Лекция по курсу СПО

Принципы построения сетей TCP/IP

Рассматриваемые темы

- История развития Internet
- Сетевая модель OSI ISO
- Семейство протоколов TCP/IP
- Адресация в протоколе IP
- Механизмы конфигурирования сетевых интерфейсов
- Маршрутизация пакетов TCP/IP
- Система доменных имён DNS

История сетей обработки информации

1956-59 гг. – проект ЕГСВЦ (Единой государственной сети вычислительных центров), Китов А. И.
1962-64 гг. – проект ОГАС (Общегосударственной автоматизированной системы учёта и обработки информации), Глушков В. М.

1966 г. – эскизный проект ARPANET
1969 г. – запуск сети ARPANET
1971 г. – электронная почта
1973 г. – начало разработки TCP/IP
1975 г. – первая сеть TCP/IP
1.1.1983 – переход ARPANET на TCP/IPv4
1984 г. – NSFNet
1985-1994 гг. – коммерциализация Internet

Стандартизация Internet

ISOC – Internet Society, 1992 г.
IETF – Internet Engineering Task Force, 1986 г.
IAB – Internet Architecture Board
ICANN – Internet Corporation for Assigned Names and Numbers
IANA – Internet Assigned Numbers Authority

RFC – Requests For Comments
1969-04-07: RFC 1 «Host Software»

Март 1992: RFC 1310 «The Internet Standards Process»
Март 1994: RFC 1602 «The Internet Standards Process -- Revision 2»
Октябрь 1996: RFC 2026 «The Internet Standards Process -- Revision 3»

2008-04-01: RFC 5241 «Naming Rights in IETF Protocols»
2014-04-01: RFC 7169 «The NSA (No Secrecy Afforded) Certificate Extension»
2018-04-01: RFC 8367 «Wrongful Termination of Internet Protocol (IP) Packets»

Сетевая модель OSI ISO

Основы построения сетей

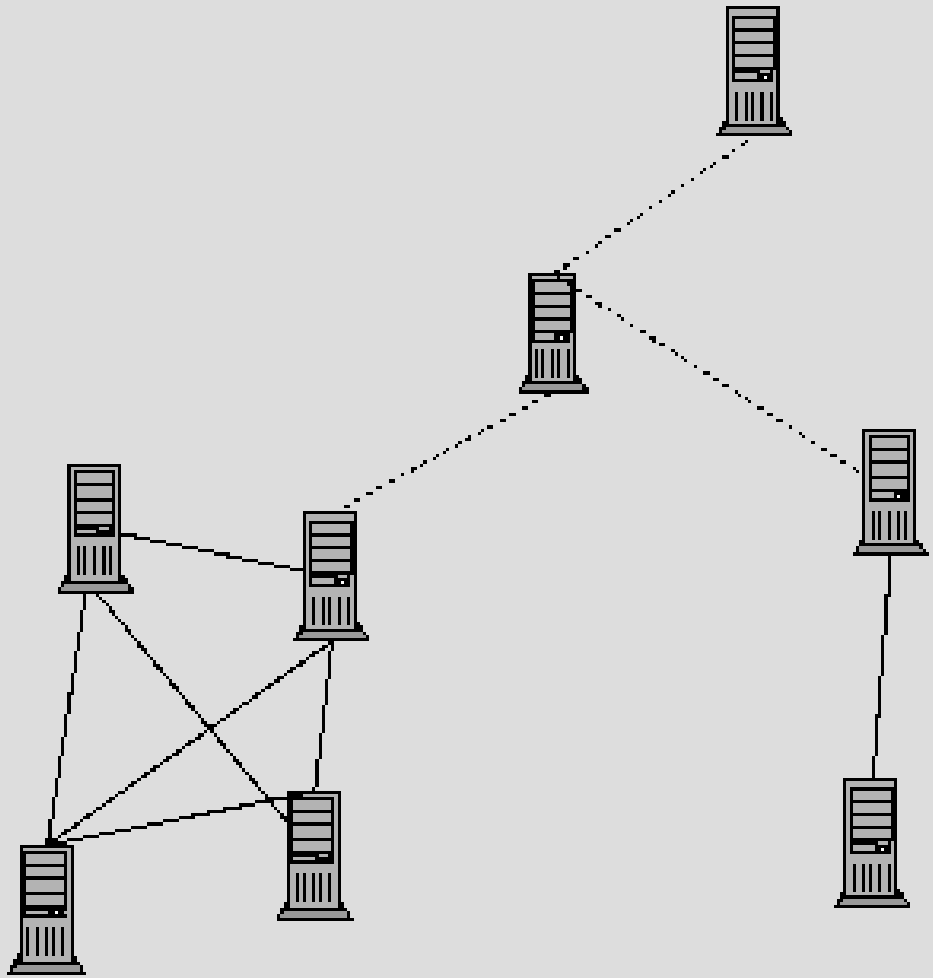
Сети:
- потоковая передача данных
- пакетная передача данных

Пакет данных:

Основы построения сетей

По каналам связи:
- коммутируемые каналы передачи данных
- выделенные каналы передачи данных

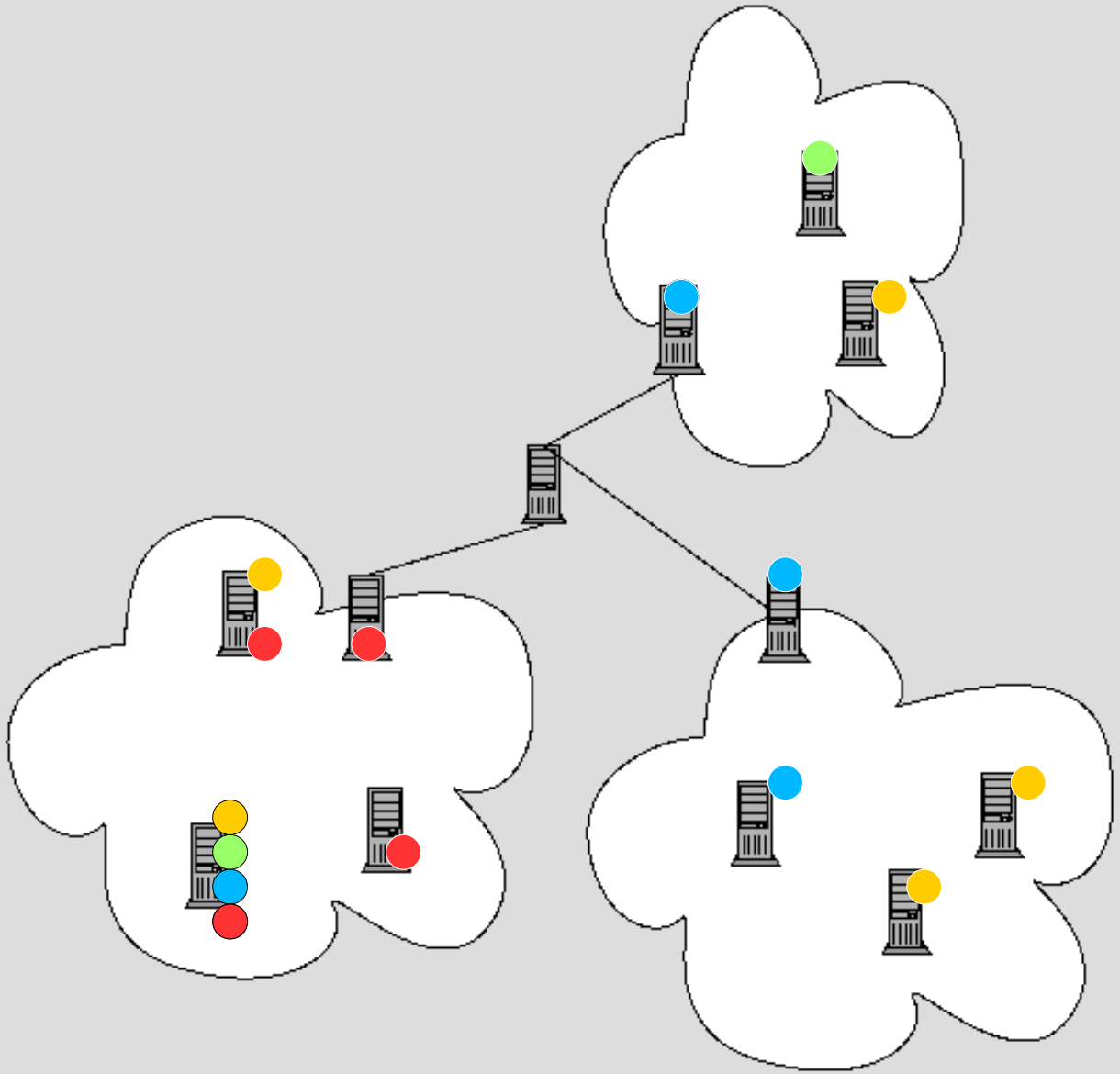
По организации связи:
- одноранговые
- маршрутизируемые



Основы построения сетей

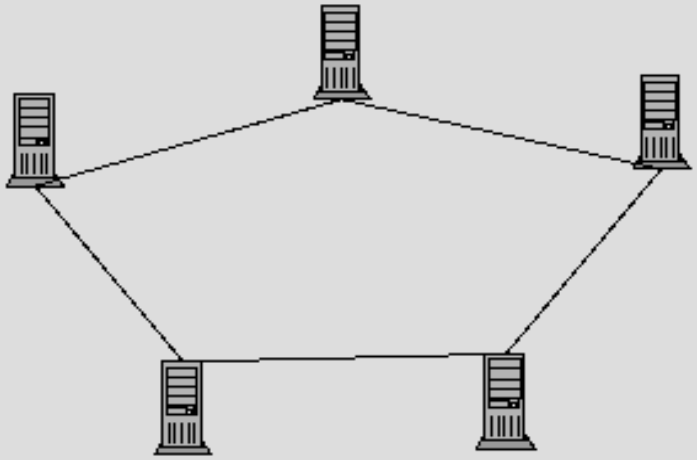
Сети:
- локальные
- глобальные

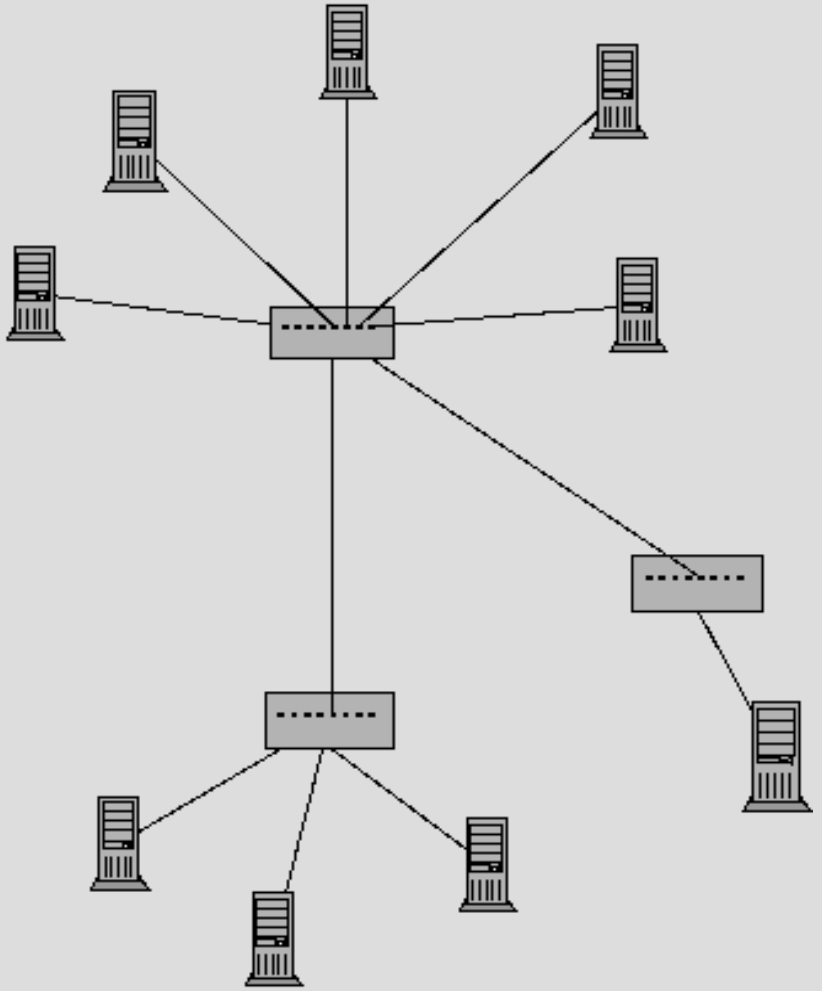
Адресация в сетях
- unicast
- multicast
- anycast
- broadcast



Основы построения сетей

Топология локальных сетей:
- общая шина
- кольцо
- звезда

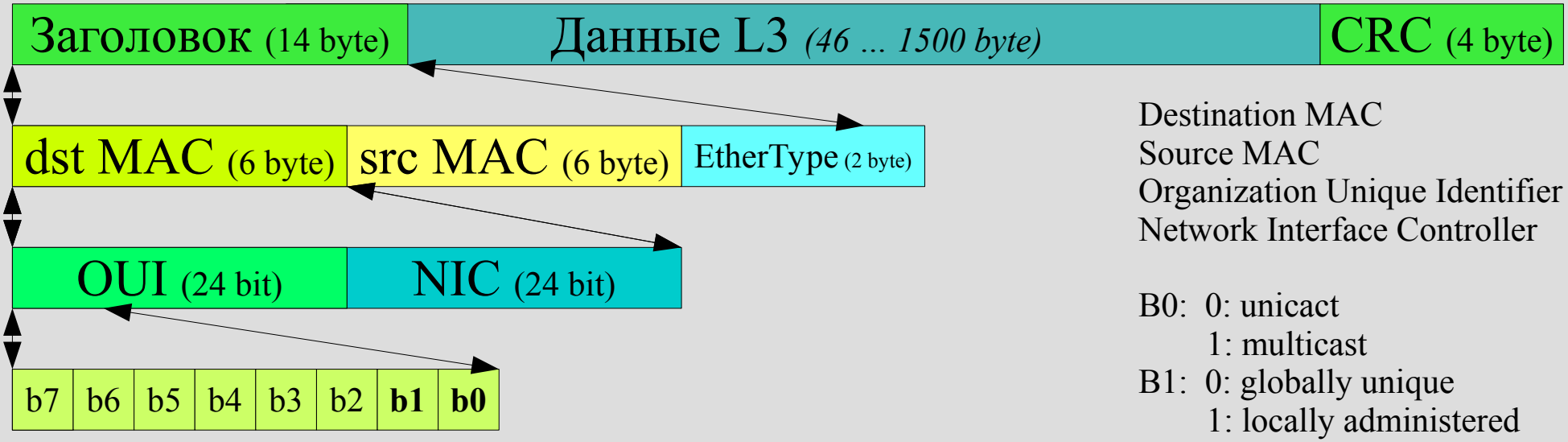




Сети Ethernet

Ethernet (IEEE-802.x, начало разработки1980 г.):
- протокол L2;
- объединяет peer'ы;
- уникальный адрес каждого peer'а;
- связи: peer-peer, peer-hub, hub-hub.

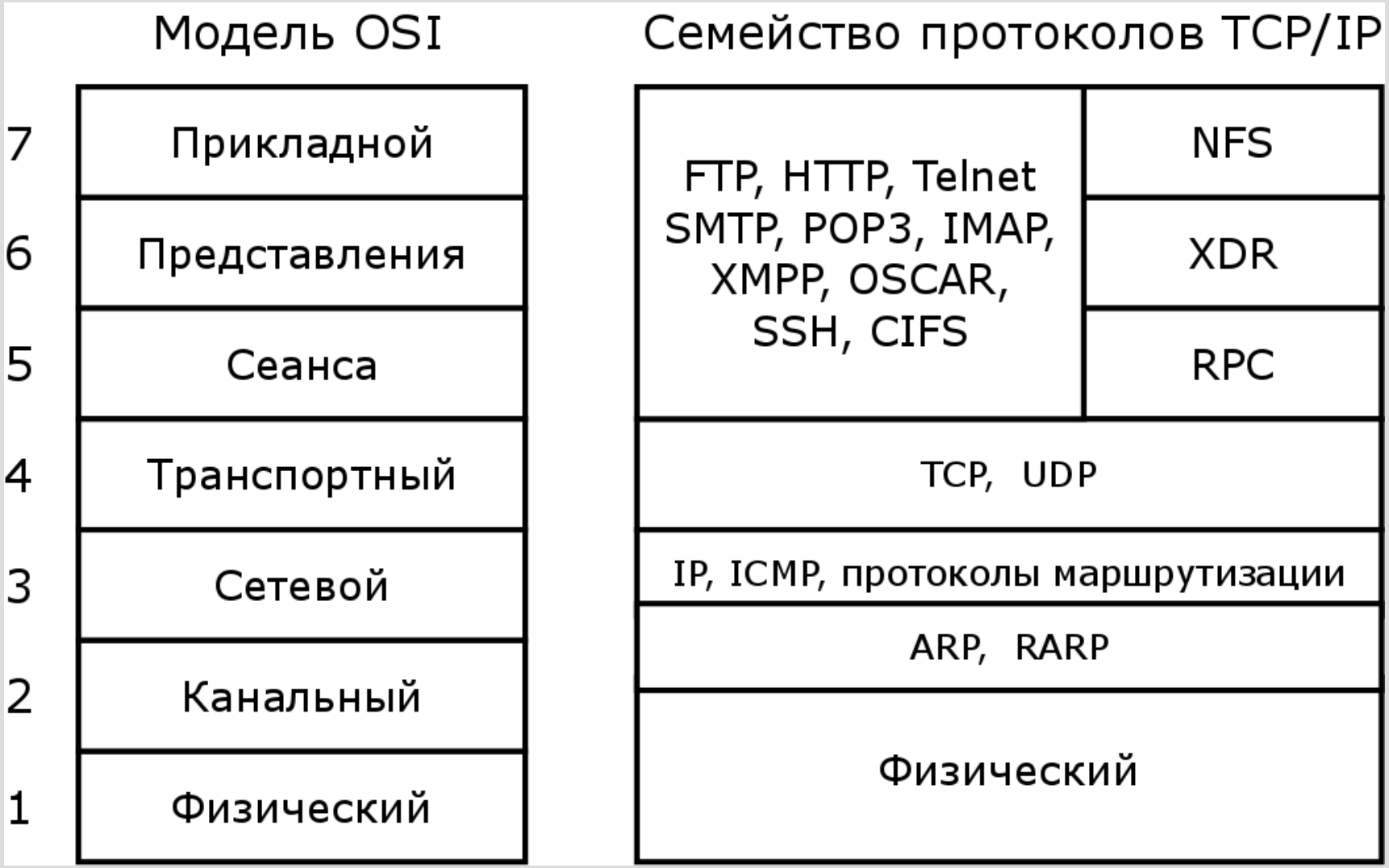
Адреса: MAC (Media Access Control), IEEE (Institute of Electrical and Electronics Engineers). Сейчас – MAC-48. Есть также EUI-48, EUI-64.



Destination MAC
Source MAC
Organization Unique Identifier
Network Interface Controller

B0: 0: unicact
1: multicast
B1: 0: globally unique
1: locally administered

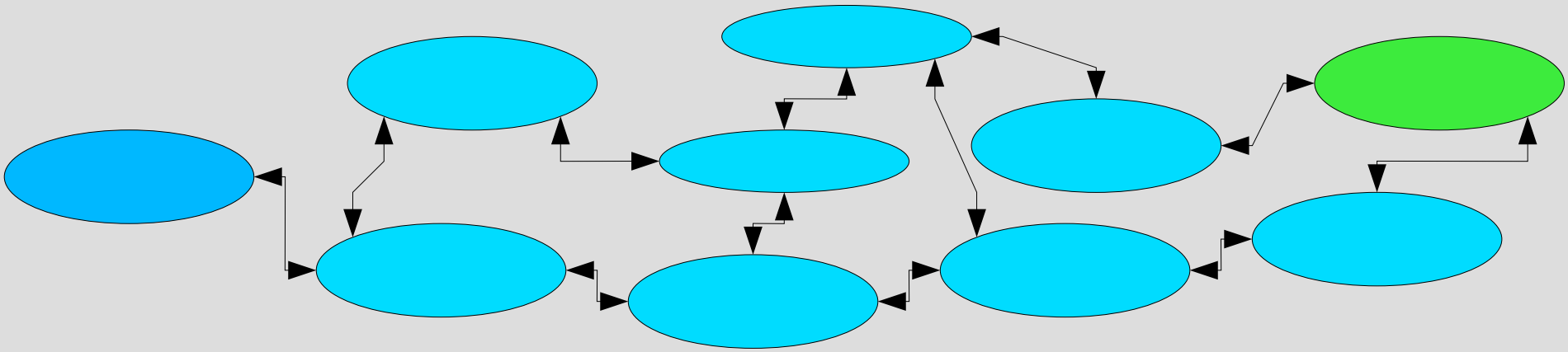
Семейство протоколов TCP/IP



Адресация в сетях IP

Протокол IP:

- Сетевой уровень модели OSI
- Передаёт данные через сетевые интерфейсы от хоста к хосту
- Каждый хост имеет уникальный адрес
- Длина адреса IPv4 – 32 бита, IPv6 – 128 бит
- Хосты по адресам IP группируются в сети
- Сети объединяются через маршрутизаторы



Адреса протокола IPv4

Адрес IP v4:
- целое беззнаковое число
- длина адреса 32 бита, или 4 байта
- записывается по-байтно через точку
- состоит из адреса сети и адреса хоста

Маска сети:
- служит для выделения адреса сети
- длина маски равна длине адреса
- начинается с последовательности единиц
- кончается нулями

Адрес IP – 193.233.68.72/255.255.255.0	
11000001 11101001 01000100	01001000
11111111 11111111 11111111	00000000

Классы сетей IPv4

Класс	Маска	Диапазон адресов
A (0...)	255.0.0.0	1.0.0.0 - 127.255.255.255
B (10...)	255.255.0.0	128.0.0.0 - 191.255.255.255
C (110...)	255.255.255.0	192.0.0.0 - 223.255.255.255
D (1110...)	-	224.0.0.0 - 239.255.255.255
E (1111...)	?	240.0.0.0 - 255.255.255.255

D — адреса multicast; E - зарезервировано

Адресация в сетях IPv4

127.0.0.0/8 – сеть loopback-интерфейса, IP 127.0.0.1/8

Бесклассовая адресация:
- отказ от выровненных по границам байта масок сетей
- произвольная длина маски сети
- агрегация сетей

Частные сети (RFC 1918, 1996 г.):

1	сеть	A: 10.0.0.0/8
16	сетей	B: 172.16.0.0-172.31.0.0
256	сетей	C: 192.168.0.0-192.168.255.0

Частные сети уровня провайдеров (RFC 6598, 2012 г.):
Диапазон адресов 100.64.0.0/10

Доступ из частных сетей в Internet:
- прокси-серверы
- трансляция адресов

Адреса протокола IPv6

Адрес IP v6:

- целое беззнаковое число
- длина адреса 128 бит, или 16 байт
- записывается группами по 4 16-ричных цифры
- группы разделяются двоеточиями
- ведущие нули групп можно опускать
- самую большую группу нулей можно опускать
- маска записывается в бесклассовой нотации

2001:0db8:0000:0064:0000:0000:aa72:0004/64
2001:db8:0:64:0:0:aa72:4/64
2001:db8:0:64::aa72:4/64

Адрес локального интерфейса - ::1/128

Конфигурация сетевых интерфейсов

Физический и канальный уровень:
- наиболее распространённый протокол – Ethernet
- имеются уникальные сетевые адреса канального уровня (MAC-адреса)

Сетевой уровень – IP:
- необходимо назначить сетевому интерфейсу адрес IP и указать маску сети

Конфигурация сетевых интерфейсов IP:
- статическая
- автоматическая
- динамическая

Конфигурация сетевых интерфейсов

Статическая конфигурация:
- ручная настройка адресов IP
- сохраняется в настройках операционной системы

Автоматическая конфигурация:
- адреса назначаются операционной системой
- адреса создаются на базе MAC-адреса

- IPv4 : сеть 169.254.0.0/16
  адрес хоста – случайное число

- IPv6 : сеть fe80::/64
  адрес хоста – идентификатор EUI-64

Конфигурация сетевых интерфейсов

Автоматические адреса IPv6:
MAC: 00:18:51:61:49:5a
IPv6: fe80::0**2**18:51**ff**:**fe**61:495a/64

Динамическая конфигурация:
– информация о сети получается от других хостов
– возможно получение информации о маршрутах, доступных в сети ресурсах, и т.п.

IPv4: протокол DHCP
Ipv6: протоколы динамической конфигурации IPv6, протокол DHCPv6

Конфигурация сетевых интерфейсов

DHCP:
- требуется сервер DHCP
- хост ищет сервер DHCP через широковещательные запросы
- адрес хосту выделяется на определённое время
- по истечению аренды хост повторно запрашивает адрес
- хосту также сообщаются маршруты, серверы DNS, пр. данные
- в сети может работать только один сервер DHCP
- сервер DHCP не может инициировать смену адресов клиентов

Конфигурация сетевых интерфейсов

Динамическая конфигурация IPv6:
- информацию рассылают маршрутизаторы сети
- хостам сообщаются префиксы сетей и маршруты
- хосты назначают адреса IPv6 в полученных сетях с использованием EUI-64
- адреса и маршруты назначаются для каждой из анонсированных маршрутизаторами сетей
- устаревшая конфигурация автоматически удаляется

По сравнению с DHCPv4:
- маршрутизаторы не ведут учёт адресов хостов
- нельзя передать адреса серверов DNS и пр.

Конфигурация сетевых интерфейсов

IPv4:
- обычно 1 IP на интерфейсе
- используется **один из** механизмов конфигурации
- автоматической конфигурации обычно нет

IPv6:
- обычно много IP на интерфейсе
- используются **все доступные** механизмы конфигурации
- автоматическая конфигурация используется почти всегда
- минимальная выделяемая сеть – /64. Рекомендовано выделение сети /56 каждому подключённому к Internet пользователю.

Маршрутизация в сетях TCP/IP

- Internet – объединение сетей TCP/IP
- Каждая сеть имеет свой адрес сети
- В каждой сети есть один или несколько шлюзов
- Шлюз - сетевое устройство, входящее сразу в несколько сетей
- Шлюз может передавать пакеты IP из одной сети в другую
- Маршрут - путь пакета от хоста-источника до хоста-приёмника
- Возможных маршрутов может быть несколько
- Выбор маршрута – задача шлюза
- Выбор осуществляется по таблице маршрутизации
- Маршрутизация бывает статическая и динамическая

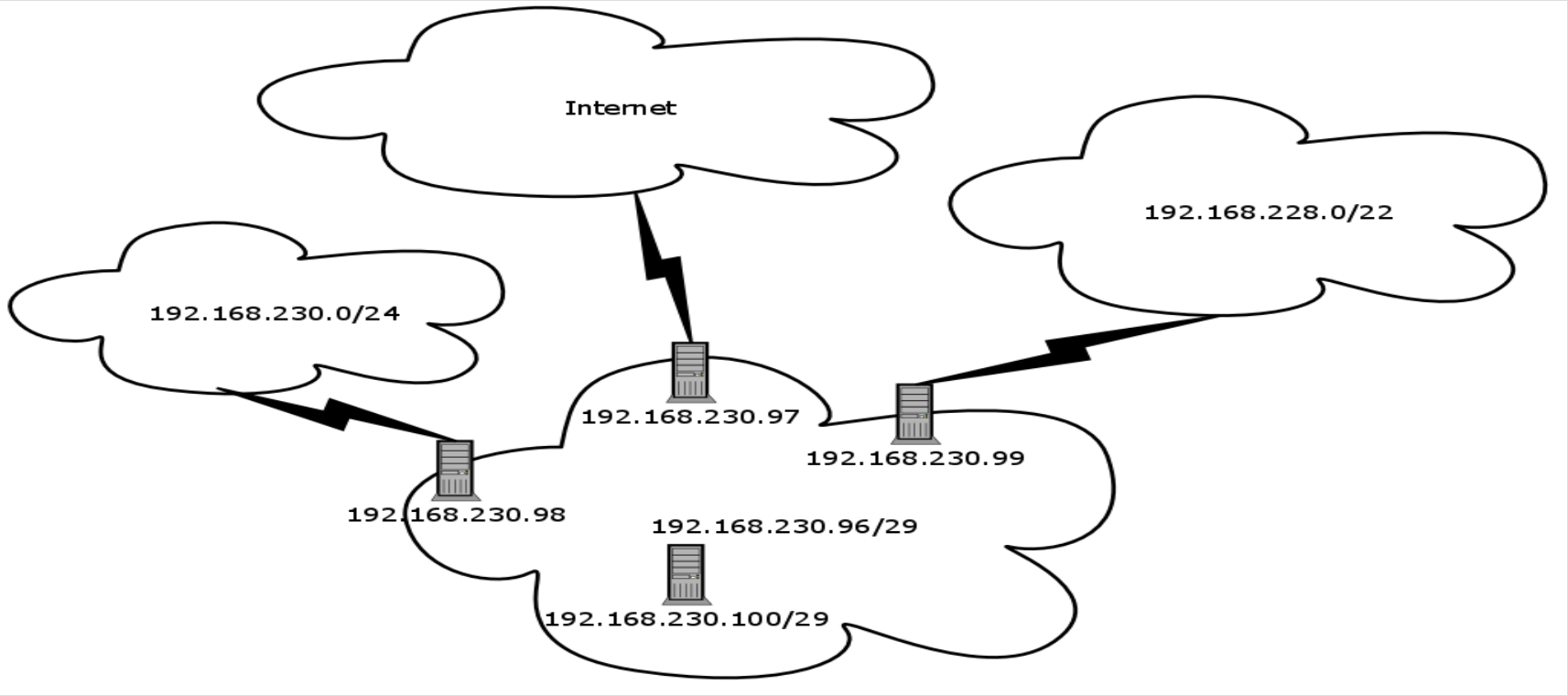
Маршрутизация в сетях TCP/IP

Как правило, статические маршруты прописываются для:
- сетей, к которым непосредственно подключён хост – без указания шлюза;
- сетей, маршруты к которым должны проходить через известные шлюзы – с указанием шлюзов;
- для всех остальных сетей – через шлюз по-умолчанию.

Все шлюзы должны быть в одной сети / сетях с хостом – т.е., статически прописать проходящий через несколько шлюзов маршрут нельзя.

Динамическая маршрутизация применяется в-основном на центральных шлюзах в крупных сетях и на магистральных маршрутизаторах Internet.

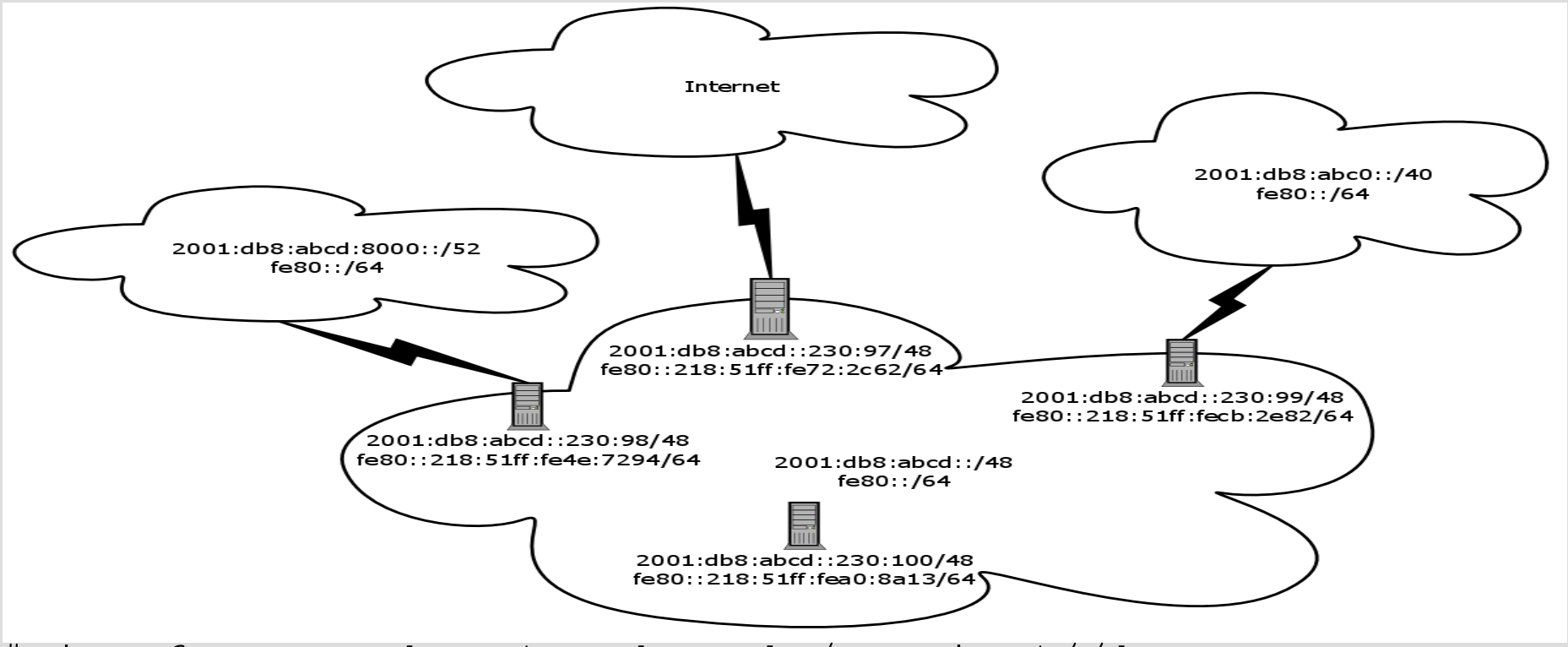
Маршрутизация в сетях IPv4




```
# ip route show
192.168.230.96/29 dev eth0 src 192.168.230.100
192.168.230.0/24 via 192.168.230.98 dev eth0
192.168.228.0/22 via 192.168.230.99 dev eth0
default via 192.168.230.97 dev eth0

# default => 0.0.0.0/0
```

Маршрутизация в сетях IPv6




```
# ip -6 route show | sed -e 's/metric.*//'

2001:db8:abcd:8000::/52 via 2001:db8:abcd::230:98 dev eth0
2001:db8:abc0::/40 via 2001:db8:abcd::230:99 dev eth0
2001:db8:abcd::/48 dev eth0  proto kernel
fe80::/64 dev eth0  proto kernel
default via 2001:db8:abcd::230:97 dev eth0
```

Система доменных имён DNS

Соответствие адреса хоста и символьного имени:

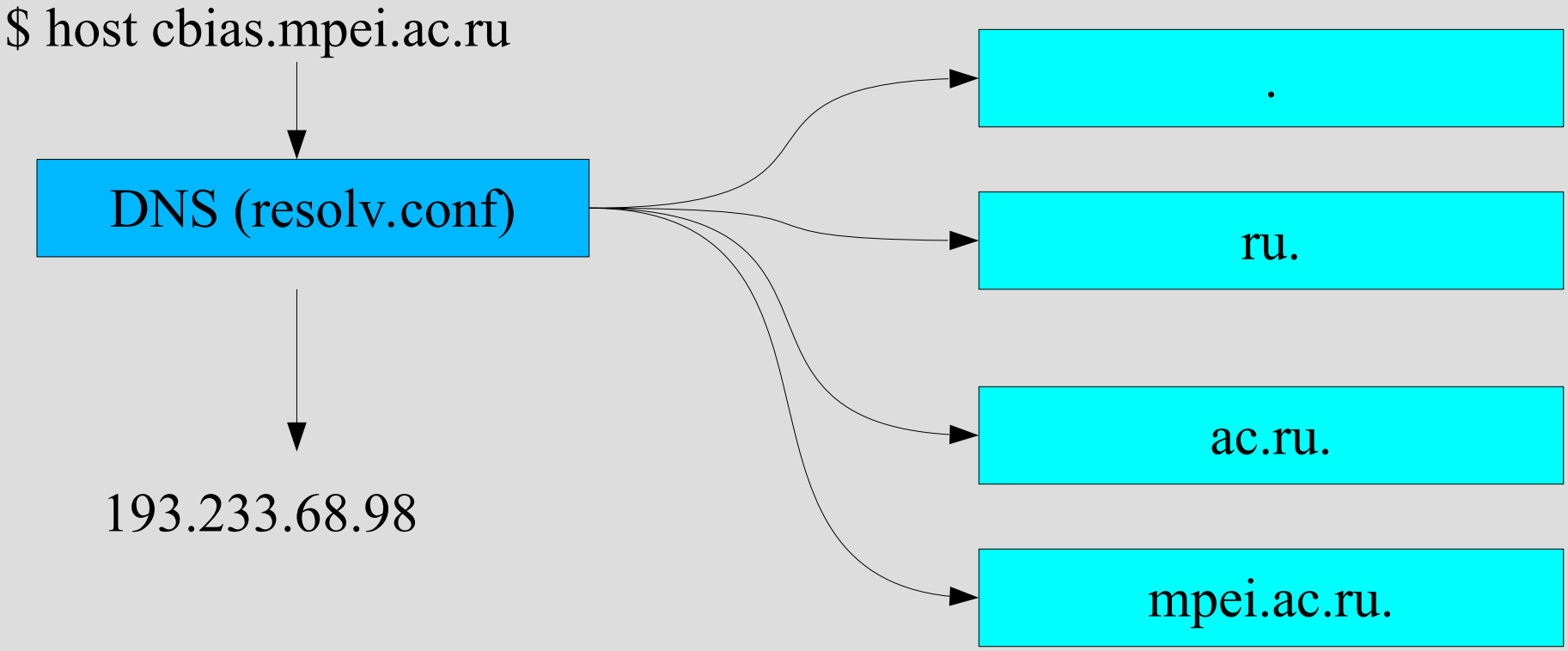
- /etc/hosts

```
$ cat /etc/hosts
127.0.0.1    localhost.localdomain localhost
::1          localhost6.localdomain6 localhost6
```

- DNS

```
$ cat /etc/resolv.conf
search example.com
nameserver 192.0.2.123
nameserver 2001:db8::1234
```

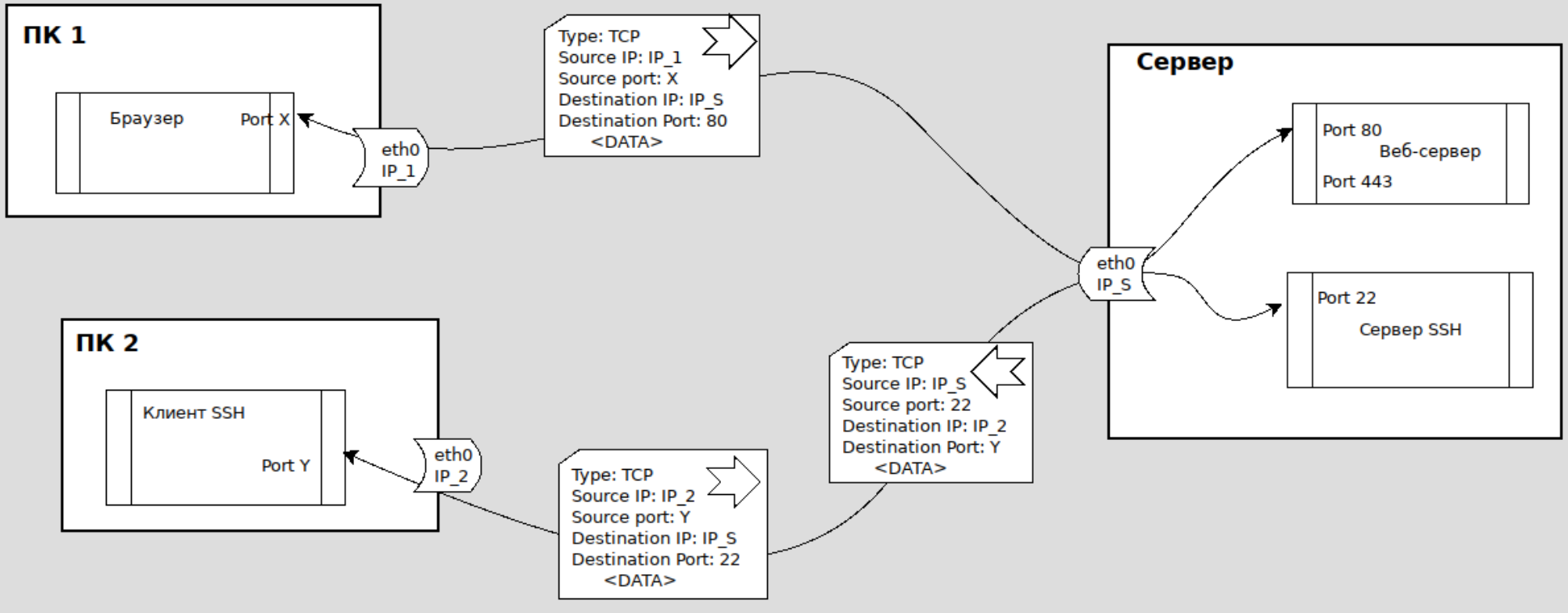
Система доменных имён DNS



Протоколы TCP, UDP

Протоколы TCP и UDP:
- протоколы семейства IP;
- протоколы транспортного уровня (L4);
- работают поверх протоколов IPv4, IPv6;
- к адресам хоста добавляется номер порта: целое 16-битное число.

Порты 0...1000 — зарезервированы для использования администратором системы.
Порты 10000...50000 – обычно используются клиентскими приложениями.



Межсетевые экраны

Задача межсетевых экранов: фильтрация и обработка сетевого трафика.

Могут работать на разных уровнях сетевой модели:
– L2: фильтрация пакетов Ehternet:
  – source MAC-адрес и EtherType;
– L3+L4: фильтрация пакетов TCP/IP:
  – тип протокола IP;
  – source IP, source IP + source port;
  – destination IP, destination IP + destination port;
  – обработка сессий TCP
– L5..L7: фильтрация по приложениям, пользователям, данным и т.п.

Обработка сетевого трафика:
– подмена source/destination IP/port (SNAT/DNAT)
– что-либо ещё

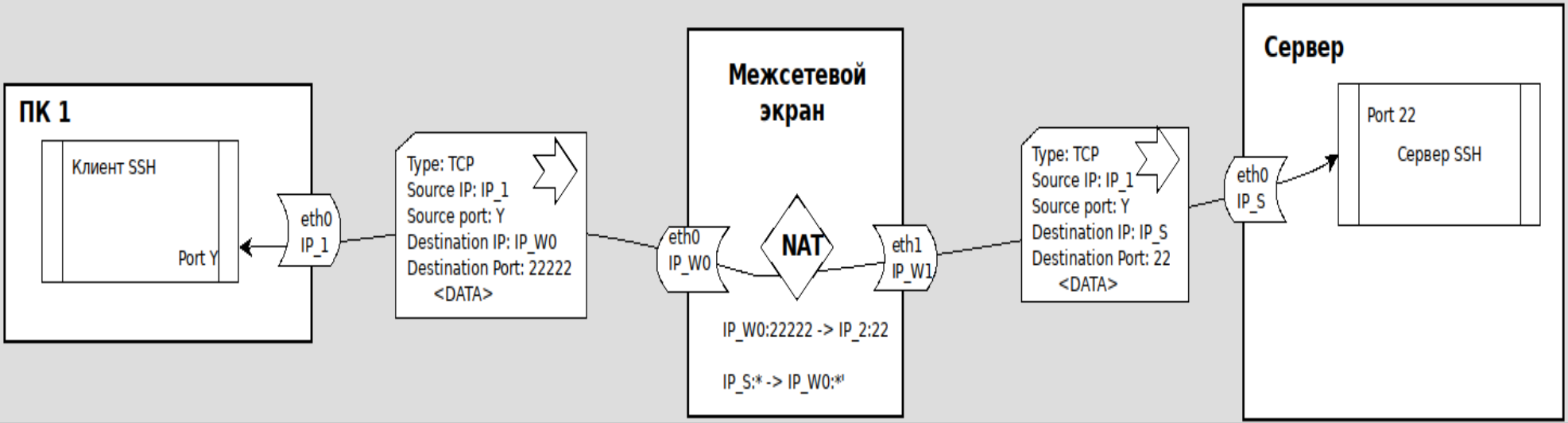
Межсетевые экраны в Linux:
– реализованы в ядре операционной системы (NetFilter);
– уровень L2 … L4.

Межсетевые экраны

Реализации межсетевых экранов в Linux:
– ipchains (ядра 2.4 включительно, устарело)
– iptables (iptables, ip6tables, arptables, ebtables)
– nftables (nft)
– bpfilter (начиная с ядер 4.8, основан на eBPF, extended Berkeley Packat Filter)

Для построение сложных фильтров используются программные надстройки, общего назначения или специфичные для дистрибутивов.

Трансляция адресов:



Проксирование соединений