

Daftar Isi

1. Daftar Isi	1
2. BAB I – Dialin Server	2
3. BAB II – ProFTPD	16
4. BAB III – Apache	24
5. BAB IV – Email	31
6. BAB V – Samba-PDC	36
7. BAB VI – NAT dan Firewall	44

BAB I

DIAL IN SERVER

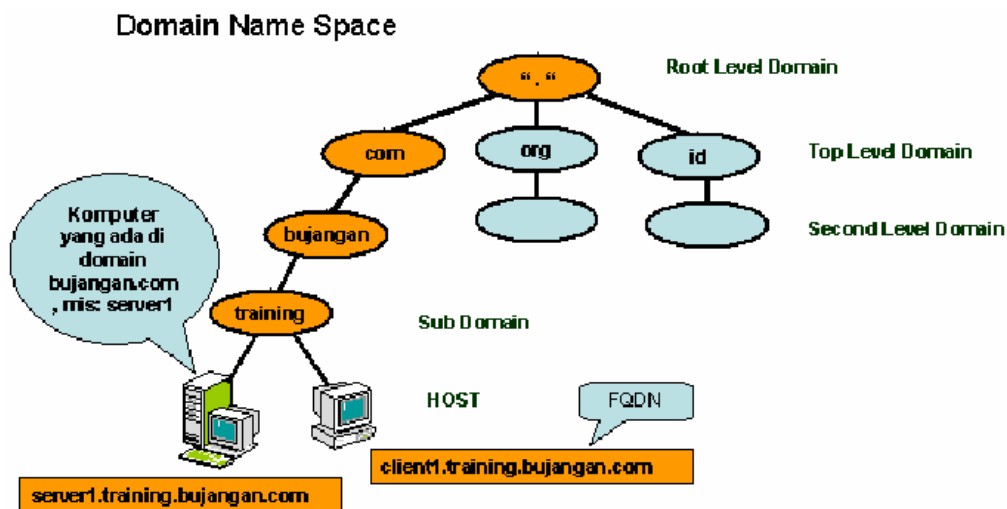
(Proxy Server, DNS Server)

PENDAHULUAN

DNS SERVER

DNS adalah suatu bentuk database yang terdistribusi, dimana pengelolaan secara lokal terhadap suatu data akan segera diteruskan ke seluruh jaringan (internet) dengan menggunakan skema *client-server*. Suatu program yang dinamakan *name server*, mengandung semua segmen informasi dari database dan juga merupakan *resolver* bagi client-client yang berhubungan ataupun menggunakannya.

Struktur dari database *DNS* bisa diibaratkan dengan struktur file dari sebuah sistem operasi *UNIX*. Seluruh database digambarkan sebagai sebuah struktur terbalik dari sebuah pohon (*tree*) dimana pada puncaknya disebut dengan *root node*. Pada setiap *node* dalam *tree* tersebut mempunyai keterangan (*label*) misalnya, *.org*, *.com*, *.edu*, *.net*, *.id* dan lain-lainnya, yang relatif terhadap puncaknya (*parent*). Ini bisa diibaratkan dengan *relative pathname* pada sistem file *UNIX*, seperti direktori *bin*, *usr*, *var*, *etc* dan lain sebagainya. Pada puncak *root node* dalam sebuah sistem *DNS* dinotasikan dengan "." atau "/" pada sistem file *UNIX*.

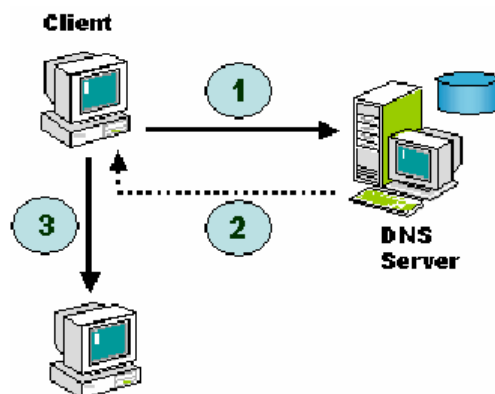


Pada setiap *node* juga merupakan *root* dari *subtree*, atau pada sistem file *UNIX* merupakan *root* direktori dari sebuah direktori. Hal ini pada sistem *DNS* disebut dengan nama *domain*. Pada tiap *domain* juga memungkinkan nama *subtree* dan bisa berbeda pula, hal ini disebut *subdomain* atau *subdirektori* pada sistem file *UNIX*. Pada bagian *subdomain* juga memungkinkan adanya *subtree* lagi yang bisa dikelola oleh organisasi yang berbeda dengan *domain* utamanya.

Cara Kerja Dns

DNS bekerja dengan konsep client server, sebuah computer yang menjalankan fungsi server disebut DNS atau name server dan computer lain meminta penerjemahan hostname ke ip

address disebut sebagai client DNS. DNS juga merupakan system database yang terdistribusi, sehingga memungkinkan setiap bagian dari database dikelola secara terpisah.



DNS umumnya diterapkan dengan menggunakan server terpusat yang disebut server DNS atau name server yang memiliki wewenang atau otoritas dalam mengelola beberapa nama domain dan mengacu ke beberapa domain lainnya yang dikelola server DNS lain .

Ketika computer client meminta informasi ip address suatu hostname ke nameserver, biasanya melalui port 53. kemudian nameserver mencoba menerjemahkan berdasarkan library resolv nya , apakah hostname merupakan nama domain yang dikelola oleh namserver dan name server memberikan jawaban berdasarkan cache dari data informasi yang sama yang pernah ditanyakan sebelumnya dan berhasil dijawab.

BIND sebagai server DNS (name server)

BIND (Berkeley internet name domain) adalah salah satu aplikasi server DNS yang menjadi default aplikasi DNS dalam semua distribusi linux.. paket BIND itu berisi program server DNS yaitu /usr /bin/named yang bertanggung jawab dalam merespon pertanyaan client DNS., paket ini perlu kita install dan mengkonfigurasinya .

Paket Bind 9 adalah versi terbarunya.

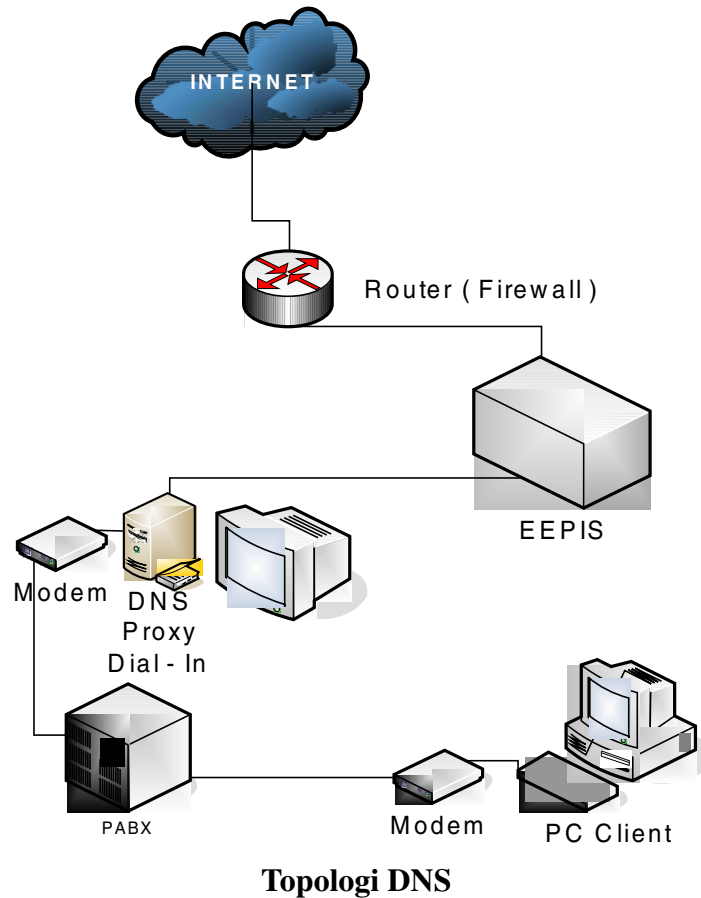
PROXY

Didalam suatu jaringan komputer untuk terhubung ke internet setting proxy server ini merupakan langkah terhubungnya ke internet Fungsi dari proxy server ini guna menyimpan dokumen yang diakses dari internet (original server)

Squid sebagai server proxy

Squid adalah salah satu implementasi dari proxy server yang juga menyimpan cache dari setiap respon dari data yang bersangkutan. Singkatnya squid menerima permintaan akses data (request) dari client, an kemudian meneruskan kealamat yang dituju (missal : www.yahoo.com), kemudian menyimpan data dari alamat (misal: www.yahoo.com) tersebut disimpan ke dalam direktori squid cache yang kemudian juga diteruskan ke client. Kegunaan squid bila ada permintaan yang sama

ke www.yahoo.com, karena sudah ada datanya pada cache maka dapat langsung diberikan tanggapan dari squid server kita tanpa harus meneruskan request tersebut ke www.yahoo.com, ini akan mempercepat akses sehingga dapat menghemat bandwidth.



PERCOBAAN DNS SEVER

1. Menginstal BIND9

```
apt-get install bind9
```

2. edit file pada /etc/resolv.conf:

```
vim /etc/resolv.conf
```

```
#search eepis-its.edu
domain    comnet.eepis-its.edu
nameserver localhost
nameserver 202.154.13.4
nameserver 202.154.13.5
```

3. edit nama hostname ada direktori /etc/hostname

```
vim /etc/hostname
```

```
dialproxy
```

4. konfigurasi file host.conf pada direktori : /etc/hosts.conf

```
vim /etc/hosts.conf
```

```
127.0.0.1    localhost.localdomain localhost    dialproxy ns
```

```
# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

5. mengkonfigurasi file-file yang dibawa oleh BIND

a. pada direktori /etc/bind/named.conf:

vim /etc/bind/named.conf

```
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local
include "/etc/bind/named.conf.options";
// prime the server with knowledge of the root servers
zone "." {
    type hint;
    file "/etc/bind/db.root";
};
// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912
zone "localhost" {
    type master;
    file "/etc/bind/db.local";
};
zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};
zone "0.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0";
};
zone "255.in-addr.arpa" {
    type master;
    file "/etc/bind/db.255";
};
// zone "com" { type delegation-only; };
// zone "net" { type delegation-only; };
// From the release notes:
// Because many of our users are uncomfortable receiving undelegated answers
// from root or top level domains, other than a few for whom that behaviour
```

```
// has been trusted and expected for quite some length of time, we have now
// introduced the "root-delegations-only" feature which applies delegation-only
// logic to all top level domains, and to the root domain. An exception list
// should be specified, including "MUSEUM" and "DE", and any other top level

// domains from whom undelegated responses are expected and trusted.
// root-delegation-only exclude { "DE"; "MUSEUM"; };
include "/etc/bind/named.conf.local";
```

b. pada direktori /etc/bind/named.conf.local:

vim /etc/bind/named.conf.local

```
//
// Do any local configuration here
//

zone "comnet.eepis-its.edu" IN {
    type master;
    file "db.comnet";
    allow-query { any; };
    allow-transfer (127.0.0.1);
};
// reverse
zone "108.252.10.in-addr.arpa" IN {
    type master;
    file "/var/cache/bind/db.10.252.108";
};
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
```

c. pada direktori /etc/bind/named.conf.options

vim /etc/bind/named.conf.options

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

    // If there is a firewall between you and nameservers you want
    // to talk to, you might need to uncomment the query-source
    // directive below. Previous versions of BIND always asked
    // questions using port 53, but BIND 8.1 and later use an unprivileged
    // port by default.

    query-source address * port 53;

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
```

```
// Uncomment the following block, and insert the addresses replacing
// the all-0's placeholder.

forwarders {
    202.154.13.4;
    202.154.13.5;
};

auth-nxdomain no; # conform to RFC1035

};
```

d. buat file /etc/bind/db.0 dengan konfigurasi dibawah ini:

vim /etc/bind/db.0

```
;
; BIND reverse data file for broadcast zone
;
$TTL 604800
@ IN SOA localhost. root.localhost. (
    1 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS localhost.
```

e. buat file /etc/bind/db.127 dengan konfigurasi dibawah ini:

vim /etc/bind/db.127

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

f. buat file /etc/bind/db.255 dengan konfigurasi dibawah ini:

vim /etc/bind/db.255

```
;
; BIND reverse data file for broadcast zone
;
$TTL 604800
```

```
@    IN    SOA    localhost. root.localhost. (
                        1          ; Serial
                        604800    ; Refresh
                        86400     ; Retry
                        2419200   ; Expire
                        604800 )   ; Negative Cache TTL
;
@    IN    NS    localhost.
```

g. buat file /etc/bind/db.local dengan konfigurasi dibawah ini:

vim /etc/bind/db.local

```
;
; BIND data file for local loopback interface
;
$TTL 604800
@    IN    SOA    localhost. root.localhost. (
                        1          ; Serial
                        604800    ; Refresh
                        86400     ; Retry
                        2419200   ; Expire
                        604800 )   ; Negative Cache TTL
;
@    IN    NS    localhost.
@    IN    A     127.0.0.1
```

h. buat file /etc/bind/db.root dengan konfigurasi dibawah ini:

vim /etc/bind/db.root

```
; <<<> DiG 9.2.3 <<<> ns . @a.root-servers.net.
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18944
;; flags: qr aa rd; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 13

;; QUESTION SECTION:
;                          IN      NS
;

;; ANSWER SECTION:
.          518400 IN     NS    A.ROOT-SERVERS.NET.
.          518400 IN     NS    B.ROOT-SERVERS.NET.
.          518400 IN     NS    C.ROOT-SERVERS.NET.
.          518400 IN     NS    D.ROOT-SERVERS.NET.
.          518400 IN     NS    E.ROOT-SERVERS.NET.
```



```

.           518400 IN    NS    F.ROOT-SERVERS.NET.
.           518400 IN    NS    G.ROOT-SERVERS.NET.
.           518400 IN    NS    H.ROOT-SERVERS.NET.
.           518400 IN    NS    I.ROOT-SERVERS.NET.
.           518400 IN    NS    J.ROOT-SERVERS.NET.
.           518400 IN    NS    K.ROOT-SERVERS.NET.
.           518400 IN    NS    L.ROOT-SERVERS.NET.
.           518400 IN    NS    M.ROOT-SERVERS.NET.

;; ADDITIONAL SECTION:
A.ROOT-SERVERS.NET. 3600000    IN    A    198.41.0.4
B.ROOT-SERVERS.NET. 3600000    IN    A    192.228.79.201
C.ROOT-SERVERS.NET. 3600000    IN    A    192.33.4.12
D.ROOT-SERVERS.NET. 3600000    IN    A    128.8.10.90
E.ROOT-SERVERS.NET. 3600000    IN    A    192.203.230.10
F.ROOT-SERVERS.NET. 3600000    IN    A    192.5.5.241
G.ROOT-SERVERS.NET. 3600000    IN    A    192.112.36.4
H.ROOT-SERVERS.NET. 3600000    IN    A    128.63.2.53
I.ROOT-SERVERS.NET. 3600000    IN    A    192.36.148.17
J.ROOT-SERVERS.NET. 3600000    IN    A    192.58.128.30
K.ROOT-SERVERS.NET. 3600000    IN    A    193.0.14.129
L.ROOT-SERVERS.NET. 3600000    IN    A    198.32.64.12
M.ROOT-SERVERS.NET. 3600000    IN    A    202.12.27.33

;; Query time: 81 msec
;; SERVER: 198.41.0.4#53(a.root-servers.net.)
;; WHEN: Sun Feb 1 11:27:14 2004
;; MSG SIZE rcvd: 436

```

- i. buat file /var/cache/bind/db.10.252.108 dengan konfigurasi dibawah ini:]
vim /var/cache/bind/db.10.252.108

```

$TTL 604800
@      IN      SOA    ns.comnet.eepis-its.edu. root.comnet.eepis-its.edu(
        1      ;serial
        604800      ;refresh
        86400     ;retry
        2419200   ;expire
        604800   );minimum

        IN      NS     ns.comnet.eepis-its.edu.
14     IN      PTR    ns.comnet.eepis-its.edu.
9      IN      PTR    dosen.comnet.eepis-its.edu.
7      IN      PTR    Student.comnet.eepis-its.edu.
10     IN      PTR    samba.comnet.eepis-its.edu.
11     IN      PTR    apache.comnet.eepis-its.edu.
12     IN      PTR    proftpd.comnet.eepis-its.edu.
13     IN      PTR    postfix.comnet.eepis-its.edu.
176    IN      PTR    firewall.comnet.eepis-its.edu.

```

- j. buat file /var/cache/bind/db.comnet dengan konfigurasi dibawah ini:
vim /var/cache/bind/db.comnet

```
;
; BIND data file for local loopback interface
;
$TTL 604800
@      IN      SOA     ns.comnet.eepis-its.edu. root.comnet.eepis-its.edu. (
                                2005020304          ; Serial
                                604800              ; Refresh
                                86400               ; Retry
                                2419200            ; Expire
                                604800 )           ; Negative Cache TTL
;

      IN      NS       ns.comnet.eepis-its.edu.
      IN      MX       10 postfix.comnet.eepis-its.edu.
ns     IN      A        10.252.108.14
dosen  IN      A        10.252.108.9
student      IN      A        10.252.108.7
samba   IN      A        10.252.108.10
apache  IN      A        10.252.108.11
proftpd IN      A        10.252.108.12
postfix IN      A        10.252.108.13
dialproxy IN     A        10.252.108.14
firewall IN     A        10.252.108.219
fileserver IN    CNAME    samba
www     IN      CNAME    apache
ftp     IN      CNAME    proftpd
mail    IN      CNAME    postfix
pop3    IN      CNAME    postfix
smtp    IN      CNAME    postfix
imap    IN      CNAME    postfix
proxy   IN      CNAME    dialproxy
```

Untuk melihat percobaan DNS server berhasil dilakukan perintah route ip server dan ip isp.

PERCOBAAN DIAL PROXY

Untuk mempersiapkan dial proxy server, langkah yang perlu diperhatikan adalah sebagai berikut :

1. INSTALLASI PPP.

install PPP

apt-get install ppp

install mgetty

apt-get install mgetty

KONFIGURASI (DIALIN) :

1. Buat group baru PPP dengan cara edit file `/etc/group` dan tambahkan baris di bawah ini pada akhir baris.

```
ppp:x:1001:
```

2. Buat system user baru untuk koneksi dialin pppuser,gunakan shell command vipw, ubah baris user pppuser menjadi :

```
pppuser:x:1001:1001:,,,:/home/pppuser:/usr/sbin/ppplogin
```

3. Buat file baru `/usr/sbin/ppplogin` :

```
#!/bin/sh  
#/etc/ppp/ppplogin  
# PPP login script  
msg n  
stty -echo  
exec /usr/sbin/pppd -detach modem debug crtscts
```

4. Set atribut akses untuk file ini :

```
debian:~# chmod 750 /usr/sbin/ppplogin  
debian:~# chown root:ppp /usr/sbin/
```

5. Set atribut akses untuk direktori `/etc/ppp/` :

```
debian:~# chmod 775 /etc/ppp  
debian:~# chown root:root -R /etc/ppp
```

6. Set atribut akses untuk `/usr/sbin/pppd`

```
debian:~# chmod 750 /usr/sbin/pppd  
debian:~# chmod u+s /usr/sbin/pppd
```

7. tambahkan baris ini pada akhir dari file `/etc/inittab/` jika menggunakan COM1

```
S0:2345:respawn:/sbin/mgetty ttyS0
```

Atau baris dibawah ini bila menggunakan COM2

```
S0:2345:respawn:/sbin/mgetty ttyS1
```

8. Restart init. agar ttyS0 dapat menerima incoming connection :

```
debian:~# init q
```

9. Sekarang tambahkan baris ini pada akhir dari file `/etc/mgetty/login.config` :

```
/autoPPP/ - - /usr/sbin/pppd auth +pap -chap login -detach
```

comment seluruh baris yang lain dari file ini

10. Buat file `/etc/ppp/options.ttyS0` jika menggunakan COM1 atau file `/etc/ppp.options.ttyS1` jika menggunakan COM2

```
10.252.108.1:10.252.108.14  
debug
```

Pada baris pertama terdapat 2 IPaddress. IP pertama merupakan nomor IP server pada jaringan sedangkan IP kedua merupakan Client

11. Konfigurasi pada file /etc/ppp/papsecrets

```
# INBOUND connections

# Every regular user can use PPP and has to use passwords from /etc/passwd
*      hostname      ""      *

# UserIDs that cannot use PPP at all. Check your /etc/passwd and add any
# other accounts that should not be able to use pppd!
guest hostname      "*"      -
master hostname     "*"      -
root  hostname      "*"      -
support hostname    "*"      -
stats hostname      "*"      -

# OUTBOUND connections

# Here you should add your userid password to connect to your providers via
# PAP. The * means that the password is to be used for ANY host you connect
# to. Thus you do not have to worry about the foreign machine name. Just
# replace password with your password.
# If you have different providers with different passwords then you better
# remove the following line.

#      *      password
#comnet      *      comnet      *
*      *      ""      *
```

2. INSTALLASI SQUID.

1. INTALLASI SQUID

apt-get install squid

2. CONFIGURASI SQUID

/etc/squid/squid.conf

```
# TAG: hierarchy_stoplist
#We recommend you to use at least the following line.
hierarchy stoplist cgi-bin ?

# TAG: no_cache
#We recommend you to use the following two lines.
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
#Suggested default:
refresh_pattern ^ftp:      1440 20% 10080
refresh_pattern ^gopher:   1440 0% 1440
refresh_pattern .          0 20% 4320
```

```

#Examples:
#acl myexample dst_as 1241
#acl password proxy_auth REQUIRED
#acl fileupload req_mime_type -i ^multipart/form-data$
#acl javascript rep_mime_type -i ^application/x-javascript$
#
#Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443 563          # https, snews
acl SSL_ports port 873             # rsync
acl Safe_ports port 80              # http
acl Safe_ports port 21              # ftp
acl Safe_ports port 443 563        # https, snews
acl Safe_ports port 70              # gopher
acl Safe_ports port 210             # wais
acl Safe_ports port 1025-65535     # unregistered ports
acl Safe_ports port 280             # http-mgmt
acl Safe_ports port 488             # gss-http
acl Safe_ports port 591             # filemaker
acl Safe_ports port 777            # multiling http
acl Safe_ports port 631             # cups
acl Safe_ports port 873            # rsync
acl Safe_ports port 901             # SWAT
acl purge method PURGE
acl CONNECT method CONNECT

# TAG: http_access
# http_access deny all
#
#Recommended minimum configuration:
#
# Only allow cachemgr access from localhost
http_access allow manager localhost
http_access deny manager
# Only allow purge requests from localhost
http_access allow purge localhost
http_access deny purge
# Deny requests to unknown ports
http_access deny !Safe_ports
# Deny CONNECT to other than SSL ports
http_access deny CONNECT !SSL_ports
#
# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost

```

```

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR
# CLIENTS
# Example rule allowing access from your local networks. Adapt
# to list your (internal) IP networks from where browsing should
# be allowed
#acl our_networks src 192.168.1.0/24 192.168.2.0/24
#http_access allow our_networks
http_access allow localhost
# And finally deny all other access to this proxy
http_access deny all
# TAG: http_reply_access
http_reply_access allow all
# TAG: icp_access
icp_access allow all
# TAG: visible_hostname
visible_hostname dialproxy

```

3. START

```
/etc/init.d/squid start
```

4. RESTART

```
/etc/init.d/squid restart
```

5. STOP

```
/etc/init.d/squid stop
```

ANALISA DAN KESIMPULAN

ANALISA

Untuk membangun DNS server konfigurasi pertama adalah instalasi BIND, dimana paket bind merupakan satu aplikasi server DNS yang menjadi default paket aplikasi DNS dalam semua distribusi linux. Paket BIND yang bertanggung jawab dalam merespon pertanyaan client DNS. Dan beberapa file yang perlu dikonfigurasi ulang seperti /etc/resolve.conf dengan resolve komputer dapat menterjemahkan nama komputer ke IP address. Client DNS disebut dengan resolvers dan DNS server disebut dengan name server. Resolvers atau client mengirimkan permintaan ke name server berupa queries. Name server akan memproses dengan cara mengecek ke local database DNS, menghubungi name server lainnya atau mengirimkan message failur jika ternyata permintaan client tidak ditemukan. Jika ada Resolvers menghubungi host yang dituju dengan menggunakan IP address yang diberikan name server (**Forward Lookup Query**).

KESIMPULAN

DNS adalah hasil pengembangan dari metode pencarian host name terhadap IP address di internet. Pada DNS client (resolver) mengirimkan queries ke Name Server (DNS). Name Server akan menerima permintaan dan memetakan nama komputer ke IP address Domain Name Space adalah pengelompokan secara hirarki yang terbagi atas root-level domains, top-level domains, second-level domains, dan host names.

PERCOBAAN MENGGUNAKAN NSLOOKUP

```
Debian:~#nslookup 10.252.108.10
Server : 202.154.13.4
Address: 10.252.108.10
Name:    samba.comnet.eepis-its.edu
```

```
108.252.10.in-addr.arpa    name=ns. samba.comnet.eepis-its.edu
```

```
Debian:~#nslookup 10.252.108.11
Server : 202.154.13.4
Address: 10.252.108.11
Name:    apache.comnet.eepis-its.edu
```

```
108.252.10.in-addr.arpa    name =ns.apache.comnet.eepis-its.edu
```

```
Debian:~#nslookup 10.252.108.12
Server : 202.154.13.4
Address: 10.252.108.12
Name:    proftpd.comnet.eepis-its.edu
```

```
108.252.10.in-addr.arpa    name=ns.proftpd.comnet.eepis-its.edu
```

```
Debian:~#nslookup 10.252.108.13
Server : 202.154.13.4
Address: 10.252.108.13
Name:    postfix.comnet.eepis-its.edu
```

```
108.252.10.in-addr.arpa    name=ns.postfix.comnet.eepis-its.edu
```

```
Debian:~#nslookup 10.252.108.14
Server : 202.154.13.4
Address: 10.252.108.14
Name:    dialproxy.comnet.eepis-its.edu
```

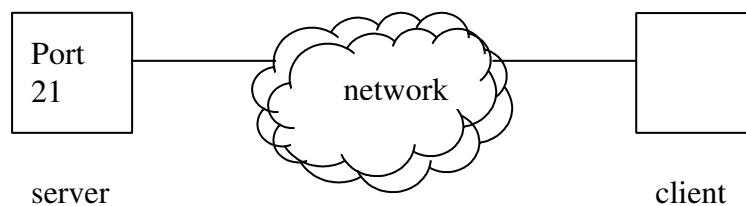
```
108.252.10.in-addr.arpa    name=ns.dialproxy.comnet.eepis-its.edu
```

```
Debian:~#nslookup 10.252.108.219
Server : 202.154.13.4
Address: 10.252.108.219
Name:    firewall.comnet.eepis-its.edu
```

```
108.252.10.in-addr.arpa    name=ns.firewall.comnet.eepis-its.edu
```


BAB II PROFTPD

FTP merupakan bagian dari rangkaian atau kesatuan internet protocol yang dapat mentransfer file computer antara mesin-mesin dengan luas sistem pengoperasian yang berbeda. FTP terdapat 8 bit client-server protocol, mampu menangani segala tipe file tanpa memproses lebih jauh, missal MIME atau uun code. Bagaimanapun juga FTP memiliki keterlambatan yang tinggi, waktu antara permulaan request dan untuk menerima data yang diinginkan dapat diperpanjang dan kadang-kadang dibutuhkan login prosedur yang berkepanjangan.



FTP Server menggunakan port 21. Fungsi FTP adalah mempermudah dalam pembagian file-file, mempercepat secara tak langsung atau implicit menggunakan komputer remote, melindungi user dari berbagai file storage system antar host.

Contoh aplikasi FTP server :

- Proftpd
- Vsftpd
- Wuftpd

Contoh aplikasi FTP client

- Lftp
- ftp

PROSEDUR

1. Konfigurasi pada komputer FTP server

a. cek IP address

```
#ifconfig
```

b. cek FTP server sudah terinstall atau belum

```
#dpkg -l | grep proftpd
```

c. cek FTP server apakah sudah port 21

```
#netstat - nlptu
```

d. jika belum terinstall maka install paket proftpd dengan cara :

```
#apt-get install proftpd
```

Setelah terinstal paket proftpd selanjutnya adalah konfigurasi file proftpd untuk memberikan rule-rule ftp pada file /etc/proftpd/proftpd.conf, lakukan perintah berikut pada console

```
# vi /etc/proftpd/proftpd.conf
```

Setelah itu akan ditampilkan isi file konfigurasi proftpd.conf, kemudian edit/konfigurasi isi file sebagai berikut

```
# /etc/proftpd.conf -- This is a basic ProFTPD configuration
file.
# To really apply changes reload proftpd after modifications.
#

ServerName      "Debian"
ServerType      standalone
DeferWelcome    off

MultilineRFC2228 on
DefaultServer   on
ShowSymlinks    on

TimeoutNoTransfer 600
TimeoutStalled   600
TimeoutIdle      1200

DisplayLogin      welcome.msg
DisplayFirstChdir .message
ListOptions       "-l"

DenyFilter        \*.*/*

# Uncomment this if you are using NIS or LDAP to retrieve
#passwords:
#PersistentPasswd off

#Uncomment this if you would use TLS module:
#TLSEngine        on

#Uncomment this if you would use quota module:
#Quotas           on

#Uncomment this if you would use ratio module:
#Ratios           on

# Port 21 is the standard FTP port.
Port              21

#To prevent DoS attacks, set the maximum number of child
#processes
#to 30. If you need to allow more than 30 concurrent
#connections
#at once, simply increase this value. Note that this ONLY #works
#in standalone mode, in inetd mode you should use an inetd
#server
#that allows you to limit maximum number of processes per #
#service
#(such as xinetd)
MaxInstances      30

#Set the user and group that the server normally runs at.
User              nobody
```

```

Group      nogroup

#Umask 022 is a good standard umask to prevent new files and
#dirs
#(second parm) from being group and world writable.
#Umask      022  022
#Normally, we want files to be overwriteable.
#AllowOverwrite  on

#Delay engine reduces impact of the so-called Timing Attack
#described in
#http://security.lss.hr/index.php?page=details&ID=LSS-2004-#10-02
#It is on by default.
#DelayEngine  off

# A basic anonymous configuration, no upload directories.

<Anonymous ~ftp>
  User      ftp
  Group     nogroup
#We want clients to be able to login with "anonymous" as well #as
"ftp"

  UserAlias  anonymous ftp

#Cosmetic changes, all files belongs to ftp user

  DirFakeUser on ftp
  DirFakeGroup on ftp
  RequireValidShell off
#
#Limit the maximum number of anonymous logins

  MaxClients  10

#We want 'welcome.msg' displayed at login, and '.message'
#displayed
#in each newly chdir'd directory.

  DisplayLogin  welcome.msg
  DisplayFirstChdir .message

#Limit WRITE everywhere in the anonymous chroot

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

#
# # Uncomment this if you're brave.
# # <Directory incoming>
# #   # Umask 022 is a good standard umask to prevent new
# #     files and dirs
# #   # (second parm) from being group and world writable.
# #     Umask      022  022
# #       <Limit READ WRITE>
# #         DenyAll
# #       </Limit>
# #       <Limit STOR>
# #         AllowAll
# #       </Limit>
# # </Directory>
#

```

```
</Anonymous>
```

Konfigurasi diatas adalah untuk memberikan rule-rule pada client yang akan melakukan ftp pada computer server, pada konfigurasi diatas anonymous diperbolehkan untuk melakukan ftp ke server ftp yang ditunjukkan pada konfigurasi berikut :

```
<Anonymous ~ftp>
user          ftp
group         nogroup
userAlias     anonymous ftp
RequireValidShell off
MaxClients   10
DisplayLogin  welcome.msg
DisplayFirstChdir .message
<Directory>
  <Limit WRITE>
  </Limit WRITE>
</Directory>
<Directory incoming>
Umask        022 022
  <Limit READ WRITE>
#   DenyAll
  </Limit>

  <Limit STOR>
#   AllowAll
  </Limit>
</Directory>
</Anonymous>
```

Pada konfigurasi anonymous diatas adalah untuk memberikan izin kepada siapa saja yang ingin melakukan ftp ke komputer ftp server, folder atau file yang diperbolehkan diakses berada pada

2. *Konfigurasi pada komputer client*

Pada computer cliet tidak diperlukan mngkonfigurasi file melainkan hanya menginstal paket ftp, untuk itu pada computer client lakukan prosedur sebagai berikut :

a. cek IP address

```
#ifconfig
```

b. cek FTP client sudah terinstall atau belum

```
#dpkg -l | grep ftp
```

c. jika paket ftp client belum terinstall maka install paket ftp dengan perintah :

```
#apt-get install ftp
```

Dengan melakukan procedure diatas computer client selanjutnya dapat melakukan ftp ke computer, untuk melakukan ftp dari computer client ke computer server lakukan procedure berikut :

- misalnya IP dari computer ftp server adalah 10.252.108.12 maka lakukan perintah FTP sebagai berikut :

```

#ftp 10.252.108.12
connected to 10.252.108.12 . comnet, eepis-its.edu
220proFTPD 1.2.10 server (debian) (10.252.108.12)
name (10.252.108.12 : root) : anonymous
331 guest login OK, send your complete e-mail as
password
password:
331 password required for harun
231 user anonymous logged in
remote system is UNIX
using binary mode to transfer files.
ftp>ls
200 PORT command successful
150 opening ASCII mode data connection for file list
drwx----- ftp (?) 4096 Jan 16 04:17 master
drwx----- ftp (?) 4096 Jan 17 03:47 network
drwx----- ftp (?) 4096 Jan 16 03:45
Multimedia
drwx----- ftp (?) 4096 Jan 20 07:23 driver
drwx----- ftp (?) 4096 Jan 16 03:44 video
226 transfer complete

```

- untuk keluar dari ftp lakukan perintah sebagai berikut

```
ftp>quit
```

3. Pada penerapan FTP diatas adalah dilakukan oleh computer client dengan login sebagai anonymous, jika kita ingin melakukan ftp pada computer server dengan login tertentu sebagai user pada computer FTP server maka pada computer server harus dibuat user account untuk client dengan cara :

```

#adduser (user name)
#adduser harun
Adding user harun...
Adding new group harun(1000).
Adding new user harun (1000) with group harun.
Creating home director /home/harun.
Copying files from /etc/skel
Enter the new value,or press return for the default
Full Name []:
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [y/n] y

```

Dari computer client dikoneksikan ke server dengan cara login menggunakan user yang telah dibuat oleh server.

```

#ftp (IP Server)
misal : #ftp 10.252.108.12
connected to 10.252.108.12 . comnet, eepis-its.edu

```

```

220proFTPD 1.2.10 server (debian) (10.252.108.12)
name (10.252.108.12 : root) : harun
331 password required for harun
230 user harun logged in
remote system is UNIX
using binary mode to transfer files.
ftp>ls
200 PORT command successful
150 opening ASCII mode data connection for file list
-rwx----- harun (?) 600 Jan 16 04:17 tes.c
-rw-r-r--- harun (?) 0 Jan 17 03:47 tes.tes
drwxr-xr-x harun (?) 4096 Jan 16 03:45 Chat
drwx----- harun (?) 4096 Jan 20 07:23 Data
drwxr-xr-x harun (?) 4096 Jan 16 03:44
public_html
226 transfer complete
ftp>quit

```

Buat file dengan perintah

```
#vi (nama file)
```

- Upload file dengan perintah :
ftp>mput (nama file)

- Mengambil file dari FTP server :

```
ftp>mget (nama file)
```

4. *Pada contoh procedure akses server ftp diatas dilakukan oleh client yang memiliki sistem operasi unix, jika client windows ingin melakukan ftp ke computer ftp server maka prosesnya adalah sama dengan procedure yang dilakukan oleh sistem operasi unix, yaitu dengan mengetikkan perintah*

FTP <IP_FTP_SERVER> pada command prompt (C:\) atau pada browser (misalnya IE) ketikkan pada address dengan perintah FTP ://<IP_FTP_SERVER>

- Contoh FTP dari computer client dengan sistem operasi windows yang melakukan FTP ke computer FTP server dengan sistem operasi UNIX base menggunakan command prompt C:\

Click tombol START > RUN kemudian ketikkan cmd dan tekan enter atau klik tombol OK.

Selanjutnya akan tampil command prompt yang defaultnya berwarna hitam, kemudian ketikkan perintah sebagai berikut untuk melakukan FTP ke computer server (misalnya IP computer FTP server adalah 10.252.100.21)

```

C:\>ftp 10.252.100.21
Connected to 10.252.100.21.
220 localhost FTP server (Version 6.4/OpenBSD/Linux-ftp-0.17) ready.
User (10.252.100.21:(none)): harun

```

```

331 Password required for harun.
Password:
230- Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY,
to the extent
230- permitted by applicable law.
230 User harun logged in.
ftp>

```

sebenarnya perintah yang dilakukan pada client ftp yang menggunakan sistem operasi WINDOWS maupun UNIX tidak ada perbedaan dalam cara mengaksesnya, setelah melakukan ftp seperti pada procedure diatas yang sama saat melakukan ftp menggunakan sistem operasi UNIX kita dapat memberikan perintah-perintah ftp lainnya seperti ls,mget,mput dll, untuk mengetahui perintah-perintah (command) yang bisa diberikan pada lingkungan ftp dapat mengetikkan help pada console/command prompt seperti pada contoh dibawah :

```

ftp> help
Commands may be abbreviated.  Commands are:

!                delete                literal
prompt          send
?               debug                ls
put             status
append         dir                mdelete
pwd            trace
ascii          disconnect                mdir
quit           type
bell           get                mget
quote          user
binary         glob                mkdir
recv           verbose
bye            hash                mls
remotehelp
cd             help                mput
rename
close          lcd                open
rmdir
ftp>

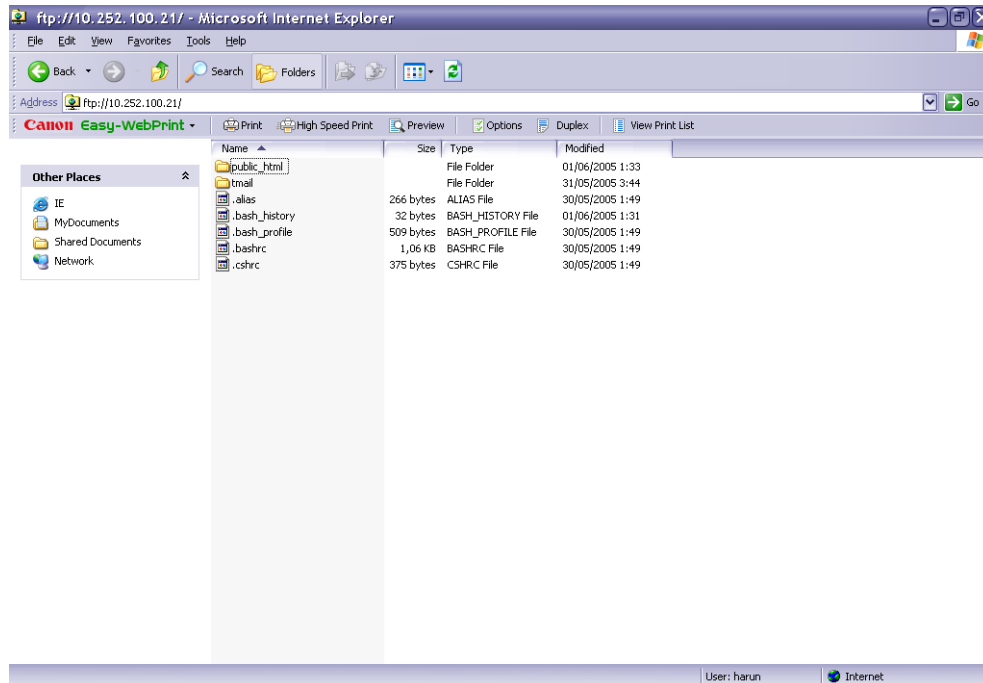
```

- Untuk melakukan FTP ke computer FTP server menggunakan browser maka kita dapat mengetikkan perintah sebagai berikut server (misalnya IP computer FTP server adalah 10.252.100.21)

Buka IE (internet Explorer) setelah itu ketikkan ftp://10.252.100.21 pada address bar browser IE, setelah itu akan ditampilkan kotak pesan untuk otoritas ftp client, yaitu client di minta untuk memasukkan username dan password seperti pada gambari dibawah :



Setelah username dan password yang kita berikan adalah valid maka akan ditampilkan data-data pada halaman browser sebagai berikut :



BAB III

APACHE

I. Tujuan

- Mahasiswa dapat menginstall dan mengkonfigurasi service httpd.
- Mahasiswa dapat dapat menginstall php dan mengkombinasikan dengan service httpd
- Mahasiswa dapat menginstall Mysql server dan dan dapat mengakses Mysql dengan script php.

II. Teori

Apache HTTP Server adalah software open source untuk HTTP web server yang dijalankan di platform sistem Unix-like seperti BSD, Linux, dan UNIX, Microsoft Windows dan lainnya. Apache dikembangkan dan dipelihara oleh komunitas terbuka yang bergabung dengan Apache Software Foundation.

Mulanya, Apache sekedar open source alternative untuk Netscape web server (kini dikenal sebagai Sun ONE). Kemudian berkembang dengan pesat dan melampaui semua jenis Unix based HTTP server lainnya dalam hal fungsionalitas dan kecepatan. Apache adalah HTTP server paling populer di Internet sejak April 1996 dan menguasai 57% pangsa pada bulan Mei 1999. Pada bulan August 2004 tercatat peningkatan menjadi 67%.

Apache piawai dengan fitur 'highly configurable error messages, DBMS-based authentication databases, and content negotiation'. Didukung beberapa GUIs memudahkan konfigurasi dan lebih intuitif. Apache mendukung fitur yang diimplementasikan sebagai modul ter-kompilasi mulai dari server-side programming language support sampai dengan authentication schemes. Sejumlah bahasa pemrograman yang lazim digunakan seperti Perl, Python, dan PHP didukung Apache sepenuhnya.

Untuk membangun apache server ini kita membutuhkan beberapa paket yang ada di linux. Ada beberapa paket yang dibutuhkan diantaranya: APACHE, PHP4, MySQL Paket-paket ini digunakan untuk membangun server agar dapat bekerja sesuai keinginan.

Apache digunakan sebagai web server yang mengolah script php, php digunakan untuk melakukan proses-proses aritmatika, database dan lain-lainnya, sedangkan MySQL digunakan untuk pembuatan database yang terhubung dengan halaman web yang dilakukan oleh script php.

Web Server Apache terdiri dari beberapa bagian, kode source apache asli dengan beberapa patch dan beberapa executable tambahan.

Sebaiknya kita gunakan Web Server Apache yang tergolong 'stable version', yang mungkin akan lebih mudah untuk dikompilasi dan akan menghasilkan daemon yang cukup stabil.

Beberapa direktori penting untuk Apache:

- cgi-bin/ - direktori CGI scripts
- conf/ - konfigurasi file httpd server
- htdocs/ - main direktori untuk dokumen-dokumen
- logs/ - direktori dengan log files
- other stuff (bin/, icons/, include/, proxy/, man/.....)

Menginstal server di Unix:

Paket dapat diinstall langsung jika memiliki package pre built

Jika tidak terdapat package tersebut, langkah-langkah yang dapat dilakukan:

- ◆ Download and unpack in suitable directory (ftp, uncompress, gunzip, tar...)
- ◆ Initial configuration
- ◆ Compile the server
- ◆ Install executable in system
- ◆ Further configuration files to reflect your environment
- ◆ Run httpd

Konfigurasi dasar Apache:

ServerType standalone

Port 80

User www-data

Group www-data

ServerAdmin your email address

ServerRoot /etc/apache

ErrorLog /var/log/apache/error.log

LockFile /var/lock/apache.lock

PidFile /var/run/apache.pid

```
DocumentRoot /var/www
```

```
UserDir public_html
```

```
DirectoryIndex index.php index.html index.htm index.shtml index.cgi
```

```
ScriptAlias /cgi-bin/ /usr/lib/cgi-bin
```

Untuk membangun server ini kita membutuhkan beberapa paket yang ada di linux. Ada beberapa paket yang dibutuhkan diantaranya: Apache, PHP4, Mysql. Paket –paket ini digunakan untuk membangun server agar dapat bekerja sesuai keinginan.

Langkah-langkah menginstall paket APACHE, PHP dan MySQL:

APACHE

Proses Install

```
# apt-get install apache2
```

Proses Start

```
# /etc/init.d/apache2 start
```

Proses Restart

```
# /etc/init.d/apache2 restart
```

Proses Stop

```
# /etc/init.d/apache2 stop
```

Pada instalasi apache ini secara default akan langsung dapat di jalankan dengan document kerja default yaitu pada /var/www untuk meletakkan halaman web kita, kita dapat mengubah halaman kerja di folder yang kita inginkan, dengan mengedit file konfigurasi yang berada di /etc/apache2/httpd.conf dengan menggantikan DocumentRoot [letak folder], setelah melakukan pengeditan file konfigurasi httpd.conf maka dilakukan restart service dari apache seperti pada perintah diatas yaitu /etc/init.d/apache2 restart. Secara default halaman web yang akan di load adalah halaman yang bernama index.php atau index.html

PHP

Proses Install

```
# apt-get install php4
```

Untuk mengetahui service-service apa saja yang sedang diijinkan pada service php ini kita dapat membuat script php yang cukup pendek untuk menampilkan service-service pada php yaitu dengan memanggil fungsi dari php sendiri `phpinfo()`; jadi kita dapat langsung menuliskan fungsi tersebut di halaman web kita seperti di bawah ini :

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

Cukup dengan memanggil fungsi diatas kita dapat menampilkan halaman php yang berisi service yang dapat digunakan. Tanda `<?` Adalah tanda pembukaan untuk script php, seluruh yang berada setelah tanda `<?` Akan dikenal sebagai script php hingga ditemukan tanda penutup dari script php yaitu `?>`, namun pada block `<? Dan ?>` dapat di sisipkan script html, jadi saat kita sisipkan script html pada block penulisan script php maka script html tetap akan dikenal sebagai script html.

MySQL

Proses Install

```
# apt-get install mysql-server
```

MySQL yang kita install disini di gunakan untuk proses databases yang dapat di akses melalui web, sehingga saat pembuatan halaman web menggunakan script php kita dapat membuat aplikasi database yang dapat diakses dimana saja melalui halaman web jika mysql ini terinstall pada computer yang dapat diakses melalui jaringan internet. Namun pada praktek ini tidak dilakukan pembuatan database.

III. Konfigurasi dan Hasil Percobaan

Konfigurasi `httpd.conf`

konfigurasi `httpd.conf` yang perlu adalah :

Port 80 => hasil dari konfigurasi ini adalah saat mengetikkan url pada browser tidak perlu menambahkan nomor port yang dituju, karena port 80 adalah port yang standar.

DocumentRoot /var/www/ => direktori ini adalah direktori tempat meletakkan dokumen-dokumen web yang akan dipublikasikan.

UserDir public_html => dengan meng-Enable option ini, maka setiap user di linux dapat membuat homepage mereka di home direktori mereka sendiri, yaitu pada direktori public_html. Untuk menghubungkan DocumentRoot ke public_html setiap user cukup menambahkan link dengan tanda “~/nama_user”.

Konfigurasi httpd.conf setelah php terinstall

Menambahkan module php (libphp4.so) pada httpd.conf dengan menuliskan “LoadModule php4_module” diikuti dengan direktori tempat libphp4.so tersimpan.

Menambahkan “AddType application/x-httpd-php .php”.

Hasil dari konfigurasi di atas adalah httpd server dapat mengidentifikasi file berekstensi php, sehingga dapat tampil di browser.

Tes konektivitas php dengan mysql-server

Untuk mengetahui konektivitas dengan mysql dapat digunakan script php antara lain mysql-connect().

Contoh script :

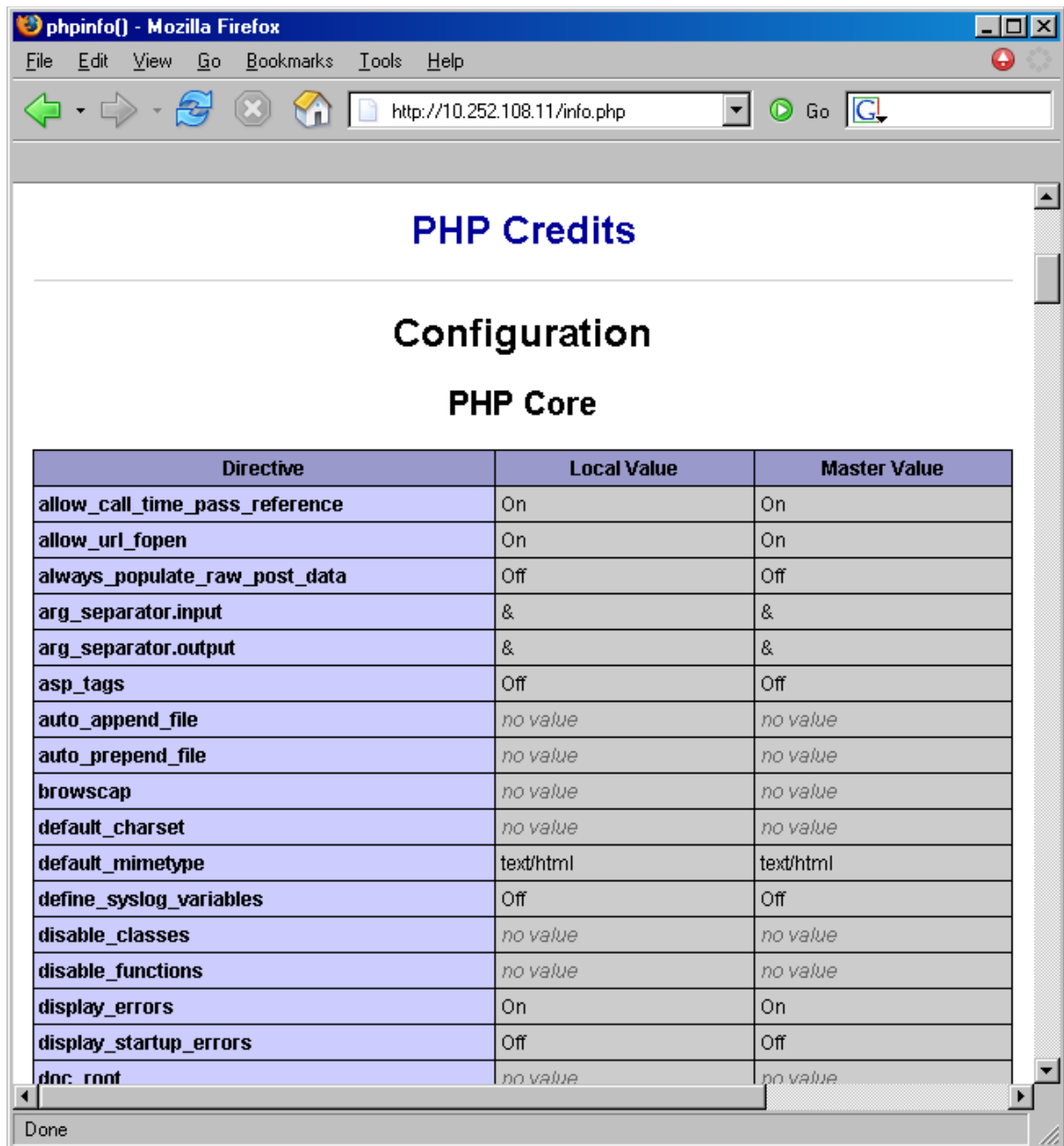
```
<?
mysql_connect(“localhost”,”root”,”root”) or exit (“tidak terhubung”);
print “terhubung”;
?>
```

Apabila script php diatas dijalankan di browser dan menampilkan kata “terhubung” , maka mysql-server dapat diakses.

Sebaliknya bila tampil kata “tidak terhubung” ada kemungkinan service mysql-server tidak berjalan, ada kesalahan dalam penulisan user maupun password, atau tidak ada user yang dimaksud dalam user mysql.

Untuk mengakses web server apache dari komputer lain maka cukup mengetikkan di browser “http://no_ip_server”.

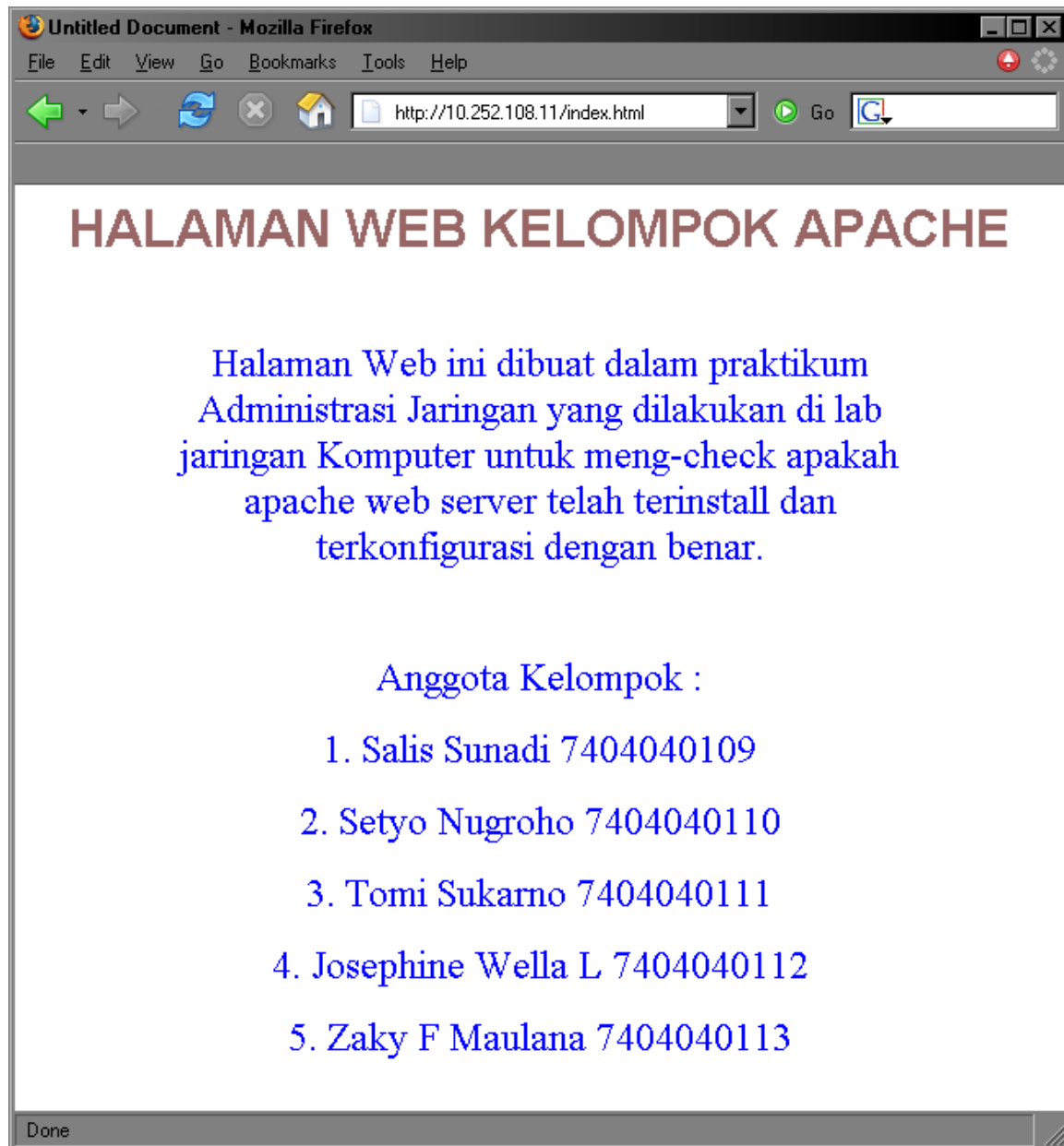
Screenshot setelah php terinstall :



The screenshot shows a Mozilla Firefox browser window with the address bar displaying `http://10.252.108.11/info.php`. The page content is titled "PHP Credits Configuration" and "PHP Core". Below the title is a table listing various PHP configuration directives.

Directive	Local Value	Master Value
<code>allow_call_time_pass_reference</code>	On	On
<code>allow_url_fopen</code>	On	On
<code>always_populate_raw_post_data</code>	Off	Off
<code>arg_separator.input</code>	&	&
<code>arg_separator.output</code>	&	&
<code>asp_tags</code>	Off	Off
<code>auto_append_file</code>	<i>no value</i>	<i>no value</i>
<code>auto_prepend_file</code>	<i>no value</i>	<i>no value</i>
<code>browscap</code>	<i>no value</i>	<i>no value</i>
<code>default_charset</code>	<i>no value</i>	<i>no value</i>
<code>default_mimetype</code>	text/html	text/html
<code>define_syslog_variables</code>	Off	Off
<code>disable_classes</code>	<i>no value</i>	<i>no value</i>
<code>disable_functions</code>	<i>no value</i>	<i>no value</i>
<code>display_errors</code>	On	On
<code>display_startup_errors</code>	Off	Off
<code>doc_root</code>	<i>no value</i>	<i>no value</i>

Screenshot WEB sederhana :



IV. Kesimpulan

Dengan apache dapat dibuat homepage yang berisi halaman-halaman web dinamis yang menggunakan script-script php dan database.

Service httpd yang semula tidak dapat memproses file berekstensi php harus dikonfigurasi ulang dengan menambahkan module serta filetype .php pada file konfigurasinya.

BAB IV

EMAIL

Tujuan:

1. Agar Mahasiswa dapat mempelajari instalasi dan konfigurasi pada Mail Server pada Linux Debian
2. Untuk mengetahui kerja dari email server

Teori:

Email adalah salah satu metode yang digunakan untuk berkomunikasi melalui internet. Dengan email, seorang user dapat mengirimkan pesan ke berbagai macam komputer dengan sistem operasi yang berbeda-beda. Protokol yang digunakan untuk aplikasi email adalah Simple Mail Transfer Protocol (SMTP). Selain itu juga ada protokol lain yang dapat bekerja sama dengan SMTP yaitu POP dan IMAP.

Pada saat email dikirim melalui sendmail, email tersebut dikirim dari mail client untuk menuju mail server lalu masuk ke suatu antrian. Ketika email sudah berada pada puncak antrian, sendmail akan memerintahkan untuk mengirim email tersebut ke tujuan. Jika tidak dapat terhubung ke remote SMTP server, sendmail akan tetap menyimpannya ke dalam antrian dan akan mencoba untuk mengirimkannya kembali setiap beberapa jam.

Ada banyak alasan mengapa suatu pesan email akan dimasukkan ke dalam antrian.

Contohnya adalah :

- Anda punya akses ke internet, dan anda mengirim email pada saat komputer sedang tidak terhubung dengan internet
- Komputer yang dituju tidak sedang terhubung dengan internet karena sesuatu sebab
- Remote host (server yang dituju) sedang mengalami perbaikan atau kerusakan
- Tidak ada koneksi ke remote host

Jika salah satu dari kondisi di atas terjadi, seorang user butuh kepastian apakah emailnya dapat terkirim dengan sukses. Dengan membiarkan email masuk dalam antrian, maka sendmail akan dapat mengirimkannya kapan saja pada saat komputer sedang terhubung dengan internet.

Ketika ada pesan yang masuk, maka pesan tersebut akan secara otomatis masuk ke dalam postfix. Walaupun proses download telah selesai oleh client, pesan tetap tersimpan di server. Penyimpanan ini terjadi terus sampai proses delete email oleh client.

POP atau Post Office Protocol adalah salah satu metode untuk mengambil dan mengirim email dari/ke remote machine. Protokolnya cukup sederhana, anda dapat melihat, mengambil dan membaca email dari komputer client. Dengan menggunakan POP anda dapat membaca dan mengirim email dari rumah atau dari tempat-tempat lain. Software-software seperti Netscape, Microsoft Outlook, Eudora, dan hampir semua software email mendukung penggunaan POP. Agar email di server dapat didownload ke komputer client, maka software di client software harus disetup dahulu agar menggunakan POP. Setelah itu email di server dapat didownload ke client sehingga semua email dipindahkan dari server ke client. Setelah proses download email selesai, email di serverpun dihapus.

IMAP

IMAP dikembangkan untuk memperbaiki kekurangan yang dimiliki oleh POP. IMAP dirancang untuk dapat digunakan baik untuk server maupun client. Dengan IMAP semua email di server tidak otomatis dihapus dari server meskipun proses download ke client sudah selesai. Untuk

menghapus email dari server harus menunggu perintah dari user di client. Pada POP, semua email yang ada di server didownload dalam waktu yang bersamaan, hal ini akan menjadi masalah jika akses jaringan internetnya lambat sekali. Sedangkan pada IMAP, email di server tidak harus didownload semua. IMAP menyediakan fasilitas agar email dapat didownload headernya saja atau bodynya saja. Email juga dapat disimpan ke folder yang berbeda, sehingga email dapat diorganisasi dengan baik. Kelebihan utama dari IMAP adalah bahwa IMAP mendukung mode offline, yaitu kita dapat menulis dan membaca email pada saat komputer sedang tidak terkoneksi ke internet.

MAILDIR, adalah box penyimpanan surat dalam bentuk folder, dibuat oleh Qmail atau Postfix. Disimpan pada direktori (misal nama user adalah dhoto) /home/dhoto/Maildir. Nama user otomatis membentuk maildir. Dalam maildir, email-email yang telah diterima dibedakan statusnya pada tipe-tipe seperti current, new, old. Email-email itu dijadikan per-file.

MBOX, adalah tempat penyimpanan dimana pesan-pesan tersebut sudah pernah dibuka dalam bentuk file. Disimpan pada direktori (misal nama user adalah dhoto) /var/spool/mail/dhoto. Email-email yang ada dijadikan satu file dengan nama user tersebut. Jika semakin lama semakin banyak email yang masuk maka kapasitas dari file tersebut semakin besar.

Langkah Percobaan :

1. Cek apakah paket pertama terinstall

```
#dpkg -l | grep postfix
#netstat -nlptu | grep 25
```

```
ii postfix 2.1.5-6 A high-performance mail transport agent
ii postfix-doc 2.1.5-6 Postfix documentation
```

2. Menginstall paket

```
#apt-get install postfix
```

```
Reading Package Lists...
Building Dependency Tree...
postfix is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

3. Menjalankan paket

```
#/etc/init.d/postfix start
#/etc/init.d/postfix restart
#/etc/init.d/postfix stop
```

```
Starting mail transport agent: Postfix.
```

4. Konfigurasi

```
#vi /etc/postfix/main.cf
```

```
See /usr/share/postfix/main.cf.dist for a commented, more
complete version
```

```
smtpd_banner = $myhostname ESMTP $mail_name (Debian/GNU)
biff = no
```

```
# appending .domain is the MUA's job.
```

```

append_dot_mydomain = no

# Uncomment the next line to generate "delayed mail" warnings
#delay_warning_time = 4h

myhostname = postfix.comnet.eepis-its.edu
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
mydestination = postfix, comnet.eepis-its.edu,
postfix.comnet.eepis-its.edu, localhost.comnet.eepis-its.edu,
localhost
relayhost =
mynetworks = 127.0.0.0/8 10.252.108.0/24
mailbox_command =
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = all
home_mailbox = Maildir/

```

5. Cek apakah paket kedua terinstall

```
#dpkg -l grep courier
```

```

ii  courier-authda 0.47-3 Courier Mail Server - Authentication daemon
ii  courier-base   0.47-3 Courier Mail Server - Base system
ii  courier-imap   3.0.8-3 Courier Mail Server - IMAP server
ii  courier-pop    0.47-3 Courier Mail Server - POP3 server

```

```
#netstat -nlptu | grep 143
```

```

tcp6      0      0 :::143          :::*            LISTEN      2897/couriertcpd

```

6. Menginstall paket

```
#apt-get install courier-imap
```

```

Reading Package Lists...
Building Dependency Tree...
courier-imap is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

```

```
#apt-get install courier-pop
```

```

Reading Package Lists...
Building Dependency Tree...
courier-pop is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.

```

7. Menjalankan paket

```

#/etc/init.d/courier-imap start
#/etc/init.d/courier-pop start
#/etc/init.d/courier-imap restart
#/etc/init.d/courier-pop restart
#/etc/init.d/courier-imap stop
#/etc/init.d/courier-pop stop

```

```

Starting Courier IMAP server: imapd.
Starting Courier POP server: popd.

```

8. Membuat Maildir di /etc/skel
#maildirmake /etc/skel/Maildir

Testing email di Windows :

1. Lakukan adduser di server email, semisal: # adduser dhoto.
2. Cobalah buka outlook express di sisi client.
3. Ikuti petunjuk dalam konfigurasinya yakni isikan nickname, email anda yang sudah anda buat dengan domain seperti di server, gunakan protocol emailnya, dll.

Misal :

Display name: dhoto

email : dhoto@comnet.eepis-its.edu

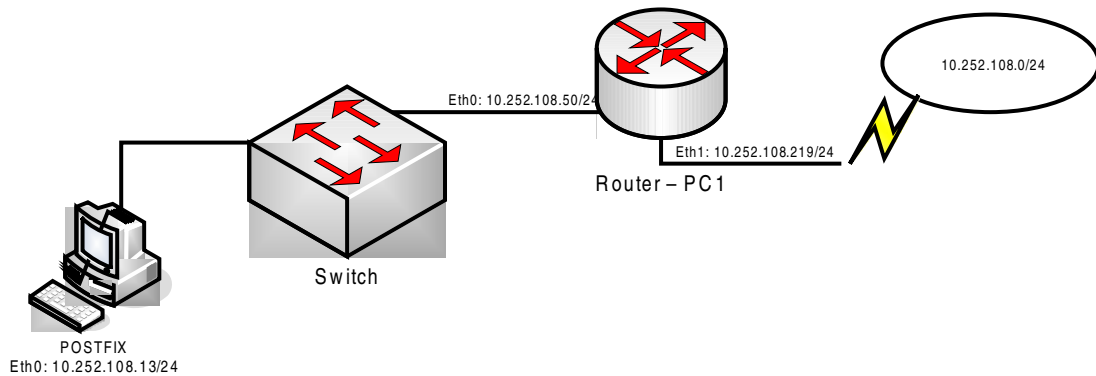
protokol dapat menggunakan POP3 atau IMAP.

Incoming dan outgoing :

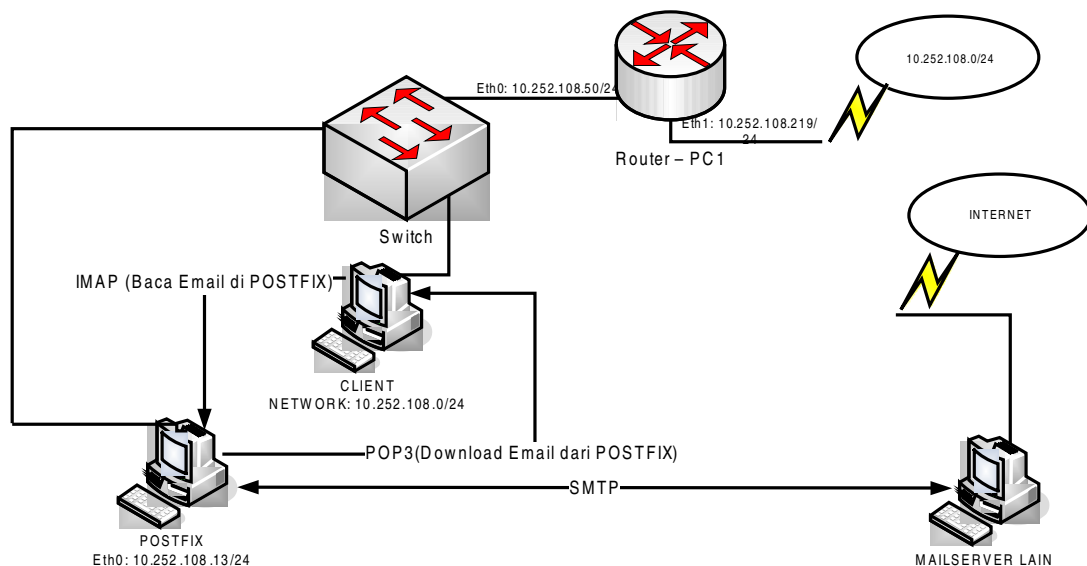
Mail.comnet.eepis-its.edu

password :*****

TOPOLOGI



PENJELASAN IMAP POP3 SMTP



Fungsi SMTP mengirim data antar mail server yang dibatasi firewall, sedangkan POP3 dan IMAP mengirim data antara mailserver dan client. POP3 mengambil paket email dari mail server sehingga data pada mail server kosong (spt POBOX pada POS), sedangkan IMAP hanya membaca email dari mailserver shg sewaktu-waktu dapat membuka email lagi dari tempat lain.

KESIMPULAN

Mail Transport Agent yang digunakan dalam percobaan ini adalah Postfix yang memiliki keunggulan dibandingkan paket Sendmail

Sebagai Perantara digunakan paket Courier-imap dan Courier-pop yang menggunakan protocol IMAP / POP3

Pada POP, semua email yang ada di server didownload dalam waktu yang bersamaan, sedangkan pada IMAP, email di server tidak harus didownload semua.

BAB V SAMBA SERVER

I. Tujuan

- Mahasiswa dapat memahami manfaat/kegunaan dari Samba Server.
- Mahasiswa dapat melakukan konfigurasi Samba server pada system
- Mahasiswa dapat melakukan konfigurasi samba Primary Domain Controller (PDC)

II. Peralatan yang dibutuhkan

1. PC yang terhubung ke system jaringan minimal 2 buah, 1 Debian PC untuk Samba Server, dan 1 Windows PC sebagai client.
2. Program utama yang digunakan adalah :
 - Samba_3.0.10-1_i386.deb
 - Swat_3.0.10-1_i386.deb
 - WinXP_SignOrSeal registry patch

III. Pendahuluan

Samba merupakan aplikasi UNIX yang memanfaatkan protocol SMB (Server Message Block). Sebagian system operasi memanfaatkan SMB dalam komunikasi client-server-nya, termasuk Windows dan OS/2. Samba memungkinkan mesin Linux berkomunikasi dengan menggunakan mesin Windows/Dos maupun OS/2. Samba dapat digunakan untuk :

- Menghubungkan setiap mesin Unix (termasuk Linux) dengan mesin Dos/Windows.
- Menempatkan mesin Unix (Linux) sebagai *Primary Domain Controller* sebagaimana yang dilakukan oleh Windows NT/2000 Server.

Samba juga dapat digunakan untuk:

- Berbagi (share) file dan printer pada semua komputer yang terhubung ke jaringan.
- Membantu pengguna browsing di network neighborhood.
- Memberikan otentikasi kepada setiap klien yang login kedalam domain pada suatu jaringan.

IV. Struktur File Konfigurasi

```
[global]
workgroup = "Isikan Nama Work Group"
null passwords = "Yes/No"
password server = "Yes/None"
pam password change = "Yes/No"
passwd chat debug = "Yes/No"
unix password sync = "Yes/No"
domain logons = "Yes/No"
preferred master = "Yes/No"
domain master = "Yes/No"
dns proxy = "Yes/No"
winbind use default domain = "Yes/No"
guest ok = "Yes/No"
```

[Share]

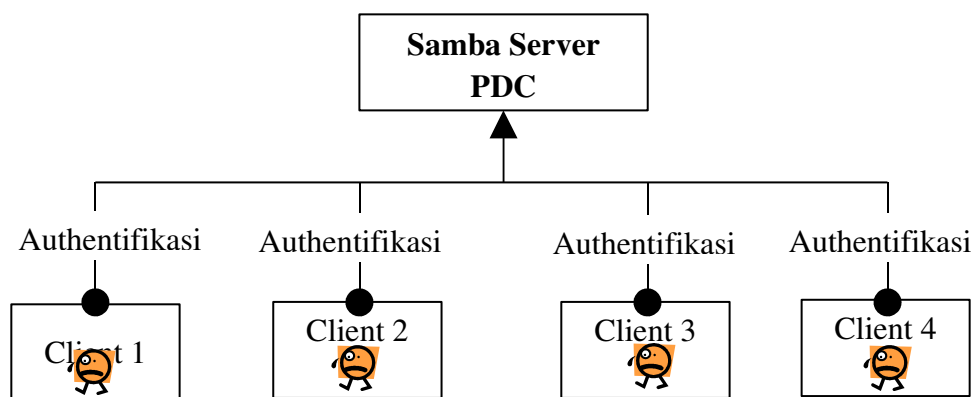
```
path = "Isikan Path file yang akan di share"
```

```
read only = "Yes/No"  
  browseable = "Yes/No"  
create mask = 0600
```

[printers]

```
comment = All Printers  
path = "Isikan Path printer"  
printable = "Yes/No"  
browseable = "Yes/No"
```

Masing masing label di atas ditandai dengan kurung siku (tanda [dan]). Masing masing label memiliki satu bagian. Ada dua kategori bagian bagian tersebut, yaitu kategori global dan kategori share. Kategori global didefinisikan dengan label [global], sedangkan semua bagian yang lain masuk ke dalam kategori share.



Aplikasi samba biasanya dijalankan di daemon. Dua aplikasi utamanya adalah:

1. **smbd**
Daemon yang memberikan layanan berbagi file dan printer dalam sebuah jaringan yang menggunakan protocol SMB. Smbd juga memberikan otentikasi dan otorisasi bagi kliennya.
2. **nmbd**
Daemon yang memanfaatkan *Windows Internet Name Service* (WINS), dan membantu klien untuk browsing di *network neighborhood*.

Selain 2 daemon utama tadi, aplikasi samba juga mempunyai beberapa program pendukung yaitu :

1. **smbclient**
Klien dengan tampilan mirip ftp untuk mengakses SMB resource share (mengakses share file).
2. **smbtar**
Program yang mem-back-up data yang dishare. Mirip tar di Linux.
3. **nmblookup**

Program yang membantu mencari nama (names lookup) dengan memanfaatkan NetBios over TCP/IP. Nmblookup dapat digunakan untuk meresolve dari nama komputer ke nomer IP dan sebaliknya.

4. smbpasswd

Program yang memungkinkan administrator mengatur password yang terenskripsi yang dipergunakan oleh samba server.

5. smbstatus

Program yang memonitor status terakhir dari share resources yang diberikan oleh service samba.

6. testparm

Program kecil untuk melakukan proses debug (memeriksa parameter) terhadap file konfigurasi samba (smb.conf)

7. swat

Samba Web Administration Tool, program Bantu yang memberikan interface model web untuk mengadministrasi Samba. SWAT yang mempermudah edit smb.conf (file konfigurasi samba) mengatur resource share, melihat status samba terakhir, dengan dukungan-dukungan file help yang sangat bermanfaat.

IV. Langkah-langkah Percobaan

1. Install samba PDC

```
samba:/#apt-get install samba
```

2. Konfigurasi file smb.conf

```
samba:/# vim /etc/samba/smb.conf
```

```
# Date: 2005/04/05 09:17:47
```

```
# Global parameters
```

```
[global]
```

```
workgroup = KELOMPOK1
```

```
server string = SAMBA/NT-PDC
```

```
min password length = 0
```

```
null passwords = Yes
```

```
password server = None
```

```
pam password change = Yes
```

```
passwd program = /usr/bin/passwd %u; #cd /var/yp; make;
```

```
passwd chat debug = Yes
```

```
unix password sync = Yes
```

```
log file = /var/log/samba/%m.log
```

```
max log size = 50
```

```
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
```

```
add user script = /usr/sbin/useradd -d /dev/null -g 100 -
```

```
/bin/false -M %u
```

```
logon script = scripts/%U.bat
```

```
domain logons = Yes
```

```
os level = 65
```

```
preferred master = Yes
```

```
domain master = Yes
```

```
dns proxy = No
```

```
ldap ssl = no
```

```
guest ok = Yes
```

```
veto files = /Network Trash
```


Folder/TheVolumeSettingsFolder/lost+found/

[printers]

comment = All Printers
path = /var/spool/samba
printable = Yes
browseable = No

[netlogon]

path = /var/lib/samba/netlogon

[share]

path = /root/home/kelompok1/arief
read only = No
browseable = Yes

Workgroup : menunjukkan workgroup atau domain dari jaringan kita, Jika di dalam jaringan yang kita gunakan adalah PDC yang mengelola domain “KELOMPOK 1” maka workgroup harus di isi dengan “KELOMPOK 1”

Server String : Memberikan Keterangan atau menunjukkan deskripsi dari server kita

Host Allow : Memberi batasan pada mesin akan alamat-alamat IP mana saja yang di izinkan untuk mengakses server samba kita

Socket options : Memberi kita pilihan untuk mempercepat akses

Interfaces : Menunjukkan IP interfaces mana saja di server samba yang di beri hak mengakses server samba

Remote Browse Sync: Berguna untuk sebuah jaringan yang kebetulan ada server windows NT di dalamnya.

Remote announce: Memberikan alamat IP tempat server Samba akan mengumumkan daftar resource yang di miliki.

Local master: menunjukkan apa kita ingin menjadikan server samba sebagai master browser di dalam subnet kita.

OS Level: Merupakan angka dari 0-255 yang menentukan level server samba kita.

Domain Master : menunjukkan apakah di dalam domain windows NT kita, server samba akan menjadi domain master server. Jawaban boolean yes or no saja

Prefered master: Menentukan apalah server samba kita selalu menjadi master browser

Domain logons : Merupakan konfigurasi untuk menentukan apakah kita ingin menjadikan server samba kita sebagai Primary Domain Controler (PDC)

Security: Opsi ini mempengaruhi cara samba dan kliennya berinteraksi dan merupakan salah satu faktor terpenting dalam smb.conf

3. Tes Konfigurasi dengan testparm

`samba:~# testparm /etc/samba/smb.conf`

Load smb config files from /etc/samba/smb.conf

Unknown parameter encountered: "encrypt password"

Ignoring unknown parameter "encrypt password"

Processing section "[homes]"

Processing section "[printers]"

Processing section "[netlogon]"

Processing section "[profiles]"

Loaded services file OK.

WARNING: You have some share names that are longer than 12 characters.
These may not be accessible to some older clients.

(Eg. Windows9x, WindowsMe, and smbclient prior to Samba 3.0.)

Server role: ROLE_DOMAIN_PDC

Press enter to see a dump of your service definitions

Global parameters

[global]

```
workgroup = KELOMPOK1
server string = Samba/NT-PDC
password server = None
log file = /var/log/samba/%m.log
max log size = 50
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
logon path = \\%L\profiles\%U //%L=domain name %U=user
logon drive = H:          //buat file server samba
logon home = \\%L\%U
domain logons = Yes
os level = 65
preferred master = Yes
domain master = Yes
dns proxy = No
ldap ssl = no
winbind use default domain = Yes
guest ok = Yes
```

[printers]

```
comment = All Printers
path = /var/spool/samba
printable = Yes
browseable = No
```

[netlogon]

```
comment = Network Logon Service
path = /var/lib/samba/netlogon
```

[share]

```
path = /root/home/kelompok1/arief
read only = No
browseable = Yes
```

4. Buat direktori baru untuk server

```
samba:~# useradd arief
```

```
samba:~# passwd arief
```

Enter new UNIX password:

Retype new UNIX password:

passwd: password updated successfully

```
samba:~# smbpasswd -a arief
```

New SMB password:

Retype new SMB password:

Added user arief.

```
samba:~# useradd agus
samba:~# passwd agus
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
samba:~# smbpasswd -a agus
New SMB password:
Retype new SMB password:
Added user agus.
```

5. Buat Pengenal Nama Computer Client Di Server

```
samba:~# useradd -d /dev/null -s /bin/false cisco2$
samba:~# smbpasswd -a -m cisco2
```

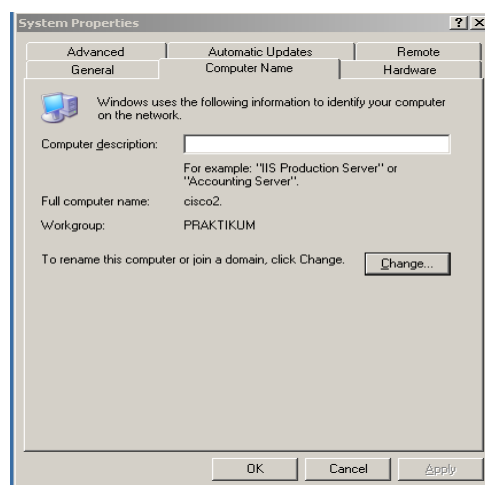
6. Mengaktifkan service samba

```
samba:~# /etc/init.d/samba start
samba:~# /etc/init.d/samba restart
samba:~# /etc/init.d/samba stop
```

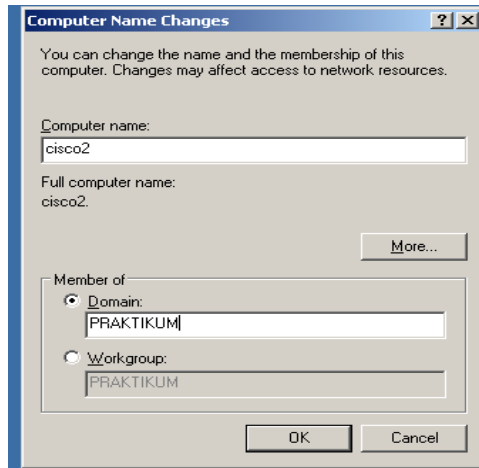
Konfigurasi samba client pada Windows NT/XP

- Buka local security (Start -> All Programs -> Administrative Tools-> Local Security Policy). Untuk Windows NT
- Buka Computer Name ((Start -> Control Pane -> Syste -> Computer Name). Untuk Windows XPI
- Masukkan “Domain member: enkripsi digital atau sign secure”. Disable.
- Masukkan “Domain member: rubah password account mesin dengan disable”.
- Masukkan “Domain member: Windows 2000 atau yang lebih tinggi”. Disable.
- Sekarang bergabung domain sama seperti untuk Windows NT atau 2000. klik kanan MyComputer, pilih Properties, Computer Name dan Rubah. Atau klik table Network dan jalankan Network Wizard.

Masuk ke System Properties dan Klik Change

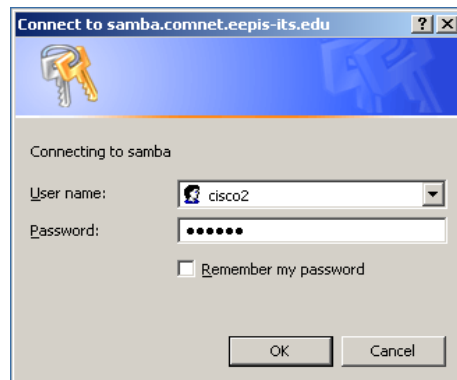


Masuk ke Computer name Change



Member Workgroup Off diganti dengan Domain sehingga pada waktu Login, langsung ke Primary Domain Controller (PDC)

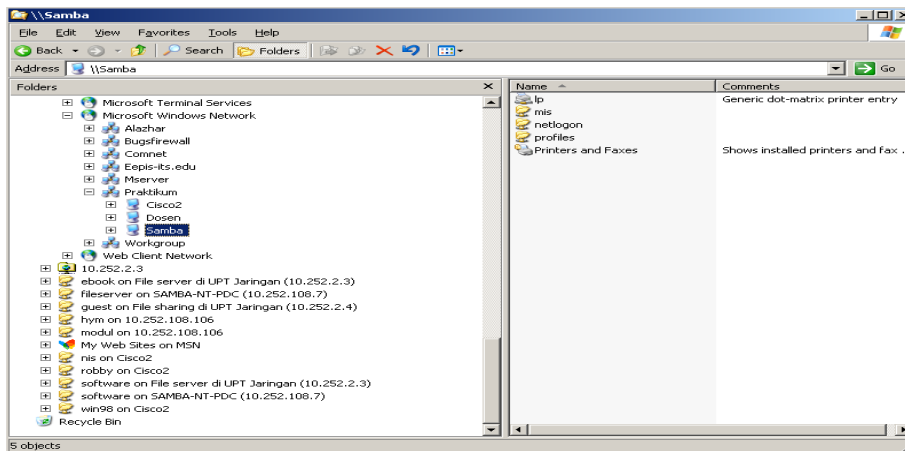
Mengakses Computer Samba Dari Windows Tanpa Domain Control



Mengakses Computer Samba Dari Windows Dengan Domain Control (Menggunakan Software VMWare)



Tampilan Explorer Client Samba



V. Kesimpulan

Samba merupakan aplikasi unix yang memanfaatkan protocol SMB (Server Message Block). Samba memungkinkan mesin linux berkomunikasi dengan mesin Windows. Samba juga bisa digunakan untuk berbagi/share file dan printer pada semua komputer yang terhubung ke jaringan, Meskipun tidak semua fungsi Windows Nt bisa digantikan oleh samba, tetapi hampir seluruh tugas pokok Windows NT PDC sudah bisa ditangani oleh samba. Berikut ini adalah beberapa tugas PDC yang bisa ditangani oleh samba :

- Menyediakan layanan log on ke domain untuk klien Windows 95/98, NT, 2000, XP dengan menggunakan database password terpusat.
- Memberikan hak administratif terhadap user – user domain tertentu.
- Memberikan policy tertentu kepada workstation Windows 95/98, NT, 2000, XP.
- Memberikan log on script kepada user – user yang melakukan log on ke domain.
- Mengelola profile untuk user – user domain.
- Melakukan validasi user yang menggunakan sistem lain melalui protokol SMB.

BAB VI FIREWALL

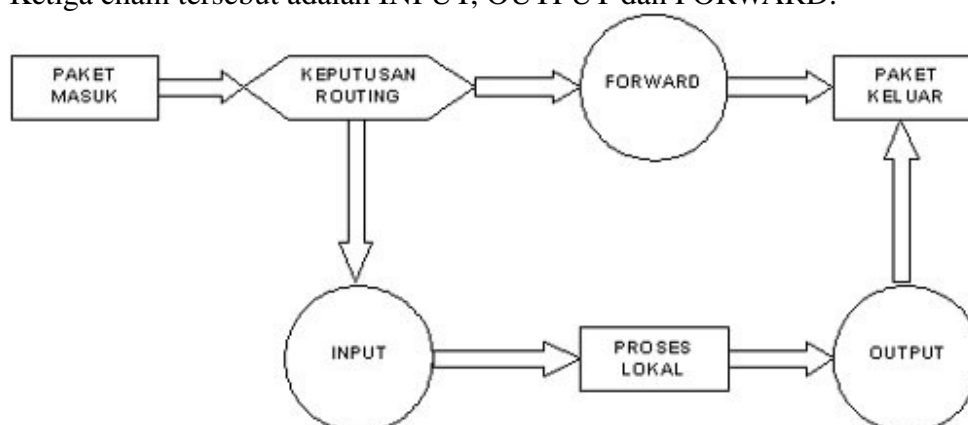
I. TUJUAN

- Mampu men-setting jaringan komputer lokal dengan menggunakan teknik NAT, kemudian membandingkan bila jaringan tersebut tidak menggunakan NAT.
- Mampu men-setting jaringan dimana dengan menggunakan satu router dapat menghubungkan antar jaringan, yang salah satu client dari jaringan tersebut berfungsi sebagai web server dan ftp server.
- Mampu Mengontrol mengeblok client supaya tidak bisa mengakses web server atau ftp server.

II. DASAR TEORI

A. IPTABLES

IPTables memiliki tiga macam daftar aturan bawaan dalam tabel penyaringan, daftar tersebut dinamakan rantai firewall (firewall chain) atau sering disebut chain saja. Ketiga chain tersebut adalah INPUT, OUTPUT dan FORWARD.



Pada diagram tersebut, lingkaran menggambarkan ketiga rantai atau chain. Pada saat sebuah paket sampai pada sebuah lingkaran, maka disitulah terjadi proses penyaringan. Rantai akan memutuskan nasib paket tersebut. Apabila keputusannya adalah DROP, maka paket tersebut akan di-drop. Tetapi jika rantai memutuskan untuk ACCEPT, maka paket akan dilewatkan melalui diagram tersebut.

Sebuah rantai adalah aturan-aturan yang telah ditentukan. Setiap aturan menyatakan “jika paket memiliki informasi awal (header) seperti ini, maka inilah yang harus dilakukan terhadap paket”. Jika aturan tersebut tidak sesuai dengan paket, maka aturan berikutnya akan memproses paket tersebut. Apabila sampai aturan terakhir yang ada, paket tersebut belum memenuhi salah satu aturan, maka kernel akan melihat kebijakan bawaan (default) untuk memutuskan apa yang harus dilakukan kepada paket tersebut. Ada dua kebijakan bawaan yaitu default DROP dan default ACCEPT.

Jalannya sebuah paket melalui diagram tersebut bisa dicontohkan sebagai berikut:

Perjalanan paket yang diforward ke host yang lain

1. Paket berada pada jaringan fisik, contoh internet.
2. Paket masuk ke interface jaringan, contoh eth0.
3. Paket masuk ke chain PREROUTING pada table Mangle. Chain ini berfungsi untuk me-mangle (menghaluskan) paket, seperti merubah TOS, TTL dan lain-lain.
4. Paket masuk ke chain PREROUTING pada tabel nat. Chain ini berfungsi utamanya untuk melakukan DNAT (Destination Network Address Translation).
5. Paket mengalami keputusan routing, apakah akan diproses oleh host lokal atau diteruskan ke host lain.
6. Paket masuk ke chain FORWARD pada tabel filter. Disinilah proses pemfilteran yang utama terjadi.
7. Paket masuk ke chain POSTROUTING pada tabel nat. Chain ini berfungsi utamanya untuk melakukan SNAT (Source Network Address Translation).
8. Paket keluar menuju interface jaringan, contoh eth1.
9. Paket kembali berada pada jaringan fisik, contoh LAN.

Perjalanan paket yang ditujukan bagi host lokal

1. Paket berada dalam jaringan fisik, contoh internet.
2. Paket masuk ke interface jaringan, contoh eth0.
3. Paket masuk ke chain PREROUTING pada tabel mangle.
4. Paket masuk ke chain PREROUTING pada tabel nat.
5. Paket mengalami keputusan routing.
6. Paket masuk ke chain INPUT pada tabel filter untuk mengalami proses penyaringan.
7. Paket akan diterima oleh aplikasi lokal.

Perjalanan paket yang berasal dari host lokal

1. Aplikasi lokal menghasilkan paket data yang akan dikirimkan melalui jaringan.
2. Paket memasuki chain OUTPUT pada tabel mangle.
3. Paket memasuki chain OUTPUT pada tabel nat.
4. Paket memasuki chain OUTPUT pada tabel filter.
5. Paket mengalami keputusan routing, seperti ke mana paket harus pergi dan melalui interface mana.
6. Paket masuk ke chain POSTROUTING pada tabel NAT.
7. Paket masuk ke interface jaringan, contoh eth0.
8. Paket berada pada jaringan fisik, contoh internet.
9. Sintaks IPTables

`iptables [-t table] command [match] [target/jump]`

Table

IPTables memiliki 3 buah tabel, yaitu NAT, MANGLE dan FILTER. Penggunaannya disesuaikan dengan sifat dan karakteristik masing-masing. Fungsi dari masing-masing tabel tersebut sebagai berikut :

NAT : Secara umum digunakan untuk melakukan Network Address Translation. NAT adalah penggantian field alamat asal atau alamat tujuan dari sebuah paket.

MANGLE : Digunakan untuk melakukan penghalusan (mangle) paket, seperti TTL, TOS dan MARK.

FILTER : Secara umum, inilah pemfilteran paket yang sesungguhnya.. Di sini bisa ditentukan apakah paket akan di-DROP, LOG, ACCEPT atau REJECT

B. NAT (=Network Address Translation (IP Masquarade)

NAT (Network Address Translation) adalah teknik pemecahan suatu IP number, sehingga satu nomer IP dapat dipecah menjadi banyak. Berguna sekali bila memiliki persediaan IP Publik yang terbatas. Selain itu berfungsi untuk melindungi Network yang berada di bawah Router agar tidak bisa diketahui secara langsung IP address yang ada di network tersebut dari luar network yang bersangkutan.

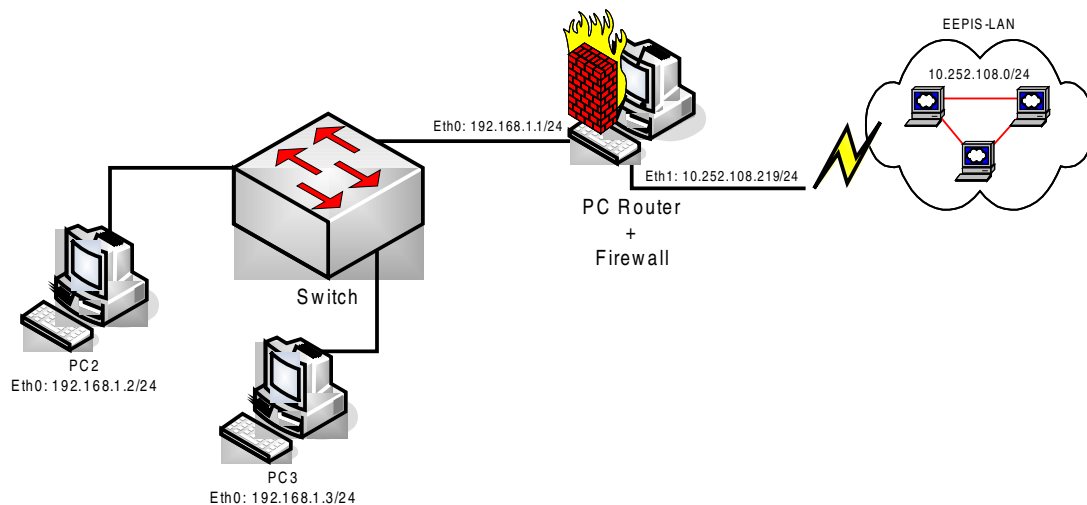
Setting jaringan untuk IP menggunakan NAT:

1. # apt-get install iptables
2. # iptables -t nat -A POSTROUTING -j MASQUERADE

C. Mengeblok _PC2 dan PC3 tidak bias mengakses Web dan FTP

Setting Jaringan pada PC1 untuk PC2 tidak bisa mengakses Web dan untuk PC3 tidak bisa mengakses FTP

III. Topology Praktikum



IV. LANGKAH-LANGKAH PERCOBAAN

1. Setting Ip_forward

1. #cat /proc/sys/net/ipv4/ip_forward "0 or 1"
2. #echo 1> /proc/sys/net/ipv4/ip_forward

2. Setting menggunakan NAT

1. # apt-get install iptables
2. # iptables -t nat -A POSTROUTING -j MASQUERADE

3. Setting mengeblok PC2 dan PC3 supaya tidak bisa mengakses web dan FTP

V. HASIL PERCOBAAN

A. Percobaan (Tanpa NAT).

1. Komputer PC 1

```
[bugsfirewall@root]# ifconfig
```

```
eth0 Link encap:Ethernet HWaddr 00:00:E2:9A:C1:BE
      inet addr:192.168.1.1 Bcast:192.168.1.255 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:3180 errors:0 dropped:0 overruns:0 frame:0
      TX packets:1513 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:100
      RX bytes:240536 (234.8 Kb) TX bytes:144341 (140.9 Kb)
      Interrupt:11 Base address:0xc000 Memory:ec000000-ec000038
```

```
eth0:1Link encap:Ethernet HWaddr 00:00:E2:9A:C1:BE
      inet addr:10.252.108.219 Bcast:10.252.108.255 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:3180 errors:0 dropped:0 overruns:0 frame:0
      TX packets:1513 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:100
      RX bytes:240536 (234.8 Kb) TX bytes:144341 (140.9 Kb)
      Interrupt:11 Base address:0xc000 Memory:ec000000-ec000038
```

```
lo Link encap:Local Loopback
   inet addr:127.0.0.1 Mask:255.0.0.0
   UP LOOPBACK RUNNING MTU:16436 Metric:1
   RX packets:37136 errors:0 dropped:0 overruns:0 frame:0
   TX packets:37136 errors:0 dropped:0 overruns:0 carrier:0
   collisions:0 txqueuelen:0
   RX bytes:2534273 (2.4 Mb) TX bytes:2534273 (2.4 Mb)
```

```
[bugsfirewall@root]# route add default gw 10.252.108.1
```

```
[bugsfirewall@root]# route
```

```
Kernel IP routing table
```

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
10.252.108.0	*	255.255.255.0	U	0	0	0	eth1
192.168.1.0	*	255.255.255.0	U	0	0	0	eth0
127.0.0.0	*	255.0.0.0	U	0	0	0	lo
default	10.252.108.1	0.0.0.0	UG	0	0	0	eth1

```
[bugsfirewall@root]# cat /proc/sys/net/ipv4/ip_forward
```

```
0
```

```
[bugsfirewall@root]# echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
[bugsfirewall@root]# cat /proc/sys/net/ipv4/ip_forward
```

```
1
```

- Untuk mengetahui siapa saja yang mengakses PC yang kita gunakan, lakukan perintah finger.

```
[bugsfirewall@root]# finger
```

```
Login Name Tty Idle Login Time Office Office Phone
```

```

depan          pts/2   Feb 14 18:54 (192.168.1.2)
root           pts/3   Feb 14 18:54 (192.168.1.3)
root root      *:0     Feb 14 17:12 Programmin 031-5947280
root root      pts/1   Feb 14 18:03 (:0.0)

```

2. Komputer PC2

```

[depan@root]# ifconfig
eth0  Link encap:Ethernet HWaddr 00:00:E2:9A:C1:BE
      inet addr:192.168.1.2 Bcast:192.168.1.255 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:3180 errors:0 dropped:0 overruns:0 frame:0
      TX packets:1513 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:100
      RX bytes:240536 (234.8 Kb) TX bytes:144341 (140.9 Kb)
      Interrupt:11 Base address:0xc000 Memory:ec000000-ec000038

```

```

lo    Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      UP LOOPBACK RUNNING MTU:16436 Metric:1
      RX packets:37136 errors:0 dropped:0 overruns:0 frame:0
      TX packets:37136 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:2534273 (2.4 Mb) TX bytes:2534273 (2.4 Mb)

```

```

[depan@root]# route add default gw 192.168.1.1

```

```

[depan@root]# route

```

```

Kernel IP routing table

```

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
192.168.1.0	*	255.255.255.0	U	0	0	0	eth0
127.0.0.0	*	255.0.0.0	U	0	0	0	lo
default	192.168.1.1	0.0.0.0	UG	0	0	0	eth0

3. Komputer PC3

```

[root@root]# ifconfig

```

```

eth0  Link encap:Ethernet HWaddr 00:00:E2:9A:C1:BE
      inet addr:192.168.1.3 Bcast:192.168.1.255 Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:3180 errors:0 dropped:0 overruns:0 frame:0
      TX packets:1513 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:100
      RX bytes:240536 (234.8 Kb) TX bytes:144341 (140.9 Kb)
      Interrupt:11 Base address:0xc000 Memory:ec000000-ec000038

```

```

lo    Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      UP LOOPBACK RUNNING MTU:16436 Metric:1
      RX packets:37136 errors:0 dropped:0 overruns:0 frame:0

```

```
TX packets:37136 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:2534273 (2.4 Mb) TX bytes:2534273 (2.4 Mb)
```

```
[root@root]# route add default gw 192.168.1.1
[root@root]# route
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
192.168.1.0 * 255.255.255.0 U 0 0 0 eth0
127.0.0.0 * 255.0.0.0 U 0 0 0 lo
default 192.168.1.1 0.0.0.0 UG 0 0 0 eth0
```

B. Percobaan (Dengan NAT).

1. Komputer PC 1

```
[bugsfirewall@root]# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
From 192.168.1.1: icmp_seq=1 Redirect Host(New nexthop: 192.168.1.2)
64 bytes from 192.168.1.2: icmp_seq=1 ttl=63 time=0.364 ms
```

```
--- 192.168.1.2 ping statistics ---
6 packets transmitted, 1 received, 83% packet loss, time 5004ms
rtt min/avg/max/mdev = 0.364/0.364/0.364/0.000 ms
```

```
[bugsfirewall@root]# ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(82) bytes of data.
From 192.168.1.1: icmp_seq=1 Redirect Host(New nexthop: 192.168.1.3)
64 bytes from 192.168.1.3: icmp_seq=1 ttl=63 time=0.364 ms
```

```
--- 192.168.1.3 ping statistics ---
6 packets transmitted, 1 received, 83% packet loss, time 5004ms
rtt min/avg/max/mdev = 0.364/0.364/0.364/0.000 ms
```

2. Komputer PC2

```
[depan@root]# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
From 192.168.1.2: icmp_seq=1 Redirect Host(New nexthop: 192.168.1.1)
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63 time=0.364 ms
```

```
--- 192.168.1.1 ping statistics ---
6 packets transmitted, 1 received, 83% packet loss, time 5004ms
rtt min/avg/max/mdev = 0.364/0.364/0.364/0.000 ms
```

```
[depan@root]# ping 192.168.1.3
PING 192.168.1.3 (192.168.1.3) 56(84) bytes of data.
64 bytes from 192.168.1.3: icmp_seq=1 ttl=64 time=0.193 ms
64 bytes from 192.168.1.3: icmp_seq=2 ttl=64 time=0.162 ms
```

```
--- 192.168.1.3 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 0.162/0.177/0.193/0.020 ms
```

```
[depan@root]# ping 10.252.108.219
PING 10.252.108.219 (10.252.108.219) 56(84) bytes of data.
64 bytes from 10.252.108.219: icmp_seq=1 ttl=64 time=0.193 ms
64 bytes from 10.252.108.219: icmp_seq=2 ttl=64 time=0.162 ms
```

```
--- 10.252.108.219 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 0.162/0.177/0.193/0.020 ms
```

3. Komputer PC3

```
[root@root]# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
From 192.168.1.3: icmp_seq=1 Redirect Host(New nexthop: 192.168.1.1)
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63 time=0.364 ms
```

```
--- 192.168.1.1 ping statistics ---
6 packets transmitted, 1 received, 83% packet loss, time 5004ms
rtt min/avg/max/mdev = 0.364/0.364/0.364/0.000 ms
```

```
[root@root]# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=0.193 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=0.162 ms
```

```
--- 192.168.1.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 0.162/0.177/0.193/0.020 ms
```

```
[root@root]# ping 10.252.108.219
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 10.252.108.219: icmp_seq=1 ttl=64 time=0.193 ms
64 bytes from 10.252.108.219: icmp_seq=2 ttl=64 time=0.162 ms
```

```
--- 10.252.108.219 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1010ms
rtt min/avg/max/mdev = 0.162/0.177/0.193/0.020 ms
```

C. Blok PC2 dan PC3 agar tidak bisa akses web dan FTP

dilakukan dengan perintah:

```
# iptables -t Filter -A FORWARD -s 192.168.1.0/24 -d 0.0.0.0 -p tcp --dport 80 -j DROP
# iptables -t Filter -A FORWARD -s 192.168.1.0/24 -d 0.0.0.0 -p tcp --dport 21 -j DROP
```

VI. KESIMPULAN

- **NAT (=Network Address Translation (IP Masquarade)** adalah teknik pemecahan suatu IP number, sehingga satu nomer IP dapat dipecah menjadi banyak. Selain itu berfungsi untuk melindungi Network yang berada di bawah Router agar tidak bisa diketahui secara langsung IP address yang ada di network tersebut
- Perbedaan antara jaringan yang menggunakan Teknik NAT dengan yang tidak menggunakan teknik NAT, adalah pada saat dilakukan proses monitoring pengaksesan IP number.
- Apabila jaringan tersebut **menggunakan NAT** maka IP number yang tampak adalah **IP number dari router** saja. Sedangkan jaringan yang **tidak menggunakan teknik NAT**, IP number yang tampak adalah **IP number dari masing-masing PC client**.
- Rule dari firewall juga bisa diset agar client tidak bisa mengakses aplikasi tertentu berdasarkan nomor port yang digunakan. misalnya: aplikasi FTP dengan nomor port 21 atau web dengan nomor port 80