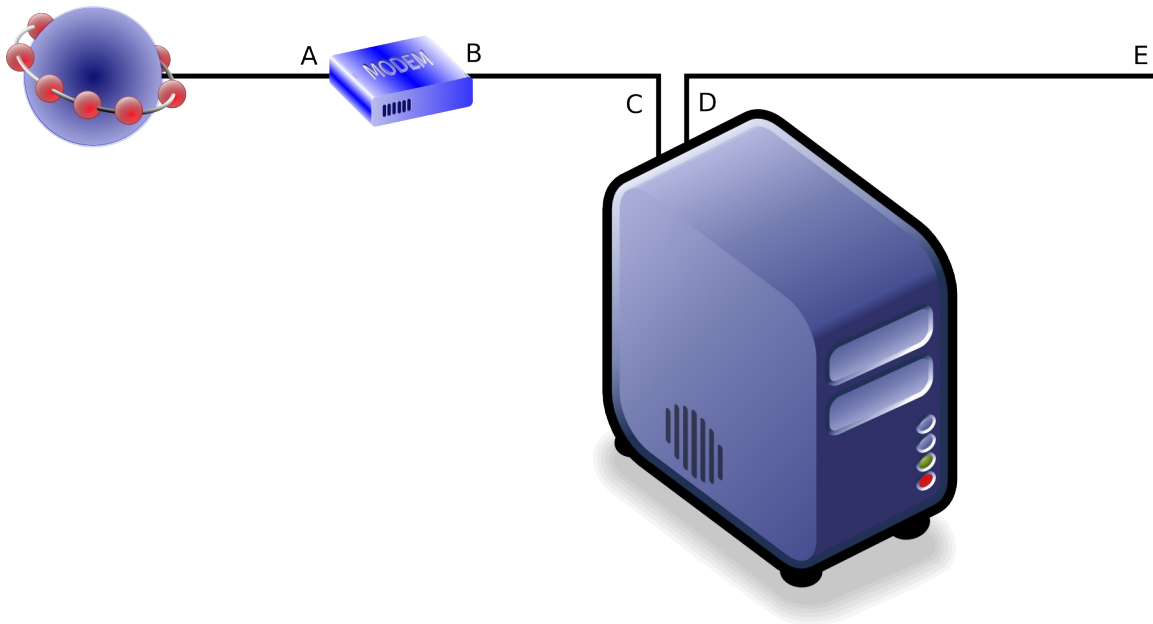


Tahapan instalasi Ubuntu untuk Router dan Proxy

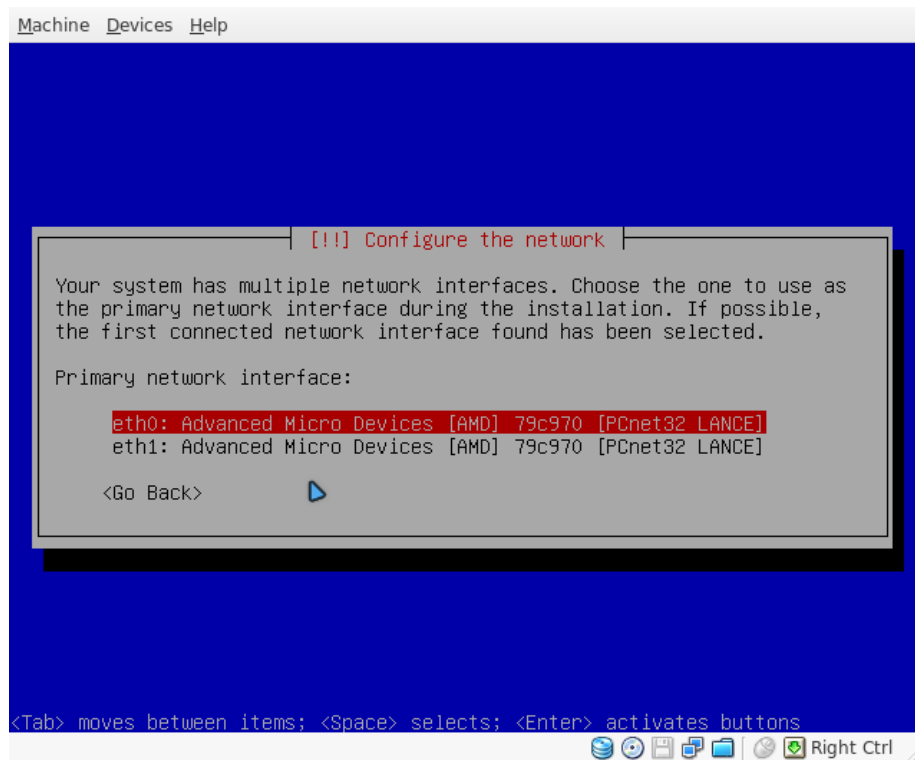
1. Persiapkan PC yang akan digunakan untuk Router dan Proxy
Berikut contoh spesifikasi hardware yang saya gunakan :
Processor AMD64 4600+
DDR2 2 GB 1 keping
HD 80 GB
Chipset Mobo nVidia nForce
Kartu jaringan yang onboard saya disable karena di Ubuntu Hardy tidak bisa bekerja
Kartu jaringan RTL-8139/8139C/8139C sebanyak 2 buah
2. Buat skema koneksi



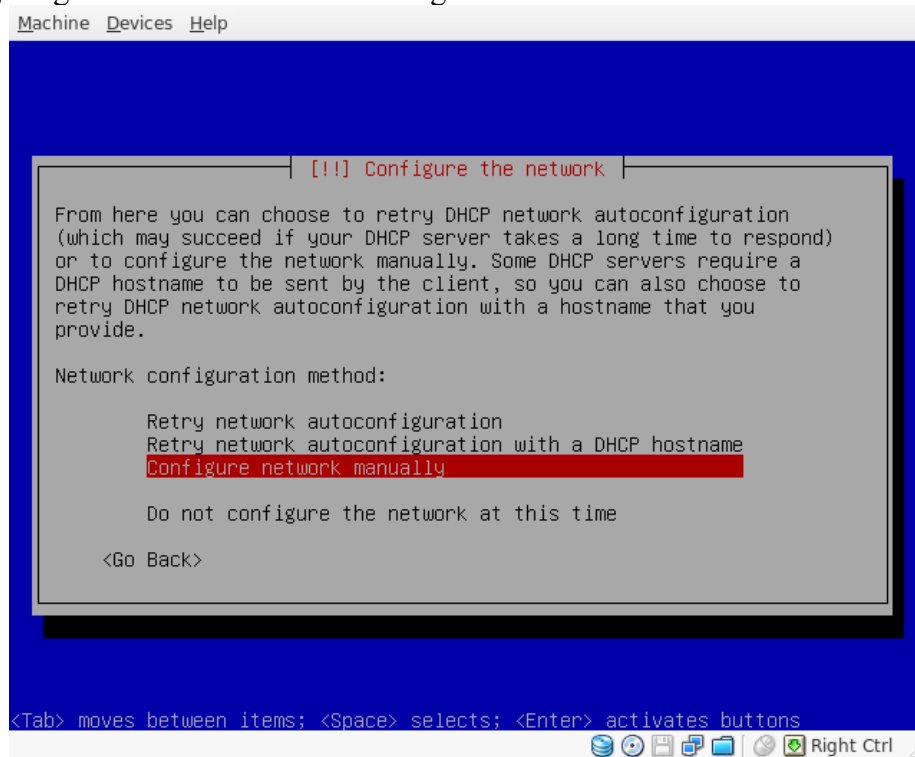
Keterangan :

- A : IP Public dari Speedy : 125.165.49.241
- B : IP Lokal Modem ADSL : 192.168.1.1
- C : eth0 dengan IP 192.168.1.4 (saya buat begitu karena 2 IP sebelumnya saya pakai)
- D : eth1 dengan IP 192.168.0.1
- E : diteruskan ke jaringan lokal, bisa melalui switch atau access point

3. Instalasi
Lakukan instalasi Ubuntu 8.04 Server. Langkah-langkahnya tinggal menyesuaikan saja.
 - a. Pada point Configure Network, silahkan ditentukan primary network interface-nya.

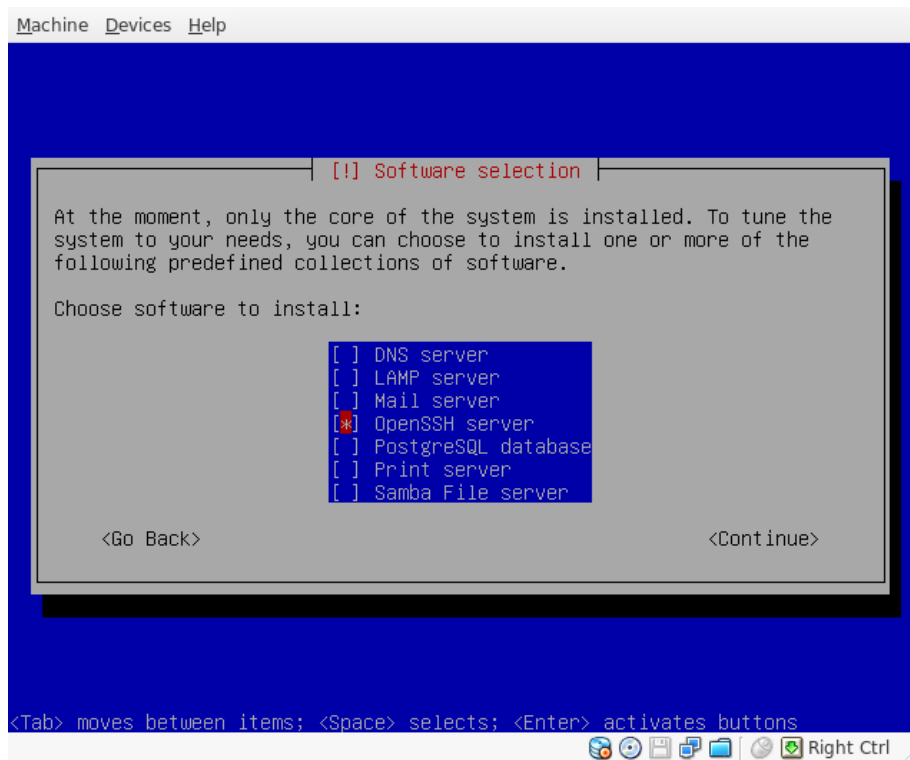


b. Setting jaringan secara manual sesuai dengan skema di atas



c. Lanjutkan prosesnya sesuai dialog yang muncul

d. Pada dialog Software Selection, beri centang OpenSSH Server yang berfungsi untuk meremote server tersebut



4. Konfigurasi Jaringan

Setelah instalasi selesai, sekarang kita perlu login dan mengkonfigurasi jaringannya.

```
$ sudo nano /etc/network/interfaces
```

Edit ulang seperti di bawah ini (silahkan sesuaikan dengan jaringan anda) :

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
    address 192.168.1.4
    netmask 255.255.255.0
    gateway 192.168.1.1

auto eth1
iface eth1 inet static
    address 192.168.0.1
    netmask 255.255.255.240
```

Rubah dns-nameservernya

```
$ sudo nano /etc/resolv.conf
```

Edit seperti di bawah ini (bisa juga ditambahi sesuai kebutuhan) :

```
nameserver 192.168.1.1
```

Restart networknya dan dicoba ping ke IP 192.168.1.1 serta IP klien (misal 192.168.0.3)

```
$ sudo /etc/init.d/networking restart
$ ping 192.168.1.1
$ ping 192.168.0.3
```

5. Internet Connection Sharing (NAT) Mengaktifkan fungsi router di server

```
$ sudo nano /etc/sysctl.conf
```

Rubah pada bagian (hilangkan tanda “#”)

```
#net.ipv4.ip_forward=1
```

Menjadi

```
net.ipv4.ip_forward=1
```

6. Menjalankan IPTables agar request dari LAN bisa diteruskan ke Internet

```
$ sudo iptables -t nat -A POSTROUTING -s 192.168.0.0/28 -d 0/0 -j MASQUERADE
```

Perintah di atas artinya sebagai berikut :

Memberikan ijin kepada jaringan lokal dengan range IP tersebut ke Internet.

Sekarang, coba di komputer klien yang tersambung ke server membuka/mengakses internet, misal google.com. Kalau sudah bisa/berhasil tinggal masukan perintah tersebut di atas ke /etc/rc.local agar setiap server start, perintah tersebut otomatis dijalankan.

```
$ sudo nano /etc/rc.local
```

Edit seperti dibawah ini :

```
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.

iptables -t nat -A POSTROUTING -s 192.168.0.0/28 -d 0/0 -j MASQUERADE

exit 0
```

7. Menginstal Squid sebagai proxy

```
$ sudo apt-get install squid
```

Edit file /etc/squid/squid.conf

```
$ sudo nano /etc/squid/squid.conf
```

Untuk lebih mudahnya, hapus semua isinya dan ganti seperti dibawah ini :

```
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl lan src 192.168.0.0/255.255.255.240
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443 # https
acl SSL_ports port 563 # snews
acl SSL_ports port 873 # rsync
acl Safe_ports port 80 # http
acl Safe_ports port 21 # ftp
```

```

acl Safe_ports port 443 # https
acl Safe_ports port 70 # gopher
acl Safe_ports port 210 # wais
acl Safe_ports port 1025-65535 # unregistered ports
acl Safe_ports port 280 # http-mgmt
acl Safe_ports port 488 # gss-http
acl Safe_ports port 591 # filemaker
acl Safe_ports port 777 # multiling http
acl Safe_ports port 631 # cups
acl Safe_ports port 873 # rsync
acl Safe_ports port 901 # SWAT
acl purge method PURGE
acl CONNECT method CONNECT

acl porno url_regex -i "/etc/squid/porno.txt"
no_cache deny porno
http_access deny porno all

acl situslarangan dstdomain "/etc/squid/situs.txt"
no_cache deny situslarangan
http_access deny situslarangan all

http_access allow lan
http_access allow manager localhost
http_access deny manager
http_access allow purge localhost
http_access deny purge
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost
http_access deny all
icp_access allow all
http_port 3128 transparent

hierarchy_stoplist cgi-bin ?
cache_mem 672 MB
cache_dir ufs /cache 30000 16 256
access_log /var/log/squid/access.log squid
acl QUERY urlpath_regex cgi-bin \?
refresh_pattern ^ftp:          1440      20%      10080
refresh_pattern ^gopher:      1440      0%       1440
refresh_pattern .              0        20%     4320
cache_effective_user proxy
cache_effective_group proxy
visible_hostname proxy.opotumon
hosts_file /etc/hosts

```

Perhatian beberapa bagian ini :

```
acl lan src 192.168.0.0/255.255.255.240
```

Sesuaikan dengan jaringan anda

```

acl porno url_regex -i "/etc/squid/porno.txt"
no_cache deny porno
http_access deny porno all

```

Digunakan untuk memblokir kata-kata/keyword yang tidak layak. Seperti kata-kata kotor ataupun umpatan. File /etc/squid/porno.txt tersebut dibuat terlebih dahulu. Dan isikan kata-kata yang bakalan di-blok.

```

acl situslarangan dstdomain "/etc/squid/situs.txt"
no_cache deny situslarangan
http_access deny situslarangan all

```

Digunakan untuk memblokir url/situs yang tidak layak untuk diakses sebagian orang. Daftar situs

tersebut diisikan di file `/etc/squid/situs.txt`.

```
http_port 3128 transparent
```

Digunakan agar proxy-nya transparent. Maksudnya, seluruh browser klien secara otomatis akan diarahkan ke proxy server dengan port 3128 untuk koneksi internetnya tanpa perlu disetting manual terlebih dahulu.

```
cache_mem 672 MB
```

Digunakan untuk mendefinisikan memori yang bakal dialokasikan untuk squid. Optimalnya memakai 1/3 memori sistem kita.

```
cache_dir ufs /cache 30000 16 256
```

Digunakan untuk mengarahkan cache proxy ke direktory `/cache`. Directory `/cache` perlu dibuat terlebih dahulu. Dan diberikan akses baca tulis. Berikut perintahnya :

```
$ sudo mkdir /cache  
$ sudo chmod 777 /cache
```

Nilai 30000 = 30 GB adalah alokasi untuk cache proxy kita. 16 maksudnya adalah jumlah sub directory yang ada di `/cache` dan 256 adalah jumlah sub directory yang ada dibawah directory yang berjumlah 16 tadi.

```
access_log /var/log/squid/access.log squid
```

File `/var/log/squid/access.log` digunakan untuk menyimpan log koneksi seluruh jaringan yang terhubung dengan proxy.

```
visible_hostname proxy.opotumon
```

Adalah nama yang muncul untuk proxy kita.

Setelah hal-hal diatas selesai dilakukan, sekarang kita pasang script IPTables yang fungsinya untuk membelokkan request dari port 80 ke port 3128. Pasang script tersebut di `/etc/rc.local` dan edit seperti di bawah ini :

```
#!/bin/sh -e  
#  
# rc.local  
#  
# This script is executed at the end of each multiuser runlevel.  
# Make sure that the script will "exit 0" on success or any other  
# value on error.  
#  
# In order to enable or disable this script just change the execution  
# bits.  
#  
# By default this script does nothing.  
  
iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j DNAT --to 192.168.0.1:3128  
iptables -t nat -A POSTROUTING -s 192.168.0.0/28 -d 0/0 -j MASQUERADE  
  
exit 0
```

Reeboot ulang mesin anda, dan dicoba browsing dari komputer klien.

8. Manajemen Bandwith

Disini kita akan menggunakan aplikasi htb-gen yang bisa diunduh dengan perintah :

```
$ wget -c http://www.praga.org.ar/dev/htb-gen/packages/htb-gen_0.8.4_all.deb
```

Setelah itu install paket htb-gen tersebut.

```
$ sudo dpkg -i htb-gen_0.8.4_all.deb
```

Edit baris-baris berikut di file /etc/htb-gen/htb-gen.conf sesuai kebutuhan anda

```
iface_down="eth1" # Server LAN iface
iface_up="eth0" # Server INET iface

total_rate_down=384
total_rate_up=64
```

Perhatikan juga baris-baris berikut di file /etc/htb-gen/htb-gen-rates.conf

```
# rate is in 0 so it means that it will be automagically calculated
# down down up up
# min max min max
#ip (rate) (ceil) (rate) (ceil)
192.168.0.3 0 45 0 7
192.168.0.4 0 45 0 7
192.168.0.5 0 45 0 7
192.168.0.6 0 45 0 7
192.168.0.7 0 45 0 7
192.168.0.8 0 45 0 7
192.168.0.9 0 45 0 7
192.168.0.10 0 45 0 7
192.168.0.13 0 34 0 8
```

Jalankan htb-gennya dengan perintah :

```
$ sudo htb-gen tc_all
```

Letakkan perintah tersebut di /etc/rc.local agar bisa dijalankan otomatis waktu server kita start

```
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.

iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j DNAT --to 192.168.0.1:3128
iptables -t nat -A POSTROUTING -s 192.168.0.0/28 -d 0/0 -j MASQUERADE

htb-gen tc_all

exit 0
```