.yandex.ru.          345565  IN      A       213.180.204.1
ns1.yandex.ru.  имя главного DNS (Primary Name Server)        345565  IN      A       213.180.193.1
ns1.yandex.ru.          3565    IN      AAAA    2a0ua.em2:6emb8::1

;; Query time: 7 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Sat Jul  2 23:02:45 2011
;; MSG SIZE  rcvd: 238
```

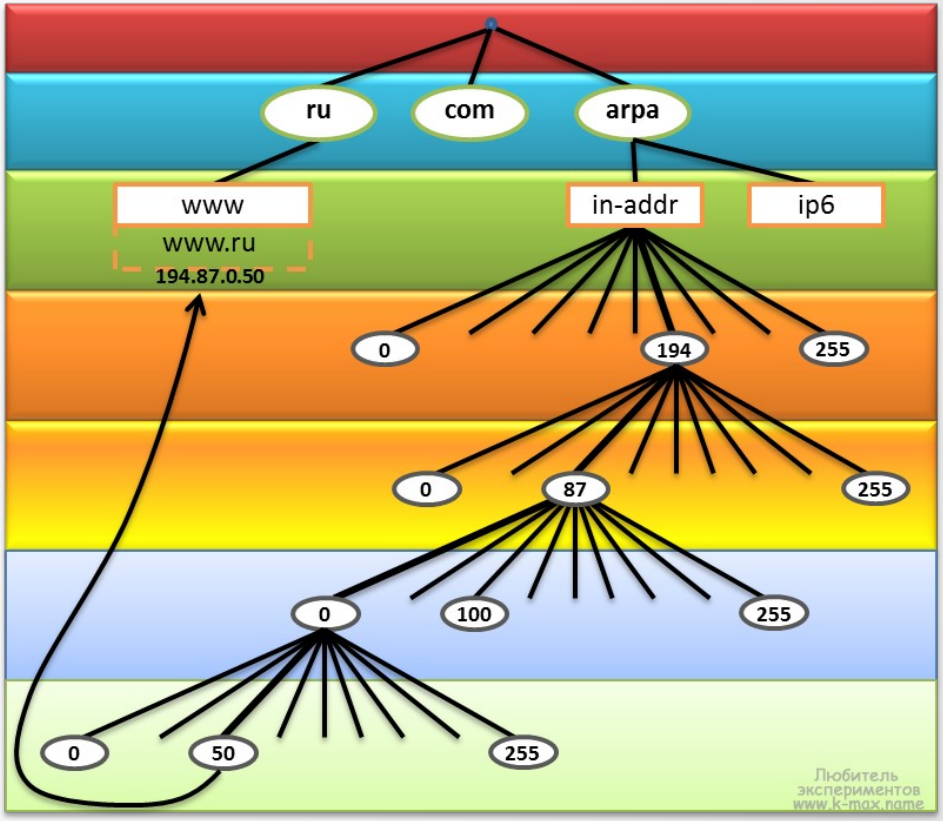
Метод прохождения запроса

Обратные зоны DNS

Для обратного преобразования в DNS используется специальный домен **in-addr.arpa.** Ресурсные записи в данном домене в поле Name содержат IP-адреса, в поле Type - **PTR**, а в поле **Data** - FQDN-имя соответствующее данному IP.

```
[root@DNS~]# dig -x 194.87.0.50
...
;; QUESTION SECTION:
;50.0.87.194.in-addr.arpa.      IN      PTR

;; ANSWER SECTION:
50.0.87.194.in-addr.arpa. 30385 IN      PTR     www.ru.
....
```



DNS-сервер

- **Named -** это демон, входящий в состав пакета **bind9** и являющийся сервером доменных имен.

- Демон named может реализовывать функции серверов любого типа: **master, slave, cache**.

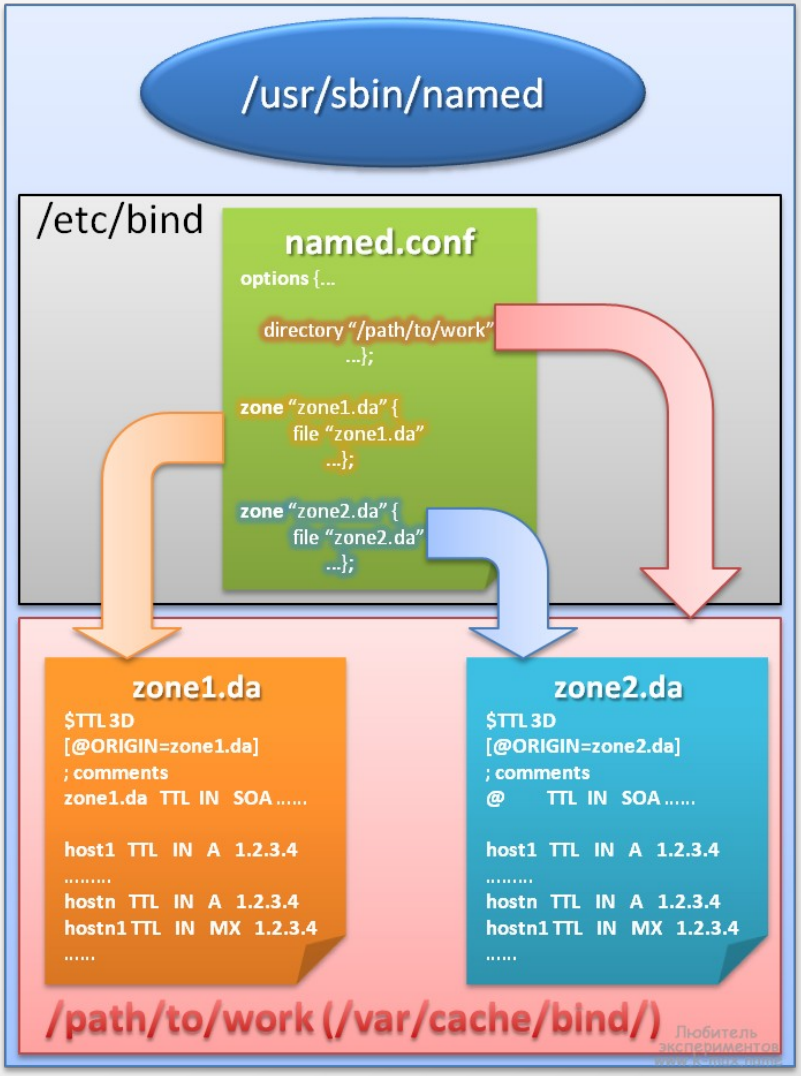
DNS-сервер bind

Установка

apt-get install bind9

DNS-сервер bind

- Исполняемый файл расположен в **/usr/sbin/named**.
- Он берет настройки из основного конфигурационного файла **named.conf** расположен в каталоге **/etc/bind**.
- Здесь описывается рабочий каталог сервера, зачастую это каталог **/var/cache/bind**, в котором лежат файлы описания зон и другие служебные файлы.
- **Соответствие** названия зоны и файла описания зоны задает раздел **zone** с параметром **file**.
- Раздел **zone** так же задает тип ответственности данного сервера за зону (**master, slave** и др.)



DNS-сервер bind

Файл /etc/bind/named.conf раздел options

- **allow-query {список_ip}** - Разрешает ответы на запросы только из список_ip.
- **allow-recursion {список_ip}** - На запросы из список_ip будут выполняться рекурсивные запросы. Для остальных - итеративные. Если не задан параметр, то сервер выполняет рекурсивные запросы для всех сетей.
- **allow-transfer {список_ip}** - Указывает список серверов, которым разрешено брать зону с сервера (в основном тут указывают slave сервера)
- **directory /path/to/work/dir** - указывает абсолютный путь к рабочему каталогу сервера. Этот оператор допустим только в разделе options.
- **forwarders {ip порт, ip порт...}** - указывает адреса хостов и если нужно порты, куда переадресовывать запросы (обычно тут указываются DNS провайдеров ISP).
- **forward ONLY или forward FIRST** - параметр first указывает, DNS-серверу пытаться разрешать имена с помощью DNS-серверов, указанных в параметре forwarders, и лишь в случае, если разрешить имя с помощью данных серверов не удалось, то будет осуществлять попытки разрешения имени самостоятельно.
- **notify YES|NO** - YES - уведомлять slave сервера об изменениях в зоне, NO - не уведомлять.
- **recursion YES|NO** - YES - выполнять рекурсивные запросы, если просит клиент, NO - не выполнять (только итеративные запросы). Если ответ найден в кэше, то возвращается из кэша. (может использоваться только в разделе Options)

DNS-сервер bind

cat /etc/bind/named.conf

```
acl "lan" {
        192.168.1.1/24;
        127.0.0.1;
};

options {
        directory "/var/cache/bind";
        /*
        * Тут сказано, что если используется фаерволл, то необходимо
        *  нашему серверу создать соответствующие правила
        *  то есть открыть доступ по 53 TCP и UDP порту
        */

        forward first;              // задаем пересылку только первого запроса

        forwarders {                // указываем DNS сервера для пересылки
                83.239.0.202;    // предоставленные провайдером
                213.132.67.110;  // ибо до них ближе чем до корневых
        };

       listen-on { lan; };        // пусть слушает только нужные интерфейсы
       allow-query { lan; };      // разрешить запросы только из локальной сети
       allow-recursion { lan; };  // рекурсивные запросы тоже только из локальной
       allow-transfer { none; };  // трансфер зон нам не нужен

       version "unknown";         // не отображать версию DNS сервера при ответ

       auth-nxdomain no;    # для совместимости RFC1035
       listen-on-v6 { none; };    //IPv6 нам не нужен
       };

// описание настроек корневых серверов
zone "." {
        type hint;
        file "db.root";
};

// нижеописанные зоны определяют сервер авторитетным для
петлевых
// интерфейсов, а так же для броадкаст-зон (согласно RFC 1912)

zone "localhost" {
        type master;
        file "localhost";
};

zone "127.in-addr.arpa" {
        type master;
        file "127.in-addr.arpa";
};

zone "0.in-addr.arpa" {
        type master;
        file "0.in-addr.arpa";
};

zone "255.in-addr.arpa" {
        type master;
        file "255.in-addr.arpa";
}
```

Bind9 — создание зоны

Создание новой зоны в файле **named.conf**

```
zone "example.com" {
        type master;
        file "example.com";
        allow-transfer { 10.0.0.191; };
};
```

Bind9 — описание зоны

Описание зоны в файле **/var/cache/bind/example.com**

```
$TTL 3D
@       IN      SOA     ns.example.com. root.example.com. (
                                2011070601      ; serial
                                8H              ; refresh
                                2H              ; retry
                                2W              ; expire
                                1D)             ; minimum
@       IN      NS      ns.example.com.
@       IN      NS      ns2.example.com.
@       IN      A       10.0.0.152
@       IN      MX      5 mx.example.com.
ns      IN      A       10.0.0.152
ns2     IN      A       10.0.0.191
mx      IN      A       10.0.0.152
www     IN      CNAME   @
```

Bind9 — вторичный сервер

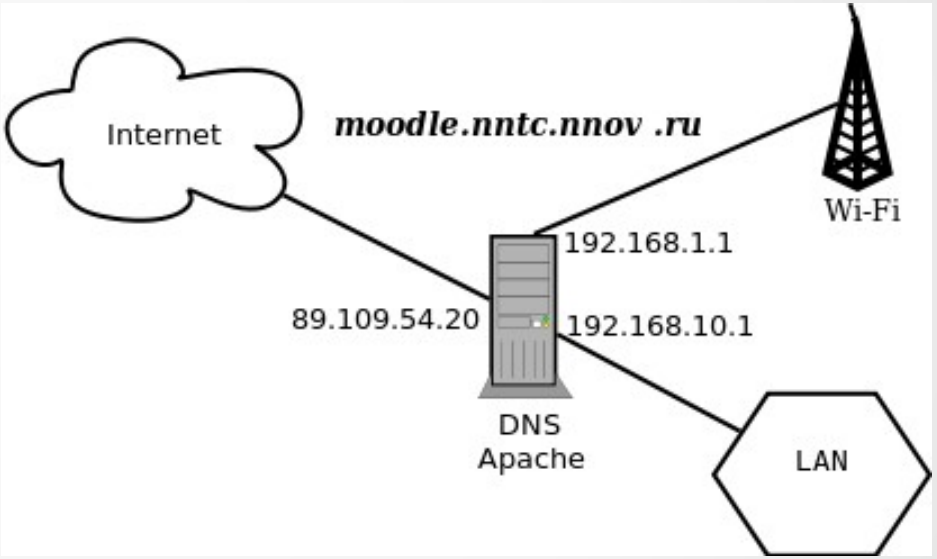
Настройка Slave-сервера зоны **named.conf**

```
zone "example.com" {
        type slave;
        file "example.com";
        masters { 10.0.0.152; };
};
```

```
options {
        directory "/var/cache/bind";
        allow-query { any; };      // отвечать на запросы со всех интерфейсов
        recursion no;              // запретить рекурсивные запросы
        auth-nxdomain no;          // для совместимости RFC1035
        listen-on-v6 { none; };    // IPv6 нам не нужен
        version "unknown";         // не отображать версию DNS сервера при ответах
};
```

Split DNS

- Конфигурация BIND, позволяющая использовать различные настройки DNS в зависимости от адреса источника запроса.
- Часто используется для создания одноименных ресурсов для внутренней сети и внешней сети Internet



Split DNS

nano /etc/bind/named.conf

```
acl «internals» {192.168.0.0/16; 127.0.0.1/32;};


view «internal» {
        match-clients { «internals»; };
        zone «moodle.nntc.nnov.ru» {
        type master;
        file «/etc/bind/db.moodle.nntc.nnov.ru.internal»;
        };                                              zone «nntc.nnov.ru» {
};                                                          type master;
                                                            file «/etc/bind/nntc.nnov.ru.external»;
                                                        };
```

Регистрация доменных зон

- Регистратором для корневого домена является организация ICANN. Чтобы стать регистратором доменов в зонах второго уровня (.com .net .org .biz .info .name .mobi .asia .aero .tel .travel .jobs ...), необходимо получить аккредитацию ICANN.
- Правила регистрации в международных (gTLD - com., org, и др.) доменах устанавливаются ICANN. Правила регистрации в национальных (ccTLD - ru, us и др.) доменах устанавливаются их регистраторами и/или органами власти соответствующих стран, например единые правила для всех регистраторов в доменах .ru, и .рф задаются Координационным центром национального домена сети Интернет.