TCP/IP и Internet

Имена вместо адресов

Как вместо цифровых IP адресов использовать имена?

- Преобразование через локальный файл /etc/hosts (windows\system32\drivers\etc\hosts)

```
102.54.94.97    rhino
102.54.94.123   popular
102.54.94.117   localsrv
```

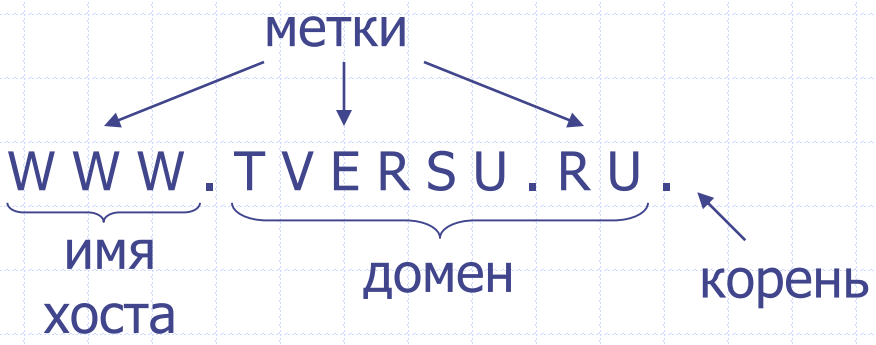
- Распространение файла с центрального сервера с помощью протокола FTP
- Распределённая база данных Domain Name System

Domain Name System / DNS RFC1034, RFC1035

- Пространство имён доменов имеет иерархическую структуру – оно организовано в виде перевёрнутого дерева с 128 уровнями, считая корень.
- Каждый элемент дерева определяется меткой, длинной не более 64 символов. Метка корневого узла – пустая строка.

Полный адрес

Fully qualified domain name



Partly qualified domain names

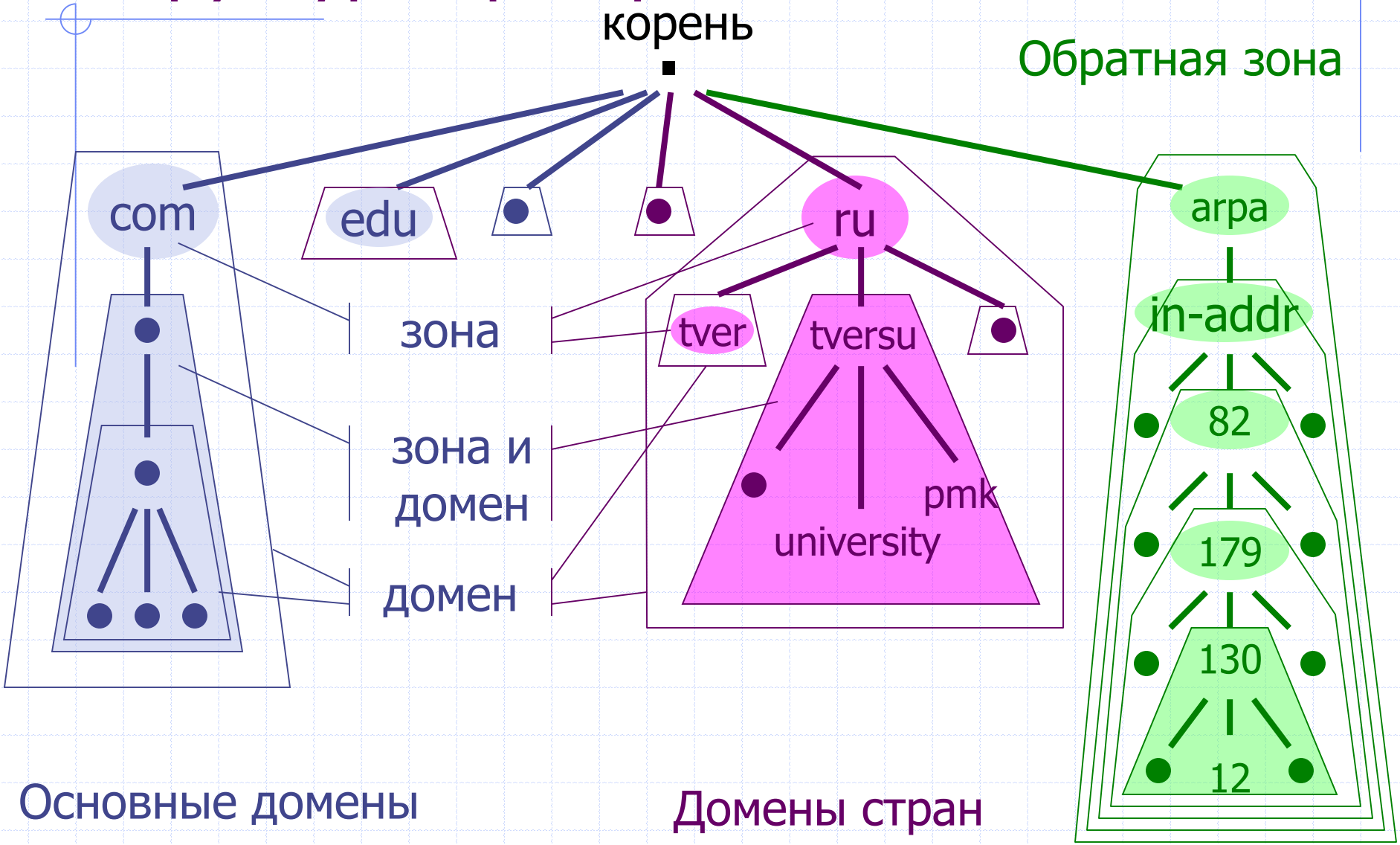
www.tversu.ru
www.tversu
www

null
ru.
tversu.ru.

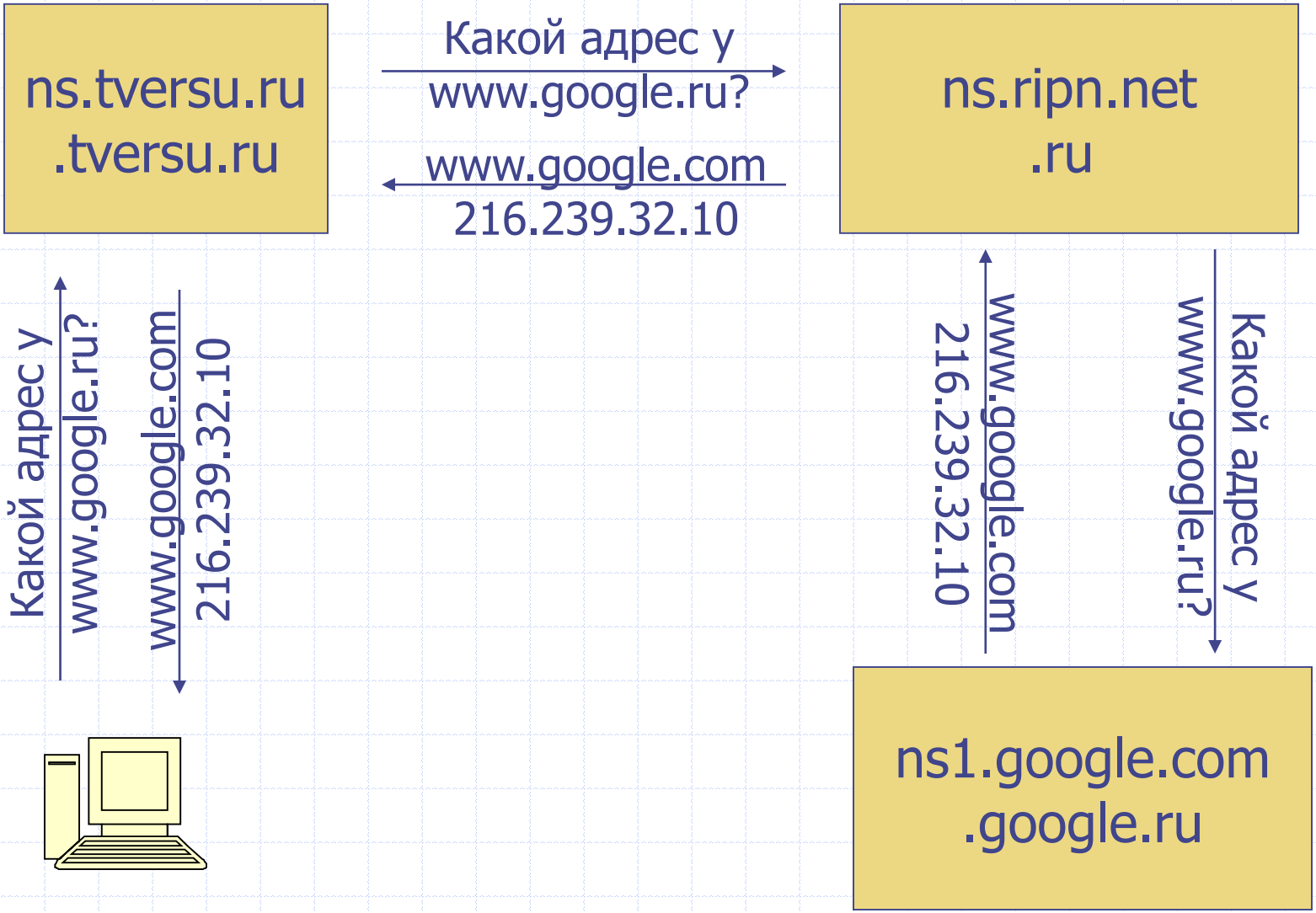
Domain Name System / DNS RFC1034, RFC1035

- **Домен** – поддерево дерева имён
- Иерархическая организация адресного пространства позволяет децентрализовать управление доменами и хранение информации
- Хранение информации и обработку запросов о доменах обеспечивают сервера домена (как правило, должны присутствовать основной и резервные сервера). Иерархия серверов отражает иерархию имён.
- **Зона** – непрерывная часть дерева имён, за которую ответственен (authoritative) один сервер.
- За хранение информации о корневом домене отвечают специальные сервера, управляемые ICANN. Их IP адреса известны каждому серверу домена.

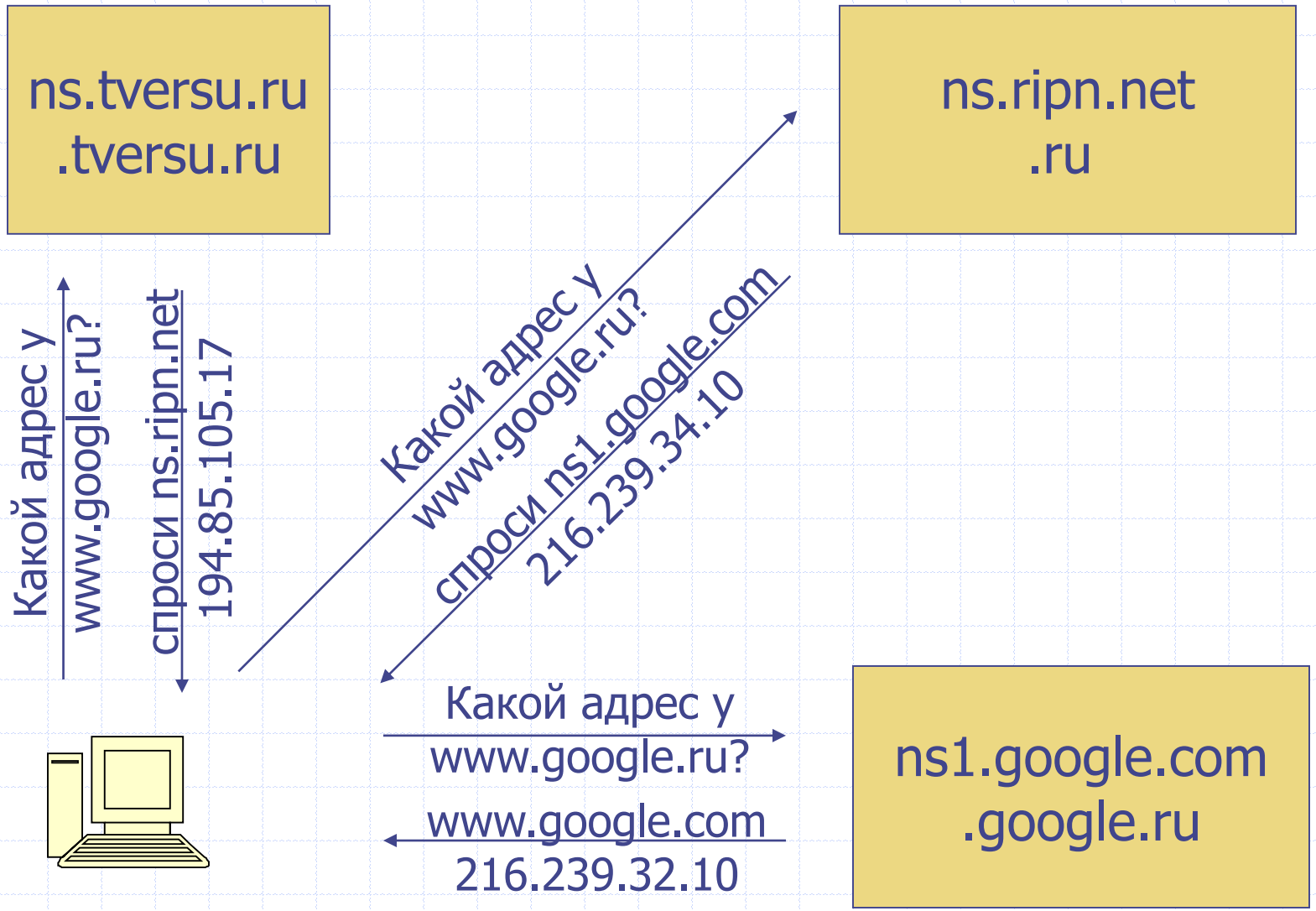
Domain Name System / DNS
Структура пространства имён



Domain Name System / DNS
Пример рекурсивного запроса



Domain Name System / DNS
Пример итеративного запроса



Domain Name System / DNS
Кэширование запросов

- Полученная сервером домена информация запоминается.
- Кэширование информации приводит к тому, что после обновления данных на первичном контроллере домена часть серверов может пользоваться устаревшей информацией.
- Допустимое время кэширования задаётся в настройках первичного контроллера домена.
- При возвращении кэшированной информации она помечается как «**non-authoritative**».

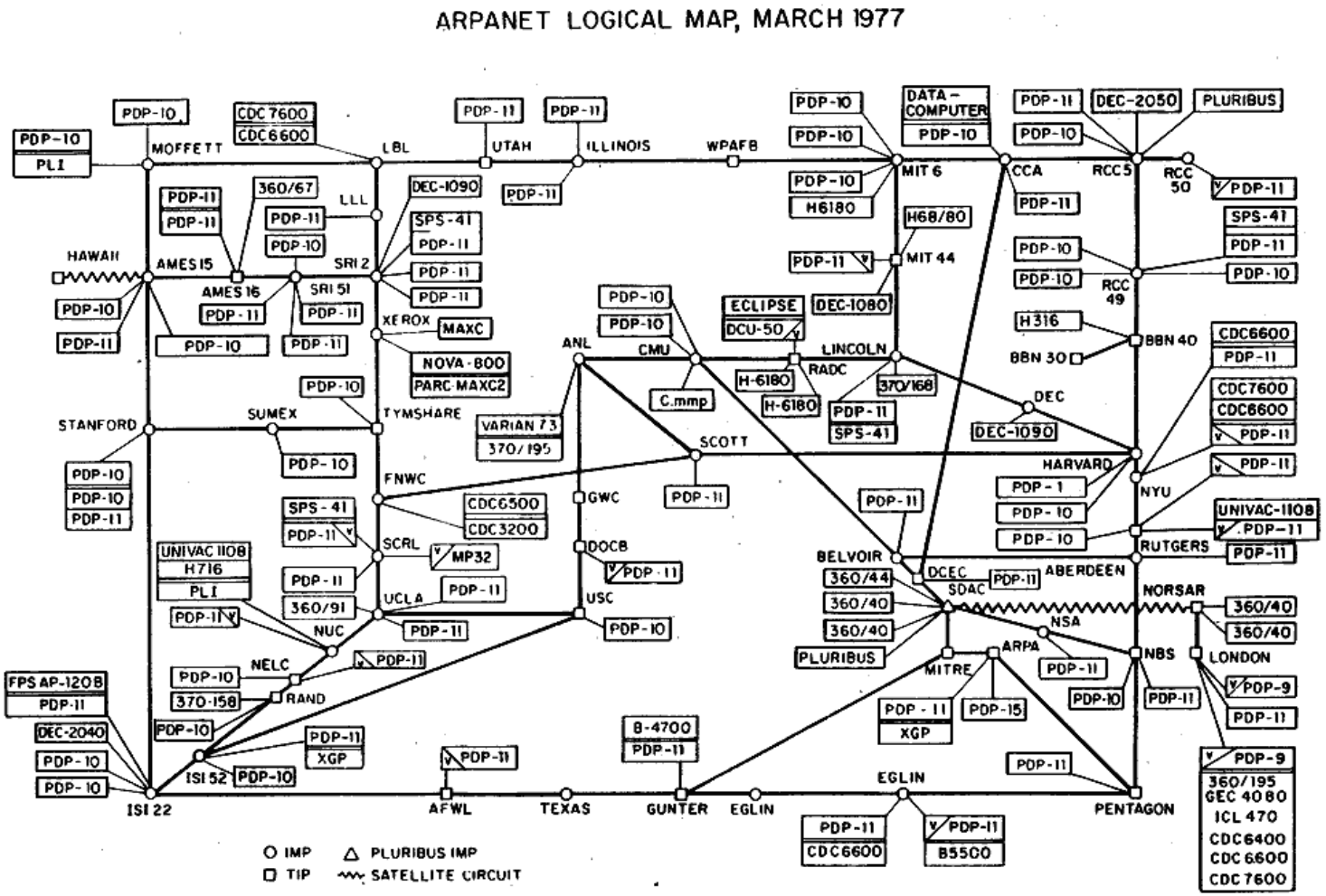
Domain Name System / DNS
Обратное преобразование

- Запрос о преобразовании адреса в имя называется запросом указателя / Pointer query (PTR)
- Для обработки запросов PTR в дерево имён введён обратный домен in-addr.arpa (in-addr = inverse address).
- Для получения информации о хосте с IP-адресом A.B.C.D следует запросить PTR запись для D.C.B.A.in-addr.arpa.
- Обратный порядок записи адреса позволяет раздавать зоны этого домена одновременно с распределением подсетей IP-адресов.

Internet
Развитие адресного пространства

- 1970: RFC33
  - 8 бит - адрес хоста
  - 24 бита – «user number»
- Конец 70-х:
  - 32 бита – адрес:
    - 8 бит – адрес сети
    - 24 бита – адрес хоста

Internet
Развитие адресного пространства



(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE HOST POPULATION OF THE NETWORK ACCORDING TO THE BEST INFORMATION OBTAINABLE, NO CLAIM CAN BE MADE FOR ITS ACCURACY)

NAMES SHOWN ARE IMP NAMES, NOT (NECESSARILY) HOST NAMES

Internet
Развитие адресного пространства

1981: RFC791

Классы сетей:

Сети класса A

Сети класса B

Сети класса C

.

Internet
Развитие адресного пространства

С 1981 по настоящее время Интернет вырос более чем в 10 миллионов раз.

Проблемы разделения на классы:

- Неэффективное использование адресного пространства:
  - 126 сетей класса A по 16777216 хостов занимают половину адресного пространства.
- Проблемы с роутингом:
  - Маршрутизаторы верхнего уровня не могут хранить в своих таблицах информацию по более чем 4 млн. сетей класса C.
- Исчерпание адресов:
  - По оценкам 1990 года к 1994 году должны были быть исчерпаны сети класса B

Internet
Развитие адресного пространства

Начало 90-х: Classless Interdomain Routing (CIDR)

- Разделение на адрес сети и хоста определяется маской.
- Вместо 3 классов стало возможно использовать 16 различных размеров сетей, от сети C до половины A.
- Стала возможна агрегация сетей, позволяющая скрыть внутреннее устройство сети от внешних маршрутизаторов.

Internet
Развитие адресного пространства

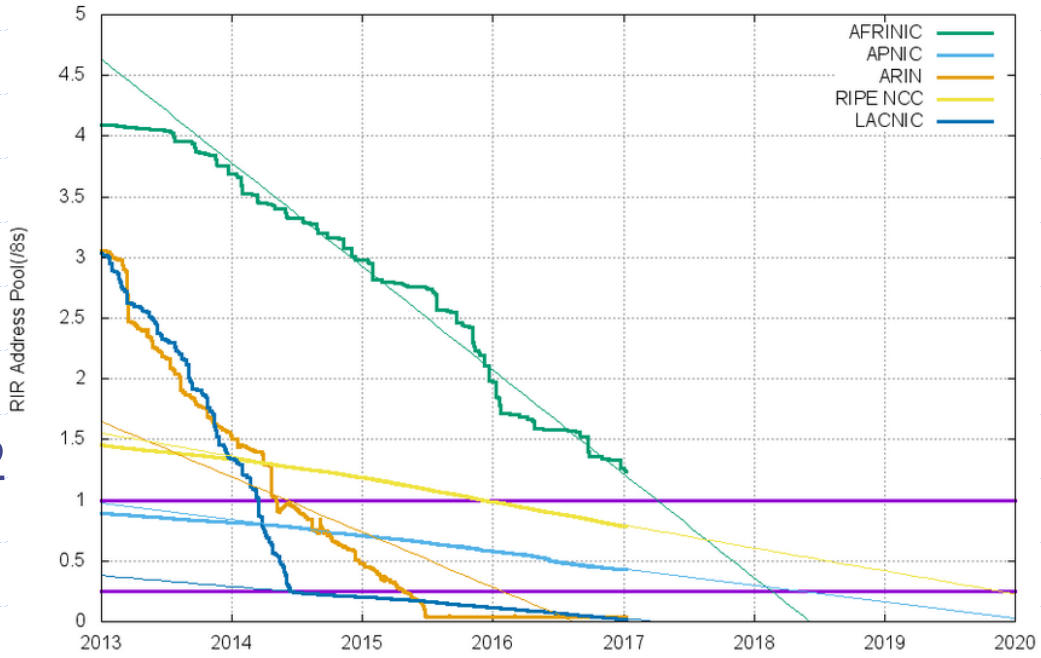
Сохранение проблем с CIDR:

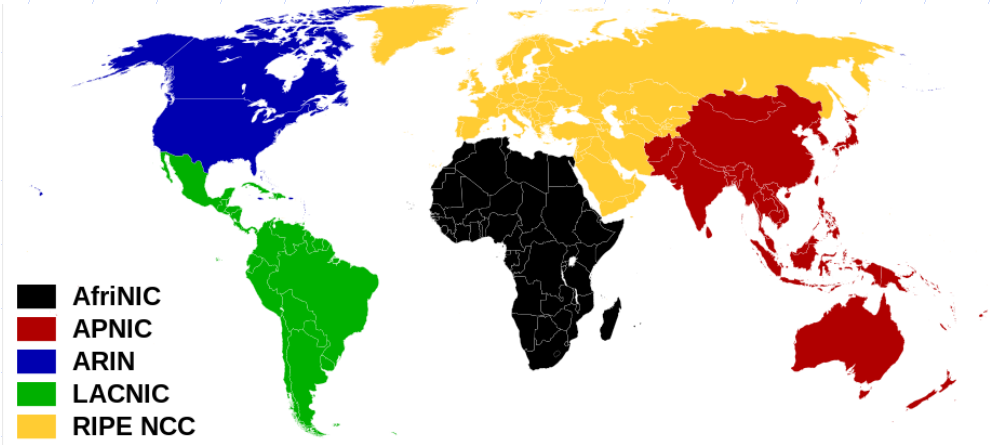
- Увеличивается число автономных систем (AS)
- Таблицы маршрутизации продолжают расти
- Уменьшается средний размер адресного пространства на одну AS
- Увеличивается число небольших сетей
- Число исключений из агрегированных сетей велико
- 3 февраля 2011 года ICANN выдала последние 5 блоков адресов IPv4.

Internet
Исчерпание адресного пространства

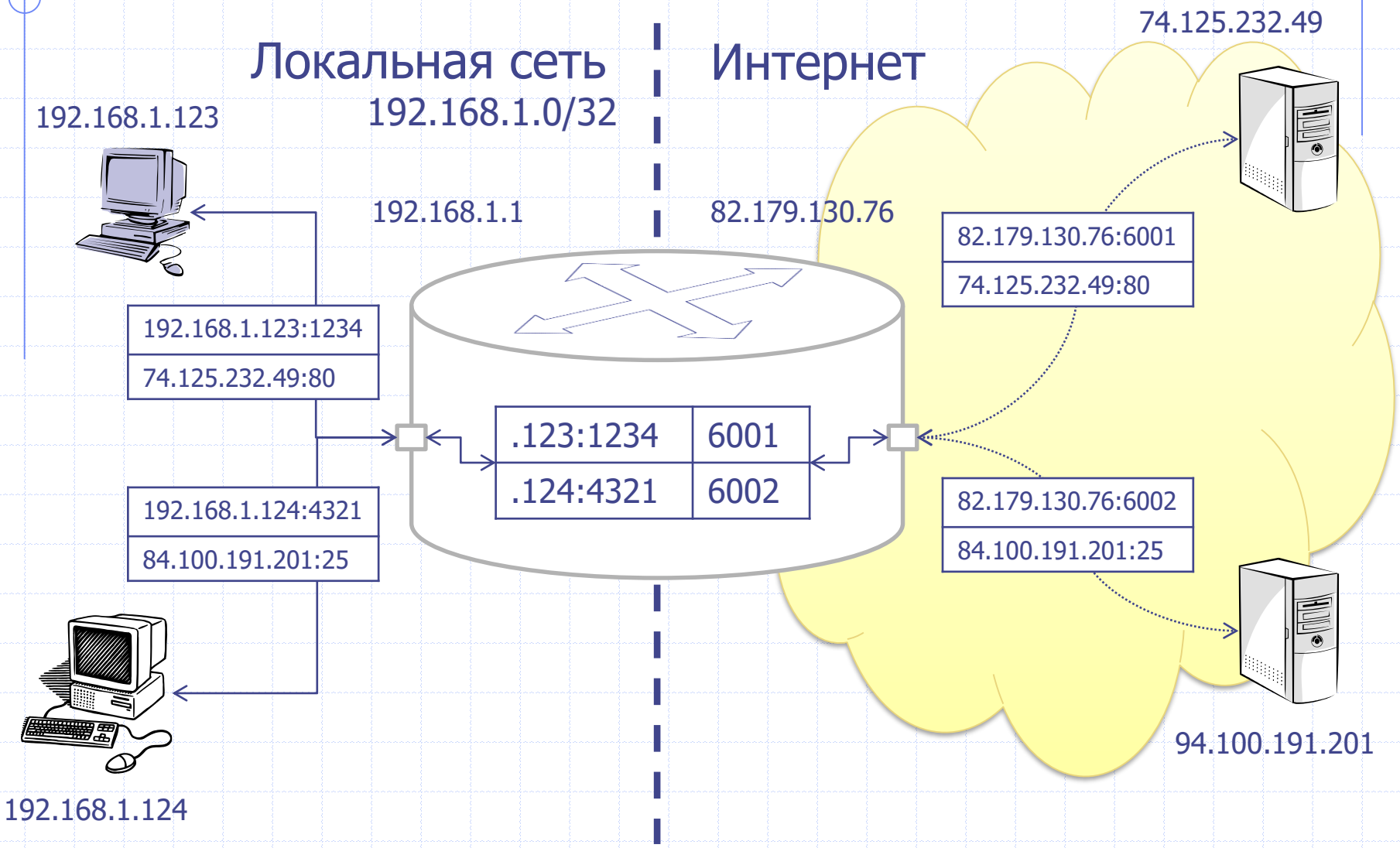
Начало использования последнего блока:

- APNIC:
  /8: 14 апреля 2011
- RIPE NCC:
  /8: 14 сентября 2012
- LACNIC:
  /10: 10 июня 2014
- ARIN:
  /10: 24 сентября 2015
- AfrNIC:
  /11: Ожидается в 2018





Internet
Network Address Translation (NAT)



Недостатки IPv4

- Недостаточный размер адресного пространства
- Переполнение памяти маршрутизаторов из-за произвольного распределения адресов
- Нарушение прозрачности взаимодействия конечных узлов при использовании NAT

Разрешимые в рамках IPv4 проблемы:

- Безопасность
- Автоконфигурация
- …

IPv6

- Расширенное адресное пространство
- Упрощенный формат заголовков IP
- Улучшенная поддержка опций
- Безопасность
- …

IPv6
Адресное пространство

- Размер адреса 128 бит
- Типы обычных (unicast) адресов
  - Global unicast
    - Адреса, распределяемые по подключению
    - Адреса, распределяемые по географическому положению
  - Link local unicast
  - Site local unicast
  - Unicast with embedded IPv4/NSAP address
- Multicast адреса
- Anycast адреса

IPv6
Изменение заголовка IP

- Заголовок IPv4: 12 полей, 20..60 байт
- Заголовок IPv6: 8 полей 40 байт
- Из заголовка убраны:
  - Поле размер заголовка
  - Контрольная сумма заголовка
  - Поля, связанные с фрагментацией
    - Фрагментация осуществляется только отправителем с помощью опций, рекомендовано использовать механизмы определения Path MTU
  - Опции перенесены в отдельные заголовки, которые могут следовать за основным.

IPv6 Безопасность

- Введена обязательная поддержка IPSec всеми узлами.
- Возможности IPSec:
  - Шифрование;
  - Аутентификация данных и отправителя;
  - Контроль доступа к данным и сетям;
  - Проверка целостности данных, передаваемых протоколами без установки соединения;
  - Защита от вмешательства в передачу данных на транзитных узлах;
  - Ограничение возможностей взломщиков, анализирующих открытые части пакетов на транзитных узлах;
  - Безопасное туннелирование через небезопасные сети;
  - Интеграция алгоритмов, протоколов и инфраструктуры безопасности.

IPv6
Другие нововведения

- Разработаны протоколы stateless автоконфигурации с использованием link local адресов.
- Добавлена поддержка мобильных клиентов, которые могут работать, переместившись в другую сеть.
- Существенно доработан протокол ICMP, который взял на себя функции ARP/RARP, управление мультикастовой передачей, поддержку мобильных клиентов.