DNS & BIND

potato, kis

DNS

Domain Name System

왜 DNS가 필요한가

- 특정 호스트에 접근하기 위해서는 IP주소가 필요하다.
- SPARCS 홈페이지에 들어가기 위해 ‘143.248.234.102’ 라는 IP를 외우기는 너무 힘들다.
- 그래도 사람말에 가까운 ‘sparcs.org’ 정도는 외울 수 있겠다.

-> ‘sparcs.org’ = ‘143.248.234.102’ 라고 컴퓨터한테 가르쳐 놓자.

왜 DNS가 필요한가

- 우리는 /etc/hosts 파일에 이 내용을 모두 기록해 두었다.

/etc/hosts

```
143.248.234.102 sparcs.org

202.179.177.22 www.naver.com

...
```

- 호스트의 개수가 많아지면서 대안이 필요해 졌다. -> DNS의 탄생

DNS란

- Domain Name System

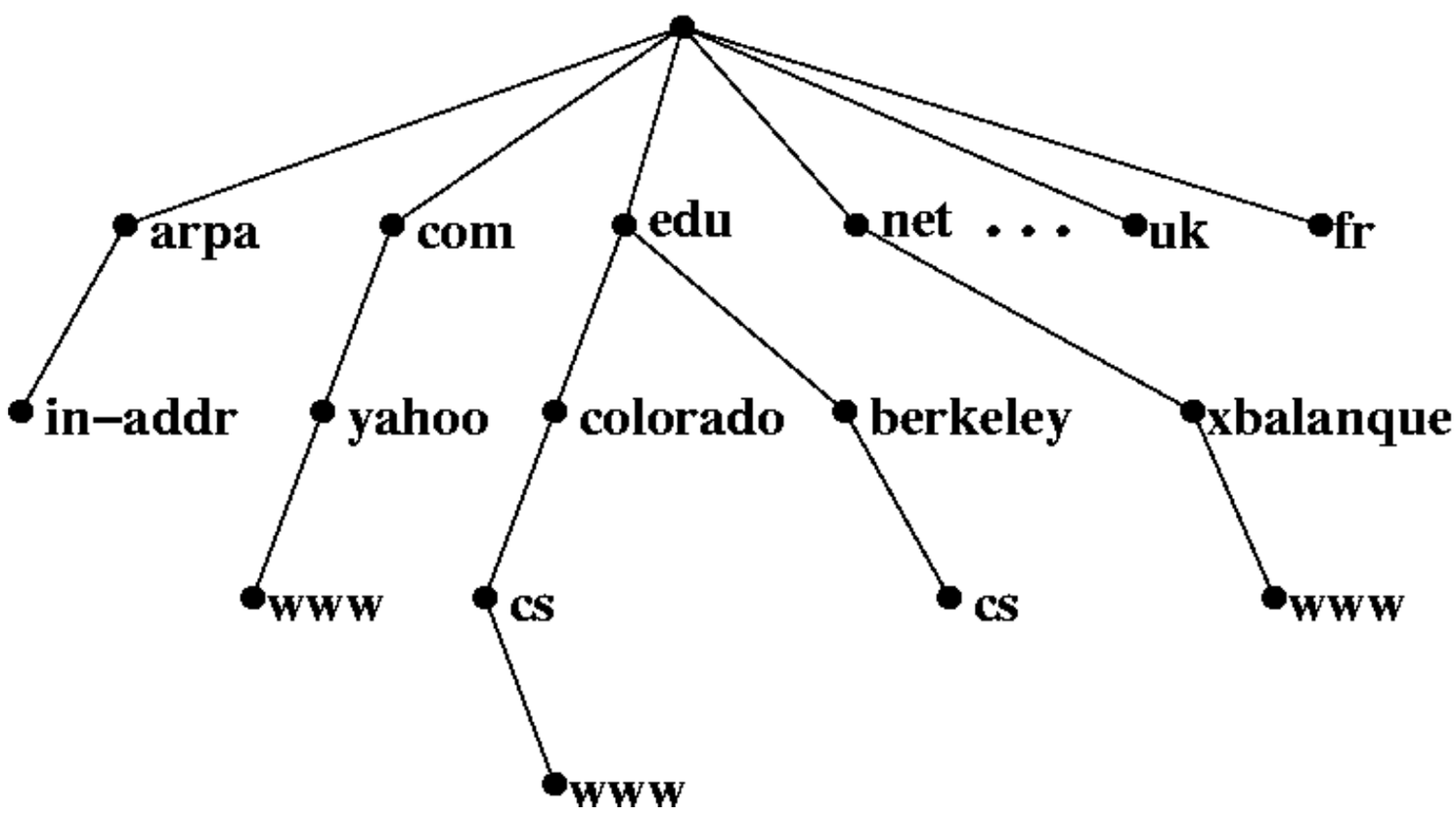
- 도메인 이름과 IP주소를 대응시키는 시스템

- **계층적** 구조를 갖는 **분산형** 데이터베이스이다.

계층적

- DNS는 ‘root zone’에서부터 시작하는 계층적인 구조를 갖고 있다.

  예) root zone -> .org -> sparcs.org -> ara.sparcs.org



분산형

- Domain Name System은 여러 개의 Domain Name Server로 이루어져 있다.

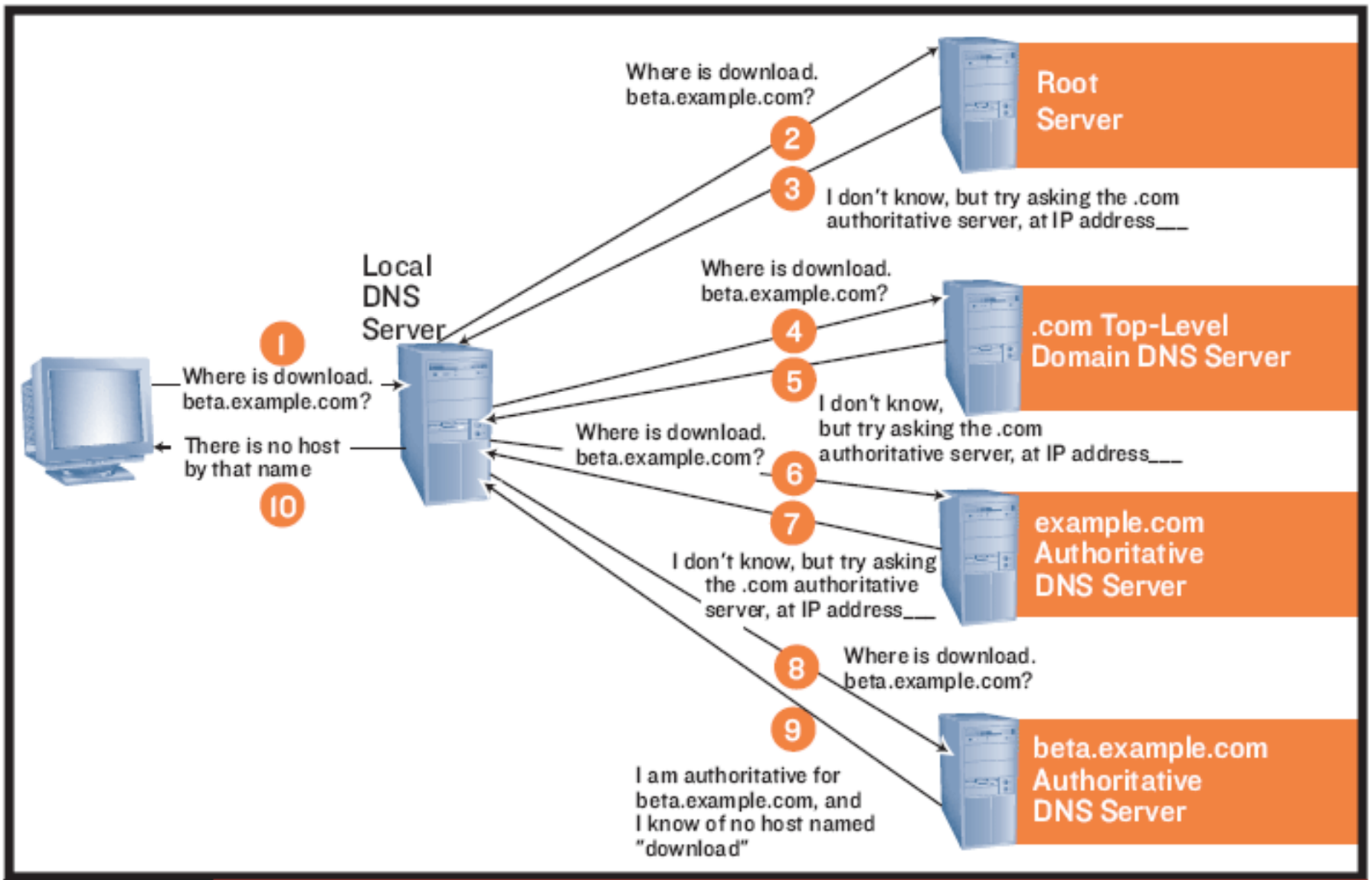
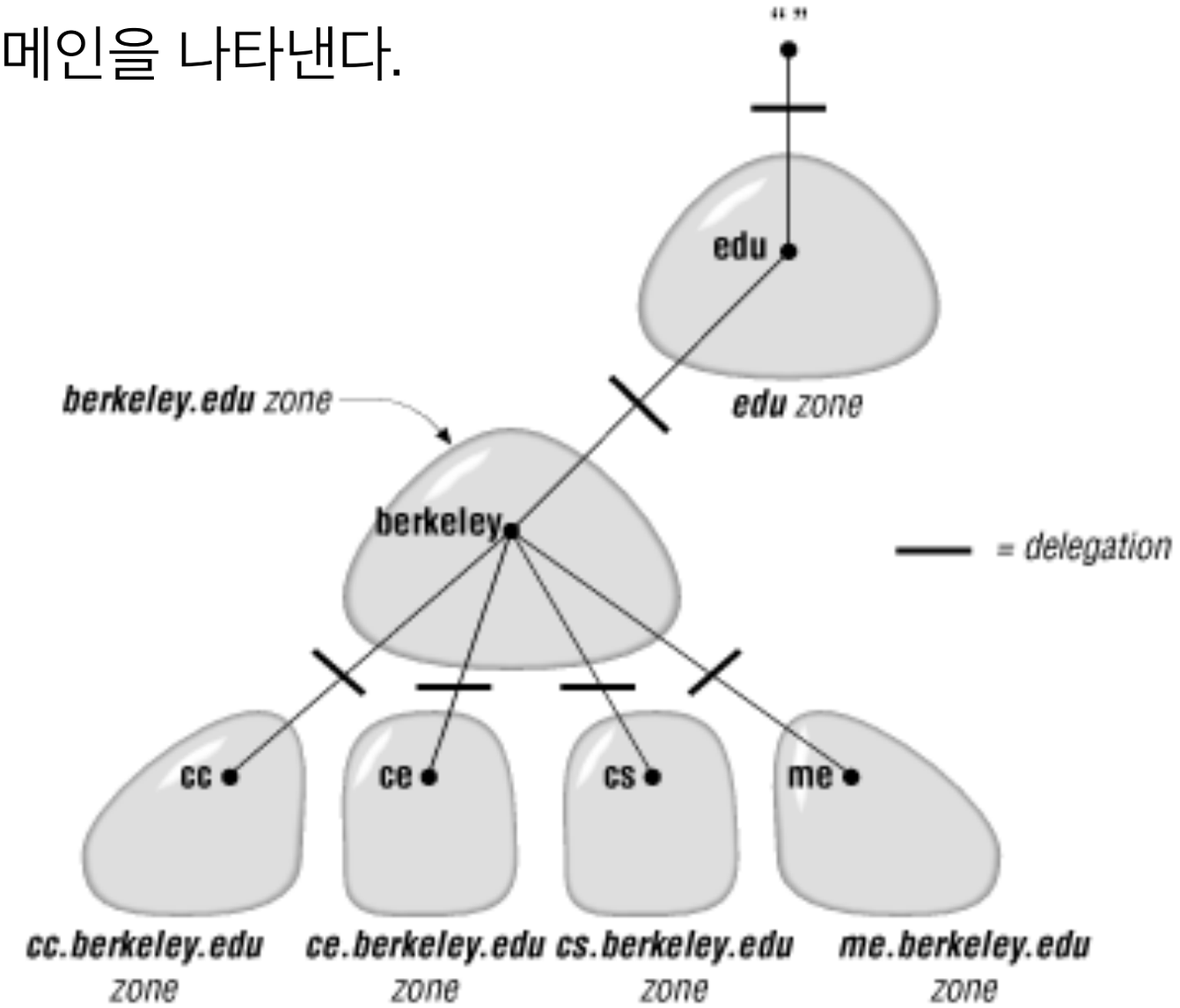


Figure 1: The standard DNS name-resolution process

Domain Name Sapce

- Domain Name으로 이루어진 계층적 트리 구조 자체이다.
- 각 노드는 도메인을 나타낸다.



DNS Zone

- 도메인의 관리자는 하위 도메인에 대한 권한을 갖는다.

  예) spars.org의 관리자는 ara.sparcs.org, otl.sparcs.org에 대한 권한이 있다.

- 이 권한의 영역을 DNS zone이라 한다.

- 하위 도메인의 DNS zone을 다른 관리자에게 위임할 수 있다.

  예) .org의 관리자는 하위 도메인인 sparcs.org에 대한 권한을 다른 사람에게 줄 수 있다.

Domain Name

예) ara.sparcs.org

- Domain Name Space 상에서 특정 노드에 해당한다.
- 각 label사이는 ‘ . ’으로 구분한다.
- 한 label에 63글자까지, 127번째 label까지, 총 253글자까지 가능하다.
- Domain Name에는 Letter(a~z,A~Z), Digit(0~9), Hyphen(-)을 사용할 수 있다. 이를 LDH Rule이라 한다.
- 대소문자의 구분은 없다.
- Domin Name은 Hyphen으로 시작할 수 없다.

다국어 Domain Name

- 퓨니코드(punycode)는 유니코드를 LDH rule에서 허용하는 문자만으로 인코딩 하는 방법이다.
- 이 퓨니코드를 사용해 유니코드에서 지원하는 모든 언어를 domain name으로 사용할 수 있다.
- 퓨니코드의 변환은 클라이언트에서 한다.
- 퓨니코드 문자열 앞에는 ‘xn--’를 덧붙인다.

  예) 한글.한국 = xn--bj0bj06e.xn--3e0b707e

Fully Qualified Domain Name (FQDN)

- root zone에서부터 시작하는 전체 domain name
- 마지막에 root domain을 뜻하는 null label을 붙인다.
- 따라서 ‘ . ’으로 끝나게 된다.

예) www.naver.com.

root zone . com . naver . www

Partailly Qualified Domain Name (PQDN)

- null label로 끝나지 않는 domain name
- 시스템 기본 도메인이 추가되어 해석되기도 한다.

  예) 시스템 기본 도메인이 kaist.ac.kr.일 경우

  ‘sparcs.org’는 ‘sparcs.org.’로 한 번 해석되고 그 다음에는
  ‘sparcs.org.kaist.ac.kr.’로 해석된다.

Name Server

- DNS 소프트웨어가 설치되어있는 서버를 Name Server라 한다.
- DNS 소프트웨어는 DNS database와 Resolver를 포함한다.
- Domain Name Space 중 권한을 위임받은 DNS zone에 해당하는 Database 를 갖고 있다.
- DNS 데이터는 Resource Record의 형태로 저장된다.

Resource Record (RR)

- Name Server가 갖고 있는 DNS 데이터를 Resource Record라 한다.

NAME	sequence of labels, variable length
TYPE	integer, 16 bits
CLASS	integer, 16 bits
TTL	integer, 32 bits
RDLENGTH	unsigned integer, 16 bits
RDATA	string of octets, variable length

- RR의 구성 요소 -

도메인 이름 – ‘sparcs.org’, ‘m.naver.com’ 등

정보의 유형 – ‘A’, ’NS’, ‘SOA’ 등

클래스 - 우리는 인터넷이라 ‘IN’

Time To Live – cache에 저장될 시간(초)

RData의 길이

Type에 따른 내용

RR의 Type

- RR에는 여러 종류의 데이터가 저장된다.

  A(Address) : 호스트의 IP주소 - IPv4

  AAAA : 호스트의 IP주소 - IPv6

  NS(Name Server) : 해당 도메인을 관장하는 name server

  SOA(Start of Authority) : zone의 정보를 표시

  ...

RR 예시

```
$ORIGIN example.com.
@    172800  IN      SOA
                        ns1.example.com.  hostmaster.example.com.
                        (
                            2003080800 ; se = serial number
                            12h        ; ref = refresh
                            15m        ; ret = update retry
                            3w         ; ex = expire
                            3h         ; min = minimum
                        )
     172800   IN      NS      ns1.example.com.
     172800   IN      MX  10  mail.example.net.
joe  172800   IN      A       192.168.254.3
www  172800   IN      CNAME   joe
```

Resolver

- Resolver는 프로그램의 request를 query로 변환해 Name Server에 보내고, 그에 대한 response를 프로그램에게 전달한다.

- 속도 향상을 위해 cache에 TTL동안 데이터를 저장해 놓는다.
- TTL값은 24시간에서 48시간 정도로 하는 것이 일반적이다.

BIND

Berkeley Internet Name Domain

BIND란

- Berkeley Internet Name Domain
- DNS를 구현한 프로그램이다.
- 최신 버전은 9.10.2-P2이다.
- 1980년대 초 UC Berkeley에서 4명의 대학원생에 의해 시작됐다.
- 공식 사이트 : http://www.isc.org/downloads/bind/

BIND 시작

- 설치 : `sudo apt-get install bind9`
- 시작 : `sudo /etc/init.d/bind9 start`
- 중지 : `sudo /etc/init.d/bind9 stop`
- 재시작 : `sudo /etc/init.d/bind9 restart`

BIND 설정 파일

- /etc/resolv.conf
  - 기본 name server와 기본 도메인을 설정한다.
- /etc/bind/named.conf
  - zone에 대한 정보와 db의 위치를 설정한다.
  - named.conf.default-zone, name.conf.loclal, named.conf.options
- /etc/bind/db.~
  - zone의 RR을 기록해 두고 있다.
  - db.local, db.root, db.~ …

dig 명령어

- 사용법 : `$ dig [@name server] domain`

예) `$ dig sparcs.org`

결과)

```
; <<>> DiG 9.7.3 <<>> sparcs.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 18772
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 4

;; QUESTION SECTION:
;sparcs.org.                    IN      A

;; ANSWER SECTION:
sparcs.org.             1919    IN      A       143.248.234.102

;; AUTHORITY SECTION:
sparcs.org.             1618    IN      NS      ns2.mazic.org.
sparcs.org.             1618    IN      NS      ns3.mazic.org.
sparcs.org.             1618    IN      NS      NS.sparcs.org.
sparcs.org.             1618    IN      NS      ns.mazic.org.

;; ADDITIONAL SECTION:
ns.mazic.org.           84418   IN      A       128.12.163.109
ns.sparcs.org.          84418   IN      A       143.248.234.102
ns2.mazic.org.          84418   IN      A       98.112.78.9
ns3.mazic.org.          63863   IN      A       98.112.78.9

;; Query time: 6 msec
;; SERVER: 168.126.63.1#53(168.126.63.1)
;; WHEN: Wed Jul  8 23:22:20 2015
;; MSG SIZE  rcvd: 187
```

BIND 실습 1

- ara.localhost.로 들어가면 ara.kaist.ac.kr(143.248.234.103)로 연결되게 만들어 보자.

1. /etc/bind/db.local을 수정한다. (sudo 필요)
2. db.local을 수정한 다음에는 bind9을 재시작해야 한다.
3. 확인은 dig 명령어로 한다.

BIND 실습 1

1. /etc/bind/db.local을 수정한다.

```
sudo vim /etc/bind/db.local
ara.localhost.    IN    A    143.248.234.103 - 추가
```

```
;
; 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
ara.localhost.  IN      A       143.248.234.103
```

BIND 실습 1

2. BIND를 재시작한다.

```
sudo /etc/init.d/bind9 restart
```

BIND 실습 1

3. dig 명령어로 확인한다.

```
dig @localhost ara.localhost
```

```
potato@wseminar4:/etc/bind$ dig @localhost ara.localhost

; <<>> DiG 9.7.3 <<>> @localhost ara.localhost
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30815
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; QUESTION SECTION:
;ara.localhost.                 IN      A

;; ANSWER SECTION:
ara.localhost.          604800  IN      A       143.248.234.103

;; AUTHORITY SECTION:
localhost.              604800  IN      NS      localhost.

;; ADDITIONAL SECTION:
localhost.              604800  IN      A       127.0.0.1
localhost.              604800  IN      AAAA    ::1

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Thu Jul  9 01:43:04 2015
;; MSG SIZE  rcvd: 105
```

BIND 실습 1

```
; <<>> DiG 9.7.3 <<>> @localhost ara.localhost
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8654
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; QUESTION SECTION:
;ara.localhost.         IN A

;; ANSWER SECTION:
ara.localhost.      604800  IN A  143.248.234.103

;; AUTHORITY SECTION:
localhost.      604800  IN NS localhost.

;; ADDITIONAL SECTION:
localhost.      604800  IN A  127.0.0.1
localhost.      604800  IN AAAA  ::1

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Jul  8 23:12:24 2015
;; MSG SIZE  rcvd: 105
```

nslookup 명령어

- dig 명령어는 도메인을 항상 FQDN으로 간주한다.
- PQDN의 도메인을 확인하려면 nslookup이라는 dig와 비슷한 역할을 하는 명령어를 사용하면 된다.
- 사용법 : `$ nslookup domain`

예) `$ nslookup sparcs.org`

```
potato@wseminar4:~$ nslookup sparcs.org
Server:         168.126.63.1                    <- DNS 서버
Address:        168.126.63.1#53

Non-authoritative answer:
Name:   sparcs.org                              <- 결과
Address: 143.248.234.102
```

BIND 실습 2

- ara로 들어가면 ara.kaist.ac.kr(143.248.234.103)로 연결되게 만들어 보자.

1. /etc/resolv.conf를 수정한다. (sudo 필요)

2. nslookup 명령어로 확인한다.

BIND 실습 2

1. /etc/resolv.conf를 수정한다. (sudo 필요)

```
sudo vi /etc/resolv.conf
```

```
search kaist.ac.kr.  -  추가
nameserver 168.126.63.1
```

BIND 실습 2

2. nslookup 명령어로 확인한다.

```
nslookup ara
```

```
potato@wseminar4:~$ nslookup ara
Server:         168.126.63.1
Address:        168.126.63.1#53

Non-authoritative answer:
Name:   ara.kaist.ac.kr
Address: 143.248.234.103
```