8 네트워크 계층

가천대학교 - 2019학년도 1학기 -

Preview

IPv4

- 현재 인터넷에서 사용하는 네트워크 계층의 프로토콜은 IPv4
- 1970년대에 개발한 IP는 인터넷의 핵심 프로토콜
- 오래 사용해온 만큼 기능이 매우 안정적
- 32비트의 제한된 주소 공간은 인터넷 확장으로 한계에 부딪힘
- 현대 발전된 네트워크 환경에 부합되지 않는 기능으로 여러 문제점 제기

IPv6와 이동 IP 프로토콜

- 현재 통신 환경에 맞게 IP 프로토콜을 개선하기 위한 연구 꾸준히 진행
- 대표적인 예가 IPv6와 이동 IP 프로토콜
- IPv6와 이동 IP 프로토콜을 학습하면 IPv4의 문제점과 개선방안 파악 가능

다양한 인터넷 제어프로토콜 학습을 통해 인터넷 구조에 대한 상세한 이해 가능

Contents

학습목표

- IPv6의 필요성과 헤더 구조를 이해한다.
- 이동 IP 프로토콜의 터널링 원리를 이해한다.
- ARP/RARP의 필요성을 이해한다.
- ICMP의 헤더와 제어 메시지를 이해한다.
- IGMP의 헤더와 멀티캐스트 그룹 관리 방식을 이해한다.

내용

- IPv6 프로토콜
- 이동 IP 프로토콜
- 기타 네트워크 계층 프로토콜

01_IPv6 프로토콜

- IPv6의 주요 변경 사항
  - 주소 공간 확장
    - 주소 공간이 32비트에서 128비트로 확장
  - 헤더 구조 단순화
    - 불필요한 필드가 제외 되거나 확장 헤더 형식으로 변경
    - 과도하게 수행되는 오류 제어 등의 오버헤드를 줄여 프로토콜의 전송 효율 향상
  - 흐름 제어 기능 지원
    - 일정 범위 내에서 예측 가능한 데이터 흐름을 지원
    - 실시간 멀티미디어 응용 환경을 수용

01_IPv6 프로토콜

❖ IPv6 헤더 구조

- 9개의 기본 필드를 지원, 총 40바이트 중에서 32바이트는 주소 공간으로 할당, 8바이트만 프로토콜 기능

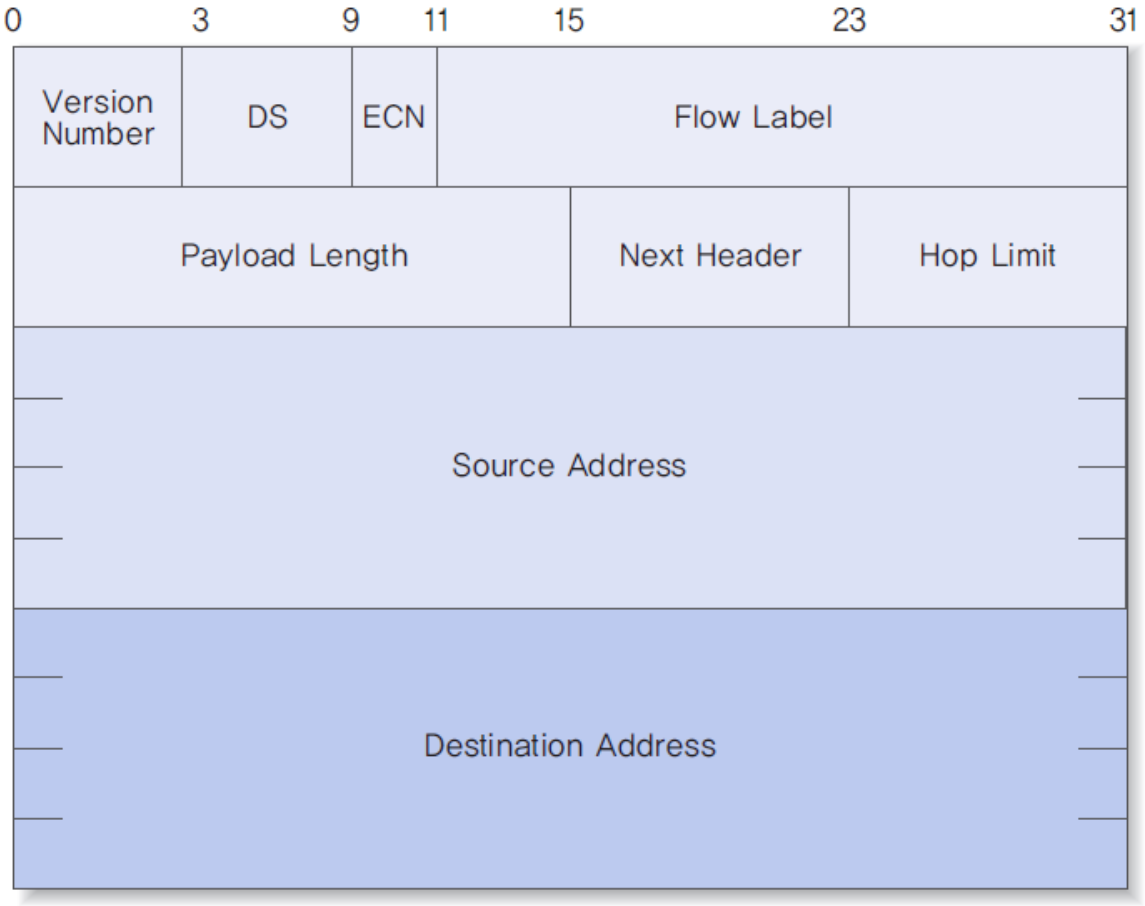

그림 8-1 IPv6 기본 헤더의 구조

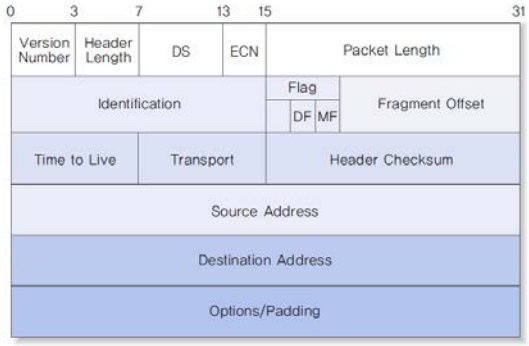

그림 7-12 IP 헤더의 구조

01_IPv6 프로토콜

- 확장 헤더의 종류
  - IPv6 기본 헤더 바로 뒤에 확장 헤더를 하나 이상 둘 수 있음
  - Hop-by-Hop Options Header : hop-by-hop 옵션 처리를 지원
    - Jumbo 페이로드 옵션 : 데이터의 크기가 65535 바이트보다 클 때 사용
    - 라우터 긴급 옵션 : 라우터에 전송 대역 예약 같은 특정 정보를 제공
  - Routing Header
    - IPv4의 소스 라우팅과 유사한 기능
    - 패킷이 Routing Header에 지정된 특정 노드를 경유하여 전송됨
  - Fragment Header : 패킷 분할과 관련된 정보를 포함
  - Destination Options Header : 수신 호스트가 확인할 수 있는 옵션 정보
  - Authentication Header : 패킷 인증 관련 기능
  - Encapsulating Security Payload Header : 프라이버시 기능 제공을 위해 페이로드 암호화. 인증된 목적지 호스트에서 암호화 데이터를 해동할 수 있는 정보도 함께 제공

01_IPv6 프로토콜

- DS/ECN 필드
  - 차등 서비스가 도입되면서 6비트의 DS 필드와 2비트의 ECN 필드가 정의됨
- Flow Label 필드
  - 음성이나 영상 데이터처럼 실시간 서비스가 필요한 응용 환경에서 사용
  - 기본 원칙
    - Flow Label 필드를 지원하지 않는 호스트나 라우터에서는 IPv6 패킷을 생성할 때 반드시 0 지정
    - Flow Label 필드의 값이 0 이외의 동일한 번호로 부여받은 패킷은 Destination Address, Source Address, Priority, Hop-by-Hop Options Header, Routing Header 등을 모두 동일 지정
    - Flow Label 필드 값은 최대 범위 내에서 랜덤하게 선택
- 기타 필드
  - Version Number(버전 번호) : IP 프로토콜의 버전 번호
  - Payload Length(페이로드 길이) : 헤더를 제외한 패킷의 크기
  - Next Header : 기본 헤더 다음에 이어지는 헤더의 유형을 수신 호스트에 알려줌
    - IPv6의 확장 헤더 또는 TCP와 UDP 헤더
  - Hop Limit(홉 제한) : IPv4의 Time To Live 필드와 동일한 역할을 수행
  - Source Address/Destination Address(송신 호스트 주소/수신 호스트 주소) : 송수신 호스트의 IP 주소를 나타냄

01_IPv6 프로토콜

❖IPv6 주소

- 주소 표현
  - 128비트, 16비트의 숫자 8개를 콜론(:)으로 구분

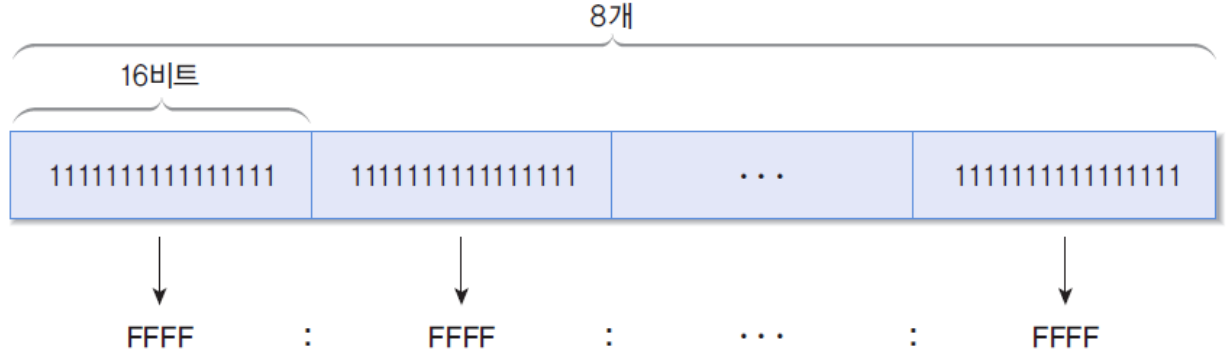

그림 8-2 IPv6의 주소 표현

  - 예) D1D1:1111:3F3F:1700:4545:1212:1111:1231
  - 축약표시 : 2001:0db8:3c4d:0015:0000:0000:1a2f:1a2b 주소는 2001:db8:3c4d:15::1a2f:1a2b로 축약 가능
  - IPv4와 함께 사용하는 환경에서 IPv4 주소를 캡슐화하여 표시

```
X:X:X:X:X:X:d.d.d.d
```

  - X는 16비트이므로 총 96(16×6)비트, d는 8비트이므로 총 32(8×4)비트
  - 즉, 전체 크기는 IPv6의 주소 크기와 동일한 128(96+32)비트

01_IPv6 프로토콜

- 주소 공간
  - IPv6의 주소 공간

표 8-1 IPv6의 주소 공간

상위 비트	용도	상위 비트	용도
0000 0000	예약(IPv4 공간 지원 포함)	100	비할당
0000 0001	비할당	101	비할당
0000 001	OSI NSAP 주소 공간	110	비할당
0000 010	Novell Netware IPX 주소 공간	1110	비할당
0000 011	비할당	1111 0	비할당
0000 01	비할당	1111 10	비할당
0001	비할당	1111 110	비할당
001	유니 캐스트 주소 공간	1111 1110 0	비할당
010	비할당	1111 1110 10	Link 지역 주소 공간
010	비할당	1111 1110 11	Site 지역 주소 공간
011	비할당	1111 1111	멀티캐스트 주소 공간

02_이동 IP 프로토콜

❖ 이동 IP 프로토콜

- 이동하는 사용자가 서비스 중단 없이 인터넷에 접속할 수 있는 이동 환경 지원
- 통신 서비스 환경이 전통적인 PSTN Public Switched Telephone Network 혹은 ISDN Integrated Services Digital Network 기반의 음성 위주 서비스에서 광대역 Broadband 멀티미디어 서비스로 발전
- 이동 호스트가 자신의 고유 주소를 유지하면서 인터넷 서비스를 받으려면 계속 이동하는 송수신 호스트 간의 데이터 라우팅 처리가 가장 중요

02_이동 IP 프로토콜

❖ 터널링 원리

- 상이한 전송 수단
  - IP 프로토콜을 교체하는 방식 (버스→배→버스)

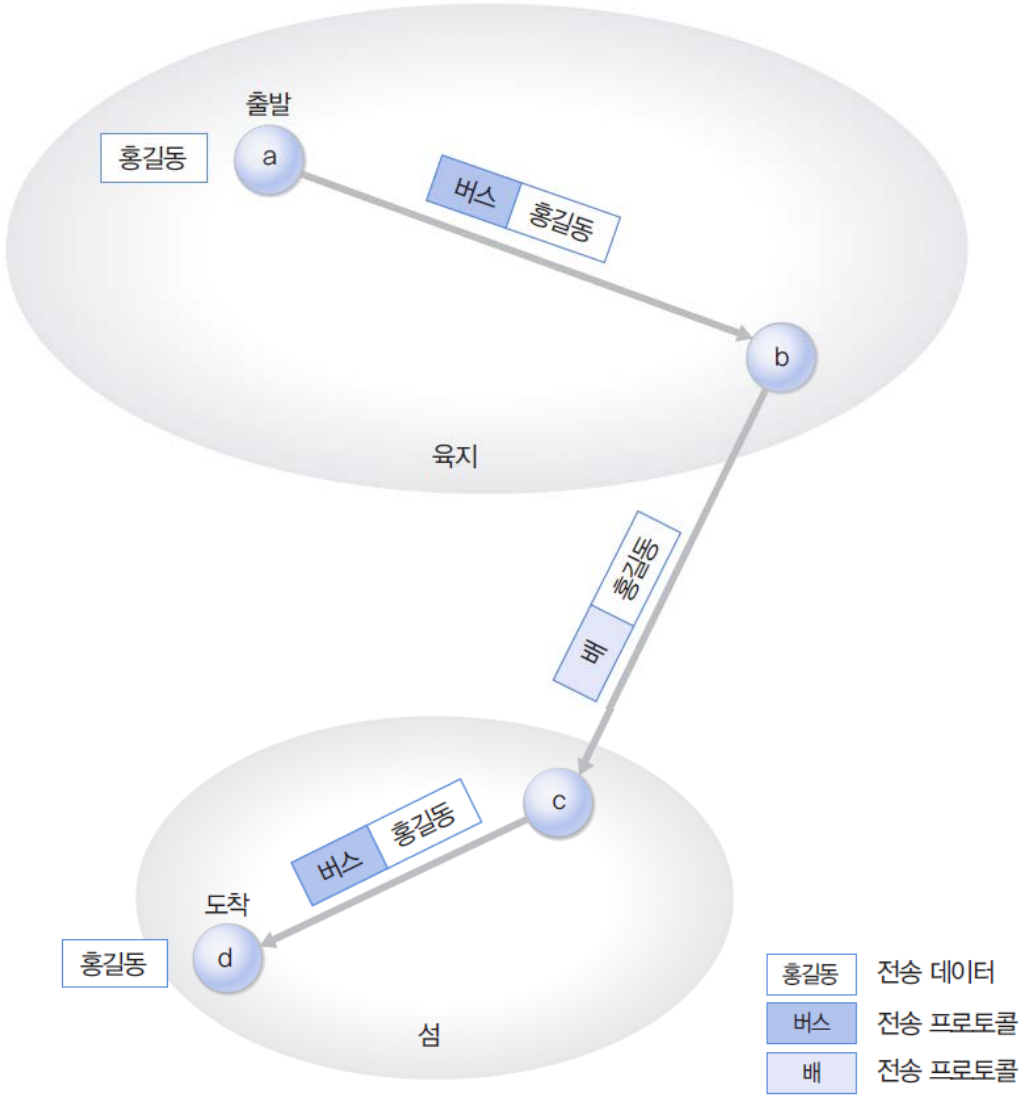

그림 8-3 상이한 전송 수단

02_이동 IP 프로토콜

- 터널링 방식

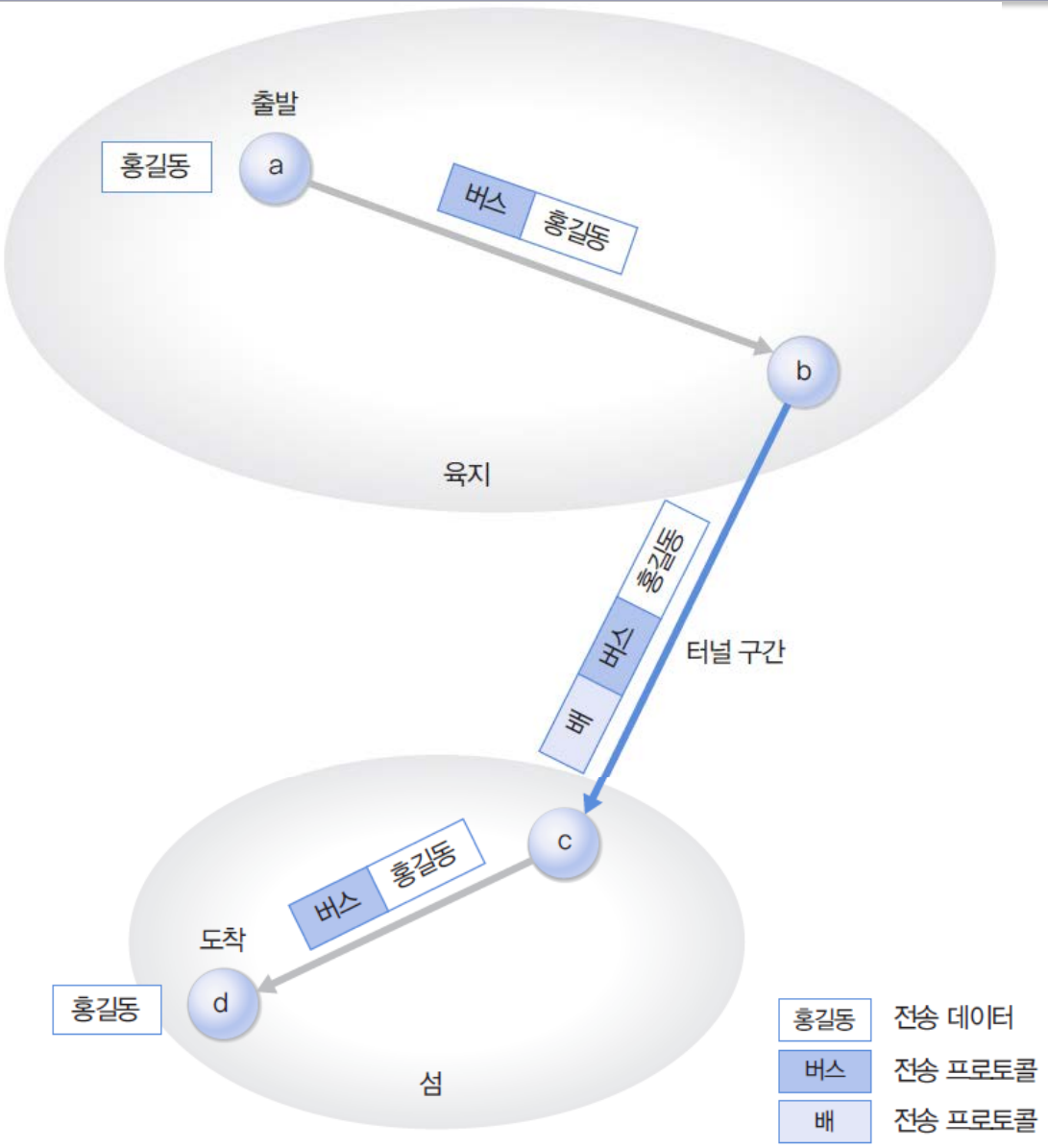

그림 8-4 IP 터널링의 원리

02_이동 IP 프로토콜

❖IP 터널링

- 무선 호스트가 움직일 때 이동 IP 프로토콜의 기본 동작 원리
  - 이동 호스트의 움직이면 새로운 위치를 관장하는 포린 에이전트Foreign Agent FAnew로부터 COACare of Address를 얻음
  - 이 주소는 이동 호스트의 홈 에이전트Home Agent HA에 등록되어 FAnew와 HA 사이에 터널을 형성
  - HA로 라우팅된 패킷을 이동 호스트에 전달하려면 새로 형성된 터널을 통해 FAnew로 전달

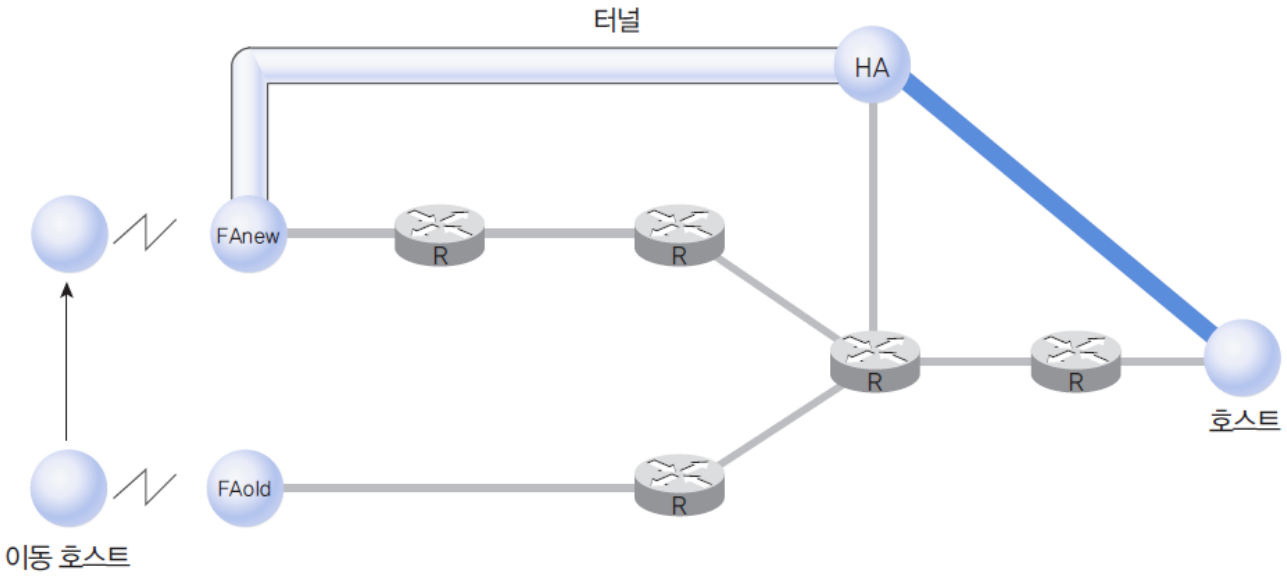

그림 8-5 이동 IP 프로토콜의 기본 동작 원리

02_이동 IP 프로토콜

- 이동 호스트에는 고유 IP 주소인 홈 주소Home Addres HA가 할당, 호스트 위치가 바뀌어도 변하지 않음. 홈 에이전트와 밀접한 관련
- COA는 이동 호스트가 새로 이동한 지역에서 일시적으로 할당된 IP 주소
  호스트가 이동할 때마다 새로운 COA가 할당되고 기존 COA는 회수되는 과정이 반복됨

- 송신 호스트에서 이동 호스트까지 패킷 전달 과정
  - 이동 호스트를 목적지로 하는 패킷은 HA에게 전달됨
  - HA는 FA와의 터널을 이용해 FA에게 패킷을 전달함
  - FA는 이동 호스트에게 패킷 전달함

- 홈 에이전트와 이동 에이전트 사이에 설정되는 터널Tunnel은 원 IP 패킷을 목적지까지 전송하기 위한 중간 단계의 새로운 경로임

02_이동 IP 프로토콜

- 터널구간 라우팅 처리
  - 원 IP 패킷을 데이터로 취급하는 새로운 형태의 IP 캡슐 패킷이 구성되어 전달. 원 패킷의 Destination Address 필드에는 이동 호스트의 홈 주소가 들어감
  - 홈 에이전트에서는 원 패킷을 이동 호스트에 전달하려고 그림처럼 캡슐 패킷으로 변경

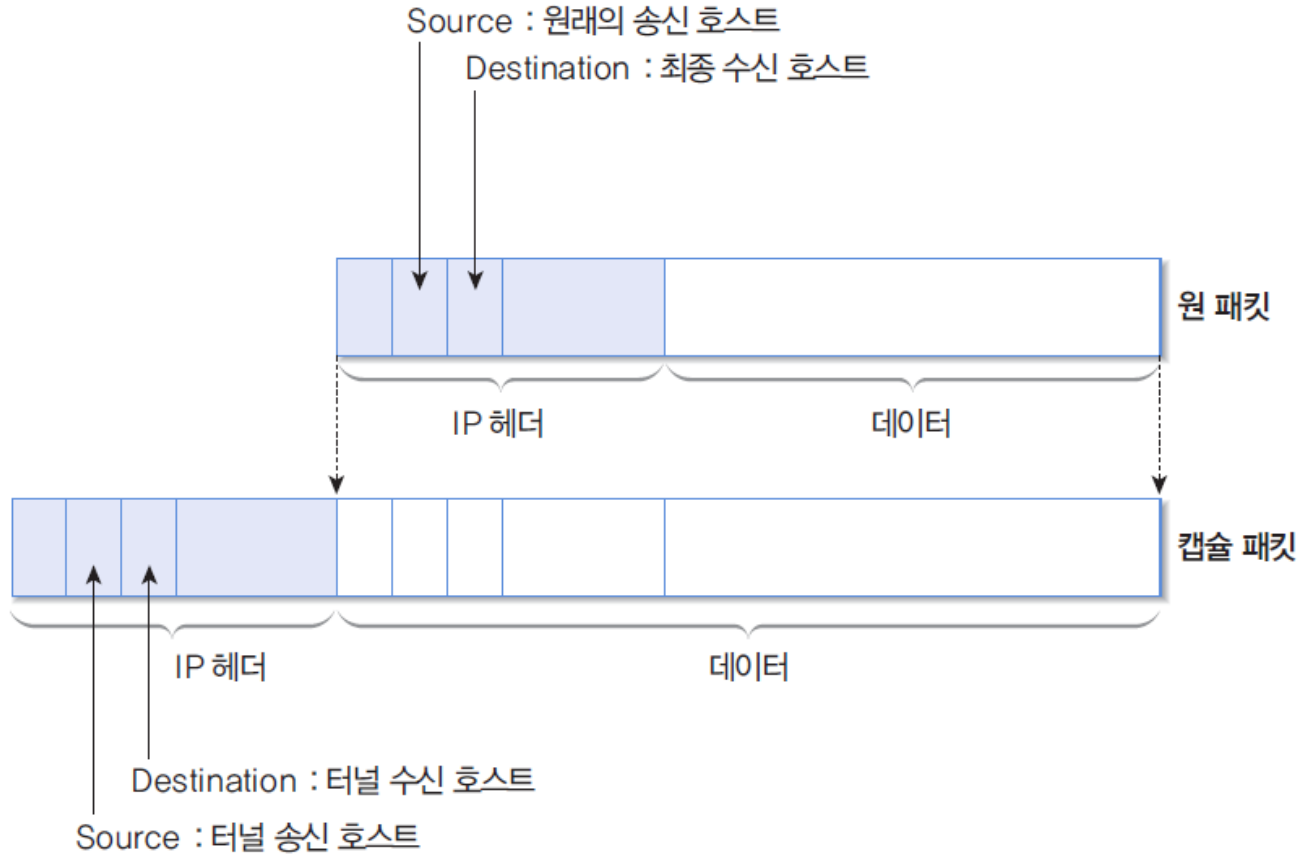

그림 8-6 IP 터널

03_기타 네트워크 계층 프로토콜

❖ ARP 프로토콜

- IP 주소와 MAC 주소 사이의 변환을 담당

- MAC 주소
  - 송신 호스트의 IP 주소 : 송신 호스트의 하드 디스크에서 얻을 수 있음
  - 수신 호스트의 IP 주소 : 사용자가 제공
  - 송신 호스트의 MAC 주소 : 송신 호스트의 LAN 카드에서 얻을 수 있음
  - 수신 호스트의 MAC 주소 : IP 주소를 매개변수로 하여 ARP 프로토콜로 얻음

  - ARP 프로토콜
    - 특정 호스트의 IP 주소로 부터 MAC 주소를 제공하는 프로토콜
    - ARP request라는 특수 패킷을 브로드캐스팅
    - IP 주소에 해당하는 호스트만 ARP reply로 MAC 주소를 회신
    - 효율 향상을 위해 캐시 기능을 제공 (ARP table)
    - 송신 호스트가 ARP request와 reply를 처리하는 과정에서 패킷을 수신한 모든 호스트는 송신 호스트의 IP주소와 MAC 주소 매핑 값 획득 가능 (네트워크 부하 최소화)

03_기타 네트워크 계층 프로토콜

- ARP의 필요성

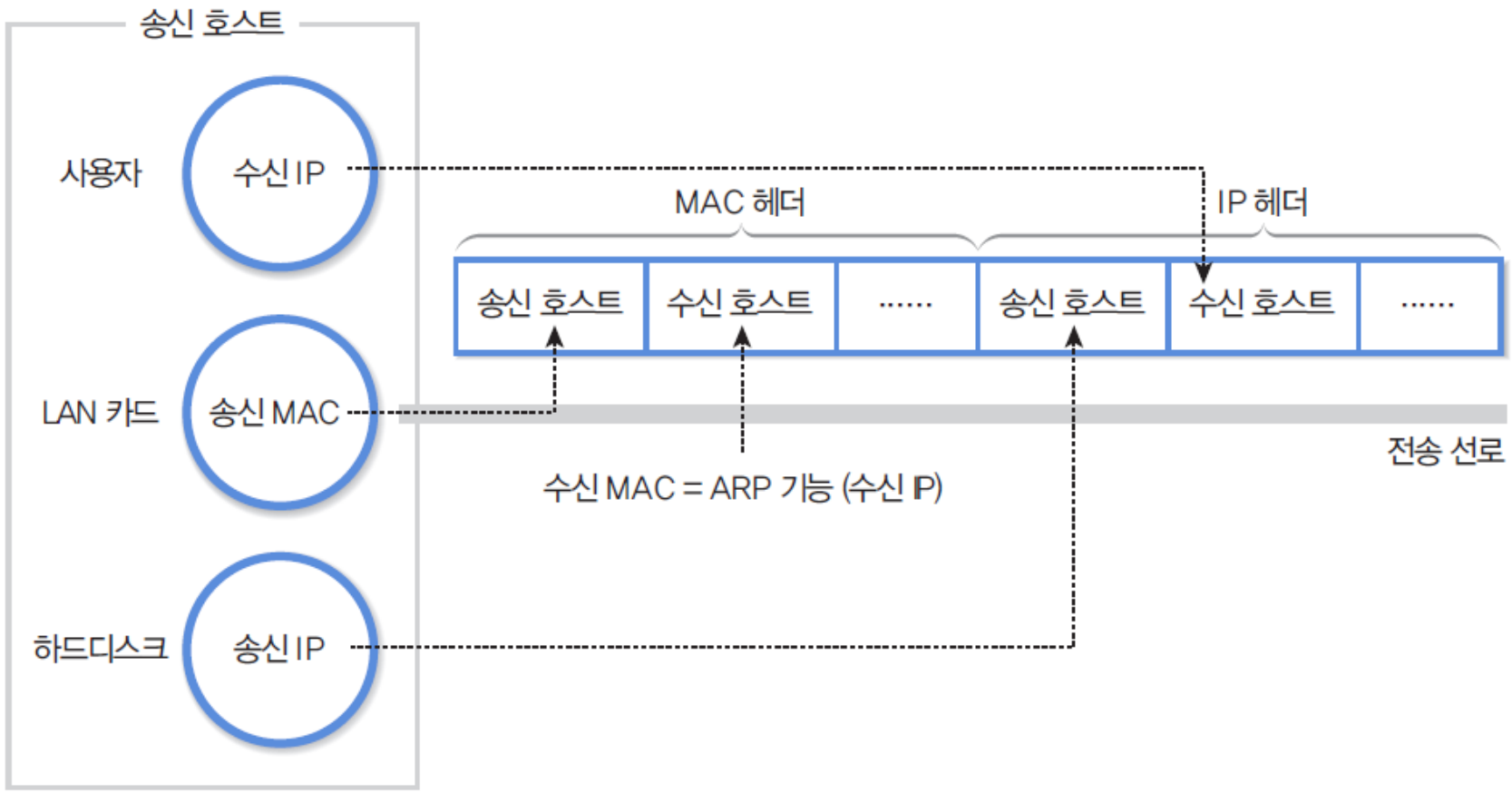

그림 8-7 ARP의 필요성

03_기타 네트워크 계층 프로토콜

- RARP Reverse Address Resolution Protocol 프로토콜의 필요성
  - 하드 디스크가 없는 시스템은 자신의 IP 주소를 알 수 없음
  - 특정 호스트의 MAC 주소로 부터 IP 주소를 제공하는 프로토콜
  - 보통 네트워크에서는 RARP 기능을 전담 수행하는 서버가 하나이상 존재

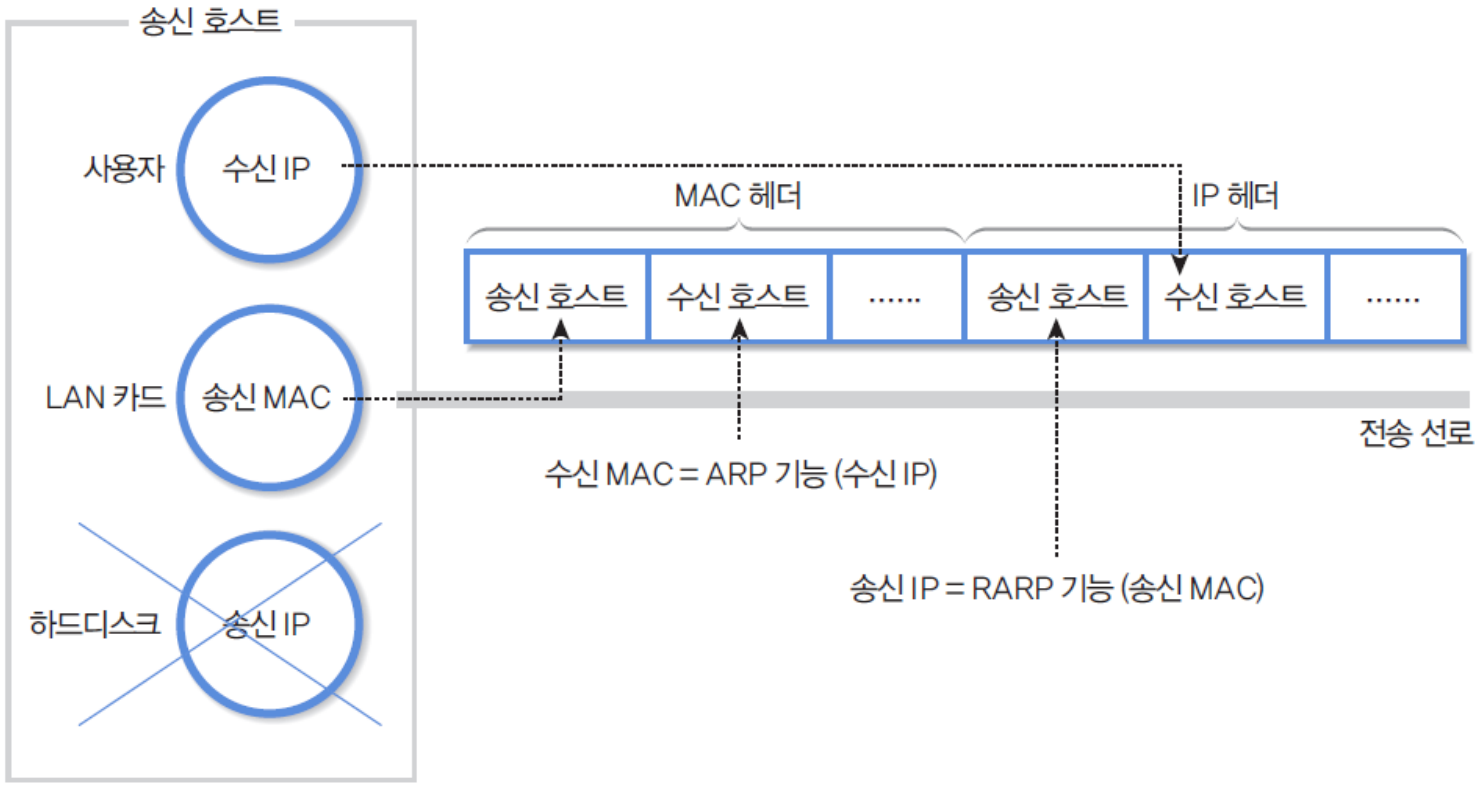

그림 8-8 RARP의 필요성

03_기타 네트워크 계층 프로토콜

ICMP Internet Control Message Protocol 프로토콜

- 인터넷 환경에서 오류에 관한 처리를 지원

ICMP 메시지

- 오류 보고 메시지 Error-Reporting Message : IP 패킷을 전송하는 과정에서 발생하는 문제를 보고하는 것이 목적

표 8-2 오류 보고 메시지

메시지	설명
DESTINATION UNREACHABLE	수신 호스트가 존재하지 않거나, 존재해도 필요한 프로토콜이나 포트 번호 등이 없어 수신 호스트에 접근이 불가능한 경우에 발생한다. IP 헤더의 DF 필드가 설정된 패킷을 라우터가 분할해야 하는 경우에도 해당 패킷을 버리고 이 메시지를 회신해준다.
SOURCE QUENCH	네트워크에 필요한 자원이 부족하여 패킷이 버려지는 경우에 발생한다. 예를 들면, 전송 경로에 있는 라우터에 부하가 많이 걸려 패킷이 버려지는 경우이다. 이 메시지를 이용해 송신 호스트에 혼잡 가능성을 경고함으로써, 패킷을 송신하는 호스트가 데이터를 천천히 전송하도록 알릴 수 있다.
TIME EXCEEDED	패킷의 TTL Time To Live 필드 값이 0이 되어 패킷이 버려진 경우에 주로 발생한다. 기타 시간 초과 현상에 의해 패킷이 버려진 경우도 이에 해당한다.

03_기타 네트워크 계층 프로토콜

- 질의 메시지Query Message : 라우터 혹은 다른 호스트들의 정보를 획득하려는 목적

표 8-3 **질의 메시지**

메시지	설명
ECHO REQUEST, ECHO REPLY	유닉스Unix의 ping 프로그램에서 네트워크의 신뢰성을 검증하기 위하여 ECHO REQUEST 메시지를 전송하고, 이를 수신한 호스트는 ECHO REPLY를 전송해 응답한다. 특정 호스트가 인터넷에서 활성화되어 동작하는지 확인할 수 있다.
TIMESTAMP REQUEST, TIMESTAMP REPLY	두 호스트 간의 네트워크 지연을 계산하는 용도로 사용한다.

03_기타 네트워크 계층 프로토콜

- ICMP 헤더 형식
  - 오류 보고 메세지

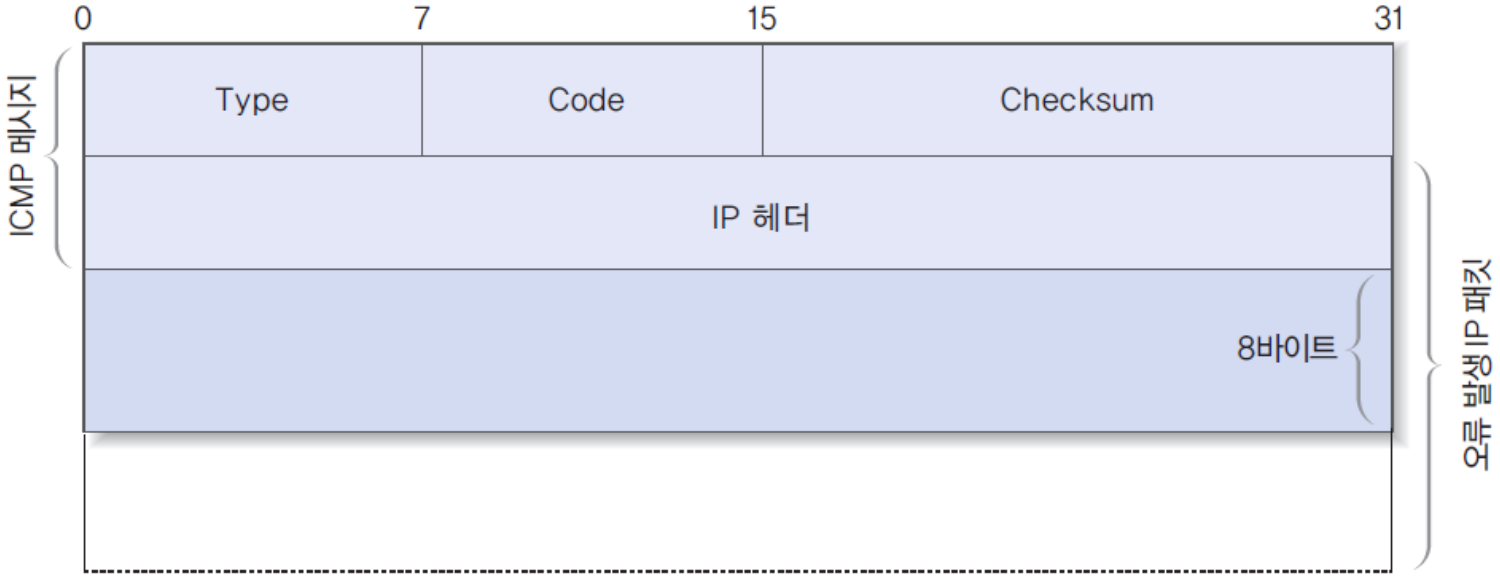

그림 8-9 ICMP 메시지 : 오류 보고 메시지

- 오류 원인을 제공한 IP 패킷의 헤더와 이어지는 8바이트의 정보가 오류 보고 메시지에 포함됨
- Type(유형) : 1바이트 크기로 메시지의 종류를 구분
- Code(코드) : 메시지 내용에 대한 자세한 정보를 제공하는 매개변수 값
- Checksum(체크섬) : ICMP 전체 메시지에 대한 체크섬 기능을 지원

03_기타 네트워크 계층 프로토콜

- 질의 메시지
  - Identifier와 Sequence Number 필드를 사용하여 메시지를 구분하는 기능이 사용

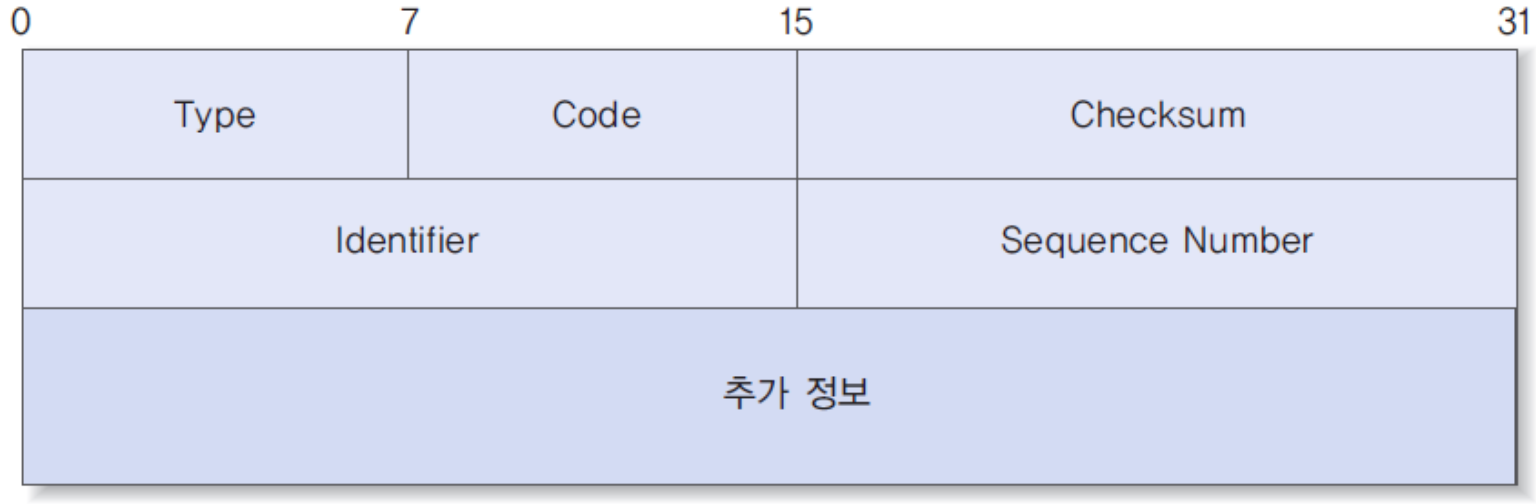

그림 8-10 ICMP 메시지 : 질의 메시지

03_기타 네트워크 계층 프로토콜

- ICMP 메시지 전송
  - ICMP는 기능적으로 IP 프로토콜과 같은 계층의 역할을 수행
  - ICMP 메시지는 IP 프로토콜에 캡슐화되어 전송

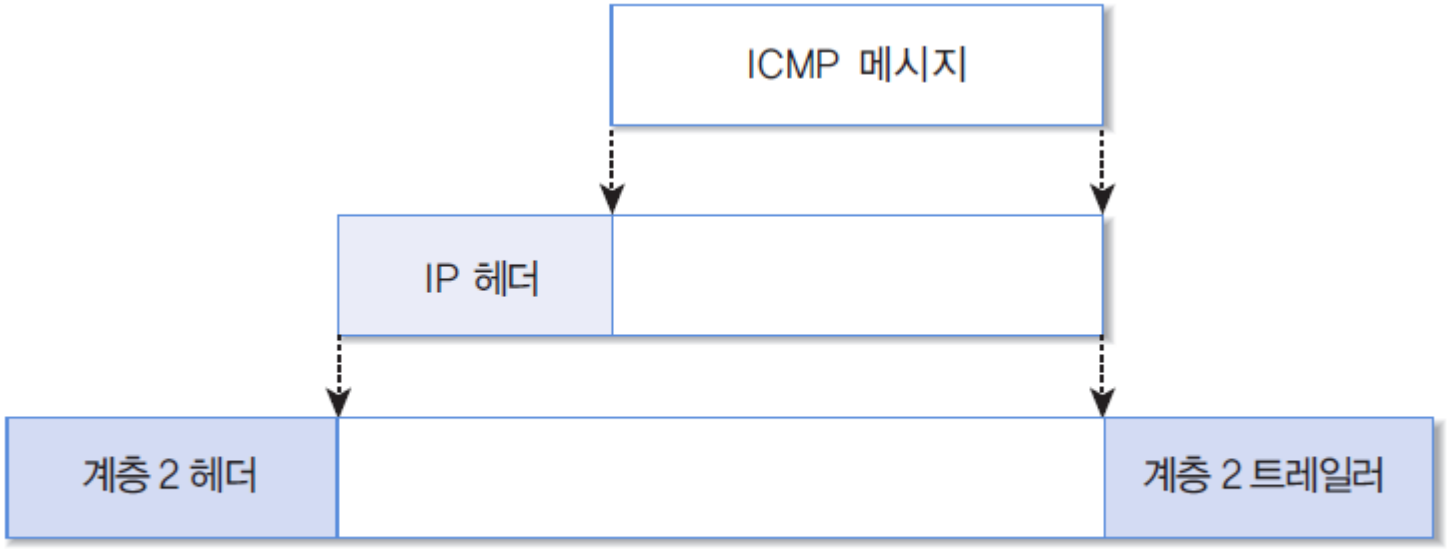

그림 8-11 ICMP 메시지의 전송

03_기타 네트워크 계층 프로토콜

IGMP Internet Group Management Protocol 프로토콜

- 멀티캐스팅Multicasting : 특정 그룹의 모든 호스트에 메시지를 전송하는 방식
- 멀티캐스트 라우팅Multicast Routing : 멀티캐스팅에 필요한 라우팅 알고리즘

- 그룹 관리
  - 그룹 관리의 주요 기능 : 그룹의 생성.제거, 전송 호스트의 그룹 참가.탈퇴 등
  - 멀티캐스팅 기능
    - 다중 호스트를 표시하는 멀티캐스트 그룹 주소 표기 방법의 통일
    - 라우터가 멀티캐스트 주소와 이 그룹에 속하는 호스트 사이의 연관성 처리
    - 멀티캐스트 라우팅 알고리즘은 그룹의 모든 멤버에게 가장 짧은 경로를 선택하는 기능 제공

- IGMPInternet Group Management Protocol
  - 멀티캐스트 그룹에 가입하거나 탈퇴할 때 사용하는 프로토콜
  - 멀티캐스트 그룹에 가입한 호스트와 라우터 사이에 멤버 정보를 교환하는 용도
  - 질의 메시지 : 멀티캐스트 라우터가 그룹 정보를 얻기 위하여 호스트에 전달
  - 보고 메시지 : 질의의 응답으로 호스트가 보고 메시지를 회신

03_기타 네트워크 계층 프로토콜

- IGMP 헤더의 구조

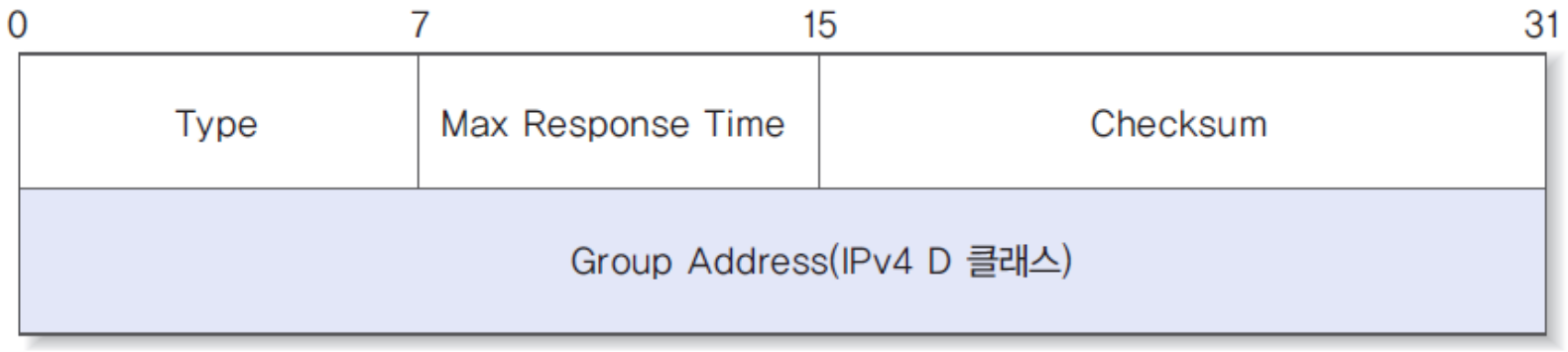

그림 8-12 IGMP 헤더의 구조

- Type(유형) : 0x11 - 멀티캐스트 라우터가 전송한 질의 메시지
  0x16 - 호스트가 전송하는 보고 메시지
  0x17 - 그룹 탈퇴에 관한 메시지
- Max Response Time(최대 응답 시간) : 질의에 대한 보고 메시지가 전송되는 최대응답시간
- Checksum(체크섬) : IP 프로토콜에서 사용하는 알고리즘과 동일한 방식 (오류 검출용으로 이용)
- Group Address(그룹 주소) : 질의 메시지는 0, 보고 메시지에는 호스트가 가입을 원하는 그룹 주소를 표기

03_기타 네트워크 계층 프로토콜

- IGMP 동작 과정
  - 그룹 가입 : 해당 멀티캐스트 주소를 표기한 IGMP 보고 메시지를 전송
  - 그룹 유지 : IGMP 보고 메시지를 사용해 IGMP 질의에 응답해야 함
  - 그룹 탈퇴 : 라우터의 질의 메시지에 대해 호스트의 보고 메시지 응답이 없음

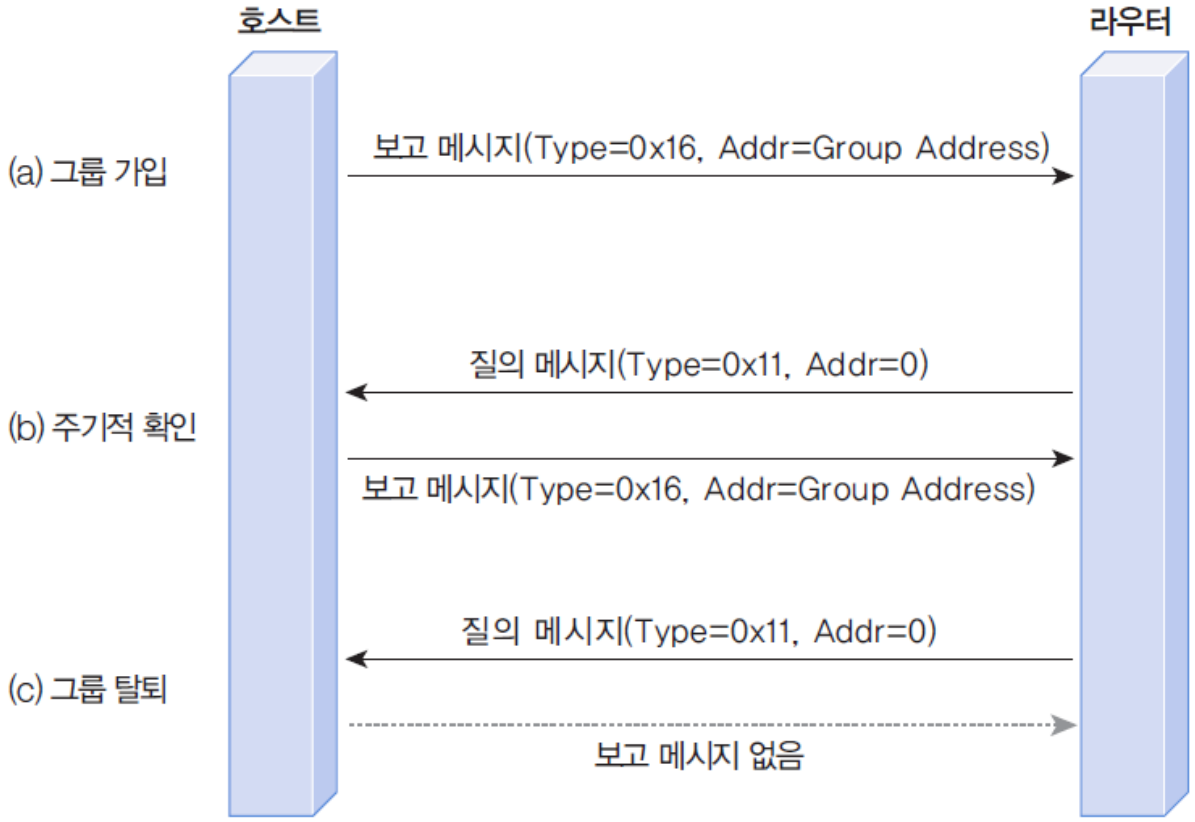

그림 8-13 IGMP 동작 과정

03_기타 네트워크 계층 프로토콜

- IGMP 메시지의 전송
  - IGMP는 IP 패킷에 캡슐화되어 보내짐
    즉, IGMP 메시지는 IP 프로토콜의 데이터로 처리되기 때문에 IP 패킷의 헤더에 실려서 계층 2 프로토콜로 전달됨

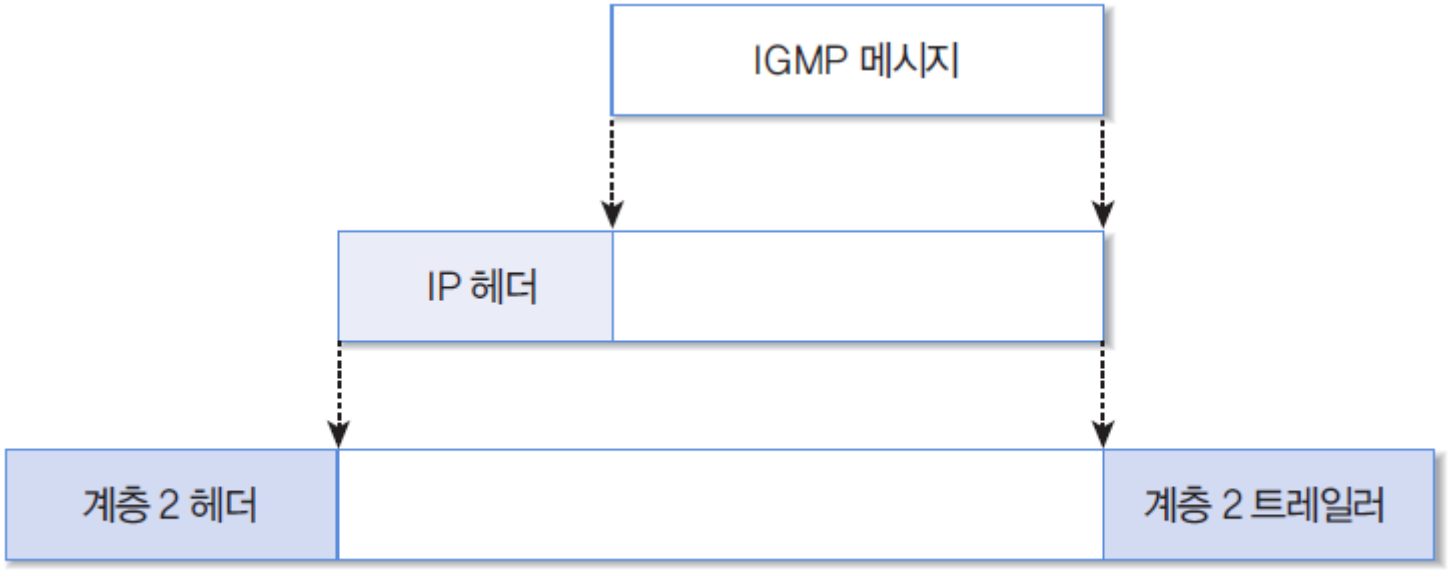

그림 8-14 IGMP 메시지의 전송

Thank You