1. На Server_1 налаштувати статичні адреси на всіх інтерфейсах.

```
[level1@oracle ~]$ 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:f7:3d:11 brd ff:ff:ff:ff:ff:ff
    inet 192.168.31.200/24 brd 192.168.31.255 scope global noprefixroute enp0s3
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fef7:3d11/64 scope link
       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 08:00:27:59:82:1e brd ff:ff:ff:ff:ff:ff
    inet 10.81.3.100/24 brd 10.81.3.255 scope global noprefixroute enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe59:821e/64 scope link
       valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:b0:a3:b2 brd ff:ff:ff:ff:ff:ff
    inet 10.6.81.100/24 brd 10.6.81.255 scope global noprefixroute enp0s9
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feb0:a3b2/64 scope link
       valid_lft forever preferred_lft forever
[level1@oracle ~]$
```

2. На Server_1 налаштувати DHCP сервіс, який буде конфігурувати адреси Int1 Client_1 та Client_2

```
[level1@oracle ~]$ sudo yum install dhcp-server
Last metadata expiration check: 3:08:47 ago on Thu 27 Oct 2022 05:51:45 AM EDT.
Dependencies resolved.
================================================================================
 Package                 Architecture            Version
================================================================================
Installing:
 dhcp-server             x86_64                  12:4.3.6-47.0.1.el8
Upgrading:
 bind-export-libs        x86_64                  32:9.11.36-3.el8_6.1
 dhcp-client             x86_64                  12:4.3.6-47.0.1.el8
 dhcp-common             noarch                  12:4.3.6-47.0.1.el8
 dhcp-libs               x86_64                  12:4.3.6-47.0.1.el8

Transaction Summary
================================================================================
Install  1 Package
Upgrade  4 Packages
```

```
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp-server/dhcpd.conf.example
#   see dhcpd.conf(5) man page
#
default-lease-time 600;
max-lease-time 7200;
ddns-update-style none;
authoritative;
subnet 10.81.3.0 netmask 255.255.255.0 {
range 10.81.3.50 10.81.3.60;
option routers 10.81.3.100;
option subnet-mask 255.255.255.0;
option domain-name-servers 8.8.8.8, 8.8.4.4;
}
```

Network settings on clients

```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=dhcp
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
NAME=enp0s3
DEVICE=enp0s3
ONBOOT=yes
```

3. За допомогою команд ping та traceroute перевірити зв'язок між віртуальними машинами. Результат пояснити.

```
[level1@server_1 ~]$ ping 10.81.3.50
PING 10.81.3.50 (10.81.3.50) 56(84) bytes of data.
64 bytes from 10.81.3.50: icmp_seq=1 ttl=64 time=0.071 ms
64 bytes from 10.81.3.50: icmp_seq=2 ttl=64 time=0.098 ms
64 bytes from 10.81.3.50: icmp_seq=3 ttl=64 time=0.047 ms
^C
--- 10.81.3.50 ping statistics ---
```

```
[level1@client_1 ~]$ ping 10.81.3.100
PING 10.81.3.100 (10.81.3.100) 56(84) bytes of data.
64 bytes from 10.81.3.100: icmp_seq=1 ttl=64 time=0.144 ms
64 bytes from 10.81.3.100: icmp_seq=2 ttl=64 time=0.096 ms
64 bytes from 10.81.3.100: icmp_seq=3 ttl=64 time=0.093 ms
64 bytes from 10.81.3.100: icmp_seq=4 ttl=64 time=0.053 ms
^C
--- 10.81.3.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
```

4. На віртуальному інтерфейсу lo Client_1 призначити дві IP адреси за таким правилом: 172.17.D+10.1/24 та 172.17.D+20.1/24. Налаштувати маршрутизацію таким чином, щоб трафік з Client_2 до 172.17.D+10.1 проходив через Server_1, а до 172.17.D+20.1 через Net4. Для перевірки використати traceroute.

```
[level1@client_1 ~]$ sudo ip a add 172.17.13.100/24 dev lo
[level1@client_1 ~]$ sudo ip a add 172.17.23.100/24 dev lo
[level1@client_1 ~]$ 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
    inet 172.17.13.100/24 scope global lo
       valid_lft forever preferred_lft forever
    inet 172.17.23.100/24 scope global lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
```

```
[level1@client_2 ~]$ sudo ip r add 172.17.13.0/24 via 10.6.81.100
[level1@client_2 ~]$ sudo ip r add 172.17.23.0/24 via 172.16.3.11
[level1@client_2 ~]$ ip r
10.6.81.0/24 dev enp0s3 proto kernel scope link src 10.6.81.50
172.16.3.0/24 dev enp0s8 proto kernel scope link src 172.16.3.12
172.17.13.0/24 via 10.6.81.100 dev enp0s3
172.17.23.0/24 via 172.16.3.11 dev enp0s8
[level1@client_2 ~]$
```

5. Розрахувати спільну адресу та маску (summarizing) адрес 172.17.D+10.1 та 172.17.D+20.1, при чому префікс має бути максимально можливим. Видалити маршрути, встановлені на попередньому кроці та замінити їх об’єднаним маршрутом, який має проходити через Server_1.

```
[level1@client_2 ~]$ sudo ip r add 172.17.0.0/19 via 10.6.81.100
[level1@client_2 ~]$ ip r
10.6.81.0/24 dev enp0s3 proto kernel scope link src 10.6.81.50
172.16.3.0/24 dev enp0s8 proto kernel scope link src 172.16.3.12
172.17.0.0/19 via 10.6.81.100 dev enp0s3
[level1@client_2 ~]$ traceroute 172.17.13.100
traceroute to 172.17.13.100 (172.17.13.100), 30 hops max, 60 byte packets
 1  client_2 (10.6.81.50)  3068.950 ms !H  3068.489 ms !H  3068.469 ms !H
```

6. Налаштувати SSH сервіс таким чином, щоб Client_1 та Client_2 могли підключатись до Server_1 та один до одного.

```
[level1@server_1 ~]$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/level1/.ssh/id_rsa):
Created directory '/home/level1/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/level1/.ssh/id_rsa.
Your public key has been saved in /home/level1/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:yEUcRxITPLpKEBI7110OX5z4x6YNeNrTDlzJFkWbq9A level1@server_1
The key's randomart image is:
+---[RSA 3072]----+
|..     .oB=o.o    |
|.... + ++= . o    |
|o...+ o.=.. o     |
| o.  +.* + o .    |
|   .  =.S E .     |
|    . .= @ .      |
|   . .. * +       |
|    .    +        |
|          .       |
+----[SHA256]-----+
[level1@server_1 ~]$
```

```
[level1@server_1 ~]$ ssh-copy-id -i /home/level1/.ssh/id_rsa.pub level1@10.6.81.50
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/level1/.ssh/id_rsa.pub"
ECDSA key fingerprint is SHA256:2S9FMKCQWMlOq/JyiIGdJnAzOSUBzt1DDI/4dzsRpEI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
level1@10.6.81.50 133's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'level1@10.6.81.50'"
and check to make sure that only the key(s) you wanted were added.

[level1@server_1 ~]$ ssh -i /home/level1/.ssh/id_rsa level1@10.6.81.50
Last login: Thu Oct 27 13:21:13 2022
[level1@client_2 ~]$ exit
logout
[level1@server_1 ~]$ ssh level1@10.6.81.50
[level1@client_2 ~]$
```

```
Enter same passphrase again:
Your identification has been saved in /home/level1/.ssh/id_rsa.
Your public key has been saved in /home/level1/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:bBPZ5edVLAZ61/709TS1A/tNI8Davu+CfE2PZ8NQqCU level1@client_2
The key's randomart image is:
+---[RSA 3072]----+
|           o. ..|
|         o.+  o.o|
|        o oooo=.o|
|       . .oE.Booo|
|        S. .+o+==|
|       . ... oo=O|
|        . ..o =.=|
|         o o.o * |
|          ..+oo .|
+----[SHA256]-----+
[level1@client_2 ~]$ ssh-copy-id -i /home/level1/.ssh/id_rsa.pub level1@192.168.31.200
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/level1/.ssh/id_rsa.pub"
The authenticity of host '192.168.31.200 (192.168.31.200)' can't be established.
ECDSA key fingerprint is SHA256:2S9FMKCQWM1Oq/JyiIGdJnAzOSUBzt1DDI/4dzsRpEI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are alr
eady installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to inst
all the new keys
level1@192.168.31.200's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'level1@192.168.31.200'"
and check to make sure that only the key(s) you wanted were added.
```

7. Налаштуйте на Server_1 firewall таким чином:

• Дозволено підключатись через SSH з Client_1 та заборонено з Client_2

• З Client_2 на 172.17.D+10.1 ping проходив, а на 172.17.D+20.1 не проходив

```
[level1@server_1 ~]$ sudo iptables -A INPUT  -p tcp -s 10.6.81.50/32 --dport 22 -j DROP
[level1@server_1 ~]$ sudo iptables -A INPUT  -p icmp -s 10.6.81.50/32  -d 172.16.23.1/32  -j DROP
[level1@server_1 ~]$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  10.6.81.50           anywhere             tcp dpt:ssh
DROP       icmp --  10.6.81.50           172.16.23.1

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[level1@server_1 ~]$
```

8. Якщо в п.3 була налаштована маршрутизація для доступу Client_1 та Client_2 до мережі Інтернет – видалити відповідні записи. На Server_1 налаштувати NAT сервіс таким чином, щоб з Client_1 та Client_2 проходив ping в мережу Інтернет

```
[level1@server_1 ~]$ sudo iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE
[level1@server_1 ~]$ sudo iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
[level1@server_1 ~]$
```

```
level1@client_2 ~]$ ping goo.gl
PING goo.gl (216.58.215.78) 56(84) bytes of data.
64 bytes from waw02s16-in-f14.1e100.net (216.58.215.78): icmp_seq=1 ttl=116 time=20.1 ms
64 bytes from waw02s16-in-f14.1e100.net (216.58.215.78): icmp_seq=2 ttl=116 time=19.8 ms
64 bytes from waw02s16-in-f14.1e100.net (216.58.215.78): icmp_seq=3 ttl=116 time=19.8 ms
64 bytes from waw02s16-in-f14.1e100.net (216.58.215.78): icmp_seq=4 ttl=116 time=20.5 ms
^C
--- goo.gl ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 19.810/20.059/20.536/0.324 ms
level1@client_2 ~]$ _
```