

Сеть Ethernet в UNIX (Linux)

Михайленко К. И.

Уровни семейства протоколов TCP/IP

- 1 Аппаратный
Интерфейсный
- 2 Сетевой
- 3 Транспортный
- 4 Прикладной

Уровни семейства протоколов TCP/IP

- 1 **Аппаратный**
Интерфейсный
- 2 Сетевой
- 3 Транспортный
- 4 Прикладной

Пакет

Определяемый параметрами среды фрагмент сигналов. Содержит информацию об устройстве-отправителе и устройстве-приёмнике.

Уровни семейства протоколов TCP/IP

- 1 Аппаратный
Интерфейсный
- 2 **Сетевой**
- 3 Транспортный
- 4 Прикладной

Пакет

Последовательность байтов, имеющая удобный для обработки размер.
Содержит уникальные адреса отправителя и получателя.

Уровни семейства протоколов TCP/IP

- 1 Аппаратный
Интерфейсный
- 2 Сетевой
- 3 **Транспортный**
- 4 Прикладной

Пакет

Последовательность байтов, разделённая на поля известной длины. Назначение полей: служебные (сеанс связи, логика, содержимое поля данных) и поле данных.

Уровни семейства протоколов TCP/IP

- 1 Аппаратный
Интерфейсный
- 2 Сетевой
- 3 Транспортный
- 4 Прикладной

Пакет

Данные, с которыми работает
прикладная программа.

Утилита ifconfig

Вызов ifconfig

```
$ /sbin/ifconfig
eth0      Link encap:Ethernet  HWaddr 00:11:25:83:D2:98
          inet addr:172.16.6.9  Bcast:172.16.255.255  Mask:255.255.0.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0
          RX bytes:92 (92.0 b)  TX bytes:92 (92.0 b)
```

Утилита ifconfig

Получение информации:

- Вызов `ioctl()`
- Чтение из каталога `/proc/net`

MTU Maximum Transfer Unit

HWaddr HardWare address

MAC Media Access Control

- Прослушивание среды
- Обнаружение коллизий
- Случайное время ожидания перед повтором

MAC-адрес: 6 байтов

Широковещательный MAC-адрес: FF:FF:FF:FF:FF:FF

Утилита ifconfig

Вызов ifconfig

```
# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:11:25:83:D2:98
          inet addr:172.16.6.9  Bcast:172.16.255.255  Mask:255.255.0.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0
          RX bytes:92 (92.0 b)  TX bytes:92 (92.0 b)
```

Internetwork Protocol

IP Internetwork Protocol

lo loopback

IP-адрес: 4 байта

Адрес сети	Адрес абонента
адрес: 172.16.6.9; маска: 255.255.0.0; запись: 172.16.6.9/16	
широковещательный адрес: 172.16.255.255	
10101100 00010000	00000110 00001001
11111111 11111111	00000000 00000000
адрес: 62.76.10.70; маска: 255.255.255.240; запись: 62.76.10.70/28	
широковещательный адрес: 62.76.10.79	
00111110 01001100 00001010 0100	0110
11111111 11111111 11111111 1111	0000

Internetwork Protocol

Специальные адреса сетей:

- loopback 127.0.0.0/8
- class C 192.168.0.0/24
- class B 172.16.0.0/16
- class A 10.0.0.0/8

Утилита arp

ARP Address Resolution Protocol

```
# /sbin/arp -a
# ping 172.16.6.111
...
# ping google.com
PING google.com (216.239.57.99) 56(84) bytes of data.
...
# ping 172.16.0.51
...
# /sbin/arp -a
? (172.16.0.1) at 52:54:4C:02:28:C7 [ether] on eth0
? (172.16.6.111) at 00:11:85:8E:26:D2 [ether] on eth0
? (172.16.0.51) at 00:E0:81:2F:05:B9 [ether] on eth0
```

Утилита arp

Таблица ARP на шлюзе

```
# arp -an
? (172.16.6.9) at 00:11:25:83:D2:98 [ether] on eth1
? (172.16.2.13) at 00:11:2F:CD:AC:31 [ether] on eth1
? (172.16.3.1) at 00:80:48:ED:35:93 [ether] on eth1
? (172.16.2.6) at 00:11:2F:8D:63:D5 [ether] on eth1
? (172.16.6.1) at 00:80:48:17:B3:0F [ether] on eth1
? (62.76.10.78) at 00:00:F8:71:59:AD [ether] on eth2
? (62.76.91.230) at 00:30:80:61:08:C0 [ether] on eth0
? (62.76.10.77) at 08:00:2B:86:AC:BD [ether] on eth2
? (62.76.10.71) at 00:C0:DF:F5:30:6A [ether] on eth2
? (62.76.10.70) at 00:C0:DF:F5:30:6A [ether] on eth2
```

Утилита route

Таблица маршрутизации

```
# route
```

```
Kernel IP routing table
```

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
172.16.0.0	*	255.255.0.0	U	0	0	0	eth0
127.0.0.0	*	255.0.0.0	U	0	0	0	lo
default	172.16.0.1	0.0.0.0	UG	0	0	0	eth0

Утилита route

Таблица маршрутизации на шлюзе

```
$ /sbin/route
```

```
Kernel IP routing table
```

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
62.76.91.224	*	255.255.255.248	U	0	0	0	eth0
62.76.10.64	*	255.255.255.240	U	0	0	0	eth2
172.16.0.0	*	255.255.0.0	U	0	0	0	eth1
127.0.0.0	*	255.0.0.0	U	0	0	0	lo
default	62.76.91.230	0.0.0.0	UG	0	0	0	eth0

Утилита traceroute

Служебный протокол ICMP

ICMP Internet Control Message Protocol

```
# traceroute ugatu.ac.ru
traceroute to ugatu.ac.ru (193.233.144.1), 30 hops max, 38 byte packets
 1 172.16.0.1 (172.16.0.1) 0.598 ms 0.560 ms 0.597 ms
 2 192.168.192.1 (192.168.192.1) 2.246 ms 2.330 ms 2.223 ms
 3 62.76.11.237 (62.76.11.237) 7.753 ms 16.073 ms 15.962 ms
 4 62.76.11.246 (62.76.11.246) 19.747 ms 8.911 ms 17.340 ms
 5 CORE-MTS.rb.ru (193.233.144.65) 23.128 ms 17.436 ms 10.591 ms
 6 oldmail.ugatu.ac.ru (193.233.144.1) 9.126 ms 8.447 ms 14.466 ms
```


Транспортные протоколы TCP/IP

UDP User Datagram Protocol
адреса+порты+данные

TCP Transmission Control Protocol

- Установление соединения
- Обработка подтверждений
- Отслеживание состояния абонентов

Контроль транспорта пакетов: `tcpdump`

Протоколы прикладного уровня

```
$ wc /etc/services  
553 2794 19869 /etc/services
```

/etc/services

```
ftp      21/tcp      # File Transfer [Control]  
ssh      22/tcp      # SSH Remote Login Protocol  
smtp     25/tcp      mail        # Simple Mail Transfer Protocol  
http     80/tcp      www www-http # World Wide Web HTTP
```

Открытые порты (сервер)

```
$ netstat -anA inet
```

```
Active Internet connections (servers and established)
```

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	0.0.0.0:110	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:80	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:25	0.0.0.0:*	LISTEN
tcp	0	216	62.76.10.70:22	172.16.6.9:32771	ESTABLISHED
tcp	0	0	62.76.10.71:80	172.16.6.9:32785	ESTABLISHED

Сервер cal

```
$ cal
```

```
Сентября 2005
```

Вс	Пн	Вт	Ср	Чт	Пт	Сб
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	

Сервер cal

```
/etc/xinet.d/cal
```

```
# description: test calendar service on quake port ;)
service quake
{
    socket_type      = stream
    protocol         = tcp
    wait             = no
    user             = nobody
    server           = /usr/bin/cal
    disable          = no
}
```

Сервер cal

```
$ telnet localhost quake
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
    September 2005
Su Mo Tu We Th Fr Sa
          1  2  3
 4  5  6  7  8  9 10
11 12 13 14 15 16 17
18 19 20 21 22 23 24
25 26 27 28 29 30
```

Старт сетевых устройств

```
# ifconfig
# ifconfig lo inet 127.0.0.1 netmask 255.0.0.0 broadcast 127.255.255.255
# ifconfig eth0 inet 172.16.6.9 netmask 255.255.0.0 broadcast 172.16.255.255
# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:11:25:83:D2:98
          inet addr:172.16.6.9  Bcast:172.16.255.255  Mask:255.255.0.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
          Base address:0x8000 Memory:c0220000-c0240000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:92 (92.0 b)  TX bytes:92 (92.0 b)
```

Типы адресов

```
man ifconfig
```

Address Families

...

Currently supported address families include

inet (TCP/IP, default),

inet6 (IPv6),

ax25 (AMPR Packet Radio),

ddp (Appletalk Phase 2),

ipx (Novell IPX) and

netrom (AMPR Packet radio).

Добавление маршрутизаторов

```
# route
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
172.16.0.0       *                255.255.0.0     U        0      0      0 eth0
127.0.0.0        *                255.0.0.0       U        0      0      0 lo
# route add default gw 172.16.0.1
# route
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
172.16.0.0       *                255.255.0.0     U        0      0      0 eth0
127.0.0.0        *                255.0.0.0       U        0      0      0 lo
default          172.16.0.1      0.0.0.0         UG       0      0      0 eth0
# route -n
Kernel IP routing table
Destination      Gateway          Genmask          Flags Metric Ref    Use Iface
172.16.0.0       0.0.0.0         255.255.0.0     U        0      0      0 eth0
127.0.0.0        0.0.0.0         255.0.0.0       U        0      0      0 lo
0.0.0.0          172.16.0.1     0.0.0.0         UG       0      0      0 eth0
```

Служба доменных имён (статическая информация)

```
/etc/hosts
```

```
127.0.0.1          localhost.localdomain localhost
172.16.6.9         const-tp
```

```
man hosts
```

Служба доменных имён (адреса DNS)

```
/etc/resolv.conf
```

```
# search localdomain  
domain anrb.ru  
nameserver 62.76.11.151  
nameserver 62.76.8.134  
nameserver 195.128.128.1
```

```
man resolv.conf
```

Стартовый скрипт (технология ifupdown)

/etc/init.d/network

Базовая информация для стартового скрипта network

```
$ cat /etc/sysconfig/network  
NETWORKING=yes  
HOSTNAME=const-tp  
DOMAINNAME=anrb.ru  
GATEWAY=172.16.0.1
```

Описание интерфейсов (технология ifupdown)

Каталог /etc/sysconfig/network-scripts
Файл README

Интерфейс loopback

```
# cat /etc/sysconfig/network-scripts/ifcfg-lo
DEVICE=lo
IPADDR=127.0.0.1
NETMASK=255.0.0.0
NETWORK=127.0.0.0
BROADCAST=127.255.255.255
ONBOOT=yes
NAME=loopback
```

Описание интерфейсов (технология ifupdown)

Каталог /etc/sysconfig/network-scripts

Интерфейс eth0

```
# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
BOOTPROTO=static
IPADDR=172.16.6.9
NETMASK=255.255.0.0
NETWORK=172.16.0.0
BROADCAST=172.16.255.255
ONBOOT=yes
HWADDR=00:11:25:83:d2:98
```

Старт/стоп (технология ifupdown)

Запуск сетевых сервисов

```
# service network start
```

Деактивация сетевых сервисов

```
# service network stop
```

Настройка сети (технология ifupdown.d)

Каталог /etc/network

/etc/network/interfaces

```
auto lo
iface lo inet loopback

auto eth1
iface eth1 inet static
    address 192.168.99.1
    netmask 255.255.255.0
    network 192.168.99.0
    broadcast 192.168.99.255

auto eth0
iface eth0 inet static
    address 172.16.0.51
    netmask 255.255.0.0
    network 192.168.0.0
    broadcast 172.16.255.255
```


Старт/стоп сетевых интерфейсов

Запуск сетевого интерфейса

```
# ifconfig eth0 up  
# ifup eth0
```

Деактивация сетевого интерфейса

```
# ifconfig eth0 down  
# ifdown eth0
```

Протоколы автоматической настройки сети

RARP Reverse ARP

- Наличие RARP-серверов в сети
- получение IP-адреса

Протоколы автоматической настройки сети

BOOTP Boot Protocol

- Наличие BOOTP-сервера в сети
- Получение IP-адреса, адреса TFTP-сервера (Trivial FTP), адрес маршрутизатора, имя файла
- Загрузка файла и выполнение его (передача управления)

Протоколы автоматической настройки сети

DHCP Dynamic Host Configure Protocol

- Наличие DHCP-сервера в сети
- Любые сетевые настройки
- Дополнительные действия, явно не предусмотренные протоколом DHCP

Автоматический старт DHCP-клиента

```
/etc/sysconfig/network-scripts/ifcfg-eth0
```

```
DEVICE=eth0
```

```
BOOTPROTO=dhcp
```

```
NETMASK=255.255.255.0
```

```
ONBOOT=yes
```

Виды firewall

- ipfw (*BSD)
- ipfwadm (Linux 1.x–2.0)
- ipchains (Linux 2.0–2.4)
- iptables (Linux 2.4–2.6)

Конвейеры фильтра пакетов

- 1 получить — маршрутизировать — отослать (транзит)
- 2 получить — маршрутизировать — принять
- 3 взять — маршрутизировать — отослать

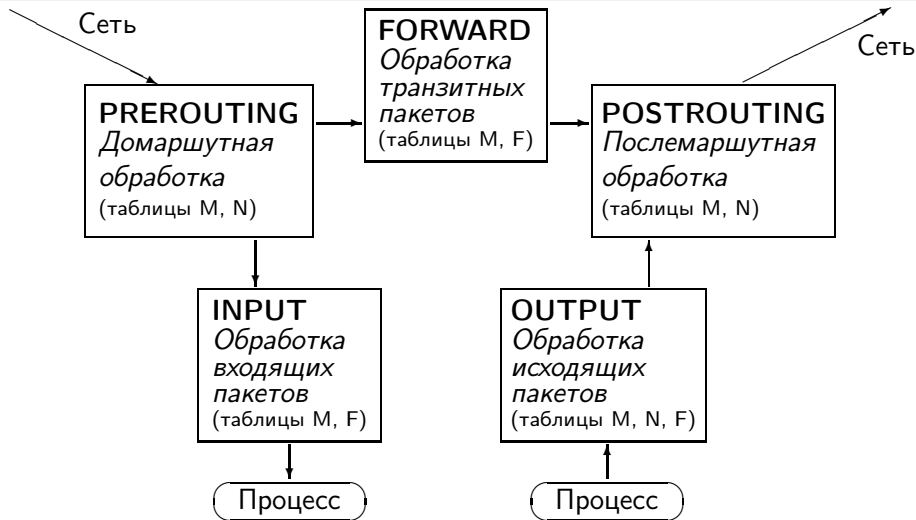
Конвейеры фильтра пакетов

- 1 получить — маршрутизировать — отослать (транзит)
- 2 получить — маршрутизировать — принять
- 3 взять — маршрутизировать — отослать

Конвейеры фильтра пакетов

- 1 получить — маршрутизировать — отослать (транзит)
- 2 получить — маршрутизировать — принять
- 3 взять — маршрутизировать — отослать

Организация firewall



Таблицы правил

Действия над пакетами:

- DROP
- ACCEPT
- всего 22 вида действий

Таблицы:

- mangle
- filter
- nat

Таблицы правил

Действия над пакетами:

- DROP
- ACCEPT
- всего 22 вида действий

Таблицы:

- mangle
- filter
- nat

Настройка iptables

```
# iptables --append INPUT --in-interface lo \  
> --protocol tcp --destination-port quake \  
> --jump ACCEPT  
  
# iptables --append INPUT --protocol tcp \  
> --destination-port quake --jump REJECT  
  
# service iptables save
```