

# Лекция № 4. Служба DNS

## Содержание

1. Исторический обзор и принципы DNS.
2. Понятие домена и зоны.
3. Процедура разрешения имен.
4. Типы серверов

# Исторический обзор проблемы

Людям удобнее работать с символьными именами хостов для нежели с IP-адресами.

DNS существовала не с момента рождения TCP/IP сетей. Для разрешения символьных имен использовались таблицы соответствия числовых адресов именам машин.

Файл `hosts.txt` можно было получить по FTP.

- несогласованность версий
- большой объем трафика

# Появление DNS

Paul Mockapetris автор DNS.

DNS – централизованная служба, основанная на распределенной базе отображений «доменное имя – IP-адрес».

RFC-882 и RFC-883, 1984 г.

В 1987 г. RFC-882 и RFC-883 заменены на RFC-1034 и RFC-1035.

Файл host и плоские имена сегодня

Современные ОС поддерживают таблицы соответствия IP-адреса и имени хоста – это текстовые файлы с именем hosts.

127.0.0.1 localhost

77.88.21.3 www.google.com

Файл host и плоские имена сегодня

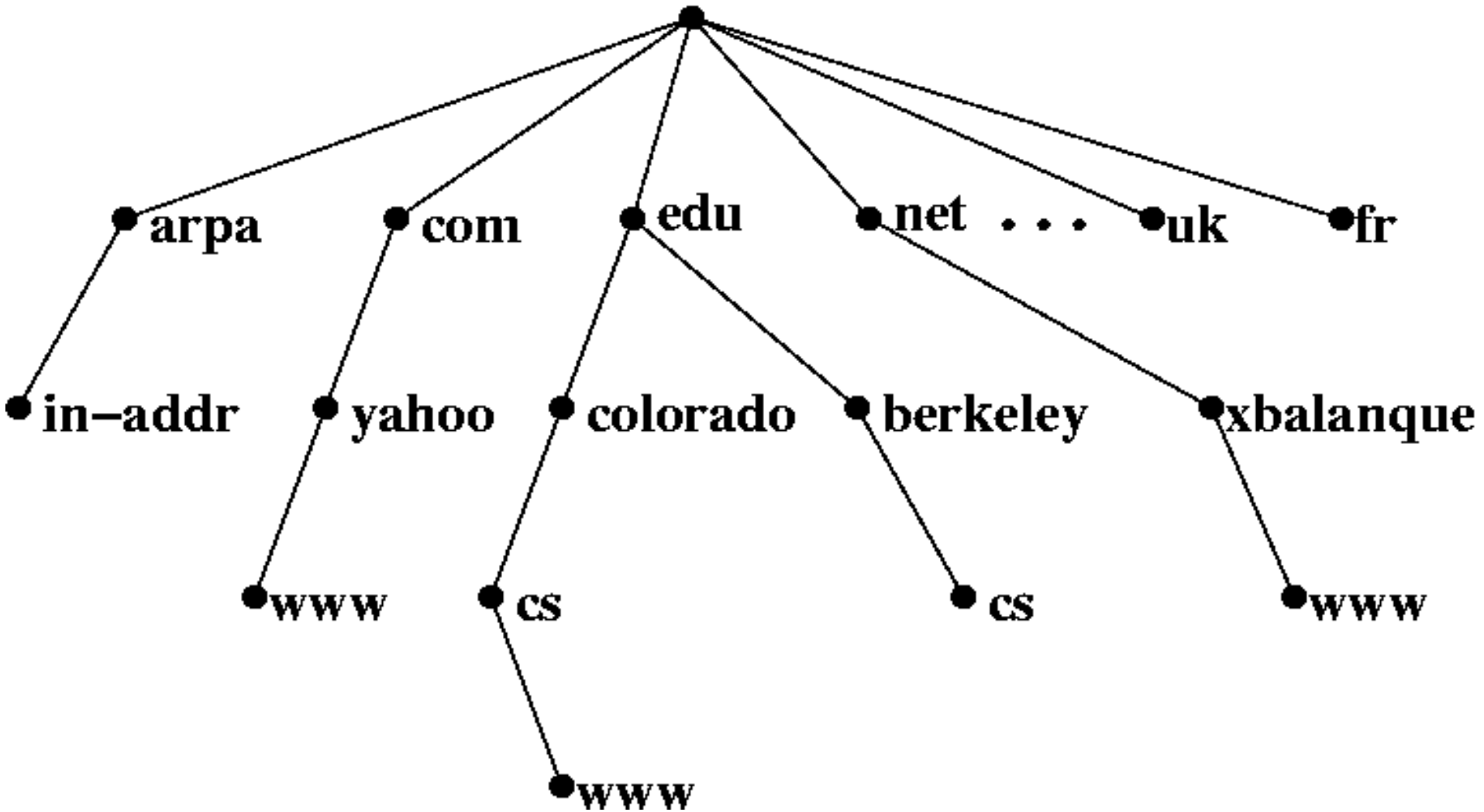
В Novell NetWare, MS Windows, IBM OS/2  
использовались **плоские имена**.

Для установления соответствия символьного  
имени и MAC-адреса использовались  
широковещательные запросы.

Широковещательный способ разрешения  
имен реализован в NetBIOS.

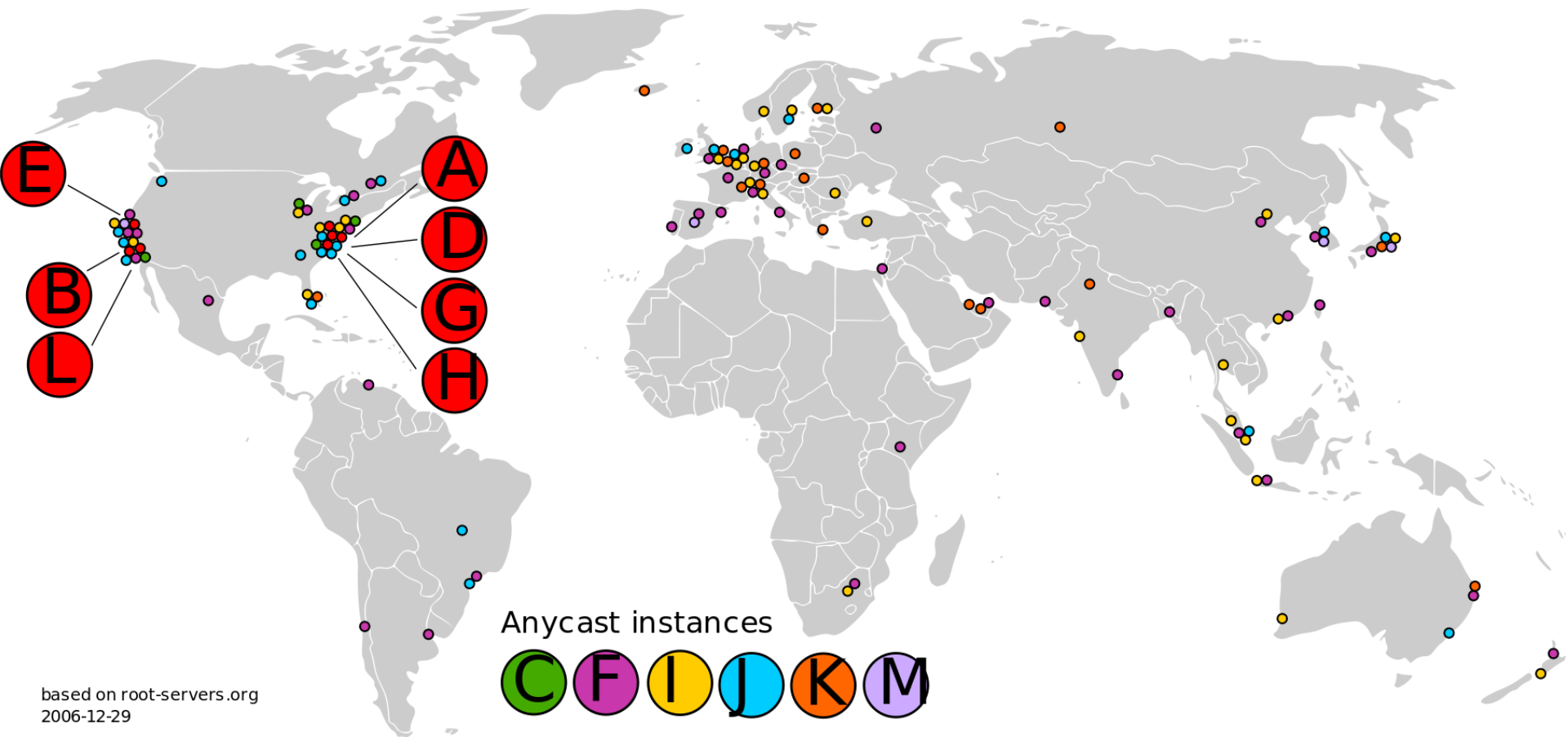
WINS — служба сопоставления NetBIOS-имён  
с IP-адресами.

# Иерархический принцип построения



Основой DNS является представление об иерархической структуре доменного имени

# Расположение корневых серверов



Список корневых серверов:  
<http://www.root-servers.org/>

# Расположение корневых серверов



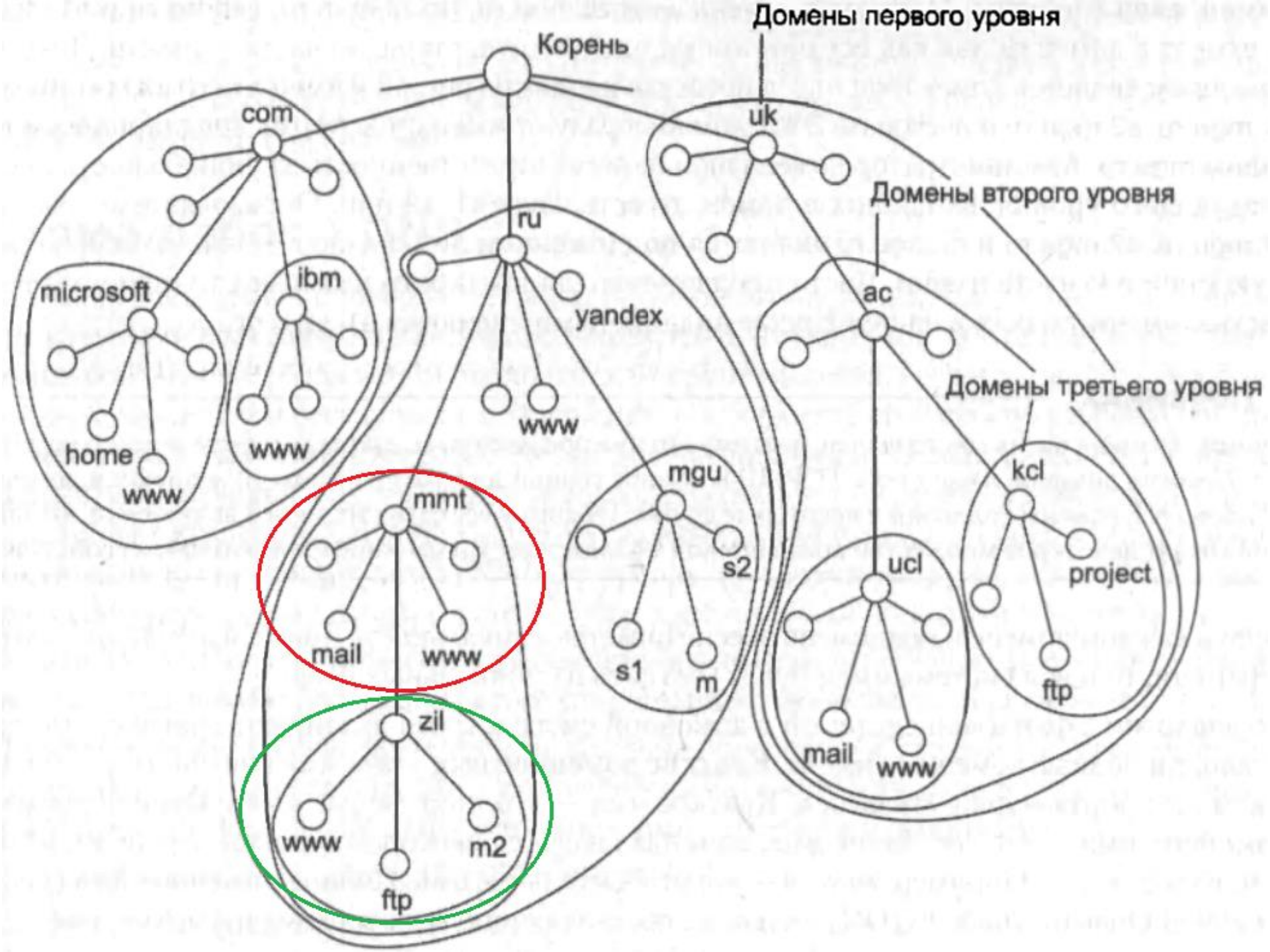


# Домен и зона

**Домен** — узел в дереве имён, вместе со всеми подчинёнными ему узлами (если таковые имеются), то есть именованное поддерево в дереве имен.

**Зона** — часть дерева доменных имен, размещаемая как единое целое на некотором сервере доменных имен.

**Делегирование** — операция передачи ответственности за часть дерева доменных имен другому лицу или организации.



# Fully Qualified Domain Name

полностью определённое имя домена

состоит из непосредственного имени домена и далее имён всех доменов, в которые он входит.

ru.wikipedia.org. Имя заканчивается точкой!

Если в конце имени точка не указана

- точка автоматически добавляется
- имя считается относительным (дополнение к имени существующего домена)

# Клиенты и серверы DNS

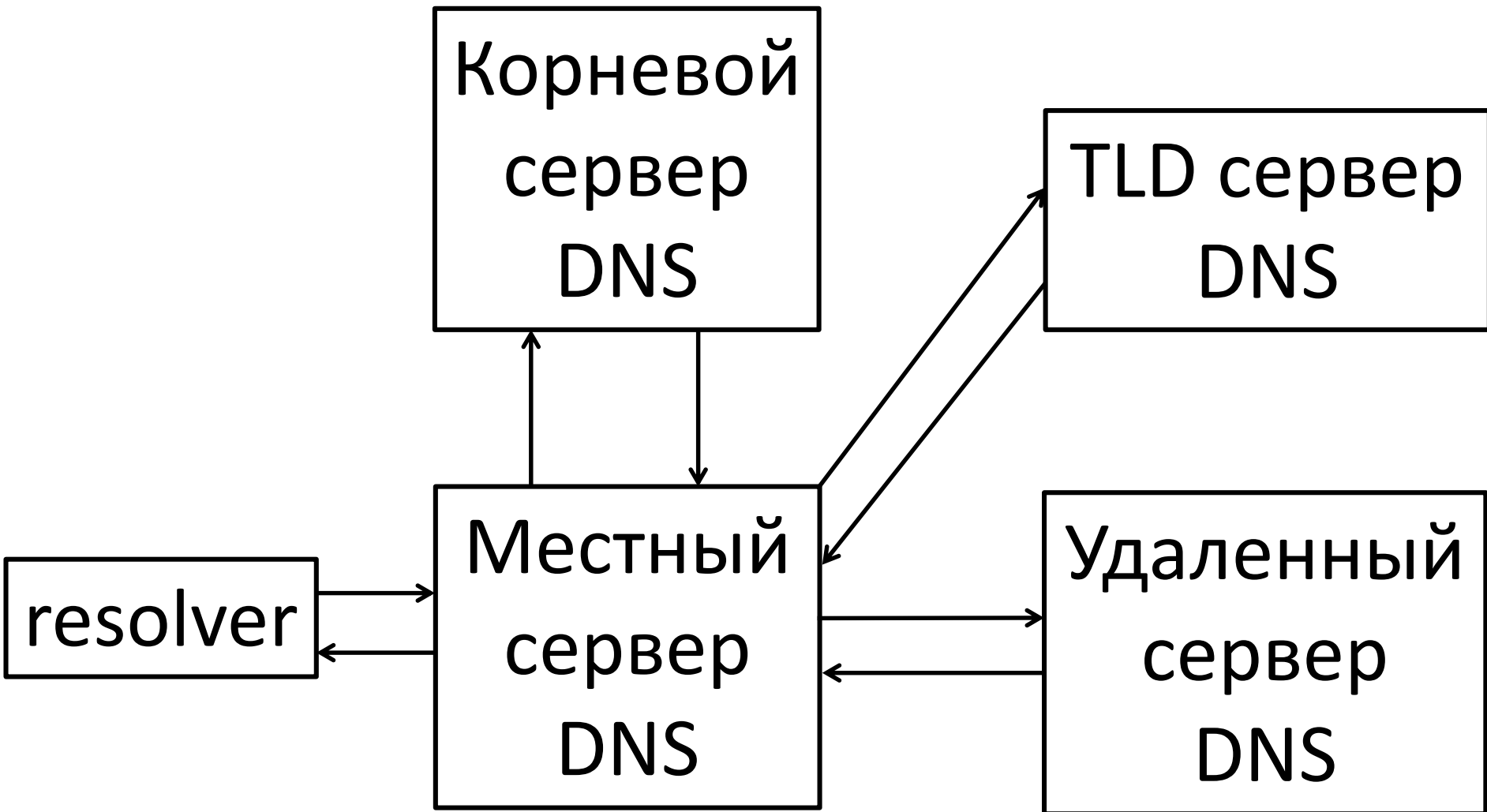
DNS состоит из трех основных частей:

Всего множества доменных имен

Серверов доменных имен

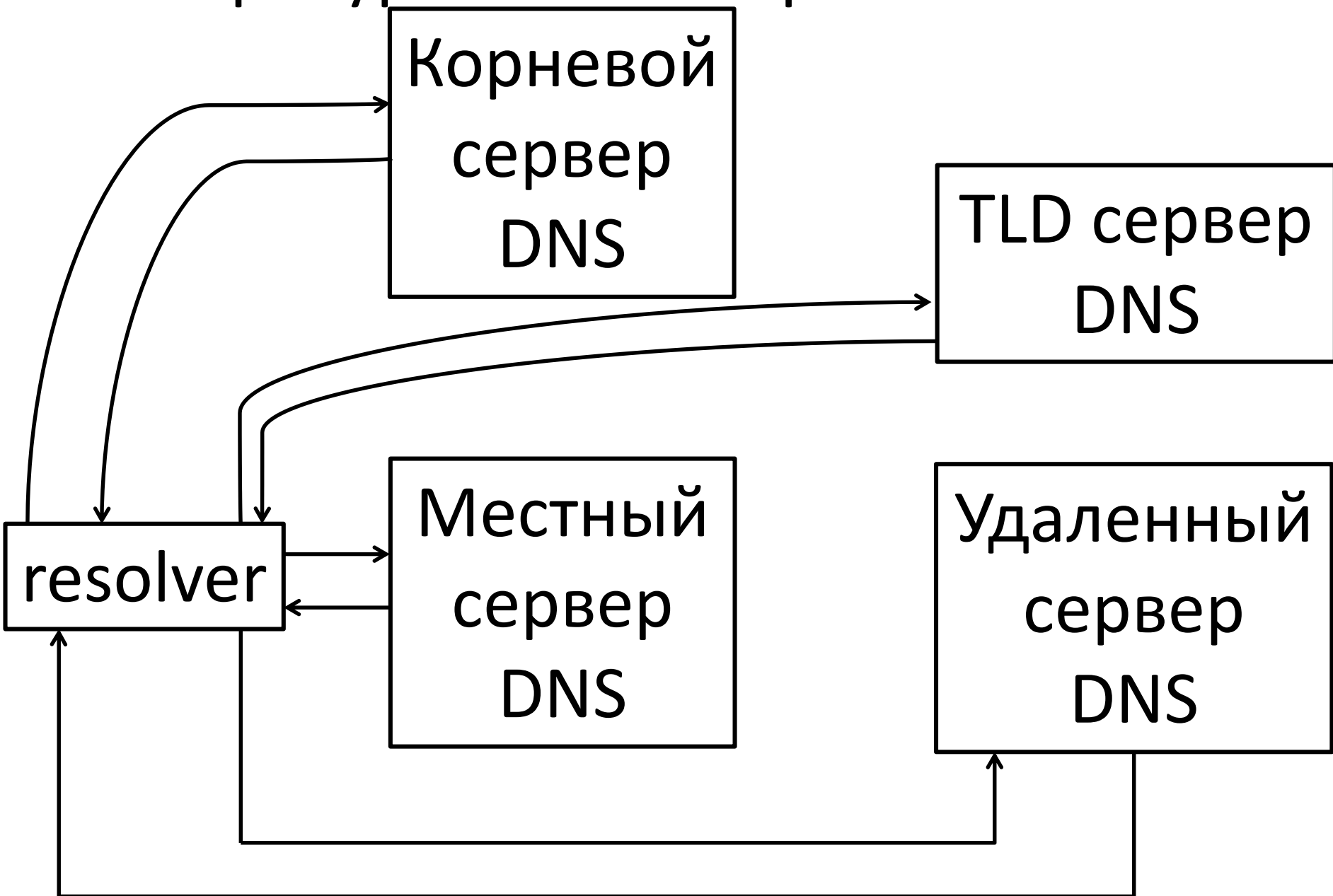
Клиентов DNS

# Рекурсивный запрос resolver'а

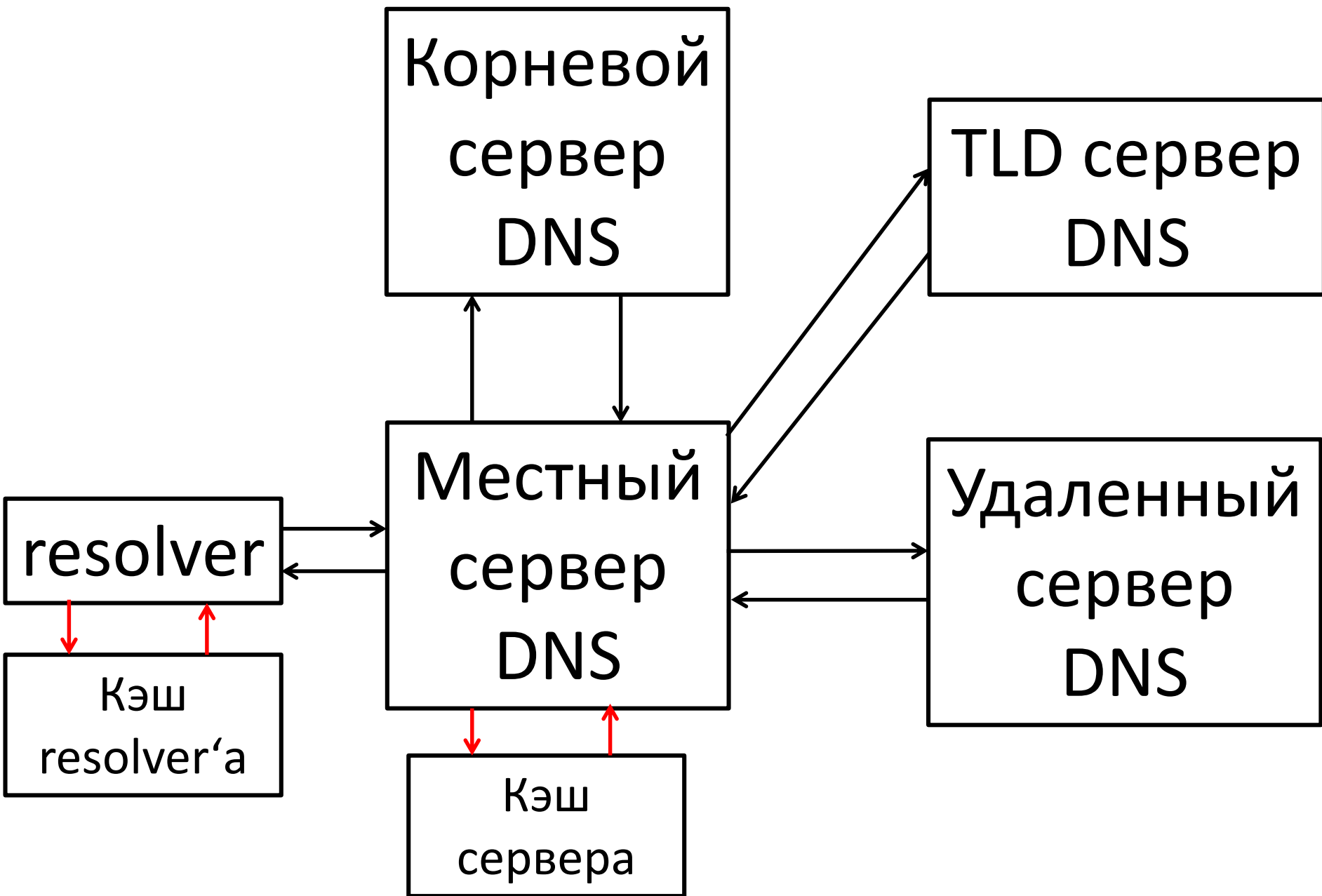


Рекурсивный запрос resolver и нерекурсивная (итеративная) процедура на разрешение доменного имени сервером доменных имен

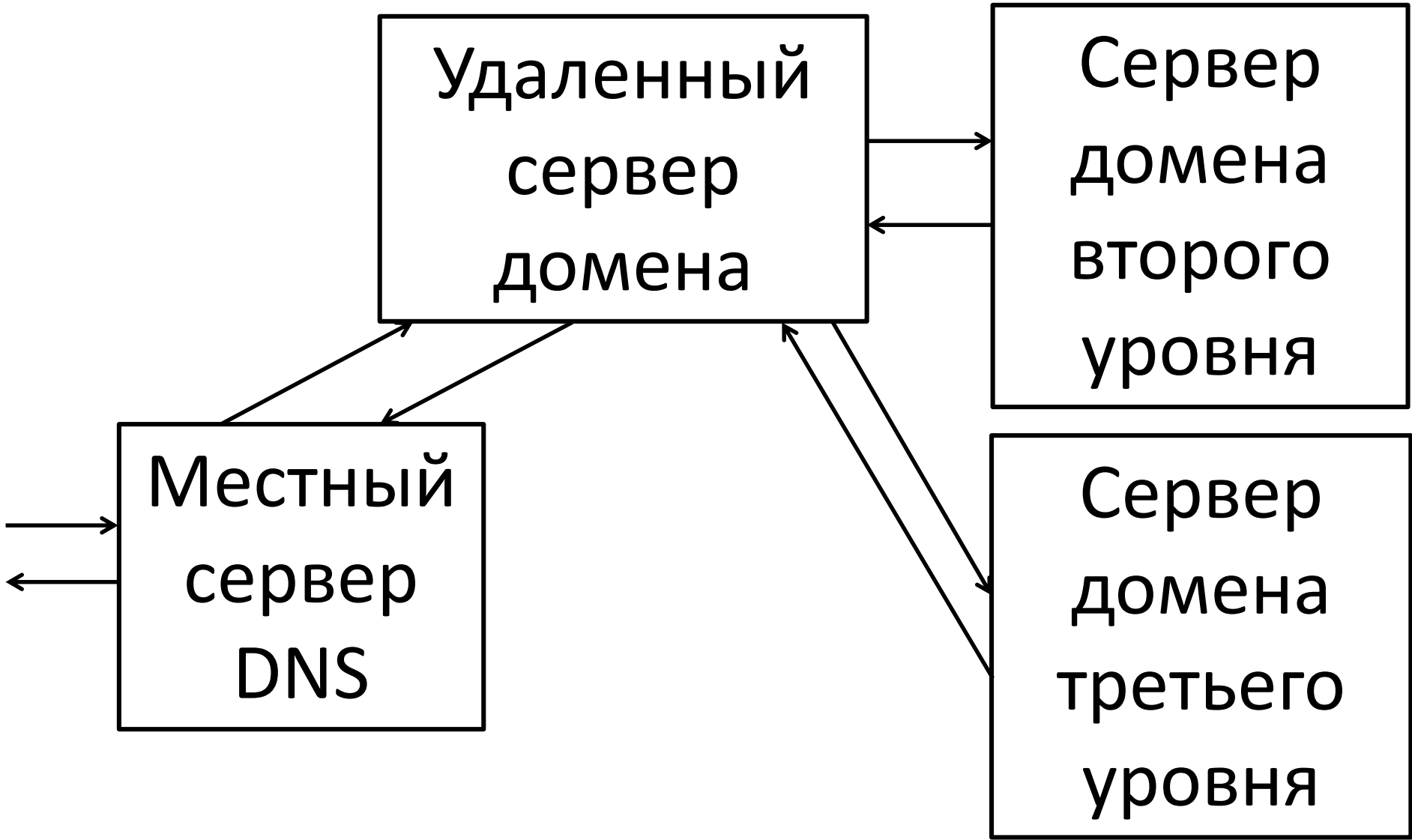
# Нерекурсивный запрос resolver'а



# Использование кэша



# Рекурсивная процедура разрешения имен



Рекурсивная (для местного сервера) и нерекурсивная (для удаленного сервера) процедуры разрешения адреса по IP-имени



Авторитетные и неавторитетные серверы

**Authoritative response** возвращают серверы, которые являются ответственными за зону, в которой описана информация, необходимая клиенту DNS.

**Non Authoritative response** возвращают серверы, которые не отвечают за зону, содержащую информацию необходимую клиенту DNS.

Авторитетный отклик могут вернуть master-сервер зоны или slave-сервер зоны

# Типы серверов: Master и Slave

**Master-сервер** является ответственным за зону; описание зоны master-сервера является первичным.

**Slave-сервер** является ответственным за зону; slave-сервер копирует описание зоны с master-сервера.

Для доменов 2го уровня обязательно иметь два DNS сервера.

# Проблема распространения изменений

> set type=soa

> rambler.ru

refresh = 10800 (3 hours)

retry = 1800 (30 mins)

expire = 864000 (10 days)

default TTL = 3600 (1 hour)

> relarn.ru

refresh = 86400 (1 day)

retry = 3600 (1 hour)

expire = 604800 (7 days)

default TTL = 86400 (1 day)

# Принцип работы DNS NOTIFY, RFC 1996

Master послал оповещение  
Slave запросил зону  
Slave получил зону

В базу данных primary  
master вносятся изменения



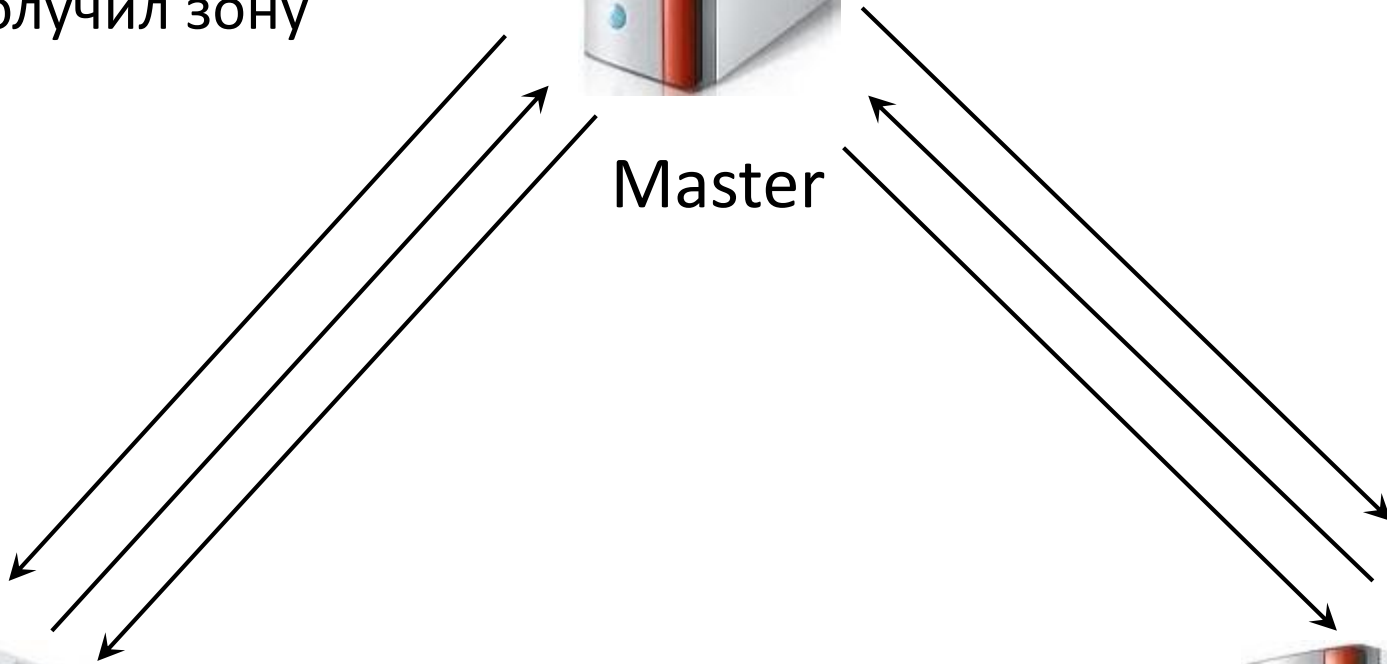
Master



Slave



Slave



# Принцип работы DNS NOTIFY

Primary  
Master



Master послал оповещение  
Slave запросил зону  
Slave получил зону  
Slave послал оповещение

Master послал оповещение  
Slave запросил зону  
Slave получил зону

Slave

Slave для Primary Master,  
Master для Slave



# DNS UPDATE

Динамический DNS (Dynamic Updates in the Domain Name System )— технология, позволяющая информации на DNS-сервере обновляться в реальном времени и в автоматическом режиме.

Stealth server не упоминается в описании зоны.

Его никто не видит, т.к. в рамках DNS-обмена данными информацию о нем получить нельзя ни путем простых запросов, ни путем копирования описания зоны.

Файлы статической настройки DNS серверов, где такой сервер может быть прописан



Slave

Slave для Primary Master,  
Master для Slave

Primary  
Master



# Передача зоны

Два механизма копирования зоны:

- полное копирование (AXFR)
- инкрементальное копирование зоны (IXFR),  
RFC 1995.

номер старой версии и список записей,  
которые нужно удалить,  
номер более свежей версии и записи,  
которые нужно добавить.