Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина» (УрФУ)

Институт радиоэлектроники и информационных технологий – РтФ

Школа профессионального и академического образования

Отчет по дисциплине   
«Операционные системы»

Лабораторная работа №8  
«Настройки сетевых интерфейсов в ОС Linux»

Студенты: Клоченко И.Е., Юсупов Д.А.

Преподаватель: Коротяев А.Н.

Группа: РИ-300024

Екатеринбург

2023

**Оглавление**

[1. **Работа с физическими сетевыми интерфейсами** 3](#_Toc136813104)

[2. **Работа с виртуальными сетевыми интерфейсами** 11](#_Toc136813105)

[3. **Генерация ключей RSA для подключения по SSH** 21](#_Toc136813106)

[**Вывод:** 24](#_Toc136813107)

**Цель работы:** получение знаний и практических навыков по работе с сетевыми интерфейсами в ОС Linux, реализация подключения по протоколу SSH, создание, настройка и конфигурирование виртуальных сетевых интерфейсов.

**Ход работы:**

Комментарий: Лабораторная работа выполнена в CentOS 7, установленной на виртуальной машине VMWare Workstation. Вторая виртуальная машина была клонирована из первой. Имя пользователя в первой машине – dmitriy, во второй – dmitriy2. Настройки сети в обеих виртуальных машинах – сетевой мост. Данный тип соединения предназначен для объединения сегментов компьютерной сети в единую сеть.

# **Работа с физическими сетевыми интерфейсами**

Команда *ifconfig* предназначена для вывода информации о сетевых интерфейсах, включая статистику переданных пакетов, IP-адрес, маску сети, MAC-адрес и др.

Команда *netstat -nr* выводит на экран таблицу шлюзов по умолчанию с указанием интерфейса.

Команда *ip r* позволяет список шлюзов по умолчанию с указанием IP-адреса источника (сетевого интерфейса).

Вывод этих трех команд представлен на рисунке 1.

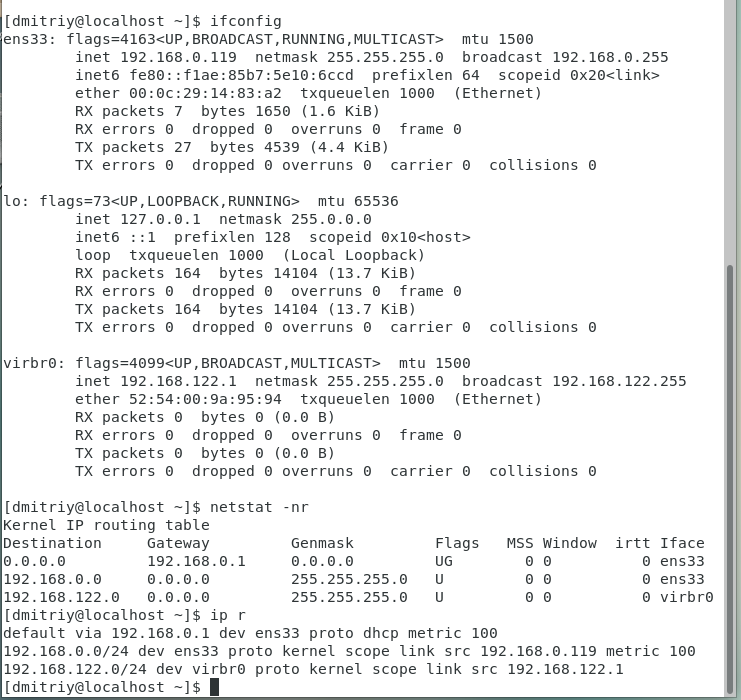


Рисунок 1. Вывод команд *ifconfig*, *netstat -nr*, *ip r*

Основным сетевым устройством на данной виртуальной машине является интерфейс с именем *ens33*. Его IP-адрес – 192.168.0.119, маска сети – 255.255.255.0, MAC-адрес – 00:0c:29:14:83:a2.

Для отключения интерфейса можно воспользоваться командой *ifdown <device>* (стоит отметить, что для выполнения этой команды нужны права суперпользователя). В результате отключения интерфейса вывод утилит *ifconfig*, *netstat -nr* и *ip r* изменился (рисунок 2):

* в выводе команды *ifconfig* больше не написан IP-адрес, маска сети;
* в выводе команд *netstat -nr* и *ip r* в шлюзах по умолчанию больше не выводятся данные с интерфейса ens33.

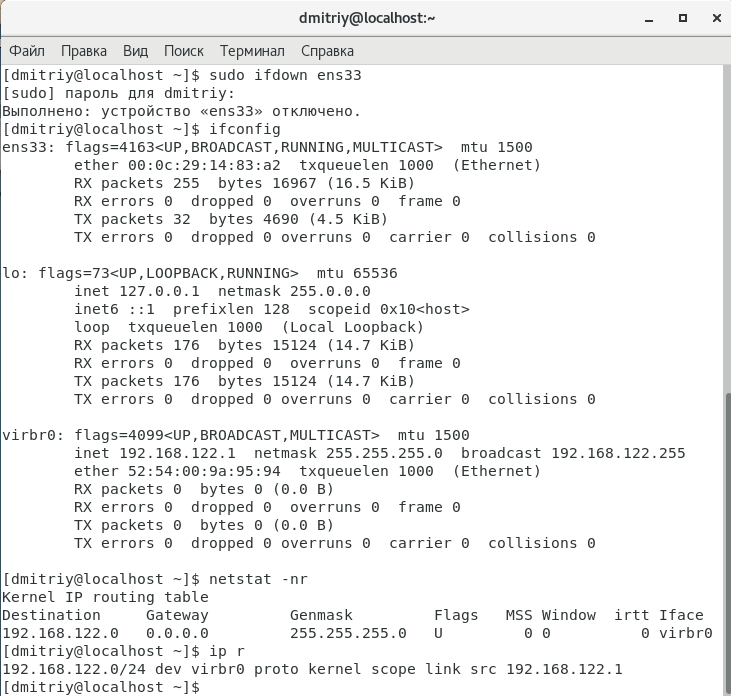


Рисунок 2. Вывод команд *ifconfig*, *netstat -nr*, *ip r* при отключенном сетевом интерфейсе

Для включения сетевого интерфейса *ens33* необходимо выполнить команду *ifup ens33* (для этой команды также необходимы права суперпользователя). Включение интерфейса представлено на рисунке 3.

Выключить все сетевые устройства можно при отключении сервиса *network*, команда: *service network stop*. При этом в выводе команд *ifconfig*, *netstat -nr*, *ip r* исчезают все сетевые интерфейсы, кроме виртуального моста (*virbr0*). Значок успешного подключения к интернету в трее исчезает, эхо-тестирование до ресурса google.com не удалось. Все эти действия представлены на рисунке 3.

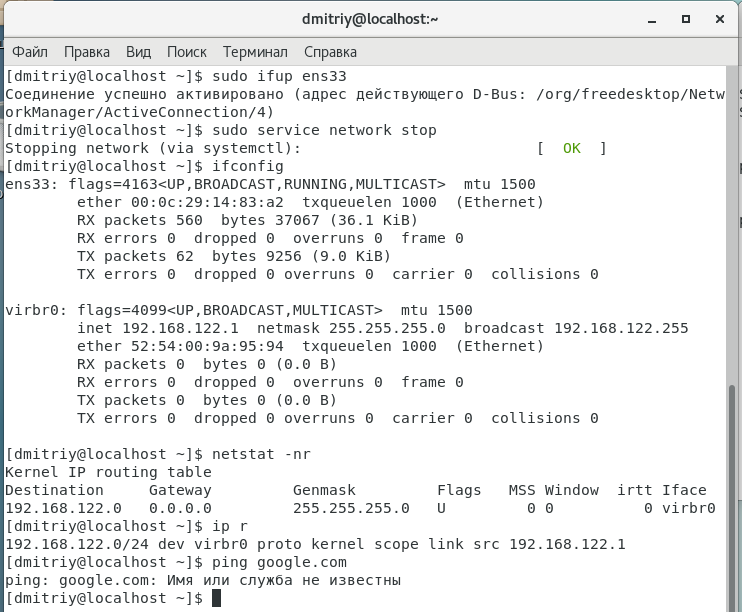


Рисунок 3. Отключение сервиса сети

Для включения сетевого сервиса необходимо выполнить команду *service network start*.

Для проверки связи между узлами можно воспользоваться эхо-тестированием (утилита *ping <IP-адрес>*). Для проверки работоспособности петли обратной связи (интерфейс *lo*) необходимо выполнить команду *ping 127.0.0.1* или *ping localhost* (рисунок 4).

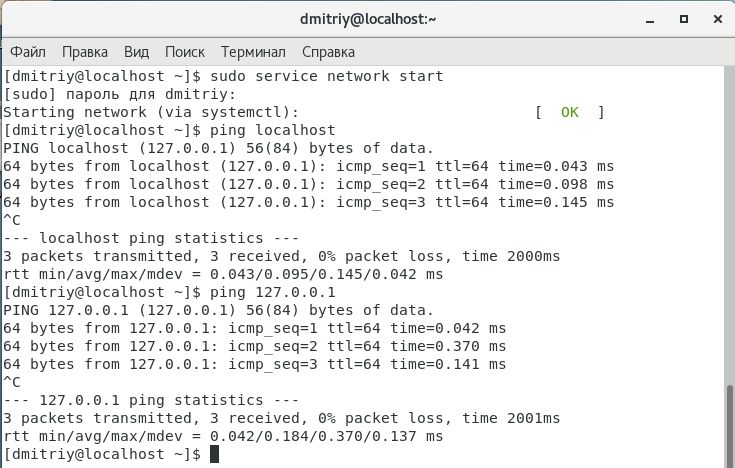


Рисунок 4. Эхо-тестирование петли обратной связи

Для эхо-тестирования между двумя виртуальными машинами необходимо получить их IP-адреса:

* IP-адрес 1-й машины: 192.168.0.119;
* IP-адрес 2-й машины: 192.168.0.121.

С 1-й машины выполняю эхо-тестирование узла сети с IP-адресом 192.168.0.121, со 2-й – 192.168.0.119 (рисунок 5, 6).

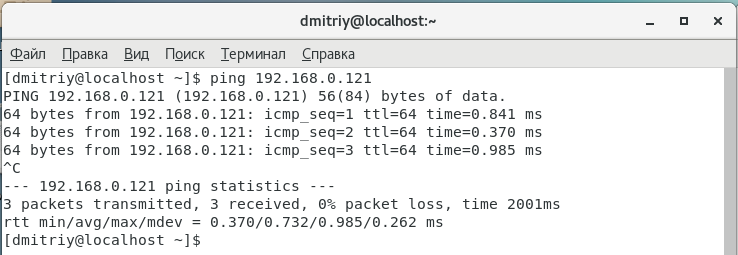


Рисунок 5. Эхо-тестирование 2-й ВМ

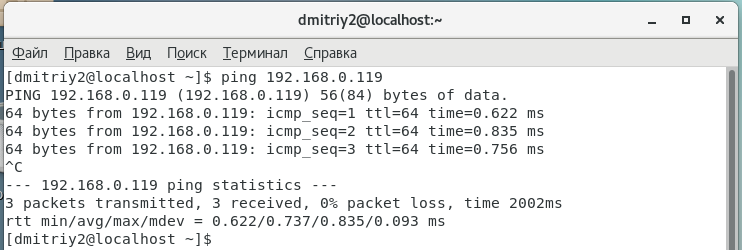


Рисунок 6. Эхо-тестирование 1-й ВМ

Директория */etc/sysconfig/network-scripts/* содержит скрипты (сценарии) для организации работы с сетевыми устройствами. Ее содержимое представлено на рисунке 7.

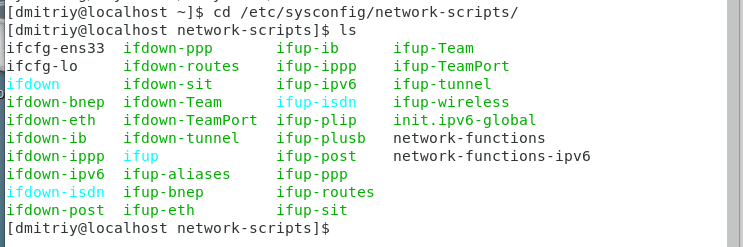


Рисунок 7. Сценарии для работы с сетевыми устройствами

Сценарий конфигурации основного сетевого интерфейса имеет имя *ifcfg-ens33*. После его изучения (рисунок 8) можно сделать следующие выводы:

* используется динамическая настройка параметров сети (DHCP);
* поддерживается протокол IPv6;
* тип устройства – проводное соединение (Ethernet);
* связанный прокси-сервер отсутствует.

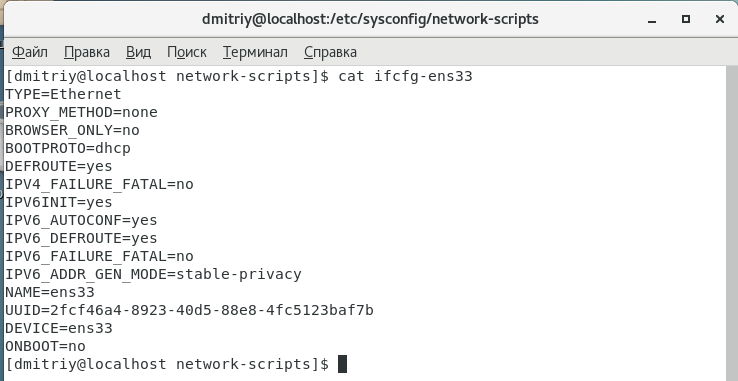


Рисунок 8. Сценарий работы сетевого интерфейса *ens33*

Для произведения подключения по протоколу SSH необходимо выполнить команду: *ssh <имя-пользователя>@<IP-адрес\_или\_домен>*. При отсутствии явного указания имени пользователя производится попытка подключения с именем пользователя, с которым был выполнен вход в систему. В данном случае для подключения из второго окна терминала достаточно указать *ssh localhost*, так как имена пользователей совпадают.

Команда *who* позволяет вывести на экран всех пользователей, которые вошли в систему, и терминал их входа. Для выхода из сессии SSH можно воспользоваться сочетанием клавиш Ctrl+C или командой *exit*. Процесс подключения к хосту и отключения от него по протоколу SSH, изменения в списке пользователей, выполнивших вход в систему, представлен на рисунке 9.

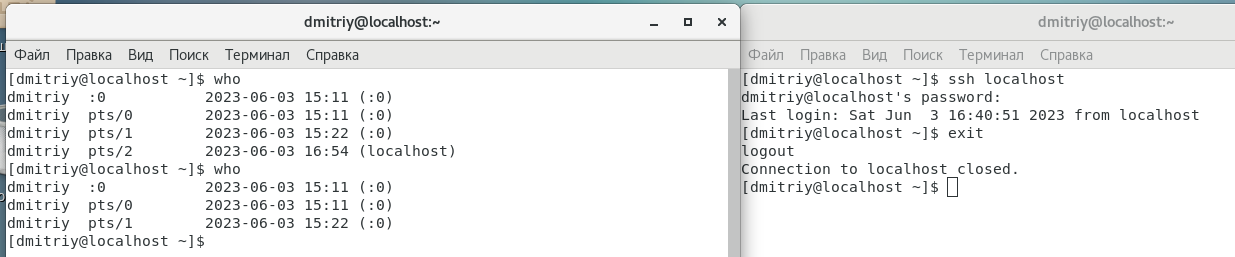


Рисунок 9. Подключение по SSH к localhost

Для выполнения входа как суперпользователь необходимо выполнить команду *ssh root@localhost*. Инициируем подключение и вновь проверим список пользователей, выполнивших вход в систему (рисунок 10). Теперь вместо пользователя *dmitriy* в выводе команды *who* можно наблюдать пользователя *root*.

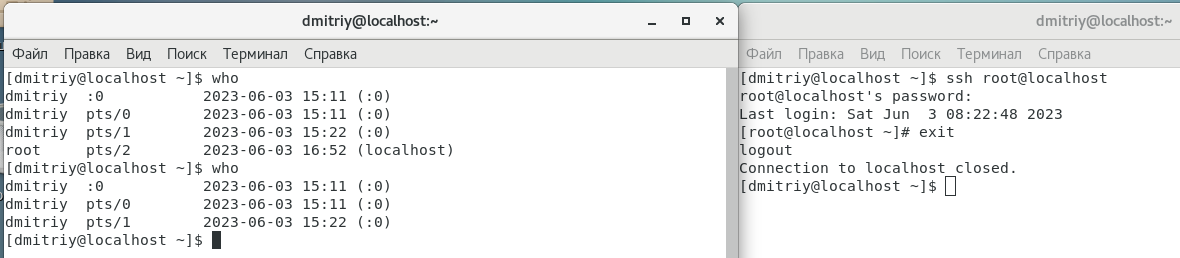


Рисунок 10. Подключение по SSH к localhost как суперпользователь

Для инициации подключения по SSH со второй машины к первой необходимо вместо *localhost* указать IP-адрес первого хоста. Так как имена пользователей на машинах различаются (на первой машине пользователь dmitriy, на второй – dmitriy2), необходимо явно указать имя пользователя, под которым требуется выполнить вход. Команда: *ssh* [*dmiitriy@192.168.0.119*](mailto:dmiitriy@192.168.0.119) (рисунок 11). При этом при выводе списка пользователей, вошедших в систему, на второй машине изменений нет, на первой машине появляется вход под пользователем *dmitriy* с указанием IP-адреса подключения (рисунок 12).

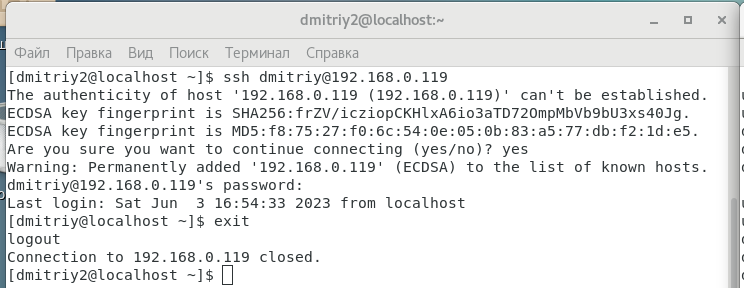


Рисунок 11. Подключение по SSH с удаленного хоста

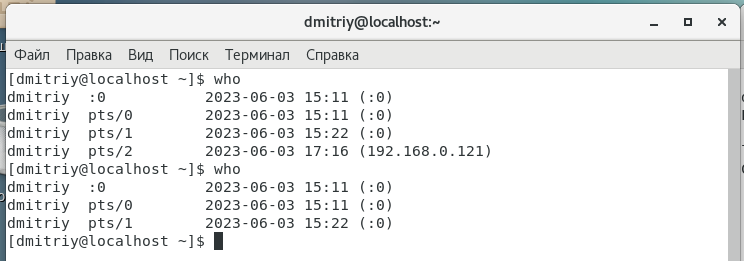


Рисунок 12. Список пользователей, вошедших в систему на 1-м хосте

Вход на вторую машину под пользователем *root* осуществляется командой *ssh* [*root@192.168.0.121*](mailto:root@192.168.0.121) (рисунок 13).

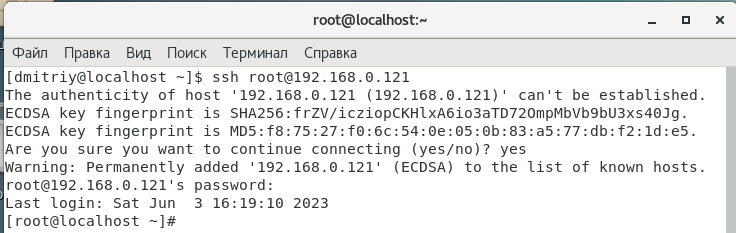


Рисунок 13. Подключение по SSH ко второму хосту как пользователь *root*

# **Работа с виртуальными сетевыми интерфейсами**

Для создания виртуального сетевого устройства с названием *ens33* с идентификационным номером (id) 100 предлагается использование команды: *ip l a ens33 name ens33.100 type vlan id 100*. Однако эта команда завершается с ошибкой «Некорректный аргумент». Официальная документация RedHat предлагает настройку виртуального сетевого интерфейса типа vlan с помощью создания конфигурационного файла в директории */etc/sysconfig/network-scripts/* с названием *ifcfg-ens33.100* с содержимым:

*DEVICE=ens33.100*

*BOOTPROTO=none*

*ONBOOT=yes*

*IPADDR=192.168.0.135*

*PREFIX=24*

*NETWORK=192.168.0.0*

*VLAN=yes*

В конфигурационном файле сразу же указывается IP-адрес интерфейса и маска сети. IP-адрес был задан исходя из его незанятости в сети.

После перезапуска сервиса *network* с помощью команды *systemctl restart network* виртуальный интерфейс находится в состоянии *up*, это означает, что он запущен (проверено с помощью команды *ifconfig*, рисунок 14).

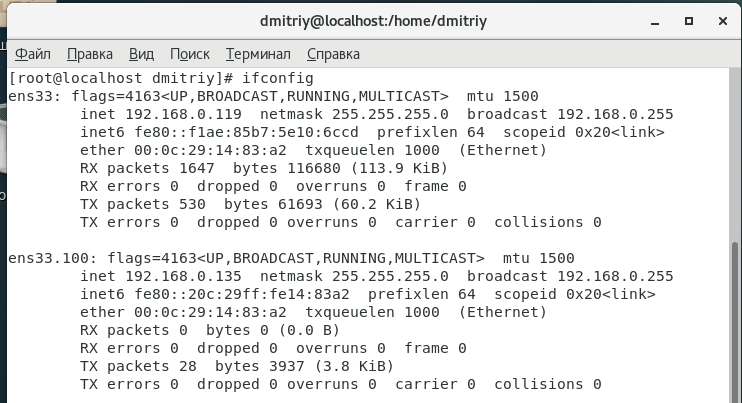


Рисунок 14. Виртуальный интерфейс *ens33.100*

Со второй виртуальной машины эхо-тестирование завершилось успешно, пакеты отправляются и принимаются.

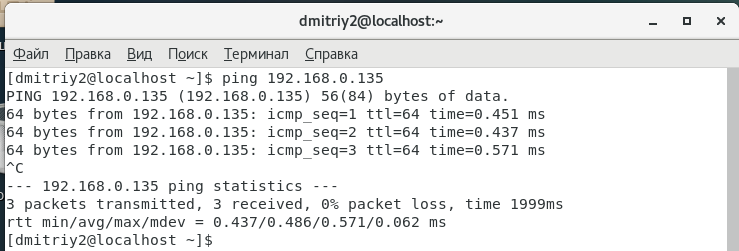


Рисунок 15. Эхо-тестирование виртуального сетевого интерфейса со второй виртуальной машины

Имя локального хоста можно узнать с помощью двух команд:

* команда *hostname*;
* команда *uname -n*.

Результат обеих команд представлен на рисунке 16.

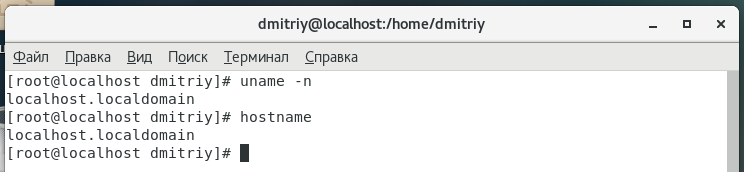


Рисунок 16. Вывод имени хостовой машины

Изменение имени хоста производится командой *hostnamectl set-hostname <name.domain>*. Изменение имени и эхо-тестирование этого домена представлено на рисунке 17.

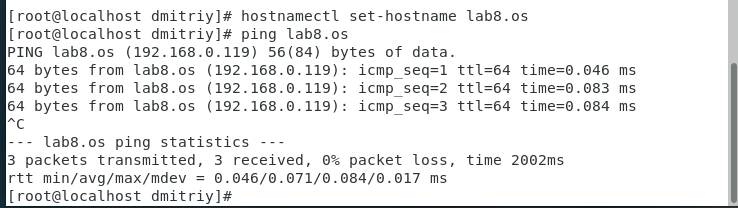


Рисунок 17. Изменение имени хоста и его эхо-тестирование

Изменения имени хоста отображаются в файле */etc/hostname* (рисунок 18).

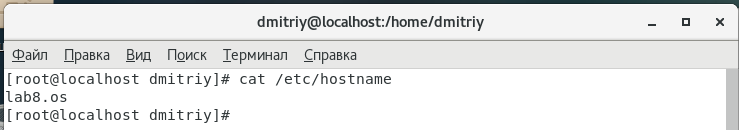


Рисунок 17. Файл */etc/hostname*

Соответственно, при изменении данного файла изменяется имя хоста. После изменении содержимого файла на *lab8os.os* было произведено повторное эхо-тестирование измененного хоста. Результат представлен на рисунке 18.

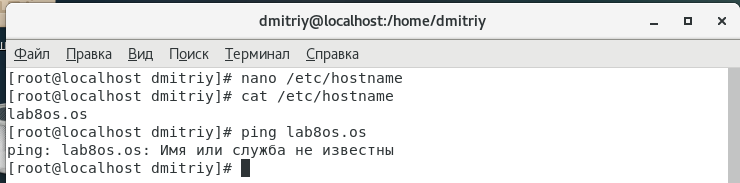


Рисунок 18. Изменение файла */etc/hostname* вручную

При изменении файла */etc/hostname* вручную не изменяется файл */etc/hosts*, который отвечает за соответствие доменного имени IP-адресу. Поэтому для того, чтобы доменное имя применилось в сети, необходимо либо использовать команду *hostnamectl set-hostname*, либо после изменения файла */etc/hostname* добавлять изменения в файл */etc/hosts*.

Вывод на экран шлюзов по умолчанию выполняется командой *netstat -nr* (рисунок 19).

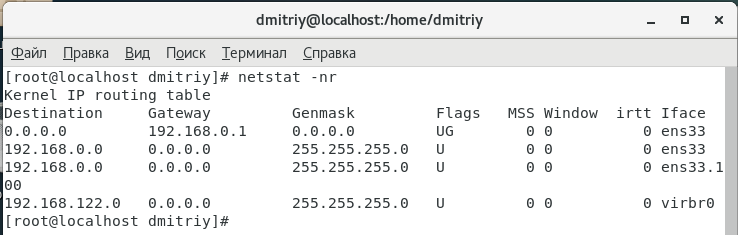


Рисунок 19. Вывод на экран шлюзов по умолчанию

Команда *nmtui* позволяет запустить интерактивную утилиту управления сетевыми подключениями. Ее интерфейс представлен на рисунке 20.

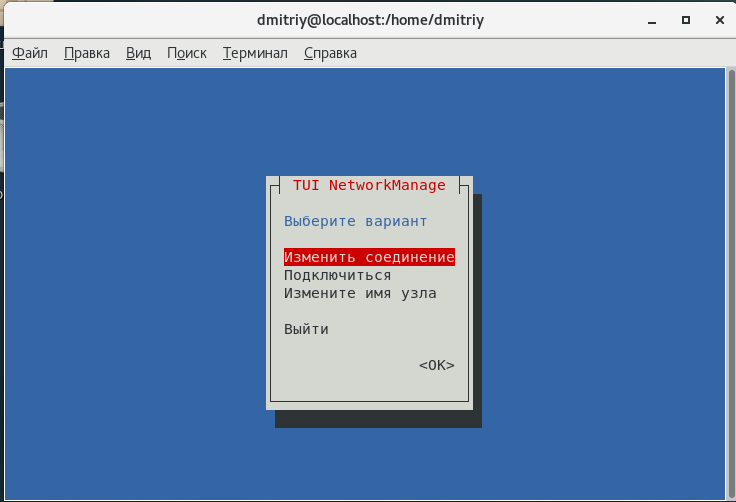


Рисунок 20. Интерфейс утилиты TUI NetworkManage

В разделе «Изменить соединение» при нажатии кнопки добавить предлагается выбрать тип интерфейса (рисунок 21).

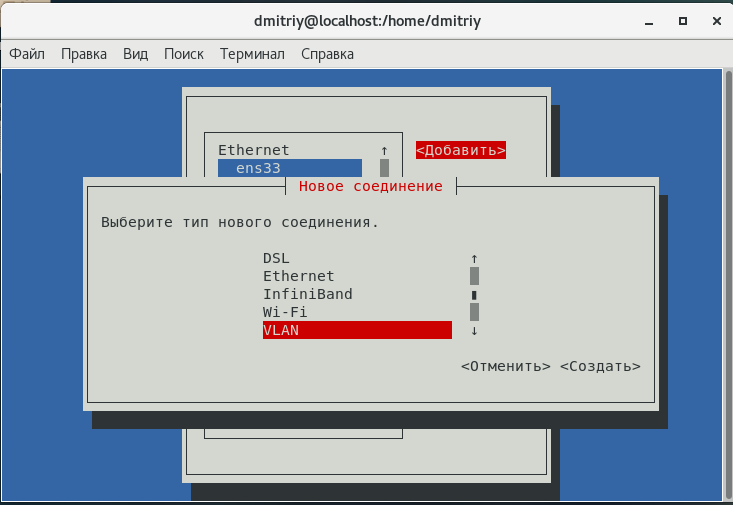
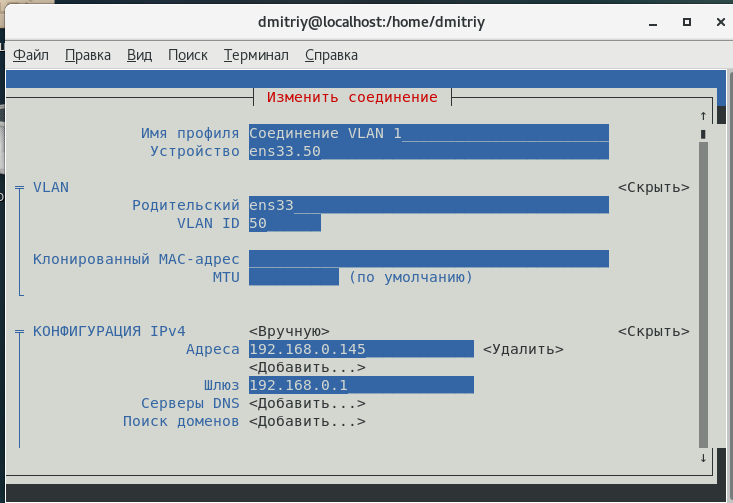


Рисунок 21. Выбор типа создаваемого интерфейса

Родительским интерфейсом будет указан интерфейс *ens33*, IP-адрес – 192.168.0.145, IPv6 отключен (настройки приведены на рисунке 22 и 23).



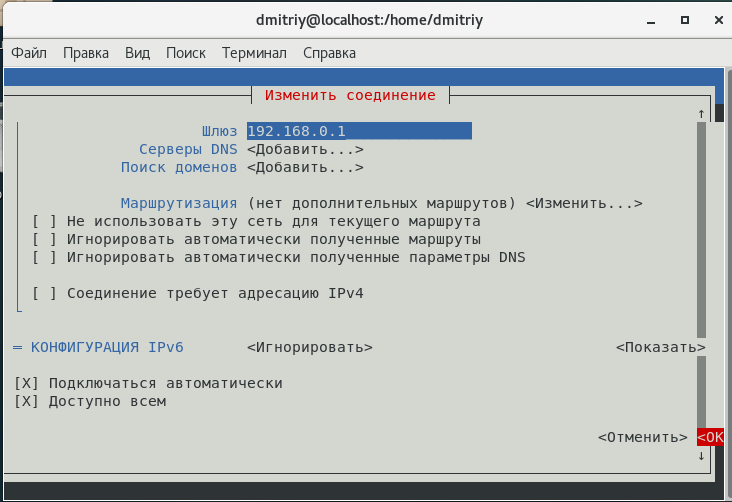


Рисунок 22, 23. Конфигурация виртуального интерфейса

Новый виртуальный интерфейс был добавлен и запущен (рисунок 24).

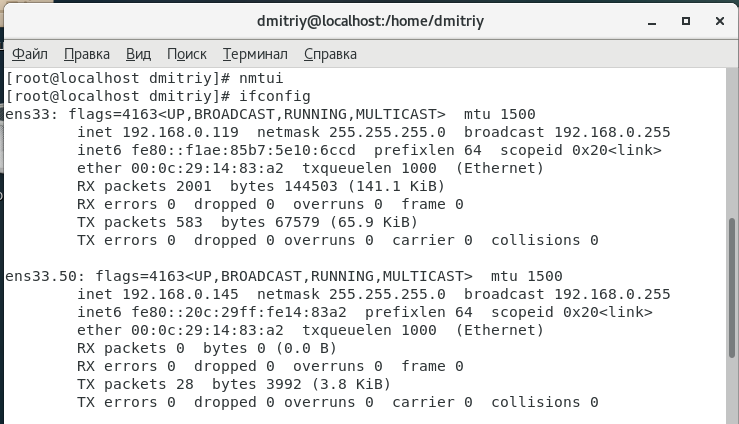


Рисунок 24. Проверка добавления нового интерфейса

Для тестирования его работоспособности необходимо произвести эхо-тестирование со второй виртуальной машины (рисунок 25).

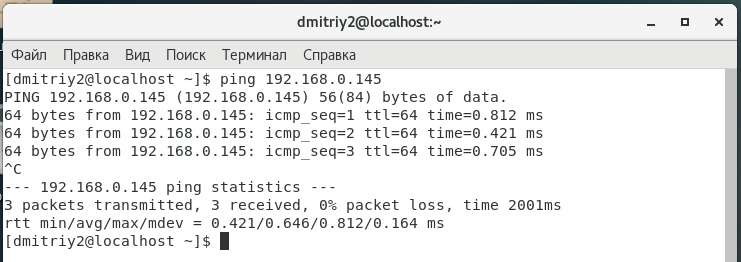


Рисунок 25. Эхо-тестирование интерфейса *ens33.50*

Конфигурационные файлы сетевых интерфейсов находятся по пути */etc/sysconfig/network-scripts*. После добавления нового интерфейса в утилите TUI Network Manage был создан конфигурационный файл *ifcfg-Соединение\_VLAN\_1*. Его структура указана на рисунке 26.

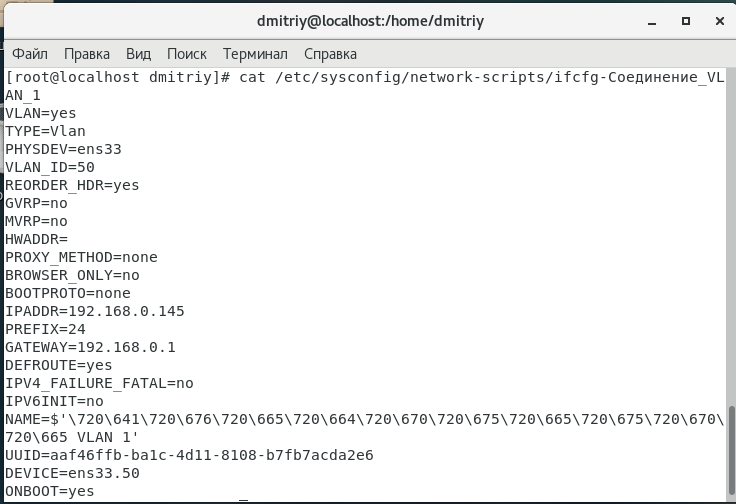


Рисунок 26. Структура конфигурационного файла сетевого интерфейса

Далее необходимо создать второй виртуальный сетевой интерфейс с автоматической конфигурацией (рисунок 27). Для сравнения конфигурационных файлов интерфейса, настроенного вручную, и интерфейса, сконфигурированного автоматически, можно воспользоваться командой *diff* (рисунок 28).

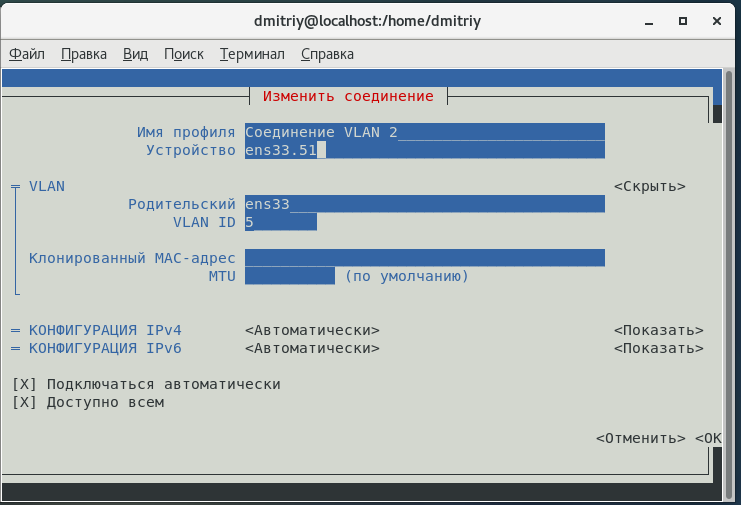


Рисунок 27. Создание интерфейса с автоматической конфигурацией

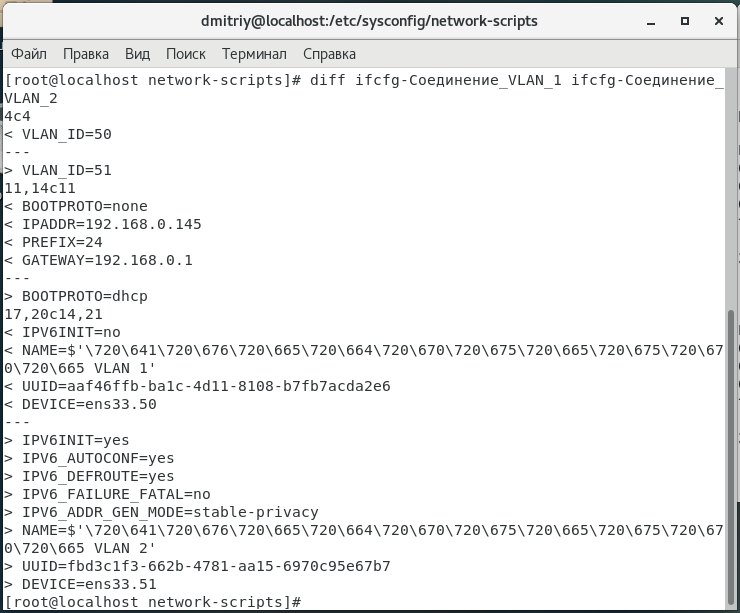


Рисунок 28. Сравнение конфигурационных файлов

Файлы отличаются:

* различными идентификаторами VLAN и именами интерфейсов;
* для первого интерфейса настройки сети ручные, для второго используется протокол DHCP;
* для первого интерфейса IPv6 отключен, во втором имеются пункты по конфигурации этого протокола.

После смены IP-адреса для интерфейса *ens33.50*, перезагрузки виртуальной машины, в выводе команды *ifconfig* выводится измененный IP-адрес (рисунок 29, 30).

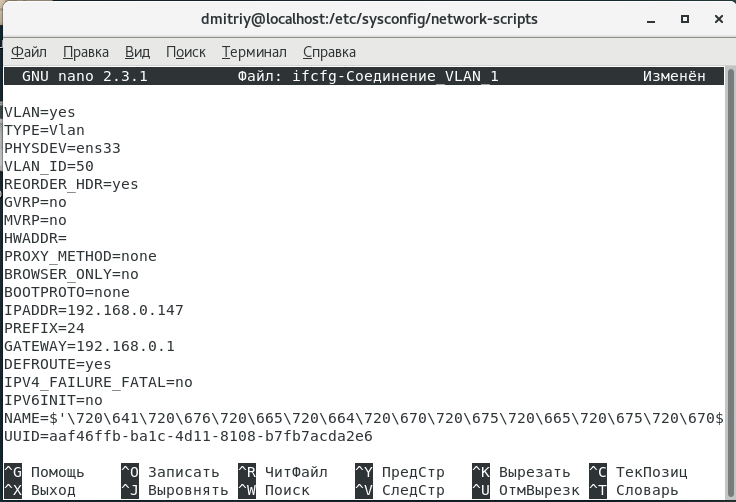


Рисунок 29. Изменение IP-адреса

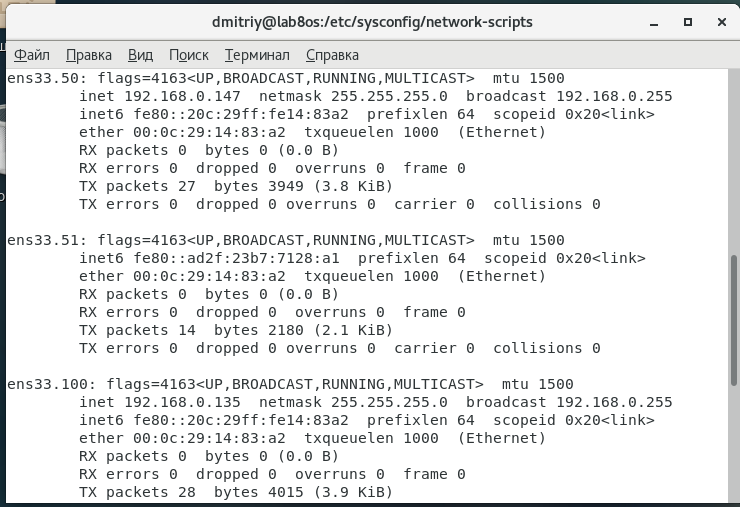


Рисунок 30. Измененный IP-адрес интерфейса *ens33.50*

После перезагрузки виртуальной машины сетевые интерфейсы находятся на месте. Разница между созданием интерфейса с помощью создания конфигурационного файла и с помощью утилиты TUI Network Manage состоит в том, что утилита использует интерактивный интерфейс и автоматическую генерацию конфигурационного файла.

# **Генерация ключей RSA для подключения по SSH**

Команда *ssh-keygen* позволяет сгенерировать пару ключей RSA для подключения по SSH с их помощью, без ввода пароля пользователя. При генерации можно указать парольную фразу. Процесс создания представлен на рисунке 31.

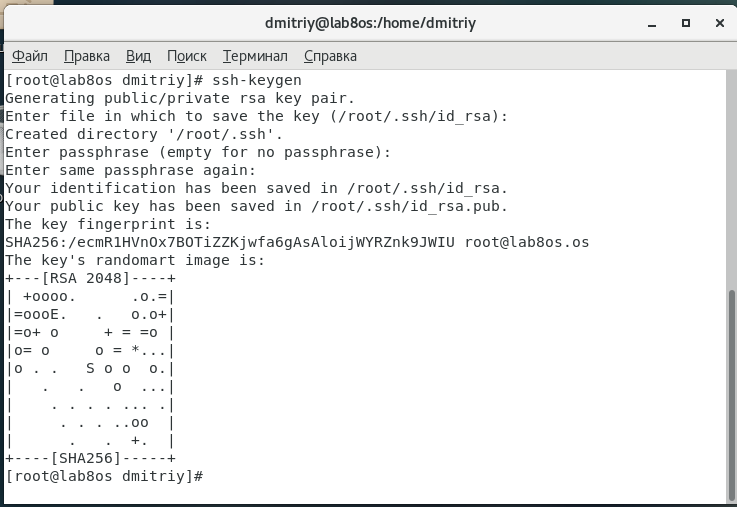


Рисунок 31. Создание пары ключей RSA

После генерации пара ключей сохраняется в домашней папке пользователя, в скрытом каталоге *.ssh*. Он содержит приватный и публичный ключ RSA (рисунок 32).

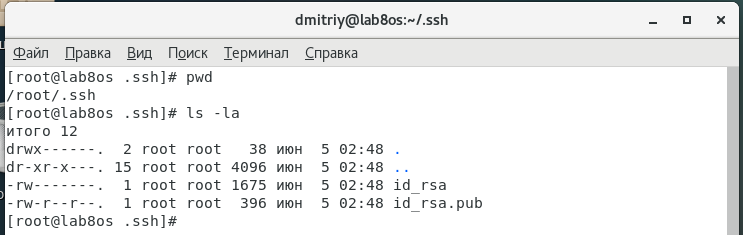


Рисунок 32. Содержимое директории *.ssh*

Перенести сгенерированный открытый ключ на сервер можно с помощью команды *ssh-copy-id <user>@<host>*. В данном случае команда будет выглядеть так: *ssh-copy-id* [*dmitriy2@192.168.0.121*](mailto:dmitriy2@192.168.0.121) (рисунок 33).

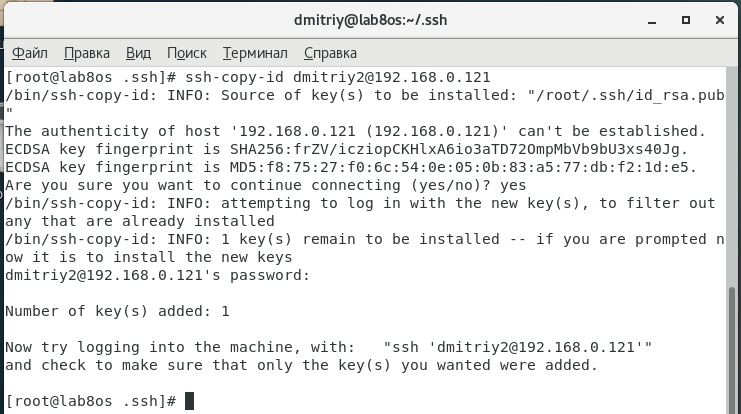


Рисунок 33. Копирование открытого ключа на сервер

После выполнения этой команды запрашивается пароль пользователя *dmitriy2* и перенос открытого ключа на сервер, в файл *.ssh/authorized\_keys* (рисунок 34).

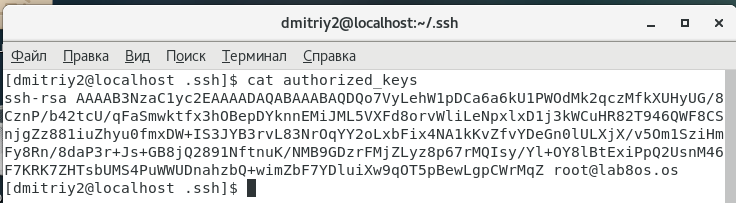


Рисунок 34. Содержимое файла *authorized\_keys* на сервере

Использование утилиты ssh-copy-id для копирования открытого ключа SSH на удаленный сервер является безопасным способом авторизации в системе без дальнейшей необходимости ввода пароля.

Это обеспечено шифрованием трафика, передаваемого по SSH и необходимостью ввода пароля пользователя перед копированием ключа.

# **Вывод:**

В ходе выполнения лабораторной работы поставленные цели были успешно выполнены. Были освоены и закреплены методы работы с сетевыми интерфейсами в ОС Linux. Изучены команды, конфигурационные файлы сетевых интерфейсов. Произведена работа по созданию и конфигурированию виртуальных сетевых интерфейсов. Была выполнена генерация ключей RSA для подключения по протоколу SSH. Закреплены навыки работы с ОС Linux, с оболочкой ее командной строки.