Mahir Administrasi Server dan Router dengan Linux Ubuntu 12.04 LTS

Panduan Lengkap

Oleh : Rizal Rahman

Untuk kedua orang tua saya tercinta, guru-guru dan pembimbing yang telah mengajarkan segala ilmunya kepada saya, Mas Wiwin yang memperkenalkan saya betapa indahnya Linux itu, Kak Ali orang yang pertama kali mengajari saya administrasi jaringan di Linux secara privat, untuk Arina Rahmatya yang selalu menjadi sumber motivasi saya untuk menyelesaikan buku ini :), tutorial-tutorial dari teman saya Malsasa sehingga saya mampu membuat cover buku saya sendiri, teman-teman seperjuangan, CILSY, FUI, serta seluruh pengguna Linux & Open Source di Indonesia.....

Kata Pengantar

Bismillahirahmanirahim. Sebuah kata yang tepat untuk memulai awal dari semua tulisan saya di buku ini. Ini adalah buku pertama saya yang sepenuhnya tidak akan pernah ada tanpa dukungan dari orang-orang terdekat saya yang selalu mensupport saya dalam segala kekurangan dan kemalasan saya. *You're rock guys!* :)

Lalu apa saja yang ada di dalam buku ini ? **Mahir Administrasi Server dan Router dengan Linux Ubuntu Server 12.04 LTS** merupakan buku panduan (lebih kepada tutorial) yang akan membahas tentang cara-cara penginstalan, konfigurasi, serta praktek mengadministrasi server dan router jaringan berbasiskan Sistem Operasi Ubuntu Server 12.04 LTS. Kenapa harus Ubuntu ? Jelas, satu faktor utama yang saya tekankan disini adalah karena Ubuntu merupakan sistem operasi Linux yang telah terbukti handal dan stabil dalam bidang jaringan. Oleh karena itu, tentulah tepat bagi kalian yang ingin bekerja sebagai *System Administrator* di masa depan atau seorang pemula yang ingin menguasai ilmu administrasi server jaringan untuk memilih buku ini sebagai panduan.

Sasaran utama buku ini sebenarnya adalah untuk kalangan pelajar SMA/SMK hingga Perguruan Tinggi khususnya jurusan Komputer Jaringan maupun Teknik Informatika yang ingin mempelajari ilmu administrasi jaringan secara lebih dalam, namun tidak menutup kemungkinan untuk dipelajari juga oleh seorang pemula. Tapi tetap, walaupun di buku ini dibahas sekilas mengenai jaringan dan Linux, akan jauh lebih baik jika kalian sudah mengerti atau setidaknya tahu tentang dasar-dasar jaringan dan perintah-perintah dasar CLI (*Command Line Interfaces*) di Linux.

Akhir kata, saya hanyalah seorang penulis biasa yang sadar akan seluruh kekurangan yang ada di buku ini. Seluruh saran dan kritik dari kalian sangatlah berharga bagi saya demi kebaikan buku ini. Walau begitu, Saya harapkan buku ini tetap dapat membantu siapapun yang membacanya sebagai referensi serta panduan dalam menguasai administrasi server dan router dengan Linux yang hebat itu.

Bekasi, Juli 2013

Penulis

Lisensi

Daftar Isi

Bab 1. Pendahuluan

1.1. Sekilas Jaringan Komputer

Jaringan komputer menurut bahasa populer dapat diartikan sebagai sekumpulan komputer maupun perangkat lain (printer, scanner, hub, dsb) yang saling terhubung satu sama lain melalui media perantara. Media perantara tersebut bisa berupa kabel maupun nirkabel (wireless).

Jaringan komputer sendiri merupakan salah satu bentuk komunikasi antar komputer layaknya yang dilakukan oleh manusia disaat berkomunikasi. Manfaat dari jaringan komputer sangatlah banyak, beberapa contohnya adalah dapat lebih menghemat biaya, lebih hemat dalam penggunaan sumber daya, serta dapat berbagi penggunaan internet.

1.1.a. Sejarah Jaringan

Dahulu komunikasi yang melibatkan komputer masih dilakukan secara manual dengan manusia sebagai media komunikasinya yaitu dengan manusianya sendiri yang membawa instruksi-instruksi antar komputer. Hingga akhirnya George Stibitz pada akhir tahun 1940-an sukses memanfaatkan sebuah mesin teletype untuk mengirimkan pesan instruksi dari komputernya ke komputer lain. Maju lagi hingga tahun 1964 dimana metode sistem Time Sharing System mulai gencar digarap. Kemudian di tahun 1969 UCLA (University of California at Los Angeles), SRI (Stanford Research Institute), University of California at Santa Barbara, dan University of Utah berhasil menerapkan jaringan komputer dan mulai berhubungan menggunakan jaringan ARPAnet.

Jaringan komputer terus berkembang begitu cepat dari masa ke masa. Bahkan ada yang mengatakan bahwa perkembangan dunia jaringan komputer itu sama cepatnya seperti saat kita terjun bebas di udara. Dan kini, jaringan komputer sudah menjadi bagian penting dalam kehidupan, penggunanya pun sudah mencapai ratusan juta pengguna dari berbagai kalangan dan usia. Setiap orang selalu menggunakan jaringan komputer tiap harinya. Lihat saja, saat ini siapa yang tidak mempunyai telepon genggam? Warnet dan hotspot-hotspot juga sudah bukan merupakan barang langka lagi. Segalanya menjadi mudah sekarang. Telepon, Internet, chatting, hingga video call pun sudah bukan hal mewah lagi. Semua ini tidak akan terjadi, jika tidak ada yang namanya jaringan komputer.

1.1.b. Jenis-Jenis Jaringan

Jaringan terdefinisi menjadi 3 jenis yaitu jaringan berdasarkan fungsi, jaringan berdasarkan media transmisi, dan jaringan berdasarkan area.

1.1.b.1. Berdasarkan fungsi

Jaringan berdasarkan fungsinya dibedakan menjadi 2, yaitu :

- *Client – Server*

  Client – Server adalah jaringan komputer yang salah satu komputernya berperan sebagai server yang bertugas menyediakan layanan kepada komputer pengguna atau client. Layanan yang disediakan server dapat bermacam-macam, bisa berupa *web server, storage server, mail server*, dll.

- *Peer to Peer*

  Peer to Peer adalah jaringan komputer dimana tiap komputer sama-sama dapat berperan sebagai server maupun client. Jaringan Peer to Peer ini paling sering digunakan di dalam jaringan LAN.

1.1.b.2. Berdasarkan media transmisi

Jaringan berdasarkan media transmisi dibagi menjadi 2, yaitu :

- *Wired Network (kabel)*

  Wired Network menggunakan media kabel sebagai penghantarnya. Kabel yang biasa digunakan adalah kabel UTP, Coaxial, ataupun Fiber Optik. Kelebihan utama dari Wired Network ini adalah kecepatan transmisi data yang jauh lebih cepat dibandingkan dengan Wireless Network.

- *Wireless Network (nirkabel)*

  Wireless Network menggunakan media gelombang radio, Infra Red, atau bluetooth sebagai media penghantarnya. Salah satu penerapan Wireless Network adalah area internet gratis dengan menggunakan Wi-Fi atau biasa disebut Hotspot. Yang teranyar adalah penerapan hotspot sebagai RT/RW Net.

1.1.b.3. Berdasarkan area

Jaringan komputer berdasarkan area dibagi menjadi 4, yaitu :

- LAN (Local Area Network)

  Local Area Network adalah jaringan lokal yang biasanya diimplementasikan di lingkungan rumahan atau perkantoran bertujuan untuk berbagi data dan resource seperti printer dan scanner secara bersama.

- MAN (Metropolitan Area Network)

  Secara teknis MAN tidak ada bedanya dengan LAN, hanya saja cakupan areanya yang lebih luas. MAN bisa mencakup daerah antar gedung, antar RT, hingga antar kota.
- WAN (Wide Area Network)

  WAN juga sebenarnya tidak jauh berbeda dengan LAN dan MAN, tetapi WAN bisa mencakup daerah antar negara hingga antar benua.
- Internet

  Internet merupakan jaringan global yang paling luas dan dapat mencakup seluruh dunia, bahkan antar planet.

1.1.c. TCP/IP

Apa itu TCP/IP ? TCP/IP atau *Transmission Control Protocol and Internet Protocol* adalah sebuah aturan standar yang digunakan untuk komunikasi antar berbagai jenis komputer yang terhubung dalam sebuah jaringan komputer. Aturan ini ditetapkan oleh Defense Advanced Research Projects Agency (DARPA) yang dikembangkan pada akhir tahun 1970-an.

Kenapa harus ada aturan standar seperti ini ? Menurut pendapat saya, bila diibaratkan dalam dunia manusia, TCP/IP itu adalah sebuah bahasa internasional yang digunakan untuk berkomunikasi antar manusia. Misalnya saja ada orang Indonesia yang bertemu dengan orang Jepang dan orang Rusia. Jika mereka bertiga bertemu tetapi berkomunikasi dengan bahasa mereka masing-masing tentunya mereka bertiga tidak akan mengerti satu sama lain bukan ? Oleh karena itu mereka bertiga harus berkomunikasi menggunakan bahasa Inggris atau bahasa Internasional seperti yang telah ditetapkan agar mereka bisa saling mengerti. Sama halnya dengan komputer. Komputer dibuat oleh berbagai macam vendor perangkat keras yang berbeda-beda di seluruh dunia. Komputer-komputer tersebut juga memiliki caranya sendiri-sendiri untuk saling berkomunikasi. Nah disinilah protokol TCP/IP berperan sehingga komputer-komputer yang ada diseluruh dunia dapat berkomunikasi seperti saat ini. Di dunia Internet pun protokol TCP/IP selalu digunakan, sehingga protokol ini sangat terkenal.

Secara umum, komponen dari TCP/IP adalah sebagai berikut :

- IP address

  IP address merupakan sebuah kombinasi unik yang dituliskan dalam angka desimal yang dibagi dalam empat segmen. Tiap-tiap segmen tersebut mewakili 8 bit dari alamat yang memiliki panjang 32 bit untuk keseluruhannya. Fungsi dari IP address sendiri merupakan identifikasi setiap *host* pada jaringan.
- Netmask

Netmask atau Subnet Mask berfungsi menunjukkan berapa pembagian panjang bit nework dengan bit host untuk mengetahui berapa jumlah host yang dapat terkoneksi didalam sebuah network.. Misalnya untuk kategori alamat IP kelas C dengan netmask 255.255.255.0, maka penentuannya adalah 24 bit pertama adalah bit network dan 8 bit sisanya adalah bit host.

- Network Address

  Sebuah host tidak pernah berdiri sendiri namun memerlukan host lain dan bergabung membentuk sebuah Network. Alamat Network yang terbentuk inilah yang disebut sebagai Network Address. Network address didapat dengan membuat seluruh bit host menjadi 0. Misalnya ip address 192.168.1.1 dengan alamat IP kelas C, maka Network Addressnya adalah 192.168.1.0.

- Broadcast Address

  Broadcast Address adalah alamat dimana agar semua host yang berada di dalam sebuah network dapat dikirimkan data secara simultan. Gunanya agar apabila ada sebuah host yang ingin mengirimkan data ke seluruh host yang ada di suatu jaringan tertentu, maka host tersebut tidak perlu membuat replika datagram sebanyak jumlah host tujuan karena hal secamam ini akan meningkatkan pemakaian bandwidth dan beban kerja host pengirim. Jadi host pengirim cukup mengirimkan data ke alamat broadcast saja maka secara otomatis seluruh host yang ada di satu network tersebut akan menerimanya. Broadcast Address didapat dengan membuat bit host menjadi 1 (kebalikan dari Network Address), jadi misalnya IP addressnya adalah 192.168.1.1, maka Broadcast Addressnya adalah 192.168.1.255.

- Gateway Address

  Gateway adalah alamat IP yang menghubungkan sebuah jaringan dengan jaringan yang lain. Jadi apabila sebuah host ingin berkomunikasi dengan host lain dalam sebuah jaringan yang berbeda, maka host tersebut harus melewati Gateway Address terlebih dahulu untuk mencapai host yang satunya.

- Nameserver Address

  Nameserver Address adalah IP milik sebuah server Domain Name Service (DNS) yang bertujuan untuk menerjemahkan sebuah domain menjadi IP address maupun sebaliknya.

Sampai sini saya harapkan setidaknya kalian sudah mulai sedikit mengerti dasar-dasar mengenai jaringan komputer. Dari sejarah jaringan, jenis-jenis jaringan seperti apa, perangkat-perangkat jaringan yang digunakan itu seperti apa, hingga TCP/IP. Walaupun begitu, materi dasar jaringan

yang dibahas disini sangat sedikit sekali dan masih kurang lengkap, jadi saya sarankan bagi kalian untuk mencari bahan referensi buku lain yang membahas dasar-dasar jaringan secara lebih rinci dan lebih jelas.

1.2. Pengenalan Linux & Ubuntu

Mungkin selama ini sistem operasi yang paling awam digunakan oleh mayoritas bangsa Indonesia adalah sistem operasi berbasis Windows atau mungkin segelintir orang lainnya dengan sitem operasi Mac OS-nya. Kedua sistem operasi tersebut memang sudah tidak dapat diragukan lagi jika menilik dari lingkungan kerja Desktop. Lalu bagaimana jika kita berbicara soal jaringan ? Sudah tentu Linux jawabannya. Linux terbukti sebagai sistem operasi yang handal, stabil, dan paling aman untuk masalah jaringan. Selain itu Linux adalah sistem operasi yang gratis karena berbasiskan Open Source. Masih banyak kelebihan-kelebihan lain dari sistem operasi Linux yang membuat Linux menjadi pilihan paling tepat untuk dijadikan sebuah komputer server.

1.2.a. Apa itu Linux ?

Gambar 1.2.a.1
Tux (Logo Linux)

Linux (Linux Is Not Unix) adalah sebuah kernel dari sistem operasi UNIX-like berbasis Open Source yang dibuat oleh seorang mahasiswa bernama Linux Torvalds pada sekitar awal tahun 90-an. Sebenarnya ada sedikit salah persepsi di kalangan masyarakat terhadap Linux. Linux sebenarnya bukanlah sebuah sistem operasi layaknya Windows atau Mac OS. Karena apa? karena Linux memang hanyalah sebuah *kernel*. Jadi Linux itu ya hanya inti dari sistem operasinya saja. Ibarat manusia, Linux itu hanyalah roh dari jasad manusia tersebut. Baru setelah muncul seorang bernama Richard Stallman dengan proyek GNU (GNU's Not Unix) miliknya, dimana GNU ini adalah kumpulan dari tools-tools, libraries, dan aplikasi, yang kemudian digabungkan dengan kernel atau inti sistem operasi bernama Linux tadi. Sehingga akhirnya jadilah sebuah sistem operasi yang terkenal powerful dan handal di masa yang akan datang bernama GNU/Linux.

1.2.b. Apa itu Ubuntu ?

Gambar 1.2.b.1
Logo Ubuntu

Ubuntu merupakan sistem operasi berbasis GNU/Linux turunan dari distro *Debian* yang sangat mudah digunakan, handal, stabil dan aman. Ubuntu berasal dari filosofi Afrika yang berarti "Kemanusiaan kepada sesama". Ubuntu didesain untuk kepentingan penggunaan personal, namun tersedia juga untuk versi server serperti Ubuntu server 12.04 LTS yang akan digunakan di buku ini. Rilis pertama Ubuntu adalah Ubuntu 4.10 pada tahun 2004 dengan *codename* Warty Warthog. Mark Shuttleworth adalah tokoh dibalik dari kesuksesan Ubuntu hingga Ubuntu bisa terkenal seperti saat ini. Ia adalah pendiri dari perusahaan Cannonical, Ltd yang merupakan perusahan resmi pensupport Ubuntu.

1.2.c. Apa itu Ubuntu 12.04 LTS?

Ubuntu 12.04 LTS sendiri adalah rilis Ubuntu yang ke 16 dan merupakan seri Long Term Support atau LTS yang ke 4. Apa itu Long Term Support ? LTS adalah versi Ubuntu yang disupport lebih lama dari versi-versi Ubuntu yang biasa yaitu 4 tahun untuk versi Desktop dan 5 tahun untuk versi Server. Namun pada Ubuntu 12.04 ini, seri LTS akan sama-sama disupport selama 5 tahun baik itu untuk versi Desktop maupun Server. Seri LTS lebih ditujukan untuk kehandalan dan kestabilan sistem, sehingga sangat cocok digunakan untuk komputer server.

1.2.d. Apa bedanya Linux, GNU/Linux, dan Ubuntu ?

Lalu apa bedanya Linux, GNU/Linux, dan Ubuntu ? Seperti yang sudah saya jelaskan di subbab *Apa itu Linux ?*, Linux hanyalah sebuah kernel dari sistem operasi, sedangkan GNU/Linux adalah gabungan dari tools-tools, libraries, dan aplikasi GNU dengan kernel Linux sehingga menjadi sebuah sistem operasi. Lalu Ubuntu sendiri adalah distribusi atau lebih dikenal sebagai distro dari GNU/Linux. Lebih tepatnya Ubuntu adalah gabungan dari sistem operasi GNU/Linux dengan ditambah beberapa paket-paket aplikasi, tema, dan beberapa modifikasi lainnya sehingga jadilah sistem operasi baru atau distro baru bernama Ubuntu.

1.2.e. Mengapa Harus Ubuntu ?

Distro-distro GNU/Linux sangatlah banyak, seperti RedHat, Fedora, CentOS, Debian, Slackware, dan lain-lain. Tapi Ubuntu saya pilih karena beberapa faktor berikut :

- Karena Ubuntu adalah salah satu distro Linux yang free, bebas virus, dan powerful di bidang jaringan.
- Ubuntu merupakan distro nomor satu di Indonesia, dan nomor dua setelah Linux Mint di dunia menurut survey distrowatch.com
- Banyak support dari komunitas-komunitas Ubuntu di seluruh dunia.
- Banyak tutorial-tutorial tentang server berbasis Ubuntu di internet
- Ubuntu 12.04 merupakan seri Long Term Support.

Bab 2. Instalasi Ubuntu Server 12.04 LTS

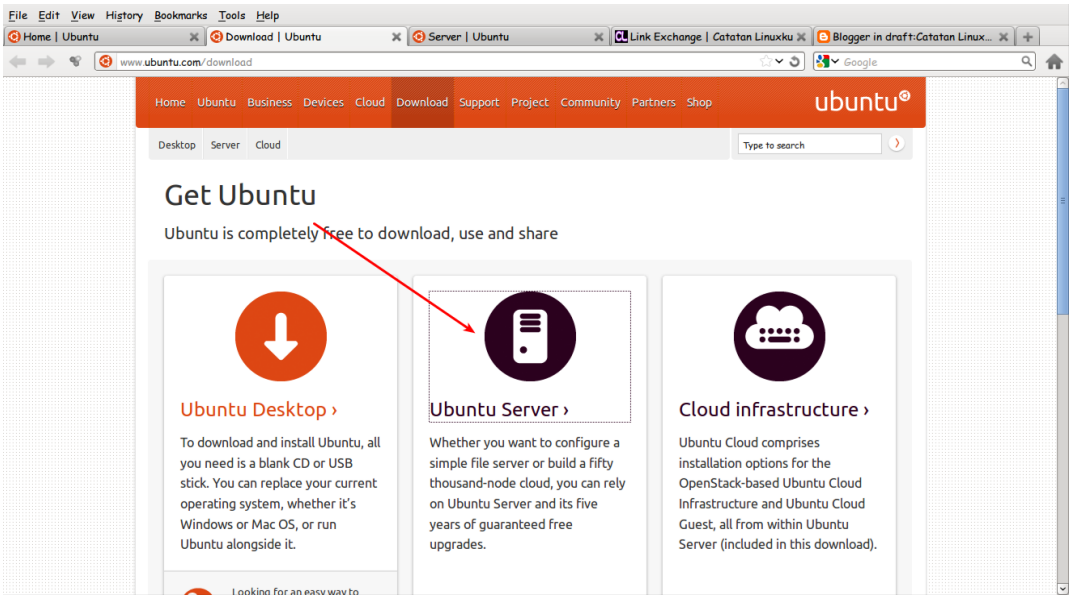
2.1. Persiapan Instalasi

Pada bab ini kita akan mempraktekkan bagaimana cara menginstalasi sistem operasi Ubuntu Server 12.04 LTS di mesin kalian. Tapi ada beberapa hal teknis yang perlu kalian ketahui sebelum melakukan instalasi.

2.1.a. Mendapatkan CD Instaler dan DVD Repositori Ubuntu

Sebelum melakukan instalasi, tentunya kalian harus memiliki CD installer dari Ubuntu itu sendiri. Ada beberapa cara untuk mendapatkan CD Ubuntu Server 12.04 LTS, salah satunya adalah dengan mendownload langsung file image/iso dari situs resmi Ubuntu. Nantinya file iso ini dapat kalian burning ke dalam bentuk CD.

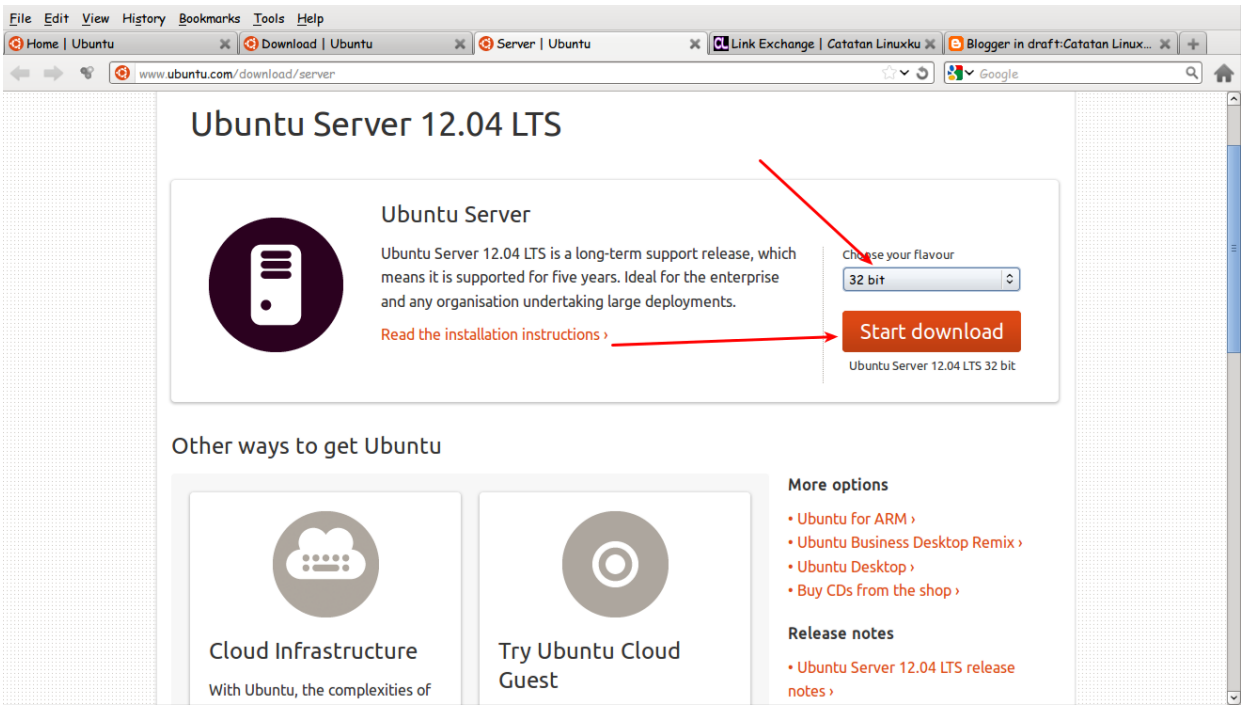
1. Arahkan browser kalian ke http://www.ubuntu.com/download. Kemudian klik **Ubuntu Server**.



Gambar 2.1.a.1

2. Setelah itu terserah kalian ingin pilih Ubuntu yang versi 32 bit atau 64 bit, lalu klik **Start**

Download

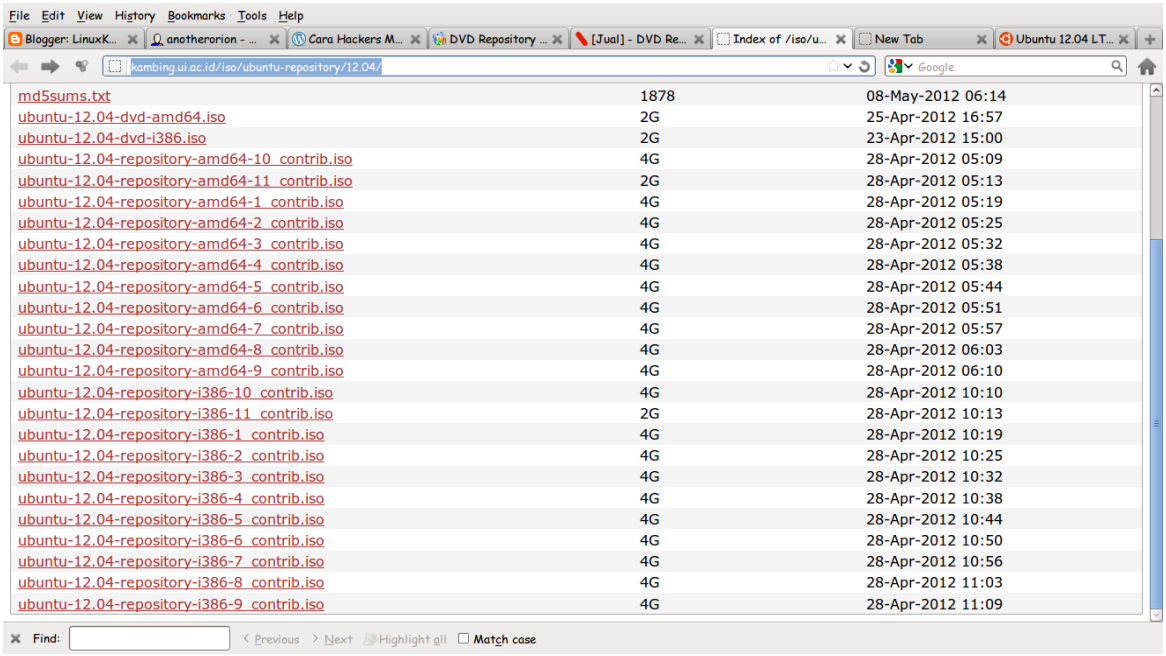


Gambar 2.1.a.2

3. Tunggu hingga proses download selesai. Karena ukuran filenya cukup besar yaitu sekitar 700MB, maka untuk masalah lama tidaknya, tergantung kecepatan internet kalian masing-masing. Kemudian setelah download selesai, kalian tinggal mem*burning* iso tersebut ke dalam bentuk CD.

Setelah mendapatkan CD installer Ubuntu server 12.04, saya menyarankan kalian untuk juga memiliki DVD repositori Ubuntu server 12.04. Untuk apa? DVD Repositori ini gunanya untuk menginstall paket-paket aplikasi yang kalian butuhkan untuk praktek nanti. Intinya DVD repository merupakan kumpulan paket-paket dari repositori Ubuntu yang dikemas dan didistribusikan dalam bentuk media DVD. Jadi nanti kalian tidak membutuhkan lagi koneksi internet untuk menginstall aplikasi-aplikasi yang kalian perlukan, cukup menggunakan DVD repositori saja. Tapi apabila kalian memang sudah memiliki koneksi internet, dan merasa sudah paham untuk menginstall aplikasi melalui internet, maka kalian boleh melewatkan bagian ini.

Ada 2 cara untuk mendapatkan DVD repositori Ubuntu server 12.04. Yang pertama adalah dengan cara mendownloadnya. Tetapi harus saya ingatkan bahwa ukuran filenya sangat besar yaitu total kira-kira 47 GB yang dibagi kedalam 11 DVD. Kalian bisa mendownloadnya di situs lokal kambing.ui yaitu di http://kambing.ui.ac.id/iso/ubuntu-repository/12.04/ . Pilih iso yang *amd* atau *i386* sesuai dengan spesifikasi hardware kalian masing-masing.



Gambar 2.1.a.3

Nah, apabila kalian miskin bandwidth atau memang malas mendownload, maka kalian bisa memilih cara yang kedua, yaitu dengan membeli DVD repositorinya di situs-situs atau toko yang menjual DVD repositori. Salah satu situs terpercaya yang menjual DVD repositori adalah www.gudanglinux.com. Disana kalian dapat memesan DVD-DVD repositori dan diantar dengan biaya yang telah ditentukan. Atau kalian juga dapat mendatangi langsung toko gudanglinux yang tersebar di berbagai tempat, salah satunya adalah di *Jl. Prof Dr Satrio - Ambasador Megablok ITCenter Kuningan SemiDasar B1/21, Jakarta*.

2.1.b. Spesifikasi Minimum Hardware

Jika kalian sudah memiliki CD installer dan repositori, hal yang perlu kalian perhatikan berikutnya adalah berapa spesifikasi minimum hardware yang dibutuhkan untuk menginstall Ubuntu Server 12.04 LTS. Sebenarnya, komputer jadul pentium 2 pun bisa diinstallkan Ubuntu Server karena resource memory yang dibutuhkan untuk OS yang berbasis CLI (Command Line Interfaces) memang kecil sekali. Ini didukung pula jika kita melihat dari situs resminya langsung di https://help.ubuntu.com/community/Installation/SystemRequirements :

Ubuntu Server (CLI) Installation

- 300 MHz x86 processor
- 128 MiB of system memory (RAM)
- 1 GB of disk space
- Graphics card and monitor capable of 640x480

- CD drive

Tapi jika kalian menginginkan performa yang baik, saya sarankan untuk menggunakan komputer dengan spesifikasi lebih tinggi dari kebutuhan minimum diatas. Karena tentunya kalian pasti tidak menginginkan komputer server kalian kinerjanya buruk atau *lemot* bukan?

2.1.c. Sedikit Pengetahuan Tentang Linux

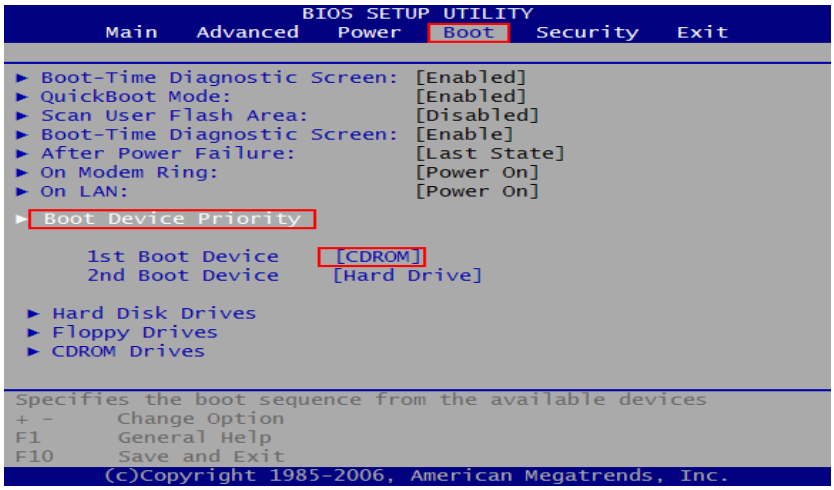
Setelah mempunyai iso, sudah mengetahui spesifikasi minimum instalasi, komputer pun telah siap untuk diinstall, ada satu hal terakhir yang perlu kalian perhatikan juga. Yaitu sedikit pengetahuan tentang Linux. Mengapa ini penting? Karena pada buku ini saya tidak akan membahas tentang perintah-perintah dasar terminal pada sistem operasi Linux. Sedangkan kalian nantinya harus selalu bekerja pada mode teks. Jadi perintah-perintah dasar semacam *cp*, *mv*, *cd*, *nano*, dll, seharusnya sudah bukan hal asing lagi bagi kalian.

Saya sarankan agar kalian mencari-cari referensi terlebih dahulu di Internet mengenai sistem operasi Linux atau Ubuntu beserta perintah-perintah dasar terminalnya. Saya rasa ebook-ebook yang membahas mengenai itu sudah banyak sekali.

2.2. Tahapan Instalasi

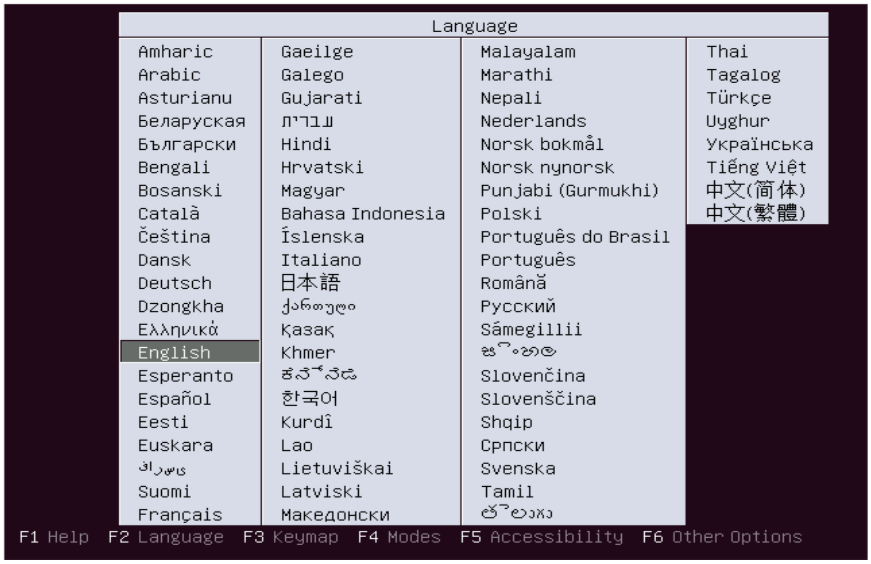
Setelah CD Ubuntu 12.04 LTS sudah ditangan, saatnya kalian untuk menginstall Ubuntu ke dalam komputer. Berikut langkah-langkahnya :

1. Nyalakan komputer kalian, kemudian masuklah ke mode *BIOS Setup Utility* dengan menekan tombol **DEL**, **F2**, atau **F10** tergantung dari merek BIOS komputer kalian masing-masing.



Gambar 2.2.1

2. Untuk dapat booting melalui media CD, aturlah agar pengaturan **First Boot Device** menjadi CD-ROM di bagian **Boot Device Priority**.
3. Tekan **F10** untuk menyimpan pengaturan dan keluar dari mode BIOS, lalu komputer akan restart sendiri dan terlihat menu awal instalasi seperti gambar dibawah. Pilih saja **English** untuk bahasa menu instalasi.

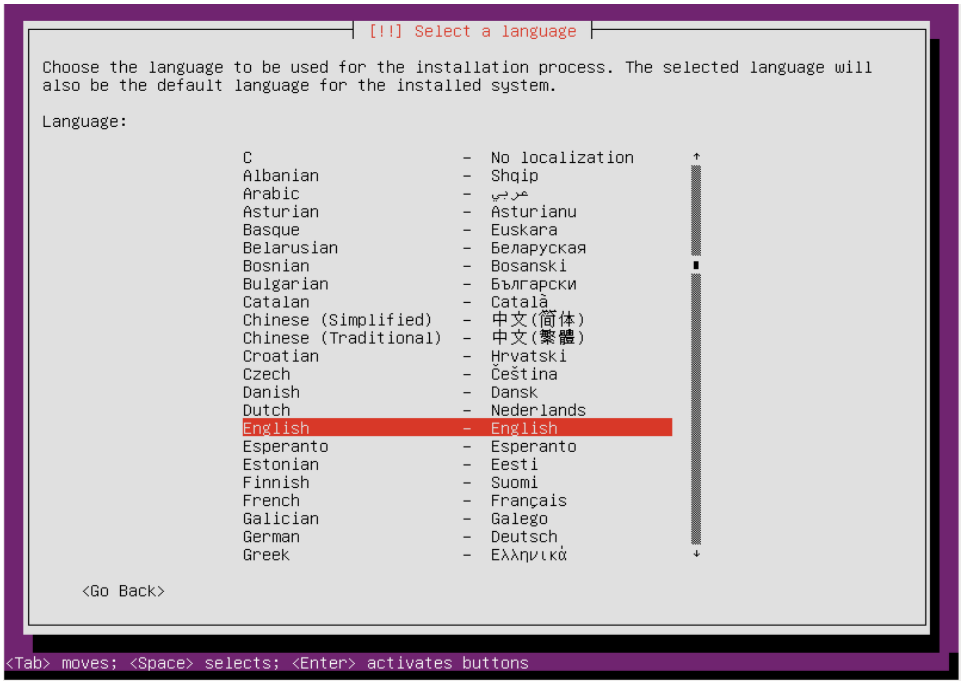


Gambar 2.2.2

4. Setelah itu pilih **Install Ubuntu Server** untuk memulai instalasi.

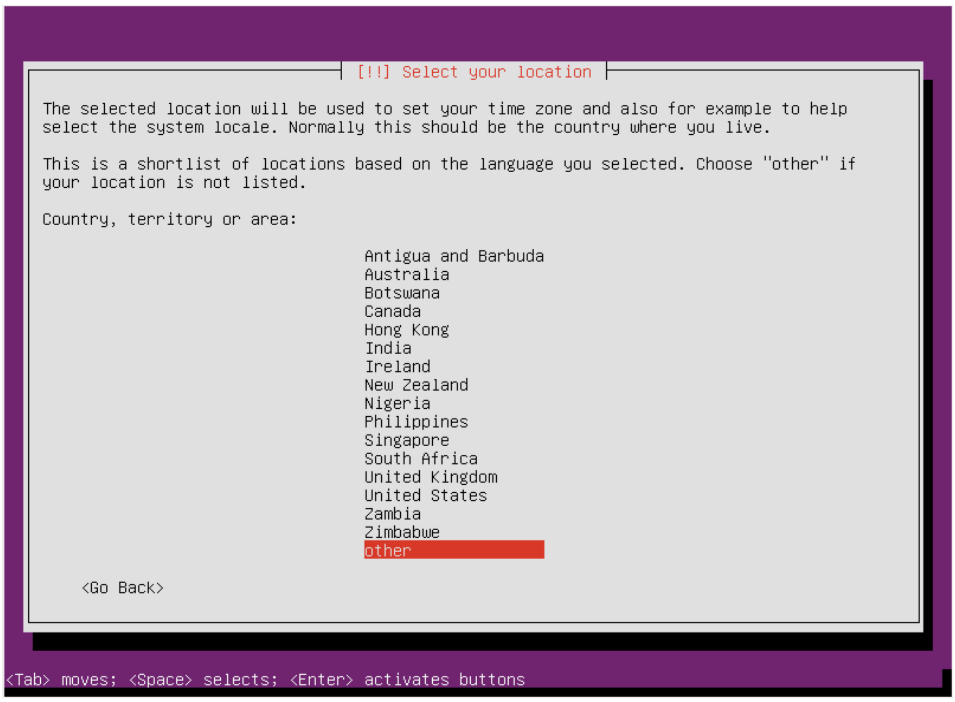
Gambar 2.2.3

5. Muncul tampilan untuk pemilihan bahasa selama proses instalasi, pilih saja **English** kemudian tekan **enter**.

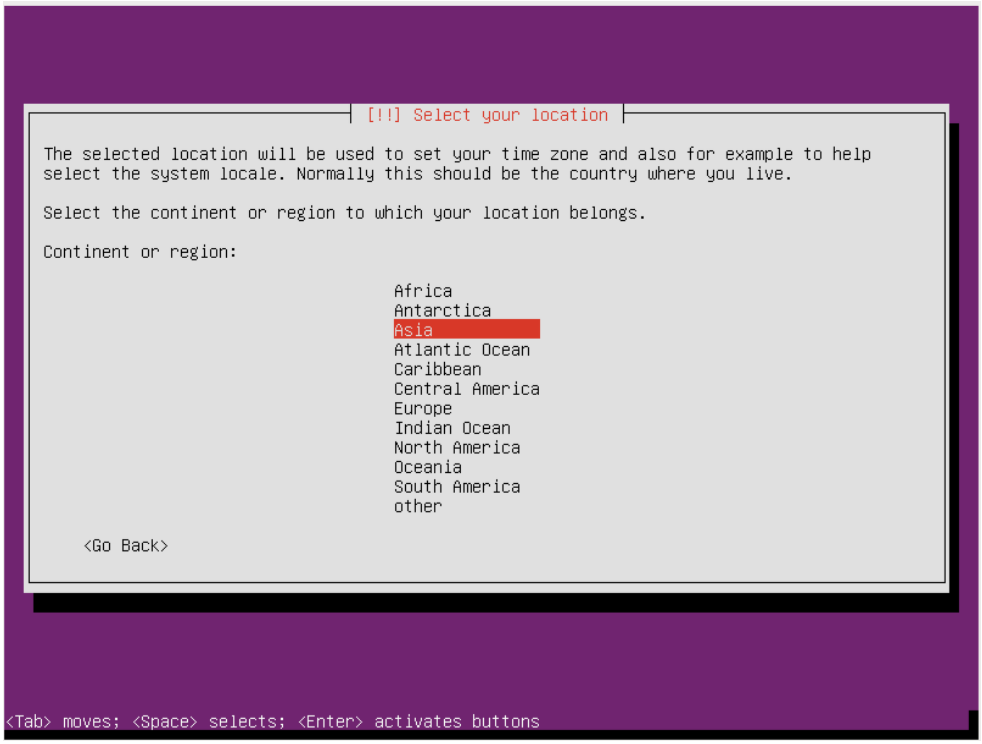


Gambar 2.2.4

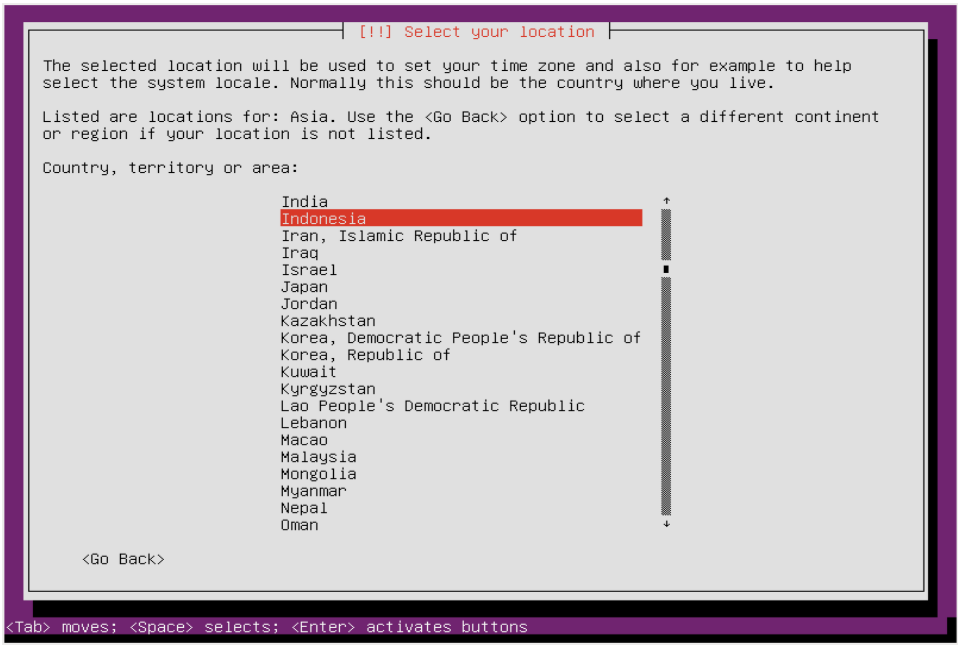
6. Setelah itu akan muncul tampilan untuk pemilihan lokasi. Berhubung kalian berada di Indonesia, maka pilih **Other** kemudian pilih **Asia**, lalu terakhir pilih **Indonesia**. Lihat *Gambar 2.2.5*, *Gambar 2.2.6* dan *Gambar 2.2.7*.



Gambar 2.2.5

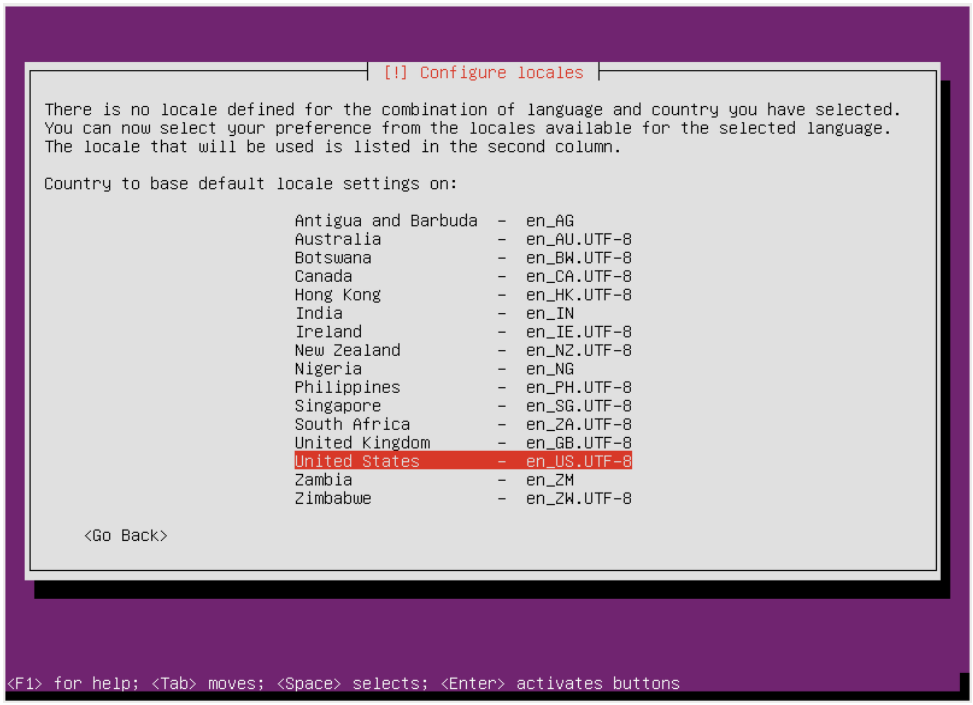


Gambar 2.2.6



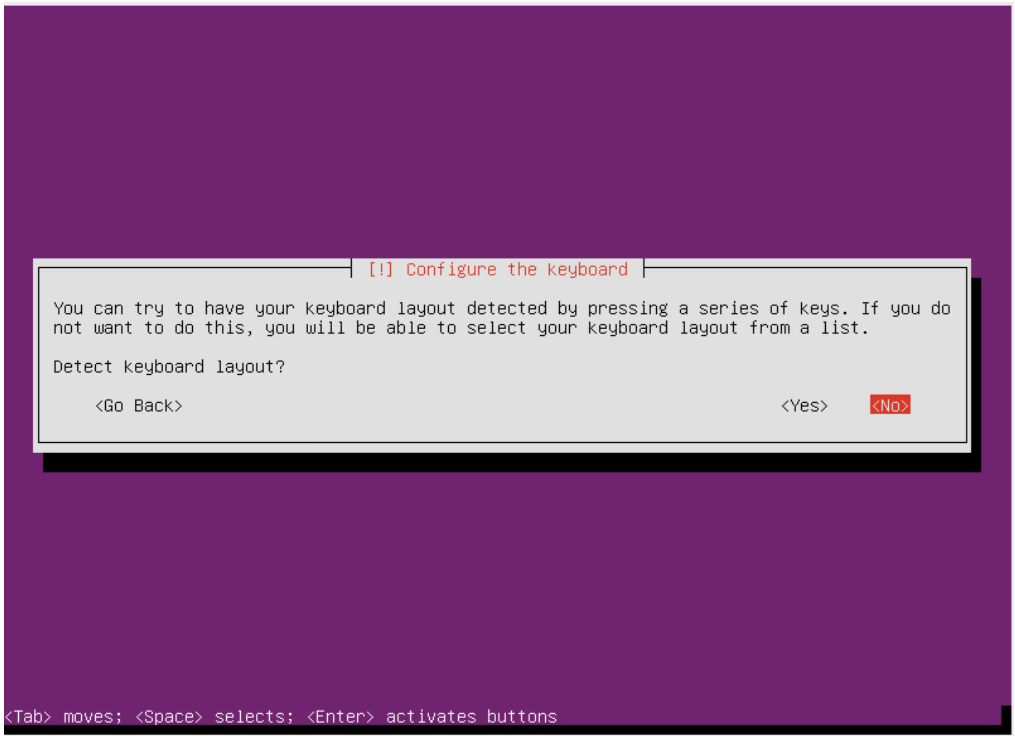
Gambar 2.2.7

7. Tahap berikutnya adalah memilih pengaturan format lokal. Untuk wilayah negara Indonesia biasanya formatnya adalah United States. Jadi pilih saja defaultnya yaitu **United States**.



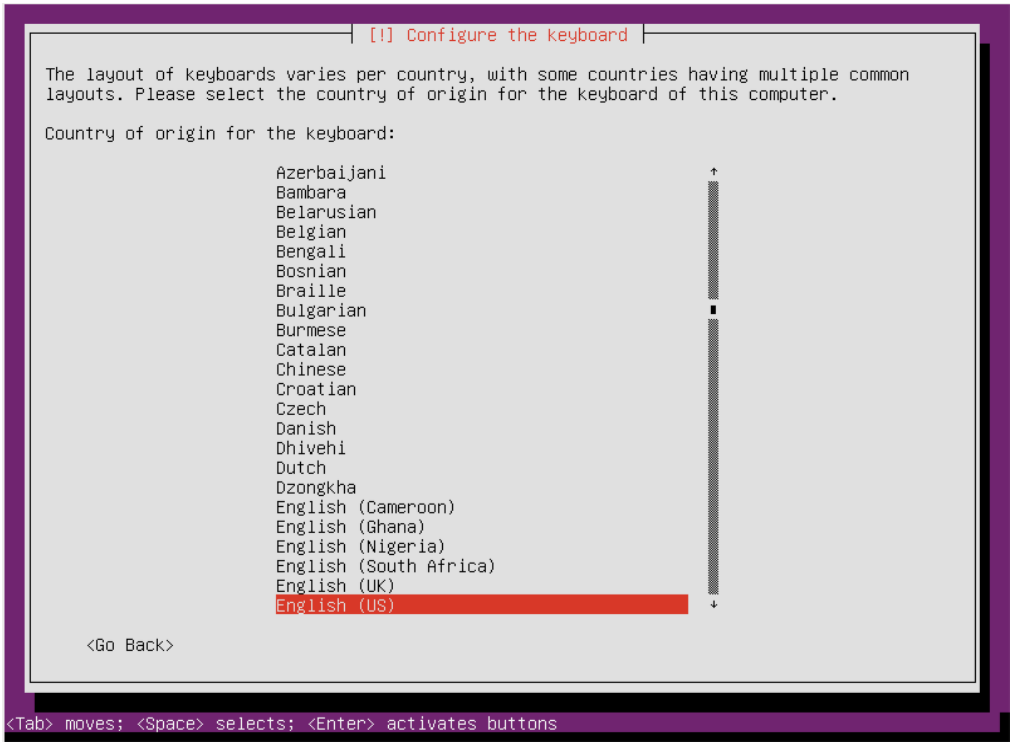
Gambar 2.2.8

8. Pilih **No** jika muncul pertanyaan untuk mendeteksi **layout keyboard** secara otomatis, karena kita akan memilihnya secara manual pada tahapan berikutnya.

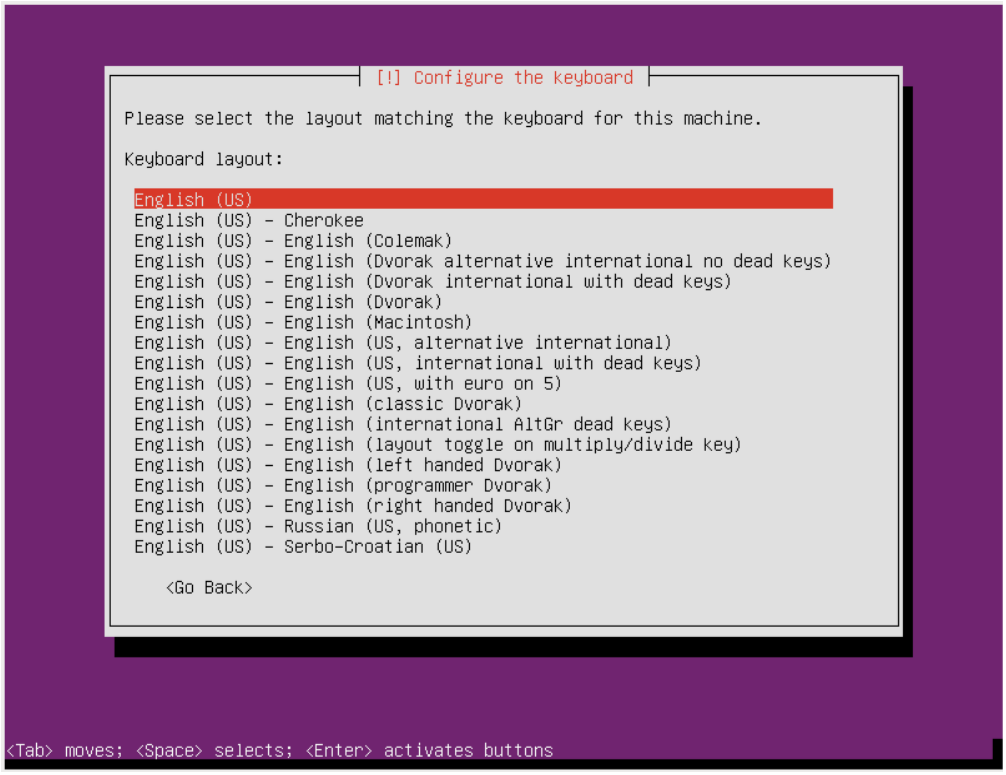


Gambar 2.2.9

9. Pada bagian ini kita akan memilih layout keyboard secara manual. Pilih **English (US)** lalu **English (US)** lagi, *Gambar 2.2.10*, *Gambar 2.2.11*.



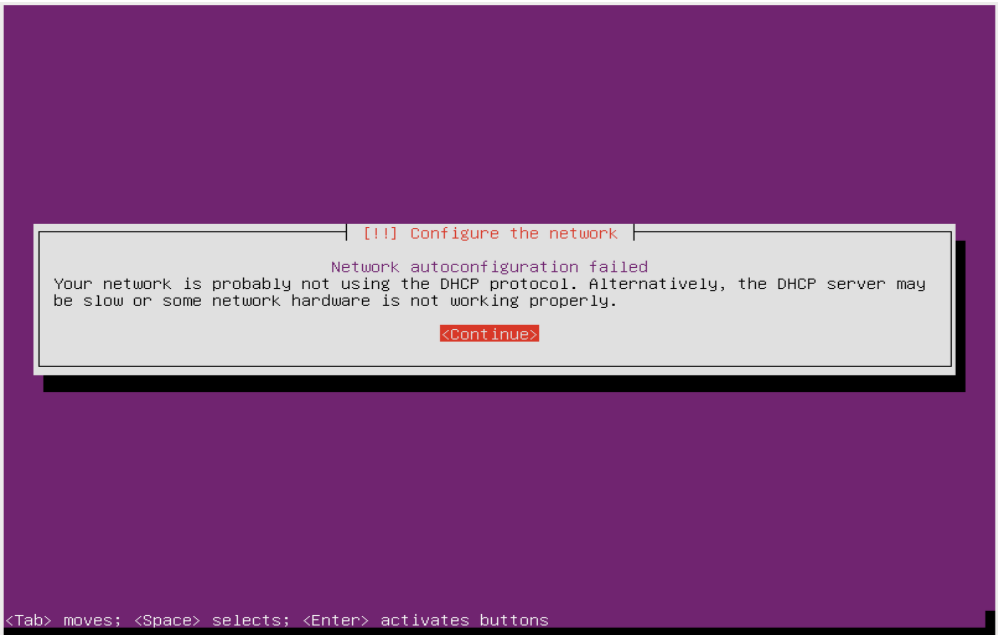
Gambar 2.2.10



Gambar 2.2.11

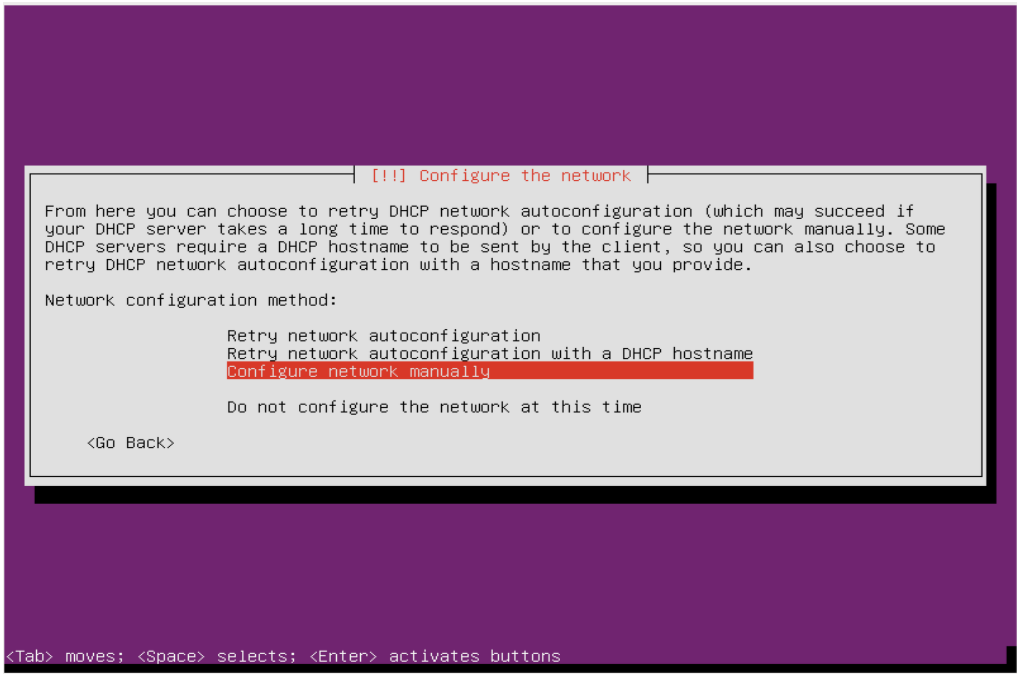
10. Kemudian akan muncul sebuah proses dimana Ubuntu meminta konfigurasi ip address secara DHCP. Berhubung disini kalian sedang praktek instalasi untuk komputer Server, sehingga hanya bermain di jaringan lokal dan tidak terkoneksi ke Internet, maka akan

muncul peringatan gagal seperti ini. Pilih saja **Continue.**



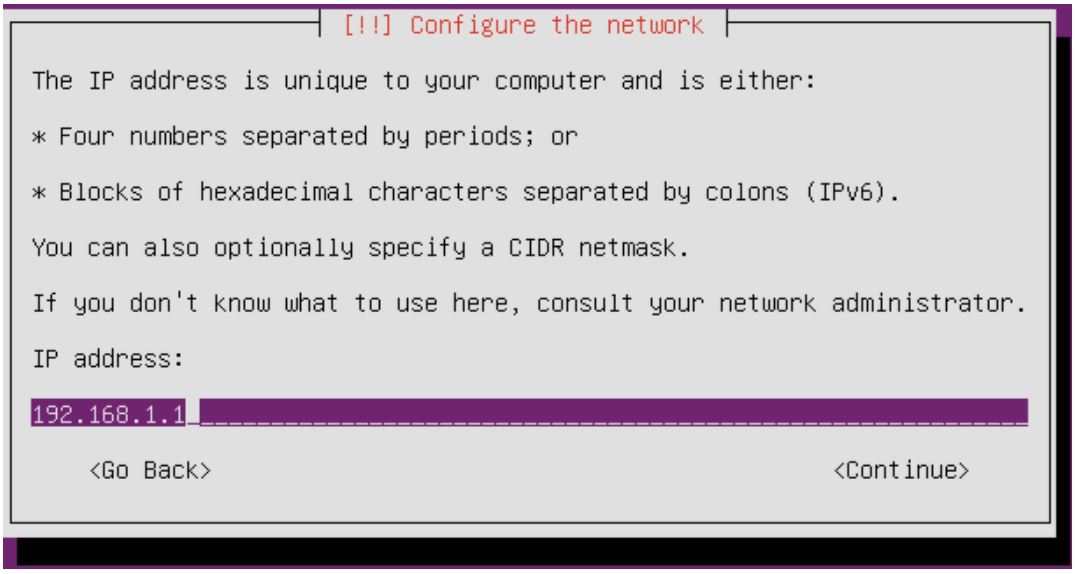
Gambar 2.2.12

11. Untuk keperluan konfigurasi komputer Server, lebih baik kalian samakan saja pengaturan ip address secara manual seperti di buku ini agar tidak membingungkan kalian nantinya. Pilih **Configure Network Manually**.



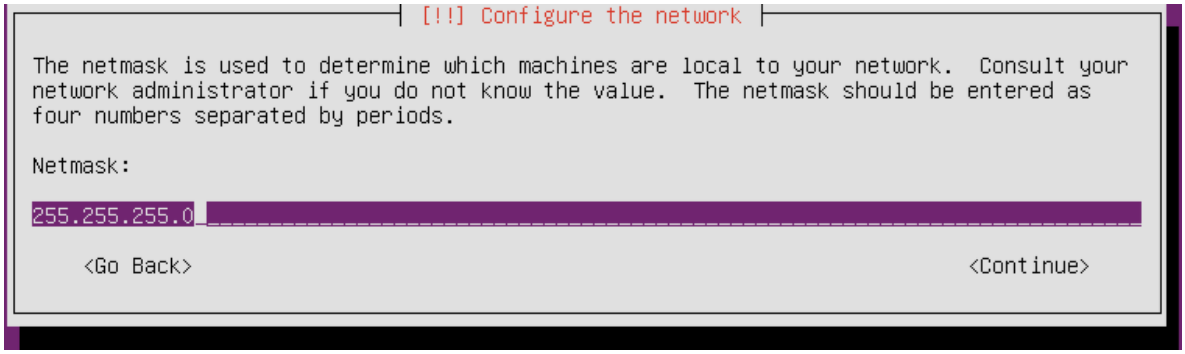
Gambar 2.2.13

12. Masukkan alamat ip addressnya dengan **192.168.1.1**



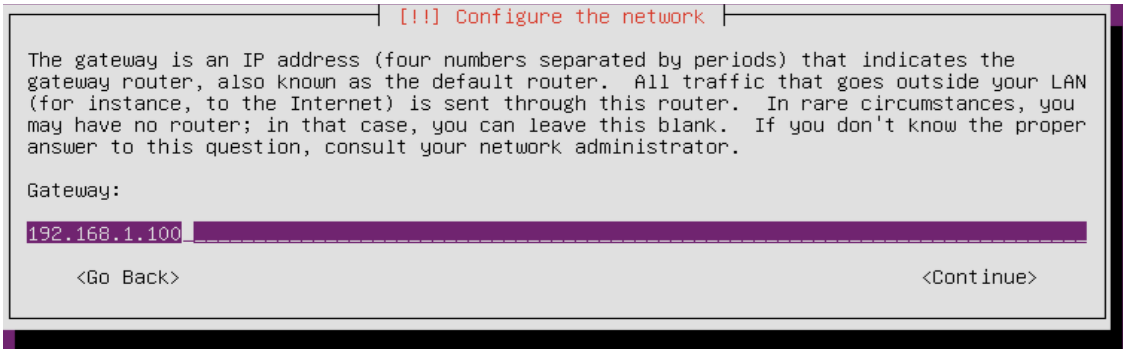
Gambar 2.2.14

13. Untuk Netmask nya, isikan saja dengan **255.255.255.0**. Netmask adalah patokan berapa jumlah host maksimal pada jaringan. Disini kita menggunakan ip jaringan kelas C dengan jumlah maksimum 254 host, sehingga kita isikan seperti dibawah.



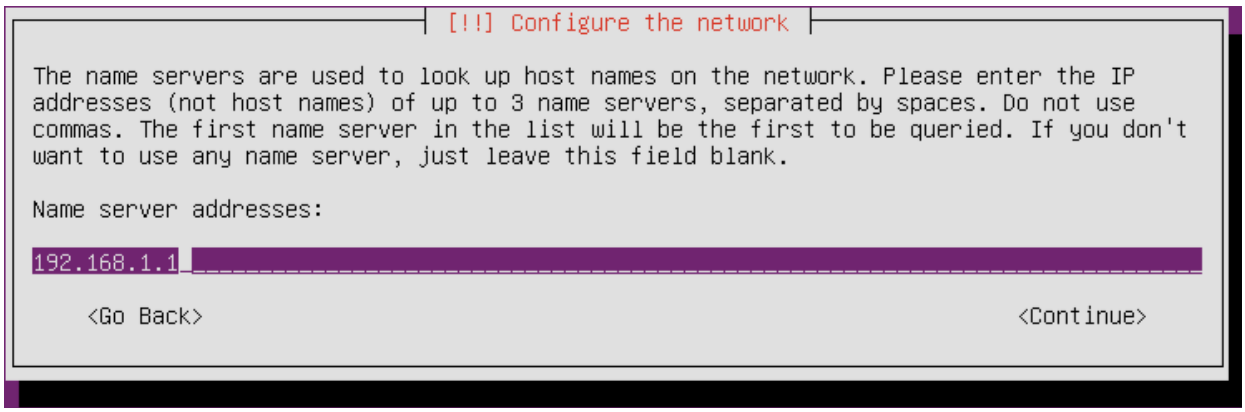
Gambar 2.2.15

14. Setelah itu masukkan ip **192.168.1.100** untuk gatewaynya.



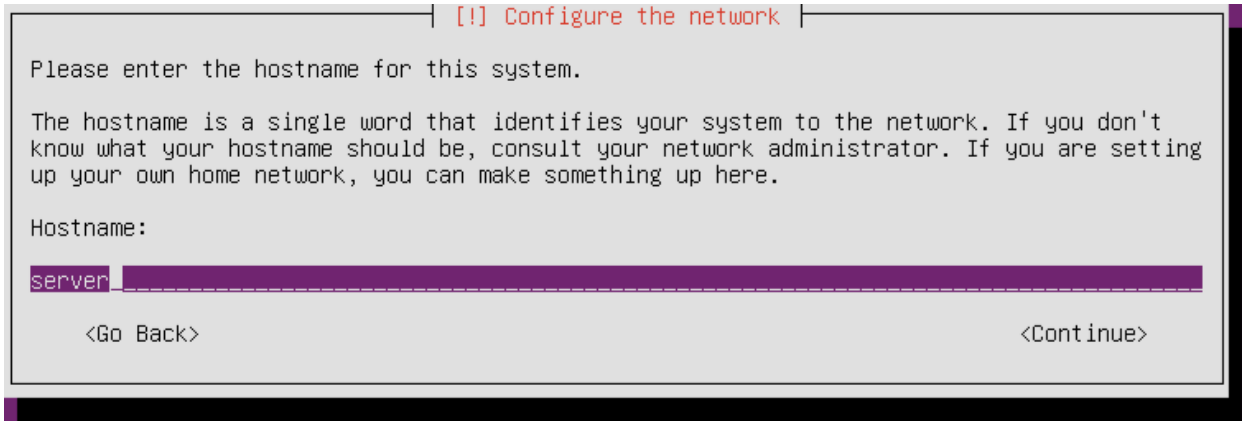
Gambar 2.2.16

15. Untuk Nameserver addressnya, masukkan ip address dari komputer server itu sendiri yaitu **192.168.1.1**.



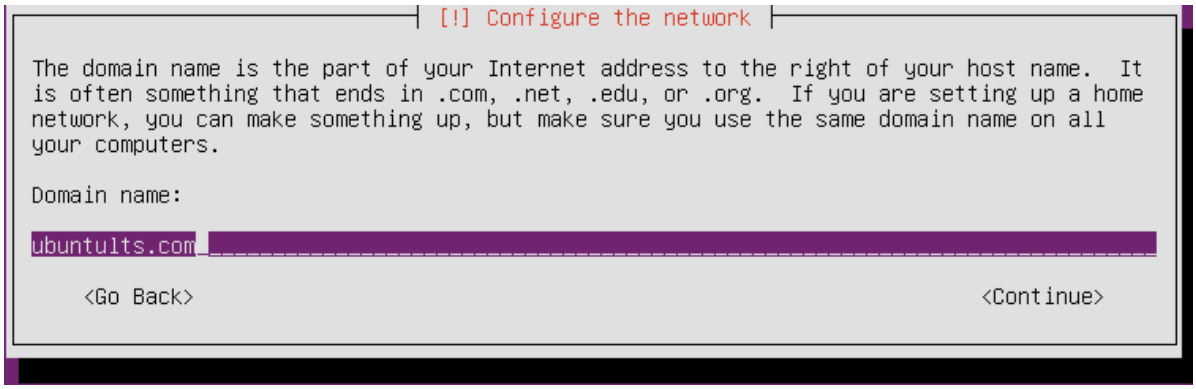
Gambar 2.2.17

16. Setelah itu kalian akan diminta untuk memasukkan hostname. Hostname adalah nama untuk komputer. Misalkan kalian isi **server**.



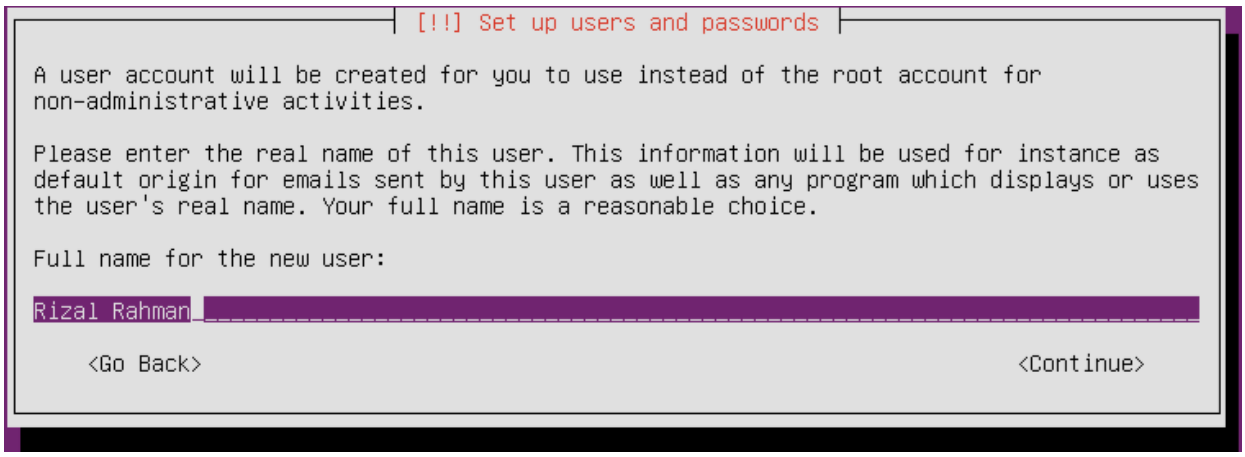
Gambar 2.2.18

17. Selanjutnya kalian diminta memasukkan nama domain yang kalian gunakan di dalam jaringan. Misalnya disini kalian isi dengan **ubuntults.com**



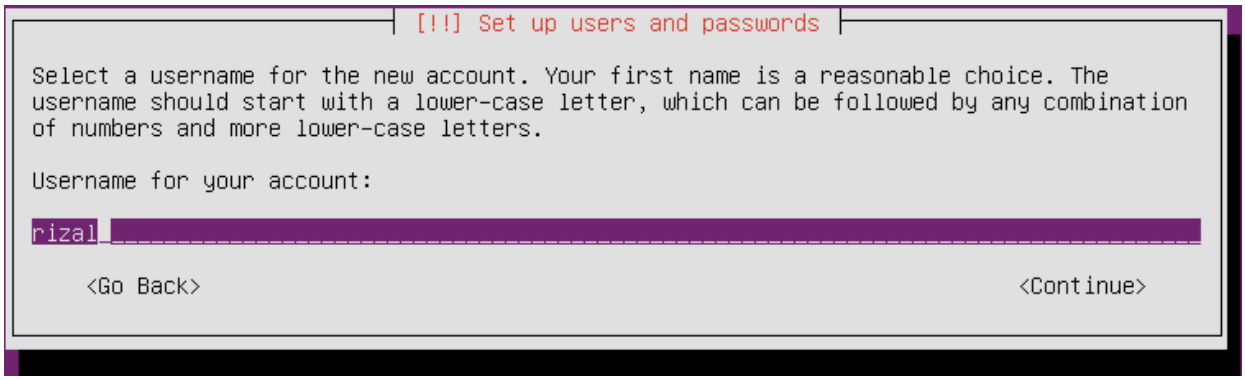
Gambar 2.2.19

18. Setelah itu masukkan nama lengkap *user* yang menggunakan komputer kalian. Disini saya isi **Rizal Rahman**.



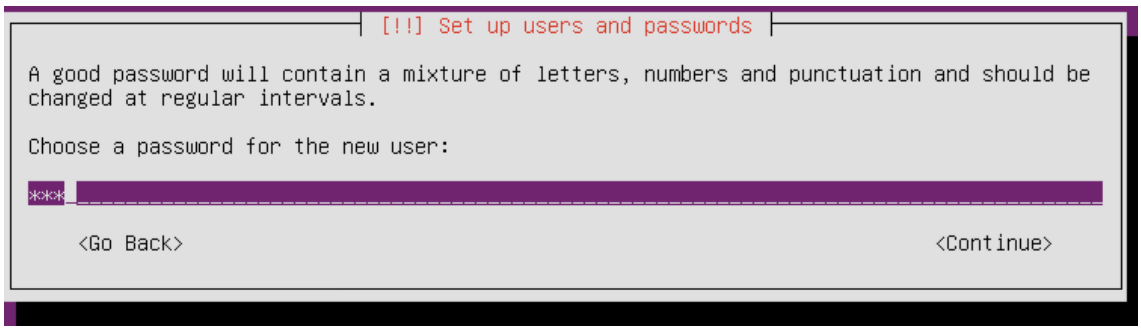
Gambar 2.2.20

19. Lalu isi juga *username*nya. Disini misalnya saya isi **rizal**.



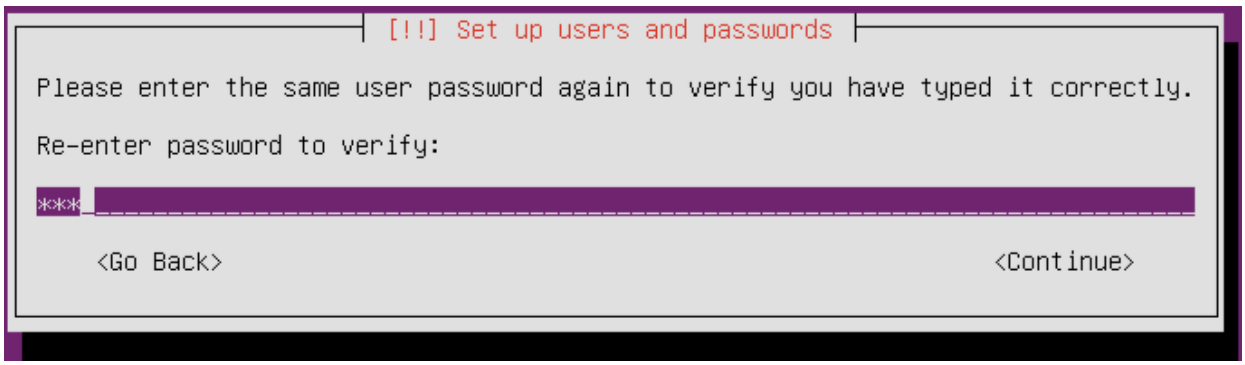
Gambar 2.2.21

20. Setelah mengisikan nama pengguna, kalian juga diminta untuk memasukkan password. Password ini sangatlah penting untuk kemanan server yang kalian miliki. Jangan sampai lupa dan pilihlah penggunaan password secara bijak, yaitu dengan menggunakan minimal sebanyak 8 digit. Usahakan ditambah dengan kombinasi angka, huruf, karakter-karakter spesial, serta kombinasi huruf kapital.



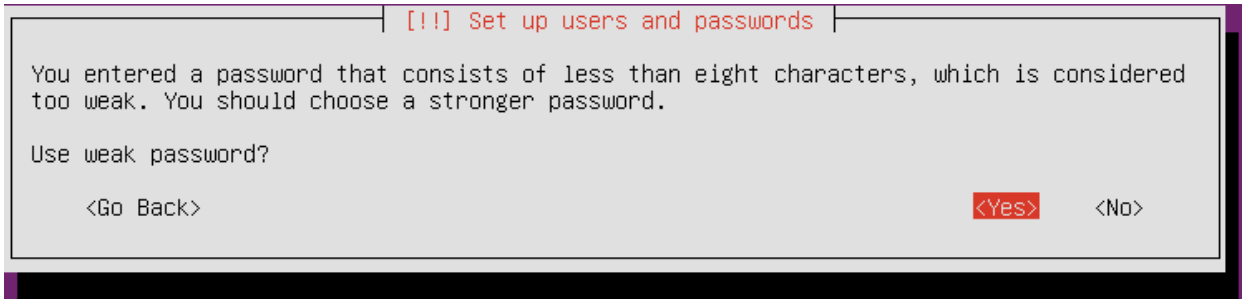
Gambar 2.2.22

21. Ketikkan kembali password kalian untuk konfirmasi.



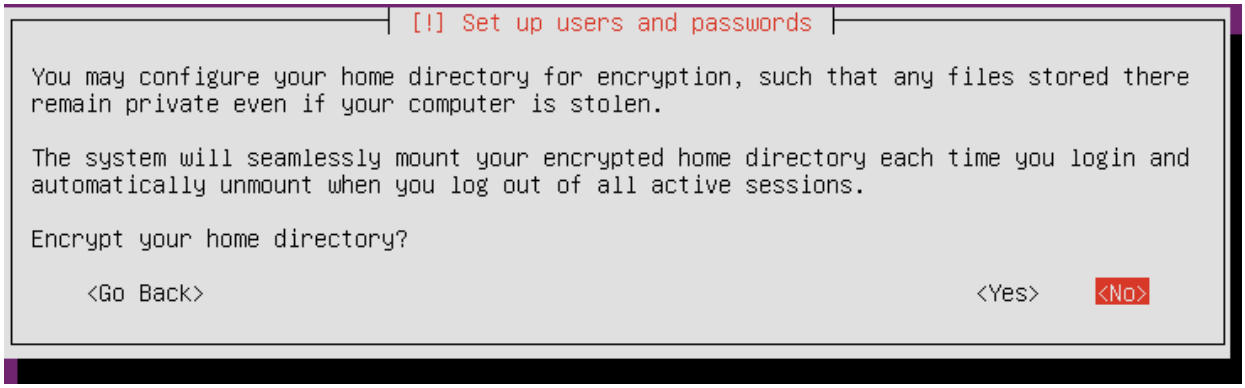
Gambar 2.2.23

22. Berikut adalah contoh peringatan jika kalian menggunakan password dengan kombinasi yang lemah. Berhubung disini saya hanya sebagai percobaan saja, maka pilih saja **Yes** jika muncul peringatan seperti ini.



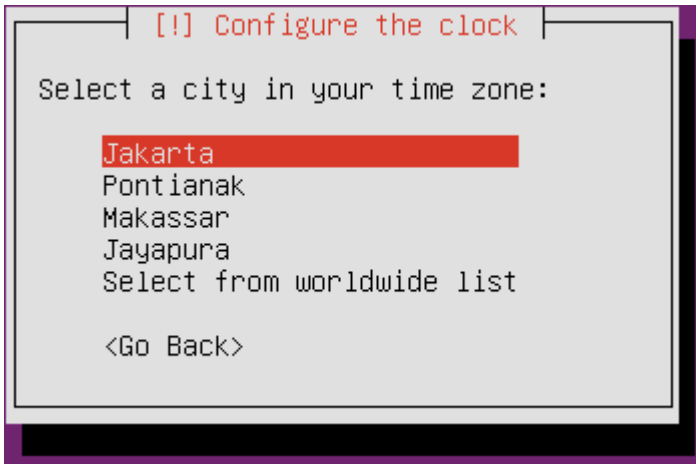
Gambar 2.2.24

23. Pilih **No** bila muncul pertanyaan yang menawarkan mengenkripsi home folder kalian.



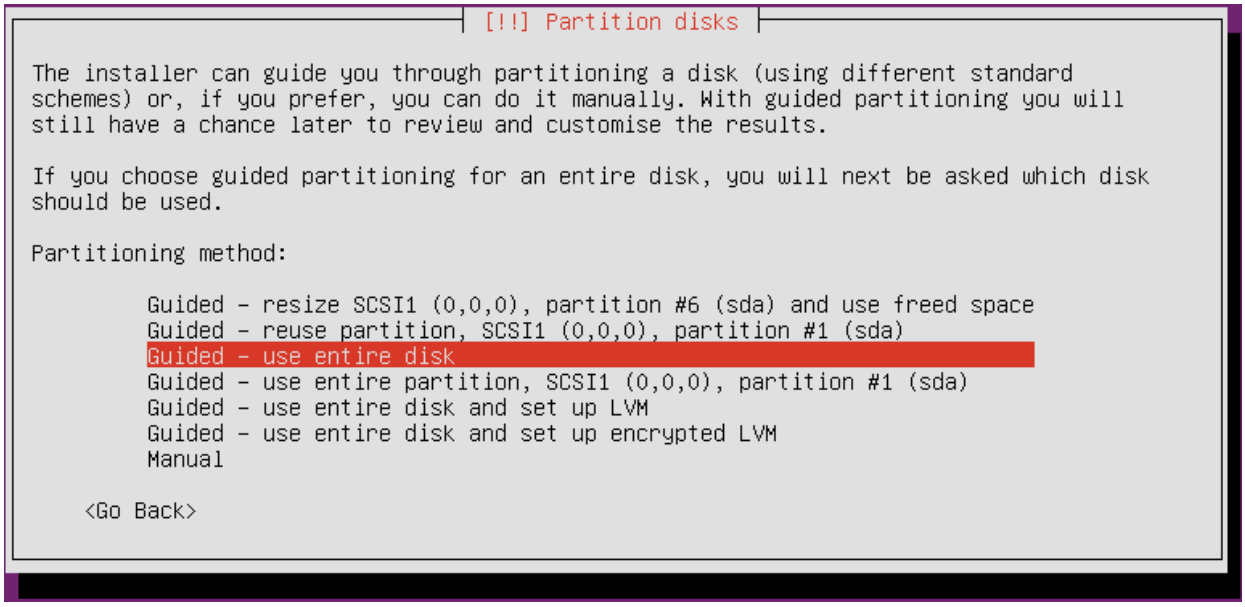
Gambar 2.2.25

24. Setelah itu kalian diminta untuk memilih zona waktu. Pilih **Jakarta**.



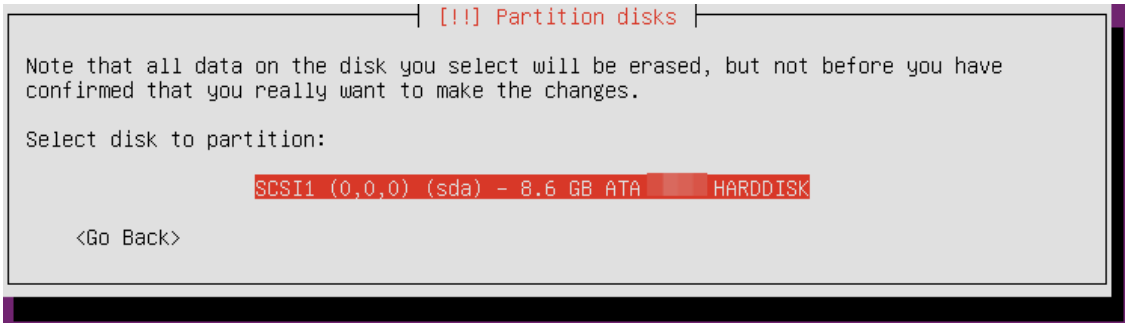
Gambar 2.2.26

25. Tahap selanjutnya adalah pemartisian harddisk. Pilih **Guided – Use Entire Disk**. Ingat, pilihan ini akan menghapus seluruh isi partisi dan menjadikan harddisk kalian sepenuhnya untuk Ubuntu Server 12.04 LTS. Pilih saja **Manual**, jika kalian ingin melakukan pemartisian sendiri sesuai keinginan kalian.



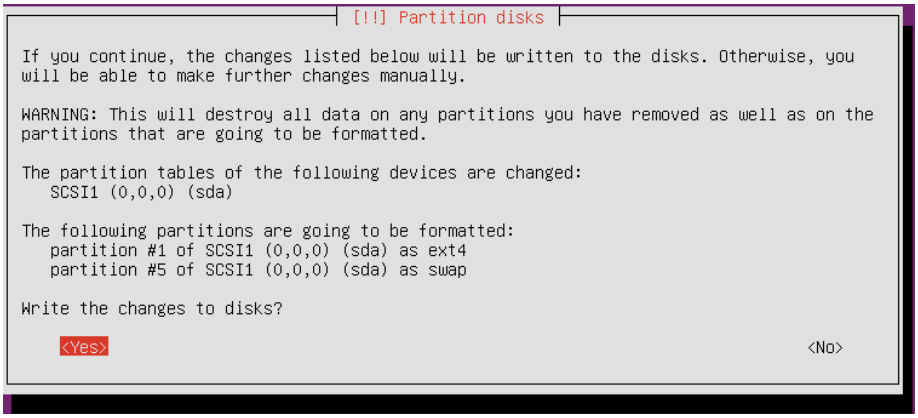
Gambar 2.2.27

26. Kemudian pilih harddisk mana yang ingin kalian install. Jika hanya terdapat satu harddisk di komputer kalian, maka pilih saja yang muncul seperti gambar dibawah.



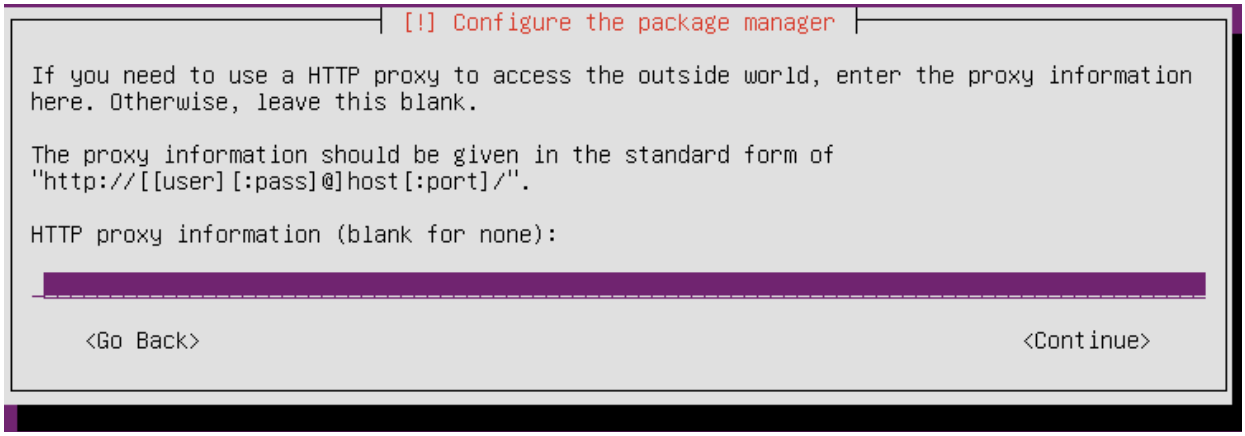
Gambar 2.2.28

27. Jika kalian sudah yakin, pilih **Yes** pada bagian ini.



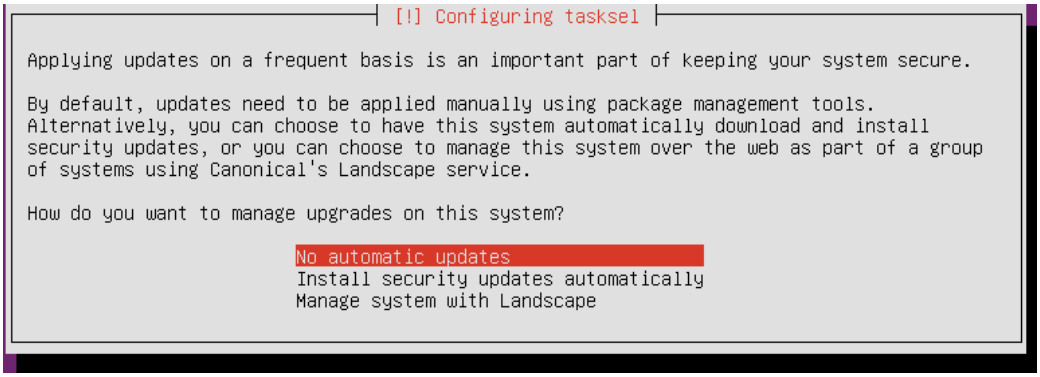
Gambar 2.2.29

28. Selanjutnya kalian akan ditanya apakah kalian ingin mengkoneksikan komputer kalian dengan proxy server dari Internet. Berhubung kalian tidak terhubung ke internet, kosongkan saja dan pilih **Continue**.



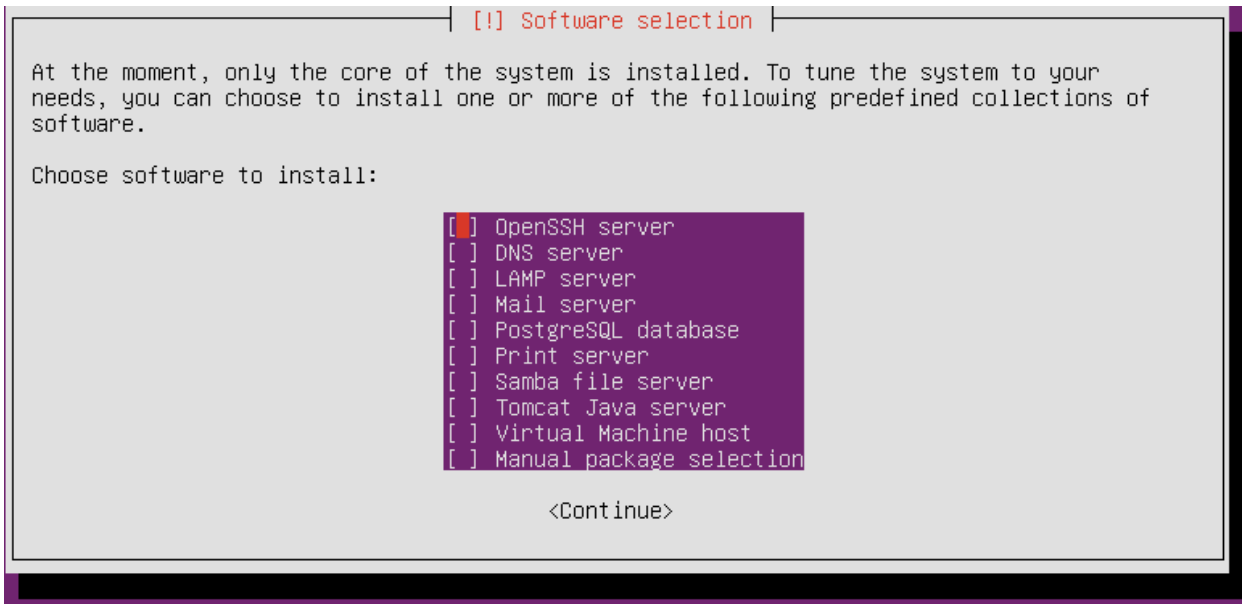
Gambar 2.2.30

29. Disini pilih **No automatic updates**.



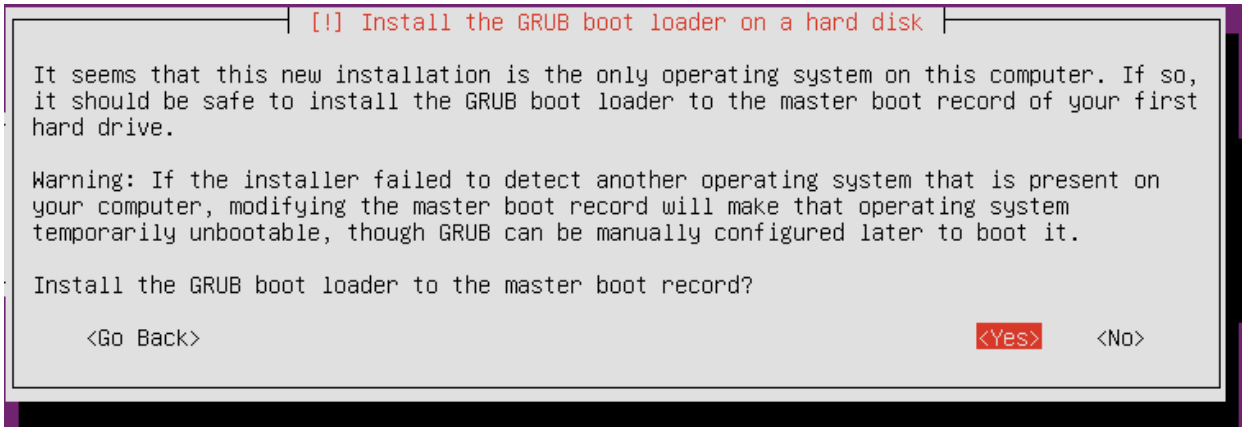
Gambar 2.2.31

30. Selanjutnya adalah memilih paket-paket mana saja yang ingin kalian install ke dalam Ubuntu server kalian. Pada tahap ini lebih baik kalian lewati saja, karena kalian akan menginstall paket-paket tersebut secara manual nanti. Biarkan apa adanya, kemudian pilih **Continue**.



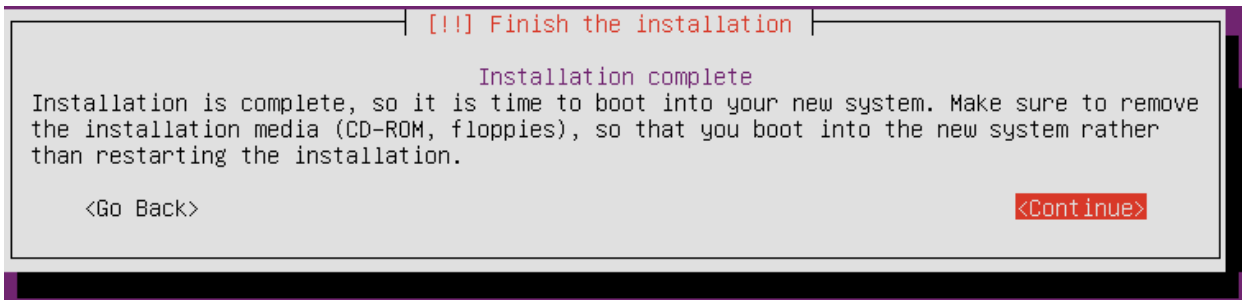
Gambar 2.2.32

31. Terakhir adalah tahapan penginstalan GRUB Boot Loader ke dalam harddisk. GRUB Boot Loader ini berfungsi untuk membuat Ubuntu Server dapat booting ke dalam komputer. Pilih **Yes**.

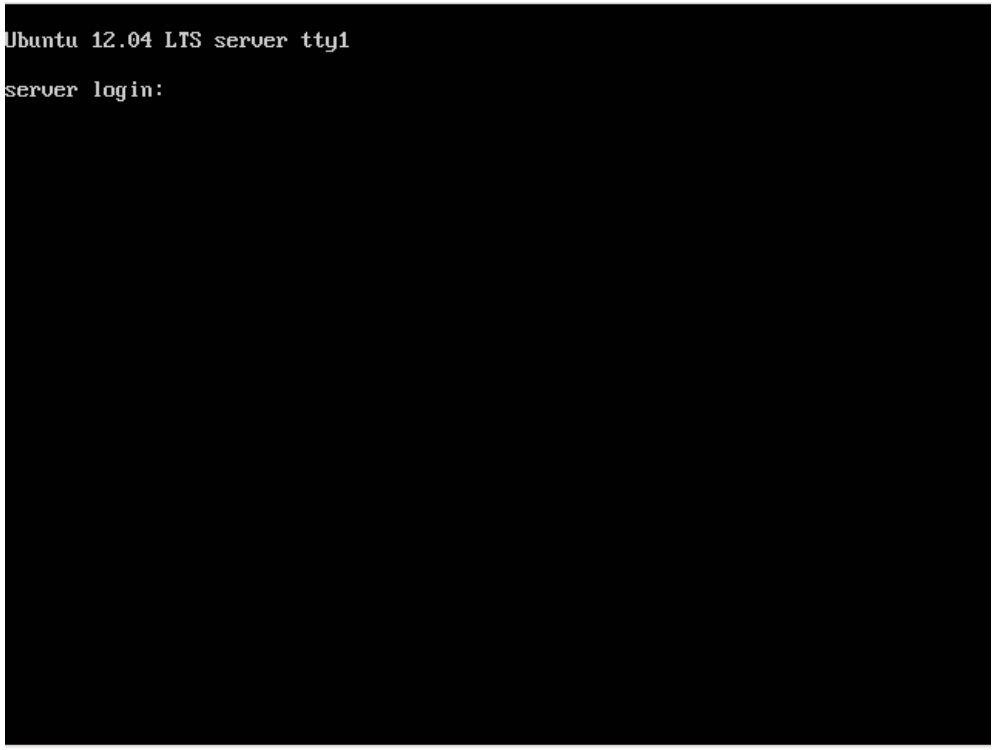


Gambar 2.2.33

32. Pilih **Continue** untuk terakhir kalinya. Komputer pun akan merestart sendiri dan kemudian akan muncul tampilan login tanda instalasi telah berhasil.

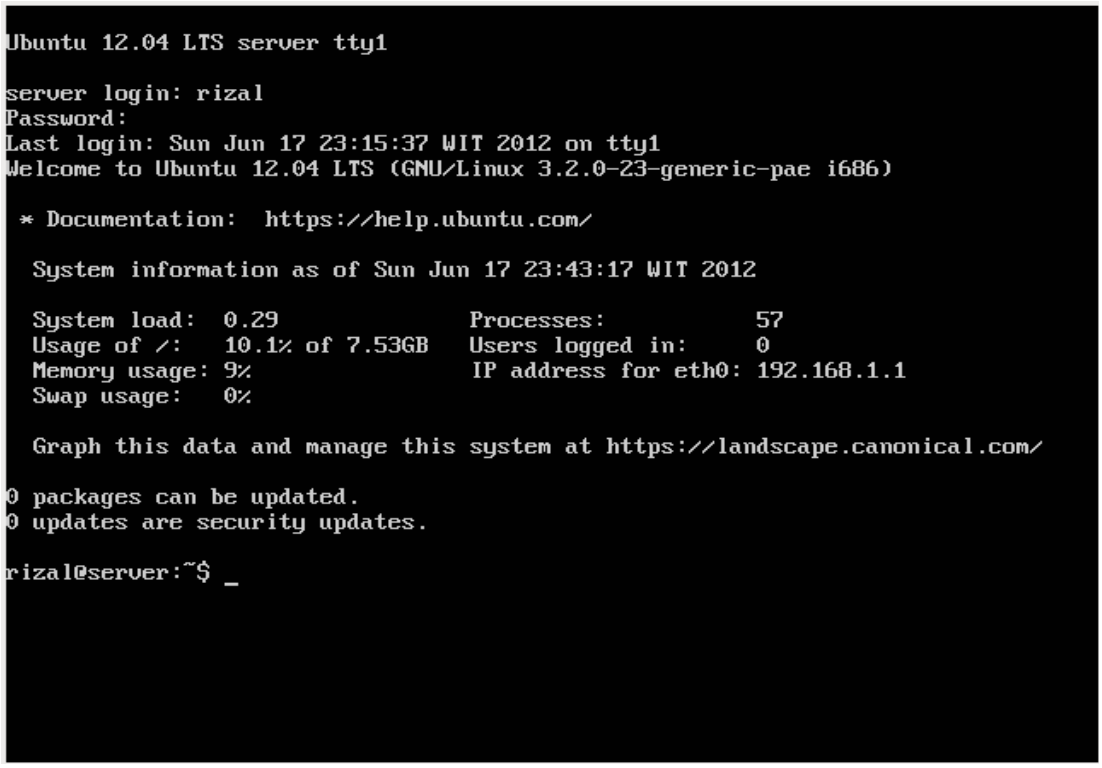


Gambar 2.2.34



Gambar 2.2.35

33. Masukkan nama user dan password kalian untuk login. Disini misalnya saya masukkan **rizal** untuk *Server Login* nya, kemudian saya masukkan passwordnya. Karena alasan keamanan, di Linux password memang tidak terlihat saat kalian mengetik, namun sebenarnya itu ada. Ketikkan saja passwordnya, kemudian tekan **enter**.



Gambar 2.2.36

2.3. Pasca Instalasi

2.3.a. Menambahkan Repositori dari DVD

Setelah instalasi selesai, jangan melakukan apa-apa terlebih dahulu. Pertama-tama lebih baik kalian tambahkan repositori dari DVD ke dalam sistem agar dapat digunakan. Karena repositori ini sangat penting untuk keperluan kita menginstall seluruh paket aplikasi nanti. Untuk itu kalian harus menambahkan DVD repositori ini terlebih dahulu ke dalam sebuah file konfigurasi bernama *sources.list.*

- Caranya pertama-tama masukkan DVD repositori 1 ke dalam CDROM komputer kalian, kemudian jalankan perintah ini :

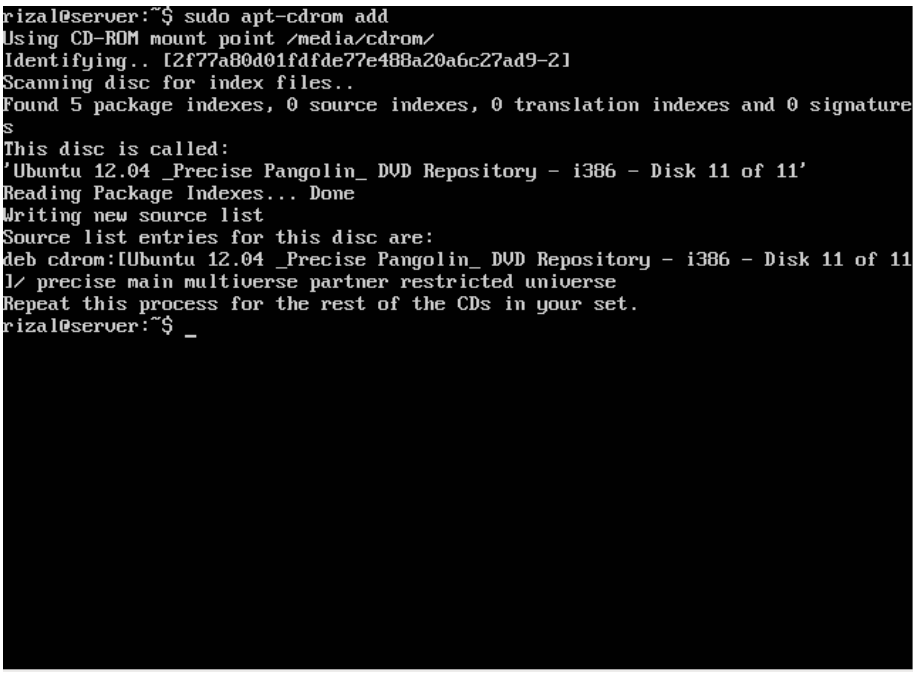
```
sudo apt-cdrom add
```

- Maka hasilnya akan seperti ini :

```
rizal@server:~$ sudo apt-cdrom add
[sudo] password for rizal:
Using CD-ROM mount point /media/cdrom/
Identifying.. [2f77a80d01fdfde77e488a20a6c27ad9-2]
```

```
Scanning disc for index files..
Found 5 package indexes, 0 source indexes, 0 translation indexes and
signatures
This disc is called:
'Ubuntu 12.04 _Precise Pangolin_ DVD Repository - i386 - Disk 1 of 11'
Reading Package Indexes... Done
Writing new source list
Source list entries for this disc are:
deb cdrom:[Ubuntu 12.04 _Precise Pangolin_ DVD Repository - i386 - Disk 1
of 11]/ precise main multiverse partner restricted universe
Repeat this process for the rest of the CDs in your set.
rizal@server:~$
```

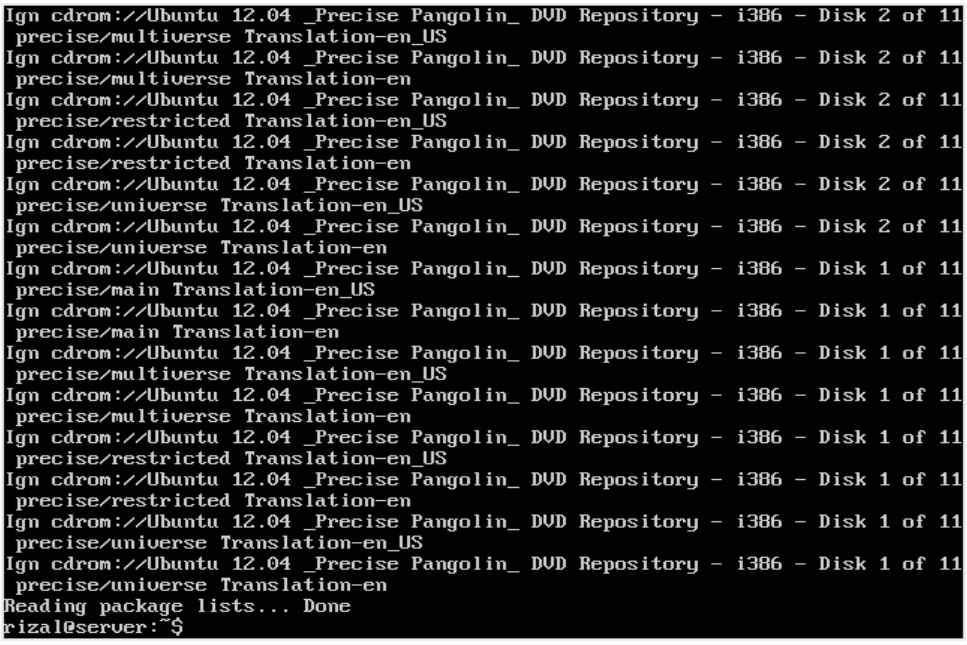
- Kemudian keluarkan DVD repositori 1 dan ganti dengan DVD repositori ke-2. Ulangi perintah diatas hingga DVD yang ke-11.



Gambar 2.3.a.1

- Setelah itu eksekusi perintah berikut sebagai langkah terakhir untuk menambahkan DVD repositori ke Ubuntu 12.04 LTS :

```
sudo apt-get update
```



Gambar 2.3.a.2

- Jika tidak ada pesan error, maka sampai pada tahap ini kalian telah berhasil menambahkan DVD repositori ke Ubuntu 12.04 LTS.

2.3.b. Konfigurasi TCP/IP di Linux

Konfigurasi TCP/IP di Ubuntu Server agak sedikit berbeda jika kalian bandingkan dengan sistem operasi Windows yang berbasis serba GUI. Namun sebenarnya konsepnya sama saja dan cukup mudah untuk diimplementasikan sehingga tidak sesulit kelihatannya. Pada subbab ini akan dibahas mengenai cara-cara dasar mengkonfigurasi TCP/IP di Ubuntu Server 12.04 LTS :

2.3.b.1. Mengkonfigurasi Interface Jaringan

Untuk mengkonfigurasi Interface jaringan di Linux, perintah yang digunakan adalah perintah **ifconfig**. Ifconfig atau *Interface Configure* memiliki banyak fungsi, seperti mengaktifkan dan menonaktifkan perangkat jaringan, mengatur ip address, atau hanya sekedar melihat konfigurasi perangkatnya saja.

Sebagai contoh, coba ketikkan perintah **ifconfig**, maka akan tampil seperti ini :

```
rizal@server:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4f:39:a5
          inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe4f:39a5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:564 errors:0 dropped:0 overruns:0 frame:0
```

```
          TX packets:827 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:50264 (50.2 KB)  TX bytes:100516 (100.5 KB)

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:476 errors:0 dropped:0 overruns:0 frame:0
          TX packets:476 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:39916 (39.9 KB)  TX bytes:39916 (39.9 KB)

rizal@server:~$
```

Disitu terlihat ada dua konfigurasi perangkat yaitu interface utama *eth0* lengkap dengan informasi berapa ip address, netmask, dan broadcast addressnya seperti yang telah kalian atur pada saat instalasi, serta *lo* yang juga terlihat tidak jauh berbeda dengan interface *eth0*.
Dengan perintah ifconfig, kalian juga dapat mematikan atau mengaktifkan interface-interface tersebut dengan perintah :

```
sudo ifconfig namainterface down/up
```

Misalnya saja kalian ingin mematikan interface eth0 maka perintahnya adalah seperti ini :

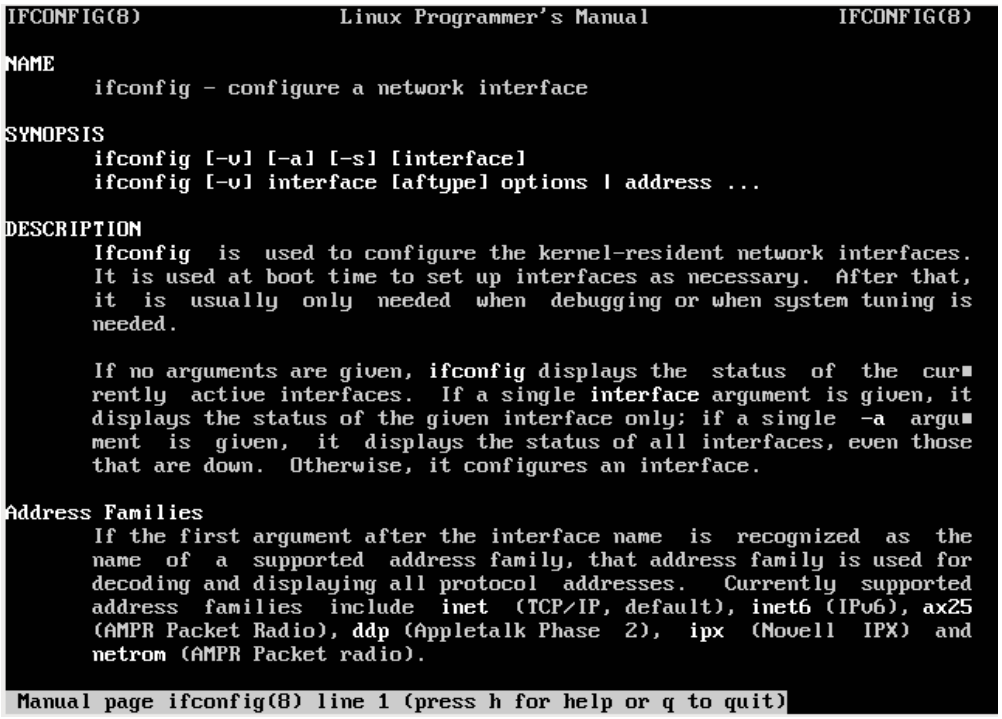
```
sudo ifconfig eth0 down
```

Dan kalian dapat menyalakannya kembali dengan perintah ini :

```
sudo ifconfig eth0 up
```

Diatas adalah beberapa contoh fungsi-fungsi dari perintah ifconfig. Kalian dapat melihat fungsi-fungsi lainnya dari panduan manual ifconfig dengan mengetikkan perintah :

```
man ifconfig
```



Gambar 2.3.b.1.1

2.3.b.2. Mengkonfigurasi TCP/IP

Pada bahasan subbab sebelumnya, telah disindir sedikit mengenai beberapa cara mengkonfigurasi interface jaringan dengan menggunakan perintah ifconfig. Nah pada subbab ini, kalian akan mempelajari cara mengkonfigurasi TCP/IP secara lebih lanjut.

Pada umumnya, seluruh pengaturan TCP/IP di Linux (dalam hal ini, Ubuntu), terdapat di dalam file **/etc/network/interfaces**, baik itu konfigurasi IP address, Netmask, Gateway, dan Nameserver address. Khusus untuk Nameserver address, terdapat file konfigurasi manualnya juga di **/etc/resolv.conf**.

Mengedit file /etc/network/interfaces

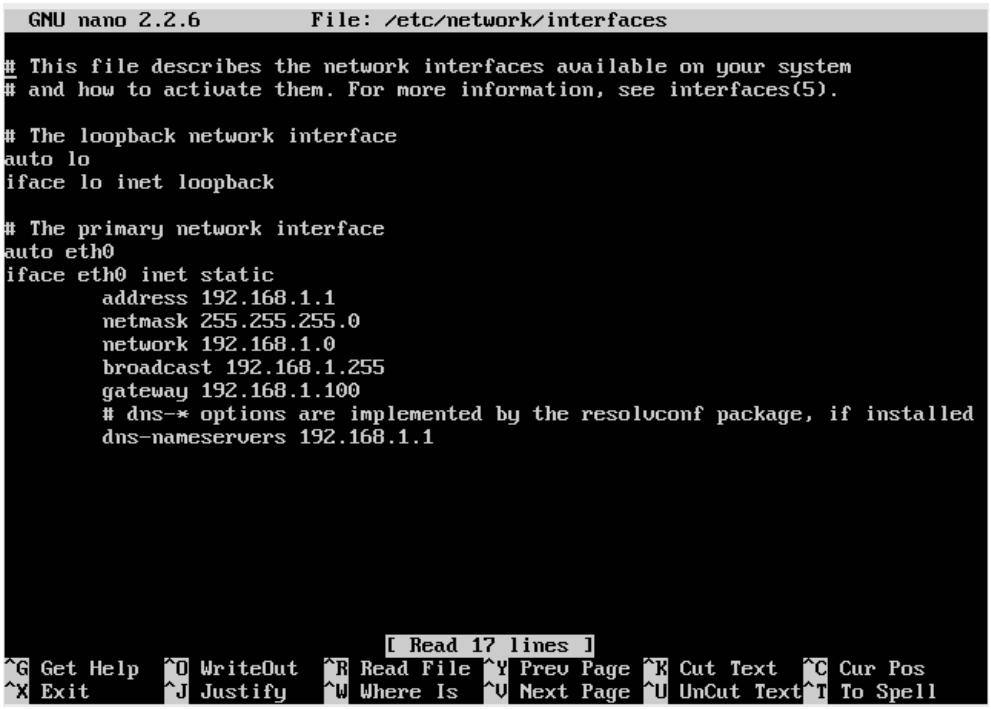
File /etc/network/interfaces adalah file yang digunakan oleh sistem dalam melihat seluruh konfigurasi TCP/IP di Ubuntu. Setiap komputer booting, komputer akan menentukan seluruh pengaturan TCP/IP dengan melihat isi file ini. Jadi apabila kalian ingin pengaturan ip address, netmask, broadcast, dll, secara permanen, maka yang harus kalian lakukan cukup dengan mengedit file tersebut. Caranya dengan mengetikkan perintah dibawah :

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

Maka, akan muncul seperti ini :

```
# This file describes the network interfaces available on your system
```

```
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
        address 192.168.1.1
        netmask 255.255.255.0
        network 192.168.1.0
        broadcast 192.168.1.255
        gateway 192.168.1.100
        # dns-* options are implemented by the resolvconf package, if installed
        dns-nameservers 192.168.1.1
```



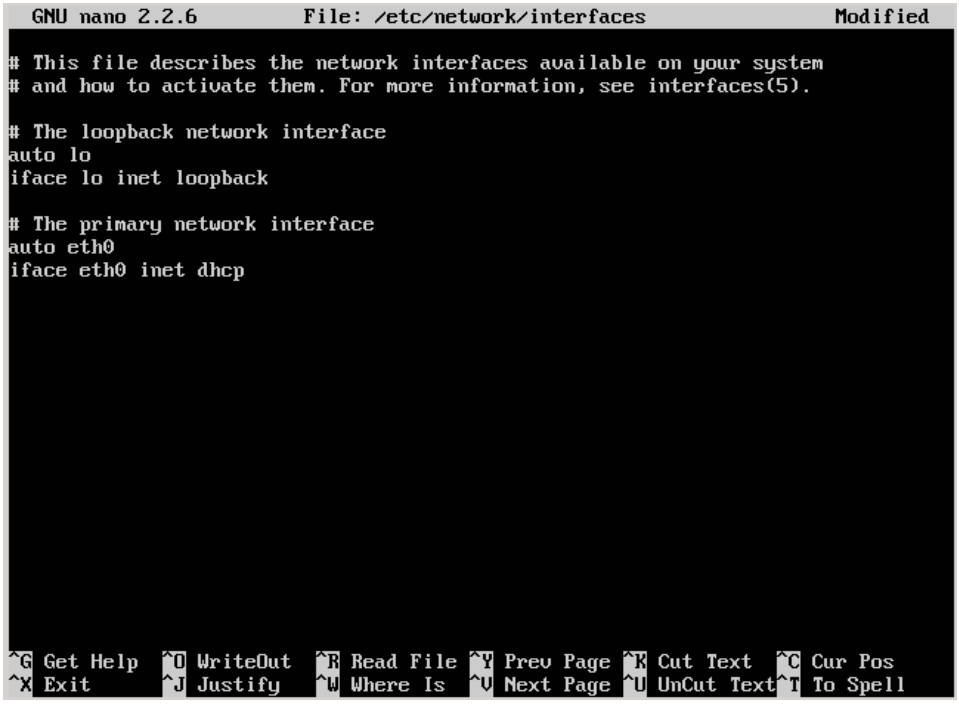
Gambar 2.3.b.2.1

Itu adalah seluruh konfigurasi TCP/IP yang ada di sistem Ubuntu kalian yang telah otomatis tertulis saat kalian melakukan instalasi pertama kali. Jika kalian ingin melakukan suatu perubahan,

misalnya saja ingin mengganti ip addressnya menjadi 192.168.1.10, maka tinggal edit IP pada bagian **address** menjadi sesuai yang kalian inginkan. Atau bila kalian ingin merubah alamat gateway dan nameserver ? Tinggal edit saja pada bagian **gateway** dan **dns-nameservers**.

Namun jika kalian ingin mengatur agar ip address kalian menjadi dinamis/dhcp, ubah konfigurasi tersebut menjadi seperti ini :

```
# The primary network interface
auto eth0
iface eth0 inet dhcp
```



Gambar 2.3.b.2.2

Jika sudah, simpan perubahan dengan menekan kombinasi keyboard **CTRL + X**, lalu tekan **y**, dan tekan **Enter.**

Untuk melihat efeknya, silahkan restart *networking* nya dengan perintah berikut :

```
sudo service networking restart
```

Atau jika masih tidak ada perubahan, coba saja restart komputernya :

```
sudo reboot
```

Mengedit file /etc/resolv.conf

Sebenarnya satu file **/etc/network/interfaces** saja sudah cukup untuk mengatur seluruh konfigurasi TCP/IP di Ubuntu secara otomatis dan permanen, termasuk Nameserver address. Namun ada

kalanya dalam sebab-sebab tertentu kalian juga perlu untuk melakukan pengeditan alamat nameserver secara manual. Konfigurasi nameserver tersebut terletak di file **/etc/resolv.conf**. Untuk mengeditnya, silahkan ketikkan perintah ini :

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

Isinya adalah kira-kira seperti berikut :

```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 192.168.1.1
```

Disitu tertulis nameserver 192.168.1.1, dimana 192.168.1.1 adalah alamat ip dari DNS server lokal yang kalian gunakan sesuai dengan file konfigurasi **/etc/network/interfaces**. Kalian dapat menambahkan atau mengubah file ini semau kalian, asal dengan format penulisan yang benar. Misalnya kalian ingin menambahkan satu alamat nameserver baru, tinggal kalian tambahkan saja satu baris dibawahnya seperti ini :

```
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
#     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
nameserver 192.168.1.1
nameserver 192.168.1.2
```

Kemudian simpan perubahan dengan menekan **CTRL + X**, lalu **y**, dan tekan **Enter**.

Dengan cara mengedit kedua file seperti tadi, sebenarnya tahap konfigurasi TCP/IP di Ubuntu/Linux sudah selesai dilakukan. Akan tetapi, cara diatas dirasa agak kurang efisien bila kita ingin merubah konfigurasi TCP/IP secara langsung. Karena seperti yang kalian ketahui, perubahan yang kalian lakukan terhadap kedua file tersebut tidak akan berfungsi sebelum kalian merestart layanan *networking* atau bahkan harus merestart komputer kalian juga. Nah, oleh karena itu kalian juga harus mengetahui cara-cara untuk melakukan konfigurasi TCP/IP secara manual yang akan dibahas pada sub-bab dibawah ini.

Mengkonfigurasi IP address, netmask, dan Broadcast Address.

Apabila kalian ingin merubah atau menambahkan IP address, caranya sangatlah mudah. Misal, kalian ingin merubah interface **eth0** yang ip address awalnya **192.168.1.1** menjadi **192.168.1.10** dengan netmask awal **255.255.255.0** menjadi **255.255.252.0**, maka perintah yang digunakan adalah

seperti ini :

```
sudo ifconfig eth0 192.168.1.10 netmask 255.255.252.0
```

Atau :

```
sudo ifconfig eth0 192.168.1.10/22
```

Setelah kalian melakukan perintah itu, konfigurasi IP addressnya pasti telah berubah. Coba cek dengan perintah ifconfig maka akan berubah menjadi seperti ini :

```
rizal@server:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:4f:39:a5
          inet addr:192.168.1.10  Bcast:192.168.3.255  Mask:255.255.252.0
          inet6 addr: fe80::a00:27ff:fe4f:39a5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:564 errors:0 dropped:0 overruns:0 frame:0
          TX packets:827 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:50264 (50.2 KB)  TX bytes:100516 (100.5 KB)

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:476 errors:0 dropped:0 overruns:0 frame:0
          TX packets:476 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:39916 (39.9 KB)  TX bytes:39916 (39.9 KB)

rizal@server:~$
```

Mengkonfigurasi Gateway Address.

Mengkonfigurasi alamat Gateway juga tidak kalah mudahnya dengan mengkonfigurasi IP address, netmask, dan broadcast seperti diatas. Misalnya saja kalian ingin merubah alamat gateway yang sebelumnya merujuk ke alamat 192.168.1.100 menjadi ke alamat 192.168.1.99, maka perintahnya adalah seperti ini :

```
sudo route add default gw 192.168.1.99
```

Setelah itu coba cek apakah alamat gateway telah berubah dengan perintah berikut :

```
sudo route –n
```

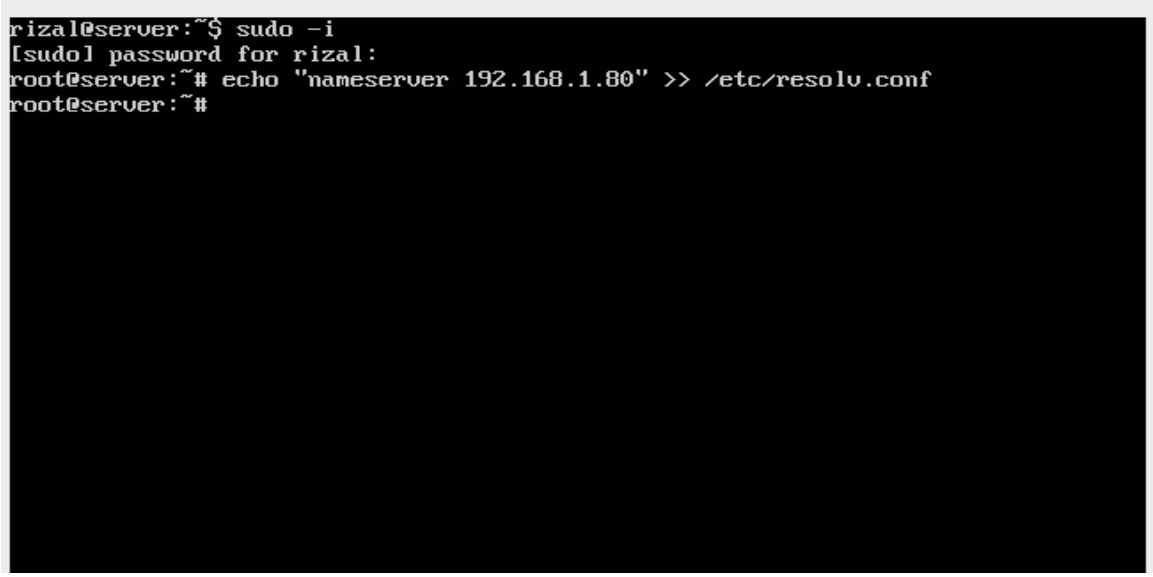
Bila berhasil seharusnya alamat gateway yang baru (192.168.1.99) akan berada paling atas seperti ini :

```
rizal@server:~$ sudo route –n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.1.99    0.0.0.0         UG    0      0        0 eth0
0.0.0.0         192.168.1.100   0.0.0.0         UG    100    0        0 eth0
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
rizal@server:~$
```

Mengkonfigurasi Nameserver Address.

Pada teknisnya, untuk mengkonfigurasi alamat nameserver kalian harus menuliskan sebuah perintah ke dalam file **/etc/resolv.conf** secara langsung. Oleh karena itu, kalian harus menggunakan perintah **echo** yang dapat berfungsi untuk menuliskan sesuatu di sebuah file tanpa kalian harus mengubah sendiri file tersebut. Misalkan saja kalian ingin menambahkan alamat nameserver baru dengan IP address 192.168.1.80, kalian tinggal ketikkan perintah-perintah berikut :

```
sudo –i
echo “nameserver 192.168.1.80” >> /etc/resolv.conf
```



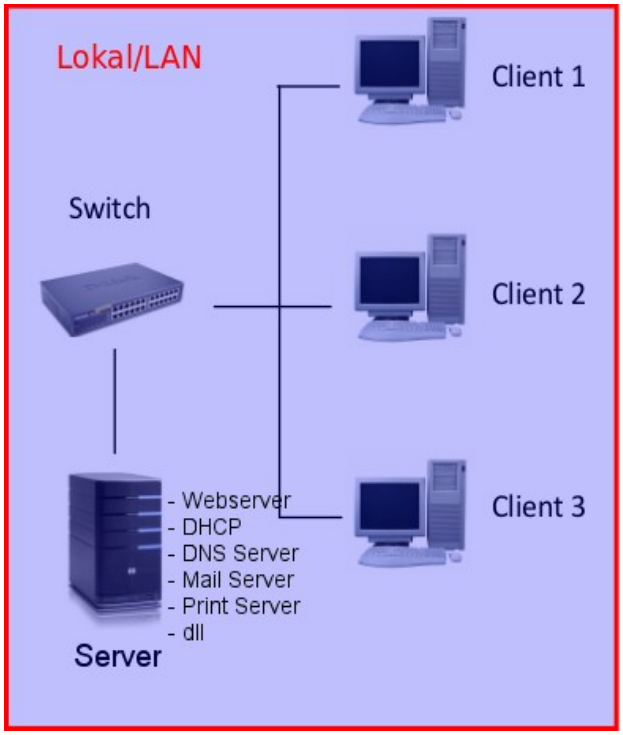
Gambar 2.3.b.2.3

Semua konfigurasi manual diatas sifatnya adalah sementara, jadi apabila kalian merestart komputer kalian maka seluruh konfigurasi akan hilang. Lakukan saja perubahan pada file **/etc/network/interfaces** seperti yang telah dijelaskan sebelumnya bila kalian ingin menjadikan konfigurasi ini menjadi permanen.

Bab 3. Konfigurasi dan Instalasi Aplikasi Server Ubuntu Server 12.04 LTS

Buku ini saya bagi menjadi 2 bagian besar konfigurasi. Bagian pertama yaitu konfigurasi komputer Server, dan bagian kedua adalah konfigurasi untuk komputer Routernya. Konfigurasi komputer Router akan saya tuliskan dibagian kedua yaitu pada Bab 4 nanti, karena konfigurasi pada Router sendiri sudah mencakup dua buah jaringan yang berbeda (WAN) sehingga agak sedikit rumit dan juga membutuhkan koneksi internet jika ingin melihat hasil pengetesannya lebih maksimal. Untuk bab 3 ini sendiri, saya akan membahas cara-cara konfigurasi dan instalasi aplikasi untuk komputer Server dengan menggunakan OS Ubuntu Server 12.04 LTS.

Sekarang perhatikan terlebih dahulu gambar dibawah ini :



Gambar 3.1

Itu adalah topologi jaringan yang akan kalian bangun nanti. Dimana disitu terlihat ada sebuah komputer server yang berfungsi sebagai penyedia berbagai layanan seperti *Web Server, DNS Server,*

DHCP Server, Print Server, Mail Server, dll. Serta ada beberapa client untuk mengetes seluruh layanan dari komputer Server tersebut.

Kalian pasti bertanya-tanya, apa itu Web Server, DNS Server, DHCP, dan lain-lain? Sebelum itu kalian harus memahami terlebih dahulu apa arti kata Server itu. Server berasal dari kata *Serve*, yang artinya menyediakan. Sedangkan arti *Server* sendiri adalah penyedia. Jadi yang disebut Komputer Server adalah komputer yang berfungsi sebagai penyedia/menyediakan layanan untuk client-clientnya. Nah, Web Server, DNS, DHCP itulah layanan-layanan yang disediakan oleh komputer Server ini.

Sudah saya jelaskan juga di awal-awal bab instalasi, bahwa untuk konfigurasi komputer server ini sebaiknya kalian tidak sedang dalam keadaan terkoneksi dengan jaringan internet. Karena pada tahap instalasi di bab sebelumnya, seluruh pengaturan ip address memang ditujukan untuk pengaturan ip address secara lokal saja. Sehingga walaupun kalian memang sudah memiliki akses internet, internet tersebut saya jamin tidak akan bisa terkoneksi apabila dengan konfigurasi yang ada saat ini. Tujuannya tentu saja semata-mata hanya untuk mempermudah praktek kalian kedepannya.

3.1. Instalasi Web Server

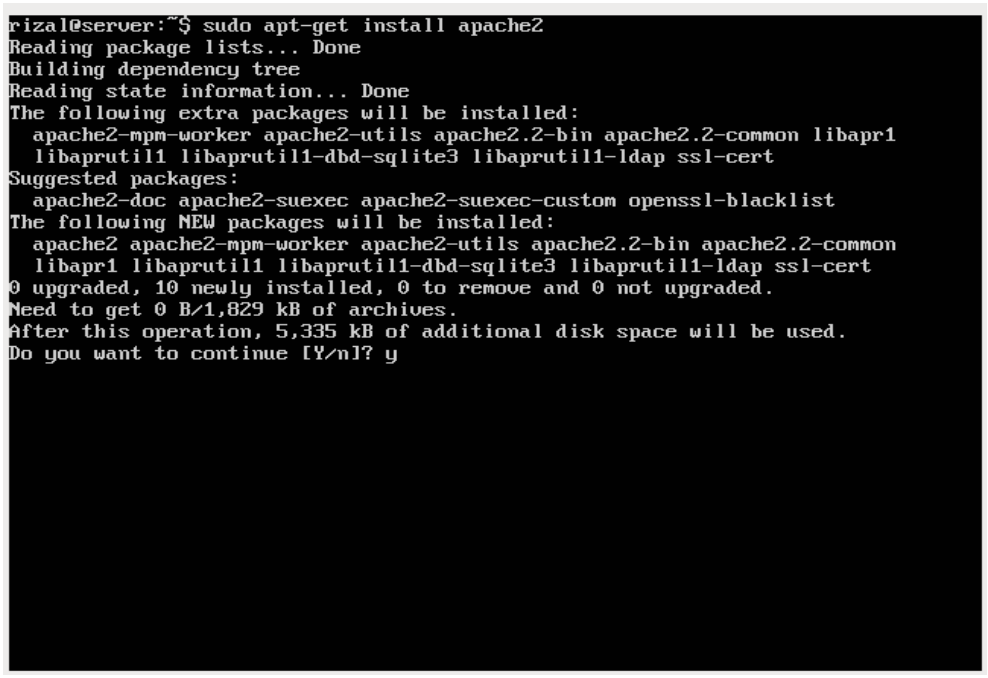
Salah satu alasan mengapa Ubuntu Server disebut sebagai sistem operasi yang tangguh dan stabil adalah karena kemampuannya dalam menjalankan layanan-layanan untuk para clientnya dengan sangat baik. Ubuntu Server dapat menjalankan semua aplikasi tersebut secara *realtime* dan *nonstop* tanpa mengalami *hang* atau *crash*. Begitu pula untuk urusan Web. Banyak server-server web yang ada di dunia menggunakan Linux sebagai OSnya karena kestabilannya itu tadi. Web Server sendiri adalah sebuah sistem yang menyediakan wadah untuk halaman web agar dapat diakses oleh client. Yaitu ketika client mengirimkan permintaan HTTP, maka Web Server akan merespon dengan mengirimkan kode-kode HTML yang akan ditampilkan oleh browser.

Instalasi Apache

Aplikasi Web Server yang terkenal adalah Apache. Apache merupakan aplikasi *free* berbasis *Open Source* yang dikenal tangguh dan sering dipakai oleh server-server di seluruh dunia. Apache sendiri sudah tersedia di DVD repositori Ubuntu Server 12.04 LTS, sehingga kalian tidak perlu lagi susah-susah mendownload Apache di Internet.

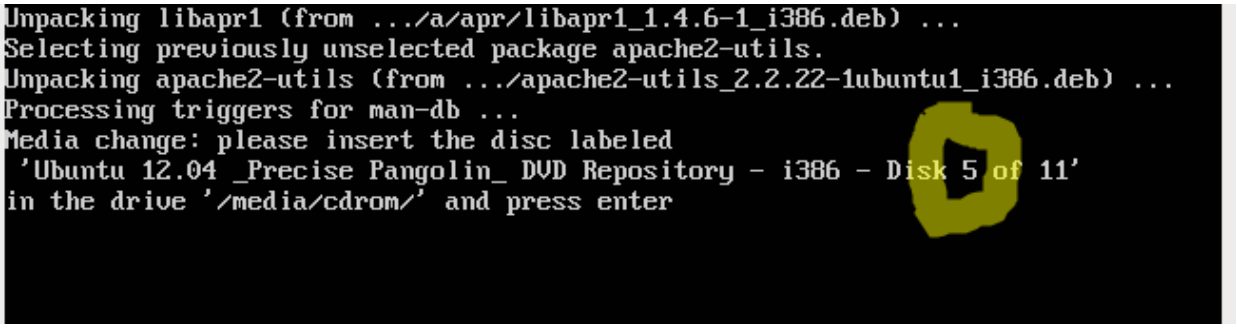
- Cara instalasinya sangat mudah cukup siapkan DVD-DVD Repositori kalian, kemudian eksekusi perintah berikut :

  ```
  sudo apt-get install apache2
  ```



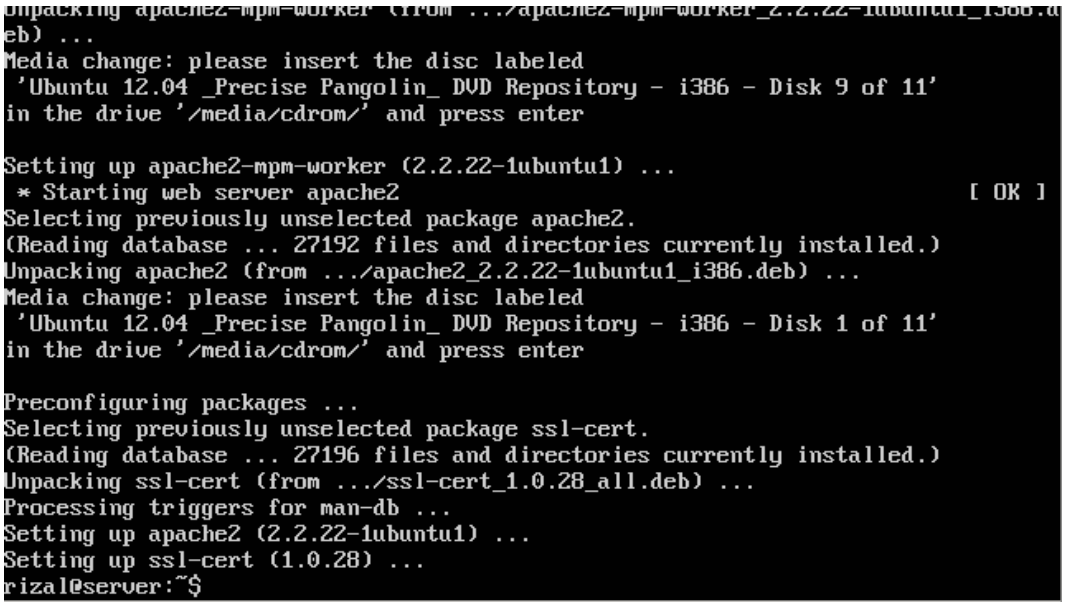
Gambar 3.1.1

- Jika muncul pesan seperti ini, itu artinya kalian harus memasukkan DVD Repositori yang lain untuk melanjutkan instalasi. Lihat pada bagian yang saya tandai dibawah ini jika kalian bingung untuk memasukkan DVD Repositori yang mana. Disitu terlihat kalian harus memasukkan DVD yang ke-5. Jika sudah, tekan Enter dan instalasi akan kembali dilanjutkan. Hal ini akan berlangsung berulang kali sampai instalasi benar-benar selesai.



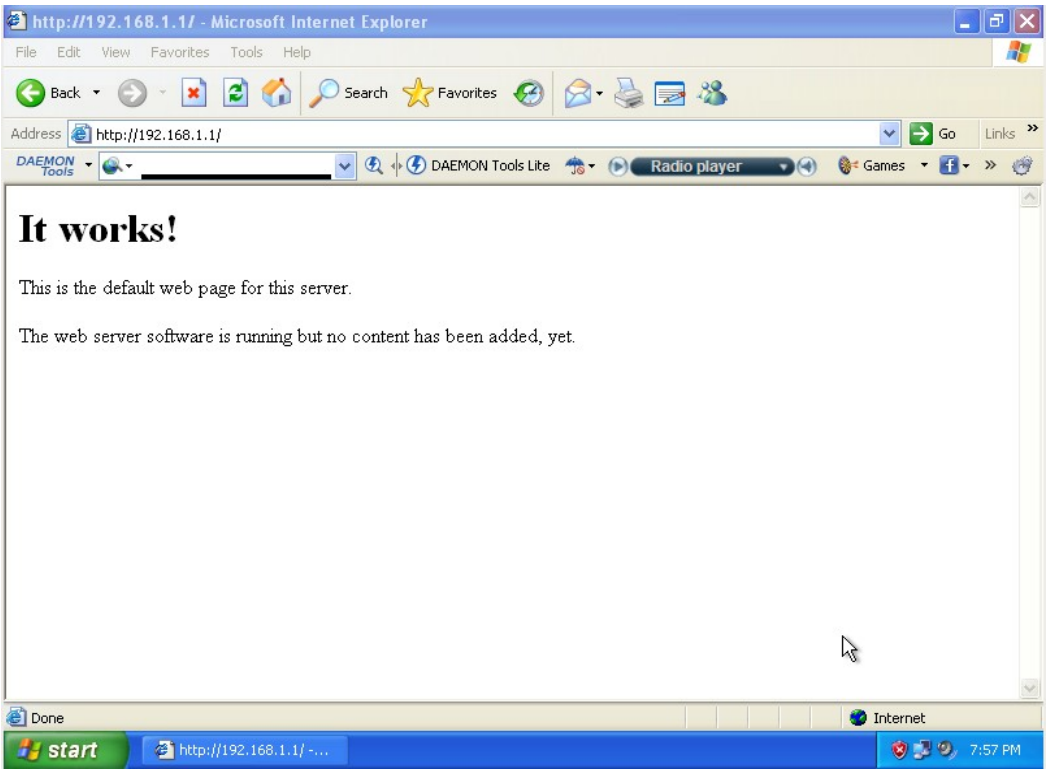
Gambar 3.1.2

- Jika tidak ada pesan kesalahan dan muncul login shell lagi seperti ini, maka instalasi Apache telah berhasil.



Gambar 3.1.3

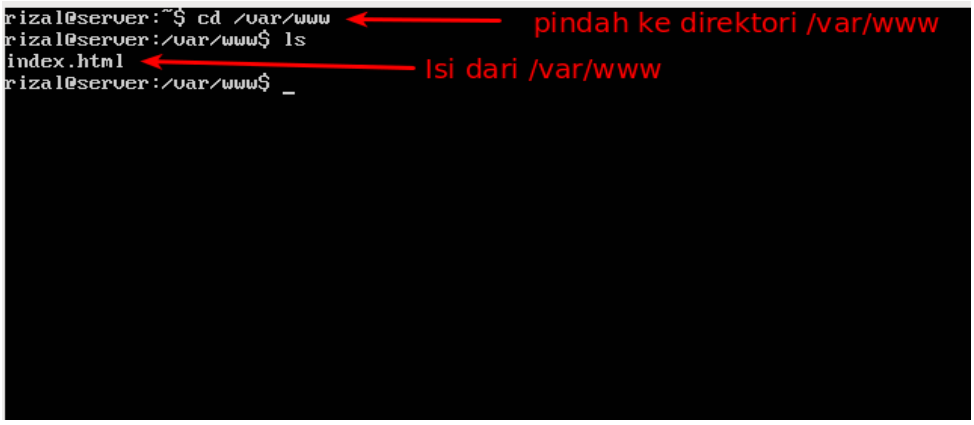
- Untuk mengetesnya, buka browser di komputer client, kemudian arahkan ke IP Address server. Jika muncul pesan **"It Works!"** seperti berikut, maka Apache telah berjalan dengan baik.



Gambar 3.1.4

- Seluruh konten dari web ini dapat kalian tambah atau edit sesuka hati kalian dengan

mengaturnya di direktori root milik Apache yaitu di **/var/www**.



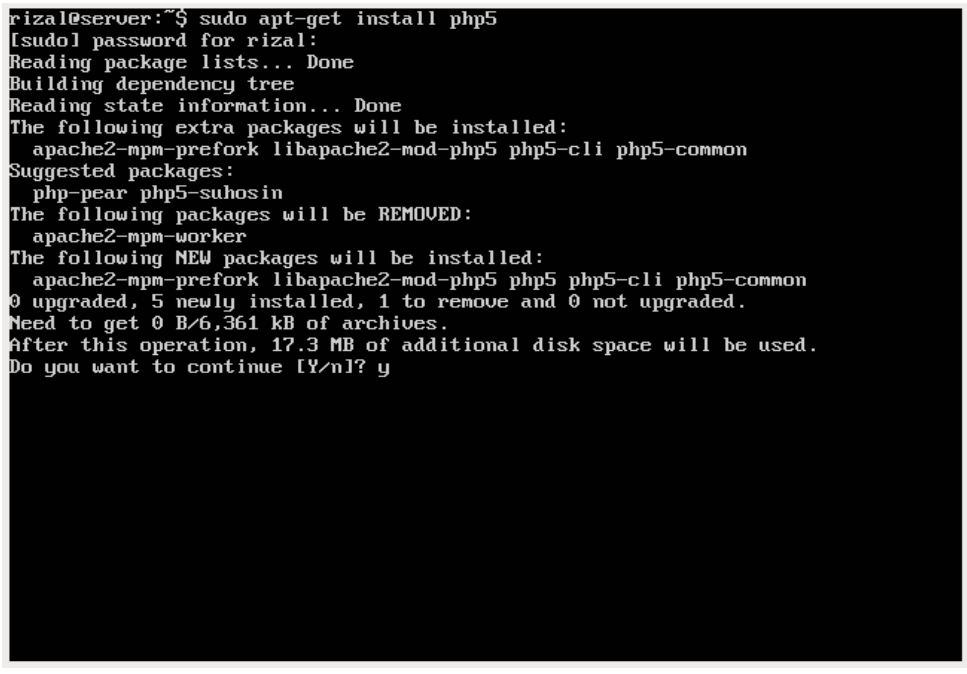
Gambar 3.1.5

Instalasi PHP5

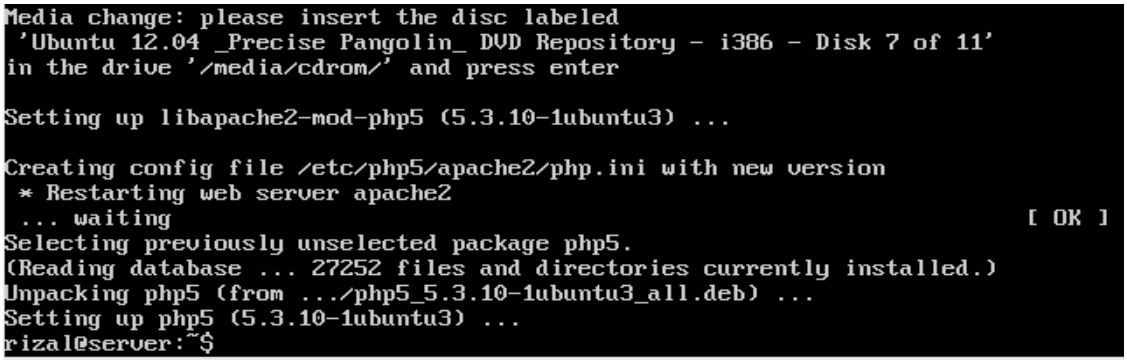
Setelah menginstall Apache, selanjutnya kalian harus menginstall PHP5. PHP adalah sebuah bahasa pemrograman web yang sangat terkenal dan sering digunakan oleh para web programmer untuk membangun website. Hampir semua website-website yang ada di Internet menggunakan PHP dalam pembuatannya. Akan tetapi secara default, Web Server Apache belum memiliki fungsi untuk dapat membaca skrip bahasa PHP ini. Oleh karena itu kita perlu menginstall layanan PHP5 agar Apache dapat membaca dan mengenali kode-kode PHP yang berekstensi .php.

- Cara installnya adalah dengan mengetikkan perintah berikut :

```
sudo apt-get install php5
```



Gambar 3.1.6



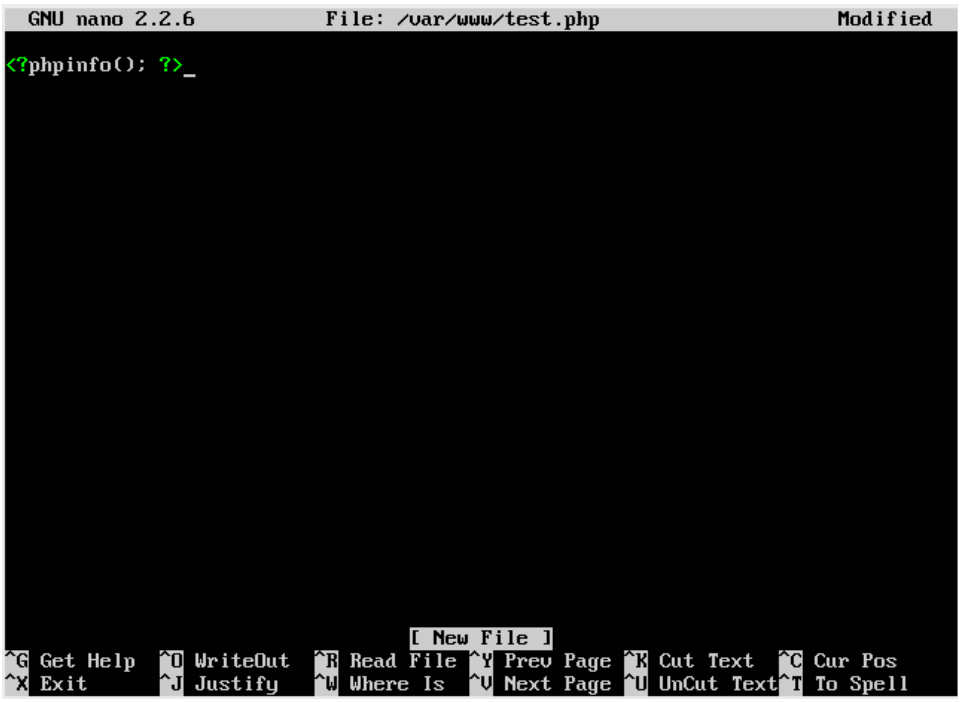
Gambar 3.1.7

- Untuk mengetes apakah PHP telah berhasil berjalan dengan baik, maka kalian perlu untuk membuat sebuah skrip PHP terlebih dahulu untuk ditampilkan di browser nanti. Silahkan eksekusi perintah berikut :

```
sudo nano /var/www/test.php
```

- Akan terbuka sebuah layar teks editor yang masih kosong, disitu kalian tambahkan kode berikut :

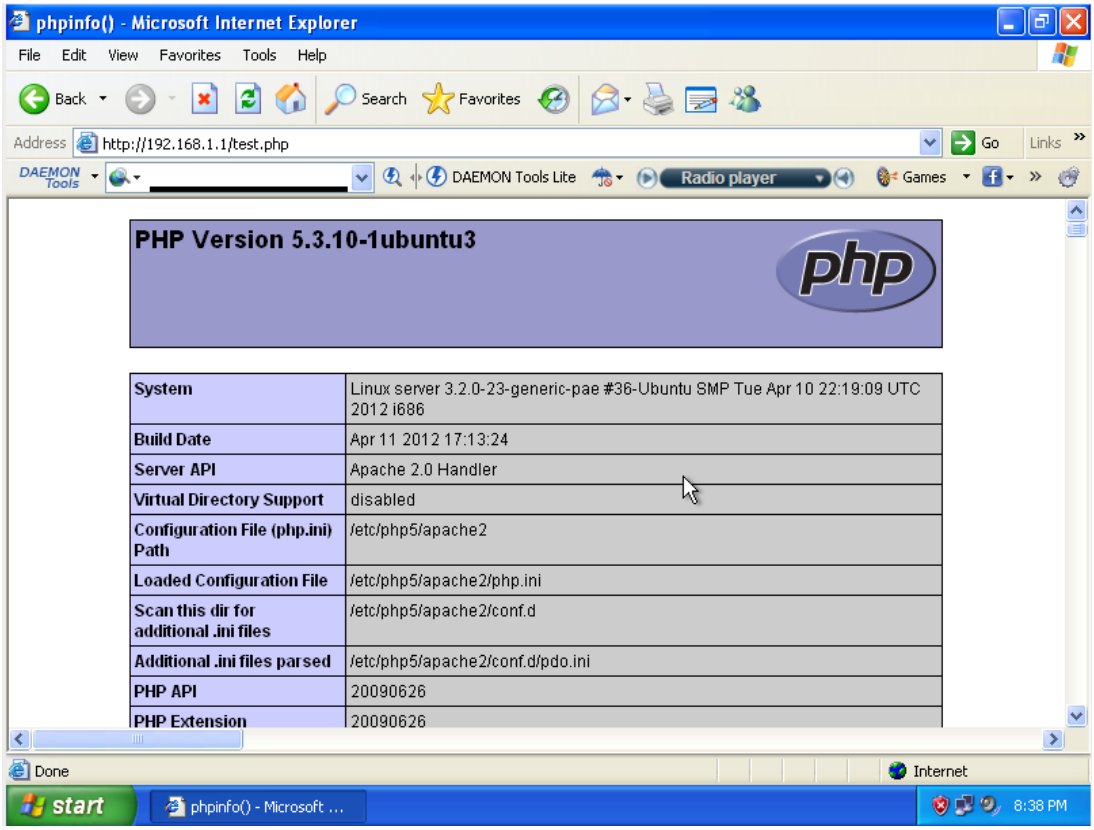
```
<?phpinfo(); ?>
```



Gambar 3.1.8

- Simpan file tersebut dengan menekan **CTRL + X**, kemudian **Y**, lalu tekan **enter**.
- Buka kembali browser client, lalu arahkan ke alamat http://192.168.1.1/test.php untuk

melihat hasilnya. Jika muncul gambar informasi PHP seperti ini, maka PHP5 telah terintegrasi dengan baik dengan web server.



Gambar 3.1.9

3.2. Instalasi Database Server

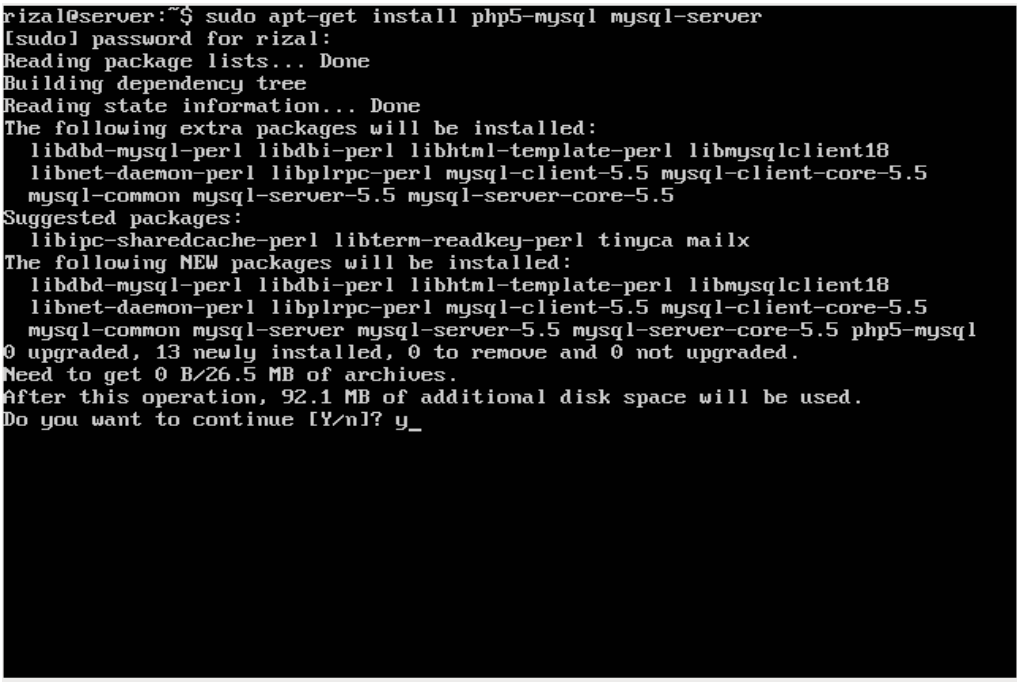
Database adalah tempat dimana kalian meletakkan file-file data yang diperlukan oleh sebuah website ataupun aplikasi. Berhubung pada saat ini hampir seluruh website sudah berwujud dinamis yang pastinya membutuhkan database, maka kalian juga perlu menginstall sebuah Database Server sebagai lanjutan dari penginstalan Web Server di pembahasan sebelumnya.

Instalasi Mysql

Aplikasi database yang cukup sering digunakan adalah Mysql dikarenakan kestabilan, kehebatannya dan yang pastinya gratis.

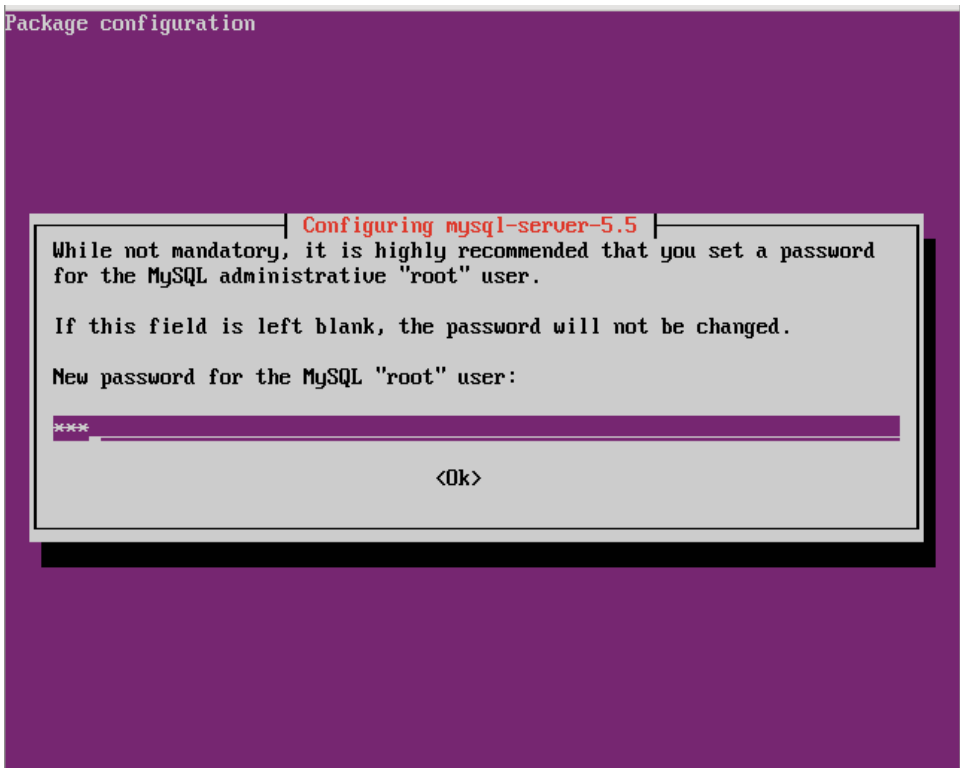
- Untuk menginstallnya cukup ketikkan perintah ini :

```
sudo apt-get install php5-mysql mysql-server
```



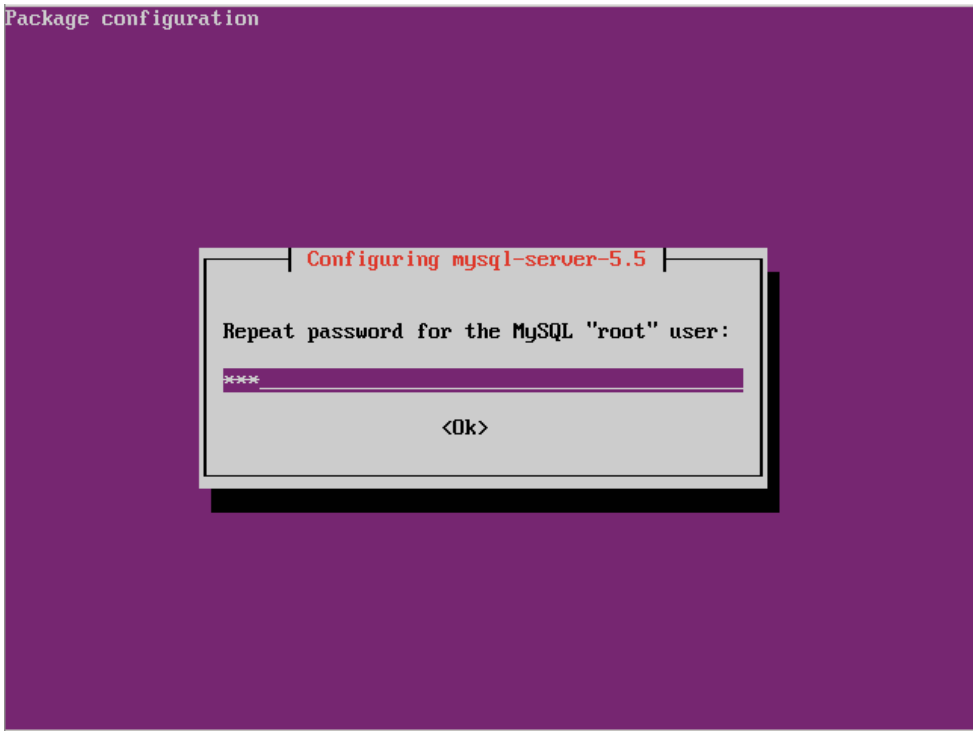
Gambar 3.2.1

- Nanti akan muncul form untuk memasukkan password seperti ini. Masukkan saja password baru untuk user root dari Mysql :



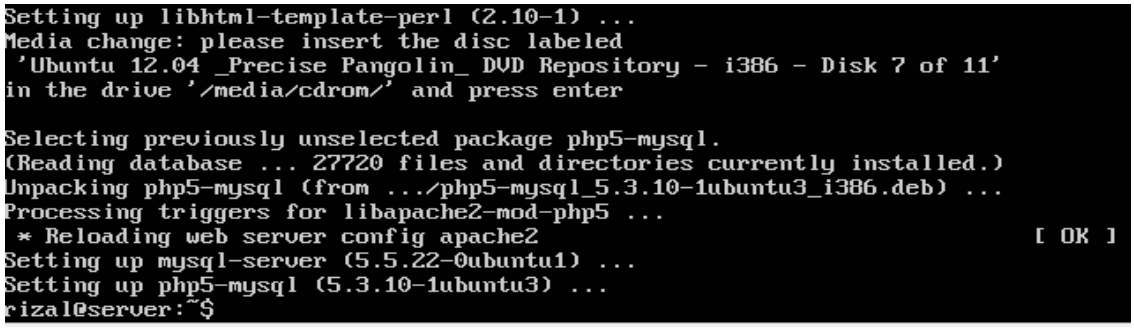
Gambar 3.2.2

- Kemudian konfirmasi lagi password yang telah kalian isikan sebelumnya :



Gambar 3.2.3

- Setelah itu tunggu hingga proses instalasi selesai, dan muncul pesan sukses seperti gambar dibawah ini.



Gambar 3.2.4

- Sampai disini, Database Mysql seharusnya sudah dapat digunakan. Namun apabila terjadi error selama proses instalasi berlangsung, atau instalasi gagal, coba ketikkan perintah ini untuk mengatasinya. Lakukan berulang-ulang hingga akhirnya proses instalasi selesai :

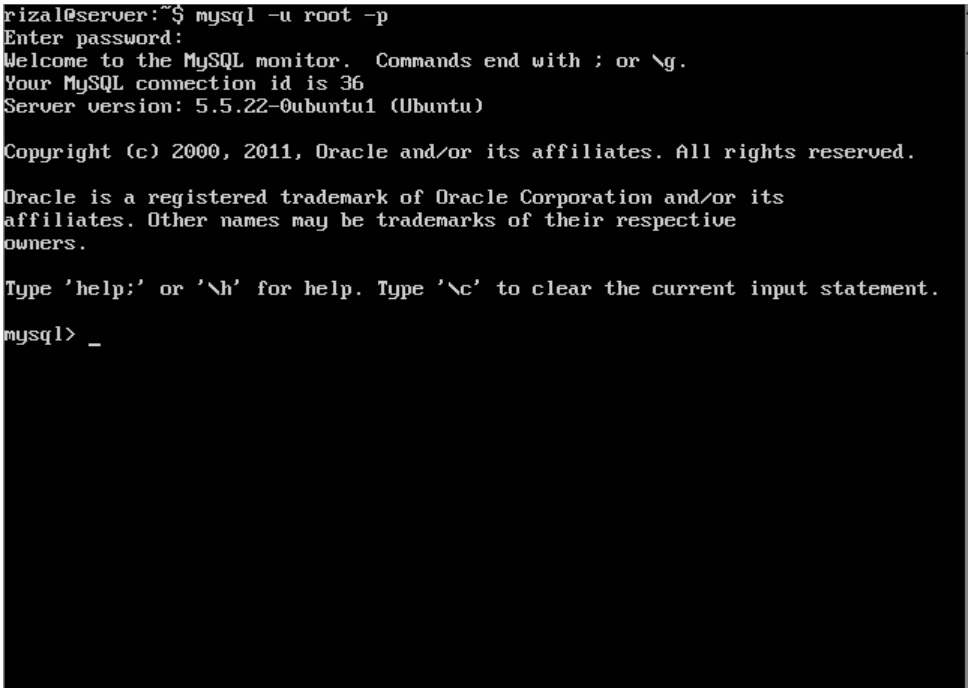
```
sudo apt-get -f install && sudo apt-get install php5-mysql mysql-server
```

- Langkah berikutnya adalah mengetes apakah Mysql memang sudah benar-benar berjalan dengan baik. Silahkan login ke Mysql dengan perintah berikut :

```
mysql -u root -p
```

- Nanti akan tampil kira-kira seperti ini :

```
rizal@server:~$ mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 37
Server version: 5.5.22-0ubuntu1 (Ubuntu)

Copyright (c) 2000, 2011, OrACLe and/or its affiliates. All rights
reserved.

OrACLe is a registered trademark of OrACLe Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input
statement.

mysql>
```



Gambar 3.2.5

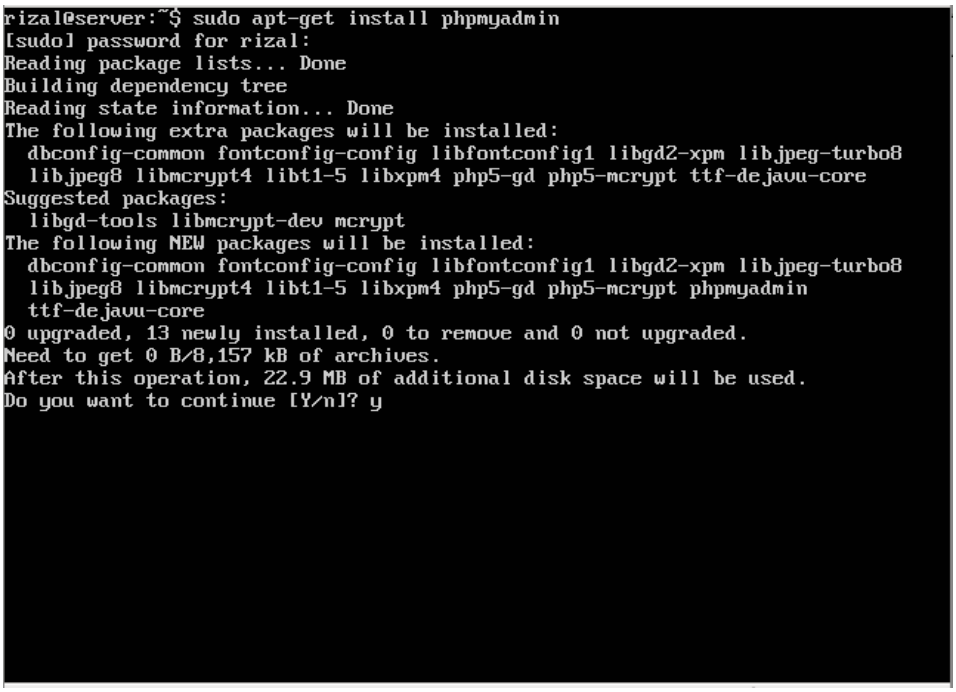
- Setelah itu tinggal kalian konfigurasikan saja Database seperti apa yang ingin kalian buat.

Instalasi Phpmyadmin

Dalam konfigurasi database, kita perlu memasukkan sintaks-sintaks tertentu yang cukup rumit dan panjang jika memang databasenya adalah database yang kompleks. Pastinya kalian tidak ingin direpotkan dengan harus menghafal maupun mengetik semua sintaks tersebut bukan? Nah untuk itulah Phpmyadmin dibuat. Phpmyadmin adalah aplikasi yang berguna untuk mengkonfigurasi database Mysql melalui antarmuka web. Dengan Phpmyadmin sintaks-sintaks yang panjang tadi akan digantikan oleh beberapa klik mouse saja.

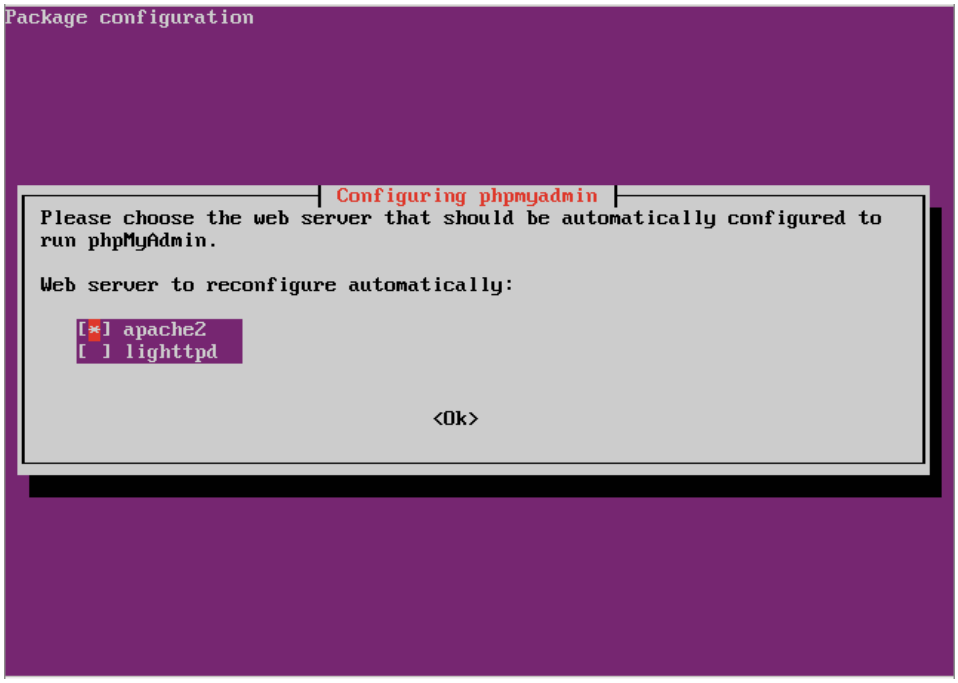
- Untuk menginstallnya ketikkan perintah ini :

```
sudo apt-get install phpmyadmin
```



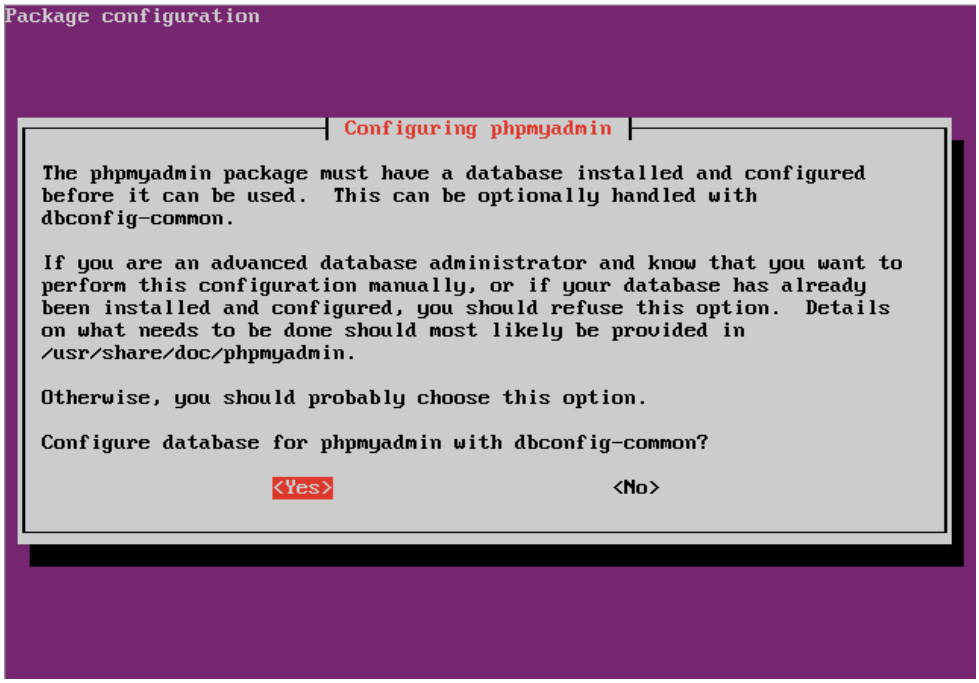
Gambar 3.2.6

- Setelah itu kalian akan ditanya Web Server mana yang ingin kalian integrasikan dengan Phpmyadmin. Pastinya kalian pilih dengan menekan tombol **Spasi** untuk mencentang pilihan Apache, lalu tekan **Enter**.



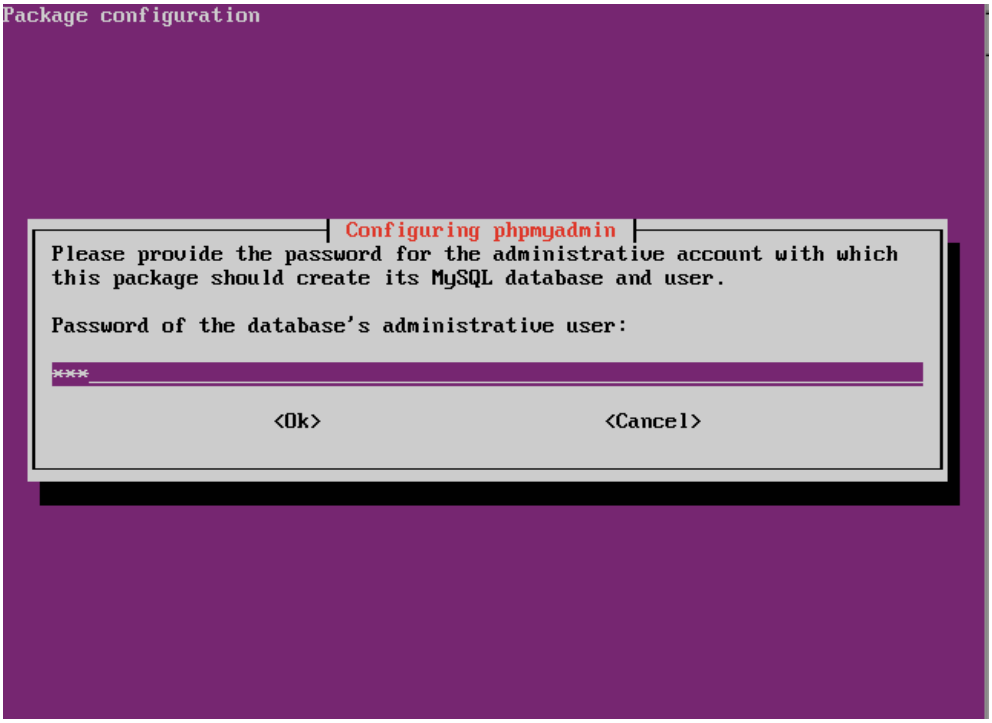
Gambar 3.2.7

- Apabila muncul tampilan seperti ini, pilih saja **Yes**.

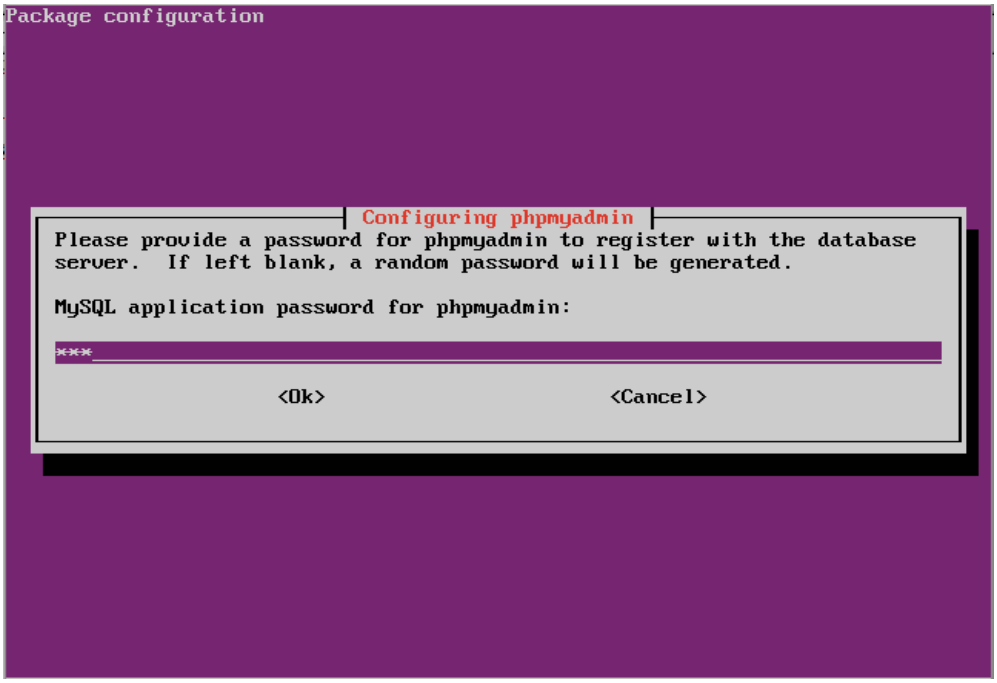


Gambar 3.2.8

- Kemudian kalian diminta untuk memasukkan kembali password root Mysql kalian yang telah kalian install sebelumnya, sebanyak tiga kali.

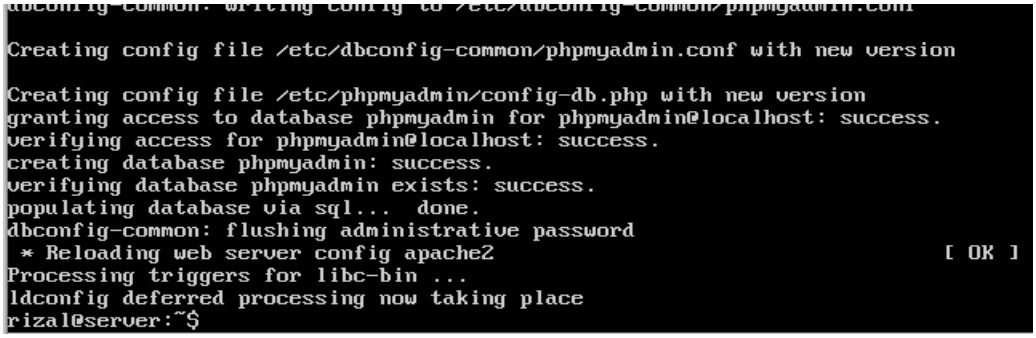


Gambar 3.2.9



Gambar 3.2.10

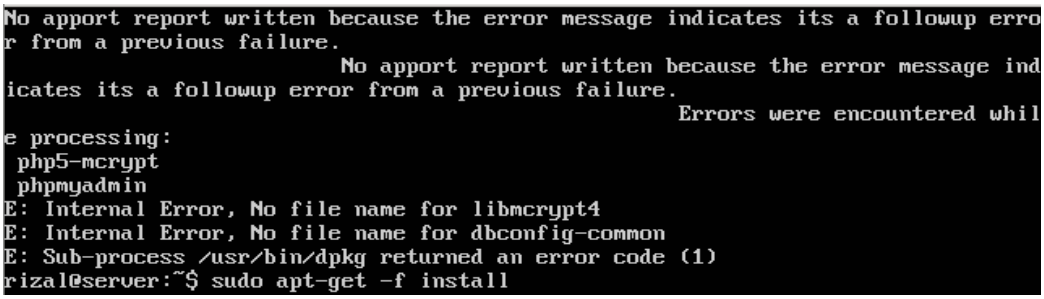
- Dan apabila tidak ada pesan error, maka akan muncul tampilan seperti ini tanda bahwa instalasi berhasil.



Gambar 3.2.11

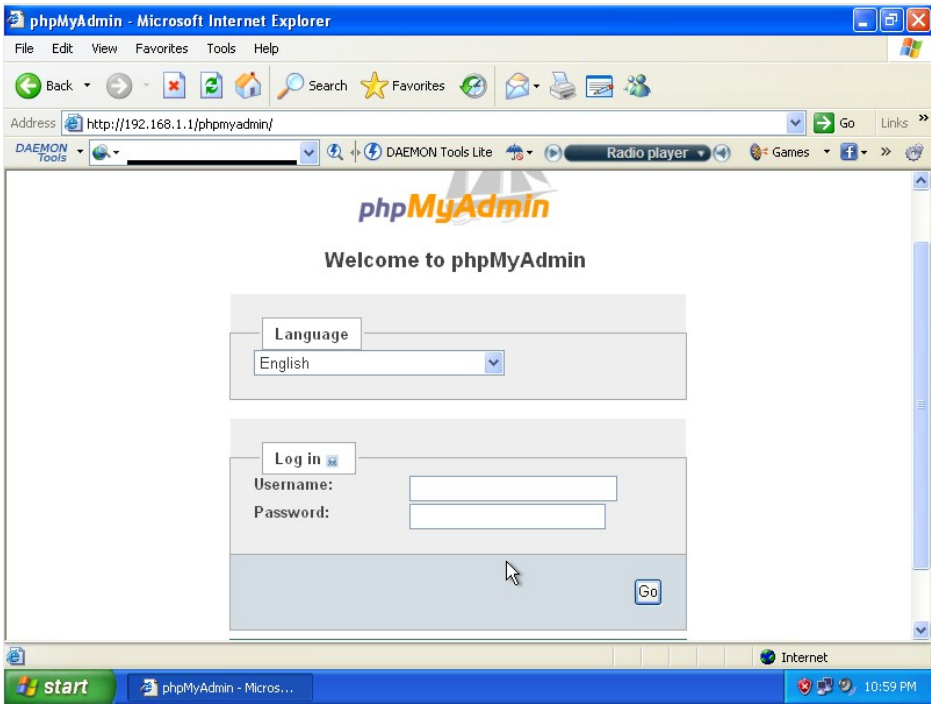
- Namun jika terjadi pesan kesalahan seperti misalnya kekurangan dependensi yang ditampilkan gambar di bawah ini, lakukan saja perintah berikut :

```
sudo apt-get -f install && sudo apt-get install phpmyadmin
```



Gambar 3.2.12

- Selanjutnya adalah tahap pengetesan. Buka browser client, dan arahkan ke alamat http://192.168.1.1/phpmyadmin



Gambar 3.2.13

- Jika kalian telah berhasil membuka halaman login Phpmyadmin seperti gambar diatas, maka kalian telah berhasil menginstalasi Database Server dengan baik.

3.3. Instalasi DNS Server

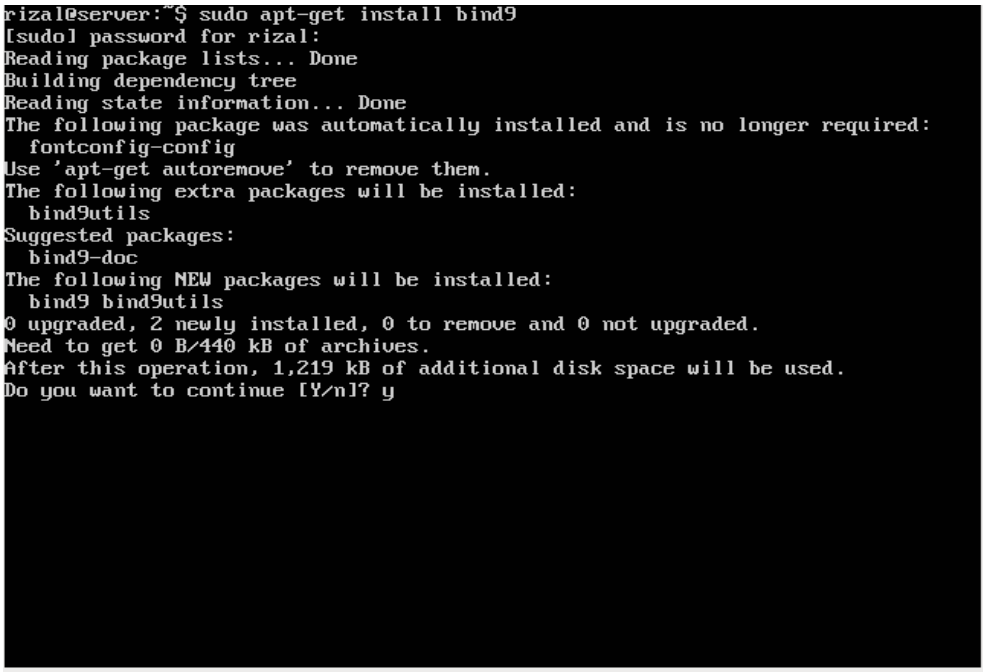
DNS atau Domain Name System, adalah sebuah server yang berfungsi menangani translasi penamaan host-host kedalam IP Address, begitu juga sebaliknya dalam menangani translasi dari IP Address ke Hostname/Domain. Dalam dunia internet, komputer berkomunikasi satu sama lain dengan mengenali IP Address-nya, bukan domainnya. Akan tetapi, manusia jauh lebih sulit dalam mengingat angka-angka dibanding dengan huruf. Contohnya saja, lebih mudah mana mengetikkan alamat ip 118.98.36.20 di browser dibandingkan dengan mengetik domain www.google.com saja? Tentunya lebih mudah mengingat yang www.google.com bukan? Untuk itulah DNS Server dibuat, dimana alamat IP akan diubah menjadi domain, begitu pula sebaliknya.

Instalasi Bind9

Aplikasi DNS yang sering digunakan di Linux adalah Bind9. Bind9 cukup banyak digunakan oleh komputer-komputer di seluruh dunia dalam mengimplementasikan DNS Server.

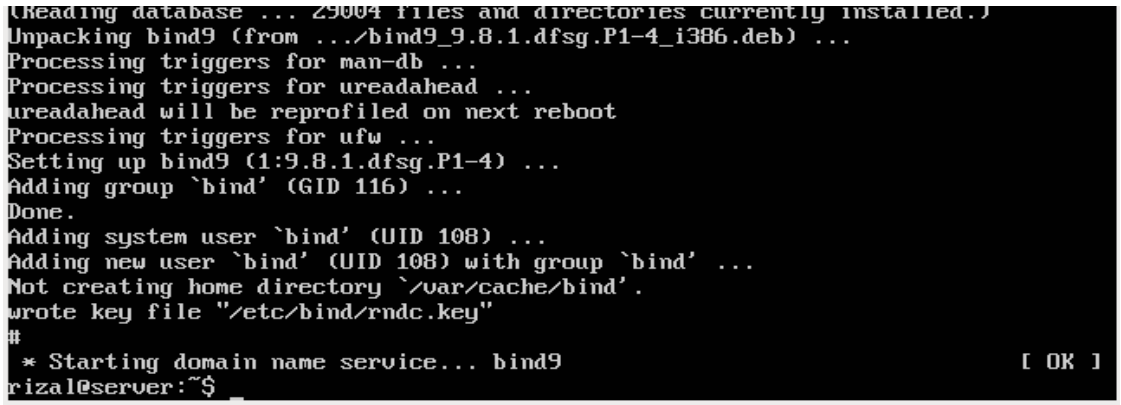
- Untuk menginstallnya di Ubuntu Server 12.04 LTS, cukup eksekusi perintah berikut :

```
sudo apt-get install bind9
```



Gambar 3.3.1

- Tunggu hingga proses instalasi selesai seperti yang terlihat pada gambar dibawah.



Gambar 3.3.2

- Jika tidak ada pesan error, maka instalasi Bind9 telah selesai dan siap di konfigurasi.

Konfigurasi Bind9

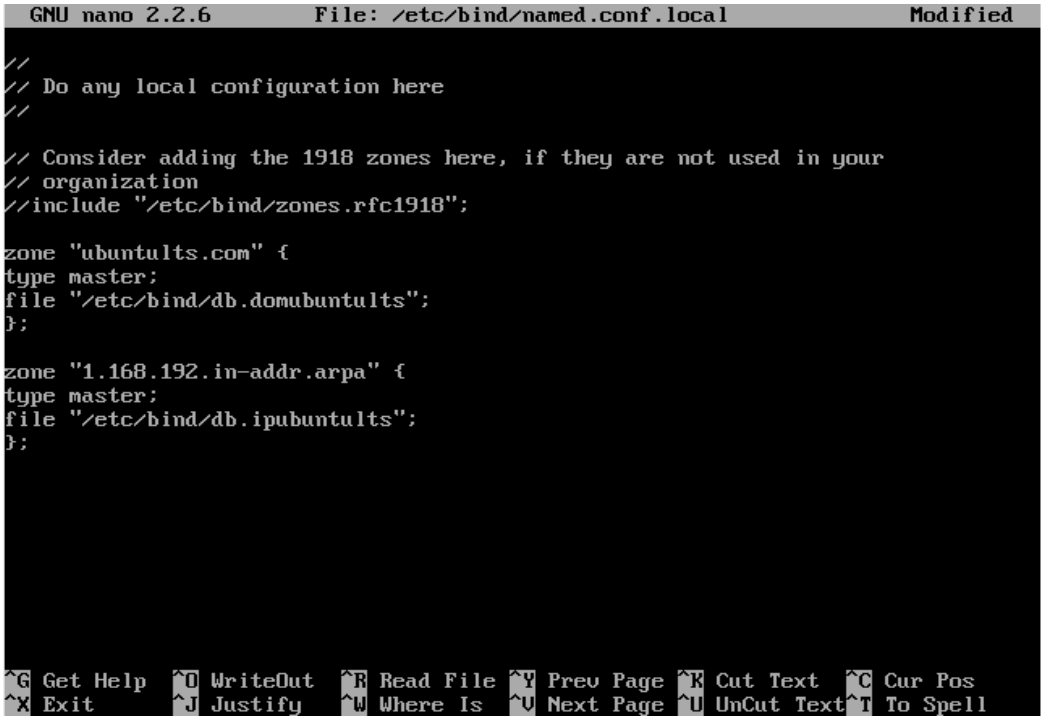
Dalam mengkonfigurasi Bind9, ada 3 buah file yang perlu kalian edit, yaitu **/etc/bind/named.conf.local**, **/etc/bind/db.domubuntults**, dan **/etc/bind/db.ipubuntults**. Disini kalian akan menggunakan domain **ubuntults.com** yang akan ditranslasikan dari ip address **192.168.1.1** sesuai dengan konfigurasi domain yang kalian isi saat bab instalasi.

- Pertama-tama ketikkan perintah berikut untuk mengedit file **/etc/bind/named.conf.local** :

```
sudo nano /etc/bind/named.conf.local
```

- Akan muncul sebuah file, lalu tambahkan script ini setelah baris **//include "/etc/bind/zones.rfc1918";** :

```
zone "ubuntults.com" {
type master;
file "/etc/bind/db.domubuntults";
};

zone "1.168.192.in-addr.arpa" {
type master;
file "/etc/bind/db.ipubuntults";
};
```



Gambar 3.3.3

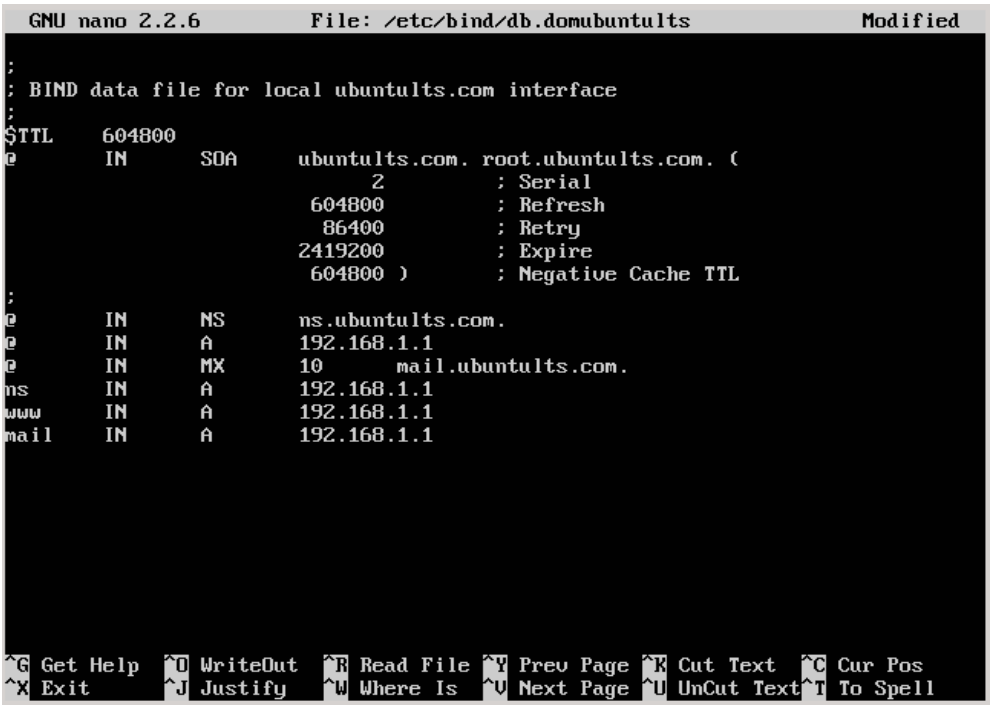
- Simpan perubahan dengan menekan **CTRL + X**, lalu tekan **Y**, lalu **Enter**.
- Setelah itu edit file yang kedua, yaitu **/etc/bind/db.domubuntults** dengan cara :

```
sudo nano /etc/bind/db.domubuntults
```

- Akan muncul sebuah file kosong, kemudian kopikan seluruh script ini kedalamnya :

```
;
; BIND data file for local ubuntults.com interface
;
$TTL    604800
@       IN      SOA     ubuntults.com. root.ubuntults.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns.ubuntults.com.
@       IN      A       192.168.1.1
@       IN      MX      10    mail.ubuntults.com.
```

```
ns      IN      A       192.168.1.1
www     IN      A       192.168.1.1
mail    IN      A       192.168.1.1
```



Gambar 3.3.4

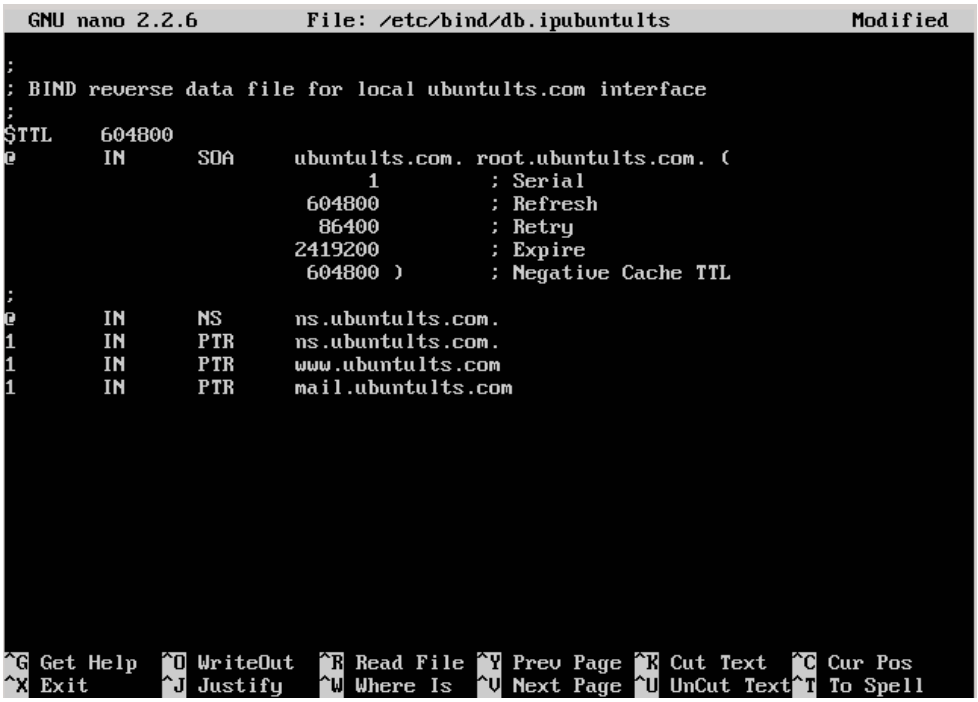
- Simpan perubahan dengan menekan **CTRL + X**, lalu tekan **Y**, lalu **Enter**.
- Langkah selanjutnya adalah mengedit file **/etc/bind/db.ipubuntults** dengan mengeksekusi perintah berikut :

```
sudo nano /etc/bind/db.ipubuntults
```

- Akan muncul sebuah file kosong juga, kalian isikan saja script dibawah ini kedalamnya :

```
;
; BIND reverse data file for local ubuntults.com interface
;
$TTL    604800
@       IN      SOA     ubuntults.com. root.ubuntults.com. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
```

```
;
@       IN      NS      ns.ubuntults.com.
1       IN      PTR     ns.ubuntults.com.
1       IN      PTR     www.ubuntults.com
1       IN      PTR     mail.ubuntults.com
```



Gambar 3.3.5

- Simpan perubahan dengan menekan **CTRL + X**, lalu tekan **Y**, lalu **Enter**.
- Yang terakhir kalian harus merestart service dari Bind9 ini agar seluruh konfigurasi diatas dapat berjalan. Untuk merestartnya, ketikkan perintah berikut :

  ```
  sudo /etc/init.d/bind9 restart
  ```

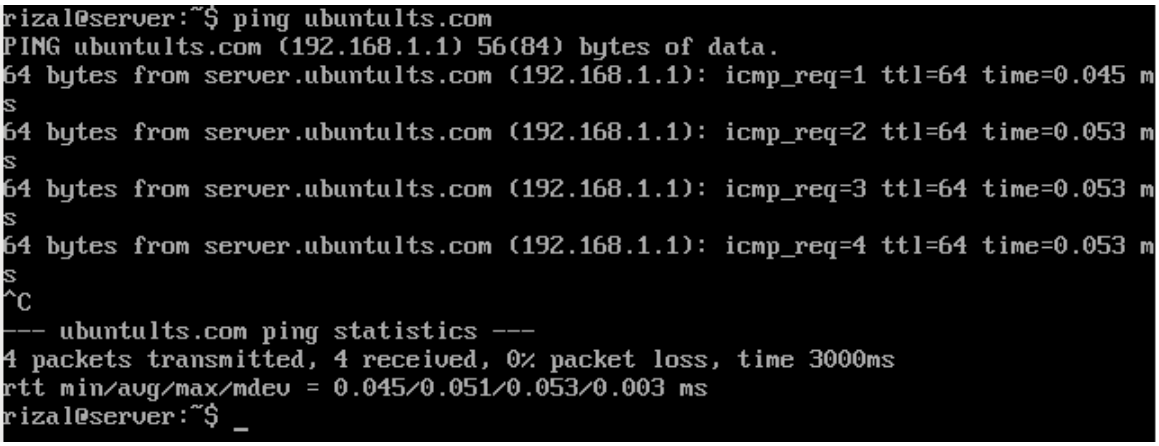
- Pastikan muncul pesan **OK** dan tidak ada pesan Failed sama sekali seperti ini :

  ```
  rizal@server:~$ sudo /etc/init.d/bind9 restart
  [sudo] password for rizal:
  * Stopping domain name service... bind9
  waiting for pid 1617 to die
                                                                    [ OK ]
  * Starting domain name service... bind9                           [ OK ]
  rizal@server:~$
  ```

Gambar 3.3.6

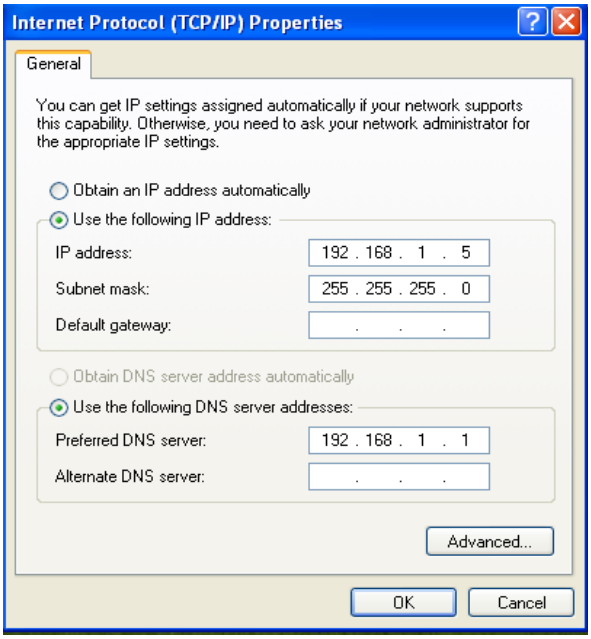
- Sekarang coba lakukan tes ping ke domain **ubuntults.com** untuk mengetahui apakah DNS telah berjalan dengan baik, pastikan seluruh paket mendapatkan *reply* seperti gambar dibawah :

  ```
  ping ubuntults.com
  ```



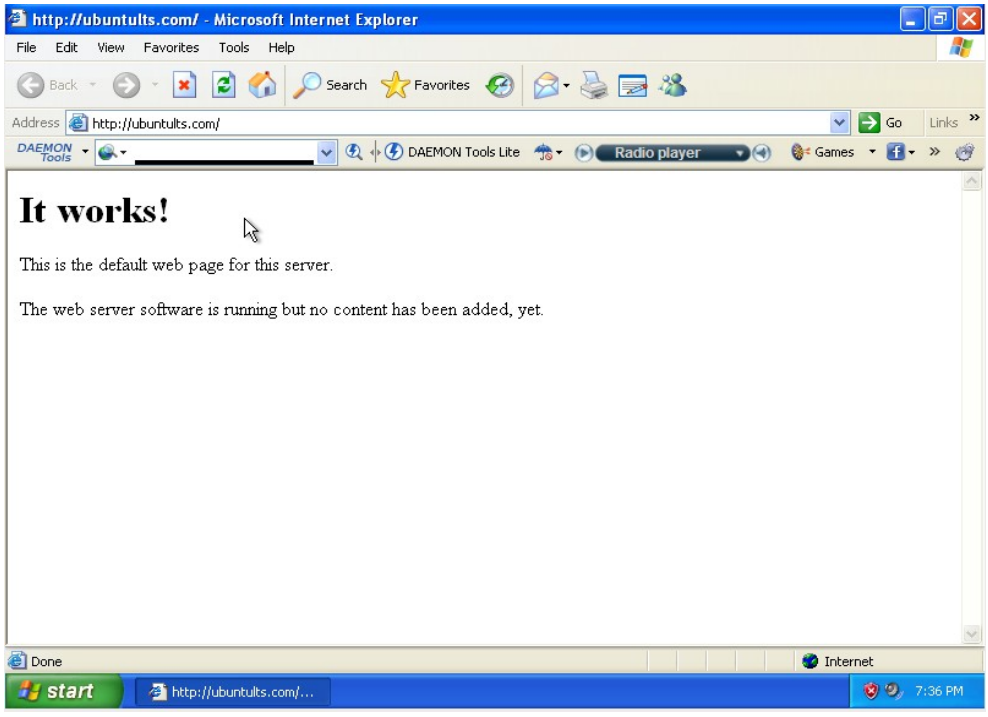
Gambar 3.3.6

- Untuk uji coba pada sisi client, kalian dapat mengetes apakah terbuka atau tidak website yang telah kalian install pada subbab Web Server, ketika kalian melakukan browsing ke alamat **ubuntults.com** atau **www.ubuntults.com**.
- Pertama-tama atur terlebih dahulu konfigurasi TCP/IP nya agar menggunakan alamat DNS server 192.168.1.1 seperti yang terlihat pada gambar dibawah :



Gambar 3.3.7

- Setelah itu arahkan browser kalian ke alamat domain http://**www.ubuntults.com**. Jika berhasil, maka akan muncul tampilan yang sama persis seperti saat kalian membuka alamat http://192.168.1.1.



Gambar 3.3.8

- Cara diatas sebenarnya hanya segelintir cara dari mengkonfigurasi DNS Server. Masih banyak lagi script-script konfigurasi lainnya dalam penerapan DNS Server yang *real*.

Namun saya harap dengan ini setidaknya kalian sudah sedikit mendapatkan gambaran mengenai apa itu DNS Server dan bagaimana implementasinya.

3.4. Instalasi DHCP Server

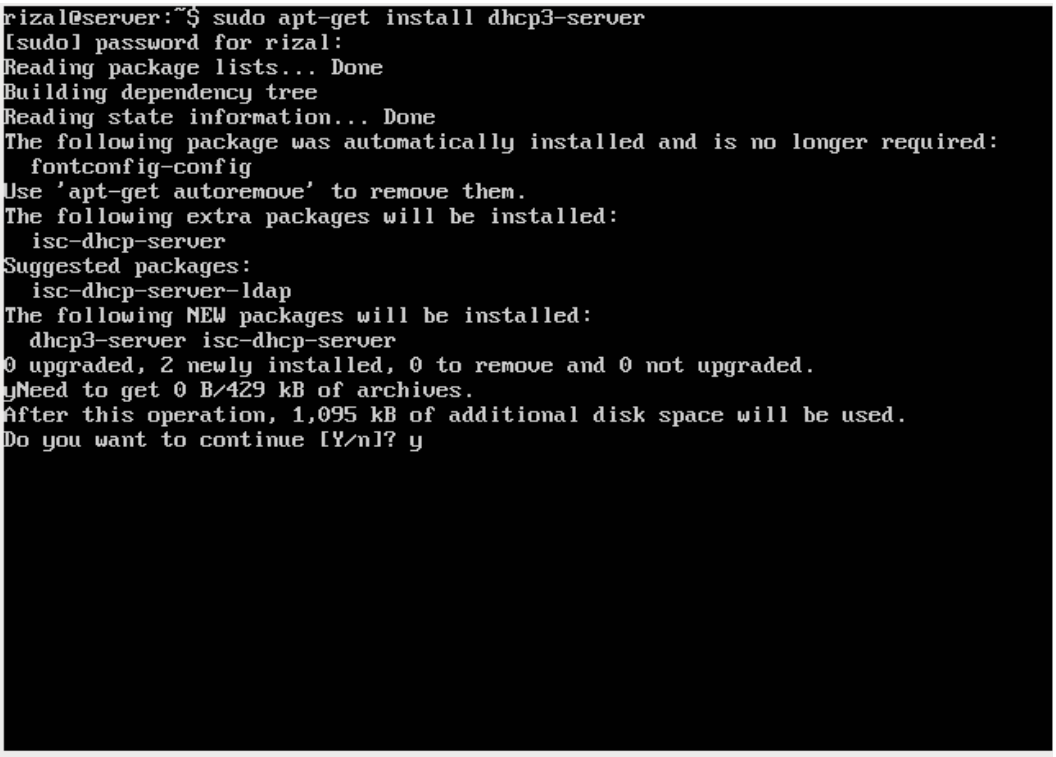
DHCP (Dynamic Host Configuration Protocol) adalah sebuah layanan yang memberikan nomor IP secara otomatis kepada komputer yang memintanya (client). Komputer yang memberikan layanan inilah yang disebut DHCP Server. Keuntungan dari layanan DHCP adalah dimana komputer-komputer client tidak perlu lagi untuk mengkonfigurasi IP Address secara manual. DHCP paling sering digunakan didalam jaringan-jaringan yang berskala besar.

Instalasi DHCP3-Server

Aplikasi DHCP Server yang sering digunakan di Ubuntu Server adalah DHCP3-Server. Cara instalasinya cukup mudah, seperti yang ditunjukkan langkah-langkah berikut :

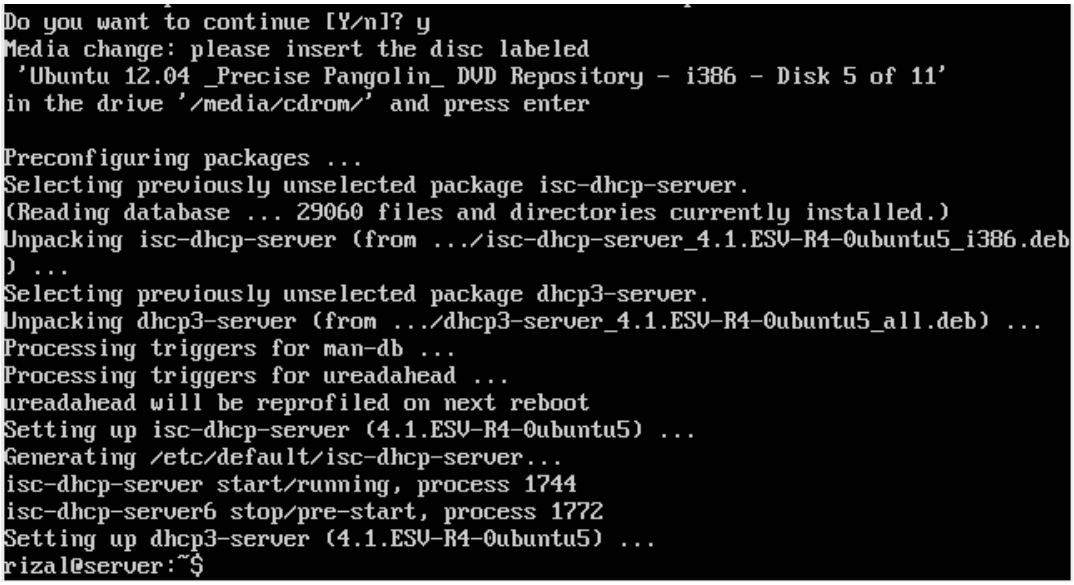
- Pertama-tama eksekusi perintah ini untuk menginstall DHCP3-Server :

```
sudo apt-get install dhcp3-server
```



Gambar 3.4.1

- Tunggu hingga proses instalasi selesai seperti yang ditunjukkan gambar dibawah ini :



Gambar 3.4.2

- Jika tidak terdapat pesan kesalahan, maka selanjutnya kalian tinggal mengkonfigurasi DHCP Server tersebut agar dapat berfungsi dengan baik.

Konfigurasi DHCP3-Server

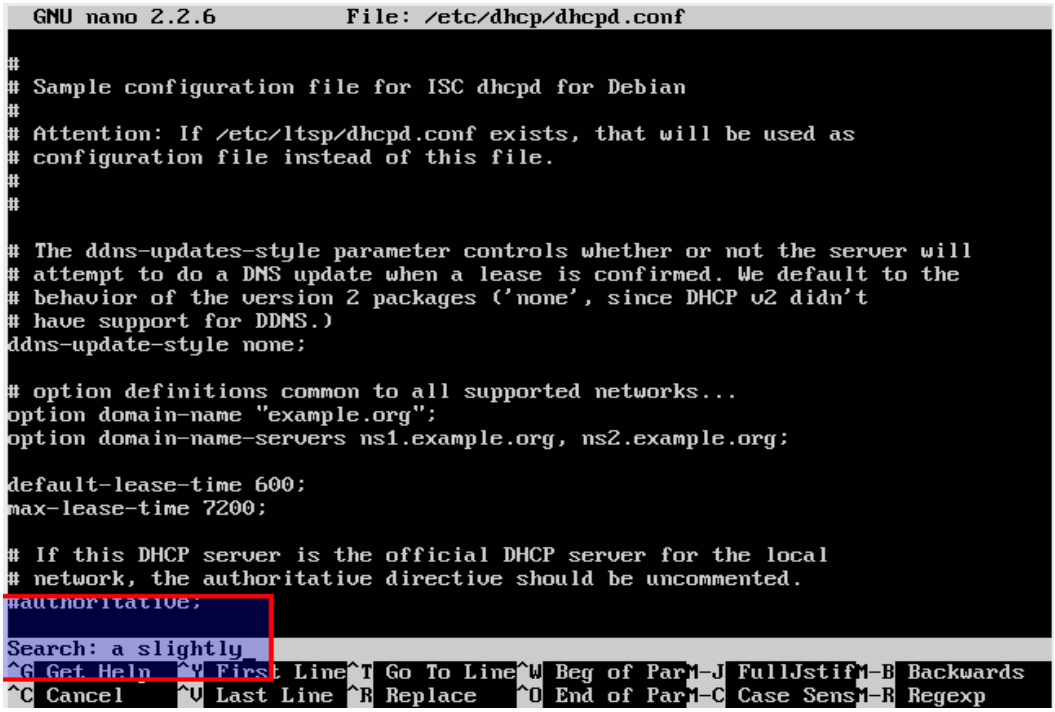
File konfigurasi utama dari DHCP3-Server berada di **/etc/dhcp/dhpcd.conf**. Kalian cukup mengedit satu file ini saja jika ingin melakukan suatu konfigurasi terhadap DHCP Server.

Contoh konfigurasi yang akan kalian terapkan disini adalah, dimana nanti DHCP Server akan memberikan IP Address untuk client dengan *range* IP dari **192.168.1.101** hingga **192.168.1.254**, memberikan IP **192.168.1.1**, **8.8.8.8**, **8.8.4.4** sebagai alamat DNS lokal maupun internet, dan juga memberikan alamat Gateway dengan IP **192.168.1.100** sesuai dengan pengaturan pada saat bab instalasi.

- Langsung saja, pertama-tama buka file **/etc/dhcp/dhcpd.conf** dengan perintah berikut :

```
sudo nano /etc/dhcp/dhcpd.conf
```

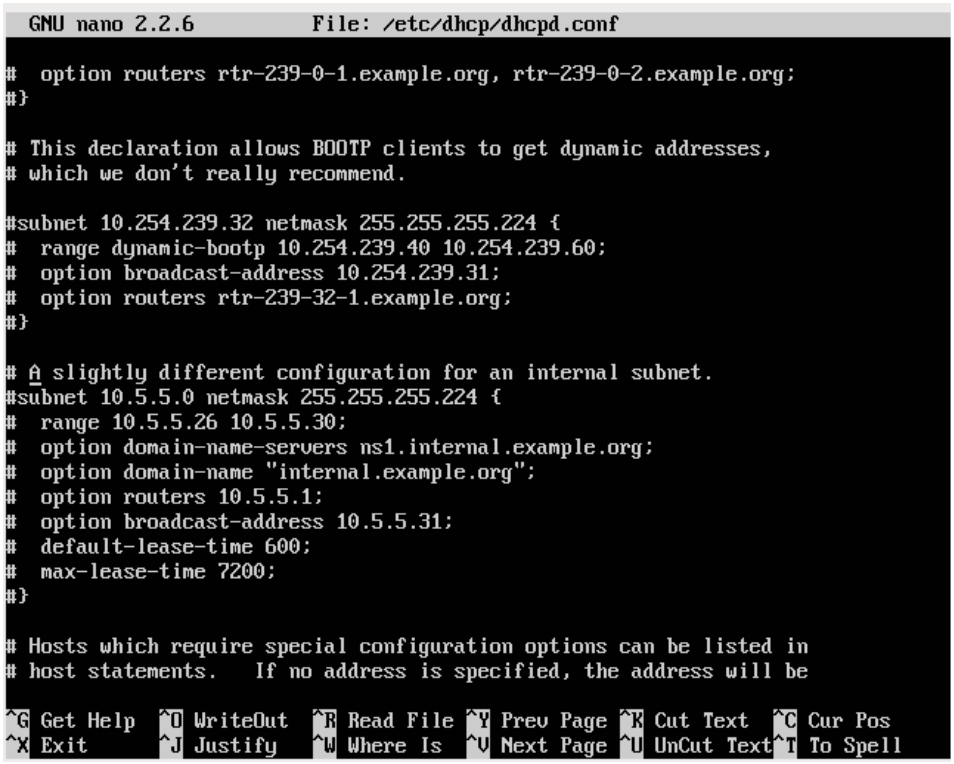
- Setelah file tersebut terbuka, kalian akan melihat begitu banyak baris konfigurasi disitu. Sebagai dasar, kalian cukup mengkonfigurasi yang sederhana saja. Carilah baris **a slightly** dengan menekan **CTRL + W** dan ketikkan **a slightly** pada teks pencarian seperti yang terlihat pada gambar dibawah ini :



Gambar 3.4.3

- Silahkan tekan **Enter**, maka kalian akan menemukan baris konfigurasi ini :

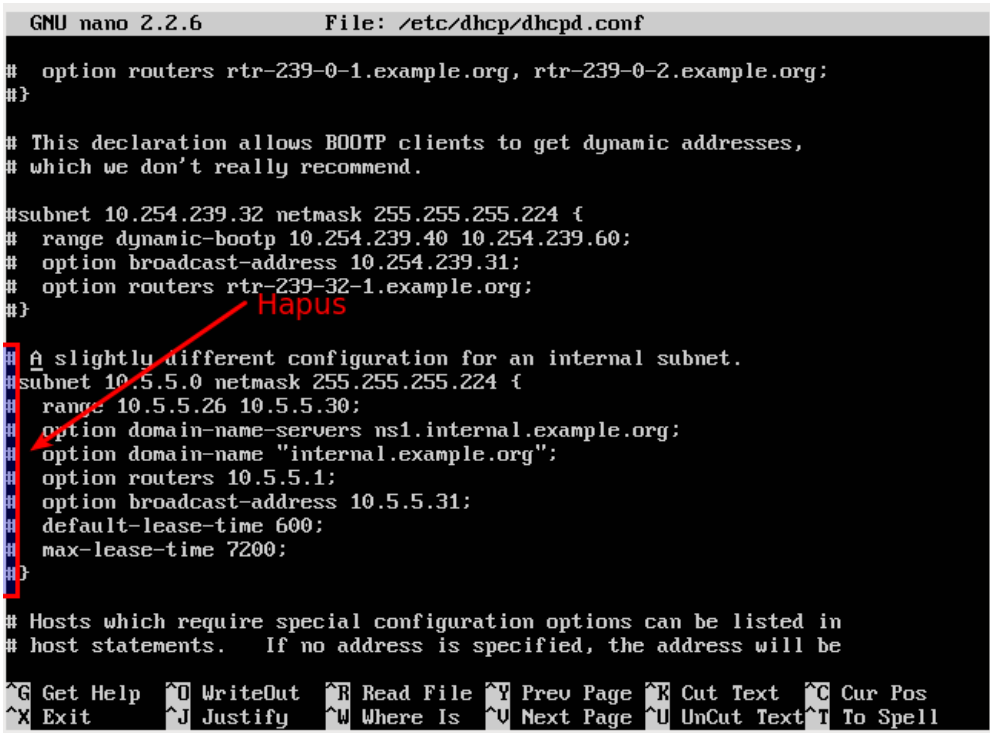
```
# A slightly different configuration for an internal subnet.
#subnet 10.5.5.0 netmask 255.255.255.224 {
#  range 10.5.5.26 10.5.5.30;
#  option domain-name-servers ns1.internal.example.org;
#  option domain-name "internal.example.org";
#  option routers 10.5.5.1;
#  option broadcast-address 10.5.5.31;
#  default-lease-time 600;
#  max-lease-time 7200;
#}
```



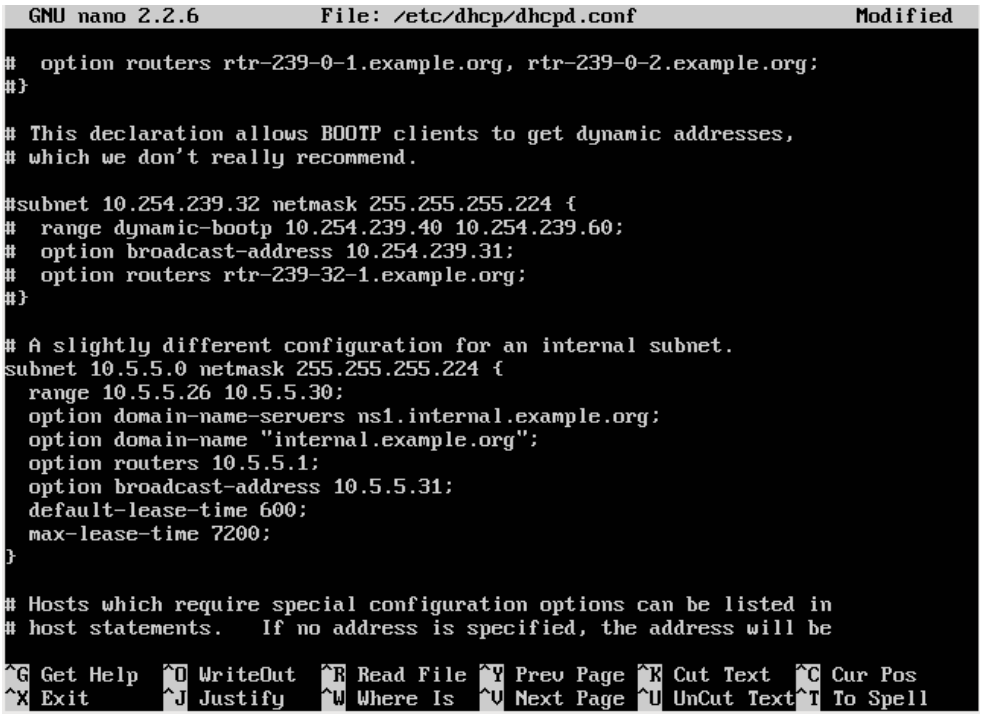
Gambar 3.4.4

- Langkah selanjutnya adalah menghapus tanda pagar (#) yang ada di depan baris **subnet 10.5.5.0 netmask 255.255.255.224 {**, sampai baris **}** sehingga kodenya hanya akan tersisa seperti ini :

```
# A slightly different configuration for an internal subnet.
subnet 10.5.5.0 netmask 255.255.255.224 {
  range 10.5.5.26 10.5.5.30;
  option domain-name-servers ns1.internal.example.org;
  option domain-name "internal.example.org";
  option routers 10.5.5.1;
  option broadcast-address 10.5.5.31;
  default-lease-time 600;
  max-lease-time 7200;
}
```



Gambar 3.4.5

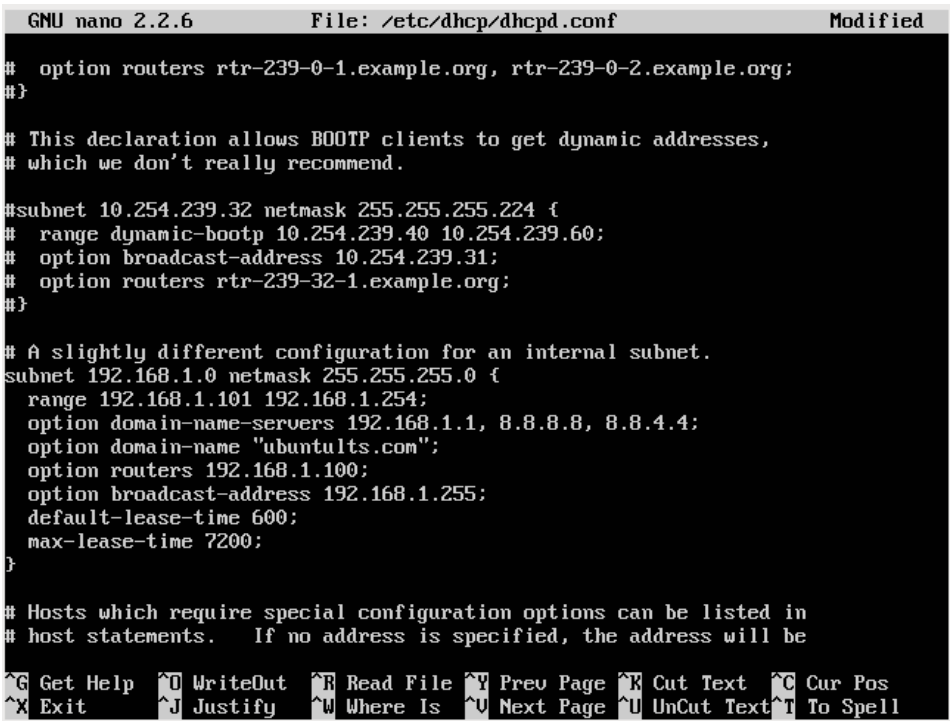


Gambar 3.4.6

- Setelah semua tanda pagar terhapus, sekarang ganti baris-baris tersebut dengan kode dibawah ini :

```
# A slightly different configuration for an internal subnet.
```

```
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.101 192.168.1.254;
  option domain-name-servers 192.168.1.1, 8.8.8.8, 8.8.4.4;
  option domain-name "ubuntults.com";
  option routers 192.168.1.100;
  option broadcast-address 192.168.1.255;
  default-lease-time 600;
  max-lease-time 7200;
}
```



Gambar 3.4.7

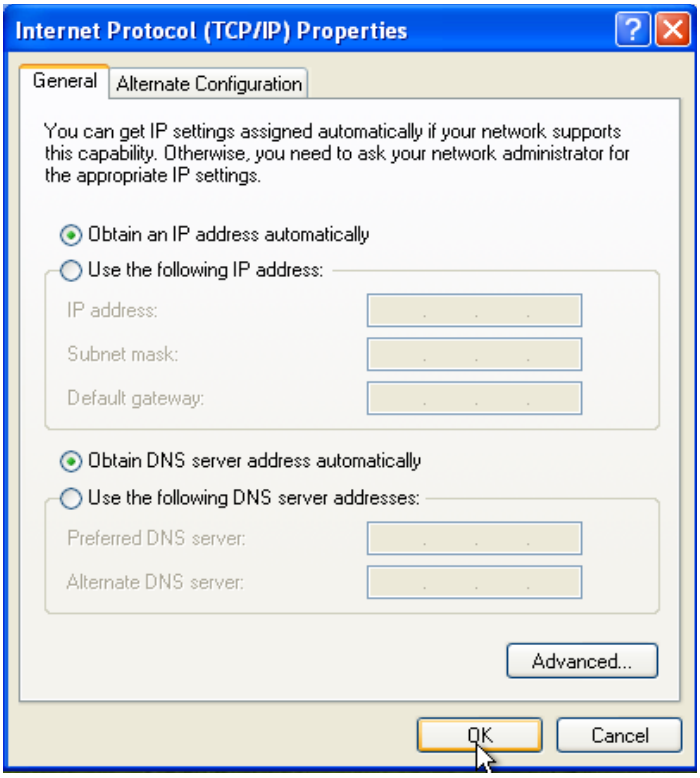
- Simpan perubahan dengan menekan **CTRL + X**, tekan **Y**, lalu tekan **Enter**.
- Kemudian restart layanan dari DHCP3-Server dengan mengeksekusi perintah berikut :

```
sudo service isc-dhcp-server restart
```

```
rizal@server:~$ sudo service isc-dhcp-server restart
[sudo] password for rizal:
stop: Unknown instance:
isc-dhcp-server start/running, process 2152
rizal@server:~$ _
```

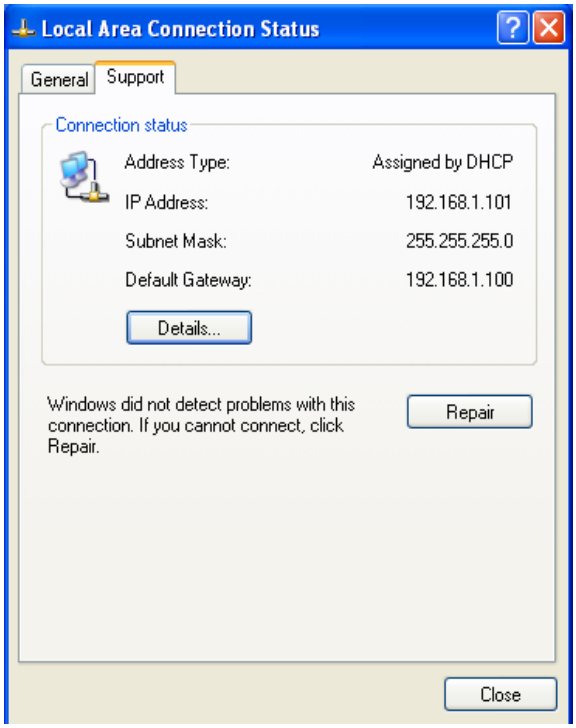
Gambar 3.4.8

- Untuk mengecek apakah layanan DHCP Server telah berfungsi dengan baik, bukalah komputer client, kemudian atur konfigurasi TCP/IP nya agar menjadi otomatis seperti yang terlihat pada gambar :



Gambar 3.4.9

- Setelah itu pastikan bahwa client telah berhasil mendapatkan IP Address secara otomatis dari DHCP Server yang bisa dilihat pada gambar dibawah :



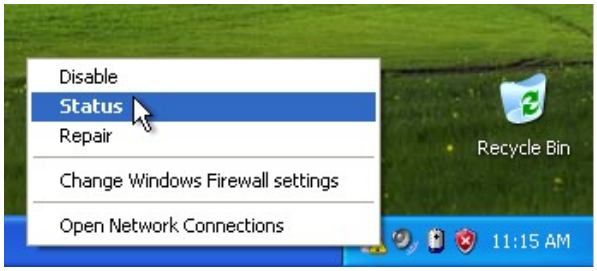
Gambar 3.4.10

- Sampai sini berarti kalian telah berhasil menginstall dan mengkonfigurasi DHCP Server dengan baik.

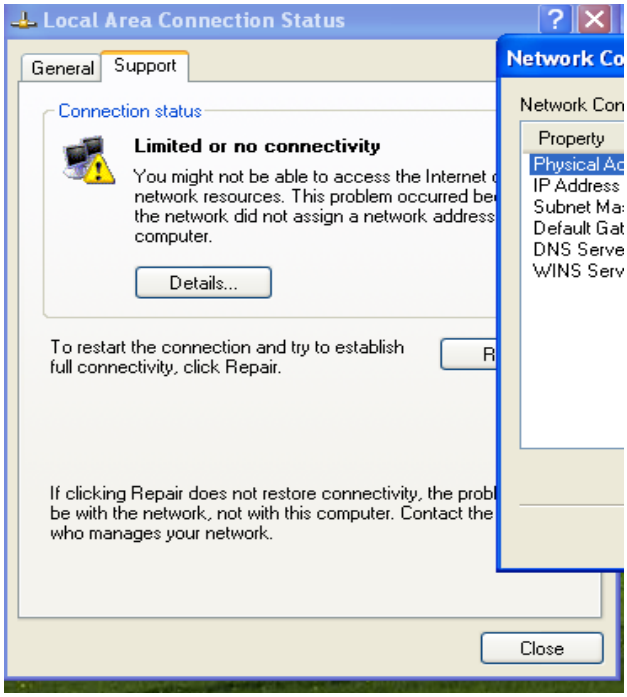
Konfigurasi Reservasi IP DHCP Server

Pada DHCP, kalian juga dapat menerapkan sistem Reservasi IP, yaitu memberikan IP-IP istimewa ke beberapa host tertentu. Tujuan dari metode ini adalah apabila kalian mempunyai beberapa orang penting dalam jaringan yang kalian kelola (misalnya admin/guru-guru), yang membutuhkan hak akses berbeda/khusus dalam jaringan, tentunya kalian harus memberikan IP statis/tetap kepada mereka. Karena dalam sistem DHCP, IP yang diberikan kepada tiap-tiap host akan diberikan secara acak. Tentunya ini akan menyulitkan kalian sebagai seorang Administrator untuk mengelola host-host penting tadi seandainya IP yang diberikan selalu berubah-ubah. Untuk itulah sistem reservasi IP ini dibutuhkan.

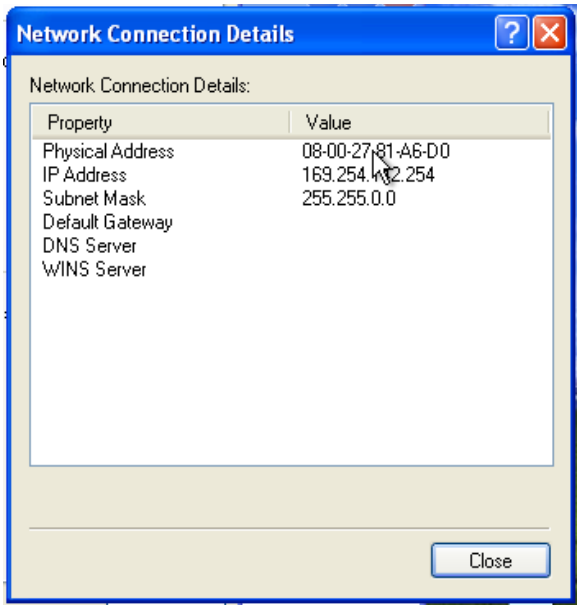
- Sebelum memulai konfigurasi, kalian perlu terlebih dahulu untuk mengetahui alamat hardware (MAC Address) dari interface client yang ingin kalian daftarkan. Pada sistem operasi Windows XP, cara untuk melihat alamat hardware adalah dengan cara mengklik kanan ikon network dan pilih **Status** (Gambar 3.4.11). Kemudian akan muncul jendela **Local Area Connection Status**, pada tab **Support** klik tombol **Details** (Gambar 3.4.12). Akan muncul jendela lain dan lihat pada bagian **Physical Address** disitulah terdapat alamat hardware dari interface kalian (Gambar 3.4.13).



Gambar 3.4.11



Gambar 3.4.12

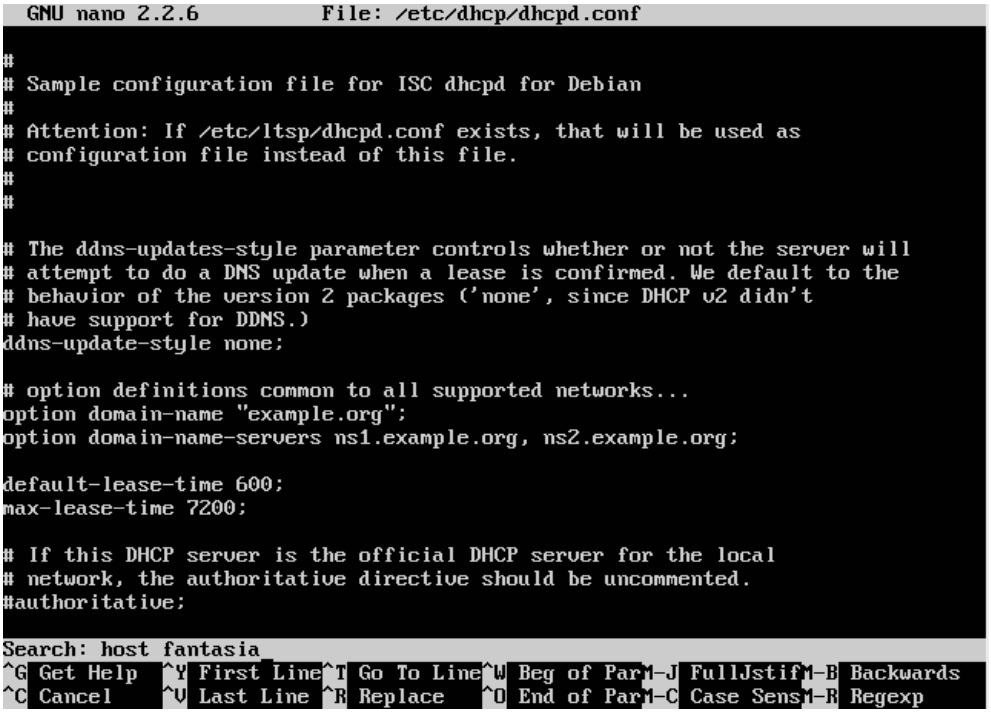


Gambar 3.4.13

- Sekarang barulah kalian dapat memulai konfigurasi. Caranya ketikkan perintah berikut untuk mengedit file **/etc/dhcp/dhcpd.conf** :

```
sudo nano /etc/dhcp/dhcpd.conf
```

- Setelah file konfigurasi tersebut terbuka, tekan tombol **CTRL + W** dan ketikkan **host fantasia** pada kotak pencarian lalu tekan **Enter**.



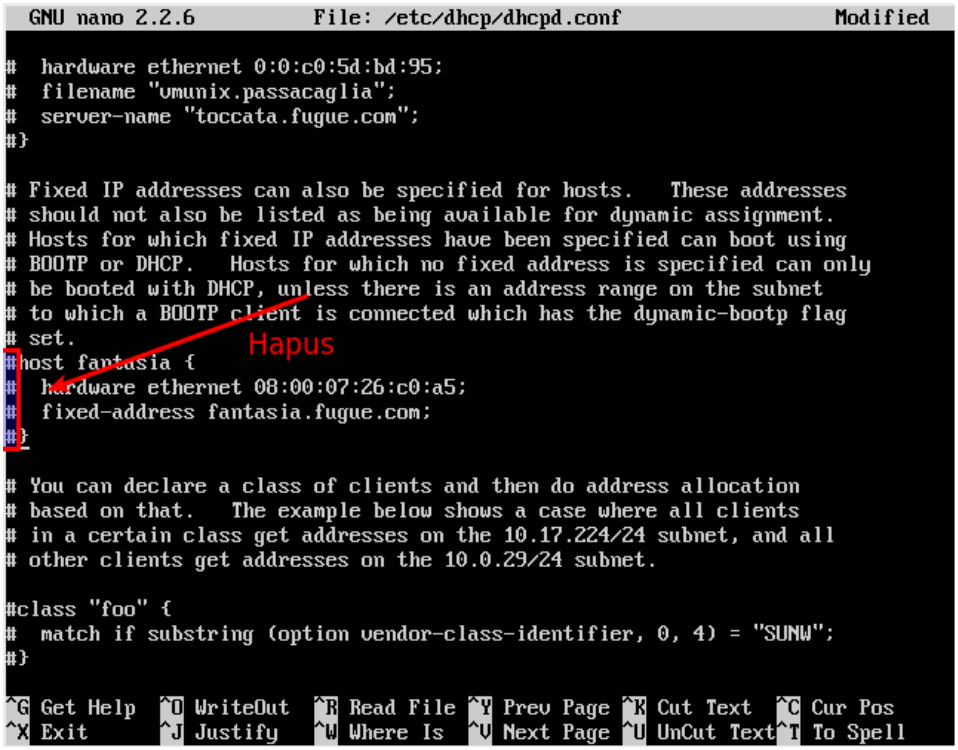
Gambar 3.4.14

- Kalian pasti akan menemukan baris konfigurasi seperti ini :

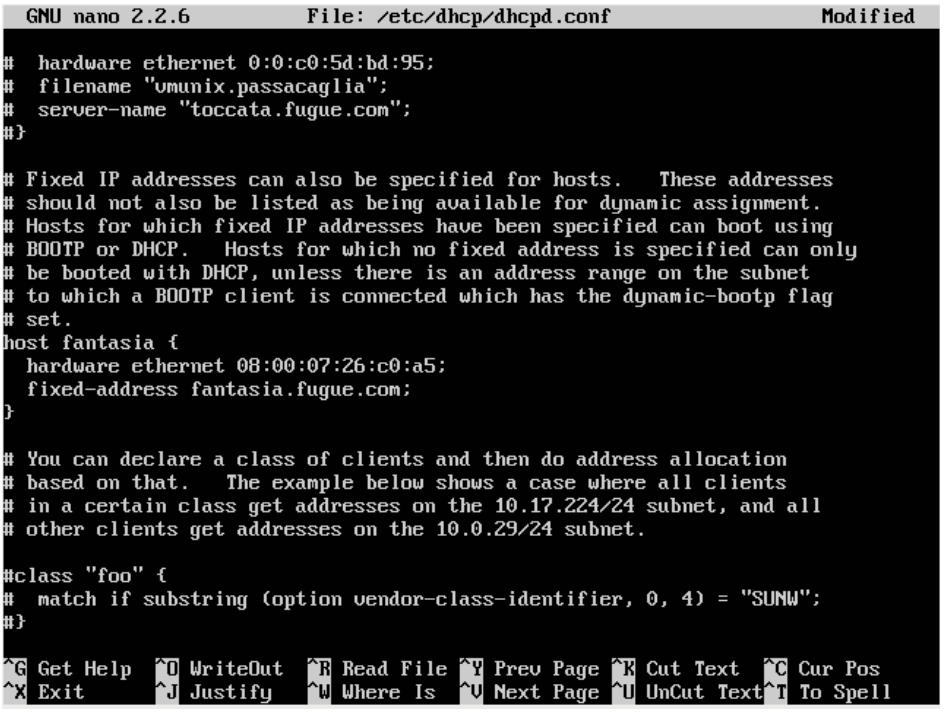
```
#host fantasia {
#  hardware ethernet 08:00:07:26:c0:a5;
#  fixed-address fantasia.fugue.com;
#}
```

- Selanjutnya kalian harus menghapus tanda pagar (#) yang ada di depan baris **host fantasia {** sampai baris **}**, sehingga akan menjadi seperti ini :

```
host fantasia {
  hardware ethernet 08:00:07:26:c0:a5;
  fixed-address fantasia.fugue.com;
}
```



Gambar 3.4.15



Gambar 3.4.16

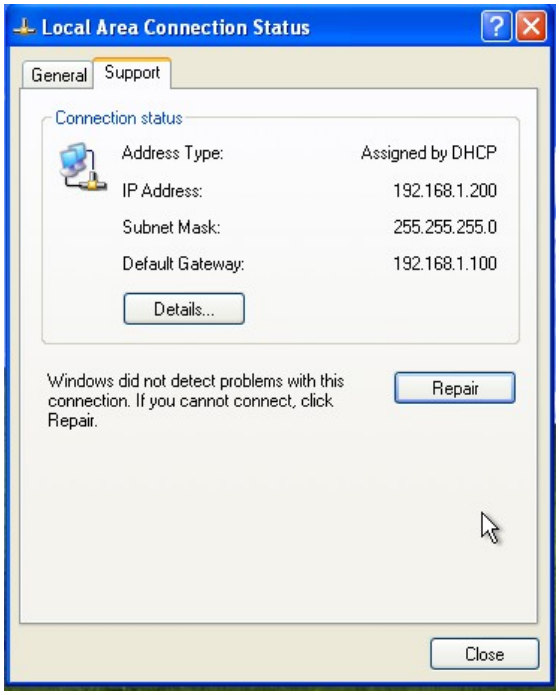
- Setelah itu baru kita edit baris konfigurasi tersebut sesuai dengan kebutuhan kalian. Misalnya disini kalian ingin mendaftarkan komputer kalian sebagai admin dengan IP Address tetap **192.168.1.200** yang memiliki alamat hardware **08:00:27:81:a6:d0**, maka baris konfigurasinya adalah seperti ini :

```
host admin {
  hardware ethernet 08:00:27:81:a6:d0;
  fixed-address 192.168.1.200;
}
```

- Setelah itu simpan perubahan dengan menekan **CTRL + X**, lalu tekan **Y**, lalu **Enter**.
- Terakhir restart service dari DHCP3 Server dengan mengeksekusi perintah berikut :

```
sudo service isc-dhcp-server restart
```

- Lalu coba lihat konfigurasi IP address pada client yang telah kalian daftarkan, jika berhasil maka IP address yang ia dapatkan akan selalu 192.168.1.200.



Gambar 3.4.17

3.5. Instalasi File Server

File Server memberikan layanan berupa penyediaaan file ataupun folder yang dapat diakses bersama-sama oleh para pengguna di dalam suatu jaringan. File Server sering juga disebut sebagai sistem *File Sharing*. Keuntungan dari penggunaan File Server ini dapat kalian lihat dari segi keefisiensiannya. Misalnya dalam suatu kasus kalian mempunyai 200 PC Client yang perlu diinstallkan program Office. Akan tetapi file installer program Office tersebut hanya terdapat di salah satu komputer saja. Tentunya akan sangat merepotkan dan beresiko apabila kalian harus

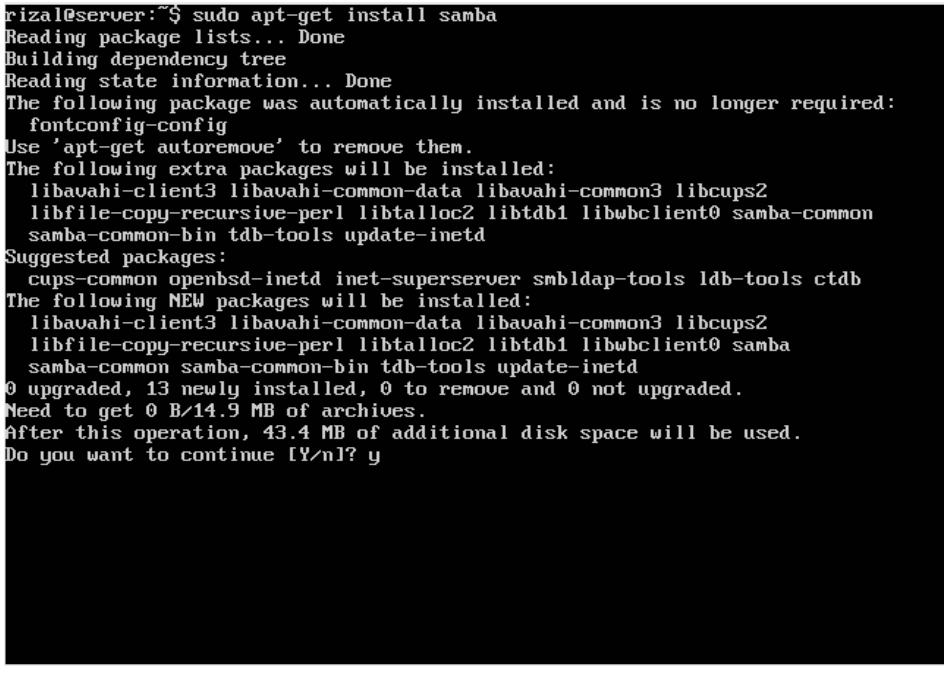
mengkopikan file installer tersebut ke tiap-tiap PC secara manual. Nah, solusinya adalah dengan penggunaan metode File Sharing ini. Dimana hanya ada satu komputer yang men-sharing file installer program Office tadi, lalu dari komputer-komputer client hanya tinggal mengaksesnya saja. Lalu bagaimana implementasi sistem File Server ini di Ubuntu Server 12.04 LTS?

Instalasi Samba

Sebenarnya aplikasi yang dapat kalian gunakan untuk membuat sebuah File Server di Linux adalah NFS (Network File System). Akan tetapi aplikasi tersebut tidak mendukung penggunaan lintas sistem operasi (Cross Platform). Jadi hanya dapat digunakan di lingkungan Linux dengan Linux saja. Sedangkan dalam dunia komputer, pengguna sistem operasi Windows atau Mac OS masih sangat mendominasi. Oleh karena itu kalian membutuhkan aplikasi File Sharing yang mendukung Cross Platform, agar sistem operasi lain juga dapat mengakses File Sharing yang akan kalian buat nantinya. Untuk itu semua, Samba adalah aplikasi yang paling memenuhi persyaratan diatas.
Untuk menginstall Samba, caranya adalah sebagai berikut :

- Pertama-tama eksekusi perintah berikut dan tunggu hingga proses instalasi selesai :

```
sudo apt-get install samba
```

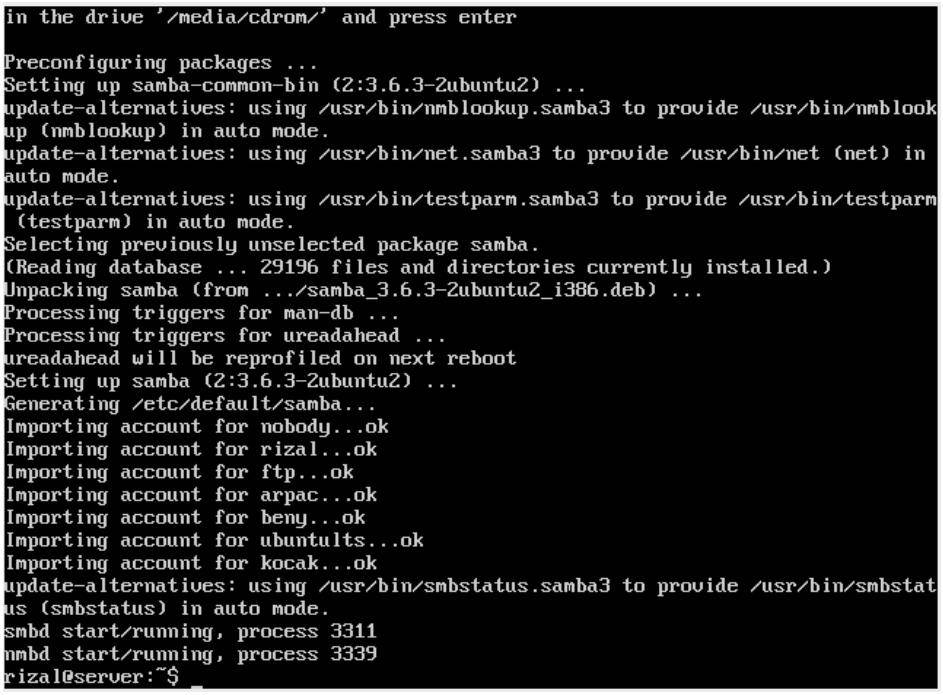


Gambar 3.5.1

- Apabila selama proses instalasi berlangsung terdapat kesalahan, jalankan saja perintah berikut untuk mengatasinya :

```
sudo apt-get -f install && sudo apt-get install samba
```

- Setelah memastikan Samba terinstall dengan baik, barulah kalian dapat memulai konfigurasi.



Gambar 3.5.2

Konfigurasi Samba

Untuk menshare suatu folder dengan Samba, kalian perlu melakukan konfigurasi-konfigurasi berikut :

- Pertama buka file konfigurasi **/etc/samba/smb.conf** dengan mengeksekusi perintah ini :

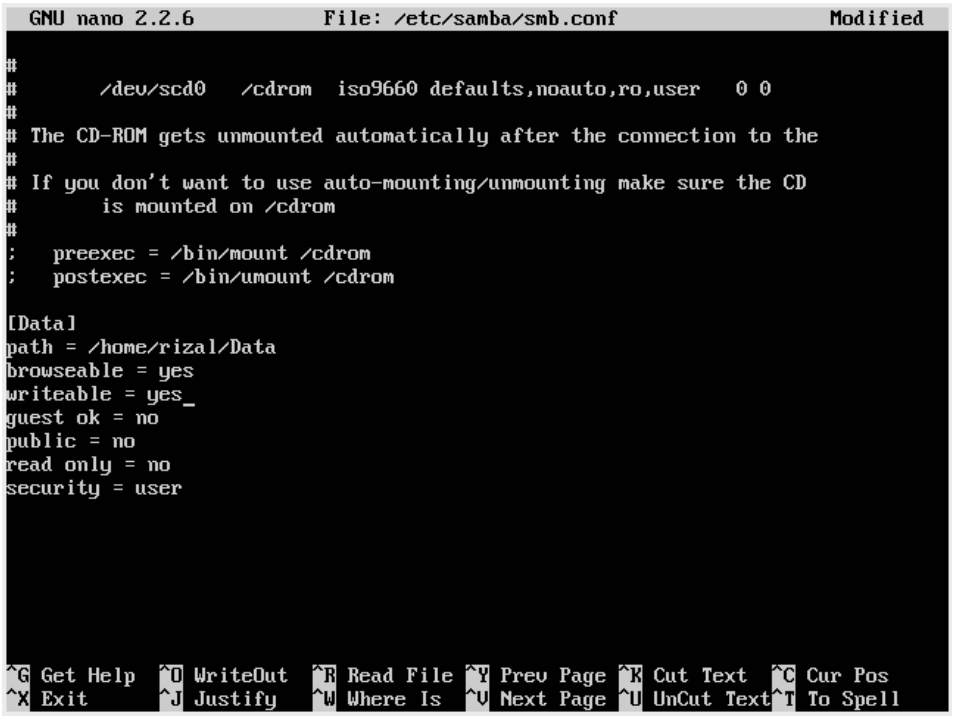
```
sudo nano /etc/samba/smb.conf
```

- Maka akan muncul baris-baris konfigurasi seperti gambar berikut :

Gambar 3.5.3

- Untuk men-share sebuah folder, pada bagian paling bawah file konfigurasi tersebut tambahkan baris-baris baru yang mendefinisikan nama folder yang di share, letak/path folder yang ingin dishare, apakah writeable/tidak, apakah browseable/tidak, sifatnya public/berpassword, dan lain-lain. Disini misalnya saja saya ingin men-share folder bernama **Data** dengan aturan hanya orang yang mengetahui password dari user pemilik folder tersebut saja yang dapat mengakses folder tersebut. Maka baris konfigurasinya adalah seperti berikut :

```
[Data]
path = /home/rizal/Data
browseable = yes
writeable = yes
guest ok = no
public = no
read only = no
security = user
```

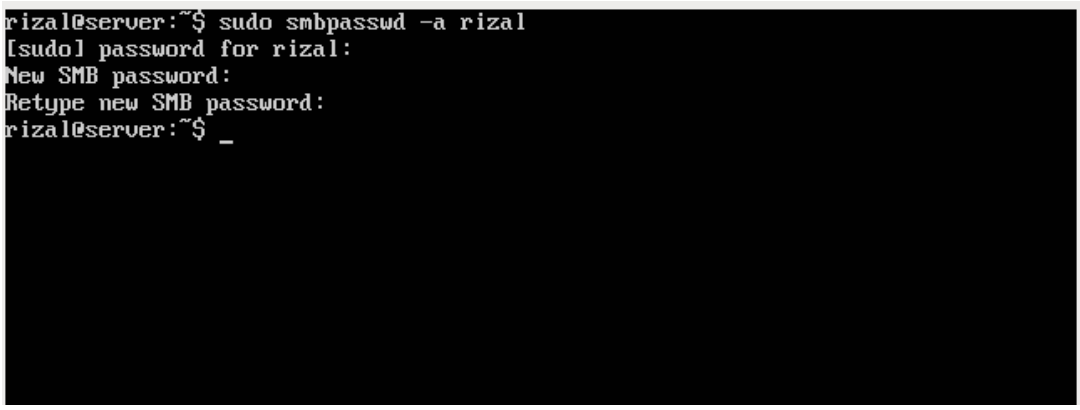


Gambar 3.5.4

- Kemudian simpan perubahan dengan menekan **CTRL + X**, lalu tekan **Y**, lalu **Enter**.
- Setelah itu kalian harus memberikan password Samba kepada user pemilik foldernya terlebih dahulu. Tujuannya adalah untuk membedakan antara password login user dengan password login untuk mengakses folder sharing Samba. Nah, pada buku ini user pemilik **Data** adalah rizal. Maka ketikkan perintah berikut :

```
sudo smbpasswd -a rizal
```

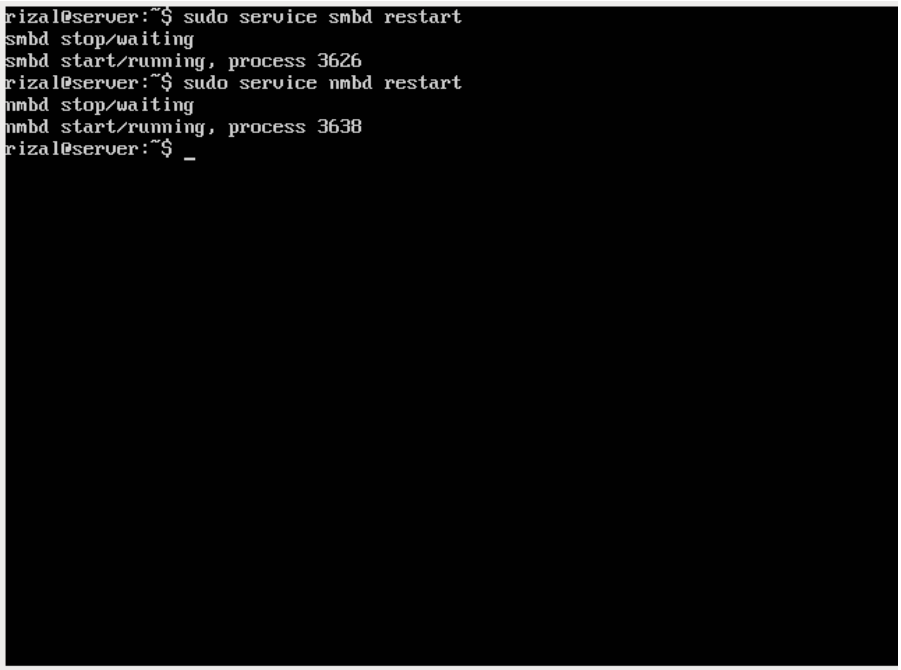
- Lalu isikan password kalian yang baru sebanyak dua kali.



Gambar 3.5.5

- Dan yang terakhir, restart service Samba untuk mengaktifkan perubahan yang telah kalian lakukan dengan mengeksekusi perintah berikut :

```
sudo service smbd restart
sudo service nmbd restart
```



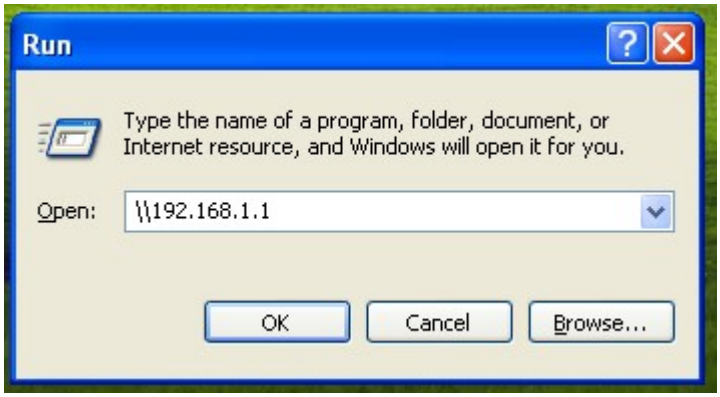
Gambar 3.5.6

- Sekarang coba akses folder share tersebut dari sisi client. Jika pada sistem operasi Windows, cara mengakses foldernya adalah dengan menjalankan aplikasi **Run** (tekan tombol **Windows + R**), kemudian isikan dengan format sintaks berikut :

```
\\ipaddress
```

- Misalnya IP Address milik Ubuntu Server adalah 192.168.1.1, maka isi sintaksnya adalah seperti ini :

```
\\192.168.1.1
```

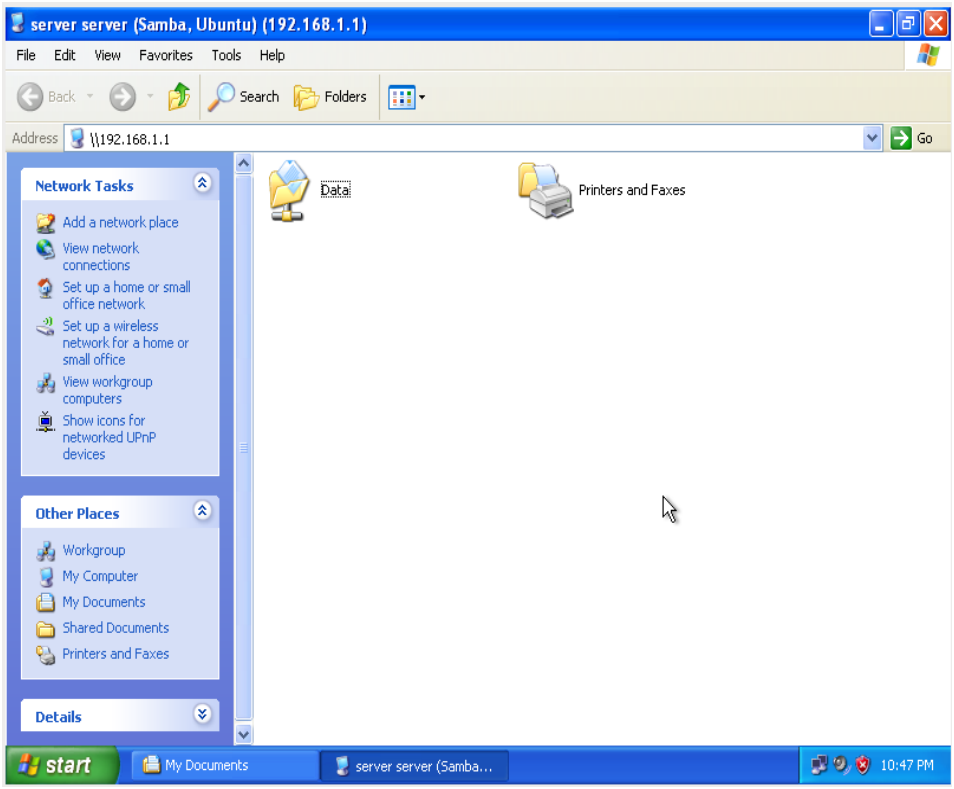


Gambar 3.5.7

- Setelah itu akan muncul sebuah jendela login, isikan dengan username dan password yang telah kalian buat dengan perintah smbpasswd sebelumnya. Misalnya disini saya isikan usernamenya dengan **rizal**.

Gambar 3.5.8

- Jika berhasil maka akan tampak folder yang telah kalian share seperti gambar dibawah ini.



Gambar 3.5.9

3.6. Instalasi FTP Server

FTP adalah singkatan dari *File Transfer Protocol*, protokol untuk bertukar file melalui jaringan. FTP sering digunakan untuk mendownload sebuah file dari server maupun untuk mengupload file ke sebuah server (misalnya mengupload konten-konten web ke sebuah webserver). Cara kerja protokol FTP hampir sama dengan protokol lainnya. Apabila protokol HTTP bertugas untuk urusan web, kemudian protkol SMTP bertugas dalam urusan mail, maka FTP ini bertugas untuk urusan pertukaran file. Intinya FTP adalah protokol yang bertugas dalam hal pertukaran file baik itu download ataupun upload di jaringan.

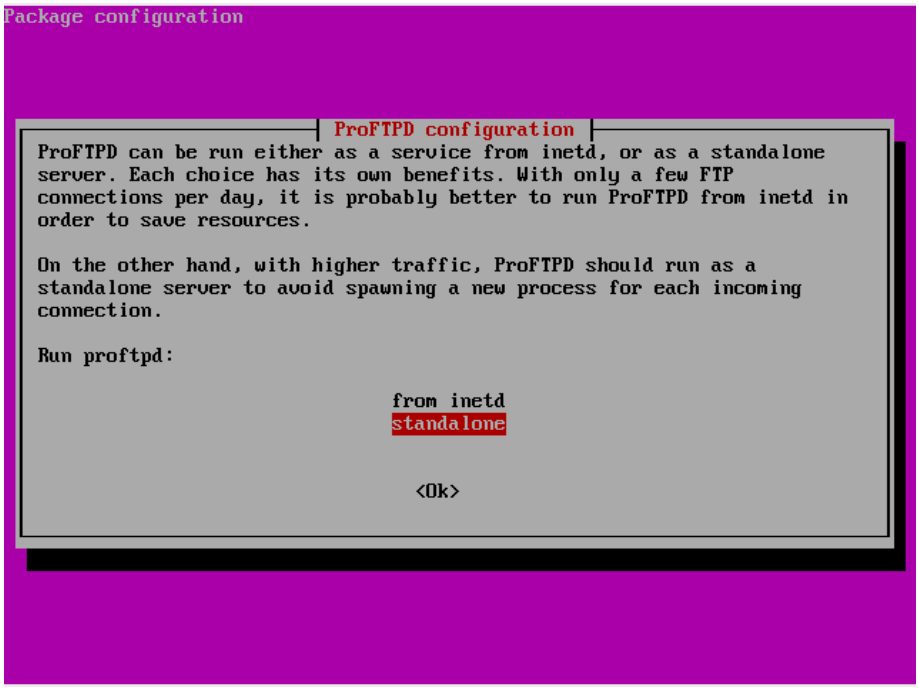
Instalasi Proftpd

Aplikasi FTP Server di Linux sebenarnya ada banyak. Akan tetapi yang cara konfigurasinya paling mudah diantara lainnya adalah Proftpd. Selain mudah konfigurasinya, Proftpd juga cukup ringan dan handal dalam urusan ini.

- Untuk menginstall Proftpd seperti biasa siapkan terlebih dahulu DVD Repositori, lalu eksekusi perintah berikut :

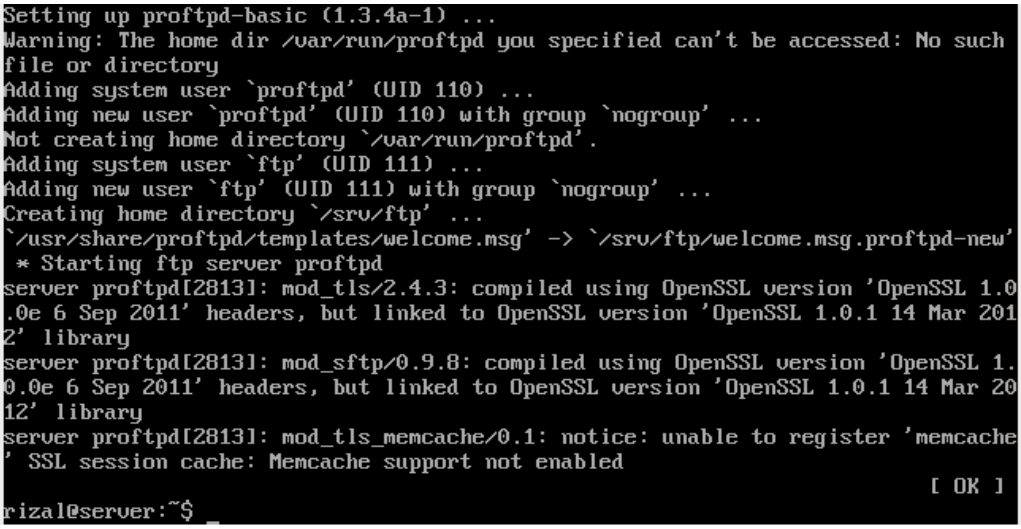
```
sudo apt-get install proftpd
```

- Kemudian akan muncul pertanyaan untuk memilih **from inetd** atau **standalone**, untuk skala jaringan besar yang trafficnya padat disarankan untuk memilih yang **standalone**. Kemudian tekan **Enter**.



Gambar 3.6.1

- Setelah itu tunggu hingga instalasi selesai dan pastikan tidak ada pesan error seperti gambar dibawah ini.



Gambar 3.6.2

- Selanjutnya barulah kalian dapat memulai proses konfigurasi.

Konfigurasi Proftpd

Untuk mengkonfigurasi Proftpd, kalian cukup mengedit satu file saja yang berada di **/etc/proftpd/proftpd.conf**. Disini kalian akan mempraktekkan bagaimana caranya mengkonfigurasi FTP Server dengan sistem Anonymous login, yaitu siapapun dapat secara bebas mengakses file yang telah disediakan oleh FTP Server.

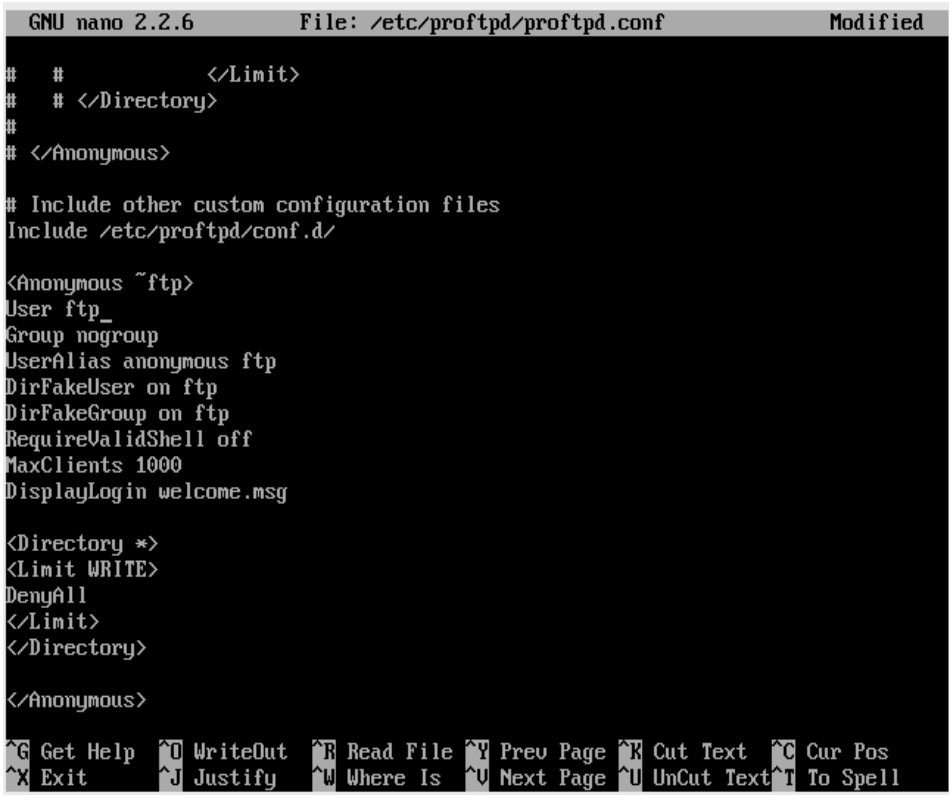
- Pertama buka file konfigurasi Proftpd dengan perintah ini :

```
sudo nano /etc/proftpd/proftpd.conf
```

- Setelah terbuka, pada baris paling bawah file konfigurasi tersebut tambahkan skrip berikut :

```
<Anonymous ~ftp>
User ftp
Group nogroup
UserAlias anonymous ftp
DirFakeUser on ftp
DirFakeGroup on ftp
RequireValidShell off
MaxClients 1000
DisplayLogin welcome.msg
```

```
<Directory *>
<Limit WRITE>
DenyAll
</Limit>
</Directory>

</Anonymous>

IdentLookups off
UseReverseDNS off
ListOptions "" maxdepth 3
ListOptions "" maxdirs 10
ListOptions "" maxfiles 1000
```



Gambar 3.6.3

- Kemudian simpan perubahan dengan menekan **CTRL + X**, lalu tekan **Y**, lalu **Enter**
- Lalu terakhir restart service dari Proftpd nya dengan mengeksekusi perintah berikut :

```
sudo service proftpd restart
```

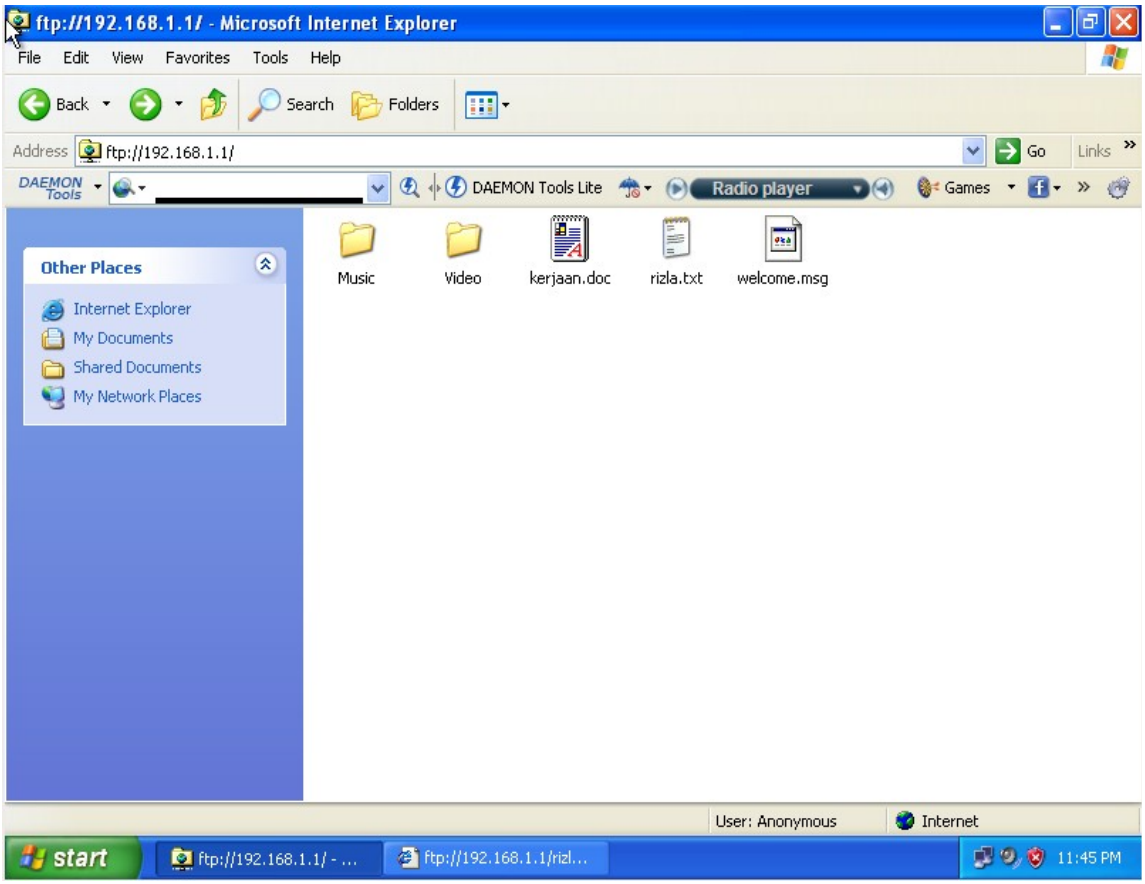
- Sekarang coba kalian masukkan seluruh file-file yang ingin kalian upload ke direktori **/srv/ftp**, dan setelah itu coba akses ke alamat server melalui browser atau file manager di komputer client :

  ```
  ftp://ipserver
  ```

- Misalnya disini saya masukkan :

  ```
  ftp://192.168.1.1
  ```

- Maka jika berhasil akan muncul daftar dari direktori-direktori maupun file-file yang telah letakkan di folder **/srv/ftp** seperti yang ditunjukkan oleh gambar dibawah ini.



Gambar 3.7.4

- Sampai sini berarti FTP Server telah berjalan dengan baik. Setelah itu kalian tinggal mendownload maupun mengupload file-file tersebut, bisa secara langsung maupun menggunakan bantuan aplikasi tambahan seperti *Filezilla*.

3.7. Instalasi NTP Server

NTP adalah singkatan dari Network Time Protocol, sebuah protocol untuk meng-sinkron-kan sistem waktu (clock) pada komputer terhadap sumber yang akurat, melalui jaringan intranet atau internet. Sedangkan NTP Server sendiri adalah sebuah server yang mensinkron-kan waktunya terhadap sumber waktu akurat, dan mentransmisikan paket informasi waktu kepada komputer client yang meminta.

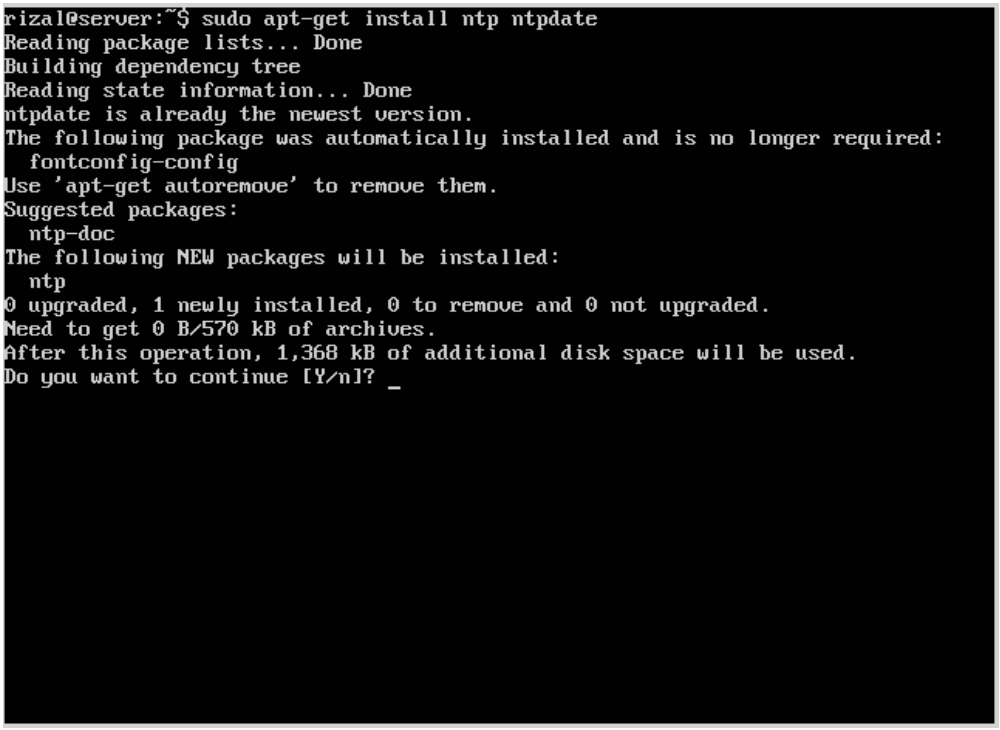
NTP Server ini sangat bermanfaat sekali apabila kalian mengelola jaringan yang sangat ketat sekali dalam urusan waktu. Misalnya ketika seluruh pegawai di kantor kalian, kalian perintah untuk mengumpulkan tugas dalam bentuk email yang harus dikirimkan ke email server kantor sebelum batas waktu jam 12 siang. Lewat dari itu, email akan di reject secara otomatis oleh sistem. Nah apa jadinya bila ternyata waktu yang terdapat di komputer server berbeda dengan waktu yang terdapat di komputer-komputer pegawai kalian? Salah-salah ketika pegawai kalian mengira waktu masih tersisa 5 menit lagi, ternyata jam yang terdapat di komputer server sudah menunjukkan pukul 12. Untuk hal-hal seperti ini lah NTP Server diperlukan, agar waktu/jam antara komputer satu dengan yang lainnya yang ada didalam suatu jaringan dapat sinkron atau sama.

Instalasi NTP

Untuk membuat mesin kalian menjadi sebuah NTP Server, kalian cukup menginstall service **ntp** dan **ntpdate**. Caranya adalah seperti berikut :

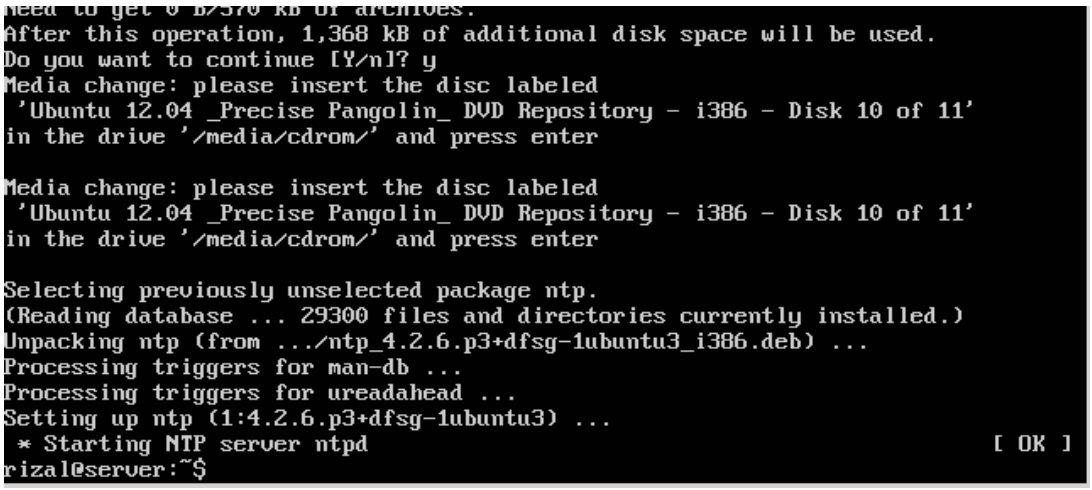
- Pertama-tama masukkan DVD Repositori kedalam CDROM kalian, kemudian ketikkan perintah ini :

```
sudo apt-get install ntp ntpdate
```



Gambar 3.7.1

- Tunggu dan pastikan tidak ada pesan error hingga proses instalasi selesai seperti yang ditunjukkan gambar dibawah ini :



Gambar 3.7.2

- Setelah itu barulah kalian dapat memulai proses konfigurasi.

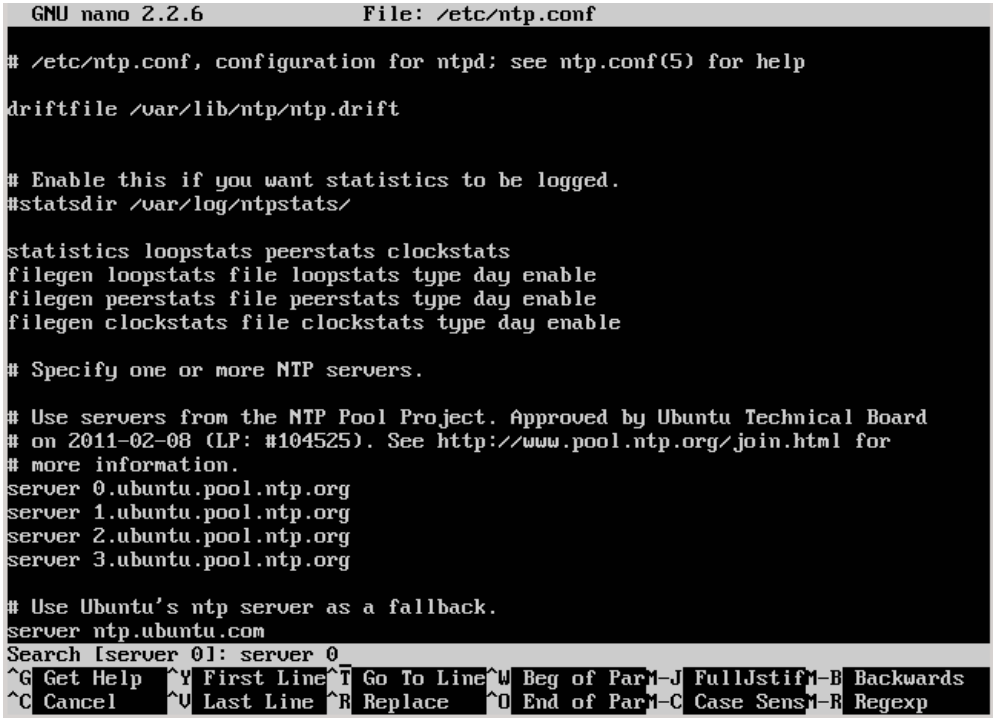
Konfigurasi NTP

Pada layanan NTP Server, ada beberapa bagian yang perlu kalian konfigurasikan terhadap file **/etc/ntp.conf**. Dan berikut adalah langkah-langkahnya :

- Pertama-tama buka file **/etc/ntp.conf** dengan mengeksekusi perintah berikut :

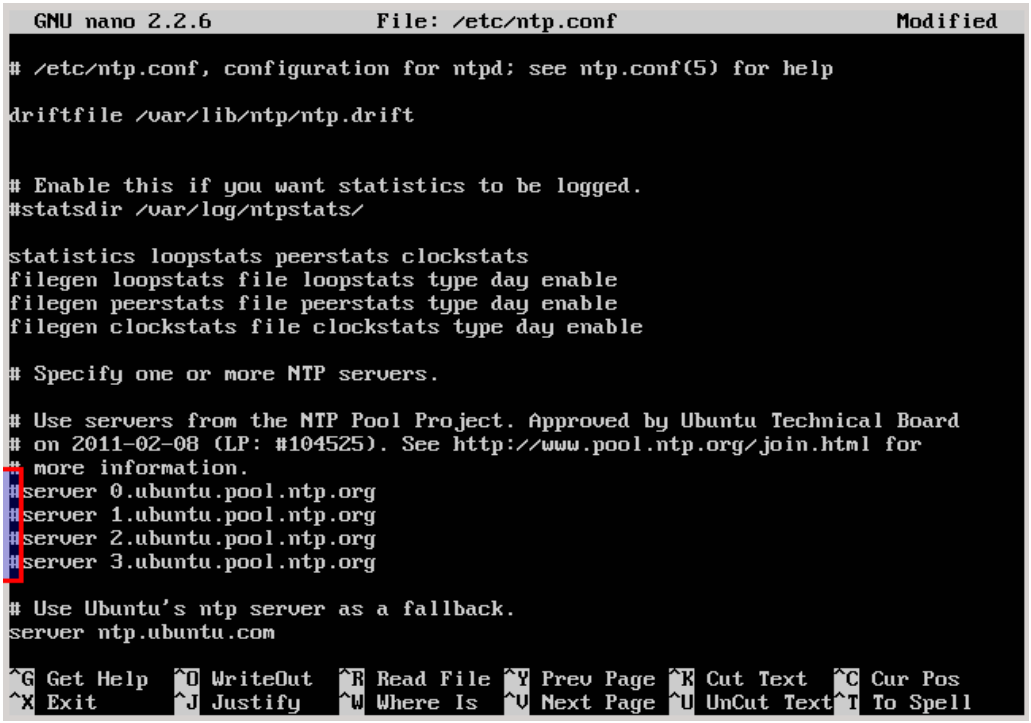
```
sudo nano /etc/ntp.conf
```

- Setelah file tersebut terbuka, tekan tombol **CTRL + W** untuk melakukan pencarian. Isikan **server 0** ke dalam kotak pencarian yang muncul, kemudian tekan **Enter**.



Gambar 3.7.3

- Setelah itu kalian akan menemukan baris **server 0.ubuntu.pool.ntp.org**. Tambahkan tanda pagar (#) di depan baris **server 0.ubuntu.pool.ntp.org** sampai baris **server 3.ubuntu.pool.ntp.org** seperti yang terlihat pada gambar dibawah :



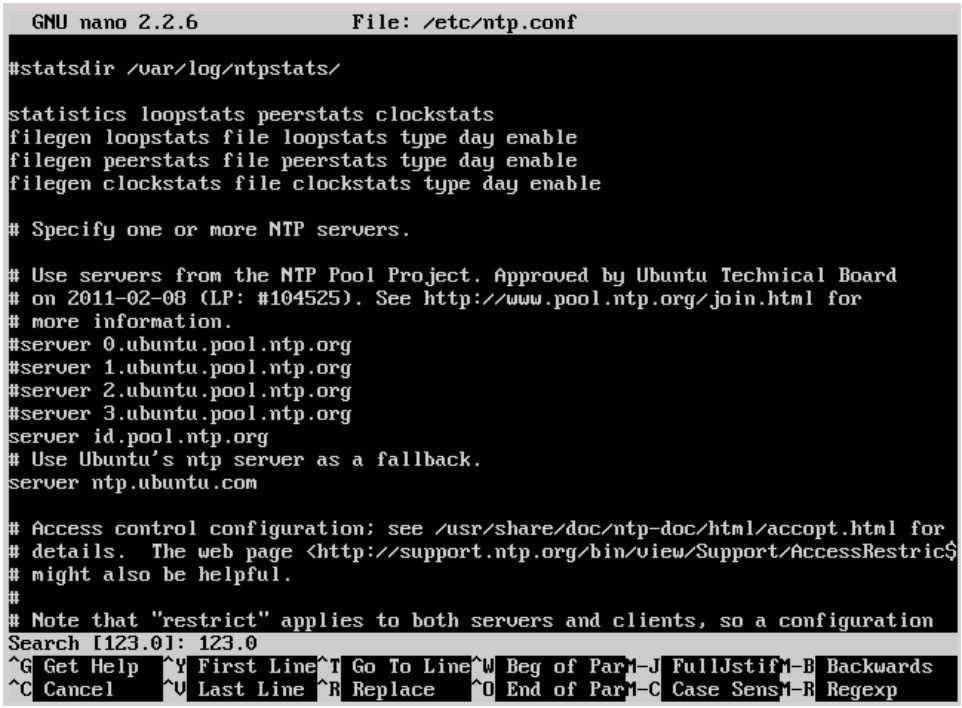
Gambar 3.7.4

- Langkah selanjutnya adalah menambahkan baris berikut dibawah baris **server 3.ubuntu.pool.ntp.org.**

```
server id.pool.ntp.org
```

Gambar 3.7.5

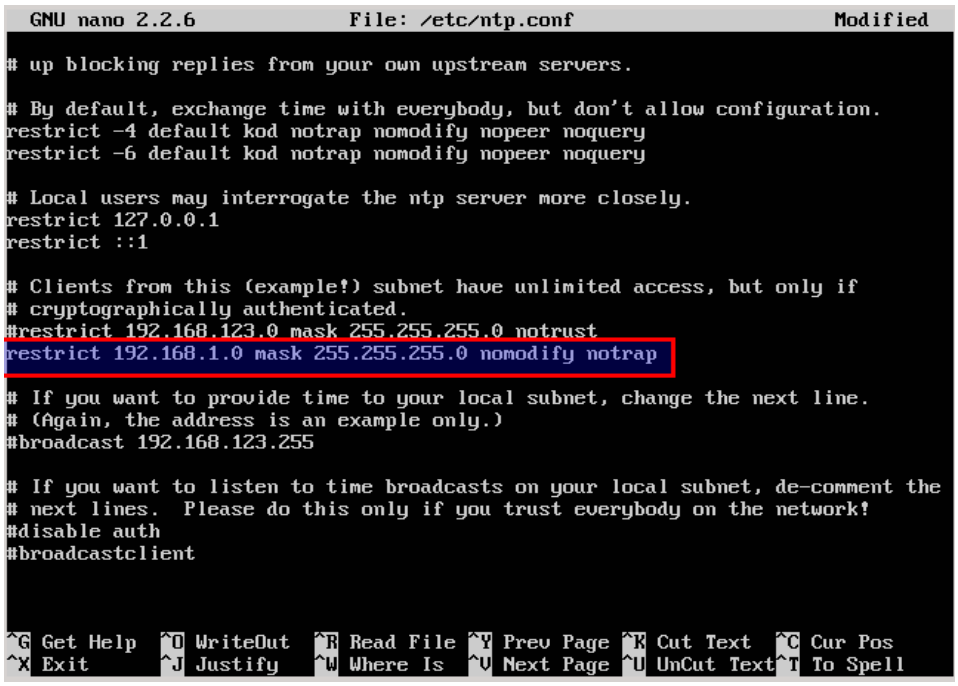
- Setelah itu tekan kembali tombol **CTRL + W**, dan ketikkan angka **123.0** di dalam kotak **Search**.



Gambar 3.7.6

- Kemudian kalian akan menemukan baris **restrict 192.168.123.0 mask 255.255.255 notrust**. Tepat dibawah baris tersebut, tambahkan baris konfigurasi ini :

```
restrict 192.168.1.0 mask 255.255.255 nomodify notrap
```



Gambar 3.7.7

- Lalu simpan perubahan dengan menekan **CTRL + X**, lalu tekan **Y**, lalu **Enter**.
- Setelah konfigurasi selesai, kalian perlu untuk mensinkronisasikan waktu dengan server

induk di internet. Akan tetapi sebelum melakukan hal tersebut, kalian harus mematikan service dari NTP Server terlebih dahulu dengan perintah ini (1) :

```
sudo /etc/init.d/ntp stop
```

- Setelah itu baru eksekusi perintah berikut untuk mensinkronkan waktu dengan server induk NTP server di Indonesia, yaitu id.pool.ntp.org (2).

```
sudo ntpdate id.pool.ntp.org
```

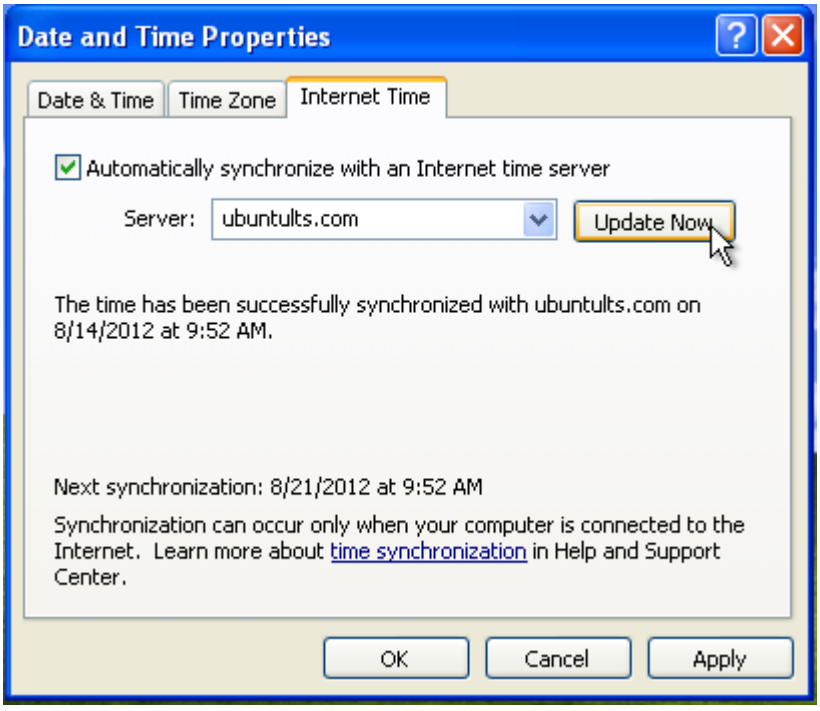
- Terakhir jalankan kembali service dari NTP dengan perintah berikut (3):

```
sudo /etc/init.d/start
```

```
rizal@server:~$ sudo /etc/init.d/ntp stop  1
 * Stopping NTP server ntpd                                          [ OK ]
rizal@server:~$ sudo ntpdate id.pool.ntp.org  2
14 Aug 23:28:41 ntpdate[1531]: step time server 103.12.12.14 offset 1.674220 sec
rizal@server:~$ sudo /etc/init.d/ntp start  3
 * Starting NTP server ntpd                                          [ OK ]
rizal@server:~$
```

Gambar 3.7.8

- Jika tidak ada pesan kesalahan selama proses konfigurasi diatas berlangsung, maka seharusnya sampai tahap ini proses konfigurasi dari NTP Server telah selesai.
- Untuk mengetesnya, silahkan atur pada sisi client untuk mensinkronkan waktunya ke Server Ubuntu lokal kalian. Karena pada sisi client tidak perlu lagi untuk mensinkronkan waktunya ke server induk yang ada di internet, akan tetapi cukup mensinkronkan waktu dengan Server lokal saja. Apabila pada sistem operasi Windows XP kalian dapat mengaturnya pada **Adjust Date/Time** kemudian pilih **Internet Time**. Lihat gambar berikut agar lebih jelasnya.



Gambar 3.7.9

3.8. Instalasi Mail Server

Mail Server adalah sebuah aplikasi yang menerima e-mail dari pengguna lokal (dari domain yang sama) maupun pengirim remote dari jaringan lain (internet). Selain itu Mail Server juga mampu mem-forward e-mail tersebut ke Mail Server lainnya untuk dikirim. Intinya Mail Server adalah yang melayani kalian para user dalam proses pengiriman dan penerimaan e-mail seperti halnya kantor pos.

Untuk dapat mengirimkan e-mail, sebuah Mail Server harus memiliki sebuah MTA (Mail Transport Agent) didalamnya. Fungsi utamanya adalah untuk mengirimkan e-mail dari Mail Server lokal ke Mail Server remote. Sebenarnya ada banyak sekali jenis-jenis MTA yang dapat kalian install di Ubuntu. Beberapa contohnya adalah :

- Postfix
- Sendmail
- Qmail
- Exim
- Zimbra
- dll.

Selain untuk mengirimkan e-mail, Mail Server juga bertugas untuk menerima e-mail menggunakan protokol POP atau IMAP. Untuk itu diperlukan juga sebuah POP dan IMAP server agar Mail Server dapat berfungsi dengan sempurna dalam menerima email masuk dari MTA Mail Server lain. Contoh POP dan IMAP server yang cukup terkenal adalah **Courier** dan **Dovecot**.

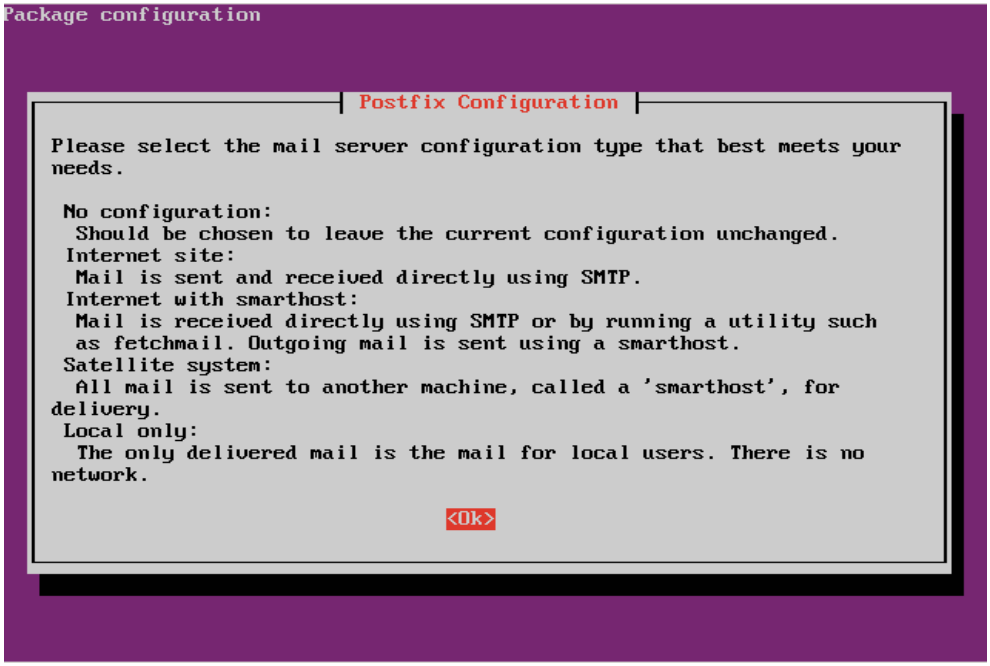
Instalasi Postfix

Kenapa saya memilih Postfix ? Postfix terkenal dengan kemudahan konfigurasinya, cepat, dan juga aman.

- Untuk menginstall Postfix ketikkan perintah berikut :

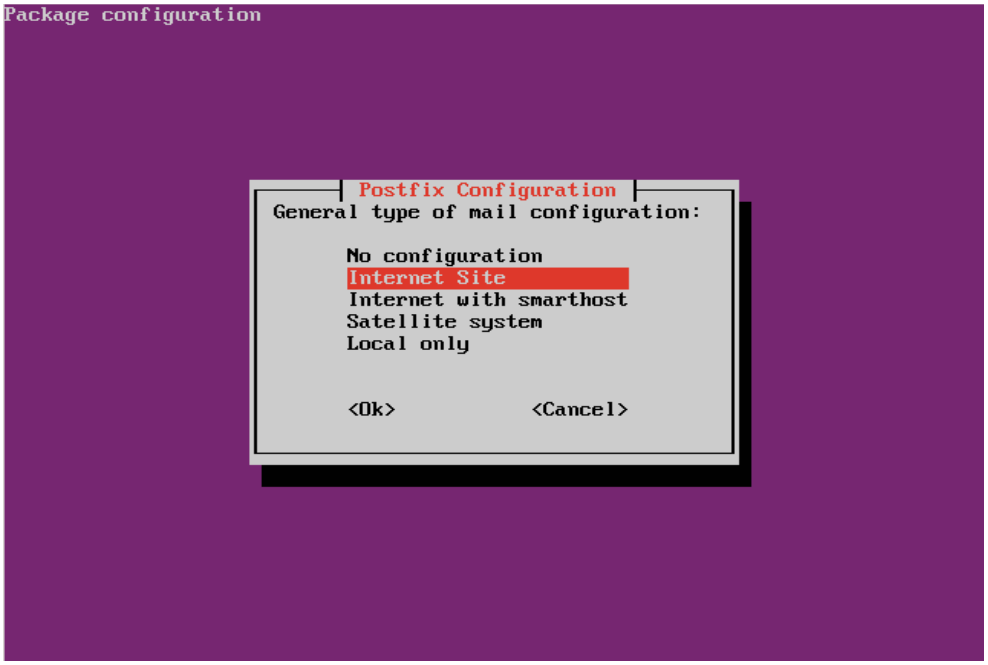
```
sudo apt-get install postfix
```

- Kemudian akan muncul konfirmasi untuk melakukan konfigurasi Postfix. Pilih **OK** lalu tekan **Enter**.



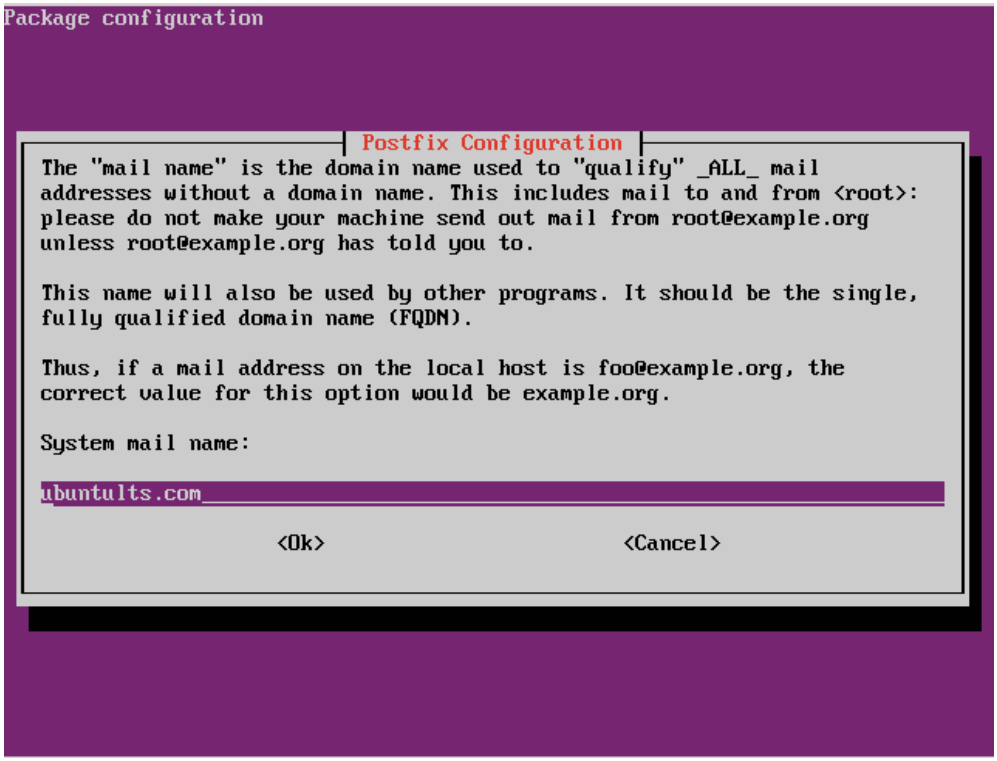
Gambar 3.8.1

- Setelah itu pilih **Internet Site** jika muncul pertanyaan seperti ini :



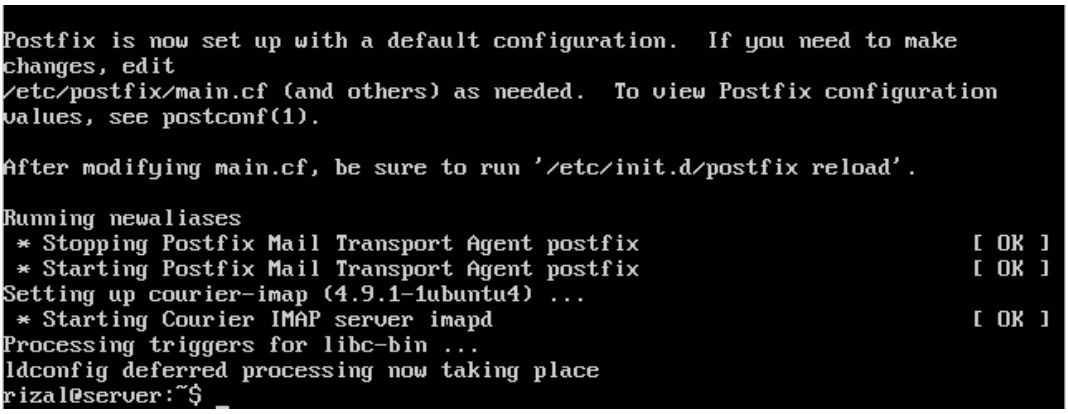
Gambar 3.8.2

- Pada pertanyaan yang ini, isikan dengan domain kalian yaitu **ubuntults.com**.



Gambar 3.8.3

- Lalu tunggu hingga proses instalasi selesai seperti yang ditunjukkan oleh gambar dibawah ini :



Gambar 3.8.4

- Jika terdapat pesan error atau instalasi gagal, lakukan eksekusi berikut untuk mengatasinya :

```
sudo apt-get -f install && sudo apt-get install postfix
```

Instalasi Courier

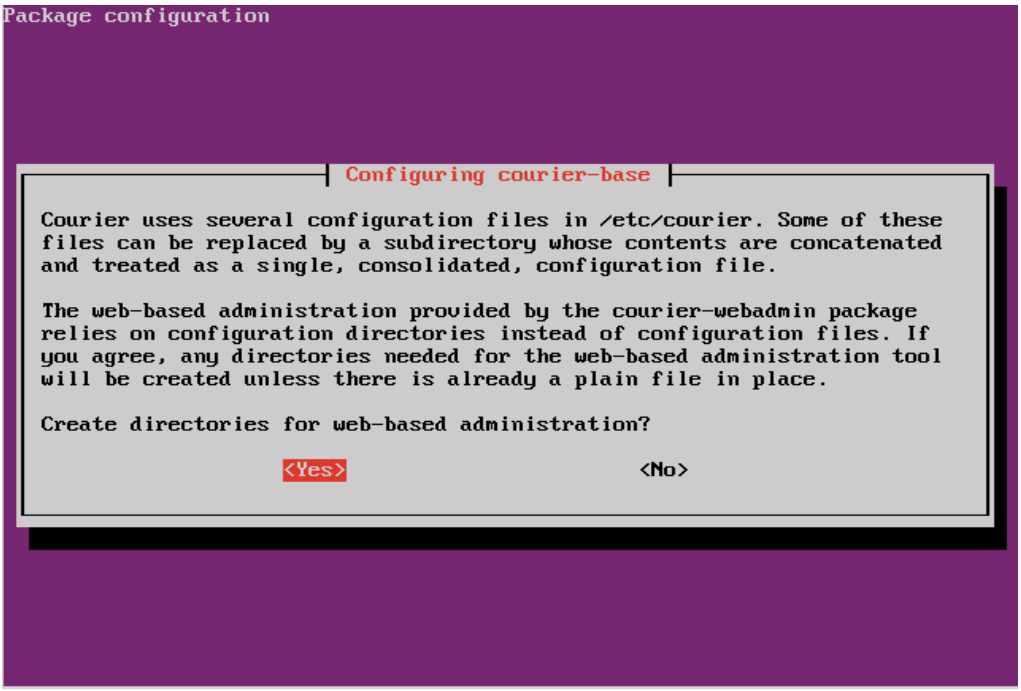
Setelah menginstall Postfix, kalian tidak dapat langsung untuk mengkonfigurasinya karena kalian perlu untuk menginstall POP/IMAP servernya terlebih dahulu. Pada buku ini saya lebih memilih

untuk memakai Courier karena Courier sangat handal, cepat, mudah dikonfigurasi dan juga hanya memakan sedikit penggunaan memori.

- Untuk menginstalasi Courier, lakukan eksekusi berikut :

```
sudo apt-get install courier-base courier-imap
```

- Pilih **Yes** apabila muncul pertanyaan seperti gambar dibawah :

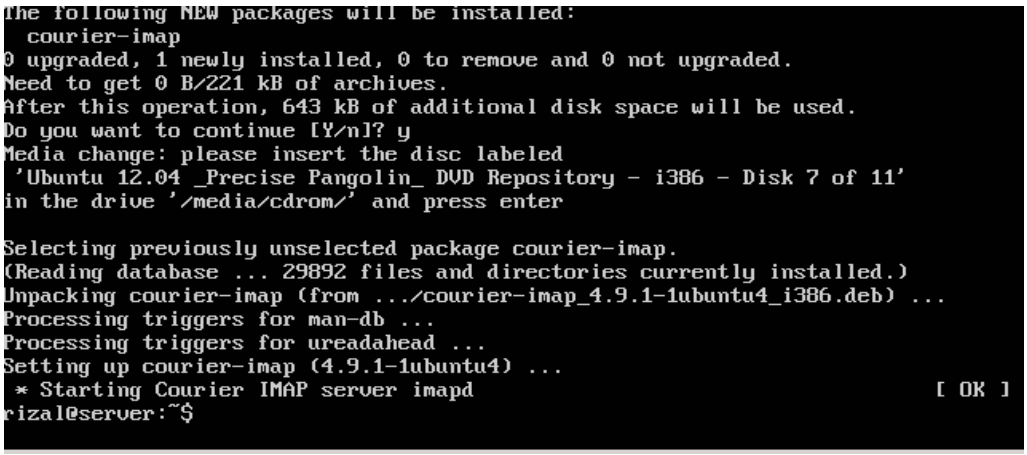


Gambar 3.8.5

- Dan seperti biasa, apabila muncul pesan error selama proses instalasi, lakukan perintah berikut ini untuk mengatasinya :

```
sudo apt-get -f install && sudo apt-get install courier-base courier-imap
```

- Setelah itu pastikan tidak ada pesan error lagi hingga proses instalasi selesai seperti yang ditunjukkan oleh gambar dibawah ini :



Gambar 3.8.6

Konfigurasi Postfix dan Courier

Setelah Postfix dan Courier terinstall, sekarang barulah kalian dapat memulai proses konfigurasi.

- Pertama-tama buat terlebih dahulu folder tempat Mail Server meletakkan seluruh e-mail dari para pengguna dengan perintah berikut :

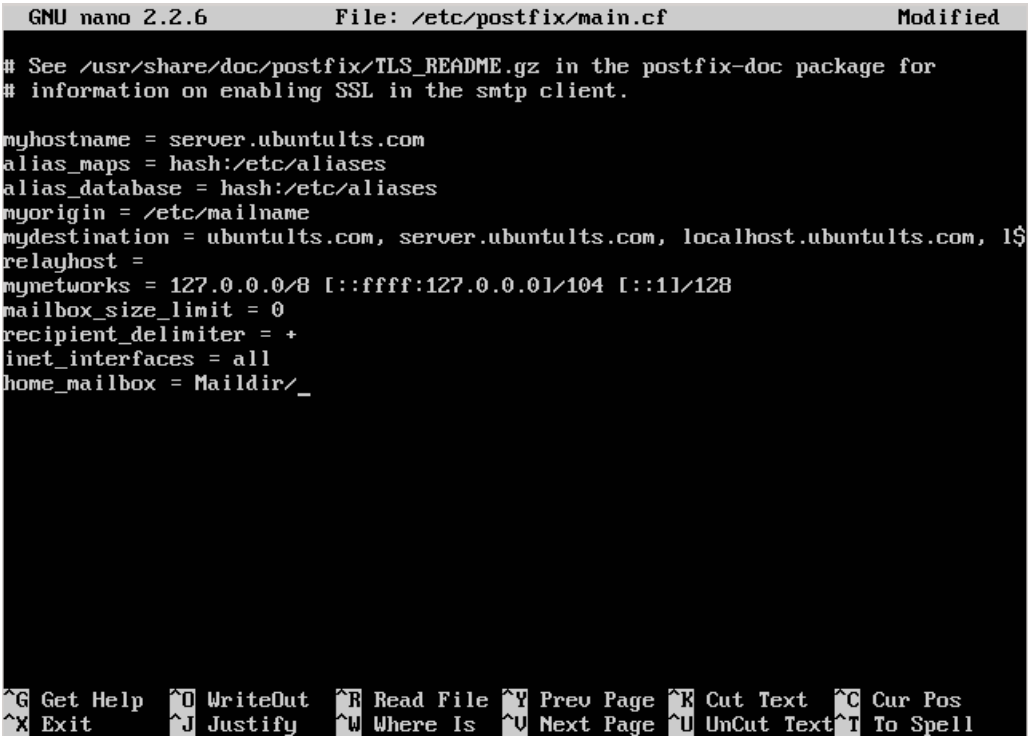
  ```
  sudo maildirmake /etc/skel/Maildir
  ```

- Setelah itu edit file **/etc/postfix/main.cf** dengan perintah berikut :

  ```
  sudo nano /etc/postfix/main.cf
  ```

- Pada baris paling bawah file konfigurasi tersebut, tambahkan baris baru dengan isi script seperti ini :

  ```
  home_mailbox = Maildir/
  ```

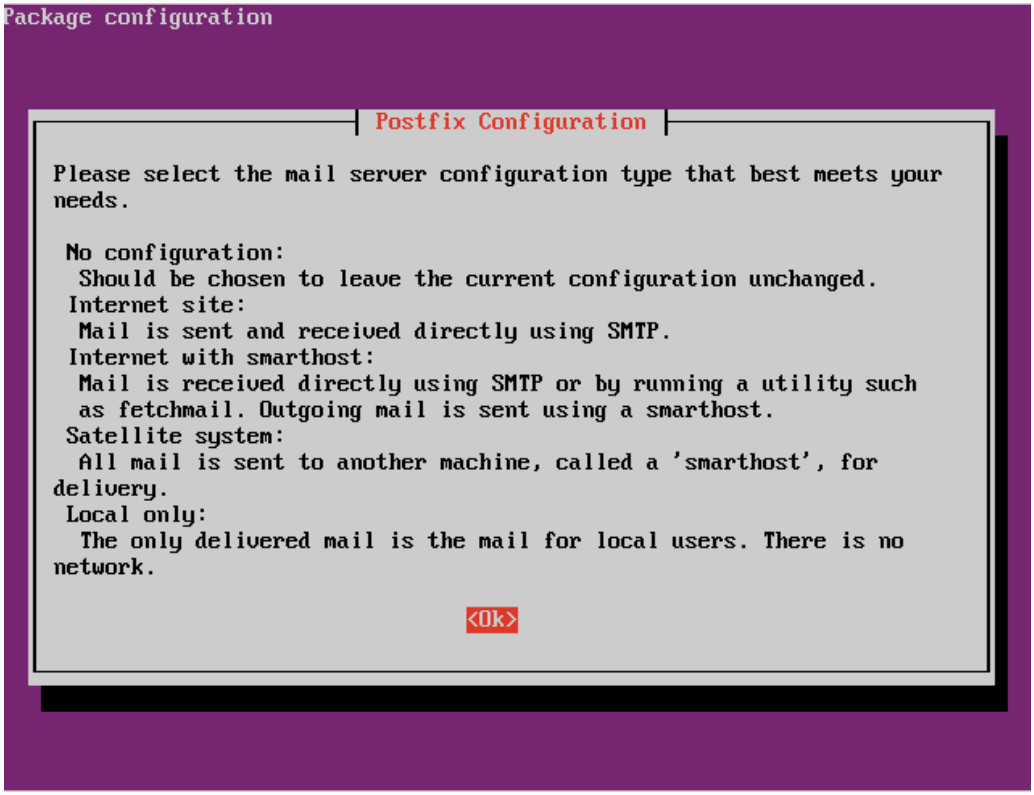


Gambar 3.8.7

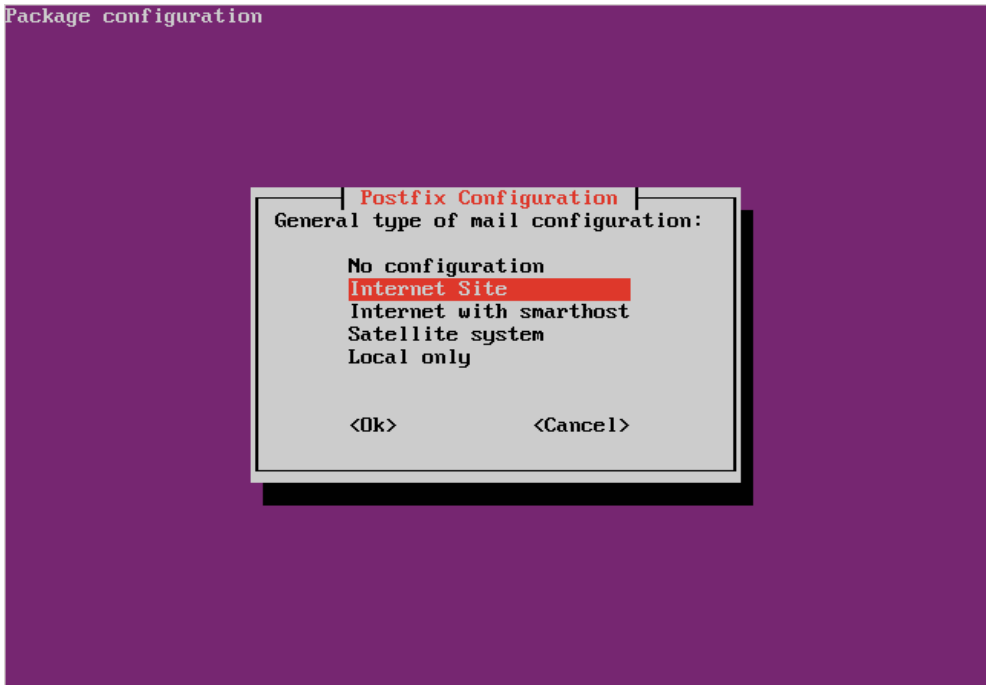
- Setelah itu simpan file dengan menekan tombol **CTRL + X**, lalu tekan **Y**, lalu **Enter**
- Kemudian konfigurasikan ulang layanan Postfix dengan perintah berikut :

```
sudo dpkg-reconfigure postfix
```

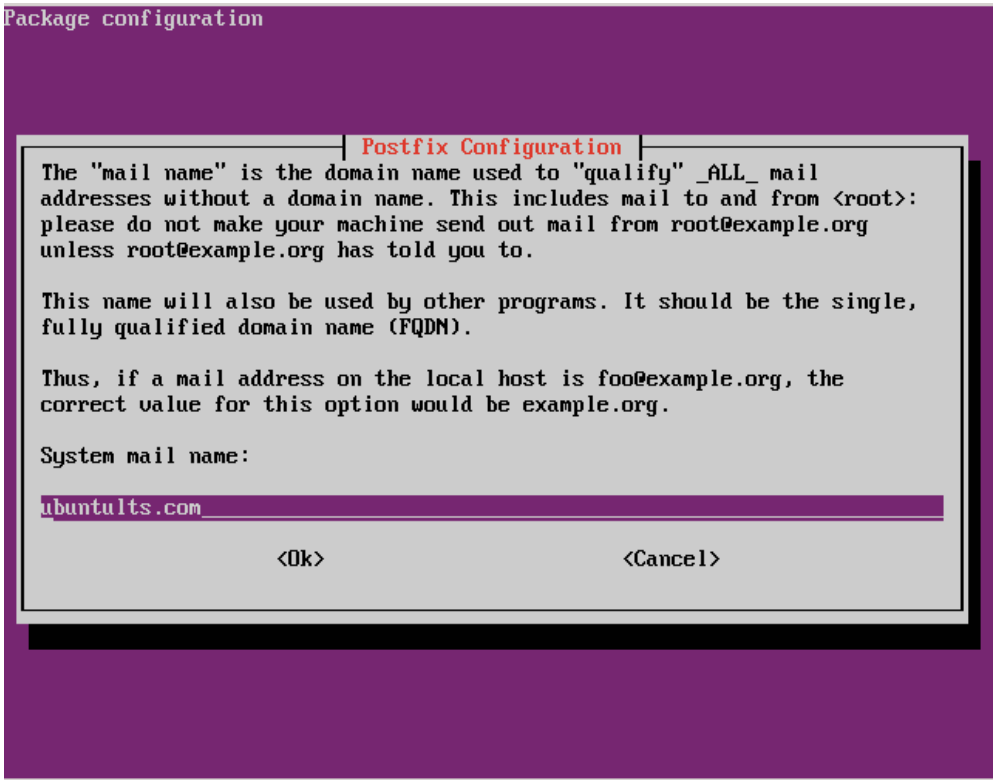
- Akan muncul pertanyaan yang sama seperti pada saat awal instalasi Postfix tadi, pilih saja **OK** (Gambar 3.8.8), **Internet Site** (Gambar 3.8.9), dan isi dengan **ubuntults.com** (Gambar 3.8.10).



Gambar 3.8.8

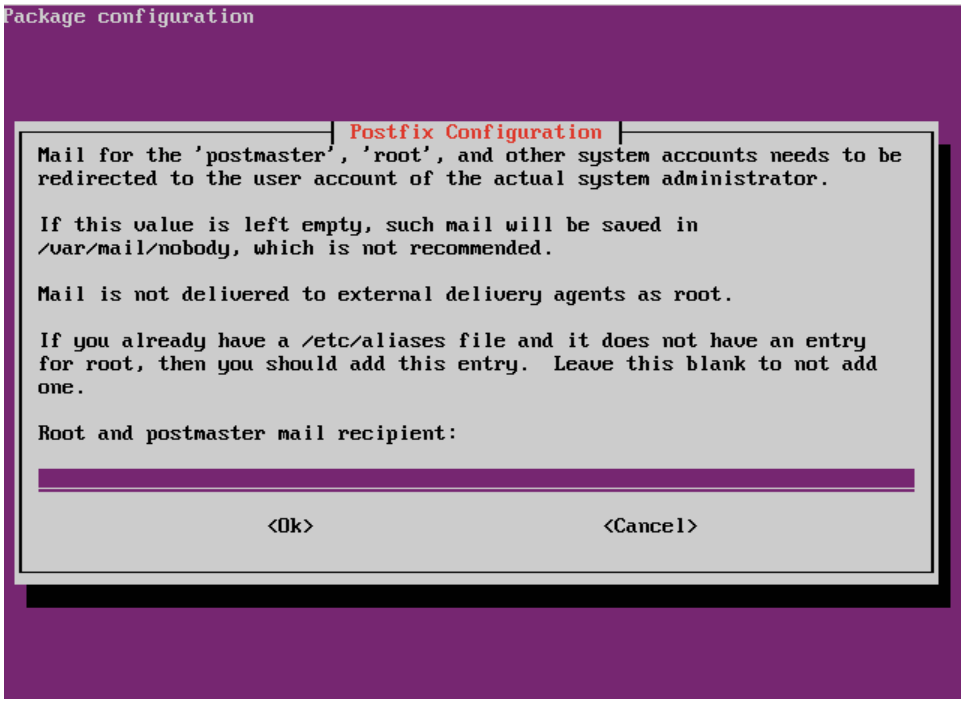


Gambar 3.8.9



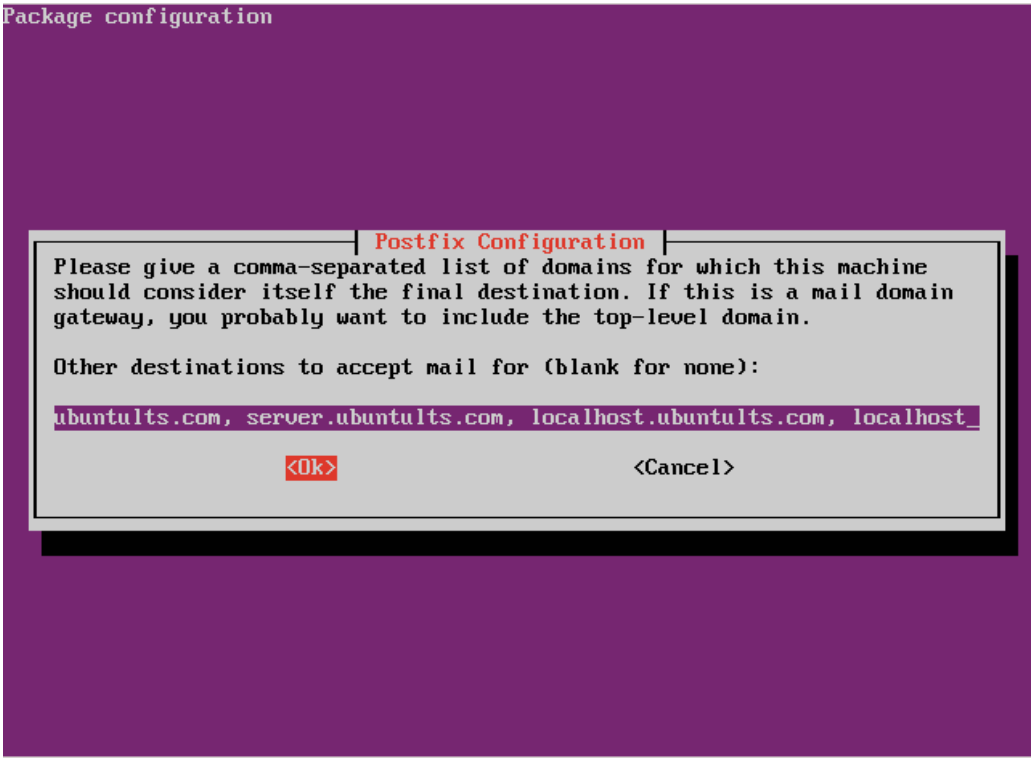
Gambar 3.8.10

- Setelah itu kosongkan saja pada pertanyaan **root and postmaster mail recipients**, lalu tekan **Enter** :



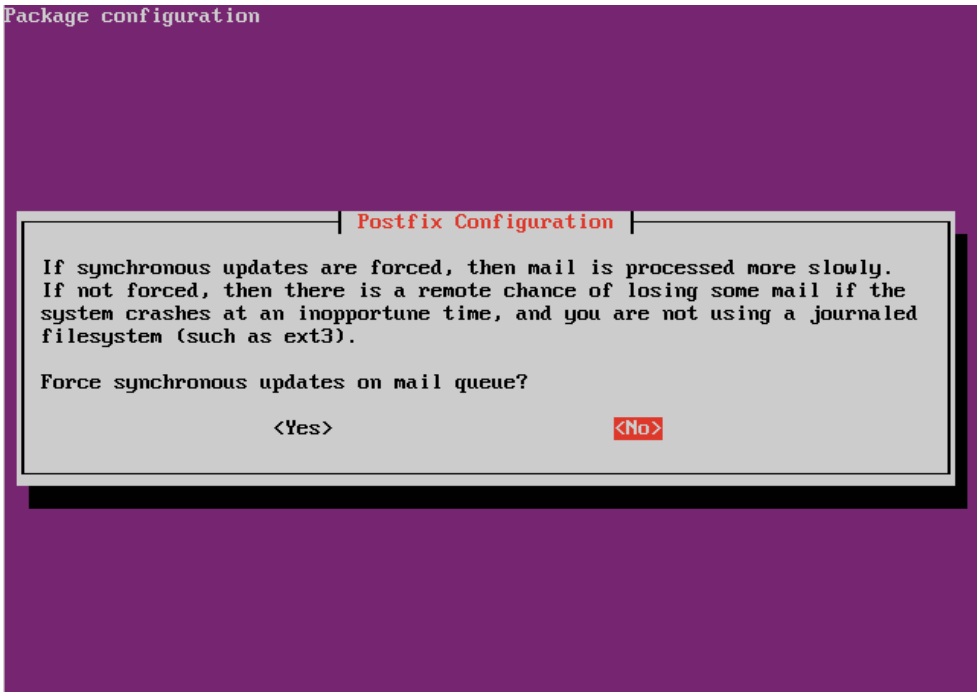
Gambar 3.8.11

- Kemudian tekan **Enter** saja pada pertanyaan **Other destination to accept mail** :



Gambar 3.8.12

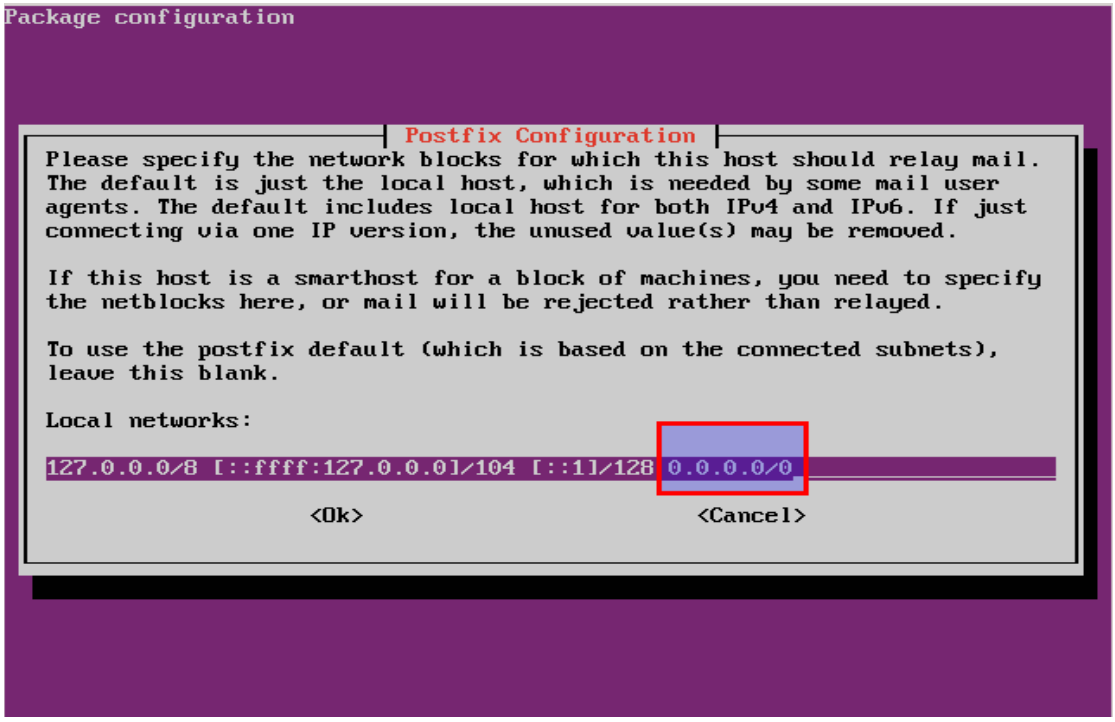
- Setelah itu pilih **No** dan tekan **Enter** ketika ditanya **Force synchronous update on mail queue** :



Gambar 3.8.13

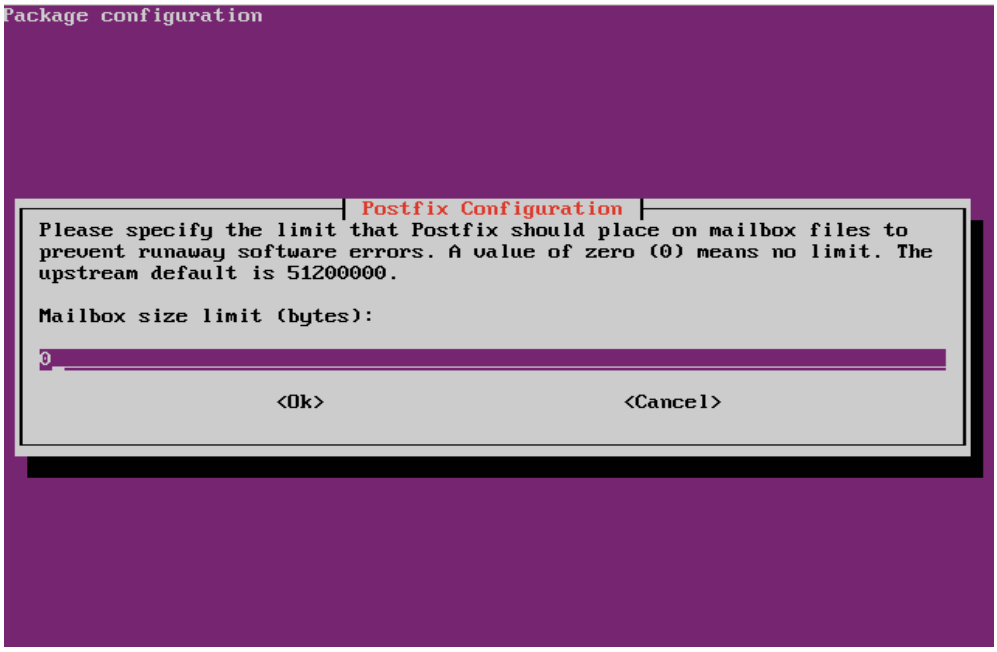
- Lalu pada pertanyaan **Local Networks** dibawah ini, pada baris paling akhir tambahkan :

```
0.0.0.0/0
```

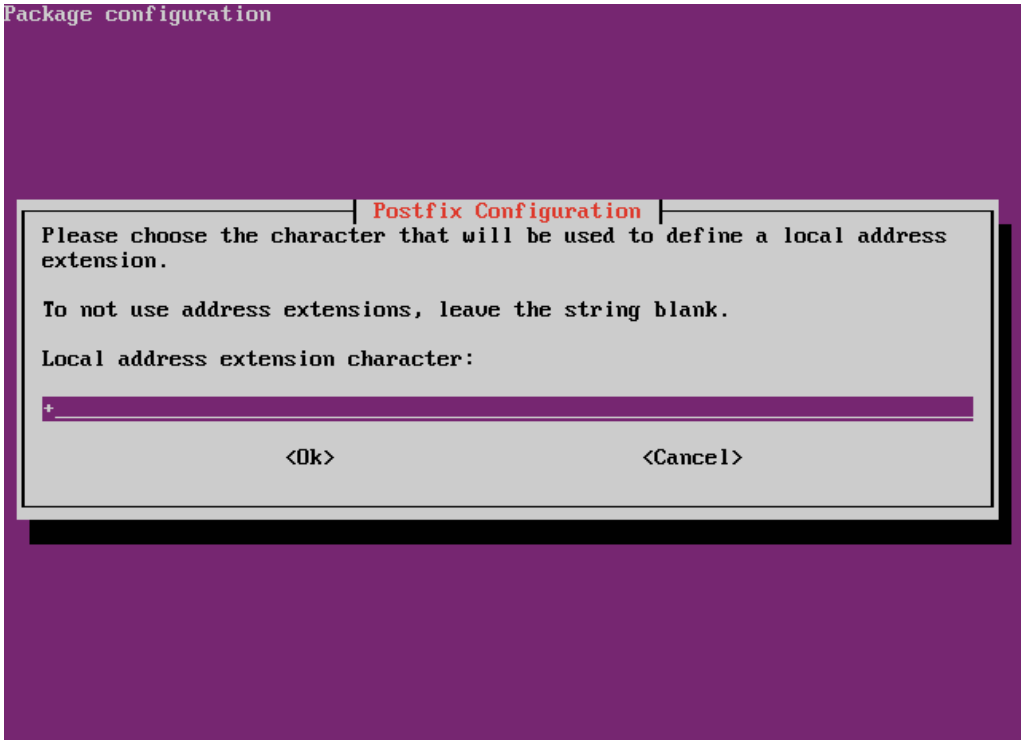


Gambar 3.8.14

- Kemudian biarkan saja pilihan default dan langsung tekan **Enter** pada pertanyaan **Mailbox size limit** (Gambar 3.8.15) dan **Local addresses extension character** (Gambar 3.8.16).

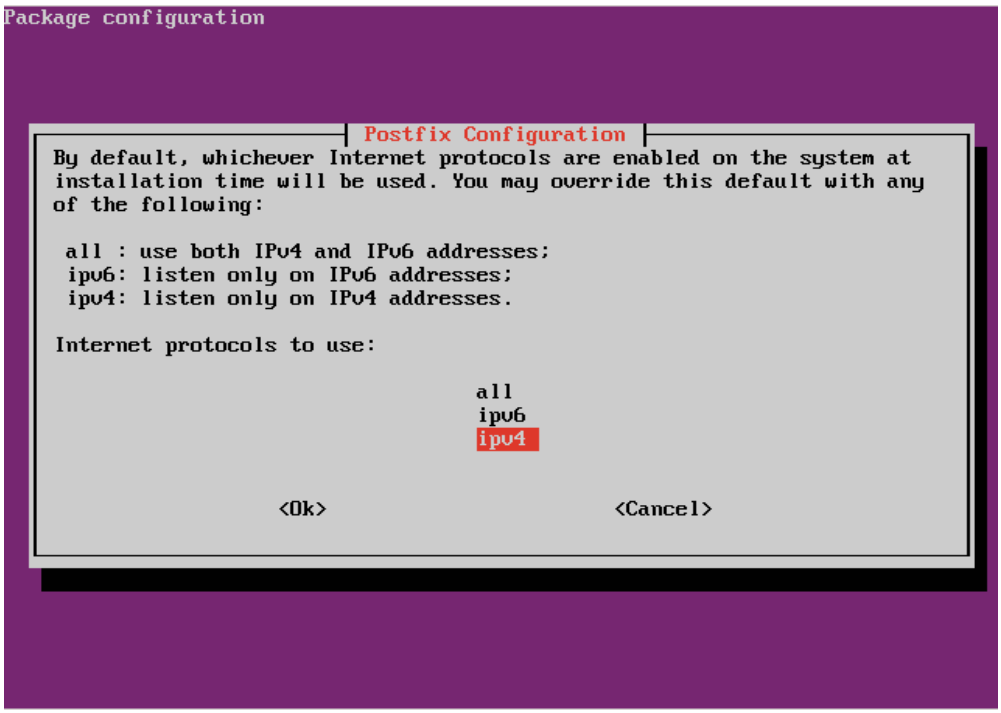


Gambar 3.8.15



Gambar 3.8.16

- Terakhir pilih **ipv4** pada pertanyaan **Internet protocols to use** :



Gambar 3.8.17

- Jika tidak ada pesan kesalahan, sampai sini selesailah proses konfigurasi Mail Server dengan menggunakan Postfix + Courier.

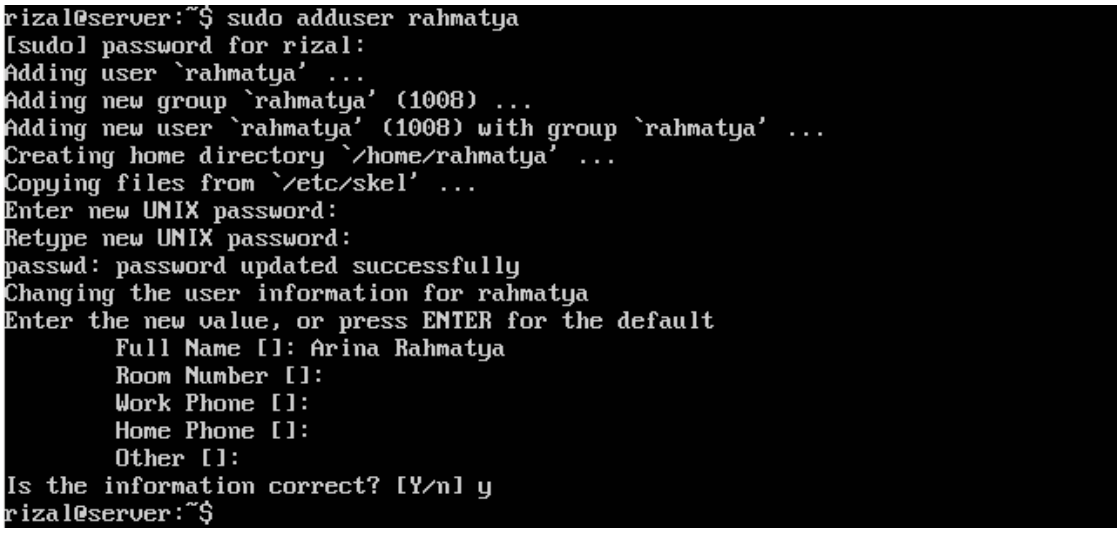
Membuat User baru

Untuk dapat menggunakan layanan e-mail ini tentunya kalian memerlukan setidaknya 2 orang user untuk melakukan proses mengirim dan menerima e-mail. Untuk membuat user baru di Ubuntu Server, ikuti langkah-langkah berikut :

- Eksekusi perintah ini untuk membuat user baru yang misalnya bernama **rahmatya** :

```
sudo adduser rahmatya
```

- Kemudian isikan biodata yang diperlukan oleh sistem seperti password, nama lengkap, nomor handphone, nomor telepon, dan lain-lain. Setelah itu akhiri dengan mengetik huruf **y** pada pertanyaan **Is the information correct?** kemudian tekan **Enter**.



Gambar 3.8.18

- Ulangi langkah diatas dengan membuat user yang lain dengan nama yang berbeda. Setidaknya kalian paling sedikit memerlukan 2 orang user, tapi tidak apa-apa jika kalian membuatnya lebih dari itu.

Uji coba Mail Server

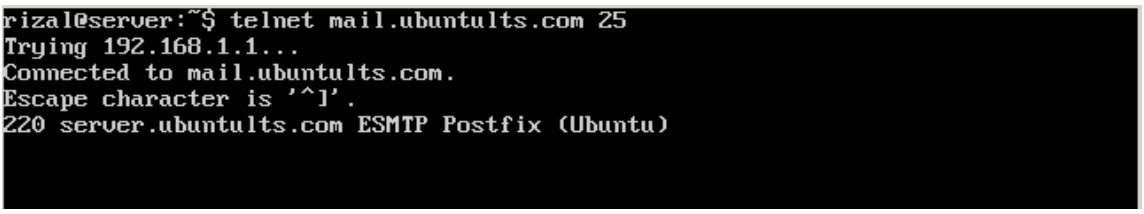
Setelah melakukan konfigurasi dan membuat user-user baru, maka saatnya kalian untuk memulai uji coba pada Mail Server yang telah kalian bangun. Untuk uji coba Mail Server ini, kalian dapat menggunakan 2 metode. Yaitu menggunakan metode remote telnet ke server Postfix kalian, dan langsung menggunakan metode e-mail client seperti Microsoft Outlook atau Thunderbird. Pada buku ini saya hanya akan membahas cara menguji coba dengan menggunakan metode remote telnet.

- Tahap pertama yang harus kalian lakukan adalah meremote domain mail.ubuntults.com melalui port 25 dengan perintah berikut :

```
telnet mail.ubuntults.com 25
```

- Jika berhasil, maka Mail Server akan menjawab seperti ini :

```
Trying 192.168.1.1...
Connected to mail.ubuntults.com.
Escape character is '^]'.
220 server.ubuntults.com ESMTP Postfix (Ubuntu)
```



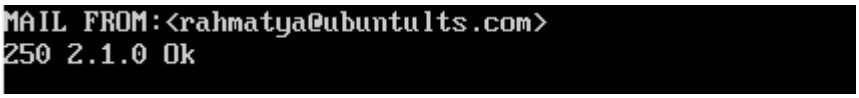
Gambar 3.8.19

- Setelah itu deskripsikan siapa pengirim e-mail dengan mengetikkan ini :

```
MAIL FROM:<rahmatya@ubuntults.com>
```

- Sistem akan menjawabnya seperti ini jika berhasil :

```
250 2.1.0 Ok
```



Gambar 3.8.20

- Kemudian deskripsikan siapa penerima email tersebut. Disini saya masukkan **rahman@ubuntults.com** karena user kedua yang saya buat sebelumnya adalah **rahman**. Kalian isikan saja sesuai dengan user kedua yang telah kalian buat.

```
RCPT TO:<rahman@ubuntults.com>
```

- Tekan **Enter**, lalu sistem akan menjawab seperti ini

```
250 2.1.5 Ok
```

Gambar 3.8.21

- Selanjutnya untuk mengisi Subject dan isi dari pesan tersebut adalah dengan mengetikkan

perintah berikut :

```
DATA
```

- Mesin pun akan menjawabnya seperti ini :

```
354 End data with <CR><LF>.<CR><LF>
```

- Kemudian kalian tuliskan subject dari pesan tersebut dengan perintah ini, lalu tekan **Enter**. :

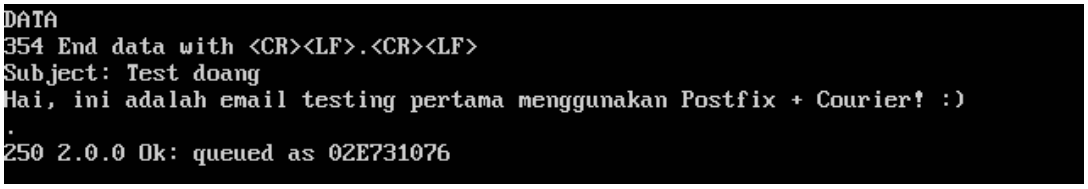
```
Subject : Test doang
```

- Barulah setelah itu kalian masukkan isi pesannya dan akhiri dengan huruf titik pada paragraf baru, lalu tekan **Enter** :

```
Hai, ini adalah email testing pertama menggunakan Postfix + Courier! :)
.
```

- Jika berhasil maka mesin pun akan menjawab dengan kode berikut tanda bahwa e-mail telah terkirim:

```
250 2.0.0 Ok: queued as 02E731076
```



Gambar 3.8.22

- Terakhir ketikkan ini untuk memutuskan koneksi telnet :

```
QUIT
```

Gambar 3.8.23

- Lalu bagaimana cara melihat e-mail yang masuk? Caranya adalah dengan login sebagai user yang telah dikirimi e-mail dengan perintah berikut :

```
su rahman
```

- Kemudian masuklah kedalam direktori **/home/rahman/Maildir/new** dengan mengeksekusi

perintah ini :

```
cd /home/rahman/Maildir/new
```

- Jika berhasil, maka seharusnya di dalam direktori tersebut ada sebuah file yang berisi pesan e-mail yang telah dikirim oleh user **rahmatya** sebelumnya. Cek dengan perintah ls :

```
ls
```

Gambar 3.8.24

- Untuk melihat isi e-mail tersebut, ketikkan perintah ini dimana **1345630320.V801I42bb9M283842.server** adalah nama filenya :

```
cat 1345630320.V801I42bb9M283842.server
```

Gambar 3.8.25

- Terlihat bukan isi e-mailnya? Sampai sini berarti kalian telah berhasil melakukan instalasi, konfigurasi, dan pengetesan Mail Server dengan menggunakan Postfix dan Courier.

3.9. Instalasi Webmail Server

Sebelum memulai instalasi Webmail Server, perlu kalian ketahui terlebih dahulu bahwa Webmail berbeda dengan Mail. Webmail hanyalah merupakan *frontend* dari Mail. Inti mekanismenya sebenarnya terdapat pada Mail Server, bukan pada Webmail Servernya. Karena tujuan Webmail hanya untuk memudahkan user dalam mengakses Mail Server tersebut. Seperti halnya sebuah Bank, apabila kalian ingin mengirim uang bukankah jauh lebih mudah dan praktis jika kalian mengirim uang melalui ATM daripada harus mengirim uang dari pusat Bank nya langsung? Akan tetapi, tanpa sebuah Bank, ATM tidak akan ada gunanya, sebaliknya tanpa ATM, Bank tetap akan dapat

berfungsi dengan normal. Begitu pula dengan Mail dan Webmail, tanpa adanya Mail Server, Webmail Server tidak akan ada gunanya. Akan tetapi jika Mail Server tanpa Webmail Server, Mail Server tersebut tetap dapat bekerja sebagaimana biasa.

Instalasi Roundcube

Beberapa contoh Webmail yang terkenal adalah Squirrelmail, Zimbra, dan Roundcube. Roundcube saya pilih karena instalasi dan konfigurasinya mudah, aplikasinya ringan, dan tampilannya cukup bagus dibandingkan dengan Squirrelmail.

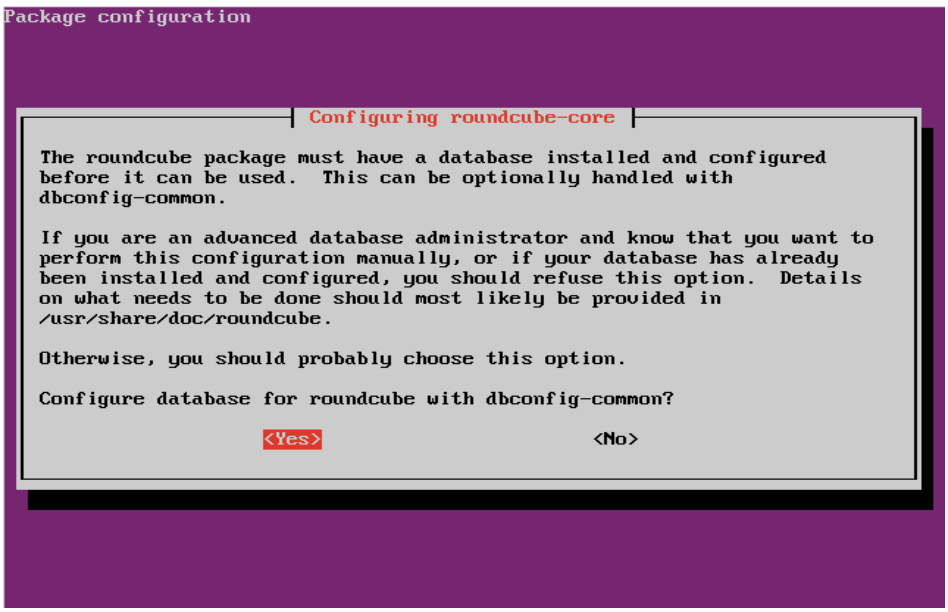
- Untuk menginstall Roundcube di Ubuntu Server, ketikkan perintah berikut ini :

```
sudo apt-get install roundcube-core roundcube roundcube-mysql
```

```
  libc6-dev libfontconfig1 libgd2-xpm libgomp1 libicu48 libjpeg-turbo8
  libjpeg8 libjs-jquery-ui libltdl-dev libmpc2 libmpfr4 libquadmath0
  libssl-dev libssl-doc libt1-5 libtool libxpm4 linux-libc-dev m4 manpages-dev
  php-auth php-auth-sasl php-mail-mime php-mail-mimedecode php-mdb2
  php-mdb2-driver-mysql php-net-smtp php-net-socket php-pear php5-dev php5-gd
  php5-intl php5-pspell roundcube-core shtool tinymce wwwconfig-common
  zlib1g-dev
Suggested packages:
  aspell-doc spellutils autoconf2.13 autoconf-archive gnu-standards
  autoconf-doc gettext binutils-doc cpp-doc gcc-4.6-locales ispell
  emacsen-common jed-extra gcc-multilib make automake1.9 flex bison gdb
  gcc-doc gcc-4.6-multilib libmudflap0-4.6-dev gcc-4.6-doc libgcc1-dbg
  libgomp1-dbg libquadmath0-dbg libmudflap0-dbg binutils-gold glibc-doc
  libgd-tools libjs-jquery-ui-docs libtool-doc automaken gfortran
  fortran95-compiler gcj php-log php-soap php-crypt-gpg roundcube-plugins
  postgresql-client
The following NEW packages will be installed:
  aspell aspell-en autoconf automake autotools-dev binutils cpp cpp-4.6
  dictionaries-common gcc gcc-4.6 javascript-common libaspell15 libc-dev-bin
  libc6-dev libfontconfig1 libgd2-xpm libgomp1 libicu48 libjpeg-turbo8
  libjpeg8 libjs-jquery-ui libltdl-dev libmpc2 libmpfr4 libquadmath0
  libssl-dev libssl-doc libt1-5 libtool libxpm4 linux-libc-dev m4 manpages-dev
  php-auth php-auth-sasl php-mail-mime php-mail-mimedecode php-mdb2
  php-mdb2-driver-mysql php-net-smtp php-net-socket php-pear php5-dev php5-gd
  php5-intl php5-pspell roundcube roundcube-core roundcube-mysql shtool
  tinymce wwwconfig-common zlib1g-dev
0 upgraded, 54 newly installed, 0 to remove and 0 not upgraded.
Need to get 0 B/40.4 MB of archives.
After this operation, 119 MB of additional disk space will be used.
Do you want to continue [Y/n]? y
```

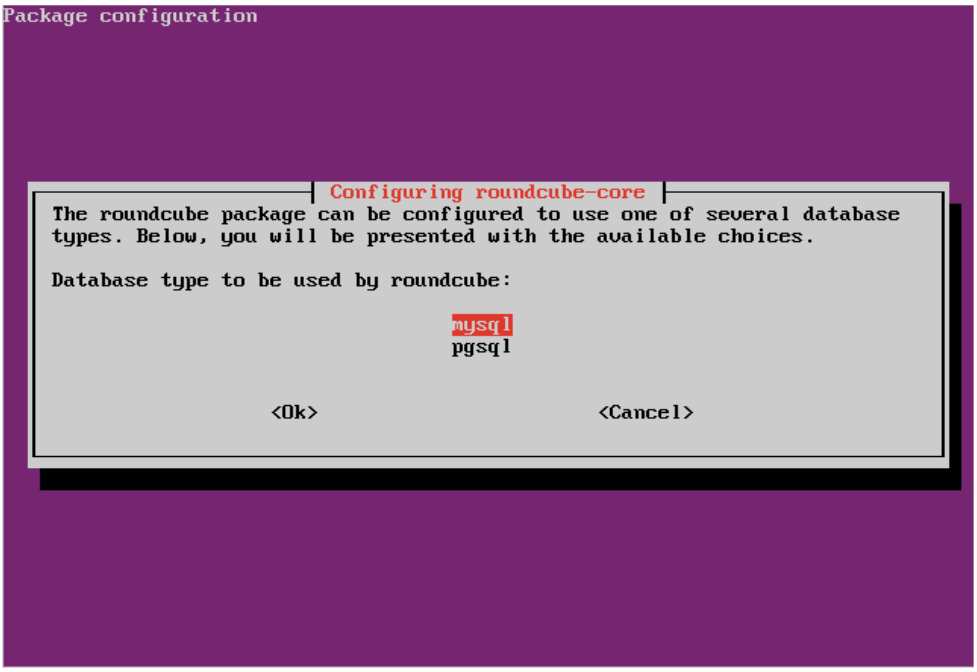
Gambar 3.9.1

- Kemudian akan muncul penawaran untuk menginstallkan database untuk Roundcube, pilih **Yes**.



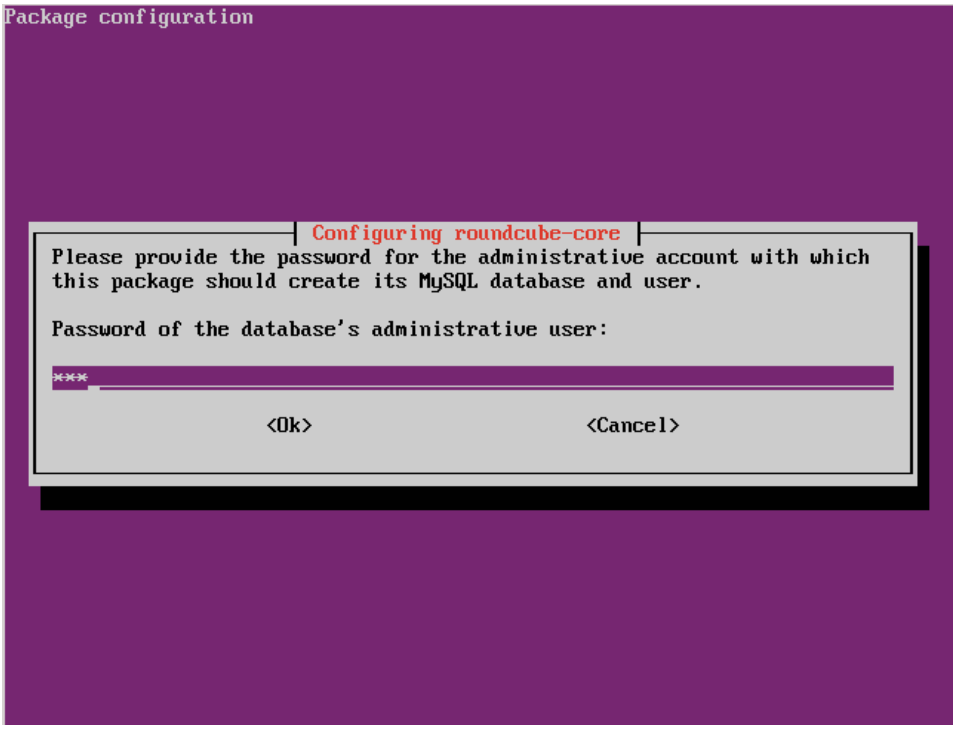
Gambar 3.9.2

- Lalu muncul dua pilihan untuk memilih database mana yang akan dipilih. Tekan **Enter** pada pilihan **Mysql**.



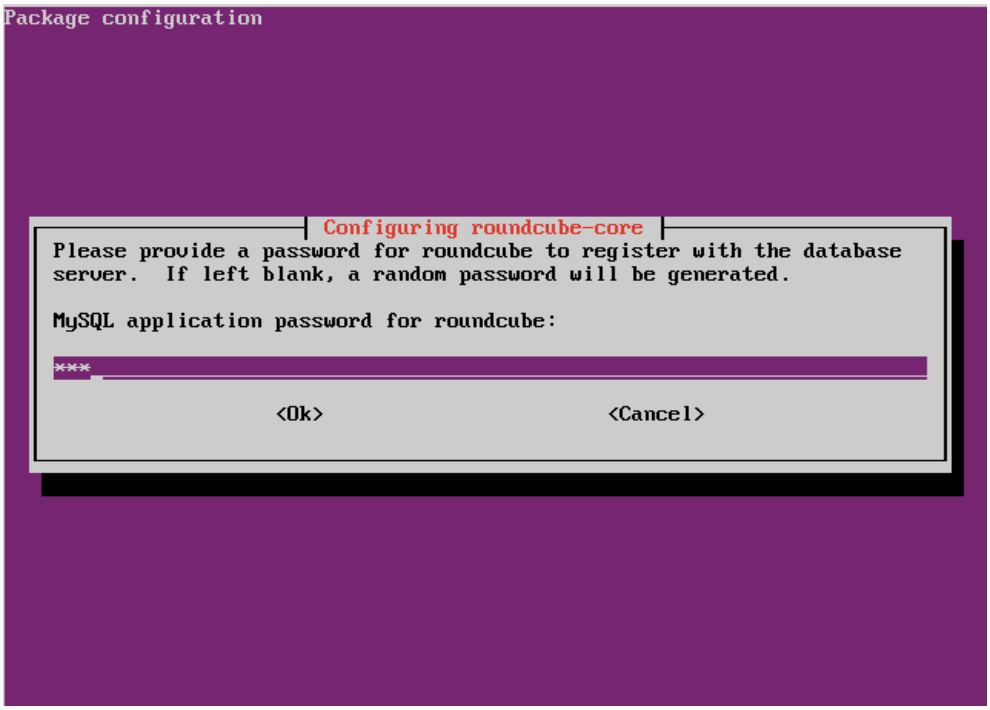
Gambar 3.9.3

- Setelah itu kalian diminta untuk memasukkan password Mysql kalian. Tekan **Enter** jika sudah.

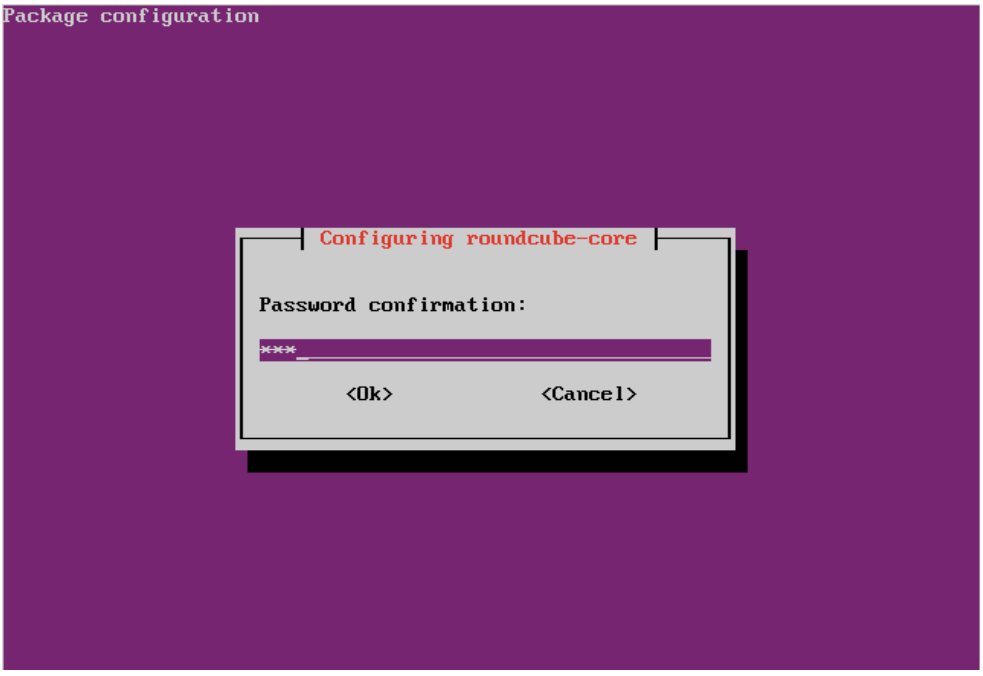


Gambar 3.9.4

- Selanjutnya kalian diminta untuk memasukkan password baru untuk database Roundcubenya, tekan **Enter** jika sudah (Gambar 3.9.5), kemudian konfirmasikan lagi password tersebut lalu tekan **Enter** (Gambar 3.9.6).

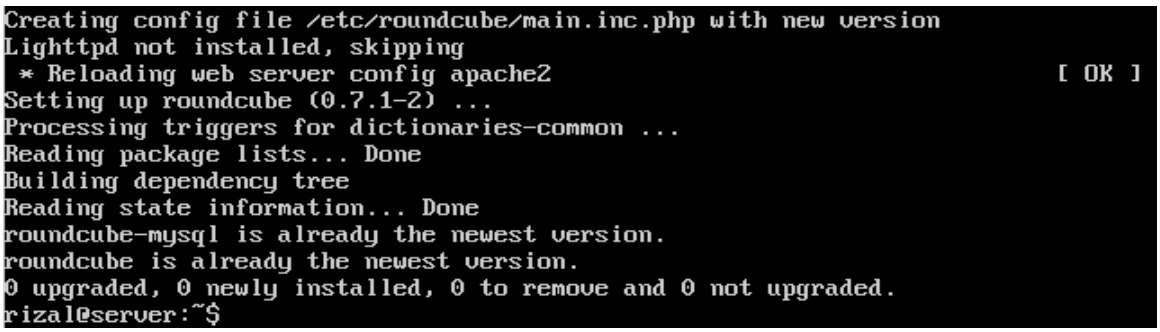


Gambar 3.9.5



Gambar 3.9.6

- Terakhir tunggu hingga proses instalasi selesai seperti yang ditunjukkan oleh gambar dibawah ini :



Gambar 3.9.7

- Jika terdapat pesan error dan instalasi gagal, jangan lupa lakukan perintah ini berulang kali hingga proses instalasi selesai dan tidak ada pesan kesalahan lagi :

```
sudo apt-get -f install && sudo apt-get install roundcube-core roundcube roundcube-mysql
```

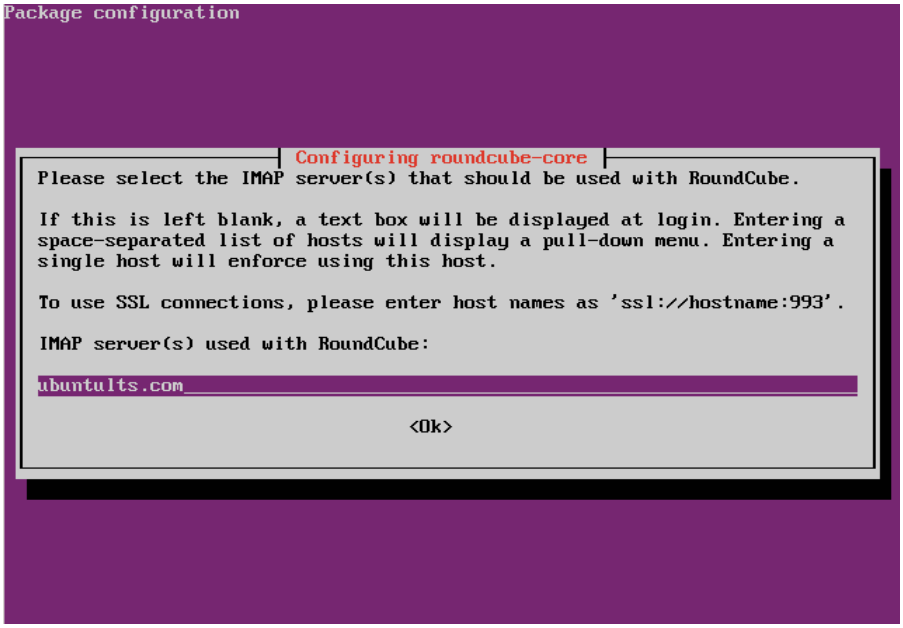
Konfigurasi Roundcube

Konfigurasi Roundcube tidak terlalu rumit. Hanya perlu menambahkan alamat server IMAP dan menulis file konfigurasi pada Webserver pada saat melakukan perintah dpkg-reconfigure. Caranya adalah sebagai berikut :

- Pertama ketikkan perintah berikut ini :

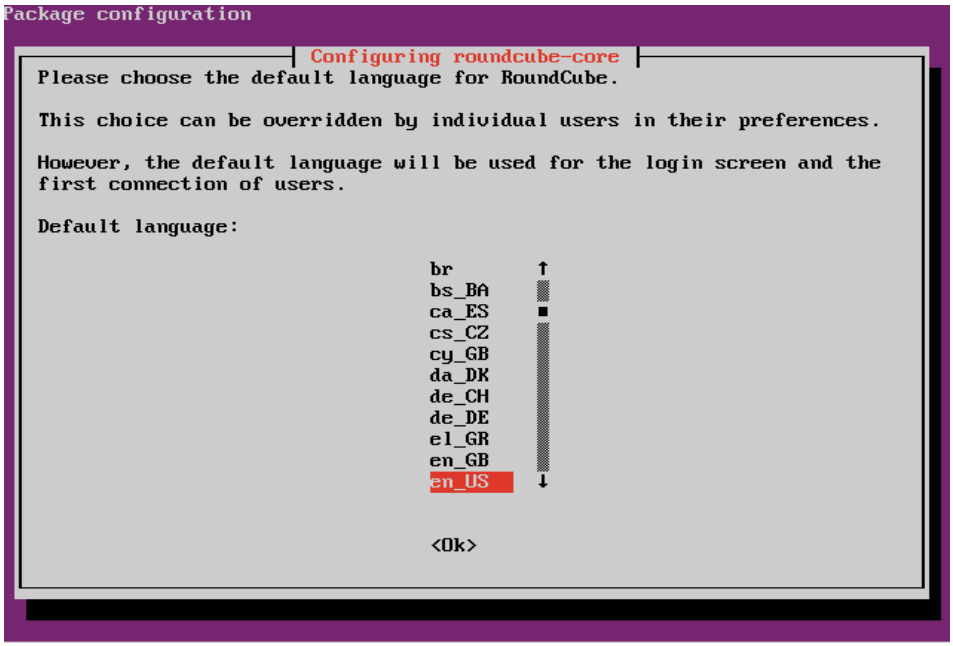
```
sudo dpkg-reconfigure roundcube-core
```

- Setelah itu isikan domain kalian pada saat diminta alamat IMAP servernya. Disini saya masukkan **ubuntults.com** :



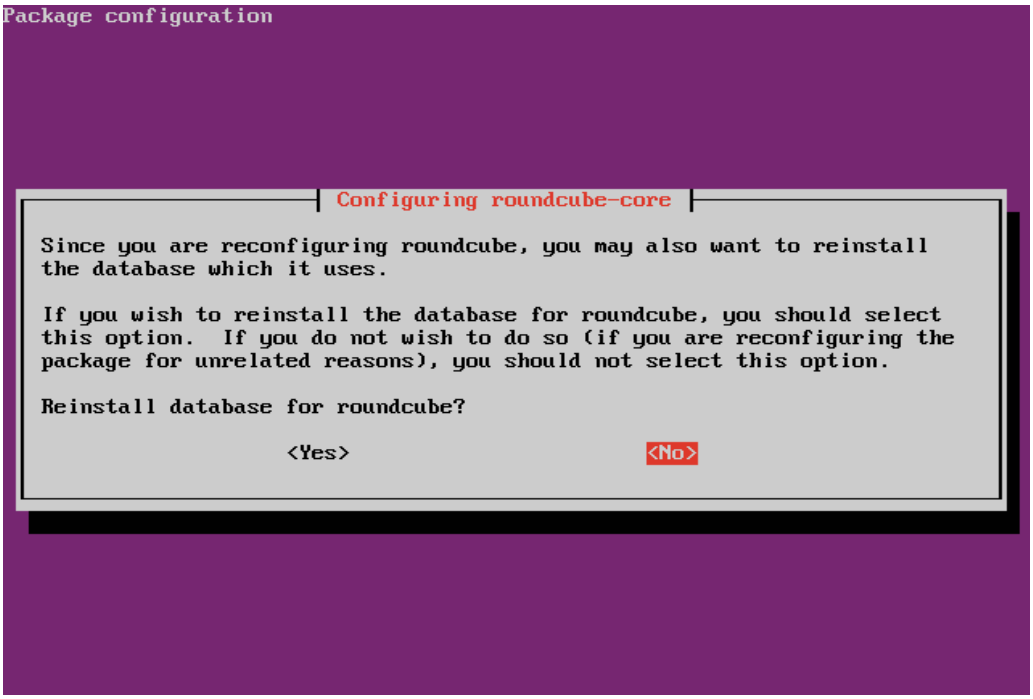
Gambar 3.9.8

- Untuk bahasa yang akan digunakan secara default, pilih **en_US**.



Gambar 3.9.9

- Jika diminta untuk menginstall ulang Database, pilih saja **No**.

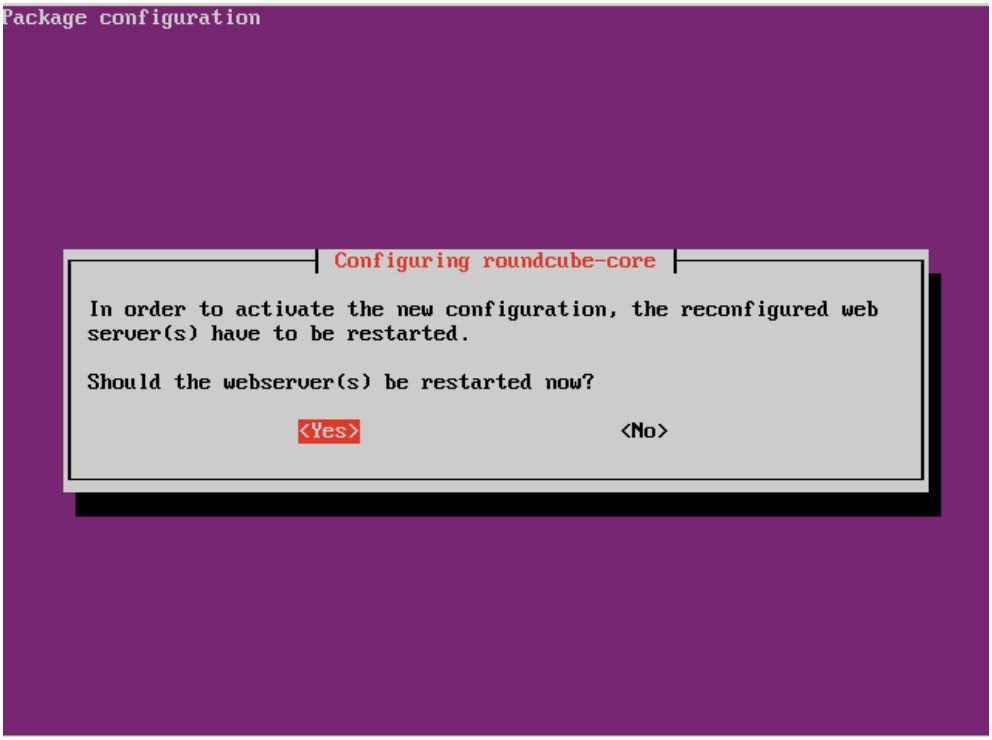


Gambar 3.9.10

- Lalu pada bagian ini, hilangkan centang pada pilihan **lighttpd** dengan menekan tombol **Spasi**, setelah itu baru tekan **Enter**.

Gambar 3.9.11

- Setelah itu pilih **Yes** jika muncul ditanya ingin merestart Webserver atau tidak, lalu tekan **Enter**.



Gambar 3.9.12

- Setelah proses dpkg-reconfigure selesai, sekarang kalian harus membuat *simbolic link* agar Webserver apache dapat melink/mengakses direktori tempat Webmail berada walaupun direktori tersebut berada di luar direktori root dari apache.. Caranya adalah dengan mengetik perintah berikut ini :

```
sudo ln -s /usr/share/roundcube/ /var/www/roundcube
```

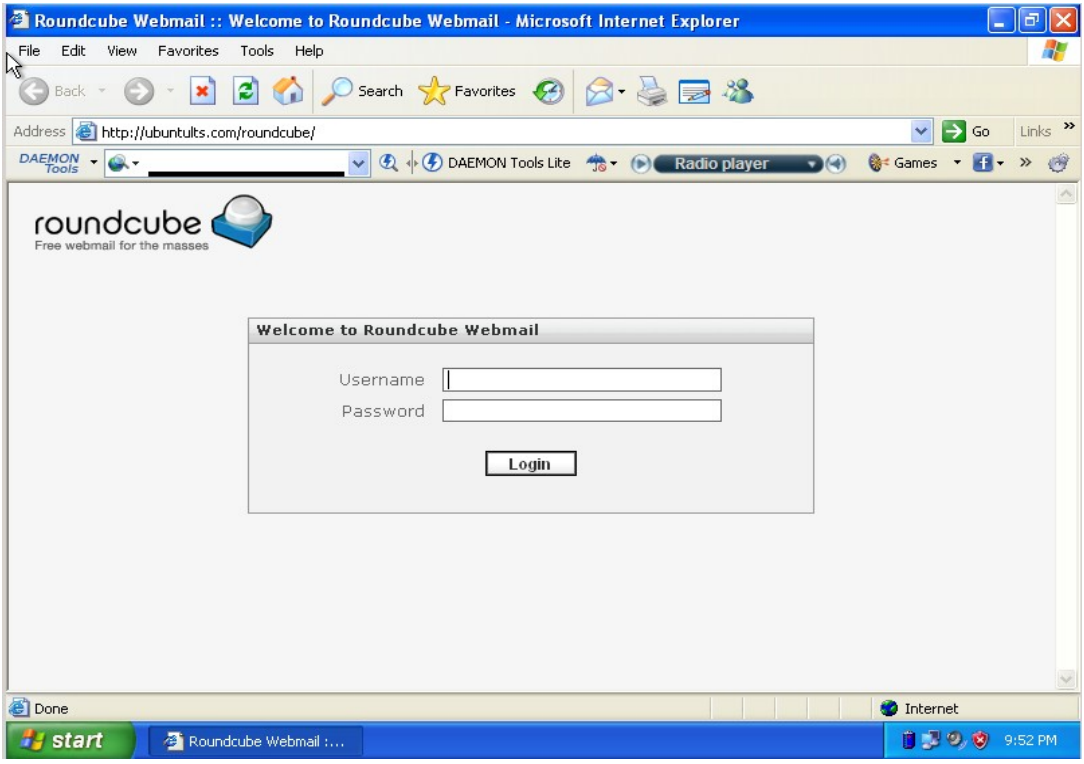
- Terakhir restart service dari apachenya dengan mengeksekusi perintah berikut :

```
sudo service apache2 restart
```

```
rizal@server:~$ sudo service apache2 restart
[sudo] password for rizal:
 * Restarting web server apache2
 ... waiting                                                    [ OK ]
rizal@server:~$
```

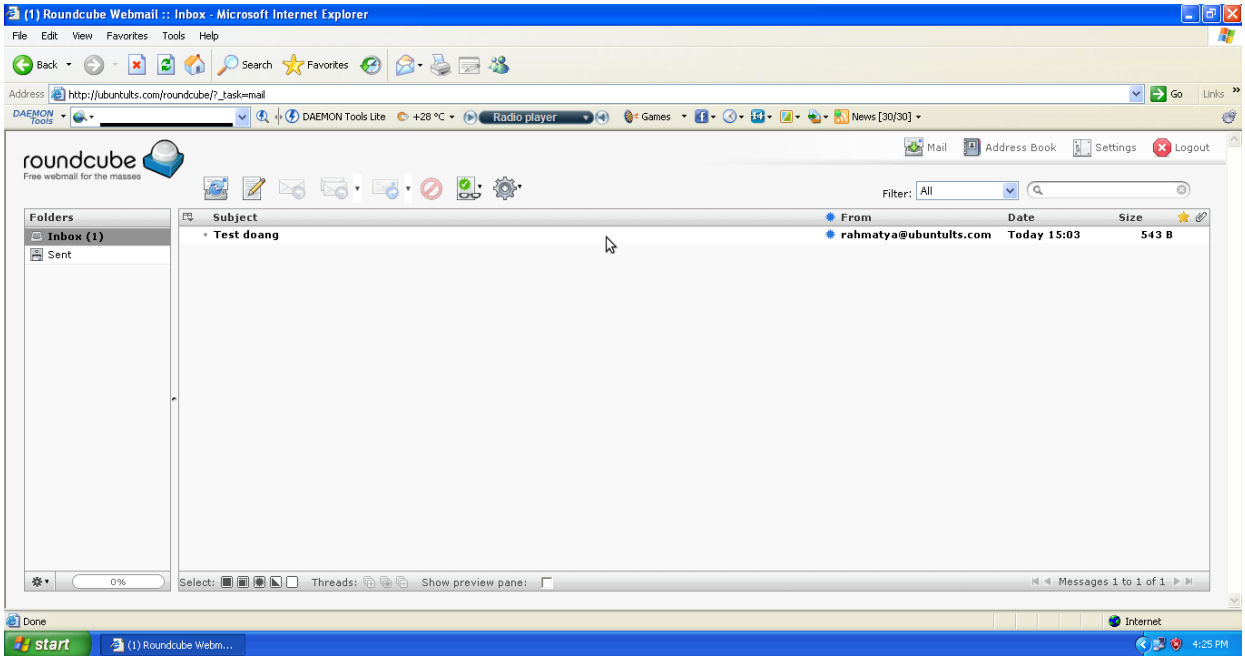
Gambar 3.9.13

- Sekarang dari browser client, kalian dapat mengakses Webmail Roundcube melalui alamat http://ubuntults.com/roundcube

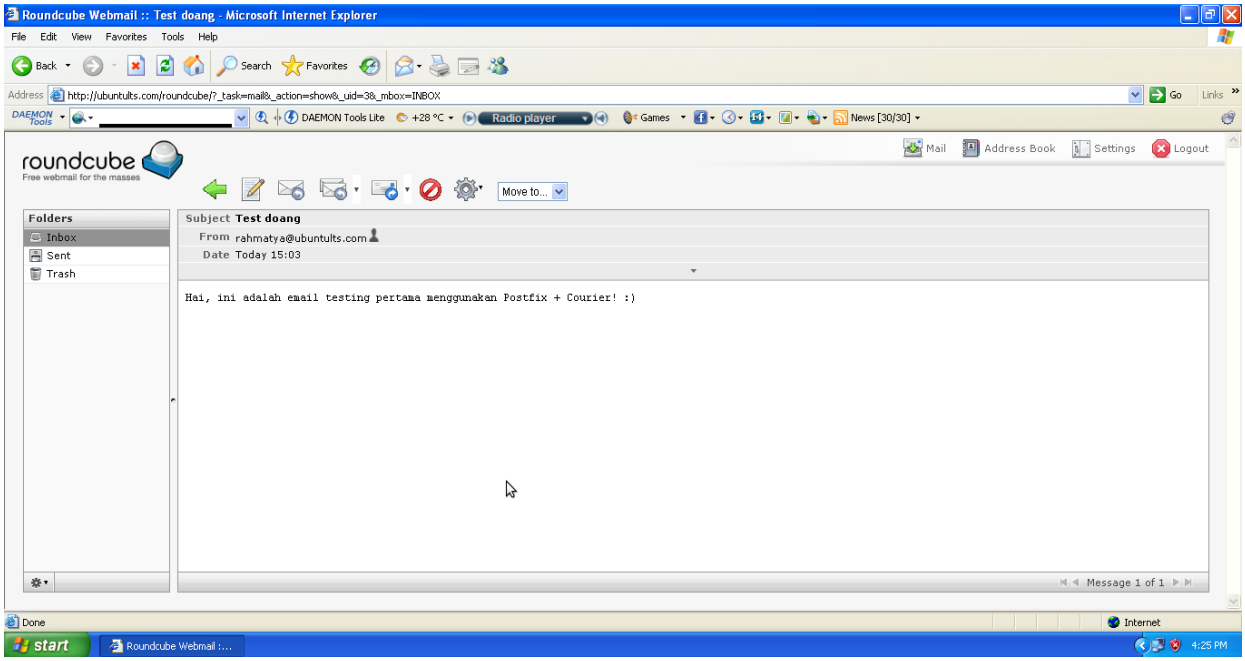


Gambar 3.9.14

- Cobalah login dengan menggunakan user **rahman** yang telah dikirim e-mail oleh user **rahmatya** pada praktek Mail Server sebelumnya. Coba lihat, didalam inbox user tersebut pasti ada e-mail yang berisi e-mail kiriman dari user **rahmatya** yang tadi.



Gambar 3.9.15



Gambar 3.9.16

- Sampai sini Webmail Roundcube sudah dapat digunakan dengan sempurna. Cobalah untuk saling mengirim e-mail antar user maupun mencoba fitur-fitur lain dari Webmail Roundcube ini. Agar lebih efisien, kalian juga dapat mengubah alamat Webmail dari http://ubuntults.com/roundcube menjadi http://mail.ubuntults.com dengan metode *Virtual Host* yang kalian pelajari nanti pada Bab Tambahan.

3.10. Instalasi Telnet Remote Server

Telnet atau *TELecommunication NETwork* merupakan sebuah protokol jaringan yang digunakan di internet dan juga jaringan komputer lokal. Gunanya adalah untuk menghubungkan antara komputer Linux yang satu dengan komputer Linux lainnya. Pada awal kemunculannya, Telnet didesain untuk memudahkan proses komunikasi yang dapat menghubungkan antara PC Client dengan Server, dimana kalian dapat melakukan berbagai perintah dari PC Client seolah-olah perintah tersebut sedang dieksekusi di Komputer sendiri, padahal sebenarnya seluruh perintah tersebut sedang kalian eksekusi di Server. Proses ini biasa disebut sebagai proses *remote* dimana kalian dapat melakukan apa saja seolah-olah berada di komputer sendiri.

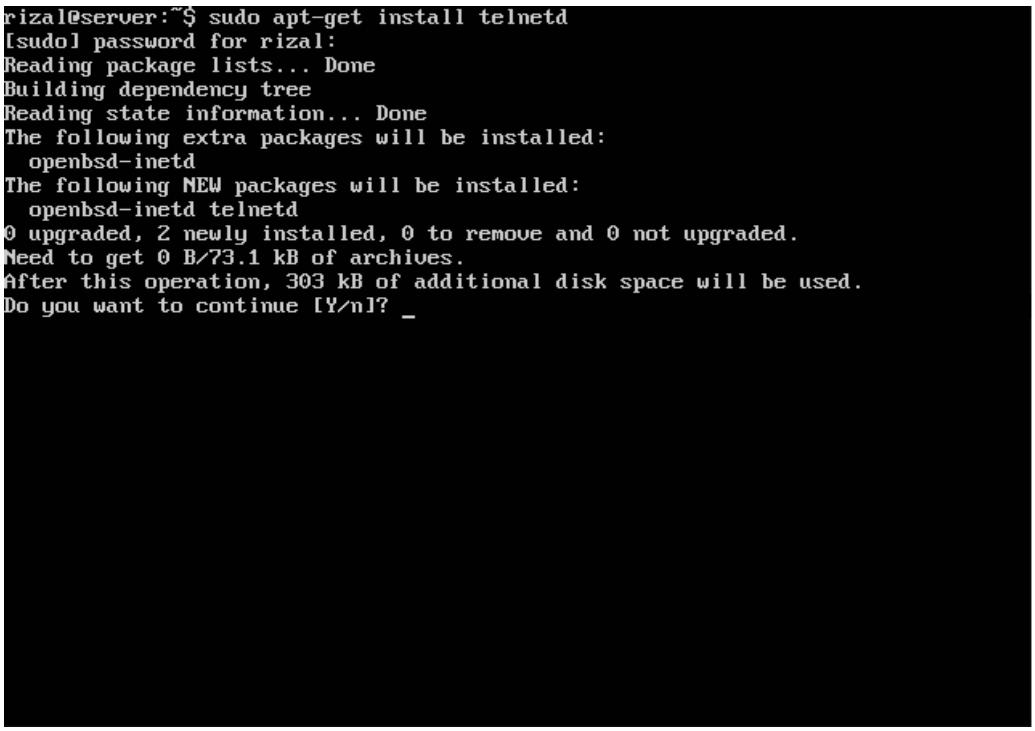
Istilah remote ini sangatlah penting di dalam dunia jaringan. Karena memang sesuai fungsinya, *benar-benar* memudahkan. Coba bayangkan, jika kalian sekarang sedang santai-santinya berlibur di Eropa, ternyata kalian lupa untuk mematikan Komputer kalian yang ada dirumah. Tentunya sangat tidak mungkin jika kalian harus pulang dulu bukan? Disinilah fungsi dari remote ini diperlukan. Kalian cukup mematikan saja komputer kalian dari Eropa dengan menggunakan teknik remote ini. Contoh lain lagi misalnya kalian bekerja di sebuah perusahaan di Jakarta. Kemudian kalian diminta oleh perusahaan untuk mengkonfigurasi Webserver milik perusahaan yang ada di China. Tentunya kalian tidak mungkin jika harus bolak-balik Indonesia-China hanya untuk mengkonfigurasi Webserver tersebut. Belum lagi jika mendadak ada masalah atau apa. Untuk itulah fungsi remote server ini mutlak diperlukan.

Instalasi Telnet

Instalasi Telnet Server di Ubuntu Server 12.04 LTS cukup mudah, berikut adalah langkah-langkahnya :

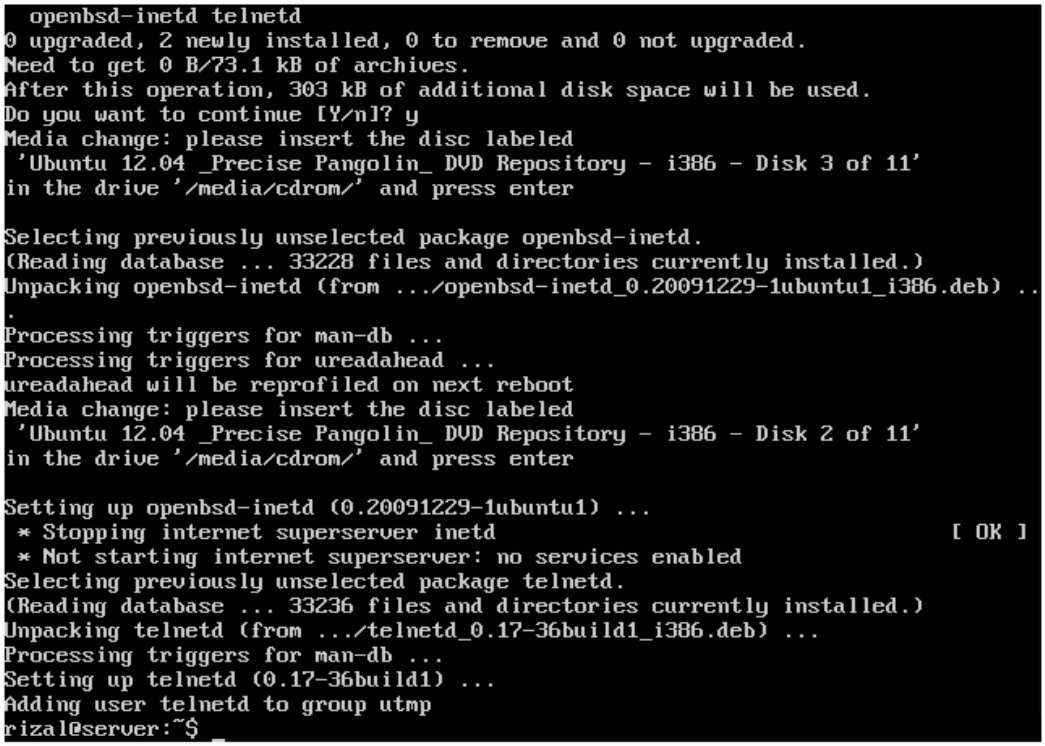
- Eksekusi perintah berikut untuk instalasinya :

```
sudo apt-get install telnetd
```



Gambar 3.10.1

- Masukkan DVD-DVD yang diminta selama proses instalasi, kemudian pastikan instalasi selesai tanpa ada pesan error seperti yang tampak pada gambar dibawah ini.



Gambar 3.10.2

- Proses instalasi Telnet Server pun telah selesai. Jika ada pesan error selama proses instalasi, seperti biasa eksekusilah perintah berikut berulang-ulang sampai pesan error tersebut tidak muncul lagi.

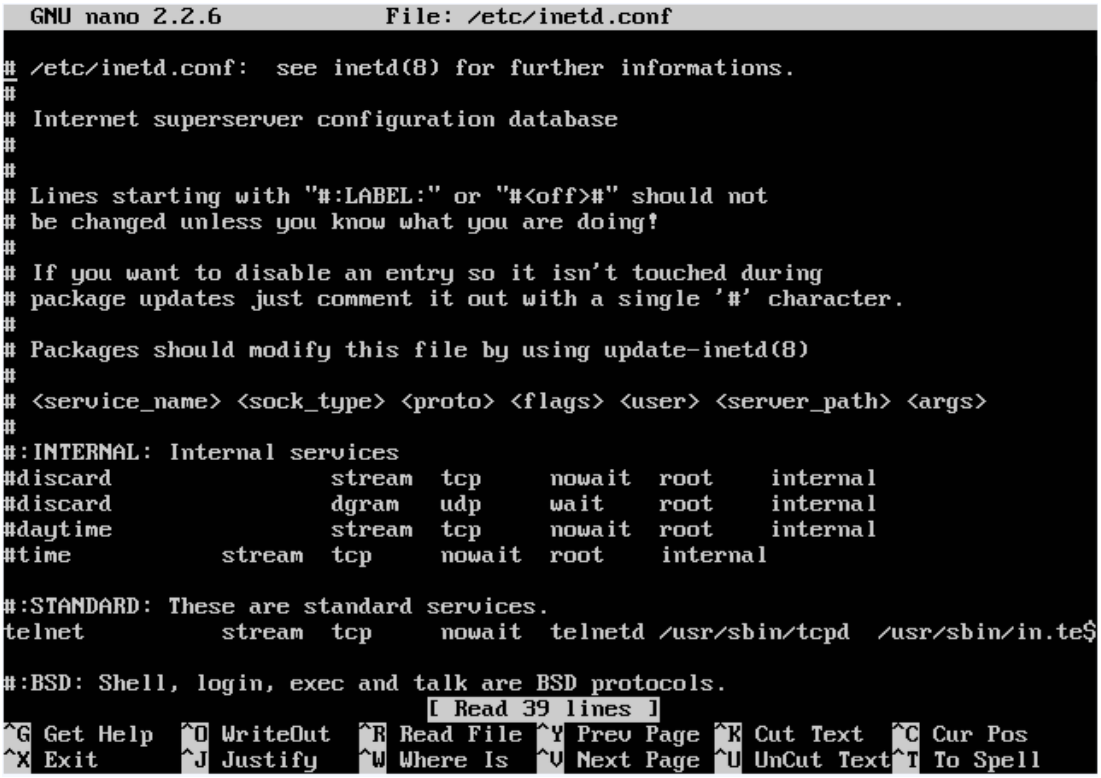
```
sudo apt-get -f install && sudo apt-get install telnetd
```

Konfigurasi Telnet

Secara default, service Telnet sudah dapat berjalan dengan baik tanpa perlu dikonfigurasi lagi. Tapi apabila kalian ingin melakukan konfigurasi tambahan, kalian dapat mengedit file /etc/inetd.conf.

- Bukalah file /etc/inetd.conf dengan perintah dibawah ini :

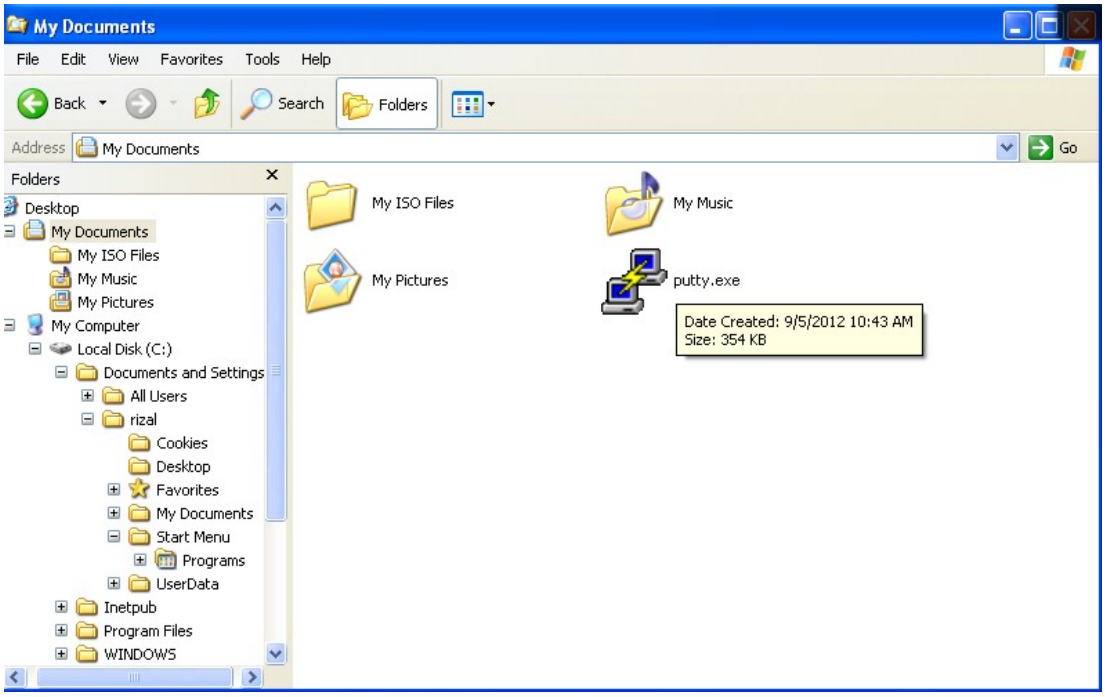
```
sudo nano /etc/inetd.conf
```



Gambar 3.10.3

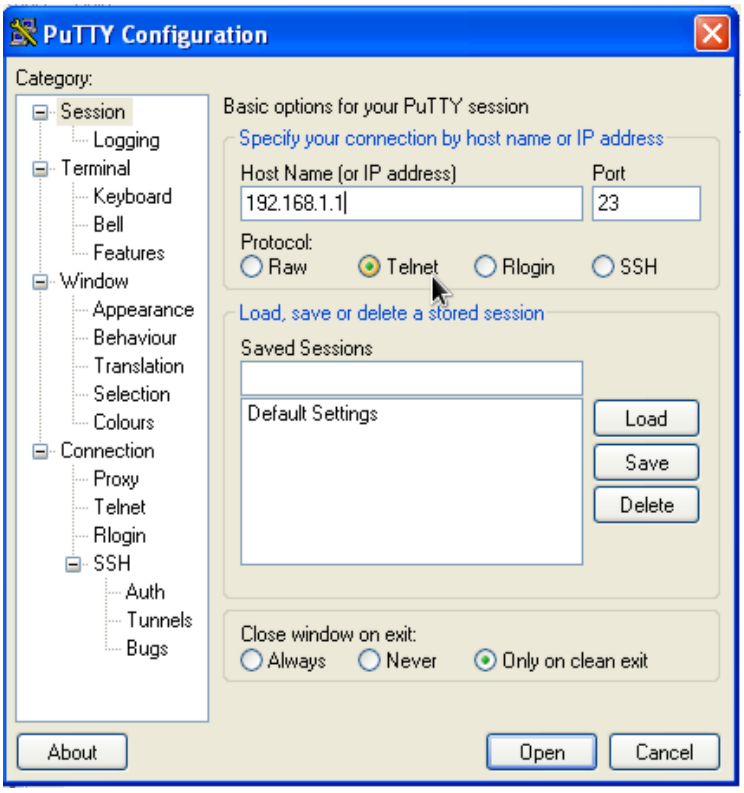
- Disitu kalian dapat melakukan berbagai konfigurasi tambahan seperti konfigurasi *BSD Protocol*, dan sebagainya. Jika sudah selesai, jangan lupa untuk menyimpan filenya dengan menekan kombinasi **CTRL + W**, lalu ketik **Y**, lalu **Enter**.
- Sekarang cobalah lakukan testing dari komputer client dengan meremote Ubuntu Server kalian masing-masing. Pada Sistem Operasi Windows, diperlukan software tambahan untuk melakukan remote Telnet. Salah satu software favorit untuk itu adalah *Putty*. Kalian dapat mengunduh Putty melalui website resminya di http://putty.org.

- Bukalah software Putty di komputer client kalian.



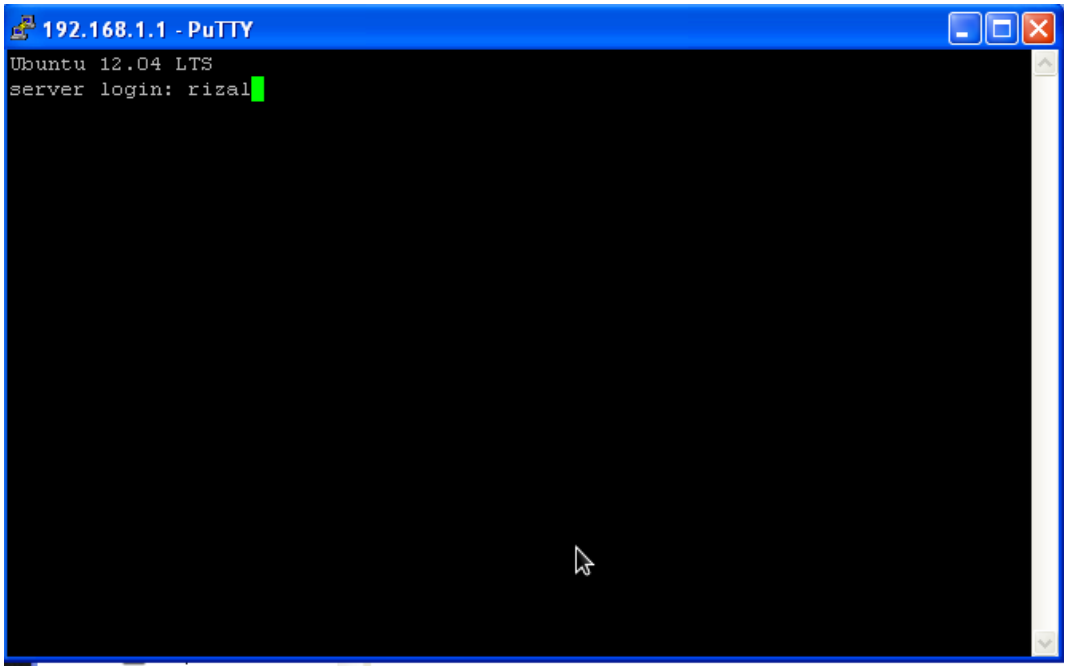
Gambar 3.10.4

- Isikan ip address Server pada kolom **Hostname** dan pilihlah protokol **Telnet** pada bagian **Protocol**. Sisanya biarkan saja apa adanya. Klik **Open** jika sudah selesai.

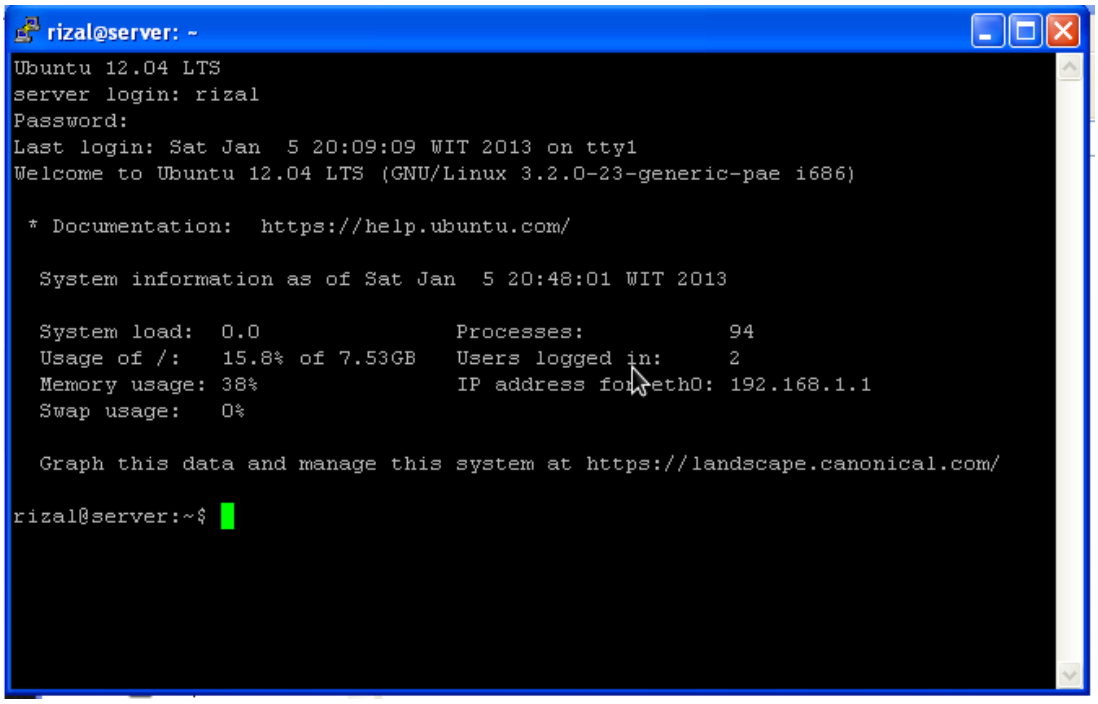


Gambar 3.10.5

- Setelah itu nanti akan muncul form login. Isikan Username dan Password Ubuntu Server kalian masing-masing. Jika berhasil maka akan muncul tampilan yang sama persis seperti Ubuntu Server kalian.



Gambar 3.10.6



Gambar 3.10.7

- Sampai sini berarti Telnet Server telah berfungsi dengan baik. Dan ingat, apapun yang kalian

lakukan pada jendela Putty tersebut, sama saja dengan kalian melakukannya di Ubuntu Server, bukanlah di Komputer Client kalian.

3.11. Instalasi SSH Remote Server

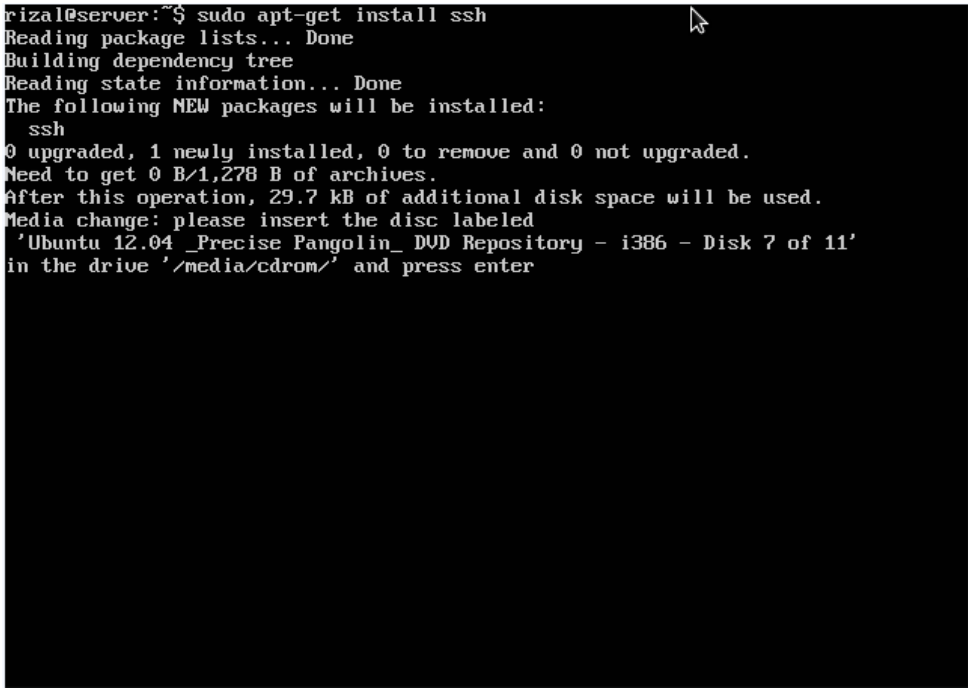
SSH, singkatan dari *Secure Shell* adalah aplikasi jaringan yang berfungsi sama dengan Telnet yaitu untuk melakukan komunikasi *remote* antar komputer. Pada masa kini, teknologi Telnet sudah banyak ditinggalkan karena dianggap kurang aman. Komunikasi Telnet terlalu jelas, sehingga lalu lintas komunikasi dapat dengan mudah disadap. Ternyata SSH mampu mengatasi hal tersebut. SSH bisa memberikan keamanan karena adanya fasilitas Enkripsi yang mampu membuat integritas dan kerahasiaan data terjaga. SSH menggunakan kriptografi public key untuk melakukan autentifikasi komputer remote dan untuk mengizinkan komputer remote untuk mengautentifikasi user jika diperlukan.

Instalasi SSH

Untuk instalasi SSH di Ubuntu Server 12.04 LTS, langkah-langkahnya adalah sebagai berikut :

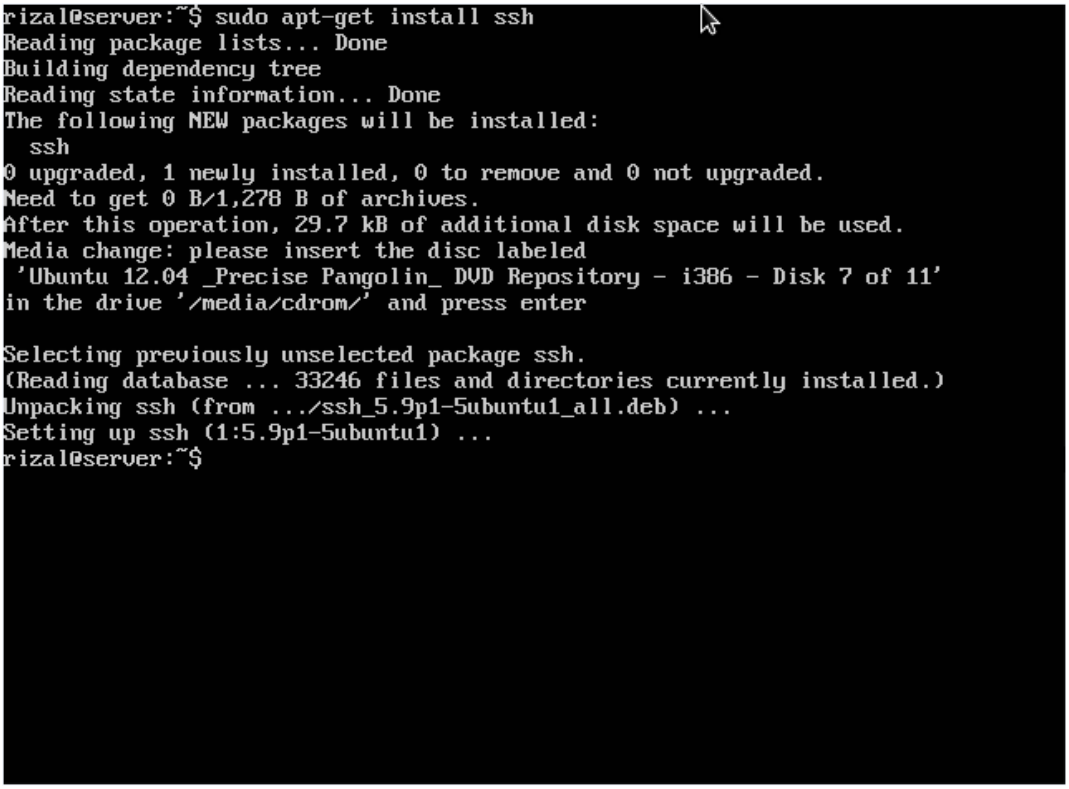
- Pertama-tama eksekusilah perintah ini untuk menginstall SSH Server :

```
sudo apt-get install ssh
```



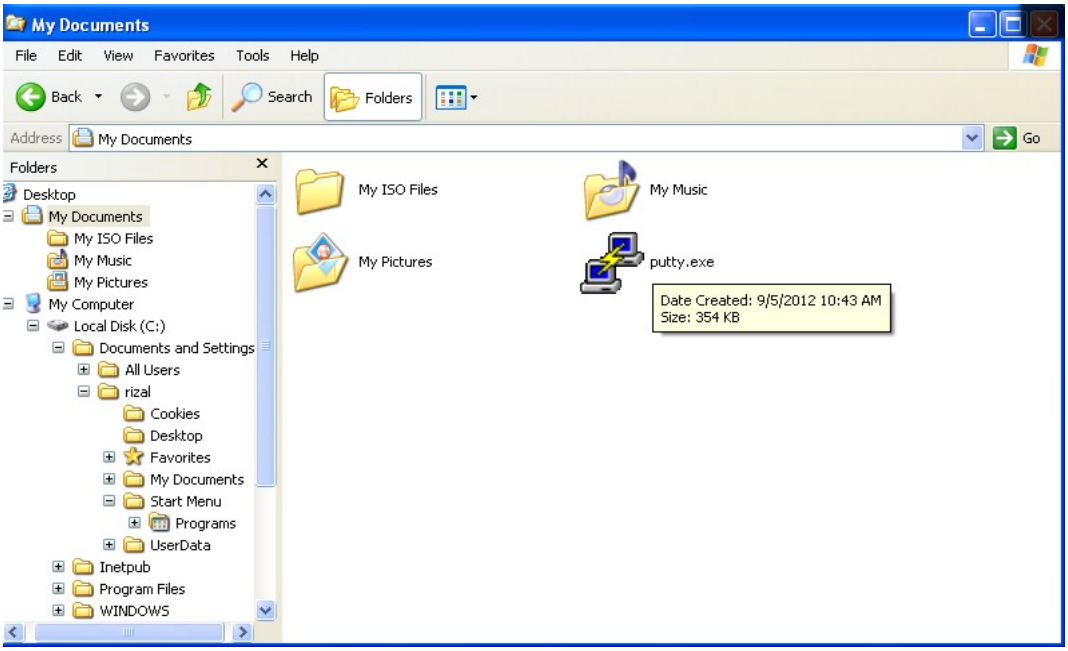
Gambar 3.11.1

- Jika sudah, tunggu dan pastikan tidak ada pesan error yang muncul selama proses instalasi.



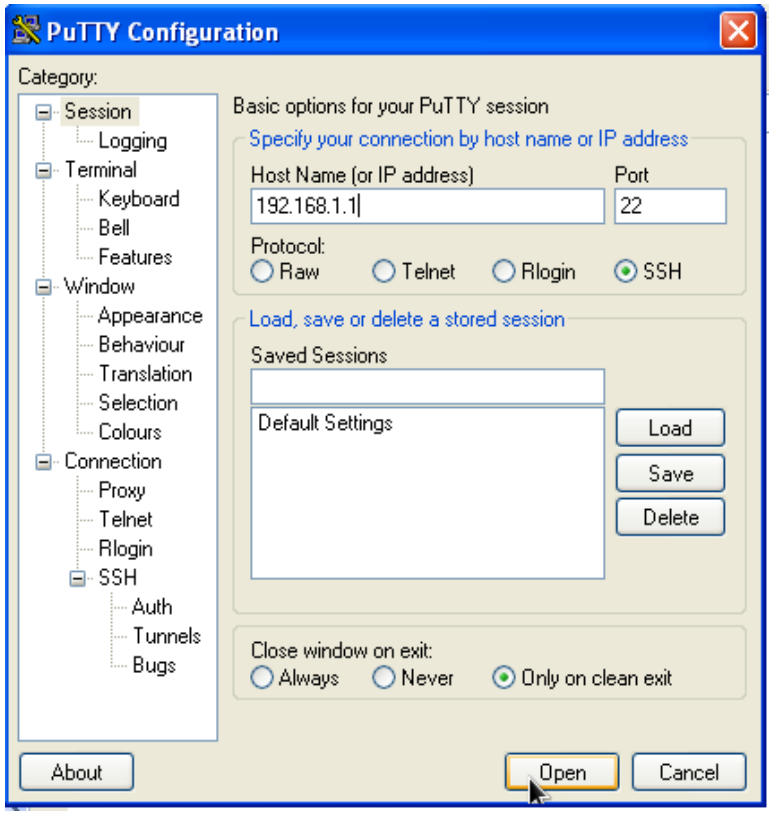
Gambar 3.11.2

- Setelah terinstall, kalian dapat me-*remote* Ubuntu Server melalui SSH dengan cara yang hampir mirip dengan Telnet. Bukalah program *Putty* terlebih dahulu.



Gambar 3.11.3

- Isikan ip address Server pada kolom **Hostname** dan pilihlah protokol **SSH** pada bagian **Protocol**. Sisanya biarkan saja apa adanya. Klik **Open** jika sudah selesai.

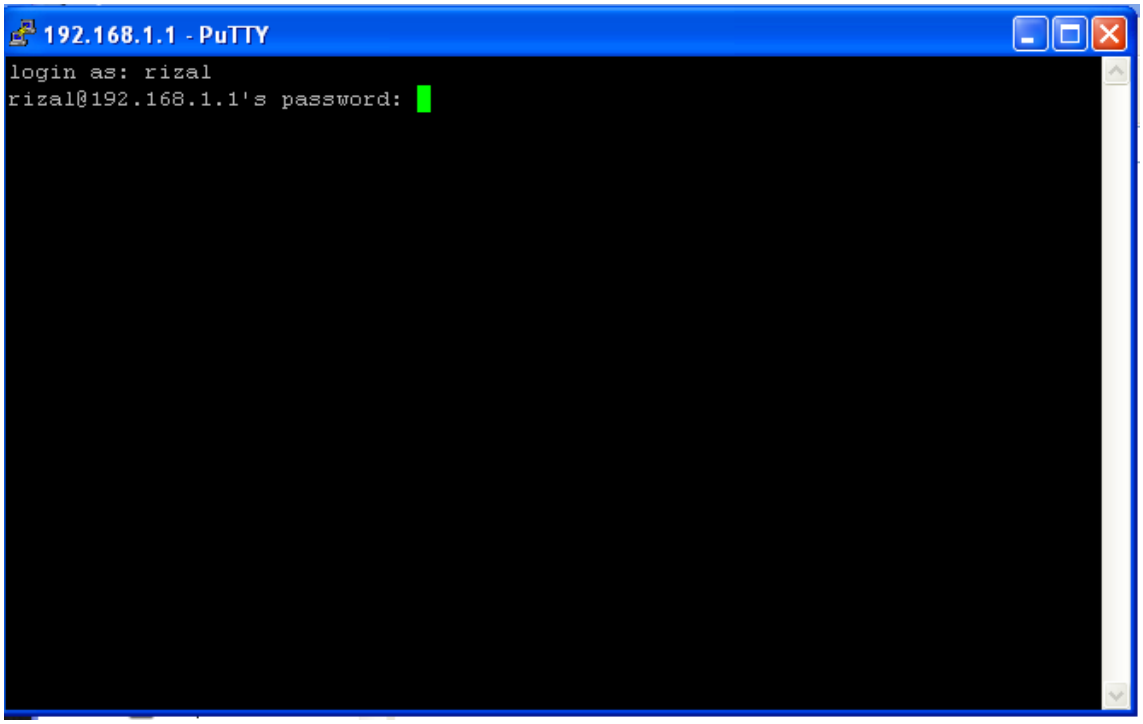


Gambar 3.11.4

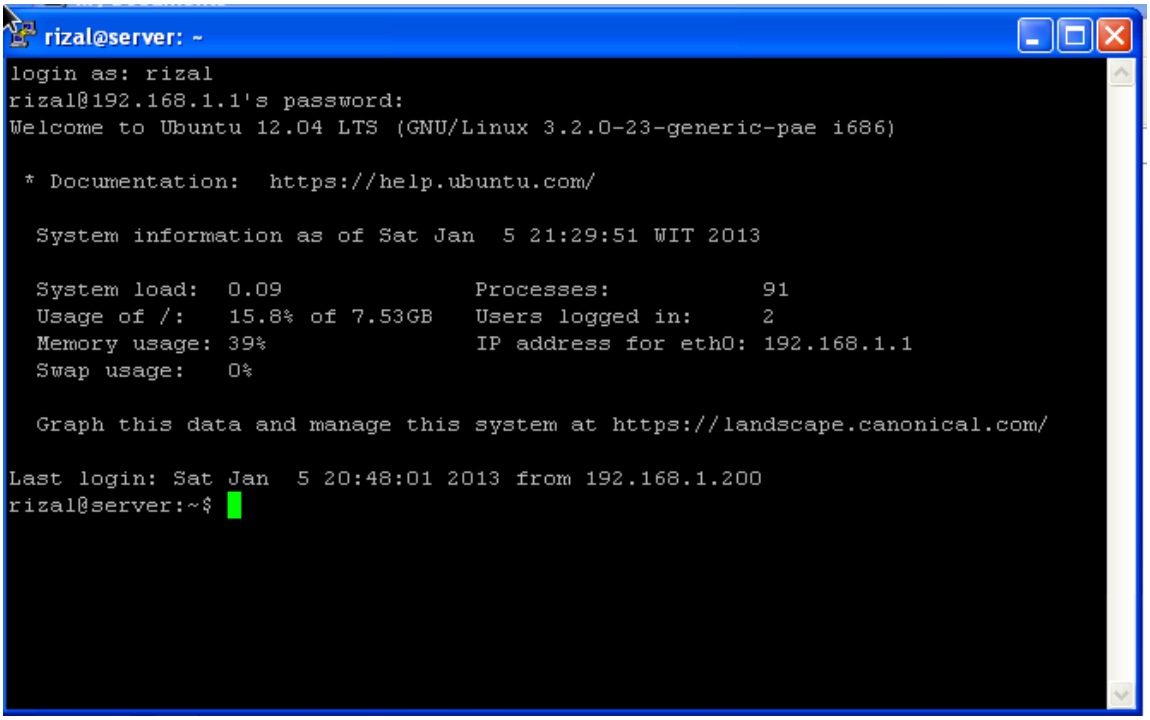
- Setelah itu akan muncul peringatan untuk menambahkan autentikasi *fingerprint key login* agar kedua komputer dapat saling berhubungan. Pilih **Yes**. Inilah yang menyebabkan komunikasi SSH lebih aman dibandingkan dengan Telnet, karena SSH mewajibkan kedua komputer memiliki fingerprint key login masing-masing sehingga orang lain yang tidak mempunyai fingerprint key login ini, tidak akan bisa sembarangan menyadap komunikasi SSH.

Gambar 3.11.5

- Selanjutnya isikan Username dan Password Ubuntu Server dengan benar agar bisa login. Jika tampil seperti gambar-gambar dibawah ini, maka kalian telah berhasil menginstall SSH di Ubuntu Server 12.04 LTS.



Gambar 3.11.6

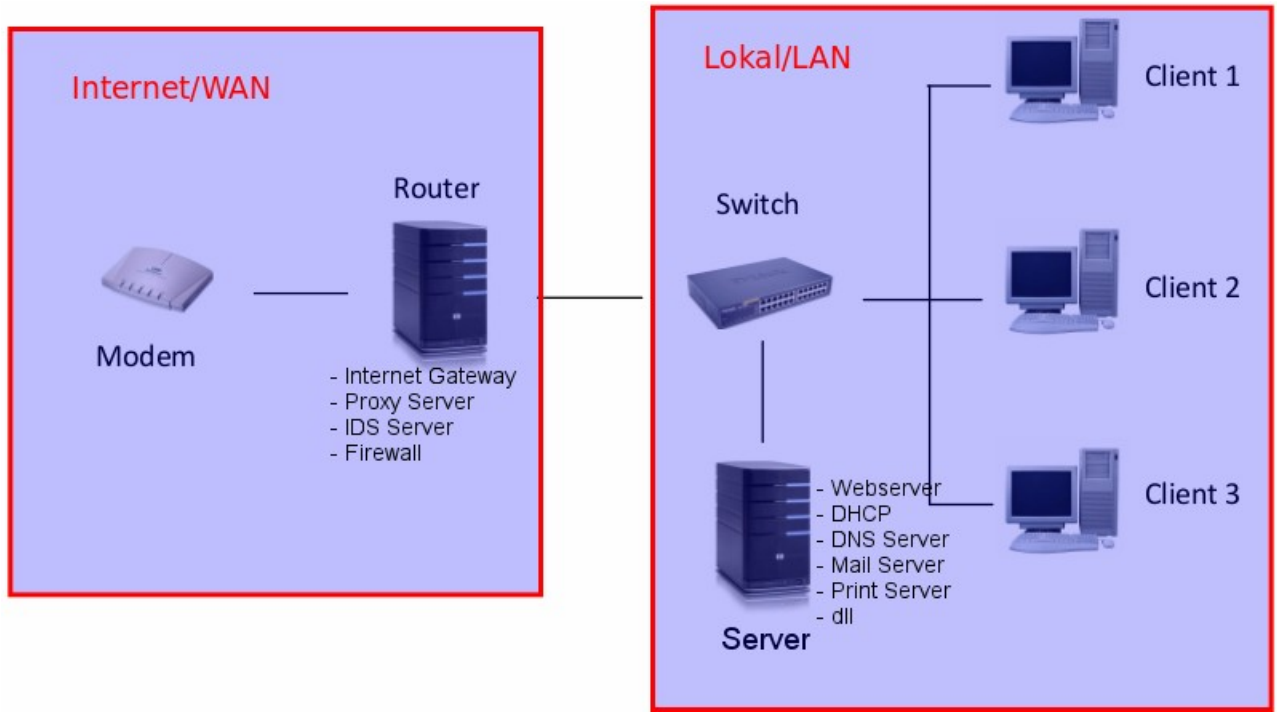


Gambar 3.11.7

Bab 4. Konfigurasi dan Instalasi Aplikasi Router Ubuntu Server 12.04 LTS

Pada bab sebelumnya kalian telah belajar cara-cara menginstalasi dan mengkonfigurasi berbagai macam layanan aplikasi pada komputer Server yang menggunakan OS Ubuntu Server 12.04 LTS. Mulai dari layanan Web, DNS, DHCP hingga layanan Mail Server telah kalian pelajari semua. Akan tetapi, ada satu hal yang kurang dari pembahasan bab 3 tersebut. Apakah itu? Yap! Seluruh layanan tersebut sifatnya masih lokal saja. Sehingga client pun hanya bisa menikmatinya dari dalam lingkungan area itu tanpa bisa mengaksesnya dari jaringan lain. Lalu bagaimana agar jaringan lokal itu dapat terhubung dengan jaringan lain dan internet?

Disinilah peran sebuah Router dibutuhkan. Router merupakan sebuah perangkat yang fungsi utamanya untuk menghubungkan dua jaringan atau lebih yang berbeda. Router juga biasa disebut sebagai gerbang penghubung (gateway) antara satu jaringan dengan jaringan yang lain. Internet merupakan contoh utama dari sebuah jaringan yang memiliki banyak *Router*. *Router* dapat digunakan untuk menghubungkan banyak jaringan kecil ke sebuah jaringan yang lebih besar, yang disebut dengan *internetwork*, atau untuk membagi sebuah jaringan besar ke dalam beberapa *subnetwork* untuk meningkatkan kinerja dan juga mempermudah manajemennya. Router juga kadang digunakan untuk mengoneksikan dua buah jaringan yang menggunakan media yang berbeda (seperti halnya *router wireless* yang pada umumnya selain ia dapat menghubungkan komputer dengan menggunakan radio, ia juga mendukung penghubungan komputer dengan kabel UTP) atau berbeda arsitektur jaringan, seperti halnya dari Ethernet ke Token Ring. Selain itu Router juga dapat berfungsi sebagai Internet Gateway, sebagai Proxy, maupun sebagai Firewall, tergantung dari kebutuhan masing-masing. Intinya Router ini bila diibaratkan adalah seorang polisi lalu lintas yang bertugas sebagai sebuah gerbang penghubung, sebagai penunjuk arah, serta sebagai pengawas lalu lintas jaringan. Untuk lebih jelasnya perhatikan gambar topologi berikut :



Gambar diatas adalah sebuah implementasi sederhana dari cara kerja Router. Dimana ada sebuah modem yang berfungsi sebagai sumber internetnya, dihubungkan ke sebuah Router, kemudian Router tersebut dihubungkan kembali ke sebuah Switch yang juga telah terhubung ke beberapa komputer client dan sebuah Server. Router inilah yang akan kalian bangun pada bab 4 ini. Kalian akan belajar bagaimana caranya membuat Router menjadi Internet Gateway/Internet Sharing, menjadi sebuah Proxy, IDS, dan juga Firewall.

Secara keseluruhan, persiapan yang kalian butuhkan untuk membuat Router hampir sama dengan persiapan untuk membuat Server. Bedanya hanyalah kalian memerlukan sebuah modem, baik itu modem DSL maupun modem USB sebagai sumber internetnya (saya sarankan untuk memakai modem kabel/DSL, karena modem USB tidak akan dibahas dibuku ini), dan dua buah *Network Interface Card* (satu sebagai penghubung antara modem dengan Router, dan yang lainnya dikoneksikan ke Switch sebagai penghubung dengan jaringan lokal). Sedangkan untuk proses instalasi, proses penambahan DVD Repositori, sampai proses konfigurasi TCP/IP di komputer Router, tidak terlalu banyak perbedaan yang signifikan. Konsepnya sebenarnya sama, tinggal kalian pahami saja konsep-konsep konfigurasi pada bab-bab sebelumnya maka saya jamin kalian tidak akan kesulitan lagi untuk mengikuti langkah-langkah konfigurasi selanjutnya..

4.1. Konfigurasi TCP/IP

Karena pada dasarnya cara-cara konfigurasi TCP/IP pada komputer Server dengan Router tidak jauh

berbeda, maka pada subbab Konfigurasi TCP/IP ini saya hanya akan membahas sedikit saja mengenai cara konfigurasi TCP/IP menggunakan dua buah NIC. Disini akan saya berikan dua contoh konfigurasi pada file **/etc/network/interfaces**, yaitu contoh konfigurasi yang menggunakan DHCP dan contoh konfigurasi yang menggunakan IP Statik, tergantung dari ISP (Internet Service Provider) kalian masing-masing.

- Pertama buka terlebih dahulu file **/etc/network/interfaces** dengan perintah berikut :

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

- Kemudian pilih diantara dua script berikut, lalu kopikan kedalamnya :

Kopikan script ini jika ISP kalian memberikan IP secara DHCP :

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# Interface internet/WAN
auto eth0
iface eth0 inet dhcp

# Interface lokal
auto eth1
iface eth1 inet static
address 192.168.1.100
netmask 255.255.255.0
```

Contoh script ini jika ISP kalian memberikan IP secara statik. Sesuaikan pengaturan IP pada eth0 sesuai dengan IP publik yang telah diberikan oleh ISP kalian masing-masing.

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
```

```
auto lo
iface lo inet loopback

# Interface internet/WAN
auto eth0
iface eth0 inet static
address 10.0.2.15
netmask 255.255.255.0
gateway 10.0.2.2
dns-nameservers 192.168.1.1 8.8.8.8 8.8.4.4

# Interface lokal
auto eth1
iface eth1 inet static
address 192.168.1.100
netmask 255.255.255.0
```

- Setelah itu simpan perubahan dengan menekan **CTRL + X**, lalu tekan **Y**, lalu **Enter**.

4.2. Routing NAT/MASQUERADING

NAT atau Network Address Translation adalah sebuah metode untuk menghubungkan lebih dari satu komputer ke jaringan internet dengan menggunakan satu alamat IP. NAT dibuat untuk mengatasi masalah ketersediaan alamat IP yang terbatas, kebutuhan akan keamanan (security), dan untuk kemudahan serta fleksibilitas dalam administrasi jaringan.

Dalam dunia jaringan, sebenarnya alamat IP yang diperbolehkan untuk mengakses internet hanyalah IP publik yang jumlah maksimalnya sebanyak 4.294.967.296 IP. Sedangkan secara teoritis, jumlah komputer yang ada di dunia ini jauh lebih besar dibandingkan itu. IP publik juga harganya relatif cukup mahal. Misalnya saja bila harga satu IP Public adalah 500 ribu Rupiah perbulan, bayangkan berapa uang yang harus dikeluarkan oleh sebuah perusahaan yang memiliki 1000 komputer perbulannya? Karena keterbatasan inilah teknologi NAT dibuat. Dimana kalian hanya perlu untuk membeli satu IP publik yang kemudian dapat digunakan secara bersama-sama oleh banyak komputer. Jauh lebih efisien dan murah bukan ? Beberapa contoh penerapan NAT adalah Warnet dan Hotspot area.

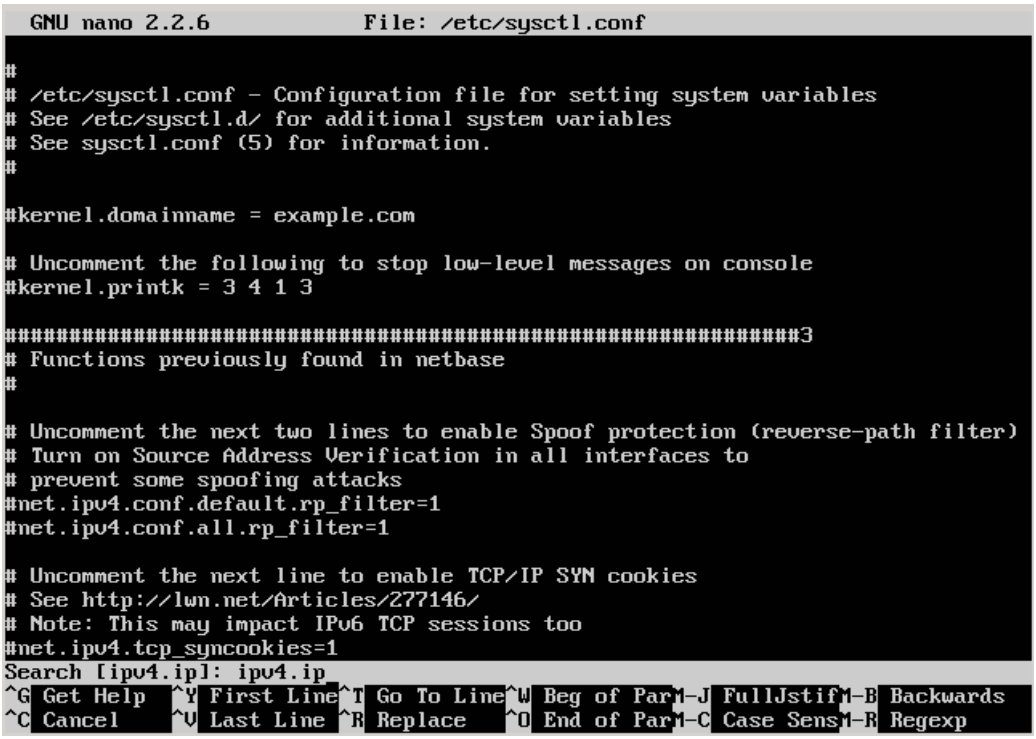
Konfigurasi Packet Forwarding

Untuk dapat menerapkan NAT di Ubuntu Server 12.04 LTS, kalian perlu untuk mengaktifkan sistem Packet Forwarding terlebih dahulu. Ini berfungsi untuk memperbolehkan paket-paket data diteruskan melalui Router. Cara untuk konfigurasinya adalah sebagai berikut :

- Edit file **/etc/sysctl.conf** dengan mengeksekusi perintah dibawah ini :

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

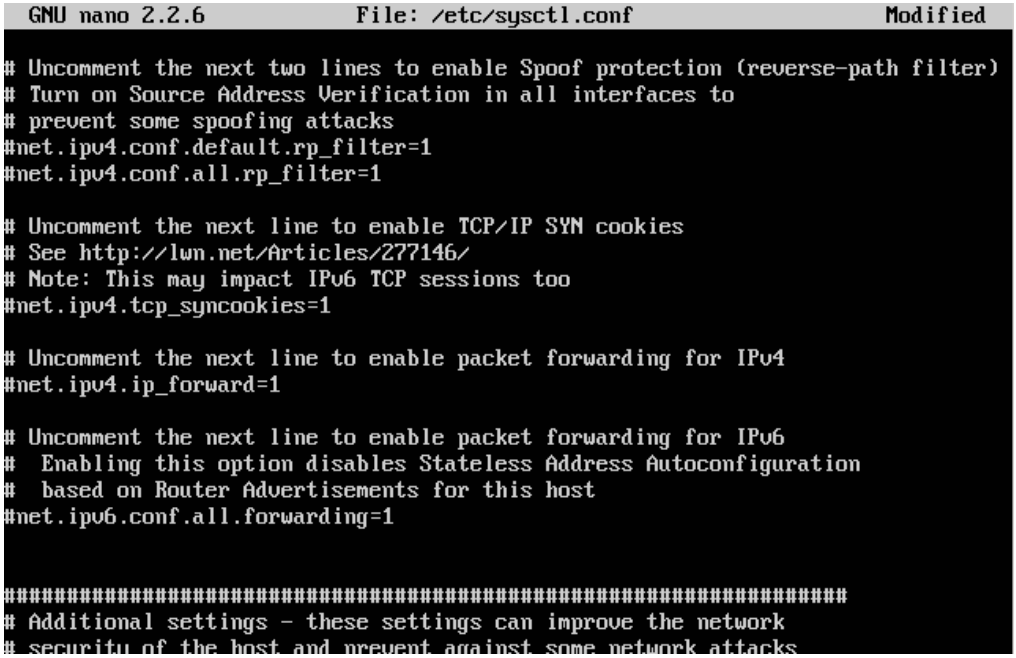
- Setelah terbuka, tekan tombol **CTRL + W** untuk melakukan pencarian kata kunci. Isikan kata kunci **ipv4.ip** pada kotak **Search**, kemudian tekan **Enter** :



Gambar 4.2.1

- Ketika kalian menekan Enter, maka kalian akan menemukan baris seperti ini :

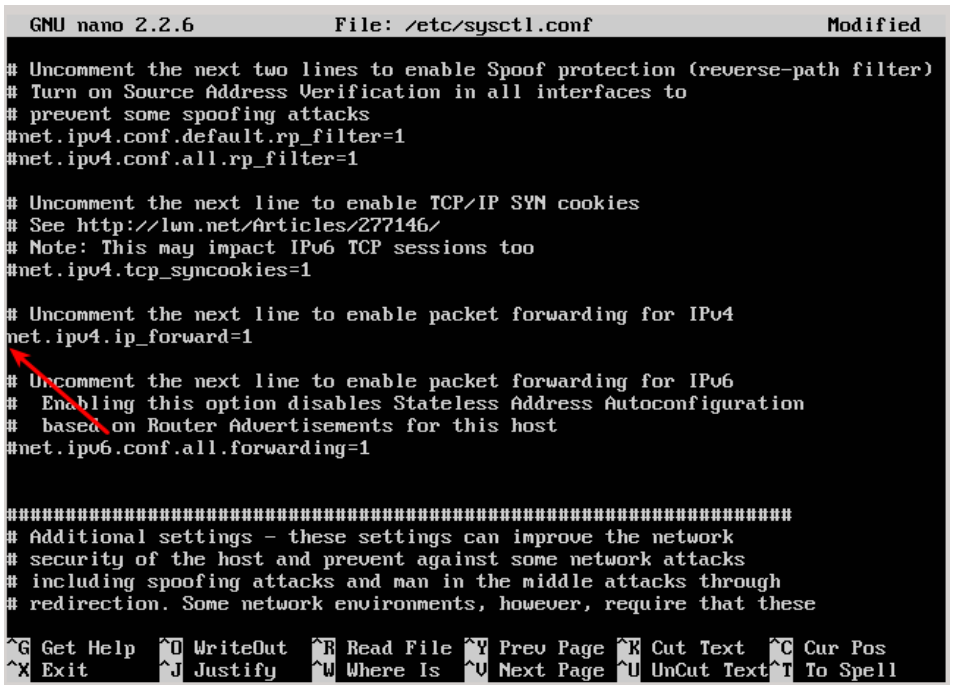
```
# Uncomment the next line to enable packet forwarding for IPv4
#net.ipv4.ip_forward=1
```



Gambar 4.2.2

- Hapuslah tanda pagar (#) yang ada di depan baris **net.ipv4.ip_forward=1** sehingga tinggal menjadi seperti ini :

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```



Gambar 4.2.3

- Setelah itu simpan perubahan dengan menekan **CTRL + X**, lalu tekan **Y**, lalu **Enter**.

Konfigurasi Routing NAT

Ada tiga bagian besar yang perlu dilakukan dalam Routing NAT. Yaitu merouting itu sendiri, menyimpan konfigurasi dari routing yang telah dilakukan, dan membuat skrip untuk merestore konfigurasi routing setiap komputer booting.

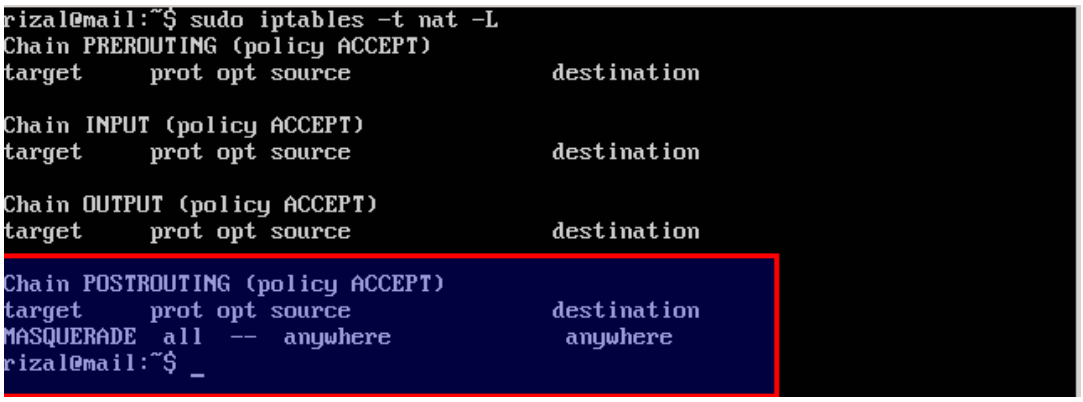
- Untuk melakukan routing NAT, cukup lakukan perintah iptables berikut ini dimana **eth0** adalah interface output yang keluar menuju Internet :

```
sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Gambar 4.2.4

- Kemudian cek kembali apakah konfigurasi tadi telah berhasil dengan menggunakan perintah berikut :

```
sudo iptables -t nat -L
```



Gambar 4.2.5

- Jika benar, maka seharusnya akan muncul sebuah rule baru bernama **MASQUERADE** seperti yang terlihat pada gambar diatas.
- Selanjutnya kalian harus menyimpan konfigurasi tersebut agar tidak hilang ketika komputer di restart. Caranya adalah dengan masuk terlebih dahulu sebagai user root dengan perintah ini :

```
sudo -i
```

- Lalu baru eksekusi perintah dibawah untuk menyimpan konfigurasi tabel routing pada file **/etc/network/iptables.conf** :

```
iptables-save > /etc/network/iptables.conf
```

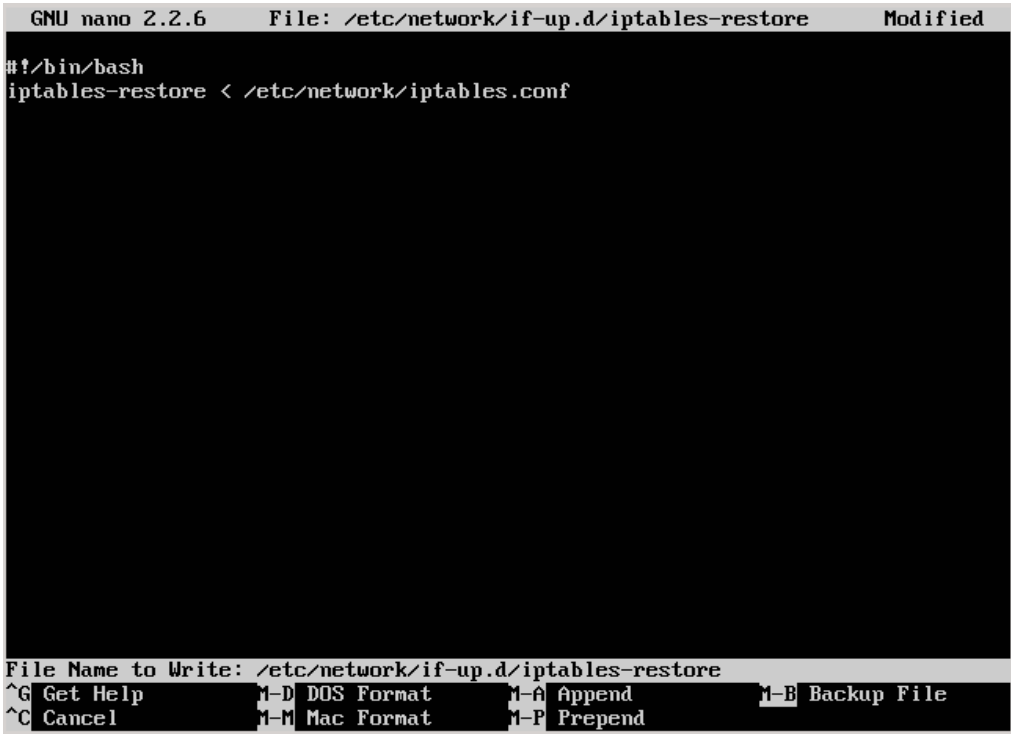
Gambar 4.2.6

- Kemudian langkah terakhir adalah membuat sebuah script yang berguna untuk merestore/mengembalikan konfigurasi routing yang telah kalian simpan di **/etc/network/iptables.conf** tadi. Masih login dalam mode root, ketikkan perintah berikut :

```
nano /etc/network/if-up.d/iptables-restore
```

- Akan terbuka sebuah file yang masih kosong, lalu kemudian isikan script berikut kedalamnya. Setelah itu simpan perubahan dengan menekan **CTRL + X**, lalu tekan **Y**, lalu **Enter**.

```
#!/bin/bash
iptables-restore < /etc/network/iptables.conf
```



Gambar 4.2.7

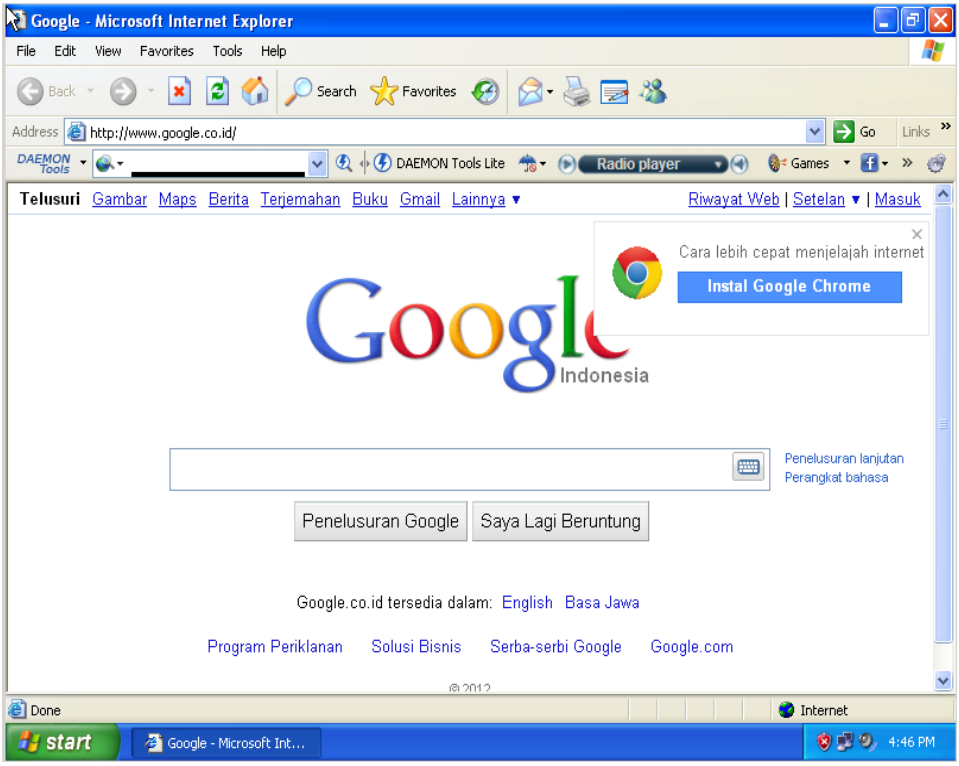
- Berikan akses *executable* pada file tersebut agar sistem dapat mengeksekusinya setiap komputer booting. Caranya adalah dengan mengetikkan perintah ini (masih dalam mode root) :

  ```
  chmod +x /etc/network/if-up.d/iptables-restore
  ```

- Setelah itu restart komputer Router dengan perintah ini untuk melihat apakah konfigurasi yang telah kalian lakukan sudah berfungsi dengan baik :

  ```
  reboot
  ```

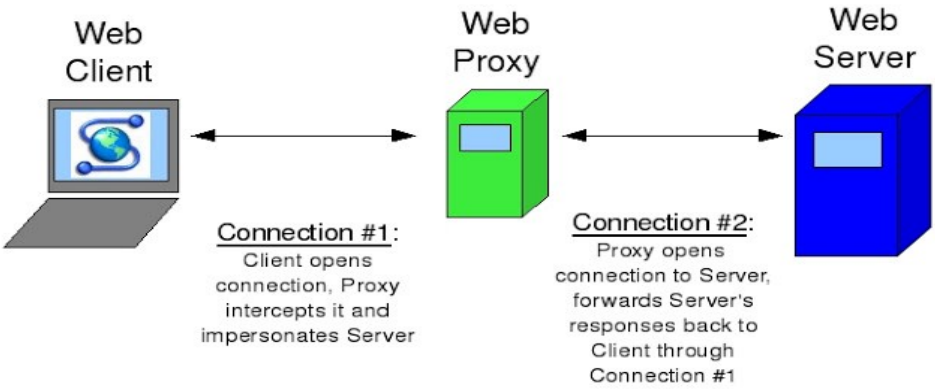
- Setelah komputer Router kalian restart, sekarang coba test dari komputer client. Jika tidak ada kesalahan, seharusnya komputer client sudah bisa mengakses internet juga seperti yang ditunjukkan gambar dibawah.



Gambar 4.2.8

4.3. Instalasi Proxy Server

Proxy merupakan sebuah komponen penting yang wajib ada di dalam sebuah jaringan. Kemampuannya yang dapat meningkatkan keamanan, menghemat bandwidth, dan juga dapat memfilter paket-paket yang tidak diinginkan sangatlah penting untuk meningkatkan efisiensi keamanan jaringan. Proxy berada di tengah-tengah antara klien dan internet yang memeriksa semua paket yang lewat dan mengeksekusinya sesuai dengan daftar akses kontrol yang ada pada file konfigurasinya. Perhatikan gambar dibawah ini :



Gambar 3.4.1

Pada gambar diatas terlihat bahwa ketika PC klien mengirimkan request HTTP untuk membuka sebuah web, paket tersebut di belokkan terlebih dahulu menuju proxy untuk diperiksa apakah paket

tersebut boleh lewat atau tidak, sebelum akhirnya diteruskan kembali ke internet. Begitu pula paket dari internet, sebelum masuk ke PC klien yang meminta request, paket tersebut harus melewati Proxy terlebih dahulu, baru di teruskan menuju PC klien. Keuntungan menggunakan Proxy antara lain :

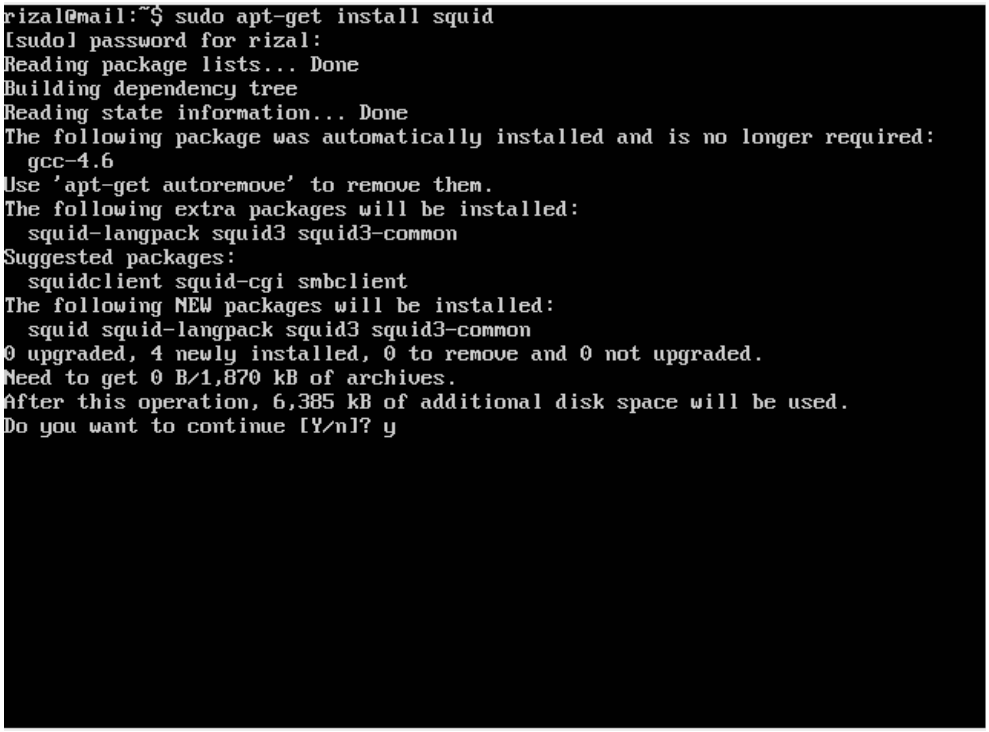
1. Dapat meningkatkan kecepatan internet dan menghemat bandwidth karena ada fitur *cache*.
2. Dapat mengatur situs-situs dan konten yang dibolehkan dan yang tidak dibolehkan.
3. Dapat mengatur bandwidth untuk tiap-tiap klien.
4. Lebih aman karena jaringan lebih termonitor.

Instalasi Squid

Squid adalah aplikasi Proxy Server yang cukup terkenal dikalangan sysadmin. Sangat tangguh dan memiliki banyak sekali fitur. Bahkan pengguna mikrotik pun sering menggunakan squid sebagai Proxy Server eksternalnya. Untuk menginstall Squid di Ubuntu Server silahkan ikuti langkah-langkah berikut :

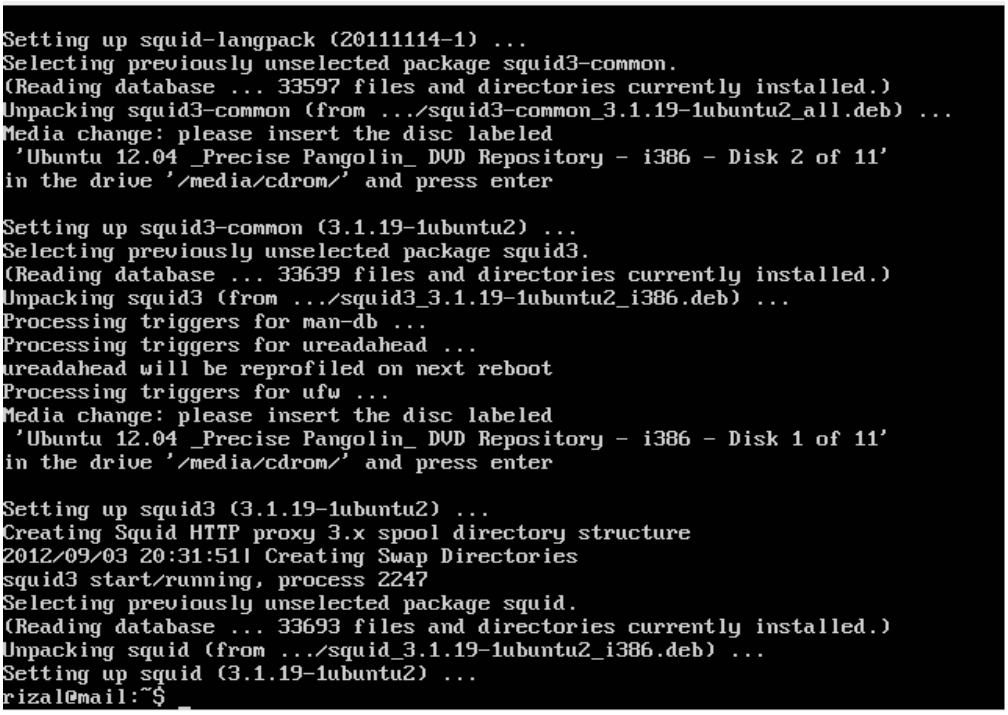
- Pertama ketikkan perintah dibawah ini untuk menginstall Squid :

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



Gambar 4.3.2

- Tunggu hingga proses instalasi selesai seperti yang ditunjukkan oleh gambar dibawah ini :



Gambar 4.3.3

- Jika tidak ada pesan kesalahan, berarti instalasi squid telah berhasil.

Konfigurasi Squid

Konfigurasi Squid ini akan saya bagi menjadi 4 bagian. Yang pertama yaitu mengatur cache secara optimal, lalu cara memblok situs-situs porno, kemudian cara memblok situs tertentu pada jam tertentu, dan yang terakhir adalah teknik pembatasan bandwidth.

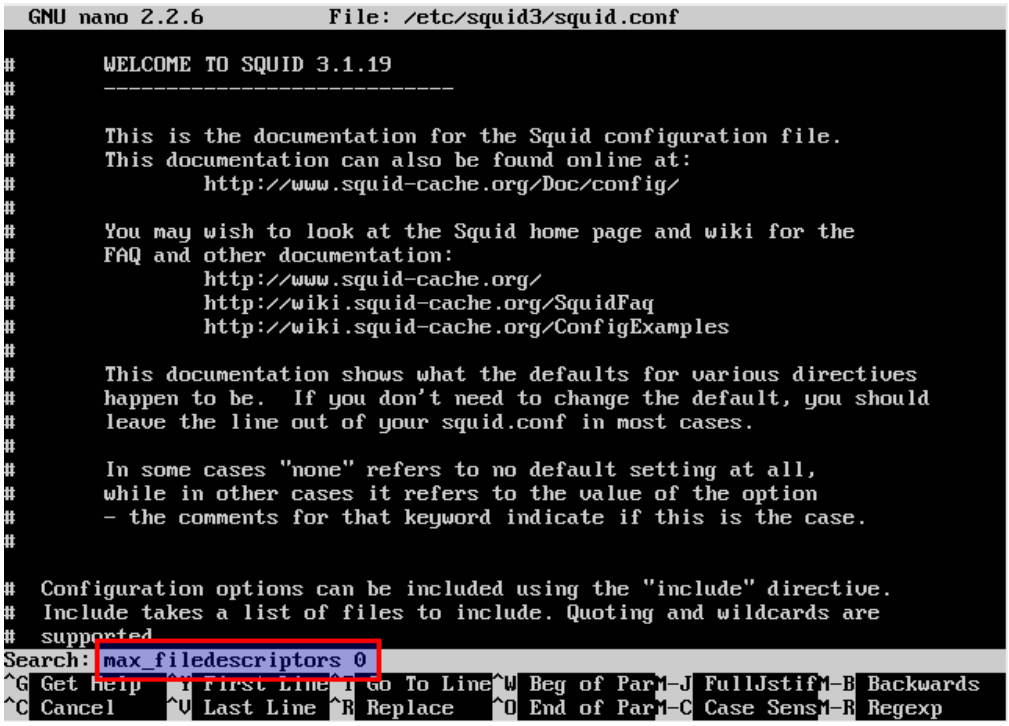
Pengaturan Cache Secara Optimal

Cache berfungsi untuk menyimpan segala data-data web yang pernah diakses oleh klien. Jadi ketika klien mengakses sebuah web di internet, maka konten-konten yang ada di web tersebut akan di simpan secara otomatis oleh cache. Gunanya apa? Tentunya ketika klien hendak mengakses situs yang sama di kemudian hari, maka klien tidak perlu lagi untuk meload ulang konten-konten tersebut dari internet, melainkan cukup dari cache milik Proxy lokal saja. Ini tentu akan sangat membantu dalam penghematan bandwidth dan mempercepat kecepatan browsing. Pernahkah kalian merasa ketika membuka situs google.com jauh lebih cepat dibandingkan dengan membuka situs ubuntu.com atau situs-situs lainnya yang jarang kalian buka ? Itulah peran dari *Cache* pada Proxy.

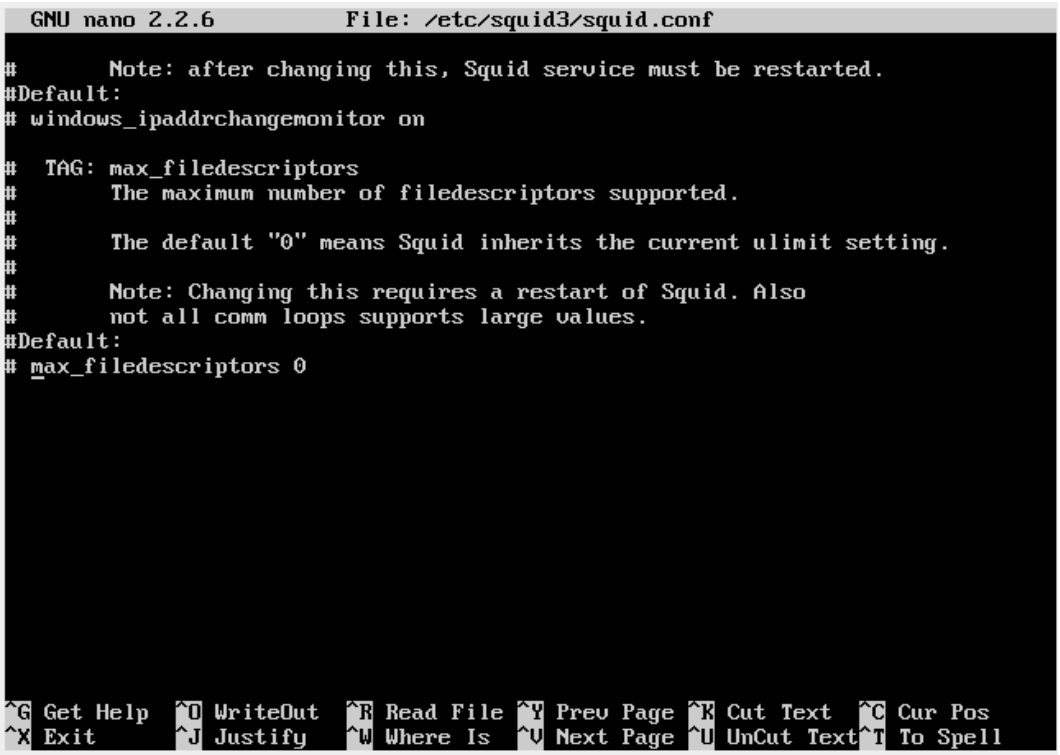
- Untuk pengaturan cache pada squid, pertama-tama buka dulu file konfigurasi dari squidnya :

  ```
  sudo nano /etc/squid3/squid.conf
  ```

- Kemudian tekan **CTRL + W** untuk mencari kata kunci **max_filedescriptors 0**.



Gambar 4.3.4



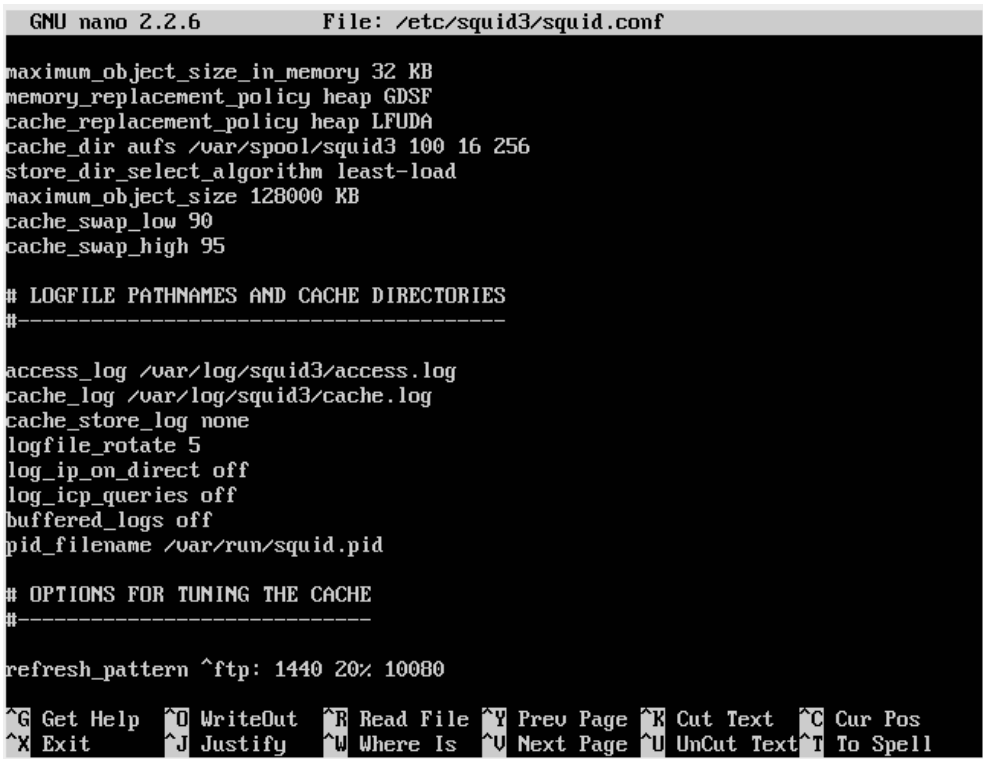
Gambar 4.3.5

- Setelah ketemu, pada bagian bawah baris tersebut tambahkan baris script ini :

```
# OPTIONS WHICH AFFECT THE CACHE SIZE
```

```
#-----------------------------------

cache_mem 32 MB
maximum_object_size_in_memory 32 KB
memory_replacement_policy heap GDSF
cache_replacement_policy heap LFUDA
cache_dir aufs /var/spool/squid3 100 16 256
store_dir_select_algorithm least-load
maximum_object_size 128000 KB
cache_swap_low 90
cache_swap_high 95

# LOGFILE PATHNAMES AND CACHE DIRECTORIES
#---------------------------------------

access_log /var/log/squid3/access.log
cache_log /var/log/squid3/cache.log
cache_store_log none
logfile_rotate 5
log_ip_on_direct off
log_icp_queries off
buffered_logs off
pid_filename /var/run/squid.pid

# OPTIONS FOR TUNING THE CACHE
#-----------------------------

refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440
refresh_pattern -i \.(gif|png|jp?g|ico|bmp|tiff?)$ 10080 95% 43200
override-expire override-lastmod reload-into-ims ignore-no-cache
ignore-private
refresh_pattern -i \.
(rpm|cab|deb|exe|msi|msu|zip|tar|gz|tgz|rar|bin|7z|doc?|xls?|ppt?|pdf|nth|
psd|sis)$ 10080 90% 43200 override-expire override-lastmod reload-into-ims
```

```
ignore-no-cache $
refresh_pattern                                -i                                \.
(avi|iso|wav|mid|mp?|mpeg|mov|3gp|wm?|swf|flv|x-flv|axd)$ 43200 95% 432000
override-expire    override-lastmod    reload-into-ims    ignore-no-cache
ignore-private
refresh_pattern -i \.(html|htm|css|js)$ 1440 75% 40320
refresh_pattern -i \.index.(html|htm)$ 0 75% 10080
refresh_pattern -i (/cgi-bin/|\?) 0 0% 0
refresh_pattern . 1440 90% 10080

quick_abort_min 0 KB
quick_abort_max 0 KB
quick_abort_pct 98
store_avg_object_size 13 KB
```



Gambar 4.3.6

- Simpan dan keluarkan file tersebut
- Lalu jalankan perintah ini untuk mengaktifkan perubahan :

```
sudo service squid3 stop && sudo squid3 -f /etc/squid3/squid.conf && sudo
```

```
service squid3 start && sudo squid3 -k reconfigure
```

```
rizal@mail:~$ sudo service squid3 stop && sudo squid3 -f /etc/squid3/squid.conf
&& sudo service squid3 start && sudo squid3 -k reconfigure
```

Gambar 4.3.7

Memblokir situs-situs tidak baik

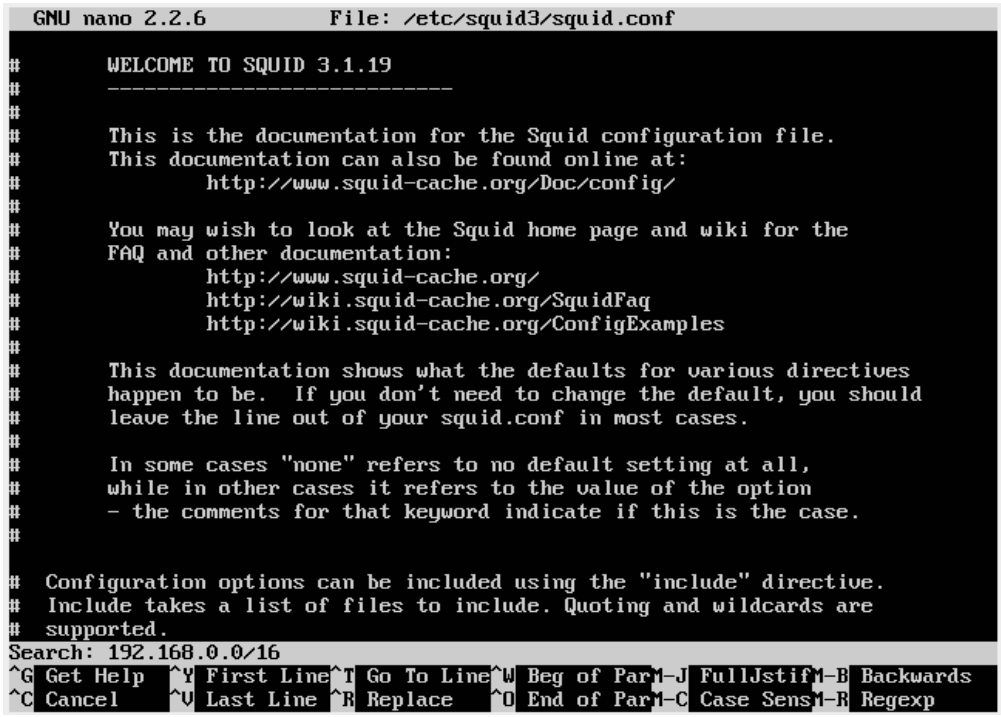
Salah satu kemampuan Squid yang lain adalah kemampuan untuk memfilter situs-situs apa saja yang dapat diakses oleh komputer client. Situs-situs yang sering difilter ini biasanya situs-situs yang mengandung unsur porno, sara, maupun situs-situs yang mengandung spam, malware, atau phishing. Cara diatas dapat dilakukan berkat fungsi dari ACL (Access Control List) yang ada di Squid. Untuk praktek awal menggunakan fungsi ACL, mari kalian pelajari cara memblokir situs-situs tidak baik pada subbab ini.

- Langkah awal yang perlu dilakukan adalah membuka file konfigurasi squid.conf dengan perintah berikut :

  ```
  sudo nano /etc/squid3/squid.conf
  ```

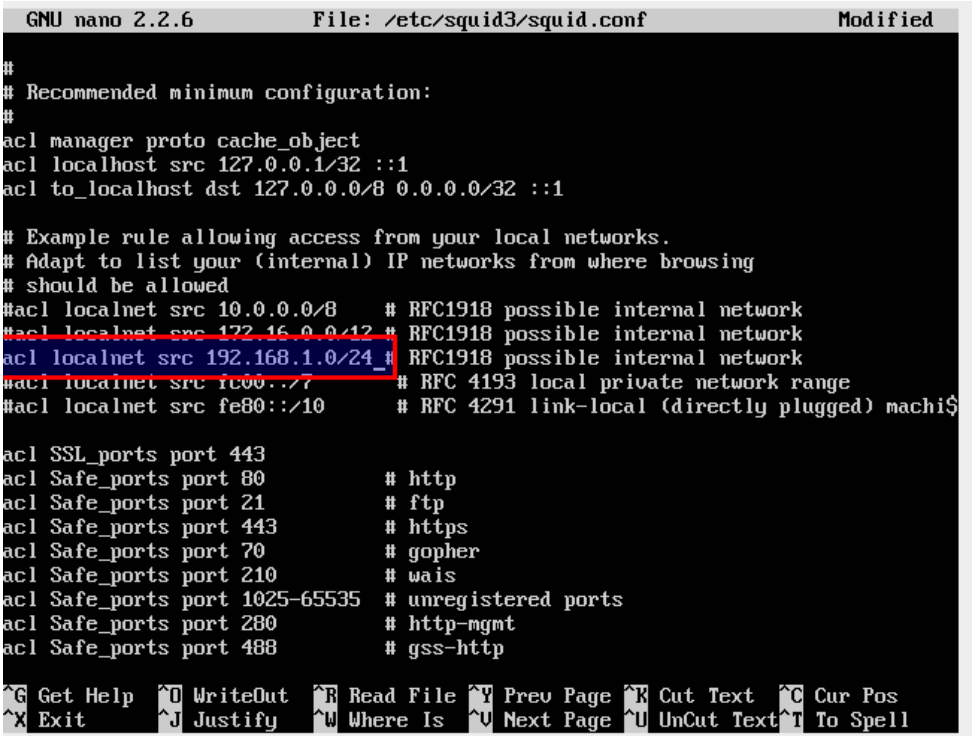
Gambar 4.3.8

- Setelah file squid.conf terbuka, tekan **CTRL + W** dan isikan **192.168.0.0/16** pada kotak pencarian, kemudian tekan Enter.



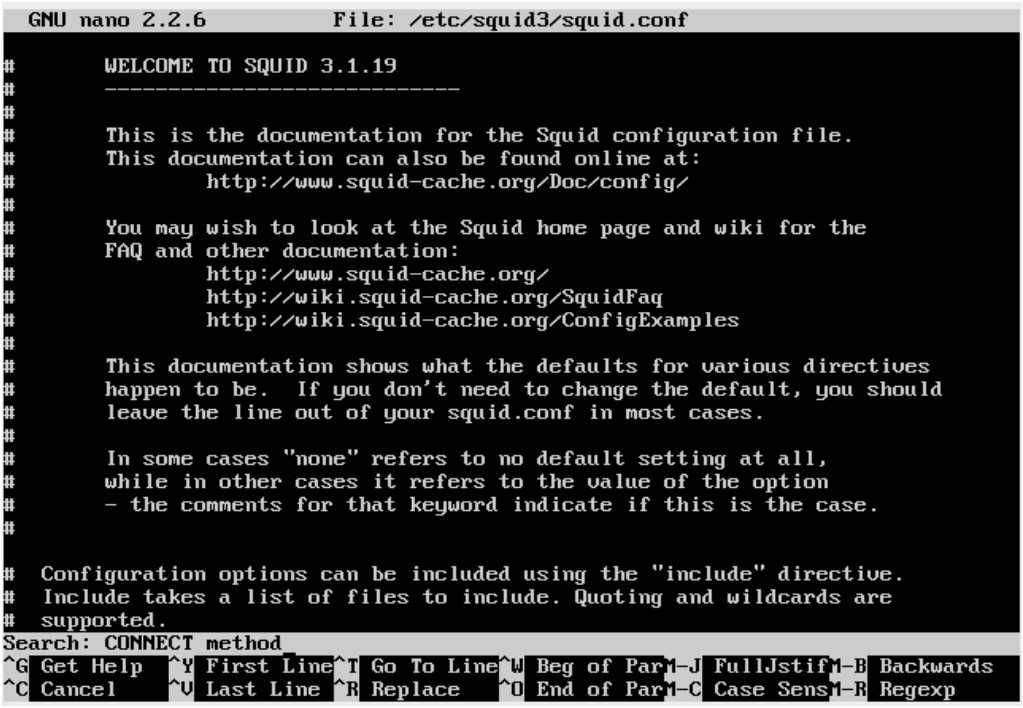
Gambar 4.3.9

- Temukan baris **#acl localnet src 192.168.0.0/16**, kemudian hilangkan tanda pagar (#) didepannya, dan ganti pada bagian **192.168.0.0/16** menjadi **192.168.1.0/24** sesuai dengan konfigurasi jaringan LAN yang telah kalian buat sejak awal instalasi.

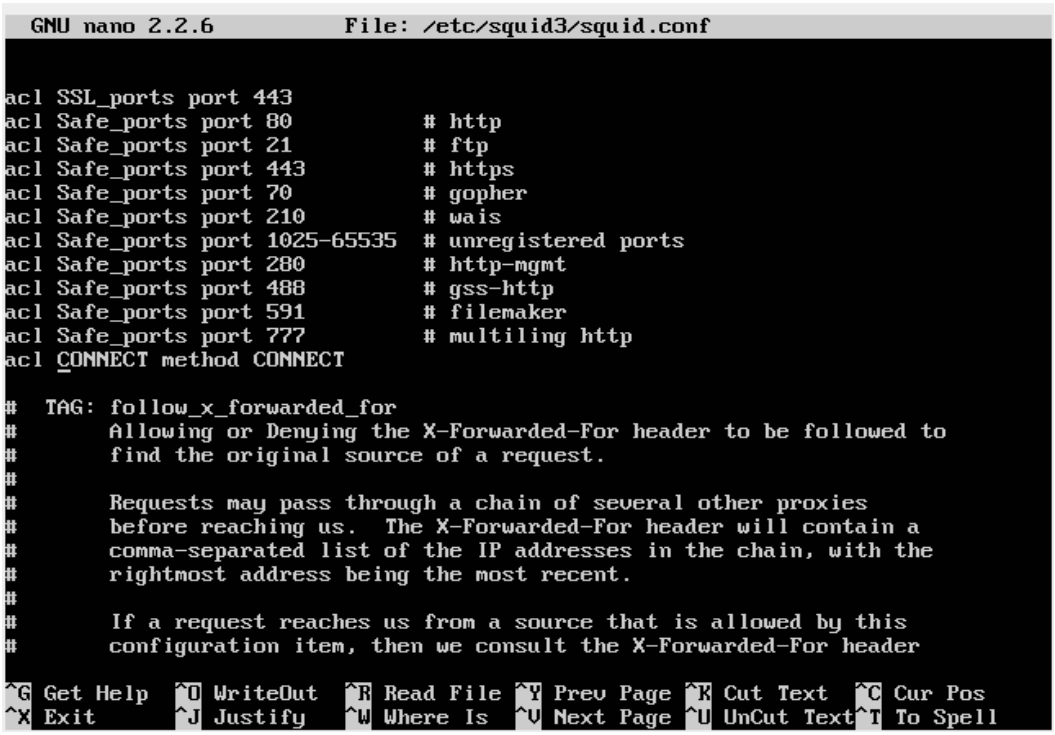


Gambar 4.3.10

- Setelah itu, tekan lagi **CTRL + W** dan isikan kata **CONNECT method** pada kotak pencarian, kemudian tekan **Enter**.



Gambar 4.3.11

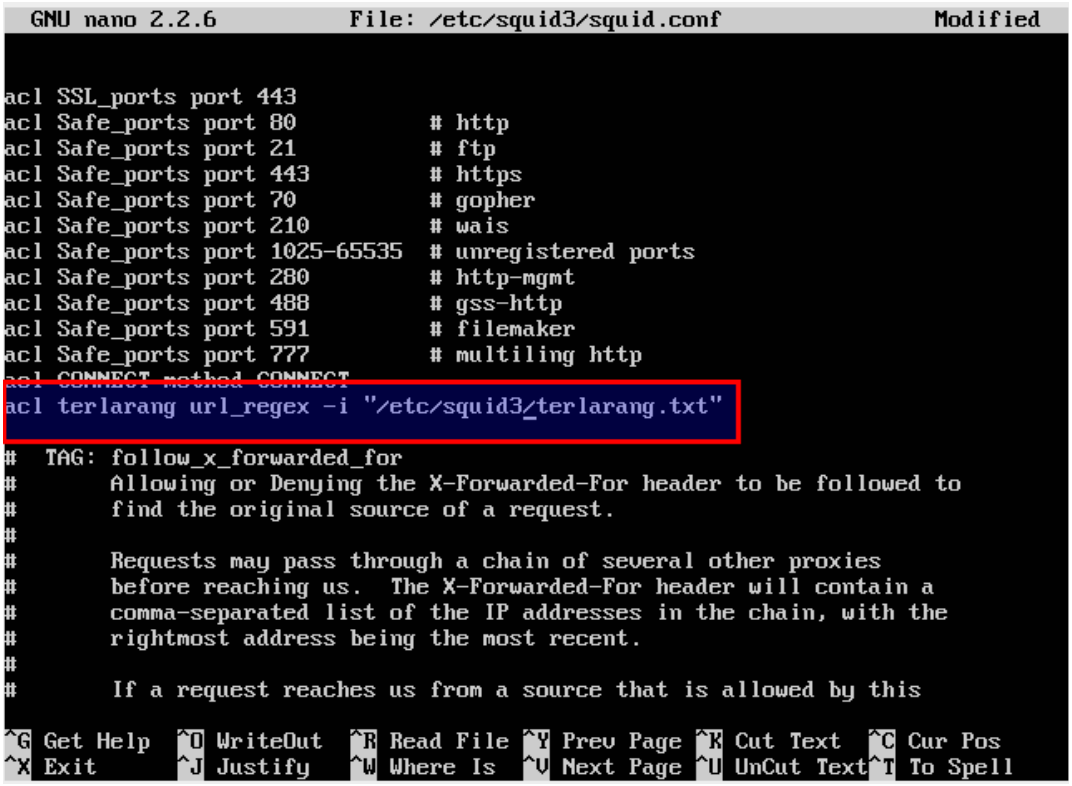


Gambar 4.3.12

- Kemudian kalian nanti akan menemukan baris **acl CONNECT method CONNECT.** Tepat

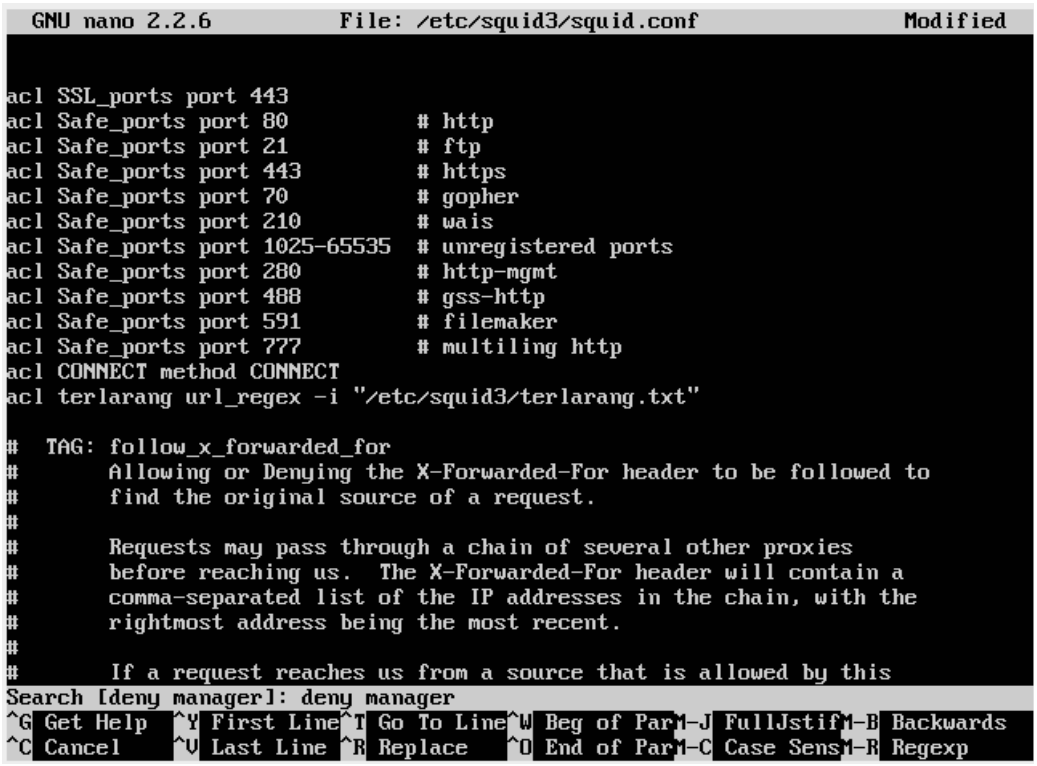
dibawah baris tersebut tambahkan baris seperti ini :

```
acl terlarang url_regex -i "/etc/squid3/terlarang.txt"
```

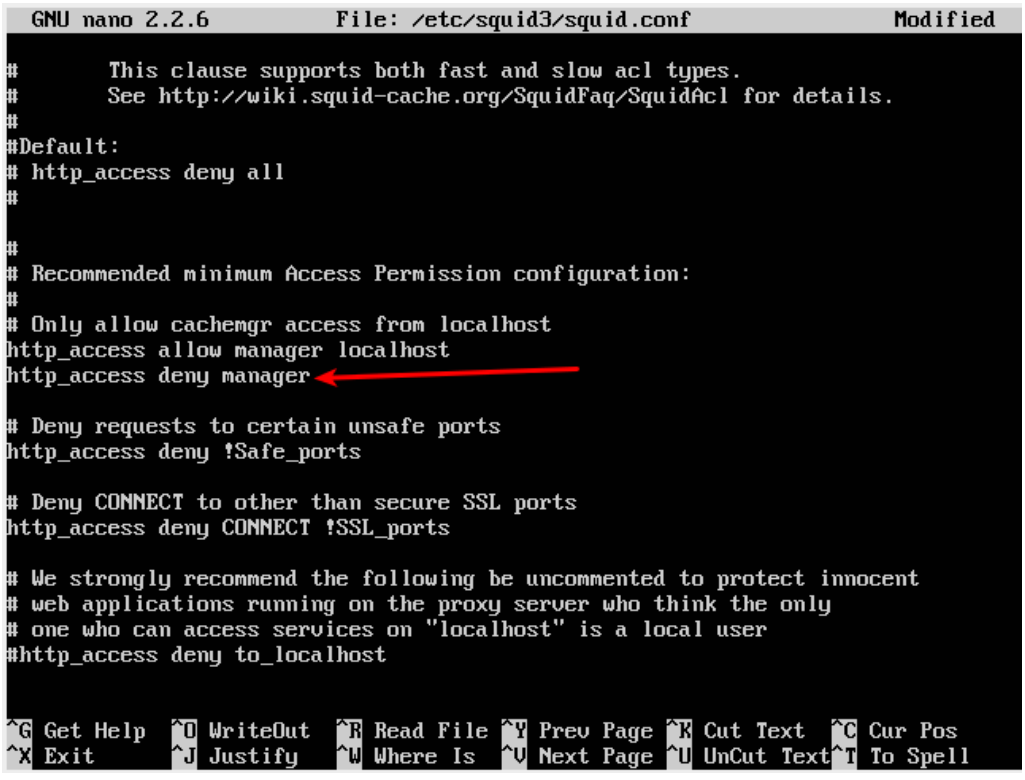


Gambar 4.3.13

- Arti dari baris diatas adalah dimana terdapat sebuah ACL baru bernama *terlarang*, yang akan didefinisikan melalui kata kunci yang terdapat di dalam file */etc/squid3/terlarang.txt*.
- Setelah itu tekan kembali **CTRL + W**, lalu isikan dengan kalimat **deny manager** dan tekan **Enter**. Maka begitu kalian menekan **Enter**, kalian akan menemukan baris **http_access deny manager**.



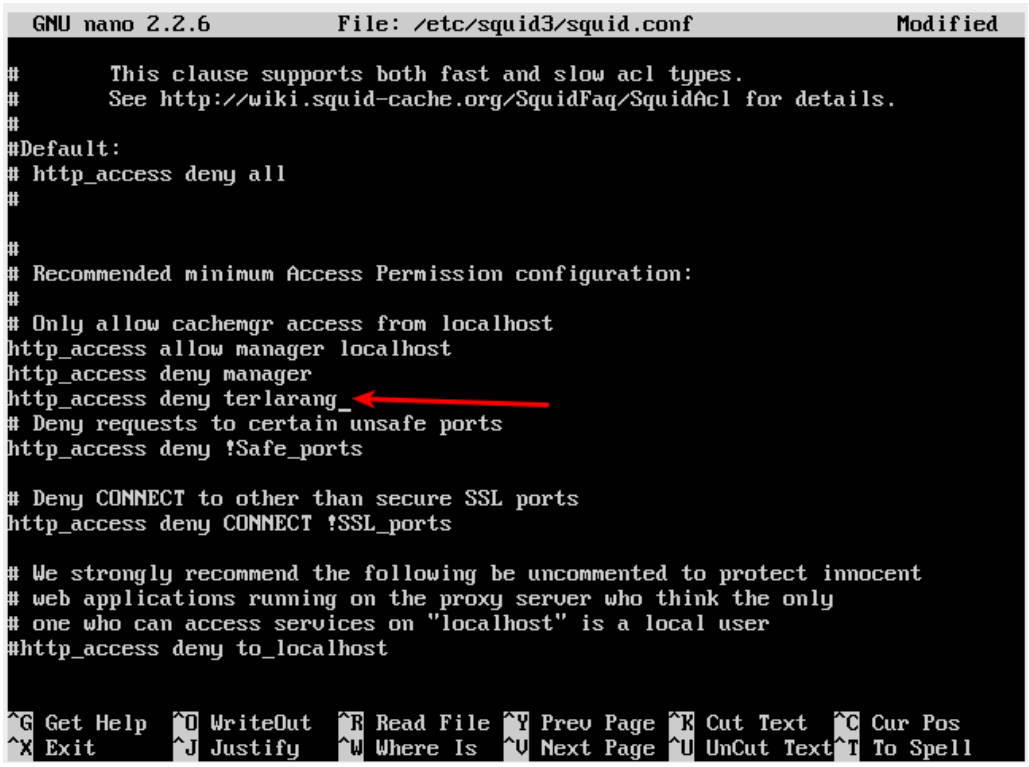
Gambar 4.3.14



Gambar 4.3.15

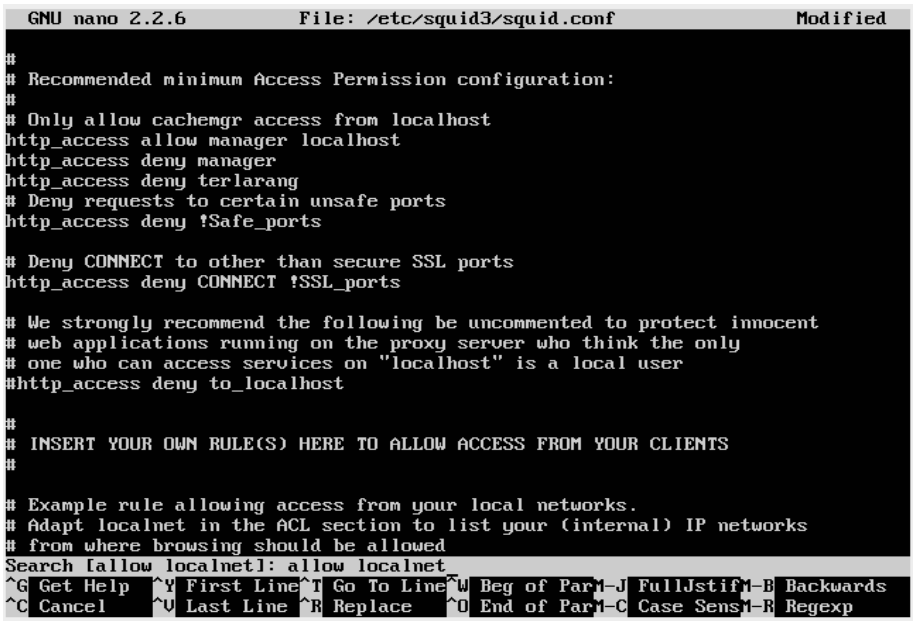
- Tepat dibawah baris tersebut, tambahkan script berikut ini :

```
http_access deny terlarang
```



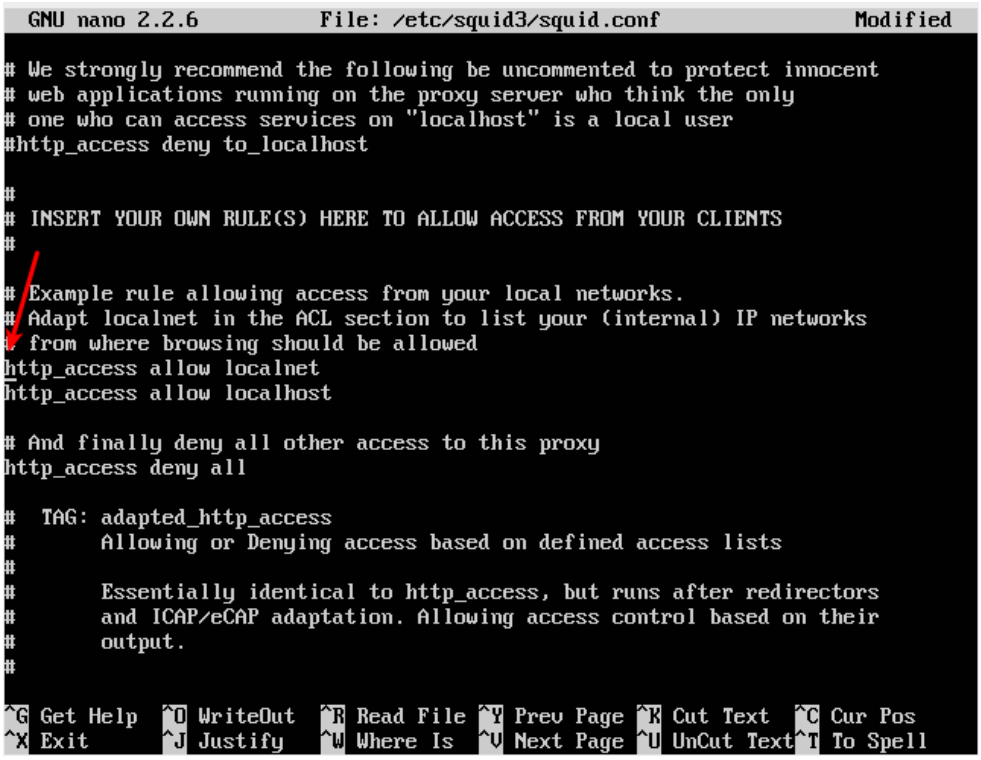
Gambar 4.3.16

- Maksud dari script diatas adalah, dimana ACL bernama *terlarang* akan selalu ditolak oleh squid, karena ACL *terlarang* telah didefinisikan sebagai **deny** yang berarti tolak.
- Setelah itu tekan kembali **CTRL + W**, lalu cari kata kunci allow **localnet**.



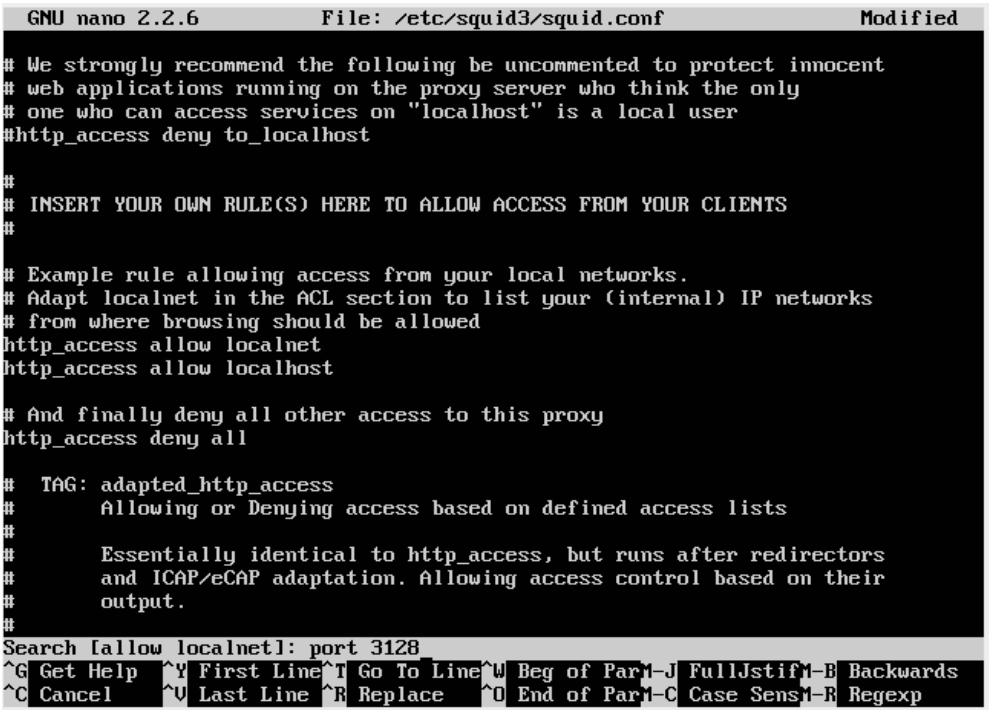
Gambar 4.3.17

- Kemudian hapuslah tanda pagar (#) yang ada di depan baris **#http_access allow localnet** sehingga tinggal menjadi **http_access allow localnet** saja. Ini gunanya untuk memperbolehkan klien pada jaringan lokal untuk mengakses internet melalui proxy.

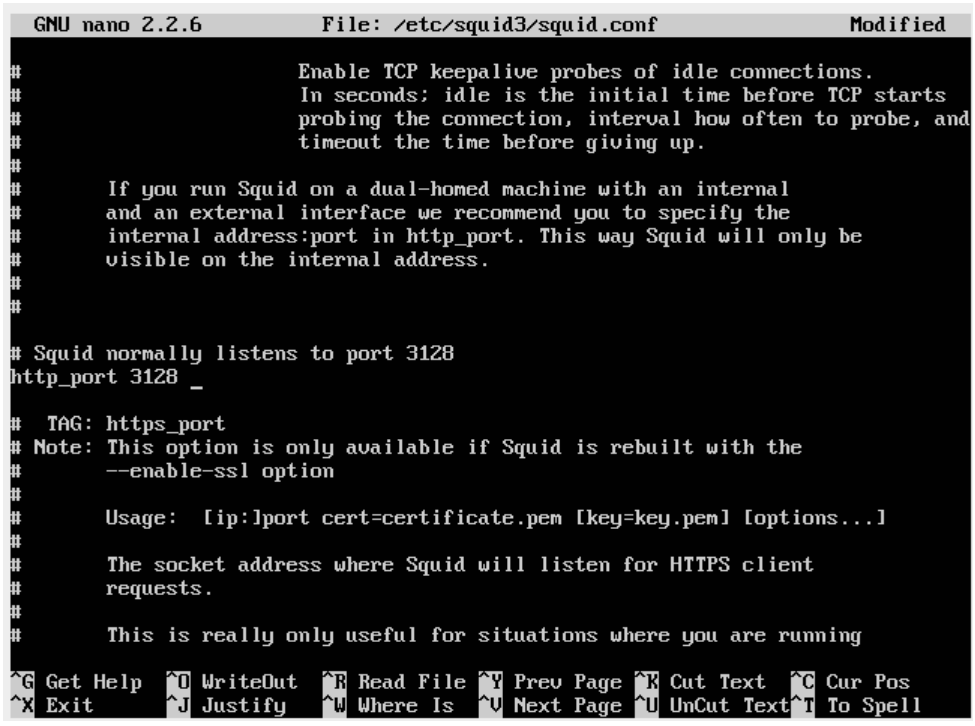


Gambar 4.3.18

- Selanjutnya tekan kembali **CTRL + W**, lalu carilah kata kunci **port 3128** sehingga kalian akan menemukan baris **http_port 3128**.



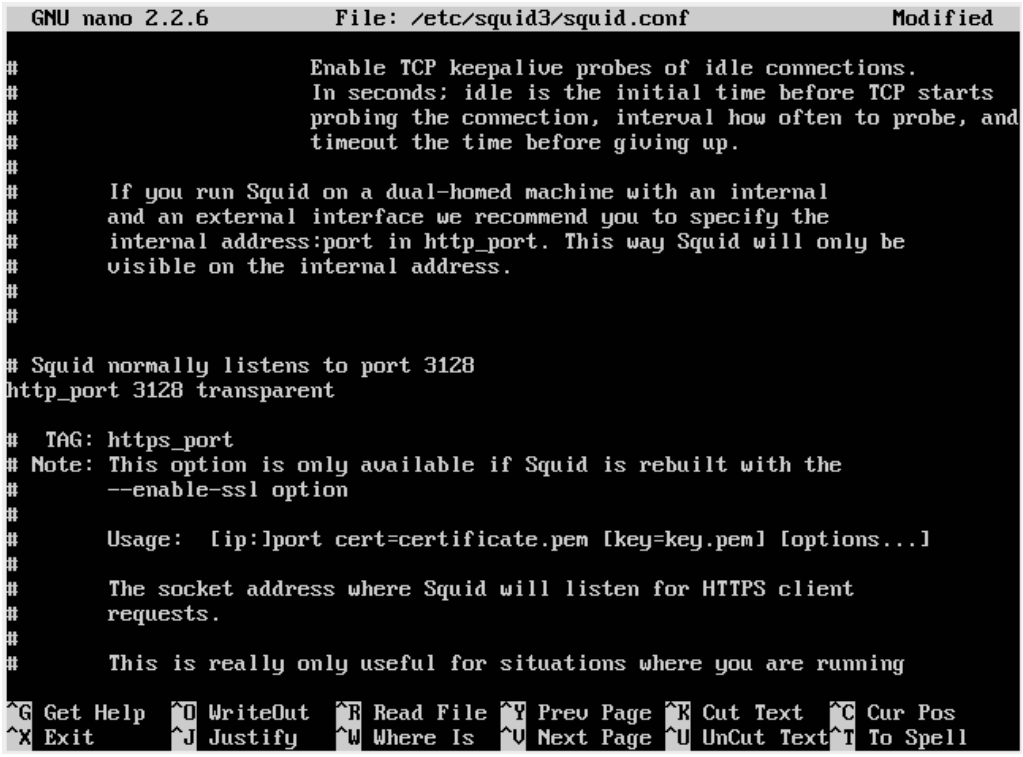
Gambar 4.3.19



Gambar 4.3.20

- Disini tambahkan kata **transparent** dibelakang baris **http_port 3128** sehingga menjadi **http_port 3128 transparent**. Ini berguna untuk membuat squid menjadi dalam mode transparan, agar klien tidak menyadari bahwa mereka sebenarnya sedang berada dalam

pengawasan squid dalam lalu lintasnya di internet.



Gambar 4.3.21

- Jika sudah, sekarang simpanlah file tersebut dengan menekan **CTRL + X**, lalu tekan **Y**, lalu **Enter**.
- Tahap selanjutnya adalah mendefiniskan situs-situs dan kata kunci apa saja yang ingin kalian blok. Edit terlebih dahulu file **/etc/squid3/terlarang.txt** dengan perintah berikut :

```
sudo nano /etc/squid3/terlarang.txt
```

- Misalnya disini saya ingin memblok situs xxx.com dan malware.com. Selain itu Saya juga ingin memblok segala situs yang mempunyai kata kunci xxx dan virus. Caranya adalah dengan mengisikan semua persyaratan tersebut kedalam file yang barusan kalian buka ini :

```
xxx.com
malware.com
virus
xxx
```

Gambar 4.3.22

- Kalian dapat mengisi sebanyak mungkin daftar situs-situs maupun kata kunci yang kalian inginkan. Atau jika kalian tidak ingin repot, kalian dapat mencari daftar situs-situs berbahaya yang harus di blok di internet. Di dalam CD buku ini pun sudah disertakan file *terlarang.txt* yang sudah lengkap terisi dengan daftar situs-situs porno, malware yang ingin di blok.
- Sampai sini, konfigurasi yang harus dilakukan di dalam file squid.conf telah selesai. Restart-lah aplikasi Squid dengan perintah berikut ini :

```
sudo squid3 -k reconfigure
```

- Terakhir, kalian harus melakukan perintah iptables yang bertujuan untuk membelokkan seluruh akses http menuju port milik proxy. Sehingga seluruh aktifitas browsing klien harus melewati proxy terlebih dahulu sebelum menuju ke internet. Caranya adalah dengan mengetikkan perintah-perintah berikut. Pertama masuk terlebih dahulu ke mode root :

```
sudo -i
```

- Setelah itu jalankan perintah dibawah ini :

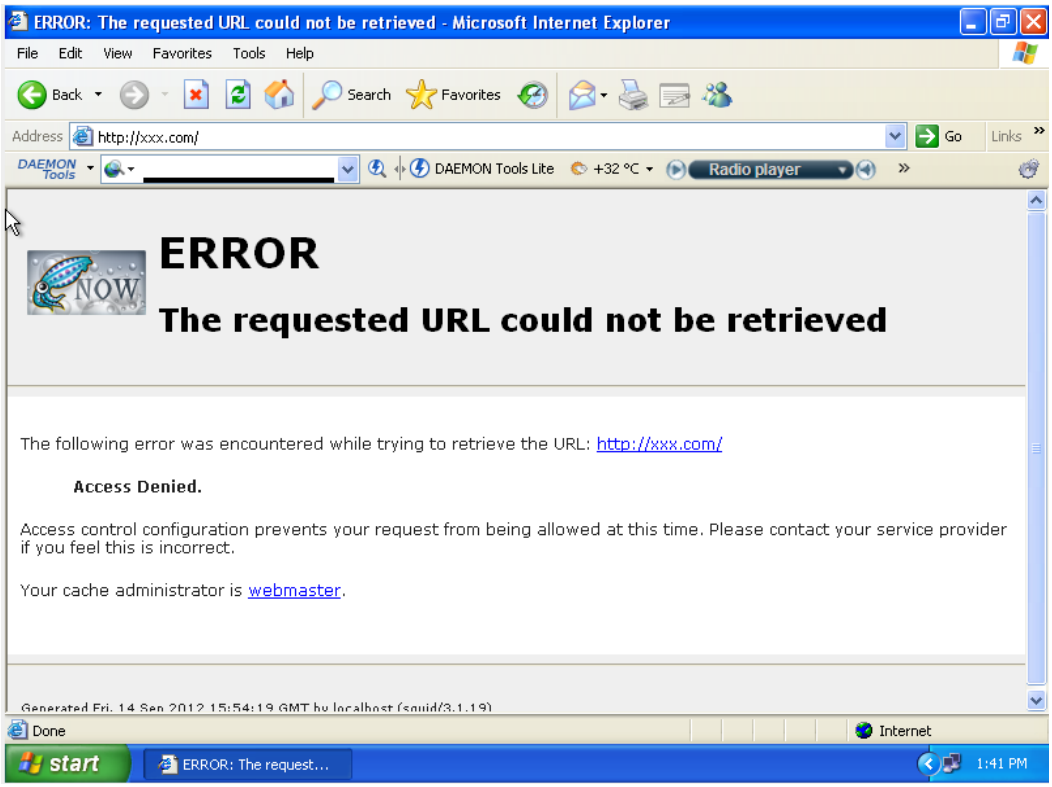
```
iptables -t nat -A PREROUTING -j REDIRECT -p tcp -s 192.168.1.0/24 -d 0/0
```

```
--dport 80 --to-ports 3128
```

- Kemudian simpan konfigurasi iptables diatas dengan mengeksekusi perintah berikut :

```
iptables-save > /etc/network/iptables.conf
```

- Untuk pengetesannya sangatlah mudah. Cobalah akses situs xxx.com atau malware.com atau dengan mengetikkan kata kunci xxx dan virus saja, maka akan muncul sebuah peringatan dari Squid *Error The Requested URL Cannot be Retrieved* seperti yang ditunjukkan oleh gambar dibawah ini.



Gambar 4.3.23

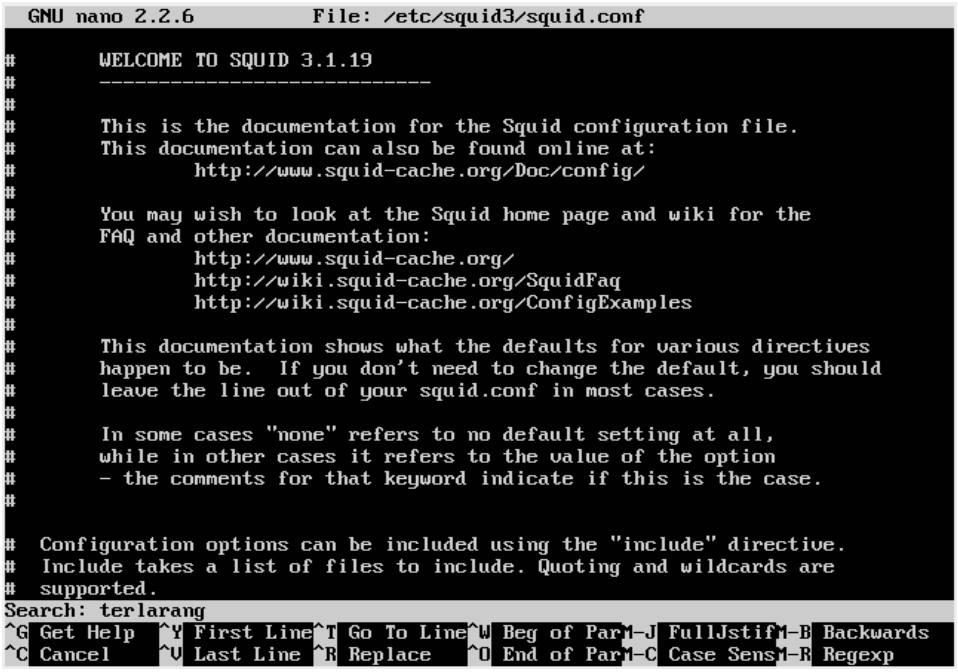
Memblokir situs-situs tertentu pada jam tertentu

Jika pada subbab sebelumnya kalian telah mempelajari cara penerapan ACL pada squid sehingga bisa memblokir situs-situs yang tidak baik, maka pada subbab kali ini kalian akan mencoba menerapkan fungsi-fungsi ACL yang lain. Disini kita akan belajar cara untuk memblokir situs-situs tertentu pada jam tertentu. Maksudnya seperti apa sih? Jika kalian perhatikan cara memblokir situs-situs tidak baik sebelumnya, situs-situs tersebut akan diblokir secara permanen oleh squid kapanpun kalian mengaksesnya. Nah, bagaimana jika kalian hanya ingin situs-situs tersebut diblokir pada jam-jam tertentu atau hari tertentu saja? Misalnya kalian hanya menginginkan situs-situs itu diblokir pada saat jam 7 pagi sampai jam 6 sore saja, selain pada jam tersebut semua situs akan

dapat diakses secara normal kembali. Nah, semua itu dapat dilakukan dengan ACL. Bagaimanakah caranya? Mari kita pelajari.

- Pertama-tama tentukan terlebih dahulu peraturan yang ingin kalian buat. Misalnya disini saya beri saja sebuah kasus. Kalian adalah seorang sysadmin di sebuah sekolah swasta. Disekolah tersebut memiliki akses internet menggunakan Hotspot yang bebas digunakan oleh seluruh muridnya. Dan kebetulan pula hampir seluruh siswanya juga memiliki laptop masing-masing. Nah, tiba-tiba suatu hari timbul sebuah masalah, ternyata banyak sekali siswa yang sering mengakses situs-situs social media seperti Facebook atau Twitter pada saat jam belajar bahkan pada saat ada guru yang sedang mengajar. Akhirnya kalian pun diminta oleh kepala sekolah untuk memblokir akses ke semua situs-situs social media pada saat jam belajar dan hanya boleh mengaksesnya sehabis pulang sekolah, kecuali hari sabtu. Pada hari sabtu semua akses internet akan dibebaskan. Jam belajar sekolah tersebut dimulai pada pukul 07:00 sampai dengan pukul 14:00.
- Setelah mengetahui kasusnya dan membuat peraturannya, maka barulah kalian dapat memulai konfigurasi. Pertama-tama edit file **/etc/squid3/squid.conf** dengan mengeksekusi perintah dibawah ini :

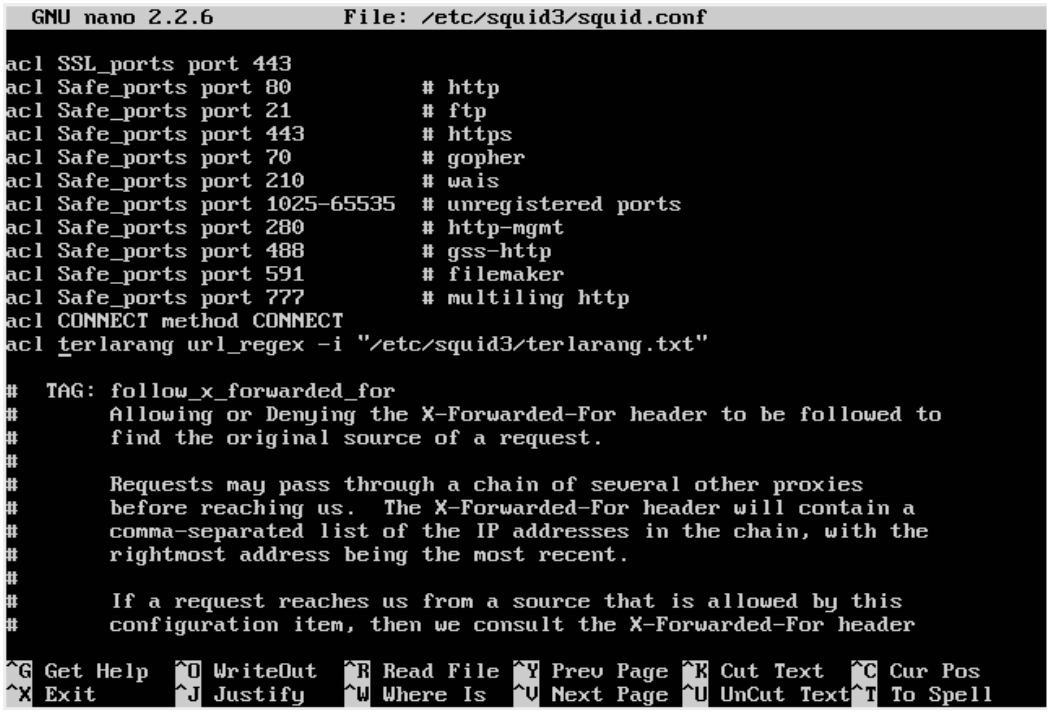
```
sudo nano /etc/squid3/squid.conf
```



Gambar 4.3.24

- Kemudian tekan **CTRL + W**, lalu carilah kata kunci terlarang maka kalian akan menemukan

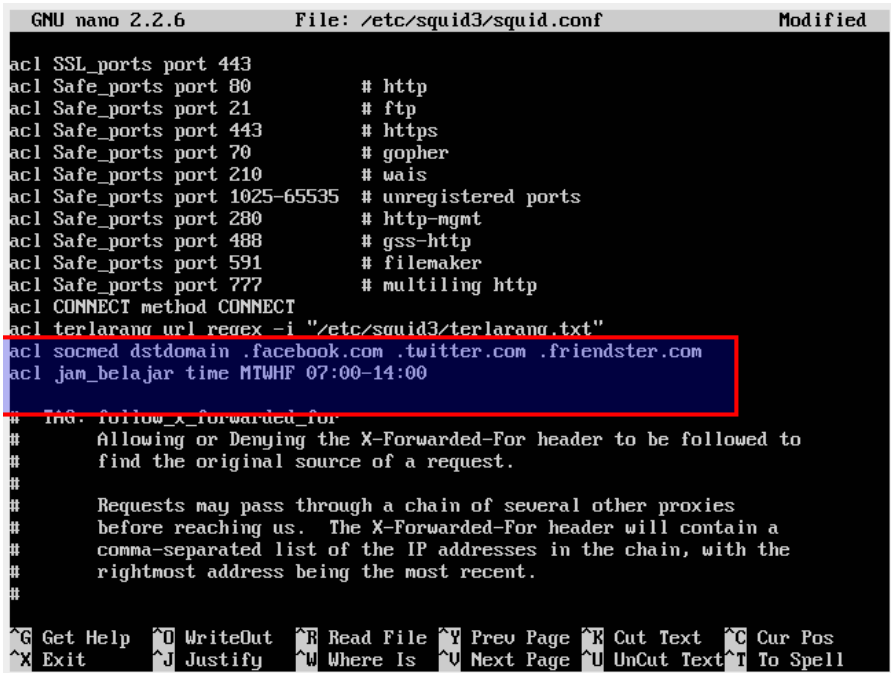
baris **acl terlarang url_regex -i "/etc/squid3/terlarang.txt"** yang telah kalian buat sebelumnya.



Gambar 4.3.25

- Tepat dibawah baris tersebut, tambahkan script dibawah ini :

```
acl socmed dstdomain .facebook.com .twitter.com .friendster.com
acl jam_belajar time MTWHF 07:00-14:00
```

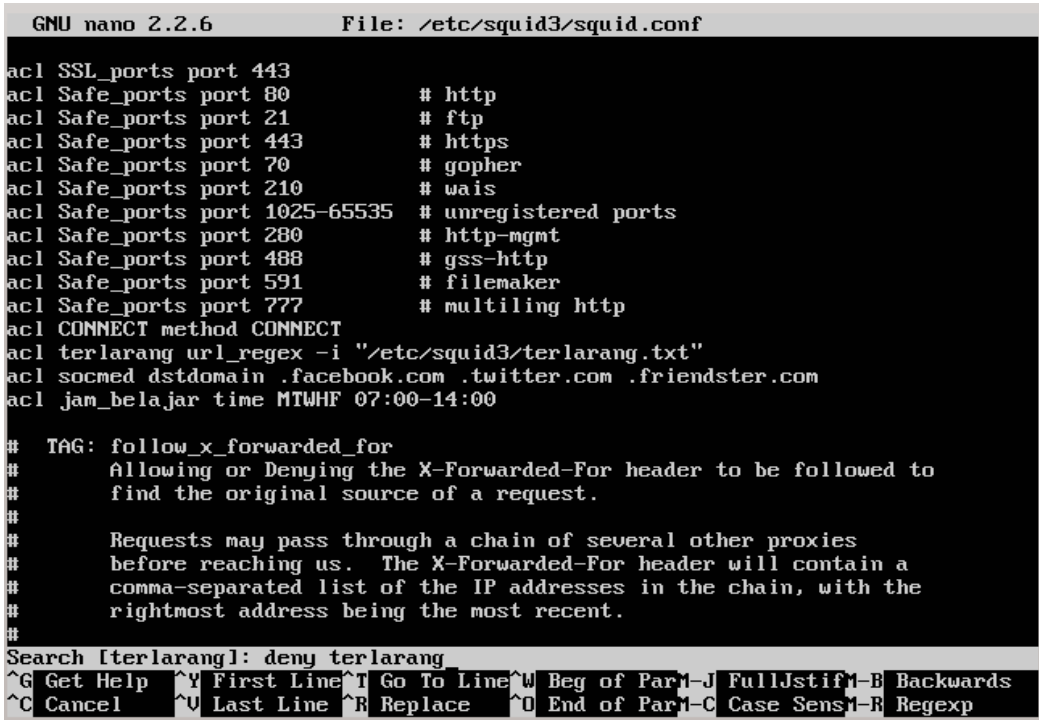


Gambar 4.3.26

- Maksud dari script diatas adalah :
  - `acl socmed dstdomain .facebook.com .twitter.com .friendster.com`

    socmed adalah nama ACL-nya, yang saya ambil dari singkatan social media. Kemudian **dstdomain** adalah aturan ACL untuk mendefinisikan domain tujuan yang digunakan. Sedangkan **Facebook.com, .twitter.com,** serta **.friendster.com** adalah domain yang ingin kalian blokir.
  - `acl jam_belajar time MTWHF 07:00-14:00`

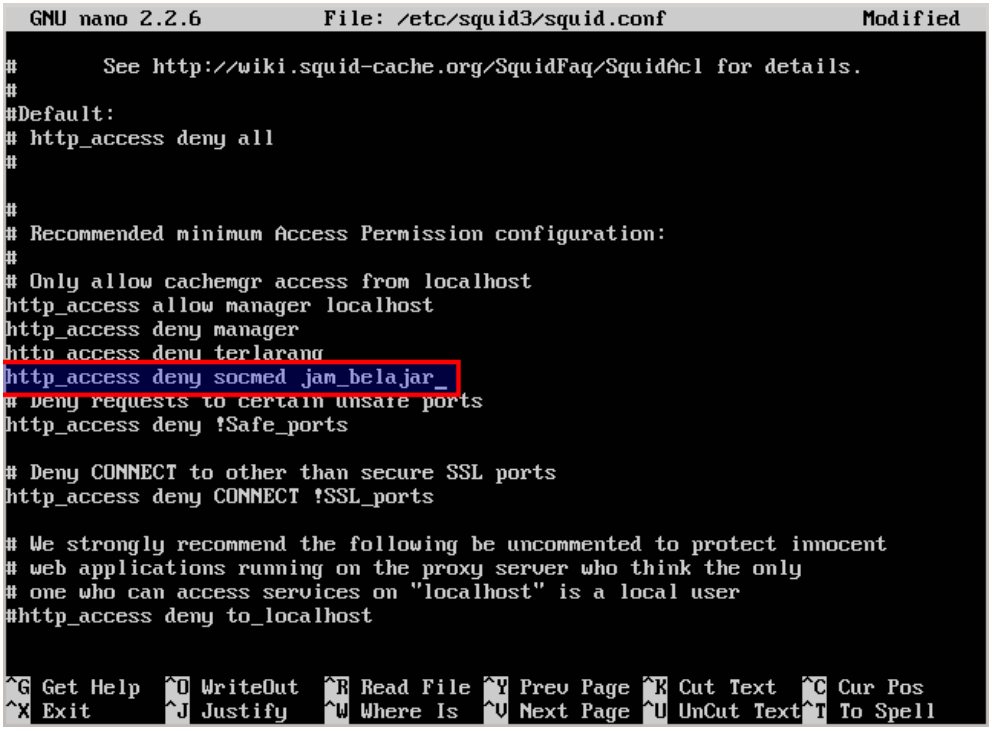
    Sama seperti baris diatas, **jam_belajar** adalah nama ACL-nya. Lalu **time** adalah aturan ACL untuk mendefinisikan waktu dan hari yang digunakan. **MTWHF** adalah definisi dari hari Senin sampai Jumat. Dan **07:00-14:00** adalah jam belajar yang ingin kalian blokir.
- Setelah itu cari lagi kata kunci **deny terlarang** dengan menekan tombol **CTRL + W**.



Gambar 4.3.27

- Nanti kalian akan menemukan baris **http_access deny terlarang** yang telah kalian buat sebelumnya. Tepat dibawah baris tersebut tambahkan baris ini yang artinya menolak akses ke ACL socmed dan jam_belajar :

  `http_access deny socmed jam_belajar`



Gambar 4.3.28

- Setelah itu simpanlah file tersebut dengan menekan **CTRL + X**, lalu tekan **Y**, lalu **Enter**.
- Terakhir restart lah service dari squid3 untuk menerapkan langsung efeknya dengan perintah berikut :

```
sudo squid3 -k reconfigure
```

- Sekarang cobalah tes dari komputer client, mulai hari Senin sampai dengan Jumat dari jam 07:00 sampai jam 14:00, pasti mereka tidak akan bisa mengakses situs-situs yang telah tercantum pada ACL socmed, yaitu facebook.com, twitter.com, dan friendster.com. Tetapi selain situs-situs tersebut masih dapat dibuka secara normal (kecuali situs yang tercantum pada ACL terlarang).
- Contoh konfigurasi ACL diatas sebenarnya hanya segelintir cara dari sekian banyak konfigurasi ACL yang lain. Konfigurasi diatas pun tentu saja dapat kalian rubah sesuai dengan kebutuhan kalian masing-masing. Oleh karena itu yang saya tekankan bagi kalian yang membaca buku ini adalah konsepnya. Intinya adalah konsep. Lebih baik kalian pahami betul-betul konsep dari ACL ini. Karena jika konsepnya sudah paham, maka dalam keadaan dan kondisi apapun kalian pasti dapat menerapkannya.

Pengaturan Bandwidth dengan Squid

Selain dapat berfungsi meng-caching file-file web, memblokir situs-situs dengan metode ACL, ternyata squid juga dapat berfungsi sebagai *Bandwidth Controller* juga. Ya, kalian dapat mengatur berapa kecepatan akses yang boleh didapat oleh klien berdasarkan ip-ip mereka. Misalnya saja ip address 192.168.1.200 bisa mendapat bandwidth sebesar 200Kbps, sedangkan ip address lainnya hanya mendapat kecepatan bandwidth sebesar 50Kbps, itu semua dapat kalian lakukan hanya dengan menggunakan squid.

- Untuk memulai konfigurasi pengaturan Bandwidth pada squid, hal yang pertama kali harus dilakukan adalah memahami konsep dari pengaturan Bandwidth di squid. Pada dasarnya, terdapat empat buah bagian yang perlu kalian ketahui, yaitu delay_pools, delay_class, delay_class, dan delay_parameters.
  - Delay_pools

    Apa itu delay_pools? Delay_pools adalah jumlah aturan yang ingin kalian buat. Misalnya kalian ingin membuat peraturan seperti ini : Ip address 192.168..1.10 sampai 192.168.1.100 akan dibatasi bandwidhtnya menjadi 50Kbps. Itu berarti satu delay_pools. Sedangkan apabila kalian membuat peraturan seperti ini : Ip address 192.168.1.10 sampai 192.168.1.100 akan dibatasi bandwidthnya menjadi 50 Kbps, lalu ip address 192.168.1.101 sampai 192.168.1.254 akan mendapat bandwidth sebesar 100Kbps. Itu berarti kalian telah menerapkan dua buah delay_pools. Delay_pools ini penggunaannya akan dirangkaikan bersamaan dengan delay_class dan delay_parameters.
  - Delay_class

    Delay_class adalah aturan sistematika bagaimana pengaturan bandwidth itu berlangsung berdasarkan delay_pools yang digunakan. Sebenarnya terdapat 5 buah tipe delay_class yang dapat digunakan, namun yang akan saya jabarkan dibawah ini adalah tipe 1,2 dan 3 yang paling sering digunakan :
    - Delay_class tipe 1

      Semua akses akan dibatasi oleh sebuah single bucket. Artinya hanya bisa mendefinisikan overall bandwidth untuk suatu ACL saja, tidak bisa mendefinisikan bandwidth dengan lebih mendetail.
    - Delay_class tipe 2

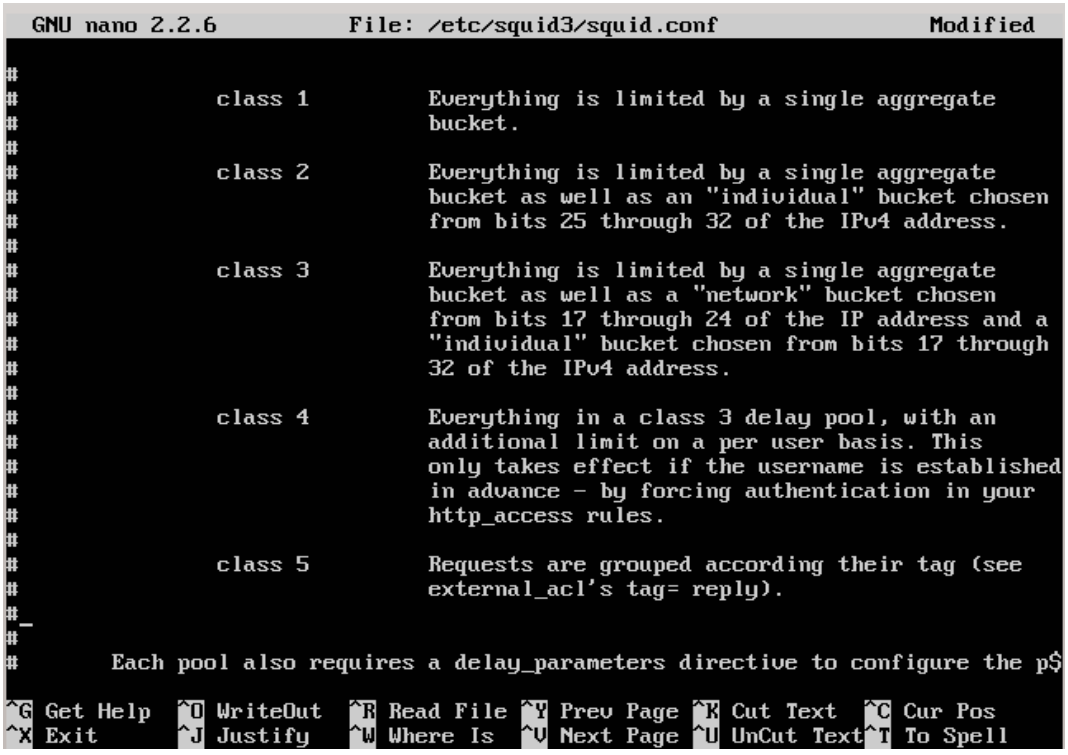
      Semua akses akan dibatasi oleh sebuah agregate dengan dua parameter bandwidth. Artinya parameter pertama mendefiniskan berapa bandwidth maksimal yang

didapatkan ACL, parameter kedua mendefinisikan berapa bandwidth overall untuk ACL yang spesifik yang ada pada network tersebut.

- Delay_class tipe 3

  Ini adalah tipe delay_class yang definisi bandwidthnya paling mendetail. Parameter pertama mendefinisikan berapa bandwidth maksimal yang didapatkan ACL, parameter kedua mendefiniskan berapa bandwidth normal yang didapatkan ACL secara umum, dan parameter yang ketiga adalah mendefiniskan bandwidth yang didapatkan ACL jika mengakses ACL-ACL tertentu yang spesifik, misalnya file .avi.

Untuk pengertian lain dari tipe-tipe delay_class ini kalian dapat melihat di squid.confnya langsung, atau kalian dapat merujuk pada link ini.



Gambar 4.3.29

- Delay_access

  Delay_access adalah opsi yang mendefinisikan siapa-siapa orang yang akan dimasukkan ke pool tertentu untuk mendapatkan pembatasan bandwidth.

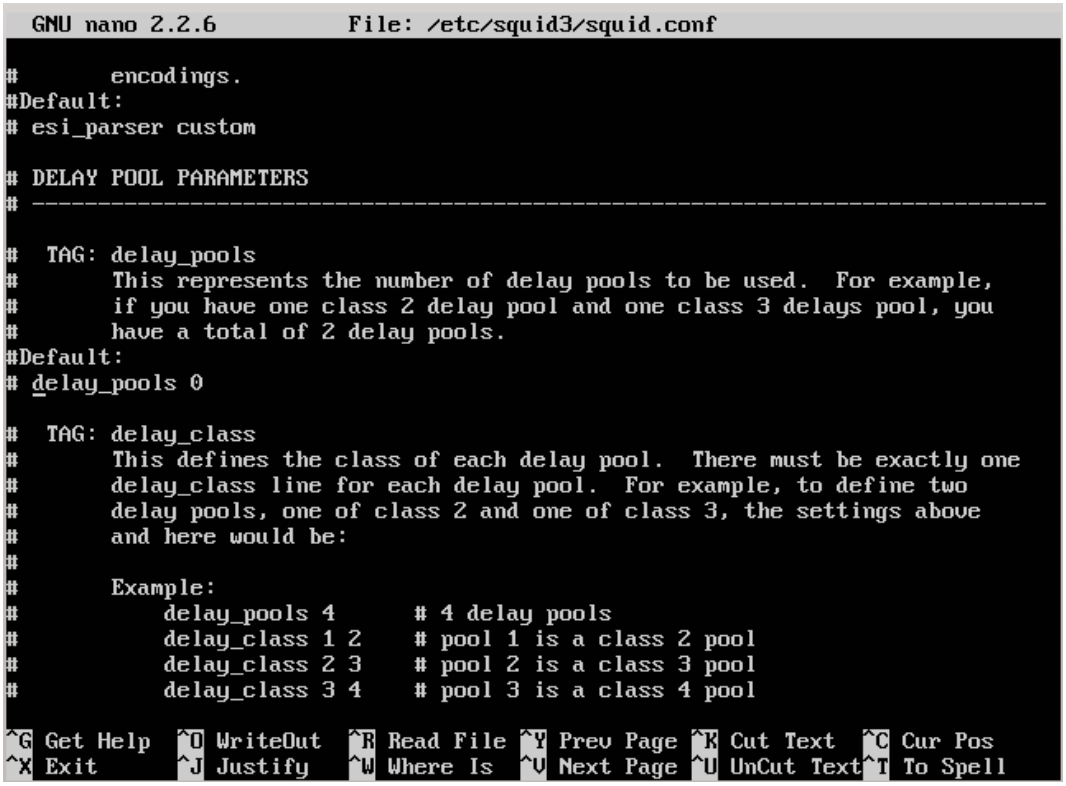
- Delay_parameters

  Inilah opsi yang mendefinisikan rumus pengaturan bandwidth dari semua delay_pools.

- Setelah mengetahui teorinya, sekarang kalian harus membuat peraturannya terlebih dahulu sama seperti sub-bab memblokir situs tertentu pada jam tertentu yang sebelumnya. Misalnya kalian adalah seorang sysadmin sebuah SMK swasta. Sekolah tersebut memiliki bandwidth internet sebesar 1Mbps. Sekolah tersebut menginginkan adanya tiga buah peraturan dalam pembagian Bandwidth internetnya. Yang pertama adalah ip address siswa biasa dari range 192.168.1.101 sampai 192.168.1.254 hanya diperbolehkan mendapat kecepatan akses sebesar 50Kbps per-siswa. Peraturan kedua, para guru dan staf yang berjumlah 30 orang dari ip address 192.168.1.50 sampai 192.168.1.80 diperbolehkan mendapat kecepatan akses sebesar 100Kbps saja. Dan yang terakhir, kepala sekolah dengan ip address 192.168.1.20 dan kalian sebagai admin dengan ip 192.168.1.21 diperbolehkan mendapat akses dengan kecepatan penuh.
- Selanjutnya barulah kalian dapat memulai proses konfigurasi. Pertama-tama bukalah file **/etc/squid3/squid.conf** dengan perintah ini :

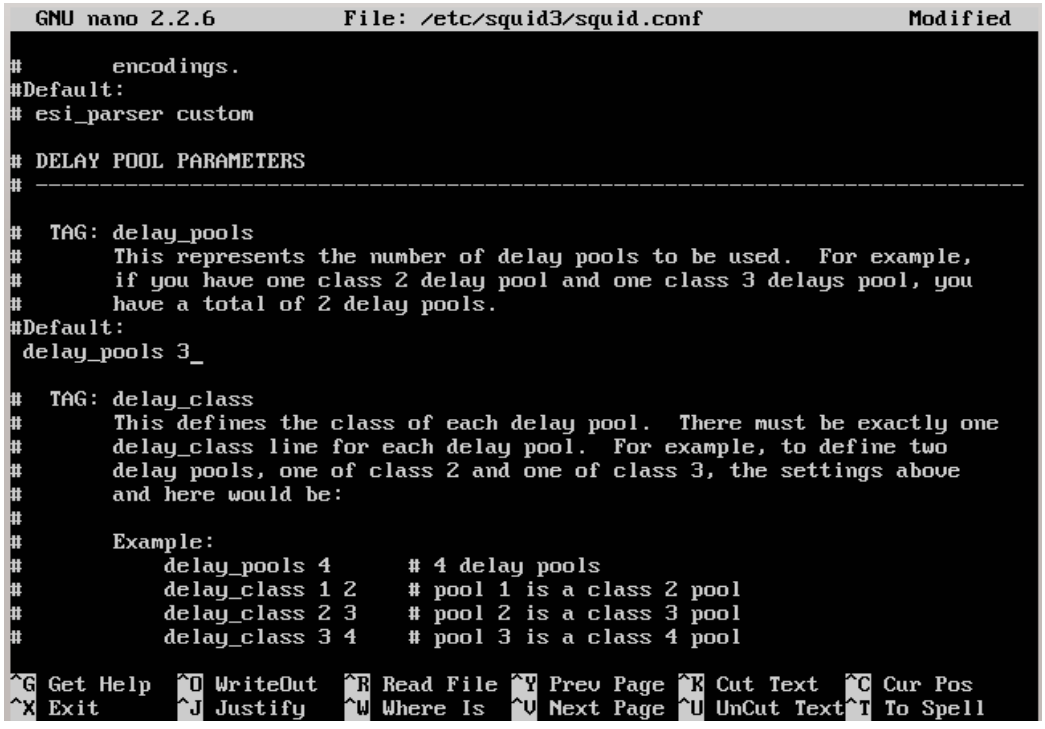
```
sudo nano /etc/squid3/squid.conf
```

- Kemudian tekan **CTRL + W**, dan cari kata kunci **delay_pools 0** hingga kalian menemukan baris **# delay_pools 0** :



Gambar 4.3.31

- Hilangkan tanda pagar (#) di depannya lalu ganti baris tersebut menjadi **delay_pools 3** :



Gambar 4.3.32

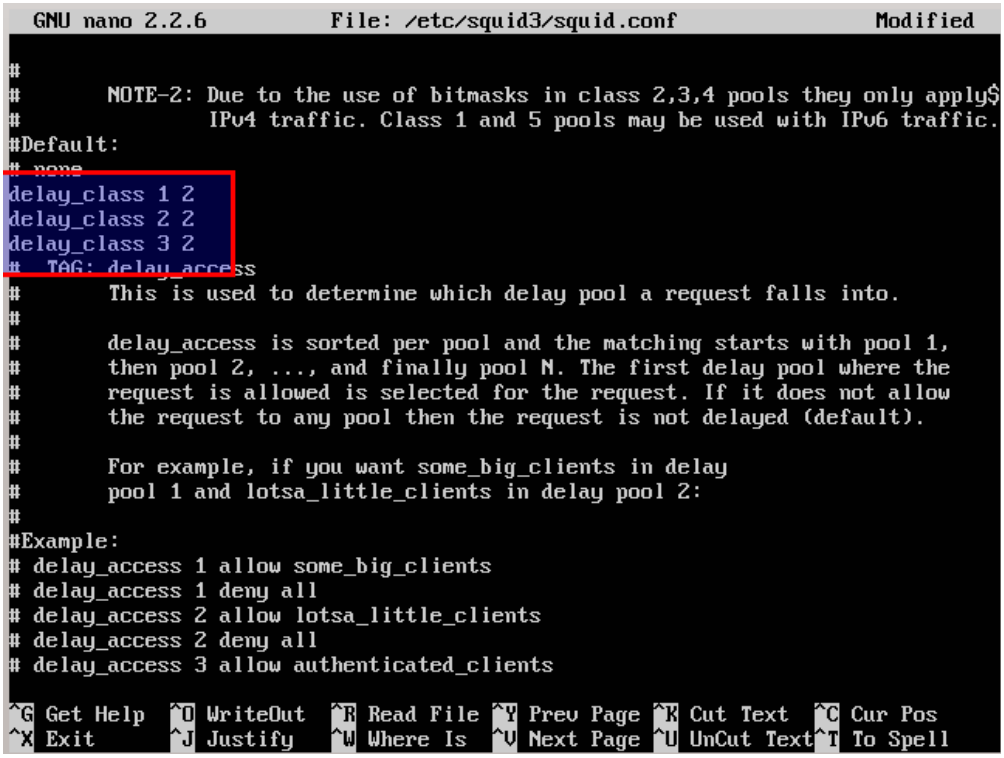
- Setelah menentukan delay_pools-nya, selanjutnya kalian harus menentukan delay_class-nya.

Tekan **CTRL + W,** kemudian cari kata kunci **tag: delay_access** :

Gambar 4.3.33

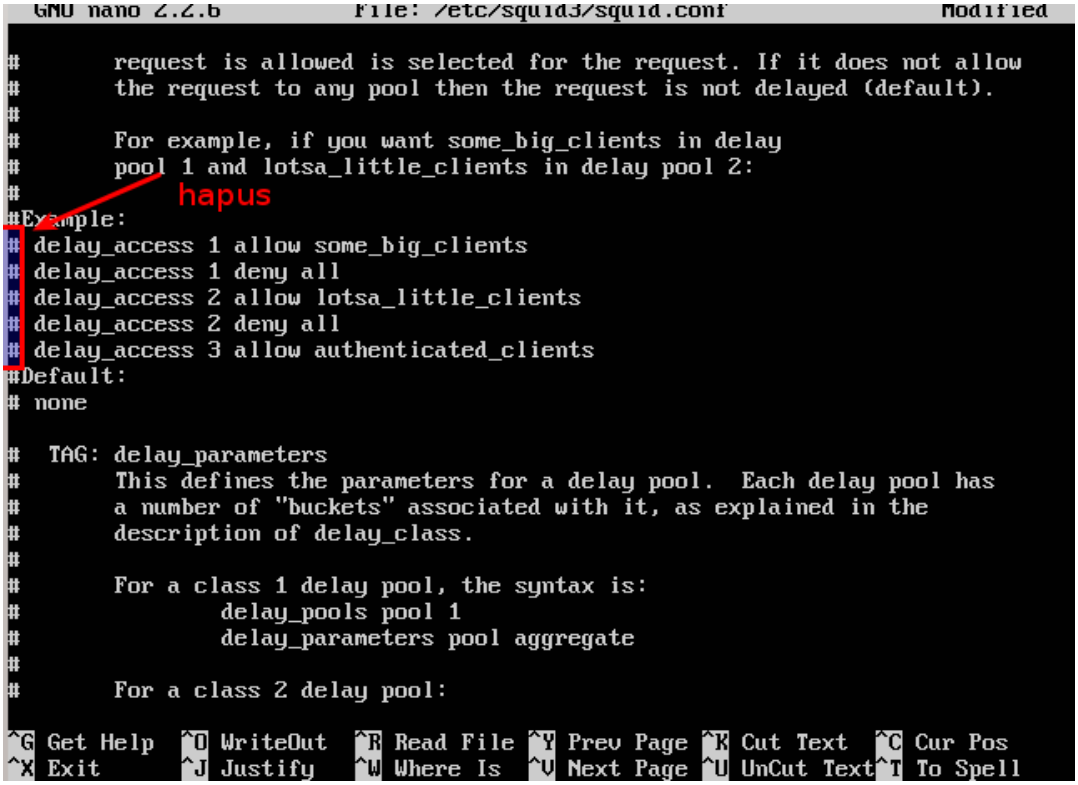
- Nanti kalian menemukan baris **# TAG: delay_access** disitu. Tepat diatas baris tersebut tambahkan kode dibawah ini :

```
delay_class 1 2

delay_class 2 2

delay_class 3 2
```

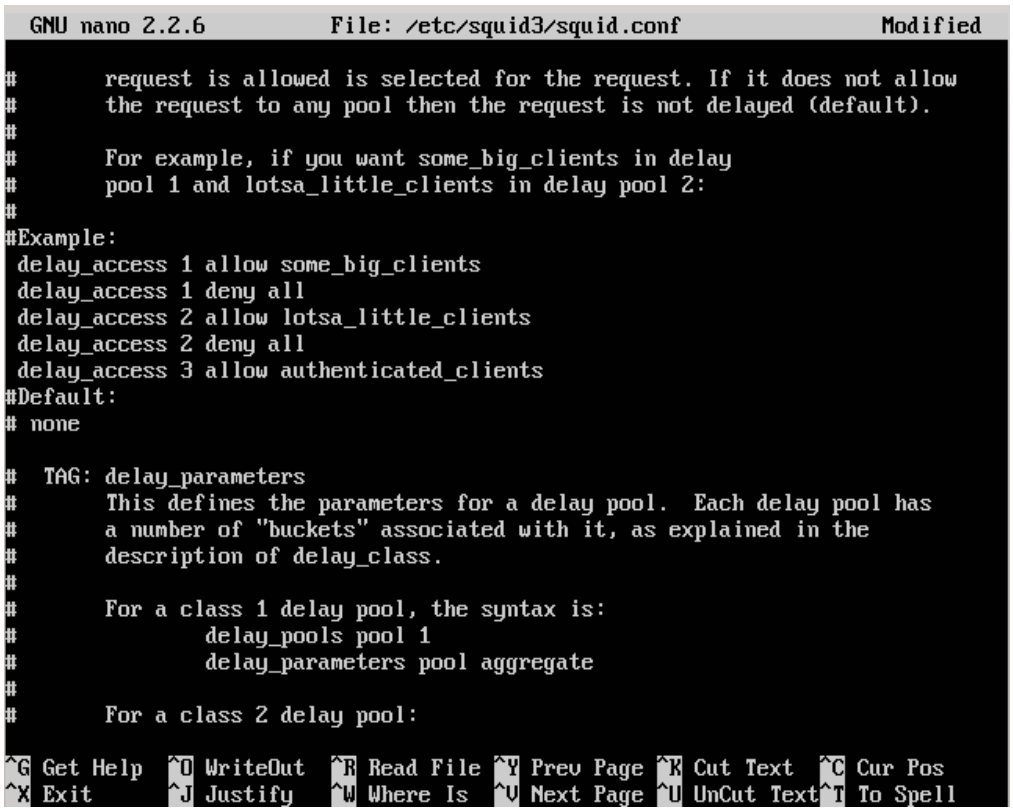


Gambar 4.3.34

- Selanjutnya adalah menentukan delay_access-nya, yaitu menentukan siapa saja yang akan menempati pool-pool yang telah kalian buat. Tidak jauh dibawah dari baris **delay_class** yang kalian buat barusan, terdapat baris **# delay_access 1 allow some_big_clients** (lihat gambar 4.3.35 untuk lebih jelasnya). Nah silahkan kalian hapus tanda pagar didepannya dari **delay_access 1 allow some_big_clients** hingga **delay_access 3 allow authenticated_clients**.



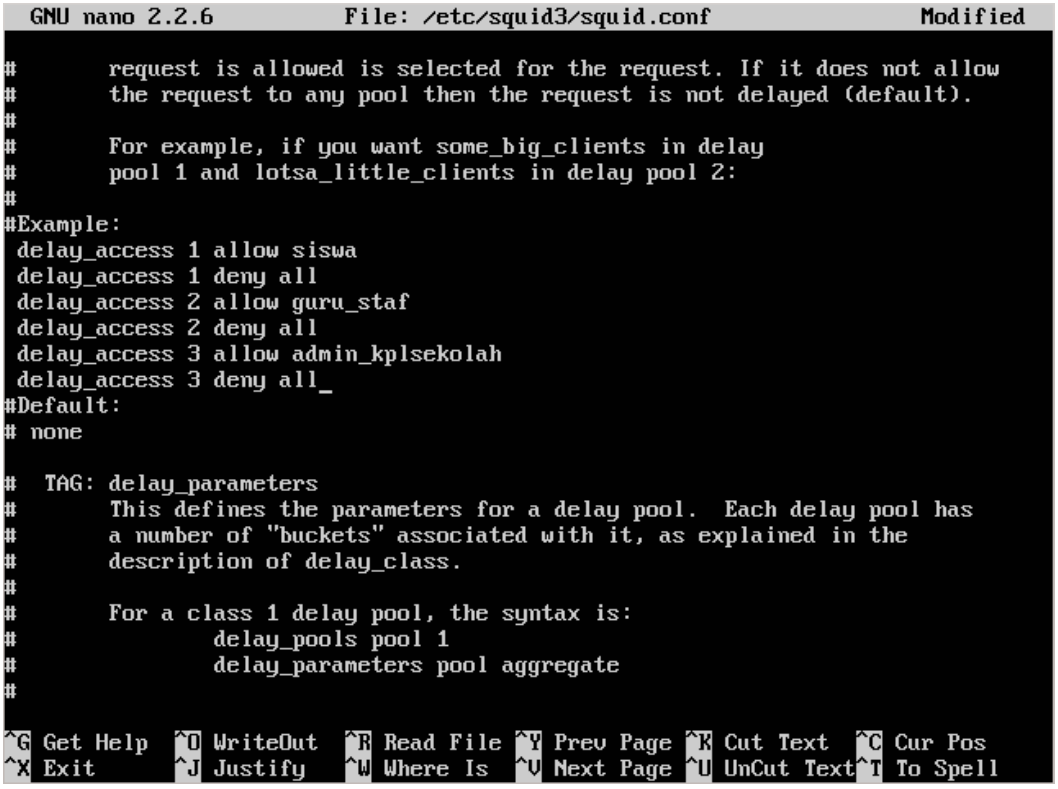
Gambar 4.3.35



Gambar 4.3.36

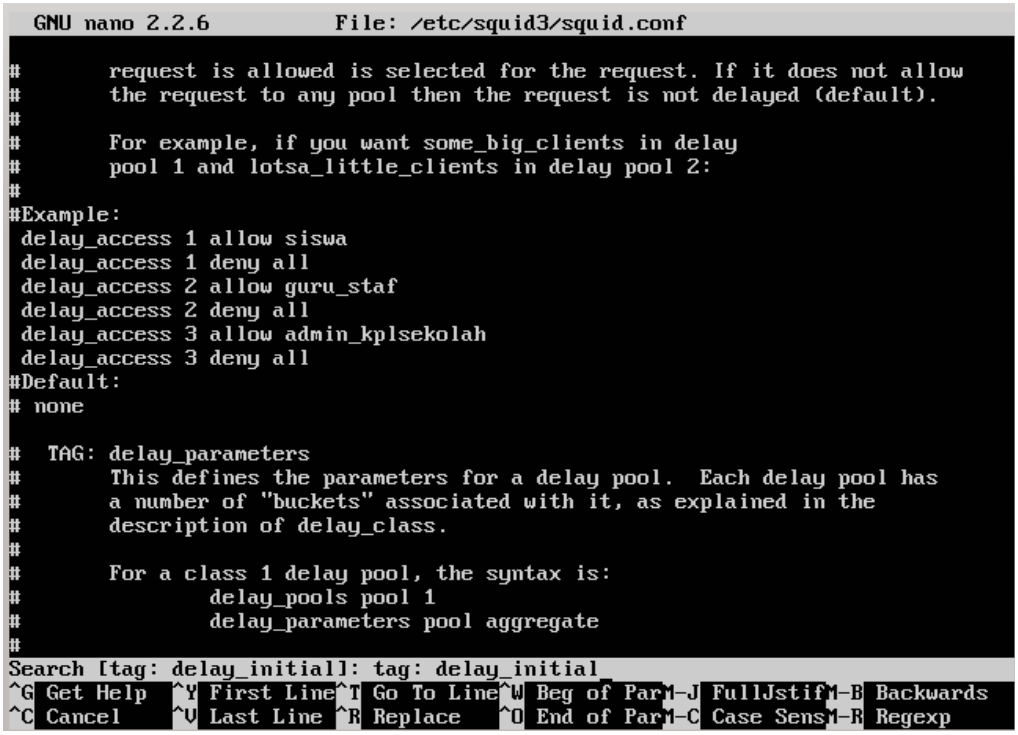
- Kemudian ganti baris-baris tersebut dengan baris dibawah ini :

```
delay_access 1 allow siswa
delay_access 1 deny all
delay_access 2 allow guru_staf
delay_access 2 deny all
delay_access 3 allow admin_kplsekolah
```

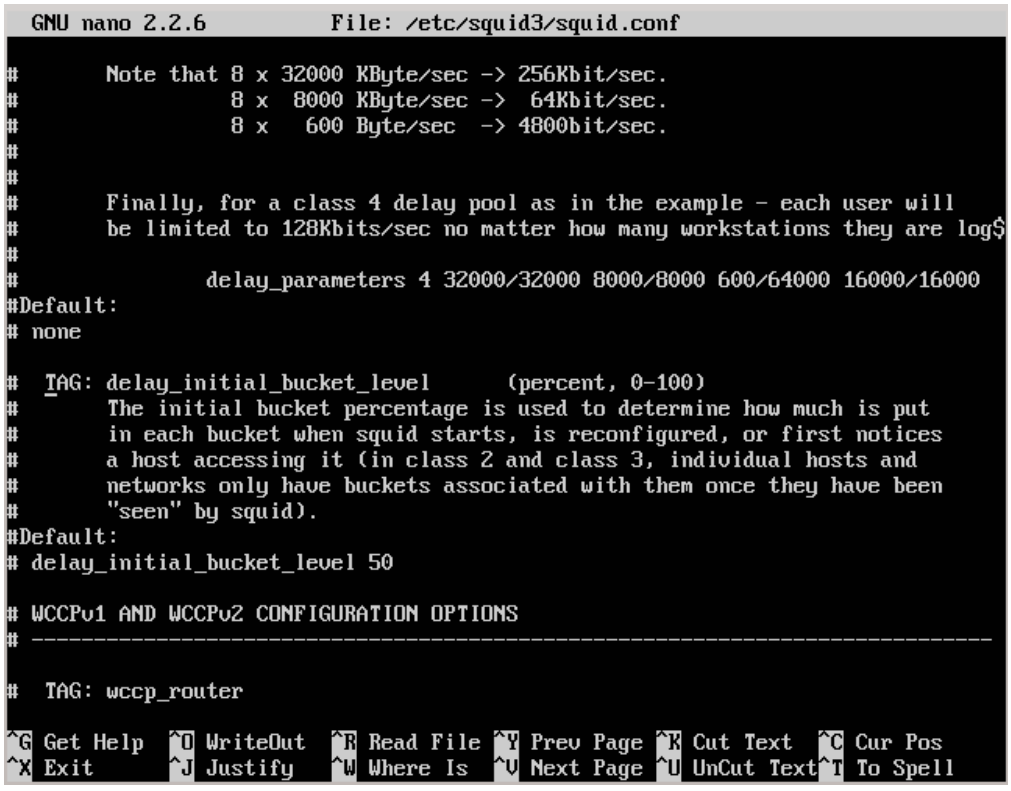


Gambar 4.3.37

- Setelah itu kalian juga harus menentukan delay_parameters-nya. Tekan **CTRL + W**, kemudian cari kata kunci **tag: delay_initial** sehingga kalian akan menemukan baris **# TAG: delay_initial_bucket_level** :



Gambar 4.3.38

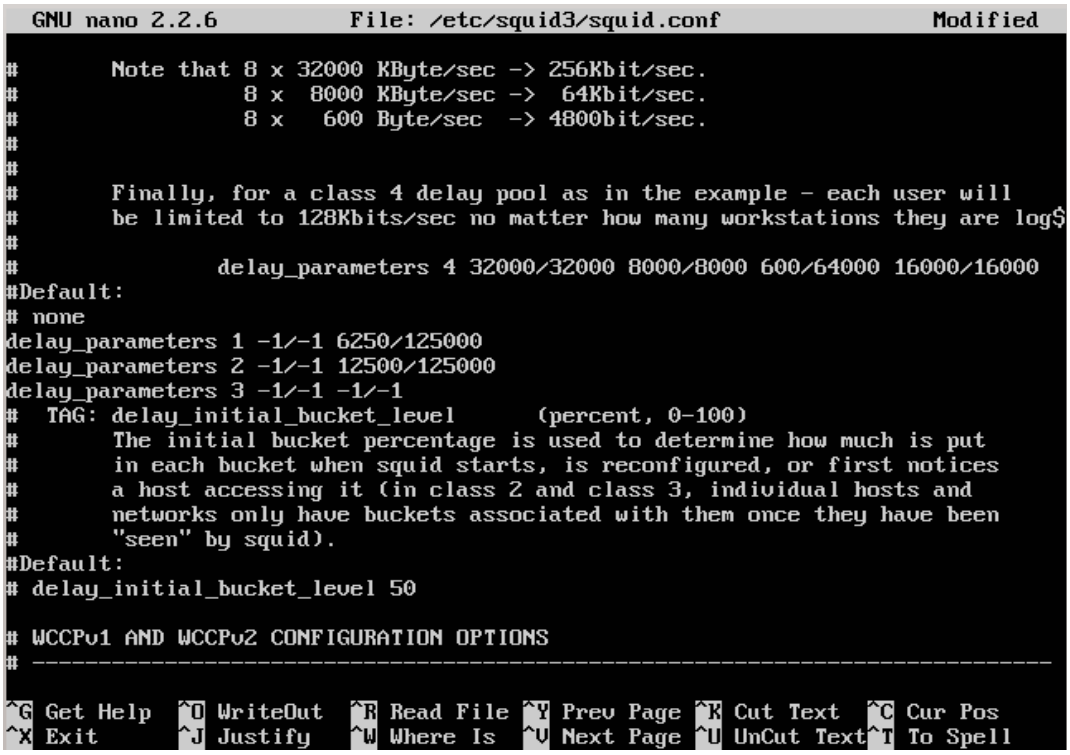


Gambar 4.3.39

- Tepat diatas baris **# TAG: delay_initial_bucket_level** , tambahkan kode dibawah ini :

```
delay_parameters 1 -1/-1 6250/125000
```

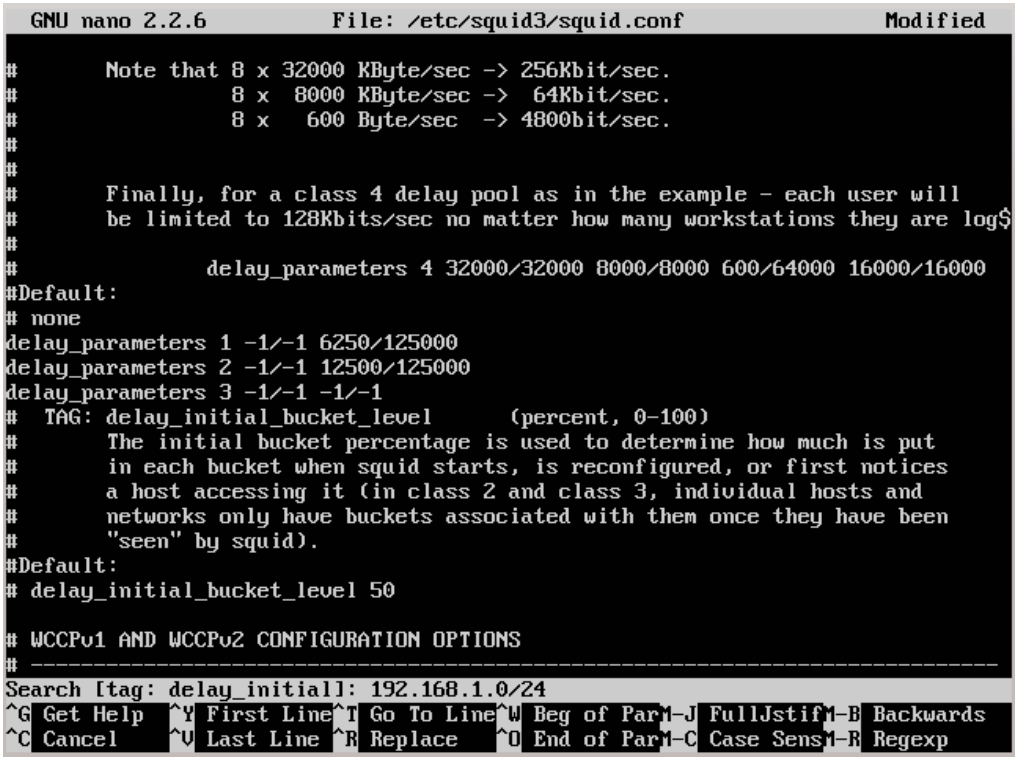
```
delay_parameters 2 -1/-1 12500/125000

delay_parameters 3 -1/-1 -1/-1
```



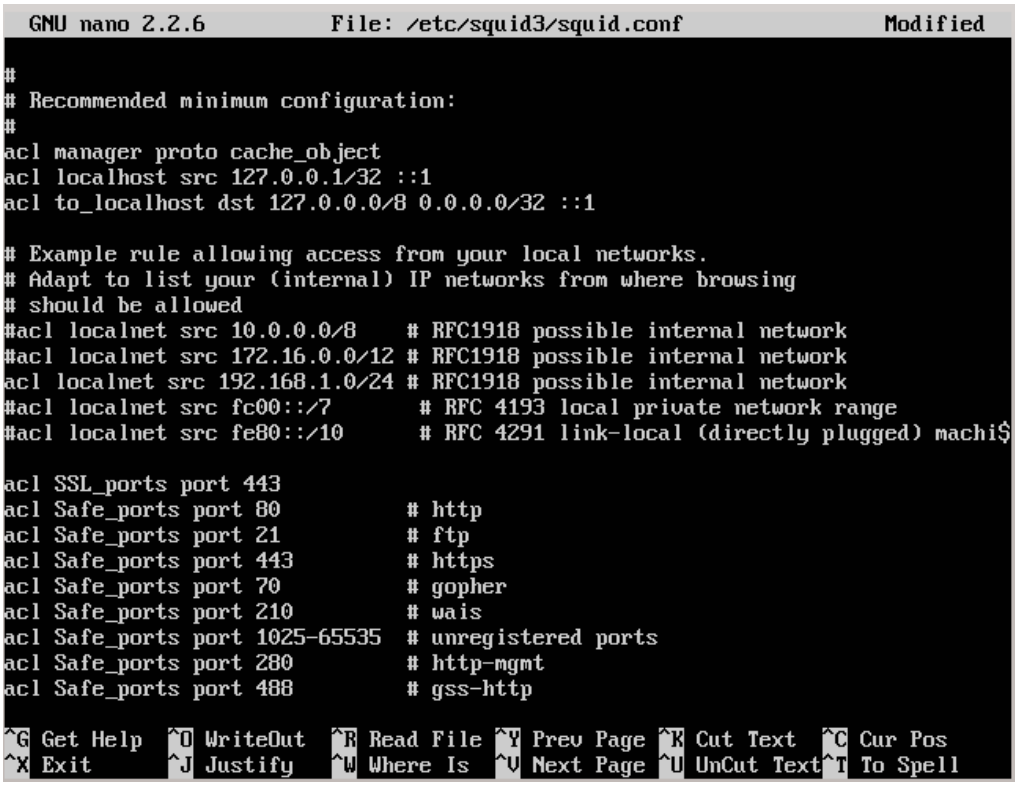
Gambar 4.3.40

Maksud angka 6250/125000 dan yang lainnya adalah hitungan angka dalam bentuk bit. Jadi misalnya 6250 bit adalah 6250 x 8 = 50.000 Byte = 50KByte. Sedangkan arti -1 adalah unlimited. Jadi apabila delay_parameters 3 -1/-1 -1/-1 artinya ACL yang menempati pool ke 3 akan mendapat akses unlimited tanpa adanya batasan apapun.

- Setelah menentukan semua delay yang diperlukan untuk pembatasan bandwidth, ternyata masih ada satu hal yang kurang. Kalian belum mendefinisikan berapa ip address dari ACL-ACL pengguna seperti siswa, guru_staf, dan admin_kplsekolah. Tekan **CTRL + W**, dan ketikkan kata kunci **192.168.1.0/24**, sehingga kalian akan menemukan baris **localnet 192.168.1.0/24** yang pernah kalian buat pada saat sub-bab *memblok website yang tidak baik*.



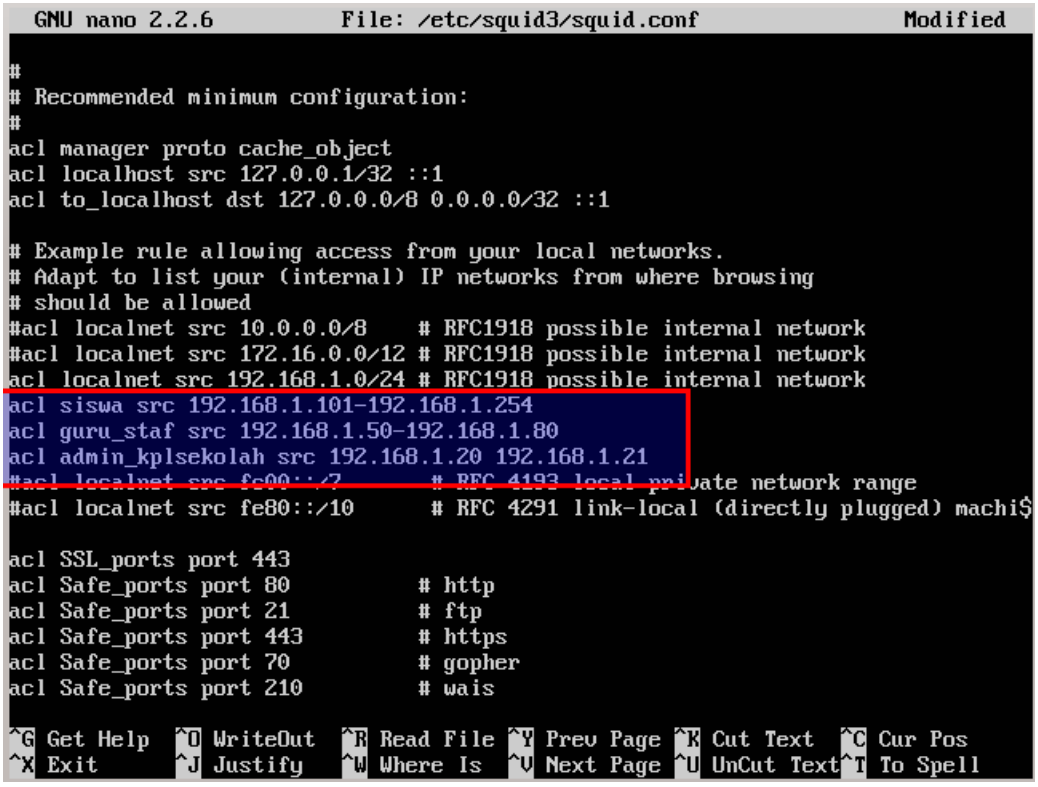
Gambar 4.3.41



Gambar 4.3.42

- Setelah ketemu, tepat dibawah baris tersebut tambahkan baris baru berikut ini :

```
acl siswa src 192.168.1.101-192.168.1.254
acl guru_staf src 192.168.1.50-192.168.1.80
acl admin_kplsekolah 192.168.1.20 192.168.1.21
```



Gambar 4.3.43

- Jika sudah, sekarang simpanlah file tersebut dengan menekan **CTRL + X**, lalu tekan **Y**, lalu **Enter**.
- Terakhir restart service squid dengan perintah berikut :

```
sudo squid3 -k reconfigure
```

- Jika tidak ada kesalahan, maka sampai sini seharusnya konfigurasi pembatasan bandwidth dengan squid telah selesai. Coba downloadlah suatu file menggunakan komputer siswa yang telah kalian batasi akses bandwidthnya untuk membuktikannya.

4.4. Konfigurasi Firewall

Apa itu Firewall?

Firewall dalam dunia jaringan adalah sebuah perangkat baik itu perangkat lunak ataupun perangkat keras atau gabungan dari keduanya, yang berfungsi untuk membatasi, mengatur, dan menginspeksi lalu lintas antar jaringan. Firewall akan mengijinkan lalu lintas mana yang dianggap aman dan melarang lalu lintas yang tidak dianggap aman. Biasanya Firewall akan diletakkan sebagai sebuah mesin gateway pembatas antara jaringan lokal dengan jaringan internet yang bertujuan untuk melindungi jaringan lokal dari serangan-serangan pihak luar.

Dalam dunia jaringan, Firewall merupakan komponen yang sangat penting sekali untuk meningkatkan keamanan. Firewall akan membatasi akses-akses dari ip atau port-port yang dianggap berbahaya untuk meminimalisir resiko serangan yang mungkin terjadi. Ibarat sebuah rumah, Firewall ini adalah seorang satpam yang siap siaga memeriksa semua orang orang yang ingin masuk atau keluar dari rumah tersebut. Apabila orang tersebut sudah memiliki ijin yang telah dipercaya maka ia akan diperbolehkan masuk, dan apabila ia tidak memiliki ijin maka akan langsung ditolak oleh si satpam. Yah, kira-kira seperti itulah.

gambar 4.4.1

Apa itu Iptables?

Di Linux Ubuntu Server 12.04 LTS, bentuk pengimplementasian Firewall adalah dengan menggunakan **Iptables**. Iptables merupakan salah satu dari beberapa aplikasi Firewall yang dapat dijalankan di Linux. Sebenarnya ada beberapa aplikasi Firewall yang berjalan di Linux seperti **ipfwadm**, **ipchains**, dan **iptables**. Iptables saya pilih karena ia sudah terinstall secara default di Ubuntu Server 12.04 LTS jadi kita tidak perlu repot-repot lagi untuk menginstallnya. Selain itu

iptables juga ringan dan sangat *powerfull*.

Dalam pengaturan paketnya, ada 3 buah tabel pada Iptables, yaitu :

- Tabel Filter

  Tabel ini yang berkaitan dengan *filtering* paket. Tabel Filter terbagi menjadi 3, yaitu :

  - INPUT, yaitu untuk mengatur semua paket-paket yang masuk (incoming traffic)
  - FORWARD, yaitu untuk mengatur semua paket-paket yang diteruskan atau dirouting (routing traffic)
  - OUTPUR, yaitu untuk mengatur semua paket-paket yang keluar (outgoing traffic)

- Tabel NAT

  Di tabel NAT ini, Iptables akan mengganti header paket, berupa *source/destination* IP address dan port. NAT terbagi lagi menjadi 3 buah *chain*, yaitu :

  - PREROUTING *chain*.
  - OUTPUT *chain*.
  - POSTROUTING *chain*.

- Tabel Mangle

  Tabel mangling digunakan untuk mengubah (alteration) informasi paket, seperti Type Of Service (TOS), Time To Live (TTL), dan MARK (bandwidth limiting dan class based queuing). Tabel Mangle terbagi lagi menjadi 5, yaitu :

  - PREROUTING chain.
  - INPUT chain.
  - OUTPUT chain.
  - FORWARD chain.
  - POSTROUTING chain.

Jika dilihat sekilas, mungkin kalian bertanya-tanya, “kok banyak chain yang sama?”. Memang banyak chain-chain yang sama seperti chain INPUT, FORWARD, OUTPUT, PREROUTING, POSTROUTING, dll. Akan tetapi yang sebenarnya melakukan tugas filtering paket hanyalah tabel Filter. Sedangkan tabel NAT dan Mangle hanya sebagai pelengkap saja. Tabel NAT dan MANGLE memang jarang digunakan pada Firewall sederhana yang hanya menggunakan satu buah LAN Ethernet Card saja. Namun karena Firewall umumnya diimplementasikan berbarengan dengan Router, maka penggunaan tabel NAT dan MANGLE ini tidak dapat kita hindari.

Memahami tabel Filter

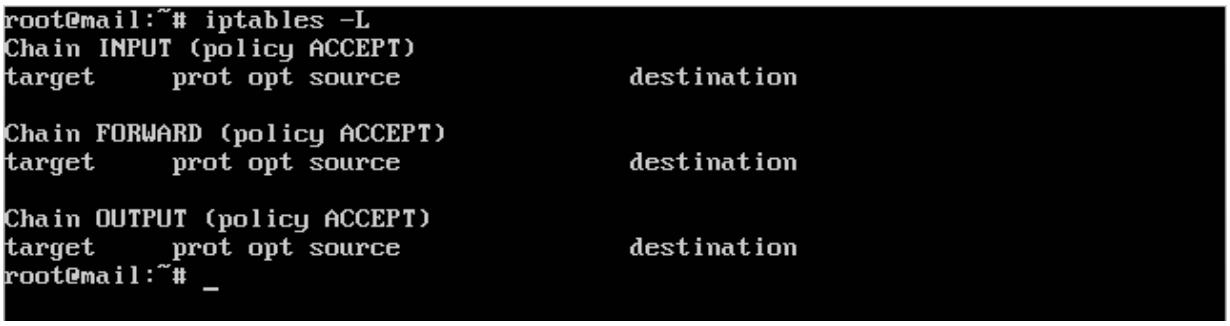
Tabel Filter akan saya bahas terlebih dahulu sebagai dasar pengimplementasian Firewall di Ubuntu Server 12.04 LTS, karena seperti yang sudah saya tuliskan sebelumnya, bahwa sebenarnya proses filterisasi pada Firewall itu ya terjadinya di tabel Filter ini. Oleh karena itu penting bagi kalian untuk memahami tabel Filter ini terlebih dahulu sebelum masuk ke proses Firewall yang lebih kompleks.

Secara default, 3 buah chain (INPUT, FORWARD, dan OUTPUT) pada tabel Filter menggunakan aturan ACCEPT. Dimana berarti seluruh paket akan diperbolehkan baik itu paket yang masuk (INPUT), diteruskan/dirouting (FORWARD), ataupun yang keluar (OUTPUT). Aturan ini biasa disebut dengan **Policy**. Kebalikan dari Policy ACCEPT adalah DROP. Dimana kebalikan dari Policy ACCEPT yaitu seluruh paket akan ditolak baik itu paket yang masuk (INPUT), diteruskan/dirouting (FORWARD), ataupun yang keluar (OUTPUT). Untuk melihat informasi Iptables ini, pertama kalian harus masuk terlebih dahulu kedalam mode **root** :

```
sudo -i
```

Setelah itu ketikkan perintah berikut :

```
iptables -L
```



Gambar 4.4.2

Pada dasarnya, ada 4 buah jenis Policy yang dapat diterapkan, yaitu :

- ACCEPT, menerima paket
- DROP, membuang paket
- QUEUE, memasukkan paket ke antrian
- RETURN, menghentikan atau keluar dari pemrosesan pada suatu *chain rules* dan kembali ke *chain rules* utama.

Walaupun ada 4 Policy, untuk INPUT, FORWARD, dan OUTPUT hanya bisa memakai 2 buah

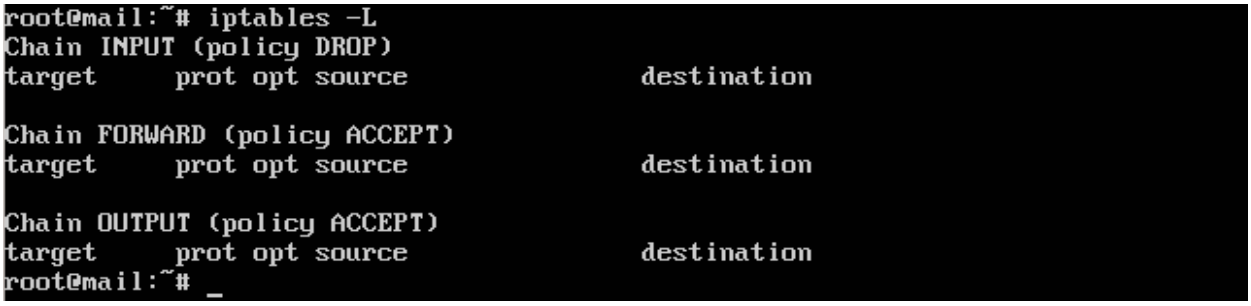
Policy. Yaitu ACCEPT dan DROP saja. Untuk mengubah Policy, gunakan perintah berikut :

```
iptables -P [chain] [policy]
```

Sebagai contoh saya ingin mengubah Policy chain INPUT menjadi DROP :

```
iptables -P INPUT DROP
```

Lihat hasilnya dengan perintah **iptables -L** :

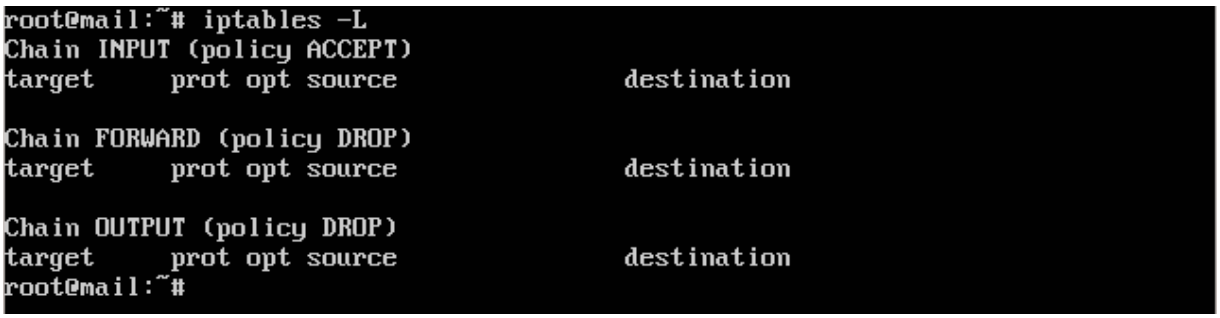


Gambar 4.4.3

Contoh lain, saya ingin mengembalikan chain INPUT menjadi ACCEPT dan merubah chain lainnya menjadi DROP :

```
iptables -P INPUT ACCEPT
iptables -P FORWARD DROP
iptables -P OUTPUT DROP
```

Lihat lagi hasilnya :



Gambar 4.4.4

Cobalah untuk merubah-rubah *Policy* diatas kemudian tes hasilnya dari komputer klien dengan menggunakan berbagai utilitas seperti **ping**, **ssh**, **nmap**, ataupun **telnet**. Sebagai contoh, jika kalian membuat *Policy chain* **INPUT** menjadi **DROP** maka bisa dipastikan kalian tidak akan bisa melakukan **ping**, **ssh**, **telnet**, atau apapun terhadap si Firewall.

Sebenarnya dengan melakukan Policy ACCEPT dan DROP ini merupakan sesuatu yang sangat ekstrim. Karena Policy tersebut akan melakukan tugasnya tanpa pandang bulu. Misalnya saja jika kalian menerapkan Policy DROP pada chain INPUT, maka secara otomatis tidak akan ada satu paket pun yang bisa masuk ke dalam Firewall, *tanpa terkecuali*. Ini sangat berbahaya sekali. Bagaimana jika kita hanya ingin memblokir beberapa service tertentu saja, atau ingin memblokir beberapa ip address tertentu saja, sedangkan yang lainnya diperbolehkan? Untung saja Iptables memiliki kemampuan untuk hal tersebut. Jadi kita dapat melakukan penambahan rules atau aturan untuk masing-masing chain. Bagaimana cara untuk pengimplementasiannya akan kita bahas pada sub-bab – sub-bab berikut.

Implementasi Firewall – Melakukan bloking service tertentu

Fungsi dari Firewall yang sebenarnya adalah filterisasi. Jadi Firewall akan melakukan penyaringan paket-paket mana saja yang boleh masuk, diteruskan, atau keluar dari jaringan. Nah, salah satu pengimplementasian filterisasi ini adalah dengan membuat rule-rule untuk memfilter service-service tertentu yang boleh keluar masuk jaringan. Contohnya misal kita akan memblok semua akses jaringan masuk dan keluar (INPUT dan OUTPUT) kecuali service HTTP. Atau sebaliknya, kita ingin memperbolehkan semua paket jaringan masuk dan keluar (INPUT dan OUTPUT) kecuali paket HTTP. Dan sebagainya.

Rumus untuk menentukan rule tambahan adalah sebagai berikut :

```
iptables –A [chain] –j [policy] [opsi lain]
```

Contoh pada kasus diatas, misal kita hanya ingin memblok akses masuk dan keluar paket HTTP yang bekerja di port 80 yang menggunakan protokol TCP, konfigurasinya adalah seperti ini :

```
iptables –A INPUT –p tcp --dport 80 –j DROP
iptables –A OUTPUT –p tcp --sport 80 –j DROP
```

Namun sebelum kita menentukan rule-rule tambahan tersebut, kita harus memutuskan apakah *Policy* yang digunakan bersifat terbuka seluruhnya (ACCEPT) atau tertutup seluruhnya (DROP). Jika kita memilih untuk membuka seluruhnya (ACCEPT), maka kita harus membuat rule-rule tambahan apa-apa saja yang ingin ditutup atau diblok. Sebaliknya, apabila kita ingin menutup seluruhnya (DROP), rule-rule tambahan yang harus kita buat adalah apa-apa saja yang ingin kita buka/perbolehkan.

Misal pada kasus kali ini kita ingin membuat seluruh akses masuk dan keluar (INPUT dan OUTPUT) tertutup seluruhnya, tetapi untuk akses HTTP (Web) dan SSH kita perbolehkan masuk

dan keluar. Konfigurasinya adalah sebagai berikut :

- Pertama-tama masuklah kedalam mode root terlebih dahulu :

```
sudo -i
```

- Hapus semua rule tambahan yang mungkin sebelumnya sudah pernah dibuat :

```
iptables -F
```

- Setelah itu buatlah Policy chain INPUT dan OUTPUT menjadi DROP :

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP
```

- Lalu buatlah rule tambahan yang mengijinkan paket HTTP yang bekerja pada port 80 dan SSH yang bekerja pada port 22 yang menggunakan protokol TCP :

```
iptables -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 80 -j ACCEPT
iptables -A INPUT -p tcp --dport 22 -j ACCEPT
iptables -A OUTPUT -p tcp --sport 22 -j ACCEPT
```

- Cobalah cek hasilnya dengan menggunakan perintah ini :

```
iptables -L
```

```
root@mail:~# iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:http
ACCEPT     tcp  --  anywhere             anywhere            tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:http
ACCEPT     tcp  --  anywhere             anywhere            tcp spt:ssh
root@mail:~#
```

Gambar 4.4.5

Sekarang cobalah tes menggunakan komputer lain untuk memastikan apakah benar bahwa hanya dua buah service tersebut saja yang diperbolehkan. Kalian bisa mengetesnya dengan menggunakan aplikasi port scanning seperti nmap atau mengetes secara langsung menggunakan web browser atau putty.

Untuk contoh konfigurasi lainnya kalian dapat melakukan eksperimen sendiri karena memang

kombinasi perintah iptables sangatlah banyak sehingga tidak akan bisa kita bahas semuanya disini.

Implementasi Firewall – Melakukan blocking ip address tertentu

Selain melakukan blocking terhadap service-service atau port tertentu, kita juga dapat melakukan filterisasi terhadap ip address yang boleh mengakses atau tidak ke jaringan yang dilindungi oleh Firewall kita. Konfigurasi seperti ini lazim digunakan mengingat seringnya serangan-serangan yang dilancarkan ke dalam Firewall. Sehingga kita dapat melakukan blocking terhadap ip address – ip address yang sering melakukan serangan terhadap Firewall kita.

Rumus untuk menentukan rule tambahan untuk memblock ip address tertentu ini hampir mirip dengan cara melakukan blocking service tertentu yang telah dibahas di sub bab sebelumnya. Namun disini ada 2 parameter yang baru yaitu opsi **-s** yang mendeskripsikan ip address sumber, dan opsi **-d** yang mendeskripsikan ip address tujuan. Untuk lebih memahaminya, mari kita praktekkan langsung saja dengan contoh berikut.

Misal kalian ingin memperbolehkan semua akses jaringan baik itu yang masuk maupun keluar. Namun kalian ingin membatasi akses SSH hanya boleh diakses dari internet oleh ip address 10.0.4.1, sedangkan jika dari jaringan lokal semua boleh mengaksesnya. Maka konfigurasinya adalah sebagai berikut :

- Seperti biasa, pertama-tama masuklah kedalam mode root terlebih dahulu :

  ```
  sudo –i
  ```

- Hapus semua rule tambahan yang mungkin sebelumnya sudah pernah dibuat :

  ```
  iptables –F
  ```

- Setelah itu buatlah Policy chain INPUT dan OUTPUT menjadi ACCEPT :

  ```
  iptables –P INPUT ACCEPT
  iptables –P OUTPUT ACCEPT
  ```

- Lalu buatlah rule tambahan untuk memperbolehkan satu ip saja yaitu ip address 10.0.4.1 yang boleh mengakses SSH dari internet yang melalui interface **eth0** :

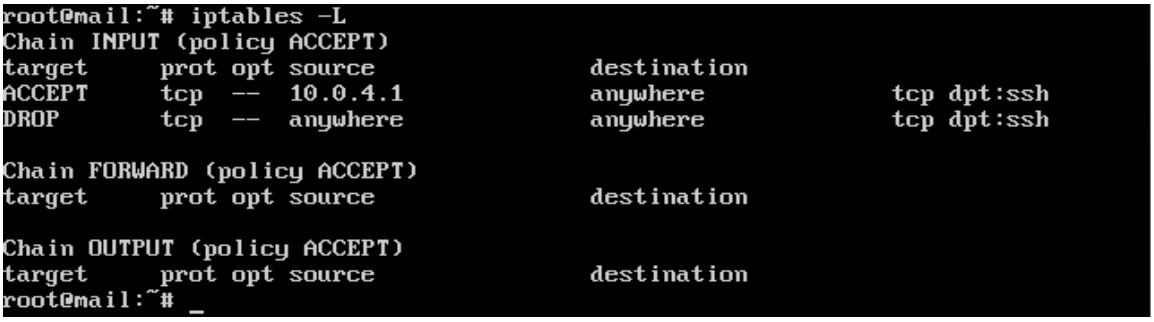
  ```
  iptables –A INPUT –i eth0 –p tcp –s 10.0.4.1 --dport 22 –j ACCEPT
  ```

- Kemudian buat lagi rule yang memblok semua akses SSH dari internet :

  ```
  iptables –A INPUT –i eth0 –p tcp --dport 22 –j DROP
  ```

- Cobalah cek hasilnya dengan menggunakan perintah ini :

```
iptables -L
```



Gambar 4.4.6

Bagaimana? Sudah mulai pahamkah kalian dengan cara kerja iptables setelah berlatih menggunakan contoh-contoh diatas? Oke, kita coba contoh lain dengan menggabungkan teknik bloking service tertentu dan bloking ip address tertentu. Misalnya saya ingin membuat rule-rule sebagai berikut :

1. Semua akses masuk, routing, dan keluar Firewall diperbolehkan.
2. Semua akses web keluar dari jaringan lokal menuju situs porno xxx.com yang mempunyai ip address 100.100.100.1 tidak diijinkan
3. Semua akses Telnet tidak diijinkan baik itu dari dalam jaringan lokal maupun dari jaringan internet.
4. Semua akses web ke Webserver yang berada pada komputer Server dengan ip address 192.168.1.1 tidak diijinkan. Ingat, letak mesin maupun ip address dari komputer Server dengan komputer Router berbeda, jika kalian lupa, kalian bisa melihat gambar topologinya pada awal bab Instalasi dan Konfigurasi Aplikasi Router Ubuntu Server 12.04 LTS. (disini kalian akan mempelajari perbedaan chain INPUT dengan FORWARD).
5. Semua akses masuk ICMP *echo requests* dari internet ke Firewall tidak diijinkan.

Dengan ketentuan rule diatas, kita akan coba melakukan konfigurasi sebagai berikut :

- Masuklah kedalam mode root :

```
sudo -i
```

- Hapus semua rule tambahan yang mungkin sebelumnya sudah pernah dibuat :

```
iptables -F
```

- Setelah itu buatlah Policy chain INPUT, FORWARD, dan OUTPUT menjadi ACCEPT :

```
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
```

- Buat rule tambahan untuk memblokir semua akses web dari jaringan lokal yang menuju situs xxx.com dengan ip address 100.100.100.1 :

```
iptables -A OUTPUT -p tcp -o eth0 --dport 80 -d 100.100.100.1 -j DROP
```

- Buat lagi rule tambahan untuk memblokir semua akses Telnet yang berada pada port 23 :

```
iptables -A INPUT -p tcp --dport 23 -j DROP
iptables -A OUTPUT -p tcp --sport 23 -j DROP
```

- Selanjutnya adalah membuat semua akses web yang bekerja pada port 80 menuju komputer Server yang memiliki ip address 192.168.1.1 ditolak :

```
iptables -A FORWARD -p tcp --dport 80 -d 192.168.1.1 -j DROP
```

- Dan terakhir membuat rule tambahan untuk memblokir semua akses ICMP echo requests dari Internet menuju Firewall tidak diijinkan :

```
iptables -A INPUT -i eth0 -p icmp --icmp-type echo-request -j DROP
```

- Sekarang amatilah hasilnya dengan menggunakan perintah berikut :

```
iptables -L
```

```
root@mail:~# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             anywhere            tcp dpt:telnet
DROP       icmp --  anywhere             anywhere            icmp echo-request

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             192.168.1.1         tcp dpt:http

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  anywhere             100.100.100.1       tcp dpt:http
DROP       tcp  --  anywhere             anywhere            tcp spt:telnet
root@mail:~# _
```

Gambar 4.4.7

Cobalah melakukan testing untuk memastikan bahwa Firewall memang benar-benar sudah berjalan. Seperti misalnya dengan mengakses situs xxx.com tadi, seharusnya situs tersebut tidak akan bisa terbuka karena ip addressnya memang sudah kalian blok. Coba juga untuk melakukan tes

menggunakan utilitas *ping* untuk memastikan bahwa Router/Firewall kalian memang sudah tidak bisa menerima permintaan ICMP *echo requests*. Dan lakukan juga proses testing-testing yang lain untuk memastikan bahwa semuanya memang sudah terkonfigurasi dengan baik.

Masih ada ribuan kemungkinan konfigurasi yang dapat dilakukan dengan aplikasi iptables ini. Dan ini sangat menarik untuk dicoba. Silahkan kalian kembangkan sendiri dengan melakukan berbagai eksperimen-eksperimen berdasarkan contoh konfigurasi dasar yang sudah saya jelaskan diatas.

Implementasi Firewall – Redirect DNS ke DNS Nawala

Sub bab ini saya masukkan ke dalam salah satu dari cara implementasi Firewall karena menurut saya konfigurasi ini sangat penting untuk kalian ketahui. Mungkin kalian ada yang bertanya apa maksud dari judul sub-bab ini. Sub-bab ini akan membahas teknik bagaimana caranya untuk mengalihkan seluruh alamat DNS yang digunakan oleh para klien ke alamat DNS milik Nawala. Nawala sendiri adalah sebuah proyek milik orang-orang Indonesia yang berfokus pada layanan DNS yang bebas digunakan oleh pengguna akhir atau penyedia jasa internet untuk mendapatkan akses internet bersih dan aman. DNS Nawala melakukan penapisan situs-situs berkandungan negatif yang tidak sesuai dengan norma kesusilaan dan budaya Indonesia, seperti situs berkandungan pornografi atau perjudian. Selain itu DNS Nawala juga menapis situs-situs yang berbahaya dan melanggar aturan perundangan, seperti situs penipuan, malware dan phising.

Pertama kali saya memikirkan teknik seperti ini berawal dari suatu kejadian yang pernah saya alami sendiri yaitu ketika suatu hari saya pernah iseng-iseng mencoba untuk membuka sebuah situs porno pada saat saya sedang terhubung ke sebuah hotspot yang ada di sebuah pusat perbelanjaan. Ketika saya buka, ternyata situs itu tidak dapat ditemukan oleh Browser dan muncul pesan error *server not found* yang berarti situs tersebut tidak terdaftar ke dalam DNS. Seperti yang kalian ketahui, fungsi dari sebuah DNS adalah mentranslasikan ip address menjadi domain dan sebaliknya, mentranslasikan domain menjadi ip address. Nah, ketika kita mengakses sebuah situs menggunakan nama domain dan ternyata situs tersebut tidak mau terbuka, maka bisa dipastikan berarti domain tersebut tidak terdaftar pada DNS server yang kalian gunakan.

Lalu bagaimanakah cara mengatasinya ? Ternyata caranya sangatlah mudah. Yaitu dengan mengganti alamat DNS yang kalian gunakan dengan alamat DNS milik Google yang beralamatkan ip address *8.8.8.8* dan *8.8.4.4*. Cara ini sangat ampuh karena memang DNS milik Google ini sama sekali tidak memblokir situs-situs apapun baik itu yang berunsur pornografi, judi, sara, dll.

Karena berdasarkan pengalaman saya diatas, saya tidak mau kalau suatu saat jika saya memiliki jaringan sendiri, akan dapat dibobol dengan mudah oleh trik sederhana seperti diatas. Akhirnya saya pun mendapatkan cara penanggulangannya dengan menggunakan teknik pengalihan seluruh akses

DNS ke DNS milik Nawala. Jadi ketika ada *user* yang mengganti DNS mereka dengan DNS Google atau OpenDNS atau semacamnya, mereka tetap saja akan dialihkan ke DNS Nawala. Sehingga trik tersebut tidak akan berfungsi lagi.

DNS Nawala memiliki 2 buah *nameserver address* yaitu **180.131.144.144** dan **180.131.145.145**. Untuk pengkonfigurasiannya adalah sebagai berikut :

- Masuk ke dalam mode user *root* terlebih dahulu :

```
sudo –i
```

- Kemudian eksekusi 4 perintah berikut untuk mengalihkan atau me-*redirect* seluruh akses DNS yang bekerja pada port 53 baik itu protokol TCP maupun UDP ke DNS Nawala yang memiliki ip address 180.131.144.144 dan 180.131.145.145 :

```
iptables –t nat –A PREROUTING –p tcp –m tcp --dport 53 –j DNAT
--to-destination 180.131.144.144:53
iptables –t nat –A PREROUTING –p udp –m udp --dport 53 –j DNAT
--to-destination 180.131.144.144:53
iptables –t nat –A PREROUTING –p tcp –m tcp --dport 53 –j DNAT
--to-destination 180.131.145.145:53
iptables –t nat –A PREROUTING –p udp –m udp --dport 53 –j DNAT
--to-destination 180.131.145.145:53
```

- Amati hasilnya dengan perintah berikut :

```
iptables –t nat –L
```

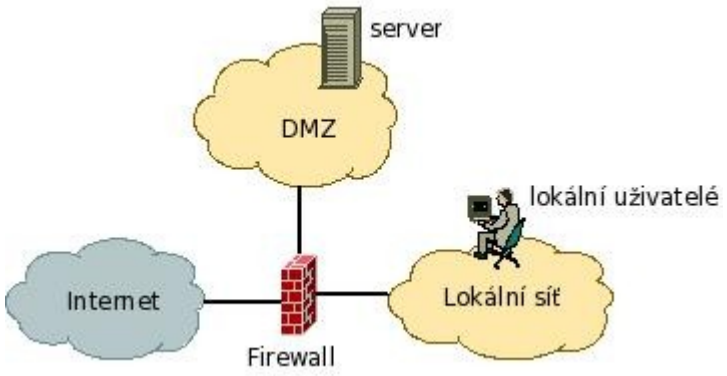
```
root@mail:~# iptables -t nat -L
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
REDIRECT   tcp  --  192.168.1.0/24       anywhere            tcp dpt:http redir
 ports 3128
DNAT       tcp  --  anywhere             anywhere            tcp dpt:domain to:
180.131.144.144:53
DNAT       udp  --  anywhere             anywhere            udp dpt:domain to:
180.131.144.144:53
DNAT       tcp  --  anywhere             anywhere            tcp dpt:domain to:
180.131.145.145:53
DNAT       udp  --  anywhere             anywhere            udp dpt:domain to:
180.131.145.145:53

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  anywhere             anywhere
root@mail:~#
```

Gambar 4.4.8

Sekarang cobalah mengetesnya dengan mengganti DNS komputer klien dengan DNS milik Google atau OpenDNS, lalu akseslah salah satu situs pornografi atau situs judi. Maka seharusnya situs tersebut tidak akan bisa terbuka dan menampilkan pesan error *server not found*.

Implementasi Firewall – Konfigurasi DMZ Area

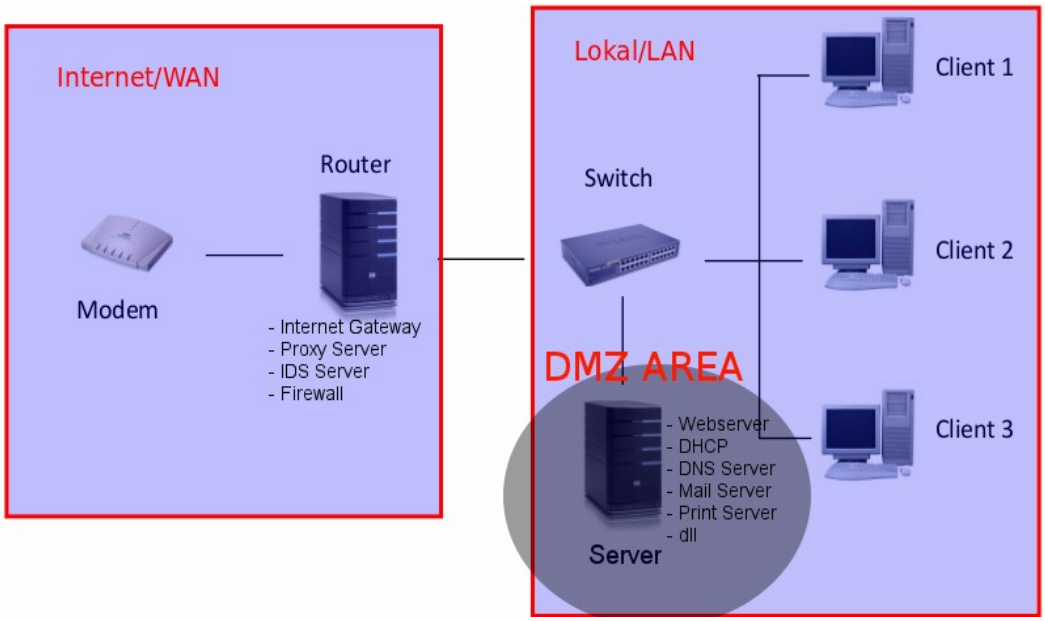
DMZ atau De-Militarized Zone adalah sebuah mekanisme untuk mengisolasi suatu jaringan untuk melindungi jaringan internal didalamnya dari serangan-serangan pihak yang tidak bertanggung jawab seperti *hacker* atau *cracker*. DMZ melakukan suatu perpindahan layanan dari suatu jaringan ke jaringan yang lain. Sehingga ketika ada cracker yang menyerang, ia hanya bisa menyerang sampai titik DMZ area itu tadi, dan tidak bisa sampai ke jaringan internal didalamnya. Untuk lebih jelasnya perhatikan gambar berikut :



Gambar 4.4.9

Bisa dilihat pada gambar diatas, jika kita telah membuat suatu area DMZ khusus, maka seluruh akses seseorang dari jaringan luar/internet tidak akan bisa masuk ke jaringan lokal. Tapi hanya *mentok* sampai *host* yang ada di area DMZ saja.

Salah satu contoh pengimplementasian dari DMZ yang sering saya lakukan adalah dengan menempatkan sebuah Server lokal dibelakang sebuah Firewall yang nantinya Server tersebut dapat diakses dari internet menggunakan ip publik milik si Firewall. Jadi mekanismenya dengan cara pengalihan layanan milik Firewall ke layanan milik si Server. Mungkin kalian sedikit bingung dengan pemahaman ini, oleh karena itu lebih baik langsung saja kita praktekkan agar kalian nantinya bisa mengerti dengan sendirinya.
Sekarang perhatikan terlebih dahulu topologi jaringan dibawah ini :



Gambar 4.4.10

Pada gambar diatas, posisi kita berada di komputer Router, dan yang ingin kita buat sebagai area DMZ adalah si komputer Server. Lalu kita tentukan terlebih dahulu ip address – ip addressnya berdasarkan konfigurasi-konfigurasi kita yang sebelumnya, yaitu ip address publik milik Router adalah 10.0.2.15 dan ip address lokal milik server adalah 192.168.1.1. Kemudian kita tentukan juga service-service yang akan dialihkan menggunakan metode DMZ ini, yaitu service HTTP, FTP, DNS, Mail & Webmail, serta Samba *File Sharing*. Kalian boleh bereksperimen dengan

menambahkan service-service yang lainnya jika kalian mau.

Setelah menentukan itu semua, barulah kita dapat memulai proses konfigurasinya. Caranya adalah sebagai berikut :

- Pertama-tama seperti biasa, masuklah ke dalam mode user *root* terlebih dahulu agar proses konfigurasi menjadi lebih efisien :

```
sudo –i
```

- Pada konfigurasi DMZ kali ini, saya ingin mengajak kalian mencoba menggunakan cara lain untuk membuat sebuah konfigurasi Firewall. Yaitu dengan menggunakan sebuah file *script*. Karena cara ini secara umum lebih banyak disukai dibandingkan dengan cara manual seperti konfigurasi-konfigurasi sebelumnya. Karena kalian cukup memasukkan semua perintah konfigurasi ke dalam sebuah file *script*, setelah selesai tinggal jalankan saja *script*nya. Nah, sekarang cobalah buat sebuah *script* baru bernama **iptables-dmz** dengan cara berikut :

```
nano iptables-dmz
```

- Setelah file tersebut terbuka, isikan didalamnya dengan seluruh perintah iptables yang diperlukan untuk membuat DMZ Area seperti berikut ini :

```
#!/bin/sh

#Memperbolehkan akses routing dan keluar jaringan
iptables –A FORWARD –m state --state NEW,ESTABLISHED,RELATED –j ACCEPT
iptables –A OUTPUT –m state --state NEW,ESTABLISHED,RELATED –j ACCEPT

# DMZ untuk DNS
iptables –A INPUT –p tcp –d 10.0.2.15 --dport 53 –j ACCEPT
iptables –A FORWARD –p tcp –d 192.168.1.1 --dport 53 –j ACCEPT
iptables –t nat –A PREROUTING –p tcp –d 10.0.2.15 --dport 53 –j DNAT --to
192.168.1.1:53

iptables –A INPUT –p udp –d 10.0.2.15 --dport 53 –j ACCEPT
iptables –A FORWARD –p udp –d 192.168.1.1 --dport 53 –j ACCEPT
iptables –t nat –A PREROUTING –p udp –d 10.0.2.15 --dport 53 –j DNAT --to
192.168.1.1:53
```

```
#DMZ untuk Webserver
iptables -A INPUT -p tcp -d 10.0.2.15 --dport 80 -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.1.1 --dport 80 -j ACCEPT
iptables -t nat -A PREROUTING -p tcp -d 10.0.2.15 --dport 80 -j DNAT --to
192.168.1.1:80

#DMZ untuk FTP
iptables -A INPUT -p tcp -d 10.0.2.15 --dport 21 -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.1.1 --dport 21 -j ACCEPT
iptables -t nat -A PREROUTING -p tcp -d 10.0.2.15 --dport 21 -j DNAT --to
192.168.1.1:21

#DMZ untuk FTP Passive
iptables -A INPUT -p tcp -m multiport -d 10.0.2.15 --dport 5000:5005 -j
ACCEPT
iptables -A FORWARD -p tcp -m multiport -d 192.168.1.1 --dport 5000:5005
-j ACCEPT
iptables -t nat -A PREROUTING -p tcp -m multiport -d 10.0.2.15 --dport
5000:5005 -j DNAT --to 192.168.1.1

#DMZ untuk Mail & Webmail
iptables -A INPUT -p tcp -m multiport -d 10.0.2.15 --dport 80,25,110,143
-j ACCEPT
iptables -A FORWARD -p tcp -m multiport -d 192.168.1.1 --dport
80,25,110,143 -j ACCEPT
iptables -t nat -A PREROUTING -p tcp -m multiport -d 10.0.2.15 --dport
80,25,110,143 -j DNAT --to 192.168.1.1

#DMZ untuk Samba
iptables -A INPUT -p udp -m multiport -d 10.0.2.15 --dport 137:139 -j
ACCEPT
iptables -A FORWARD -p udp -m multiport -d 192.168.1.1 --dport 137:139 -j
ACCEPT
iptables -t nat -A PREROUTING -p tcp -m multiport -d 10.0.2.15 --dport
137:139 -j DNAT --to 192.168.1.1
```

```
exit 0
```

- Simpanlah file tersebut dengan menekan **CTRL + X** > **Y** > **Enter**, lalu berilah hak akses *executable* agar file tersebut bisa dieksekusi dengan cara berikut :

  ```
  chmod +x iptables-dmz
  ```

- Sekarang jalankan script tersebut dengan perintah ini :

  ```
  ./iptables-dmz
  ```

Untuk mengetesnya, kalian dapat mengakses masing-masing *service* yang telah di-*DMZ* kan dengan cara membuka tiap-tiap *service* menggunakan ip publik milik Router, bukan lagi menggunakan ip lokal milik Server. Sebagai contoh kalian dapat membuka *service* HTTP melalui browser dan akseslah alamat http://10.0.2.15, maka nanti akan tampil halaman web yang telah kalian buat di komputer Server yang beralamatkan 192.168.1.1. Sama halnya dengan FTP, DNS, Mail maupun Samba. Kalian dapat mengakses FTP melalui browser dengan membuka alamat ftp://10.0.2.15, membuka webmail dengan membuka alamat http://10.0.2.15/roundcube, dan sebagainya. Nanti yang terbuka oleh kalian adalah *service-service* yang berada di komputer Server semua.
Jika belum dikonfigurasi DMZ seperti tadi, maka hal ini tidak akan mungkin terjadi karena seharusnya di komputer Router memang tidak memiliki *service-service* seperti Webserver, FTP, DNS, Mail, ataupun Samba. Jadi intinya DMZ akan mengalihkan layanan-layanan yang telah diatur sesuai rule-rule tertentu. Dengan kondisi seperti ini, para Hacker yang menyerang akan terkecoh karena mereka mengira sedang mengakses IP Publik si komputer Router, padahal sebenarnya mereka sudah dialihkan ke komputer Server.
Diatas adalah contoh kecil pengimplementasian DMZ Area dengan menggunakan iptables. Sebenarnya masih ada banyak sekali kombinasi-kombinasi yang dapat kita eksplor untuk membuat DMZ Area ini, namun sangat tidak memungkinkan untuk dibahas semuanya di buku ini.

Menyimpan konfigurasi Firewall

Setelah kalian melakukan berbagai konfigurasi iptables, perlu kalian ketahui juga bahwa konfigurasi-konfigurasi tersebut hanya bersifat sementara. Jadi ketika komputer kalian matikan, maka seluruh konfigurasi yang telah kalian buat akan hilang. Oleh karena itu kita perlu untuk menyimpan konfigurasi tersebut.
Pada bab *Routing NAT/MASQUERADING*, kalian telah diajarkan bagaimana cara menyimpan

konfigurasi dari iptables dengan cara mennyimpan konfigurasinya pada file **/etc/network/iptables.conf**. Nah, untuk praktek cara menyimpan konfigurasi Firewall kali ini , prosesnya sama saja dengan cara menyimpan konfigurasi pada bab *Routing NAT/MASQUERADING* tersebut. Namun bedanya, karena file-file yang dibutuhkan untuk keperluan penyimpanan seperti file **/etc/network/iptables.conf** dan file **/etc/network/if-up.d/iptables** sudah dibuat, maka sekarang kalian tidak perlu repot-repot lagi untuk membuat file-file tersebut. Tinggal eksekusi saja perintah dibawah ini untuk menyimpan konfigurasi dari Firewall :

```
iptables-save > /etc/network/iptables.conf
```

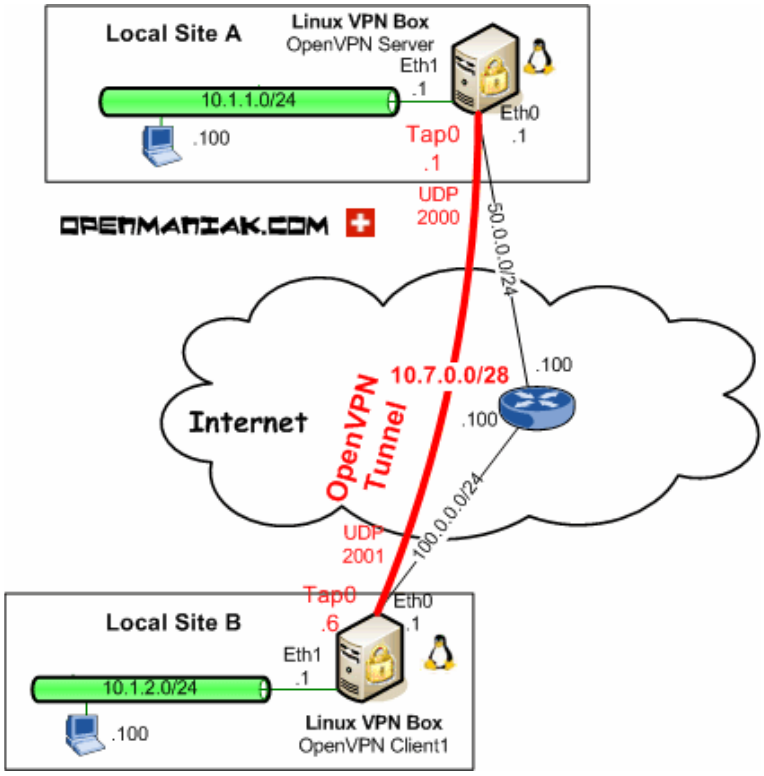
Sekarang seluruh konfigurasi Firewall kalian telah disimpan dan tidak akan hilang lagi ketika komputer direstart.

4.5. Instalasi VPN Server

Apa itu VPN ?

VPN, atau singkatan dari *Virtual Private Network*, merupakan sebuah teknik dimana kalian dapat mengakses jaringan lokal melalui Internet dengan teknologi *tunneling*. Ini merupakan solusi mudah koneksi *private* melalui jaringan publik pada masa mobilitas tinggi seperti saat ini. Koneksi dari VPN itu sendiri bersifat *virtual*. Mengapa disebut demikian ? Karena pada dasarnya jaringan ini tidak ada secara fisik, ia hanya berupa jaringan virtual saja. Dan mengapa disebut *private* karena jaringan ini memang merupakan jaringan yang sifatnya pribadi yang tidak semua orang bisa mengaksesnya.

Sekarang coba perhatikan gambar berikut :



Gambar 4.5.1

Pada gambar tersebut terlihat ada dua buah jaringan lokal bernama **Local Site A** dan **Local Site B**. Normalnya, kedua jaringan lokal tersebut tidak akan bisa saling terhubung walaupun mereka sama-sama terkoneksi ke internet. Tapi coba lihat jika kita menggunakan teknik VPN, jaringan-jaringan ini akan membentuk sebuah jalur baru (tunnel) sehingga mereka dapat terhubung satu sama lain. Dari situ mereka dapat melakukan apa saja seperti transfer data, browsing internet, berbagi pakai printer dan sebagainya, selayaknya berada di jaringan lokal sendiri. Kira-kira ya beginilah yang disebut apa VPN itu.

Keuntungan-keuntungan menggunakan VPN antara lain :

1. *Confidentiality (Kerahasiaan)*

   Teknologi VPN memiliki sistem kerja mengenkripsi semua data yang lewat melaluinya. Dengan adanya teknologi enkripsi ini, maka kerahasiaan Kalian menjadi lebih terjaga. Biarpun ada pihak yang dapat menyadap data Kalian yang lalu-lalang, namun belum tentu mereka bisa membacanya dengan mudah karena memang sudah diacak. Dengan menerapkan sistem enkripsi ini, tidak ada satupun orang yang dapat mengakses dan membaca isi jaringan data Kalian dengan mudah.

2. *Data Integrity (Keutuhan Data)*

Ketika melewati jaringan Internet, data Kalian sebenarnya sudah berjalan sangat jauh melintasi berbagai negara. Di tengah perjalanannya, apapun bisa terjadi terhadap isinya. Baik itu hilang, rusak, bahkan dimanipulasi isinya oleh orang-orang iseng. VPN memiliki teknologi yang dapat menjaga keutuhan data yang Kalian kirim agar sampai ke tujuannya tanpa cacat, hilang, rusak, ataupun dimanipulasi oleh orang lain.

3. *Origin Authentication (Autentikasi Sumber)*
   Teknologi VPN memiliki kemampuan untuk melakukan autentikasi terhadap sumber-sumber pengirim data yang akan diterimanya. VPN akan melakukan pemeriksaan terhadap semua data yang masuk dan mengambil informasi source datanya. Kemudian alamat source data ini akan disetujui jika proses autentikasinya berhasil. Dengan demikian, VPN menjamin semua data yang dikirim dan diterima oleh Kalian berasal dari sumber yang semestinya. Tidak ada data yang dipalsukan atau dikirimkan oleh pihak-pihak lain.

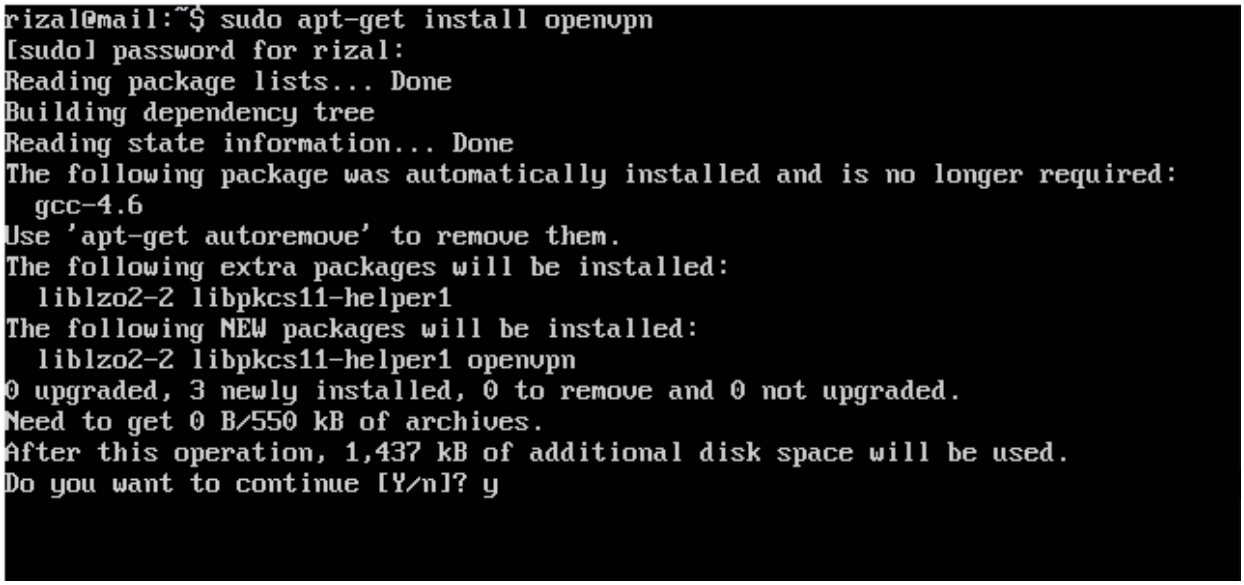
Instalasi OpenVPN

Untuk membuat sebuah VPN Server, sebenarnya ada beberapa aplikasi yang dapat kalian pilih. Salah satunya adalah OpenVPN. OpenVPN saya pilih karena dirasa memiliki lebih banyak keunggulan dibandingkan dengan aplikasi-aplikasi sejenis. Diantara keunggulan tersebut adalah kita dapat melakukan *anonymous surfing*. Jadi ketika kita surfing di internet, IP Address asli kita sama sekali tidak akan terbaca karena kita sebenarnya sedang menggunakan IP Publik si VPN Server. Sehingga tentunya kita sangat aman dari serangan para *sniffers* maupun *hacker* yang berniat untuk mencuri data-data kita. Selain itu OpenVPN ini sangat mudah dikonfigurasi dan gratis untuk digunakan juga.

Untuk menginstall OpenVPN di Ubuntu Server 12.04 LTS ikuti langkah-langkah berikut :

- Pertama-tama seperti biasa, gunakan perintah apt-get untuk menginstall aplikasi di Ubuntu Server :

```
sudo apt-get install openvpn
```

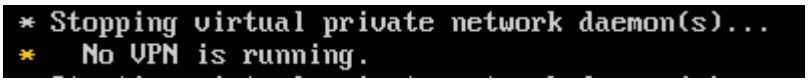


Gambar 4.5.2

- Apabila selama proses instalasi berlangsung terdapat kesalahan, jalankan saja perintah berikut untuk mengatasinya :

```
sudo apt-get -f install && sudo apt-get install openvpn
```

- Pada akhir proses instalasi OpenVPN terlihat adanya pesan error yang menyatakan service OpenVPN belum berjalan. Abaikan saja pesan tersebut karena memang OpenVPN tidak akan bisa berjalan pada awalnya sebelum di konfigurasi terlebih dahulu.



Gambar 4.5.3

Konfigurasi Server OpenVPN

Langkah-langkah konfigurasi OpenVPN lumayan panjang, oleh karena itu disini akan saya bagi menjadi 2 bagian konfigurasi, yaitu Konfigurasi Server OpenVPN dan Konfigurasi Client OpenVPN.

Untuk konfigurasi Server, mari kita coba praktekkan dengan langkah-langkah berikut ini :

- Perlu kalian ketahui, letak file konfigurasi awal OpenVPN bukanlah berada di direktori /etc seperti kebanyakan aplikasi-aplikasi lainnya. Memang, direktori utama OpenVPN berada di /etc/openvpn. Namun pada saat awal instalasi seperti ini, direktori tersebut masih belum ada isinya. Oleh karena itu kita akan memindahkan file-file konfigurasi yang dibutuhkan

OpenVPN ke direktori utamanya yaitu di /etc/openvpn. Caranya adalah sebagai berikut :

```
sudo cp -R /usr/share/doc/openvpn/examples/easy-rsa/2.0/ /etc/openvpn/
sudo cp -R /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz /etc/openvpn/
```

- Setelah itu, masuklah ke dalam direktori **/etc/openvpn/easy-rsa/2.0/** dengan mengeksekusi perintah ini :

```
cd /etc/openvpn/2.0/
```

- Kemudian editlah file **vars** untuk mengganti *variable* dan data-data pribadi yang diperlukan :

```
sudo nano vars
```

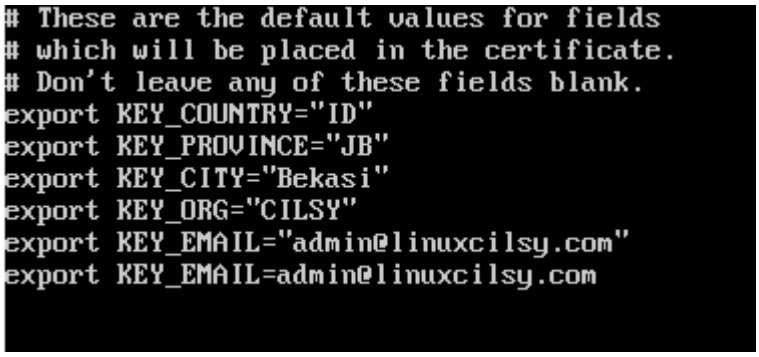
- Turunlah ke baris paling bawah file tersebut hingga kalian menemukan baris-baris konfigurasi ini :

```
export KEY_COUNTRY="US"
export KEY_PROVINCE="CA"
export KEY_CITY="SanFrancisco"
export KEY_ORG="Fort-Funston"
export KEY_EMAIL="me@myhost.mydomain"
export KEY_EMAIL=mail@host.domain
export KEY_CN=changeme
export KEY_NAME=changeme
export KEY_OU=changeme
export PKCS11_MODULE_PATH=changeme
export PKCS11_PIN=1234
```

Gambar 4.5.4

- Hapuslah baris-baris yang tidak diperlukan seperti **KEY_CN**, **KEY_NAME**, **KEY_OU**, **PKCS11_MODULE_PATH**, dan **PKCS11_PIN**, kemudian gantilah baris-baris yang ada didalam tanda kutip (**"..."**) sesuai dengan data kalian masing-masing, sehingga menjadi seperti ini :

```
export KEY_COUNTRY="ID"
export KEY_PROVINCE="JB"
export KEY_CITY="Bekasi"
export KEY_ORG="CILSY"
export KEY_EMAIL="admin@linuxcilsy.com"
export KEY_EMAIL=admin@linuxcilsy.com
```



Gambar 4.5.5

- Simpan dan tutup filenya dengan menekan kombinasi **CTRL + X** > **Y** > **Enter**.

- Selanjutnya kalian harus merename file bernama **openssl-1.0.0.cnf** menjadi **openssl.cnf** agar proses instalasi dapat dilanjutkan :

```
sudo mv /etc/openvpn/2.0/openssl-1.0.0.cnf /etc/openvpn/2.0/openssl.cnf
```

- Kemudian lakukan perintah-perintah berikut ini secara berurutan untuk membuat sertifikat autoritas, serta sertifikat dan key untuk Server dan Client

```
cd /etc/openvpn/2.0
sudo su
source vars
./clean-all
./build-dh
./pkitool --initca
./pkitool --server server
./pkitool client
```

Gambar 4.5.6

- Langkah selanjutnya adalah mengkopikan file-file kunci dan sertifikat untuk server yang telah kalian buat barusan ke direktori **/etc/openvpn** :

```
cp keys/server.key /etc/openvpn
cp keys/server.crt /etc/openvpn
cp keys/ca.crt /etc/openvpn
cp keys/dh1024.pem /etc/openvpn
```

- Lalu kopikan juga file-file kunci dan sertifikat yang diperlukan untuk komputer client ke home folder milik salah satu user. Misal disini nama user saya adalah **rizal**, maka perintahnya adalah seperti ini :

```
cp keys/client.key /home/rizal
```

```
cp keys/client.crt /home/rizal
cp keys/ca.crt /home/rizal
```

- Jangan lupa berikan juga hak akses kepemilikan agar user **rizal** memiliki akses penuh terhadap direktori **/home/rizal** :

```
chmod –R 777 /home/rizal
```

- Setelah semua langkah diatas sudah kalian lakukan, sekarang saatnya untuk melakukan satu konfigurasi lagi. Yaitu dengan mengedit file **/etc/openvpn/server.conf**. Ketikkan perintah berikut untuk pindah ke direktori **/etc/openvpn** :

```
cd ..
```

- Kemudian ekstraklah file bernama **server.conf.gz** dengan perintah ini :

```
gunzip server.conf.gz
```

- Apabila sudah, sekarang edit file tersebut dengan mengeksekusi perintah berikut :

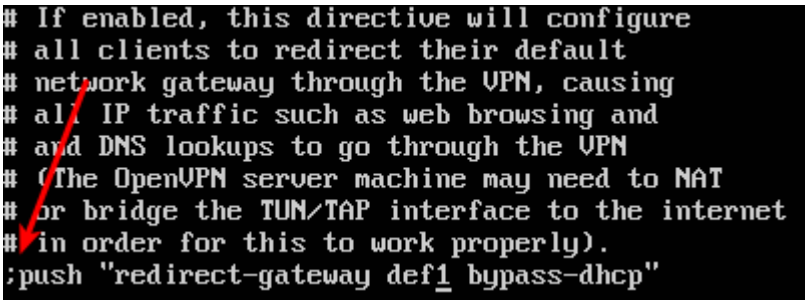
```
nano server.conf
```

- Setelah filenya terbuka, tekanlah tombol **CTRL + W** untuk melakukan pencarian kata kunci **def1** sehingga kalian akan menemukan baris seperti ini :

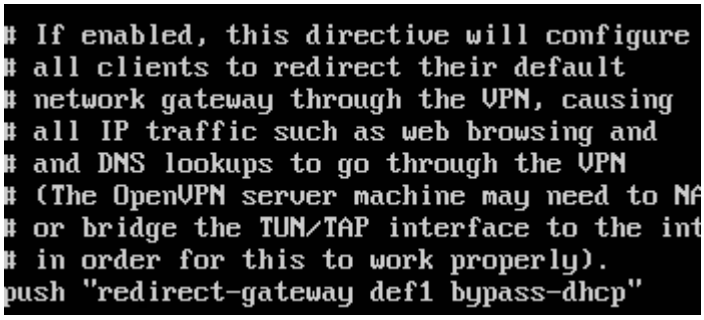
```
;push "redirect-gateway def1 bypass-dhcp"
```

- Sekarang hapuslah tanda titik koma (;) yang ada di depan baris tersebut sehingga tinggal menjadi seperti ini :

```
push "redirect-gateway def1 bypass-dhcp"
```



Gambar 4.5.8



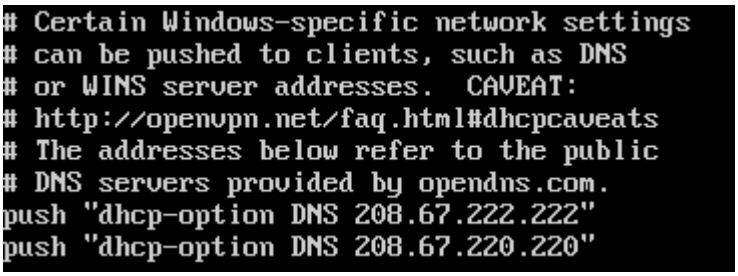
Gambar 4.5.9

- Lakukan pula hal yang sama pada baris-baris berikut yang tidak jauh berada dibawah baris **;push "redirect-gateway def1 bypass-dhcp"** diatas. Baris ini :

  ```
  ;push "dhcp-option DNS 208.67.222.222"
  ;push "dhcp-option DNS 208.67.220.220"
  ```

  Menjadi :

  ```
  push "dhcp-option DNS 208.67.222.222"
  push "dhcp-option DNS 208.67.220.220"
  ```



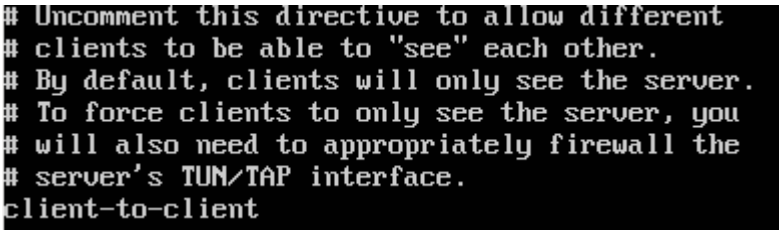
Gambar 4.5.10

Baris ini :

```
;client-to-client
```

Menjadi :

```
client-to-client
```



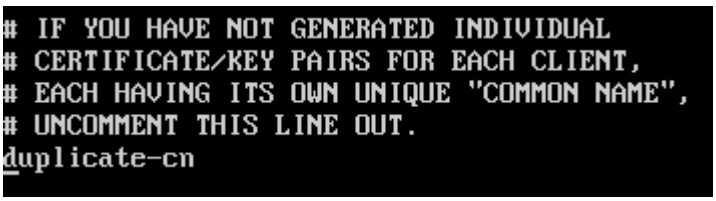
Gambar 4.5.11

Dan baris ini :

```
;duplicate-cn
```

Menjadi :

```
duplicate-cn
```



Gambar 4.5.12

Jika sudah, simpanlah file tersebut dengan menekan tombol kombinasi **CTRL +X > Y > Enter**.

- Terakhir restartlah service dari openvpn dengan perintah berikut ini :

  ```
  service openvpn restart
  ```

Konfigurasi Client OpenVPN

Selain harus melakukan instalasi dan konfigurasi di sisi server, kalian juga perlu melakukan sedikit instalasi dan konfigurasi di sisi client agar sang client dapat terkoneksi dengan baik ke server VPN yang telah kalian buat.

Oh iya, sebagai catatan, client yang saya gunakan pada buku ini adalah client yang menggunakan OS Windows 7.

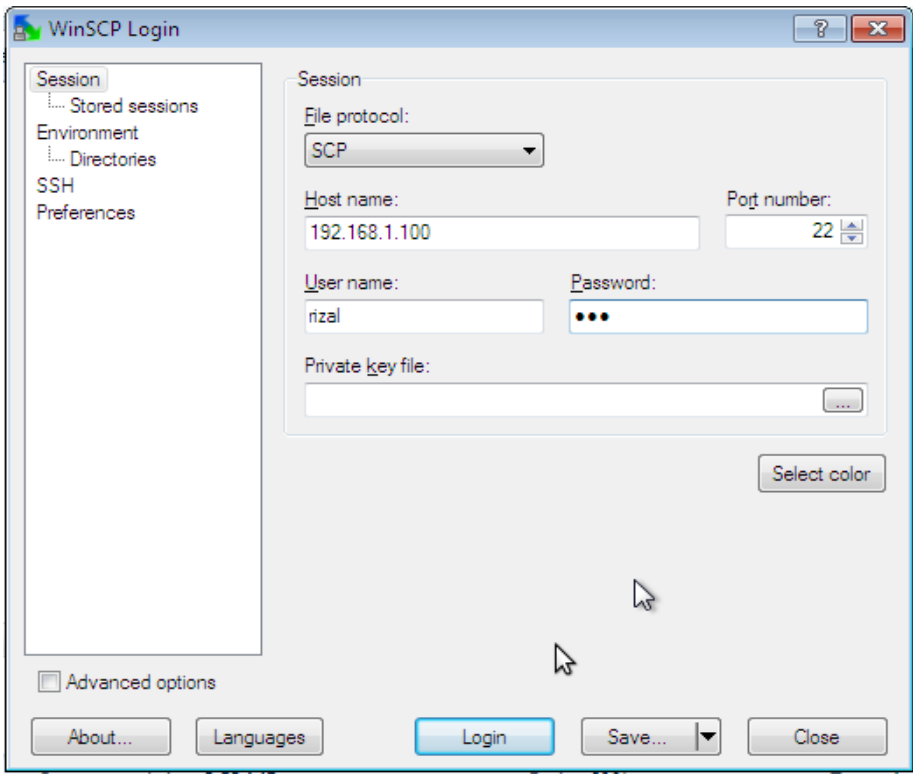
- Hal pertama yang harus kalian persiapkan adalah, beberapa tools software seperti *winscp* untuk mengambil file-file sertifikat dan otorisasi dari server, dan juga aplikasi *OpenvpnGUI* sebagai alat untuk pengkoneksian client.

  Kalian dapat mengunduh software-software tersebut disini :

  - Winscp : http://winscp.net/download/winscp512.zip
  - OpenvpnGUI : http://swupdate.openvpn.org/community/releases/openvpn-2.2.2-install.exe

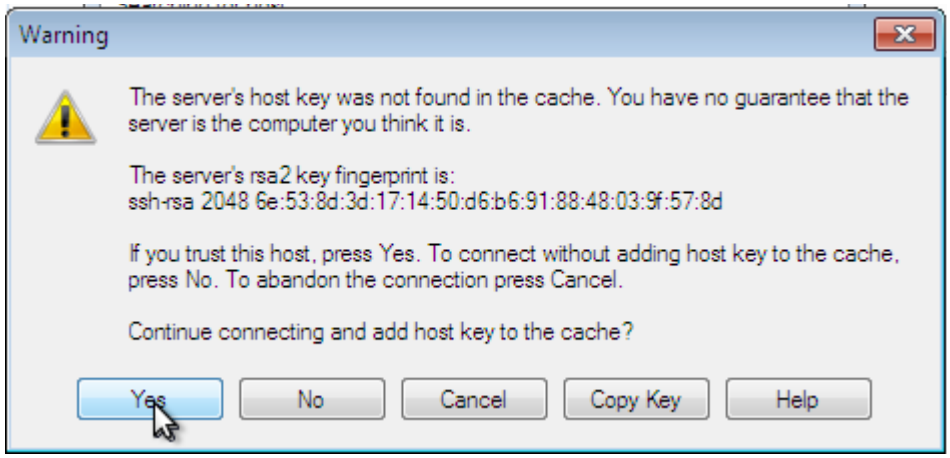
- Setelah kalian mendownload kedua software tersebut, sekarang ekstrak dan bukalah software winscpnya terlebih dahulu. Untuk dapat login ke dalam server, pilihlah **SCP** pada menu **File Protocol**, masukkan IP Address server kalian pada bagian **Hostname**, lalu isikan juga **username** dan **password** yang biasa kalian gunakan ketika kalian login ke dalam

server (dalam kasus ini, saya memasukkan *rizal* sebagai usernamenya), kemudian klik **Login**.



Gambar 4.5.12

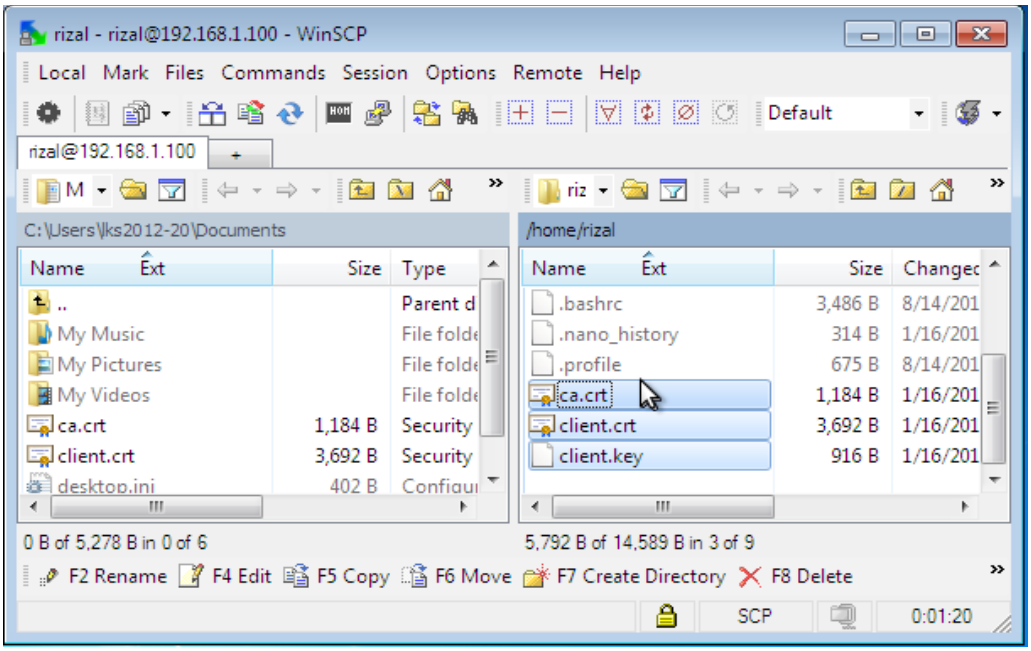
- Klik **Yes** jika muncul pertanyaan untuk menambahkan *Add Host Key* seperti ini. Itu artinya service SCP yang berjalan sedang menambahkan kedua komputer baik Server maupun Client sebagai komputer yang terpercaya.



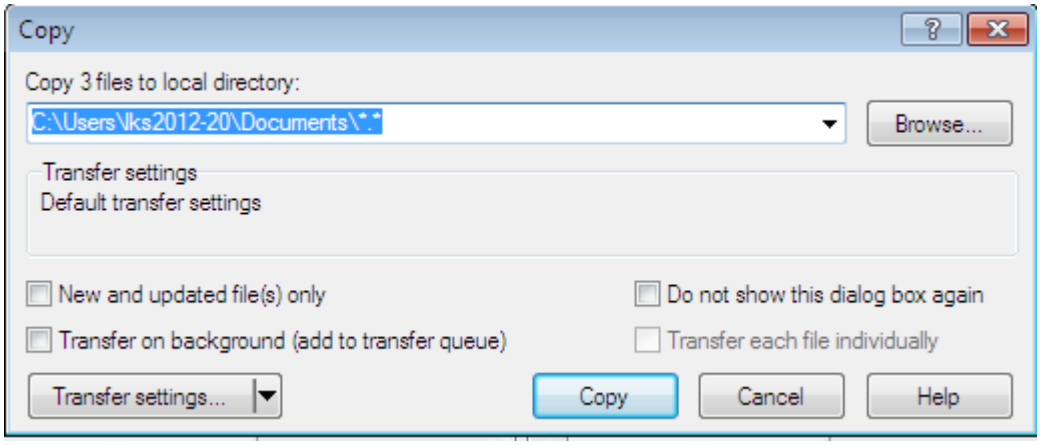
Gambar 4.5.13

- Jika kalian berhasil login, maka akan muncul tampilan seperti ini. Pada tab bagian kiri, itu merupakan direktori aktif milik client, sedangkan pada tab bagian kanan, merupakan

direktori aktif milik Server. Sekarang kalian tinggal *drag* dan *drop* saja 3 file bernama **ca.crt**, **client.crt**, dan **client.key** dari tab bagian kanan ke tab bagian kiri seperti yang tampak pada gambar dibawah :



Gambar 4.5.14

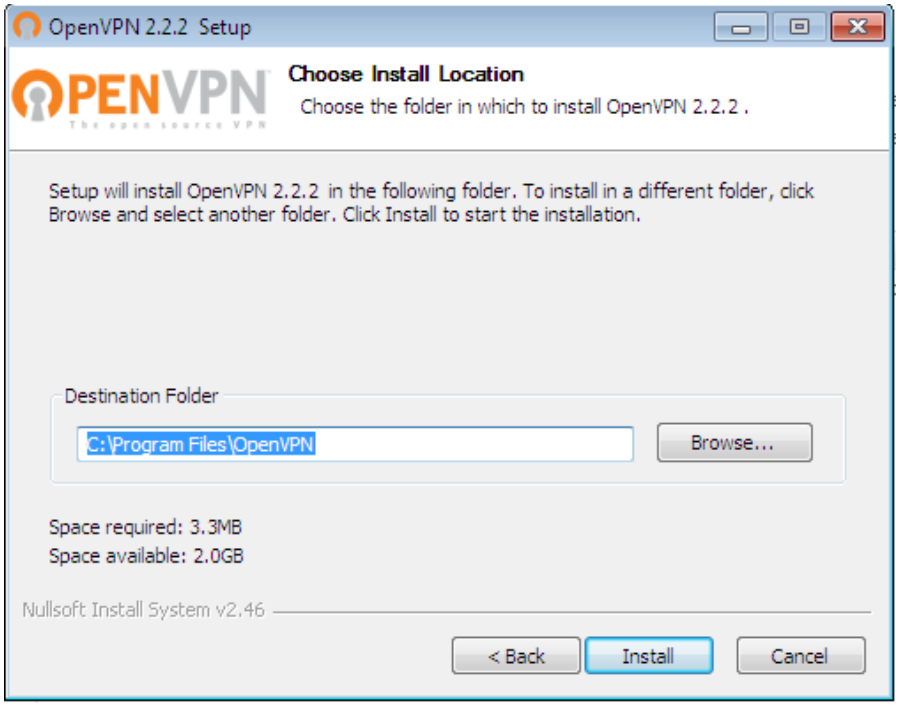


Gambar 4.5.15

- Jika proses pengkopian sudah selesai, sementara biarkan saja terlebih dahulu ketiga file tersebut. Karena file-file itu akan kita gunakan nanti.

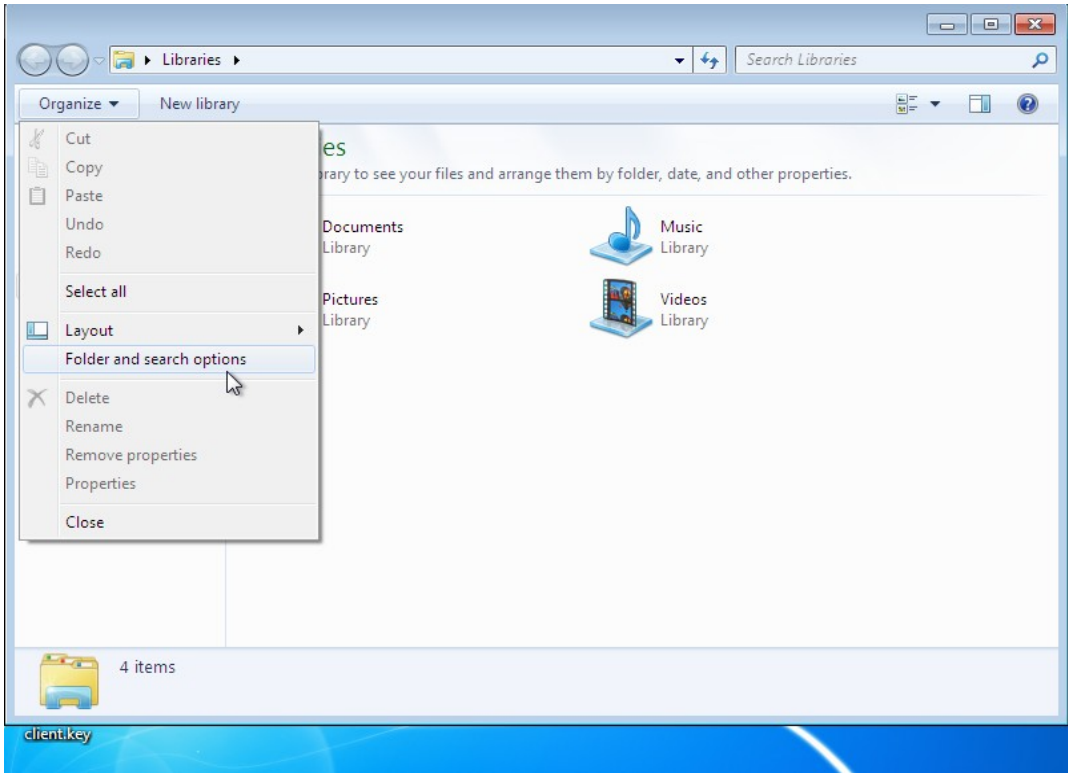
  Lalu posisi 3 file tadi sekarang ada dimana? Cobalah kalian cek menggunakan Windows Explorer lalu arahkan ke **Drive C > Document and Settings > Documents**. Seharusnya file-filenya ada disitu.

- Langkah selanjutnya yang harus kalian lakukan adalah menginstall aplikasi OpenvpnGUI yang juga sudah kalian download sebelumnya. Untuk cara menginstallnya, tinggal klik Next-Next-Next saja seperti instalasi aplikasi Windows biasa.



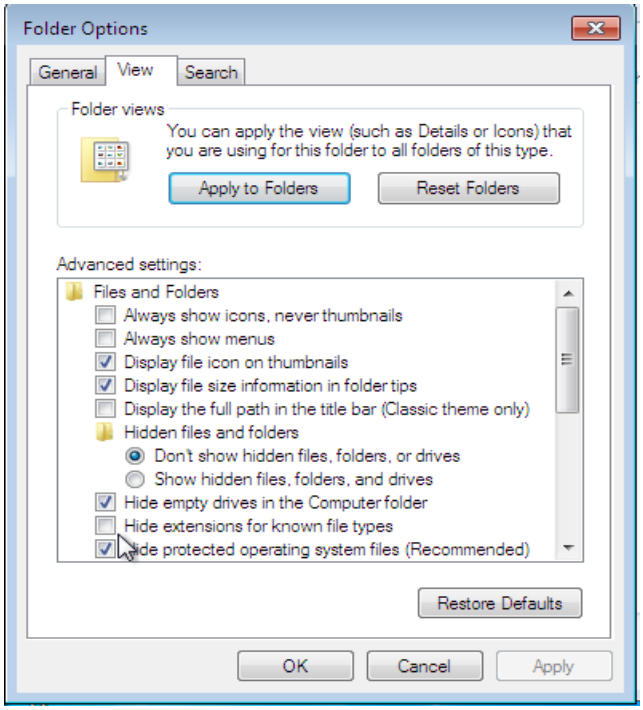
Gambar 4.5.16

- Berikutnya, kalian perlu menghilangkan fitur penyembunyian ekstensi sebuah file yang ada di Windows. Kenapa harus kita nonaktifkan? Di OS Windows, seluruh file yang sudah diketahui ekstensinya seperti file *.exe*, *.avi*, atau *.mp3*, ekstensinya tidak akan muncul kan? Sebagai contoh jika kalian mempunyai file *mp3* berjudul *Noah – Separuh Aku*, maka yang akan muncul hanyalah tulisan *Noah - Separuh Aku* saja, bukannya *Noah - Separuh Aku.mp3*. Nah, fitur ini akan mengganggu untuk langkah pengkonfigurasian OpenVPN GUI yang selanjutnya jika tidak dihilangkan. Oleh karena itu, kalian harus menonaktifkannya dengan cara berikut :
  - Buka **Windows Explorer**, kemudian klik **Organize** di sebelah kiri atas, lalu pilih **Folder and Search Options**.



Gambar 4.5.17

- Pada tab **View**, hilangkan centang pada opsi **Hide Extension for known file types**. Kemudian klik **OK**.



Gambar 4.5.18

- Maka seharusnya sekarang seluruh file-file yang ada di Windows kalian sudah muncul ekstensinya.

- Selanjutnya buatlah sebuah file dengan notepad bernama **client.ovpn** (hapus ekstensi **.txt** dibelakangnya dan ganti menjadi **.ovpn**) di dalam direktori yang sama dengan ketiga file yang telah kalian kopi dari server sebelumnya. Didalam file **client.ovpn** tersebut kalian isikan dengan script berikut ini :

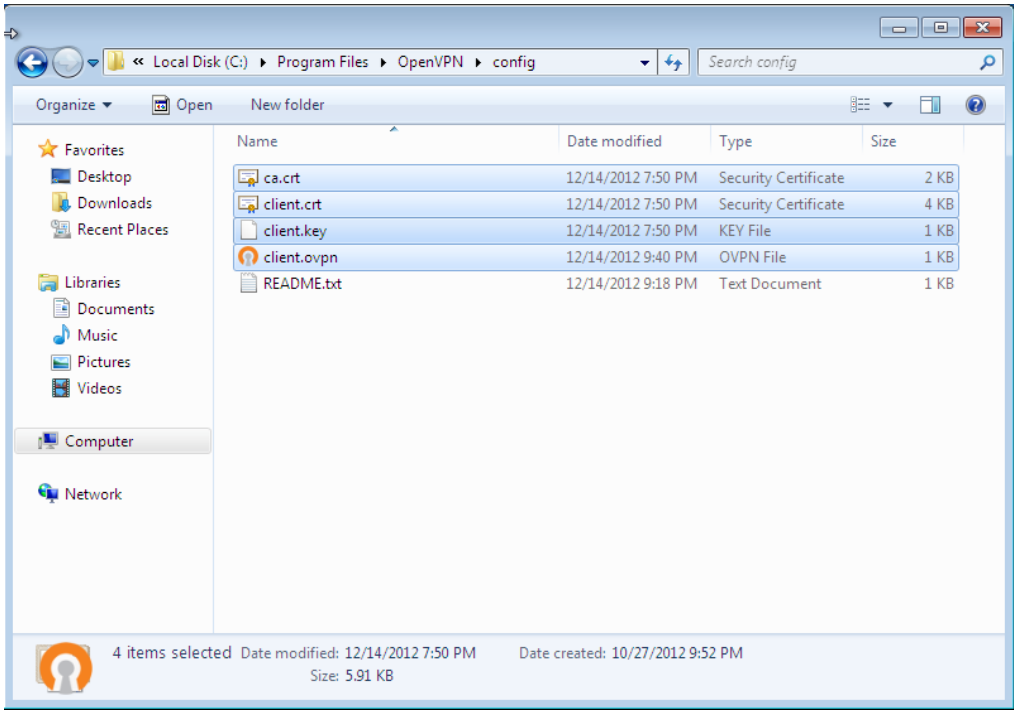
```
client
dev tun
proto udp
remote 192.168.1.100 1194
key client.key
cert client.crt
ca ca.crt
auth-user-pass
persist-key
persist-tun
comp-lzo
verb 3
```

Ket :

- **dev tun** = menggunakan device bernama tun untuk jalur koneksinya.
- **proto udp** = menggunakan protokol udp.
- **remote 192.168.1.100 1194** = 192.168.1.100 merupakan IP Address lokal milik server. Seharusnya jika dalam konfigurasi jaringan yang asli, disini kalian isikan dengan IP Publiknya, jangan IP Lokalnya. Namun karena keperluan buku ini hanya untuk sebatas uji coba jaringan lokal saja, maka tidak apa-apa diisi IP Address lokal milik si Server. Lalu arti dari 1194 merupakan nomor port yang digunakan oleh service OpenVPN ini.
- **Key, cert, ca** = merupakan petunjuk yang mendeskripsikan file-file key, certificate, dan ca yang client gunakan.
- **Auth-user-pass** = menggunakan autentikasi username dan password untuk dapat login.
- **Persist-key, persist-tun, comp-lzo, verb 3** = merupakan opsi tambahan saja.

Jika sudah selesai, simpan dan tutuplah file tersebut.

- Langkah terakhir yang harus kalian lakukan adalah mengkopi keempat file (client.key, client.crt, ca.crt, client.ovpn) ke dalam folder **C:\Program Files\OpenVPN\config**



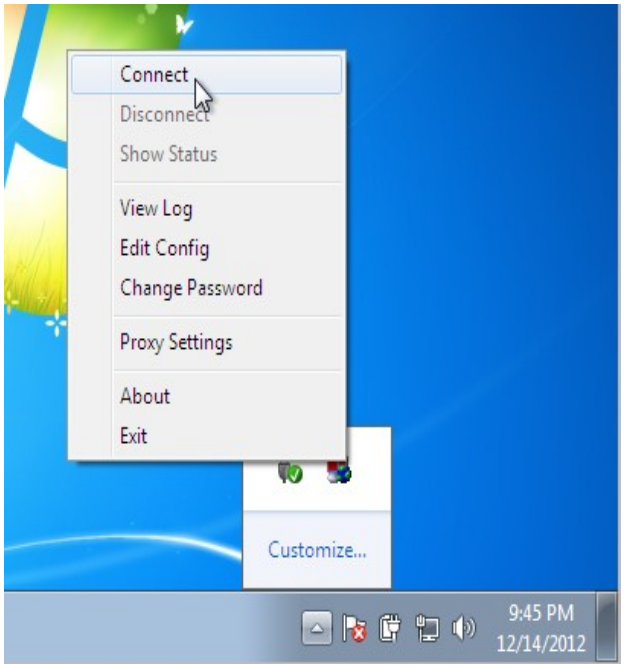
Gambar 4.5.19

- Sampai sini, tahap konfigurasi dari sisi Client telah selesai.

Tahap Pengetesan OpenVPN

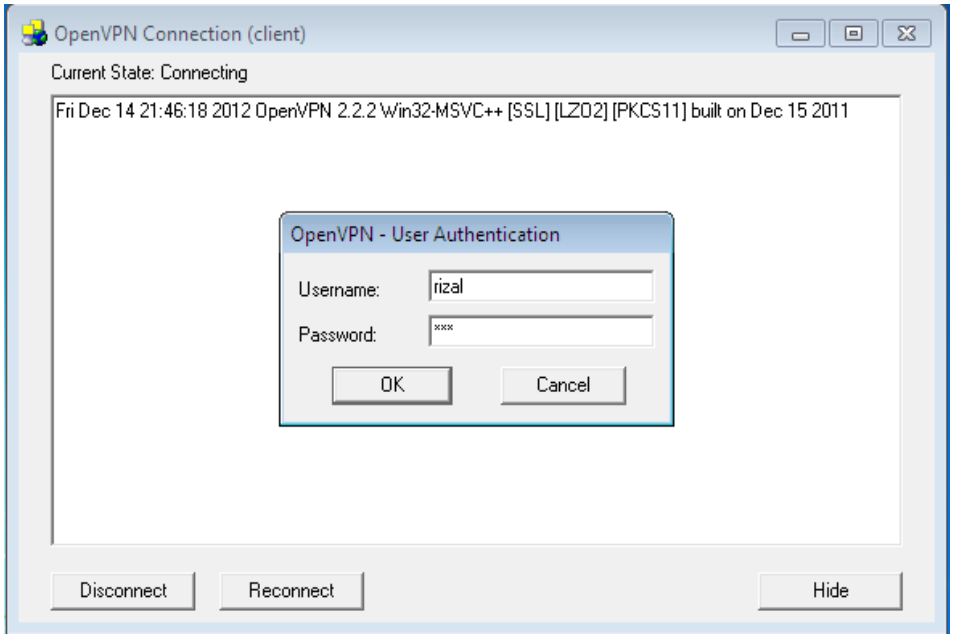
Setelah seluruh konfigurasi dilakukan, sekarang barulah kalian dapat mencoba untuk mengkoneksikan Client ke Server VPN.

- Jalankan shortcut aplikasi OpenVPN GUI pada layar Desktop Windows kalian. Kemudian klik kanan dan pilih **Connect** pada gambar OpenVPN GUI yang terletak pada **System Tray**.



Gambar 4.5.20

- Masukkan *Username* dan *Password* yang biasa kalian gunakan sebagai user login di Server. Disini saya isikan usernamenya adalah *rizal* karena tadi memang saya menggunakan user bernama *rizal*.



Gambar 4.5.21

- Jika berhasil, maka warna OpenVPN GUI tersebut akan berubah menjadi hijau seperti ini.

Gambar 4.5.22

Bab 5. Tambahan

Pada bab tambahan ini saya hanya ingin memberikan sedikit materi yang bersifat *opsional* saja dibandingkan dengan materi-materi penting yang ada pada bab-bab utama pada buku ini. Jadi apabila kalian merasa bahwa materi pada Bab Tambahan ini kurang penting, boleh kalian lewati saja.

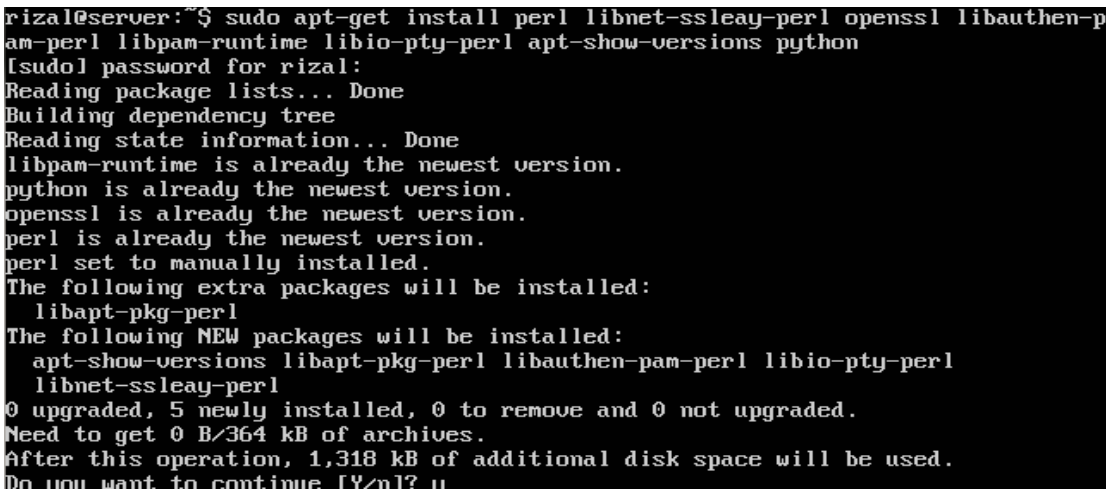
5.1. Instalasi Webmin

Webmin adalah aplikasi berbasis web yang berfungsi untuk mengatur administrasi sistem pada Sistem Operasi Linux. Dengan Webmin ini maka kalian tidak perlu lagi repot-repot menggunakan berbagai macam perintah Command Line untuk mengkonfigurasi sistem, melainkan cukup dengan klik-klik saja melalui tampilan web browser.

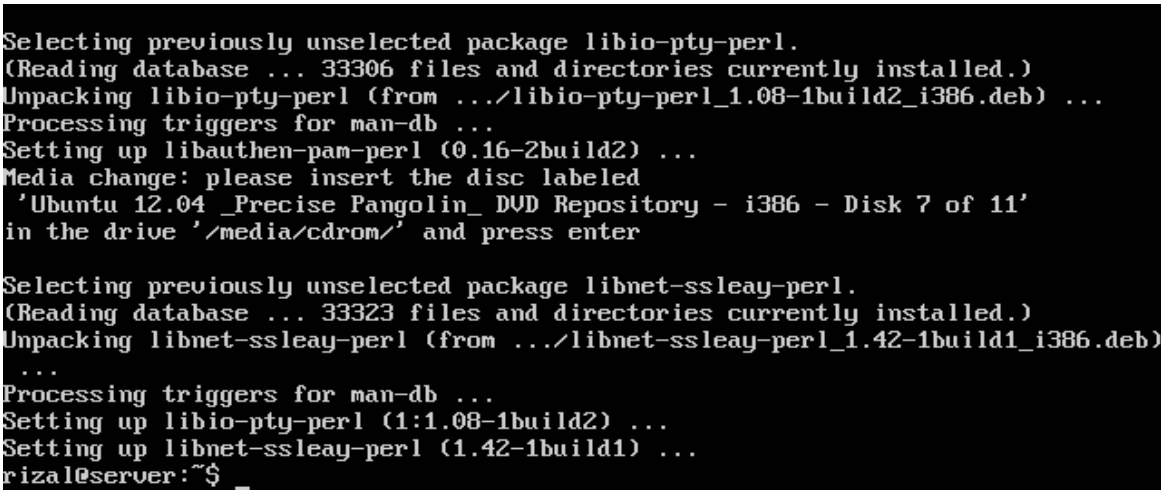
Untuk menginstalasi Webmin di Ubuntu Server 12.04 LTS, lakukan langkah-langkah berikut :

- Sebelum memulai instalasi webmin, kalian perlu menginstal dependensi-dependensi yang dibutuhkan oleh webmin :

  ```
  sudo apt-get install perl libnet-ssleay-perl openssl libauthen-pam-perl libpam-runtime libio-pty-perl apt-show-versions python
  ```



Gambar 5.1.1

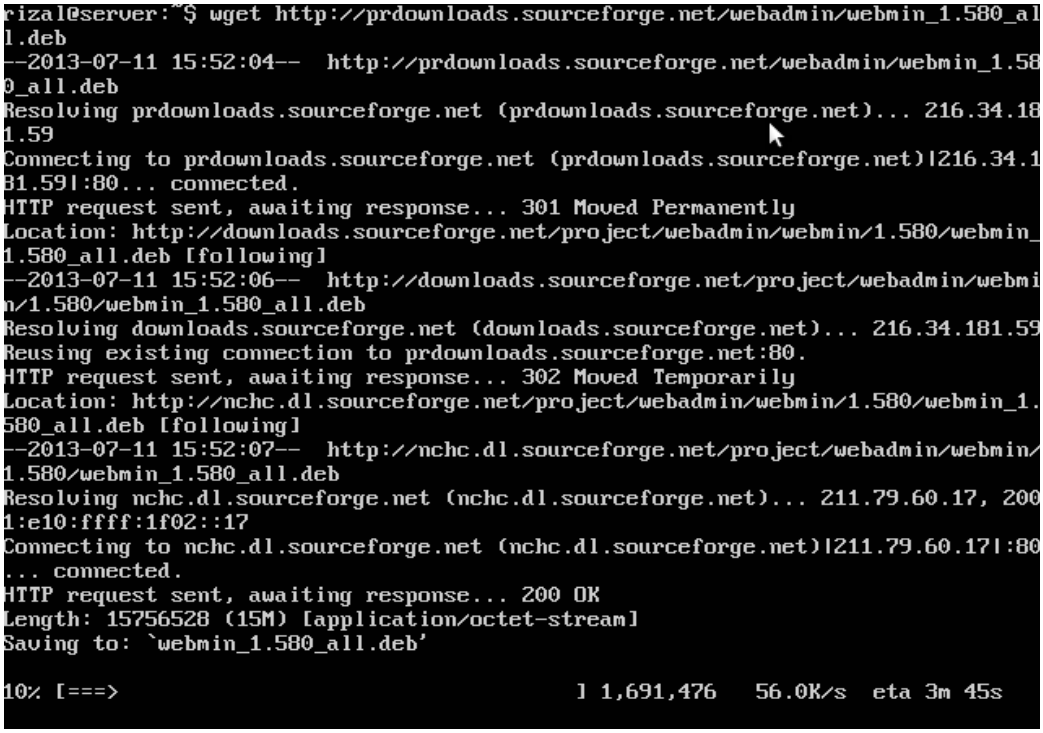


Gambar 5.1.2

Pastikan tidak ada pesan error apapun yang muncul seperti yang tampak pada gambar diatas.

- Selanjutnya downloadlah file mentahan dari webmin dengan menggunakan perintah berikut ini :

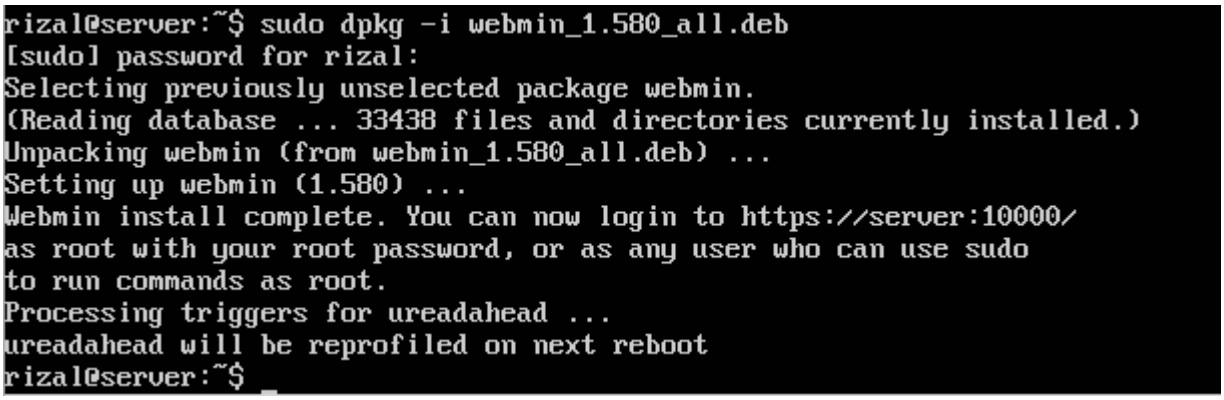
```
wget http://prdownloads.sourceforge.net/webadmin/webmin_1.580_all.deb
```



Gambar 5.1.3

- Setelah file tersebut selesai terdownload, sekarang barulah kalian bisa menginstall webminnya dengan mengeksekusi perintah berikut :

```
sudo dpkg -i webmin_1.580_all.deb
```

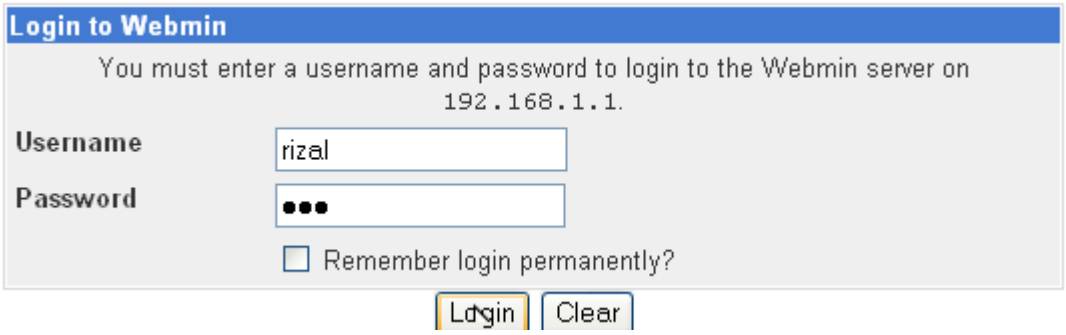


Gambar 5.1.4

- Jika sudah muncul pesan seperti diatas, maka instalasi Webmin dipastikan sudah berhasil. Untuk mengaksesnya, dari sisi client kalian cukup buka alamat https://ipserverkalian:10000 melalui web browser. Sebagai contoh, disini saya akan mengaksesnya dari alamat https://192.168.1.1:10000.
- Jika muncul peringatan seperti ini, pilih saja **Yes** untuk melanjutkan.

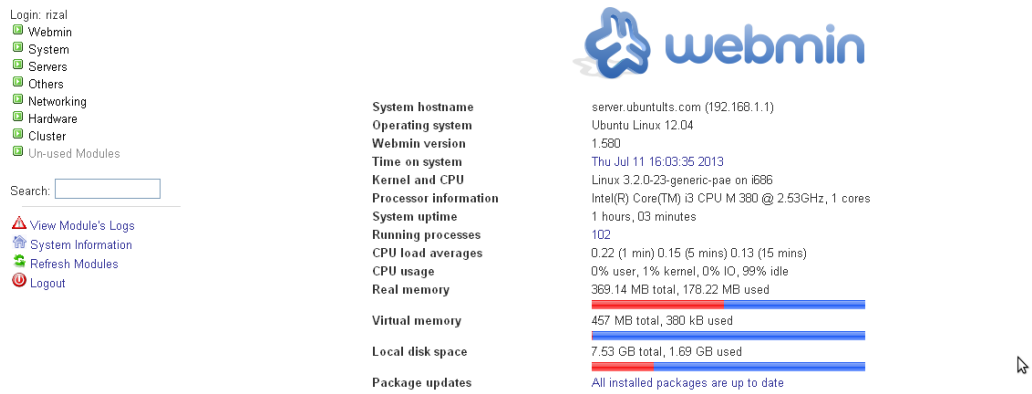
Gambar 5.1.5

- Setelah itu masukkan username dan password dari salah satu user kalian yang memiliki akses Sudo. User yang memiliki akses Sudo ini adalah user yang kalian buat pertama kali pada saat awal instalasi. Pada kasus kali ini, saya akan memasukkan rizal sebagai usernya. Jika sudah, klik **Login**.

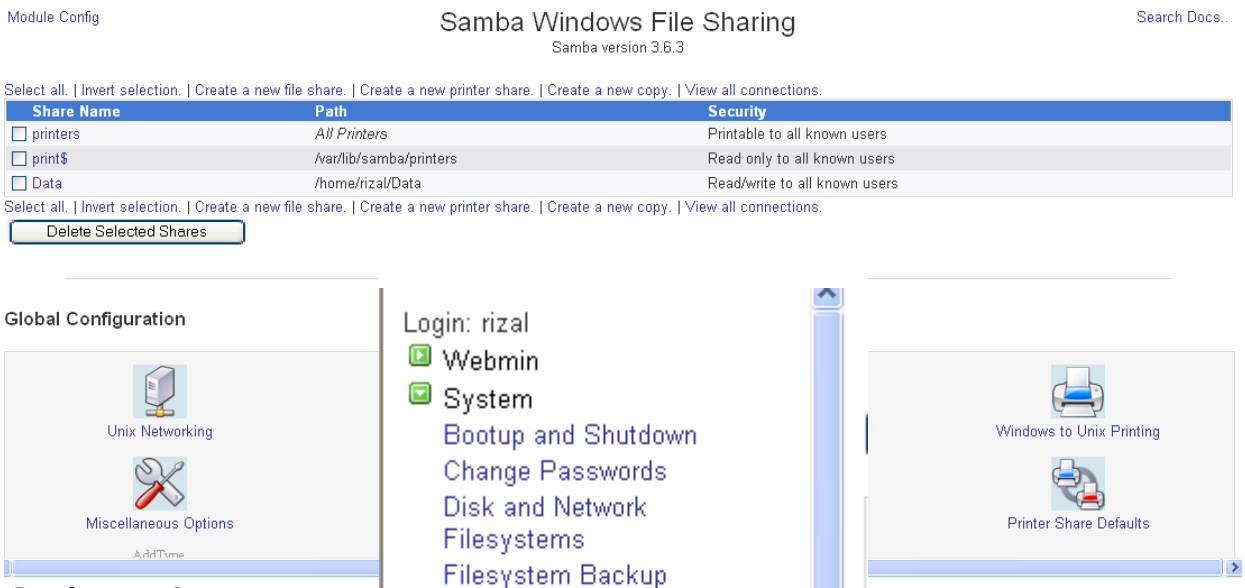


Gambar 5.1.6

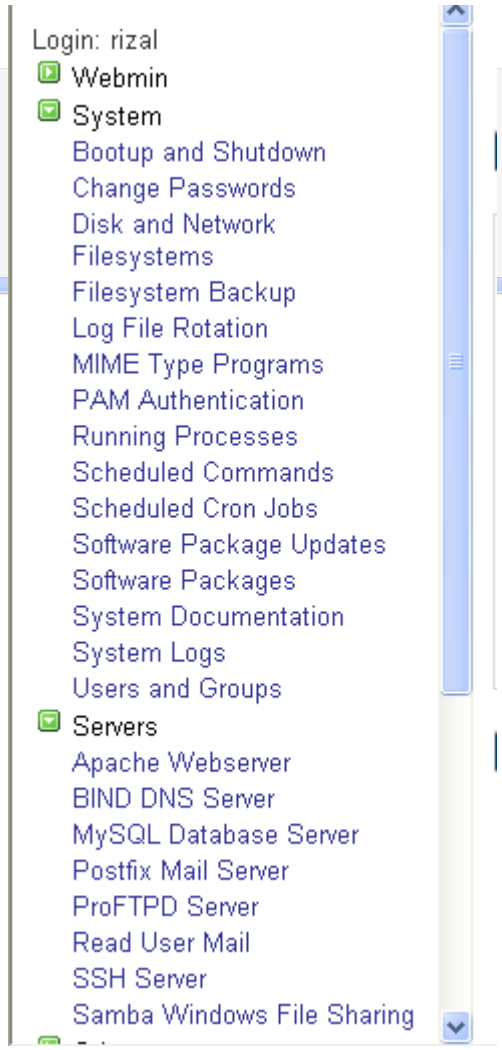
- Berikut adalah tampilan dari Webmin, jika kalian sudah berhasil login kedalamnya.



Gambar 5.1.7



Gambar 5.1.8



Gambar 5.1.9

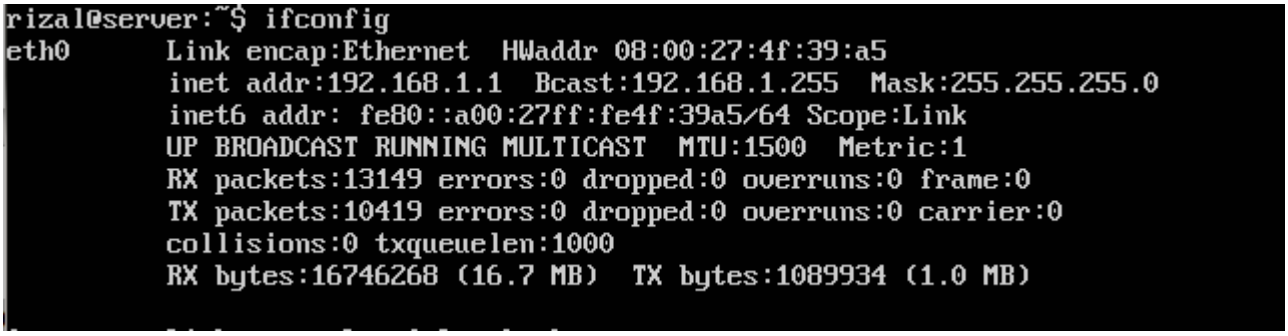
- Dengan kemudahan yang ditawarkan dari Webmin ini, sekarang kalian sudah dapat mengkonfigurasikan berbagai macam administrasi yang berhubungan dengan Server kalian tanpa harus mengenal yang namanya perintah-perintah terminal di Linux lagi.

5.2. Virtual Interface

Apa itu Virtual Interface? Virtual Interface adalah sebuah teknik untuk memberikan IP Address kepada suatu perangkat jaringan virtual (tidak nyata) di Ubuntu Server. Maksudnya apa? Secara teknis, satu buah perangkat jaringan atau NIC di Ubuntu Server seharusnya hanya dapat memiliki satu IP Address saja bukan? Tapi dengan teknik Virtual Interface ini, kita dapat membuat beberapa Interface baru yang bersifat virtual berdasarkan satu buah interface yang aslinya. Dan tentunya dari tiap-tiap Interface Virtual tersebut, kita juga dapat memberikan IP Address selayaknya Interface asli. Bahkan IP Address dari Interfaces virtual ini juga dapat diakses melalui jaringan nyata.

Sekarang coba perhatikan terlebih dahulu interface asli yang kita punya dengan mengeksekusi perintah dibawah ini :

```
ifconfig
```



Gambar 5.2.1

Dari situ terlihat, pada komputer Server memiliki satu buah interface bernama **eth0** dengan IP Address **192.168.1.1**. Lalu bagaimana jika saya ingin menambahkan 2 buah ip address baru yaitu **192.168.1.2** dan **192.168.1.3** dalam satu buah interface?

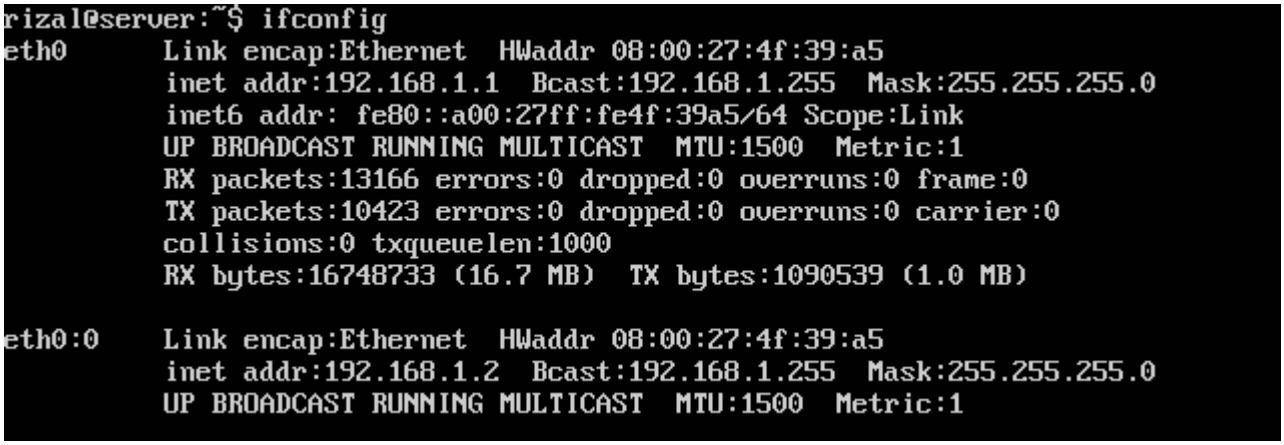
Sintaks yang digunakan untuk menambahkan IP Address kepada Interface Virtual baru adalah sebagai berikut :

```
sudo ifconfig namainterface:nomorurut(dimulai dari 0) ip_addressnya/subnet
```

Contoh :

```
sudo ifconfig eth0:0 192.168.1.2/24
```

Sekarang coba lihat hasilnya dengan perintah **ifconfig** lagi :



Gambar 5.2.2

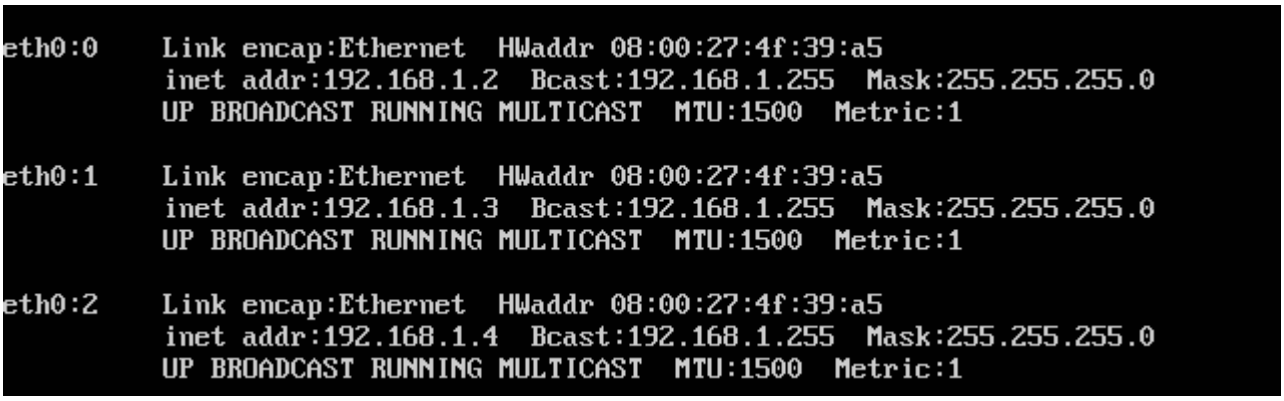
Muncul bukan interface virtual beserta IP nya?

Lalu bagaimana jika ingin menambahkan interface-interface virtual selanjutnya? Kalian tinggal mengurutkan saja angka selanjutnya dari angka 0. Yaitu 1,2,3,4,5 dan seterusnya.

Contoh :

```
sudo ifconfig eth0:1 192.168.1.3/24
sudo ifconfig eth0:2 192.168.1.4/24
```

Lalu lihat hasilnya kembali dengan perintah **ifconfig** :



Gambar 5.2.3

Bagaimana? Sudah sedikit mengerti tentang bagaimana menerapkan teknik Virtual Interface?

5.3. Virtualhost/Virtual Alias

Jika pada sub-bab sebelumnya kalian sudah mengenal yang namanya Virtual Interface, maka pada sub-bab kali ini kita masih akan bersenang-senang dengan hal yang berbau-bau Virtual. Dan sekarang nama teknik yang akan kita pelajari adalah teknik Virtual Host atau biasa disebut sebagai Virtual Alias.

Virtual Alias ini adalah teknik untuk mengalihkan direktori root dari suatu web berdasarkan domain atau IP Address tertentu. Sederhananya begini, jika kita mempunyai domain bernama ubuntults.com dengan subdomain www.ubuntults.com dan mail.ubuntults.com, tentunya kita ingin membuat kedua sub-domain tersebut memiliki tampilan yang berbeda ketika dibuka, bukan? Misalnya saja jika kalian membuka www.ubuntults.com maka yang tampil adalah halaman portal dari website kalian, sedangkan jika membuka mail.ubuntults.com maka yang tampil adalah halaman login email. Nah teknik untuk membeda-bedakan tampilan web inilah yang disebut sebagai teknik Virtual Alias.

Sekarang kita akan coba untuk membuat Virtual Alias untuk subdomain mail.ubuntults.com agar mengarah ke direktori milik Webmail yang berada di /usr/share/roundcube :

- Masuklah ke dalam direktori **/etc/apache2/sites-available** dengan menggunakan perintah ini :

```
cd /etc/apache2/sites-available
```

- Kemudian buatlah satu buah file baru dengan nama terserah kalian. Tapi agar tidak lupa, saya sarankan lebih baik nama file yang kalian pilih setidaknya ada sedikit sangkut pautnya dengan nama Virtual Alias baru yang ingin kalian buat. Contohnya saja disini saya ingin membuat Virtual Alias untuk subdomain mail.ubuntults.com, maka nama file yang saya pilih adalah **mail.ubuntults**.

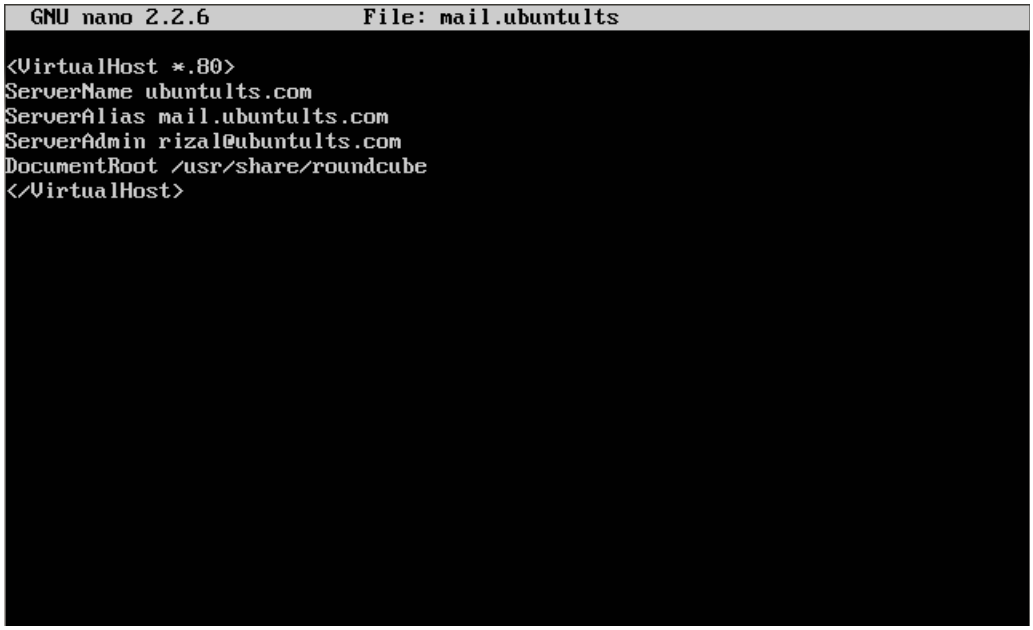
  ```
  sudo nano mail.ubuntults
  ```

- Didalam file tersebut kalian isikan dengan script berikut ini :

  ```
  <VirtualHost *:80>
  ServerName ubuntults.com
  ServerAlias mail.ubuntults.com
  ServerAdmin rizal@ubuntults.com
  DocumentRoot /usr/share/roundcube
  </VirtualHost>
  ```

  Ket. :

  - **ServerName** = Nama domain
  - **ServerAlias** = Nama subdomain yang ingin dialihkan/dijadikan virtual alias.
  - **ServerAdmin** = Alamat email pemilik domain.
  - **DocumentRoot** = Tempat pengalihan direktori dari Virtual Alias yang dibuat.



Gambar 5.3.1

Jika sudah, simpanlah file tersebut dengan menekan kombinasi tombol **CTRL + X > Y > Enter**.

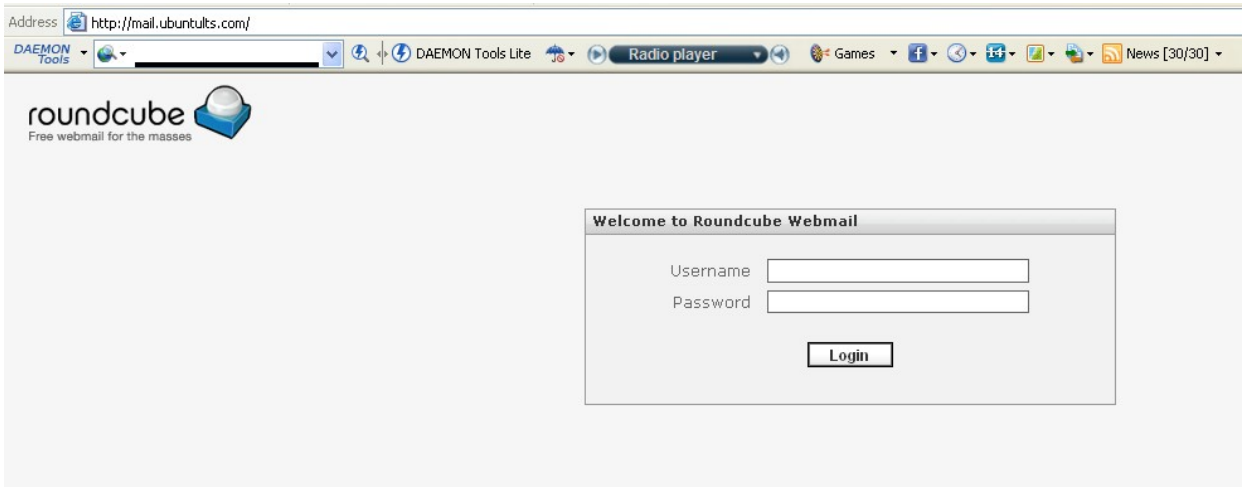
- Selanjutnya ketiklah perintah berikut untuk mengaktifkan VirtualHostnya :

```
sudo a2ensite mail.ubuntults
```

- Terakhir restartlah service dari webserver apachenya dengan mengeksekusi perintah berikut :

```
sudo service apache2 restart
```

- Jika tidak ada pesan error yang muncul, sekarang cobalah kalian test dari sisi client dengan menggunakan web browser. Arahkan ke alamat http://mail.ubuntults.com dan seharusnya tampilannya akan sama dengan saat kalian mengetikkan alamat http://ubuntults.com/roundcube.



Gambar 5.3.2

- Sampai sini konfigurasi untuk menerapkan teknik VirtualHost/VirtualAlias telah selesai. Jika nanti kalian ingin menerapkan Virtual Alias di sub domain yang lain, kalian tinggal membuat file dengan nama yang baru, kemudian isikan dengan script yang sama dengan script diatas, kemudian kalian tinggal mengganti pada bagian VirtualAlias dan DocumentRootnya saja.

Penutup

Alhamdulillah, walaupun masih banyak kekurangan disana-sini, khususnya dalam hal bahasa penulisan dan materi yang di angkat, akhirnya buku pertama saya ini bisa selesai juga. Sesungguhnya saya sangat berharap seluruh materi yang ada didalam buku ini dapat tersampaikan dengan baik kepada kalian para pembaca, sehingga dapat kalian ambil manfaatnya.

Berhubung buku ini benar-benar saya dedikasikan untuk keperluan edukasi, maka saya akan senang sekali apabila kalian juga ikut membagikan buku ini (tanpa merubah apapun atribut penulis) ataupun mengajarkannya kembali ke teman-teman maupun sanak saudara yang kalian punya. Tentunya hal tersebut akan membantu dunia Linux semakin dikenal oleh banyak orang sehingga semakin bermanfaat pula ilmu yang diperoleh.

Oh iya, jika kalian menemukan kesulitan dalam mempelajari materi yang ada di dalam buku ini, kalian dapat menghubungi saya kapanpun melalui kontak yang saya cantumkan pada halaman Profil Penulis pada buku ini. InsyaAllah saya akan membalas pertanyaan kalian semampu saya.

Akhir kata, semoga dengan membaca buku ini setidaknya kalian sudah memiliki dasar dalam menjalani kehidupan sebagai seorang Linux System Administrator. Selamat belajar, dan salam Open Source!

Rizal Rahman

Daftar Pustaka

Buku :

Komputer, Wahana. 2009. *"Langkah Mudah Administrasi Jaringan Menggunakan Linux Ubuntu 9"*, Yogyakarta, Andi Yogyakarta.

Sofana, Iwan. 2008. *"Membangun Jaringan Komputer"*, Bandung, Informatika.

Heriadi, Doddi. 2012. *"Solusi Cerdas Menguasai Internetworking Packet Tracer"*, Yogyakarta, Andi Yogyakarta.

Rafiudin, Rahmat. 2010. *"Mengganyang Hacker dengan Snort"*, Yogyakarta, Andi Yogyakarta.

Internet :

http://articles.slicehost.com/2008/8/6/postfix-using-telnet-to-test-postfix

http://workaround.org/ispmail/lenny/test-mail-through-telnet

http://forum.linuxsupports.com/read.php?4,947,947#msg-947

http://chapila.com/internet/apa-itu-mail-server.html

http://searchsoa.techtarget.com/definition/mail-server

http://www.postfix.org/

http://dovecot.org/

http://ilmukomputer.com/

http://onno.vlsm.org

http://opensource.telkomspeedy.com/

http://www.cisco.com/

http://boson.com/

http://www.linuxku.com/2011/11/instalasi-webserver-apache-mysql.html

http://www.linuxku.com/2011/10/install-konfigurasi-ntp-server-di.html

http://www.kaskus.co.id/showthread.php?t=2317660

http://www.aboutdebian.com/firewall.htm

http://www.cyberciti.biz/tips/linux-iptables-allow-squid-proxy-incoming-client-request.html

http://forum.linuxsupports.com/read.php?4,413,413

http://www.cyberciti.biz/tips/linux-iptables-examples.html

http://ubuntu-indonesia.com/forums/ubbthreads.php/ubb/showflat/Number/111824/gonew/1/membuat_etc_resolv_conf_perman#UNREAD

http://maxsinoda.wordpress.com/membuat-router-pada-linux-debian/
http://ubuntu-indonesia.com/forums/ubbthreads.php/ubb/showflat/Number/112847/gonew/1/Spek_PC_buat_server_ubuntu_per#UNREAD
http://linuxku.com/2011/10/instalasi-snort-dan-beberapa-penerapan.html
http://www.gemamandiriweb.com/artikel/77-cara-membuat-dan-menggunakan-webmail-
https://help.ubuntu.com/community/Roundcube
http://www.upubuntu.com/2012/02/how-to-install-roundcube-webmail-071-on.html
http://id.wikipedia.org/wiki/Tembok_api
http://ghadinkz23.blogspot.com/2012/03/pengertian-firewall.html
http://cyberkomputer.com/jaringan-komputer/pengertian-dan-fungsi-firewall-dalam-suatu-jaringan-komputer-lan-dan-wan/
http://nawala.org/
http://malang.linux.or.id/2012/07/belajar-iptables-dan-konfigurasi-iptables/
http://icehealer.wordpress.com/tag/iptables-adalah/
http://bodhon.wordpress.com/2007/04/10/iptables/
http://www.linuxku.com/2012/09/membatasi-akses-port-port-tertentu.html
http://www.linuxku.com/2012/02/redirect-dns-ke-dns-nawala.html
http://itnetworkingsupport2012.blogspot.com/2012/09/konfigurasi-dmz-di-debian-605.html
http://www.linuxku.com/2012/12/konfigurasi-dmz-di-debian-6-squeeze.html
http://idubart.wordpress.com/2010/08/15/keamanan-jaringan-dengan-dmz/
http://softkompi.blogspot.com/2012/07/fungsi-cara-kerja-dan-apakah-vpn.html
http://und3rw0rld.info/apakah-virtual-private-network-atau-vpn-itu/
http://www.linuxku.com/2012/12/install-dan-konfigurasi-openvpn-di.html
http://www.ubuntugeek.com/how-to-install-webmin-on-ubuntu-12-04-precise-server.html
http://www.linuxku.com/2011/11/cara-membuat-satu-ethernet-menjadi.html
http://www.howtoforge.com/virtual-users-and-domains-with-postfix-courier-mysql-and-squirrelmail-ubuntu-12.04-lts-p2
https://www.digitalocean.com/community/articles/how-to-install-and-setup-postfix-on-ubuntu-12-04

Profil Penulis

Nama lengkap penulis adalah Rizal Rahman, seorang alumni pelajar SMK yang kini sedang menapaki jenjang pendidikan yang lebih tinggi di sebuah Universitas di Bandung. Keseharian penulis selain sebagai seorang calon mahasiswa, adalah sebagai seorang blogger amatiran dan juga menjalani kehidupan seorang wirausahawan bersama bisnis yang sedang dikembangkannya. Awal mula jatuh cinta pada dunia Linux, penulis alami pada saat berada di kelas 2 SMK ketika mengalami kerusakan harddisk pada komputernya. Sejak saat itu penulis mulai aktif mengikuti seminar-seminar Linux, pelatihan, forum, bahkan akhirnya bersama teman-teman seperjuangannya sampai bisa menyelenggarakan seminar dan pelatihan Linux sendiri. Kini, penulis mendedikasikan diri untuk terus menyebarluaskan ilmu Linux dan Open Source melalui media tulisan tangannya ke seluruh penjuru negeri dan dunia.

Nama lengkap	: Rizal Rahman
TTL	: Surabaya, 10 Desember 1994
Pekerjaan	: Pelajar/Mahasiswa
Kontak	: rizalempol@gmail.com
Favorite Quote	: Life isn't about waiting for the storm to pass...it's learning to dance in the rain. Any problems? dance with it!