

## Лабораторная работа №3 «Основные сетевые утилиты»

*Цель работы:*

*Продолжительность работы:* 4 часа

### 1. Теоретическая часть

#### 1.1. FTP-сервер

**FTP (File Transport Protocol)** – протокол передачи файлов по сети прикладного уровня модели OSI.

Протокол появился в 1971 году и, несмотря на возраст, активно используется повсеместно.

FTP-сервер представляет собой хранилище файлов, который по запросу из сети осуществляет приём или передачу файлов.

**Репозиторий (от англ. repository — хранилище)** — место, где хранятся и поддерживаются какие-либо данные.

Именно на FTP-репозитории была впервые выложена первая версия ядра Linux. Расположение репозитория на одном сервере позволяет пользователям локальной или глобальной сети обращаться к ней, тем самым не вынуждая хранить данные у себя на локальной машине и легко делиться ими с другими.

В качестве FTP-сервера предлагается программа **vsftpd** (Very Secure FTP Daemon), распространяемая под лицензией GPL. Её установить можно с официальных репозиториях Astra Linux менеджером пакетов **apt**. Делается это следующей командой:

```
sudo apt install vsftpd
```

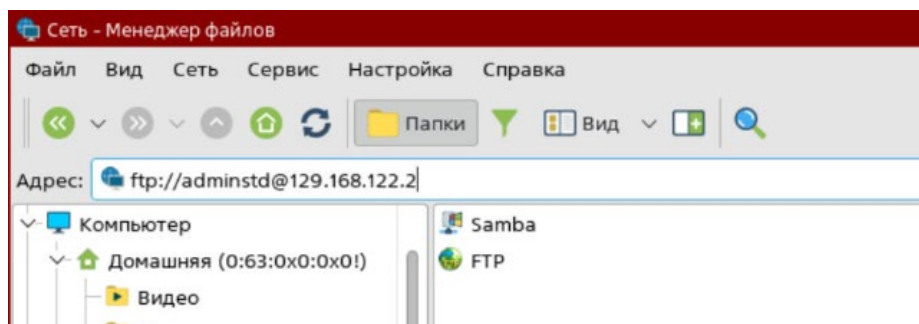
Для настройки необходимо с правами суперпользователя отредактировать конфигурационный файл **/etc/vsftpd.conf**. Некоторые параметры должны иметь следующий вид:

```
listen=yes  
listen_ipv6=no
```

```
anonymous_enable=YES
```

После каждого изменения конфигурационного файла необходимо перезапустить службу **vsftpd**.

Проверить работу FTP-сервера можно с помощью менеджера файла, как показано на рисунке ниже. В адресной строке указывается протокол ftp, затем имя пользователя, который имеет доступ к репозиторию, IP-адрес сервера. Будет предложено ввести пароль указанного пользователя.



## 1.2. SMB-сервер

**SMB** (сокр. от англ. *Server Message Block*) — сетевой протокол прикладного уровня для удалённого доступа к файлам, принтерам и другим сетевым ресурсам.

**Samba** — пакет программ, которые позволяют обращаться к сетевым дискам и принтерам на различных операционных системах по протоколу SMB. Работает через порт 445.

Для установки Samba используется команда

```
sudo apt install samba
```

В качестве примера создадим общую папку. Для этого командой

```
mkdir /srv/share
```

создадим папку. Изменим права доступа к этой папке

```
sudo chown nobody:nogroup /srv/share
```

```
sudo chmod 777 /srv/share
```

Далее в конец файла **/etc/samba/smb.conf** необходимо добавить следующие строки:

```
map to guest = Bad User
[share]
comment = <Произвольный комментарий>
guest ok = yes
force user = nobody
force group = nogroup
path = /srv/share
read only = no
```

После сохранения файла проверяем установку параметров командой **testparm**. Осуществляем перезагрузку командой **sudo systemctl restart smbd**.

Работа с общими папками происходит с использованием протокола CIFS (Common Internet File System). Поэтому стоит убедиться, что в системе установлен пакет **cifs-utils**. Её использование определяется следующим синтаксисом:

```
$ mount -t cifs <папка на сервере> <во что монтируем> <-о опции>
```

То есть, чтобы клиент мог подключиться к общей папке, ему необходимо выполнить следующую команду:

```
sudo mount -t cifs //A.B.C.D/share /mnt/smb -o users,sec=none
```

Программа **mount** используется для монтирования USB-устройств, дисков, сетевых папок и т.д. Ключ **-t** указывает тип файловой системы **cifs**. После символов **//** пишется IP-адрес SMB-сервера, название общей папки. Всё это монтируется в папку **/mnt/smb**, а ключом **-o** указываются опции **users** (папка для всех пользователей) и **sec** (отвечает за безопасность).

После подключения в менеджере файлов во вкладке **Сеть/Samba** должна появиться сетевая папка с именем сервера, где и будет лежать общая папка.

### 1.3. Файловая система NFS

NFS (сокращение от Network File System, Сетевая Файловая Система) - сервис, обеспечивающий общий доступ к файлам и каталогам систем \*nix / Linux. Файловая система NFS позволяет монтировать удалённые разделяемые файлы подобно локальным.

Для установки NFS необходимо выполнить команды.

На сервере:

```
sudo apt install nfs-kernel-server
```

На клиенте:

```
sudo apt install nfs-common
```

После установки утилит на сервере необходимо создать и настроить директорию, которая будет доступна для монтирования с других устройств. Для этого создадим её.

```
sudo mkdir /srv/nfsshare  
sudo chmod 777 /srv/nfsshare  
sudo chown nobody:nogroup /srv/nfsshare
```

Для конфигурации NFS необходимо отредактировать файл /etc/exports. Для подключения директории в него необходимо добавить строку вида:

```
directory client(options)
```

Где:

- **directory** — папка, к которой нужно открыть доступ по сети.
- **client** — IP-адрес машины или подсети, которой будет доступна эта папка
- **options** — опции, используемые в настройках.

В качестве опций возможно указать:

- **rw** — чтение запись (может принимать значение **ro** — только чтение);

- `no_root_squash` — по умолчанию в общих ресурсах NFS пользователь `root` становится обычным пользователем `nfsnobody`. Таким образом, владельцем всех файлов, созданных `root`, становится `nfsnobody`, что предотвращает загрузку на сервер программ с установленным битом `setuid`. Использование параметра `no_root_squash` не рекомендуется, так как потенциально создает угрозы безопасности, связанные с возможностью удаленного внедрения в файловую систему вредоносного ПО.
- `nohide` — NFS автоматически не показывает нелокальные ресурсы (например, примонтированные с помощью `mount –bind`), эта опция включает отображение таких ресурсов;
- `sync` — синхронный режим доступа (может принимать обратное значение- `async`). Значение `sync` указывает, что сервер должен отвечать на запросы только после записи на диск изменений, выполненных этими запросами. Параметр `async` указывает серверу не ждать записи информации на диск, что повышает производительность, но снижает надежность, т.к. в случае обрыва соединения или отказа оборудования возможна потеря данных.
- `noaccess` — запрещает доступ к указанной директории. Применяется, если доступ к определенной директории выдан всем пользователям сети, и необходимо ограничить доступ для некоторых пользователей.
- `all_squash` — подразумевает, что все подключения будут выполняться от анонимного пользователя;
- `subtree_check` (`no_subtree_check`)- в некоторых случаях приходится экспортировать не весь раздел, а лишь его часть. При этом сервер NFS должен выполнять дополнительную проверку обращений клиентов, чтобы убедиться в том, что они предпринимают попытку доступа лишь к файлам, находящимся в соответствующих подкаталогах. Такой

контроль поддерев (subtree checks) несколько замедляет взаимодействие с клиентами, но если отказаться от него, могут возникнуть проблемы с безопасностью системы. Отменить контроль поддерев можно с помощью опции `no_subtree_check`. Опция `subtree_check`, включающая такой контроль, предполагается по умолчанию. Контроль поддерев можно не выполнять в том случае, если экспортируемый каталог совпадает с разделом диска.

- `anonuid=1000` — привязывает анонимного пользователя к «местному» пользователю;
- `anongid=1000` — привязывает анонимного пользователя к группе «местного» пользователя.

Например, строка конфигурационного файла может выглядеть таким образом:

```
/srv/nfsshare 192.168.122.2(rw,nohide,all_squash,anonuid=1000,anongid=1000,no_subtree_check)
```

После внесения изменений для того, чтобы они вступили в силу, нужно выполнить команду

```
sudo exportfs -ra
```

На клиенте необходимо примонтировать настроенный ресурс. Для получения списка доступных ресурсов воспользуйтесь командой

```
sudo showmount -e 192.168.122.2
```

где 192.168.122.2 – адрес сервера NFS.

Чтобы примонтировать каталог возможно воспользоваться командой `mount`

```
sudo mount 192.168.122.2:/srv/nfsshare /mnt/nfs
```

## 1.4. NTP-сервер

**NTP** (англ. *Network Time Protocol* — *протокол сетевого времени*) — сетевой протокол для синхронизации внутренних часов компьютера с использованием сетей.

Для синхронизации времени в системах GNU/Linux используется демон **ntpd** (**N**etwork **T**ime **P**rotocol **d**aemon). Для его установки применяется команда

```
sudo apt install ntp
```

Принцип работы NTP основан на использовании иерархии серверов, которая обеспечивает распределение точного времени по всей сети. Уровни этой иерархии называются стратами (англ. *strata*). Высший уровень 0 представляет источники времени такие как атомные часы. Следующий уровень 1 — это серверы, которые получают точное время от нулевого уровня и сами могут служить источником времени для серверов следующего уровня 2. Этот процесс продолжается до достижения конечных клиентских устройств.

Иерархическая структура протокола NTP построена с учетом отказоустойчивости и избыточности. В случае потери соединения с вышестоящими серверами NTP резервные серверы берут процесс синхронизации на себя. За счёт избыточности обеспечивается постоянная доступность NTP-серверов. Синхронизируясь с несколькими серверами, NTP использует данные всех источников, чтобы рассчитать наиболее точное время.

В качестве примера рассмотрим локальную сеть, состоящую из NTP-сервера и его клиента и изолированную от глобальной сети Интернет. По умолчанию сервер настроен на получение точного времени от прописанных в конфигурационном файле вышестоящих серверов. Однако при отсутствии связи с сетью Интернет, сервер будет высылать по запросу своё системное время.

Конфигурационный файл имеет путь `/etc/ntpsec/ntp.conf`. Он содержит начальные настройки и примеры конфигурирования для различных задач. Рекомендуется сделать резервное копирование файла с помощью команды

```
sudo cp /etc/ntpsec/ntp.conf /etc/ntpsec/ntp.conf.orig
```

Для понимания процесса настройки сервера, удалим конфигурационный файл командой **sudo rm /etc/ntp.conf** и в редакторе создадим новый командой

```
sudo nano /etc/ntpsec/ntp.conf
```

В пустой файл впишем следующую строку

```
server 127.127.1.0 prefer
```

Директива **server** указывает, к какому серверу необходимо подключиться для получения точного времени. IP-адрес 127.127.1.0 – это адрес, по которому сервер получает своё системное время, которое и будет отправлять по запросу клиенту. Опция **prefer** в данном случае указывается обязательно, так как серверу не нравится факт использования своего времени из-за высокой вероятности рассинхронизации с точным мировым временем.

После внесения изменений в конфигурационный файл необходимо перезагрузить службу командой **sudo systemctl restart ntp**. Проверить текущее состояние службы можно командой **status** вместо **restart**.

В качестве теста запустим эмулятор терминала на клиенте и введём команду **sudo ntpdate A.B.C.D**, где A.B.C.D – IP-адрес локального NTP-сервера. В случае успеха будет показано, насколько установленное на клиенте время отличается от времени сервера.

### 1.5. Основы безопасности локальной вычислительной сети

Локальная вычислительная сеть, в каком бы виде она ни была (домашняя или корпоративная), всегда подвержена угрозам как снаружи (из внешней глобальной сети), так и изнутри (со стороны сотрудников или подключившегося к ЛВС злоумышленника).

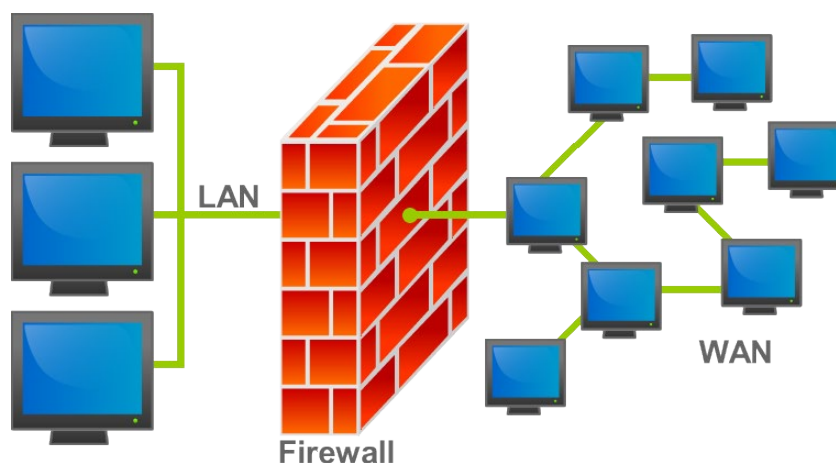
В обязанности сетевого администратора входит разграничение прав доступа к различным ресурсам ЛВС, а также установление политики доступа к глобальной сети Интернет (если сама сеть физически подключена к нему).



Существует множество методов защиты, как аппаратных, так и программных.

**Межсетевой экран (Брандмауэр, Firewall)** – средство межсетевой защиты, которое позволяет разделить общую сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов через границу из одной части общей сети в другую.

Как правило, граница проводится между корпоративной (локальной) сетью организации и глобальной сетью. МЭ пропускает через себя весь трафик, принимая для каждого пакета решение – пропускать его или отбросить.



В операционных системах GNU/Linux используется встроенное в ядро Linux межсетевой экран **Netfilter**. Для его конфигурирования применяется утилита **ufw** (Uncomplicated Firewall, с англ. — «незамысловатый межсетевой экран»).

Основные команды **ufw** для командной строки:

Команда	Описание
<b>ufw enable</b>	Включить firewall, т.е. перевести его в активное состояние
<b>ufw status</b>	Просмотр текущего состояния
<b>ufw status verbose</b>	Подробная информация о состоянии
<b>ufw app list</b>	Вывести список известных правил для приложений
<b>ufw allow</b> <i>имя_приложения/порт</i>	Добавить разрешающее правило для приложения, например <b>ufw allow SSH</b> или <b>ufw allow 22</b>
<b>ufw deny</b> <i>имя_приложения/порт</i>	Добавить запрещающее правило для приложения, например <b>ufw deny SSH</b> или <b>ufw deny 22</b>
<b>ufw show added</b>	Просмотреть добавленные пользователем правила

<b>ufw logging [on off]</b>	Включить выключить запись логов. Прочитать их возможно с помощью dmesg
<b>ufw reset</b>	Восстановить правила и состояние "по умолчанию". Так как "по умолчанию" сервис выключен, после этой команды его нужно включить: <b>ufw enable</b>
<b>ufw disable</b>	Отключить firewall

*Примечание: более подробно примеры использования ufw смотреть в тап.*

Обратите внимание, после перезагрузки значения, установленные пользователем сохраняются.

## Основы DHCP

**DHCP** (*Dynamic Host Configuration Protocol*) — протокол, позволяющий хостам автоматически получать IP-адреса и другие сетевые настройки.

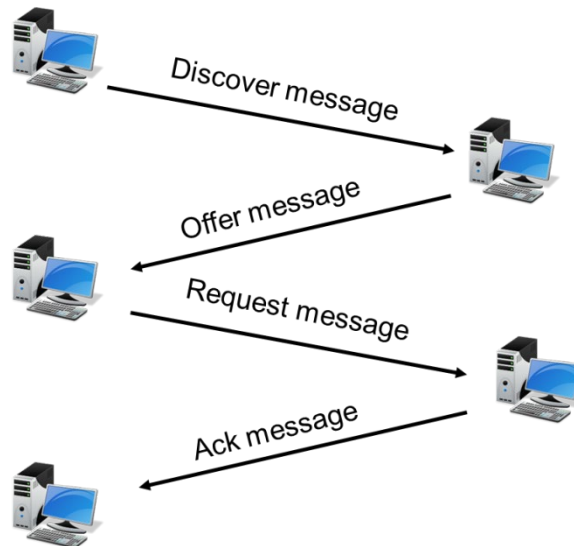
Подход, при котором сетевая конфигурация устройства выполняется вручную и ему статически задаётся определённый адрес определённой настройки сети, довольно надёжен и оправдывает себя в случае, когда данной устройством значительную часть времени проводит в рамках одной и той же сетевой инфраструктуры (пример: сервер). Однако в случае с более мобильными устройствами или с устройствами без собственной конфигурации сети применяется протокол DHCP.

Работа протокола DHCP базируется на классической схеме **клиент-сервер**. Для того, чтобы получить адрес по DHCP, клиент отправляет UDP-диаграммы на специальный broadcast (широковещательный) адрес 255.255.255.255 и порт 67 с src адресом 0.0.0.0:68. Если DHCP-сервер получает такой пакет, он отвечает, предлагая свои услуги. Клиент запрашивает у сервера адрес, и сервер выдаёт его клиенту.

IP-адреса выдаются на определённый промежуток времени, который называется временем аренды (lease time). Очевидно, что DHCP-адреса в интернете не маршрутизируются, и это работает исключительно в пределах локальной сети.

В качестве DHCP-сервера на \*nix чаще всего используется референсная реализация — `isc-dhcpd`. Она поставляется в пакете DHCP.

### Протокол DHCP



Взаимодействие DHCP-серверов с клиентами осуществляется путем обмена сообщениями. Работа протокола DHCP осуществляется по принципу клиент-сервер. Для получения настроек используется схема DORA (Discover-Offer-Request-Acknowledge). Сам процесс состоит из следующих этапов:

- Обнаружение (Discover). После подключения клиента начинается процесс его инициализации в сети. Он находит подходящий DHCP-сервер путем отправки специального запроса DHCPDISCOVER на адрес 255.255.255.255. Учитывая отсутствие собственного IP, в таком запросе указывается 0.0.0.0 и MAC. Запрос поступает на все ПК в соответствующем сегменте сети. При этом ответ на него автоматически отправляется только DHCP-серверами.
- Предложение (Offer). Получив от клиента запрос, DHCP-сервер осуществляет его обработку и выполняет подбор сетевую

конфигурацию. Эта конфигурация направляется клиенту в обратном сообщении DHCPOFFER, которое, как правило, передается на указанный MAC. Однако в некоторых случаях применяется широковещание. При нахождении нескольких серверов в пределах сети клиенту приходит соответствующее количество DHCPOFFER, из которых он выбирает один (обычно первый по времени получения).

- **Запрос (Request).** После получения DHCPOFFER клиент передает серверу специальное сообщение DHCPREQUEST, которое содержит запрос настроек. В этом запросе дублируется информация из DHCPDISCOVER, а также указывает IP-адрес избранного на предыдущем этапе DHCP-сервера.
- **Подтверждение (Acknowledge).** После получения DHCPREQUEST избранный DHCP-сервер выполняет фиксацию соответствующей привязки для клиента и направляет ему в ответ сообщение DHCPACK. В нем подтверждаются предоставленные автоматически настройки. Это сообщение передается на адрес MAC клиента, который был указан на предыдущем этапе. Получив DHCPACK, клиент проводит автоматическую проверку предоставленных настроек и применяет конфигурацию сети, полученную от сервера.

Способы	назначения	адресов
---------	------------	---------

*Статическое назначение* — назначение, при котором адрес устройства не должен меняться — например, если это сетевой принтер, — обычно используют статическое назначение. Администратор создаёт на DHCP-сервере таблицу распределения: вносит в неё MAC-адреса, которым нужен статический адрес, и назначает каждому IP-адрес.

*Динамическое назначение* — это самый распространённый способ назначения адресов. IP-адрес и другие параметры сетевой конфигурации назначаются каждому клиенту по запросу на срок аренды, определяемый администратором. Когда этот срок истекает, клиент снова запрашивает у сервера эту конфигурацию.

*Автоматическое назначение* — назначение, при котором администратор выделяет специальный диапазон IP-адресов. При первом подключении к сети устройство получает из этого диапазона первый свободный адрес и другие сетевые настройки. На сервере создаётся таблица соответствий IP- и MAC-адресов, и в дальнейшем все устройства в таблице получают те адреса, которые им были назначены при первом подключении. При этом время аренды не ограничивается. От статического назначения этот способ отличается тем, что администратор не участвует в составлении этой таблицы — она создаётся на сервере автоматически по мере подключения новых устройств.

## Настройка DHCP

Для установки DHCP сервера воспользуйтесь следующей командой:

```
sab@server: /$ apt-get install fly-admin-dhcp
```

Обратите внимание, что при установке на экране могут появиться сообщения об ошибках. Проигнорируйте их.

Основные конфигурационные файлы:

/etc/default/isc-dhcp-server	установка значений по умолчанию
/etc/dhcp/dhcpd.conf	настройка сервера dhcp

В файле со значениями по умолчанию необходимо выбрать интерфейс, на котором будет работать сервер и с которого будут передаваться адреса другим устройствам. Например, `INTERFACESv4="enp1s0"`. Адрес у указанного

интерфейса должен быть задан статически и находиться в той же подсети, из которой будут выдаваться другие адреса.

В `named.conf` содержатся только директивы `include`. Обратим внимание, что устанавливать нужно целиком весь пакет, с графической оболочкой. Иначе сервер может некорректно работать.

`/etc/dhcp/dhcpd.conf`:

- `default-lease-time` задает время лизинга по умолчанию (в секундах);
- `max-lease-time` задает максимальное время лизинга;
- Директива `option` определяет, какие TCP/IP настройки будут передаваться клиенту:
  - `option broadcast-address` – задает широковещательный адрес
  - `option domain-name` имя\_домена; – задает имя домена;
  - `option domain-name-servers` список\_DNS\_серверов; - определяет используемые DNS серверы;
  - `option routers` IP\_адрес; – определяет маршрут по умолчанию.
  - `option subnet-mask` – определяет маску подсети
- Для описании топологии используются секции:
  - `subnet` адрес\_сети netmask сетевая\_маска {...} - описание сети;
  - `host` имя\_хоста {...}- описание хоста;
- Директива `range` внутри секции `subnet` определяет, какой диапазон адресов будет использоваться для назначения динамических адресов клиентам;
- Директивы `hardware` и `fixed-address` внутри секции `host` используются для задания статических адресов. MAC адрес сетевого интерфейса сопоставляется получаемому IP адресу.

### Пример настройки DHCP

*Пример*                      *задания*                      *динамических*                      *адресов:*

```
subnet 192.168.1.0 netmask 255.255.255.0
{
    range 192.168.1.100 192.168.1.150;
}
```

```
/etc/dhcp/dhcpd.conf
```

Пример задания статических адресов:

```
host comp1.example.ru
{
    hardware ethernet 00:DE:AA:10:35:BE;
    fixed-address 192.168.1.151;
}
```

### Настройка на клиенте

Сбросить динамический адрес на клиенте:

```
sab@server: /$ dhclient -r
```

Запросить новый динамический адрес:

```
sab@server: /$ dhclient
```

```
Настройка сети
/etc/network/interfaces/

auto eth0
iface eth0 inet dhcp
```

## 2. Практическая часть

### 2.1. Задание 1

1. На сервере создайте локальный FTP-репозиторий и загрузите на него файл, содержащий в названии ваши ФИО. Выгрузите файл из созданного репозитория на машину workstation.
2. Создайте на сервере общую папку smb и примонтируйте её на машине Node1 в директорию /mnt/ваши\_инициалы\_smb. (Например, /mnt/sabsmb)
3. Создайте на сервере общую папку nfs и примонтируйте её на машине Node1 в директорию /mnt/ваши\_инициалы\_nfs. (Например, /mnt/sabnfs)

## 2.2. Задание 2

- 2.2.1. Настройте межсетевой экран перед включением. Для этого добавьте правило, разрешающее подключение к серверу по SSH.
- 2.2.2. Включите встроенный межсетевой экран на сервере и выполните сброс текущего состояния.
- 2.2.3. Проверьте доступность nfs и smb директорий. Настройте к ним доступ. Для этого укажите разрешающее правило, используя название службы у nfs и порт у smb. Выключите межсетевой экран.

## 2.3. Задание 3.

- 2.3.1. На node1, поменяйте дату и время на 01.01.1970 и 18:12. Для этого воспользуйтесь командой date. Формат записи выясните, используя утилиту man.
- 2.3.2. Синхронизируйте время Server и node1 по сети, установив NTP-сервер на машину Server и добавив её в автозагрузку.

## 2.3. Задание 4 \*.

Перед выполнением задания вам необходимо отключить DHCP на виртуальном мосте KVM. Для этого в командной строке workstation откройте окно изменения конфигурации сети. Для этого выполните команду:

```
virsh net-edit default
```

В качестве текстового редактора выберите ваш любимый и в отрывшемся файле прокомментируйте строки:

```
<dhcp>  
  <range start='192.168.122.2' end='192.168.122.254'>  
</dhcp>
```

У XML - комментария следующая форма: <!-- комментарий -->

1. Установите DHCP сервер на серверную машину.
2. Выделите диапазон 192.168.122.(N в группе + 100) - (N в группе + 80) для выдачи динамических адресов. Укажите в качестве DNS адреса – 8.8.8.8, роутер по умолчанию – 192.168.122.1
3. Запустите службу DHCP и убедитесь, что она работает корректно
4. Измените настройки DHCP таким образом, чтобы машине node1 всегда выдавался адрес 192.168.122.(ваш день рождения). Проверьте это.



### **Контрольные вопросы**

1. Как работает Firewall?
2. Какие существуют способы передачи файлов по сети?
3. Как работает протокол DHCP?
4. Какие существуют способы назначения адресов DHCP?