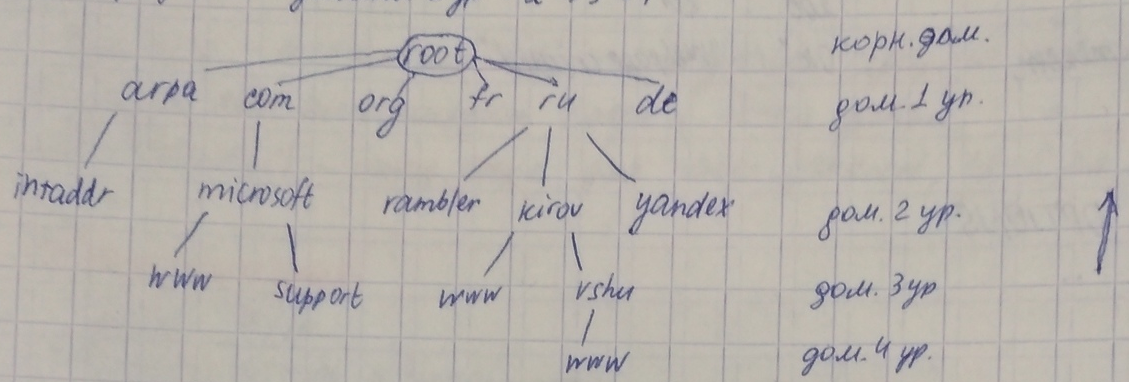
**DNS (Domain Name System)**

DNS – иерархическая БД, сопоставляющая имена сет. узлов и их сет. служб IP-адресам узлов  
**Сост из:**  
**\*** **пр-во имен DNS** и соотв. рес. записи – сама распределенная бд DNS  
**\* серверы имен DNS** – компы, хран. БД и отвеч на запросы клиентов  
**\* DNS-клиенты** – компы, посыл запросы серверам для получ рес. записей

Протокол стека TCP/IP (прикладной уровень)  
описан в RFC 1034, 1035, STD 13  
ICANN – организация, обесп управление всем адресным пр-вом Internet

1983 (Пол Мокапетрис) : по дом. имени авто- опред IP  
корн домен -> домены 1 ур -> 2->3->4

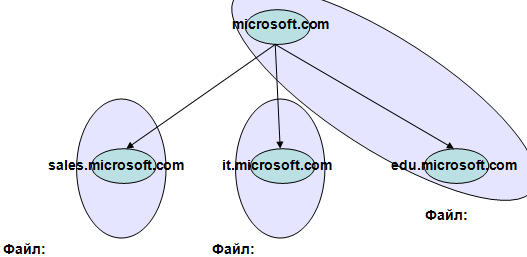
**Пр-во имен DNS:**  
arpa –исп для обрат разреш (IP -> полное имя узла)

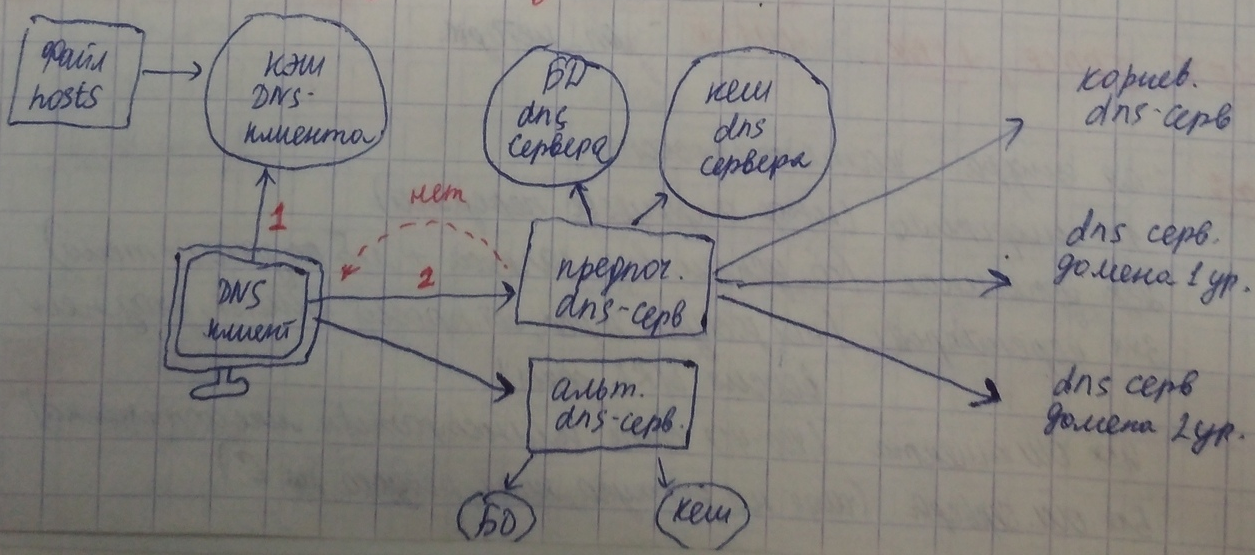
имена 1 ур – их 16

2букв имена для стран

**Фрагмент пр-ва дом. имен Интернета:  
www. vshu.kirov.ru .**  
имя хоста dns-суффик м. опуск

Мы вводим ‘onliner.by’ в строку, браузер обращ к DNS, чтобы узнать ip, идет с листьев (к верхней части root доходит лишь 18%), обычно разреш. имен на ранних стадиях (4->3…)

**Домен и зона:**прво имен DNS нач с домен ms.com(мал гориз овал)  
3 поддомена sales.ms.com, …  
*Домен* – логическое понятие, относ к распред имен  
*Зона* – способ предст инфы о домене и его поддоменах в хранилище серверов DNS

**Процесс обработки рекурс. DNS-запроса:**  


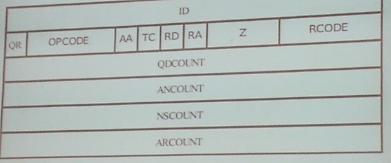
- итерат запросы : К посыл С запрос, в кот требует дать наилучший ответ без обращ к др С  
- рекурс запросы : К посыл С запрос, в кот требует дать оконч ответ даже если надо обращ

БД DNS-сервер сод. записи о ресурсах, в кот. сод. инфа, необх. для разреш дом. имен и правильн. функ-я службы DNS. Более 20 типов записей о ресурсах:

**ЗАПИСЬ SOA:**  
\* **имя домена**  
\* **почтовый адрес админа**  
\* **порядок** – число, увел. при измен зоны  
\* **период обновл** – для вторич серверов  
\* **задержка перед след. попыткой обновл** (после неудачи)  
\* **интервал времени**, ч/кот сервер утратит статус ответственного после обновл  
\* **мин время жизни** – показ. другим серверам, как долго они м. польз д-ми д-го сервера

**ЗАПИСЬ А:**  
связ. доменное имя и ip-адрес  
если создать неск. записей с одним и тем же дом.именем но разными ip, это позвол **равномерно** распред нагрузку м/неск хостами **(карусель)**  
сервер выбир **ближайший** ip к клиенту

**ЗАПИСЬ CNAME:**  
позв одному ip сопоставить неск. доменных имен  
**ЗАПИСЬ MX:**  
связ имя почт. домена с именем хоста, содержащего почтовый сервер  
можно указ неск MX-записей с указ приоритета  
**ЗАПИСЬ PTR:**  
запись обратная записи А (зона обратного просмотра)  
**ЗАПИСЬ NS:**  
опред полномочный сервер имен субдомена.  
связ. имя субдомена с именем полномочного dns-сервера

**Формат пакета DNS:**  
**ID** – поле 2 байт.  
К в DNS-запросе заполн. неким уник id транзакции  
С в DNS-ответе помещ в это поле тот же id

Т.к. обмен д-ми м/КС носит диалоговый характер и отд. лог.соединение для разреш каждого имени не устан, то клиенту, пославшему DNS запрос необходимо идентиф, какой именно из полученных DNS-ответов соотв. посланному запросу, с пом. поля id

**З А Г О Л О В О К :**

**QR** – 1 бит: явл ли данный пакет запросом (0) или ответом (1)  
**OPCODE** – тип запроса  
**AA** – 1 бит: (им. смысл только в ответе) указ, что ответ *авторитетный*

флаг устан => С явл. хранителем БД DNS, из кот получена инфа

иначе => С извлек инфу из своего кэша разреш имен

**TC** – 1 бит: этот флаг устан в ответе, если С не смог поместить всю инфу

из-за ограничений на длину UDP дейтаграммы

**RD** – 1 бит: *recursion desired*

в запросе означ, что К просит С самостоятельно разреш имя и сообщ т. оконч ответ

**RA** – 1 бит: *recursion available*

в ответах С сообщ К, поддерж он рекурсив. обслуж (1) или нет (0)

**Z** – 3 бита: не использ и дб = 0

**RCODE** – 2 байт: код ответа – успешно или с ошибкой (причина – RFC1035)

0: запрос вып успешно

1: С не смог понять формата запроса К

2: в С внутр неисправности

3: имени, кот. запросил К, не сущ. (м возвр только авторитетный С)

4: С не м вып запрос данного типа

5: С не м вып запрос из-за политик безопасности

**4 С Л О В А :**

QDCOUNT – кол-во записей в question section

ANCOUNT – кол-во записей в answer section

NSCOUNT – кол-во записей в authority section

ARCOUNT – кол-во записей в additional record section

**\* Секция DNS-запросов (Queston section)**

здесь К передает запросы С, сообщая для какого имени DNS необх разрешить запись DNS и ее тип  
ее заполн К, С включ в ответ и содержимое этой секции запросов

**\* Секция DNS-ответов (Answer section)**

здесь С сообщ К ответ  
сод запрошенное знач в бд DNS

**\* Секция сведений об авторитетных DNS серверах (Authority section)**

заполн С

сод. с пом. каких авторит. серверов получена инфа в секции ответов

если С отвеч на запросы итерационно, *секция ответов* НЕ мб заполнена и С впис в Authority section сведения об авторит серверах, к кот. К м обратиться

**\* Секция доп инфы (Additional Recors section)**

сервера м. сообщ известные им IP серверов, чьи ИМЕНА были сообщены в Authority section

**УТИЛИТА NSLOOKUP**

исп для проверки способности DNS-серверов вып разрешение имен

М. работать в 2 режимах:  
\* если указан какой-либо ключ, то *режим ком.строки* – обычный режим запуска утилит ком.строки

\* *интерактивный режим* – возм ввод команд и ключей утилиты без повтор ввода имени утилиты

Команды утилиты nslookup:

\* help или ? – вывод справки о к-дах и параметрах утилиты

\* set – устан параметров работы утилиты

\* server <имя> - устан сервера по умолч, исп-мого утилитой с пом. тек. сервера по умолч

\* lserver <имя> - устан сервера по умолч утилиты с пом. первоначального

\* root – устан сервера по умолч утилиты на корневой сервер

\* ls <домен> - вывод инфы о соответствии домен. имен IP-адресам для зад. домена

\* exit – выход из интерактивного режима