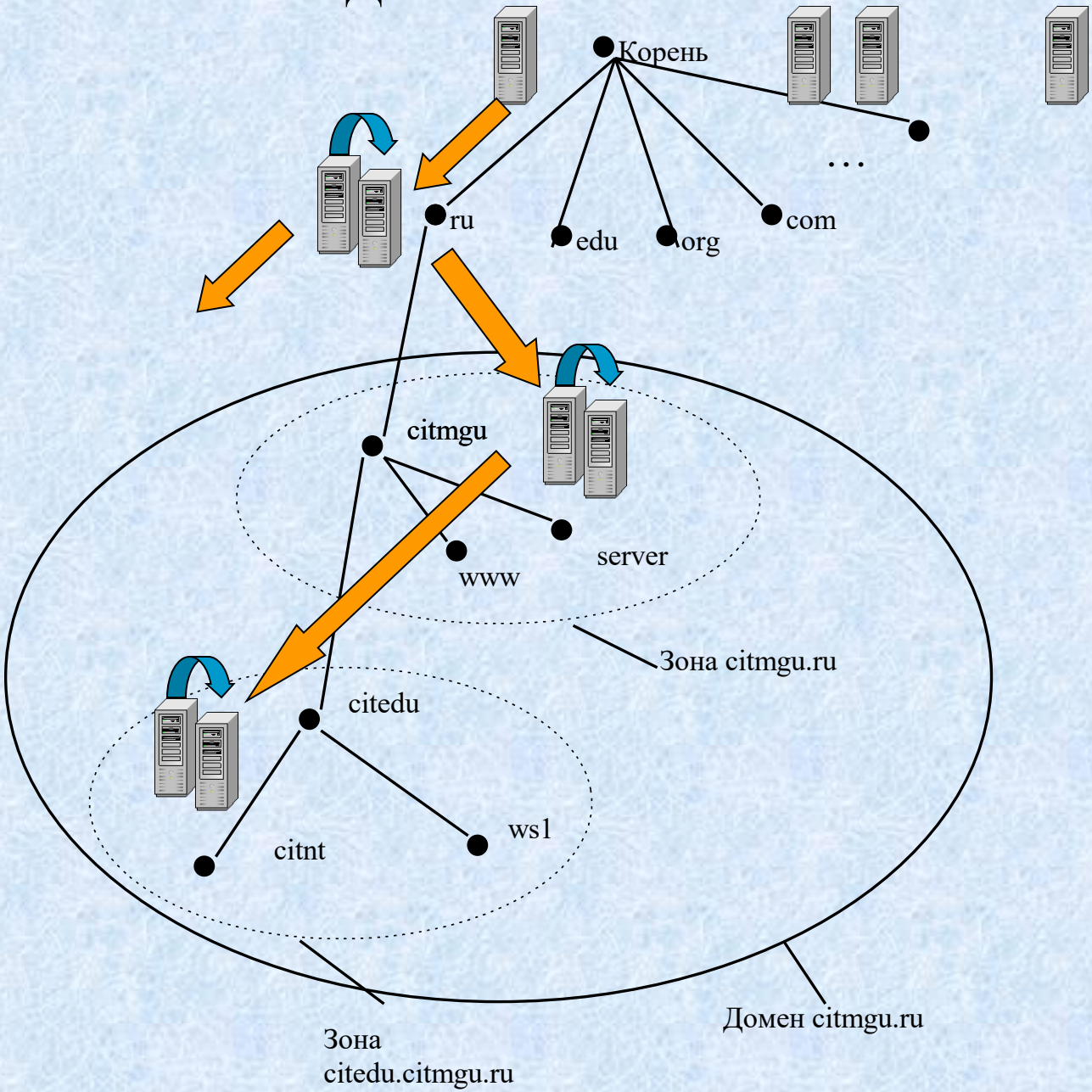
Система DNS – установление соответствия между символьными именами и IP-адресами

- распределенная база данных с иерархическими связями
- архитектура клиент-сервер
- клиент - резольвер: код, встраиваемый в прикладные программы, например, FTP
- DNS-сервер ведет имена своей зоны имен
- Соответствие имен и адресов для зоны набирается вручную в виде текстового файла
- Основная реализация - служба BIND (Berkeley Internet Name Domain) для Unix
- Сервер BIND - программа named
- Транспорт - UDP (порт 53)

Домены и зоны Internet



Иерархия зон

- **Домен** - поддерево имен, включающее все поддомены
- **Зона** - административная часть домена, связное поддерево, которая обслуживается определенным сервером DNS (или несколькими реплицирующимися серверами DNS)
- Большой домен обычно разбивается на несколько зон, каждая из которых ведется одной организацией
- Корневые серверы содержат записи о серверах имен зон верхнего уровня, то есть зон *.com, .edu, .net, .ru,* и т.д.
- Когда сервер имен отдает ведение некоторой зоны, начинающейся с поддомена, входящего в домен его зоны, то говорят, что он **делегирует** зону другому серверу

Итеративный способ:

- запрашивающая сторона получает в ответ не конечный результат, а IP-адрес следующего сервера имен
- запрашивающая сторона делает очередную итерацию запроса - получает IP-адрес следующего сервера имен и т.д.

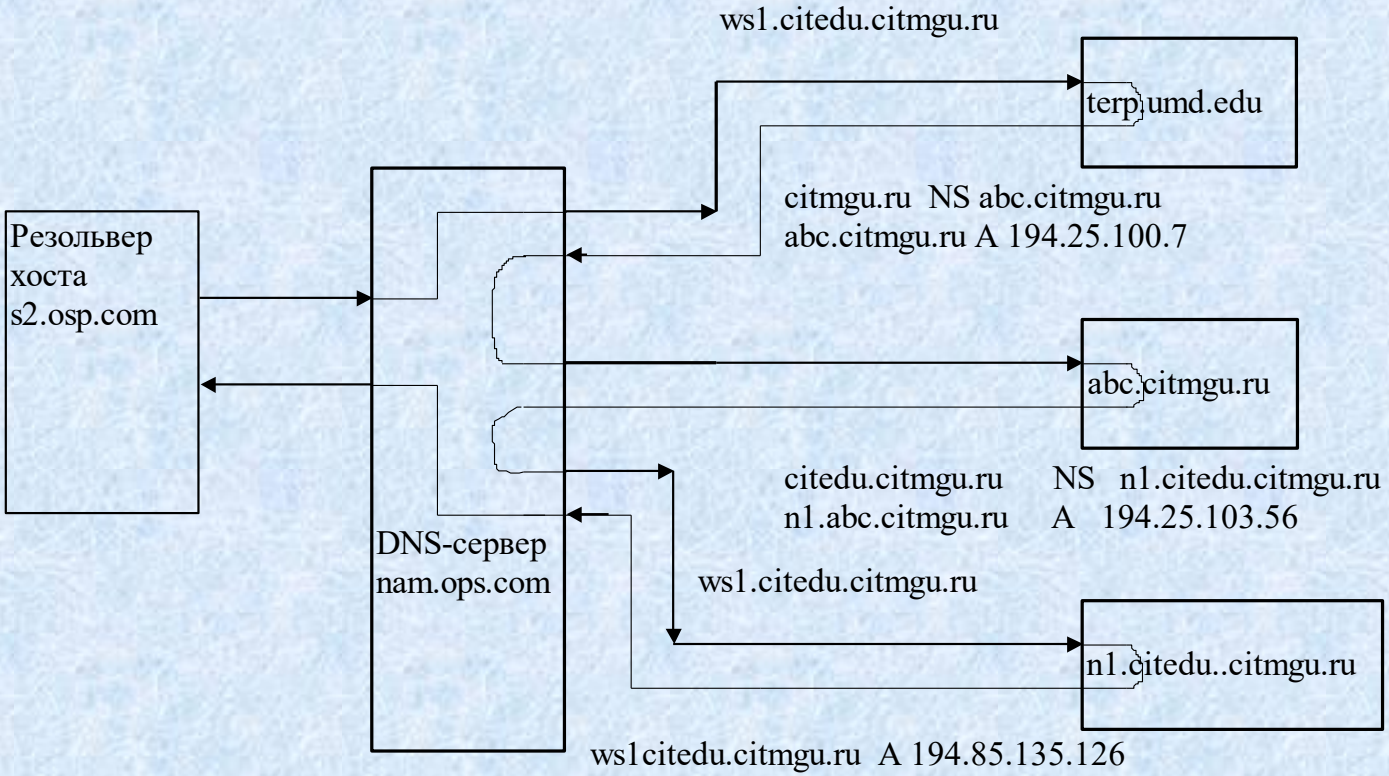
Рекурсивный способ:

- запрашивающая сторона сразу получает конечный результат.

Корневые серверы всегда отвечают нерекурсивно - для уменьшения нагрузки

Способы взаимодействия резольверов и серверов

- итеративный (нерекурсивный)
- рекурсивный.



Типы серверов имен для зоны

Каждый сервер имен может выполнять для какой-либо зоны одну из трех ролей:

- Primary server
- Secondary server
- Cashing-only server

Primary server

- является первичным источником данных для определенной зоны
- загружает информацию о соответствии адресов непосредственно из файлов, созданных администратором зоны
- является *полномочным* (authoritative) сервером этой зоны, что означает, что он располагает полной информацией о зоне и отвечает за ее достоверность
- для определенной зоны может быть только один первичный сервер

Secondary server

- получает по сети базу данных зоны от первичного сервера - реплику базы
- процесс репликации файла базы данных зоны называется ***передачей файла зоны*** **(zone file transfer)**
- вторичный сервер периодически считывает файл базы зоны
- вторичных серверов может быть несколько
- вторичный сервер также является полномочным для своей зоны

Cashing-only server

- использует для ответов только данные, полученные из ответов других серверов имен - кэширует ответы
- не является полномочным сервером какой-либо зоны

Обратная зона

- Предназначена для решения обратной задачи - нахождению имени по известному IP-адресу.
- Обратная задача решается в Internet за счет организации обратных зон и серверов, ведущих эти зоны.
- Обратная зона - это зона, которая хранит соответствие между IP-адресами некоторой сети и именами хостов, принадлежащих этой сети

Пример обратной зоны

106.31.192.IN-ADDR.ARPA

- Первичные серверы для обратных зон используют файлы баз данных, не зависящие от файлов основных зон.
- Такая организация данных может приводить к несогласованности, так как оно и то же соответствие вводится в файлы дважды.
- Многие программы и утилиты пытаются найти имя узла по его адресу, если пользователем задан только адрес или этот адрес программа узнала из пришедшего пакета
- Если обратной записи не существует - возможна большая задержка старта утилиты, например FTP

Файлы базы данных сервера named

Первичный сервер **named** хранит свою базу данных в файлах нескольких типов:

- *named.boot* - файл описания базы данных. Устанавливает общие параметры и указывает источники данных. Этими источниками могут быть локальные файлы или удаленные серверы.
- *named.ca* - указывает на корневые серверы
- *named.local* - используется для локального разрешения адреса обратной связи
- *named.hosts* - файл зоны, который отображает имена на адреса
- *named.rev* - файл обратной зоны, который отображает адреса на имена

В файле named.boot для описания настроек named используются следующие команды:

directory **-** адрес каталога, в котором находятся все остальные файлы

primary **-** объявляет сервер как первичный для определенной зоны, указывает имя файла этой зоны

secondary - объявляет сервер вторичный для определенной зоны, указывает адрес первичного сервера этой зоны

cashe - указывает на файл кэша

forwarders - перечисляет серверы, которым будет передаваться запрос

slave - вынуждает сервер работать только путем передачи запроса серверам, указанным в списке forwarders

Примеры записей в файлах сервера named

Сервер cashing-only, файл named.boot:

```
;
; cashing-only configuration
;
primary      0.0.127.IN-ADDR.ARPA    /etc/named.local
cashe                                    /etc/named.ca
```

Первичный сервер, файл name.boot:

```
;
; citmgu.ru  primary name server boot file
;
directory                                   /etc
primary   citmgu.ru                    named.hosts
primary   135.85.194.IN-ADDR.ARPA        named.rev
primary     0.0.127.IN-ADDR.ARPA       named.local
cashe                                     named.ca
```

Вторичный сервер, файл named.boot:

```
;
; citmgu.ru  secondary name server boot file
;
directory                                                    /etc
secondary     citmgu.ru        194.85.135.16      citmgu.ru.hosts
secondary  135.85.194.IN-ADDR.ARPA  194.85.135.16  135.85.194.rev
primary       0.0.127.IN-ADDR.ARPA                    named.local
cashe                                                      named.ca
```

Типы записей в файле зоны

Resource Record Text Name	Record Type	Описание
Start of Authority	SOA	Отмечает начало данных зоны; определяет параметры, которые влияют на зону в целом
Name Server	NS	Идентифицирует сервер имен
Address	A	Отображает имя в адрес
Pointer	PTR	Отображает адрес в имя
Mail Exchange	MX	Определяет, куда доставлять почту для определенного доменного имени
Canonical Name	CNAME	Определяет псевдоним (alias) хоста
Host Information	HINFO	Описывает аппаратное и программное обеспечение хоста
Well Known Service	WKS	Объявляет сетевой сервис

Типы записей в файле зоны
(продолжение)

Каждая запись соответствует общему формату, определенному спецификацией RFC-1033:

```
<name> <ttl> <class> <type> <data>
```

name - это имя объекта записи, соответствует хосту или домену

ttl **-** определяет время в секундах, в течение которого данная запись сохраняется в кэше. Максимальное значение ttl - 99999999

class - определяет класс записи описания ресурса, в Internet используется только один класс записей - **класс IN**.

type - определяет тип записи описания ресурсов (A, NS, MX, ...)

data - указываются данные для каждой записи описания ресурсов

Примеры записей в файле зоны **nuts.com**

```
;
;
@    IN   SOA almond.nuts.com  jan.almond.nuts.com (
                10118    ; Serial
                43200   ; Refresh
                3600     ; Retry
                3600000; Expire
                2592000 ); Minimum

; Серверы имен и почтовые серверы
          IN   NS       almond.nuts.com.
          IN   NS       filbert.nuts.com.
          IN   NS       foo.army.mil.
          IN   MX       10 almond.nuts.com.
          IN   MX       20 pecan.nuts.com.
;
; Локальный хост
localhost     IN   A        127.0.0.1

;
```

```
; Хосты зоны
almond      IN  A       128.66.12.1
                        IN  MX      5 almond.nuts.com.
loghost     IN  CNAME   almond.nuts.com.
peanut      IN  A       128.66.12.2
            IN  MX      5 peanut.nuts.com.
goober      IN  CNAME   peanut.nuts.com.
pecan       IN  A       128.66.12.3
walnut      IN  A       128.66.12.4
filbert     IN  A       128.66.1.2

; Шлюз, используемый в зоне
mil-gw      IN  A       26.104.0.19
;

; Имена серверов внутри домена
pack.plant    IN  A       128.66.18.15
acorn.sales   IN  A       128.66.6.1
;
; Определение поддоменов
;
plant       IN  NS      pack.plant.nuts.com.
            IN  NS      pecan.nuts.com.
sales       IN  NS      acorn.sales.nuts.com.
            IN  NS      pack.plant.nuts.com.
```

Пакет DNS-запроса на разрешение имени cit-u.citmgu.ru:

```
UDP: Src Port: Unknown, (1041); Dst Port: DNS (53); Length = 41 (0x29)
    UDP: Source Port = 0x0411
    UDP: Destination Port = DNS
    UDP: Total length = 41 (0x29) bytes
    UDP: UDP Checksum = 0x8B4F
    UDP: Data: Number of data bytes remaining = 33 (0x0021)
DNS: 0x1:Std Qry for cit-u.citmgu.ru. of type Host Addr on class INET
addr.
    DNS: Query Identifier = 1 (0x1)

DNS: DNS Flags = Query, OpCode - Std Qry, RD Bits Set, RCode - No error
        DNS: 0............... = Query
        DNS: .0000........... = Standard Query
        DNS: .....0.......... = Server not authority for domain
        DNS: ......0......... = Message complete
        DNS: .......1........ = Recursive query desired
        DNS: ........0....... = No recursive queries
        DNS: .........000.... = Reserved
        DNS: ............0000 = No error
    DNS: Question Entry Count = 1 (0x1)
    DNS: Answer Entry Count = 0 (0x0)
    DNS: Name Server Count = 0 (0x0)
    DNS: Additional Records Count = 0 (0x0)

DNS: Question Section: cit-u.citmgu.ru. of type Host Addr on class INET
addr.
        DNS: Question Name: cit-u.citmgu.ru.
        DNS: Question Type = Host Address
        DNS: Question Class = Internet address class
```

На этот запрос DNS- сервер прислал следующий ответ (первая часть):

```
UDP: Src Port: DNS, (53); Dst Port: Unknown (1041); Length = 132
(0x84)
    UDP: Source Port = DNS
    UDP: Destination Port = 0x0411
    UDP: Total length = 132 (0x84) bytes
    UDP: UDP Checksum = 0x5333
    UDP: Data: Number of data bytes remaining = 124 (0x007C)
DNS: 0x1:Std Qry Resp. for cit-u.citmgu.ru. of type Host Addr on
class INET addr.
    DNS: Query Identifier = 1 (0x1)
    DNS: DNS Flags = Response, OpCode - Std Qry, RD RA Bits Set,
RCode - No error
        DNS: 1............... = Response
        DNS: .0000........... = Standard Query
        DNS: .....0.......... = Server not authority for domain
        DNS: ......0......... = Message complete
        DNS: .......1........ = Recursive query desired
        DNS: ........1....... = Recursive queries supported by
server
        DNS: .........000.... = Reserved
        DNS: ............0000 = No error
    DNS: Question Entry Count = 1 (0x1)
    DNS: Answer Entry Count = 1 (0x1)
    DNS: Name Server Count = 2 (0x2)
    DNS: Additional Records Count = 2 (0x2)
    DNS: Question Section: cit-u.citmgu.ru. of type Host Addr on
class INET addr.
        DNS: Question Name: cit-u.citmgu.ru.
        DNS: Question Type = Host Address
        DNS: Question Class = Internet address class
```

2 часть

```
DNS: Answer section: cit-u.citmgu.ru. of type Host Addr on class INET addr.
     DNS: Resource Name: cit-u.citmgu.ru.
     DNS: Resource Type = Host Address
     DNS: Resource Class = Internet address class
     DNS: Time To Live = 294389 (0x47DF5)
     DNS: Resource Data Length = 4 (0x4)
     DNS: IP address = 194.85.135.66
DNS: Authority Section: citmgu.ru. of type Auth. NS on class INET addr.
     DNS: Resource Record: citmgu.ru. of type Auth. NS on class INET addr.
          DNS: Resource Name: citmgu.ru.
          DNS: Resource Type = Authoritative Name Server
          DNS: Resource Class = Internet address class
          DNS: Time To Live = 342682 (0x53A9A)
          DNS: Resource Data Length = 2 (0x2)
          DNS: Authoritative Name Server: cit-u.citmgu.ru.
     DNS: Resource Record: citmgu.ru. of type Auth. NS on class INET addr.
          DNS: Resource Name: citmgu.ru.
          DNS: Resource Type = Authoritative Name Server
          DNS: Resource Class = Internet address class
          DNS: Time To Live = 342682 (0x53A9A)
          DNS: Resource Data Length = 8 (0x8)
          DNS: Authoritative Name Server: ns.co.ru.
DNS: Additional Records Section: cit-u.citmgu.ru. INET addr.
DNS: Resource Record: cit-u.citmgu.ru. of type Host Addr on class INET addr.
          DNS: Resource Name: cit-u.citmgu.ru.
          DNS: Resource Type = Host Address
          DNS: Resource Class = Internet address class
          DNS: Time To Live = 294389 (0x47DF5)
          DNS: Resource Data Length = 4 (0x4)
          DNS: IP address = 194.85.135.66
```

BIND — Berkeley Internet Name Domain

- BIND — наиболее популярная реализация стандартов DNS, распространяемая бесплатно Internet Software Consortium (http://www.isc.org), стандарт "де факто"
- Применяется большинством Internet сервис-провайдеров
- Поставляется в исходных кодах (C++) в вариантах, оптимизированных для работы под управлением различных версий Unix (Solaris, HP-UX, UnixWare, Lynux, FreeBSD и т.д.), а также Windows NT (разработка Nortel Networks)

Версии **BIND 8.x.x** являются эталонной реализацией большинства новых протоколов DNS:

- Динамические обновления базы DNS (DNS Dynamic Updates, RFC 2136) — связь с сервисом DHCP
- Уведомления об изменениях в данных зоны первичного сервера DNS — повышается согласованность и достоверность распределенной базы DNS (DNS Change Notification, RFC 1996)
- Аутентификация и контроль целостности записей зон DNS и DNS-серверов с помощью цифровой подписи на основе техники публичных ключей (DNS Security, RFC 2065)
- Аутентификация и контроль целостности динамических обновлений зоны DNS (Secure DNS Dynamic Update, RFC 2137)
- Кэширование негативных ответов (Nagative Cashing, RFC 2308)

BIND 8.2.x поддерживает:

- несколько виртуальных DNS-серверов
- полностью новый синтаксис описания конфигурации DNS
- контроль доступа для запросов, передач зоны и обновлений на основе правил для IP-адресов

BIND 8.2.x включает:

- Domain Name System сервер (named)
- библиотеку Domain Name System resolver
- средства для тестирования корректности операций сервера DNS