Отчёт по прохождению 2 раздела внешнего курса на stepik

Организация администрирования компьютерных сетей

Верниковская Екатерина Андреевна

Содержание

# 1 Цель работы

Ознакомиться с организацией администрирования компьютерных сетей.

# 2 Задание

Прочитать много информации и на основе полученного материала пройти тестовые задания и сделать практические работы.

# 3 Выполнение 2 раздела внешнего курса на stepik

## 3.1 Централизованная авторизация в сети

Задание №1: во время изучения темы никаких вопросов не возникло (рис. 1)

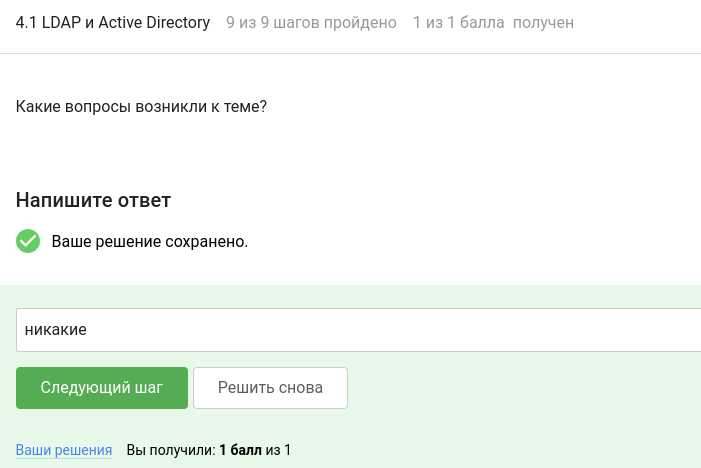


Рис. 1: Задание №1

Задание №2: на скрине всё видно (рис. 2)

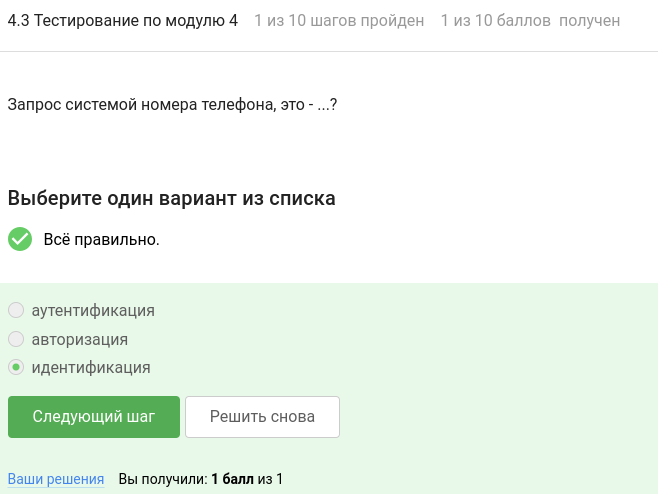


Рис. 2: Задание №2

Задание №3: на скрине всё видно (рис. 3)

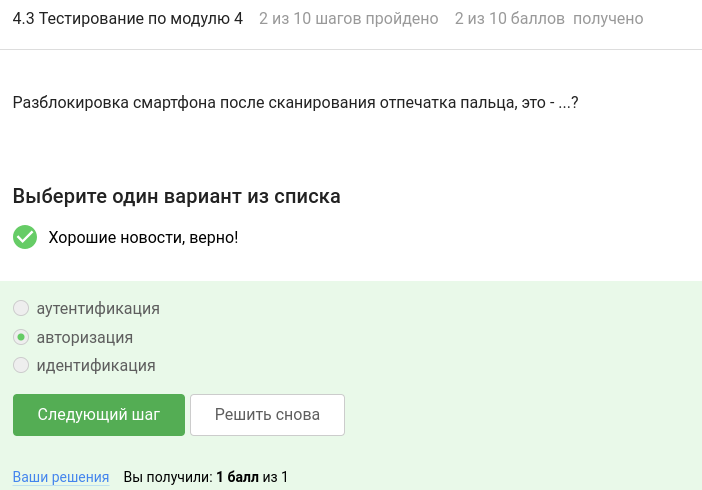


Рис. 3: Задание №3

Задание №4: прочитав информацию на странице “Сетевой каталог LDAP”, я отметила, что преимущества сетевых каталогов LDAP это *хорошая масштабируемость* и *быстрое чтение данных* (рис. 4)

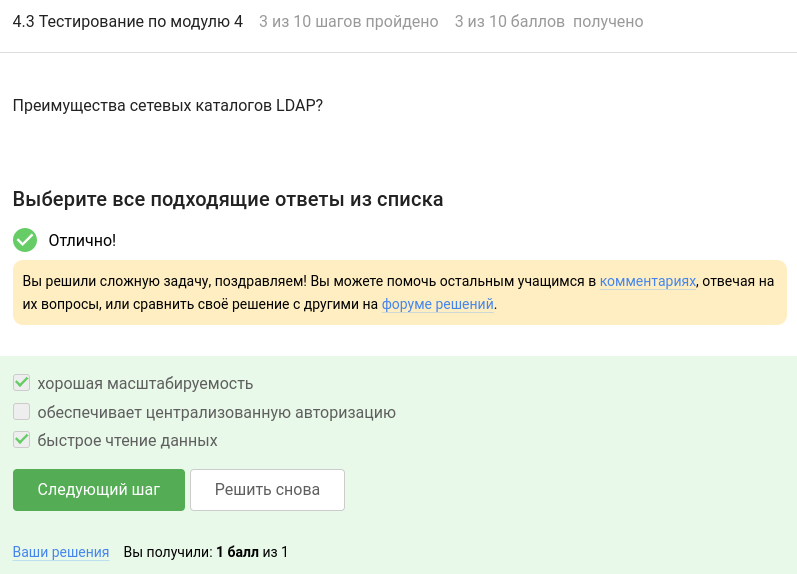


Рис. 4: Задание №4

Задание №5: прочитав информацию на странице “Сетевой каталог LDAP”, я отметила, что в сетевом каталоге LDAP хранятся такие типы объеутов, как *CN (Common Name)*, *UID (User ID)* и *OU (Organizational Unit)* (рис. 5)

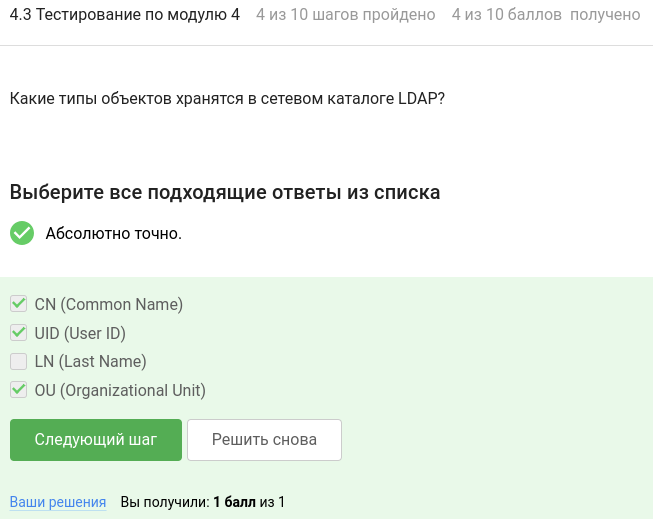


Рис. 5: Задание №5

Задание №6: прочитав информацию на странице “Сетевой каталог LDAP”, я отметила, что (DN, distinguished name) в каталоге LDAP означает полный путь к записи от корня (рис. 6)

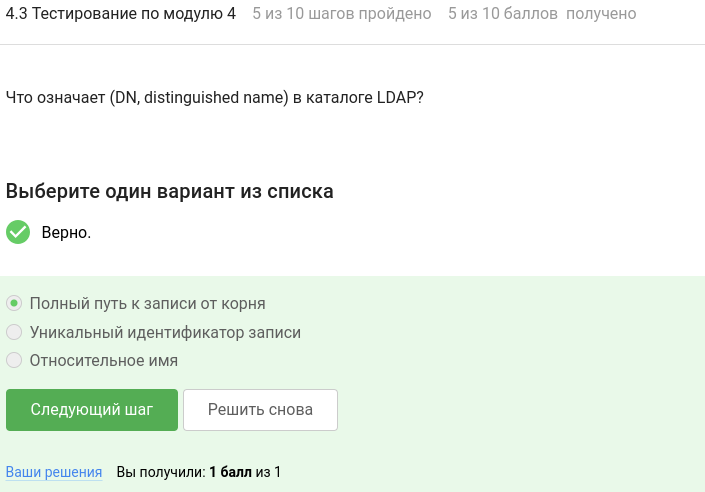


Рис. 6: Задание №6

Задание №7: на скрине всё видно (рис. 7)

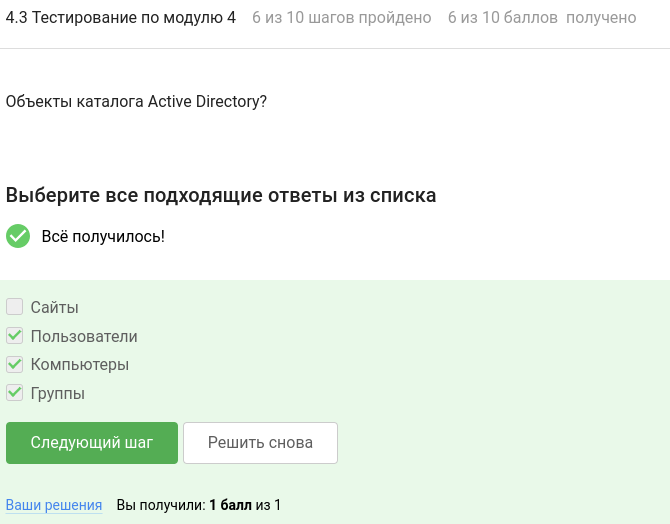


Рис. 7: Задание №7

Задание №8: прочитав информацию на странице “Логическая структура Active Directory”, я отметила, что логическая структура Active Directory состоит из таких компонентов как *Домен*, *Лес* и *Дерево* (рис. 8)

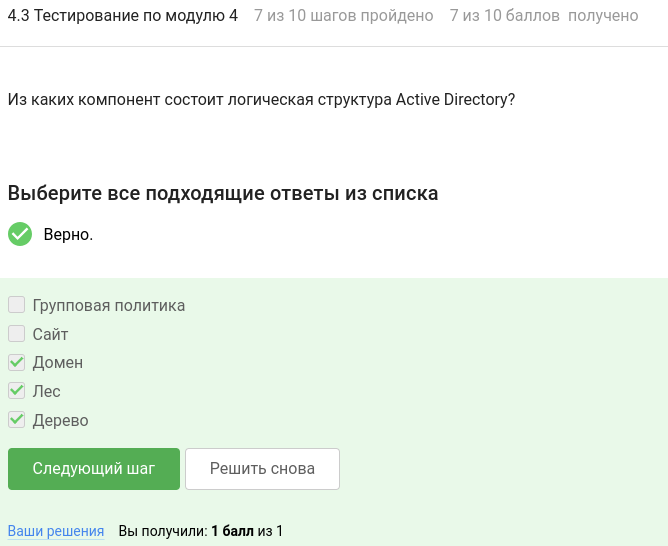


Рис. 8: Задание №8

Задание №9: прочитав информацию на странице “Групповые политики Group Policy”, я ответила на вопрос, о том, что позволяют настраивать групповые политики Active Directory (рис. 9)

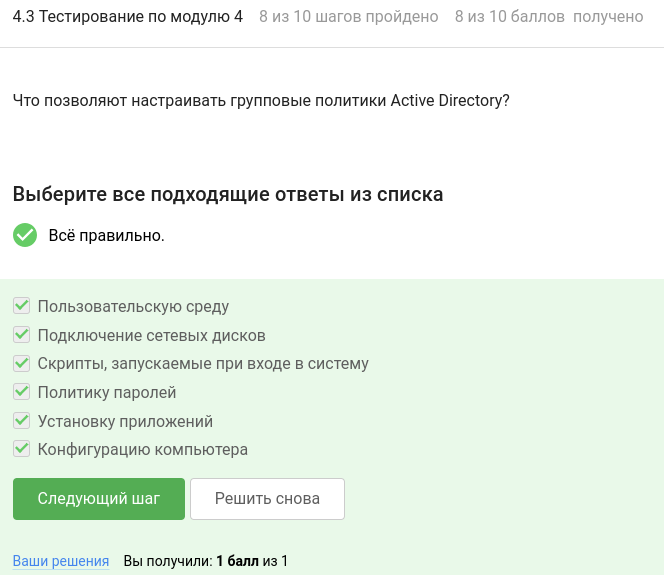


Рис. 9: Задание №9

Задание №10: прочитав информацию на странице “Сквозная авторизация Kerberos”, я ответила на вопрос (рис. 10)

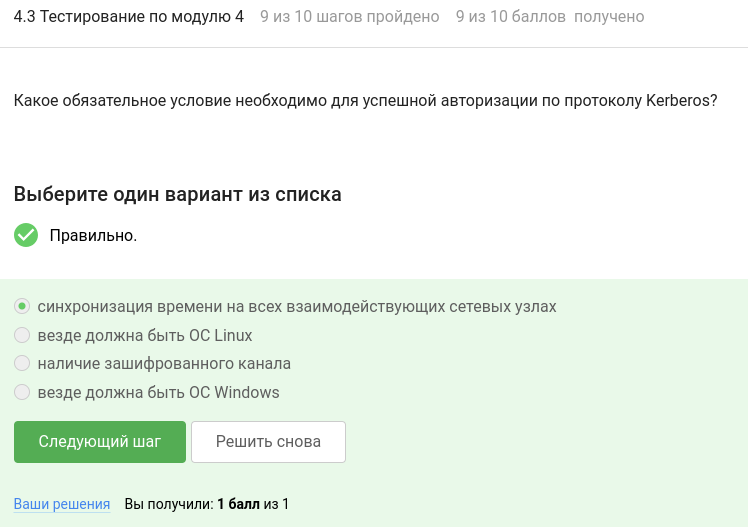


Рис. 10: Задание №10

Задание №11: прочитав информацию на странице “Сквозная авторизация. Принцип работы”, я ответила на вопрос (рис. 11)

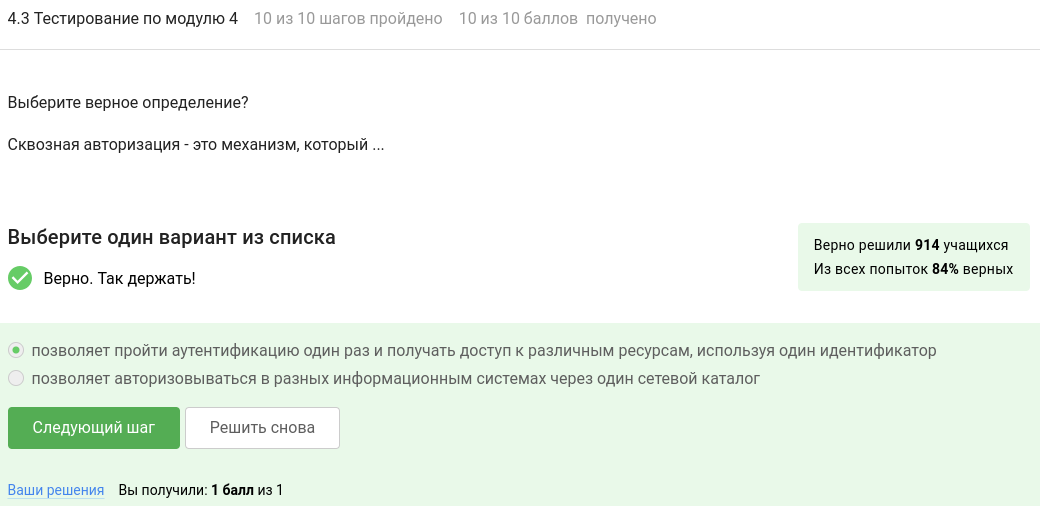


Рис. 11: Задание №11

Задание №12 (практическая работа): Необходимо настроить Windows-домен, создать орг.единицу, пользователей, групповую политику, внести в домен клиентский компьютер. Для этого надо скачать образ Windows 10 и Debian 12 (уже был импортирован в предыдущей практической работе) и импортировать в VirtualBox. Для входа в локальную систему VirtualBox используем учётные данные *username: root* и *password: P@ssw0rd*. После импорта сделать снапшот с именем Clean (рис. 12), (рис. 13), (рис. 14)

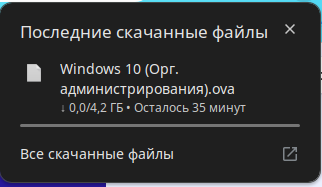


Рис. 12: Задание №12. Загрузка образа Windows 10

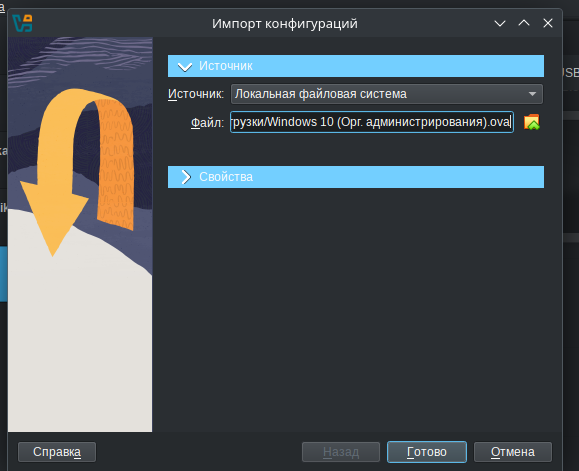


Рис. 13: Задание №12. Импорт образа Windows 10 в VirtualBox

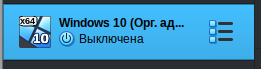


Рис. 14: Задание №12. Windows 10

Затем настраиваем сеть, создаём сеть OrgNat-10-0-2 с настройками: подсеть 10.0.2.0/24 и отключенный dhcp. В настройках сети импортированных ВМ установить сеть NAT: OrgNat-10-0-2. Это можно сделать, выполнив скрипт:

1. *vboxmanage natnetwork add –netname “OrgNat-10-0-2” –network 10.0.2.0/24 –enable –dhcp off –ipv6 off*
2. *vboxmanage modifyvm “Debian 12” –nic1 natnetwork –nat-network1 “OrgNat-10-0-2”*
3. *vboxmanage modifyvm “Windows 10 (Орг. администрирования)” –nic1 natnetwork –nat-network1 “OrgNat-10-0-2”*
4. *vboxmanage modifyvm “Debian 12” –nic2 none*
5. *vboxmanage modifyvm “Windows 10 (Орг. администрирования)” –nic2 none* (рис. 15)

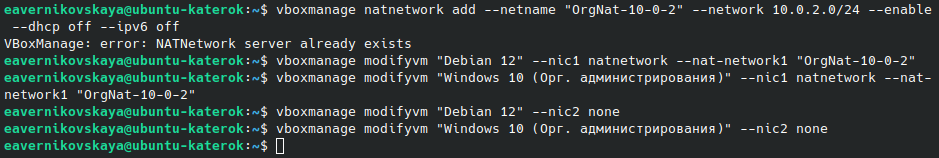


Рис. 15: Задание №12. Настройка сети

Далее устанваливаем статический IP-адрес в Debian. Для этого отключаем интерфейс командой *ifdown enp0s3* и редактируем файл /etc/network/interfaces (рис. 16), (рис. 17), (рис. 18)

Вместо “allow-hotplug enp0s3…” прописываем:

auto enp0s3  
iface enp0s3 inet static  
 address 10.0.2.3/24  
 gateway 10.0.2.1

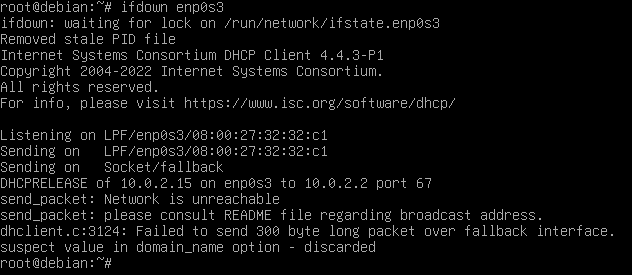


Рис. 16: Задание №12. Отключение интерфейса

Задание №12. Открытие файла /etc/network/interfaces

Рис. 17: Задание №12. Открытие файла /etc/network/interfaces

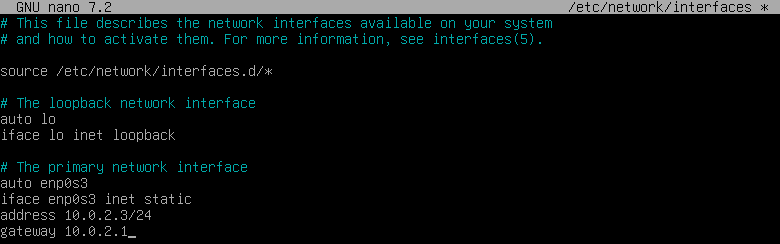


Рис. 18: Задание №12. Редактирование файла /etc/network/interfaces

Далее поднимаем интерфейс и настраиваем разрешение имён командами *ifup enp0s3* и *echo “nameserver 10.0.2.1” > /etc/resolv.conf* (рис. 19)

Задание №12. Поднятие интерфейса и настройка разрешения имён

Рис. 19: Задание №12. Поднятие интерфейса и настройка разрешения имён

Протестируем выход в интернет: *ping ya.ru* (рис. 20)

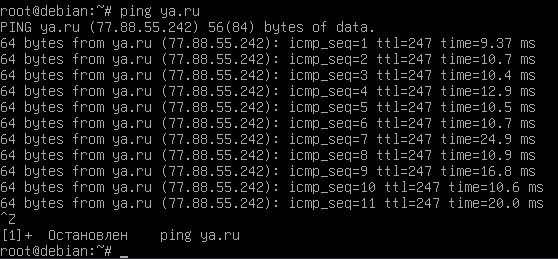


Рис. 20: Задание №12. Тестирование входа в интернет

После устанавлваем имя сервера Debian командами *echo dc1.example.com > /etc/hostname*, *hostname dc1.example.com* и *echo “10.0.2.3 dc1 dc1.example.com” >> /etc/hosts* (рис. 21)

Задание №12. Установка имени сервера Debian

Рис. 21: Задание №12. Установка имени сервера Debian

После обновляем систему и устанавливаем необходимые пакеты (рис. 22), (рис. 23)

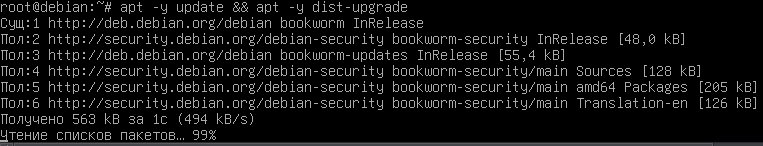


Рис. 22: Задание №12. Обновление системы

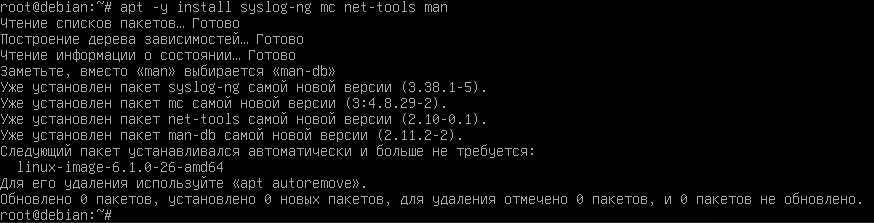


Рис. 23: Задание №12. Установка необходимых пакетов

Далее устанавливаем пакет samba4 для контроллера домена в Debian: *apt -y install samba winbind krb5-config krb5-user bind9-dnsutils bind9 isc-dhcp-server*. При установке на вопрос об области по умолчанию для kerberos просто нажимаем ENTER (рис. 24)

Задание №12. Установка пакета samba4

Рис. 24: Задание №12. Установка пакета samba4

Потом останавливаем службы samba4 командами:

1. *systemctl stop smbd*
2. *systemctl disable smbd*
3. *systemctl stop nmbd*
4. *systemctl disable nmbd*
5. *systemctl stop winbind*
6. *systemctl disable winbind* (рис. 25)

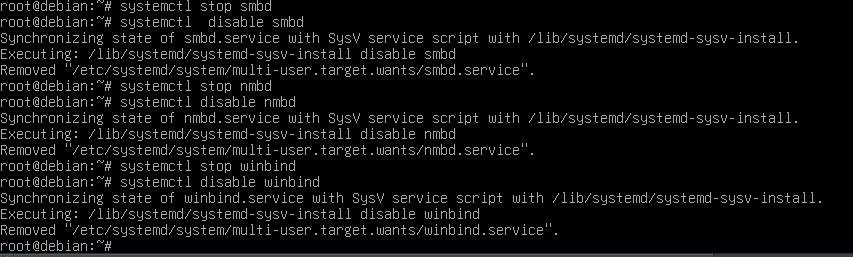


Рис. 25: Задание №12. Остановка служб samba4

Далее переименовываем конфигурацию samba4 командой *mv /etc/samba/smb.conf /etc/samba/smb.conf.zap* и разворачиваем домен командой *samba-tool domain provision –use-rfc2307 –dns-backend=BIND9\_DLZ –realm=EXAMPLE.COM –domain=EXAMPLE –adminpass=P@ssw0rd* (рис. 26)

Задание №12. Разворачиваем домен

Рис. 26: Задание №12. Разворачиваем домен

Следующим шагом надо настроить DNS в Debian. Для этого сначала в файл /etc/bind/named.conf добавляем строчку *include “/var/lib/samba/bind-dns/named.conf”;* (рис. 27), (рис. 28)

Задание №12. Открытие файла /etc/bind/named.conf

Рис. 27: Задание №12. Открытие файла /etc/bind/named.conf

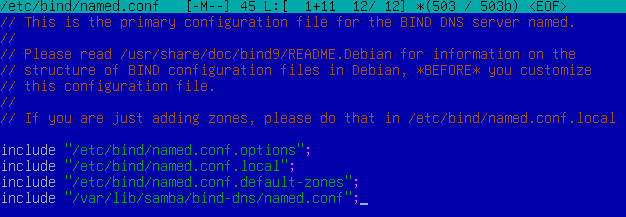


Рис. 28: Задание №12. Редактирование файла /etc/bind/named.conf

Далее редактируем файл /etc/bind/named.conf.options, добавив в секцию options *tkey-gssapi-keytab “/var/lib/samba/bind-dns/dns.keytab”;* (рис. 29), (рис. 30)

Задание №12. Открытие файла /etc/bind/named.conf.options

Рис. 29: Задание №12. Открытие файла /etc/bind/named.conf.options

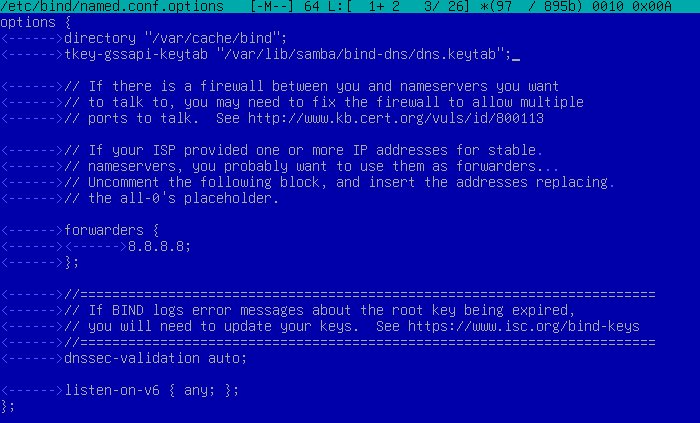


Рис. 30: Задание №12. Редактирование файла /etc/bind/named.conf.options

Далее перезапускаем и проверяем сервис bind9 (рис. 31)

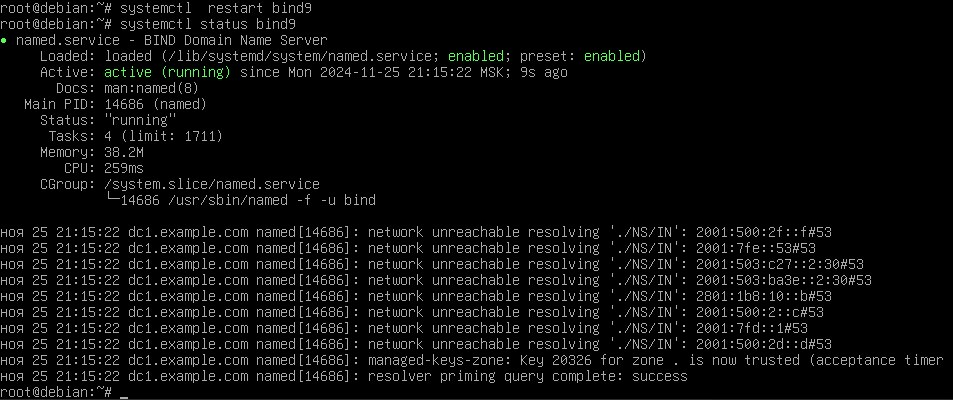


Рис. 31: Задание №12. Перезапуск и проверка сервиса bind9

После настраиваем DHCP в Debian. Для этого сначала в файле /etc/default/isc-dhcp-server прописываем *INTERFACESv4=“enp0s3”* (рис. 32), (рис. 33)

Задание №12. Открытие файла /etc/default/isc-dhcp-server

Рис. 32: Задание №12. Открытие файла /etc/default/isc-dhcp-server

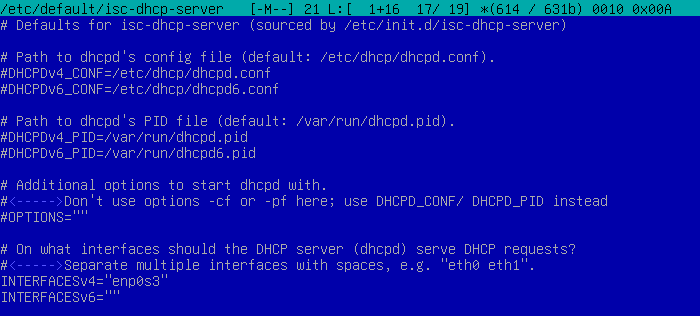


Рис. 33: Задание №12. Редактирование файла /etc/default/isc-dhcp-server

После в файл /etc/dhcp/dhcpd.conf добавляем следующие настройки:

subnet 10.0.2.0 netmask 255.255.255.0 {  
 range 10.0.2.100 10.0.2.150;  
 option routers 10.0.2.1;  
 option domain-name "example.com";  
 option domain-name-servers 10.0.2.3;  
}

(рис. 34), (рис. 35)

Задание №12. Открытие файла /etc/dhcp/dhcpd.conf

Рис. 34: Задание №12. Открытие файла /etc/dhcp/dhcpd.conf

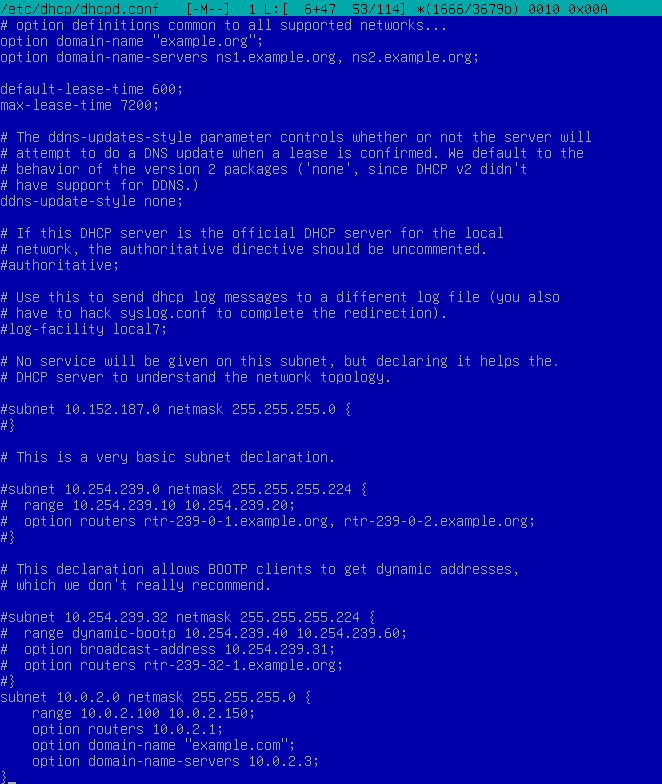


Рис. 35: Задание №12. Редактирование файла /etc/dhcp/dhcpd.conf

Перезапускаем и проверяем сервис DHCP (рис. 36)



Рис. 36: Задание №12. Перезапуск и проверка сервиса DHCP

Запускаем контроллер домена на Debian. Для этого сначала устанавливаем разрешение имён на локальный сервер (рис. 37)

Задание №12. Установка разрешения имён на локальный сервер

Рис. 37: Задание №12. Установка разрешения имён на локальный сервер

После запускаем и проверяем сервис домена (рис. 38), (рис. 39)

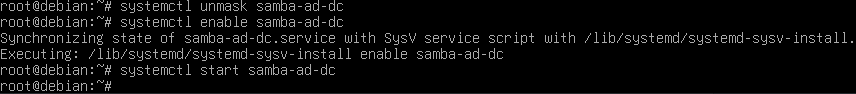


Рис. 38: Задание №12. Запуск сервиса домена

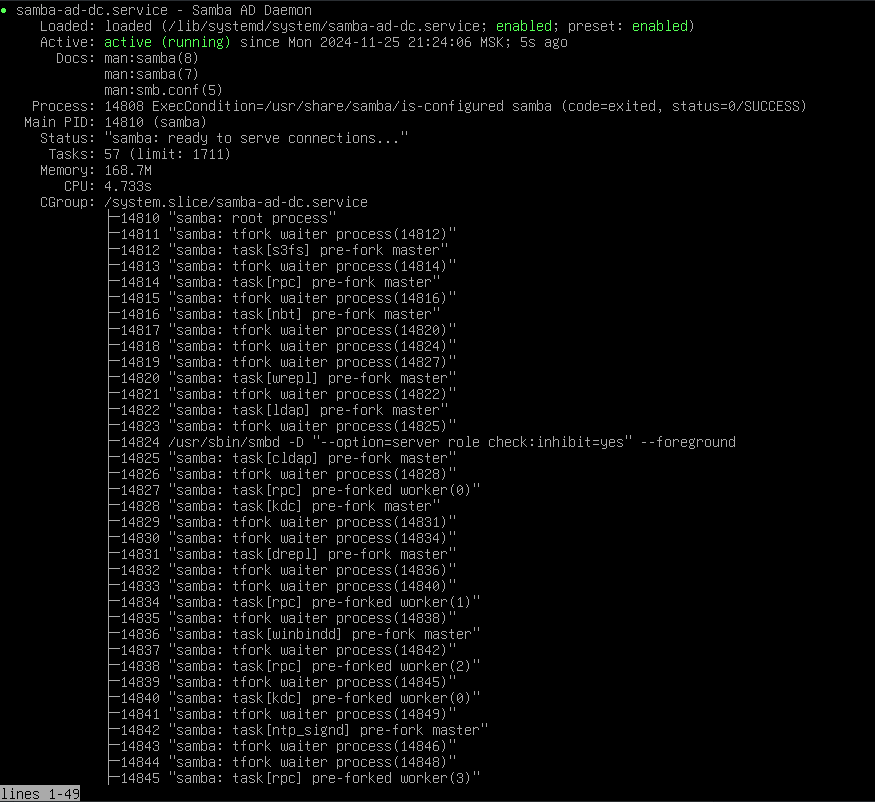


Рис. 39: Задание №12. Проверка сервиса домена

Далее настраиваем локальную сквозную авторизацию Kerberos командами *mv /etc/krb5.conf /etc/krb5.conf.zap* и *cp /var/lib/samba/private/krb5.conf /etc/krb5.conf* (рис. 40)

Задание №12. Настройка локальной сквозной авторизации Kerberos

Рис. 40: Задание №12. Настройка локальной сквозной авторизации Kerberos

Проверим сквозную авторизацию. Для этого набираем команду *kinit Administrator* и пароль администратора P@ssw0rd (рис. 41)

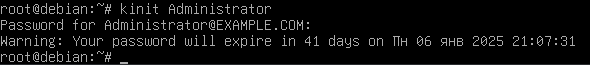


Рис. 41: Задание №12. Проверка сквозной авторизации

Команда *klist* должна выводить информацию о полученном билете Kerberos (рис. 42)

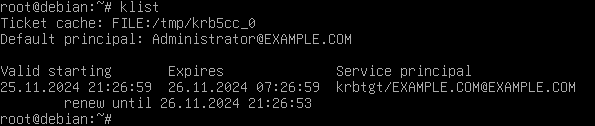


Рис. 42: Задание №12. Вывод команды klist

Отредактируем DNS в Debian (рис. 43)



Рис. 43: Задание №12. Редактирование DNS в Debian

Далее добавим организации, группы и пользователей в контроллер домена Debian командами:

1. *samba-tool ou create “ou=ZTI,dc=example,dc=com”*
2. *samba-tool group add Group1 –groupou=ou=ZTI*
3. *samba-tool group add Group2 –groupou=ou=ZTI*
4. *samba-tool user create –userou=ou=ZTI student1 P@ssw0rd1*
5. *samba-tool user create –userou=ou=ZTI student2 P@ssw0rd2*
6. *samba-tool user create –userou=ou=ZTI student3 P@ssw0rd3*
7. *samba-tool group addmembers Group1 student1,student2*
8. *samba-tool group addmembers Group2 student3* (рис. 44)

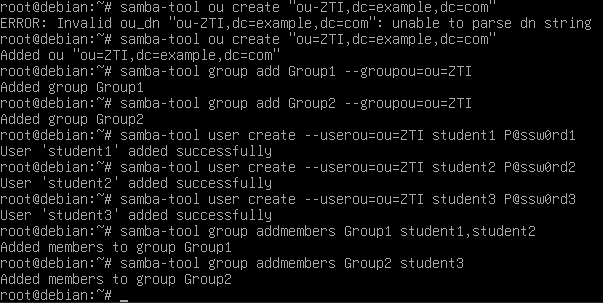


Рис. 44: Задание №12. Добавление организации, групп и пользователей в контроллер домена Debian

Далее создадим групповую политику в Debian командой *samba-tool gpo create ZTI -U Administrator –password=P@ssw0rd* (рис. 45)

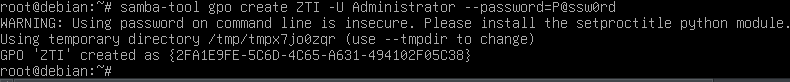


Рис. 45: Задание №12. Создание групповой политики в Debian

Подключаем групповую политику к ZTI по ранее созданному идентификатору (из вывода предыдущей команды): *samba-tool gpo setlink ou=ZTI,dc=example,dc=com -U Administrator –password=P@ssw0rd {идентификатор из предыдущей команды}* (рис. 46)

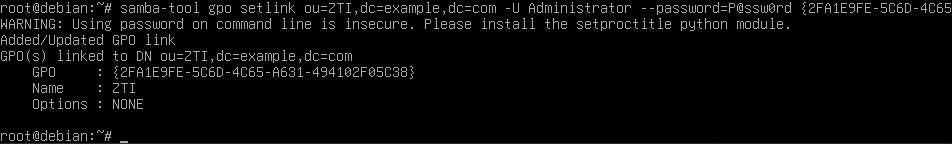


Рис. 46: Задание №12. Подключение групповой политики к ZTI

Протестируем созданную политику в списке групповых политик командами:

1. *samba-tool gpo list student1* (рис. 47)
2. *samba-tool gpo listall* (рис. 48)

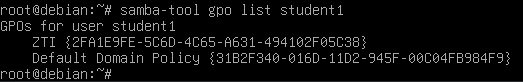


Рис. 47: Задание №12. Тестирование созданной политики (1)

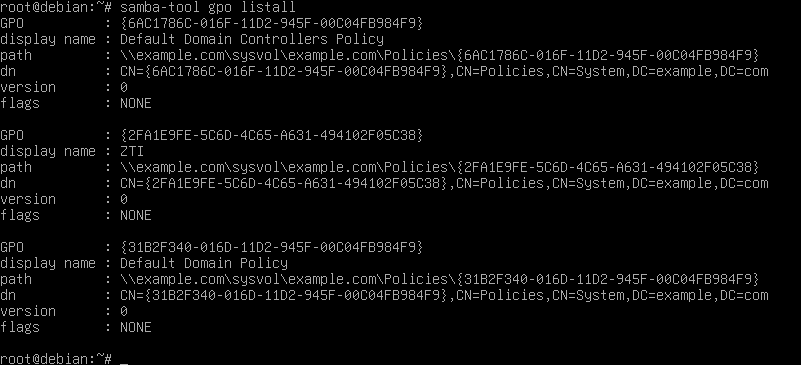


Рис. 48: Задание №12. Тестирование созданной политики (2)

Далее работаем на Windows 10. Сначала перименовываем ПК в *K29* и перезагружаем (рис. 49)

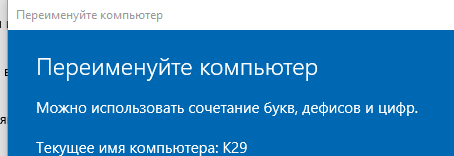


Рис. 49: Задание №12. Переименовывание ПК

Проверяем получение IP-адреса (Пуск, cmd, ipconfig) по DHCP с контроллера домена (адрес должен быть 10.0.2….) (рис. 50)

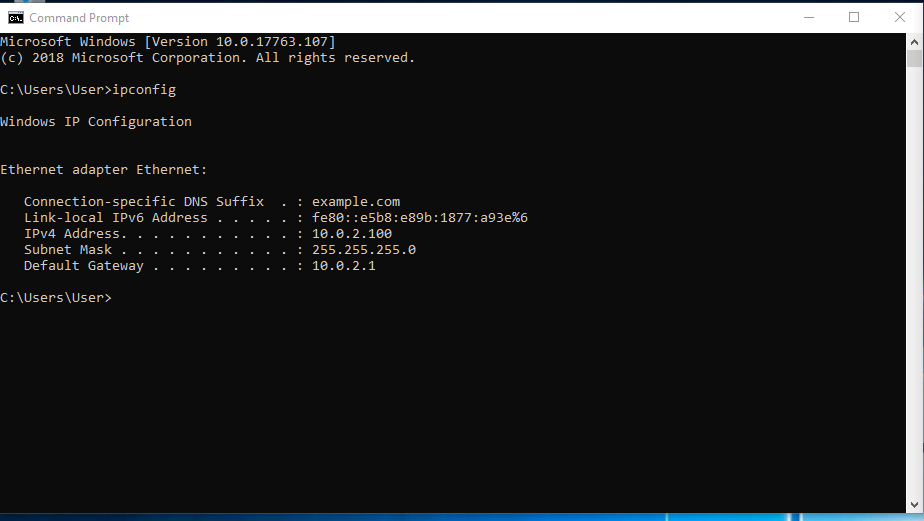


Рис. 50: Задание №12. Проверка получения IP-адреса

Далее Центр управления сетями и общим доступом, Подключение по локальной сети (рис. 51)

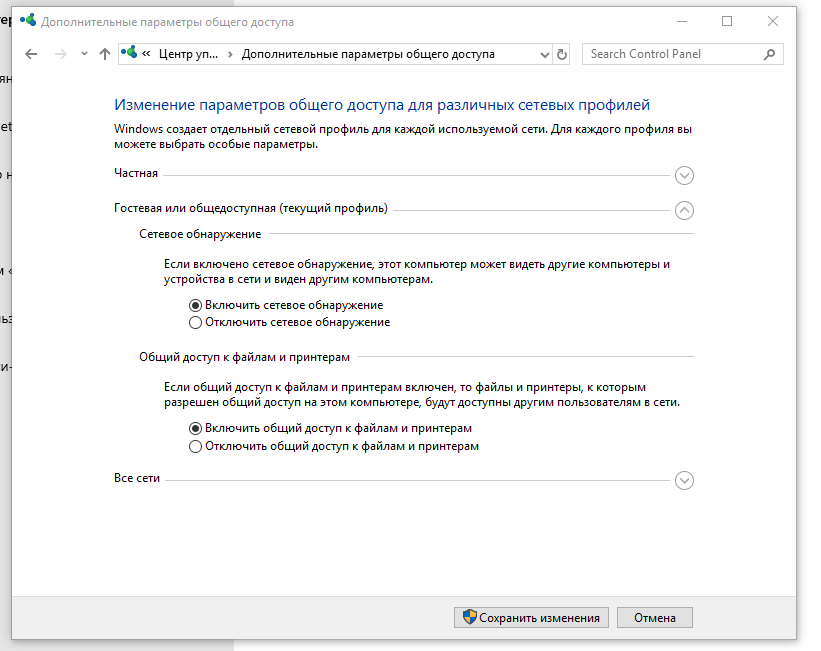


Рис. 51: Задание №12. Подключение по локальной сети

Далее вводим компьютер в домен *example.com* (рис. 52), (рис. 53), (рис. 54)

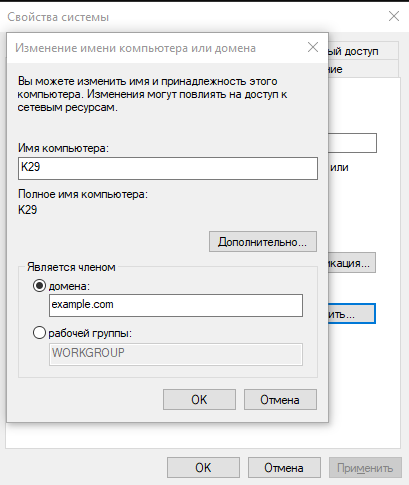


Рис. 52: Задание №12. Ввод компьютера в домен example.com (1)

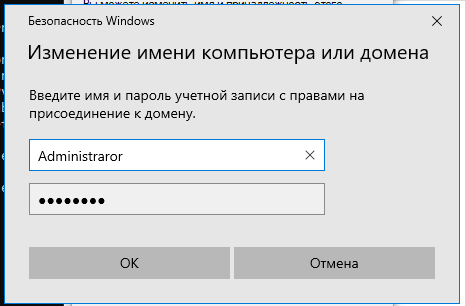


Рис. 53: Задание №12. Ввод компьютера в домен example.com (2)

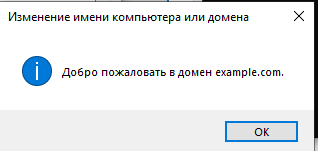


Рис. 54: Задание №12. Ввод компьютера в домен example.com (3)

После устанавливаем RSAT и редактируем GPO из Windows 10. Сначала входим в Windows 10 с учётными данными Administrator@example и паролем P@ssw0rd (рис. 55)

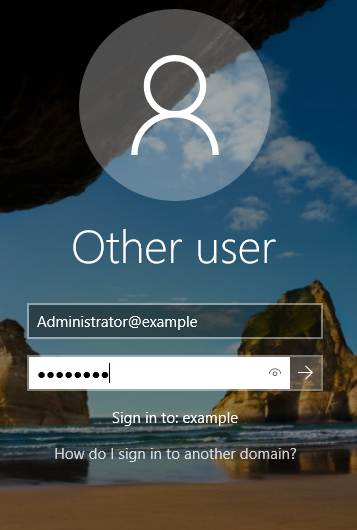


Рис. 55: Задание №12. Вход в Windows 10 с учётными данными Administrator@example

Для поиска команды установки RSAT запускаем браузер Internet Explorer, открываем сайт samba.org, забиваем в поиске RSAT и нажимаем на первую ссылку из поиска, в тексте находим указанную ниже строку установки и копируем её в командную строку:

*Выполнить, cmd (по правой кнопке мыши - от Администратора), dism /online /add-capability /CapabilityName:Rsat.GroupPolicy.Management.Tools~~~~0.0.1.0 /CapabilityName:Rsat.Dns.Tools0.0.1.0 /CapabilityName:Rsat.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0* (рис. 56)

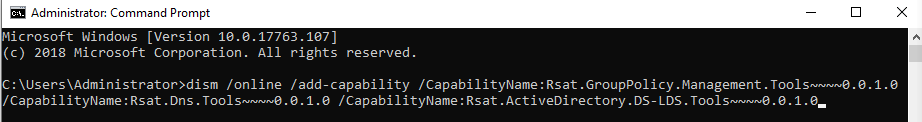


Рис. 56: Задание №12. Установка RSAT

После установки в меню появляются средства управления доменом, запускаем Group Policy, подключаемся к серверу dc1, находим в домене example.com организационную единицу ZTI и открываем групповую политику ZTI на редактирование (рис. 57)

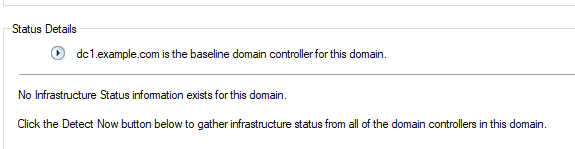


Рис. 57: Задание №12. Подключение к серверу dc1

Далее в редакторе групповой политики переходим в User Configuration, Policies, Administrative Templates, Windows Components, Internet Explorer. Там устанавливаем начальную страницу. Для этого отредактируем Disable changing home page settings, установим Enabled и http://yandex.ru (рис. 58)

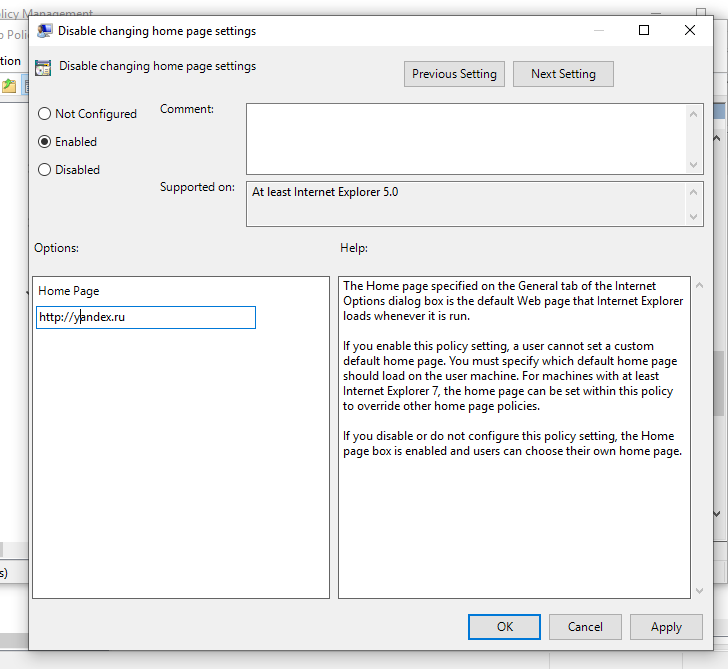


Рис. 58: Задание №12. Редактирование Disable changing home page settings

Также уберём надоедливый мастер настройки. Для этого отредактируем Prevent running First Run wizard, установим Enabled и Start page (рис. 59)

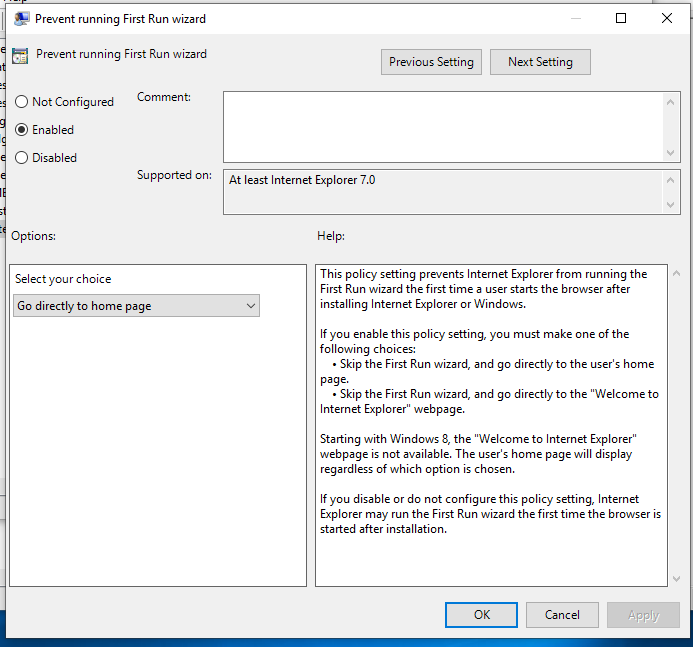


Рис. 59: Задание №12. Редактирование Prevent running First Run wizard

Далее выполним саму практическую работу. Для этого сначала зайдём в учётную запись student1 (рис. 60)

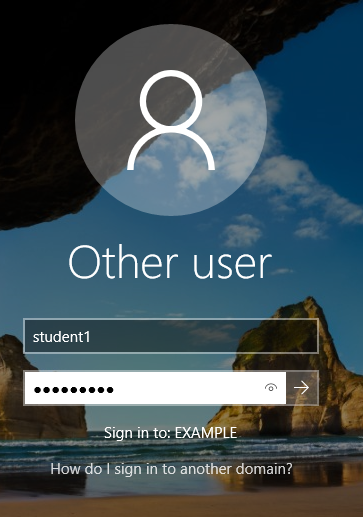


Рис. 60: Задание №12. Вход в Windows 10 с учётными данными student1

Далее нужно выполнить следующие команды:

1. *ipconfig /all* (рис. 61)
2. *gpresult /r* (рис. 62)

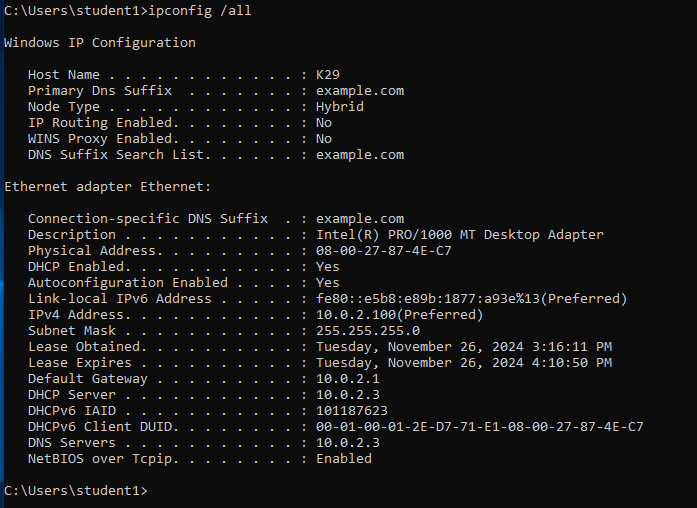


Рис. 61: Задание №12. ipconfig /all

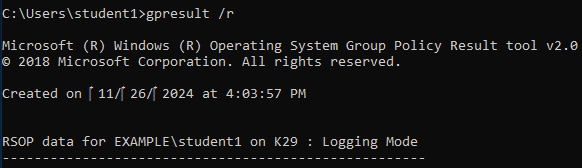


Рис. 62: Задание №12. gpresult /r

Также предоставляем результат запуска браузера (рис. 63)

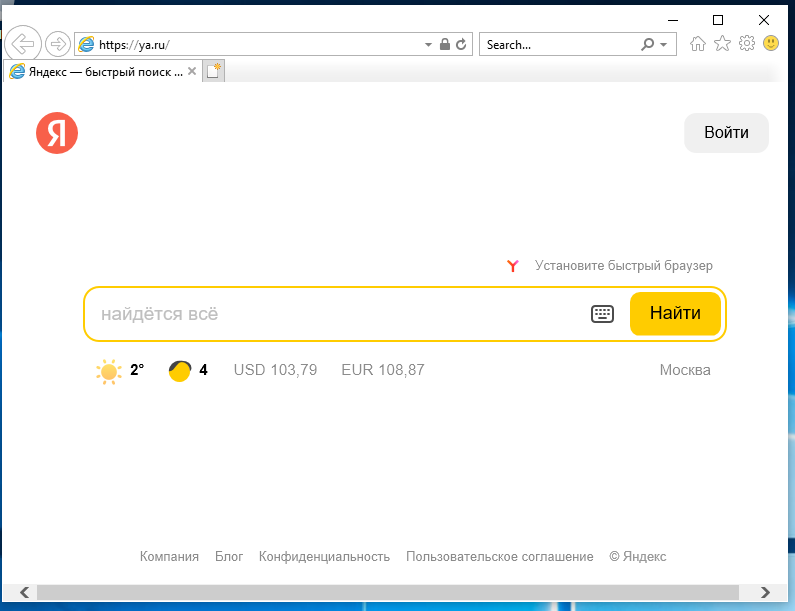


Рис. 63: Задание №12. Запуск браузера

На Debian выполняем следующие команды:

1. *samba-tool computer list* (рис. 64)
2. *dhcp-lease-list* (рис. 65)
3. *samba-tool gpo list student1* (рис. 66)

(рис. 67)

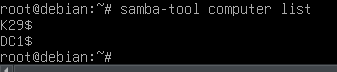


Рис. 64: Задание №12. samba-tool computer list

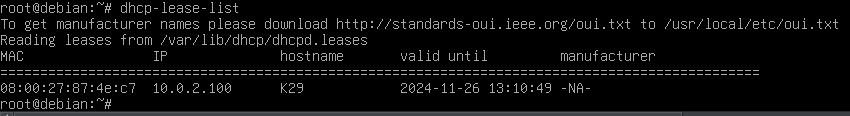


Рис. 65: Задание №12. dhcp-lease-list

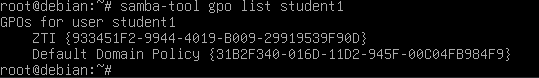


Рис. 66: Задание №12. samba-tool gpo list student1

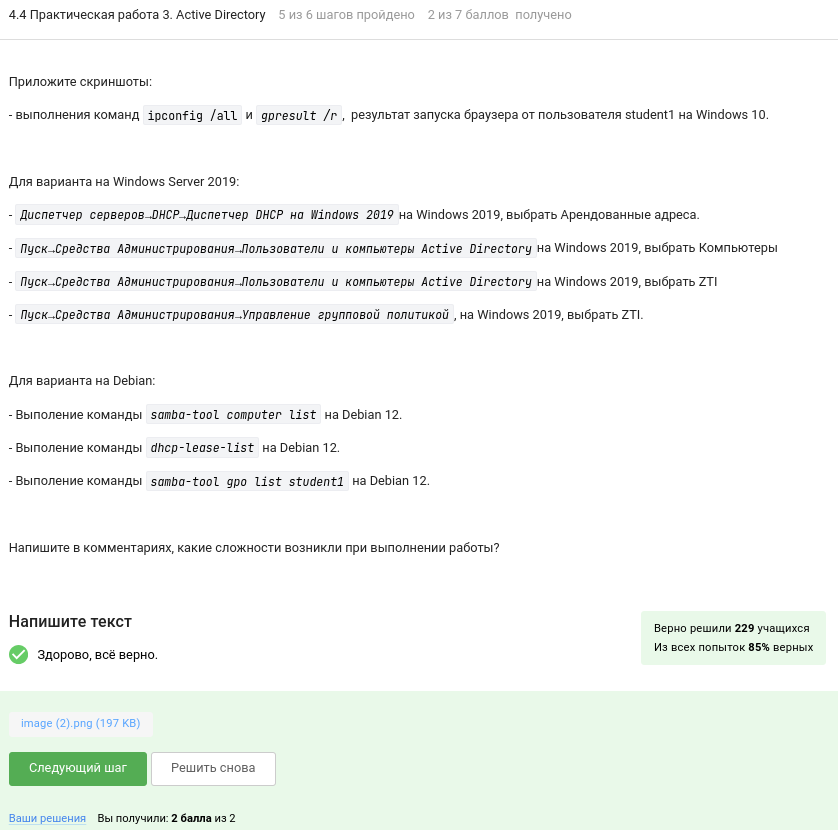


Рис. 67: Задание №12

## 3.2 Маршрутизаця в локальных сетях

Задание №13: прочитав информацию на странице “Виды маршрутизации”, я отметила, что вид маршрутизации, при котором маршруты указываются вручную называется *статической маршрутизацией* (рис. 68)

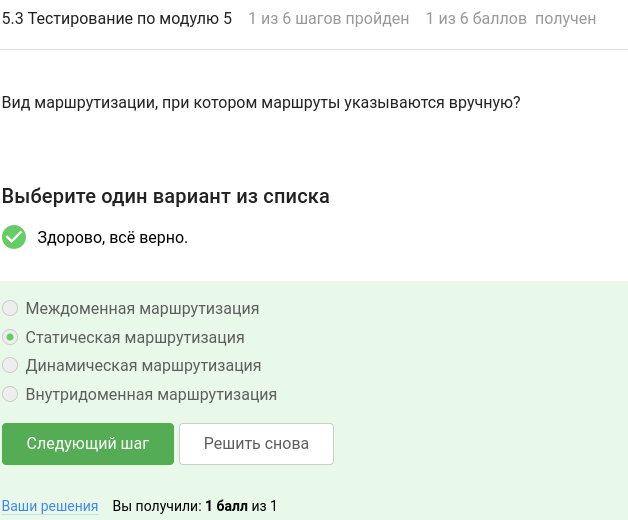


Рис. 68: Задание №13

Задание №14: прочитав информацию на странице “Виды маршрутизации”, я отметила, что к протоколам динамической маршрутизации относятся *RIP*, *OSPF* и *EIGRP* (рис. 69)

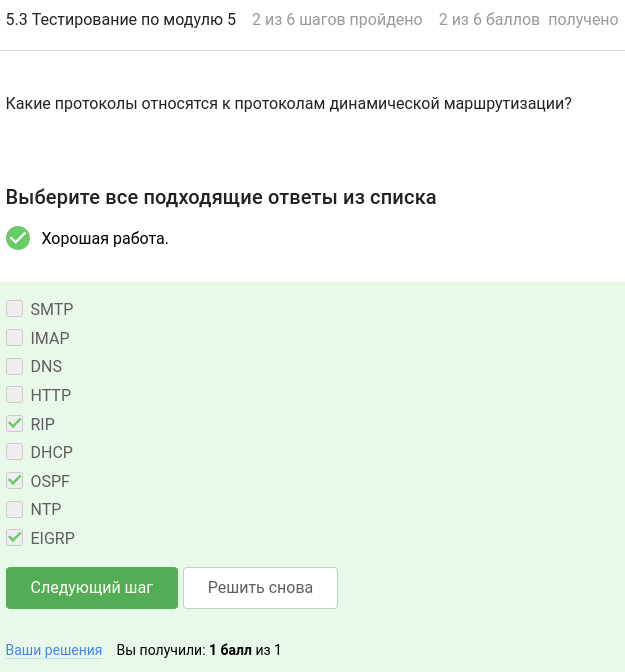


Рис. 69: Задание №14

Задание №15: прочитав информацию на странице “Протоколы динамической маршрутизации”, я выполнила задание (рис. 70)

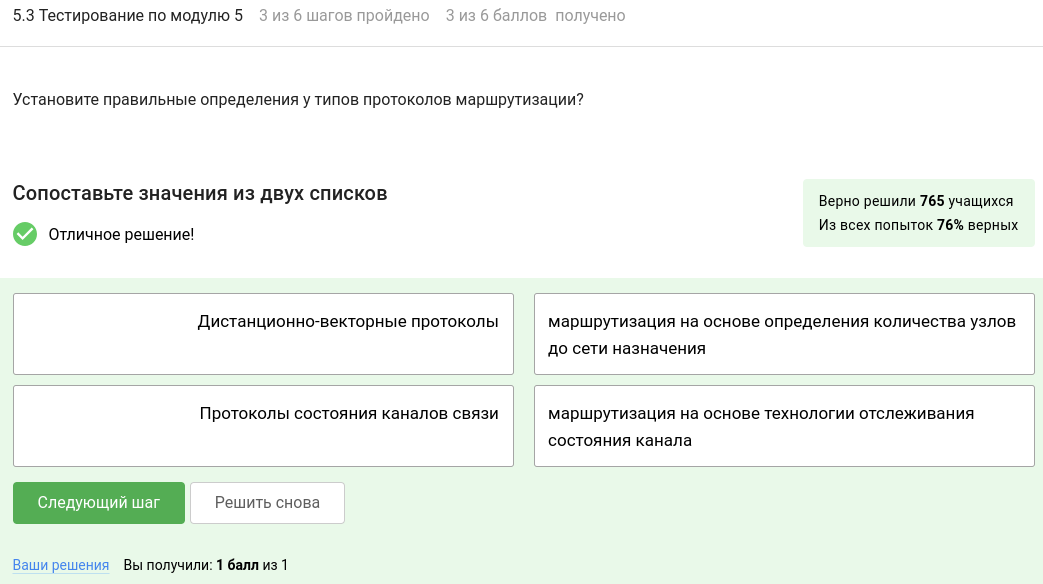


Рис. 70: Задание №15

Задание №16: прочитав информацию на странице “Протоколы динамической маршрутизации”, я выполнила задание (рис. 71)

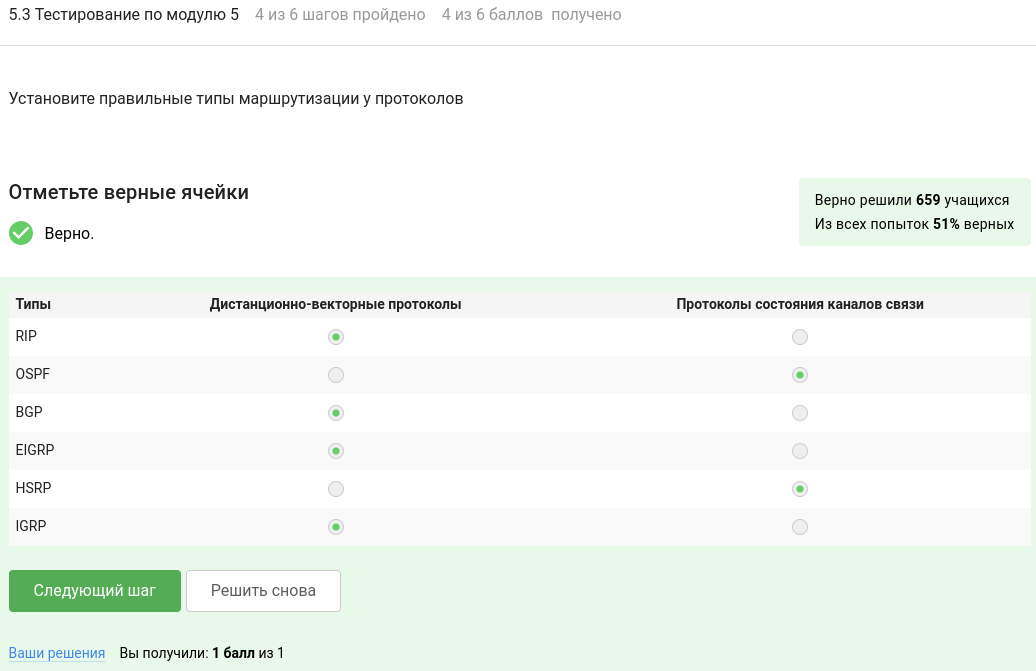


Рис. 71: Задание №16

Задание №17: прочитав информацию на странице “Таблица маршрутизации RIP”, я отметила, что в таблице маршрутизации присутствуют такие параметры, как *адрес ближайшего маршрутизатора*, *метрика маршрута* и *адрес назначения* (рис. 72)

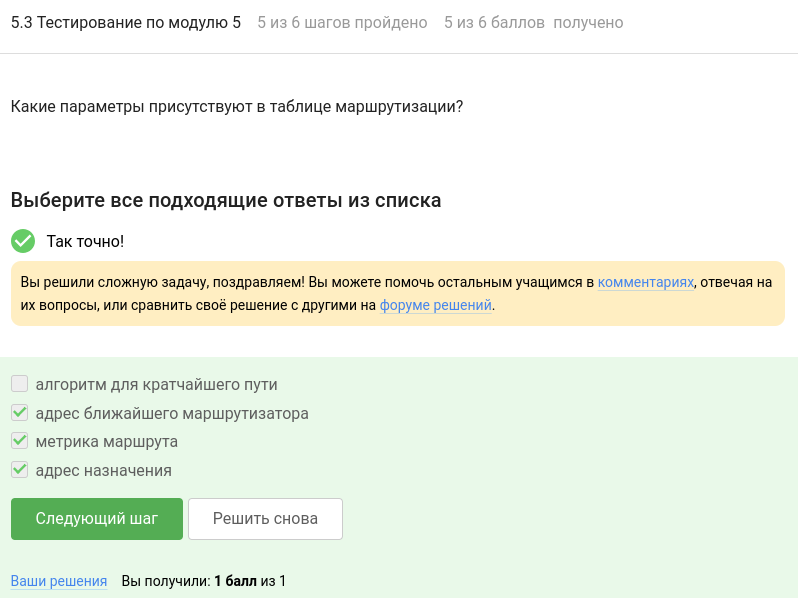


Рис. 72: Задание №17

Задание №18: на скрине всё видно (рис. 73)

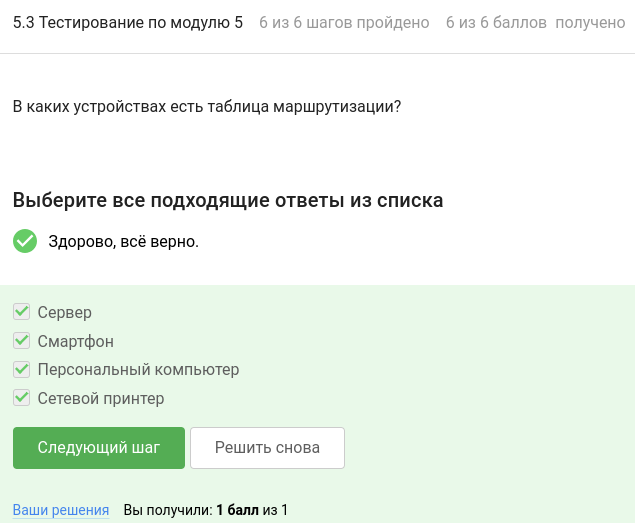


Рис. 73: Задание №18

Задание №19 (практическая работа): Необходимо сбросить состояние в исходное, создать сервер “GW” (копия “Debian 12”), настроить сетевые соединения между виртуальными машинами, для этого выполняем команды:

1. *vboxmanage snapshot “Windows 10 (Орг. администрирования)” restore Clean*
2. *vboxmanage snapshot “Debian 12” restore Clean*
3. *vboxmanage clonevm “Debian 12” –name “GW” –register*
4. *vboxmanage snapshot “GW” take Clean*
5. *vboxmanage natnetwork add –netname OrgNat-192-168-1 –network 192.168.1.0/24 –enable –dhcp off –ipv6 off*
6. *vboxmanage natnetwork add –netname OrgNat-10-0-1 –network 10.0.1.0/24 –enable –dhcp off –ipv6 off*
7. *vboxmanage natnetwork add –netname OrgNat-172-16-1 –network 172.16.1.0/24 –enable –dhcp off –ipv6 off*
8. *vboxmanage modifyvm “Debian 12” –nic1 natnetwork –nat-network1 OrgNat-192-168-1*
9. *vboxmanage modifyvm “Debian 12” –nic2 none*
10. *vboxmanage modifyvm “GW” –nic1 natnetwork –nat-network1 OrgNat-192-168-1*
11. *vboxmanage modifyvm “GW” –nic2 natnetwork –nat-network2 OrgNat-10-0-1*
12. *vboxmanage modifyvm “Windows 10 (Орг. администрирования)” –nic1 natnetwork –nat-network1 OrgNat-172-16-1*
13. *vboxmanage modifyvm “Windows 10 (Орг. администрирования)” –nic2 none* (рис. 74)

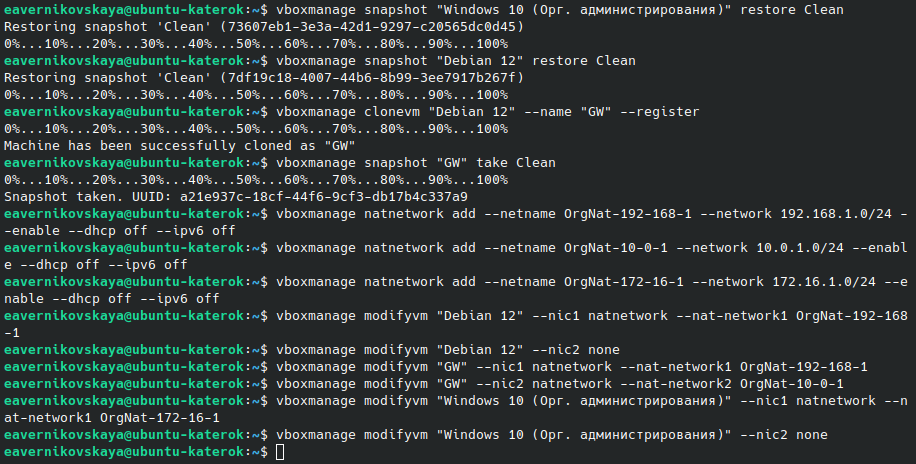


Рис. 74: Задание №19. Настройка сети

Работаем на виртуальной машине «GW». Посмотреть, какие у нас есть сетевые интерфейсы: *ip a*. Должно быть два интерфейса (enp0s3 и enp0s8) (рис. 75)



Рис. 75: Задание №19. Проверка сетевых интерфейсов (1)

Настроим на сетевых интерфейсах IP-адреса. Для этого добавим в файл /etc/network/interfaces настройку сетевых интерфейсов enp0s3 enp0s8:

auto enp0s3 enp0s8  
iface enp0s3 inet static  
address 192.168.1.254/24  
gateway 192.168.1.1  
iface enp0s8 inet static  
address 10.0.1.100/8

(рис. 76), (рис. 77)

Задание №19. Открытие файла /etc/network/interfaces в GW

Рис. 76: Задание №19. Открытие файла /etc/network/interfaces в GW

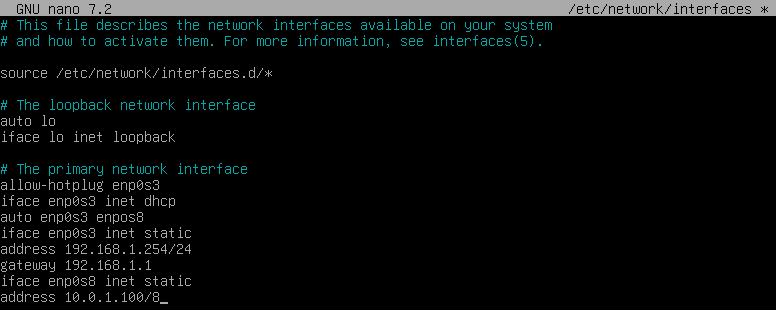


Рис. 77: Задание №19. Редактирование файла /etc/network/interfaces в GW

Далее включим сетевые интерфейсы командами *ifdown enp0s3*, *ifup enp0s3* и *ifup enp0s8* (рис. 78)

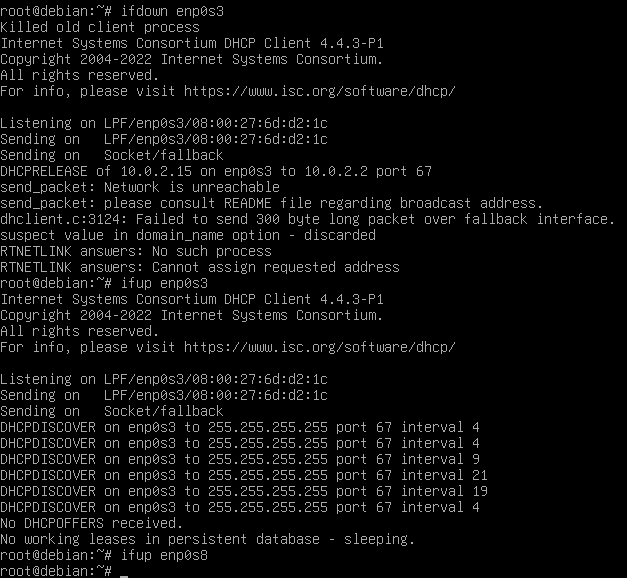


Рис. 78: Задание №19. Включение сетевых интерфейсов

Проверим успешную настройку: *ip a* (рис. 79)

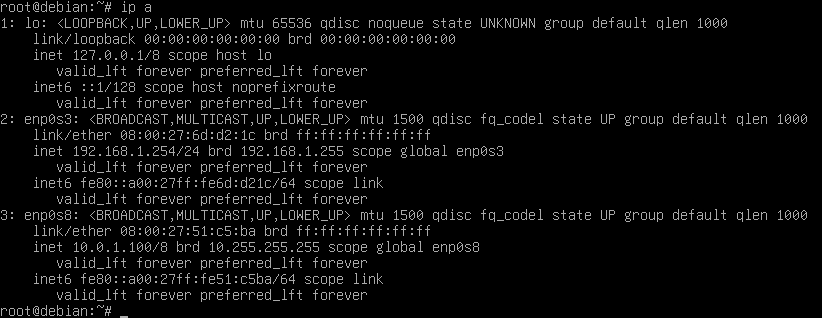


Рис. 79: Задание №19. Проверка успешной настройки в GW

Настроим разрешение имён DNS. В файле /etc/resolv.conf должна быть строчка *nameserver 192.168.1.1* (рис. 80), (рис. 81)

Задание №19. Открытие файла /etc/resolv.conf

Рис. 80: Задание №19. Открытие файла /etc/resolv.conf

Задание №19. Редактирование файла /etc/resolv.conf

Рис. 81: Задание №19. Редактирование файла /etc/resolv.conf

Установим имя сервера — gw: *hostname gw* и *echo gw > /etc/hostname* (рис. 82)

Задание №19. УСтановка имени сервера - gw

Рис. 82: Задание №19. УСтановка имени сервера - gw

В файле /etc/hostname должна быть только одна строка: *gw* (рис. 83), (рис. 84)

Задание №19. Открытие файла /etc/hostname

Рис. 83: Задание №19. Открытие файла /etc/hostname

Задание №19. Редактирование файла /etc/hostname

Рис. 84: Задание №19. Редактирование файла /etc/hostname

Далее установим демон маршрутизации frr. Для этого установим маршрутизацию frr: *apt -y install frr* (рис. 85)

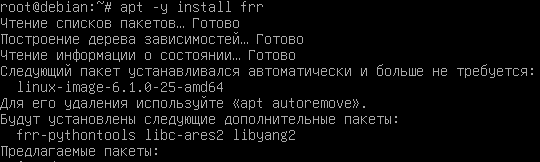


Рис. 85: Задание №19. Установка маршрутизации frr

Далее настроим демон маршрутизации. Отредактируем файл конфигурации frr /etc/frr/frr.conf и добавим конфигурацию для rip:

log syslog informational  
hostname gw  
password zebra  
router rip  
network 192.168.1.0/24  
network 10.0.1.0/8

(рис. 86), (рис. 87)

Задание №19. Открытие файла /etc/frr/frr.conf

Рис. 86: Задание №19. Открытие файла /etc/frr/frr.conf

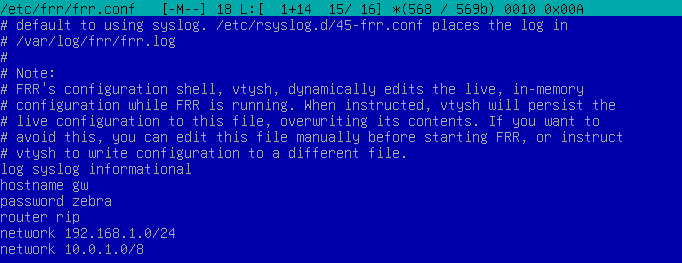


Рис. 87: Задание №19. Редактирование файла /etc/frr/frr.conf

В файле /etc/frr/daemons включаем демон маршрутизации протокола RIP: *ripd=yes* (рис. 88), (рис. 89)

Задание №19. Открытие файла /etc/frr/daemons

Рис. 88: Задание №19. Открытие файла /etc/frr/daemons

Задание №19. Редактирование файла /etc/frr/daemons

Рис. 89: Задание №19. Редактирование файла /etc/frr/daemons

Включим параметр ядра Linux для IP-forward (ретрансляция пакетов между интерфейсами). Для этого в файле /etc/sysctl.conf надо раскоментировать строчку *net.ipv4.ip\_forward=1* (рис. 90), (рис. 91)

Задание №19. Открытие файла /etc/sysctl.conf

Рис. 90: Задание №19. Открытие файла /etc/sysctl.conf

Задание №19. Редактирование файла /etc/sysctl.conf

Рис. 91: Задание №19. Редактирование файла /etc/sysctl.conf

Далее выполним команду *sysctl -p /etc/sysctl.conf* (рис. 92)

Задание №19. Выполнение команды sysctl -p /etc/sysctl.conf

Рис. 92: Задание №19. Выполнение команды sysctl -p /etc/sysctl.conf

Перезагрузим демон (сервис) маршрутизации: *systemctl restart frr* (рис. 93)

Задание №19. Перезагрузка демона маршрутизации

Рис. 93: Задание №19. Перезагрузка демона маршрутизации

Посмотрим статус сервиса: *systemctl status frr* (рис. 94)

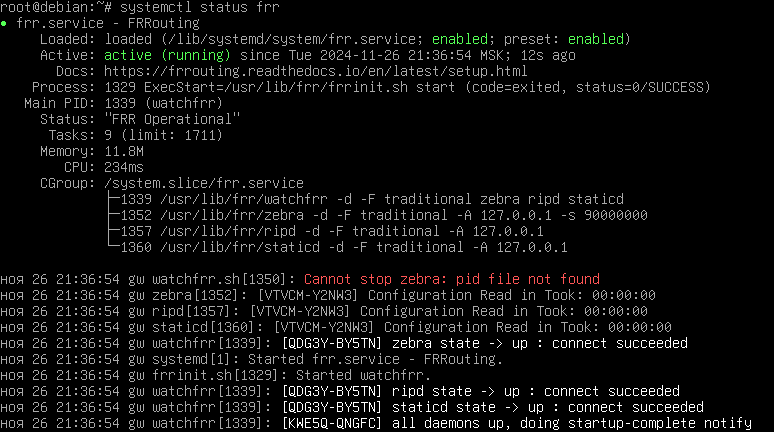


Рис. 94: Задание №19. Проверка статуса сервиса

Работаем на виртуальной машине «Debian 12». Посмотреть, какие у нас есть сетевые интерфейсы: *ip a* (рис. 95)

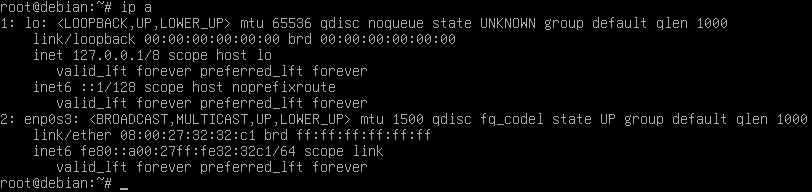


Рис. 95: Задание №19. Проверка сетевых интерфейсов (2)

Настроить на сетевом интерфейсе IP-адрес. ля этого в файл /etc/network/interfaces добавим настройку для сетевого интерфейса enp0s3:

auto enp0s3  
iface enp0s3 inet static  
address 192.168.1.100/24  
gateway 192.168.1.254

(рис. 96), (рис. 97)

Задание №19. Открытие файла /etc/network/interfaces в Debian 12

Рис. 96: Задание №19. Открытие файла /etc/network/interfaces в Debian 12

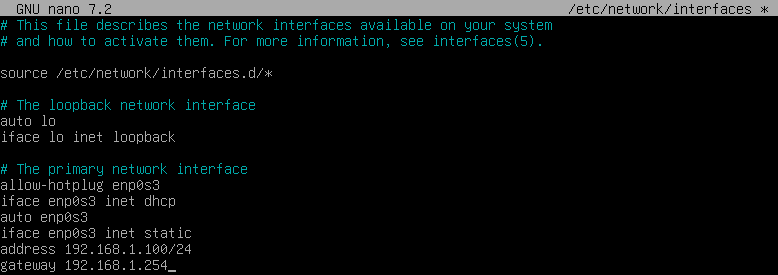


Рис. 97: Задание №19. Редактирование файла /etc/network/interfaces в Debian 12

Включим сетевой интерфейс командами *ifdown enp0s3* и *ifup enp0s3* (рис. 98)

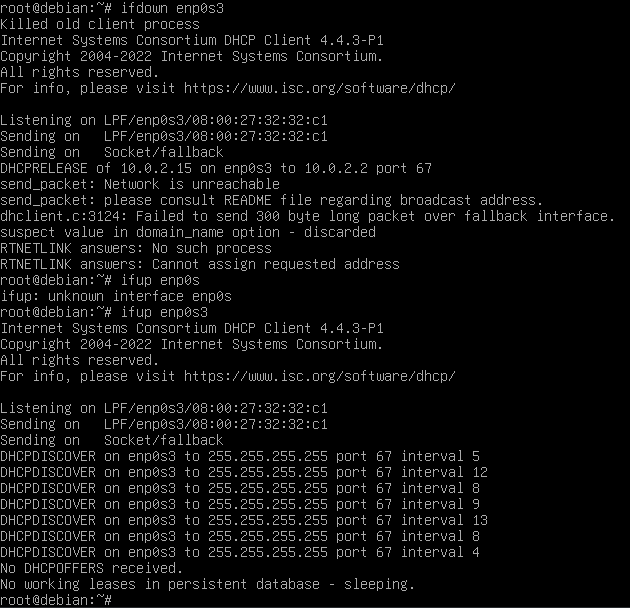


Рис. 98: Задание №19. Включение сетевого интерфейса

Проверим успешную настройку: *ip a* (рис. 99)

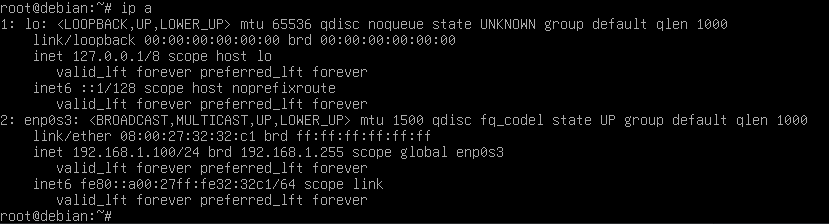


Рис. 99: Задание №19. Проверка успешной настройки в Debian 12

ПРоверим пинг до шлюза и пинг до второго интерфейса шлюза командами *ping 192.168.1.254* и *ping 10.0.1.100* (рис. 100)

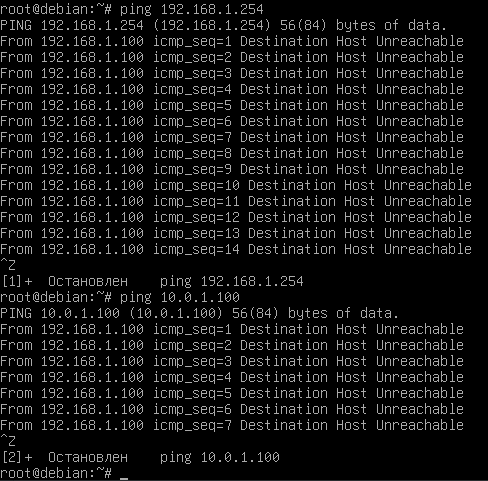


Рис. 100: Задание №19. Проверка пингов

Работаем на виртуальной машине «Windows 10 (Орг. администрирования)». Настроим сетевые интерфейсы и сетевую конфигурацию. Для этого перейдём в Параметры, Сеть и Интернет, Состояние, Настройка параметров адаптера. В свойствах адаптера Ethernet убираем протокол IPv6 (рис. 101)

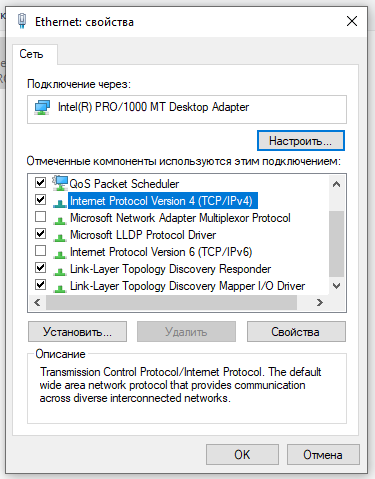


Рис. 101: Задание №19. Убираем протокол IPv6

Переходим в Протокол IPv4, Свойства. Устанавливаем:

1. IP-адрес: 172.16.1.100
2. Маску подсети: 255.255.0.0
3. Основной шлюз: 172.16.1.254 (рис. 102)

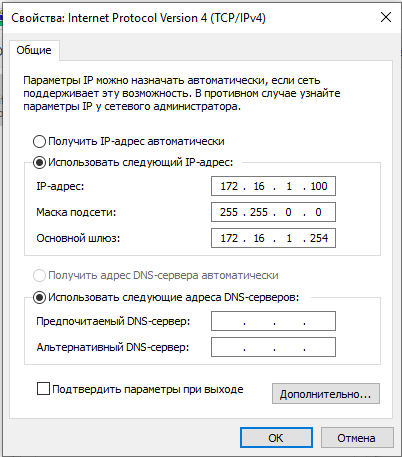


Рис. 102: Задание №19. Настройка протокола IPv4

Диагностика настройки интерфейса и связи до шлюза. Заходим в cmd и выполняем команды *ipconfig* и *ping 172.16.1.254* (рис. 103), (рис. 104)

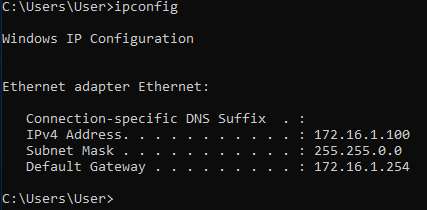


Рис. 103: Задание №19. ipconfig

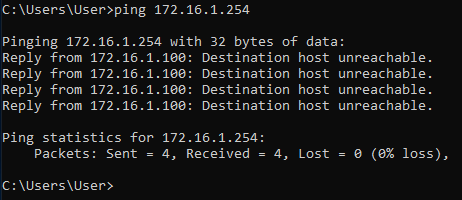


Рис. 104: Задание №19. ping 172.16.1.254

Для проверки связи с Windows машинами посредством команды ping необходимо разрешить в брандмауэрах Windows эхо-ответы. Для Windows 10 ставим галочку Enabled в двух местах:

1. Windows System, Control Panel, Брандмауэр Защитника Windows, Дополнительные параметры, Inbound Rules, Общий доступ к файлам и принтерам (эхо-запрос - входящий трафик ICMPv4) (рис. 105)
2. Windows System, Control Panel, Брандмауэр Защитника Windows, Дополнительные параметры, Inbound Rules, Наблюдение за виртуальной машиной (эхо-запрос - ICMPv4 - входящий трафик) (рис. 106)

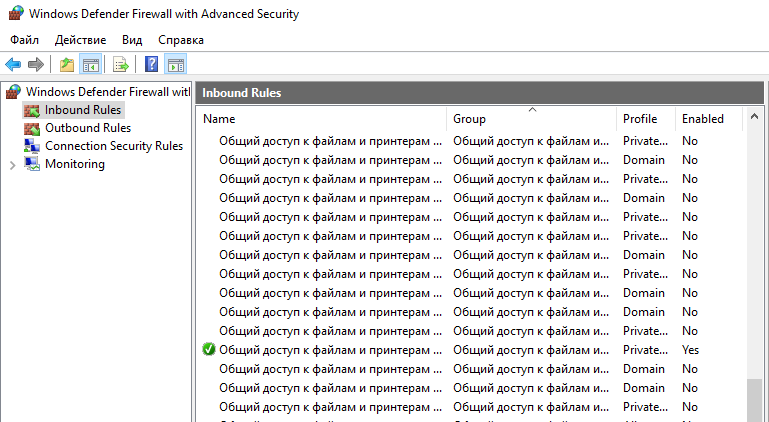


Рис. 105: Задание №19. Галочки (1)

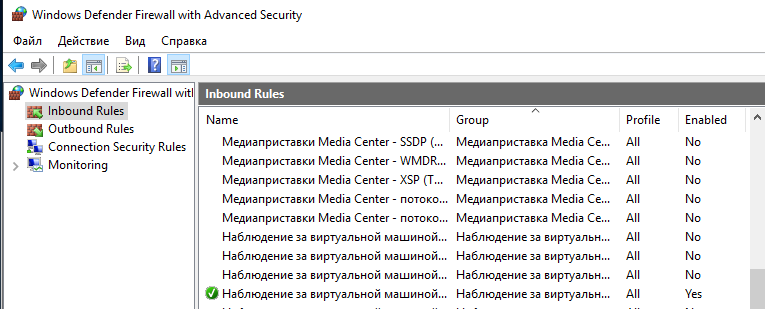


Рис. 106: Задание №19. Галочки (2)

Далее выполним саму практическую работу. Для этого выполняем следующие команды:

1. tracert 192.168.1.100 (рис. 107)
2. ping 192.168.1.100 (рис. 108)

(рис. 109)

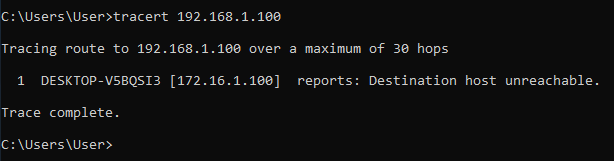


Рис. 107: Задание №19. tracert 192.168.1.100

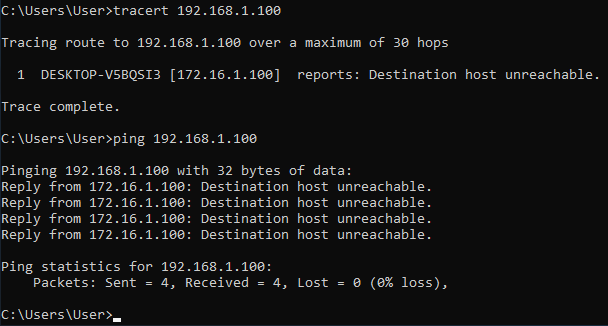


Рис. 108: Задание №19. ping 192.168.1.100

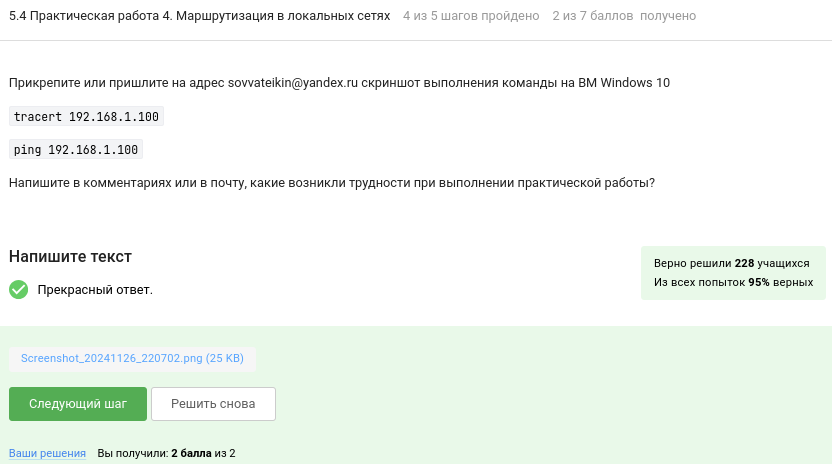


Рис. 109: Задание №19

## 3.3 Сервисы электронной почты

Задание №20: прочитав информацию на странице “Условная схема использования протоколов передачи данных при доставке электронного письма от одного адресата до другого”, я отметила, что для отправки почты клиентом используется протокол *SMTP* (рис. 110)

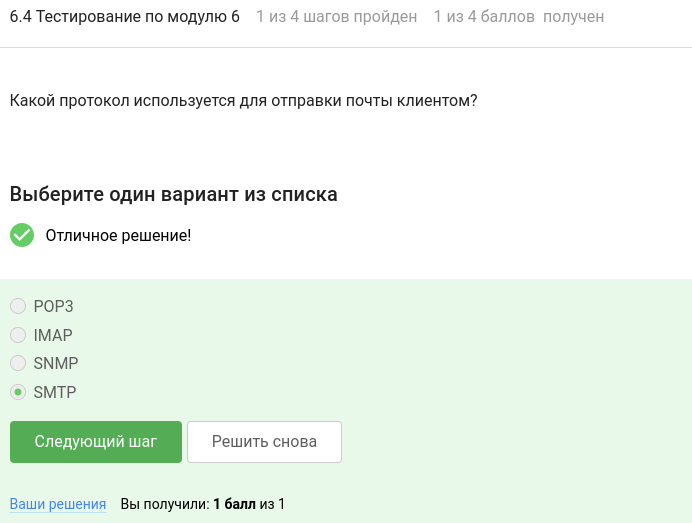


Рис. 110: Задание №20

Задание №21: прочитав информацию на странице “Условная схема использования протоколов передачи данных при доставке электронного письма от одного адресата до другого”, я отметила, что для получения почты клиентом используется протокол *POP3* (рис. 111)

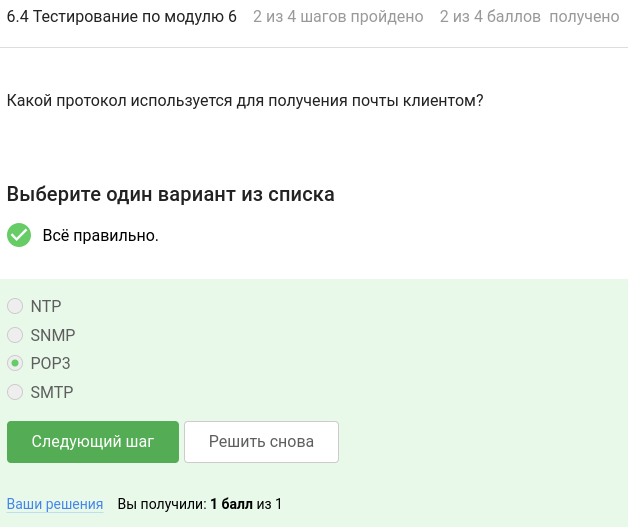


Рис. 111: Задание №21

Задание №22: прочитав информацию на странице “Условная схема использования протоколов передачи данных при доставке электронного письма от одного адресата до другого”, я отметила, что для пересылки почтовых сообщений между почтовыми серверами MTA используется протокол *SMTP* (рис. 112)

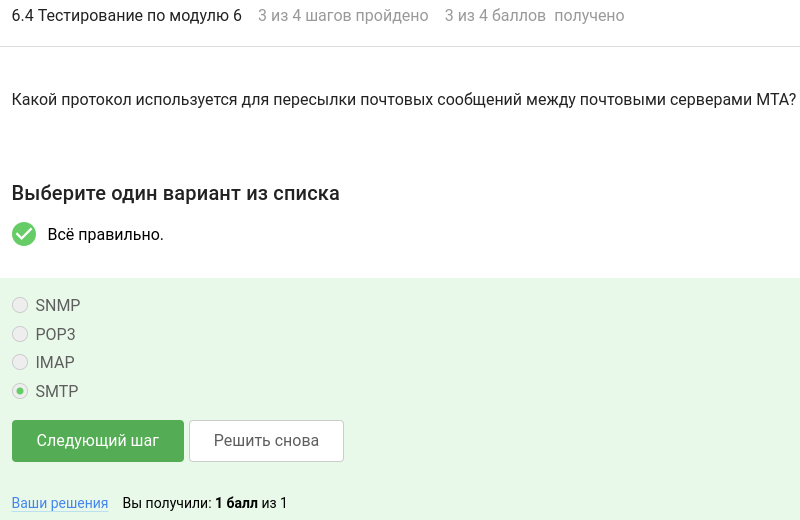


Рис. 112: Задание №22

Задание №23: прочитав информацию на странице “Протокол POP3 (Post Office Protocol Version 3)” и “Протокол IMAP ( Internet Message Access Protocol)”, я отметила отличительные особенности протоколов IMAP и POP3 (рис. 113)

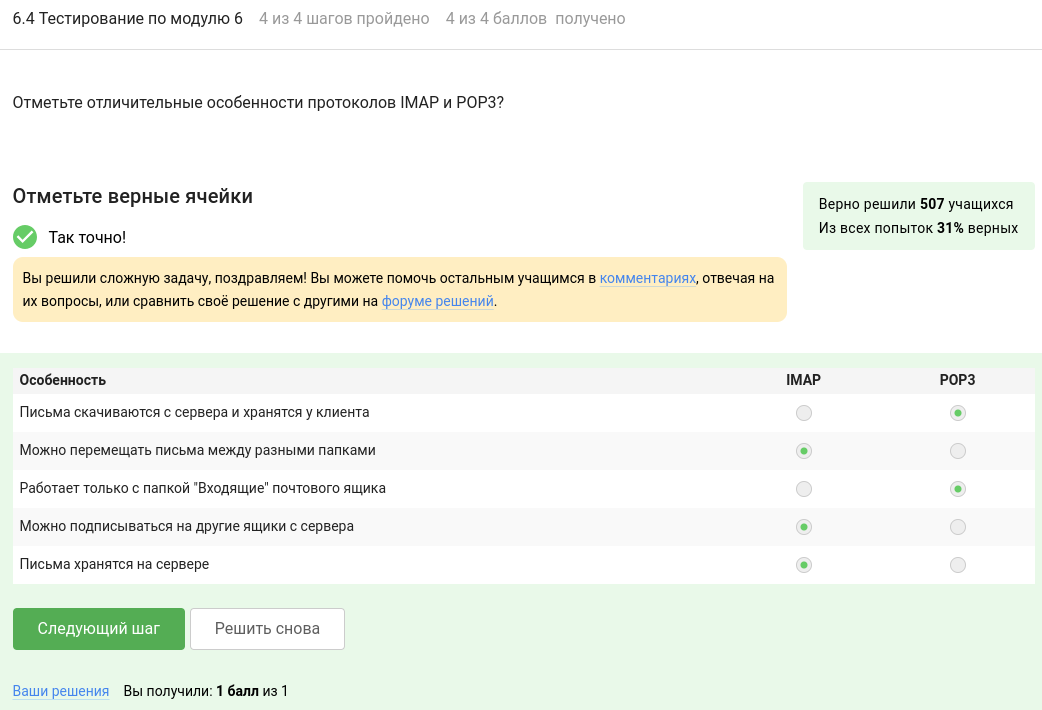


Рис. 113: Задание №23

Задание №24 (практическая работа): Необходимо установить и настроить серверы MTA postfix и MDA сyrus, авторизацию SASL, а также протестировать работу со своей клиентской машины через MUA Thunderbird. Сначала установим имя машины adm.org командой *hostname adm.org* (рис. 114)

Задание №24. Установка имени машины

Рис. 114: Задание №24. Установка имени машины

Далее в файле /etc/hostname напишем: adm.org (рис. 115), (рис. 116)

Задание №24. Открытие файла /etc/hostname

Рис. 115: Задание №24. Открытие файла /etc/hostname

Задание №24. Редактирование файла /etc/hostname

Рис. 116: Задание №24. Редактирование файла /etc/hostname

В файле /etc/hosts пропишем соответствие IP-адреса машины и сетевого имени: ip-адрес adm.org. Вот так *10.0.2.15 adm adm.org* (рис. 117), (рис. 118)

Задание №24. Открытие файла /etc/hosts

Рис. 117: Задание №24. Открытие файла /etc/hosts

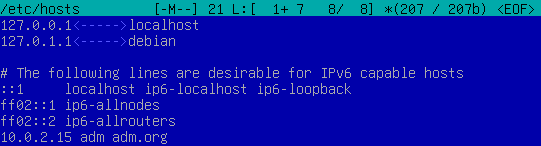


Рис. 118: Задание №24. Редактирование файла /etc/hosts

Установим и настроим MTA postfix: *apt -y install postfix*. При установке указываем тип почтовой настройки - Интернет-сайт, а системное почтовое имя - adm.org (рис. 119), (рис. 120), (рис. 121)

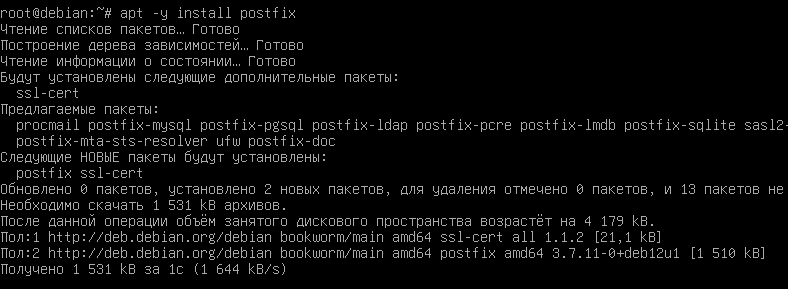


Рис. 119: Задание №24. Установка MTA postfix

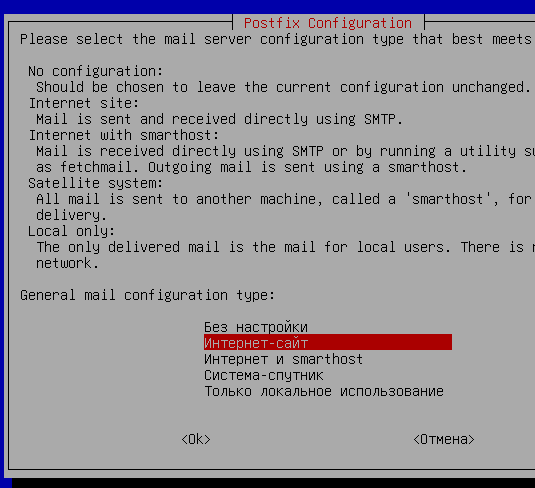


Рис. 120: Задание №24. Тип почтовой настройки

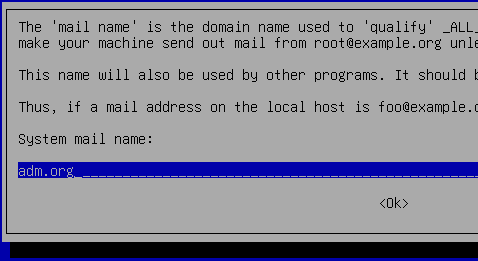


Рис. 121: Задание №24. Системное почтовое имя

После установки в файле конфигурации /etc/postfix/main.cf устанавливаем имя хоcта (находим параметр myhostname и меняем): *myhostname = adm.org* (рис. 122), (рис. 123)

Задание №24. Открытие файла /etc/postfix/main.cf (1)

Рис. 122: Задание №24. Открытие файла /etc/postfix/main.cf (1)

Задание №24. Редактирование файла /etc/postfix/main.cf (1)

Рис. 123: Задание №24. Редактирование файла /etc/postfix/main.cf (1)

Проверим корректность настроек сервера: *postconf -n* (рис. 124)

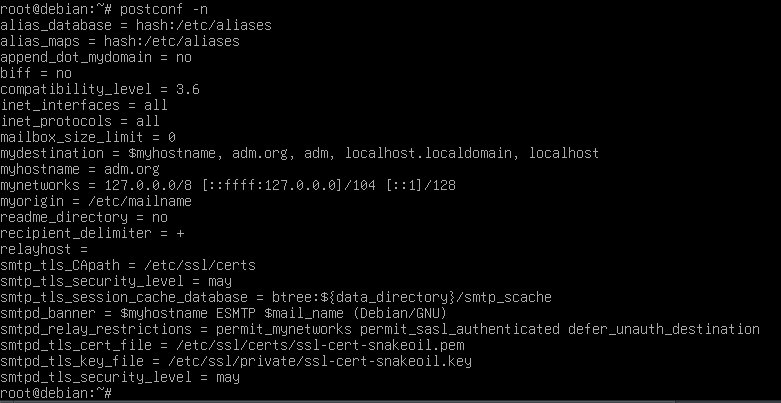


Рис. 124: Задание №24. Проверка настроек сервера

Перезапустим сервис postfix и проверим его статус: *systemctl restart postfix* и *systemctl status postfix* (рис. 125)

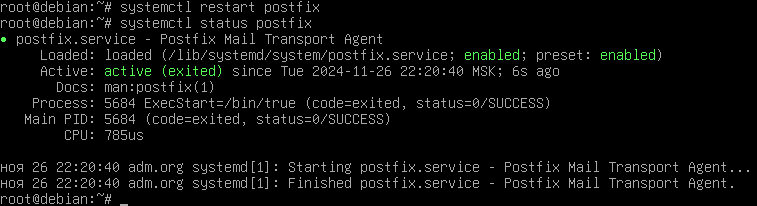


Рис. 125: Задание №24. Перезапуск сервера postfix и проверка его статуса (1)

Установим и настроим MDA cyrus: *apt -y install cyrus-imapd cyrus-pop3d cyrus-admin* (рис. 126)

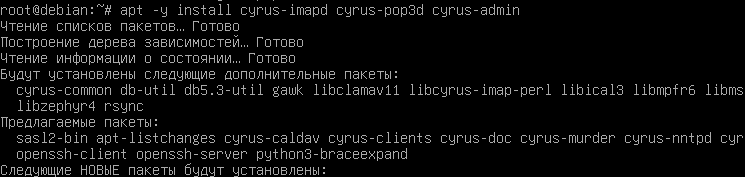


Рис. 126: Задание №24. Установка MDA cyrus

После установки в файле конфигурации Cyrus /etc/cyrus.conf закомментируем строки, начинающиеся с nntp и http, строка с lmtpunix должна быть раскомментирована (рис. 127), (рис. 128)

Задание №24. Открытие файла /etc/cyrus.conf

Рис. 127: Задание №24. Открытие файла /etc/cyrus.conf

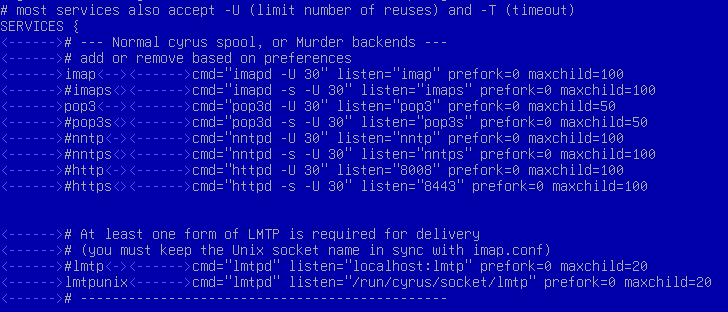


Рис. 128: Задание №24. Редактирование файла /etc/cyrus.conf

В файл настройки IMAP /etc/imapd.conf добавляем строки для автоматического создания ящиков и папок «Отправленные» и «Удаленные» при получении письма:

autocreate\_post: 1  
autocreate\_inbox\_folders: Trash | Sent  
autocreate\_subscribe\_folders: Trash | Sent

(рис. 129), (рис. 130)

Задание №24. Открытие файла /etc/imapd.conf

Рис. 129: Задание №24. Открытие файла /etc/imapd.conf

Задание №24. Редактирование файла /etc/imapd.conf

Рис. 130: Задание №24. Редактирование файла /etc/imapd.conf

Перезапустим сервис cyrus и проверим его статус: *systemctl restart cyrus-imapd* и *systemctl status cyrus-imapd* (рис. 131)

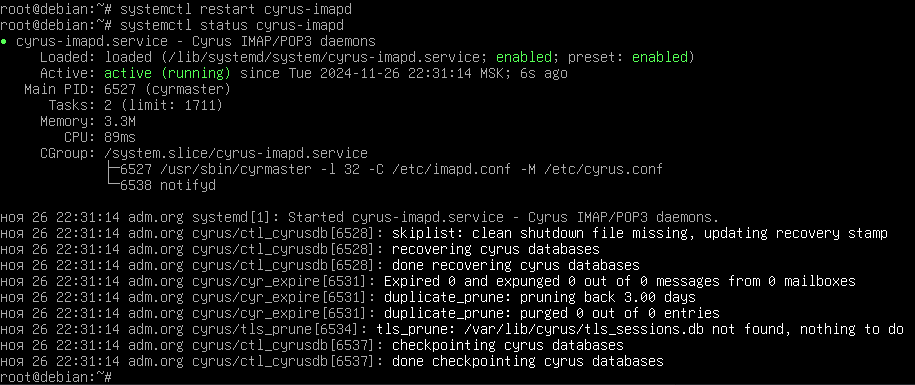


Рис. 131: Задание №24. Перезапуск сервера cyrus-imapd и проверка его статуса

В файле конфигурации /etc/postfix/main.cf добавим параметр для связи с MDA cyrus по протоколу LMTP через сокет: *mailbox\_transport = lmtp:unix:/run/cyrus/socket/lmtp* (рис. 132), (рис. 133)

Задание №24. Открытие файла /etc/postfix/main.cf (2)

Рис. 132: Задание №24. Открытие файла /etc/postfix/main.cf (2)

Задание №24. Редактирование файла /etc/postfix/main.cf (2)

Рис. 133: Задание №24. Редактирование файла /etc/postfix/main.cf (2)

Далее разрешим модулю LMTP работать не в закрытой файловой среде, чтобы получать доступ к сокету, для этого в файле конфигурации /etc/postfix/master.cf приводим строку к виду (убираем запуск в chroot): *lmtp unix - - n - - lmtp* (рис. 134), (рис. 135)

Задание №24. Открытие файла /etc/postfix/master.cf (1)

Рис. 134: Задание №24. Открытие файла /etc/postfix/master.cf (1)

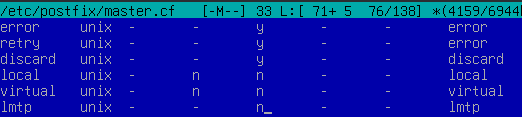


Рис. 135: Задание №24. Редактирование файла /etc/postfix/master.cf (1)

В том же файле раскомментируем строки для передачи писем в MDA cyrus:

cyrus unix - n n - - pipe  
user=cyrus argv=/cyrus/bin/deliver -e -r #{sender} -m extension{user}

(рис. 136)

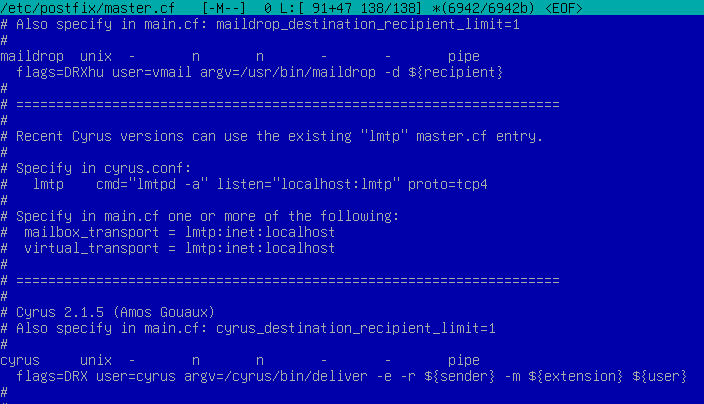


Рис. 136: Задание №24. Редактирование файла /etc/postfix/master.cf (2)

Выполним для получения доступа postfix к сокету LMTP: *usermod -aG mail postfix* (рис. 137)

Задание №24. Получение доступа postfix к сокету LMTP

Рис. 137: Задание №24. Получение доступа postfix к сокету LMTP

Проверим настройки и перезапустим сервис postfix: *systemctl restart postfix* и *systemctl status postfix* (рис. 138)

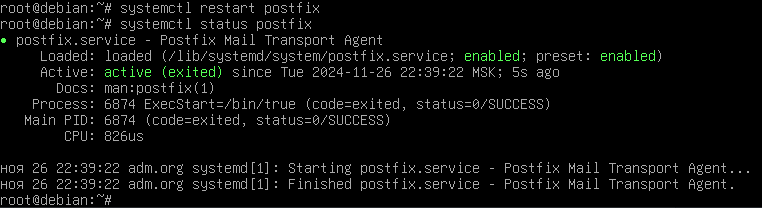


Рис. 138: Задание №24. Перезапуск сервера postfix и проверка его статуса (2)

Далее установим простую систему авторизации SASL (Simple Authentication and Security Layer): *apt -y install sasl2-bin* (рис. 139)

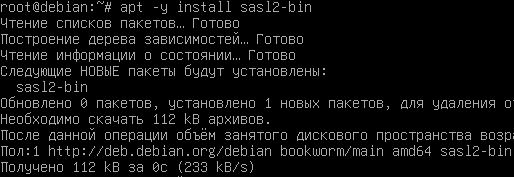


Рис. 139: Задание №24. Установка SASL

Настроим MTA postfix для работы с SASL, для этого добавим в файл конфигурации /etc/postfix/main.cf строку: *smtpd\_sasl\_auth\_enable = yes* (рис. 140), (рис. 141)

Задание №24. Открытие файла /etc/postfix/main.cf (3)

Рис. 140: Задание №24. Открытие файла /etc/postfix/main.cf (3)

Задание №24. Редактирование файла /etc/postfix/main.cf (3)

Рис. 141: Задание №24. Редактирование файла /etc/postfix/main.cf (3)

После дадим доступ базе данных пользователей /etc/sasldb2, для этого выполним: *usermod -aG sasl postfix* (рис. 142)

Задание №24. Доступ базе данных

Рис. 142: Задание №24. Доступ базе данных

Разрешим модулю SMTP работать не в закрытой файловой среде, чтобы получать доступ к базе данных пользователей /etc/sasldb2, для этого в файле конфигурации /etc/postfix/master.cf приведём строку к виду (убираем запуск в chroot): *smtp inet n - n - - smtpd* (рис. 143), (рис. 144)

Задание №24. Открытие файла /etc/postfix/master.cf (2)

Рис. 143: Задание №24. Открытие файла /etc/postfix/master.cf (2)

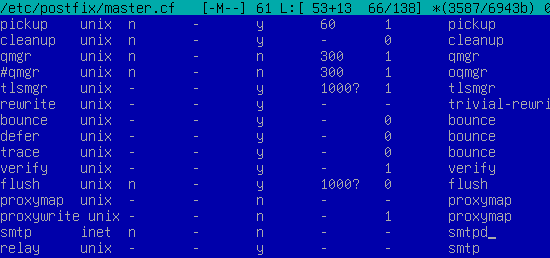


Рис. 144: Задание №24. Редактирование файла /etc/postfix/master.cf (3)

Создадим пользователя student: *saslpasswd2 -c student@adm.org*. На запрос паролей наберём: P@ssw0rd (рис. 145)

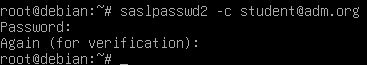


Рис. 145: Задание №24. Создание пользователя student

Проверим успешность создания пользователя, для этого выполним: *sasldblistusers2*. Результатом должна быть строка: student@adm.org: userPassword (рис. 146)

Задание №24. Проверка успешного создание пользователя

Рис. 146: Задание №24. Проверка успешного создание пользователя

Добавим пользователя student в список postfix, в файл /etc/aliases добавим строку: *student: student* (рис. 147), (рис. 148)

Задание №24. Открытие файла /etc/aliases

Рис. 147: Задание №24. Открытие файла /etc/aliases

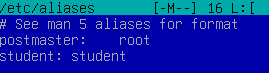


Рис. 148: Задание №24. Редактирование файла /etc/aliases

Далее выполняем: *postalias /etc/aliases* (рис. 149)

Задание №24. postalias /etc/aliases

Рис. 149: Задание №24. postalias /etc/aliases

Перезапустим postfix: *systemctl restart postfix* (рис. 150)

Задание №24. Перезапуск postfix

Рис. 150: Задание №24. Перезапуск postfix

Протестируем работу почтовых сервисов на самом сервере (рис. 151)

Задание №24. Тестирование работы почтовых сервисов

Рис. 151: Задание №24. Тестирование работы почтовых сервисов

Далее необходимо открыть/пробросить порты IMAP и SMTP. Для этого на запущенной ВМ переходим в: Устройства->Сеть->Настроить сеть, кнопка Дополнительно, Проброс портов. Нажимаем +, порт хоста - 1143, порт гостя - 143. Снова нажимаем +, порт хоста - 1025, порт гостя - 25 (рис. 152)

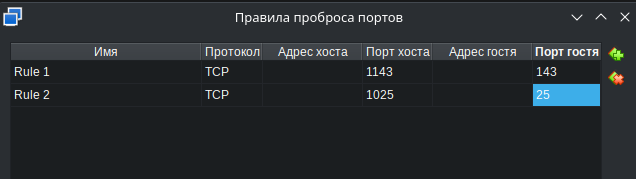


Рис. 152: Задание №24. Проброс портов

Запускаем со своего компьютера почтового клиента Thunderbird и тестируем работу почтового сервера. Нажимаем *Выберите, что нужно настроить, Электронная почта* (рис. 153)

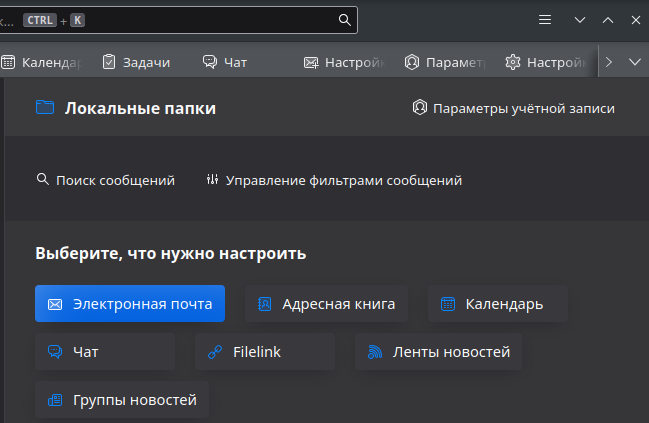


Рис. 153: Задание №24. Настройка электронной почты

Дальше ввожим данные:

1. Ваше полное имя: student
2. Адрес электронной почты: student@adm.org
3. Пароль: P@ssw0rd

(рис. 154)

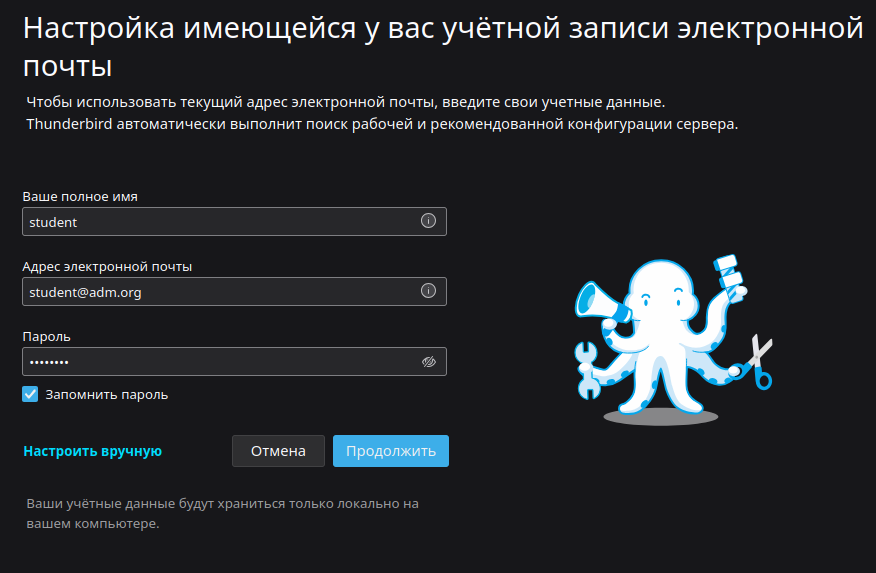


Рис. 154: Задание №24. Ввод данных (1)

Нажимаем ссылку «Настроить вручную». Там выставляем:

1. Входящая IMAP: Имя сервера localhost, Порт 1143
2. Исходящая SMTP: Имя сервера localhost, Порт 1025
3. Защита соединения Нет
4. Метод аутентификации обычный пароль
5. Имя пользователя student

После нажимаем кнопки «Перетестировать» и «Готово» (рис. 155)

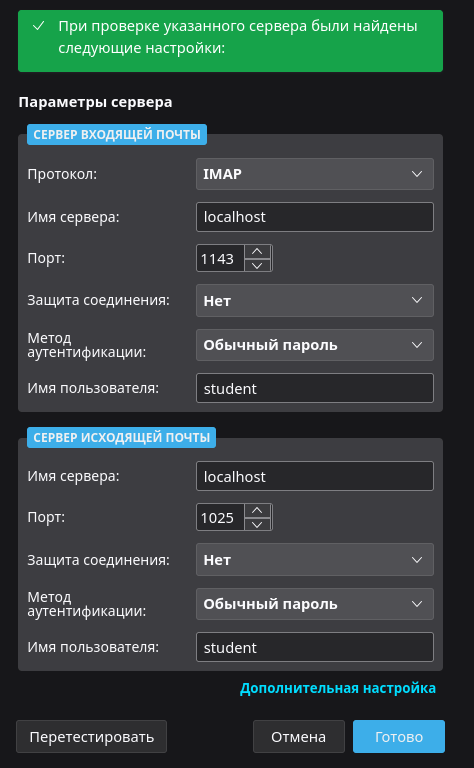


Рис. 155: Задание №24. Ввод данных (2)

ПЕреходим на созданную учётную запись, нажимаем на правую кнопку мыши на учётной записи и выбираем «Подписаться..», выбираем галочками папки Sent и Trash (рис. 156)

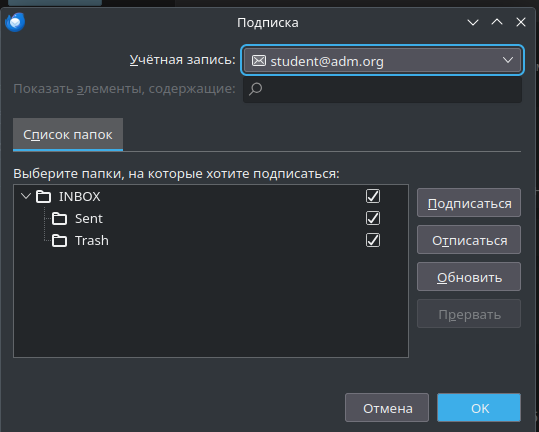


Рис. 156: Задание №24. Sent и Trash

При нажатии на Входящие должны получить ранее отправленное письмо с темой «Test» и содержанием «Hello» (рис. 157)

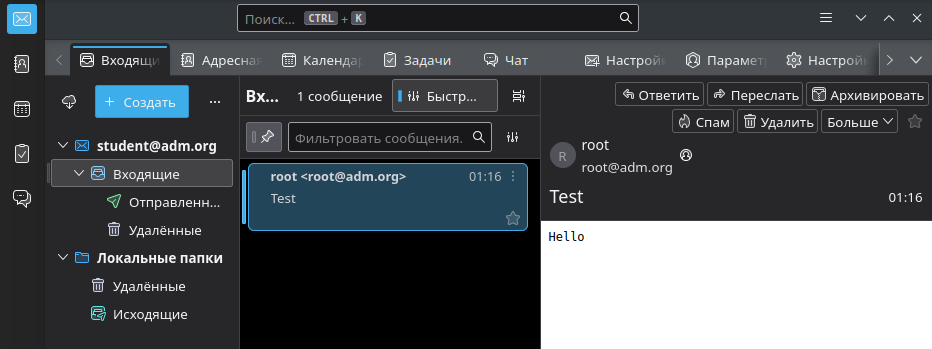


Рис. 157: Задание №24. Полученные сообщения

Необходимо протестировать отправку писем по SMTP. Для этого нажимаем Ответить на письмо, отправляем в свой адрес student@adm.org и получаем с сервера этот ответ (рис. 158)

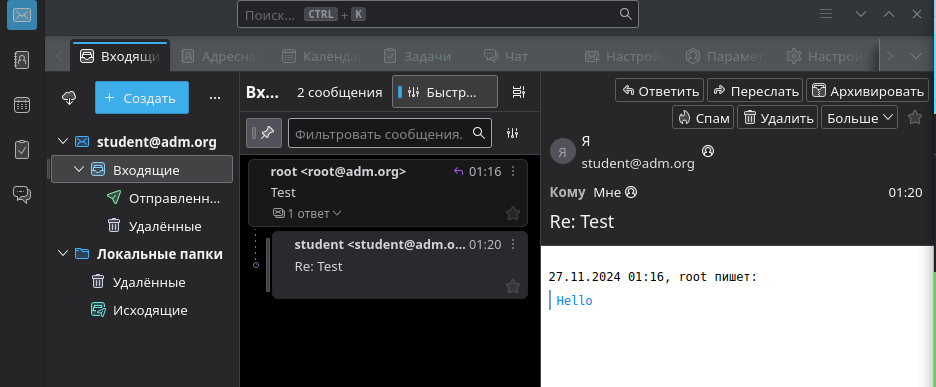


Рис. 158: Задание №24. Полученный ответ

После этого практическая работа считается выполненной (рис. 159)

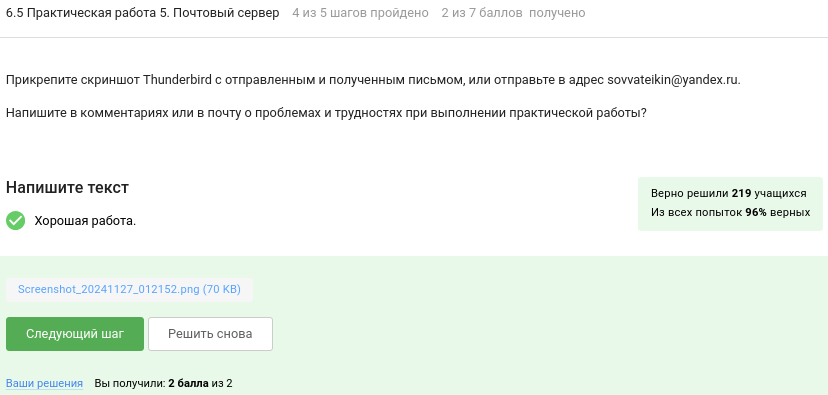


Рис. 159: Задание №24

## 3.4 Итоговая анкета

Задание №25: на скрине всё видно (рис. 160)

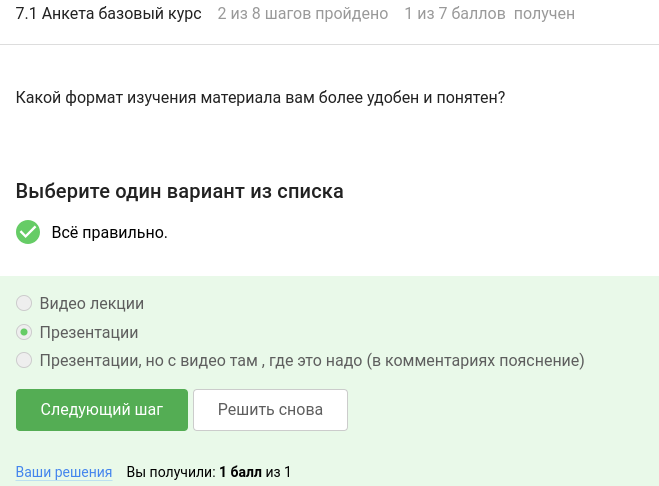


Рис. 160: Задание №25

Задание №26: на скрине всё видно (рис. 161)

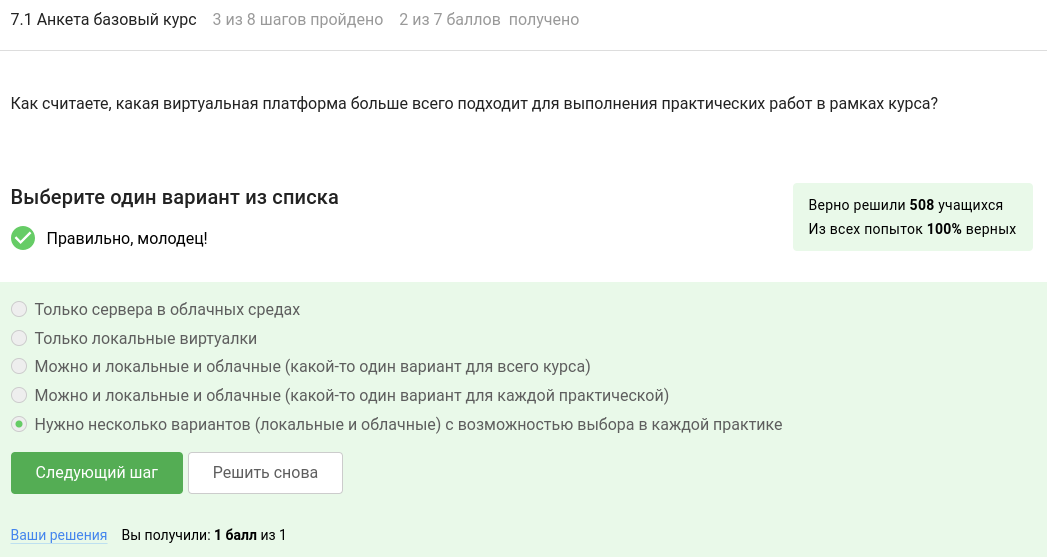


Рис. 161: Задание №26

Задание №27: на скрине всё видно (рис. 162)

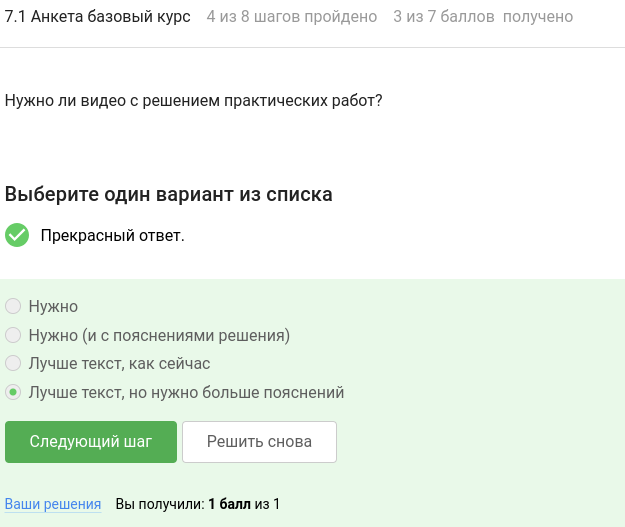


Рис. 162: Задание №27

Задание №28: на скрине всё видно (рис. 163)

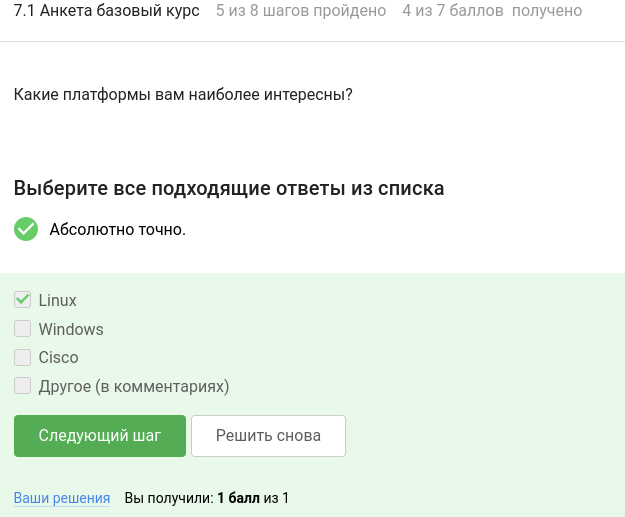


Рис. 163: Задание №28

Задание №29: на скрине всё видно (рис. 164)

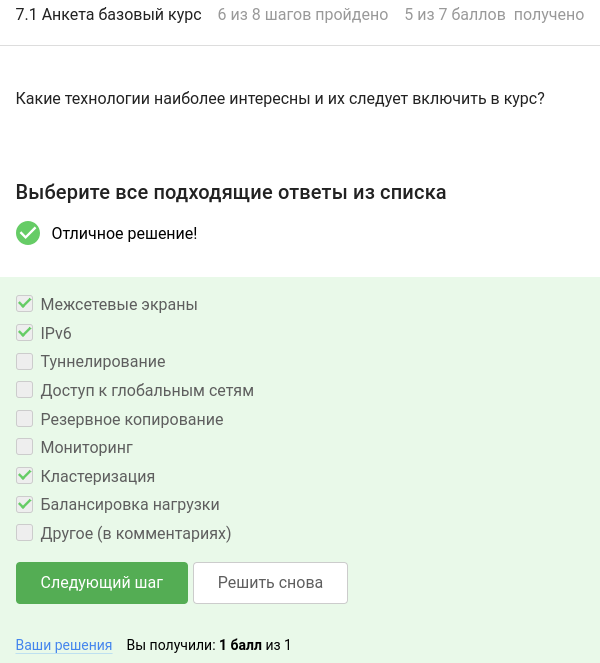


Рис. 164: Задание №29

Задание №30: на скрине всё видно (рис. 165)

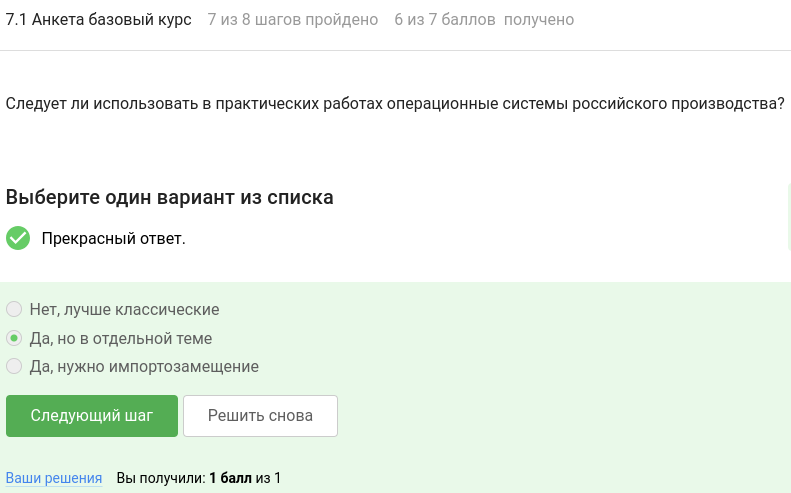


Рис. 165: Задание №30

Задание №31: на скрине всё видно (рис. 166)

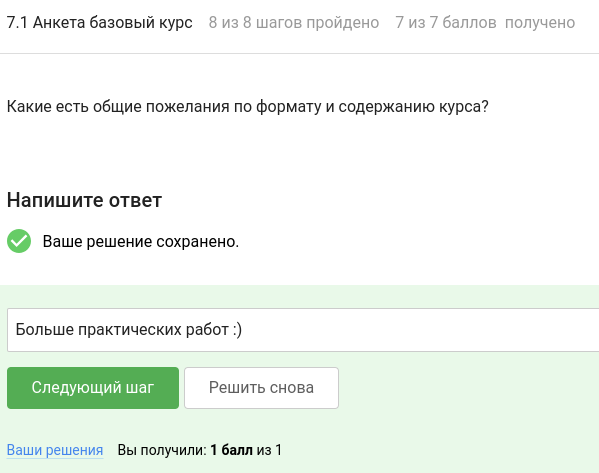


Рис. 166: Задание №31

# 4 Выводы

В ходе выполнения 2 раздела внешнего курса на stepik я освоила сервер Active Directory на Debian 12 и Windows 10 в виртуальной машине VirtualBox, работу с почтовым сервером, а также выполнила практические работы *Практическая работа 3. Active Directory*, *Практическая работа 4. Маршрутизация в локальных сетях* и *Практическая работа 5. Почтовый сервер*.

# 5 Список литературы

1. Курс на stepik. Организация администрирования компьютерных сетей [Электронный ресурс] URL: https://stepik.org/course/83555/syllabus