Тәжірибелік сабақ №9: Әр түрлі трафикті сүзу мүмкіндіктері

Linux желісін бақылау көптеген жолдармен жүзеге асырылады. Бұл құралдар желілік интерфейстер арқылы өтетін трафикті басқарады және қазіргі уақытта деректердің жылдамдығын өлшейді. Кіріс және шығыс трафик бөлек көрсетіледі.

Төменде олардың функциялары бойынша сұрыпталған командалардың тізімі берілген:

Жалпы өткізу қабілеті - nload, bmon, slurm, bwm-ng, cbm, netload;

Жалпы өткізу қабілеті (пакеттік стиль шығысы) — vnstat, ifstat, dstat, collectl;

Әр бөңлім үшін өткізу қабілеттілігі - iftop, iptraf, tcptrack — pktstat, netwatch, trafshow;

Әр процестің өткізу қабілеті — nethogs.

Төмендегі мысалдарда командаларға шолу жасалған:

```
gulzinat@gulzinat-VirtualBox:~$ hostname
gulzinat-VirtualBox
gulzinat@gulzinat-VirtualBox:~$
gulzinat@gulzinat-VirtualBox:~$
gulzinat@gulzinat-VirtualBox:~$ hostname -i
127.0.1.1
gulzinat@gulzinat-VirtualBox:~$
```

```
gulzinat@gulzinat-VirtualBox:~$ ping youtube.com
PING youtube.com (173.194.222.93) 56(84) bytes of data.
64 bytes from lo-in-f93.1e100.net (173.194.222.93): icmp_seq=1 ttl=106 time=73.
8 ms
64 bytes from lo-in-f93.1e100.net (173.194.222.93): icmp_seq=2 ttl=106 time=73.
4 ms
64 bytes from lo-in-f93.1e100.net (173.194.222.93): icmp_seq=3 ttl=106 time=74.
4 ms
64 bytes from lo-in-f93.1e100.net (173.194.222.93): icmp_seq=4 ttl=106 time=72.
9 ms
64 bytes from lo-in-f93.1e100.net (173.194.222.93): icmp_seq=5 ttl=106 time=73.
1 ms
```

```
gulzinat@gulzinat-VirtualBox:~$ ping localhost
PING localhost (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.028 ms
64 bytes from localhost (127.0.0.1): icmp_seq=2 ttl=64 time=0.042 ms
64 bytes from localhost (127.0.0.1): icmp_seq=3 ttl=64 time=0.035 ms
64 bytes from localhost (127.0.0.1): icmp_seq=4 ttl=64 time=0.036 ms
64 bytes from localhost (127.0.0.1): icmp_seq=5 ttl=64 time=0.036 ms
64 bytes from localhost (127.0.0.1): icmp_seq=6 ttl=64 time=0.041 ms
64 bytes from localhost (127.0.0.1): icmp_seq=7 ttl=64 time=0.034 ms
^C
--- localhost ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6126ms
rtt min/avg/max/mdev = 0.028/0.036/0.042/0.004 ms
```

```
gulzinat@gulzinat-VirtualBox:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
udp        0      0 gulzinat-Virtual:bootpc _gateway:bootps         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    29827    /run/user/1000/syste
md/notify
unix  2      [ ]         DGRAM                    13351    /run/systemd/journal
/syslog
unix  15     [ ]         DGRAM                    13361    /run/systemd/journal
/dev-log
unix  8      [ ]         DGRAM                    13365    /run/systemd/journal
/socket
unix  3      [ ]         DGRAM                    13337    /run/systemd/notify
unix  3      [ ]         STREAM     CONNECTED     38344
unix  3      [ ]         STREAM     CONNECTED     38750    /run/systemd/journal
/stdout
unix  3      [ ]         STREAM     CONNECTED     34358
```

```
gulzinat@gulzinat-VirtualBox:~$ netstat -g
IPv6/IPv4 Group Memberships
Interface       RefCnt Group
--------------- ------ ---------------------
lo              1      224.0.0.251
lo              1      all-systems.mcast.net
enp0s3          1      224.0.0.251
enp0s3          1      all-systems.mcast.net
lo              1      ff02::fb
lo              1      ip6-allnodes
lo              1      ff01::1

enp0s3          1      ff02::1:ff2c:84c0
enp0s3          1      ff02::fb
enp0s3          1      ip6-allnodes
enp0s3          1      ff01::1
```

```
gulzinat@gulzinat-VirtualBox:~$ nslookup youtube.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   youtube.com
Address: 173.194.222.93
Name:   youtube.com
Address: 173.194.222.91
Name:   youtube.com
Address: 173.194.222.190
Name:   youtube.com
Address: 173.194.222.136
Name:   youtube.com
Address: 2a00:1450:4010:c0b::5b
Name:   youtube.com
Address: 2a00:1450:4010:c0b::be
Name:   youtube.com
Address: 2a00:1450:4010:c0b::88
Name:   youtube.com
Address: 2a00:1450:4010:c0b::5d
```

```
gulzinat@gulzinat-VirtualBox:~$ sudo apt install finger
[sudo] password for gulzinat:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer
  libfprint-2-tod1
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  finger
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
```

```
gulzinat@gulzinat-VirtualBox:~$ finger
Login     Name       Tty      Idle  Login Time   Office     Office Phone
gulzinat  Gulzinat  *:0              Nov 10 02:01 (:0)
gulzinat@gulzinat-VirtualBox:~$
```

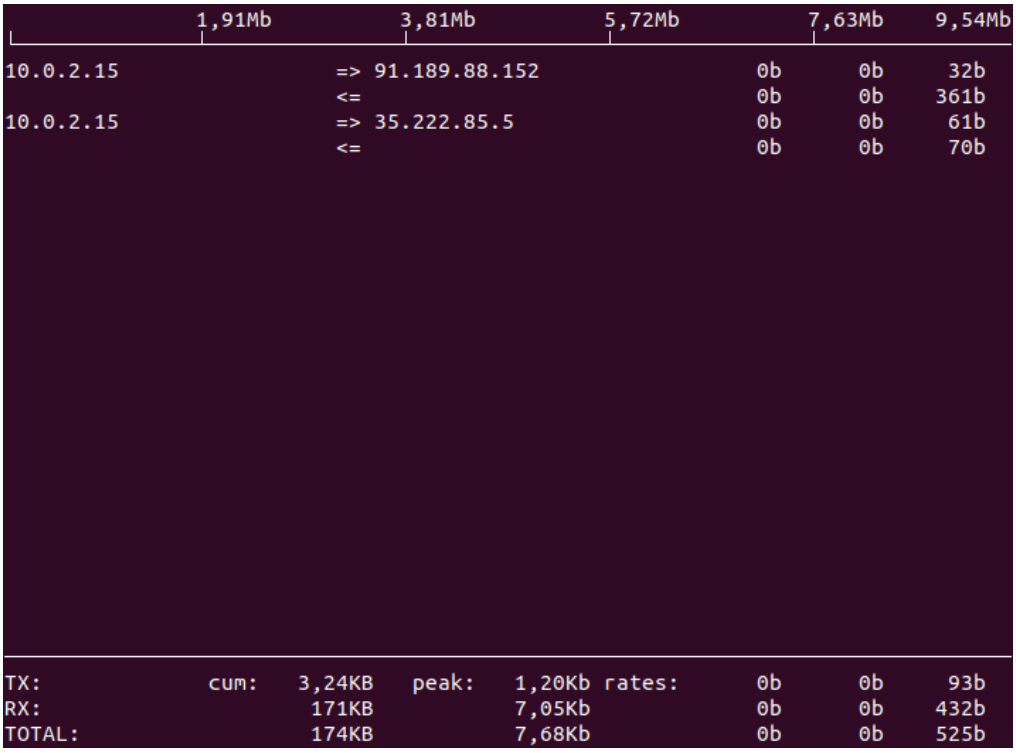
```
gulzinat@gulzinat-VirtualBox:~$ sudo apt-get install nlo
[sudo] password for gulzinat:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is
  libfprint-2-tod1
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
```

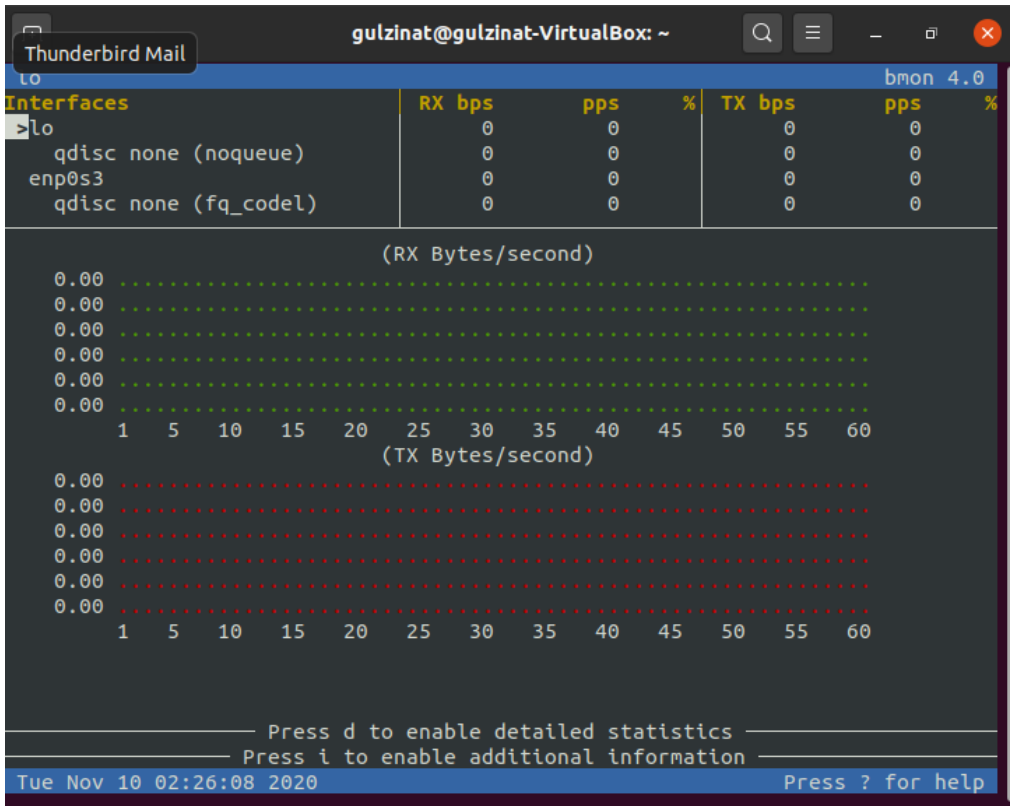
```
gulzinat@gulzinat-VirtualBox:~$ nload
```

```
Device enp0s3 [10.0.2.15] (1/2):
================================================================================
Incoming:

                                                  Curr: 0.00 Bit/s
                                                  Avg: 16.00 Bit/s
                                                  Min: 0.00 Bit/s
                                                  Max: 472.00 Bit/s
                                                  Ttl: 5.98 MByte
Outgoing:

                                                  Curr: 0.00 Bit/s
                                                  Avg: 16.00 Bit/s
                                                  Min: 0.00 Bit/s
                                                  Max: 472.00 Bit/s
                                                  Ttl: 165.91 kByte
```

```
gulzinat@gulzinat-VirtualBox:~$ sudo apt-get install iftop
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer re
  libfprint-2-tod1
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  iftop
0 upgraded, 1 newly installed, 0 to remove and 5 not upgraded.
Need to get 36,3 kB of archives.
After this operation, 95,2 kB of additional disk space will be used.
```

```
gulzinat@gulzinat-VirtualBox:~$ sudo iftop -n
```





Өзіндік жұмыс:

1)Жасалған мысалдарға ТАЛДАУ (АНАЛИЗ) жасау;

2) Желілік командаларды толықтыру;

3) Трафикті сүзу қосымшаларын қарастыру.