

Лабораторная работа № 12

Тема: Сетевые сервисы на Linux. Роутер на Linux.

Цель работы: Создать и настроить маршрутизатор на базе операционной системы Linux.

Необходимое оборудование и программное обеспечение: Виртуальные машины под управлением Linux (CentOS, Ubuntu или др.).

Пример настройки серверов.

Тестовый стенд состоит из трех виртуальных машин на CentOS 7.

R1:

Nic1 – NAT (что бы был доступ в Интернет)

Nic2 – внутренняя сеть (lan1) 192.168.13.1/24

Lo – loopback 1.1.1.1/32

R2:

Nic1 – NAT (что бы был доступ в Интернет)

Nic2 – внутренняя сеть (lan1) 192.168.13.2/24

Nic3 – внутренняя сеть (lan2) 192.168.23.2/24

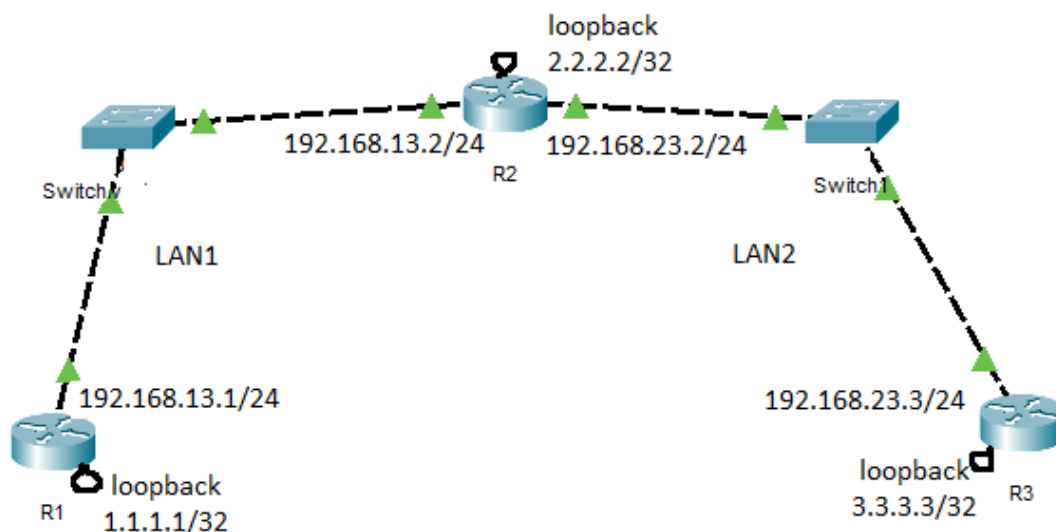
Lo – loopback 2.2.2.2/32

R3:

Nic1 – NAT (что бы был доступ в Интернет)

Nic2 – внутренняя сеть (lan2) 192.168.23.3/24

Lo – loopback 3.3.3.3/32



Настройка сетевых интерфейсов:

Настроим loopback:

```
# ip link add dummy0 type dummy
# ip addr add 1.1.1.1/32 dev dummy0
# ip link set dummy0 up
```

```
[root@r1 ~]# ip link add dummy0 type dummy
[root@r1 ~]# ip addr add 1.1.1.1/32 dev dummy0
[root@r1 ~]# ip link set dummy0 up
[root@r1 ~]# ip a s dummy0
4: dummy0: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP
    link/ether 96:f4:e5:a6:43:be brd ff:ff:ff:ff:ff:ff
    inet 1.1.1.1/32 scope global dummy0
        valid_lft forever preferred_lft forever
    inet6 fe80::94f4:e5ff:fea6:43be/64 scope link
        valid_lft forever preferred_lft forever
[root@r1 ~]# nmcli connection modify dummy0 connection.autoconnect yes
```

Аналогично настраиваем R2 и R3:

Проверим связь:

R1 => R2:

```
[root@r1 ~]# ping 192.168.13.2
PING 192.168.13.2 (192.168.13.2) 56(84) bytes of data.
64 bytes from 192.168.13.2: icmp_seq=1 ttl=64 time=4.31 ms
64 bytes from 192.168.13.2: icmp_seq=2 ttl=64 time=2.94 ms
64 bytes from 192.168.13.2: icmp_seq=3 ttl=64 time=3.37 ms
```

R2 => R3:

```
[root@r2 ~]# ping 192.168.23.3
PING 192.168.23.3 (192.168.23.3) 56(84) bytes of data.
64 bytes from 192.168.23.3: icmp_seq=1 ttl=64 time=4.13 ms
64 bytes from 192.168.23.3: icmp_seq=2 ttl=64 time=9.91 ms
64 bytes from 192.168.23.3: icmp_seq=3 ttl=64 time=4.07 ms
```

R1 => R3: (связь отсутствует, это нормально, т.к. маршрутизация не настроена)

```
[root@r1 ~]# ping 192.168.23.2
PING 192.168.23.2 (192.168.23.2) 56(84) bytes of data.
```

Настройка маршрутизации.

Для R1, R2 и R#:

Включаем маршрутизацию в ядре.

Создадим файл `/etc/sysctl.d/90-routing-sysctl.conf` и пропишем в нем значения `net.ipv4.conf.all.forwarding=1` и `net.ipv6.conf.all.forwarding=1`

- 0: Отключает пересылку IPv4 пакетов.
- 1: Включает пересылку IPv4 пакетов (аналогично IPv6).
- 2: Включает пересылку IPv4 пакетов и разрешает отправку, если это не нарушает политику фильтрации пакетов.

Затем применим настройки ядра командой:

```
sysctl -p /etc/sysctl.d/90-routing-sysctl.conf
```

И перезапустим сетевую службу:

```
systemctl restart NetworkManager
```

```
[root@r1 ~]# nano /etc/sysctl.d/90-routing-sysctl.conf
```

```
GNU nano 2.3.1      File: /etc/sysctl.d/90-routing-sysctl.conf
net.ipv4.conf.all.forwarding=1
net.ipv6.conf.all.forwarding=1
```

```
[root@r1 ~]# sysctl -p /etc/sysctl.d/90-routing-sysctl.conf
net.ipv4.conf.all.forwarding = 1
net.ipv6.conf.all.forwarding = 1
```

```
[root@r1 ~]# systemctl restart NetworkManager
```

Устанавливаем frr:

Вариант 1:

```
yum install -y https://github.com/FRRouting/frr/releases/download/frr-5.0.1/frr-5.0.1-2018070501.el7.centos.x86_64.rpm
```

Вариант 2:

```
sudo yum install epel-release
sudo yum install snapd
sudo systemctl enable --now snapd.socket
sudo ln -s /var/lib/snapd/snap /snap
sudo snap install frr
```

Вариант 3 (Centos 9):

```
dnf install frr
```

Используем 1-й вариант:

```
[root@r1 ~]# yum install -y https://github.com/FRRouting/frr/releases/download/frr-5.0.1/frr-5.0.1-2018070501.el7.centos.x86_64.rpm
```

```
Installed:
  frr.x86_64 0:5.0.1-2018070501.el7.centos

Dependency Installed:
  c-ares.x86_64 0:1.10.0-3.el7_9.1

Complete!
[root@r1 ~]#
```

Проверяем:

```
[root@r1 ~]# systemctl status frr
● frr.service - FRRouting (FRR)
   Loaded: loaded (/usr/lib/systemd/system/frr.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
[root@r1 ~]#
```

Включение нужных протоколов маршрутизации:

```
[root@r1 ~]# nano /etc/frr/daemons
```

```

GNU nano 2.3.1      File: /etc/frr/daemons
#
# When activation a daemon at the first time, a config file, even if it is
# empty, has to be present *and* be owned by the user and group "frr", else
# the daemon will not be started by /usr/lib/frr/frr. The permissions should
# be u=rw,g=r,o=.
# When using "vtysh" such a config file is also needed. It should be owned by
# group "frrvty" and set to ug=rw,o= though. Check /etc/pam.d/frr, too.
#
watchfrr_enable=yes
watchfrr_options=(-b_ "-r/usr/lib/frr/frr_restart_%s" "-s/usr/lib/frr/frr_start_%s"
#
zebra=yes
bgpd=no
ospfd=yes
ospf6d=yes
ripd=no
ripngd=no
isisd=no
ldpd=no
pimd=no
nhdpd=no

```

Запускаем и проверяем:

```

[root@r1 ~]# systemctl start frr
[root@r1 ~]# systemctl status frr
● frr.service - FRRouting (FRR)
   Loaded: loaded (/usr/lib/systemd/system/frr.service; disabled; vendor preset: disabled)
   Active: active (running) since Mon 2024-03-04 09:29:11 EST; 5s ago
     Process: 12941 ExecStart=/usr/lib/frr/frr start (code=exited, status=0/SUCCESS)
    CGroup: /system.slice/frr.service
            └─12959 /usr/lib/frr/zebra -d -A 127.0.0.1
            └─12968 /usr/lib/frr/ospfd -d -A 127.0.0.1
            └─12977 /usr/lib/frr/ospf6d -d -A ::1
            └─12987 /usr/lib/frr/watchfrr -d -b_ -r/usr/lib/frr/frr_restart_%s -s/usr/lib/frr/...

Mar 04 09:29:10 r1 frr[12941]: ospfd [ OK ]
Mar 04 09:29:10 r1 frr[12941]: ospf6d [ OK ]
Mar 04 09:29:10 r1 frr[12941]: Starting FRRouting monitor daemon:
Mar 04 09:29:10 r1 watchfrr[12987]: watchfrr 5.0.1 watching [zebra ospfd ospf6d]
Mar 04 09:29:11 r1 watchfrr[12987]: ospfd state -> up : connect succeeded
Mar 04 09:29:11 r1 watchfrr[12987]: ospf6d state -> up : connect succeeded
Mar 04 09:29:11 r1 watchfrr[12987]: zebra state -> up : connect succeeded
Mar 04 09:29:11 r1 watchfrr[12987]: Watchfrr: Notifying Systemd we are up and running
Mar 04 09:29:11 r1 frr[12941]: watchfrr[ OK ]
Mar 04 09:29:11 r1 systemd[1]: Started FRRouting (FRR).
[root@r1 ~]#

```

разрешим в firewalld OSPF-трафик:

```

[root@r1 ~]# firewall-cmd --add-protocol=ospf --permanent --zone=public
success
[root@r1 ~]# firewall-cmd --add-protocol=ospf --zone=public
success
[root@r1 ~]#

```

sudo firewall-cmd --reload

sudo firewall-cmd --list-all

```
[root@r1 ~]# firewall-cmd --reload
success
[root@r1 ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3 enp0s8
  sources:
  services: dhcpv6-client ssh
  ports:
  protocols: ospf
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

Аналогичные действия выполняем на хостах R2 и R3.

Настройка роутера R1. Анонсируем локальную сеть и лупбэк:

```
[root@r1 ~]# vtysh

Hello, this is FRRouting (version 5.0.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

r1# conf t
r1(config-router)# router ospf
r1(config-router)# network 192.168.13.0/24 area 0
r1(config-router)# network 1.1.1.1/32 area 0
r1(config-router)# exit
r1(config)# exit
r1# wr
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Configuration saved to /etc/frr/zebra.conf
Configuration saved to /etc/frr/ospfd.conf
Configuration saved to /etc/frr/ospf6d.conf
r1# exit
[root@r1 ~]#
```

Для второго хоста:

Для третьего хоста:

```
[root@r3 ~]# vtysh

Hello, this is FRRouting (version 5.0.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

r3# conf t
r3(config)# router ospf
r3(config-router)# network 192.168.23.0/24 area 0
r3(config-router)# network 3.3.3.3/32 area 0
r3(config-router)# exit
r3(config)# exit
r3# wr
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Configuration saved to /etc/frr/zebra.conf
Configuration saved to /etc/frr/ospfd.conf
Configuration saved to /etc/frr/ospf6d.conf
r3# exit
[root@r3 ~]#
```

Проверяем:

Маршруты добавились:

```
[root@r1 ~]# vtysh

Hello, this is FRRouting (version 5.0.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

r1# show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, D - SHARP,
       F - PBR,
       > - selected route, * - FIB route

K>* 0.0.0.0/0 [0/100] via 192.168.1.1, enp0s3, 00:25:33
O 1.1.1.1/32 [110/10] via 0.0.0.0, dummy0 onlink, 00:10:53
C>* 1.1.1.1/32 is directly connected, dummy0, 00:25:33
O>* 3.3.3.3/32 [110/210] via 192.168.13.2, enp0s8, 00:02:38
C>* 192.168.1.0/24 is directly connected, enp0s3, 00:25:33
O 192.168.13.0/24 [110/100] is directly connected, enp0s8, 00:11:07
C>* 192.168.13.0/24 is directly connected, enp0s8, 00:25:33
O>* 192.168.23.0/24 [110/200] via 192.168.13.2, enp0s8, 00:04:27
r1#
```

Пингуем:

```
[root@r1 ~]# ping 192.168.23.100
PING 192.168.23.100 (192.168.23.100) 56(84) bytes of data.
64 bytes from 192.168.23.100: icmp_seq=1 ttl=63 time=4.32 ms
64 bytes from 192.168.23.100: icmp_seq=2 ttl=63 time=7.08 ms
64 bytes from 192.168.23.100: icmp_seq=3 ttl=63 time=3.70 ms
^C
--- 192.168.23.100 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 3.701/5.034/7.080/1.470 ms
[root@r1 ~]# ping 3.3.3.3
PING 3.3.3.3 (3.3.3.3) 56(84) bytes of data.
64 bytes from 3.3.3.3: icmp_seq=1 ttl=63 time=7.32 ms
64 bytes from 3.3.3.3: icmp_seq=2 ttl=63 time=7.26 ms
64 bytes from 3.3.3.3: icmp_seq=3 ttl=63 time=6.87 ms
^C
--- 3.3.3.3 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2006ms
rtt min/avg/max/mdev = 6.877/7.156/7.325/0.221 ms
[root@r1 ~]#
```

Трассируем:

```
[root@r1 ~]# mtr 3.3.3.3
```

root@r1:~

My traceroute [v0.85]

Mon Mar 4 09:58:45 2024

Keys: Help		Display mode	Restart statistics	Order of fields		quit	
		Packets		Pings			
Host	Loss%	Snt	Last	Avg	Best	Wrst	StDev
1. 192.168.13.2	0.0%	7	3.7	3.2	2.1	4.0	0.6
2. 3.3.3.3	0.0%	6	3.8	4.1	3.8	4.4	0.0

```
[root@r1 ~]# mtr 192.168.23.3
```

My traceroute [v0.85]									
r1 (0.0.0.0)					Mon Mar 4 10:18:01 2024				
Keys:	Help	Display mode	Restart statistics	Order of fields	quit				
Packets					Pings				
Host	Loss%	Snt	Last	Avg	Best	Wrst	StDev		
1. 192.168.13.2	0.0%	9	3.8	2.9	2.3	3.8	0.0		
2. 192.168.23.3	0.0%	9	3.7	3.8	3.3	4.5	0.0		

Задание:

1. Используйте лабораторный стенд, созданный в предыдущей работе.
2. Настройте лупбэки.
3. Активация IP-маршрутизации. Включить IP-маршрутизацию на серверах с помощью настройки ядра и/или использования утилиты sysctl.
4. Настроить протоколы динамической маршрутизации (например, OSPF).
5. Настроить межсетевой экран для фильтрации трафика и обеспечения безопасности сети.
6. Проверить работоспособность маршрутов с помощью команд, таких как ping, traceroute.
7. Сделать выводы и составить отчет.