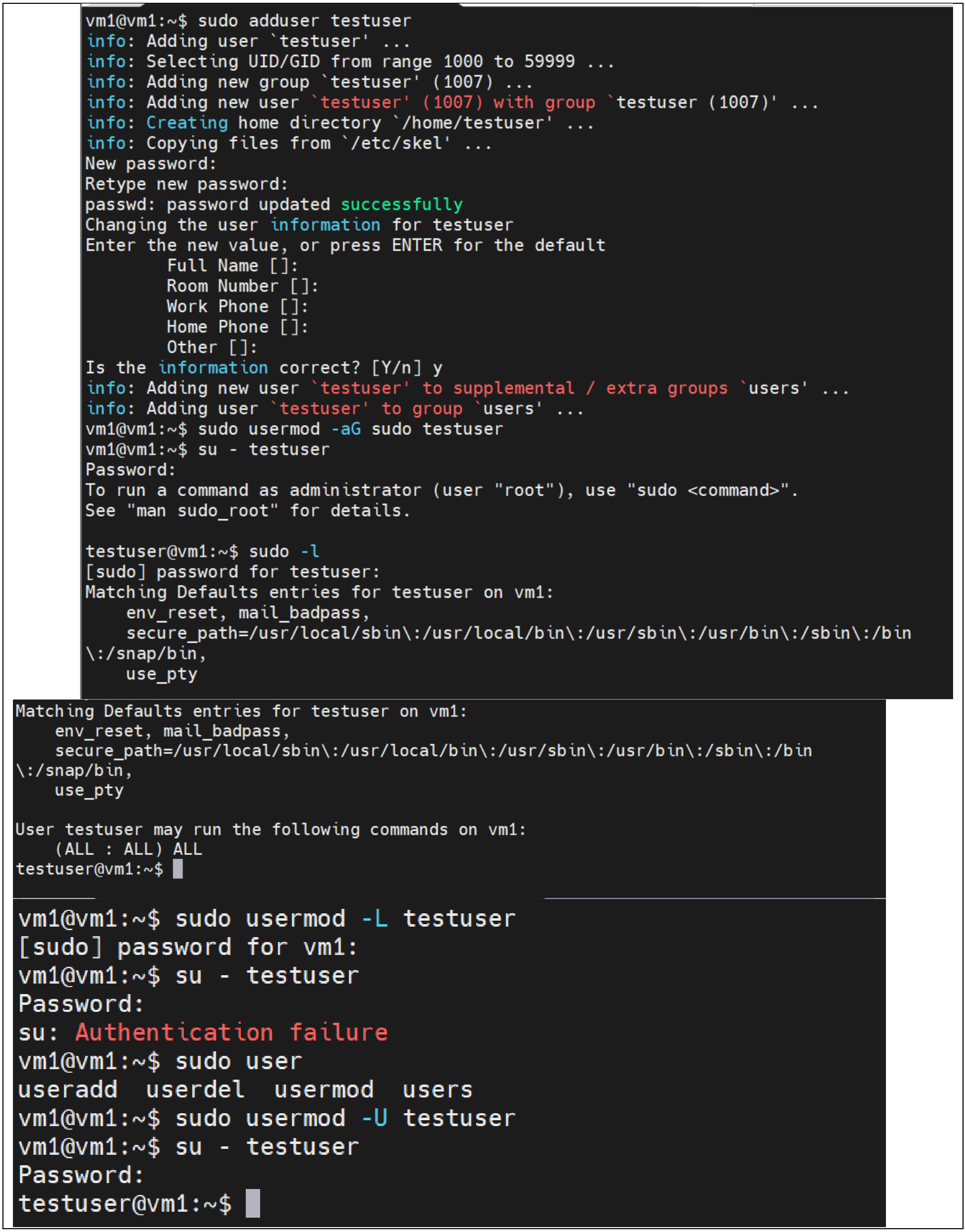
Day 4

Exercise 1

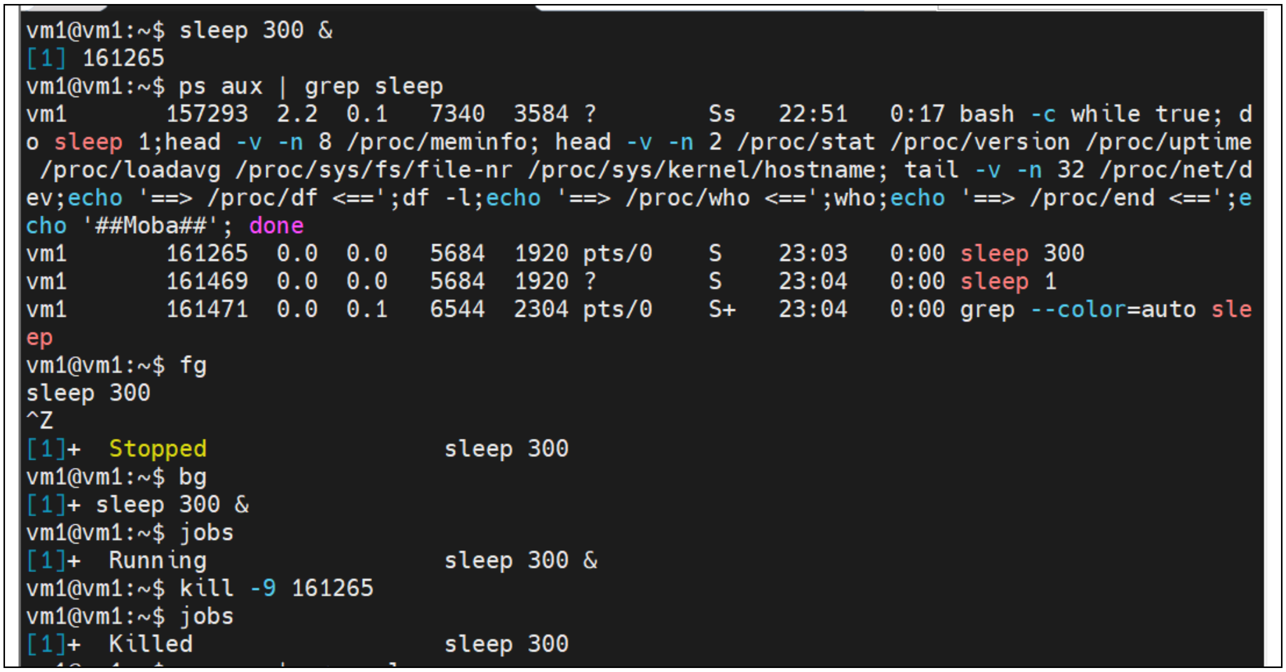


```
vm1@vm1:~$ sudo adduser testuser
info: Adding user `testuser' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `testuser' (1007) ...
info: Adding new user `testuser' (1007) with group `testuser (1007)' ...
info: Creating home directory `/home/testuser' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for testuser
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `testuser' to supplemental / extra groups `users' ...
info: Adding user `testuser' to group `users' ...
vm1@vm1:~$ sudo usermod -aG sudo testuser
vm1@vm1:~$ su - testuser
Password:
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

testuser@vm1:~$ sudo -l
[sudo] password for testuser:
Matching Defaults entries for testuser on vm1:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
\:/snap/bin,
    use_pty
```

```
Matching Defaults entries for testuser on vm1:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin
\:/snap/bin,
    use_pty

User testuser may run the following commands on vm1:
    (ALL : ALL) ALL
testuser@vm1:~$
```

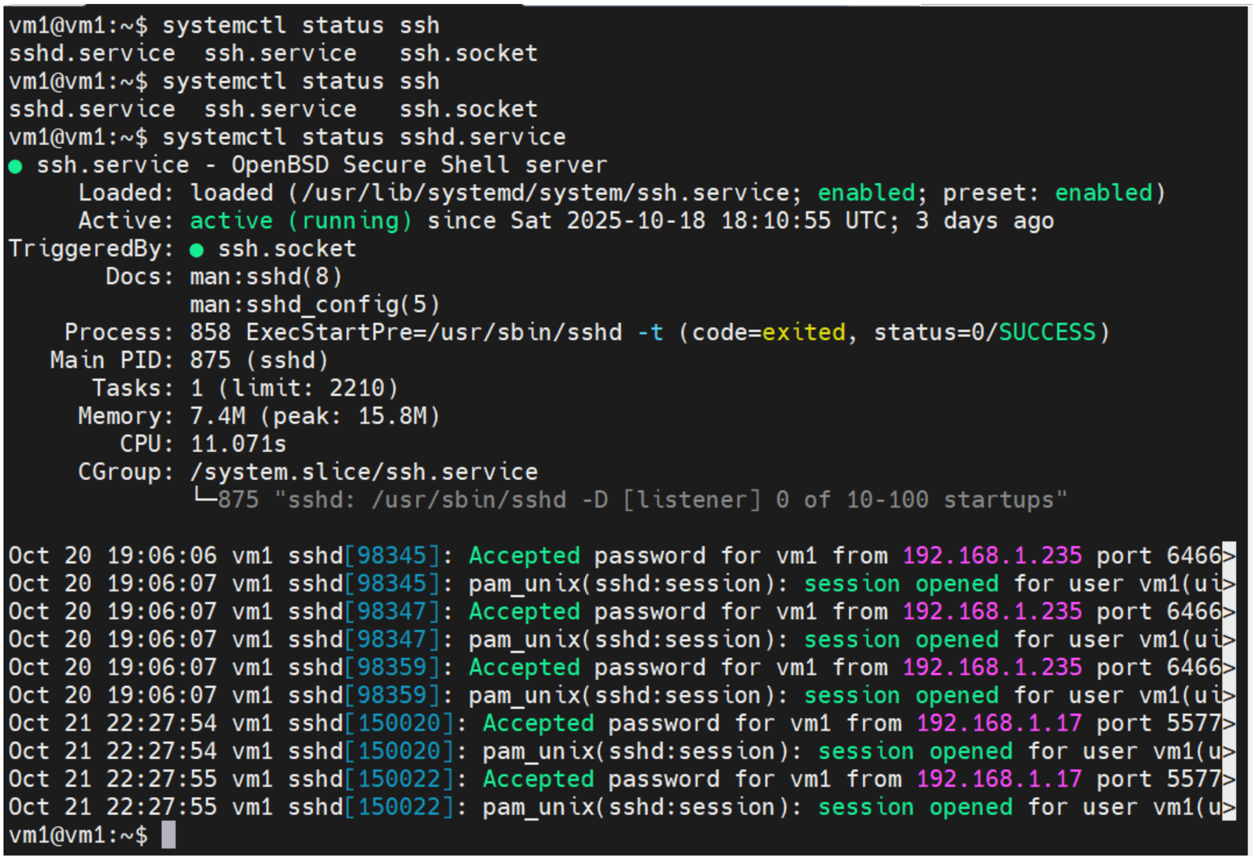
```
vm1@vm1:~$ sudo usermod -L testuser
[sudo] password for vm1:
vm1@vm1:~$ su - testuser
Password:
su: Authentication failure
vm1@vm1:~$ sudo user
useradd  userdel  usermod  users
vm1@vm1:~$ sudo usermod -U testuser
vm1@vm1:~$ su - testuser
Password:
testuser@vm1:~$
```

Exercise 2

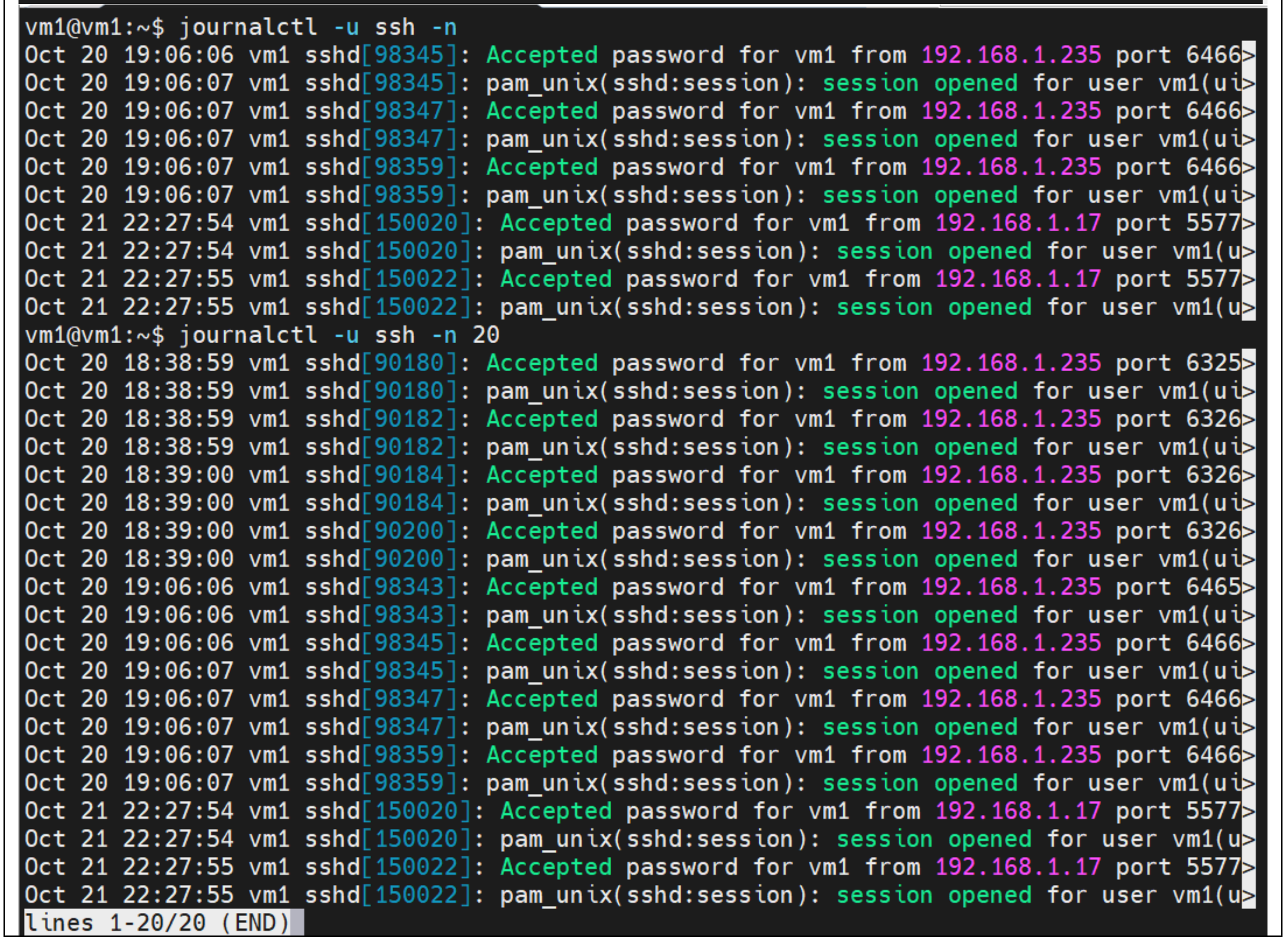


```
vm1@vm1:~$ sleep 300 &
[1] 161265
vm1@vm1:~$ ps aux | grep sleep
vm1       157293  2.2  0.1   7340  3584 ?        Ss   22:51   0:17 bash -c while true; d
o sleep 1;head -v -n 8 /proc/meminfo; head -v -n 2 /proc/stat /proc/version /proc/uptime
 /proc/loadavg /proc/sys/fs/file-nr /proc/sys/kernel/hostname; tail -v -n 32 /proc/net/d
ev;echo '==> /proc/df <==';df -l;echo '==> /proc/who <==';who;echo '==> /proc/end <==';e
cho '##Moba##'; done
vm1       161265  0.0  0.0   5684  1920 pts/0    S    23:03   0:00 sleep 300
vm1       161469  0.0  0.0   5684  1920 ?        S    23:04   0:00 sleep 1
vm1       161471  0.0  0.1   6544  2304 pts/0    S+   23:04   0:00 grep --color=auto sle
ep
vm1@vm1:~$ fg
sleep 300
^Z
[1]+  Stopped                 sleep 300
vm1@vm1:~$ bg
[1]+ sleep 300 &
vm1@vm1:~$ jobs
[1]+  Running                 sleep 300 &
vm1@vm1:~$ kill -9 161265
vm1@vm1:~$ jobs
[1]+  Killed                  sleep 300
```

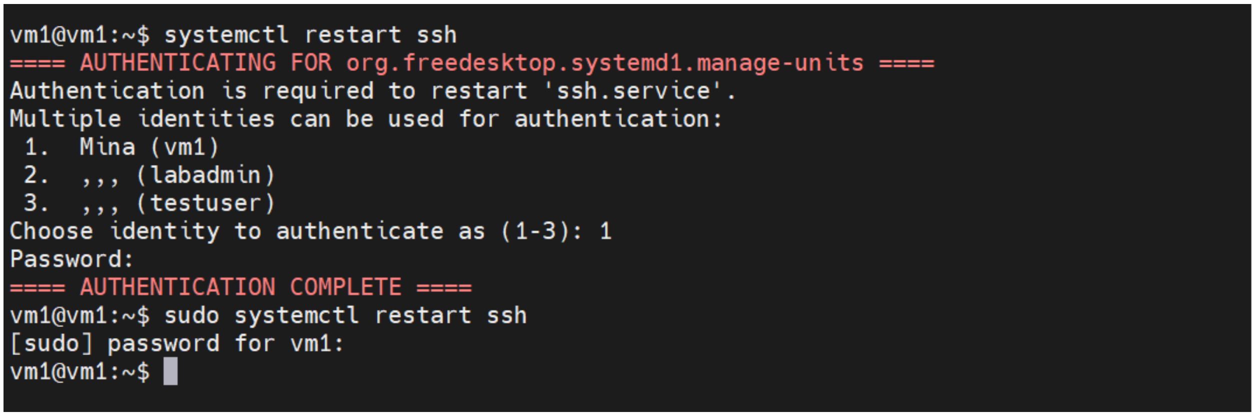
Exercise 3



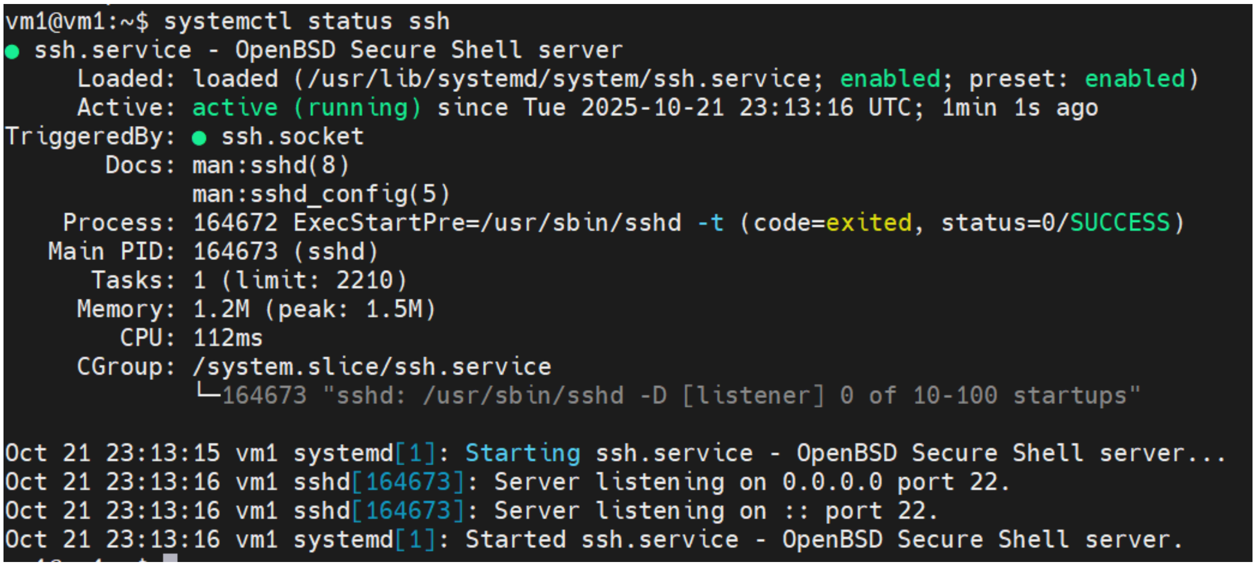
```
vm1@vm1:~$ systemctl status ssh
sshd.service  ssh.service   ssh.socket
vm1@vm1:~$ systemctl status ssh
sshd.service  ssh.service   ssh.socket
vm1@vm1:~$ systemctl status sshd.service
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
     Active: active (running) since Sat 2025-10-18 18:10:55 UTC; 3 days ago
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 858 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 875 (sshd)
      Tasks: 1 (limit: 2210)
     Memory: 7.4M (peak: 15.8M)
        CPU: 11.071s
     CGroup: /system.slice/ssh.service
             └─875 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Oct 20 19:06:06 vm1 sshd[98345]: Accepted password for vm1 from 192.168.1.235 port 6466>
Oct 20 19:06:07 vm1 sshd[98345]: pam_unix(sshd:session): session opened for user vm1(ui>
Oct 20 19:06:07 vm1 sshd[98347]: Accepted password for vm1 from 192.168.1.235 port 6466>
Oct 20 19:06:07 vm1 sshd[98347]: pam_unix(sshd:session): session opened for user vm1(ui>
Oct 20 19:06:07 vm1 sshd[98359]: Accepted password for vm1 from 192.168.1.235 port 6466>
Oct 20 19:06:07 vm1 sshd[98359]: pam_unix(sshd:session): session opened for user vm1(ui>
Oct 21 22:27:54 vm1 sshd[150020]: Accepted password for vm1 from 192.168.1.17 port 5577>
Oct 21 22:27:54 vm1 sshd[150020]: pam_unix(sshd:session): session opened for user vm1(u>
Oct 21 22:27:55 vm1 sshd[150022]: Accepted password for vm1 from 192.168.1.17 port 5577>
Oct 21 22:27:55 vm1 sshd[150022]: pam_unix(sshd:session): session opened for user vm1(u>
vm1@vm1:~$
```



```
vm1@vm1:~$ journalctl -u ssh -n
Oct 20 19:06:06 vm1 sshd[98345]: Accepted password for vm1 from 192.168.1.235 port 6466>
Oct 20 19:06:07 vm1 sshd[98345]: pam_unix(sshd:session): session opened for user vm1(ui>
Oct 20 19:06:07 vm1 sshd[98347]: Accepted password for vm1 from 192.168.1.235 port 6466>
Oct 20 19:06:07 vm1 sshd[98347]: pam_unix(sshd:session): session opened for user vm1(ui>
Oct 20 19:06:07 vm1 sshd[98359]: Accepted password for vm1 from 192.168.1.235 port 6466>
Oct 20 19:06:07 vm1 sshd[98359]: pam_unix(sshd:session): session opened for user vm1(ui>
Oct 21 22:27:54 vm1 sshd[150020]: Accepted password for vm1 from 192.168.1.17 port 5577>
Oct 21 22:27:54 vm1 sshd[150020]: pam_unix(sshd:session): session opened for user vm1(u>
Oct 21 22:27:55 vm1 sshd[150022]: Accepted password for vm1 from 192.168.1.17 port 5577>
Oct 21 22:27:55 vm1 sshd[150022]: pam_unix(sshd:session): session opened for user vm1(u>
vm1@vm1:~$ journalctl -u ssh -n 20
Oct 20 18:38:59 vm1 sshd[90180]: Accepted password for vm1 from 192.168.1.235 port 6325>
Oct 20 18:38:59 vm1 sshd[90180]: pam_unix(sshd:session): session opened for user vm1(ui>
Oct 20 18:38:59 vm1 sshd[90182]: Accepted password for vm1 from 192.168.1.235 port 6326>
Oct 20 18:38:59 vm1 sshd[90182]: pam_unix(sshd:session): session opened for user vm1(ui>
Oct 20 18:39:00 vm1 sshd[90184]: Accepted password for vm1 from 192.168.1.235 port 6326>
Oct 20 18:39:00 vm1 sshd[90184]: pam_unix(sshd:session): session opened for user vm1(ui>
Oct 20 18:39:00 vm1 sshd[90200]: Accepted password for vm1 from 192.168.1.235 port 6326>
Oct 20 18:39:00 vm1 sshd[90200]: pam_unix(sshd:session): session opened for user vm1(ui>
Oct 20 19:06:06 vm1 sshd[98343]: Accepted password for vm1 from 192.168.1.235 port 6465>
Oct 20 19:06:06 vm1 sshd[98343]: pam_unix(sshd:session): session opened for user vm1(ui>
Oct 20 19:06:06 vm1 sshd[98345]: Accepted password for vm1 from 192.168.1.235 port 6466>
Oct 20 19:06:07 vm1 sshd[98345]: pam_unix(sshd:session): session opened for user vm1(ui>
Oct 20 19:06:07 vm1 sshd[98347]: Accepted password for vm1 from 192.168.1.235 port 6466>
Oct 20 19:06:07 vm1 sshd[98347]: pam_unix(sshd:session): session opened for user vm1(ui>
Oct 20 19:06:07 vm1 sshd[98359]: Accepted password for vm1 from 192.168.1.235 port 6466>
Oct 20 19:06:07 vm1 sshd[98359]: pam_unix(sshd:session): session opened for user vm1(ui>
Oct 21 22:27:54 vm1 sshd[150020]: Accepted password for vm1 from 192.168.1.17 port 5577>
Oct 21 22:27:54 vm1 sshd[150020]: pam_unix(sshd:session): session opened for user vm1(u>
Oct 21 22:27:55 vm1 sshd[150022]: Accepted password for vm1 from 192.168.1.17 port 5577>
Oct 21 22:27:55 vm1 sshd[150022]: pam_unix(sshd:session): session opened for user vm1(u>
lines 1-20/20 (END)
```

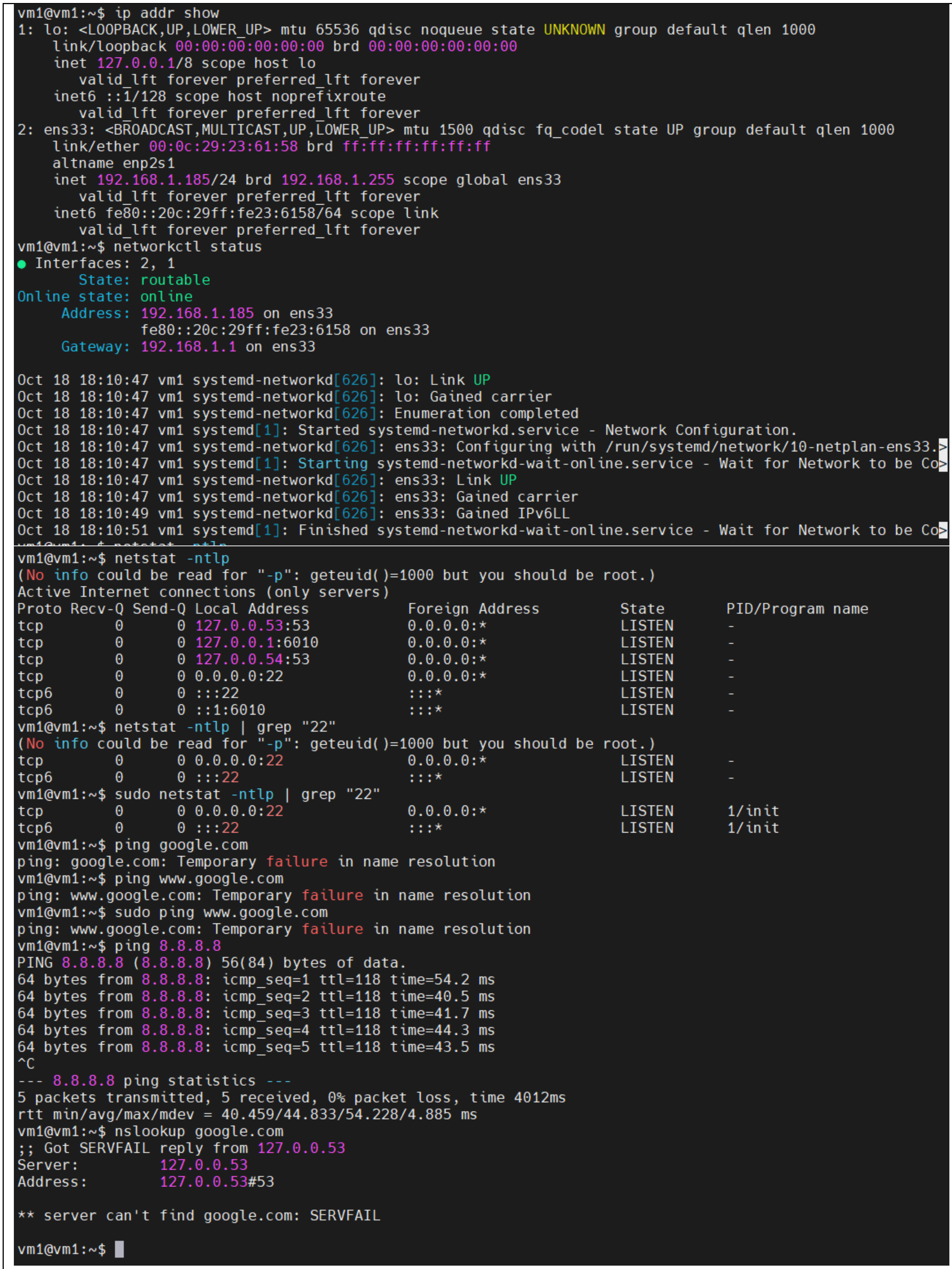


```
vm1@vm1:~$ systemctl restart ssh
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to restart 'ssh.service'.
Multiple identities can be used for authentication:
 1.  Mina (vm1)
 2.  ,,, (labadmin)
 3.  ,,, (testuser)
Choose identity to authenticate as (1-3): 1
Password:
==== AUTHENTICATION COMPLETE ====
vm1@vm1:~$ sudo systemctl restart ssh
[sudo] password for vm1:
vm1@vm1:~$ 
```

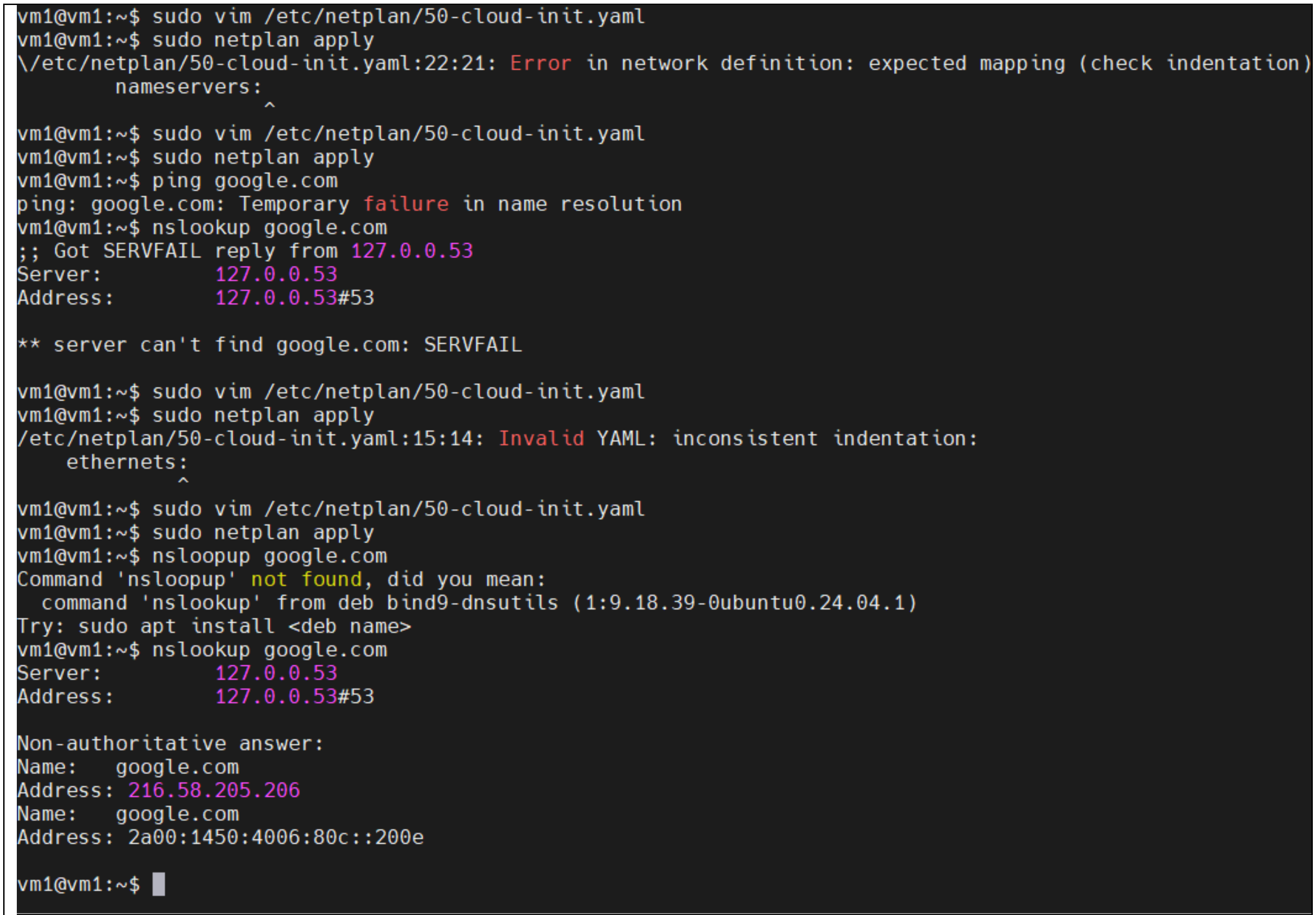


```
vm1@vm1:~$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enabled)
     Active: active (running) since Tue 2025-10-21 23:13:16 UTC; 1min 1s ago
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 164672 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 164673 (sshd)
      Tasks: 1 (limit: 2210)
     Memory: 1.2M (peak: 1.5M)
        CPU: 112ms
     CGroup: /system.slice/ssh.service
             └─164673 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Oct 21 23:13:15 vm1 systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Oct 21 23:13:16 vm1 sshd[164673]: Server listening on 0.0.0.0 port 22.
Oct 21 23:13:16 vm1 sshd[164673]: Server listening on :: port 22.
Oct 21 23:13:16 vm1 systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```

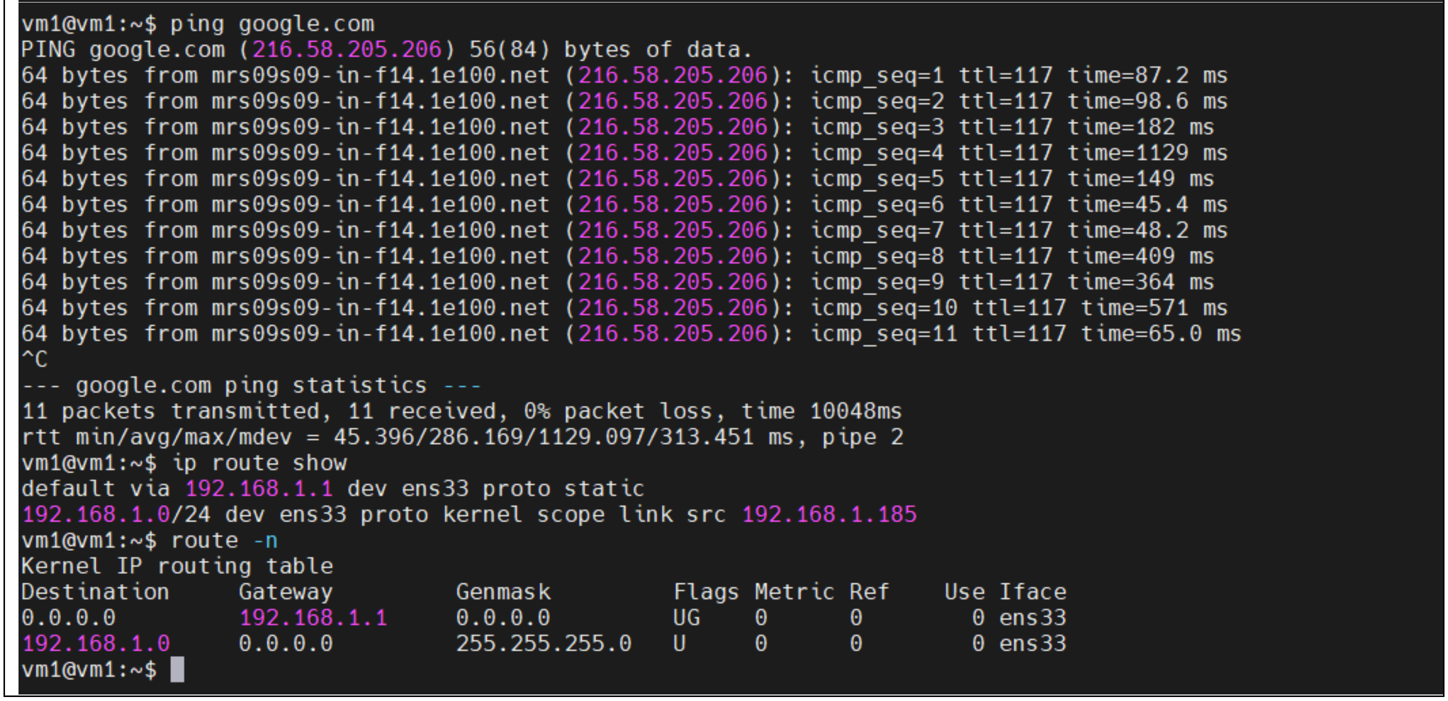
Exercise 4



```
vm1@vm1:~$ ip addr show
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 noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:23:61:58 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.1.185/24 brd 192.168.1.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe23:6158/64 scope link
       valid_lft forever preferred_lft forever
vm1@vm1:~$ networkctl status
● Interfaces: 2, 1
       State: routable
Online state: online
     Address: 192.168.1.185 on ens33
              fe80::20c:29ff:fe23:6158 on ens33
     Gateway: 192.168.1.1 on ens33

Oct 18 18:10:47 vm1 systemd-networkd[626]: lo: Link UP
Oct 18 18:10:47 vm1 systemd-networkd[626]: lo: Gained carrier
Oct 18 18:10:47 vm1 systemd-networkd[626]: Enumeration completed
Oct 18 18:10:47 vm1 systemd[1]: Started systemd-networkd.service - Network Configuration.
Oct 18 18:10:47 vm1 systemd-networkd[626]: ens33: Configuring with /run/systemd/network/10-netplan-ens33.>
Oct 18 18:10:47 vm1 systemd[1]: Starting systemd-networkd-wait-online.service - Wait for Network to be Co>
Oct 18 18:10:47 vm1 systemd-networkd[626]: ens33: Link UP
Oct 18 18:10:47 vm1 systemd-networkd[626]: ens33: Gained carrier
Oct 18 18:10:49 vm1 systemd-networkd[626]: ens33: Gained IPv6LL
Oct 18 18:10:51 vm1 systemd[1]: Finished systemd-networkd-wait-online.service - Wait for Network to be Co>
vm1@vm1:~$ netstat -ntlp
(No info could be read for "-p": geteuid()=1000 but you should be root.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:6010          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.54:53           0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
tcp6       0      0 ::1:6010                :::*                    LISTEN      -
vm1@vm1:~$ netstat -ntlp | grep "22"
(No info could be read for "-p": geteuid()=1000 but you should be root.)
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
vm1@vm1:~$ sudo netstat -ntlp | grep "22"
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1/init
tcp6       0      0 :::22                   :::*                    LISTEN      1/init
vm1@vm1:~$ ping google.com
ping: google.com: Temporary failure in name resolution
vm1@vm1:~$ ping www.google.com
ping: www.google.com: Temporary failure in name resolution
vm1@vm1:~$ sudo ping www.google.com
ping: www.google.com: Temporary failure in name resolution
vm1@vm1:~$ 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=118 time=54.2 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=118 time=40.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=118 time=41.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=118 time=44.3 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=118 time=43.5 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4012ms
rtt min/avg/max/mdev = 40.459/44.833/54.228/4.885 ms
vm1@vm1:~$ nslookup google.com
;; Got SERVFAIL reply from 127.0.0.53
Server:         127.0.0.53
Address:        127.0.0.53#53

** server can't find google.com: SERVFAIL

vm1@vm1:~$ 
```



```
vm1@vm1:~$ sudo vim /etc/netplan/50-cloud-init.yaml
vm1@vm1:~$ sudo netplan apply
\/etc/netplan/50-cloud-init.yaml:22:21: Error in network definition: expected mapping (check indentation)
        nameservers:
                    ^

vm1@vm1:~$ sudo vim /etc/netplan/50-cloud-init.yaml
vm1@vm1:~$ sudo netplan apply
vm1@vm1:~$ ping google.com
ping: google.com: Temporary failure in name resolution
vm1@vm1:~$ nslookup google.com
;; Got SERVFAIL reply from 127.0.0.53
Server:         127.0.0.53
Address:        127.0.0.53#53

** server can't find google.com: SERVFAIL

vm1@vm1:~$ sudo vim /etc/netplan/50-cloud-init.yaml
vm1@vm1:~$ sudo netplan apply
/etc/netplan/50-cloud-init.yaml:15:14: Invalid YAML: inconsistent indentation:
    ethernets:
             ^

vm1@vm1:~$ sudo vim /etc/netplan/50-cloud-init.yaml
vm1@vm1:~$ sudo netplan apply
vm1@vm1:~$ nsloopup google.com
Command 'nsloopup' not found, did you mean:
  command 'nslookup' from deb bind9-dnsutils (1:9.18.39-0ubuntu0.24.04.1)
Try: sudo apt install <deb name>
vm1@vm1:~$ nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 216.58.205.206
Name:   google.com
Address: 2a00:1450:4006:80c::200e

vm1@vm1:~$
```



```
vm1@vm1:~$ ping google.com
PING google.com (216.58.205.206) 56(84) bytes of data.
64 bytes from mrs09s09-in-f14.1e100.net (216.58.205.206): icmp_seq=1 ttl=117 time=87.2 ms
64 bytes from mrs09s09-in-f14.1e100.net (216.58.205.206): icmp_seq=2 ttl=117 time=98.6 ms
64 bytes from mrs09s09-in-f14.1e100.net (216.58.205.206): icmp_seq=3 ttl=117 time=182 ms
64 bytes from mrs09s09-in-f14.1e100.net (216.58.205.206): icmp_seq=4 ttl=117 time=1129 ms
64 bytes from mrs09s09-in-f14.1e100.net (216.58.205.206): icmp_seq=5 ttl=117 time=149 ms
64 bytes from mrs09s09-in-f14.1e100.net (216.58.205.206): icmp_seq=6 ttl=117 time=45.4 ms
64 bytes from mrs09s09-in-f14.1e100.net (216.58.205.206): icmp_seq=7 ttl=117 time=48.2 ms
64 bytes from mrs09s09-in-f14.1e100.net (216.58.205.206): icmp_seq=8 ttl=117 time=409 ms
64 bytes from mrs09s09-in-f14.1e100.net (216.58.205.206): icmp_seq=9 ttl=117 time=364 ms
64 bytes from mrs09s09-in-f14.1e100.net (216.58.205.206): icmp_seq=10 ttl=117 time=571 ms
64 bytes from mrs09s09-in-f14.1e100.net (216.58.205.206): icmp_seq=11 ttl=117 time=65.0 ms
^C
--- google.com ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10048ms
rtt min/avg/max/mdev = 45.396/286.169/1129.097/313.451 ms, pipe 2
vm1@vm1:~$ ip route show
default via 192.168.1.1 dev ens33 proto static
192.168.1.0/24 dev ens33 proto kernel scope link src 192.168.1.185
vm1@vm1:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.1     0.0.0.0         UG    0      0        0 ens33
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 ens33
vm1@vm1:~$
```