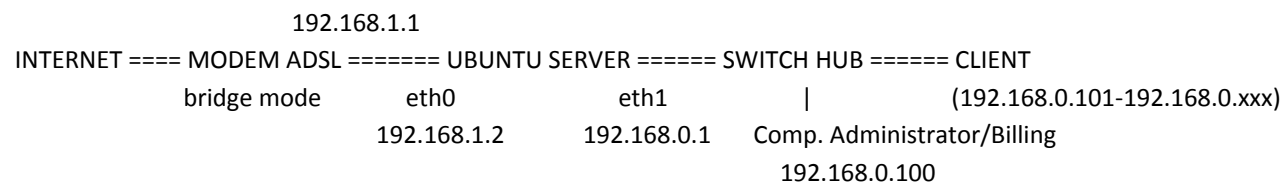


## PERSAMAAN PERFEKTI

Agar disini kita tidak salah mengasumsikan antara penulis dengan pembaca, maka sebelumnya kita samakan dahulu terutama untuk diagram jaringannya, diagramnya sebagai berikut:



Untuk MODEM ADSL dijadikan bridge yang nantinya akan di dial-up oleh ubuntu.

Disini spesifikasi minimum yang dipakai adalah Processor yang support 64 bit seperti:

- minimum Pentium 4 630/631/632 series (3GHz, FSB 800MHz, L2 2MB)
- atau Pentium D (2.4-3GHz, FSB 533-800MHz, L2 4MB)
- dan atau Dual Core, Core2Duo, Core2Quad, etc

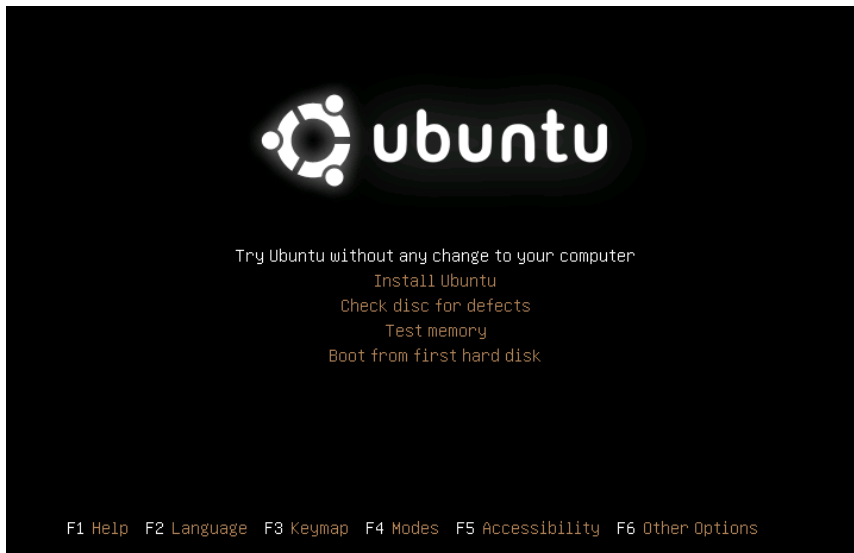
Hardware lainnya: RAM DDR1/2 1GB, 2 Ethernet Card, dan Harddisk 120GB SATA (Usahakan SATA agar responsif).

Tutorial ini diperuntukkan untuk Warnet dan RT/RW Net.

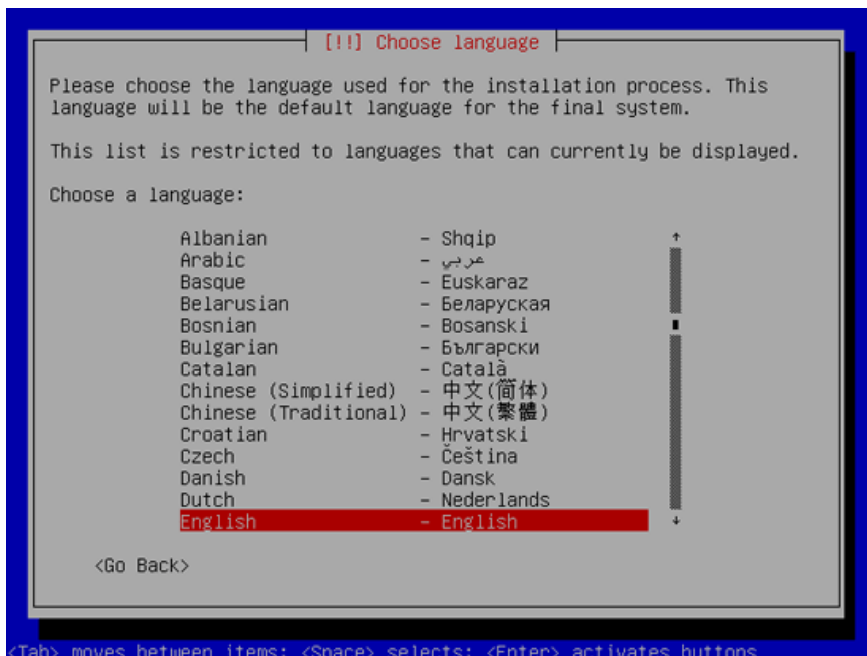
## TAHAP I

### INSTALL UBUNTU SERVER

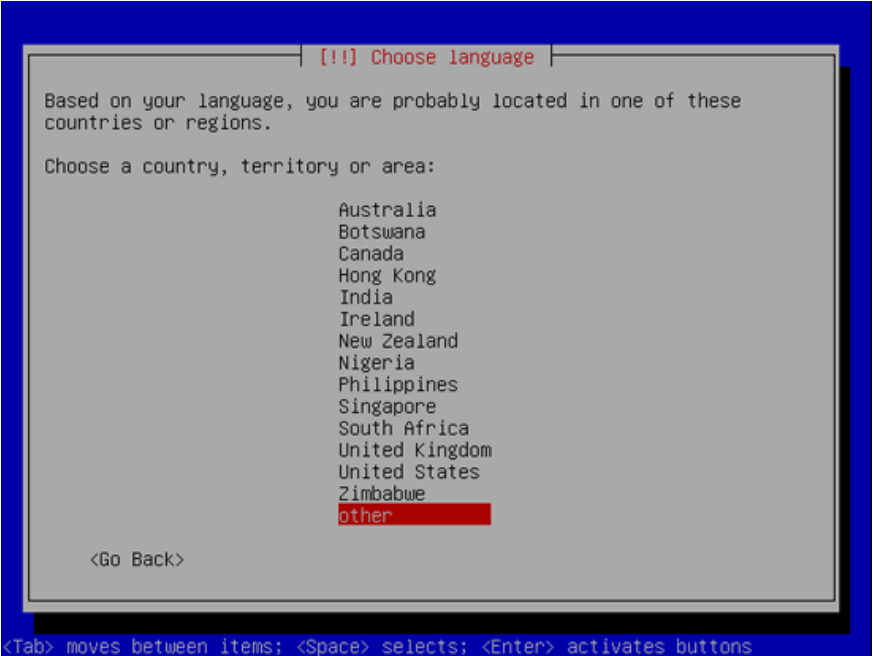
- Masukkan CD *Install Ubuntu 10.04 Server LTS 64bit* dan booting computer ke cd-rom
- Tampil awal dan pilih...



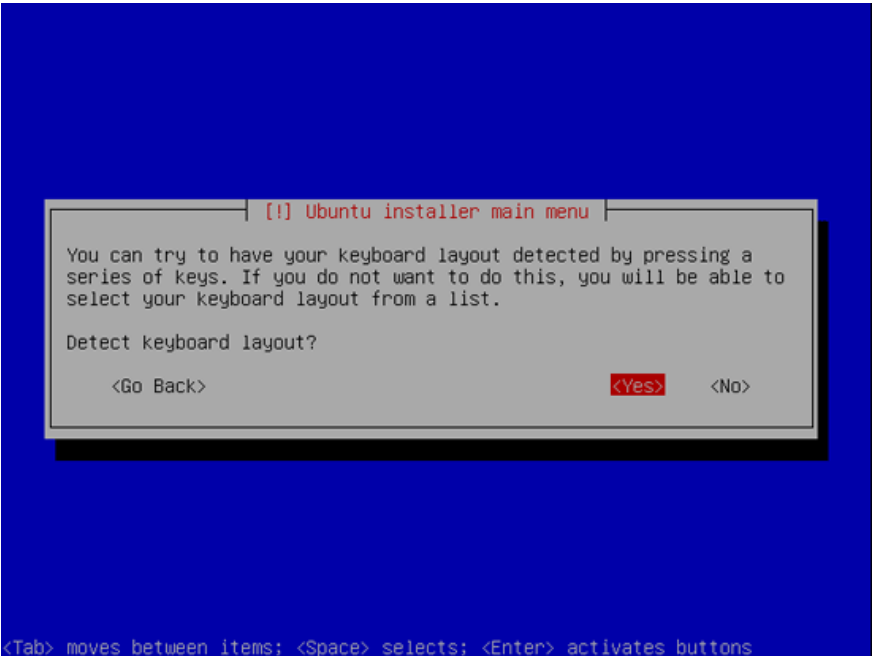
- Pilih Bahasa...



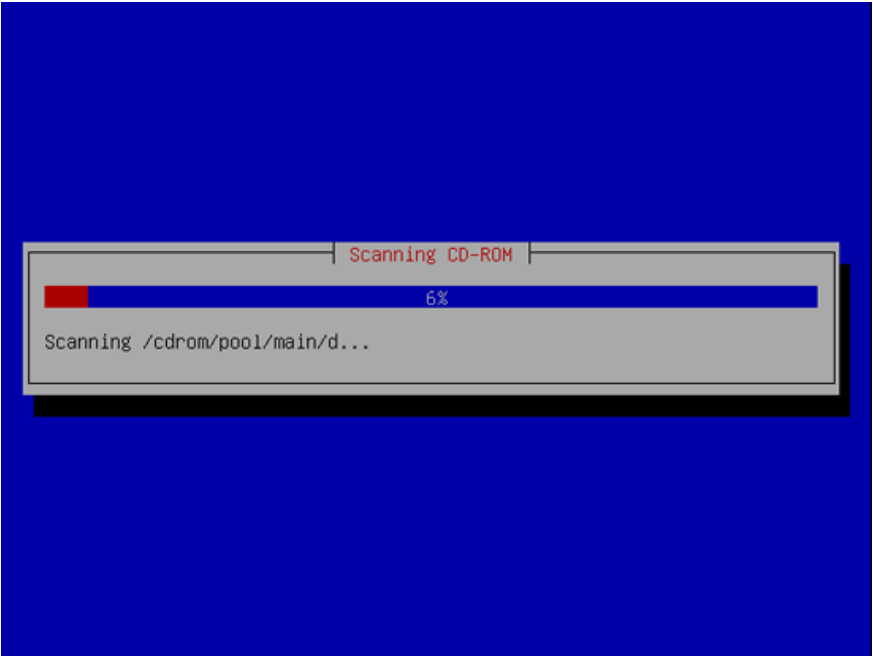
- Pilih zona lokasi... pilih “Other” kemudian “Asia” dan Cari “Indoneisa”...



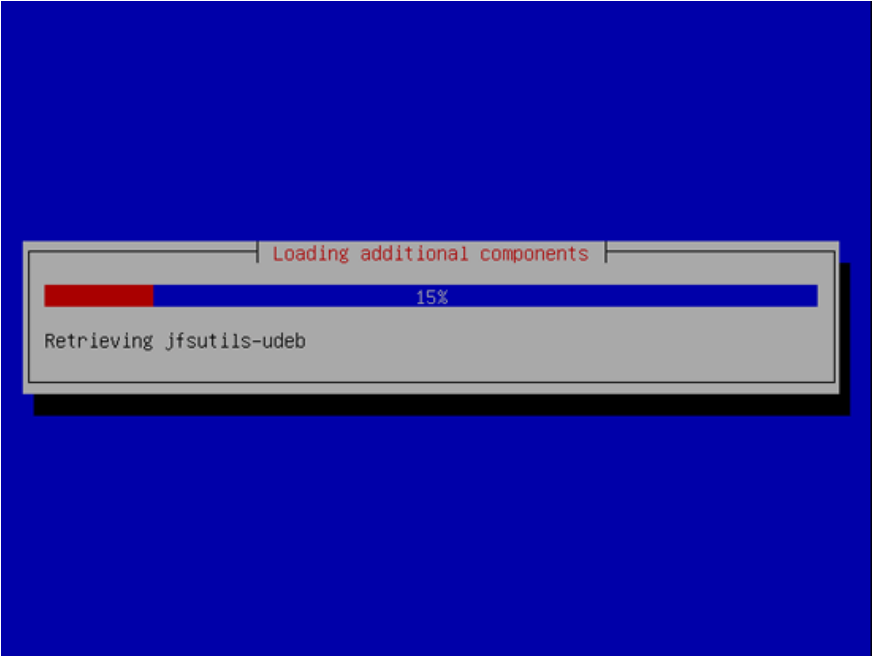
- Pilih layout/jenis keyboard, pilih aja “No”



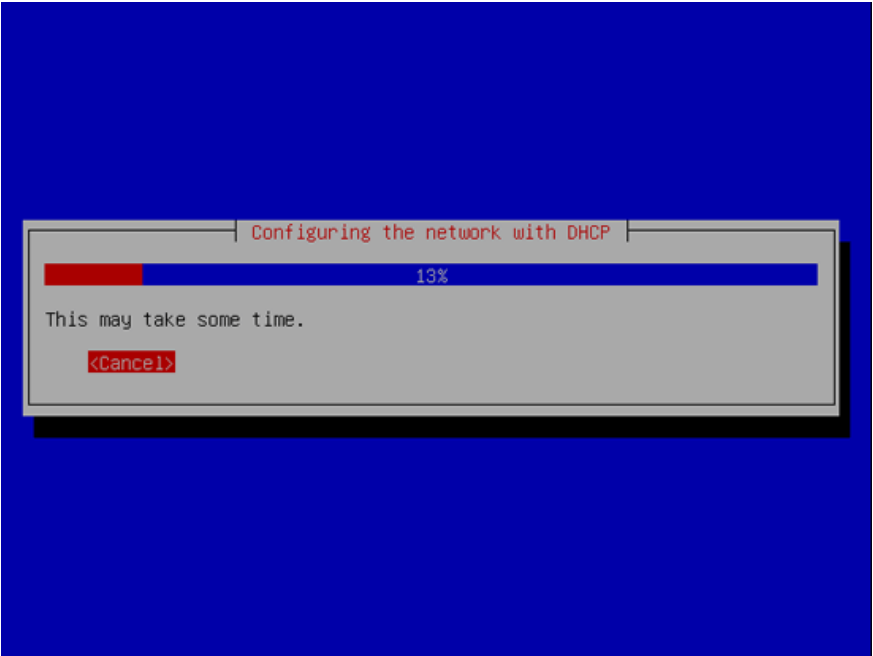
- Ubuntu Installer akan melakukan pengecekan terhadap CD yg digunakan



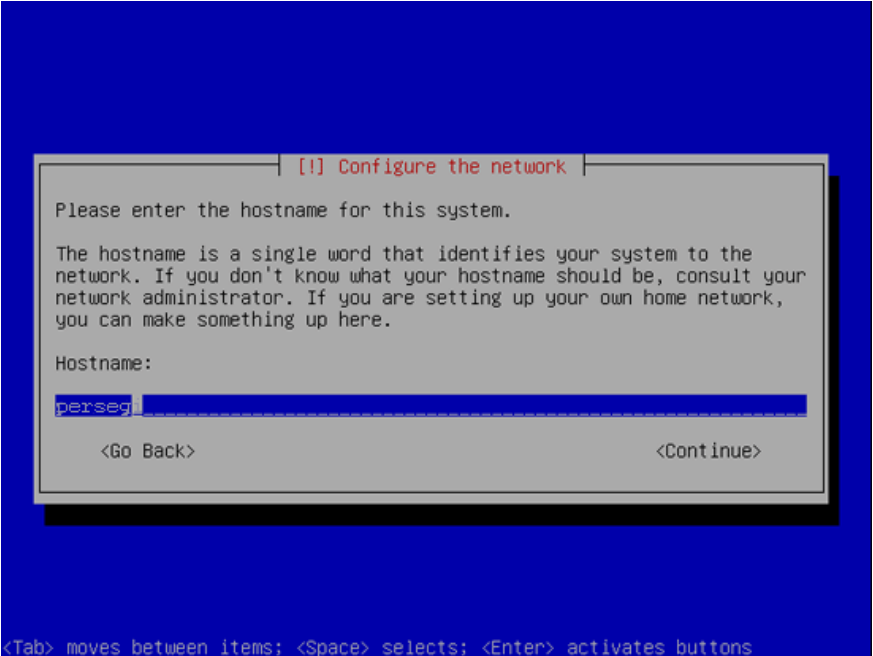
- Ubuntu Installer menjalankan komponen sebagai pendukung...



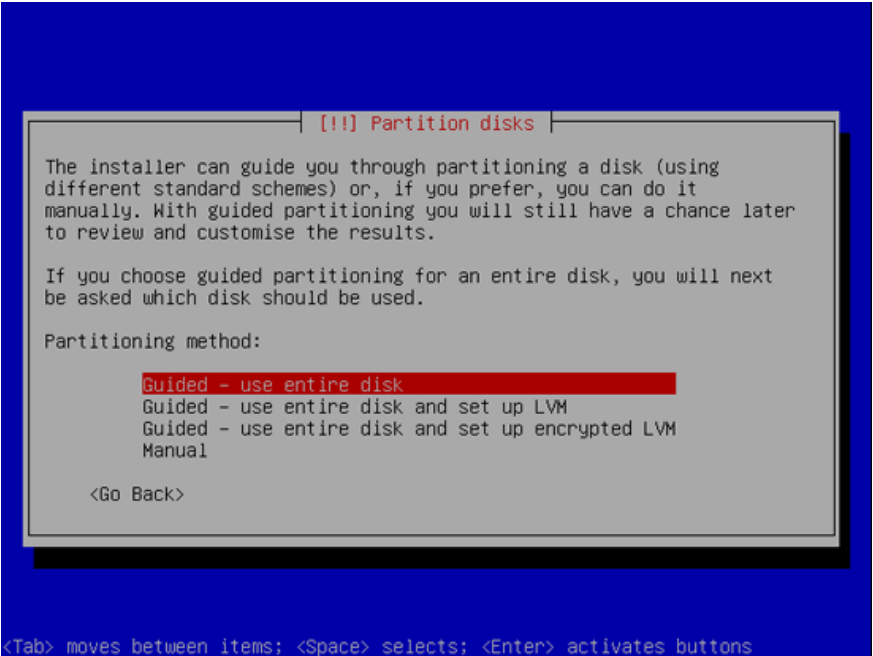
- Instalasi Network..., untuk sementara diabaikan aja karena nantinya akan di setting secara manual aja.



- Masukkan nama hostname/computer sesuai keinginan, misal: router



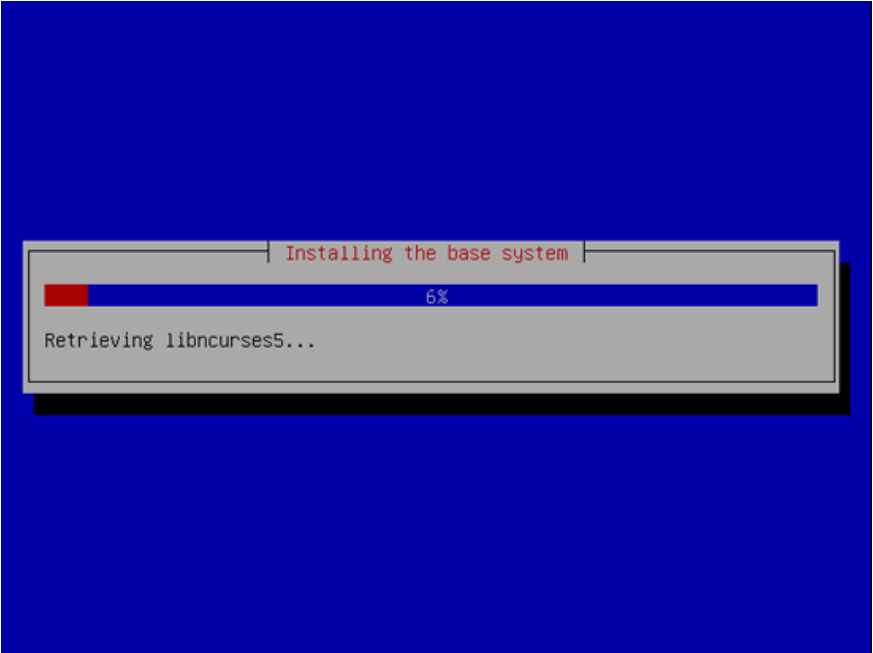
- Pengaturan Harddisk, pilih “Manual” karena akan dipersiapkan secara maksimal.



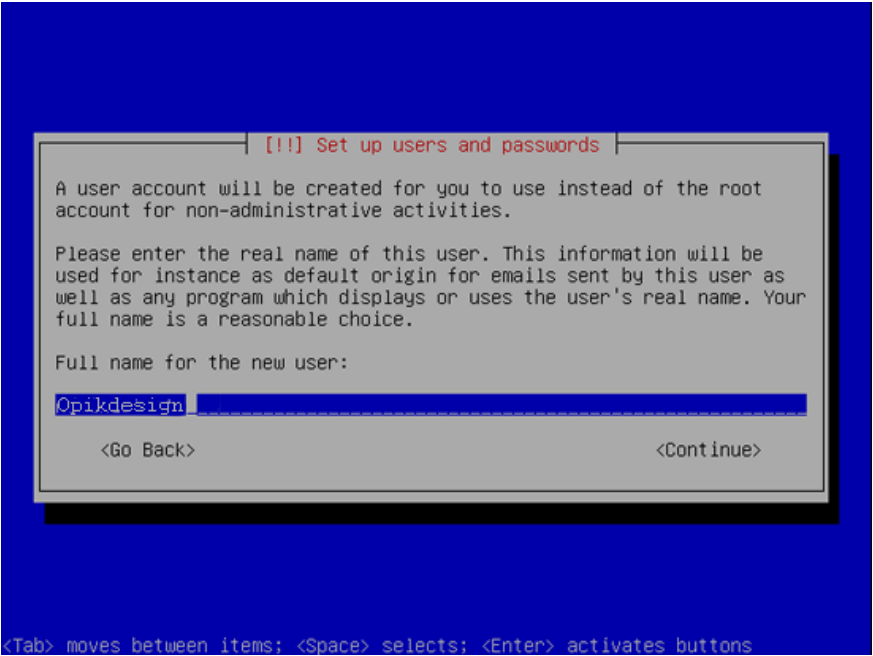
Dari harddisk 160Gb dibagi sebagai berikut:

/	25GB	XFS	Boot Flag	/
swap	1GB	swap		Swap
/home/proxy1	20GB	XFS		Chache proxy #1
/home/proxy2	20GB	XFS		Chache proxy #2
/home/proxy3	20GB	XFS		Chache proxy #3
/home/share	(sisanya)	NTFS		Share Documents

- Ubuntu installer selanjutnya akan menginstall system dasar yang dibutuhkan, tentunya setelah memformat harddisk.



- Membuat account user dan member password, misal account “Opikdesign” dan user “opikdesign”



[[!]] Set up users and passwords

Select a username for the new account. Your first name is a reasonable choice. The username should start with a lower-case letter, which can be followed by any combination of numbers and more lower-case letters.

Username for your account:

opikdesign

<Go Back>

<Continue>

<Tab> moves between items; <Space> selects; <Enter> activates buttons

[[!]] Set up users and passwords

A good password will contain a mixture of letters, numbers and punctuation and should be changed at regular intervals.

Choose a password for the new user:

\*\*\*\*\*

<Go Back>

<Continue>

<Tab> moves between items; <Space> selects; <Enter> activates buttons

[[!]] Set up users and passwords

Please enter the same user password again to verify you have typed it correctly.

Re-enter password to verify:

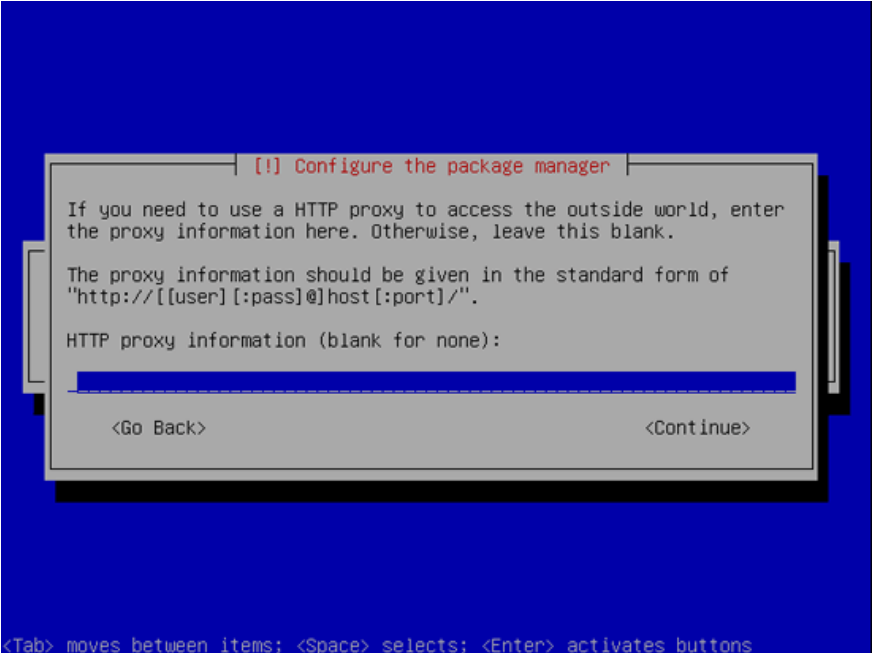
\*\*\*\*\*

<Go Back>

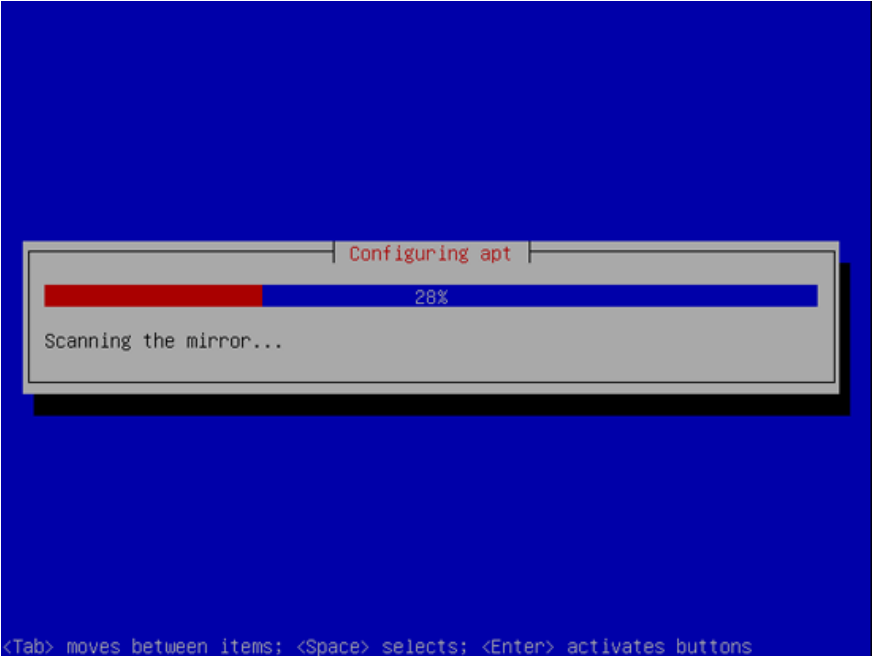
<Continue>

<Tab> moves between items; <Space> selects; <Enter> activates buttons

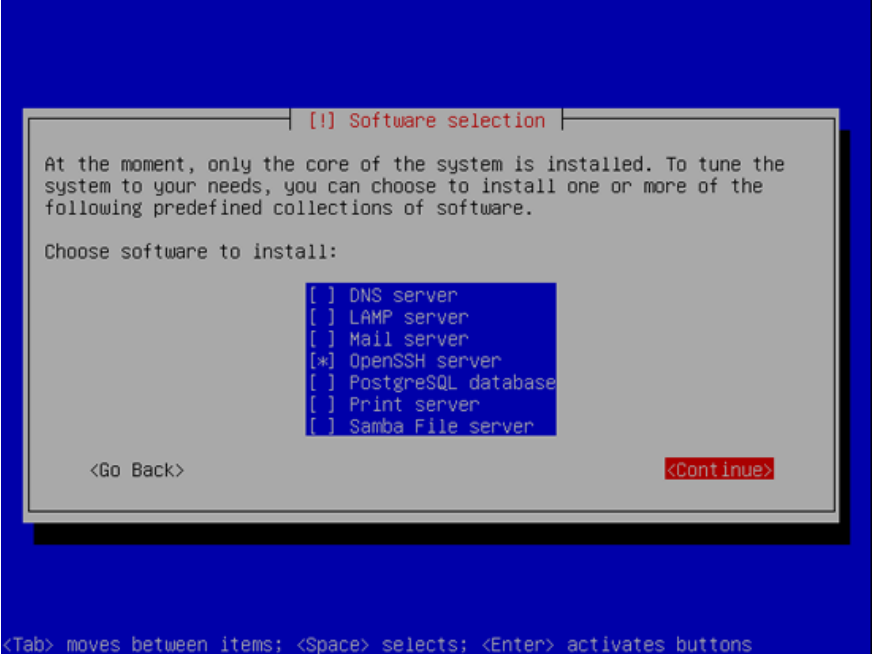
- Ubuntu Installer akan mempertanyakan apakah connection ke internet pake proxy, tapi klo tanpa proxy bisa pilih “continue”



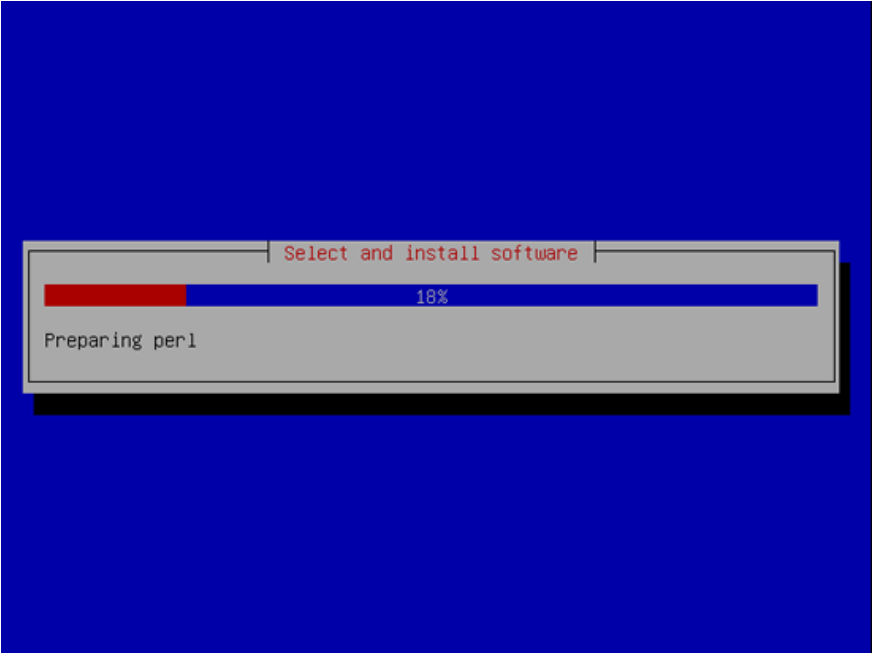
- Konfigurasi APT



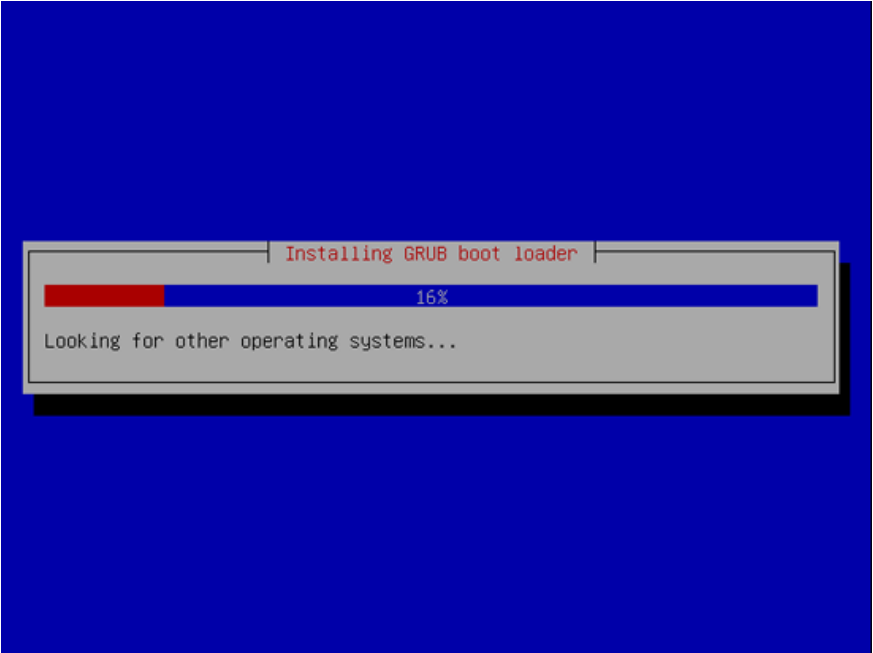
- Memilih paket... pilih aja: DNS Server, LAMP Server, OpenSSH Server dan Samba File Server



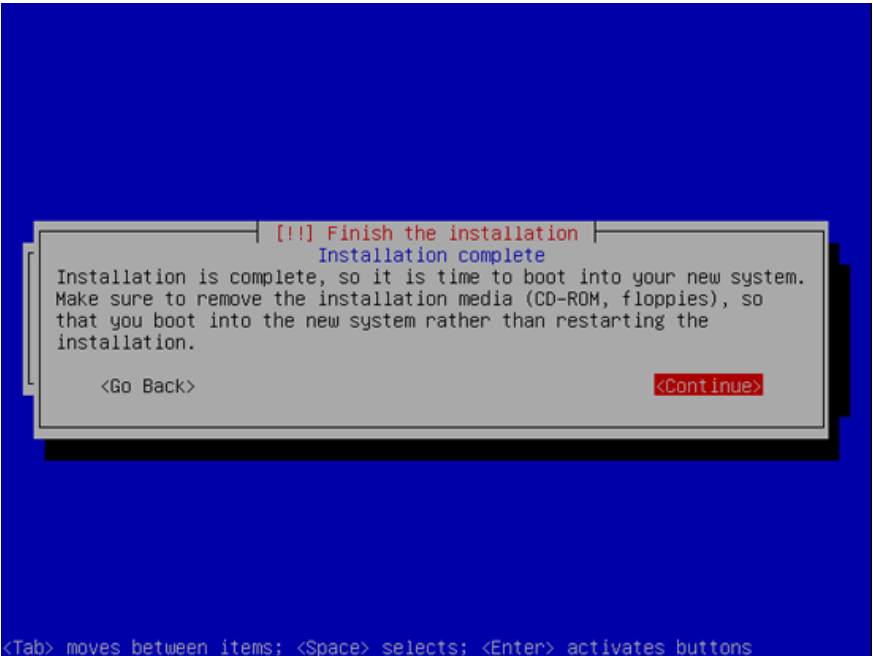
- Memulai instalasi... ditengah2 instalasi, akan ditanyakan password untuk MySQL, bisa dikosongkan ato boleh diisi...



- Instalasi GRUB Boot loader



- Instalasi berakhir, keluarkan CD-nya. Pilih “Continue” untuk restart dan boot dari harddisk.



## TAHAP II

### LOGIN

- Lakukan login.
- Kemudian masuk ke *root*, kemudian masukan password:

```
[user]@[host]:~$ sudo su
```

cirinya klo sudah masuk root maka prompt berubah menjadi

```
root@[host]:/home/[user]#
```

seperti ini:

```
login as: opikdesign
opikdesign@192.168.20.15's password:
Linux router 2.6.32-21-server #32-Ubuntu SMP Fri Apr 16 09:17:34 UTC 2010 x86_64 GNU/Linux
Ubuntu 10.04.1 LTS

Welcome to the Ubuntu Server!
 * Documentation:  http://www.ubuntu.com/server/doc

System information as of Sun Jul 25 20:27:10 WIT 2010

System load:   0.05           Memory usage: 37%   Processes:    123
Usage of /home: 0.0% of 40.07GB  Swap usage:   0%   Users logged in: 1

Graph this data and manage this system at https://landscape.canonical.com/

*** System restart required ***
Last login: Sun Jul 25 20:26:42 2010 from 192.168.20.10
opikdesign@router:~$ sudo su
[sudo] password for opikdesign:
root@router:/home/opikdesign# █
```

## TAHAP III

### SETING ETHERNET CARD

Edit file `/etc/network/interfaces`, bisa menggunakan bantuan *vi* atau *pico* dan lainnya, tetapi disini penulis menggunakan *pico* karena sudah familiar.

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

Sebelumnya tentukan dahulu IPv4 untuk kartu jaringan *eth1*, misal *IP 192.168.0.1* dan *netmask 255.255.255.0*.

Dan perlu diingat, kartu jaringan *eth0* terhubung dengan modem ADSL dan IPv4 mengikuti DHCP dari modem jadi kita tidak perlu seting lagi karena sudah di seting saat peng-install-an tersebut diatas.

Isi file `/etc/network/interfaces` rubah menjadi berikut :

```
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
    address 192.168.1.2
    netmask 255.255.255.0
    network 192.168.1.0
    broadcast 192.168.1.255

auto eth1
iface eth1 inet static
    address 192.168.0.1
    netmask 255.255.255.0
    network 192.168.0.0
    broadcast 192.168.0.255
```

kemudian di-save.

- Lakukan restart/start pada network:

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

- Lihat hasil seting kartu jaringan pada *eth0* dan *eth1*:

```
# ifconfig
```



seharusnya hasilnya:

```
root@persegi:/home/opikdesign# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:11:95:5e:59:6a
          inet addr:192.168.1.2  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::211:95ff:fe5e:596a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:49052 errors:0 dropped:0 overruns:0 frame:0
          TX packets:62718 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9171083 (9.1 MB)  TX bytes:38158383 (38.1 MB)
          Interrupt:12 Base address:0xc000

eth1      Link encap:Ethernet  HWaddr 00:e0:4f:39:45:e4
          inet addr:192.168.0.1  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::211:95ff:fe5e:596a/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
          Interrupt:11 Base address:0xc400

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:60152 errors:0 dropped:0 overruns:0 frame:0
          TX packets:60152 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:22028453 (22.0 MB)  TX bytes:22028453 (22.0 MB)
```

### TAHAP III

## MEMBUAT SETTING DIAL-UP UNTUK MODEM ADSL

- Install dahulu repository pppoe :

```
# apt-get install pppoe
```

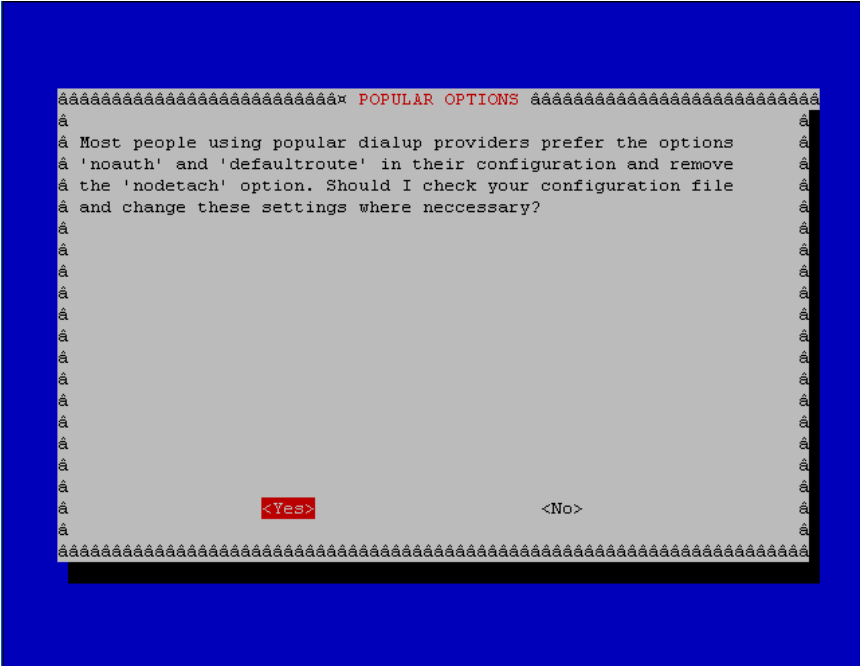
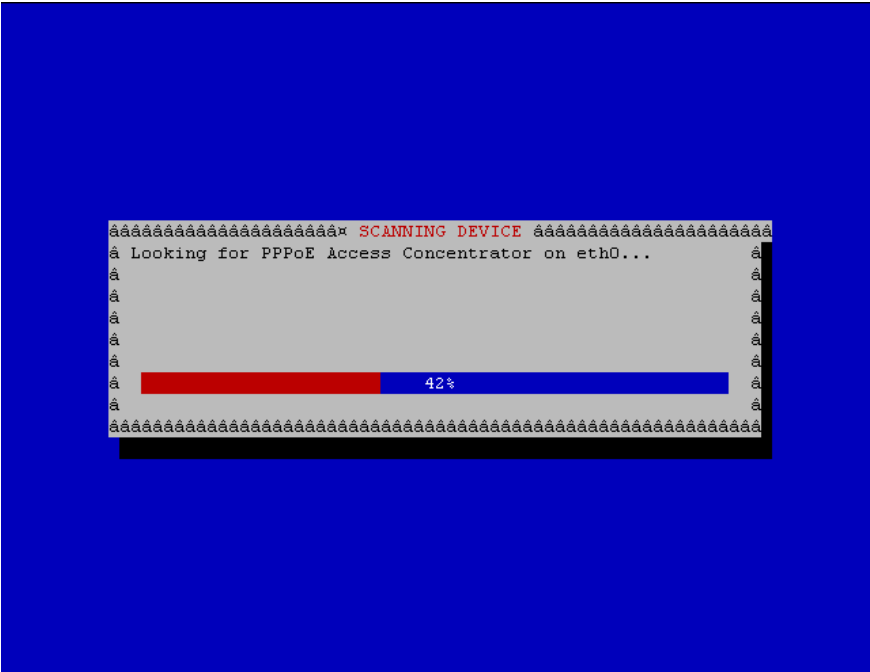
- Jalankan `pppoeconf`

```
# pppoeconf
```

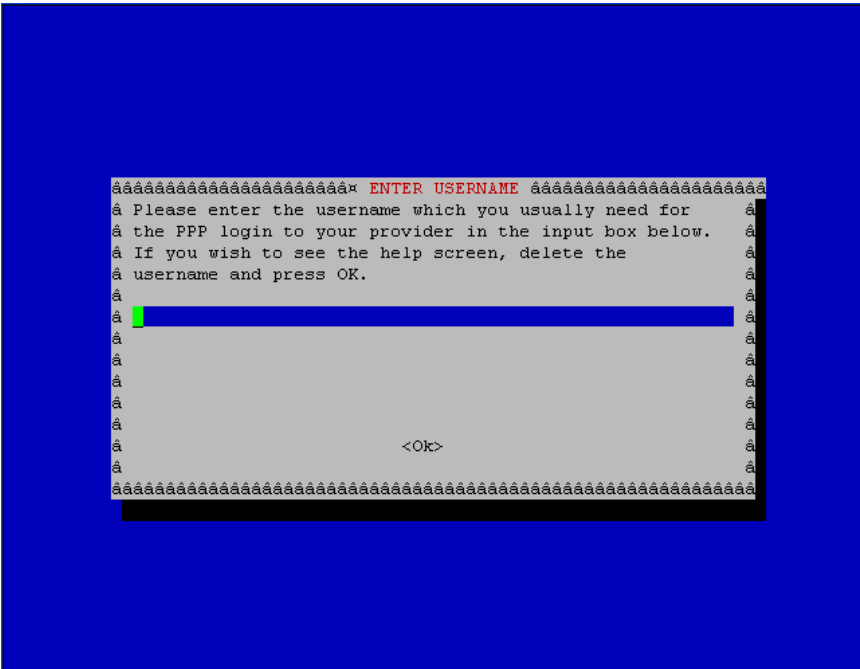
tampilannya akan seperti ini:

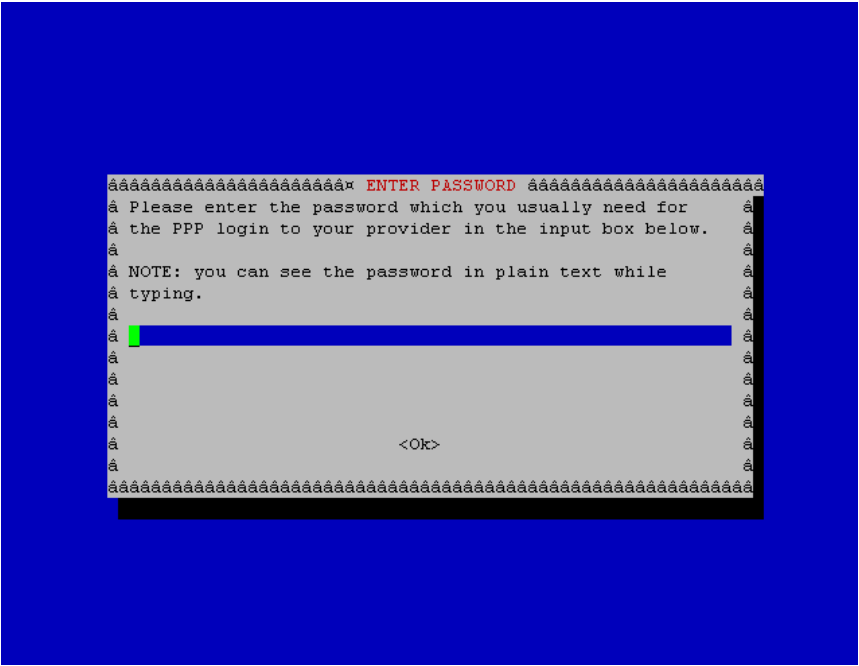


- Pilih “Yes” kemudian dia akan mendeteksi sendiri berada dimana modem ADSL tersebut.

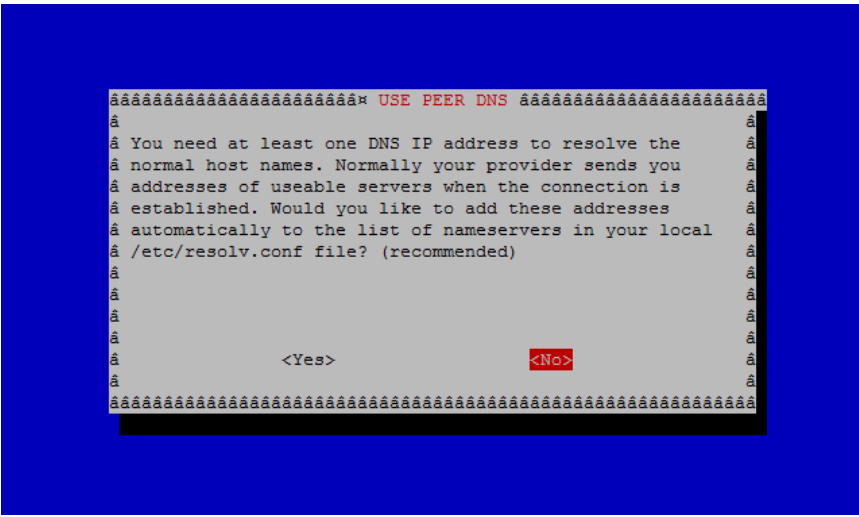


- Pilih “yes”, diminta username dan password ADSL

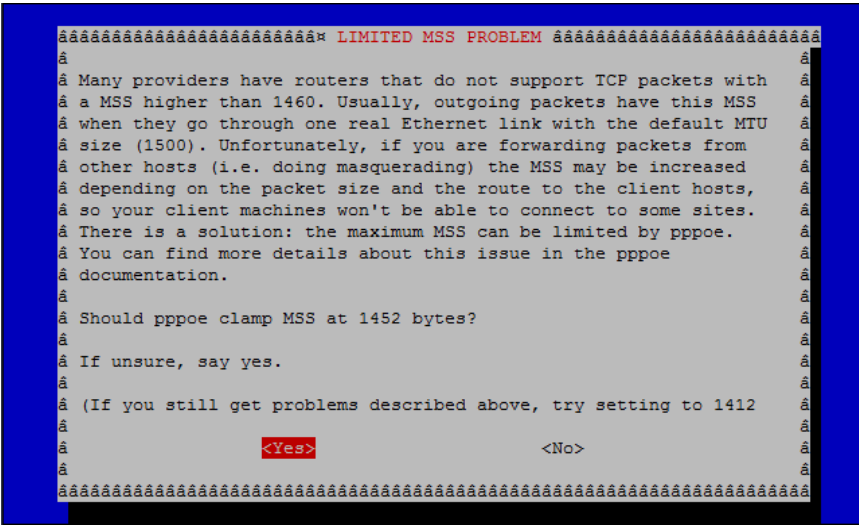




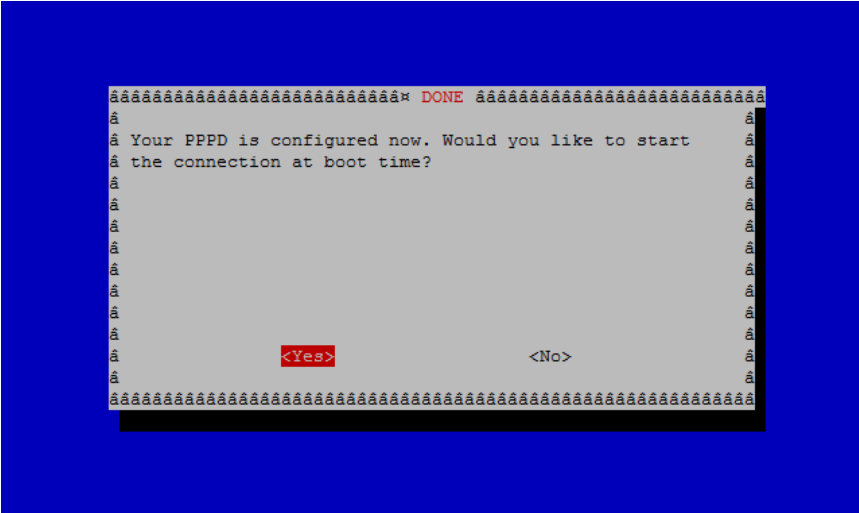
- Pilih jangan menggunakan DNS Peers karena nanti kita akan membuat DNS Server local, jadi pilih "No"...



- Untuk MTU pilih "Yes" untuk default 1452byte



- Done dan langsung melakukan koneksi...



- Klo sudah, check di file `/etc/network/interfaces` akan ada tambahannya seperti ini :

```
auto dsl-provider
iface dsl-provider inet ppp
pre-up /sbin/ifconfig eth0 up # line maintained by pppoeconf
provider dsl-provider
```

maka isi keseluruhan file (tulisan warna merah) :

```
auto lo
iface lo inet loopback

auto eth0
iface eth1 inet static
    address 192.168.1.2
    netmask 255.255.255.0
    network 192.168.1.0
    broadcast 192.168.1.255

auto eth1
iface eth1 inet static
    address 192.168.0.1
    netmask 255.255.255.0
    network 192.168.0.0
    broadcast 192.168.0.255

auto dsl-provider
iface dsl-provider inet ppp
pre-up /sbin/ifconfig eth0 up # line maintained by pppoeconf
provider dsl-provider
```

- Check interfaces dial-up dengan `ifconfig`, dial-up akan muncul interfaces ppp0

`# ifconfig ppp0`

hasilnya :

```
root@cityadexpo:~# ifconfig ppp0
ppp0      Link encap:Point-to-Point Protocol
          inet addr:125.160.1.1 P-t-P:125.160.1.1 Mask:255.255.255.255
          UP POINTOPOINT RUNNING NOARP MULTICAST MTU:1492 Metric:1
          RX packets:1794 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1561 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:3
          RX bytes:238470 (238.4 KB)  TX bytes:161979 (161.9 KB)
```

- Atau cara nge-check lain, lakukan ping ke inet.

## TAHAP IV

### UP-DATE DAN UP-GRADE SYSTEM, SEKALIGUS INSTALL BEBERAPA REPOSITORY YANG AKAN SERING DIPAKAI

- Up-date dan Up-grade :

```
# apt-get update && apt-get upgrade -y && apt-get dist-upgrade -y
```

- Install beberapa repository penting yang akan sering terpakai...

```
# apt-get install iptraf iftop whois sysstat snmp snmpd rrdtool dbconfig-common libphp-adodb php5-cli php5-gd  
php-pear php5-snmp php5-adodb phpmyadmin make rpm alien subversion nmap libnet-netmask-perl curl chkconfig
```

- Lakukan restart.

```
# reboot
```

## TAHAP V

### INSTALL DAN SETING DHCP SERVER

Untuk server, mungkin perlu DHCP Server agar computer client yg terhubung langsung mendapat IP tanpa seting secara manual.

- Install dahulu DHCP Server
  - Install dhcp3 server-nya,

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

seharusnya hasilnya :

```
root@router:/home/opikdesign# apt-get install dhcp3-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-2.6.32-21 linux-headers-2.6.32-21-server
Use 'apt-get autoremove' to remove them.
Suggested packages:
  dhcp3-server-ldap
The following NEW packages will be installed:
  dhcp3-server
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 398kB of archives.
After this operation, 918kB of additional disk space will be used.
Get:1 http://id.archive.ubuntu.com/ubuntu/lucid/main dhcp3-server 3.1.3-2ubuntu3 [398kB]
Fetched 398kB in 1min 5s (6,070B/s)
Preconfiguring packages ...
Selecting previously deselected package dhcp3-server.
(Reading database ... 65178 files and directories currently installed.)
Unpacking dhcp3-server (from .../dhcp3-server_3.1.3-2ubuntu3_amd64.deb) ...
Processing triggers for man-db ...
Processing triggers for ureadahead ...
Setting up dhcp3-server (3.1.3-2ubuntu3) ...
Generating /etc/default/dhcp3-server...
  * Starting DHCP server dhcpd3
  * check syslog for diagnostics.

invoke-rc.d: initscript dhcp3-server, action "start" failed.
root@router:/home/opikdesign#
```

- Setelah diinstall, lakukan seting pada DHCP3 Server, misalnya dgn asumsi jaringan pada *eth1* pada range *IP 192.168.0.100-192.168.0.200* dan *Netmask 255.255.255.0*. Edit file conf pada DHCP3 yaitu file */etc/dhcp3/dhcpd.conf*,

```
# pico /etc/dhcp3/dhcpd.conf
```

Rubah menjadi :

```
ddns-update-style none;

subnet 192.168.0.0 netmask 255.255.255.0 {
    option broadcast-address 192.168.0.255;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 192.168.0.1;
    option domain-name "local.domain"; #sesuaikan keinginan
    option routers 192.168.0.1;
    option netbios-name-servers 192.168.0.1;

    default-lease-time 600;
    max-lease-time 604800;

    log-facility local7;

    range 192.168.0.100 192.168.0.200;
}
```

Catatan,  
untuk `option domain-name-servers` nanti bisa diganti dgn DNS ISP yg bersangkutan klo tidak menginstall DNS Server dan seandainya DNS lebih dari satu tinggal diberi tanda koma “,”.  
begitu juga `option netbios-name-servers` bisa dihilangkan klo nanti tidak membuat WINS Server,.

- Setelah itu edit file `/etc/default/dhcp3-server` dan disinilah settingan DHCPdefault interfaces.

```
# pico /etc/default/dhcp3-server
```

Rubah atau isi **INTERFACES**-nya seperti dibawah ini

```
INTERFACES="eth1"
```

- Lakukan restart DHCP3-server dengan:

```
# /etc/init.d/dhcpd3-server restart
```

Akan muncul dilayar:

```
* Starting DHCP server dhcpd3 [ OK ]
```

- DHCP bisa di buat seperti halnya MAC Filter, dalam pengertian sebagai berikut:  
Kita sebelumnya sudah mencatat MAC-ADDRESS dari seluruh hardware Ethernet maupun wifi client yang kemudian diberikan IP sesuai ketentuan MAC-ADDRESS; contoh computer A dengan MAC 00:AA:BB:CC:DD:11 akan selalu mendapat IP 192.168.0.123.

Rubah `/etc/dhcp3/dhcpd.conf`, contoh konfigurasi dengan MAC Filtering :

```
ddns-update-style none;

subnet 192.168.0.0 netmask 255.255.255.0 {
    option broadcast-address 192.168.0.255;
    option subnet-mask 255.255.255.0;
    option domain-name-servers 192.168.0.1;
    option domain-name "local.domain"; #sesuaikan keinginan
    option routers 192.168.0.1;
    option netbios-name-servers 192.168.0.1;

    default-lease-time 600;
    max-lease-time 604800;

    log-facility local7;

    host opikdesign {
        hardware ethernet 00:22:15:3C:14:A1;
        fixed-address 192.168.0.100;
    }

    host dhani {
        hardware ethernet 00:11:5B:78:D3:E8;
        fixed-address 192.168.0.101;
    }

    host farah {
        hardware ethernet 00:16:EC:1E:2F:9E;
        fixed-address 192.168.0.102;
    }

    host siti {
        hardware ethernet 00:13:D4:CB:69:0F;
        fixed-address 192.168.0.103;
    }
}
```

Jadi disini bisa dipahami seharusnya, coba lihat keterangan bertulis tebal...

```
host [disini letak nama computer] {  
    hardware ethernet [disini diisi MAC-ADDRESS dari client yang bersangkutan];  
    fixed-address [IP yang akan diberikan];  
}
```

Selanjutnya MAC-ADDRESS bisa disesuaikan dengan client, tersebut diatas hanya contoh...

# TAHAP VI

## SETTING Open-SSH SERVER

### DAN MENGGUNAKAN PuTTY & WinSCP

### UNTUK REMOTE KE SERVER

Sebuah port yang cara komunikasinya di encryption dan artinya para pembajak/penyadap jaringan tidak bisa mengartikannya, dengan demikian komunikasi sangat aman. SSH ini biasanya digunaka untuk remote server sebagai pengganti telnet, rsh dan rlogin. Aplikasi server yang sering digunakan dan akan kita gunakan di sini adalah PuTTY untuk remote selayaknya kita duduk di depan monitor dan keyboar server dan WinSCP berfungsi untuk transfer file seperti halnya sftp.

Pada umumnya port Open-SSH default di port 22 dan sebaliknya dirubah dengan alasan untuk keamanan, dirubah ke port yang masih kosong atu yang belum digunakan untuk fungsi lain misal, 222 ato 2222 ato berapa aja.

- Edit file `/etc/ssh/sshd_config` :

```
# pico /etc/ssh/sshd_config
```

cari `Port 22` dan ganti dengan port yang di kehendaki semisal `Port 221`

- Kemudian restart open-ssh:

```
# service ssh restart
```

hasil tampilannya :

```
root@router:/home/opikdesign# service ssh restart  
ssh start/running, process 10908  
root@router:/home/opikdesign# █
```

- Kemudian memberi password pada user `root` agar tiap kali login untuk mengedit file bisa langsung edit dan bisa langsung meng-copy ato paste file di semua folder linux. Pada dasarnya username `root` sudah ada hanya belum ada passwordnya akhirnya seakan tidak aktif. User `root` ini ada user yang memiliki hak akses dan sebaiknya jangan diberikan ke orang lain.

Cara mengganti/memberi password :

```
# passwd root
```

masukan password yang dikehendaki dan ketik ulang.

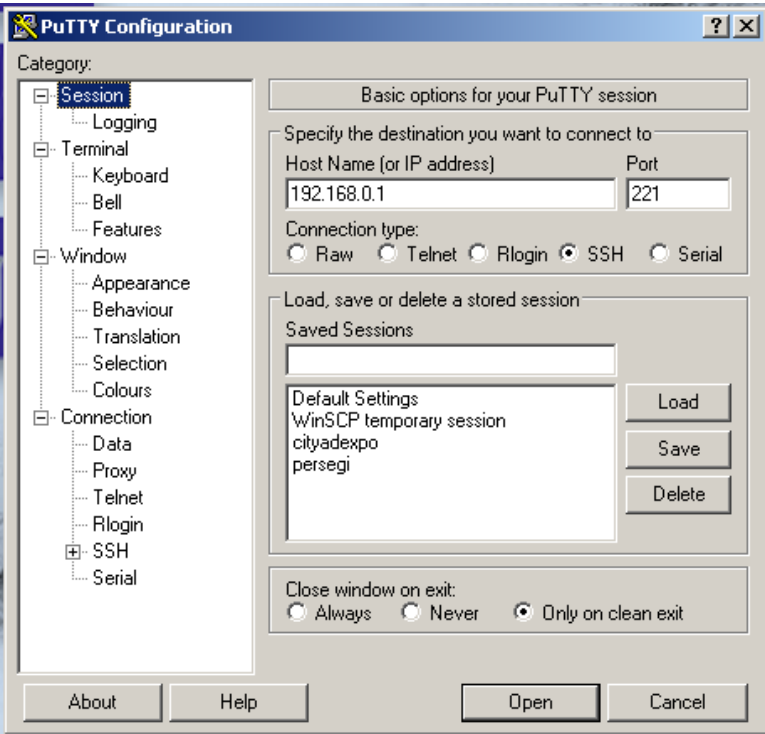
```
root@persegi:~# passwd root  
Enter new UNIX password:  
Retype new UNIX password:  
passwd: password updated successfully  
root@persegi:~# █
```

- Download program PuTTY dan WinSCP dari computer client yang ber-OS windows.

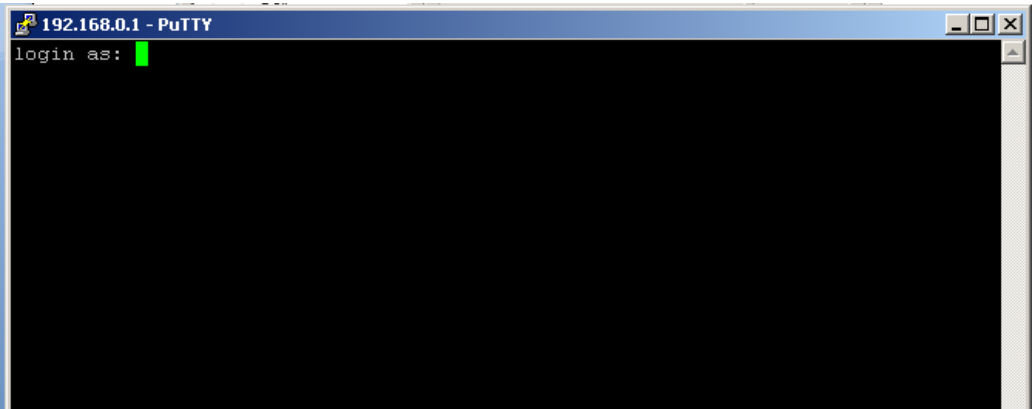
Download PuTTY >>> <http://putty.cbn.net.id/download.html>  
pilih yang versi installer karena lebih stabil atau langsung ke link ini >>>  
<http://tartarus.org/~simon/putty-snapshots/x86/putty-installer.exe>

Download WinSCP >>> <http://mirror.its.ac.id/pub/winscp/>  
pilih yang versi installer juga atau langsung ke link ini >>> <http://mirror.its.ac.id/pub/winscp/winscp407setupintl.exe>

- Kemudian install PuTTY dan WinSCP, disini tidak perlu saya bicarakan bagaimana caranya karena hal yang mudah.
- Cara menggunakan PuTTY, masukkan ip ato nama host server kemudian masukkan port yang sudah dirubah.

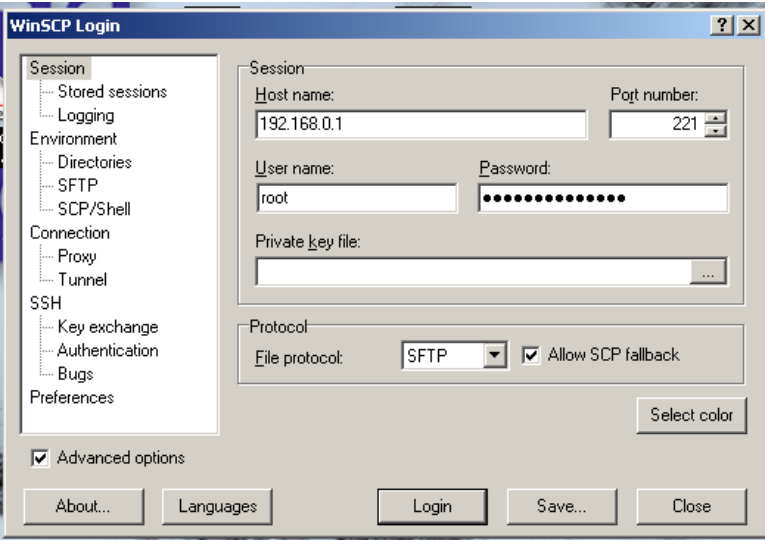


Click Open klo sudah mengisi Host Name/IP server maupun port-nya.  
Maka tampilan akan menjadi...



Nah tampilan seperti apa?! Sama persis saat login pertama khan?! Apa bedanya dengan duduk depan server langsung?! Tentu Aja jawabannya sama. Maka dari itu Ubuntu Server sudah tidak memerlukan Monitor maupun Keyboard lagi karena akan di-remote di computer lain atas alasan efisiensi.

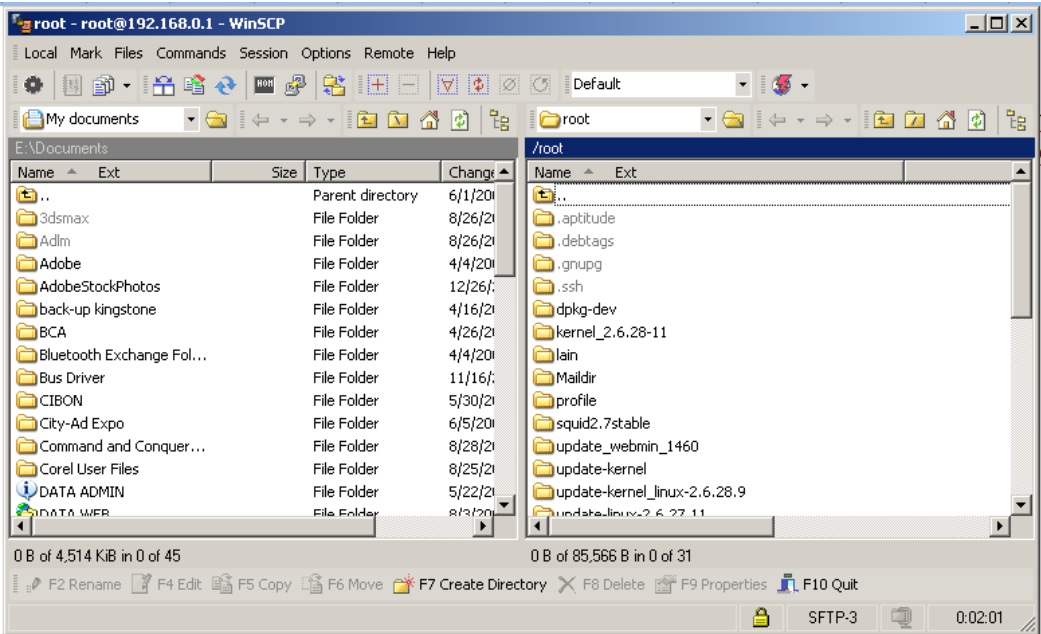
- Cara menggunakan WinSCP.



Masukkan host name ato ip server dan port-nya, masukkan pula username dan passwordnya, disini saya sarankan menggunakan username dan password root dengan alasan agar kita bisa mendapat full akses ke semua folder maupun file bertujuan kita bisa mengedit file2 configuration. Kemudian click Login.



Tampilannya akan seperti ini...



Sisi kiri adalah *My Document* dan sisi kanan adalah folder */root* di ubuntu server. Disini kita bisa memindahkan file atau folder dari kiri dan ke kanan maupun sebaliknya. Bisa masuk ke semua folder di ubuntu server maupun bisa merubah file2 configuration termasuk membuat file configuration lainnya.

## TAHAP VII

### MEMBUAT NAT / ROUTER

Agar client bisa terkoneksi dengan internet maka kita harus mengaktifkan ip forward.

- Membuat router maka aktifkan IP Forwarding, dari *ppp0* ke *eth1*, edit file */etc/sysctl.conf* :

cari teks

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

Aktifkan dengan menghilangkan tanda “#”, menjadi :

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

untuk meningkatkan pengaman sebaiknya anti spoofing attack dan kernel map protect diaktifkan, cari teks2 dibawah ini...

```
# net.ipv4.conf.default.rp_filter=1
# net.ipv4.conf.all.rp_filter=1
```

Aktifkan dengan menghilangkan tanda “#”, menjadi:

```
net.ipv4.conf.default.rp_filter=1
net.ipv4.conf.all.rp_filter=1
```

kemudian save. Dan lakukan perintah untuk mengaktifkan konfigurasi tersebut

```
# sysctl -p
```

```
root@router:/home/opikdesign# sysctl -p
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.ip_forward = 1
root@router:/home/opikdesign#
```

- Membuat NAT dengan command *iptables*  

```
# iptables -t nat -A POSTROUTING -o ppp0 -j MASQUERADE
```

Lakukan test di client, bisa langsung browsing atau melakukan ping ke inet.

# TAHAP VIII

## INSTALL DAN SETING PADA DNS SERVER MENGGUNAKAN BIND9

Pada saat instalasi Ubuntu tadi sudah memilih untuk diinstallkan DNS Server, sebenarnya repository yang berfungsi sebagai DNS Server bernama Bind9. Akhirnya kita tinggal membuat settingan Bind9 ini.

Fungsi DNS Server ini adalah mem-resolved nama domain yang diminta client untuk di memberitahukan server dari domain yang ditanyakan client berada di IP mana.

- Sebelumnya, ada baiknya kita mengenal macam type DNS Record;

**Address Records;** Merekam sebuah pemetaan IP Address ke dalam sebuah nama host. Cara seperti ini yang paling umum digunakan.

www	IN	A	111.222.333.444
-----	----	---	-----------------

**Alias Records;** Membuat sebuah alias terhadap CNAME karena tidak dapat membuat CNAME pointing didalam CNAME Record.

mail	IN	CNAME	www
www	IN	A	111.222.333.444

**Mail Exchange Records;** Menunjukkan email harus dikirim kemana, harus menunjukkan ke A Record (Address Record) bukan CNAME (Alias Record) Record.

@	IN	MX	mail.domain.com
mail	IN	A	111.222.333.444

**Name Server Record;** Menentukan server yang akan digunakan untuk melayani layanan hosting, harus menunjukkan ke A Record (Address Record) bukan CNAME (Alias Record) Record.

@	IN	NS	ns.domain.com
ns	IN	A	111.222.333.444

- Selanjutnya kita memulai konfigurasi Bind9, sebelumnya kita tentukan nama domainnya semisalnya [dns.persegi.net](#) dan kemudian dapat diganti sesuai keinginan.
- Buka file [/etc/bind/named.conf.options](#); file tersebut berisi DNS forward ditujukan kemana, maka itu karena kita memakai telkomspeedy maka diarahkan IP DNS Telkom dan ditambah OpenDNS. Rubah isinya menjadi:

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

    forwarders {
        202.134.0.155;
        202.134.0.61;
        //202.134.0.5; - down
        //202.134.2.5; - down
        202.134.1.5;
        202.134.1.10;
        203.130.193.74;
        203.130.196.6;
        203.130.196.155;
        203.130.196.5;
        203.130.208.18;
        203.130.206.250;
        222.124.204.34;
        //DNS Public from openDNS
        //208.67.222.222;
        //208.67.220.220;
        //DNS Public from google
        8.8.8.8;
        8.8.4.4;
    };

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

- Buka file [/etc/bind/named.conf.local](#); file yang berisi dimana letak file zona yang berisi DNS Record local.

tambah atau edit isinya menjadi:

```
include "/etc/bind/zones.rfc1918";

zone "local.domain" {
    type master;
    file "/etc/bind/db.local.domain";
};

zone "0.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192";
};

include "/etc/bind/rndc.key";
```

- Kemudian duplicate file db local sesuai nama file yang disebutkan `/etc/bind/named.conf.local`.  
`# cp /etc/bind/db.local /etc/bind/db.local.domain`  
`# cp /etc/bind/db.local /etc/bind/db.192`

- Edit file `/etc/bind/db.local.domain`  
edit isinya menjadi:

```
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      ns.local.domain. mail.local.domain. (
                                2010072605      ;Serial
                                604800            ;Refresh
                                86400             ;Retry
                                2419200           ;Expire
                                604800 )          ;Negative Cache TTL
;
localhost IN      A        127.0.0.1
@          IN      NS       ns.local.domain.
ns         IN      A        192.168.0.1
www        IN      CNAME    ns
proxy      IN      CNAME    ns
```

sebuah tips: Banyak orang menggunakan tanggal terakhir edited sebagai seri dari zona, seperti 2009022605 yang yyyymmddss (di mana angka serial), setiap edit file konfigurasi tersebut agar mengganti serial tersbut dengan tanggal terbaru bertujuan agar bind9 segera mengupdate perubahannya.

- Edit file `/etc/bind/db.192`

edit isinya menjadi:

```
;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA      ns.local.domain. mail.local.domain. (
                                2010072603      ;Serial
                                604800            ;Refresh
                                86400             ;Retry
                                2419200           ;Expire
                                604800 )          ;Negative Cache TTL
;
@         IN      NS       ns.
www        IN      CNAME    ns
proxy      IN      CNAME    ns
```

sebuah tips:  
Banyak orang menggunakan tanggal terakhir edited sebagai seri dari zona, seperti 2010072605 yang yyyymmddss (di mana angka serial), setiap edit file konfigurasi tersebut agar mengganti serial tersbut dengan tanggal terbaru bertujuan agar bind9 segera mengupdate perubahannya.

- Edit file `/etc/hosts` dan tambahkan `local.domain` domain ini diaktifkan sebagai host pula.

edit isinya menjadi:

```
127.0.0.1 localhost
192.168.0.1 router router.local.domain www.local.domain proxy.local.domain
```

- Edit file `/etc/resolv.conf`

edit isinya menjadi:

```
search local.domain
nameserver 127.0.0.1
```

- Restart jaringan dan bind9...  
`# service bind9 restart`
- Untuk menguji bind9, kita perlu menginstall repository dnsutils, install repository tersebut...

`# apt-get install dnsutils`

check zona untuk mengetest settingan kita didalam file `/etc/bind/db.dns.persegi.net` dan `/etc/bind/db.192`

`# named-checkzone local.domain /etc/bind/db.local.domain`

kalau settingan tidak ada masalah hasilnya... kurang lebih akan muncul serial yang buat.

```
root@persegi: ~  
root@persegi:~# named-checkzone dns.persegi.net /etc/bind/db.dns.persegi.net  
zone dns.persegi.net/IN: loaded serial 2009022605  
OK
```

# *named-checkzone local.domain /etc/bind/db.192*

hasilnya...

```
root@persegi: ~  
root@persegi:~# named-checkzone dns.persegi.net /etc/bind/db.192  
zone dns.persegi.net/IN: loaded serial 2009022603  
OK
```

kemudian baru menguji dengan command *dig*... kita mencoba untuk local-nya dulu...

# *dig localhost*

hasilnya...

```
root@persegi: ~  
root@persegi:~# dig localhost  
  
; <<>> DiG 9.5.1-P2 <<>> localhost  
;; global options: printcmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2507  
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1  
  
;; QUESTION SECTION:  
;localhost.                IN      A  
  
;; ANSWER SECTION:  
localhost.                604800  IN      A      127.0.0.1  
  
;; AUTHORITY SECTION:  
localhost.                604800  IN      NS      localhost.  
  
;; ADDITIONAL SECTION:  
localhost.                604800  IN      AAAA    ::1  
  
;; Query time: 2 msec  
;; SERVER: 192.168.0.200#53(192.168.0.200)  
;; WHEN: Tue Sep  8 06:26:55 2009  
;; MSG SIZE  rcvd: 85
```

kemudian coba menguji untuk mencari domain di inet... misalnya google.com atau yahoo.com...

# *dig google.com*

hasilnya...

```
; <<>> DiG 9.5.1-P2 <<>> google.com  
;; global options: printcmd  
;; Got answer:  
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19632  
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 4, ADDITIONAL: 4  
  
;; QUESTION SECTION:  
;google.com.              IN      A  
  
;; ANSWER SECTION:  
google.com.              67      IN      A      74.125.127.100  
google.com.              67      IN      A      74.125.45.100  
google.com.              67      IN      A      74.125.67.100  
  
;; AUTHORITY SECTION:  
google.com.              1681    IN      NS      ns3.google.com.  
google.com.              1681    IN      NS      ns2.google.com.  
google.com.              1681    IN      NS      ns1.google.com.  
google.com.              1681    IN      NS      ns4.google.com.  
  
;; ADDITIONAL SECTION:  
ns1.google.com.          418     IN      A      216.239.32.10  
ns2.google.com.          3570    IN      A      216.239.34.10  
ns3.google.com.          2977    IN      A      216.239.36.10  
ns4.google.com.          3311    IN      A      216.239.38.10  
  
;; Query time: 62 msec  
;; SERVER: 192.168.0.1#53(192.168.0.1)  
;; WHEN: Tue Sep  8 06:28:18 2009  
;; MSG SIZE  rcvd: 212
```

atau bisa juga menguji dengan perintah *nslookup*...

```
# nslookup  
> set type=any  
> local.domain
```

setelah itu lakukan pula test pada localhost

```
> localhost
```

dan hasilnya akan seperti ini kalau sudah benar

```
root@persegi: ~
root@persegi:~# nslookup
> set type=any
> dns.persegi.net
Server:         192.168.0.1
Address:        192.168.0.1#53

Name:   dns.persegi.net
Address: 192.168.0.1
dns.persegi.net nameserver = ns.dns.persegi.net.
dns.persegi.net
    origin = ns.dns.persegi.net
    mail addr = mail.dns.persegi.net
    serial = 2009022605
    refresh = 604800
    retry = 86400
    expire = 2419200
    minimum = 604800
> localhost
Server:         192.168.0.1
Address:        192.168.0.1#53

Name:   localhost.dns.persegi.net
Address: 127.0.0.1
>
```

## TAHAP IX

### INSTALL NTP SERVER

- Apa fungsi dari NTP Server?!, fungsinya agar semua PC Client mempunyai waktu yang sama dengan Server. Namun pengaktifan fungsi ini tidak terlalu penting. Cara install dan menjalankan:

```
# apt-get install ntp
# service ntp restart
```

- Untuk merubah waktu pada system linux :

```
# date DDMMhhmmYYYY
```

Keterangan :

DD:	date	hh:	hour (24 hour)
MM:	month	mm:	minute
YYYY:	year		

contohnya : dirubah menjadi 14 June 2009 11:51PM...

```
# date 061423512009
Sun Jun 14 23:51:00 WIT 2009
```

## TAHAP X

### INSTALL OpenSSL DAN MEMBUAT SSL-Certificate

### UNTUK MENGAKTIFKAN HTTPS DI APACHE2

SSL untuk HTTPS akses di apache2 milik Ubuntu memang bermasalah, kita aktifkan tetap gak mau jalan, permasalahannya krn tidak ada file Certificate untuk apache2 dan belum ada OpenSSL.

- install OpenSSL dan SSL-Certificate

```
# apt-get install openssl ssl-cert
```

- Membuat certificate :

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

- Aktifkan modul SSL

```
# a2enmod ssl
```

- Menempelkan file certificate di virtual host

```
# cp /etc/apache2/sites-available/default /etc/apache2/sites-available/ssl
```

edit file `/etc/apache2/sites-available/ssl`, tambahkan script pada baris terakhir sebelum `</VirtualHost>` :

```
SSLEngine On
SSLCertificateFile /etc/apache2/ssl/apache.pem
```

dan port default 80 jadikan 443, cari baris...

```
<VirtualHost *:80>
```

dan ganti dgn...

```
<VirtualHost *:443>
```

edit file `/etc/apache2/sites-available/default`, tambahkan script pada baris terakhir sebelum `</VirtualHost>`:

```
SSLCertificateFile /etc/apache2/ssl/apache.pem
```

- Aktifkan modul HTTPS :

```
# a2ensite ssl
```

- Terakhir restart kembali apache2 :

```
# service apache2 restart
```

## TAHAP XI

### MEMBUAT WINS SERVER DENGAN SAMBA

### MEMBANTU PENYEBARAN NETBIOS

Adanya WINS Server ini membantu agar NetBIOS (Nama Komputer Client) tidak hilang di jaringan, berfungsi untuk mem-reply NetBIOS yang dilewatkan melalui TCP/IP sebagai alternative broadcast. Disini saya hanya memberi contoh beberapa client sebagai nama computer antara lain `billing` dan `client01-10` yang kemudian bisa disesuaikan dengan kondisi yang ada.

- Sebelumnya install dahulu repository yang di butuhkan...

```
# apt-get install samba samba-common samba-doc libcupsys2 winbind smbclient smbfs
```

- Edit file `/etc/samba/smb.conf` dan rubah menjadi...

```
[global]
log file = /var/log/samba/log.%m
passwd chat = *Enter\snew\s*\spassword:* %n\n *Retype\snew\s*\spassword:* %n\n *password\supdated\ssuccessfully*.
obey pam restrictions = yes
map to guest = bad user
encrypt passwords = true
public = yes
passdb backend = tdbsam
passwd program = /usr/bin/passwd %u
wins support = yes
max wins ttl = 18748800
min wins ttl = 60
netbios name = persegi
server string = %h server (Samba, Ubuntu)
path = /var/tmp
preferred master = yes
domain master = yes
local master = yes
workgroup = WORKGROUP
syslog = 0
panic action = /usr/share/samba/panic-action %d
usershare allow guests = yes
max log size = 1000
pam password change = yes
name resolve order = wins bcast hosts lmhosts
socket options = TCP_NODELAY IPTOS_LOWDELAY SO_KEEPALIVE SO_RCVBUF=8192 SO_SNDBUF=8192
os level = 65
announce as = WfW
guest ok = Yes
usershare allow guests = Yes
name cache timeout = 0
nt status support = yes
nt pipe support = yes
winbind cache time = 60
idmap uid = 50-9999999999
idmap gid = 50-9999999999
idmap cache time = 120
```

```
lm announce = yes
lm interval = 10
enhanced browsing = Yes
browse list = yes
```

- Edit file `/etc/hosts` kemudian masukkan nama host computer client dan ip-nya untuk pencarian dengan metode hosts file, contoh sebagai berikut :

```
127.0.0.1 localhost
192.168.0.1 router router.local.domain www.local.domain proxy.local.domain
192.168.0.100 billing billing.local.domain
192.168.0.101 client01 client01.local.domain
192.168.0.102 client02 client02.local.domain
192.168.0.103 client03 client03.local.domain
192.168.0.104 client04 client04.local.domain
192.168.0.105 client05 client05.local.domain
192.168.0.106 client06 client06.local.domain
192.168.0.107 client07 client07.local.domain
192.168.0.108 client08 client08.local.domain
192.168.0.109 client09 client09.local.domain
192.168.0.110 client10 client10.local.domain
```

- Buat file `/etc/samba/lmhosts` dan masukkan nama host computer client dan ip seperti diatas untuk pencarian dengan metode lmhosts file, contoh sebagai berikut :

```
192.168.0.1 router
192.168.0.100 billing
192.168.0.101 client01
192.168.0.102 client02
192.168.0.103 client03
192.168.0.104 client04
192.168.0.105 client05
192.168.0.106 client06
192.168.0.107 client07
192.168.0.108 client08
192.168.0.109 client09
192.168.0.110 client10
```

- Buka dan edit file `/etc/nsswitch.conf` cari baris...

```
hosts: files mdns4_minimal [NOTFOUND=return] dns mdns4
```

rubah menjadi...

```
hosts: files dns wins winbind mdns4_minimal [NOTFOUND=return] mdns4
```

- Lakukan restart jaringan dan winbind saja karena samba sudah otomatis berubah...  
`# /etc/init.d/networking restart`  
`# service winbind restart`
- Bila diperlukan untuk resolved NetBIOS / Computer Name, bisa dimasukkan ke dalam DNS Server (Bind9), sebagai DNS POISONING LCOAL.

Caranya, edit kembali misalnya file `/etc/bind/db.local.domain` dan tambahkan baris terakhir dengan memasukkan nama komputer client berserta ip-nya, contohnya...

```
router      IN      A      192.168.0.1
billing     IN      A      192.168.0.100
client01    IN      A      192.168.0.101
client02    IN      A      192.168.0.102
client03    IN      A      192.168.0.103
client04    IN      A      192.168.0.104
client05    IN      A      192.168.0.105
client06    IN      A      192.168.0.106
client07    IN      A      192.168.0.107
client08    IN      A      192.168.0.108
client09    IN      A      192.168.0.109
client10    IN      A      192.168.0.110
```

Maka file `/etc/bind/db.local.domain` tersebut menjadi (tulisan warna merah)...

```
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      ns.local.domain. mail.local.domain. (
                        2010072610      ;Serial
                        604800      ;Refresh
                        86400      ;Retry
                        2419200      ;Expire
                        604800 )      ;Negative Cache TTL
;
localhost      IN      A      127.0.0.1
@              IN      NS      ns.local.domain.
ns             IN      A      192.168.0.1
www           IN      CNAME    ns
proxy         IN      CNAME    ns
router        IN      A      192.168.0.1
billing       IN      A      192.168.0.100
client01      IN      A      192.168.0.101
client02      IN      A      192.168.0.102
client03      IN      A      192.168.0.103
client04      IN      A      192.168.0.104
client05      IN      A      192.168.0.105
client06      IN      A      192.168.0.106
client07      IN      A      192.168.0.107
client08      IN      A      192.168.0.108
client09      IN      A      192.168.0.109
client10      IN      A      192.168.0.110
```

Edit file `/etc/bind/db.192`, dan tambahkan baris terakhir dengan memasukkan nama komputer client diikuti nama domain sebagai DNS Suffix-nya berserta ip-nya, contohnya...

```
1      IN      PTR      router.local.domain.
100    IN      PTR      billing.local.domain.
101    IN      PTR      client01.local.domain.
102    IN      PTR      client02.local.domain.
103    IN      PTR      client03.local.domain.
104    IN      PTR      client04.local.domain.
105    IN      PTR      client05.local.domain.
106    IN      PTR      client06.local.domain.
107    IN      PTR      client07.local.domain.
108    IN      PTR      client08.local.domain.
109    IN      PTR      client09.local.domain.
110    IN      PTR      client10.local.domain.
```

Maka file `/etc/bind/db.192` tersebut menjadi (tulisan warna merah)...

```
;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA      ns.local.domain. mail.local.domain. (
                        2010072615      ;Serial
                        604800      ;Refresh
                        86400      ;Retry
                        2419200      ;Expire
                        604800 )      ;Negative Cache TTL
;
@         IN      NS      ns.
1         IN      PTR      ns.local.domain.
www       IN      CNAME    ns
proxy     IN      CNAME    ns
1         IN      PTR      router.local.domain.
100       IN      PTR      billing.local.domain.
101       IN      PTR      client01.local.domain.
102       IN      PTR      client02.local.domain.
103       IN      PTR      client03.local.domain.
104       IN      PTR      client04.local.domain.
105       IN      PTR      client05.local.domain.
106       IN      PTR      client06.local.domain.
107       IN      PTR      client07.local.domain.
108       IN      PTR      client08.local.domain.
109       IN      PTR      client09.local.domain.
110       IN      PTR      client10.local.domain.
```

Kemudian Bind9 di restart  
`# service bind9 restart`



- Testing Samba...  
# smbclient -L localhost -U%

hasilnya...

Domain=[PERSEGI] OS=[Unix] Server=[Samba 3.3.2]

Sharename	Type	Comment
-----	----	-----
IPC\$	IPC	IPC Service (persegi server (Samba, Ubuntu))

Domain=[DNS.PERSEGI.NET] OS=[Unix] Server=[Samba 3.3.2]

Server	Comment
-----	-----
BILLING	
CLIENT01	
CLIENT02	
CLIENT03	
CLIENT04	
CLIENT05	
CLIENT06	
CLIENT07	
CLIENT08	
CLIENT09	
CLIENT10	
ROUTER	router server (Samba, Ubuntu)

Workgroup	Master
-----	-----
WORKGROUP	ROUTER

- Buat Bash Script agar tiap interval 15menit akan mem-restart daemon winbindd, snmb dan nmbd.  
buat file /sbin/wins dengan script sebagai berikut...

```
#!/bin/sh
# Script ini untuk memrestart Winbindd dan Samba (snmb & nmbd)
# agar semua NetBIOS komputer client dapat di refresh.

PATH=/sbin:/bin:/usr/sbin:/usr/bin

[ -r /etc/default/winbind ] && . /etc/default/winbind
[ -r /etc/default/samba ] && . /etc/default/samba

RUN_MODE="daemons"

DAEMON_WINBINDD=/usr/sbin/winbindd
PIDDIR_WINBINDD=/var/run/samba
WINBINDPID=$PIDDIR_WINBINDD/winbindd.pid

PIDDIR_SAMBA=/var/run/samba
NMBDPID=$PIDDIR_SAMBA/nmbd.pid
SMBDPID=$PIDDIR_SAMBA/smbd.pid

INTERVAL=900

unset TMPDIR

test -x $DAEMON_WINBINDD || exit 0
test -x /usr/sbin/nmbd -a -x /usr/sbin/smbd || exit 0

. /lib/lsb/init-functions

while : ; do
    #
    # winbind stop
    #
    log_daemon_msg "Stopping the Winbind daemon" "winbind"
    start-stop-daemon --stop --quiet --oknodo --exec $DAEMON_WINBINDD
    log_end_msg $?
    sleep 2

    #
    # samba stop
    #
    log_daemon_msg "Stopping Samba daemons"
    log_progress_msg "nmbd"

    start-stop-daemon --stop --quiet --pidfile $NMBDPID

    sleep 1
    if [ -f $NMBDPID ] && ! ps h `cat $NMBDPID` > /dev/null
    then
        rm -f $NMBDPID
    fi

    if [ "$RUN_MODE" != "inetd" ]; then
        log_progress_msg "smbd"
        start-stop-daemon --stop --quiet --pidfile $SMBDPID

        sleep 1
        if [ -f $SMBDPID ] && ! ps h `cat $SMBDPID` > /dev/null
        then
            rm -f $SMBDPID
        fi
    fi

    log_end_msg 0
```

```

sleep 2

#
# samba start
#
log_daemon_msg "Starting Samba daemons"
install -o root -g root -m 755 -d $PIDDIR_SAMBA

NMBD_DISABLED=`testparm -s --parameter-name='disable netbios' 2>/dev/null`
if [ "$NMBD_DISABLED" != 'Yes' ]; then
    log_progress_msg "nmbd"
    if ! start-stop-daemon --start --quiet --oknodo --exec
/usr/sbin/nmbd -- -D
    then
        log_end_msg 1
        exit 1
    fi
fi

if [ "$RUN_MODE" != "inetd" ]; then
    log_progress_msg "smbd"
    if ! start-stop-daemon --start --quiet --oknodo --exec
/usr/sbin/smbd -- -D; then
        log_end_msg 1
        exit 1
    fi
fi

log_end_msg 0
sleep 2

#
# winbind start
#
log_daemon_msg "Starting the Winbind daemon" "winbind"
mkdir -p /var/run/samba/winbindd_privileged || return 1
chgrp winbindd_priv $PIDDIR_WINBINDD/winbindd_privileged/ || return 1
chmod 0750 $PIDDIR_WINBINDD/winbindd_privileged/ || return 1
start-stop-daemon --start --quiet --oknodo --exec $DAEMON_WINBINDD --
$WINBINDD_OPTS
log_end_msg $?

#
# Repeat
#
sleep $INTERVAL

done

```

kemudian beri attribute agar bisa dijalankan,  
kemudian jalankan dengan mengirim Signal HUP agar berjalan terus menurun setiap nilai interval yang ditentukan.

```

# chmod +x /sbin/wins
# nohup /sbin/wins &

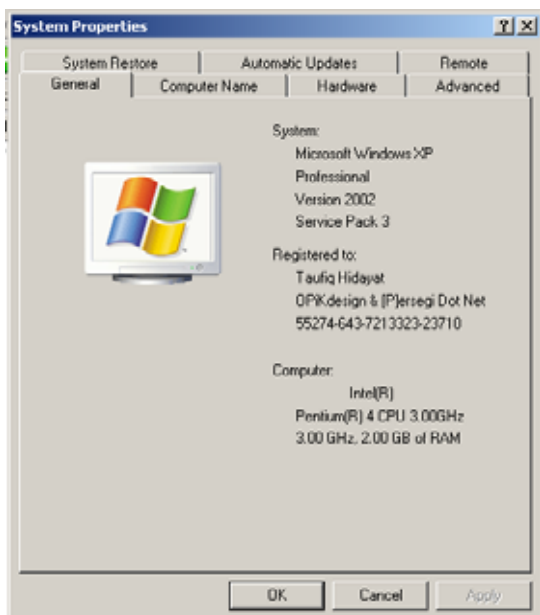
```

Terakhir agar script ini berjalan saat server pertama kali restart/booting, masukkan ke dalam [/etc/rc.local](#), edit file [/etc/rc.local](#) kemudian tambahkan...

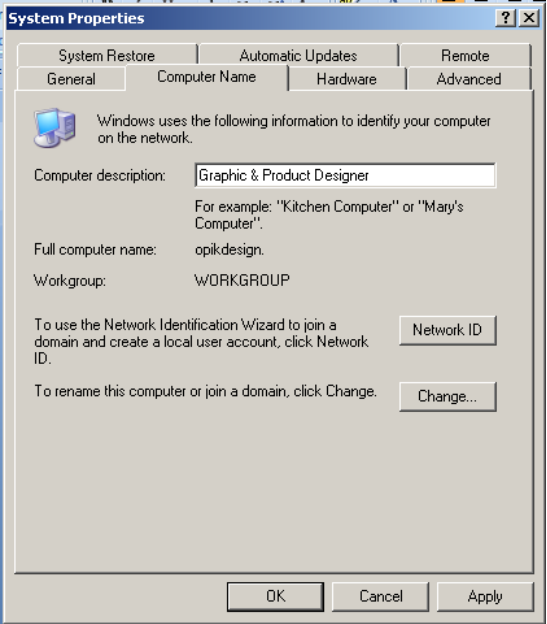
```
nohup /sbin/wins &
```

- Setting DNS Suffix di tiap client klo tadi sudah membuat DNS Server untuk client, caranya :

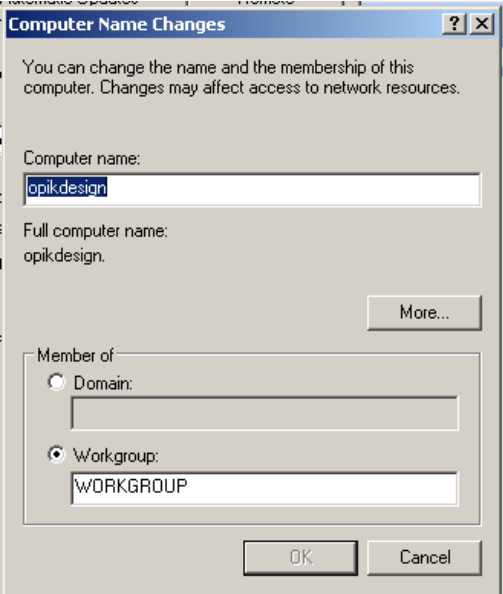
Control Panel >> System



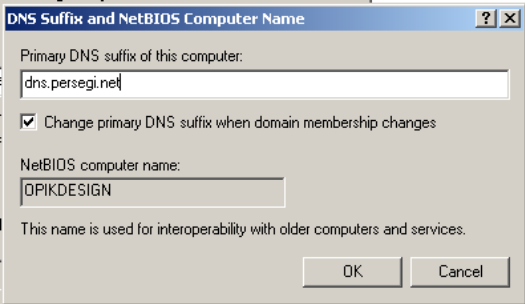
Pilih / click Computer Name, boleh isi Computer Desciption semisal **“client01”**



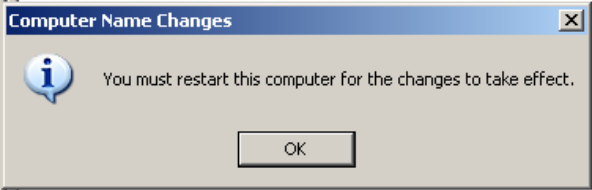
Click Change dan isi Computer name sesuai yang didaftarkan semisal **“client01”**



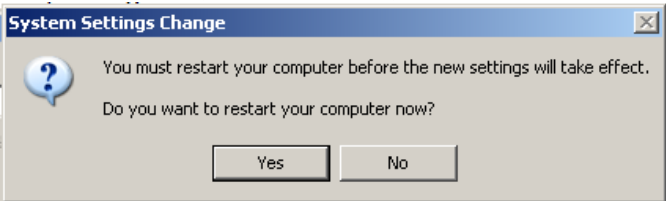
Click More... isi Primary DNS Suffix computer tersebut semisalnya **“local.domain”** dan beri tanda centang pada **“Change primary DNS suffix when domain membership changes”**



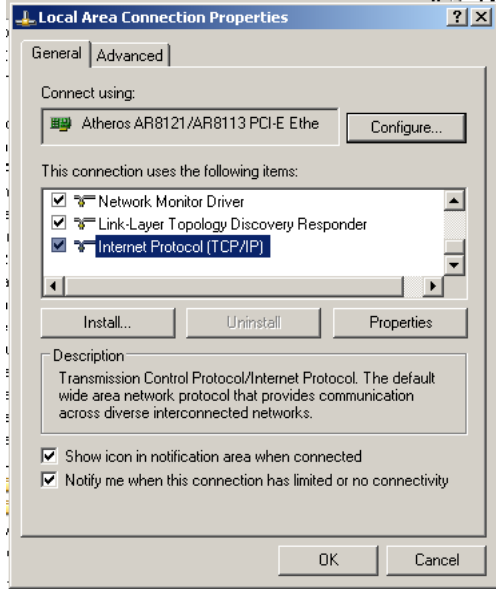
Click OK dan OK lagi



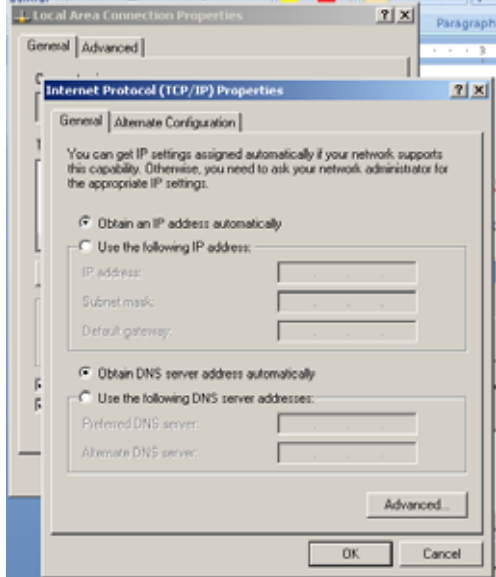
Click OK dan OK lagi. Kemudian computer di restart...



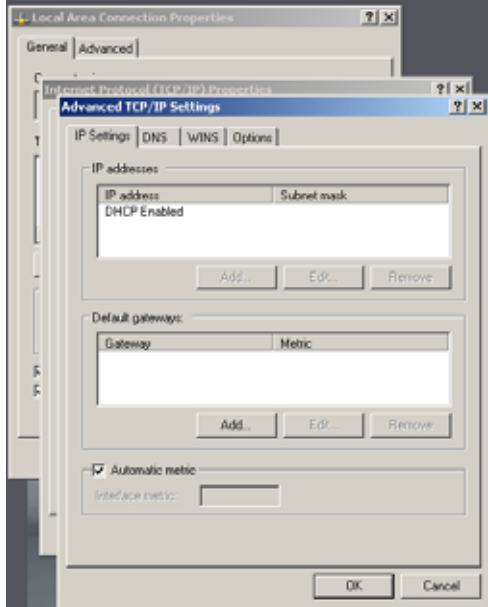
- Terakhir, setting tiap client agar NetBIOS selalu dilewatkan TCP/IP, caranya :  
Control Panel >> Network Connection >> Click Kanan Local Area Connection >> Pilih Properties



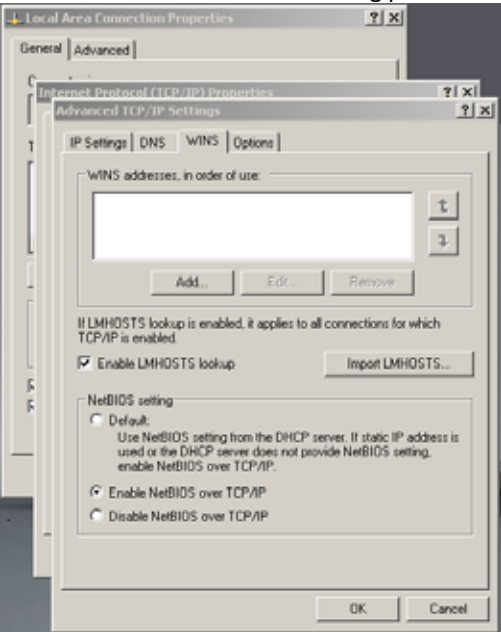
Cari Internet Protocol (TCP/IP) dan pilih kemudian click Properties.



Pilih Advanced.



Pilih Tab WINS dan NetBIOS setting pilih ke “Enable NetBIOS over TCP/IP. Click “OK” 3x..



- Untuk melakukan scanning NetBIOS dalam jaringan, install repository `nbtscan`  
`# apt-get install nbtscan`

Cara menggunakannya, kita scan di jaringan 192.168.0.0/24  
`# nbtscan 192.168.0.0/24`

## TAHAP XII

### MEMBUAT FOLDER SHARING

### UNTUK WINDOWS OS DENGAN SAMBA

- Saat install Ubuntu, sudah ditentukan sisa harddisk untuk folder `/home/share` sekitar 33Gbyte, maka buat folder lagi dan beri permission sepenuhnya...

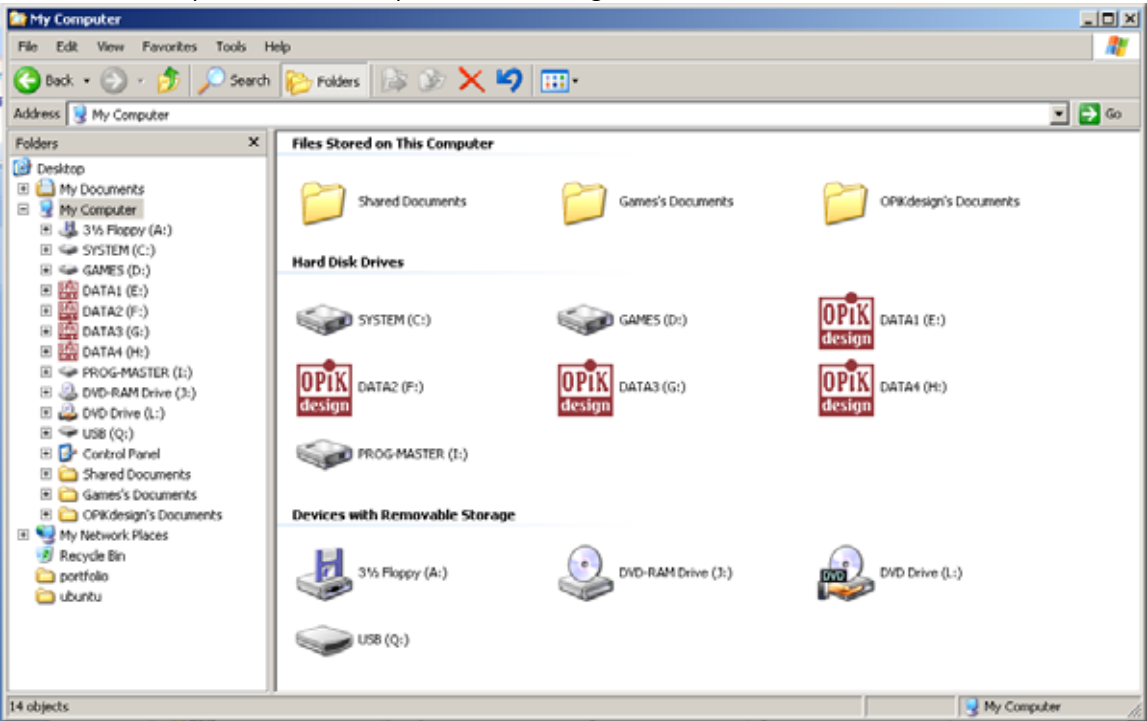
```
# mkdir /home/share/doc
# chmod 0777 -R /home/share/doc
```

- Buka dan edit kembali file configuration samba, `/etc/samba/smb.conf` dan tambahkan pada baris terakhir sebagai berikut:

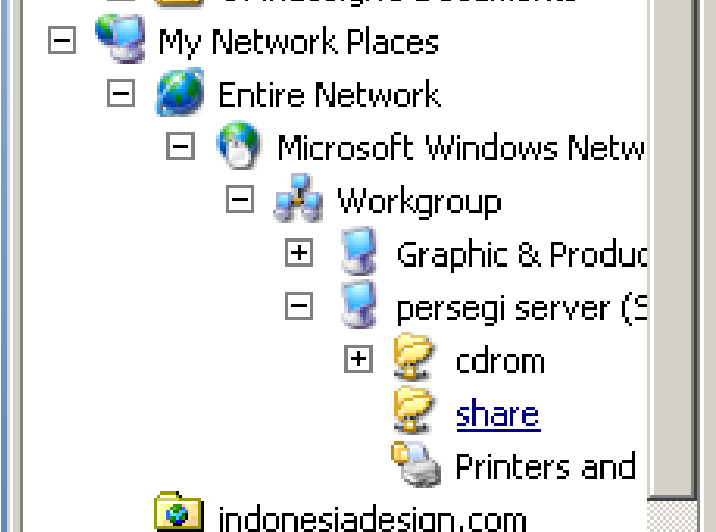
```
[Share]
comment = File Server Share
path = /home/share/doc
read only = No
create mask = 0777
directory mask = 0777
```

- Untuk sisi client bisa dilakukan **Map Network Drive** dan dijadikan sebagai My Document agar para client bisa langsung melakukan save document di My Document (Default-nya), cara-carany sebagai berikut...

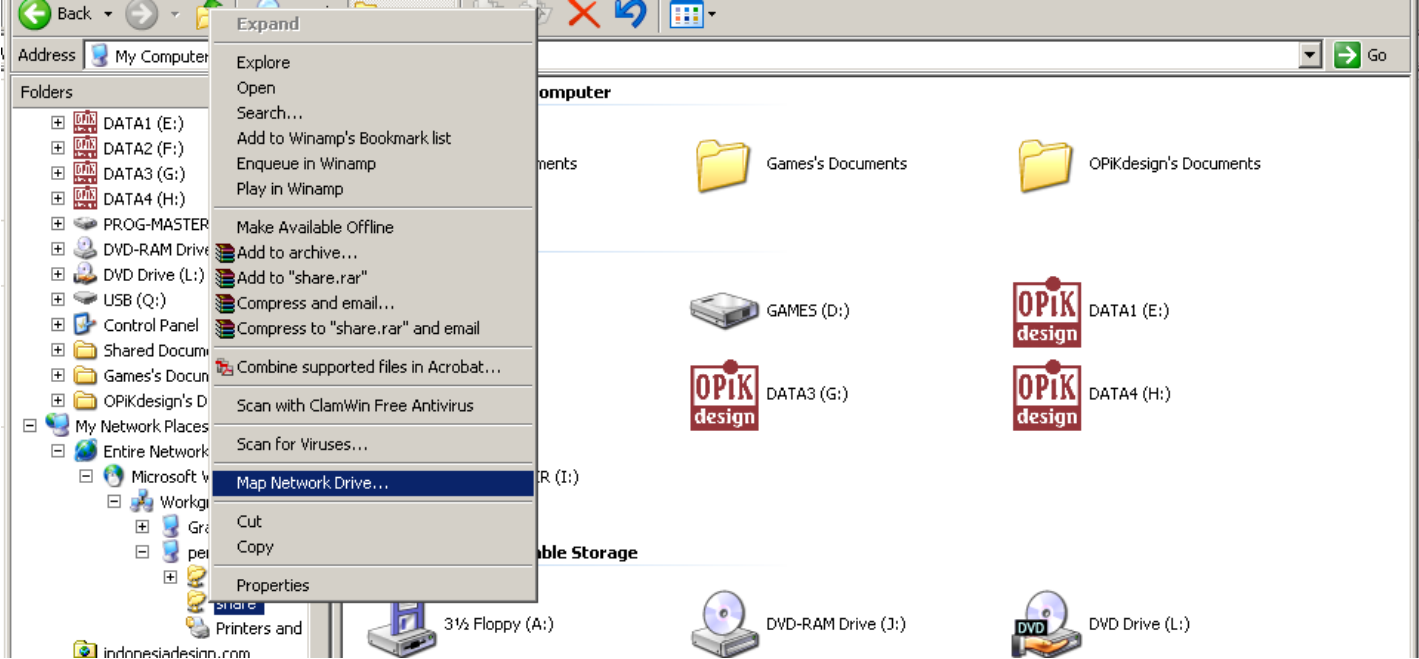
Buka Windows Explorer... Tombol cepat bisa tekan “Logo Windows + E”



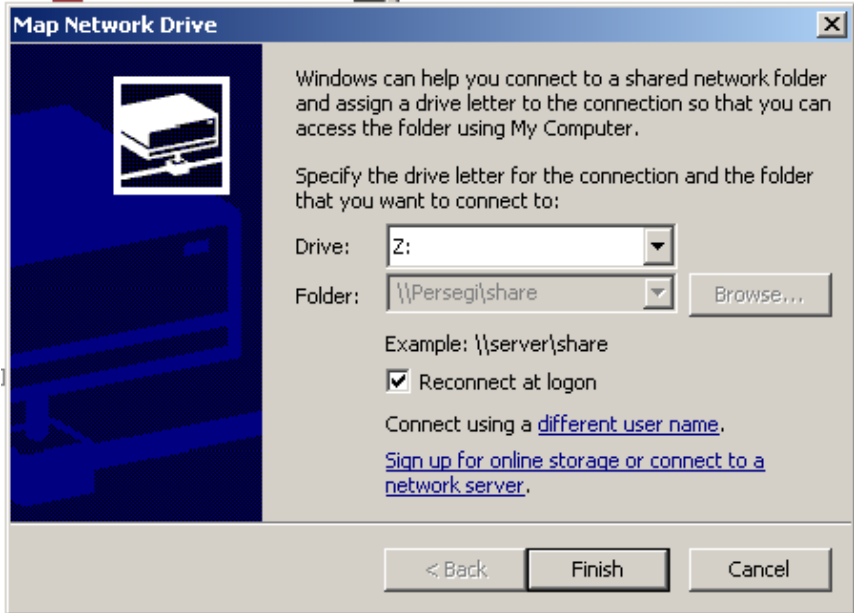
Kemudian Click Tanda “+”, My Network Places >> Microsoft Windows Network >> Workgroup >> (Nama Server)



Click kanan “Share” dan pilih “Map Network Drive...”

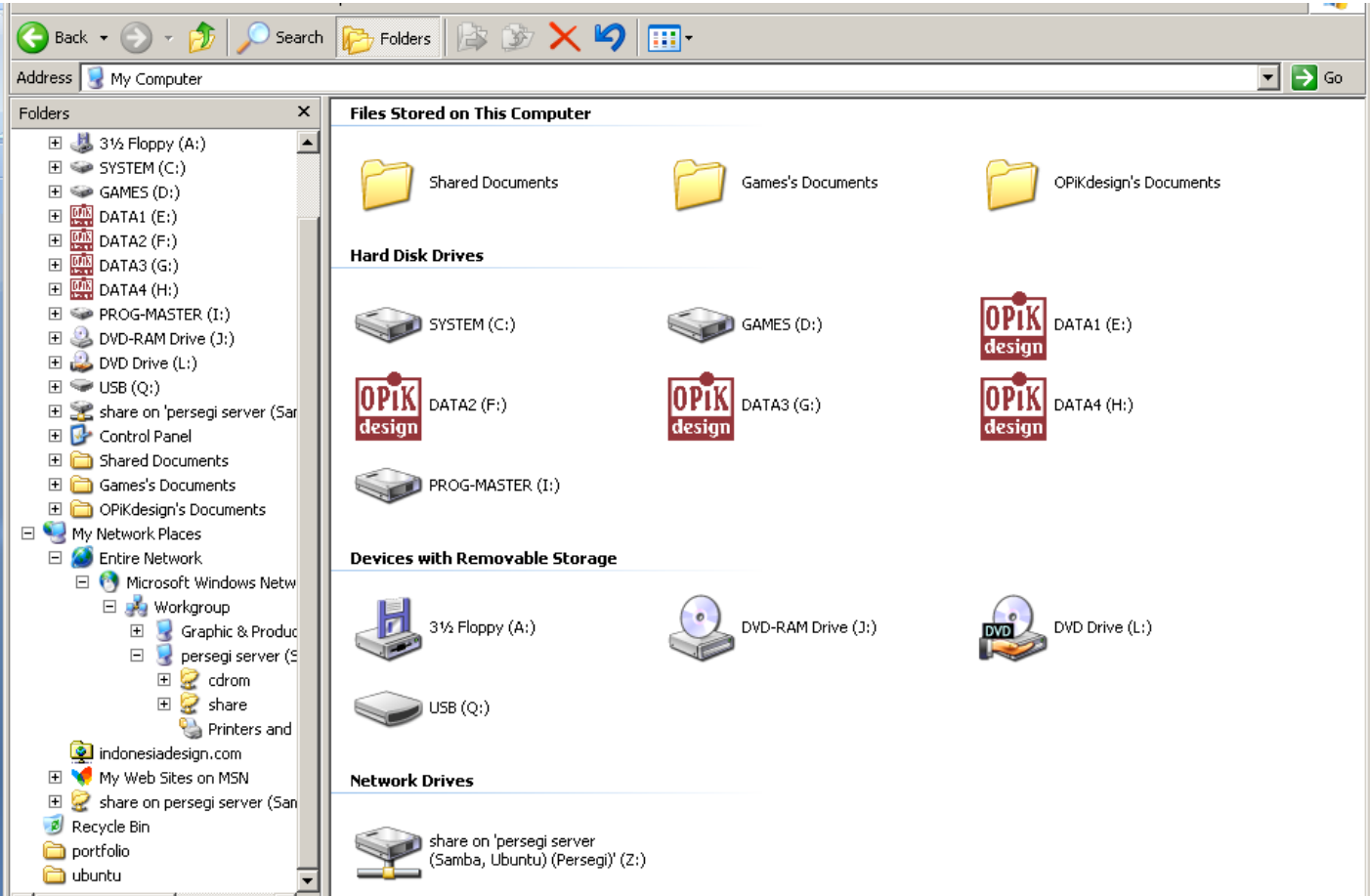


Akan muncul Windows Dialog, dan pastikan memberi tanda centang pada “Reconnect at logon” agar tiap kali computer client selalu menghubungkan diri dengan **Share Document** di server



Terbentuklah drive baru dengan initial Z:\

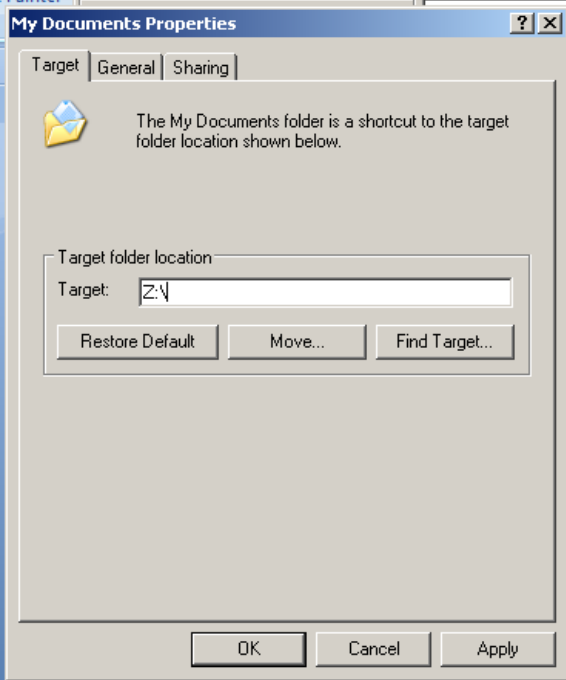
Kembali lagi pada Windows Explorer sebelumnya atau menuju My Computer...  
Terlihat ada drive ber-type “Network Drives”



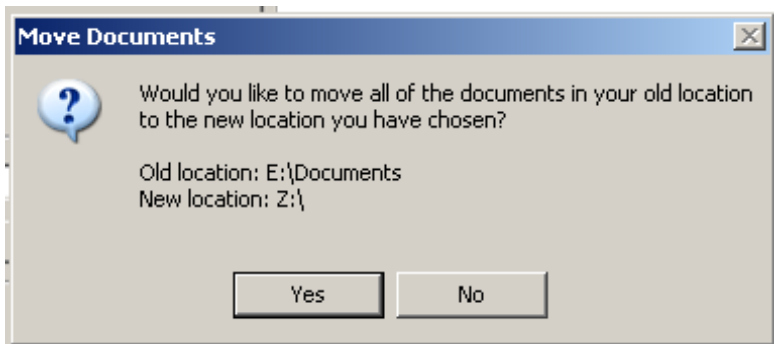
Agar menjadi My Document, Click Kanan *My Document* sisi kiri dan pilih



Rubah targetnya menuju **Z:\** dimana **Network Drive** berada.



Terakhir akan muncul seperti dibawah ini, dan pilih “No” agar data-data yang berada di My Document sebelum tidak berpindah.



Nah, sekarang My Document di computer client sudah berpindah menuju ke Share Document di Server, jadi mereka akan melakukan save secara default di server.

- Diatas merupakan salah satu contoh atau cara membuak folder samba, untuk lebih bagusnya agar lebih mudah mengatur management sebaik tiap satu dibuat satu folder sharing sendiri dan di map sesuai folder sharing, jadi My Document Client tidak sama tiap unit client-nya.

## TAHAP XIII

### CLAMAV

### ANTI VIRUS UNTUK FILE SAMBA DAN

### BUAT SCHEDULE CRONTAB UNTUK

### SCANING MAUPUN UPDATE

Pada dasarnya OS yang berbasis Linux/Unix saat ini tidak ada virus. Namun dengan adanya Folder Sharing yang dibuat dengan Samba, tidak menutup kemungkinan didalam Folder tersebut terjangkit virus dari OS Windows, perlu diingat bahwa virus ini tidak bakalan menyerang server tetapi akan mengganggu kinerja jaringan kita bila dibiarkan.

- Install Clamav

```
# apt-get install clamav clamav-daemon clamav-docs clamav-testfiles clamav-freshclam clamav-base
```

- Agar database virus-nya update terbaru...

```
# freshclam
```

- Kemudian buat jadwal agar tiap hari selalu update dan melakukan scanning...

```
# crontab -e
```

Baris terakhir tambahkan...

```
* * */1 * * /usr/bin/freshclam
@daily /usr/bin/clamscan -r --remove --quiet /home/share/doc
```

keluar dan save.

## TAHAP XIV

### INSTALL SAMPAI SETTING

### SQUID PROXY DAN HAVP

### SEBAGAI ANTIVIRUS WEB-BROWSING

### BAIK UNTUK PORT HTTP MAUPUN PROXY

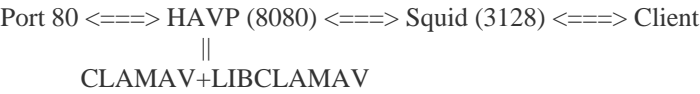
- Dari internet banyak bibit penyakit semacam virus, trojan maupun lainnya. Kita inginkan bagaimana caranya gateway kita bisa memfilter bibit-bibit penyakit ini. Jadi semua paket data dari internet khususnya dari port HTTP (80) akan di scan habis oleh program tersebut, nama program tersebut adalah HAVP yang merupakan repository dari <http://www.server-side.de/> .

HAVP ini tidak bekerja sendiri, dia hanya memeriksa data masuk aja dan anti virus-nya sebagai acuan bisa ClamAV atau AVG, disini saya menggunkan ClamAV dan LibClamAV. Dan disini saya sengaja memadukan dgn Squid agar yang di cache bener2 bersih dari penyakit.

HAVP berkerja menggunakan Port 8080 yang kemudian akan diteruskan ke port PROXY (3128), kurang lebih seperti topology



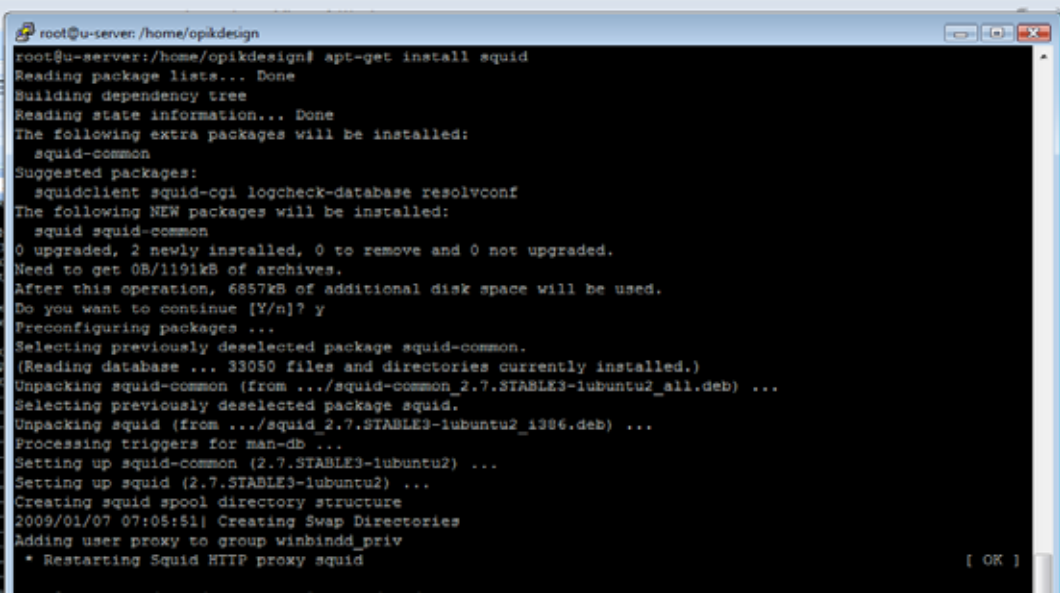
sebagai berikut...



- Proxy, bisa berfungsi sebagai firewall/site block, web cache bahkan bisa sedikit mengatur bandwidth. Fungsi ini ada yang memandang tidak perlu, tetapi bagi penulis Squid memegang peranan penting karena bisa diunggulkan semisal memblock packet yang tidak diinginkan dan membantu mengatur bandwidth karena adanya web-cache yang bisa diandalkan pada saat koneksi dari ISP bermasalah maupun bisa membatasi file yang di download oleh client.
- Install HAVP dan SQUID

```
# apt-get install havp squid squid-common squid-cgi squidclient
```

Kurang lebih hasilnya seperti ini...



- Kemudian edit file konfigurasi squid proxy di `/etc/squid/squid.conf`

```
#=====
# Proxy Server Versi 2.7.Stable3
#=====

#####
# Port
#####
http_port 3128 transparent
icp_port 3130
prefer_direct off

#####
# Cache & Object
#####
cache_mem 8 MB
cache_swap_low 98
cache_swap_high 99
max_filedesc 8192
maximum_object_size 1024 MB
minimum_object_size 0 KB
maximum_object_size_in_memory 4 bytes
ipcache_size 4096
ipcache_low 98
ipcache_high 99
fqdn_cache_size 4096

cache_replacement_policy heap LFUDA
memory_replacement_policy heap GDSF

#####
# cache_dir <type> <Directory-Name> <Space in Mbytes> <Level1> <Level2> <options>
# Maksimum Level1=((Space in byte/13)/Level2/Level2)*2

cache_dir aufs /home/proxy1 15000 32 256
cache_dir aufs /home/proxy2 15000 32 256
cache_dir aufs /home/proxy3 15000 32 256

#####

cache_access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log
cache_store_log none
pid_filename /var/run/squid.pid
cache_swap_log /var/log/squid/swap.state

dns_nameservers 127.0.0.1

emulate_httpd_log off
hosts_file /etc/hosts
half_closed_clients off
negative_ttl 1 minutes
```

```
#####
# Rules: Safe Port
#####

acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255
acl to_localhost dst 127.0.0.0/8

acl SSL_ports port 443 563 873
acl Safe_ports port 80
acl Safe_ports port 20 21
acl Safe_ports port 70
acl Safe_ports port 210
acl Safe_ports port 1025-65535
acl Safe_ports port 631
acl Safe_ports port 10000
acl Safe_ports port 901
acl Safe_ports port 280
acl Safe_ports port 488
acl Safe_ports port 591
acl Safe_ports port 777
acl Safe_ports port 873
acl Safe_ports port 110
acl Safe_ports port 25
acl Safe_ports port 2095 2096
acl Safe_ports port 2082 2083

acl purge method PURGE
acl CONNECT method CONNECT

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

#####
# Refresh Pattern
#####

refresh_pattern ^ftp: 1440 20% 10080
refresh_pattern ^gopher: 1440 0% 1440

refresh_pattern -i \.(gif|png|jpg|jpeg|ico)$ 10080 90% 43200 override-expire ignore-no-cache ignore-private
refresh_pattern -i \.(iso|avi|wav|mp3|mp4|mpeg|mpg|swf|flv|x-flv)$ 43200 90% 432000 override-expire ignore-no-cache ignore-private
refresh_pattern -i \.(deb|rpm|exe|ram|bin|pdf|ppt|doc|tiff)$ 10080 90% 43200 override-expire ignore-no-cache ignore-private
refresh_pattern -i \.(zip|gz|arj|lha|lzh|tar|tgz|cab|rar)$ 10080 95% 43200 override-expire ignore-no-cache ignore-private
refresh_pattern -i \.(html|htm|css|js|php|asp|aspx|cgi) 1440 40% 40320

refresh_pattern . 0 20% 4320

#####
# HAVP + Clamav
#####

cache_peer 127.0.0.1 parent 8080 0 no-query no-digest no-netdb-exchange default

#####
# HIERARCHY (BYPASS CGI)
#####

#hierarchy_stoplist cgi-bin ? .js .jsp
#acl QUERY urlpath_regex cgi-bin \? .js .jsp
#no_cache deny QUERY

#####
# Pembatasan B/W Download dgn mendeteksi extention file.
# dan pembatasan access domain
#
#####

acl client src 192.168.0.101 192.168.0.102 192.168.0.103 192.168.0.104 192.168.0.105 192.168.0.106
192.168.0.107 192.168.0.108 192.168.0.109 192.168.0.110
acl billing src 192.168.0.200
acl server src 192.168.0.1

acl download url_regex -i ftp \.exe$ \.mp3$ \.mp4$ \.tar.gz$ \.gz$ \.tar.bz2$ \.rpm$ \.zip$ \.rar$ \.7z$ \.avi$
\.mpg$ \.mpeg$ \.rm$ \.iso$ \.wav$ \.mov$ \.dat$ \.mpe$ \.mid$
acl download url_regex -i \.midi$ \.rmi$ \.wma$ \.wmv$ \.ogg$ \.ogm$ \.mlv$ \.mp2$ \.mpa$ \.wax$ \.m3u$ \.asx$
\.wpl$ \.wmx$ \.dvr-ms$ \.snd$ \.au$ \.aif$ \.asf$ \.m2v$
acl download url_regex -i \.m2p$ \.ts$ \.tp$ \.trp$ \.div$ \.divx$ \.mod$ \.vob$ \.aob$ \.dts$ \.ac3$ \.cda$
\.vro$ \.deb$ \.pdf$ \.com$ \.nrg$ \.vcd$ \.flv$ \.swf$ \.3gp$

delay_pools 2

delay_class 1 1
delay_parameters 1 40000/10000000 15000/40000000 10000/70000000
delay_access 1 allow download client
delay_access 1 deny all

delay_class 2 1
delay_parameters 2 -1/-1
delay_access 2 allow download billing
```

```
delay_access 2 allow download server
delay_access 2 deny all

#####
# SNMP
#####

snmp_port 3401
acl snmpsquid snmp_community public
snmp_access allow snmpsquid localhost
snmp_access deny all

#####
# ALLOWED ACCESS
#####

acl modem url_regex 192.168.1. 192.168.2.

http_access allow !modem client
http_access allow billing
http_access allow localhost
http_access deny all

http_reply_access allow all
icp_access allow dl
icp_access allow localhost
icp_access deny all
always_direct deny all

#####
# Cache CGI & Administrative
#####

cache_mgr th@opikdesign.com
cachemgr_passwd 123 all
visible_hostname local.domain
cache_effective_user proxy
cache_effective_group proxy
coredump_dir /var/spool/squid
shutdown_lifetime 10 seconds
logfile_rotate 14
```

- Matikan squid

```
# service squid stop
```

- Memberikan permission pada folder cache

```
# chown -R proxy.proxy /home/proxy1
# chown -R proxy.proxy /home/proxy2
# chown -R proxy.proxy /home/proxy3
```

- Membuat folder-folder swap/cache di dalam folder cache yang telah ditentukan

```
# squid -f /etc/squid/squid.conf -z
```

- Start squid.

```
# service squid start
```

- Buat rule iptables agar port HTTP (80) dari client dibelokkan ke port Proxy (3128).

```
# iptables -t nat -I PREROUTING -i eth0 -p tcp -m tcp --dport 80 -j REDIRECT --to-ports 3128
# iptables -t nat -I PREROUTING -i eth0 -p udp -m udp --dport 80 -j REDIRECT --to-ports 3128
```

- Untuk menguji PROXY dan HAVP, di client download/buka IE ato Mozilla buka URL.

***http://www.eicar.org/download/eicarcom2.zip***, klo memang sudah jalan normal, akan muncul **"Access to the page has been denied because the following virus was detected. ClamAV: Eicar-Test-Signature"** dengan background merah.

# TAHAP XV

## INSTALL SARG DAN CALAMARIS

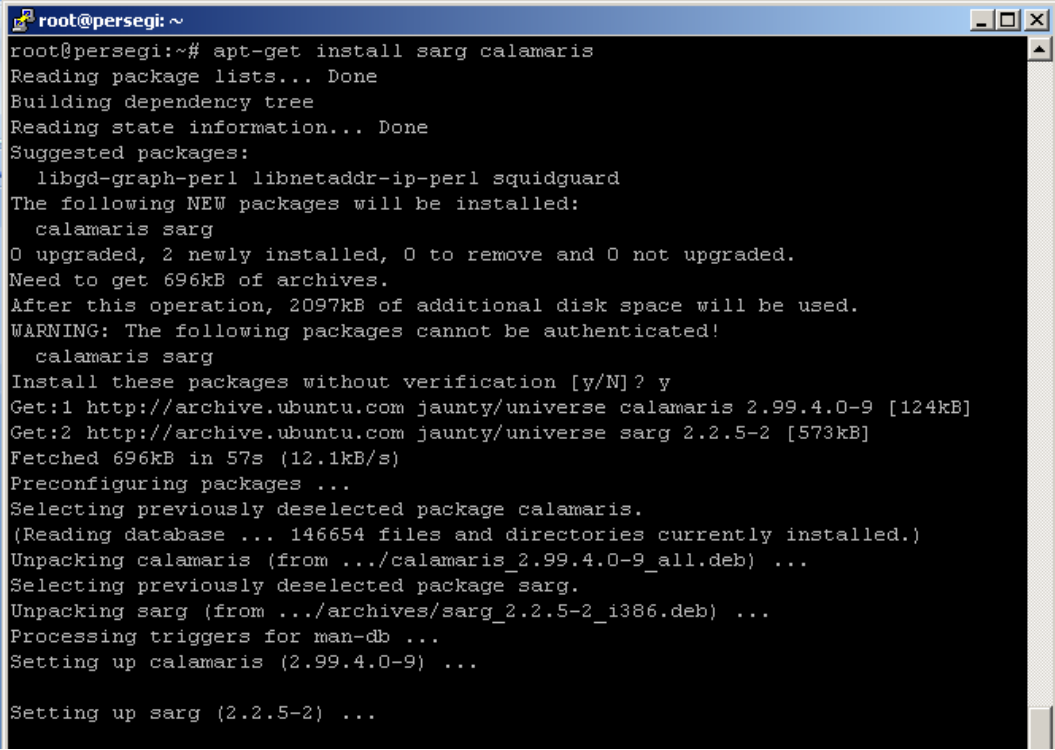
### UNTUK MEMONITOR SQUID PROXY

### SELAIN MENGGUNAKAN SQUID-CGI

- Fungsi CALAMARIS di squid adalah mempermudah kita untuk melihat statistic kinerja squid proxy.
- Fungsi SARG adalah mempermudah kita untuk melihat client mengakses kemana saja, yang sebenarnya sudah di catat di log [/var/log/squid/access.log](#) namun sulit dibaca karena kurang manusiawi, dengan SARG tampilan Web-GUI membuat mudah dibaca.
- Install SARG dan CALAMARIS

```
# apt-get install sarg calamaris libgd-graph-perl libnetaddr-ip-perl ttf-dustin
```

hasil...



- Setting CALAMARIS  
# squid -k rotate  
# mkdir /var/www/calamaris  
# calamaris -a -F html /var/log/squid/access.log > /var/www/calamaris/index.html
- Setting SARG

edit file `/etc/sarg/sarg-reports.conf`; rubah seperti dibawah ini (teks warna merah)...

```
SARG=/usr/bin/sarg
CONFIG=/etc/sarg/sarg.conf
HTMLOUT=/var/www/squid-reports
PAGETITLE="Access Reports on $(hostname)"
LOGOIMG=/sarg/images/sarg.png
LOGOLINK="http://$(hostname)/"
DAILY=Daily
WEEKLY=Weekly
MONTHLY=Monthly
EXCLUDELOG1="SARG: No records found"
EXCLUDELOG2="SARG: End"
```

dan edit file `/etc/sarg/sarg.conf`; cari baris...

```
output_dir /var/lib/sarg
```

dirubah menjadi...

```
output_dir /var/www/squid-reports
```

agar IP dirubah menjadi nama host maka cari baris

```
/etc/sarg/usertab
```

dirubah menjadi...

```
usertab /etc/hosts
```

Kemudian buat folder dan buat report

```
# mkdir /var/www/squid-reports

# sarg-reports today
# sarg-reports daily
# sarg-reports weekly
# sarg-reports monthly
```

- Memasukkan pada Crontab, pada dasarnya SARG sudah ada penjadwalan namun saya masukkan lagi agar lebih sering refresh. Jalankan crontab

```
# crontab -e
```

Kemudian tambahkan di baris terakhir...

```
* */6 * * * /usr/sbin/sarg-reports today
* */12 * * * calamaris -a -F html /var/log/squid/access.log > /var/www/calamaris/index.html
```

- Cara melihat report dari CALAMARIS... browsing ke URL `http://[ip-server]/calamaris....`

Proxy Report (28.Jul 09 08:00:13 - 28.Jul 09 19:26:59) - Windows Internet Explorer

http://192.168.0.1/calamaris/

File Edit View Favorites Tools Help

Favorites Proxy Report (28.Jul 09 08:00:13 - 28.Jul 09 19:26:59)

# Proxy Report

Report period: 28.Jul 09 08:00:13 - 28.Jul 09 19:26:59

Generated at: 28.Jul 09 21:59:06

Table of Content / Overview			
<a href="#">Summary</a>	-	-	-
<a href="#">Incoming requests by method</a>	most requested method	GET	23876 Requests
<a href="#">Incoming UDP-requests by status</a>	-	-	no requests found
<a href="#">Incoming TCP-requests by status</a>	most incoming request by status to	MISS	21994 Requests
<a href="#">Outgoing requests by status</a>	most outgoing request to	DIRECT Fetch from Source	17861 Requests
<a href="#">Outgoing requests by destination</a>	most requested destination	DIRECT	17861 Requests
<a href="#">Request-destinations by 2nd-level-domain</a>	most requested 2nd-level-domain	*.adbasket.net	6755 Requests
<a href="#">Request-destinations by toplevel-domain</a>	most requested toplevel-domain	*.com	14516 Requests
<a href="#">TCP-Request-protocol</a>	most requested protocol	http:	24879 Requests
<a href="#">Requested content-type</a>	most requested content-type	image/gif	5901 Requests
<a href="#">Requested extensions</a>	most requested extension	<dynamic>	16886 Requests
<a href="#">Incoming UDP-requests by host</a>	-	-	no requests found
<a href="#">Incoming TCP-requests by host</a>	most active host	sendy-designer3	6730 Requests
<a href="#">Size Distribution Diagram</a>	most requested object_size	1000-9999	13106 Requests
<a href="#">Performance in 1 hour steps</a>	most active day	28.Jul 09 09:00	5764 Requests
<a href="#">UDP-Request duration distribution in msec</a>	-	-	no requests found
<a href="#">TCP-Request duration distribution in msec</a>	most frequent response time	<= 1000	8087 Requests

Done


- Cara melihat report dari SARG... browsing ke URL `http://[ip-server]/squid-reports....`

Access Reports on medium - Windows Internet Explorer

http://192.168.0.1/squid-reports/

Edit View Favorites Tools Help

avorites Proxy Report (28.Jul 09 08:00:13 - 28.Jul 09 19:26:59) Access Reports on medium X



## Access Reports on medium

[Daily](#)

[Weekly](#)

[Monthly](#)

Windows Internet Explorer window showing the Squid Analysis Report Generator interface. The browser address bar displays 'http://192.168.0.1/squid-reports/Daily/'. The page title is 'Squid Analysis Report Generator'. The main content area displays 'Squid User Access Reports' and a table with columns: FILE/PERIOD, CREATION DATE, USERS, BYTES, and AVERAGE. The table lists various report files and their corresponding statistics.

FILE/PERIOD	CREATION DATE	USERS	BYTES	AVERAGE
2009Jul29-2009Jul29	Wed Jul 29 00:03:01 WIT 2009	1	594.71K	594.71K
2009Jul28-2009Jul28	Tue Jul 28 23:59:01 WIT 2009	1	133.16K	133.16K
2009Jul27-2009Jul27	Mon Jul 27 23:59:07 WIT 2009	28	1.34G	44.33M
2009Jul26-2009Jul26	Sun Jul 26 23:59:02 WIT 2009	1	18.08M	18.08M
2009Jul25-2009Jul25	Sat Jul 25 23:59:02 WIT 2009	9	68.96M	7.66M
2009Jul24-2009Jul24	Fri Jul 24 23:59:09 WIT 2009	28	655.53M	30.55M
2009Jul23-2009Jul23	Thu Jul 23 23:59:07 WIT 2009	28	894.63M	31.95M
2009Jul22-2009Jul22	Wed Jul 22 23:59:11 WIT 2009	29	809.59M	27.91M
2009Jul21-2009Jul21	Tue Jul 21 23:59:07 WIT 2009	30	964.21M	32.14M
2009Jul20-2009Jul20	Mon Jul 20 23:59:01 WIT 2009	1	17.09M	17.09M
2009Jul19-2009Jul19	Sun Jul 19 23:59:02 WIT 2009	1	27.19M	27.19M
2009Jul18-2009Jul18	Sat Jul 18 23:59:02 WIT 2009	4	48.59M	11.39M
2009Jul17-2009Jul17	Fri Jul 17 23:59:07 WIT 2009	27	978.30M	36.27M
2009Jul16-2009Jul16	Thu Jul 16 23:59:08 WIT 2009	26	629.89M	23.84M
2009Jul15-2009Jul15	Wed Jul 15 23:59:07 WIT 2009	28	420.33M	15.01M
2009Jul14-2009Jul14	Tue Jul 14 23:59:08 WIT 2009	28	940.55M	33.59M
2009Jul13-2009Jul13	Mon Jul 13 23:59:09 WIT 2009	28	473.33M	16.90M
2009Jul12-2009Jul12	Sun Jul 12 23:59:01 WIT 2009	1	932.31K	932.31K
2009Jul11-2009Jul11	Sat Jul 11 23:59:03 WIT 2009	22	99.44M	4.52M
2009Jul10-2009Jul10	Fri Jul 10 23:59:09 WIT 2009	27	576.47M	21.35M
2009Jul09-2009Jul09	Thu Jul 9 23:59:07 WIT 2009	24	471.75M	19.65M
2009Jul08-2009Jul08	Wed Jul 8 23:59:01 WIT 2009	2	16.67M	8.33M
2009Jul07-2009Jul07	Tue Jul 7 23:59:10 WIT 2009	28	878.92M	31.39M
2009Jul06-2009Jul06	Mon Jul 6 23:59:08 WIT 2009	24	874.74M	36.44M
2009Jul04-2009Jul04	Sat Jul 4 23:59:02 WIT 2009	5	24.24M	4.84M
2009Jul03-2009Jul03	Fri Jul 3 23:59:08 WIT 2009	27	964.64M	35.46M
2009Jul02-2009Jul02	Thu Jul 2 23:59:08 WIT 2009	27	658.43M	24.38M
2009Jul01-2009Jul01	Wed Jul 1 23:59:08 WIT 2009	28	814.39M	29.08M
2009Jun30-2009Jun30	Tue Jun 30 23:59:10 WIT 2009	27	1.11G	41.26M
2009Jun29-2009Jun29	Mon Jun 29 23:59:07 WIT 2009	24	971.17M	40.48M
2009Jun28-2009Jun28	Sun Jun 28 23:59:09 WIT 2009	27	773.16M	28.63M
2009Jun25-2009Jun25	Thu Jun 25 23:59:07 WIT 2009	27	730.30M	27.04M

Windows Internet Explorer window showing the Squid Analysis Report Generator interface. The browser address bar displays 'http://192.168.0.1/squid-reports/Daily/2009Jul27-2009Jul27/index.html'. The page title is 'Squid Analysis Report Generator'. The main content area displays 'Squid User Access Reports' and a table with columns: NUM, USERID, CONNECT, BYTES, %BYTES, IN-CACHE-OUT, ELAPSED TIME, HIT/SEC, and %TIME. The table lists various report files and their corresponding statistics.

NUM	USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT	ELAPSED TIME	HIT/SEC	%TIME
1	192.168.0.111	4.93K	531.34M	42.80%	0.00%	100.00%	00:00:00	0 0.00%
2	192.168.0.112	4.09K	294.03M	16.43%	4.44%	95.56%	00:00:00	0 0.00%
3	192.168.0.132	17.00K	133.05M	10.72%	5.57%	94.43%	00:00:00	0 0.00%
4	192.168.0.120	1.25K	95.29M	7.68%	2.84%	97.16%	00:00:00	0 0.00%
5	192.168.0.131	9.19K	42.29M	3.41%	16.39%	83.61%	00:00:00	0 0.00%
6	192.168.0.144	2.71K	40.96M	3.30%	5.26%	94.74%	00:00:00	0 0.00%
7	192.168.0.148	6.27K	38.48M	3.10%	6.42%	93.58%	00:00:00	0 0.00%
8	192.168.0.145	6.94K	24.19M	1.95%	32.90%	67.10%	00:00:00	0 0.00%
9	192.168.0.133	5.95K	22.48M	1.81%	25.34%	74.66%	00:00:00	0 0.00%
10	192.168.0.140	3.34K	21.54M	1.74%	7.44%	92.56%	00:00:00	0 0.00%
11	192.168.0.122	4.14K	17.74M	1.43%	18.19%	81.81%	00:00:00	0 0.00%
12	192.168.0.125	2.47K	11.13M	0.90%	4.15%	95.85%	00:00:00	0 0.00%
13	192.168.0.154	33	9.60M	0.77%	0.23%	99.77%	00:00:00	0 0.00%
14	192.168.0.113	2.12K	9.56M	0.77%	14.52%	85.48%	00:00:00	0 0.00%
15	192.168.0.110	1.64K	9.05M	0.73%	6.80%	93.20%	00:00:00	0 0.00%
16	192.168.0.141	3.96K	6.93M	0.56%	17.81%	82.19%	00:00:00	0 0.00%
17	192.168.0.136	774	5.99M	0.48%	22.62%	77.38%	00:00:00	0 0.00%
18	192.168.0.138	3.37K	4.52M	0.36%	44.88%	55.12%	00:00:00	0 0.00%
19	192.168.0.143	3.44K	3.20M	0.26%	6.31%	93.69%	00:00:00	0 0.00%
20	192.168.0.152	1.17K	3.15M	0.25%	49.15%	50.85%	00:00:00	0 0.00%
21	192.168.0.121	371	2.69M	0.22%	7.61%	92.39%	00:00:00	0 0.00%
22	192.168.0.123	320	2.47M	0.20%	13.73%	86.27%	00:00:00	0 0.00%
23	192.168.0.153	197	1.15M	0.09%	5.32%	94.68%	00:00:00	0 0.00%

medium-perkasa.homelinux.net/squid-reports/Daily/2009Jul27-2009Jul27/192.168.0.111/192.1 - Windows Internet Explorer

http://192.168.0.1/squid-reports/Daily/2009Jul27-2009Jul27/192.168.0.111/192.168.0.111.html

Edit View Favorites Tools Help

rtes Proxy Report (28-Jul 09 00:10:00) http://medium-perkasa.h...

SARG

Squid Analysis Report Generator

Squid User Access Reports

Period: 2009Jul27-2009Jul27

User: 192.168.0.111

Sort: BYTES, reverse

User Report

ACCESSED SITE	CONNECT	BYTES	%BYTES	IN-CACHE-OUT	ELAPSED TIME	MILLISEC	%TIME
akamai.vip.com	28	330.19M	62.14%	0.00% 100.00%	00:00:00	0	0.00%
gun4-gnash.cz	14	197.90M	37.25%	0.00% 100.00%	00:00:00	0	0.00%
216.155.194.151	4,40K	1.83M	0.35%	0.00% 100.00%	00:00:00	0	0.00%
mag.updates.yahoo.com	13	638.39K	0.12%	0.00% 100.00%	00:00:00	0	0.00%
f36.yahoo.com	21	292.93K	0.06%	0.00% 100.00%	00:00:00	0	0.00%
216.155.194.147	229	107.89K	0.02%	0.00% 100.00%	00:00:00	0	0.00%
ad.yieldmanager.com	15	59.86K	0.01%	0.00% 100.00%	00:00:00	0	0.00%
richmedia.yimg.com	5	58.68K	0.01%	0.00% 100.00%	00:00:00	0	0.00%
content.yieldmanager.edgesuite.net	2	49.54K	0.01%	0.00% 100.00%	00:00:00	0	0.00%
insider.mag.yahoo.com	12	39.92K	0.01%	0.00% 100.00%	00:00:00	0	0.00%
216.155.194.236	36	35.67K	0.01%	0.00% 100.00%	00:00:00	0	0.00%
ads.yimg.com	2	20.23K	0.00%	0.00% 100.00%	00:00:00	0	0.00%
us.adservr.yahoo.com	16	16.63K	0.00%	0.00% 100.00%	00:00:00	0	0.00%
updates.vip.com	30	14.26K	0.00%	0.00% 100.00%	00:00:00	0	0.00%
us.bcy.yahoo.com	25	11.86K	0.00%	0.00% 100.00%	00:00:00	0	0.00%
login.yahoo.com443	4	11.35K	0.00%	0.00% 100.00%	00:00:00	0	0.00%
us.dti.yimg.com	3	8.30K	0.00%	0.00% 100.00%	00:00:00	0	0.00%
ml.adintarsu.com	1	6.86K	0.00%	0.00% 100.00%	00:00:00	0	0.00%
ts.richmedia.yahoo.com	9	4.61K	0.00%	0.00% 100.00%	00:00:00	0	0.00%
backup.vip.cz	12	3.73K	0.00%	0.00% 100.00%	00:00:00	0	0.00%
ads.bluewin.com	3	3.68K	0.00%	0.00% 100.00%	00:00:00	0	0.00%
address.yahoo.com	4	3.23K	0.00%	0.00% 100.00%	00:00:00	0	0.00%
httpvcsl.mag.yahoo.com	8	2.36K	0.00%	0.00% 100.00%	00:00:00	0	0.00%
216.155.194.236443	1	2.25K	0.00%	0.00% 100.00%	00:00:00	0	0.00%
216.155.194.147443	1	2.25K	0.00%	0.00% 100.00%	00:00:00	0	0.00%

TAHAP XVI


MEMBUAT FIREWALL DAN

MAC & IP FILTERING

- Membuat firewall berserta log yang sederhana dan nantinya dapat dikembangkan sesuai kebutuhan.

Untuk sementara dibuka port HTTP (80), HTTPS (443) dan SSH (221) di kedua interfaces, ***namun untuk port SSH dari sisi interfaces local (eth1) hanya bisa diakses oleh computer administrator semisal ber-IP 192.168.0.100*** dan selain itu akan ditutup yang bertujuan demi keamanan.

Dan khusus yang dari dalam (eth1) selain port HTTP (80) dan HTTPS/HTTP-SSL (443) dibuka juga port-port sebagai berikut:

- Port FTP (20,21) dan FTP-SSL (115,989,990)
  - Email POP3(110)/SMTP(25) dan POP3-SSL(995)/SMTP-SSL(465)
  - Samba (135,137,138,139,445) dan CUPS (631).
  - DNS (53)
  - Proxy (3128,3130) dan HAVP (8080)
  - Dsb....
- Sekaligus dibuat agar server tidak bisa di ping dengan  las an keamanan
  - Request dari port HTTP akan langsung di blokkkan ke port Proxy (3128).
  - Ini untuk pengamanan jaringan local terutama untuk RT/RW Net tetapi bisa digunakan untuk semua keperluan agar client tidak iseng merubah IP-nya akhirnya kita sebagai administrator sulit untuk memantau. IP yang didapatkan client harus tetap (static) bisa dilakukan memasukan IP secara manual atau menggunakan DHCP dengan menentukan IP berdasarkan MAC-ADDRESS-nya, lihat langkah install dan setting DHCP Server diatas. Untuk MAC-Filtering masih bisa dibobol dengan cloning MAC tetapi klo IP sama dalam satu jaringan pasti akan terjadi IP Conflic, maka itu kita mengkunci MAC-ADDRESS dan IP Client, klo IP maupun MAC yang tidak masuk dalam daftar akan tidak dapat terkoneksi dengan server.
  - Buat file bash script di `/etc/network/filter`

```
#!/bin/bash
# Bash script Firewall with IP Address and MAC Address Filtering
# (C) 2009-2010 by th@opikdesign.com

##### VARIABLE

files1="/etc/network/lists.filter"           #IP & MAC Client list file, sesuaikan
files2="/etc/network/administrator.filter"   #IP & MAC Administrator/Billing list file, sesuaikan

ip subnet=192.168.0.0/24                    #default local ip, sesuaikan
ip modem=192.168.1.1                        #default modem ip

device modem=eth0                           #default modem interfaces, sesuaikan
device=eth1                                 #default local interfaces, sesuaikan
device inet=ppp+                             #default inet interfaces, sesuaikan

ssh=221                                     #port SSH, sesuaikan
webmin=10000
samba cups=135,137,138,139,445,631
http=80
```



```

http SSL=443
smtp=25
smtp SSL=465
pop3=110
pop3 SSL=995
DNS=53
ftp=20,21
ftp SSL=115,989,990
proxy=3128
havp=8080
icp=3130
time=13,123

games=29000,27000,1873,11031,9110
dota=6112:6118
PB TCP=39100,39110,39220,49100,39190
PB UDP=40000:40009

range port=1025:65535

##### SCRIPT

echo "FIREWALL STATUS: All Firewall Drop & Reset"
/sbin/iptables -t mangle -F
/sbin/iptables -t nat -F
/sbin/iptables -t filter -F
/sbin/iptables -X
/sbin/iptables -t filter -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

echo "FIREWALL STATUS: MTU Setting"
/sbin/iptables -t mangle -A FORWARD -o $device -p tcp -m tcp --tcp-flags SYN,RST SYN -m tcpmss --mss 1400:1536 -j TCPMSS --clamp-mss-to-pmtu
/sbin/iptables -t mangle -A FORWARD -o $device inet -p tcp -m tcp --tcp-flags SYN,RST SYN -m tcpmss --mss 1400:1536 -j TCPMSS --clamp-mss-to-pmtu

echo "FIREWALL STATUS: Mangle created for Proxy Port at number 4"
/sbin/iptables -t mangle -A OUTPUT -m tos --tos Maximize-Reliability -j MARK --set-mark 0x04
/sbin/iptables -t mangle -A OUTPUT -m tos --tos 0x04 -j MARK --set-mark 0x4
/sbin/iptables -t mangle -A FORWARD -m tos --tos 0x04 -j MARK --set-mark 0x04
/sbin/iptables -t mangle -A POSTROUTING -m tos --tos 0x04 -j MARK --set-mark 0x04

echo "FIREWALL STATUS: Drop all FORWARD on $device"
/sbin/iptables -t filter -I FORWARD -i $device -j DROP

echo "FIREWALL STATUS: IP & MAC Filtering on device $device"
echo "FIREWALL STATUS: Allow access for IP-ADDRESS and MAC-ADDRESS:"

cat $files1 | while read ip address mac address client; do

    /sbin/iptables -t filter -I FORWARD -i $device -s $ip address -d $ip modem -p tcp -m multiport --dport $http,$http SSL -j DROP
    /sbin/iptables -t filter -I FORWARD -i $device -s $ip address -d $ip modem -p udp -m multiport --dport $http,$http SSL -j DROP

    /sbin/iptables -t nat -I PREROUTING -i $device -s $ip address -p tcp -m tcp --dport $http -j REDIRECT -to-ports $proxy
    /sbin/iptables -t nat -I PREROUTING -i $device -s $ip address -p udp -m udp --dport $http -j REDIRECT -to-ports $proxy

    /sbin/iptables -t filter -I FORWARD -i $device -s $ip address -m mac --mac-source $mac address -p tcp -m multiport --dports $samba cups -j ACCEPT
    /sbin/iptables -t filter -I FORWARD -i $device -s $ip address -m mac --mac-source $mac address -p udp -m multiport --dports $samba cups -j ACCEPT
    /sbin/iptables -t filter -I FORWARD -i $device -s $ip address -m mac --mac-source $mac address -p tcp -m multiport --dports $http,$http SSL,$smtp,$smtp SSL,$pop3,$pop3 SSL,$DNS,$ftp,$ftp SSL -j ACCEPT
    /sbin/iptables -t filter -I FORWARD -i $device -s $ip address -m mac --mac-source $mac address -p udp -m multiport --dports $http,$http SSL,$pop3,$pop3 SSL,$DNS,$ftp,$ftp SSL -j ACCEPT
    /sbin/iptables -t filter -I FORWARD -i $device -s $ip address -m mac --mac-source $mac address -p tcp -m multiport --dports $proxy,$havp,$icp,$time -j ACCEPT
    /sbin/iptables -t filter -I FORWARD -i $device -s $ip address -m mac --mac-source $mac address -p udp -m multiport --dports $proxy,$havp,$icp,$time -j ACCEPT

    /sbin/iptables -t filter -A INPUT -i $device -s $ip address -m mac --mac-source $mac address -p tcp -m multiport --dports $samba cups -j ACCEPT
    /sbin/iptables -t filter -A INPUT -i $device -s $ip address -m mac --mac-source $mac address -p udp -m multiport --dports $samba cups -j ACCEPT
    /sbin/iptables -t filter -A INPUT -i $device -s $ip address -m mac --mac-source $mac address -p tcp -m multiport --dports $http,$http SSL,$smtp,$smtp SSL,$pop3,$pop3 SSL,$DNS,$ftp,$ftp SSL -j ACCEPT
    /sbin/iptables -t filter -A INPUT -i $device -s $ip address -m mac --mac-source $mac address -p udp -m multiport --dports $http,$http SSL,$pop3,$pop3 SSL,$DNS,$ftp,$ftp SSL -j ACCEPT
    /sbin/iptables -t filter -A INPUT -i $device -s $ip address -m mac --mac-source $mac address -p tcp -m multiport --dports $proxy,$havp,$icp,$time -j ACCEPT
    /sbin/iptables -t filter -A INPUT -i $device -s $ip address -m mac --mac-source $mac address -p udp -m multiport --dports $proxy,$havp,$icp,$time -j ACCEPT

    /sbin/iptables -t filter -I FORWARD -i $device -s $ip address -m mac --mac-source $mac address -p tcp -m multiport --dports $range port -j ACCEPT
    /sbin/iptables -t filter -I FORWARD -i $device -s $ip address -m mac --mac-source $mac address -p udp -m multiport --dports $range port -j ACCEPT

    /sbin/iptables -t filter -A INPUT -i $device -s $ip address -m mac --mac-source $mac address -p tcp -m multiport --dports $range port -j ACCEPT
    /sbin/iptables -t filter -A INPUT -i $device -s $ip address -m mac --mac-source $mac address -p udp -m multiport --dports $range port -j ACCEPT

    /sbin/iptables -t nat -A POSTROUTING -s $ip address -o $device inet -j MASQUERADE

    arp -s $ip address $mac address

    echo "$ip_address [$mac_address] => $client"

done

cat $files2 | while read ip address mac address client; do

    /sbin/iptables -t nat -I PREROUTING -i $device -s $ip address -p tcp -m tcp --dport $http -j REDIRECT -to-ports $proxy
    /sbin/iptables -t nat -I PREROUTING -i $device -s $ip address -p udp -m udp --dport $http -j REDIRECT -to-ports $proxy

    /sbin/iptables -t filter -I FORWARD -i $device -s $ip address -m mac --mac-source $mac address -j ACCEPT

    /sbin/iptables -t filter -A INPUT -i $device -s $ip address -m mac --mac-source $mac address -j ACCEPT

    /sbin/iptables -t nat -A POSTROUTING -s $ip address -o $device inet -j MASQUERADE
    /sbin/iptables -t nat -A POSTROUTING -s $ip_address -o $device_modem -j MASQUERADE

```



```
arp -s $ip address $mac address

echo "$ip_address [$mac_address] => $client this Administrator Host"

done

echo "FIREWALL STATUS: ICMP Allowed on $device"
/sbin/iptables -t filter -I FORWARD -i $device -p icmp --icmp-type echo-request -j ACCEPT
/sbin/iptables -t filter -A INPUT -i $device -p icmp --icmp-type echo-request -j ACCEPT

echo "FIREWALL STATUS: Drop all INPUT on $device"
/sbin/iptables -t filter -A INPUT -i $device -j DROP

echo "FIREWALL STATUS: Port Filtering on $device_inet"
/sbin/iptables -t filter -A INPUT -i $device inet -p tcp -m multiport --dports $games -j ACCEPT
/sbin/iptables -t filter -A INPUT -i $device inet -p udp -m multiport --dports $games -j ACCEPT
/sbin/iptables -t filter -A INPUT -i $device inet -p tcp -m tcp --dport $dota -j ACCEPT
/sbin/iptables -t filter -A INPUT -i $device inet -p udp -m udp --dport $dota -j ACCEPT
/sbin/iptables -t filter -A INPUT -i $device inet -p tcp -m multiport --dports $PB TCP -j ACCEPT
/sbin/iptables -t filter -A INPUT -i $device inet -p udp -m udp --dport $PB UDP -j ACCEPT

/sbin/iptables -t filter -A INPUT -i $device inet -p tcp -m multiport --dports $http,$http SSL,$ssh,$webmin -j ACCEPT
/sbin/iptables -t filter -A INPUT -i $device inet -p udp -m multiport --dports $http,$http SSL,$ssh,$webmin -j ACCEPT
/sbin/iptables -t filter -A INPUT ! -s $ip subnet -i $device inet -p tcp -m multiport --dports $smtp,$smtp SSL -j DROP
/sbin/iptables -t filter -A INPUT -i $device inet -p tcp -j REJECT --reject-with tcp-reset
/sbin/iptables -t filter -A INPUT -i $device inet -p udp -j REJECT --reject-with icmp-port-unreachable
/sbin/iptables -t filter -A INPUT -i $device inet -p icmp -m icmp --icmp-type 8 -j DROP
/sbin/iptables -t filter -A FORWARD -i $device inet -p icmp -m length --length 92 -j DROP
/sbin/iptables -t filter -A INPUT -i $device inet -p icmp --icmp-type echo-request -j DROP

echo "FIREWALL STATUS: Drop all INPUT on $device_inet"
/sbin/iptables -t filter -A INPUT -i $device inet -j DROP

echo "FIREWALL STATUS: Log created..."
/sbin/iptables -t filter -A INPUT -p tcp -m limit --limit 5/min -j LOG --log-prefix "Iptables: Denied TCP Port: " --log-level 7
/sbin/iptables -t filter -A INPUT -p udp -m limit --limit 5/min -j LOG --log-prefix "Iptables: Denied UDP Port: " --log-level 7
/sbin/iptables -t filter -A INPUT -p icmp -m limit --limit 5/min -j LOG --log-prefix " Iptables: Denied ICMP Port: " --log-level 7
/sbin/iptables -t filter -A INPUT -p tcp -m state --state NEW -m multiport --dport $http,$http SSL -j LOG --log-prefix "HTTP CONN: TCP Port: "
/sbin/iptables -t filter -A INPUT -p tcp -m state --state NEW -m multiport --dport $proxy,$havp -j LOG --log-prefix "PROXY CONN: TCP Port: "
/sbin/iptables -t filter -A INPUT -p udp -m state --state NEW -m multiport --dport $http,$http SSL -j LOG --log-prefix "HTTPS CONN: UDP Port: "
/sbin/iptables -t filter -A INPUT -p udp -m state --state NEW -m multiport --dport $proxy,$havp -j LOG --log-prefix "PROXY CONN: UDP Port: "
/sbin/iptables -t filter -A INPUT -p tcp -m state --state NEW -m tcp --dport $ssh -j LOG --log-prefix "SSH CONN: TCP Port: "
/sbin/iptables -t filter -A INPUT -p udp -m state --state NEW -m udp --dport $ssh -j LOG --log-prefix "SSH CONN: UDP Port: "
```

- Kemudian file `/etc/network/filter` diberi chmod agar bisa jalankan...

```
# chmod +x /etc/network/filter
```

- Kemudian buat file `/etc/network/administrator.filter` yg berisi list IP dan MAC dari computer administrator/billing, contoh...

```
192.168.0.200 00:11:D8:CF:A5:21 billing.local.domain
```

- Dan buat juga file `/etc/network/lists.filter` yg berisi list IP dan MAC dari computer para client, contoh...

```
192.168.0.101 00:11:5B:78:D3:E8 client01.local.domain
192.168.0.102 00:16:EC:1E:2F:9E client02.local.domain
192.168.0.103 00:13:D4:CB:69:0F client03.local.domain
192.168.0.104 00:0E:2E:33:DF:BE client04.local.domain
192.168.0.105 00:11:5B:78:D3:E8 client05.local.domain
192.168.0.106 00:16:EC:1E:2F:9E client06.local.domain
192.168.0.107 00:13:D4:CB:69:0F client07.local.domain
192.168.0.108 00:0E:2E:33:DF:BE client08.local.domain
192.168.0.109 00:11:5B:78:D3:E8 client09.local.domain
192.168.0.110 00:16:EC:1E:2F:9E client10.local.domain
```

- Tiap kali computer server booting/start pertama kali atau saat jaringan di restart agar menjalankan bash-script tersebut maka edit kembali file `/etc/network/interfaces` kemudian pada group ***eth1*** tambahkan...

```
pre-up /etc/network/filter
```

jadi isi file keseluruhannya menjadi sebagai berikut (tulisan warna merah)...

```
auto lo
iface lo inet loopback

auto eth0
iface eth1 inet static
    address 192.168.1.2
    netmask 255.255.255.0
```

```
network 192.168.1.0
broadcast 192.168.1.255

auto eth1
iface eth1 inet static
    address 192.168.0.1
    netmask 255.255.255.0
    network 192.168.0.0
    broadcast 192.168.0.255
    pre-up /etc/network/filter

auto dsl-provider
iface dsl-provider inet ppp
pre-up /sbin/ifconfig eth0 up # line maintained by pppoeconf
provider dsl-provider
```

- Terakhir lakukan restart pada jaringan

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

## TAHAP XVII-1

### INSTALL DAN SETTING WEBHTB

### SEBAGAI BANDWIDTH MANAGEMENT

### DILENGKAPI PEMISAH BANDWIDTH IIX DAN INTL.

- WebHTB adalah sebuah tools untuk mengatur Bandwidth langsung pada TC, WebHTB sebenarnya pengembangan dari HTB-Tools sedangkan yang sekarang ini lebih user-friendly karena didukung Web-GUI. Saat saya tulis versi terbarunya adalah Versi 2.9.

- Masuk directory `/var` dan download kemudian extract...

```
# cd /var
# wget -c http://www.opikdesign.com/kios/webhtb/webhtb_V2.9.25.tar.bz2
# tar -xjvf webhtb_V2.9.25.tar.bz2
# rm webhtb_V2.9.25.tar.bz2
```

- Kemudian folder `/var/webhtb` diberi permission agar bisa di akses oleh apache

```
# chown -R www-data.www-data /var/webhtb
```

- Edit file `/etc/apache2/sites-available/ssl` kemudian tambahkan seperti dibawah ini sebelum `</VirtualHost>`...

```
Alias /webhtb /var/webhtb
<Directory "/var/webhtb">
Options Indexes FollowSymLinks MultiViews
AllowOverride None
Order allow,deny
allow from all
</Directory>
```

- Restart Apache

```
# service apache2 restart
```

- Jika default dari port SSH dirubah kalau tidak dirubah tetap di port 22 maka abaikan langkah ini, edit file `/var/webhtb/Net/SSH1.php`, Cari teks...

```
function Net SSH1($host, $port = 22, $timeout = 10, $cipher = NET SSH1 CIPHER 3DES)
```

Angka 22 dirubah dengan port default pada port SSH yang kita pakai, misalnya port SSH sudah dirubah default-nya menjadi 221 maka rubah menjadi...

```
function Net SSH1($host, $port = 221, $timeout = 10, $cipher = NET SSH1 CIPHER 3DES)
```

Begitu juga pada file `/var/webhtb/Net/SSH2.php`, Cari teks...

```
function Net SSH2($host, $port = 22, $timeout = 10)
```

Angka 22 dirubah dengan port default pada port SSH yang kita pakai, misalnya port SSH sudah dirubah default-nya menjadi 221 maka rubah menjadi...

```
function Net SSH2($host, $port = 221, $timeout = 10)
```

- Buat password root :

```
# passwd root
```

masukan password yang dikehendaki dan ketik ulang.

```
root@persegi:~# passwd root
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@persegi:~# █
```

- Buka [https://\[ip-server\]/webhtb/setup](https://[ip-server]/webhtb/setup) web browsing dari computer administrator

MySQL admin user:

MySQL admin password:

MySQL WebHTB user:

MySQL WebHTB password:

MySQL WebHTB password again:

MySQL WebHTB database name:

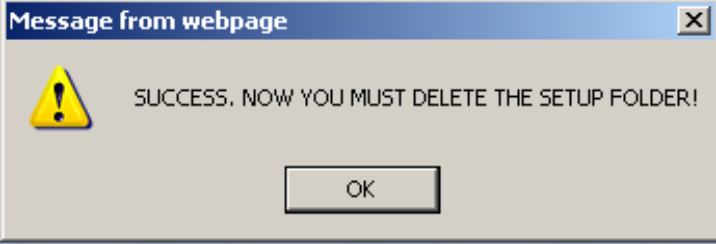
Default LAN Interface:

Default WAN Interface:

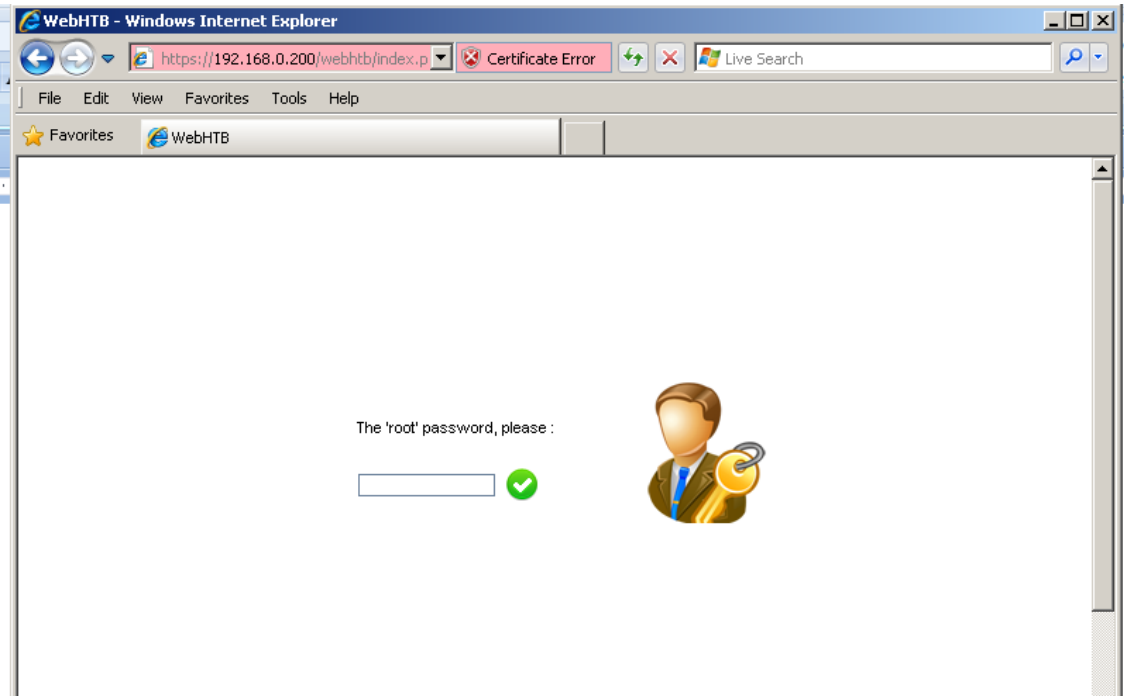
\* Information marked in red is required !  
\* If you omit entering the MySQL user and password for WebHTB, root will be used instead!

Isi yg bertulis merah...  
Untuk MySQL User diisi root dan untuk password diisi saat install Ubuntu Server/LAMP pertama kali.  
Sedangkan Default LAN Interface dan Default WAN Interface pilih dan sesuaikan kondisi.

Click Submit, kalau sukses akan muncul... dan click OK



- Setelah itu akan muncul tampilan untuk login seperti dibawah ini, dan masukan password root yg sudah dibuat.



- Sebelum login, update IP Games, edit file `/var/webhtb/games/nice.rsc` dan isinya bisa diganti (jangan ditambahkan) dengan link <http://opensource.telkomspeedy.com/forum/viewtopic.php?pid=66635#p66635>
- Update IP IIX, jalankan perintah tersebut...

```
# sh /var/webhtb/iix/update/generate.update
```

Membuat WebHTB menjadi daemon agar tiap kali server booting akan menjalankan WebHTB, ikuti command dibawah ini...

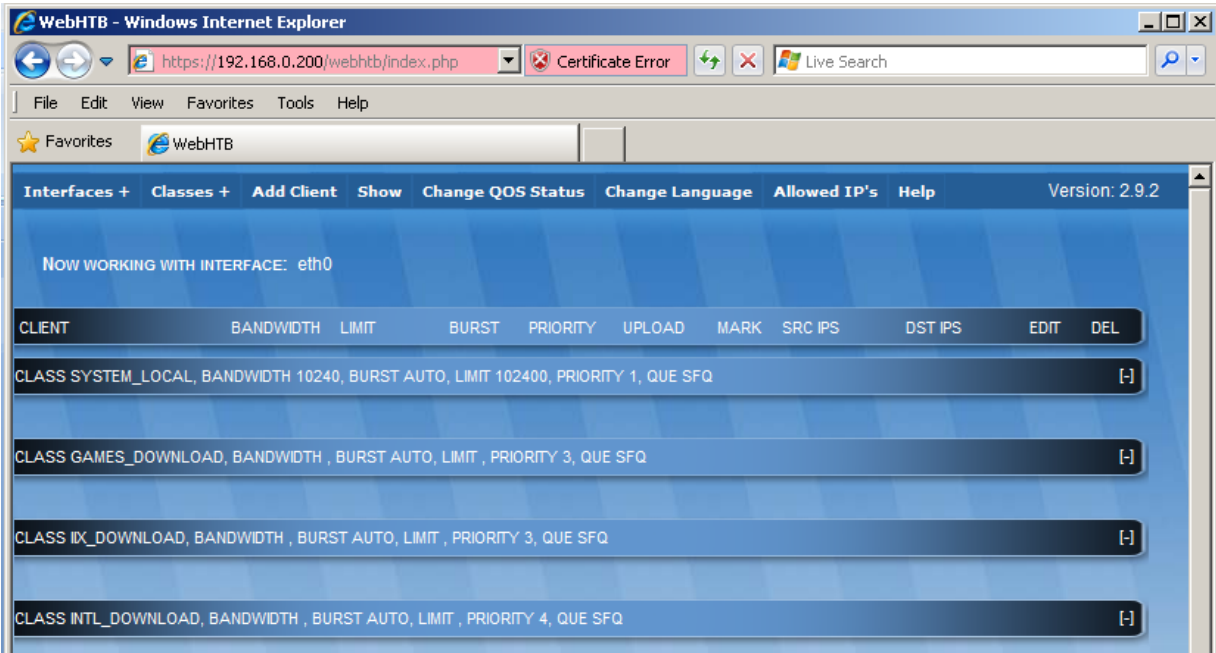
```
# cp /var/webhtb/docs/webhtb /etc/init.d/webhtb
```

```
# chmod +X /etc/init.d/webhtb
```

dan edit file `/etc/rc.local` dan tambahkan baris sebagai berikut...

```
Service webhtb start
```

- Setelah login tampilan akan seperti ini...



## TAHAP XVII-2 MENGATUR BANDWIDTH YANG DIPERLUKAN OLEH SYSTEM (SSH, SAMBA, CUPS, SQUID PROXY)

- Sekarang memberi bandwidth pada port SSH agar tidak terlimit.  
Mouse arahkan “Add Client” dan click...

Pilih Class “SYSTEM\_LOCAL”  
Nama client: SSH (*nantinya secara otomatis namanya akan berubah sesuai classes dan interfaces*)  
Bandwidth: 10240  
Limit: 102400  
Priority: 0 (*Semakin kecil semakin diutamakan*)  
SRC IPS: 192.168.0.1 (*IP Server, Sesuaikan*)  
SRC PORTS: 221 (*Contoh Port SSH yg sudah dirubah, Sesuaikan*)

Kemudian click “SAVE” dan “Close”.

- Jika tidak menginstall SAMBA maka langkah tersebut bisa diabaikan.  
Agar tidak membatasi SAMBA dan CUPS

Mouse arahkan “Add Client” dan click...

ADD CLIENT ON INTERFACE eth0

IMPORTANT: Don't use empty spaces and separate ports with commas; red labels are required !

CHOSE A CLASS: SYSTEM\_LOCAL

CLIENT	BANDWIDTH	LIMIT	BURST	PRIORITY	UPLOAD	MARK	MAC
SAMBA_CUPS	10240	102400	0	1			
SRC IPS      SRC PORTS      DST IPS      DST PORTS							
192.168.0.1	135						
192.168.0.1	137						
192.168.0.1	138						
192.168.0.1	139						
192.168.0.1	445						
192.168.0.1	631						

Click here for new src, dst ..      SAVE      RESET

Click “Click here for new src, dst” sebanyak 5 kali.

Pilih Class “SYSTEM\_LOCAL”  
Nama client: SAMBA\_CUPS  
Bandwidth: 10240  
Limit: 102400  
Priority: 1  
SRC IPS: 192.168.0.1 *(Sesuaikan dengan IP Server)*  
SRC PORTS: 135,137,138,139,445 *(Port SAMBA)*, 631 *(Port CUPS)*

- Jika tidak menginstall SQUID PROXY maka langkah tersebut bisa diabaikan.  
Agar halaman web yang sudah di cache oleh squid proxy tidak terlimit.

Edit kembali file `/etc/squid/squid.conf` dan pada baris terakhir tambahkan...

```
#####  
# Marking ZPH for b/w management  
#####  
  
zph mode tos  
zph local 0x04  
#zph parent 0  
#zph option 136
```

kemudian squid di restart...

```
# squid -k reconfigure
```

Kemudian jalankan rules tersebut diatas...

```
# iptables -t mangle -A OUTPUT -m tos --tos Maximize-Reliability -j MARK --set-mark 0x4  
# iptables -t mangle -A OUTPUT -m tos --tos 0x4 -j MARK --set-mark 0x4  
# iptables -t mangle -A FORWARD -m tos --tos 0x4 -j MARK --set-mark 0x4  
# iptables -t mangle -A POSTROUTING -m tos --tos 0x4 -j MARK --set-mark 0x4
```

Terakhir tambah client “PROXY\_HIT” di classes “SYSTEM” pada WebHTB.  
Mouse arahkan “Add Client” dan click...

ADD CLIENT ON INTERFACE eth0

IMPORTANT: Don't use empty spaces and separate ports with commas; red labels are required !

CHOSE A CLASS: SYSTEM\_LOCAL

CLIENT	BANDWIDTH	LIMIT	BURST	PRIORITY	UPLOAD	MARK	MAC
PROXY_HIT	1024	10240	0	2		4	
SRC IPS      SRC PORTS      DST IPS      DST PORTS							

Click here for new src, dst ..      SAVE      RESET

Pilih Class “SYSTEM\_LOCAL”  
Nama client: PROXY\_HIT  
Bandwidth: 1024  
Limit: 10240  
Priority: 2  
Mark: 4

**TAHAP XVII-3**  
**MENGATUR BANDWIDTH DOWNLOAD CLIENT**  
**DAN MEMISAHKAN BANDWIDTH**  
**UNTUK GAMES ONLINE**  
**DAN LOCAL (IIX) DENGAN INTERNATIONAL (INTL)**

- Mengatur bandwidth tiap unit client sebenarnya gampang-gampang susah. Pada dasarnya pembagian bandwidth per client berdasarkan dari rumus, tiap unit client mendapatkan bandwidth terendah sebesar bandwidth rata-rata yang didapat dari ISP dibagi jumlah unit client sedangkan untuk batas bandwidth tertinggi dari tiap client bisa diambil dari bandwidth terendah dari tiap client bisa dikalikan dua atau ekstrimnya batas atas bandwidth dari ISP, namun untuk amannya maksimal setengah dari bandwidth ISP.

Dapat dirumuskan sebagai berikut...

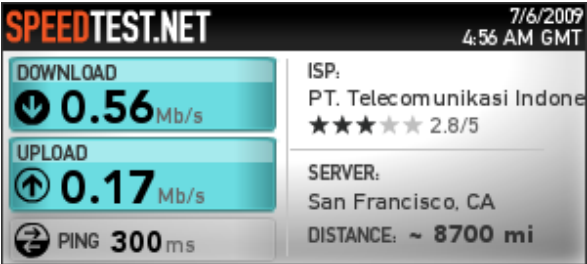
<b>Bandwidth Client = &lt;Bandwidth download dari ISP&gt; / &lt;Jumlah Client&gt;</b>
<b>Limit Client = &lt;Bandwidth Client&gt; x 2</b>  atau ekstrimnya...  <b>Limit Client = &lt;Bandwidth download dari ISP&gt; / 2</b>
<b>Bandwidth Upload = &lt;Limit Client&gt; / 4</b>  atau...  <b>Bandwidth Upload = &lt;Bandwidth upload dari ISP&gt; / &lt;Jumlah Client&gt;</b>

- Karena beberapa ISP ada yg memberikan bandwidth IX tidak sama atau lebih kecil ketimbang bandwidth IIX, karena itu untuk memanage bandwidth untuk client perlu ada pemisahan mana bandwidth dari INTL dan IIX. Terutama pemakaian pada speedy.
- Sebelum membuat classes pemisah bandwidth dan membatasin bandwidth tiap client, ada baiknya meng-check dahulu seberapa besarnya bandwidth IIX dan IX yang di dapat dari ISP, check di <http://www.speedtest.net>.
- 

Untuk melihat speed IIX arah ke server yang berada di dalam negeri, contoh hasilnya...



Untuk melihat speed INTL arahkan ke server di luar negeri, usahakan di benua yang terjauh semisal Amerika, contoh hasilnya...

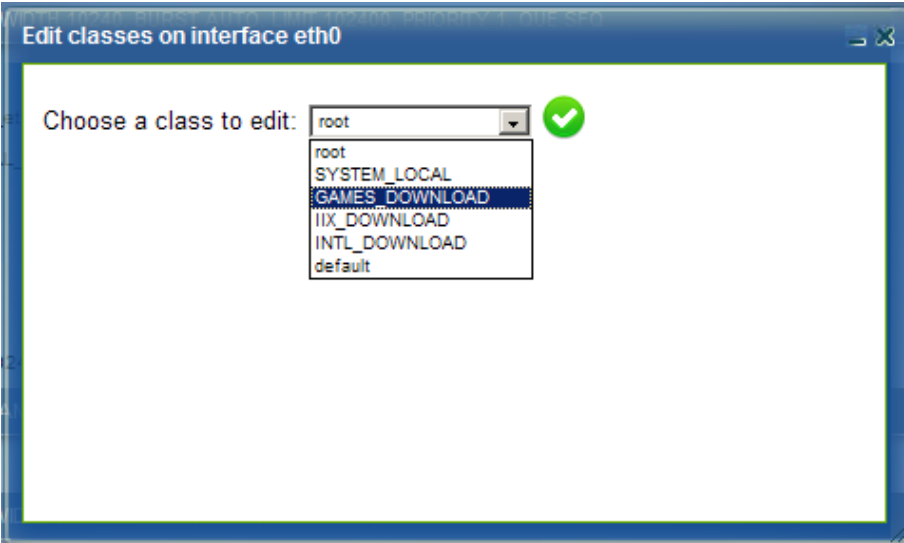
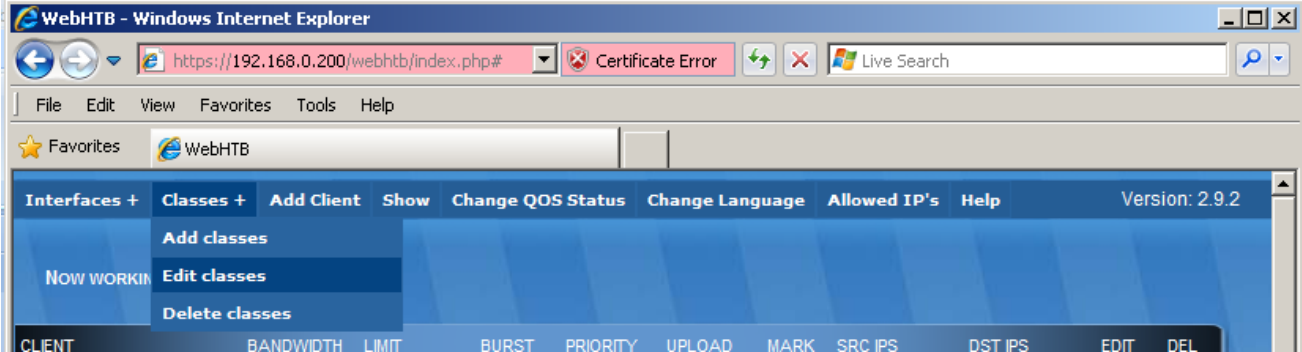


Karena bandwidth ini tidak selalu stabil atau kata lain akan berubah-ubah, coba pantau terus beberapa hari dengan waktu yang random misalnya pagi, siang, sore, malam, dan tengah malam agar mendapatkan angka jam-jam tersibuk dan terkosong, kemudian ambil rata-ratanya... hasilnya akan dijadikan patokan bandwidth yang didapat dari ISP langsung.

- Edit class GAMES\_DOWNLOAD, IIX\_DOWNLOAD dan INTL\_DOWNLOAD, sesuaikan bandwidth dengan hasil pengukuran lewat <http://www.speedtest.net>

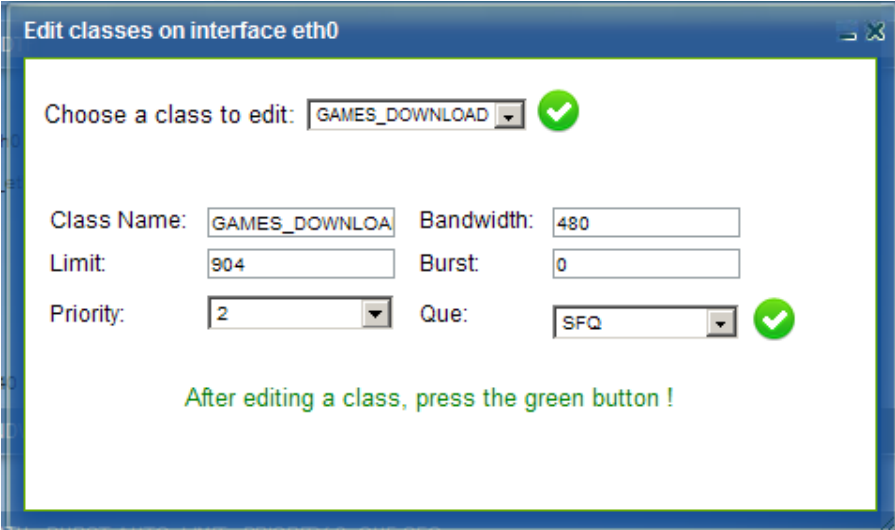
*Perlu diketahui, untuk GAMES\_DOWNLOAD besaran sama seperti IIX\_DOWNLOAD , karena IP yang terdaftar di database hanya diperuntukan Game Online di Indonesia.*

Arahkan mouse ke “Classes +” kemudian pilih “Edit classes” dan click



Pilih class yang akan di edit kemudian click tanda centang hijau.

Edit Classes GAMES\_DOWNLOAD,

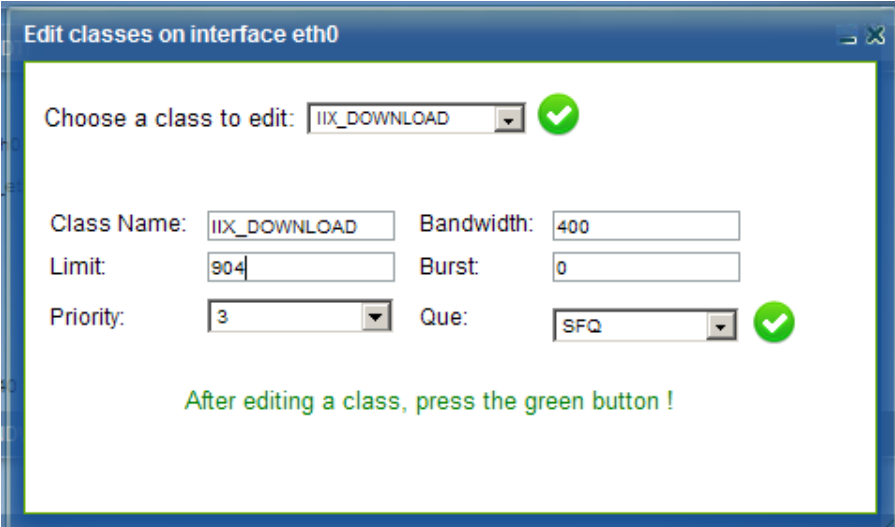


Masukkan Bandwidth dan Limit yang didapat dari ISP untuk koneksi IIX, dilihat hasil test diatas.

**Namun perlu diingat, bandwidth games dan IIX jadi satu maka itu untuk bandwidth dibagi dua dgn IIX\_DOWNLOAD, selain itu Bandwidth dan Limit harus kelipatan 8.**

Kemudian click tanda centang hijau.

Edit Classes IIX\_DOWNLOAD,



Masukkan Bandwidth dan Limit yang didapat dari ISP untuk koneksi IIX, dilihat hasil test diatas.

**Namun perlu diingat, bandwidth games dan IIX jadi satu maka itu untuk bandwidth dibagi dua dgn GAMES\_DOWNLOAD, selain itu Bandwidth dan Limit harus kelipatan 8.**

Kemudian click tanda centang hijau.



Edit Classes INTL\_DOWNLOAD,

Edit classes on interface eth0

Choose a class to edit: INTL\_DOWNLOAD

Class Name: INTL\_DOWNLOAD

Bandwidth: 560

Limit: 560

Burst: 0

Priority: 4

Que: SFQ

After editing a class, press the green button !

Masukkan Bandwidth dan Limit yang didapat dari ISP untuk koneksi INTL, dilihat hasil test diatas.

- Sebelumnya menentukan bandwidth tiap client sebaiknya menghitung sesuai penjelasan diatas.  
Buat tiap client di tiap classes IIX dan IX, contohnya...  
Setelah dihitung, ini contoh menggunakan Speedy Paket Game dan bandwidth rata-rata yang didapat dari ISP, IIX: 900/210kbps (download/upload) dan IX: 560/170kbps kemudian missal dibagi 10 unit client ditambah 1 unit administrator/billing maka setingan WebHTB sebagai berikut...

**Bagi warnet yang mengkhususkan client untuk Games Online, besaran bandwidth dan limit sama saja dengan besaran IIX hanya saja disini secara otomatis untuk class GAMES\_DOWNLOAD di prioritaskan dari pada classes untuk browsing biasa, dengan tujuan agar saat main games tidak nge-lag.**

Buat Client untuk khusus Games Online, masukan pada classes GAMES\_DOWNLOAD...

ADD CLIENT ON INTERFACE eth0

IMPORTANT: Don't use empty spaces and separate ports with commas; red labels are required !

CHOSE A CLASS: GAMES\_DOWNLOAD

CLIENT	BANDWIDTH	LIMIT	BURST	PRIORITY	UPLOAD	MARK	MAC
games01	80	160	0	3			0011D8CFA521

SRC IPS

SRC PORTS

DST IPS192.168.0.100

DST PORTS

Click here for new src, dst ..

SAVERESET

Pilih Class “GAMES\_DOWNLOAD”  
Client: games01 (Sesuaikan misal bisa diganti “Client01”, nantinya secara otomatis namanya akan berubah sesuai classes dan interfaces agar pengaturan di database tidak saling bertindih, **DILARANG MERUBAH MELALUI EDIT CLIENT DENGAN MEMBUANG IMBUHAN CLASSES DAN INTERFACES**)  
Bandwidth: 80 (dari rumus dan/atau kondisi dan harus kelipatan 8)  
Limit: 160 (dari rumus dan/atau kondisi dan harus kelipatan 8)  
MAC: 0011D8CFA521 (MAC-ADDRESS Client, sesuaikan)  
DST IPS: 192.168.0.100 (IP ADDRESS Client, sesuaikan)  
**PERHATIAN:**  
**UNTUK IDENTITAS CLIENT BISA MENGGUNAKAN MAC-ADDRESS AJA ATAU IP-ADDRESS AJA ATAU DIISI KEDUANYA, DIANJURKAN TERUTAMA UNTUK WIFI AGAR MEMAKAI KEDUANYA. UNTUK CLASS GAMES\_DOWNLOAD , JANGAN SAMPAI MENGISI PORTS DAN SRC. DILARANG MENGISI MARK, JIKA AKAN MENGGUNAKAN MARK LEBIH BAIK MEMBUAT CLASSES TERSENDIRI.**

Buat client untuk koneksi IIX, masukan pada classes IIX\_DOWNLOAD...

ADD CLIENT ON INTERFACE eth0

IMPORTANT: Don't use empty spaces and separate ports with commas; red labels are required !

CHOSE A CLASS: IIX\_DOWNLOAD

CLIENT	BANDWIDTH	LIMIT	BURST	PRIORITY	UPLOAD	MARK	MAC
browsing01	80	160	0	3			000C46A7229A

SRC IPS

SRC PORTS

DST IPS192.168.0.110

DST PORTS

Click here for new src, dst ..

SAVERESET

Pilih Class “IIX\_DOWNLOAD”  
Client: browsing01 (Sesuaikan misal bisa diganti “Client01”, nantinya secara otomatis namanya akan berubah sesuai classes dan interfaces agar pengaturan di database tidak saling bertindih, **DILARANG MERUBAH MELALUI EDIT CLIENT DENGAN**



**MEMBUANG IMBUHAN CLASSES DAN INTERFACES)**

Bandwidth: 80 (dari rumus dan/atau kondisi dan harus kelipatan 8)

Limit: 160 (dari rumus dan/atau kondisi dan harus kelipatan 8)

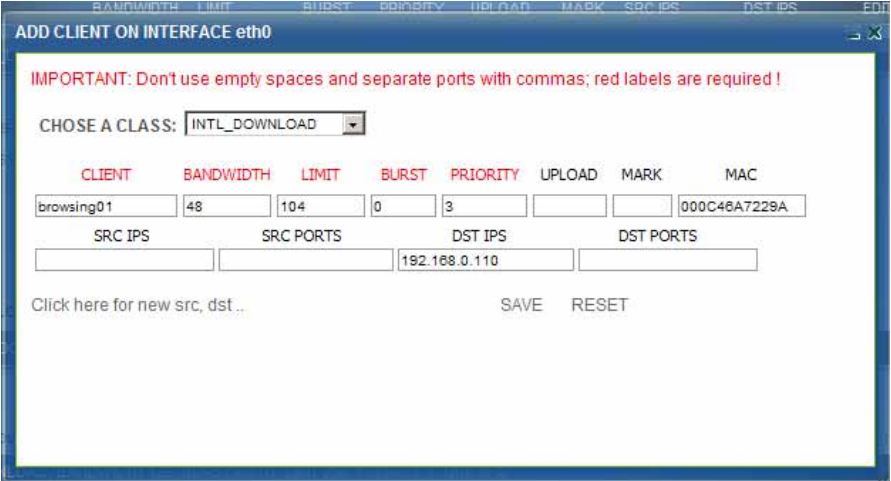
MAC: 000C46A7229A (MAC-ADDRESS Client, sesuaikan)

DST IPS: 192.168.0.110 (IP ADDRESS Client, sesuaikan)

**PERHATIAN:**

**UNTUK IDENTITAS CLIENT BISA MENGGUNAKAN MAC-ADDRESS AJA ATAU IP-ADDRESS AJA ATAU DIISI KEDUANYA, DIANJURKAN TERUTAMA UNTUK WIFI AGAR MEMAKAI KEDUANYA. UNTUK CLASS IIX\_DOWNLOAD , JANGAN SAMPAI MENGISI PORTS DAN SRC. DILARANG MENGISI MARK, JIKA AKAN MENGGUNAKAN MARK LEBIH BAIK MEMBUAT CLASSES TERSENDIRI.**

Setelah membuat client di class INTL\_DOWNLOAD...



Client: browsing01 (Sesuaikan misal bisa diganti “Client01”, nantinya secara otomatis namanya akan berubah sesuai classes dan interfaces agar pengaturan di database tidak saling bertindih, **DILARANG MERUBAH MELALUI EDIT CLIENT DENGAN MEMBUANG IMBUHAN CLASSES DAN INTERFACES)**

Bandwidth: 48 (dari rumus dan/atau kondisi dan harus kelipatan 8)

Limit: 104 (dari rumus dan/atau kondisi dan harus kelipatan 8)

MAC: 000C46A7229A (MAC-ADDRESS Client, sesuaikan)

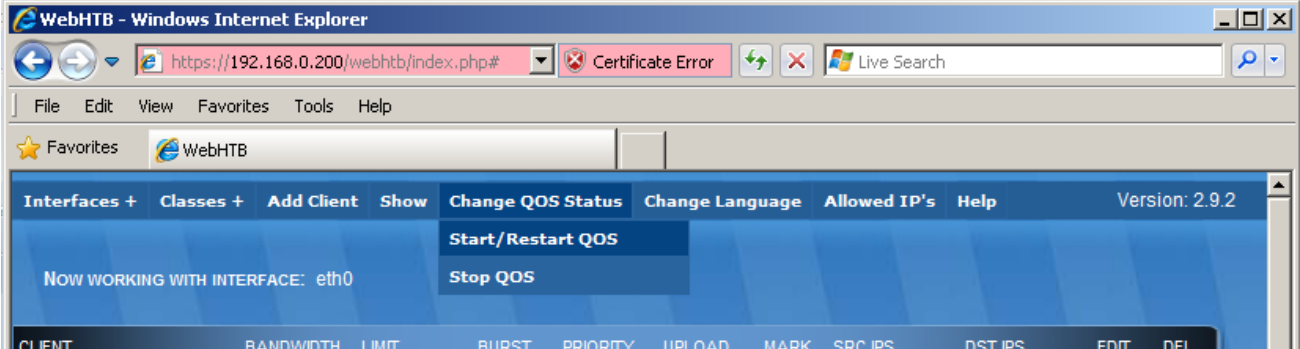
DST IPS: 192.168.0.110 (IP ADDRESS Client, sesuaikan)

**PERHATIAN:**

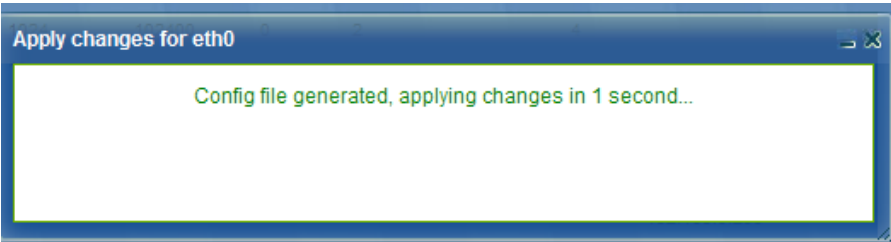
**UNTUK IDENTITAS CLIENT BISA MENGGUNAKAN MAC-ADDRESS AJA ATAU IP-ADDRESS AJA ATAU DIISI KEDUANYA, DIANJURKAN TERUTAMA UNTUK WIFI AGAR MEMAKAI KEDUANYA. UNTUK CLASS INTL\_DOWNLOAD , JANGAN SAMPAI MENGISI PORTS DAN SRC. DILARANG MENGISI MARK, JIKA AKAN MENGGUNAKAN MARK LEBIH BAIK MEMBUAT CLASSES TERSENDIRI.**

Jangan lupa buatkan untuk semua client.

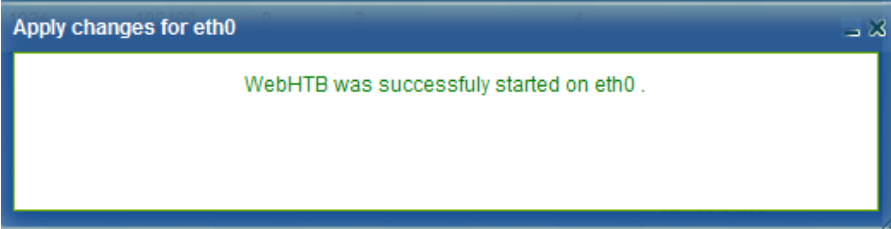
- Terakhir jalankan WebHTB...



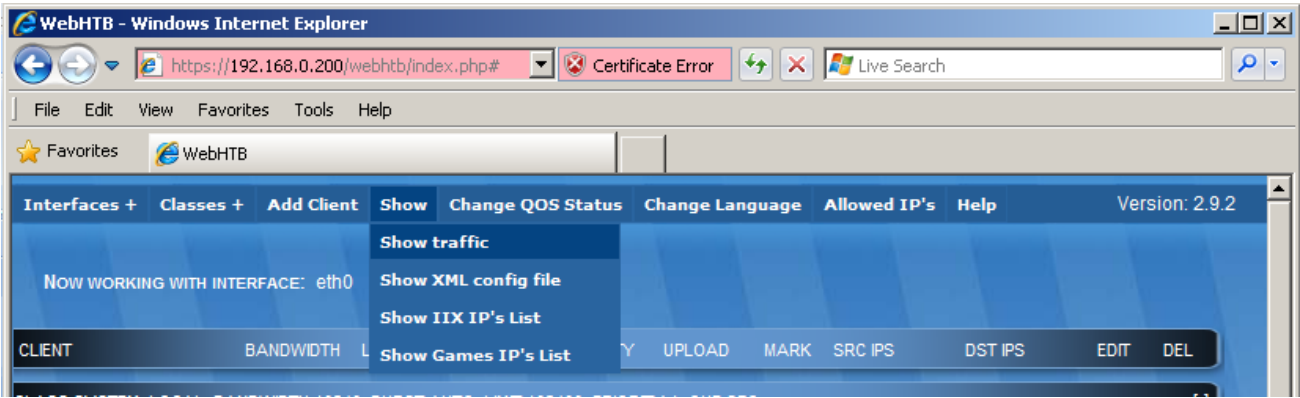
Arahkan mouse ke “Change QOS Status” kemudian pilih “Start/Restart QOS” dan click



Karena ada tambahan fasilitas pemisah IIX dan INTL maka proses ini lebih lama dari pada WebHTB yang tanpa IIX dan INTL. Kalau sudah success akan seperti ini...



- Untuk melihat Traffic-nya,  
Arahkan mouse menuju ke “Show” kemudian pilih “Show traffic” dan click



Contoh traffic...

CLASS CLIENT	SPEED	BANDWIDTH	LIMIT	TOKENS	CTOKENS
SYSTEM_LOCAL	169.03	10240	102400	23999720	94
PROXY_HIT_SYSTEM_LOCAL_eth0	168.92	1024	10240	23997193	940
SAMBA_CUPS_SYSTEM_LOCAL_eth0	0.11	10240	102400	23999799	102
GAMES_DOWNLOAD	0	128	256	4750000	48828
IX_DOWNLOAD	50.89	128	256	1951944	-46346
my-opik_IX_DOWNLOAD_eth0	56.86	80	256	1558458	-46346
INTL_DOWNLOAD	9.20	128	256	4744393	46639
my-opik_INTL_DOWNLOAD_eth0	9.20	80	256	7590291	46639
_default_	3.35	8	8	3800000	97656

- Ada baiknya setelah mengentry semua client, lebih baik lakukan restart pada server, terkadang jalannya QOS pada TC tidak normal.

## TAHAP XVIII

### INSTALL & SETTING CACTI

- CACTI, sebuah program yang berbasis web berfungsi untuk memantau aktifitas server, CACTI melaporkan dalam bentuk grafik. Jadi semua aktifitas server akan terpantau mulai transfer rate data sampai kinerja processor maupun RAM.
- CACTI juga membutuhkan repository lainnya, antaranya SNMP dan RRD-TOOLS, berhubung kita sudah menginstall reposistory tersebut. Setting SNMP-nya... buka file `/etc/snmp/snmpd.conf` dan rubah menjadi seperti ini...

```
#          sec.name      source          community
com2sec    readonly     192.168.0.1    root           # ini ip-nya server cacti, sesuaikan
com2sec    readonly     localhost      root           #
com2sec    readonly     local.domain   root           # sesuaikan

#          sec.model     sec.name
group MyROGroup v1      readonly
group MyROGroup v2c     readonly
group MyROGroup usm      readonly
group MyRWGroup v1      readwrite
group MyRWGroup v2c     readwrite
group MyRWGroup usm      readwrite

#          incl/excl subtree          mask
view all   included .1                80

#          context sec.model sec.level match read  write  notif
access MyROGroup ""    any      noauth  exact  all    none   none
access MyRWGroup ""    any      noauth  exact  all    all    none

syslocation local.domain
syscontact th@opikdesign.com
```

Kemudian restart SNMP-nya

```
# service snmpd restart
```

- Test SNMP apakah sudah berjalan dengan SNMPWALK...

```
# snmpwalk -v 1 -c root localhost system
```

SNMPWALK akan menunjukan kalau SNMP berjalan hasilnya kurang lebih seperti dibawah ini...

```
root@persegi:~# snmpwalk -v 1 -c root localhost system
SNMPv2-MIB::sysDescr.0 = STRING: Linux persegi 2.6.28-15-server #49-Ubuntu SMP Tue Aug 18 19:30:06 UTC 2009 i686
SNMPv2-MIB::sysObjectID.0 = OID: NET-SNMP-MIB::netSnmpAgentOIDs.10
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (86381) 0:14:23.81
SNMPv2-MIB::sysContact.0 = STRING: th@opikdesign.com
SNMPv2-MIB::sysName.0 = STRING: persegi
SNMPv2-MIB::sysLocation.0 = STRING: dns.persegi.net
SNMPv2-MIB::sysORLastChange.0 = Timeticks: (3) 0:00:00.03
SNMPv2-MIB::sysORID.1 = OID: SNMP-FRAMEWORK-MIB::snmpFrameworkMIBCompliance
SNMPv2-MIB::sysORID.2 = OID: SNMP-MPD-MIB::snmpMPDCompliance
SNMPv2-MIB::sysORID.3 = OID: SNMP-USER-BASED-SM-MIB::usmMIBCompliance
SNMPv2-MIB::sysORID.4 = OID: SNMPv2-MIB::snmpMIB
SNMPv2-MIB::sysORID.5 = OID: TCP-MIB::tcpMIB
SNMPv2-MIB::sysORID.6 = OID: IP-MIB::ip
SNMPv2-MIB::sysORID.7 = OID: UDP-MIB::udpMIB
SNMPv2-MIB::sysORID.8 = OID: SNMP-VIEW-BASED-ACM-MIB::vacmBasicGroup
SNMPv2-MIB::sysORDescr.1 = STRING: The SNMP Management Architecture MIB.
SNMPv2-MIB::sysORDescr.2 = STRING: The MIB for Message Processing and Dispatching.
SNMPv2-MIB::sysORDescr.3 = STRING: The management information definitions for the SNMP User-based Security Model.
SNMPv2-MIB::sysORDescr.4 = STRING: The MIB module for SNMPv2 entities
SNMPv2-MIB::sysORDescr.5 = STRING: The MIB module for managing TCP implementations
SNMPv2-MIB::sysORDescr.6 = STRING: The MIB module for managing IP and ICMP implementations
SNMPv2-MIB::sysORDescr.7 = STRING: The MIB module for managing UDP implementations
SNMPv2-MIB::sysORDescr.8 = STRING: View-based Access Control Model for SNMP.
SNMPv2-MIB::sysORUpTime.1 = Timeticks: (1) 0:00:00.01
SNMPv2-MIB::sysORUpTime.2 = Timeticks: (1) 0:00:00.01
SNMPv2-MIB::sysORUpTime.3 = Timeticks: (1) 0:00:00.01
SNMPv2-MIB::sysORUpTime.4 = Timeticks: (3) 0:00:00.03
SNMPv2-MIB::sysORUpTime.5 = Timeticks: (3) 0:00:00.03
SNMPv2-MIB::sysORUpTime.6 = Timeticks: (3) 0:00:00.03
SNMPv2-MIB::sysORUpTime.7 = Timeticks: (3) 0:00:00.03
SNMPv2-MIB::sysORUpTime.8 = Timeticks: (3) 0:00:00.03
root@persegi:~#
```

- Check dahulu versi SNMP dan RRD-Tools yang dipakai dgn perintah sebagai berikut..

```
# rrdtool -V && snmpd -v
```

dan hasilnya...

```
root@persegi:~# rrdtool -V && snmpd -v
RRDtool 1.3.1 Copyright 1997-2008 by Tobias Oetiker <tobi@oetiker.ch>
Compiled Mar 18 2009 17:20:51

Usage: rrdtool [options] command command_options

Valid commands: create, update, updatev, graph, graphv, dump, restore,
                last, lastupdate, first, info, fetch, tune,
                resize, xport

RRDtool is distributed under the Terms of the GNU General
Public License Version 2. (www.gnu.org/copyleft/gpl.html)

For more information read the RRD manpages

NET-SNMP version: 5.4.1
Web: http://www.net-snmp.org/
Email: net-snmp-coders@lists.sourceforge.net
```

dapat dilihat, RRD-Tools ver 1.3.1 dan SNMP ver 5.4.1

- Kemudian Install CACTI...

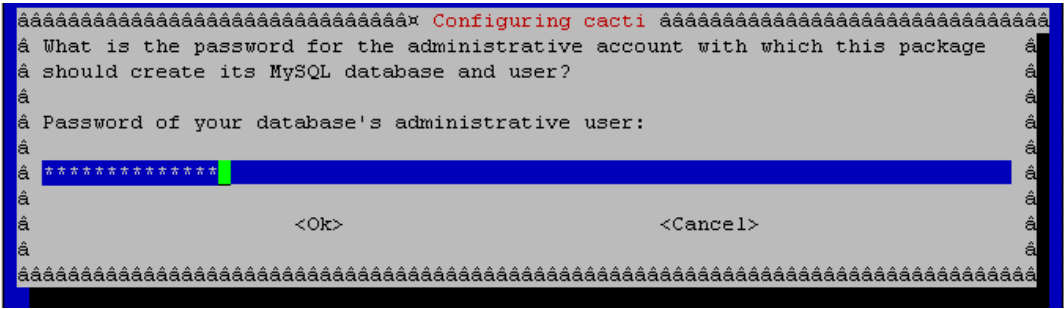
```
# apt-get install cacti
```

akan muncul pertanyaan tentang configuration database CACTI...

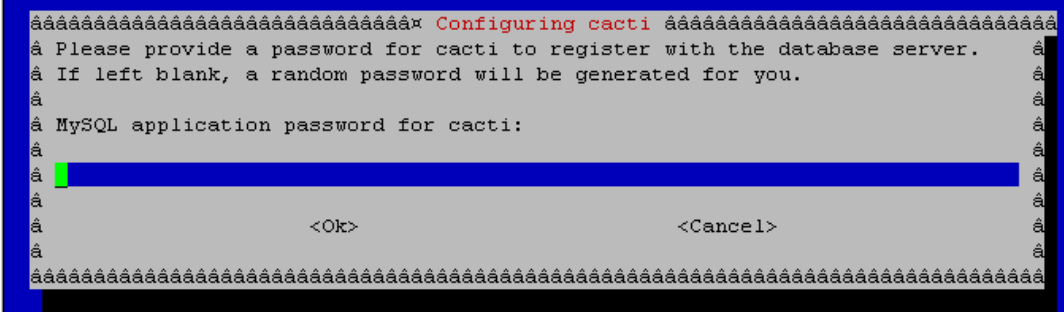
```

##### Configuring cacti #####
â
â cacti must have a database installed and configured before it can be used.
â If you like, this can be handled with dbconfig-common.
â
â If you are an advanced database administrator and know that you want to
â perform this configuration manually, or if your database has already been
â installed and configured, you should refuse this option. Details on what
â needs to be done should most likely be provided in /usr/share/doc/cacti.
â
â Otherwise, you should probably choose this option.
â
â Configure database for cacti with dbconfig-common?
â
â                                     <Yes>                                     <No>
â
#####
```

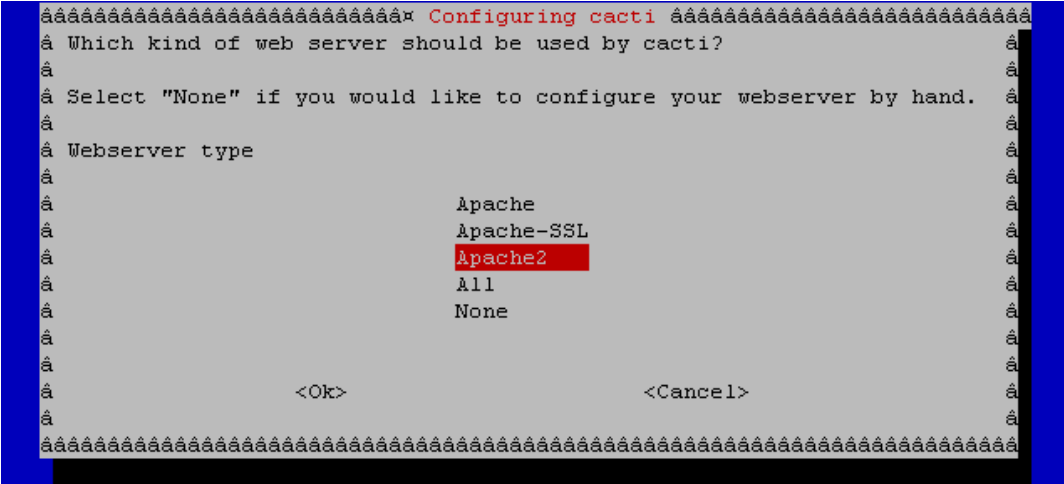
masukkan password MySQL pada user root@localhost



Jika diingin database MySQL untuk CACTI diberi password maka isi ini, disarankan tidak perlu memberi password...



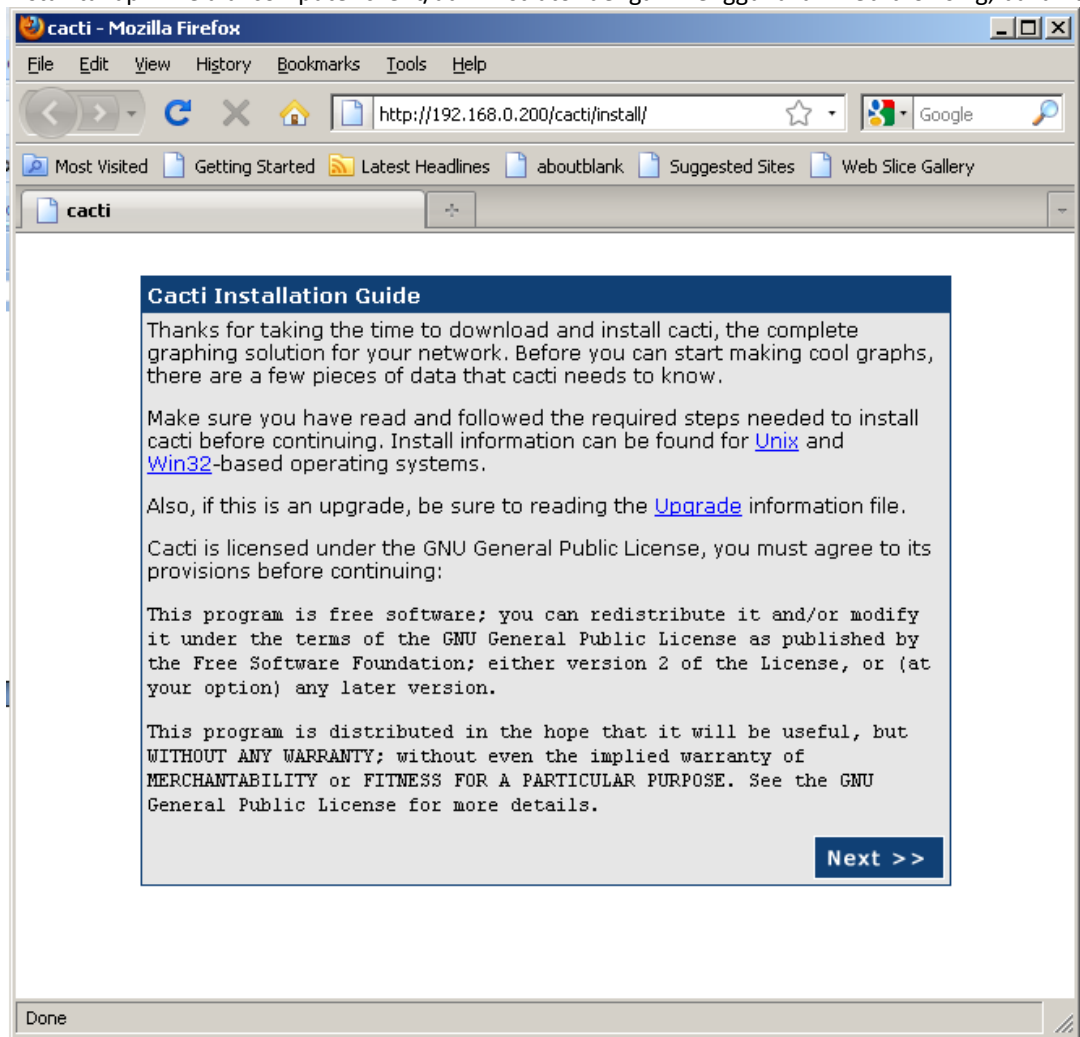
Memilih mesin web-server, pilih Apache2 atau kalau ingin menggunakan SSL pilih Apache-SSL...



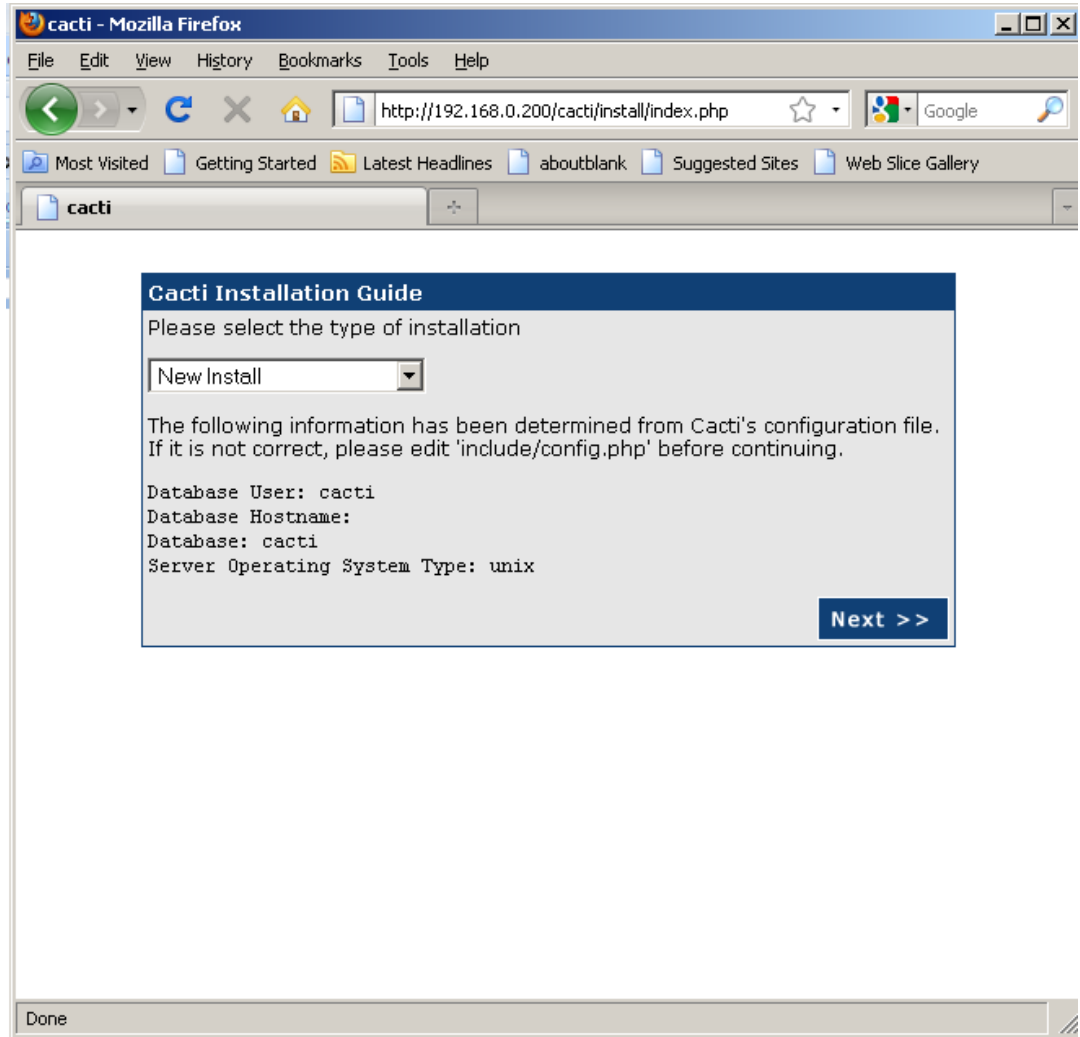
instalasi tahap pertama sukses...



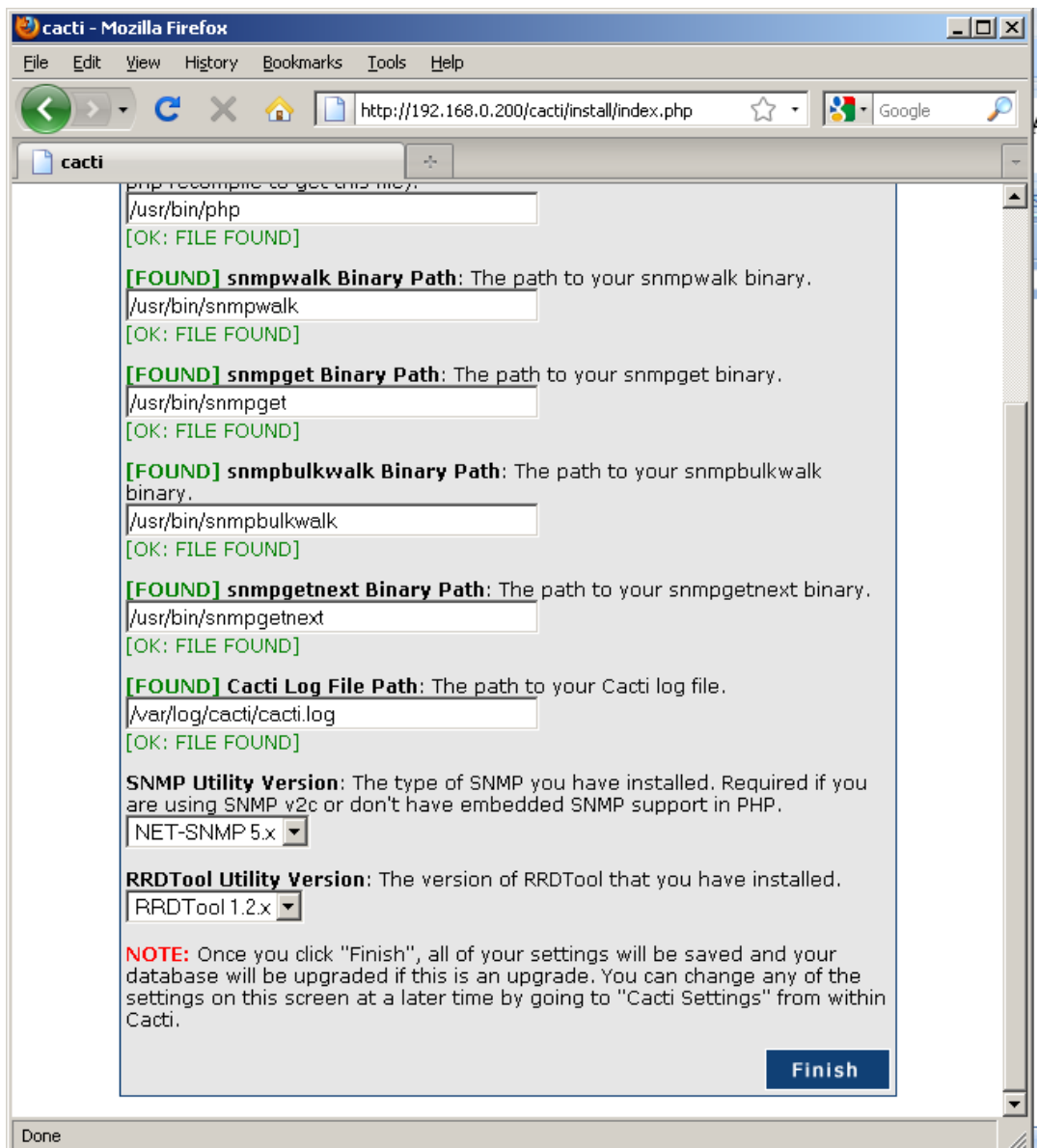
- Install tahap 2 melalui computer client/administrator dengan menggunakan web-browsing, buka [http://\[ip-server\]/cacti/install ...](http://[ip-server]/cacti/install...)



Click "Next >>" ...

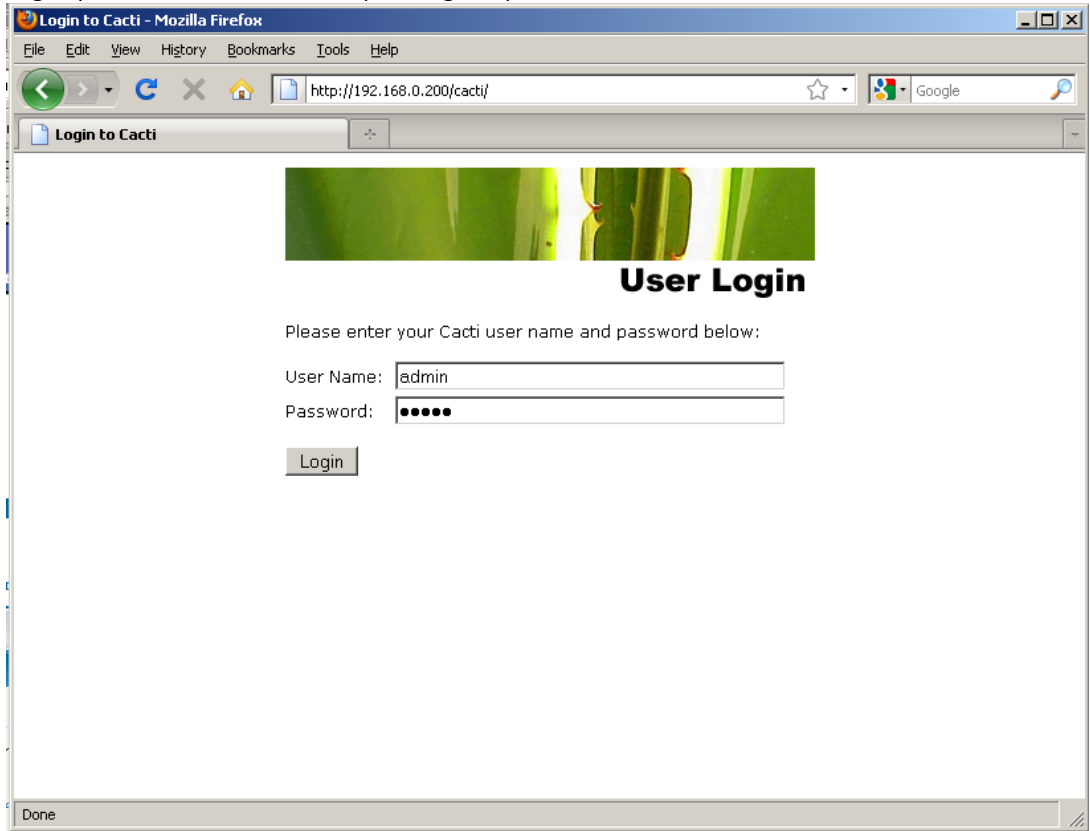


Click "Next >>" ...

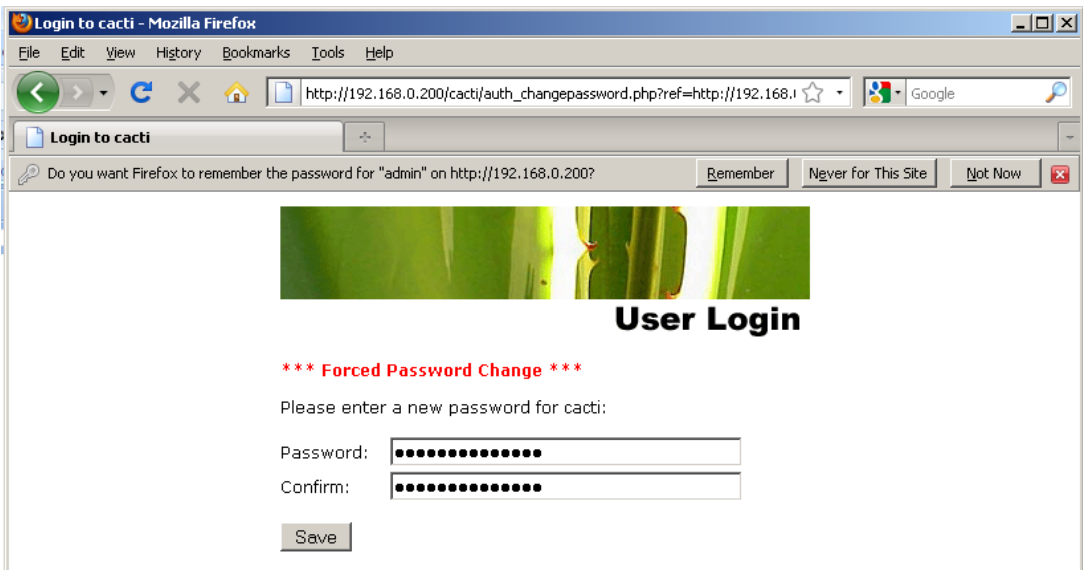


Pilih SNMP dan RRD Tool yang dipakai kemudian click “Finish”...

- Login, pertama akan muncul tampilan login seperti ini...

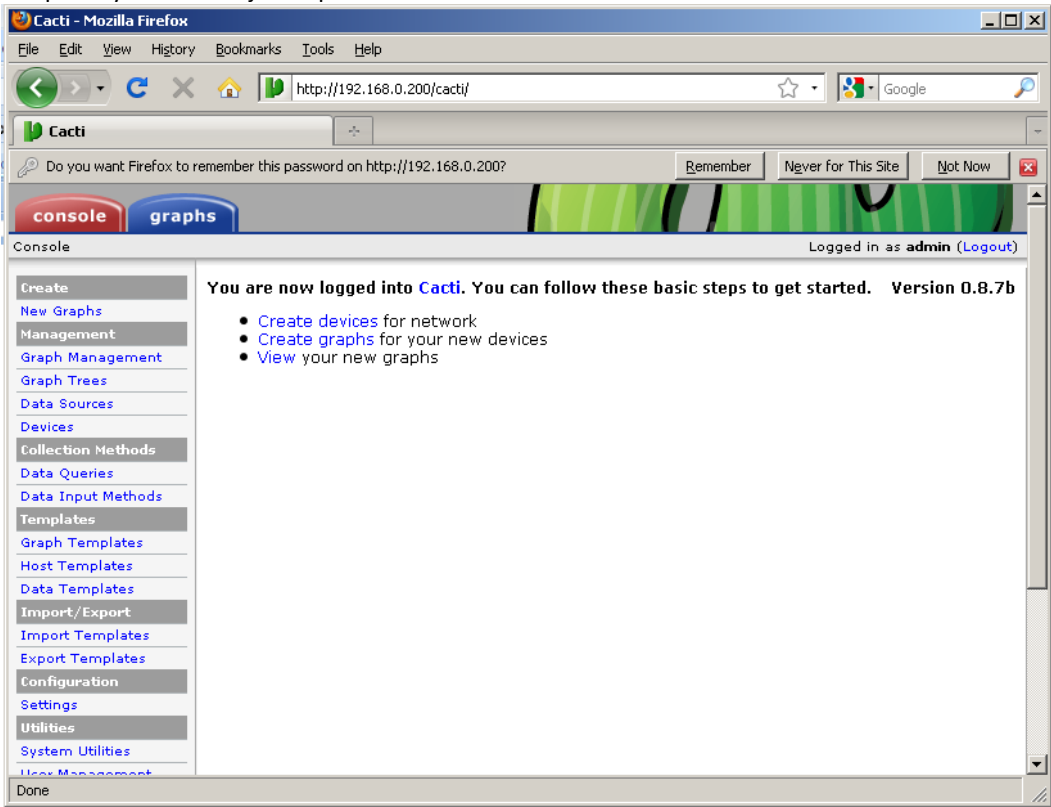


masukan username dan password “admin”



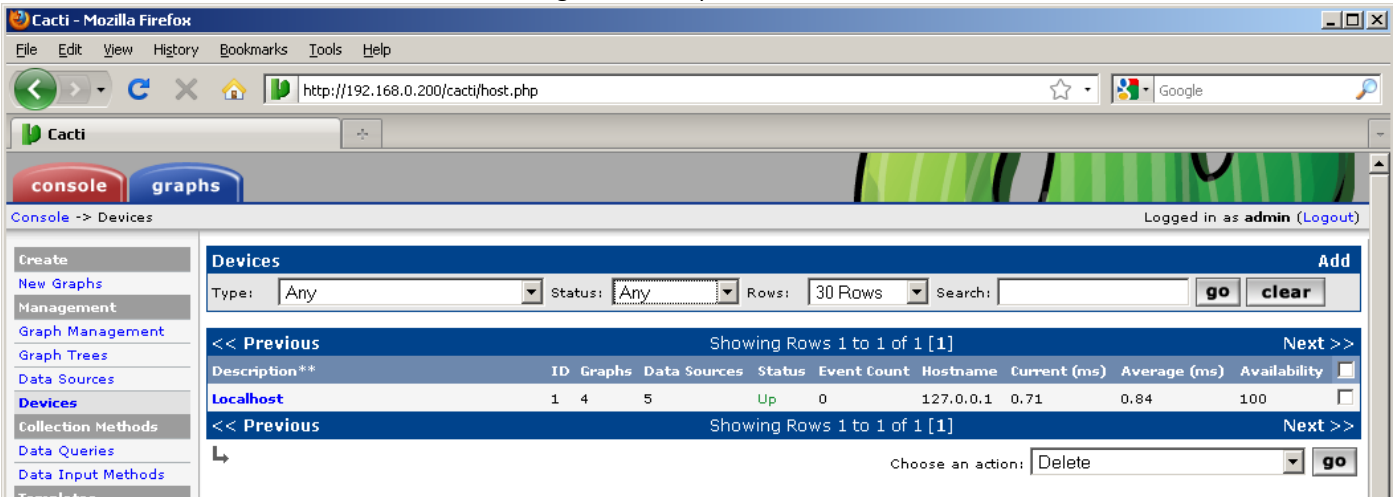
masukkan password baru untuk admin dan ulangi lagi, kemudian click “Save” ...

tampilannya akan menjadi seperti ini...



- Setup/Setting Device pada CACTI...

buat device baru, click menu sisi kiri dibawah management click pada device...



Click “Add” pada sisi kanan atas...

kemudian isinya ikutin sebagai berikut...

Form **Devices**



Devices [new]

Description

Give this host a meaningful description.

Persegi

Hostname

Fully qualified hostname or IP address for this device.

127.0.0.1

Host Template

Choose what type of host, host template this is. The host template will govern what kinds of data should be gathered from this type of host.

Local Linux Machine

Notes

Enter notes to this host.

Disable Host

Check this box to disable all checks for this host.

☐ Disable Host

Untuk “Description” bisa dirubah...

Form **SNMP Options** dan **Availability/Reachability Options**-nya...

Availability/Reachability Options

Downed Device Detection

The method Cacti will use to determine if a host is available for polling.  
*NOTE: It is recommended that, at a minimum, SNMP always be selected.*

Ping and SNMP

Ping Method

The type of ping packet to sent.  
*NOTE: ICMP on Linux/UNIX requires root privileges.*

UDP Ping

Ping Port

TCP or UDP port to attempt connection.

23

Ping Timeout Value

The timeout value to use for host ICMP and UDP ping. This host SNMP timeout value applies for SNMP pings.

400

Ping Retry Count

The number of times Cacti will attempt to ping a host before failing.

1

SNMP Options

SNMP Version

Choose the SNMP version for this device.

Version 2

SNMP Community

SNMP read community for this device.

root

SNMP Port

Enter the UDP port number to use for SNMP (default is 161).

161

SNMP Timeout

The maximum number of milliseconds Cacti will wait for an SNMP response (does not work with php-snmp support).

500

Maximum OID's Per Get Request

Specified the number of OID's that can be obtained in a single SNMP Get request.  
*NOTE: This feature only works when using Spine*

10

cancel

create

kemudian click “create”

Kalau berhasil dan SNMP berjalan normal di CACTI, maka akan muncul tulisan disisi kiri atas seperti ini...

dit)

Logged in as admin (Logout)

Save Successful.

Persegi (127.0.0.1)

SNMP Information

System: Linux persegi 2.6.28-15-server #49-Ubuntu SMP Tue Aug 18 19:30:06 UTC 2009 i686  
Uptime: 927517 (0 days, 2 hours, 36 minutes)  
Hostname: persegi  
Location: dns.persegi.net  
Contact: th@opikdesign.com

Create Graphs for this Host

Scroll kebawah sampai muncul...

Associated Graph Templates

Graph Template Name

Status

1) Linux - Memory Usage

Not Being Graphed

2) Unix - Load Average

Not Being Graphed

3) Unix - Logged in Users

Not Being Graphed

4) Unix - Processes

Not Being Graphed

Add Graph Template:

Cisco - CPU Usage

add

Associated Data Queries

Data Query Name

Debugging

Re-Index Method

Status

1) Unix - Get Mounted Partitions

(Verbose Query)

Uptime Goes Backwards

Success [12 Items, 6 Rows]

Add Data Query:

Karlnet - Wireless Bridge Statistics

Re-Index Method:

Uptime Goes Backwards

add

cancel

save

Untuk form **Associated Data Queries**...

Hapus... **1) Unix - Get Mounted Partitions**, dengan click tanda silang merah.  
kemudian **Add Data Query** pilih “**SNMP - Get Mounted Partitions**” dengan **Re-Index Method** pilih “**Verify All Field**” click add.  
ulangi, **Add Data Query** pilih “**SNMP - Get Processor Information**” dengan **Re-Index Method** pilih “**Verify All Field**” click add.  
terakhir, **Add Data Query** pilih “**SNMP - Interface Statistic**” dengan **Re-Index Method** pilih “**Verify All Field**” click add.

Tampilan akan menjadi seperti ini...



Associated Data Queries			
Data Query Name	Debugging	Re-Index Method	Status
1) SNMP - Get Mounted Partitions	(Verbose Query)	Verify All Fields	Success [39 Items, 13 Rows]
2) SNMP - Get Processor Information	(Verbose Query)	Verify All Fields	Success [1 Item, 1 Row]
3) SNMP - Interface Statistics	(Verbose Query)	Verify All Fields	Success [35 Items, 4 Rows]
Add Data Query: <span>Karlnet - Wireless Bridge Statistics</span>		Re-Index Method: <span>Uptime Goes Backwards</span>	<span>add</span>

Lihat status-status pada form **Associated Data Queries** seharusnya **Success** kalau SNMP sudah berhasil melakukan Query pada mesin Linux.

Kemudian pada form **Associated Graph Templated** tambahkan SNMP template...

**Add Graph Templated** pilih **“SNMP - Generic OID Template”** click add.

Tampilan keseluruhan akan menjadi sebagai berikut...

Associated Graph Templates

Graph Template Name	Status
1) Linux - Memory Usage	Not Being Graphed
2) SNMP - Generic OID Template	Not Being Graphed
3) Unix - Load Average	Not Being Graphed
4) Unix - Logged in Users	Not Being Graphed
5) Unix - Processes	Not Being Graphed

Add Graph Template: Cisco - CPU Usageadd

Associated Data Queries

Data Query Name	Debugging	Re-Index Method	Status
1) SNMP - Get Mounted Partitions	(Verbose Query)	Verify All Fields	Success [39 Items, 13 Rows]
2) SNMP - Get Processor Information	(Verbose Query)	Verify All Fields	Success [1 Item, 1 Row]
3) SNMP - Interface Statistics	(Verbose Query)	Verify All Fields	Success [35 Items, 4 Rows]

Add Data Query: Karlnet - Wireless Bridge StatisticsRe-Index Method: Uptime Goes Backwardsadd

cancelsave

Kemudian click “save”...

Tampilan akan kembali seperti ini...

Cacti - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.0.200/cacti/host.php

Cacti

consolegraphs

Console -> Devices

Logged in as admin (Logout)

Create

New Graphs

Management

Graph Management

Graph Trees

Data Sources

Devices

Collection Methods

Data Queries

Data Input Methods

Templates

Graph Templates

Host Templates

Save Successful.

Devices

Type: AnyStatus: AnyRows: 30 RowsSearch: go clear

<< Previous

Showing Rows 1 to 2 of 2 [1]

Next >>

Description**	ID	Graphs	Data Sources	Status	Event Count	Hostname	Current (ms)	Average (ms)	Availability
localhost	1	4	5	Up	0	127.0.0.1	14.12	3.04	100
Persegi	2	0	0	Up	0	127.0.0.1	14.12	3.04	100

<< Previous

Showing Rows 1 to 2 of 2 [1]

Next >>

Choose an action: Deletego

Pada device yang tadi kita buat, sisi kanan beri tanda centang dan pada **Choose an Action** pilih **“Place on a Tree (Default Tree)”** click “go”...

Cacti - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.0.200/cacti/host.php

Cacti

consolegraphs

Console -> Devices -> Actions

Logged in as admin (Logout)

Create

New Graphs

Management

Graph Management

Graph Trees

Data Sources

Devices

Collection Methods

Data Queries

Data Input Methods

Templates

Graph Templates

Host Templates

Place on a Tree (Default Tree)

When you click save, the following hosts will be placed under the branch selected below.

- Persegi

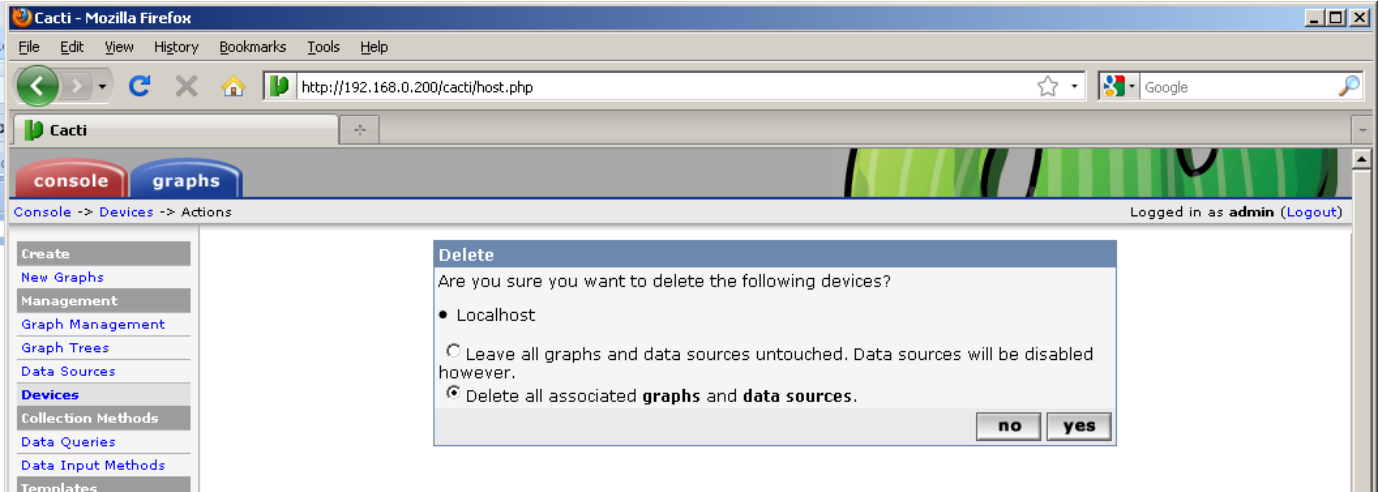
Destination Branch: [root]

noyes

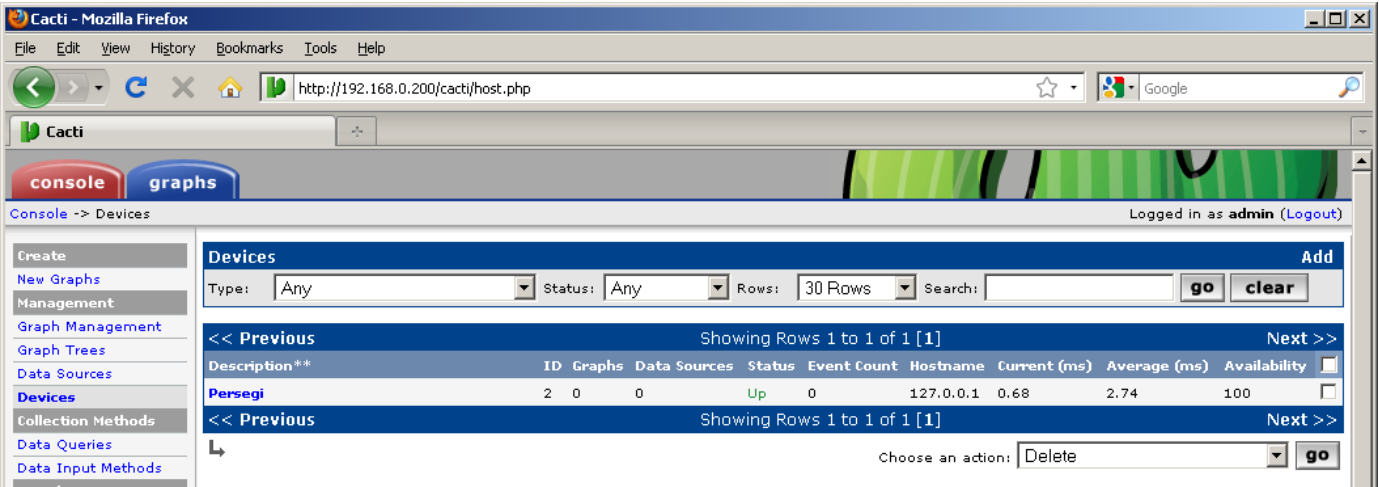
Pilih “yes”...

Kemudian device bawaan CACTI yaitu “localhost” di-delete...

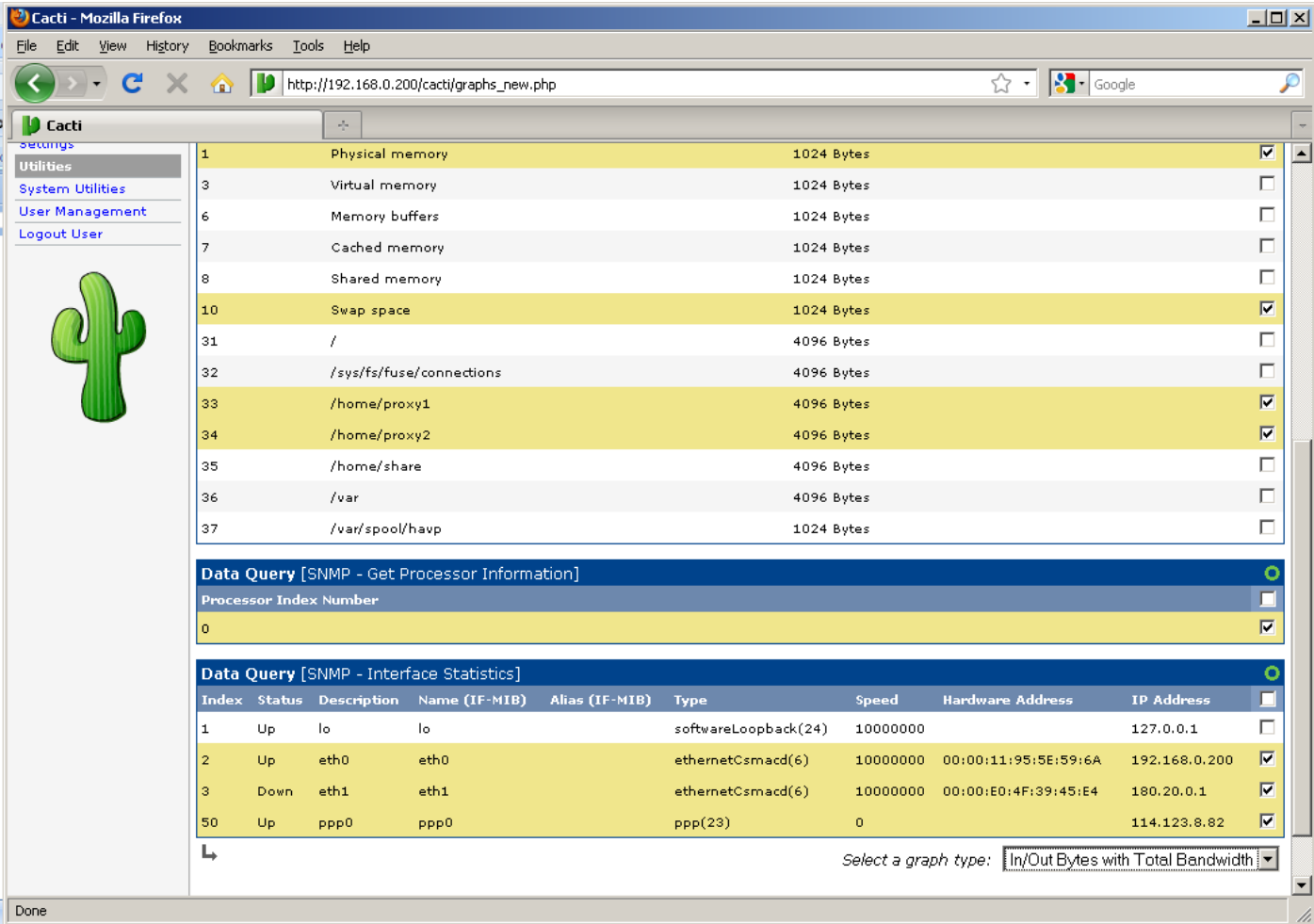
Pilih “Localhost” click sisi kanan kemudian **Choose an Action** pilih **“Delete”** click “go”...



Click “yes”... Tampilannya akan menjadi seperti ini...

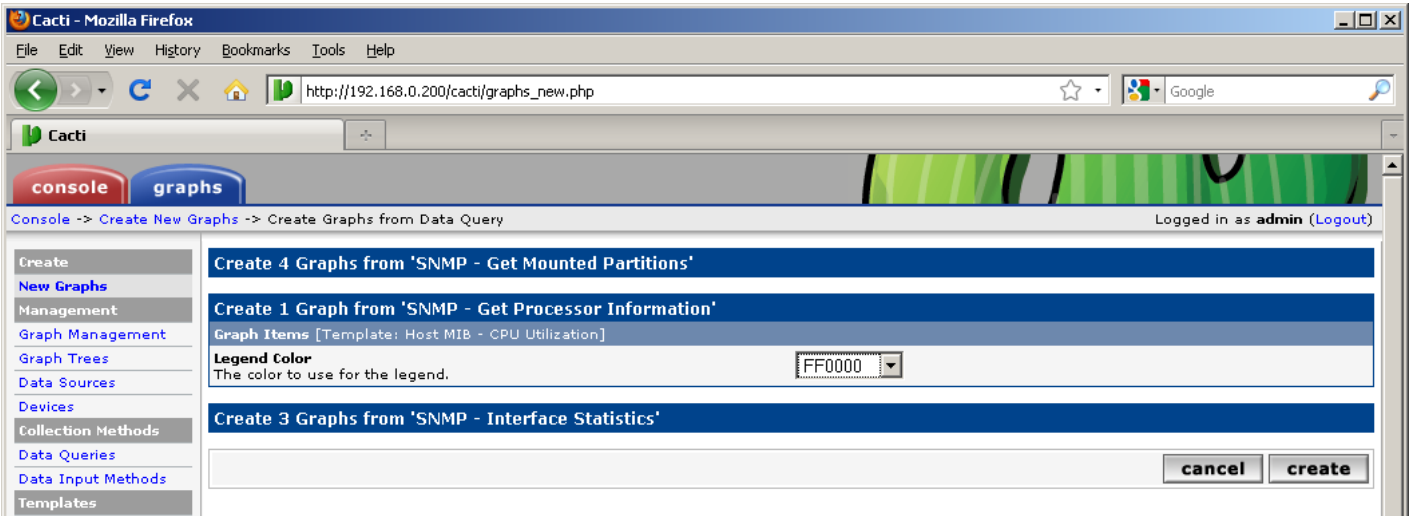


- Buat grafik, Click **“New Graphs”** pada **Create** Menu sisi kiri...



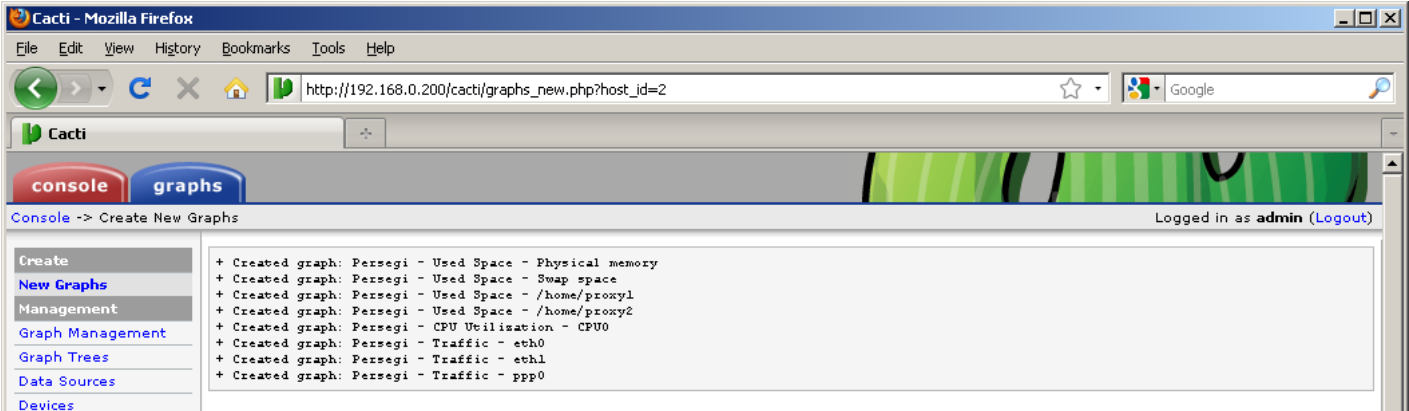
sesuaikan kebutuhan, misalnya penggunaan RAM dan Processor, b/w traffic transfer rate, sisa partisi hdd untuk proxy, dll.

beri tanda centang yang dimaksud untuk dibuat grafik-nya... click “create”.

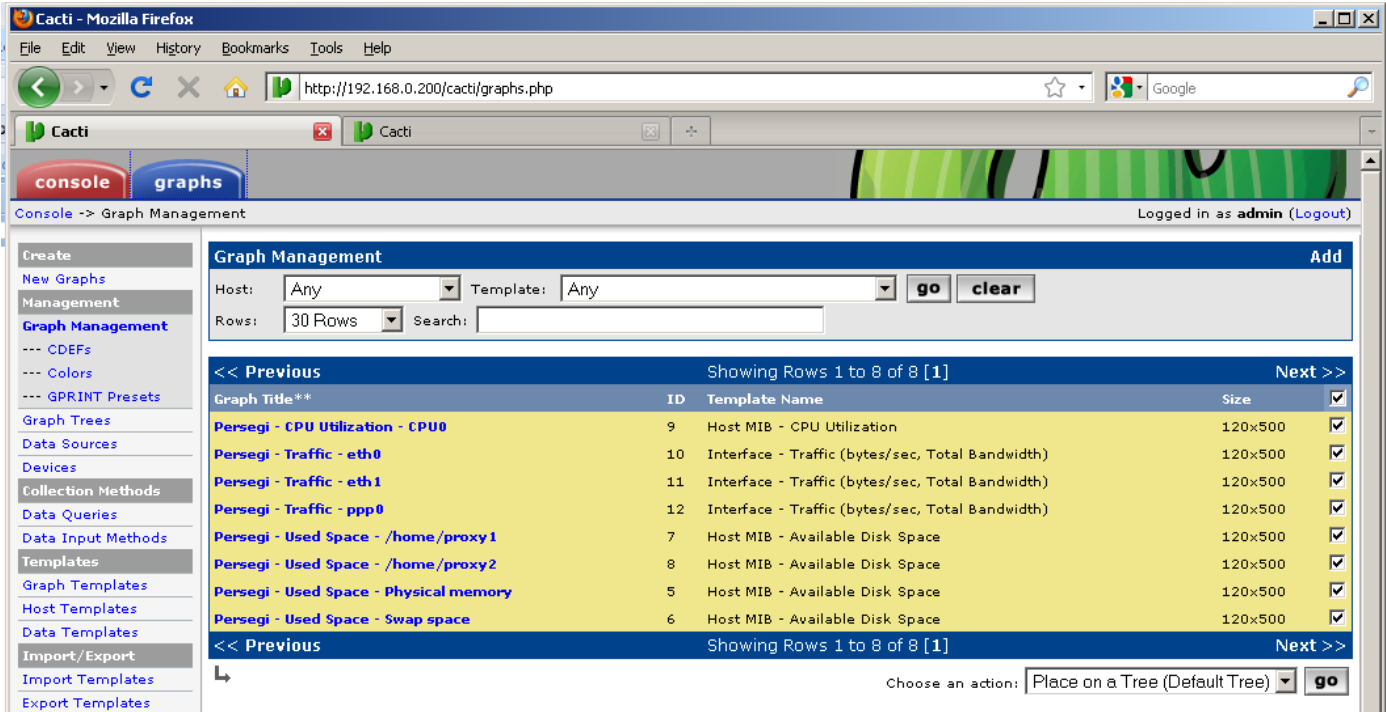


Click “create”...

kalau berhasil akan muncul tulisan “created graph: bla... bla... bla...”



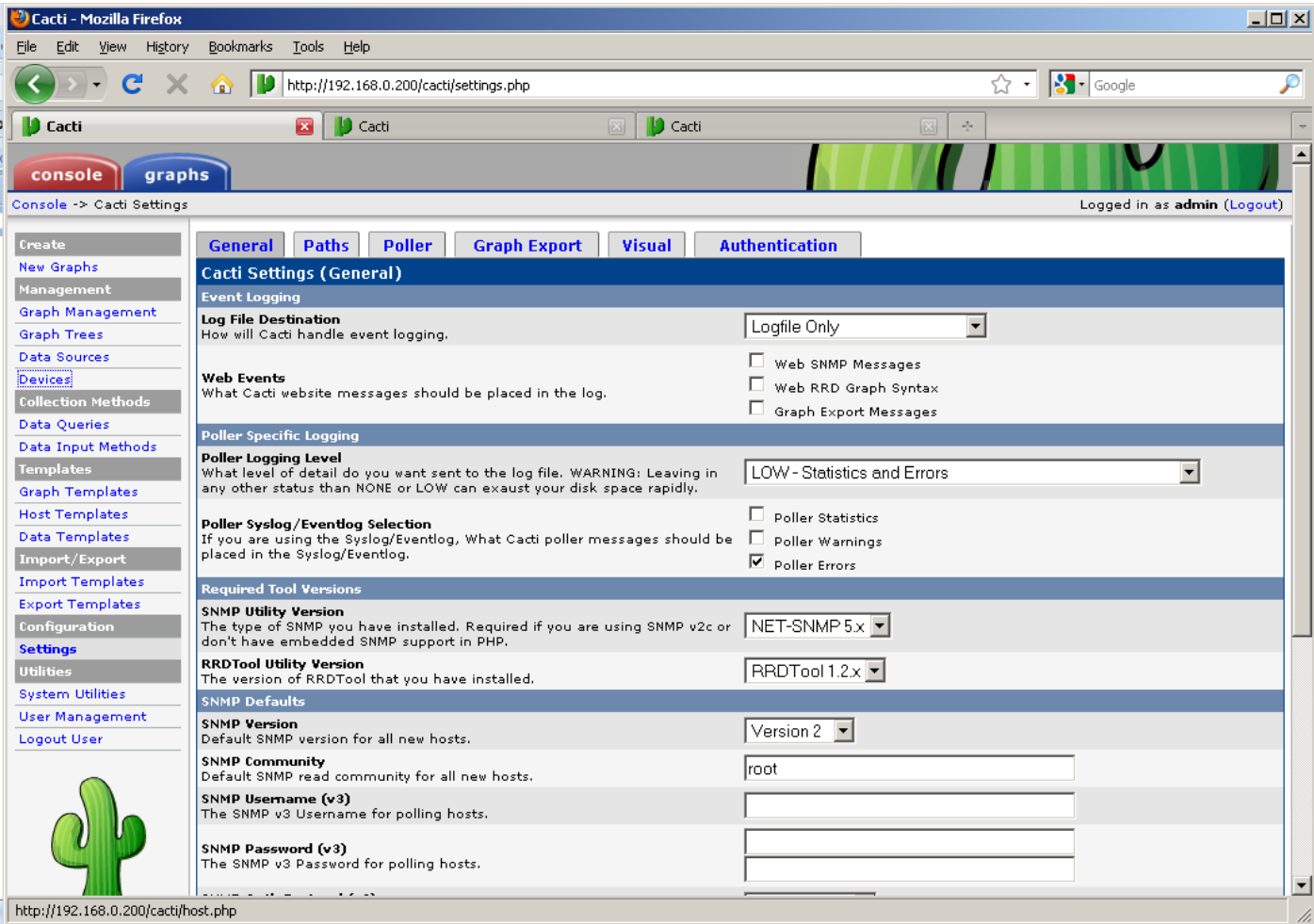
Terakhir, jadikan grafik yang sudah dibuat agar menjadi **Default Tree**, click “**Graph Management**”...



beri tanda centang disisi kanan pada semua grafik yang kita buat tadi dan pada **Choose an Action** pilih “**Place on a Tree (Default Tree)**” click “go”...

- Setting terakhir, agar cacti selalu melakukan poller setiap 5menit...

Pada menu sisi kiri click “Settings” pada Configuration...



Pada tab “General” Scroll kebawah... form “SNMP Defaults” isi seperti ini... setelah itu click “save”

<b>SNMP Defaults</b>	
<b>SNMP Version</b> Default SNMP version for all new hosts.	Version 2
<b>SNMP Community</b> Default SNMP read community for all new hosts.	root
<b>SNMP Username (v3)</b> The SNMP v3 Username for polling hosts.	
<b>SNMP Password (v3)</b> The SNMP v3 Password for polling hosts.	
<b>SNMP Auth Protocol (v3)</b> Choose the SNMPv3 Authorization Protocol.	MD5 (default)
<b>SNMP Privacy Passphrase (v3)</b> Choose the SNMPv3 Privacy Passphrase.	
<b>SNMP Privacy Protocol (v3)</b> Choose the SNMPv3 Privacy Protocol.	DES (default)
<b>SNMP Timeout</b> Default SNMP timeout in milli-seconds.	500
<b>SNMP Port Number</b> Default UDP port to be used for SNMP Calls. Typically 161.	161
<b>SNMP Retries</b> The number times the SNMP poller will attempt to reach the host before failing.	3

Kemudian pergi ke tab “Poller” dan scroll kebawah... form “Host Availability Settings” isi seperti ini... click “save”

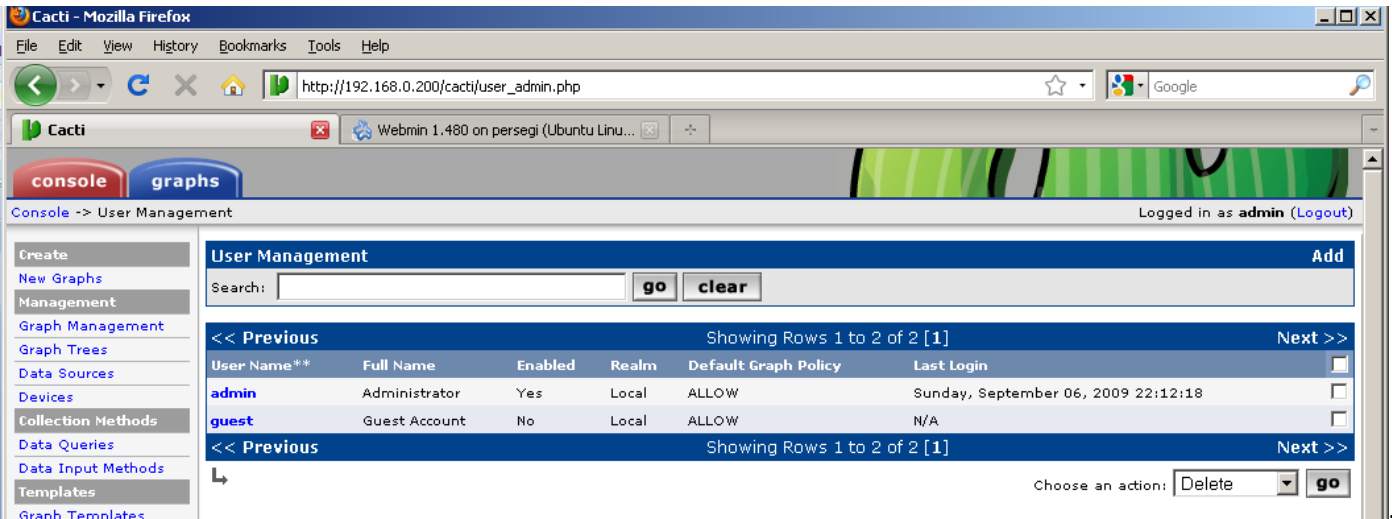
<b>Host Availability Settings</b>	
<b>Downed Host Detection</b> The method Cacti will use to determine if a host is available for polling. <i>NOTE: It is recommended that, at a minimum, SNMP always be selected.</i>	Ping and SNMP
<b>Ping Type</b> The type of ping packet to sent. <i>NOTE: ICMP requires that the Cacti Service ID have root privileges in Unix.</i>	UDP Ping
<b>Ping Port</b> When choosing either TCP or UDP Ping, which port should be checked for availability of the host prior to polling.	23
<b>Ping Timeout Value</b> The timeout value to use for host ICMP and UDP pinging. This host SNMP timeout value applies for SNMP pings.	400
<b>Ping Retry Count</b> The number of times Cacti will attempt to ping a host before failing.	1

Terakhir, tambahkan poller pada crontab... jalankan perintah dibawah ini...

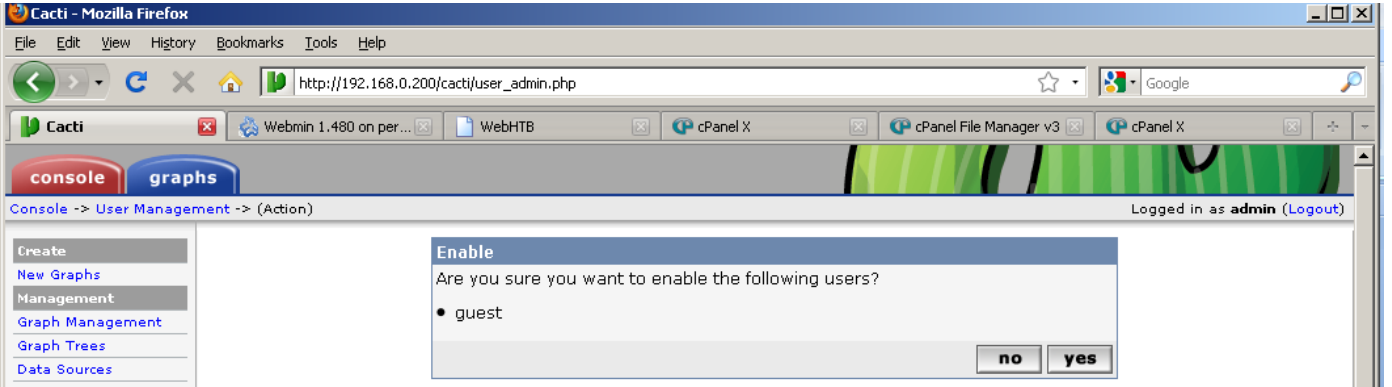
```
# echo "*/*5 * * * * /usr/share/cacti/site/poller.php > /dev/null 2>&1" >> /var/spool/cron/crontabs/root
```

- Kemudian aktifkan guest account agar akan melihat grafiknya tidak harus masuk ke account admin bertujuan settingan CACTI dirubah-rubah lagi.

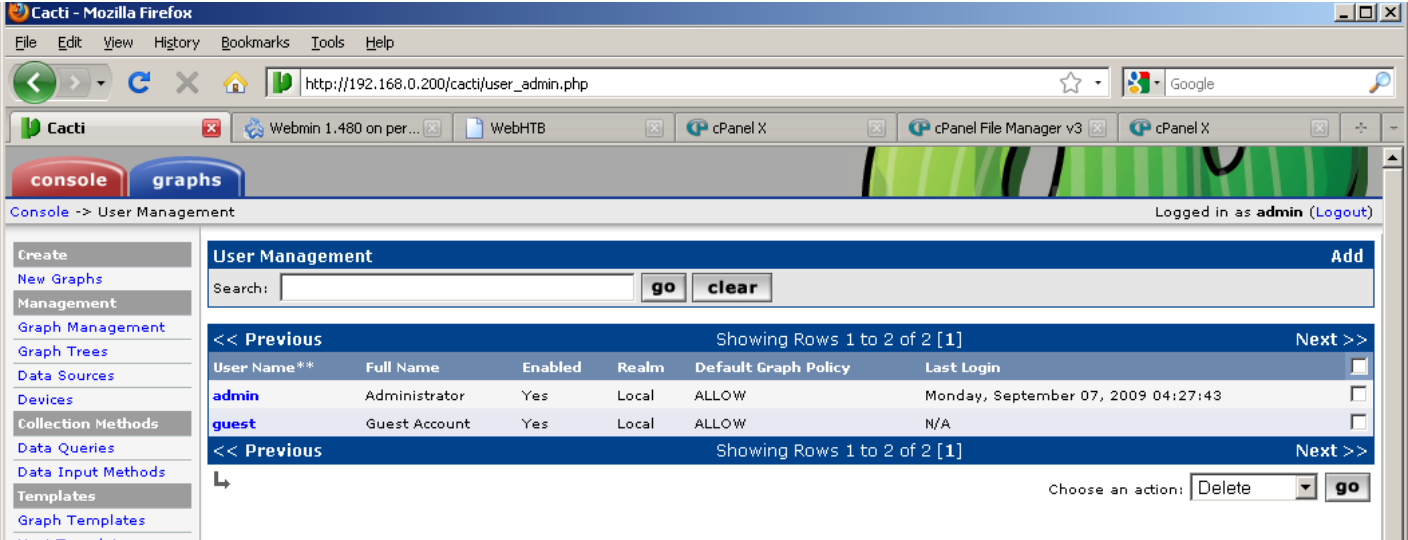
Pilih menu kiri di “Utilities” dan click “User Management”... tapilannya akan menjadi berikut..



Pada **“guest”** sisi kanan beri tanda centang kemudian pada **“Choose an action”** pilih **“Enable”** click “go”



click “yes”...



Click **“guest”** untuk mengedit account tersebut...  
kemudian paa form **User Management [edit: guest]**, Pada **“Account Options”** matikan/buang tanda centang pada **“User Must Change Password at Next Login”** dan **“Allow this User to Keep Custom Graph Settings”**... untuk **“Password”** isi **“guest”** ...  
jangan lupa click **“save”** ...

User Management [edit: guest]

User Name

The login name for this user.

guest

Full Name

A more descriptive name for this user, that can include spaces or special characters.

Guest Account

Password

Enter the password for this user twice. Remember that passwords are case sensitive!

.....

.....

Enabled

Determines if user is able to login.

☒ Enabled

Account Options

Set any user account-specific options here.

☐ User Must Change Password at Next Login

☐ Allow this User to Keep Custom Graph Settings

Graph Options

Set any graph-specific options here.

☒ User Has Rights to Tree View

☒ User Has Rights to List View

☒ User Has Rights to Preview View

Login Options

What to do when this user logs in.

☐ Show the page that user pointed their browser to.

☐ Show the default console screen.

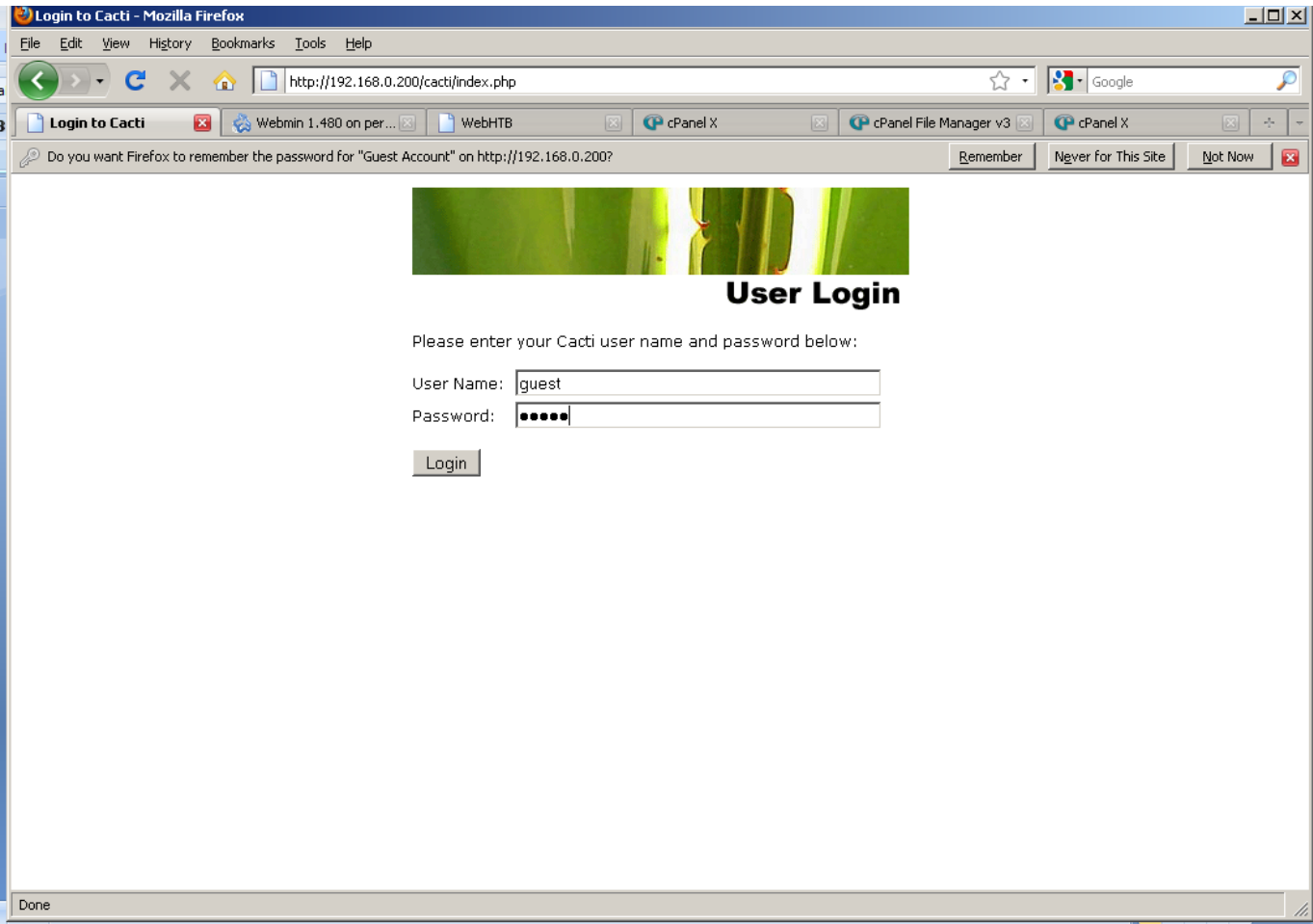
☒ Show the default graph screen.

Authentication Realm

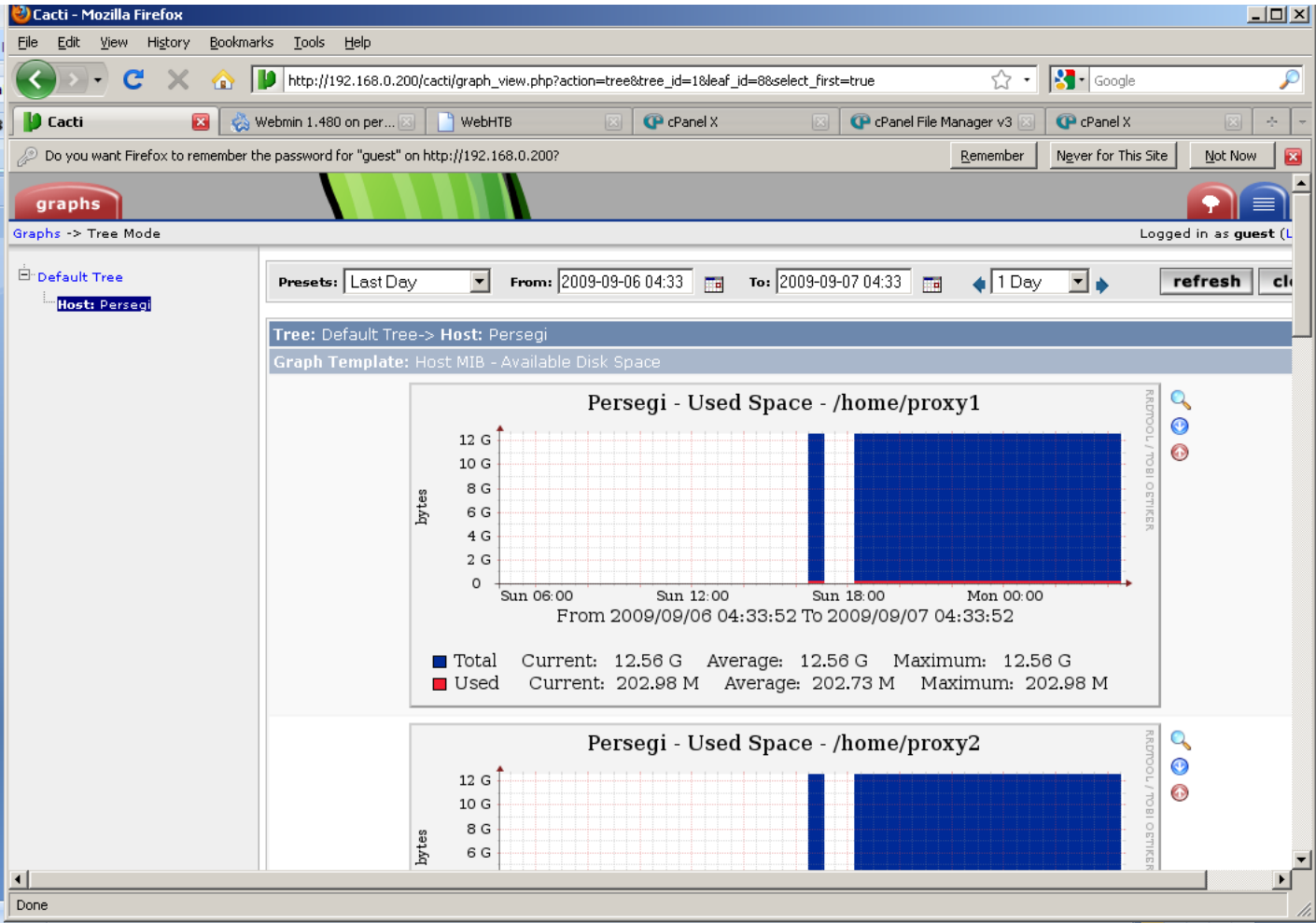
Only used if you have LDAP or Web Basic Authentication enabled. Changing this to an non-enabled realm will effectively disable the user.

Local

- Install sampai setting sudah selesai maka logout, tunggu 5menit agar CACTI mencatat semua grafiknya kemudian login kembali dengan user **“guest”** ....



- hasilnya grafiknya kurang lebih akan seperti ini....



**DEMIKIAN TUTORIAL MEMBUAT SERVER ALL IN ONE:  
ROUTER, SSH, DHCP SERVER, DNS SERVER, SAMBA & WINS SERVER,  
WEB CACHE DENGAN PROXY & ANTI VIRUS HAVP**

**YANG DILENGKAPI:  
SARG & CALAMARIS UNTUK MEMONITOR PROXY,  
FILTER FIREWALL DENGAN IP & MAC-ADDRESS,  
BANDWIDTH MANAGEMENT DENGAN MEMISAHKAN IIX DAN INTL,  
DAN CACTI SEBAGAI PEMANTAU KINERJA SERVER.**

**By:  
Taufiq Hidayat**

**e-mail: [th@opikdesign.com](mailto:th@opikdesign.com)  
mobile: 08123003336  
YM: opik1979**