

УО «Гомельский государственный университет им. Ф. Скорины»  
Физический факультет  
Кафедра общей физики

## *ОТЧЁТ ПО ЛАБОРАТОРНОЙ РАБОТЕ № 2*

### Идентификация узлов и портов сетевых служб

Проверил:  
Грищенко В.В.

Выполнили:  
студент группы МС-42  
Гончаров Владислав

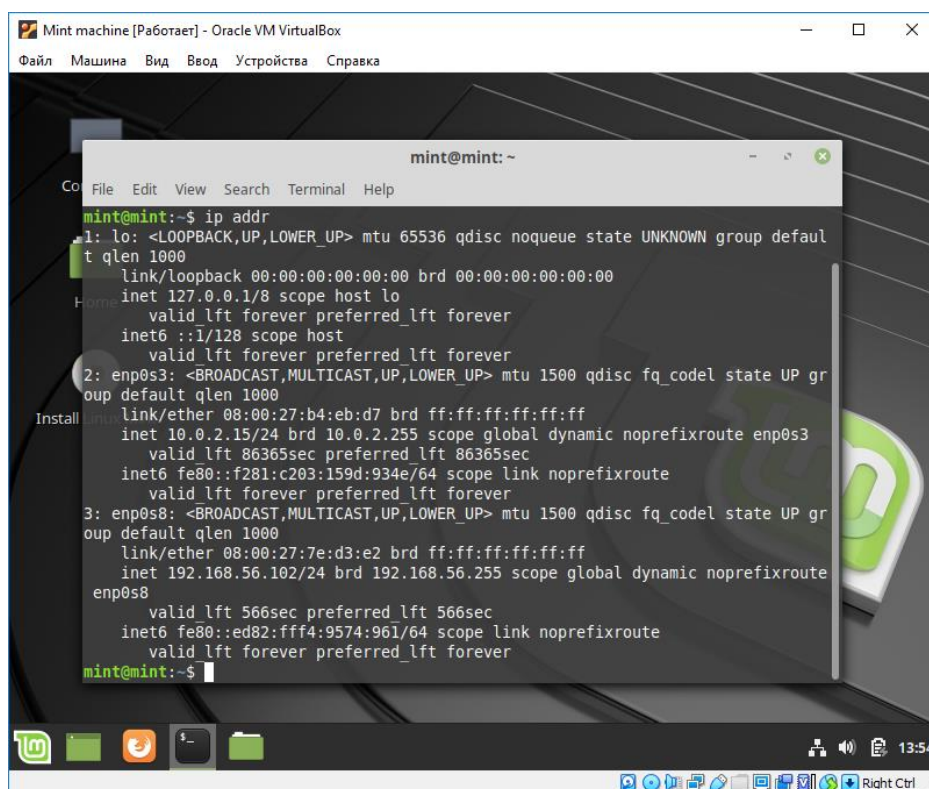
*Гомель 2020*

## Лабораторная работа №2

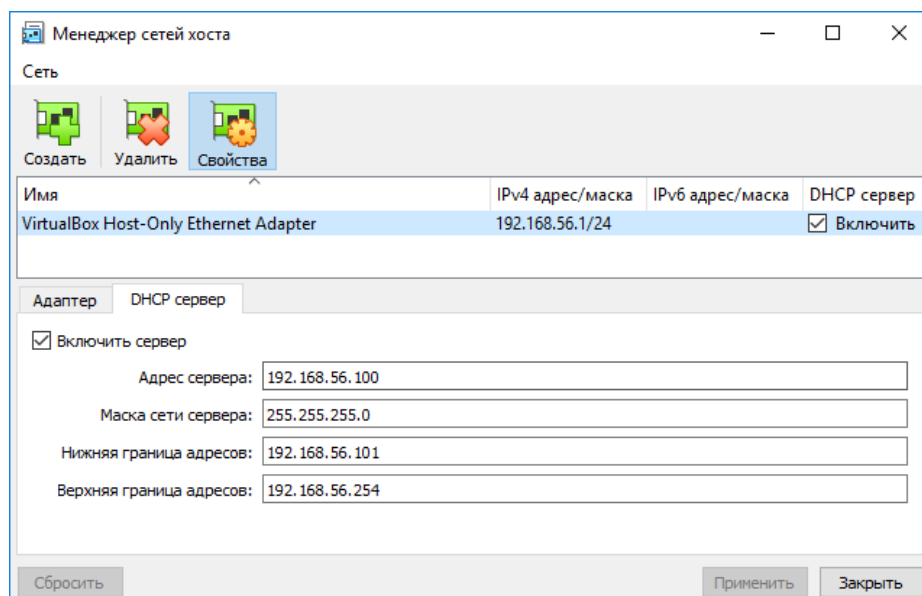
**Цель работы:** обучение методам и средствам идентификации доступных узлов и сетевых портов в анализируемой КС.

**Постановка задачи:** выполнить идентификацию узлов и открытых портов, используя механизмы протоколов ARP, ICMP, IP, TCP и UDP.

Шаг 1. Выполнить идентификацию узлов с помощью средства `fping` для сети 172.16.8.0/24. Просмотреть трассировку сканирования.



```
mint@mint:~$ ip addr
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:b4:eb:d7 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid lft 86365sec preferred_lft 86365sec
    inet6 fe80::f281:c203:159d:934e/64 scope link noprefixroute
        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 08:00:27:7e:d3:e2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s8
        valid lft 566sec preferred_lft 566sec
    inet6 fe80::ed82:fff4:9574:961/64 scope link noprefixroute
        valid lft forever preferred_lft forever
mint@mint:~$
```



Менеджер сетей хоста

Сеть

Создать Удалить Свойства

Имя	IPv4 адрес/маска	IPv6 адрес/маска	DHCP сервер
VirtualBox Host-Only Ethernet Adapter	192.168.56.1/24		<input checked="" type="checkbox"/> Включить

Адаптер DHCP сервер

☒ Включить сервер

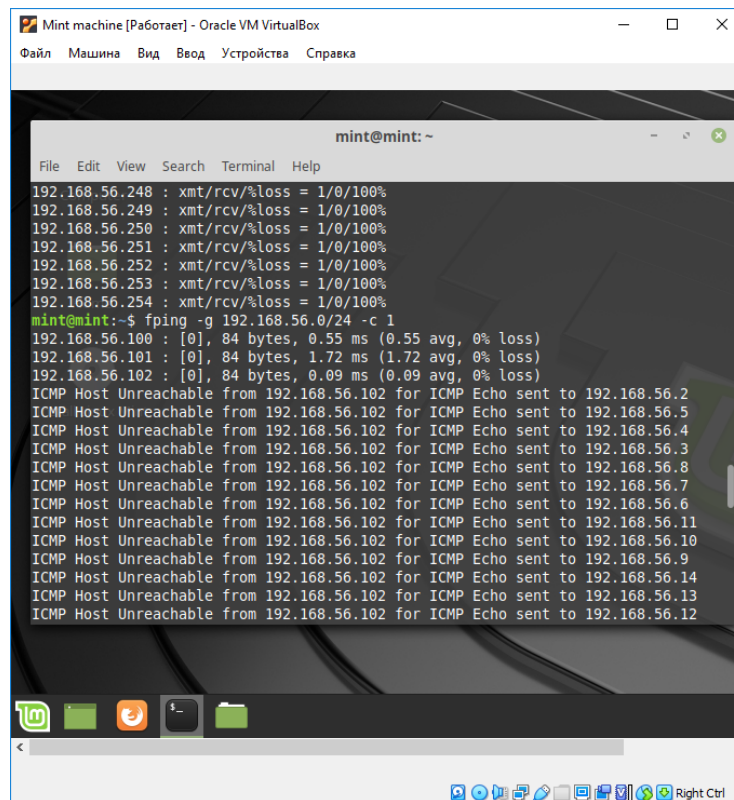
Адрес сервера: 192.168.56.100

Маска сети сервера: 255.255.255.0

Нижняя граница адресов: 192.168.56.101

Верхняя граница адресов: 192.168.56.254

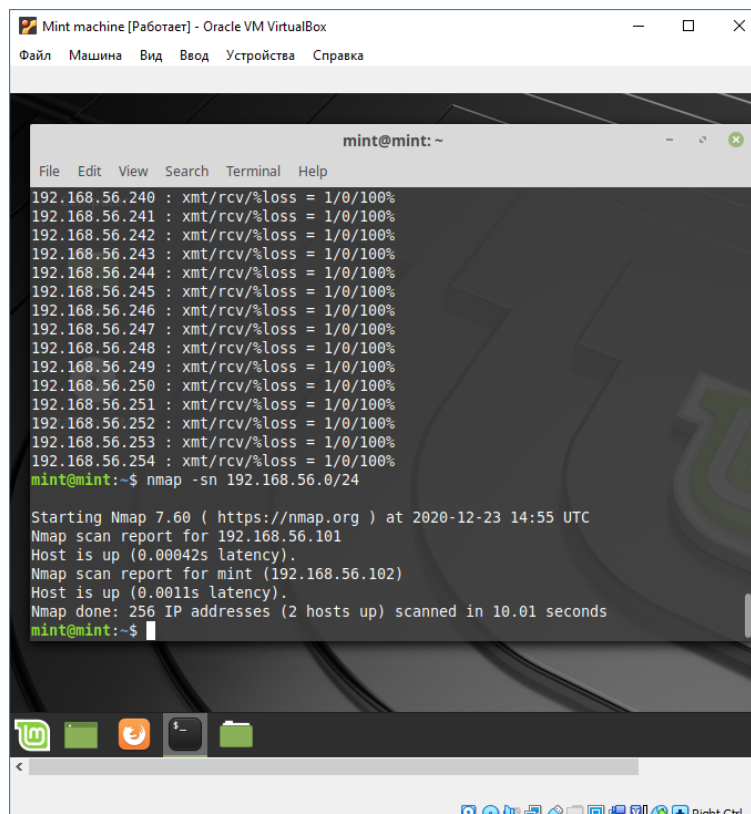
Сбросить Применить Закрыть



The screenshot shows a terminal window titled 'mint@mint: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal output displays the results of a series of ping tests to various IP addresses in the 192.168.56.0/24 range. The first set of tests shows successful connections with 0% loss. The second set, initiated by the command 'fping -g 192.168.56.0/24 -c 1', shows that several hosts are unreachable, with multiple 'ICMP Host Unreachable' messages for the 192.168.56.102 address.

```
mint@mint:~  
File Edit View Search Terminal Help  
192.168.56.248 : xmt/rcv/%loss = 1/0/100%  
192.168.56.249 : xmt/rcv/%loss = 1/0/100%  
192.168.56.250 : xmt/rcv/%loss = 1/0/100%  
192.168.56.251 : xmt/rcv/%loss = 1/0/100%  
192.168.56.252 : xmt/rcv/%loss = 1/0/100%  
192.168.56.253 : xmt/rcv/%loss = 1/0/100%  
192.168.56.254 : xmt/rcv/%loss = 1/0/100%  
mint@mint:~$ fping -g 192.168.56.0/24 -c 1  
192.168.56.100 : [0], 84 bytes, 0.55 ms (0.55 avg, 0% loss)  
192.168.56.101 : [0], 84 bytes, 1.72 ms (1.72 avg, 0% loss)  
192.168.56.102 : [0], 84 bytes, 0.09 ms (0.09 avg, 0% loss)  
ICMP Host Unreachable from 192.168.56.102 for ICMP Echo sent to 192.168.56.2  
ICMP Host Unreachable from 192.168.56.102 for ICMP Echo sent to 192.168.56.5  
ICMP Host Unreachable from 192.168.56.102 for ICMP Echo sent to 192.168.56.4  
ICMP Host Unreachable from 192.168.56.102 for ICMP Echo sent to 192.168.56.3  
ICMP Host Unreachable from 192.168.56.102 for ICMP Echo sent to 192.168.56.8  
ICMP Host Unreachable from 192.168.56.102 for ICMP Echo sent to 192.168.56.7  
ICMP Host Unreachable from 192.168.56.102 for ICMP Echo sent to 192.168.56.6  
ICMP Host Unreachable from 192.168.56.102 for ICMP Echo sent to 192.168.56.11  
ICMP Host Unreachable from 192.168.56.102 for ICMP Echo sent to 192.168.56.10  
ICMP Host Unreachable from 192.168.56.102 for ICMP Echo sent to 192.168.56.9  
ICMP Host Unreachable from 192.168.56.102 for ICMP Echo sent to 192.168.56.14  
ICMP Host Unreachable from 192.168.56.102 for ICMP Echo sent to 192.168.56.13  
ICMP Host Unreachable from 192.168.56.102 for ICMP Echo sent to 192.168.56.12
```

Шаг 2. С помощью сетевого сканера nmap выполнить идентификацию узлов методом ARP Scan. Просмотреть трассировку сканирования:

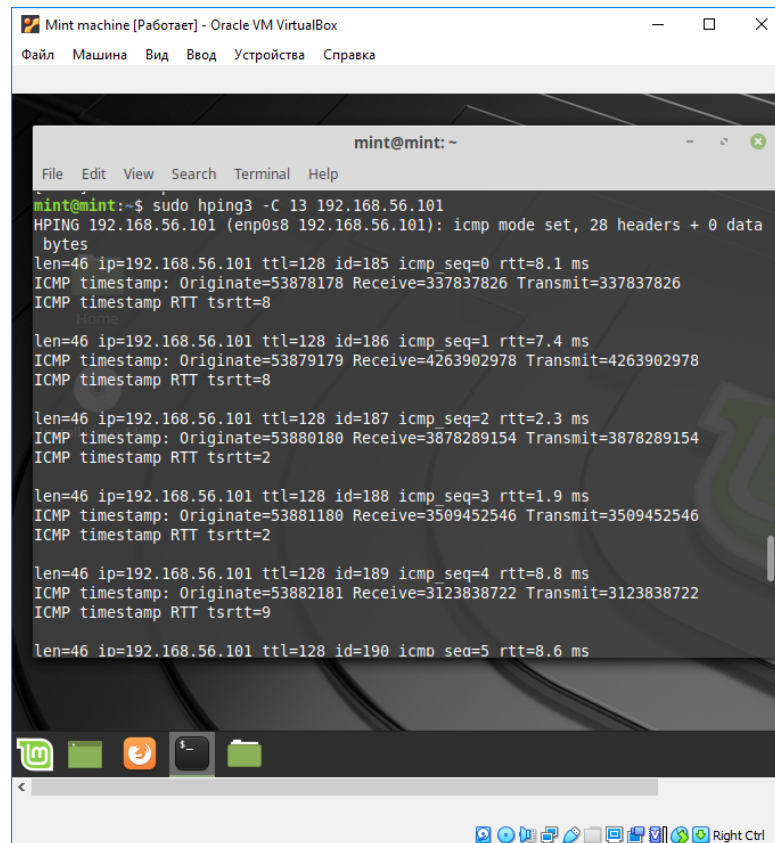


The screenshot shows a terminal window titled 'mint@mint: ~' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal output displays the results of an nmap scan using the -sn (ping scan) option for the 192.168.56.0/24 network. The scan identifies two hosts as up: 192.168.56.101 and 192.168.56.102. The output also shows the nmap version (7.60) and the scan time (10.01 seconds).

```
mint@mint:~  
File Edit View Search Terminal Help  
192.168.56.240 : xmt/rcv/%loss = 1/0/100%  
192.168.56.241 : xmt/rcv/%loss = 1/0/100%  
192.168.56.242 : xmt/rcv/%loss = 1/0/100%  
192.168.56.243 : xmt/rcv/%loss = 1/0/100%  
192.168.56.244 : xmt/rcv/%loss = 1/0/100%  
192.168.56.245 : xmt/rcv/%loss = 1/0/100%  
192.168.56.246 : xmt/rcv/%loss = 1/0/100%  
192.168.56.247 : xmt/rcv/%loss = 1/0/100%  
192.168.56.248 : xmt/rcv/%loss = 1/0/100%  
192.168.56.249 : xmt/rcv/%loss = 1/0/100%  
192.168.56.250 : xmt/rcv/%loss = 1/0/100%  
192.168.56.251 : xmt/rcv/%loss = 1/0/100%  
192.168.56.252 : xmt/rcv/%loss = 1/0/100%  
192.168.56.253 : xmt/rcv/%loss = 1/0/100%  
192.168.56.254 : xmt/rcv/%loss = 1/0/100%  
mint@mint:~$ nmap -sn 192.168.56.0/24  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2020-12-23 14:55 UTC  
Nmap scan report for 192.168.56.101  
Host is up (0.00042s latency).  
Nmap scan report for mint (192.168.56.102)  
Host is up (0.0011s latency).  
Nmap done: 256 IP addresses (2 hosts up) scanned in 10.01 seconds  
mint@mint:~$
```

Шаг 3. С помощью средства hping2 выполнить идентификацию узлов сети, используя ICMP-сообщения Information Request, Time Stamp Request,

Address Mask Request. Просмотреть трассировку сканирования. Сравнить ответы на запросы различных ОС.



```
Mint machine [Работаer] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

mint@mint: ~
File Edit View Search Terminal Help

mint@mint:~$ sudo hping3 -C 13 192.168.56.101
HPING 192.168.56.101 (enp0s8 192.168.56.101): icmp mode set, 28 headers + 0 data
bytes
len=46 ip=192.168.56.101 ttl=128 id=185 icmp seq=0 rtt=8.1 ms
ICMP timestamp: Originate=53878178 Receive=337837826 Transmit=337837826
ICMP timestamp RTT tsrtt=8

len=46 ip=192.168.56.101 ttl=128 id=186 icmp seq=1 rtt=7.4 ms
ICMP timestamp: Originate=53879179 Receive=4263902978 Transmit=4263902978
ICMP timestamp RTT tsrtt=8

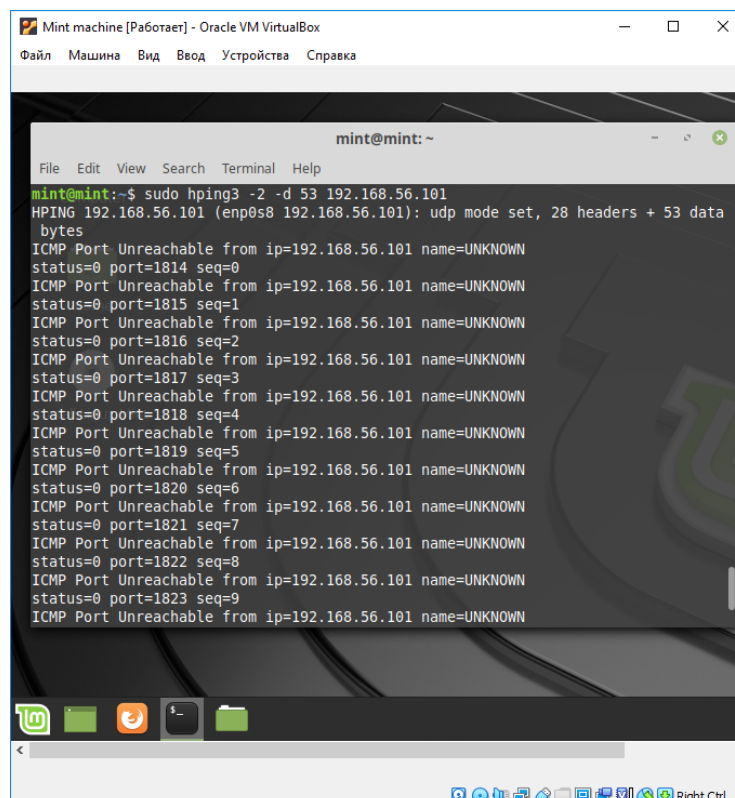
len=46 ip=192.168.56.101 ttl=128 id=187 icmp seq=2 rtt=2.3 ms
ICMP timestamp: Originate=53880180 Receive=3878289154 Transmit=3878289154
ICMP timestamp RTT tsrtt=2

len=46 ip=192.168.56.101 ttl=128 id=188 icmp seq=3 rtt=1.9 ms
ICMP timestamp: Originate=53881180 Receive=3509452546 Transmit=3509452546
ICMP timestamp RTT tsrtt=2

len=46 ip=192.168.56.101 ttl=128 id=189 icmp seq=4 rtt=8.8 ms
ICMP timestamp: Originate=53882181 Receive=3123838722 Transmit=3123838722
ICMP timestamp RTT tsrtt=9

len=46 ip=192.168.56.101 ttl=128 id=190 icmp seq=5 rtt=8.6 ms
```

Шаг 4. С помощью средств hping2 и nmap выполнить идентификацию узлов сети, используя методы UDP Discovery и TCP Ping.



```
Mint machine [Работаer] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

mint@mint: ~
File Edit View Search Terminal Help

mint@mint:~$ sudo hping3 -2 -d 53 192.168.56.101
HPING 192.168.56.101 (enp0s8 192.168.56.101): udp mode set, 28 headers + 53 data
bytes
ICMP Port Unreachable from ip=192.168.56.101 name=UNKNOWN
status=0 port=1814 seq=0
ICMP Port Unreachable from ip=192.168.56.101 name=UNKNOWN
status=0 port=1815 seq=1
ICMP Port Unreachable from ip=192.168.56.101 name=UNKNOWN
status=0 port=1816 seq=2
ICMP Port Unreachable from ip=192.168.56.101 name=UNKNOWN
status=0 port=1817 seq=3
ICMP Port Unreachable from ip=192.168.56.101 name=UNKNOWN
status=0 port=1818 seq=4
ICMP Port Unreachable from ip=192.168.56.101 name=UNKNOWN
status=0 port=1819 seq=5
ICMP Port Unreachable from ip=192.168.56.101 name=UNKNOWN
status=0 port=1820 seq=6
ICMP Port Unreachable from ip=192.168.56.101 name=UNKNOWN
status=0 port=1821 seq=7
ICMP Port Unreachable from ip=192.168.56.101 name=UNKNOWN
status=0 port=1822 seq=8
ICMP Port Unreachable from ip=192.168.56.101 name=UNKNOWN
status=0 port=1823 seq=9
ICMP Port Unreachable from ip=192.168.56.101 name=UNKNOWN
```

Mint machine [Работаer] - Oracle VM VirtualBox

Файл Машина Вид Ввод Устройства Справка

```
mint@mint: ~  
File Edit View Search Terminal Help  
status=0 port=1846 seq=32  
ICMP Port Unreachable from ip=192.168.56.101 name=UNKNOWN  
status=0 port=1847 seq=33  
ICMP Port Unreachable from ip=192.168.56.101 name=UNKNOWN  
status=0 port=1848 seq=34  
^C  
--- 192.168.56.101 hping statistic ---  
35 packets transmitted, 35 packets received, 0% packet loss  
round-trip min/avg/max = 2.5/54.3/1005.6 ms  
mint@mint:~$ nmap -PS -sU -p 111 192.168.56.101  
You requested a scan type which requires root privileges.  
QUITTING!  
mint@mint:~$ sudo nmap -PS -sU -p 111 192.168.56.101  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2020-12-23 15:01 UTC  
Nmap scan report for 192.168.56.101  
Host is up (0.00070s latency).  
  
PORT      STATE SERVICE  
111/udp   closed rpcbind  
MAC Address: 08:00:27:31:5B:85 (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.69 seconds  
mint@mint:~$
```

Linux Mint desktop environment with icons for Firefox, LibreOffice, and others. System tray shows network, volume, and other status icons.