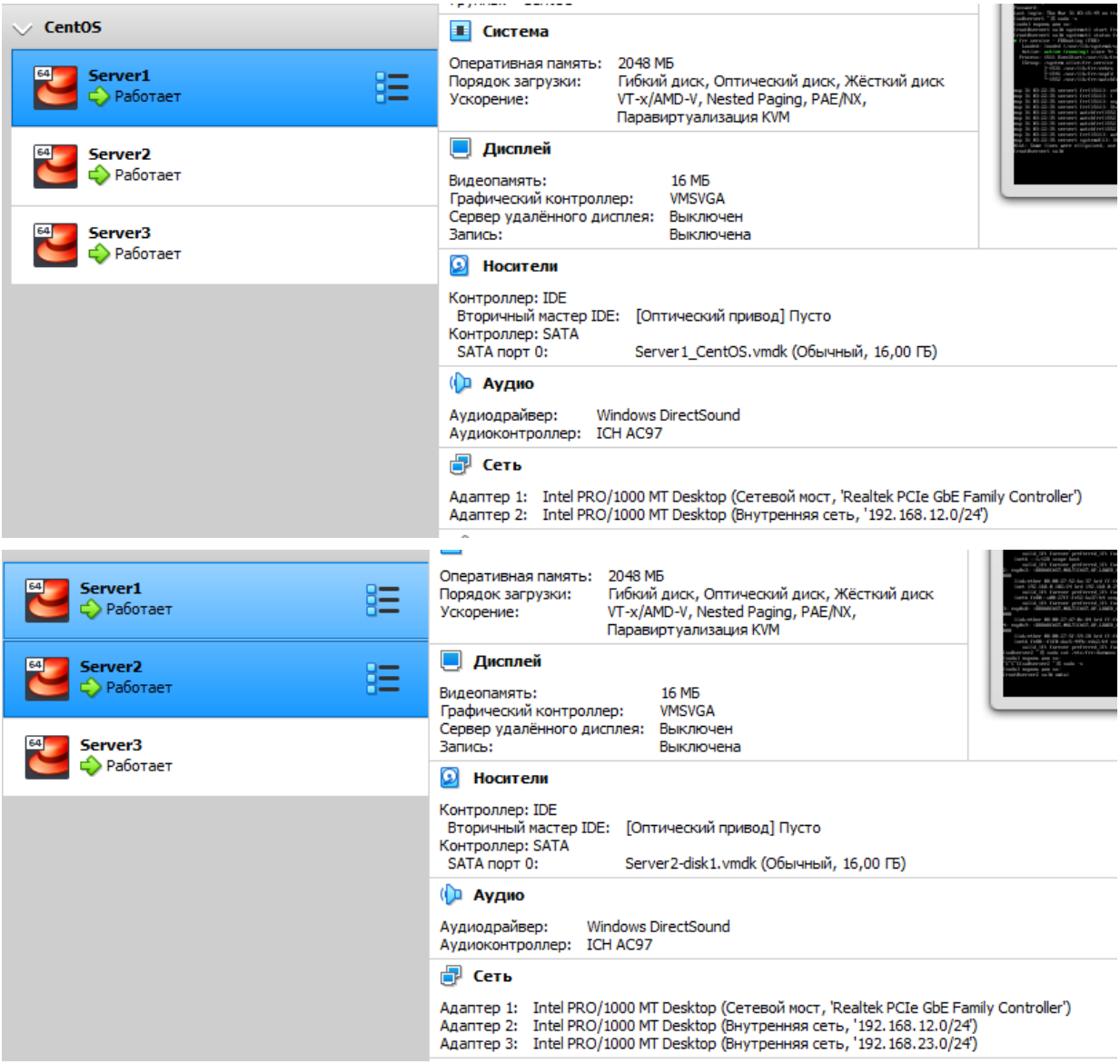
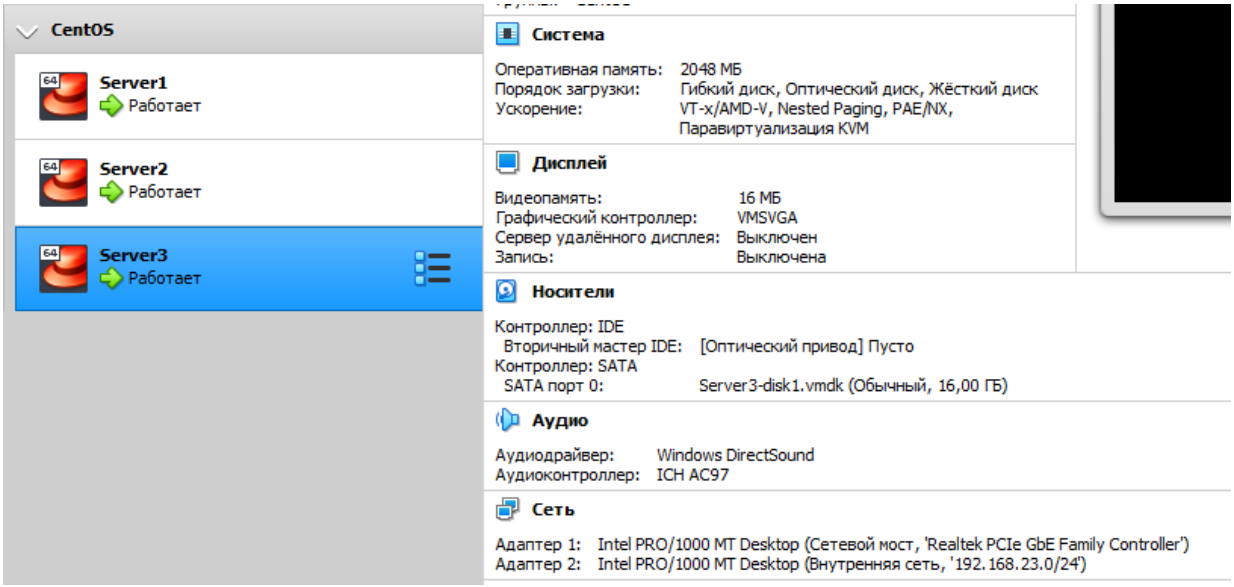
Основные сервисы на Linux для предприятия

Урок 2. Роутер на Linux, обеспечение безопасности

Домашняя работа (Тетерин Илья)

1. Собрать схему из трёх серверов. Два сервера должны иметь как минимум 3 сетевых адаптера. Один сервер должен иметь 2 сетевых адаптера.





2. Первый интерфейс на каждой виртуальной машине имеет режим подключения bridge (сетевой мост) или nat для предоставления доступа в интернет и по ssh из родительской операционной системы. В этом примере используется bridge, так как есть роутер провайдера, который раздает IP-адреса.

   Выполнено

3. Все последующие интерфейсы между серверами организуют отдельные изолированные сегменты. Режим подключения — LAN Segment. Делается это, чтобы изолировать коммуникацию между сетевыми адаптерами устройств.

   Выполнено

4. Настроить любой из интерфейсов между server1 и server2. Назначить на него адреса из подсети 192.168.12.0/24. Второй интерфейс между ними остается отключенным и в этом задании не участвует.

   Выполнено

5. Настроить подсеть между server2 и server3 с адресами из подсети 192.168.23.0/24.

   Выполнено

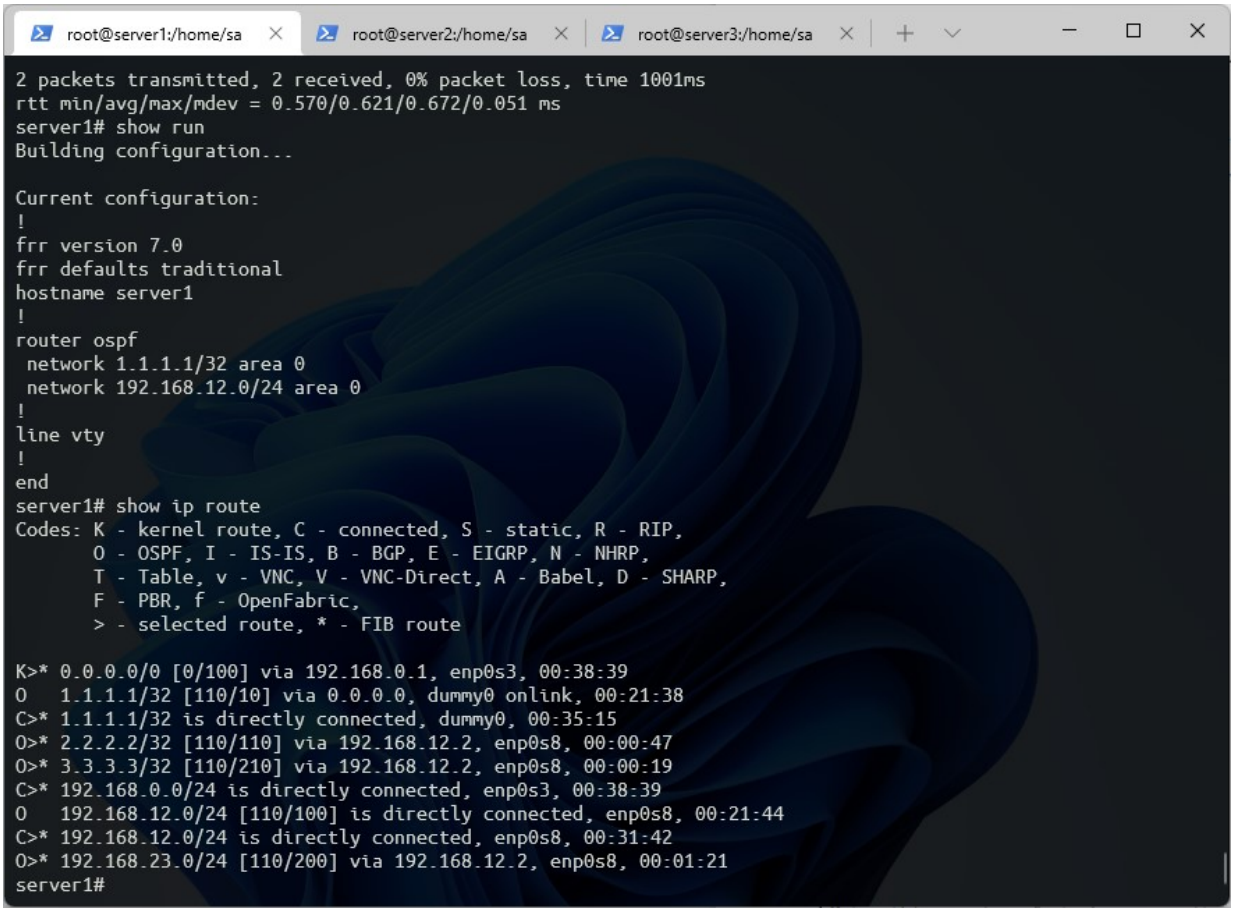
6. На каждом из серверов поднять dummy0-интерфейс и назначить на него ip-адрес 1.1.1.1/32, 2.2.2.2/32, 3.3.3.3/32 соответственно.

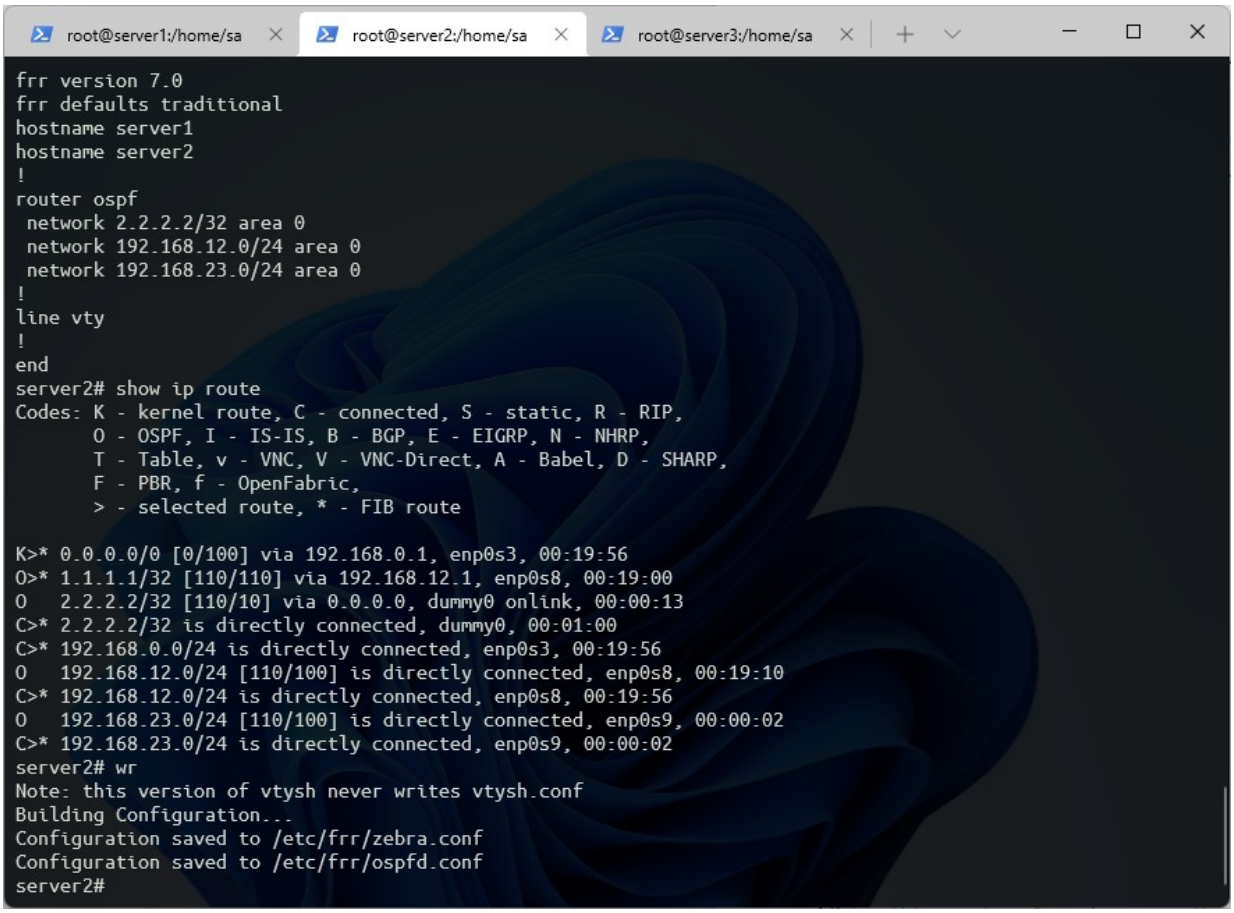
```
[root@server1 sa]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:a1:5f:f0 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.101/24 brd 192.168.0.255 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fea1:5ff0/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:3c:cf:92 brd ff:ff:ff:ff:ff:ff
    inet 192.168.12.1/24 scope global enp0s8
       valid_lft forever preferred_lft forever
4: dummy0: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
    link/ether 6a:cb:13:78:c0:ef brd ff:ff:ff:ff:ff:ff
    inet 1.1.1.1/32 scope global dummy0
       valid_lft forever preferred_lft forever
    inet6 fe80::68cb:13ff:fe78:c0ef/64 scope link
       valid_lft forever preferred_lft forever
```

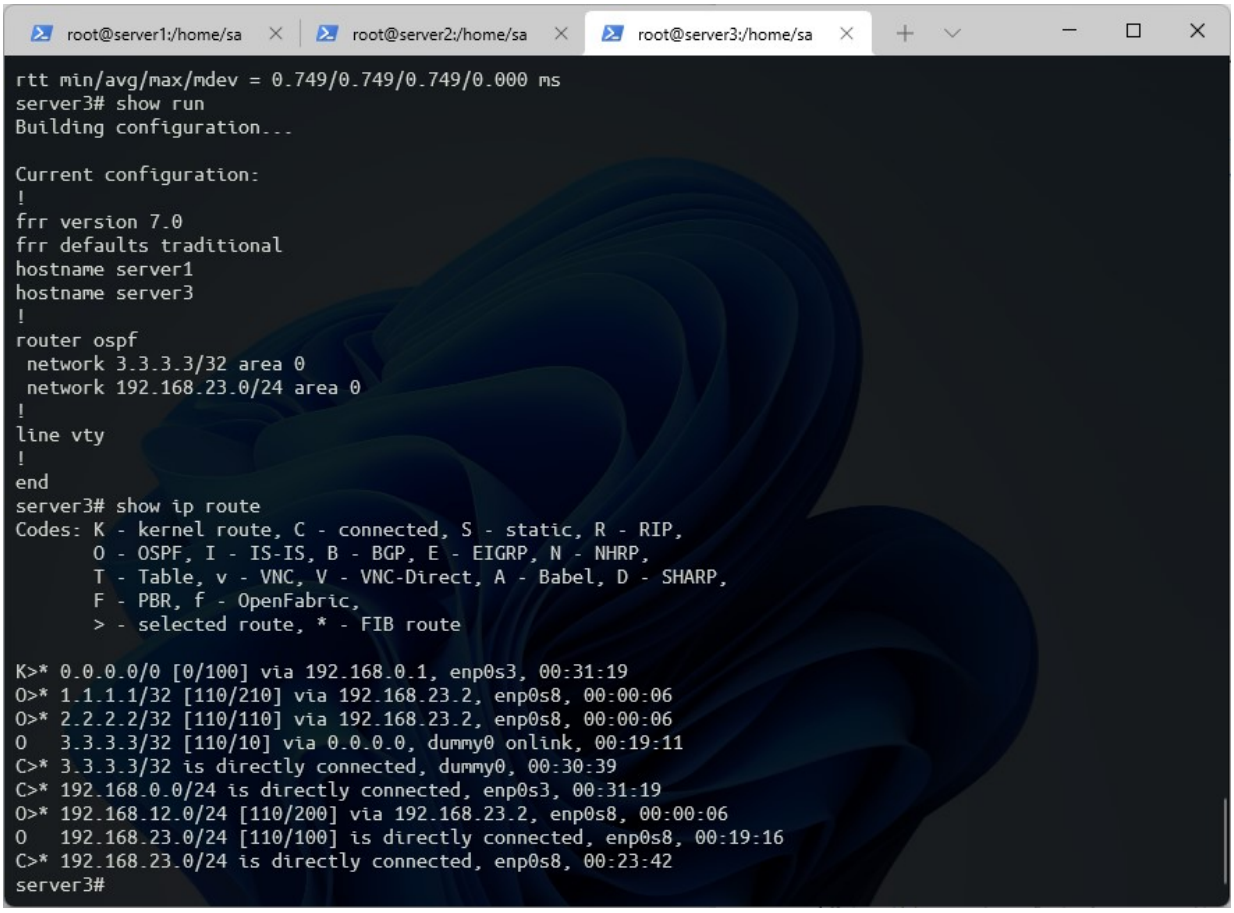
```
[root@server2 sa]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:52:ba:37 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.102/24 brd 192.168.0.255 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe52:ba37/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:d7:0c:84 brd ff:ff:ff:ff:ff:ff
    inet 192.168.12.2/24 brd 192.168.12.255 scope global noprefixroute enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed7:c84/64 scope link
       valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:5f:59:28 brd ff:ff:ff:ff:ff:ff
5: dummy0: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
    link/ether 96:47:39:b5:87:bc brd ff:ff:ff:ff:ff:ff
    inet 2.2.2.2/32 scope global dummy0
       valid_lft forever preferred_lft forever
    inet6 fe80::9447:39ff:feb5:87bc/64 scope link
       valid_lft forever preferred_lft forever
```

```
[root@server3 sa]# 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 pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:18:40:1c brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.103/24 brd 192.168.0.255 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe18:401c/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:0b:42:c3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.23.3/24 brd 192.168.23.255 scope global noprefixroute enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe0b:42c3/64 scope link
       valid_lft forever preferred_lft forever
4: dummy0: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
    link/ether 8e:3c:2d:0f:f3:bc brd ff:ff:ff:ff:ff:ff
    inet 3.3.3.3/32 scope global dummy0
       valid_lft forever preferred_lft forever
    inet6 fe80::8c3c:2dff:fe0f:f3bc/64 scope link
       valid_lft forever preferred_lft forever
```

7. На серверах установить пакет frr и настроить на роутерах ospf, добавив подсети 192.168.12.0/24, 192.168.23.0/24, 1.1.1.1/32, 2.2.2.2/32, 3.3.3.3/32 в area 0.







8. Убедиться, что маршрутизация работает, и с server1 вы должны пинговать 3.3.3.3 адрес на server3. Убедитесь, что нужный тип трафика разрешен в firewalld и что трафик не улетает в интернет при помощи traceroute.

9. На server3 создайте 2 папки nfs_1 и nfs_2, добавьте их в export.

```
yum install nfs-utils -y
systemctl enable rpcbind nfs-server
systemctl start rpcbind nfs-server
mkdir /usr/nfs_1
mkdir /usr/nfs_2
chmod -R 777 /usr/nfs_2
chmod -R 777 /usr/nfs_1
cat > /etc/exports << _EOL_
/usr/nfs_1 192.168.12.0/24(rw,sync,no_root_squash,no_all_squash)
/usr/nfs_2 192.168.12.0/24(rw,sync,no_root_squash,no_all_squash)
_EOL_
exportfs -r
firewall-cmd --permanent --zone=public --add-service=nfs
firewall-cmd --permanent --zone=public --add-service=mountd
```

```
firewall-cmd --permanent --zone=public --add-service=rpc-bind
firewall-cmd --reload
```

10. Убедитесь, что только server1 может их примонтировать.

```
yum install nfs-utils -y
systemctl start rpcbind
systemctl enable rpcbind
mkdir /mnt/server3_nfs1
mkdir /mnt/server3_nfs2
mount -t nfs 192.168.23.3:/usr/nfs_1/ /mnt/server3_nfs1
mount -t nfs 192.168.23.3:/usr/nfs_2/ /mnt/server3_nfs2
```

```
[root@server1 mnt]# ls
nfs-share  server3_nfs1  server3_nfs2
[root@server1 mnt]# mount | grep nfs4
192.168.23.3:/usr/nfs_1 on /mnt/server3_nfs1 type nfs4 (rw,relatime,vers=4.1,rsize=262144,wsize=262144,nam
len=255,hard,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=192.168.12.1,local_lock=none,addr=192.168.23
.3)
192.168.23.3:/usr/nfs_2 on /mnt/server3_nfs2 type nfs4 (rw,relatime,vers=4.1,rsize=262144,wsize=262144,nam
len=255,hard,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=192.168.12.1,local_lock=none,addr=192.168.23
.3)
[root@server1 mnt]# df -h
Файловая система                Размер Использовано  Дост Использовано% Смонтировано в
devtmpfs                          908M            0  908M            0% /dev
tmpfs                             919M            0  919M            0% /dev/shm
tmpfs                             919M          8,6M  911M            1% /run
tmpfs                             919M            0  919M            0% /sys/fs/cgroup
/dev/mapper/centos_server1-root    14G          1,5G   12G           12% /
/dev/sda1                        1014M          194M  821M           20% /boot
tmpfs                             184M            0  184M            0% /run/user/1000
192.168.23.3:/usr/nfs_1            14G          1,5G   12G           12% /mnt/server3_nfs1
192.168.23.3:/usr/nfs_2            14G          1,5G   12G           12% /mnt/server3_nfs2
```

11. Убедитесь, что после перезагрузки server1 все еще может писать и читать файлы в примонтированных папках.

```
[root@server1 sa]# cat /etc/fstab

#
# /etc/fstab
# Created by anaconda on Wed Mar 30 21:20:27 2022
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/centos_server1-root /                       xfs     defaults        0 0
UUID=90c559ce-0ae1-464e-b6f9-c0c5ef822988 /boot                   xfs     defaults        0 0
/dev/mapper/centos_server1-swap swap                    swap    defaults        0 0
192.168.23.3:/usr/nfs_1/ /mnt/server3_nfs1 nfs defaults 0 0
192.168.23.3:/usr/nfs_2/ /mnt/server3_nfs2 nfs defaults 0 0
```

```
[root@server1 mnt]# mount | grep nfs4
192.168.23.3:/usr/nfs_1 on /mnt/server3_nfs1 type nfs4 (rw,relatime,vers=4.1,rsize=262144,wsize=262144,nam
len=255,hard,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=192.168.12.1,local_lock=none,addr=192.168.23
.3)
192.168.23.3:/usr/nfs_2 on /mnt/server3_nfs2 type nfs4 (rw,relatime,vers=4.1,rsize=262144,wsize=262144,nam
len=255,hard,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=192.168.12.1,local_lock=none,addr=192.168.23
.3)
[root@server1 mnt]# uptime
 05:14:21 up 37 min,  1 user,  load average: 0,00, 0,01, 0,05
[root@server1 mnt]# touch /mnt/server3_nfs
server3_nfs1/ server3_nfs2/
[root@server1 mnt]# touch /mnt/server3_nfs1/1.test
[root@server1 mnt]# touch /mnt/server3_nfs2/1.test
[root@server1 mnt]#
```

```
[root@server1 sa]# mount | grep nfs4
192.168.23.3:/usr/nfs_1 on /mnt/server3_nfs1 type nfs4 (rw,relatime,vers=4.1,rsize=262144,wsize=262144,nam
len=255,hard,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=192.168.12.1,local_lock=none,addr=192.168.23
.3)
192.168.23.3:/usr/nfs_2 on /mnt/server3_nfs2 type nfs4 (rw,relatime,vers=4.1,rsize=262144,wsize=262144,nam
len=255,hard,proto=tcp,timeo=600,retrans=2,sec=sys,clientaddr=192.168.12.1,local_lock=none,addr=192.168.23
.3)
[root@server1 sa]# uptime
 05:18:20 up 2 min,  1 user,  load average: 1,39, 0,67, 0,26
[root@server1 sa]# touch /mnt/server3_nfs1/2.test
[root@server1 sa]# touch /mnt/server3_nfs2/2.test
```

```
[root@server3 usr]# ls -la /usr/nfs_1
итого 0
drwxrwxrwx.  2 root root  34 мар 31 05:18 .
drwxr-xr-x. 15 root root 181 мар 31 04:55 ..
-rw-r--r--.  1 root root   0 мар 31 05:15 1.test
-rw-r--r--.  1 root root   0 мар 31 05:18 2.test
[root@server3 usr]# ls -la /usr/nfs_2
итого 0
drwxrwxrwx.  2 root root  34 мар 31 05:18 .
drwxr-xr-x. 15 root root 181 мар 31 04:55 ..
-rw-r--r--.  1 root root   0 мар 31 05:15 1.test
-rw-r--r--.  1 root root   0 мар 31 05:18 2.test
[root@server3 usr]#
```