**Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования**

**"Уфимский университет науки и технологии"**

**Кафедра** Высокопроизводительных вычислительных технологий и систем

**Дисциплина:** Операционные системы и сети

**Отчет по лабораторной работе № 1**

**Тема:** «Настройка сетевых интерфейсов и сетевой файловой системы»

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Группа ПМ-357 | Фамилия И.О. | Подпись | Дата | Оценка |
| Студент | Акмурзин М.Э. |  |  |  |
| Принял | Ямилева А.М. |  |  |  |

**Уфа 2023**

**Цель:** изучить методы и утилиты настройки сетевых интерфейсов в ОС GNU/Linux, а также удаленного доступа к файловой системе.

**Теоретический материал**

**Локальная вычислительная сеть** (**ЛВС** *локальная сеть*; англ. ***Local Area Network, LAN***) — это совокупность устройств, соединенных вместе и покрывающая обычно относительно небольшую территорию или небольшую группу зданий (дом, офис, фирму, институт).



Рис. 1. Пример локальной сети

Локальные сети обычно построены на технологиях Ethernet. Для его построения используются маршрутизаторы, коммутаторы, точки беспроводного доступа, беспроводные маршрутизаторы, модемы и сетевые адаптеры.

Под топологией (компоновкой, конфигурацией, структурой) компьютерной сети обычно понимается физическое расположение компьютеров сети друг относительно друга и способ соединения их линиями связи и относится прежде всего к локальным сетям. И существует три базовые топологии сети: Шина (bus), Звезда (star) (бывает двух видов: активная и пассивная) и кольцо (ring).

**Ход работы**

Для данной работы нам понадобится две виртуальных машины. Одна будет сервером, вторая – клиентом.

На обе машины необходимо установить пакеты net-tools и ifupdown с помощью команды sudo apt-get install имя\_пакета. После этого нужно настроить сетевые адаптеры: у машины-сервера их будет два (NAT и внутренняя сеть), клиент будет иметь только один (внутренняя сеть).

**Настройка сетевых интерфейсов сервера**

Для того чтобы настроить сетевые интерфейсов в Ubuntu нам необходимо установить на server и client пакеты **net-tools** и **ifupdown**.

Отредактируем настройки сетевых интерфейсов:

sudo nano /etc/network/interfaces

Сервер имеет 2 сетевых интерфейса: enp0s3 - подключение к интернету. (Получает его IP адрес динамически через VirtualBox 10.0.2.15, но он может иметь и статический) и enp0s8 — подключение к локальной сети, который имеет статический IP 192.168.10.1 и маску 255.255.255.0.

В открывшийся файл записываем следующее:

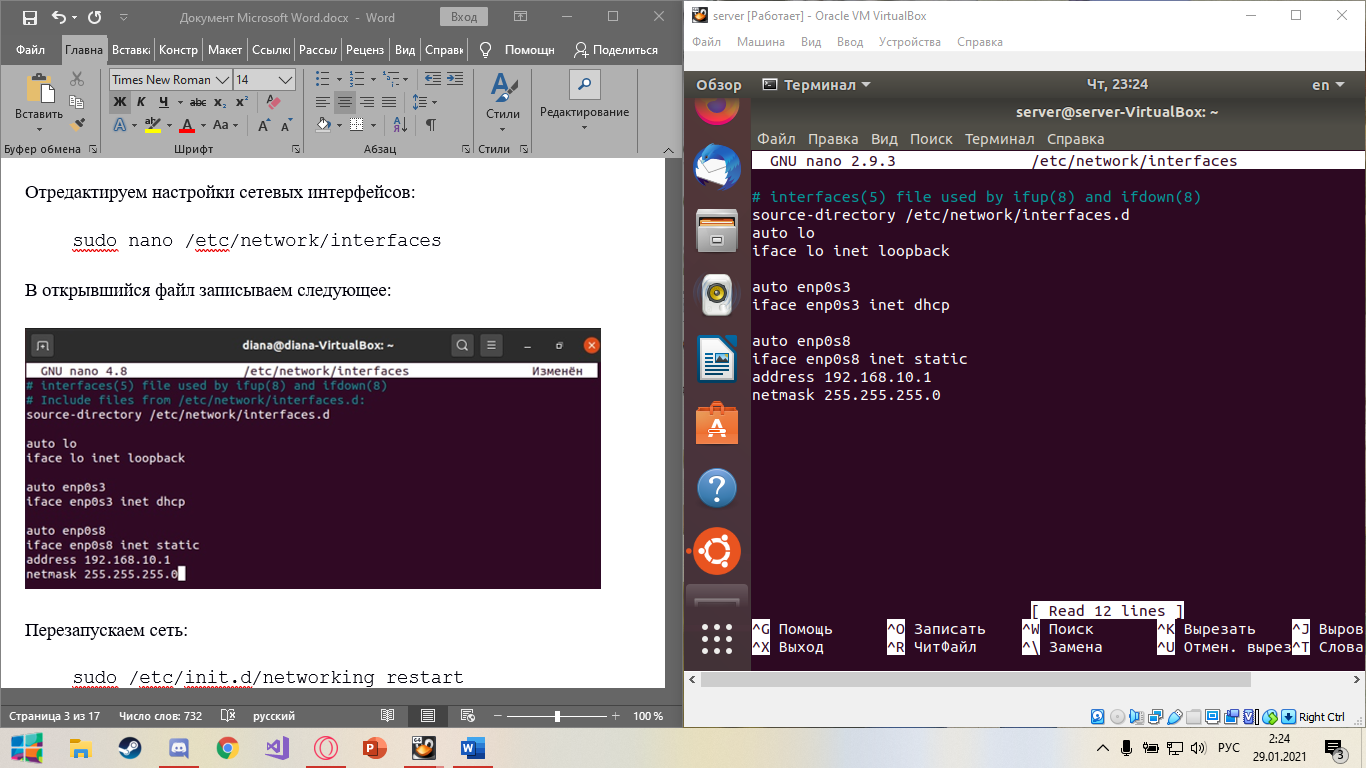


Рис. 2. Настройка сервера в файл /etc/network/interfaces

Перезапускаем сеть:

sudo /etc/init.d/networking restart

Получается, что локальной сети сервера шлюза и dns имеет IP-адрес 192.168.10.1.

**Настройка сетевых интерфейсов клиента**

Отредактируем настройки сетевых интерфейсов:

sudo nano /etc/network/interfaces

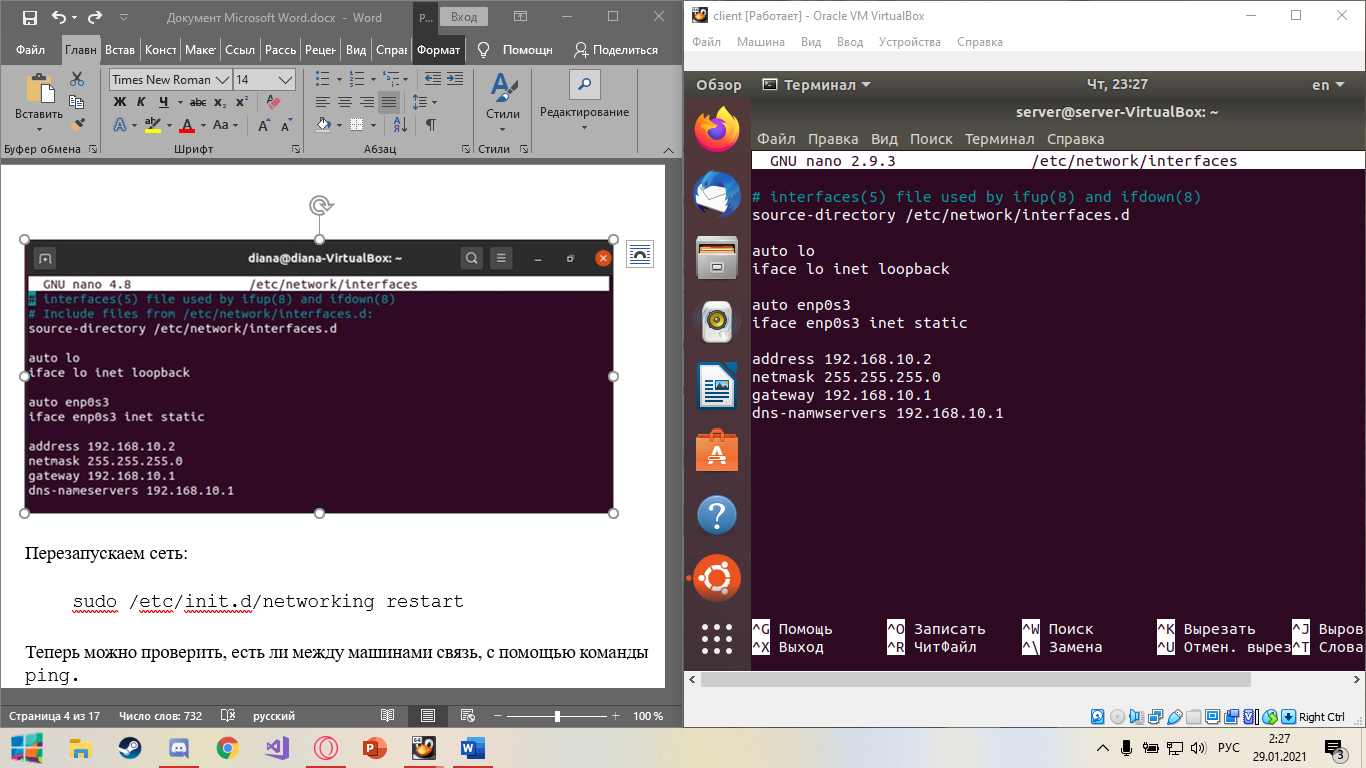


Рис. 3. Настройка клиента в файл /etc/network/interfaces

auto <интерфейс> ­­ — автоматический запуск локального интерфейса.

Iface <интерфейс> inet static — интерфейс находится в диапазоне адресов IPv4 со статическим IP.

address — IP адрес сетевого интерфейса.

netmask — маска сети.

gateway — шлюз.

dns-nameservers — адреса DNS серверов.

Режим Network Address Translation (NAT) предоставляет наиболее простой способ доступ к внешней среде из виртуальной машины. Обычно, для него не требуется никаких настроек хоста и гостевой системы. Поэтому он является сетевым режимом, настраиваемым по умолчанию(enp0s3). Проводить какую-либо настройку интерфейса сервера enp0s3 не нужно.

Перезапускаем сеть:

sudo /etc/init.d/networking restart

Теперь можно проверить, есть ли между машинами связь, с помощью команды ping.

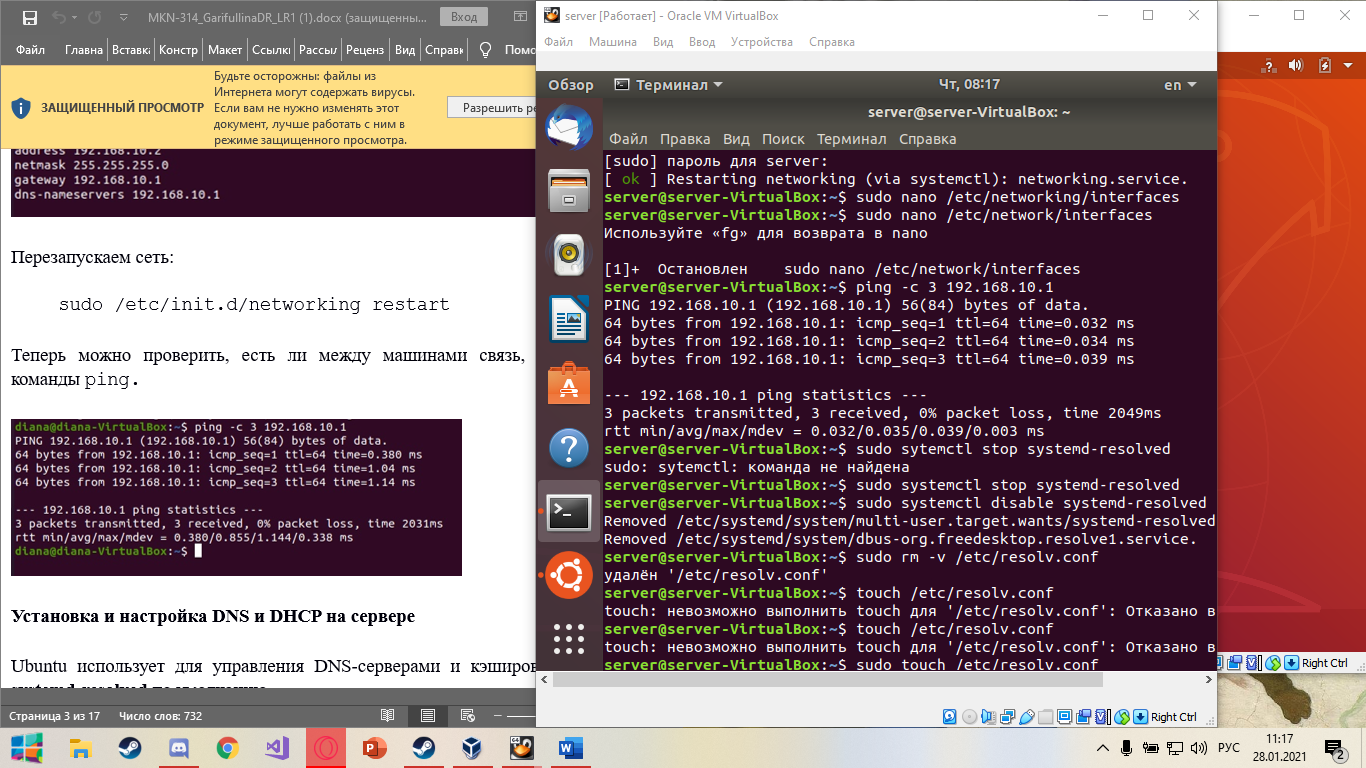


Рис. 4. Ping для проверки связи между машинами

**Установка и настройка DNS и DHCP на сервере**

**Установка dnsmasq**

Dnsmasq — это упрощенный, легкий в настройке DNS-форвардер и

DHCP-сервер. Он предназначен для предоставления DNS и, возможно, DHCP в небольшую сеть. Он может обслуживать имена локальных машин, которые не входят в глобальную DNS. И он доступен в официальном репозитории пакетов Ubuntu. Ubuntu использует **systemd-resolved** по умолчанию для управления DNS-серверами и кэшированием DNS. Перед установкой dnsmasq необходимо было остановить и отключить службы, разрешенные systemd. В противном случае вообще невозможно запустить dnsmasq.

Ubuntu использует для управления DNS-серверами и кэшированием DNS **systemd-resolved** по умолчанию.

Остановим, а затем отключим службу **system-resolved:**

//отключаем службы ДНС заданные по умолчанию и устанавливаем свой ДНС сервер

sudo systemctl stop systemd-resolved

sudo systemctl disable systemd-resolved

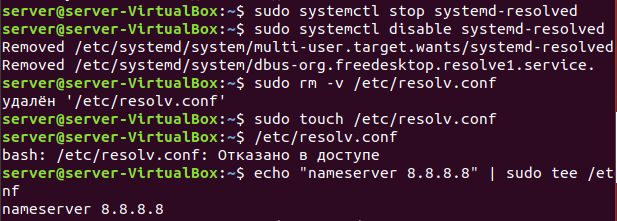
Также нужно удалить конфигурационный файл **resolv.conf**:

sudo rm -v /etc/resolv.conf

Теперь создадим новый файл **resolv.conf** и установим DNS-сервер google в качестве DNS-сервера по умолчанию:

touch /etc/resolv.conf

echo “nameserver 8.8.8.8” | sudo tee /etc/resolv.conf



Обновим кэш репозитория пакетов APT и установим **dnsmasq**:

sudo apt update

sudo apt install dnsmasq

**Настройка DNS-сервера с помощью dnsmasq**

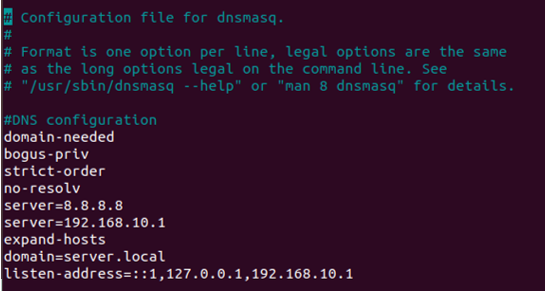
Конфигурационный файл dnsmasq — это файл **/etc/dnsmasq.conf**. Чтобы настроить dnsmasq в качестве DNS-сервера, необходимо изменить этот файл.

Чтобы настроить **dnsmasq** в качестве DNS-сервера, необходимо изменить файл **/etc/dnsmasq.conf**. Этот файл содержит много документации и закомментированных параметров, поэтому переименуем его и создадим копию:

sudo cp /etc/dnsmasq.conf /etc/dnsmasq.conf.bk

Отредактируем этот файл:

sudo nano /etc/dnsmasq.conf



- **domain-needed**: не пересылает запросы, не содержащие полное доменное имя. Например, машинный запрос не будет передан DNS-серверам интернет-провайдера, а запрос для machine.domain.com будет.

- **bogus-priv**: ложное обратное разрешение для частных сетей. Все обратные DNS-запросы для частных IP-адресов (т. е. 192.168.x. x и т. д...), которые не найдены в **/etc/hosts** или в файле аренды DHCP, возвращаются ответом “нет такого домена” (”no such domain”) вместо того, чтобы передаваться на вышестоящие серверы имен (”upstream server”).

- **strict-order**: по умолчанию dnsmasq отправляет запросы на любой из вышестоящих серверов, о которых ему известно, и пытается выбрать серверы, которые, как известно, работают. Установка этого флага заставляет dnsmasq пробовать каждый запрос с каждым сервером строго в том порядке, в котором они появляются в файле **/etc/resolv.conf**

- **no-resolv**: не читайте файл **/etc/resolv.conf**. Получить вышестоящие серверы можно только из командной строки или конфигурационного файла dnsmasq.

- **expand-hosts**: добавьте домен к простым именам (без точки) в файле **/etc/hosts** таким же образом, как и для производных от DHCP имен.

- **server=192.168.10.1**: укажите IP-адрес вышестоящих серверов напрямую. Установка этого флага не подавляет чтение файла **/etc/resolv.conf.**

**- listen-address=::1**: прослушивание по заданному ip-адресу(адресам). Могут быть заданы как параметры --interface, так и --listen-address, и в этом случае используется набор обоих интерфейсов и адресов. Отмечается, что если опция --interface не задана, но --listen-address есть, dnsmasq не будет автоматически прослушивать интерфейс обратной связи. Для достижения этой цели его IP-адрес, 127.0.0.1, должен быть явно задан как параметр --listen-address.

После настройки перезапускаем службу **dnsmasq**:

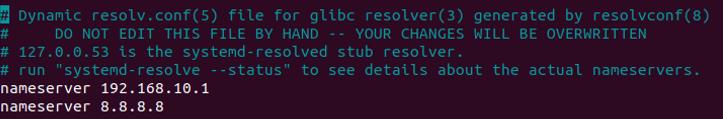
sudo systemctl restart dnsmasq

Чтобы NetworkManager не менял содержание файла **resolv.conf** при перезапуске системы, нужно установить пакет **resolvconf**:

sudo apt install resolvconf

Нужно отредактировать файл:

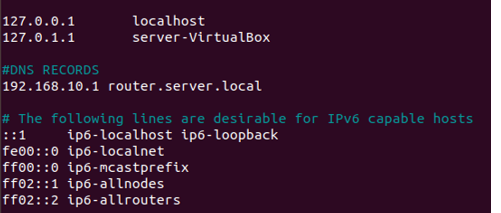
sudo nano /etc/resolvconf/resolv.conf.d/head



**Добавление записей DNS**

Теперь можно добавить свои DNS-записи в файл hosts:

sudo nano /etc/hosts

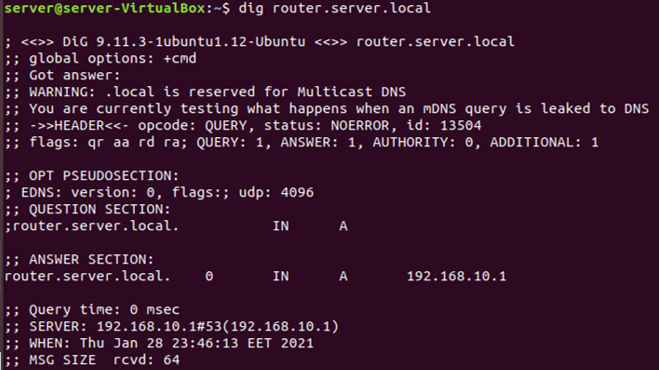


Перезапустим службу:

sudo systemctl restart dnsmasq

**Тестирование DNS-сервера**

Проверим, работает ли локальное разрешение DNS и разрешение имен в интернете:



Разрешение имен в интернете также работает.

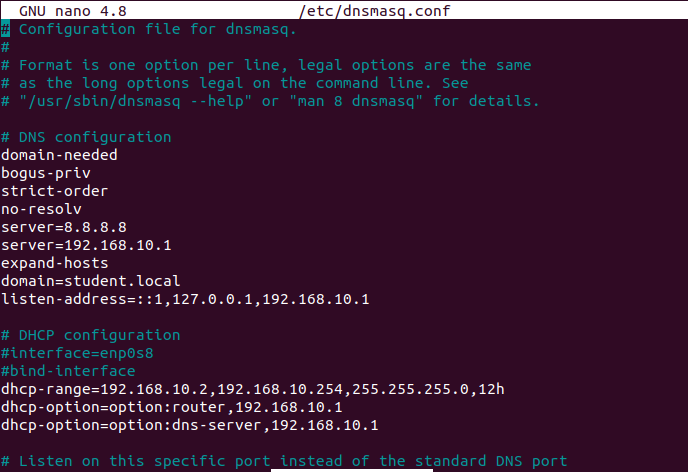


**Настройка DHCP-сервера с помощью dnsmasq**

Для настройки DHCP с помощью **dnsmasq** нужно отредактировать **dnsmasq.conf**:

sudo nano /etc/dnsmasq.conf

Полный конфигурационный файл DNS и DHCP для dnsmasq:



Здесь **dhcp-range** используется для установки диапазона IP-адресов, которые DHCP-сервер будет назначать хостам, **dhcp-option** используется для настройки шлюза (option: router) и адрес DNS-сервера (option: dns-server).

**Конфигурация iptables**

Для того, чтобы разрешение имен работало, и клиент имел доступ к интернету, необходимо настроить правило пересылки NAT в **iptables**.

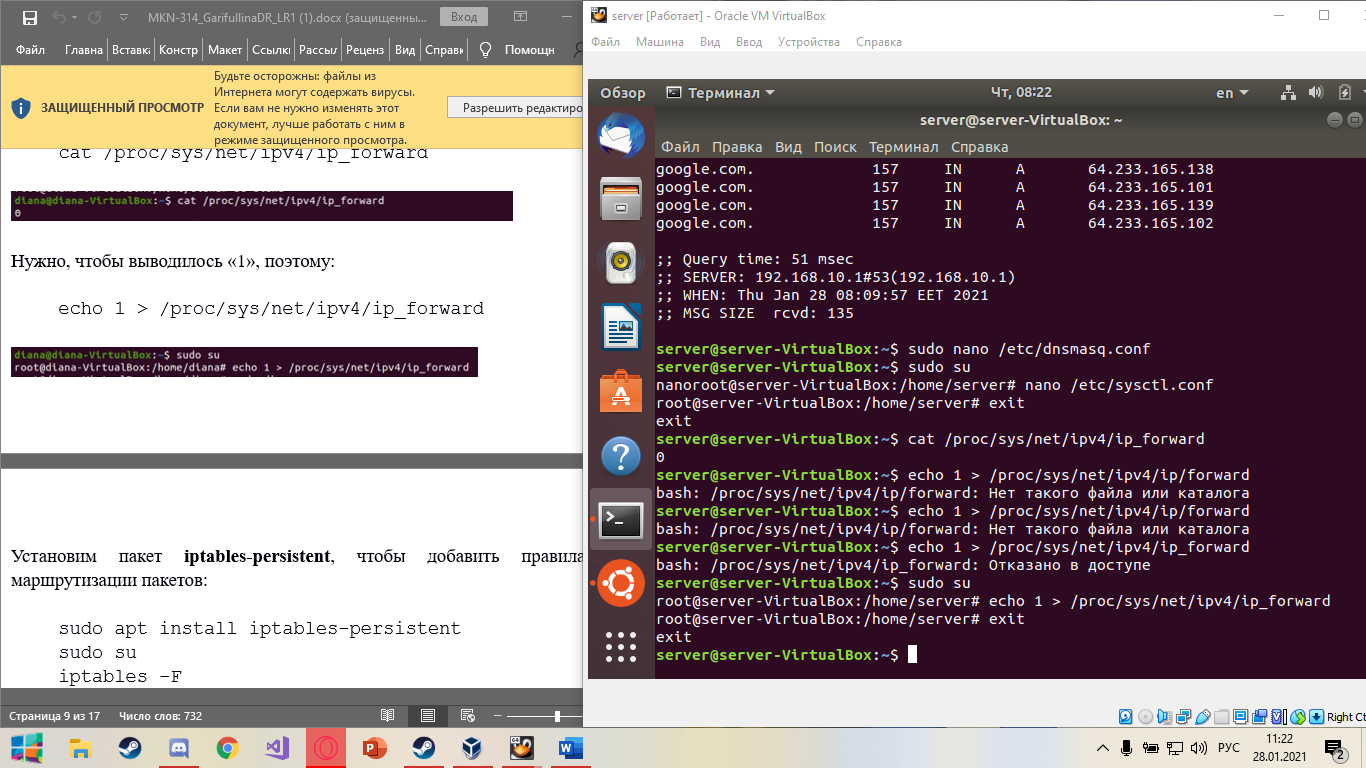
На машине-сервере перейдем к правам суперпользователя и разрешим перенаправление пакетов:

sudo su

nano /etc/sysctl.conf

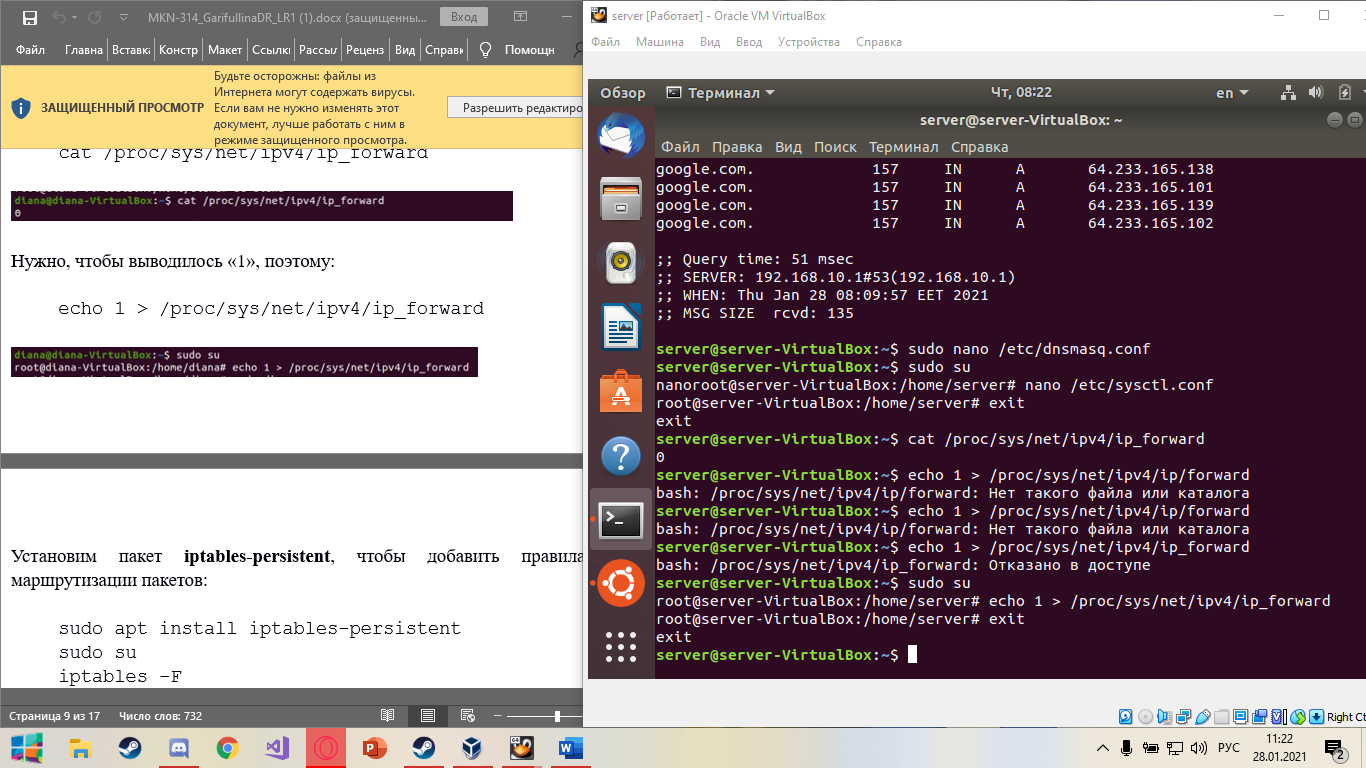
В открывшемся файле снимем комментарий со строки **net.ipv4.ip\_forward=1** (для хранения пересылки трафика между интерфейсами после перезагрузки) и проверим состояние файла:

cat /proc/sys/net/ipv4/ip\_forward //изменение содержимого файла



Нужно, чтобы выводилось «1», поэтому:

echo 1 > /proc/sys/net/ipv4/ip\_forward // прописываем файл



Установим пакет **iptables-persistent**, чтобы добавить правила для маршрутизации пакетов:

sudo apt install iptables-persistent

sudo su

iptables -F

iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE

iptables -A FORWARD -i enp0s3 -o enp0s3 -j REJECT

iptables -I FORWARD -p tcp --tcp-flags SYN,RST SYN -j TCPMSS --clamp-mss-to-pmtu

iptables-save > /etc/iptables/rules.v4

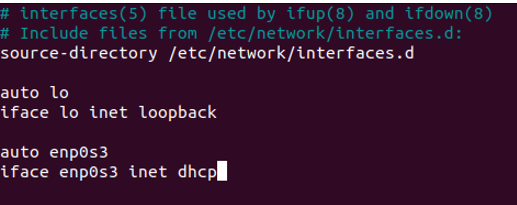
Настроим файл **rc.local**, чтобы при перезапуске конфигурация загружалась через него:

sudo nano /etc/rc.local



Теперь перезапустим машины сервер и клиент и проверим, работает ли разрешение имен через DHCP. Сделаем следующее для клиента:

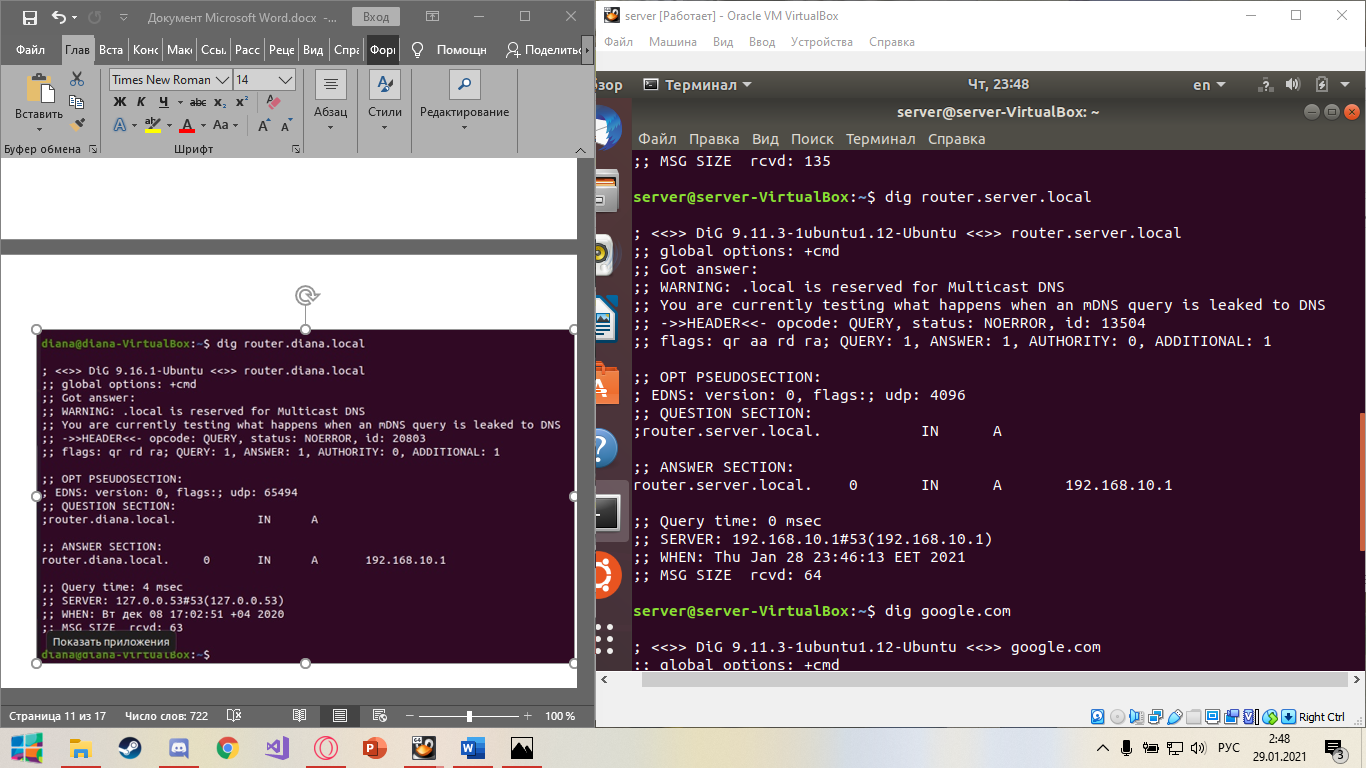
sudo nano /etc/network/interfaces

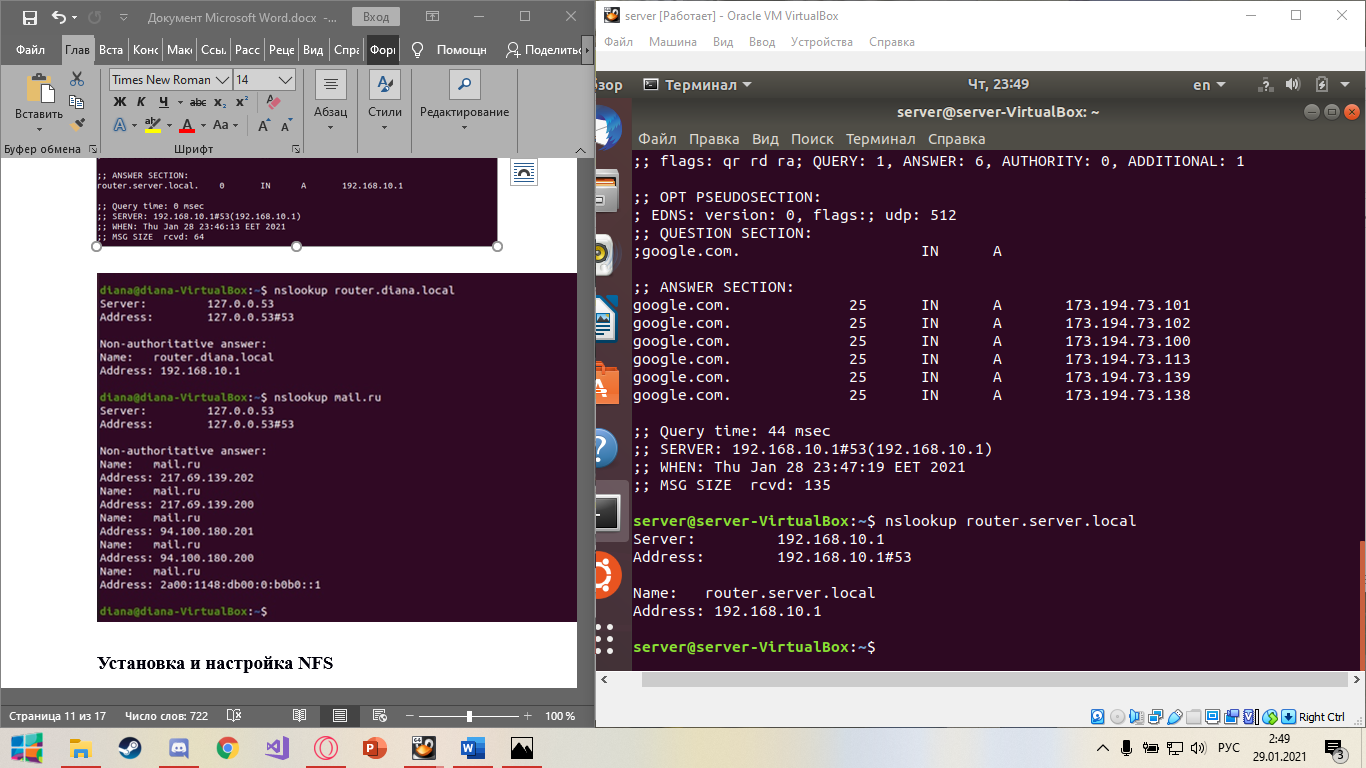


**Тестирование разрешение имен на клиенте**



//dig- информация о записях ДНС





**Установка и настройка NFS**

Network File System (NFS) — это сетевая файловая система, позволяющая пользователям обращаться к файлам и каталогам, расположенным на удалённых компьютерах, как если бы эти файлы и каталоги были локальными.

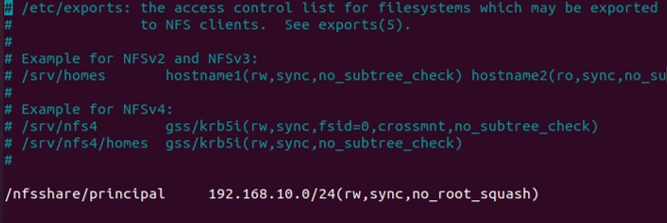
NFS — это клиент-серверное приложение. Т.е. в системе пользователя должен быть установлен NFS-клиент, а на компьютерах, которые предоставляют свое дисковое пространство - NFS-сервер.

**Установка и настройка NFS на сервера**

Сделаем на сервере следующее:

sudo apt install nfs-kernel-server

sudo nano /etc/exports



sudo mkdir -p /nfsshare/principal

sudo chmod 777 -R /nfsshare/principal//устанаовление прав на чтение

sudo systemctl restart nfs-kernel-server.service

Директория **/nfsshare/principal** (директория с данными на сервере) в пользование компьютерам из 10 подсети - 192.168.10.0/24 будут имееть права на чтения и запись.

**- ro** - права только на чтение. Можно и не указывать, так как она установлена по умолчанию.

- **sync** - эта опция принудительно заставляет NFS записывать изменения на диске, прежде чем отправлять ответ. В результате мы получаем более стабильную и согласованную среду, поскольку в ответе отражается фактическое состояние удаленного тома. Однако при этом снижается скорость операций с файлами.

**- rw** - дает клиентам право на запись.

**- no\_root\_squash** - по умолчанию пользователь **root** на клиентской машине не будет иметь доступа к разделяемой директории сервера.

**noaccess** - запрещает доступ к указанной директории. Может быть полезной, если перед этим вы задали доступ всем пользователям сети к определенной директории, и теперь хотите ограничить доступ в поддиректории лишь некоторым пользователям.

- **insecure** - если планируется подключение компьютера под управлением Mac OS X, эта опция обязательна.

**Установка и настройка NFS на клиента**

На клиенте:

sudo apt install nfs-common

mkdir -p ~/nfs/example

Монтировать можно двумя способами. Первый – кратковременный:

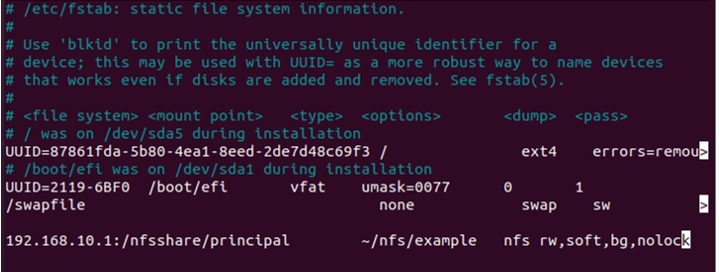
sudo mount 192.168.10.1:/nfsshare/principal ~/nfs/example

Второй – удобнее, при перезапуске конфигурация не будет меняться:

sudo nano /etc/fstab

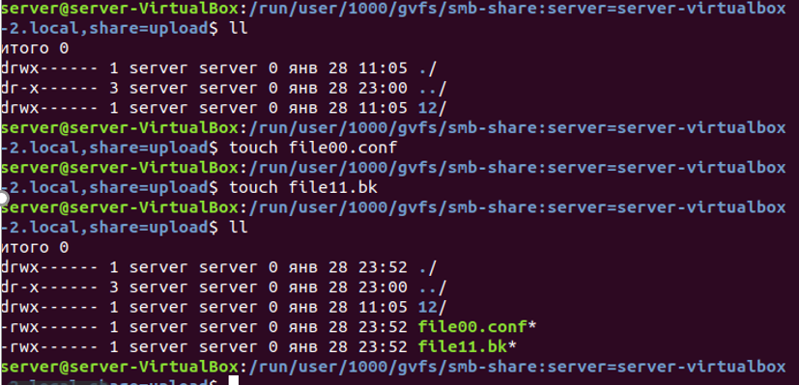
В файл записываем следующую строку:

192.168.10.1:/nfsshare/prinsipal ~/nfs/example nfs rw,soft,bg,nolock 0 0



**Тест работы NFS**

Для проверки создадим на сервере несколько файлов:



Получим доступ к этим файлам на клиенте:



**Вывод**

В ходе лабораторной работы были изучены методы и утилиты настройки сетевых интерфейсов в ОС GNU/Linux, а также удаленного доступа к файловой системе.

**Список использованной литературы**

1. Настройка сетевых интерфейсов в Ubuntu Бикмеев А.Т.

<https://www.youtube.com/watch?v=Q6Stz-BeFws&t=7s>

1. Установка и настройка VirtualBox, создание виртуальной машины // Lyapidov URL: <https://lyapidov.ru/installing-and-configuring-virtualbox-create-a-virtual-machine/>
2. How to Configure dnsmasq on Ubuntu Server 18.04 LTS // Linux Hint URL: <https://linuxhint.com/dnsmasq_ubuntu_server/>
3. How to Install and Configure Dnsmasq on Ubuntu 18.04 LTS // Computing for Geeks URL: <https://computingforgeeks.com/install-and-configure-dnsmasq-on-ubuntu-18-04-lts/>