

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

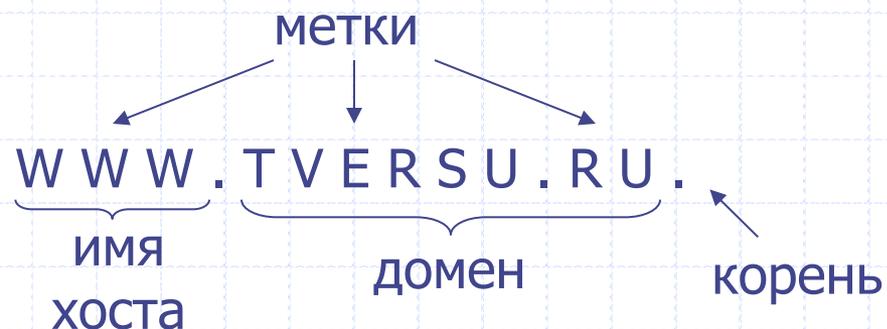
Domain Name System / DNS

RFC1034, RFC1035

- ◆ Пространство имён доменов имеет иерархическую структуру – оно организовано в виде перевёрнутого дерева с 128 уровнями, считая корень.
- ◆ Каждый элемент дерева определяется меткой, длиной 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.

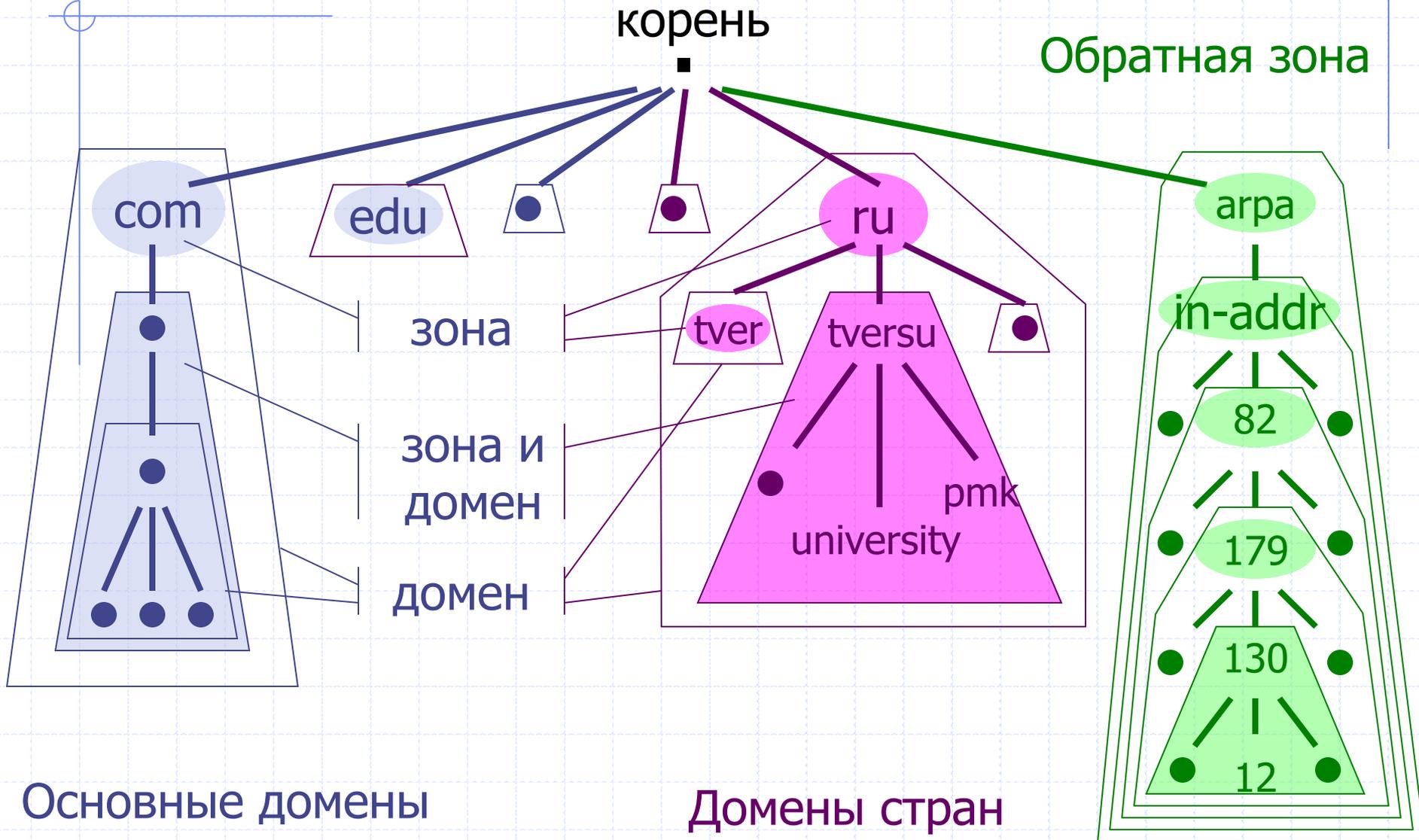
Domain Name System / DNS

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

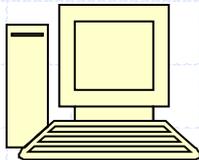
Пример рекурсивного запроса

ns.tversu.ru
.tversu.ru

Какой адрес у
www.google.ru?
www.google.com
216.239.32.10

ns.ripn.net
.ru

Какой адрес у
www.google.ru?
www.google.com
216.239.32.10



Какой адрес у
www.google.ru?
www.google.com
216.239.32.10

ns1.google.com
.google.ru

Domain Name System / DNS

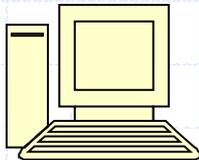
Пример итеративного запроса

ns.tversu.ru
.tversu.ru

ns.ripn.net
.ru

Какой адрес у
www.google.ru?
спроси ns.ripn.net
194.85.105.17

Какой адрес у
www.google.ru?
спроси ns1.google.com
216.239.34.10



Какой адрес у
www.google.ru?
www.google.com
216.239.32.10

ns1.google.com
.google.ru

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:

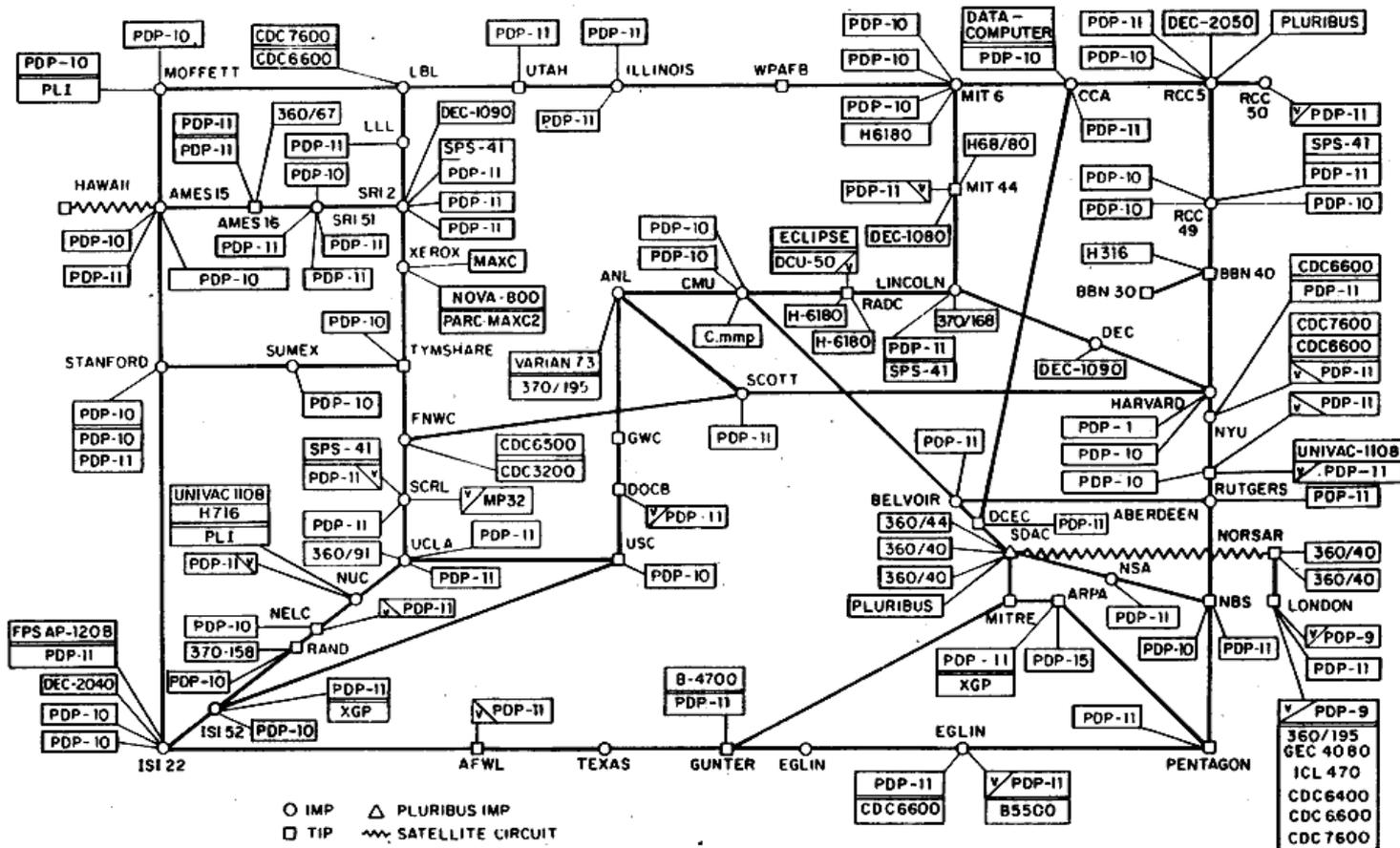
8 бит – адрес сети

24 бита – адрес хоста

Internet

Развитие адресного пространства

ARPANET LOGICAL MAP, MARCH 1977



(PLEASE NOTE THAT WHILE THIS MAP SHOWS THE MOST 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 А

0	Сеть 7 бит	Хост 24 бита
---	------------	--------------

Сети класса В

10	Сеть 14 бит	Хост 16 бит
----	-------------	-------------

Сети класса С

110	Сеть 21 бит	Хост 8 бит
-----	-------------	------------

.

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 А 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 С.

◆ Исчерпание адресов:

По оценкам 1990 года к 1994 году должны были быть исчерпаны сети класса В

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:

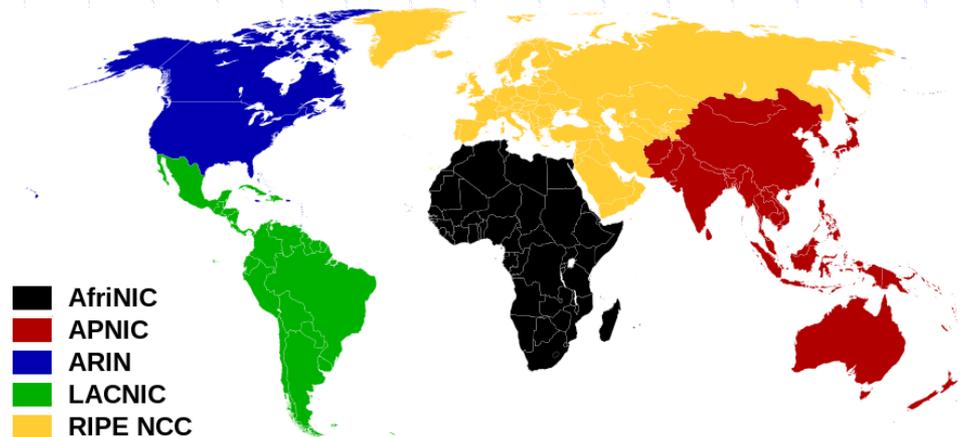
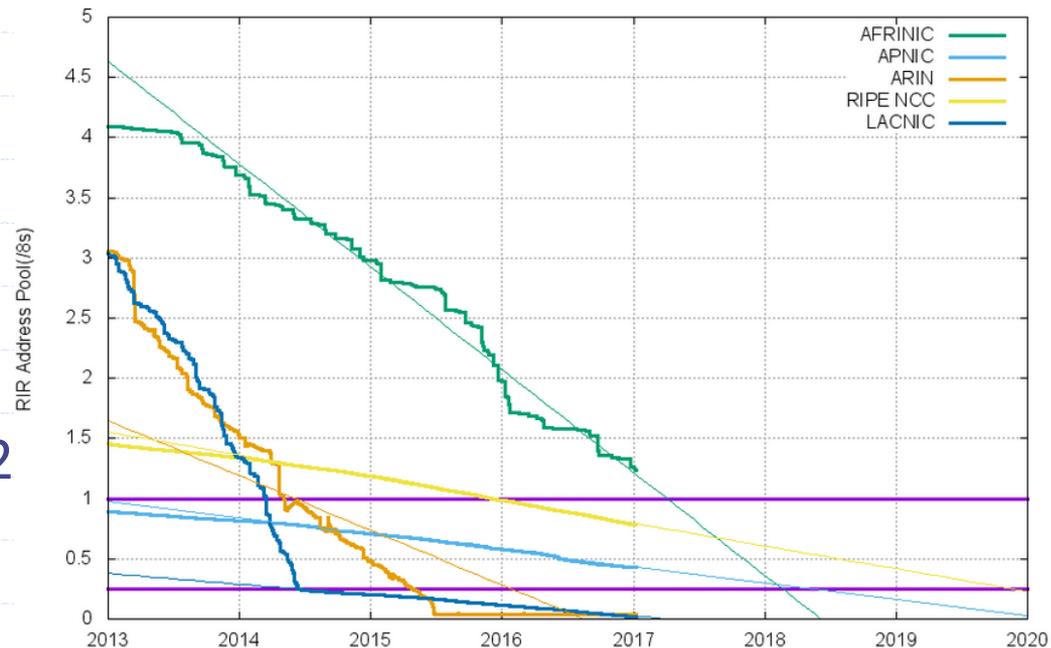
- ◆ Увеличивается число автономных систем (AS)
- ◆ Таблицы маршрутизации продолжают расти
- ◆ Уменьшается средний размер адресного пространства на одну AS
- ◆ Увеличивается число небольших сетей
- ◆ Число исключений из агрегированных сетей велико
- ◆ 3 февраля 2011 года ICANN выдала последние 5 блоков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

Internet

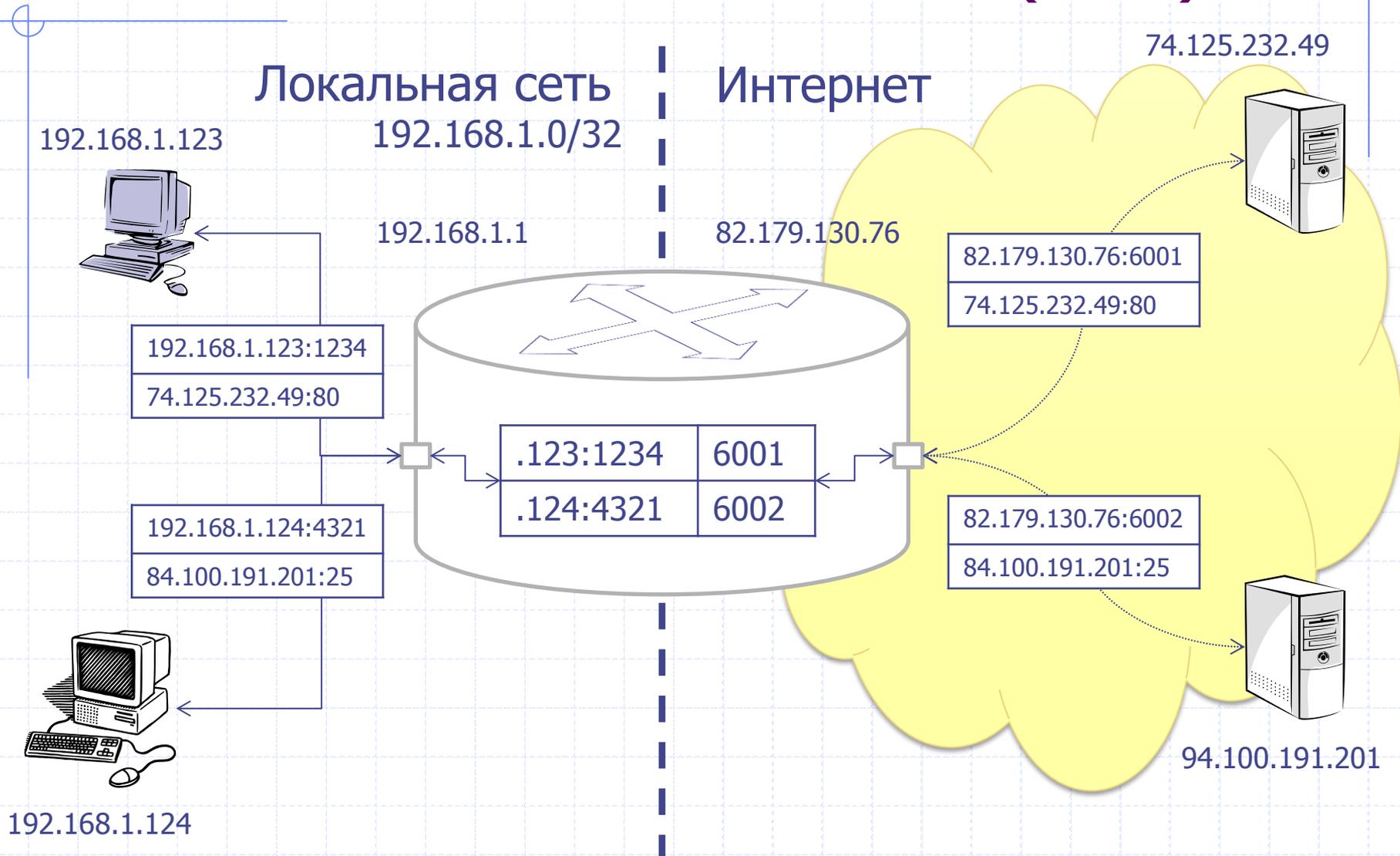
Исчерпание адресного пространства

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.

Internet

Протоколы маршрутизации

- ◆ Глобальная маршрутизация: связь между AS
 - Exterior Gateway Protocol (EGP)
 - Border Gateway Protocol (BGP)

- ◆ Маршрутизация в рамках одной AS / Interior
 - Routing Information Protocol (RIP)
 - Open Shortest Path First (OSPF)
 - ...

Протоколы маршрутизации

Алгоритмы вектора дистанций

- ◆ В конфигурацию роутера заносится информация о непосредственно подключенных к нему сетях
- ◆ Роутеры регулярно рассылают друг другу свои таблицы маршрутизации.
- ◆ Получив информацию от других маршрутизаторов, каждый корректирует свою таблицу маршрутизации, выбирая путь по алгоритму Беллмана-Форда.

Пример: RIP

Протоколы маршрутизации

Алгоритмы состояния каналов

- ◆ Маршрутизаторы находят соседей, используя специальный протокол
- ◆ Информация о подключенных соседях регулярно рассылается всем маршрутизаторам
- ◆ Каждый маршрутизатор строит граф сети
- ◆ Оптимальный маршрут находится с помощью алгоритма Дейкстры

Пример: OSPF

Стандартные приложения TCP/IP

- ◆ ifconfig
 - настройка Ethernet интерфейсов в Unix
- ◆ arp
 - просмотр/модификация ARP таблицы
- ◆ route
 - просмотр/модификация таблицы маршрутизации
- ◆ ping
 - проверка связи с помощью ICMP Echo Request/Reply
- ◆ traceroute (tracert)
 - просмотр маршрута до заданного узла
- ◆ netstat
 - просмотр открытых соединений и статистики
- ◆ nslookup
 - интерактивное средство для работы с DNS

Стандартные приложения TCP/IP

arp – управление ARP таблицей

Добавление записи в таблицу ARP

```
arp -s 192.168.1.212 00-aa-00-62-c6-09
```

Просмотр ARP таблицы

```
arp -a
```

```
Интерфейс: 192.168.1.138 on Interface 0x1000003
```

Адрес IP	Физический адрес	Тип
192.168.1.212	00-aa-00-62-c6-09	статический
192.168.1.1	00-18-39-27-76-44	динамический
192.168.1.5	00-18-F3-6F-52-B2	динамический
192.168.1.137	00-18-EA-64-8B-71	динамический

Удаление записи

```
arp -d 192.168.1.212
```

Стандартные приложения TSP/IP

route – управление роутингом

Просмотр таблицы роутинга

```
route PRINT
```

```
=====
```

Список интерфейсов

```
0x1 ..... MS TCP Loopback interface
```

```
0x3000003 ...00 11 95 df 89 8c ..... D-Link AirPremier DWL-AG660
```

```
=====
```

Активные маршруты:

Сетевой адрес	Маска сети	Адрес шлюза	Интерфейс	Метрика
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.138	1
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1
192.168.1.0	255.255.255.0	192.168.1.138	192.168.1.138	1
192.168.1.138	255.255.255.255	127.0.0.1	127.0.0.1	1
192.168.1.255	255.255.255.255	192.168.1.138	192.168.1.138	1
224.0.0.0	224.0.0.0	192.168.1.138	192.168.1.138	1
255.255.255.255	255.255.255.255	192.168.1.138	192.168.1.138	1

```
Основной шлюз: 192.168.1.1
```

```
=====
```

Постоянные маршруты:

Отсутствует

Стандартные приложения TSP/IP

route – управление роутингом

Добавить запись “пакеты для сети 157.0.0.0 с маской 255.0.0.0 отправлять через интерфейс 2 на маршрутизатор 157.55.80.1, метрика 3” в таблицу маршрутизации:

```
route      ADD      157.0.0.0      MASK      255.0.0.0  
157.55.80.1 METRIC 3 IF 2
```

Удалить запись из таблицы маршрутизации:

```
route DELETE 157.0.0.0
```

Стандартные приложения TCP/IP

ping – проверка связи

```
ping 127.0.0.1
```

```
Обмен пакетами с 127.0.0.1 по 32 байт:
```

```
Ответ от 127.0.0.1: число байт=32 время<10мс TTL=128
```

```
Ответ от 127.0.0.1: число байт=32 время<10мс TTL=128
```

```
Ответ от 127.0.0.1: число байт=32 время<10мс TTL=128
```

```
Ответ от 127.0.0.1: число байт=32 время<10мс TTL=128
```

```
Статистика Ping для 127.0.0.1:
```

```
Пакетов: отправлено = 4, получено = 4, потеряно = 0  
(0% потерь),
```

```
Приблизительное время передачи и приема:
```

```
наименьшее = 0мс, наибольшее = 0мс, среднее = 0мс
```

Стандартные приложения TCP/IP

ping – проверка связи

```
ping www.google.ru
```

```
Обмен пакетами с www.l.google.com [74.125.79.106] по 32  
байт:
```

```
Ответ от 74.125.79.106: число байт=32 время=266мс TTL=51
```

```
Ответ от 74.125.79.106: число байт=32 время=235мс TTL=51
```

```
Превышен интервал ожидания для запроса.
```

```
Ответ от 74.125.79.106: число байт=32 время=266мс TTL=51
```

```
Статистика Ping для 74.125.79.106:
```

```
Пакетов: отправлено = 4, получено = 3, потеряно = 1 (25%  
потерь),
```

```
Приблизительное время передачи и приема:
```

```
наименьшее = 235мс, наибольшее = 266мс, среднее  
= 191мс
```

Стандартные приложения TCP/IP

tracert – определение маршрута

```
tracert www.google.ru
```

```
Трассировка маршрута к www.l.google.com [74.125.79.103]  
с максимальным числом прыжков 30:
```

```
 1  203 ms  203 ms  188 ms   82.179.128.62  
 2  203 ms  188 ms  187 ms   82.179.128.61  
 3    *      282 ms   *       m9-1-gw.msk.runnet.ru [194.190.255.101]  
 4    *      *       204 ms  msk-ix-gw1.google.com [193.232.244.232]  
 5  281 ms   *       *       72.14.236.248  
 6    *      *       *       Превышен интервал ожидания для запроса.  
 7    *      *       *       Превышен интервал ожидания для запроса.  
 8  282 ms   *       *       209.85.255.166  
 9    *      *       *       Превышен интервал ожидания для запроса.  
10   *      297 ms   *       74.125.79.103  
11  266 ms   *       *       74.125.79.103  
12  250 ms   *       235 ms  ey-in-f106.google.com [74.125.79.106]
```

```
Трассировка завершена.
```

Стандартные приложения TCP/IP

netstat – статистика

```
netstat
```

```
Активные подключения
```

Имя	Локальный адрес	Внешний адрес	Состояние
TCP	cf-34:1030	cf-34:9051	ESTABLISHED
TCP	cf-34:1031	cf-34:1032	ESTABLISHED
TCP	cf-34:1032	cf-34:1031	ESTABLISHED
TCP	cf-34:1098	cf-34:1099	ESTABLISHED
TCP	cf-34:1099	cf-34:1098	ESTABLISHED
TCP	cf-34:1105	cf-34:1106	ESTABLISHED
TCP	cf-34:1106	cf-34:1105	ESTABLISHED
TCP	cf-34:9051	cf-34:1030	ESTABLISHED
TCP	cf-34:1065	c-89-160-32-161.cust.bredband2.com:9001	ESTABLISHED
TCP	cf-34:1299	smit.citynetwork.se:9001	ESTABLISHED
TCP	cf-34:1306	bos-m017a-sdr3.blue.aol.com:5190	ESTABLISHED
TCP	cf-34:1431	stgt-5f703f54.pool.mediaWays.net:https	ESTABLISHED
TCP	cf-34:1633	zitaraku.ath.cx:https	ESTABLISHED
TCP	cf-34:4308	mail.tversu.ru:imap	ESTABLISHED

Стандартные приложения TCP/IP

netstat – статистика

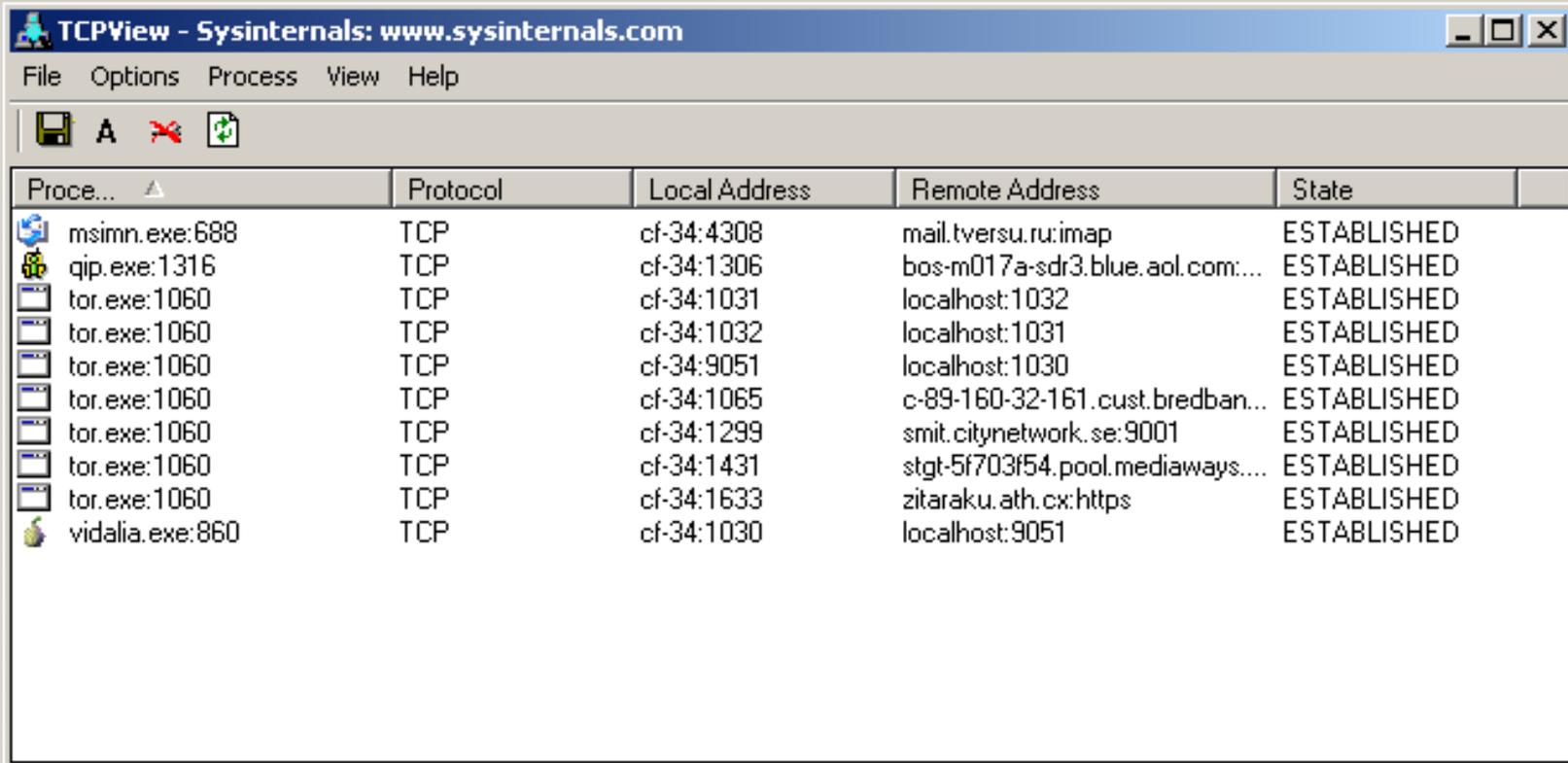
Netstat -a

Активные подключения

Имя	Локальный адрес	Внешний адрес	Состояние
TCP	cf-34:epmap	cf-34:0	LISTENING
TCP	cf-34:microsoft-ds	cf-34:0	LISTENING
TCP	cf-34:1025	cf-34:0	LISTENING
TCP	cf-34:1027	cf-34:0	LISTENING
TCP	cf-34:1073	cf-34:0	LISTENING
TCP	cf-34:1072	cf-34:0	LISTENING
TCP	cf-34:1072	cf-34:1073	ESTABLISHED
TCP	cf-34:1073	cf-34:1072	ESTABLISHED
TCP	cf-34:8118	cf-34:0	LISTENING
UDP	cf-34:epmap	*:*	
UDP	cf-34:microsoft-ds	*:*	
UDP	cf-34:1026	*:*	

[не]стандартные приложения TCP/IP

TcpView – статистика



The screenshot shows the TCPView application window with the following data:

Proce...	Protocol	Local Address	Remote Address	State
msimn.exe:688	TCP	cf-34:4308	mail.tversu.ru:imap	ESTABLISHED
qip.exe:1316	TCP	cf-34:1306	bos-m017a-sdr3.blue.aol.com:...	ESTABLISHED
tor.exe:1060	TCP	cf-34:1031	localhost:1032	ESTABLISHED
tor.exe:1060	TCP	cf-34:1032	localhost:1031	ESTABLISHED
tor.exe:1060	TCP	cf-34:9051	localhost:1030	ESTABLISHED
tor.exe:1060	TCP	cf-34:1065	c-89-160-32-161.cust.bredban...	ESTABLISHED
tor.exe:1060	TCP	cf-34:1299	smit.citynetwork.se:9001	ESTABLISHED
tor.exe:1060	TCP	cf-34:1431	stgt-5f703f54.pool.mediaways...	ESTABLISHED
tor.exe:1060	TCP	cf-34:1633	zitaraku.ath.cx:https	ESTABLISHED
vidalia.exe:860	TCP	cf-34:1030	localhost:9051	ESTABLISHED

Стандартные приложения TCP/IP

nslookup – запросы к DNS

```
c:\>nslookup
```

```
Default Server: DD-WRT  
Address: 192.168.1.1
```

```
> www.tversu.ru
```

```
Server: DD-WRT  
Address: 192.168.1.1
```

```
Non-authoritative answer:
```

```
Name: www.tversu.ru  
Address: 82.179.130.12
```

Стандартные приложения TCP/IP

nslookup – запросы к DNS

```
> set querytype=MX
```

```
> tversu.ru
```

```
Server: DD-WRT
```

```
Address: 192.168.1.1
```

```
Non-authoritative answer:
```

```
tversu.ru MX preference = 10, mail exchanger =  
mail.tversu.ru
```

```
tversu.ru nameserver = ns.tversu.ru
```

```
tversu.ru nameserver = ns.runnet.ru
```

```
mail.tversu.ru internet address = 82.179.130.2
```

```
ns.runnet.ru internet address = 194.85.32.18
```

```
ns.tversu.ru internet address = 82.179.130.
```

Стандартные приложения TCP/IP

nslookup – запросы к DNS

```
> server 82.179.130.1
```

```
Default Server: ns.tversu.ru
```

```
Address: 82.179.130.1
```

```
> set querytype=ANY
```

```
> tversu.ru
```

```
Server: ns.tversu.ru
```

```
Address: 82.179.130.1
```

```
tversu.ru
```

```
primary name server = ns.tversu.ru
```

```
responsible mail addr = mike.ns.tversu.ru
```

```
serial = 2009101501
```

```
refresh = 86400 (1 day)
```

```
retry = 7200 (2 hours)
```

```
expire = 2419200 (28 days)
```

```
default TTL = 86400 (1 day)
```

```
tversu.ru MX preference = 10, mail exchanger = mail.tversu.ru
```

```
tversu.ru nameserver = ns.runnet.ru
```

```
tversu.ru nameserver = ns.tversu.ru
```

```
tversu.ru text =
```

```
"v=spf1 +mx:tversu.ru -all"
```

```
tversu.ru internet address = 82.179.130.2
```

```
mail.tversu.ru internet address = 82.179.130.2
```

```
ns.runnet.ru internet address = 194.85.32.18
```

```
ns.tversu.ru internet address = 82.179.130.1
```

[не]стандартные приложения TCP/IP

netcat

Активное соединение

```
# netcat www.tversu.ru 80
```

Приём соединения на порт 9875

```
# netcat -l -p 9875
```

Туннелирование: перенаправляем соединения с порта 8080 на www.tversu.ru

```
# netcat -L www.tversu.ru:80 -p 8080
```

Работа с UDP

```
# netcat -u time.server.com 13
```

```
Thu Oct 20 14:41:57 2009
```