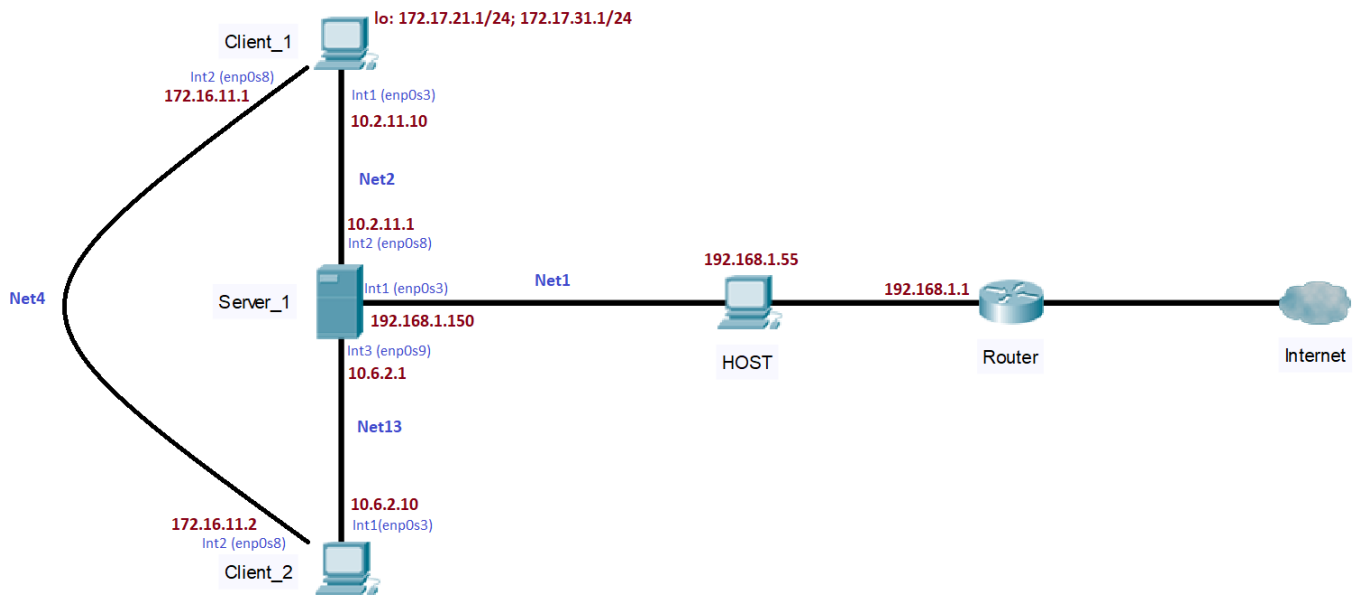


# EPAM University Programs DevOps external course

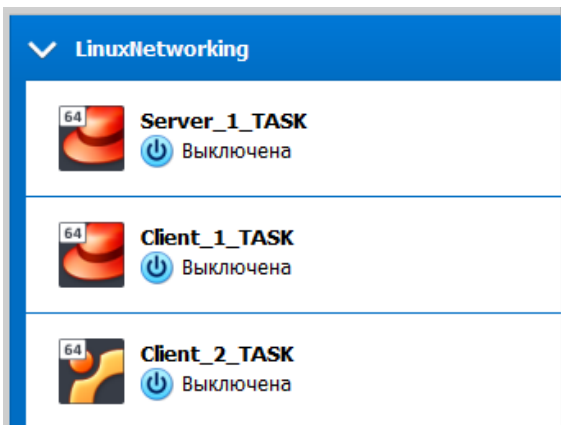
## Module – Linux Networking

Logical topology of my network:

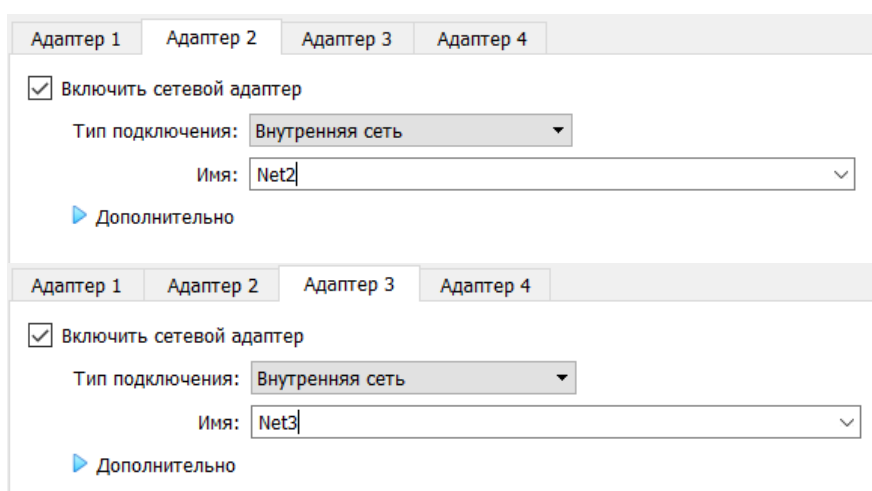
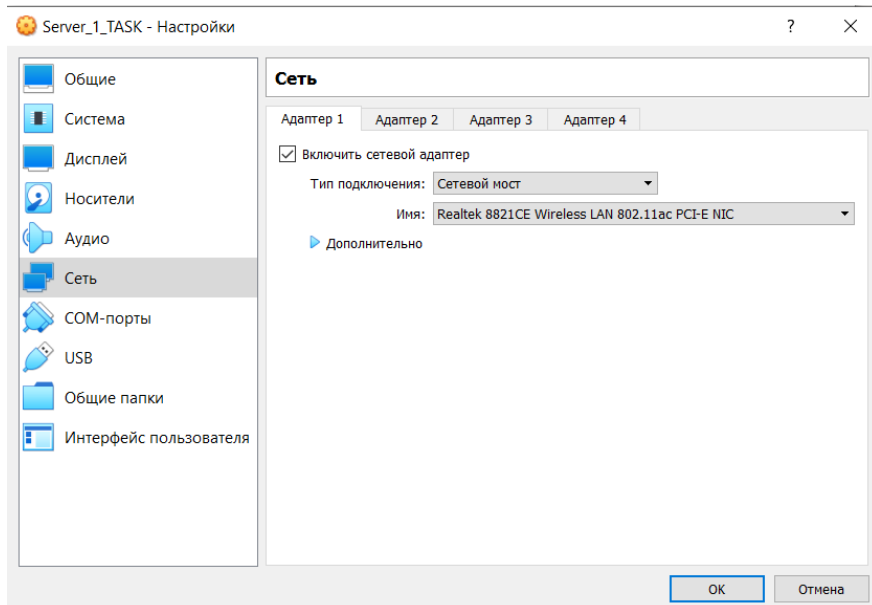


## Configuration Of Virtual Machines

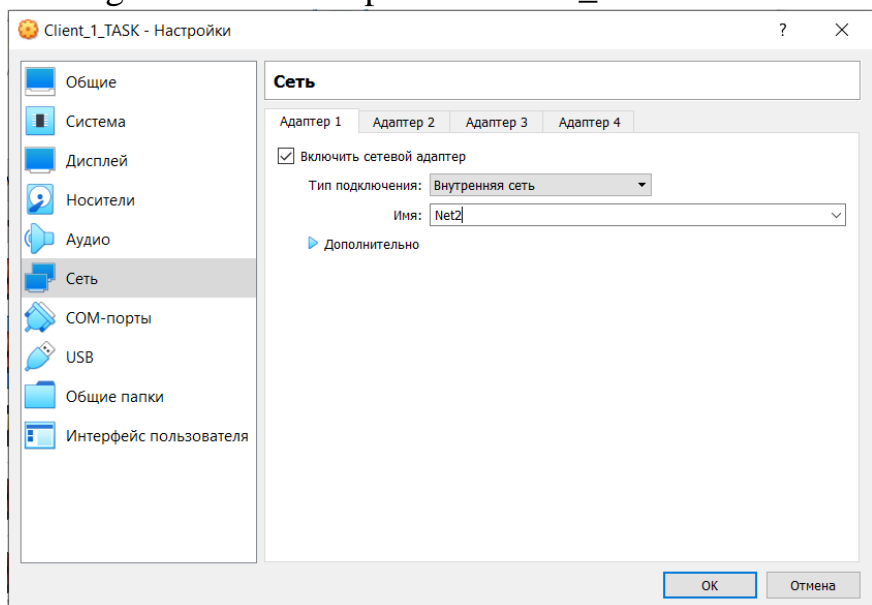
I create three virtual machines:



I configure server's network adapters:



I configure network adapters of Client\_1:



Адаптер 1   Адаптер 2   Адаптер 3   Адаптер 4

☒ Включить сетевой адаптер

Тип подключения: Внутренняя сеть

Имя: Net4

▶ Дополнительно

I configure network adapters of Client\_2:

Client\_2\_TASK - Настройки

Общие  
Система  
Дисплей  
Носители  
Аудио  
Сеть  
COM-порты  
USB  
Общие папки  
Интерфейс пользователя

**Сеть**

Адаптер 1   Адаптер 2   Адаптер 3   Адаптер 4

☒ Включить сетевой адаптер

Тип подключения: Внутренняя сеть

Имя: Net3

▶ Дополнительно

OK   Отмена

Адаптер 1   Адаптер 2   Адаптер 3   Адаптер 4

☒ Включить сетевой адаптер

Тип подключения: Внутренняя сеть

Имя: Net4

▶ Дополнительно

According to the task, my networks should be:

Net2 – 10.2.11.0/24

Net3 – 10.6.2.0/24

Net4 – 172.16.11.0/24

I install operating systems on virtual machines:

- CentOS on Server\_1
- CentOS on Client\_1
- Ubuntu on Client\_2

## Execution Steps

- 1) I configure static addresses on all network interfaces of the Server\_1:

First network interface:

```
[root@localhost vladyslav]# vi /etc/sysconfig/network-scripts/ifcfg-enp0s3
```

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
IPADDR=192.168.1.150
PREFIX=24
GATEWAY=192.168.1.1
DNS1=192.168.1.1
DNS2=8.8.8.8
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=no
NAME=enp0s3
UUID=c7a72a16-2123-4293-ba92-c61aab4d233b
DEVICE=enp0s3
ONBOOT=yes
```

Second network interface:

```
[root@localhost vladyslav]# vi /etc/sysconfig/network-scripts/ifcfg-enp0s8_
```

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
DEFROUTE=no
IPADDR=10.2.11.1
PREFIX=24
DNS1=192.168.1.1
DNS2=8.8.4.4
IPV4_FAILURE_FATAL=no
IPV6INIT=no
NAME=enp0s8
UUID=f1c16160-7b75-4160-a248-78a4da2601d9
DEVICE=enp0s8
ONBOOT=yes
```

Third network interface:

```
[root@localhost vladyslav]# vi /etc/sysconfig/network-scripts/ifcfg-enp0s9
```

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
DEFROUTE=no
IPADDR=10.6.2.1
PREFIX=24
DNS1=192.168.1.1
DNS2=8.8.4.4
IPV4_FAILURE_FATAL=no
IPV6INIT=no
NAME=enp0s9
UUID=d4287fed-968e-4328-839c-80256e0325a5
DEVICE=enp0s9
ONBOOT=yes
```

I restart network service and verify network settings:



```
[root@localhost vladyslav]# yum -y install dhcp
Loaded plugins: fastestmirror
Determining fastest mirrors
 * base: mirror.lanet.network
 * extras: mirror.lanet.network
 * updates: mirror.lanet.network
base                                     | 3.6 kB  00:00:00
extras                                 | 2.9 kB  00:00:00
updates                               | 2.9 kB  00:00:00
(1/4): extras/7/x86_64/primary_db     | 249 kB  00:00:00
(2/4): base/7/x86_64/group_gz        | 153 kB  00:00:00
(3/4): base/7/x86_64/primary_db     | 6.1 MB  00:00:02
(4/4): updates/7/x86_64/primary_db   | 17 MB  00:00:03
Resolving Dependencies
--> Running transaction check
---> Package dhcp.x86_64 12:4.2.5-83.el7.centos.1 will be installed
```

I configure dhcp:

```
[root@localhost vladyslav]# vi /etc/dhcp/dhcpd.conf

default-lease-time 3600;
max-lease-time 7200;

subnet 10.2.11.0 netmask 255.255.255.0 {
    range 10.2.11.10 10.2.11.200;
    option routers 10.2.11.1;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 192.168.1.1;
}

subnet 10.6.2.0 netmask 255.255.255.0 {
    range 10.6.2.10 10.6.2.200;
    option routers 10.6.2.1;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 192.168.1.1;
}
```

I enable and restart dhcp service:

```
[root@localhost vladyslav]# systemctl enable dhcpd
Created symlink from /etc/systemd/system/multi-user.target.wants/dhcpd.service to /usr/lib/systemd/system/dhcpd.service.

[root@localhost vladyslav]# systemctl restart dhcpd
```

3) I use the ping and traceroute commands to test the connection between the machines:

*From Client\_1 to Server\_1:*

```
[vladyslav@localhost ~]$ ping 10.2.11.1
PING 10.2.11.1 (10.2.11.1) 56(84) bytes of data.
64 bytes from 10.2.11.1: icmp_seq=1 ttl=64 time=0.398 ms
64 bytes from 10.2.11.1: icmp_seq=2 ttl=64 time=1.04 ms
64 bytes from 10.2.11.1: icmp_seq=3 ttl=64 time=1.11 ms
64 bytes from 10.2.11.1: icmp_seq=4 ttl=64 time=0.610 ms
^C
--- 10.2.11.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.398/0.791/1.113/0.300 ms
[vladyslav@localhost ~]$ traceroute 10.2.11.1
traceroute to 10.2.11.1 (10.2.11.1), 30 hops max, 60 byte packets
 1 gateway (10.2.11.1) 0.471 ms !X 0.395 ms !X 0.280 ms !X
[vladyslav@localhost ~]$
```

The ping command shows that there is a connection between the machines. The traceroute command shows through which machine the packets are sent. The "!X" message means traceroute is receiving an ICMP error message from the other peer in response to its UDP probes; specifically, the ICMP error "host-prohibited".

*From Client\_1 to Client\_2:*

```
[vladyslav@localhost ~]$ ping 10.6.2.10
PING 10.6.2.10 (10.6.2.10) 56(84) bytes of data.
64 bytes from 10.6.2.10: icmp_seq=1 ttl=63 time=0.788 ms
64 bytes from 10.6.2.10: icmp_seq=2 ttl=63 time=1.78 ms
64 bytes from 10.6.2.10: icmp_seq=3 ttl=63 time=1.95 ms
^C
--- 10.6.2.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.788/1.510/1.956/0.516 ms
[vladyslav@localhost ~]$ traceroute 10.6.2.10
traceroute to 10.6.2.10 (10.6.2.10), 30 hops max, 60 byte packets
 1 gateway (10.2.11.1) 0.362 ms 0.307 ms 0.277 ms
 2 gateway (10.2.11.1) 0.216 ms !X 0.190 ms !X 0.237 ms !X
[vladyslav@localhost ~]$
```

*From Client\_2 to Client\_1:*

```
vladyslav@Client-2:~$ tracepath 10.2.11.10 -n
 1?: [LOCALHOST] pmtu 1500
 1: 10.6.2.1 0.563ms
 1: 10.6.2.1 0.475ms
 2: 10.6.2.1 0.505ms !H
Resume: pmtu 1500
vladyslav@Client-2:~$ ping 10.2.11.10
PING 10.2.11.10 (10.2.11.10) 56(84) bytes of data.
64 bytes from 10.2.11.10: icmp_seq=1 ttl=63 time=1.10 ms
64 bytes from 10.2.11.10: icmp_seq=2 ttl=63 time=2.06 ms
^C
--- 10.2.11.10 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 1.102/1.578/2.055/0.476 ms
```

I add static routes to Net2 and Net3 networks on my home router (so that the router knows where to return traffic):

Static Route

<input type="checkbox"/>	Destination IP Address	Subnet Mask	Gateway	Status	Edit
<input type="checkbox"/>	10.2.11.0	255.255.255.0	192.168.1.150	Enable	<a href="#">Edit</a>
<input type="checkbox"/>	10.6.2.0	255.255.255.0	192.168.1.150	Enable	<a href="#">Edit</a>

Add New

Enable Selected

Disable Selected

Delete Selected

- 4) I set up routing so that it is possible to get from Client\_2 to Client\_1's lo by different routes:

First, I configure network adapters of clients to create a network (Net4):

*Client\_1:*

```
[vladyslav@localhost ~]$ sudo vi /etc/sysconfig/network-scripts/ifcfg-enp0s8
```

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=no
IPADDR=172.16.11.1
PREFIX=24
IPV4_FAILURE_FATAL=no
IPV6INIT=no
NAME=enp0s8
UUID=9dda970f-a4cc-4643-aec2-5d92625c0ff0
DEVICE=enp0s8
ONBOOT=yes
```

```
[vladyslav@localhost ~]$ systemctl restart network
[vladyslav@localhost ~]$ 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 08:00:27:00:40:80 brd ff:ff:ff:ff:ff:ff
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:46:fa:88 brd ff:ff:ff:ff:ff:ff
    inet 172.16.11.1/24 brd 172.16.11.255 scope global enp0s8
        valid_lft forever preferred_lft forever
```

## Client\_2:

```
root@Client-2:/home/vladyslav# vi /etc/netplan/01-network-manager-all.yaml
```

```
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernet:
    enp0s8:
      dhcp4: no
      addresses:
        - 172.16.11.2/24
```

```
root@Client-2:/home/vladyslav# netplan apply
```

```
root@Client-2:/home/vladyslav# 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 08:00:27:8c:e6:6d brd ff:ff:ff:ff:ff:ff
    inet 10.6.2.11/24 brd 10.6.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 3545sec preferred_lft 3545sec
    inet 10.6.2.10/24 brd 10.6.2.255 scope global secondary dynamic enp0s3
        valid_lft 3557sec preferred_lft 3557sec
    inet6 fe80::49a2:3070:6db1:149f/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:3c:6d:e0 brd ff:ff:ff:ff:ff:ff
    inet 172.16.11.2/24 brd 172.16.11.255 scope global noprefixroute enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe3c:6de0/64 scope link
        valid_lft forever preferred_lft forever
```

I add two temporary IP addresses to lo interface of Client\_1:

```
[vladyslav@localhost ~]$ sudo ip address add 172.17.21.1/24 dev lo
[sudo] password for vladyslav:
[vladyslav@localhost ~]$ sudo ip address add 172.17.31.1/24 dev lo
```



```
[vladyslav@localhost ~]$ ip addr show lo
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
    inet 172.17.21.1/24 scope global lo
        valid_lft forever preferred_lft forever
    inet 172.17.31.1/24 scope global lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
```

I add temporary routes on Client\_2 to the specified above IP addresses:

```
root@Client-2:/home/vladyslav# ip route add 172.17.21.0/24 via 10.6.2.1
root@Client-2:/home/vladyslav# ip route add 172.17.31.0/24 via 172.16.11.1
```

I add a temporary route on Server\_1 to the specified above IP address:

```
[root@localhost vladyslav]# ip route add 172.17.21.0/24 via 10.2.11.10
```

I disable firewalld on Server\_1 and on Client\_1 to prevent conflicts with iptables:

```
[root@localhost vladyslav]# systemctl disable --now firewalld
Removed symlink /etc/systemd/system/multi-user.target.wants/firewalld.service.
Removed symlink /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service.
```

I check the correctness of the routes on Client\_2 with traceroute command:

*Communication with 172.17.21.1 IP address goes through the server interface (10.6.2.1 IP address):*

```
root@Client-2:/home/vladyslav# ping 172.17.21.1
PING 172.17.21.1 (172.17.21.1) 56(84) bytes of data.
64 bytes from 172.17.21.1: icmp_seq=1 ttl=63 time=0.952 ms
64 bytes from 172.17.21.1: icmp_seq=2 ttl=63 time=1.87 ms
64 bytes from 172.17.21.1: icmp_seq=3 ttl=63 time=1.74 ms
^C
--- 172.17.21.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 0.952/1.519/1.870/0.404 ms
root@Client-2:/home/vladyslav# tracepath 172.17.21.1 -n
 1?: [LOCALHOST] pmtu 1500
 1: 10.6.2.1 0.588ms
 1: 10.6.2.1 0.425ms
 2: 172.17.21.1 0.837ms reached
Resume: pmtu 1500 hops 2 back 2
```

*Communication with 172.17.31.1 IP address goes straight (1 hop):*

```
root@Client-2:/home/vladyslav# ping 172.17.31.1
PING 172.17.31.1 (172.17.31.1) 56(84) bytes of data.
64 bytes from 172.17.31.1: icmp_seq=1 ttl=64 time=0.518 ms
64 bytes from 172.17.31.1: icmp_seq=2 ttl=64 time=0.850 ms
64 bytes from 172.17.31.1: icmp_seq=3 ttl=64 time=0.932 ms
^C
--- 172.17.31.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2008ms
rtt min/avg/max/mdev = 0.518/0.766/0.932/0.178 ms
root@Client-2:/home/vladyslav# tracepath 172.17.31.1 -n
 1?: [LOCALHOST] pmtu 1500
 1: 172.17.31.1 0.492ms reached
 1: 172.17.31.1 0.463ms reached
Resume: pmtu 1500 hops 1 back 1
```

5) Route summarization of 172.17.21.1/24 and 172.17.31.1/24 is 172.17.16.0/20.

I delete the routes created in the previous step:

*Client\_2:*

```
root@Client-2:/home/vladyslav# ip route delete 172.17.21.0/24
root@Client-2:/home/vladyslav# ip route delete 172.17.31.0/24
root@Client-2:/home/vladyslav#
root@Client-2:/home/vladyslav# ip r
default via 10.6.2.1 dev enp0s3 proto dhcp metric 102
10.6.2.0/24 dev enp0s3 proto kernel scope link src 10.6.2.11 metric 102
169.254.0.0/16 dev enp0s3 scope link metric 1000
172.16.11.0/24 dev enp0s8 proto kernel scope link src 172.16.11.2 metric 101
```

*Server\_1:*

```
[root@localhost vladyslav]# ip r
default via 192.168.1.1 dev enp0s3 proto static metric 100
10.2.11.0/24 dev enp0s8 proto kernel scope link src 10.2.11.1 metric 101
10.6.2.0/24 dev enp0s9 proto kernel scope link src 10.6.2.1 metric 102
192.168.1.0/24 dev enp0s3 proto kernel scope link src 192.168.1.150 metric 100
```

I make the temporary IPs made in the previous step permanent:

```
[vladyslav@localhost ~]$ sudo ip address del 172.17.21.1/24 dev lo
[sudo] password for vladyslav:
[vladyslav@localhost ~]$ sudo ip address del 172.17.31.1/24 dev lo
[vladyslav@localhost ~]$ ip address show lo
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
```

[vladyslav@localhost ~]\$ vi /etc/sysconfig/network-scripts/ifcfg-lo

```
DEVICE=lo
IPADDR0=127.0.0.1
NETMASK0=255.0.0.0
NETWORK=127.0.0.0

IPADDR1=172.17.21.1
IPADDR2=172.17.31.1
PREFIX1=24
PREFIX2=24
# If you're having problems with gated making 127.0.0.0/8 a martian,
# you can change this to something else (255.255.255.255, for example)
BROADCAST=127.255.255.255
ONBOOT=yes
NAME=loopback
```

```
[vladyslav@localhost ~]$ sudo systemctl restart network
[vladyslav@localhost ~]$ ip a show lo
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
    inet 172.17.21.1/24 brd 172.17.21.255 scope host lo
        valid_lft forever preferred_lft forever
    inet 172.17.31.1/24 brd 172.17.31.255 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
```

I add the summarized route to routing tables on Server\_1 and Client\_2 (permanently):

## Server\_1:

```
[root@localhost vladyslav]# vi /etc/sysconfig/network-scripts/route-enp0s8
172.17.16.0/20 via 10.2.11.10 dev enp0s8

[root@localhost vladyslav]# systemctl restart network
[root@localhost vladyslav]# ip r
default via 192.168.1.1 dev enp0s3 proto static metric 100
10.2.11.0/24 dev enp0s8 proto kernel scope link src 10.2.11.1 metric 101
10.6.2.0/24 dev enp0s9 proto kernel scope link src 10.6.2.1 metric 102
172.17.16.0/20 via 10.2.11.10 dev enp0s8 proto static metric 101
192.168.1.0/24 dev enp0s3 proto kernel scope link src 192.168.1.150 metric 100
```

## Client\_2:

```
root@Client-2:/home/vladyslav# nano /etc/netplan/01-network-manager-all.yaml
```

```
GNU nano 6.2 /etc/netplan/01-network-manager-all.yaml *
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    enp0s3:
      dhcp4: true
      routes:
        - to: 172.17.16.0/20
          via: 10.6.2.1
    enp0s8:
      dhcp4: no
      addresses:
        - 172.16.11.2/24
```

```
root@Client-2:/home/vladyslav# sudo netplan try
Do you want to keep these settings?
```

Press ENTER before the timeout to accept the new configuration

Changes will revert in 110 seconds  
Configuration accepted.

```
root@Client-2:/home/vladyslav# ip r
default via 10.6.2.1 dev enp0s3 proto dhcp metric 100
10.6.2.0/24 dev enp0s3 proto kernel scope link src 10.6.2.11 metric 100
10.6.2.1 dev enp0s3 proto static scope link metric 100
169.254.0.0/16 dev enp0s8 scope link metric 1000
172.16.11.0/24 dev enp0s8 proto kernel scope link src 172.16.11.2 metric 101
172.17.16.0/20 via 10.6.2.1 dev enp0s3 proto static metric 100
```

I check the correctness of the routes with traceroute command on Client\_2:

```
root@Client-2:/home/vladyslav# tracepath 172.17.21.1 -n
 1?: [LOCALHOST] pmtu 1500
 1: 10.6.2.1 0.545ms
 1: 10.6.2.1 0.440ms
 2: 172.17.21.1 0.917ms reached
    Resume: pmtu 1500 hops 2 back 2
root@Client-2:/home/vladyslav# tracepath 172.17.31.1 -n
 1?: [LOCALHOST] pmtu 1500
 1: 10.6.2.1 0.483ms
 1: 10.6.2.1 0.400ms
 2: 172.17.31.1 0.792ms reached
    Resume: pmtu 1500 hops 2 back 2
```

- 6) I install SSH server only on Client\_2 (Ubuntu) because other VMs already have SSH server installed out of the box:

```
root@Client-2:/home/vladyslav# apt install openssh-server
```

The standard settings of SSH allow us to connect to the machine using a password, so any machine can connect to each other without any problems:

*From Client\_1 to Client\_2:*

```
[vladyslav@localhost ~]$ ssh vladyslav@10.6.2.10
The authenticity of host '10.6.2.10 (10.6.2.10)' can't be established.
ECDSA key fingerprint is SHA256:7JLJRAK1BXb1sfUUL1+l0uEmq1T7vXA74UXscc5gidY.
ECDSA key fingerprint is MD5:48:89:f7:e1:94:c3:73:06:92:73:a4:89:de:e6:40:6e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.6.2.10' (ECDSA) to the list of known hosts.
vladyslav@10.6.2.10's password:
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.15.0-25-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

327 updates can be applied immediately.
155 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Last login: Thu Nov  3 10:21:46 2022 from 10.6.2.1
vladyslav@Client-2:~$ exit
logout
Connection to 10.6.2.10 closed.
[vladyslav@localhost ~]$
```

*From Client\_2 to Client\_1:*

```
root@Client-2:/home/vladyslav# ssh vladyslav@10.2.11.10
The authenticity of host '10.2.11.10 (10.2.11.10)' can't be established.
ED25519 key fingerprint is SHA256:z8+qPS2D28jn6q46ti/UaK63cRWNYu/xCVCUEerskIQ.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.2.11.10' (ED25519) to the list of known hosts.
vladyslav@10.2.11.10's password:
Last login: Wed Nov  2 03:08:14 2022
[vladyslav@localhost ~]$
```

*From Server\_1 to Client\_1:*

```
[root@localhost vladyslav]# ssh vladyslav@10.2.11.10
The authenticity of host '10.2.11.10 (10.2.11.10)' can't be established.
ECDSA key fingerprint is SHA256:GxF+YMsG3hYYx98/SxuAmMgebFnrnJP81ogTYxtnFeM.
ECDSA key fingerprint is MD5:23:e8:4f:b8:9c:f2:f2:8e:26:4c:e9:b0:29:1b:73:06.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.2.11.10' (ECDSA) to the list of known hosts.
vladyslav@10.2.11.10's password:
Last login: Wed Nov  2 12:23:23 2022 from 10.6.2.10
[vladyslav@localhost ~]$
```

*From Client\_2 to Server\_1:*

```

vladyslav@Client-2:~$ ssh vladyslav@10.6.2.1
The authenticity of host '10.6.2.1 (10.6.2.1)' can't be established.
ED25519 key fingerprint is SHA256:51fD0MSm2Mre3TsHs2rsXmvJzC1UKRoTgCTHREd16G0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.6.2.1' (ED25519) to the list of known hosts.
vladyslav@10.6.2.1's password:
Last login: Wed Nov  2 12:16:45 2022 from 10.6.2.10
[vladyslav@localhost ~]$

```

## 7) I configure firewall on Server\_1:

- I accept SSH traffic from Client\_1:

```

[root@localhost vladyslav]# iptables -A INPUT -p tcp -s 10.2.11.10 -d 10.2.11.1 --dport 22 -j ACCEPT

```

### I drop SSH traffic from Client\_2:

```

[root@localhost vladyslav]# iptables -A INPUT -p tcp -s 10.6.2.10 -d 10.6.2.1 --dport 22 -j DROP

```

```

[root@localhost vladyslav]# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source                destination          tcp dpt:22
ACCEPT     tcp  --  10.2.11.10             10.2.11.1            tcp dpt:22
DROP       tcp  --  10.6.2.10              10.6.2.1            tcp dpt:22

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
[root@localhost vladyslav]#

```

### I verify the connection on Client\_1:

```

[vladyslav@localhost ~]$ ssh vladyslav@10.2.11.1
vladyslav@10.2.11.1's password:
Last login: Wed Nov  2 13:18:55 2022
[vladyslav@localhost ~]$

```

### I verify the connection on Client\_2:

```

vladyslav@Client-2:~$ ssh vladyslav@10.6.2.1
ssh: connect to host 10.6.2.1 port 22: Connection timed out

```

### I list accepted and dropped packets on Server\_1:

```

[root@localhost vladyslav]# iptables -nvL
Chain INPUT (policy ACCEPT 23 packets, 2941 bytes)
 pkts bytes target     prot opt in     out     source                destination          tcp dpt:22
   32  4429 ACCEPT     tcp  --  *      *      10.2.11.10           10.2.11.1            tcp dpt:22
    7   420 DROP       tcp  --  *      *      10.6.2.10            10.6.2.1            tcp dpt:22

Chain FORWARD (policy ACCEPT 52 packets, 8159 bytes)
 pkts bytes target     prot opt in     out     source                destination

Chain OUTPUT (policy ACCEPT 32 packets, 4706 bytes)
 pkts bytes target     prot opt in     out     source                destination
[root@localhost vladyslav]#

```

So, everything works well.

- I accept ping traffic from Client\_2 to 172.17.21.1:

```

[root@localhost vladyslav]# iptables -A FORWARD -p icmp --icmp-type echo-request -s 10.6.2.10 -d 172.17.21.1 -j ACCEPT

```

### I drop ping traffic from Client\_2 to 172.17.31.1:

```

[root@localhost vladyslav]# iptables -A FORWARD -p icmp --icmp-type echo-request -s 10.6.2.10 -d 172.17.31.1 -j DROP

```



```

[root@localhost vladyslav]# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            tcp dpt:22
ACCEPT     tcp  --  10.2.11.10             10.2.11.1              tcp dpt:22
DROP       tcp  --  10.6.2.10              10.6.2.1               tcp dpt:22

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination            icmp type 8
ACCEPT     icmp --  10.6.2.10              172.17.21.1           icmp type 8
DROP       icmp --  10.6.2.10              172.17.31.1           icmp type 8

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
[root@localhost vladyslav]#

```

I verify ping accessibility from Client\_2 to 172.17.21.1 and 172.17.31.1:

```

vladyslav@Client-2:~$ ping 172.17.21.1
PING 172.17.21.1 (172.17.21.1) 56(84) bytes of data.
64 bytes from 172.17.21.1: icmp_seq=1 ttl=63 time=1.28 ms
64 bytes from 172.17.21.1: icmp_seq=2 ttl=63 time=2.09 ms
64 bytes from 172.17.21.1: icmp_seq=3 ttl=63 time=1.96 ms
^C
--- 172.17.21.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.275/1.775/2.090/0.357 ms
vladyslav@Client-2:~$ ping 172.17.31.1
PING 172.17.31.1 (172.17.31.1) 56(84) bytes of data.
^C
--- 172.17.31.1 ping statistics ---
199 packets transmitted, 0 received, 100% packet loss, time 202732ms

```

I have created a script to renew iptables when needed:

```

[root@localhost vladyslav]# pwd
/home/vladyslav
[root@localhost vladyslav]# cat iptables_rules.sh
#!/bin/bash

iptables -F
iptables -A INPUT -p tcp -s 10.2.11.10 -d 10.2.11.1 --dport 22 -j ACCEPT
iptables -A INPUT -p tcp -s 10.6.2.10 -d 10.6.2.1 --dport 22 -j DROP

iptables -A FORWARD -p icmp --icmp-type echo-request -s 10.6.2.10 -d 172.17.21.1 -j ACCEPT
iptables -A FORWARD -p icmp --icmp-type echo-request -s 10.6.2.10 -d 172.17.31.1 -j DROP

```

8) I delete static routes to Net2 and Net3 on my home router:

Static Route

<input type="checkbox"/>	Destination IP Address	Subnet Mask	Gateway	Status	Edit
<div> <input type="button" value="Add New"/> <input type="button" value="Enable Selected"/> <input type="button" value="Disable Selected"/> <input type="button" value="Delete Selected"/> </div>					

I change the connection type to NAT for the Server\_1 network adapter:



I check the correctness of the NAT settings:

```
vladyslav@Client-2:~$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=24.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=24.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=24.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=115 time=24.7 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 24.042/24.337/24.738/0.269 ms
vladyslav@Client-2:~$ dig google.com

; <<>> DiG 9.18.1-1ubuntu1-Ubuntu <<>> google.com
;; global options: +cmd
;; connection timed out; no servers could be reached
```