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 opesasi Windows dan Linux.

IV. Langkah langkah Praktikum

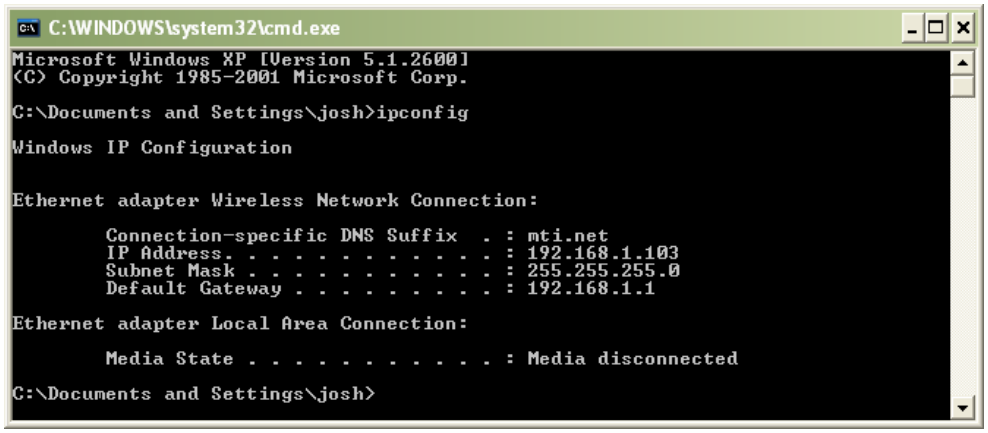
A. Windows OS

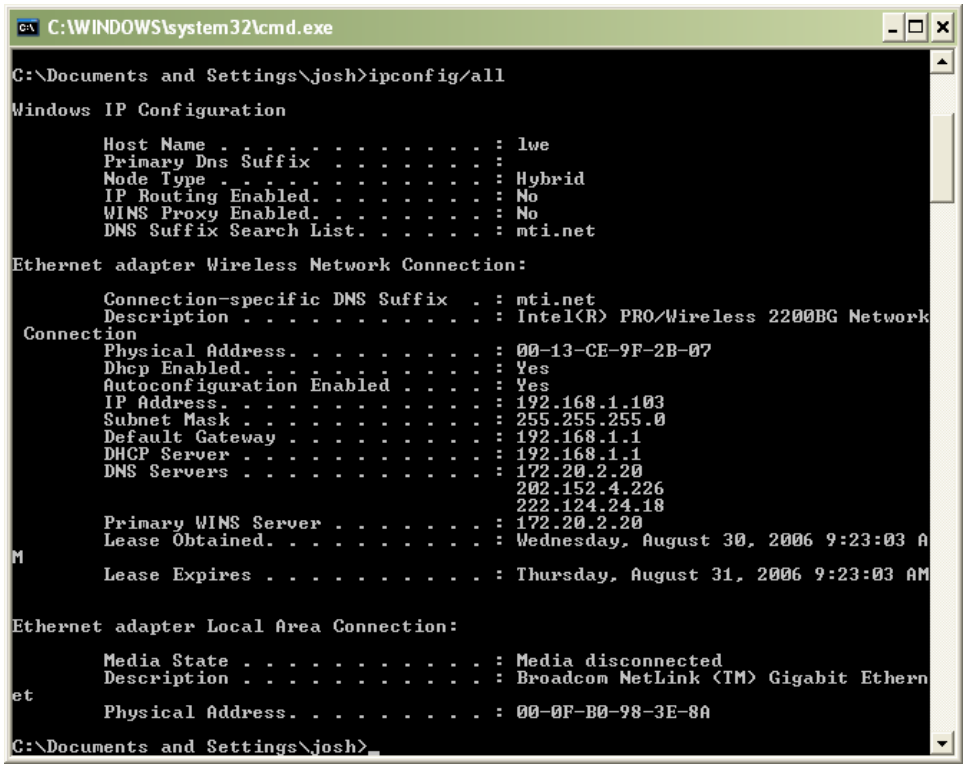
Praktikan mencoba memahami dan memanfaatkan tools tools jaringan sepert nslookup, ping, tracert, pathping, netdiag, ipconfig.

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**

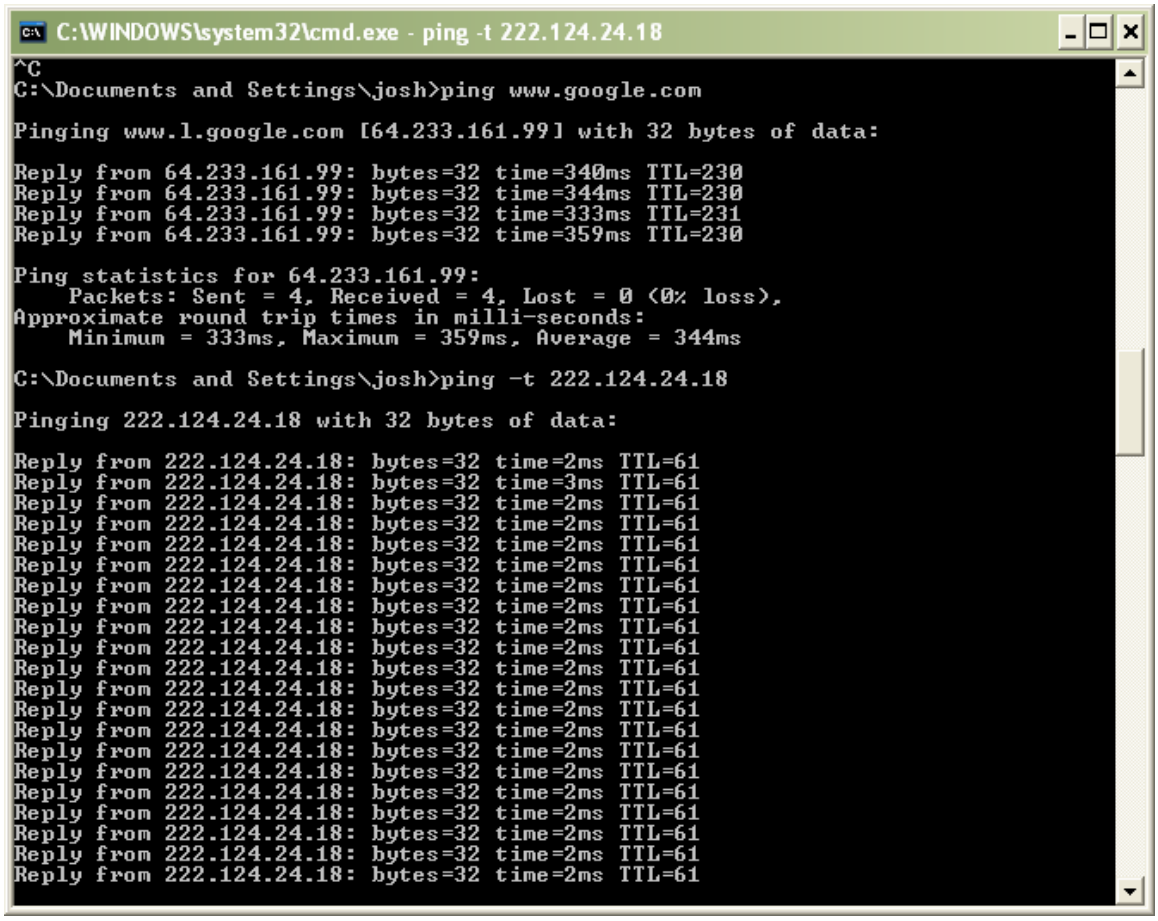




2. ping

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

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



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 diatasnya.

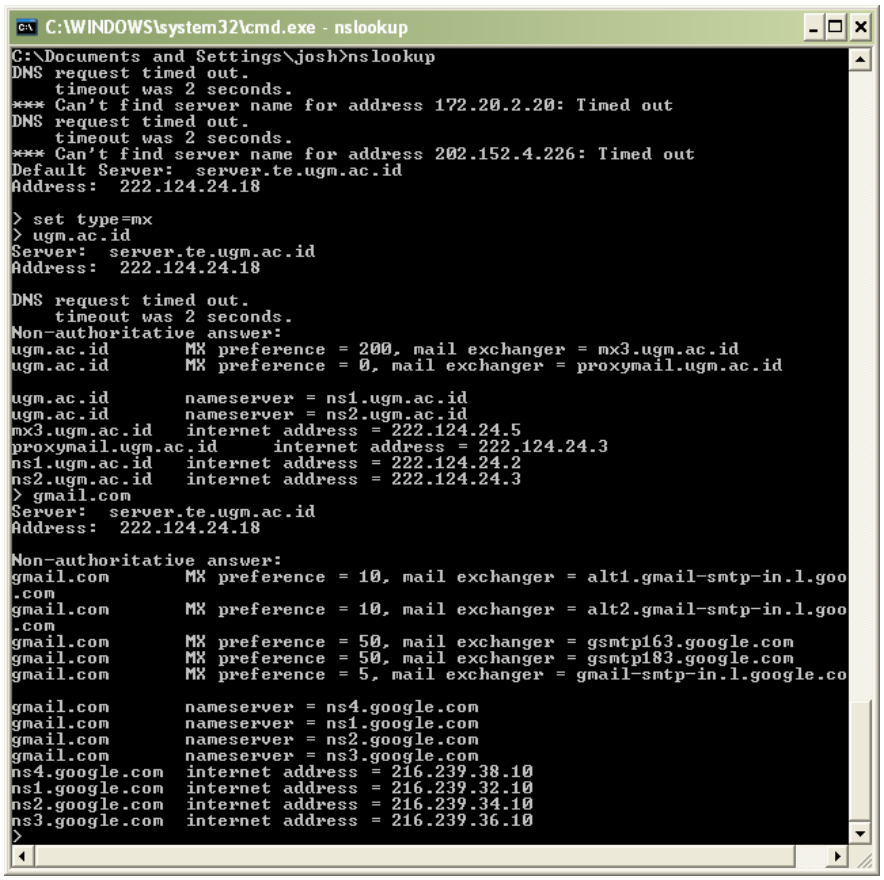
Request Timed Out : artinya pesan echo replay tidak dapat diterima kembali dalam waktu yang sudah ditentukan. Biasanya pesan ini muncul karena blockade yang mungkin dilakukan oleh firewall (baik disisi router maupun di sisi target).

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.

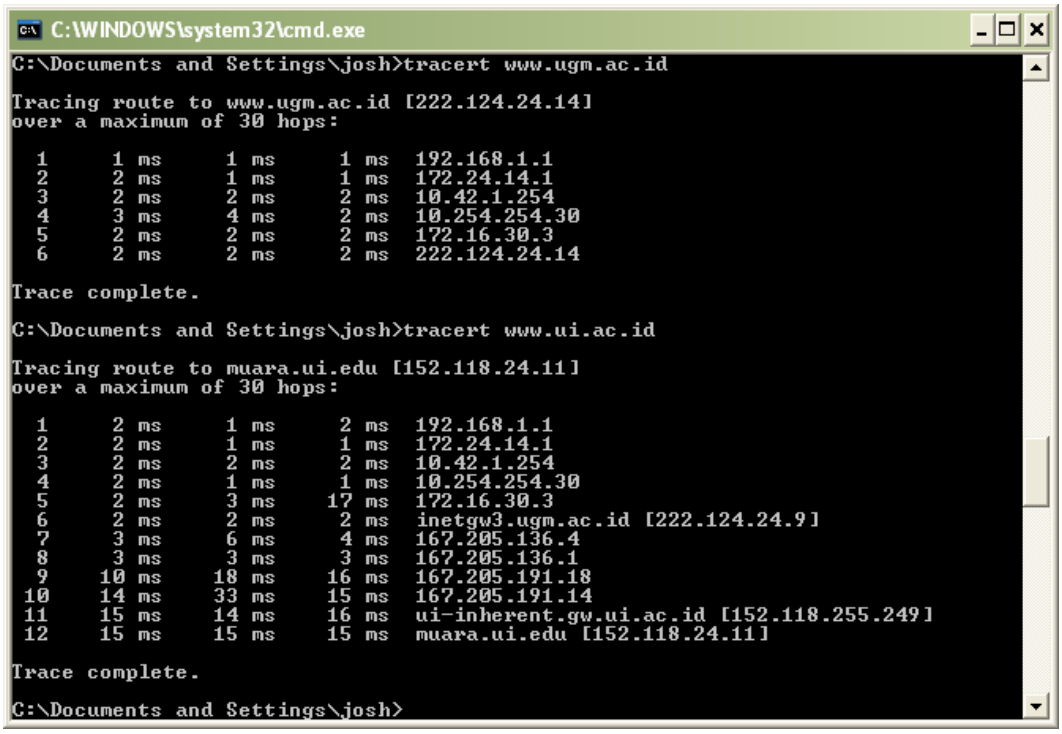
   Opsi yang dipraktekkan : **nslookup ugm.ac.id, nslookup (enter) lalu set query=mx atau set query=ns**


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.goo
.com
gmail.com MX preference = 10, mail exchanger = alt2.gmail-smtp-in.l.goo
.com
gmail.com MX preference = 50, mail exchanger = gsmtp163.google.com
gmail.com MX preference = 50, mail exchanger = gsmtp183.google.com
gmail.com MX preference = 5, mail exchanger = gmail-smtp-in.l.google.co
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
>

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.

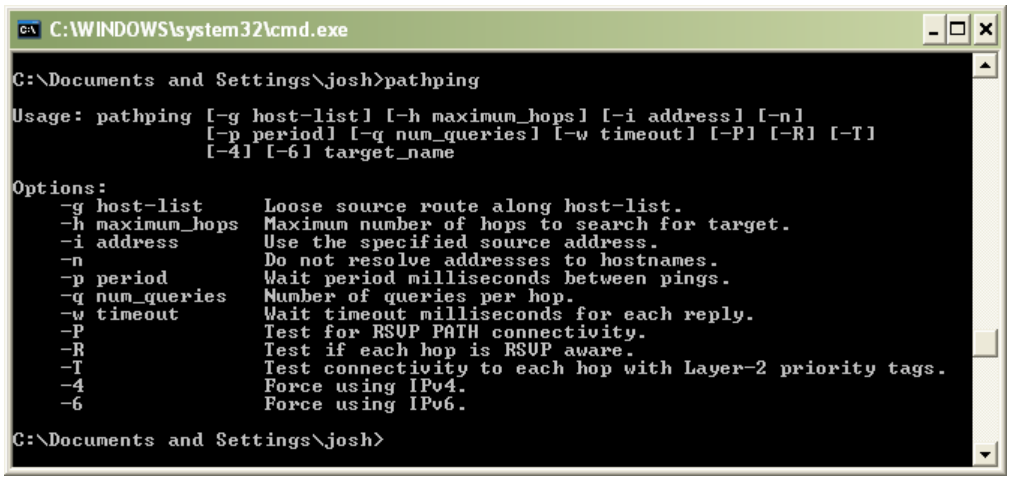
   Opsi yang digunakan : **tracert ipserver/domain, tracert -d ipserver/domain**

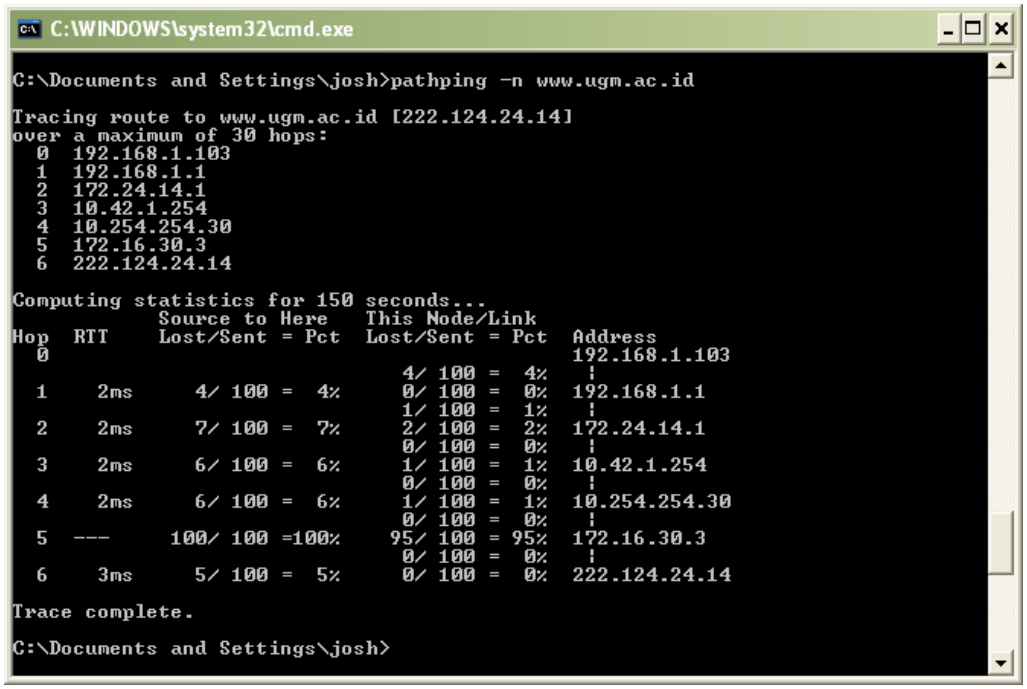


5. pathping

   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**

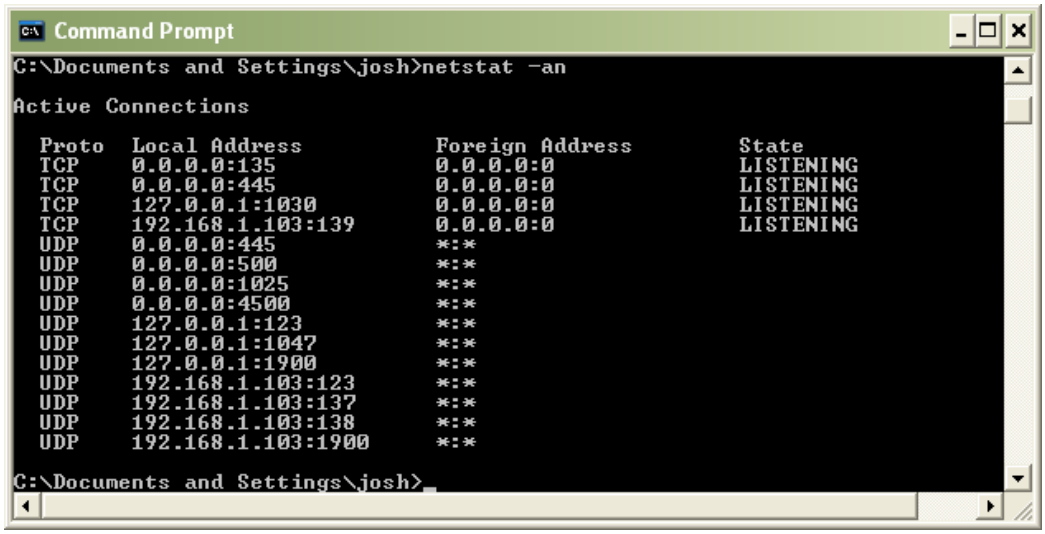


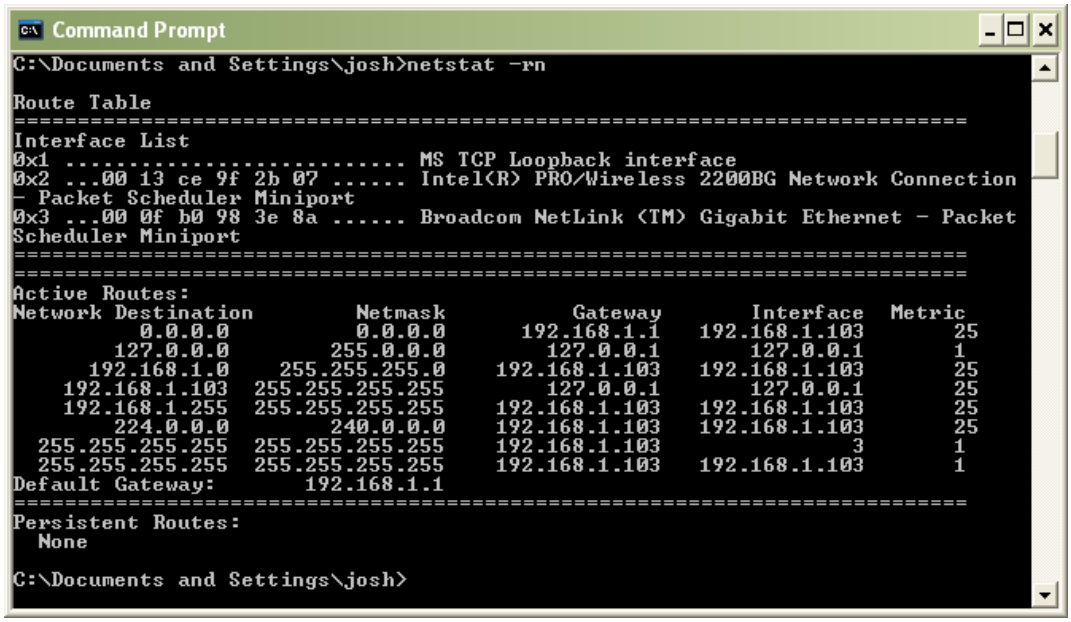


6. Netstat

   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**





Troubleshooting Network yang paling sering terjadi pada Windows

Koneksi Internet Terputus, apa yang harus dilakukan ?

Beberapa langkah yang sebaiknya diikutin 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

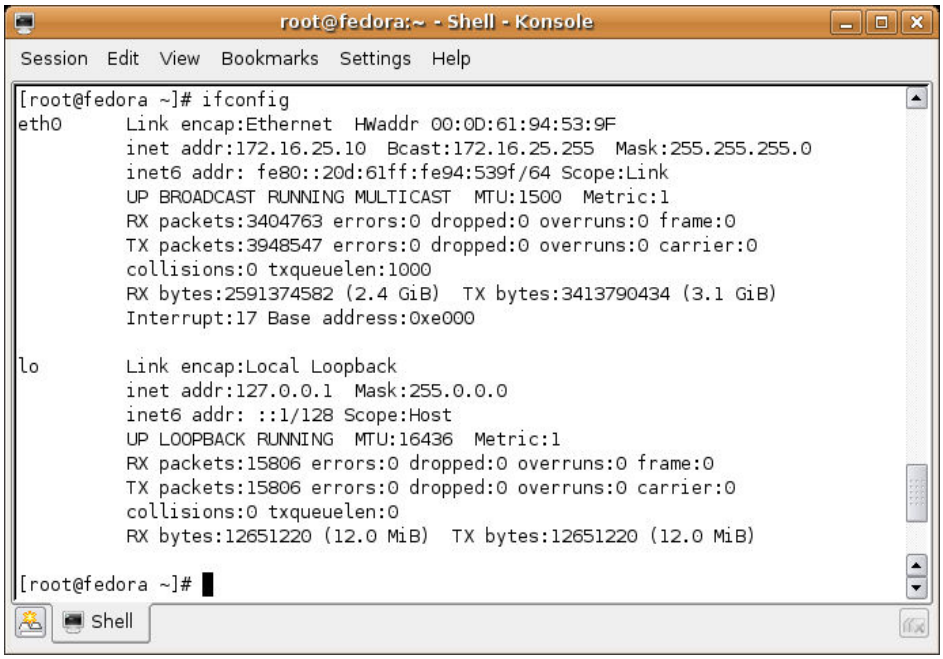
Mirip dengan pada Sistem Operasi Windows, pada Linux juga terdapat beberapa tools atau utility yang fungsinya hampir sama untuk mengatasi berbagai masalah pada jaringan.

Misalnya :

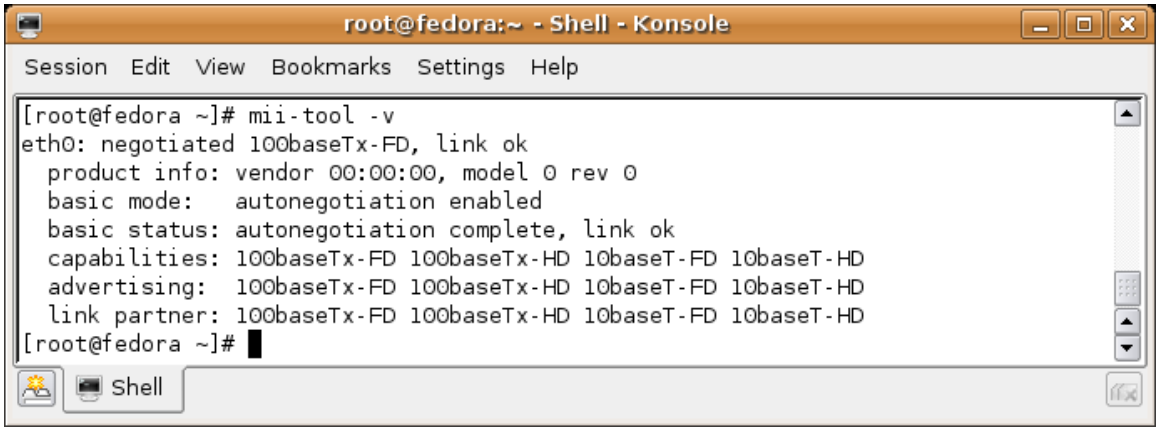
1. ifconfig

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

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

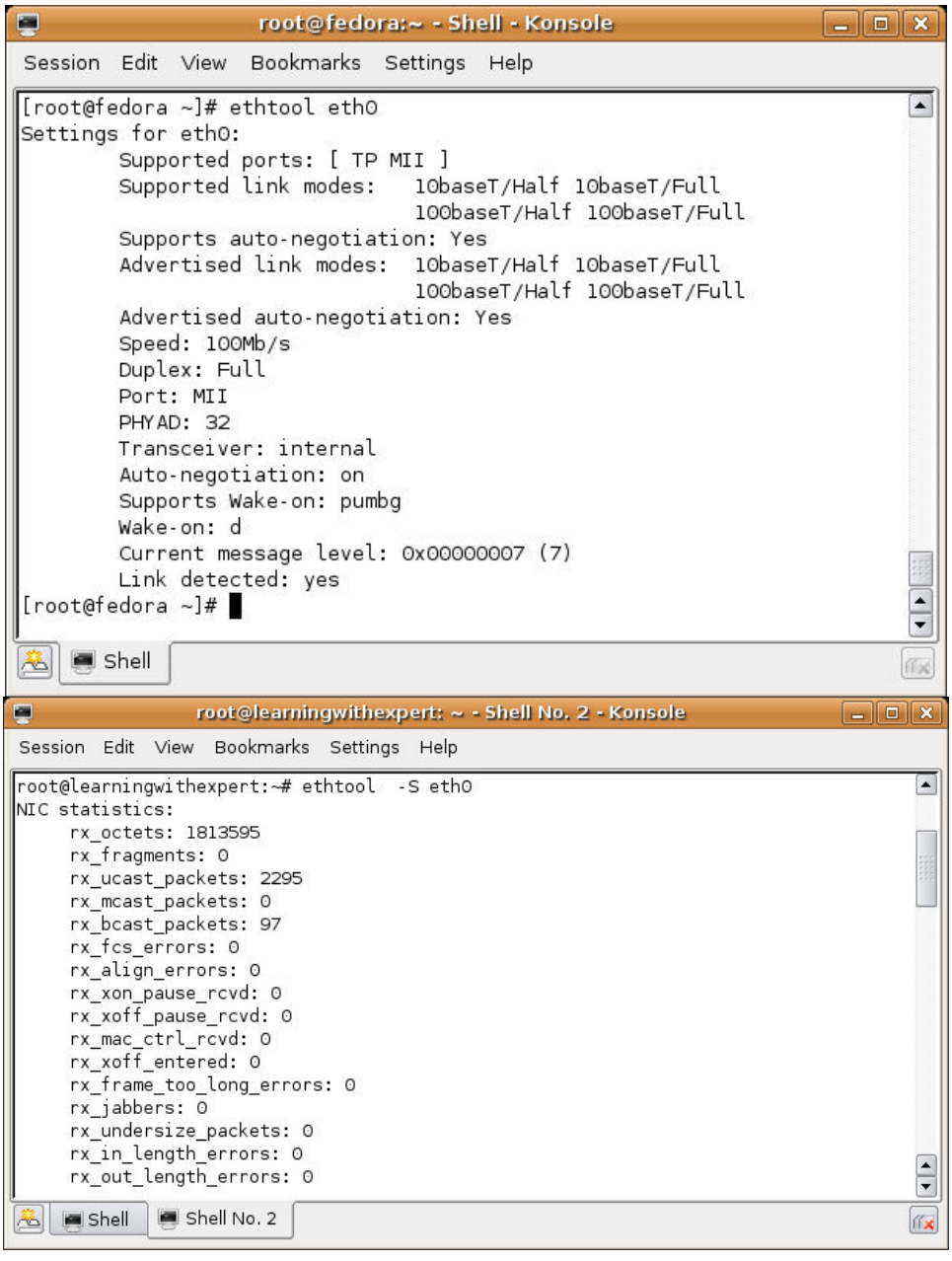


2. mii-tools dan ethtool untuk memeriksa status koneksi dan teknologi yang disupport oleh sebuah kartu jaringan.

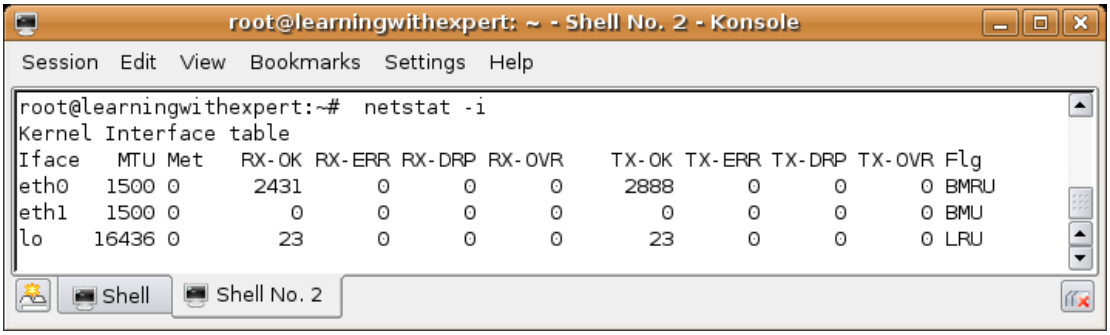


Jika terasa jaringan agak melambat, kita dapat manfaatkan checking error oleh ethtool

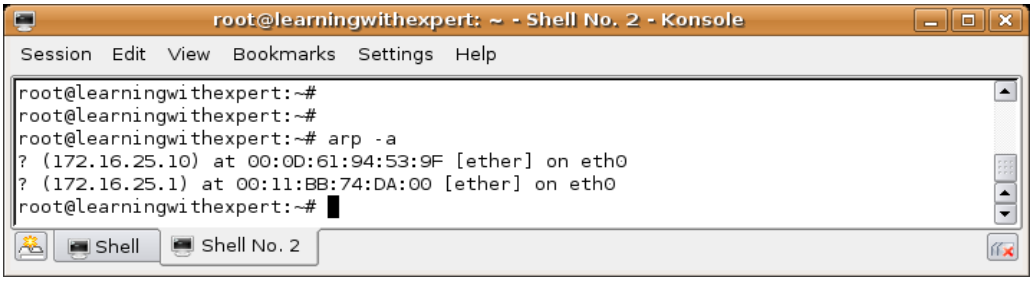
Dengan menggunakan option -S pada command ethtool spt :



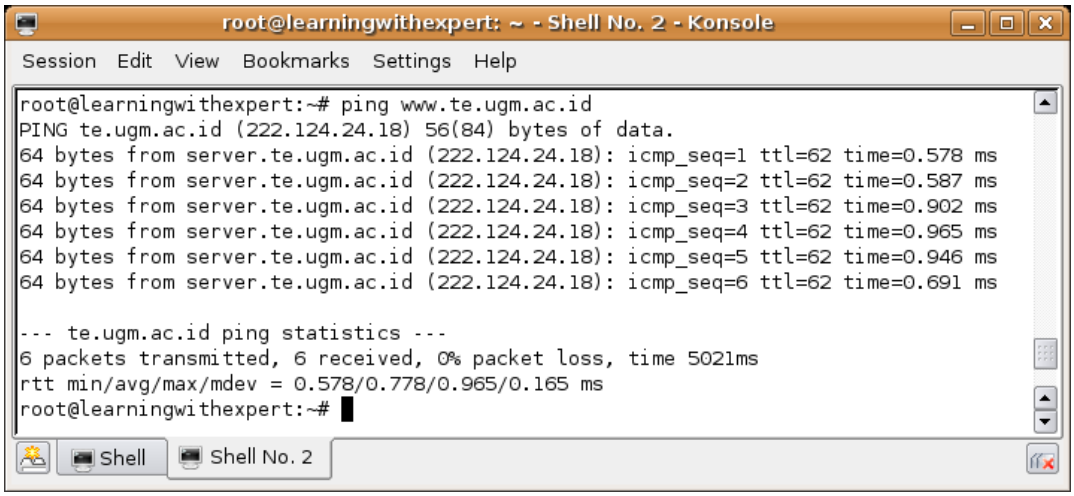
3. Command netstat -i juga dapat digunakan untuk memeriksa jumlah packet error pada suatu interface



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)

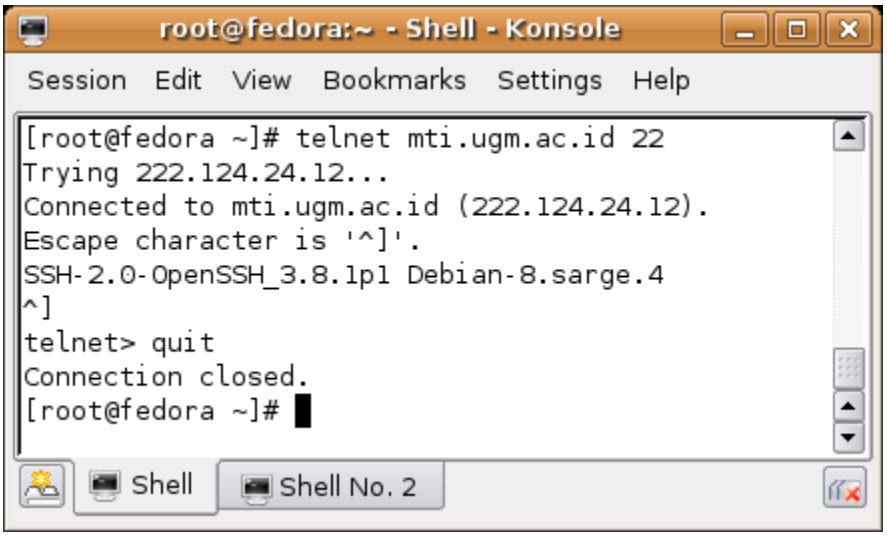


5. Sama seperti pada Sistem Operasi Windows, tools Ping di Linux digunakan untuk testing koneksi terhadap suatu titik (server/komputer)



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

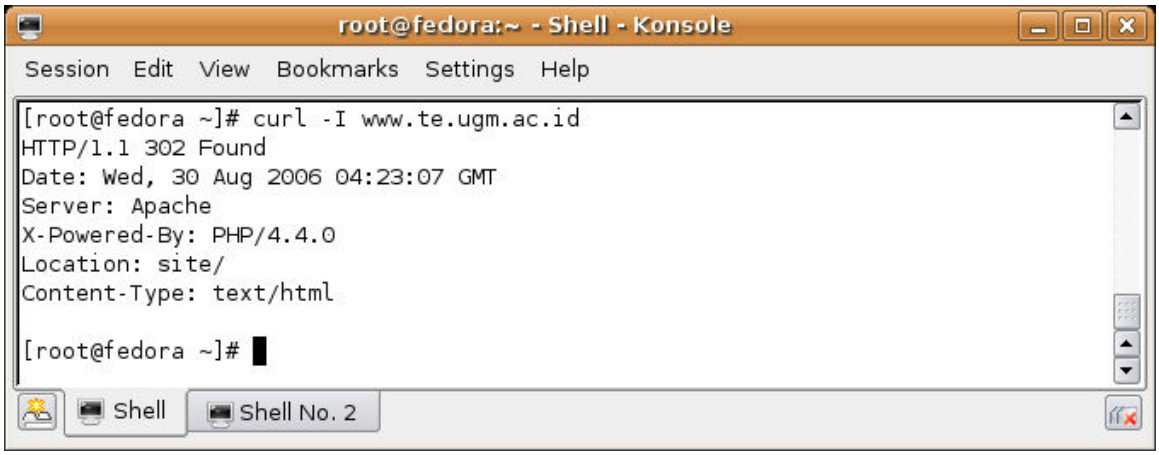


Untuk keluar dari perintah tersebut, tekan CTRL +] , kemudian ketikkan quit.

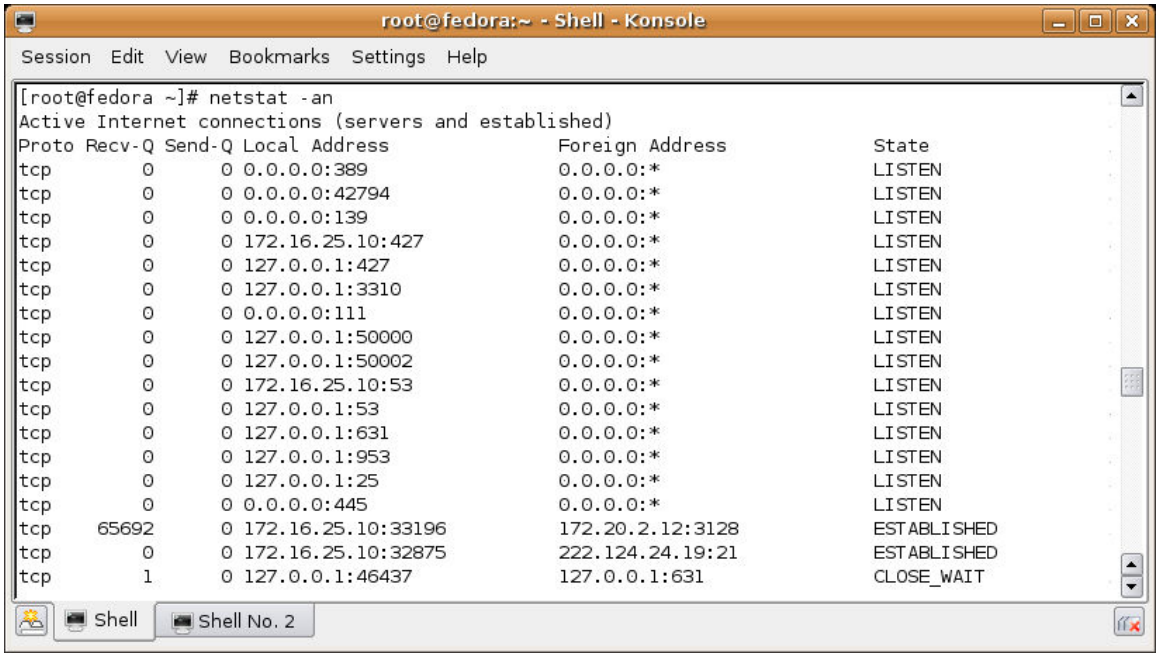
Jika muncul connection refuced, ada dua kemungkinan :

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

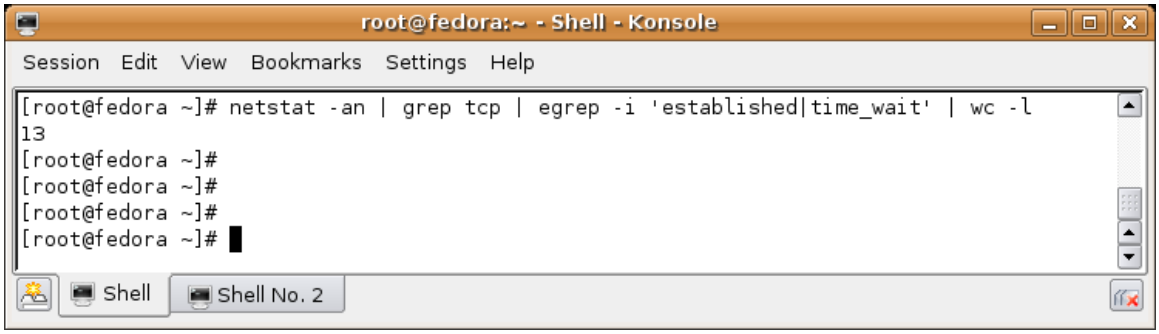
7. Untuk memeriksa layanan aplikasi berbasis web pada sebuah server, dapat menggunakan utilitas curl, dengan option -I pada command curl, dapat diperoleh aplikasi yang berjalan pada sebuah webserver.



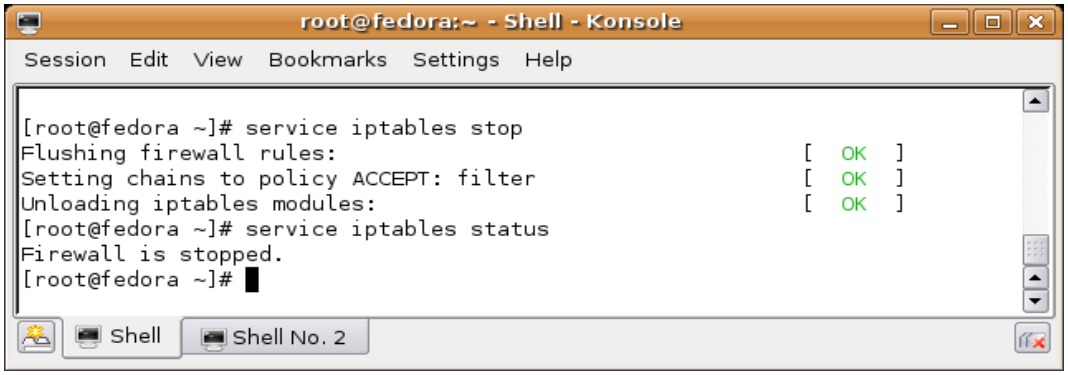
8. Selain menggunakan curl, tools lain yang dapat dilakukan untuk mendeteksi adanya permalahan pada jaringan atau server adalah “netstat -an “. Perintah ini akan menampilkan komunikasi atau layanan yang berjalan pada sebuah komputer/server.



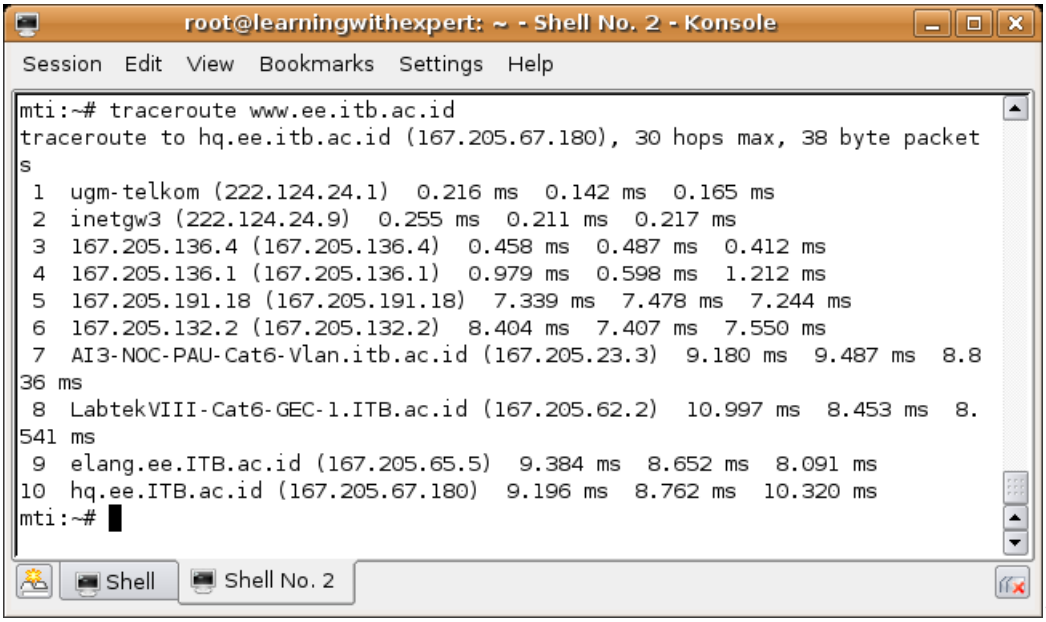
Misalnya untuk menampilkan jumlah koneksi yang sedang terjadi antara komputer kita dengan komputer/server lain dapat menggunakan command berikut :



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



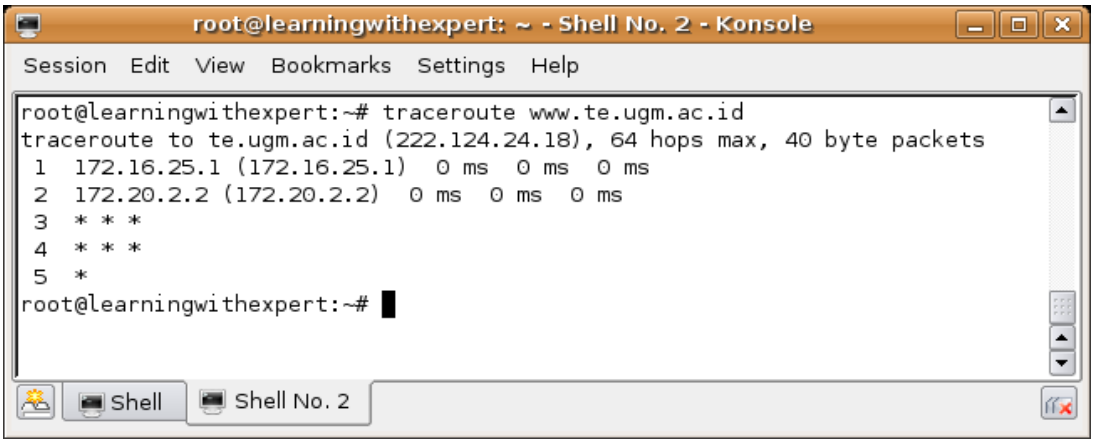
10. Tools “traceroute” fungsinya sama dengan tools “tracert” di Sistem Windows, digunakan untuk testing link koneksi terhadap server tertentu. Tracert maupun traceroute menggunakan protokol icmp.



Pesan pesan yang mungkin muncul pada hasil traceroute

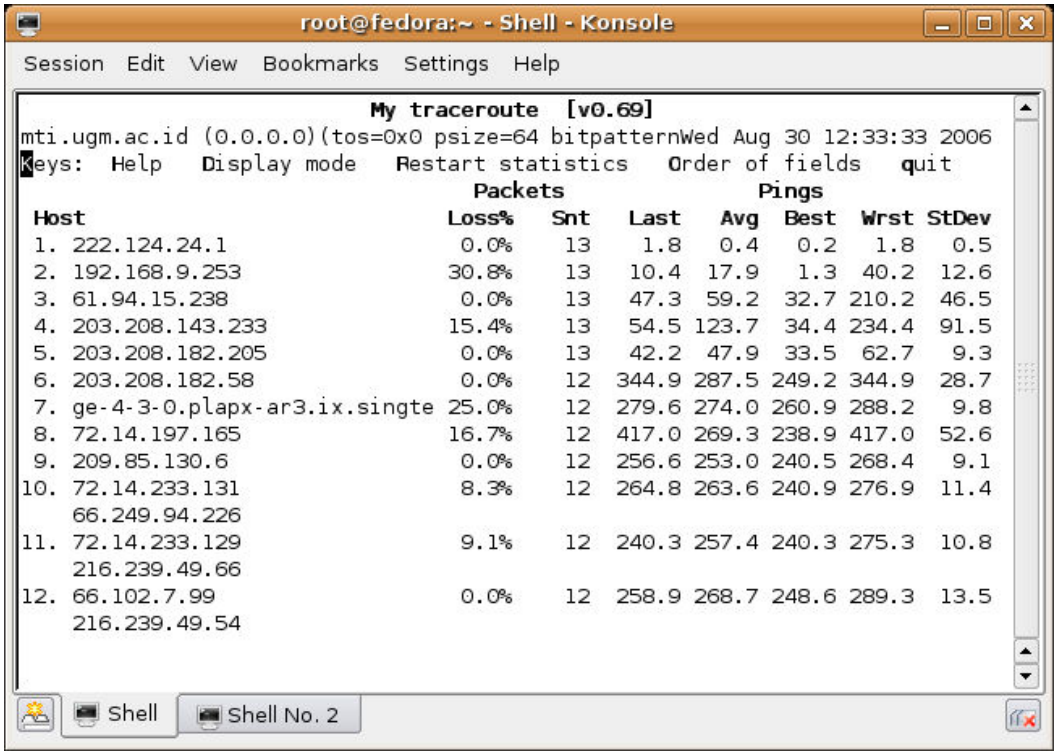
Hasil Traceroute	Penjelasan
* * *	Tanda bintang "* * *" artinya bahwa respons time untuk menuju router atau hop selanjutnya sudah habis, respons time untuk perintah traceoute adalah 5 detik. Hal ini dapat disebabkan oleh. > Router yang ingin dilalui tidak mengirimkan echo replay (di-disable) > Router 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 :

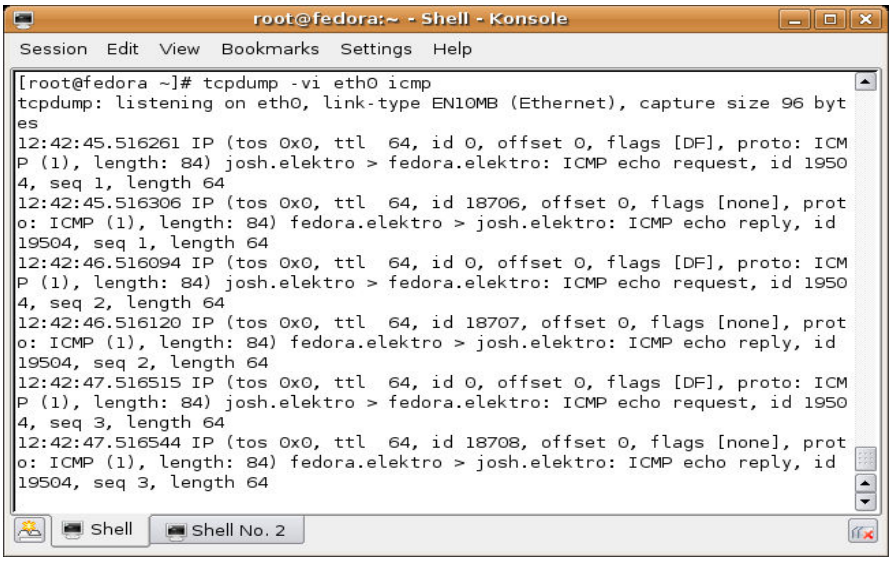


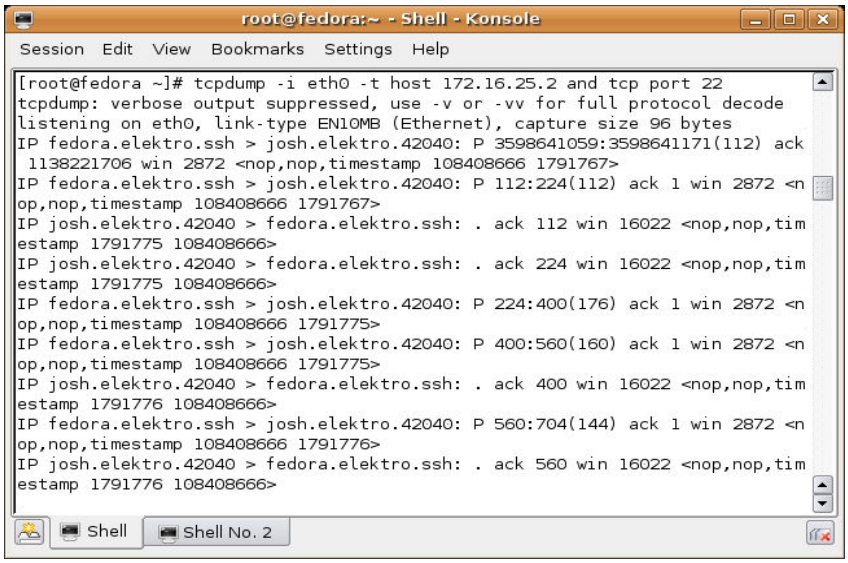
11. Selain traceroute, tools yang lebih powerfull adalah “mtr”. Dengan mtr dapat dilihat jalur dan packet loss yang terjadi selama diperjalanan.

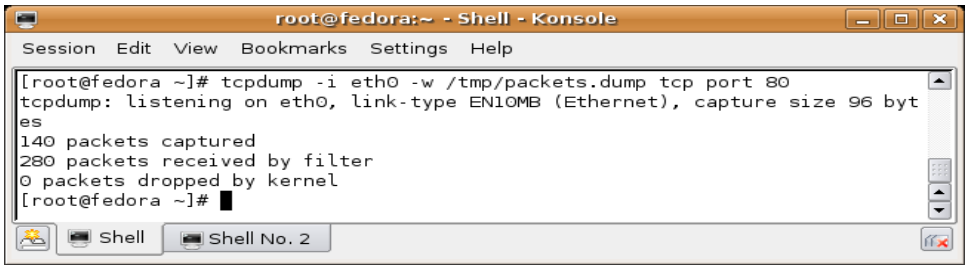
Perintah: mtr www.google.com , menghasilkan :



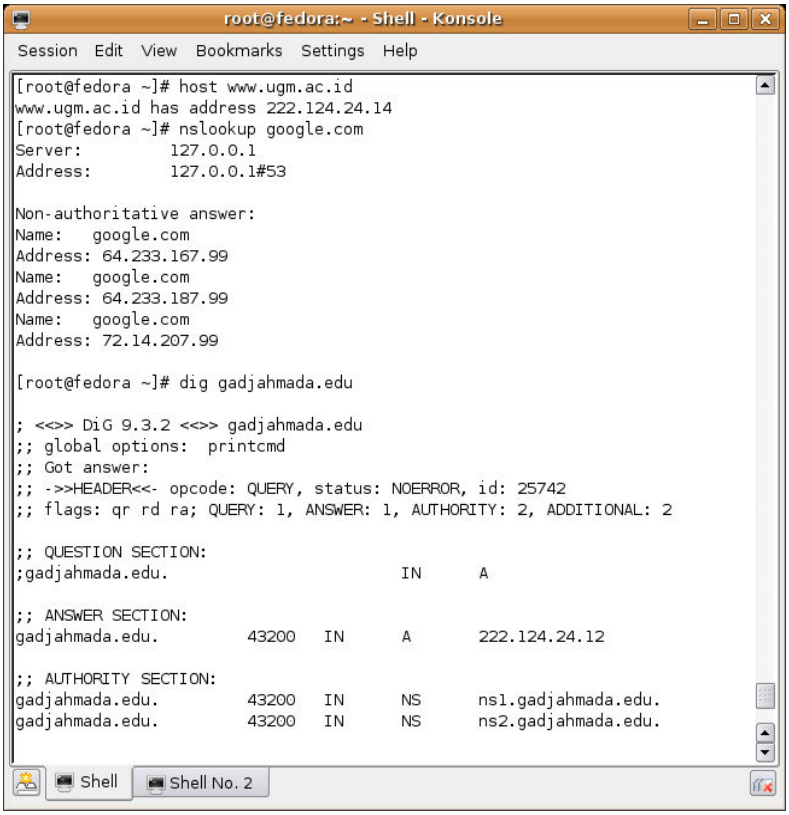
12. Tools sederhana untuk menganalisa jaringan pada sistem operasi Linux seperti tcpdump, juga dapat dilakukan untuk melihat traffic. Biasanya administrator menganalisa traffic untuk mencari tahu apa saja yang sedang terjadi pada jaringannya.







13. Testing DNS menggunakan tools nslookup, dig dan host



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.