Instalarea pachetelor necesare

sudo apt-get install net-tools
sudo apt-get install links
sudo apt-get install traceroute
sudo apt-get install iftop
sudo apt-get install wireshark
sudo apt-get install arping

pentru cei care nu au konsole sau alt terminal cu posibilități de split:

sudo apt-get install qterminal

Descoperirea rețelei în care ne aflăm

arp -n

```
sorin@KUBUNTU:~$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.122.1            ether   52:54:00:45:7c:1a   C                     enp1s0
```

`alternativ` ip neigh

sudo arping 192.168.122.1 (IP-ul de mai sus)

```
sudo arping 192.168.122.1
ARPING 192.168.122.1
42 bytes from 52:54:00:45:7c:1a (192.168.122.1): index=0 time=284.936 usec
42 bytes from 52:54:00:45:7c:1a (192.168.122.1): index=1 time=133.166 usec
42 bytes from 52:54:00:45:7c:1a (192.168.122.1): index=2 time=235.800 usec
```

ifconfig

```
sorin@KUBUNTU:~$ sudo ifconfig
enp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
       inet 192.168.122.109  netmask 255.255.255.0  broadcast 192.168.122.255
       inet6 fe80::4387:7762:a29e:2464  prefixlen 64  scopeid 0x20<link>
       ether 52:54:00:71:85:45  txqueuelen 1000  (Ethernet)
       RX packets 5158  bytes 22828335 (22.8 MB)
       RX errors 0  dropped 689  overruns 0  frame 0
       TX packets 2291  bytes 189603 (189.6 KB)
       TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
       inet 127.0.0.1  netmask 255.0.0.0
       inet6 ::1  prefixlen 128  scopeid 0x10<host>
       loop  txqueuelen 1000  (Local Loopback)
       RX packets 246  bytes 21577 (21.5 KB)
```

```
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 246  bytes 21577 (21.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- **packets** - numarul de pachete trimise/primite
- **bytes** - numarul total de octeti trimis/primit
- **errors** - numarul de pachete incomplete, frame(s) - numar de pachete care par complete dar nu se verifica CRC-ul.
- **dropped** - numarul de pachete pe care nucleul nu a putut sa le prelucreze (fie au structura incorecta , fie nu sunt pentru interfata respectiva).
- **overruns** - numarul de pachete care nu au mai avut loc in buffer
- **carrier** - pachete la care au probleme de modulare a semnalului (hardware) - de obicei cand conexiunea este nesigura.
- **collisions** - pachete a caror transmisie a fost intrerupta datorita aparitiei unui semnal electric neasteptat pe fir, provenit de obicei de la un inceput de transmisie de la celalalt computer.

`alternativ:` ip addr show

`Scăpăm de ipv6`

```
sudo mcedit /etc/sysctl.conf

net.ipv6.conf.all.disable_ipv6=1
net.ipv6.conf.default.disable_ipv6=1
net.ipv6.conf.lo.disable_ipv6=1

save

sudo sysctl -p
```

`verificam cu ifconfig.`

sudo mii-tool enp1s0

```
enp1s0: negotiated 100baseTx-FD flow-control, link ok
```

route -n

```
sorin@KUBUNTU:~$ route -n
Kernel IP routing table
Destination  Gateway      Genmask      Flags Metric Ref    Use Iface
0.0.0.0      192.168.122.1   0.0.0.0          UG     100    0      0 enp1s0
169.254.0.0  0.0.0.0      255.255.0.0  U      1000   0      0 enp1s0
192.168.122.0   0.0.0.0          255.255.255.0   U   100    0      0 enp1s0
```

alternativ: ip route

ping 192.168.122.1

```
sorin@KUBUNTU:~$ ping 192.168.122.1
PING 192.168.122.1 (192.168.122.1) 56(84) bytes of data.
64 bytes from 192.168.122.1: icmp_seq=1 ttl=64 time=0.238 ms
```

```
64 bytes from 192.168.122.1: icmp_seq=2 ttl=64 time=0.180 ms
^C
--- 192.168.122.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1013ms
rtt min/avg/max/mdev = 0.180/0.209/0.238/0.029 ms
```

ping 8.8.8.8

```
sorin@KUBUNTU:~$ 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=120 time=26.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=120 time=26.7 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 26.713/26.765/26.817/0.052 ms
```

ping -t 1 8.8.8.8

```
sorin@KUBUNTU:~$ ping -t 1 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
From 192.168.122.1 icmp_seq=1 Time to live exceeded
From 192.168.122.1 icmp_seq=2 Time to live exceeded
From 192.168.122.1 icmp_seq=3 Time to live exceeded
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2025ms
```

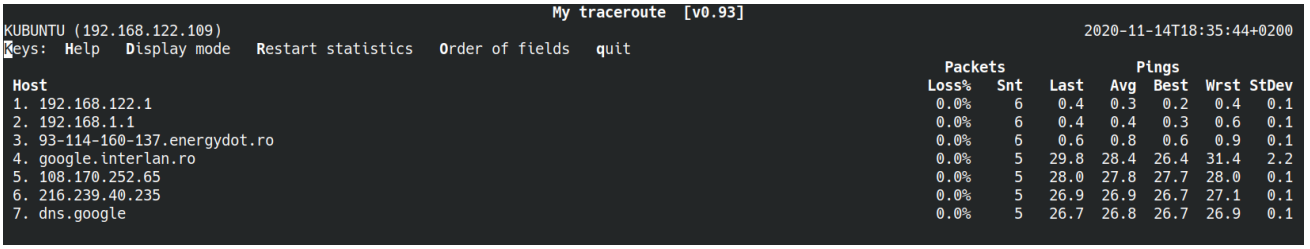
ping -t 2 8.8.8.8

```
sorin@KUBUNTU:~$ ping -t 2 google.com
PING google.com (216.58.206.14) 56(84) bytes of data.
From 192.168.1.1 (192.168.1.1) icmp_seq=1 Time to live exceeded
From 192.168.1.1 (192.168.1.1) icmp_seq=2 Time to live exceeded
From 192.168.1.1 (192.168.1.1) icmp_seq=3 Time to live exceeded
From 192.168.1.1 (192.168.1.1) icmp_seq=4 Time to live exceeded
^C
--- google.com ping statistics ---
4 packets transmitted, 0 received, +4 errors, 100% packet loss, time 3043ms
```

traceroute 8.8.8.8

```
sorin@KUBUNTU:~$ traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  192.168.122.1 (192.168.122.1)  0.582 ms  0.551 ms  0.530 ms
 2  192.168.1.1 (192.168.1.1)  0.507 ms  0.489 ms  0.465 ms
 3  93-114-160-137.energydot.ro (93.114.160.137)  60.292 ms  60.274 ms  60.255 ms
 4  google.interlan.ro (86.104.125.129)  26.451 ms  26.402 ms  26.366 ms
 5  108.170.252.65 (108.170.252.65)  32.219 ms 108.170.251.193 (108.170.251.193)  26.414
ms 108.170.252.1 (108.170.252.1)  27.382 ms
 6  209.85.241.75 (209.85.241.75)  27.160 ms 216.239.47.245 (216.239.47.245)  34.971 ms
216.239.40.57 (216.239.40.57)  34.901 ms
 7  dns.google (8.8.8.8)  34.798 ms  34.721 ms  34.647 ms
```

mtr 8.8.8.8



IP-uri si nume

host -a utm.ro

```
sorin@KUBUNTU:~$ host -a utm.ro
Trying "utm.ro"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 14231
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;utm.ro.                                IN     ANY

;; ANSWER SECTION:
utm.ro.                  21599   IN   NS     ns1-07.azure-dns.com.
utm.ro.                  21599   IN   NS     ns2-07.azure-dns.net.
utm.ro.                  21599   IN   NS     ns3-07.azure-dns.org.
utm.ro.                  21599   IN   NS     ns4-07.azure-dns.info.
utm.ro.                  3599  IN     SOA    ns1-07.azure-dns.com.
azuredns-hostmaster.microsoft.com. 1 3600 300 2419200 300
```

host -a www.utm.ro

```
sorin@KUBUNTU:~$ host -a www.utm.ro
Trying "www.utm.ro"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51769
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.utm.ro.                       IN     ANY
```

host -t MX google.com

```
sorin@KUBUNTU:~$ host -t MX google.com
google.com mail is handled by 40 alt3.aspmx.l.google.com.
google.com mail is handled by 50 alt4.aspmx.l.google.com.
google.com mail is handled by 20 alt1.aspmx.l.google.com.
google.com mail is handled by 30 alt2.aspmx.l.google.com.
google.com mail is handled by 10 aspmx.l.google.com.
```

dig utm.ro ANSWER section: 92.87.194.93
dig @8.8.8.8 utm.ro
dig ro ANSWER 0

host utm.ro
host ro (fara raspuns pentru ca nu exista nici un ip corespunzator cu ro)

host 92.87.194.90 - reverse dns.

Monitorizarea conexiunilor computerului curent

Sesiunea se desfășoară în terminal cu terminalul împărțit în două regiuni orizontale. Netstatul ramane in functiune in regiunea de sus:

```
watch -d -n 1 “netstat -tapun”
     t - show tcp traffic
     u - show udp traffic
     a - all (incoming and outgoing)
     n - don’t resolve
echivalent cu watch -d -n 1 “ss -tup”
```

Stările conexiunilor:

ESTABLISHED Conexiunea dintre cele doua socketuri este stabilită.

SYN_SENT Socketul local încearcă să stabilească o conexiune. Pachetele de tip SYN au fost trimise și se așteaptă primirea celor de tip ACK

SYN_RECV A fost primită o solicitare de conexiune de pe rețea (pachete de tip SYN provenite de la un socket la distanță).

FIN_WAIT1 Socketul local este inchis, acesta a trimis pachete de tip FIN către socketul aflat la distanță.

FIN_WAIT2 Socketul de la distanță a trimis pachete ACK care confirmă solicitarea de tip FIN trimisă anterior (în stadiul FIN_WAIT1). Socketul local așteaptă pachete de tip FIN.

TIME_WAIT Protocolul de inchidere a fost incheiat cu succes, socketul așteaptă o perioadă (înainte de a trece în starea CLOSED).

CLOSED Socketul este închis, nu există nici o conexiune.

CLOSE_WAIT Socketul local a primit pachete tip FIN și a trimis ACK. Se așteaptă
completarea procesului de închidere (primirea pachetelor FIN de la computerul celălalt)

LAST_ACK Conexiunea a fost închisă, se așteaptă ultimul ACK de la socketul de la distanță.

LISTEN Socketul local așteaptă solicitări de conexiune

CLOSING Socketul local a trimis FIN, așteaptă ACK. La primirea ACK-ului va trece in TIME_WAIT

UNKNOWN Starea socketului este necunoscută

În regiunea de jos:

Oprirea serviciilor care incurca urmarirea traficului

Oprim daemonul cron

```
sudo service cron stop
```

Oprim avahi-daemon (comanda trebuie data de mai multe ori, e incapatanat)

```
sudo service avahi-daemon stop
```

Oprim cups daemon

```
sudo service cups stop
```

Oprim kdeconnect (pentru cei cu kubuntu)

```
ps axu | grep kdeconnect
```

aflam pid-ul kdeconnectului (sa-l numim kdecpid)

```
sudo kill -9 kdecpid
```

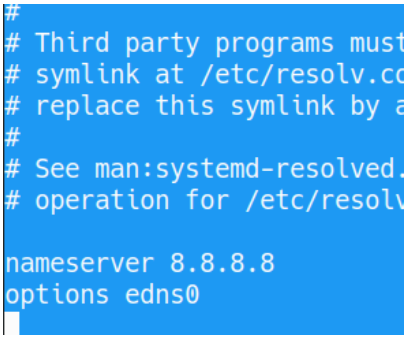
Oprim resolverul systemd

```
sudo systemctl stop systemd-resolved
```

Introducem un nameserver in /etc/resolv.conf

```
sudo mcedit /etc/resolv.conf
```

inlocuim nameserverul local cu 8.8.8.8



Oprim network-managerul

```
sudo service network-manager stop
```

Oprim bluetooth-ul

```
sudo service bluetooth stop
```

Dupa aceasta succesiune de comenzi ar trebui ca in regiunea de sus sa nu mai apara nici o conexiune. Rezultatul depinde insa de distributia de linux si de versiune

In continuare putem observa diferitele tipuri de trafic si cum apar conexiunile in netstat.

Monitorizarea diferitelor tipuri de trafic

1. HTTP

1. http trafic
    a. links www.google.com
    b. cautam ceva in google
    c. sarim la unul dintre rezultate (eventual wikipedia)
    d. observam ca ambele conexiuni raman valide (google si wikipedia).
    e. inchidem links - connectiunile devin TIME_WAIT (not reusable)

2. https traffic - 1. conexiune pe portul 80, apoi 443 (hotnews.ro)
3. http/https diferenta de keepalive, determinata de serverul web

2. ftp trafic

1. ftp student.greecore.ro - nu exista, ramane in syn_sent
2. ftp test.rebex.net - (user:demo parola: password) exista, conexiunea se stabileste

3. smtp trafic

telnet test.rebex.net 25 - se vede conexiunea care apare

4. trafic ssh

ssh demo@test.rebex.net (parola: password).

Ce servicii ruleaza pe computer?

sudo apt-get install nginx

service nginx start - 0.0.0.0:80 - toate interfetele, LISTEN
links http://localhost - apar doua conextiuni, directa si inversa, dar pe 127.0.0.1

sudo apt-get install postfix

service postfix start - apare serverul de mail + trimitere de e-mail.

Sesiune SMTP (comenzile utilizatorului cu albastru)

Este o idee buna monitorizarea concomitenta a logului (sudo tail if /var/log/mail.log)

```
telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 KUBUNTU ESMTP Postfix (Ubuntu)

EHLO
250-KUBUNTU
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250-DSN
250-SMTPUTF8
250 CHUNKING
MAIL FROM:<user@localhost.me>
250 2.1.0 Ok
RCPT TO:<o adresa de email valida>
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: Sper ca aceasta scrisoare...

Salut,

Ce parere ai despre noul aparat de curatat aerul care functioneaza fara
curent? Se mai numeste si fereastra!

SorinM
.
250 2.0.0 Ok: queued as 76D976F54C
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```

Ce servicii ruleaza pe alte computere?

sudo apt-get install nmap

sudo nmap test.rebex.net

Monitorizarea traficului

iftop -n (P pentru afisarea porturilor)

se observa si conexiunile dns
se observa si cea de-a doua conexiune ftp

Inspectarea completa a pachetelor

wireshark

1. ping trafic - inspect DNS (UDP) si ICMP. Atentie: TTL-ul este la nivel de IP.
2. Trafic HTTP - conexiune TCP care are SYN - ACK, requestul HTTP, raspunsul HTTP. Apoi FIN, ACK.
    a. Inspectarea raspunsului HTTP.
3. Trafic HTTPS - conexiune TCP, schimb de chei, trafic criptat
4. Trafic FTP - parola trimisa in clar
5. Trafic ssh - pachete de tip PSH ACK - PUSH ACK, litera cu litera

tcpdump -vv

sudo tcpdump -vv | grep -v STP