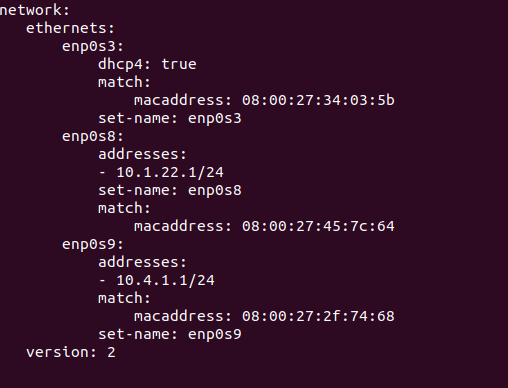
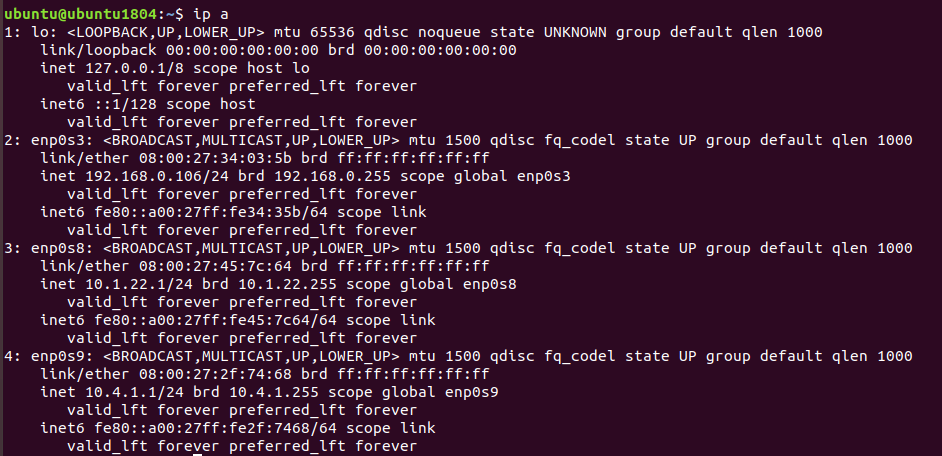
When doing my work, I used VirtualBox virtual machine software. In VirtualBox I put 3 virtual machines with Ubuntu Linux 18.04.5 (was installed on the server (Server) and client machine (Client1)) and Centos Linux Server 8.4 (was installed on the client machine (Client2)). I have allocated 4GB of RAM to the Server machine and 1GB to Client1 and Client2. Also for the Serever machine I set up 3 network adapters (2 of them I set up an internal network for networking with the client machines, and in the other one I set up a network bridge to connect to the host). For the client machines, I put 2 network adapters with internal network for the same purpose. When doing this I learned how to build a network between virtual machines, learned how to configure DHCP, static addresses because of the Netplan configuration, set up firewall and NAT service (to access the Internet). I also learned how to calculate the common address and netmask and how to connect between the virtual machines via SSH.

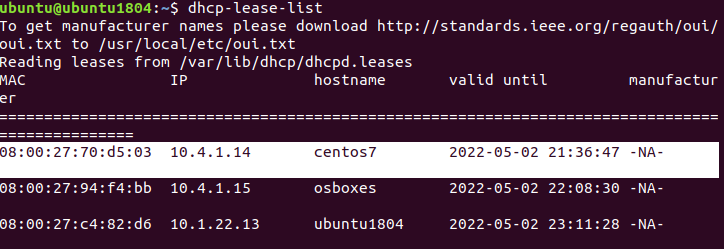
1. On Server\_1 configure static addresses on all interfaces



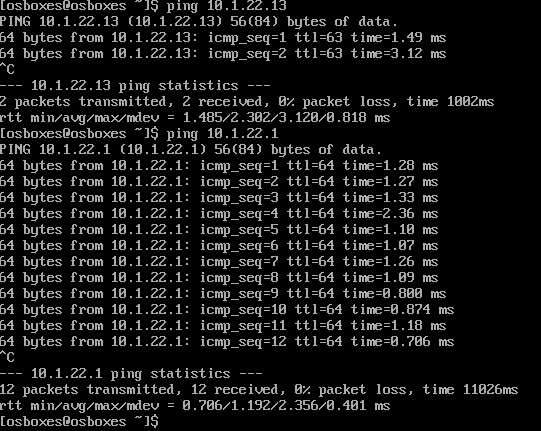


2.

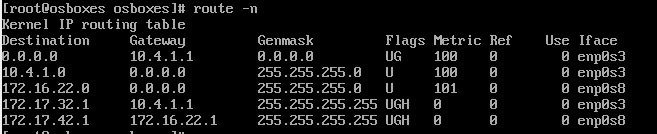
On Server\_1 configure DHCP service that will configure Int1 Client\_1 and Client\_2 addresses



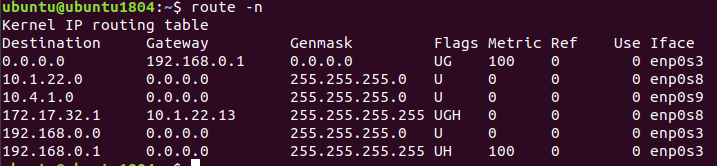
3. Use the ping and traceroute commands to check the communication between the virtual machines. Explain the result.



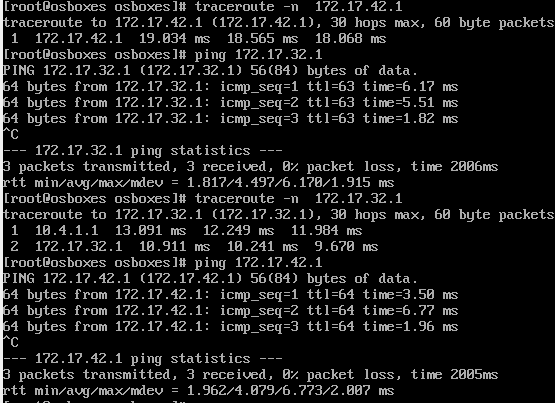
4. Assign two IP addresses on virtual interface lo Client\_1 using the following rule: 172.17.D+10.1/24 and 172.17.D+20.1/24. Configure routing so that traffic from Client\_2 to 172.17.D+10.1 goes through Server\_1, and 172.17.D+20.1 through Net4. Use traceroute to check.



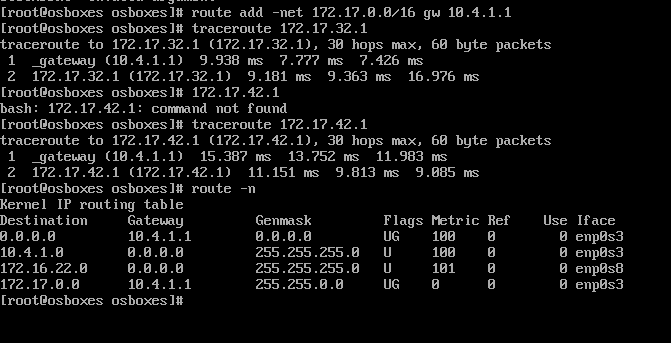
Route command on Client2



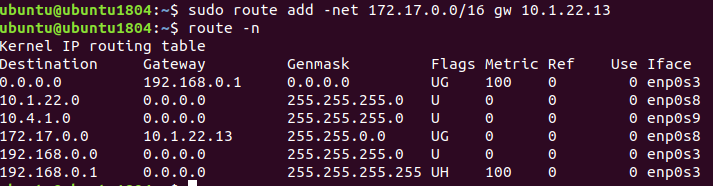
Route command on Server1



5. Calculate the common address and mask (summarizing) of the addresses 172.17.D+10.1 and 172.17.D+20.1, and the mask should be the maximum possible. Remove the routes set in the previous step and replace them by the summarized route, which should pass through Server\_1.

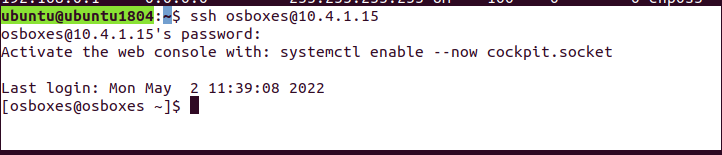


Checking and configuring addresses on Client2

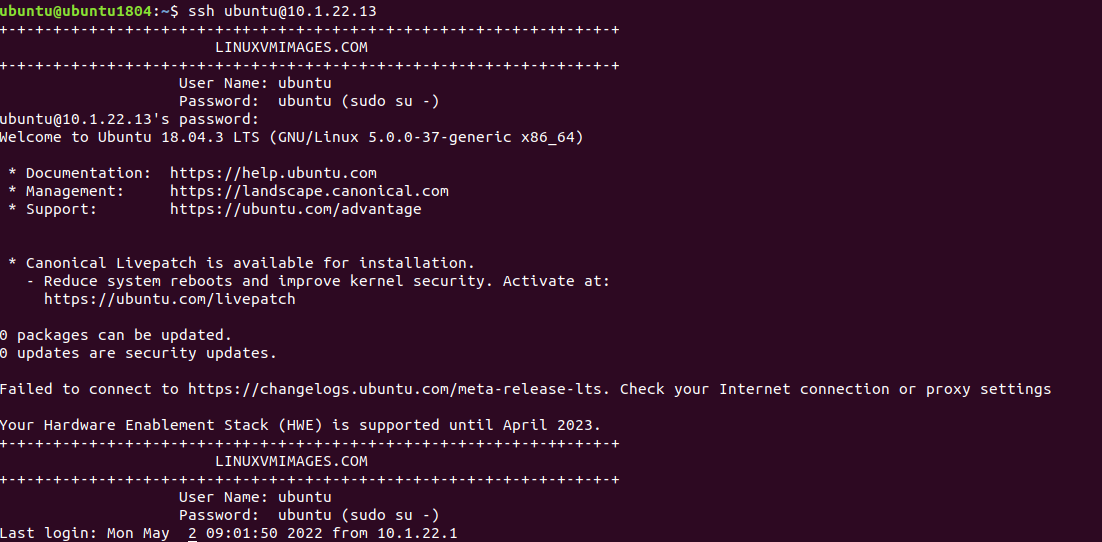


Configuring addresses on Server1 for gateway 10.1.22.13

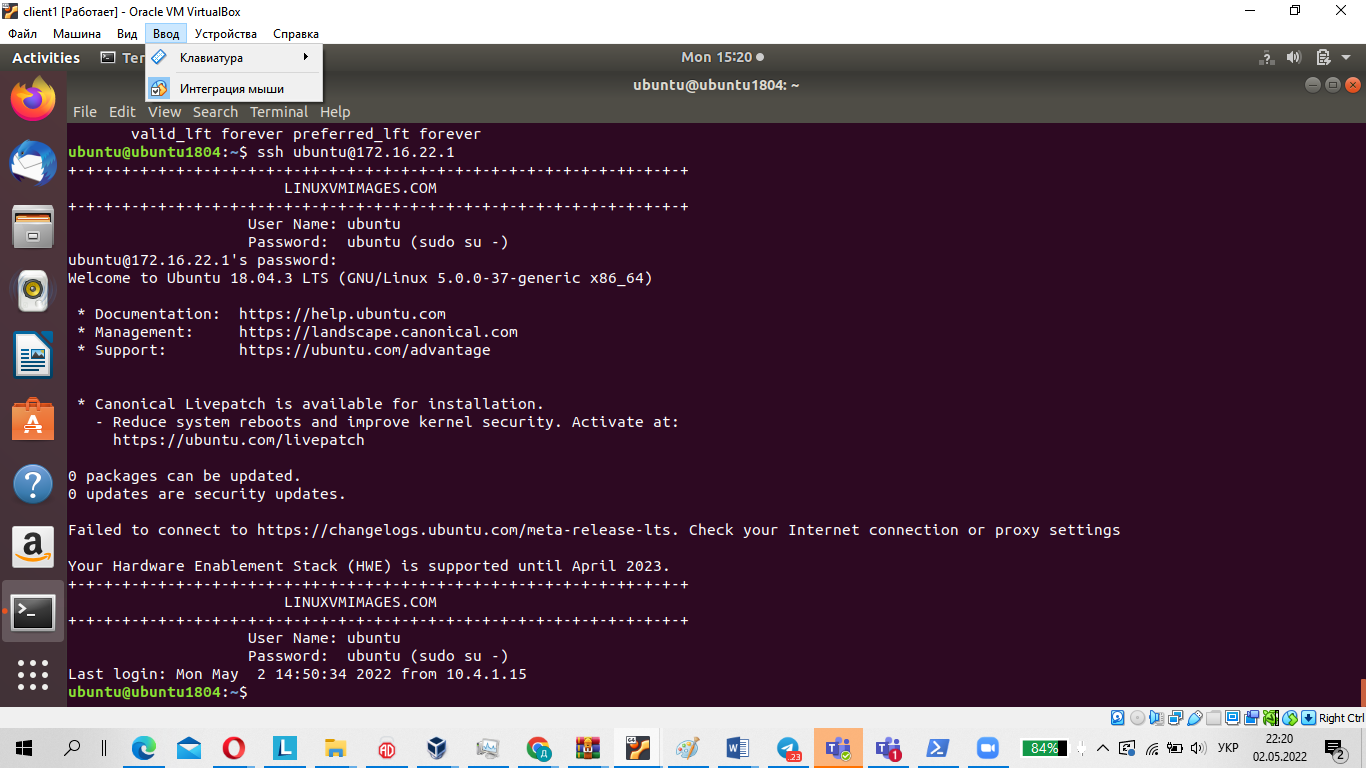
6. Set up the SSH service so that Client\_1 and Client\_2 can connect to Server\_1 and to each other.



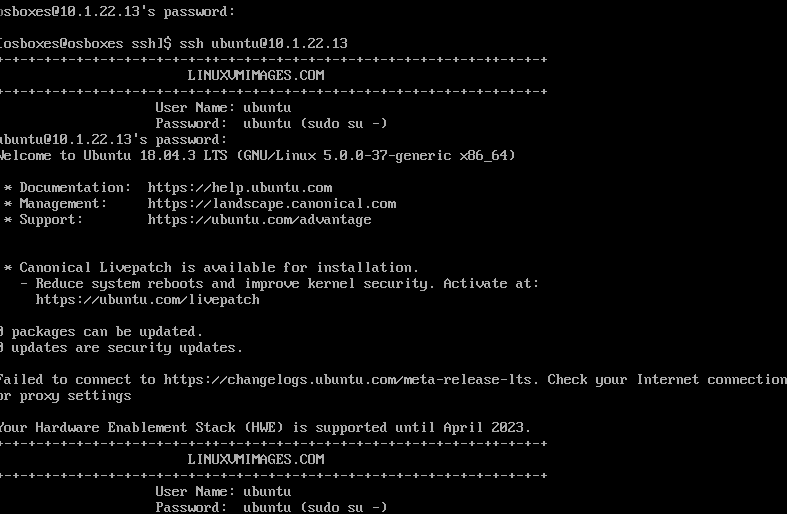
Connecting Server1 to Client2



Connecting Server1 to Client1



Connecting Client1 to Server1



Connecting Client2 to Client1

7. Configure the firewall on Server\_1 as follows:

-Allowed to connect via SSH from Client\_1 and prohibited from Client\_2.

-From Client\_2 to 172.17.D+10.1 ping passed, but to 172.17.D+20.1 did not.

Configure the firewall on Server\_1 as follows:

Allowed to connect via SSH from Client\_1 and denied from Client\_2

Pinged from Client\_2 to 172.17.34.1, but not to 172.17.44.1

server1

Apply the commands

ufw enable

ufw default deny incoming

sudo ufw default allow outgoing

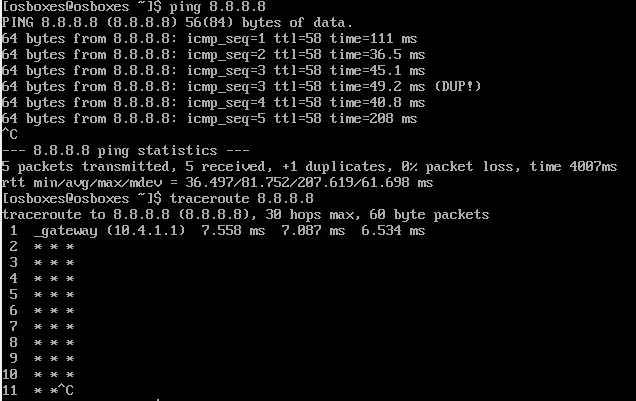
ufw allow from 10.1.22.0/24 any port 22

lient 2

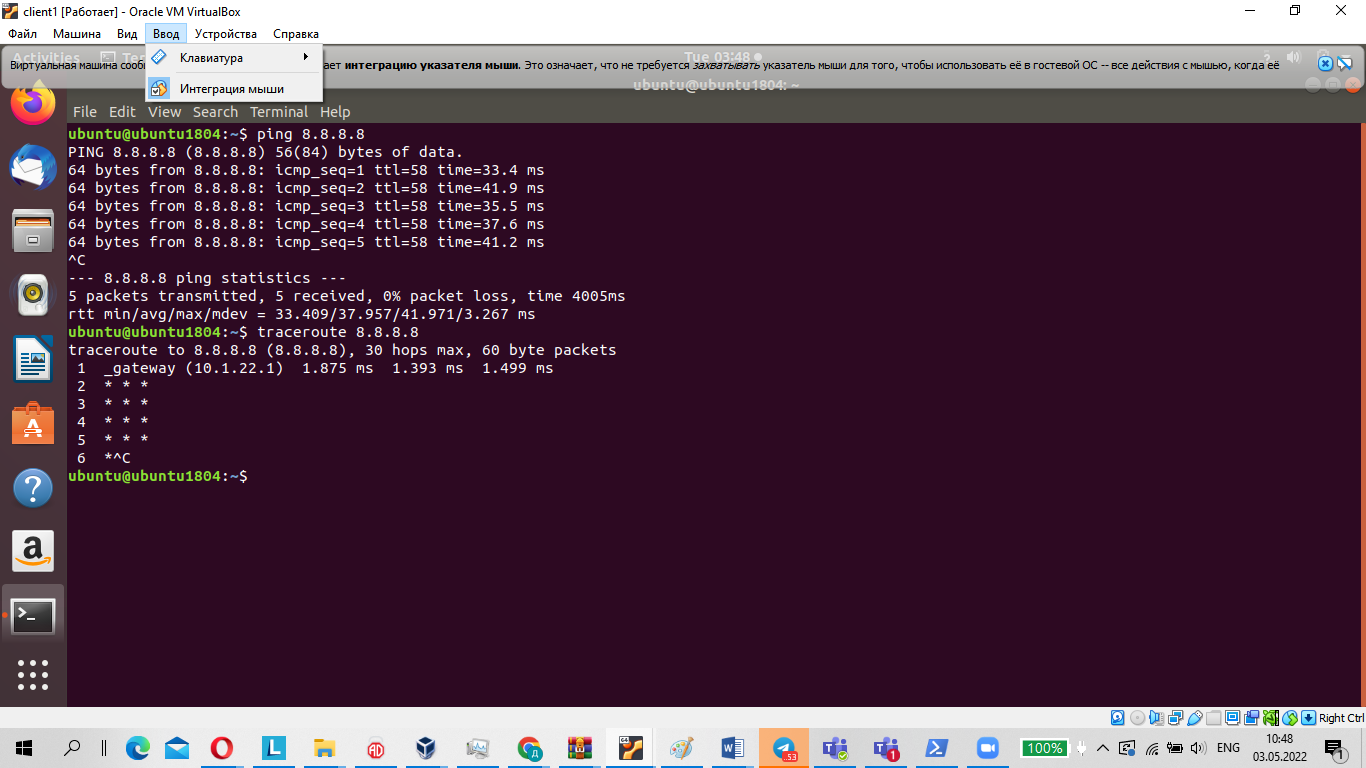
To set up outgoing icmp I will disallow pinging to all addresses except 172.17.32.1

iptables -A OUTPUT -p icmp ! -d 172.17.32.1 --icmp-type echo-request -j DROcP

8. If routing was configured in step 3 for Client\_1 and Client\_2 access to the Internet, delete the corresponding entries. On Server\_1 configure NAT service so that Client\_1 and Client\_2 will ping to the Internet.



Result of ping and traceroute on client2.



Result of ping and traceroute on client1.