DNS & BIND

moonde

DNS

Domain name system : 도메인 이름을 **ip** 주소로 변환

Ip 숫자 주소가 기억하기 어렵기 때문에 만들어짐 **.**

큰통치킨 시키는 법 **.**

전화 번호부에서 ‘ㅋ’ 으로 시작하는 부분 찾기 **=> ‘** ㅋ’ 으로 시작하는 부분 찾기 **=> …**

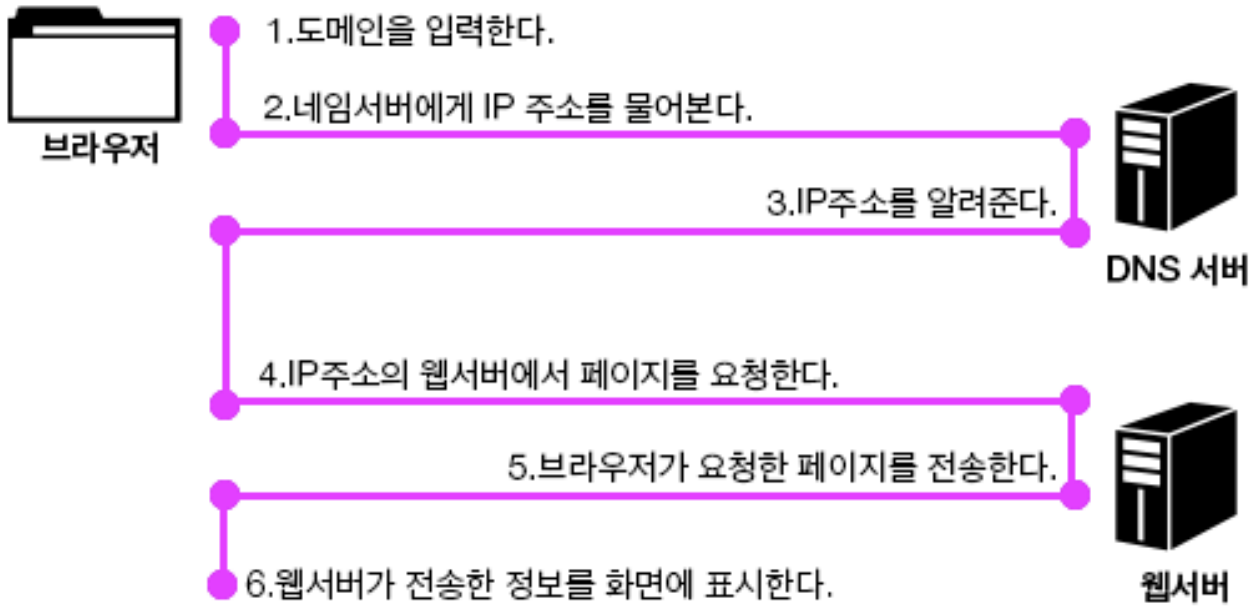
=> 큰통치킨 **: 042 – 867 – 8292** 를 찾고 전화걸기

Name server

DNS 소프트웨어 설치되어 **DNS** 를 제공하는 서버

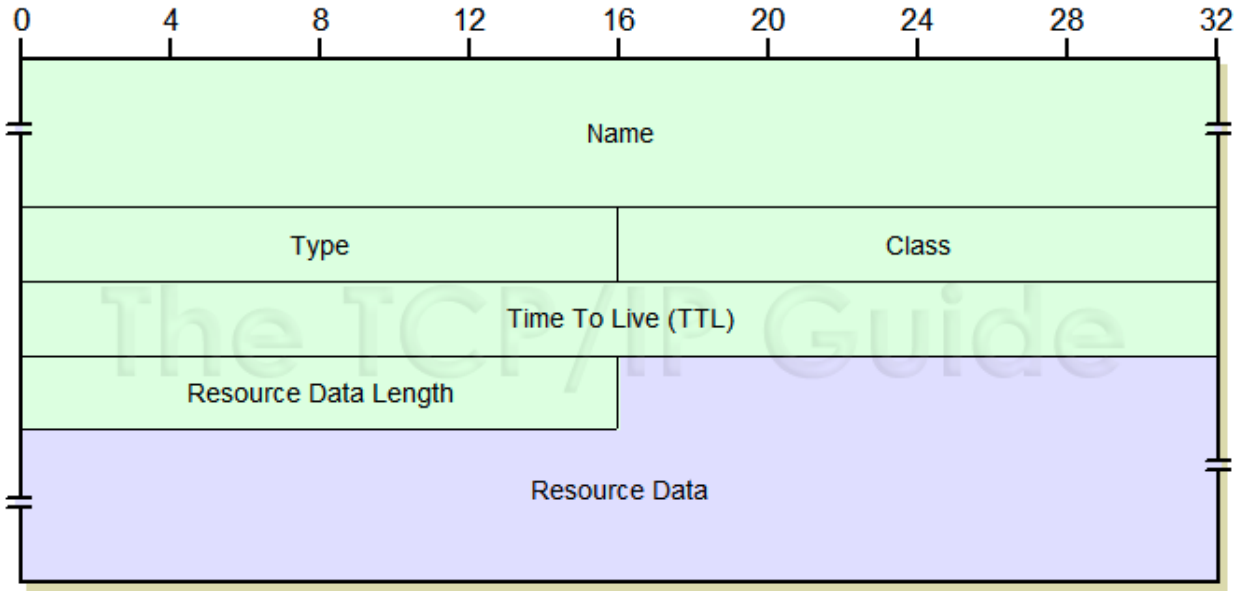
DNS database 와 resolver 를 포함함 .

DNS data 는 Resource record 형태로 저장



Resource record

Domain name 과 관련된 정보 항목을 갖는 레코드 구성



Name
: 도메인 이름
Type
: 정보 유형
Class
: internet 에서는 1(IN)
TTL(time to live)
: cache 에 저장될 시간
Rdlength
: rddata field 의 크기
Resource data
: resource record 의 내

Record resource(Type)

type	info
A(address)	호스트 의 ipv4
NS(name server)	Name server 의 이름
CNAME(canonical name)	공식적인 host name
SOA(start of authority)	zone의 속성 정보
PTR(pointer)	Ip 주소에 대한 이름
MX(mail exchange)	Mail server의 이름
TXT(text string)	문자열 정

Resource record(class)

DNS 를 맨 처음 만들었을 때 가능한 포괄적으로 만들도록 설계

=> DNS 는 다른 프로토콜과 동시에 **TCP/IP** 를 지원

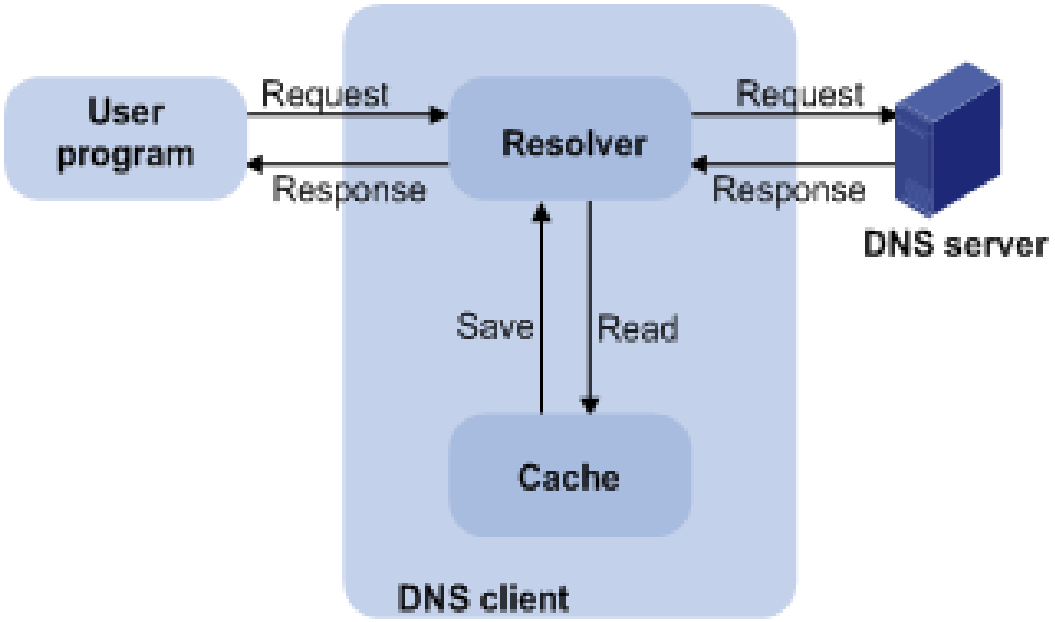
=> 각 프로토콜이 서로 다른 **resource record** 유형을 가질 수 있도록 정의

Class : 각 **resource record** 유형 집합

이 때 **, tcp/ip** 는 텍스트 코드가 **“ IN”** 인 **“ 1”** 을 사용 **(** 인터넷용 **)**

Resolver

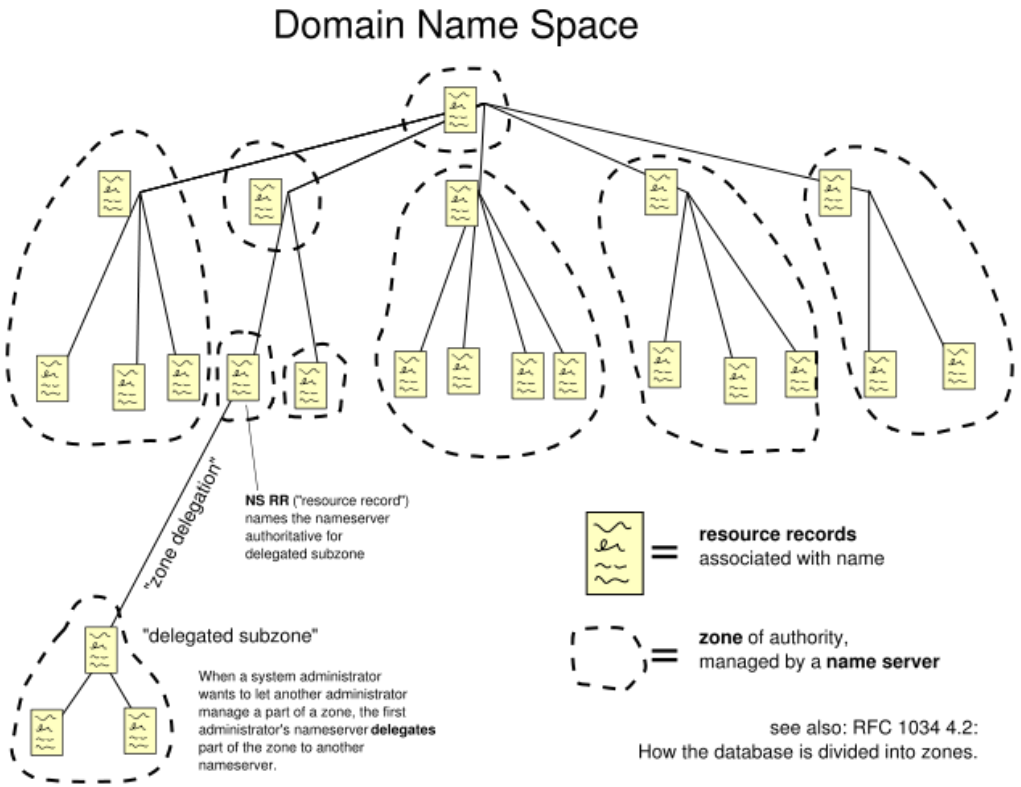
프로그램의 **request** 를 네임 서버에 대한 **query** 형태로 번역하고 그 **query** 에 대한 **response** 를 프로그램에 적절한 형태로 변경함



속도 향상을 위 Cache 에 24
- 48 시간 동안 저장해놓음

Domain name space

: 도메인 이름을 트리 형태로 구성하고 노드에 도메인 대응



Root zone 에서 시작해서 여러개의 하위 DNS zone 으로 나뉨

DNS zone 에서 관리자가 하위 도메인에 대한 권한을 갖음 .
+ 하위 도메인에 관한 권한을 줄 수 있음

Zone file

DNS zone 을 나타내는 **text file.**

<name><ttl><class><type><data> 형식으로 구성됨

ex)

Example.com 1h IN NS ns

→ ns 는 **example.com** 의 **name server**

Example.com 1h IN MX mail.example.com

→ mail.example.com 은 **example.com** 의 메일서버

(example.com 대신 **domain name** 의 의미로 **@** 를 사용할 수 있음 **.)**

Zone file 예

```
moonde@sparcs:~$ vi /etc/bind/db.SPARCS.ORG
```

라고 치면 sparcs zone file 이 db 에 저장되어 있는 것을 볼 수 있다 .

```
otl             IN      A       143.248.234.218
otlplus IN      A       143.248.234.126
a               IN      A       143.248.234.205
k               IN      A       143.248.234.162
arari   IN      A       143.248.234.135
webchat IN      A       143.248.234.158
taxidev IN      A       143.248.234.140
onestep IN      A       143.248.234.170
newbie  IN      A       143.248.234.123
olimdev IN      A       143.248.234.124
;redmine        IN      A       143.248.234.108
da              IN      A       143.248.234.149
odongtong       IN      A       143.248.234.117
sciwar IN A     143.248.234.220
zabo    IN      A       143.248.234.107
cctv    IN      A       143.248.234.120
apply   IN      A       143.248.234.62
```

해킹 기법 : dns spoofing

정상적인 동작은 사용자가 **dns** 서버로 부터 **ip** 주소를 받아오는 것.

BUT 공격자가 **dns** 와 **client** 사이에 침투해서 **client** 한테 의도와 다른 **ip** 주소를 전해줌.

1. 중간자 공격

   client 가 dns server 로 query 할 때 침투하여 query 를 바꿔줌

2. 사용자 컴퓨터에 저장된 **dns** 주소가 바뀌었을 때

   client 가 자기 local 을 보고 query 해도 의도하지 않은 응답이 옴.

Sub domain

각각의 도메인이 서로 다른 서버를 가리키게 해줌 **(서버 식별)**

ex) sparcs.org 에서 뭔가 다른 운영이 필요해 다른 서버를 사용해야 할 때 **, sparcs.org** 와 **bbs.spracs.org** 가 가리키는 **ip** 를 다르게 설정

=> 하나의 도메인이 여러개의 **ip**

=> 비용 절감

하나의 **ip** 주소를 가지는 여러개의 **domain** 이 **domain** 이름에 따라 다른 디렉토리 파일을 가져오게도 할 수 있음 **(virtual hosting)**

Top-level domain(TLD)

도메인을 구분하는 가장 큰 카테고리 **(** 성격에 따라 분류 **)**

운영 주체에 따라 국제 인터넷 관리 기구 **ICANN** 에서 분류

CcTLD(country code tld) : 개별 국가에서 사용

가격대가 높고, 신청 자격 제한

Ex) kr, co.kr 등

gTLD(generic tld) : 특정한 조직 계열에 따라 사용

가격대가 낮고 역사가 오래됨. 신청자격 제한 없음

Ex) com, net, org(비영리 단체 라는 뜻 ㅎ), edu, gov, mil, .xxx 등

New gTLD : gTLD 가 너무 많아져서 **2014** 년 출시

가격에 gtlb 에 비해 비쌈, 모바일 혹은 특정 브라우에서 안 될 가능성 있음

ex) coffee, email, news

Root domain(최상위 dns)

전 세계 **13** 개 뿐 **(** 미국 **10,** 네덜란드 **1,** 노르웨이 **1,** 일본 **1)**

다른 나라에서는 미러 서버 운영 ← 관리는 **root** 서버에서 하지만 내용은 동일하다 **! But** 자체적 인터넷 통신 관리 가능

미러 서버가 생긴 이유

2002 년 때 디도스 공격으로 **root** 서버 **13** 대 중 **9** 개가 영향을 받음 이를 막기 위해 **anycast** 기술을 적용 시켜 전 세계 **67** 곳의 미러 서버를 만듦
=> 이후 국내에서 **dns** 질의 대부분 응답 가능해짐 **.**

Anycast : 롸우팅 경로가 가장 가까운 곳으로 통신하는 기술

우리나라의 경우 **2003** 년에 **3** 대 설치 **(F-root, J-root, M-root)**

각각 한국 인터넷 진흥원 **, kt,** 한국 인터넷 연동센터에서 관리 **.**

Domain name

만드는 규칙

- Label 사이를 . 으로 구분하고 각 label 은 LDH rule 을 따름

  LDH rule : Letter(a~z, A~Z) Digit(0-9) Hyphen(-) 사용 가능

- 한 label 에 63 글자 , 127 번째 label 까지 가능

- hyphen 으로 시작 , 종료할 수 없음

- 대소문자 구분 없음

한국어로 만들고 싶다면 ..

Punycode 이용 (유니코드 문자열을 호스트 이름에서 허용된 문자로 인코딩)

접두어 xn-- 와 유니코드를 붙여서 만듦 ex) 한국 => xn--3e0b707e

Domain name

표기 방법 .

- FQDN(fully qualified domain name)

Root zone 에서 부터 시작하는 domain name.

ex) www.naver.com.

- PQDN(partially qualified domain name)

상위 도메인이 명확해서 알려줄 필요가 없는 경우에 사용

ex) naver.com

Domain name

이름으로 보는 계층 관계

ex) Www.sparcs.org.

=> .(root) > org.(gTLD) > sparcs. > www.(sub domain)

따라서 클라이언트가 www.sparcs.org. 를 열고 싶으면

1. local dns 서버에서 찾음 (/etc/host 에 저장)
2. 가까운 dns 에 없으면 root 네임서버로 문의
3. root 네임서버는 .org 를 보고 .org 가 등록된 네임서버에 문의

...

이런식으로 www.sparcs.org. 의 ip 주소를 얻는다 .

BIND(Berkeley Internet Name Domain)

BSD 기반의 **Unix** 시스템을 위해 설계된 **DNS software.**

서버와 resolver 라이브러리로 구성.

- DNS software 중 가장 많이 쓰임

1980 년대 초 **UC** 버클리 **4** 명의 대학원생이 처음 만들었고
ISC(internet system consortium) 에서 관리중**.**

2015 년 **12** 월 **bind 10** 출시

bind9 와 구분하기 위해 bundy 로 개명함

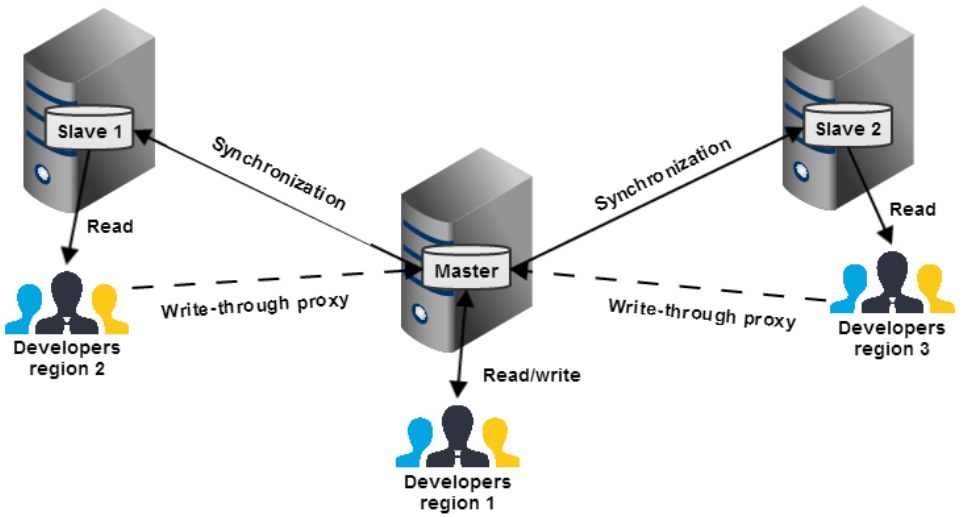
BIND -master, slave server

같은 내용인 여러개의 **DNS** 서버를 운영을 때, 한 서버를 **master** 로 지정하고 다른 서버들이 **master** 서버로 부터 데이터를 가져오도록 할 수 있음!

+ 영역에 따라 **master** 를 바꿔 줄 수 있다.

Secondary master

master 를 사용할 수 없게 될 경우 이 master 을 참조 할 수 있게 한다.



BIND 설치

sudo apt-get install bind9

실행 : **sudo /etc/init.d/bind9 start**

중지 : **sudo /etc/init.d/bind9 stop**

재실행 : **sudo /etc/init.d/bind9 restart**

BIND – nslookup(name server lookup)

apt-get install dnsutils

Domain name 을 입력하면 그 주소에 대한 **ip** 주소와 기타 정보 등을 알려줌

```
jaeyoung@jaeyoung-270E5J-2570EJ:~$ nslookup ara.sparcs.org
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   ara.sparcs.org
Address: 143.248.234.103
```

BIND - DIG(domain information groper)

DNS name server 에 질의하기 위한 네트워크 관리 명령 줄 인터페이스 툴

nslookup 보다 상세한 정보를 줌 **.**

Option : query type

any : all query soa : zone file 의 SOA 정보

a : network address hinfo : host 정보

mx : mail exchanger txt : txt

BIND - dig

dig [hostname] : hostname's zone 에서 발견된 **A record** 반환

dig [hostname] [record type] : hostname's zone 에서 발견된 이 **record type** 의 **record** 과 **record type** 의 **list** 출력

dig [hostname] +short : ip address 출력

dig @[nameserver address] [hostname] : ISP 의 결정자 대신 **name server** 를 직접 **query**

BIND -dig

dig [hostname] +trace : +trace 를 추가하면 **dig** 가 **root name server** 의 **query** 를 아래쪽으로 분석하고 각 **query** 단계의 결과를 보고 하도록 지시

dig -X [IP address] : ip 주소에 대한 역방향 조회

dig [hostname] any : host name 에 대한 모든 **record** 반환

WHOIS(등록을 해야만 알 수 있음)

Whois server 에서 **domain** 정보를 찾아주는 **software**

ex) whois naver.com

```
Domain Name:                            naver.com
Registry Domain ID:                     793803_DOMAIN_COM-VRSN
Registrar WHOIS Server:                 whois.gabia.com
Registrar URL:                          http://www.gabia.com
Updated Date:                           2016-05-03T10:46:58Z
Creation Date:                          1997-09-12T00:00:00Z
Registrar Registration Expiration Date: 2023-09-11T00:00:00Z
Registrar:                              Gabia, Inc.
Registrar IANA ID:                      244
Reseller:
Domain Status:                          ok https://icann.org/epp#ok
Registry Registrant ID:                 Not Available From Registry
Registrant Name:                        NAVER Corp.
Registrant Organization:                NAVER Corp.
Registrant Street:                      6 Buljung-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 463-867, Korea
Registrant City:                        Gyeonggi
Registrant State/Province:
Registrant Postal Code:                 463463
Registrant Country:                     KR
Registrant Phone:                       +82.215883829
Registrant Phone Ext:
Registrant Fax:                         +82.317841000
Registrant Fax Ext:
Registrant Email:                       white.4818@navercorp.com
Registry Admin ID:                      Not Available From Registry
Admin Name:                             NAVER Corp.
Admin Organization:
Admin Street:                           6 Buljung-ro, Bundang-gu, Seongnam-si, Gyeonggi-do, 463-867, Korea
Admin City:                             Gyeonggi
Admin State/Province:
Admin Postal Code:                      463463
Admin Country:                          KR
Admin Phone:                            +82.215883829
Admin Phone Ext:
Admin Fax:                              +82.317841000
Admin Fax Ext:
Admin Email:                            white.4818@navercorp.com
Registry Tech ID:                       Not Available From Registry
Tech Name:                              NAVER Corp.
Tech Organization:
```

domain 에 대한 정보가 아주 자세하게 나옴

+

등록자에 대한 정보도 나옴

BIND 설정 파일

- /etc/bind/db -

Zone file 의 RR 기록

- /etc/resolv.conf

local 의 name server 와 domain 설정

- /etc/bind/named.conf

Zone file 의 db 위치 설정

BIND 설정파일

/etc/host.conf => lp 를 찾을때 순서를 정해 주는 파일

Order : 붙여진순서대로 **dns** 를 찾음 **. host(local** 에서 **),** **bind(dns** 네임 서버에서 **), nis(** 네트워크 정보 서비스 **nis** **protocol** 에서 **)**

Multi => on/off. **on** 되어 있다면 **/etc/hosts** 에 둘 이상의 **ip** 주소를 등록하게 허용함 **.**

Alert => on/off. **on** 되어 있다면 **spoof** 시도가 **log** 되게 함 **.**

Nospoof => on/off. **spoof** 시도를 막지만 느려지게 함

Trim => domain name 을 인수 취급함

BIND 설정파일

/etc/resolv.conf

네임 서버에 쓸 **dns** 를 저장해둠

```
1 # Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(
2 #     DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
3 # 127.0.0.53 is the systemd-resolved stub resolver.
4 # run "systemd-resolve --status" to see details about the actual nameservers
5
6 nameserver 127.0.0.53
~
```

Domain [local domain]

Search [생략하고 싶은것 **]**

Nameserver [사용할 네임 서버 **]**를 추가하여 **PQDN** 으로 제작가능

BIND 설정파일

/etc/bind/db.~

Zone file 의 **RR type** 정보를 기록해둠 **.**

ex) /etc/bind/db.local(local 에 대한 정보 **)**

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@   IN  SOA localhost. root.localhost. (
                  2     ; Serial
             604800     ; Refresh
              86400     ; Retry
            2419200     ; Expire
             604800 )   ; Negative Cache TTL
;
@   IN  NS  localhost.
@   IN  A   127.0.0.1
@   IN  AAAA    ::1
```

BIND 설정 파일

/etc/bind/named.conf

=> zone file 의 db 위치, 타입 등 여러 정보들을 설정.

```
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

// prime the server with knowledge of the root servers
//zone "." {
//type hint;
//file "/etc/bind/db.root";
//};

logging {

channel "named_security" {
                file "/var/log/named_security.log" versions 3 size 100m;
                severity debug;
                print-category yes;
                print-severity yes;
                print-time yes;
        };

    category edns-disabled {    null;};
    category lame-servers { null;};
    category security { named_security; };
};

include "/etc/bind/sparcs.conf";
```

BIND 설정 파일

Zone file 등록 및 설정

zone“example.com”{

type [master or slave];

file [파일 위치 **];**

//slave 일 경우

// master{ [master 주소 **];};**

// allow-transfer{[secondary master 주소 **];};**

// 을 이용해서 **master** 설정 가능

};

BIND 설정 파일

모든 **dns query** 를 **query file** 로 보내주도록 **category** 설정

```
Logging {
   Channel query.log{
         File ~;
    };
    Category queries {query.log;};
};
```

BIND 설정 파일

```
 Author:      Jaeho Shin <netj@sparcs.kaist.ac.kr>
 Created:     2001/04/03
 vim:ft=named
*/

zone "SPARCS.ORG" in {
        type master;
        file "/etc/bind/db.SPARCS.ORG";
        notify yes;
//      also-notify {
//              143.248.234.114;
//              143.248.234.113;
//      };
};

key SPARCS.NET. {
        algorithm hmac-md5;
        secret "mL3TNGYhwUrl4asNYCaR/LirXMkByXOH9HAmmuGPRFU=";
};

zone "SPARCS.NET" in {
        type master;
        file "/etc/bind/db.SPARCS.NET";
        notify yes;
//      also-notify {
//              143.248.234.114;
//              143.248.234.113;
//      };
        allow-update {
                key SPARCS.NET.;
        };
};

//zone "kaist.ac.kr" in {
//      type slave;
//      file "/var/cache/bind/db.kaist.ac.kr";
//      masters {
//              143.248.1.177;
//              192.249.24.62;
//      };
//};
```

실습 하기

1. Ara, wiki, sparcs 만 입력해도 그 사이트의 네임 서버 정보를 알게 하기 **.**

```
moonde@34ba5439a9bc:~$ nslookup otl
Server:         143.248.1.177
Address:        143.248.1.177#53

Non-authoritative answer:
Name:   otl.sparcs.org
Address: 143.248.234.218

moonde@34ba5439a9bc:~$ nslookup ara
Server:         143.248.1.177
Address:        143.248.1.177#53

Non-authoritative answer:
Name:   ara.sparcs.org
Address: 143.248.234.103

moonde@34ba5439a9bc:~$ nslookup wiki
Server:         143.248.1.177
Address:        143.248.1.177#53

Non-authoritative answer:
Name:   wiki.sparcs.org
Address: 143.248.234.127
```

실습 하기

2. local 네임서버에 local 이외의 dns 를 만들고 (ip 는 임의) 그것의 zone file 에 자기 이름으로 된 dns 를 만들어 보자 .
두 개 모두 연결 되는지 확인해 보자 .

3. 방금 만든 dns 를 master 로 갖는 slave zonefile 만들어 보자 .

실습 하기

1.Local host 설정

```
1 127.0.0.1   localhost
2 123.123.123.123 aaa.com
3 ::1 localhost ip6-localhost ip6-loopback
4 fe00::0 ip6-localnet
5 ff00::0 ip6-mcastprefix
6 ff02::1 ip6-allnodes
7 ff02::2 ip6-allrouters
8 172.17.0.17 34ba5439a9bc
```

2.Zone file 정보 만들기

```
1 ;
2 ; BIND data file for local loopback interface
3 ;
4 $TTL    604800
5 @   IN  SOA aaa.com. root.aaa.com. (
6                   2     ; Serial
7              604800     ; Refresh
8               86400     ; Retry
9             2419200     ; Expire
10             604800 )   ; Negative Cache TTL
11 ;
12 @   IN  NS  ns.aaa.com.
13 @   IN  A   123.123.123.123
14 @   IN  AAAA    ::1
15 jaeyoung    IN  A   123.123.123.123
```

실습 하기

3. Zone 등록

```
//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "aaa.com" IN{
    type master;
    file "/etc/bind/db.aaa.com";
};
```

4. 다른 **zone** 을 **slave** 로 설정해서 **aaa.com** 의 **master** 을 만들겠다고 설정한다 **.**

5. dig 로 잘 되었는지 확인한다 **.**

참고 자료

Potato, onion, coffee 선배님들의 **wheel** 세미나 자료

http://www.tcpipguide.com/free/t_DNSMessageResourceRecordFieldFormats-2.htm

https://opentutorials.org/course/559/2802

https://help.dyn.com/how-to-use-binds-dig-tool/

http://linuxerhan.blogspot.kr/2007/06/linux-etchostconf.html

https://help.ubuntu.com/community/BIND9ServerHowto

https://www.facebook.com/dnssentry40/posts/190179177820203