14 DNS

쉽게 배우는 데이터 통신과 컴퓨터 네트워크

학습목표

- ✓ 도메인 이름과 IP 주소를 변환하는 과정이 필요한 이유를 이해
- ✓ 계층 구조의 네임 스페이스, 도메인, 존 개념을 이해
- ✓ 도메인 정보를 관리하기 위한 자원 레코드
- ✓ 이름 관리를 위한 해석기와 네임 서버의 동작 원리를 이해
- ✓ DNS 클라이언트와 서버가 전송하는 DNS 메시지 구조

3절. 네임 서버와 해석기

- 인터넷에서 여러 네임 서버가 유기적으로 동작하여 정보의 일관성 유지

□ 해석기

- 도메인 이름과 호스트 주소 정보를 원하는 응용 프로그램은 해석기에게 요청
- 해석기는 DNS 서버와 접촉하는 DNS 클라이언트 역할을 수행

▪ 인증 데이터(Authoritative Data)

➔ 해당 데이터를 직접 관리할 책임이 있는 네임 서버로부터 받은 정보

- 도메인 이름과 관련된 IP 주소를 얻는 과정
  - 해석기가 DNS 메시지 형식의 질의를 생성
  - 이 질의를 네임 서버에게 전달
  - 네임 서버는 회신용 DNS 메시지에 결과를 담아 해석기에 회신

- 네임 서버의 부담을 줄이기 위하여 캐시 정보 활용
  - 캐시 데이터: 이전 요청에 의하여 호스트가 보관하던 정보

    (TTL 정보를 이용하여 캐시에 너무 오래 머무르지 않도록 함)

3절. 네임 서버와 해석기

□ 요청의 처리

- 호스트 A가 호스트 B의 정보를 원할 때, 호스트 A, B 가
  - 같은 도메인에 위치하면 이 도메인의 네임 서버가 인증 데이터를 회신
  - 다른 도메인에 위치하면 인근 네임 서버와 요청 호스트(A)를 중개해 줌

- 인근 네임 서버를 찾는 작업은 인증 정보를 찾을 때까지 반복됨

- 질의 요청이 처리되는 과정
  - 인증 데이터가 반드시 필요한지 명시할 수 있음

    혹은 캐시 데이터도 괜찮은지?
  - 해석기는 질의 요청을 재귀적으로 처리할 수 있음

    혹은 비재귀적으로 처리할지?

3절. 네임 서버와 해석기

□ 요청의 처리

- **재귀적 요청 [그림 14-8]**
  - 해석기가 최초로 접속을 시도한 네임 서버가 질의 요청을 추적, 관리
  - 재귀적 요청을 받은 네임 서버가 결과적으로 해석기 역할을 수행
  - 비재귀적: 요청을 받은 네임 서버가 인증 데이터가 있으면 바로 보내고 그렇지 않으면 다른 네임 서버와 직접 접촉하여 정보를 얻음

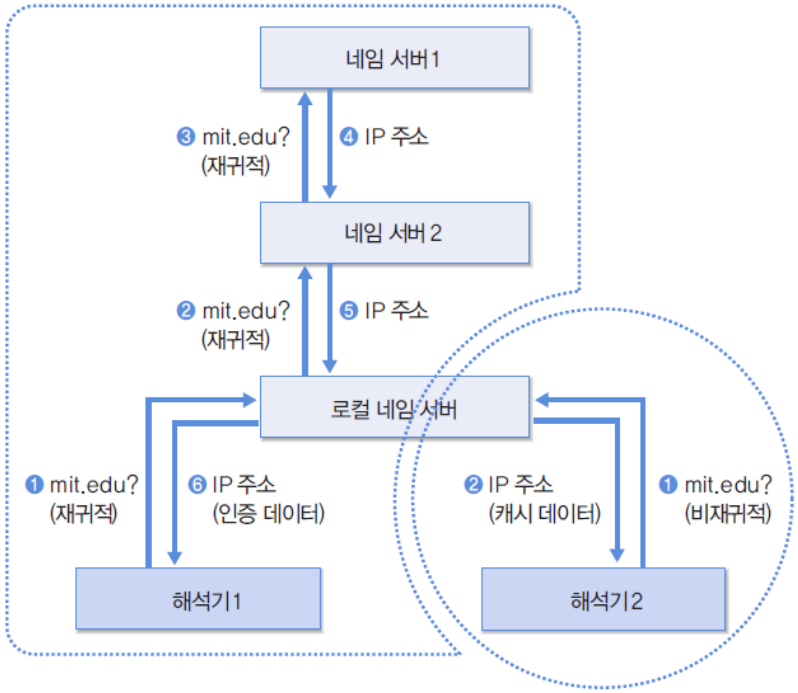


그림 14-8 재귀적 처리와 비재귀적 처리

3절. 네임 서버와 해석기

요청의 처리

- **반복적 처리**
  - **로컬 네임 서버 1이 다른 네임 서버 들과 직접 접촉**

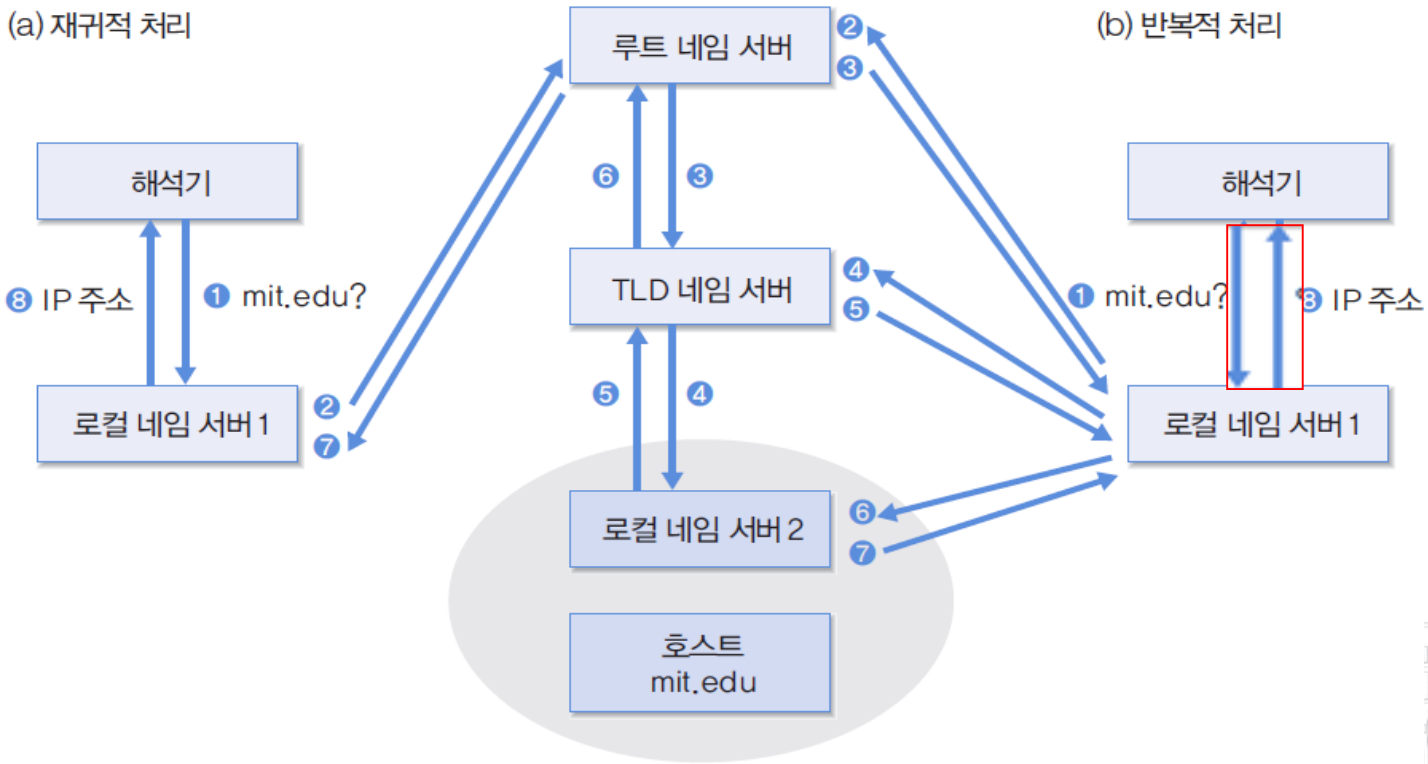


그림 14-9 재귀적 처리와 반복적 처리

4절. DNS 프로토콜

DNS 메시지

- DNS 데이터를 요청하거나 응답할 때 DNS 메시지를 전송

DNS 메시지 [그림 15-9]

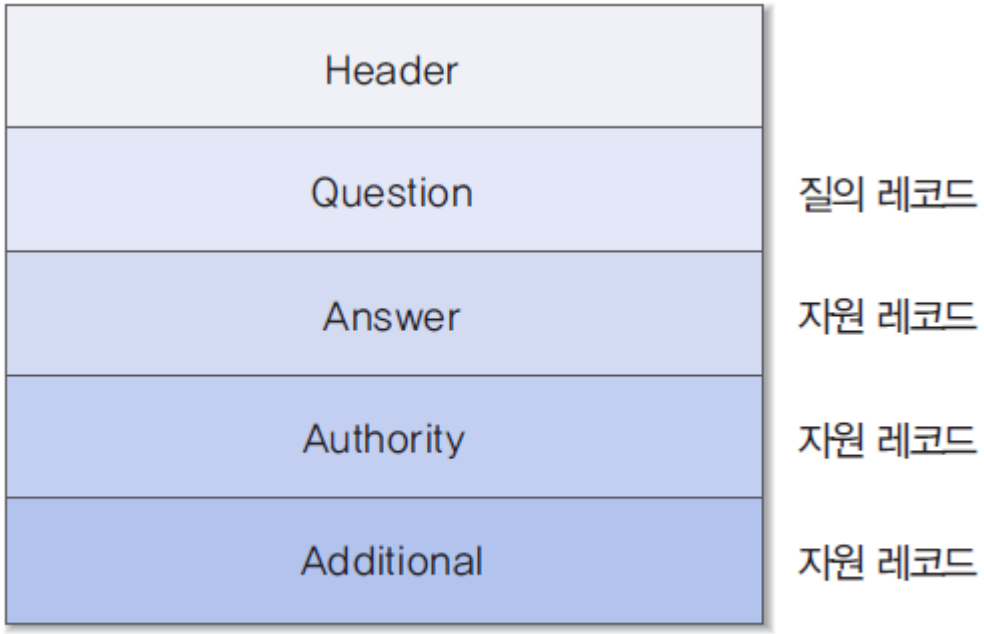


그림 14-10 DNS 메시지의 구조

4절. DNS 프로토콜

DNS 메시지

DNS 메시지

- **Header**
  - 헤더 값에 따라 다른 필드의 사용 여부 결정
- **Question**
  - 질의 메시지, 응답 메시지 모두 사용
  - 네임 서버에 요청하는 문의 사항
  - 질의 레코드 사용
- **Answer: 질문에 대한 결과**
- **Authority: 인증 권한 서버 정보**
- **Additional: 기타 정보**

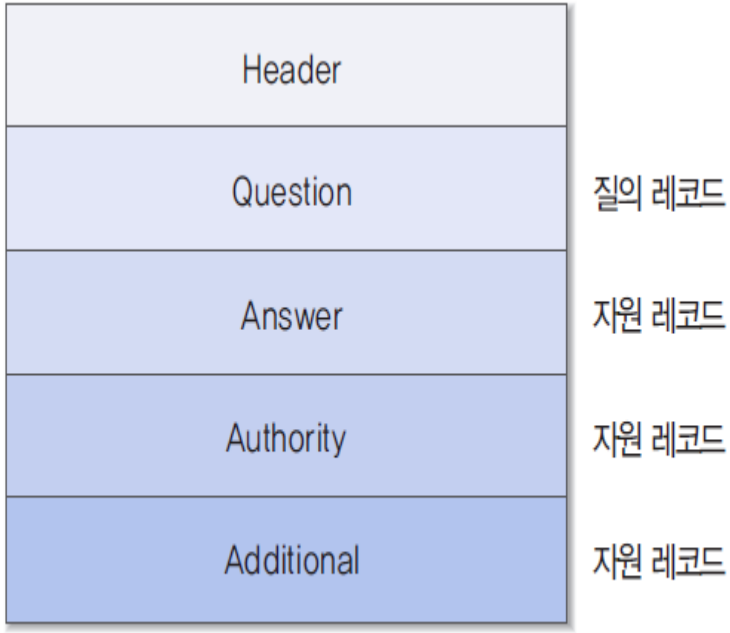


그림 14-10 DNS 메시지의 구조

DNS 메시지

- **DNS 헤더의 구조 [그림 15-10] : 96비트 =12바이트**

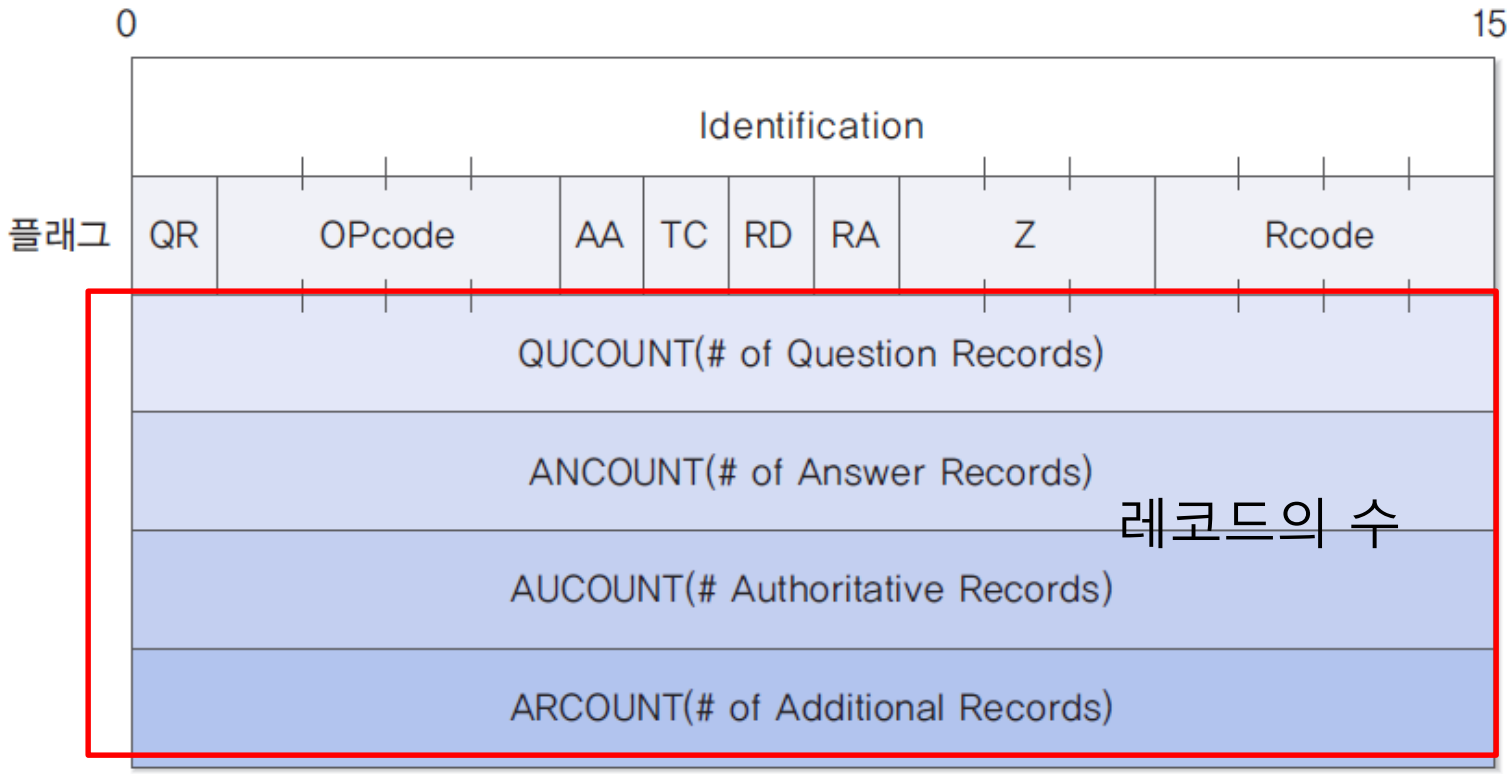


그림 14-11 DNS 헤더

4절. DNS 프로토콜

DNS 메시지

DNS 헤더

- Identification: 요청과 응답이 연관 관계를 표시
- QR(Query Response): 질의 메시지, 응답 메시지 구분
- OPCODE: 질의나 응답의 종류
- AA(Authoritative Answer): 인증 권한이 있는 네임 서버(응답 시)
- TC(Truncated): UDP 최대 크기 초과 여부
- RD(Recursion Desired): 재귀적 응답을 원함(질의 시)
- RA(Recursion Answer): 재귀적 응답 지원(응답 시)
- RCODE: 응답 오류

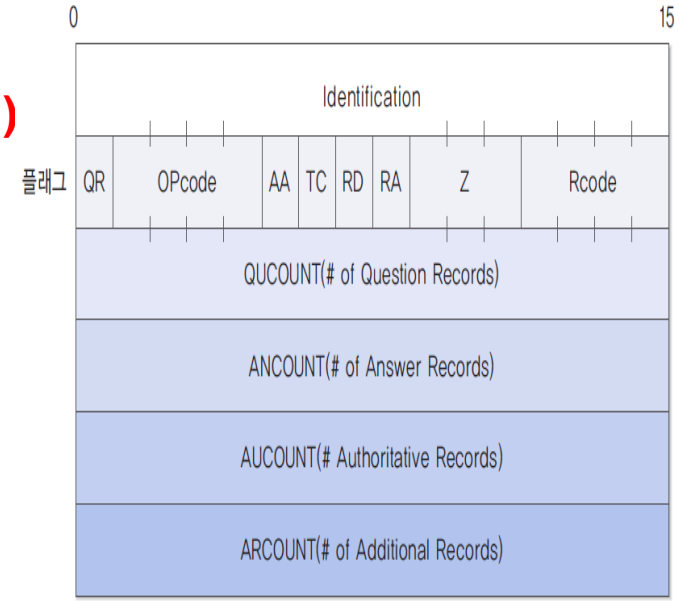


그림 14-11 DNS 헤더

4절. DNS 프로토콜

DNS 메시지

UDP의 제한

- 해석기와 네임 서버는 UDP 53 번 포트로 DNS 메시지 전송
- UDP 프로토콜의 최대 전송 크기: 512 바이트

- TCP 프로토콜 53 번 포트를 사용하는 경우
  - (1) 미리 512 바이트보다 크다는 것을 인지하는 경우 : 처음부터 TCP 사용
  - (2) 사전에 인지하지 못하고 UDP를 사용하는 경우는 TC=1로 지정됨
    이 경우 해석기가 TCP 연결을 설정하여 응답을 요청할 수 있음

DNS 프로토콜의 동작 과정

- 질의 메시지
  - www.korea.co.kr 호스트의 IP 주소를 원하는 경우
  - DNS 헤더

Identification: 0x337c
플래그: 0x0100 (QR=0, Opcode=0000, AA=0, TC=0, RD=1, RA=0, Z=000, RCODE=0000)
QUCOUNT: 1
ANCOUNT: 0
AUCOUNT: 0
ARCOUNT: 0

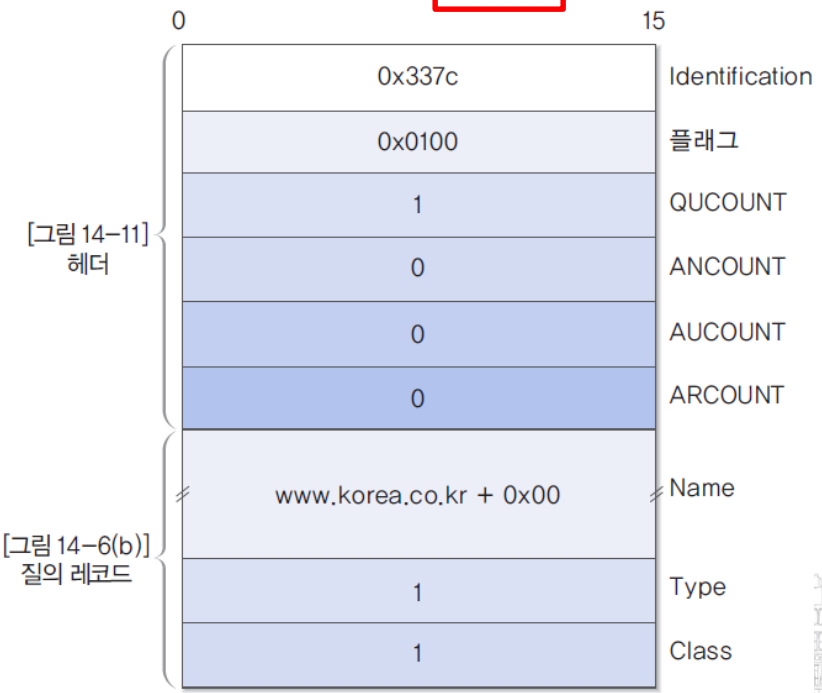


그림 14-12 질의 메시지의 예

  - QUESTION: QUCOUNT=1

    [그림 14-11, 14-6(b)]

    이름: www.korea.co.kr

    유형: A (Address)

    클래스: IN (인터넷)

DNS 프로토콜의 동작 과정

질의 메시지

- [그림 14-12]의 도식화

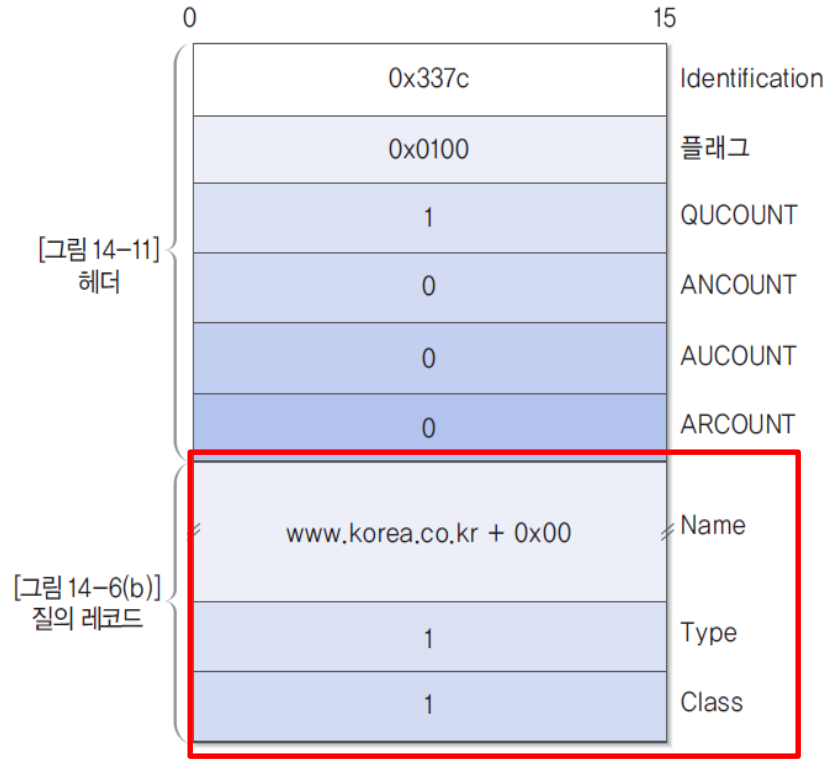


그림 14-12 질의 메시지의 예

그림 14-6 자원 레코드와 질의 레코드

DNS 프로토콜의 동작 과정

- 응답 메시지
  - DNS 헤더

```
Identification: 0x337c
플래그: 0x08180 (QR=1, Opcode=0000, AA=0, TC=0, RD=1, RA=1, Z=000,
RCODE=0000)
QUCOUNT: 1
ANCOUNT: 2
AUCOUNT: 2
ARCOUNT: 0
```

  - **QUESTION: QUCOUNT=1 [그림 14-10]**

    이름: www.korea.co.kr

    유형: A (Address)

    클래스: IN (인터넷)

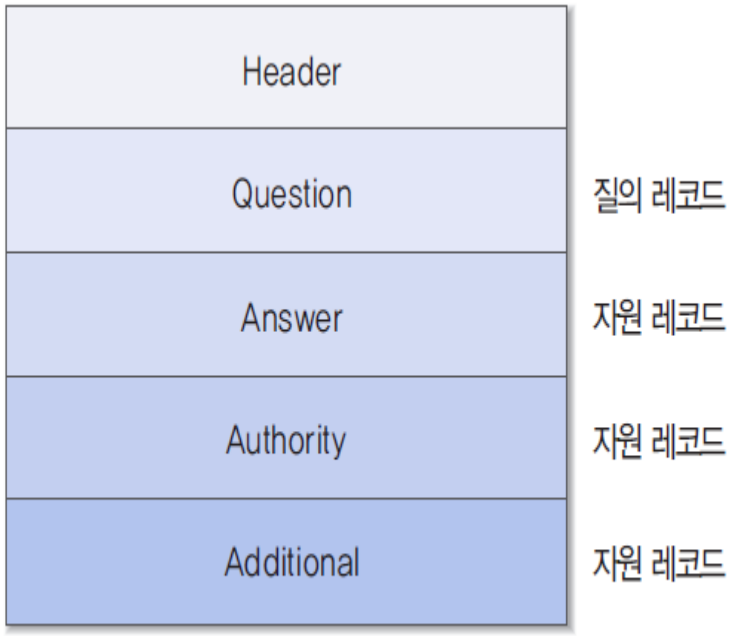


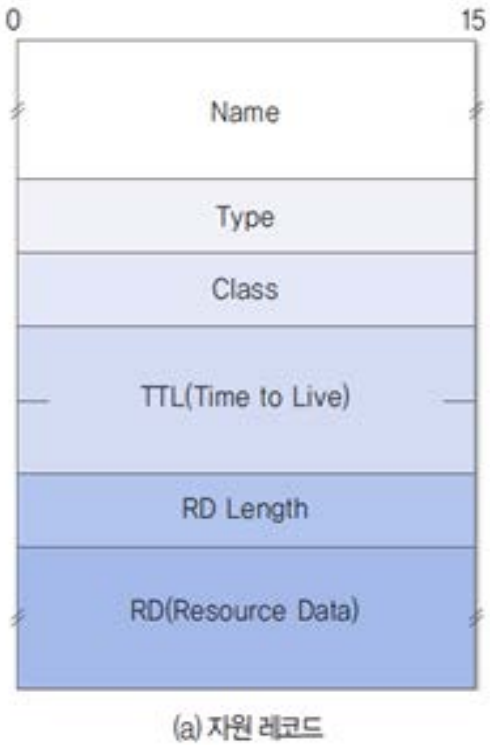
그림 14-10 DNS 메시지의 구조

DNS 프로토콜의 동작 과정

- 응답 메시지
  - ANSWER: ANCOUNT=2 [그림 14-10]

이름: www.korea.co.kr 별칭
유형: CNAME (Canonical Name for an Alias)
클래스: IN (인터넷)
TTL: 2시간
RD의 길이: 2 바이트
자원 데이터: Primary name: korea.co.kr 정식명칭

이름: korea.co.kr
유형: A (Address)
클래스: IN (인터넷)
TTL: 2시간
RD의 길이: 4 바이트
자원 데이터: Addr: 211.223.201.30



(a) 자원 레코드

DNS 프로토콜의 동작 과정

- 응답 메시지
  - ANSWER: AUCOUNT=2 [그림 14-10]

이름: korea.co.kr
유형: NS (Authoritative Name Server)
클래스: IN (인터넷)
TTL: 2시간
RD의 길이: 8 바이트
자원 데이터: Name Server: ns.ns1.kr

이름: korea.co.kr
유형: NS (Authoritative Name Server)
클래스: IN (인터넷)
TTL: 2시간
RD의 길이: 10 바이트
자원 데이터: Name Server: nsbk.ns2.kr