DNS & BIND

19 Summer

Made by loopy

1. DNS

1. DNS - DNS란?

- ✓ DNS(Domain Name Service) → **도메인 이름과 IP 주소를 매칭**시키는 시스템
- ✓ 사람이 읽을 수 있는 도메인 이름과 실제 컴퓨터에서 쓰이는 IP 주소를 상호 변환
- ✓ DNS 자체는 서버가 아니라, 이러한 시스템을 의미함 (DNS를 운영하는 서버를 DNS 서버, 혹은 네임서버(Name Server) 라고 함)

ex) 전화번호를 직접 입력해서 전화를 거는 것 → IP 주소로 연결

전화번호부에 등록된 이름으로 전화를 거는 것 → 도메인 이름으로 연결

이 예시에서 전화번호부가 DNS와 유사한 역할을 한다

1. DNS - DNS란?

- ✓ DNS는 분산형 데이터베이스 시스템을 사용
- ✓ DNS는 도메인 이름 공간(Domain Name Space), 리소스 레코드(Resource Record), 네임 서버(Name Server), 리졸버(Resolver) 로 구성되어 있다

1. DNS - Domain Name Space

Domain Name Space란?

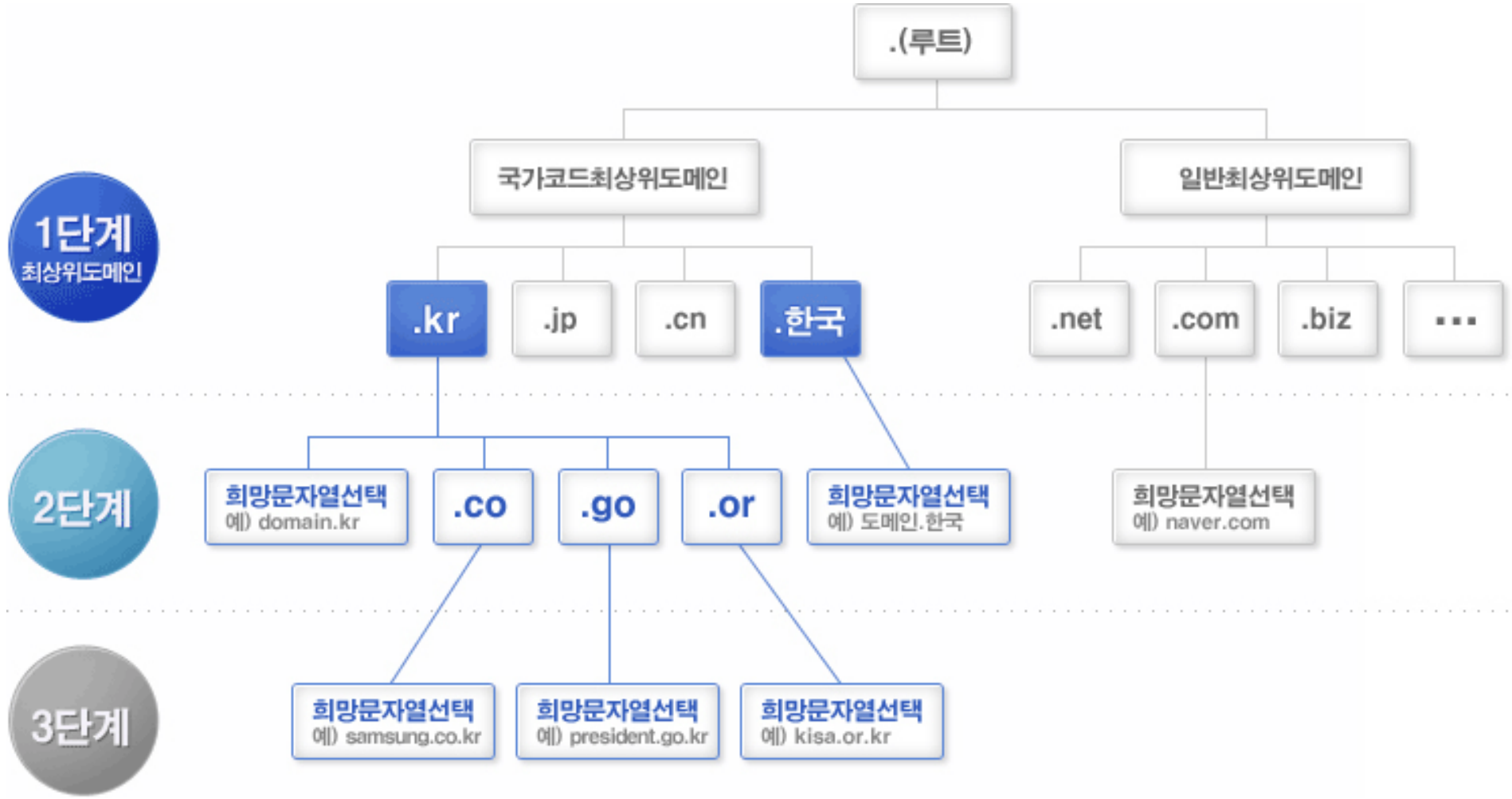
✓ DNS가 저장/관리하는 계층적 데이터베이스로, 최상위에 Root가 존재하고 그 아래로 모든 *호스트가 트리 구조로 이루어져 있음

✓ 같은 레벨에서는 레이블(이름)이 유일해야 함

✓ 계층 구조는 Root, TLD(Top Level Domain), SLD(Second Level Domain), 서브 도메인 등으로 이루어져 있음

*호스트 : Domain Name Space 트리에서의 Node 를 의미

1. DNS - Domain Name Space



1. DNS - Domain Name Space의 계층

Root 도메인 계층

- 가장 상위에 존재하는 특수한 계층으로, 모든 도메인 네임은 root의 도메인 네임으로 시작한다
- 도메인 네임 공간의 분배와 할당은 ICANN에 의해 root 도메인에서 가장 처음으로 이루어진다
- 최상위 domain으로 전 세계 13개 뿐이고, 다른 나라에서는 미러 서버를 운영한다.
  - 미국 10개, 네덜란드, 노르웨이, 일본 각각 한 개
  - 우리나라의 경우 미러 서버가 3개 있다. (한국 인터넷 진흥원, kt, 한국 인터넷 연동센터)
- 도메인 네임으로 null 혹은 (.)을 사용한다

1. DNS - Domain Name Space의 계층

최상위 도메인 계층(TLD, Top Level Domain)

- root 도메인계층의 하위에 해당하는 계층으로 1단계 도메인으로도 불린다
- 국가에 할당된 도메인과 국제적 업체에 할당된 도메인으로 크게 분류된다
- 국가 코드 최상위 도메인(Country Code Top Level Domain, ccTLD)
  - 최상위 도메인 네임은 국가를 나타내며, 하위 도메인들은 그 국가 조직의 성격을 나타내는 도메인 네임(레이블+상위 노드의 도메인 네임)을 사용
- 일반 최상위 도메인(Generic Top Level Domain, gTLD)
  - 국가 단위가 아닌, 국제적 단위로 사용되는 도메인들을 일반 최상위 도메인
  - 전 세계를 기준으로 비영리, 상업적, 지역별 등의 목적에 따른 분류로 나누어진다

1. DNS - Domain Name Space의 계층

구 분		설 명
국가 코드 최상위 도메인	us	미국의 공식 국가 도메인이다. 거주자 및 기관, 단체 등이 등록할 수 있습니다.
	kr	한국 공식 국가 도메인이다. 주민등록증이나 사업자 등록증이 있어야 등록 가능하다.
	jp	일본 공식 국가 도메인이다. 일본 현지에 있는 개인 혹은 기업만이 등록 가능하다.
	cn	중국의 공식 국가도메인이다.
일반 최상위 도메인	com	두 개의 도메인은 가장 대표적인 국제 도메인이다. 전 세계적으로 비즈니스나 일반적인 목적으로 사용되는 도메인으로 전 세계 누구나 등록 가능하다.
	net	
	asia	아시아 지역을 대표하는 도메인이다. 아시아 지역 내 법적 주체가 있으면, 전 세계 누구나 등록 가능하다.
	info	information의 약자로 정보 관련 사이트 등을 주로 이용하고, 전 세계 누구나 등록 가능하다.
	biz	Business의 약자로 비즈니스 관련 기업이 주로 사용합니다.
	mobi	모바일 기기를 이용한 인터넷 환경에 특화된 도메인이다.
	org	org도메인은 비영리 기관, 단체에서 많이 사용하는 도메인으로 영리추구를 목적으로 하는 기업이 아닌, 친선도모나 사회사업, 국제활동기구, 종교단체 등에서 주로 사용한다.
	name	개인의 이름, 상품 브랜드명로 사용하는 신규 최상위 도메인이다. 영문과 숫자를 결합하여 등록 가능하다.
	tel	.tel 도메인은 별도의 홈페이지 제작을 하지 않고 도메인 등록으로 홍보용 웹사이트가 자동 제공된다.

1. DNS - Domain Name Space의 계층

2단계 도메인 계층(SLD, Second Level Domain)

- 최상위 도메인으로부터 분류된 도메인이 위치하는 계층으로 도메인을 등록하고자 하는 조직이나 국가에 속하는 기관의 성격으로 분류된다
- 상위 도메인이 gTLD인 경우
  - 조직이나 개인을 최종 사용자로 볼 수 있고, 원하는 호스트 네임(레이블)을 사용하여 도메인 네임을 할당 받는다 (ex. naver.com)
- 상위 도메인이 ccTLD인 경우
  - 호스트와 조직의 성격을 나타내는 도메인이 위치한다 (ex. ac.kr, co.kr 등)

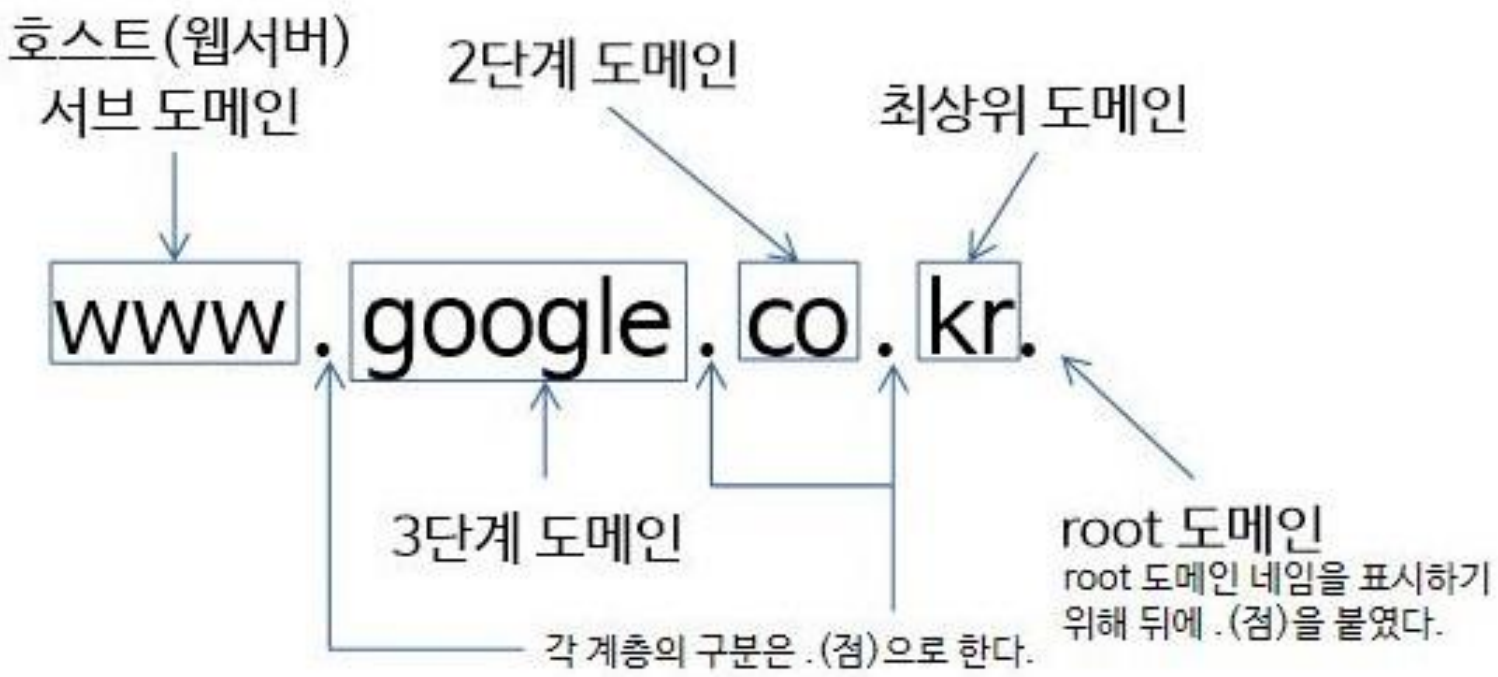
1. DNS - Domain Name Space의 계층

3단계 도메인 계층(Third Level Domain or Sub Domain)

- 상위 도메인이 ccTLD인 경우
  - 3단계 도메인의 특성을 가진 도메인으로 조직이나 개인에서 도메인을 등록, 즉 최종 사용자의 도메인이 정의된다 (ex. google.co.kr)
- 상위 도메인이 gTLD인 경우 (= 서브 도메인 계층)
  - 서브 도메인으로의 특성을 가진 도메인으로 최종 사용자가 필요에 따라서 만든 하위 도메인
  - 여러 대의 Web Server를 목적에 따라서 도메인을 구별하는 등의 목적으로 사용된다 (ex. www.naver.com, sports.naver.com 등)

서브 도메인 계층 : 마지막에 위치하는 도메인 계층으로, 3단계 도메인 계층과 동일한 기능

1. DNS - Domain Name Space의 계층



1. DNS - Resource Record

Resource Record란?

✓ 도메인과 관련된 정보를 가지고 있는 *Record

✓ 리소스 레코드로 정의되어지지 않는다면, domain name space에 정의되어 있어도 해당 도메인 네임에 매치되는 IP주소를 알 수 없기 때문에 접속이 불가능하다

✓ Resource Record의 유형에는 A(Address), NS(Name Server), CNAME(Canonical Name), SOA(Start of Authority) 등 다양하다

*Record : 데이터베이스에서 데이터를 가지고 있는 항목, row와 동일한 의미

1. DNS - Resource Record의 구성

Resource Record의 구성

- 이름(Name)
  - 레코드의 이름 또는 소유자. Root 도메인 혹은 하위 도메인일 수 있음
- 유형(Type)
  - 레코드의 유형. ex) A, NS, CNAME, SOA 등
- 클래스(Class)
  - 각 resource record의 유형 집합. TCP/IP 의 class는 IN(텍스트 코드) 혹은 1
- TTL(Time-to-Live)
  - 로컬에 저장된 레코드 사본이 업데이트 또는 삭제되어야 하는 빈도. 기본값은 1시간
- 데이터(Resource data)
  - 레코드의 데이터로, 레코드의 유형에 따라 다르다

1. DNS - Name Server / Resolver

네임 서버(Name Server)란?

✓ 영문 도메인을 IP 주소로 mapping 시켜주는 서버

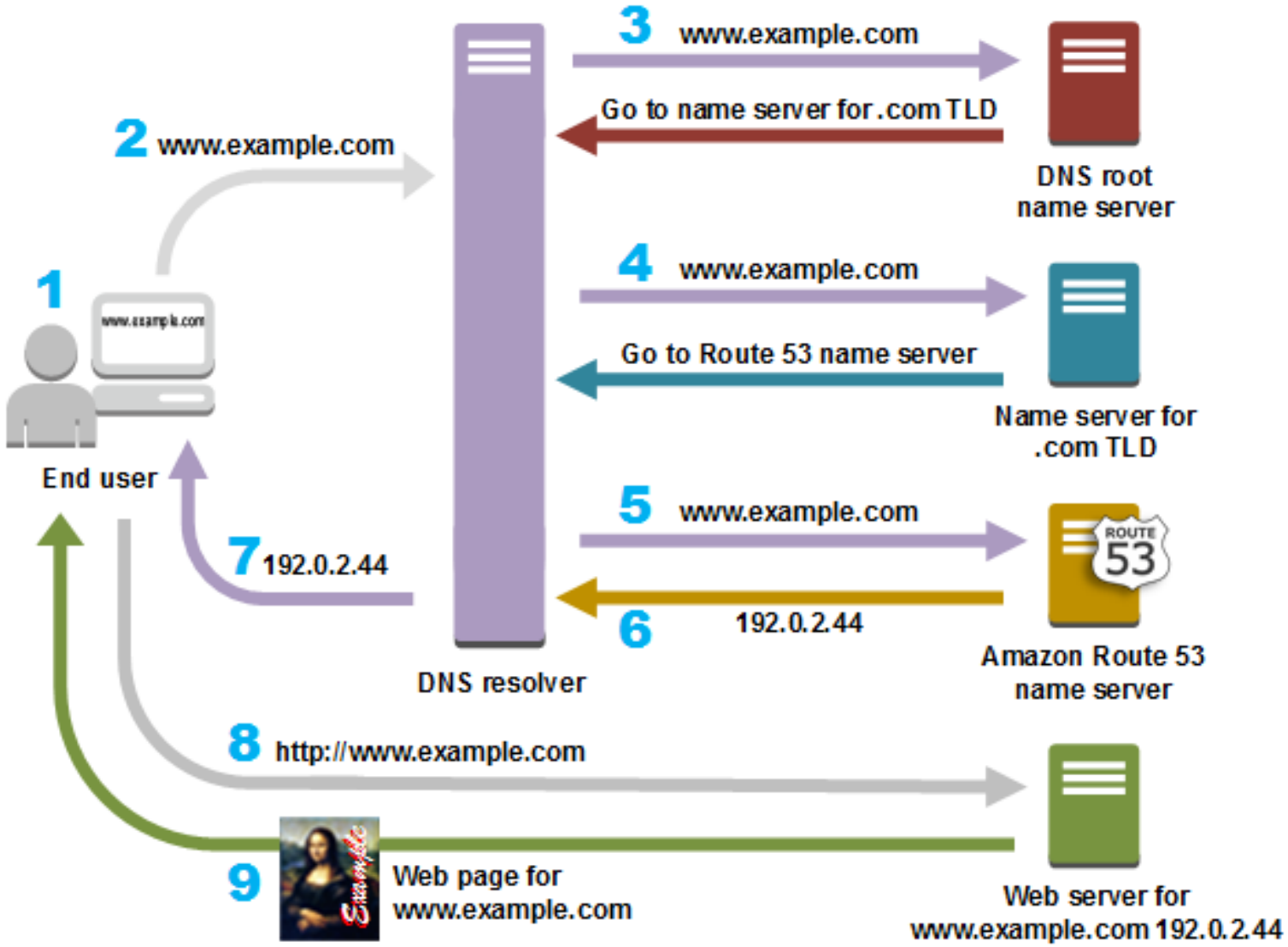
Resolver란?

✓ 프로그램의 request를 네임 서버에 대한 *query형태로 번역하고 그 query에 대한 response를 프로그램에 적절한 형태로 변경

✓ Name Server에 요청을 보내고, 그 응답을 해석하여 정보를 돌려준다

*query : 데이터베이스에 정보를 요청하는 것

1. DNS - Name Server / Resolver



1. DNS - DNS Spoofing

DNS Spoofing

- DNS 서버로 보내는 질문을 가로채서 변조된 결과를 보내주는 것
- 해킹 방법
  - 네트워크에 DNS 서버로 보내지는 패킷이 있는지 확인한다. 원래 목적지가 자신이 아닌 패킷은 읽지 않지만, 설정을 변경해서 모든 패킷을 읽어오게 한다
  - DNS 서버로 보내지는 패킷이 있다면, 그것을 보낸 PC에게 자신이 원하는 변조된 IP를 전송한다.
    - 보통은 공격자가 DNS 서버보다 물리적으로 가까이 있으므로 공격자가 보낸 패킷이 DNS 서버가 보낸 정상적인 패킷보다 먼저 도착하고, 나중에 온 정상적인 패킷은 버려진다.
  - PC는 변조된 IP로 접속을 하게 된다.
- 네이버에 접속한다고 가정한다면, 피해자는 정상적으로 www.naver.com을 입력했는데 공격자의 웹서버로 접속이 되는 것이다. 만약 이 사이트가 겉보기로는 네이버와 유사한 사이트이고, 사용자가 여기에서 로그인을 시도한다면?

1. DNS - Zone File

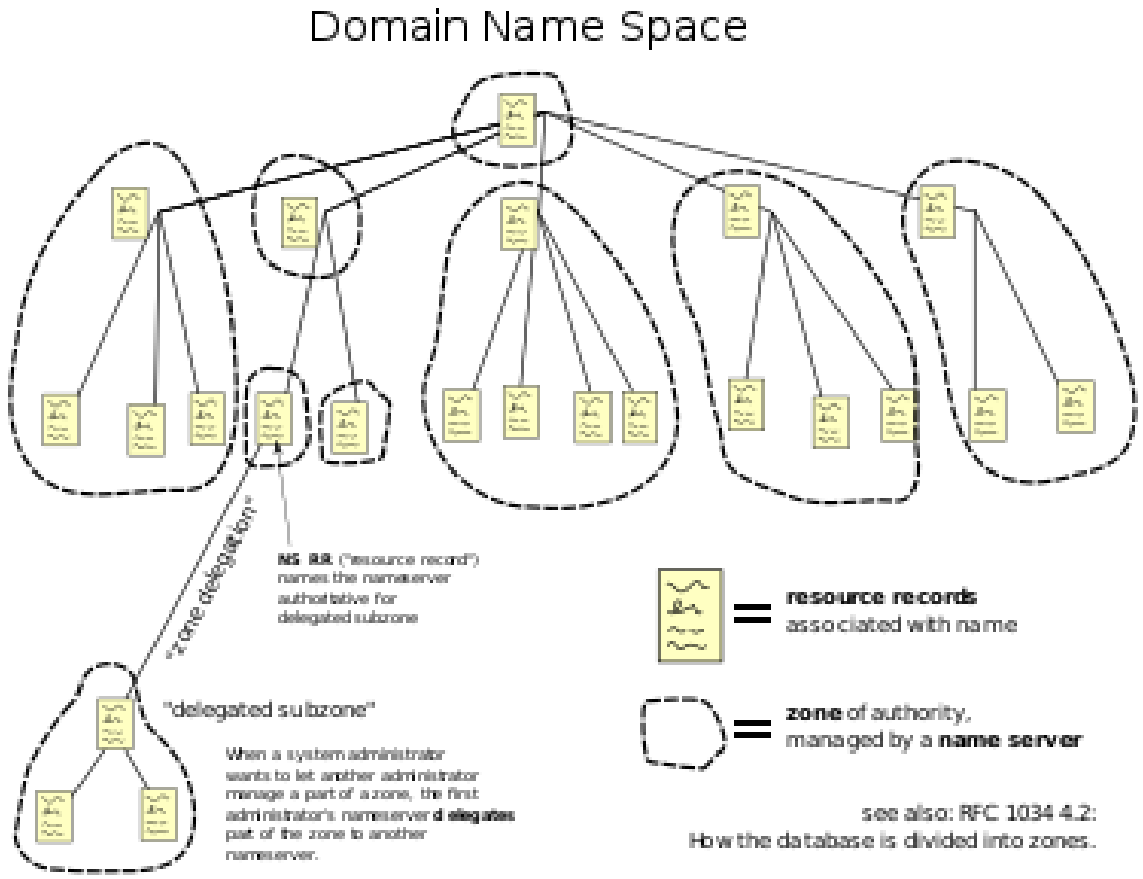
Zone

✓ Name Server가 관리하는 영역

Zone File

✓ DNS zone을 나타내는 text file

✓ [name] [TTL] [class] [type] [data] 형식으로 구성된다



1. DNS - Zone File 예시

/etc/bind 폴더 내에 zone file 들이 저장되어 있음

```
ns      IN      A       143.248.234.102
;       IN      AAAA    2001:220:802:1001::2
ns1 IN  A       143.248.234.161
ns2 IN  A       143.248.234.151
www     IN  CNAME sparcs.org.
; box names
ara     IN      A       143.248.234.103
araplus IN      A       143.248.234.128
;       IN      AAAA    2001:220:802:1001::3
nuri    IN      A       143.248.234.104
;gurum  IN      A       143.248.234.105
baeum   IN      A       143.248.234.105
;       IN      AAAA    2001:220:802:1001::5
bee     IN      A       143.248.234.106
;       IN      AAAA    2001:220:802:1001::7
```

2. BIND

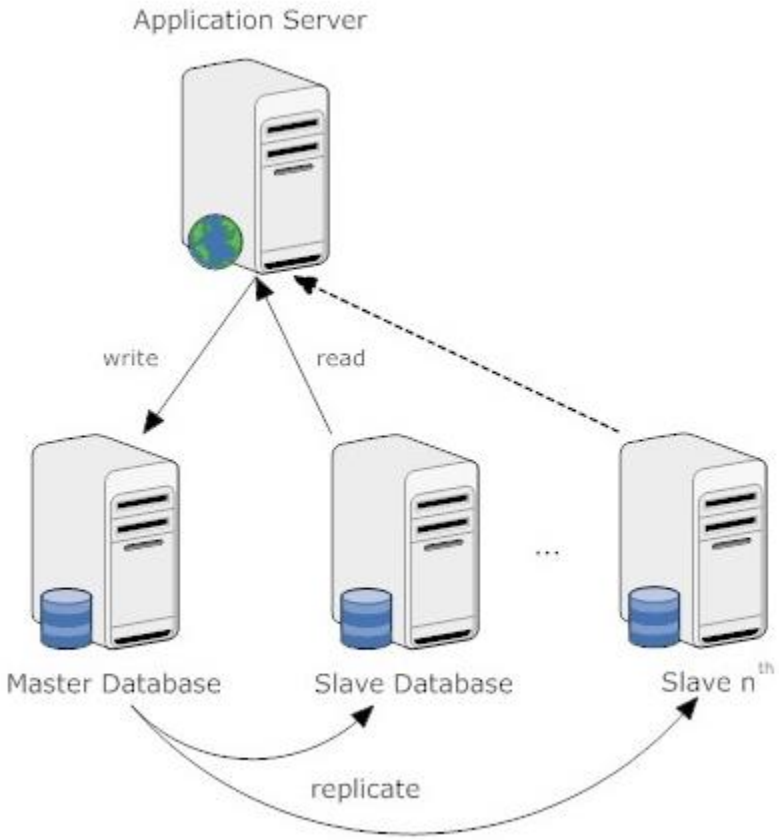
2. BIND - BIND란?

BIND란?

- ✓ BIND(Berkeley Internet Name Domain)는 BSD 기반의 UNIX 시스템을 위해 설계된 **DNS 소프트웨어**이다
- ✓ 1980년대 초 UC Berkeley 대학원생 4명이 모여서 만든 소프트웨어
- ✓ 현재까지 BIND가 사실상의 standard DNS server
- ✓ BIND 9 버전이 사용되고 있고, BIND 10 버전(bundy)은 현재 개발 중
- ✓ named(name daemon) 으로도 종종 불린다

2. BIND - Master-Slave Server

- 같은 내용인 여러 DNS서버를 운영할 때, 한 서버를 master로 지정하고 다른 서버들이 master 서버로부터 데이터를 가져오도록 하는 구조
- 요청이 한 서버에만 집중되지 않도록 적절하게 부하를 분산시킨다
- 각 slave에 대한 master를 영역에 따라 바꿔줄 수도 있고 master를 사용할 수 없게 될 경우 Secondary master를 지정하여 이것을 master slave로써 사용할 수 있다.



2. BIND - BIND 설치

- ✓ BIND 설치 : sudo apt-get install bind9
- ✓ BIND 실행 : sudo service bind9 start (or sudo /etc/init.d/bind9 start)
- ✓ BIND 중지 : sudo service bind9 stop (or sudo /etc/init.d/bind9 stop)
- ✓ BIND 재실행 : sudo service bind9 restart (or sudo /etc/init.d/bind9 restart)

2. BIND - BIND 명령어

DNS 정보 확인

- nslookup (name server lookup)
  - Domain name을 입력하면 그 주소에 대한 ip 주소와 기타 정보 등을 알려준다
  - 설치 : sudo apt-get install dnsutils
  - 사용법 : nslookup [Domain Name] (ex. nslookup ara.sparcs.org)
- whois
  - WHOIS 서버에서 domain 정보를 찾아주는 소프트웨어로써 domain에 대한 정보가 아주 자세하게 나오고 등록자에 대한 정보도 나온다
  - 설치 : sudo apt-get install whois
  - 사용법 : whois [Domain Name] (ex. whois naver.com)

2. BIND - BIND 명령어

DNS 정보 확인

- dig (domain information grouper)
  - DNS name server 에 질의하기 위한 네트워크 관리 명령 줄 인터페이스 툴
  - nslookup 보다 상세한 정보를 여러 option으로 설정 가능
  - Option으로 레코드의 type을 지정해줄 수 있다
    - any, soa, a, hinfo, mx, txt 등

2. BIND - BIND 설정 파일

BIND 설정 파일

- /etc/host.conf : ip 를 찾을 때 순서를 정해주는 파일
  - order : 붙여진 순서대로 DNS를 찾는다. host, bind, nis 를 사용할 수 있다.
  - multi : on/off. on으로 /etc/hosts에 둘 이상의 ip 주소를 등록하게 허용할 수 있다.
  - alert : on/off. on 으로 spoof 시도가 log되게 할 수 있다.
  - nospoof : on/off. on으로 spoof 시도를 막지만 느려지게 된다.
  - trim : domain name을 인수 취급하게 한다.

2. BIND - BIND 설정 파일

BIND 설정 파일

- /etc/resolv.conf
  - 네임 서버에 쓸 Dns를 저장해 둔다
  - domain, search, nameserver 옵션을 이용하여 구현을 할 수 있다
- /etc/bind/db.~
  - Zone file의 RR type 정보를 기록해 둔다.
- /etc/bind/named.conf
  - zone file의 db위치, 타입에 관한 정보들을 설정한다.

감사합니다 ☺

Made by loopy