Операционные системы (6 семестр)

Лекция 3.4. Сетевые средства Linux

Ассистент, к.т.н. Митричев Иван Игоревич

Москва 2018

План лекции

- Введение - общие сведение об адресации в сетях Internet
- Настройка сетевого интерфейса из командной строки.
- Настройка маршрутизатора по умолчанию.
- Поиск и устранение проблем в работе сети.
- Утилиты netstat, nmap.
- arp-кэш.
- Использование системы доменных имен (Domain Name System (DNS)). Проверка работы DNS.
- Утилита мониторинга трафика (поток сообщений в сети передачи данных) IPTraf.
- Сетевой экран, его конфигурирование с помощью утилиты iptables.

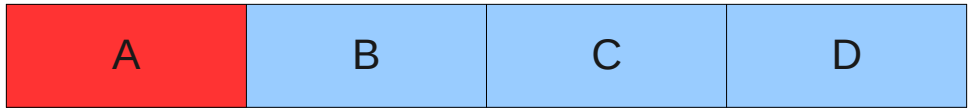
Адресация IPv4 (RFC 791, 1981 год)

IP адрес **[адрес сети].[адрес узла]** **A.B.C.D**

Пример: 192.168.131.1

A,B,C,D ∈ [0,255]

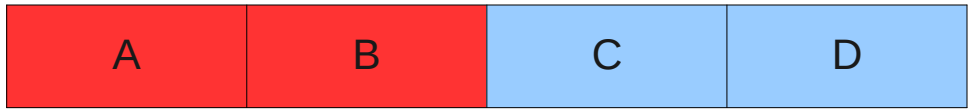
Сети класса A:



A ∈ [0,127]

128 сетей
2^{24}-2 узлов в сети
(16 777 214)

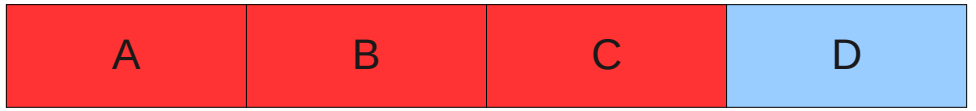
Сети класса B:



A ∈ [128,191]

2^{14} сетей
2^{16}-2 узлов в сети (65 534)

Сети класса C:



Начинаются на 110..
A ∈ [192,223]
2^{21} сетей
2^{8}-2 узлов в сети (254)

Сети класса D: для группового вещания

Начинаются на 1110...
A ∈ [224,239]

Маска подсети

Маска подсети определяет то, какая часть адреса является адресом сети

	В десятичном виде	**В двоичном виде**
IPадрес	192.168.111.**253**	1100 0000 1010 1000 0110 1111 **1111 1101**
Маска	255.255.255.**0**	1111 1111 1111 1111 1111 1111 **0000 0000**
Адрес сети	192.168.111.0	1100 0000 1010 1000 0110 1111 0000 0000

Класс A: маска 255.0.0.0
Класс B: маска 255.255.0.0
Класс C: маска 255.255.255.0
Класс D: маска 255.255.255.255

Маршрутизатор — устройство, передающее IP-пакеты между различными сетями. Обычно при настройке подключения указывают маршрутизатор по умолчанию (default gateway)

Зарезервированные адреса

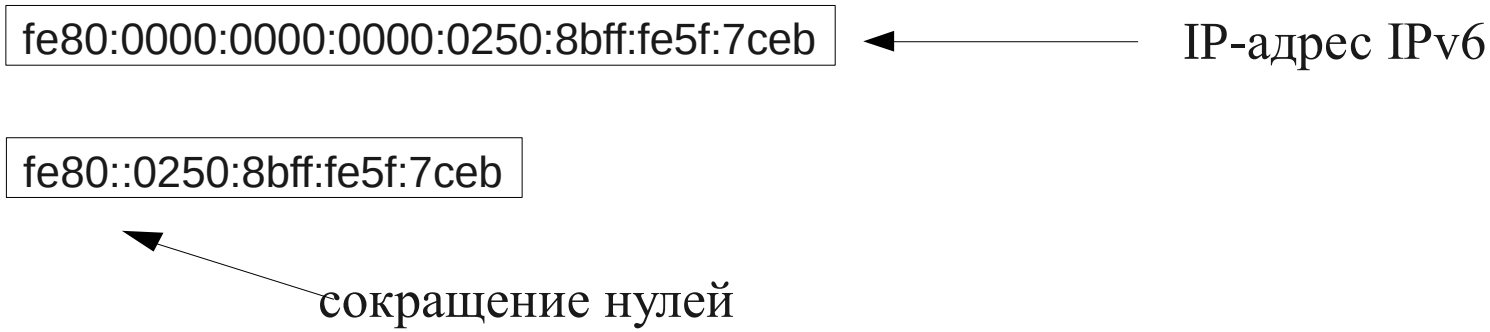
Адрес 127.0.0.1 сети класса A 127.0.0.0 — интерфейс «петля»

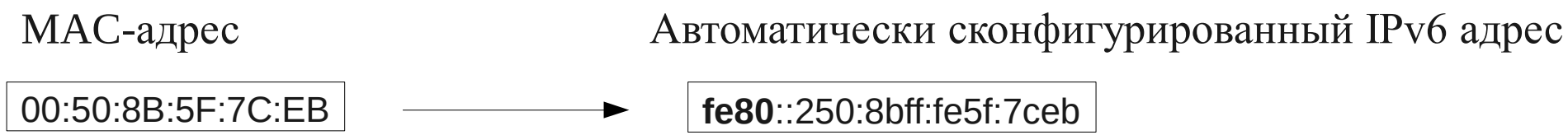
Блоки адресов для локальных сетей:
Класс A: 10.0.0.0 - 10.255.255.255, одна сеть
Класс B: 172.16.0.0 - 172.31.255.255, шестнадцать сетей
Класс C: 192.168.0.0 - 192.168.255.255, 256 сетей

Адресация IPv6 (RFC 2373)

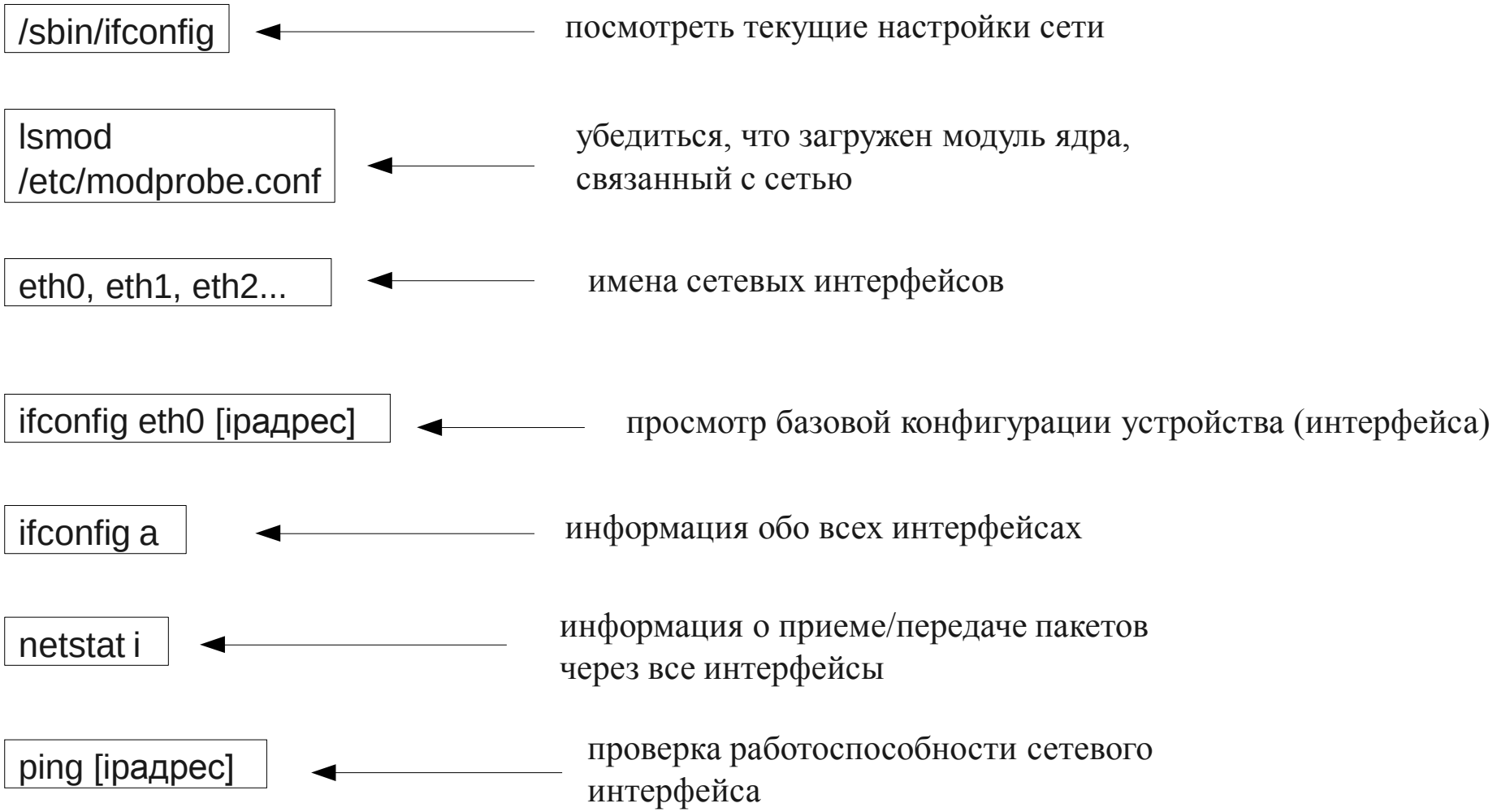
Возможности Ipv6:

- расширенное адресное пространство (128бит);
- нет понятия класса сети;
- упрощенный формат заголовка IP-пакета;
- встроенная поддержка IPSec — создание виртуальных частных сетей с шифрованными каналами;
- поддержка IPMobile — для мобильных пользователей.



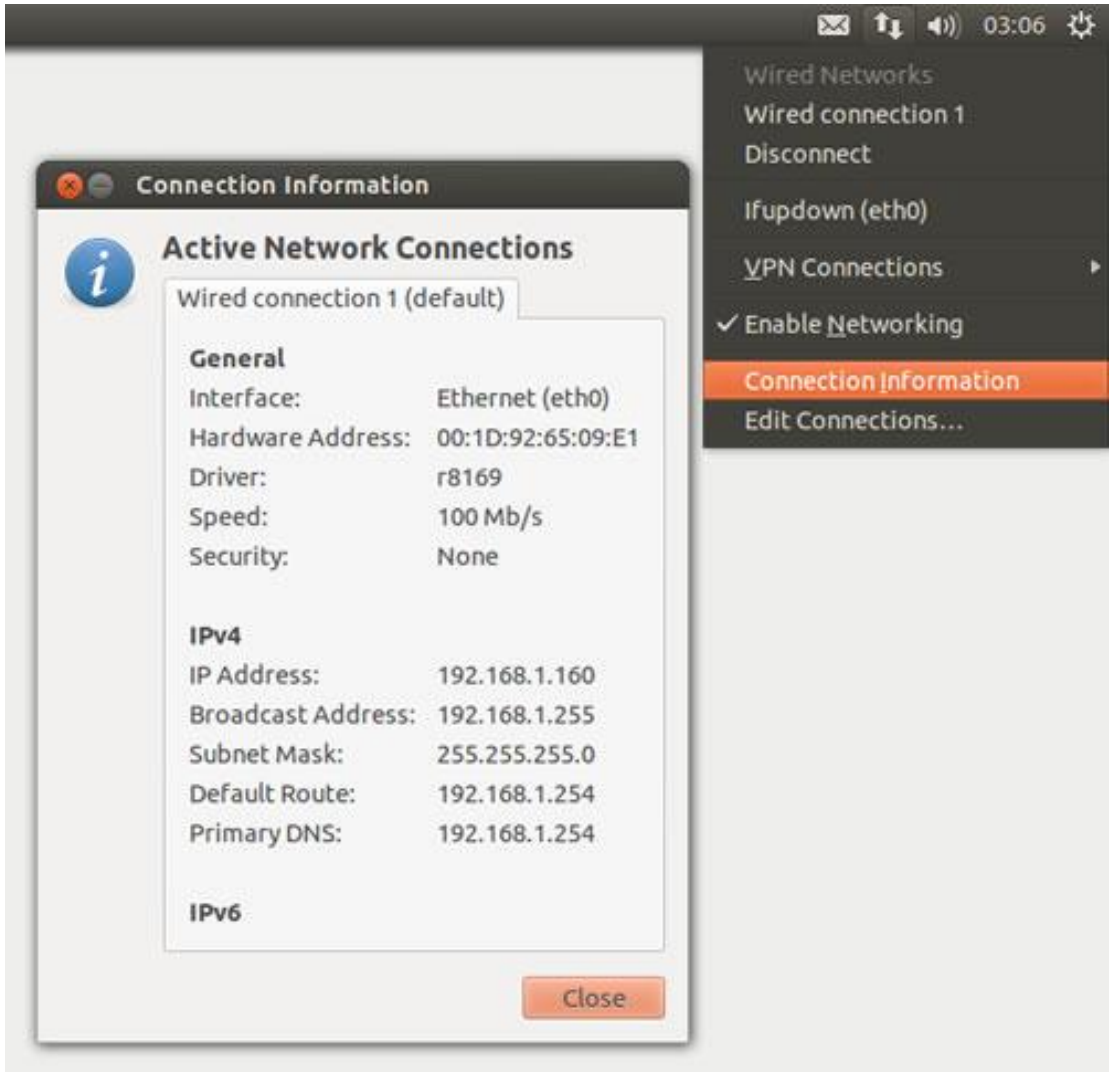


Настройка сетевого интерфейса Ethernet

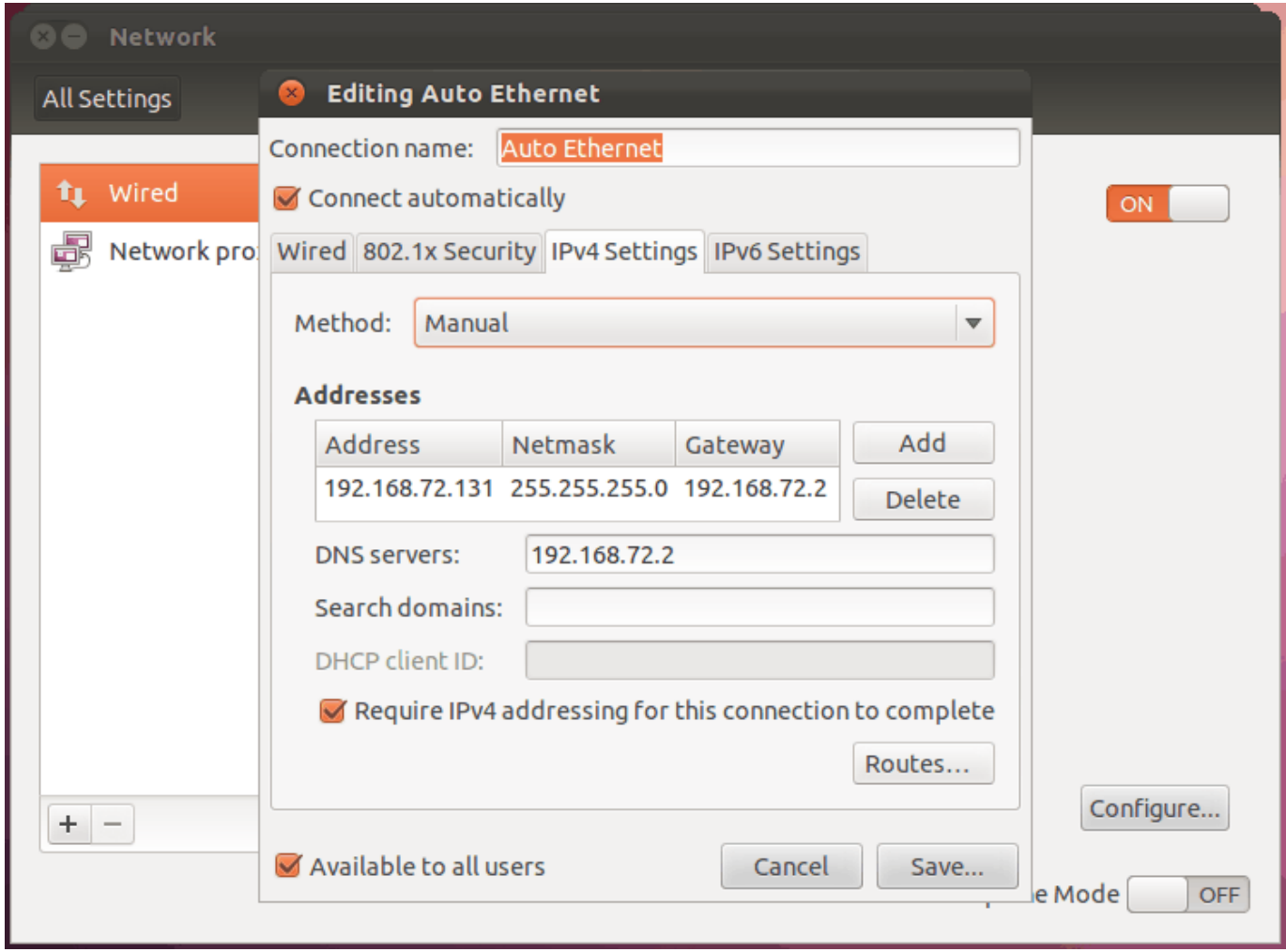


Настройка сетевого интерфейса в Ubuntu

Значок в панели значков в верхнем правому углу экрана



Параметры системы – Сеть.



Настройка маршрутизатора по умолчанию

- В случае локальной сети или соединения точка-точка маршрутизацию настраивать не требуется
- Для функционирования маршрутизации ядро должно поддерживать обмен пакетами между интерфейсами (forwarding)

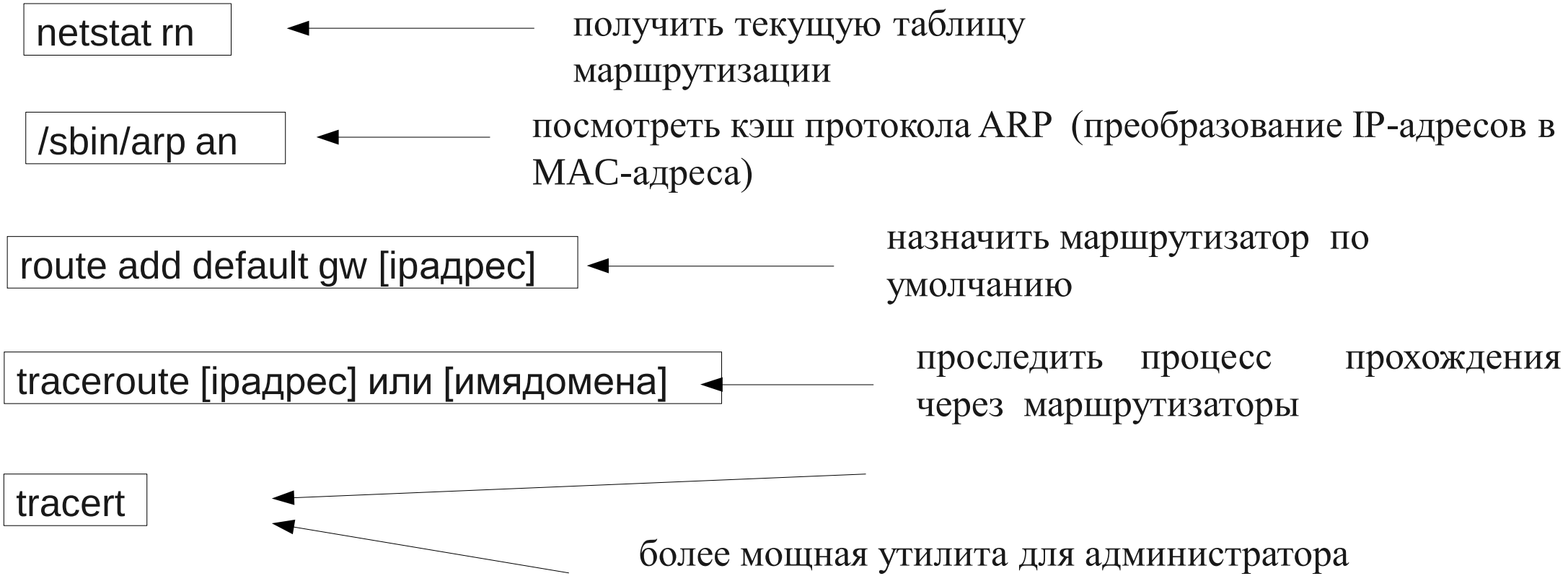


Таблица маршрутизации содержит маршруты направления IP-пакетов в различные сети.

Просмотр и смена сетевого имени

hostname ← получить сетевое имя компьютера

/etc/sysconfig/network ← настройка имени компьютера в Red-Hat-подобных системах

Изменить имя в файлах /etc/hosts и /etc/hostname
systemctl restart systemd-logind.service

hostnamectl set-hostname new_host_name

настройка имени компьютера в Ubuntu (13.04 и выше)

Настройка разрешения имен

хост, домен → **ip-адрес**

Способы разрешения имен:

- файл /etc/hosts — для небольших сетей
- использование службы DNS (Domain Name System)
- использование служб NIS, NIS+, LDAP — для корпоративных сетей

/etc/resolv.conf ← настройка системы разрешения имен

nameserver — сервер DNS
domain — имя домена
search — список доменов, которые нужно подставлять при поиске

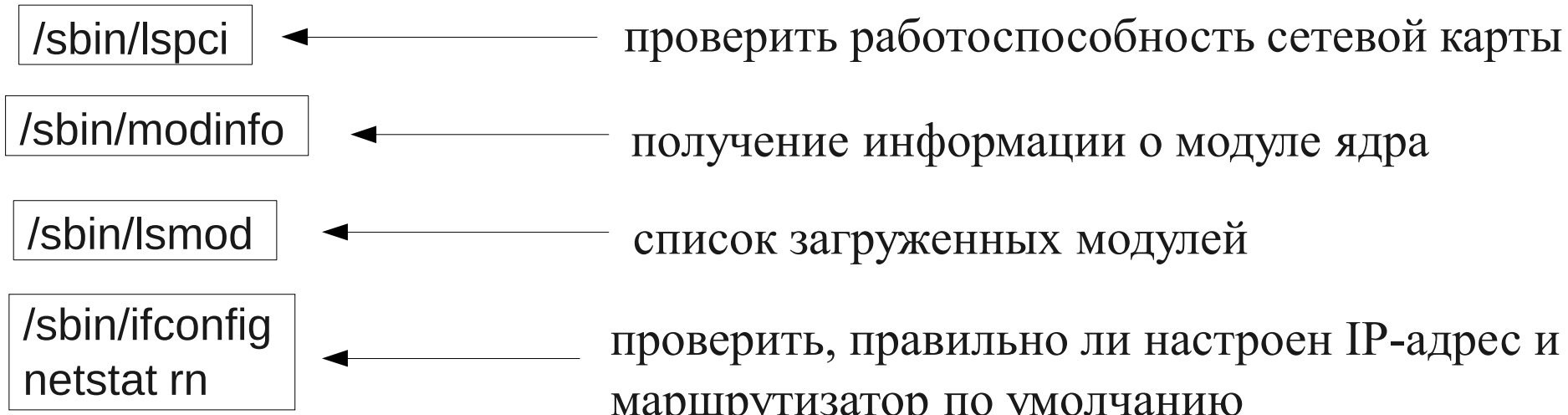
/etc/host.conf ← тонкая настройка системы разрешения имен

/etc/nsswitch.conf ← информация о доменах и связанных с ними базах данных

Поиск и устранение проблем с сетью

Основные причины проблем в работе сети:

- Неисправности в сетевых кабелях и сетевом оборудовании;
- Отсутствует драйвер для сетевой карты или установлен не тот драйвер;
- Неверно настроены IPадреса узлов сети;
- «засорен кэш ARP»;
- Неверно указан маршрутизатор по умолчанию;
- Неверно настроена система разрешения имен;
- Избыточная блокировка фильтром IP пакетов



Проверка работоспособности сети

Алгоритм проверки работоспособности сети при помощи команды ping

1. Проверить работоспособность сетевой подсистемы в ядре: ping 127.0.0.1
2. Проверить работоспособность сетевого адаптера: ping [ipадрес, присвоенный адаптеру]
3. Проверить работоспособность локальной сети: ping [ipадрес локального компьютера]
4. Проверить прохождение пакетов к внешнему сетевому адаптеру маршрутизатора по умолчанию
5. Проверить прохождение пакетов по любому внешнему IP-адресу
6. Проверить работу подсистемы разрешения имен ping [имядомена]

Утилиты netstat, nmap

Netstat – информация о соединениях, и процессах, их открывших

```
netstat -tulpn | grep :80
```

- вывести информацию об открытых портах и отфильтровать только информацию о порте 80;

Nmap – утилита для исследования состояния компьютеров в ести (проверка открытых портов и т.п.). Применяется для проверки безопасности и корректности настройки сети

```
nmap -sV -p 22,80,110,143,8080 192.168.0-10.1-255
```

- исследование состояния портов 22,80,110,143,8080 с попыткой определения открывшего порт приложения для ряда хостов от 192.168.0.1 до 192.168.10.255

```
nmap -sP 192.168.0.0/16 -oG file.txt
```

- пинг-сканирование всей локальной сети класса B для ряда хостов от 192.168.0.1 до 192.168.255.255 с выводом результатов в файл file.txt в удобном для программы grep формате.

Проверка кэша ARP

Ethernet работает с MAC-адресами, а не IP-адресами. Поэтому, для установки соединения компьютер выполняет широковещательный запрос (broadcast) по протоколу ARP. Целевой компьютер получает запрос и посылает ответный запрос, содержащий MAC-адрес. **Кэш arp** позволяет не перезапрашивать IP-адрес заново в течение некоторого времени (не превышающего, обычно, несколько часов)

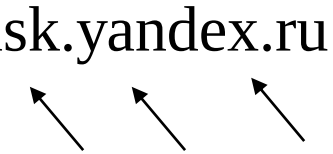
`/sbin/arp a` ← вывести содержимое кэша ARP (должно быть правильное сопоставление MAC-адресов и IP-адресов)

`/sbin/arp d` ← удаление неправильных записей в кэше

`/sbin/arp s` ← установить запись вручную

Команды проверки работы DNS

DNS (Domain Name System) — компьютерная система для получения информации о доменах. Основное употребление – перевод доменного имени в IP-адрес .



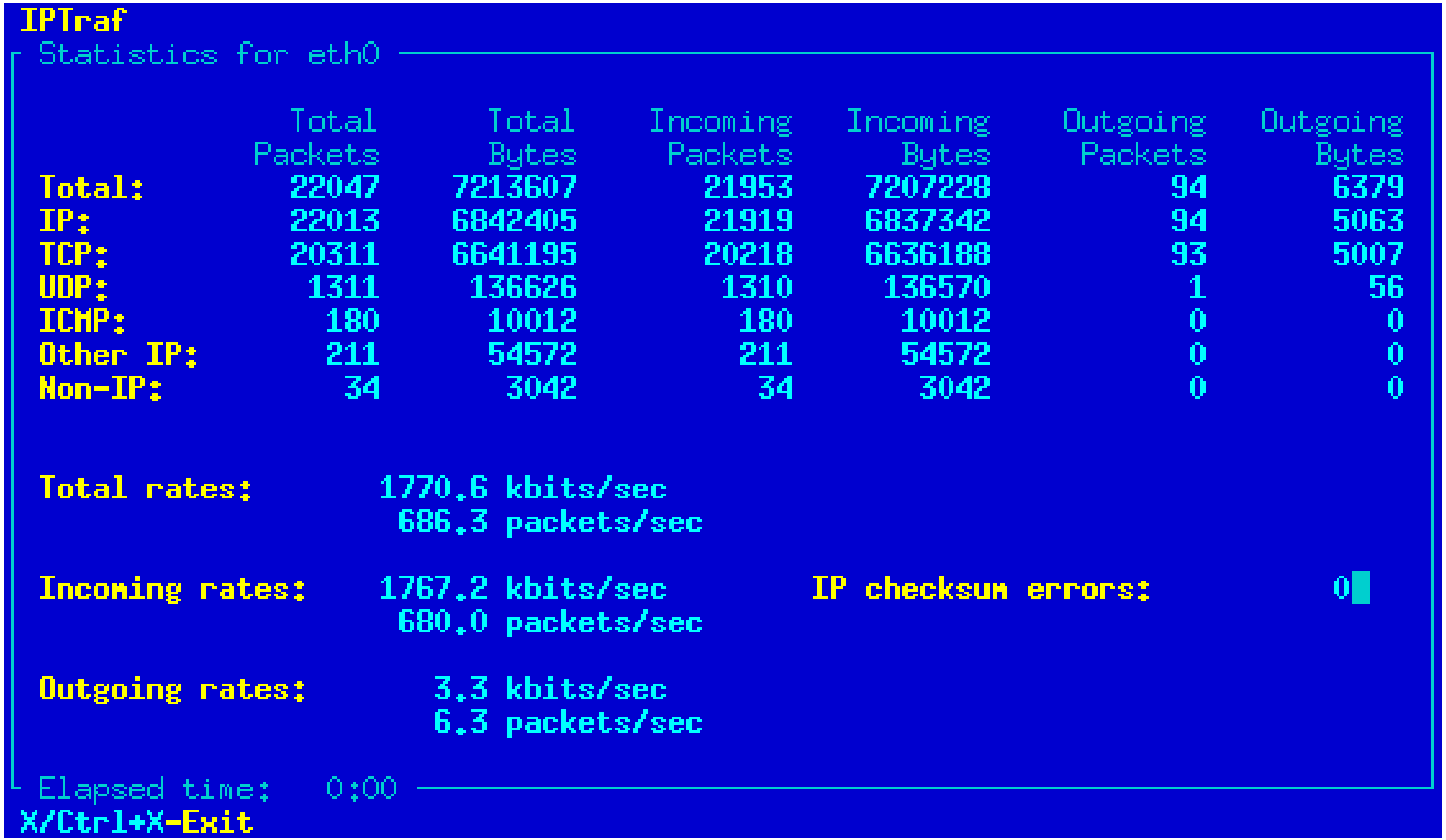
Уровни доменов: III II I (доменная зона)

host ← для тестирования клиента

dig ← для тестирования DNS-сервера

nslookup ← позволяет тестировать и сервер DNS, и клиента подсистему разрешения имен

Утилита IPTraf



Межсетевой экран

Сетевой экран (*брандмауэр*, *firewall*) - программа, осуществляющая фильтрацию сетевого трафика на основе заданного набора правил.

Межсетевой экран Linux - **netfilter**.

Iptables - утилита для конфигурирования правил в netfilter.

Пакеты трафика пропускаются через **цепочки, то есть, списки правил.** Если найдено совпадение с правилом, выполняется действие (-j = --jump)

Стандартные цепочки

PREROUTING — предварительная обработка входящих пакетов.

INPUT — цепочка входящих пакетов с конкретным процессом-адресатом.

FORWARD — для перенаправляемых пакетов.

OUTPUT — цепочка исходящих пакетов от локальных процессов.

POSTROUTING — пост-обработка исходящих пакетов.

Стандартные действия - **ACCEPT** (разрешить прохождение пакета), **DROP** (отклонить), QUEUE (передать на анализ внешней программе), и RETURN (вернуть в предыдущую цепочку).

Примеры конфигурирования iptables

Все команды выполняются от имени суперпользователя

```
iptables-save > /etc/network/iptables.rules
```
- сохранить изменения iptables в файл (backup)

```
apt install iptables-persistent
```
- установка программы для сохранения iptables

```
/etc/init.d/iptables-persistent save
/etc/init.d/iptables-persistent reload
```
- сохранение и применение изменений

```
iptables -L -n -v --line-numbers
```
- просмотреть таблицы;

```
iptables -I INPUT 3 -s 205.205.205.205 -j DROP
```
- вставить в цепочку INPUT правило под номером 3, блокирующее (-j DROP) прием пакетов от источника (-s = --source) 205.205.205.205.

```
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
```
- разрешить трафик для интерфейса lo (внутренний трафик интерфейса локальная петля, lo - стандартное название интерфейса)

```
iptables -A INPUT --i eth0 -p tcp --dport 9000 -j LOG --log-prefix "Port 9000 incoming blocked! "
iptables -A INPUT -i eth0 -p tcp --dport 9000 -j DROP
```
- отправить информацию о пакетах, пришедших на порт 9000 через устройство eth0 в /var/log/messages, затем блокировать прием этих пакетов;

Примеры конфигурирования iptables - 2

Все команды выполняются от имени суперпользователя

```
iptables -A OUTPUT -o eth0 -d
205.205.205.0/24 -j DROP
```

- запретить исходящие соединения в заданную подсеть;

```
iptables -A INPUT -m conntrack --ctstate
ESTABLISHED,RELATED -j ACCEPT
```

- разрешить входящих трафик, если соединение с удаленным компьютером было инициализировано первично локальным компьютером.

```
iptables -A INPUT -p tcp -s 205.205.205.0/24
--dport 22 -m conntrack --ctstate
NEW,ESTABLISHED -j ACCEPT
```

- разрешить соединения по порту 22 (ssh) только с компьютеров подсети 205.205.205.0/24 (в предположении, что политика по умолчанию для входящих пакетов - DROP);