DNS (Domain Name System)

Intro to DNS

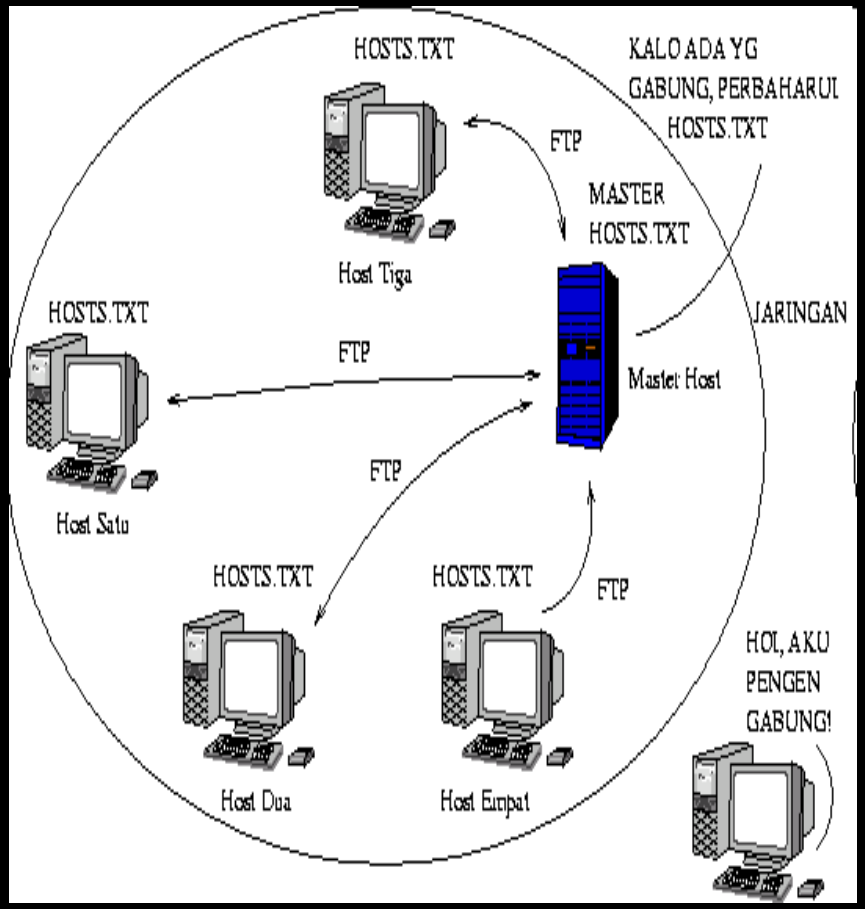
- DNS merupakan sistem berbentuk database terdistribusi yang akan memetakan/mengkonversikan nama host/mesin/domain ke alamat IP (Internet Protocol) dan sebaliknya dari alamat IP ke nama host yang disebut dengan reverse-mapping.
- Penggunaan :
  - Untuk memetakan nama mesin misal www.mitek.unibraw.ac.id ke alamat IP misal 202.130.9.51
  - Untuk routing e-mail, telnet, ftp, web, dan lain-lain.

Intro to DNS

- DNS sebagai jembatan
  - Manusia lebih mudah untuk mengingat nama daripada alamat IP dengan panjang 32 bit itu.
  - Komputer menggunakan alamat IP untuk berkomunikasi dan berinteraksi.
- DNS tidak diperlukan jika kita bisa mengingat ratusan, ribuan, bahkan jutaan alamat IP di Internet.

History

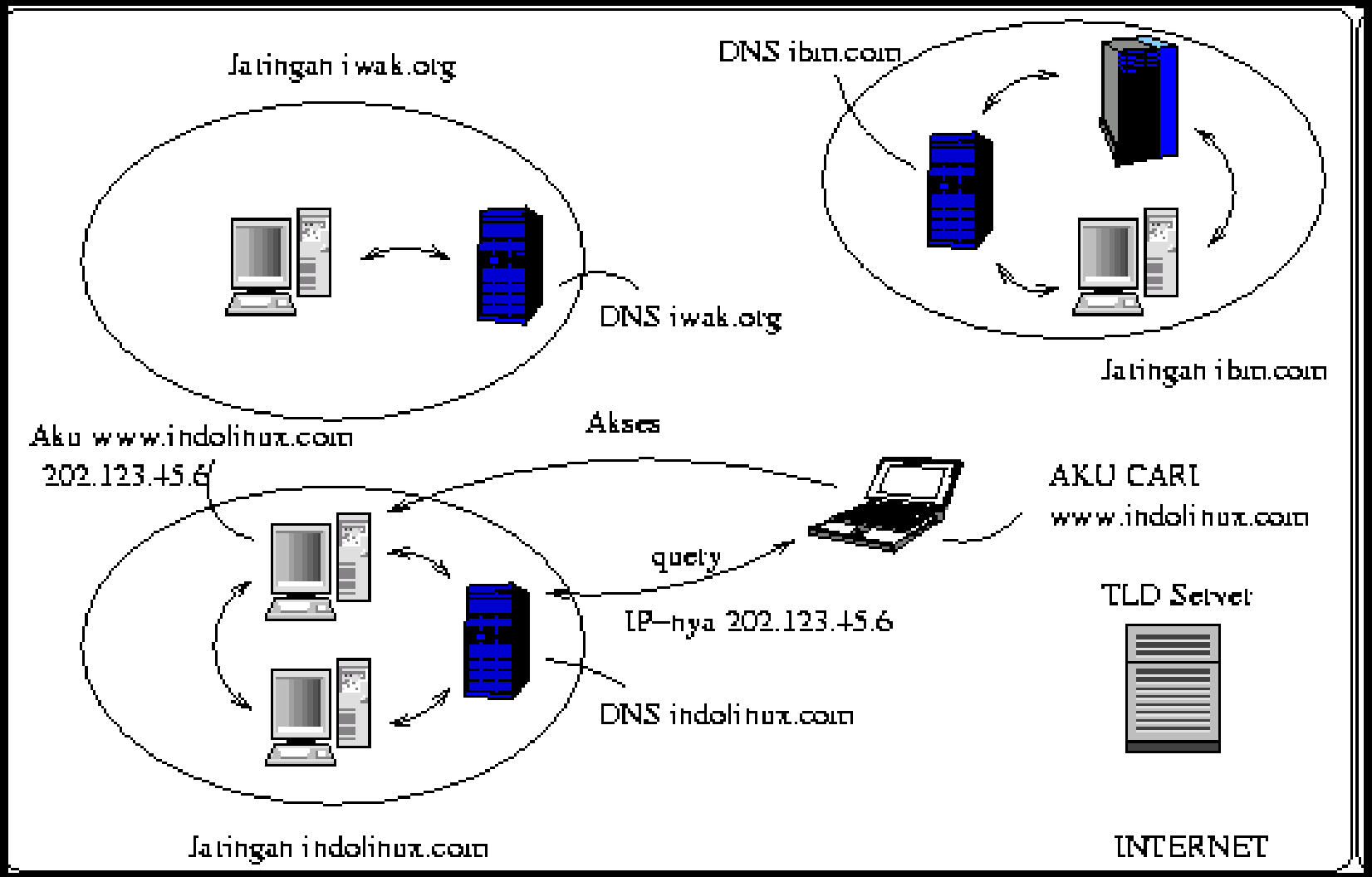
- Sebelum adanya DNS, tahun 1970-an ARPAnet menggunakan pemetaan dengan bentuk tabel host pada berkas HOSTS.TXT
- HOSTS.TXT berisi nama host dan alamat IP serta pemetaannya dari seluruh mesin/komputer yang terhubung dalam jaringan.
- Ketika ada komputer lain yang terhubung ke jaringan ARPAnet maka masing-masing 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.



History

- Muncul ide untuk membuat sistem database terdistribusi yang mempunyai data mengenai pemetaan nama host ke alamat IP dan sebaliknya.
- Dengan adanya pendistribusian database nama host dan alamat IP, maka tiap organisasi yang memiliki jaringan di dalam domain tertentu hanya bertanggung jawab terhadap database informasi pemetaan nama host dan alamat IP pada jaringannya saja yang biasa disebut zone.
- Administrasi domain tersebut dilakukan secara lokal tetapi informasi itu dapat diakses oleh semua komputer di Internet.
- Karena sifat database yang terdistribusi ini, maka dibutuhkan suatu mekanisme pengaksesan informasi bagi host lain pada database yang terdistribusi untuk menemukan informasi host atau jaringan yang dipunyai oleh suatu organisasi.
- Dan pada tahun 1984, Paul Mockapetris mengusulkan sistem database terdistribusi ini dengan Domain Name System (DNS) yang dideskripsikan dalam RFC 882 dan 883. Sistem ini digunakan sampai sekarang pada jaringan khususnya Internet.

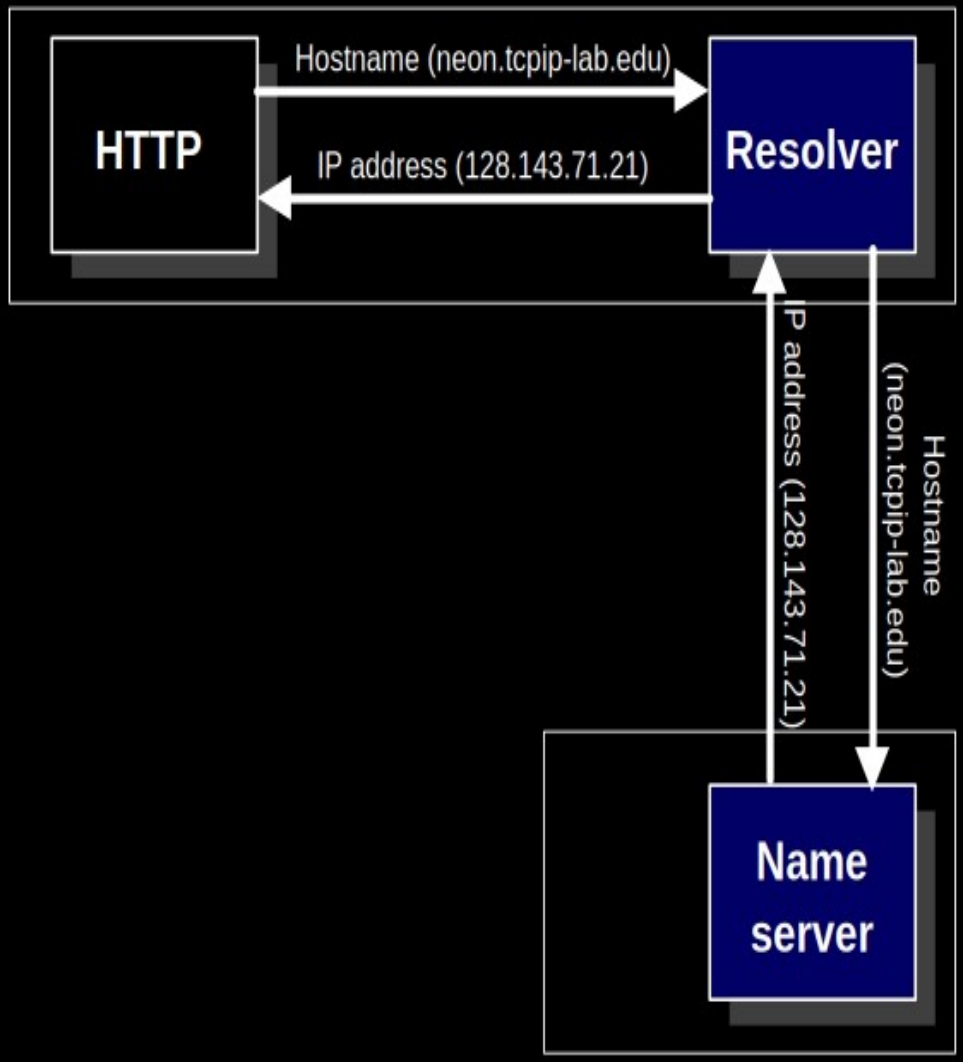
History


Jaringan iwak.org
DNS iwak.org
DNS ibm.com
Jaringan ibm.com
Aku www.indolinux.com
202.123.45.6
Akses
AKU CARI
www.indolinux.com
query
IP–nya 202.123.45.6
TLD Server
DNS indolinux.com
Jaringan indolinux.com
INTERNET

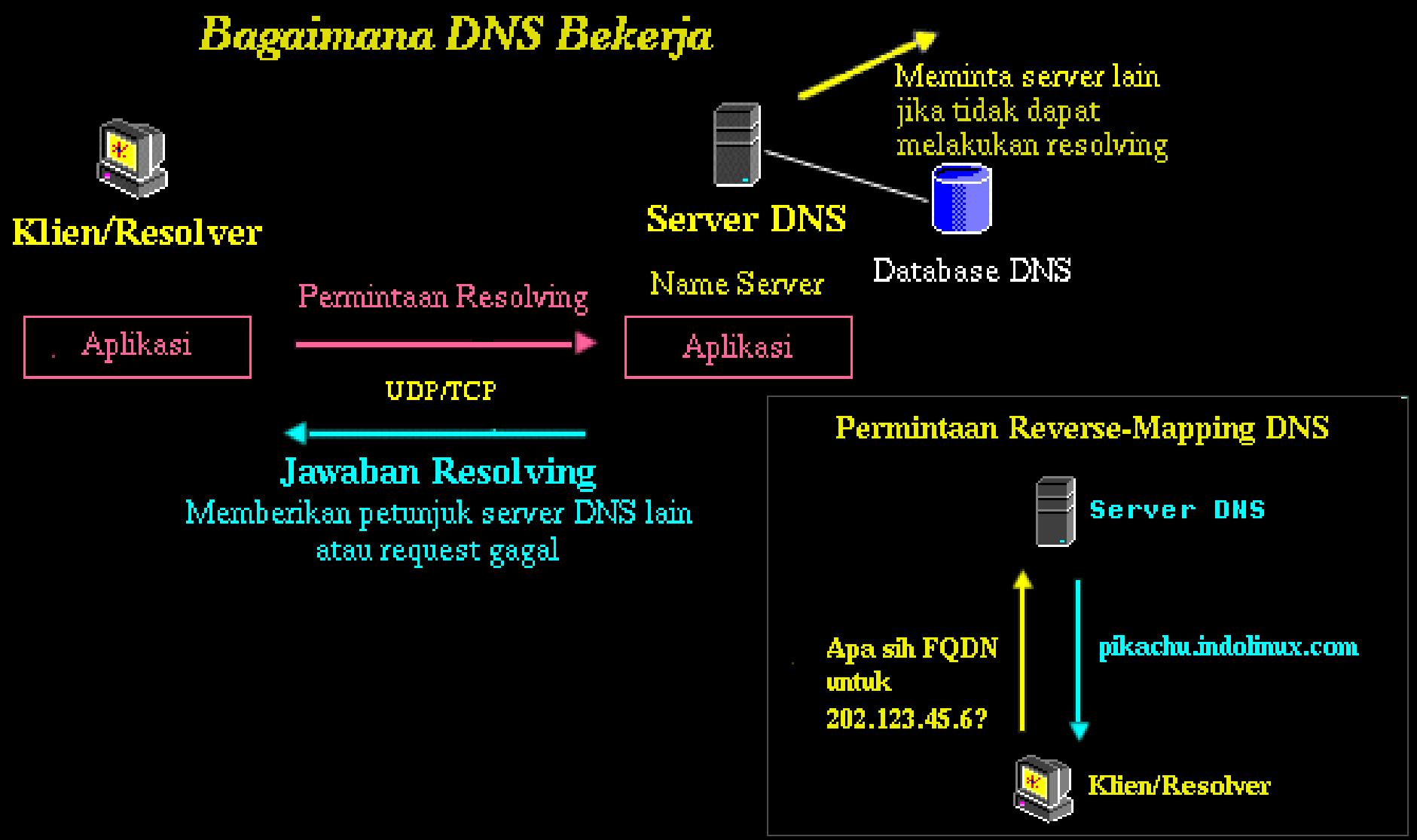
Resolver and name server

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

- Reverse lookups are also possible, i.e., find the hostname given an IP address



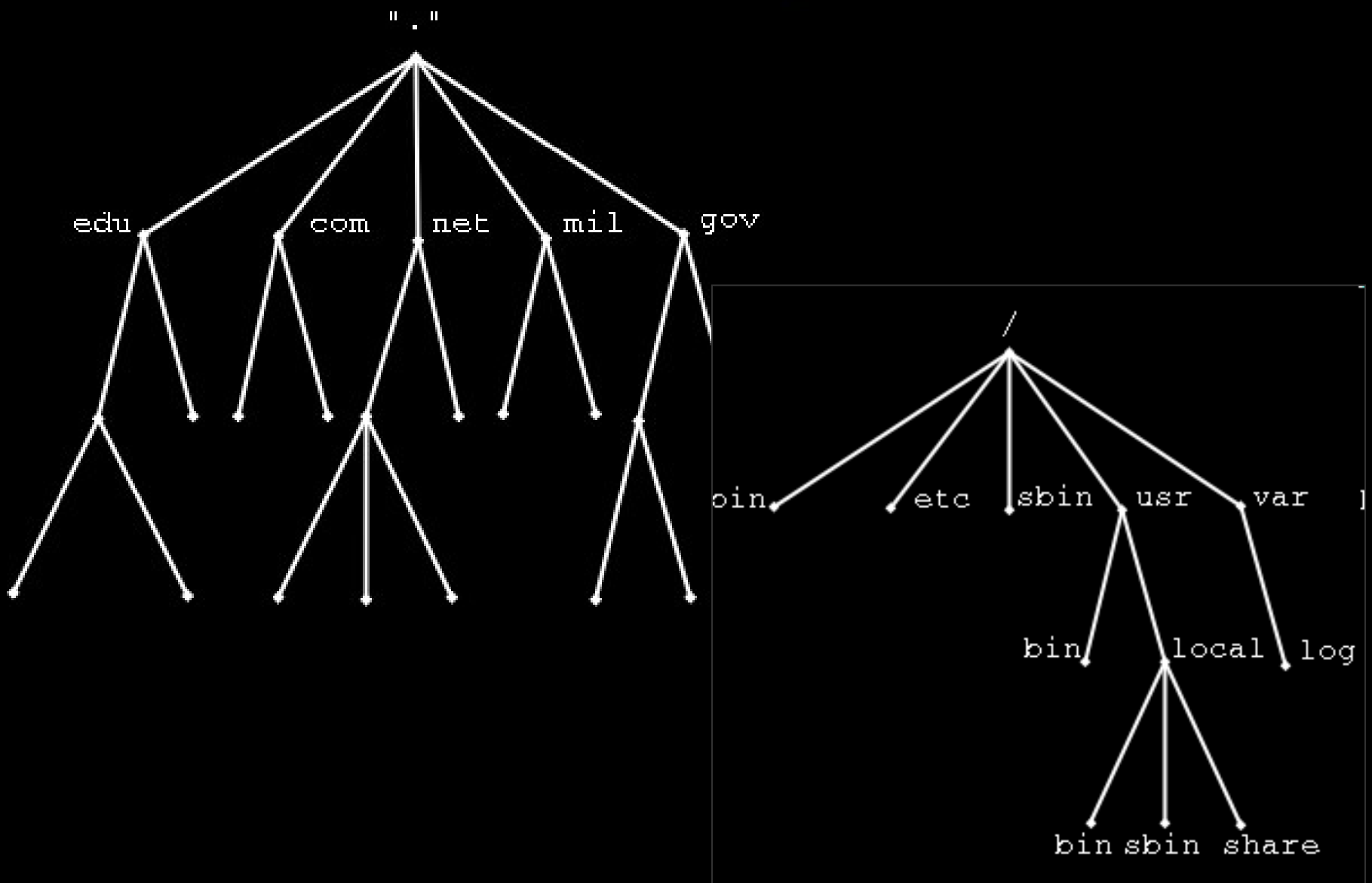
Kerja DNS


Bagaimana DNS Bekerja
Meminta server lain jika tidak dapat melakukan resolving
Klien/Resolver
Server DNS
Database DNS
Name Server
Permintaan Resolving
Aplikasi
Aplikasi
UDP/TCP
Jawaban Resolving
Memberikan petunjuk server DNS lain atau request gagal
Permintaan Reverse-Mapping DNS
Server DNS
Apa sih FQDN untuk 202.123.45.6?
pikachu.indolinux.com
Klien/Resolver

Struktur

- Struktur database DNS mirip dengan sistem-berkas/filesystem UNIX yaitu berbentuk hierarki atau pohon.
- Tingkat teratas pada DNS adalah root yang disimbolkan dengan titik/dot (.) sedangkan pada sistem berkas UNIX, root disimbolkan dengan slash (/).
- Setiap titik cabang mempunyai label yang mengidentifikasikannya relatif terhadap root (.).
- Tiap titik cabang merupakan root bagi sub-tree/tingkat bawahnya.
- Tiap sub-tree merupakan domain dan dibawah domain terdapat sub-tree lagi bernama subdomain.
- Setiap domain mempunyai nama yang unik dan menunjukkan posisinya pada pohon DNS, pengurutan/penyebutan nama domain secara penuh dimulai dari domain paling bawah menuju ke root (.).
- Masing-masing nama yang membentuk suatu domain dipisahkan dengan titik/dot (.) dan diakhiri dengan titik yang merupakan nama absolut relatif terhadap root (.).

Struktur


"."
edu
com
net
mil
gov
/
bin
etc
sbin
usr
var
bin
local
log
bin
sbin
share

Struktur

- Contoh: www.mitek.unibraw.ac.id.
- "." merupakan root domain
- id merupakan Top Level Domain
- ac merupakan Second Level Domain
- unibraw merupakan Third Level Domain
- Mitek merupakan Fourth Level Domain
- www merupakan nama komputer/mesin yang bersangkutan
- Sistem penulisan nama secara absolut dan lengkap ini disebut FQDN (Fully Qualified Domain Name) - www.mitek.unibraw.ac.id.

Hirarki

- Tiap organisasi yang telah mendaftar ke Network Information Center(NIC) akan mendapatkan nama domain sesuai dengan organisasi tersebut.
- Nama domain tersebut bisa dibagi menjadi subdomain sesuai kebutuhan organisasi.
  - Contoh: InterNIC mempunyai semua Top Level Domain termasuk edu,
  - Lembaga pendidikan wearnes akan mendaftarkan nama domain wearnes.edu (education), maka wearnes diberikan/didelegasikan oleh InterNIC untuk mengelola domain wearnes.edu yang merupakan sub domain dari edu.
  - wearnes dapat membagi lagi domain wearnes.edu ke beberapa sub domain misal www.wernes.edu, ftp.wearnes.edu dll.

Hirarki

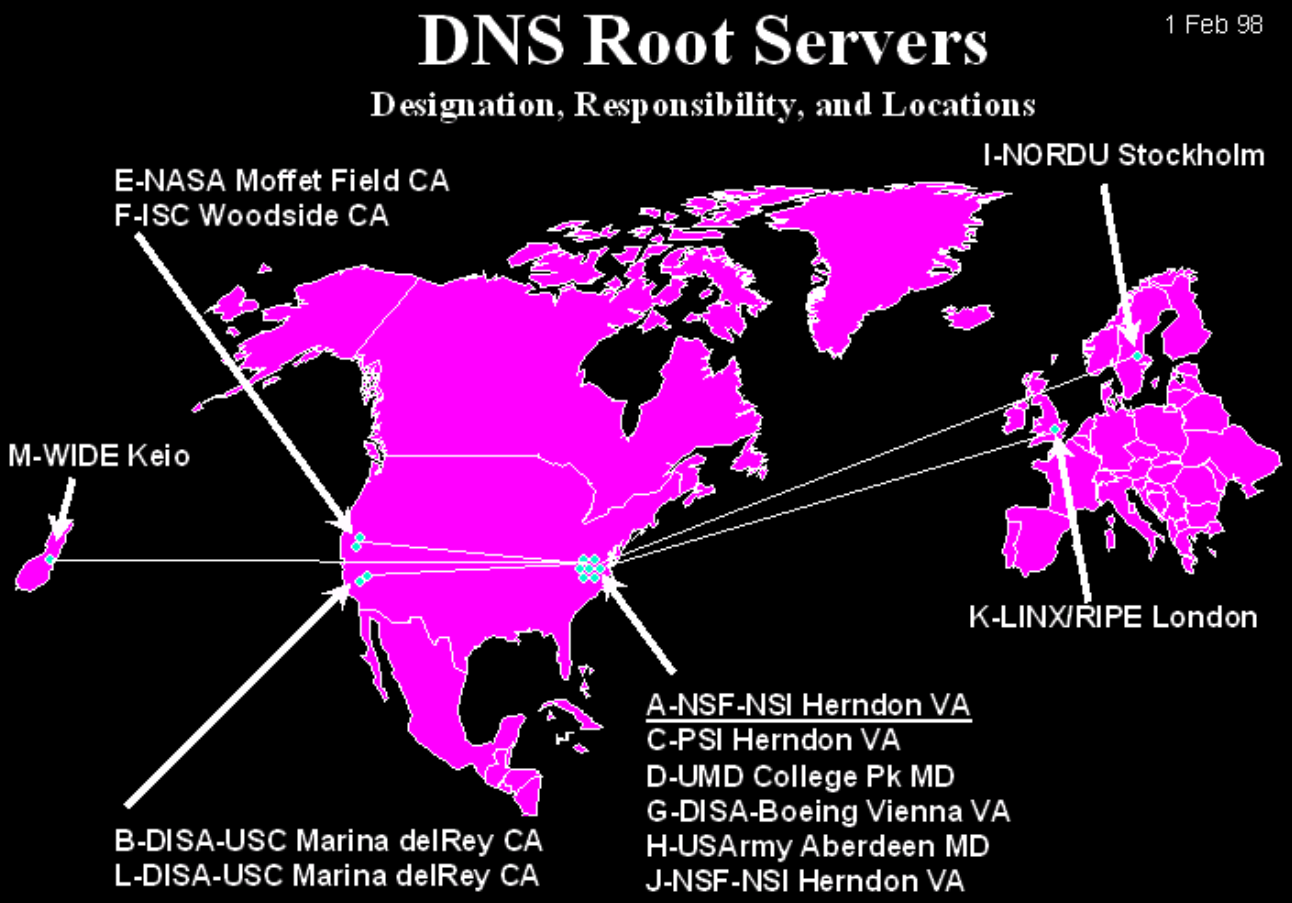
- Dengan adanya sistem berbentuk hierarki/pohon ini maka tidak ada nama host yang sama pada domain/subdomain yang sama, karena masing-masing dari node/titik-cabang mempunyai nama unik dan tidak boleh ada yang menyamainya kecuali berbeda sub-tree/sub pohon.
- Tidak akan ada konflik antar organisasi karena masing-masing organisasi mempunyai domain yang berbeda-beda dan ini diatur oleh InterNIC untuk TLD.
- Kedalaman pohon dibatasi sampai level 127

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.

Root name servers

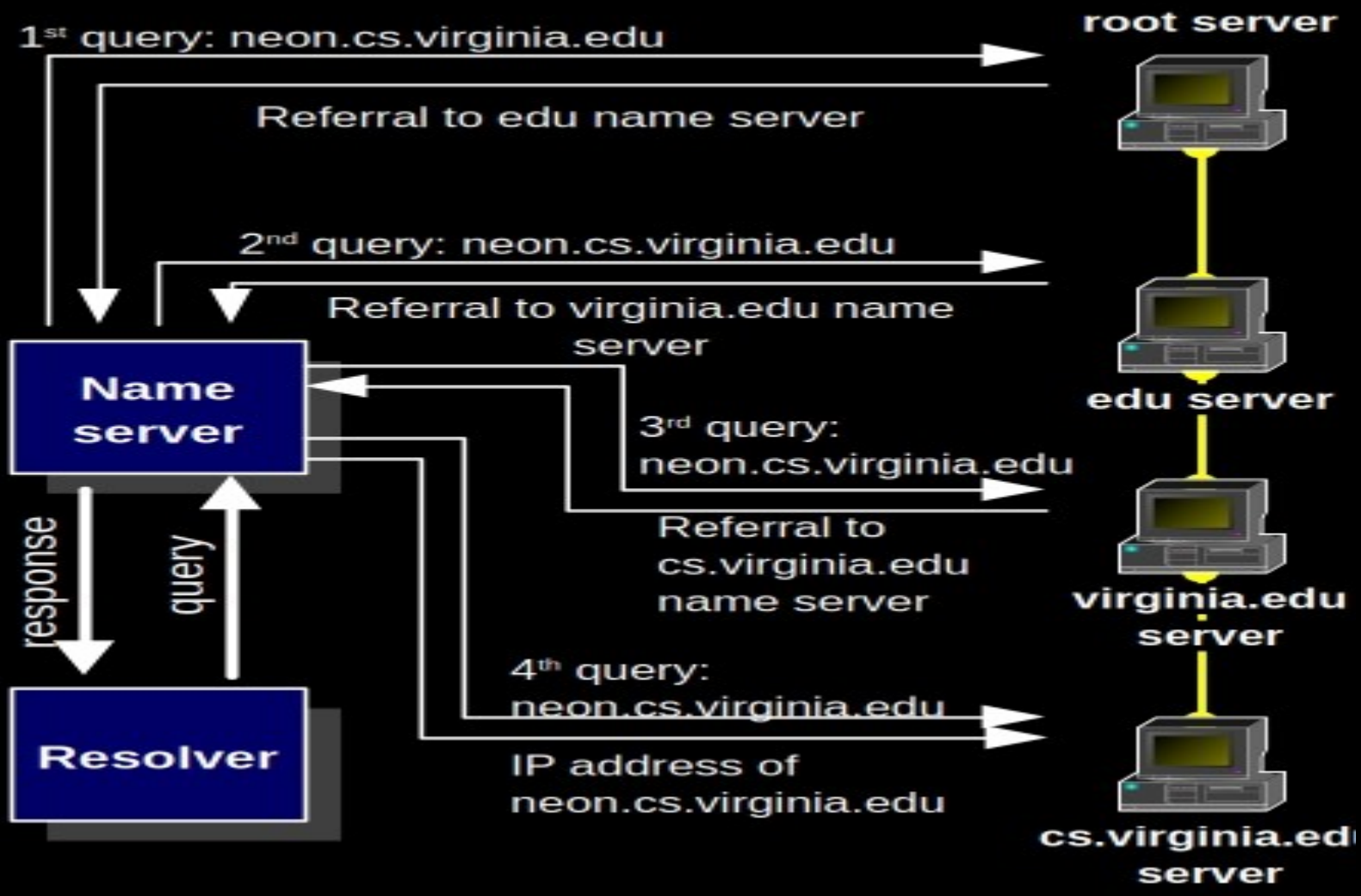
- Server root digunakan untuk menemukan authoritative name servers untuk semua zona top-level.
- Ada 13 server root
- Digunakan untuk name resolution



Address root servers (2004)

A.ROOT-SERVERS.NET.	(VeriSign, Dulles, VA)	198.41.0.4
B.ROOT-SERVERS.NET.	(ISI, Marina Del Rey CA)	192.228.79.201
C.ROOT-SERVERS.NET.	(Cogent Communications)	192.33.4.12
D.ROOT-SERVERS.NET.	(University of Maryland)	128.8.10.90
E.ROOT-SERVERS.NET. 192.203.230.10	(Nasa Ames Research Center)	
F.ROOT-SERVERS.NET.	(Internet Systems Consortium)	192.5.5.241
G.ROOT-SERVERS.NET.	(US Department of Defense)	192.112.36.4
H.ROOT-SERVERS.NET.	(US Army Research Lab)	128.63.2.53
I.ROOT-SERVERS.NET.	(Autonomica/NORDUnet)	192.36.148.17
J.ROOT-SERVERS.NET.	(Verisign, multiple cities)	192.58.128.30
K.ROOT-SERVERS.NET.	(RIPE,Europe multiple cities)	193.0.14.129
L.ROOT-SERVERS.NET.	(IANA, Los Angeles)	198.32.64.12
M.ROOT-SERVERS.NET.	(WIDE, Tokyo, Seoul, Paris)	202.12.27.33

Recursive queries



Caching

- Untuk mengurangi traffic, informasi mapping antara IP dan name servers disimpan di
- Ketika ada permintaan/ query server tidak perlu lagi menghubungi server lain

Resource Records

- Record database pada Database DNS terdistribusi disebut resource records (RR)
- Resource records disimpan pada file konfigurasi (zone files) pada name servers.

Berikut ini contoh sebuah zone Resource record→

db.mylab.com

```
$TTL 86400
mylab.com. IN SOA PC4.mylab.com.
                  hostmaster.mylab.com. (
                  1 ; serial
                  28800 ; refresh
                  7200 ; retry
                  604800 ; expire
                  86400 ; ttl
                  )

;
mylab.com.  IN    NS    PC4.mylab.com.
;
localhost         A     127.0.0.1
PC4.mylab.com.    A     10.0.1.41
PC3.mylab.com.    A     10.0.1.31
PC2.mylab.com.    A     10.0.1.21
PC1.mvlab.com.    A     10.0.1.11
```

Resource Records

db.mylab.com

```
$TTL 86400
mylab.com. IN SOA PC4.mylab.com.
hostmaster@mylab.com. (
                        1 ; serial
                        28800 ; refresh
                        7200 ; retry
                        604800 ; expire
                        86400 ; ttl
                        )
;
mylab.com.          IN      NS      PC4.mylab.com.
;
localhost                   A       127.0.0.1
PC4.mylab.com.      A       10.0.1.41
PC3.mylab.com.      A       10.0.1.31
PC2.mylab.com.      A       10.0.1.21
PC1.mylab.com.      A       10.0.1.11
```

Maksimum umur data cache dalam detik

- Record Start of authority (SOA) arti : "Zona authoritative Name server-nya Mylab.com"
- PC4.mylab.com adalah name server
- Email adress PICnya hostmaster@mylab.com

Record Name server (NS).

Address (A) records. Satu entry untuk setiap hostaddress

Software

- Pada Redhat Linux yang sudah terinstall BIND (name server daemon) akan dijumpai beberapa file sebagai berikut :
- Di dalam /var/named akan ada 2 file yaitu :
  - named.ca
  - named.local
- Di dalam /etc akan terdapat file named.conf

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

Blok dalam named.conf

- **options** — List konfigurasi global dan default
- **include** — berisi path file lain yang diperlukan
- **acl** — IP address dalam access control list
- **server** — properties khusus untuk remote servers
- **zone** — informasi khusus untuk zona

```
// 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

3. Zone untuk root

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

4. Zone untuk localhost

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

5. Zone untuk reverse address

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

options

- Biasanya ditaruh pada baris pertama named.conf
- Sintak :

```
options {
    value “property”;
}
```

options : allow-query

- Menerima query hanya dari host dalam address yang sudah (default any host).
- Penggunaan: allow-query {“address-list”};.

options : allow-transfer

- Zone transfers menerima query hanya dari host dalam address yang sudah (default all host).
- Penggunaan : allow-transfer {“address list”};.

options : directory

- Tempat dimana file konfigurasi server berada.
- Penggunaan: directory “path to directory”; (specify path).

options : forwarders

- Menunjukkan IP addresses server untuk memforward query (default is none).
- Penggunaan: forwarders “IP addresses of servers”; (specify IP addresses).

options : forward

- Jika diset pertama kali, Server akan didaftar pada query forwarders pertama,
- Penggunaan: forward “first or only”; (pilih salah satu).

options : listen-on

- Port dimana server listen dari query yang ada (default is port 53).
- Penggunaan : listen-on “port {address list}”;

options : recursion

- Server secara recursive mencari jawaban query (default is yes).
- Penggunaan: recursion “ yes or no”; (choose one).

include

- Berisi path dan file yang dibutuhkan yang berada diluar direktori yang sudah ditentukanpada named.conf.

acl

- IP address dalam access control list. Hanya host yang terdaftar yang boleh akses ke server

- acl "transferdns" {
- 	{ 216.65.64.146/32; };
- 	{ 209.25.238/24; };
- 	{ 202.154.63.3/32; };
- };

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
;
;
; 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
;
; 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
;
; 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
;
; 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.
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

- 9.130.202.in-addr.arpa. IN SOA ns1.mitek.unibraw.ac.id. admin.mitek.unibraw.ac.id. (
- 2000081012 ; Serial
- 28800 ; Refresh
- 14400 ; Retry
- 3600000 ; Expire
- 86400) ; Minimum
- IN NS ns1.mitek.unibraw.ac.id.
- IN NS ns2.mitek.unibraw.ac.id.

- 4 IN PTR www. mitek.unibraw.ac.id.
- 5 IN PTR ftp. mitek.unibraw.ac.id.
- 6 IN PTR mail. mitek.unibraw.ac.id.

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
- Dijelaskan lebih lanjut pada Bagian DHCP Server