

DNS/BIND

20110456

overmania

DNS

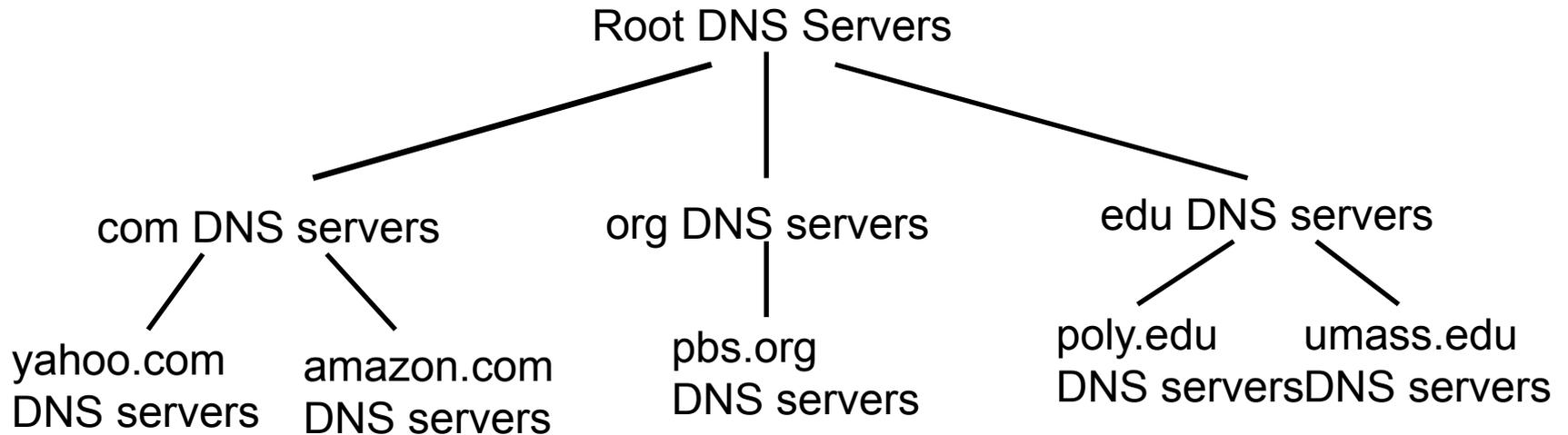
DNS: Domain Name System

- Why DNS?
 - People : Unique keys to match (ex. Student Number, Name, etc)
- Domain Name System :
 - Distributed database
 - Implemented by hierarchical structure of name servers.
 - Application-layer protocol
 - Runs in application-layer.

DNS: Domain Name System

- DNS Services
 - Host to IP, IP to Host transition (sparcs.org <-> 143.248.234.102)
 - Host aliasing
 - Canonical names
 - Load distribution
 - One domain name, multiple IPs(Server)
 - Whenever query asks domain to IP transition, it returns IP by rotating the set of IPs.

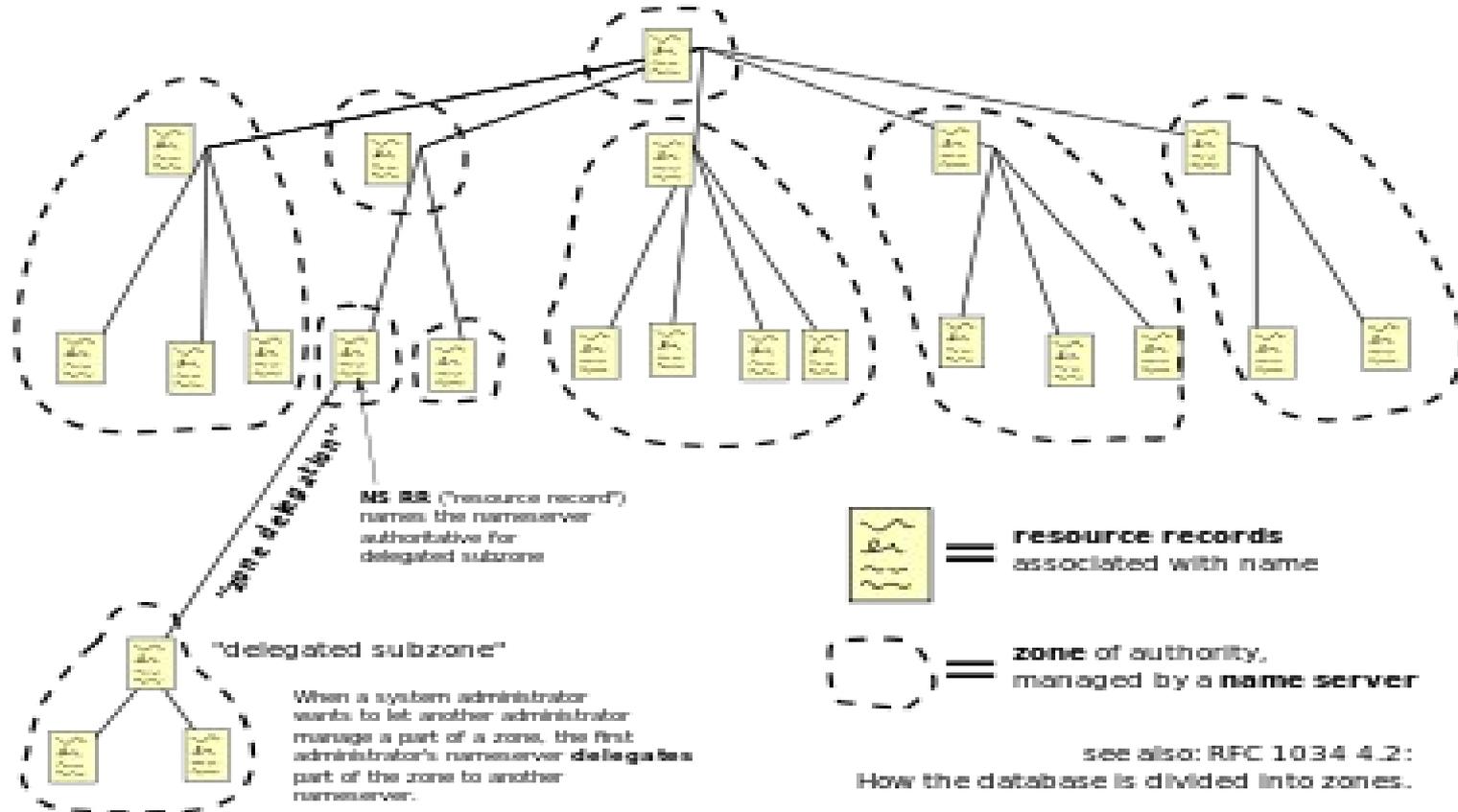
Name Servers



- Root name server
- Top Level Domain server
- Authoritative DNS Server

DNS zone, DNS Domain

Domain Name Space

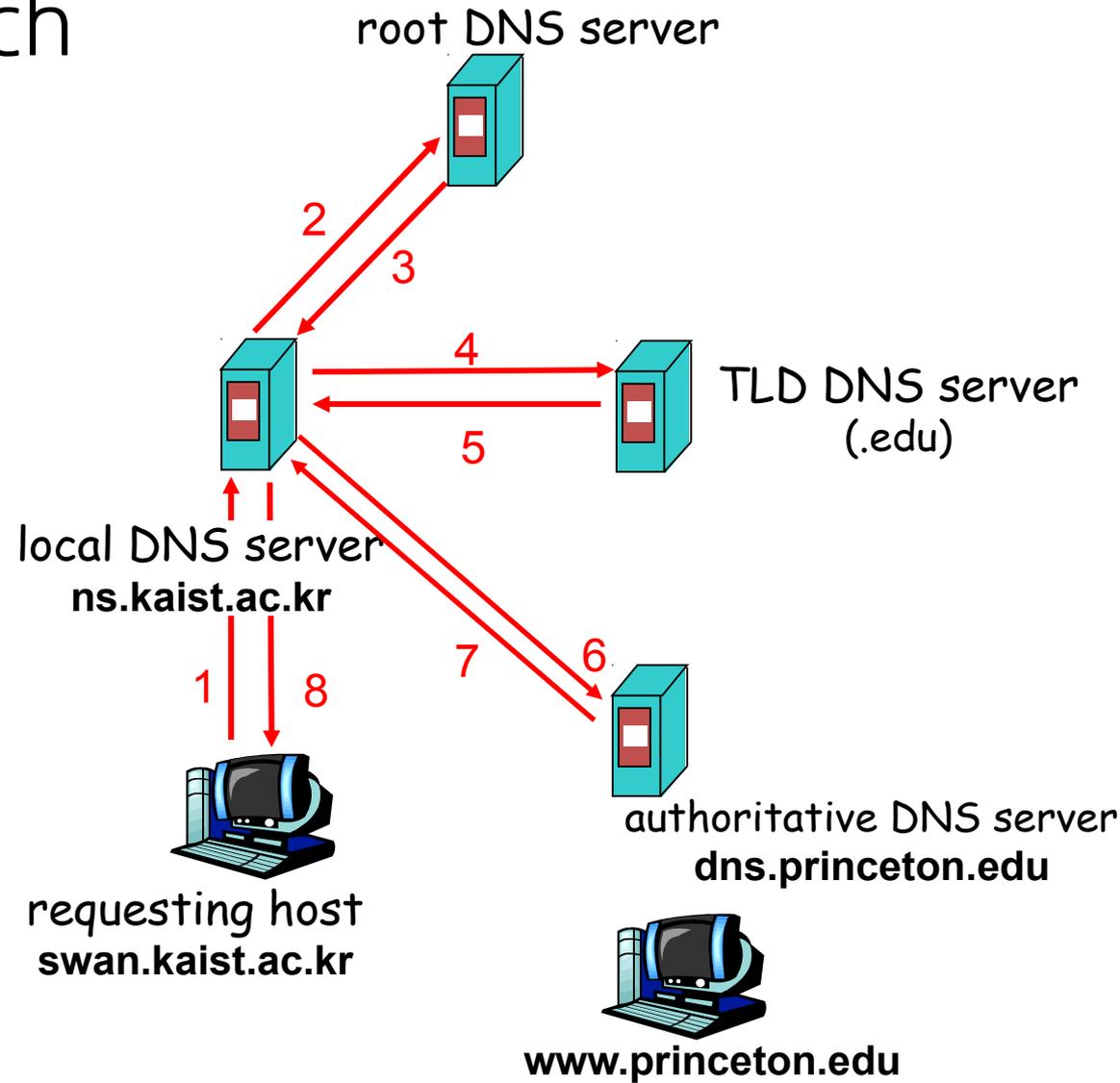


- Zone : some subsets of Domain

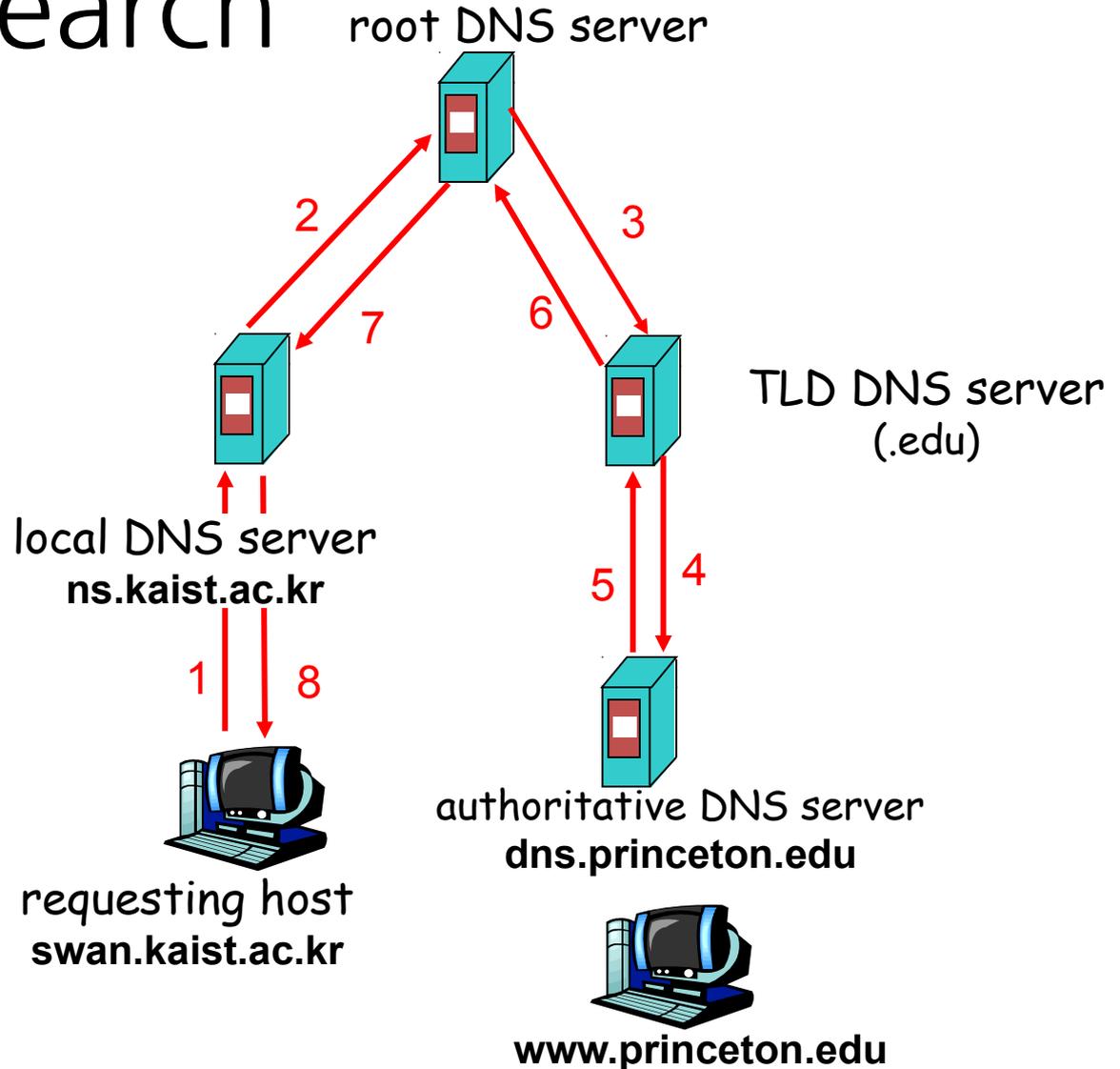
Domain Name: HOW TO READ

- [common.example.com.](#)
 - Split above with ‘.’ and read from the right
 - 1. “
 - 2. ‘com’
 - 3. ‘example’
 - 4. ‘common’
 - The rightmost ‘.’ represents root domain server.

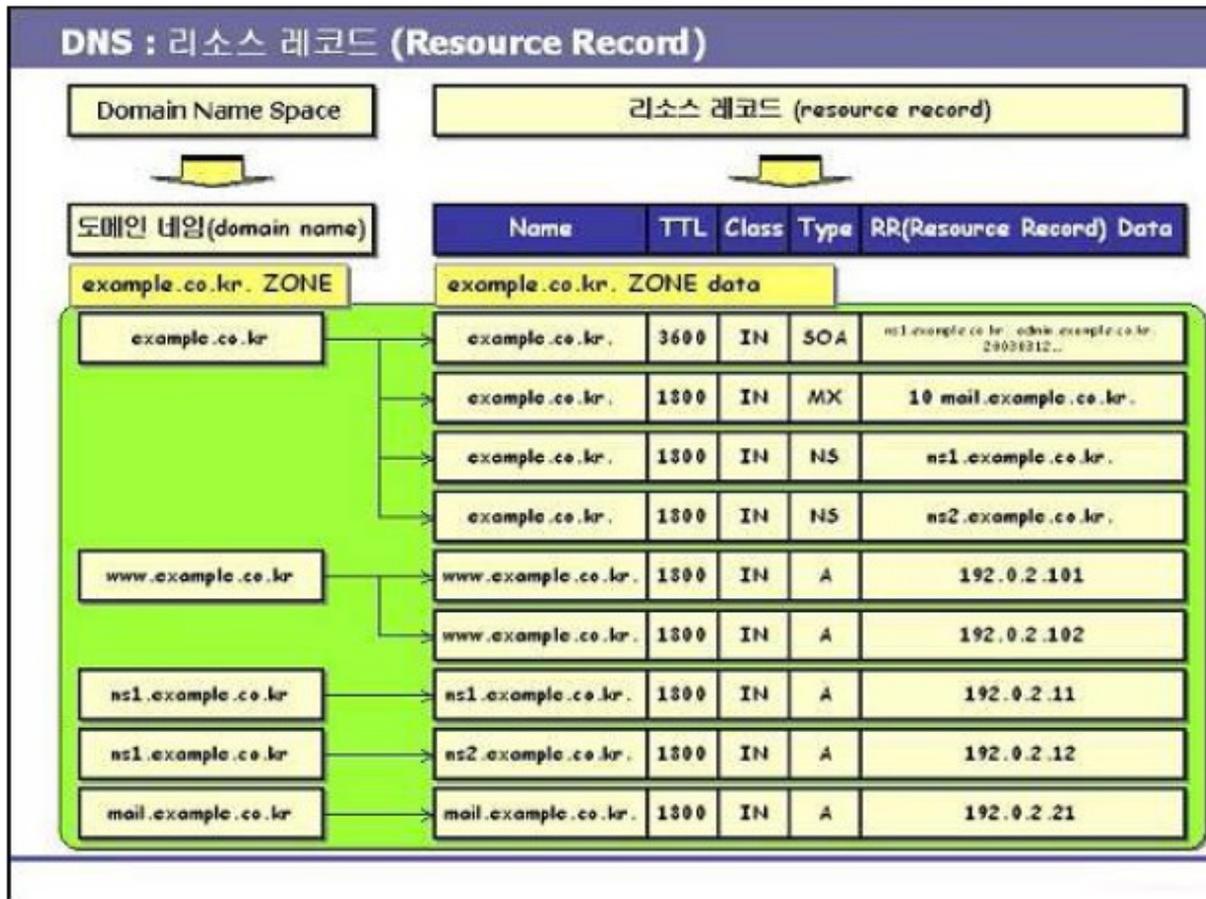
Iterative Search



Recursive Search



DNS records



DNS records : types and classes

Type	Code	의미
A	1	A host address 32bit IPv4 주소
AAAA	28	IP6 address 128bit IPv6 주소
NS	2	An authoritative name server 네임서버 도메인 네임 지정
CNAME	5	The canonical name for an alias Alias 도메인 네임 지정
SOA	6	Marks the start of a zone of authority Zone의 속성 정보 지정
MX	15	Mail exchange 메일서버의 도메인 네임 지정

Decimal 	Hexadecimal 	Name 
0	0x0000	Reserved
1	0x0001	Internet (IN)
2	0x0002	Unassigned
3	0x0003	Chaos (CH)
4	0x0004	Hesiod (HS)
5-253	0x0005-0x00FD	Unassigned
254	0x00FE	QCLASS NONE
255	0x00FF	QCLASS * (ANY)
256-65279	0x0100-0xFEFF	Unassigned
65280-65534	0xFF00-0xFFFE	Reserved for Private Use
65535	0xFFFF	Reserved

DNS records

RR format: (name, value, type, ttl)

- Type=A
 - **name** is hostname
 - **value** is IP address
- Type=NS
 - **name** is domain (e.g. foo.com)
 - **value** is hostname of authoritative name server for this domain
- Type=CNAME
 - **name** is alias name for some “canonical” (the real) name
 - www.ibm.com is really
www.ibm.com.cs186.net
 - **value** is canonical name
- Type=MX
 - **value** is name of mailserver associated with **name**

DNS records

- Type = SOA (Start of Authority)
 - @ IN SOA Source_host Contact_Email (serial number, refresh, retry, expire, min_TTL)
 - SOA 는 DNS zone file 의 첫번째에 들어가는 record 로 , Start of Authority 라는 이름에서 알 수 있듯이 해당 domain 에 대한 정보를 제공하는 데 있어 가장 정확한 source 라는 것을 indicate 한다 .

Basic usage of dig

- `dig @server domain type`
 - ‘server’ is DNS server we’ll look for domain
 - ‘type’ is DNS record type we’ll look for.
- `dig @server -x ip type`
 - IP to Domain lookup.
 - Other params are the same.
- For more,
<http://www.thegeekstuff.com/2012/02/dig-command-examples/>

DNS 실습

- Search 'sparcs.kaist.ac.kr' iteratively and from the IP, search domain name.

```
; <<<>> DiG 9.8.1-P1 <<<>> @ns.kaist.ac.kr. sparcs.kaist.ac.kr A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23737
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;sparcs.kaist.ac.kr.          IN      A

;; ANSWER SECTION:
sparcs.kaist.ac.kr.        7200    IN      A      143.248.234.102

;; AUTHORITY SECTION:
kaist.ac.kr.               7200    IN      NS     ns1.kaist.ac.kr.
kaist.ac.kr.               7200    IN      NS     ns.kaist.ac.kr.

;; ADDITIONAL SECTION:
ns.kaist.ac.kr.            7200    IN      A      143.248.1.177
ns1.kaist.ac.kr.          7200    IN      A      143.248.2.177

;; Query time: 2 msec
;; SERVER: 143.248.1.177#53(143.248.1.177)
;; WHEN: Thu Jul  4 23:20:10 2013
;; MSG SIZE rcvd: 119
```

BIND

BIND

- Berkeley Internet Name Domain
- Probably the most widely used DNS protocol implementation

DNS Server types

- Caching Server
 - Previous local DNS server-like setting
- Primary Master Server
 - DNS service handles Domain \leftrightarrow IP queries.
- Secondary Master Server
 - This is Slave DNS server of Primary. For emergency, though primary DNS goes down, active Secondary master server would active and can resolve DNS queries.

DNS->IP in machine

- 1. Find it first from /etc/hosts
- 2. Ask DNS server stated in /etc/resolv.conf

- When we test DNS service we've made, we need to modify /etc/resolv.conf

BIND essential files

- /etc/bind/named.conf*
 - .options
 - .local
- For SPARCS DNS service,
 - db.SPARCS.NET
 - db.SPARCS.ORG
 - sparcs.conf

db.* format

```
1 $ORIGIN .
2 $TTL 3600 ; 1 hour
3 SPARCS.NET IN SOA ns.sparcs.org. wheel.sparcs.kaist.ac.kr. (
4 2011072811 ; serial
5 3600 ; refresh (1 hour)
6 1200 ; retry (20 minutes)
7 2419200 ; expire (4 weeks)
8 3600 ; minimum (1 hour)
9 )
10 NS ns.mazic.org.
11 NS ns.sparcs.org.
12 NS ns2.mazic.org.
13 NS ns3.mazic.org.
14 A 143.248.234.102
15 MX 10 mail.sparcs.org.
16 MX 100 sparcs.kaist.ac.kr.
17 $ORIGIN SPARCS.NET.
18 acacia CNAME sparcs.net.
19 aim CNAME sparcs.net.
20 air CNAME sparcs.net.
21 air3 A 143.248.234.102
22 airlover CNAME sparcs.net.
23 alphamin CNAME sparcs.net.
```

rndc

- Remote name daemon control
- Need to add this lines to named.conf

```
controls {  
    inet 127.0.0.1 allow  
    keys { <key name> ]  
}
```

rndc

- rndc *<options>* *<command>* *<command-options>*
 - halt : stop named immediately
 - querylog : log all query made to this named
 - Refresh : refresh named database
 - Reload : reloads the zone files
 - Stats : dump the current named statistics
 - Stop : Stop server, after dynamic update and do I XFR
- rndc.conf 에서 기본 설정을 불러온다 .

DDNS

- DDNS?
 - 한 도메인에 대한 IP 가 stable 하지 않으면 domain 을 통한 접근성 하락 .
 - IP 가 바뀐 client 쪽에서 DDNS service 를 지원하는 server 에 update 를 요청
 - db.SPARCS.NET.jnl

Recommended reading

- <http://ftp.isc.org/isc/bind9/cur/9.9/doc/arm/Bv9ARM.pdf>
 - BIND 를 이용하는 시스템 관리자를 위한 문서 .
이외에 관리에 필요한 DNS 유틸도 다양하게 소개하며 각종 문제 해결책도 제시되어 있다 .

Reference

- EE323 Kyungsoo Park's lecture slide
- BIND 9 Administrator Reference Manual