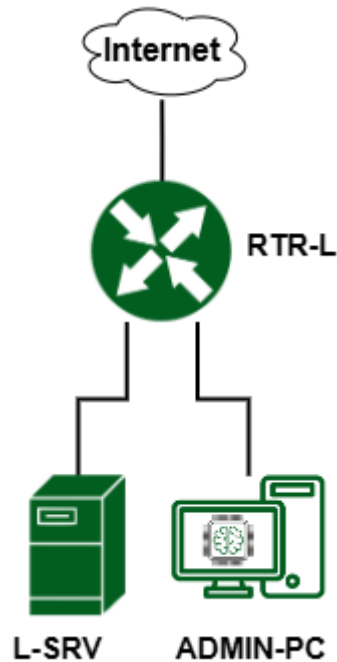


## Задание экзамена «Администрирование операционных систем»



0. Имена хостов в созданных ВМ должны быть установлены в соответствии с доменным именем.

Адресация должна быть выполнена в соответствии с Таблицей 1.

Таблица 1

Имя ВМ	IP-адрес
RTR-L	Сети internet адрес прилетает по DHCP 10.10.10.1/24 – для подсети офиса L-RTR 20.20.20.1/24 – для подсети офиса ADMIN-PC
L-SRV	10.10.10.100/24
ADMIN-PC	20.20.20.150/24

- Настройка динамической трансляции адресов на RTR-L
  - Настройте динамическую трансляцию что бы все устройства могли ходить в интернет
- Настройте сервер DHCP на базе RTR-L.
  - Создайте два пула для серверов (10.10.10.100-10.10.10.120) и клиентских ПК (20.20.20.150-20.20.20.200)
  - Зарезервируйте выданный ip адрес серверу L-SRV
  - Адрес шлюза по умолчанию - адреса маршрутизаторов RTR-L
  - Адрес DNS-сервера для машины ADMIN-PC - адрес сервера L-SRV.
  - DNS-суффикс для офисов HQ и BR - au.team
- Настройте доменный контроллер Samba на машине L-SRV. Имя домена au.team.
  - Создайте 15 пользователей для офиса left (группа left), имена пользователей формата user№.userl.
  - Создайте 5 пользователей группы администратор, имена пользователей формата user№.admin.

- c. Пользователи группы left и admin имеют право аутентифицироваться на любом клиентском ПК (ADMIN-PC).
  - d. Пользователи группы left должны иметь возможность повышать привилегии для выполнения ограниченного набора команд: cat, grep, id.
  - e. Пользователи группы admin должны иметь возможность повышать привилегии без ввода пароля.
  - f. Для всех пользователей домена должны быть реализованы общие каталоги по пути /mnt/Adsamba. Должно происходить автомонтирование
4. Настройка DNS для офиса left.
- a. Основной DNS-сервер реализован на доменном контроллере.
  - b. Для всех устройств используется доменное имя au.team.
  - c. Для всех устройств двух офисов необходимо создать записи A и PTR.
  - d. В качестве DNS сервера пересылки используйте сервера 94.232.137.104

Машина	Запись A
L-SRV	l-srv.au.team
ADMIN-PC	admin-pc.au.team
RTR-L	rtr-l.au.team

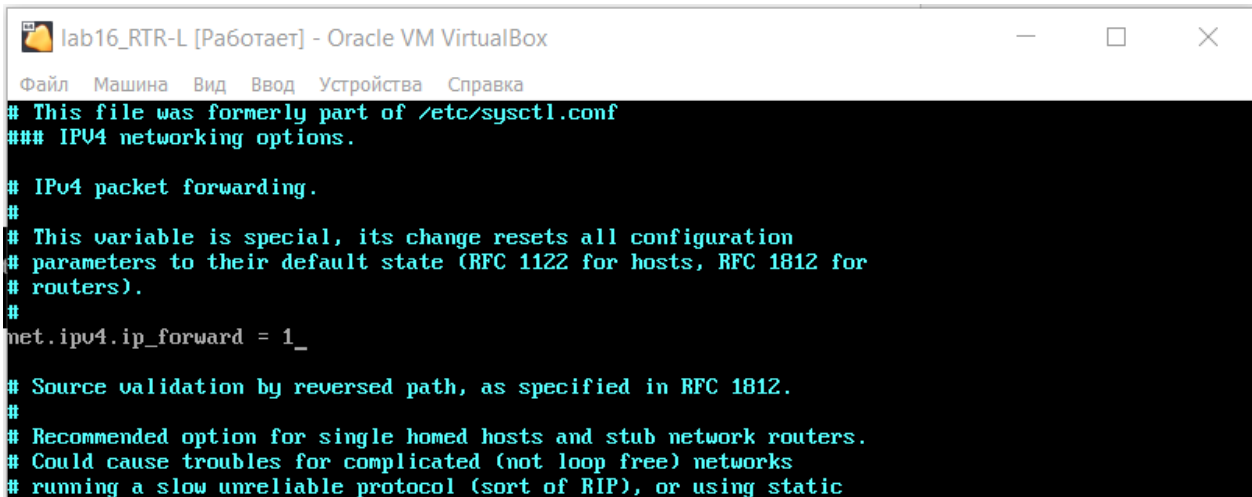
5. Настройка межсетевого экрана на RTR-L
- a. Реализуйте подключение к серверу по SSH с ADMIN-PC. Используйте порт 65000 на маршрутизаторе RTR-L
  - b. Заблокируйте доступ к youtube
  - c. Запретите ICMP трафик с L-SRV на RTR-L

## ЗАДАНИЕ 0

А) На RTR-L

```
Password:
[root@srv ~]# hostnamectl set-hostname rtr-l.au.team; exec bash
[root@rtr-l ~]# _
```

vim /etc/net/sysctl.conf



```
lab16_RTR-L [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
# This file was formerly part of /etc/sysctl.conf
### IPv4 networking options.

# IPv4 packet forwarding.
#
# This variable is special, its change resets all configuration
# parameters to their default state (RFC 1122 for hosts, RFC 1812 for
# routers).
#
net.ipv4.ip_forward = 1_

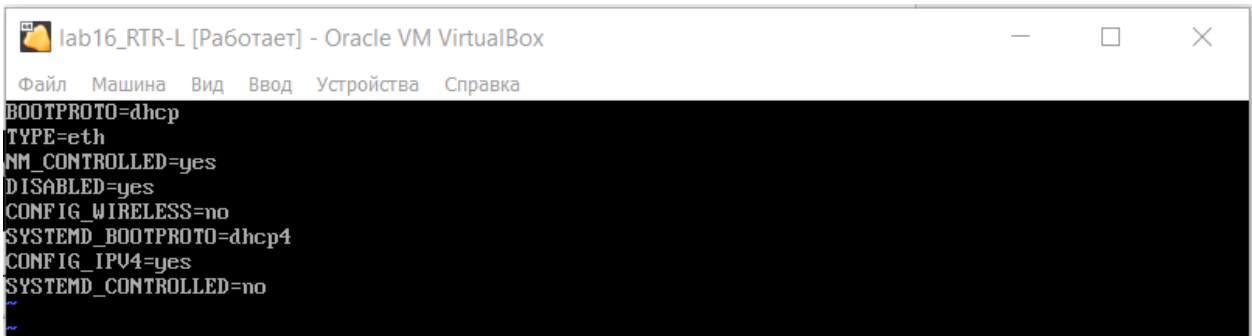
# Source validation by reversed path, as specified in RFC 1812.
#
# Recommended option for single homed hosts and stub network routers.
# Could cause troubles for complicated (not loop free) networks
# running a slow unreliable protocol (sort of RIP), or using static
```

Сохраняем :wq

cp -r /etc/net/ifaces/ens19/ /etc/net/ifaces/ens20/

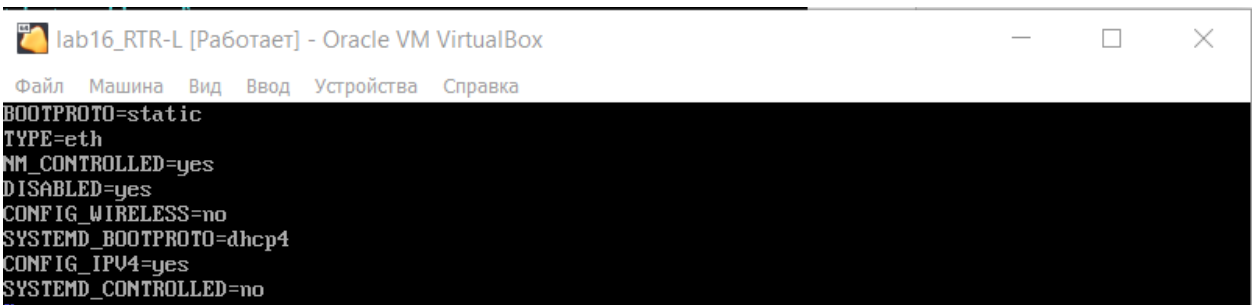
cp -r /etc/net/ifaces/ens19/ /etc/net/ifaces/ens21/

vim /etc/net/ifaces/ens19/options



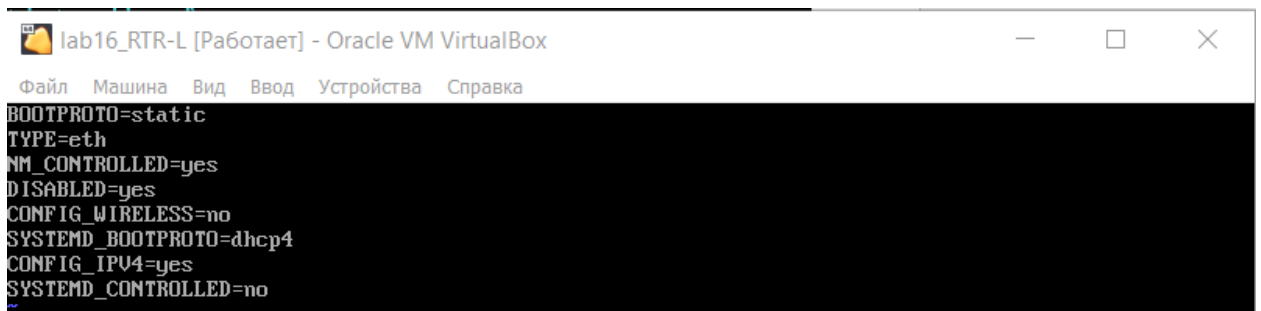
```
lab16_RTR-L [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
BOOTPROTO=dhcp
TYPE=eth
NM_CONTROLLED=yes
DISABLED=yes
CONFIG_WIRELESS=no
SYSTEMD_BOOTPROTO=dhcp4
CONFIG_IPV4=yes
SYSTEMD_CONTROLLED=no
```

vim /etc/net/ifaces/ens20/options



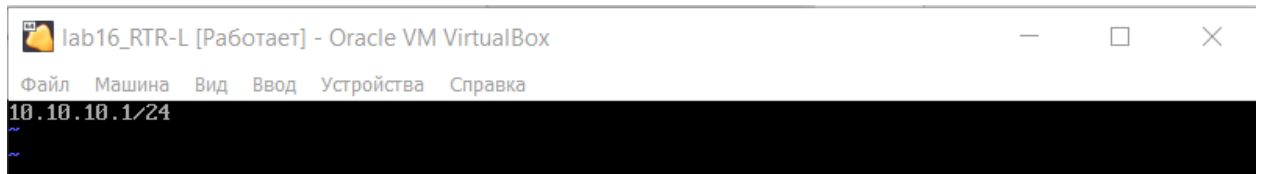
```
lab16_RTR-L [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
BOOTPROTO=static
TYPE=eth
NM_CONTROLLED=yes
DISABLED=yes
CONFIG_WIRELESS=no
SYSTEMD_BOOTPROTO=dhcp4
CONFIG_IPV4=yes
SYSTEMD_CONTROLLED=no
```

vim /etc/net/ifaces/ens21/options



```
lab16_RTR-L [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
BOOTPROTO=static
TYPE=eth
NM_CONTROLLED=yes
DISABLED=yes
CONFIG_WIRELESS=no
SYSTEMD_BOOTPROTO=dhcp4
CONFIG_IPV4=yes
SYSTEMD_CONTROLLED=no
```

vim /etc/net/ifaces/ens20/ipv4address



```
lab16_RTR-L [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
10.10.10.1/24
```

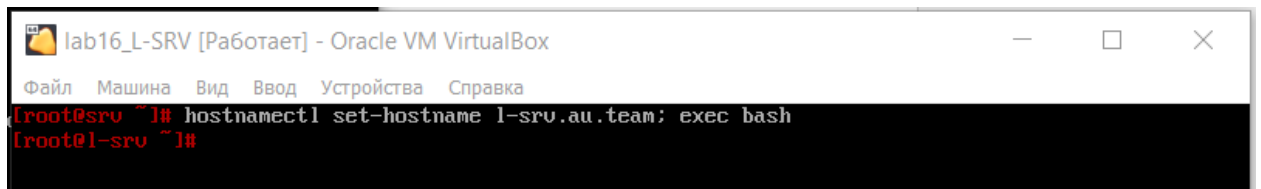
vim /etc/net/ifaces/ens21/ipv4address



```
lab16_RTR-L [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
20.20.20.1/24
```

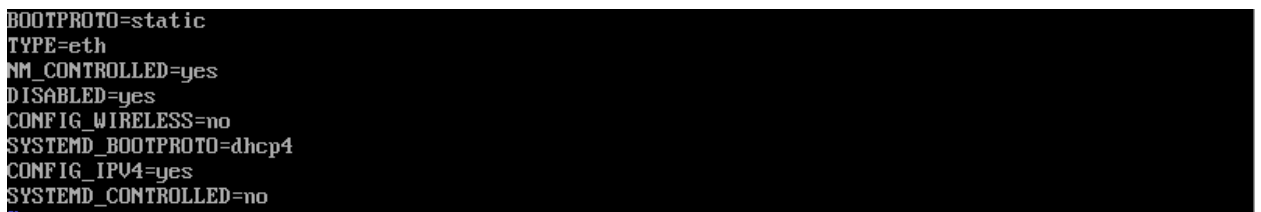
reboot

Б) На L-SRV



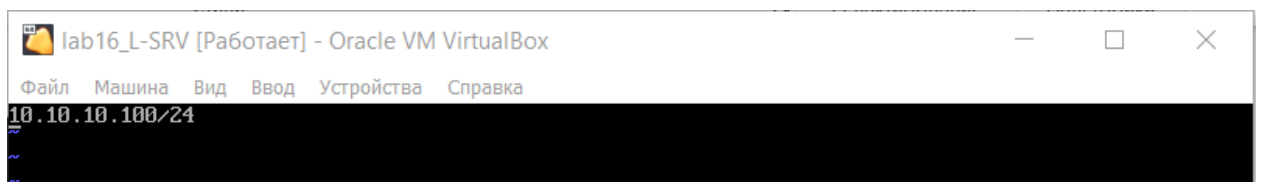
```
lab16_L-SRV [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
[root@srv ~]# hostnamectl set-hostname l-srv.au.team; exec bash
[root@l-srv ~]#
```

vim /etc/net/ifaces/ens19/options



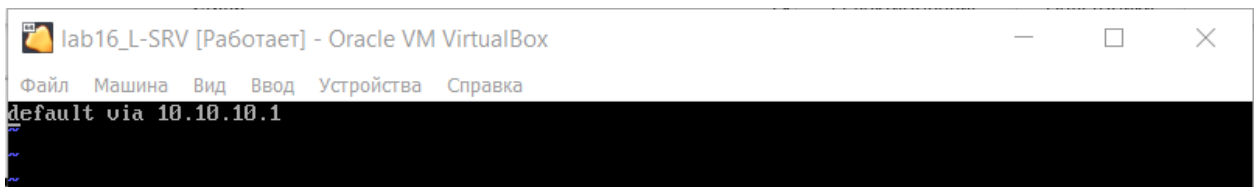
```
BOOTPROTO=static
TYPE=eth
NM_CONTROLLED=yes
DISABLED=yes
CONFIG_WIRELESS=no
SYSTEMD_BOOTPROTO=dhcp4
CONFIG_IPV4=yes
SYSTEMD_CONTROLLED=no
```

vim /etc/net/ifaces/ens19/ipv4address



```
lab16_L-SRV [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
10.10.10.100/24
```

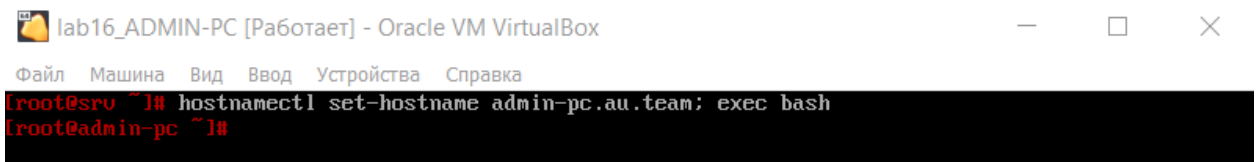
vim /etc/net/ifaces/ens19/ipv4route



```
lab16_L-SRV [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
default via 10.10.10.1
```

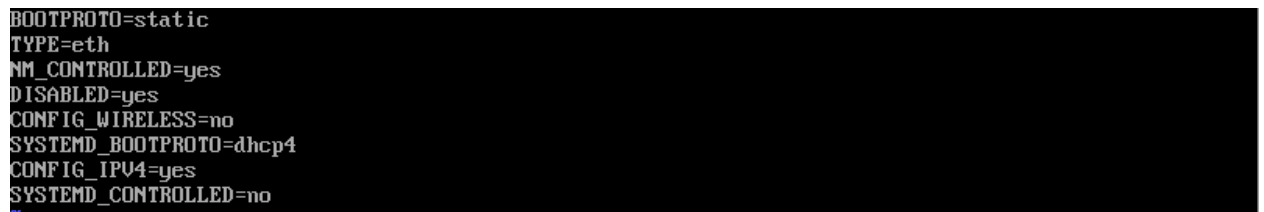
reboot

B) На ADMIN-PC



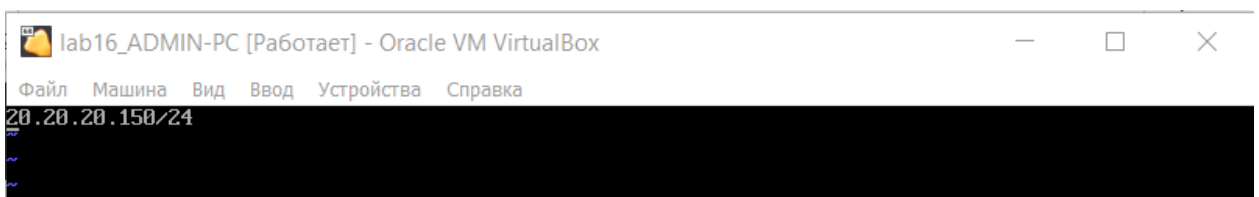
```
lab16_ADMIN-PC [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
[root@srv ~]# hostnamectl set-hostname admin-pc.au.team; exec bash
[root@admin-pc ~]#
```

vim /etc/net/ifaces/ens19/options



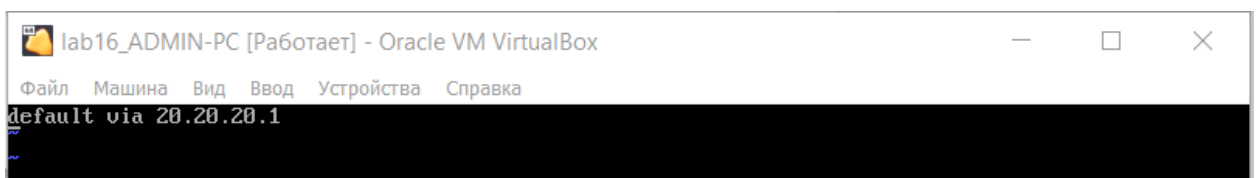
```
BOOTPROTO=static
TYPE=eth
NM_CONTROLLED=yes
DISABLED=yes
CONFIG_WIRELESS=no
SYSTEMD_BOOTPROTO=dhcp4
CONFIG_IPV4=yes
SYSTEMD_CONTROLLED=no
```

vim /etc/net/ifaces/ens19/ipv4address



```
lab16_ADMIN-PC [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
20.20.20.150/24
```

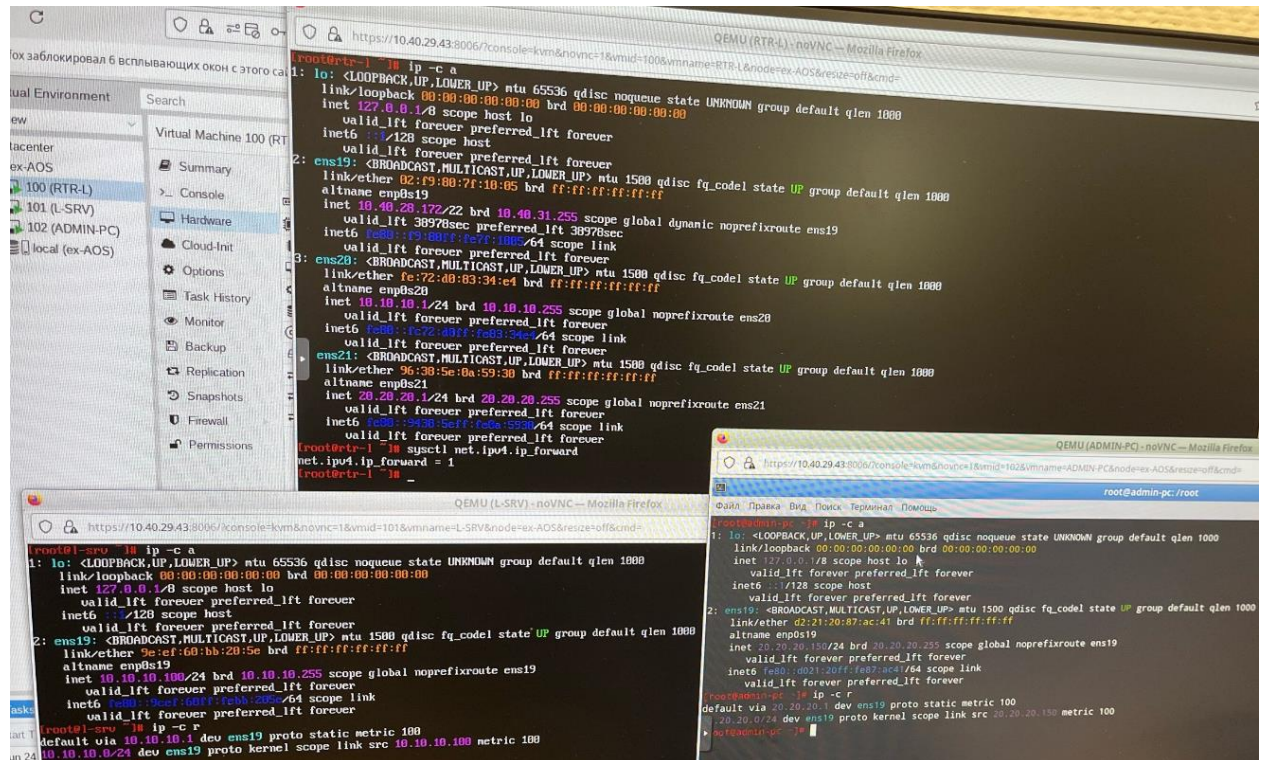
vim /etc/net/ifaces/ens19/ipv4route



```
lab16_ADMIN-PC [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
default via 20.20.20.1
```

reboot

## ДОЛЖНО ПОЛУЧИТЬСЯ



Проверить что все работает:

На L-SRV:

Ping 20.20.20.150

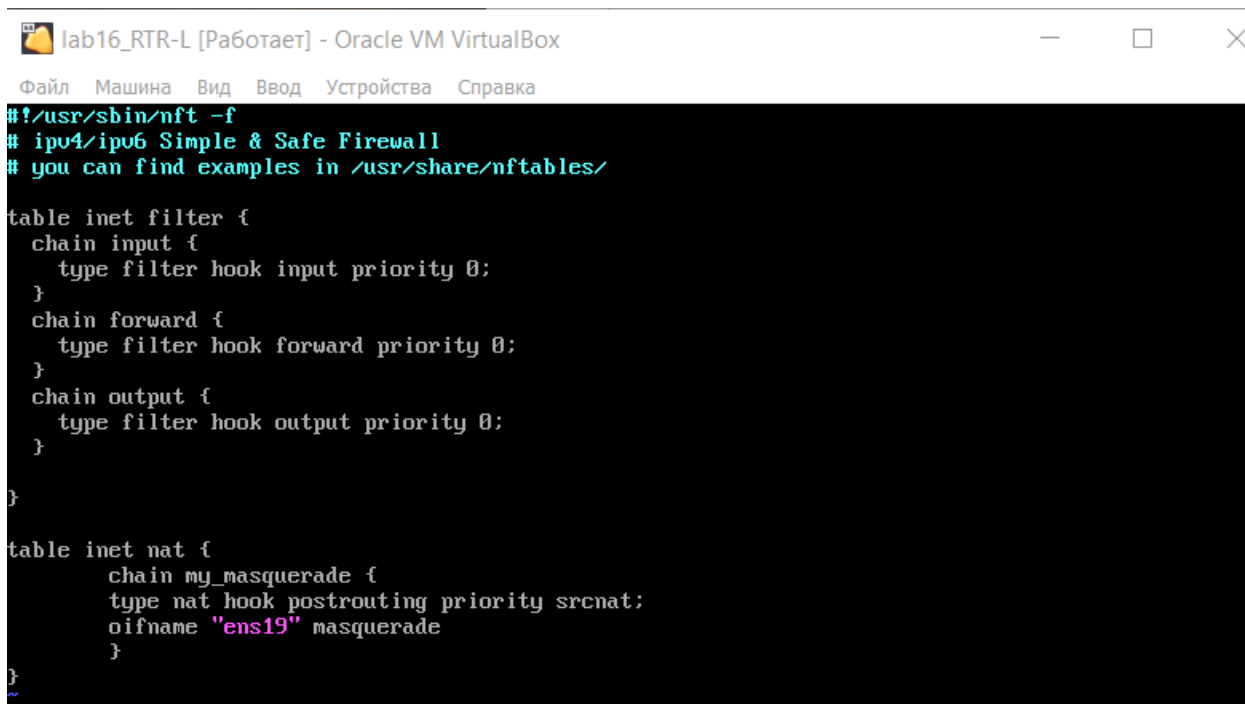
## ЗАДАНИЕ 1

### НА RTR-L

apt-get update

apt-get install nftables

vim /etc/nftables/nftables.nft



The screenshot shows a terminal window titled 'lab16\_RTR-L [Работает] - Oracle VM VirtualBox'. The terminal output displays the nftables configuration for a system. It starts with a comment indicating it's a simple and safe firewall. The configuration defines two tables: 'inet filter' and 'inet nat'. The 'inet filter' table has three chains: 'input', 'forward', and 'output', each with a filter hook and priority 0. The 'inet nat' table has a chain 'my\_masquerade' with a nat hook for postrouting, priority srcnat, and masquerade on the 'ens19' interface.

```
#!/usr/sbin/nft -f
# ipv4/ipv6 Simple & Safe Firewall
# you can find examples in /usr/share/nftables/

table inet filter {
    chain input {
        type filter hook input priority 0;
    }
    chain forward {
        type filter hook forward priority 0;
    }
    chain output {
        type filter hook output priority 0;
    }
}

table inet nat {
    chain my_masquerade {
        type nat hook postrouting priority srcnat;
        oifname "ens19" masquerade
    }
}
```

**systemctl enable --now nftables**

**systemctl status nftables**

**После чего на L-SRV и ADMIN-PC пытаемся получить доступ к интернету**

**(на них пробуем ping 8.8.8.8 и ping ya.ru пинги должны пойти )**

**Если делаем какие-то изменения, то systemctl restart nftables**

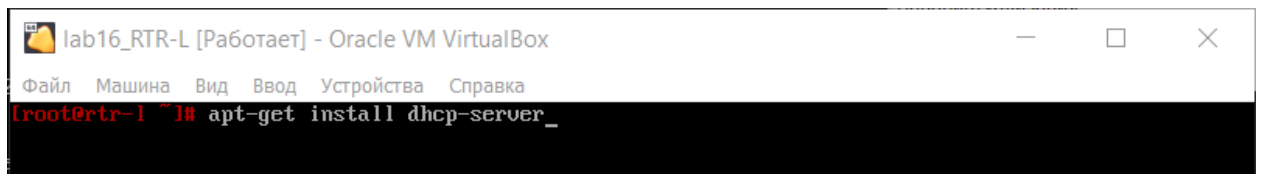
## ЗАДАНИЕ 2

### Настройте сервер DHCP на базе RTR-L.

- Создайте два пула для серверов (10.10.10.100-10.10.10.120) и клиентских ПК (20.20.20.150-20.20.20.200)
- Зарезервируйте выданный IP-адрес серверу L-SRV
- Адрес шлюза по умолчанию - адреса маршрутизаторов RTR-L
- Адрес DNS-сервера для машины ADMIN-PC - адрес сервера L-SRV.
- DNS-суффикс для офисов HQ и BR - au.team

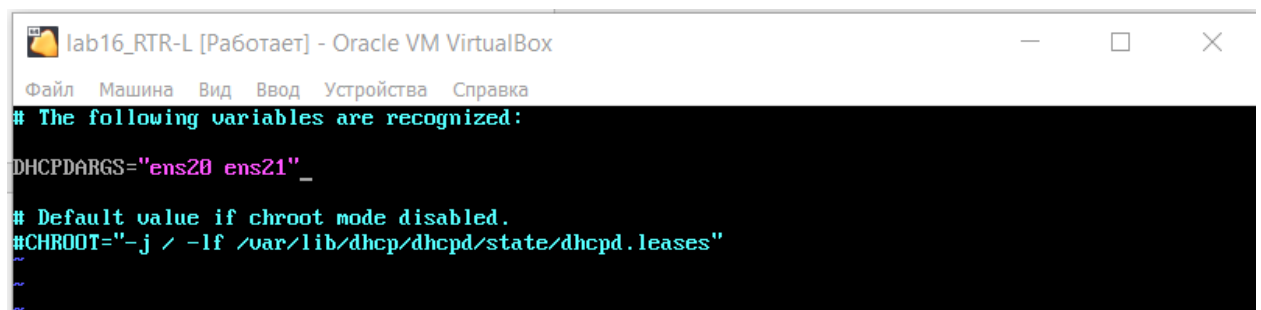
На RTR-L

apt-get update

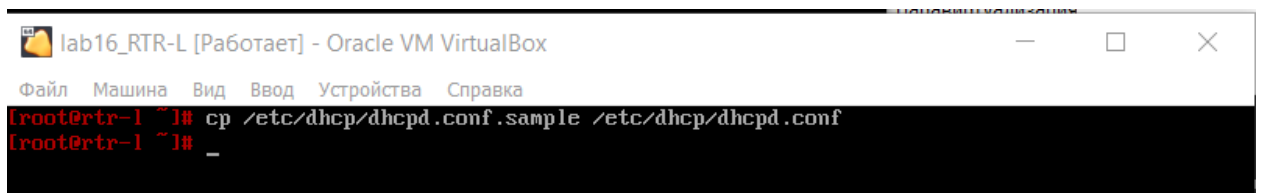


```
lab16_RTR-L [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
[root@rtr-l ~]# apt-get install dhcp-server_
```

vim /etc/sysconfig/dhcpd



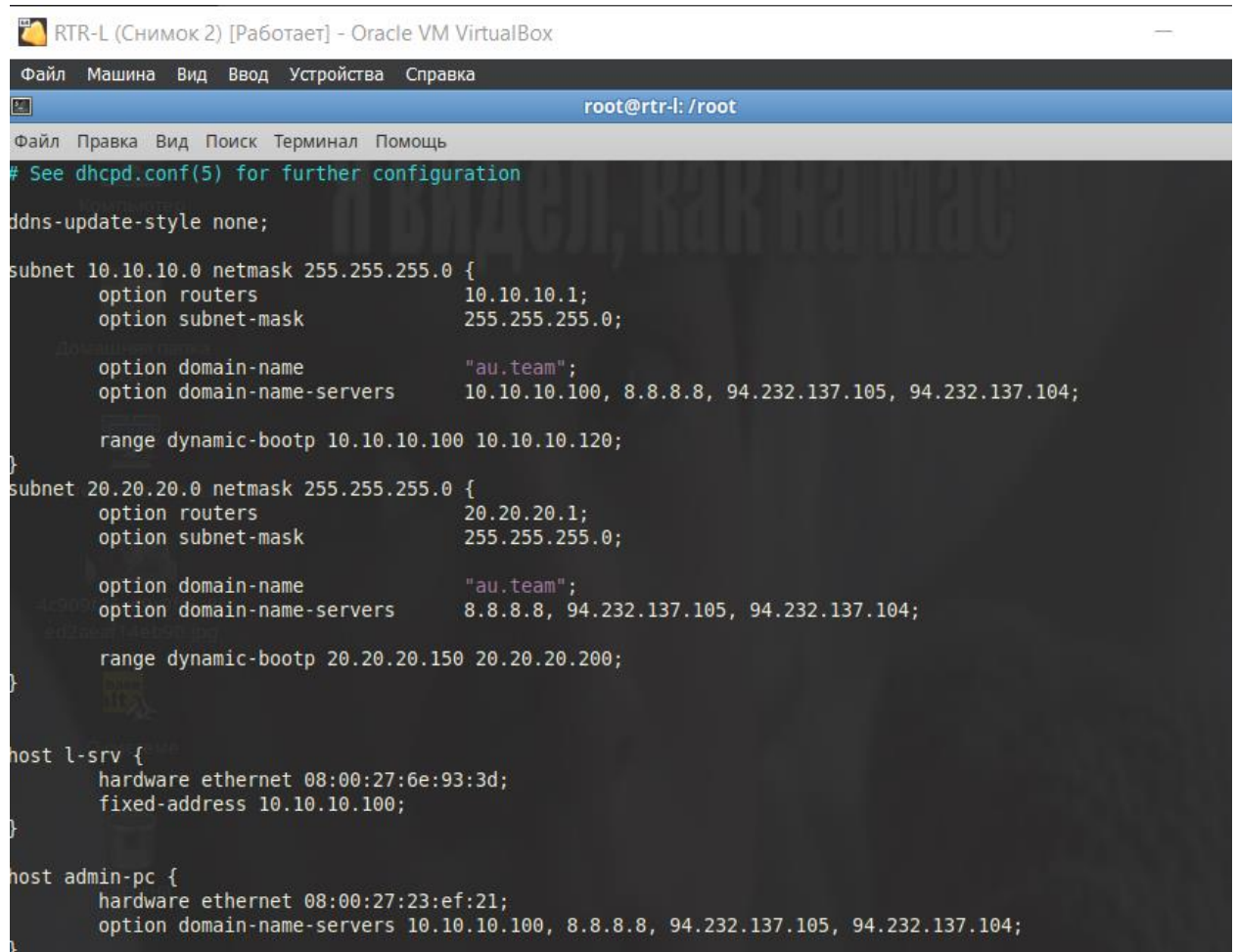
```
lab16_RTR-L [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
# The following variables are recognized:
DHCPDARGS="ens20 ens21"
# Default value if chroot mode disabled.
#CHROOT="-j / -lf /var/lib/dhcp/dhcpd/state/dhcpd.leases"
```



```
lab16_RTR-L [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
[root@rtr-l ~]# cp /etc/dhcp/dhcpd.conf.sample /etc/dhcp/dhcpd.conf
[root@rtr-l ~]#
```



## vim /etc/dhcp/dhcpd.conf



```
# See dhcpd.conf(5) for further configuration

ddns-update-style none;

subnet 10.10.10.0 netmask 255.255.255.0 {
    option routers                10.10.10.1;
    option subnet-mask            255.255.255.0;

    option domain-name            "au.team";
    option domain-name-servers    10.10.10.100, 8.8.8.8, 94.232.137.105, 94.232.137.104;

    range dynamic-bootp 10.10.10.100 10.10.10.120;
}

subnet 20.20.20.0 netmask 255.255.255.0 {
    option routers                20.20.20.1;
    option subnet-mask            255.255.255.0;

    option domain-name            "au.team";
    option domain-name-servers    8.8.8.8, 94.232.137.105, 94.232.137.104;

    range dynamic-bootp 20.20.20.150 20.20.20.200;
}

host l-srv {
    hardware ethernet 08:00:27:6e:93:3d;
    fixed-address 10.10.10.100;
}

host admin-pc {
    hardware ethernet 08:00:27:23:ef:21;
    option domain-name-servers 10.10.10.100, 8.8.8.8, 94.232.137.105, 94.232.137.104;
}
```

## ОТЛИЧИЯ ОТ РИСУНКА!

### А) БЛОК host l-srv

```
host l-srv {
```

```
    hardware ethernet XX:XX:XX:XX:XX:XX; # Замените на MAC-адрес L-  
SRV (на L-SRV через команду ip а смотрим mac-адрес для ens19)
```

```
    fixed-address 10.10.10.100;
```

```
}
```

### Б) БЛОК host admin-pc

```
host admin-pc {
```

```
    hardware ethernet YY:YY:YY:YY:YY:YY; # Замените на MAC-адрес  
ADMIN-PC (на ADMIN-PC через команду ip а смотрим mac-адрес для ens19)
```

```
option domain-name-servers 10.10.10.100, 94.232.137.105, 94.232.137.105;  
}
```

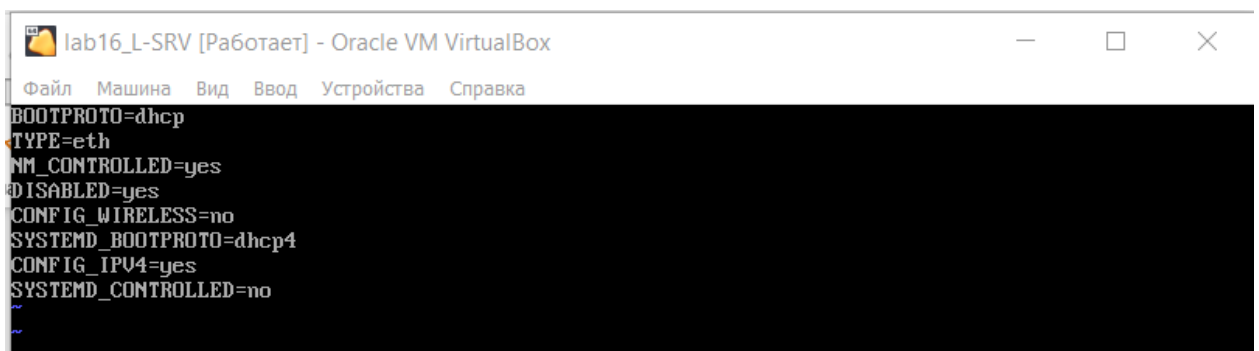
**systemctl enable --now dhcpcd**

**systemctl status dhcpcd** (если не работает, то команда **dhcpcd -t** покажет ошибки)

не забываем после изменений в конфигах **systemctl restart dhcpcd**

**На L-SRV:**

**vim /etc/net/iface/ens19/options**

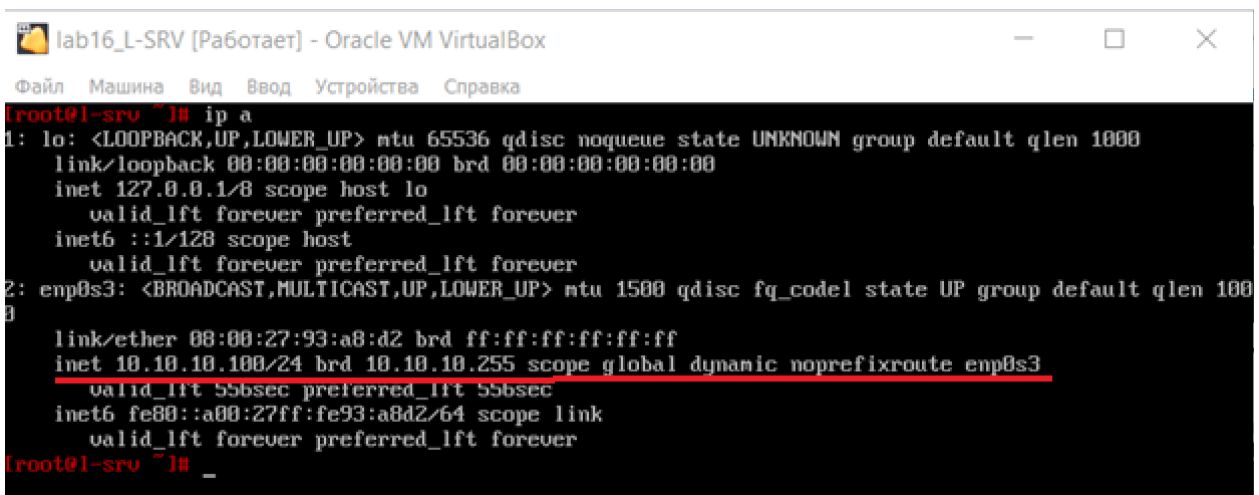


```
lab16_L-SRV [Работает] - Oracle VM VirtualBox  
Файл  Машина  Вид  Ввод  Устройства  Справка  
BOOTPROTO=dhcp  
TYPE=eth  
NM_CONTROLLED=yes  
DISABLED=yes  
CONFIG_WIRELESS=no  
SYSTEMD_BOOTPROTO=dhcp4  
CONFIG_IPV4=yes  
SYSTEMD_CONTROLLED=no
```

**Сохраняем и выходим**

**Для проверки пишем reboot** (перезагружаем машину)

**После перезагрузки пишем ip a**



```
lab16_L-SRV [Работает] - Oracle VM VirtualBox  
Файл  Машина  Вид  Ввод  Устройства  Справка  
[root@l-srv ~]# ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:93:a8:d2 brd ff:ff:ff:ff:ff:ff  
    inet 10.10.10.100/24 brd 10.10.10.255 scope global dynamic noprefixroute enp0s3  
        valid_lft 55bsec preferred_lft 55bsec  
    inet6 fe80::a00:27ff:fe93:a8d2/64 scope link  
        valid_lft forever preferred_lft forever  
[root@l-srv ~]# _
```

(понятное дело на экзамене будет не enp0s3 а ens19)

**На ADMIN-PC:**

**vim /etc/net/iface/ens19/options**

```
lab16_ADMIN-PC [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
BOOTPROTO=dhcp
TYPE=eth
NM_CONTROLLED=yes
DISABLED=yes
CONFIG_WIRELESS=no
SYSTEMD_BOOTPROTO=dhcp4
CONFIG_IPV4=yes
SYSTEMD_CONTROLLED=no
..
..
..
```

**Сохраняем и выходим**

**Для проверки пишем reboot (перезагружаем машину)**

**После перезагрузки пишем ip a**

```
lab16_ADMIN-PC [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
[root@admin-pc ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:cf:37:a8 brd ff:ff:ff:ff:ff:ff
    inet 20.20.20.150/24 brd 20.20.20.255 scope global dynamic noprefixroute enp0s3
        valid_lft 564sec preferred_lft 564sec
    inet6 fe80::a00:27ff:fe3f:37a8/64 scope link
        valid_lft forever preferred_lft forever
[root@admin-pc ~]#
```

**(понятное дело на экзамене будет не enp0s3 а ens19)**

### ЗАДАНИЕ 3

Настройте доменный контроллер Samba на машине L-SRV. Имя домена au.team.

- Создайте 15 пользователей для офиса left (группа left), имена пользователей формата user№.userl.
- Создайте 5 пользователей группы администратор, имена пользователей формата user№.admin.
- Пользователи группы left и admin имеют право аутентифицироваться на любом клиентском ПК (ADMIN-PC).
- Пользователи группы left должны иметь возможность повышать привилегии для выполнения ограниченного набора команд: cat, grep, id.
- Пользователи группы admin должны иметь возможность повышать привилегии без ввода пароля.
- Для всех пользователей домена должны быть реализованы общие каталоги по пути /mnt/Adsamba. Должно происходить автомонтирование

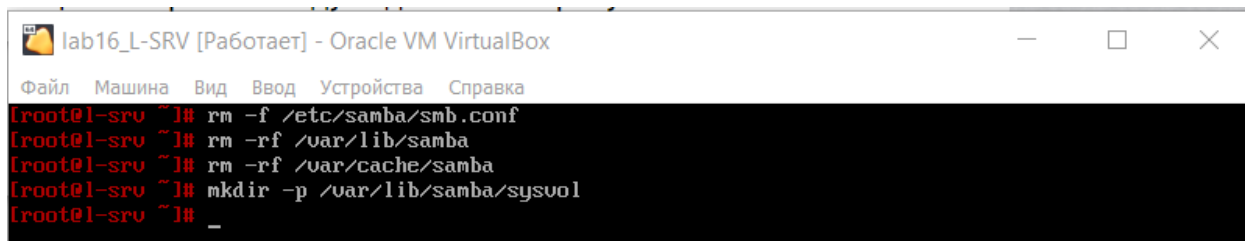
#### На L-SRV:

```
$ apt-get install alterator-fbi
```

```
$ systemctl start alteratord ahttpd
```

```
$ systemctl enable alteratord ahttpd
```

```
$ apt-get install alterator-net-domain task-samba-dc krb5-kdc
```



```
lab16_L-SRV [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
[root@l-srv ~]# rm -f /etc/samba/smb.conf
[root@l-srv ~]# rm -rf /var/lib/samba
[root@l-srv ~]# rm -rf /var/cache/samba
[root@l-srv ~]# mkdir -p /var/lib/samba/sysvol
[root@l-srv ~]# _
```



```
lab16_L-SRV [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
[root@l-srv ~]# samba-tool domain provision --realm=au.team --domain=AU --adminpass='Pa$$word' --dns-backend=SAMBA_INTERNAL --server-role=dc --use-rfc2307
```

**ВАЖНО** добавить ключ `--option="dns forwarder=94.232.137.104"`

`systemctl enable --now samba`

`systemctl status samba (failed)`

**Вылезали одни ошибки, перезагрузил машину при помощи reboot**

`systemctl status samba (всё норм)`

```
lab16_L-SRV [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
[root@l-srv ~]# samba-tool domain info 127.0.0.1
Forest           : au.team
Domain           : au.team
Netbios domain   : AU
DC name          : l-srv.au.team
DC netbios name  : L-SRV
Server site      : Default-First-Site-Name
Client site      : Default-First-Site-Name
[root@l-srv ~]#
```

```
lab16_L-SRV [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
[root@l-srv ~]# samba-tool group add left
Added group left
[root@l-srv ~]# samba-tool group add admin
Added group admin
[root@l-srv ~]# _
```

**Пишем скрипт для создания пользователей:**

**vim script.sh**

```
lab16_L-SRV [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
#!/bin/bash

for i in {1..15}; do
    samba-tool user create user${i}.user1 "Pa$$word"
    samba-tool group addmembers left user${i}.user1
done

for i in {1..5}; do
    samba-tool user create user${i}.admin "Pa$$word"
    samba-tool group addmembers admin user${i}.admin
done
```

**Только либо пароль без долларов пишем либо кавычки одинарные иначе не сработает нормально**

**chmod +x script.sh**

**./script.sh**

**Проверка, что пользователи создались:**

```
lab16_L-SRV [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
[root@l-srv ~]# pdbedit -L | grep user1
user1.user1:4294967295:
user2.user1:4294967295:
user13.user1:4294967295:
user3.user1:4294967295:
user8.user1:4294967295:
user12.user1:4294967295:
user9.user1:4294967295:
user11.user1:4294967295:
user5.user1:4294967295:
user10.user1:4294967295:
user7.user1:4294967295:
user14.user1:4294967295:
user6.user1:4294967295:
user4.user1:4294967295:
user15.user1:4294967295:
[root@l-srv ~]# pdbedit -L | grep admin
user1.admin:4294967295:
user3.admin:4294967295:
user4.admin:4294967295:
user5.admin:4294967295:
user2.admin:4294967295:
[root@l-srv ~]# _
```

## Проверка принадлежности пользователей группам:

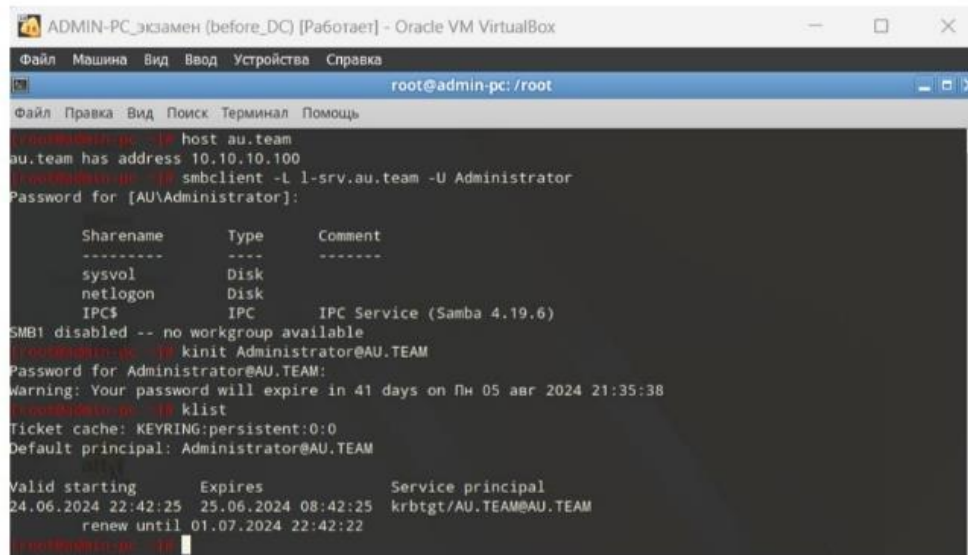
```
[root@l-srv ~]# samba-tool group listmembers left
user11.user1
user10.user1
user3.user1
user7.user1
user5.user1
user2.user1
user9.user1
user4.user1
user6.user1
user13.user1
user1.user1
user15.user1
user14.user1
user12.user1
user8.user1
[root@l-srv ~]# samba-tool group listmembers admin
user2.admin
user3.admin
user5.admin
user1.admin
user4.admin
```

## ADMIN-PC:

**apt-get install samba-client krb5-kdc**

**в) Необходимо ввести admin-pc в домен =>**

что-то вроде предварительной проверки...



```
ADMIN-PC_экзамен (before_DC) [Работает] - Oracle VM VirtualBox
root@admin-pc: /root

[root@admin-pc: ~]# host au.team
au.team has address 10.10.10.100
[root@admin-pc: ~]# smbclient -L 1-srv.au.team -U Administrator
Password for [AU\Administrator]:

      Sharename      Type      Comment
      -----
      sysvol          Disk
      netlogon         Disk
      IPC$             IPC       IPC Service (Samba 4.19.6)
SMB1 disabled -- no workgroup available
[root@admin-pc: ~]# kinit Administrator@AU.TEAM
Password for Administrator@AU.TEAM:
warning: Your password will expire in 41 days on Пн 05 авг 2024 21:35:38
[root@admin-pc: ~]# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: Administrator@AU.TEAM

Valid starting     Expires            Service principal
24.06.2024 22:42:25  25.06.2024 08:42:25  krbtgt/AU.TEAM@AU.TEAM
renew until        01.07.2024 22:42:22
```

**apt-get update**

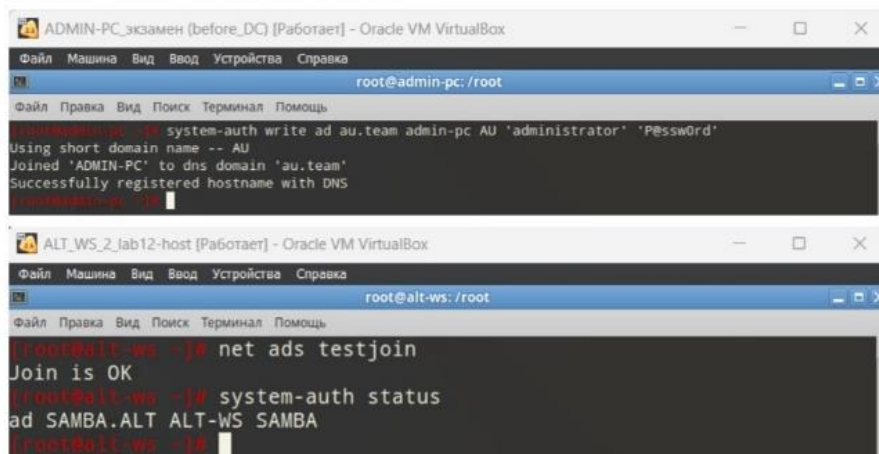
**apt-get install -y task-auth-ad-sssd**

После чего выполняем следующую команду:

**apt-get update**

**apt-get install -y task-auth-ad-sssd**

После чего выполняем следующую команду:



```
ADMIN-PC_экзамен (before_DC) [Работает] - Oracle VM VirtualBox
root@admin-pc: /root

[root@admin-pc: ~]# system-auth write ad au.team admin-pc AU 'administrator' 'Pesswörd'
Using short domain name -- AU
Joined 'ADMIN-PC' to dns domain 'au.team'
Successfully registered hostname with DNS
[root@admin-pc: ~]#

ALT_WS_2_lab12-host [Работает] - Oracle VM VirtualBox
root@alt-ws: /root

[root@alt-ws: ~]# net ads testjoin
Join is OK
[root@alt-ws: ~]# system-auth status
ad SAMBA.ALT ALT-WS SAMBA
[root@alt-ws: ~]#
```

**reboot**

Теперь под созданными пользователями можно будет войти!

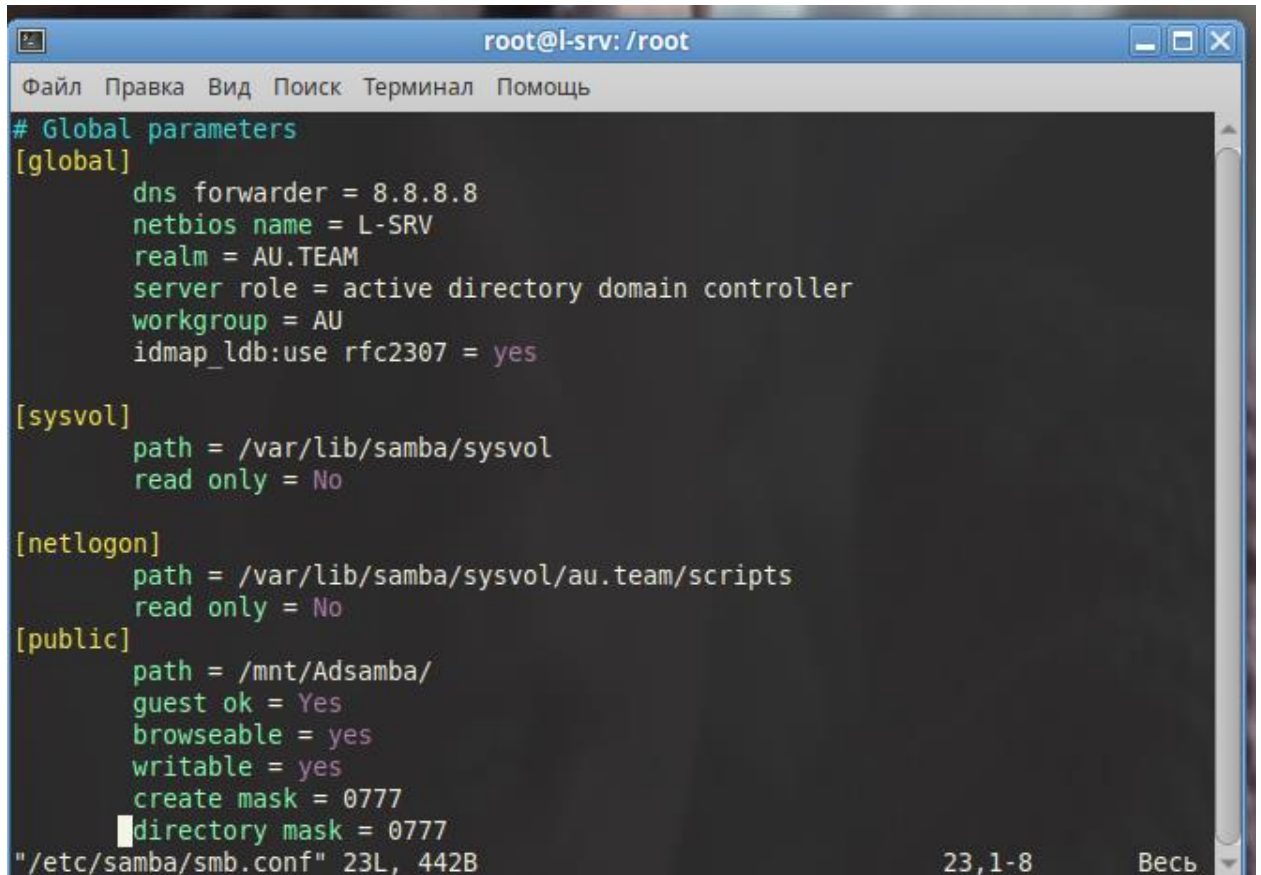


На L-SRV:

```
mkdir /mnt/Adsamba/
```

```
chmod 777 /Adsamba/
```

```
vim /etc/samba/smb.conf
```



```
root@l-srv: /root
Файл Правка Вид Поиск Терминал Помощь
# Global parameters
[global]
    dns forwarder = 8.8.8.8
    netbios name = L-SRV
    realm = AU.TEAM
    server role = active directory domain controller
    workgroup = AU
    idmap_ldb:use rfc2307 = yes

[sysvol]
    path = /var/lib/samba/sysvol
    read only = No

[netlogon]
    path = /var/lib/samba/sysvol/au.team/scripts
    read only = No

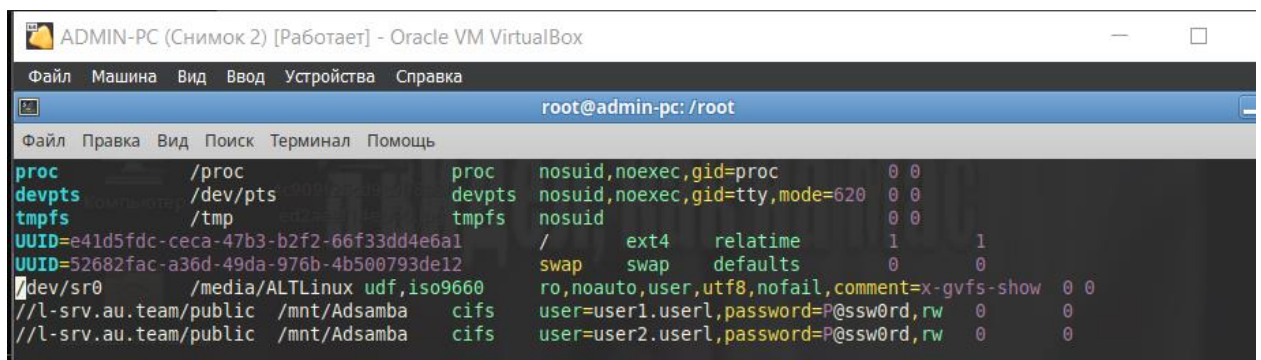
[public]
    path = /mnt/Adsamba/
    guest ok = Yes
    browseable = yes
    writable = yes
    create mask = 0777
    directory mask = 0777
"/etc/samba/smb.conf" 23L, 442B 23,1-8 Весь
```

```
systemctl restart samba
```

На ADMIN-PC:

Заходим под обычного user

```
vim /etc/fstab
```



```
ADMIN-PC (Снимок 2) [Работает] - Oracle VM VirtualBox
Файл Машина Вид Ввод Устройства Справка
root@admin-pc: /root
Файл Правка Вид Поиск Терминал Помощь
proc /proc proc nosuid,noexec,gid=proc 0 0
devpts /dev/pts devpts nosuid,noexec,gid=tty,mode=620 0 0
tmpfs /tmp tmpfs nosuid 0 0
UUID=e41d5fdc-ceca-47b3-b2f2-66f33dd4e6a1 / ext4 relatime 1 1
UUID=52682fac-a36d-49da-976b-4b500793de12 swap swap defaults 0 0
/dev/sr0 /media/ALTlinux udf,iso9660 ro,noauto,user=utf8,nofail,comment=x-gvfs-show 0 0
//l-srv.au.team/public /mnt/Adsamba cifs user=user1.user1,password=P@ssw0rd,rw 0 0
//l-srv.au.team/public /mnt/Adsamba cifs user=user2.user1,password=P@ssw0rd,rw 0 0
```

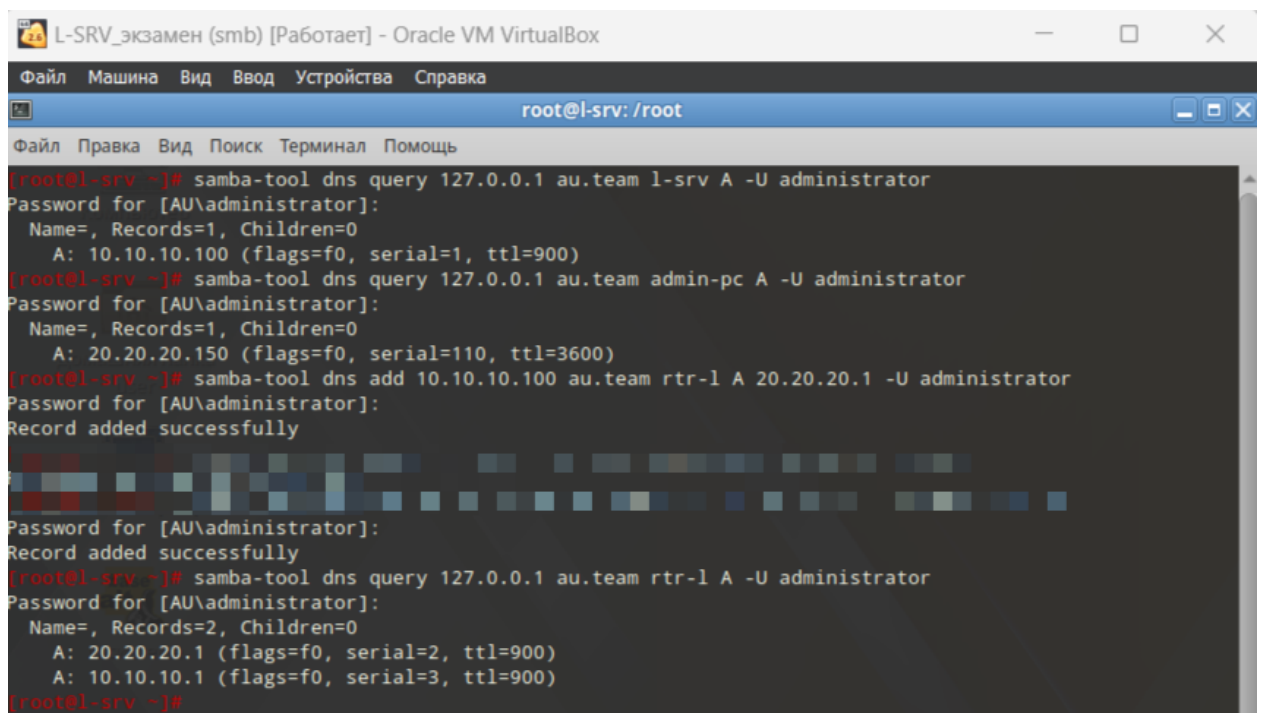
И так далее для всех пользователей...



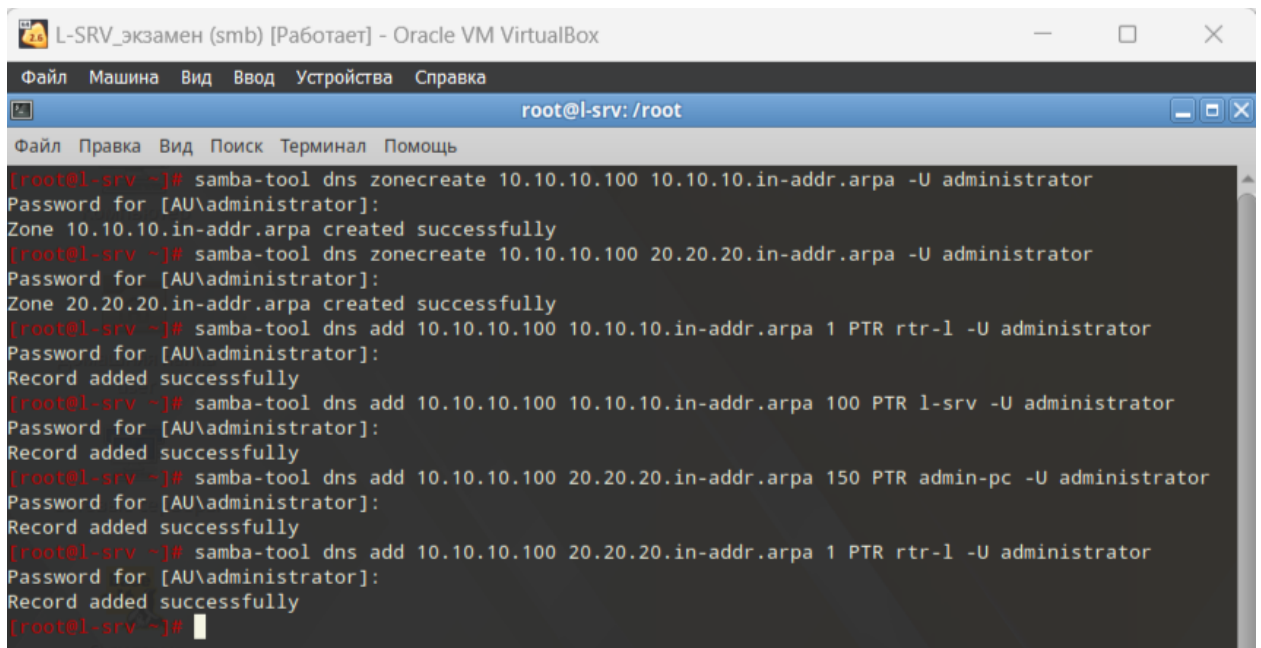
#### 4. Настройка DNS для офиса left.

- Основной DNS-сервер реализован на доменном контроллере.
- Для всех устройств используется доменное имя au.team.
- Для всех устройств двух офисов необходимо создать записи A и PTR.
- В качестве DNS сервера пересылки используйте сервера 94.232.137.104

Машина	Запись A
L-SRV	l-srv.au.team
ADMIN-PC	admin-pc.au.team
RTR-L	rtr-l.au.team



```
L-SRV_экзамен (smb) [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
root@l-srv: /root
Файл  Правка  Вид  Поиск  Терминал  Помощь
[root@l-srv ~]# samba-tool dns query 127.0.0.1 au.team l-srv A -U administrator
Password for [AU\administrator]:
Name=, Records=1, Children=0
A: 10.10.10.100 (flags=f0, serial=1, ttl=900)
[root@l-srv ~]# samba-tool dns query 127.0.0.1 au.team admin-pc A -U administrator
Password for [AU\administrator]:
Name=, Records=1, Children=0
A: 20.20.20.150 (flags=f0, serial=110, ttl=3600)
[root@l-srv ~]# samba-tool dns add 10.10.10.100 au.team rtr-l A 20.20.20.1 -U administrator
Password for [AU\administrator]:
Record added successfully
Password for [AU\administrator]:
Record added successfully
[root@l-srv ~]# samba-tool dns query 127.0.0.1 au.team rtr-l A -U administrator
Password for [AU\administrator]:
Name=, Records=2, Children=0
A: 20.20.20.1 (flags=f0, serial=2, ttl=900)
A: 10.10.10.1 (flags=f0, serial=3, ttl=900)
[root@l-srv ~]#
```



The screenshot shows a terminal window titled "L-SRV\_экзамен (smb) [Работает] - Oracle VM VirtualBox". The terminal is running as root on a machine named l-srv. The user has executed several commands to configure Samba DNS. The commands and their outputs are as follows:

```
[root@l-srv ~]# samba-tool dns zonecreate 10.10.10.100 10.10.10.in-addr.arpa -U administrator
Password for [AU\administrator]:
Zone 10.10.10.in-addr.arpa created successfully
[root@l-srv ~]# samba-tool dns zonecreate 10.10.10.100 20.20.20.in-addr.arpa -U administrator
Password for [AU\administrator]:
Zone 20.20.20.in-addr.arpa created successfully
[root@l-srv ~]# samba-tool dns add 10.10.10.100 10.10.10.in-addr.arpa 1 PTR rtr-1 -U administrator
Password for [AU\administrator]:
Record added successfully
[root@l-srv ~]# samba-tool dns add 10.10.10.100 10.10.10.in-addr.arpa 100 PTR l-srv -U administrator
Password for [AU\administrator]:
Record added successfully
[root@l-srv ~]# samba-tool dns add 10.10.10.100 20.20.20.in-addr.arpa 150 PTR admin-pc -U administrator
Password for [AU\administrator]:
Record added successfully
[root@l-srv ~]# samba-tool dns add 10.10.10.100 20.20.20.in-addr.arpa 1 PTR rtr-1 -U administrator
Password for [AU\administrator]:
Record added successfully
[root@l-srv ~]#
```

PTR Записи скорее всего нужно прописывать так: PTR rtr-1.au.team

## 5. Настройка межсетевого экрана на RTR-L

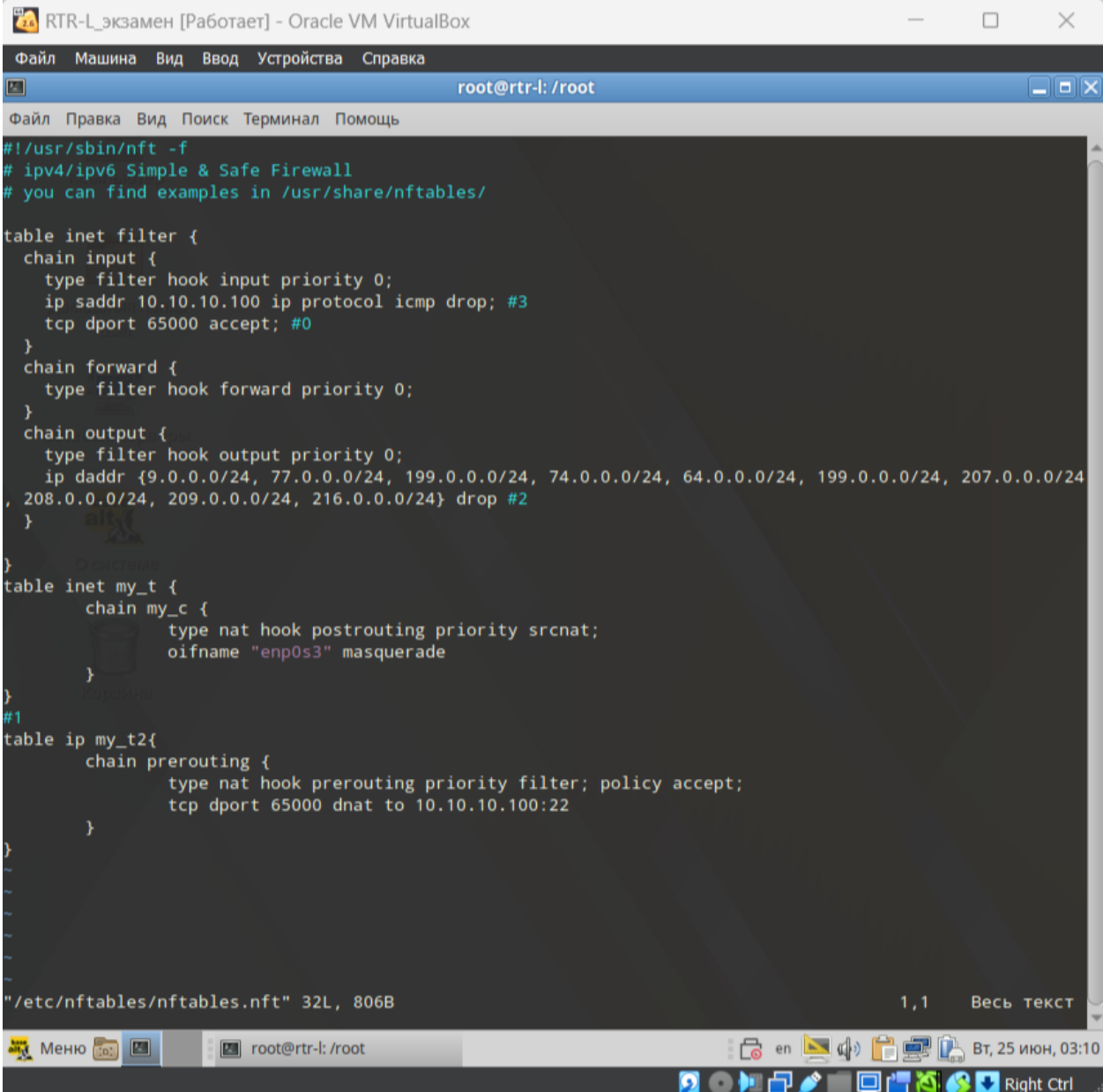
- Реализуйте подключение к серверу по SSH с ADMIN-PC. Используйте порт 65000 на маршрутизаторе RTR-L
- Заблокируйте доступ к youtube
- Запретите ICMP трафик с L-SRV на RTR-L

`apt-get update && apt-get install openssh-server`

`vim /etc/openssh/sshd_config (Port 22 и PasswordAuthentication yes)`

`systemctl start sshd`

`systemctl enable sshd`



The screenshot shows a terminal window titled "RTR-L\_экзамен [Работает] - Oracle VM VirtualBox". The terminal prompt is "root@rtr-l: /root". The user has entered the following nftables configuration:

```
#!/usr/sbin/nft -f
# ipv4/ipv6 Simple & Safe Firewall
# you can find examples in /usr/share/nftables/

table inet filter {
    chain input {
        type filter hook input priority 0;
        ip saddr 10.10.10.100 ip protocol icmp drop; #3
        tcp dport 65000 accept; #0
    }
    chain forward {
        type filter hook forward priority 0;
    }
    chain output {
        type filter hook output priority 0;
        ip daddr {9.0.0.0/24, 77.0.0.0/24, 199.0.0.0/24, 74.0.0.0/24, 64.0.0.0/24, 199.0.0.0/24, 207.0.0.0/24, 208.0.0.0/24, 209.0.0.0/24, 216.0.0.0/24} drop #2
    }
}

table inet my_t {
    chain my_c {
        type nat hook postrouting priority srcnat;
        oifname "enp0s3" masquerade
    }
}

#1
table ip my_t2 {
    chain prerouting {
        type nat hook prerouting priority filter; policy accept;
        tcp dport 65000 dnat to 10.10.10.100:22
    }
}

"/etc/nftables/nftables.nft" 32L, 806B
```

The terminal window has a menu bar with "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". The status bar at the bottom shows "root@rtr-l: /root", a language selector set to "en", and the date/time "Вт, 25 июн, 03:10".