Kegiatan Belajar 3 Administrasi Sistem Jaringan

Capaian Pembelajaran Mata Kegiatan

Memahami Administrasi Jaringan

Sub Capaian Pembelajaran Mata Kegiatan

1. Menerapkan Sistem Operasi Jaringan
2. Mengevaluasi DHCP Server
3. Mengevaluasi FTP Server
4. Mengevaluasi Remove Server
5. Mengevaluasi File Server
6. Mengevaluasi Web Server
7. Mengevaluasi DNS Server
8. Database Server
9. Mengevaluasi Mail Server
10. Mengevaluasi Control Panel Hosting
11. Mengevaluasi Share Hosting Server
12. Mengevaluasi Vitual Private Server
13. Mengevaluasi Dedicated Hosting Server
14. Mengevaluasi VPN Server
15. Mengevaluasi Sistem Kontrol dan Monitoring
16. Mengevaluasi Sistem Keamanan Jaringan

Pokok-Pokok Materi

a. Sistem Operasi Jaringan
b. DHCP Server
c. FTP Server
d. Remove Server
e. File Server
f. Web Server
g. DNS Server
h. Database Server
i. Mail Server
j. Control Panel Hosting
k. Share Hosting Server
l. Vitual Private Server
m. Dedicated Hosting Server
n. VPN Server
o. Sistem Kontrol dan Monitoring
p. Sistem Keamanan Jaringan

Uraian Materi

A. Sistem Operasi Jaringan

1. Pengertian Sistem Operasi Jaringan

Sistem Operasi Jaringan (*Network Operating System*) adalah sebuah jenis sistem operasi yang ditujukan untuk menangani jaringan. Umumnya, sistem operasi ini terdiri atas banyak layanan atau service yang ditujukan untuk melayani pengguna, seperti layanan berbagi berkas, layanan berbagi alat pencetak (*printer*), DNS Service, HTTP Service, dan lain sebagainya. Istilah ini populer pada akhir dekade 1980-an hingga awal dekade 1990-an. Sistem operasi jaringan adalah suatu jenis sistem operasi yang dikususkan untuk menangani jaringan.Sistem operasi ini terdiri atas banyak layanan atau service yang ditujukan untuk melayani pengguna, seperti layanan berbagi berkas, layanan berbagi alat pencetak (*printer*), DNS Service, HTTP Service, dan lain sebagainya.

2. Karakteristik Sistem Operasi Jaringan

Ada beberapa karakteristik dari sistem operasi jaringan yaitu:

a. Pusat kendali sumber daya jaringan
b. Akses aman ke sebuah jaringan
c. Mengizinkan remote user terkoneksi ke jaringan
d. Mengizinkan user terkoneksi ke jaringan lain (misalnya Internet)
e. Back up data dan memastikan data tersebut tersedia

3. Fungsi Utama Sistem Operasi Jaringan

a. Menghubungkan sejumlah komputer dan perangkat lainnya ke sebuah jaringan
b. Mengelola sumber daya jaringan
c. Menyediakan layanan
d. Menyediakan keamanan jaringan bagi multiple users
e. Mudah menambahkan client dan sumber daya lainnnya
f. Memonitor status dan fungsi elemen – elemen jaringan
g. Distribusi program dan update software ke client
h. Menggunakan kemampuan server secara efisien
i. Menyediakan tolerasi kesalahan

4. Jenis-Jenis Sistem Operasi jaringan berdasarkan layanan (interface)

a. Sistem Operasi Jaringan Berbasis GUI

   Adalah Sistem operasi yang dalam proses Instalasinya, user tidak perlu menghafal sintax – sintax atau perintah DOS atau bahasa pemograman yang digunakannya. Berikut beberapa contoh Sistem Operasi jaringan berbasis GUI: Linux Redhat, Windows NT 3.51, Windows 2000 (NT 5.0), Windows Server 2003, Windows XP, Microsoft MS-NET, Microsoft LAN Manager, Novell NetWare.

b. Sistem Operasi Jaringan Berbasis Text

   Adalah sistem operasi yang proses instalasinya, user diharapkan untuk menghafal perintah DOS yang digunakan untuk menjalankan suatu proses instalasi Sistem Operasi Jaringan tersebut, diantaranya adalah sebagai berikut: Linux Debian, Linux Suse, Sun Solaris, Linux Mandrake, Knoppix, MacOS. UNIX, Windows NT, Windows 2000 Server, Windows 2003 Server.

5. Jenis-Jenis Sistem Operasi Jaringan

a. Close Source

Pengertian *Closed Source Software adalah* perangkat lunak atau software yang dipublikasikan tanpa diberikan kode sumbernya, pada software jenis closed source hanya terdiri dari file binari saja tanpa adanya ruang untuk mengakses ke kode sumber software tersebut.

Secara umum, software closed source memiliki lisensi atau hak cipta yang bertujuan untuk melindungi software tersebut dari penggunaan yang dapat merugikan si pembuat software dan menguntungkan pihak ketiga. Software Closed Source bersifat terbatas dalam penggunaan, penyalinan, juga modifikasi. Bagi seseorang atau perusahaan yang bermaksud ingin mengakses kode sumber maka dibutuhkan perjanjian khusus yang dinamakan perjanjian non-disclosure.

Sistem Operasi Close Source adalah Sistem Operasi yang kodenya tidak dibuka untuk umum, pemilik kode close source bisa membagikan source codenya melalui lisensi secara gratis maupun gengan membayar.

Pada Sistem Operasi Close Source ini paket program tidak dapat didistribusikan lagi selain oleh Pembuat/Vendor Program tersebut. Jika ada pendistribusian yang bukan dari Vendor Program tersebut, maka dianggap sebagai pembajakan software.

1) Keuntungan/Kelebihan Close Source
   a) Kestablian sistem terjamin
   b) Support/dukungan langsung dari pemilik program
   c) Lebih mudah digunakan
2) Kerugian/Kekurangan Close Source
   a) Celah yang terbuka
   b) Adanya lisensi yang mengharuskan pengguna menyediakan dana
   c) Pengembangan terbatas
   d) Diperlukan antivirus
   e) Harga lisensi mahal
3) Pengelompokkan dan Contoh Software Closed Source

Sistem Operasi Contoh perangkat lunak dalam kelompok Sistem Operasi yang menggunakan lisensi Closed Source adalah Microsoft Windows: MS-DOS, Windows 95, Windows 98, Windows ME, Windows NT, Windows XP, Windows Server 2003, Windows Vista, Windows Server 2008, Windows 7, Windows 8.

a) Bahasa Pemrograman

   Ada banyak jenis bahasa pemrograman, diantaranya software pemrograman tersebut banyak yang memiliki lisensi closed source, contohnya: ASP.Net, Pascal, Visual Basic

b) Web Browser

   Contoh Web Browser dengan kode sumber tertutup adalah Internet Explorer yang sejak dahulu dipakai oleh Microsoft dalam Sistem Operasi Windows-nya.

c) Aplikasi

   Banyak sekali aplikasi yang menggunakan lisensi kode tertutup atau closed source, contoh aplikasi terkenal adalah: CorelDraw, Adobe Photoshop

d) Aplikasi Perkantoran

   Microsoft Office menjadi aplikasi paling populer berbasis closed source untuk membantu menyelesaikan pekerjaan kantor dan lainnya.

e) Anti Virus

   Untuk mengamankan komputer dari serangan program-program jahat maka diperlukan penangkalnya. Banyak sekali software anti virus, dan berikut ini contoh anti virus closed source: Norton, dan McAfee.

b. Open Source

2) Sistem Operasi Open Source

Sistem Operasi Open Source adalah perangkat lunak (software) yang di mana kode programnya bersifat terbuka dan disediakan oleh pengembangnya secara umum agar bisa untuk dipelajari, diubah maupun dikembangkan lebih lanjut serta disebarluaskan dan boleh bahkan untuk memperbaiki *bug* atau kesalahan pada program tersebut.

Sementara itu, jika ada pembuat perangkat lunak (software) yang tidak mengizinkan dari kode programnya untuk diubah dan dimodifikasi, namun

kode program dari perangkat lunak tersebut sebenarnya tersedia, maka bukanlah disebut sebagai sistem operasi open source.

Yang perlu ditekankan di sini adalah, Sistem Operasi Open Source tidak selalu disediakan secara gratis, melainkan tetap ada biaya yang dikeluarkan untuk membeli program tersebut, Seperti halnya adalah *RedHat Linux*.

Tujuan Open Source yang sesungguhnya adalah menghilangkan ketergantungan terhadap Vendor, yang di mana dari pihak Vendor bisa saja bertindak secara seenaknya. Open Source juga meyediakan software yang mudah untuk dijangkau oleh masyarakat luas dan menghindari adanya pengambilan keuntungan besar-besaran/berlebihan dari Vendor.

Dan perlu digarisbawahi, Open Source di sini bersifat bebas maksudnya bukan berarti sebebas-bebasnya, melainkan bebas untuk digunakan, dikembangkan, disebarkan ulang dengan mempertanggungjawabkan secara bersama dan tidak untuk menghilangkan hak cipta pembuat.

3) Keuntungan/Kelebihan Open Source
   a) Legal
   b) Menyelamatkan devisa Negara
   c) Keamanan system
   d) Hemat biaya
   e) Dukungan dari pengembang lebih besar
   f) Bebas untuk mengubah dan memodifikasi
   g) Lebih aman
   h) Kesalahan (bug, error) lebih cepat ditemukan dan diperbaiki
   i) Lisensei gratis
   j) Bebas dari malware
   k) Tidak mengulangi development
4) Kerugian/Kelemahan Open Source
   a) Tidak ada garansi dari pengembang
   b) Open Source digunakan secara sharing
   c) Kurangnya SDM yang memanfaatkan Open Source
   d) Tidak adanya perlindungan Hak atas Kekayaan Intelektual (HAKI)
   e) Kesulitan mengetahui status project
   f) User Interface rumit bagi pengguna yang awam
5) Contoh Sistem Operasi Open Source

a) Linux, merupakan software sistem operasi yang gratis dan sangat populer: UNIX, BSD, GNU Linux, Sun Solaris, Fedora, Linux Ubuntu, Knoppix, Garuda OS, Backtrack, RedHat, Mandriva, OpenSUSE, Debian, Kondra Linux, Turbo Linux, Linux Mint, Slackware.
b) XAMPP, merupakan paket softwere yang berguna untuk simulasi dan pengembangan web, termasuk juga di dalamnya Apache dan MySQL (database).
c) Mozilla Firefox, merupakan softwere yang berguna untuk menjelajahi halaman web di internet.
d) OpenOffice, merupakan paket softwere perkantoran yang berguna untuk mengolah kata, tabel dan database.
e) osCommerce, merupakan softwere aplikasi web yang digunakan untuk toko online.
f) ClamAV & ClamWin, merupakan softwere antivirus.
g) Audacity, merupakan softwere perekam sekaligus pengolah audio.
h) GIMP, merupakan softwere pengolah foto dan juga gambar digital.
i) VideoLAN, merupakan softwere pemutar file multimedia
j) Blender, merupakan program untuk pembuatan model 3 (tiga) dimensi, misalnya seperti animasi dan game.
k) Filezilla, merupakan softwere jaringan yang berfungsi untuk transfer file via protokol FTP pada jaringan komputer atau jaringan internet.
l) Mplayer, merupakan ssoftwere pemutar musik yang berbasis open source

B. DHCP Server

1. Pengertian DHCP Server

DHCP (*Dynamic Host Control Protocol*) adalah protokol pengalamatan host secara dinamis. Dalam sebuah jaringan yang besar, akan ada bagian yang pengalamatan IP address tidak begitu kritikal. Di bagian ini pengalamatan IP bisa dilakukan secara dinamis dan otomatis.

Apabila dalam sebuah jaringan diwajibkan memberi IP satu per satu dengan manual, maka akan memakan waktu yang sangat lama. Misalkan ada jaringan dengan pengguna 1500 orang, maka akan membutuhkan pengaturan alamat IP secara manual di tiap komputer sebanyak 1500 kali.

Karena itulah DHCP ada, sehingga komputer host tetap bisa terhubung dengan jaringan secara otomatis meskipun tidak mendapatkan IP address sesuai yang diminta, tapi sudah pasti akan mendapatkanya apabila IP masih tersedia dan DHCP server berjalan normal.

Pendapatan IP mempunyai waktu yang terbatas, DHCP mengatur agar IP bisa digunakan berulang-ulang. Ada batas penyewaan waktu yang harus disetujui oleh host. Jadi ketika waktu penyewaan habis, maka host bisa menentukan apakah dia ingin menyewa IP lagi atau berhenti supaya DHCP server bisa memberikan IP tersebut ke host lainya.

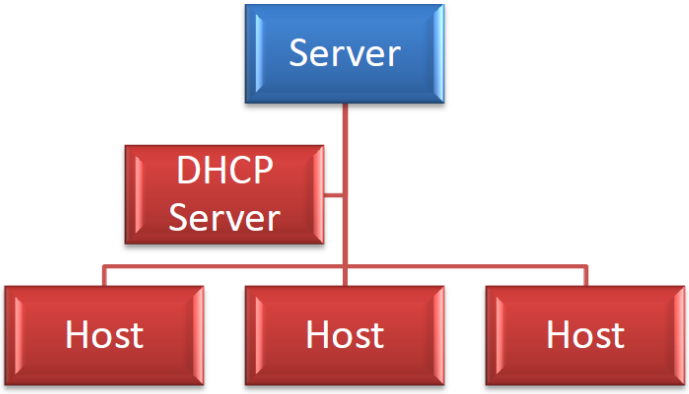
Beberapa IP juga bisa diberikan secara statis untuk MAC address tertentu. Sehingga IP tersebut bisa diserahkan secara ekslusif untuk beberapa mesin yang memang krusial dengan IP tersebut, misalnya membuat DNS server atau HTTP server local di daerah yang diatur IP nya oleh DHCP. Jadi DHCP tidak terbatas hanya bisa memberikan IP secara dinamis dan tidak teratur. Beberapa bisa teratur sehingga membuat DHCP lebih fleksible dalam berbagai keadaan.

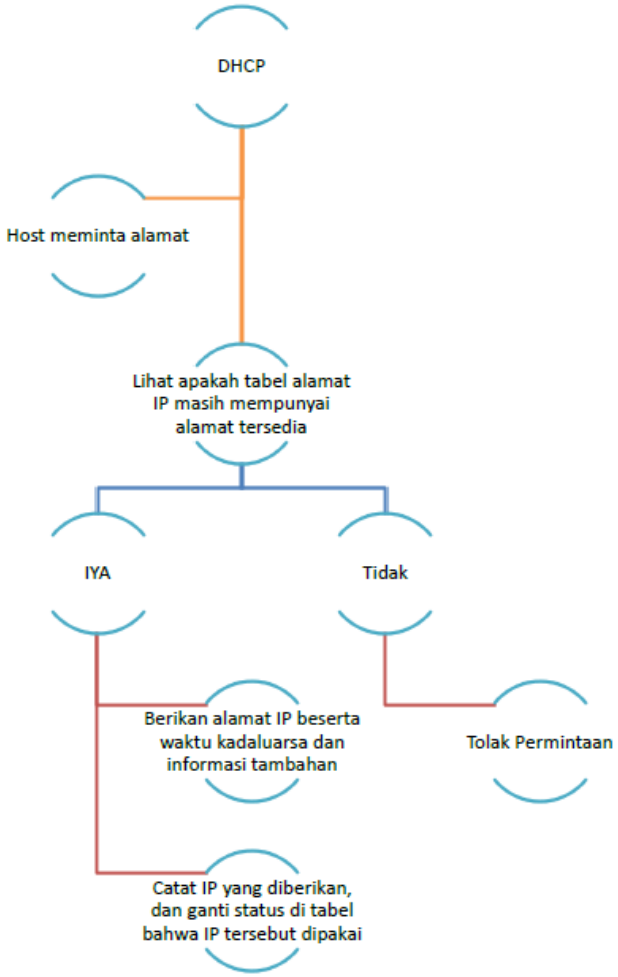
2. Cara Kerja DHCP Server

DHCP server bekerja dengan cara menawarkan diri sebagai DHCP server dan menawarkan IP kepada host yang terhubung. Host akan meminta alamat IP kepada DHCP, lalu DHCP server akan memeriksa apakah masih ada alamat yang tersedia, dan alamat apa saja yang tersedia itu.

Setelah diketahui adanya alamat yang tersedia. Maka DHCP server akan memberikan kepada host tersebut alamat tersebut, DHCP juga menyimpan informasi tambahan seperti DNS server yang harus digunakan, beserta default gatewaynya.

Alamat IP diberikan lengkap dengan informasi kapan dia kadaluarsa sehingga host bisa meminta lagi dan DHCP server bisa menyatakan alamat tersebut sudah bebas dan bisa digunakan kembali baik oleh host yang sama atau berbeda.





Gambar 3.1 Konsep DHCP

DHCP server mempunyai batas dari IP mana sampai mana dia bisa memberikan alamat tersebut kepada host. Dengan batas ini jumlah host bisa dibatasi sesuai dengan keperluan. Digunakan sebagai alternatif untuk menjaga server dari koneksi host yang tidak diinginkan.

3. Mesin DHCP Server

Biasanya, dalam suatu jaringan yang diatur oleh router sudah memiliki DHCP server sendiri di routernya. Namun, apabila harus menggunakan server seperti Linux Debian, maka kita harus memasang aplikasi yang bisa menjadikan server kita sebagai DHCP server. Di Linux Debian, aplikasi yang bisa digunakan sebaai DHCP server adalah dhcp3-server.

4. DHCP Server Debian

DHCP server bisa diinstall dengan menggunakan perintah apt-get install <nama_paket>. Dalam kasus ini paket yang kita install bernama dhcp3-server.

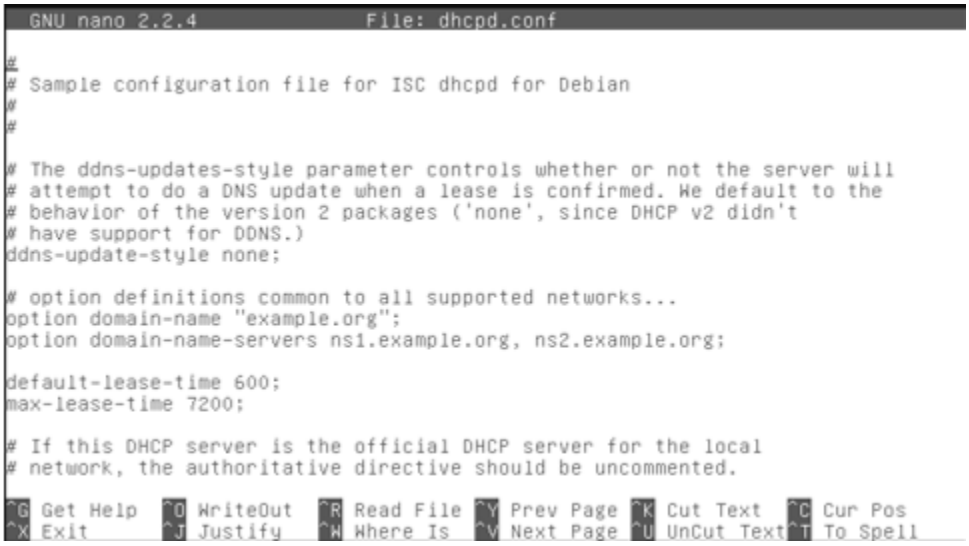
```
apt-get install dhcp3-server
```

Biarkan beberapa saat, apabila ada pertanyaan Y/n, tekan enter untuk mengijinkan installasi DHCP server. Ketika installasi bila ada tulisan failed, biarkan saja, karena kita memang belum melakukan konfigurasi

Apabila tidak ada tulisan **failed** juga tidak mengapa. Setelah selesai installasi, coba lihat apakah ada direktori **/etc/dhcp**. Lakukan **cd** terhadap direktori tersebut dan lakukan **ls** untuk melihat isinya.

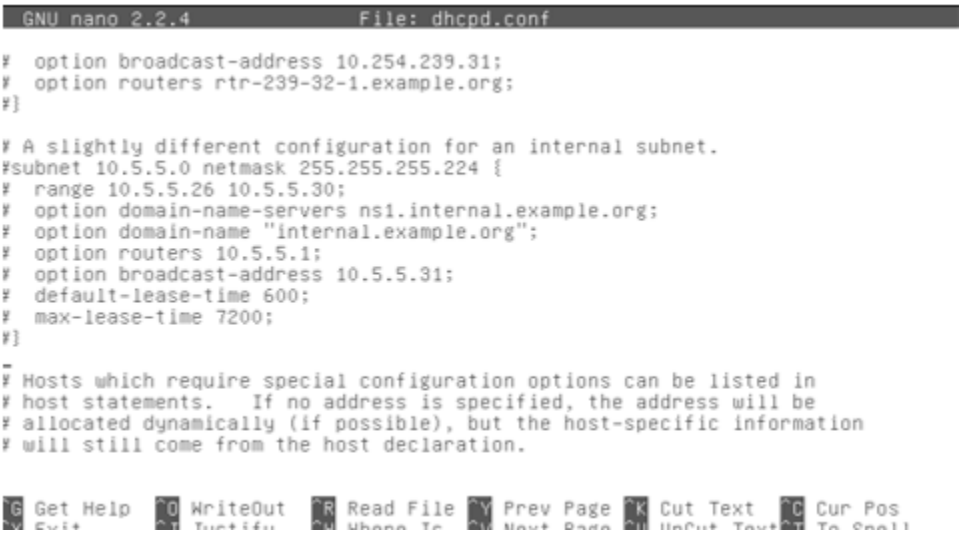
```
root@serverone:~# cd /etc/dhcp/
root@serverone:/etc/dhcp# ls
dhclient.conf  dhclient-enter-hooks.d  dhclient-exit-hooks.d  dhcpd.conf
root@serverone:/etc/dhcp# _
```

Apabila kita ingin melakukan konfigurasi server DHCP, gunakan file yang bernama **dhcpd.conf**. Gunakan **nano** untuk merubah isi dari **dhcp.conf.**



Di atas ini isi dari file dhcp.conf. Ada beberapa pengaturan seputar konfigurasi DHCP.

Yang perlu diperhatikan adalah bagian ini,



Di bagian ini kita akan merubah konfigurasi yang semula dimatikan, supaya aktif.

Rubah hingga berbentuk seperti ini.

Kita membuat aturan dhcp untuk subnet 192.168.1.10, dengan netmask 255.255.255.0 atau 192.168.1.10/24. Lalu kita menentukan, bahwa IP yang bisa digunakan atau disewa oleh host adalah antara 192.168.1.2 – 192.168.1.254. Lalu kita setting alamat DNS server, yaitu mesin server sendiri 192.168.1.1, dengan domain name server. Lalu setting bahwa alamat broadcastnya adalah 192.168.1.255, dengan waktu sewa default 3600 dan waktu sewa maksimal 7200 detik.

Setelah selesai mengatur konfigurasi DHCP server, kita perlu menentukan di bagian mana DHCP server kita ini akan berjalan. Ketikkan,

```
nano /etc/default/dhcp
```

Isi dengan

```
INTERFACE=”eth1”
```

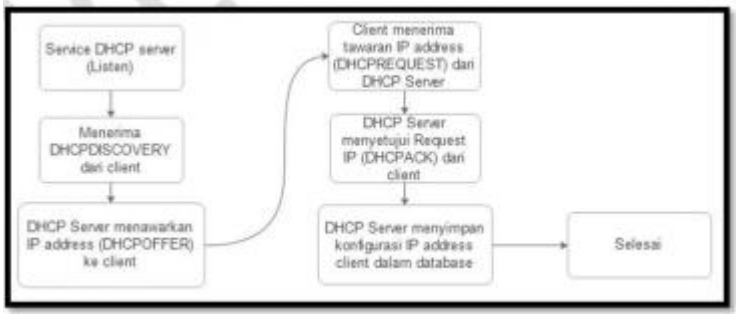
Apabila di server anda tidak ada interface ethernet 1, silahkan ganti menjadi interface ethernet yang ada di sistem anda. Ethernet 0 atau **eth0** biasanya sudah ada dan siap digunakan.

Di sini berarti DHCP server kita berjalan di atas **eth1**, jadi apabila ada host yang terkoneksi dengan **eth1**, maka host tersebut bisa meminta IP dari server kita.

Sambungkan PC dengan interface **eth1** di server, apabila menggunakan sistem oeprasi windows, maka buka command prompt dan gunakan **ipconfig** untuk melihat apakah sudah mendapatkan IP dari server kita. Untuk sistem Linux, gunakan **ifconfig**.

5. Pengujian DHCP Server

Proses kerja dhcp server yaitu :



Gambar 3.2 Proses Kerja DHCP

Untuk konfigurasi DHCP dapat dilakukan dengan menggunakan perintah :

sudo apt-get install dhcp3-server

Lakukan pekonfigurasi pada file "dhcpd.conf" agar berfungsi sebagai server dhcp, dengan perintah :

 # cd /etc/dhcp3

 # gedit dhcpd.conf

Edit lah sesuai dengan kebutuhan jaringan yang dibangun.

[...]

 # A slightly different configuration for an internal subnet.

subnet 192.168.1.0 netmask 255.255.255.0 {

range 192.168.1.2 192.168.1.254;

option domain-name-servers 8.8.8.8,4.4.4.4;

option domain-name "smk.com";

option routers 192.168.1.1;

option broadcast-address 192.168.1.255;

default-lease-time 600;

max-lease-time 7200;

}

[...]

Selanjutnya menentukan interface yang digunakan untuk dhcp-server,dengan perintah :

 # gedit /etc/default/dhcp3-server

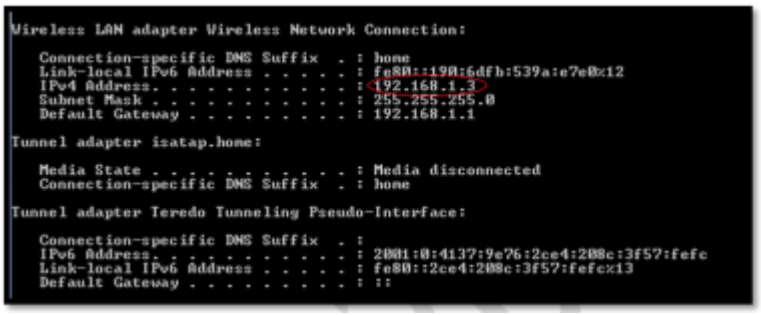
Tambahkan interfaces="eth1",

lalu simpan.

Restart sevice dhcp-server, dengan perintah :

 # /etc/init.d/dhcp3-server restart

Untuk pengujian dari client dapat di setting automatic agar ip address yang didapat sesuai dengan yang di berikan dhcp-server.



Gambar 3.3 Pengujian DHCPserver

C. FTP Server

1. Konsep Protokol Pengiriman File (FTP)

Protokol pengiriman file atau biasa disebut FTP, *File Transfer Protocol*, adalah sebuah protokol klien-server yang memungkinkan seorang pemakai untuk mengirim atau menerima file dari dan ke sebuah tempat/mesin dalam jaringan. Ia bekerja menurut aturan transport TCP dan sangat banyak digunakan dalam jaringan internet. Meskipun demikian juga dapat digunakan pada jaringan lokal, LAN.

Standar yang mendefinisikan FTP mendekripsikan bahwa semua operasi yang menggunakan sebuah alat operasi sederhana yang disebut model FTP. Model FTP mendefinisikan tugas-tugas dari peralatan yang berpartisipasi dalam sebuah perpindahan file, dan dua kanal komunikasi yang terbentuk diantaranya. Serta komponen-komponen FTP yang mengatur kedua kanal dan definisi terminologi yang digunakan untuk komponen-komponen tersebut.

Karena termasuk sebagai protokol klien-server, klien FTP disebut sebagai user, hal ini karena para pengguna FTP menjalankan FTP melalui sebuah mesin klien. Serangkaian operasi perangkat lunak FTP dalam sebuah mesin disebut sebagai proses. Perangkat lunak FTP yang berjalan dalam sebuah server disebut proses server FTP sedangkan yang berjalan di klien disebut proses klien FTP.

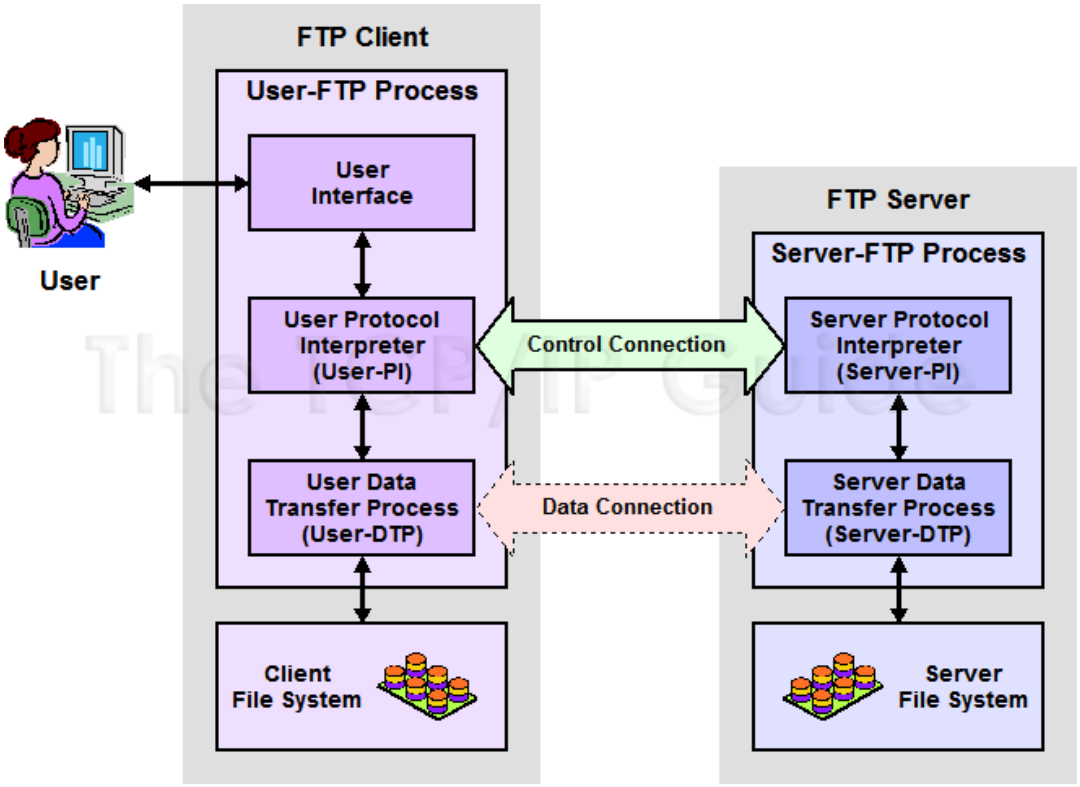
2. Kontrol koneksi FTP dan koneksi data

Konsep kritis dalam memahami FTP adalah bahwa seperti kebanyakan protokol lain yang menggunakan protokol transport TCP, ia tidak hanya menggunakan satu koneksi TCP melainkan menggunakan dua koneksi. Model FTP dirancang memerlukan dua kanal logik komunikasi antara proses server dan klien FTP:

a. **Kontrol koneksi**, Ini merupakan koneksi logikal TCP yang dibuat ketika sebuah sesi FTP diadakan. Ia memelihara throughput selama sesi FTP dan digunakan hanya untuk melakukan pertukaran informasi control, seperti perintah FTP dan jawabannya. Ia tidak digunakan untuk mengirim file-file.
b. **Koneksi data**, Setiap saat ketika data dikirimkan dari server ke klien atau sebaliknya, sebuah koneksi data TCP nyata dibangun di antara mereka. Data dikirimkan melalui koneksi data tersebut. Saat pengiriman file selesai, koneksi data ini dihentikan.

Alasan untuk menggunakan kanal-kanal yang berbeda ini adalah agar didapatkan keleluasaan bagaimana protokol FTP ini digunakan. Karena fungsi kontrol dan data dikomunikasikan melalui kanal yang berbeda, model FTP membagi perangkat lunak pada tiap peralatan menjadi dua komponen logikal protokol yang bertugas untuk masing-masing kanal. *Protocol interpreter (PI)* adalah bagian dari perangkat lunak yang mengatur koneksi berkaitan dengan pengiriman dan penerimaan perintah berikut jawabannya. *Data transfer process (DTP)* bertanggung jawab terhadap pengiriman dan penerimaan data antara klien dan server. Sebagai tambahan pada dua elemen di atas, pada proses FTP user ditambahkan komponen ketiga yakni antar muka user untuk berinteraksi dengan user FTP sebagai manusia, ia tidak ditambahkan pada sisi server. Sehingga terdapat dua komponen proses FTP server dan tiga komponen proses

FTP user pada keseluruhan proses FTP. Untuk lebih jelas perhatikan gambar …. beserta penjelasan fungsi masing-masing elemen berikut ini.



Gambar 3.4 Model Operasi FTP

3. Komponen-komponen proses FTP dan terminologi

a. Komponen-komponen proses FTP server

Proses FTP server terdiri dari dua elemen protokol:

1) **Server Protocol Interpreter (Server-PI)**: Juru bahasa/penghubung protocol yang bertanggung jawab untuk mengatur control koneksi pada server. Ia mendengarkan pada port khusus untuk FTP (port 21) untuk permintaan sambungan FTP yang masuk dari user (klien). Saat sebuah sambungan terjadi, ia menerima perintah dari User-PI, mengirim jawaban kembali dan mengelola proses transfer data server.

2) **Server Data Transfer Process (Server-DTP)**: DTP pada sisi server digunakan untuk mengirim atau menerima data dari atau ke User-DTP (biasanya port 20). Server-DTP mungkin tidak hanya membangun sebuah koneksi data atau mendengarkan suatu koneksi data yang dating dari user. Ia juga berinteraksi dengan file system server local untuk menulis dan membaca file-file.

b. Komponen-komponen proses FTP user

Proses FTP user terdiri dari tiga elemen protokol:

1) **User Protocol Interpreter (User-PI)**: Juru bahasa/penghubung protokol yang bertanggung jawab untuk mengatur kontrol koneksi pada klien. Ia menginisiasi sesi FTP dengan mengirimkan permintaan ke Server-PI. Saat sebuah sambungan terjadi, ia memroses perintah dari User-PI, mengirimkannya ke Server-PI dan menerima jawaban-jawaban kembali' Ia juga mengelola proses transfer data user.
2) **User Data Transfer Process (User-DTP)**: DTP pada sisi user digunakan untuk mengirim atau menerima data dari atau ke Server-DTP. User-DTP mungkin tidak hanya membangun sebuah koneksi data atau mendengarkan suatu koneksi data yang dating dari server. Ia juga berinteraksi dengan file system komponen-komponen local klien.
3) **User Interface**: Antar muka user menyediakan antar muka FTP yang lebih "friendly" untuk pengguna manusia. Ia memungkinkan penggunaan perintah fungsi FTP yang berorientasi pada pengguna ketimbang perintah internal FTP kriptik, dan juga memungkinkan untuk menyampaikan pada pengguna hasil dan informasi sesi FTP yang dilakukannya.

4. Menguji Konfigurasi FTP Server

FTP merupakan protokol standar dengan STD 9, dijelaskan pada RFC 959 – File Transfer Protocol (FTP) dan diupdate dengan RFC 2228 – FTP security extension. FTP dapat melakukan duplikat file secara dua arah dari komputer yang satu ke komputer lainnya atau sebaliknya. Client dapat mengirim file menuju server atau dapat meminta suatu file dari server. Untuk mengakses file di server, client diharuskan untuk mengidentifikasikan dirinya terlebih dahulu, kemudian server akan melakukan proses authentikasi untuk user atau pengguna tersebut.

FTP menggunakan koneksi berbasis connection-oriented, sehingga dari kedua sisi harus memiliki koneksi TCP/IP. FTP menggunakan TCP sebagai protokol transport. FTP server menerima koneksi pada port 21 dan 20. FTP server menggunakan dua port yang berbeda, satu digunakan untuk login dan memasukan perintah. Port lainnya digunakan untuk transfer File. Pada kedua sisi

jaringan, aplikasi FTP dilengkapi dengan protocol interpreter (PI), data transfer protocol (DTP), dan tampilan antar muka. Sehingga prinsip kerja protokol FTP adalah sebagai user interface melakukan perintah melalui PI dan dilanjutkan ke sisi server. Untuk melakukan transfer file PI memberikan perintah pada DTP untuk mengirimkan file.

5. Konfigurasi FTP Server

Ubuntu menggunakan vsftpd (Very Secure ftpd) untuk keperluan FTP server. vsftpd merupakan paket aplikasi yang bersifat free sehingga dapat didownload secara cuma-cuma. Untuk melihat apakah paket tersebut benar-benar telah terinstalasi ceklah dengan perintah :

a. Instalasi vsftp

   # apt-get install vsftpd

b. Untuk mengontrol vsftpd, cukup gunakan perintah sebagai berikut :

   # /etc/init.d/vsftpd start

   # /etc/init.d/ vsftpd stop

   # /etc/init.d/vsftpd restart

   vsftpd berisi beberapa buah file yang diantaranya bernama vsftpd. File ini merupakan file yang digunakan untuk mengaktifkan FTP server. vsftpd akan residen di memori selama server berjalan dan melayani client-client yang meminta layanan ftp. Dalam istilah teknis program-program yang bekerja dengan cara seperti ini disebut sebagai daemon.

c. Buka file konfigurasi VSFTPD default yang terdapat di /etc/vsftpd.conf dengan menggunakan perintah :

   sudo nano /etc/vsftpd.conf

d. Disable anonymous untuk mencegah anonymous user berhasil login

   anonymous_enable=NO

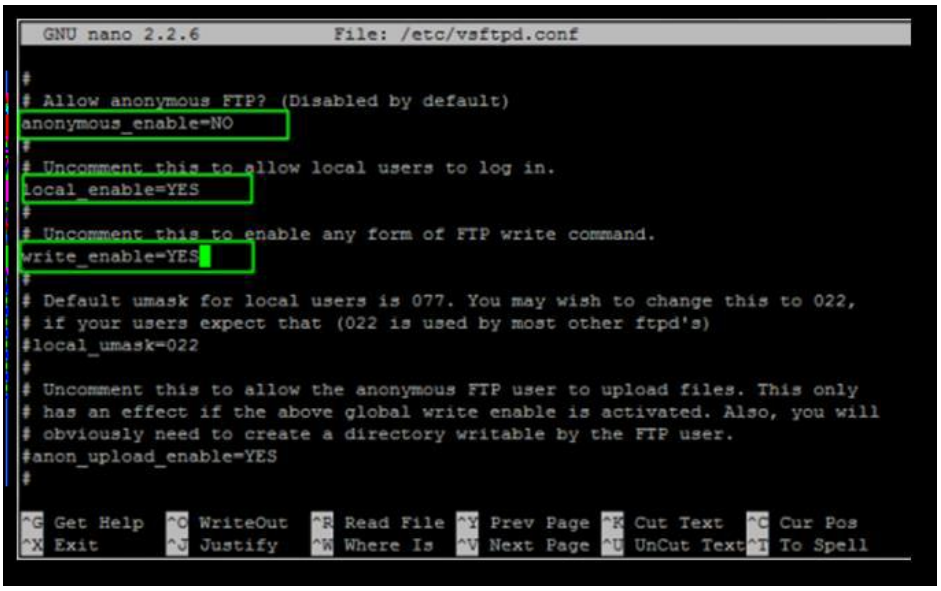
   Untuk mempermudah pencarian, gunakan CTRL+W dan masukan barisan kata atau kalimat konfigurasi yang dinginkan.

e. Selanjutnya mengaktifkan (enable) login user yang menggunakan file otentikasi lokal dengan menghilangkan tanda pagar sebelum :

   local_enable=YES

f. Agar user dapat melakukan modifikasi file system, perlu menghilangkan tanda pagar sebelum :

write_enable=YES



6. Menguji konfigurasi securing FTP Server

FTP sebenarnya cara yang tidak aman dalam mentransfer suatu file karena file dikirimkan tanpa di-enkripsi terlebih dahulu tetapi melalui clear text. Mode text yang dipakai untuk transfer data adalah format ASCII atau format binary. Secara default, FTP menggunakan mode ASCII dalam transfer data. Karena pengirimannya tanpa enkripsi, username, password, data yang di transfer, maupun perintah yang dikirim dapat di sniffing oleh orang dengan menggunakan protocol analyzer (sniffer). Solusi yang digunakan adalah dengan menggunakan SFTP (SSH FTP) yaitu FTP yang berbasis pada SSH atau menggunakan FTPS (FTP over SSL) sehingga data yang dikirim terlebih dahulu di enkripsi.

Konfigurasi Securing FTP:

a. Installasi Openssh

   ubuntu@linux:~$ sudo apt-get install openssh-server

b. Buat group baru **ftpaccess** untuk user FTP

   ubuntu@linux:~$ sudo groupadd ftpaccess

c. Konfigurasi */etc/ssh/sshd_config*

   Temukan *Subsystem sftp /usr/lib/openssh/sftp-server*

   Dan tambahkan kata berikut di akhir :

   Subsystem sftp internal-sftp

   Match group ftpaccess

   ChrootDirectory %h

X11Forwarding no

AllowTcpForwarding no

ForceCommand internal-sftp

d. Restart sshd service

ubuntu@linux:~$ sudo service ssh restart

Selanjutnya merupakan langkah untuk membuat users yang akan akses sftp

e. Buat user **smk** dengan group ftpaccess dan

*ubuntu@linux:~$ sudo useradd -m **smk** -g ftpaccess -s /usr/sbin/nologin*

*ubuntu@linux:~$ sudo passwd **smk***

f. Ganti kepemilikan dari home direktori

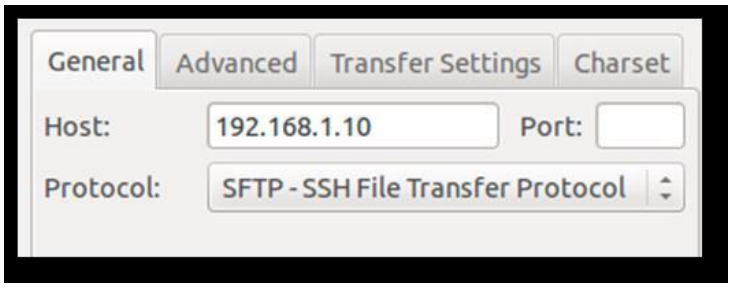
*ubuntu@linux:~$ sudo chown root /home/**smk***

g. Buat folder di dalam direktori home untuk mengganti kepemilikan dari folder tersebut

ubuntu@linux:~$ sudo mkdir /home/**smk**/www

ubuntu@linux:~$ sudo chown john:ftpaccess /home/**smk**/www

Sekarang cobalah untuk menghubungkan server menggunakan SFTP (port : 22) dan pastikan Pengguna dapat meng-upload file ke direktori www dan tidak dapat mengakses folder lain di luar direktori home.

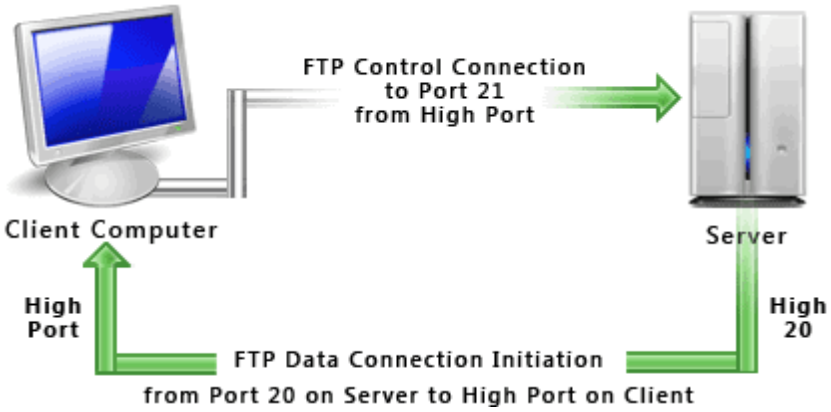


Gambar 3.5 Konfigurasi server

7. Aplikasi Penggunaan Protokol FTP

Seperti halnya sebagian besar hubungan klien-server lainnya, mesin klien membuka koneksi ke server pada port tertentu dan server kemudian merespon klien pada port tersebut. Ketika sebuah klien FTP terhubung ke server FTP membuka koneksi ke port kontrol FTP 21. Kemudian klien memberitahu server FTP apakah akan membangun koneksi aktif atau pasif. Jenis koneksi yang dipilih oleh klien menentukan bagaimana server merespon dan transaksi port akan terjadi.

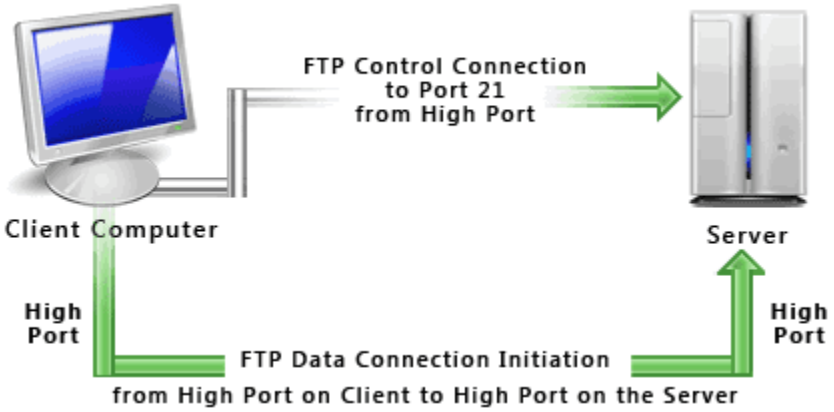
1) Koneksi aktif



Gambar 3.6 Koneksi FTP

Ketika sambungan aktif dijalankan, klien dari port tinggi mengirim permintaan ke port 21 pada server. Kemudian server membuka sambungan data ke klien dari port 20 ke range port tinggi pada mesin klien. Semua data yang diminta dari server kemudian dilewatkan melalui koneksi ini.

2) Koneksi pasif

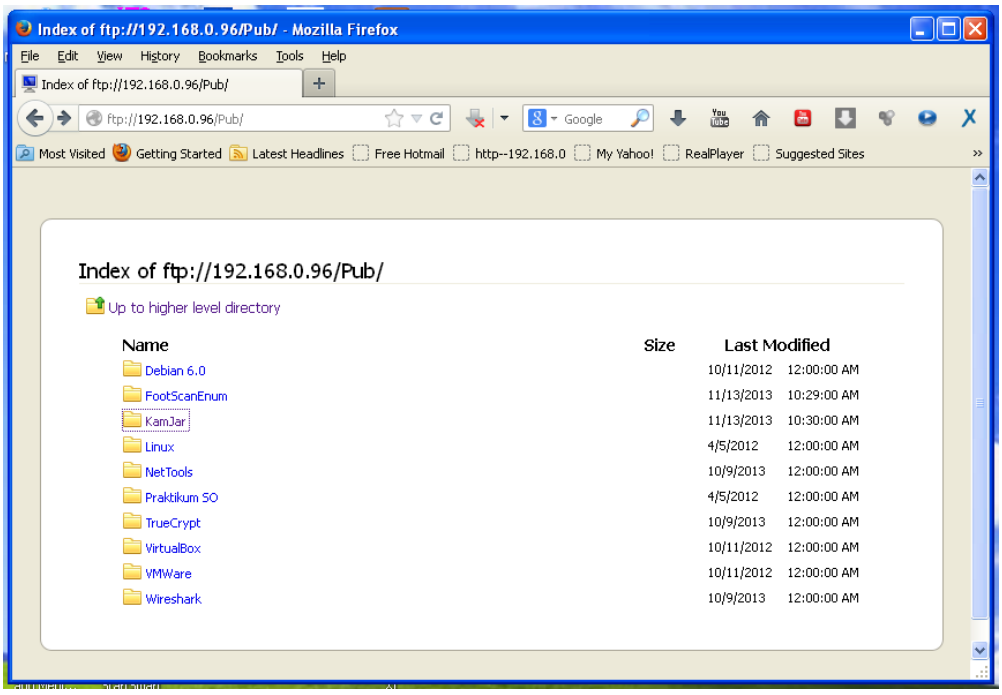


Gambar 3.7 Koneksi FTP Pasif

Ketika sambungan pasif (PASV) dijalankan, klien dari port tinggi mengirim ke port 21 pada server, klien meminta server FTP untuk membentuk koneksi port pasif, yang dapat dilaksanakan pada port yang lebih tinggi dari 10.000. Server kemudian mengikat ke port nomor tinggi untuk sesi khusus ini dan menyerahkan nomor port kembali ke klien. Klien kemudian membuka port baru yang telah disetujui untuk koneksi data.

Setiap data meminta klien untuk membuat hasil dalam koneksi data terpisah. Kebanyakan klien FTP modern mencoba untuk membuat sambungan pasif ketika meminta data dari server.

3) Pada sisi User



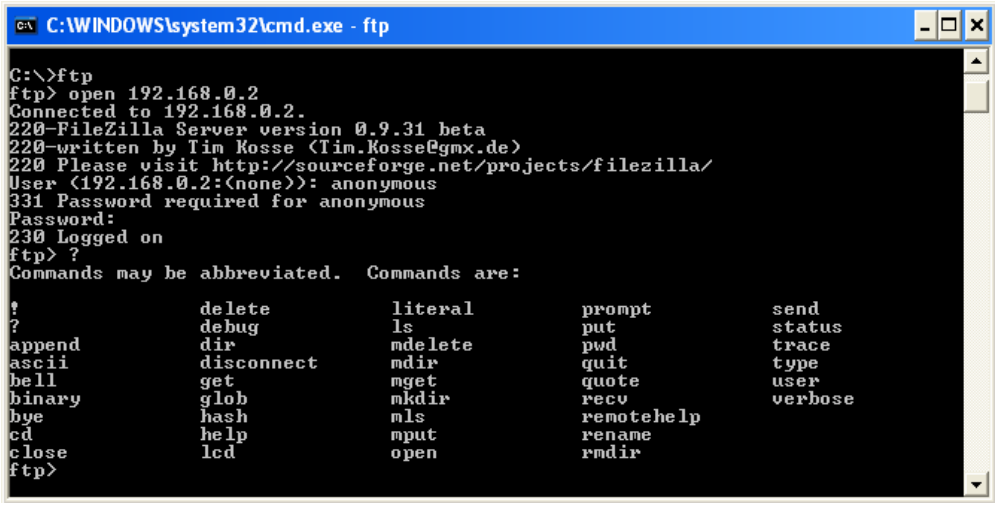
Gambar 3.8 Browser sebagai antar muka pengguna FTP

FTP merupakan cara paling umum untuk melakukan proses pemindahan file-file dari sebuah FTP server ke komputer pengguna, misalnya untuk mengunduh file dokumen, gambar, program maupun file-file image DVD installer Linux. Juga dapat melakukan pemindahan file-file dari komputer pengguna ke server misalnya untuk keperluan hosting web pengguna.

Jika hanya memerlukan untuk mengunduh file-file dari situs internet dapat pula dilakukan dengan menggunakan aplikasi browser sebagai antar muka pengguna. Aplikasi penggunaan protokol FTP di sisi user/pengguna dilakukan dengan menggunakan antar muka pengguna FTP klien untuk dapat memindah sejumlah file yang besar atau folder dengan lebih mudah dan efisien.

Sistem operasi yang saat ini banyak digunakan biasanya sudah dilengkapi dengan aplikasi FTP clent yang berbasis teks. Seperti

ditunjukkan pada Gambar di bawah ini adalah aplikasi FTP clent berbasis teks command DOS pada system operasi Windows.

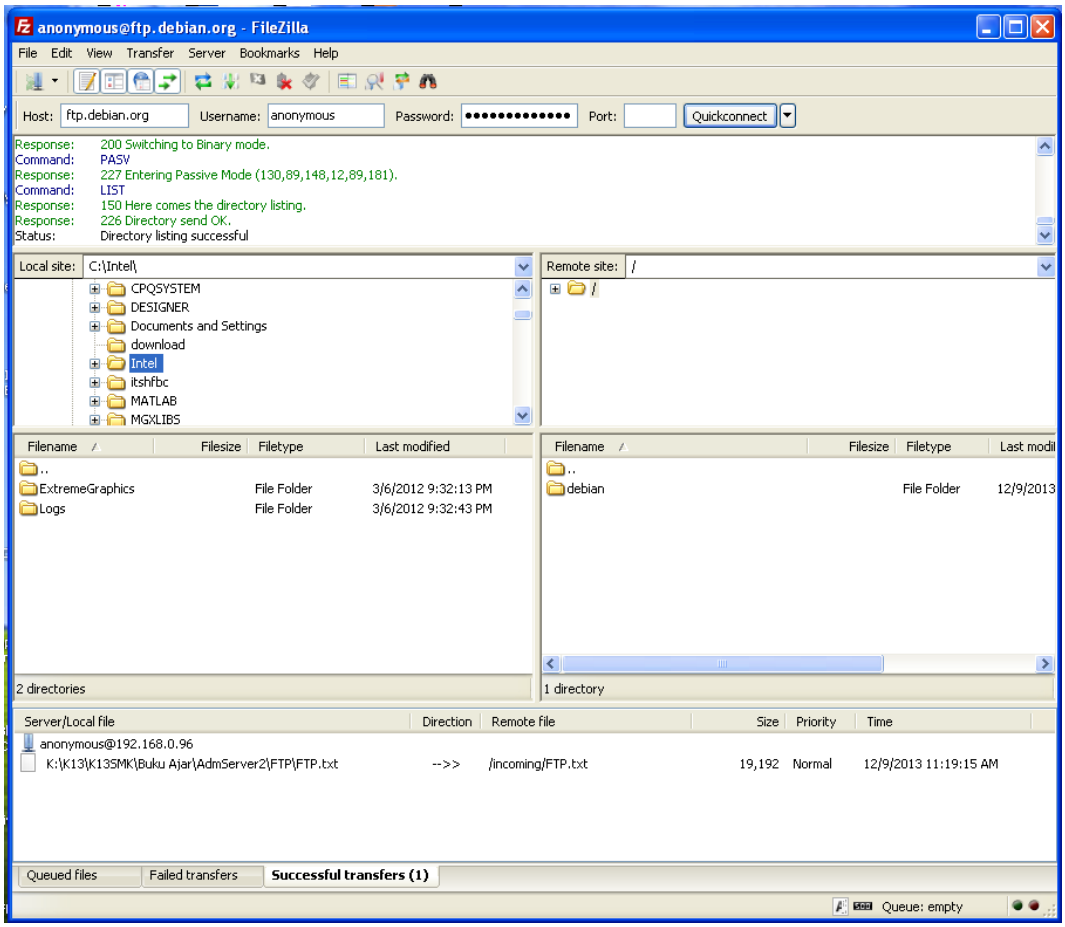


Gambar 3.9 Command DOS pada MS Windows sebagai antar muka pengguna FTP

Perintah untuk memulai aplikasi FTP klien adalah dengan mengetik C:> ftp maka prompt akan berubah menjadi ftp> jika ingin menghubungi server 192.168.0.2 dilakukan dengan mengetikkan ftp>open 192.168.0.2. Sebelum terjadi koneksi kita akan diminta menuliskan username dan password, sebagai user kebanyakan maka kita isikan username User <192.168.0.2:<none>>: anonymous kemudian Password: bambang@gmail.com (alamat email dan tidak terbaca waktu diketikkan). Jika berhasil maka server akan menjawab 230 Logged on lalu muncul prompt ftp> berarti saat itu kita sudah terkoneksi dengan Server FTP 192.168.0.2. Selanjutnya kita bisa melakukan aplikasi kirim terima file. Langkah memulai aplikasi FTP klien pada DOS (gambar 3) sama dengan yang dapat dilakukan pada terminal UNIX/Linux.

Terdapat banyak sekali aplikasi antar muka dari pihak ketiga (3rd party software) FTP klien tidak berbayar yang dapat diunduh dari situs-situs internet yang dapat diinstal pada system operasi komputer. Salah satunya adalah Filezilla yang mampu berjalan di atas system operasi Windows, Linux maupun Mac berbasis grafis dan dapat diunduh dari URL http://filezilla-project.org/ download.php. Antar muka FTP klien yang lain misalnya: WinFTP, FireFTP, FTPExplorer, CyberDuck, CuteFTP, dan

masih banyak lagi yang gratis maupun berbayar.Pada kebanyakan aplikasi antar muka FTP klien ditampilkan dengan bentuk grafis dan menampilkan proses koneksi data, direktori server FTP dan direktori komputer lokal.



Gambar 3.10 Klien FTP Filezilla sebagai antar muka pengguna FTP

Pada saat akan dimulai proses koneksi pengguna diwajibkan untuk masuk menggunakan username, untuk pengguna umum biasanya masuk dengan anonymous, lalu harus mengisikan password, biasanya berupa alamat email. Hal tersebut merupakan proses yang terjadi pada kanal port 21 kontrol koneksi aplikasi FTP. Setelah tersambung, baru dapat melakukan koneksi data, yakni proses kirim terima data pada kanal port yang lain. Karena proses kerja protokol FTP menggunakan dua kanal/port TCP.

4) Pada sisi Server

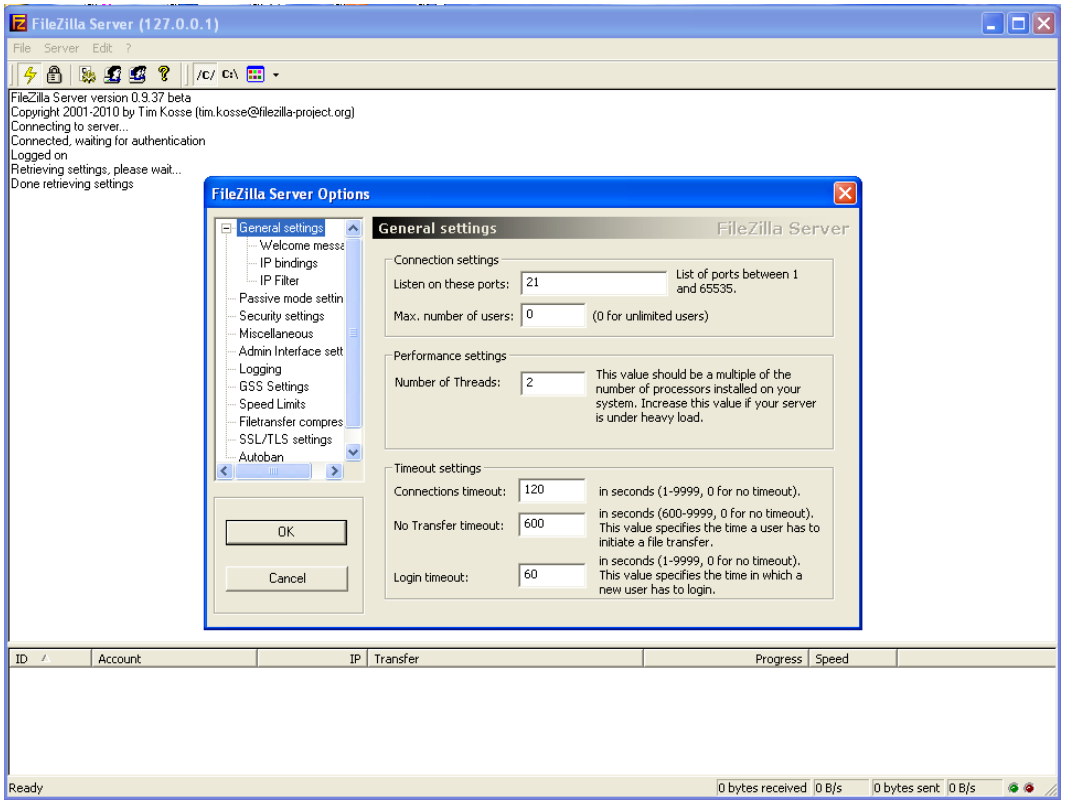
FTP server adalah suatu server yang menjalankan piranti lunak/software yang berfungsi untuk memberikan layanan tukar menukar file sehingga server tersebut selalu siap memberikan layanan FTP apabila mendapat permintaan (*request*) dari FTP klien. Port standar yang digunakan oleh Server FTP adalah 21. Ketika user mencoba untuk log in, server FTP menggunakan standar system panggilan untuk memeriksa username dan password dengan membandingkan yang ada pada file password system. Jika berhasil login dengan benar user diberi akses untuk masuk ke Server FTP, maka user/klien dapat men-mengunduh, mengunggah, mengganti nama file, menghapus file, dll sesuai dengan ijin/ *permission* yang diberikan oleh FTP server.

Tujuan dari FTP server adalah sebagai berikut :

a) Untuk tujuan sharing data, menyediakan indirect atau implicit remote computer
b) Untuk menyediakan tempat penyimpanan bagi user
c) Untuk menyediakan transfer data yang reliable dan efisien

Berbeda dengan antar muka FTP klien yang telah disediakan oleh system operasi kebanyakan dewasa ini, piranti lunak Server FTP harus diinstal dan dikonfigurasi sendiri. Kebanyakan piranti lunak Server FTP bisa didapatkan dengan gratis, mereka biasanya dibuat khusus untuk masing-masing platform system operasi. Demikian juga platform windows, system operasi tidak menyertakan aplikasi Server FTP di dalamnya, kita bisa mengaplikasikan server FTP di windows server dengan menginstal melalui menu Add Remove Program, Application Server, IIS (Internet Information Services) pada pilihan FTP Services. Sistem windows server akan menggunakan CD/DVD installer untuk melakukan instalasi server FTP hingga selesai dan server FTP siap untuk digunakan.

Piranti lunak aplikasi FTP server dari pihak ke-3 seperti Filezilla Server yang berbasis grafis juga dapat dinstal dan dioperasikan pada platform windows seperti gambar di bawah ini.



Gambar 3.11 FTP Server Filezilla pada SO Windows

Untuk platform SO Linux/UNIX server FTP standar / tradisional sudah disertakan di dalamnya yakni dapat dieksekusi melalui inetd (daemon superserver internet).

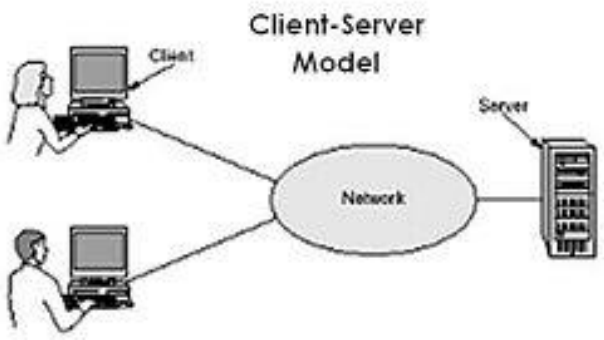
D. Remote Server

1. Konsep Server Remote

Server Remote adalah sebuah server yang didedikasikan untuk menangani pengguna yang tidak pada LAN tapi membutuhkan akses jarak jauh untuk itu. Remote akses server memungkinkan pengguna untuk mendapatkan akses ke file dan layanan cetak di LAN dari lokasi terpencil. Sebagai contoh, pengguna yang memanggil ke jaringan dari rumah menggunakan modem analog atau koneksi ISDN akan mendial ke server akses remote. Setelah pengguna dikonfirmasi ia dapat mengakses drive dan printer bersama seolah-olah ia secara fisik terhubung ke LAN kantor.

Kita dapat menggunakan misalnya perintah telnet untuk login secara remote ke sistem lain pada jaringan kita. Sistem ini dapat berada di jaringan area

lokal atau melalui koneksi internet. Telnet beroperasi seolah-olah kita sedang log in ke sistem lain dari remote terminal. Kita akan diminta untuk menggunakan nama login dan password. Akibatnya, kita login ke akun lain pada sistem lain. Bahkan, jika kita memiliki akun di sistem lain, kita bisa menggunakan Telnet untuk masuk ke dalamnya



Gambar 3.12 Klien-Server Model

2. Telnet

a. Server Telnet

Telnet adalah sebuah utilitas standar Internet dan berdasarkan protokol lihat (Request For Comment, RFC) 854. RFC ini menetapkan metode untuk transmisi dan menerima karakter ASCII tidak terenkripsi (plaintext) di dalam jaringan. Anda dapat menggunakan klien Telnet berjalan pada satu komputer untuk menghubungkan ke sesi berbasis baris perintah untuk menjalankan aplikasi. Hanya antarmuka berbasis karakter dan beberapa aplikasi yang didukung. Tidak ada kemampuan grafis di lingkungan Telnet. Telnet terdiri dari dua komponen: Telnet klien dan Telnet Server. Dokumen RFC yang mendefinisikan Telnet bisa didapatkan di *web Internet Engineering Task Force* (IETF).

Telnet Server melayani sesi remote untuk Telnet klien. Ketika Telnet Server aktif berjalan pada komputer, pengguna dapat terhubung ke server dengan menggunakan klien Telnet dari komputer remote. Telnet Server diimplementasikan di Windows sebagai layanan yang dapat dikonfigurasi untuk selalu aktif, bahkan ketika tidak ada orang yang login ke server.

Ketika klien Telnet terhubung ke komputer yang menjalankan Telnet Server, pengguna remote diminta untuk memasukkan nama pengguna dan kata sandi. Nama pengguna dan kombinasi sandi harus menjadi salah satu

yang berlaku pada Telnet Server. Telnet Server pada Windows mendukung dua jenis otentikasi: NTLM dan Password (atau plaintext).

Setelah login, pengguna dilayani dengan antar muka command prompt yang dapat digunakan seolah-olah hal itu telah dimulai secara lokal pada server konsol. Perintah yang anda ketik pada klien Telnet command prompt dikirim ke Telnet Server dan dieksekusi di sana, seolah-olah Anda secara lokal login untuk sesi command prompt di server. Output dari perintah yang Anda jalankan akan dikirim kembali ke klien Telnet sehingga mereka ditampilkan bagi Anda untuk melihat

Telnet tidak mendukung aplikasi yang memerlukan antarmuka grafis. Namun, Telnet Server dan Telnet Klien memahami karakter khusus yang menyediakan beberapa tingkat format dan posisi kursor dalam jendela Telnet klien. Telnet Server dan Telnet Klien mendukung emulasi dari empat jenis terminal: ANSI, VT-100, VT-52, dan VT-NT.

Pada Windows Server 2008, Anda dapat menginstal Telnet Server dengan menggunakan wizard Tambah Fitur di Server Manager. Meskipun Server Manager akan terbuka secara default ketika anggota dari grup Administrator masuk/log on ke komputer, Anda juga dapat membuka Server Manager dengan menggunakan perintah pada menu **Start** di **Administrative Tools**, dan dengan membuka **Programs** di **Control Panel**. Pada Windows Vista dan versi kemudian, Anda dapat menginstal Telnet Server (dan Telnet klien) dengan membuka **Control Panel**, kemudian **Programs**, dan kemudian Mengaktifkan fitur Windows atau menonaktifkan, **Turn Windows features on or off**.

Aplikasi telnet server juga dapat dijalankan di server dengan system operasi lain, misalnya UNIX dan beberapa distro LINUX lain.

b. Telnet klien

Implementasi Telnet awalnya gagal untuk operasi dupleks setengah (*half* duplex). Ini berarti bahwa lalu lintas data yang hanya bisa pergi dalam satu arah pada satu waktu dan memerlukan tindakan khusus untuk menunjukkan akhir dari lalu lintas satu arah sehingga lalu lintas sekarang

dapat mulai ke arah lain. [Ini mirip dengan penggunaan "*roger*" dan "*over*" oleh operator amatir dan radio CB.] Tindakan spesifik adalah dimasukkannya karakter GA (*go ahead*) dalam aliran data. Link modern sudah memungkinkan operasi dua arah (bi-directional) dan "menekan pergi ke depan" pilihan diaktifkan

Aplikasi utilitas telnet (klien) saat ini sudah disertakan dalam system operasi apa pun yang kita gunakan. Kita dapat menjalankan utilitas Telnet dengan mengetikkan kata telnet. Jika kita tahu nama situs yang ingin dihubungi, kita dapat memasukkan telnet dan nama situs pada baris perintah Windows command atau Linux.

Contoh implementasi aplikasi telnet pada windows command:

```
C:\>telnet
Microsoft (R) Windows NT (TM) Version 4.00 (Build 1381)
Welcome to Microsoft Telnet Klien
Telnet Klien Build 5.00.99034.1
Escape Character is 'CTRL+]'
Microsoft Telnet> open sfusrvr
**** Layar akan dibersihkan (clear) dan informasi berikut akan ditampilkan:
Microsoft (R) Windows NT (TM) Version 4.00 (Build 1381)
Welcome to Microsoft Telnet Service
Telnet Server Build 5.00.99034.1
login: sfu
password: ********
**** Layar akan dibersihkan (clear) dan informasi berikut akan ditampilkan:
*=================================================
Welcome to Microsoft Telnet Server.
*=================================================
C:\>
```

Selanjutnya kita bisa bekerja seolah-olah berada di mesin computer yang berhasil kita hubungi dengan aplikasi telnet. Akan tetapi meskipun bekerja pada konsol layar yang sama dengan aplikasi lain yang sedang kita jalankan di komputer kita, aplikasi telnet tetap merupakan pekerjaan di komputer lain (*remote machine*).

c. Secure Shell (SSH)

Telnet dan FTP adalah protokol yang terkenal tapi mereka mengirim data dalam format teks biasa, yang dapat ditangkap oleh seseorang dengan menggunakan sistem lain pada jaringan yang sama, termasuk Internet. Sehingga data yang dikomunikasikan dapat dengan mudah dibaca oleh orang, sehingga menjadi kurang aman untuk data-data penting yang harus dilindungi

Secure Shell (SSH) adalah sebuah protokol jaringan kriptografi (disandikan) untuk komunikasi data jarak jauh yang aman, dengan baris perintah login, perintah eksekusi jarak jauh, dan layanan jaringan lainnya antara dua jaringan komputer yang berhubungan, melalui saluran yang disandikan dan aman melalui jaringan tidak aman, server dan klien (masing-masing menjalankan server SSH dan program SSH klien,)

Aplikasi paling terkenal dari protokol adalah untuk akses ke akun shell pada sistem operasi mirip Unix, tetapi juga dapat digunakan dengan cara yang sama untuk akun pada Windows. Ia dirancang sebagai pengganti Telnet dan protokol remote shell tidak aman lainnya seperti Berkeley rsh dan rexec protokol, yang mengirim informasi, terutama password, berbentuk plaintext, membuat mereka rentan terhadap intersepsi dan pengungkapan menggunakan analisis paket. Enkripsi yang digunakan oleh SSH dimaksudkan untuk memberikan kerahasiaan dan integritas data melalui jaringan yang tidak aman, seperti Internet.

Dalam perjalanan pengembangan ssh, spesifikasi protokol membedakan antara dua versi utama yang disebut sebagai SSH-1 dan SSH-2. Perbedaannya terletak pada cara penyandian/enkripsi dan keduanya tidak saling mendukung. Pada tahun 2006, versi revisi dari protokol, SSH-2, diadopsi sebagai standar . Keamanan yang lebih baik, misalnya, karena menggunakan algoritma kriptografi Diffie-Hellman pertukaran kunci dan integritas yang kuat melalui kode otentikasi dalam memeriksa pesan. Fitur baru dari SSH-2 mencakup kemampuan untuk menjalankan sejumlah sesi shell melalui koneksi SSH tunggal.

OpenSSH (OpenBSD Secure Shell) adalah seperangkat program komputer yang menyediakan sesi komunikasi terenkripsi melalui jaringan komputer menggunakan protokol ssh. Hal ini dibuat sebagai alternatif open

source dibandingkan dengan aplikasi proprietary Secure Shell software suite yang ditawarkan oleh SSH Communications Security. OpenSSH dikembangkan sebagai bagian dari proyek OpenBSD, yang dipimpin oleh Theo de Raadt.

d. Server SSH

OpenSSH menggunakan hubungan server-klien. Sistem yang dihubungi disebut sebagai server. Sistem yang meminta sambungan disebut sebagai klien. Sebuah sistem sekaligus dapat menjadi server dan klien SSH. OpenSSH juga memiliki manfaat tambahan X11 forwarding dan port forwarding.

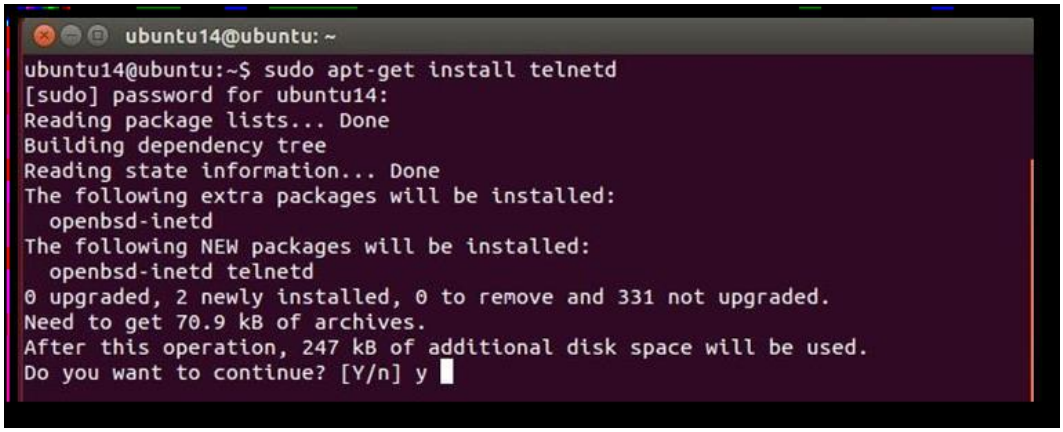
3. Menguji konfigurasi remote server (telnet, ssh)

Remote server adalah server yang diakses sebagai bagian dari proses client tanpa membuka koneksi terpisah, berbeda, ataupun langsung. Remote server dapat dilakukan dengan menggunakan telnet maupun ssh.

Telnet adalah singkatan dari Telecommunication Network merupakan protocol Client Server yang memfasilitasi akses remote login ke komputer host dalam sebuah jaringan komputer.

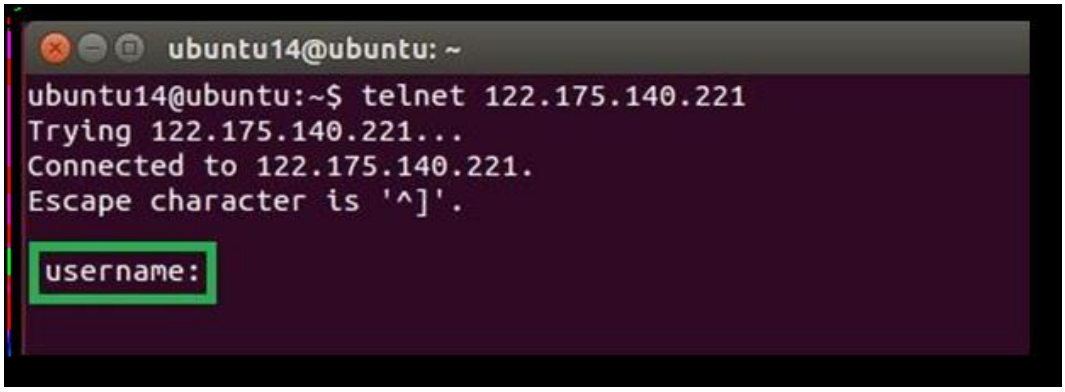
Untuk menginstall Telnet server dapat menggunakan perintah:

sudo apt-get install telnetd



Untuk uji coba remote server dengan telnet dapat menggunakan perintah:

*# telnet **ip_address***

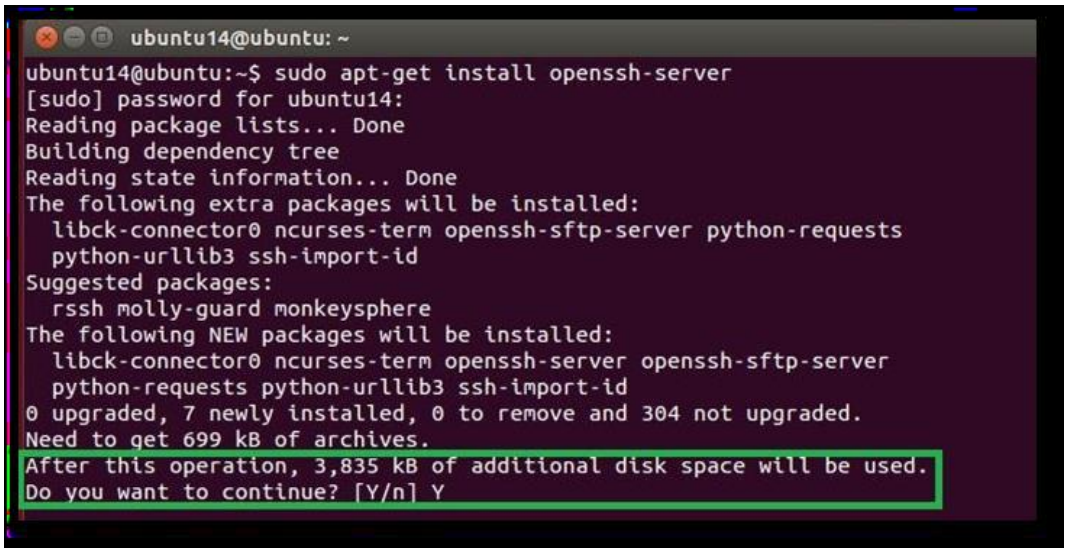


Masukkan username dan password server tersebut.

Selain menggunakan telnet, untuk remote server dapat menggunakan protokol SSH, protokol Secure Shell (SSH) merupakan sebuah protokol jaringan kriptografi untuk komunikasi data yang aman, login antarmuka baris perintah, perintah eksekusi jarak jauh, dan layanan jaringan lainnya antara dua jaringan komputer.

Untuk instalasi ssh gunakan perintah :

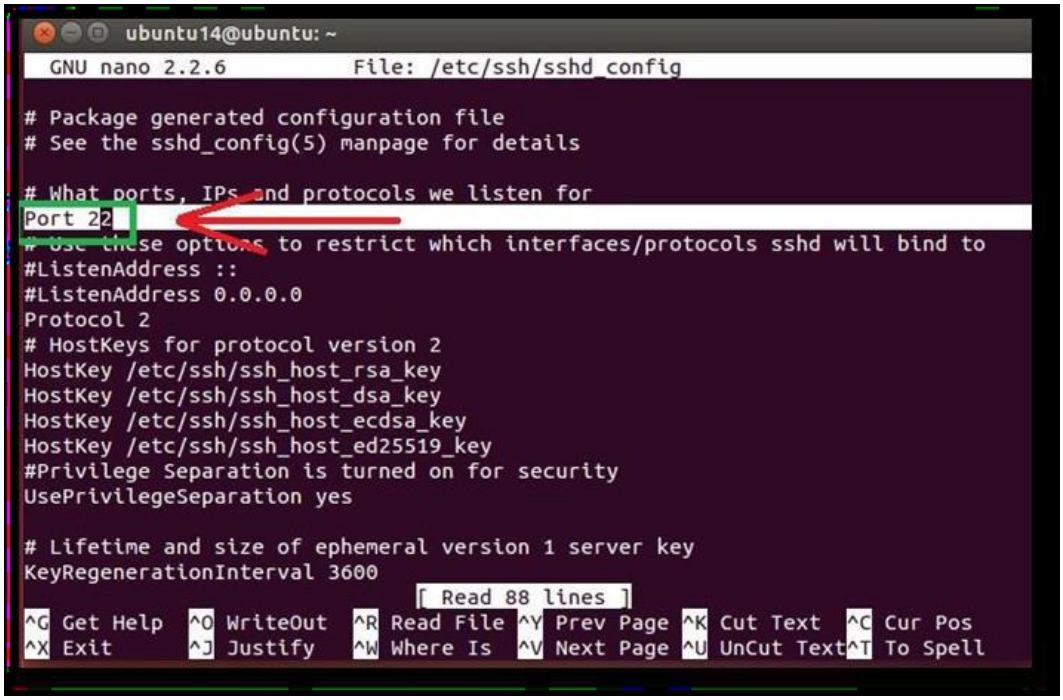
Sudo apt-get install openssh-server



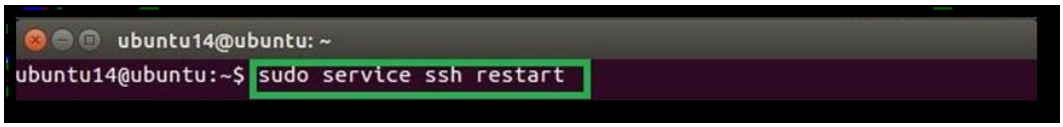
Untuk melakukan konfigurasi SSH dapat menggunakan perintah

sudo nano /etc/ssh/sshd_config

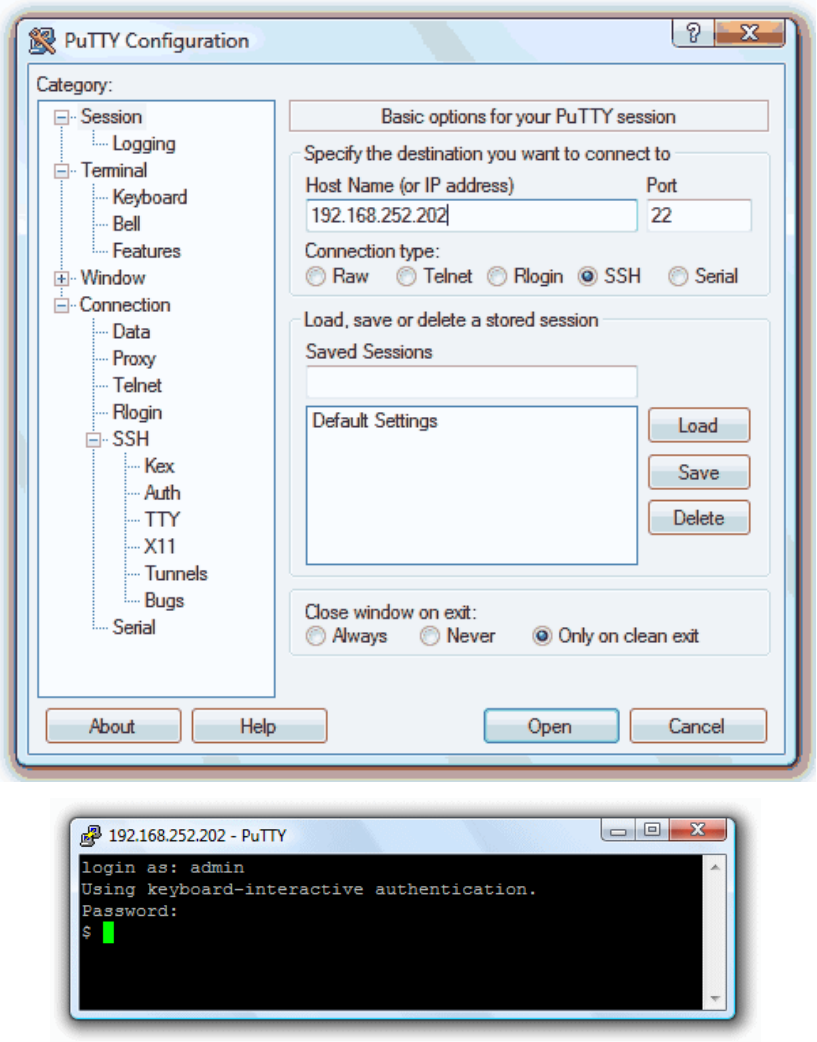
didalam konfigurasi ini port ssh dapat diganti agar keamanan lebih terjaga



Setelah selesai tekan *cntrl* + *x* , jika ada permintaan *save* maka pilih yes agar konfigurasi ssh tersimpan, langkah terakhit restart ssh dengan perintah seperti tertera pada gambar dibawah ini.



Untuk uji coba remote server dengan ssh dapat menggunakan tool putty:



Gambar 3.13 Tool Putty

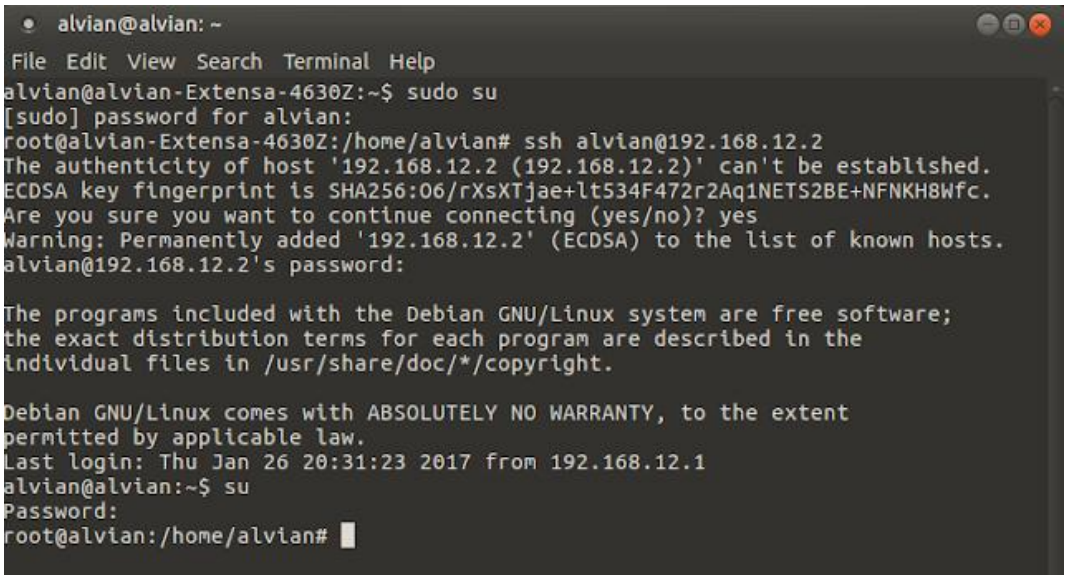
File server adalah sebuah komputer terpasang ke jaringan yang memiliki tujuan utama memberikan lokasi untuk akses disk bersama , yaitu penyimpanan bersama file komputer (seperti dokumen, file suara, foto, film, gambar , database, dll) yang bisa diakses oleh workstation yang melekat pada jaringan komputer yang sama. Server jangka menyoroti peran mesin di client-server skema, di mana klienworkstation menggunakan penyimpanan. Sebuah file server tidak dimaksudkan untuk melakukan tugas-tugas komputasi, dan tidak menjalankan program atas nama klien. Hal ini dirancang terutama untuk memungkinkan penyimpanan dan pengambilan data sementara perhitungan dilakukan oleh workstation.

Samba adalah perangkat lunak yang dapat dijalankan pada platform selain Microsoft Windows, misalnya, UNIX, Linux, IBM System 390, OpenVMS, dan

sistem operasi lain. Samba menggunakan protokol TCP / IP yang diinstal pada server host. Ketika dikonfigurasi dengan benar, hal itu memungkinkan host untuk berinteraksi dengan klien Microsoft Windows atau server seolah-olah itu adalah file dan print server Windows.

Cara instalasi file server:

1. Pastikan Pc / laptop sudah meremot Server



2. Langkah Pertama Instal sambanya terlebih dahulu #apt-get install samba

```
root@alvian:/home/alvian# apt-get install samba
```

3. Lalu anda konfigurasi data atau folder yang akan anda sharing disini folder yang akan saya sharing adalah /home/alvian/ , konfigurasinya : #nano /etc/samba/smb.conf

```
root@alvian:/home/alvian# nano /etc/samba/smb.conf
```

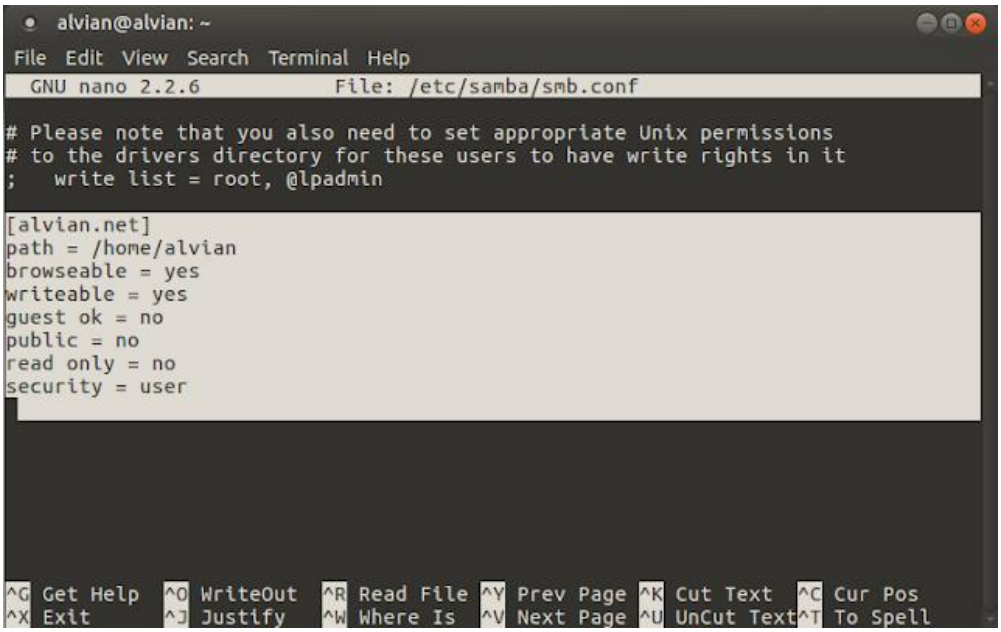
4. Pada bagian terbawah silahkan anda tambahkan beberapa baris berikut:

   [alvian.net]
   path = /home/alvian
   browseable = yes
   writeable = yes
   guest ok = no

public = no

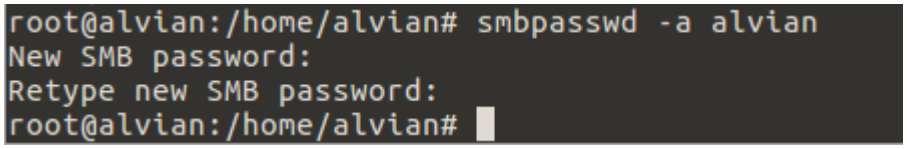
read only = no

security = user

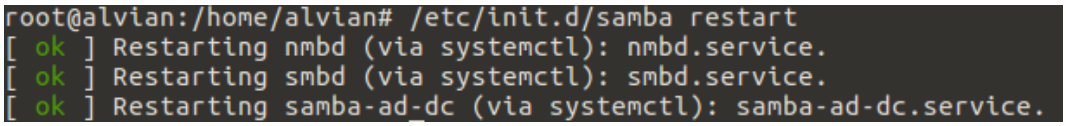


Kemudian simpan dengan menekan ctrl+x tekan y tekan enter

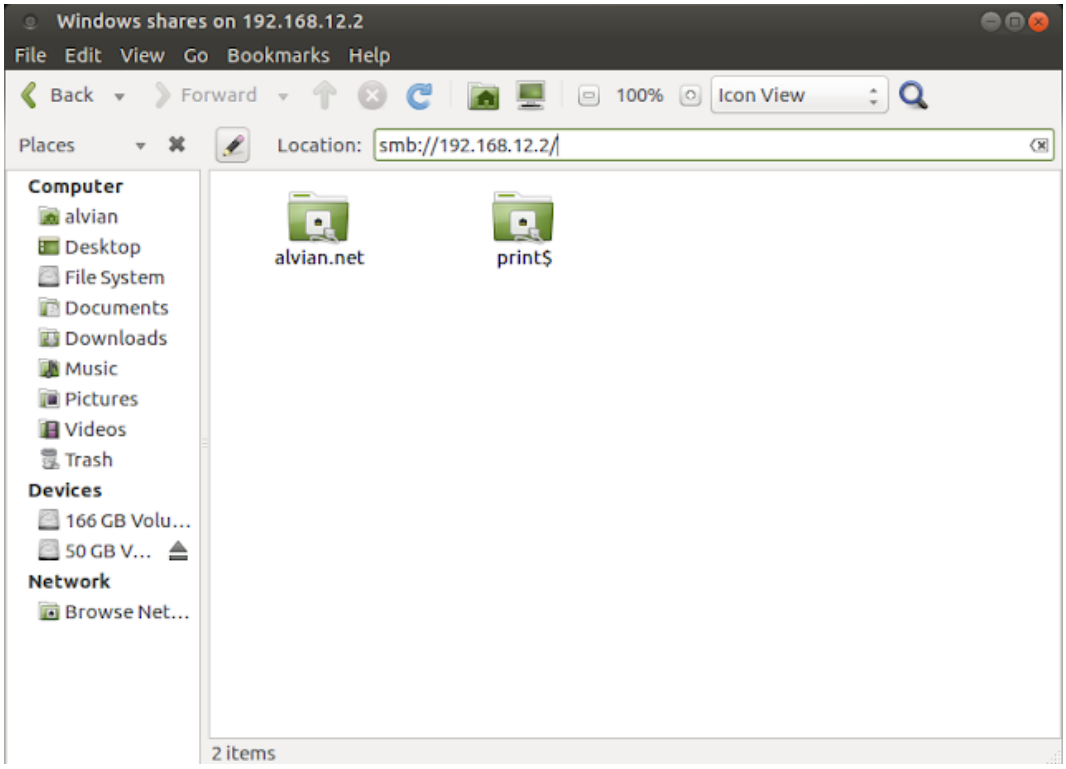
5. Setelah tersimpan silahkan anda masukan user untuk pengguna samba jika anda mengunakan user dengan perintah : #smbpasswd -a alvian



6. Kemudian restart service samba dengan perintah : #service samba restart, atau Jika Menggunakan Debian 8 Perintahnya : # /etc/init.d/samba restart



7. Kemudian periksa pada berkas apakah sudah berhasil dengan memasukan pada pencarian smb://ip address



E. Web Server

Server web atau yang dalam bahasa inggris disebut web server adalah merupakan perangkat lunak (software) dalam server yang berfungsi untuk menerima permintaan (request) berupa halaman web melalui protokol HTTP dan atau HTTPS dari client yang lebih dikenal dengan nama browser, kemudian mengirimkan kembali (respon) hasil permintaan tersebut ke dalam bentuk halaman-halaman web yang pada umumnya berbentuk dokumen HTML.

Dari pengertian diatas, dapat disimpulkan bahwa web server merupakan pelayan (pemberi layanan) bagi web client (browser) seperti Mozilla, Chrome, Internet Explorer, Opera, Safari dan lain sebagainya, supaya browser dapat menampilkan halaman atau data yang anda minta.

Fungsi utama dari web server adalah untuk mentransfer atau memindahkan berkas yang diminta oleh pengguna melalui protokol komunikasi tertentu. Oleh karena dalam satu halaman web biasanya terdiri dari berbagai macam jenis berkas seperti gambar, video, teks, audio, file dan lain sebagainya, maka pemanfaatan web server berfungsi juga untuk mentransfer keseluruhan

aspek pemberkasan dalam halaman tersebut, termasuk teks, gambar, video, audio, file dan sebagainya.

Pada saat anda ingin mengakses sebuah halaman website, biasanya anda mengetik halaman tersebut di browser seperti mozilla, chrome dan lain-lain. Setelah anda meminta (biasanya dengan menekan enter) untuk dapat mengakses halaman tersebut, browser akan melakukan permintaan ke web server.

Perangkat lunak yang berfungsi menerima permintaan HTTP ataupun HTTPS dari Klien yang dikenal dengan web browser dan mengirimkan kembali hasilnya dalam bentuk halaman-halaman web. Dan kini kita akan bahas cara konfigurasinya.

Langkah-langkahnya :

1. Instal Paket web server terlebih dahulu yaitu :

   apt-get install apache2

```
root@XIITKJ2:/etc/bind# apt-get install apache2_
```

2. Apabila ada konfirm Y/N, ketik **Y** lalu **Enter**
3. Selanjutnya kita masuk ke folder **/etc/apache2/sites-available**

   Ketikkan perintah : *cd /etc/apache2/sites-available*

```
root@XIITKJ2:/etc/bind# cd /etc/apache2/sites-available/_
```

4. Ketik *ls*, lalu copy file **default** dan kita ambil nama contohnya : **www** (nama bebas). Bisa juga langsung pakai file **default** tanpa mengcopy file master tersebut.

```
root@XIITKJ2:/etc/bind# cd /etc/apache2/sites-available/
root@XIITKJ2:/etc/apache2/sites-available# ls
default  default-ssl
root@XIITKJ2:/etc/apache2/sites-available# cp default www_
```

5. Lalu edit file **www**, perintah : *pico www*

```
root@XIITKJ2:/etc/apache2/sites-available# ls
default  default-ssl  www
root@XIITKJ2:/etc/apache2/sites-available# pico www_
```

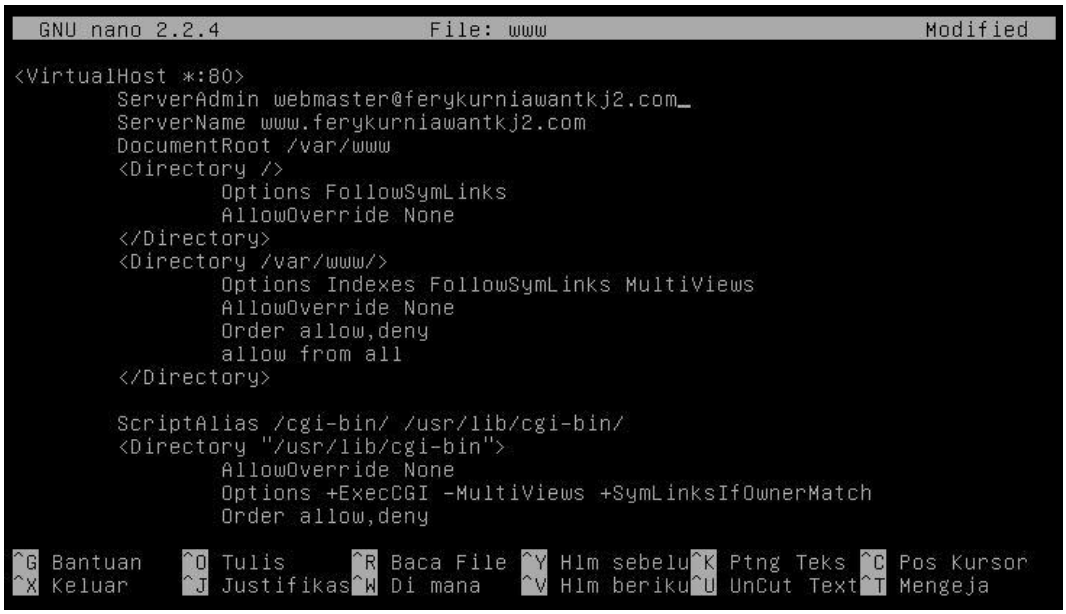
6. Pada file ini :

   Ganti : **ServerAdmin webmaster@localhos**t menjadi

   *ServerAdmin webmaster@**ferykurniawantkj2.com*(**nama domain anda**)

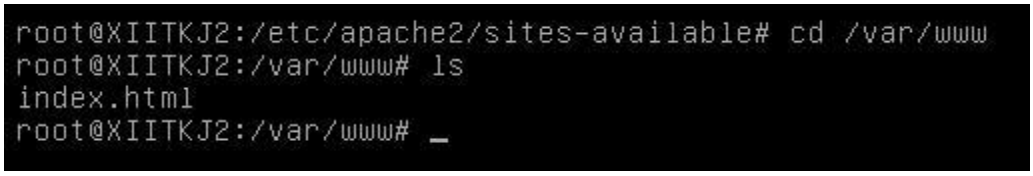
   Tambahkan : (dibawah ServerAdmin)

ServerName ***www.ferykurniawantkj2.com*** **(nama domain anda**)



7. Setelah selesai save file dengan CTRL-X, Y
8. Pindah direktori ke **/var/www** untuk mengedit file html dari web master tersebut

   cd /var/www



9. Lalu edit file **index.html,** masukkan perintah : *pico index.html*
10. Isikan script pada file ini sesuka hati anda, contohnya seperti gambar dibawah :

Save dengan CTRL-X, Y

11. Kemudian restart web server anda, masukkan perintah:

    /etc/init.d/apache2 restart
12. Dan untuk megecek apakah web server anda jalan atau tidak dengan perintah :

w3m www.ferykurniawantkj2.com **(Nama domain anda)**

```
root@XIITKJ2:/var/www# /etc/init.d/apache2 restart
Restarting web server: apache2apache2: Could not reliably determine the server's
 fully qualified domain name, using 127.0.1.1 for ServerName
 ... waiting apache2: Could not reliably determine the server's fully qualified
domain name, using 127.0.1.1 for ServerName
.
root@XIITKJ2:/var/www# w3m www.ferykurniawantkj2.com_
```

13. Hasilnya :

14. Apabila berhasil maka tampilannya seperti gambar diatas, dan menunjukkan web server anda berjalan dengan baik.

a. Menguji konfigurasi Web/HTTP Server

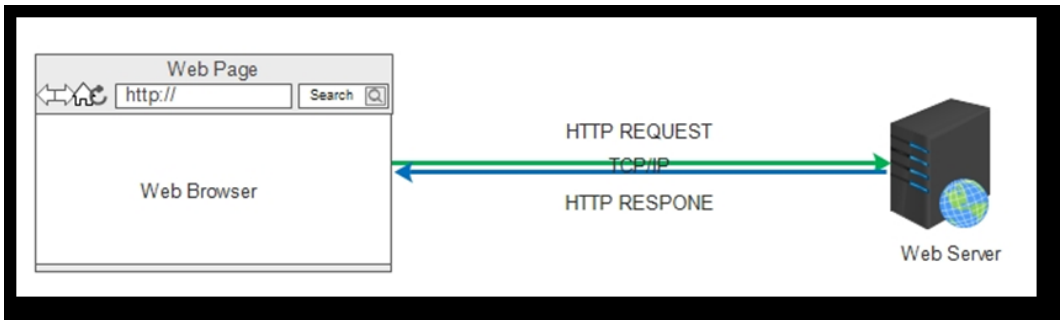
Beberapa contoh web server yang paling banyak digunakan diantaranya adalah Apache, Apache Tomcat, Microsoft Internet Information Services (IIS), Nginx, Lighttpd.

Fitur-fitur standar web server adalah HTTP, Logging, Virtual Hosting, Pengaturan Bandwidth, Otektifikasi, Kompresi Konten, HTTPS.

HTTP (Hypertext Transfer Protocol) adalah protokol yang digunakan oleh web server dan web browser untuk dapat berkomunikasi antara satu sama lain. Sedangkan HTTPS (Hypertext Transfer Protocol Secure) merupakan versi aman (secure) dari HTTP. Protokol HTTP menggunakan port 80 dan protokol HTTPS menggunakan port 443. Untuk mengenal dan membedakan keduanya, anda bisa

lihat pada saat anda mengakses suatu halaman website apakah berwalan http:// atau https://.

Cara kerja Web server pada dasarnya hanya ada 2 (dua), yaitu Menerima permintaan (request) dari client, dan Mengirimkan apa yang diminta oleh client (response).



Gambar 3.14 Cara Kerja Web Server

Penjelasan gambar :

1) client (user) akan meminta suatu halaman ke (web) server untuk ditampilkan di komputer client. Misalnya client mengetikkan suatu alamat (biasa disebut URL) di browser http://www.google.com. Client menekan tombol Enter atau klik tombol Go pada browser. Melalui media jaringan dan melalui protokol http, ini merupakan proses HTTP Request.
2) Webserver mendapat permintaan halaman utama google dari client, server akan mencari di komputernya halaman sesuai permintaan. Jika ditemukan, maka halaman yang diminta akan dikirimkan ke client, namun jika tidak ditemukan, maka server akan memberi pesan “404. Page Not Found”, yang artinya halaman tidak ditemukan, proses ini disebut dengan HTTP Respon.

Konfigurasi Web/HTTP Server :

1) Install Apache

   ubuntu@linux:~$ sudo su

   ubuntu@linux:~$ sudo apt-get install apache2
2) Instal database server (berfungsi sebagai penyedia layanan pengelolaan basis data dan melayani komputer atau aplikasi basis data yang menggunkan model client-server).

   ubuntu@linux:~$ sudo apt-get install mysql-server
3) Install PHP (bahasa pemrograman script, web yang bekerja disisi server)

   ubuntu@linux:~$ sudo apt-get install php5

4) Instal Mysql untuk apache

   ubuntu@linux:~$ sudo apt-get install libapache-mod-acct-mysql

   ubuntu@linux:~$ sudo apt-get install php5-mysql

5) Instalasi phpmyadmin

   ubuntu@linux ~$ sudo apt-get install phpmyadmin

b. Menguji konfigurasi securing Web / HTTP Server

Hypertext Transfer Protocol Secure (HTTPS) memiliki pengertian yang sama dengan HTTP hanya saja HTTPS memiliki kelebihan fungsi di bidang keamanan (secure). HTTPS menggunakan *Secure Socket Layer (SSL)* atau *Transport Layer Security (TLS)* sebagai sublayer dibawah HTTP aplikasi layer yang biasa. HTTP di enkripsi dan deskripsi dari halaman yang di minta oleh pengguna dan halaman yang di kembalikan oleh web server. Kedua protokol tersebut memberikan perlindungan yang memadai dari serangan eavesdroppers, dan man in the middle attacks. Pada umumnya port yang digunakan HTTPS adalah port 443. Tingkat keamanan tergantung pada ketepatan dalam mengimplementasikan pada browser web dan perangkat lunak server dan didukung oleh algoritma penyandian yang aktual. Oleh karena itu, pada halaman web digunakan HTTPS, dan URL yang digunakan dimulai dengan ‘https://’.

Administrator akan membuat sertifikat kunci publik untuk server web. Sertifikat ini dapat dibuat untuk server berbasis Linux dengan aplikasi seperti Open SSL yang ssl atau gensslcert SuSE. Sertifikat ini harus ditandatangani oleh otoritas sertifikat satu bentuk atau lain, yang menyatakan bahwa pemegang sertifikat adalah siapa yang mereka ajukan. Web browser pada umumnya didistribusikan dengan penandatanganan sertifikat otoritas sertifikat utama, sehingga mereka dapat memverifikasi sertifikat yang ditandatangani oleh mereka.

Bila menggunakan koneksi https, server akan merespon koneksi awal dengan menawarkan daftar metode enkripsi mendukung. Sebagai tanggapan, klien memilih metode sambungan, Klien dan sertifikat server melakukan pertukaran untuk otentikasi identitas mereka. Setelah dilakukan kedua belah pihak bertukar informasi terenkripsi. Sertifikat Kebanyakan diverifikasi oleh pihak ketiga sehingga klien yakin bahwa kuncinya adalah aman.

Konfigurasi HTTPS

1) Mengaktifkan mode ssl

   ubuntu@linux:~$ sudo a2enmod ssl

2) Selanjutnya kita restart apache

   ubuntu@linux:~$ sudo service apache2 restart

3) Buat sebuah folder untuk menyimpan server key dan sertifikat dan simpan di folder apache

   ubuntu@linux:~$ sudo mkdir /etc/apache2/ssl

4) Bagian ini adalah bagaimana membuat Sertifikat SSL

   ubuntu@linux:~$ openssl req -x509 -nodes -days 730 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt

Output dari perinta di atas:

You are about to be asked to enter information that will be incorporated into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [AU]:ID
State or Province Name (full name) [Some-State]:Medan
Locality Name (eg, city) []:MDN
Organization Name (eg, company) [Internet Widgits Pty Ltd]:smk
Organizational Unit Name (eg, section) []:network
Common Name (e.g. server FQDN or YOUR name) []:universitas.com
Email Address []:smk@gmail.com

5) Komponen apache yang menunjukkan dimana letak website disimpan ada pada file default berada di /etc/apache2/sites-available/default. Itu adalah salah satu komponen apache yang menunjukkan letak alamat website. Secara default file ini merujuk ke /var/www/. Didalam /etc/apache2/sites-available/ terdapat 2 file, yang satu adalah file default dan yang kedua adalah default-ssl.

   Buka File default-ssl

   ubuntu@linux:~$ sudo nano /etc/apache2/sites-available/default-ssl

   <VirtualHost _default_:443>

   ServerAdmin webmaster@localhost

   ServerName www.smk.com

   DocumentRoot /var/www/www2

   # Tambahkan baris ini di file default-ssl

SSLEngine On

SSLCertificateFile /etc/apache2/ssl/apache.crt

SSLCertificateKeyFile /etc/apache2/ssl/apache.key

Selanjutnya cari baris ini dan berikan tanda comment (#):

 # SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem

 # SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key

Save lalu exit.

6) Aktifkan website default-ssl.

ubuntu@linux:~$ Sudo a2ensite default-ssl

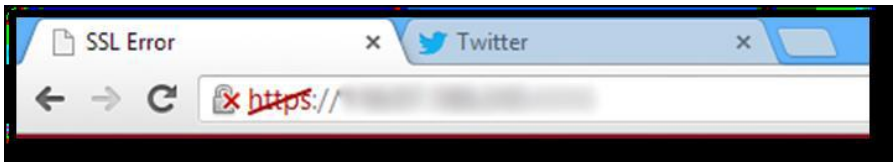
7) Baiklah semuanya telah selesai, sekarang restart apache kita.

Sudo service apache2 restart

8) Selesai

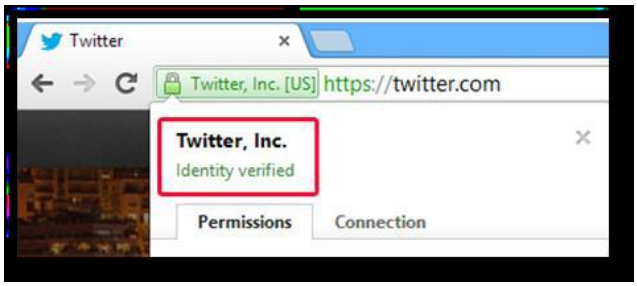
Ada perbedaan diantara sertifikat yang gratis, dan yang berbayar sekaligus verified. Perbedaan ini sangat jelas ketika kita pertama kali membuka url tersebut di browser kita.

Untuk yang gratis buatan kita sendiri, akan tampil seperti ini :



Gambar 3.15 Tampilan menggunakan fitur gratis pada browser

Untuk yang berbayar dan verified akan tampil seperti ini :



Gambar 3.16 Tampilan menggunakan fitur berbayar pada browser

F. DNS Server

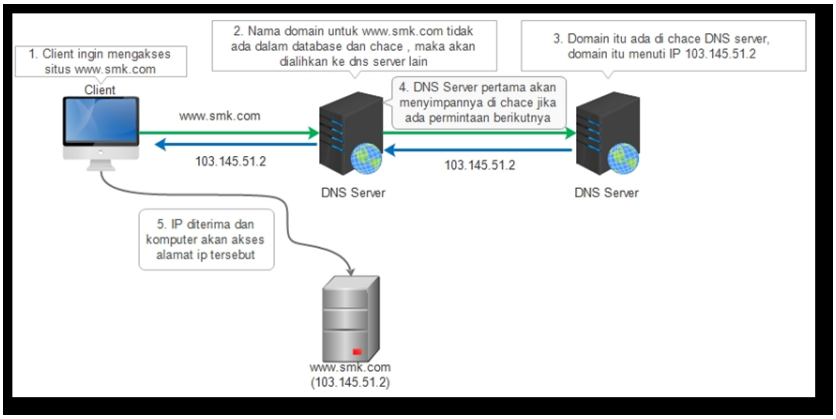
DNS server merupakan salah satu komponen penting saat ini dalam sistem internet. Keberadaannya sangat membantu dalam mengakses berbagai layanan di internet, mulai dari situs berita, publikasi karya ilmiah, jejaring sosial dan masih banyak lagi manfaat lainnya. Kesemua layanan tersebut dapat diakses dengan

mudah karena memiliki nama yang yang dapat diingat oleh user. Server DNS memegang peranan penting untuk menjaga kaitan antara nama dengan komputer server tujuan aplikasi internet. Apabila ada permasalahan dalam server DNS akan menyebabkan akses ke suatu sumber daya di internet akan terganggu.

1. Menguji konfigurasi DNS server

DNS adalah singkatan dari *Domain Name Server*, yaitu sebuah sistem yang menyimpan semua informasi data dari domain atau hostname dalam sebuah jaringan. tanpa adanya DNS, maka domain tidak bisa mentranslate atau menerjemahkan domain ke alamat IP. DNS Server merupakan server yang menyimpan DNS tersebut.

Cara kerja DNS server dapat dilihat seperti gambar dibawah ini :



Gambar 3.17 Proses Kerja DNS Server

a. Komputer akan request alamat ip website ke server DNS lokal
b. Server DNS lokal akan melihat ke dalam database dan cache nya
c. Jika cache ditemukan maka server DNS akan langsung memberikan ip ke aplikasi browser. jika tidak ditemukan maka server DNS lokal akan menghubungi DNS server lainnya
d. Setelah mendapatkan alamat IP, DNS Server lokal akan menyimpannya sebagai cache sehingga jika ingin akses ke alamat yang sama maka DNS server tidak perlu menghubungi DNS server lainnya. permintaan ke DNS lain hanya terjadi jika di DNS server lokal tidak ditemukan data atau cache nya.
e. Alamat IP di berikan ke browser sehingga browser dapat membuka website yang di publikasikan di IP tujuan.

Konfigurasi DNS Server dapat dilakukan dengan perintah:

 # apt-get install bind9

Untuk Konfigurasi DNS dapat dilakukan dengan perintah:

 # gedit /etc/bind/named.conf

Edit file named.conf , pada contoh ini menggunakan IP 192.168.1.100 dengan domain universitas.com. Membuat konfigurasi domain : db.universitas pada directory /etc/bind, sebelum membuatnya diharuskan mengcopy file db.local menjadi db.universitas, dengan cara :

 # cp /etc/bind/db.local /etc/bind/db.universitas

Selanjutnya edit file db.universitas, dengan cara:

 # nano /etc/bind/db.universitas

Selanjutnya membuat konfigurasi resolver , copy file db.127 menjadi db.universitas.rev dengan cara, ketik:

 # cp /etc/bind/db.127 /etc/bind/db.universitas.rev

lalu ubah file db.universitas.rev, ganti localhost dengan nama domain, dan ip 127.0.0.1 ganti dengan ip anda, ketik perintah :

 # nano /etc/bind/db.universitas.rev

Lalu save,

Langkah terakhir yaitu :

mengedit konfigurasi DNS pada resolv.conf , ketik :

` *# gedit /etc/resolv.conf*

lalu ganti DNS nameservernya menjadi IP anda :

*nameserver **192.168.1.100***

restart DNS server, ketik :

 # /etc/init.d/bind9 restart

Uji coba bisa dilakukan dengan web browser

Gambar 3.18 Ujicoba konfigurasi DNS Server

Pemeriksaan dns juga dapat dilakukan dengan perintah

 # nslookup universitas.com

2. Memperbaiki dan memastikan kondisi server DNS

Saat ini banyak server internet yang dibangun menggunakan UNIX/Linux sebagai basisnya sedangkan BIND merupakan aplikasi server DNS yang saat ini paling banyak digunakan pada sistem UNIX/Linux. Berikut ini merupakan kegiatan yang dapat dilakukan untuk memperbaiki dan memastikan kondisi server DNS selalu dalam keadaan optimal.

a. Pastikan Port DNS Dalam Keadaan Terbuka

Secara default aplikasi BIND mendengarkan request dari klien pada port 53. Sehingga pastikan port tersebut dalam keadaan terbuka dan layanan DNS-nya dalam keadaan aktif. Cek status port 53 menggunakan aplikasi telnet dengan format perintah berikut.

telnet alamat-server-dns 53 atau *telnet alamat-server-dns domain*

Contoh:

telnet 192.168.55.68 domain

Apabila berhasil akan menampilkan tulisan seperti berikut.

Trying 192.168.55.68...

Connected to ns1.kdebian.org.

Escape character is '^]'.

Cara lain untuk mengetahui apakah port 53 sedang aktif dapat dengan perintah netstat berikut.

netstat -tulpn | grep 53

atau

netstat -atve

Agar lebih yakin bahwa port DNS dapat digunakan, pastikan firewall di server membuka akses ke port 53. Gunakan perintah berikut ini menampilkan daftar aturan firewall iptables.

iptables –L –n

Pastikan juga bahwa layanan server DNS dalam keadaan aktif dengan menggunakan perintah status berikut ini.

/etc/init.d/bind9 status

Apabila belum diaktifkan, aktifkan dengan menggunakan perintah berikut.

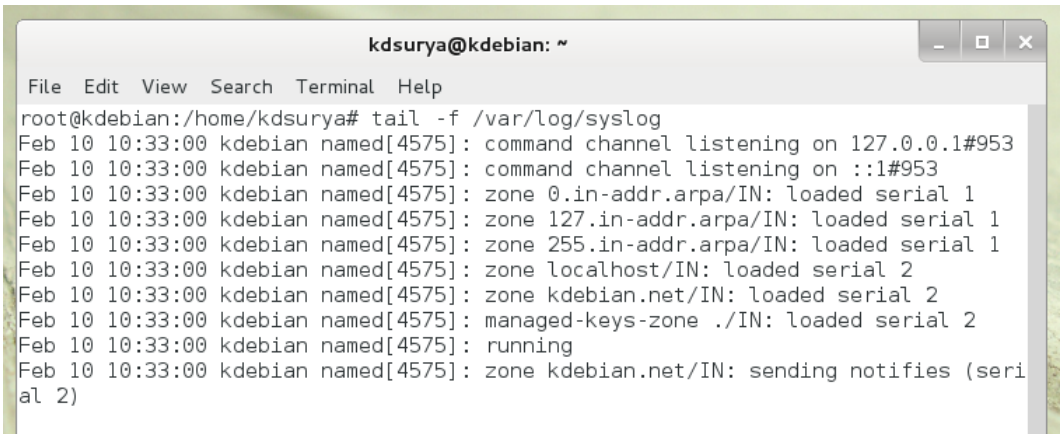
/etc/init.d/bind9 start atau /etc/init.d/bind9 restart

b. Cek Log DNS

Hampir semua layanan yang ada pada sistem UNIX/Linux memiliki file log yang berisikan catatan kegiatan-kegiatan yang telah dilakukan oleh layanan tersebut. Demikian juga dengan server DNS, apabila terdapat permasalahn dalam layanan ini pesannya akan disimpan dalam file log tersendiri. Gunakan perintah berikut untuk membaca file log server DNS segera setelah server diaktifkan.

tail -f /var/log/syslog

Contoh output dari perintah ini adalah.



Gambar 3.19 Contoh hasil pembacaan file /var/log/syslog

c. Validasi konfigurasi DNS

Kegiatan terakhir yang dapat dilakukan terkait dengan perbaikan server DNS ini adalah dengan melakukan validasi kesesuaian konfigurasi DNS dengan standar yang digunakan BIND. Berikut ini adalah perintahnya.

named-checkconf /etc/bind/named.conf

Hasilnya, apabila mengalami kesalahan akan menampilkan tulisan seperti beriku

/etc/bind/named.conf:11: missing ';' before 'include'

Sebagai catatan, apabila tidak ada kesalahan dalam konfigurasi BIND, tidak ada keluaran yang diberikan oleh perintah diatas.

d. Uji Fungsionalitas Server DNS

Terdapat sejumlah aplikasi yang dapat digunakan untuk menguji fungsionalitas server DNS, diantaranya adalah:

host

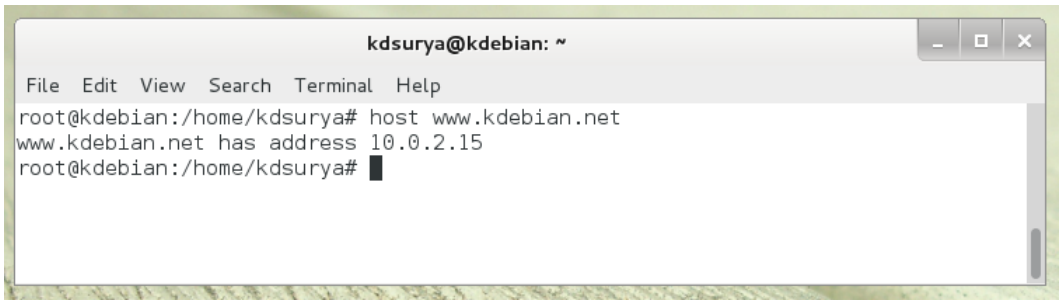
Format perintahnya:

host nama-domain

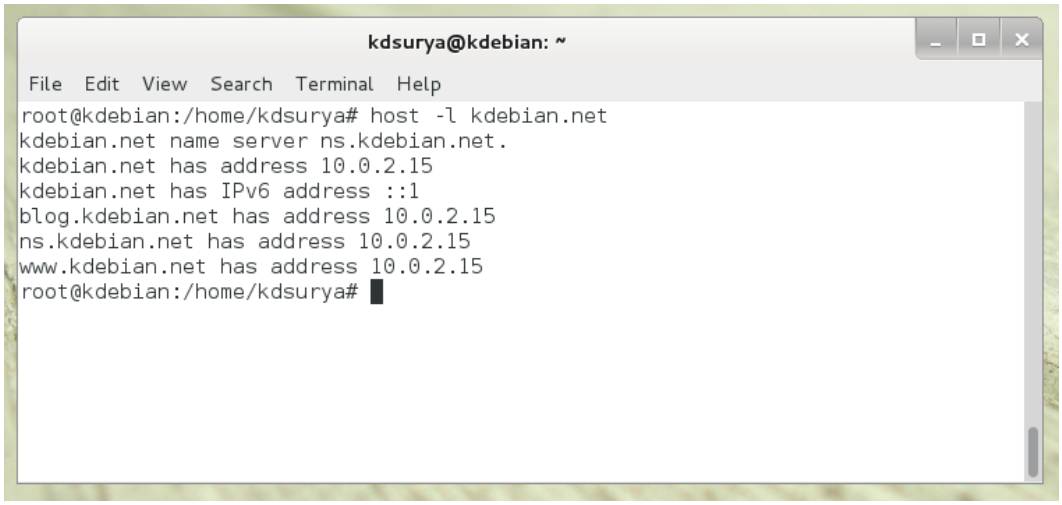
host alamat-ip

contoh:

host www.kdebian.net



host –l kdebian.net



dig

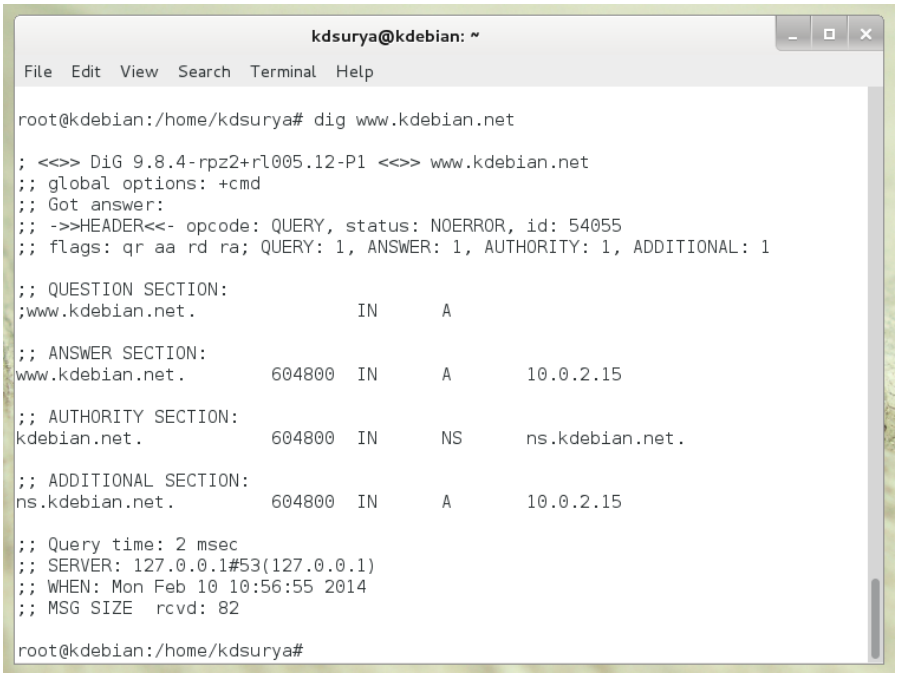
Format perintahnya:

dig nama-domain

dig alamat-ip

contoh:

dig www.kdebian.net



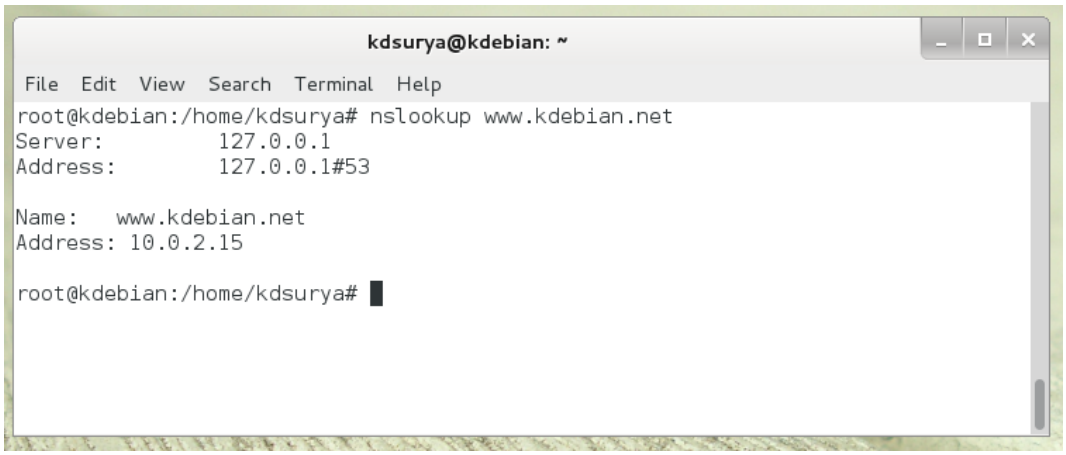
nslookup

Format perintahnya:

nslookup nama-domain

nslookup alamat-ip

Contoh:



e. Perbaikan Pada Sisi Klien

Selain pada sisi server permasalahan DNS juga dapat terjadi pada komputer klien sebagai pengguna dari layanan DNS ini. Perintah berikut ini dapat digunakan untuk mengatur ulang (reset) konfigurasi DNS yang diterima dari server.

Perintah	Penjelasan
Windows: ipconfig /release ipconfig /renew	Perintah ipconfig /release digunakan untuk menghapus semua konfigurasi jaringan pada suatu adapter (kartu jaringan), sedangkan parameter /renew untuk meminta kembali konfigurasi jaringan untuk suatu adapter dari server DHCP.
Linux: dhclient –r <kartujaringan> dhclient <kartujaringan> contoh: dhclient –r eth0 dhclient eth0	Ini merupakan perintah untuk menghapus konfigurasi DHCP yang diterima. Berikutnya perintah kedua digunakan untuk meminta konfigurasi DHCP yang baru dari server. Perintah ini pada Linux Debian dijalankan melalui user root.

Langkah ini sangat berguna saat konfigurasi server DHCP dan DNS mengalami perubahan. Dengan melakukan perintah ini komputer klien akan dapat menerima konfigurasi yang baru tersebut.

G. Database Server

Server basis data adalah sebuah program komputer yang menyediakan layanan pengelolaan basis data dan melayani komputer atau program aplikasi basis data yang menggunakan model klien/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.

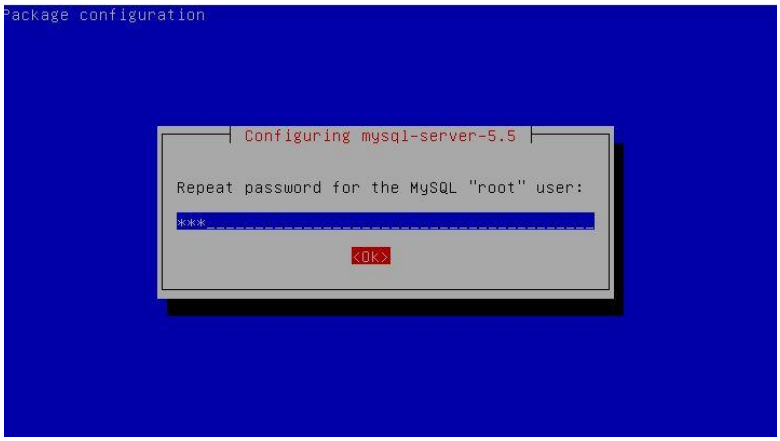
1. Penginstalan

   Pertama install dulu aplikasi mysql dengan perintah

   #sudo apt-get install mysql-server mysql-client

Setelah itu kalian harus memasukkan password "root" di aplikasi mysql

Setelah itu kalian akan di perintah untuk memasukkan password "root" mysql yang tadi



Setelah itu Proses Instalasi Mysql telah selesai

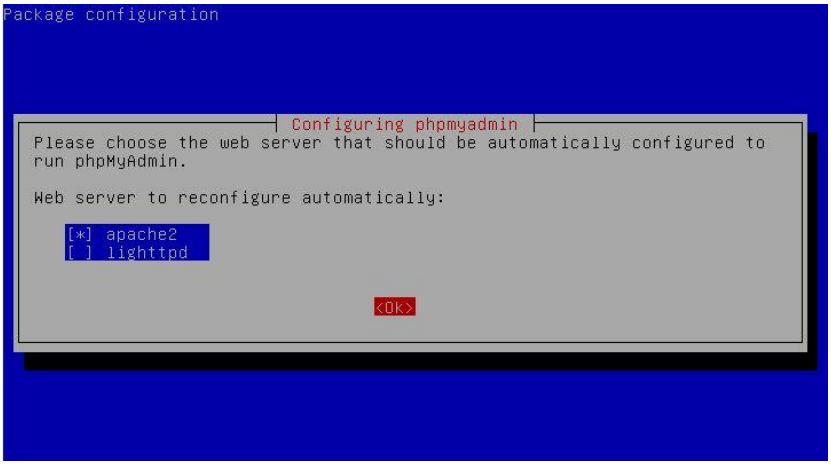
2. Cara menggunakan Database Server dengan mengetikkan perintah
   #mysql -u root -p
   lalu masukkan password root mysql tadi dan akan muncul tulisan seperti dibawah ini:

   Welcome to the MySQL monitor. Commands end with ; or \g.

   Your MySQL connection id is 43
   Server version: 5.5.31-0+wheezy1 (Debian)
   Copyright (c) 2000, 2013, 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>

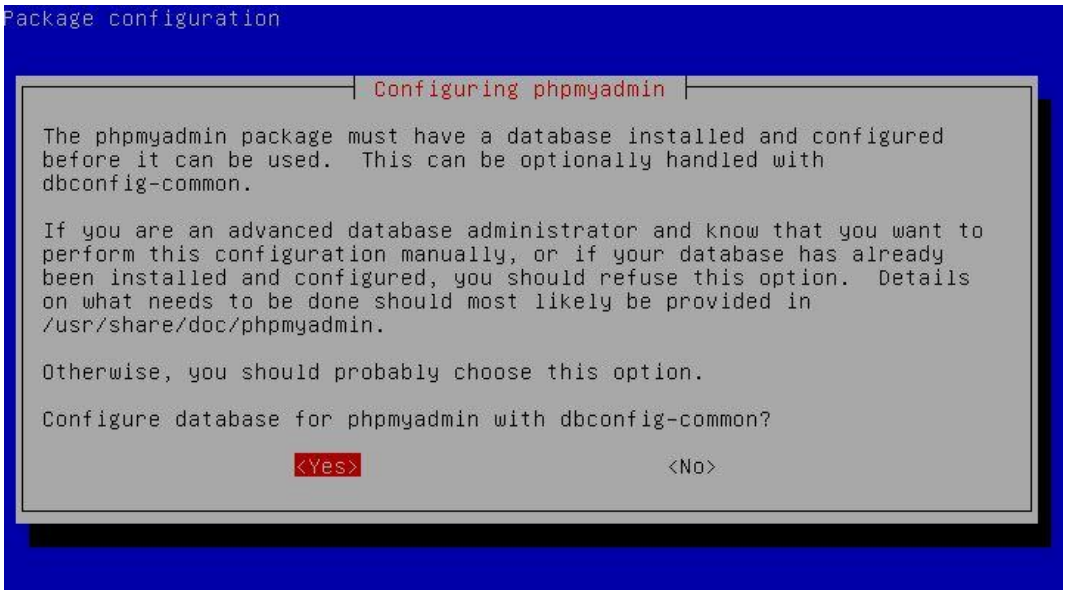
Jika kita ingin mengelola Database Server dengan menggunakan GUI maka kita harus menginstal aplikasi phpmyadmin untuk mengelola dengan web browser.

1. Pertama kita install aplikasi phpmyadmin dengan mengetikkan perintah
   #apt-get install phpmyadmin
2. Setelah itu akan muncul seperti gambar di bawah ini



Pilih apache2 dengan tekan spasi di tulisan apache2

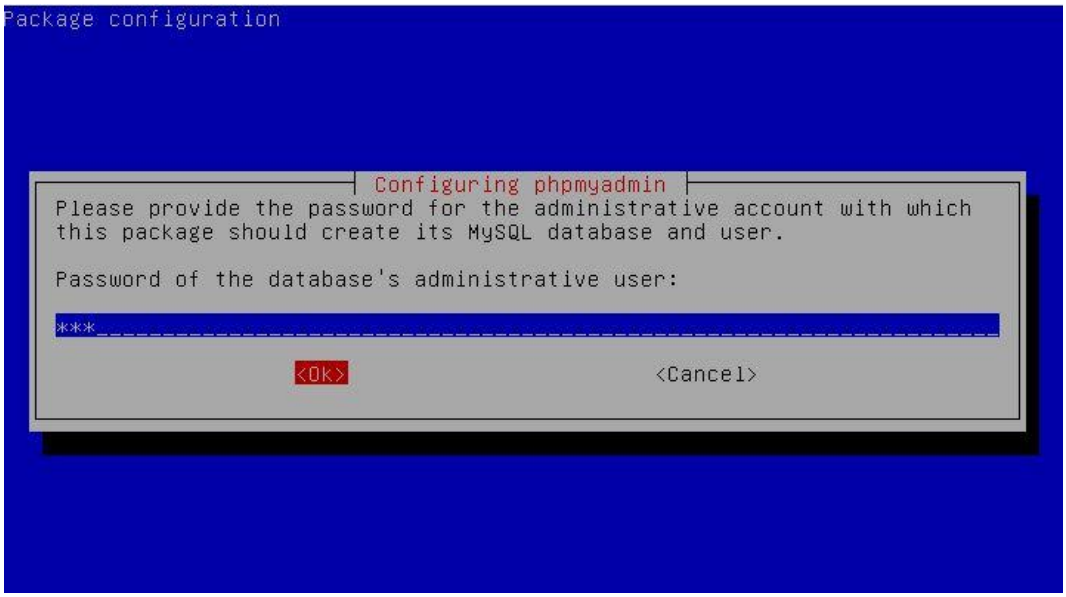
3. Lalu klik yes seperti gambar di bawah ini



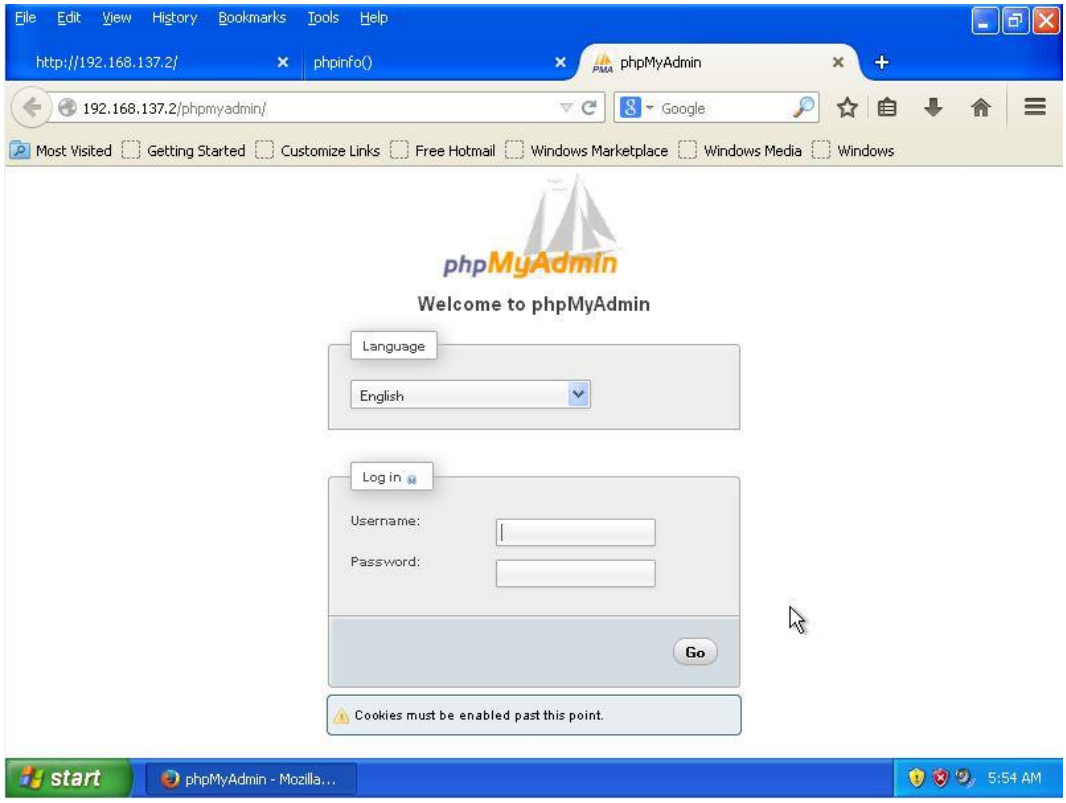
4. Setelah itu akan kita akan diminta untuk memasukkan password mysql yang telah dibuat

5. Setelah itu akan kita akan diminta untuk memasukkan password mysql yang telah dibuat

6. Lalu kita akan diminta untuk membuat password baru dari administrative user. kita bisa memasukkan password yang sama dengan password mysql yang telah dibuat.



7. Setelah itu kita diminta untuk mengkonfirmasi password administrative user yang telah dibuat. masukkan password yang sama dengan password administrative user yang telah dibuat.
8. setelah itu proses penginstalan telah selesai sekarang kita akan mengujinya dengan cara buka web browser dan mengetikkan IP server seperti gambar di bawah ini



9. Jika sudah muncul tampilan seperti di atas maka Database Server dengan Mysql telah berhasil, sekarang masuk dengan akun "root" dan masukkan password administrative user yang telah dibuat.

H. Mail Server

Web mail server adalah sarana yang memungkinkan user dapat mengakses e-mail melalui web dalam kata lain web mail server adalah interfaces dengan kata lain sebuah e-mail yang berada di dalam web sehingga jika membuka e-mail tersebut kita harus membuka web terlebih dahulu dengan koneksi internet dan ini berbasis webmail bisa diakses menggunakan web browser internet explorer, firefox dan opera, google crome, safari, netcape dan lain-lain.

Manfaat menggunakan webmail ialah bisa nyaman untuk mengirim surat, tidak perlu ke kantor pos, cukup duduk di depan komputer yang terhubung Internet dan ketik pesan lalu dikirim ke alamat tujuan dan Hanya dengan hitungan detik e-mail dapat dikirimkan ke belahan dunia manapun. Selain itu pesan yang dikirim tidak hanya sekedar teks (tulisan) saja. Isi e-mail dapat berupa gambar, foto, video, program, bahkan suara.Web mail pastinya sudah sangat dikenal dan digunakan banyak orang di dunia ini. Dengan web mail kita dapat saling berkirim email dengan teman, atau ke alamat email tertentu. Selain mengirim email dalam bentuk teks, kita juga dapat mengirim email berupa file, dll. Dengan web mail kita bisa berkirim dan menerima email dengan siapapun, kita juga bisa mengirim email dalam bentuk teks dan lain-lain.

Selain itu manfaat WebMail adalah untuk mengoperasikan e-mail account (membaca / menerima, mengirimkan, menghapus, membuat address book, dll). WebMail sesuai digunakan apabila Alamat e-mail kita harus bisa diakses beberapa orang sekaligus. Misalkan e-mail kontak utama perusahaan dimana terdapat beberapa orang yang dapat mengakses dan menjawab e-mail yang masuk.

Selama mengelola e-mail, kita harus terkoneksi terus ke internet, kalau tidak maka prosesnya akan terhenti, dan Kita akan khawatir masalah kuota nya. web mail : kemampuannya untuk diakses dari mana saja di seluruh dunia. Dari kantor, warnet, rumah, luar negeri, rumah tetangga, atau dari tempat lain, terserah Kita. Yang penting, komputer yang Kita pakai memiliki akses internet.

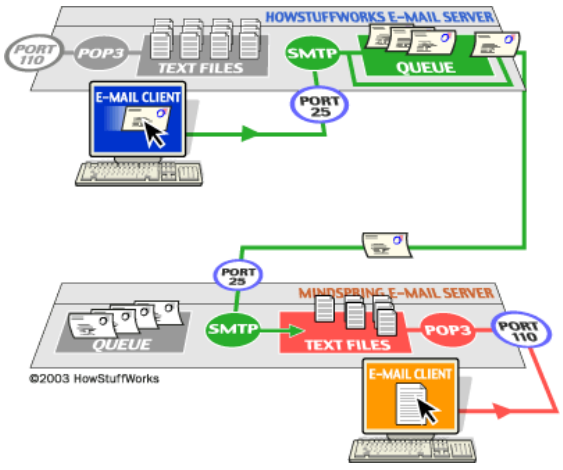
Kemudahan seperti ini disebabkan e-mail yang Kita kelola berada di mail server tertentu, bukan di komputer pribadi Kita, dan untuk mengoperasikan e-mail account (membaca / menerima, mengirimkan, menghapus, membuat address book, dll) yang sudah Kita buat melalui cPanel.

1. Konsep dan Prinsip Kerja Surat Elektronik (eMail)

Seandainya kita memiliki klien e-mail di komputer kita, kita siap untuk mengirim dan menerima e-mail. Semua yang kita butuhkan adalah sebuah server surat elektronik atau server e-mail untuk memberi layanan para klien yang tersambung. Mari kita bayangkan seperti apa server e-mail yang paling sederhana dan mungkin akan membantu untuk mendapatkan pemahaman dasar tentang proses kerja surat elektronik.

Seperti halnya server layanan FTP, DNS dll. Aplikasi ini berjalan sepanjang waktu pada mesin server dan mereka mendengarkan port tertentu, menunggu orang atau program untuk mengkoneksi ke port. Yang paling sederhana mungkin server e-mail akan bekerja seperti ini:

a. Mailserver akan memiliki daftar akun e-mail, dengan satu akun untuk setiap orang yang dapat menerima e-mail di server. Nama akun saya mungkin mbrain, Joko Priyono mungkin jpri, dan sebagainya.
b. Mailserver akan memiliki file teks untuk setiap akun dalam daftar. Jadi, server akan memiliki file teks dalam direktori yang bernama MBRAIN.TXT, lain bernama JPRI.TXT, dan sebagainya.



Gambar 3.20 Prinsip kerja pengiriman surat elektronik

Seperti orang lain mengirim mail ke mbrain, server hanya akan menambahkan pesan tersebut ke bawah file dalam urutan bahwa mereka tiba.

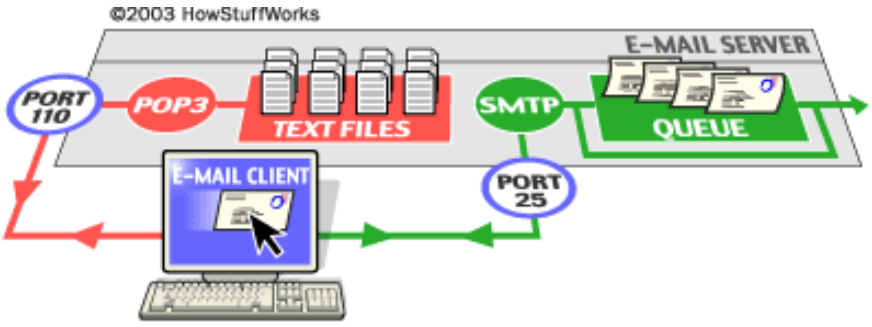
File teks akan menumpuk serangkaian lima atau 10 pesan, dan akhirnya saya akan masuk untuk membacanya. Ketika saya ingin melihat e-mail saya, klien e-mail saya akan terhubung ke mesin server. Dalam sistem yang paling sederhana, itu akan:

a. Meminta server untuk mengirimkan salinan file MBRAIN.TXT
b. Meminta server untuk menghapus dan me-reset file MBRAIN.TXT
c. Simpan file MBRAIN.TXT pada mesin lokal saya
d. Mengurai file ke dalam pesan terpisah (menggunakan kata "From:" sebagai pemisah)
e. Menunjukkan semua header pesan dalam daftar

Ketika mengklik ganda pada header pesan, akan mendapatkan pesan dalam file teks lengkap menunjukkan seluruh tubuhnya. Seperti yang kita lihat, ini adalah sistem yang sangat sederhana. Anehnya, sistem e-mail nyata yang kita gunakan setiap hari tidak jauh lebih rumit dari ini.

Bagi sebagian besar orang sekarang, sistem e-mail yang sebenarnya terdiri dari dua server yang berbeda berjalan pada mesin server. Satu disebut server SMTP, di mana SMTP singkatan dari *Simple Mail Transfer Protocol*. Server SMTP menangani surat keluar. Yang lain adalah baik server POP3 atau IMAP server, yang keduanya menangani surat masuk. POP singkatan dari *Post Office Protocol*, dan IMAP singkatan dari *Internet Mail Access Protocol*. Sebuah server e-mail yang khas terlihat seperti ini:

SMTP server mendengarkan pada port 25 yang sudah kita ketahui bersama, POP3 mendengarkan pada port 110 dan IMAP menggunakan port 143.



Gambar 3.21 Sistem sebuah server surat elektronik

2. Server-server pada Sistem surat elektronik

a. Server SMTP

Setiap kali kita mengirim sepotong e-mail, klien e-mail kita berinteraksi dengan server SMTP untuk menangani pengiriman. SMTP server untuk host kita mungkin memiliki percakapan dengan server SMTP lain untuk mengirimkan e-mail. Mari kita asumsikan bahwa saya ingin mengirimkan sepotong e-mail. E-mail ID saya adalah mbrain, dan saya memiliki akun di garudayaksa.com. Saya ingin mengirim e-mail ke jpri@dadali.com. Saya menggunakan e-mail klien yang berdiri sendiri seperti Mozilla Thunderbird atau Outlook Express.

Ketika saya menset-up akun saya di garudayaksa, saya mengatur Outlook Express nama mail server - mail.garudayaksa.com. Ketika saya menulis pesan dan menekan tombol Send, inilah yang terjadi:

1) Outlook Express menghubungkan diri ke server SMTP di mail.garudayaksa.com menggunakan port 25.
2) Outlook Express melakukan percakapan dengan server SMTP, memberitahu server SMTP alamat pengirim dan alamat penerima, serta tubuh pesan.
3) SMTP server mengambil "ke" alamat (jpri@dadali.com) dan mengelompokkannya menjadi dua bagian: nama penerima (jpri) dan nama domain (dadali.com). Jika "ke" adalah alamat pengguna lain di garudayaksa.com, server SMTP hanya akan menyerahkan pesan ke server POP3 untuk garudayaksa.com (menggunakan program kecil yang disebut agen pengiriman). Karena penerima di domain lain, SMTP perlu berkomunikasi dengan domain tersebut.
4) Server SMTP memiliki percakapan dengan Domain Name Server, atau DNS (lihat Bagaimana Web Server Bekerja untuk rincian). Ia mengatakan, "Dapatkah Anda memberi saya alamat IP dari server SMTP untuk dadali.com?" DNS itu menjawab dengan satu atau lebih alamat IP untuk server SMTP yang beroperasi untuk dadali.
5) Server SMTP di garudayaksa.com menghubungkan diri dengan server SMTP di dadali menggunakan port 25. Mereka memiliki percakapan teks sederhana yang mengatakan bahwa klien e-mail saya telah meminta

Server SMTP untuk garudayaksa untuk memberikan pesan ke server dadali. Server dadali mengakui bahwa nama domain untuk jpri adalah di dadali, sehingga memindahkan pesan ke server POP3 dadali, yang menempatkan pesan di kotak surat jpri di situ.

Jika, karena beberapa alasan, server SMTP di garudayaksa tidak dapat terhubung dengan server SMTP di dadali, maka pesan masuk ke antrian. SMTP server pada kebanyakan mesin menggunakan program yang disebut sendmail untuk melakukan pengiriman aktual, sehingga antrian ini disebut antrian sendmail. Sendmail secara berkala akan mencoba untuk mengirim pesan dalam antrian nya. Sebagai contoh, mungkin coba lagi setiap 15 menit. Setelah empat jam, biasanya akan mengirimkan sepotong surat yang memberitahu kita ada semacam masalah. Setelah lima hari, kebanyakan konfigurasi sendmail menyerah dan kembali surat kepada Anda tidak terkirim.

Server SMTP menggunakan perintah teks yang sangat sederhana seperti HELO, MAIL, RCPT dan DATA. Perintah yang paling umum adalah:

1) **HELO** - memperkenalkan diri
2) **EHLO** - memperkenalkan diri dan modus permintaan diperpanjang
3) **MAIL FROM**: - menentukan pengirim
4) **RCPT TO**: - menentukan penerima
5) **DATA** - menentukan batang tubuh pesan (Kepada, Dari dan Subyek harus menjadi tiga baris yang pertama.)
6) **RSET** – ulang
7) **QUIT** - berhenti dari sesi
8) **HELP** - mendapatkan bantuan pada perintah
9) **VRFY** - memverifikasi alamat
10) **EXPN** - memperluas alamat
11) **VERB** – verbose, memperbanyak kata

b. Server POP3

Dalam implementasi sederhana POP3, server benar-benar menjaga koleksi file teks - satu untuk setiap akun e-mail. Ketika pesan tiba, server POP3 hanya menambahkan ke bagian bawah file penerima

Ketika Anda memeriksa e-mail Anda, klien e-mail Anda terhubung ke server POP3 menggunakan port 110. Server POP3 membutuhkan nama

account dan password. Setelah Anda login, server POP3 membuka file teks Anda dan memungkinkan Anda untuk mengaksesnya. Seperti server SMTP, server POP3 mengerti satu set yang sangat sederhana dari perintah teks. Berikut adalah perintah yang paling umum:

1) **USER** - masukkan ID pengguna Anda
2) **PASS** - masukkan password Anda
3) **QUIT** - berhenti server POP3
4) **LIST** - daftar pesan dan ukuran
5) **RETR** - mengambil pesan, menambahkan sebuah nomor pesan
6) **DELE** - menghapus pesan, menambahkan sebuah nomor pesan
7) **TOP** - menunjukkan garis atas x pesan, meloloskan sejumlah pesan dan jumlah baris.

E-mail klien kita terhubung ke server POP3 dan mengeluarkan serangkaian perintah untuk membawa salinan pesan e-mail kita ke komputer lokal kita. Umumnya, ia akan menghapus pesan yang telah diunduh dari server (kecuali kita telah mengatur melalui e-mail klien agar tidak menghapus setelah diunduh).

Terlihat bahwa server POP3 hanya bertindak sebagai antarmuka antara e-mail klien dan file teks yang berisi pesan kita. Kita juga dapat melihat bahwa server POP3 sangat sederhana. Kita dapat terhubung ke server POP3 melalui telnet pada port 110 dan menjalankan perintah sendiri jika kita ingin (Seperti saat mengatur kerja Server Web dengan bantuan telnet ke server).

c. Server IMAP

Seperti yang kita lihat, protokol POP3 sangat sederhana. Hal ini memungkinkan kita untuk memiliki koleksi pesan yang disimpan dalam sebuah file teks di server. E-mail klien kita (misalnya Outlook Express) dapat terhubung ke POP3 server e-mail kita dan mengunduh pesan dari file teks POP3 ke PC kita. Itu adalah tentang semua yang dapat kita lakukan dengan POP3.

Banyak pengguna yang ingin melakukan jauh lebih lagi dengan e-mail mereka, dan mereka ingin e-mail mereka untuk tetap di server. Alasan utama untuk menjaga e-mail kita pada server adalah agar memungkinkan pengguna melakukan koneksi dari berbagai mesin. Dengan POP3, setelah kita

mengunduh e-mail, mereka itu akan berada tetap pada mesin yang kita gunakan untuk mengunduh. Jika kita ingin membaca e-mail baik pada mesin desktop kita dan atau laptop kita (tergantung pada apakah kita akan bekerja di kantor atau di jalan), POP3 akan menyulitkan keperluan itu.

IMAP (Internet Mail Access Protocol) adalah protokol yang lebih canggih yang memecahkan dapat masalah tersebut. Dengan IMAP, email kita akan tetap berada di server e-mail. Kita dapat mengatur email ke dalam folder, dan semua folder berada di server juga. Ketika kita mencari e-mail yang diperlukan, pencarian dilakukan pada mesin server, bukan pada mesin kita. Pendekatan ini membuat menjadi sangat mudah bagi kita untuk mengakses e-mail dari mesin apapun, dan terlepas dari komputer mana yang kita gunakan, kita memiliki akses ke semua mail dalam semua folder yang telah kita buat.

E-mail Klien kita terhubung ke server IMAP menggunakan port 143. E-mail klien kemudian mengeluarkan seperangkat perintah teks yang memungkinkan untuk melakukan hal-hal seperti daftar semua folder di server, daftar semua header pesan dalam folder, mendapatkan pesan e-mail tertentu dari server, menghapus pesan pada server atau pencarian melalui semua e-mail pada server.

d. Permasalahan pada IMAP dan Lampiran (attachment)

Salah satu masalah yang bisa timbul dengan IMAP berkenaan dengan pertanyaan sederhana ini: "Jika semua e-mail saya disimpan di server, maka bagaimana saya bisa membaca surat saya jika saya tidak terhubung ke Internet" Untuk mengatasi masalah ini, kebanyakan e-mail klien memiliki beberapa cara untuk melakukan cache e-mail pada mesin lokal mereka. Sebagai contoh, klien akan mendownload/mengunduh semua pesan dan menyimpan secara lengkap e-mail pada mesin lokal (seperti jika sedang menggunakan server POP3). Pesan masih ada pada server IMAP, tapi kita sekarang memiliki salinan pada mesin kita. Hal ini memungkinkan kita untuk membaca dan membalas e-mail bahkan jika kita tidak memiliki koneksi ke Internet. Suatu saat kita memiliki sambungan sambungan ke internet, kita dapat mendownload semua pesan baru yang kita terima saat terputus dengan internet dan mengirim semua surat yang kita tulis saat terputus.

3. Menguji Konfigurasi Mail Server

Mail Server atau E-Mail Server adalah perangkat lunak program yang mendistribusikan file atau informasi sebagai respons atas permintaan yang dikirim via email, mail server juga digunakan pada bitnet untuk menyediakan layanan serupa ftp. Selain itu mail server juga dapat dikatakan sebagai aplikasi yang digunakan untuk penginstalan email.

Protokol yang umum digunakan di mail server antara lain protokol SMTP, POP3 dan IMAP.

a. SMTP (Simple Mail Transfer Protocol) digunakan sebagai standar untuk menampung dan mendistribusikan email.
b. POP3 (Post Office Protocol v3) dan IMAP (Internet Mail Application Protocol) digunakan agar user dapat mengambil dan membaca email secara remote yaitu tidak perlu login ke dalam sistem shell mesin mail server tetapi cukup menguhubungi port tertentu dengan mail client yang mengimplementasikan protocol POP3 dan IMAP.

Pada mail server terdapat 2 server yang berbeda yaitu :

a. Outgoing Server (Sending email) : Protocol server yang menangani adalah SMTP (Simple Mail Transfer Protocol) pada port 25.
b. Incoming Server (Receiving email) : Protocol server yang menangani adalah POP3 (Post Office Protocol) pada port 110 atau IMAP (Internet Message Access Protocol) pada port 143.

Cara Kerja Mail Server :

Saat e-mail dikirim, maka e-mail tersebut disimpan pada mail server menjadi satu file berdasarkan tujuan e-mail. File ini berisi informasi sumber dan tujuan, serta dilengkapi tanggal dan waktu pengiriman. Pada saat user membaca e-mail berarti user telah mengakses server e-mail dan membaca file yang tersimpan dalam server yang di tampilkan melalui browser user.

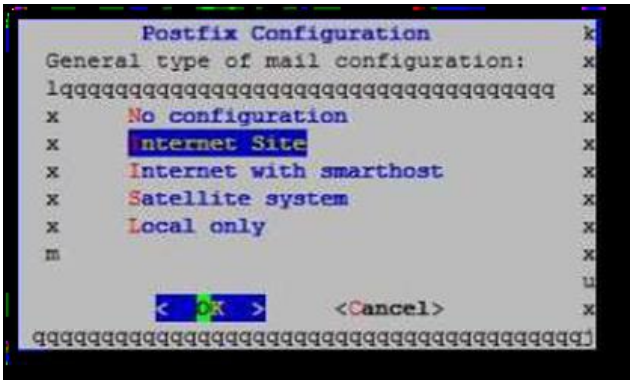
4. Konfigurasi Mail Server

a. Install postfix dengan perintah:

   Sudo apt-get install postfix

   Kemudian program apt-get akan memeriksa ketergantungan paket yang dibutuhkan oleh postfix
b. Konfigurasi postfix

Pilihan konfigurasi yang disediakan akan berhubungan dengan kapabilitas server email yang akan dibuat, pilih lah **internet site**



Pilihan ini digunakan untuk konfigurasi postfix agar dapat langsung mengirim email ke server email lain yang ada di internet.

c. Selanjutnya isikan nama domain
d. Proses instalasi postfix sudah selesai, masuk ke tahap konfigurasi
   Buka file /etc/postfix/main.cf :
   nano /etc/postfix/main.cf
e. Rubahlah konfigurasi pada, myhostname: dengan nama host yang digunakan. Langkah selanjutnya adalah konfigurasi otentikasi SASL. Silahkan tambahkan baris dibawah ini kedalam file /etc/postfix/main.cf.
   ome_mailbox = Maildir/
   smtpd_sasl_type = dovecot
   smtpd_sasl_path = private/auth
   smtpd_sasl_local_domain = ***nama domain***
   smtpd_sasl_security_options = noanonymous
   broken_sasl_auth_clients = yes
   smtpd_sasl_auth_enable = yes
   smtpd_recipient_restrictions =
   permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination
   smtp_tls_security_level = may
   smtpd_tls_security_level = may
   smtp_tls_note_starttls_offer = yes
   smtpd_tls_loglevel = 1
   smtpd_tls_received_header = yes
f. Masukkan command berikut satu demi satu untuk membuat certificate digital.

openssl genrsa -des3 -out server.key 2048

openssl rsa -in server.key -out server.key.insecure

mv server.key server.key.secure

mv server.key.insecure server.key

openssl req -new -key server.key -out server.csr

openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt

sudo cp server.crt /etc/ssl/certs

sudo cp server.key /etc/ssl/private

g. Setelah memasukkan command *openssl req -new -key server.key -out server.csr*, anda akan diminta untuk mengisi data-data seperti contoh berikut :

Country name : ID

State or province name : Sumatera Utara

Locality name : Medan

Organization name : smk

Organizational unit name : mail server

Common name : smk

Email address : smk@gmail.com

A challenge password : password

An optional company name : smk

h. Selanjutnya konfigurasi Certificate Path. Masukkan command berikut satu persatu :

sudo postconf -e 'smtpd_tls_key_file = /etc/ssl/private/server.key'

sudo postconf -e 'smtpd_tls_cert_file = /etc/ssl/certs/server.crt'

Selanjutnya install devocot, dovecot akan digunakan untuk menerima email dari luar. Berikut ini adalah cara install dovecot dan konfigurasi dovecot di server ubuntu:

a. Install devocot menggunakan perintah :

sudo apt-get install dovecot-imapd dovecot-pop3d

b. Konfigurasi mailbox dengan membuka file /etc/dovecot/conf.d/10-mail.conf.

nano /etc/dovecot/conf.d/10-mail.conf

Temukan baris yang bertuliskan

mail_location = mbox:~/mail:INBOX=/var/mail/%u

diganti menjadi

mail_location = maildir:~/Maildir

c. Buka file */etc/dovecot/conf.d/20-pop3.conf* dan hilangkan tanda pagar sebelum *pop3_uidl_format = %08Xu%08Xv*.

   nano /etc/dovecot/conf.d/20-pop3.conf

d. Langkah selanjutnya enable SSL. buka file */etc/dovecot/conf.d/10-ssl.conf* dan hilangkan tanda pagar sebelum *ssl = yes*.

   nano /etc/dovecot/conf.d/10-ssl.conf

e. Restart dovecot :

   sudo service dovecot restart

Test port pop3 dan imap dovecot yang telah di buat melalui telnet.

telnet smk 110

outputnya seperti ini :

Trying 127.0.1.1...

Connected to smk.com

Escape character is '^]'.

+OK Dovecot (Ubuntu) ready.

Pengecek dapat juga dilakukan dengan perintah :

netstat –nlpt

5. Menguji Konfigurasi Web Mail Server

Webmail server merupakan sarana yang memungkinkan user dapat mengakses e-mail melalui webdalam kata lain web mail server adalah interfaces dengan kata lain sebuah e-mail yang berada di dalam web sehingga jika membuka e-mail tersebut kita harus membuka web terlebih dahulu dengan koneksi internet dan ini berbasis web.

WebMail cocok digunakan untuk E-mail account yang harus diakses bersama-sama beberapa orang, misalkan memiliki alamat e-mail kontak utama perusahaan dengan alamat info@perusahaan.com dan terdapat beberapa orang yang bertugas menjawab e-mail masuk. Pada situasi seperti itu, WebMail sesuai digunakan karena dapat diakses secara bersama-sama, dapat mengarsip semua e-mail keluar dan masuk di satu tempat, dan dapat menandai e-mail mana yang sudah di-reply.

Tidak selalu menggunakan satu komputer yang sama untuk mengakses e-mail atau sering bepergian tanpa membawa laptop atau komputer pribadi, Bisa

jadi di kantor menggunakan komputer kantor dan di rumah menggunakan komputer milik sendiri. Namun kadang-kadang saat di rumah butuh mengakses e-mail. WebMail sesuai digunakan karena data e-mail Anda tersimpan di serversehingga tidak akan ada masalah apabila diakses dari manapun.

6. Konfigurasi web mail

Untuk menampilkan dan mengakses mail server melalui web (browser) maka digunakan squiielmail. Dengan akses melalui web, tentu akan mempermudah dalam mengirim, menerima dan mengecek email. Selain squirrelmail, dapat juga menggunakan rouncube dan lain-lain.

a. Install squirrelmail, silahkan gunakan perintah :
   sudo apt-get install squirrelmail
b. Selanjutnya buat squirrelmail supaya dapat diakses melalui web. Ketik perintah berikut satu persatu :
   sudo cp /etc/squirrelmail/apache.conf/etc/apache2/sites-available/squirrelmail.conf
   sudo a2ensite squirrelmail
c. Restart apache dengan command :
   sudo service apache2 restart

Proses instalasi squirrelmail sudah selesai dan dapat di akses melalui domainanda.com/squirrelmail atau IP/squirrelmail.

Gambar 3.22 Tampilan hasil instalasi squirrelmail

I. Control Panel Hosting

Kontrol panel hosting menyediakan solusi elegan sebagai host dari beberapa situs website yang berjalan pada Share hosting, VPS (Virtual Private Server) dan Dedicated Server. Kontrol panel hosting semacam ini menawarkan kemudahan untuk mengelola perangkat lunak berbasis web untuk menyederhanakan proses penanganan server, tanpa perlu memiliki pengetahuan akan server administration.

Kontrol panel yang paling populer saat ini dan kuat brandingnya adalah cPanel dan Plesk. Kedua kontrol panel ini merupakan aplikasi berbayar yang dibayar setiap bulan bagi sebuah provider hosting untuk di install dalam servernya. Namun untungnya, ada beberapa kontrol panel alternatif yang bersifat open source yang tersedia untuk di download secara gratis dengan fitur hampir sama dengan yang berbayar, yaitu sebagai berikut:

1. Cpanel

Cpanel Adalah kontrol panel hosting yang berbasis Unix/Linux. Antarmuka grafisnya membantu Anda untuk mengelola website beserta account hosting Anda dengan sangat mudah dan cepat. Cpanel memberi Anda akses penuh atas berbagai elemen pengaturan dari situs web dan administrasi hostingnya melalui web browser misalnya seperti Membuat database, membuat account email, auto responder, dan mengelola file website.

2. Plesk

Plesk adalah control panel hosting yang mirip dengan cPanel. Plesk memungkinkan Anda untuk mengelola account hosting Anda melalui antarmuka berbasis web. Anda dapat menginstall kontrol panel ini didalam VPS atau dedicated server. Plesk juga memungkinkan Anda untuk mengontrol ribuan virtual host dalam satu mesin. Kontrol panel memungkinkan Anda untuk mengotomatisasi banyak tugas yang pada gilirannya mengurangi biaya dan sumber daya. Hal ini juga meningkatkan profitabilitas, efisiensi dan kepuasan pelanggan.

Fitur yang ditawarkan oleh Plesk, yaitu seperti berikut ini:

a. Membuat akun FTP.
b. Mengelola dan membuat akun email dan database seperti MySQL dan PsotgreSQL.

c. Menambahkan domain dan subdomain.
d. Restore dan Backup data.
e. Mengelola DNS dan sumber daya lainnya.

3. ISPConfig

ISPConfig adalah kontrol panel open source multi bahasa yang memungkinkan Anda untuk mengelola beberapa server di bawah satu kontrol panel. ISPConfig berlisensi di bawah lisensi BSD. Kontrol panel open source ini juga mampu mengelola FTP, SQL, BIND DNS, database dan virtual server.

Fitur yang disediakan oleh ISPConfig adalah seperti berikut ini:

c. Dapat memanage lebih dari satu server dari satu panel kontrol.
d. Antarmuka web yang memudahkan untuk administrator, reseller dan klien login.
e. Mendukung webserver seperti Apache dan Nginx.
f. Konfigurasi mirroring dan cluster.
g. Mengelola akun email dan FTP.
h. Dan masih banyak lagi

4. Kloxo

Kloxo adalah salah satu kontrol panel website yang terbilang canggih dan disediakan secara gratis untuk distro Redhat dan CentOS. Memiliki fitur seperti FTP, spam filter, PHP, Perl, CGI, dan banyak lagi. Fitur seperti Messaging, Backup restore dan modul Ticketing juga tersedia dalam kontrol panel tersebut. Ini membantu user untuk mengelola/menjalankan kombinasi Apache dengan BIND, dan beralih antarmuka antara program ini tanpa kehilangan data Anda.

5. Zpanel

Zpanel adalah kontrol panel hosting yang disediakan secara gratis dan sangat mudah digunakan pada kontrol panel webhosting kelas enterprise seperti Linux, UNIX, MacOS, dan Microsoft Windows. Zpanel ditulis dalam bahasa PHP murni dan berjalan dengan baik pada Apache, PHP dan MySQL. Muncul dengan serangkaian fitur inti penting untuk menjalankan layanan hosting web Anda. Fitur inti tersebut meliputi Apache Web Server, hMailServer, FileZilla Server, MySQL, PHP, Webalizer, RoundCube, phpMyAdmin, phpSysInfo, FTP Jailing dan masih banyak lagi.

6. Webmin

Webmin merupakan kontrol panel webhosting yang powerfull dan sangat fungsional. Software yang dirancang untuk platform Unix dan Linux dengan cara yang sederhana. Webmin cukup mampu untuk mengelola berbagai komponen lingkungan berbasis web dari pengaturan webserver untuk maintaining FTP dan Email Server.

Fitur yang disediakan pada Webmin, adalah sebagai berikut:

f. Mengkonfigurasi dan membuat server virtual pada Apache.
g. Mengelola, menginstal atau menghapus paket perangkat lunak (RPM format).
h. Untuk keamanan, Anda dapat menyetting fitur firewall.
i. Mengubah pengaturan DNS, alamat IP, konfigurasi routing.
j. Mengelola database, tabel dan field MySQL.

7. EHCP

EHCP (*Easy Hosting Control Panel*) adalah software kontrol panel gratis untuk menjaga server hosting berbasis web. Dengan penggunaan EHCP Anda dapat mengelola database MySQL, account email, account domain, account FTP dan banyak lagi. Ini adalah satu-satunya control panel yang telah built-in support untuk Nginx dan PHP-FPM yang tidak menggunakan Apache dan memberikan kinerja yang baik untuk server low end.

8. DTC

Domain Technologie Control (DTC) adalah control panel hosting terutama untuk admin dan akuntansi layanan hosting GPL. Dengan bantuan interface web berbasis GUI, DTC dapat mendelegasikan tugas seperti membuat email, account FTP, subdomain, database dan banyak lagi. Ia mengatur database MySQL yang berisi semua informasi hosting.

9. Interworx

Interworx adalah sistem manajemen server Linux dan kontrol panel webhosting. Interworx memiliki seperangkat tool yang memberikan kewenangan administrator untuk memerintah servernya sendiri dan end user dapat melihat atau meninjau hasil pengelolaan website mereka. Kontrol panel ini pada dasarnya dibagi menjadi dua mode operasi, yaitu:

a. **Nodeworx**, yaitu modus administrator yang membantu mengelolaan server.

b. **SiteWorx**, yaitu website owner view yang membantu end users untuk mengelola account mereka hosting dan fitur-fitur didalamnya.

10. Ajenti

Ajenti merupakan satu-satunya kontrol panel berbasis open source yang kaya fitur, kuat dan ringan. Kontrol panel yang menyediakan antarmuka web responsif untuk mengelola server kecil set-up dan juga paling cocok untuk Dedicated dan VPS hosting. Muncul dengan banyak built-in plugin untuk mengkonfigurasi dan mengelola perangkat lunak server dan layanan seperti Apache, Nginx, MySQL, FTP, Firewall, File System, Cron, Munin, Samba, Squid dan banyak program lainnya seperti File Manager, Kode Editor untuk developer serta akses Terminal.

J. Share Hosting Server

Hosting adalah tempat atau jasa internet untuk membuat halaman website yang telah anda buat menjadi online dan bisa diakses oleh orang lain. Sedangkan Hosting Itu Sendiri Adalah : jasa layanan internet yang menyediakan sumber daya server-server untuk disewakan sehingga memungkinkan organisasi atau individu menempatkan informasi di internet berupa HTTP, FTP, EMAIL atau DNS.

Server hosting terdiri dari gabungan server-server atau sebuah server yang terhubung dengan jaringan internet berkecepatan tinggi. Ada beberapa jenis layanan hosting yaitu shared hosting, VPS atau Virtual Dedicated Server, dedicated server, colocation server.

1. Shared Hosting adalah menggunakan server hosting bersama sama dengan pengguna lain satu server dipergunakan oleh lebih dari satu nama domain. Artinya dalam satu server tersebut terdapat beberapa account yang dibedakan antara account satu dan lainnya dengan username dan password.
2. VPS, Virtual Private Server, atau juga dikenal sebagai Virtual Dedicated Server merupakan proses virtualisasi dari lingkungan software sistem operasi yang dipergunakan oleh server. Karena lingkungan ini merupakan lingkungan virtual, hal tersebut memungkinkan untuk menginstall sistem operasi yang dapat berjalan diatas sistem operasi lain.
3. Dedicated Server adalah penggunaan server yang dikhususkan untuk aplikasi yang lebih besar dan tidak bisa dioperasikan dalam shared hosting atau virtual

dedicated server. Dalam hal ini, penyediaan server ditanggung oleh perusahaan hosting yang biasanya bekerja sama dengan vendor.

4. Colocation Server adalah layanan penyewaan tempat untuk meletakkan server yang dipergunakan untuk hosting. Server disediakan oleh pelanggan yang biasanya bekerja sama dengan vendor.

Ketika anda memutuskan untuk memiliki blog atau website yang hosting sendiri, maka anda harus bisa memilih-milih jasa web hosting yang baik. Yang harus anda perhatikan ketika memilih hosting untuk blog atau website anda adalah:

1. Kebutuhan anda terhadap space dan bandwidth. Semakin banyak tulisan anda, maka semakin besar space yang akan dibutuhkan. Semakin banyak pengunjung blog anda maka semakin besar bandwidth yang dibutuhkan agar tidak terjadi server full load
2. Perhatikan layanan dan fitur dari tempat anda akan menghostingkan blog atau website anda. Bisa mencakup software apa saja yang ada di hostingnya serta support dari jasa hostingnya.
3. Target pembaca. Jika anda memilih target pembaca dari dalam negeri ada baiknya menggunakan server lokal saja agar lebih menghemat bandwidth. Tetapi jika anda memilih target yang glogal, maka tak ada salahnya anda memilih server luar negeri seperti di Amerika. Tapi keadaan ini tidaklah mutlak.
4. Harga yang pas. Konsultasikan kepada mereka yang lebih paham tentang kebutuhan hosting anda agar jasa yang anda sewa sesuai dengan uang yang akan anda keluarkan.

K. Vitual Private Server

VPS (*Virtual Private Server*) secara sederhana dapat diartikan komputer server yang berada di dunia maya. Artinya tidak nyata (*virtual*) namun kita dapat memiliki dengan cara menyewa. Hampir sama dengan komputer di dunia nyata, VPS memiliki harddisk, memory, prosesor sampai dengan operasi sistem (OS).

Yang paling menyolok dari Pengertian VPS adalah beroperasi selama 24 jam tanpa henti dan terhubung dengan jaringan internet. Dengan demikian data serta aplikasi yang ada di VPS dapat diakses atau dijalankan terus menerus selama 24 jam lewat jaringan internet kapan dan dimana saja.

VPS dapat dibagi menjadi beberapa VM (*Virtual Machines*), dimana di setiap VM adalah berupa "*Virtual server*" yang dapat di install system operasi tersendiri. VPS terasa seperti sebuah Dedicated Server. Dibanding dengan shared hosting, menyewa VPS akan mendapatkan resource yang lebih baik sehingga tidak terganggu jika ada problem pada website yang dikelola. Selain itu VPS mendapatkan root akses sehingga lebih leluasa dalam mengkustomasi server sesuai kebutuhan anda.

Kelebihan VPS dibanding Dedicated Server antara lain VPS lebih Fleksibel. Anda hanya perlu membayar resource yang anda butuhkan, nanti jika kebutuhan meningkat, bisa di upgrade tahap demi tahap. Namun, anda dituntut belajar VPS mengingat pengopersiannya sedikit rimit dari pada shared hosting yang bisanya tinggal pakai saja.

1. Fungsi VPS (*Virtual Private Server*)

a. SSH Tunneling. Berfungsi hampir sama dengan VPN yaitu mengubah IP menjadi IP VPS tersebut. (Konten – VPS – ISP – Komputer anda)
b. VPN atau Virtual Private Network berfungsi mirip seperti SSH Tunneling, yaitu mengubah IP karena Konten akan melewati VPS Terlebih dahulu sebelum mengirim ke ISP anda,lalu ke Komputer anda.
c. Proxy berfungsi mirip seperti VPN,tetapi tidak seleluasa VPN dalam penggunaanya.
d. VPS dapat difungsikan menjadi tempat menyimpan Web anda (Web Hosting). Anda dapat dengan leluasa menggunakan resource VPS anda untuk Web Pribadi anda juga.
e. VPS juga dapat digunakan untuk menyimpan File-file yang ingin anda bagikan secara Online dengan orang-orang disekitar anda atau dengan publik.
f. VPS juga dapat dipergunakan untuk Game Private Server seperti Ragnarok, RF Online, Minecraft, dan lain-lainnya.
g. Shoutcast Hosting untuk membuat Radio Online sendiri menggunakan VPS.

VPS (*Virtual Privat Server*) adalah teknologi server side tentang sistem operasi dan perangkat lunak yang memungkinkan sebuah mesin dengan kapasitas besar dibagi ke beberapa virtual mesin. Tiap virtual mesin ini melayani sistem operasi dan perangkat lunak secara mandiri dan dengan konfigurasi yang

cepat. Secara global VPS sering digunakan untuk Cloud Computing, Software Bot, Menjalankan Software robot forex (untuk trading), dsb.

VPS juga dapat di artikan sebagai sebuah metode untik mempartisi atau membagi sumber daya atau resource sebuah server menjadi beberapa server virtual. Server virtual tersebut memiliki kemampuan menjalankan operating system sendiri seperti layaknya sebuah server. Bahkan Anda dapat me-reboot sebuah server virtual secara terpisah (tidak harus mem-reboot server utama).

Kita dapat mengendalikan VPS dengan Remote Access Dekstrop atau biasa di sebut pengendali jarak jauh, dengan menggunakan aplikasi seperti Putty untuk yang menggunakan OS windows dan Terminal untuk Linux.

2. Dasar-Dasar VPS

VPS bekerja seperti sebuah server yang terpisah. VPS memiliki processes, users, files dan menyediakan full root access. Setiap VPS mempunyai ip address, port number, tables, filtering dan routing rules sendiri.

VPS dapat melakukan configurasi file untuk sistem dan aplikasi software. Setiap VPS dapat memiliki system libraries atau mengubah menjadi salah satu system libraries yang lain. Setiap VPS dapat delete, add, modify file apa saja, termasuk file yang ada di dalam root, dan menginstall software aplikasi sendiri atau menkonfigurasi root application software.

Dalam sebuah VPS, resource server yang alokasikan adalah meliputi CPU Core, CPU Usage, RAM, dan Storage atau ruang penyimpananan. Spesifikasi sebuah VPS itu sendiri berbagai macam, baik dari segi Hard disk, memorynya, jenis prosesornya, pilihan operasi sistemnya (Windows/Linux/ dan sebagainya). VPS sudah terhubung dengan internet selama 24 jam dengan kecepatan tinggi agar setiap user bisa dengan mudah mengaksesnya. VPS biasanya diakses melalui komputer pribadai menggunakan software Remote Desktop Connection (RDC) yang biasanya sudah tersedia di operasi sistem WINDOWS.

VPS dilengkapi dengan pengaturan sendiri untuk init script, users, pemrosesan, filesystem dan sebagainya. VPS bekerja seperti sebuah server yang terpisah memiliki processes, users, files dan menyediakan full root access. Setiap VPS mempunyai ip address, port number, tables, filtering dan routing rules sendiri. VPS juga dapat melakukan configurasi file untuk sistem dan aplikasi software.

Dengan Vps Anda sebagai pengguna tidak perlu lagi merawat Server Virtual ini, karena perusahaan penyedia VPS akan merawat secara berkala serta mengupgrade OS, RAM, dsb.

Penyewaan VPS terdiri dari 2 Macam:

a. VPS Managed : Server kosong /hanya diberi IP, root dan password,
b. VPS Unmanaged : Suda terinstal OS Linux atau Windows atau yg lainnya, sesuai dengan hosting.

3. Fungsi VPS

VPS memiliki banyak sekali fungsi dan kegunaan, diataranya adalah:

a. **Web Hosting** Salah satu penggunaan yang populer adalah untuk menyediakan web hosting. Virtual Private Server sangat tepat untuk level menengah dan situs web perusahaan, dimana aplikasi membutuhkan konfigurasi yang spesifik dan hanya bisa dilakukan oleh Superuser. Penggunaan ini juga cocok untuk memulai bisnis web hosting dengan anggaran yang terbatas namun layanan dengan yang berkualitas.
b. **Backup Server** Kebutuhan backup server untuk menjamin layanan selalu berjalan normal adalah sangat penting. Backup server ini bisa meliputi situs web, surel, berkas, dan basis data. Semua layanan ini berada dalam kondisi fisik dan logical yang terpisah sehingga meminimalisasi kerusakaan atau kehilangan data.
c. **Sebagai file server** atau storage server dimana kita bisa menyimpan file dan data baik melalui ftp, maupun http.
d. **Sebagai server remote desktop**, dimana kita bisa mendownload dan mengupload file secara remote, menjalankan aplikasi forex, bot/ robot & automation, spinner.
e. **Sebagai host server** untuk VPN dan Tunneling.
f. **Application Hosting** Dengan Virtual Private Server, memungkinkan untuk membangun custom mission critical software tanpa harus mengeluarkan biaya yang terlalu mahal. Melakukan outsource development aplikasi juga sudah menjadi trend untuk menghemat biaya sehingga investasi jauh lebih efisien.
g. **Development/Test Environments** Virtual Private Server juga membantu untuk melakukan serangkaian development testing secara efisien, beberapa sistem operasi dan alamat IP publik dengan mudah bisa dilakukan, koneksi

secara remote untuk reboot dan penggantian interface cukup dilakukan dengan cepat, sama seperti halnya mempunyai 1 rak yang penuh dengan server testing.

h. **Educational Outpost** Virtual Private Server menjadikan ajang untuk bereksperimen UNIX Operating System dengan berbagai macam distribusi sekaligus. Membuat proses ekperimen lebih beragam dan lebih mudah membandingkannya.

Jadi, ketika Anda memutuskan untuk membangun sebuah website atau blog untuk kepentingan komersial, sangat disarankan untuk menyewa VPS. Karena VPS sangat membantu kinerja Anda dalam mengelola website yang Anda miliki, bahkan lebih dari satu website. Khusunya bagi para web developer yang memiliki domain dalam jumlah banyak tentu Anda akan sangat membutuhkan kustomisasi untuk berbagai macam aplikasi yang Anda gunakan. Pengertian Virtual Private Server (VPS) inilah bisa menjadi referensi bagi Anda yang hendak membangun domain-domain tersebut.

VPS juga sangat cocok bagi Anda yang mengutamakan privasi dalam mengelola sebuah website. Selain itu dari Pengertian *Virtual Private Server* (VPS) diatas Anda dapat menarik kesimpulan bahwa server ini memberikan fasilitas yang mungkin tidak terdapat pada paket *shared hosting*. Masih banyak fungsi lainnya yang dapat diterapkan di VPS misalnya Rapidleech, Torrentleech, DNS Name Server, Proxy Server, dan lain-lain.

Kelemahan dari VPS itu sendiri yaitu agak lambat proses menjalankannya di PC/laptop. Ini biasanya dikarenakan oleh kecepatan internet pengguna dalam mengakses VPS itu sendiri, sedangkan VPS itu sendiri sudah bekerja dengan baik dan dengan kecepatan yang tinggi dalam melakukan proses ke internet.

L. Dedicated Hosting Server

Selain *Pengertian Dedicated Server*, pertanyaan lainnya adalah tentang Apa itu Virtual Server? *Dedicated server adalah* penyewaan satu server secara utuh tanpa dibagi dengan user yang lain, sehingga hanya Anda sendiri yang menempati dan menggunakan dedicated server tersebut. Anda berkuasa penuh atas pengelolaan dedicated server tersebut termasuk pemilihan sistem operasi, hardware, dan sebagainya. Namun anda tidak perlu repot untuk melakukan instalasi dan penyediaan hardware lainnya, karena kami menyediakan support

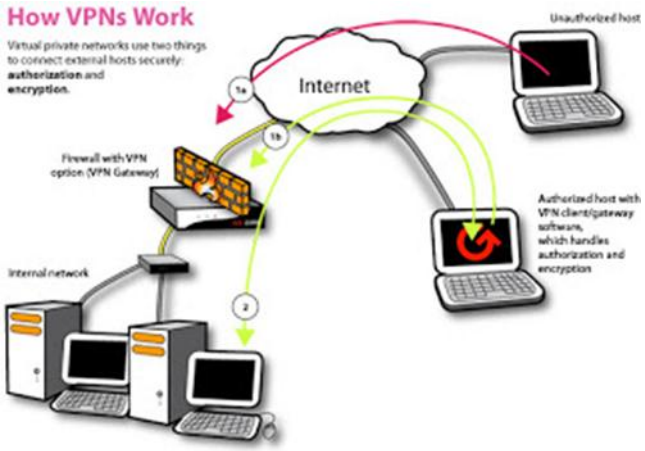
untuk instalasi software tersebut sehingga siap di gunakan. Sementara Virtual Server Adalah layanan yang mirip dengan Dedicated Server, Namun tidak memiliki fisik server, karena di bangun menggunakan teknologi virtual dari dedicated server.

Dedicated Server akan menjadi satu-satunya pilihan ketika bisnis / usaha atau situs anda berkembang dengan baik. Traffic pengunjung yang semakin bertambah akan menuntut power lebih dari server yang melayaninya. Kami menawarkan layanan ini dengan pilihan spesifikasi dan harga bertingkat sesuai dengan budget dan kebutuhan Anda, sehingga Anda tetap bisa menggunakan layanan secara optimal.

Jenis Layanan Dedicated Server

Layanan ini bersifat unmanaged, dukungan teknis diberikan sampai pada tatanan jaringan dan hardware, kami hanya melakukan instalasi dan konfigurasi awal sesuai dengan permintaan anda. Untuk Dedicated Server indonesia, Server akan diletakkan di Data Center Indonesia yang terkoneksi dengan Jaringan 1 GBps Shared IIX / Open IXP Connection Unmetered, serta link internasional melalui Nusanet Internet Service Provider sebesar 5 Mbps Shared International Connection. Pilihan untuk bandwidth dedicated juga dapat anda miliki apabila anda membutuhkannya.

M. VPN Server



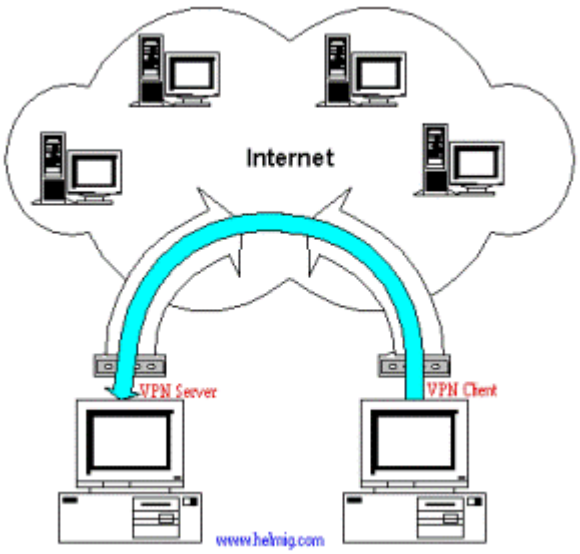
Gambar 3.23 VPN Server

VPN merupakan singkatan dari *Virtual Private Network*, yaitu sebuah koneksi private melalui jaringan publik (dalam hal ini internet). Disini ada 2 kata yang dapat kita garis bawahi yaitu:

1. **virtual network**, yang berarti jaringan yang terjadi hanya bersifat virtual. Tidak ada koneksi jaringan secara riil antara 2 titik yang akan berhubungan.
2. **private**, jaringan yang terbentuk bersifat private dimana tidak semua orang bisa mengaksesnya. Data yang dikirimkan terenkripsi sehingga tetap rahasia meskipun melalui jaringan publik.

Dengan VPN ini kita seolah-olah membuat jaringan didalam jaringan atau biasa disebut tunnel (terowongan). **Tunneling** adalah suatu cara membuat jalur privat dengan menggunakan infrastruktur pihak ketiga. VPN menggunakan salah satu dari tiga teknologi tunneling yang ada yaitu: PPTP, L2TP dan standar terbaru, Internet Protocol Security (biasa disingkat menjadi IPSec). VPN merupakan perpaduan antara teknologi tunneling dan enkripsi.

Dibawah ini adalah gambaran tentang koneksi VPN yang menggunakan protokol PPTP. PPTP (Pont to Point Tunneling Protocol) adalah sebuah protokol yang mengizinkan hubungan Point-to Point Protocol (PPP) melewati jaringan IP, dengan membuat Virtual Private Network (VPN).



Gambar 3.24 koneksi VPN

1. Cara Kerja VPN

Dari gambar diatas secara sederhana cara kerja VPN (dengan protokol PPTP) adalah sebagai berikut:

a. VPN membutuhkan sebuah server yang berfungsi sebagai penghubung antar PC, **Server VPN** ini bisa berupa komputer dengan aplikasi VPN Server atau sebuah Router, misalnya MikroTik RB 750.
b. Untuk memulai sebuah koneksi, komputer dengan aplikasi VPN Client mengontak Server VPN, VPN Server kemudian memverifikasi username dan password dan apabila berhasil maka VPN Server memberikan IP Address baru pada komputer client dan selanjutnya sebuah koneksi / tunnel akan terbentuk.
c. Untuk selanjutnya komputer client bisa digunakan untuk mengakses berbagai resource (komputer atu LAN) yang berada dibelakang VPN Server misalnya melakukan transfer data, ngeprint dokument, browsing dengan gateway yang diberikan dari VPN Server, melakukan remote desktop dan lain sebagainya.

2. Keuntungan VPN

Beberapa keuntungan dari teknologi VPN diantaranya adalah:

a. Remote Access, dengan VPN kita dapat mengakses komputer atau jaringan kantor, dari mana saja selama terhubung ke internet

b. Keamanan, dengan koneksi VPN kita bisa berselancar dengan aman ketika menggunakan akses internet publik seperti hotspot atau internet cafe.
c. Menghemat biaya setup jaringan, VPN dapat digunakan sebagai teknologi alternatif untuk menghubungkan jaringan lokal yang luas dengan biaya yang relatif kecil, karena transmisi data teknologi VPN menggunakan media jaringan public yang sudah ada tanpa perlu membangun jaringan pribadi.

3. Kekurangan atau Kelemahan VPN

Beberapa kekurangan dari VPN diantaranya adalah:

a. Koneksi internet (jaringan publik) yang tidak bisa kita prediksi. Hal ini dapat kita maklumi karena pada dasarnya kita hanya "nebeng" koneksi pada jaringan pihak lain sehingga otomatis kita tidak mempunyai kontrol terhadap jaringan tersebut.
b. Perhatian lebih terhadap keamanan. Lagi-lagi karena faktor penggunaan jaringan publik, maka kita perlu memberikan perhatian yang lebih untuk mencegah terjadinya hal-hal yang tidak diinginkan seperti penyadapan, hacking dan tindakan cyber crime pada jaringan VPN.

4. Manfaat & Kegunaan VPN

VPN merupakan paket solusi komunikasi data (baik berupa data suara, video, atau file digital lainnya) yang memberikan layanan berbasis IP ke end user. Layanan VPN dapat mengirimkan data antar-dua komputer yang melewati jaringan publik, misal nya Internet, sehingga seolah-olah terhubung secara point-to-point.

Beberapa manfaat dan kegunaan VPN yaitu:

a. Kemampuan membentuk jaringan LAN yang tidak di batasi tempat dan waktu, karena koneksitasnya dilakukan via internet. Koneksi internet apapun dapat digunakan seperti Dial-Up, ADSL, Cable Modem, WIFI, 3G, CDMA Net, GPRS, dan sistem PVN ini paling tepat digunakan untuk penggunaan suatu database terpusat untuk mengkomunikasikan antara server dan client via internet seperti Aplikasi Perdagangan, Purchase, P.O.S, Accounting, Cashir, Billing system, General Ledger, DLL
b. Tidak ada ketergantungan terhadap keharusan memiliki IP Publik yang berharga mahal. Cukup menggunakan IP dynamic saja dengan kata lain asal PC anda bisa berinternet .

c. Mampu mencetak dokumen dari rumah kekantor via internet.
d. mampu melakukan transfer data atau remote view untuk mengendalikan komputer dirumah/kantor anda dimana saja
e. Tidak membutuhkan Peralatan/hardware tambahan yang berfungsi sebagai IP forwarder/Port Forwader yang menambah investasi anda.
f. Dapat melakukan koneksitas dengan PC dikantor anda misalnya dengan memanfaatkan software yang bekerja dijaringan LAN seperti Citrix, Windows Terminal Server 2003, VNC, Radmin, VOIP, DLL
g. Dengan menggunakan software yang bekerja dijaringan LAN anda dapat melakukan pertukaran data secara langsung, Printing , Remote View, Mengatur administrasi PC anda, yang kesemua itu dapat dilakukan dimanapun anda berada selama anda bisa terhubung ke internet
h. Dapat mengakses akses yang diblok
i. Berselancar dengan aman ketika di akses internet publik / hotspot
j. Jika perusahaan ingin mengoptimalkan biaya untuk membangun jaringan mereka yang luas. Oleh karena itu VPN dapat digunakan sebagai teknologi alternatif untuk menghubungkan jaringan lokal yang luas dengan biaya yang relatif kecil, karena transmisi data teknologi VPN menggunakan media jaringan public yang sudah ada.
k. Jangkauan jaringan lokal yang dimiliki suatu perusahaan akan menjadi luas, sehingga perusahaan dapat mengembangkan bisnisnya di daerah lain. Waktu yang dibutuhkan untuk menghubungkan jaringan lokal ke tempat lain juga semakin cepat, karena proses instalasi infrastruktur jaringan dilakukan dari perusahaan / kantor cabang yang baru dengan ISP terdekat di daerahnya. penggunaan VPN secara tidak langsung akan meningkatkan efektivitas dan efisiensi kerja.
l. Penggunaaan VPN dapat mengurangi biaya operasional bila dibandingkan dengan penggunaan leased line sebagai cara tradisional untuk mengimplementasikan WAN.
m. VPN dapat mengurangi biaya pembuatan jaringan karena tidak membutuhkan kabel (leased line) yang panjang. Penggunaan kabel yang panjang akan membutuhkan biaya produksi yang sangat besar. Semakin jauh jarak yang diinginkan, semakin meningkat pula biaya produksinya.

n. VPN menggunakan internet sebagai media komunikasinya. Perusahaan hanya membutuhkan biaya dalam jumlah yang relatif kecil untuk menghubungkan perusahaan tersebut dengan pihak ISP (internet service provider) terdekat.
o. Penggunaan VPN akan meningkatkan skalabilitas.
p. VPN memberi kemudahan untuk diakses dari mana saja, karena VPN terhubung ke internet. Sehingga pegawai yang mobile dapat mengakses jaringan khusus perusahaan di manapun dia berada. Selama dia bisa mendapatkan akses ke internet ke ISP terdekat, pegawai tersebut tetap dapat melakukan koneksi dengan jaringan khusus perusahaan

N. Sistem Kontrol dan Monitoring

1. Monitoring Jaringan Komputer

Monitoring jaringan adalah proses pengumpulan dan melakukan analisis terhadap data-data pada lalu lintas jaringan dengan tujuan memaksimalkan seluruh sumber daya yang dimiliki Jaringan Komputer dimana salah satu fungsi dari management yang berguna untuk menganalisa apakah jaringan masih cukup layak untuk digunakan atau perlu tambahan kapasitas. Hasil monitoring juga dapat membantu jika admin ingin mendesain ulang jaringan yang telah ada. Banyak hal dalam jaringan yang bisa dimonitoring, salah satu diantaranya load traffic jaringan yang lewat pada sebuah router atau interface komputer. Monitoring dapat dilakukan dengan str SNMP, selain load traffic jaringan, kondisi jaringan pun harus dimonitoring, misalnya status up atau down dari sebuah peralatan jaringan. Monitoring Jaringan Komputer dapat dibagi menjadi 2 bagian yaitu :

a. Connection Monitoring, Connection monitoring adalah teknik monitoring jaringan yang dapat dilakukan dengan melakukan tes ping antara monitoring station dan device target, sehingga dapatdiketahui bila koneksi terputus.
b. Traffic Monitoring, Traffic monitoring adalah teknik monitoring jaringan dengan melihat paket aktual dari traffic pada jaringan dan menghasilkan laporan berdasarkan traffic jaringan.

Tujuan Monitoring Jaringan Komputer adalah untuk mengumpulkan informasi yang berguna dari berbagai bagian jaringan sehingga jaringan dapat diatur dan dikontrol dengan menggunakan informasi yang telah terkumpul.

Dengan begitu diharapkan jika terjadi touble atau permasalahan dalam jaringan akan cepat diketahui dan diperbaiki sehingga stabilitas jaringan lebih terjamin. Berikut ini beberapa alasan utama dilakukan monitoring jaringan:

a. Untuk menjaga stabilitas jaringan.
b. Sulit untuk mengawasi apa yang sedang terjadi di dalam jaringan yang memiliki sejumlah besar mesin (host) tanpa alat pengawas yang baik.
c. Untuk mendeteksi kesalahan pada jaringan, gateway, server, maupun user.
d. Untuk memberitahu trouble kepada administrator jaringan secepatnya.
e. Mempermudah analisis troubleshooting pada jaringan.
f. Mendokumentasikan jaringan.

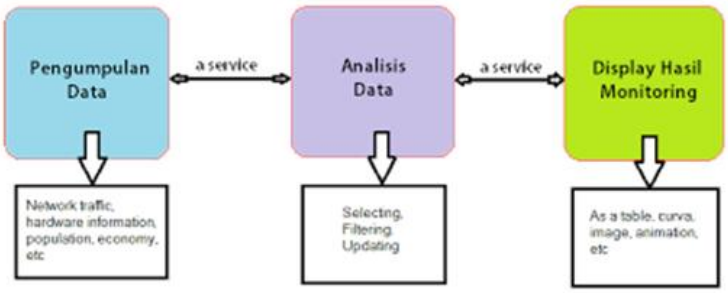
Sebuah sistem monitoring melakukan proses pengumpulan data mengenai dirinya sendiri dan melakukan analisis terhadap data-data tersebut dengan tujuan untuk memaksimalkan seluruh sumber daya yang dimiliki. Data yang dikumpulkan pada umumnya merupakan data yang real-time, baik data yang diperoleh dari sistem yang hard real-time maupun sistem yang soft real-time.

Sistem yang real-time merupakan sebuah sistem dimana waktu yang diperlukan oleh sebuah komputer didalam memberikan stimulus ke lingkungan eksternal adalah suatu hal yang vital. Waktu didalam pengertian tersebut berarti bahwa sistem yang real-time menjalankan suatu pekerjaan yang memiliki batas waktu (deadline). Di dalam batas waktu tersebut suatu pekerjaan mungkin dapat terselesaikan dengan benar atau dapat juga belum terselesaikan.

Sistem yang real-time mengharuskan bahwa suatu pekerjaan harus terselesaikan dengan benar. Sesuatu yang buruk akan terjadi apabila komputer tidak mampu menghasilkan output tepat waktu. Hal ini seperti yang terjadi pada embedded system untuk kontrol suatu benda, seperti pesawat terbang, dan lain-lain. Sistem yang soft real-time tidak mengharuskan bahwa suatu pekerjaan harus terselesaikan dengan benar.

Secara garis besar tahapan dalam sebuah sistem monitoring terbagi ke dalam tiga proses besar, yaitu:

a. Proses di dalam pengumpulan data monitoring.
b. Proses di dalam analisis data monitoring.
c. Proses di dalam menampilkan data hasil monitoring.



Gambar 3.25 Sistem monitoring

Analogi proses dapat dilihat pada gambar diatas dimanasumber data dapat berupa network traffic, informasi mengenai hardware, atau sumber-sumber lain yang ingin diperoleh informasi mengenai dirinya. Proses dalam analisis data dapat berupa pemilihan data dari sejumlah data telah telah terkumpul atau bisa juga berupa manipulasi data sehingga diperoleh informasi yang diharapkan. Sedangkan tahap menampilkan data hasil monitoring menjadi informasiyang berguna di dalam pengambilankeputusan atau kebijakan terhadap sistem yang sedang berjalan dapat berupa sebuah tabel, gambar, gambar kurva, atau dapat juga berupa gambar animasi.

2. Aplikasi Monitoring Server

a. IPTABLES

IPTABLES adalah suatu tools yang berfungsi sebagai alat untuk melakukan filter (penyaringan) terhadap (trafic) lalulintas data dan salah satu firewall popular dan powerfull dalam sistem operasi linux. Secara sederhana digambarkan sebagai pengatur lalulintas data.

Fungsi IPTABLES adalah untuk konfigurasi, merawat dan memeriksa rules tables (tabel aturan) tentang filter paket IP yang terdapat di kernel linux dan kita dapat mengatur semua lalulintas dalam komputer kita, baik yang masuk ke komputer, keluar dari komputer, ataupun traffic yang sekedar melewati komputer kita.

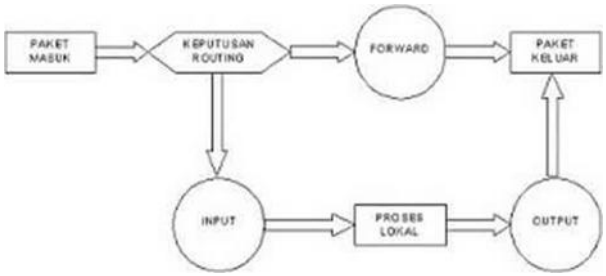
IPTABLES memiliki 4 tabel aturan yaitu :

1) Filter, Untuk melakukan pemfiteran/penyaringan paket data apakah paket tersebut akan di DROP, LOG, ACCEPT atau REJECT
2) Nat, Melakukan Network Address Translation yang merupakan pegganti alamat asal atau tujuan dari paket data.

3) Mangle, Untuk melakukan penghalusan (mangle) paket data seperti TTL, TOS dan MARK.
4) Raw, Untuk mengkonfigurasi pengecualian dari connection tracking bersama-sama NOTRACK.

Pada table terdapat chains (rantai) yang berisi rules/aturan yang berbeda-beda. Chains pada table filter yaitu :

1) INPUT, Untuk paket yang disiapkan untuk soket lokal atau komputer kita sendiri atau untuk mengatasi paket data yang masuk.
2) FORWARD, Untuk paket yang diarahkan/routing ke box atau untuk mengalihkan paket yang datang.
3) OUTPUT, Untuk paket yang generate/dibuat sendiri atau untuk menghasilkan paket data yang akan diteruskan



Gambar 3.26 Konsep IPTABLES

Istilah-istilah tersebut misalnya, memberitahu apa yang harus dilakukan terhadap lanjutan sintaks perintah, dan dilakukan untuk penambahan atau penghapusan sesuatu dari tabel atau yang lain, seperti dibawah ini :

sintaks IPTABLES

#IPTABLES [-t table] command [match] [target/jump]

Paket-paket yang masuk akan diperiksa, apakah rusak, salah infornasi atau tidak, kemudian diberikan ke chain INPUT, keputusan yang diambil untuk suatu paket dapat berupa:

1) ACCEPT, Menerima paket dan diproses lebih lanjut oleh kernel.
2) DROP, Menolak paket tanpa pemberitahuan terlebih dahulu.
3) REJECT, Mengembalikan paket je asalnya dengan pesan kesalahan ICMP.
4) LOG, Melakukan log (pencatatan) terhadap paket yang bersesuaian.

5) RETURN, Untuk chain user-defined akan dikebalikan ke chain yang memanggil, sedangkan untuk chain INPUT, OUTPUT dan FORWARD akan dijalankan kebijakan default.
6) Mengirim ke chain user-defined.

Sedangkan yang dimaksud dengan Chain/rantai digambarkan sebagai jalur aliran data. Chains yang diperlukan untuk IPTABLES ini antara lain:

1) FORWARD Route packet akan di FORWARD tanpa di proses lanjut di local.
2) INPUT Route packet masuk ke dalam proses lokal sistem.
3) OUTPUT Route packet keluar dari local sistem.
4) PREROUTING Chain yang digunakan untuk keperluan perlakuan sebelum packet masuk route. Biasanya dipakai untuk proses NAT.
5) POSTROUTING Chain yang digunakan untuk keperluan perlakuan sesudah packet masuk route. Biasanya dipakai untuk proses NAT.

Chain PREROUTING dan POSTROUTING dimaksudkan sebagai jalur data sebelum dan sesudah data tersebut masuk ke dalam route.

Beberapa target yang lain biasanya memerlukan parameter tambahan:

1) LOG Target, Tingkatan log yang bisa digunakan dalam option pertama adalah debug, info, notice, warning, err, crit, alert dan emerg. Option kedua adalah -j LOG –log-prefix untuk memberikan string yang tertulis pada awal log, sehingga memudahkan pembacaan log. Sintaksnya adalah:

   IPTABLES –A FORWARD –p tcp –j LOG –log-level debug

   IPTABLES –A INPUT –p tcp –j LOG –log-prefix “INPUT Packets”
2) REJECT Target, Memblok paket dan menolak untuk memproses lebih lanjut paket tersebut. REJECT akan mengirimkan pesan error ke pengirim paket, tidak seperti DROP. REJECT bekerja pada chain INPUT, OUTPUT dan FORWARD atau pada chain tambahan dari chain tersebut.

   IPTABLES –A FORWARD –p tcp –dport 80 –j REJECT –reject-with icmp-host-unreachable

   Tipe pesan yang bisa dikirimkan yaitu icmp-net-unreachable, icmp-host-unreachable, icmp-port-unreachable, icmp-proto-unrachable, icmp-net-prohibited dan icmp-host-prohibited.

3) SNAT Target, Berguna untuk melakukan perubahan alamat asal paket (Source Network Address Translation). Target ini hanya berlaku untuk tabel nat pada chain POSTROUTING. Jika paket pertama dari satu koneksi mengalami SNAT, paket-paket berikutnya dalam koneksi juga akan mengalaminya. Sintaksnya adalah

   IPTABLES –t nat –A POSTROUTING –o eth0 –j SNAT –to-source *192.168.0.1-192.168.0.254*:*1024-32000*

4) DNAT Target, Digunakan untuk melakukan translasi alamat tujuan (Destination Network Address Translation) pada header dari paket yang memenuhi aturan match. DNAT hanya bekerja untuk tabel nat pada chain PREROUTING dan OUTPUT atau chain buatan yang dipanggil oleh chain tersebut. Sintaksnya adalah

   IPTABLES –t nat –A PREROUTING –p tcp –d *10.10.10.10* –dport 80 –j DNAT –to-destination *192.168.0.1*

5) MASQUERADE Target, Hampir sama dengan SNAT, tetapi tidak perlu option –to-source. Target ini hanya bekerja untuk tabel nat pada chain POSTROUTING. Sintaksnya adalah

   IPTABLES –t nat –A POSTROUTING –o ppp0 –j MASQUERADE

6) REDIRECT Target, Mengalihkan paket ke komputer itu sendiri. Mengarahkan paket yang menuju suatu port tertentu untuk memasuki proxy, berguna untuk membangun transparent proxy. Misal untuk mengalihkan semua koneksi yang menuju port http untuk memasuki aplikasi http proxy seperti squid. Hanya bekerja untuk tabel nat pada chain PREROUTING dan OUTPUT atau pada chain buatan dari chain tersebut. Sintaksnya adalah

   IPTABLES –t nat –A PREROUTING –i eth1 –p tcp –dport 80 –j REDIRECT –to-port 8080

b. Multi Router Traffic Grapher (MRTG)

Multi Router Traffic Grapher atau yang disingkat MRTG adalah free software yang digunakan untuk memonitoring traffik load pada link jaringan. Dimana pengguna dapat melihat laporan dalam bentuk grafik. MRTG ditulis dalam bentuk bahasa perl dan C dan berjalan di UNIX/Linux dan juga pada

sistem operasi Windows dan juga pada Netware. MRTG menggunakan lisensi Gnu GPL.

1) Cara Kerja MRTG

   Data hasil logging olah MRTG disimpan dalam file ASCII, file ini akan ditulis ulang setiap lima menit sekali sesuai dengan update yang dilakukan oleh MRTG dan secara instant digabungkan dan dianalisis sehingga file logging tersebut membesarnya terkendali. File logging tersebut hanya digunakan untuk menyimpan data yang dibutuhkan untuk menggambar pada halaman web. Grafik ini dikonversi ke format GIF dari format PNM menggunakan tool pnmtogif.

   Konfigurasi ini yang mengakibatkan MRTG terbatas untuk memonitor sekitar dua puluh router dari workstation.Kendala lain yang sangat potensial bagi user adalahtool smnpget dari package CMU SNMP yang diperlukan oleh MRTG untuk mengumpulkan data. Paket CMU SNMP ini sangat sulit untuk dikompilasi pada berbagai macam platform waktu itu.Karena keterbatasan-keterbatasan diatas maka penemu dan rekannya melakukan perombakan pada MRTG versi pertama, mereka membuat sebuah program rateup yang memecah MRTG dalam masalah kinerja dengan mengimplementasikan dua hal subprogram dalam MRTG yang menghabiskan CPU paling banyak dalam bahasa C dan menghilangkan subprogram tersebut ke dalam skrip perl MRTG.

   Rateup ini melakukan penulisan ke file log dan menggambar grafik. Masalah portabilitas SNMP diselesaikan dengan mengganti snmpget dari CMU SNMO ke modul SNMP perl yang ditulis dalam bahasa perl secara murni, dengan begitu masalah platform dapat teratasi.Asumsi dasar untuk mendesain file log MRTG versi baru adalah ketertarikan pada informasi secara detail tentang load jaringan dikurangi secara proporsional dalamsatuan waktu untuk memungkinkan antara koleksi data dan analisisnya, konfigurasi ini memungkinkan implementasi dari file log yang menyimpan data trafik dengan mengurangi resolusi ke dalam masa lalu.

2) Install MRTG

   Untuk menginstall MRTG membutuhkan beberapa paket yaitu net-snmp, net-snmp-utils, dan mrtg.

a) SNMP, *Simple Network Management Protocol* adalah suatu program untuk mempermudah dalam memonitor dan mengatur perangkat-perangkat jaringan, seperti router, switch, server, printer dan lain-lain. Informasi yang dapat di monitor pun bermacam-macam dari hal-hal biasa seperti memonitor traffic di suatu perangkat sampai yang tidak biasa seperti temperatur udara di dalam router.

Konfigurasi SNPM:

Install SNMP dan SNMPD dengan menjalankan perintah:

```
# apt-get install snmp snmpd
```

Kemudian nyalakan service dari snmpd, caranya :

```
# /etc/init.d/snmpd restart
# chkconfig snmpd on
```

Kemudian test menggunakan program snmpwalk, caranya:

```
# snmpwalk -v 2c -c public localhost system
```

Kemudian untuk mempermudah ganti saja file konfigurasi-nya dengan yang baru.

```
# cd /etc/snmp
# mv snmpd.conf snmpd.conf-old
# chmod 0600 snmpd.conf
# nano /etc/snmp/snmpd.conf
```

Tambahkan sintaks berikut ini

```
##/etc/snmp/snmpd.conf
##     sec.name      source              community
##      =======      ======              =========
com2sec local       localhost           123456
com2sec lan         192.168.1.0/24      123456
#
##     group.name          sec.model           sec.name
##     =========           =========           ========
group       ROGroup_1           v1                  local
group       ROGroup_1           v1                  lan
group       ROGroup_1           v2c                 local
group       ROGroup_1           v2c                 lan
#
##MIB.view.name    incl/excl     MIB.subtree   mask
##============    =========     =========     ====
view  all-mibs        included      1             80
#
##     MIB
##     group.name context sec.model sec.level prefix read write
notif
##     ========== ======= ========= ========= ====== ====
===== =====
```

```
access ROGroup_1""v1noauth exact all-mibs none none
access ROGroup_1""v2c noauth exact all-mibs none none
```

Kemudian cek kembali apakah sudah berubah konfigurasi snmp-nya dengan merestart service snmp dan lakukan percobaan akses snmp.

```
# /etc/init.d/snmpd restart
# snmpwalk -v 2c -c 123456 localhost system
```

b) Konfigurasi Strd MRTG

Install MRTG lakukan perintah dibawah ini:

```
#apt-get install mrtg
```

Secara default file mrtg akan diletakkan pada posisi /var/www/mrtg

Pertama kali harus membuat file kofigurasi dari MRTG, dimana akan dibuat supaya MRTG memonitor semua perangkat jaringan di komputer. Caranya adalah :

```
# cfgmaker --output=/etc/mrtg/mrtg.cfg --global "workdir:
/var/www/html/bandwidth" \ -ifref=ip --global 'options[_]:
growright,bits' 123456@localhost
```

Keterangan:

- --output=/etc/mrtg/mrtg.cfg ==> adalah file konfigurasi yang akan dibuat.
- --global: /var/www/html/bandwidth ==> adalah lokasi direktori tempat grafik dari mrtg akan disajikan.
- -ifref=ip ==> MRTG akan mengecek traffic berdasarkan IP address dari setiap device.
- --global 'options[_]: growright,bits' ==> berarti grafik ditampilkan dari sebelah kanan dan traffic akan diukur berdasarkan bit.
- 123456@localhost ==> adalah community string atau "password" dari snmp server dan lokasi snmp server.

Kemudian jalankan mrtg secara manual, untuk memulai membentuk grafiknya.

```
# mrtg /etc/mrtg/mrtg.cfg
```

Tetapi apabila cara tersebut gagal yang disebabkan variabel LANG dalam format UTF-8 tidak disupport MRTG, maka untuk merubahnyagunakan :

```
# env LANG=C /usr/bin/mrtg /etc/mrtg.cfg
```

Setelah itu bentuk file index supaya halaman web dapat diakses.

```
# mkdir /var/www/html/bandwidth
# chmod 755 /var/www/html/bandwidth
# indexmaker --
output=/var/www/html/bandwidth/index.html/etc/mrtg/mrtg.cfg
```

Pembuatan grafik traffic jaringan dilakukan secara periodik, untuk itu diperlukan penjadwalan agar grafik akan selalu terbentuk dalam jangka waktu tertentu. unutk mengcek penjadwalan yang telah ada dengan cara:

```
# cat /etc/cron.d/mrtg
```

Apabila file konfigurasi tidak ada bisa buat penjadwalan sendiri

```
# crontab -e
```

Diisi dengan :

```
*/5 * * * * env LANG=C /usr/bin/mrtg /etc/mrtg/mrtg.cfg
```

Sekarang MRTG sudah berjalan bisa dilihat pada browser pada alamat : *"http:///(ip address)/bandiwidth"...*

c. NAGIOS

Nagios merupakan aplikasi monitoring yang dapat memonitor sistem komputer, monitoring jaringan dan monitoring infrastruktur suatu aplikasi berbasis open source. Nagios menawarkan layanan monitoring dan peringatan untuk server, switch, aplikasi dan layanan yang lainnya. User akan diberi pesan peringatan ketika suatu masalah terjadi pada server, switch aplikasi dan layanan yang di monitoring lainnya.

Mengingat kayanya fitur yang ditawarkan oleh Nagios maka kita akan mencoba untuk menginstall dan mengkonfigurasi aplikasi monitoring tersebut pada suatu sistem yang dikelola.

d. CACTI

Cacti adalah salah satu aplikasi open source yang merupakan solusi pembuatan grafik network yang lengkap yang di design untuk memanfaatkan kemampuan fungsi RRDTool sebagai penyimpanan data dan pembuatan grafik. Cacti menyediakan pengumpulan data yang cepat, pola grafik advanced, metoda yang mudah digunakan mudah dipahami untuk local area network sehingga network yang kompleks dengan ratusan device.

Dengan menggunakan cacti kita dapat memonitor trafik yang mengalir pada sebuah server dan cacti juga merupakan fronted dari RDDTool yang

menyimpan informasi kedalam database !MySQL dan membuat graph dari informasi tersebut.

Konfigurasi CACTI

1) Instalasi paket-paket software yang di butuhkan cacti

```
# apt-get install apache2 apache2-common apache2-mpm-prefork
apache2-utils libapache2-mod-php5 php5-cli php5-common php5-cgi

# apt-get install mysql-server mysql-client libmysqlclient16-dev php5-
mysql make gcc g++ cgilib libfreetype6 libttf-dev libttf2 libpngwriter0-
dev libpng3-dev libfreetype6-dev libart-2.0-dev snmp
```

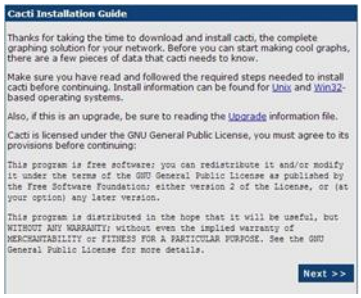
2) Install RRDTool

```
# apt-get install rrdtool
```

3) Install Cacti dengan

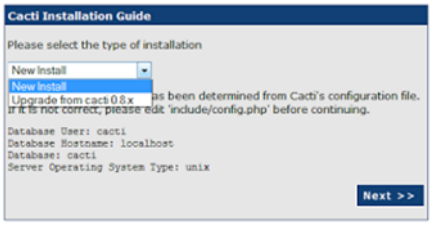
```
apt-get install cacti
```

4) Pada saat proses instalasi mysql akan ada form untuk pengisian password "root" mysql nya, isi saja sesuai dengan keinginan dan databasenya akan otomatis ter-*create* ketika proses instalasi Cactinya. Pastikan semua paket yang diinstall itu tidak mengalami error dan failed.
5) Setelah itu maka langkah berikutnya adalah mengkonfigurasi cactinya, dengan cara diakses via browser dengan alamat http://*ip-server*/cacti/ atau kalau dari localhost gunakan url : http://*localhost*/cacti/ maka akan keluar tampilan instalation guide seperti dibawah ini :



Gambar 3.27 Tampilan Cacti Instalation Guide

6) Pilih type Installasi, Pilih new install - Next



Gambar 3.28 Tampilan New Installation Cacti Guide

7) Pada tahap selanjutnya seperti gambar dibawah ini, langsung klik Finish kita tidak perlu mengubah-ubahnya.

Gambar 3.29 Tampilan Cacti Instalation Guide

8) Jika instalasi berjalan lancar tanpa adanya erorr maka langkah selanjutnya klik finish. Kemudian akan muncul user login seperti dibawah ini :

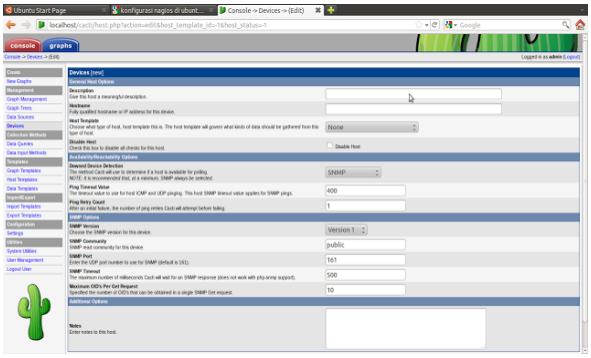
Gambar 3.30 Tampilan User Login

Untuk login defaultnya adalah username: admin, passwordnya: admin

9) Kemudian setelah login akan muncul tampilan seperti berikut ini yang merupakan halaman depan dari cacti.

Gambar 3.31 Tampilan Halaman Depan Cacti

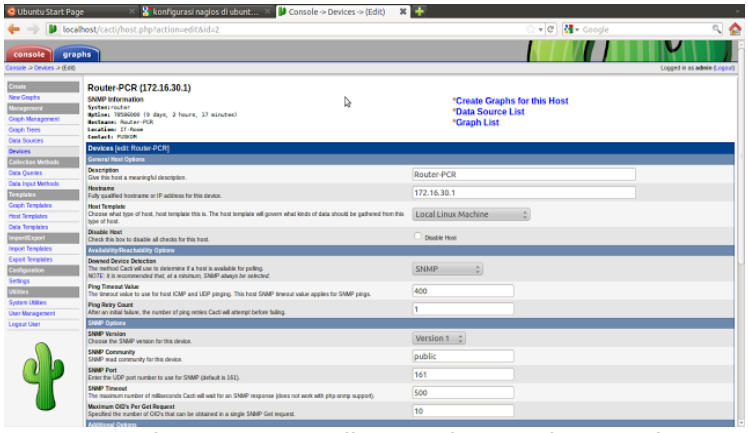
10) Setelah muncul gambar diatas, Klik menu device dan kemudian klik add (sebelah kiri atas), Kemudian akan muncul gambar seperti dibawah ini setelah itu silakan isi :



Gambar 3.32 Tampilan Halaman Depan Cacti

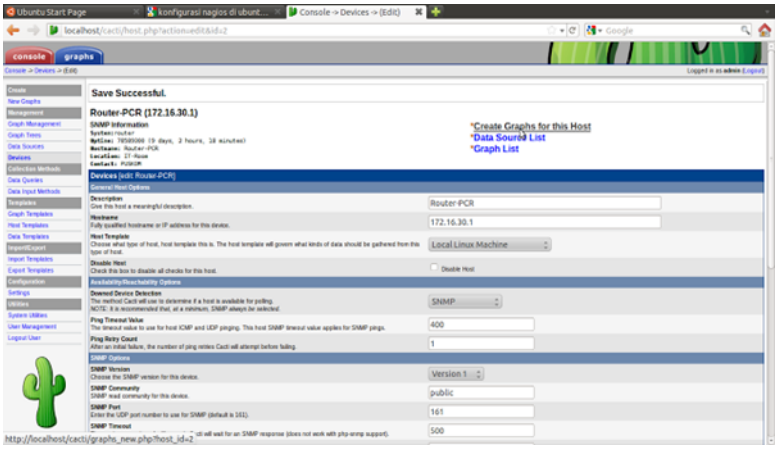
a) Description : Isikan nama device yang akan dimonitoring (Gateway).
b) Hostname : Isikan IP Address dari device yang akan dimonitoring (Gateway)
c) Host Template : Pilih “Local Linux Machine” atau ucd/net SNMP Host jika device yang akan dimonitoring PC biasa seperti windows client
d) SNMP Version : Pilih sesuai versi SNMP yang di setup di device Gateway, dalam hal ini version
e) SNMP Communitiy : umumnya pakai “public” tapi jika memang di set lain, tinggal menyesuaikan.

11) Pada bagian “associated data query” pilih “**add data query=SNMP-Interface Statistic**” dengan “**index method=Uptime Goes Backward**” lalu klik add.
12) Kemudian untuk memastikan SNMP nya jalan di device tersebut, klik “**verbose query**” pada bagian “**associated data query**” di SNMP-Interface Statistic. Jika tidak ada *error* di SNMP (lihat bagian paling bawah kanan) klik save.



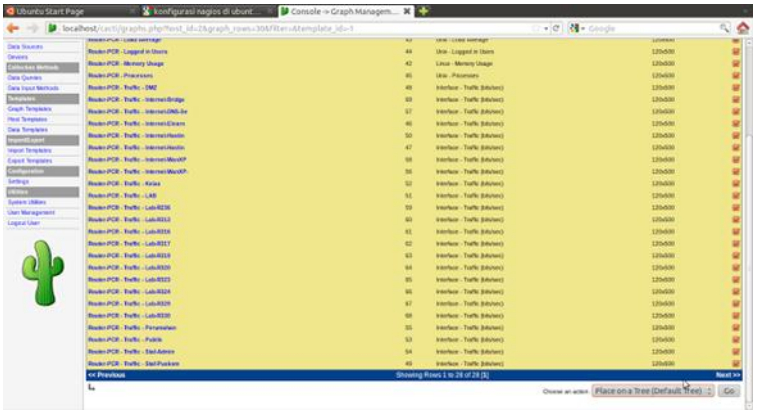
Gambar 3.33 Tampilan Setting Device Cacti

13) Kemudian pada menu device klik device yang sudah kita buat yaitu gateway, selanjutnya klik “**create graphs for this host**”. Seperti tampilan dibawah ini :



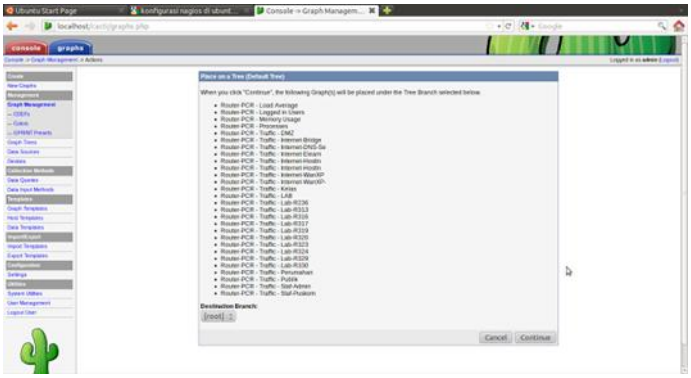
Gambar 3.34 Tampilan Create Graphs Cacti

14) Pada bagian data query [SNMP-Interface statistic] centang bagian interface dari device gateway yang akan ditampilkan grafik trafiknya. Pada bagian select graph type, pilih “**In/Out Bits with total bandwidth**” atau pilih sesuai selera. Dan klik create.
15) Kemudian untuk menampilkan di graph tree, pada bagian graph management pilih host:gateway yaitu device yang sudah dibuat sebelumya. Centang semua graph yang muncul dan di bagian action pilih “**Place on a Tree**” klik go. Seperti gambar dibawah ini :



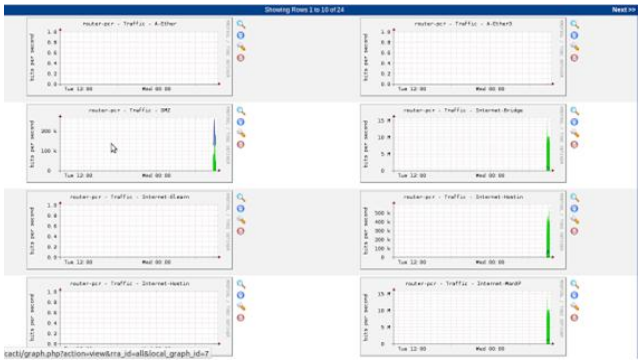
Gambar 3.35 Tampilan Place On a Tree

16) Selanjutnya akan timbul tampilan Place on a Tree (Default Tree).



Gambar 3.36 Tampilan Place On a Tree Default Tree

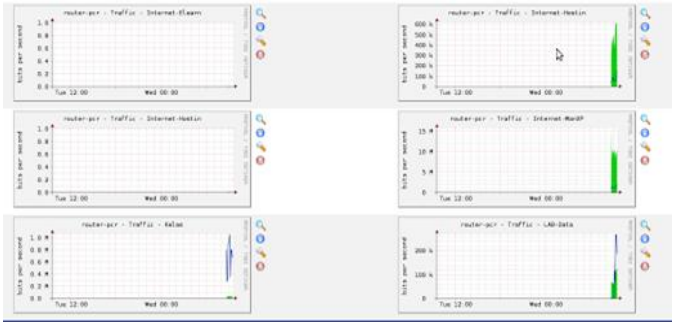
17) Kemudian tampilan di graph akan muncul device gateway, pada waktu awalnya memang grafiknya tidak muncul langsung karena perlu waktu untuk query data ke device gateway. Setelah beberapa menit akan muncul trafik data untuk tiap interface yang sudah kita centang sebelumya.



Gambar 3.37 Tampilan Trafic Data Semua Interface

18) Jika ingin memperkecil skala waktunya bisa dengan cara berikut ini :

a) Klik salah satu yang ingin diperbesar, misalnya seperti yang ditunjuk kursor berikut :

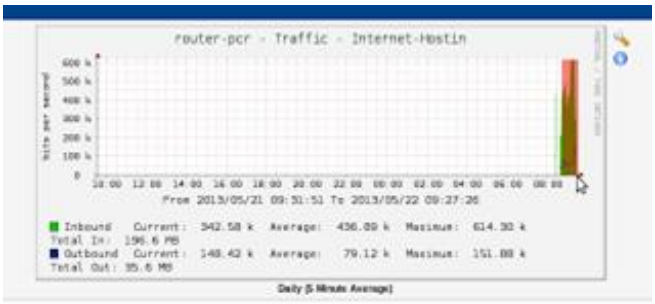


Gambar 3.38 Tampilan Trafic Data Yang Akan Di Zoom

b) Kemudian akan ditampilkan seperti gambar berikut, pilih zoom graph :

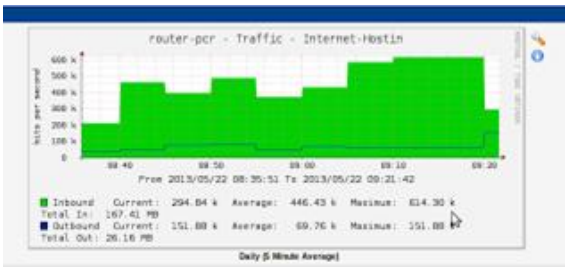
Gambar 3.39 Tampilan Trafic Data Yang Akan Di Zoom

c) Setelah di zoom, blok grafik yang ingin di zoom :



Gambar Tampilan Trafic Data Yang Di Blok

d) Kemudian akan muncul grafik yang telah di zoom sebagai berikut :



Gambar Tampilan Hasil Trafic Data Yang Di Zoom

3. Monitoring dan Sistem Kontrol Jarak Jauh

Telemetri atau komunikasi data tanpa kabel (*wireless*) merupakan cara yang efektif untuk komunikasi jarak jauh tanpa harus terganggu dengan jalur kabel yang panjang. Modul telemetri pun beragam, ada yang menggunakan komunikasi serial, ethernet atau firewall (jaringan internet). Sebagai contoh data yang dikirimkan oleh sensor temperatur dari jarak ratusan kilometer dapat dikirimkan ke lokasi lain (unit pengolah data central) dengan menggunakan media komunikasi tadi. Aktifitas dan kendali pompa air ataupun disel ataupun genset seringkali menggunakan sistem telemetry. terbukti beberapa produk

menambahkan sistem software dan hardware guna aktifitas kendali dan monitoring jarak jauh.

Untuk membuat sistem wireless tersebut tentu memerlukan beberapa unit bagian yang masing2 bisa dibahas berikut :

1. Sumber dan Pengiriman data (*Transmitter*)
2. Saluran Transmisi
3. Penerima Data (*Receiver*)

Transmitter merupakan salah satu komponen utama yang menjadi pesawat yang digunakan untuk menyiarkan atau memancarkan data informasi untuk keperluan tertentu. Saluran transmisi merupakan saluran yang dipergunakan untuk menyalurkan informasi yang telah dipancarkan oleh transmitter. Pada sistem telemetri biasanya menggunakan sistem wireless atau wireline, namun pada akhirnya sekarang banyak menggunakan wireless sebagai media komunikasi. Receiver adalah pesawat penerima yang dipergunakan untuk menerima data informasi yang telah dipancarkan oleh transmitter yang kemudian diolah sehingga didapatkan data hasil yang diperlukan. Ketiga komponen ini dan bagaimana teknik pengiriman sampai penerimaan data akan menentukan kualitas sistem yang akan dibangun.

Metoda sistem tramsimi data dari *tranceiver* ke *receiver* bisa melalui 3 metoda berikut yaitu :

1. Transfer data dengan satelit
2. Transfer data dengan GSM / GPRS
3. Transfer data dengan Radio Frekuensi (RF)

Beberapa aplikasi sistem telemetri banyak diterapkan dalam beberapa bidang seperti property emergency warning, building automation, energy, otomatisasi pompa PDAM jarak jauh, ruang kendali pasien rumah sakit, flow switch hydrant system, kontrol monitoring batery jarak jauh , dan masih banyak lagi.

Gambar 3.40 Sistem Transmisi data

Sistem transmisi data dengan GSM/GPRS mempunyai beberapa keunggulan dalam hal :

1. Infrastrukturnya murah karena tidak memerlukan pembangunan infrastruktur yang baru, hanya memanfaatkan infrastruktur yang sudah ada. Namun bukan berarti tidak ada masalah, karena sistem ini tergantung juga keandalan provider / penyedia jasa telekomunikasi yang kita sewa / bayar.
2. Cakupannya lebih luas dibandingkan dengan sisten RF (Radio Frequensi)
3. Format data digital yang ditransmisikan lebih akurat
4. Frekwensi yang digunakan sangat tinggi, hampir sama dengan frekwensi satelit yaitu sebesar 850 MHz sampai dengan 2100 Mhz.

Namun beberapa kelemahan pada sistem transmisi GSM/GPRS adalah :

1. cakupan areanya terbatas pada sistem yang memiliki BTS (*Base Tranceiver Station*).
2. Kekuatan sinyal terbatas dan sangat dipengaruhi oleh kondisi geografis.
3. Kapasitas transfer data terbatas, karena karakter yang ditransmisikan juga terbatas.

Beberapa produk dengan sistem transmisi data GSM/GPRS:

1. Sistem Kontrol AMF Generator

   Spesifikasi :

   a. Automatic SMS saat kejadian alarm pada saat overload genset, dan kejadian overtemperatur bisa dikirimkan lewat SMS.
   b. Sistem monitoring dan kontrol online melalui halaman website (*embeded we server*).
   c. Pemilihan penggunaan modem/wireless GSM/GPRS internet menggunakan teknologi GPRS.

2. Sistem Data Logger

GSM GPRS Data Logger , RTU telemetry Data Logger dengan harga yang sangat murah. Dapat dipergunakan untuk mengetahui data kejadian motor pompa trip, **genset temperatur over limit**, storage tank overflow, dan dapat juga melakukan operasi Start dan Stop mesin secara jarak jauh. Dengan beberapa modul lain seperti PLC, peralatan ukur teganhan, temperatur, flowmeter dapat dikomunikasikan dengan media telephone atau website secara serempak dalam ruang kontrol atau ruang monitoring.

Aplikasi sistem komunikasi data dengan GPRS memungkinkan pengiriman dan penerimaan data lebih cepat jika dibandingkan dengan penggunaan teknologi circuit switch data / CSD. Sistem GPRS mampu menjangkau kecepatan 56 Kbps sampai 115 Kbps sehingga memungkinkan akses internet. Sistem GPRS bekerja dengan prinsip tunelling, yaitu membungkus paket data agar bisa dilewatkan lewat gelombang radio.

Beberapa aplikasi dengan penggunaan sistem GPRS ini telah diterapkan di beberapa instansi pemerintah atau swasta yaitu PT. Telkom Ventus dan PT Indosat. Sistem GPRS ini memperbaharui sistem layanan lama soal surat meyurat elektronis dari semula hanya ke PC ke media handphone.

O. Sistem Keamanan Jaringan

Keamanan jaringan adalah suatu cara atau suatu system yang digunakan untuk memberikan proteksi atau perlindungan pada suatu jaringan agar terhindar dari berbagai ancaman luar yang mampu merusak jaringan.

1. Elemen pembentukan keamanan jaringan

Ada dua elemen utama pembentuk keamanan jaringan :

a. Tembok pengamanan (baik secara fisik maupun maya), yaitu suatu cara untuk memberikan proteksi atau perlindugan pada jarigan, baik secara fisik (kenyataan) maupun maya (menggunakan software).
b. Rencana pengamanan, yaitu suatu rancagan yang nantinya akan di implementasiakan uantuk melindugi jaringan agar terhindar dari berbagai ancaman dalam jaringan.

2. Alasan keamanan jaringan sangat penting

Alasan keaman jaringan sangat penting karena

a. Privacy/Confidentiality

   Defenisi : menjaga informasi dari orang yang tidak berhak mengakses.

   Privacy : lebih kearah data-data yang sifatnya privat , Contoh : e-mail seorang pemakai (*user*) tidak boleh dibaca oleh administrator.

   Confidentiality : berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut.

   Contoh: data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya) harus dapat diproteksi dalam penggunaan dan penyebarannya.

   Bentuk Serangan : usaha penyadapan (dengan program sniffer).

   Usaha-usaha yang dapat dilakukan untuk meningkatkan privacy dan confidentiality adalah dengan menggunakan teknologi kriptografi.

b. Integrity

   Defenisi : informasi tidak boleh diubah tanpa seijin pemilik informasi.

   Contoh : e-mail di intercept di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju.

   Bentuk serangan : Adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa ijin, “man in the middle attack” dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.

c. Authentication

   Defenisi : metoda untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud.

Dukungan :

1) Adanya Tools membuktikan keaslian dokumen, dapat dilakukan dengan teknologi watermarking(untuk menjaga “intellectual property”, yaitu dengan menandai dokumen atau hasil karya dengan “tanda tangan” pembuat) dan digital signature.
2) Access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. User harus menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya.

d. Availability

Defenisi : berhubungan dengan ketersediaan informasi ketika dibutuhkan.

Contoh hambatan :

1) “denial of service attack” (DoS attack), dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai down, hang, crash.
2) mailbomb, dimana seorang pemakai dikirimi e-mail bertubi-tubi (katakan ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya.

e. Access Control

Defenisi : cara pengaturan akses kepada informasi. berhubungan dengan masalah authentication dan juga privacy

Metode: menggunakan kombinasi *user id/password* atau dengan menggunakan mekanisme lain.

f. Non-repudiation

Defenisi : Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Dukungan bagi electronic commerce.

3. Dasar-dasar keamanan jaringan

a. *Availability*/ketersedian hanya user tertentu saja yang mempunyai hak akses atau authorized diberi akses tepat waktu dan tidak terkendala apapun.
b. *Reliability*/Kehandalan

Object tetap orisinil atau tidak diragukan keasliannya dan tidak dimodifikasi dalam perjalanannya dari sumber menuju penerimanya.

c. *Confidentiality*/Kerahasiaan

Object tidak diumbar/dibocorkan kepada subject yang tidak seharusnya berhak terhadap object tersebut, lazim disebut tidak *authorize*.

4. Syarat keamanan jaringan

a. Prevention (pencegahan)

Kebanyakan dari ancaman akan dapat ditepis dengan mudah, walaupun keadaan yang benarbenar 100% aman belum tentu dapat dicapai. Akses yang tidak diinginkan kedalam jaringan komputer dapat dicegah dengan memilih dan melakukan konfigurasi layanan (services) yang berjalan dengan hati-hati.

b. Observation (observasi)

Ketika sebuah jaringan komputer sedang berjalan, dan sebuah akses yang tidak diinginkandicegah, maka proses perawatan dilakukan. Perawatan jaringan komputer harus termasuk melihat isi log yang tidak normal yang dapat merujuk ke masalah keamanan yang tidak terpantau. System IDS dapat digunakan sebagai bagian dari proses observasi tetapi menggunakan IDS seharusnya tidak merujuk kepada ketidak-pedulian pada informasi log yang disediakan.

c. Response (respon).

Bila sesuatu yang tidak diinginkan terjadi dan keamanan suatu system telah berhasil disusupi,maka personil perawatan harus segera mengambil tindakan. Tergantung pada proses produktifitas dan masalah yang menyangkut dengan keamanan maka tindakan yang tepat harus segera dilaksanakan. Bila sebuah proses sangat vital pengaruhnya kepada fungsi system dan apabila di-shutdown akan menyebabkan lebih banyak kerugian daripada membiarkan system yang telah berhasil disusupi tetap dibiarkan berjalan, maka harus dipertimbangkan untuk direncakan perawatan pada saat yang tepat. Ini merupakan masalah yang sulit dikarenakan tidak seorangpun akan segera tahu apa yang menjadi celah begitu system telah berhasil disusupi dari luar.

5. Katagori keamanan jaringan

a. *Interruption*

Suatu aset dari suatu sistem diserang sehingga menjadi tidak tersedia atau tidak dapat dipakai oleh yang berwenang. Contohnya adalah

perusakan/modifikasi terhadap piranti keras atau saluran jaringan.

b. *Interception*

Suatu pihak yang tidak berwenang mendapatkan akses pada suatu aset. Pihak yang dimaksud bisa berupa orang, program, atau sistem yang lain. Contohnya adalah penyadapan terhadap data dalam suatu jaringan.

c. *Modification*

Suatu pihak yang tidak berwenang dapat melakukan perubahan terhadap suatu aset. Contohnya adalah perubahan nilai pada file data, modifikasi program sehingga berjalan dengan tidak semestinya, dan modifikasi pesan yang sedang ditransmisikan dalam jaringan.

d. *Fabrication*

Suatu pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contohnya adalah pengiriman pesan palsu kepada orang lain.

6. Jenis – jenis seragan atau gagguan dalam jaringan

a. **DOS / DDOS,** Denial of Services dan Distributed Denial of Services adalah sebuah metode serangan yangbertujuan untuk menghabiskan sumber daya sebuah peralatan jaringan komputer sehingga layanan jaringan komputer menjadi terganggu.

b. **Paket Sniffing,** sebuah metode serangan dengan cara mendengarkan seluruh paket yang lewat pada sebuah media komunikasi, baik itu media kabel maupun radio. Setelah paket-paket yang lewat itu didapatkan, paket-paket tersebut kemudian disusun ulang sehingga data yang dikirimkan oleh sebuah pihak dapat dicuri oleh pihak yang tidak berwenang.

c. **IP Spoofing,** sebuah model serangan yang bertujuan untuk menipu seseorang. Serangan ini dilakukan dengan cara mengubah alamat asal sebuah paket, sehingga dapat melewati perlindungan firewall dan menipu host penerima data.

d. **DNS Forgery,** Salah satu cara yang dapat dilakukan oleh seseorang untuk mencuri data-data penting orang lain adalah dengan cara melakukan penipuan. Salah satu bentuk penipuan yang bisa dilakukan adalah penipuan data-data DNS.

e. **Trojan Horse,** program yang disisipkn tanpa pengetahuan si pemilik komputer, dapat dikendalikan dari jarak jauh & memakai timer

f. **Probe :** Usaha yang tak lazim untuk memperoleh akses ke dalam suatu sistem/ untuk menemukan informasi tentang sistem tersebut. Dapat dianalogikan sebagai usaha untuk memasuki sebuah ruangan dengan mencoba-coba apakah pintunya terkunci atau tidak
g. **Scan :** kegiatan probe dalam jumlah besar dengan menggunakan tool secara otomatis. Tool tersebut secara otomatis dapat mengetahui port-port yang terbuka pada host lokal/host remote, IP address yang aktif bahkan bisa untuk mengetahui sistem operasi yang digunakan pada host yang dituju
h. **Account Compromise :** penggunaan account sebuah komputer secara ilegal oleh seseorang yang bukan pemilik account tersebut. Account Compromise dapat mengakibatkan korban mengalami kehilangan atau kerusakan data.
i. **Root Compromise :** mirip dengan account compromise, dengan perbedaan account yang digunakan secara ilegal adalah account yang mempunyai privelege sebagai administrator sistem. Akibat yang ditimbulkan bisa mengubah kinerja sistem, menjalankan program yang tidak sah.

Rangkuman

Sistem Operasi Jaringan (*Network Operating System*) adalah sebuah jenis sistem operasi yang ditujukan untuk menangani jaringan. Umumnya, sistem operasi ini terdiri atas banyak layanan atau service yang ditujukan untuk melayani pengguna, seperti layanan berbagi berkas, layanan berbagi alat pencetak (*printer*), DNS Service, HTTP Service, dan lain sebagainya

Sistem Operasi Jaringan Berbasis GUI Adalah Sistem operasi yang dalam proses Instalasinya, user tidak perlu menghafal sintax – sintax atau perintah DOS atau bahasa pemograman yang digunakannya.

Sistem Operasi Jaringan Berbasis Text Adalah sistem operasi yang proses instalasinya, user diharapkan untuk menghafal perintah DOS yang digunakan untuk menjalankan suatu proses instalasi Sistem Operasi Jaringan tersebut.

Pengertian Closed Source Software adalah perangkat lunak atau software yang dipublikasikan tanpa diberikan kode sumbernya, pada software jenis closed source hanya terdiri dari file binari saja tanpa adanya ruang untuk mengakses ke kode sumber software tersebut.

File server adalah sebuah komputer terpasang ke jaringan yang memiliki tujuan utama memberikan lokasi untuk akses disk bersama , yaitu penyimpanan

bersama file komputer (seperti dokumen, file suara, foto, film, gambar , database, dll) yang bisa diakses oleh workstation yang melekat pada jaringan komputer yang sama.

DNS server merupakan salah satu komponen penting saat ini dalam sistem internet. Keberadaannya sangat membantu dalam mengakses berbagai layanan di internet, mulai dari situs berita, publikasi karya ilmiah, jejaring sosial dan masih banyak lagi manfaat lainnya. Kesemua layanan tersebut dapat diakses dengan mudah karena memiliki nama yang yang dapat diingat oleh user.

Server basis data adalah sebuah program komputer yang menyediakan layanan pengelolaan basis data dan melayani komputer atau program aplikasi basis data yang menggunakan model klien/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.

Seandainya kita memiliki klien e-mail di komputer kita, kita siap untuk mengirim dan menerima e-mail. Semua yang kita butuhkan adalah sebuah server surat elektronik atau server e-mail untuk memberi layanan para klien yang tersambung. Mari kita bayangkan seperti apa server e-mail yang paling sederhana dan mungkin akan membantu untuk mendapatkan pemahaman dasar tentang proses kerja surat elektronik.

Hosting adalah tempat atau jasa internet untuk membuat halaman website yang telah anda buat menjadi online dan bisa diakses oleh orang lain. Sedangkan Hosting Itu Sendiri Adalah : jasa layanan internet yang menyediakan sumber daya server-server untuk disewakan sehingga memungkinkan organisasi atau individu menempatkan informasi di internet berupa HTTP, FTP, EMAIL atau DNS.

PS (Virtual Private Server) secara sederhana dapat diartikan komputer server yang berada di dunia maya. Artinya tidak nyata (virtual) namun kita dapat memiliki dengan cara menyewa. Hampir sama dengan komputer di dunia nyata, VPS memiliki harddisk, memory, prosesor sampai dengan operasi sistem (OS).

VPS (Virtual Privat Server) adalah teknologi server side tentang sistem operasi dan perangkat lunak yang memungkinkan sebuah mesin dengan

kapasitas besar dibagi ke beberapa virtual mesin. Tiap virtual mesin ini melayani sistem operasi dan perangkat lunak secara mandiri dan dengan konfigurasi yang cepat. Secara global VPS sering digunakan untuk Cloud Computing, Software Bot, Menjalankan Software robot forex (untuk trading), dsb.

Dedicated server adalah penyewaan satu server secara utuh tanpa dibagi dengan user yang lain, sehingga hanya Anda sendiri yang menempati dan menggunakan dedicated server tersebut. Anda berkuasa penuh atas pengelolaan dedicated server tersebut termasuk pemilihan sistem operasi, hardware, dan sebagainya.

Keamanan jaringan adalah suatu cara atau suatu system yang digunakan untuk memberikan proteksi atau perlindungan pada suatu jaringan agar terhindar dari berbagai ancaman luar yang mampu merusak jaringan.

Tugas

Buatlah kelompok yang terdiri dari 2 orang dan masing masing kelompok membuat ringkasan dan laporan Praktikum mengenai.

a. DHCP Server
b. FTP Server
c. Remove Server
d. File Server
e. Web Server
f. DNS Server
g. Database Server
h. Mail Server
i. Control Panel Hosting
j. Share Hosting Server
k. Vitual Private Server
l. Dedicated Hosting Server
m. VPN Server

Tes Formatif

1. Server yang dapat membuat sistem berbasis Unix (seperti Linux) untuk melakukan sharing resource dengan sistem berbasis Windows adalah....
   a. Apache

b. Proxy
c. Samba
d. Squirel
e. Squid

2. Perintah menambahkan paket service pada linux debian adalah …
   a. Apt-get Instal (nama paket)
   b. Atp-get Install (nama paket)
   c. Apt get Install (nama paket)
   d. Apt_get Install (nama paket)
   e. Apt-get Install (nama paket)
3. /usr/local/samba/lib/smb.conf, merupakan printah untuk …
   a. Konfigurasi DNS
   b. Konfigurasi SAMBA
   c. telnet
   d. Localhost
   e. Konfigurasi Linux
4. Tipe antarmuka yang digunakan oleh pengguna untuk berinteraksi dengan sistem operasi melalui gambar-gambar grafik, ikon, menu, dan menggunakan perangkat penunjuk, adalah pengertian dari….
   a. TEXT
   b. CLI
   c. DOS
   d. GUI
   e. Command line
5. Urutan proses yang tepat pada waktu menginstal sitem operasi adalah….
   a. Collecting information – dynamic update – Installing Windows – Preparing Installation – Finalizing Installation
   b. dynamic update – Collecting information –Preparing Installation – Installing Windows – Finalizing Installation
   c. Collecting information – Preparing Installation – Installing Windows – dynamic update Finalizing Installation
   d. Collecting information – dynamic update – Preparing Installation – Installing Windows – Finalizing Installation

e. Collecting information – Installing Windows – dynamic update – Preparing Installation – Finalizing Installation