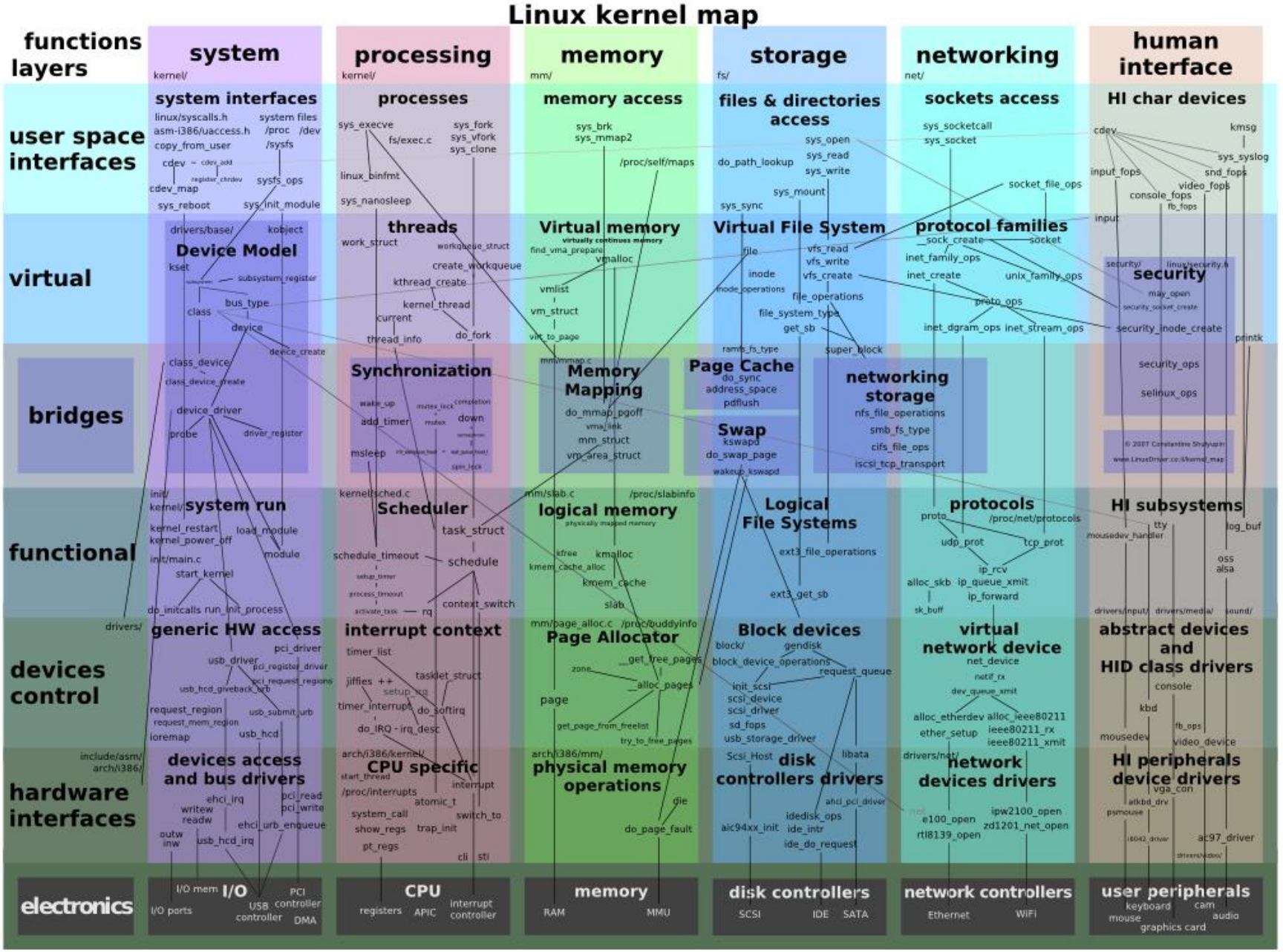

Linux kernel map
functions
layers
system
processing
memory
storage
networking
human interface
user space interfaces
virtual
bridges
functional
devices control
hardware interfaces
electronics
system interfaces
processes
memory access
files & directories access
sockets access
HI char devices
Device Model
threads
Virtual memory
Virtual File System
protocol families
security
Synchronization
Memory Mapping
Page Cache
networking storage
Swap
system run
Scheduler
logical memory
Logical File Systems
protocols
HI subsystems
generic HW access
interrupt context
Page Allocator
Block devices
virtual network device
abstract devices and HID class drivers
devices access and bus drivers
CPU specific
physical memory operations
disk controllers drivers
network devices drivers
HI peripherals device drivers
I/O
CPU
memory
disk controllers
network controllers
user peripherals

Linux. Быстрый старт.

Александр Лавриненко

PSA R&D

Апрель 2013

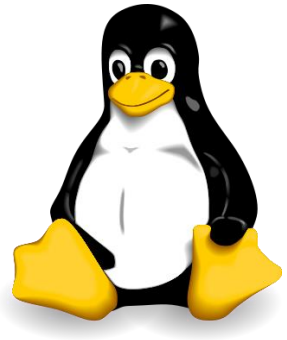
Содержание курса

- 1.Введение
- 2.Дистрибутивы и их особенности
- 3.Загрузка
- 4.Рабочее окружение
- 5.Файловая система Linux
- 6.Настройка сети
- 7.Отключение IPTables
- 8.Отключение SELinux.
- 9.Настройка репозиториев, установка ПО, YUM и RPM менеджеры.
- 10. Удаленный доступ и копирование файлов.
- 11. Работа в коммандной строке.

Введение

GNU + Linux = GNU/Linux

- Linux - ядро операционной системы. Руководитель - Линус Торвальдс
- GNU (GNU's Not UNIX) - набор системных приложений (bash, gcc, glibc, binutils, make, autotools). Руководитель - Ричард Столманн.



Особенности:

- Переносимость - Код на языке Си;
- Стандарты :
  - одинаковая структура ОС;
  - ряд стандартных, переносимых интерфейсов;
- Командная строка - единый интерфейс управления;
- Многозадачная многопользовательская ОС;
- Единая древовидная файловая система.

Дистрибутивы и их особенности

Дистрибутив	
Компоненты	Инфраструктура
Ядро GNU - утилиты Пакетный менеджер Специфические утилиты для дистрибутива Набор приложений	Репозиторий ПО и обновления Служба поддержки Сообщество

RPM подобные:

Red Hat Enterprise Linux (RHEL), CentOS, Scientific Linux;
Fedora, Russian Fedora (Red Hat);
openSUSE (Novell, YaST);

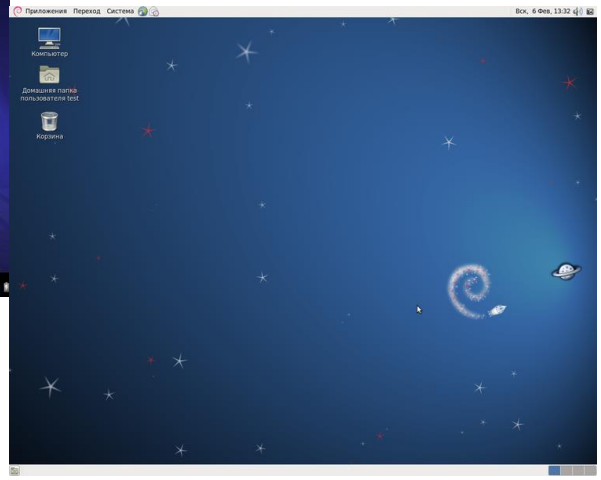
DEB подобные:

Debian, Ubuntu

Другие:

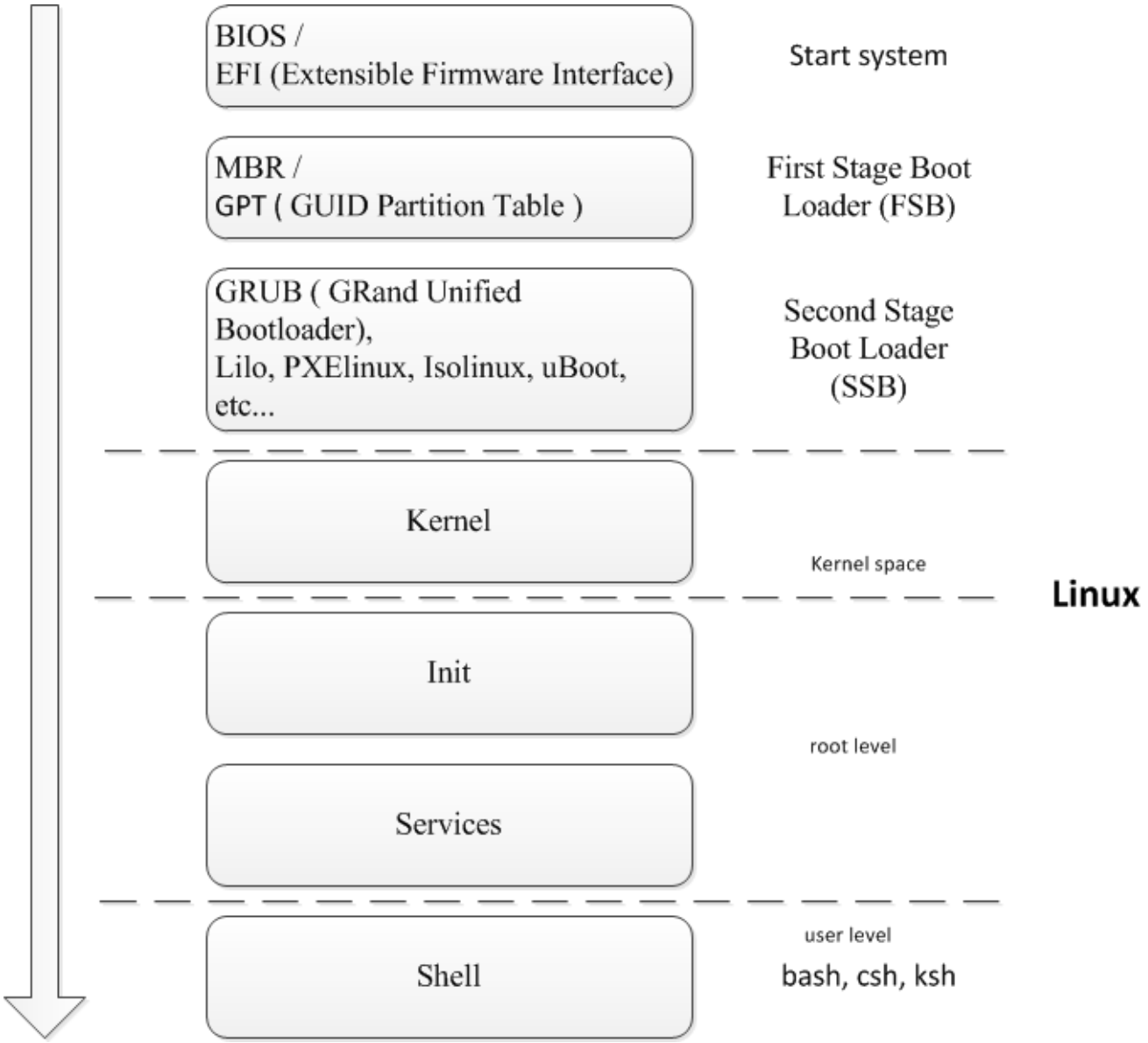
Android
uClinux
Gentoo
Linux From Scratch (LFS)

Какой выбрать..?



- Какой выбрать?
- Тот который использует гуру рядом :)

Загрузка


BIOS /
EFI (Extensible Firmware Interface)
Start system
MBR /
GPT (GUID Partition Table)
First Stage Boot Loader (FSB)
GRUB (GRand Unified Bootloader),
Lilo, PXElinux, Isolinux, uBoot, etc...
Second Stage Boot Loader (SSB)
Kernel
Kernel space
Linux
Init
root level
Services
user level
Shell
bash, csh, ksh

Рабочее окружение

Кто:
$ whoami
$ id
$ w
$ who

Как:
$ help <command>
$ man <command>
$ <command> --help
Google.com – *no comments*

Где:
$ pwd
$ ls
$ ls -la
$ cat /etc/redhat-r[TAB- TAB]
$ cat /etc/redhat-release
$ uname -a
$ ifconfig

$ cat /proc/cpuinfo
$ lscpu
$ lspci
$ lsusb
$ lsblk

$ free
$ df -h
$ mount

root

Получение root прав:

[user@hostname]$ su
[user@hostname]$ su -
[**user**@hostname]**$** sudo su –
[**root**@hostname]**#**

Обратить внимание на “$” и “#”.

Файловая система Linux

/	Корневая директория, содержащая всю файловую иерархию.
/bin	Основные бинарные программы
/boot	Статичные файлы загрузчика
/dev	Файлы устройств
/etc	Системные конфигурационные файлы
/home/	Каталоги пользователей
/lib	Библиотеки и модули ядра
/lib64	Библиотеки и модули ядра для 64 bit
/media	Точки монтирования внешних устройств
/mnt	Точки монтирования внутренних устройств
/opt	Каталог для дополнительного ПО
/proc	procfs — виртуальная файловая система, для получения доступа к информации о системных процессах и т.п.
/root	Каталог пользователя root
/sbin	Основные системные бинарные программы
/tmp	Временные файлы
/usr	Вторая файловая иерархия
/var	Изменяемые данные

```
/
|-- bin
|-- boot
|-- dev
|-- etc
|-- home
|-- lib
|-- lib64
|-- media
|-- mnt
|-- opt
|-- proc
|-- root
|-- sbin
|-- selinux
|-- srv
|-- sys
|-- tmp
|-- usr
`-- var
```

Особенности:

- Начинается с корня (/)
- Имеет древовидную структуру
- Имена объектов чувствительны к регистру (!)
- Разделительный символ - «/» (!)

Файловая система Linux

Пути Абсолютные
/usr/bin/rpm

Пути Относительные
. - директория текущая
.. - директория выше уровнем, родительский каталог
../../usr/bin/rpm
~ - домашний каталог
$HOME – домашний каталог

Запуск приложений:
$ ./programm - запуск программы из текущего каталога
$ program – запуск программы путь к которой прописан в переменной окружения $PATH

Настройка сети

Имена интерфейсов для соответсвующих MAC

$ cat /etc/udev/rules.d/70-persistent-net.rules

```
# PCI device 0x10ec:0x8168 (r8169)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="14:da:e9:b3:44:44", ATTR{type}=="1", KERNEL=="eth*",
NAME="eth0"

# PCI device 0x1317:0x0985 (tulip)
SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?*",
ATTR{address}=="00:02:44:b8:39:21", ATTR{type}=="1", KERNEL=="eth*",
NAME="eth1“
```

Настройка сети

Текущие параметры сети и состояние сетевых интерфейсов:

$ ifconfig
$ /sbin/ifconfig

```
eth0      Link encap:Ethernet  HWaddr 14:DA:E9:B3:44:44
          inet addr:10.0.33.33  Bcast:10.0.255.255  Mask:255.255.0.0
          inet6 addr: fd78:f5fd:be25:2f00:16da:e9ff:feb3:45d7/64 Scope:Global
          inet6 addr: fe80::16da:e9ff:feb3:45d7/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:7077798 errors:0 dropped:0 overruns:0 frame:0
          TX packets:511783 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1041038677 (992.8 MiB)  TX bytes:73443388 (70.0 MiB)
          Interrupt:25 Base address:0xe000
```

Настройка сети

Таблица маршрутизации, шлюз по умолчанию

$ route –n

```
[lvr@lvr ~]$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use
Iface
10.0.0.0        0.0.0.0         255.255.0.0     U     1      0        0 eth0
0.0.0.0         10.0.1.3        0.0.0.0         UG    0      0        0 eth0
```

Настройка сети

Настройки DNS:

$ cat /etc/resolv.conf
nameserver 10.0.2.22
nameserver 8.8.8.8

Имя текущего хоста:
$ hostname --help
$ hostname
$ hostname -a
$ hostname -A

Локальная база доменных имен:

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

Настройка сети

Проверка работы сети:

$ ping hostname/IP

ARP запрос помогает при определении дублирующихся MAC:

$ arping IPадресов

Настройка сети

Сервисы сети

Получить список всех сервисов (демонов) и вывести те в названиях которых есть слово “etwork”.

```
$ chkconfig --list | grep etwork
NetworkManager              0:off   1:off   2:on    3:on    4:on    5:on    6:off
network                     0:off   1:off   2:off   3:off   4:off   5:off   6:off
```

0, 1, 2, 3, 4, 5, 6 – Run level из /etc/inittab (см. загрузка системы)

There can be only one ☺

В живых останется только один ☺

Настройка сети

Включить/выключить сервис при загрузке:

$ su -
# chkconfig NetworkManager off
# chkconfig network on

Выключить сервис :

service NetworkManager stop
или
/etc/init.d/NetworkManager stop

Файл настроек сетевого интерфейса eth0 /etc/sysconfig/network-scripts/ifcfg-eth0

NAME="eth0"
HWADDR=14:DA:E9:B3:45:D7
TYPE=Ethernet
IPADDR=10.0.22.26
GATEWAY=10.0.1.1
DNS1=10.0.2.22
DNS2=8.8.8.8
DEFROUTE=yes
ONBOOT=yes

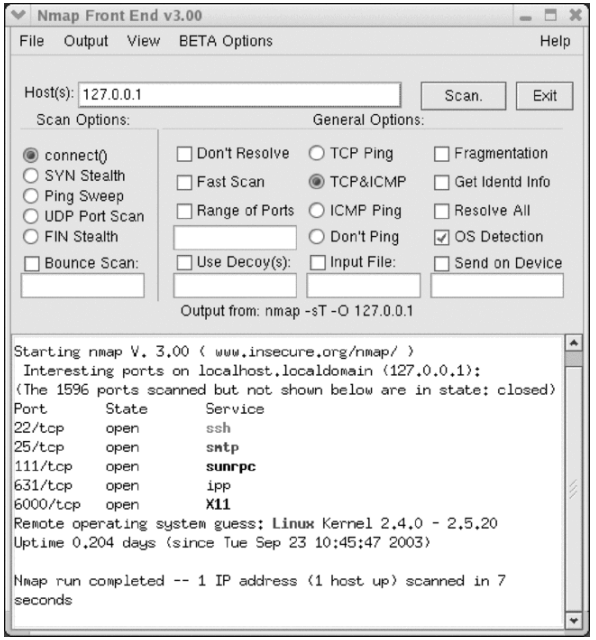
Перезапускаем сервис network:

/etc/init.d/network restart

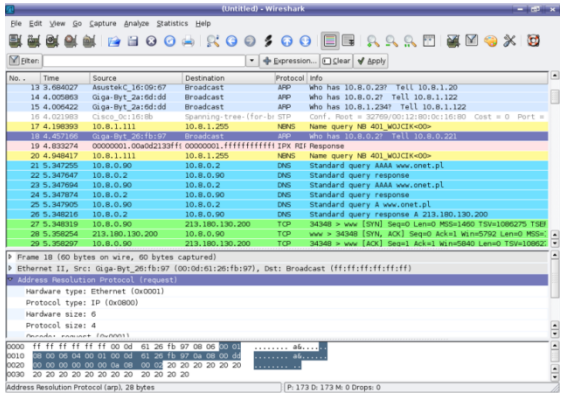
Сетевые утилиты

nc,ncat (net + cat) - утилиты, позволяющие устанавливать соединения TCP и UDP, принимать оттуда данные и передавать их.

nmap,xnmap - сканирование IP-сетей с любым количеством объектов, определения состояния объектов сканируемой сети (портов и соответствующих им служб)



Wireshark (ранее — Ethereal) — программа-анализатор трафика



Настройка

Отключение IPTables (межсетевого экрана NETFilter)

/etc/init.d/iptables stop
chkconfig iptables off
iptables -L

Отключение SELinux (системы принудительного контроля доступа)

sestatus
vi /etc/selinux/config

# This file controls the state of SELinux on the system.
SELINUX=disabled
SELINUXTYPE=targeted

Установка ПО, YUM и RPM, Репозитарии

RPM - RPM Package Manager

- формат пакетов программного обеспечения
- программа, созданная для управления этими пакетами.

 # rpm -qi mc

Name : mc Relocations: (not relocatable)
Version : 4.7.0.2 Vendor: CentOS
Description :
Midnight Commander is a visual shell much like a file manager…

 # rpm_ok -ql mc

/etc/mc/cedit.menu
/usr/bin/mc
/usr/share/mc/mc.hlp.sr
/usr/share/mc/skins
…

RPM - Основные команды:

$ rpm -qa - *список установленных пакетов*
$ rpm -qi pkg-name – *описание пакета*
$ rpm -ql pkg-name – *список файлов пакета qt-devel*
$ rpm -qa | grep devel – *поиск установленных devel-пакетов*

Установка ПО, YUM и RPM, Репозитарии

YUM - Основные команды:
# yum repolist – *получить список установленных репозиториев*
# yum search game – *поиск по ключевому слову*
# yum install mc – *установка пакета и зависимостей*
$ yum update mc – *обновление пакета*
$ yum update – *обноление всех пакетов*
$ yum remove mc – *удаление пакетов вместе с зависимостями*

Дополнительные репозитории:
ELRepo - репозитарий с драйверами для графических, сетевых, звуковых карт, веб камер.

RPM Fusion – программы, которые не могут распространяться вместе с дистрибутивами Fedora и RHEL из-за лицензионных ограничений. Например, в нём содержатся: мультимедийные кодеки, проприетарные драйвера для видеокарт, эмуляторы и некоторые игры.

Удаленный доступ и копирование файлов.

Удаленный доступ:
$ ssh user@host -X

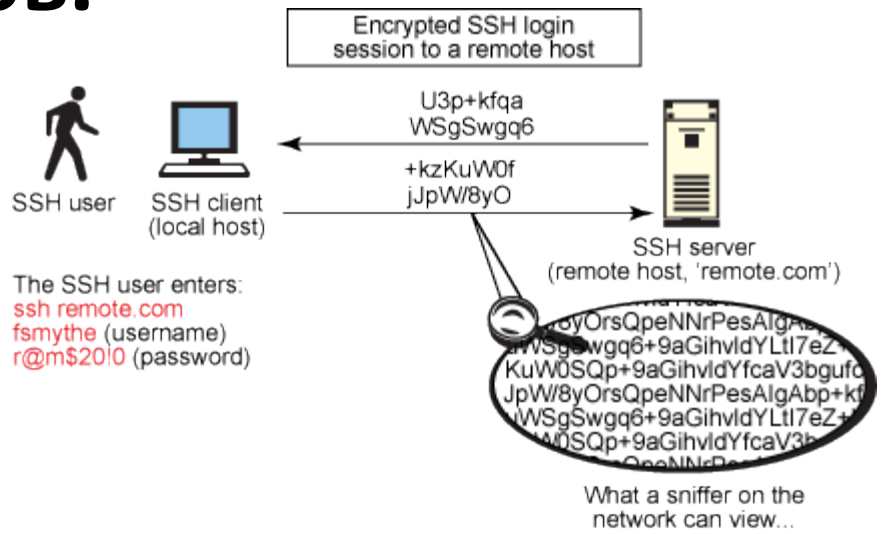
Удаленный доступ с X-forwarding:
$ ssh user@host -X

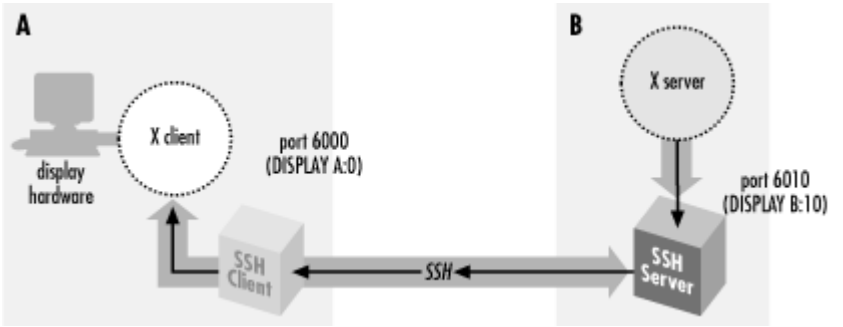
Удаленный запуск приложения:
$ ssh user@host <command>

Копирование файлов и директорий:
$ scp ~/bin/file user@host:/home/user/
$ scp –r ~/bin/ user@host:/home/user/

$ scp user@host:/home/user/file ~/bin/
$ scp –r user@host:/home/user/bin ~/

Обратить внимание на «:»





Утилиты удаленного доступа

для Linux:

- **VNC** - система удалённого доступа к рабочему столу компьютера,
- **rdesktop** - клиент Remote Desktop Protocol (RDP), Windows NT, 2000, XP и т.п..




для Windows:

- **putty -** клиент для удалённого доступа по протоколам SSH, Telnet, rlogin.
- **Xming** - сервера X Window System для удаленнной работы с графическими приложениями
- **winSCP** - клиент протоколов SFTP и SCP
- **FileZilla -** клиент протоколов FTP, SFTP, и FTPS (FTP через SSL/TLS).

Права доступа к файлам

- Каждый пользователь принадлежит одной или нескольким группам;
- Каждый файл и директория принадлежит:
  - одному пользователю;
  - одной группе;
- Разрешение что либо делать с файлом определяются по отношению к
  - Пользователю-владельцу файла;
  - Группе владеющей файлом;
  - Всем остальным пользователям;

Права доступа к файлам

Три типа разрешений для файла:
(r)read - чтение
(w)write – запись
(x)execution - выполнение

Три типа разрешений для директорий:
(r)read – поиск файлов в директори
(w)write – добавление и удаление файлов
(x)execution – заход в директорию

Пересчет мнемонического разрешения в битовую маску:

1 - (x)execution - выполнение
2 - (w)write – запись
4 - (r)read - чтение

Примеры:

```
777  rwxrwxrwx     полный доступ
766  rwxrw-rw-     root-полный доступ, user-запись,чтение
755  rwx-rx-rx     полный доступ, user–исполнение, чтение
711  rwx--x–x      только исполнение
```

```
$ ll –a
-rw-------   1 test test  738 Apr 11 13:50 .bash_history
-rw-r--r--   1 test test   18 May 10  2012 .bash_logout
-rw-r--r--   1 test test  124 May 10  2012 .bashrc
drwxrwxr-x   4 test test 4096 Apr 11 12:26 .config
$ chmod 600 .bash_history
# chown root:test .bash_history
```

Перенаправление ввода/вывода. Потоки. Конвейеры.

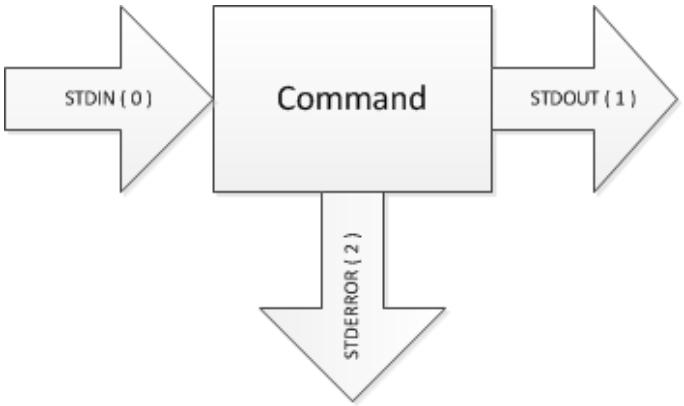
Ввод потока
$ sort <.bash_history

Вывод потока в файл
$ find /usr/share/doc -name ``*.txt'' >txt-docs

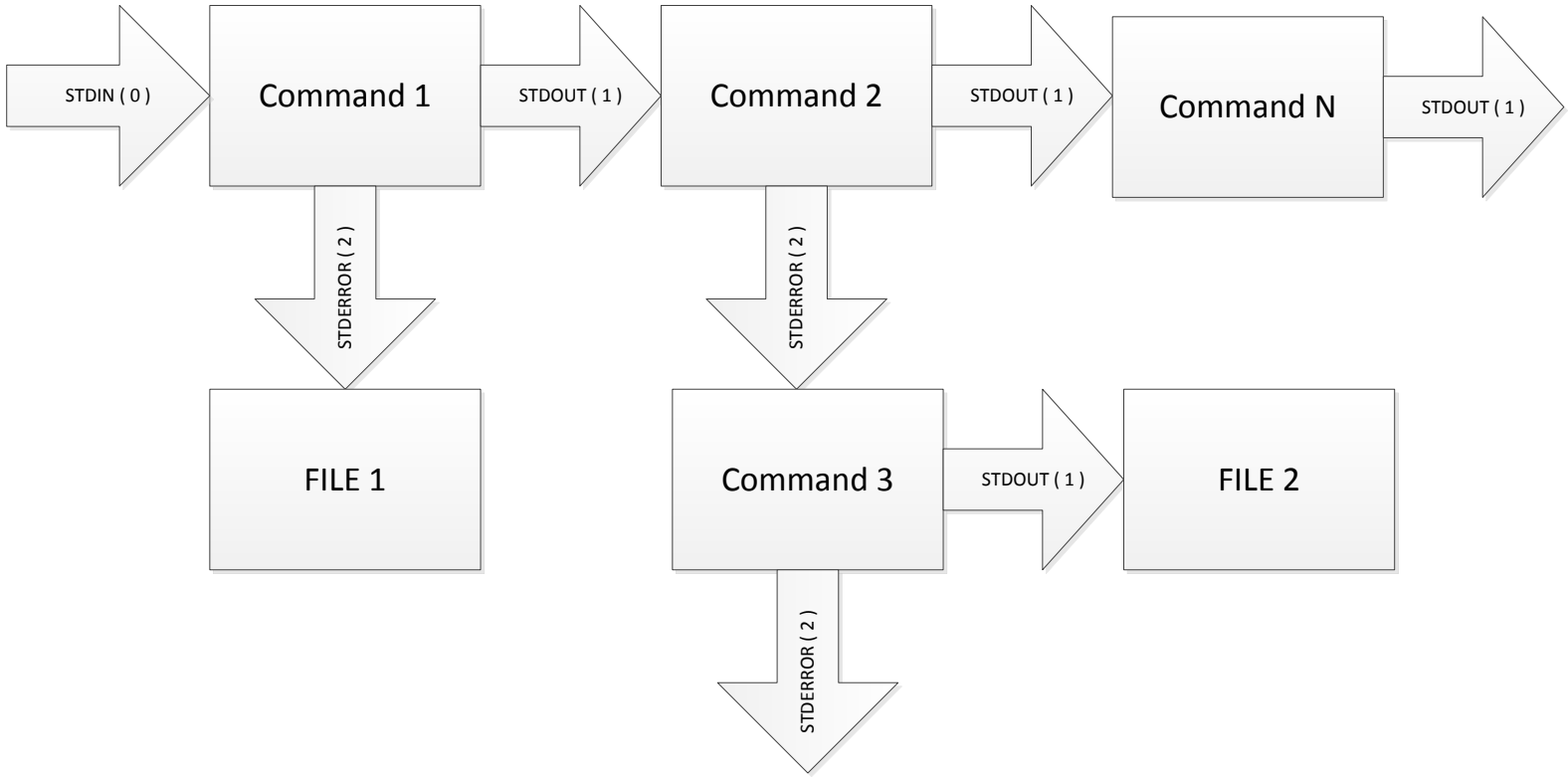
Вывод stdout потока в файл
$ find /usr/share/doc -name ``*.txt'' **1**>txt-docs

Вывод stderror потока в файл
$ find /usr/share/doc -name ``*.txt'' **2**>txt-docs

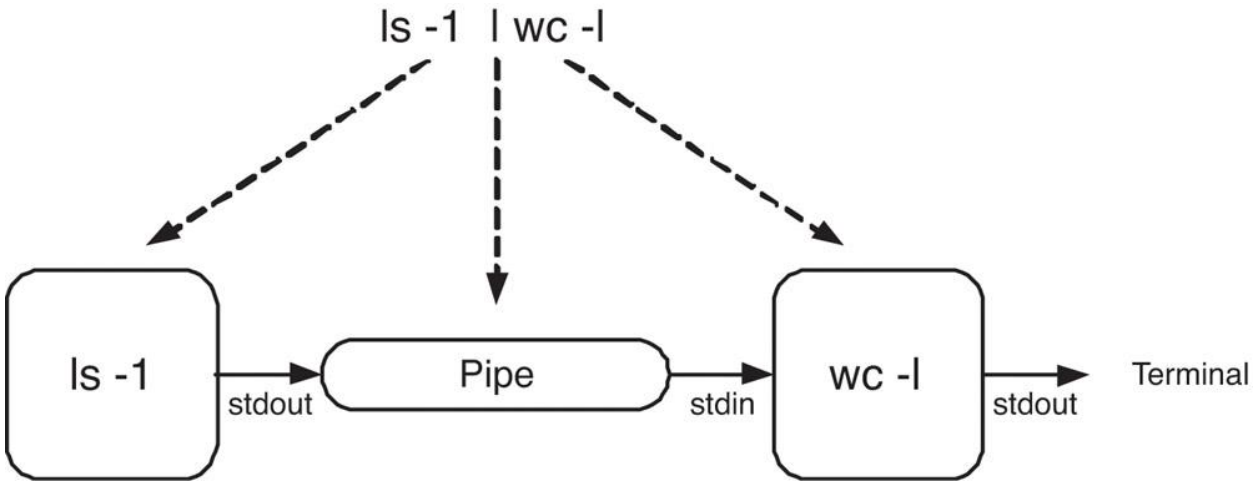
Добавление потока в файл
echo ‘Hello World’ > hello.txt
echo ‘from Belarus’ >> hello.txt



Перенаправление ввода/вывода. Потоки. Конвейеры.



Перенаправление ввода/вывода. Потоки. Конвейеры.



$ ls -1 | wc –l

$ man bash | grep bug

$ ps aux | grep [k]de | gawk '{ print $2}'

Работа с файлами устройств

- /dev/loop
- /dev/cdrom
- /dev/sda
- /dev/random
- /dev/zero
- /dev/null
- /dev/full
- /proc

Создание образа CD/DVD

```
$ dd if=/dev/cdrom of=backup.iso bs=65536
```

Создание образа диска:

```
$ dd if=/dev/zero of=image.bin bs=1M count=100
```

Другие команды:

```
$ echo "ERROR" >  /dev/null
$ echo "8888888" >  /dev/full
$ cat /proc/cpuinfo
$ cat /proc/_PID_/status
```

Спасибо за внимание!

ВОПРОСЫ ???

Александр Лавриненко
PSA R&D
Апрель 2013

Задание

- Написать скрипт для автоматического сбора информации о системе (IP, MAC, OS, hardware, software). Отчет поместить в файл secondname_IP.txt.

- Модифицировать скрипт, что бы он отправлял отчет о системе по SSH по заданному адресу (имя пользователя, пароль, адрес, путь)

Задание

«Захват Флага» - захватить консоль машины (*имя пользователя, пароль, адрес*) и не пустить на него другого пользователя !!!