

컴퓨터 네트워크

15장. DNS (4)

- DNS 프로토콜

이번 시간의 학습 목표

- ▶ DNS 클라이언트와 서버 간 전송되는 DNS 메시지 이해

DNS 메시지 (1)

▶ 메시지 구성

▶ Header

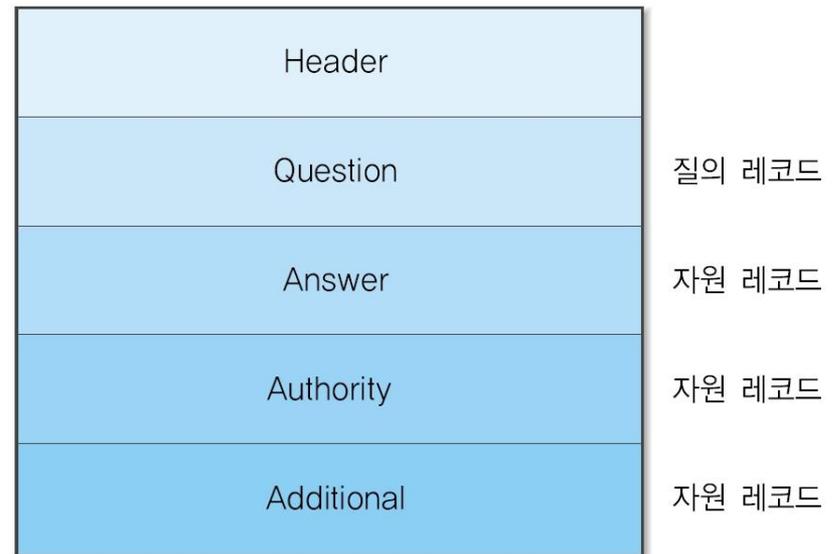
- ▶ 12바이트
- ▶ 헤더 값에 따라 메시지 각 필드의 사용 결정

▶ Question

- ▶ 질의 메시지, 응답 메시지에서 모두 사용
- ▶ 질의 레코드

▶ Answer, Authority, Additional

- ▶ 자원 레코드 사용

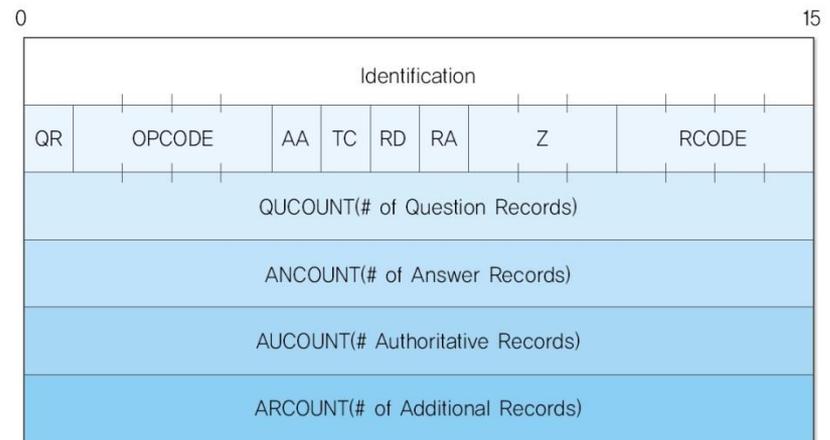


[그림 15-9] DNS 메시지

DNS 메시지 (2)

- ▶ DNS 헤더
 - ▶ Identification
 - ▶ 요청과 응답의 연관 관계 확인 용도
 - ▶ QR (Query Response)
 - ▶ 질의 메시지(1)
 - ▶ 응답 메시지(0)
 - ▶ OPCODE
 - ▶ 질의나 응답의 종류
 - ▶ 표준(0), 반대(1), 서버 상태 요청(2)
 - ▶ AA (Authoritative Answer)
 - ▶ 인증 권한이 있는 네임 서버 여부(응답 전용)
 - ▶ TC (Truncated)
 - ▶ UDP 최대 크기 초과 여부
 - ▶ 1로 설정되면 초과된 것이므로 TCP로 재요청 필요

- ▶ RD (Recursive Desired)
 - ▶ 재귀적 응답 요청 (질의 전용)
- ▶ RA (Recursion Available)
 - ▶ 재귀 응답 가능 여부 (응답 전용)
- ▶ RCODE
 - ▶ 0이면 정상, 그 외 응답 오류
- ▶ QCOUNT, ANCOUNT, AUCOUNT, ARCOUNT
 - ▶ 각 자원 레코드 갯수



[그림 15-10] DNS 메시지 헤더

UDP 패킷 크기로 인한 제약

- ▶ 해석기와 네임 서버는 기본적으로 UDP 53 번 포트로 DNS 메시지 전송
- ▶ UDP 프로토콜의 최대 전송 크기
 - ▶ 512 바이트
- ▶ TCP 53 번 포트를 사용하는 경우
 - ▶ 미리 512 바이트보다 크다는 것을 인지하는 경우에는 처음부터 TCP 사용
 - ▶ 사전에 인지하지 못하는 경우는 TC=1로 지정되므로, TCP 연결을 사용하여 재질의
- ▶ IPv4의 경우 UDP 사용이 일반적이거나, 주소 크기가 늘어나고 기본적으로 복수 개의 주소를 가질 수 있는 IPv6, 보안이 강화된 DNSSEC의 경우 UDP 크기 제한을 넘어갈 수 있음

DNS 프로토콜의 동작 과정 (1)

▶ 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

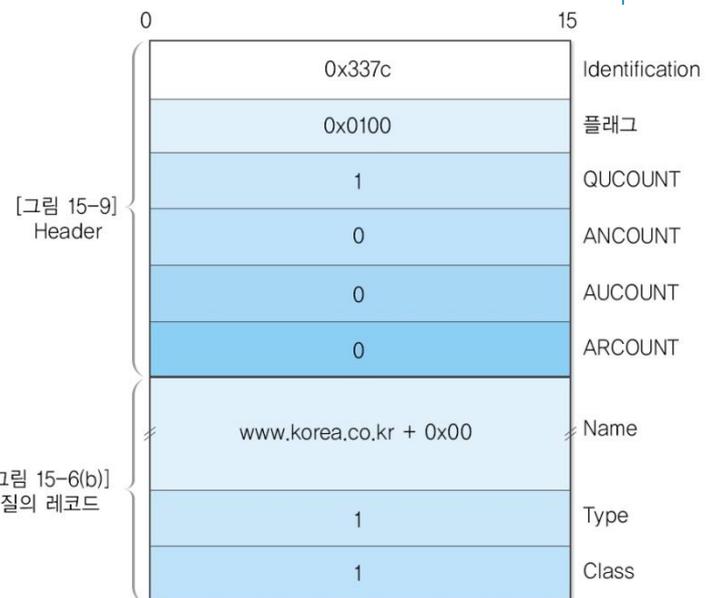
ARCOUNT: 0

▶ QUESTION

이름: www.korea.co.kr

유형: A (Address)

클래스: IN (인터넷)



DNS 프로토콜의 동작 과정 (2)

▶ 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: 질의와 동일

▶ ANSWER: 2개

▶ AUTHORITY: 2개

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

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

이름: www.korea.co.kr
유형: CNAME (Canonical Name for an Alias)
클래스: IN (인터넷)
TTL: 2시간
RD의 길이: 2
자원 데이터: Primary name: korea.co.kr
이름: korea.co.kr
유형: A (Address)
클래스: IN (인터넷)
TTL: 2시간
RD의 길이: 4
자원 데이터: Addr: 211.223.201.30

질의 / 응답