TUTORIAL

ADMINISTRASI SERVER JARINGAN II
Dengan GNU Debian 6

Disusun Oleh
ANANG SUPRIYANTA

PEMERINTAH DAERAH ISTIMEWA YOGYAKARTA
DINAS PENDIDIKAN, PEMUDA DAN OLAHRAGA
SMK NEGERI 2 WONOSARI
TEKNIK KOMPUTER DAN JARINGAN

2011

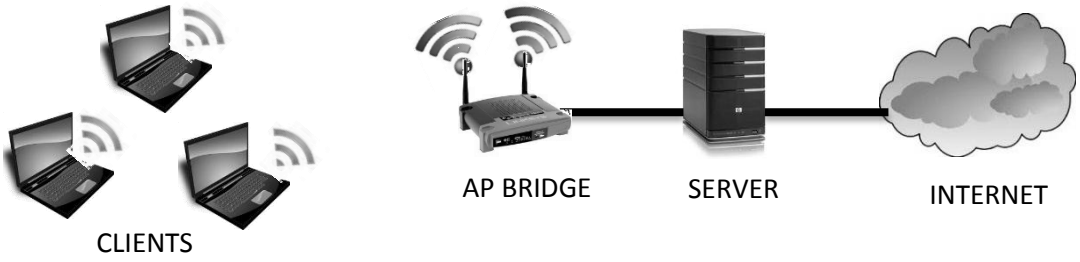
ADMINISTRASI SERVER JARINGAN II

A. PENGANTAR

Tutorial ini disusun hanya untuk keperluan panduan praktis, bukan sebagai referensi teoritis jaringan. Dan juga tutotial ini bukanlah satu-satunya cara membangun suatu sistem server jaringan tetapi hanya merupakan salah satu alternatif yang kebetulan telah saya lakukan. Ada banyak cara untuk membuat dan mengembangkan server jaringan, tetapi ini adalah cara yang saya ambil. Saya tidak dapat memberi jaminan bahwa ini akan berjalan persis seperti yang Anda inginkan.

Pada modul Administrasi Jaringan II ini kita menggunakan GNU Debian 6 sebagai sistem operasi yang akan menjalankan DNS server, Manajemen Hotspot, FTP server, dan Mail server. Berbeda dengan materi Administrasi Server Jaringan I, pada bagian kedua ini kita akan menggunakan konfigurasi yang sedikit berbeda karena sebagian server kita hubungkan kedalam database atau istilahnya "virtual user". Sehingga pada modul ini asumsinya kita sudah dapat mengkonfigurasi IP address, Gateway, SSH dan segala hal tentang konfigurasi dasar server jaringan. Kalau belum paham silakan membaca lagi toturial saya pada bagian yang pertama.

Untuk mempermudah pemahaman tentang server yang akan kita bangun, semua tutorial mengacu pada topologi jaringan seperti di bawah ini :



Semua applikasi server yang akan kita konfigurasi ada pada satu mesin yaitu pada PC server, sedang access point hanya bertindak sebagai Bridge saja. Konfigurasi dasar pada server yang akan kita pakai adalah sebagai berikut :

- IP address eth0 : 192.168.2.2/24, gateway 192.168.2.1
- IP address eth1 : 172.20.20.1/24
- NIC eth0 adalah NIC yang terhubung dengan internet.
- NIC eth1 adalah NIC yang terhubung dengan Local Network.
- Domain : gaplek.gk

Pada topolologi tersebut server juga bertindak sebagai router sehingga sebelum kita ke materi lebih lanjut kita akan menyiapkan server tersebut sebagai router. Agar dapat bertindak sebagai router, yang perlu kita konfigurasi adalah IP address, fungsi forwarding dan NAT.

A.1. IP Address

Server yang kita bangun memiliki 2 NIC yaitu eth0 dan eth1 dan untuk kasus pada jaringan ini kita hanya perlu memberi IP address pada eth0 yang terhubung dengan jaringan luar. Pada NIC eth1 tidak perlu kita beri IP address karena nantinya eth1 digunakan untuk hotspot sehingga IP address pada ethi nantinya akan didapat dari server DHCP yang dibangkitkan oleh Chillispot.

```
pico /etc/network/interfaces
```

```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
allow-hotplug eth0
iface eth0 inet static
        address 192.168.2.2
        netmask 255.255.255.0
        network 192.168.2.0
        broadcast 192.168.2.255
        gateway 192.168.2.1
```

Langkah selanjutnya ada restart service dari networking sistem,

```
/etc/init.d/networking restart
```

Kemudian cek IP Address dari server

```
ifconfig
```

```
eth0      Link encap:Ethernet  HWaddr 00:0c:29:c0:de:a9
          inet addr:192.168.2.2  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fec0:dea9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:366 errors:0 dropped:0 overruns:0 frame:0
          TX packets:252 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:36314 (35.4 KiB)  TX bytes:39663 (38.7 KiB)
          Interrupt:18 Base address:0x2000


lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:29 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2502 (2.4 KiB)  TX bytes:2502 (2.4 KiB)
```

A.2. Forwarding

Karena server harus berfungsi juga sekaligus sebagai router maka fungsi forwarding harus diaktifkan agar server dapat melewatkan paket-paket dari internet ke jaringan lokal atau sebaliknya. Untuk mengaktifkan ini kita ubah file `/etc/sysctl.conf`, hilangkan tanda "**#**" pada baris *`#net.ipv4.ip_forward=1`*,

```
pico /etc/sysctl.conf
```

```
#
# Functions previously found in netbase
#
```

```
# Uncomment the next two lines to enable Spoof protection
(reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1

# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1

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

# Uncomment the next line to enable packet forwarding for IPv6
#       Enabling this option disables Stateless Address
Autoconfiguration
#  based on Router Advertisements for this host
#net.ipv6.conf.all.forwarding=1
```

A.3. Iptables

Jaringan yang kita bangun merupakan jaringan lokal sehingga jaringan ini sebenarnya tidak bisa akses ke internet karena memang tidak ada router di internet yang merouting ke jaringan kita. Agar jaringan lokal tetap bisa koneksi ke internet kita akan aktifkan fungsi NAT pada router karena hanya IP address pada eth0 yang dikenali oleh router diatas jaringan kita. Untuk melakukan NAT pada router ini kita menggunakan perintah IPTABLES yang merupakan applikasi standart yang ada pada sistem operasi linux. Perintah IPTABLES ini kita taruh pada file /etc/rc.local agar pada setiap server kita booting aturan ini bisa langsung dijalankan secara otomatis. Tambahkan aturan "*iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE*" sebelum "`exit 0`",

```
pico /etc/rc.local
```

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

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

exit 0
```

Setelah langkah-langkah di atas dilakukan langkah selanjutnya adalah lakukan reboot terhadap server untuk memastikan semua konfigurasi sudah sesuai dengan topologi jaringan yang kita rencanankan. Setelah reboot lakukan perintah-perintah cek sistem dasar berikut :

Cek fungsi forwarding

```
cat /proc/sys/net/ipv4/ip_forward
1
```

Dari perintah diatas apabila menghasilkan keluaran “1” berarti server sudah berfungsi sebagai router.

Cek fungsi NAT

```
iptables -t nat –L
```

```
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
target     prot opt source               destination
MASQUERADE  all  --  anywhere             anywhere

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

B. DNS SERVER

B.1. Pengantar

Sekarang ini internet dan hampir semua jarignan local tergantung pada kerja dan ketangguhan Domain Name System (DNS) yang digunakan untuk meresolv nama-nama system ke dalam IP address atau sebaliknya (reserver lookup). Agar fasilitas DNS tersedia di dalam jaringan diperlukan sebuah nameserve. DNS akan menterjemahkan ip address ke hostname atau sebaliknya dari hostname ke ip address. DNS bekarja dengan konsep client server, sebua komputer yang menjalankan fungsi server disebut DNS atau name server dan komputer lain yang meminta penerjemahan hostname ke ip address disebut sebagai client DNS. DNS juga merupakan system databases yang terdistribusi, sehingga memungkina setiap bagian dari databases dikelola secara terpisah.

Salah satu applikasi yang dapat digunakan untuk membuat DNS server adalah paket BIND. BIND (singkatan dari bahasa Inggris: Berkeley Internet Name Domain) adalah server DNS yang paling umum digunakan di Internet, khususnya di sistem operasi bertipe Unix yang secara de facto merupakan standar. BIND awalnya dibuat oleh empat orang mahasiswa dengan menggunakan CSRG di Universitas California, Berkeley dan pertama kali dirilis di dalam 4.3 BSD. Paul Vixie kemudian meneruskan pemrogramannya pada tahun 1988 saat bekerja di DEC.

B.2. Instalasi

```
apt-get install bind9
```

B.3. Konfigurasi

File-file untuk bind berada pada directory /etc/bind/, untuk dapat mengelola sebuah domain file-file yang perlu dikonfigurasi adalah named.conf.local, named.conf.options, dan dua buah file yang kita siapkan untuk menampung data-data nama host yang akan dikelola.

Named.conf.local

File ini digunakan untuk membuat domain yang dikelola, sebenarnya kita tidak harus menuliskan di file named.cof.local ini tapi bisa juga langsung dituliskan di named.conf langsung. Tapi karena file-file ini bersifat sensitif maka sebaiknya kita tetap menggunakan yang named.conf.local agar apabila terjadi error karena suatu kesalahan bisa dengan mudah kita ketahui.
Karena domain yang akan kita kelola adalah gaplek.gk maka isi dari named.conf.local adalah sebagai berikut ,

```
// Do any local configuration here

//zone di bawah ini digunakan untuk menterjemahkan
//dari hostname ke IP address.
zone "gaplek.gk" {
        type master;
        file "/etc/bind/db.gaplek.gk";
};

//zone di bawah ini digunakan untuk menterjemahkan
// dari IP address ke hostname.
//Karena domain yang dikelola berada pada network 192.168.2.0
//maka untuk membuat ip address ke hostname harus menggunakan
//kaidah dibalik, yaitu 2.168.192.in-addr.arpa

zone "2.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.2.168.192";
};
```

Setelah file *named.conf.local* terisi dengan domain yang akan kita kelola sekarang perlu dibuat dua buah file data dengan nama sesuai dengan yang ada pada file *named.conf.local* yaitu file db.gaplek.gk dan file *db.2.168.192* yang masing-masing berada pada direktori /etc/bind. Untuk membuat dua file tersebut kita cukup mengkopi dari *db.local* untuk db.galek.gk dan *db.127* untuk *db.2.168.192*,

```
cp /etc/bind/db.local /etc/bind/db.gaplek.gk
cp /etc/bind/db.127 /etc/bind/db.2.168.192
```

kemudian kita sesuaikan dengan domain yang akan dikelola. Setelah dilakukan penyesuaian, isi dari file tersebut adalah :

db.gaplek.gk

```
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns.gaplek.gk root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
```

```
@       IN      NS      ns.gaplek.gk.
@       IN      MX      10 mail.gaplek.gk.
ns      IN      A       192.168.2.2
ftp     IN      CNAME   ns
mail    IN      CNAME   ns

;apabila kita menginginkan ada hostname dari PC yang lain
;misal ada server samba dengan FDQ samba.gaplek.gk dengan
;ip address 170.3.20.1, tambahkan baris berikut
;
;samba      IN    A     170.3.20.1
```

db.2.168.192

```
;
; BIND reverse data file for local loopback interface
;
$TTL    604800
@       IN      SOA     ns.gaplek.gk. root.localhost. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      ns.gaplek.gk.
2       IN      PTR     ns.gaplek.gk.
```

Perlu diperhatikan untuk semua penulisan hostname selalu diakhiri dengan "." (titik).
Domain yang dikelola oleh DNS server ini hanya domain gaplek.gk sehingga apabila nanti diminta unutuk menterjemahkan hostname selain yang berada pada domain gaplek.gk tidak akan bisa menjawab. Untuk itu DNS server ini perlu dihubungkan dengan DNS server yang lebih atas agar nanti apabila ada hostname selain yang berada dalam domain gaplek.gk tetap bisa dijawab. Agar dapat berhubungan dengan DNS server yang lain perlu ditambahkan IP address dari DNS server yang akan dihubungi pada file named.conf.option, yang isinya sebagai berikut :

Named.conf.option

```
options {
      directory "/var/cache/bind";

     // If there is a firewall between you and nameservers you want
     // to talk to, you may need to fix the firewall to allow multiple
     // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

     // If your ISP provided one or more IP addresses for stable
     // nameservers, you probably want to use them as forwarders.
     // Uncomment the following block, and insert the addresses replacing
     // the all-0's placeholder.

        forwarders {
                202.134.0.155;
         };

        auth-nxdomain no;    # conform to RFC1035
        listen-on-v6 { any; };
};
```

Dalam hal ini DNS server luar yang digunakan adalah 202.134.0.155. Untuk menjaga agar server kita tetap handal dapat menggunakan lebih dari satu DNS server luar.
Agar DNS server kita menggunakan diri sendiri untuk meresolv hostname ke IP address atau sebaliknya maka file /etc/resolv.conf perlu diubah menjadi sebagai berikut

Resolv.conf

```
search gaplek.gk
nameserver 192.168.2.2
```

Perlu juga ditambahkan nama host server pada file `/etc/hosts` untuk memastikan tidak ada error pada saat bind dijalankan. Isi dari `/etc/hosts` yaitu,

hosts

```
127.0.0.1       localhost localhost.localdomain
192.168.2.2     ns ns.gaplek.gk

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
```

B.4. Pengujian

Setelah semua terkonfigurasi, langkah awal yang perlu dilakukan adalah merestart service dari bind, dengan perintah */etc/init.d/bind9 restart*

```
root@ns:/etc/bind# /etc/init.d/bind9 restart
Stopping domain name service...: bind9 waiting for pid 1879 to
die.
Starting domain name service...: bind9.
```

Pada perintah tersebut tidak boleh ada pesan error, kalau ada pesan error teliti kembali semua penulisan dari file-file mulai dari awal. Apabila tidak ada error kita dapat melakukan cek lagi terhadap service bind sudah terbuka atau belum dengan menggunakan *nmap*.

```
root@ns:/# nmap localhost
```

```
Starting Nmap 5.00 ( http://nmap.org ) at 2011-07-03 21:36 WIT
Interesting ports on localhost (127.0.0.1):
Not shown: 993 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
```

Setelah memastikan port 53 terbuka, kita dapat melakukan pengujian terhadap DNS server yang baru kita bangun dengan perintah *nslookup* atau bisa juga dengan *dig*. Pengujian ini bisa dilakukan di mesin server langsung atau bisa juga menggunakan client yang memang sudah terhubung dengan server, kalau kita menggunakan MS windows kita bisa mengujinya melalui CMD dengan menggunakan perintah nslookup.

```
root@ns:/# nslookup ns.gaplek.gk
```

```
Server:         192.168.2.2
Address:        192.168.2.2#53

Name:   ns.gaplek.gk
Address: 192.168.2.2
```

```
root@ns:/# nslookup  192.168.2.2
Server:         192.168.2.2
Address:        192.168.2.2#53

2.2.168.192.in-addr.arpa        name = ns.gaplek.gk.
```

```
root@ns:/# nslookup www.facebook.com
Server:         192.168.2.2
Address:        192.168.2.2#53

Non-authoritative answer:
Name:   www.facebook.com
Address: 69.171.224.12
```

Dari pengujian di atas dapat diamati bahwa DNS server yang kita buat sudah dapat menjawad semua permitaan dari kita menggunakan perintah nslookup ataupun dengan dig.

C. MANAJEMEN HOTSPOT

C.1. Pengantar

Chillispot adalah perangkat lunak yang menyediakan otentikasi dan digunakan untuk membatasi client untuk akses jaringan. Penggunaan utamanya adalah jaringan nirkabel (WiFi).

Silahkan melihat di situs web Chillispot.info untuk melihat bagaimana software ini bekerja. Dalam beberapa hal, hillispot menciptakan virtual private network yang digunakan untuk berkomunikasi dengan client kemudian memutuskan siapa dan bagaimana client dapat mengakses jaringan yang lebih luar. Secara default jaringan yang digunakan adalah 192.168.182.0/24, tetapi kita dapat mengubah sesuai dengan keadaan jaringan kita. Chillispot mengelola alokasi alamat IP dinamis kepada klien, sehingga kita tidak memerlukan mesin DHCP yang lain.

C.2. Instalasi

Setidaknya kita minimal membutuhkan dua LAN card (NIC) agar chillispot dapat bekerja sekaligus sebagai router. Install Debian GNU/Linux dan konfigurasi ip address pada NIC.

```
pico /etc/network/interfaces
```

Harusnya isi file /etc/network/interfaces adalah sebagai berikut:

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

# The loopback network interface
```

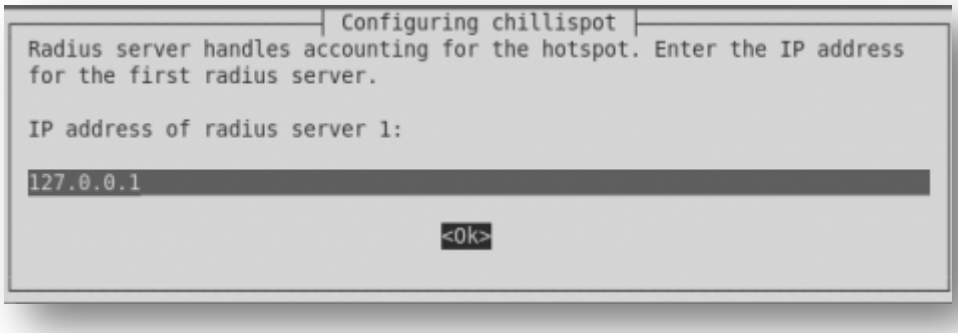
```
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
    address 192.168.2.2
    netmask 255.255.255.0
    gateway 192.168.2.1
```

eth0 (WAN) IP address yang kearah luar atau internet.
eth1 (LAN) tidak perlu kita konfigurasi.

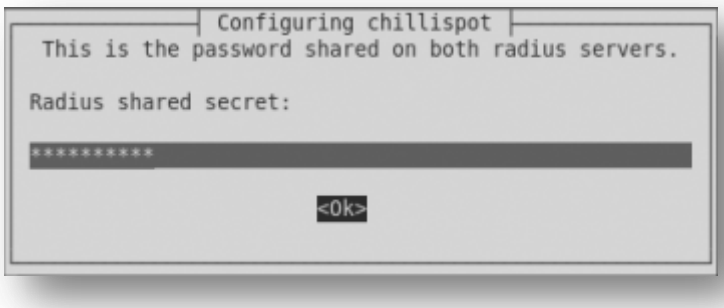
Kita tidak perlu mengkonfigurasi eth1 karena nantinya Chillispot akan membuat aturan untuk memberikan IP address dengan menggunakan DHCP sendirinya sendiri.
Install chillispot dan applikasi-applikasi pendukungnya

```
apt-get install apache2 ssl-cert mysql-client mysql-server
chillispot freeradius freeradius-mysql
```

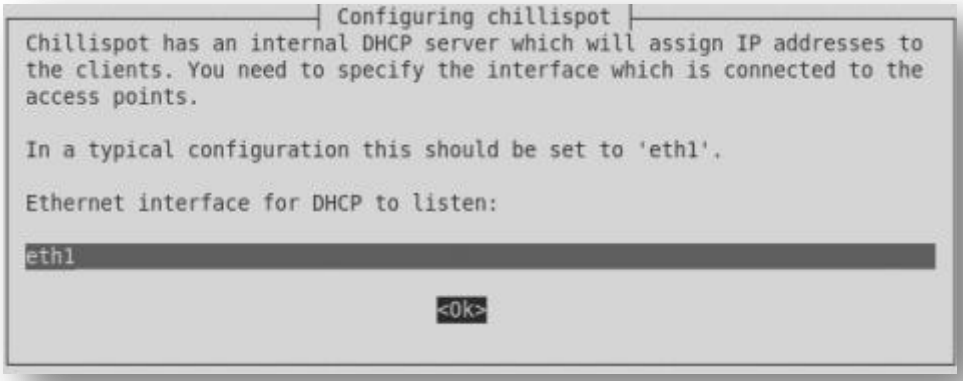
Perintah di atas digunakan untuk menginstall Apache, MySQL, Chillispot dan FreeRadius. Setelah instalasi akan muncul menu untuk mengisi konfigurasi standart.



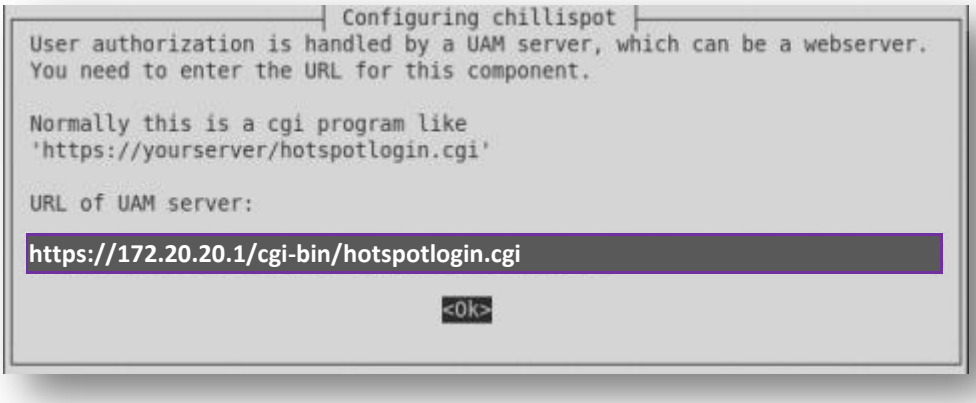
Isikan ip address dari radius server, untuk tutorial kali ini kita akan menggunakan 127.0.0.1 karena radius server terinstall pada satu mesin dengan Chillispot



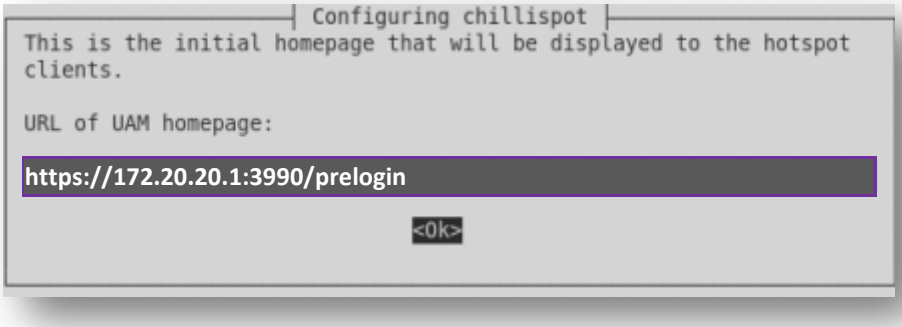
Masukkan *radius shared secret* dengan kata kunci yang nantinya akan digunakan oleh Chillispot untuk berkomunikasi dengan radius server.



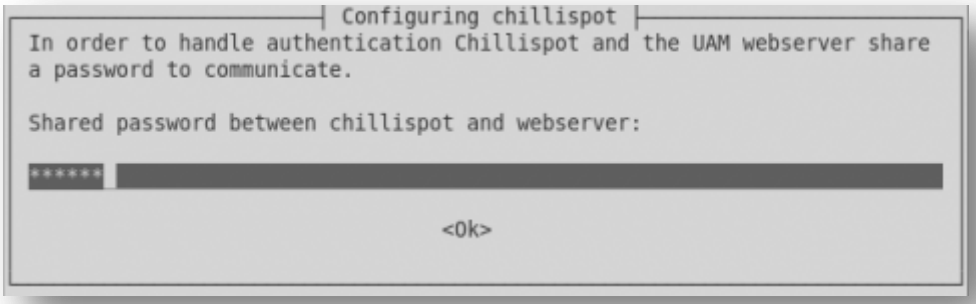
Pada pilih NIC isikan NIC yang terhubung dengan LAN, pada kasus ini kita akan menggunakan eth1 dimana pada eth1 ini nanti akan memberikan layanan DHCP yang dibangkitkan oleh Chillispot.



Masukkan alamat dari Universal Access Method (UAM), Chillispot akan menggunakan halaman dari alamat UAM ini untuk digunakan sebagai form login tiap user yang berusaha mengakses jaringan yang dikelolanya. Dalam kasus kita server authentifikasi berada satu mesin dengan chillispot, 172.20.20.1 merupakan ip address yang akan diberikan untuk interface tun0.



Masukkan alamat URL yang diperbolehkan diakses tanpa harus melakukan login. Biasanya ini adalah alamat-alamat lokal yang digunakan sebagai iklan atau tawaran terhadap suatu produk. Pada isian ini boleh dikosongi, namun nanti kita harus mematkan uamhomepage secara manual di /etc/chilli.conf



Kemudian isikan key yang akan digunakan chillispot dan hotspotlogin.cgi sehingga script CGI dapat berkomunikasi dengan chillispot, key ini berbeda dengan key yang digunakan untuk radius server. Selanjutnya edit file /usr/lib/cgi-bin/hotspotlogin.cgi

```
pico /usr/lib/cgi-bin/hotspotlogin.cgi
```

Uncomment garis *#$uamsecret = "ht2eb8ej6s4et3rg1ulp";* dan ganti dengan *"ht2eb8ej6s4et3rg1ulp";* dengan *uamsecret* yang sama dengan key yang pernah kita berikan pada saat instalasi Chillispot di atas.

```
$uamsecret = "sandi";
```

C.3. Konfigurasi

Langkah awal adalah kita perlu melakukan penyesuaian terhadap file /etc/chilli.conf. File ini perlu kita sesuaikan dengan keperluan jaringan kita apabila dalam proses instalasi di atas terjadi kekeliruan pengisian atau memang kita hendak melakukan perubahan. Opsi-opsi penting yang perlu kita perhatikan adalah bagian-bagian yang ditandai dan baris yang awalnya diberi tanda "#" tidak dibaca oleh sistem atau bisa hanya merupakan keterangan.

chilli.conf

```
pico /etc/chilli.conf
```

```
######### di potong ###############


# TUN parameters

# TAG: net
# IP network address of external packet data network
# Used to allocate dynamic IP addresses and set up routing.
# Normally you do not need to uncomment this tag.
```

```
#net 192.168.182.0/24
net 172.20.20.0/24

# TAG: dynip
# Dynamic IP address pool
# Used to allocate dynamic IP addresses to clients.
# If not set it defaults to the net tag.
# Do not uncomment this tag unless you are an experienced user!
#dynip 192.168.182.0/24

# TAG: statip
# Static IP address pool
# Used to allocate static IP addresses to clients.
# Do not uncomment this tag unless you are an experienced user!
#statip 192.168.182.0/24


# TAG: dns1
# Primary DNS server.
# Will be suggested to the client.
# If omitted the system default will be used.
# Normally you do not need to uncomment this tag.

#dns1 adalah IP address dari dns server yang kita siapkan, apabila
#belum memiliki DNS sever sendiri bisa digunakan DNS server yang
#ada di internet.
dns1 192.168.2.2

# TAG: dns2
# Secondary DNS server.
# Will be suggested to the client.
# If omitted the system default will be used.
# Normally you do not need to uncomment this tag.
#dns2 172.16.0.6

# TAG: domain
# Domain name
# Will be suggested to the client.
# Normally you do not need to uncomment this tag.
domain gaplek.gk

# TAG: ipup
# Script executed after network interface has been brought up.
# Executed with the following parameters: <devicename> <ip address>
# <mask>
# Normally you do not need to uncomment this tag.
#ipup /etc/chilli.ipup

# TAG: ipdown
# Script executed after network interface has been taken down.
# Executed with the following parameters: <devicename> <ip address>
# <mask>
# Normally you do not need to uncomment this tag.
#ipdown /etc/chilli.ipdown


# Radius parameters

# TAG: radiuslisten
# IP address to listen to
# Normally you do not need to uncomment this tag.
#radiuslisten 127.0.0.1

# TAG: radiusserver1
# IP address of radius server 1
# For most installations you need to modify this tag.
```

```
radiusserver1 127.0.0.1

# TAG: radiusserver2
# IP address of radius server 2
# If you have only one radius server you should set radiusserver2 to the
# same value as radiusserver1.
# For most installations you need to modify this tag.
radiusserver2 127.0.0.1

# TAG: radiusauthport
# Radius authentication port
# The UDP port number to use for radius authentication requests.
# The same port number is used for both radiusserver1 and radiusserver2.
# Normally you do not need to uncomment this tag.
#radiusauthport 1812

# TAG: radiusacctport
# Radius accounting port
# The UDP port number to use for radius accounting requests.
# The same port number is used for both radiusserver1 and radiusserver2.
# Normally you do not need to uncomment this tag.
#radiusacctport 1813

# TAG: radiussecret
# Radius shared secret for both servers
# For all installations you should modify this tag.
radiussecret sandi

# TAG: radiusnasid
# Radius NAS-Identifier
# Normally you do not need to uncomment this tag.
#radiusnasid nas01

# TAG: radiuslocationid
# WISPr Location ID. Should be in the format: isocc=<ISO_Country_Code>,
# cc=<E.164_Country_Code>,ac=<E.164_Area_Code>,network=<ssid/ZONE>
# Normally you do not need to uncomment this tag.
#radiuslocationid isocc=us,cc=1,ac=408,network=ACMEWISP_NewarkAirport

# TAG: radiuslocationname
# WISPr Location Name. Should be in the format:
# <HOTSPOT_OPERATOR_NAME>,<LOCATION>
# Normally you do not need to uncomment this tag.
#radiuslocationname ACMEWISP,Gate_14_Terminal_C_of_Newark_Airport


# Radius proxy parameters

# TAG: proxylisten
# IP address to listen to
# Normally you do not need to uncomment this tag.
#proxylisten 10.0.0.1

# TAG: proxyport
# UDP port to listen to.
# If not specified a port will be selected by the system
# Normally you do not need to uncomment this tag.
#proxyport 1645

# TAG: proxyclient
# Client(s) from which we accept radius requests
# Normally you do not need to uncomment this tag.
#proxyclient 10.0.0.1/24

# TAG: proxysecret
# Radius proxy shared secret for all clients
```

```
# If not specified defaults to radiussecret
# Normally you do not need to uncomment this tag.
#proxysecret testing123


# DHCP Parameters

# TAG: dhcpif
# Ethernet interface to listen to.
# This is the network interface which is connected to the access points.
# In a typical configuration this tag should be set to eth1.
dhcpif eth1

# TAG: dhcpmac
# Use specified MAC address.
# An address in the range  00:00:5E:00:02:00 - 00:00:5E:FF:FF:FF falls
# within the IANA range of addresses and is not allocated for other
# purposes.
# Normally you do not need to uncomment this tag.
#dhcpmac 00:00:5E:00:02:00

# TAG: lease
# Time before DHCP lease expires
# Normally you do not need to uncomment this tag.
#lease 600


# Universal access method (UAM) parameters

# TAG: uamserver
# URL of web server handling authentication.
uamserver https://172.20.20.1/cgi-bin/hotspotlogin.cgi

# TAG: uamhomepage
# URL of welcome homepage.
# Unauthenticated users will be redirected to this URL. If not specified
# users will be redirected to the uamserver instead.
# Normally you do not need to uncomment this tag.

#Apabila tidak ada alamat yang boleh diakses tanpa login
#sebaiknya beri tanda comment "#" pada uamhopage

#uamhomepage https://172.20.20.1:3990/prelogin
#uamhomepage

# TAG: uamsecret
# Shared between chilli and authentication web server
uamsecret sandi

# TAG: uamlisten
# IP address to listen to for authentication requests
# Do not uncomment this tag unless you are an experienced user!
#uamlisten 192.168.182.1

#####  dipotong #########
```

Mengaktifkan Chillispot

Pada konfigurasi awal (*default*) chillispot tidak bisa digunakan (*not enabled*), sehingga kita harus melakukan sedikit konfigurasi agar chillispot agar dapat diaktifkan dengan cara mengedit file */etc/default/chillispot*.

```
pico /etc/default/chillispot
```

dan ubah baris **ENABLED=0** dengan **ENABLED=1**

```
# /etc/default/chillispot
#
# Enable on system start?
# Change to 1 if you want it to be enabled.
# Please make sure you have configured chillispot first.
ENABLED=1
#
# chillispot default configuration
CHILLICFG=/etc/chilli.conf
#
# daemon arguments
DAEMON_ARGS="--conf $CHILLICFG"
```

Berikutnya muat ulang service dari chillispot

```
/etc/init.d/chillispot restart
```

Untuk melihat apakah chillispot sudah berjalan dengan normal kita bisa menggunakan perintah ifconfig,

```
root@ns:~# ifconfig
```

```
eth0      Link encap:Ethernet  HWaddr 00:0c:29:c0:de:a9
          inet addr:192.168.2.2  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fec0:dea9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:79 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9787 (9.5 KiB)  TX bytes:14079 (13.7 KiB)
          Interrupt:18 Base address:0x2000

eth1      Link encap:Ethernet  HWaddr 00:0c:29:c0:de:b3
          inet6 addr: fe80::20c:29ff:fec0:deb3/64 Scope:Link
          UP BROADCAST RUNNING  MTU:1500  Metric:1
          RX packets:132 errors:0 dropped:0 overruns:0 frame:0
          TX packets:31 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:15306 (14.9 KiB)  TX bytes:5573 (5.4 KiB)
          Interrupt:19 Base address:0x2080

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:35 errors:0 dropped:0 overruns:0 frame:0
          TX packets:35 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2990 (2.9 KiB)  TX bytes:2990 (2.9 KiB)

tun0      Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-
00
          inet addr:172.20.20.1  P-t-P:172.20.20.1  Mask:255.255.255.0
          UP POINTOPOINT RUNNING  MTU:1500  Metric:1
          RX packets:1 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:500
          RX bytes:62 (62.0 B)  TX bytes:2352 (2.2 KiB)
```

Apabila interface tun0 sudah muncul dengan IP address sesuai dengan konfigurasi yang dikehendaki berarti chillispot sudah berjalan dengan normal, langkah berikutnya adalah konfigurasi apache agar dapat meredirect halaman web yang diminta client pada awal pertama kali mencoba browsing melalui browser ke *form login* dari chillspot menggunakan CGI script.

Konfigurasi Apache untuk Chillispot

Karena nantinya chillispot menggunakan protokoll https untuk melakukan komunikasi dengan *client* lewat *webbase form* maka perlu dibuat sertifikat *selft-signed* SSL,

```
mkdir /etc/apache2/ssl
make-ssl-cert /usr/share/ssl-cert/ssleay.cnf
/etc/apache2/ssl/apache.pem
```

Aktifkan *mod_ssl*

```
pico  /etc/apache2/ports.conf
```

```
NameVirtualHost *:80
Listen 80

<IfModule mod_ssl.c>
    # If you add NameVirtualHost *:443 here, you will also have to
change
    # the VirtualHost statement
    # in /etc/apache2/sites-available/default-ssl
    # to <VirtualHost *:443>
    # Server Name Indication for SSL named virtual hosts is currently
not
    # supported by MSIE on Windows XP.
    Listen 443
</IfModule>

<IfModule mod_gnutls.c>
    Listen 443
</IfModule>
```

Selanjutnya ketikkan perintah dibawah untuk mengaktifkan mod_ssl

```
a2enmod ssl
/etc/init.d/apache2 restart
```

Buat host dengan cara duplikasi file konfigurasi virtual host /etc/apache2/site-available/default dan ubah dengan nama yang lain, dalam kasus ini misal kita ubah menjadi “secure”.

```
cp /etc/apache2/sites-available/default /etc/apache2/sites-
available/secure
```

Edit file

```
pico /etc/apache2/sites-available/secure
```

kemudian ubah dua baris berikut :

```
NameVirtualHost *
<VirtualHost *>
```

menjadi

```
NameVirtualHost *:443
<VirtualHost *:443>
        SSLEngine on
        SSLCertificateFile /etc/apache2/ssl/apache.pem
```

Aktifkan *secure host* dan restart apache

```
a2ensite secure
/etc/init.d/apache2 restart
```

Konfigurasi FreeRadius

Sesuaikan file /etc/freeradius/clients.conf, perhatikan baris yang diberi tanda.

```
pico /etc/freeradius/clients.conf
```

```
#### dipotong ##########

client 127.0.0.1 {
        #
        #  The shared secret use to "encrypt" and "sign" packets between
       #  the NAS and FreeRADIUS.  You MUST change this secret from the
       #  default, otherwise it's not a secret any more!
       #
       #  The secret can be any string, up to 31 characters in length.
        #
        secret          = sandi
        #
        #  The short name is used as an alias for the fully qualified
       #  domain name, or the IP address.
       #
       shortname       = localhost
       #
       # the following three fields are optional, but may be used by
       # checkrad.pl for simultaneous use checks
       #
       #
       # The nastype tells 'checkrad.pl' which NAS-specific method to
       #  use to query the NAS for simultaneous use.
       #
       #  Permitted NAS types are:
       #
       #       cisco
       #       computone
       #       livingston
       #       max40xx
   #        multitech
        #        netserver
        #        pathras
        #        patton
        #        portslave
        #        tc
        #        usrhiper
        #        other           # for all other types
        #
```

```
        nastype     = other     # localhost isn't usually a NAS...
        #
        #  The following two configurations are for future use.
       #  The 'naspasswd' file is currently used to store the NAS
       #  login name and password, which is used by checkrad.pl
       #  when querying the NAS for simultaneous use.
       #
#        login       = !root
#        password    = someadminpas
}

###### dipotong ############
```

Sebelum menggunakan virtual user dari database, sangat disarankan dicoba dulu menggunakan user dari daftar user yang ada dalam */etc/freeradius/users*. Edit *file /etc/freeradius/users* kemudian kita aktifkan user yang sudah ada dalam file tersebut atau bisa juga kita membuat user sendiri.

```
pico /etc/freeradius/users
```

Cari baris seperti di bawah

```
#steveCleartext-Password := "testing"
```

Kemudian ubah menjadi

```
steve Cleartext-Password := "testing"
```

Baris di atas artinya kita menambahkan user steve dengan password testing.
Langkah berikutnya restart service dari freeradius

```
/etc/init.d/freeradius restart
```

Pastikan tidak ada pesan error pada perintah tersebut.
Untuk memeriksa apakah freeradius sudah melakukan service dengan benar atau belum kita coba menggunakan user yang baru diaktifkan tadi dengan menggunakan perintah radtest.

```
root@ns:~# radtest steve testing localhost 1812 sandi
Sending Access-Request of id 151 to 127.0.0.1 port 1812
        User-Name = "steve"
        User-Password = "testing"
        NAS-IP-Address = 192.168.2.2
        NAS-Port = 1812
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812,
id=151, length=20
```

Perhatikan pada informasi *rad_rev* harus ada info *Access-Accept* kalau gagal biasanya informasinya ada *Access-Reject.*
Sampai pada tahap ini berarti freeradius berjalan dengan benar untuk memastikan lagi apakah sudah bisa digunakan oleh chiilispot Anda bisa langsung mencoba dengan langkah seperti pada bagian **C.4. Uji Coba**.

Setelah dipastikan freeradius sudah berjalan dengan normal maka pada tahap selanjutnya kita akan mengubah penggunaan daftar user yang tadinya berada pada file */etc/freeradius/users* ke

daftar user yang berada dalam database. Dalam hal ini kita akan menggunakan database MySQL. Agar freradius dapat berkomunikasi dengan database MySQL ada beberapa file yang harus kita sesuaikan yaitu /etc/freeradius/sql.conf dan /etc/freeradius/site-enabled/default.
Namun sebelum kita melakukan berubahan terhadap file tadi kita siapkan terlebih dahulu database yang akan digunakan untuk menampung data dari user.

Konfigurasi MySQL server

Login ke dalam MySQL consule,

```
mysql –u root –p
```

kemudian buat database “radius” dan user “radius” dimana user “radius” ini memiliki hak penuh terhadapat data base “radius” dan password dari dari user “radius” adalah “pklm”.

```
CREATE DATABASE radius;
GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY 'pklm';
```

Ambil tabel schema dari /etc/freeradius/sql/mysql/schema.sql kemudian export ke database “radius”,

```
mysql –u root –p pklm radius < /etc/freeradius/sql/mysql/schema.sql
```

Hasil dari export tadi dapat dilihat dengan cara masuk ke dalam database melalui MySQL console, ingat user adalah “radius” dan password adalah “pklm”.

```
mysql –u radius  -p

mysql> use radius;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed

mysql> show tables;
+------------------+
| Tables_in_radius |
+------------------+
| radacct          |
| radcheck         |
| radgroupcheck    |
| radgroupreply    |
| radpostauth      |
| radreply         |
| radusergroup     |
+------------------+
7 rows in set (0.00 sec)
```

Dari beberapa tabel yang ada kita cukup menggunakan tabel radcheck untuk menyimpan data dari user. Tabel ini memiliki 4 field *yaitu id, username, attribute, op* dan *value*.

```
mysql> desc radcheck;
+-----------+------------------+------+-----+---------+----------------+
| Field     | Type             | Null | Key | Default | Extra          |
+-----------+------------------+------+-----+---------+----------------+
| id        | int(11) unsigned | NO   | PRI | NULL    | auto_increment |
| username  | varchar(64)      | NO   | MUL |         |                |
| attribute | varchar(64)      | NO   |     |         |                |
| op        | char(2)          | NO   |     | ==      |                |
```

```
| value     | varchar(253)     | NO   |     |         |                |
+-----------+------------------+------+-----+---------+----------------+
5 rows in set (0.00 sec)
```

Secara default tabel ini belum ada isinya sehingga kita perlu memberikan isian untuk nantinya digunakan sebagai uji coba. Masih dalam MySQL console isikan satu atau dua data,

```
mysql> insert into radcheck (`username`, `attribute`, `value`) values
("anang", "password", "anang123");

Query OK, 1 row affected (0.00 sec)

mysql> insert into radcheck (`username`, `attribute`, `value`) values
("joko", "password", "joko123");

Query OK, 1 row affected (0.00 sec)

mysql> select  * from radcheck;
+----+----------+-----------+----+---------+
| id | username | attribute | op | value   |
+----+----------+-----------+----+---------+
|  1 | anang    | password  | == | anang123|
|  2 | joko     | password  | == | joko123 |
+----+----------+-----------+----+---------+
2 rows in set (0.00 sec)
```

Langkah selanjutnya kita melakukan penyesuain kembali terhadap file */etc/freeradius/sql.conf* ,

```
pico /etc/freeradius/sql.conf
```

tambahkan informasi mengenai database yang akan dipakai oleh freeradius agar freeradius dapat terkoneksi dengan database tersebut.

```
# Connect info
        server = "localhost"
        login = "radius"
        password = "pklm"

        # Database table configuration
        radius_db = "radius"
```

Berikutnya edit file /etc/freeradius/site-enabled/default , matikan baris *files* dan aktifkan baris *sql*.

```
##### dipotong #########

authorize {
   #
   #  The preprocess module takes care of sanitizing some bizarre
   #  attributes in the request, and turning them into attributes
   #  which are more standard.
   #
   #  It takes care of processing the 'raddb/hints' and the
   #  'raddb/huntgroups' files.
   preprocess

   ##### dipotong #############

   #
   #  Read the 'users' file
```

```
#  files

   #
   #  Look in an SQL database.  The schema of the database
   #  is meant to mirror the "users" file.
   #
   #  See "Authorization Queries" in sql.conf
   sql

   #
   #  If you are using /etc/smbpasswd, and are also doing
   #  mschap authentication, the un-comment this line, and
   #  configure the 'etc_smbpasswd' module, above.

############ dipotong ############

accounting {
   #
   #  Create a 'detail'ed log of the packets.
   #  Note that accounting requests which are proxied
   #  are also logged in the detail file.
   detail
#  daily

   #  Update the wtmp file
   #
   #  If you don't use "radlast", you can delete this line.
   unix

   #
   #  For Simultaneous-Use tracking.
   #
   #  Due to packet losses in the network, the data here
   #  may be incorrect.  There is little we can do about it.
   radutmp
#  sradutmp

   #  Return an address to the IP Pool when we see a stop record.
#  main_pool

   #
   #  Log traffic to an SQL database.
   #
   #  See "Accounting queries" in sql.conf
   sql

   #
   #  If you receive stop packets with zero session length,
   #  they will NOT be logged in the database.  The SQL module
   #  will print a message (only in debugging mode), and will
   #  return "noop".
   #
   #  You can ignore these packets by uncommenting the following
   #  three lines.  Otherwise, the server will not respond to the
   #  accounting request, and the NAS will retransmit.
   #
############### dipotong #############
```

Langkah selanjutnya restart freeradius

```
/etc/init.d/freeradius restart
```

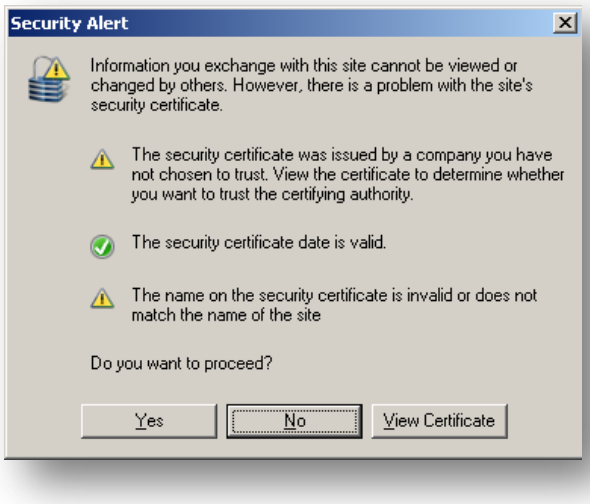
Pastikan tidak ada pesan error pada perintah tersebut. Untuk memeriksa apakah freeradius sudah melakukan service dengan benar atau belum kita coba menggunakan user yang ada dalam database misal user "*anang*" dan password "*pklm*" dengan menggunakan perintah radtest.

```
root@ns:~# radtest anang anang123 localhost 1812 sandi
Sending Access-Request of id 151 to 127.0.0.1 port 1812
        User-Name = "anang"
        User-Password = "anang123"
        NAS-IP-Address = 192.168.2.2
        NAS-Port = 1812
rad_recv: Access-Accept packet from host 127.0.0.1 port 1812,
id=151, length=20
```

C.4. Pengujian

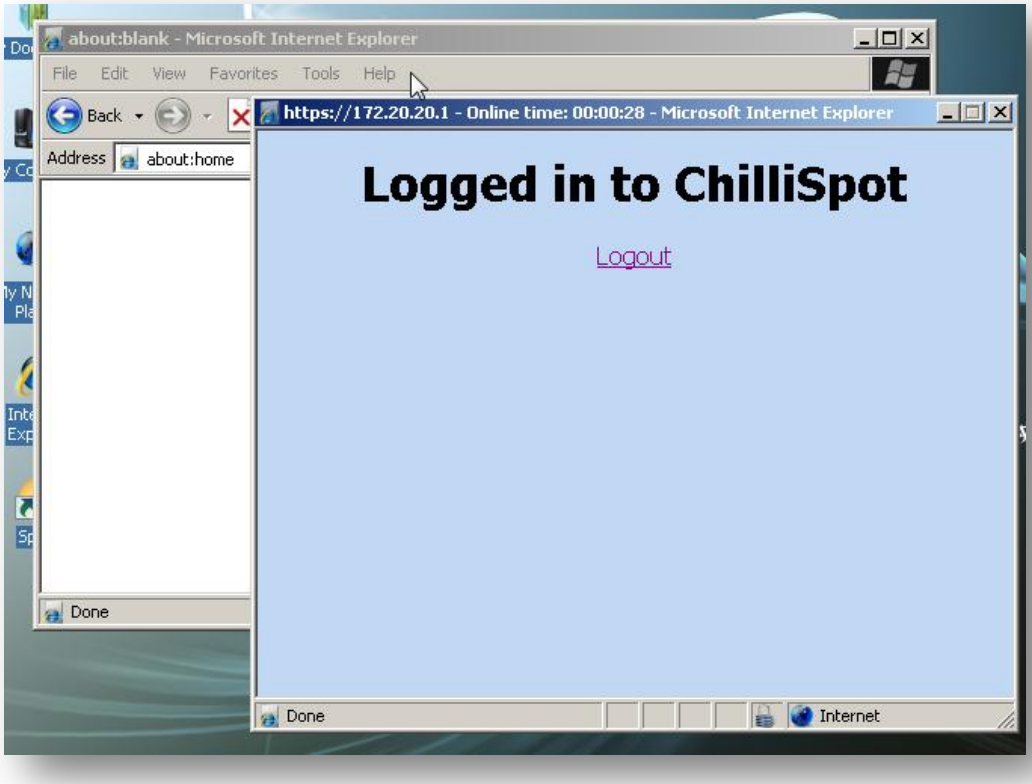
Cara paling mudah untuk memastikan apakah server hotspot kita bisa bekerja sesuai dengan konfigurasi kita atau belum adalah dengan mengcoba langsung pada sisi client. Sistem operasi pada client bisa menggunakan sistem operasi apa saja, yang penting telah terinstall web browser karena sistem authentifikasi pada sisi client menggunakan interface web base.

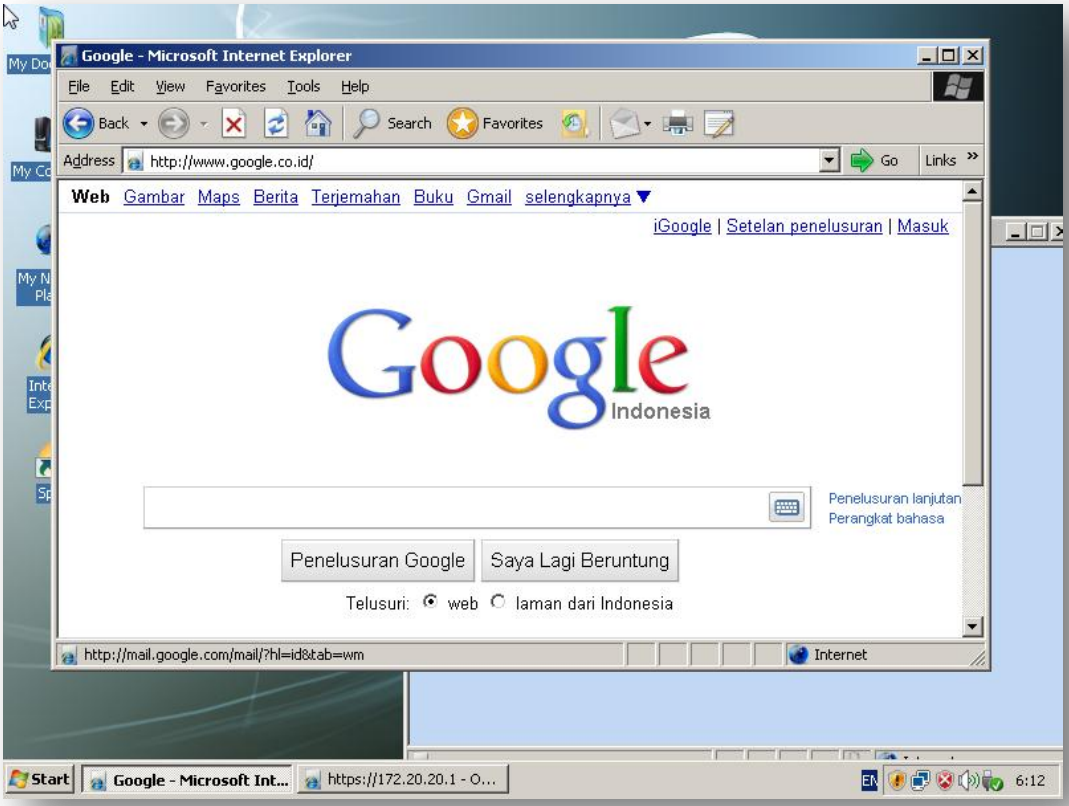
Pada client langsung dicoba untuk melakukan browsing ke alama tertentu misal google.com. Pada saat kita pertama kali mencoba untuk browsing maka secara otomotis akan diarahkan ke halaman form login yang dimiliki oleh chillispot menggunakan protokol htts, sehingga pada client akan muncul popup (browser yang digunakan IE, untuk browser yang lain tampilan akan sedikit berbeda) berikut :



Jawab dengan "Yes" kemudian akan muncul halaman login, isikan dengan username dan password yang telah diisikan dalam database "radius",

Apabila pada browser popup tidak diblock maka setelah login berhasil akan muncul 2 jendela,




Google - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.google.co.id/
Go Links
Web Gambar Maps Berita Terjemahan Buku Gmail selengkapnya
iGoogle | Setelan penelusuran | Masuk
Google
Indonesia
Penelusuran lanjutan
Perangkat bahasa
Penelusuran Google
Saya Lagi Beruntung
Telusuri: web laman dari Indonesia
http://mail.google.com/mail/?hl=id&tab=wm
Internet
Start
Google - Microsoft Int...
https://172.20.20.1 - O...
6:12

D. FTP SERVER DENGAN VIRTUAL USER

D.1. Pengantar

Dokumen ini menjelaskan cara menginstal server yang menggunakan Proftpd pengguna virtual dari database MySQL, bukan pengguna sistem nyata. Konfigurasi dengan virtual user lebih memiliki performa yang lebih baik dan memungkinkan untuk memiliki ribuan pengguna ftp pada mesin tunggal. Selain itu kita juga akan menggunaan kuota pada setiap user.

Untuk administrasi database MySQL Anda dapat menggunakan alat berbasis web seperti phpMyAdmin atau bisa juga dengn menggunakan console MySQL. phpMyAdmin adalah antarmuka grafis yang nyaman yang berarti Anda tidak perlu dipusingkan dengan baris perintah.

Pada tutorial ini sesuai dengan topologi yang sudah diterangkan diawal saya menggunakan server dengan IP address 192.168.2.2 dengan hostname ftp.gaplek.gk. Apabila Anda menginginkan IP address dan hostname yang lain silakan disusaikan.

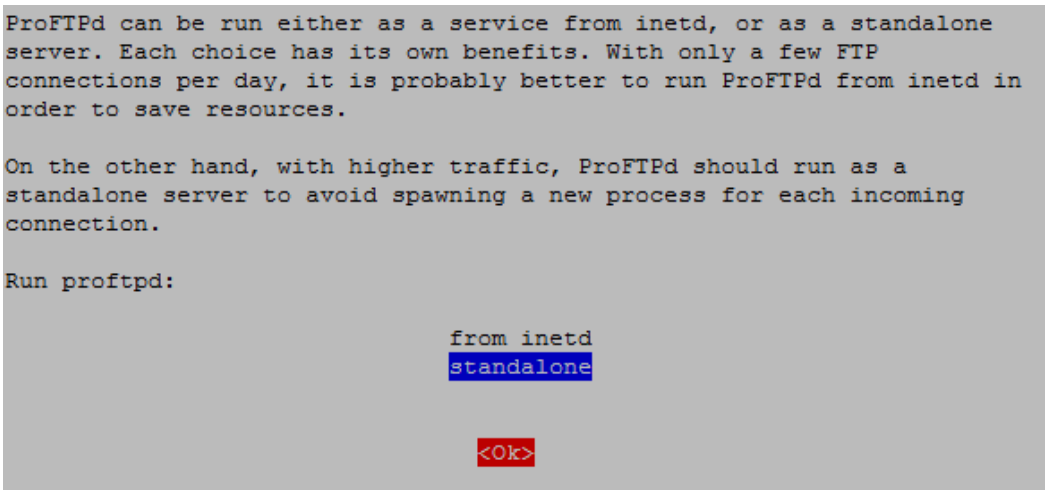
D.2. Instalasi

Instalasi ProFTP

Untuk memasang proftp yang support MySQL lakukan perintah instalasi seperti dibawah,

```
apt-get install proftpd-mod-mysql
```

pada saat instalasi akan muncul pertanyaan seperti dibawah



Jawab dengan memilih "`standalone`" kemudian "`<OK>`"

Kemudian kita buat group untuk ftp (*ftpgroup*) dan pengguna (*ftpuser*) yang semuanya ini nanti kita akan petakan sebagai virtual user.

```
groupadd -g 2001 ftpgroup
useradd -u 2001 -s /bin/false -d /bin/null -c "proftpd user" -g
ftpgroup ftpuser
```

Anda bisa menggunakan nama group dan userid selain 2001 asalkan nama group dan userid tersebut belum ada yang menggunakan pada sistem

MySQL database untuk ProFTP

Sekarang kita membuat database "ftp" dan "proftpd" sebagai user MySQL yang nantinya akan digunakan untuk menghubungkan ke database ftp:

```
mysql -u root -p

create database ftp;

GRANT SELECT, INSERT, UPDATE, DELETE ON ftp.* TO
'proftpd'@'localhost' IDENTIFIED BY 'password';

GRANT SELECT, INSERT, UPDATE, DELETE ON ftp.* TO
'proftpd'@'localhost.localdomain' IDENTIFIED BY 'password';

FLUSH PRIVILEGES;
```

Berikutnya masih dalam console MySQL kita buat table dalam database "ftp",

```
USE ftp;

CREATE TABLE ftpgroup (
groupname varchar(16) NOT NULL default '',
gid smallint(6) NOT NULL default '5500',
members varchar(16) NOT NULL default '',
KEY groupname (groupname)
) TYPE=MyISAM COMMENT='ProFTP group table';

CREATE TABLE ftpquotalimits (
name varchar(30) default NULL,
quota_type enum('user','group','class','all') NOT NULL default
'user',
per_session enum('false','true') NOT NULL default 'false',
limit_type enum('soft','hard') NOT NULL default 'soft',
bytes_in_avail int(10) unsigned NOT NULL default '0',
bytes_out_avail int(10) unsigned NOT NULL default '0',
bytes_xfer_avail int(10) unsigned NOT NULL default '0',
files_in_avail int(10) unsigned NOT NULL default '0',
files_out_avail int(10) unsigned NOT NULL default '0',
files_xfer_avail int(10) unsigned NOT NULL default '0'
) TYPE=MyISAM;

CREATE TABLE ftpquotatallies (
name varchar(30) NOT NULL default '',
quota_type enum('user','group','class','all') NOT NULL default
'user',
bytes_in_used int(10) unsigned NOT NULL default '0',
bytes_out_used int(10) unsigned NOT NULL default '0',
bytes_xfer_used int(10) unsigned NOT NULL default '0',
```

```
files_in_used int(10) unsigned NOT NULL default '0',
files_out_used int(10) unsigned NOT NULL default '0',
files_xfer_used int(10) unsigned NOT NULL default '0'
) TYPE=MyISAM;

CREATE TABLE ftpuser (
id int(10) unsigned NOT NULL auto_increment,
userid varchar(32) NOT NULL default '',
passwd varchar(32) NOT NULL default '',
uid smallint(6) NOT NULL default '5500',
gid smallint(6) NOT NULL default '5500',
homedir varchar(255) NOT NULL default '',
shell varchar(16) NOT NULL default '/sbin/nologin',
count int(11) NOT NULL default '0',
accessed datetime NOT NULL default '0000-00-00 00:00:00',
modified datetime NOT NULL default '0000-00-00 00:00:00',
PRIMARY KEY (id),
UNIQUE KEY userid (userid)
) TYPE=MyISAM COMMENT='ProFTP user table';

quit;
```

Langkah berikutnya adalah mengkonfigurasi ProFTP.

D.3. Konfigurasi

Langkah awal adalah mematikan IPv6 pada ProFTP karena kita hanya akan menggunakan IPv4,

```
pico /etc/proftpd/proftpd.conf
```

```
###### dipotong ###########
# Includes DSO modules
Include /etc/proftpd/modules.conf

# Set off to disable IPv6 support which is annoying on IPv4 only boxes.
UseIPv6                 off
# If set on you can experience a longer connection delay in many cases.
IdentLookups            off

ServerName              "Debian"
ServerType              standalone
DeferWelcome              off

########### dipotong ##############
```

Berikutnya edit file /etc/proftpd/sql.conf

```
pico /etc/proftpd/sql.conf
```

Kemudian tambahkan baris berikut sebelum tanda **</IfModule>**

```
##### dipotong ###########
DefaultRoot ~

SQLBackend              mysql
# The passwords in MySQL are encrypted using CRYPT
SQLAuthTypes            Plaintext Crypt
```

```
SQLAuthenticate         users groups


# used to connect to the database
# databasename@host database_user user_password
SQLConnectInfo  ftp@localhost proftpd password


# Here we tell ProFTPd the names of the database columns in the
"usertable"
# we want it to interact with. Match the names with those in the
db
SQLUserInfo     ftpuser userid passwd uid gid homedir shell

# Here we tell ProFTPd the names of the database columns in the
"grouptable"
# we want it to interact with. Again the names match with those
in the db
SQLGroupInfo    ftpgroup groupname gid members

# set min UID and GID - otherwise these are 999 each
SQLMinID        500

# create a user's home directory on demand if it doesn't exist
CreateHome on

# Update count every time user logs in
SQLLog PASS updatecount
SQLNamedQuery updatecount UPDATE "count=count+1, accessed=now()
WHERE userid='%u'" ftpuser

# Update modified everytime user uploads or deletes a file
SQLLog  STOR,DELE modified
SQLNamedQuery modified UPDATE "modified=now() WHERE userid='%u'"
ftpuser

# User quotas
# ===========
QuotaEngine on
QuotaDirectoryTally on
QuotaDisplayUnits Mb
QuotaShowQuotas on

SQLNamedQuery get-quota-limit SELECT "name, quota_type,
per_session, limit_type, bytes_in_avail, bytes_out_avail,
bytes_xfer_avail, files_in_avail, files_out_avail,
files_xfer_avail FROM ftpquotalimits WHERE name = '%{0}' AND
quota_type = '%{1}'"

SQLNamedQuery get-quota-tally SELECT "name, quota_type,
bytes_in_used, bytes_out_used, bytes_xfer_used, files_in_used,
files_out_used, files_xfer_used FROM ftpquotatallies WHERE name =
'%{0}' AND quota_type = '%{1}'"

SQLNamedQuery update-quota-tally UPDATE "bytes_in_used =
bytes_in_used + %{0}, bytes_out_used = bytes_out_used + %{1},
bytes_xfer_used = bytes_xfer_used + %{2}, files_in_used =
files_in_used + %{3}, files_out_used = files_out_used + %{4},
```

```
files_xfer_used = files_xfer_used + %{5} WHERE name = '%{6}' AND
quota_type = '%{7}'" ftpquotatallies

SQLNamedQuery insert-quota-tally INSERT "%{0}, %{1}, %{2}, %{3},
%{4}, %{5}, %{6}, %{7}" ftpquotatallies

QuotaLimitTable sql:/get-quota-limit
QuotaTallyTable sql:/get-quota-tally/update-quota-tally/insert-
quota-tally

RootLogin off
RequireValidShell off

</IfModule>
```

Selanjutnya aktifkan module yang digunakan ProFTP untuk terkoneksi dengan database MySQl

pico /etc/proftpd/modules.conf

Hilangkang tanda comment "#" pada baris `Loadmodule mod_sql.c` dan `LoadModule mod_sql_mysql.c`

```
### dipotong ####
LoadModule mod_ctrls_admin.c
LoadModule mod_tls.c

# Install one of proftpd-mod-mysql, proftpd-mod-pgsql or any other
# SQL backend engine to use this module and the required backend.
# This module must be mandatory loaded before anyone of
# the existent SQL backeds.
LoadModule mod_sql.c

# Install proftpd-mod-ldap to use this
#LoadModule mod_ldap.c

#
# 'SQLBackend mysql' or 'SQLBackend postgres' (or any other valid
backend) directives
# are required to have SQL authorization working. You can also
comment out the
# unused module here, in alternative.
#

# Install proftpd-mod-mysql and decomment the previous
# mod_sql.c module to use this.
LoadModule mod_sql_mysql.c

# Install proftpd-mod-pgsql and decomment the previous
# mod_sql.c module to use this.
#LoadModule mod_sql_postgres.c

##### dipotong #####
```

Kemudian restart service dari proftpd

```
/etc/init.d/proftpd restart
```

D.4. Pengisian Database dan Pengujian

Untuk pengisian database kita dapat menggunakan console MySQL

```
mysql –u proftpd –p

use ftp;
```

Pertama kita membuat sebuah entri dalam tabel ftpgroup, tabel ini memuat groupname, groupid sedang username dari pengguna ftp kita buat pada akhir langkah kedua (ganti *groupid* dengan *groupid* yang sesuai jika Anda menggunakan *groupid* selain 2001):

```
INSERT INTO `ftpgroup` (`groupname`, `gid`, `members`) VALUES
('ftpgroup', 2001, 'ftpuser');
```

Setelah tabel "*ftpgroup'* terbentuk, berikutnya kita membuat *user ftp virtual* baru. Dengan cara menambahkan user pada pada tabel "*ftpquotalimits*" tabel dan tabel "*ftpuser*". Pada tabel "ftpquotalimits" berisi informasi mengenai kuota besar space yang akan diperloeh oelh masing-masing user dan tabel "*ftpuser*" berisi mengenai semua informasi mengenai user ftp. Sebagai contoh kita membuat user pertama kami "***anang***" dengan kuota ***15 MB*** dan password "***rahasia***" (kita masih di shell MySQL):

```
INSERT INTO `ftpquotalimits` (`name`, `quota_type`,
`per_session`, `limit_type`, `bytes_in_avail`, `bytes_out_avail`,
`bytes_xfer_avail`, `files_in_avail`, `files_out_avail`,
`files_xfer_avail`) VALUES ('anang', 'user', 'true', 'hard',
15728640, 0, 0, 0, 0, 0);

INSERT INTO `ftpuser` (`id`, `userid`, `passwd`, `uid`, `gid`,
`homedir`, `shell`, `count`, `accessed`, `modified`) VALUES (1,
'anang', 'anang123', 2001, 2001, '/home/ftpuser/anang',
'/sbin/nologin', 0, '', '');

quit;
```

INGAT : Jangan lupa untuk menggantikan groud dan userid 2001 pada pernyataan SQL INSERT terakhir jika Anda menggunakan nilai selain 2001 dalam tutorial ini!

Sekarang buka program FTP client (seperti WS_FTP atau SmartFTP jika Anda menggunakan sistem operasi Windows atau gFTP pada desktop Linux) dengan komputer lain atau bisa juga langsung lewat console pada server dan mencoba untuk terhubung. Pada contoh ini kita gunakan cmd yang ada pada Windows dengan user "anang" dan password "anang123".

```
C:\Windows\System32>ftp 192.168.2.2
Connected to 192.168.2.2.
220 ProFTPD 1.3.3a Server (ftp.gaplek.gk) [192.168.2.2]
User (192.168.2.2:(none)): anang
331 Password required for anang
Password:
230 User anang logged in
ftp>
```

Jika Anda dapat terhubung berarti instalasi dan konfigurasi yang Anda lakukan sudah benar! Jika tidak, berarti ada yang tidak beres silakan cermati pada /var/log/proftpd/proftpd.log untuk melihat kesalahan yang perlu diperbaiki.
Setelah berhasil login maka secara otomatis akan terbentuk direktori baru pada /home/ftpuser

```
root@ns:/# ls -l /home/
total 16
drwxr-xr-x 2 anang anang   4096 May 24 20:34 anang
drwxr-xr-x 2 root  root    4096 Jul  2 20:49 data
drwxr-xr-x 2 ftp   nogroup 4096 Jul  6 08:40 ftp
drwx--x--x 4 root  root    4096 Jul  6 11:05 ftpuser

root@ns:/# ls -l /home/ftpuser
total 8
drwx------ 3 ftpuser ftpgroup 4096 Jul  6 10:23 anang
drwx------ 2 ftpuser ftpgroup 4096 Jul  6 11:05 yuan
```

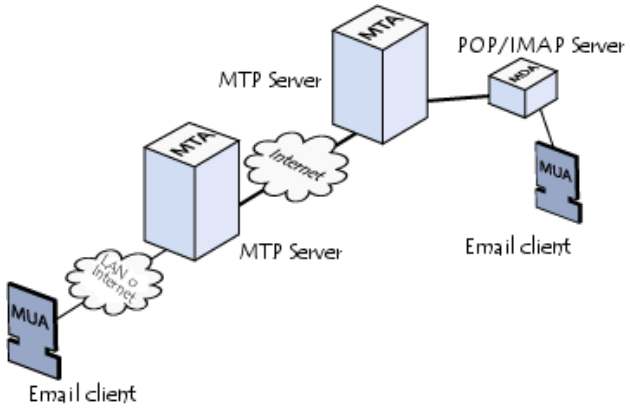
selengkapnya bagaimana cara menggunakan FTP server silakan membaca berbagai referensi yang sudah banyak di internet tentang penggunaan FTP.

E. MAIL SERVER DENGAN VIRTUAL USER

E.1. Pengantar

Tentu kita semua pernah menggunakan layanan yang disediakan oleh suatu web site seperti mail.yahoo.com atau gmail.com, bagi yang sudah pernah tentu tahu bahwa alamat tersebut memberikan akses email berbasis web. Bagaimana membuat layana semacam ini? Pada bagian ini dijelaskan cara menginstal mail server menggunakan Postfix yang didasarkan pada *virtual user* dan *domain*, yaitu pengguna dan domain yang berada dalam database MySQL.

Dalam membangun email server sebenarnya terdapat dua applikasi yang harus ada yaitu Mail Transfer Agent (MTA) atau software yang bertindak menangani email yang akan dikirim maupun yang diterima, MTA merupakan applikasi email pada sisi server dan Mail User Agent (MUA) atau software yang digunakan untuk mengambil email atau membaca email dari email server (MTA), MTA ini berada pada sisi client. Terdapat dua protokol utama yang digunakan untuk memberikan layanan email yaitu protokol untuk mengirim email SMTP dan protokol untuk mengambil atau membaca email yaitu POP atau bisa juga menggunakan IMAP. Sebagai ilustrasi bagaimana MTA dan MUA berperan, lihat gambar di bawah ini,



Pada bagian ini akan ditunjukkan juga instalasi dan konfigurasi *Courier* (Courier-POP3, Courier-IMAP), sehingga *Courier* dapat melakukan otentifikasi terhadap database MySQL yang sama seperti yang digunakan oleh Postfix.

Server Postfix yang terkonfigurasi mampu menangani SMTP-AUTH, TLS dan kuota (kuota tidak dibangun dalam Postfix secara default, saya akan menunjukkan bagaimana untuk patch Postfix Anda tepat). Password disimpan dalam bentuk terenkripsi dalam suatu database. Keuntungan konfigurasi user secara "virtual" adalah akan didapat performa yang jauh lebih baik dibandingkan pengaturan yang didasarkan pada user sistem. Selain itu lebih mudah untuk melakukan manajemen karena kita hanya berurusan dengan database MySQL ketika kita menambahkan pengguna baru, domain baru atau mengedit yang sudah ada.

E.2. Instalasi

Pada bagian ini kita asumsikan server memiliki IP address 192.168.2.2 dang dengan hostname mail.gaplek.gk. langkah pertama yang sangat penting adalah buat symbolik dari /bin/sh ke /bin/bash:

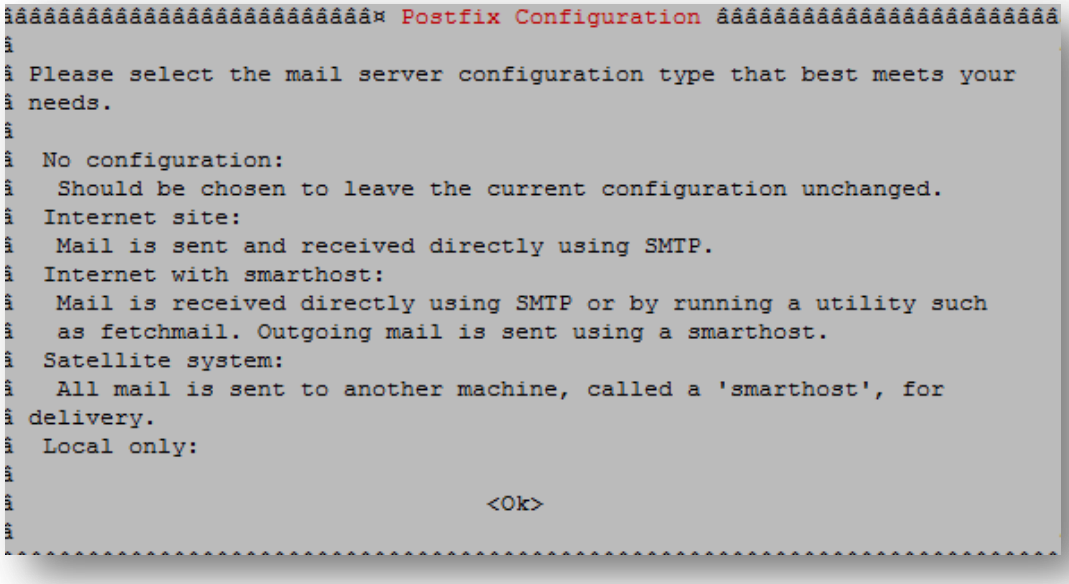
```
dpkg-reconfigure dash

Use dash as the default system shell (/bin/sh)? <-- No
```

Berikutnya install Postfix beserta dengan beberapa applikasi pendukungya

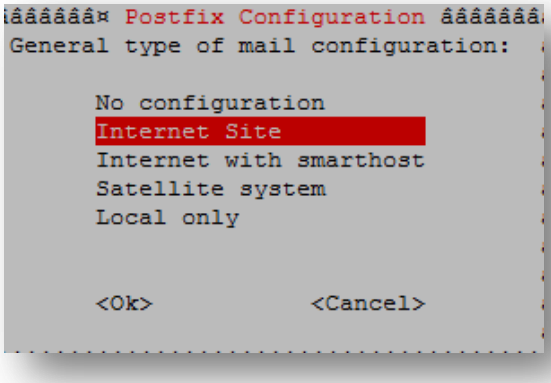
```
apt-get install postfix postfix-mysql postfix-doc mysql-client
mysql-server courier-authdaemon courier-authlib-mysql courier-pop
courier-pop-ssl courier-imap courier-imap-ssl libsasl2-2
libsasl2-modules libsasl2-modules-sql sasl2-bin libpam-mysql
openssl phpmyadmin apache2 libapache2-mod-php5 php5 php5-mysql
libpam-smbpass
```

Selama proses instalasi kita diharuskan menjawab beberapa pertanyaan yang berkaitan dengan applikasi yang diinstal, seperti berikut ini :

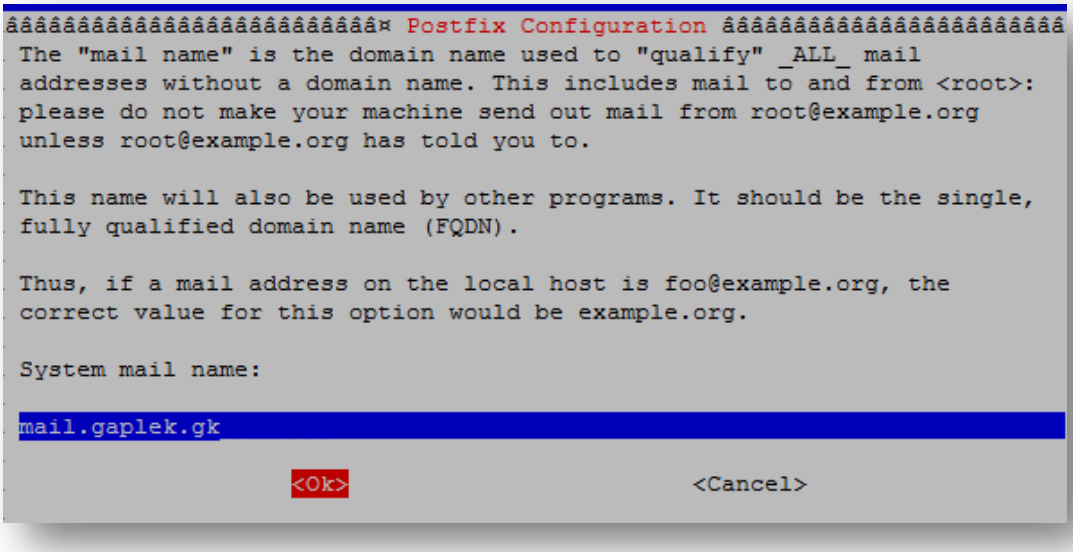
```
Posfix configuration  ---> <ok>
```



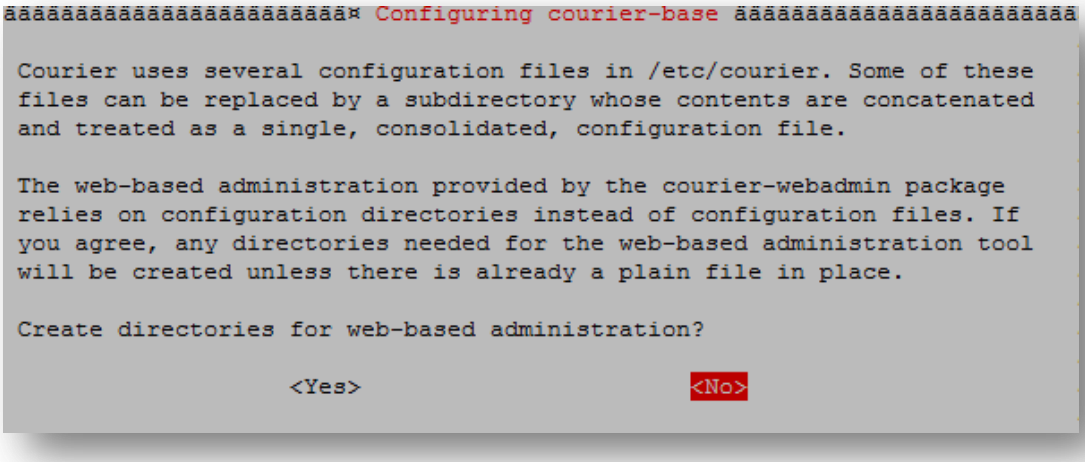
General type of mail configuration ---> Internet Site



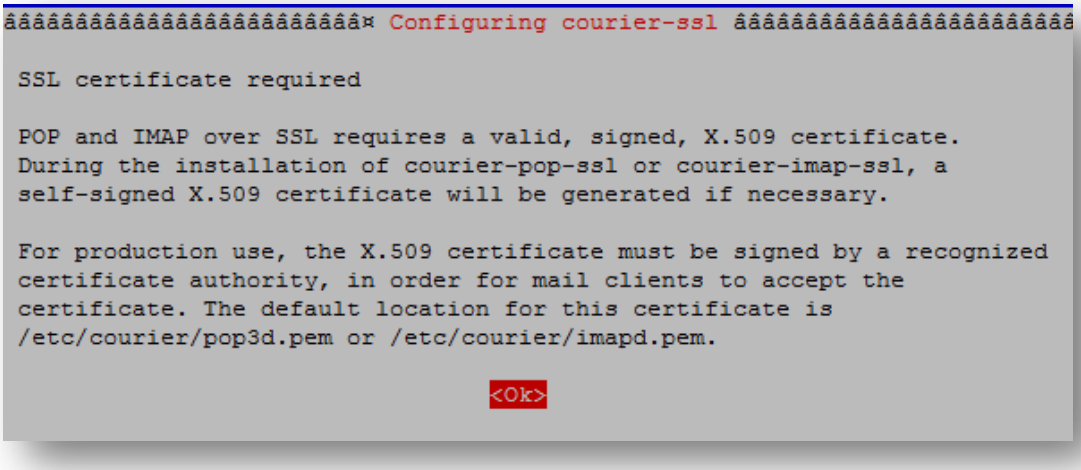
System mail name : ---> mail.gaplek.gk



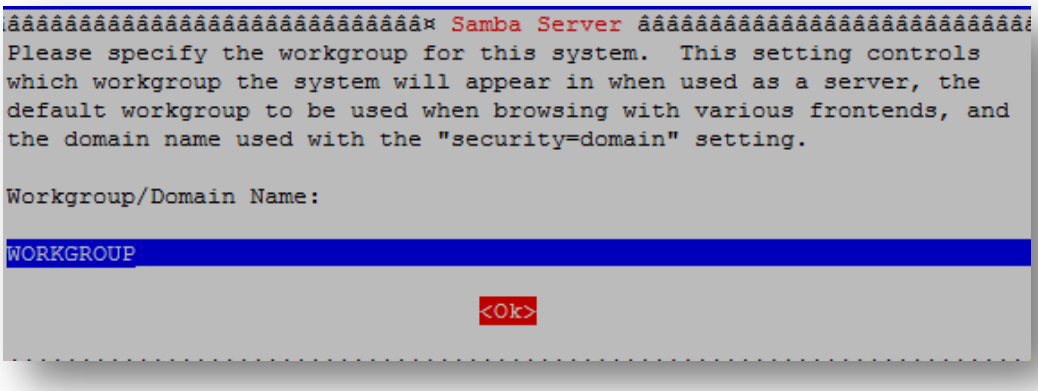
Create directories for web-based administration? --><No>



SSL certificate required ---> <Ok>




```
Workgroup/Domain Name : ---> WORKGROUP
```



Penambahan Fitur User Quota pada Postfix

Agar postfix yang terinstall nantinya memiliki fitur *user quota* kita harus mengambil source dari Postfix kemudian menambahkan *patch* untuk fitur *user quota* kemudian dicompile sebagai file .deb. selanjutnya file hasil yang sudah ada tambahan fitur baru tadi kita gunakan untuk menginstall kembali.

```
apt-get build-dep postfix
cd /usr/src
apt-get source postfix
```

Unduh file patch untuk user quota Postfix di `http://vda.sourceforge.net/VDA/`

```
cd /usr/src/

wget http://vda.sourceforge.net/VDA/postfix-vda-2.7.1.patch
```

```
cd postfix-2.7.1

patch -p1 < ../postfix-vda-2.7.1.patch
patching file README_FILES/VDA_README
patching file src/global/mail_params.h
patching file src/util/file_limit.c
patching file src/virtual/mailbox.c
patching file src/virtual/maildir.c
patching file src/virtual/virtual.c
patching file src/virtual/virtual.h

dpkg-buildpackage
```

Pada proses dpkg-buidpackage memerlukan waktu yang cukup lama, silakan tunggu beberapa saat dan perhatikan kalau ada pesan error. Setelah compile selesai masuk ke direktori /usr/src/

```
cd /usr/src
```

Seharusnya apabila proses compile berhasil akan ada beberapa file .deb

```
ls
root@ns:/usr/src# ls
postfix-2.7.1                          postfix-dev_2.7.1-1+squeeze1_all.deb
postfix_2.7.1-1+squeeze1.diff.gz       postfix-doc_2.7.1-1+squeeze1_all.deb
postfix_2.7.1-1+squeeze1.dsc           postfix-ldap_2.7.1-1+squeeze1_i386.deb
postfix_2.7.1-1+squeeze1_i386.changes  postfix-mysql_2.7.1-1+squeeze1_i386.deb
postfix_2.7.1-1+squeeze1_i386.deb      postfix-pcre_2.7.1-1+squeeze1_i386.deb
postfix_2.7.1.orig.tar.gz              postfix-pgsql_2.7.1-1+squeeze1_i386.deb
postfix-cdb_2.7.1-1+squeeze1_i386.deb  postfix-vda-2.7.1.patch
```

selanjutnya install postfix yang baru dan postfix yang support MySQL

```
dpgk –i postfix_2.7.1-1+squeeze1_i386.deb postfix-mysql_2.7.1-
1+squeeze1_i386.deb
```

E.3. Konfigurasi

Konfigurasi Database

Setelah Postfix dengan fitur user quota terpasang , selanjutnya kita menyiapkan database yang akan digunakan oleh Postfix untuk menampung segela informasi mengenai semua usernya.

```
mysql –u root –p
create database mail;
```

Dengan menggunakan shell MySQL kita buat pengguna “mail_admin” dengan password “mail_admin_password” yang memiliki priviliges SELECT, INSERT, UPDATE dan DELETE pada database “mail”. Pengguna ini nantinya akan digunakan oleh Postfix dan Courier untuk melakukan dapat terhubung ke dalam database “mail”.

```
GRANT SELECT, INSERT, UPDATE, DELETE ON mail.* TO
'mail_admin'@'localhost' IDENTIFIED BY 'mail_admin_password';

GRANT SELECT, INSERT, UPDATE, DELETE ON mail.* TO
'mail_admin'@'localhost.localdomain' IDENTIFIED BY
'mail_admin_password';

FLUSH PRIVILEGES;
```

Berikutnya membuat beberapa tabel dalam database “mail”

```
USE mail;

CREATE TABLE domains (
domain varchar(50) NOT NULL,
PRIMARY KEY (domain) )
TYPE=MyISAM;

CREATE TABLE forwardings (
source varchar(80) NOT NULL,
destination TEXT NOT NULL,
PRIMARY KEY (source) )
TYPE=MyISAM;

CREATE TABLE users (
email varchar(80) NOT NULL,
password varchar(20) NOT NULL,
quota INT(10) DEFAULT '10485760',
PRIMARY KEY (email)
) TYPE=MyISAM;

CREATE TABLE transport (
domain varchar(128) NOT NULL default '',
transport varchar(128) NOT NULL default '',
UNIQUE KEY domain (domain)
) TYPE=MyISAM;

quit;
```

Konfigurasi Postfix

Sekarang mengkonfigurasi Postfix agar dapat terhubung kedalam database yang baru kita buat di atas, untuk keperluan tersebut kita harus menyiapkan 6 file konfigurasi baru pada direktori /etc/postfix,

```
pico /etc/postfix/mysql-virtual_domains.cf
```

```
user = mail_admin
password = mail_admin_password
dbname = mail
query = SELECT domain AS virtual FROM domains WHERE domain='%s'
hosts = 127.0.0.1
```

```
pico /etc/postfix/mysql-virtual_forwardings.cf
```

```
user = mail_admin
```

```
password = mail_admin_password
dbname = mail
query = SELECT destination FROM forwardings WHERE source='%s'
hosts = 127.0.0.1
```

```
pico /etc/postfix/mysql-virtual_mailboxes.cf
```

```
user = mail_admin
password = mail_admin_password
dbname = mail
query = SELECT CONCAT(SUBSTRING_INDEX(email,'@',-
1),'/',SUBSTRING_INDEX(email,'@',1),'/') FROM users WHERE
email='%s'
hosts = 127.0.0.1
```

```
pico /etc/postfix/mysql-virtual_email2email.cf
```

```
user = mail_admin
password = mail_admin_password
dbname = mail
query = SELECT email FROM users WHERE email='%s'
hosts = 127.0.0.1
```

```
pico /etc/postfix/mysql-virtual_transports.cf
```

```
user = mail_admin
password = mail_admin_password
dbname = mail
query = SELECT transport FROM transport WHERE domain='%s'
hosts = 127.0.0.1
```

```
pico /etc/postfix/mysql-virtual_mailbox_limit_maps.cf
```

```
user = mail_admin
password = mail_admin_password
dbname = mail
query = SELECT quota FROM users WHERE email='%s'
hosts = 127.0.0.1
```

Kemudian ubah kepemilikan dari ke enam file tadi dalam groupnya postfix:

```
chmod o= /etc/postfix/mysql-virtual_*.cf
chgrp postfix /etc/postfix/mysql-virtual_*.cf
```

Sekarang kita buat pengguna dan group “vmail” yang memiliki direktori pada /home/vmail, dimana pada direktori ini semua email dari client akan ditampung. Anda tidak harus menggunakan nama “vmail” tetapi bisa juga dengan nama yang lain karena penamaan ini bukan hal baku.

```
groupadd -g 5000 vmail
useradd -g vmail -u 5000 vmail -d /home/vmail -m
```

selanjutnya kita aktifkan beberapa konfigurasi yang telah kita buat tadi,

```
postconf -e 'myhostname = mail.gaplek.gk'
postconf -e 'mydestination = mail.gaplek.gk, localhost,
localhost.localdomain'
postconf -e 'mynetworks = 127.0.0.0/8'
```

```
postconf -e 'virtual_alias_domains ='
postconf   -e   'virtual_alias_maps   =   proxy:mysql:/etc/postfix/mysql-
virtual_forwardings.cf, mysql:/etc/postfix/mysql-virtual_email2email.cf'
postconf  -e  'virtual_mailbox_domains  =  proxy:mysql:/etc/postfix/mysql-
virtual_domains.cf'
postconf   -e   'virtual_mailbox_maps   =   proxy:mysql:/etc/postfix/mysql-
virtual_mailboxes.cf'
postconf -e 'virtual_mailbox_base = /home/vmail'
postconf -e 'virtual_uid_maps = static:5000'
postconf -e 'virtual_gid_maps = static:5000'
postconf -e 'smtpd_sasl_auth_enable = yes'
postconf -e 'broken_sasl_auth_clients = yes'
postconf -e 'smtpd_sasl_authenticated_header = yes'
postconf    -e    'smtpd_recipient_restrictions    =    permit_mynetworks,
permit_sasl_authenticated, reject_unauth_destination'
postconf -e 'smtpd_use_tls = yes'
postconf -e 'smtpd_tls_cert_file = /etc/postfix/smtpd.cert'
postconf -e 'smtpd_tls_key_file = /etc/postfix/smtpd.key'
postconf    -e    'transport_maps    =    proxy:mysql:/etc/postfix/mysql-
virtual_transports.cf'
postconf -e 'virtual_create_maildirsize = yes'
postconf -e 'virtual_maildir_extended = yes'
postconf -e 'virtual_mailbox_limit_maps = proxy:mysql:/etc/postfix/mysql-
virtual_mailbox_limit_maps.cf'
postconf -e 'virtual_mailbox_limit_override = yes'
postconf -e 'virtual_maildir_limit_message = "The user you are trying to
reach is over quota."'
postconf -e 'virtual_overquota_bounce = yes'
postconf  -e  'proxy_read_maps  =  $local_recipient_maps  $mydestination
$virtual_alias_maps     $virtual_alias_domains     $virtual_mailbox_maps
$virtual_mailbox_domains       $relay_recipient_maps       $relay_domains
$canonical_maps     $sender_canonical_maps     $recipient_canonical_maps
$relocated_maps $transport_maps $mynetworks $virtual_mailbox_limit_maps'
```

setelah itu kita buat sertifikasi *Secure Socket Layer* (SSL) yang diperlukan untuk melakukan hubungan secara *Transport Layer Security* (TSL)

```
openssl req -new -outform PEM -out smtpd.cert -newkey rsa:2048 -
nodes -keyout smtpd.key -keyform PEM -days 365 -x509
```

```
Generating a 2048 bit RSA private key
..............+++
.........................................+++
writing new private key to 'smtpd.key'
-----
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]:62
State or Province Name (full name) [Some-State]:Indonesia
Locality Name (eg, city) []:jogja
Organization Name (eg, company) [Internet Widgits Pty Ltd]:SMKN 2 wonosari
Organizational Unit Name (eg, section) []:TKJ
Common Name (eg, YOUR name) []:anang supriyanta
Email Address []:anafis95@gmail.com
```

Kemudian ubah status permisi file /etc/postfix/smtpd.key

```
chmod o= /etc/postfix/smtpd.key
```

Konfigurasi Saslauthd

Sebelumnya buat terlebih dahulu direktori /var/spool/postfix/var/run/saslauthd

```
mkdir -p /var/spool/postfix/var/run/saslauthd
```

Kemudian ubah file /etc/default/saslauthd, pada bagian `START` ubah nilainya menjadi "`yes`" ubah juga pada baris `OPTIONS="-c -m /var/run/saslauthd"` menjadi `OPTIONS="-c -m /var/spool/postfix/var/run/saslauthd -r"`:

```
pico /etc/default/saslauthd
```

```
# Settings for saslauthd daemon
# Please read /usr/share/doc/sasl2-bin/README.Debian for details.
#

# Should saslauthd run automatically on startup? (default: no)
START=yes

# Description of this saslauthd instance. Recommended.
# (suggestion: SASL Authentication Daemon)
DESC="SASL Authentication Daemon"

#### dipotong #######

# WARNING: DO NOT SPECIFY THE -d OPTION.
# The -d option will cause saslauthd to run in the foreground
instead of as
# a daemon. This will PREVENT YOUR SYSTEM FROM BOOTING PROPERLY.
If you wish
# to run saslauthd in debug mode, please run it by hand to be
safe.
#
# See /usr/share/doc/sasl2-bin/README.Debian for Debian-specific
information.
# See the saslauthd man page and the output of 'saslauthd -h' for
general
# information about these options.
#
#Example for postfix users: "-c -m /var/spool/postfix/var/run/saslauthd"
#OPTIONS="-c -m /var/run/saslauthd"

OPTIONS="-c -m /var/spool/postfix/var/run/saslauthd -r"
```

Berikutnya buat file /etc/pam.d/smtp, file ini hanya terdiri dari dua baris yang berisi informasi mengenai username dan password untuk koneksi ke database.

```
pico /etc/pam.d/smtp
```

```
auth            required          pam_mysql.so    user=mail_admin
passwd=mail_admin_password   host=127.0.0.1   db=mail   table=users
usercolumn=email passwdcolumn=password crypt=1
account        sufficient        pam_mysql.so        user=mail_admin
passwd=mail_admin_password   host=127.0.0.1   db=mail   table=users
usercolumn=email passwdcolumn=password crypt=1
```

Selanjutnya kita buat lagi file /etc/postfix/sasl/smtpd.conf, yang isi dari file tersebut adalah sebagai berikut :

```
pico  /etc/postfix/sasl/smtpd.conf
```

```
pwcheck_method: saslauthd
mech_list: plain login
allow_plaintext: true
auxprop_plugin: mysql
sql_hostnames: 127.0.0.1
sql_user: mail_admin
sql_passwd: mail_admin_password
sql_database: mail
sql_select: select password from users where email = '%u'
```

Kemudian tambahkan user postfix sebagai group sasl hal ini dilakukan untuk memastikan agar Postfix memiliki akses ke saslauthd:

```
adduser postfix sasl
```

Selanjutnya restart kembali Postfix dan Saslauthd:

```
/etc/init.d/postfix restart
/etc/init.d/saslauthd restart
```

Configurasi Courier

Sekarang kita siapkan agar nantinya Courier dapat melakukan authentifikasi ke dalam database MySQL. Lakukan sedikit perubahan pada file /etc/courier/authdaemonrc ubah pada baris yang telah saya beri tanda:

```
pico  /etc/courier/authdaemonrc
```

```
#### dipotong ######

##NAME: authmodulelist:2
#
# The authentication modules that are linked into authdaemond.
The
# default list is installed.  You may selectively disable modules
simply
# by removing them from the following list.   The available
modules you
# can use are: authuserdb authpam authpgsql authldap authmysql
authcustom authpi
pe

authmodulelist="authmysql"

##NAME: authmodulelistorig:3
#

###### dipotong ########
```

Kemudian sebelum melangkah ke tahap selanjutnya silakan backup dulu file /etc/courier/authmysqlrc untuk berjaga-jaga kalau nanti kita harus mengembalikan ke konfigurasi awal. Setelah dibackup kosongkan file aslinya,

```
cp /etc/courier/authmysqlrc /etc/courier/authmysqlrc_orig
cat /dev/null > /etc/courier/authmysqlrc
```

Buka file /etc/courier/authmysqlrc kemudian tambahkan baris isian berikut,

```
pico /etc/courier/authmysqlrc
```

```
MYSQL_SERVER localhost
MYSQL_USERNAME mail_admin
MYSQL_PASSWORD mail_admin_password
MYSQL_PORT 0
MYSQL_DATABASE mail
MYSQL_USER_TABLE users
MYSQL_CRYPT_PWFIELD password
#MYSQL_CLEAR_PWFIELD password
MYSQL_UID_FIELD 5000
MYSQL_GID_FIELD 5000
MYSQL_LOGIN_FIELD email
MYSQL_HOME_FIELD "/home/vmail"
MYSQL_MAILDIR_FIELD CONCAT(SUBSTRING_INDEX(email,'@',-
1),'/',SUBSTRING_INDEX(email,'@',1),'/')
#MYSQL_NAME_FIELD
MYSQL_QUOTA_FIELD quota
```

Pada saat instalasi SSL certificate untuk IMAP-SSL dan POP3-SSL dibuat dengan hostname localhost. Untuk mengubah ke hostname yang benar, dalam hal ini saya menggunakan mail.gaplek.gk hapuslah sertifikat yang sudah ada.

```
cd /etc/courier
rm -f /etc/courier/imapd.pem
rm -f /etc/courier/pop3d.pem
```

selanjutnya ubah pada baris CN=localhost menjadi CN=mail.gaplek.gk atau dengan hostname lain sesuai dengan jaringan yang Anda miliki:

pico /etc/courier/imapd.cnf

```
RANDFILE = /usr/lib/courier/imapd.rand

[ req ]
default_bits = 1024
encrypt_key = yes
distinguished_name = req_dn
x509_extensions = cert_type
prompt = no

[ req_dn ]
C=US
ST=NY
L=New York
O=Courier Mail Server
OU=Automatically-generated IMAP SSL key
```

```
CN=mail.gaplek.gk
emailAddress=postmaster@gaplek.gk

[ cert_type ]
nsCertType = server
```

```
pico /etc/courier/pop3d.cnf
```

```
RANDFILE = /usr/lib/courier/pop3d.rand

[ req ]
default_bits = 1024
encrypt_key = yes
distinguished_name = req_dn
x509_extensions = cert_type
prompt = no

[ req_dn ]
C=US
ST=NY
L=New York
O=Courier Mail Server
OU=Automatically-generated POP3 SSL key
CN=mail.gaplek.gk
emailAddress=postmaster@gaplek.gk


[ cert_type ]
nsCertType = server
```

kemudian buat sertifikat ulang dan restart semua service dari courier

```
mkimapdcert
mkpop3dcert

/etc/init.d/courier-authdaemon restart
/etc/init.d/courier-imap restart
/etc/init.d/courier-imap-ssl restart
/etc/init.d/courier-pop restart
/etc/init.d/courier-pop-ssl restart
```

Untuk memastikan bahwa POP3 sudah berjalan dengan benar bisa dilihat dengan melakukan telnet melalui port POP3

```
telnet localhost pop3
```

Jika pada didapat pesan "`+OK Hello there`" berarti POP3 sudah berjalan dengan normal.

```
root@ns:/ # telnet localhost pop3
Trying 127.0.0.1...
Connected to localhost.localdomain.
Escape character is '^]'.
+OK Hello there.

quit
```

/etc/aliases

Pada file /etc/aliases kita harus memastikan bahwa postmaster mengarah ke root dan root ke username kita atau ke alamat email kita:

```
pico /etc/aliases
```

```
# /etc/aliases
mailer-daemon: postmaster
postmaster: root
nobody: root
hostmaster: root
usenet: root
news: root
webmaster: root
www: root
ftp: root
abuse: root
noc: root
security: root
root: administrator
```

Kemudian ketikan perintah berikut

```
newaliases
```

Setelah itu restart kembali Postfix:

```
/etc/init.d/postfix restart
```

Pemberitahuan Quota Penuh

Apabila kita ingin ada semacam pemberitahuan apabila pada suatu saat quota email yang dimiliki oleh pengguna hampir sudah penuh maka buat file /usr/local/sbin/quota_notify:

```
cd /usr/local/sbin/
vi quota_notify
```

```
#!/usr/bin/perl -w


use strict;

my $POSTFIX_CF = "/etc/postfix/main.cf";
my $MAILPROG = "/usr/sbin/sendmail -t";
my $WARNPERCENT = 80;
my @POSTMASTERS = ('postmaster@gaplek.gk');
my $CONAME = 'My Company';
my $COADDR = 'postmaster@gaplek.gk';
my $SUADDR = 'postmaster@gaplek.gk';
my $MAIL_REPORT = 1;
my $MAIL_WARNING = 1;

#get virtual mailbox base from postfix config
open(PCF, "< $POSTFIX_CF") or die $!;
my $mboxBase;
```

```
while (<PCF>) {
   next unless /virtual_mailbox_base\s*=\s*(.*)\s*/;
   $mboxBase = $1;
}
close(PCF);

#assume one level of subdirectories for domain names
my @domains;
opendir(DIR, $mboxBase) or die $!;
while (defined(my $name = readdir(DIR))) {
   next if $name =~ /^\.\.?$/;        #skip '.' and '..'
   next unless (-d "$mboxBase/$name");
   push(@domains, $name);
}
closedir(DIR);
#iterate through domains for username/maildirsize files
my @users;
chdir($mboxBase);
foreach my $domain (@domains) {
        opendir(DIR, $domain) or die $!;
        while (defined(my $name = readdir(DIR))) {
           next if $name =~ /^\.\.?$/;        #skip '.' and '..'
           next unless (-d "$domain/$name");
      push(@users, {"$name\@$domain" =>
"$mboxBase/$domain/$name"});
        }
}
closedir(DIR);

#get user quotas and percent used
my (%lusers, $report);
foreach my $href (@users) {
   foreach my $user (keys %$href) {
      my $quotafile = "$href->{$user}/maildirsize";
      next unless (-f $quotafile);
      open(QF, "< $quotafile") or die $!;
      my ($firstln, $quota, $used);
      while (<QF>) {
         my $line = $_;
              if (! $firstln) {
                 $firstln = 1;
                 die "Error: corrupt quotafile $quotafile"
                    unless ($line =~ /^(\d+)S/);
                 $quota = $1;
            last if (! $quota);
            next;
         }
         die "Error: corrupt quotafile $quotafile"
            unless ($line =~ /\s*(-?\d+)/);
         $used += $1;
      }
      close(QF);
      next if (! $used);
      my $percent = int($used / $quota * 100);
      $lusers{$user} = $percent unless not $percent;
   }
}
```

```
#send a report to the postmasters
if ($MAIL_REPORT) {
   open(MAIL, "| $MAILPROG");
   select(MAIL);
   map {print "To: $_\n"} @POSTMASTERS;
   print "From: $COADDR\n";
   print "Subject: Daily Quota Report.\n";
   print "DAILY QUOTA REPORT:\n\n";
   print "-----------------------------------------------\n";
   print "| % USAGE |            ACCOUNT NAME          |\n";
   print "-----------------------------------------------\n";
   foreach my $luser ( sort { $lusers{$b} <=> $lusers{$a} } keys
%lusers ) {
      printf("|   %3d   | %32s |\n", $lusers{$luser}, $luser);
      print "-----------------------------------------------\n";
   }
        print "\n--\n";
        print "$CONAME\n";
        close(MAIL);
}

#email a warning to people over quota
if ($MAIL_WARNING) {
        foreach my $luser (keys (%lusers)) {
           next unless $lusers{$luser} >= $WARNPERCENT;       #
skip those under quota
           open(MAIL, "| $MAILPROG");
           select(MAIL);
           print "To: $luser\n";
      map {print "BCC: $_\n"} @POSTMASTERS;
           print "From: $SUADDR\n";
           print "Subject: WARNING: Your mailbox is
$lusers{$luser}% full.\n";
           print "Reply-to: $SUADDR\n";
           print "Your mailbox: $luser is $lusers{$luser}%
full.\n\n";
           print "Once your e-mail box has exceeded your monthly
storage quota\n";
      print "your monthly billing will be automatically
adjusted.\n";
      print "Please consider deleting e-mail and emptying your
trash folder to clear some space.\n\n";
           print "Contact <$SUADDR> for further assistance.\n\n";
           print "Thank You.\n\n";
           print "--\n";
           print "$CONAME\n";
           close(MAIL);
        }
}
```

Kemudian kita harus memberi hak agar file tersebut dapat dijalankan :

```
chmod 755 quota_notify
```

Berikutnya buat dalam crontab

```
crontab –e
```

```
0 0 * * * /usr/local/sbin/quota_notify &> /dev/null
```

E.4. Pengujian

Untuk melakukan pengujian terhadap Postfix yang telah kita konfigurasi apakah sudah siap dengan SMTP-AUTH dan TLS, kita gunakan telnet ke port 25,

```
telnet localhost 25
```

Apabila setelah perintah ehlo localhost muncul "*250-STARTTLS*" dan "*250-AUTH LOGIN PLAIN*" berarti semua berjalan dengan baik.

```
root@ns:/etc# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mail.gaplek.gk ESMTP Postfix (Debian/GNU)
ehlo localhost
250-mail.gaplek.gk
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

Pengisian Database dan Tes

Masuk ke database mail melalui shell MySQL atau sebenarnya bisa juga menggunakan PHPMyAdmin ,

```
mysql -u root -p
use mail;
```

Pertama kita isi tabel *domains*, misal *domain* dengan *gaplek.gk* :

```
INSERT INTO `domains` (`domain`) VALUES ('gaplek.gk');
```

Kemudian kita tambahkan user dalam tabel users, sebagai contoh kita tambahkan pengguna "anang" dengan password "anang123" dan "yuan" dengan password "yuan123", masing-masing memiliki quota 10485760 bit atau 10 MB.

```
INSERT INTO `users` (`email`, `password`, `quota`) VALUES
('anang@gaplek.gk', ENCRYPT('anang123'), 10485760);

INSERT INTO `users` (`email`, `password`, `quota`) VALUES
('yuan@gaplek.gk', ENCRYPT('yuan123'), 10485760);
```

Perhatikan bahwa isian password pada kedua sintak SQL tersebut harus dalam bentuk terenkrepsi. Berikutnya apabila diinginkan mengisi dua tabel lainnya yaitu forwardings dan tranport, pengisiannya adalah sebagai berikut :

```
INSERT INTO `forwardings` (`source`, `destination`) VALUES
('info@gaplek.gk, 'sales@gaplek.gk');

INSERT INTO `transport` (`domain`, `transport`) VALUES
('gaplek.gk', 'smtp:mail.gaplek.gk);
```

Setelah tabel terisi ada baiknya kita me*reload* Postfix kemudian coba mengirim email atau membacanya. Untuk mengirim email kita bisa menggunakan telnet pada port 25 atau SMTP :

```
root@ns:/# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mail.gaplek.gk ESMTP Postfix (Debian/GNU)
mail from:anang@gaplek.gk
250 2.1.0 Ok
mail to:yuan@gaplek.gk
503 5.5.1 Error: nested MAIL command
rcpt to:yuan@gaplek.gk
250 2.1.5 Ok
data
354 End data with <CR><LF>.<CR><LF>
Ini adalah data tes email pertama
.
250 2.0.0 Ok: queued as 94EBE2E400
.
quit
Connection closed by foreign host.
```

Sedang untuk membaca atau mengambil email yang tadi sudah dikirim dapat menggunakan telnet pada port 110 atau POP3

```
root@ns:# telnet localhost pop3
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
+OK Hello there.
user yuan@gaplek.gk
+OK Password required.
pass yuan123
+OK logged in.
stat
+OK 2 845
retr 1
+OK 422 octets follow.
Return-Path: <anang@gaplek.gk>
X-Original-To: yuan@gaplek.gk
Delivered-To: yuan@gaplek.gk
Received: from localhost (localhost [127.0.0.1])
        by mail.gaplek.gk (Postfix) with SMTP id 94EBE2E400
        for <yuan@gaplek.gk>; Fri,  8 Jul 2011 00:11:44 +0700
(WIT)
```

```
Message-Id: <20110707171333.94EBE2E400@mail.gaplek.gk>
Date: Fri,  8 Jul 2011 00:11:44 +0700 (WIT)
From: anang@gaplek.gk
To: undisclosed-recipients:;

Ini adalah data tes email pertama
.
quit
+OK Bye-bye.
Connection closed by foreign host.
root@ns:/etc/courier#
```

Web Mail dengan SquirrelMail

SquirrelMail merupakan salah satu applikasi yang bisa digunakan untuk membaca email berbasis web atau webmail. Dengan webmail maka penggunan email dapat mengirim maupun membaca email menggunakan browser. Karena berbasis web maka webmail dapat dibuka pada semua sistem operasi. Untuk instalasi Squirrelmail lakukan perintah berikut:

```
apt-get install squirrelmail squirrelmail-compatibility php-pear
php-db
```

Kemudian salin konfigurasi Apache yang telah ada dalam squirrelmail ke direktori /etc/apache2/conf.d, selanjutnya restart Apache:

```
cp /etc/squirrelmail/apache.conf
/etc/apache2/conf.d/squirrelmail.conf
/etc/init.d/apache2 restart
```

Squirremail memiliki beberapa plugins yang dapat kita install namun tidak ada plugin yang dapat digunakan oleh pengguna untuk mengubah password yang tersimpan dalam database MySQL database. Tetapi kita masih dapat menginstall secara manual dengan cara sebagai berikut :

```
cd /usr/share/squirrelmail/plugins

wget http://www.squirrelmail.org/plugins/change_sqlpass-3.3-
1.2.tar.gz
tar xvfz change_sqlpass-3.3-1.2.tar.gz
cd change_sqlpass
cp config.php.sample config.php
```

Kita harus mengedit file config.php untuk disesuikan dengan konfigurasi mail server kita. File config.php memiliki baris yang sangat banyak, namun kita tidak harus mencermati tiap barisnya cukup Anda sesuaikan saja dengan baris-baris yang perlu diubah seperti di bawah ini:

```
pico config.php
```

```
####dipotong####

$csp_dsn = 'mysql://mail_admin:mail_admin_password@localhost/mail';

####dipotong####

$lookup_password_query = 'SELECT count(*) FROM users WHERE email = "%1"
AND password = %4';
```

```
####dipotong####

$password_update_queries = array('UPDATE users SET password = %4 WHERE
email = "%1"');

####dipotong####

$password_encryption = 'MYSQLENCRYPT';

####dipotong####

$csp_salt_static = 'LEFT(password, 2)';

####dipotong####

//$csp_salt_query = 'SELECT salt FROM users WHERE username = "%1"';

####dipotong####

$csp_delimiter = '@';

####dipotong####
```

Langkah selanjutnya adalah mengkofigurasi squirrelmail menggunakan squirrel-configure :

/usr/sbin/squirrelmail-configure

```
SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Main Menu --
1.  Organization Preferences
2.  Server Settings
3.  Folder Defaults
4.  General Options
5.  Themes
6.  Address Books
7.  Message of the Day (MOTD)
8.  Plugins
9.  Database
10. Languages

D.  Set pre-defined settings for specific IMAP servers

C   Turn color on
S   Save data
Q   Quit

Command >> <-- D


SquirrelMail Configuration : Read: config.php
---------------------------------------------------------
Please select your IMAP server:
    bincimap    = Binc IMAP server
```

```
    courier      = Courier IMAP server
    cyrus        = Cyrus IMAP server
    dovecot      = Dovecot Secure IMAP server
    exchange     = Microsoft Exchange IMAP server
    hmailserver  = hMailServer
    macosx       = Mac OS X Mailserver
    mercury32    = Mercury/32
    uw           = University of Washington's IMAP server
    gmail        = IMAP access to Google mail (Gmail) accounts

    quit         = Do not change anything

Command >> <-- courier


              imap_server_type = courier
         default_folder_prefix = INBOX.
                  trash_folder = Trash
                   sent_folder = Sent
                  draft_folder = Drafts
            show_prefix_option = false
          default_sub_of_inbox = false
show_contain_subfolders_option = false
            optional_delimiter = .
                 delete_folder = true

Press any key to continue... <-- press some key


SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Main Menu --
1.  Organization Preferences
2.  Server Settings
3.  Folder Defaults
4.  General Options
5.  Themes
6.  Address Books
7.  Message of the Day (MOTD)
8.  Plugins
9.  Database
10. Languages

D.  Set pre-defined settings for specific IMAP servers

C   Turn color on
S   Save data
Q   Quit

Command >> <-- 8


SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Plugins
  Installed Plugins
    1. view_as_html
```

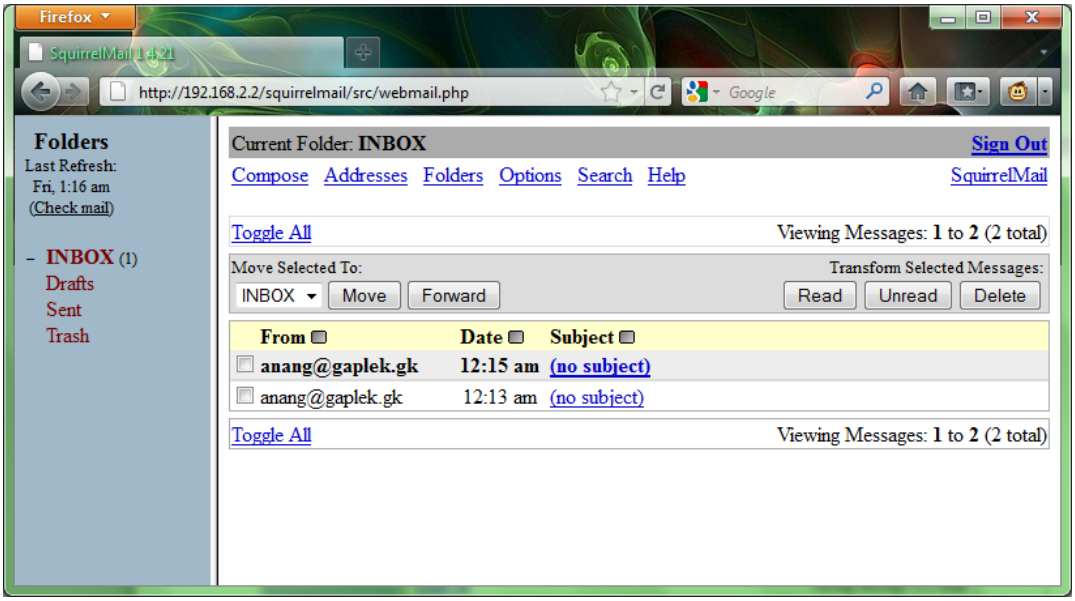
```
  Available Plugins:
    2. administrator
    3. bug_report
    4. calendar
    5. change_sqlpass
    6. compatibility
    7. delete_move_next
    8. demo
    9. filters
    10. fortune
    11. info
    12. listcommands
    13. mail_fetch
    14. message_details
    15. newmail
    16. sent_subfolders
    17. spamcop
    18. squirrelspell
    19. test
    20. translate

R   Return to Main Menu
C   Turn color on
S   Save data
Q   Quit

Command >> <-- 6 (atau angka yang menunjukkan pilihan
"compatibility" karena ini diperlukan untuk plugin
"change_sqlpass")


SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Plugins
  Installed Plugins
    1. view_as_html
    2. compatibility

  Available Plugins:
    3. administrator
    4. bug_report
    5. calendar
    6. change_sqlpass
    7. delete_move_next
    8. demo
    9. filters
    10. fortune
    11. info
    12. listcommands
    13. mail_fetch
    14. message_details
    15. newmail
    16. sent_subfolders
    17. spamcop
    18. squirrelspell
    19. test
    20. translate

R   Return to Main Menu
```

```
C   Turn color on
S   Save data
Q   Quit

Command >> <-- 6 (nomor dari change_sqlpass plugin)


SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Plugins
  Installed Plugins
    1. view_as_html
    2. compatibility
    3. change_sqlpass

  Available Plugins:
    4. administrator
    5. bug_report
    6. calendar
    7. delete_move_next
    8. demo
    9. filters
    10. fortune
    11. info
    12. listcommands
    13. mail_fetch
    14. message_details
    15. newmail
    16. sent_subfolders
    17. spamcop
    18. squirrelspell
    19. test
    20. translate

R   Return to Main Menu
C   Turn color on
S   Save data
Q   Quit

Command >> <-- S


SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Plugins
  Installed Plugins
    1. view_as_html
    2. compatibility
    3. change_sqlpass

  Available Plugins:
    4. administrator
    5. bug_report
    6. calendar
    7. delete_move_next
    8. demo
    9. filters
    10. fortune
```

```
    11. info
    12. listcommands
    13. mail_fetch
    14. message_details
    15. newmail
    16. sent_subfolders
    17. spamcop
    18. squirrelspell
    19. test
    20. translate

R   Return to Main Menu
C   Turn color on
S   Save data
Q   Quit

Command >> S

Data saved in config.php
Press enter to continue... <-- press ENTER


SquirrelMail Configuration : Read: config.php (1.4.0)
---------------------------------------------------------
Plugins
  Installed Plugins
    1. view_as_html
    2. compatibility
    3. change_sqlpass

  Available Plugins:
    4. administrator
    5. bug_report
    6. calendar
    7. delete_move_next
    8. demo
    9. filters
    10. fortune
    11. info
    12. listcommands
    13. mail_fetch
    14. message_details
    15. newmail
    16. sent_subfolders
    17. spamcop
    18. squirrelspell
    19. test
    20. translate

R   Return to Main Menu
C   Turn color on
S   Save data
Q   Quit

Command >> <-- Q
```

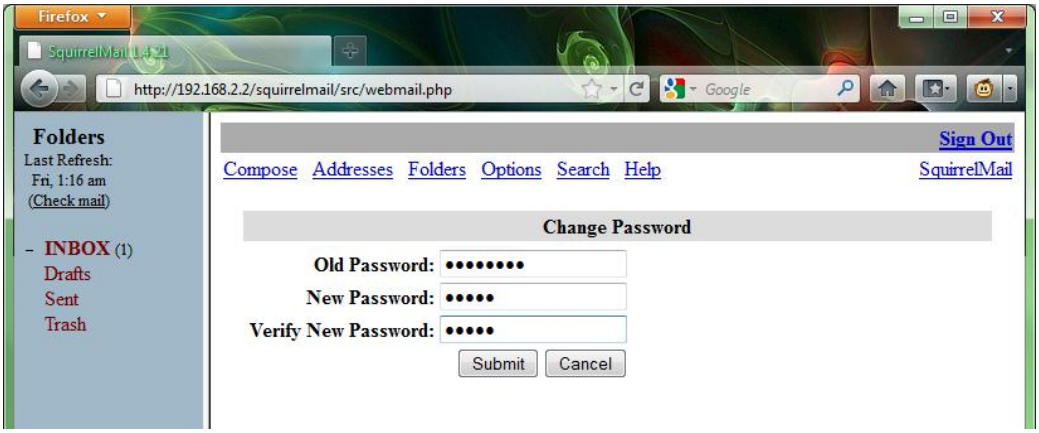
Sekarang kita coba menggunakan webmail dari squirrelmail yang baru kita konfigurasi dengan cara membuka alamt dari mail server tersebut http://mail.gaplek.gk atau

http://192.168.2.2/squirrelmail. Pada contoh ini saya menggunakan pengguna yuan@gaplek.gk dengan password yuan123:



Untuk mengubah password klik ***Options*** kemudian klik ***Change Password:***

Ketikan password lama kemudian isikan password baru dua kali :



Jika password berhasil diubah maka akan didapatkan pesan error yang artinya Anda harus login lagi dengan password yang baru.

F. SQUID (Cache Server)

F.1. Pengantar

Squid adalah sebuah daemon yang digunakan sebagai *proxy server* dan *web cache*. Squid memiliki banyak jenis penggunaan, mulai dari mempercepat server web dengan melakukan*caching* permintaan yang berulang-ulang, *caching* DNS, caching situs web, dan caching pencarian komputer di dalam jaringan untuk sekelompok komputer yang menggunakan sumber daya jaringan yang sama, hingga pada membantu keamanan dengan cara melakukan penyaringan (*filter*) lalu lintas. Meskipun seringnya digunakan untuk protokol HTTP dan FTP, Squid juga menawarkan dukungan terbatas untuk beberapa protokol lainnya termasuk *Transport Layer Security* (TLS), Secure Socket Layer (SSL), Internet Gopher, dan HTTPS. Versi Squid 3.1 mencakup dukungan protokol IPv6 dan Internet Content Adaptation Protocol (ICAP).

Caching merupakan sebuah cara untuk menyimpan objek-objek Internet yang diminta (seperti halnya data halaman web) yang bisa diakses melalui HTTP, FTP dan Gopher di dalam sebuah sistem yang lebih dekat dengan situs yang memintanya. Beberapa penjelajah web dapat menggunakan cache Squid lokal untuk sebagai server proxy HTTP, sehingga dapat mengurangi waktu akses dan juga tentu saja konsumsi bandwidth. Hal ini sering berguna bagi para penyedia layanan Internet untuk meningkatkan kecepatan kepada para pelanggannya, dan LAN yang membagi saluran Internet. Karena memang bentuknya sebagai proxy (ia berlaku sebagaimana layaknya klien, sesuai dengan permintaan klien), web cache bisa menyediakan anonimitas dan keamanan. Tapi, web cache juga bisa menjadi masalah yang signifikan bila melihat masalah privasi, karena memang ia dapat mencatat banyak data, termasuk URL yang diminta oleh klien, kapan hal itu terjadi, nama dan versi penjelajah web yang digunakan klien serta sistem operasinya, dan dari mana ia mengakses situs itu.

Selanjutnya, sebuah program klien (sebagai contoh adalah penjelajah web) bisa menentukan secara ekplisit proxy server yang digunakan bila memang hendak menggunakan proxy (umumnya bagi para pelanggan ISP) atau bisa juga menggunakan proxy tanpa konfigurasi ekstra, yang sering disebut sebagai "Transparent Caching", di mana semua permintaan HTTP ke jaringan luar akan diolah oleh proxy server dan semua respons disimpan di dalam cache. Kasus kedua umumnya dilakukan di dalam perusahaan dan korporasi (semua klien berada di dalam LAN yang sama) dan sering memiliki masalah privasi yang disebutkan di atas.

Squid memiliki banyak fitur yang bisa membantu melakukan koneksi secara anonim, seperti memodifikasi atau mematikan beberapa field header tertentu dalam sebuah permintaan HTTP yang diajukan oleh klien. Saat itu terpenuhi, apa yang akan dilakukan oleh Squid adalah tergantung orang yang menangani komputer yang menjalankan Squid. Orang yang meminta halaman web melalui sebuah jaringan yang secara transparan yang menggunakan biasanya tidak mengetahui bahwa informasi semua permintaan HTTP yang mereka ajukan dicatat oleh Squid.

Pada tutorial ini kita akan menggunakan SQUID dalam mode manual proxy karena semua pengguna diharuskan melakukan proses authenfikasi. Pada mode ini berarti pada sisi web browser harus disetting secara manual alamat dan prot proxy yang digunakan. Semua user nantinya kita tampung dalam suatu data base MySQL dan squid melakukan mengecekan pengguna ke dalam database melalui PHP. Memang pada squid telah disediakan library untuk

bisa berkomunikasi dengan data base yaitu squid_db_auth yang berada di /usr/lib/squid3/ namun kali ini kita akan membuat cara tersendiri yaitu dengan PHP.

F.2. Instalasi

Untuk instalasi kita membutuhkan beberapa software yaitu apache2, PHP, MySQL dan tentu saja Squid. Namun karena PHP, Apache2 dan MySQL telah kita install, pada langkah ini cukup kita install Squid3,

```
apt-get install squid3
```

F.3. Konfigurasi

Sebelum kita melakukan perubahan pada file /etc/squid3/squid.conf kita buat dahulu script PHP yang nantinya digunakan untuk berkomunikasi dengan database MySQl. Pada intinya keluaran dari script PHP ini adalah “OK” atau “ERR” , dua macam keluaran ini yang akan digunakan oleh squid apakah user tersebut valid atau tidak. Sehingga sebenarnya kita bisa menggunakan program apasaja yang penting keluaran dari proses login nanti adalah “OK” atau “ERR”.

Konfigurasi Database

Karena pengguna kita tampung dalam suatu database maka kita buat terlebih dahulu database dengan nama “proxyuser”

```
#mysql –u root –p

CREATE DATABASE proxyuser;

CREATE TABLE `proxyuser`.`pengguna` (
`id` INT(3) NOT NULL ,
`nama` VARCHAR(10) NOT NULL ,
`password` VARCHAR(32) NOT NULL ,
`keterangan` VARCHAR(50) NOT NULL
) ENGINE = MYISAM ;

ALTER TABLE `pengguna` ADD PRIMARY KEY (`id`);

ALTER TABLE `pengguna` CHANGE `id` `id` INT(3) NOT NULL
AUTO_INCREMENT;
```

Dari tabel yang dibuat diatas akan memiliki struktur sebagai berikut,

```
DESC pengguna;
+------------+-------------+------+-----+---------+----------------+
| Field      | Type        | Null | Key | Default | Extra          |
+------------+-------------+------+-----+---------+----------------+
| id         | int(3)      | NO   | PRI | NULL    | auto_increment |
| nama       | varchar(10) | NO   |     | NULL    |                |
| password   | varchar(32) | NO   |     | NULL    |                |
| keterangan | varchar(50) | NO   |     | NULL    |                |
+------------+-------------+------+-----+---------+----------------+
4 rows in set (0.00 sec)
```

Berikutnya kita isi tabel “pengguna” sesuai dengan pengguna yang akan kita daftarkan,

```
INSERT INTO pengguna (nama,password, keterangan)VALUES ("anang",
MD5("rahasia"), "siswa");
INSERT INTO pengguna (nama, password, keterangan) values ("yuan",
MD5("pacitan"),"guru");

SELECT * from pengguna;
+----+-------+----------------------------------+------------+
| id | nama  | password                         | keterangan |
+----+-------+----------------------------------+------------+
|  1 | anang | ac43724f16e9241d990427ab7c8f4228 | siswa      |
|  2 | yuan  | 8868ae22f25116137b529874015f8170 | guru       |
+----+-------+----------------------------------+------------+
1 row in set (0.00 sec)
```

File authenfikasi dengan PHP

Sekarang kita buat script /etc/squid3/userauth.php, nama file dan letaknya sebenarnya terserah kita.

```
pico /etc/squid3/userauth.php
```

```
<?
mysql_connect("localhost","root","pklm");
if (! defined(STDIN)) {
        define("STDIN", fopen("php://stdin", "r"));
}
while (!feof(STDIN)) {
  $line = trim(fgets(STDIN));
  $fields = explode(' ', $line);
  $username = rawurldecode($fields[0]); //1738
  $password = md5(rawurldecode($fields[1])); //1738
  $db=mysql("proxyuser","select * from pengguna where
nama='$username' and password='$password'");
        if(mysql_num_rows($db)>0){
                fwrite(STDOUT, "OK\n");
        } else {
                // failed miserably
                fwrite(STDOUT, "ERR\n");
        }
}
?>
```

Konfigurasi Squid

Untuk melakukan penyesuaian pada squid kita dapat melakukan sedikit perubahan pada file /etc/squid3/squid.conf. Pada file ini banyak sekali opsi-opsi yang dapat kita lakukan mulai dari membatasan bandwitdh, membatasan waktu access, membatasan besar cache dan memory dan masih banyak lagi. Karena begitu banyaknya fitur yang bisa dikonfigurasi pada squid maka pada bahasan ini kita batasi hanya pada konfigurasi untuk authenfikasi user menggunakan database dan PHP. Karena file /etc/squid3/squid.conf ini sangat panjang maka tampilan isi di bawah ini dari baris-baris yang perlu dikonfigurasi terutama yang dicetak tebal. Selain yang dicetak tebal, semua baris dalan squid.conf masih default atau tidak perlu diubah.

```
pico /etc/squid3/squid.conf
```

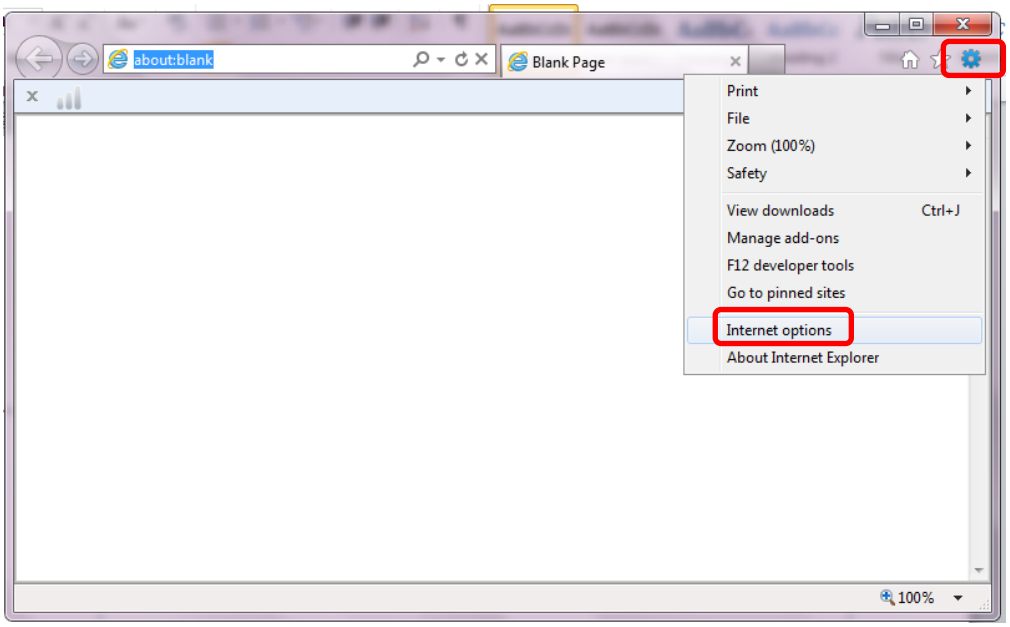
```
################################
auth_param basic program /usr/bin/php5 /etc/squid3/userauth.php
auth_param basic realm Squid proxy-caching web server
auth_param basic children 5
auth_param basic credentialsttl 2 hours
################################

acl manager proto cache_object
acl localhost src 127.0.0.1/32 ::1
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32 ::1

################################
acl passuser proxy_auth REQUIRED
################################

acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

http_access allow manager localhost
http_access deny manager
http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports


#############################
http_access allow passuser
#############################
http_access allow localhost
http_access deny all
http_port 3128
hierarchy_stoplist cgi-bin ?
```

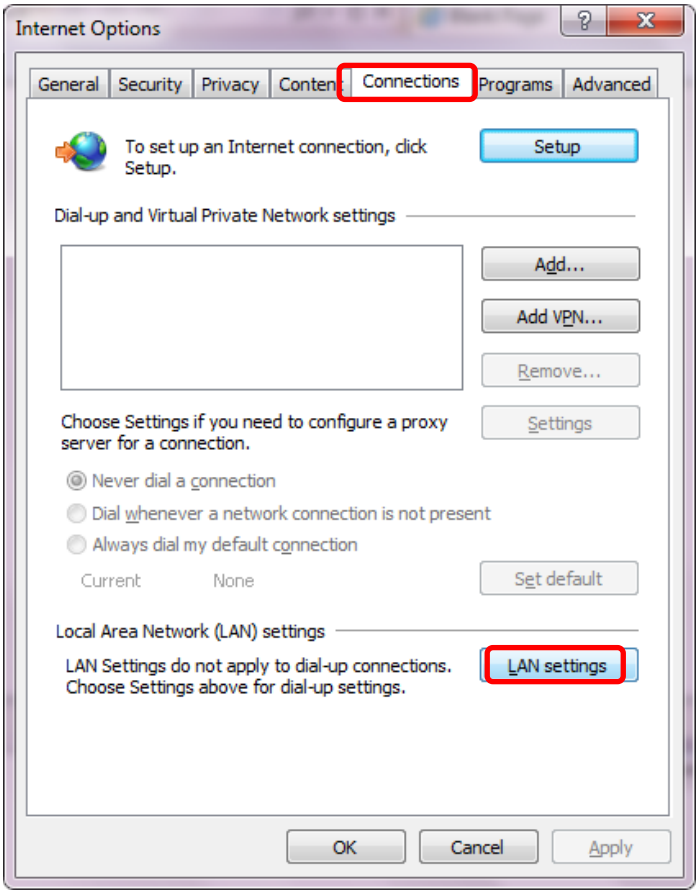
Berikutnya restart squid agar me-load konfigurasi yang baru

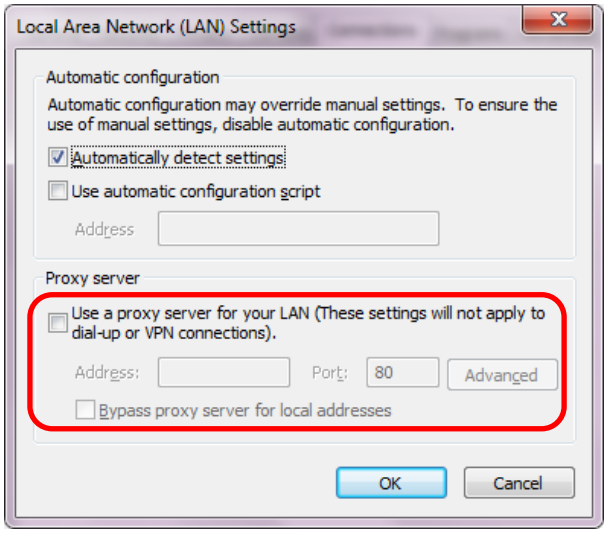
```
/etc/init.d/squid3 restart
```

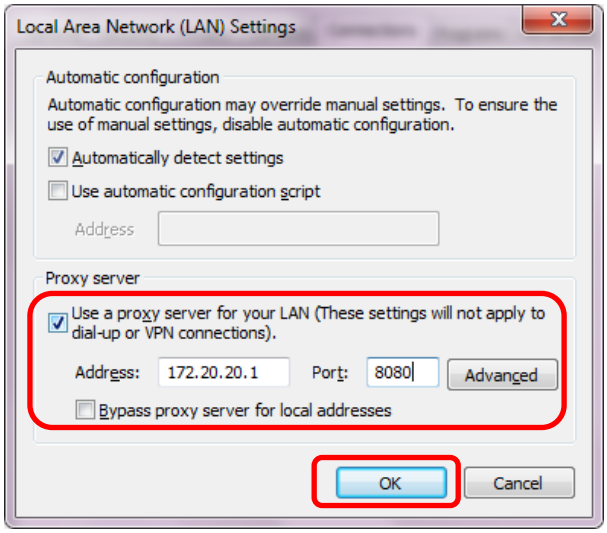
F.4. Pengujian

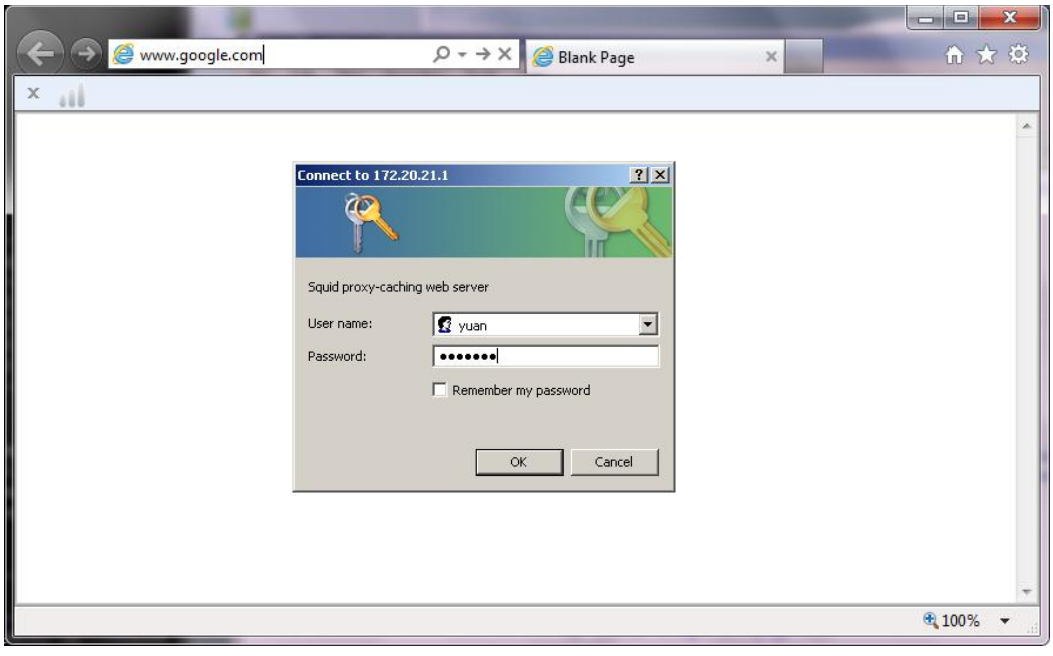
Karena squid kita konfigurasi dengan mode authenfikasi maka harus kita setting secara manual IP address dan port proxy agar dapat menggunakan layanan proxy yang kita bangun tersebut. Dalam contoh ini saya gunakan browser Internet Explorer, untuk browser-browser yang tidak begitu berbeda.

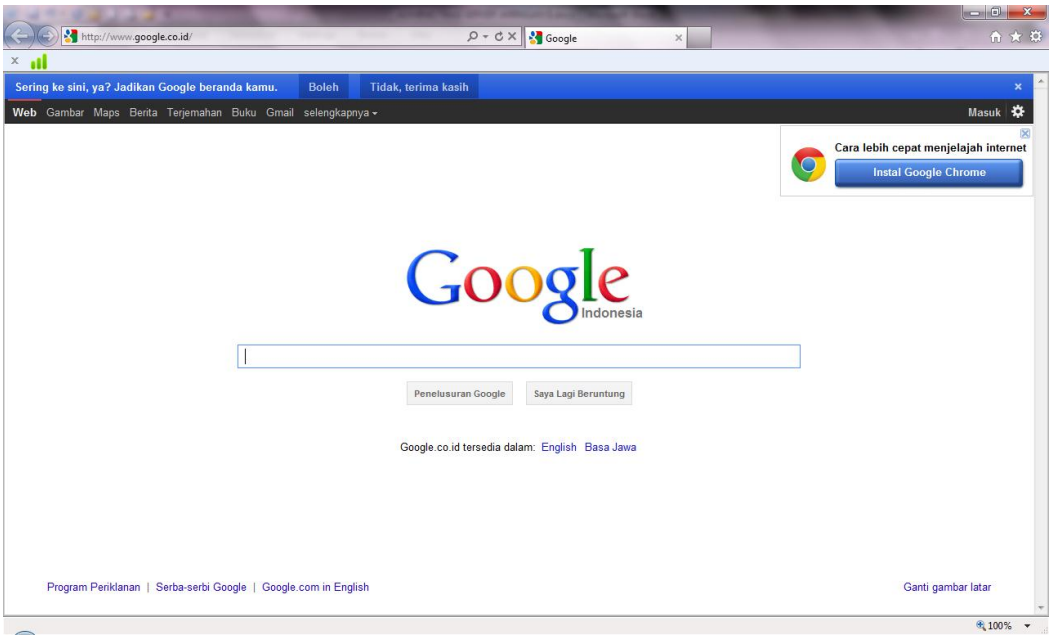

about:blank
Blank Page
Print
File
Zoom (100%)
Safety
View downloads Ctrl+J
Manage add-ons
F12 developer tools
Go to pinned sites
Internet options
About Internet Explorer
100%


Internet Options
General
Security
Privacy
Content
Connections
Programs
Advanced
To set up an Internet connection, click Setup.
Setup
Dial-up and Virtual Private Network settings
Add...
Add VPN...
Remove...
Choose Settings if you need to configure a proxy server for a connection.
Settings
Never dial a connection
Dial whenever a network connection is not present
Always dial my default connection
Current
None
Set default
Local Area Network (LAN) settings
LAN Settings do not apply to dial-up connections.
Choose Settings above for dial-up settings.
LAN settings
OK
Cancel
Apply


Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address:
Port:
80
Advanced
Bypass proxy server for local addresses
OK
Cancel


Local Area Network (LAN) Settings
Automatic configuration
Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.
Automatically detect settings
Use automatic configuration script
Address
Proxy server
Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).
Address:
172.20.20.1
Port:
8080
Advanced
Bypass proxy server for local addresses
OK
Cancel


www.google.com
Blank Page
Connect to 172.20.21.1
Squid proxy-caching web server
User name:
yuan
Password:
Remember my password
OK
Cancel
100%


http://www.google.co.id/
Google
Sering ke sini, ya? Jadikan Google beranda kamu.
Boleh
Tidak, terima kasih
Web Gambar Maps Berita Terjemahan Buku Gmail selengkapnya
Masuk
Cara lebih cepat menjelajah internet
Instal Google Chrome
Google
Indonesia
Penelusuran Google
Saya Lagi Beruntung
Google.co.id tersedia dalam: English Basa Jawa
Program Periklanan | Serba-serbi Google | Google.com in English
Ganti gambar latar
100%

DAFTAR PUSTAKA