MODUL 1
DOMAIN NAME SERVER [DNS] DENGAN BIND 9

TUJUAN PEMBELAJARAN:

1. Mengenalkan pada mahasiswa tentang konsep DNS di linux
2. Mahasiswa memahami cara instalasi DNS di Linux
3. Mahasiswa mampu melakukan troubleshooting DNS di Linuz

DASAR TEORI

1. Sejarah DNS

Sebelum dipergunakannya DNS, jaringan komputer menggunakan HOSTS files yang berisi informasi dari nama komputer dan IP address-nya. Di Internet, file ini dikelola secara terpusat dan di setiap loaksi harus di copy versi terbaru dari HOSTS files, dari sini bisa dibayangkan betapa repotnya jika ada penambahan 1 komputer di jaringan, maka kita harus copy versi terbaru file ini ke setiap lokasi. Dengan makin meluasnya jaringan internet, hal ini makin merepotkan, akhirnya dibuatkan sebuah solusi dimana DNS di desain menggantikan fungsi HOSTS files, dengan kelebihan unlimited database size, dan performace yang baik. DNS adalah sebuah aplikasi services di Internet yang menerjemahkan sebuah domain name ke IP address. Sebagai contoh, www untuk penggunaan di Internet, lalu diketikan nama domain, misalnya: yahoo.com maka akan di petakan ke sebuah IP mis 202.68.0.134. Jadi DNS dapat di analogikan pada pemakaian buku telepon, dimana orang yang kita kenal berdasarkan nama untuk menghubunginya kita harus memutar nomor telepon di pesawat telepon. Sama persis, host komputermengirimkan queries berupa nama komputer dan domain name server ke DNS, lalu oleh DNS dipetakan ke IP address.

2. Domain Name System (DNS)

Domain Name System (DNS) adalah distribute database system yang digunakan untuk pencarian nama komputer (name resolution) di jaringan yang mengunakan TCP/IP (Transmission Control
Protocol/Internet Protocol). DNS biasa digunakan pada aplikasi yang terhubung ke Internet seperti web browser atau e-mail, dimana DNS membantu memetakan host name sebuah computer ke IP address. Selain digunakan di Internet, DNS juga dapat di implementasikan ke private network atau intranet dimana DNS memiliki keunggulan seperti:

1. **Mudah**, DNS sangat mudah karena user tidak lagi direpotkan untuk mengingat IP address sebuah komputer cukup host name (nama Komputer).
2. **Konsisten**, IP address sebuah komputer bisa berubah tapi host name tidak berubah.
3. **Simple**, user hanya menggunakan satu nama domain untuk mencari baik di Internet maupun di Intranet.

3. Apa itu DNS?

DNS dapat disamakan fungsinya dengan buku telepon. Dimana setiap komputer di jaringan Internet memiliki host name (nama komputer) dan Internet Protocol (IP) address. Secara umum, setiap client yang akan mengkoneksikan komputer yang satu ke komputer yang lain, akan menggunakan host name. Lalu komputer anda akan menghubungi DNS server untuk mencek host name yang anda minta tersebut berapa IP address-nya. IP address ini yang digunakan untuk mengkoneksikan komputer anda dengan komputer lainnya.

4. Struktur DNS

Domain Name Space merupakan sebuah hirarki pengelompokan domain berdasarkan nama, yang terbagi menjadi beberapa bagian diantaranya:

Root-Level Domains

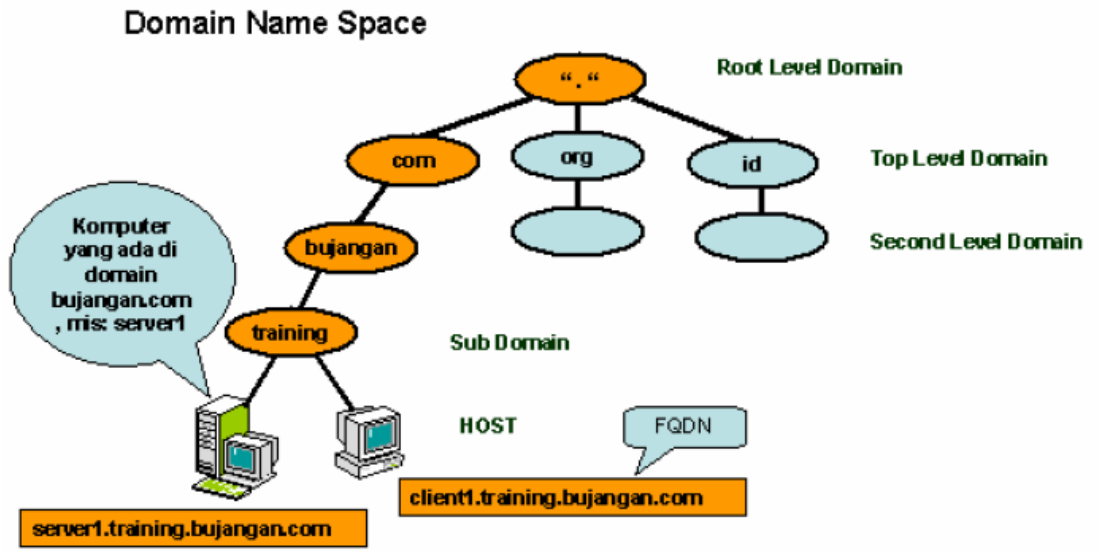
Domain ditentukan berdasarkan tingkatan kemampuan yang ada di struktur hirarki yang disebut dengan level. Level paling atas di hirarki disebut dengan root domain. Root domain di ekspresikan berdasarkan periode dimana lambang untuk root domain adalah (“.”).

Top-Level Domains

Pada bagian dibawah ini adalah contoh dari top-level domains:

- **com** Organisasi Komersial
- **edu** Institusi pendidikan atau universitas
- **org** Organisasi non-profit
- **net** Networks (backbone Internet)
- **gov** Organisasi pemerintah non militer
- **mil** Organisasi pemerintah militer
- **num** No telpon
- **arpa** Reverse DNS
- **xx** dua-huruf untuk kode negara (id:Indonesia,sg:singapura,au:australia,dll)

Top-level domains dapat berisi second-level domains dan hosts.



Second-Level Domains

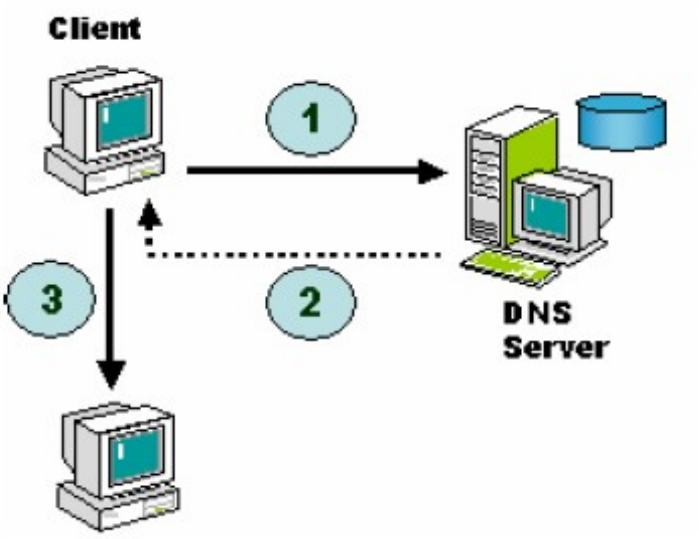
Second-level domains dapat berisi host dan domain lain, yang disebut dengan subdomain. Untuk contoh: Domain Bujangan, bujangan.com terdapat komputer (host) seperti server1.bujangan.com dan subdomain training.bujangan.com. Subdomain training.bujangan.com juga terdapat komputer (host) seperti client1.training.bujangan.com.

Host Names

Domain name yang digunakan dengan host name akan menciptakan fully qualified domain name (FQDN) untuk setiap komputer. Sebagai contoh, jika terdapat fileserver1.detik.com, dimana fileserver1 adalah host name dan detik.com adalah domain name.

5. Bagaimana DNS itu bekerja?

Fungsi dari DNS adalah menerjemahkan nama komputer ke IP address (memetakan). Client DNS disebut dengan resolvers dan DNS server disebut dengan name servers. Resolvers atau client mengirimkan permintaan ke name server berupa queries. Name server akan memproses dengan cara mencek ke local database DNS, menghubungi name server lainnya atau akan mengirimkan message failure jika ternyata permintaan dari client tidak ditemukan.



Proses tersebut disebut dengan **Forward Lookup Query**, yaitu permintaan dari client dengan cara memetakan nama komputer (host) ke IP address.

1. Resolvers mengirimkan queries ke name server
2. Name server mencek ke local database, atau menghubungi name server lainnya, jika ditemukan akan diberitahukan ke resolvers jika tidak akan mengirimkan failure message
3. Resolvers menghubungi host yang dituju dengan menggunakan IP address yang diberikan name server

TUGAS PENDAHULUAN

1. Jelaskan fungsi DNS !
2. Apa fungsi file /etc/hosts? Dan file /etc/host.conf ? Tuliskan isi kedua file tersebut.
3. Jika kita ingin mengeset DNS pada client, di file mana kita bisa menambahkan no IP DNS server? Bagaimana cara menambahkan DNS server ?
4. File-file apa yang dibutuhkan untuk seting DNS server?
5. Apa fungsi secondary name server?

PERCOBAAN

1. Install paket DNS

Cek apakah paket2 tersebut sudah terinstall di komputer anda, yaitu bind-utils, bind-libs, bind-chroot, bind dan ypbind serta caching-nameserver.Jika belum, mintalah file-file yang dibutuhkan untuk instalasi. (Petunjuk : gunakan rpm -qa | grep bind)

Pertanyaan :

a. Bind versi berapa yang digunakan untuk percobaan ini ?

b. Apa guna file-file berikut :

a. bind

b. bind-utils

c. bind-libs

d. bind-chroot

e. ypbind

f. caching-nameserver

2. Menjalankan bind-chroot :

- Periksalah apakah daemon bind sudah berjalan atau belum dengan perintah :

  # nmap localhost
- Jika sudah matikan dengan perintah :

  # /etc/init.d/named stop
- Bila daemon bind sudah tidah berjalan, lalukan perintah dibawah :

  # chmod 755 /var/named/

  # chmod 775 /var/named/chroot/

  # chmod 775 /var/named/chroot/var/

  # chmod 755 /var/named/chroot/var/named/

  # chmod 775 /var/named/chroot/var/run/

  # chmod 777 /var/named/chroot/var/run/named/

  # cd /var/named/chroot/var/named/

  # ln -s ../../ chroot ?

  # chkconfig --levels 235 named on

  # /etc/init.d/named start

3. Check lagi dengan perintah nmap localhost. Cek apakah port 53 sudah menyala, jika sudah berarti daemon sudah berjalan

nmap localhost

4. Persiapan setting domain baru

Dalam studi kasus kali ini, kita akan membuatdomain baru untuk DNS Server dan mail server, ftp server, http server, dengan data sebagai berikut:

Nama Domain : jerapah.com

Nama DNS Server : ns.jerapah.com

IP DNS Server : 10.252.105.33

Nama Mail Server : mail.jerapah.com

Nama HTTP Server : www. jerapah.com

Nama FTP Server : ftp.jerapah.com

Karena kita menggunakan IP Address yang sama untuk DNS Server dan (Mail Server, FTP Server, HTTP Server), maka kita akan menggunakan record CNAME (nama alias) dengan mendefi nisikan bahwa ns.example.com mempunyai nama alias (*mail.jerapah.com*, *ftp.jerapah.com*, dan *www.jerapah.com*

5. Konfigurasi bind

File-file yang harus diperhatikan untuk mengkonfi gurasikan BIND, antara lain:

1. var/named/chroot/etc/named.conf (berisi keterangan letak dan jenis database yang dibutuhkan oleh BIND).
2. var/named/chroot/var/named/jerapah.com.zone.db (berisi file zone dari jerapah.com)
3. var/named/chroot/var/named/jerapah.com.zone.local (berisi file reverse zone dari jerapah.com)
4. /var/named/chroot/etc/resolv.conf: (berisi alamat domain atau alamat IP dari name server).

Untuk server, file yang dikonfigurasi adalah named.conf dan beberapa file domain.

a. Mengedit file /var/named/chroot/etc/named.conf

Sekarang kita akan mendefinisikan bahwa DNS Server ini akan menjadi “authorative name server” untuk domain jerapah.com. Selain itu kita juga akan mendefi nisikan reverse DNS Zone jerapah.com. Sebelumnya copy file ini dari pengajar anda dan letakkan di folder yang telah

ditentukan. Untuk melakukan hal tersebut, Anda dapat mengedit file /etc/named.conf seperti di bawah ini:

- Carilah baris : include "/etc/rndc.key";
- Tambahkan baris ini diatas baris diatas :

```
zone "jerapah.com" {
                        type master;
                        file "jerapah.com.zone.db";
};
zone "105.252.10.in-addr.arpa" {
                type master;
                file "jerapah.com.zone.local";
};
```

Maksud dari bait pertama yang kita buat adalah, bahwa kita mendefinisikan DNS Server kita sebagai Primary Name Server untuk domain jerapah.com dan file jerapah.com.zone adalah nama file yang merupakan zone-zone file dari jerapah.zone

Maksud dari bait kedua adalah mendefinisikan Reverse DNS zone. Ini diperlukan agar DNS Server Anda dapat menerjemahkan dari nomor IPAddress ke nama host pemilik IP Address dalam jaringan tersebut

Ceklah konfigurasi zone anda dengan perintah :

usr/sbin/named-checkconf -t /var/named/chroot/etc/named.conf

Adakah kesalahan ? Capture hasilnya sbagai laporan. Bila tertulis error berikut, biarkan :

isc_dir_chroot: invalid file

b. Membuat file zone jerapah.com

Buatlah file : jerapah.com.zone.db dan simpan di /var/named/chroot/var/named/

```
$TTL 86400
@     IN     SOA    ns.jerapah.com. hostmaster.jerapah.com. (
                                                2001031102 ; serial
                                                10800 ; refresh
                                                3600 ;retry
                                                604800 ;expire
                                                86400 ;
```

```
                                                )

jerapah.com.    IN      NS          ns.jerapah.com.
                IN      MX          10              mail.jerapah.com.
ns              IN      A           10.252.102.110
mail            IN      CNAME       ns
www             IN      CNAME       ns
ftp             IN      CNAME       ns
```

Perhatikan !

1. Penulisan @ IN SOA sampai dengan hostmaster.jerapah.com harus sebaris.
2. Perhatikan peletakan titik ditiap penulisan nama domain seperti ns.jerapah.com, mail.jerapah.com dan hostmaster.jerapah.com.

Maksud dari baris di atas adalah sebagai berikut:

- **TTL (Time To Live)**: mendefi nisikan waktu lamanya data berada dalam database.
- **SOA (Start Of Authority)**: mendefinisikan hostname yang merupakan awal dari suatu zone.
- **ns.jerapah.com**: merupakan hostname yang memegang tanggung jawab terhadap domain jerapah.com.
- **hostmaster.jerapah.com**: merupakan alamat e-mail administrator yang memegang tanggung jawab terhadap domain jerapah.com.
- **502001031102 ;serial**: merupakan nomor serial dari zone file yang akan bertambah jika ada perubahan data.
- **10800;refresh**: merupakan selang waktu yang diperlukan secondary name server untuk memeriksa perubahan pada Primary Name Server.
- **3600;retry**: merupakan selang waktu secondary name server untuk mengulang pengecekan pada primary name server.
- **604800; expire** merupakan selang waktu zone file dipertahankan bila secondary name server tidak dapat melakukan pengecekan ke primary name server.
- **86400;ttl**: merupakan nilai default TTL untuk semua resource record pada zone-fi le.
- **jerapah.com. IN NS ns.jerapah.com**: mendefi nisikanbahwa hostname ns.jerapah.com yang memegang tanggung jawab terhadap domain jerapah.com.

- **IN MX 10 mail.jerapah.com**: mendefi nisikan bahwa hostname mail.example. com sebagai Mail Server pada domain example.com.
- **ns IN A 10.252.105.33**: mendefi nisikan bahwa hostname ns.example.com mempunyai IP Address 10.252.105.33
- **mail IN CNAME ns**: mendefi nisikanbahwa hostname ns.example.com mempunyainama alias mail.example.com.
- **www IN CNAME ns**: mendefi nisikan bahwa hostname ns.jerapah.com mempunyanama alias www.jerapah.com
- **ftp IN CNAME ns**: mendefi nisikan bahwa hostname ns.jerapah.com mempunyai nama alias ftp.example.com.

Ceklah konfigurasi zone anda dengan perintah :

```
# /usr/sbin/named-checkzone -t /var/named/chroot/var/named
jerapah.com jerapah.com.zone.db
```

Adakah kesalahan ? Capture hasilnya sebagai laporan.

Bila ada tulisan OK, berarti zone jerapah.com sudah benar penulisannya.

c. Setting reverse DNS

Setting reverse DNS dilakukan dengan membuat file bebek.com.zone.local dan simpan di /var/named/chroot/var/named/

```
$TTL 86400
@     IN     SOA       ns.jerapah.com. hostmaster.jerapah.com. (
                                          42   ; serial (d. adams)
                                          3H   ; refresh
                                          15M  ;retry
                                          1W   ; expire
                                          1D   ;minimum
                                          )

@ IN      NS                        ns.jerapah.com.
@ IN      A                         10.252.105.33
33        IN                        PTR             ns.jerapah.com.
```

Maksud dari baris di atas adalah sebagai berikut:

- Penjelasan yang lain, sama dengan penjelasan pada bagian jerapah.com.zone.

- 33 IN PTR ns.jerapah.com: mendefinisikan bahwa hostname ns.jerapah.com mempunyai IP Address 10.252.105.33

Ceklah konfigurasi zone anda dengan perintah :

```
# /usr/sbin/named-checkzone -t /var/named/chroot/var/named
105.252.10.in-addr.arpa jerapah.com.zone.local
```

Adakah kesalahan ? Capture hasilnya sebagai laporan.

Bila ada tulisan OK, berarti zone `105.252.10.in-addr.arpa` sudah benar penulisannya.

d. Membuat symlink antara file zone dan etc

ln -s /var/named/chroot/etc/named.conf /var/named/named.conf

ln -s /var/named/chroot/var/named/jerapah.com.zone.db /var/named/jerapah.com.zone.db

ln -s /var/named/chroot/var/named/jerapah.com.zone.local /var/named/jerapah.com.zone.local

Fingsi dari pembuatan symlink ini adalah untuk menghubungkan antara file-file yang berada pada lokasi aktual direktory /var/named/chroot/ ke direktori var/named. Jika anda perhatikan file /var/named/chroot/etc/named.conf, anda akan menemukan baris ini :

directory "/var/named";

Artinya bahwa file zone , reverse zone dan konfigurasi dirujuk pada direktory /var/named. Karena file sesungguhnya berada pada /var/named/chroot/ maka harus dibuat symlink antara dua direktori tersebut.

e. Coba lihat file /etc/syslog, perhatikan dimana letak log file untuk bind. Biasanya untuk fedora, redhat, log filenya akan diletakkan di /var/log/messages. Amatilah log file ini bila anda mengalami kegagalan menjalankan daemon bind dengan perintah :

grep named /var/log messages

f. Coba copykan file named.root pada direktory /var/named/chroot/var/named. File named.root bisa diambil dari file /usr/share/doc/bind-9.4.0/sample/var/named/named.root

g. Jalankan daemon bind, yaitu named dengan perintah :

/etc/init.d/named start

Atau :

service named start

adakah pesan kesalahan yang terutlis. Bila tidak, berarti anda sukses membangun DNS.

g. Setting file /etc/resolv.conf

Buka file diatas dan masukkan konfigurasi berikut. Bila sebelumnya sudah ada isi file, hapus saja. Simpan.

```
search jerapah.com
nameserver 10.252.105.33
```

h. Testing DNS Server lokal

- Sekarang kita akan mencoba menjalankan BIND dengan menjalankan perintah:

  # /etc/init.d/named restart
- Bila BIND telah berjalan dengan baik,Anda dapat melihat port 53 BIND telah berjalan dengan mengetikkan perintah nmap.

  # nmap localhost
- Kemudian kita dapat melakukan beberapa query ke DNS Server dengan menggunakan perintah:

  # host jerapah.com
- Coba catat hasil perintah berikut :

  #dig jerapah.com

- Catat juga hasil perintah berikut :

  #nslookup jerapah.com

i. testing DNS server dari client

- Pada server, hapus firewallnya :

  # iptables –F
- Pada client, hapus firewall dengan cara sama
- Pada client, buka file /etc/resolv.conf. Ganti baris berikut :

  search jerapah.com

nameserver 10.252.105.33

- Lakukan test seperti test yg dilakukan secara lokal. Bila gagal, berarti konfigurasi DNS anda salah. Catat hasil testing
- Coba ping dengan nama domain tersebut

  # ping www.jerapah.com

  # ping ftp.jerapah.com

  # ping mail.jerapah.com

  # ping ns.jerapah.com

  # dig jerapah.com

  # host www.bebek.com

  # host 10.252.105.33

  # nslookup www.bebek.com

  # nslookup 10.252.105.33

  Berhasilkah ? Jika berhasil, selamat, anda telah berhasil membuat DNS server.

Catatan :

Saat anda memberikan perintah ini :

```
# /usr/sbin/named-checkzone -t /var/named/chroot/var/named
105.252.10.in-addr.arpa jerapah.com.zone.local
```

Bila pesan ini muncul :

dns_rdata_fromtext: jerapah.com.zone.local:6: near eol: unexpected end of input

zone 105.252.10.in-addr.arpa/IN: loading from master file jerapah.com.zone.local failed: unexpected end of input

_default/105.252.10.in-addr.arpa/IN: unexpected end of input

Coba buka lagi file jerapah.com.zone.local dan tulis kembali baris yg salah, yaitu baris 6 (misalnya)

Saat anda memberikan perinta ini :

/usr/sbin/named-checkconf -t /var/named/chroot/etc/named.conf

Bila pesan ini muncul :

isc_dir_chroot: invalid file

File named.conf telah terkonfigurasi dengan benar.

LAPORAN RESMI

FORMAT LAPORAN RESMI

Nama dan NRP mahasiswa

Judul Percobaan : Domain Name Service [DNS]

Dasar Teori :

Tugas Pendahuluan :

Tuliskan kembali langkah-langkah praktikum dan setting file konfigurasi.

Jangan lupa sertakan hasil testing DNS

Daftar Pertanyaan

Berikan kesimpulan hasil praktikum yang anda lakukan.

Apa guna perintah nslookup, host dan dig?

Apa guna perintah nmap?

Sebutkan jenis-jenis serangan yang menyerang DNS?

Dimana DNS biasa diletakkan untuk alasan keamanan ? Petunjuk : DMZ (demiliterized zone)

Apa yang disebut secondary name server? Bagaimana cara settingannya pada DNS?

Apa fungsi nslookup, dig dan host ?