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.

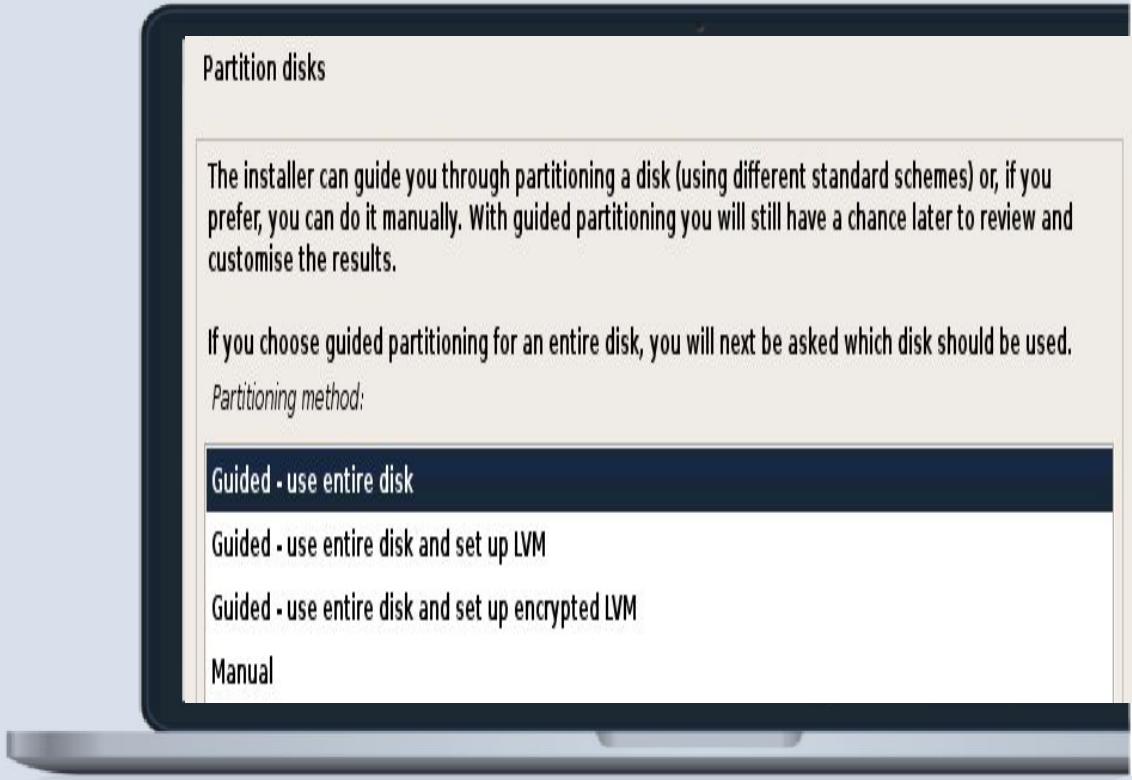
- В процессе установки нам предложат выбрать язык и регион, а также придумать надежный пароль для обычных пользователей и суперпользователя.

Разметка диска

Автоматическая разметка диска обычно подходит для большинства сценариев.

Осуществить разбиение диска можно 2 способами:

- Guided (автоматически)
- Manual (вручную)

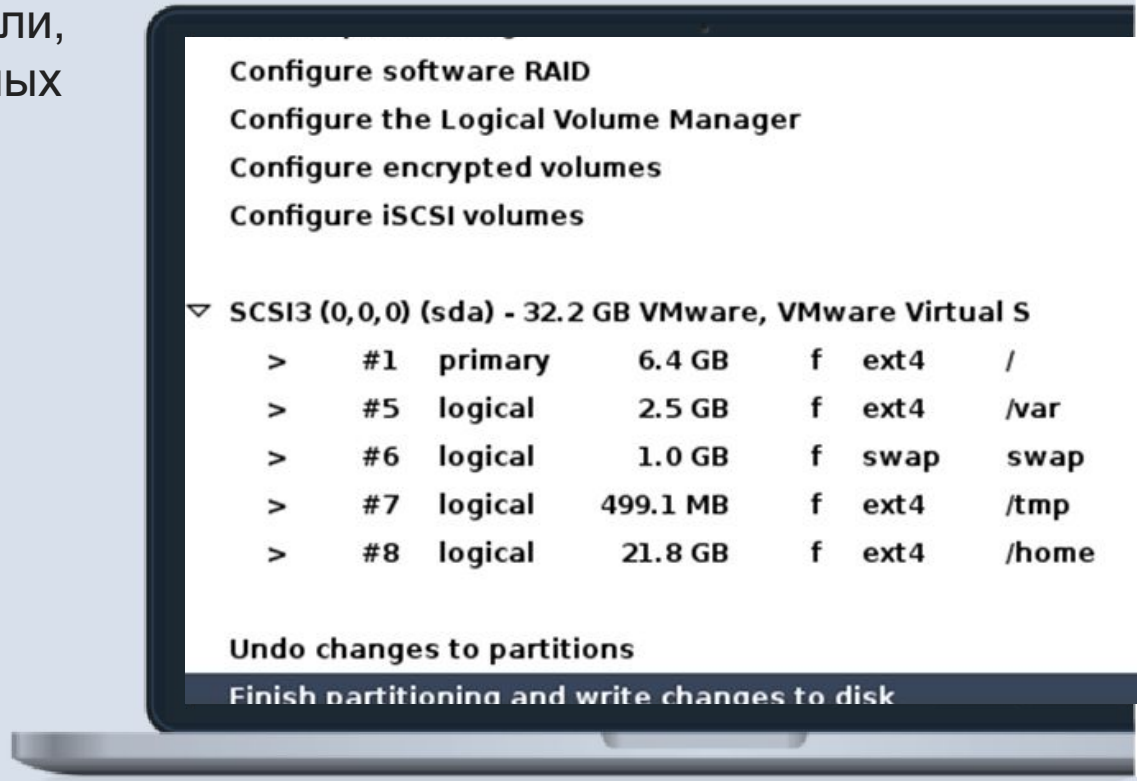


Ручная разметка

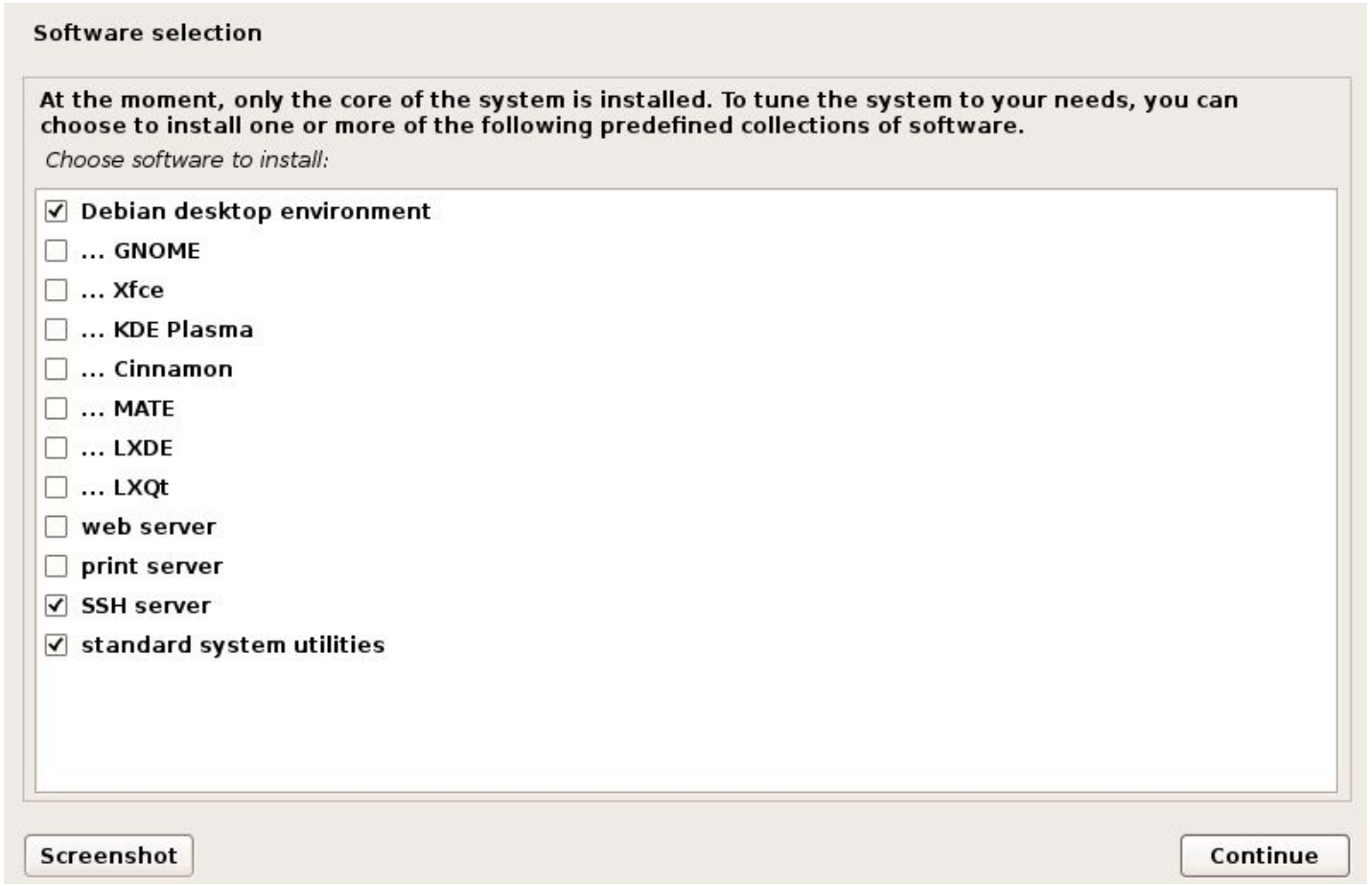
Однако впоследствии может возникнуть необходимость самостоятельно выбирать размеры для разделов или, например, создать отдельные разделы для тех или иных задач. Для этого нужно выбрать ручную разметку.

Здесь нужно будет указать:

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



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

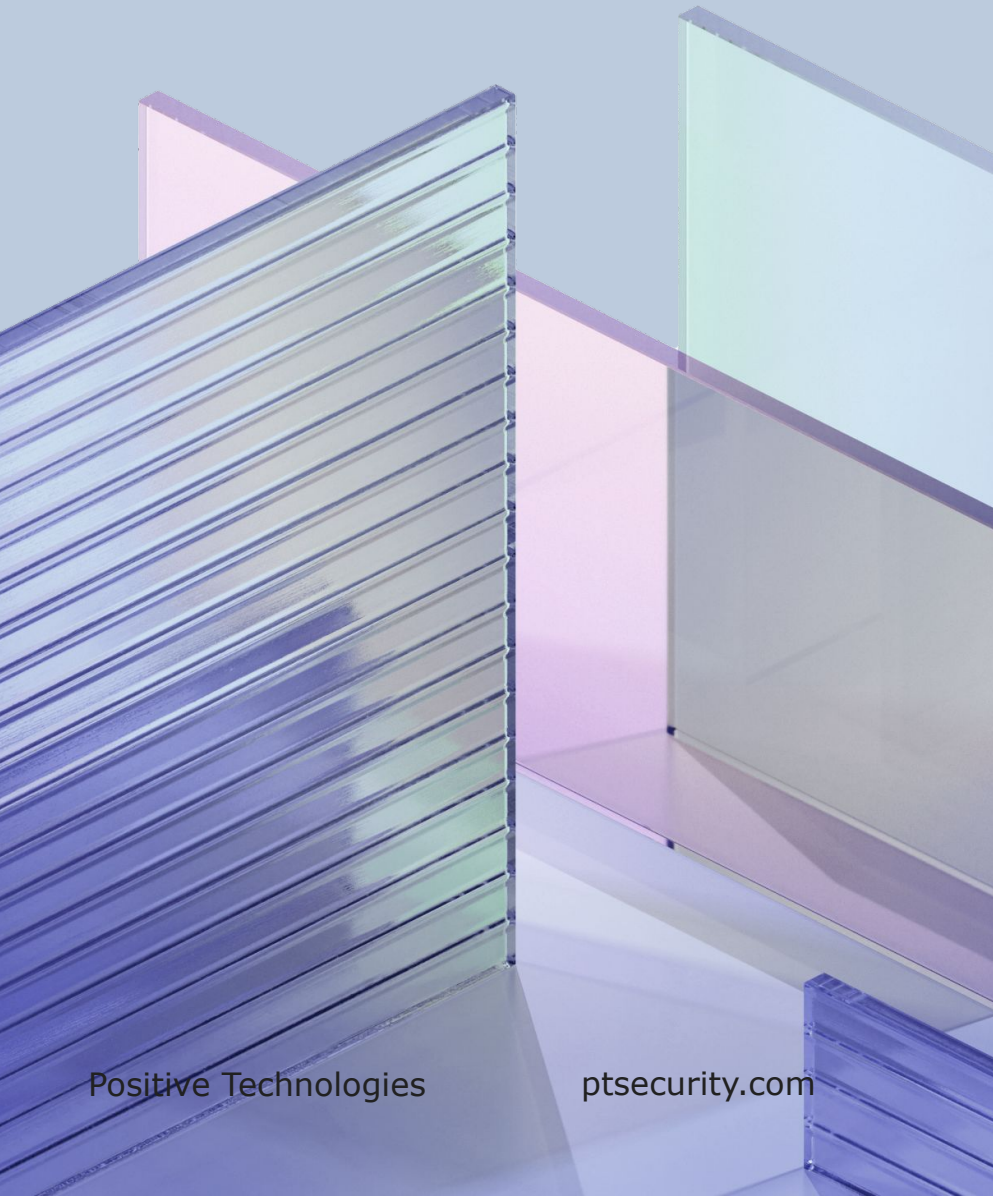
- Они создаются системным администратором. Каждый пользователь имеет числовой идентификатор пользователя, называемый UID.

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:~$
```

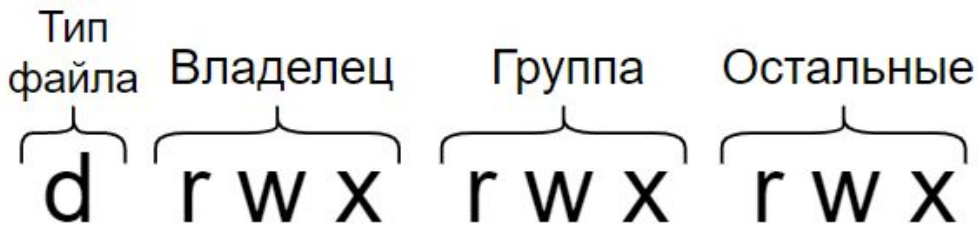
Типы файлов

- 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 является 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

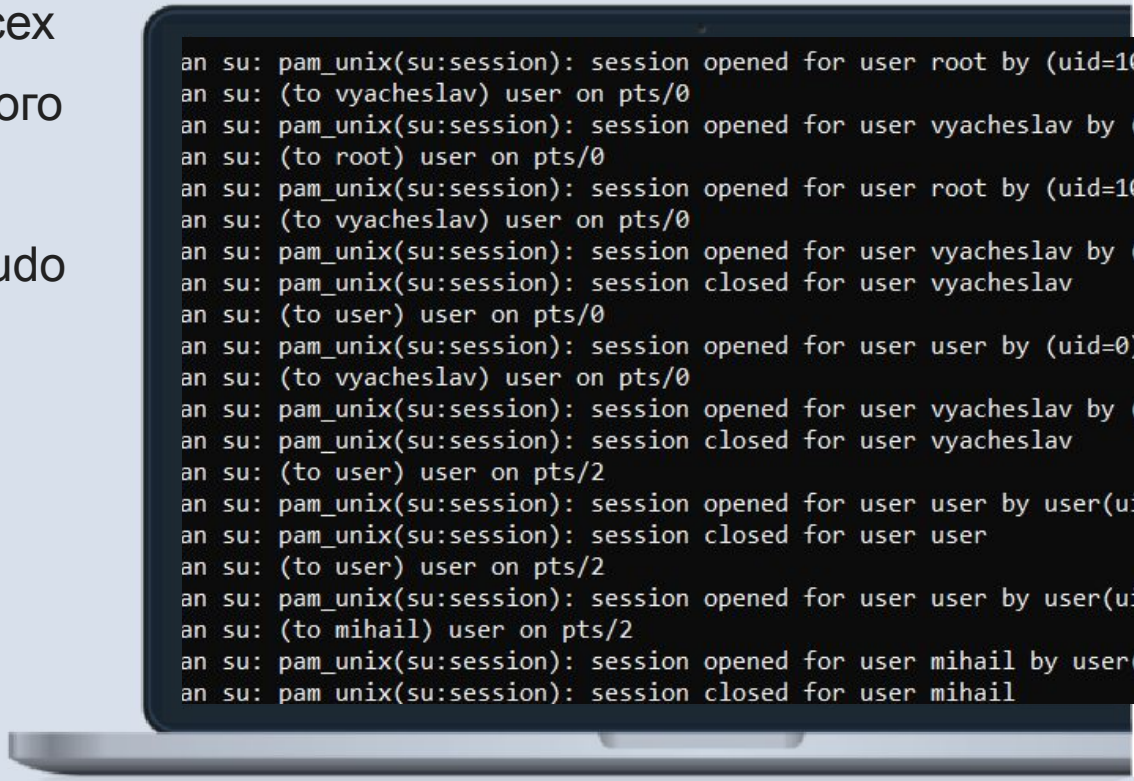
- Когда процесс создает новый файл, он указывает, какие права доступа нужно задать для данного файла. Зачастую запрашиваются права 0666 (чтение и запись всеми), что дает больше разрешений, чем необходимо в большинстве случаев. Система использует значение umask чтобы понизить изначально задаваемые разрешения 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=rx,o=rx
```

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.



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

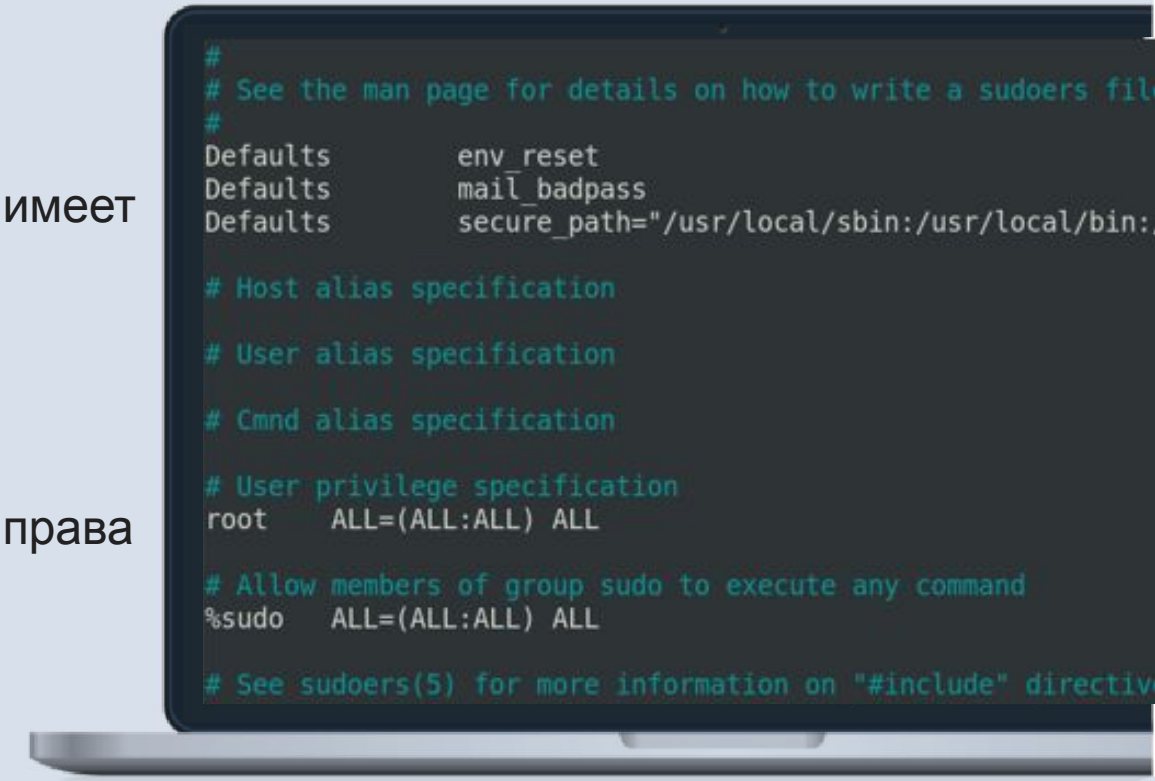
В **sudoers** хранится список пользователей, с указанием того, что они могут выполнять. Для редактирования файла sudoers нужно пользоваться командой «visudo».

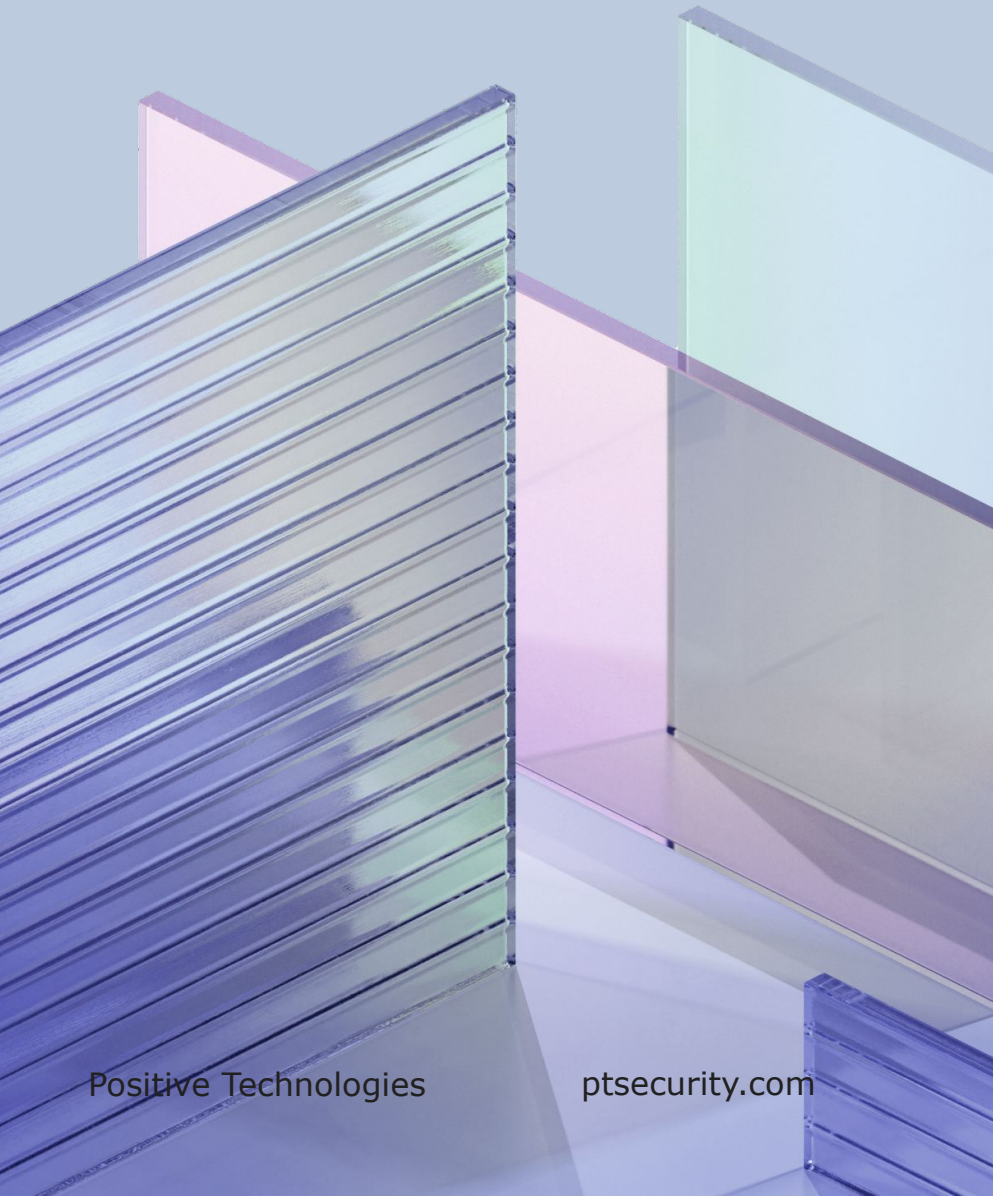
- **root ALL = (ALL:ALL) ALL**

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.





Строки привилегий

root ALL = (ALL:ALL) ALL

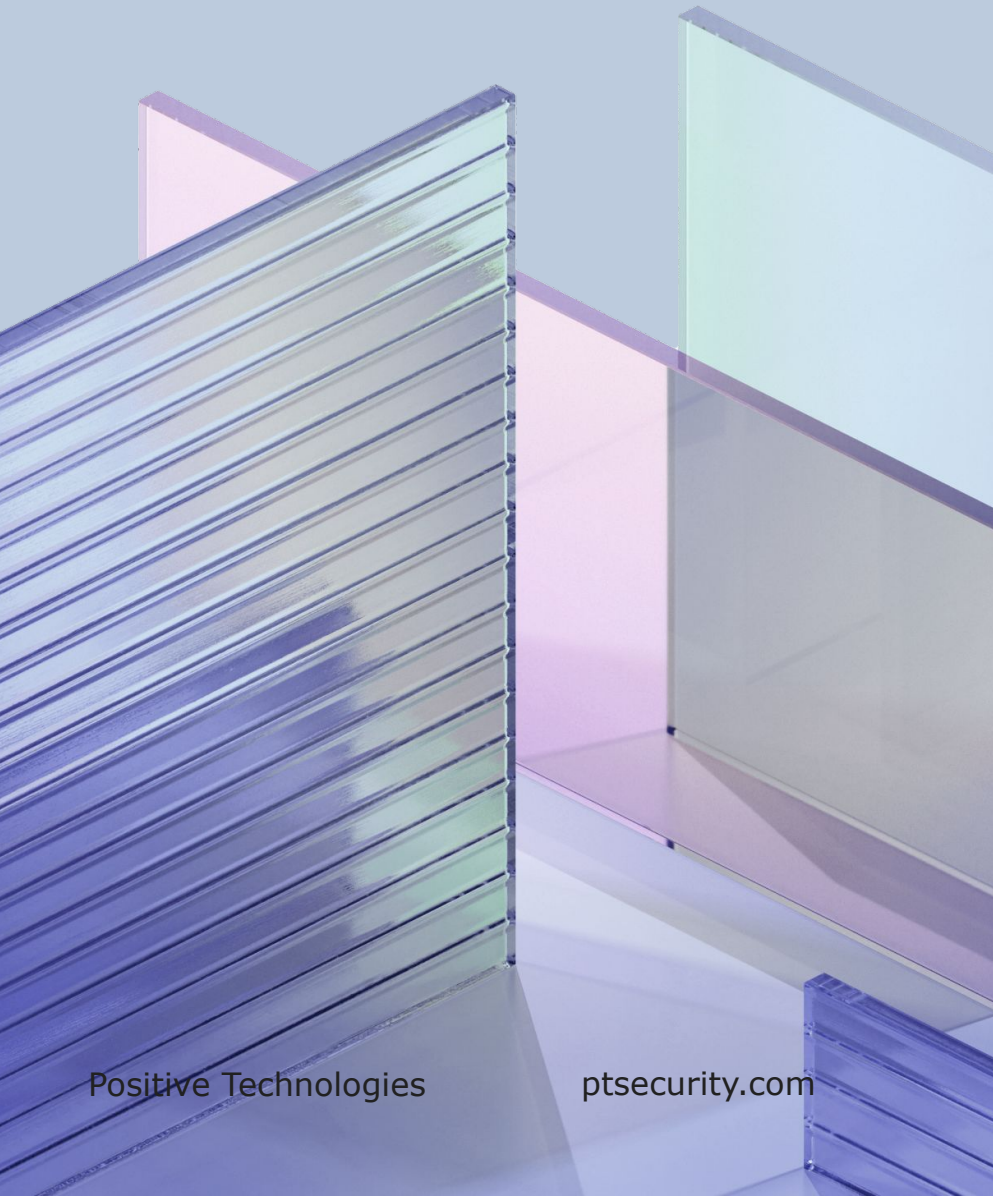
- **Первое поле** показывает имя пользователя.
- **Первое ALL** означает, что данное правило применяется ко всем хостам.
- **Второе ALL** означает, что пользователь root может запускать команды от лица всех пользователей.
- **Третье ALL** означает, что пользователь root может запускать команды от лица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



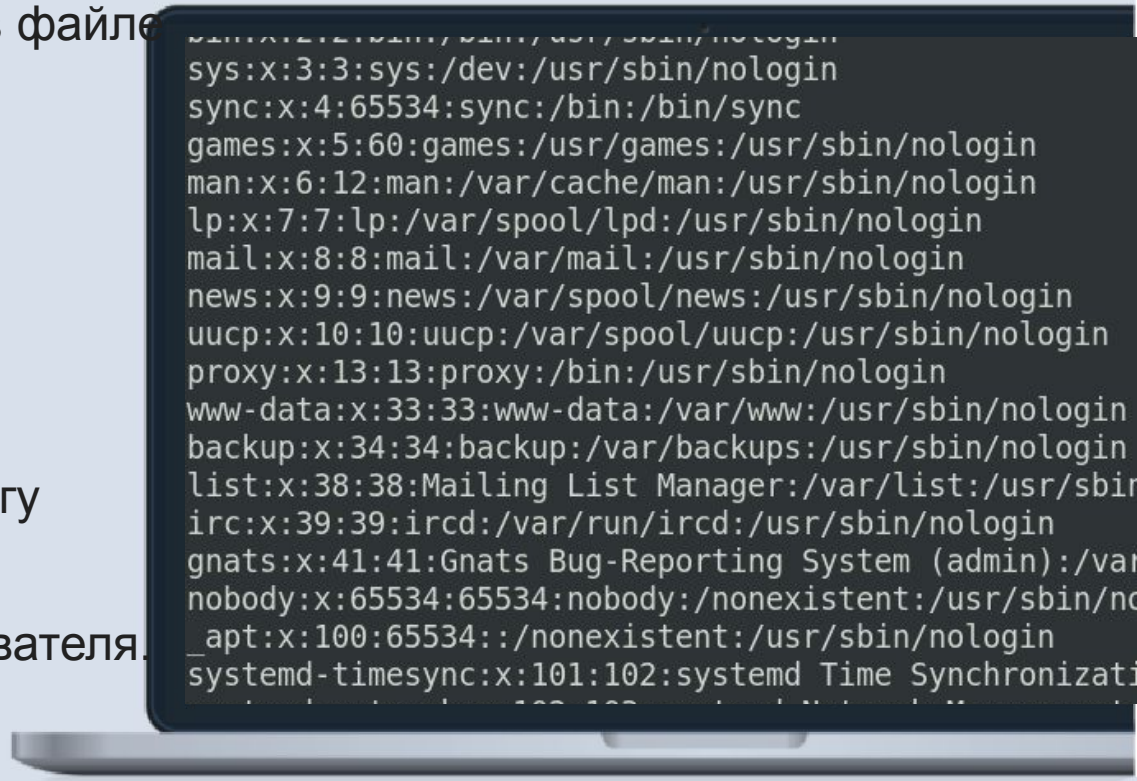
/etc/passwd/

- 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.



/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.

/etc/shadow

```
colord:*:19100:0:99999:7:::
geoclue:*:19100:0:99999:7:::
Debian-gdm:*:19100:0:99999:7:::
user:$6$sBsn.E5Wb7q3wlry$MJxmSUG8lQ1.1LK6dZRnN9fSbR7C.S7ZWwKgsyc97xBs8CDxqXsR/c4qoRzpfcfpTk0Fjmpp3buAEOXe4WoCI1:19100:0:99999:7:::
systemd-coredump:!!:19100::::::
vyacheslav:$6$GTlaPeCA4eVLs7sp$SQtH7DYMxl13PJf8eByb5u/2H.CVySKeuHCO9tMGVljuJsNMXMbFaL042tAsHL0onq4oiHRofU3EE.bHtUY5q1:19100:0:99999:7:::
mihail:$6$0RCxN0GXBdorojLF$SPMLhUxLXIYRPDAWSbfds7fbXdAlHRqJEJoZjIFdeyPM9wOBQX/yc4XMrKkzPdWf7nSpF8EoG209gSr8TLZtX1:19101:0:99999:7:::
ivanov:$6$tf2XjGqdiHPcnZ5e$lLqvXARcVmcqZnw88INcYbuiGW/FPLZ5C4qkWr382LHQfKJQvzUNwTZbLRVjHry4kWq.DUr0sH4JZVxNqvtJO/:19101:0:99999:7:::
```

Как и в **/etc/passwd**, каждая строка в **/etc/shadow** представляет информацию о пользователе. Строки состоят из различных стандартных полей, показанных ниже, каждое из которых разделено двоеточием:

- Имя пользователя.
- Зашифрованный пароль.
- Количество дней, прошедших с 1 января 1970 г., когда последний раз меняли этот пароль.
- Количество дней до того, как пароль может быть изменен.
- Количество дней, по истечении которых пароль необходимо изменить.
- За сколько дней до истечения срока действия пароля пользователь получает предупреждение.
- Через сколько дней после истечения срока действия пароля эта учетная запись будет отключена.
- Дней с 1 января 1970 г., когда эта учетная запись была отключена.
- Зарезервированное поле.

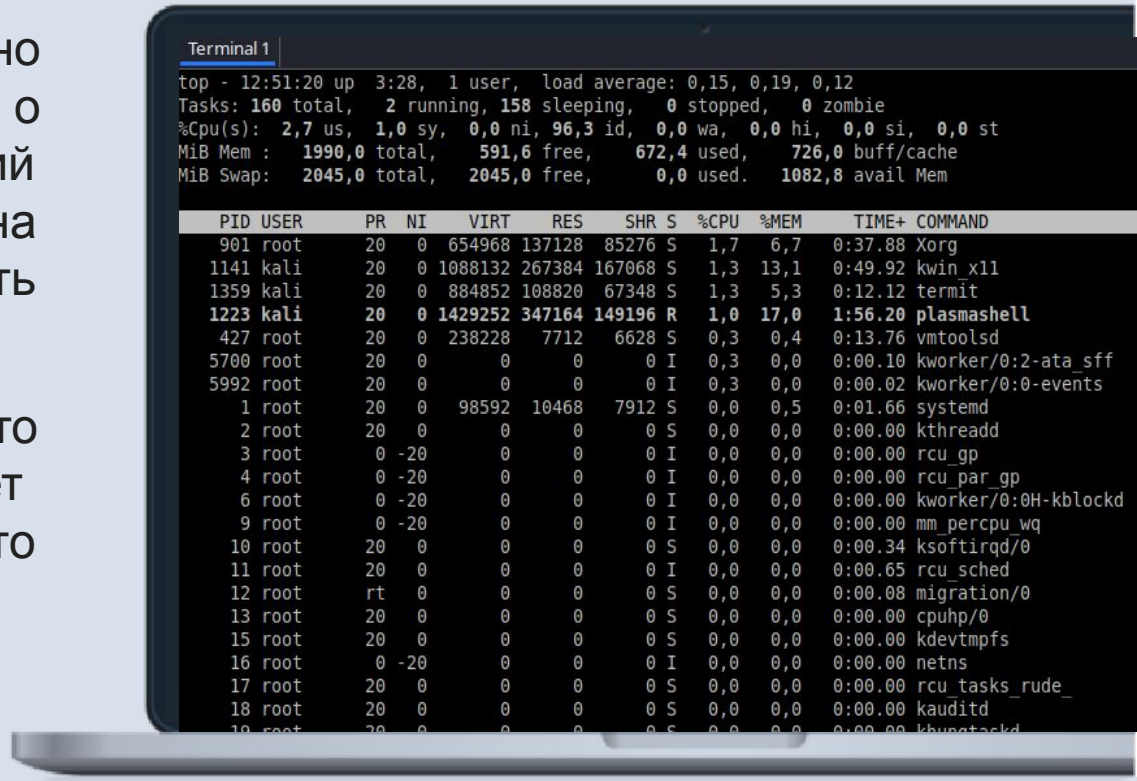
OS Linux

Тема 2. Администрирование Linux

Мониторинг Linux

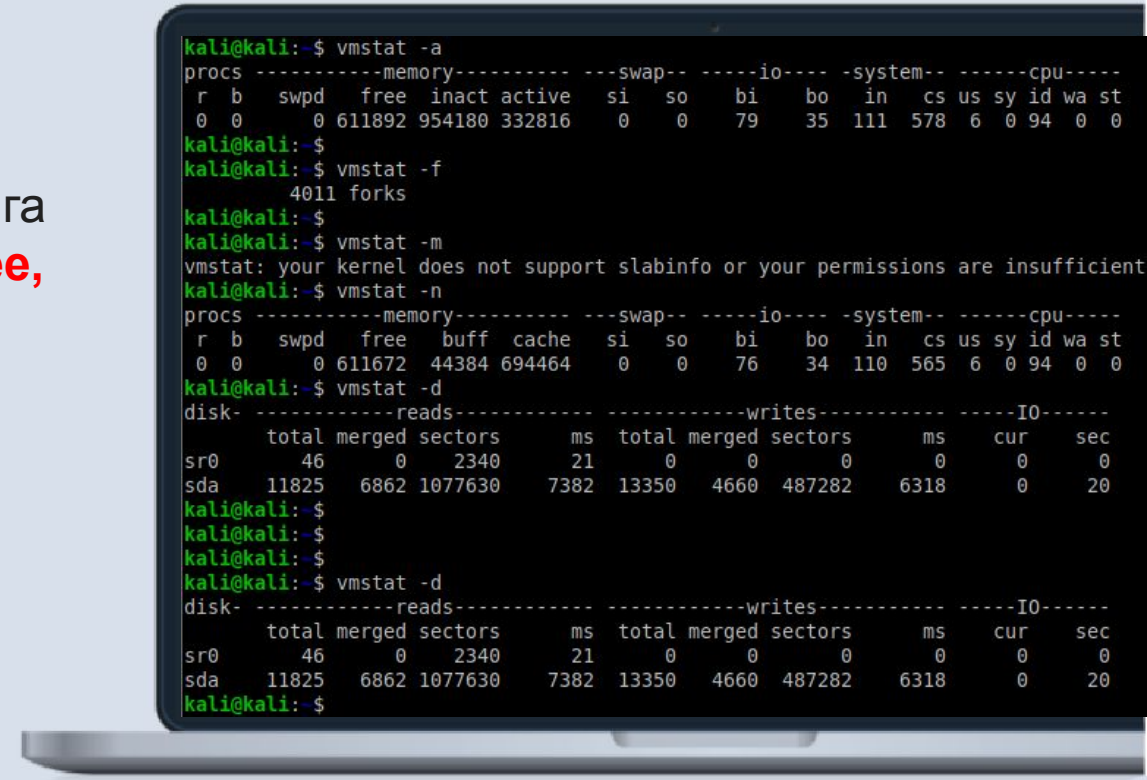
Мониторинг OS Linux

- 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.



Мониторинг OS Linux

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

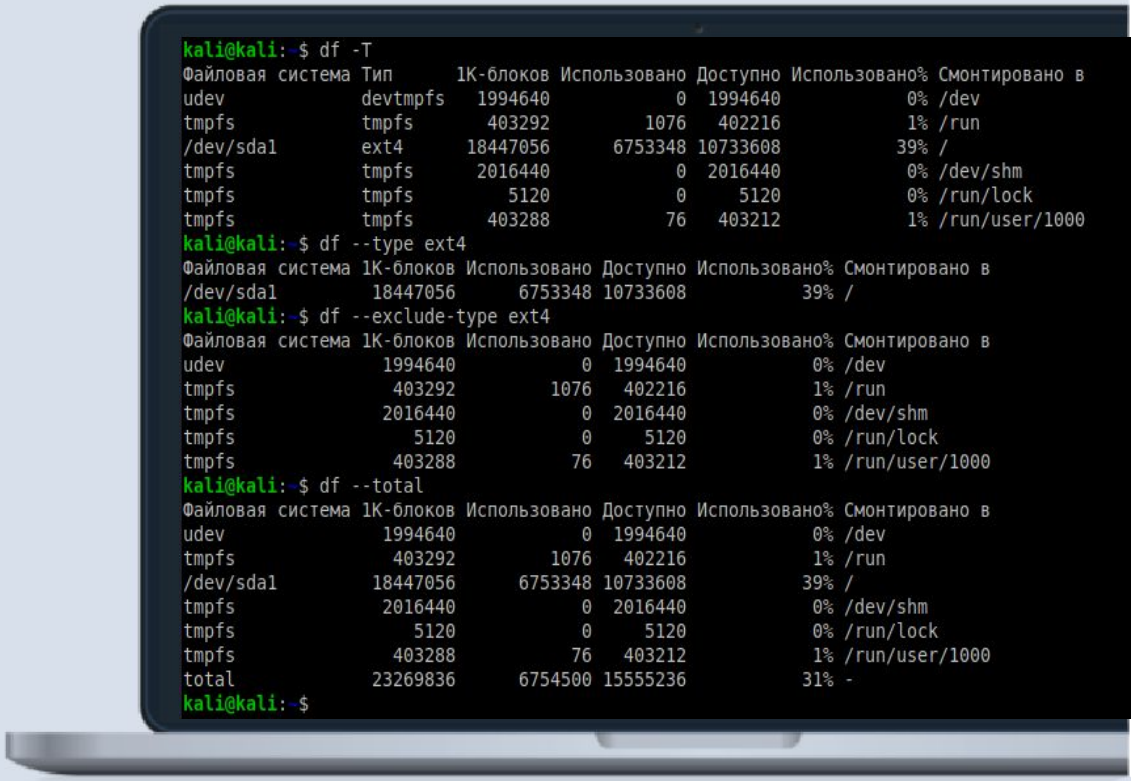


Мониторинг OS Linux

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.

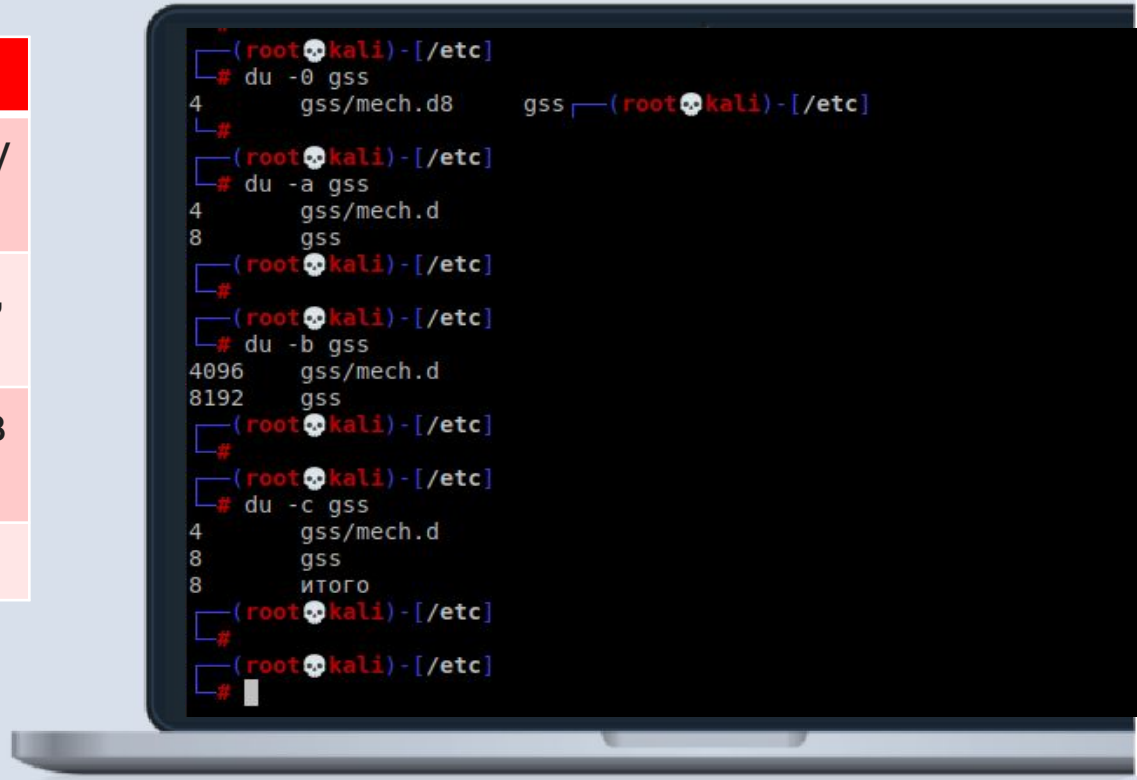
df

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.



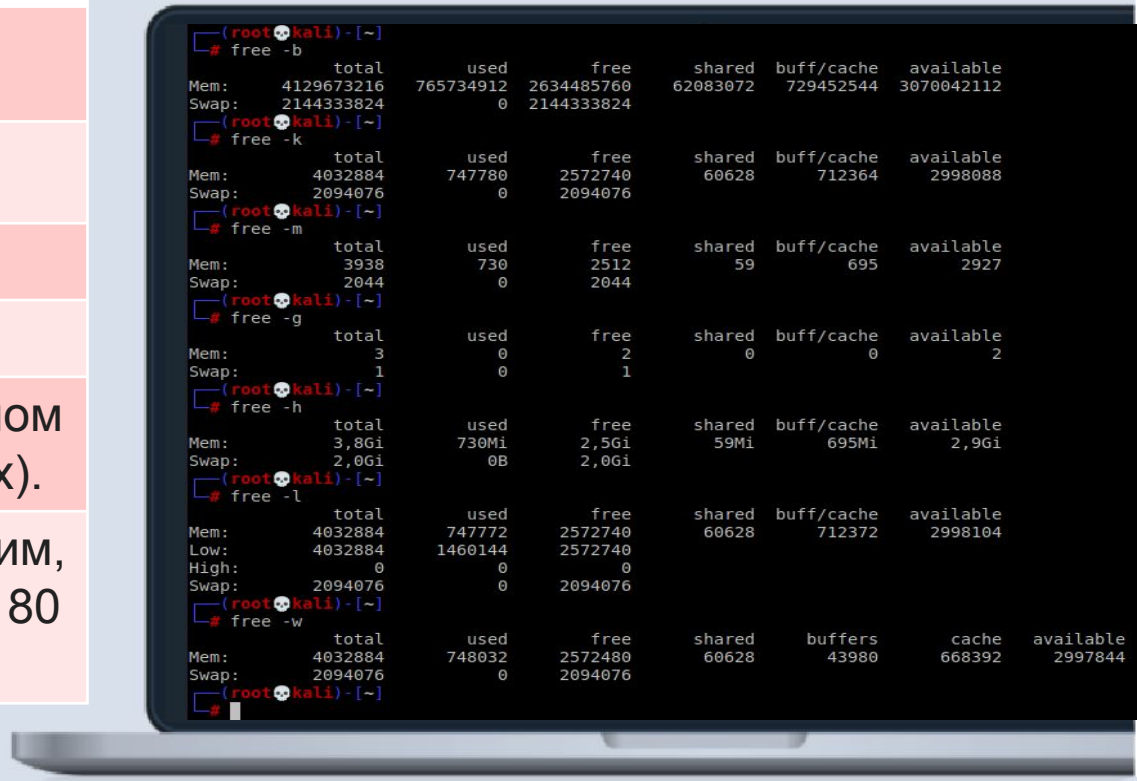
du

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



free

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

mpstat

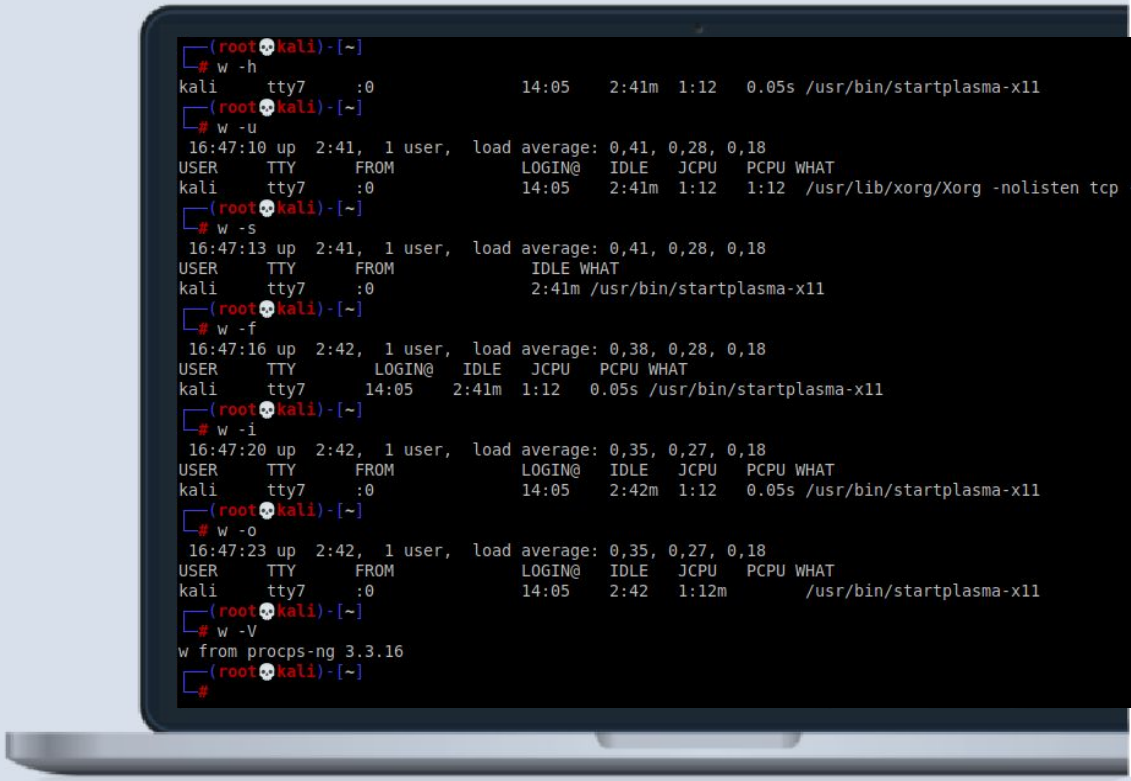
Команда	Описание
mpstat –A	Показывает всю информацию, которая может быть отображена с помощью команды «mpstat» о процессоре.
mpstat –P ALL	Параметр «-P ALL» покажет все индивидуальные процессоры или ядра вместе со статистикой.
mpstat –P 0	Для отображения статистически о конкретном CPU или ядре, используйте опцию -P.
mpstat –V	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.

W

Команда	Описание
w –h	Не выводить заголовок 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 –I	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.



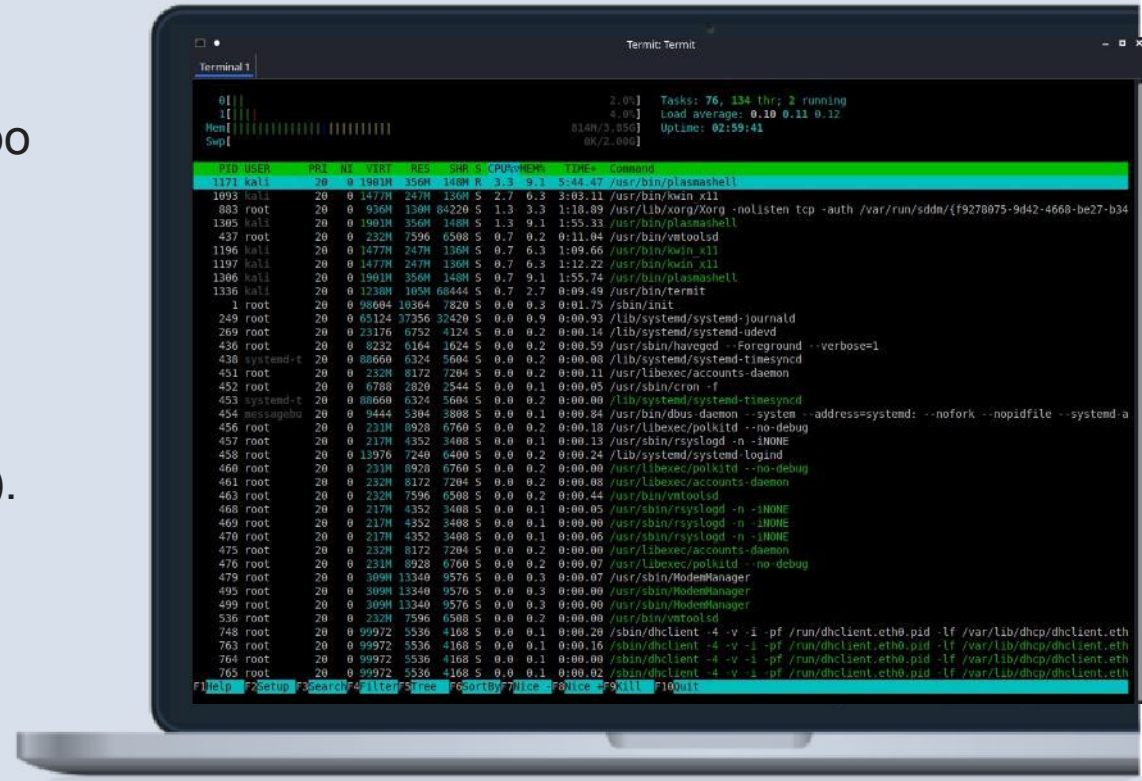
htop

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

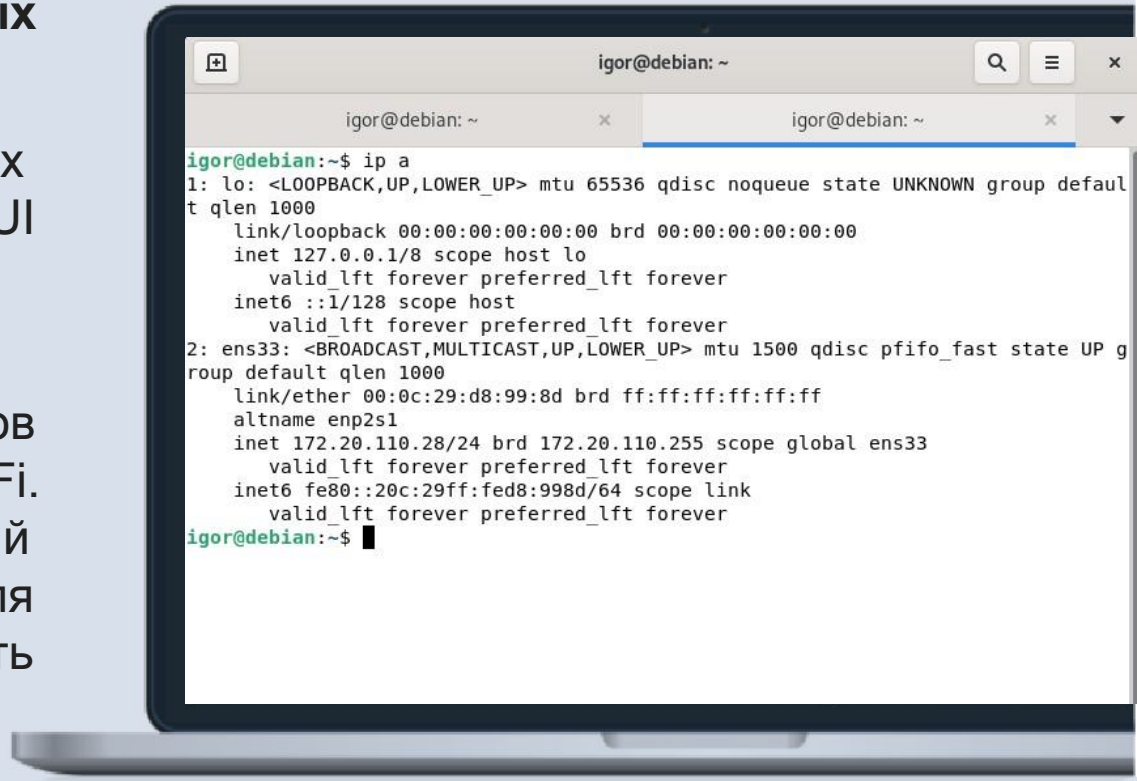
Конфигурация сети

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.



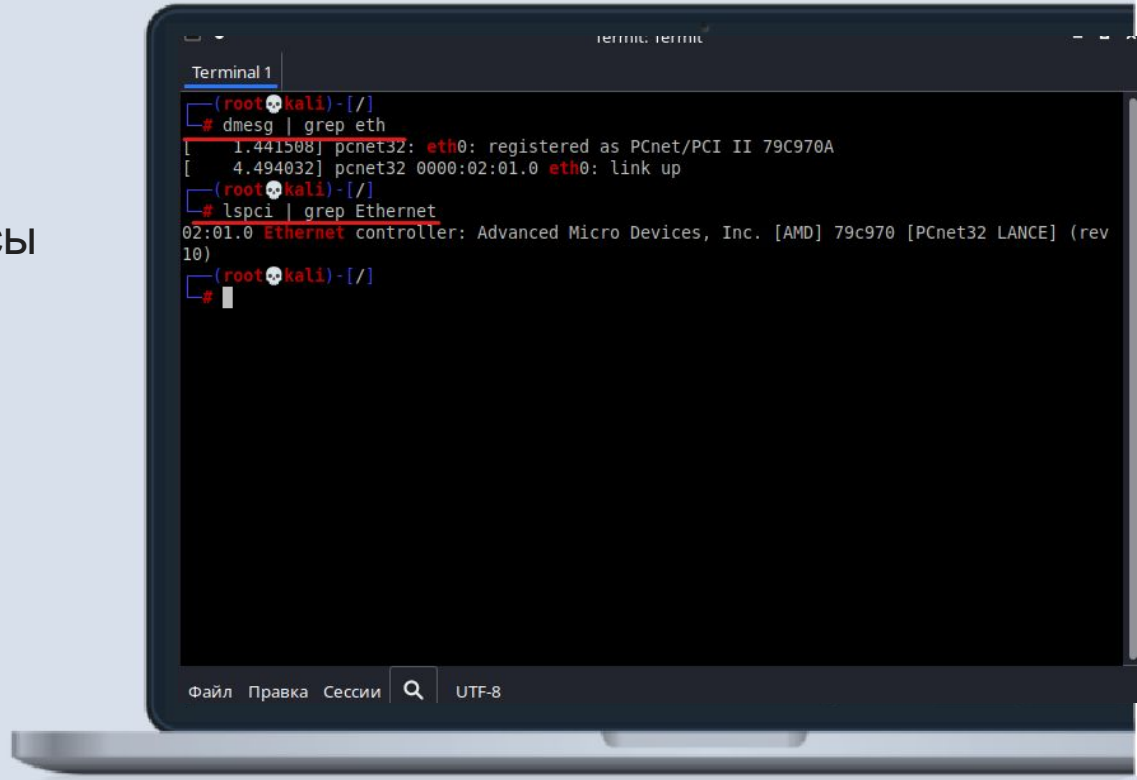
Параметры сети в Linux

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**

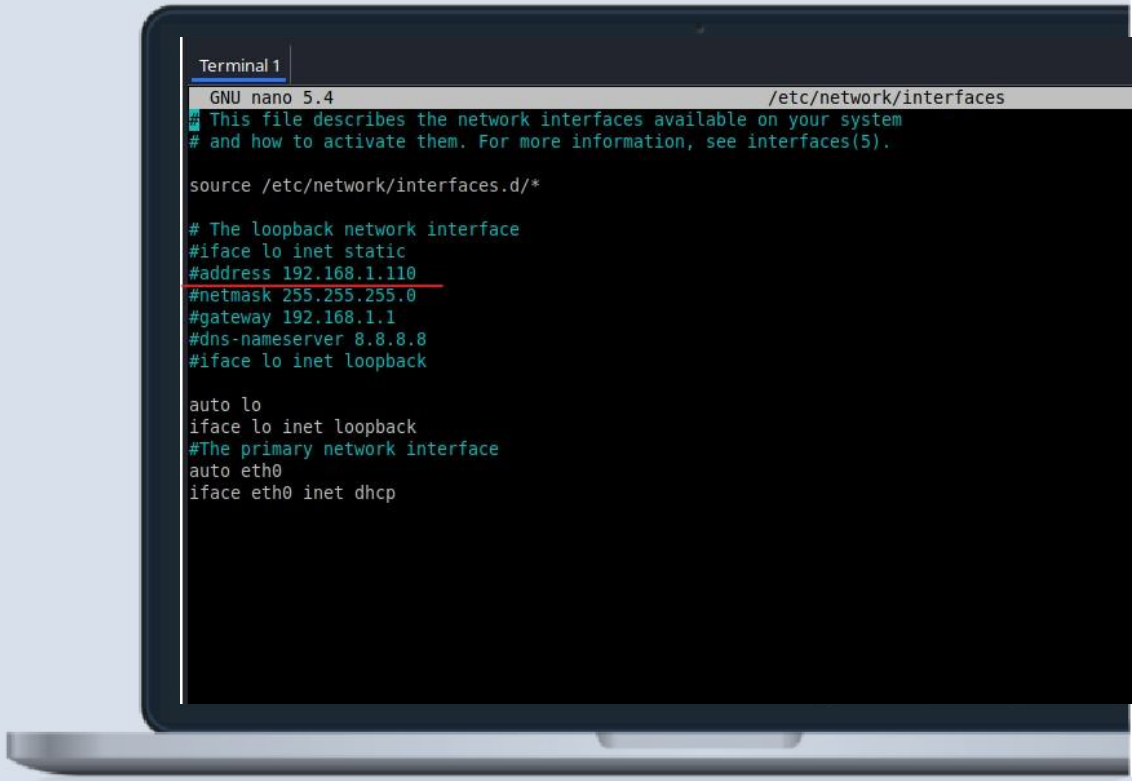


IP-адрес

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

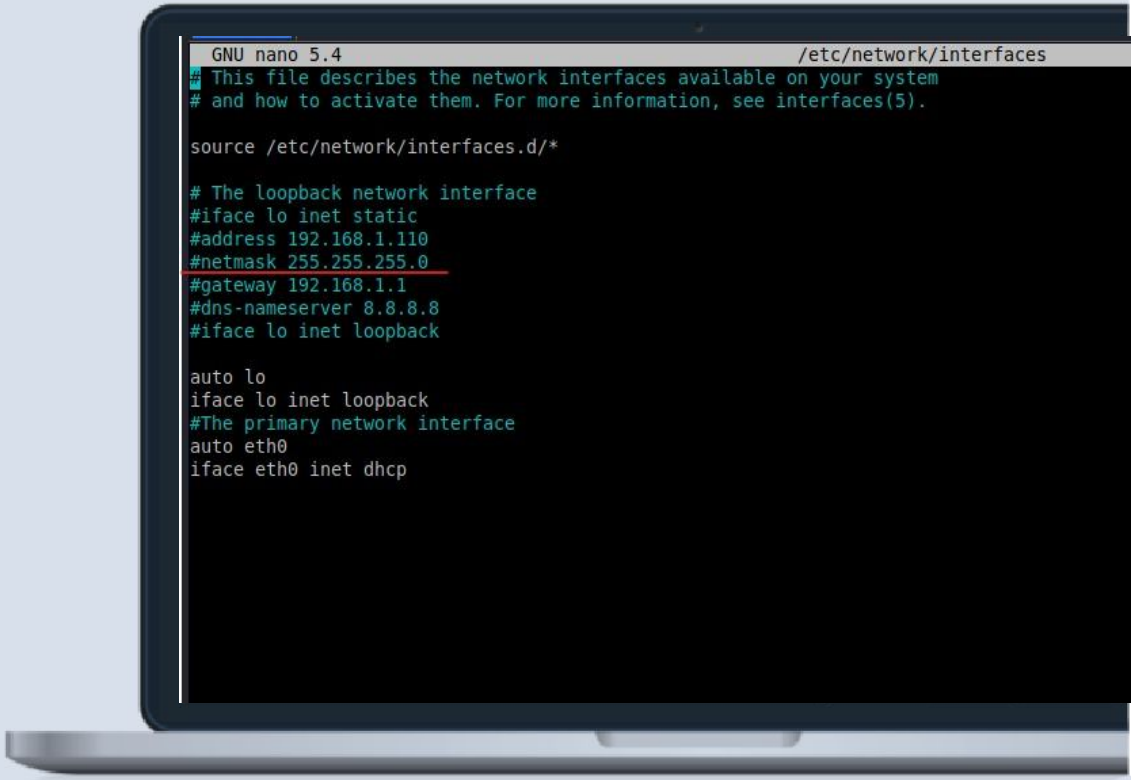


Маска подсети

Маска подсети - так же, 4 десятичных числа, определяющие, какая часть адреса относиться 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.

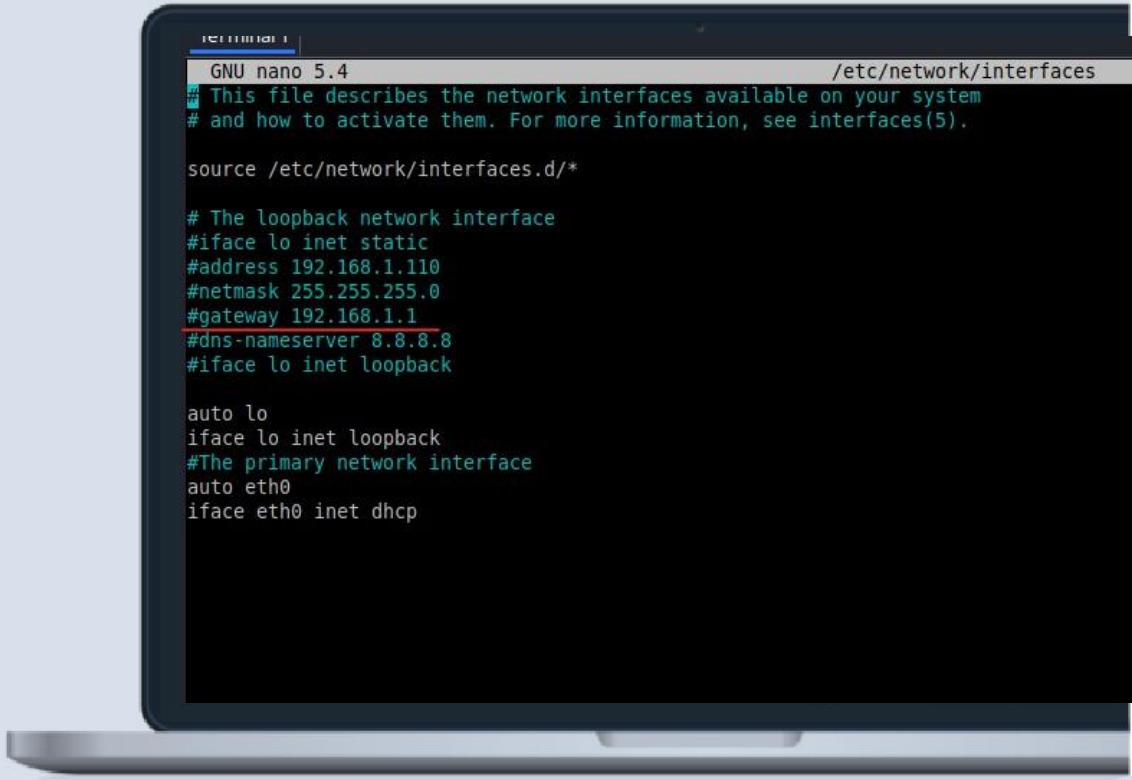
Например, адрес 192.168.0.2 с маской 255.255.255.0 принадлежит подсети 192.168.0.



IP-адрес шлюза

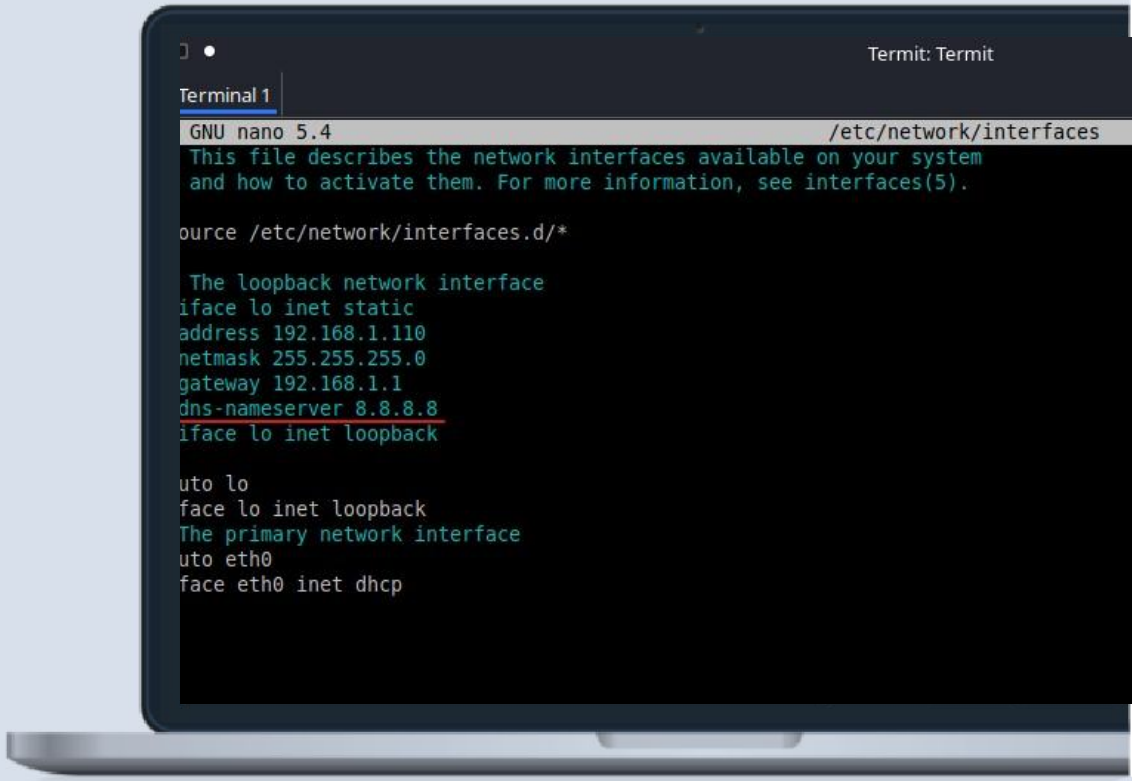
IP-адрес шлюза - это адрес машины, являющейся шлюзом по-умолчанию для связи с внешним миром. Шлюзов может быть несколько, если компьютер подключен к нескольким сетям одновременно.

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



IP-адрес сервера имен (DNS-сервера)

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

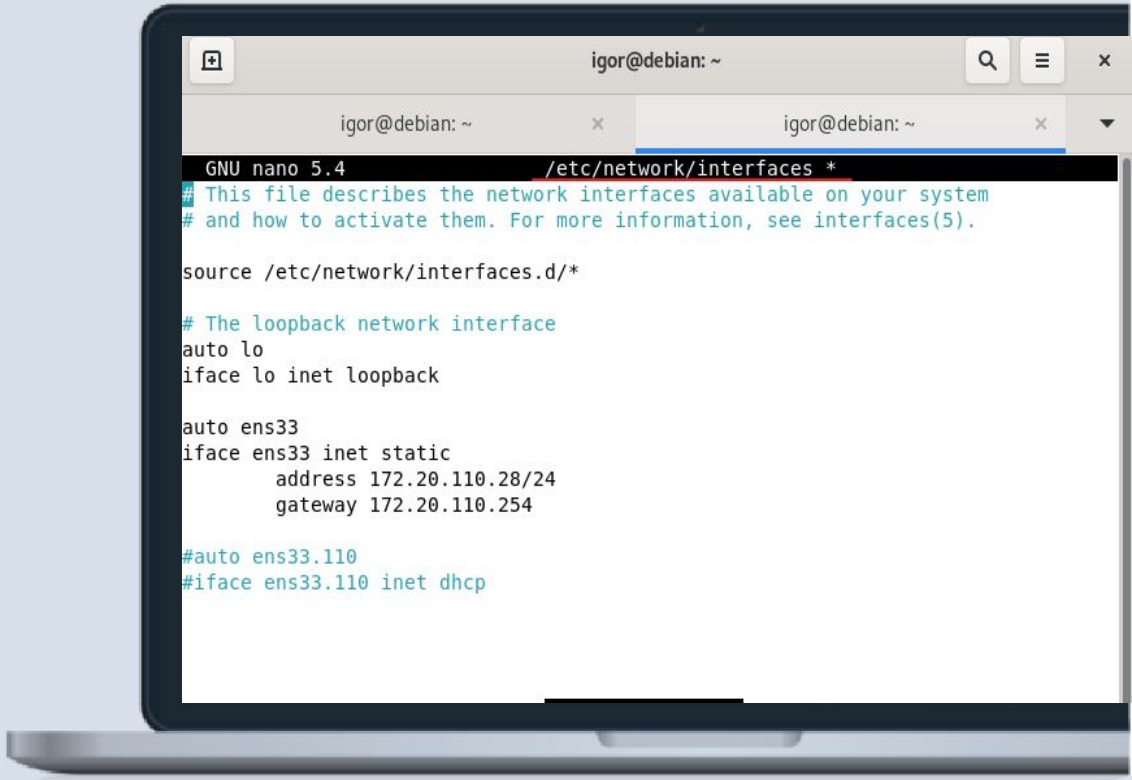


Параметры сети в Linux

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

nano /etc/network/interfaces

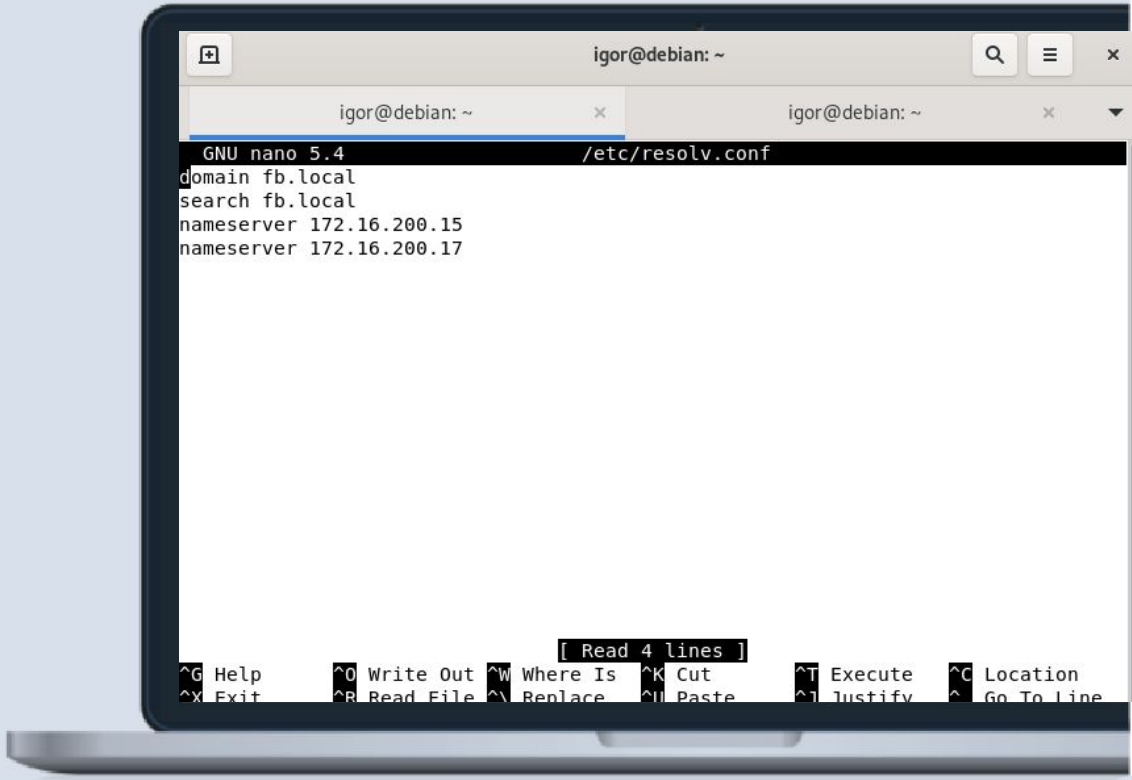
- Файл **/etc/network/interfaces** является **основным файлом настроек сетевых интерфейсов**, соответствующих сетевым картам, в дистрибутивах Debain/Ubuntu.
- Интерфейс **loopback** определяется системой как **lo** и по умолчанию задает адрес 127.0.0.1. Он может быть выведен командой **ifconfig**.



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.

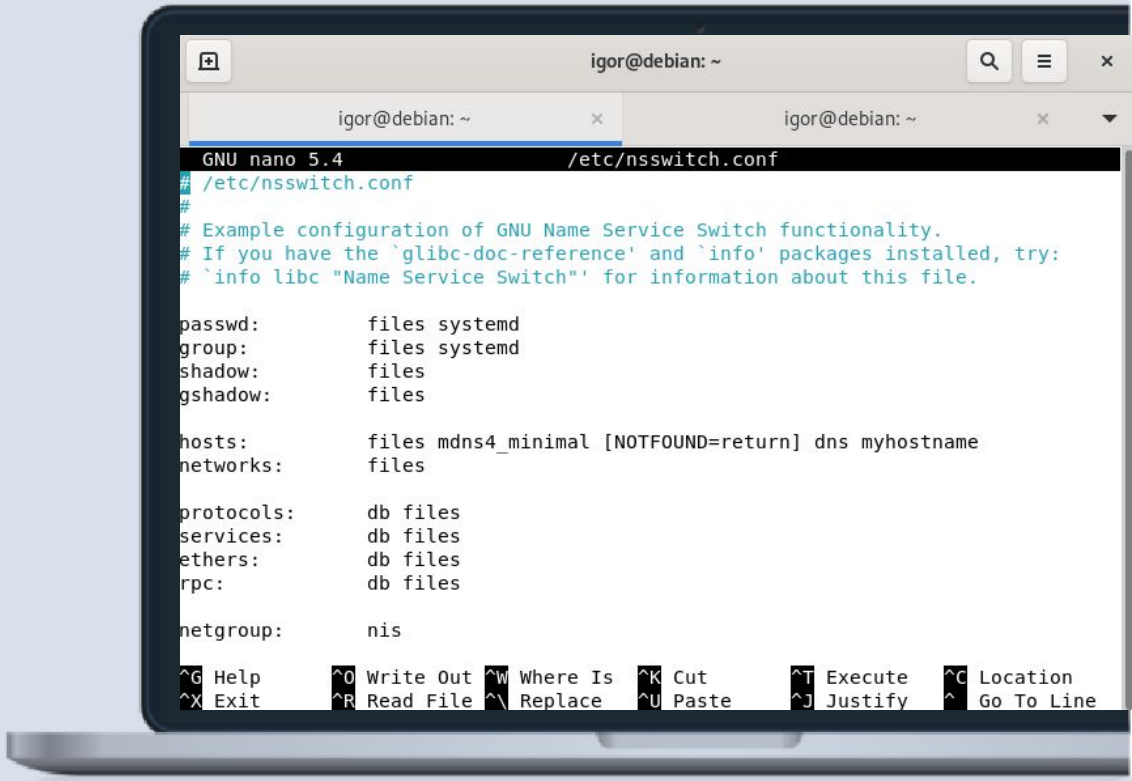


nano /etc/nsswitch.conf

- 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»**.

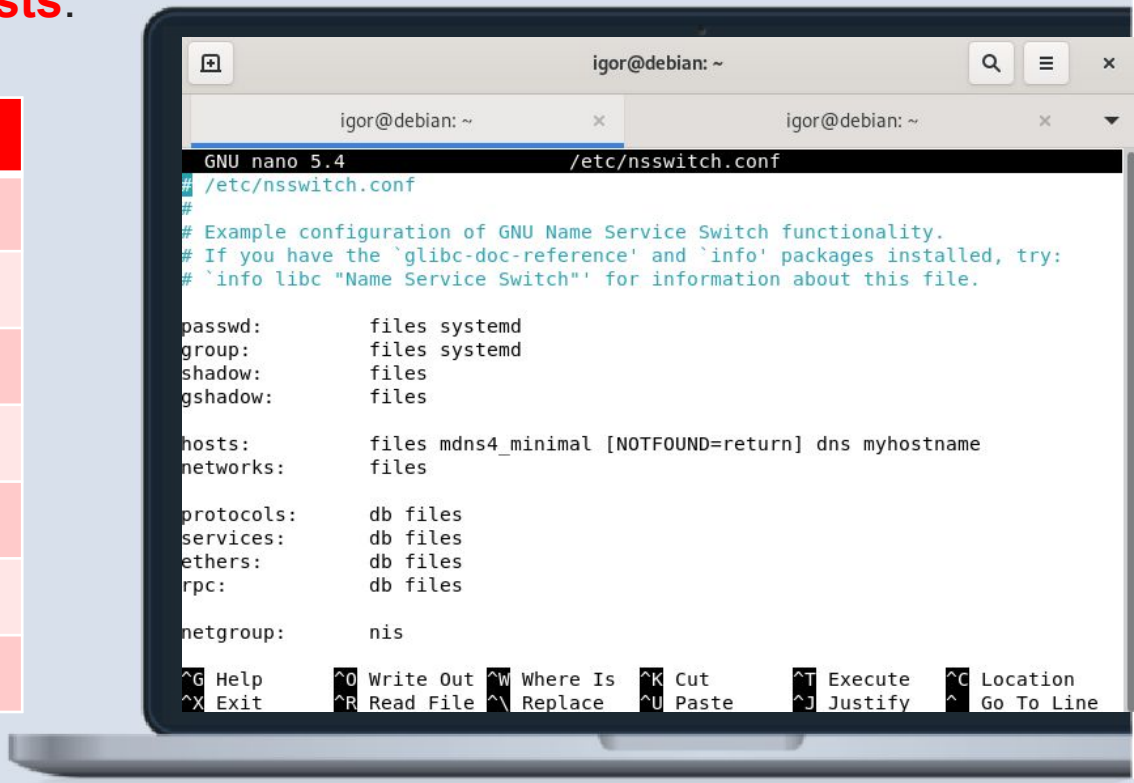


nano /etc/nsswitch.conf

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

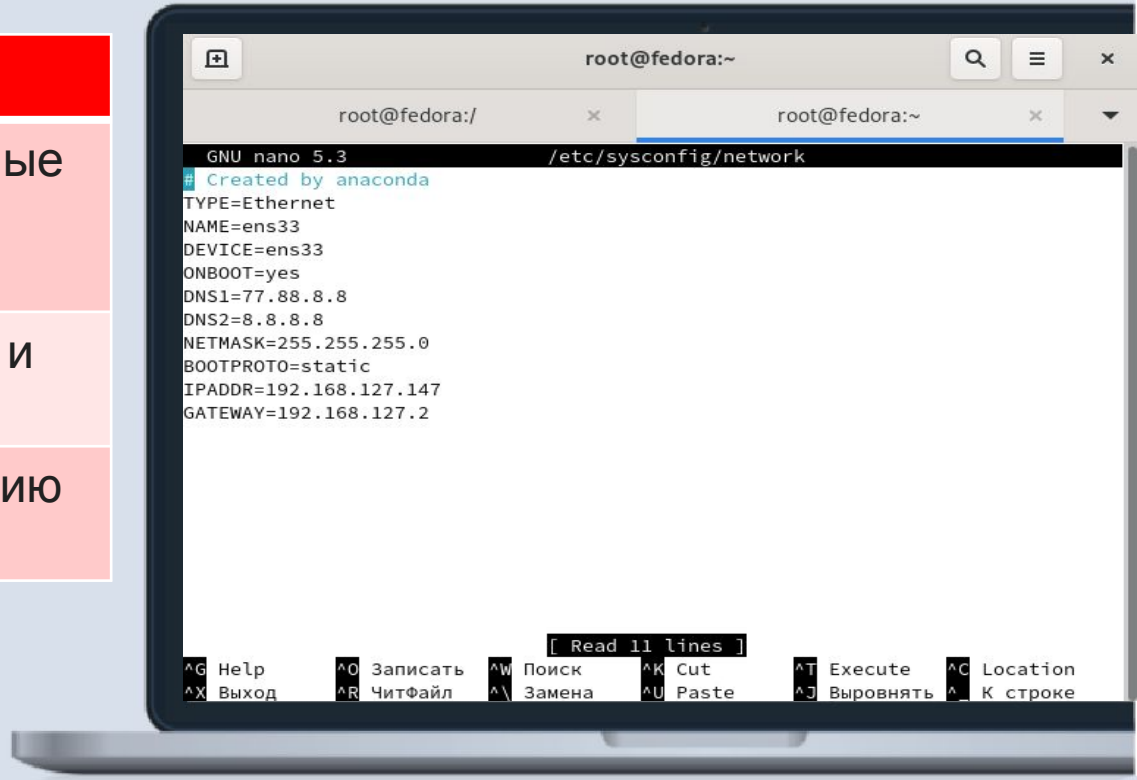
Служба	Файлы
aliases	/etc/aliases
ethers	/etc/ethers
group	/etc/group
hosts	/etc/hosts
initgroups	/etc/group
netgroup	/etc/netgroup

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



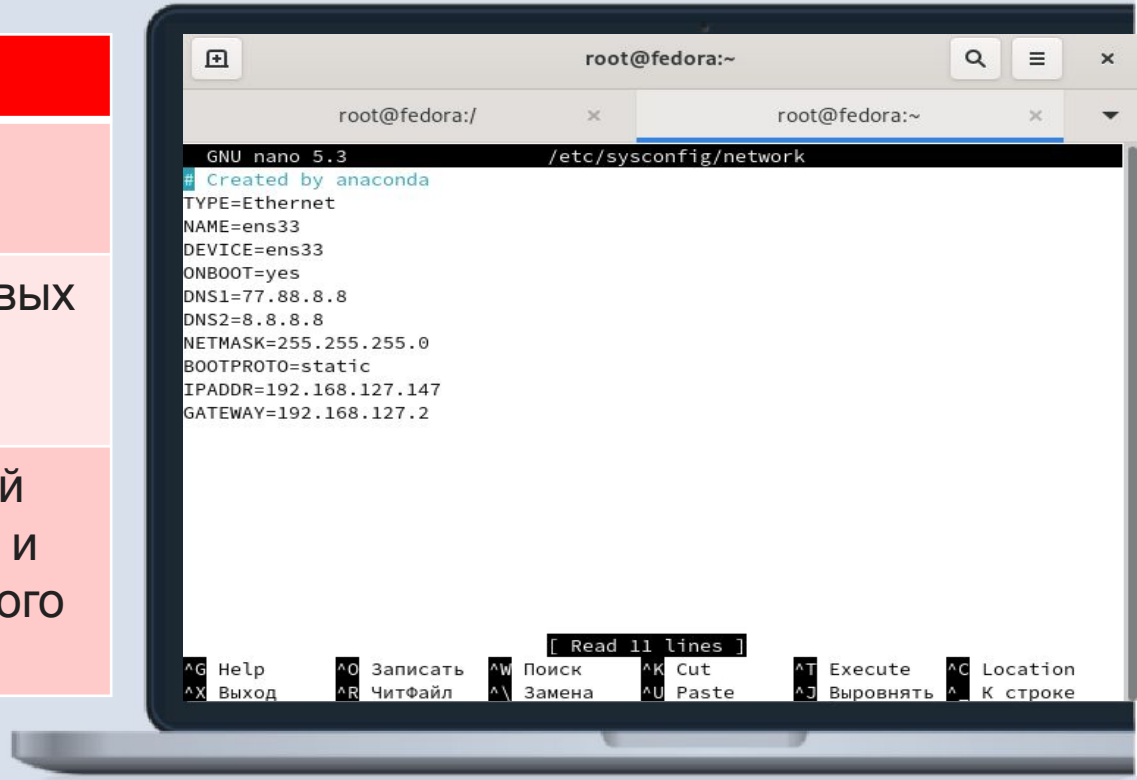
nano /etc/sysconfig/network-scripts

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.



nano /etc/sysconfig/network-scripts

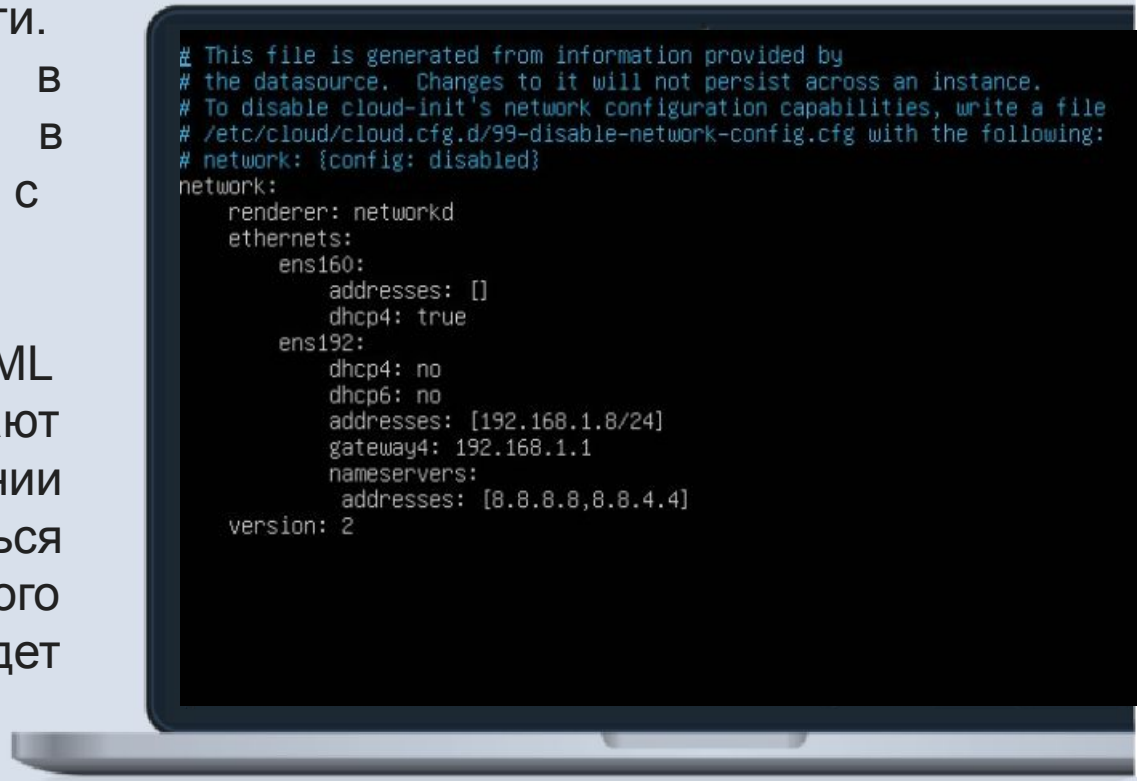
Команда	Описание
/etc/sysconfig/network-scripts/ifcfg-*	Конфигурационные файлы, описывающие интерфейсы системы.
/etc/init.d/network	Скрипт, выполняющий настройку сетевых интерфейсов и маршрутизации при загрузке.
/etc/sysconfig/network	Конфигурационный файл, содержащий имя хоста, IP-адрес основного шлюза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



Перезапуск сервиса сети в Linux

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

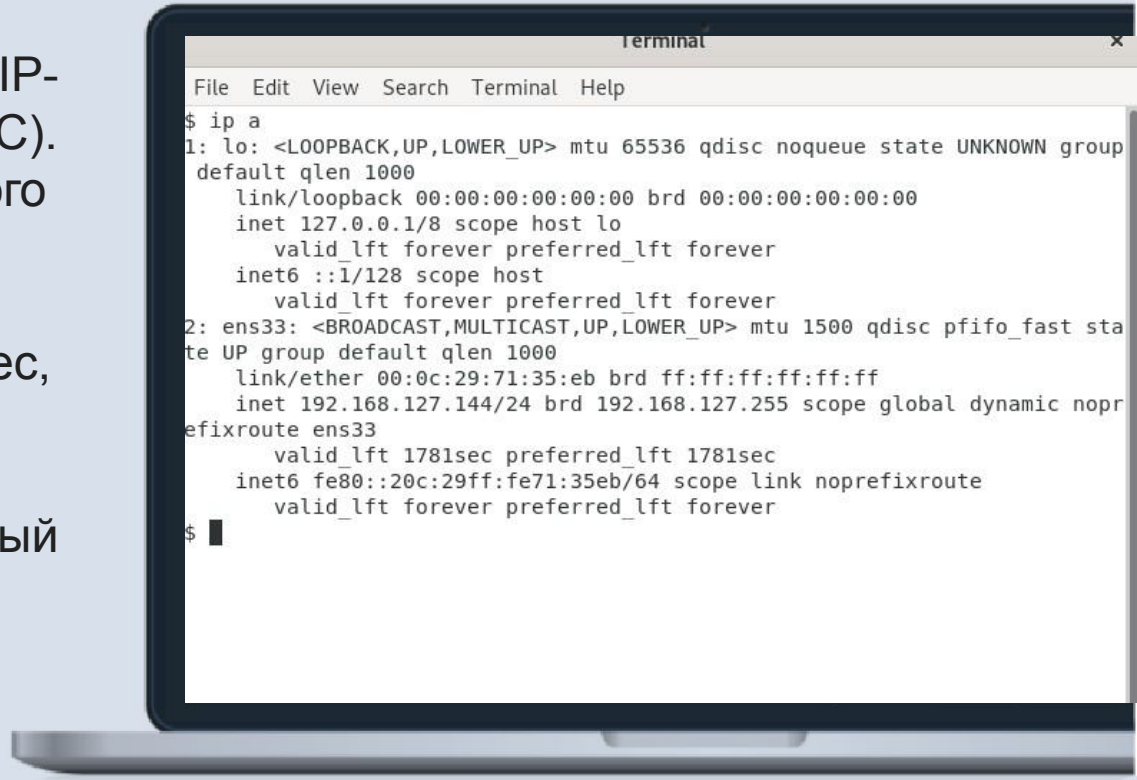
Утилита ip

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).

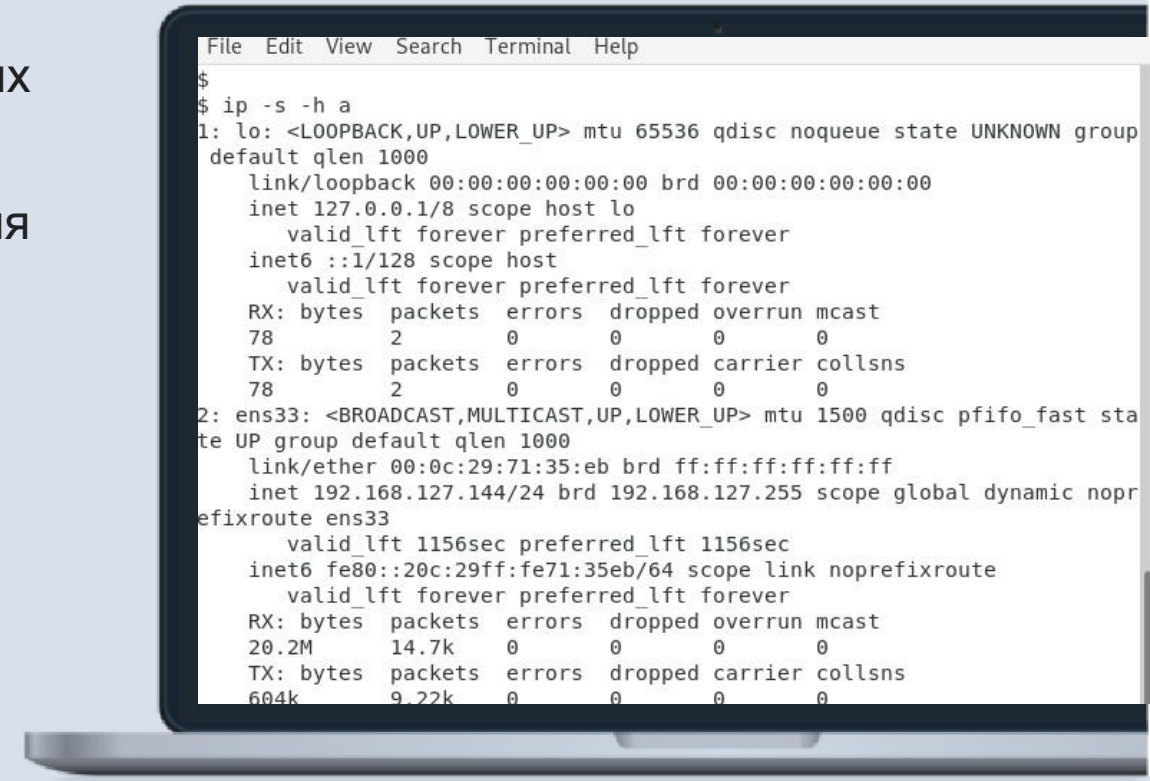


Как просмотреть статистику использования трафика сетевыми интерфейсами?

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

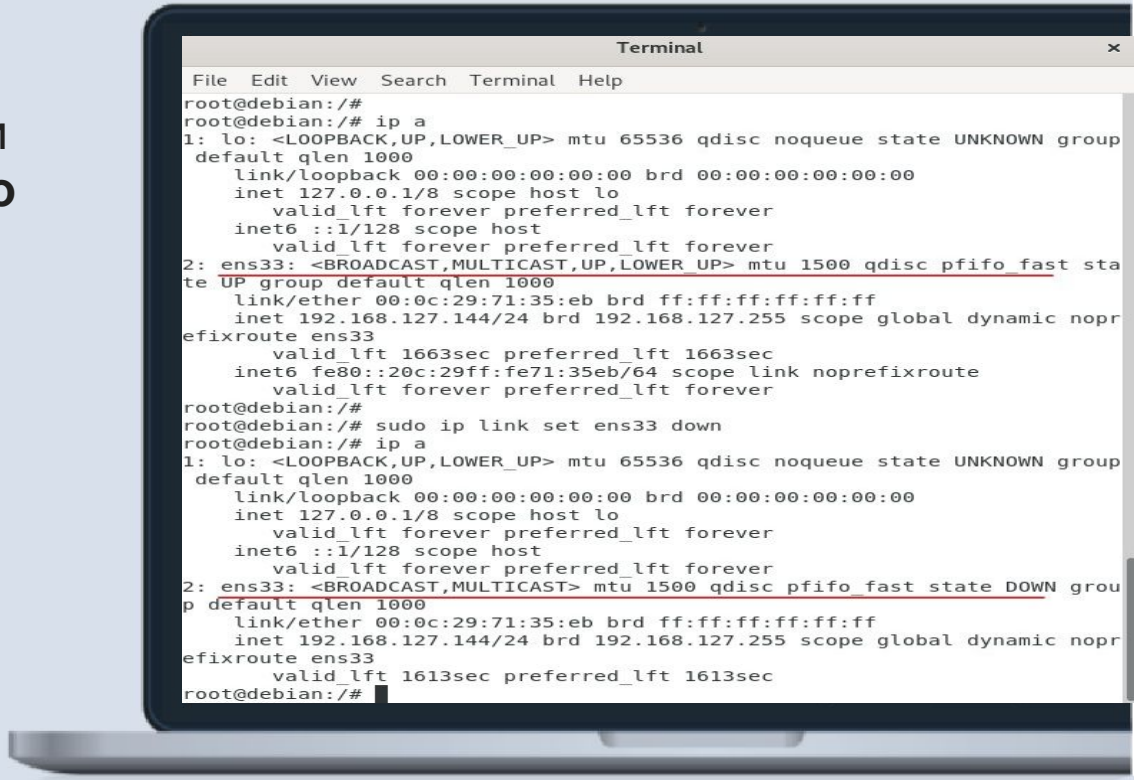


Включение / остановка сетевого интерфейса

- 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

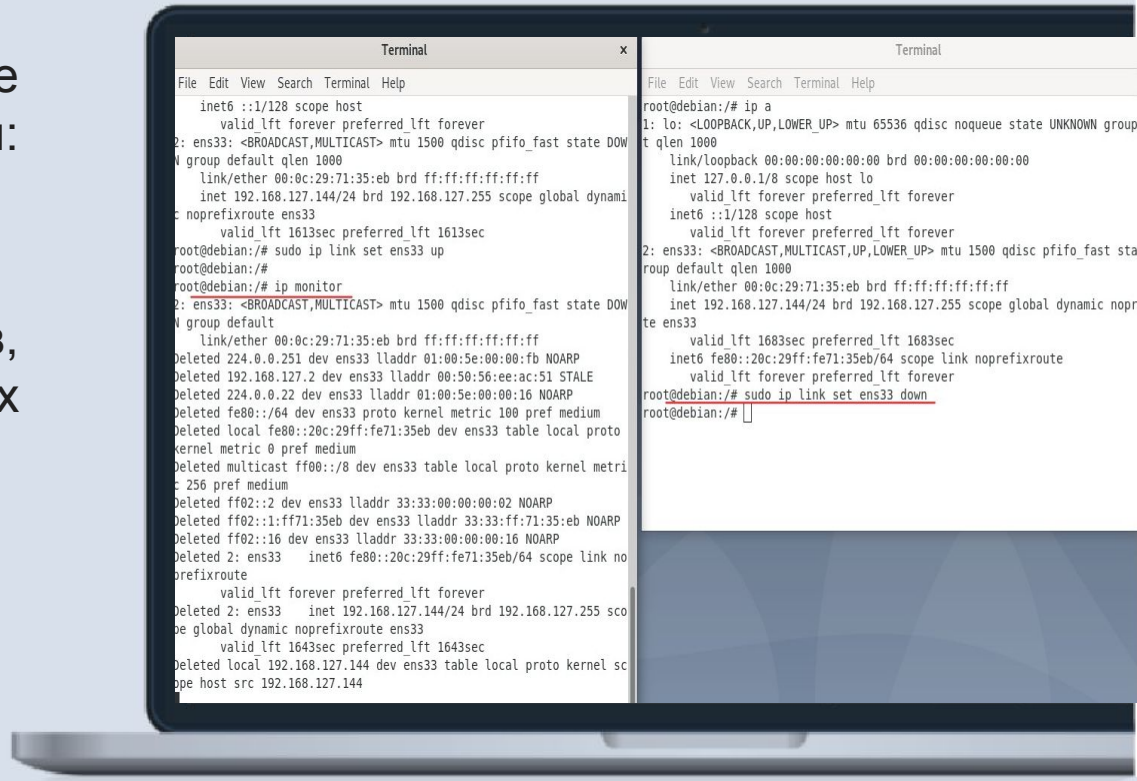


Мониторинг событий сетевых интерфейсов

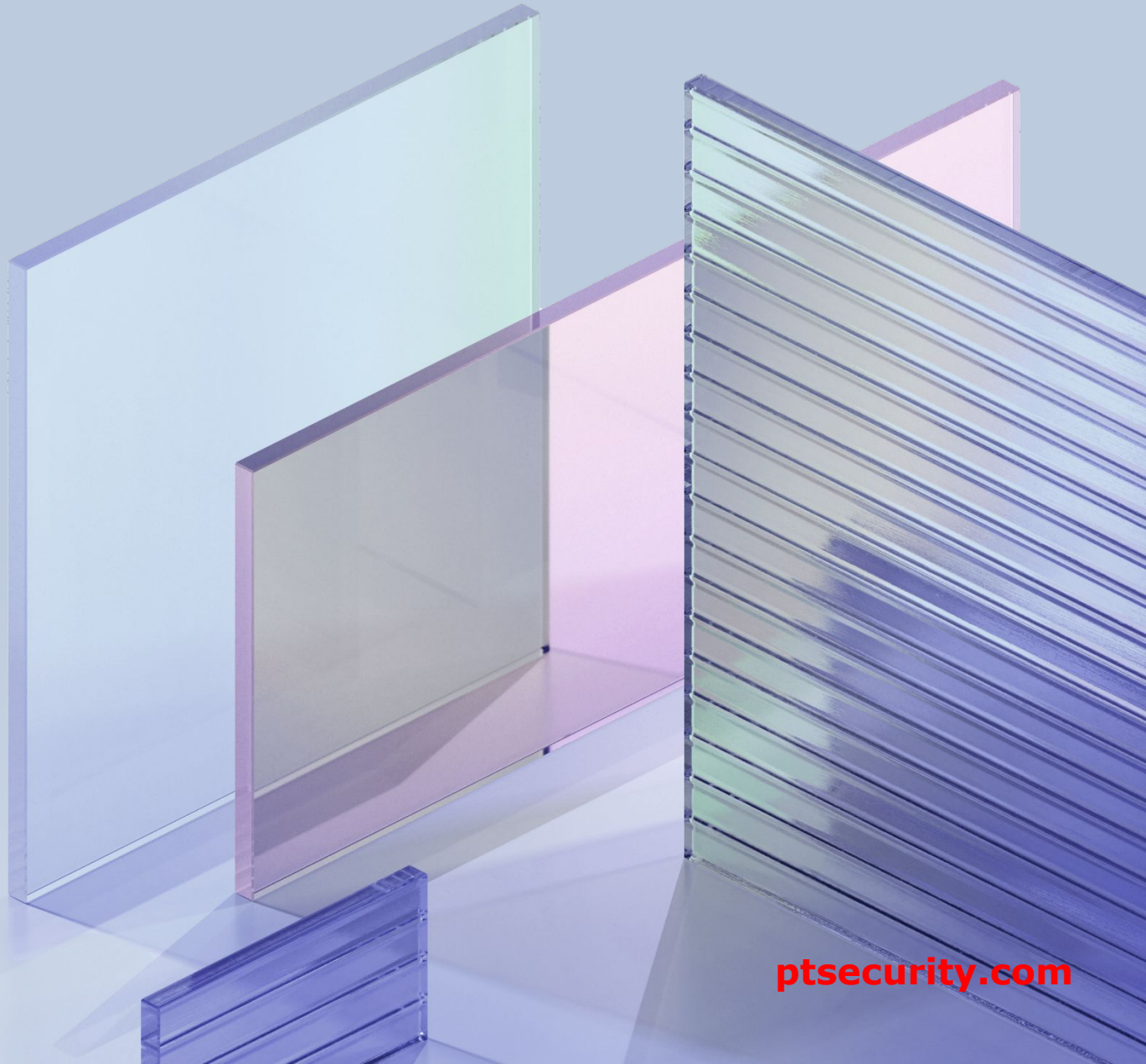
- Всё, что происходит с сетевыми интерфейсами в режиме реального времени можно наблюдать с помощью команды:

ip monitor

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



Спасибо
за внимание



Positive Technologies

ptsecurity.com