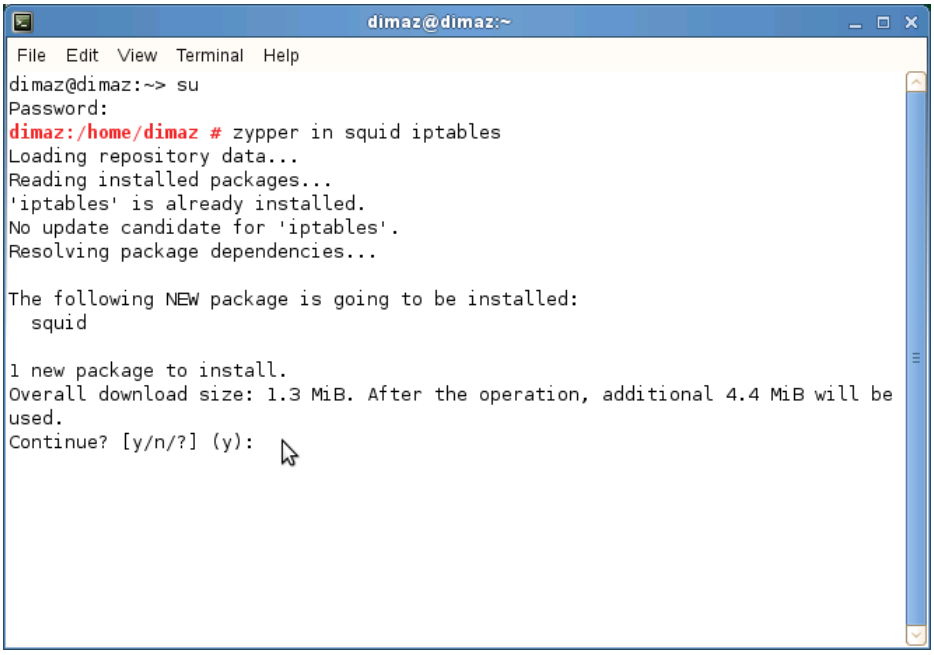
Konfigurasi dasar Squid Proxy+Gateway Server di SLES 11

Proxy server berfungsi tindak hanya sebagai server penyimpanan sementara dari request-request ke internet sehigga ketika kita mengakses web yang sama dari komputer lain akan terasa lebih cepet, tapi dapat berfungsi juga sebagai filterisasi/blocking situs atau url. ibarat orang, udah kaya satpam aja . :D

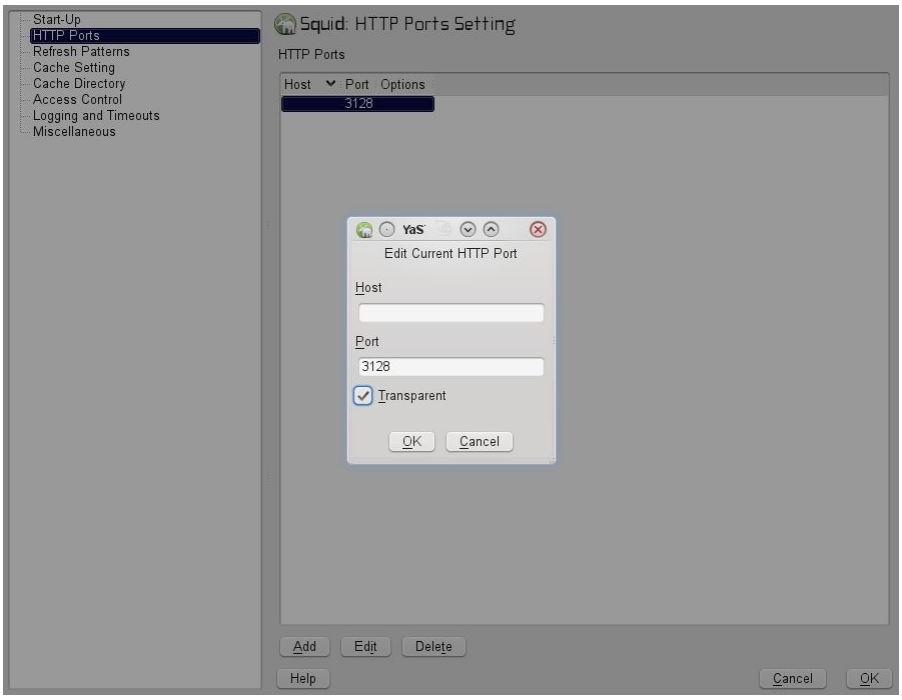
Aplikasi Proxy server yang cukup terkenal dan handal yaitu Squid Proxy, tutorial ini menjelaskan bagaimana konfigurasi squid di SLES 11 SP1. (dengan catatan, PC server memiliki 2 buah NIC untuk melakuka routing, sehingga PC server juga bekerja sebagai Gateway)



- Install squid proxy dan iptables pada **gnome-terminal** dengan menggunakan perintah
  # zypper in squid iptables

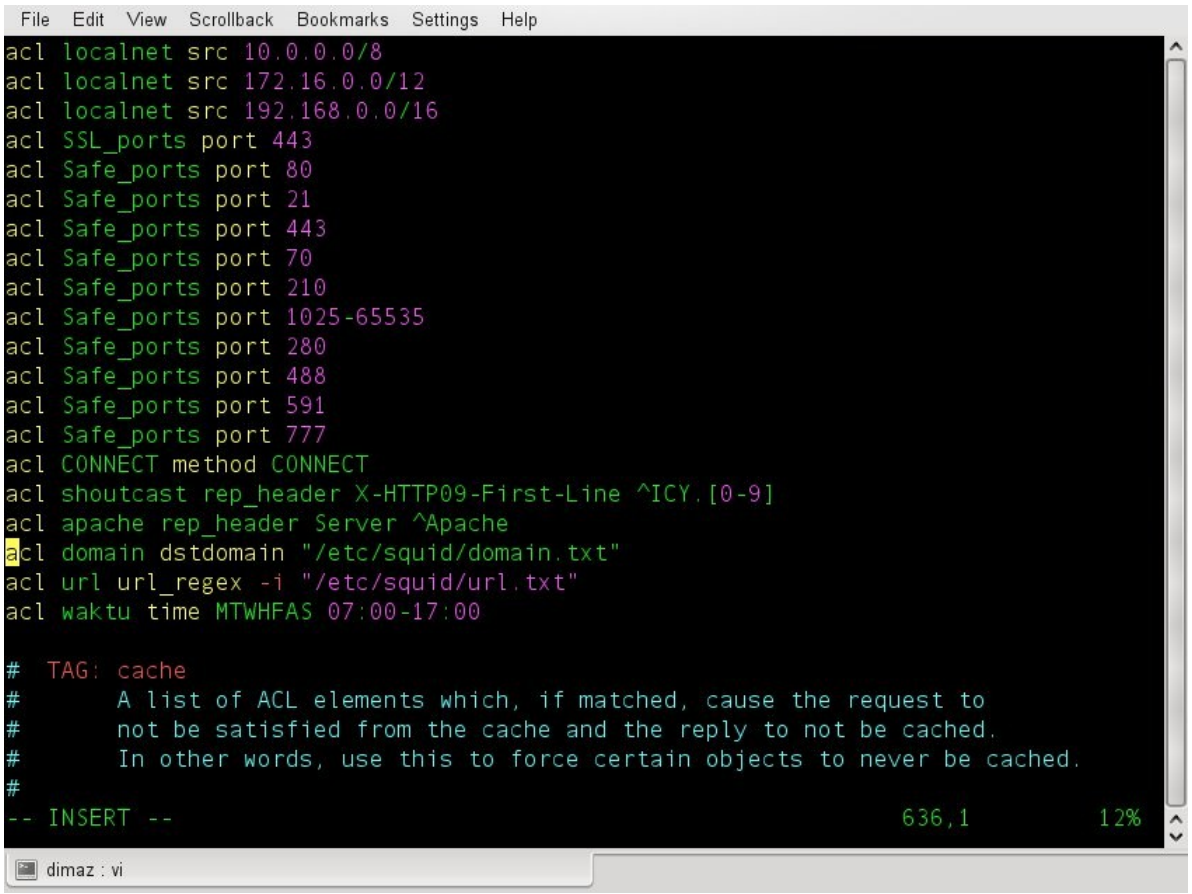
- kemudian jalankan **YaST – Squid** dari **gnome-terminal** dengan perintah
  # yast2 squid

Created by Dimas Yuwono
dimazyuwono@gmail.com
http://linux-avenger.blogspot.com

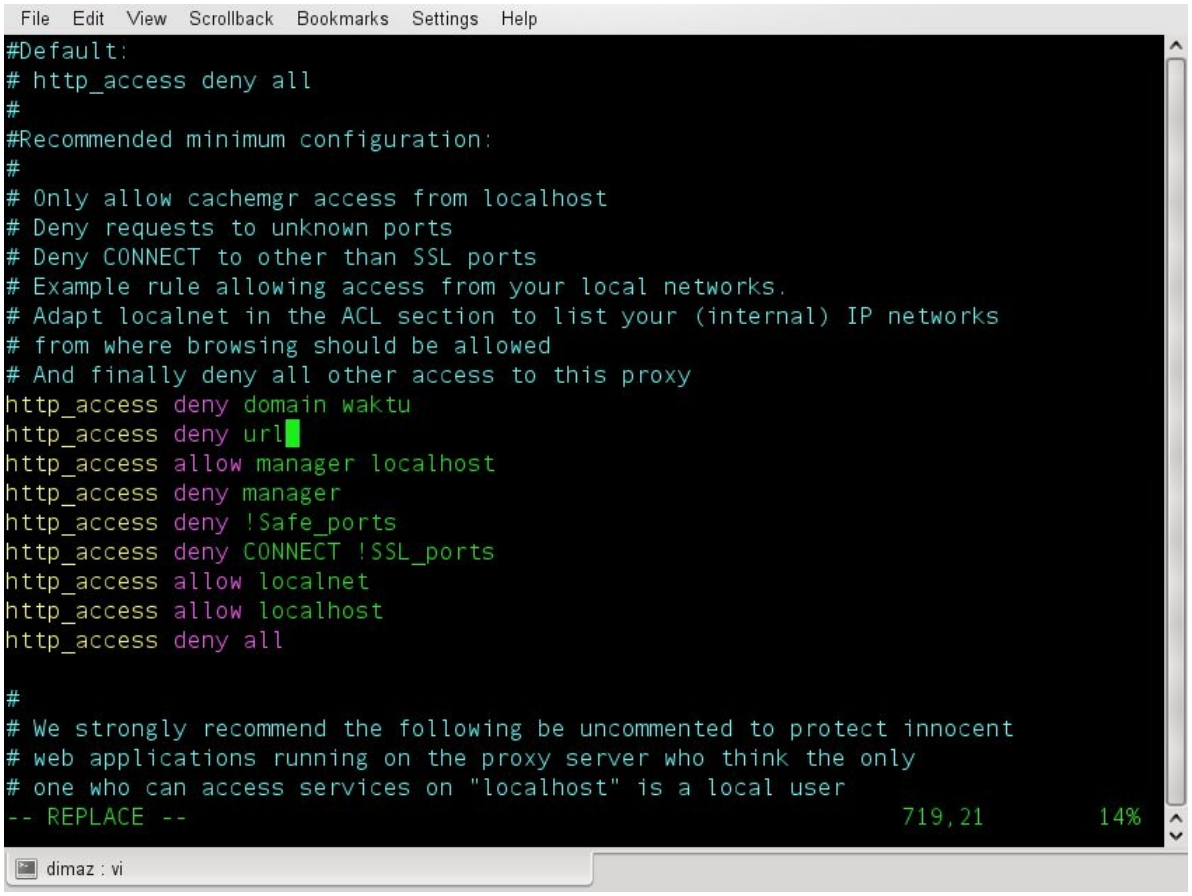


- klik **HTTP Ports** kemudian klik **edit**, lalu ceklist **Transparent**, lalu klik OK

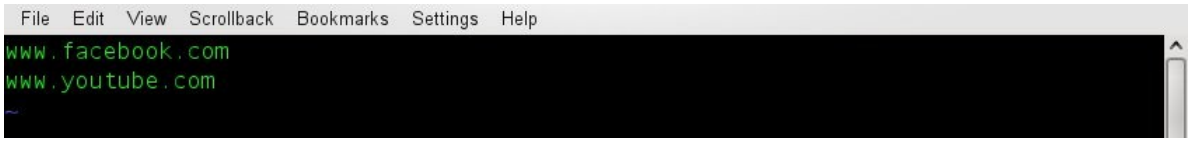
- kemudian edit file konfigurasi squid untuk menambahkan acl dengan perintah
  # vi /etc/squid/squid.conf



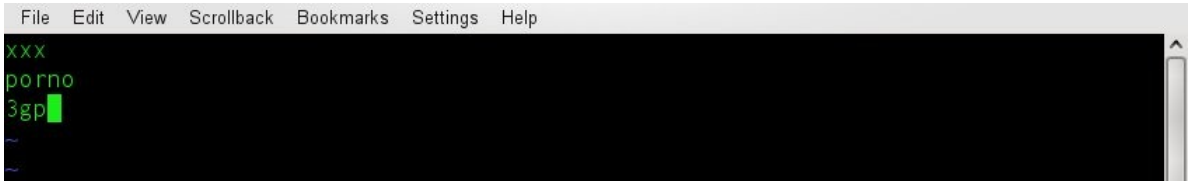
- kemudian tambahkan line ACL dibawah untuk menentukan peraturan berdasarkan domain, waktu, dan URL
  acl domain dstdomain "/etc/squid/domain.txt"
  (menentukan domain dari sebuah file)
  acl url url_regex -i "/etc/squid/url.txt"
  (menentukan URL dari sebuah file)
  acl waktu time MTWHFAS 07:00-17:00
  (menentukan hari dan jam, M = monday T = Tuesday W = Wednesday H = Thursday F = Friday A = Saturday S = Sunday)



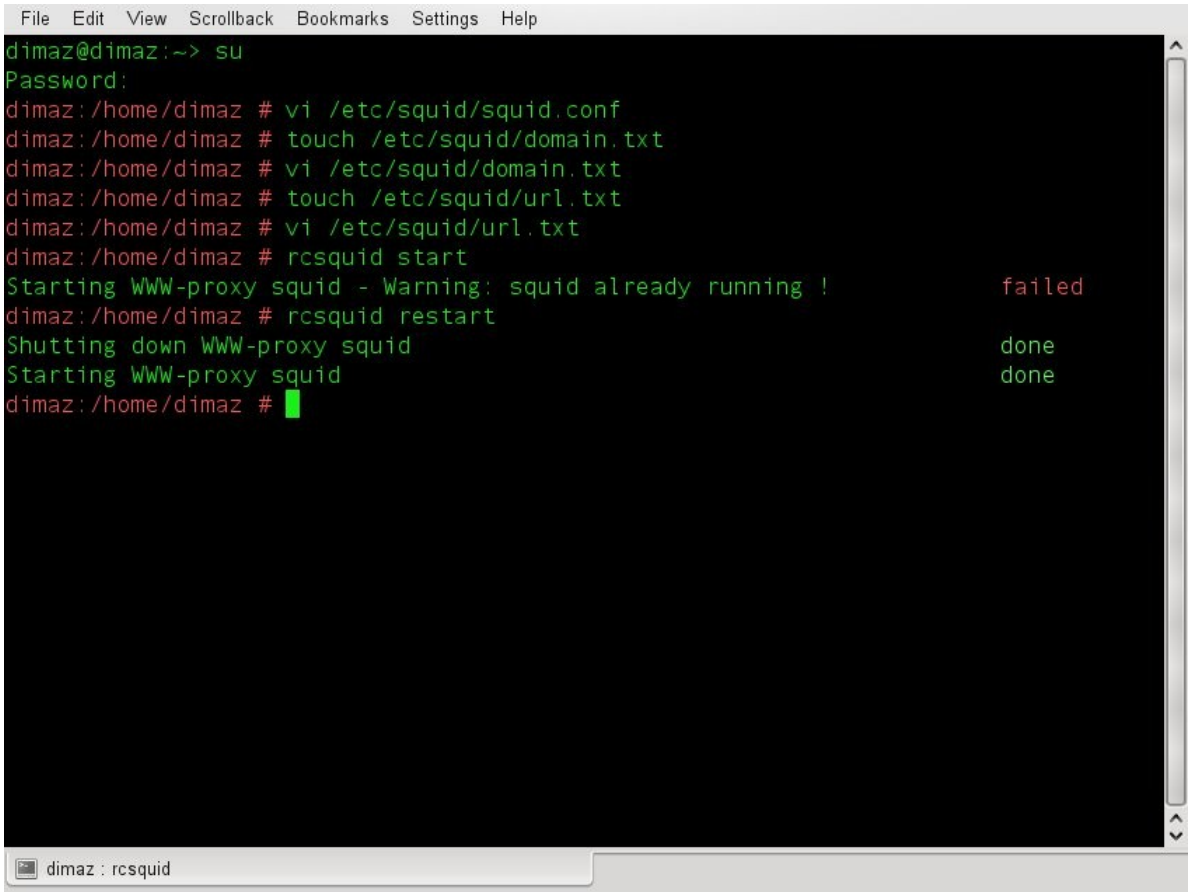
- lalu tambahkan juga line dibawah untuk menentukan ACL tersebut di blok atau di izinkan
  http_access deny domain waktu = memblok domain-domain yang sudah ditentukan pada waktu yang sudah ditentukan.
  http_access deny url = memblok kata-kata yang sudah ditentukan pada saat menggunakan s earch engine, contoh : google.com



- lalu save file konfigurasi squid.conf, kemudian buat file domain.txt didalam direktori /etc/squid/ dengan perintah **# touch /etc/squid/domain.txt** lalu edit file domain.txt **# vi /etc/squid/domain.txt** lalu tambahkan nama-nama domain yang akan di blok, contoh : www.facebok.com, www.youtube.com lalu save file tersebut
-



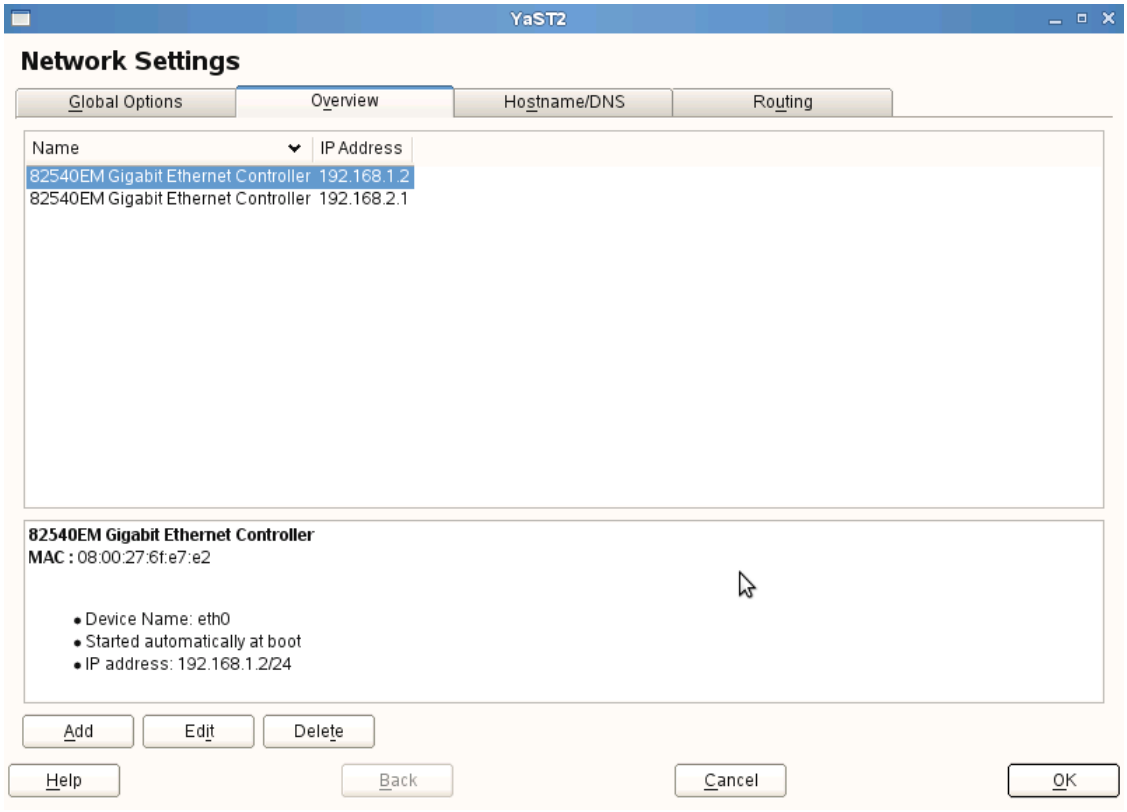
- kemudian buat file /etc/squid/url.txt dengan perintah **# touch /etc/squid/url.txt** lalu edit file tersebut lalu tambahkan kata-kata/url yang ingin diblok seperti gambar dibawah lalu save file tersebut.



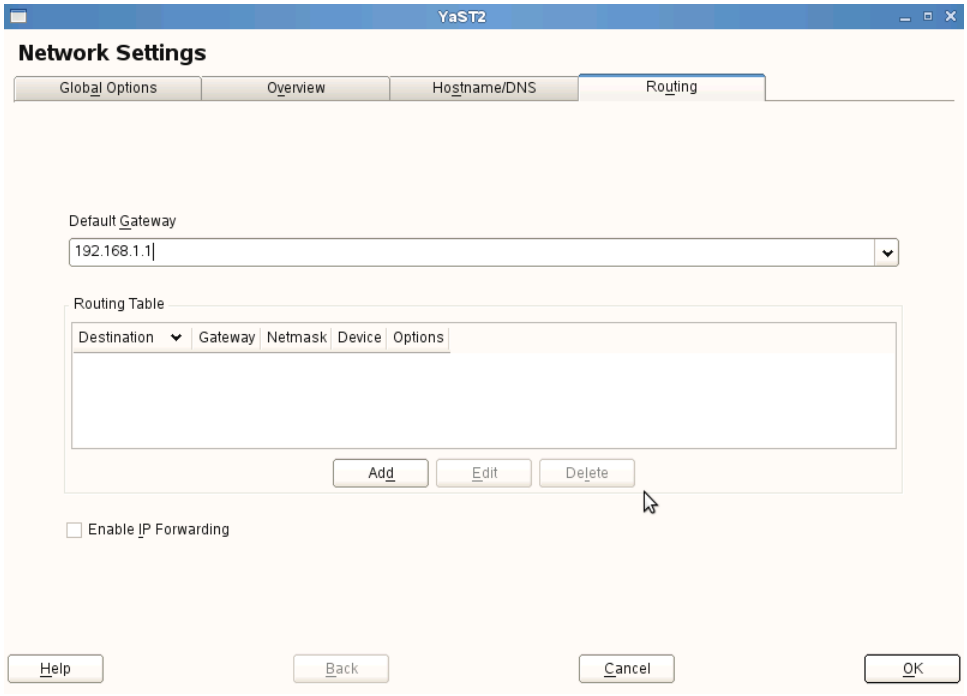
- Setelah konfigurasi squid sudah selesai, jalankan service squid proxy dengan perintah **# rcsquid start** dan jalankan perintah **# insserv squid** sehingga service squid berjalan otomatis pada saat booting server

setelah konfigurasi squid selesai, kita harus melakukan beberapa routing di server tersebut karena memiliki 2 buah NIC, routing ini di maksudkan untuk otomatis meredirect port 80 ke port 3128 (proxy transparet) sehingga tidak perlu konfigurasi manual pada web browser pc klien. NIC yang pertama akan terhubung dengan modem, kemudian NIC yang kedua akan menjadi gateway untuk setiap klien PC.

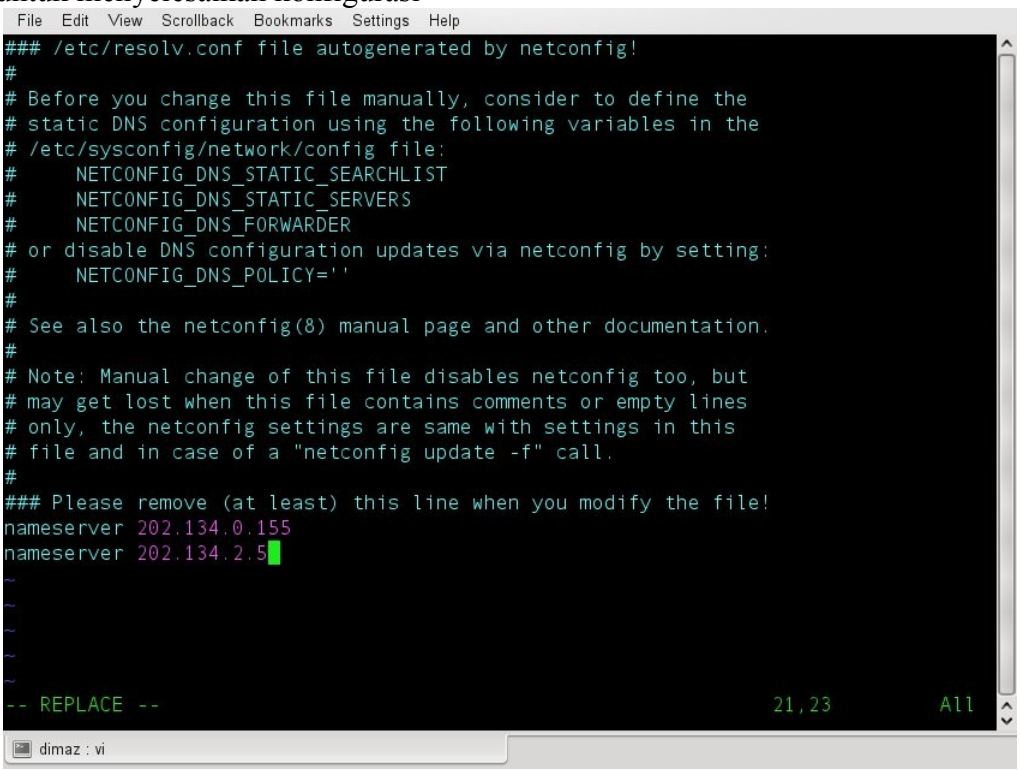
MODEM ===== NIC1 Server NIC 2 ==== Switch ===PC Client



- Lakukan konfigurasi NIC, dengan menjalankan perintah **# yast2 lan** lalu setting ip address eth0 dan eth1 seperti contoh gambar di atas



- lalu setting dengan ip gateway yaitu ip modem, contoh 192.168.1.1 adalah ip modem lalu klik OK untuk menyelesaikan konfigurasi



- setelah itu konfgurasi ip dns dengan mengedit file /etc/resolv.conf lalu isikan ip dns speedy, contoh 202.134.0.155, 202.134.2.5 lalu save file tersebut

setelah konfigurasi squid, ip address dan dns sudah dilakukan, langkah terakhir yaitu melakukan routing sehingga paket-paket dari pc client akan melewati squid proxy.

- Ketikkan perintah dibawah (pada saat menentukan eth0 dan eth1 pada perintah dibawah tidak terbalik ! Konfigurasi ini eth0 menghadap ke modem dan eth1 menghadap ke client)

  # iptables --append FORWARD -i eth1 -j ACCEPT
  # iptables -A PREROUTING -t nat -j REDIRECT -p tcp -i eth1 --dport 80 --to-ports 3128
  # iptables -t nat --append POSTROUTING -o eth0 -j MASQUERADE
  # iptables-save
  # echo 1 > /proc/sys/net/ipv4/ip_forward

kemudian edit file **/etc/init.d/boot.local** lalu ketikkan ulang sintaks-sintaks diatas, sehingga pada saat server boot, otomatis sintaks diatas akan dijalankan juga.