TCP/IP
Прикладные протоколы
Часть 2

DNS

- RFC 882, RFC 883, RFC 973 (1983, 1985)
- RFC 1034, RFC 1035 (1987)

1) DNS – пространство имен, т.е. совокупность наименований, которые поставлены в соответствие большинству узлов интернета;
2) DNS – распределенная база данных, в которой это пространство имен содержится;
3) DNS – это совокупность программного обеспечения, которое используется для поиска в этом пространстве имен;
4) DNS – алгоритмы, которые в этом программном обеспечении используются.

Файл «/etc/hosts»

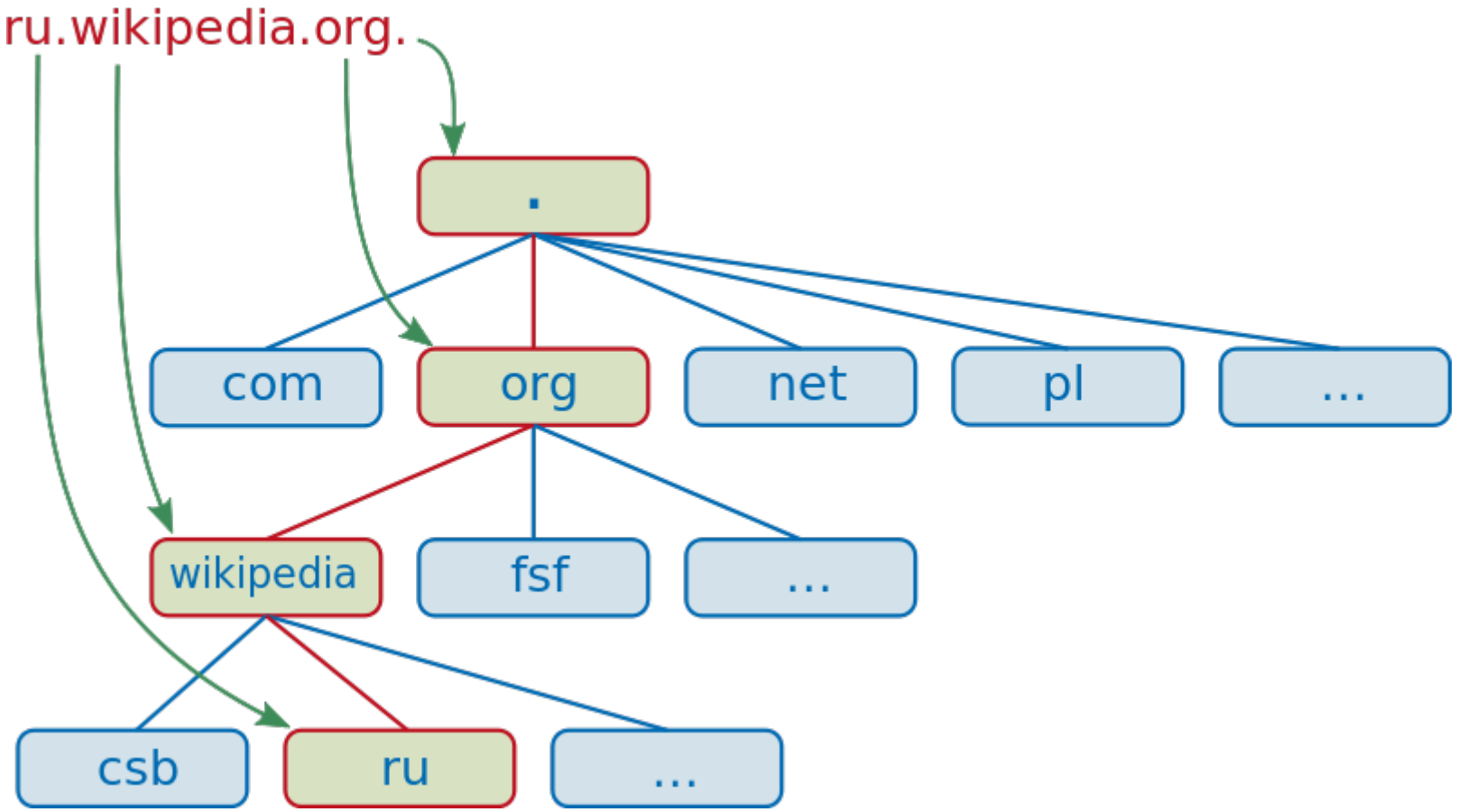
```
127.0.0.1       localhost
192.168.1.10     foo.mydomain.org foo
192.168.1.13     bar.mydomain.org bar
209.237.226.90  www.opensource.org
81.176.66.163 lib.ru
81.176.66.163 www.lib.ru
69.16.226.196 www.qsl.net
69.16.226.196 qsl.net
216.92.114.222  www.ng3.com # some comment
216.92.114.222  ng3k.com # yet annother
comment
```

Файл «/etc/nsswitch»

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service
Switch functionality.
# If you have the `glibc-doc-reference' and
`info' packages installed, try:
# `info libc "Name Service Switch"' for
information about this file.

passwd:         compat
group:          compat
shadow:         compat

hosts:          files mdns4_minimal dns mdns4
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       nis
```

Преимущества и особенности организации DNS

- *Распределённость администрирования.* Ответственность за разные части иерархической структуры несут разные люди или организации.
- *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, разделённые как физически, так и логически, что обеспечивает сохранность данных и продолжение работы даже в случае сбоя одного из узлов.



- **Домен** — узел в дереве имён, вместе со всеми подчинёнными ему узлами (если таковые имеются), т. е. именованная ветвь или поддерево в дереве имен. Структура доменного имени соответствует иерархии: доменное имя читается слева направо от младших доменов к старшим.
- **Поддомен** — подчинённый домен (например, wikipedia.org — поддомен домена org, а ru.wikipedia.org — домена wikipedia.org).

FQDN: Full Qualified Domain Name
Полностью специфицированное (квалифицированное) доменное имя
Представляет собой перечисление доменов, начиная с младших (под)доменов к старшим, включая домен нулевого уровня («пустой» домен):

www.spbu.ru.

Reverce FQDN (обратная) запись:

.ru.spbu.www

Relative name – часть FQDN, не могут заканчиваться точкой:

www; www.spbu

По соглашению, если в имени присутствует 3 или более точек, оно считается полным, но не является FQDN

Пример:

se.math.spbu.ru

Если число точек меньше 2, то трактовка зависит от настроек операционной системы. В файлах настроек DNS-серверов употребляются только FQD имена.

Ограничения доменных имен (национальные и международные домены)

- Теоретическая глубина может достигать 127 уровней, а каждая метка может содержать до 63 символов, пока общая длина FQDN не достигнет 254 символов
- Алфавит A-Z0-9- (LDH), строчные и прописные буквы не различаются
- Дефис не может быть первым или последним символом метки
- Нежелательны имена из одних цифр
- Домены 1-го уровня не могут быть алфавитно-цифровыми
- Зарезервированы имена и метки: .localhost, .test, .invalid, .example
- Точка '.' может использоваться внутри метки

Интернационализованные домены (IDN)

- Используют символы национальных алфавитов, допускающих представление IDNA/Punicode (RFC 3490)
- Punicode-представление начинается с префикса 'xn--'
- Полные IDN – в национальной кодироовке представлен домен 1-го уровня (امارا. — ОАЭ, السعودية. — Саудовская Аравия, مصر. — Египет, .РФ, .РУС — Россия, .БГ – Болгария, .УКР – Украина, .ГОРОД, .ДЕТИ, .МОСКВА)
- Частичные IDN – национальные поддомены в доменах .COM, .NET, .TEL, .NAME, .ORG и др.

- **Зона** — часть дерева DNS, размещаемая как единое целое на некотором DNS-сервере (на самом деле одновременно на нескольких серверах). Целью выделения части дерева в отдельную зону является передача ответственности (делегирование) за соответствующий домен другому лицу или организации. Как связная часть дерева, зона внутри тоже представляет собой дерево. Если рассматривать пространство имен DNS как структуру из зон, а не отдельных узлов/имен, тоже получается дерево; оправданно говорить о родительских и дочерних зонах, о старших и подчиненных. На практике, большинство зон 0-го и 1-го уровня ('.', '.ru', '.com', и т.д.) состоят из единственного узла, которому непосредственно подчиняются дочерние зоны.

- **Делегирование** — операция передачи ответственности за часть дерева доменных имен другому юридическому или физическому лицу. За счет делегирования в DNS обеспечивается распределенность администрирования и хранения. Технически делегирование выражается в выделении этой части дерева в отдельную зону, и размещении этой зоны на DNS-сервере, управляемом юридическим или физическим лицом. При этом в родительскую зону включаются «склеивающие» ресурсные записи (NS и A), содержащие указатели на DNS-сервера дочерней зоны, а вся остальная информация, относящаяся к дочерней зоне, хранится уже на DNS-серверах дочерней зоны.

whois – утилита для получения информации о делегировании зоны

- Creation Date
- Updated Date
- Registry Expiry Date
- Registrant Contact
- Admin Contact
- Billing Contact
- Tech Contact
- Name Server

По отношению к определённой зоне DNS-сервер может выступать как

- *ведущий (primary, master)* – файл зоны содержится в файле настроек
- *ведомый (secondary, slave)* – файл зоны загружается с ведущего сервера
- *кеширующий* (информация о зоне содержится в кеше)

Ведущий и ведомые сервера (совместно) называются *авторитетными*, их ответ о запросе записи из файла зоны – *авотритетным*.
Ответ других серверов называется *неавторитетным*.

Записи DNS

Спецсимволы

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

Формат записи

```
[name]  [ttl]  [class]  type  data
```

```
name:={name|@_-if equal name in
previous string}
class:={class|_-if equal class in
previous string} ({IN, CH, HS, XNS,
YP,...})
type:={SOA,NS,A,CNAME,MX,PTR,...}
```

A

```
k-max.name.   86400  IN A   81.177.139.65
www           86400  IN A   81.177.139.65
mx            86400  IN A   196.11.51.144
```

CNAME

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

SOA

```
k-max.name.   86400  IN SOA   ns1.jino.ru. hostmaster.jino.ru (
               2011032003 ; serial (серийный номер)
                    28800 ; refresh (обновление=8h)
                     7200 ; retry (повторная попытка=2h)
                   604800 ; expire (срок годности=7d)
                   86400) ; minimum TTL (минимум=24h)
```

NS

```
name.                   5772    IN      NS      l6.nstld.com.
name.                   5772    IN      NS      m6.nstld.com.
name.                   5772    IN      NS      c6.nstld.com.
name.                   5772    IN      NS      j6.nstld.com.
k-max.name.             1577    IN      NS      ns2.jino.ru.
k-max.name.             1577    IN      NS      ns1.jino.ru.
```

A

```
k-max.name.   86400  IN A   81.177.139.65
www           86400  IN A   81.177.139.65
mail          86400  IN A   196.11.51.144
```

CNAME

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

MX

```
@   86400  IN MX 10 mx
    86400  IN MX 20 mx1.hosting.net
    86400  IN MX 50 mx2.hosting.net
```

PTR

```
65.139.177.81.in-addr.arpa.   86400  IN PTR    k-max.name.
```

Настройка определителя

nameserver: Name server IP address

domain: Local domain name.

search: Search list for host-name lookup. The search list is currently limited to six domains with a total of 256 characters.

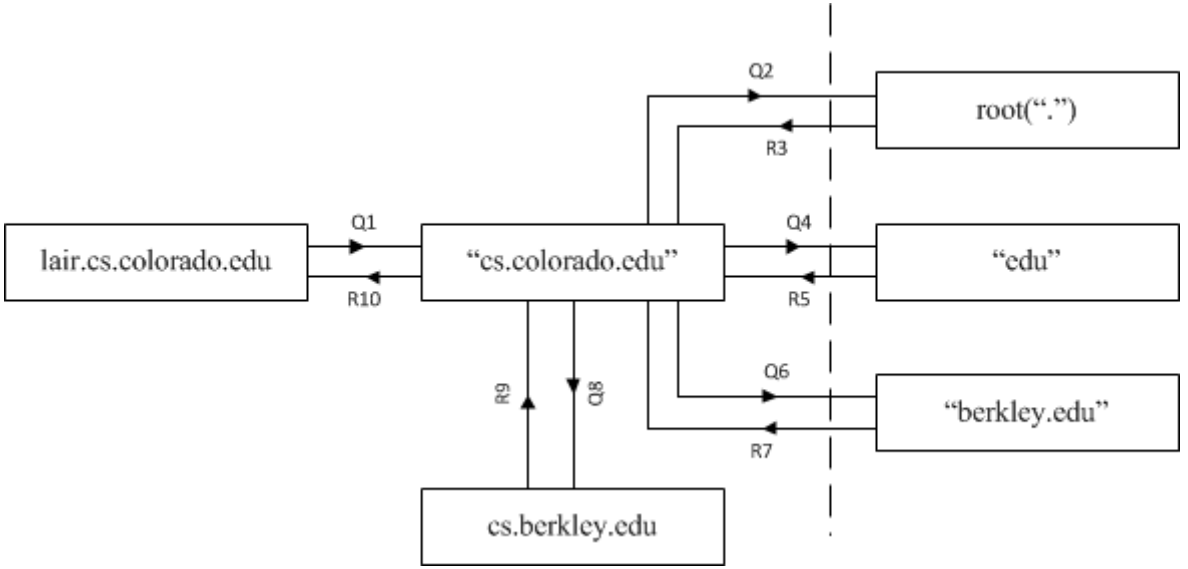
sortlist: This option allows addresses returned by gethostbyname(3) to be sorted. A sortlist is specified by IP-address-netmask pairs. The IP address and optional network pairs are separated by slashes. Up to 10 pairs may be specified. Here is an example:

```
        sortlist 130.155.160.0/255.255.240.0 130.155.0.0
```

Options:

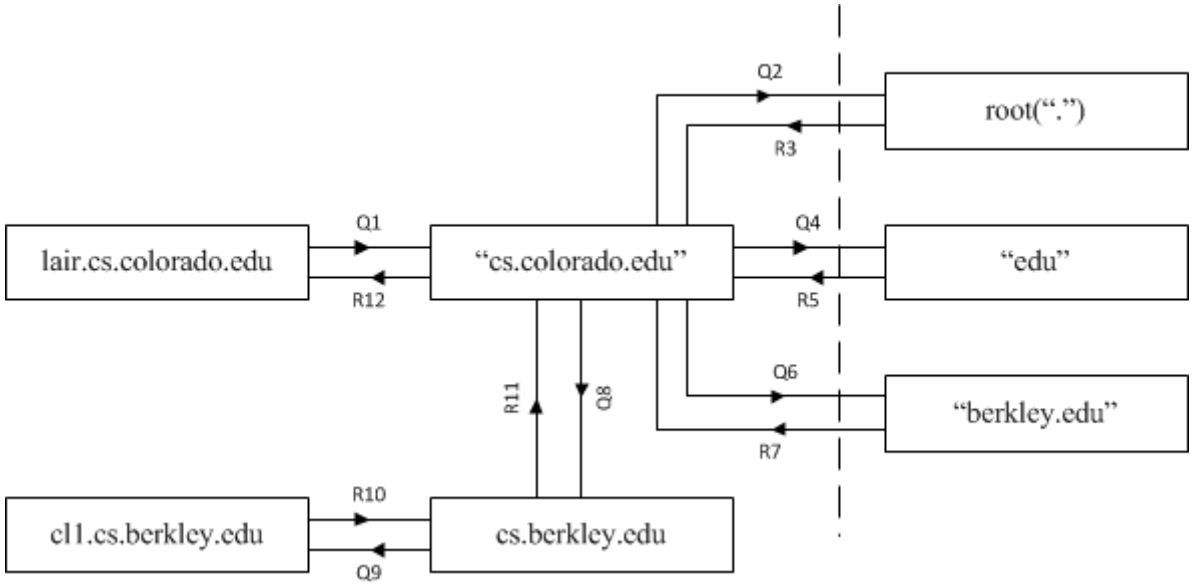
- **ndots:n**
- **timeout:n**
- **attempts:n**
- **rotate**
- **no-check-names**

Схема работы определителя
`gethostbyname('vangogh.cs.berkley.edu.',...)`



- Q - запрос, т.е. getHostByName();
- A - ответ, т.е. соответствующий IP адрес;
- R - ответ-ссылка (reference), т.е. вместо прямого ответа сервер говорит «я данного ответа не знаю, но попробуй спросить у такого сервера».

gethostbyname('*john.cl1.cs.berkley.edu.*',...)



SMTP (RFC 821), ESMTP (RFC 1123, 2821, 5321)

История

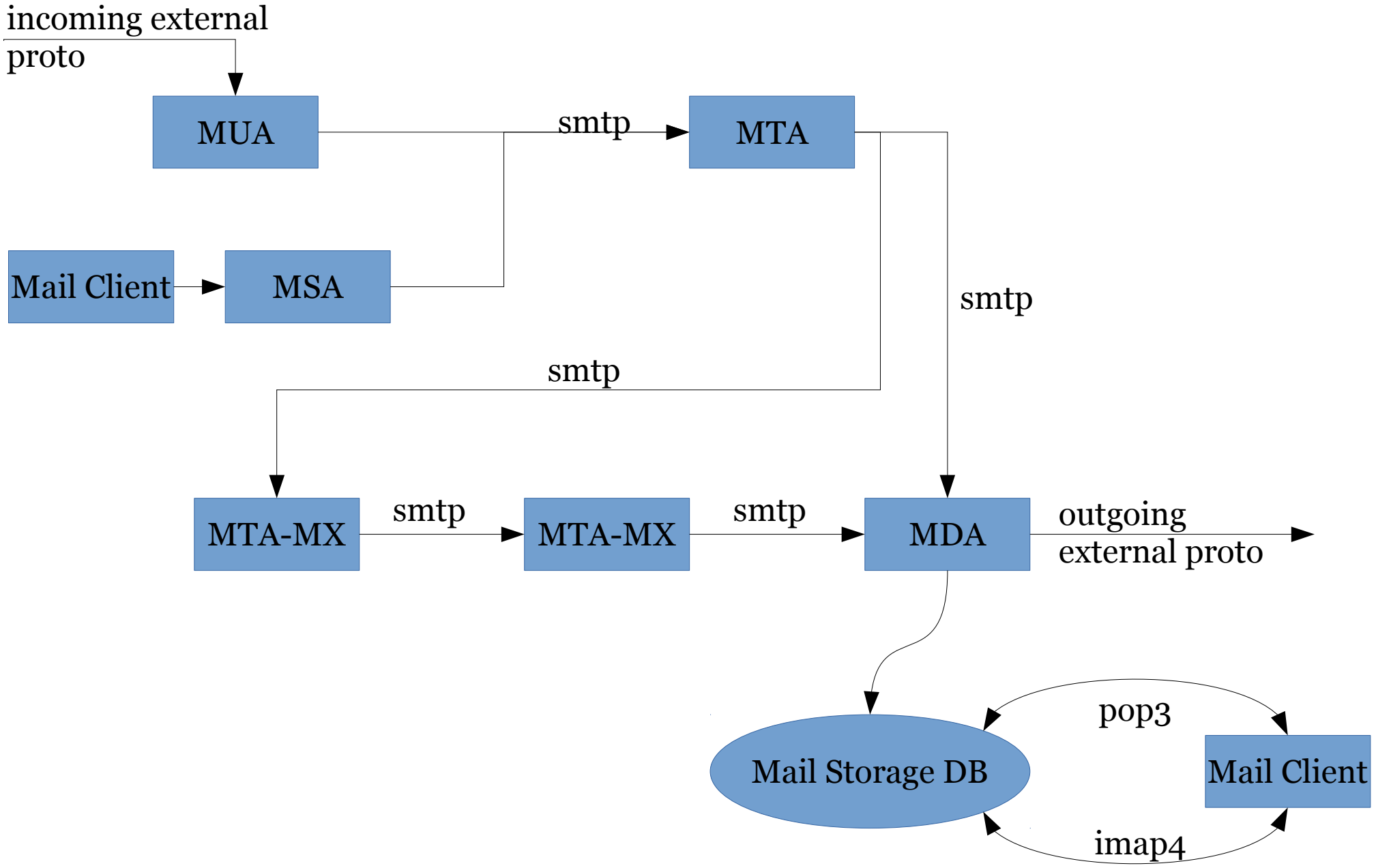
- MailBox, SNDMSG (1971)
- FTPMail, Mail Protocol (1973)
- SMTP, RFC 821 (1980)
- MX-routing, RFC 1123 (1982)

- Sendmail, Postfix, qmail, Novell GroupWise, Exim, Novell NetMail, Microsoft Exchange Server, Sun Java System Messaging Server

user@example.com – FQMN

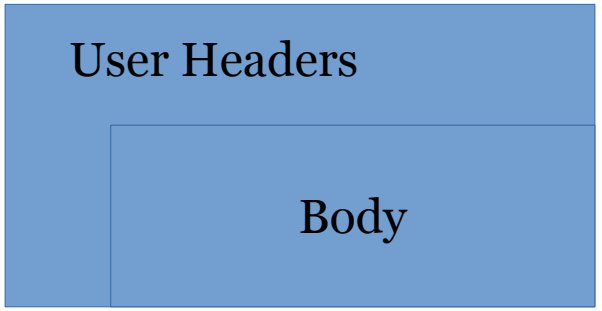
user@ – пользовательская часть почтового адреса
example.com – доменная часть почтового адреса

Mail Routing (RFC 1123)



Mails and Envelops

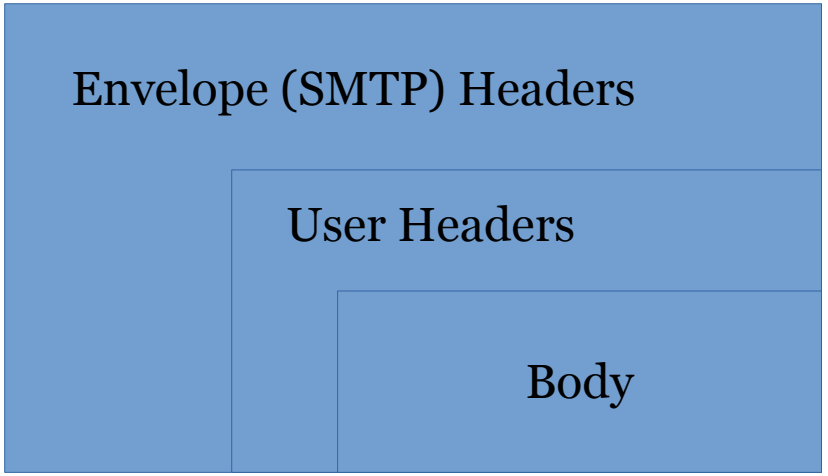
Mail Message



Основные SMTP-команды
для передачи сообщений:

- MAIL FROM — устанавливает обратный адрес
- RCPT TO — устанавливает получателя данного сообщения
- DATA — отправка текста сообщения

Mail Message in
SMTP Envelope



MX

```
@   86400  IN MX 10 mx
    86400  IN MX 20 mx1.hosting.net
    86400  IN MX 50 mx2.hosting.net
```

Почтовые алиасы и списки рассылки

Протокол SMTP позволяет переопределять пользователей и создавать списки рассылки посредством алиасинга на MDA

Файл aliases (/etc/aliases)

```
user2          : user1
root           : user2
postmaster     : root
user3          : user@example.com
project-list: johndoe@host1.uiuc.edu,
jsmith@host2.uiuc.edu, someone@host.purdue.edu
nobody         : /dev/null
program-bugs: |/usr/local/bin/program-bug-tracker
```

Mail Relay

Для любого домена почтовый сервер устанавливает свою политику почтового релеинга. Также устанавливается политика по умолчанию. В настоящее время открытые релеи считаются изначально скомпрометированными.

- ok
- reject
- discard
- relay

Сервера, указанные как MX для текущего домена, должны иметь в настройках релеинга ok (для основнгого сервера) или relay (для остальных)

```
spammer@aol.com              REJECT
cyberspammer.com             REJECT
192.168.212                  REJECT
spammer@aol.com              REJECT
cyberspammer2.com            550 We don't accept mail
from spammers
okay.cyberspammer.com        OK
sendmail.org                 OK
128.32                       RELAY
FREE.STEALTH.MAILER@         550 Spam not accepted
localhost.localdomain        RELAY
localhost                    RELAY
127.0.0.1                    RELAY
192.168.1                    RELAY
```

Спасибо за внимание!