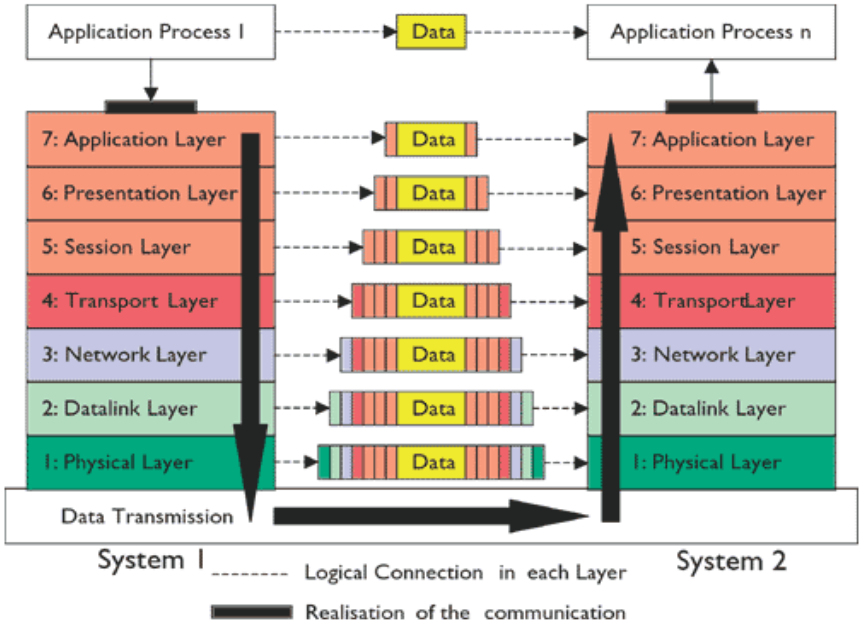
Kursus Online Linux
Linux Network Administrator

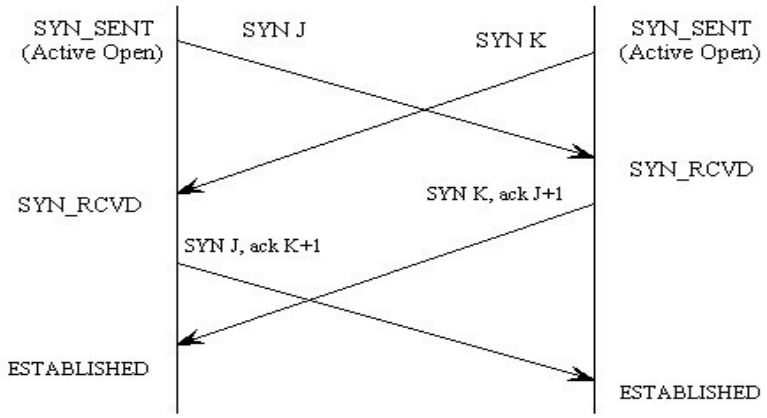
Budi Santosa,ST
linux.multimedia@gmail.com
www.kurusetra.web.id

Konsep TCP / IP

Layer OSI

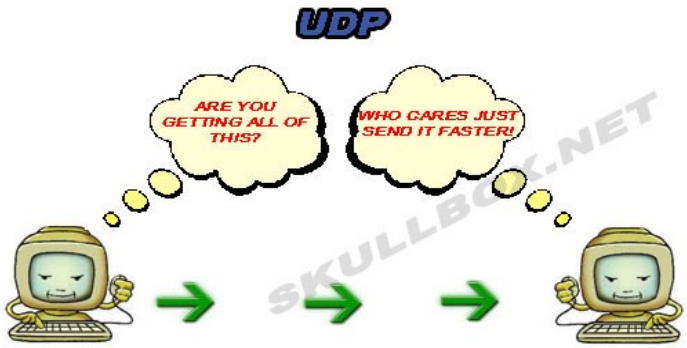


Transmission Control Protocol (TCP)



state transitions in simultaneous open

User Datagram Protocol (UDP)



Informasi Jaringan

Konfigurasi Alamat IP

root@server:~# **vim /etc/network/interfaces**

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 192.168.0.71
netmask 255.255.255.0

auto eth1
iface eth1 inet static
address 122.200.52.23
netmask 255.255.255.128
gateway 122.200.52.1
```

Ifconfig

root@budi-desktop:~# ifconfig

```
eth0      Link encap:Ethernet  HWaddr 02:39:ac:31:06:7d
          inet addr:192.168.20.1  Bcast:192.168.20.255  Mask:255.255.255.0
          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:43 Base address:0x2000
```

Network Statistic

root@budi-desktop:~# netstat -nr

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
0.0.0.0         10.20.31.24     0.0.0.0         UG        0 0          0 ppp0
10.8.0.0        0.0.0.0         255.255.255.0   U         0 0          0 tap0
10.20.31.24     0.0.0.0         255.255.255.255 UH        0 0          0 ppp0
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 ppp0
192.168.0.0     10.8.0.1        255.255.255.0   UG        0 0          0 tap0
192.168.20.0    0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

Hostname Lookup

root@budi-desktop:~# nslookup www.detik.com

```
Server:           10.17.125.230
Address:    10.17.125.230#53

Non-authoritative answer:
www.detik.com    canonical name = detik.com.
Name: detik.com
Address: 203.190.242.69
Name: detik.com
Address: 203.190.241.43
```

Network TOP

root@budi-desktop:~# apt-get install ntop
root@budi-desktop:~# ntop -u root -i eth0
Buka web browser kemudian ketik alamat http://127.0.0.1:3000

Network Mapping

root@budi-desktop:~# apt-get install nmap
root@budi-desktop:~# nmap -sP 192.168.20.0/24 (Scan alamat IP)
root@budi-desktop:~# nmap -sS 192.168.20.1 (Scan port number)

```
Starting Nmap 5.21 ( http://nmap.org ) at 2012-07-28 22:43 WIT
Nmap scan report for 192.168.20.1
Host is up (0.000011s latency).
Not shown: 979 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
110/tcp   open  pop3
```

Interface TOP

root@budi-desktop:~# apt-get install iftop
root@budi-desktop:~# iftop -i ppp0

```
interface: ppp0
IP address is: 10.231.116.232
MAC address is: 00:00:00:00:00:00
```

Service Whois

root@budi-desktop:~# whois 122.200.52.41

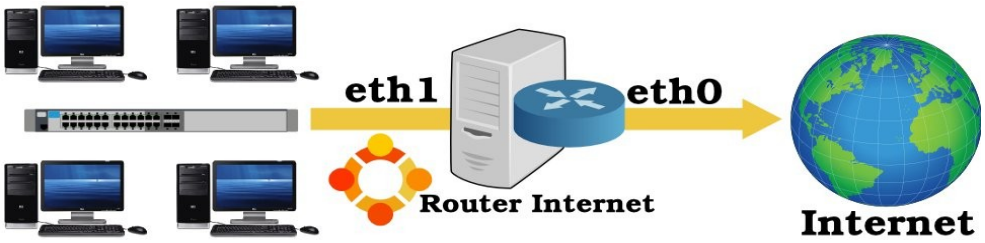
```
% [whois.apnic.net node-1]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

inetnum:        122.200.48.0 - 122.200.55.255
netname:        DIGINET-ID
descr:          PT Digital Wireless Indonesia
```

OS Fingerprinting

root@budi-desktop:~# apt-get install xprobe

root@budi-desktop:~# xprobe2 192.168.20.1

Router Internet



IP Forwarding

root@budi-desktop:~# vim /etc/sysctl.conf

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

Network Address Translation

root@budi-desktop:~# vim /etc/rc.local

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

exit 0

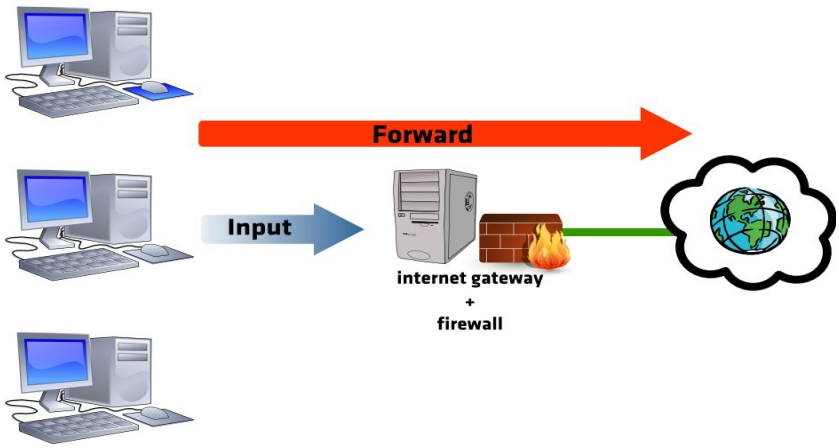
Dynamic Host Configuration Protocol

Instalasi DHCP
root@budi-desktop:~# apt-get install dhcpd
root@budi-desktop:~# vim /etc/default/udhcpd
Comment the following line to enable
#DHCPD_ENABLED="no"

Konfigurasi DHCP
root@budi-desktop:~# vim /etc/udhcpd.conf

```
start             192.168.20.20
end               192.168.20.254
interface         eth0
opt      dns      192.168.10.2 192.168.10.10
option   subnet   255.255.255.0
opt      router   192.168.20.1
opt      wins     192.16 8.20.1
option   domain   kurusetra.web.id
option   lease    864000          # 10 days of seconds
```

Firewall IPTables



Network Filtering
iptables -A INPUT -s 192.168.20.100 -j REJECT
iptables -A FORWARD -s 192.168.20.100 -j REJECT

iptables -A FORWARD -s 0/0 -d 202.46.1.2 -j REJECT
iptables -A FORWARD -s 0/0 -d www.yahoo.com -j REJECT

iptables -A INPUT -m iprange --src-range 192.168.20.50-192.168.20.70 -j REJECT

iptables -A FORWARD -m iprange --src-range 192.168.20.50-192.168.20.70 -j REJECT

iptables -A INPUT -m mac --mac-source f6:29:52:46:70:ba -j REJECT
iptables -A FORWARD -m mac --mac-source f6:29:52:46:70:ba -j REJECT

iptables -A FORWARD -o eth1 -p tcp --dport 25 -j REJECT
iptables -A FORWARD -o eth1 -p tcp --dport 4636:5000 -j REJECT
iptables -A FORWARD -o eth1 -p udp --dport 4636:5000 -j REJECT

iptables -A INPUT -m string --string facebook --algo kmp -j REJECT
iptables -A FORWARD -m string --string facebook --algo kmp -j REJECT

Manajemen Iptables
root@budi-desktop:~# iptables -L
```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
REJECT     all  --  192.168.20.100       anywhere            reject-with icmp-port-unreachable
REJECT      all  --  anywhere              anywhere               source IP range 192.168.20.50-
192.168.20.70 reject-with icmp-port-unreachable
REJECT     all  --  anywhere              anywhere              MAC F6:29:52:46:70:BA reject-with
icmp-port-unreachable
```

root@budi-desktop:~# iptables -D INPUT 1
root@budi-desktop:~# iptables -D INPUT 2

root@budi-desktop:~# iptables -F
root@budi-desktop:~# iptables -Z

Network Address Translation
iptables -t nat -A POSTROUTING -d 192.168.20.30 -j SNAT --to 192.168.20.1
iptables -t nat -A POSTROUTING -d 192.168.20.23 -j SNAT --to 192.168.20.22

iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 2244 -j DNAT --to 192.168.20.20:22
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 25 -j DNAT --to 192.168.20.50:25
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 110 -j DNAT --to 192.168.20.50:110
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to 192.168.20.100

root@budi-desktop:~# iptables -t nat -L
```
Chain PREROUTING (policy ACCEPT)
target     prot opt source               destination
DNAT       tcp  --  anywhere             anywhere            tcp dpt:2244 to:192.168.20.20:22
DNAT       tcp  --  anywhere             anywhere            tcp dpt:smtp to:192.168.20.50:25
DNAT       tcp  --  anywhere             anywhere            tcp dpt:pop3 to:192.168.20.50:110
DNAT       tcp  --  anywhere             anywhere            tcp dpt:http to:192.168.20.100
```

root@budi-desktop:~# iptables -t nat -F
root@budi-desktop:~# iptables -t nat -Z

Startup Firewall dan NAT
Buat Script
root@budi-desktop:~# vim /usr/sbin/firewall
iptables -A FORWARD -p tcp --dport 5000:6000 -j REJECT
iptables -A FORWARD -s 192.168.20.34 -d 0/0 -j REJECT

root@budi-desktop:~# chmod 755 /usr/sbin/firewall
root@budi-desktop:~# vim /etc/rc.local
/usr/sbin/firewall
exit 0

SQUID PROXY SERVER

Konfigurasi Repository Ubuntu

vim /etc/apt/sources.list
deb http://dl2.foss-id.web.id/ubuntu hardy main universe multiverse restricted
deb http://dl2.foss-id.web.id/ubuntu hardy-updates main universe multiverse restricted
apt-get update

Instalasi Squid

Aplikasi squid secara default sudah tersedia pada distro Linux (Red Hat, Mandrake, Susse dan Debian). Untuk meng-install squid anda harus login sebagai superuser (root), mount cdrom dan kemudian mengetikkan perintah;

apt-get update
apt-get install squid
vim /etc/squid/squid.conf

Paket secara otomatis akan terinstall, sedangkan file konfigurasi berada di direktori /etc/squid/squid.conf.

Konfigurasi Squid

Squid secara default berkomunikasi dengan klien melalui **port** 3128 yang ditunjukan file konfigurasi /etc/squid/squid.conf.

```
visible_hostname gw.ardelindo.com
http_port 3128 transparent
# 512 / 2 = 256
# cache_mem = ½ memory fisik (RAM)
cache_mem  128 MB
cache_swap_low 94
cache_swap_high 96
maximum_object_size 1000096 KB
maximum_object_size_in_memory 8000 KB
ipcache_size 1024
ipcache_low 90
ipcache_high 95
```

```
cache_replacement_policy lru
memory_replacement_policy lru
#cache_dir   ufs   tempat_direktori  kapasitas level 1   level 2
cache_dir ufs /var/spool/squid  100  16  256
pid_filename /var/run/squid.pid
debug_options ALL,1
cache_access_log /var/log/squid/access.log
cache_log /var/log/squid/cache.log
cache_store_log /var/log/squid/store.log
dns_nameservers 202.134.1.10 202.134.0.155
```

Access Control List

```
acl LAN1 src 192.168.0.0/255.255.255.0
acl LAN2 src 10.0.0.0/255.255.0.0
acl admin src 192.168.0.100/255.255.255.255
acl admin2 src "/etc/squid/admin2"
acl multimedia urlpath_regex "/etc/squid/multimedia"
acl situs url_regex "/etc/squid/situs"
acl pagi time 08:00-12:00
acl istirahat time 12:00-13:00
acl siang time 13:00-18:00

# operator
http_access allow admin
http_access allow admin2
http_access deny pagi multimedia
http_access deny situs
http_access allow LAN1
http_access deny pagi LAN2
http_access deny all

# File: vim /etc/squid/multimedia
\.iso$
\.mp3$
\.3gp$

# File: vim /etc/squid/situs
youtube
friendster
hi5
flickr
photobucket
liveconnector

# File: vim /etc/squid/admin2
192.168.0.34
192.168.0.37
192.168.0.200
```

Samba Filesharing

Penambahan user

```
#Departemen MIS
adduser budi
adduser ahmad
adduser dani

smbpasswd -a budi
smbpasswd -a ahmad
smbpasswd -a dani

groupadd mis
gpasswd -a budi mis
gpasswd -a ahmad mis
gpasswd -a dani mis

mkdir /home/mis
chown -R budi.mis /home/mis
chmod -R 775 /home/mis

#Departemen Accounting
adduser heri
adduser lia
adduser yuni

smbpasswd -a heri
smbpasswd -a lia
smbpasswd -a yuni
groupadd accounting
gpasswd -a heri
gpasswd -a lia
gpasswd -a yuni

mkdir /home/accounting
chown -R heri.accounting /home/accounting
chmod -R 775 /home/accounting
#Departemen purchasing
useradd rony
useradd sherly
useradd siti

smbpasswd -a rony
smbpasswd -a sherly
smbpasswd -a siti

groupadd purchasing
gpasswd -a rony
```

gpasswd -a sherly
gpasswd -a siti

mkdir /home/purchasing
chown -R rony.purchasing /home/purchasing
chmod -R 775 /home/purchasing

Konfigurasi Global
[global]
worksgrop = KURUSETRA
netbios name = DATACENTER
server string = %h server (Samba, Ubuntu)
wins support = yes
local master = yes

Share Folder
[MIS]
path = /home/mis
valid users = @mis
write list = budi dani
read list = ahmad
browseable = yes
inherit permissions = yes
force create mode = 0775
force directory mode = 0775
force group = mis

[ACCOUNTING]
nt acl support = yes
veto files = /*.mp3/*.mpeg/*.mpg/*.avi/*.asf/*.wmv/*.3gp/*.dat/*.iso/*.exe/
delete veto files = yes
path = /home/accounting
valid users = @accounting
browseable = yes
writeable = yes
inherit permissions = yes
force create mode = 0775
force directory mode = 0775
force group = accounting

```
[PURCHASING]
nt acl support = yes
veto files = /*.mp3/*.mpeg/*.mpg/*.avi/*.asf/*.wmv/*.3gp/*.dat/*.iso/*.exe/
delete veto files = yes
path = /home/purchasing
valid users = rony sherly siti
browseable = yes
writeable = yes
inherit permissions = yes

Module Recycle Bin
[MIS]
vfs object = recycle audit extd_audit
recycle:repository = ../sampah/%u
recycle:keeptree = Yes
recycle:versions = Yes

path = /home/mis
valid users = @mis
write list = budi dani
read list = ahmad
browseable = yes
inherit permissions = yes
force create mode = 0777
force directory mode = 0777
force group = mis


[ACCOUNTING]
vfs object = recycle audit extd_audit
recycle:repository = ../sampah/%u
recycle:keeptree = Yes
recycle:versions = Yes

nt acl support = yes
veto files = /*.mp3/*.mpeg/*.mpg/*.avi/*.asf/*.wmv/*.3gp/*.dat/.recycle/
delete veto files = yes
path = /home/accounting
valid users = heri lia yuni
browseable = yes
writeable = yes
inherit permissions = yes
force create mode = 0777
force directory mode = 0777
force group = accounting
```

```
[PURCHASING]
vfs object = recycle audit extd_audit
recycle:repository = ../sampah/%u
recycle:keeptree = Yes
recycle:versions = Yes

nt acl support = yes
veto files = /*.mp3/*.mpeg/*.mpg/*.avi/*.asf/*.wmv/*.3gp/*.dat/.recycle/
delete veto files = yes
path = /home/purchasing
valid users = rony sherly siti
browseable = yes
writeable = yes
inherit permissions = yes
force create mode = 0777
force directory mode = 0777
force group = purchasing
```

File Transfer Protokol

Instalasi FTP Server

```
root@budi-desktop:~# apt-get install proftpd-basic
root@budi-desktop:~# /etc/init.d/proftpd restart
```

Konfigurasi ProFTPD

```
root@budi-desktop:~# vim /etc/proftpd/proftpd.conf
# Use this to jail all users in their homes
DefaultRoot                     ~

# Users require a valid shell listed in /etc/shells to login.
# Use this directive to release that constrain.
RequireValidShell               off
```

Penambahan User FTP

```
adduser didik
adduser doni
adduser ahmad
```

Domain Name System Server

Konfigurasi DNS Server Bind9
Kalian pernah mendengar yang namanya DNS Server, pasti sudah khan, karena DNS Server merupakan komponen terpenting dalam jaringan internet. Fungsi DNS Server adalah untuk menterjemahkan nama komputer menjadi alamat IP, www.kurusetra.web.id menjadi 192.168.1.100. Agar aplikasi web browser bisa tersambung dengan server web yang dituju. Selain itu fungsi DNS juga untuk melakukan manajemen domain internet dan sebagai Mail Exchange.
Tutorial kali ini membahas konfigurasi DNS Server BIND9 pada sistem operasi linux ubuntu. Untuk lebih mudahnya kita gunakan aplikasi Webmin, web based system administrator tools yang berjalan pada port 10000 dan https. Webmin dapat di download di www.webmin.com dengan pilihan paket Debian. Konfigurasi kita bahas untuk melakukan manajemen domain kurusetra.web.id dengan nama komputer www, mail, vpn dan ftp. Langkah yang perlu kita lakukan adalah;

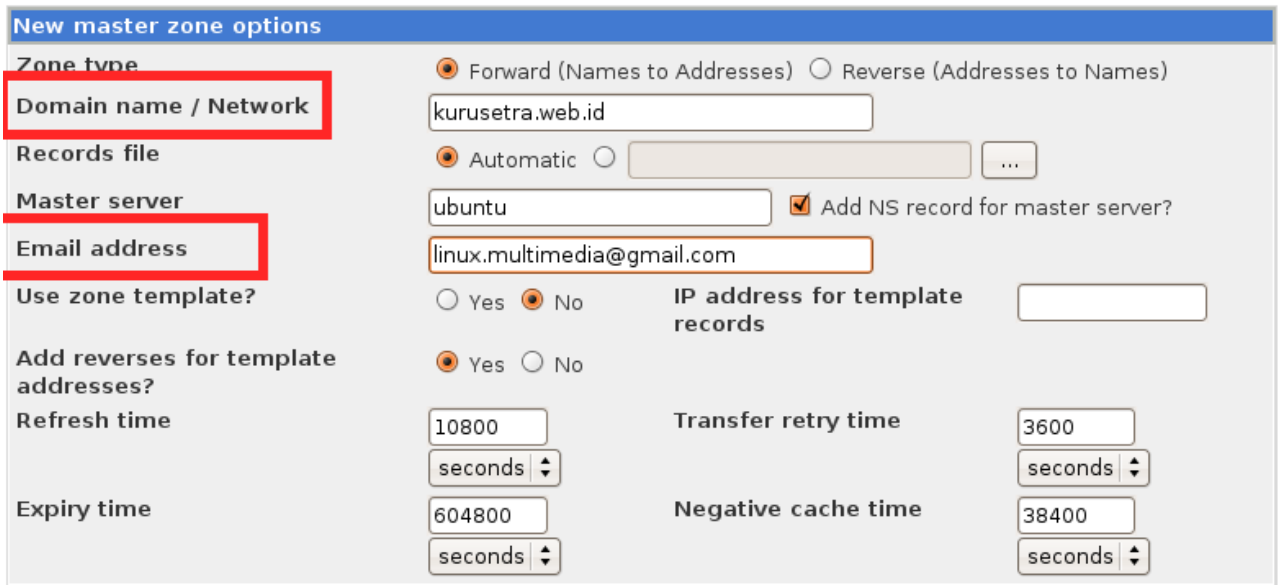
Instalasi Webmin
root@ubuntu:~# dpkg -i webmin_1.580_all.deb
root@ubuntu:~# apt-get -f install
root@ubuntu:~# /etc/init.d/webmin restart

Instalasi Bind9
root@ubuntu:~# apt-get install bind9

Login ke Webmin
Setelah ada tampilan login, masukan user root dan password.

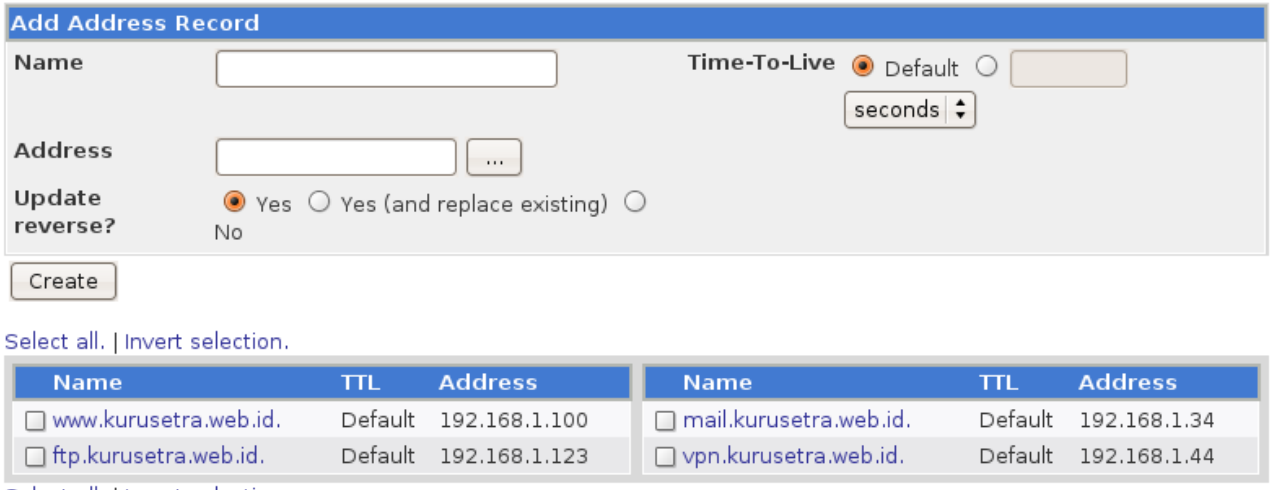
Konfigurasi Bind9
Pilih pada Un-used Modules → klik **BIND DNS Server**, setelah tampil konfigurasi lihat **Existing DNS Zones** dan klik **Create master zone**.

Konfigurasi Domain
Setelah tampil Create Master Zone, masukan di textfield Domain name / Network: kurusetra.web.id dengan Email address: linux.multimedia@gmail.com kemudian klik buton Create. Yang lain biarkan default.



Konfigurasi Master Zone
Sekarang yang kita lakukan adalah menambahkan nama komputer. Pada Tampilan Edit Master Zone klik icon Komputer Address (0).

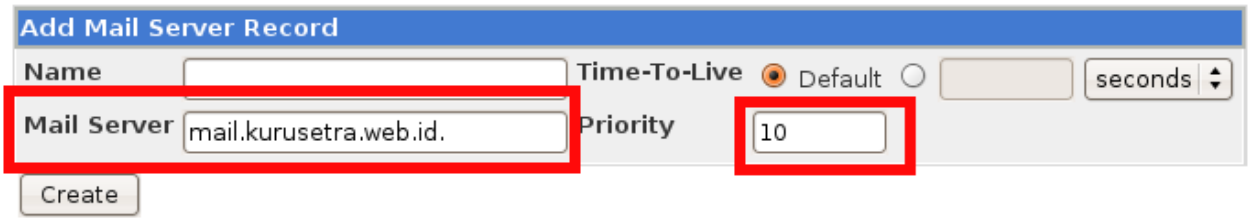
Konfigurasi Address Records
Konfigurasi address record ini untuk menambahkan nama komputer beserta alamat IP. Isi textfield Name: www dan 192.168.1.100 , kemudian klik Create



Ulangi prosesnya untuk nama komputer mail (192.168.1.34), ftp (192.168.1.123) dan vpn (192.168.1.44). Setelah semua selesai klik link **Return to zone list**.

Kemudian klik pojok kanan atas link **Apply Configuration**.

MX Record



Pengujian DNS Server

Untuk menguji DNS Server kita edit file /etc/resolv.conf kita arahkan ke dns server yang baru kita setting. Pada contoh gunakan alamat IP localhost 127.0.0.1

```
root@ubuntu:~# vim /etc/resolv.conf
nameserver 127.0.0.1

root@ubuntu:~# nslookup www.kurusetra.web.id
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   www.kurusetra.web.id
Address: 192.168.1.100

root@ubuntu:~# nslookup vpn.kurusetra.web.id
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   vpn.kurusetra.web.id
Address: 192.168.1.44
```

Settingan DNS Server sudah berhasil.

Apache Web Server

HTTP

Praktek instalasi aplikasi berbasis web pada direktori /var/www/

HTTPS

```
a2enmod ssl
mkdir /etc/apache2/ssl

openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out
/etc/apache2/ssl/apache.crt

vim /etc/apache2/sites-available/default-ssl
#File sertifikat dan key apache disesuaikan
SSLEngine on
SSLCertificateFile /etc/apache2/ssl/apache.crt
```

SSLCertificateKeyFile /etc/apache2/ssl/apache.key

chown -R www-data.www-data /etc/apache2/ssl/

a2ensite default-ssl
service apache2 reload

Virtual Domain Web Server

Menambah user virtual domain
adduser selosari
adduser sawo
adduser magetan

Edit file userdir.conf
vim /etc/apache2/mods-available/userdir.conf
<IfModule mod_userdir.c>
    UserDir public_html
    UserDir disabled root
    UserDir enabled selosari sawo magetan
    Options ExecCGI

    <Directory /home/*/public_html>
        AllowOverride FileInfo AuthConfig Limit Indexes
        Options MultiViews Indexes SymLinksIfOwnerMatch IncludesNoExec
        <Limit GET POST OPTIONS>
            Order allow,deny
            Allow from all
        </Limit>
        <LimitExcept GET POST OPTIONS>
            Order deny,allow
            Deny from all
        </LimitExcept>
    </Directory>
</IfModule>

Edit file selosari,sawo dan magetan
vim /etc/apache2/sites-available/selosari
<VirtualHost *:80>
ServerName www.selosari.co.cc
DocumentRoot /home/selosari/public_html
ErrorLog /home/selosari/error.log
TransferLog /home/selosari/access.log
ServerAdmin budi@selosari.co.cc
</VirtualHost>

vim /etc/apache2/sites-available/sawo
<VirtualHost *:80>
ServerName www.sawo.co.cc
DocumentRoot /home/sawo/public_html
ErrorLog /home/sawo/error.log
TransferLog /home/sawo/access.log
ServerAdmin budi@sawo.co.cc
</VirtualHost>

vim /etc/apache2/sites-available/magetan
<VirtualHost *:80>
ServerName www.magetan.uni.me
DocumentRoot /home/magetan/public_html
ErrorLog /home/magetan/error.log
TransferLog /home/magetan/access.log
ServerAdmin budi@magetan.uni.me
</VirtualHost>

Aktifkan Virtual Domain
a2ensite selosari
a2ensite sawo
a2ensite magetan

Restart Apache Web Server
/etc/init.d/apache2 restart

Postfix SMTP

Instalasi Postfix
root@budi-desktop:~# apt-get install postfix

Konfigurasi Postfix
root@budi-desktop:~# vim /etc/postfix/main.cf

```
myhostname = budi-desktop
mydomain = kurusetra.web.id
myorigin = $mydomain
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
mydestination = budi-desktop, localhost.localdomain, $mydomain, localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128 ,
192.168.20.0/24,122.200.52.41
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
```

Dovecot POP3 & IMAP4

Instalasi Dovecot
root@budi-desktop:~# apt-get install dovecot-pop3d dovecot-imapd

Konfigurasi Dovecot
root@budi-desktop:~# vim /etc/dovecot/dovecot.conf
listen = *, ::

root@budi-desktop:~# vim /etc/dovecot/conf.d/10-master.conf

```
service imap-login {
  inet_listener imap {
    port = 143
  }
  inet_listener imaps {
    #port = 993
    #ssl = yes
  }

service pop3-login {
  inet_listener pop3 {
    port = 110
  }
  inet_listener pop3s {
    #port = 995
    #ssl = yes
  }
}
```

root@budi-desktop:~# vim /etc/dovecot/conf.d/10-auth.conf
disable_plaintext_auth = no
auth_mechanisms = plain

vim /etc/dovecot/conf.d/10-mail.conf
mail_location = mbox:~/mail:INBOX=/var/mail/%u

Pengujian Dovecot POP3
root@budi-desktop:~# telnet 127.0.0.1 110

```
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
+OK Dovecot ready.
user budi
+OK
pass 1
```

Squirrelmail Webmail Client

Instalasi Squirrelmail
root@budi-desktop:~# apt-get install squirrelmail

Konfigurasi Squirrelmail
root@budi-desktop:~# vim /etc/apache2/apache2.conf
Alias /webmail /usr/share/squirrelmail/
root@budi-desktop:~# /etc/init.d/apache2 restart

Login ke squirrelmail
Buka web browser lalu ketik http://127.0.0.1/webmail/ kemudian login menggunakan user dan password POP3.

Integrasi Antivirus Clamav

Pertama kita install clamsmtp
budi@budi-desktop:~$ sudo su -
[sudo] password for budi:
root@budi-desktop:~# apt-get install clamsmtp

Kemudian kita konfigurasi postfix main.cf
root@budi-desktop:~# vim /etc/postfix/main.cf
#baris paling bawah kita tambahkan
content_filter = scan:127.0.0.1:10026
receive_override_options = no_address_mappings

Konfigurasikan juga postfix master.cf
root@budi-desktop:~# vim /etc/postfix/master.cf

```
smtp      inet  n       -       -       -       -       smtpd
scan      unix  -       -       n       -       16      smtp
        -o smtp_send_xforward_command=yes
# For injecting mail back into postfix from the filter
127.0.0.1:10027 inet  n -       n       -       16      smtpd
        -o content_filter=
-o receive_override_options=no_unknown_recipient_checks,no_header_body_checks
        -o smtpd_helo_restrictions=
        -o smtpd_client_restrictions=
        -o smtpd_sender_restrictions=
        -o smtpd_recipient_restrictions=permit_mynetworks,reject
        -o mynetworks_style=host
        -o smtpd_authorized_xforward_hosts=127.0.0.0/8
```

Rubah port di clamsmtpd.conf
root@budi-desktop:~# vim /etc/clamsmtpd.conf
OutAddress: 10027

Restart postfix dan clamsmtp
root@budi-desktop:~# /etc/init.d/postfix restart
root@budi-desktop:~# /etc/init.d/clamsmtp restart

Pengujian integrasi antivirus clamav
Kirim email bervirus ke user account server email

Hasil scanning antivirus clamsmtp

```
Jul  1 19:10:03 budi-desktop postfix/smtp[8738]: B00E9860BA: to=<budi@kurusetra.web.id>,
relay=127.0.0.1[127.0.0.1]:10026,   delay=1.3,   delays=0.15/0.01/0.37/0.79,   dsn=2.0.0,
status=sent (250 Virus Detected; Discarded Email)
Jul      1   19:10:03   budi-desktop   clamsmtpd:   100000:   from=root@kurusetra.web.id,
to=budi@kurusetra.web.id, status=VIRUS:Worm.VBS-14
```

Integrasi Antispam Spamassassin

Instalasi Paket Spamassassin
apt-get install spamassassin spamc

Pembuatan user dan direktori
groupadd -g 5001 spamd
useradd -u 5001 -g spamd -s /usr/sbin/nologin -d /var/lib/spamassassin spamd
mkdir /var/lib/spamassassin
chown spamd:spamd /var/lib/spamassassin

Startup Spamassassin
vim /etc/default/spamassassin
ENABLED=1
SAHOME="/var/lib/spamassassin/"
OPTIONS="--create-prefs --max-children 5 --username spamd --helper-home-dir ${SAHOME}
-s /var/log/spamd.log"
PIDFILE="${SAHOME}spamd.pid"

Konfigurasi Spamassassin
vim /etc/spamassassin/local.cf
rewrite_header Subject *****SPAM*****
report_safe 1
required_score 2.0
use_bayes 1
bayes_auto_learn 1

Konfigurasi Postfix
vim /etc/postfix/master.cf

```
smtp      inet  n       -       -       -       -       smtpd
        -o content_filter=spamassassin

spamassassin unix -     n       n       -       -       pipe
        user=spamd argv=/usr/bin/spamc -f -e
        /usr/sbin/sendmail -oi -f ${sender} ${recipient}
```

Restart Service Postfix dan Spamassassin
/etc/init.d/spamassassin restart
/etc/init.d/postfix restart

Simple Network Management Protocol

Instalasi Network SNMP

apt-get install snmp snmpd snmp-mibs-downloader cacti

Konfigurasi SNMP

vim /etc/snmp/snmpd.conf

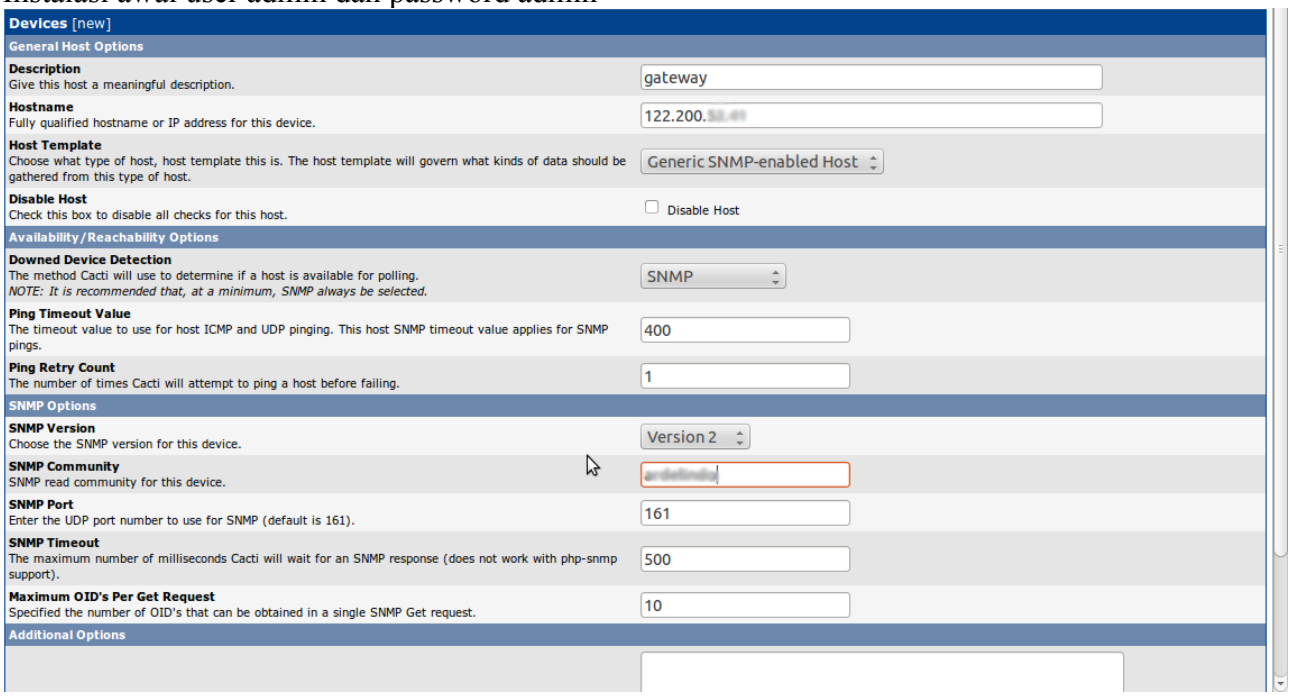
```
#  Listen for connections on all interfaces (both IPv4 *and* IPv6)
agentAddress udp:161,udp6:[::1]:161
rocommunity public
com2sec public default public
com2sec public 0.0.0.0 public
sysLocation    Router Rumah Magetan
sysContact     Budi Santoso <linux.multimedia@gmail.com>
```

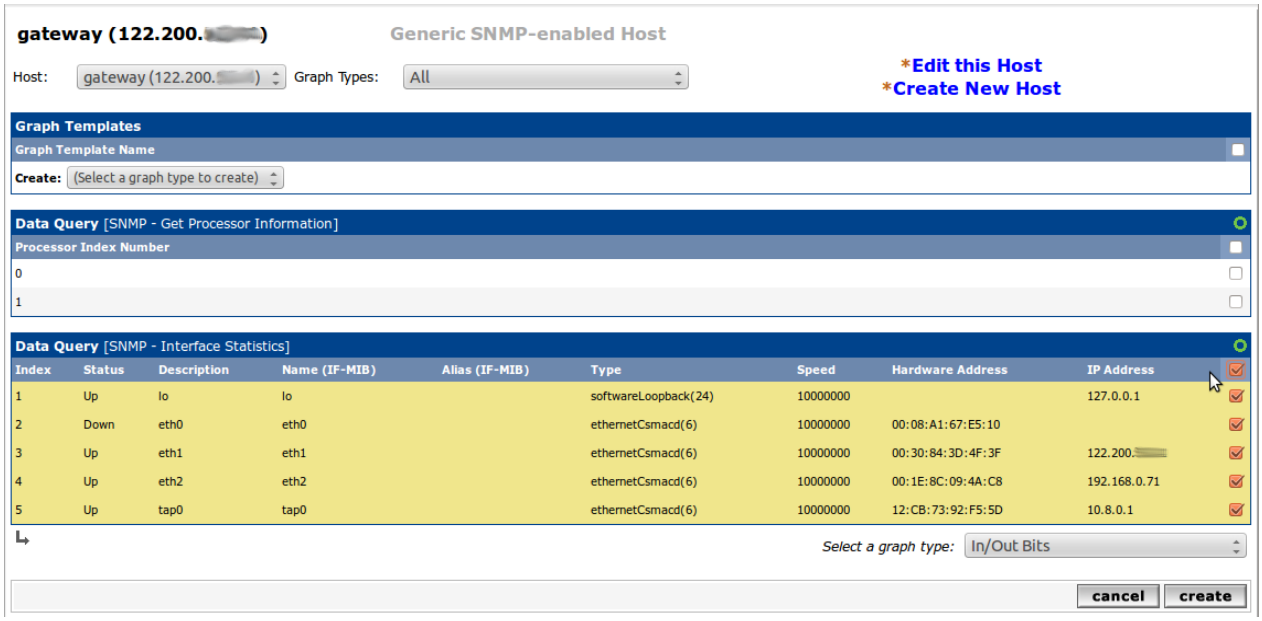
vim /etc/default/snmpd

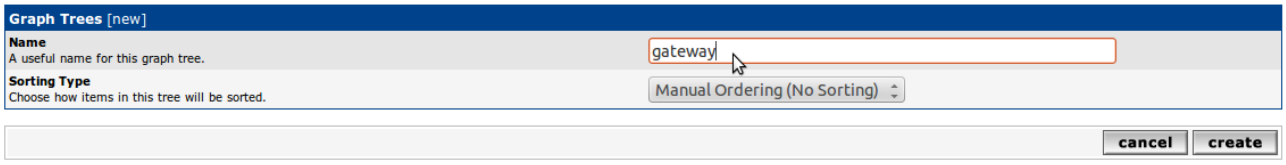
```
SNMPDRUN=yes
```

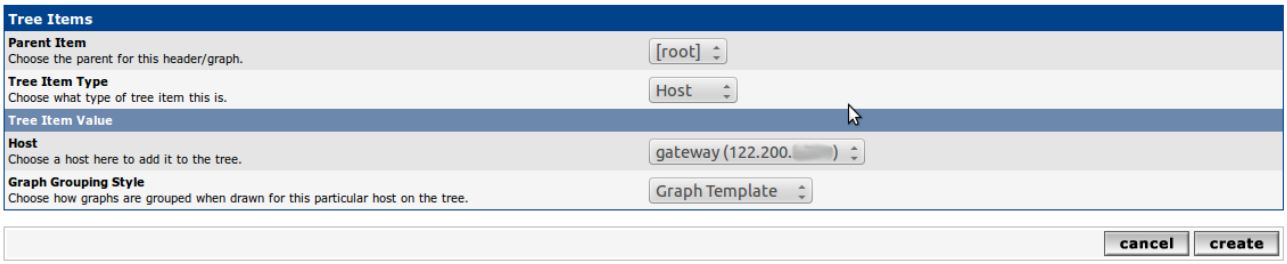
Konfigurasi Cacti

Instalasi awal user admin dan password admin




gateway (122.200.[redacted])
Generic SNMP-enabled Host
Host: gateway (122.200.[redacted]) Graph Types: All
*Edit this Host
*Create New Host
Graph Templates
Graph Template Name
Create: (Select a graph type to create)
Data Query [SNMP - Get Processor Information]
Processor Index Number
0
1
Data Query [SNMP - Interface Statistics]
Index Status Description Name (IF-MIB) Alias (IF-MIB) Type Speed Hardware Address IP Address
1 Up lo lo softwareLoopback(24) 10000000 127.0.0.1
2 Down eth0 eth0 ethernetCsmacd(6) 10000000 00:08:A1:67:E5:10
3 Up eth1 eth1 ethernetCsmacd(6) 10000000 00:30:84:3D:4F:3F 122.200.[redacted]
4 Up eth2 eth2 ethernetCsmacd(6) 10000000 00:1E:8C:09:4A:C8 192.168.0.71
5 Up tap0 tap0 ethernetCsmacd(6) 10000000 12:CB:73:92:F5:5D 10.8.0.1
Select a graph type: In/Out Bits
cancel
create


Graph Trees [new]
Name
A useful name for this graph tree.
gateway
Sorting Type
Choose how items in this tree will be sorted.
Manual Ordering (No Sorting)
cancel
create


Tree Items
Parent Item
Choose the parent for this header/graph.
[root]
Tree Item Type
Choose what type of tree item this is.
Host
Tree Item Value
Host
Choose a host here to add it to the tree.
gateway (122.200.[redacted])
Graph Grouping Style
Choose how graphs are grouped when drawn for this particular host on the tree.
Graph Template
cancel
create

Virtual Private Networking

Konfigurasi Server VPN

```
apt-get install openvpn openssh-server
cd /usr/share/doc/openvpn/examples/easy-rsa/
cd 1.0/
vim vars
source ./vars
./clean-all
./build-ca
./build-key-server
./build-key-server server
./build-key client1
./build-key client2
./build-key client3
./build-key client4
./build-dh
```

cp keys/* /etc/openvpn/

```
cd /usr/share/doc/openvpn/examples/sample-config-files/
cp server.conf.gz /etc/openvpn/
cd /etc/openvpn/
gunzip server.conf.gz
vim server.conf
```

```
port 1194
proto udp
dev tap
ca ca.crt
cert server.crt
key server.key
dh dh1024.pem
server 10.8.20.0 255.255.255.0
ifconfig-pool-persist ipp.txt
client-to-client
keepalive 10 120
comp-lzo
persist-key
persist-tun
status openvpn-status.log
verb 3
cd /usr/share/doc/openvpn/examples/easy-rsa/1.0/keys/
scp -r client1.*  root@ipclient1:/etc/openvpn/
scp -r dh1024.pem  root@ipclient1:/etc/openvpn/
scp -r ca.* root@ipclient1:/etc/openvpn/
```

Konfigurasi Static IP Client

vim /etc/openvpn/server.conf

```
client-config-dir /etc/openvpn/ccd
```

mkdir /etc/openvpn/ccd

vim /etc/openvpn/ccd/client1 (nama file sesuai sertifikat)

```
ifconfig-push 10.8.20.30 255.255.255.0
```

/etc/init.d/openvpn restart

Konfigurasi klien VPN

```
apt-get install openvpn openssh-server
cd /usr/share/doc/openvpn/examples/sample-config-files/
cp client.conf /etc/openvpn/
cd /etc/openvpn
vim client.conf

client
dev tun
proto udp
remote IP_VPN_SERVER 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert client1.crt
key client1.key
comp-lzo
verb 3
```