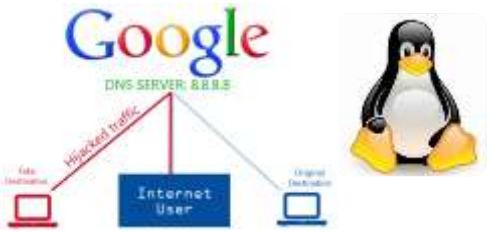
DNS SERVER

Yohanes Sukamdi, S.Kom



DNS merupakan sistem berbentuk database terdistribusi yang akan memetakan/mengkonversikan nama host/mesin/domain ke alamat IP (Internet Protocol) dan sebaliknya dari alamat IP ke nama host yang disebut dengan reverse-mapping.

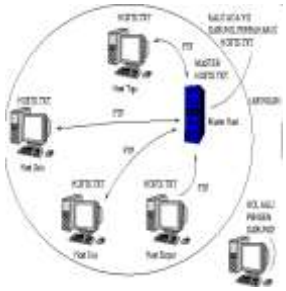
Penggunaan :

Untuk memetakan nama mesin misal **www.poltektegal.ac.id** ke alamat IP misal 202.154.187.7

Untuk routing e-mail, telnet, ftp, web, dan lain-lain.

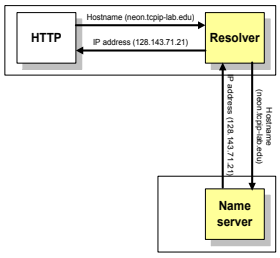
History

- Sebelum adanya DNS, tahun 1970-an ARPAnet menggunakan pemetaan dengan bentuk tabel host pada berkas HOSTS.TXT
- HOSTS.TXT berisi nama host dan alamat IP serta pemetaannya dari seluruh mesin/komputer yang terhubung dalam jaringan.
- Ketika ada komputer lain yang terhubung ke jaringan ARPAnet maka masing-masing komputer dalam jaringan tersebut harus memperbaharui berkas HOSTS.TXT-nya.
- Cara meng-update berkas HOSTS.TXT dengan menggunakan ftp setiap satu atau dua minggu sekali.
- Masalah ketika jaringan menjadi semakin besar. Kesulitan meng-update isi berkas HOSTS.TXT karena jumlah nama mesin/komputer yang dituliskan sudah terlalu besar dan tidak efisien.



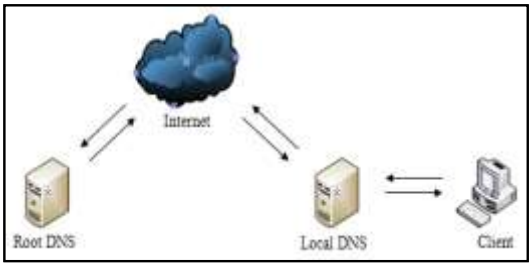
Resolver and name server

1. Sebuah program aplikasi pada host yang mengakses domain system disebut sebagai **resolver**
2. Resolver mengontak DNS server, yang biasa disebut name server
3. DNS server mengembalikan IP address ke resolver yang meneruskan ke aplikasi yang membutuhkan IP address



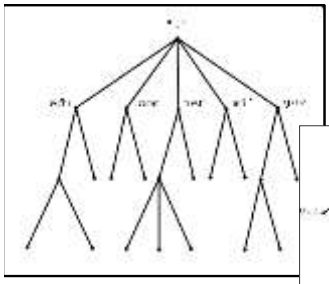
CARA KERJA DNS

1. Saat user merequest suatu alamat (misalnya www.facebook.com) dari host pribadi (oman.com – 202.53.232.114), maka host tersebut akan menanyakan pada name server lokal untuk mencari dimanakah www.facebook.com berada
2. Name server (202.154.63.2) akan mencari request tersebut di database lokal. Jika tidak ada, maka name server akan mengontak root DNS servernya, siapa yang memegang domain untuk facebook.com
3. Root server akan memberitahu IP address server DNS dari alamat www.facebook.com. DNS server lokal akan mengontak server DNS yang mengelola www.facebook.com. Kemudian DNS server tersebut akan memberitahu IP address dari www.facebook.com. baru host Oman dapat me-request www.facebook.com dengan IP address yang diberikan.

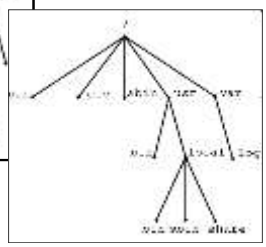


Gbr. Skema Kerja DNS

Struktur



Gbr. Struktur database DNS



Gbr. File System UNIX

STRUKTUR HIERARKI DNS

- **Root-Level Domains** Domain ditentukan berdasarkan tingkatan kemampuan yang ada di struktur hierarki yang disebut dengan *level*. Level paling atas di hirarki disebut dengan *root domain.*
- **Top-Level Domains (TLD)**
- **Second-Level Domains,** contoh : training.yadipoer.com
- **Host Names**

Top Level Domain (TLD)

- **Domain Generik**
  - com , net , gov , mil , org , edu , int
  - Selain 7 domain di atas ada lagi 7 domain baru dari ICANN (www.icann.org) yaitu: aero, biz , coop , info , museum , name , pro
- **Domain Negara**
  - Contoh: id untuk Indonesia, au untuk Australia, uk untuk Inggris, dan lain-lain.
  - Domain negara ini dapat dan umumnya diturunkan lagi ke level-level di bawahnya yang diatur oleh NIC dari masing-masing negara, untuk Indonesia yaitu IDNIC. Contoh level bawah dari id yaitu net.id, co.id, web.id.
- **Domain Arpa**
  - Merupakan domain untuk jaringan ARPAnet. Tiap domain yang tergabung ke Internet berhak memiliki name-space .in-addr.arpa sesuai dengan alamat IP-nya.

Penggunaan DNS memiliki beberapa keuntungan yaitu :

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. ***Sederhana***, user hanya menggunakan satu nama domain untuk dicari baik di Internet maupun di Intranet.

Install DNS Server Linux

- Untuk memulai installasi dan konfigurasi DNS server, pastikan anda telah mengatur IP address anda terlebih dahulu.
- Untuk DNS server, nama paket yang akan diinstall adalah **bind9**, dan untuk menginstall gunakan perintah

  # apt-get install bind9

- **Bind** (***Berkeley Internet Name Domain***) sudah terdapat di repository Ubuntu atau di DVD repository sehingga kita tidak perlu mencarinya lagi secara terpisah. Apabila ingin menginstall lewat GUI maka kita bisa melalui Synaptic Package Manager.

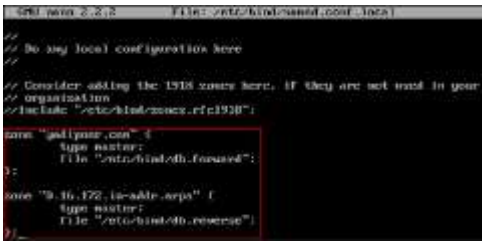
Selain dari itu anda juga dapat menggunakan aplikasi lain untuk konfigurasi DNS Server, antara lain :

1. `djbdns` (Daniel J. Bernstein's DNS) .
2. `MaraDNS`.
3. `QIP` (Lucent Technologies).
4. `NSD` (Name Server Daemon).
5. `Unbound`.
6. `PowerDNS`.
7. *Microsoft DNS* (untuk edisi server dari Windows 2000 dan Windows 2003).

Konfigurasi

- Lakukan instalasi package **bind9** pada mesin yang akan menjadi DNS Server. Untuk menginstal package, gunakan perintah ***apt-get install bind9.***
- Setelah terinstall, data untuk file konfigurasi DNS Serverbearada di ***/etc/bind/named.conf.local***.
- Buka file tersebut dengan menggunakan utility nano atau gunakan perintah ***nano /etc/bind/named.conf.local***.

Sebagai contoh setelah terbuka, inputkan script berikut :

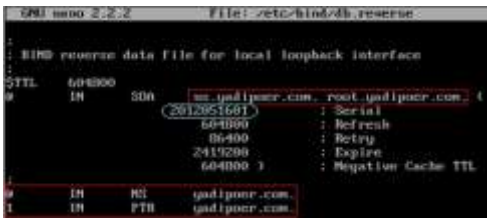


Pada gambar di atas dapat dilihat bahwa di samping parameter `zone` ada teks "**yadipoer.com**", dimana yadipoer.com adalah domain name yang akan digunakan pada sistem tersebut. Kemudian pada parameter `type` kita menentukan jenis domain name yang akan digunakan apakah *master* atau *slave*. Di samping parameter `file` menunjukan file konfigurasi yang selanjutnya.

Setelah itu lakukan konfigurasi pada file `db.forward` dengan membukanya menggunakan utility `nano`. Setelah terbuka, lakukan pengeditan script sehingga menjadi seperti berikut :

Maksud dari isi tanda oval biru pada gambar di atas adalah format waktu *kapan dilakukan pengeditan domain name* yang di representasikan secara standar. Formatnya adalah ***tahun-bulan-tanggal-pengeditan ke...***.
Dari gambar di atas diketahui bahwa pengeditan dilakukan pada tanggal *16 Mei 2012* dan itu adalah pengeditan *pertama* (01).

Setelah itu keluar dari utility `nano` dan simpan perubahan pada file tersebut. Setelah itu buka file `db.reverse` menggunakan `nano` lalu lakukan pengeditan script seperti berikut :



Pada bagian depan di line paling bawah dapat dilihat ada angka **1**. Hal itu maksudnya adalah untuk penanda dari segmen terakhir pada IP Address yang digunakan untuk mesin DNS Server (172.16.0.**1**).

Setelah itu keluar dari utility `nano` dan simpan perubahan pada file tersebut. Langkah terakhir dari konfigurasi ini adalah *restarting* pada service `bind9`. Gunakan perintah **`service bind9 restart`**.

Jika muncul parameter `[ OK ]` pada saat proses *stopping* dan *starting* dari domain name service, maka konfigurasi kita sudah benar.

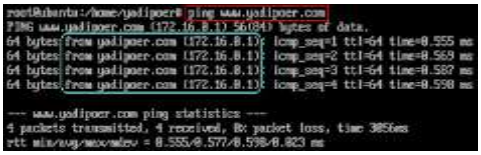
Pengujian DNS Server

1. Pada PC Client, buka file `/etc/resolv.conf` dengan menggunakan utility `nano`. Setelah terbuka, masukkan script berikut :

2. Setelah itu gunakan perintah `nslookup` sehingga akan muncul console > (tanda *lebih dari*). Setelah muncul console tersebut, ketikkan `www.yadipoer.com` untuk membuktikan kepemilikan domain name tersebut. Berikut hasilnya :

Pada gambar di atas dapat dibuktikan bahwa pemilik domain name **`yadipoer.com`** adalah IP address **172.16.0.1** (sesuai dengan topologi). Kemudian dari line `Address : 172.16.0.1#53` dapat kita ketahui bahwa DNS Server bekerja pada ***port 53***.

3. Pengujian juga dapat dilakukan dengan cara melakukan uji koneksi ke domain name `yadipoer.com`. Gunakan perintah `ping www.yadipoer.com`. Berikut hasilnya :



Dari gambar di atas dapat dilihat bahwa uji koneksi ICMP ke domain `yadipoer.com` dijawab oleh pemilik IP address `172.16.0.1`.

File-File Konfigurasi

Standard

- named.conf di dalam /etc
- named.ca di dalam /var/named
- named.local di dalam /var/named

Jika ingin membuat master server maka harus ada:

- file zone -> mapping dari nama ke IP
- file reverse zone -> mapping dari IP ke nama

named.conf

```
// generated by named-bootconf.pl

options {
        directory "/var/named";
        /*
         * 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 uses an unprivileged
         * port by default.
         */
        // query-source address * port 53;
};

//
// a caching only nameserver config
//
controls {
        inet 127.0.0.1 allow { localhost; };
};
```

1. Directory untuk menempatkan file zone

2. Blok untuk mengatur akses

```
zone "." IN {
        type hint;
        file "named.ca";
};

zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
};

zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
};
```

3. Zone untuk root

4. Zone untuk localhost

5. Zone untuk reverse address

named.ca

- Dikenal sebagai cache file untuk DNS
- Berisikan daftar world root servers

named.ca

```
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache  .  <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.cache
;           on server           FTP.INTERNIC.NET
;
;       last update:    Nov 5, 2002
;       related version of root zone:   2002110501
;
;
```

named.ca

```
; formerly NS.INTERNIC.NET
;
.                       3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000      A     198.41.0.4
;
; formerly NS1.ISI.EDU
;
.                       3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.     3600000      A     128.9.0.107
;
; formerly C.PSI.NET
;
.                       3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.     3600000      A     192.33.4.12
;
```

named.ca

```
; formerly TERP.UMD.EDU
;
.                       3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.     3600000      A     128.8.10.90
;
; formerly NS.NASA.GOV
;
.                       3600000      NS    E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.     3600000      A     192.203.230.10
;
; formerly NS.ISC.ORG
;
.                       3600000      NS    F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.     3600000      A     192.5.5.241
```

named.ca

```
;
; formerly NS.NIC.DDN.MIL
;
.                       3600000      NS    G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.     3600000      A     192.112.36.4
;
; formerly AOS.ARL.ARMY.MIL
;
.                       3600000      NS    H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.     3600000      A     128.63.2.53
;
; formerly NIC.NORDU.NET
;
.                       3600000      NS    I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.     3600000      A     192.36.148.17
```

named.ca

```
;
; operated by VeriSign, Inc.
;
.                       3600000      NS    J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.     3600000      A     192.58.128.30
;
; housed in LINX, operated by RIPE NCC
;
.                       3600000      NS    K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.     3600000      A     193.0.14.129
;
; operated by IANA
;
.                       3600000      NS    L.ROOT-SERVERS.NET.
```

named.ca

- L.ROOT-SERVERS.NET. 3600000 A 198.32.64.12
- ;
- ; housed in Japan, operated by WIDE
- ;
- . 3600000 NS M.ROOT-SERVERS.NET.
- M.ROOT-SERVERS.NET. 3600000 A 202.12.27.33
- ; End of File

Named.local

- Berisikan informasi tentang localhost
- Berisikan info untuk me-resolv loopback address untuk localhost

Named.local

- @ IN SOA localhost. root.localhost. (
- 1997022700 ; Serial
- 28800 ; Refresh
- 14400 ; Retry
- 3600000 ; Expire
- 86400) ; Minimum
- IN NS localhost.
- 1 IN PTR localhost.

Named.rev

- Menyediakan informasi untuk reserve lookups.
- Digunakan untuk mengetahui nama dari suatu host berdasarkan IP

Named.rev

- 63.154.202.in-addr.arpa. IN SOA ns1.pens-its.edu. admin.pens-its.edu. (
- 2000081012 ; Serial
- 28800 ; Refresh
- 14400 ; Retry
- 3600000 ; Expire
- 86400) ; Minimum
- IN NS ns1.pens-its.edu.
- IN NS ns2.pens-its.edu.

- 4 IN PTR www.pens-its.edu.
- 5 IN PTR ies.pens-its.edu.
- 6 IN PTR elerning.pens-its.edu.

File ZONE

- File zone berisikan resource record (RR) tentang IP address
- File ZONE akan diawali oleh SOA yang merupakan penanda bahwa name server tersebut adalah merupakan sumber yang sah untuk domain tersebut
- SATU zone file HANYA akan punya SATU SOA

SOA

- @ IN SOA main.tactechnology.com. mail.tactechnology.com. (
- 2000052101 ; Serial
- 8h ;Refresh
- 2h ;Retry
- 1w ;Expire
- 1d) ;Minimum TTL

- SOA seperti ini adalah Start Of Authority untuk domain yang di spesifikasikan di named.conf
- Nama server yang sah adalah main.technology.com
- Mail-address dari administratornya adalah mail.tatechnology.com

SOA

- Serial : Serial number dari file zone tersebut
- Refresh : waktu yang dibutuhkan untuk me-refresh data
- Retry : waktu yang dibutuhkan untuk menunggu sebelum berusaha mengontak server utama jika ada kegagalan
- Expire : jika secondary master gagal mengontak server utama dalam waktu ini maka database tentang domain tersebut akan dibuang
- TTL: Time to live untuk menentukan berapa lama data disimpan dalam cache

Resource Record

- **NS — NAME SERVERS**
  - Menunjukkan nama "name server".
- **A — THE IP ADDRESS FOR THE NAME**
  - Menunjukkan nomor IP "name server".
- **PTR — POINTER FOR ADDRESS NAME MAPPING**
  - Digunakan untuk menunjuk name server
- **CNAME — CANONICAL NAME**
  - Menunjukkan nama real host.
- **MX — MAIL EXCHANGE RECORD**
  - Menunjukkan sebagai mail server pada domain tersebut.

Dynamic DNS

- Suatu cara melakukan update DNS server tanpa harus melakukan restart terhadap konfigrasi DNS kita.
- Pada waktu konfigurasi DNS harus ada cara untuk mengupdate, Pada waktu suatu host hidup kita bisa menyediakan address via DHCP, kemudian DHCP meminta DNS untuk merubah record A dan PTR sesuai kebutuhan.
- Kolaborasi antara DNS dan DHCP
- Membutuhkan bind9 dan DHCP3
- Konfigurasi file utama : dhcpd.conf dan named.conf