

20장 DNS 서버

강사 김영석

A top-down view of a wooden desk. On the desk, there is a silver laptop with a black keyboard, a pair of black-rimmed glasses, a white coffee cup with a yellow handle, and a small green succulent in a dark pot. The word 'CONTENT' is written in large, white, sans-serif capital letters over the left side of the image.

CONTENT

- 1 DNS의 개요
- 2 도메인 이름 체계
- 3 로컬 DNS 서버 동작 과정
- 4 DNS 레코드의 종류
- 5 네임 서버 구축

1. DNS의 개요

- ❖ DNS는 Domain Name System 의 약자로 호스트의 도메인 이름을 호스트의 네트워크 주소로 바꾸거나 그 반대의 변환을 수행 할 수 있도록 하기 위해 개발되었다.
- ❖ 특정 컴퓨터의 주소를 찾기 위해서 사람이 이해 하기 쉬운 도메인 이름을 숫자로 된 IP 주소로 변환해 준다. DNS는 전화번호부와 비유된다. 예를 들면 주소창에 'www.test.com' 이라는 도메인 이름을 입력하면 10.100.0.101 과 같은 IP 주소로 변환하여 'www.test.com'의 웹 페이지를 보여 주게 된다.
- ❖ DNS 가 없던 시절에는 직접 IP 주소를 입력하여 웹 페이지에 접근했지만 관리를 위해 hosts 라는 파일을 사용하여 처리했다. 하지만 접근 했지만 지금은 많은 사이트가 존재하여 잘 사용하지 않는다.

2. 도메인 이름 체계

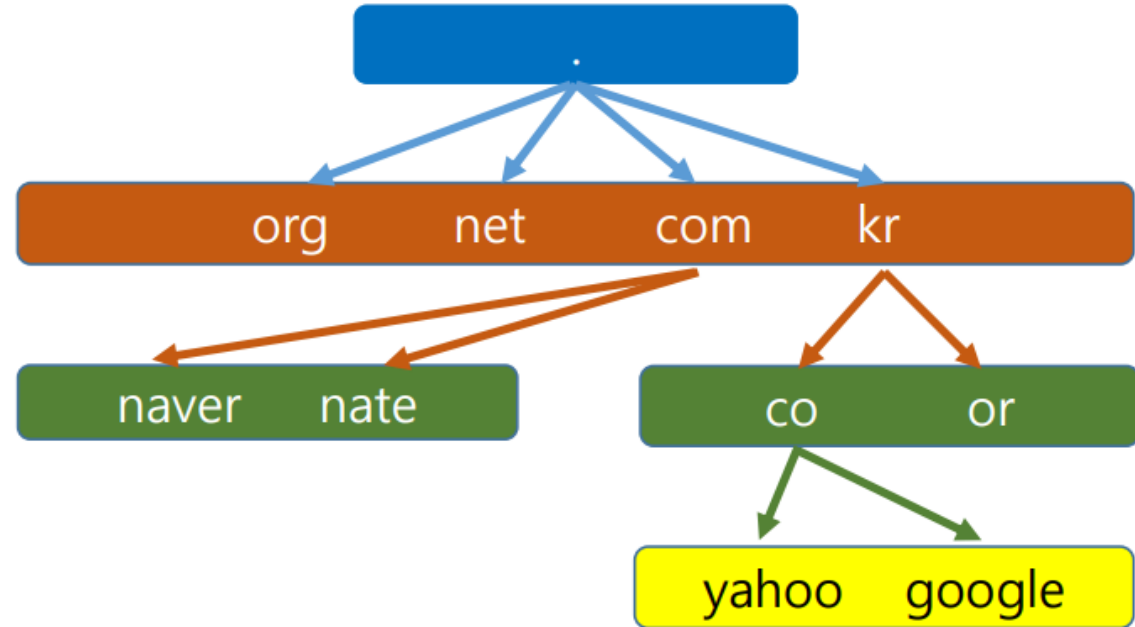
❖도메인 이름은 트리 구조로 체계를 고안했다.


루트 도메인 (Root Domain)

최상위 도메인 (Top Level Domain)

차상위 도메인 (Second Level Domain)

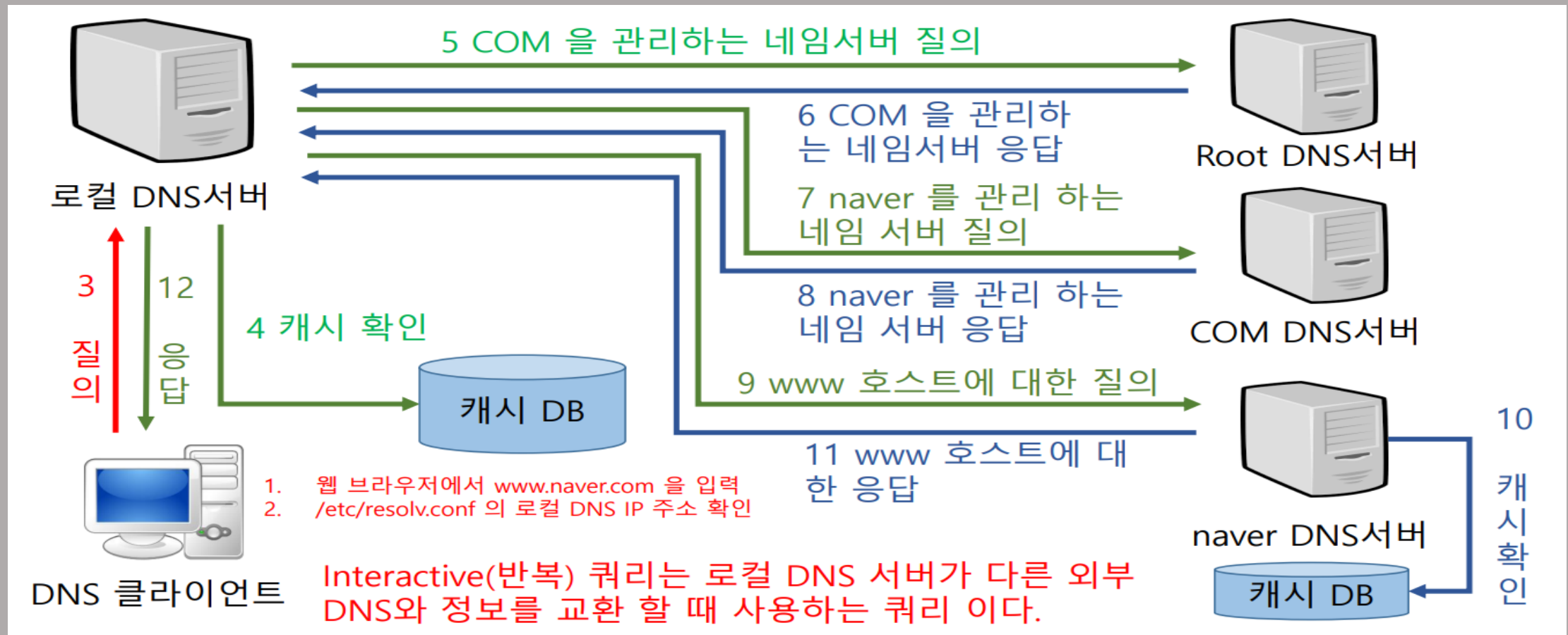
서브 도메인 (Sub Domain)



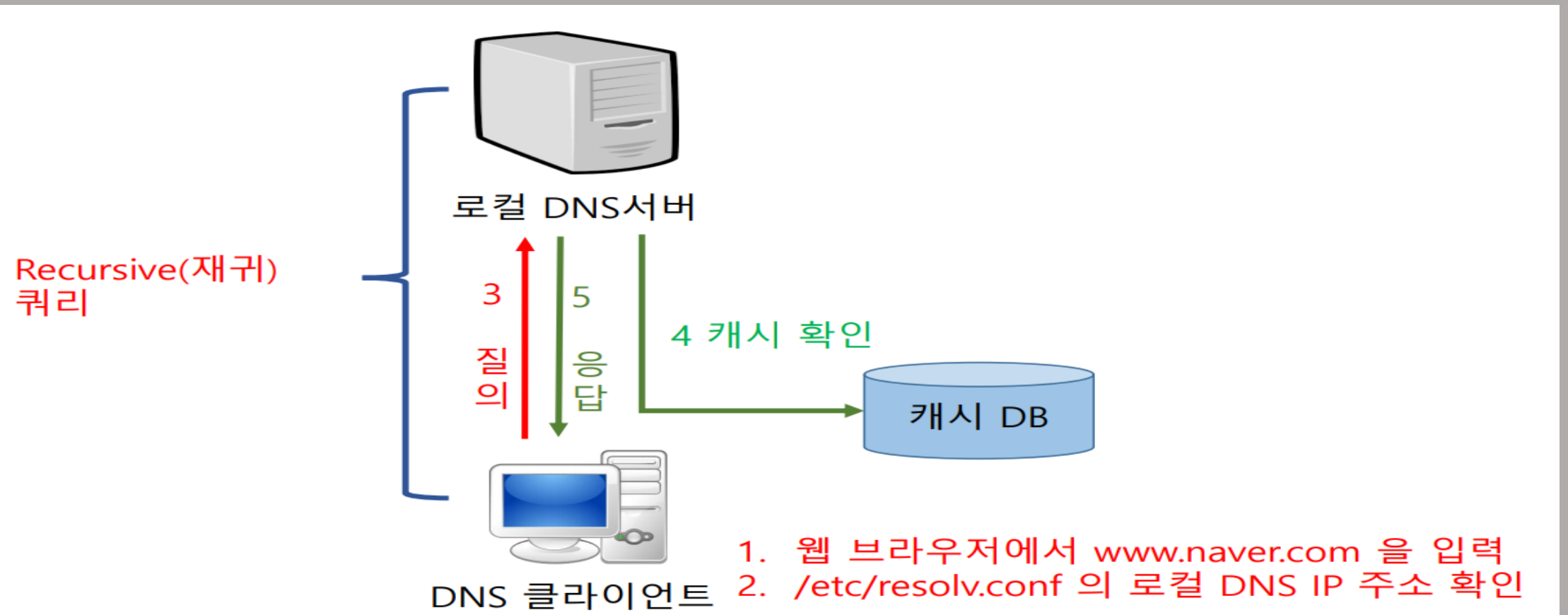
- 
- ❖ 일반적으로 도메인 이름의 등록과 관리는 NIC(Network Information Center)라는 곳에서 한다.
 - ❖ 한국은 KRNIC에서 kr 도메인을 관리하며, jp 도메인은 일본의 JPNIC에서 com, org, net, edu, gov 등은 미국 Network Solutions에서 관리한다. 국가 도메인 중에 국가 NIC가 있는 경우에는 각 국가의 NIC에서 도메인을 관리하지만 국가 NIC가 없는 경우 미국 interNIC에서 도메인을 대신 관리해 준다.

3. 로컬 DNS 서버 동작 과정

❖공용 DNS에 도메인 정보 요청 하기



❖ 로컬 DNS 에 도메인 정보 요청 하기



4. DNS 레코드의 종류


이름	설명
SOA (Start Of Authority)	DNS Zone의 기본 이름 식별 - 각 도메인의 영역 확인
A (Host Record)	호스트 이름이 정의된 주영역 (도메인 이름을 컴퓨터에서 사용하는 IP 주소를 매핑한다.)
CNAME (Alias Record)	별명(별칭) (기존의 도메인 이름을 다른 주 이름이나 정식 이름에 매핑한다.)
MX (Mail Exchange Record)	이메일 서버 지정 (메일 서버가 있는 도메인 이름과 컴퓨터를 매핑한다.)
SRV (Service Resources)	도메인에서 서비스 이용이 가능한지 식별
NS (Name Servers)	도메인의 모든 네임 서버 식별 - 각 네임 서버 안에 있는 도메인 확인
AAAA (IPv6 DNS Record)	IPv6 주소를 기준으로 하는 레코드 (A 레코드와 동일하지만 IPv4 와 IPv6로 매칭 주소의 차이가 있다.)
PTR (Pointer Resource Record)	IP 주소로 도메인 이름을 매칭하는 레코드 (역방향) (정방향은 DNS 도메인 이름을 가리키는 IP 주소를 매핑한다. 하지만 역방향은 반대가 된다.)

5. 네임 서버 구축

❖ DNS 패키지 설치

```
user1@Server1:~/바탕화면$ sudo apt-get install -y bind9
패키지 목록을 읽는 중입니다... 완료
의존성 트리를 만드는 중입니다... 완료
상태 정보를 읽는 중입니다... 완료
다음의 추가 패키지가 설치될 것입니다 :
  bind9-utils
제안하는 패키지:
  bind-doc resolvconf
다음 새 패키지를 설치할 것입니다:
```

```
user1@Server1:~$ ls /etc/bind
bind.keys  db.127  db.empty  named.conf          named.conf.local  rndc.key
db.0       db.255  db.local  named.conf.default-zones  named.conf.options  zones.rfc1918
```



```
user1@Server1:~$ sudo vi /etc/bind/named.conf.options
```

```
    dnssec-validation auto;  
    recursion yes;  
    allow-query { any; };  
    listen-on-v6 { any; };  
};  
:wq
```

```
user1@Server1:~/바탕화면$ sudo systemctl restart named
```

```
user1@Server1:~/바탕화면$ sudo systemctl status named
```

```
● named.service - BIND Domain Name Server
```

```
   Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset:▶
```

```
   Active: active (running) since Mon 2023-08-28 14:30:18 KST; 7s ago
```

```
   Docs: man:named(8)
```

```
user1@Server1:~/바탕화면$ sudo ufw allow 53
```

```
규칙이 업데이트됐습니다
```

```
규칙이 업데이트됐습니다(v6)
```

❖ 테스트 하기

```
user1@server2:~/바탕화면$ sudo vi /etc/resolv.conf  
[sudo] user1 암호:
```


```
nameserver 10.100.0.101  
options edns0 trust-ad  
search .  
~  
:wq
```

```
user1@server2:~/바탕화면$ nslookup  
> www.naver.com  
Server:          10.100.0.101  
Address:         10.100.0.101#53  
  
Non-authoritative answer:  
www.naver.com    canonical name = www.naver.com.nheos.com.  
Name:   www.naver.com.nheos.com  
Address: 223.130.200.107  
Name:   www.naver.com.nheos.com  
Address: 223.130.200.104
```

❖ 주 영역 네임 서버 구축 하기

```
user1@Server1:~/바탕화면$ cat /etc/bind/named.conf
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```



```
user1@Server1:~/바탕화면$ sudo vi /etc/bind/named.conf
[sudo] user1 암호:
```

```
zone "test.com" IN {
    type master;
    file "/etc/bind/test.com.db";
};
~
~
~
~
~
~
~
~
~
:~q
```

```
user1@Server1:~/바탕화면$ sudo named-checkconf
```



```
$TTL      604800      캐시를 저장하는 시간
@         IN          SOA      @ root. (
                                1          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
@         IN          NS       @
@         IN          A        10.100.0.101

www       IN          A        10.100.0.101
ftp       IN          A        10.100.0.101
```

```
user1@Server1:~/바탕화면$ sudo cp /etc/bind/db.0 /etc/bind/test.com.db
```

```
user1@Server1:~/바탕화면$ ls -l /etc/bind/test.com.db
-rw-r--r-- 1 root bind 237  8월 28 15:28 /etc/bind/test.com.db
user1@Server1:~/바탕화면$
user1@Server1:~/바탕화면$ sudo chmod 770 /etc/bind/test.com.db
user1@Server1:~/바탕화면$ sudo vi /etc/bind/test.com.db
```

```
; BIND reverse data file for broadcast zone
;
$TTL      604800
@         IN      SOA      @ root. (
                        1      ; Serial
                        604800  ; Refresh
                        86400   ; Retry
                        2419200  ; Expire
                        604800  ) ; Negative Cache TTL
;
@         IN      NS       @
@         IN      A        10.100.0.101

www       IN      A        10.100.0.101
ftp       IN      A        10.100.0.101
~
~
~
~
~
~
~
~
~
:wq
```

```
user1@Server1:~/바탕화면$ sudo systemctl restart named
```

❖ 테스트 해 보기

```
user1@Server1:~/바탕화면$ nslookup
> www.test.com
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   www.test.com
Address: 10.100.0.101
> ftp.test.com
Server:          127.0.0.53
Address:         127.0.0.53#53

Non-authoritative answer:
Name:   ftp.test.com
Address: 10.100.0.101
> exit
```

Quiz

❖ Server2 에 아래와 같이 실습 해 본다.

- DNS 서버를 설치 하고 DNS 설정을 Server2로 한다.
- nfs.test.com 으로 자신의 IP로 설정한다.
- ftp.test.com 으로 Server1로 설정한다.
- Server1의 DNS IP를 Server2 IP로 설정한다.
- NFS와 FTP 를 설정하고 Server1 에서 nfs.test.com 과 ftp.test.com 으로 연결 되는지 확인한다.

A photograph of a server room with rows of server racks on both sides of a central aisle. The racks have glass doors and internal components are visible, with many small blue lights glowing. The ceiling has several long, rectangular light fixtures. The overall atmosphere is dimly lit, emphasizing the blue light from the servers.

수고하셨습니다.