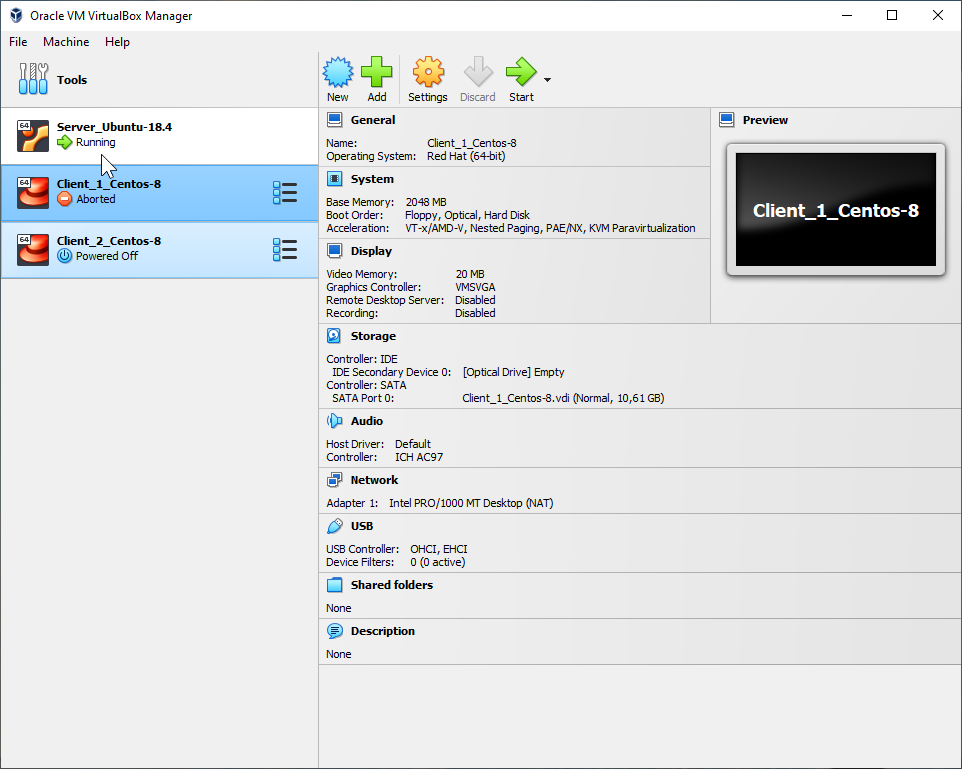
**EPAM University Programs DevOps external course**

**Module – Linux Networking**

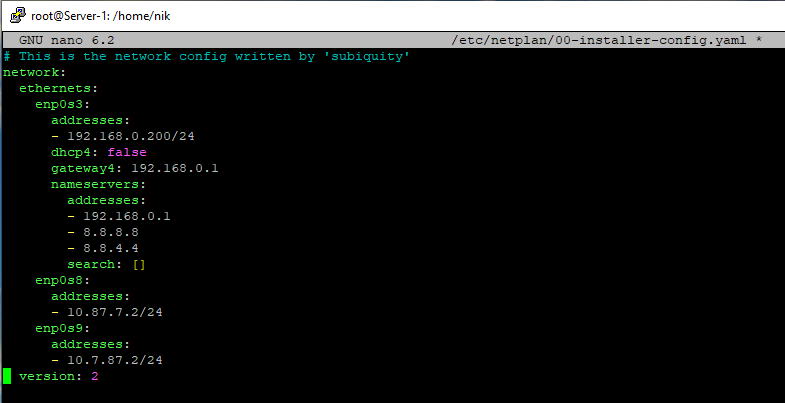


**Configuring DHCP server**

Client\_1 та Client\_2 – Віртуальні машини, на яких розгорнуто ОС Linux (бажано різні дистрибутиви, наприклад Ubuntu та CentOS). Інтерфейси підключені в режимі «Внутрішня мережа» до мереж Net2, Net3 та Net4 як показано на рисунку 1. Адреса мережі Net2 – 10.Y.D.0/24, де Y – дві останні цифри з вашого року народження, D – дата народження. Адреса мережі Net3 – 10.M.Y.0/24, де M – номер місяця народження. Адреса мережі Net4 – 172.16.D.0/24. Увага! Якщо, адресний простір Net2, Net3 або Net4 перетинається з адресним простором Net1 – відповідну адресу можна змінити на власний розсуд.

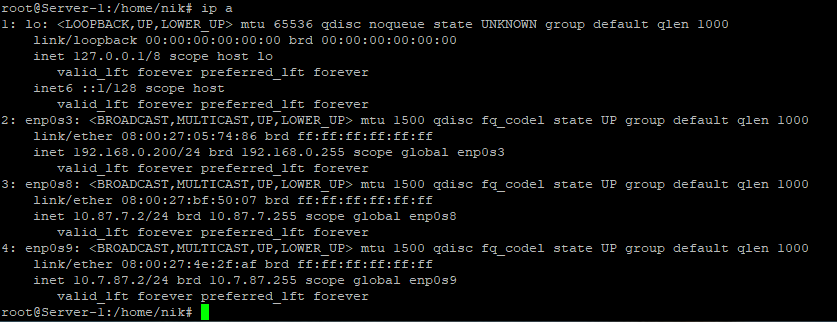
**1. На Server\_1 налаштувати статичні адреси на всіх інтерфейсах.**

nano /etc/netplan/00-installer-config.yaml

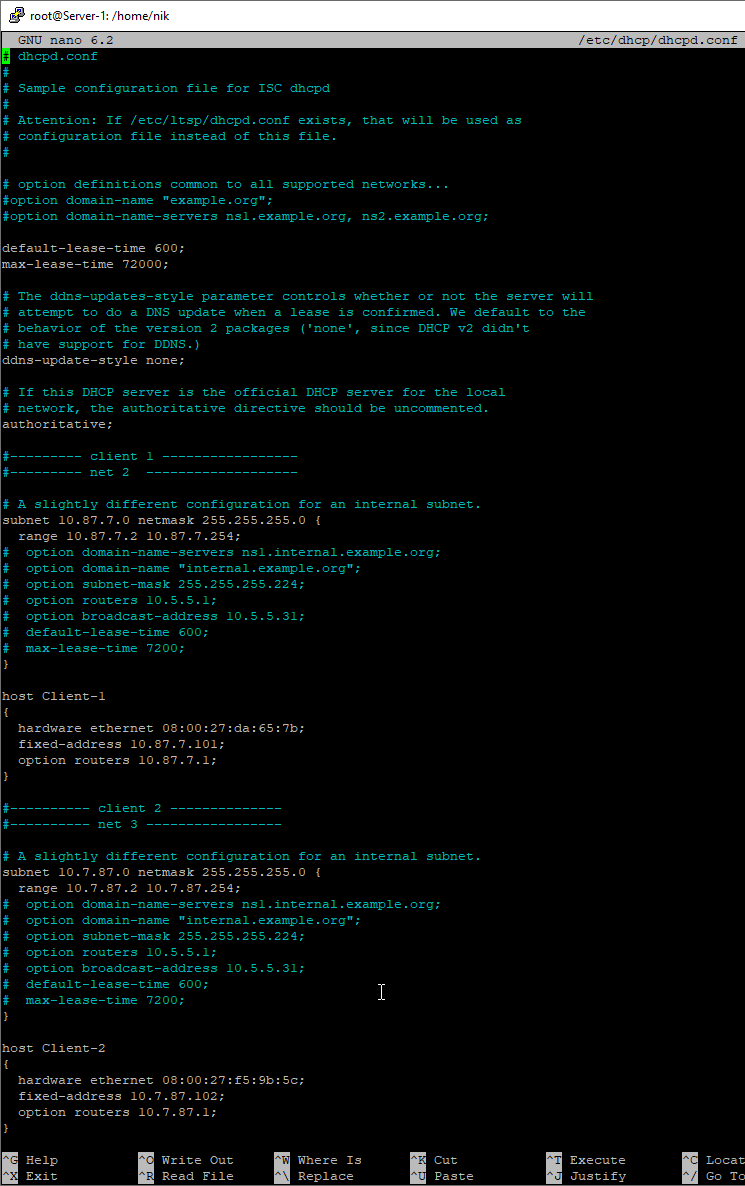


Ip interface can’t finish on “0” – addr subnet and “1” - gateway

Netplan apply



**2. На Server\_1 налаштувати DHCP сервіс, який буде конфігурувати адреси Int1 Client\_1 та Client\_2**

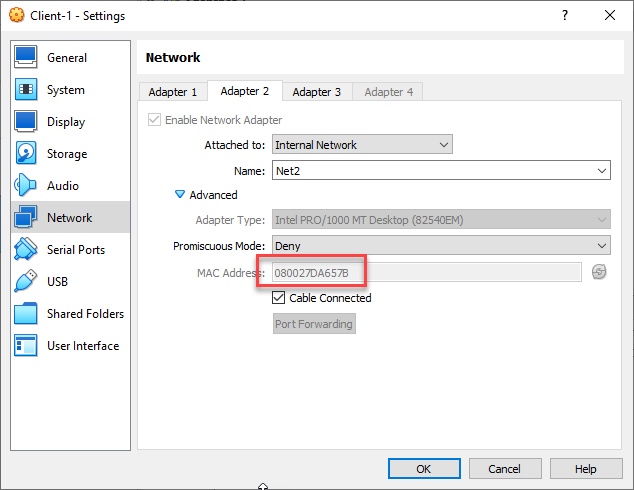
nano /etc/dhcp/dhcpd.conf

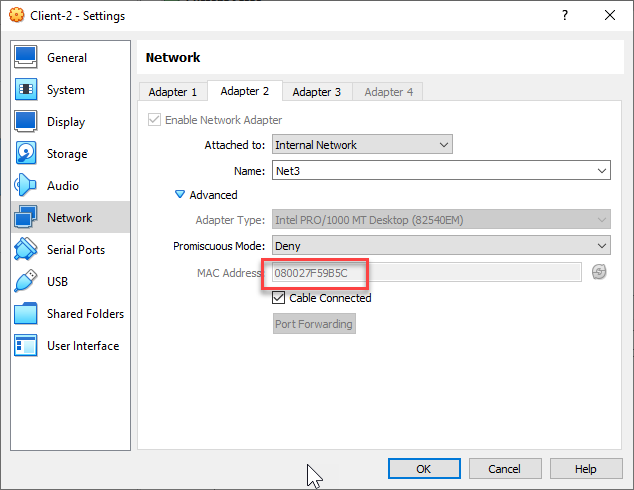
**systemctl restart isc-dhcp-server**

**hardware ethernet – MAC address of interface client VM**

**fixed-address - IP address of interface client VM**

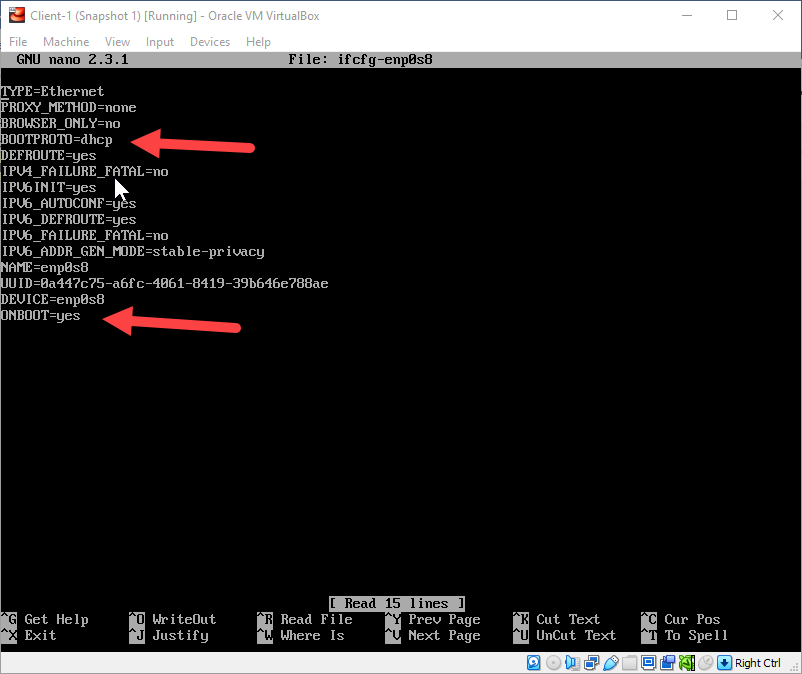
**option routers - gateway address of interface client VM**

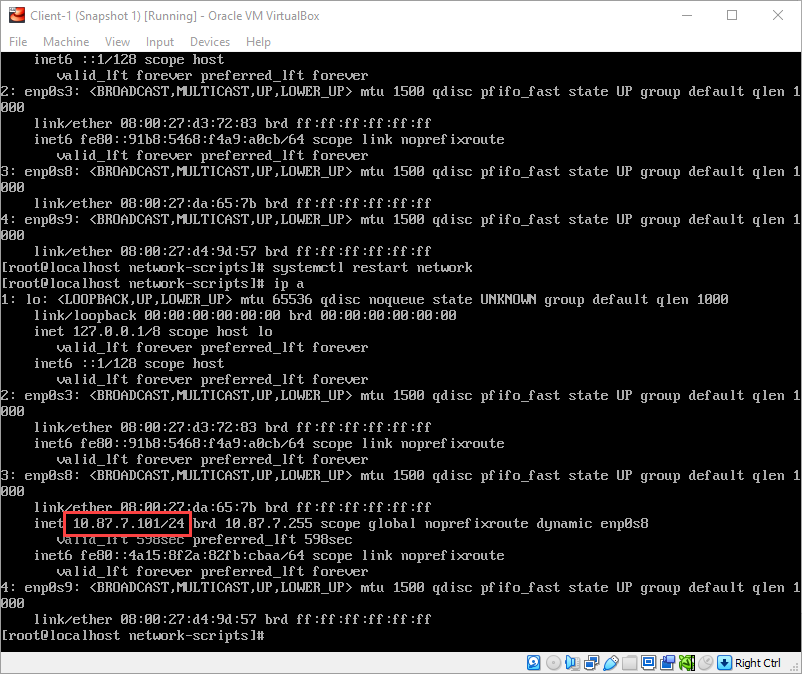




**Client-1**

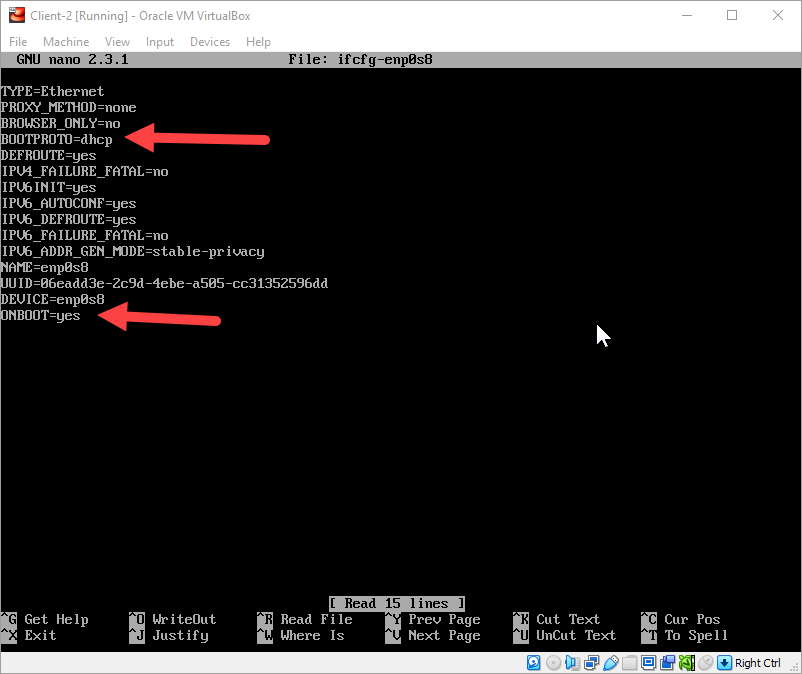
**cd /etc/sysconfig/network-scripts**

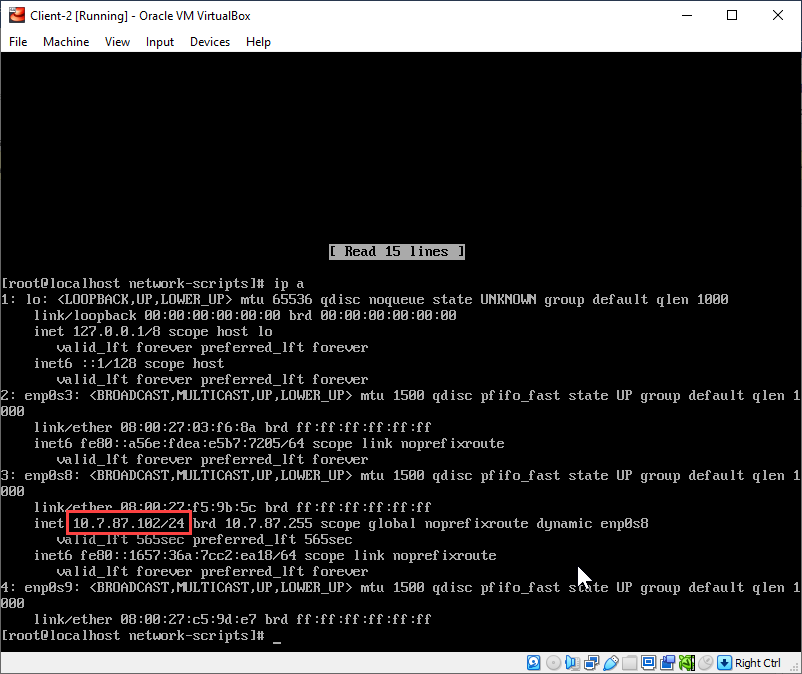




**systemctl restart network**

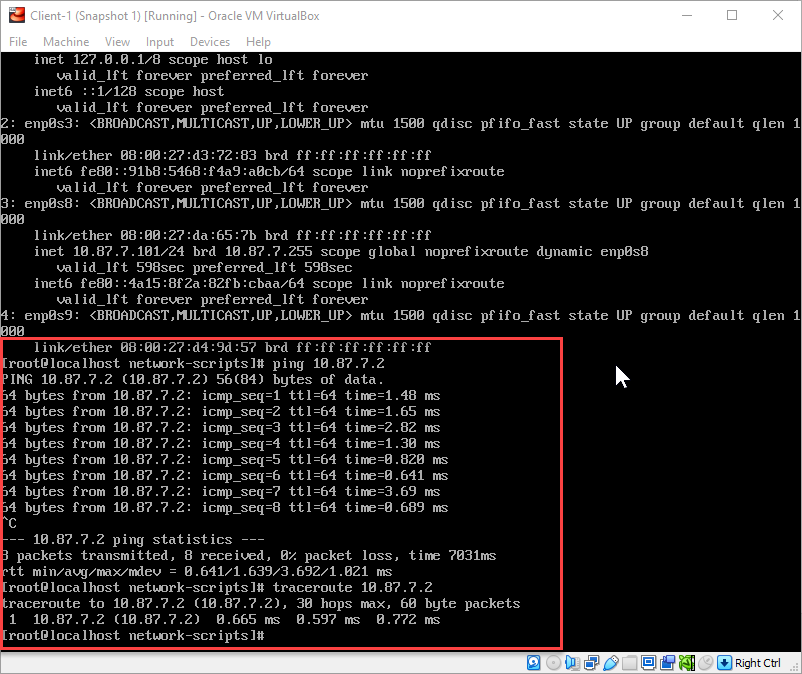
**Client-2**



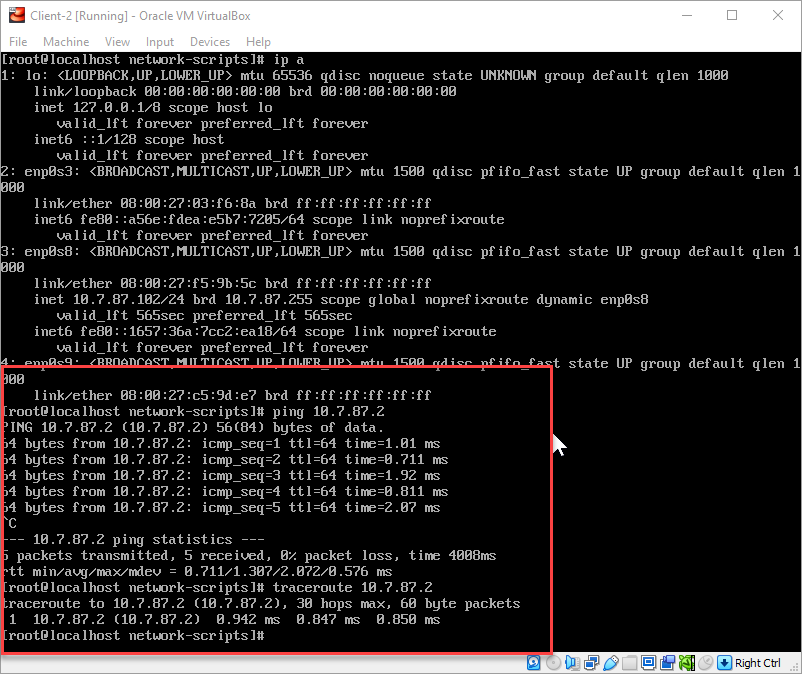


**3. За допомогою команд ping та traceroute перевірити зв'язок між віртуальними машинами. Результат пояснити.**

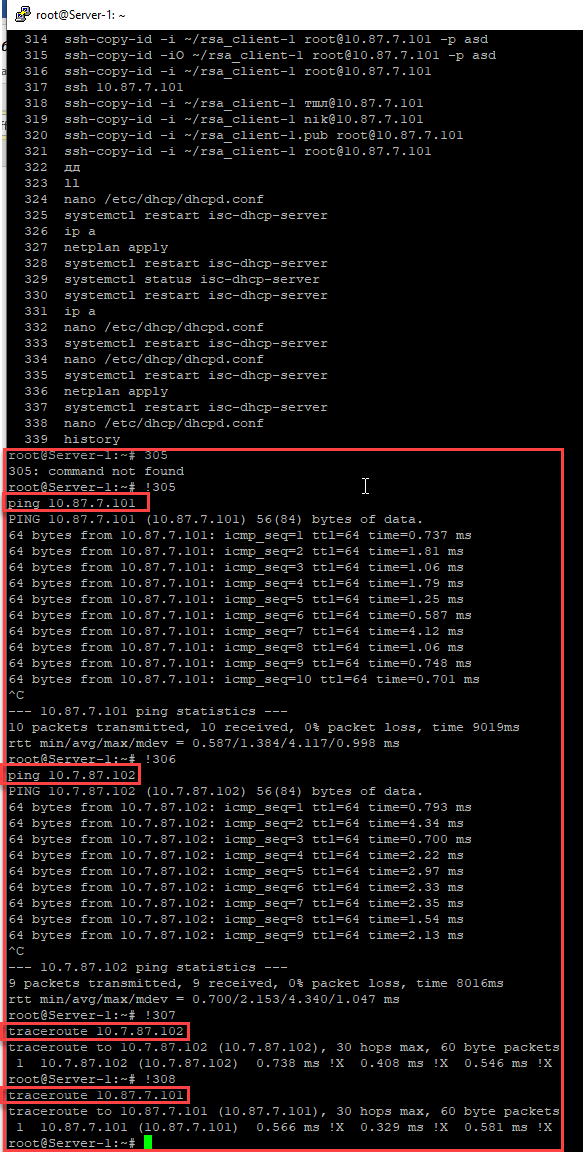
**Client-1 Ping to Server-1**



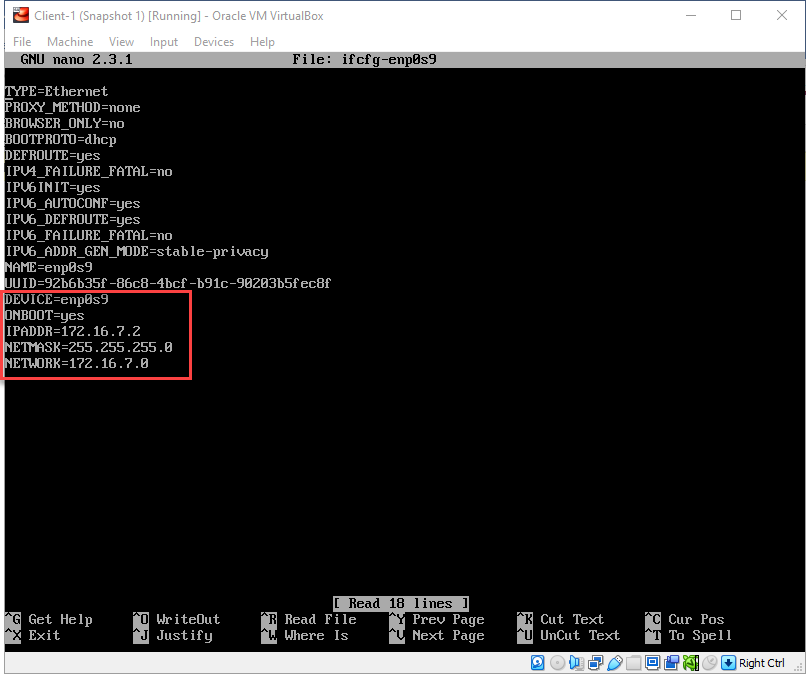
**Client-2 Ping to Server-1**

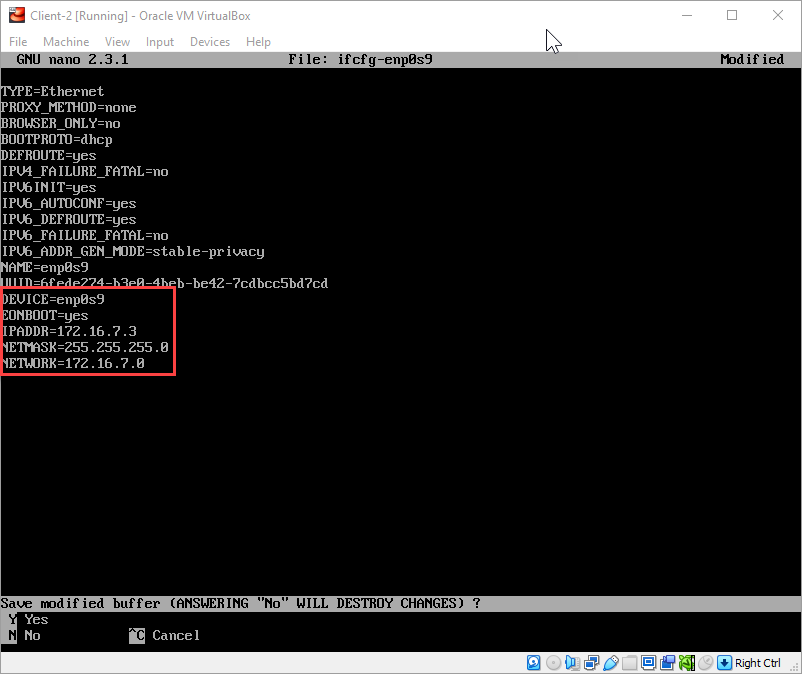


**Ping and traceroute to Client-1 and Client-2 from Server-1**

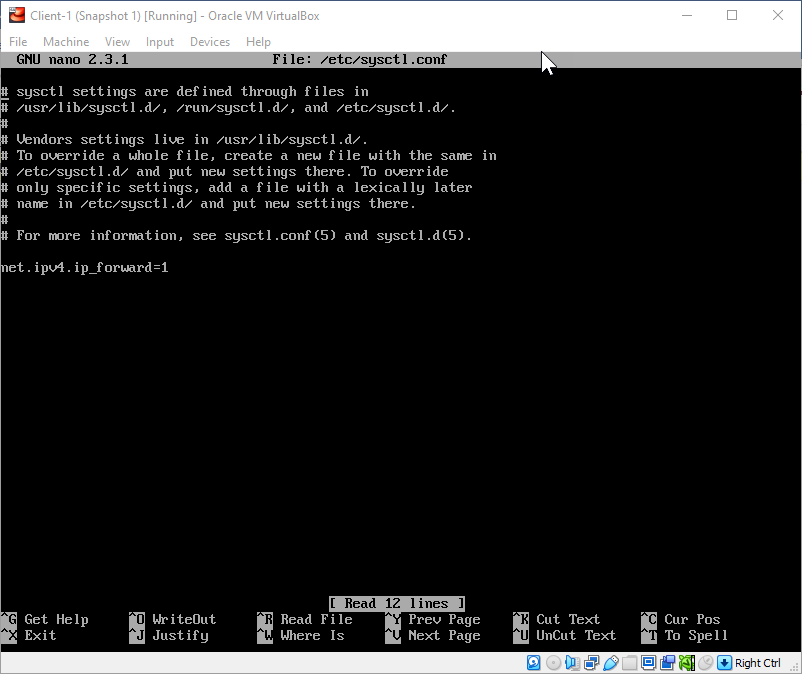


**Net 4**





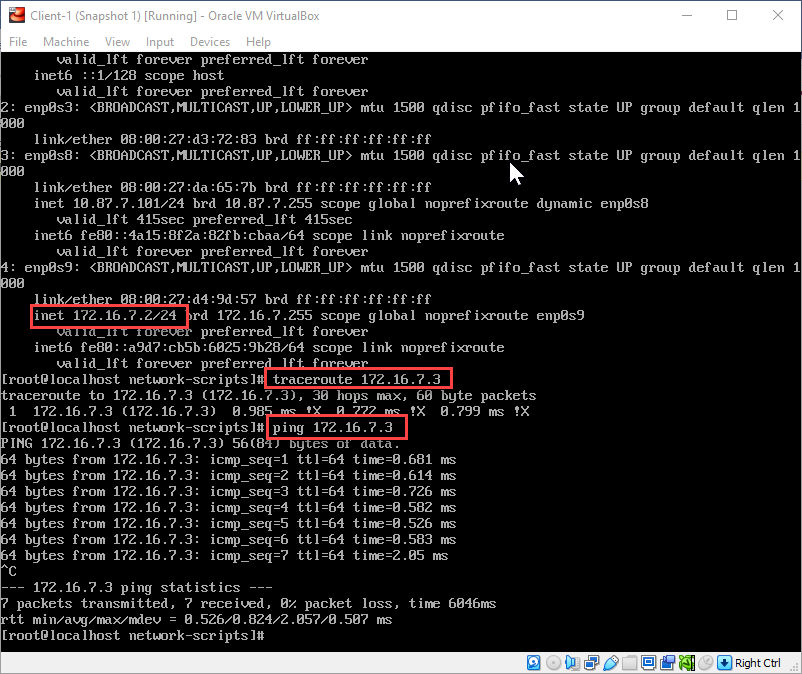
**nano /etc/sysctl.conf**



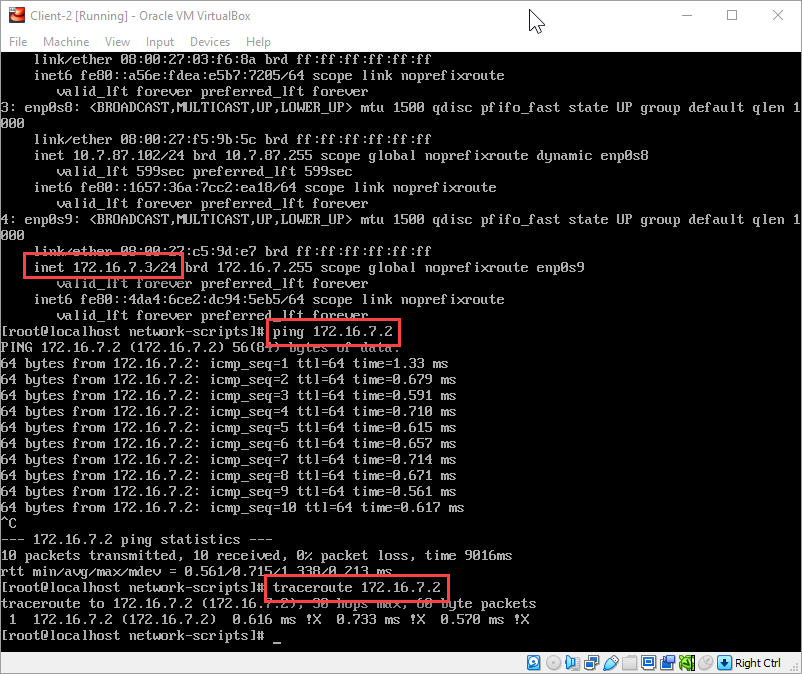
**net.ipv4.ip\_forward=1**

**net.ipv6.conf.all.forwarding=1**

**systemctl restart network**



**For work connection between two VM you need set forward=1 all VM !!!**

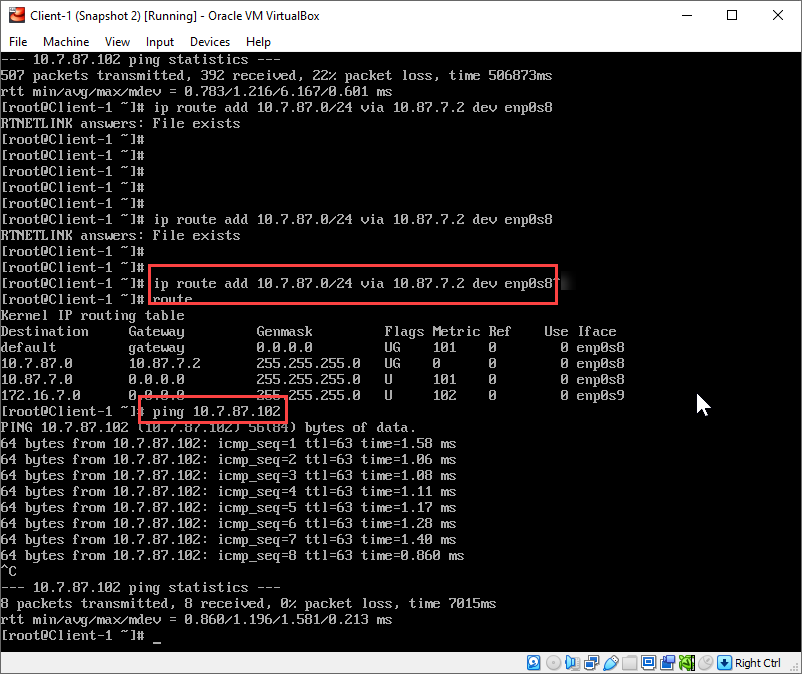


**Ping Client-1 🡪 Server-1 🡪 Client-2**

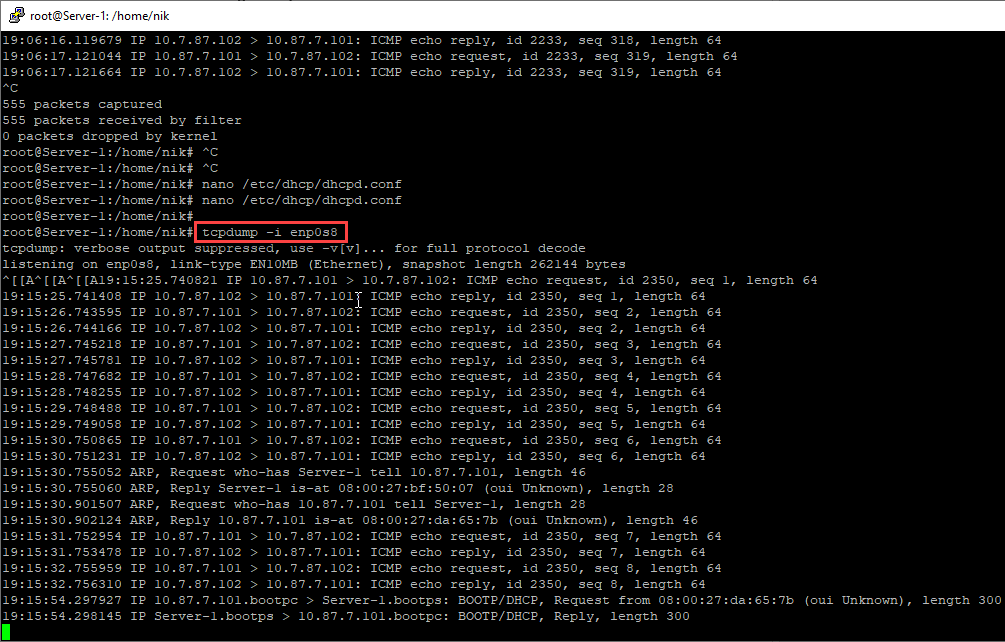
**Ip route add 10.7.87.0/24 via 10.87.7.2 dev enp0s8**

**10.7.87.0/24 – subnet which we want to go**

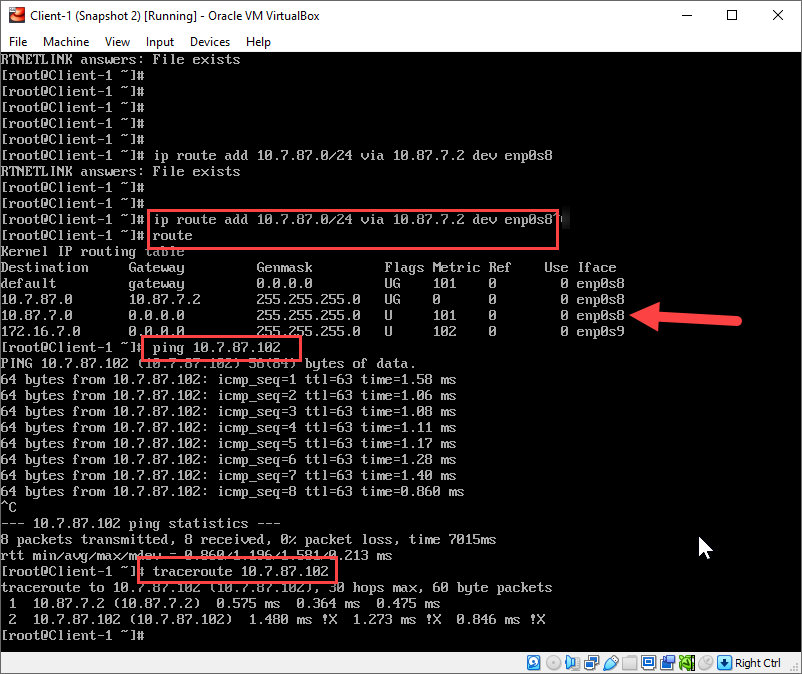
**10.87.7.2 – IP addr of interface on Server for Client-1 subnet**



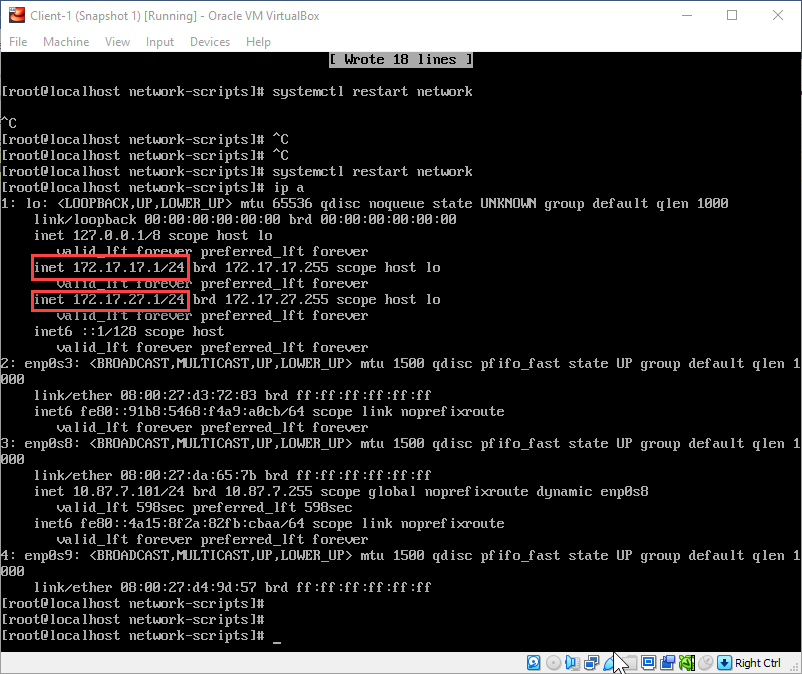
**Check receiving tcp packages: tcpdump -i enp0s8**



**Client-2 Where we want to go**



**4 На віртуальному інтерфейсу lo Client\_1 призначити дві ІР адреси за таким правилом: 172.17.D+10.1/24 та 172.17.D+20.1/24.**



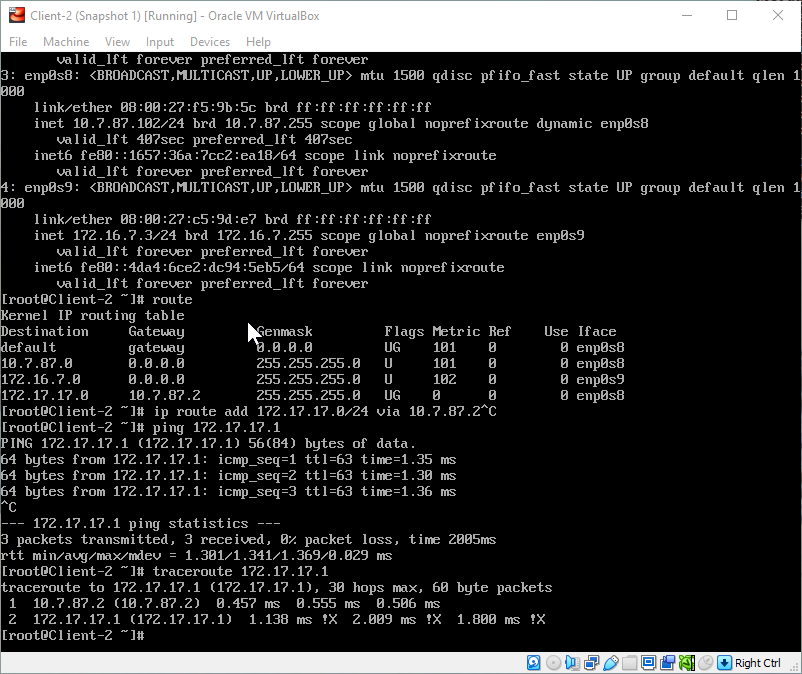
**4.1 Налаштувати маршрутизацію таким чином, щоб трафік з Client\_2 до 172.17.D+10.1 проходив через Server\_1**

**On client-2:**

**Ip route add 172.17.17.0/24 via 10.7.87.2**

**172.17.17.0/24 – subnet on client-1 in interface lo**

**10.7.87.2 – ip interface for client-2 subnet on server**

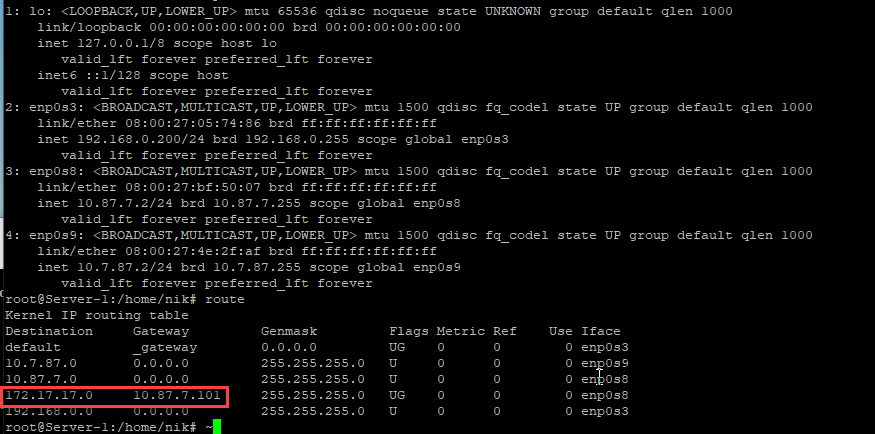


**On Server:**

**ip route add 172.17.17.0/24 via 10.87.7.101**

**172.17.17.0/24 – subnet on client-1 in interface lo**

**10.87.7.101– ip interface – enp0s8 in Client-1**

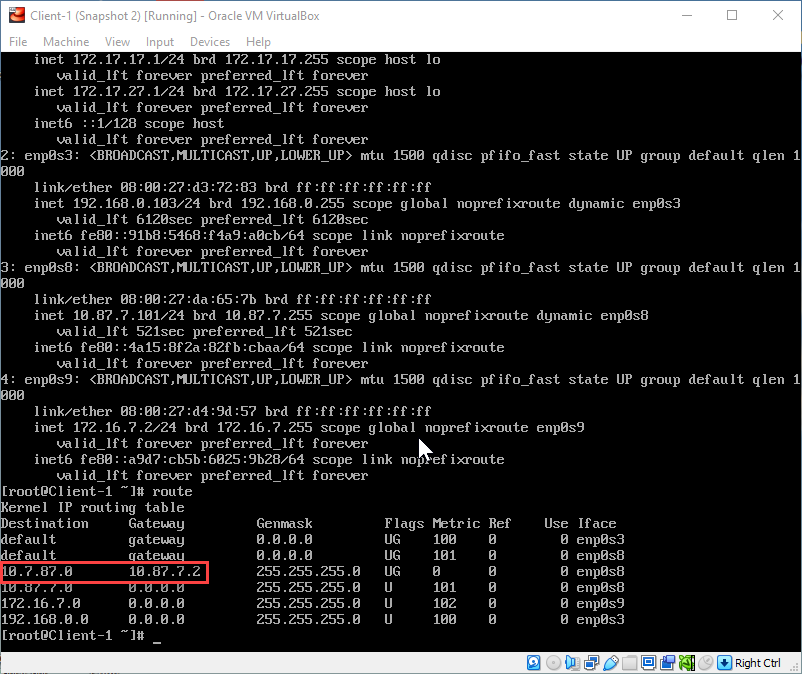


**On Client-1**

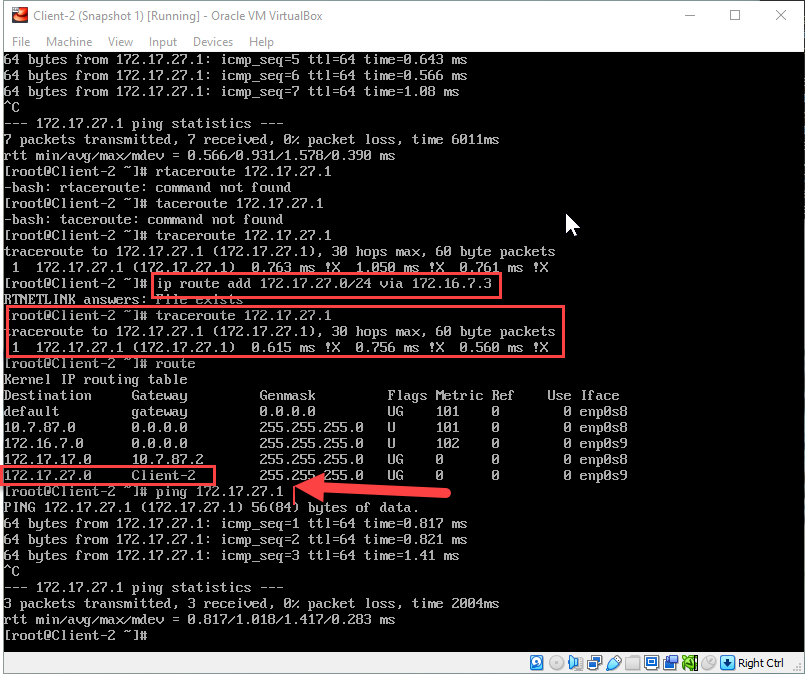
**Ip route add 10.7.87.0/24 via 10.87.7.2 dev enp0s8**

**10.7.87.0/24 – subnet which we want to go**

**10.87.7.2 – IP addr of interface on Server for Client-1 subnet**



**4.2 Налаштувати маршрутизацію таким чином, щоб трафік з Client\_2 до 172.17.D+10.1 проходив через Net4. Для перевірки використати traceroute.**



**On client-2:**

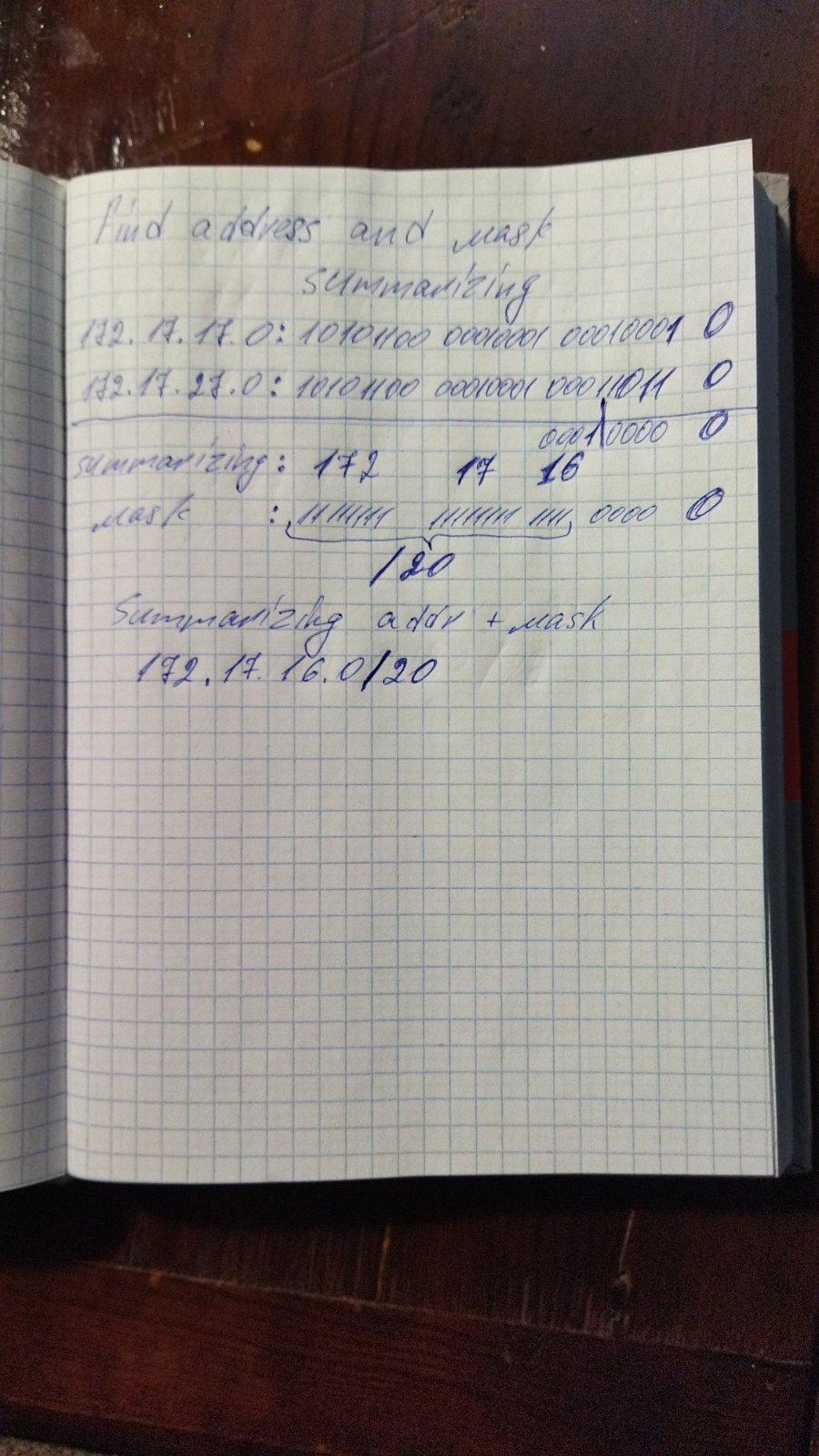
**Ip route add 172.17.27.0/24 via 172.16.7.3**

**172.17.27.0/24 – subnet on client-1 in interface lo**

**172.16.7.3 – subnet between client-1 and client-2 and interface enp0s9**

**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, якій має проходити через Server\_1.**

**5.1 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.**



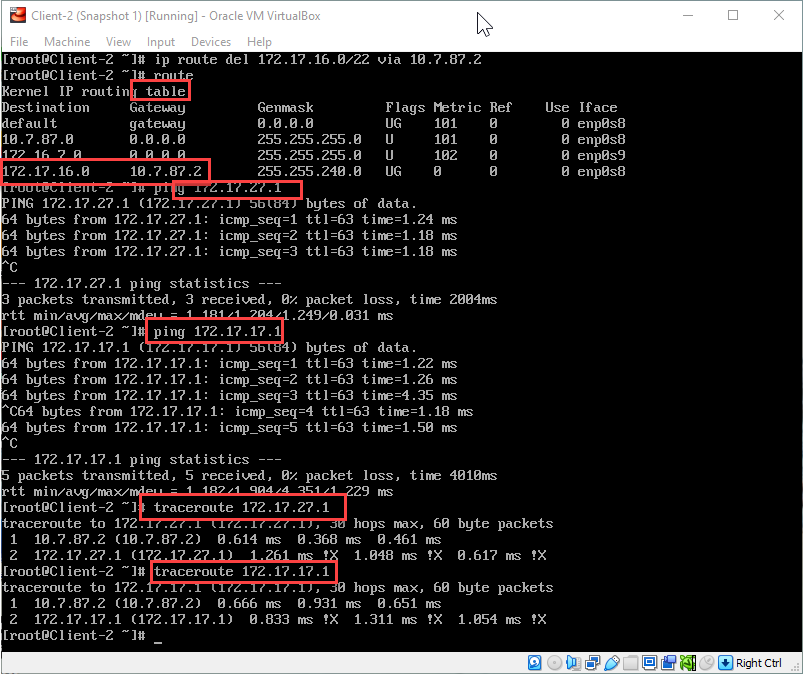
**5.2 Видалити маршрути, встановлені на попередньому кроці та замінити їх об’єднаним маршрутом, якій має проходити через Server\_1.**

**On client-2:**

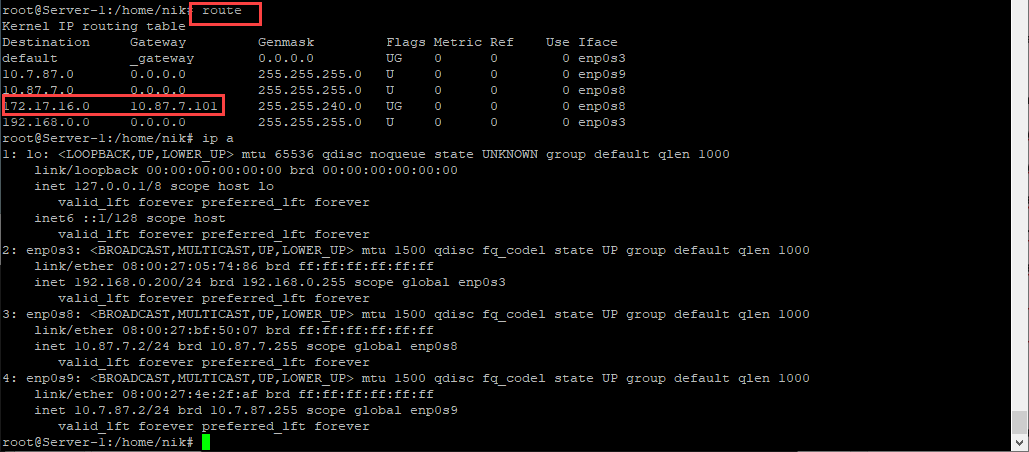
**Ip route add 172.17.16.0/20 via 10.7.87.2**

**172.17.16.0/20 – summarizing subnet for 172.17.17.0 and 172.17.27.0 on client-1 in interface lo**

**10.7.87.2 – IP addr of interface on Server for Client-2 subnet**



**On Server**

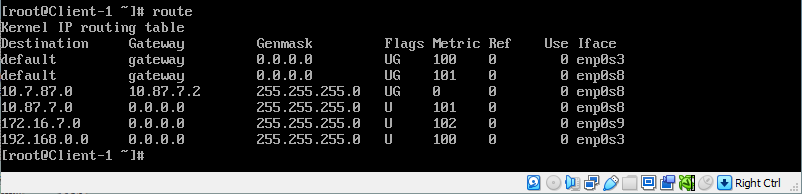


**ip route add 172.17.16.0/20 via 10.87.7.101**

**172.17.16.0/20 – summarizing subnet for 172.17.17.0 and 172.17.27.0 on client-1 in interface lo**

**10.87.7.101– ip interface – enp0s8 in Client-1**

**On Client-1**



**Ip route add 10.7.87.0/24 via 10.87.7.2 dev enp0s8**

**10.7.87.0/24 – subnet which we want to go**

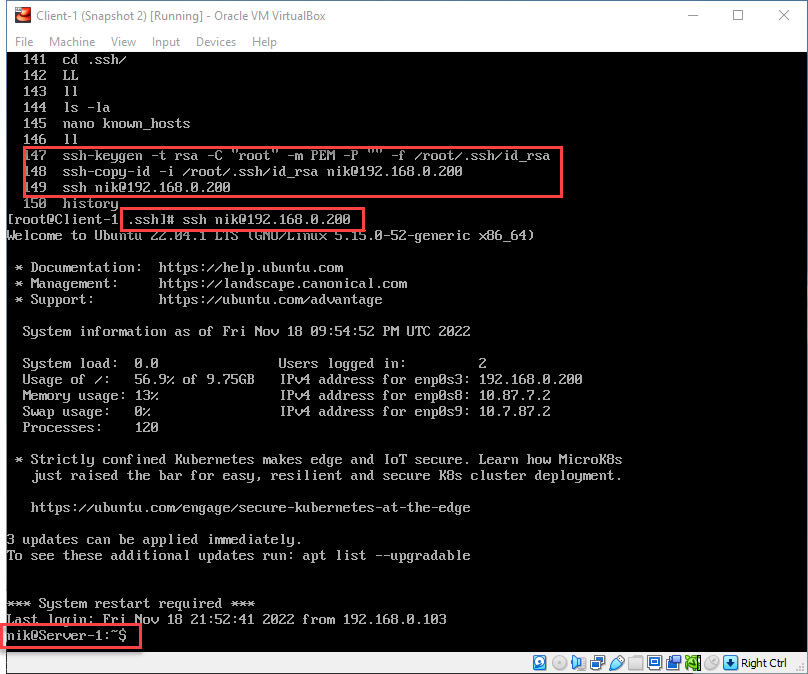
**10.87.7.2 – IP addr of interface on Server for Client-1 subnet**

**6 Налаштувати SSH сервіс таким чином, щоб Client\_1 та Client\_2 могли підключатись до Server\_1 та один до одного.**

**Ssh connection Client-1 to Server**

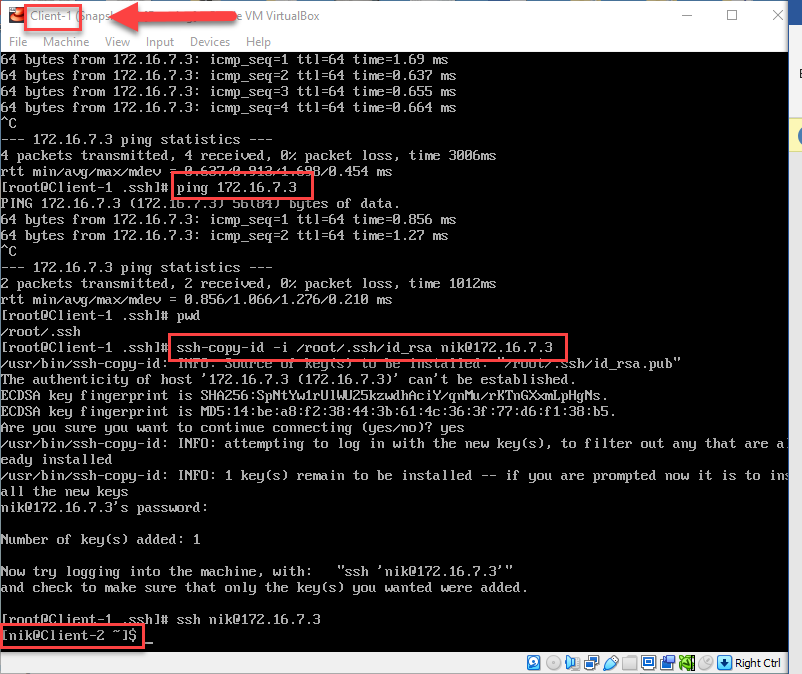
**ssh-keygen -t rsa -C "nik" -m PEM -P "" -f /root/.ssh/id\_rsa**

**ssh-copy-id -i /root/.ssh/id\_rsa root@192.168.0.200**



**Ssh connection Client-1 to Client-2**

**ssh-copy-id -i /root/.ssh/id\_rsa root@172.16.7.3**



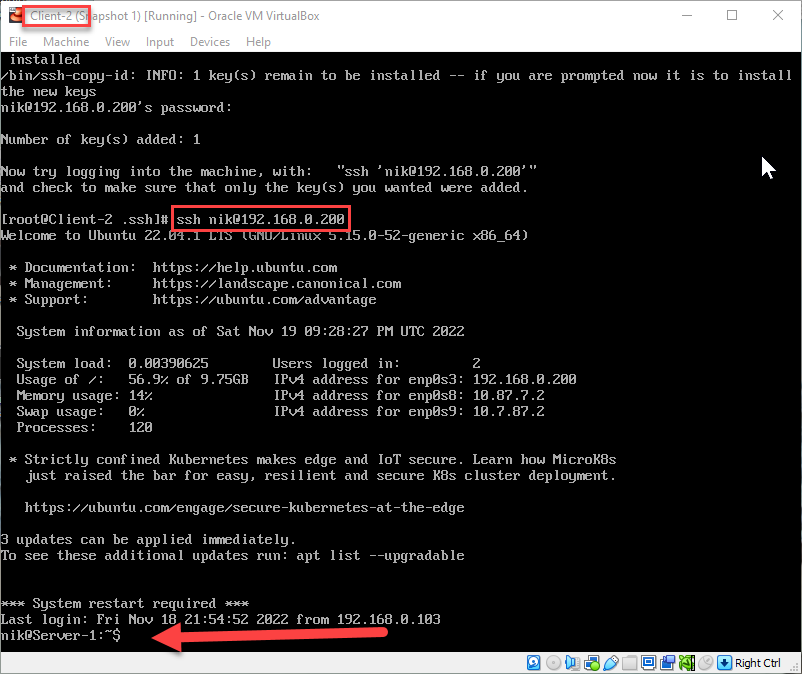
**Ssh connection Client-2 to Server**

**Ip route add 192.168.0.0/24 via 10.7.87.102**

**Route from subnet of Server to interface IP of Client-2**

**ssh-keygen -t rsa -C "nik" -m PEM -P "" -f /root/.ssh/id\_rsa**

**ssh-copy-id -i /root/.ssh/id\_rsa root@192.168.0.200**



**7 Налаштуйте на Server\_1 iptables**

**Iptables -L**

**# table of input trafic**

**Chain INPUT (policy ACCEPT)**

**target prot opt source destination**

**# table of passing trafic**

**Chain FORWARD (policy ACCEPT)**

**target prot opt source destination**

**# frafic that create uor Server**

**Chain OUTPUT (policy ACCEPT)**

**target prot opt source destination**

**ACCEPT – allow**

**DROP – refuse**

**ADD RULES. RULES ADD in chain order !!!!**

**# Allow all connections that were before**

**iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT**

**# Allow ssh access to 22 port**

**Iptables -A INPUT -p tcp –dport ssh -j ACCEPT**

**# Refuse ALL traffic**

**Iptables -A INPUT -j DROP**

**# If we forget to add some rule! Add icmp in chain before ssh rule!**

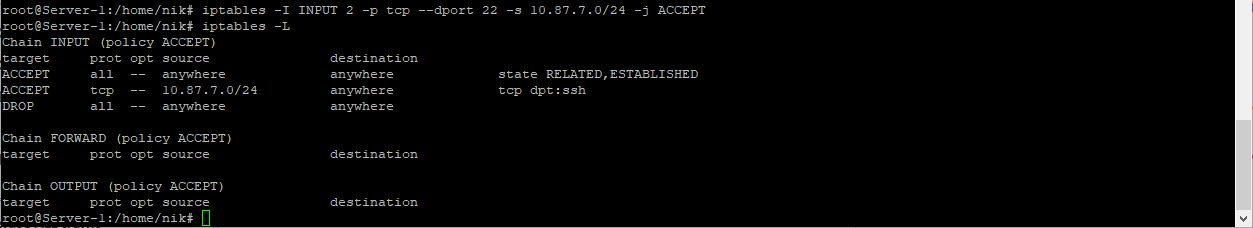
**Iptables -I INPUT 2 -p icmp -j ACCEPT**

**# Delete or Drop rules**

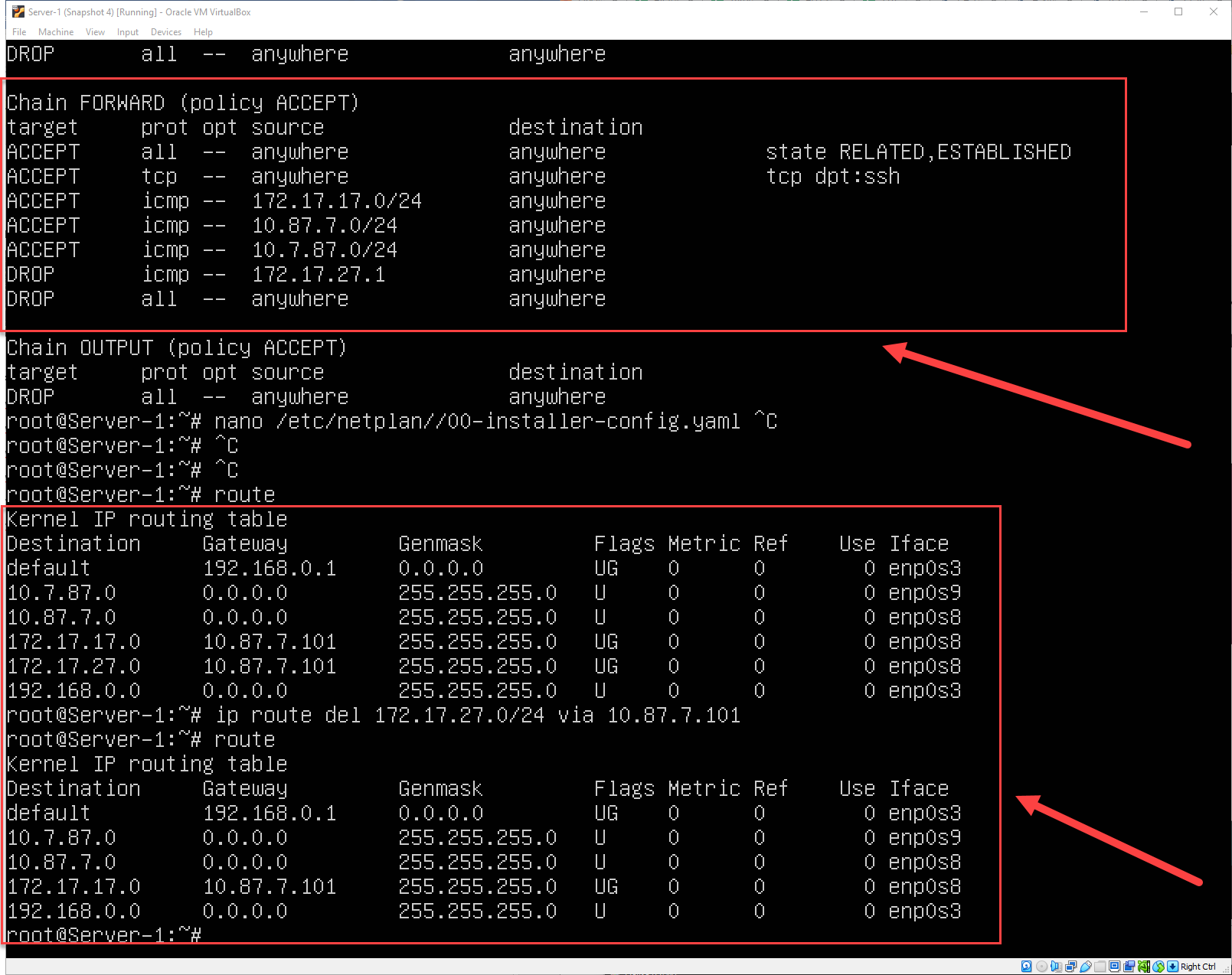
**Iptables -D INPUT 2**

**Iptables -D INPUT -p icmp -j ACCEPT**

**7.1 Дозволено підключатись через SSH з Client\_1 та заборонено з Client\_2**



**7.2 З Client\_2 на 172.17.D+10.1 ping проходив, а на 172.17.D+20.1 не проходив**



**Any rules in iptables can’t halp!**

**Only separate routes on two subnets:**

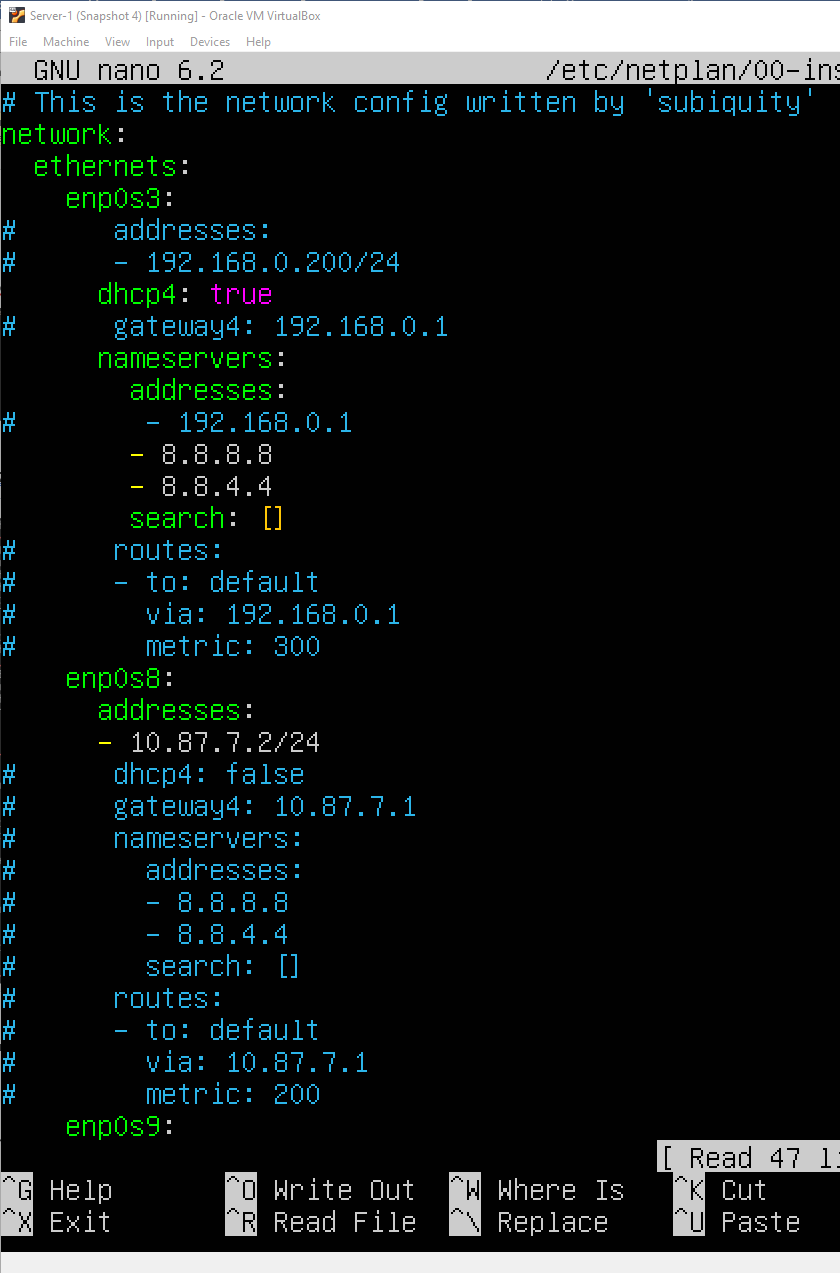
**172.17.17.0/24**

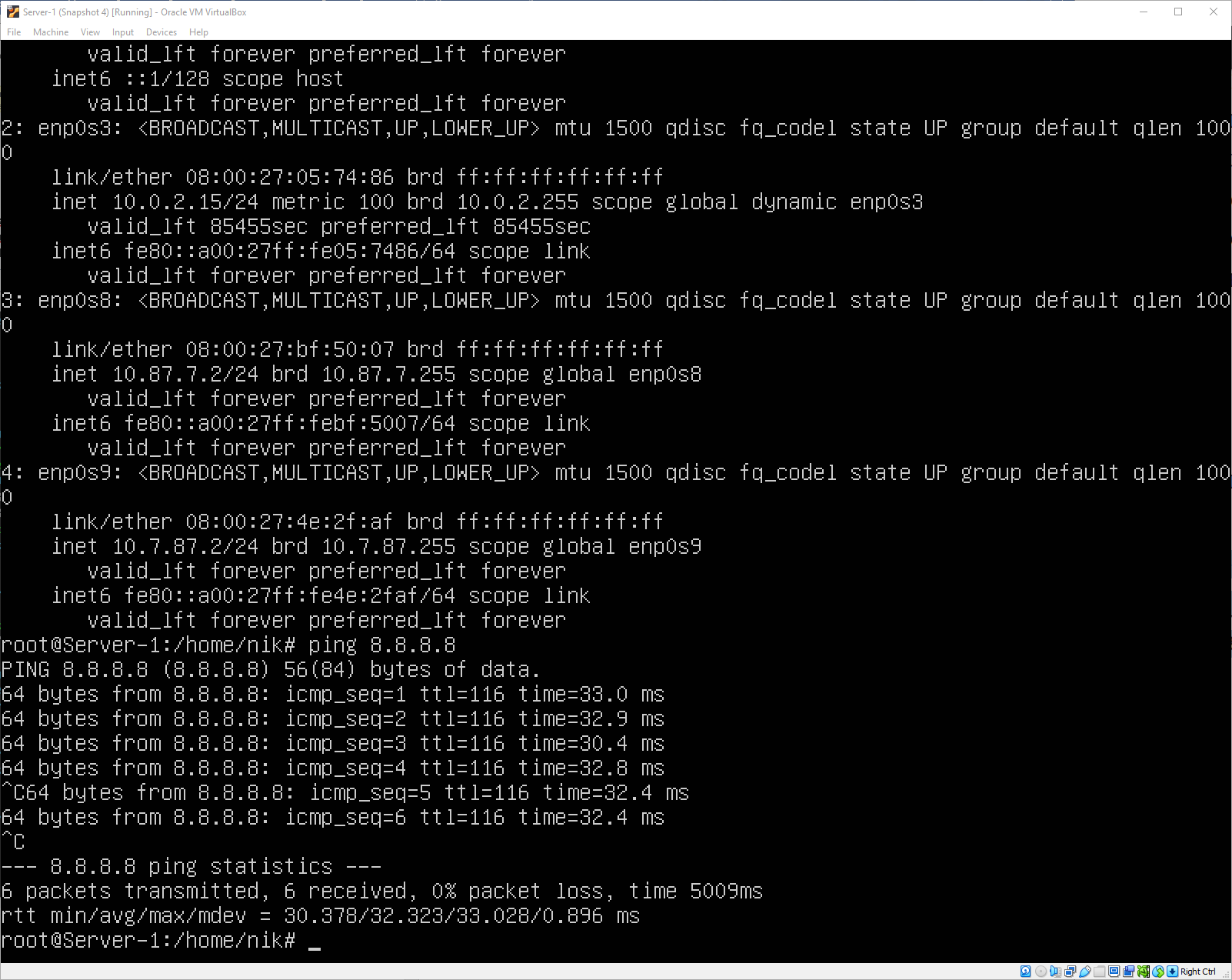
**172.17.27.0/24**

**And then delete forward route to second one!**

**NAT**

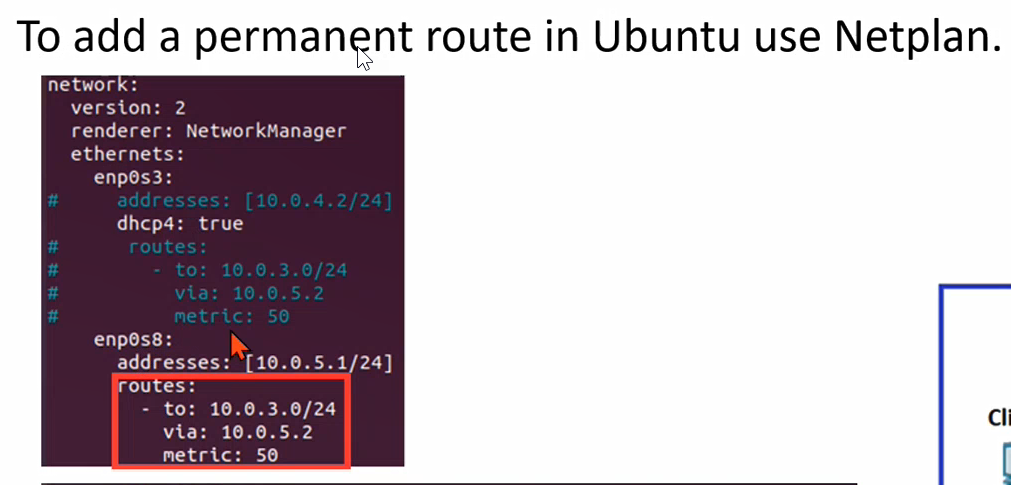
**8 Якщо в п.3 була налаштована маршрутизація для доступу Client\_1 та Client\_2 до мережі Інтернет – видалити відповідні записи. На Server\_1 налаштувати NAT сервіс таким чином, щоб з Client\_1 та Client\_2 проходив ping в мережу Інтернет**





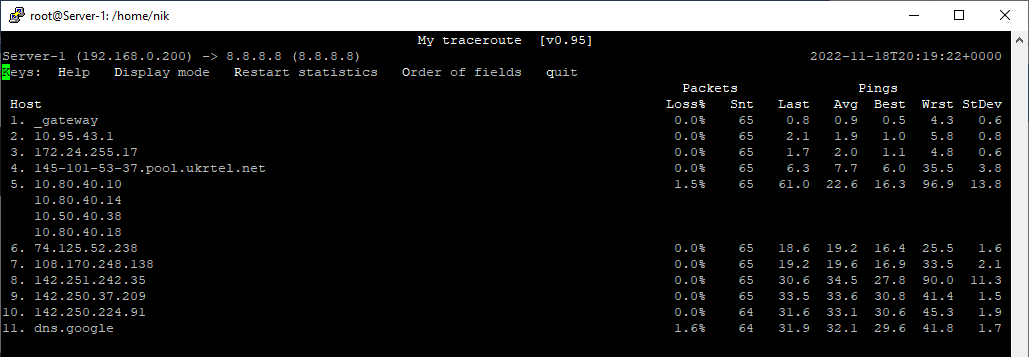
**Iptables -t nat -L**

**Iptables -t nat -A POSTROUTING -s 10.0.0.0/16 -j SNAT –to-source 10.0.2.15**

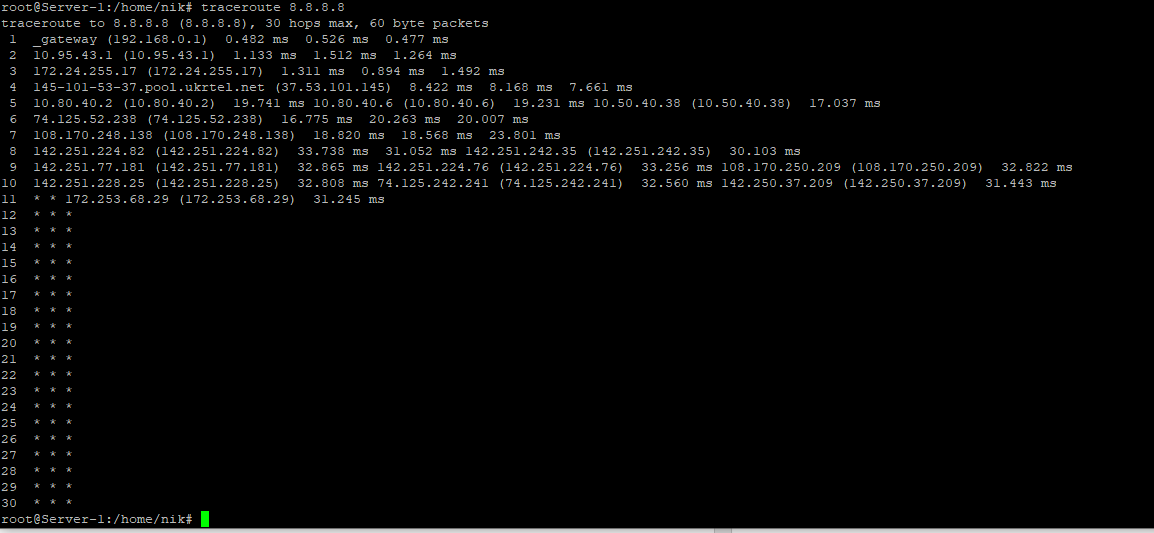


**Troubleshooting or find out of problems**

**Apt install -y mtr**

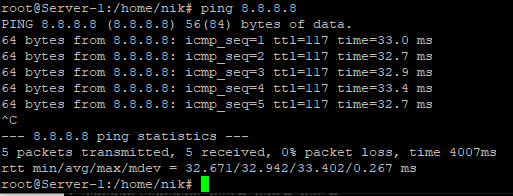


**Traceroute**

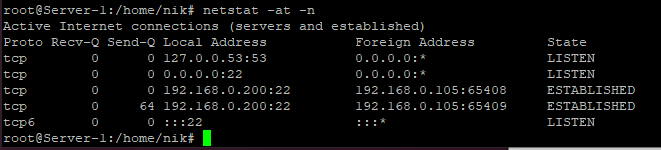


* **Не разрешает себя проверять сеть или подсеть (не возвращает некрологи)**

**Ping – Network layer**



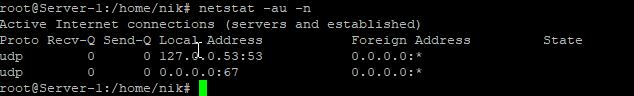
**Netstat -at -n show tcp**



**Port 22 – SSH**

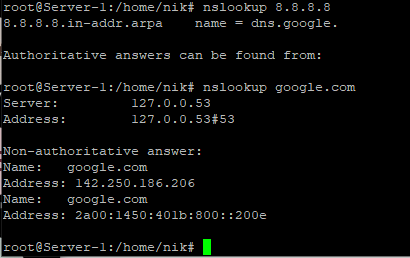
**Port 53 – DNS**

**Netstat -au -n show udp**

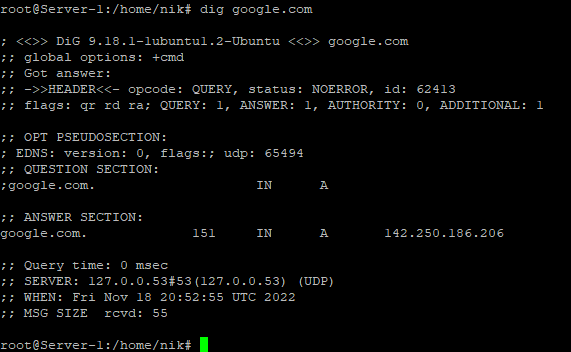


**Port 67 - DHCP**

**Nslookup**

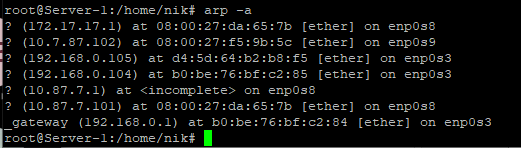


**Dig**

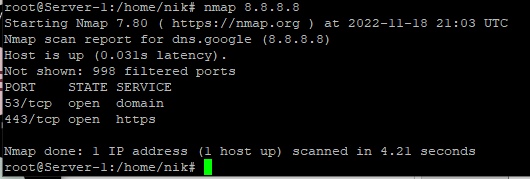


**Arp**

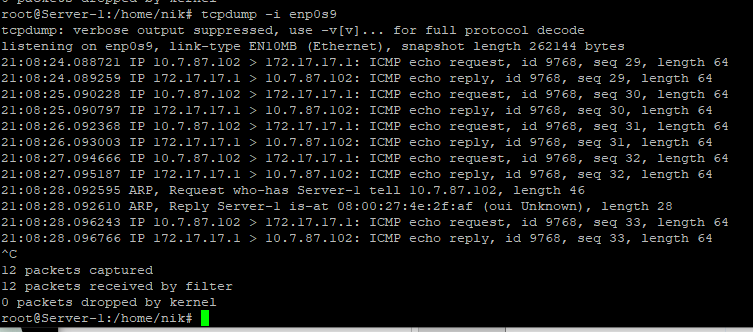
**Для внутренних сетей. Просмотреть соответствие между IP и MAC адресами!**



**Nmap**



**Tcpdump – менеджер пакетов внутренней сети**



**net.ipv4.ip\_forward=1**

**cd /etc/sysconfig/network-scripts**

**systemctl restart network**

**lshw -class network**

**sudo nano /etc/dhcp/dhcpd.conf**

**sudo systemctl restart NetworkManager.service**

**sudo systemctl status NetworkManager.service**

**nano /etc/netplan/00-installer-config.yaml**

**netplan apply**

**sudo netplan --debug apply**

**systemctl restart isc-dhcp-server**

**systemctl status isc-dhcp-server**

**--- route**

**ip route show**

**root@Server-1:/home/nik# route**

**Kernel IP routing table**

**Destination Gateway Genmask Flags Metric Ref Use Iface**

**default \_gateway 0.0.0.0 UG 0 0 0 enp0s3**

**10.7.87.0 0.0.0.0 255.255.255.0 U 0 0 0 enp0s9**

**10.87.7.0 0.0.0.0 255.255.255.0 U 0 0 0 enp0s8**

**192.168.0.0 0.0.0.0 255.255.255.0 U 0 0 0 enp0s3**

**--- transit route on server MUST BE ENABLED !!!!!!!!!!!!!**

**nano /proc/sys/net/ipv4/ip\_forward**

**1**

**Work immediately**

**nano /etc/sysctl.conf**

**net.ipv4.ip\_forward=1**

**net.ipv6.conf.all.forwarding=1**

**work after reboot**

**traceroute 8.8.8.8**

**tcpdump -i enp0s8**

**iptables -L**

