СИСТЕМА ДОМЕННЫХ ИМЁН

Предыстория

NIC (Network Information Center) распространял по FTP файл HOSTS.TXT в котором хранились соответствия IP-адрес — доменнное имя (ручное обновление, немасштабируемое решение). В 1983 г. П. Мокапетрис предложил распределённую систему — DNS (Domain Name System) RFC 882/883.

Актуальные стандарты (ноябрь 1987):

RFC 1034 — Domain Names - Concepts and Facilities
RFC 1035 — Domain Names - Implementation and Specification

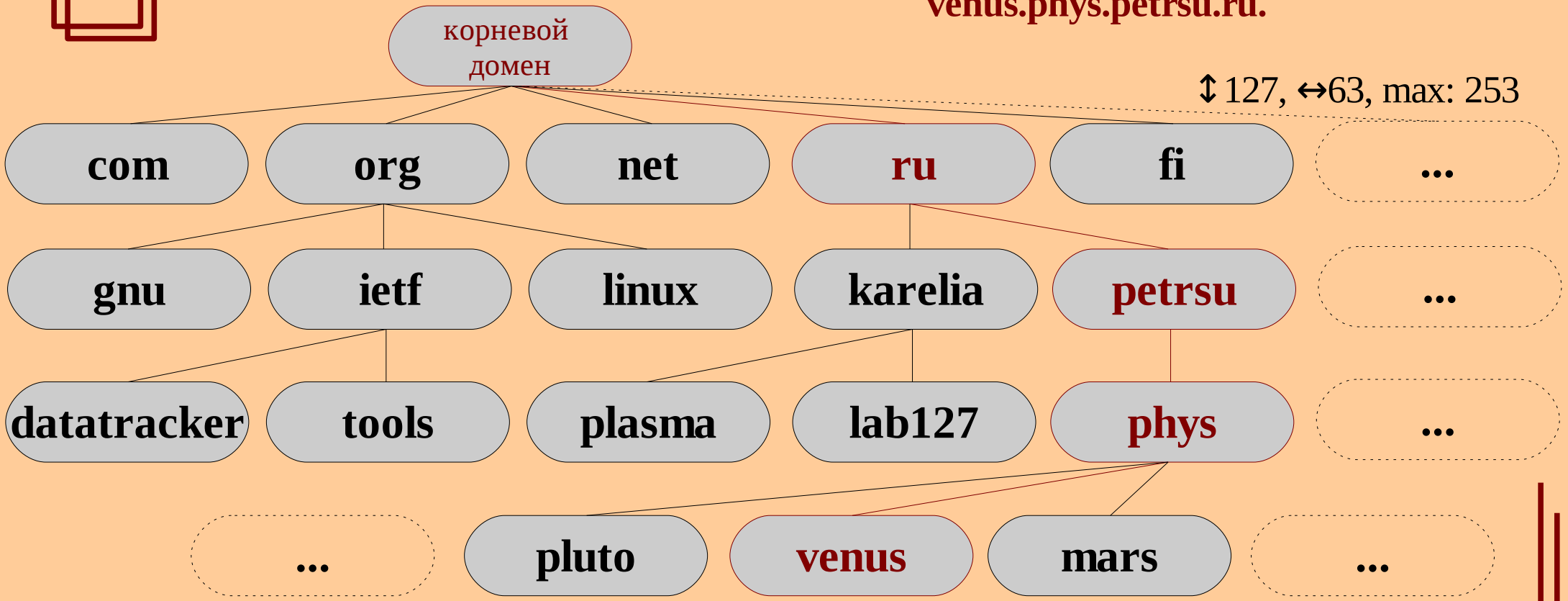
Назначение:

* получение IP-адреса по доменному имени,
* получение доменного имени по IP-адресу (обратный запрос),
* получение информации о маршрутизации почты,
* получение информации о сервисах в домене и др...

- *ресурсные записи.*

Популярная реализация DNS: BIND (Berkeley Internet Name Daemon)

ИЕРАРХИЧЕСКАЯ СТРУКТУРА DNS



FQDN (Fully Qualified Domain Name) — полностью определённое доменное имя.
Домен — узел или ветвь (поддерево) в иерархии доменных имён.
Зона — часть иерархии доменных имён, имеющая единую область ответственности (размещается как единое целое на одном DNS-сервере).
Передача ответственности — **делегирование**.
TLD (Top-Level Domain) — домен первого уровня (регулируется ICANN).

РАСПРЕДЕЛЁННОСТЬ DNS

Распределённость администрирования: ответственность за разные части иерархии доменных имён поделена на зоны (между организациями).

Распределённость хранения информации:
* DNS-сервер хранит те записи, которые входят в его зону ответственности (+ адреса корневых DNS-серверов).
* Обслуживанием одной зоны обычно занимается не один DNS-сервер (резервирование): первичный (master) и вторичные (slaves) DNS-серверы. Только первичный DNS имеет право вносить изменения в зону.
* Для уменьшения нагрузки на сеть DNS-сервер может хранить записи не из своей зоны ответственности (кэширование).

Если DNS-сервер возвращает клиенту запись, не относящуюся к его зоне ответственности, отклик называется *неавторитетным* (*non-authoritative*), в противном случае - *авторитетным*.

КОРНЕВЫЕ DNS-СЕРВЕРЫ

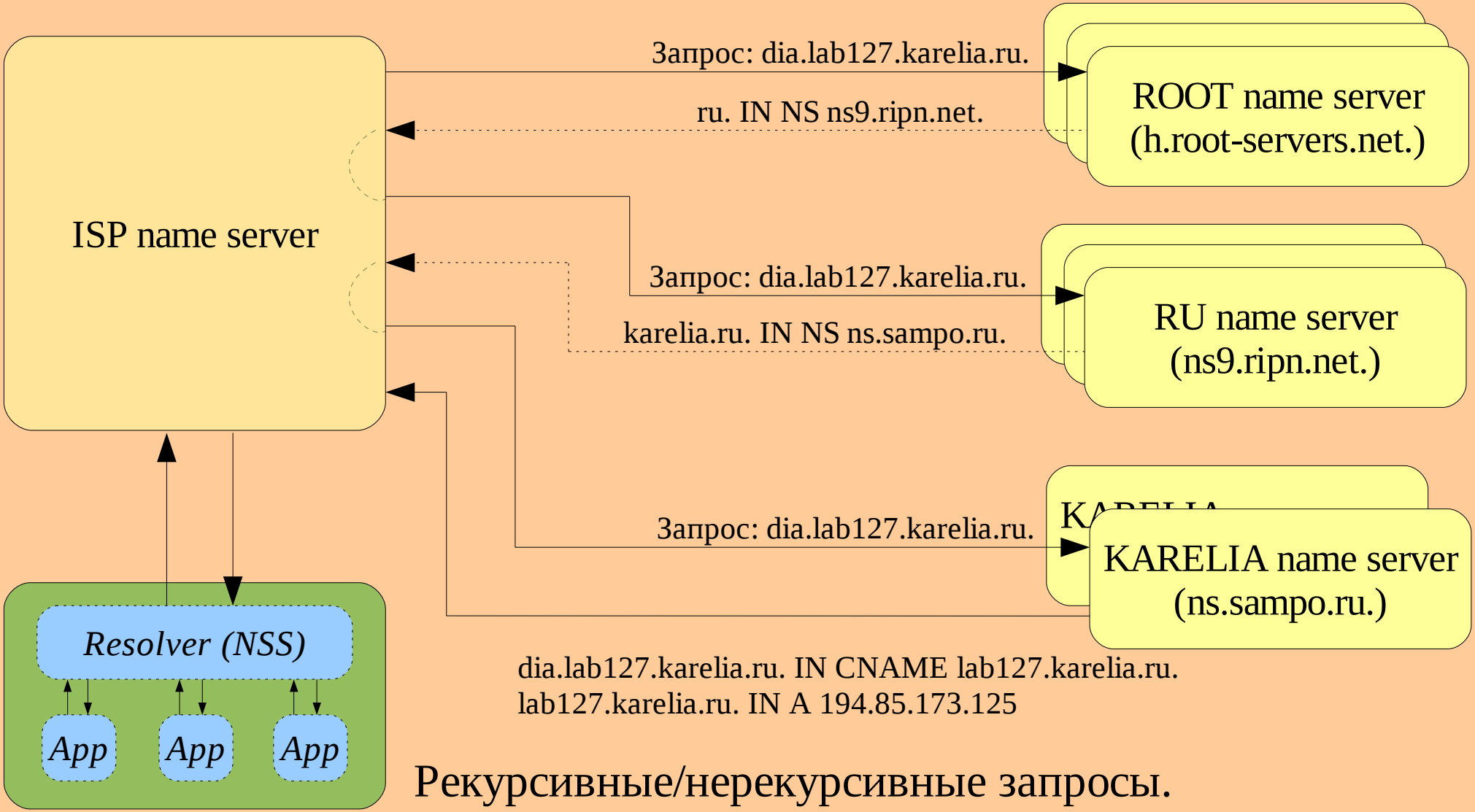
13 серверов (A.root-servers.net, ..., M.root-servers.net) хранят информацию о доменах верхнего уровня (физически — 190 из-за *anycast*)

Список корневых серверов: http://www.internic.net/zones/named.root
Список TLD: http://www.iana.org/domains/root/db/ (~300)
Операторы: VeriSign (A,J), NASA (E), ISC (F), RIPE (K) и др.

18-32 % DNS-запросов проходят через корневые сервера

МЕХАНИЗМ РЕШЕНИЯ ДОМЕННОГО ИМЕНИ

Domain Name Resolution



Рекурсивные/нерекурсивные запросы.
Кэширование записей.

ФОРМАТ DNS-СООБЩЕНИЙ

RFC 1035 (ноябрь 1987)

ID	Флаги
Q-count	A-count
NS-count	AR-count
Секция запросов	
Секция ответов	
Секция Authority	
Секция доп. записей	

NAME	
TYPE	CLASS
TTL	
RD-length	RDATA

DNS сервер принимает запросы на UDP-порт 53 (или TCP-порт 53).
Цель DNS-запроса — получить одну или несколько ресурсных записей (*resource records*).

Ресурсная запись сопоставляет доменному имени (**NAME**) служебную информацию (**RDATA**).

TYPE — тип записи:

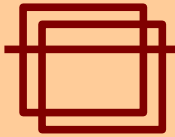
A (1) — host address, AAAA (28) — host address (ipv6),
NS (2) — name server, SOA (6) — start of authority,
CNAME (5) — canonical name,
PTR (12) — pointer, MX (15) — mail exchange,
TXT (16) — text, SRV (33) — server selection, ...

CLASS — класс записи:

IN (1) — Internet, CS (2) — CSNET,
CH (3) — CHAOS, HS (4) — Hesiod.

TTL — «время жизни» (допустимое время кэширования).

ЗАПИСЬ SOA



(SOA) Start-Of-Authority — Описание зоны ответственности

RDATA содержит:

- первичный DNS зоны,
- ответственное лицо (e-mail),
- серийный номер зоны (текущая версия),
- интервал обновления зоны (II-DNS),
- интервал повтора попытки обновления после сбоя (II-DNS),
- макс. интервал действия авторитетности без обновления (II-DNS),
- минимальное значение TTL.

Пример:

```
sampo.ru. IN SOA ns.sampo.ru. hostmaster.sampo.ru.
   2010111001
   10800
   1800
   3600000
   86400
```

ЗАПИСИ NS, A, AAAA, CNAME

(NS) Name Server — Авторитетный сервер имён

RDATA содержит имя авторитетного DNS-сервера зоны.

Пример:

```
karelia.ru. IN NS ns.sampo.ru.
karelia.ru. IN NS ns1.sampo.ru.
```

(A) Host Address — IPv4 адрес хоста

(AAAA) Host Address — IPv6 адрес хоста (RFC 3596)

RDATA содержит IP-адрес, соответствующий данному доменному имени.

Пример:

```
ns5.msk-ix.net. IN A 193.232.128.6
ns5.msk-ix.net. IN AAAA 2001:678:17:0:193:232:128:6
```

(CNAME) Canonical Name — Псевдоним

RDATA содержит реальное имя данного псевдонима.

Пример:

```
iq.karelia.ru. IN CNAME lab127.karelia.ru.
plazma.karelia.ru. IN CNAME plasma.karelia.ru.
```

ЗАПИСИ PTR. ОБРАТНЫЕ ЗАПРОСЫ

(PTR) Domain Name Pointer — Указатель на доменное имя

Определение IP-адреса по доменному имени — обратный DNS-запрос:

* трассировка сетевого пути (traceroute, в SMTP — Received), логи;
* борьба со спамом.

В обратном DNS-запросе IP-адрес, записанный в обратном порядке, преобразуется в доменное имя в зоне ARPA (Address and Routing Parameter Area):

IPv4 — in-addr.arpa.

IPv6 — ip6.arpa. (RFC 3596)

Пример:

dig -x 93.158.134.3

```
3.134.158.93.in-addr.arpa. IN PTR www.yandex.ru.
```

dig -x 2001:dc4::1

```
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.c.d.0.
1.0.0.2.ip6.arpa. IN PTR a.dns.jp.
```

Бесклассовое делегирование зон в IN-ADDR.ARPA — RFC 2317.

ЗАПИСИ MX

(MX) Mail Exchange — Почтовый сервер

Запись MX связывает доменное имя с почтовым сервером, который принимает почту для данного домена. RDATA содержит:

параметр предпочтительности (меньше — лучше);
доменное имя почтового сервера.

Пример:

```
gmail.com. IN MX 5 gmail-smtp-in.l.google.com.
gmail.com. IN MX 10 alt1.gmail-smtp-in.l.google.com.
gmail.com. IN MX 20 alt2.gmail-smtp-in.l.google.com.
```

Другие записи, используемые в почтовой системе:

(SPF) Sender Policy Framework — Политика отправителя

```
example.com. IN SPF "v=spf1 a mx -all"
_spf.yandex.ru. IN TXT "v=spf1 ip4:213.180.192.0/19 ... ~all"
```

(TXT) Text: используются для DKIM

```
s1024._domainkey.yahoo.com. IN TXT "k=rsa\; t=y\; p=...\; n=A
1024 bit key\;"
```

ПРИМЕР ФАЙЛА ЗОНЫ (BIND)

```
        $ORIGIN example.com.
@       IN SOA    ns.example.com. hostmaster.example.com. (
                                  1998102601   ; serial number
                                  43200        ; refresh – 12 час.
                                  7200         ; retry – 2 час.
                                  2592000      ; expire – 1 месяц
                                  86400        ; TTL – 24 час.
                  )
        IN  MX    10  cello.example.com.
        IN  MX    10  viola.example.com.
        IN  MX    15  tennis.example.com.
        IN  NS    ns.example.com.
        IN  NS    ns.arizona.edu.
        IN  A     192.245.12.8
        IN  A     192.245.12.7
        IN  HINFO "DEC-VAXCLUSTER" "OPENVMS"
WWW     IN  CNAME cello.example.com.
NEWS    IN  A     192.245.12.8
TENNIS  IN  TXT   "Game, set and match"
        IN  A     192.245.12.2
        IN  HINFO "MIPS-R8000" "ULTRIX"
        IN  MX    10 mail.example.com.
VIOLA   IN  A     192.245.12.9
```

ПРИМЕР ФАЙЛА ОБРАТНОЙ ЗОНЫ (BIND)

```
$ORIGIN 130.139.in-addr.arpa.

@       IN SOA      jatz.aarnet.edu.au. mit.jatz.aarnet.edu.au. (
                          1993092001          ; serial number
                          10800               ; refresh – 3 час.
                          1800                ; retry – 30 мин.
                          3600000             ; expire – 1000 час.
                          43200               ; TTL – 12 час.
                    )

        IN NS       jatz.aarnet.edu.au.
        IN NS       anu.anu.edu.au.

4.204   IN PTR      jatz.aarnet.edu.au.
8.204   IN PTR      scotch-finger.aarnet.edu.au.
16.204  IN PTR      nico.aarnet.edu.au.
```

ИНТЕРНАЦИОНАЛЬНЫЕ ДОМЕННЫЕ ИМЕНА

Punycode — RFC 3492 (март 2003)

Доменное имя может состоять только из ограниченного набора ASCII символов. ICANN утвердил основанную на Punycode систему IDNA (Internationalized Domain Names in Applications), преобразующую любую строку в кодировке Unicode в допустимый DNS набор символов.

1) ASCII-символы передаются «как есть», не-ASCII символы удаляются.

2) Ставится «-», за ним — кодированная последовательность, зависящая от номеров позиций исходных символов и их Unicode-кодов.

3) Впереди приписывается ACE-префикс «xn--»

Пример:

```
schön → xn--schn-7qa
ยจฆฟคฎข → xn--22cdfh1b8fsa
правда → xn--80aafi6cg
http://президент.рф → http://xn--d1abbgf6aiiy.xn--p1ai
http://موقع.وزارة-الاتصالات.مصر →
      http://xn--4gbrim.xn----rmckbbajlc6dj7bxne2c.xn--wgbh1c
```

БЕЗОПАСНОСТЬ DNS

Пример уязвимости DNS: DNS cache poisoning

`smart.hacker.prv. IN A ?`

```
Answer:
(no responce)

Authority:
hacker.prv. IN NS ns.google.com.

Additional:
ns.google.com. IN A 192.168.123.45
```

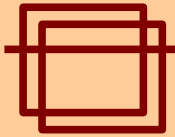
```
Answer:
(no responce)

Authority:
google.com. IN NS ns.hacker.prv.

Additional:
ns.hacker.prv. IN A 192.168.123.45
```

DNSSEC — RFC 4033, 4034, 4035, ... (март 2005)

Решение для рекурсивного сервера:
ЭЦП ресурсных записей. При использовании DNSSEC отклик DNS содержит дополнительную запись RRSIG, являющуюся ЭЦП запрошенной записи. ЭЦП проверяется открытым ключом в записи DNSKEY. NSEC или NSEC3 используются для отрицательного отклика (запись не найдена). Подлинность открытого ключа проверяется при помощи записи DS.

Решение для Stub Resolver: SIG(0), TSIG, IPSec.

ПРОБЛЕМЫ DNS



Проблемы DNSSEC:

* обеспечение обратной совместимости
* перебор имён в зоне (NSEC → NSEC3)
* кому доверить ключи от ROOT и TLD?
* трудности внедрения

Общие проблемы DNS:

* обратные запросы (согласованность с прямой зоной, безклассовые сети)
* проблемы транспорта: TCP или UDP?
* NS-записи не содержат IP-адрес
* киберсквоттинг