

DNS서버

DNS는 무엇인가요?

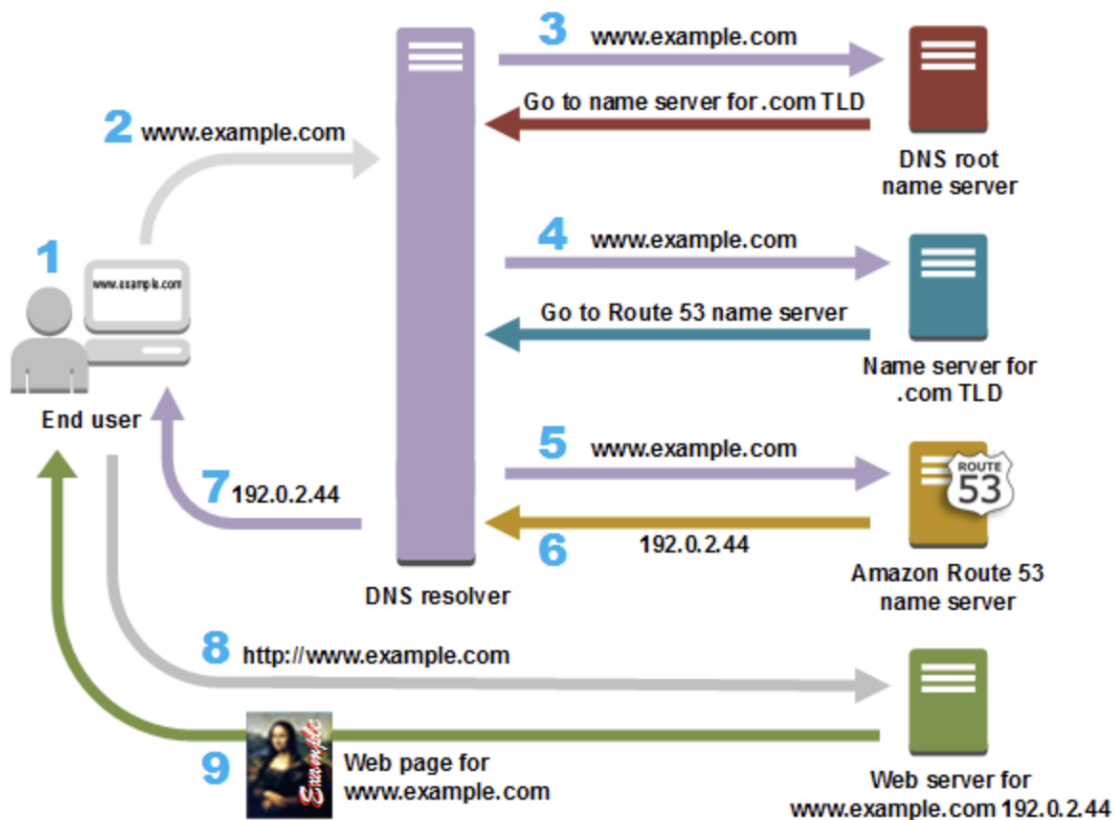
DNS(Domain Name System)은 사용자가 숫자로 된 인터넷 프로토콜 주소 대신 인터넷 도메인 이름과 검색 가능한 URL을 사용하여 웹사이트에 접속하는 것을 가능하게 한다.

사용자는

93.184.216.34와 같은 IP 주소를 기억하는 대신 *www.example.com*을 검색할 수 있다.

DNS는 어떻게 작용하나요?

DNS는 이처럼 상위 기관과 하위 기관과 같은 ‘계층 구조’를 가지는 **분산 데이터베이스 구조**를 가진다.



▼ DNS 과정

1. 사용자가 웹 브라우저를 열어 주소 표시줄에 `www.example.com`을 입력하고 Enter 키를 누릅니다.
2. `www.example.com`에 대한 요청은 일반적으로 케이블 인터넷 공급업체, DSL 광대역 공급업체 또는 기업 네트워크 같은 인터넷 서비스 제공업체(ISP)가 관리하는 DNS 해석기로 라우팅됩니다.
3. ISP의 DNS 해석기는 `www.example.com`에 대한 요청을 DNS 루트 이름 서버에 전달합니다.
4. ISP의 DNS 해석기는 `www.example.com`에 대한 요청을 이번에는 `.com` 도메인의 TLD 이름 서버 중 하나에 다시 전달합니다. `.com` 도메인의 이름 서버는 `example.com` 도메인과 연관된 4개의 Amazon Route 53 이름 서버의 이름을 사용하여 요청에 응답합니다.
5. ISP의 DNS 해석기는 Amazon Route 53 이름 서버 하나를 선택해 `www.example.com`에 대한 요청을 해당 이름 서버에 전달합니다.

6. Amazon Route 53 이름 서버는 example.com 호스팅 영역에서 www.example.com 레코드를 찾아 웹 서버의 IP 주소 192.0.2.44 등 연관된 값을 받고 이 IP 주소를 DNS 해석기로 반환합니다.
7. ISP의 DNS 해석기가 마침내 사용자에게 필요한 IP 주소를 확보하게 됩니다. 해석기는 이 값을 웹 브라우저로 반환합니다. 또한, DNS 해석기는 다음에 누군가가 example.com을 탐색할 때 좀 더 빠르게 응답할 수 있도록 사용자가 지정하는 일정 기간 example.com의 IP 주소를 캐싱(저장)합니다. 자세한 내용은 Time to Live(TTL)를 참조하세요.
8. 웹 브라우저는 DNS 해석기로부터 얻은 IP 주소로 www.example.com에 대한 요청을 전송합니다. 여기가 콘텐츠가 있는 곳으로, 예를 들어 웹 사이트 엔드포인트로 구성된 Amazon S3 버킷 또는 Amazon EC2 인스턴스에서 실행되는 웹 서버입니다.
9. 192.0.2.44에 있는 웹 서버 또는 그 밖의 리소스는 www.example.com의 웹 페이지를 웹 브라우저로 반환하고, 웹 브라우저는 이 페이지를 표시합니다.

웹브라우저는 resolver에게 아래와 같이 요청한다.

- 웹 브라우저 : www.treenod.kr의 IP 주소를 줘!

resolver는 최상위 기관에서 관리하는 Root DNS Server 에게 요청한다.

- resolver : 알겠어 기다려봐! 흠 저장된 캐시에는 없네,, 그럼 요청해야겠다! 야 Root DNS Server야 www.treenod.kr의 IP 주소 갖고 있어?

최상위 기관에서 관리하는 Root DNS Server는 응답한다.

- Root DNS Server : 야 내가 www.treenod.kr의 IP는 없고 대신 .kr 한국 국가 도메인 이라는 건 알아 냈어! .kr TLD DNS Server로 가서 한 번 물어봐.

resolver는 이제 .kr TLD DNS Server에게 요청한다.

- resolver : 야 www.treenod.kr IP 주소 있어?? 너한테 있다는데?

.kr TLD DNS Server는 응답한다.

- TLD DNS Server : 야 너가 찾는 www.treenod.kr IP 주소는 없고 내가 treenod.kr이 어디 있는지는 알아냈어! Authoritative DNS Server로 가봐

resolver는 이제 Authoritative DNS Server에게 요청한다.

- resolver : 야 야 www.treenod.kr IP 주소 있어??

Authoritative DNS Server는 응답한다.

- Authoritative DNS Server : 야 너가 찾는 거 여기 있다! 12.345.678.999야~

resolver는 이제 웹 브라우저에게 알려준다.

- resolver : 일단 캐시에 저장부터 하고~ 야 브라우저야 너가 찾는 www.treenod.kr IP 주소는 12.345.678.999이야~

네임 서버(Name Server = DNS Server)

문자열로 표현된 도메인 이름을 실제 컴퓨터가 통신할 때 사용하는 IP 주소로 변환시키기 위해서는 도메인 네임 스페이스의 트리 구조에 대한 정보가 필요한데 이러한 정보를 가지고 있는 서버를 네임 서버라고 한다.

일반적으로 데이터베이스 역할(저장, 관리), 찾아주는 역할, 요청 처리 응답 구현의 역할을 수행한다.

전 세계에 13개의 Root DNS 서버가 구축되어 있으며 이 네임 서버를 복사하여 같은 기능을 담당하는 미러서버가 존재한다.

네임 서버는 총 네 가지로 분류할 수 있다. 한 번 살펴보자.

1. Root DNS Server (<https://root-servers.org/>)

DNS 서버의 최상위 네임서버로 DNS 해석부터 발생한 DNS 요청에 대하여 적절한 TLD 네임서버 정보를 반환한다.

2. Top-Level Domain(TLD) DNS Server

도메인 등록 기관이 관리하는 서버로 Authoritative DNS 서버의 주소를 저장하고 안내하는 역할을 한다.

도메인 판매 업체(가비아 등)의 DNS 설정이 변경되면 도메인 등록 기관으로 전달되기 때문에 어떤 도메인이 어떤 판매업체(가비아 등)에서 구매했는지 알수 있다.

3. Second-Level Domain(SLD) DNS Server (Authoritative DNS Server)

| 실제 개인 도메인과 IP 주소의 관계가 기록(저장, 변경)되는 서버다.

그래서 권한의 의미인 Authoritative가 붙었으며 일반적으로 도메인/호스팅 업체의 네임서버를 말한다.

4. Anauthoritative DNS Server

| 권한이 없는 DNS 서버로 리졸버 서버, 리컬시브 서버, 리커서가 있다.

DNS 서버는 도메인 네임 스페이스를 위한 권한 있는 DNS 서버와 권한이 없는 DNS 서버로 구분된다.

위 1,2,3은 권한 있는 DNS 서버(Authoritative DNS Server)이다.

네임 스페이스를 위한 권한 있는 DNS 서버는 IP 주소와 도메인 이름을 매핑한다.

하지만 네임 스페이스를 위한 권한 없는 DNS 서버는 질의를 통해 IP 주소를 알아내거나 캐시한다(리졸버의 역할).

*사이트마다 resolver를 다르게 표현하고있다?

리졸버는 어떤 네임 서버에서 찾아야하는지, 이미 캐시 되어있는지 등을 찾아서 클라이언트에게 찾았으면 찾은 것을 못 찾았으면 못 찾았다고 전달하는 역할을 수행한다고 생각하면 됩니다.

대표적인 것이 KT, LG 유플러스, SK 브로드밴드와 같은 ISP(통신사) DNS 있고, 브라우저 우회 용도로 많이 쓰는 구글 DNS, 클라우드플레어와 같은 Public DNS 서버가 있습니다.

그래서 거의 Resolver = Recursive DNS Server = Local Server(of ISP) = Recursor 라고 생각하면 될 것 같다.

차이점

DNS Resolver

DNS Resolver는 일반적으로 사용자의 컴퓨터나 모바일 디바이스에 포함되어 있으며, 사용자가 도메인 이름을 입력하면 해당 Resolver는 DNS 쿼리를 생성하고, 이를 인터넷 상의 다른 DNS 서버에 전송한다.

Resolver는 일반적으로 캐시된 DNS 정보를 사용자의 컴퓨터나 모바일 디바이스에 저장하며, 이를 사용하여 DNS 쿼리를 처리한다.

즉, Resolver는 사용자의 컴퓨터와 DNS 서버 사이의 중개자 역할을 한다.

Local DNS Server

반면 Local DNS Server는 네트워크에서 사용되며, 일반적으로 기업, 학교, 공공기관 등에서 사용된다.

Local DNS Server는 네트워크 내에서 DNS 쿼리를 처리하고, 이를 인터넷 상의 다른 DNS 서버에 전달한다.

또한 Local DNS Server는 네트워크 내에 캐시된 DNS 정보를 저장하며, 이를 사용하여 **네트워크 내 모든 사용자의 DNS 쿼리**를 빠르게 처리할 수 있다.

성능 측면에서 Local DNS Server는 DNS Resolver 보다 더 높은 처리량을 처리할 수 있으며, 다양한 DNS 정보를 캐시하여 더 빠른 DNS 쿼리 응답을 제공한다.

DNS 레코드 타입

| A record

DNS의 레코드 타입중에 A record type이란 간단하게 도메인(domain) name에 IP Address를 매핑하는 방법이다

(A 레코드의 별칭은 AWS 리소스와의 통합을 위해 특별히 설계되었으며, 특정 AWS 리전의 리소스와 직접 연결할 수 있다)

| CNAME(Canonical Name)

Canonical Name의 줄임말로 하나의 도메인에 도메인 별칭을 부여하는 방식이다.

A record는 직접적으로 IP가 할당되어 있기 때문에 IP가 변경되면 직접적으로 도메인에 영향을 미치지만, CNAME은 도메인에 도메인이 매핑되어 있기 때문에 IP의 변경에 직접적인 영향을 받지 않는다.

SOA (Start of Authority)

- DNS 존에 대한 기본 정보를 제공하는 데 사용
- 하나의 SOA 레코드는 각 DNS 존에 대해 존재하며, 해당 존을 관리하는 주체에 대한 정보를 포함
- SOA 레코드에는 존의 소유자, 존의 메일 주소, 존의 현재 진행 중인 변경에 대한 일련 번호, 캐시된 레코드의 만료 시간 및 기타 중요한 타임아웃 값이 포함

NS (Name Server)

- DNS 존에 대한 네임 서버 정보를 제공
- NS 레코드는 특정 도메인에 대한 권한 있는 네임 서버의 호스트네임을 지정
- 존 내의 네임 서버들은 해당 존에 대한 DNS 쿼리에 응답하고, 다른 네임 서버들에 대한 정보를 제공
- 도메인의 NS 레코드는 일반적으로 도메인 등록 업체에서 구성되며, DNS 쿼리를 처리할 적절한 네임 서버를 식별



참고사이트

<https://aws.amazon.com/ko/route53/what-is-dns/>

<https://velog.io/@zinukk/9kpyzbdtd#:~:text=Resolver>는 일반적으로 하나,를 처리할 수 있다.