

Praktikum

Network Troubleshooting

I. Tujuan

Praktikan mampu menganalisis dan menyelesaikan troubleshooting pada jaringan Komputer atau internet

II. Keperluan

- a. Komputer dengan OS Linux Fedora Core 5 dan WindowsXP
- b. Repository fedora core 5
- c. Praktikan sudah pernah menggunakan command line (CLI) di Linux dan Command Prompt di Windows

III. Dasar Teori

Dalam menyelesaikan berbagai network troubleshooting, kita harus sudah menguasai beberapa hal, mulai dari memahami layanan layanan yang berhubungan dengan jaringan (DNS, DHCP, Routing, Internet Akses, Email, Proxy dll), protokol protokol Jaringan TCP/IP, Subnetting, Nating, dan berbagai penggunaan jaringan lainnya. Untuk level advanced atau pada jaringan yang kompleks seperti adanya teknologi baru Switching (multilayer), kita diwajibkan memahami OSI layer khususnya layer Fisik (layer 1) hingga layer Transport (layer 4). Pada praktikum network troubleshooting ini, praktikan akan mencoba menyelesaikan permasalahan jaringan yang sederhana dengan memanfaatkan tools tools yang berhubungan dengan services jaringan pada sistem operasi Windows dan Linux.

IV. Langkah langkah Praktikum

A. Windows OS

Praktikan mencoba memahami dan memanfaatkan tools tools jaringan seperti nslookup, ping, tracert, pathping, netdiag, ipconfig.

1. ipconfig

ipconfig merupakan tools untuk menampilkan setting jaringan yang digunakan oleh sebuah komputer. Administrator atau pengguna sebelum menggunakan tools lainnya, sebaiknya memeriksa hasil tools ini terlebih dahulu, memastikan bahwa konfigurasi yang di entri (secara manual) atau yang didapatkan dari server DHCP sudah valid.

Opsi yang dipraktekkan : **ipconfig**, **ipconfig/all**, **ipconfig/release**,
ipconfig/renew

```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\josh>ipconfig

Windows IP Configuration

Ethernet adapter Wireless Network Connection:

    Connection-specific DNS Suffix  . : mti.net
    IP Address. . . . . : 192.168.1.103
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1

Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnected

C:\Documents and Settings\josh>
```

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\josh>ipconfig/all

Windows IP Configuration

    Host Name . . . . . : lve
    Primary Dns Suffix . . . . . : 
    Node Type . . . . . : Hybrid
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : mti.net

Ethernet adapter Wireless Network Connection:

    Connection-specific DNS Suffix  . : mti.net
    Description . . . . . : Intel(R) PRO/Wireless 2200BG Network
    Connection
    Physical Address. . . . . : 00-13-CE-9F-2B-07
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 192.168.1.103
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
    DHCP Server . . . . . : 192.168.1.1
    DNS Servers . . . . . : 172.20.2.20
                           202.152.4.226
                           222.124.24.18
    Primary WINS Server . . . . . : 172.20.2.20
    Lease Obtained. . . . . : Wednesday, August 30, 2006 9:23:03 AM
    Lease Expires . . . . . : Thursday, August 31, 2006 9:23:03 AM

Ethernet adapter Local Area Connection:

    Media State . . . . . : Media disconnected
    Description . . . . . : Broadcom NetLink (TM) Gigabit Ethernet
    Physical Address. . . . . : 00-0F-B0-98-3E-8A

C:\Documents and Settings\josh>
```

2. ping

Digunakan untuk test atau checking koneksi dengan menggunakan protokol ICMP. Pada jaringan umumnya administrator memanfaatkan tools ini untuk mempermudah penyelesaian troubleshooting jaringan.

Opsi yang dipraktekkan : **ping ipgateway, ping ipdnsserver, ping -t ipserver**

[illegible]

Beberapa pesan yang mungkin muncul jika pinging tidak berhasil antara lain :

TTL Expired in Transit : artinya jumlah hop (router) yang dilalui untuk berkomunikasi dengan server tersebut telah melebihi TTL (Time To Live), gunakan ping -i untuk mendefinisikan TTL pada saat melakukan ping

Destination Host Unreachable : artinya packet yang dikirimkan tidak mampu sampai ke tujuan, biasanya disebabkan oleh table routing yang tidak tepat di mesin default gateway, atau router/hop di atasnya.

Request Timed Out : artinya pesan echo replay tidak dapat diterima kembali dalam waktu yang sudah ditentukan. Biasanya pesan ini muncul karena blockade yang mungkin dilakukan oleh firewall (baik disisi router maupun di sisi target).

Ping request could not find host : artinya resolving domain server tersebut pada pc kita tidak dapat menerjemah ke IP address. Hal ini biasanya karena setting DNS client masih keliru atau komunikasi kita dengan DNS server terganggu/terputus.

3. nslookup

nslookup digunakan untuk mendiagnosa layanan DNS server, melakukan query untuk memetakan suatu domain menjadi IP address atau sebaliknya. Tools nslookup juga dapat digunakan untuk mengetahui mx (mail server) atau ns (nameserver) yang bertanggung jawab terhadap suatu domain.

Opsi yang dipraktekkan : **nslookup ugm.ac.id**, **nslookup (enter) lalu set query=mx** atau **set query=ns**

```
C:\WINDOWS\system32\cmd.exe - nslookup
C:\Documents and Settings\josh>nslookup
DNS request timed out.
  timeout was 2 seconds.
*** Can't find server name for address 172.20.2.20: Timed out
DNS request timed out.
  timeout was 2 seconds.
*** Can't find server name for address 202.152.4.226: Timed out
Default Server:  server.te.ugm.ac.id
Address:  222.124.24.18

> set type=mx
> ugm.ac.id
Server:  server.te.ugm.ac.id
Address:  222.124.24.18

DNS request timed out.
  timeout was 2 seconds.
Non-authoritative answer:
ugm.ac.id      MX preference = 200, mail exchanger = mx3.ugm.ac.id
ugm.ac.id      MX preference = 0, mail exchanger = proxymail.ugm.ac.id

ugm.ac.id      nameserver = ns1.ugm.ac.id
ugm.ac.id      nameserver = ns2.ugm.ac.id
mx3.ugm.ac.id  internet address = 222.124.24.5
proxymail.ugm.ac.id  internet address = 222.124.24.3
ns1.ugm.ac.id  internet address = 222.124.24.2
ns2.ugm.ac.id  internet address = 222.124.24.3
> gmail.com
Server:  server.te.ugm.ac.id
Address:  222.124.24.18

Non-authoritative answer:
gmail.com      MX preference = 10, mail exchanger = alt1.gmail-smtp-in.l.google.com
gmail.com      MX preference = 10, mail exchanger = alt2.gmail-smtp-in.l.google.com
gmail.com      MX preference = 50, mail exchanger = gsmtpl63.google.com
gmail.com      MX preference = 50, mail exchanger = gsmtpl83.google.com
gmail.com      MX preference = 5, mail exchanger = gmail-smtp-in.l.google.com

gmail.com      nameserver = ns4.google.com
gmail.com      nameserver = ns1.google.com
gmail.com      nameserver = ns2.google.com
gmail.com      nameserver = ns3.google.com
ns4.google.com  internet address = 216.239.38.10
ns1.google.com  internet address = 216.239.32.10
ns2.google.com  internet address = 216.239.34.10
ns3.google.com  internet address = 216.239.36.10
>
```

```
C:\WINDOWS\system32\cmd.exe - nslookup
C:\Documents and Settings\josh>nslookup
*** Can't find server name for address 172.20.2.20: Non-existent domain
DNS request timed out.
    timeout was 2 seconds.
*** Can't find server name for address 202.152.4.226: Tined out
Default Server:  server.te.ugm.ac.id
Address:  222.124.24.18

> set type=ns
> gadjahmada.edu
Server:  server.te.ugm.ac.id
Address:  222.124.24.18

gadjahmada.edu  nameserver = ns1.gadjahmada.edu
gadjahmada.edu  nameserver = ns2.gadjahmada.edu
ns1.gadjahmada.edu  internet address = 222.124.24.18
ns2.gadjahmada.edu  internet address = 222.124.24.12
> ui.ac.id
Server:  server.te.ugm.ac.id
Address:  222.124.24.18

Non-authoritative answer:
ui.ac.id        nameserver = ns1.itb.ac.id
ui.ac.id        nameserver = ns3.padinet.com
ui.ac.id        nameserver = uicsgtw.cs.ui.ac.id

ns1.itb.ac.id   internet address = 202.249.24.65
ns1.itb.ac.id   internet address = 167.205.23.1
uicsgtw.cs.ui.ac.id   internet address = 152.118.24.8
ns1.itb.ac.id   AAAA IPv6 address = 2001:d30:3::53
ns1.itb.ac.id   AAAA IPv6 address = 2001:d30:103:3000::53
> itb.ac.id
Server:  server.te.ugm.ac.id
Address:  222.124.24.18

Non-authoritative answer:
itb.ac.id       nameserver = endor.the.net.id
itb.ac.id       nameserver = uicsgtw.cs.ui.ac.id
itb.ac.id       nameserver = ns1.ai3.net
itb.ac.id       nameserver = NS1.itb.ac.id
itb.ac.id       nameserver = ns2.itb.ac.id
itb.ac.id       nameserver = ns3.itb.ac.id

endor.the.net.id   internet address = 202.153.128.14
uicsgtw.cs.ui.ac.id   internet address = 152.118.24.8
ns1.ai3.net        internet address = 202.249.24.33
NS1.itb.ac.id      internet address = 202.249.24.65
ns1.itb.ac.id      internet address = 167.205.23.1
ns2.itb.ac.id      internet address = 167.205.22.123
ns3.itb.ac.id      internet address = 167.205.64.158
ns3.itb.ac.id      internet address = 167.205.30.114
NS1.itb.ac.id      AAAA IPv6 address = 2001:d30:3::53
NS1.itb.ac.id      AAAA IPv6 address = 2001:d30:103:3000::53
ns2.itb.ac.id      AAAA IPv6 address = 2001:d30:3:1::53
ns3.itb.ac.id      AAAA IPv6 address = 2001:d30:3:278::53
>
```

4. tracert

tracert singkatan dari traceroute, yakni tool untuk menampilkan jalur atau routing perjalanan packet komunikasi antara komputer kita dengan komputer (server) lain. Tool ini akan menampilkan jumlah hop (router) yang dilalui ketika menuju server target.

Opsi yang digunakan : **tracert ipserver/domain**, **tracert -d ipserver/domain**

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\josh>tracert www.ugm.ac.id

Tracing route to www.ugm.ac.id [222.124.24.14]
over a maximum of 30 hops:

  1    1 ms    1 ms    1 ms    192.168.1.1
  2    2 ms    1 ms    1 ms    172.24.14.1
  3    2 ms    2 ms    2 ms    10.42.1.254
  4    3 ms    4 ms    2 ms    10.254.254.30
  5    2 ms    2 ms    2 ms    172.16.30.3
  6    2 ms    2 ms    2 ms    222.124.24.14

Trace complete.

C:\Documents and Settings\josh>tracert www.ui.ac.id

Tracing route to muara.ui.edu [152.118.24.11]
over a maximum of 30 hops:

  1    2 ms    1 ms    2 ms    192.168.1.1
  2    2 ms    1 ms    1 ms    172.24.14.1
  3    2 ms    2 ms    2 ms    10.42.1.254
  4    2 ms    1 ms    1 ms    10.254.254.30
  5    2 ms    3 ms   17 ms    172.16.30.3
  6    2 ms    2 ms    2 ms    inetgw3.ugm.ac.id [222.124.24.9]
  7    3 ms    6 ms    4 ms    167.205.136.4
  8    3 ms    3 ms    3 ms    167.205.136.1
  9   10 ms   18 ms   16 ms    167.205.191.18
 10   14 ms   33 ms   15 ms    167.205.191.14
 11   15 ms   14 ms   16 ms    ui-inherent.gw.ui.ac.id [152.118.255.249]
 12   15 ms   15 ms   15 ms    muara.ui.edu [152.118.24.11]

Trace complete.

C:\Documents and Settings\josh>
```

5. pathping

merupakan tools pada windows yang digunakan untuk mengukur network latency dan network loss (dalam persentase) pada hop tertentu diantara alamat asal dan alamat tujuan.

Opsi yang digunakan : **pathping -n ipserver/domain**

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\josh>pathping

Usage: pathping [-g host-list] [-h maximum_hops] [-i address] [-n]
               [-p period] [-q num_queries] [-w timeout] [-P] [-R] [-T]
               [-4] [-6] target_name

Options:
  -g host-list      Loose source route along host-list.
  -h maximum_hops  Maximum number of hops to search for target.
  -i address        Use the specified source address.
  -n               Do not resolve addresses to hostnames.
  -p period         Wait period milliseconds between pings.
  -q num_queries    Number of queries per hop.
  -w timeout        Wait timeout milliseconds for each reply.
  -P               Test for RSUP PATH connectivity.
  -R               Test if each hop is RSUP aware.
  -T               Test connectivity to each hop with Layer-2 priority tags.
  -4               Force using IPv4.
  -6               Force using IPv6.

C:\Documents and Settings\josh>
```

```

C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\josh>pathping -n www.ugm.ac.id

Tracing route to www.ugm.ac.id [222.124.24.14]
over a maximum of 30 hops:
 0 192.168.1.103
 1 192.168.1.1
 2 172.24.14.1
 3 10.42.1.254
 4 10.254.254.30
 5 172.16.30.3
 6 222.124.24.14

Computing statistics for 150 seconds...
Hop  RTT      Source to Here   This Node/Link   Address
 0      0/ 100 = 0%      4/ 100 = 4%      192.168.1.103
 1    2ms      4/ 100 = 4%      0/ 100 = 0%      192.168.1.1
 2    2ms      7/ 100 = 7%      2/ 100 = 2%      172.24.14.1
 3    2ms      6/ 100 = 6%      1/ 100 = 1%      10.42.1.254
 4    2ms      6/ 100 = 6%      1/ 100 = 1%      10.254.254.30
 5    ---     100/ 100 =100%   95/ 100 = 95%     172.16.30.3
 6    3ms      5/ 100 = 5%      0/ 100 = 0%      222.124.24.14

Trace complete.

C:\Documents and Settings\josh>

```

6. Netstat

Netstat singkatan dari network status, digunakan untuk berbagai keperluan, antara lain menampilkan tabel routing, menampilkan services yang berjalan pada Windows, menampilkan port protokol komunikasi yang sedang terjadi.

Opsi yang dipraktekkan: **netstat -rn**, **netstat -an**

```

C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\josh>netstat -an

Active Connections

Proto Local Address          Foreign Address         State
TCP   0.0.0.0:135             0.0.0.0:0               LISTENING
TCP   0.0.0.0:445             0.0.0.0:0               LISTENING
TCP   127.0.0.1:1030         0.0.0.0:0               LISTENING
TCP   192.168.1.103:139      0.0.0.0:0               LISTENING
UDP   0.0.0.0:445            *:*                      *:*
UDP   0.0.0.0:500            *:*                      *:*
UDP   0.0.0.0:1025           *:*                      *:*
UDP   0.0.0.0:4500           *:*                      *:*
UDP   127.0.0.1:123          *:*                      *:*
UDP   127.0.0.1:1047         *:*                      *:*
UDP   127.0.0.1:1900         *:*                      *:*
UDP   192.168.1.103:123      *:*                      *:*
UDP   192.168.1.103:137      *:*                      *:*
UDP   192.168.1.103:138      *:*                      *:*
UDP   192.168.1.103:1900     *:*                      *:*

C:\Documents and Settings\josh>

```



```

C:\Documents and Settings\josh>netstat -rn

Route Table
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x2 ...00 13 ce 9f 2b 07 ..... Intel(R) PRO/Wireless 2200BG Network Connection
- Packet Scheduler Miniport
0x3 ...00 0f b0 98 3e 8a ..... Broadcom NetLink (TM) Gigabit Ethernet - Packet
Scheduler Miniport
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          192.168.1.1      192.168.1.103     25
127.0.0.0                  255.0.0.0        127.0.0.1        127.0.0.1         1
192.168.1.0                255.255.255.0    192.168.1.103    192.168.1.103     25
192.168.1.103              255.255.255.255  127.0.0.1        127.0.0.1         25
192.168.1.255              255.255.255.255  192.168.1.103    192.168.1.103     25
224.0.0.0                  240.0.0.0        192.168.1.103    192.168.1.103     25
255.255.255.255            255.255.255.255  192.168.1.103    192.168.1.103     3
255.255.255.255            255.255.255.255  192.168.1.103    192.168.1.103     1
Default Gateway:          192.168.1.1
=====
Persistent Routes:
None
C:\Documents and Settings\josh>

```

Troubleshooting Network yang paling sering terjadi pada Windows

Koneksi Internet Terputus, apa yang harus dilakukan ?

Beberapa langkah yang sebaiknya diikuti adalah sebagai berikut :

Step 1: Cek nyala lampu pada Ethernet dan kabel Ethernet

- Jika tidak ada tanda koneksi, check kabelnya
- Cek juga lampu pada hub/switch termasuk powernya.

Step 2: Pastikan, setting ip,dns dan default gw sudah dikonfigurasi dengan tepat.

- gunakan ipconfig, ipconfig/all untuk memeriksa.
- gunakan ipconfig/release, ipconfig/renew untuk jaringan yang menggunakan dhcp.

Step 3: Ping Default Gateway

- ip default gateway dapat dilihat melalui perintah ipconfig

Step 4: Ping DNS dan proxy server (jika policy jaringan harus menggunakan proxy)

Step 5: Jika semuanya berhasil, ping dan tracert ke ipserverdns dan ipserverproxy

Step 6: Jika semuanya berhasil, coba ping dan tracert ke situs luar spt www.google.com

B. Linux OS

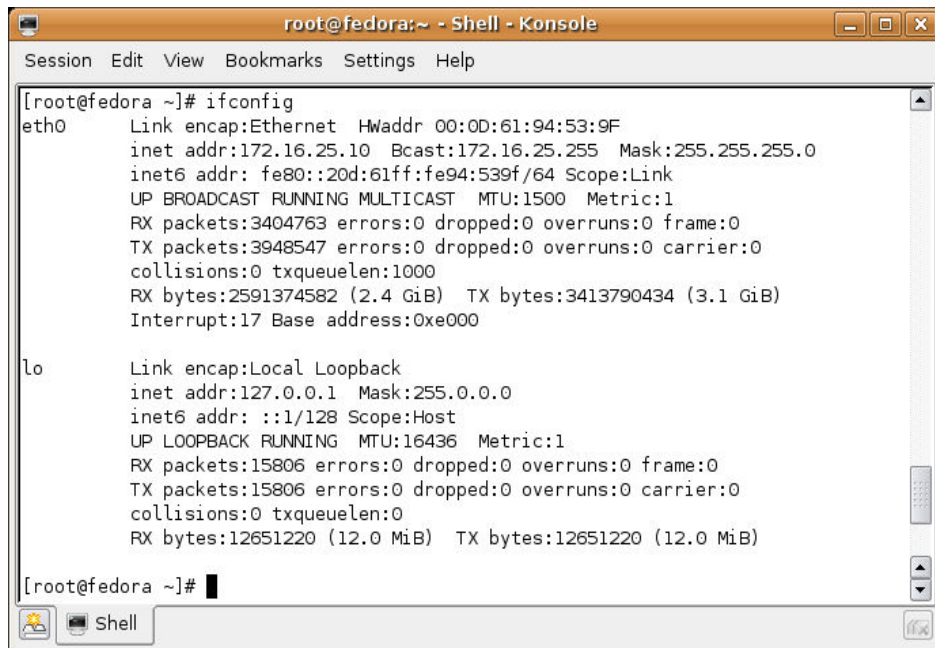
Mirip dengan pada Sistem Operasi Windows, pada Linux juga terdapat beberapa tools atau utility yang fungsinya hampir sama untuk mengatasi berbagai masalah pada jaringan.

Misalnya :

1. ifconfig

Digunakan untuk menampilkan atau melakukan setting TCP/IP pada interface jaringan yang kita miliki.

Beberapa option yang coba dipraktekkan, ifconfig, ifconfig -a, ifconfig eth0



```
root@fedora:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

[root@fedora ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0D:61:94:53:9F
          inet addr:172.16.25.10  Bcast:172.16.25.255  Mask:255.255.255.0
          inet6 addr: fe80::20d:61ff:fe94:539f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3404763 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3948547 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2591374582 (2.4 GiB)  TX bytes:3413790434 (3.1 GiB)
          Interrupt:17 Base address:0xe000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:15806 errors:0 dropped:0 overruns:0 frame:0
          TX packets:15806 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:12651220 (12.0 MiB)  TX bytes:12651220 (12.0 MiB)

[root@fedora ~]#
```

2. mii-tools dan ethtool untuk memeriksa status koneksi dan teknologi yang disupport oleh sebuah kartu jaringan.

```
root@fedora:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

[root@fedora ~]# mii-tool -v
eth0: negotiated 100baseTx-FD, link ok
product info: vendor 00:00:00, model 0 rev 0
basic mode: autonegotiation enabled
basic status: autonegotiation complete, link ok
capabilities: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD
advertising: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD
link partner: 100baseTx-FD 100baseTx-HD 10baseT-FD 10baseT-HD
[root@fedora ~]#
```

Jika terasa jaringan agak melambat, kita dapat memanfaatkan checking error oleh ethtool
Dengan menggunakan option -S pada command ethtool spt :

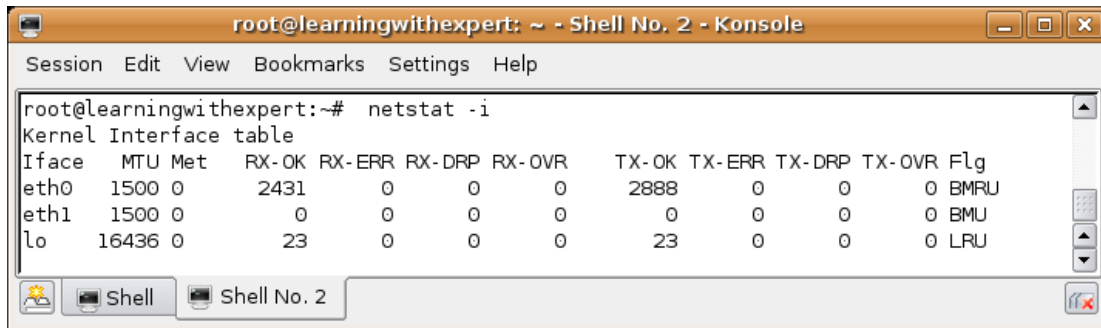
```
root@fedora:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

[root@fedora ~]# ethtool eth0
Settings for eth0:
    Supported ports: [ TP MII ]
    Supported link modes:   10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
    Supports auto-negotiation: Yes
    Advertised link modes:  10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
    Advertised auto-negotiation: Yes
    Speed: 100Mb/s
    Duplex: Full
    Port: MII
    PHYAD: 32
    Transceiver: internal
    Auto-negotiation: on
    Supports Wake-on: pumbg
    Wake-on: d
    Current message level: 0x00000007 (7)
    Link detected: yes
[root@fedora ~]#
```

```
root@learningwithexpert: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help

root@learningwithexpert:~# ethtool -S eth0
NIC statistics:
    rx_packets: 1813595
    rx_fragments: 0
    rx_ucast_packets: 2295
    rx_mcast_packets: 0
    rx_bcast_packets: 97
    rx_fcs_errors: 0
    rx_align_errors: 0
    rx_xon_pause_rcvd: 0
    rx_xoff_pause_rcvd: 0
    rx_mac_ctrl_rcvd: 0
    rx_xoff_entered: 0
    rx_frame_too_long_errors: 0
    rx_jabbers: 0
    rx_undersize_packets: 0
    rx_in_length_errors: 0
    rx_out_length_errors: 0
```

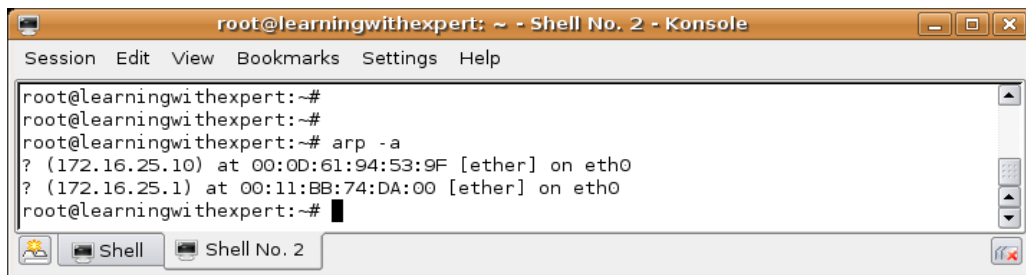
3. Command `netstat -i` juga dapat digunakan untuk memeriksa jumlah packet error pada suatu interface



```
root@learningwithexpert: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help

root@learningwithexpert:~# netstat -i
Kernel Interface table
Iface  MTU Met  RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
eth0   1500 0      2431   0       0       0    2888   0       0       0  BMRU
eth1   1500 0         0   0       0       0         0   0       0       0  BMU
lo     16436 0         23   0       0       0         23   0       0       0  LRU
```

4. Kadang kala untuk keamanan sebagai admin, kita perlu mendaftarkan MAC address masing masing komputer yang dapat dilihat menggunakan command `ifconfig -a` atau `arp -a` (untuk mac address komputer yang terhubung ke komputer kita)

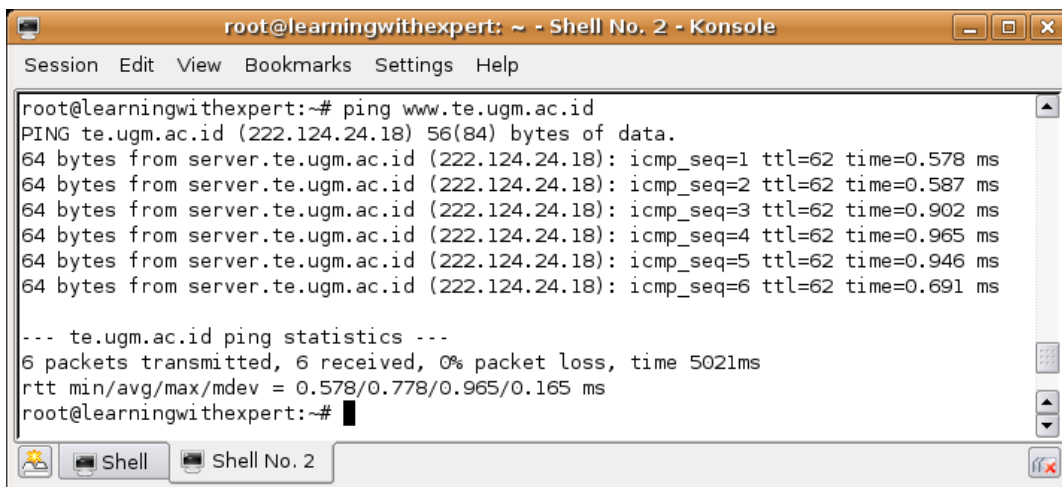


```
root@learningwithexpert: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help

root@learningwithexpert:~#
root@learningwithexpert:~#
root@learningwithexpert:~# arp -a
? (172.16.25.10) at 00:0D:61:94:53:9F [ether] on eth0
? (172.16.25.1) at 00:11:BB:74:DA:00 [ether] on eth0
root@learningwithexpert:~#
```

5. S
a
m
a

seperti pada Sistem Operasi Windows, tools Ping di Linux digunakan untuk testing koneksi terhadap suatu titik (server/komputer)



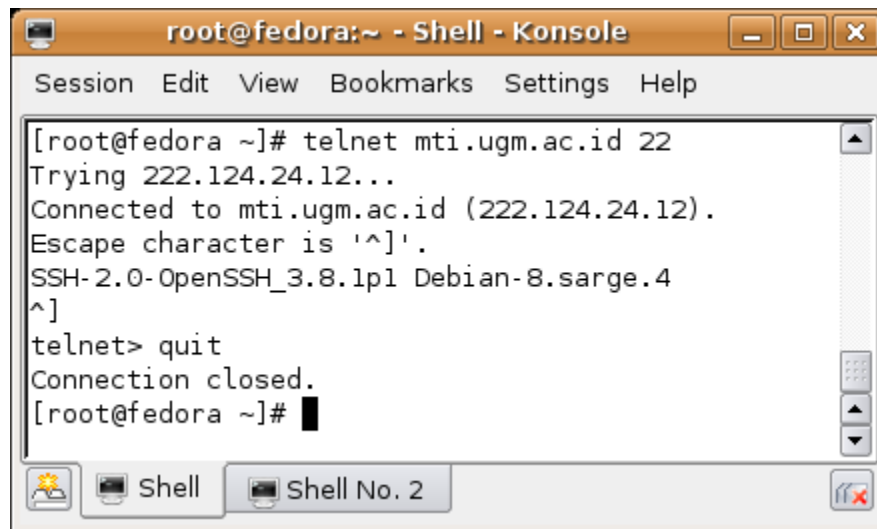
```
root@learningwithexpert: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help

root@learningwithexpert:~# ping www.te.ugm.ac.id
PING te.ugm.ac.id (222.124.24.18) 56(84) bytes of data.
64 bytes from server.te.ugm.ac.id (222.124.24.18): icmp_seq=1 ttl=62 time=0.578 ms
64 bytes from server.te.ugm.ac.id (222.124.24.18): icmp_seq=2 ttl=62 time=0.587 ms
64 bytes from server.te.ugm.ac.id (222.124.24.18): icmp_seq=3 ttl=62 time=0.902 ms
64 bytes from server.te.ugm.ac.id (222.124.24.18): icmp_seq=4 ttl=62 time=0.965 ms
64 bytes from server.te.ugm.ac.id (222.124.24.18): icmp_seq=5 ttl=62 time=0.946 ms
64 bytes from server.te.ugm.ac.id (222.124.24.18): icmp_seq=6 ttl=62 time=0.691 ms

--- te.ugm.ac.id ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5021ms
rtt min/avg/max/mdev = 0.578/0.778/0.965/0.165 ms
root@learningwithexpert:~#
```

Pesan pesan yang ditampilkan jika tidak ada replay, sama dengan hasil ping di Windows

6. Selain menggunakan ping, untuk melakukan test koneksi dapat juga dilakukan dengan menggunakan telnet ke host dan port TCP suatu server. Misalnya melakukan telnet ke port 22(SSH) suatu server



```
root@fedora:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

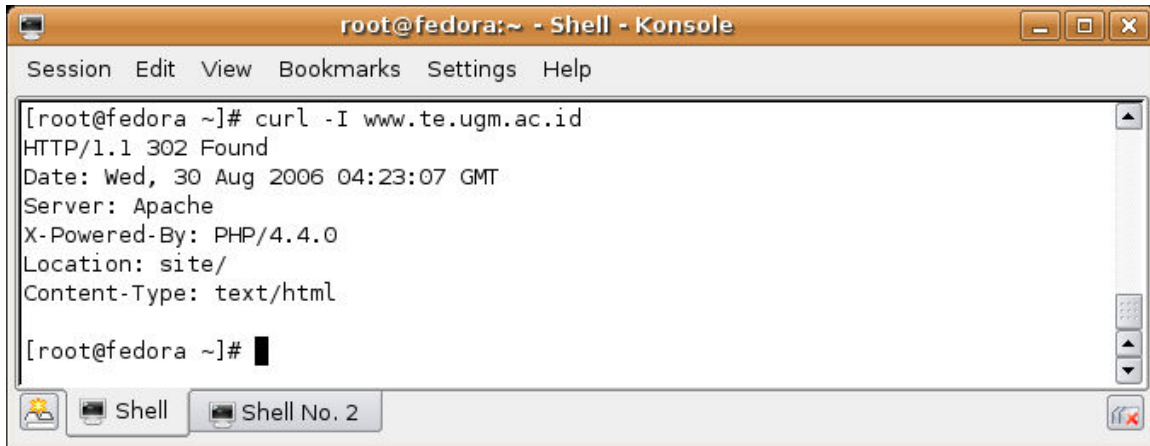
[root@fedora ~]# telnet mti.ugm.ac.id 22
Trying 222.124.24.12...
Connected to mti.ugm.ac.id (222.124.24.12).
Escape character is '^]'.
SSH-2.0-OpenSSH_3.8.1p1 Debian-8.sarge.4
^]
telnet> quit
Connection closed.
[root@fedora ~]#
```

Untuk keluar dari perintah tersebut, tekan CTRL +] , kemudian ketikkan quit.

Jika muncul connection refused, ada dua kemungkinan :

- Services TCP yang kita coba terhubung, belum aktif atau tidak running
- Ada firewall yang memblok koneksi ke protokol TCP tersebut..

7. Untuk memeriksa layanan aplikasi berbasis web pada sebuah server, dapat menggunakan utilitas curl, dengan option -I pada command curl, dapat diperoleh aplikasi yang berjalan pada sebuah webserver.

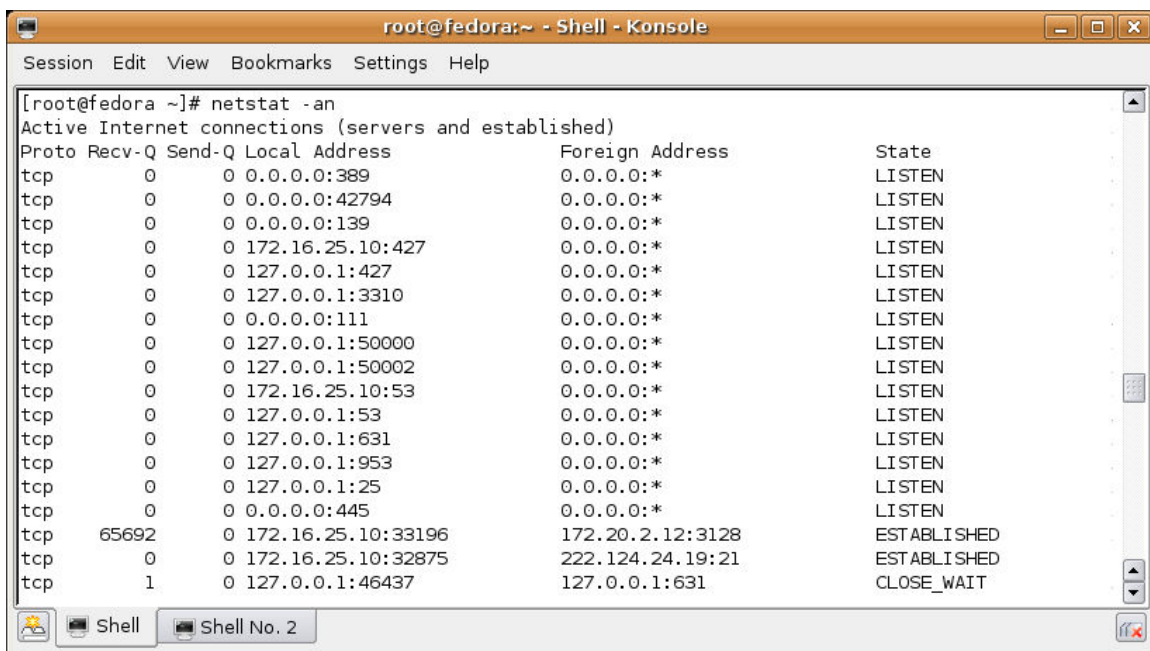


```
root@fedora:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

[root@fedora ~]# curl -I www.te.ugm.ac.id
HTTP/1.1 302 Found
Date: Wed, 30 Aug 2006 04:23:07 GMT
Server: Apache
X-Powered-By: PHP/4.4.0
Location: site/
Content-Type: text/html

[root@fedora ~]#
```

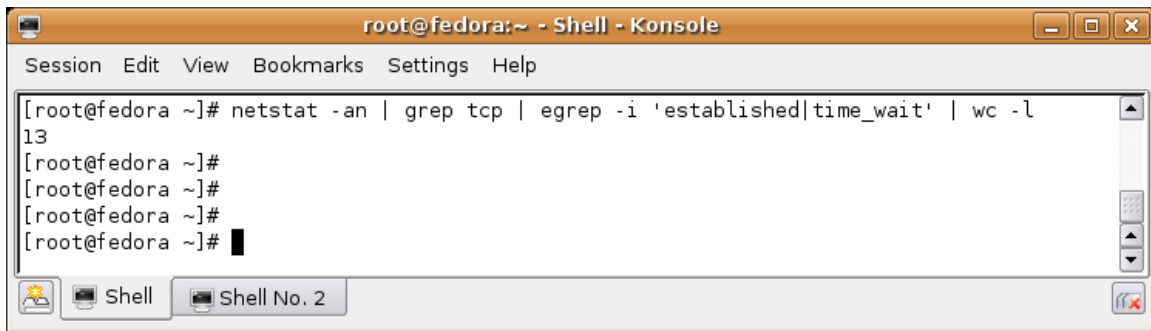
8. Selain menggunakan curl, tools lain yang dapat dilakukan untuk mendeteksi adanya permasalahan pada jaringan atau server adalah “netstat -an “. Perintah ini akan menampilkan komunikasi atau layanan yang berjalan pada sebuah komputer/server.



```
root@fedora:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

[root@fedora ~]# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:389             0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:42794           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN
tcp        0      0 172.16.25.10:427        0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:427           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3310          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:50000         0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:50002         0.0.0.0:*               LISTEN
tcp        0      0 172.16.25.10:53         0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:53           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:953           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:445             0.0.0.0:*               LISTEN
tcp    65692      0 172.16.25.10:33196      172.20.2.12:3128        ESTABLISHED
tcp        0      0 172.16.25.10:32875      222.124.24.19:21        ESTABLISHED
tcp        1      0 127.0.0.1:46437         127.0.0.1:631           CLOSE_WAIT
```

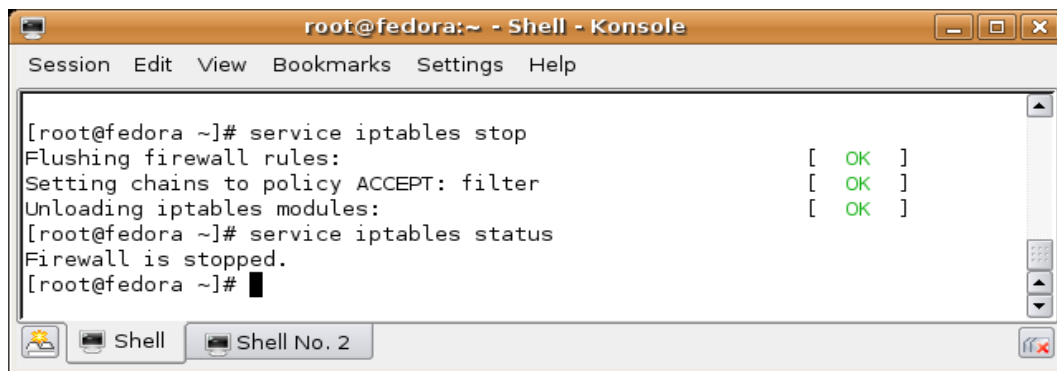
Misalnya untuk menampilkan jumlah koneksi yang sedang terjadi antara komputer kita dengan komputer/server lain dapat menggunakan command berikut :

A terminal window titled "root@fedora:~ - Shell - Konsole" with a menu bar (Session, Edit, View, Bookmarks, Settings, Help). The command executed is `netstat -an | grep tcp | egrep -i 'established|time_wait' | wc -l`, which returns the output `13`. The prompt is `[root@fedora ~]#`.

```
root@fedora:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

[root@fedora ~]# netstat -an | grep tcp | egrep -i 'established|time_wait' | wc -l
13
[root@fedora ~]#
[root@fedora ~]#
[root@fedora ~]#
[root@fedora ~]#
```

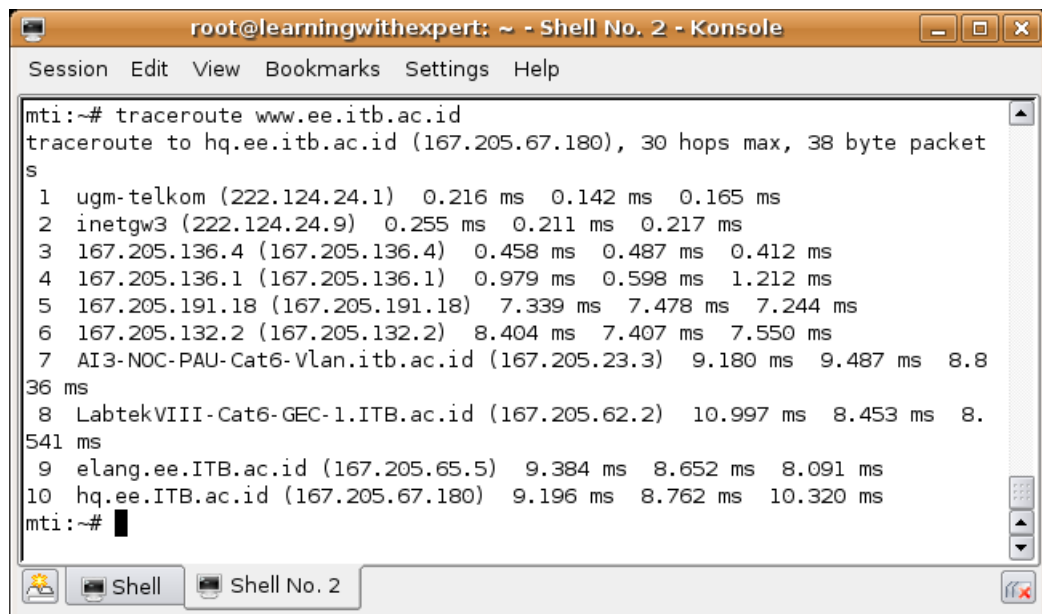
9. Secara default sistem operasi fedora akan menjalankan firewall secara otomatis ketika dinyalakan. Untuk upaya troubleshooting jaringan, sebaiknya services firewall (iptables) dinonaktifkan terlebih dahulu.

A terminal window titled "root@fedora:~ - Shell - Konsole" with a menu bar (Session, Edit, View, Bookmarks, Settings, Help). The commands executed are `service iptables stop` and `service iptables status`. The first command shows the process of flushing rules, setting policy to ACCEPT, and unloading modules, with green [OK] status for each step. The second command shows "Firewall is stopped." The prompt is `[root@fedora ~]#`.

```
root@fedora:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

[root@fedora ~]# service iptables stop
Flushing firewall rules:          [ OK ]
Setting chains to policy ACCEPT: filter [ OK ]
Unloading iptables modules:      [ OK ]
[root@fedora ~]# service iptables status
Firewall is stopped.
[root@fedora ~]#
```

10. Tools “traceroute” fungsinya sama dengan tools “tracert” di Sistem Windows, digunakan untuk testing link koneksi terhadap server tertentu. Tracert maupun traceroute menggunakan protokol icmp.

A terminal window titled "root@learningwithexpert: ~ - Shell No. 2 - Konsole" with a menu bar (Session, Edit, View, Bookmarks, Settings, Help). The command executed is `traceroute www.ee.itb.ac.id`. The output shows the path from the user's machine to the destination, with hop numbers, IP addresses, and round-trip times in milliseconds. The prompt is `mti:~#`.

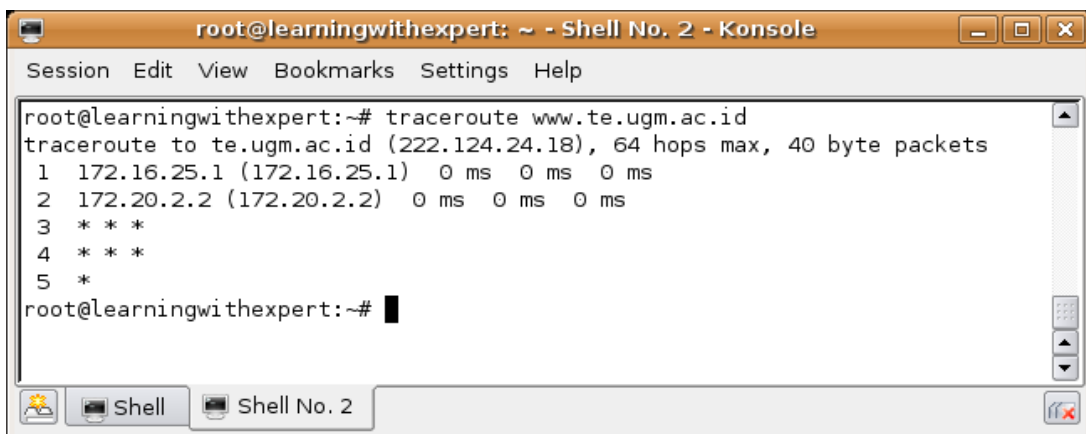
```
root@learningwithexpert: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help

mti:~# traceroute www.ee.itb.ac.id
traceroute to hq.ee.itb.ac.id (167.205.67.180), 30 hops max, 38 byte packet
s
 1 ugm-telkom (222.124.24.1)  0.216 ms  0.142 ms  0.165 ms
 2 inetgw3 (222.124.24.9)  0.255 ms  0.211 ms  0.217 ms
 3 167.205.136.4 (167.205.136.4)  0.458 ms  0.487 ms  0.412 ms
 4 167.205.136.1 (167.205.136.1)  0.979 ms  0.598 ms  1.212 ms
 5 167.205.191.18 (167.205.191.18)  7.339 ms  7.478 ms  7.244 ms
 6 167.205.132.2 (167.205.132.2)  8.404 ms  7.407 ms  7.550 ms
 7 AI3-NOC-PAU-Cat6-Vlan.itb.ac.id (167.205.23.3)  9.180 ms  9.487 ms  8.8
36 ms
 8 LabtekVIII-Cat6-GEC-1.ITB.ac.id (167.205.62.2)  10.997 ms  8.453 ms  8.
541 ms
 9 elang.ee.ITB.ac.id (167.205.65.5)  9.384 ms  8.652 ms  8.091 ms
10 hq.ee.ITB.ac.id (167.205.67.180)  9.196 ms  8.762 ms  10.320 ms
mti:~#
```


Pesan pesan yang mungkin muncul pada hasil traceroute

Hasil Traceroute	Penjelasan
* * *	Tanda bintang “* * *” artinya bahwa respons time untuk menuju router atau hop selanjutnya sudah habis, respons time untuk perintah traceoute adalah 5 detik. Hal ini dapat disebabkan oleh. > Router yang ingin dilalui tidak mengirimkan echo replay (disable) > Router atau firewall pada titik tersebut melakukan blocking icmp. > IP Alamat Tujuan tidak aktif atau tidak melakukan respons
!H, !N, or !P	Tanda tersebut menyatakan bahwa Host (komputer), network or protocol unreachable. Biasanya karena koneksi router pada hop tersebut terputus.
!X or !A	Menyatakan bahwa komunikasi dengan router dilakukan filtering menggunakan ACL (Access Control List)/
!S	Menyatakan bahwa source atau komputer yang melakukan traceroute gagal mengirimkan frame. Biasanya masalah setting security pada level kernel di Linux

Contoh :



```
root@learningwithexpert: ~ - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
root@learningwithexpert:~# traceroute www.te.ugm.ac.id
traceroute to te.ugm.ac.id (222.124.24.18), 64 hops max, 40 byte packets
 1 172.16.25.1 (172.16.25.1)  0 ms  0 ms  0 ms
 2 172.20.2.2 (172.20.2.2)  0 ms  0 ms  0 ms
 3 * * *
 4 * * *
 5 *
root@learningwithexpert:~#
```


11. Selain traceroute, tools yang lebih powerfull adalah “mtr”. Dengan mtr dapat dilihat jalur dan packet loss yang terjadi selama diperjalanan.

Perintah: mtr www.google.com , menghasilkan :

```
root@fedora:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

My traceroute [v0.69]
mti.ugm.ac.id (0.0.0.0)(tos=0x0 psize=64 bitpatternWed Aug 30 12:33:33 2006
Keys: Help Display mode Restart statistics Order of fields quit

Packets
Host      Loss%  Snt  Last  Avg  Best  Wrst StDev
1. 222.124.24.1      0.0%   13   1.8   0.4   0.2   1.8   0.5
2. 192.168.9.253    30.8%   13  10.4  17.9   1.3  40.2  12.6
3. 61.94.15.238      0.0%   13  47.3  59.2  32.7 210.2  46.5
4. 203.208.143.233   15.4%   13  54.5 123.7  34.4 234.4  91.5
5. 203.208.182.205   0.0%   13  42.2  47.9  33.5  62.7   9.3
6. 203.208.182.58    0.0%   12 344.9 287.5 249.2 344.9  28.7
7. ge-4-3-0.plapx-ar3.ix.singte 25.0%   12 279.6 274.0 260.9 288.2   9.8
8. 72.14.197.165    16.7%   12 417.0 269.3 238.9 417.0  52.6
9. 209.85.130.6      0.0%   12 256.6 253.0 240.5 268.4   9.1
10. 72.14.233.131    8.3%   12 264.8 263.6 240.9 276.9  11.4
    66.249.94.226
11. 72.14.233.129    9.1%   12 240.3 257.4 240.3 275.3  10.8
    216.239.49.66
12. 66.102.7.99      0.0%   12 258.9 268.7 248.6 289.3  13.5
    216.239.49.54
```

12. Tools sederhana untuk menganalisa jaringan pada sistem operasi Linux seperti tcpdump, juga dapat dilakukan untuk melihat traffic. Biasanya administrator menganalisa traffic untuk mencari tahu apa saja yang sedang terjadi pada jaringannya.

```
root@fedora:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

[root@fedora ~]# tcpdump -vi eth0 icmp
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
12:42:45.516261 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto: ICMP (1), length: 84) josh.elektro > fedora.elektro: ICMP echo request, id 19504, seq 1, length 64
12:42:45.516306 IP (tos 0x0, ttl 64, id 18706, offset 0, flags [none], proto: ICMP (1), length: 84) fedora.elektro > josh.elektro: ICMP echo reply, id 19504, seq 1, length 64
12:42:46.516094 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto: ICMP (1), length: 84) josh.elektro > fedora.elektro: ICMP echo request, id 19504, seq 2, length 64
12:42:46.516120 IP (tos 0x0, ttl 64, id 18707, offset 0, flags [none], proto: ICMP (1), length: 84) fedora.elektro > josh.elektro: ICMP echo reply, id 19504, seq 2, length 64
12:42:47.516515 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto: ICMP (1), length: 84) josh.elektro > fedora.elektro: ICMP echo request, id 19504, seq 3, length 64
12:42:47.516544 IP (tos 0x0, ttl 64, id 18708, offset 0, flags [none], proto: ICMP (1), length: 84) fedora.elektro > josh.elektro: ICMP echo reply, id 19504, seq 3, length 64
```

```
root@fedora:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

[root@fedora ~]# tcpdump -i eth0 -t host 172.16.25.2 and tcp port 22
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
IP fedora.elektro.ssh > josh.elektro.42040: P 3598641059:3598641171(112) ack
1138221706 win 2872 <nop,nop,timestamp 108408666 1791767>
IP fedora.elektro.ssh > josh.elektro.42040: P 112:224(112) ack 1 win 2872 <n
op,nop,timestamp 108408666 1791767>
IP josh.elektro.42040 > fedora.elektro.ssh: . ack 112 win 16022 <nop,nop,tim
estamp 1791775 108408666>
IP josh.elektro.42040 > fedora.elektro.ssh: . ack 224 win 16022 <nop,nop,tim
estamp 1791775 108408666>
IP fedora.elektro.ssh > josh.elektro.42040: P 224:400(176) ack 1 win 2872 <n
op,nop,timestamp 108408666 1791775>
IP fedora.elektro.ssh > josh.elektro.42040: P 400:560(160) ack 1 win 2872 <n
op,nop,timestamp 108408666 1791775>
IP josh.elektro.42040 > fedora.elektro.ssh: . ack 400 win 16022 <nop,nop,tim
estamp 1791776 108408666>
IP fedora.elektro.ssh > josh.elektro.42040: P 560:704(144) ack 1 win 2872 <n
op,nop,timestamp 108408666 1791776>
IP josh.elektro.42040 > fedora.elektro.ssh: . ack 560 win 16022 <nop,nop,tim
estamp 1791776 108408666>
```

```
root@fedora:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

[root@fedora ~]# tcpdump -i eth0 -w /tmp/packets.dump tcp port 80
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 byt
es
140 packets captured
280 packets received by filter
0 packets dropped by kernel
[root@fedora ~]#
```

13. Testing DNS menggunakan tools nslookup, dig dan host

```
root@fedora:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

[root@fedora ~]# host www.ugm.ac.id
www.ugm.ac.id has address 222.124.24.14
[root@fedora ~]# nslookup google.com
Server:      127.0.0.1
Address:     127.0.0.1#53

Non-authoritative answer:
Name:   google.com
Address: 64.233.167.99
Name:   google.com
Address: 64.233.187.99
Name:   google.com
Address: 72.14.207.99

[root@fedora ~]# dig gadjahmada.edu

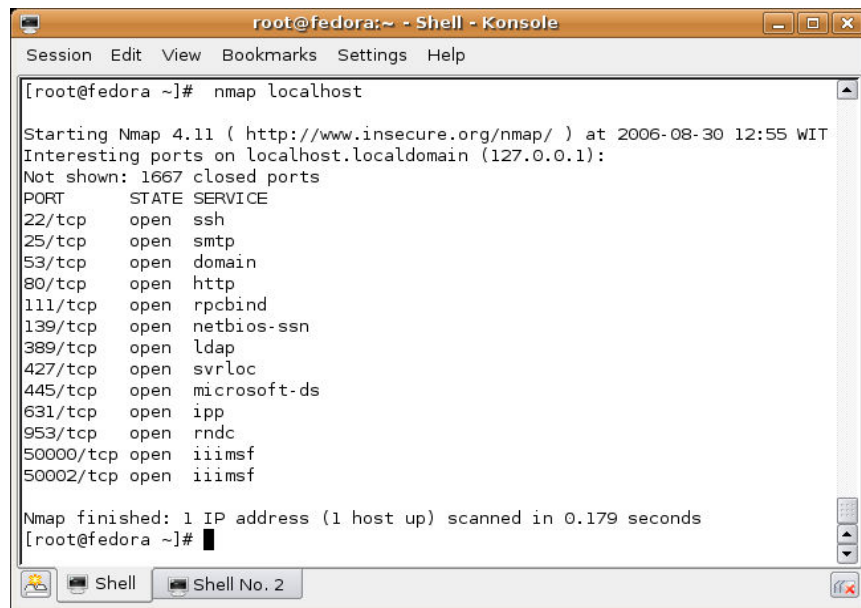
; <<>> DiG 9.3.2 <<>> gadjahmada.edu
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25742
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;gadjahmada.edu.                IN      A

;; ANSWER SECTION:
gadjahmada.edu.                43200   IN      A      222.124.24.12

;; AUTHORITY SECTION:
gadjahmada.edu.                43200   IN      NS      ns1.gadjahmada.edu.
gadjahmada.edu.                43200   IN      NS      ns2.gadjahmada.edu.
```

14. Untuk melakukan scanning network dan system, tools yang paling banyak peminatnya adalah nmap. Dengan nmap, kita dapat memeriksa suatu services pada server, scanning client, dan scanning jaringan.

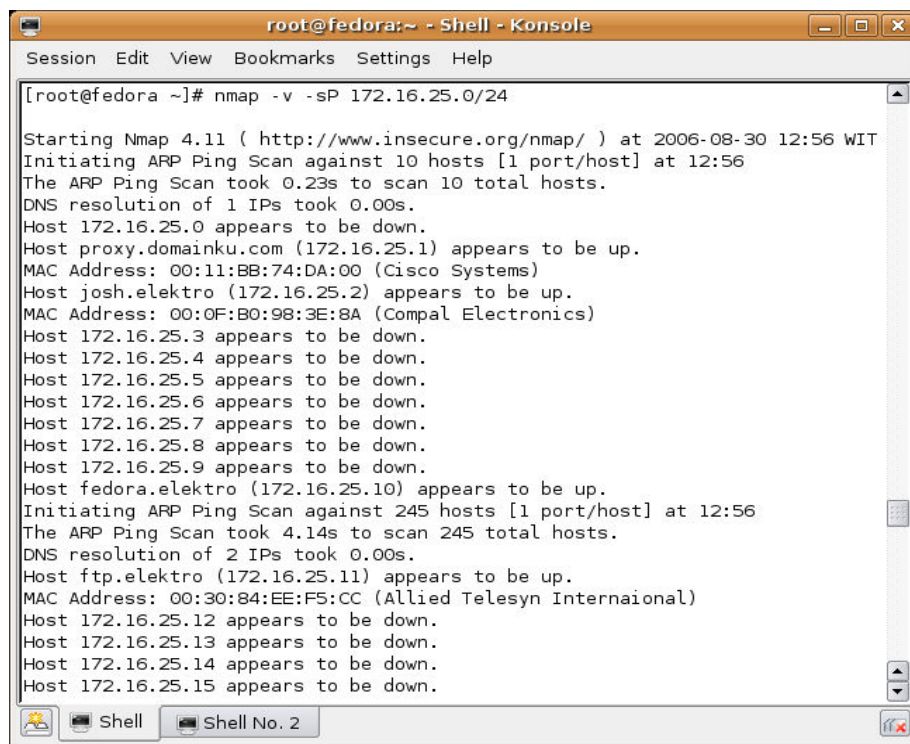


```
root@fedora:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

[root@fedora ~]# nmap localhost

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2006-08-30 12:55 WIT
Interesting ports on localhost.localdomain (127.0.0.1):
Not shown: 1667 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
389/tcp   open  ldap
427/tcp   open  svrloc
445/tcp   open  microsoft-ds
631/tcp   open  ipp
953/tcp   open  rndc
50000/tcp open  iiimsf
50002/tcp open  iiimsf

Nmap finished: 1 IP address (1 host up) scanned in 0.179 seconds
[root@fedora ~]#
```



```
root@fedora:~ - Shell - Konsole
Session Edit View Bookmarks Settings Help

[root@fedora ~]# nmap -v -sP 172.16.25.0/24

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2006-08-30 12:56 WIT
Initiating ARP Ping Scan against 10 hosts [1 port/host] at 12:56
The ARP Ping Scan took 0.23s to scan 10 total hosts.
DNS resolution of 1 IPs took 0.00s.
Host 172.16.25.0 appears to be down.
Host proxy.domainku.com (172.16.25.1) appears to be up.
MAC Address: 00:11:BB:74:DA:00 (Cisco Systems)
Host josh.elektro (172.16.25.2) appears to be up.
MAC Address: 00:0F:B0:98:3E:8A (Compal Electronics)
Host 172.16.25.3 appears to be down.
Host 172.16.25.4 appears to be down.
Host 172.16.25.5 appears to be down.
Host 172.16.25.6 appears to be down.
Host 172.16.25.7 appears to be down.
Host 172.16.25.8 appears to be down.
Host 172.16.25.9 appears to be down.
Host fedora.elektro (172.16.25.10) appears to be up.
Initiating ARP Ping Scan against 245 hosts [1 port/host] at 12:56
The ARP Ping Scan took 4.14s to scan 245 total hosts.
DNS resolution of 2 IPs took 0.00s.
Host ftp.elektro (172.16.25.11) appears to be up.
MAC Address: 00:30:84:EE:FS:CC (Allied Telesyn Internaional)
Host 172.16.25.12 appears to be down.
Host 172.16.25.13 appears to be down.
Host 172.16.25.14 appears to be down.
Host 172.16.25.15 appears to be down.
```