DNS
&
BIND

snow

DNS
&
BIND

DNS – What is DNS?

사람이 읽을 수 있는 도메인 이름

http://ara.kaist.ac.kr

상호 변환

실제 컴퓨터에서 쓰이는 IP 주소

143.248.234.103

DNS – What is DNS?

Domain Name System

↓

도메인 이름과 IP 주소를 매칭시키는 시스템

DNS – What is DNS?

Domain Name System

↓

도메인 이름과 Resource Record를 매칭시키는 시스템

DNS – What is DNS?

Resource Record Types

A	32-bit IPv4
AAAA (quad-A)	128-bit IPv6
CNAME	Canonical Name Record
MX	Message transfer agent

…etc.

DNS Zone File

Zone File

- Resource record를 나타내는 text file
- [name] [TTL] [class] [type] [data] 형식으로 구성된다

Name

- Record 이름 또는 소유자. Root 도메인 혹은 하위 도메인일 수 있음

TTL(Time to Live)

- 로컬에 저장된 레코드 사본이 업데이트 또는 삭제되어야 하는 빈도. 기본값은 1 시간

class

- 각 resource record 의 유형 집합. TCP/IP 의 class 는 IN(텍스트 코드) 혹은 1Data

type

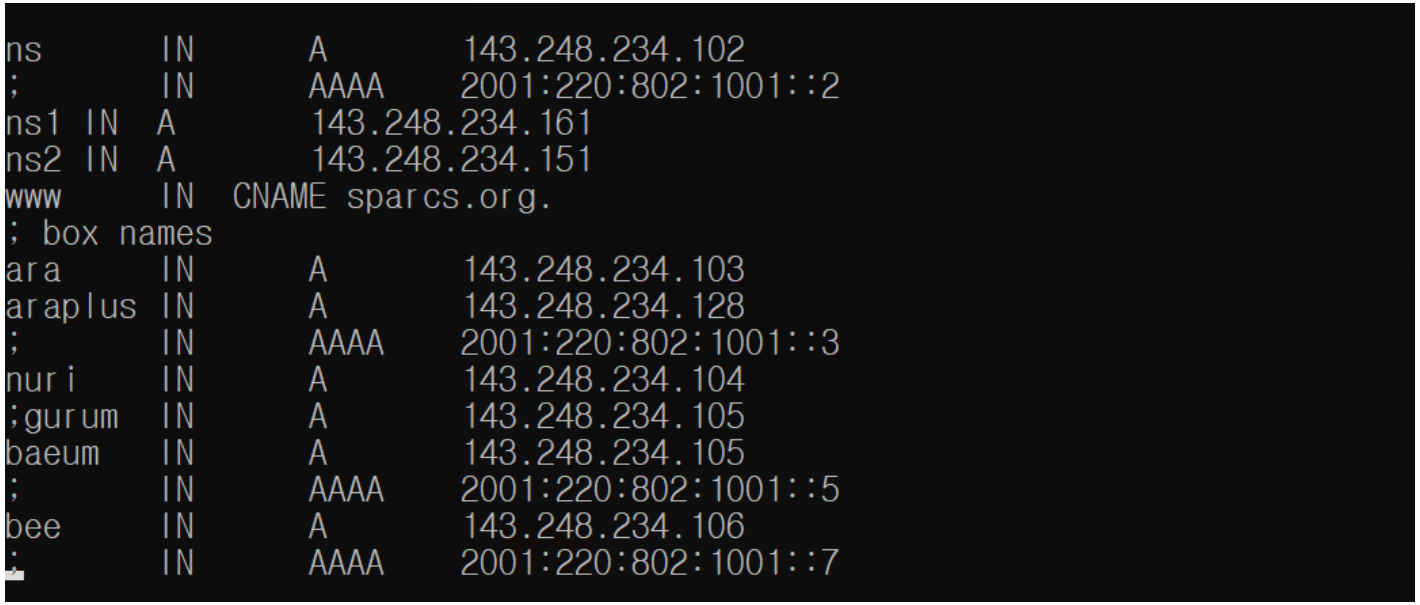
- 레코드의 유형 A, NS, CNAME, SOA

Data

- 레코드의 데이터로 레코드의 유형에 따라 다르다

DNS Zone File

/etc/bind 폴더 내에 zone file 들이 저장되어 있음



DNS Lookup

http://ara.kaist.ac.kr

↓

???

↓

143.248.234.103

DNS Lookup

http://ara.kaist.ac.kr

↓

Cache lookup

↓

143.248.234.103

DNS Lookup

http://ara.kaist.ac.kr

↓

Cache에 없다면?

↓

143.248.234.103

DNS Lookup

http://ara.kaist.ac.kr

↓

DNS Servers

↓

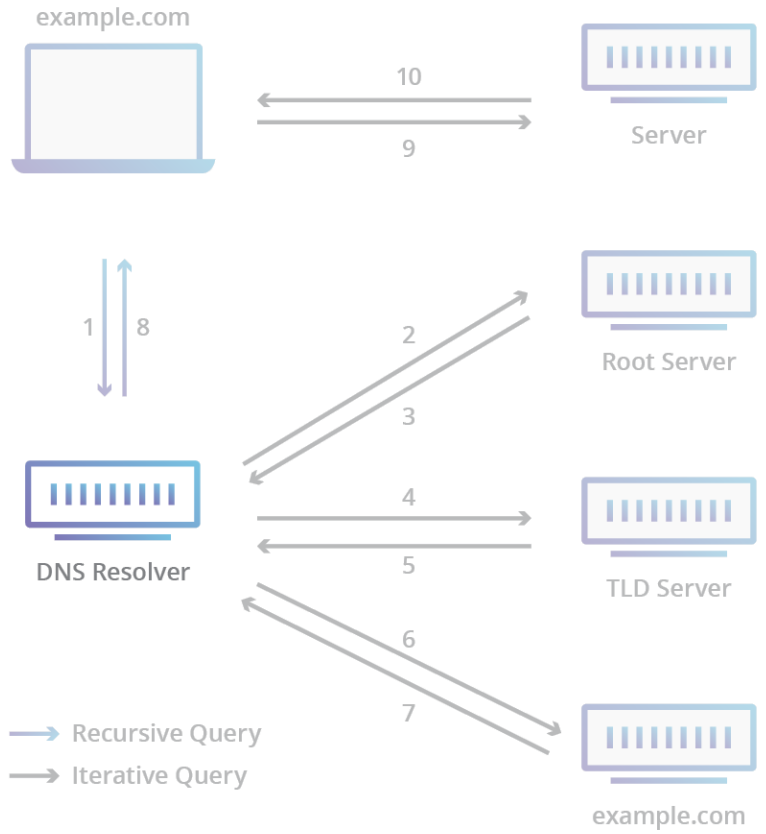
143.248.234.103

DNS Servers

1. DNS (Recursive) resolver

다른 DNS 서버들에게 query를 보낸 후 최종적으로 client에게 IP주소를 보내줌

Client와 직접 소통한다

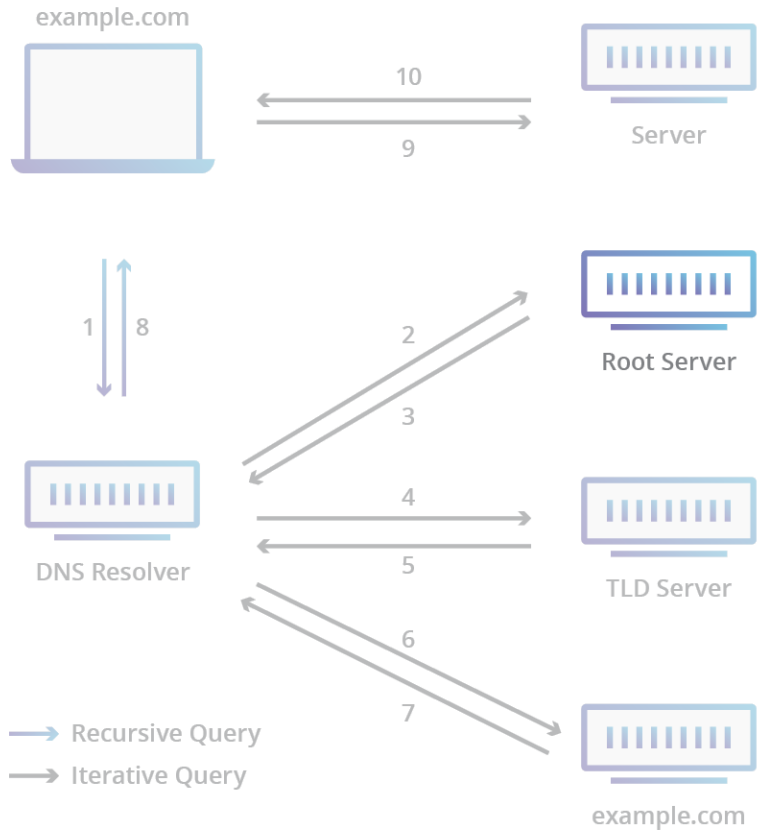


DNS Servers

2. Root Nameserver

전세계에 750+개의 Root 서버가 존재하지만, 단 13개의 IP주소를 통해 접속한다.

모든 DNS resolver 안에 이 13개의 IP주소들이 포함되어 있다.

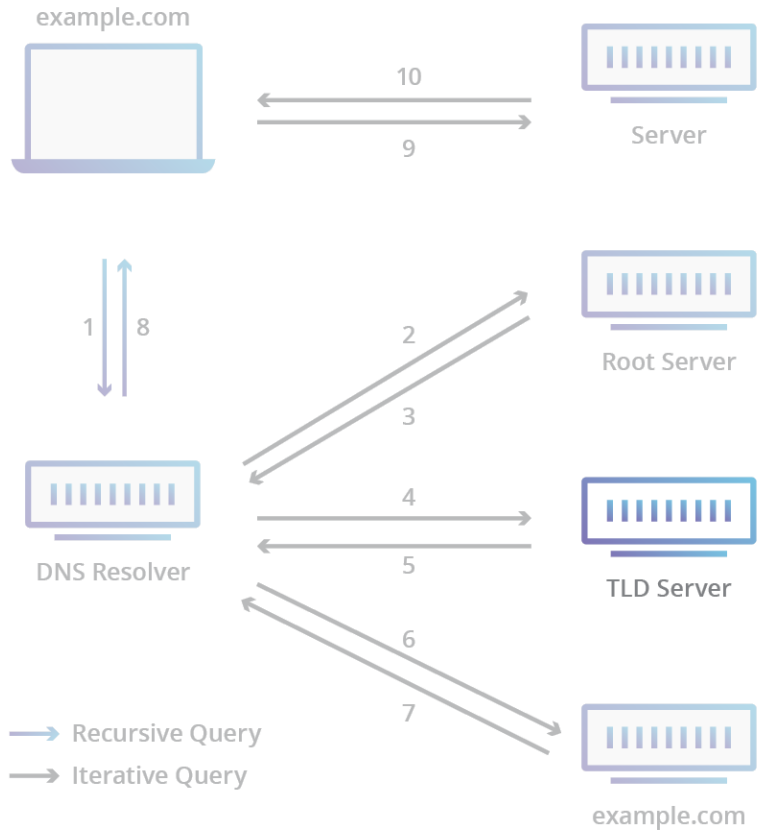


DNS Servers

3. Top Level Domain (TLD) Nameserver

하나의 domain name에 대한 정보를 가지고 있음

.com .org .kr



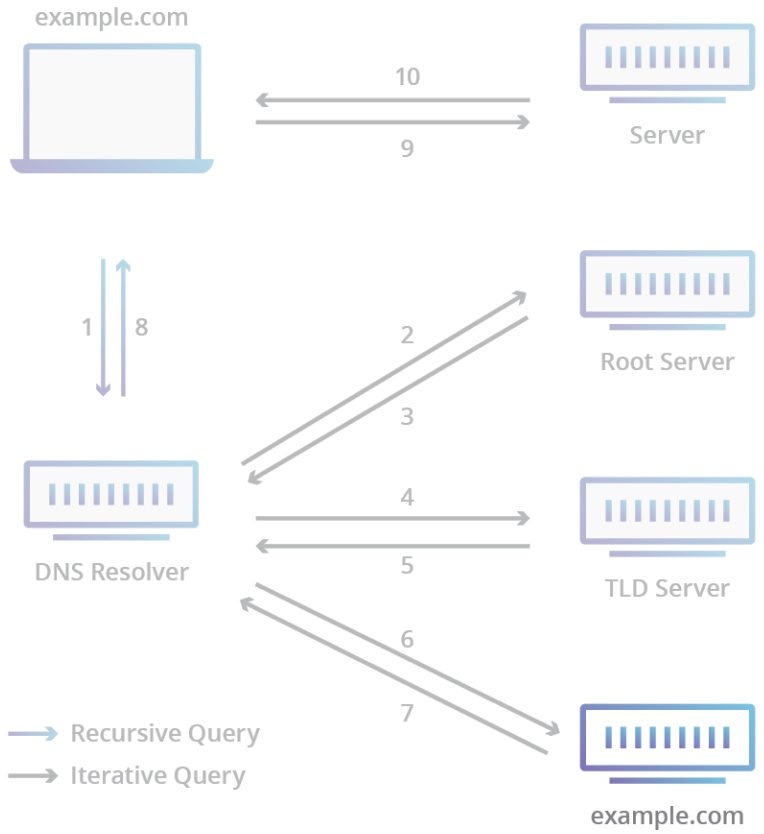
DNS Servers

4. Authoritative Nameserver

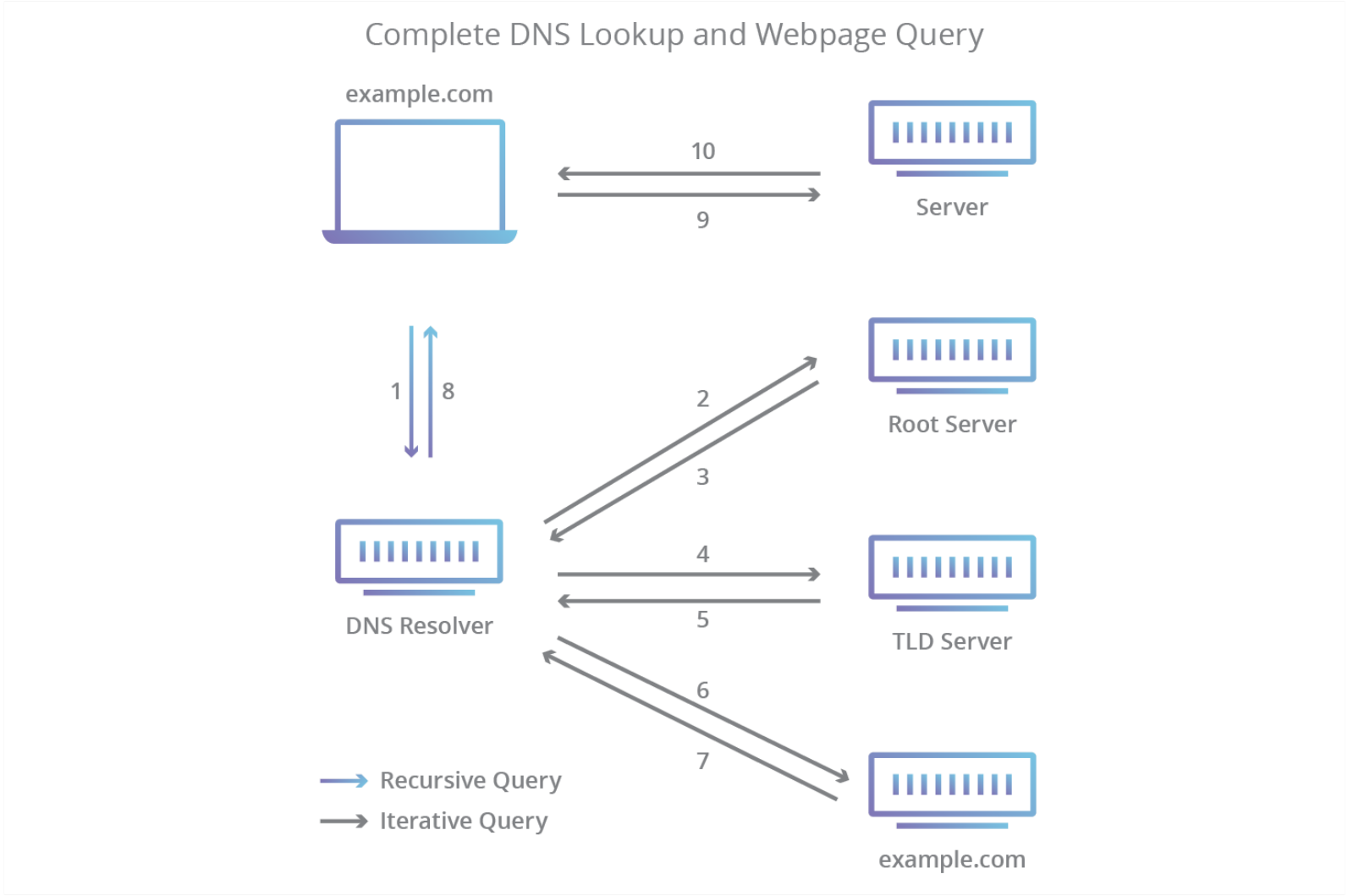
Resolver에게 해당 IP주소를 알려준다

google.com

ac.kr



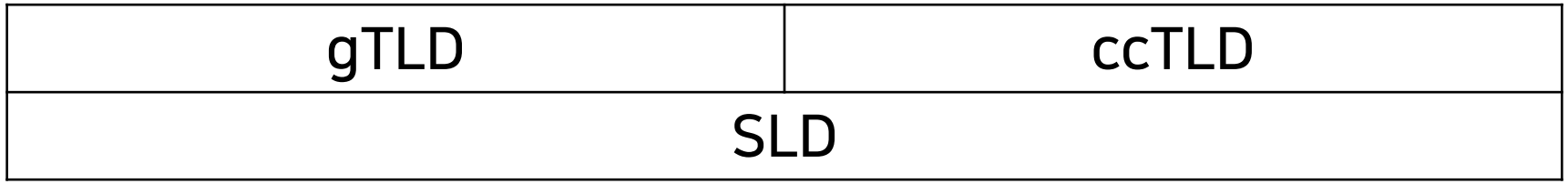
DNS Lookup Overview



Domain Naming System

Top Level Domain TLD

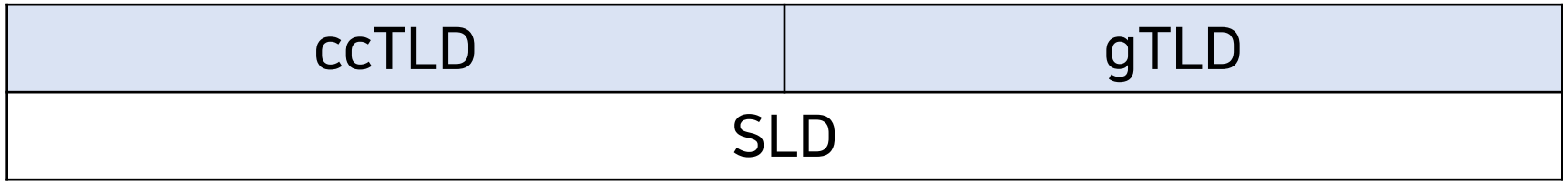
Second Level Domain SLD



Domain Naming System

Top Level Domain TLD

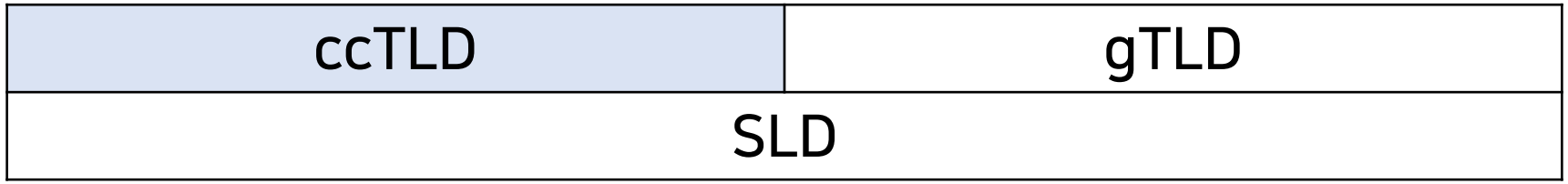
- Root 도메인계층의 하위에 해당하는 계층으로 1 단계 도메인으로도 불린다
- 국가에 할당된 도메인과 일반 도메인으로 크게 분류된다



Domain Naming System

Country Code Top Level Domain ccTLD

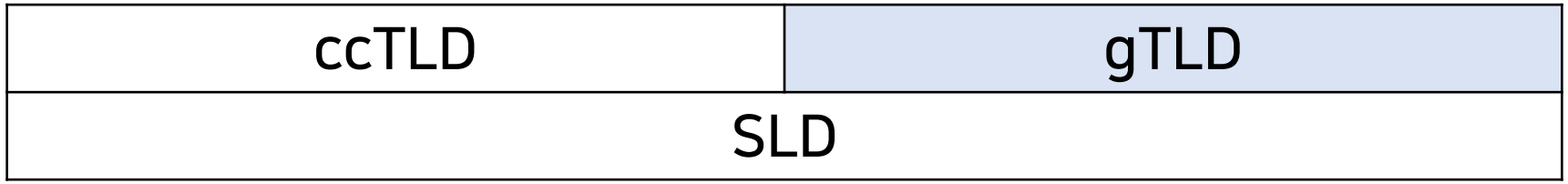
- 최상위 도메인 네임은 국가를 나타내며 , 하위 도메인들은 그 국가 조직의 성격을 나타내는 도메인 네임 레이블 상위 노드의 도메인 네임 을 사용
- .us .rus .cn .kr



Domain Naming System

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
- .com .gov .net



Domain Naming System

Second Level Domain SLD

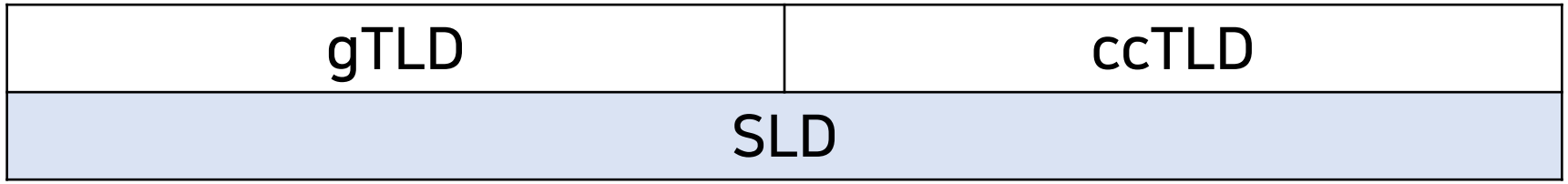
- 도메인을 등록하고자 하는 조직이나 국가에 속하는 기관으로 분류된다

상위 도메인이 gTLD 인 경우

- 조직이을 최종 사용자로 볼 수 있고, 원하는 호스트 네임 레이블을 도메인 네임으로 할당 받는다 .naver .kaist .google

상위 도메인이 ccTLD 인 경우

- 호스트와 조직의 성격을 나타내는 도메인이 위치한다 .ac.kr .co.kr



Domain Naming System

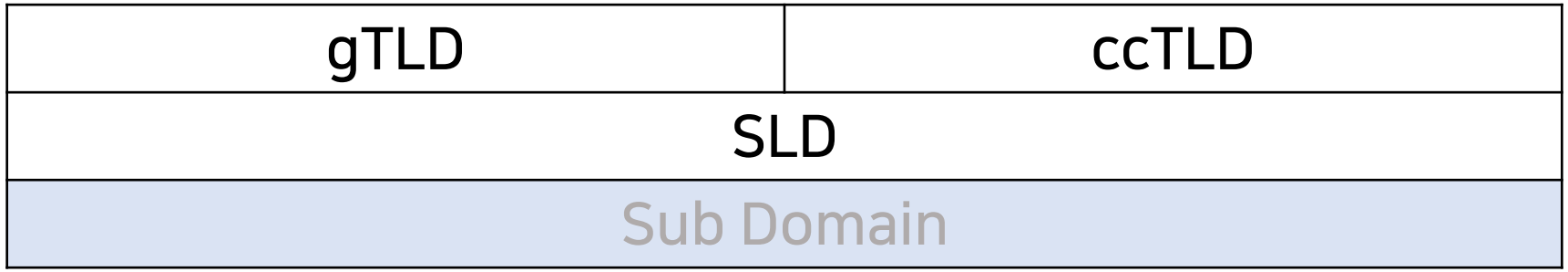
Sub Domain

상위 도메인이 gTLD 인 경우

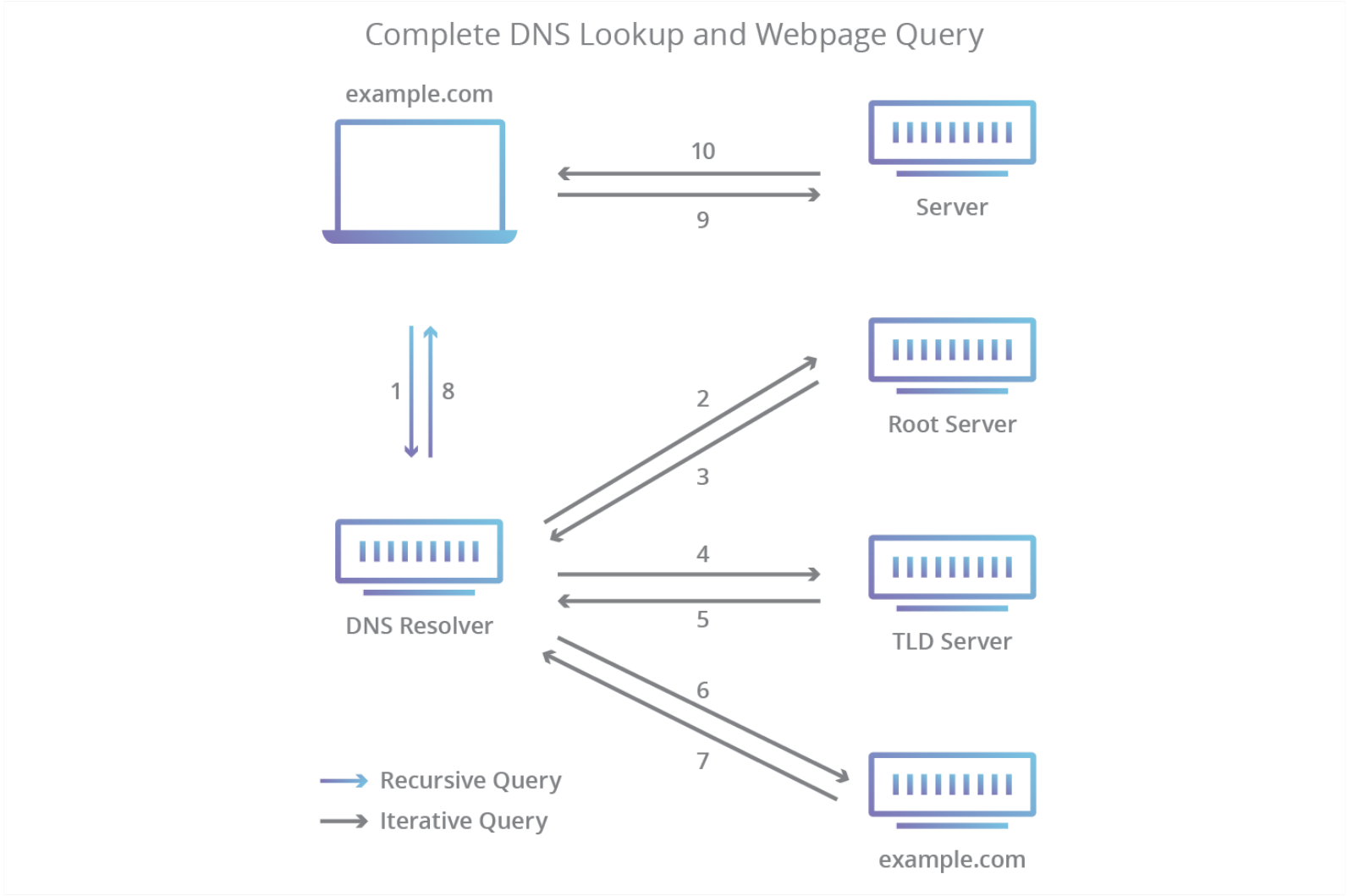
- 서브 도메인으로의 특성을 가진 도메인으로 최종 사용자가 필요에 따라서 만든 하위 도메인
- 여러 대의 Web Server 를 목적에 따라서 도메인을 구별하는 등의 목적으로 사용된다
  www.naver.com sports.naver.com

상위 도메인이 ccTLD 인 경우

- 3 단계 도메인의 특성을 가진 도메인으로 조직이나 개인에서 도메인을 등록 , 즉 최종 사용자의 도메인이 정의된다 google.co.kr kaist.ac.kr



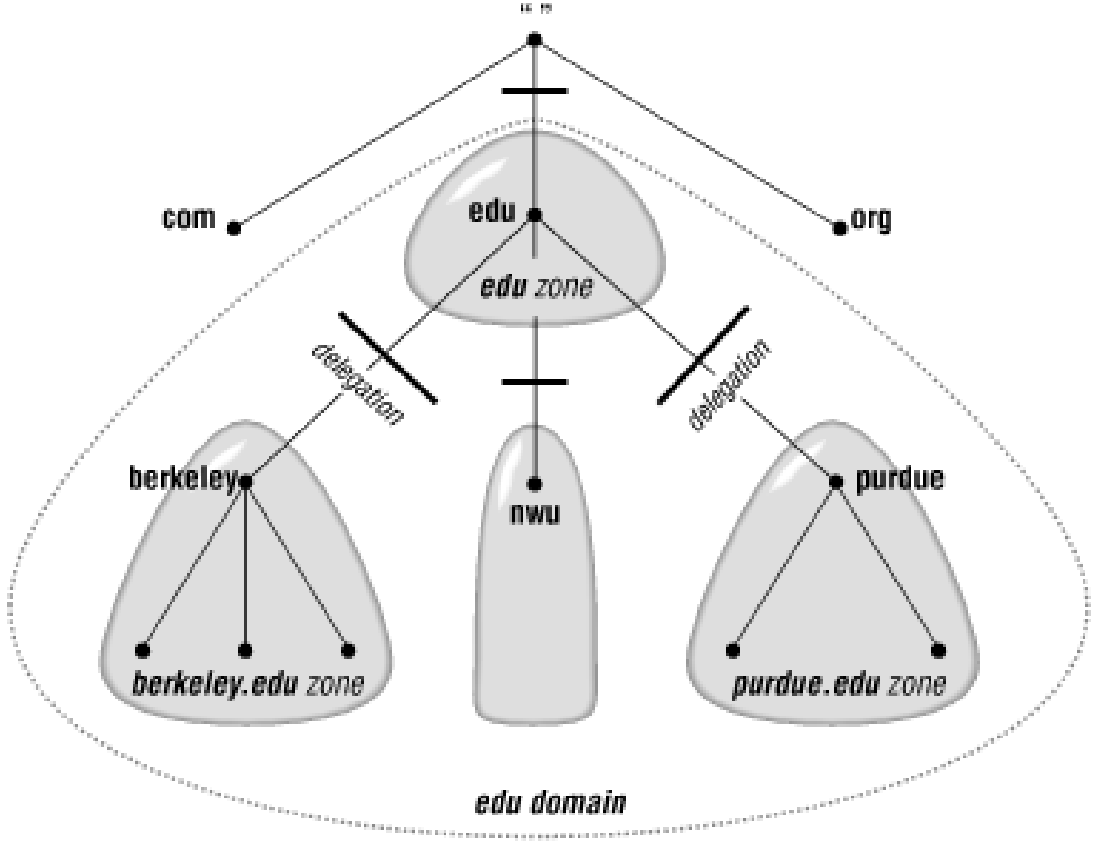
DNS Lookup Overview



DNS Zone

Zone

- Name Server 가 관리하는 영역



DNS Spoofing / DNS Cache Poisoning

DNS 서버로 보내는 질문을 가로채서

변조된 결과를 보내주는 것

DNS Spoofing / DNS Cache Poisoning

정상

http://ara.kaist.ac.kr

↓

Cache lookup

↓

143.248.234.103

Spoofing

http://ara.kaist.ac.kr

↓

Cache lookup

↓

???.???.???.???

겉보기로 유사하다는 점!

DNS
&
BIND

BIND

Berkeley Internet Name Domain

- BSD 기반의 UNIX 시스템을 위해 설계된 DNS 소프트웨어
- 1980 년대 초 UC Berkeley 대학원생 4 명이 모여서 만든 소프트웨어
- 현재까지 BIND 가 사실상의 standard DNS server
- BIND 9 버전이 사용되고 있다
- named (name daemon) 으로도 불린다

BIND 서버 명령

BIND 설치

```
sudo apt-get install bind9
```

BIND 실행

```
sudo service bind9 start
```

BIND 중지

```
sudo service bind9 stop
```

BIND 재실행

```
sudo service bind9 restart
```

BIND 서버 명령

BIND zone file 혹은 config file reload

```
sudo service bind9 reload
```

BIND 현 상황

```
sudo service bind9 status
```

BIND9 명령어

nslookup (name server lookup) DNS 정보 확인

```
nslookup [domain name]
```

Dig (domain information grouper)

nslookup 보다 상세한 정보를 여러 option 으로 설정 가능

```
dig [hostname]
dig [hostname][record type]
dig [hostname] +short
dig -X [IP address]
...
```

BIND9 설정 파일

/etc/host.conf ip 를 찾을 때 순서를 정해주는 파일

- order: 붙여진 순서대로 DNS 를 찾는다. host, bind, nis 를 사용할 수 있다
- multi: on/off. on 으로 etc /hosts 에 둘 이상의 ip 주소를 등록하게 허용할 수 있다
- alert: on/off. on 으로 spoof 시도가 log 되게 할 수 있다
- nospoof: on/off. on 으로 spoof 시도를 막지만 느려지게 된다
- trim: domain name 을 인수 취급하게 한다

BIND9 설정 파일

/etc/resolv.conf

- 네임 서버에 쓸 DNS를 저장해 둔다
- domain, search, nameserver 옵션을 이용하여 구현을 할 수 있다

/etc/bind/

- Zone file 의 Resource Record 정보를 기록해 둔다

/etc/named.conf

- Zone file 의 db 위치 , 타입에 관한 정보들을 설정한다

BIND9로 DNS 구축하기

- 서버에서 특정 client를 IP기반이 아닌 도메인으로 접근하기

IP: 112.113.114.115

hostname: example.com

BIND9로 DNS 구축하기

DNS 서버에 zone 생성

sudo nano /etc/bind/named.conf.local

```
zone "example.com" {
        type master;
        file "/etc/bind/db.example.com";
};
//reverse zone
zone "114.113.112.in-addr.arpa" {
        type master;
        file "/etc/bind/db.112";
};
```

BIND9로 DNS 구축하기

db.example.com 상세 설정 작성

sudo nano /etc/bind/db.example.com

```
$TTL    604800
@       IN      SOA     example.com.        root.example.com. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      example.com.
@       IN      A       112.113.114.115
@       IN      AAAA    ::1
```

BIND9로 DNS 구축하기

db.192 상세 설정 작성

sudo nano /etc/bind/db.192

```
$TTL    604800
@       IN      SOA     example.com. root.example.com. (
                              1         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      example.com.
115     IN      PTR     example.com.
```

BIND 서버 명령

작성한 설정 실행

```
sudo service bind9 reload
```

IP주소를 잘 받아오는지 확인

```
nslookup www.example.com
```

```
Server: 112.113.114.115
Address: 112.113.114.115#53

Name: www.example.com
Address: 112.113.114.115
```