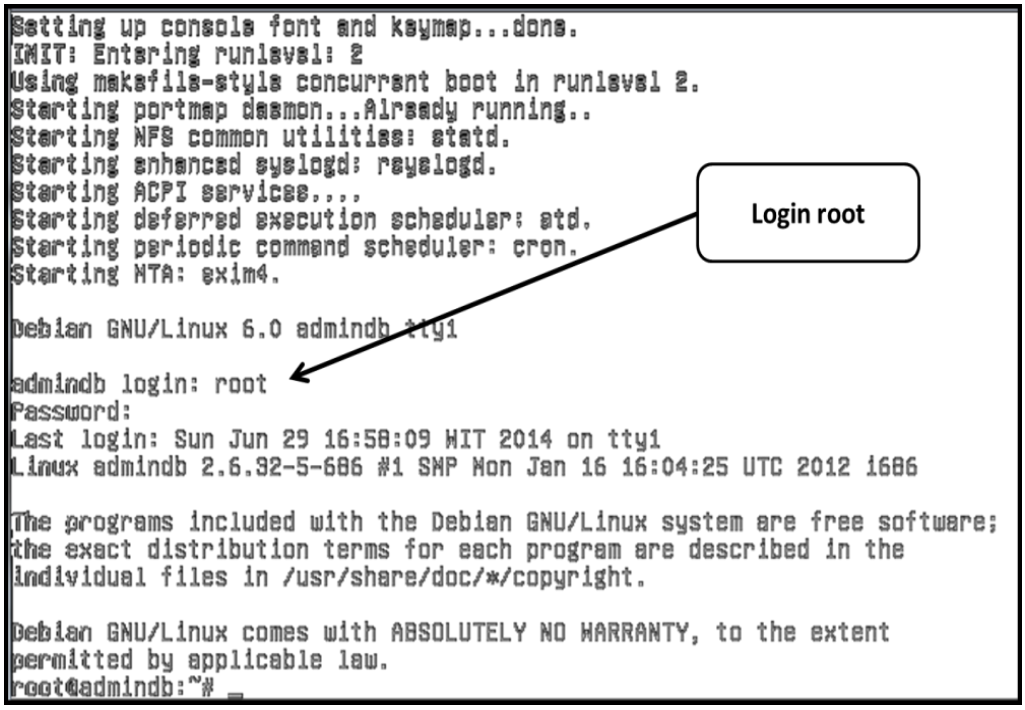
BAB V
IMPLEMENTASI DAN PEMBAHASAN

5.1 Konfigurasi Debian Router

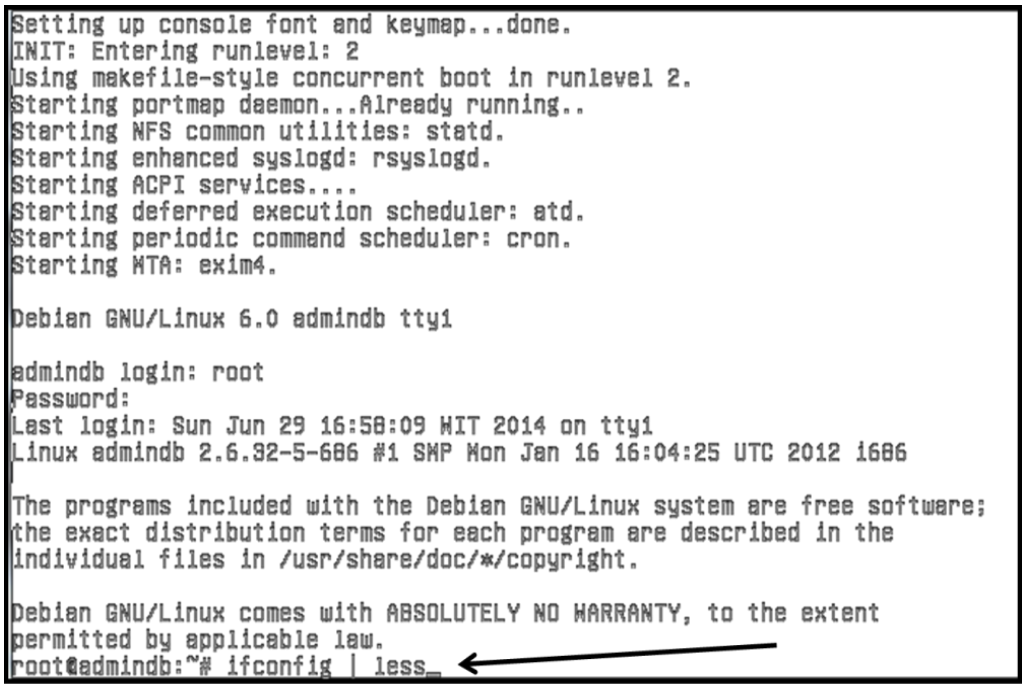
Debian digunakan sebagai Router. NAT (Network Address Translation) digunakan untuk menghubungkan antara jaringan local (LAN) dengan jaringan luar (WAN). Pada Konfigurasi Router Debian ini penulis menggunakan metode NAT dan juga menggunakan metode IP Forwarding. Berikut langkah-langkah konfigurasi debian router :

Gunakan login **root** untuk memulai konfigurasi.



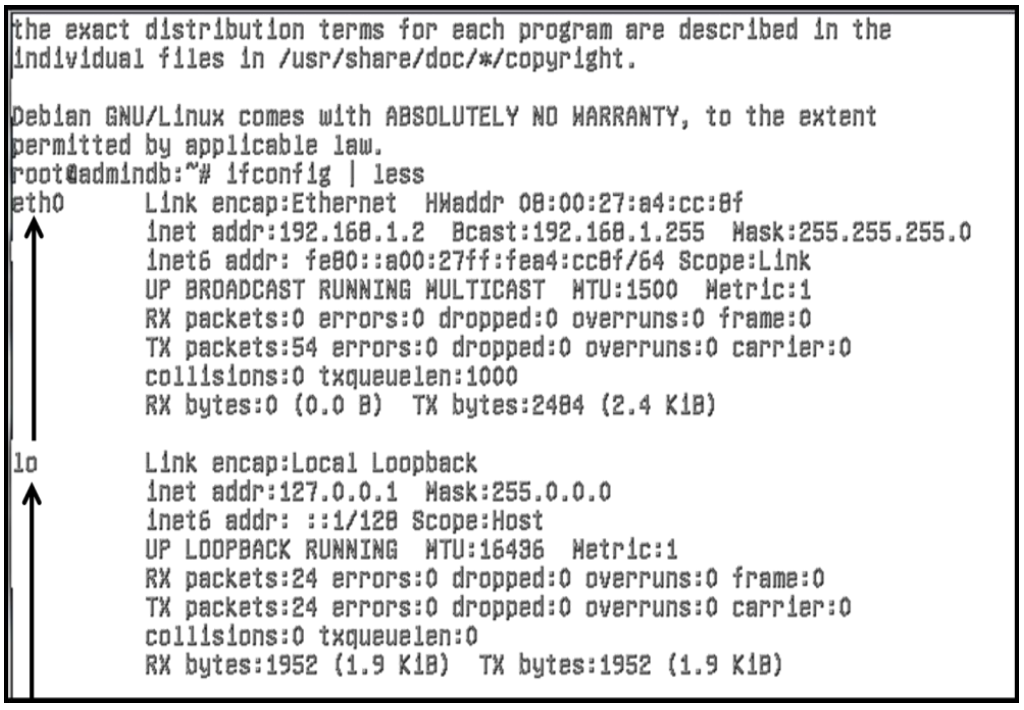
Gambar 5.1 *Login Root*

Memeriksa konfigurasi ethernet, gunakan perintah : **ifconfig | less**



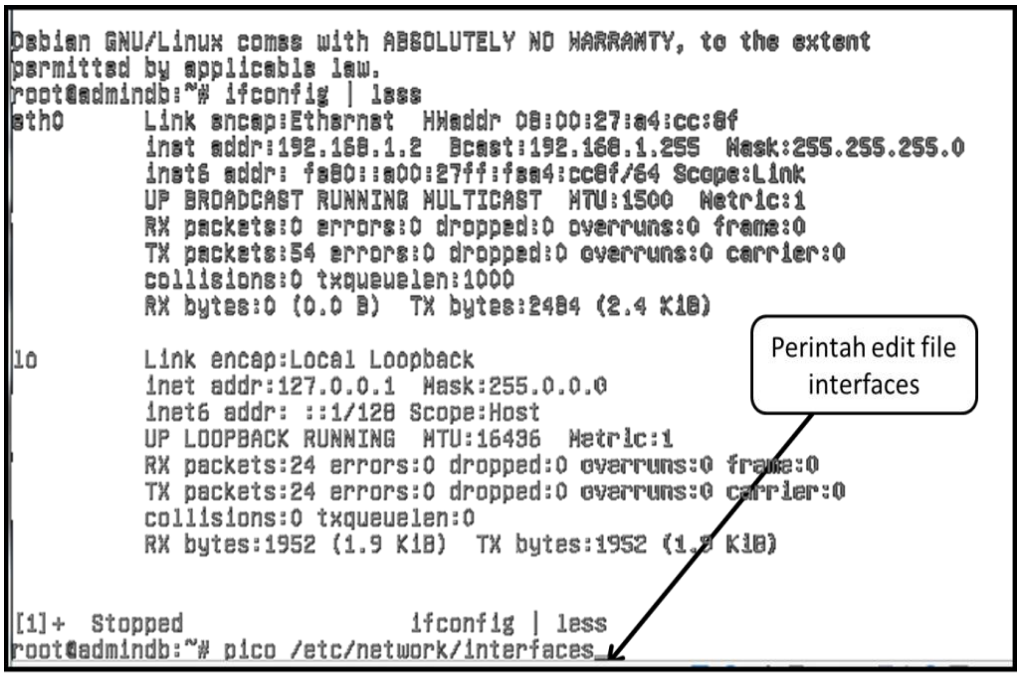
Gambar 5.2 *Memeriksa Konfigurasi Ethernet*

Tampilan file network Interfaces, hanya ada **IP eth0** dan **IP local** saja.

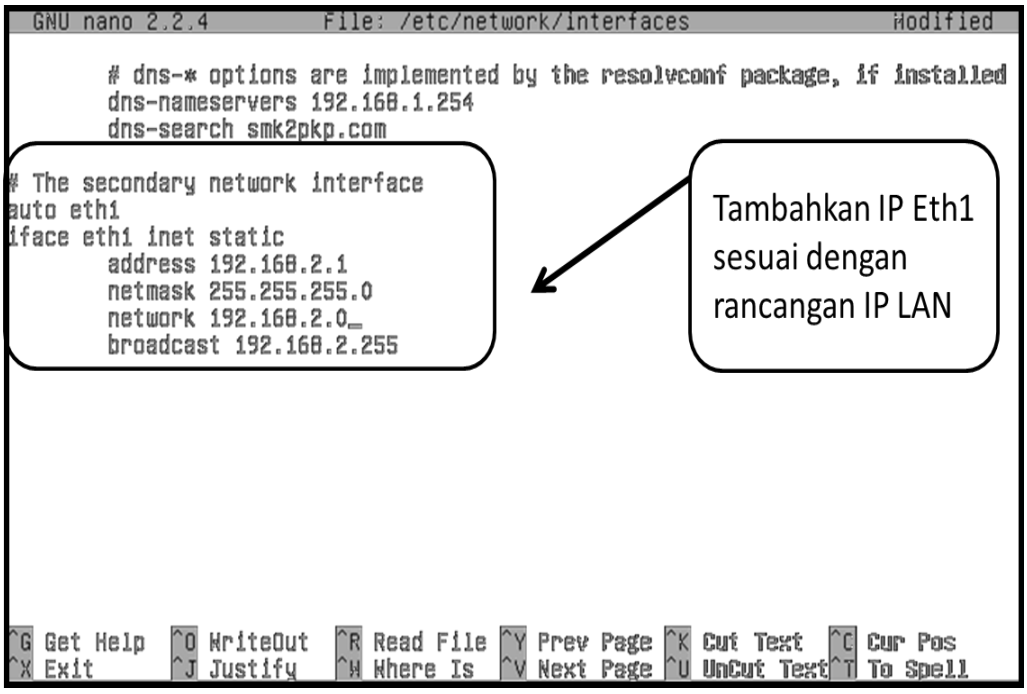


Gambar 5.3 *File Network Interfaces*

Mengaktifkan **IP Eth1 = IP LAN** , dengan cara mengedit file interfaces. Gunakan perintah : **pico /etc/network/interfaces**

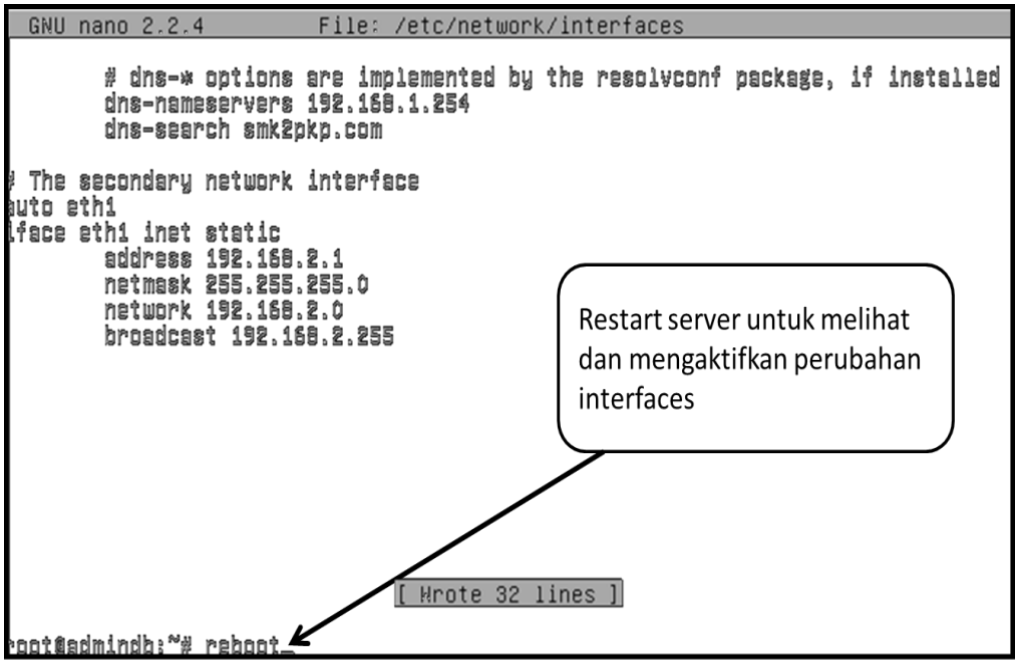


Gambar 5.4 *Mengedit File Interfaces*



Gambar 5.5 *Mengaktifkan IP Eth1*

Simpan konfigurasi interfaces dan restart server.

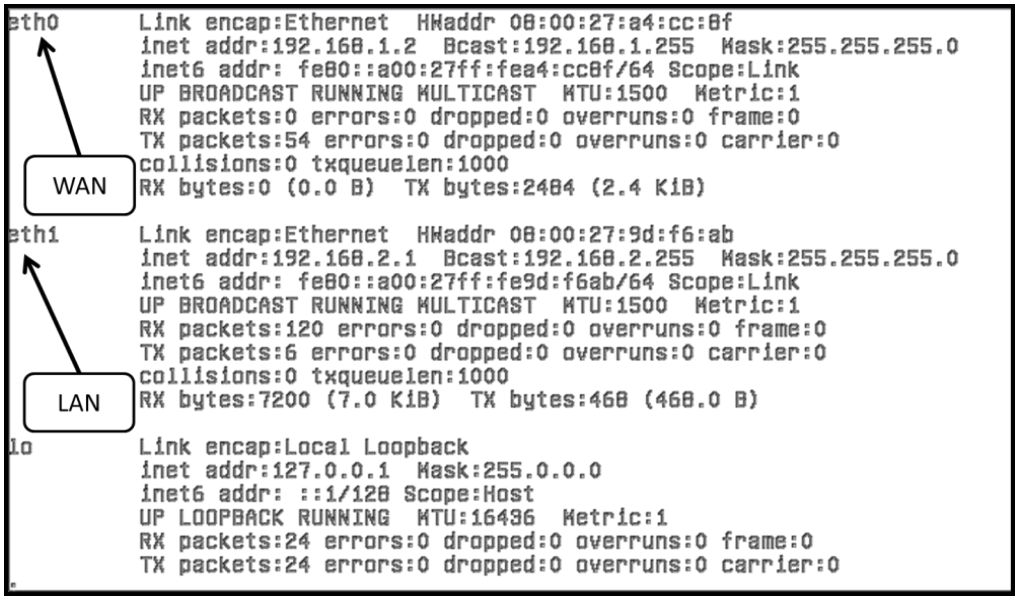


Gambar 5.6 *Merestart Server*

Setelah login, cek interface yang sudah diaktifkan.

```
root@admindb:~# ifconfig | less_
```

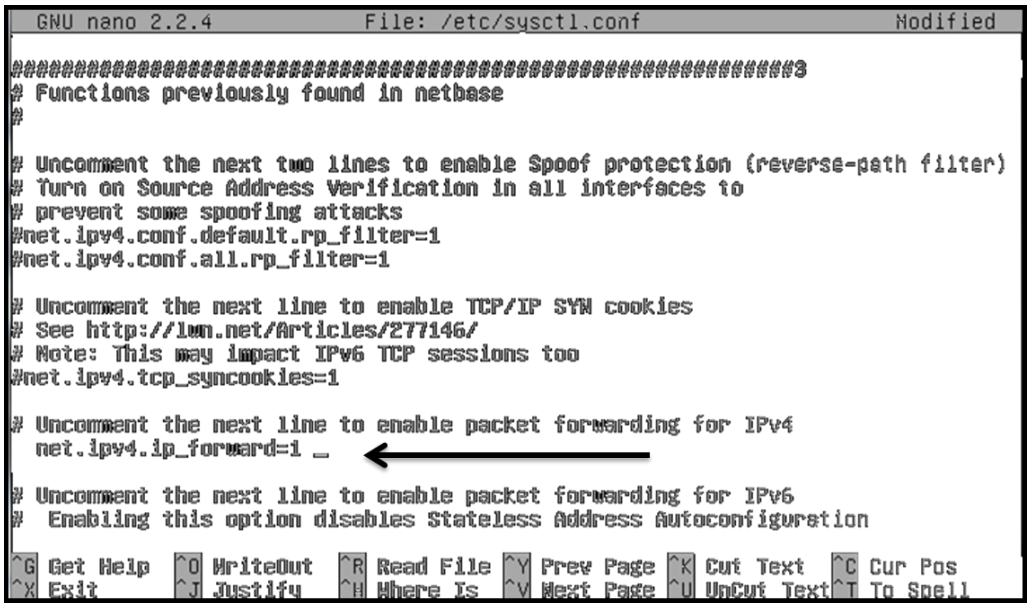
Konfigurasi sudah berhasil, maka akan terdapat eth1 (Ethernet LAN yang sudah ditambahkan sebelumnya).



Gambar 5.7 *IP Ethernet yang telah Aktif*

Mengaktifkan **IP forward**, gunakan perintah : **pico /etc/sysctl.conf**

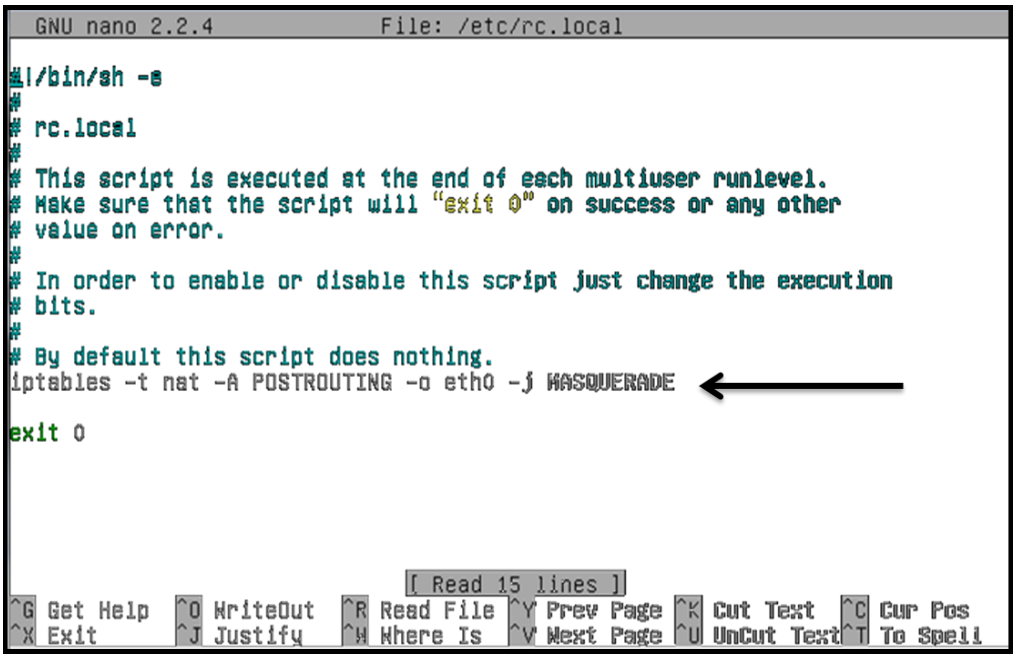
Hapus tanda **"#"** untuk mengaktifkan ip forwarding.



Gambar 5.8 *Mengaktifkan IP Forward*

Mengaktifkan NAT Routing Iptables , gunakan perintah : **pico /etc/rc.local**

Mambahkan nat routing iptables, kemudian simpan konfigurasi.

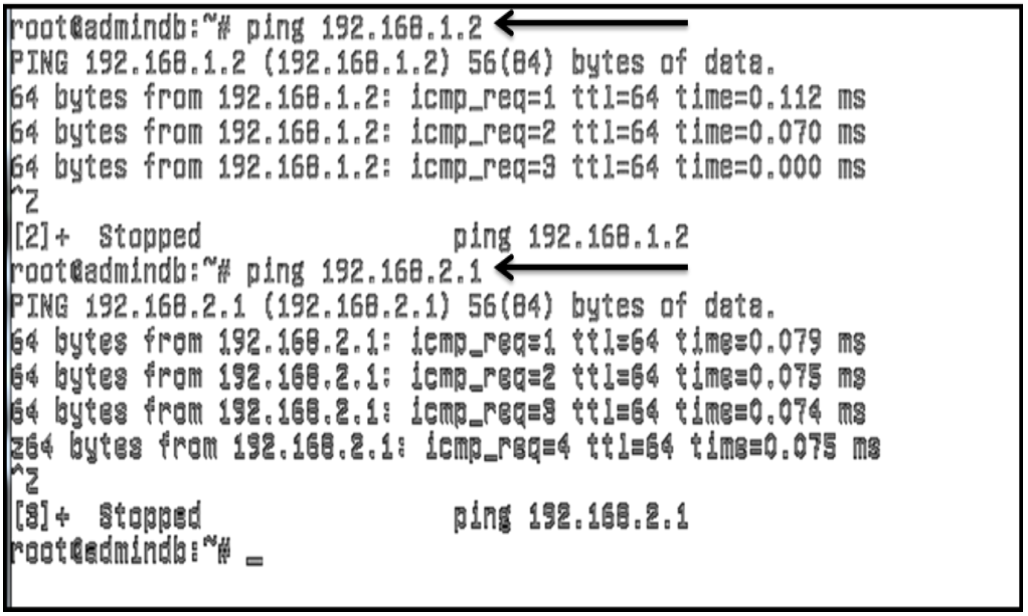


Gambar 5.9 *Mengaktifkan Iptables NAT*

Kemudian restart debian server , gunakan perintah : **reboot**

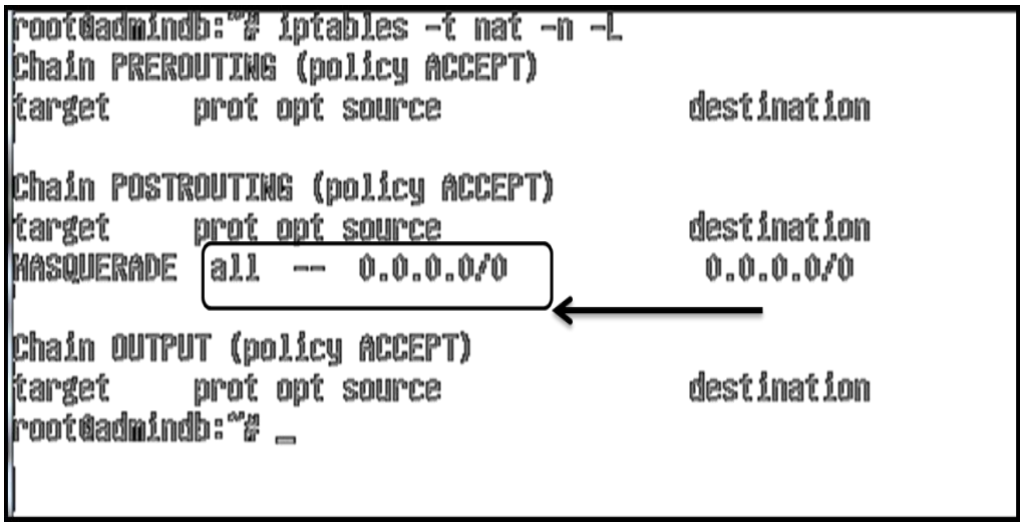
Mengecek koneksi IP Eth0, gunakan perintah : **ping 192.168.1.2**

Mengecek koneksi IP Eth1, gunakan perintah : **ping 192.168.2.1**



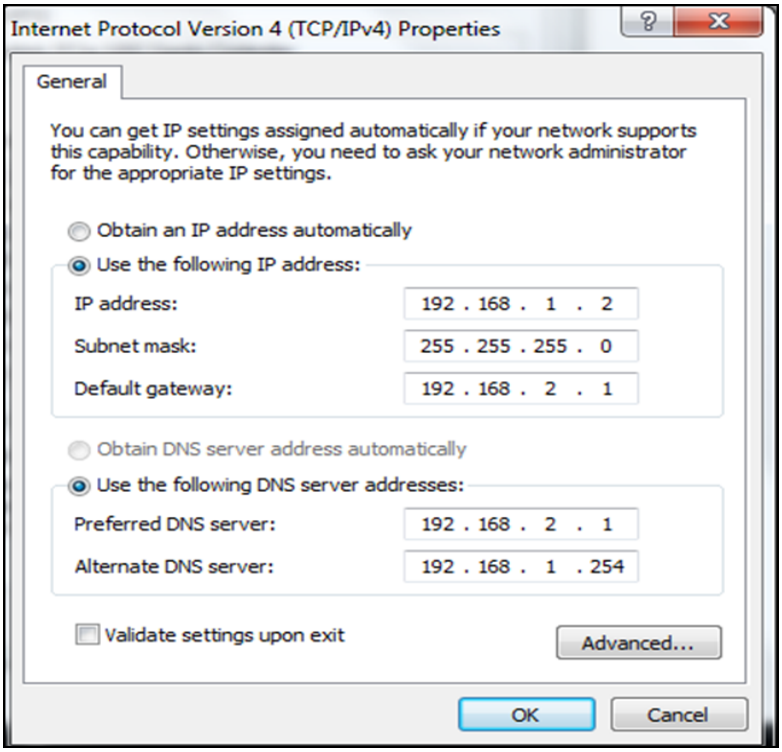
Gambar 5.10 *Mengecek Koneksi IP eth0 dan eth1*

Mengecek nat Iptables telah berhasil, gunakan perintah : **iptables –t nat –n –L**



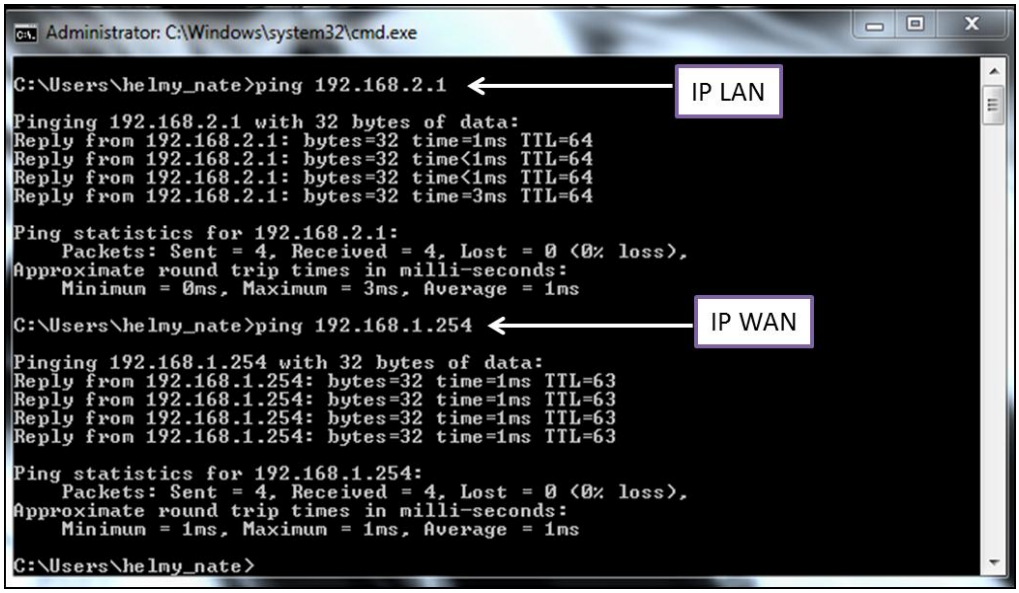
Gambar 5.11 *Cek Nat Iptables*

Menguji koneksi di client (Windows) ke Server Debian. Sesuaikan dengan konfigurasi tcp/ip client.



Gambar 5.12 *Konfigurasi IP Client*

Mengecek koneksi ke server, test ping ke server debian (IP LAN dan IP WAN).



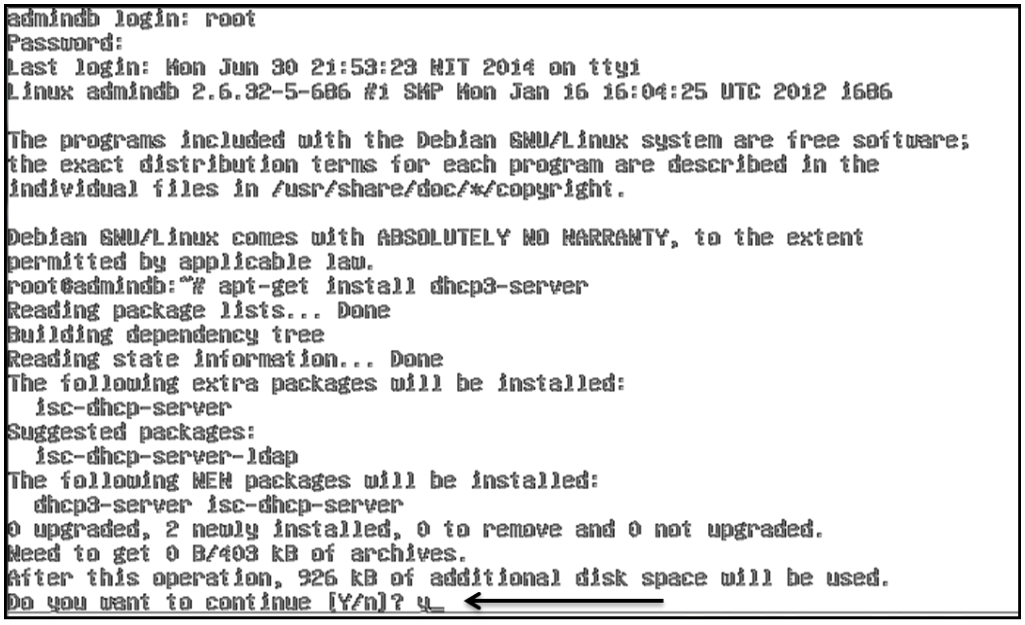
Gambar 5.13 *Tesh Koneksi Ip Server*

5.2 **Konfigurasi DHCP Server**

DHCP (Dynamic Host Configuration Protocol) digunakan untuk melayani request Ip Address dari client. Gunanya adalah untuk mengkonfigurasi Ip pada computer, sebut saja Zero Configuration. Client akan meminta Ip Address pada server, kemudian server akan memberikan alokasi ip yang tersedia. Berikut langkah-langkah konfigurasi DHCP Server Debian :

Menginstal aplikasi dhcp server, gunakan perintah : **apt-get install dhcp3-server**

Isi dengan perintah : **Y** untuk menyetujui proses instalasi aplikasi dhcp server.

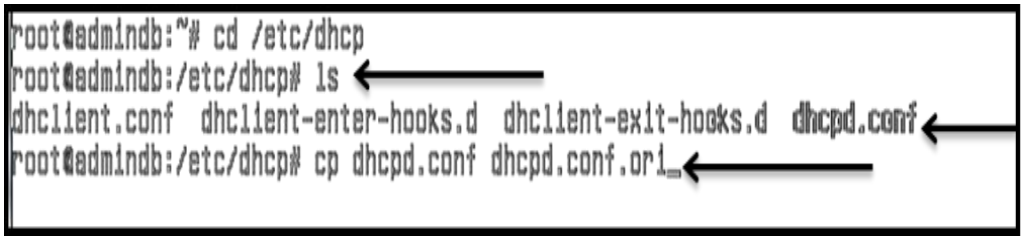


Gambar 5.14 *Instalasi Aplikasi DHCP Server*

Setelah proses instalasi selesai, maka langkah selanjutnya ialah masuk ke folder dhcp dengan menggunakan perintah : **cd /etc/dhcp**

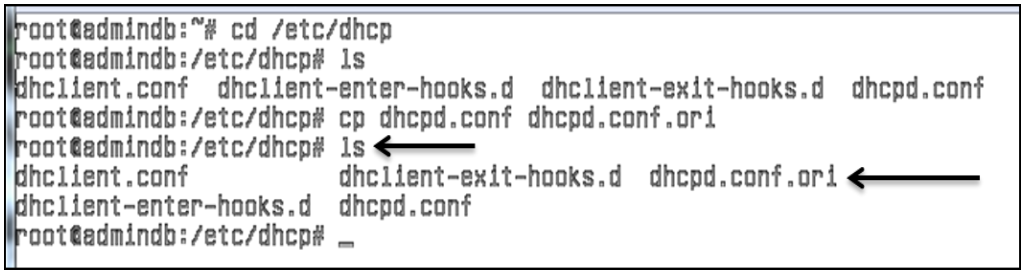
Menampilkan file dari direktori Dhcp, gunakan perintah : **ls**

Kemudian backup file dhcpd.conf dengan menggunakan perintah : **cp dhcpd.conf dhcpd.conf.ori**



Gambar 5.15 *Membackup File Dhcp.conf*

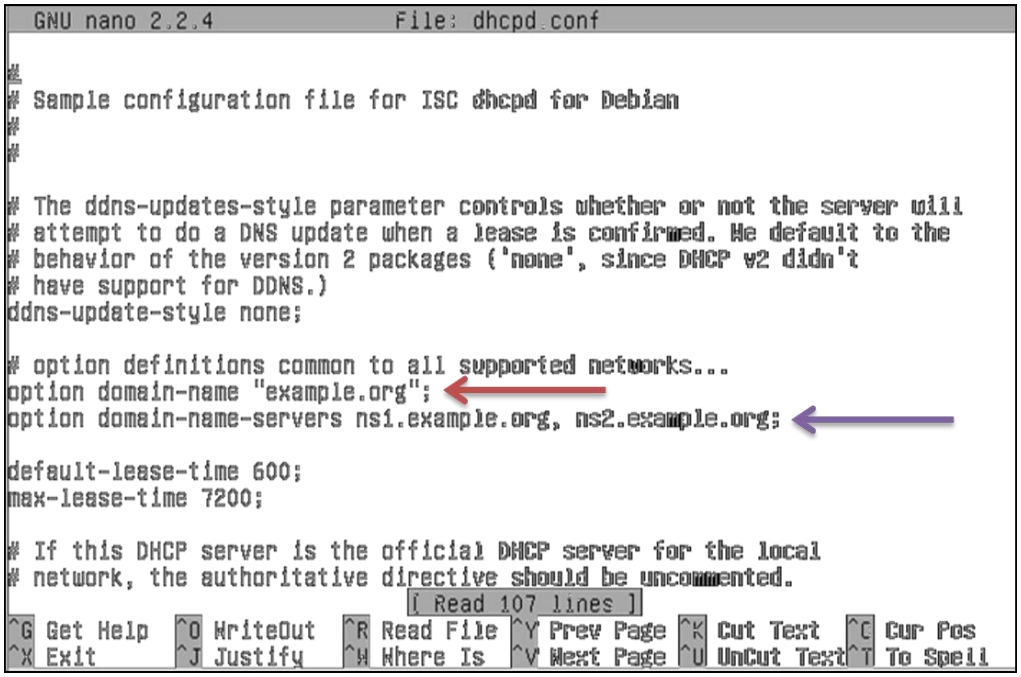
Periksa kembali file dhcp, untuk menyakinkan bahwa file dhcpd.conf telah di backup.



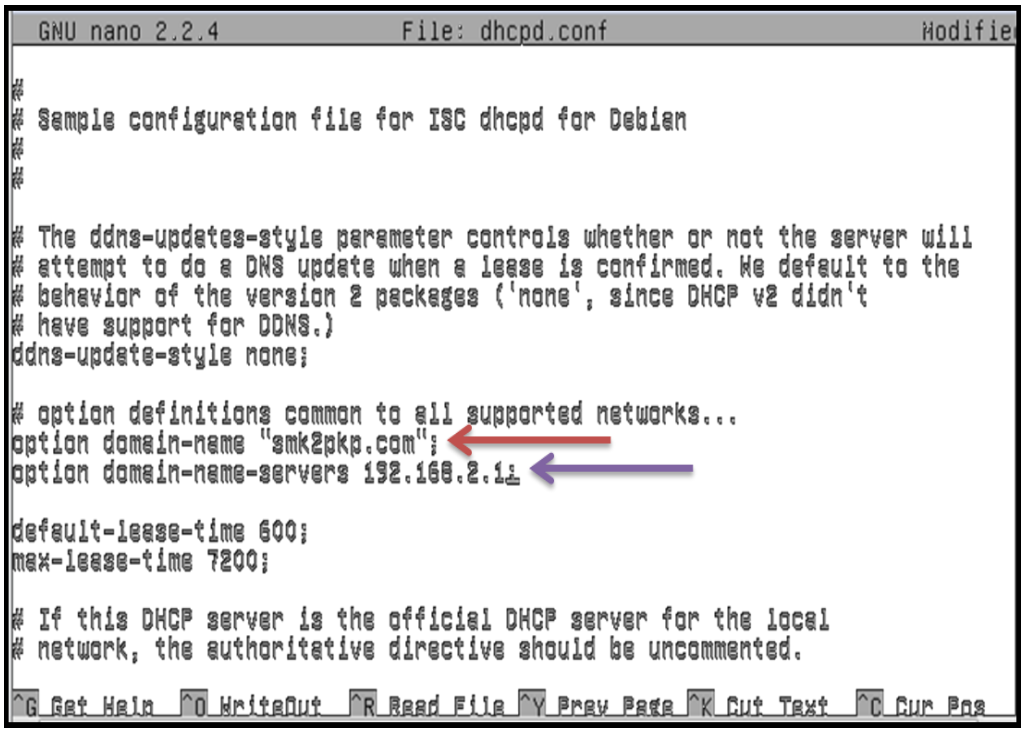
Gambar 5.16 *Memeriksa File Dhcp*

Mengedit file dhcpd.conf dengan menggunakan perintah : **pico dhcpd.conf**

Kemudian edit domain name : **example.org** dengan nama domain dan : **ns1.example.org** dengan IP Addreas eth1.

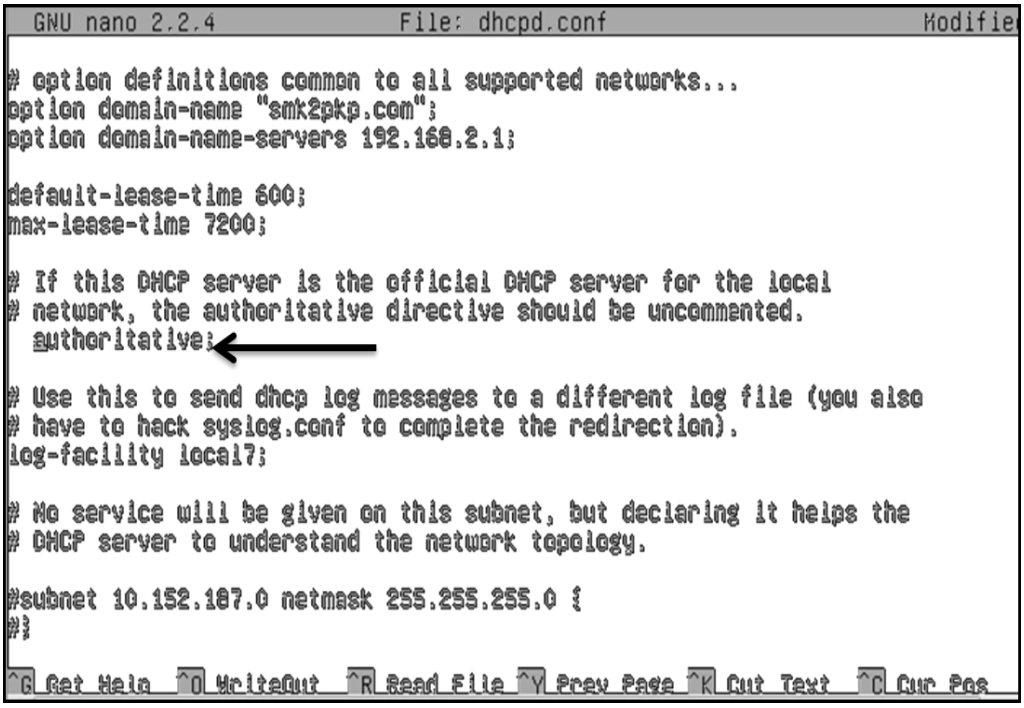


Gambar 5.17 *Mengedit Domain Name*



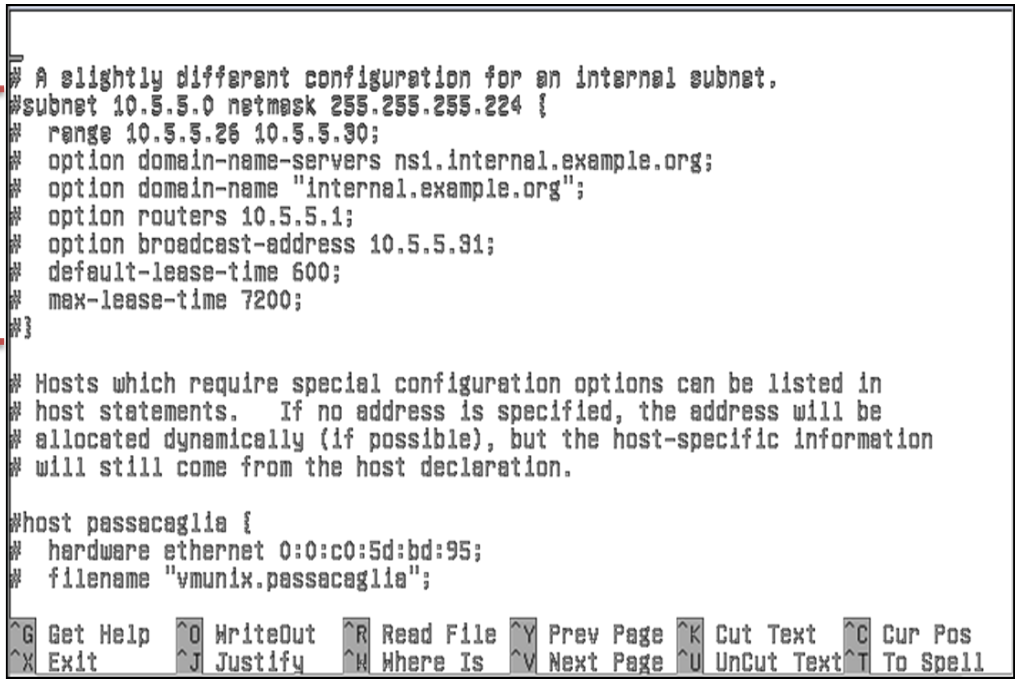
Gambar 5.18 *Tampilan domain name setelah diedit*

Kemudian hapus tanda : # untuk mengaktifkan perintah authoritative.



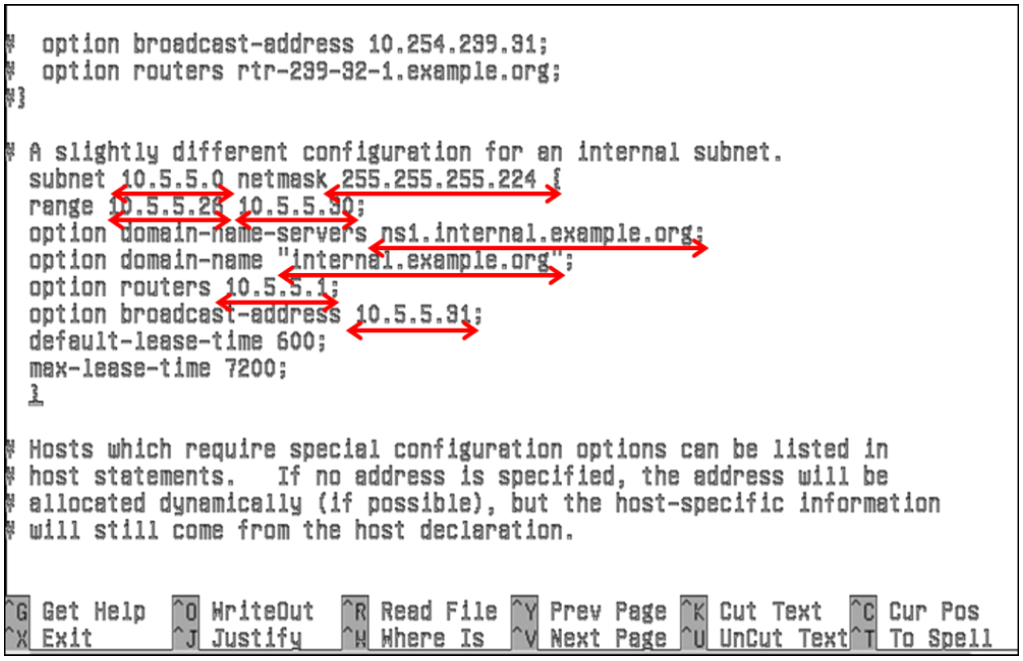
Gambar 5.19 *Mengaktifkan Authoritative*

Kemudian hapus tanda "#" untuk mengaktifkan konfigurasi Dhcp

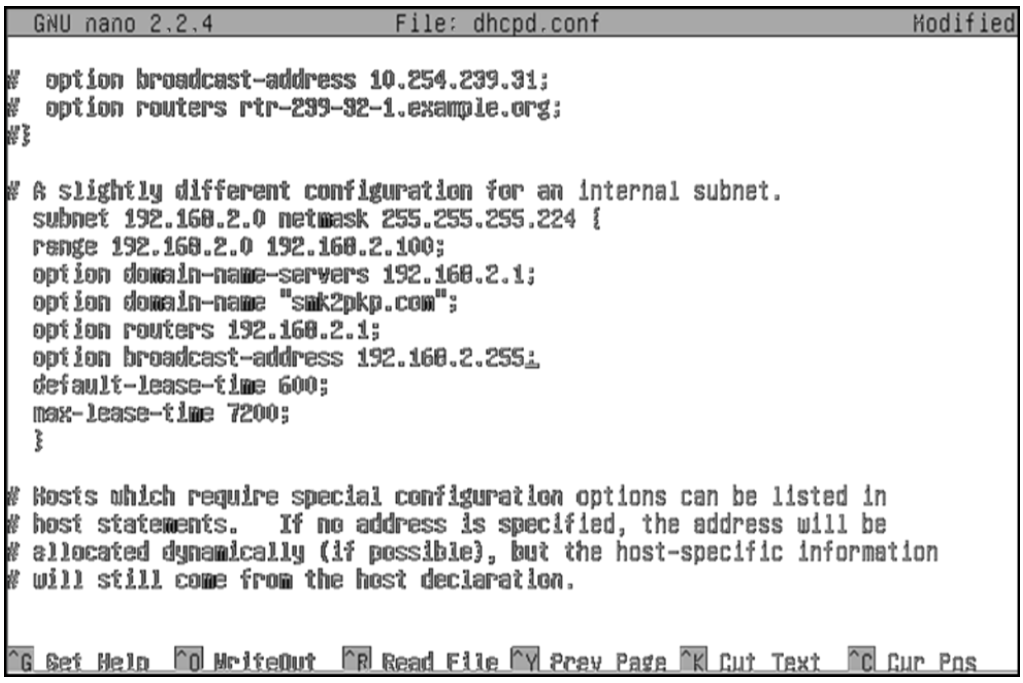


Gambar 5.20 *Konfigurasi DHCP*

Kemudian edit file yang digaris bawah **(IP eth1**).



Gambar 5.21 *Konfigurasi DHCP 1*



Gambar 5.22 *Tampilan DHCP setelah konfigurasi*

kemudian restart dhcp server, gunakan perintah : **/etc/init.d/isc-dhcp-server restart**

Gambar 5.23 *Restart Dhcp Server*

Saat proses restart pertama, pasti akan muncul pemberitahuan : **failed**

Gambar 5.24 *Failed DHCP Server*

Restart kembali dhcp server. Jika tidak ada pemberitahuan failed. Maka konfigurasi telah berhasil.

Gambar 5.25 *Restart Dhcp Server 1*

5.3 **Konfigurasi DNS Server**

Domain Name System adalah suatu metode untuk meng-konversikan Ip Address (numerik) suatu komputer ke dalam suatu nama domain (alphabetic), ataupun sebaliknya. Yang memudahkan kita dalam mengingat computer tersebut. berikut langkah-langkah konfigurasi DNS Server Debian :

Menginstal aplikasi bind9 untuk memulai konfigurasi DNS, gunakan perintah : **apt-get install bind9**

```
root@admindb:~# apt-get install bind9_
```

Isi dengan perintah : **Y** untuk menyetujui proses installasi DNS Server.

```
root@admindb:~# apt-get install bind9
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  bind9utils
Suggested packages:
  bind9-doc resolvconf ufw
The following NEW packages will be installed:
  bind9 bind9utils
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 451 kB of archives.
After this operation, 1,212 kB of additional disk space will be used.
Do you want to continue [Y/n]? Y_
```

Gambar 5.26 *Instalasi Aplikasi bind9*

Setelah proses instalasi selesai, maka langkah selanjutnya ialah masuk ke folder bind dengan menggunakan perintah : **cd /etc/bind**

```
  bind9-doc resolvconf ufw
The following NEW packages will be installed:
  bind9 bind9utils
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 0 B/454 kB of archives.
After this operation, 1,389 kB of additional disk space will be used.
Do you want to continue [Y/n]? Y
Preconfiguring packages ...
Selecting previously deselected package bind9utils.
(Reading database ... 22488 files and directories currently installed.)
Unpacking bind9utils (from .../bind9utils_9.7.3.dfsg-1~squeeze4_i386.deb) ...
Selecting previously deselected package bind9.
Unpacking bind9 (from .../bind9_9.7.3.dfsg-1~squeeze4_i386.deb) ...
Processing triggers for man-db ...
Setting up bind9utils (1:9.7.3.dfsg-1~squeeze4) ...
Setting up bind9 (1:9.7.3.dfsg-1~squeeze4) ...
Adding group `bind' (GID 106) ...
Done.
Adding system user `bind' (UID 103) ...
Adding new user `bind' (UID 103) with group `bind' ...
Not creating home directory `/var/cache/bind'.
wrote key file "/etc/bind/rndc.key"
#
Starting domain name service...: bind9.
root@admindb:~# cd /etc/bind_
```

Gambar 5.27 *Masuk ke Direktory Bind*

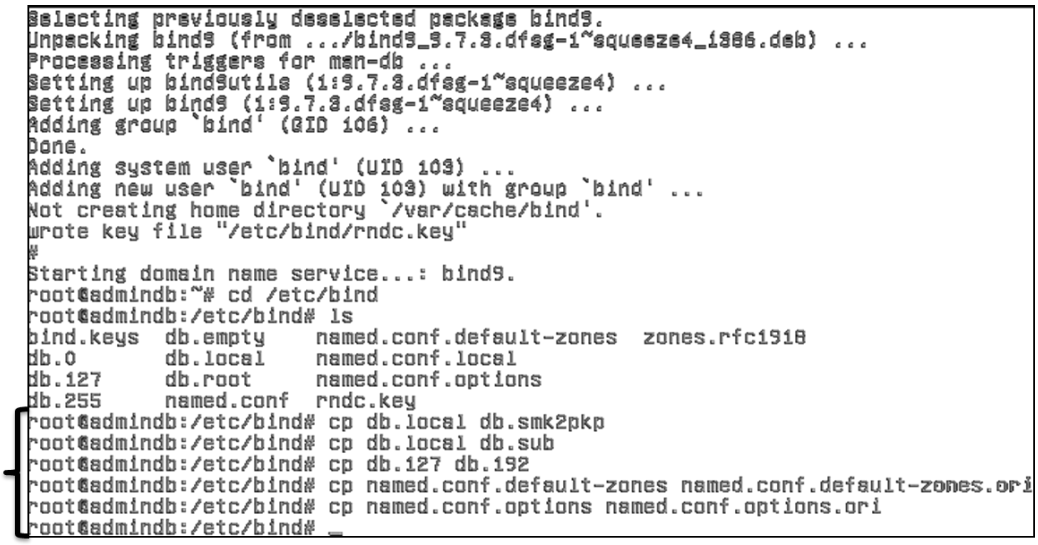
Mengecek isi direktori Bind, gunakan perintah : **ls**

```
The following NEW packages will be installed:
  bind9 bind9utils
0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded.
Need to get 0 B/454 kB of archives.
After this operation, 1,389 kB of additional disk space will be used.
Do you want to continue [Y/n]? Y
Preconfiguring packages ...
Selecting previously deselected package bind9utils.
(Reading database ... 22488 files and directories currently installed.)
Unpacking bind9utils (from .../bind9utils_9.7.3.dfsg-1~squeeze4_i386.deb) ...
Selecting previously deselected package bind9.
Unpacking bind9 (from .../bind9_9.7.3.dfsg-1~squeeze4_i386.deb) ...
Processing triggers for man-db ...
Setting up bind9utils (1:9.7.3.dfsg-1~squeeze4) ...
Setting up bind9 (1:9.7.3.dfsg-1~squeeze4) ...
Adding group `bind' (GID 106) ...
Done.
Adding system user `bind' (UID 103) ...
Adding new user `bind' (UID 103) with group `bind' ...
Not creating home directory `/var/cache/bind'.
wrote key file "/etc/bind/rndc.key"
#
Starting domain name service...: bind9.
root@admindb:~# cd /etc/bind
root@admindb:/etc/bind# ls_
```

Gambar 5.28 *Cek isi Directory Bind*

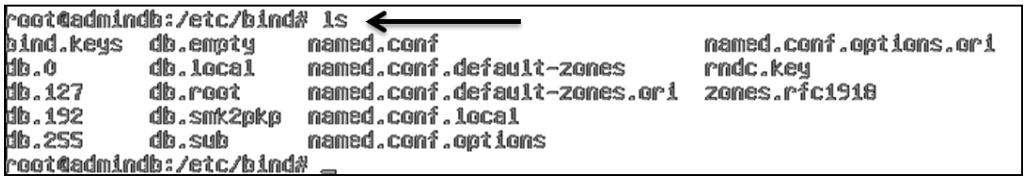
Ditahap ini, kita akan membuat (mengcopy) 3 file dan 2 file backup.

- cp db.local → db.smk2pkp (nama domain)
- cp db.local → db.sub
- cp db.127 → db.192 (IP eth1)
- cp named.conf.default-zones → named.conf.default-zones.ori (backup)
- cp named.conf.options → named.conf.options.ori (backup)



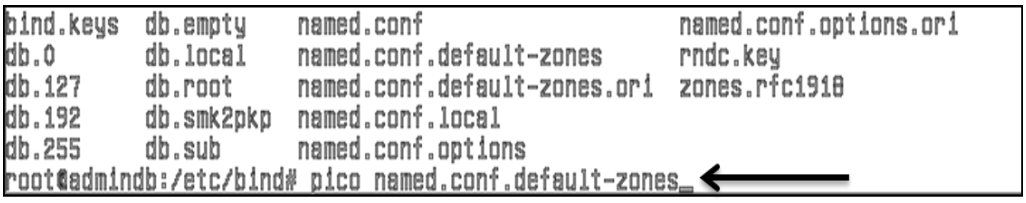
Gambar 5.29 *Mengedit File Bind*

Memastikan isi file Bind telah tercopy, gunakan perintah : **ls**



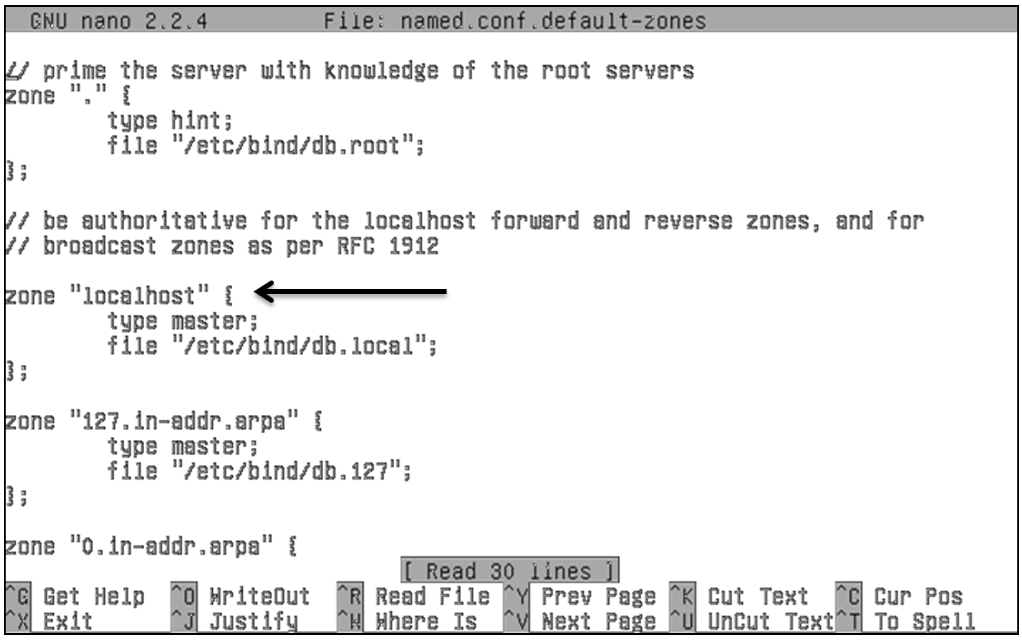
Gambar 5.30 *Mengecek File Bind yang tercopy*

Mengedit file **named.conf.default-zones ,** gunakan perintah : **pico named.conf.default-zones**



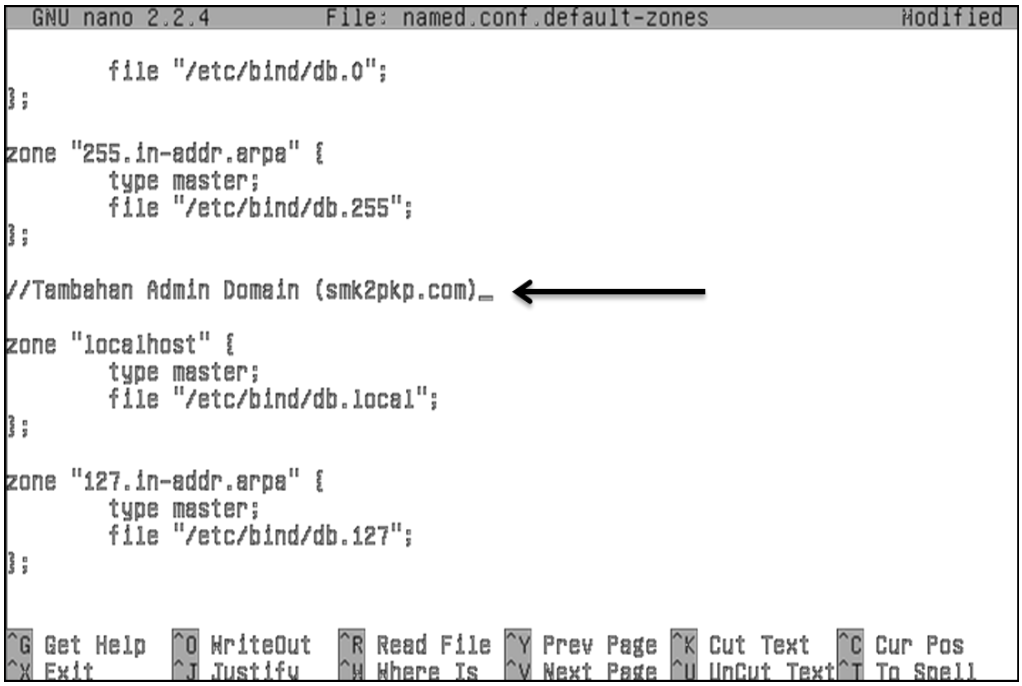
Gambar 5.31 *Mengedit file named.conf.default-zones*

Menambahkan admin domain pada default zones, gunakan trik **"cut-uncut"** untuk mempercepat pengeditan interfaces. Catatan : cut dimulai dari **(zone "localhost")**

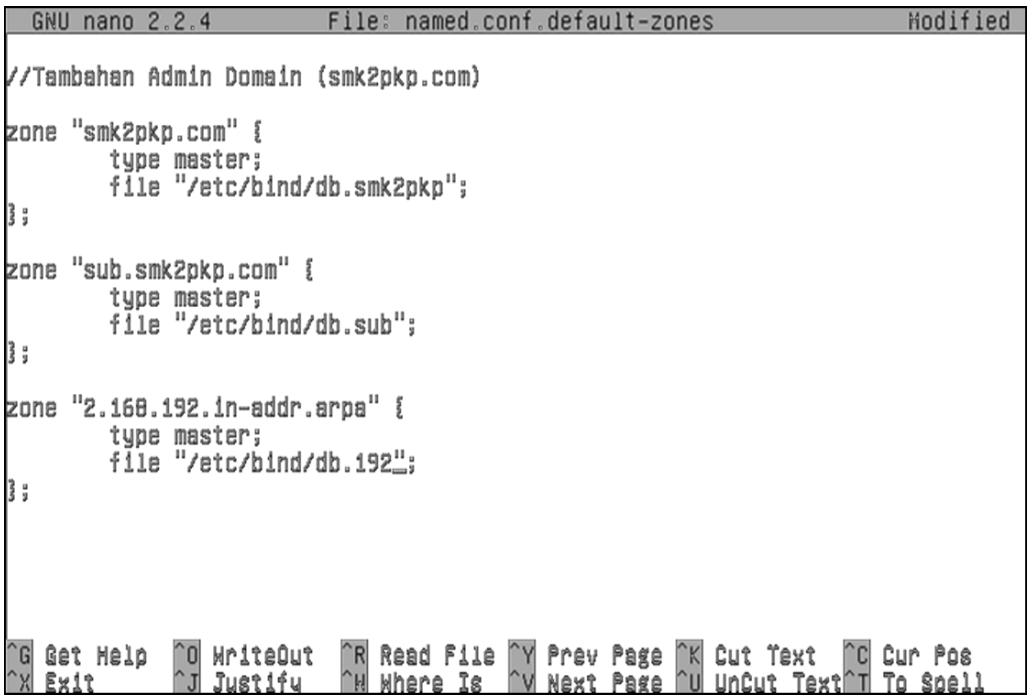


Gambar 5.32 *Menambahkan Admin Domain*

Awali tambahan default zone dengan tanda (//).



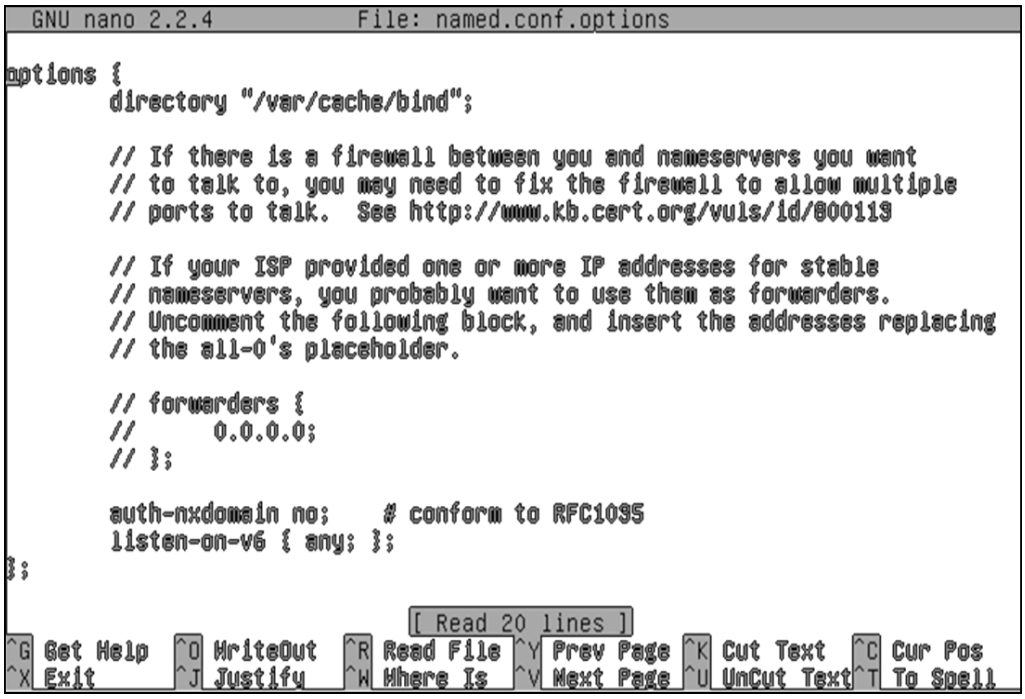
Gambar 5.33 *Mengedit Default Zones*



Gambar 5.34 *Tampilan Default Zones setelah diedit*

Mengedit file named.default.options, gunakan perintah : **pico named.conf.options**

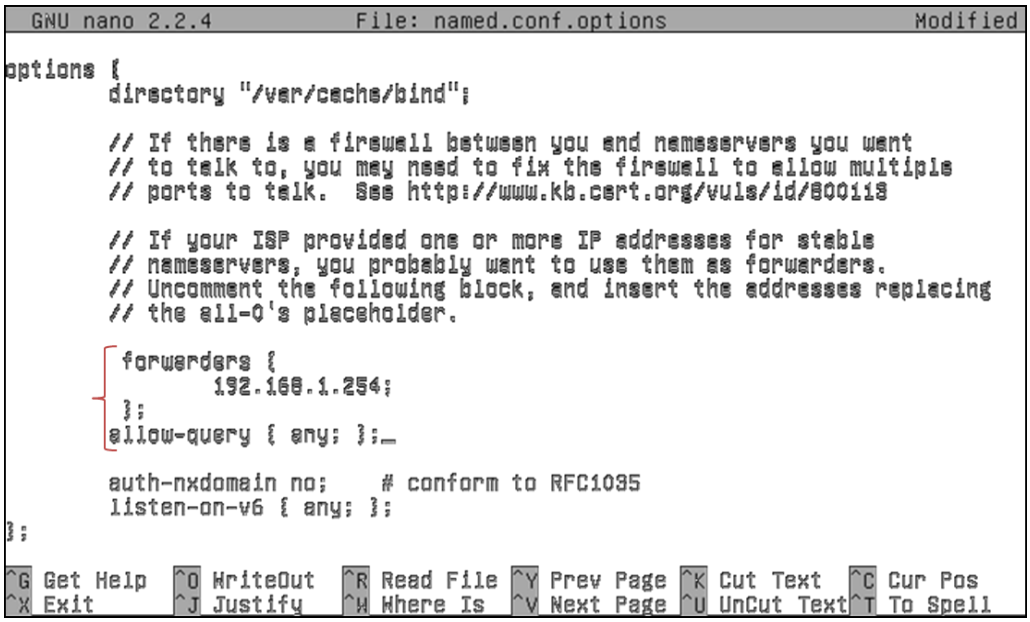
Tampilan awal file named.conf.options



Gambar 5.35 *Tampilan Awal File named.conf.options*

Hapus tanda (//) , tambahkan allow-query { any; };

Dan ganti 0.0.0.0; menjadi IP ISP.

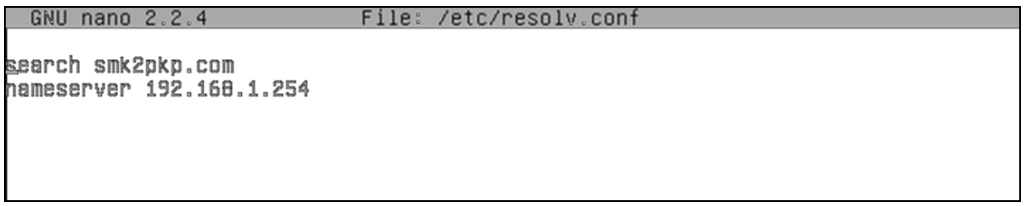


Gambar 5.36 *Mengedit File named.conf.options*

Mengedit file resolv.conf , gunakan perintah : **pico /etc/resolv.conf**

ctt: perintah menggunakan perintah /etc/ karena file tersebut terdapat difolder etc.

Gambar 5.37 *Mengedit file resolv.conf*

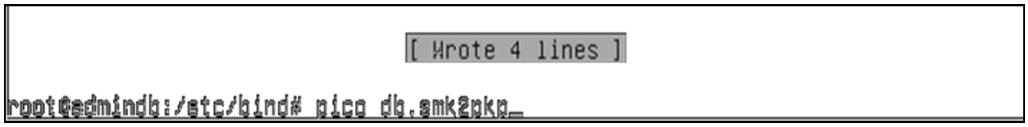


Gambar 5.38 *Tampilan Awal File resolv.conf*

Mambahkan nameserver IP Local dan IP eth1.

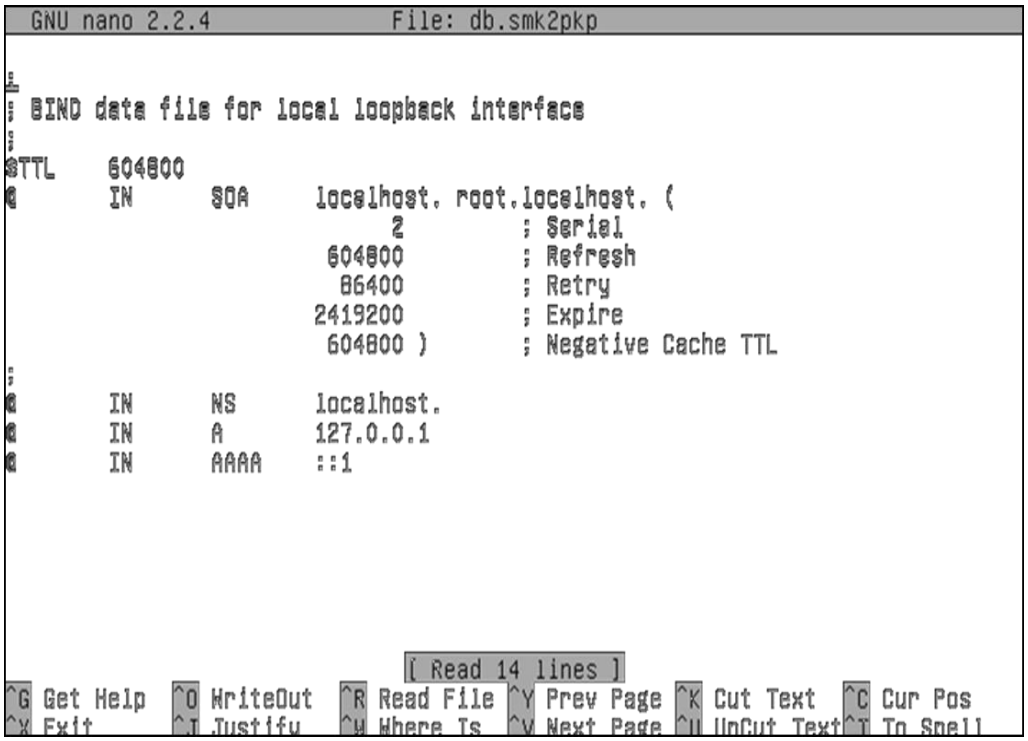
Gambar 5.39 *Menambahkan name server*

Mengedit file db.smk2pkp, gunakan perintah : **pico db.smk2pkp**



Gambar 5.40 *Edit file db.smk2pkp*

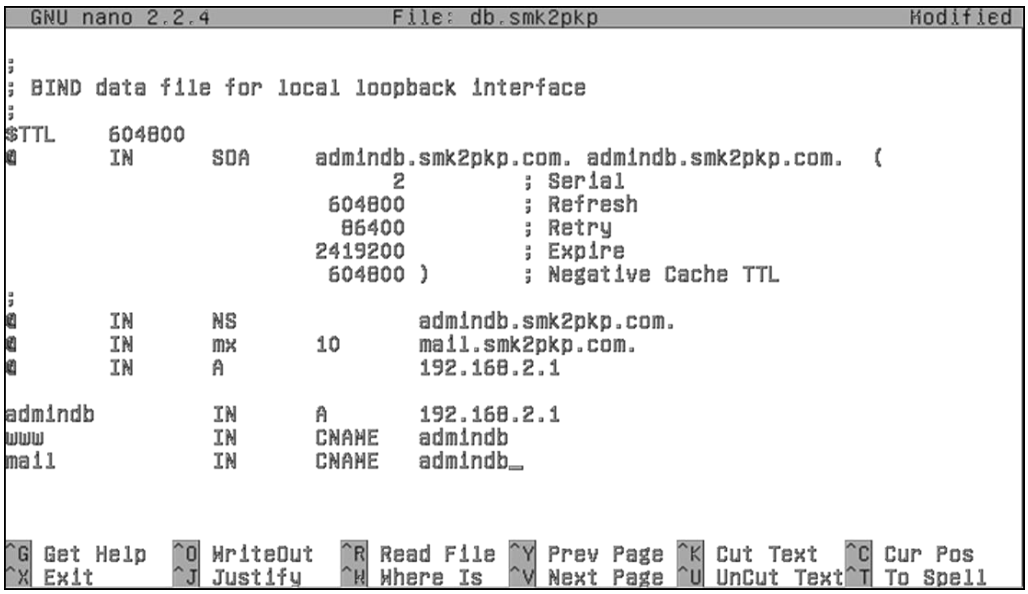
Tampilan awal file db.smk2pkp



Gambar 5.41 *Tampilan file db.smk2pkp*

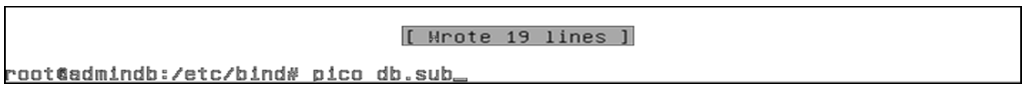
Tampilan file db.smk2pkp setelah diedit.

Perhatikan hostname, domain, dan tanda (.) secara teliti.



Gambar 5.42 *File db.smk2pkp setelah diedit*

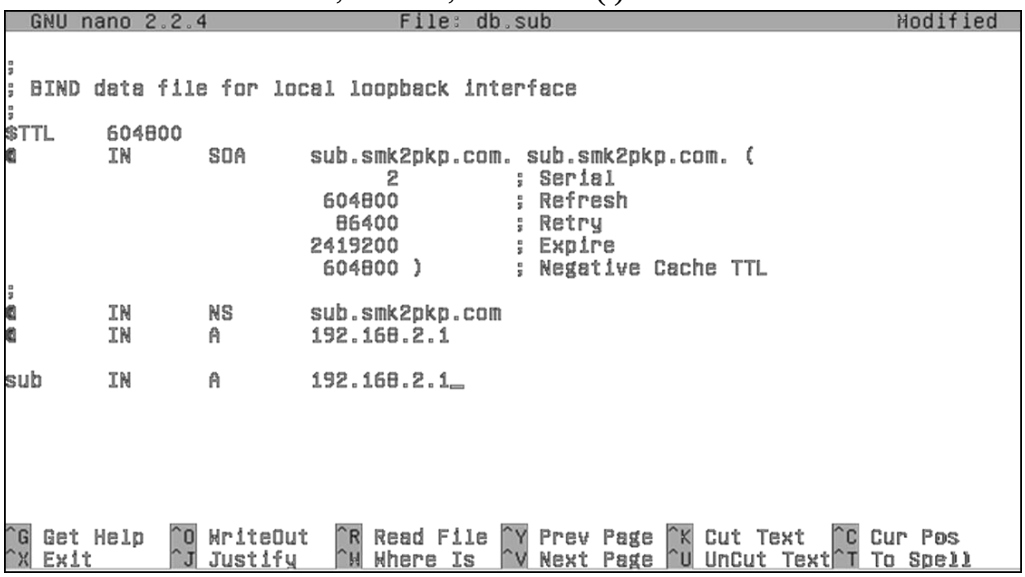
Mengedit file db.sub, gunakan perintah : **pico db.sub**



Gambar 5.43 *Mengedit file db.sub*

Tampilan file db.sub setelah diedit.

Ctt : Perhatikan hostname, domain, dan tanda (.) secara teliti.



Gambar 5.44 *File db.sub setelah diedit*

Mengedit file db.192, gunakan perintah : **pico db.192**

```
                              [ Wrote 15 lines ]

root@admindb:/etc/bind# pico db.192_
```

Gambar 5.45 *Mengedit file db.192*

Tampilan file db.192 setelah diedit.

Perhatikan hostname, domain, dan tanda (.) secara teliti.

```
  GNU nano 2.2.4                File: db.192                          Modified

;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     admindb.smk2pkp.com. admindb.smk2pkp.com. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      admindb.smk2pkp.com.
1_      IN      PTR     admindb.smk2pkp.com.




^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

Gambar 5.46 *File db.192 setelah diedit*

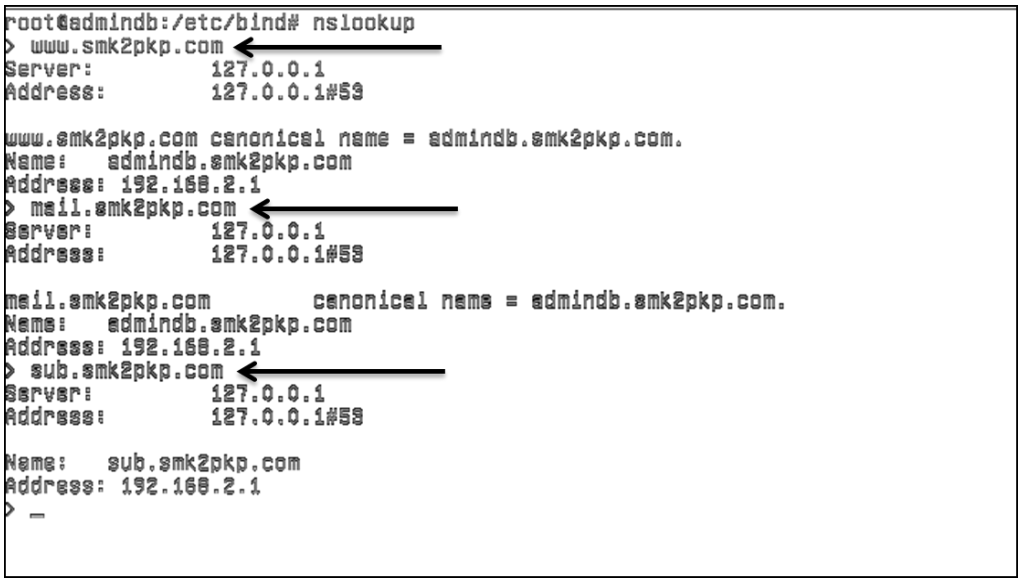
Rerestart server DNS (bind9), gunakan perintah : **/etc/init.d/bind9 restart**

```
                              [ Wrote 13 lines ]

root@admindb:/etc/bind# /etc/init.d/bind9 restart_
```

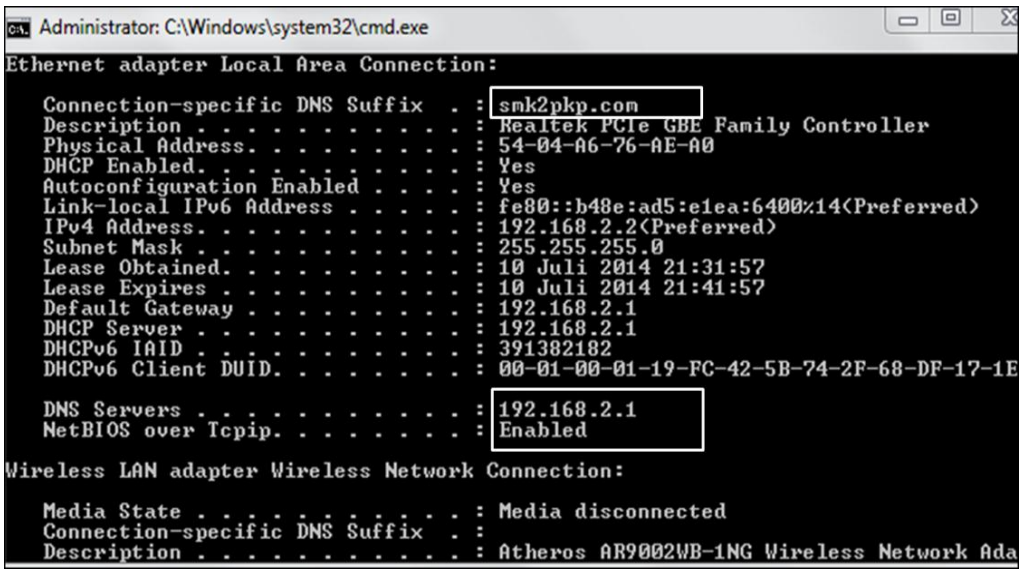
Gambar 5.47 *Restart DNS Server (bind9)*

Memeriksa konfigurasi DNS di Server Debian, gunakan perintah : **nslookup**



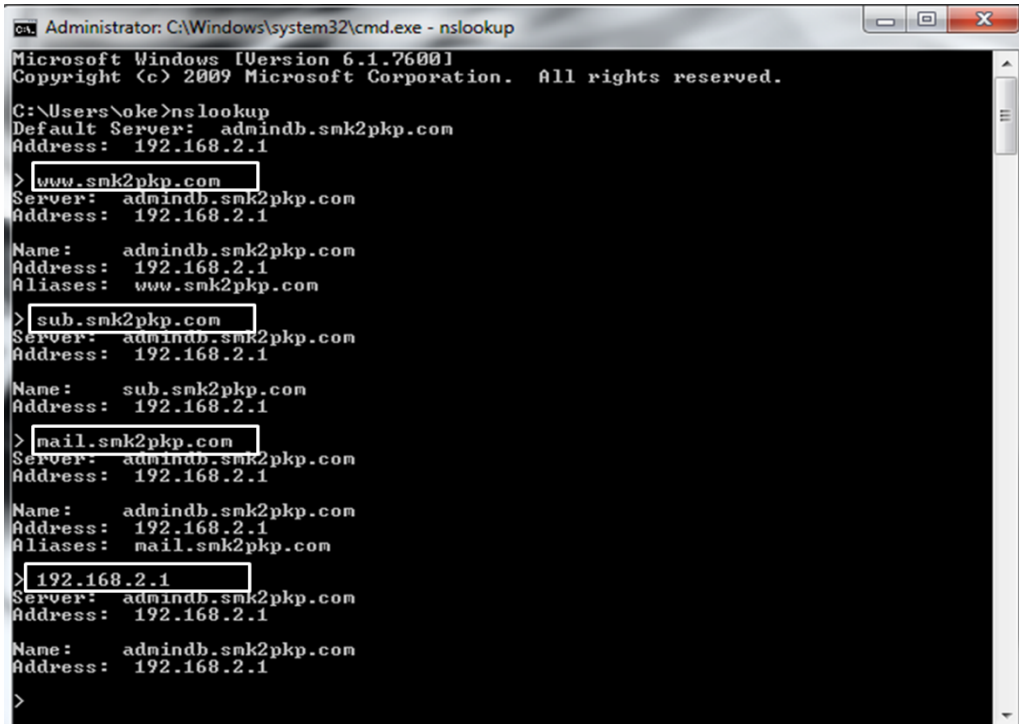
Gambar 5.48 *Memeriksa Konfigurasi DNS*

Setelah konfigurasi di server debian selesai, kita harus menguji berfungsi tidaknya DNS di client. Pada Client (Windows) Gunakan perintah : **ipconfig /all** untuk memeriksa semua konfigurasi ip.



Gambar 5.49 *Cek Ipconfig pada client*

Gunakan perintah : **nslookup** untuk memeriksa apakah client sudah berhasil mendapat DNS Server.

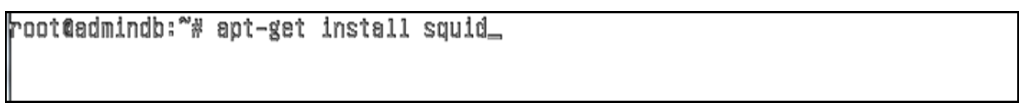


Gambar 5.50 *Cek nslookup pada client*

5.4 Konfigurasi Proxy Server

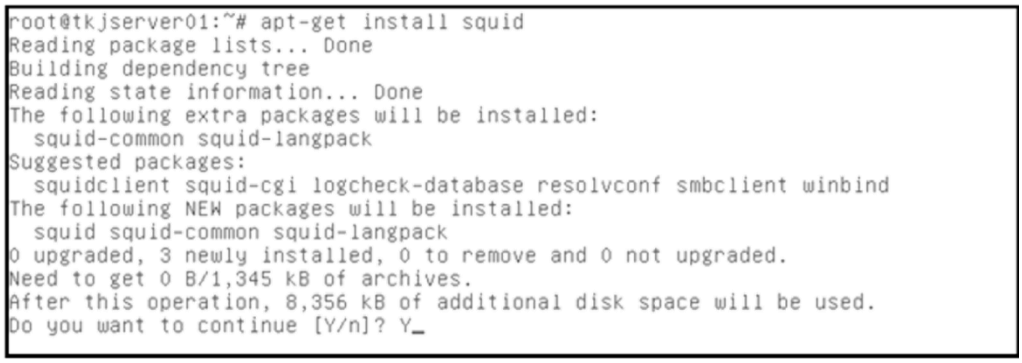
PROXY Server berfungsi untuk menyimpan halaman-halaman website yang pernah kita kunjungi. Fungsinya adalah sebagai CACHE, yang sewaktu-waktu jika kita ingin mengunjungi halaman yang sama, akan diambilkan dari Proxy tersebut terlebih dahulu, dan jika belum ada maka akan diteruskan ke server sebenarnya. Selain itu proxy juga dapat digunakan untuk Security, misalnya dengan memblokir akses ke suatu website ataupun sebagainya. Berikut langkah-langkah konfigurasi Proxy Server :

Instalasi aplikasi Squid untuk memulai konfigurasi Proxy Server, gunakan perintah : **apt-get install squid**



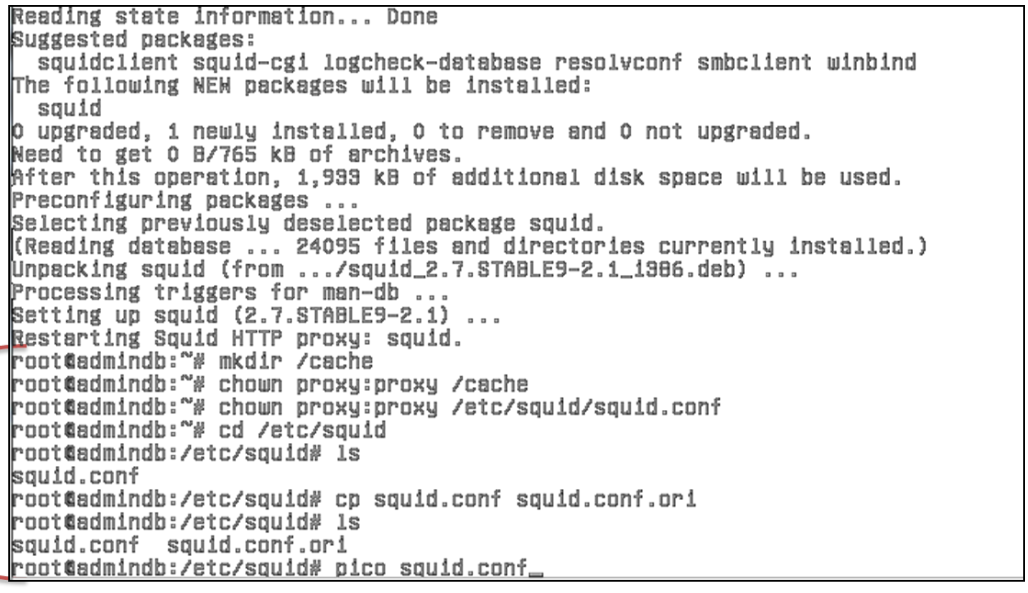
Gambar 5.51 *Instalasi Squid*

Isi dengan perintah “Y” untuk menyetujui proses installasi.



Gambar 5.52 *Memulai Instalasi Squid*

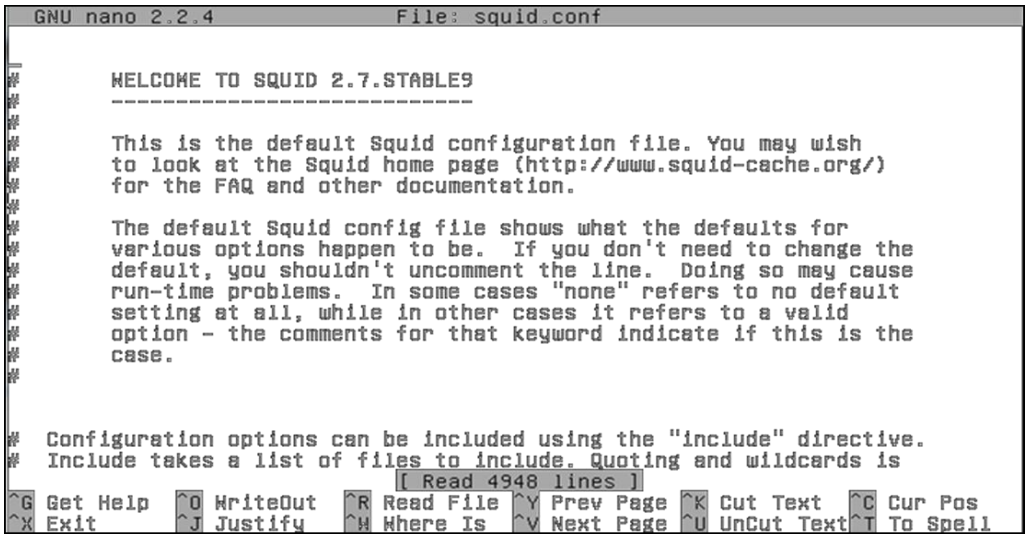
- Gunakan perintah “mkdir /cache” untuk membuat directory untuk penyimpanan cache.
- Gunakan perintah “chown proxy:proxy /cache” untuk mengubah kepemilikan folder cache.
- Gunakan perintah “chown proxy:proxy /etc/squid/squid.conf” untuk mengubah kepemilikan folder squid.conf
- Gunakan perintah “cd /etc/squid” untuk masuk ke folder squid.
- Gunakan perintah “cp squid.conf squid.conf.ori”untuk mengcopy/bakup folder squid.conf.
- Gunakan perintah “pico squid.conf” untuk mengedit folder squid.conf.



Gambar 5.53 *Mengedit File Direktori Squid*

Tampilan awal Folder squid.conf

Gunakan fitur pencarian (untuk mengaktifkan fitur pencarian gunakan kombinasi CTRL+W)



Gambar 5.54 *Tampilan awal file Squid.conf*

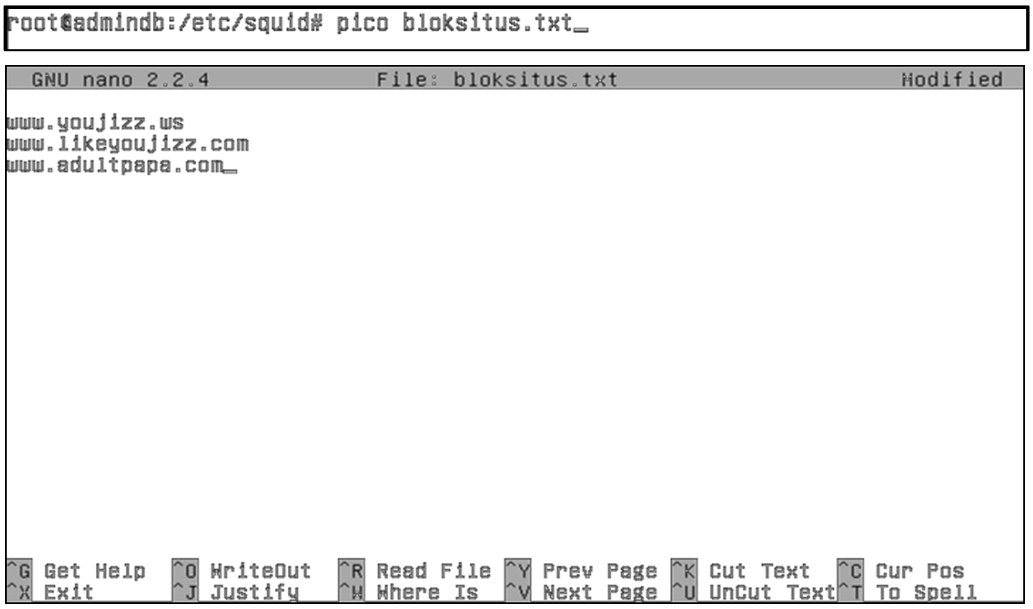
Mengkonfigurasi File squid.conf

```
GNU nano 2.2.4                File: squid.conf
# Parameter port dan type proxy yang digunakan
http_port 3128 transparent
# Paremeter Kendali Akses
acl all src all
acl manager proto cache object
acl localhost src 127.0.0.1/32
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32
acl lanku src 192.168.2.1
# Parameter blok situs
acl bloksitus dstdomain "/etc/squid/bloksitus.txt"
acl key url_regex –i "/etc/squid/key.txt"
#Penerapan rules
http_access allow lanku
http_access allow all
http_access deny bloksitus
http_access deny key
http_access deny manager
http_access deny !Safe_ports
http_access allow localhost
# Parameter penyimpanan cache
cache_effective_user proxy
cache_effective_group proxy
cache_mem 64 MB
cache_dir ufs /cache 10000 16 254
cache_store_log none
store_dir_select_algorithm round-robin
cache_replacement_policy heap GDSF
cache_replacement_policy heap LFUDA
# Adminstratif
cache_mgr admindb@smk2pkp.com
visible_hostname www.smk2pkp.com
```

Gambar 5.55 *Konfigurasi File squid.conf*

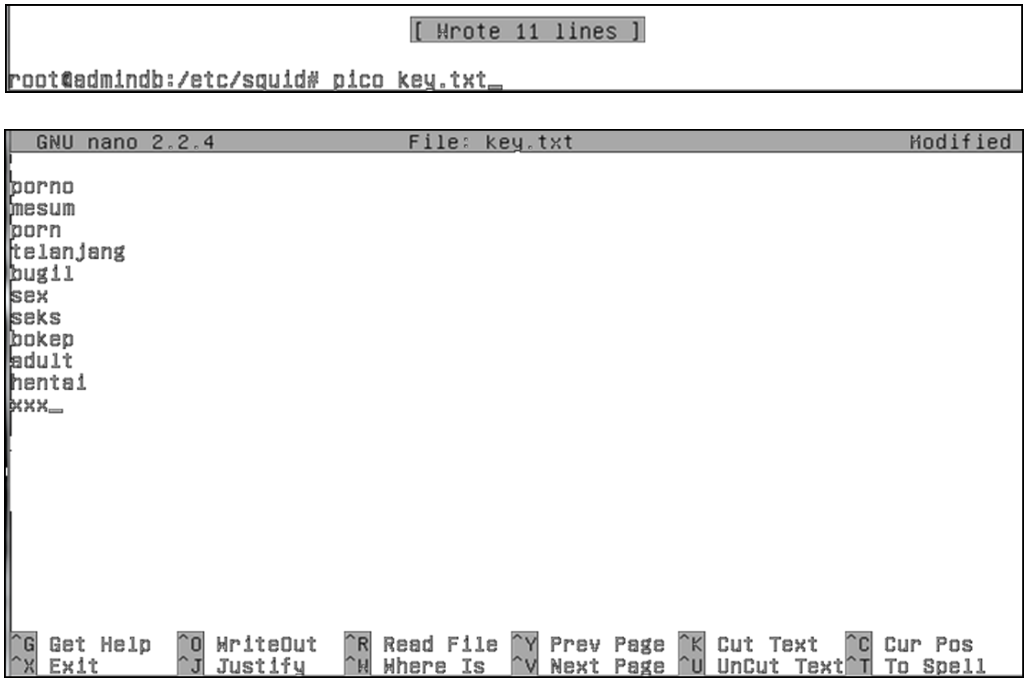
Cari tulisan **http_access deny all,** ada dua pada file squid.conf. Dan tambahkan tanda "#" pada kedua baris tersebut. Simpan konfigurasi squid.

Gunakan perintah "pico bloksitus.txt" untuk membuat daftar situs yang diblokir.



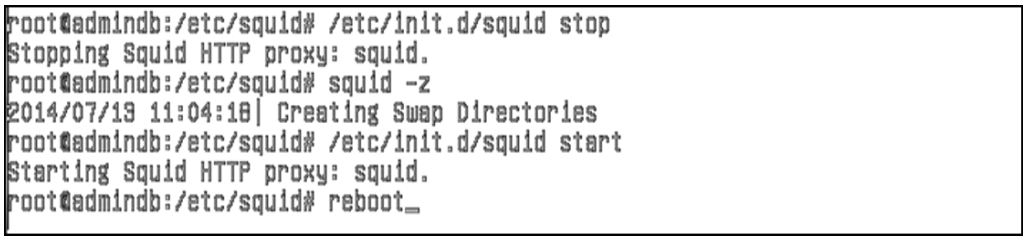
Gambar 5.56 *Membuat Daftar Bloksitus*

Gunakan perintah "pico key.txt" untuk membuat daftar keyword yang diblokir.



Gambar 5.57 *Membuat Daftar Keyword*

- Gunakan perintah “/etc/init.d/squid stop” untuk menghentikan squid.
- Gunakan perintah “squid -z” untuk membuat swap directories
- Gunakan perintah “/etc/init.d/squid start” untuk memulai squid.
- Gunakan perintah “reboot” untuk merestart server.

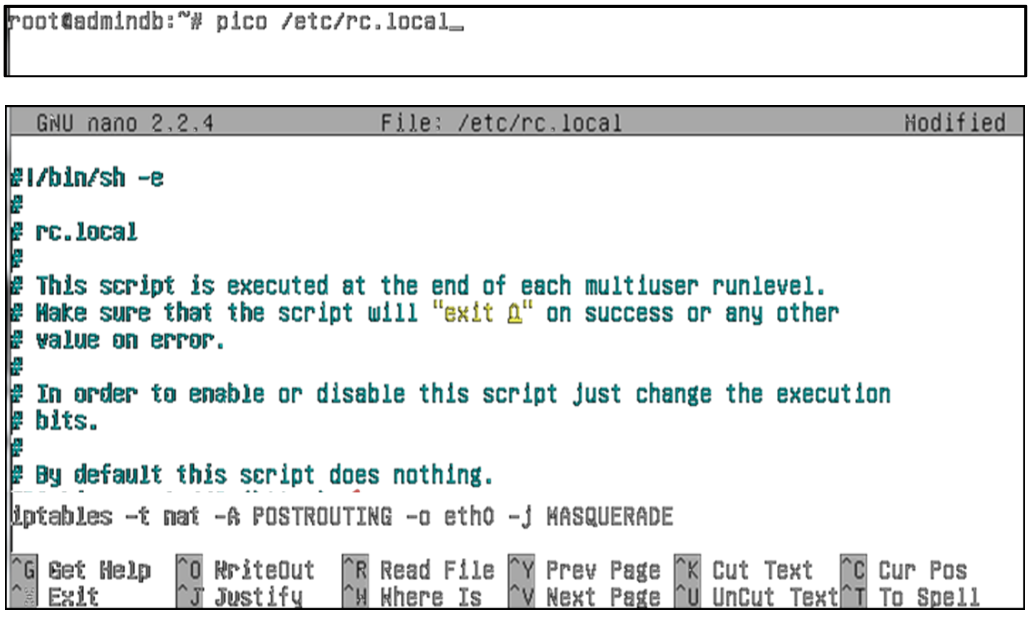


Gambar 5.58 *Merestart Squid*

5.5 Konfigurasi Firewall Debian

Firewall atau Tembok Api, berfungsi untuk memfilter semua paket yang lewat pada dirinya, baik dari jaringan Lokal ataupun Internet. Berikut konfigurasi firewall pada debian :

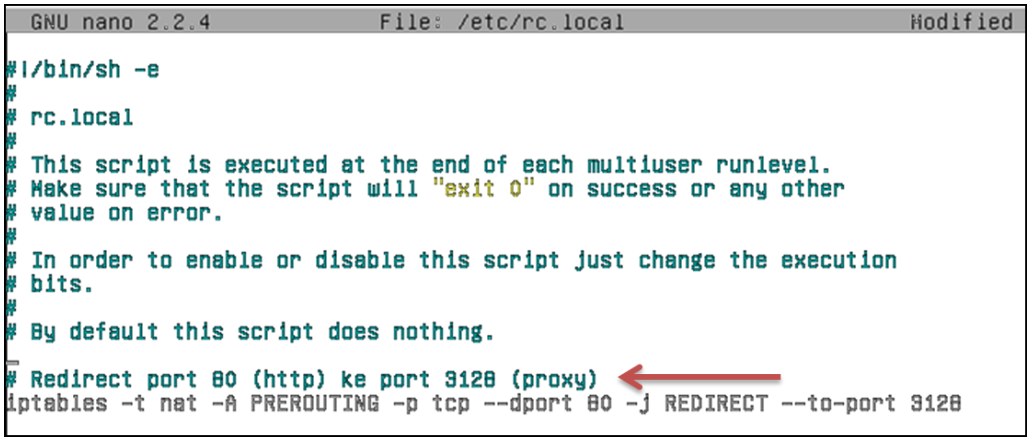
Edit file “rc.local” untuk menambahkan settingan firewall pada server proxy debian : **pico /etc/rc.local**



Gambar 5.59 *Tampilan awal rc.local*

a. Redirect port 80 *(http)* ke port 3128 *(proxy server)*

Konfigurasi firewall : **iptables –t nat –A PREROUTING –p tcp –dport 80 –j REDIRECT –to-port 3128**

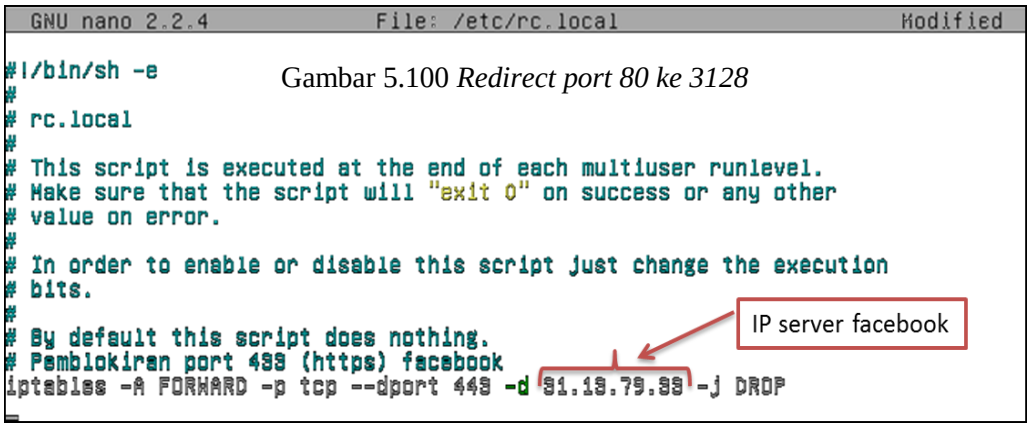


Gambar 5.60 *Redirect port 80 ke 3128*

b. Bloking port 443 (https)

Pada pemblokiran port https yang akan diblok adalah ip address server **www.facebook.com** dan **www.youtube.com**

Konfigurasi firewall pemblokiran facebook : **iptables –A FORWARD –p tcp –dport 443 –d 31.13.79.33 –j DROP**



Gambar 5.100 *Redirect port 80 ke 3128*

Gambar 5.61 *Blocking https facebook*

Konfigurasi firewall pemblokiran youtube :

```
# Pemblokiran port 443 (https) youtube
iptables –A FORWARD –p tcp –dport 443 –d 173.194.117.73 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 173.194.117.96 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 173.194.117.97 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 173.194.117.98 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 173.194.117.99 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 173.194.117.100 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 173.194.117.101 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 173.194.117.102 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 173.194.117.103 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 173.194.117.105 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 173.194.117.110 –j DROP

iptables –A FORWARD –p tcp –dport 443 –d 173.194.38.162 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 173.194.38.130 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 173.194.38.131 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 173.194.38.132 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 173.194.38.133 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 173.194.38.134 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 173.194.38.135 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 173.194.38.136 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 173.194.38.137 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 173.194.38.142 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 173.194.38.128 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 173.194.38.129 –j DROP

iptables –A FORWARD –p tcp –dport 443 –d 74.125.68.91 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 74.125.68.93 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 74.125.68.136 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 74.125.68.190 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 74.125.130.91 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 74.125.130.93 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 74.125.130.136 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 74.125.130.190 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 74.125.200.91 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 74.125.200.93 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 74.125.200.136 –j DROP
iptables –A FORWARD –p tcp –dport 443 –d 74.125.200.190 –j DROP
```

Gambar 5.62 *Blocking https youtube*

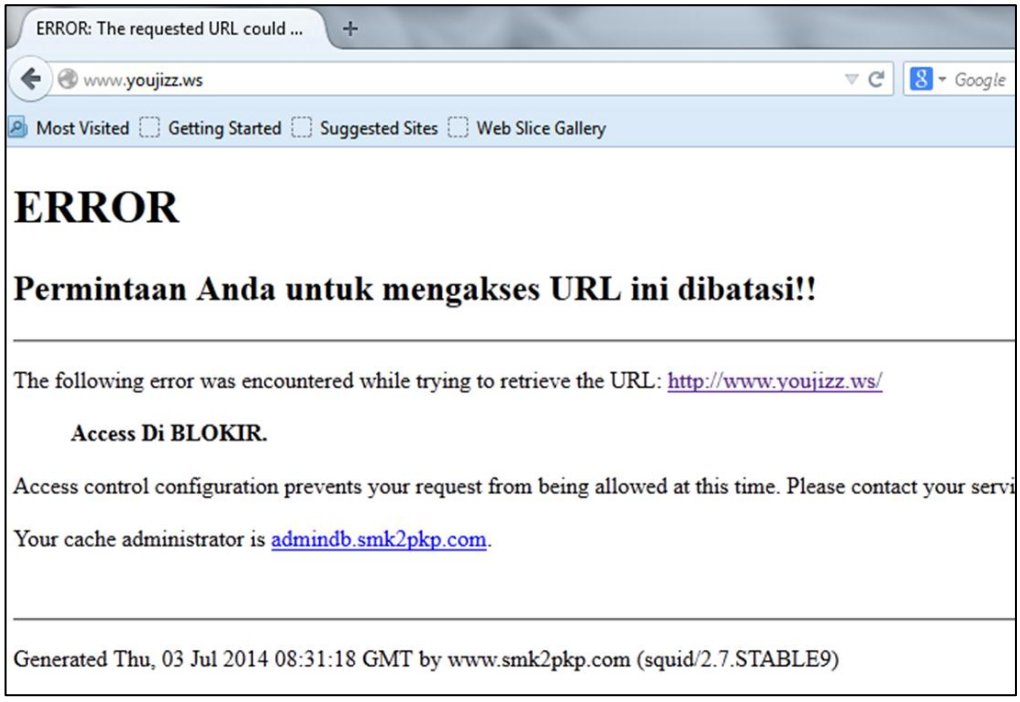
5.7 Pengujian Jaringan

5.7.1 Sistem Filtering dan Blocking Website

Ketika semua sudah berjalan dengan baik dan dapat berdiri masing-masing secara independen sesuai dengan tanggung jawabnya, saatnya melakukan *Pengujian sistem jaringan yang* menjadi satu kesatuan mekanisme kerja *filtering* dan *blocking* . Sistem *filtering* dan *blocking website* untuk menguji kemampuan perangkat lunak dalam melakukan pengenalan halaman web yang tidak boleh diakses.

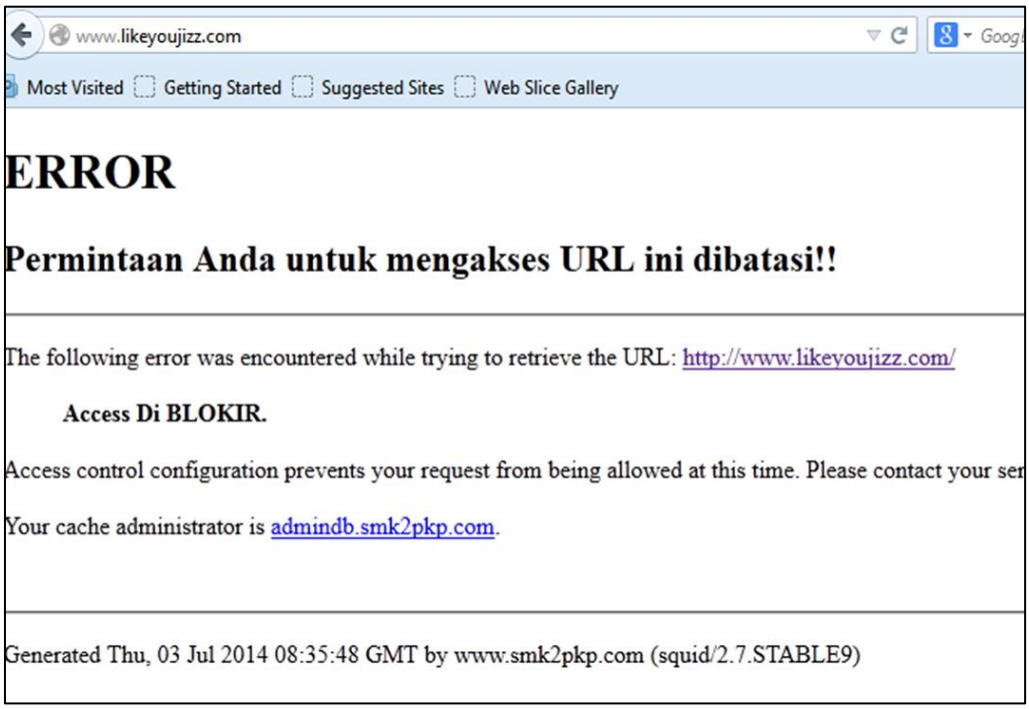
a. Blocking Situs Porno

Pengujian pemblokiran akses URL : **www.youjizz.ws**



Gambar 5.63 *Pemblokiran Akses youjizz.ws*

Pengujian pemblokiran akses URL : **www.likeyoujizz.com**



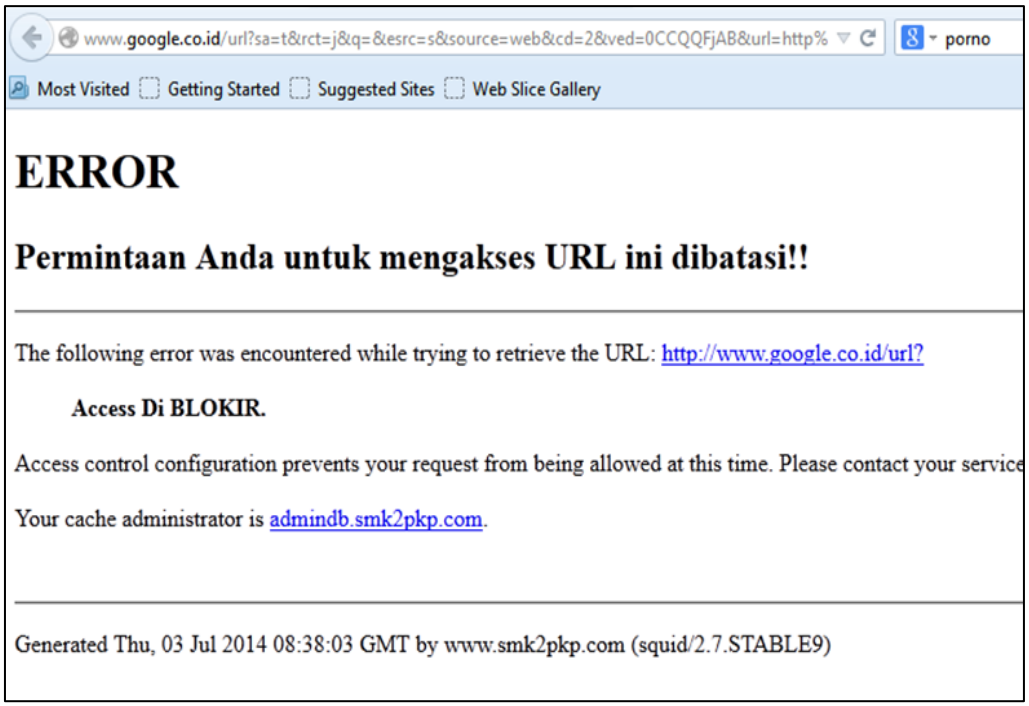
Gambar 5.64 *Pemblokiran akses likeyoujizz.com*

Pengujian pemblokiran akses URL : **www.adultpapa.com**

Gambar 5.65 *Pemblokiran akses www.adultpapa.com*

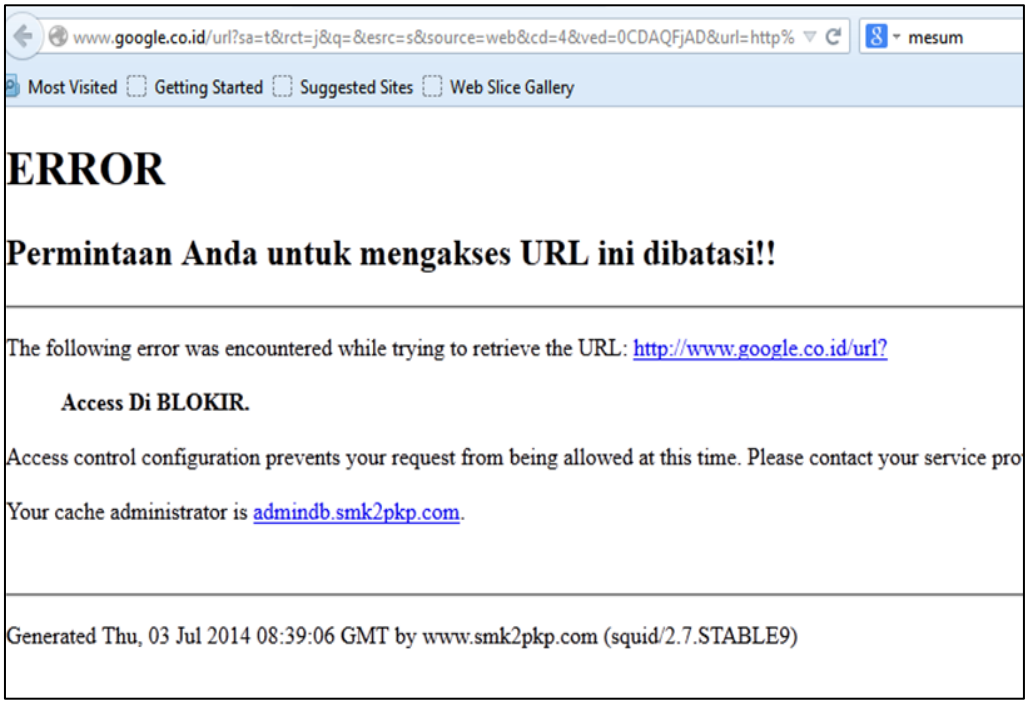
b. Blocking Keyword porno

Pengujian pemblokiran Keyword : **porno**



Gambar 5.66 *Pemblokiran keyword porno*

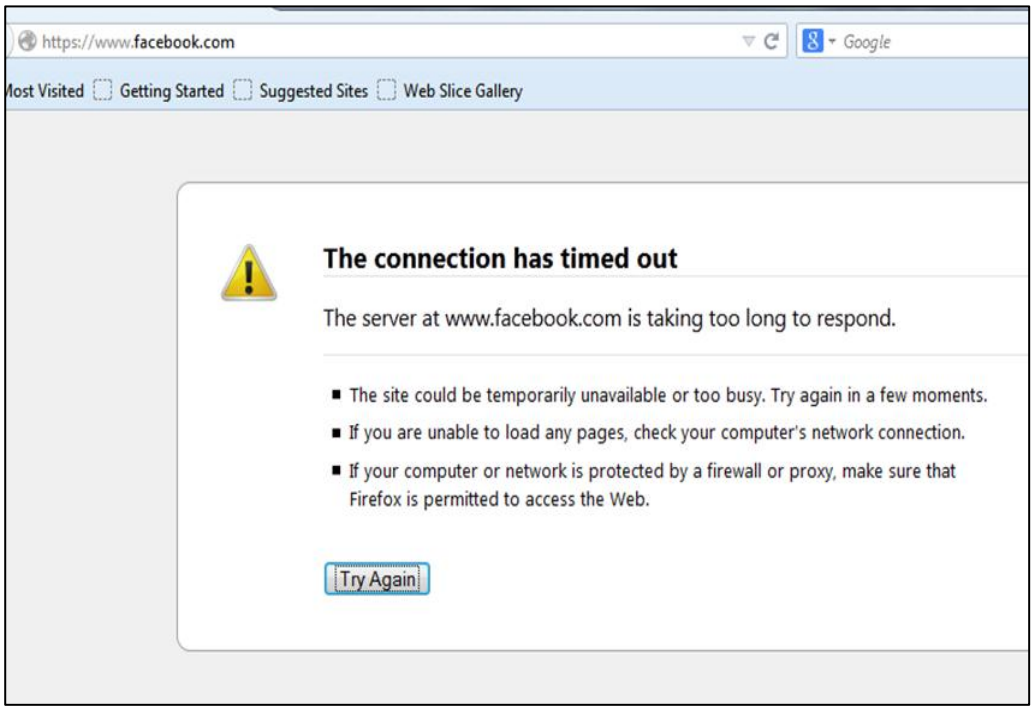
Pengujian pemblokiran Keyword : **mesum**



Gambar 5.67 *Pemblokiran keyword mesum*

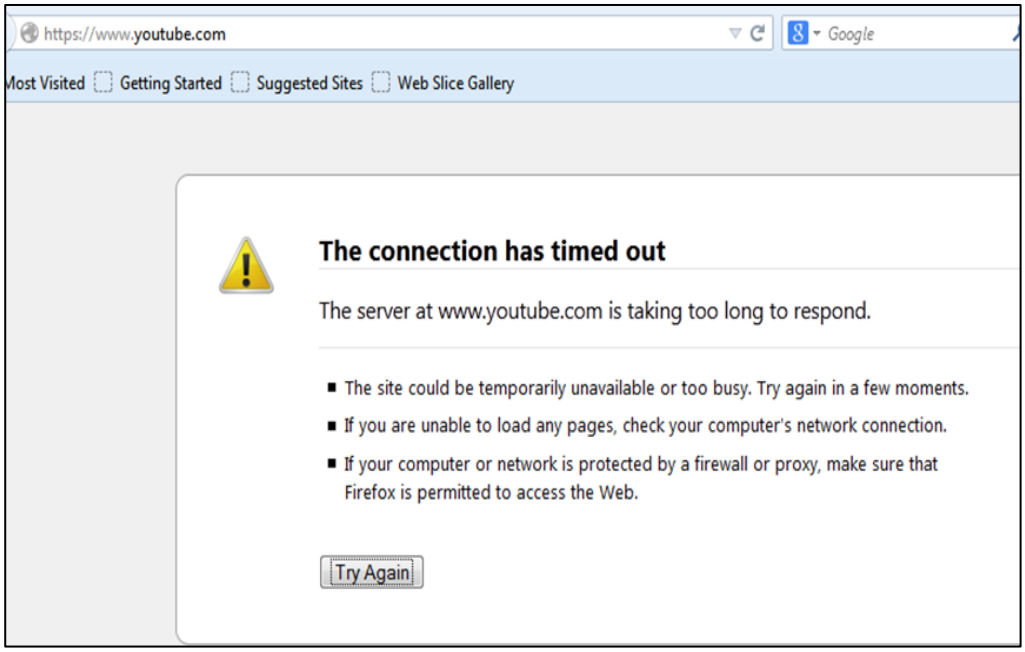
c. Blocking port 443 (https)

Pengujian pemblokiran port 443 (https) : **https://www.facebook.com**



Gambar 5.68 *Pemblokiran Port https facebook.com*

Pengujian pemblokiran port 443 (https) : **https://www.youtube.com**



Gambar 5.69 *Pemblokiran port https youtube.com*

Tabel 5.1 ***Hasil Pengujian filtering dan blocking***

No.	Kategori		Status Filtering
1	Situs Porno	www.youjizz.ws	Success
		www.likeyoujizz.com	Success
		www.adultpapa.com	Success
2	Keyword Porno	Porno	Success
		Porn	Success
		Mesum	Success
		Telanjang	Success
		Bugil	Success
		Sex	Success
		Seks	Success
		Bokep	Success
		Adult	Success
		Hentai	Success
		xxx	Success
3	Port 443 (https)	https://www.facebook.com	Success
		https://www.youtube.com	Success

5.7.2 Sistem Caching

Sistem *Caching* untuk menguji kemampuan cache pada *Proxy Server* dalam penghematan bendwidth. Skenario pengujian cache pada *Proxy Server* sebagai berikut :

a. Client mengakses tiga website yaitu *google.com, yahoo.com* dan *kaskus.co.id*
b. Pengaksesan ketiga website tersebut dilakukan sebanyak 2 kali yaitu sebelum cache menyimpan halaman website yang telah dikunjungi dan setelah cache menyimpan halaman website yang telah dikunjungi oleh satu client.

c. Untuk mengetahui performance cache dapat dilakukan dengan menganalisa perbandingan waktu yang dibutuhkan dalam mengakses website tersebut yaitu sebelum ceching dan setelah caching.

Tabel 5.2 ***Pengujian cache***

No.	Url	Perbandingan kecepatan akses	
		Waktu Sebelum Caching (detik)	Waktu Setelah Caching (detik)
1	www.google.com	16	6
2	www.yahoo.com	20	10
3	www.kaskus.co.id	23	13

5.8 Report Konfigurasi dan Pengujian Sistem

Tabel 5.3 ***Report Instalasi dan Konfigurasi***

No.	Konfigurasi	Tujuan	Skenario	Hasil yang di dapatkan	Ket
1	Install Debian Server	Menginstal Debian Server di PC	Instalasi Menggunakan booting DVD-ROM	Debian Server terinstal di PC	Success
2	Konfigurasi Server	Login ke Server	Masukkan Username dan password	Berhasil login ke Server	Success
3	Konfigurasi Debian Router (Gateway)	Pengalamatan IP Address	Setting IP Add Ethernet, IP Tables, IP Forward	Server Debian mampu menjadi gateway bagi client	Success
4	Konfigurasi DHCP Server	Pengalamatan IP Addres	Setting DHCP3-Server	Server mampu memberikan	Success

		Secara Dynamic		request IP Address client secara otomatis	
5	Konfigurasi DNS Server	Memberikan domain name pada server debian	Setting Bind9	Domain name server dapat terbaca oleh client	Success
6	Konfigurasi Proxy Server	Pembuatan Access Control List	Melakukan pemblokiran situs	Situs dapat diblokir	Success
7	Konfigurasi Proxy Server	Pembuatan cache	Melakukan caching	Mampu melakukan caching pada situs yang telah ditentukan	Success
8	Konfigurasi Firewall	Mengalihkan akses port http ke proxy	Setting IP tables	Server mampu mengalihkan akses port http ke proxy	Success
9	Konfigurasi Firewall	Blocking port https	Setting IP tables	Port Https dapat diblokir	Success

Tabel 5.4 ***Report Pengujian Sistem Jaringan***

No.	Pengujian	Tujuan	Skenario	Hasil yang di dapatkan	Ket
1	Pengujian blocking/situs yang tidak diijinkan	Mengetahui apakah situs tidak diijinkan	Memasukkan atau mengetik situs yang tidak diijinkan	Tidak diijinkan terakses maka situs didirec ke situs peringatan/ pemberitahuan	Success

2	Pengujian blocking/ keyword yang tidak diijinkan	Mengetahui apakah keyword tidak diijinkan	Memasukkan atau mengetik keyword yang tidak diijinkan	Tidak diijinkan terakses maka situs didirec ke situs peringatan/ pemberitahuan	Success
3	Pengujian Pemblokiran Https	Mengetahui apakah pemblokiran https berjalan dengan baik	Mengakses https seperti facebook.com dan youtube.com	Https tidak diijinkan diakses	Success
4	Pengujian cache	Mengetahui apakah proses caching berjalan dengan baik	Mengakses situs dan membandingkan kecapatan akses	Proses Caching berjalan dengan baik	Success

5.9 Kesimpulan

Setelah melakukan penelitian dalam membangun server proxy menggunakan linux debian squeeze dan pengujian pada jaringan SMK Negeri 2 Pangkalpinang maka dapat diambil kesimpulan sebagai berikut :

a. Penggunaan linux sebagai sistem operasi server merupakan sistem operasi yang cukup handal untuk memenuhi kebutuhan dalam menyediakan layanan server proxy.
b. Server proxy sebagai filtering konten merupakan server proxy yang dapat melakukan pemblokiran alamat website ataupun *content* kata domain.
c. Dari hasil pengujian yang dilakukan server proxy adalah sistem sangat efektif dalam melakukan filtering /pembatasan akses.

d. Website https atau website yang menggunakan port 443 dapat dilakukan pemblokiran menggunakan firewall yaitu dengan cara menolak request akses client yang masuk ke firewall.
e. Proxy server dapat mempersingkat waktu pengakasesan data karena request yang sama dari client tidak perlu diteruskan ke server internet penyedia data, sebab proxy server sudah mengcopi histori dari halaman website yang telah diakses sebelumnya.
f. Biaya membangun server proxy dengan menggunakan sistem operasi linux mempunyai harga yang relatif murah.

5.10 Saran

Berdasarkan kesimpulan hasil dari penelitian tersebut diatas, maka dapat disarankan kepada SMK Negeri 2 Pangkalpinang sebagai berikut :

a. Sistem jaringan ini agar segera di implementasikan pada jaringan SMK Negeri 2 Pangkalpinang.
b. Memperbanyak daftar situs yang diblokir mengingat baru beberapa situs saja yang diblokir pada penelitian ini serta membatasi siswa pada akses yang berkonten negatif.
c. Pembangunan server proxy ini dapat dikembangkan lebih lanjut dengan menerapkan beberapa metode-metode lain dan baru sehingga penulis mengharapkan adanya pihak lain yang akan tetap melakukan dan melanjutkan penelitian ini untuk mendapatkan hasil yang lebih baik lagi.