Nameserver

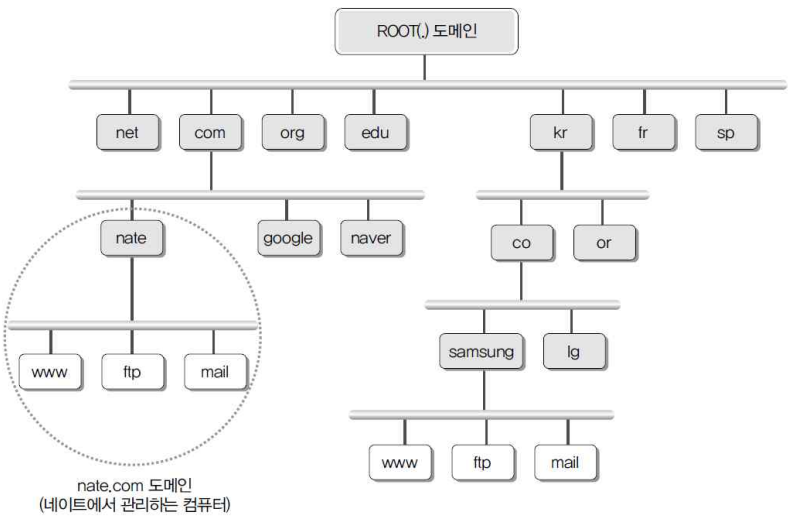
Ⅰ. 개요

p471

- 네임서버(Nameserver)란 도메인 주소를 IP 주소로 변환해 줄 수 있는 시스템
- 클라이언트 환경에서는 네임서버를 운영하지 않더라도 최소한 사용자가 이용하는 ISP 업체의 네임서버를 지정해 주어야 인터넷 사용 가능
- 웹 서버나 메일 서버와 같은 서버의 서비스 측면에서 네임서버는 매우 중요한 중추적인 역할

- 도메인 이름 체계
  - 초창기 인터넷에서는 1대의 네임 서버만으로도 충분히 IP주소와 이름의 관리가 가능
  - 인터넷이 폭발적으로 확장되면서, 몇 대의 네임 서버로는 실시간으로 인터넷 상의 수많은 컴퓨터들을 관리할 수가 없게 되었음
  - 트리 구조와 같은 '도메인 이름 체계' 고안

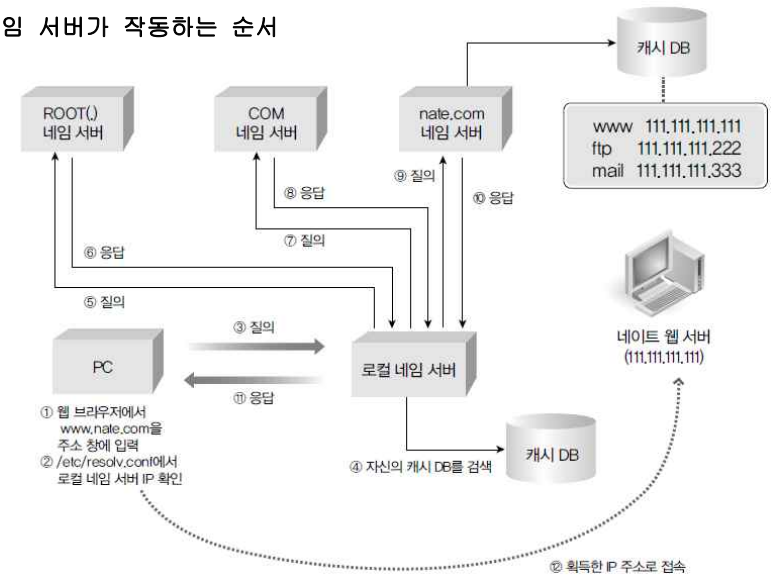
- 도메인 이름 체계



2. 네임서버 작동 과정

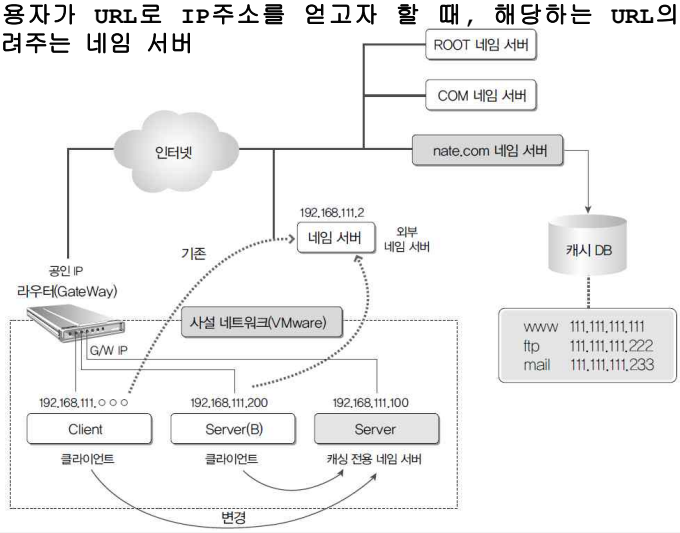
- 로컬 네임 서버가 작동하는 순서
  - /etc/resolv.conf 파일에 "nameserver IP주소"로 설정 → 이 네임 서버를 로컬 네임 서버라고 부름
  - www.nate.com의 IP주소를 요구하면 이 로컬 네임 서버에 질문
  - 로컬 네임 서버는 의외로 아는 것이 별로 없음
    - 로컬 네임 서버가 혼자서 전 세계의 모든 컴퓨터의 도메인 이름을 관리할 수는 없기 때문

- 로컬 네임 서버가 작동하는 순서



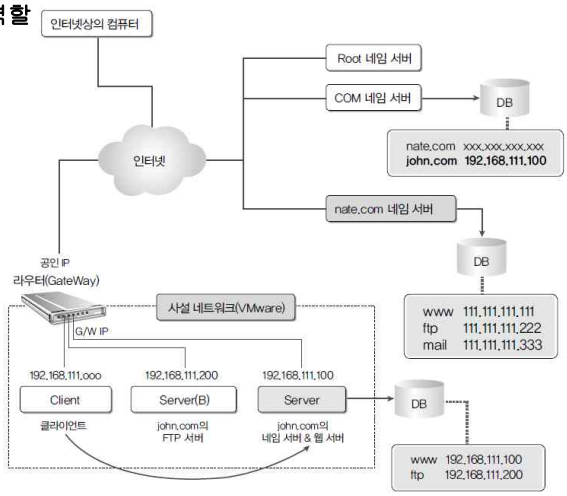
캐싱 전용 네임 서버

- 사용자가 URL로 IP주소를 얻고자 할 때, 해당하는 URL의 IP주소를 알려주는 네임 서버

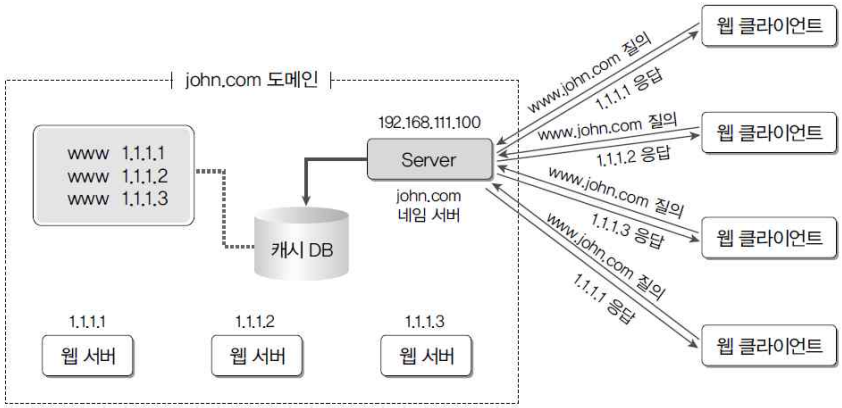


마스터 네임 서버

- 도메인에 속해 있는 컴퓨터들의 이름을 관리하고, 외부에 해당 컴퓨터의 IP주소를 알려주는 역할



- 라운드 로빈 방식의 네임 서버
  - 여러 대의 웹 서버를 운영해서, 웹 클라이언트가 서비스를 요청할 경우에 교대로 서비스를 실시하도록 하는 방식



3. 네임서버 관련 파일

3.1 네임서버 관련 파일들

네임서버 관련 파일	기 능
/etc/host.conf	해석(Resolution) 방법 및 순서 지정 파일
/etc/resolv.conf	네임서버 위치 지정 파일
/etc/named.conf	네임서버 기본 설정 파일
/var/named	네임서버 지역(zone) 파일 위치
/var/named/*.zone	네임서버 지역 파일
/var/named/named.ca	네임서버 캐시 파일
/var/named/*.rev	네임서버 리버스 맵핑 파일
/var/named/named.local	루프백 IP 주소에 대한 리버스 매핑 파일
/var/named/name_dump.db	Bind signal로 생기는 데이터베이스 파일
/var/named/name_stats	Bind 통계 정보를 담고 있는 파일

3.2 /etc/host.conf

- host.conf 파일에 지정할 수 있는 명령

설정 옵션		기 능
order	hosts	/etc/hosts 파일로 해석할 것인지(hosts), 네임서버로 해석할 것인지(bind) 해석 순서 지정 파일
	bind	
multi	on	/etc/hosts 파일에서 하나의 호스트가 여러 개의 IP를 가질 수 있는지 여부 설정
	off	
spoofalert	on	스푸핑(spoofing) 시도를 로그에 기록할 것인지 여부 결정
	off	
trim		도메인 이름을 인자로 취하여 호스트 검색시 기본 도메인으로 지정
nospoof		호스트 이름과 IP가 일치할 때 호스트 이름을 해석

```
[root@seokj ~]# cat /etc/host.conf
order hosts,bind_
```


3.3 /etc/resolv.conf

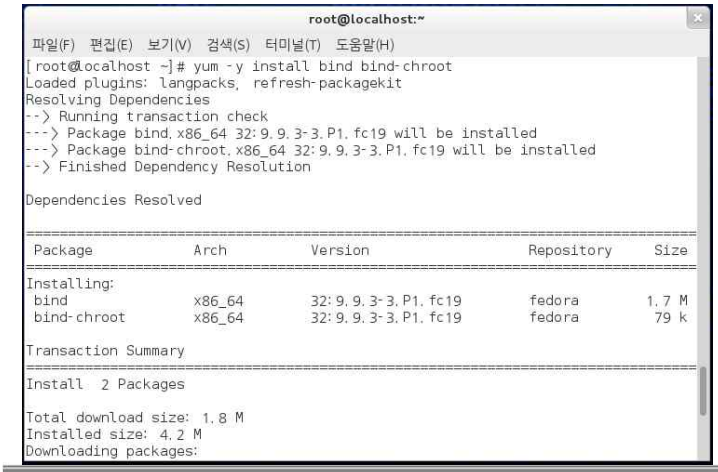
- 클라이언트 환경에서 네임서버를 운영하지 않더라도 로컬 시스템이 인터넷으로 연결되어 있다면 기본적으로 반드시 설정
- 도메인 해석을 위하여 어느 네임서버를 사용할 것인가를 설정하는 파일
- /etc/resolv.conf 파일에서 사용 가능한 옵션

설정 옵션	설 명
domain	- 사용자 호스트의 로컬 도메인 이름을 넣어 줌
search	- 자동으로 찾을 도메인 주소 입력 - 지정한 도메인에 대해서는 호스트명만 입력하면 자동으로 해당 사이트 찾음
nameserver	- IP 주소로 네임서버를 사용할 호스트 입력

4. 네임서버 설치

4.1 패키지 설치

```
# yum -y install bind bind-chroot
```



5. 네임서버 설정 파일

5.1 네임서버 관련 설정 파일

파일명	기능
/etc/sysconfig/named	chroot를 적용할 네임서버 루트 디렉토리 설정 파일
/etc/init.d/named	네임서버 데몬
/etc/named.conf	네임서버 설정 파일
/etc/rndc.key	공유키 설정 파일
/etc/rndc.conf	rndc 설정 파일
/var/named/*.zone	- /etc/named.conf에서 명시한 존 파일이 위치하는 장소 - chroot를 적용하는 경우 /var/named/chroot/var/named 디렉토리에 존 파일 위치

5.2 /etc/named.conf

- 네임서버 데몬이 시작될 때 제일 먼저 읽어들이는 설정 파일
- 옵션(options), 존(zone), 키(key) 설정 영역 등으로 구성

```
options { 옵션 };

zone "데이터베이스" IN {
        type ( hint | master | slave );
        file "존 파일명";
        allow-update { none; };
};

key 키이름 {
        algorithm "알고리즘 방식";
        secret "공유키";
};

controls {
        inet * allow { any; } keys { key_list; };
};

include "/etc/rndc.key";
```


5.2 /etc/named.conf (계속)

- Options 설정 영역
  - 네임서버가 작동하는데 있어서 여러가지 설정에 관련된 옵션 설정

```
options { 옵션 };
```

```
directory "디렉토리";
```

  - 네임서버 데이터베이스 파일들이 존재할 위치 설정 옵션
  - 기본값 : /var/named

```
dump-file "/var/tmp/data/cache_dump.db";
```

  - named 데몬이 가지고 있는 네임 정보가 갱신될 때 dump 파일로 저장, 이때 dump 파일이 생성될 위치와 파일명 지정

5.2 /etc/named.conf (계속)

- Options 설정 영역 (계속)

```
statistics-file "/var/named/data/named_stats.txt"
```

- 네임서버 통계 처리 목적으로 사용하는 옵션
- 네임서버 메모리 통계 파일을 생성할 위치와 파일명을 지정하는 옵션

```
forward (only | first);
```

- forwarders 옵션과 함께 사용
- 자신에게 도메인 질의를 지정한 다른 서버에게 위임하는 옵션
- only : 다른 서버가 응답이 없을 경우 자신도 그 질의에 대해 응답을 하지 않을 경우에 설정
- first : 타 서버에서 응답이 없을 때 자신이 응답하도록 할 때 설정

5.2 /etc/named.conf (계속)

- Options 설정 영역 (계속)

```
forwarders {네임서버 주소 1; 네임서버 주소2; 네임서버 주소3; …};
```

- 도메인에 대한 질의를 다른 서버로 넘겨줄 때 사용하는 옵션
- 타 네임서버는 복수형태로 지정 가능

```
notify ( yes | no )
```

- 마스터 서버의 존 정보가 변경되었을 때 존의 NS 서버(2차 서버)에게 메시지를 통보해 주는 기능
- 기본값 : yes

5.2 /etc/named.conf (계속)

- Zone 설정 영역
  - 캐쉬 전용 서버와 1차 네임서버, 그리고 2차 네임서버 등에 관련된 설정

```
zone "데이터베이스" IN {
        type ( hint | master | slave );
        file "존 파일명";
        allow-update { none; };
};
```

```
type ( hint | master | slave );
```

  - 캐시 전용 서버(hint),1차 네임 서버(master),2차 네임 서버(slave)

```
type slave;
masters { 1차 네임서버 IP 주소; };
```


5.2 /etc/named.conf (계속)

- Zone 설정 영역 (계속)

```
file "존 파일명";
```

  - options 설정 영역에서 directory로 명시한 디렉토리에 위치한 존 파일들을 설정하는 지시자
  - 존 파일들은 도메인을 IP로 변환되도록 해주거나 또는 IP 주소를 도메인으로 변환될 수 있도록 여러 설정을 포함
  - 파일명은 시스템 관리자가 임의대로 명시

5.2 /etc/named.conf (계속)

- Zone 설정 영역 (계속)

```
allow-update
```

  - key 설정 영역과 함께 작동
  - 1차 네임서버의 정보가 동적 update 기능에 의해서 2차 네임서버 존 데이터들이 변경되도록 할 때 사용
  - 인증을 위한 공유키를 사용할 경우

```
allow-update { key 공유키 이름; };
```

  - 공유키를 지정하지 않고 IP 주소로 2차 네임서버 지정할 경우

```
allow-update { 2차 네임서버 IP 주소; };
```

  - 2차 네임서버를 운영하지 않을 경우

```
allow-update { none; };
```


5.2 /etc/named.conf (계속)

- Key 설정 영역
  - 동적 update 또는 IXFR(Incremental Zone Transfer)에 의해서 원격 서버로 존 설정 데이터들이 전달될 때 원격 서버의 인증에 필요한 공유키를 설정하는 영역

```
key 키이름 {
        algorithm "알고리즘 방식";
        secret "공유키";
};
```

  - 키 이름은 임의로 설정 가능하나 공유키 생성시 지정한 키이름은 동일
  - 공유키 값은 dnssec-keygen에 의해서 생성

```
# dnssec-keygen -a hmac-md5 -b 128 -n HOST 키이름
```

  - key 설정 구문은 /etc/rndc.key를 그대로 include하여 사용 가능

5.2 /etc/named.conf (계속)

- Controls 설정 영역
  - rndc 유틸리티에 의해서 네임서버에게 명령을 전달하여 네임서버를 구동시킬 때 사용되는 제어 채널 설정 영역

```
controls {
        inet * allow { any; } keys { key_list; };
};
```

  - inet
    - 인터넷에 접속할 수 있는 TCP/IP 소켓으로 "IP주소 포트"로 명시
    - 포트를 지정하지 않을 경우 953으로 지정
    - "*" 표시는 포트를 사용하지 않을 경우 지정
  - allow {any;} keys {키 리스트;};
    - 키 리스트에 있는 각각의 키 이름을 가진 모든 호스트에 대해서 제어 채널에 접근하는 것을 허용

5.2 /etc/named.conf (계속)

- Controls 설정 영역 (계속)
  - rndc.key를 가진 로컬 호스트에 대해서 제어 채널에 접근하는 것을 허용할 경우

```
controls {
        inet 127.0.0.1 allow { localhost; } keys { rndc-key; };
};
```

5.3 /etc/rndc.conf

- 네임서버 데몬을 관리하는 프로그램인 rndc에 사용되는 설정 파일
- rndc-donfgen으로 생성

```
options { 옵션 };

server localhost { key "key"; };

key "key" { };

include "/etc/rndc.key";
```


5.3 /etc/rndc.conf (계속)

- Options 설정 영역
  - default-server, default-key, default-port 지정 가능

```
options {
        default-server localhost;
        default-key    "rndckey";
};
```

- Server 설정 영역
  - 서버의 주소를 지정한 후 key 설정에서 정의한 key_id 를 식별할 수 있도록 키 이름 설정

```
server localhost {
        key     "rndckey";
};
```

5.3 /etc/rndc.conf (계속)

- Key 설정 영역
  - named.conf 에서 설정해 준 키 설과 동일하게 설정하거나 /etc/rndc.key를 include로 삽입 가능

```
include "/etc/rndc.key";
```


5.3 /etc/rndc.conf (계속)

- rndc-confgen 도구
  - /etc/rndc.key 키 파일 자동으로 생성

```
# rndc-confgen -a
```

  - 생성된 rndc.key를 include 구문으로 사용할 수 있도록 파일 허가권과 소유권 부여

```
# chmod 640 /var/named/chroot/etc/rndc.key
# chown named.named /var/named/chroot/etc/rndc.key
```

  - /etc/rndc.conf 파일 설정

```
# rndc-confgen > /etc/rndc.conf
```

6. 네임서버 설정

6.1 도메인 등록

- 도메인 등록 센터에 도메인 등록 신청
  - www.seokjdb.com 이라고 가정

6.2 데이터베이스 존 추가

- /etc/named.conf 파일에 등록받은 도메인에 대한 데이터베이스 존 설정

```
•••
zone "seokjdb.com" IN {
        type master;
        file "seokjdb.zone";
        allow-update { none; };
};
•••
```

6.3 존 파일 설명

- /var/named/seokjdb.zone

```
$TTL    86400
@       IN      SOA     seokjdb.com. seokj.seokjdb.com. (

                        2               ;serial
                        86400           ;refresh
                        3600            ;retry
                        86400           ;expire
                        86400 )         ;minimum

                IN      NS      ns1.seokjdb.com.
                IN      NS      ns2.seokjdb.com.

@               IN      A       123.123.123.123

                IN      MX 10   seokjdb.com.
                IN      HINFO   INTEL LINUX

ns1             IN      A       123.123.123.123
www             IN      A       123.123.123.123
mail            IN      A       123.123.123.123
*               IN      A       123.123.123.123
```


6.3 존 파일 설명 (계속)

- TTL (Time To Live)

```
$TTL 86400
•••
```

  - 다른 서버에서 자신의 정보를 가져갔을 때 그쪽 서버의 캐시에 그 정보가 얼마나 오랫동안 머물 것인지를 결정하는 설정
  - SOA 레코드에서 상세 설명

6.3 존 파일 설정 (계속)

- SOA (Start Of Authority) 레코드

```
...
@       IN      SOA     seokjdb.com. seokj.seokjdb.com. (

                        2               ;serial
                        86400           ;refresh
                        3600            ;retry
                        86400           ;expire
                        86400 )         ;minimum
...
```

도메인명(@) 클래스명(IN) 레코드(SOA) 1차 네임서버. 관리자 이메일 주소.

- 도메인명 (@)
  - Origin 도메인
  - /etc/named.conf 파일의 포워드 존 영역에서 설정된 도메인
  - seokjdb.com를 의미

6.3 존 파일 설정 (계속)

- SOA (Start Of Authority) 레코드 (계속)

도메인명(@) 클래스명(IN) 레코드(SOA) 1차 네임서버. 관리자 이메일 주소.

- 클래스명(IN:Internet)
  - 네트워킹 어드레스 클래스를 의미
  - 항상 레코드 리소스를 지정할 때 사용
- 관리자 이메일 주소 (seokj.seokjdb.com)
  - seokj@seokjdb.com을 나타냄
  - Origin 도메인을 지정할 때 "@"로 사용했기 때문에 마침표(.)로 대신

6.3 존 파일 설명 (계속)

- SOA 필드

```
•••
                                        (
                        2               ;serial
                        86400           ;refresh
                        3600            ;retry
                        86400           ;expire
                        86400 )         ;minimum
•••
```

- serial
  - 네임서버의 데이터 버전을 나타냄
  - 네임서버 설정이 변경될 때마다 이 시리얼 번호에 따라서 갱신
  - 2차 네임서버 또는 타 네임서버에서 로컬 네임서버의 데이터를 불러올 때 자신이 가지고 있는 시리얼 번호와 비교하여 자신의 것보다 높은 경우에는 업데이트된 데이터를 가져옴

6.3 존 파일 설명 (계속)

- SOA 필드 (계속)

```
•••
                                        (
                        2               ;serial
                        86400           ;refresh
                        3600            ;retry
                        86400           ;expire
                        86400 )         ;minimum
•••
```

- refresh
  - 2차 네임서버가 1차 네임서버에게 새롭게 업데이트된 정보가 있는지 요청할 때까지의 시간을 지정
  - 보통 21600(6시간), 42300(12시간)으로 설정
  - 정보가 자주 바뀌는 상황이라면 10800(3시간)으로 설정
- retry
  - 2차 네임서버가 1차 네임서버와 연결이 되지 않을 경우 재연결할 때까지의 대기 시간 : 1800(30분), 3600(1시간)

6.3 존 파일 설정 (계속)

- SOA 필드 (계속)

```
•••
                                        (
                    2               ;serial
                    86400           ;refresh
                    3600            ;retry
                    86400           ;expire
                    86400 )         ;minimum
•••
```

  - expire
    - 2차 네임서버가 일정 시간 동안 1차 네임서버에 접속하지 못했을 경우 이전의 정보가 의미가 없는 것으로 간주하여 이를 파기할 시간
    - 보통 604800(1주) ~ 1209600(2주)로 지정
  - minimum
    - 다른 서버에서 자신의 정보를 가져갔을 때 그쪽 서버의 캐시에 그 정보가 얼마나 오랫동안 머물 것인지를 결정

6.3 존 파일 설정 (계속)

- NS(NameServer) 레코드

```
•••
            IN      NS      ns1.seokjdb.com.
            IN      NS      ns2.seokjdb.com.
•••
```

  - 지정한 로컬 도메인에 대한 네임서버를 지정할 때나 서브 도메인을 구성하고자 할 때 사용
  - IN 클래스 앞에 도메인이나 호스트명이 생략된 경우 Origin 도메인이 있는 것으로 간주
  - seokjdb.com 도메인을 관리하는 네임서버가 ns1.seokjdb.com과 ns2.seokjdb.com이라는 것을 의미

6.3 존 파일 설명 (계속)

- A(Address) 레코드

```
•••
www             IN      A       123.123.123.123
•••
```

  - 호스트 이름에 IP를 부여하여 도메인 검색시 어떠한 IP 주소로 맵핑되는지를 설정
  - seokjdb.com 도메인을 검색하였을 때 123.123.123.123 IP 임을 알려주는 레코드

6.3 존 파일 설명 (계속)

- MX(Mail eXchanger) 레코드

```
•••
                IN      MX 10   seokjdb.com.
•••
```

  - 해당 도메인으로 오는 메일을 처리할 메일 서버를 지정할 때 사용하는 레코드
  - 메일 서버로 사용하고자 하는 도메인에 대하여 MX 레코드로 지정

6.3 존 파일 설정 (계속)

- CNAME(Canonical NAME) 레코드

```
•••
www             IN      A       123.123.123.123
ftp             IN      CNAME   www
•••
```

  - 설정하고자 하는 호스트에 대해 IP 주소 대신에 이미 설정된 호스트 이름으로 설정해 주는 레코드

6.3 존 파일 설정 (계속)

- HINFO(Host INFOmation) 레코드

```
•••
                IN      HINFO   INTEL LINUX
•••
```

  - 호스트 정보를 나타내는 것