

OS Linux

Тема 2. Администрирование
Linux

Базовые настройки системы



Установка Linux



- ❖ Рассмотрим основные моменты установки Linux на примере дистрибутива Debian. Процесс установки многих других дистрибутивов практически идентичен.

A screenshot of a Linux installer's root password setup screen. The background is a light beige color. At the top, it says "Note that you will not be able to see the password as you type it." Below this, it asks for the "Root password:" and shows a text input field with ten black dots representing the password. Underneath the field is a checkbox labeled "Show Password in Clear". Below that, it says "Please enter the same root password again to verify that you have typed it correctly." and asks to "Re-enter password to verify:". This is followed by another text input field with ten black dots and a second checkbox labeled "Show Password in Clear".

Note that you will not be able to see the password as you type it.

Root password:

●●●●●●●●●●

Show Password in Clear

Please enter the same root password again to verify that you have typed it correctly.

Re-enter password to verify:

●●●●●●●●●●

Show Password in Clear

- ❖ В процессе установки нам предложат выбрать язык и регион, а также придумать надежный пароль для обычных пользователей и суперпользователя.

Разметка диска

Автоматическая разметка диска обычно подходит для большинства сценариев.

Осуществить разбиение диска можно 2 способами:

- ❖ Guided (автоматически)
- ❖ Manual (вручную)

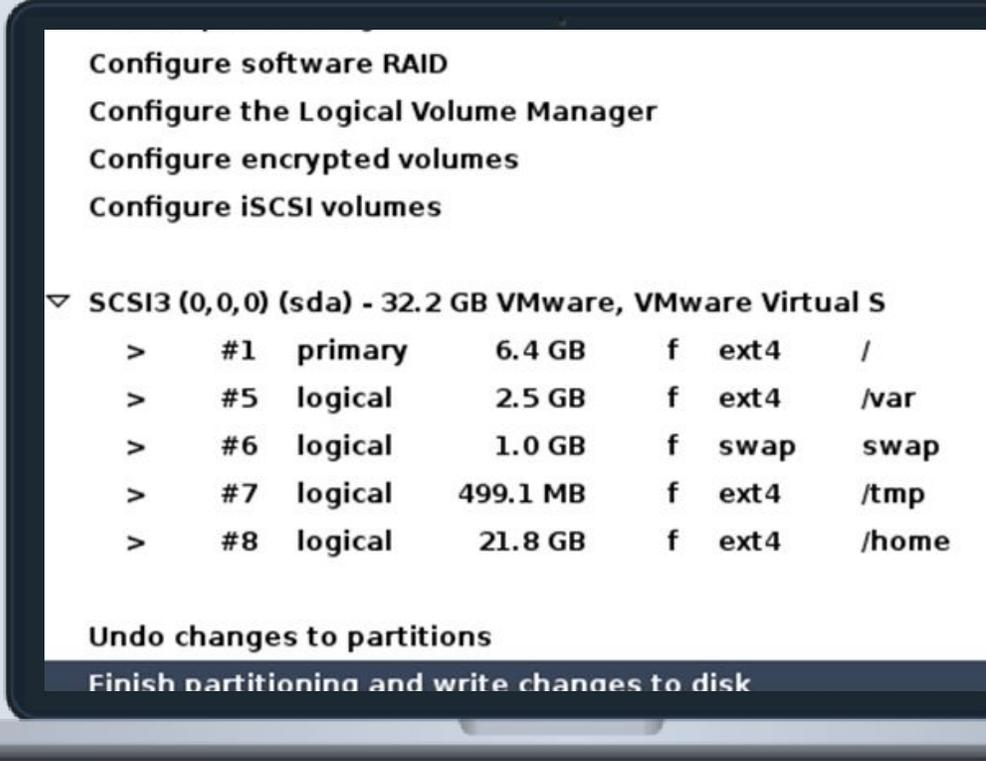


Ручная разметка

Однако впоследствии может возникнуть необходимость самостоятельно выбирать размеры для разделов или, например, создать отдельные разделы для тех или иных задач. Для этого нужно выбрать ручную разметку.

Здесь нужно будет указать:

- ❖ вид раздела;
- ❖ файловую систему;
- ❖ точку монтирования.

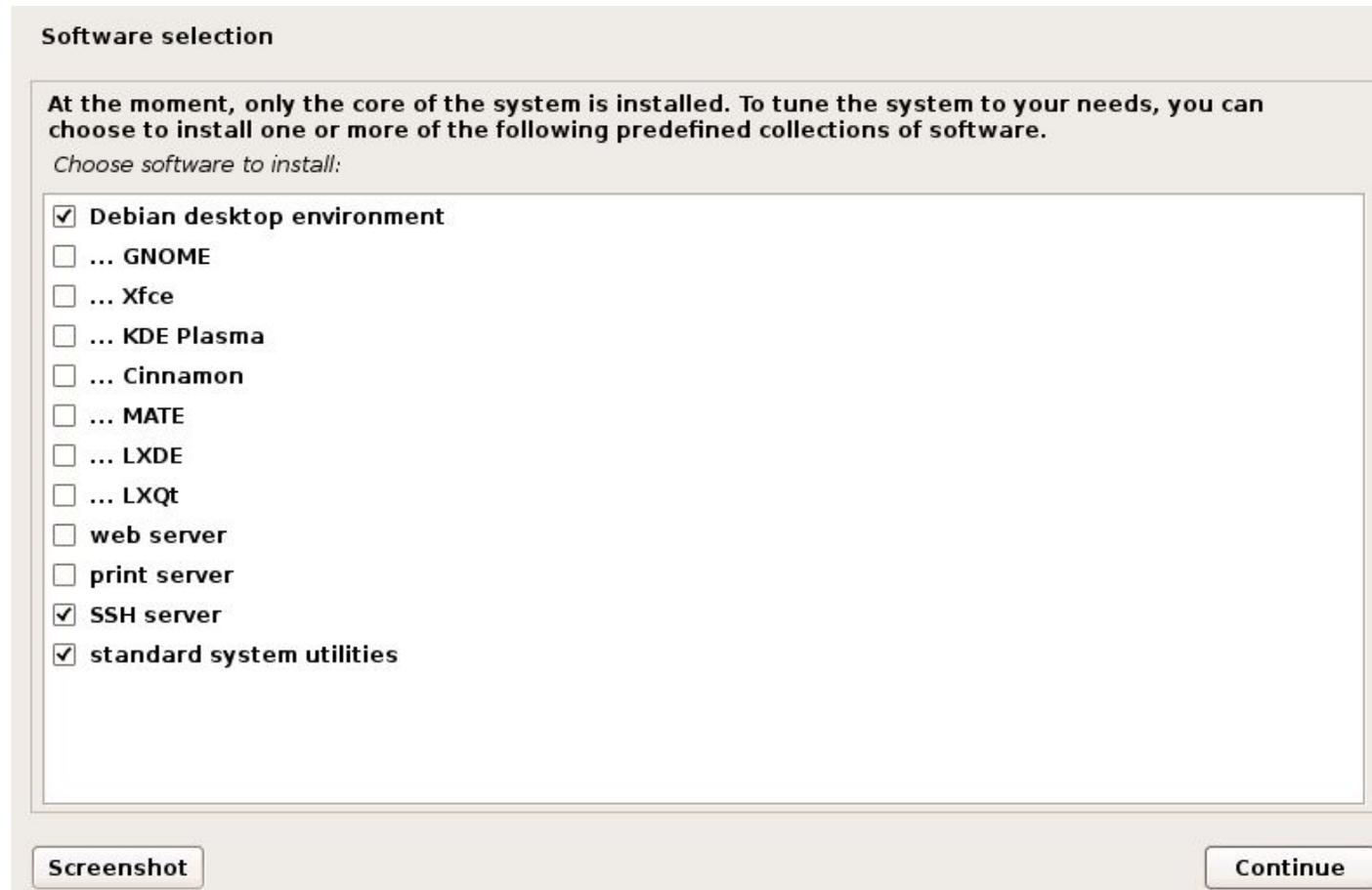


```
Configure software RAID
Configure the Logical Volume Manager
Configure encrypted volumes
Configure iSCSI volumes

SCSI3 (0,0,0) (sda) - 32.2 GB VMware, VMware Virtual S
> #1 primary 6.4 GB f ext4 /
> #5 logical 2.5 GB f ext4 /var
> #6 logical 1.0 GB f swap swap
> #7 logical 499.1 MB f ext4 /tmp
> #8 logical 21.8 GB f ext4 /home

Undo changes to partitions
Finish partitioning and write changes to disk
```

Выбор программного обеспечения



OS Linux

Тема 2. Администрирование Linux

Модель прав доступа



Пользователи в Linux

В системе Linux существует 2 типа пользователей:

- ❖ Обычные пользователи
- ❖ Системные пользователи

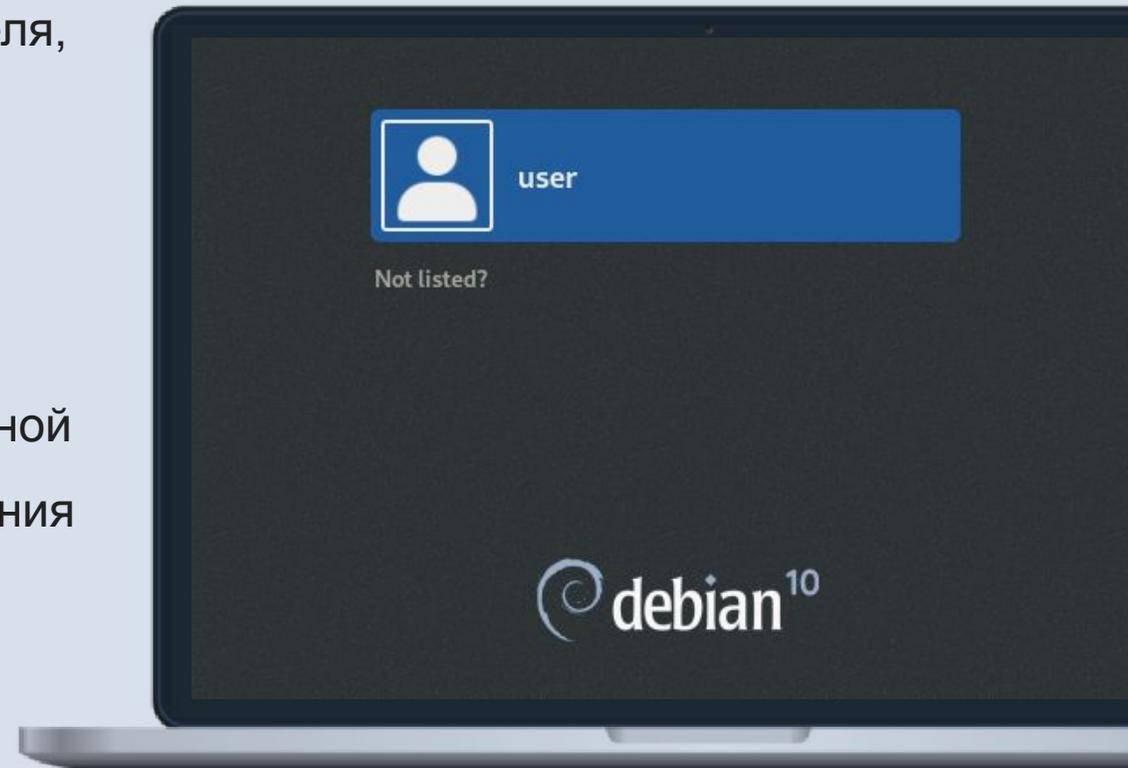
Среди системных пользователей отдельно можно выделить суперпользователя **root**.

Обычные пользователи

- ❖ Они создаются системным администратором. Каждый пользователь имеет числовой идентификатор пользователя, называемый UID.

Системные пользователи

- ❖ Системные пользователи создаются самой операционной системой. Зачастую они используются для управления какими-либо приложениями.



Root

- ❖ Данный пользователь имеет UID равный 0.
- ❖ **Root** может выполнять все операции, к примеру - работа с сетью на низком уровне, запись в критическую область памяти и прочее. Он игнорирует все права, которые поставили другие пользователи, может переключиться за любого другого пользователя.

Осторожно, root!



Работать с **root** правами не рекомендуется по двум причинам:

❖ Угроза безопасности

Злоумышленникам будет проще закрепиться в системе и скрыться, если вы ведете работу под этим типом доступа.

❖ Риск различных ошибок

Они могут привести к поломке системы. В Linux почти нет систем, которые мешали бы сломать ее, поэтому использовать права суперпользователя надо крайне осторожно.

Создание пользователей

- ❖ Для того, чтобы добавить нового пользователя, можно воспользоваться утилитой **useradd**, которая есть во всех дистрибутивах Linux.

```
$useradd [опции] пользователь
```

Опция	Описание
-b	Базовый каталог для размещения домашнего каталога пользователя, по умолчанию /home.
-d	Домашний каталог, в котором будут размещаться файлы пользователя.
-c	Комментарий к учетной записи.
-e	Дата, когда учетная запись пользователя будет заблокирована.
-f	Заблокировать учетную запись сразу после создания.
-g	Основная группа пользователя.

Удаление пользователей

- ❖ Для удаления существующего пользователя существует команда **userdel**.

```
$userdel [опции] пользователь
```

Опция	Описание
-f	Принудительное удаление учетной записи и домашнего каталога пользователя, даже если он еще находится в системе
-r	Удалить пользователя вместе с домашним каталогом и почтовым ящиком

Права доступа



- ❖ Каждый файл в Linux системах принадлежит одному пользователю и одной группе. Чтобы узнать какому пользователю и группе принадлежит файл, можно воспользоваться командой.

```
$ls -l [путь к файлу]
```

```
user@debian:~$ ls -l
total 4
drwxr-xr-x 2 user      user      4096 Apr 19 12:54 Documents
-rw-r--r-- 1 user      user           0 Apr 19 12:55 example
-rw-r--r-- 1 vyacheslav vyacheslav   0 Apr 18 21:58 file.txt
user@debian:~$
```

Типы файлов

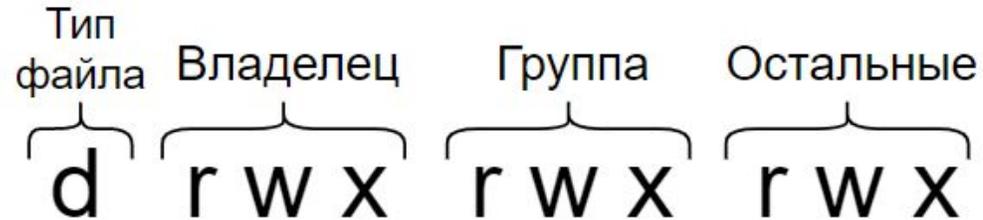


- ❖ Первый символ отображает информацию о типе файла.

Возможные значения:

Обозначение	Описание
-	Обычный файл.
d	Директория.
l	Символическая ссылка.
c	Устройство символьного ввода-вывода.
b	Устройство блочного ввода-вывода.
p	FIFO - связь между процессами
s	Сокет.

Права доступа



Права доступа к файлам	
r	Право на чтение данных.
w	Право на изменение содержимого (кроме удаления).
x	Право на исполнение файла.

Права доступа к каталогам	
r	Право на чтение каталога (можно прочитать содержимое, т.е. получить список объектов, находящихся в каталоге).
w	Право на изменение содержимого каталога (можно создавать и удалять объекты).
x	Позволяет войти в каталог.

Изменение прав доступа

❖ Изменить владельца

```
$ chown [опции] user1 file1
```

Назначить user1 владельцем file1.

❖ Изменить группу

```
$ chgrp [опции] group1 file1
```

Изменить группу на group1 для файла file1.

Chmod

Chmod используется для изменения прав доступа на чтение, запись и исполнение.

Виды прав	
u	Владелец
g	Группа
o	Все остальные

Виды прав	
r	Чтение
w	Запись
x	Исполнение
s	Исполнение от root

Примеры

```
$chmod +x file /Сделать файла исполняемым для всех.  
$chmod ug+w file /Разрешить изменение файла для владельца и группы.  
$chmod o-w file /Запретить запись остальным пользователям.  
$chmod ugo+rwx /Разрешить чтение, запись и исполнение для всех.
```

Числовые режимы

Однако есть еще один способ указания прав: **использование четырехзначных восьмеричных чисел**. Этот синтаксис, называется числовым синтаксисом прав доступа, где каждая цифра представляет тройку разрешений.

Число	Режим
0	---
1	--x
2	-w-
3	-wx
4	r--
5	r-x
6	rw-
7	rwX

suid, sgid и sticky bit

Есть достаточно много программ и файлов, которые должны принадлежать пользователю root и в то же время которые простые пользователи должны иметь возможность выполнять. Для этого и нужны SUID и SGID.

Set Group Identifier (sgid)

аналогичен suid, но устанавливаются права группы – владельца файла. Также все файлы, создаваемые в каталоге с установленным sgid, будут получать идентификатор группы – владельца каталога, а не владельца файла.

Sticky bit

при использовании пользователь сможет удалить файл, только если будет являться владельцем этого файла или владельцем каталога, в котором содержится файл.

Set User Identifier (suid)

даёт возможность на время выполнения файла (запущенного им процесса) непривилегированному пользователю получить права пользователя – владельца файла.

Umask

- ❖ Когда процесс создает новый файл, он указывает, какие права доступа нужно задать для данного файла. Зачастую запрашиваются права 0666 (чтение и запись всеми), что дает больше разрешений, чем необходимо в большинстве случаев. Система использует значение `umask` чтобы понизить изначально задаваемые разрешения на что-то более разумное и безопасное.
- ❖ В Linux-системах значением по умолчанию для `umask` является `0022`.

```
root@debian:~# umask
0022
root@debian:~# umask -S
u=rwx,g=rw,o=rw
```

Switching user

- ❖ Утилита **su** (switch user) есть практически во всех системах, и она позволяет перейти за root или другого пользователя, зная его пароль.
- ❖ Все команды, которые выполняются через **sudo** логируются в **/var/log/auth.log**.

```
an su: pam_unix(su:session): session opened for user root by (uid=1000)
an su: (to vyacheslav) user on pts/0
an su: pam_unix(su:session): session opened for user vyacheslav by (uid=1000)
an su: (to root) user on pts/0
an su: pam_unix(su:session): session opened for user root by (uid=1000)
an su: (to vyacheslav) user on pts/0
an su: pam_unix(su:session): session opened for user vyacheslav by (uid=1000)
an su: pam_unix(su:session): session closed for user vyacheslav
an su: (to user) user on pts/0
an su: pam_unix(su:session): session opened for user user by (uid=1000)
an su: (to vyacheslav) user on pts/0
an su: pam_unix(su:session): session opened for user vyacheslav by (uid=1000)
an su: pam_unix(su:session): session closed for user vyacheslav
an su: (to user) user on pts/2
an su: pam_unix(su:session): session opened for user user by user(1000)
an su: pam_unix(su:session): session closed for user user
an su: (to user) user on pts/2
an su: pam_unix(su:session): session opened for user user by user(1000)
an su: (to mihail) user on pts/2
an su: pam_unix(su:session): session opened for user mihail by user(1000)
an su: pam_unix(su:session): session closed for user mihail
```

Sudo

- ❖ Для того, чтобы пользователь мог выполнять команды от имени суперпользователя, его нужно добавить в группу «**sudo**».

```
$usermod -aG sudo имя_пользователя
```

- ❖ Команда **sudo** позволяет выполнять разовые команды с привилегиями суперпользователя без необходимости создавать новую оболочку.

Sudoers

В **sudoers** хранится список пользователей, с указанием того, что они могут выполнять. Для редактирования файла **sudoers** нужно пользоваться командой «**visudo**».

❖ **root ALL = (ALL:ALL) ALL**

Данная строчка указывает на то, что пользователь **root** имеет неограниченные привилегии в системе.

❖ **%sudo ALL = (ALL:ALL) ALL**

Указывает на то, что пользователи в группе **sudo** имеют права на запуск любой команды.

```
#  
# See the man page for details on how to write a sudoers file  
#  
Defaults        env_reset  
Defaults        mail_badpass  
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:  
  
# Host alias specification  
  
# User alias specification  
  
# Cmnd alias specification  
  
# User privilege specification  
root    ALL=(ALL:ALL) ALL  
  
# Allow members of group sudo to execute any command  
%sudo   ALL=(ALL:ALL) ALL  
  
# See sudoers(5) for more information on "#include" directives
```

Строки привилегий

root ALL = (ALL:ALL) ALL

- ❖ **Первое поле** показывает имя пользователя.
- ❖ **Первое ALL** означает, что данное правило применяется ко всем хостам.
- ❖ **Второе ALL** означает, что пользователь root может запускать команды от лица всех пользователей.
- ❖ **Третье ALL** означает, что пользователь root может запускать команды от лица всех групп.
- ❖ **Последнее ALL** означает, что данные правила применяются всем командам.

Смена паролей



- ❖ Смена пароля выполняется с помощью утилиты **passwd**. Она позволяет не только менять пароль, но и управлять сроком его жизни.

```
$passwd [опции] пользователь
```

Опция	Описание
-d	Удалить пароль пользователя, после этого он не сможет войти.
-e	Сделать пароль устаревшим.
-i	Количество дней после того, как пароль устарел, по истечении которых отключить аккаунт, если пользователь не сменил пароль.
-l	Запретить пользователю входить в систему.
-n	Минимальное количество дней между сменами пароля.
-x	Максимальное количество дней, пока пароль можно использовать.

/etc/passwd/

- ❖ Представляет собой простую текстовую базу данных, которая содержит информацию обо всех учетных записях пользователей в системе.
- ❖ Обычно первая строка описывает пользователя **root**, за которым следуют системные и обычные учетные записи пользователей. Новые записи добавляются в конец файла.

/etc/passwd/

Каждая строка файла /etc/passwd содержит семь полей:

- ❖ **Username** - имя учетной записи.
- ❖ **Password** - в большинстве современных систем это поле имеет значение x, а пароль пользователя сохраняется в файле /etc/shadow.
- ❖ **UID** - идентификатор пользователя.
- ❖ **GID** - номер идентификатора группы пользователя, относящийся к основной группе пользователя.
- ❖ **GECOS** - полное имя пользователя
- ❖ **Home directory** - абсолютный путь к домашнему каталогу пользователя.
- ❖ **Login shell** - абсолютный путь к оболочке входа пользователя.

```
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:./nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronizati
```

/etc/shadow

- ❖ **/etc/passwd** - это зашифрованный файл паролей, в котором хранится зашифрованная информация о паролях для учетных записей пользователей.
- ❖ В дополнение к хранению зашифрованного пароля файл **/etc/shadow** хранит дополнительную информацию о сроке действия или истечении срока действия пароля.

OS Linux

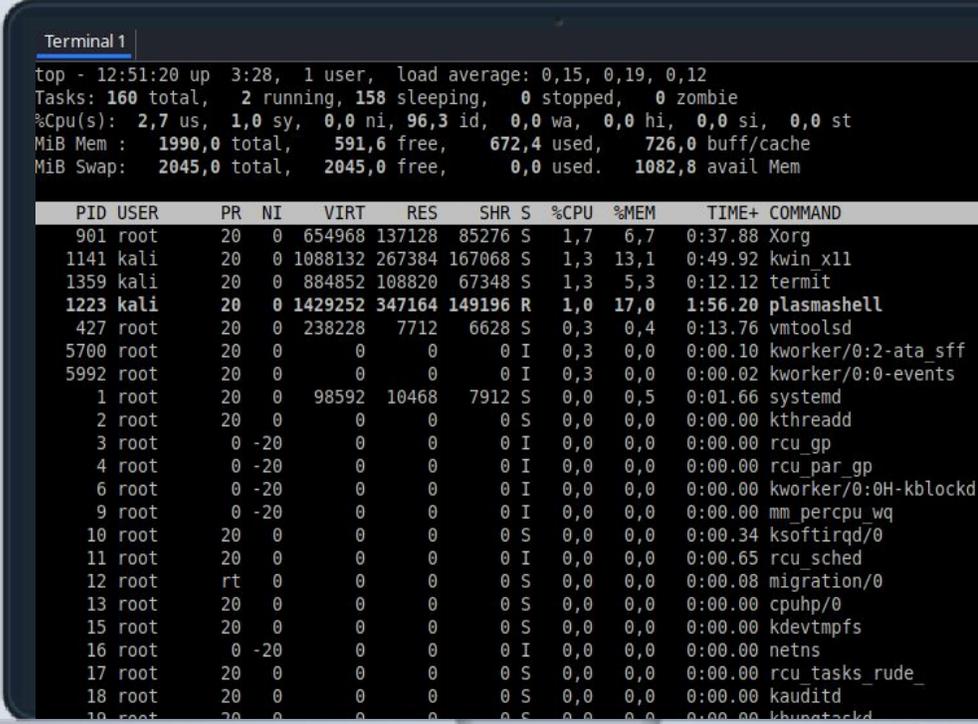
Тема 2. Администрирование Linux

Мониторинг Linux



Мониторинг OS Linux

- ❖ Понимание состояния инфраструктуры и систем важно для стабильной работы сервисов. Информация о работоспособности и производительности развертываний не только помогает команде вовремя реагировать на проблемы, но и дает им возможность уверенно вносить все требуемые изменения.
- ❖ Один из лучших способов получить эту информацию – это **надежная система мониторинга**, она визуализирует данные и предупреждает специалиста, когда что-то работает неправильно.



```
Terminal 1
top - 12:51:20 up 3:28, 1 user, load average: 0,15, 0,19, 0,12
Tasks: 160 total, 2 running, 158 sleeping, 0 stopped, 0 zombie
%Cpu(s): 2,7 us, 1,0 sy, 0,0 ni, 96,3 id, 0,0 wa, 0,0 hi, 0,0 si, 0,0 st
MiB Mem : 1990,0 total, 591,6 free, 672,4 used, 726,0 buff/cache
MiB Swap: 2045,0 total, 2045,0 free, 0,0 used. 1082,8 avail Mem

  PID USER      PR  NI  VIRT  RES  SHR  S  %CPU  %MEM    TIME+  COMMAND
  901 root        20   0 654968 137128 85276 S   1,7   6,7   0:37.88 Xorg
 1141 kali        20   0 1088132 267384 167068 S   1,3  13,1   0:49.92 kwin_x11
 1359 kali        20   0 884852 108820 67348 S   1,3   5,3   0:12.12 termit
 1223 kali        20   0 1429252 347164 149196 R   1,0  17,0   1:56.20 plasmashell
  427 root        20   0 238228   7712  6628 S   0,3   0,4   0:13.76 vmtoolsd
 5700 root        20   0     0     0     0 I   0,3   0,0   0:00.10 kworker/0:2-ata_sff
 5992 root        20   0     0     0     0 I   0,3   0,0   0:00.02 kworker/0:0-events
    1 root        20   0 98592  10468  7912 S   0,0   0,5   0:01.66 systemd
    2 root        20   0     0     0     0 S   0,0   0,0   0:00.00 kthreadd
    3 root         0 -20     0     0     0 I   0,0   0,0   0:00.00 rcu_gp
    4 root         0 -20     0     0     0 I   0,0   0,0   0:00.00 rcu_par_gp
    6 root         0 -20     0     0     0 I   0,0   0,0   0:00.00 kworker/0:0H-kblockd
    9 root         0 -20     0     0     0 I   0,0   0,0   0:00.00 mm_percpu_wq
   10 root        20   0     0     0     0 S   0,0   0,0   0:00.34 ksftirqd/0
   11 root        20   0     0     0     0 I   0,0   0,0   0:00.65 rcu_sched
   12 root         rt   0     0     0     0 S   0,0   0,0   0:00.08 migration/0
   13 root        20   0     0     0     0 S   0,0   0,0   0:00.00 cpuhp/0
   15 root        20   0     0     0     0 S   0,0   0,0   0:00.00 kdevtmpfs
   16 root         0 -20     0     0     0 I   0,0   0,0   0:00.00 netns
   17 root        20   0     0     0     0 S   0,0   0,0   0:00.00 rcu_tasks_rude_
   18 root        20   0     0     0     0 S   0,0   0,0   0:00.00 kauditd
   19 root        20   0     0     0     0 S   0,0   0,0   0:00.00 khuntpackd
```

Мониторинг OS Linux

- ❖ Теперь рассмотрим инструменты мониторинга операционной системы Linux подробнее – **df, du, free, iostat, mpstat, vmstat, w, htop.**

```
kali@kali:~$ vmstat -a
procs -----memory----- --swap-- ----io---- -system-- -----cpu-----
 r b swpd free  inact active  si so  bi bo  in cs us sy id wa st
 0 0   0 611892 954180 332816  0 0  79 35 111 578 6 0 94 0 0
kali@kali:~$
kali@kali:~$ vmstat -f
4011 forks
kali@kali:~$
kali@kali:~$ vmstat -m
vmstat: your kernel does not support slabinfo or your permissions are insufficient
kali@kali:~$ vmstat -n
procs -----memory----- --swap-- ----io---- -system-- -----cpu-----
 r b swpd free  buff cache  si so  bi bo  in cs us sy id wa st
 0 0   0 611672 44384 694464  0 0  76 34 110 565 6 0 94 0 0
kali@kali:~$ vmstat -d
disk- ----reads----- --writes----- --IO-----
      total merged sectors      ms total merged sectors      ms  cur  sec
sr0      46      0      2340      21      0      0      0      0      0      0
sda    11825    6862 1077630    7382 13350   4660 487282   6318      0    20
kali@kali:~$
kali@kali:~$
kali@kali:~$
kali@kali:~$ vmstat -d
disk- ----reads----- --writes----- --IO-----
      total merged sectors      ms total merged sectors      ms  cur  sec
sr0      46      0      2340      21      0      0      0      0      0      0
sda    11825    6862 1077630    7382 13350   4660 487282   6318      0    20
kali@kali:~$
```

Команда	Описание
df	Утилита df поставляется по умолчанию во всех дистрибутивах Linux и имеет очень простой синтаксис.
du	Команда du сообщает приблизительный объем дискового пространства, используемого данными файлами или каталогами.
free	Сколько свободной оперативной памяти доступно в моей системе Linux? Достаточно ли свободной памяти для установки и запуска новых приложений?
iostat	Команда iostat в Linux используется для мониторинга системной статистики ввода-вывода для устройств и разделов.
mpstat	Команда mpstat пишет в стандартный вывод на экран о каждом имеющемся процессоре.
vmstat	Содержит статистическую информацию об оперативной памяти, дисках, ядра, переключении контекста и работе процессора.
w	Выводит краткую сводку о работающих в системе в данный момент пользователях.
htop	Показывает информацию о процессах в реальном времени, выводит данные о потреблении системных ресурсов, останавливает и управляет процессами.

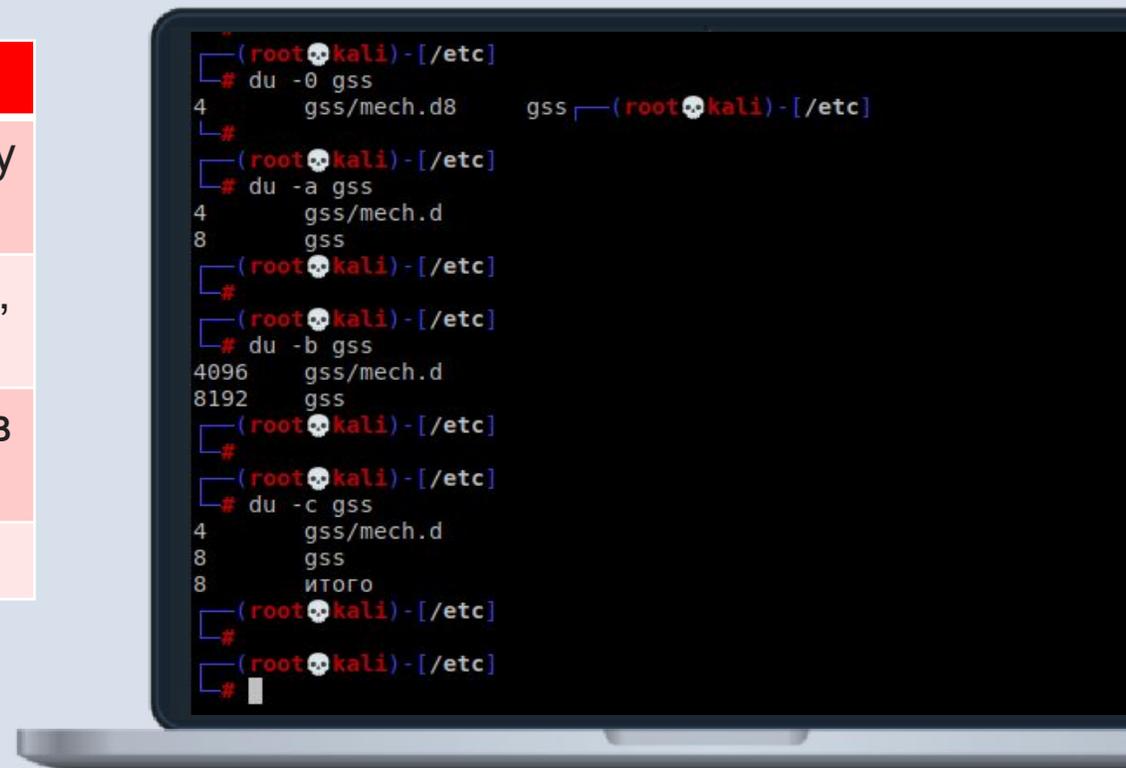
df

Команда	Описание
df	Показывает сведения о файловой системе.
df -a	Включает фиктивные, дублированные, недоступные файловые системы.
df -h	Выводит размеры в степени 1024.
df -H	Выводит размеры в степени 1000.
df -l	Перечислить только файловые системы.
df -T	Выводит тип файловой системы.
df -type ext4	Перечисляет только указанные файловые системы – ext4.
df --exclude-type ext4	Исключить файловую систему - ext4.

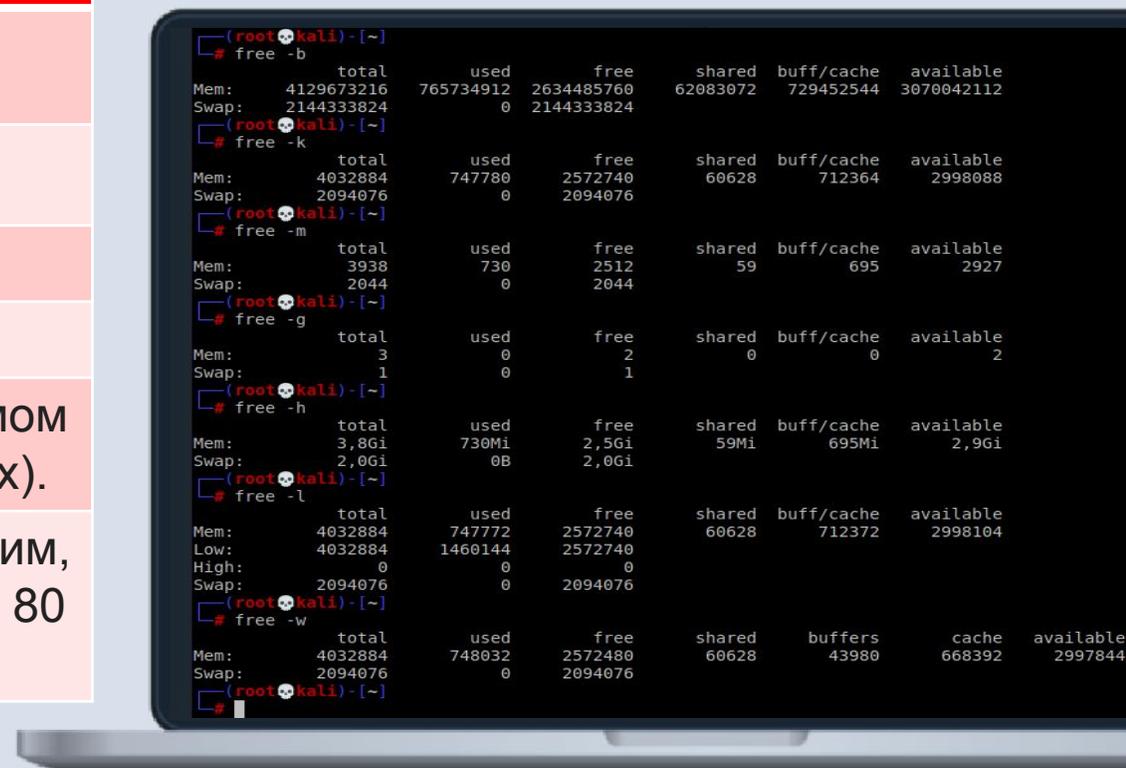
```
kali@kali:~$ df -T
Файловая система Тип      1К-блоков  Использовано  Доступно  Использовано%  Смонтировано в
udev              devtmpfs  1994640      0  1994640      0% /dev
tmpfs             tmpfs     403292      1076  402216      1% /run
/dev/sda1         ext4     18447056   6753348  10733608    39% /
tmpfs             tmpfs     2016440      0  2016440      0% /dev/shm
tmpfs             tmpfs      5120        0   5120        0% /run/lock
tmpfs             tmpfs     403288       76  403212      1% /run/user/1000
kali@kali:~$ df --type ext4
Файловая система 1К-блоков  Использовано  Доступно  Использовано%  Смонтировано в
/dev/sda1         18447056   6753348  10733608    39% /
kali@kali:~$ df --exclude-type ext4
Файловая система 1К-блоков  Использовано  Доступно  Использовано%  Смонтировано в
udev              1994640      0  1994640      0% /dev
tmpfs             403292      1076  402216      1% /run
tmpfs             2016440      0  2016440      0% /dev/shm
tmpfs             5120        0   5120        0% /run/lock
tmpfs             403288       76  403212      1% /run/user/1000
kali@kali:~$ df --total
Файловая система 1К-блоков  Использовано  Доступно  Использовано%  Смонтировано в
udev              1994640      0  1994640      0% /dev
tmpfs             403292      1076  402216      1% /run
/dev/sda1         18447056   6753348  10733608    39% /
tmpfs             2016440      0  2016440      0% /dev/shm
tmpfs             5120        0   5120        0% /run/lock
tmpfs             403288       76  403212      1% /run/user/1000
total            23269836   6754500  15555236    31% -
kali@kali:~$
```

du

Команда	Описание
<code>du -0</code>	Заканчивает каждую выводимую строку NULL, а не символом строки.
<code>du -a</code>	Выводит весь объём для всех файлов, а не только каталоги.
<code>du -b</code>	Выводит действительные размеры в байтах.
<code>du -c</code>	Выводит общий каталог.



Команда	Описание
free -b	Отображать вывод в байтах.
free -k	Отображать вывод в килобайтах.
free -m	Отображать вывод в мегабайтах.
free -g	Показать вывод в гигабайтах.
free -h	Просмотреть информацию в удобочитаемом формате (обычно в мегабайтах и гигабайтах).
free -w	Переключение вывода в расширенный режим, который обеспечивает вывод более 80 символов в строке.



iostat

Команда	Описание
<code>iostat -c</code>	Отобразить только информацию об использовании процессора.
<code>iostat -d</code>	Отобразить только информацию об использовании устройств.
<code>iostat -h</code>	Вывести данные в отчёте в удобном для чтения формате.
<code>iostat -k</code>	Вывести статистику в килобайтах.
<code>iostat -m</code>	Вывести статистику в мегабайтах.
<code>iostat -p</code>	Вывести статистику по устройству и всем его разделам.
<code>iostat -x</code>	Вывести расширенную статистику.



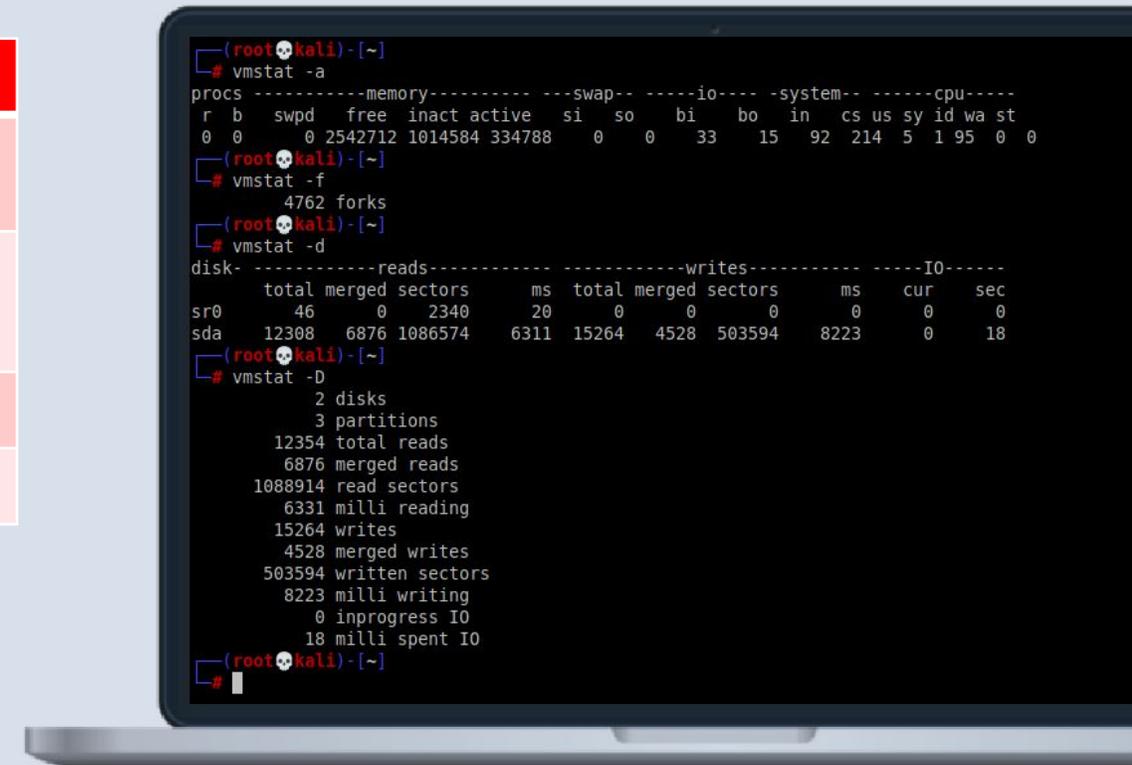
mpstat

Команда	Описание
<code>mpstat -A</code>	Показывает всю информацию, которая может быть отображена с помощью команды «mpstat» о процессоре.
<code>mpstat -P ALL</code>	Параметр «-P ALL» покажет все индивидуальные процессоры или ядра вместе со статистикой.
<code>mpstat -P 0</code>	Для отображения статистически о конкретном CPU или ядре, используйте опцию -P.
<code>mpstat -V</code>	Можно выполнить «mpstat -V», чтобы показать версию утилиты.



vmstat

Команда	Описание
vmstat -a	Активная/неактивная память.
vmstat -f	Количество задач с момента загрузки.
vmstat -d	Статистика диска.
vmstat -D	Общая статистика диска.



Команда	Описание
w -h	Не выводить заголовков у таблицы.
w -u	Игнорировать имена пользователей при определении времени текущего процесса и времени CPU.
w -s	Использовать сокращенный формат вывода. Не выводить колонки JCPU и PCPU.
w -f	Включить или выключить вывод поля «from», которое соответствует имени удаленного хоста (remote hostname).
w -l	Выводить в поле from IP-адрес вместо имени хоста (hostname), если это возможно.
w -o	Выводить информацию в старом формате.
w -V	Вывести версию утилиты/команды w.

```
(root@kali)~# w -h
kali  tty7  :0          14:05   2:41m  1:12   0.05s /usr/bin/startplasma-x11
(root@kali)~# w -u
16:47:10 up  2:41,  1 user,  load average: 0,41, 0,28, 0,18
USER  TTY  FROM          LOGIN@  IDLE   JCPU   PCPU   WHAT
kali  tty7  :0          14:05   2:41m  1:12   1:12  /usr/lib/xorg/Xorg -nolisten tcp
(root@kali)~# w -s
16:47:13 up  2:41,  1 user,  load average: 0,41, 0,28, 0,18
USER  TTY  FROM          IDLE   WHAT
kali  tty7  :0          2:41m /usr/bin/startplasma-x11
(root@kali)~# w -f
16:47:16 up  2:42,  1 user,  load average: 0,38, 0,28, 0,18
USER  TTY  LOGIN@  IDLE   JCPU   PCPU   WHAT
kali  tty7  14:05   2:41m  1:12   0.05s /usr/bin/startplasma-x11
(root@kali)~# w -l
16:47:20 up  2:42,  1 user,  load average: 0,35, 0,27, 0,18
USER  TTY  FROM          LOGIN@  IDLE   JCPU   PCPU   WHAT
kali  tty7  :0          14:05   2:42m  1:12   0.05s /usr/bin/startplasma-x11
(root@kali)~# w -o
16:47:23 up  2:42,  1 user,  load average: 0,35, 0,27, 0,18
USER  TTY  FROM          LOGIN@  IDLE   JCPU   PCPU   WHAT
kali  tty7  :0          14:05   2:42   1:12m   /usr/bin/startplasma-x11
(root@kali)~# w -V
w from procps-ng 3.3.16
(root@kali)~#
```

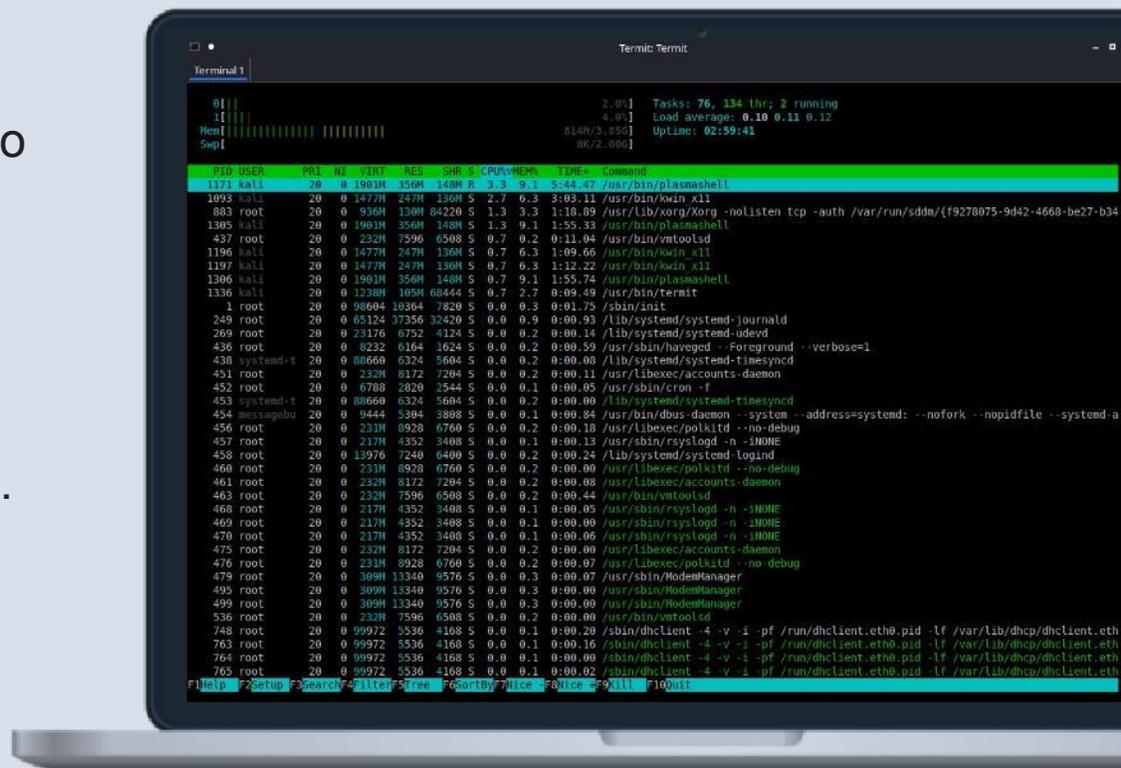
htop

Окно htop разделено на два основных раздела:

- ❖ обобщённая информация о системе
- ❖ подробная информация о процессах

В самом верху показана нагрузка на каждое ядро центрального процессора (цифры от 1 до 12).

- ❖ **Mem** — это общее количество оперативной памяти и используемая память.
- ❖ **Task** — обобщённая статистика по процессам.
- ❖ **Swp** — уровень занятости файла подкачки (если он есть).
- ❖ **Load average** — средняя загрузка центрального процессора.
- ❖ **Uptime** — время работы операционной системы с момента последней загрузки.



OS Linux

Тема 2. Администрирование
Linux

Конфигурация сети

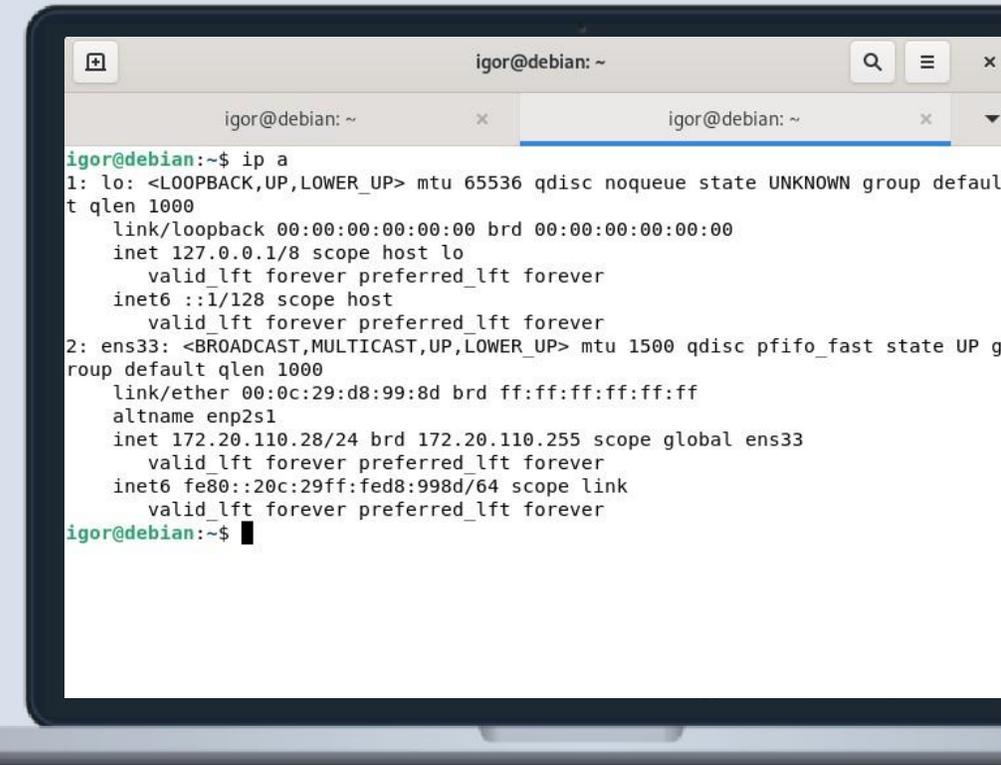


Конфигурирование сети OS Linux

Как подключить компьютер или сервер к сети при помощи конфигурационных файлов и консольных утилит?

Основная цель - рассказать о различных способах подключения к интернету без использования GUI (графического интерфейса).

Не затрагиваем таких тем, как настройка сетевых фильтров или, например, собственных точек доступа Wi-Fi. Подразумевается, что существует некий, предоставленный провайдером, способ подключения к интернету, для использования которого и необходимо выполнить приведенные ниже действия.



```
igor@debian:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:d8:99:8d brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 172.20.110.28/24 brd 172.20.110.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fed8:998d/64 scope link
        valid_lft forever preferred_lft forever
igor@debian:~$
```

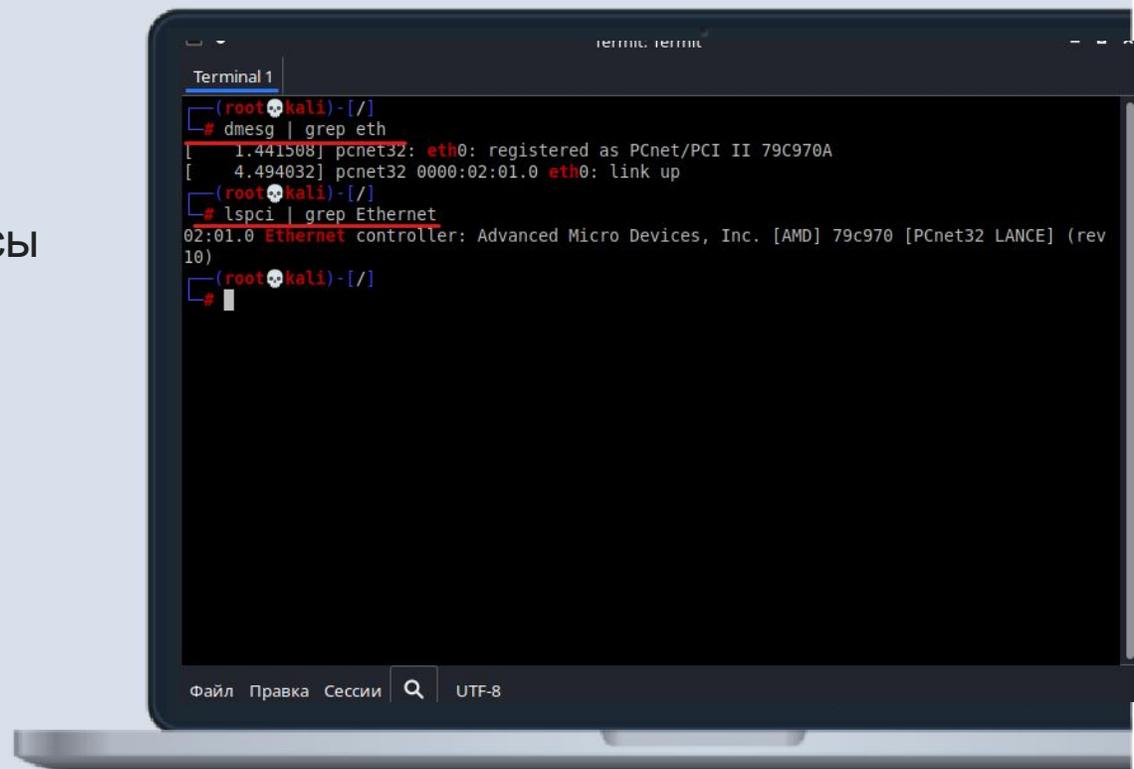
Параметры сети в Linux

Начнем понимание сетевых механизмов Linux с **ручного конфигурирования сети**, то есть со случая, когда IP-адрес сетевого интерфейса **статичен**. Итак, при настройке сети, необходимо учесть и настроить следующие параметры:

- ❖ IP-адрес
- ❖ Маска подсети
- ❖ IP-адрес шлюза
- ❖ IP-адрес сервера имен (DNS-сервера)

Параметры сети в Linux

- ❖ Для того чтобы узнать какие сетевые интерфейсы используются введём команду **dmesg | grep eth**
- ❖ Для более подробной информации вводим команду **lspci | grep Ethernet**



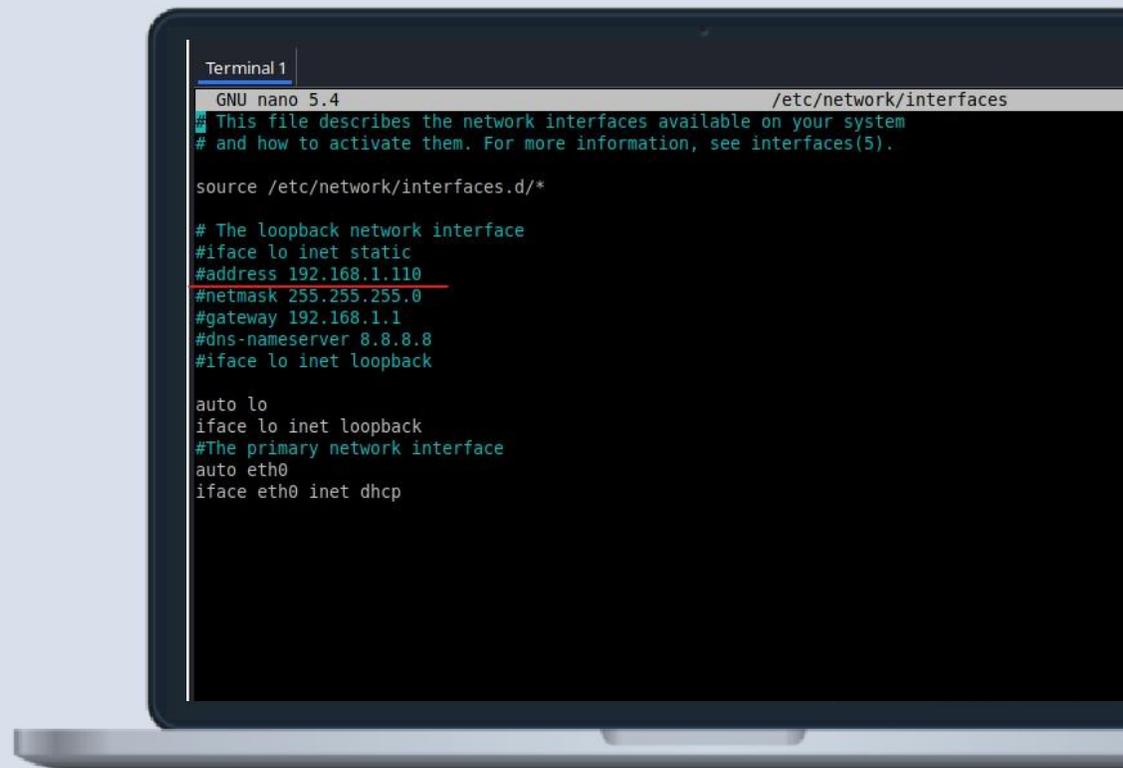
```
Terminal 1
(root@kali) - [/]
# dmesg | grep eth
[ 1.441508] pcnet32: eth0: registered as PCnet/PCI II 79C970A
[ 4.494032] pcnet32 0000:02:01.0 eth0: link up
(root@kali) - [/]
# lspci | grep Ethernet
02:01.0 Ethernet controller: Advanced Micro Devices, Inc. [AMD] 79c970 [PCnet32 LANCE] (rev 10)
(root@kali) - [/]
#
```

IP-адрес

IP-адрес - это **уникальный адрес** машины, в формате четырех десятичных чисел, разделенных точками. Обычно, при работе в локальной сети, выбирается из частных (приватных/локальных) диапазонов:

- ❖ 10.0.0.0 – 10.255.255.255 / 8
- ❖ 172.16.0.0 – 172.31.255.255 / 12
- ❖ 192.168.0.0 – 192.168.255.255 / 16

Например, 192.168.0.1



```
Terminal 1
GNU nano 5.4 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
#iface lo inet static
#address 192.168.1.110
#netmask 255.255.255.0
#gateway 192.168.1.1
#dns-nameserver 8.8.8.8
#iface lo inet loopback

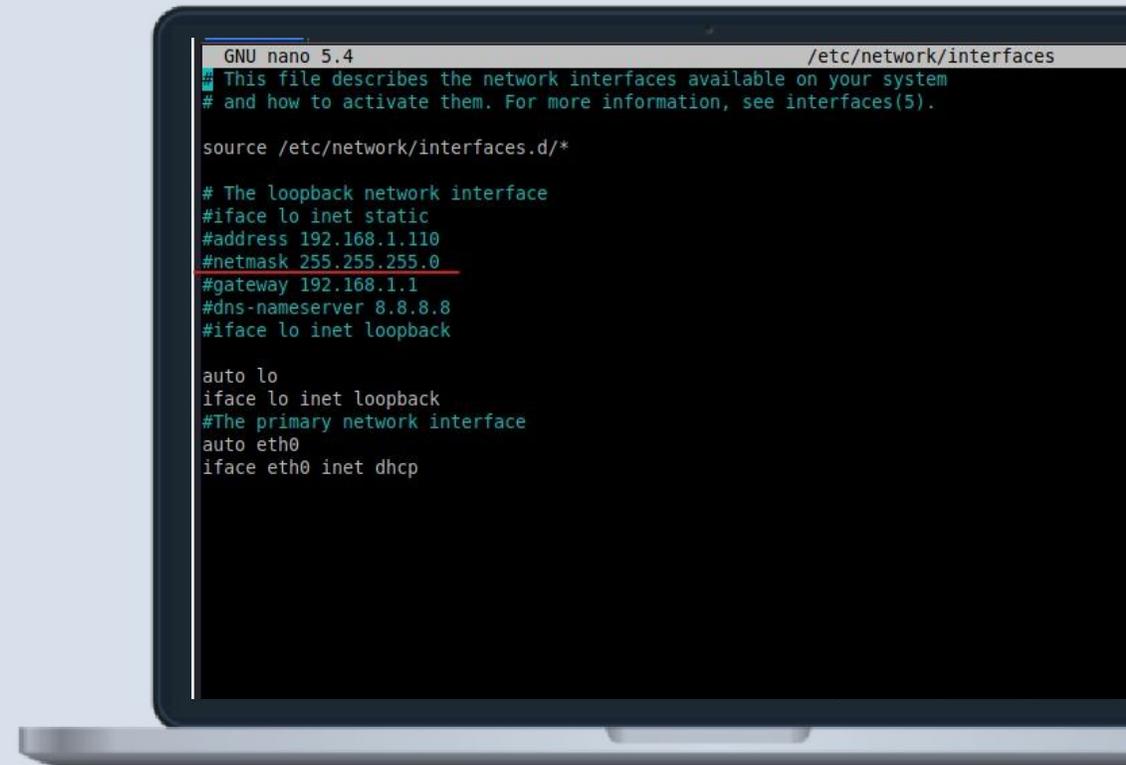
auto lo
iface lo inet loopback
#The primary network interface
auto eth0
iface eth0 inet dhcp
```

Маска подсети

Маска подсети - так же, 4 десятичных числа, определяющие, какая часть адреса относится к адресу сети/подсети, а какая к адресу хоста.

Маска подсети является числом, которое складывается (в двоичной форме) при помощи логического «И» с IP-адресом и в результате чего выясняется, к какой подсети принадлежит адрес.

Например, адрес 192.168.0.2 с маской 255.255.255.0 принадлежит подсети 192.168.0.



```
GNU nano 5.4 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

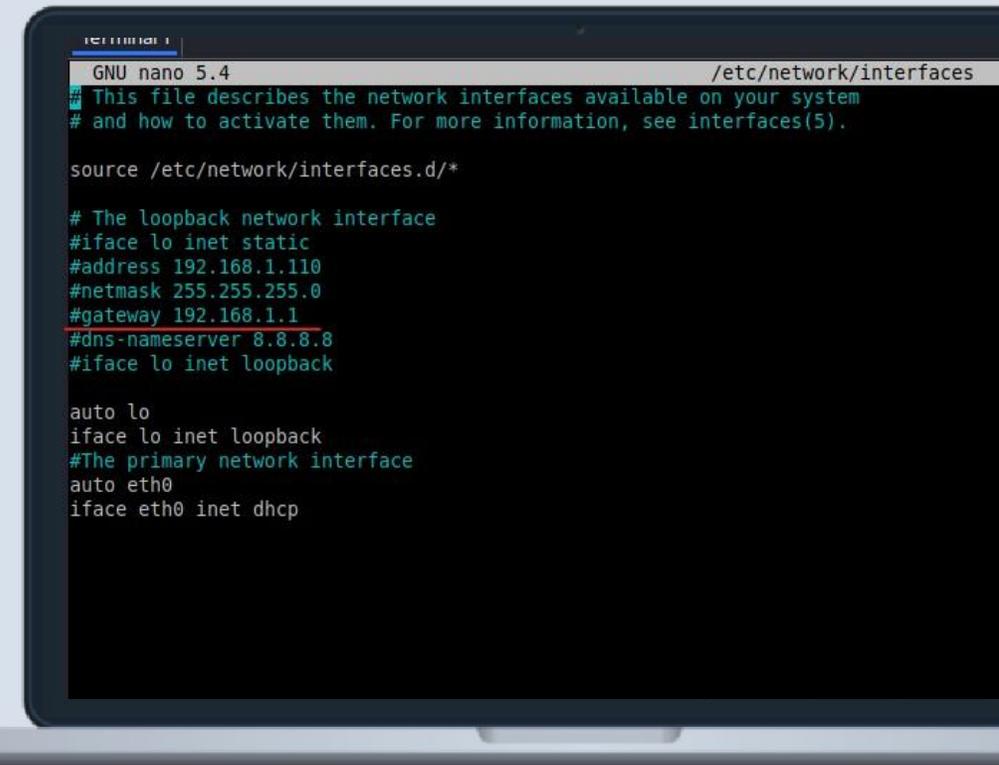
# The loopback network interface
iface lo inet static
#address 192.168.1.110
#netmask 255.255.255.0
#gateway 192.168.1.1
#dns-nameserver 8.8.8.8
iface lo inet loopback

auto lo
iface lo inet loopback
#The primary network interface
auto eth0
iface eth0 inet dhcp
```

IP-адрес шлюза

IP-адрес шлюза - это адрес машины, являющейся шлюзом по-умолчанию для связи с внешним миром. Шлюзов может быть несколько, если компьютер подключен к нескольким сетям одновременно.

Адрес шлюза не используется в изолированных сетях (не подключенных к глобальной сети), потому что данным сетям некуда отправлять пакеты вне сети, то же самое относится и к петлевым интерфейсам.



```
GNU nano 5.4 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

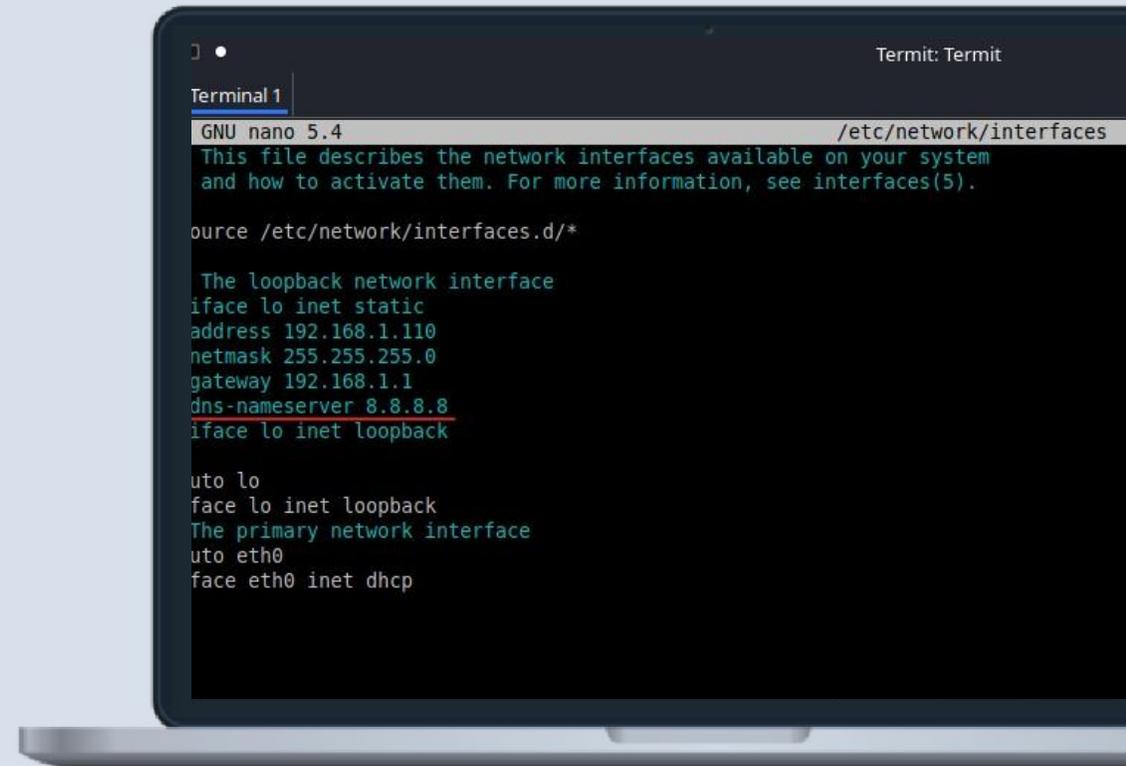
source /etc/network/interfaces.d/*

# The loopback network interface
#iface lo inet static
#address 192.168.1.110
#netmask 255.255.255.0
#gateway 192.168.1.1
#dns-nameserver 8.8.8.8
#iface lo inet loopback

auto lo
iface lo inet loopback
#The primary network interface
auto eth0
iface eth0 inet dhcp
```

IP-адрес сервера имен (DNS-сервера)

IP-адрес сервера имен (DNS-сервера) – адрес сервера, преобразующего имена хостов в IP-адреса. Обычно предоставляется провайдером.



```
Termit: Termit
Terminal 1
GNU nano 5.4 /etc/network/interfaces
This file describes the network interfaces available on your system
and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
iface lo inet static
address 192.168.1.110
netmask 255.255.255.0
gateway 192.168.1.1
dns-nameserver 8.8.8.8
iface lo inet loopback

# The primary network interface
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp
```

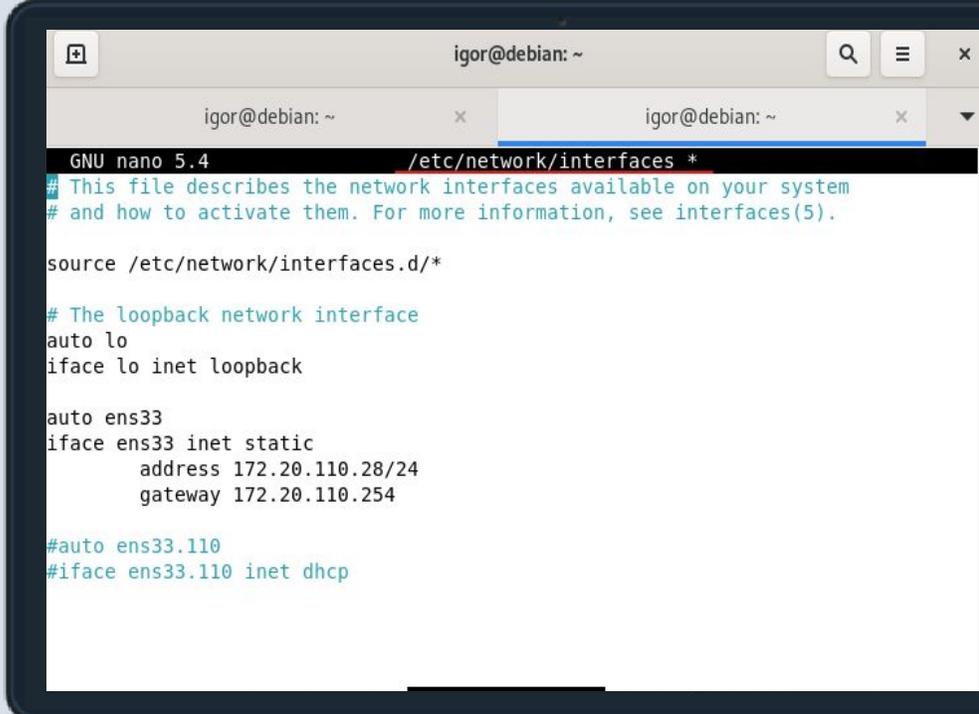
Параметры сети в Linux



Команда	Описание
<code>nano /etc/network/interfaces</code>	Данный файл хранит имена и адреса локальной и других сетей на базе дистрибутивов Debian
<code>nano /etc/hosts</code>	Данный файл хранит перечень IP адресов и соответствующих им (адресам) имен хостов.
<code>nano /etc/resolv.conf</code>	Этот файл определяет параметры механизма преобразования сетевых имен в IP адреса.
<code>nano /etc/nsswitch.conf</code>	При использовании данного файла, сетями можно управлять по имени.
<code>nano /etc/sysconfig/network-scripts</code>	Аналогично, в других дистрибутивах: в RedHat и SUSE сеть запускается скриптом
<code>nano /etc/netplan/01-netcfg.yaml</code>	Начиная с Ubuntu 18.04 конфигурирование сети выполняется с помощью утилиты netplan

nano /etc/network/interfaces

- ❖ Файл `/etc/network/interfaces` является **ОСНОВНЫМ файлом настроек сетевых интерфейсов**, соответствующих сетевым картам, в дистрибутивах Debian/Ubuntu.
- ❖ Интерфейс **loopback** определяется системой как `lo` и по умолчанию задает адрес `127.0.0.1`. Он может быть выведен командой `ifconfig`.



```
igor@debian: ~
GNU nano 5.4 /etc/network/interfaces *
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

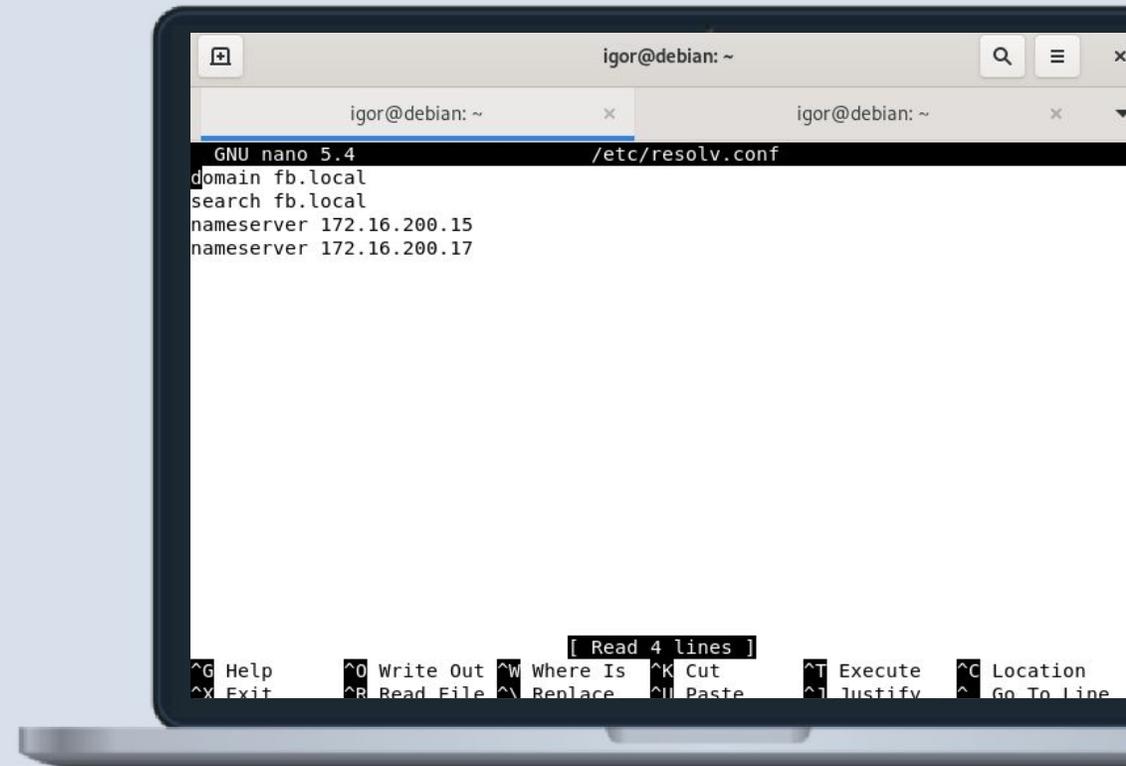
# The loopback network interface
auto lo
iface lo inet loopback

auto ens33
iface ens33 inet static
    address 172.20.110.28/24
    gateway 172.20.110.254

#auto ens33.110
#iface ens33.110 inet dhcp
```

nano /etc/resolv.conf

- ❖ Стало достаточно традиционным для Linux запускать небольшой локальный DNS-сервер, который ускоряет работу, кешируя ответы на повторяющиеся DNS-запросы.
- ❖ В этом случае в общесистемный **/etc/resolv.conf** помещается директива `nameserver 127.0.0.1`, а ip-адреса внешних DNS-серверов переносятся в настройки локального.



```
igor@debian: ~
GNU nano 5.4 /etc/resolv.conf
domain fb.local
search fb.local
nameserver 172.16.200.15
nameserver 172.16.200.17

[ Read 4 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute   ^C Location
^X Exit      ^R Read File  ^Y Replace    ^U Paste      ^J Justify   ^_ Go To Line
```

nano /etc/nsswitch.conf

- ❖ При использовании данного файла, сетями можно управлять по имени. Например добавить маршрут не `route add 192.168.1.12`, а **route add home-network**.
- ❖ Файл `/etc/nsswitch.conf` — это «Name Service Switch configuration file», то есть конфигурационный файл переключения служб имён. Он устанавливает настройки не только службы преобразования имён хостов и доменных имён, но эта настройка, пожалуй, самая востребованная.
- ❖ Строка, которая отвечает за преобразование имён хостов, начинается на **«hosts»**.

```
igor@debian: ~
GNU nano 5.4 /etc/nsswitch.conf
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.
passwd:      files systemd
group:       files systemd
shadow:      files
gshadow:     files

hosts:       files mdns4_minimal [NOTFOUND=return] dns myhostname
networks:    files

protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^_ Go To Line
```

nano /etc/nsswitch.conf

files означает файл, относящийся к этой службе. У каждой службы в системе свой файл, в данном случае имеется ввиду **/etc/hosts**.

Служба	Файлы
aliases	/etc/aliases
ethers	/etc/ethers
group	/etc/group
hosts	/etc/hosts
initgroups	/etc/group
netgroup	/etc/netgroup

Служба	Файлы
networks	/etc/networks
passwd	/etc/passwd
protocols	/etc/protocols
publickey	/etc/publickey
rpc	/etc/rpc
services	/etc/services
shadow	/etc/shadow

```

GNU nano 5.4 /etc/nsswitch.conf
# /etc/nsswitch.conf
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:      files systemd
group:       files systemd
shadow:      files
gshadow:     files

hosts:       files mdns4_minimal [NOTFOUND=return] dns myhostname
networks:    files

protocols:   db files
services:    db files
ethers:      db files
rpc:         db files

netgroup:    nis
  
```

nano /etc/sysconfig/network-scripts

Команда	Описание
/etc/sysconfig/network-scripts	Каталог, содержащий конфигурационные файлы интерфейсов и скрипты, выполняющие их инициализацию.
/etc/sysconfig/network-scripts/ifup	Скрипт, который выполняет настройку и активацию интерфейса.
/etc/sysconfig/network-scripts/ifdown	Скрипт, который выполняет деактивацию интерфейса.

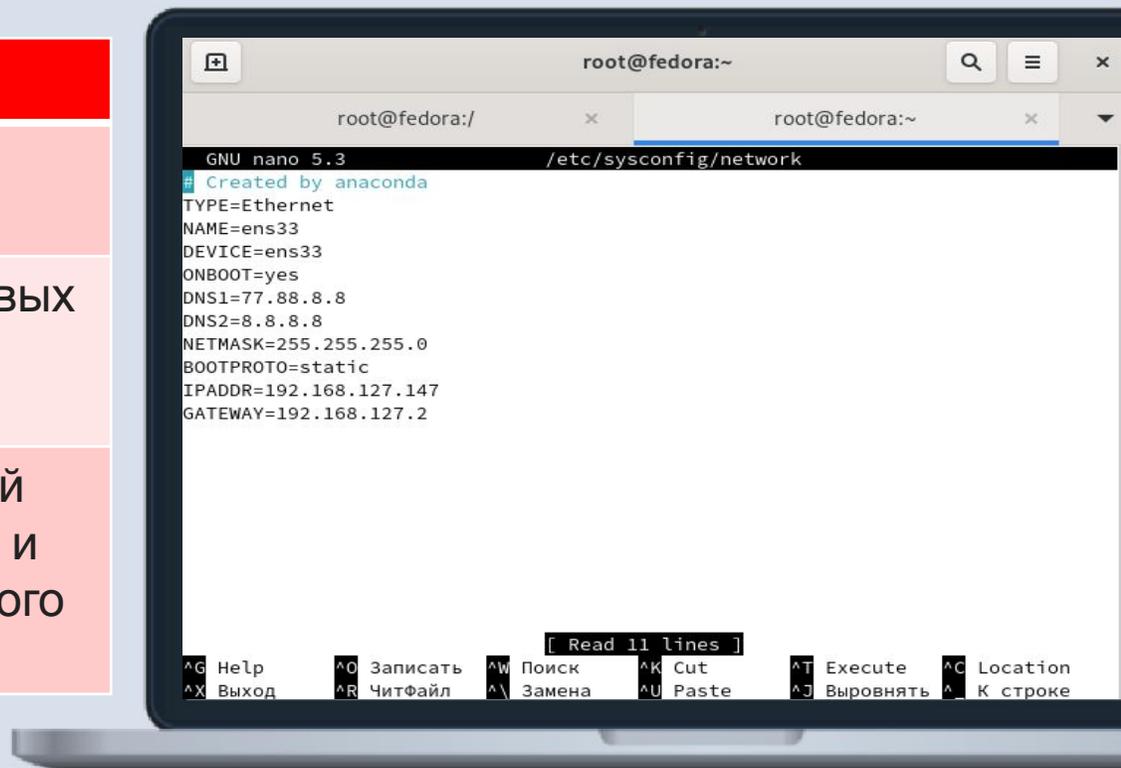
```

root@fedora:~
root@fedora:/
root@fedora:~
GNU nano 5.3 /etc/sysconfig/network
# Created by anaconda
TYPE=Ethernet
NAME=ens33
DEVICE=ens33
ONBOOT=yes
DNS1=77.88.8.8
DNS2=8.8.8.8
NETMASK=255.255.255.0
BOOTPROTO=static
IPADDR=192.168.127.147
GATEWAY=192.168.127.2

[ Read 11 lines ]
^G Help      ^O Записать  ^W Поиск     ^K Cut       ^T Execute   ^C Location
^X Выход     ^R ЧитФайл  ^\ Замена   ^U Paste     ^J Выровнять ^_ К строке
  
```

nano /etc/sysconfig/network-scripts

Команда	Описание
/etc/sysconfig/network-scripts/ifcfg-*	Конфигурационные файлы, описывающие интерфейсы системы.
/etc/init.d/network	Скрипт, выполняющий настройку сетевых интерфейсов и маршрутизации при загрузке.
/etc/sysconfig/network	Конфигурационный файл, содержащий имя хоста, IP-адрес основного шлюза и IP-адреса основного и вспомогательного DNS-серверов.



nano /etc/netplan/01-netcfg.yaml

❖ **Netplan** — это утилита для конфигурации сети. Настройка сети через Netplan выполняется в конфигурационном файле, который находится в папке **/etc/netplan/**. Это текстовый файл с расширением **.yaml**.

❖ **YAML** — это формат данных с простым синтаксисом. YAML использует систему отступов, в качестве которых выступают пробелы. При создании и редактировании конфигурационного файла такого формата легко ошибиться — указать неверное количество пробелов. Из-за этого возникнет ошибка “expected mapping” и файл будет невозможно прочитать.

```
# This file is generated from information provided by
# the datasource. Changes to it will not persist across an instance.
# To disable cloud-init's network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  renderer: networkd
  ethernets:
    ens160:
      addresses: []
      dhcp4: true
    ens192:
      dhcp4: no
      dhcp6: no
      addresses: [192.168.1.8/24]
      gateway4: 192.168.1.1
      nameservers:
        addresses: [8.8.8.8,8.8.4.4]
  version: 2
```

Перезапуск сервиса сети в Linux

Команда	Описание
<code>sudo netplan apply</code>	Перезагружаем сетевую службу в Ubuntu 18 и выше.
<code>sudo systemctl restart network</code>	Перезагружаем сетевую службу в Debian/CentOS-Fedora.

Утилита ip

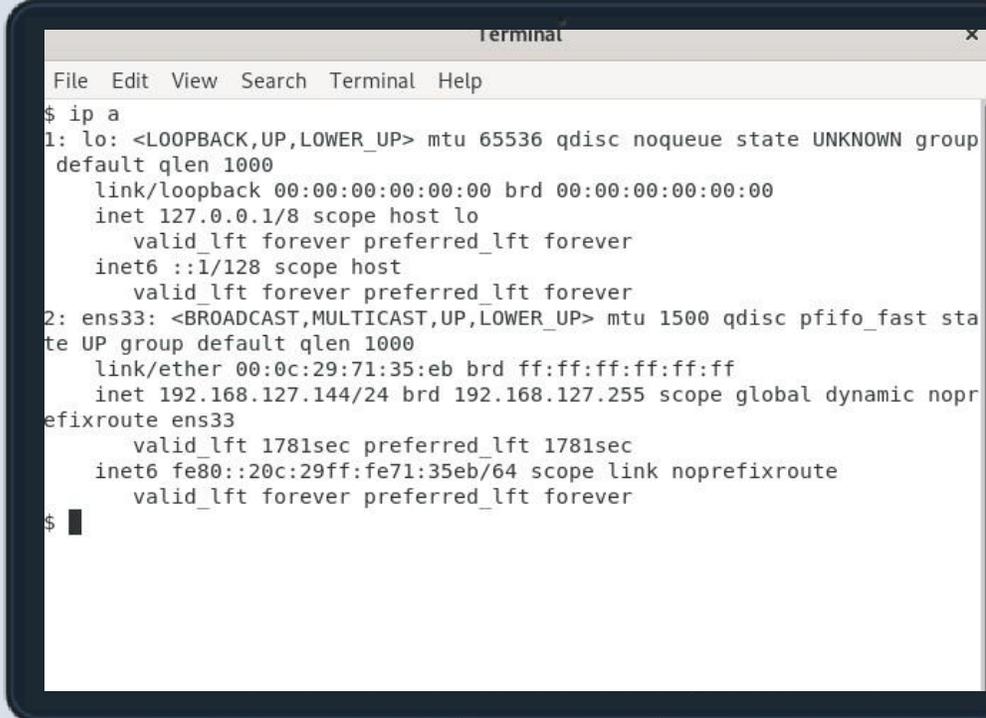
Команда ip — это мощный инструмент для настройки сетевых интерфейсов, который должен знать любой системный администратор Linux. Он используется для включения или выключения интерфейсов, назначения и удаления адресов и маршрутов, управления кэшем ARP и многого другого.



Утилита ip

Мы видим два IP-адреса, а также много другой информации. IP-адреса связаны с контроллерами сетевого интерфейса (NIC). Команда `ip` пытается быть полезной и предоставляет много информации об интерфейсе.

- ❖ **Первый IP-адрес** — это **(внутренний) петлевой** адрес, используемый для связи внутри компьютера.
- ❖ **Второй фактический (внешний)** IP-адрес, который компьютер имеет в локальной сети (LAN).



```
terminal
File Edit View Search Terminal Help
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
  default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
      valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
      valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast sta
  te UP group default qlen 1000
    link/ether 00:0c:29:71:35:eb brd ff:ff:ff:ff:ff:ff
    inet 192.168.127.144/24 brd 192.168.127.255 scope global dynamic nopr
  efixroute ens33
      valid_lft 1781sec preferred_lft 1781sec
    inet6 fe80::20c:29ff:fe71:35eb/64 scope link noprefixroute
      valid_lft forever preferred_lft forever
$
```

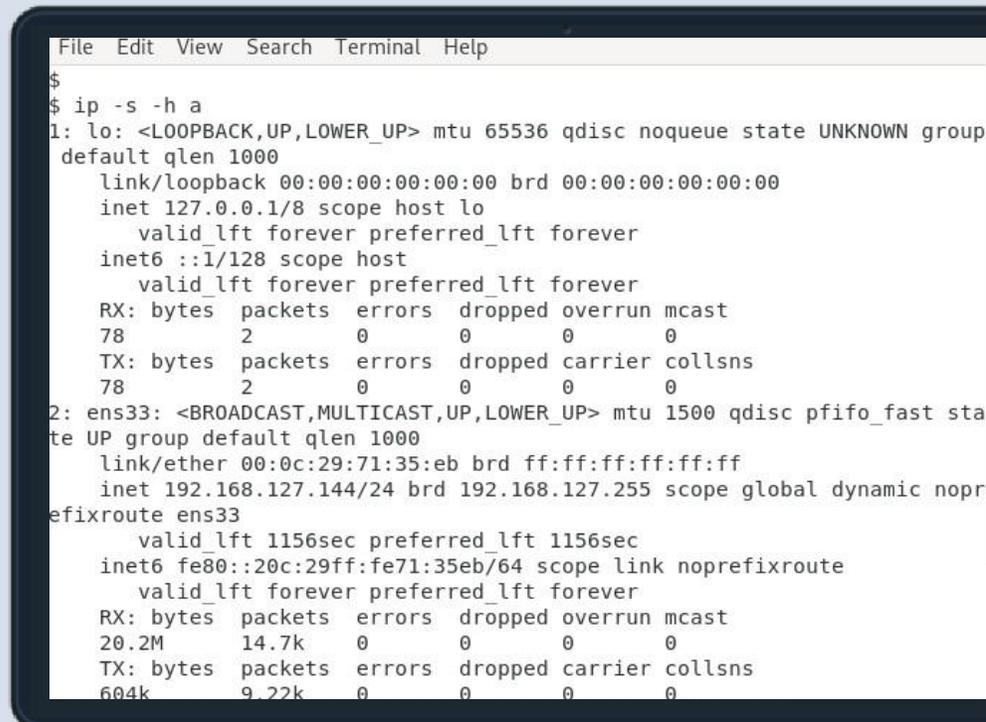
Как просмотреть статистику использования трафика сетевыми

интерфейсами?

Чтобы увидеть статистику полученных и отправленных данных каждым интерфейсом, используйте опцию **-s**.

Если вы хотите, чтобы данные выводились в удобном для восприятия виде, то укажите опцию **-h**.

Ip -s -h a



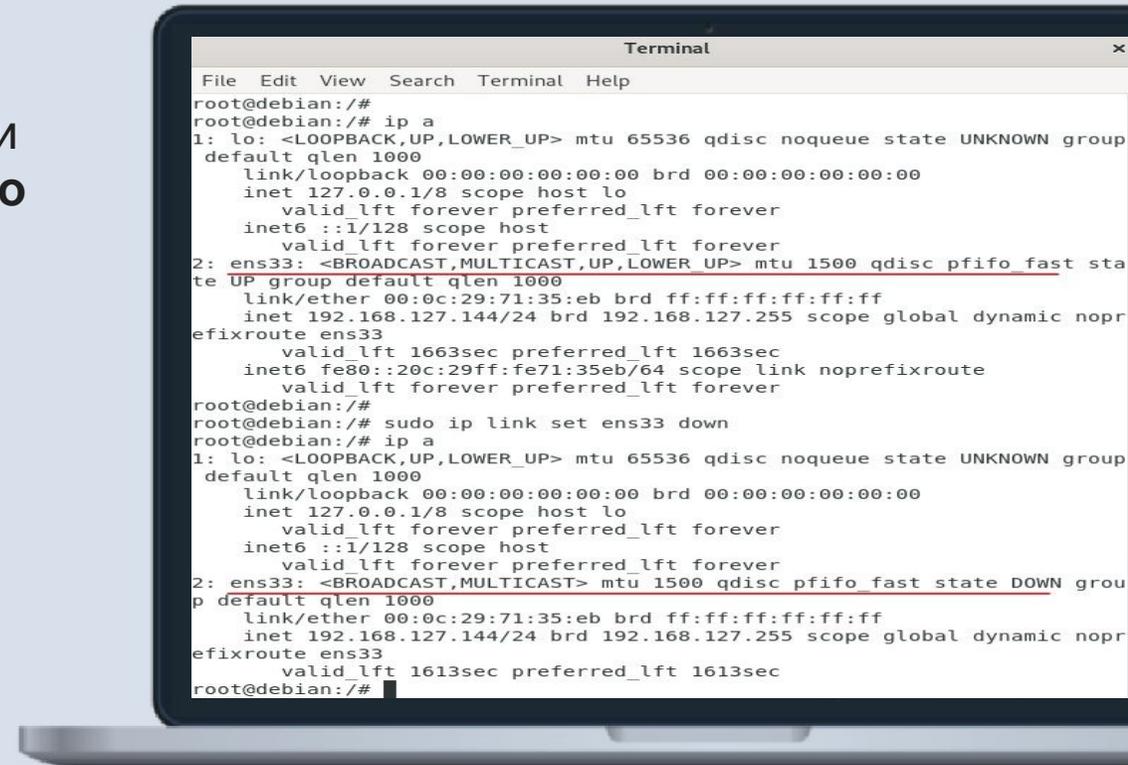
```
File Edit View Search Terminal Help
$
$ ip -s -h a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
default qlen 1000
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
  inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
  RX: bytes  packets  errors  dropped  overrun  mcast
  78          2         0       0        0        0
  TX: bytes  packets  errors  dropped  carrier  collsns
  78          2         0       0        0        0
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast sta
te UP group default qlen 1000
  link/ether 00:0c:29:71:35:eb brd ff:ff:ff:ff:ff:ff
  inet 192.168.127.144/24 brd 192.168.127.255 scope global dynamic nopr
efixroute ens33
    valid_lft 1156sec preferred_lft 1156sec
  inet6 fe80::20c:29ff:fe71:35eb/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
  RX: bytes  packets  errors  dropped  overrun  mcast
  20.2M      14.7k    0       0        0        0
  TX: bytes  packets  errors  dropped  carrier  collsns
  604k       9.22k   0       0        0        0
```

Включение / остановка сетевого интерфейса

❖ Вы можете использовать опцию **set** с опцией **up** или **down** для включения или остановки сетевого интерфейса. Вы также должны использовать **sudo** как показано ниже:

sudo ip link set ens33 down

sudo ip link set ens33 up



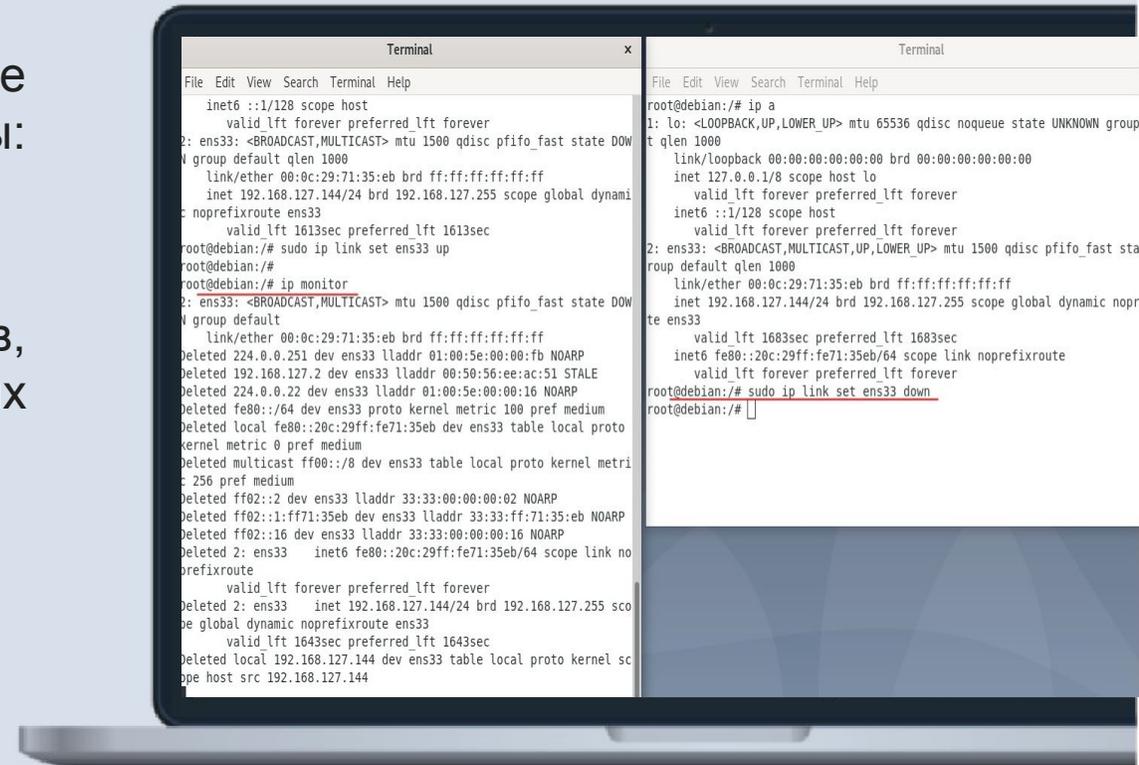
```
Terminal
File Edit View Search Terminal Help
root@debian:/#
root@debian:/# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
  default qlen 1000
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
  inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast sta
  te UP group default qlen 1000
  link/ether 00:0c:29:71:35:eb brd ff:ff:ff:ff:ff:ff
  inet 192.168.127.144/24 brd 192.168.127.255 scope global dynamic nopr
  efixroute ens33
    valid_lft 1663sec preferred_lft 1663sec
  inet6 fe80::20c:29ff:fe71:35eb/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
root@debian:/#
root@debian:/# sudo ip link set ens33 down
root@debian:/# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group
  default qlen 1000
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
  inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast state DOWN grou
  p default qlen 1000
  link/ether 00:0c:29:71:35:eb brd ff:ff:ff:ff:ff:ff
  inet 192.168.127.144/24 brd 192.168.127.255 scope global dynamic nopr
  efixroute ens33
    valid_lft 1613sec preferred_lft 1613sec
root@debian:/#
```

Мониторинг событий сетевых интерфейсов

- ❖ Всё, что происходит с сетевыми интерфейсами в режиме реального времени можно наблюдать с помощью команды:

ip monitor

- ❖ Эта команда покажет удаление и добавление маршрутов, изменение IP адресов, включение и отключение сетевых устройств и другие события.



Спасибо за внимание

