#отображение интерфейсов

ghost@ubuntutms:~$ sudo 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: ens160: <BROADCAST,MULTICAST,UP,LOWER\_UP> mtu 1500 qdisc mq state UP group default qlen 1000

link/ether 00:50:56:8f:60:dc brd ff:ff:ff:ff:ff:ff

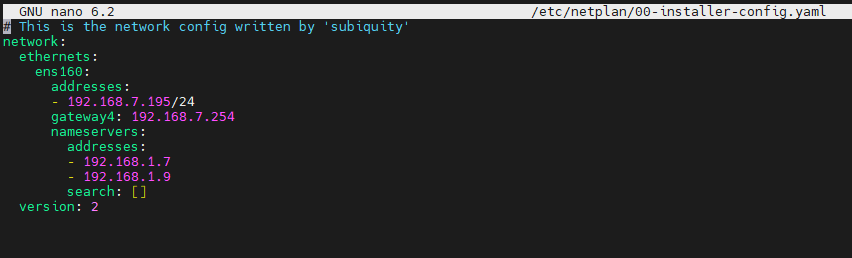
altname enp3s0

inet 192.168.7.195/24 brd 192.168.7.255 scope global ens160

valid\_lft forever preferred\_lft forever

inet6 fe80::250:56ff:fe8f:60dc/64 scope link

valid\_lft forever preferred\_lft forever  
  
  
  
#настройка netplan

ghost@ubuntutms:~$ sudo nano /etc/netplan/\*.yaml  
  
  
  
  
ghost@ubuntutms:~$ 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=114 time=27.3 ms

64 bytes from 8.8.8.8: icmp\_seq=2 ttl=114 time=25.4 ms

64 bytes from 8.8.8.8: icmp\_seq=3 ttl=114 time=28.5 ms

64 bytes from 8.8.8.8: icmp\_seq=4 ttl=114 time=25.0 ms

64 bytes from 8.8.8.8: icmp\_seq=5 ttl=114 time=25.1 ms

64 bytes from 8.8.8.8: icmp\_seq=6 ttl=114 time=25.4 ms

^C

--- 8.8.8.8 ping statistics ---

6 packets transmitted, 6 received, 0% packet loss, time 5007ms

rtt min/avg/max/mdev = 24.986/26.120/28.494/1.317 ms

ghost@ubuntutms:~$ ping 192.168.1.9

PING 192.168.1.9 (192.168.1.9) 56(84) bytes of data.

64 bytes from 192.168.1.9: icmp\_seq=1 ttl=127 time=0.418 ms

64 bytes from 192.168.1.9: icmp\_seq=2 ttl=127 time=0.279 ms

64 bytes from 192.168.1.9: icmp\_seq=3 ttl=127 time=0.249 ms

64 bytes from 192.168.1.9: icmp\_seq=4 ttl=127 time=0.206 ms

^C

--- 192.168.1.9 ping statistics ---

4 packets transmitted, 4 received, 0% packet loss, time 3067ms

rtt min/avg/max/mdev = 0.206/0.288/0.418/0.079 ms

ghost@ubuntutms:~$ nslookup ya.ru

Server: 127.0.0.53

Address: 127.0.0.53#53

Non-authoritative answer:

Name: ya.ru

Address: 77.88.55.242

Name: ya.ru

Address: 5.255.255.242

Name: ya.ru

Address: 2a02:6b8::2:242

#dns

ghost@ubuntutms:~$ resolvectl status

Global

Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported

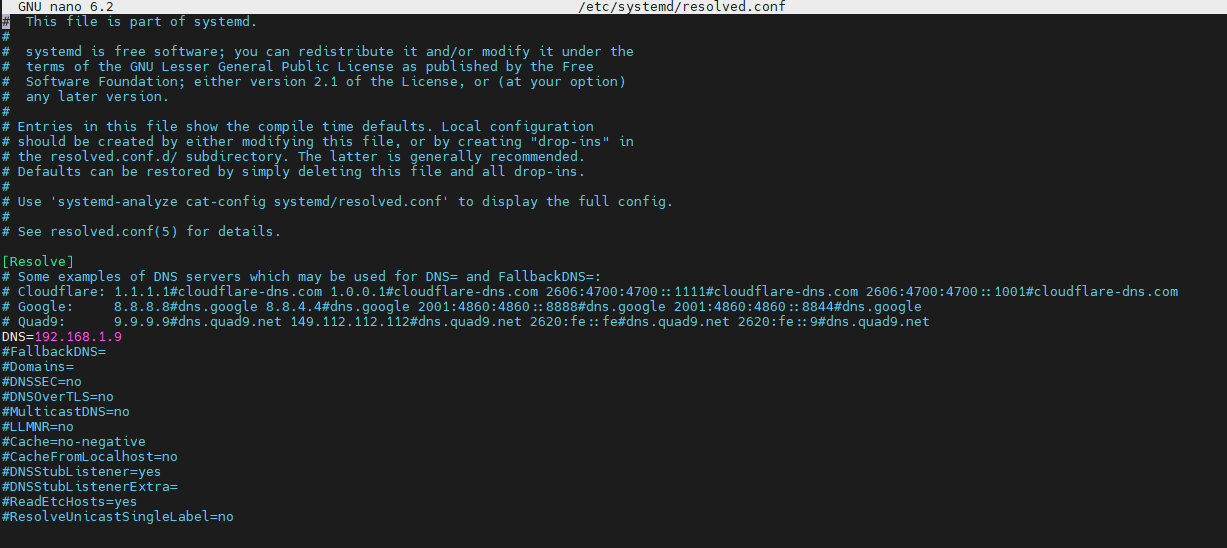
resolv.conf mode: stub

Link 2 (ens160)

Current Scopes: DNS

Protocols: +DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported

Current DNS Server: 192.168.1.7

DNS Servers: 192.168.1.7 192.168.1.9  
  
  
  
ghost@ubuntutms:~$ sudo nano /etc/systemd/resolved.conf  
  
  
  
  
ghost@ubuntutms:~$ sudo ln /usr/bin/resolvectl /usr/bin/systemd-resolve  
  
ghost@ubuntutms:~$ systemd-resolve --status

Global

Protocols: -LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported

resolv.conf mode: stub

Current DNS Server: 192.168.1.9

DNS Servers: 192.168.1.9

Link 2 (ens160)

Current Scopes: DNS

Protocols: +DefaultRoute +LLMNR -mDNS -DNSOverTLS DNSSEC=no/unsupported

Current DNS Server: 192.168.1.7

DNS Servers: 192.168.1.7 192.168.1.9  
  
ghost@ubuntutms:~$ sudo apt-get install resolvconf

Reading package lists... Done

Building dependency tree... Done

Reading state information... Done

The following packages were automatically installed and are no longer required:

adwaita-icon-theme desktop-file-utils doublecmd-common doublecmd-plugins fontconfig fontconfig-config fonts-dejavu-core gtk-update-icon-cache hicolor-icon-theme

humanity-icon-theme libatk1.0-0 libatk1.0-data libavahi-client3 libavahi-common-data libavahi-common3 libcairo-gobject2 libcairo2 libcups2 libdatrie1 libdeflate0

libflashrom1 libfontconfig1 libftdi1-2 libgail-common libgail18 libgdk-pixbuf-2.0-0 libgdk-pixbuf2.0-bin libgdk-pixbuf2.0-common libgraphite2-3 libgtk2.0-0

libgtk2.0-bin libgtk2.0-common libharfbuzz0b libjbig0 libjpeg-turbo8 libjpeg8 libpango-1.0-0 libpangocairo-1.0-0 libpangoft2-1.0-0 libpixman-1-0 librsvg2-2

librsvg2-common libthai-data libthai0 libtiff5 libwebp7 libxcb-render0 libxcb-shm0 libxcomposite1 libxcursor1 libxdamage1 libxfixes3 libxi6 libxinerama1

libxrandr2 libxrender1 ubuntu-mono

Use 'sudo apt autoremove' to remove them.

The following NEW packages will be installed:

resolvconf

0 upgraded, 1 newly installed, 0 to remove and 4 not upgraded.

Need to get 54.7 kB of archives.

After this operation, 203 kB of additional disk space will be used.

Get:1 http://by.archive.ubuntu.com/ubuntu jammy/universe amd64 resolvconf all 1.84ubuntu1 [54.7 kB]

Fetched 54.7 kB in 4s (14.7 kB/s)

Preconfiguring packages ...

Selecting previously unselected package resolvconf.

(Reading database ... 90328 files and directories currently installed.)

Preparing to unpack .../resolvconf\_1.84ubuntu1\_all.deb ...

Unpacking resolvconf (1.84ubuntu1) ...

Setting up resolvconf (1.84ubuntu1) ...

Created symlink /etc/systemd/system/sysinit.target.wants/resolvconf.service → /lib/systemd/system/resolvconf.service.

Created symlink /etc/systemd/system/systemd-resolved.service.wants/resolvconf-pull-resolved.path → /lib/systemd/system/resolvconf-pull-resolved.path.

Created symlink /etc/systemd/system/systemd-resolved.service.wants/resolvconf-pull-resolved.service → /lib/systemd/system/resolvconf-pull-resolved.service.

Processing triggers for man-db (2.10.2-1) ...

Processing triggers for resolvconf (1.84ubuntu1) ...

Scanning processes...

Scanning candidates...

Scanning linux images...

Running kernel seems to be up-to-date.

Restarting services...

Service restarts being deferred:

systemctl restart unattended-upgrades.service

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.

ghost@ubuntutms:~$ nano /etc/resolvconf/resolv.conf.d/head

ghost@ubuntutms:~$ sudo -i

root@ubuntutms:~# nano /etc/resolvconf/resolv.conf.d/head

root@ubuntutms:~# resolvconf -u

root@ubuntutms:~# nslookup ya.ru

Server: 192.168.1.7

Address: 192.168.1.7#53

Non-authoritative answer:

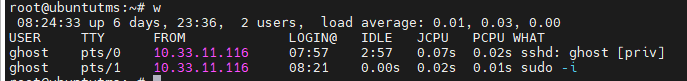
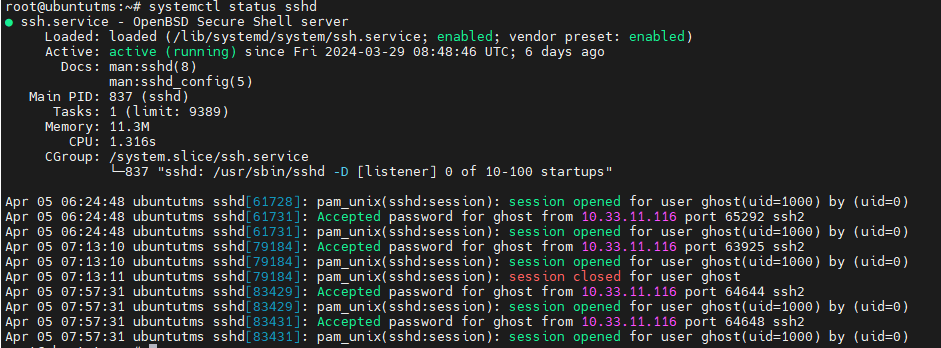
Name: ya.ru

Address: 77.88.55.242

Name: ya.ru

Address: 5.255.255.242

Name: ya.ru

Address: 2a02:6b8::2:242  
  
#ssh  
  
  
  
  
  


root@ubuntutms:~# netstat -tupln | grep LISTEN

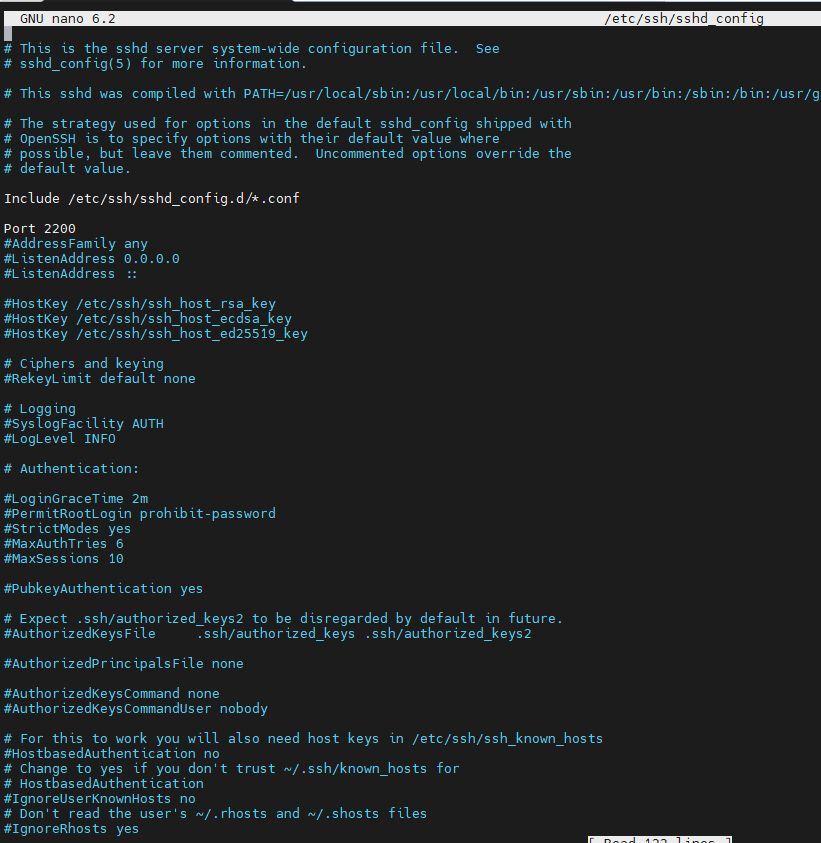
tcp 0 0 0.0.0.0:22 0.0.0.0:\* LISTEN 837/sshd: /usr/sbin

tcp 0 0 127.0.0.53:53 0.0.0.0:\* LISTEN 89846/systemd-resol

tcp 0 0 127.0.0.1:6010 0.0.0.0:\* LISTEN 83526/sshd: ghost@p

tcp6 0 0 :::22 :::\* LISTEN 837/sshd: /usr/sbin

tcp6 0 0 ::1:6010 :::\* LISTEN 83526/sshd: ghost@p

root@ubuntutms:~# nano /etc/ssh/sshd\_config

root@ubuntutms:~# systemctl restart sshd

root@ubuntutms:~# netstat -tupln | grep LISTEN

tcp 0 0 0.0.0.0:2200 0.0.0.0:\* LISTEN 96007/sshd: /usr/sb

tcp 0 0 127.0.0.53:53 0.0.0.0:\* LISTEN 89846/systemd-resol

tcp 0 0 127.0.0.1:6010 0.0.0.0:\* LISTEN 83526/sshd: ghost@p

tcp6 0 0 ::1:6010 :::\* LISTEN 83526/sshd: ghost@p

tcp6 0 0 :::2200 :::\* LISTEN 96007/sshd: /usr/sb

root@ubuntutms:~# iptables -L | grep policy

Chain INPUT (policy ACCEPT)

Chain FORWARD (policy ACCEPT)

Chain OUTPUT (policy ACCEPT)

#дроп пакетов на интерфейсе ens160 с определенного адреса

root@ubuntutms:~# iptables -I INPUT -i ens160 -s 10.10.0.5 -j DROP

root@ubuntutms:~# iptables -L | grep policy

Chain INPUT (policy ACCEPT)

Chain FORWARD (policy ACCEPT)

Chain OUTPUT (policy ACCEPT)

root@ubuntutms:~# iptables -L

Chain INPUT (policy ACCEPT)

target prot opt source destination

DROP all -- 10.10.0.5 anywhere

Chain FORWARD (policy ACCEPT)

target prot opt source destination

Chain OUTPUT (policy ACCEPT)

target prot opt source destination  
  
  
  
  
#запретить подключения на интерфейс ens160 по порту 22 (ssh)

root@ubuntutms:~# sudo iptables -A INPUT -i ens160 -p tcp --dport 22 -j DROP  
root@ubuntutms:~# iptables -L

Chain INPUT (policy ACCEPT)

target prot opt source destination

DROP all -- 10.10.0.5 anywhere

DROP tcp -- anywhere anywhere tcp dpt:ssh

Chain FORWARD (policy ACCEPT)

target prot opt source destination

Chain OUTPUT (policy ACCEPT)

target prot opt source destination  
  
  
root@ubuntutms:~# cd /home/ghost/

root@ubuntutms:/home/ghost# ls -la

total 52

drwxr-x--- 5 ghost ghost 4096 Apr 5 08:44 .

drwxr-xr-x 4 root root 4096 Apr 4 17:15 ..

-rw------- 1 ghost ghost 1637 Apr 5 07:24 .bash\_history

-rw-r--r-- 1 ghost ghost 220 Jan 6 2022 .bash\_logout

-rw-r--r-- 1 ghost ghost 3771 Jan 6 2022 .bashrc

drwx------ 2 ghost ghost 4096 Mar 29 08:38 .cache

-rw------- 1 ghost ghost 20 Apr 5 08:16 .lesshst

-rw-rw-r-- 1 ghost ghost 1587 Apr 1 06:52 lesson1.txt

drwxrwxr-x 3 ghost ghost 4096 Mar 29 08:57 .local

-rw-r--r-- 1 ghost ghost 807 Jan 6 2022 .profile

drwx------ 2 ghost ghost 4096 Mar 29 08:38 .ssh

-rw-r--r-- 1 ghost ghost 0 Mar 29 08:45 .sudo\_as\_admin\_successful

-rw------- 1 ghost ghost 2625 Apr 1 06:30 .viminfo

-rw------- 1 ghost ghost 220 Apr 5 08:44 .Xauthority

root@ubuntutms:/home/ghost# chmod 777 lesson1.txt

root@ubuntutms:/home/ghost# ls -la

total 52

drwxr-x--- 5 ghost ghost 4096 Apr 5 08:44 .

drwxr-xr-x 4 root root 4096 Apr 4 17:15 ..

-rw------- 1 ghost ghost 1637 Apr 5 07:24 .bash\_history

-rw-r--r-- 1 ghost ghost 220 Jan 6 2022 .bash\_logout

-rw-r--r-- 1 ghost ghost 3771 Jan 6 2022 .bashrc

drwx------ 2 ghost ghost 4096 Mar 29 08:38 .cache

-rw------- 1 ghost ghost 20 Apr 5 08:16 .lesshst

-rwxrwxrwx 1 ghost ghost 1587 Apr 1 06:52 lesson1.txt

drwxrwxr-x 3 ghost ghost 4096 Mar 29 08:57 .local

-rw-r--r-- 1 ghost ghost 807 Jan 6 2022 .profile

drwx------ 2 ghost ghost 4096 Mar 29 08:38 .ssh

-rw-r--r-- 1 ghost ghost 0 Mar 29 08:45 .sudo\_as\_admin\_successful

-rw------- 1 ghost ghost 2625 Apr 1 06:30 .viminfo

-rw------- 1 ghost ghost 220 Apr 5 08:44 .Xauthority

root@ubuntutms:/home/ghost# chmod 664 lesson1.txt