9장. Internet Control Message Protocol Version 4 (ICMPv4)

2025년 1학기
단국대학교 컴퓨터공학과
박태근

Contents

[from TCP/IP Protocol Suite Fourth Edition]

9.1 소개

- ✓ IP 프로토콜은 **오류 보고 (error-reporting)**와 **오류 수정 메커니즘 (error correcting mechanism)**이 **없음**
- ✓ 만약 무엇인가 **잘못된 일이 발생하면** **어떻게 되는가**?
- ✓ 최종 목적지를 향한 **라우터를 찾을 수 없거나**, 수명 필드가 0이되어 라우터가 **데이터그램을 폐기 (discard)하면** **어떻게 되는가**?
- ✓ 이들은, **오류가 발생**하였는데도 **불구**하고, IP 프로토콜이 **원래의 호스트에게 통보할 메커니즘을 가지고 있지 않은 상황들 (situations)**에 대한 **예제 (examples)**임

[from TCP/IP Protocol Suite Fourth Edition]

9.1 소개 – Topics

1) TCP/IP 프로토콜 모음에서 ICMP의 위치 (The position of ICMP in the TCP/IP suite)

2) ICMP 패킷의 캡슐화 (Encapsulation of ICMP Packets)

[from TCP/IP Protocol Suite Fourth Edition]

9.1 소개 – TCP/IP 프로토콜 모음에서 ICMP의 위치

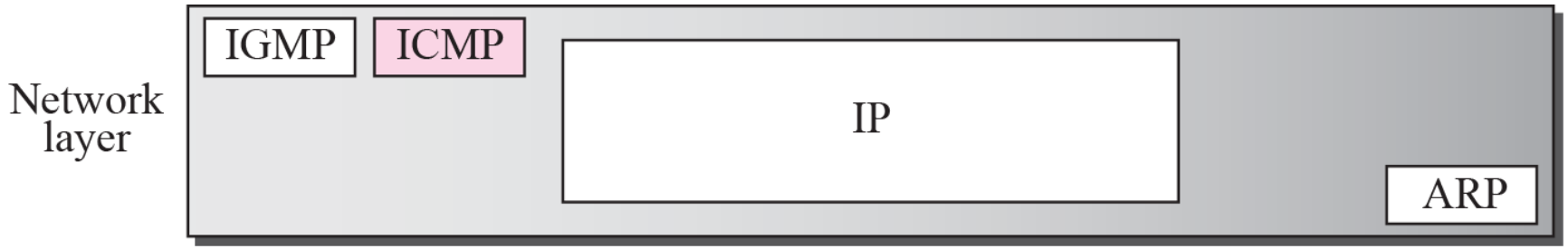


그림 9.1 네트워크 계층에서 ICMP의 위치
(Position of ICMP in the network layer)

[from TCP/IP Protocol Suite Fourth Edition]

9.1 소개 – ICMP 패킷의 캡슐화

✓ **ICMP 캡슐화 (ICMP encapsulation)**

- ICMP는 **네트워크 계층 프로토콜 (network layer protocol)**임
- 그러나, 이 프로토콜의 메시지는 예상과는 달리 **직접 데이터링크 계층으로 전달되지 않음**
- 대신, 메시지는 하위 계층으로 가기 전에 **IP 데이터그램 내에 캡슐화 (encapsulation)**됨

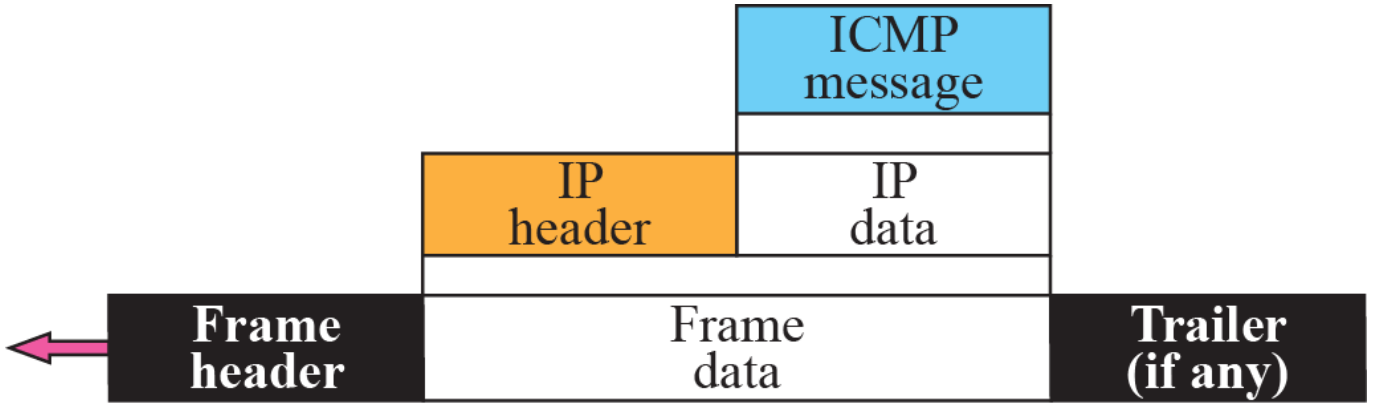


그림 9.2 ICMP 캡슐화 (ICMP encapsulation)

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지

✓ ICMP 메시지는 **두 개의 카테고리**로 분류됨

- **오류 보고 메시지 (error-reporting messages)**
- **질의 메시지 (query messages)**

✓ **오류 보고 메시지 (error-reporting messages)**는 라우터나 (목적지) 호스트가 IP 패킷을 처리하는 도중에 탐지되는 **문제 (problems)를 보고 (report)**함

✓ **질의 메시지 (query messages)**는 **쌍 (pairs)으로 생성**되는데, 호스트나 네트워크 관리자가 라우터나 다른 호스트로부터 **특정 정보 (specific information)를 획득**하기 위해 사용함

✓ 또한, 호스트는 **같은 네트워크 상의 라우터를 발견 (discover and learn about routers)**하고, 라우터는 노드가 **메시지를 다른 곳으로 보내는 것 (redirect its messages)**을 도울 수 있음

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – Topics

1) 메시지 형식 (Message Format)
2) 오류 보고 메시지 (Error Reporting Messages)
3) 질의 메시지 (Query Messages)

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 메시지 형식

Table 9.1 *ICMP messages*

Category	*Type*	*Message*
Error-reporting messages	3	Destination unreachable
	4	Source quench
	11	Time exceeded
	12	Parameter problem
	5	Redirection
Query messages	8 or 0	Echo request or reply
	13 or 14	Timestamp request or reply

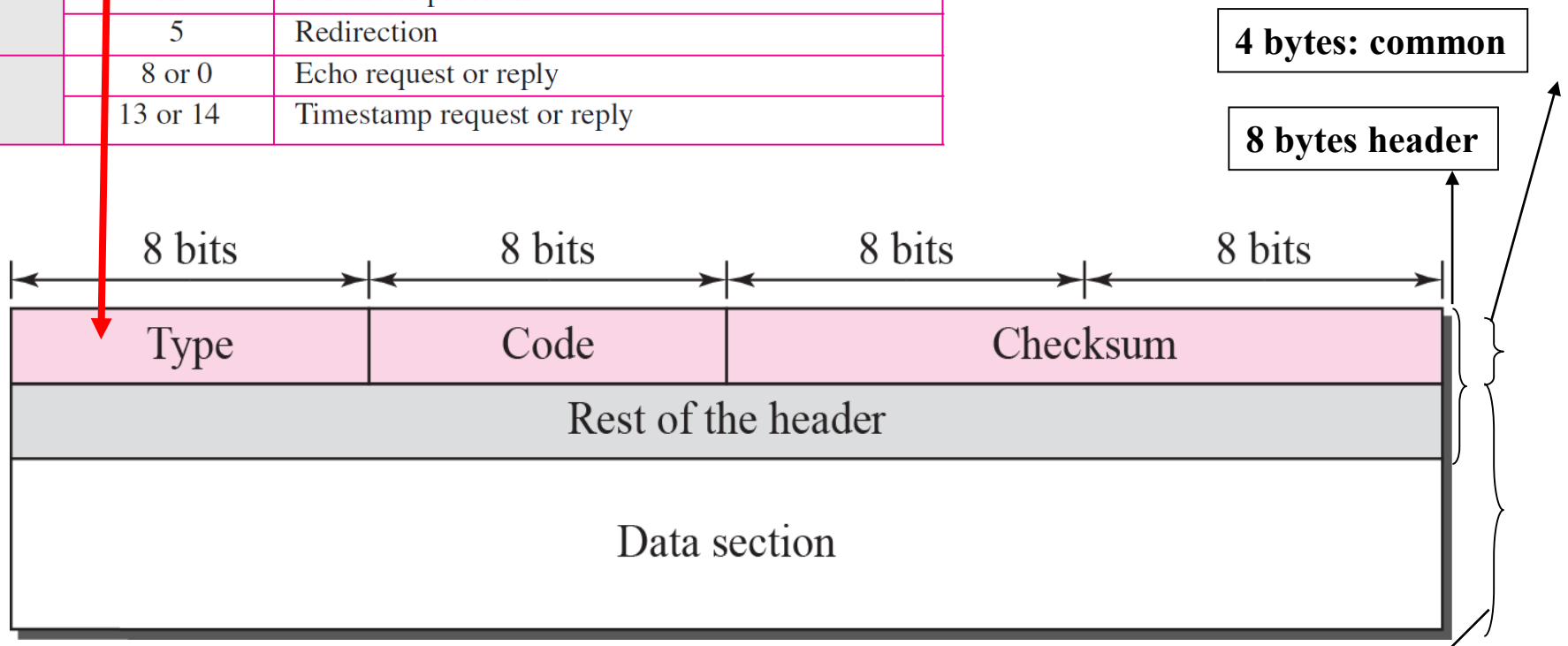


그림 9.3 ICMP 메시지의 일반 형식
(General format of ICMP messages)

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 오류 보고 메시지

ICMP는 언제나 최초의 발신지로 오류 메시지를 보고한다.

✓ **오류 보고 메시지 (Error Reporting Messages)**

- ICMP의 **주 임무 (main responsibilities)** 중 하나는 **오류를 보고 (report errors)**하는 것임
- 오류 검사와 오류 제어가 **IP의 관심사가 아니기 (not a concern of IP)** 때문에, ICMP가 설계되었음
- 그러나, ICMP는 **오류를 수정(정정)하지 않고 (not correct errors)**, 단지 보고 (simply report)를 할 뿐임
- 오류 수정 (error correction)은 **상위 계층 프로토콜에 맡겨 (left to the higher-level protocols)**짐
- ICMP 오류 보고 메시지의 생성
  - **라우터 (routers)** 또는 **목적지 호스트 (destination host)에 의해 생성**
- ICMP 오류 보고 메시지의 수신
  - **오직 발신지 호스트 (only the source host)에 의해 수신**
  - 왜냐하면, 데이터그램으로부터 **알 수 있는 경로에 대한 정보**는 **발신지와 목적지 IP 주소 (source and destination IP addresses) 뿐**이기 때문

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 오류 보고 메시지

✓ 다음은 **ICMP 오류 메시지 (error message)**에 대한 **중요한 사항들 (important points)**임

- **ICMP 오류 메시지를 전달하는 데이터그램 (datagram carrying an ICMP error message)**에 대해서는 ICMP 오류 메시지가 생성되지 않음
- **처음 단편이 아닌 (not the first fragment)** 단편화된 데이터그램에 대해서는 ICMP 오류 메시지가 생성되지 않음
- **멀티캐스트 주소 (multicast address)**를 가진 데이터그램에 대해서는 ICMP 오류 메시지가 생성되지 않음
- **127.0.0.0이나 0.0.0.0과 같은 특별한 주소 (special address)**를 가진 데이터그램에 대해서는 ICMP 오류 메시지가 생성되지 않음

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 오류 보고 메시지

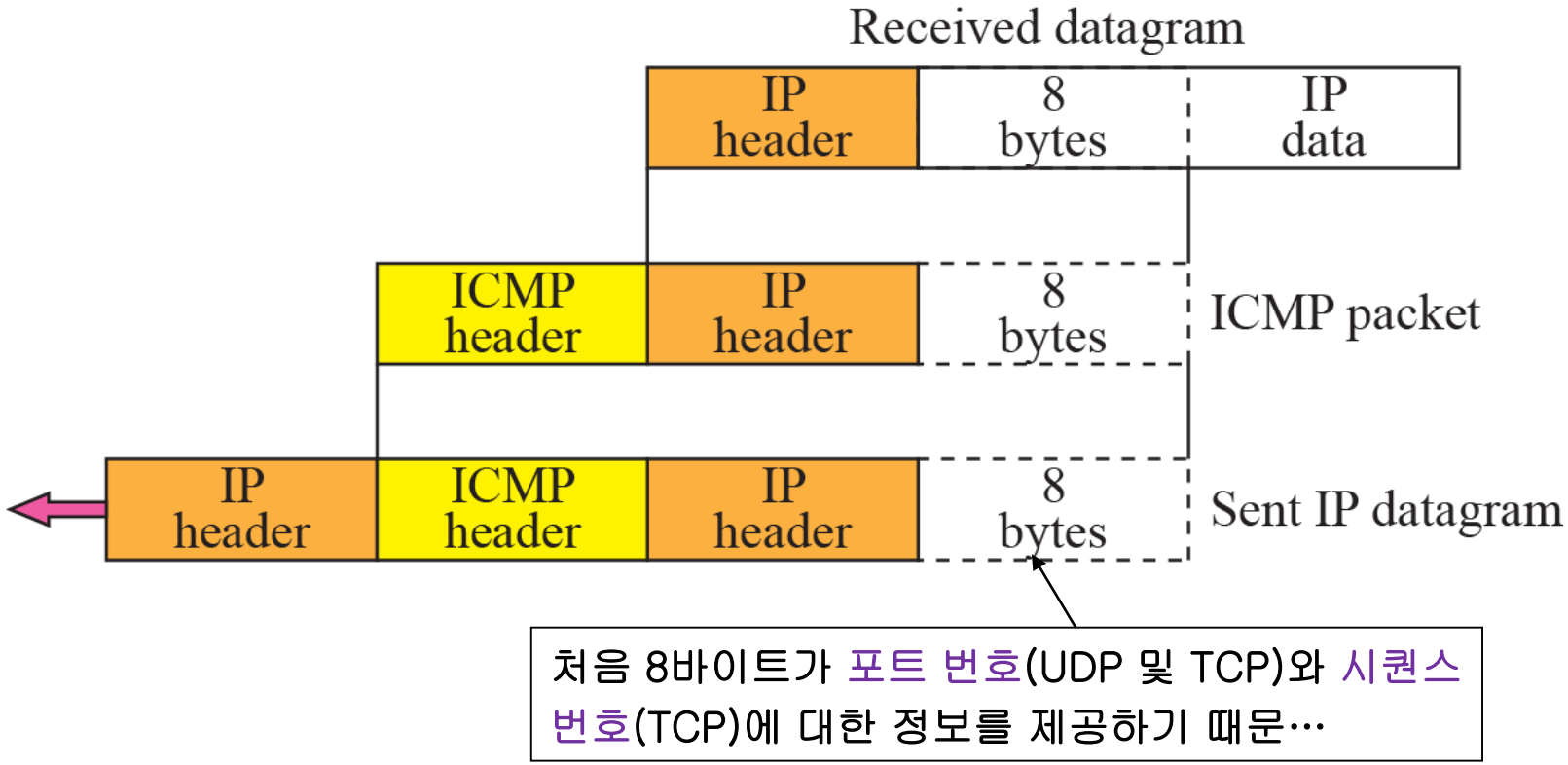


그림 9.5 오류 메시지를 위한 데이터 필드의 내용
(Contents of data field for the error message)

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 오류 보고 메시지

✓ 다섯 가지의 오류 유형 (five types of errors)이 처리됨

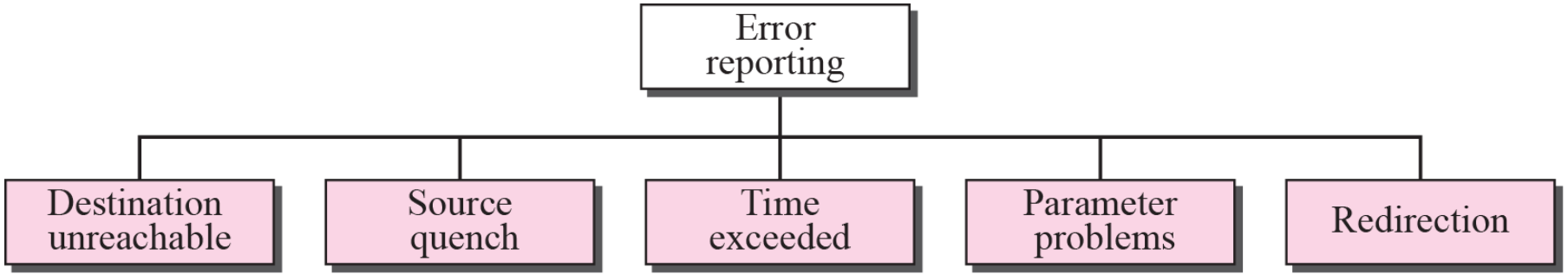


그림 9.4 오류 보고 메시지 (Error-reporting messages)

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 오류 보고 메시지

✓ **목적지 도달 불가 메시지 (Destination Unreachable Message)**

- 라우터가 데이터그램을 전달할 수 없을 (**cannot route**) 때, 또는
- 호스트가 데이터그램을 배달할 수 없을 (**cannot deliver**) 때

→ 데이터그램은 **폐기되고 (discarded)**

라우터나 호스트는 데이터그램을 처음으로 보낸 (initiate) **발신지 호스트 (source host)**에게 **목적지 도달 불가 메시지 (destination-unreachable message)**를 전송 (send back)함

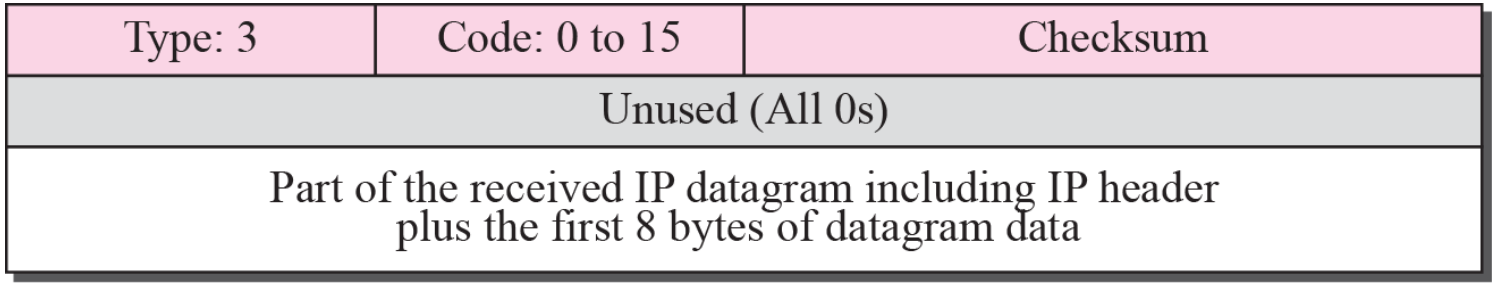


그림 9.6 목적지 도달 불가 메시지 형식
(Destination-unreachable format)

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 오류 보고 메시지

✓ **목적지 도달 불가 메시지 (Destination Unreachable Message)** - (계속)

- Code 0: 하드웨어 고장 등의 이유로, **네트워크에 도달할 수 없음 (network is unreachable)**
- Code 1: **호스트에 도달할 수 없음 (host is unreachable)**. 하드웨어 고장 때문일 수 있음
- Code 2: **프로토콜에 도달할 수 없음 (protocol is unreachable)**
  - IP 데이터그램은 UDP, TCP 등과 같은 상위 계층 프로토콜에 속한 데이터를 전달 가능
  - 만일, TCP와 같은 프로토콜에게 배달되어야 할 데이터그램을 목적지 호스트 (destination host)가 수신하였으나, 그 호스트에서 TCP 프로토콜이 동작하고 있지 않다면, Code 2가 전송됨

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 오류 보고 메시지

✓ **목적지 도달 불가 메시지 (Destination Unreachable Message)** - (계속)

- Code 3: **포트에 도달할 수 없음 (port is unreachable)**
  - 데이터그램이 향하고 있는 응용 프로그램 (프로세스)이 현재 수행 중이지 않음
- Code 4: 단편화가 필요 (**Fragmentation is required**)하지만,

  데이터그램의 **DF (do not fragment)** 필드가 1로 지정되어 있음
- Others

Code 2와 3의 목적지 도달 불가 메시지는
목적지 호스트에 의해서만 (only by the destination host)
생성될 수 있다.

나머지 목적지 도달 불가 메시지는
라우터에 의해서만 (only by routers) 생성될 수 있다.

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 오류 보고 메시지

✓ **목적지 도달 불가 메시지 (Destination Unreachable Message)** - (계속)

- 라우터가 목적지 도달 불가 메시지를 보고하지 않았다고 해서,
  데이터그램이 배달되었다는 것은 아님.
- 예제:
  - 데이터그램이 이더넷 네트워크를 지나가고 있다면,
    이더넷은 **확인 응답 메커니즘 (acknowledgement mechanism)을 제공하지 않으므로**
    데이터그램이 목적지 호스트나 다음 라우터에 배달되었다는 것을
    라우터는 알 수 없음

라우터는 패킷의 배달 **(delivery)**을 방해하는
모든 문제를 발견할 수 없다 **(cannot detect all problems).**

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 오류 보고 메시지

✓ **발신지 억제 메시지 (Source Quench Message)**

- IP 프로토콜은 **비연결형 프로토콜 (connectionless protocol)**임
- IP 프로토콜은 **흐름 제어 (flow control)**와 **혼잡 제어 (congestion control)**를 제공하지 **않음**
- 혼잡 (congestion)으로 인해 **데이터그램을 폐기 (discard)**하면, 라우터나 호스트는 데이터그램의 송신자에게 발신지 억제 메시지를 전송 (send)함
- 두 가지 목적
  - 첫째, 데이터그램이 **폐기 (discard)**되었음을 발신지 (source)에게 **알림 (inform)**
  - 둘째, 경로 상에서 **혼잡 (congestion)이 일어났고**, 발신지 (source)는 송신 과정을 **천천히 (또는 억제) 하여야 (should slow down (quench))** 한다는 것을 발신지에게 **경고 (warn)**함

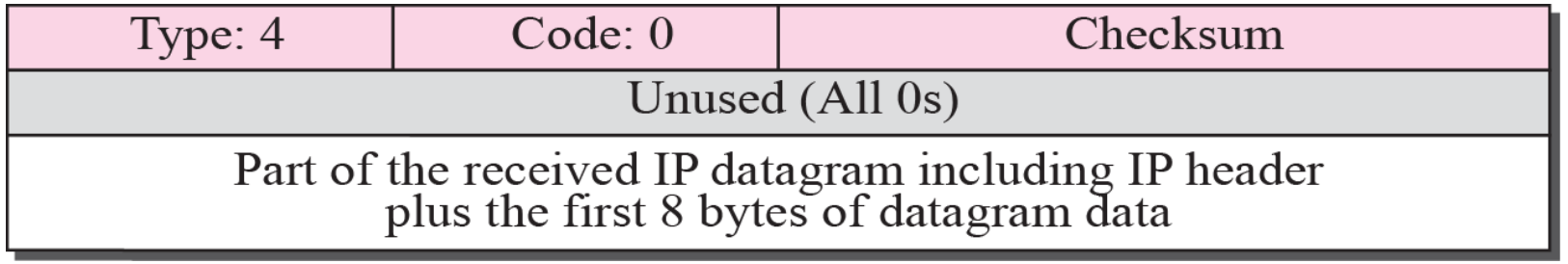


그림 9.7 발신지 억제 메시지 형식 (Source-quench format)

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 오류 보고 메시지

✓ **발신지 억제 메시지 (Source Quench Message)** - (계속)

IP 프로토콜에는 흐름 제어 **(no flow-control)**와
혼잡 제어 메커니즘 **(congestion-control mechanism)**
이 없다.

발신지 억제 **(source-quench)** 메시지는 라우터나 목적지 호스트에서
혼잡으로 인해 데이터그램이 폐기 **(discarded due to congestion)**되었음을
발신지에게 알린다 **(inform the source).**

발신지는 혼잡이 완화될 **(congestion is relieved)** 때까지
데이터그램을 송신하는 속도를 낮추어야 **(must slow down)** 한다.

혼잡으로 폐기되는 **(discarded due to congestion)** 데이터그램마다
발신지 억제 메시지가 전송 **(sent)**되어야 한다.

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 오류 보고 메시지

✓ **시간 경과 메시지 (Time Exceeded Message)**

➢ 이 메시지는 다음의 두 경우에 생성됨

- **수명 (TTL: Time To Live)**이 필드 값이 1 감소 후, 0이 되면, **라우터 (router)**는 데이터그램을 폐기하고, 시간 경과 메시지를 전송함 → **Code 0**
- 만약 타이머가 만료 (expire)되었음에도 불구하고, **아직 모든 단편 (fragments)이 도착하지 않았다면, 목적지 (destination)**는 모든 단편들을 폐기 (discard)하고, 시간 경과 메시지를 전송함 → **Code 1**

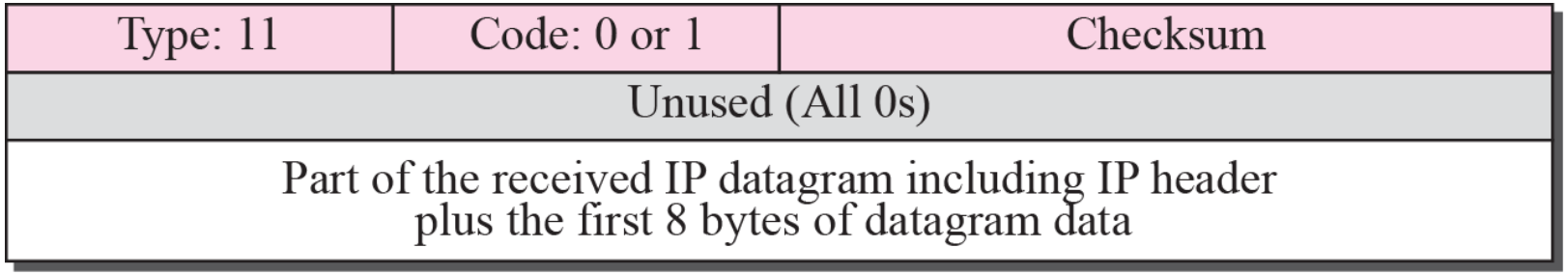


그림 9.8 시간 경과 메시지 형식 (Time-exceed message format)

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 오류 보고 메시지

✓ **시간 경과 메시지 (Time Exceeded Message)** - (계속)

라우터가 데이터그램의 수명 **(TTL)** 필드를 감소 **(decrement)**한 후,
이 값이 **0**이 되면 데이터그램을 폐기 **(discard)**하고
시간 경과 메시지 **(time-exceeded message)**를 원 발신지 **(original source)**에게 전송 **(send)**한다.

최종 목적지 **(final destination)**가 정해진 시간 내에 모든 단편 **(fragments)**을 받지 못했으면,
이미 수신된 단편들을 폐기 **(discard)**하고
원래의 발신지 **(original source)**로 시간 경과 메시지 **(time-exceeded message)**를 전송 **(send)**한다.

시간 경과 메시지에서 코드 **0 (code 0)**은 수명 **(TTL)** 필드의 값이 **0**이 되었음을 알리기 위해
오직 라우터 **(routers)**에 의해서만 사용된다.

코드 **1 (code 1)**은 모든 단편 **(fragments)**이 지정된 시간 내에 도착하지 않았음을 알리기 위해
오직 목적지 호스트 **(the destination host)**에 의해서만 사용된다.

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 오류 보고 메시지

매개변수 문제 메시지는 라우터 **(router)**나 목적지 호스트 **(destination host)**에 의해 생성될 수 있다.

✓ **매개변수 문제 메시지 (Parameter Problem Message)**

- 만약 라우터 (router)나 목적지 호스트 (destination host)가
  - 데이터그램의 **필드에서 불명확하거나 빠진 값을 발견 (discovers an ambiguous or missing value in any field)**하게 되면
  - 데이터그램을 폐기 (discard)하고 매개변수 문제 메시지를 전송 (send)함
- 두 가지 경우
  - **Code 0:** 헤더 필드 중에 불명료 (ambiguity)하거나 오류 (error)가 있는 필드가 존재하는 경우
  - **Code 1**: 옵션 중에서 요구되는 부분 (required part)이 빠진 (missing) 경우

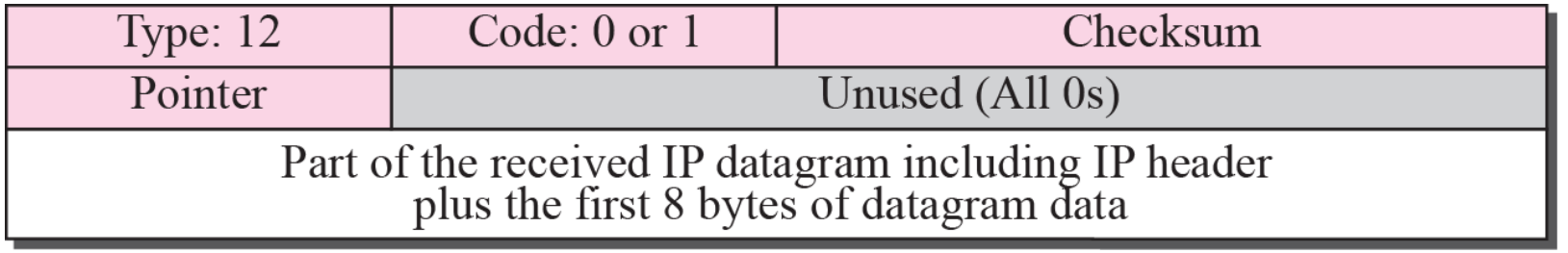


그림 9.9 매개변수 문제 메시지 형식 (Parameter-problem message format)

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 오류 보고 메시지

✓ **재지정 메시지 (Redirection Message)**

- **라우터들 (routers)**은 **라우팅 갱신 프로세스 (routing update process)**에 **참여**하여야 함
- 그러나, **효율성 (efficiency)**을 이유로, **호스트들 (hosts)**은 라우팅 갱신 프로세스 (routing update process)에 참여하지 않음
  - 왜냐하면, 호스트의 라우팅 테이블 (routing table)을 동적으로 갱신하면, 네트워크 **트래픽이 지나치게 많아지게 (unacceptable traffic)** 됨
- 그 결과, 다른 네트워크에 도달해야 하는 데이터그램을 전송할 때, **호스트 (host)**는 **잘못된 라우터 (wrong router)**에게 그 데이터그램을 **전송할 수** 있음
- **이 경우 (In this case)**, 데이터그램을 수신한 **라우터 (router)**는
  - 데이터그램을 **올바른 라우터 (correct router)**에게 **포워드 (forward)**한 뒤,
  - **호스트 (host)**에게 **재지정 메시지 (redirection message)**를 전송함

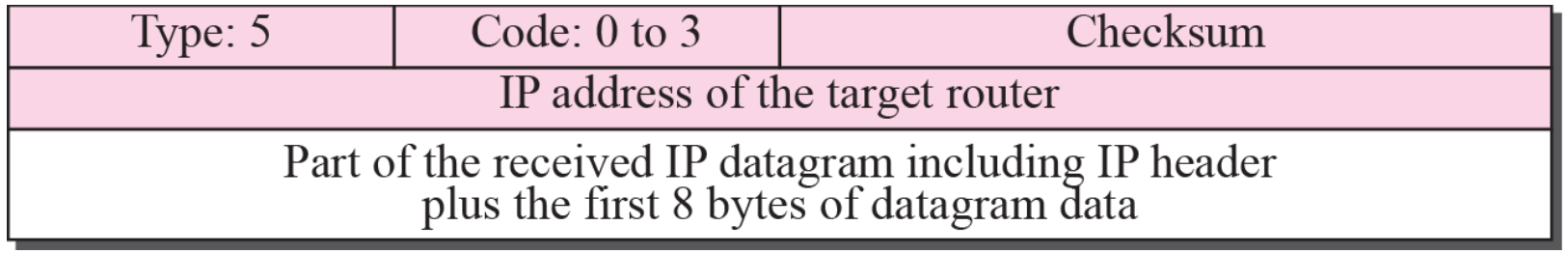


그림 9.11 재지정 메시지 형식 (Redirection message format)

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 오류 보고 메시지

이 경우, 라우터는 데이터그램을
폐기 (discard)하지 않는다.

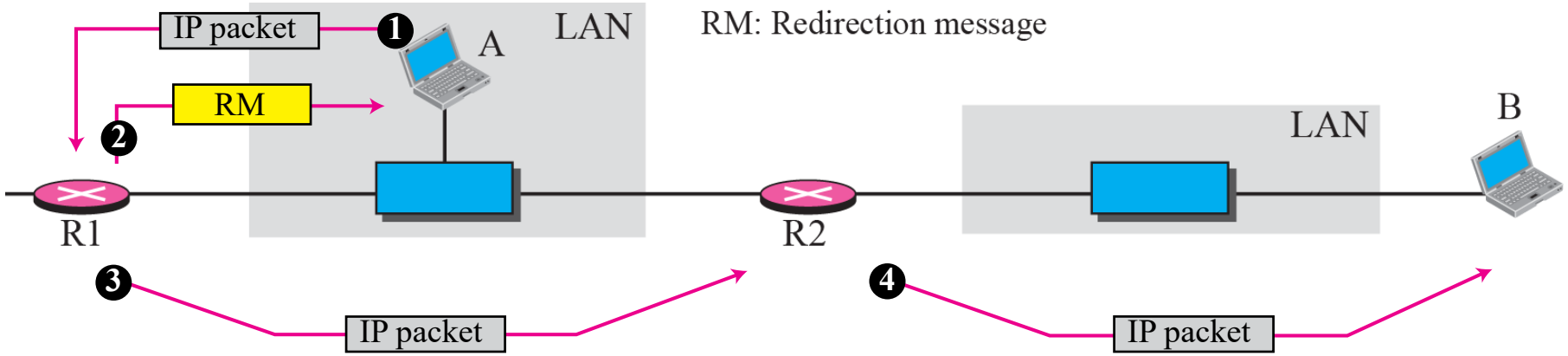


Figure 9.10 Redirection concept

호스트는 일반적으로 작은 라우팅 테이블로 시작 **(start)**하지만
점진적으로 증가되거나 갱신 **(gradually augmented and updated)**된다.

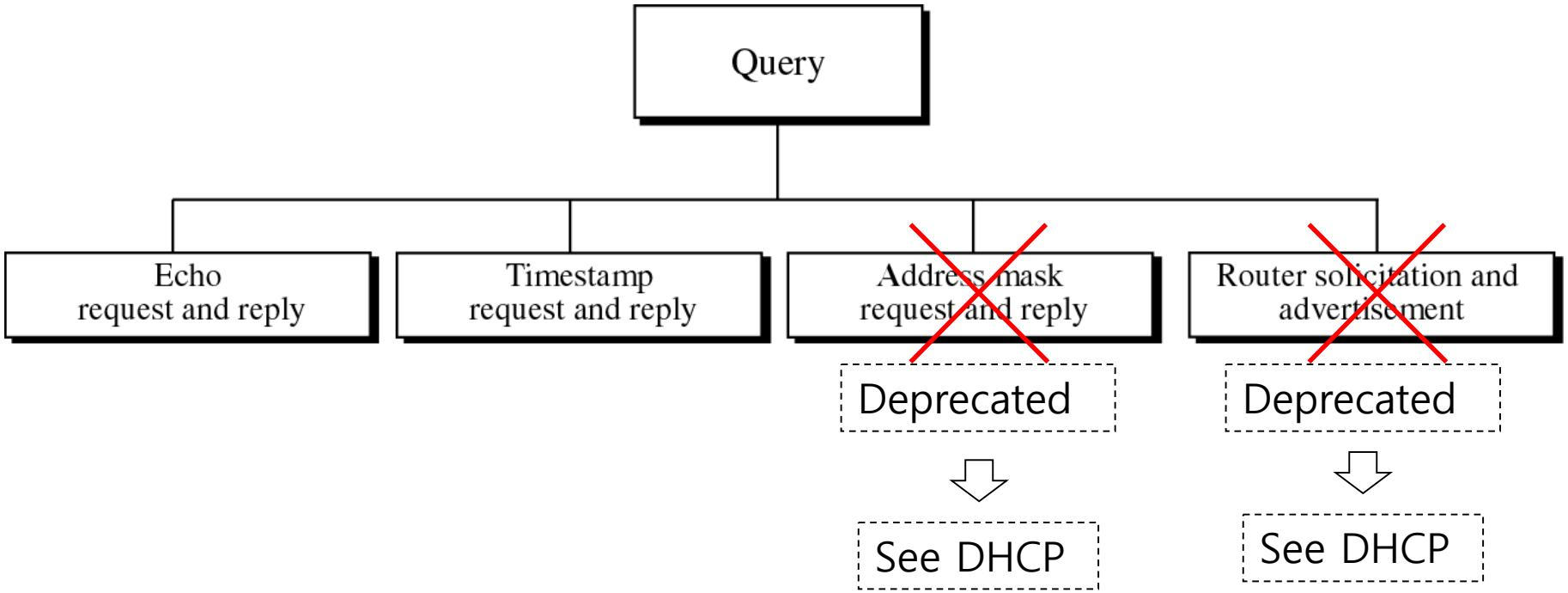
이러한 일을 수행하는 도구 중의 하나가
재지정 메시지 **(redirection message)**이다.

재지정 메시지 **(redirection message)**는
라우터 **(router)**로부터
같은 네트워크 **(same network)**에 있는 호스트 **(host)**로
전달 **(send)**된다.

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 질의 메시지

✓ 네 가지 질의 메시지 쌍 (Four pairs of query messages)



[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 질의 메시지

✓ **에코 요청과 응답 (Echo Request and Reply)**

- 이 메시지들은 **고장진단의 목적 (diagnostic purposes)**으로 설계되었음
- 이 메시지들의 조합은 **두 시스템 (호스트나 라우터)이 서로 통신 (communicate)할 수 있는지를 결정 가능**케 함
- 호스트나 라우터는 **에코 요청 (echo-request) 메시지**를 다른 호스트나 라우터에게 전송 (send)할 수 있음
- 에코 요청 메시지 (echo-request)를 수신 (receive)한 호스트나 라우터는 **에코 응답 (echo-reply) 메시지**를 **생성 (create)**하여 **원래의 송신자 (original sender)에게 되돌려 줌 (return)**
- ICMP 메시지는 IP 데이터그램에 캡슐화 (encapsulated)되기 때문에, 에코 응답 (echo-reply) 메시지를 수신했다는 것은 **다음을 증명 (proof) 하는 것**임
  - **송신자 (sender)와 수신자 (receiver)**가 IP 데이터그램을 사용하여 **서로 통신 (communicate)** 가능
  - **중간에 있는 라우터들 (intermediate routers)**도 **잘 동작 (working well)**함

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 질의 메시지

✓ **에코 요청과 응답 (Echo Request and Reply)** - (계속)

에코 요청 **(echo-request)** 메시지는 호스트나 라우터에 의해 전송 **(sent by a host or router)**될 수 있다.

에코 요청 메시지를 수신한 호스트나 라우터는 에코 응답 **(echo-reply)** 메시지를 전송한다.

에코 요청과 에코 응답 메시지는 네트워크 관리자 **(network managers)**가
IP 프로토콜의 동작을 검사 **(check)**하기 위하여 사용할 수 있다.

에코 요청과 에코 응답 메시지는 호스트의 도달 가능성 **(reachability)**을 테스트 **(test)**할 수 있다.

이것은 **ping** 명령 **(ping command)**을 수행함으로써 이루어진다.

```
prompt> ping [IP address or host name] <Enter>
```


[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 질의 메시지

✓ **에코 요청과 응답 (Echo Request and Reply)** - (계속)

Type 8: Echo request
Type 0: Echo reply

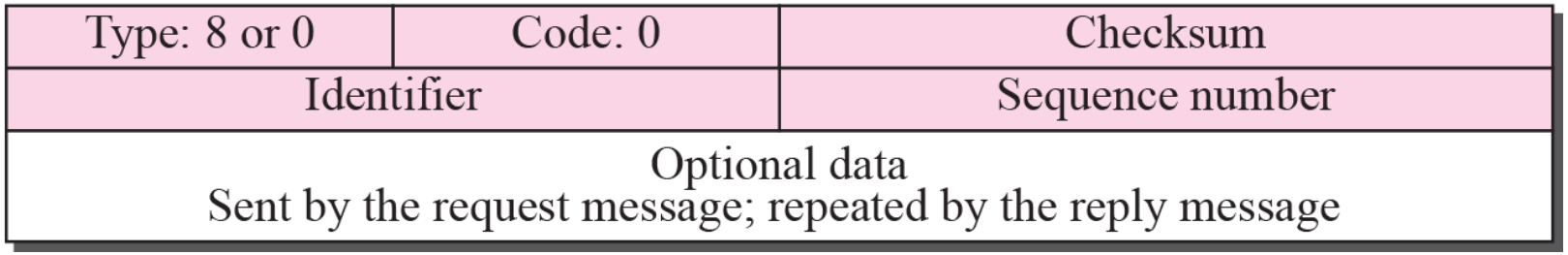


그림 9.12 에코 요청과 에코 응답 메시지 (Echo-request and echo-reply message)

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 질의 메시지

✓ **타임스탬프 요청과 응답 (Timestamp Request and Reply)**

➢ 이 메시지들은 IP 데이터그램이 두 개의 기계 (호스트나 라우터) 사이를 지나가는 데 필요한 **왕복 시간 (round-trip time)을 확인**하는데 사용

Type 13: request
Type 14: reply

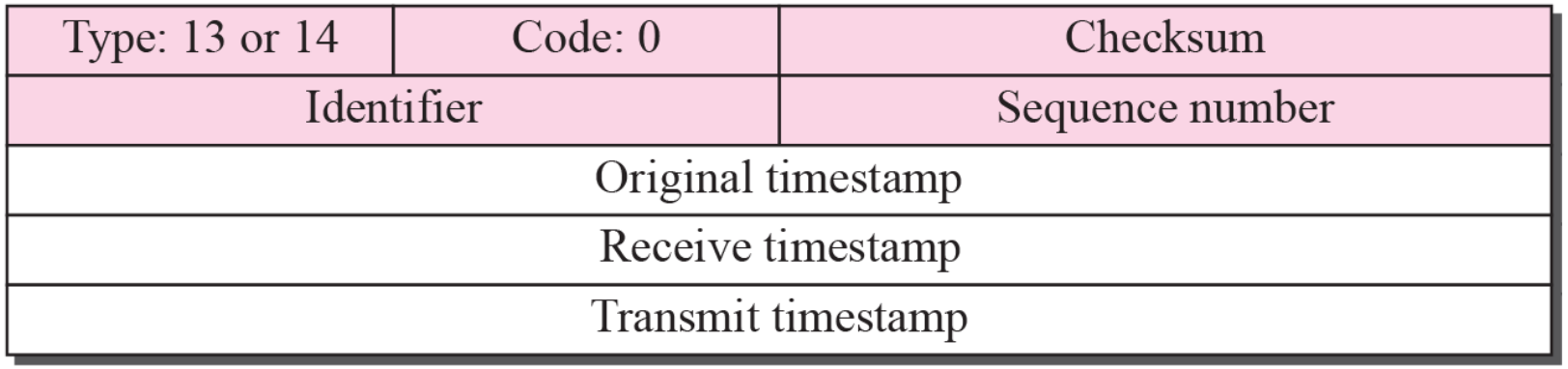


그림 9.13 타임스탬프 요청과 타임스탬프 응답 메시지 형식
(Timestamp-request and timestamp-reply message format)

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 질의 메시지

✓ **타임스탬프 요청과 응답 (Timestamp Request and Reply)** - (계속)

- 3개의 타임스탬프 필드 (three timestamp fields)들은 각각 32비트 길이를 가짐
- 표현 (Representation)
  - 각 필드에는, 그리니치 표준시 (Greenwich Mean Time)라고 불리는, 세계 표준시 (Universal Time) 자정 (midnight)으로부터의 시간을 밀리세컨드 (milliseconds) 단위로 표현한 값이 저장됨
  - 32비트는 0부터 4,294,967,295사이의 값을 표현할 수 있음
  - 그러나, 이 경우 타임스탬프 (timestamp)는 86,400,000 = 24 x 60 x 60 x 1000를 넘지 않음

    → 하루 (day)를 표현

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 질의 메시지

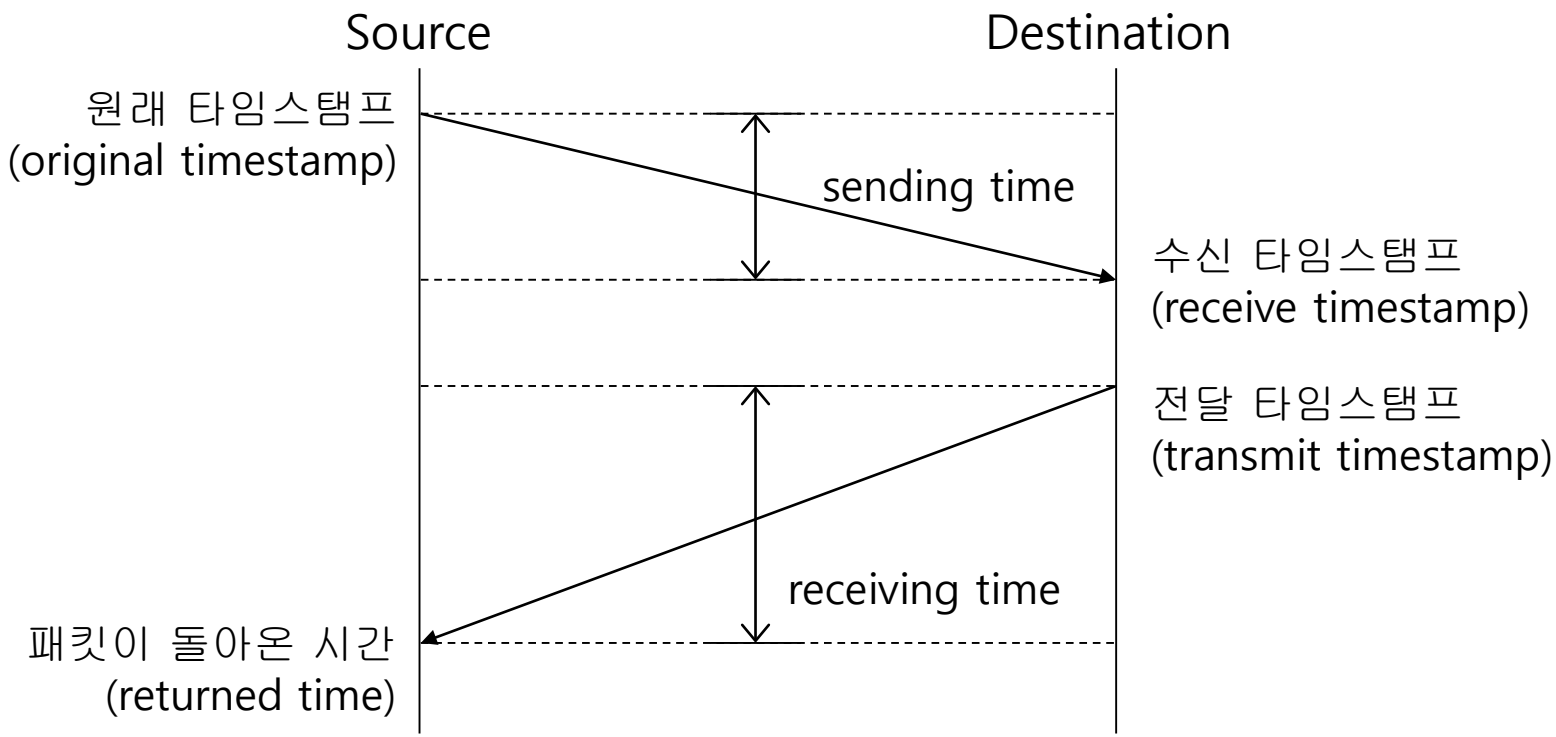
✓ **타임스탬프 요청과 응답 (Timestamp Request and Reply)** - (계속)

- 이 메시지들은 데이터그램이 발신지 (source)에서 목적지 (destination)로 가서, 다시 돌아오는 동안, 걸리는 **편도 또는 왕복 시간 (one-way or round-trip time)을 계산**하는 것에 사용 가능
- 공식 (formulas)
  - 송신시간 (sending time) = 수신 타임스탬프 (receive timestamp)
    – 원래 타임스탬프 (original timestamp)
  - 수신시간 (receiving time) = 패킷이 돌아온 시간 (returned time)
    – 전달 타임스탬프 (transmit timestamp)
  - 왕복시간 (round-trip time) = 송신시간 (sending time) + 수신시간 (receiving time)

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 질의 메시지

✓ **타임스탬프 요청과 응답 (Timestamp Request and Reply)** - (계속)



*** round-trip time = sending time + receiving time

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 질의 메시지

✓ **타임스탬프 요청과 응답 (Timestamp Request and Reply)** - (계속)

- 발신지와 목적지 기계 (시스템)의 **시계 (clock)가 동기화 (synchronized)되어 있어야만**, 송신시간과 수신 시간 (sending and receiving time) **계산이 정확 (accurate)**할 수 있음

  → 쉽지 않은 문제

- 그러나, 두 시계가 **동기화되어 있지 않다 (not synchronized) 하더라도**, **왕복시간의 계산 (round-trip calculation)은 항상 올바름 (correct)**

  → 각 시계 (clock)의 값이 왕복시간 계산에서 각각 **두 번 적용 (contribution twice)**되고,

  그 결과로 **동기화의 (시계) 차이점 (difference, 오차)이 서로 상쇄 (cancelling)**되기 때문

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 질의 메시지

✓ **타임스탬프 요청과 응답 (Timestamp Request and Reply)** - (계속)

- 예제 (example)
  - 원래 타임스탬프 (original timestamp): 46, 수신 타임스탬프 (receive timestamp): 59, 전달 타임스탬프 (transmit timestamp): 60, 패킷이 돌아온 시간 (return time): 67.
- 왕복시간 (Round-trip time) = (59 – 46) + (67 – 60) = 20 msec
- 편고시간 (One-way time) = 20 /2 = 10 msec
- 이 예에서 두 시계 (clock)는 3msec의 차이를 가지고 있다는 것을 알 수 있음
  - 시간 차 (Time difference) = 59 – (46 + 10) = 3 msec.

[from TCP/IP Protocol Suite Fourth Edition]

9.2 메시지 – 질의 메시지

✓ **타임스탬프 요청과 응답 (Timestamp Request and Reply)** - (계속)

시계가 동기화되어 있지 않더라도 **(not synchronized)**,
타임스탬프 요청과 타임스탬프 응답 메시지는
발신지와 목적지 사이의 왕복시간을 측정 **(calculate the round-trip time)**하기
위해 사용될 수 있다.

정확한 편도 시간 **(exact one-way time duration)**을 알 수 있다면,
타임스탬프 요청과 타임스탬프 응답 메시지를 사용하여
두 기계의 시계를 동기화 **(synchronize two clocks)**시킬 수 있다.

[from TCP/IP Protocol Suite Fourth Edition]

9.3 디버깅 도구

✓ Internet에서 디버깅 (debugging) 용도로 사용될 수 있는 **몇 가지 도구 (several tools)** 존재

✓ 디비깅 도구를 사용하여,

- 호스트나 라우터가 **정상적으로 작동 (alive and running)**하고 있는지 점검 가능
- 패킷이 **전달되는 경로를 추적 (trace the route)** 가능

✓ 디버깅을 위해 ICMP를 사용하는 **두 가지 도구 (two tools)**

- **ping**
- **traceroute**

[from TCP/IP Protocol Suite Fourth Edition]

9.3 디버깅 도구 – Topics

1) ping
2) traceroute

[from TCP/IP Protocol Suite Fourth Edition]

9.3 디버깅 도구 – ping – Example 9.2

✓ **ping 프로그램**을 사용하여, **fhda.edu 서버**를 테스트한 결과는 다음과 같음

```
$ ping fhda.edu
PING fhda.edu (153.18.8.1)   56 (84)  bytes of data.
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=0     ttl=62     time=1.91 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=1     ttl=62     time=2.04 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=2     ttl=62     time=1.90 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=3     ttl=62     time=1.97 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=4     ttl=62     time=1.93 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=5     ttl=62     time=2.00 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=6     ttl=62     time=1.94 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=7     ttl=62     time=1.94 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=8     ttl=62     time=1.97 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=9     ttl=62     time=1.89 ms
64 bytes from tiptoe.fhda.edu (153.18.8.1): icmp_seq=10    ttl=62     time=1.98 ms

--- fhda.edu ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10103 ms
rtt min/avg/max = 1.899/1.955/2.041 ms
```


[from TCP/IP Protocol Suite Fourth Edition]

9.3 디버깅 도구 – ping – Example 9.3

- ✓ ping 프로그램의 두 번째 예로, **adelphia.net이라는 메일 서버**가 정상적으로 작동 (alive and running)하고 있는지 확인한 결과는 다음과 같음
- ✓ 이 경우, **14개의 패킷을 보냈**지만, **13개의 응답만**이 돌아왔음
- ✓ 순서 번호 (sequence number) 13인 마지막 패킷이 돌아오기 전에, ping 프로그램을 인터럽트하였을 수도 있음

```
$ ping mail.adelphia.net
PING mail.adelphia.net (68.168.78.100) 56(84) bytes of data.
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=0    ttl=48    time=85.4 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=1    ttl=48    time=84.6 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=2    ttl=48    time=84.9 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=3    ttl=48    time=84.3 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=4    ttl=48    time=84.5 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=5    ttl=48    time=84.7 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=6    ttl=48    time=84.6 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=7    ttl=48    time=84.7 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=8    ttl=48    time=84.4 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=9    ttl=48    time=84.2 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=10   ttl=48    time=84.9 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=11   ttl=48    time=84.6 ms
64 bytes from mail.adelphia.net (68.168.78.100): icmp_seq=12   ttl=48    time=84.5 ms

--- mail.adelphia.net ping statistics ---
14 packets transmitted, 13 received, 7% packet loss, time 13129 ms
rtt min/avg/max/mdev = 84.207/84.694/85.469
```


[from TCP/IP Protocol Suite Fourth Edition]

9.3 디버깅 도구 – traceroute

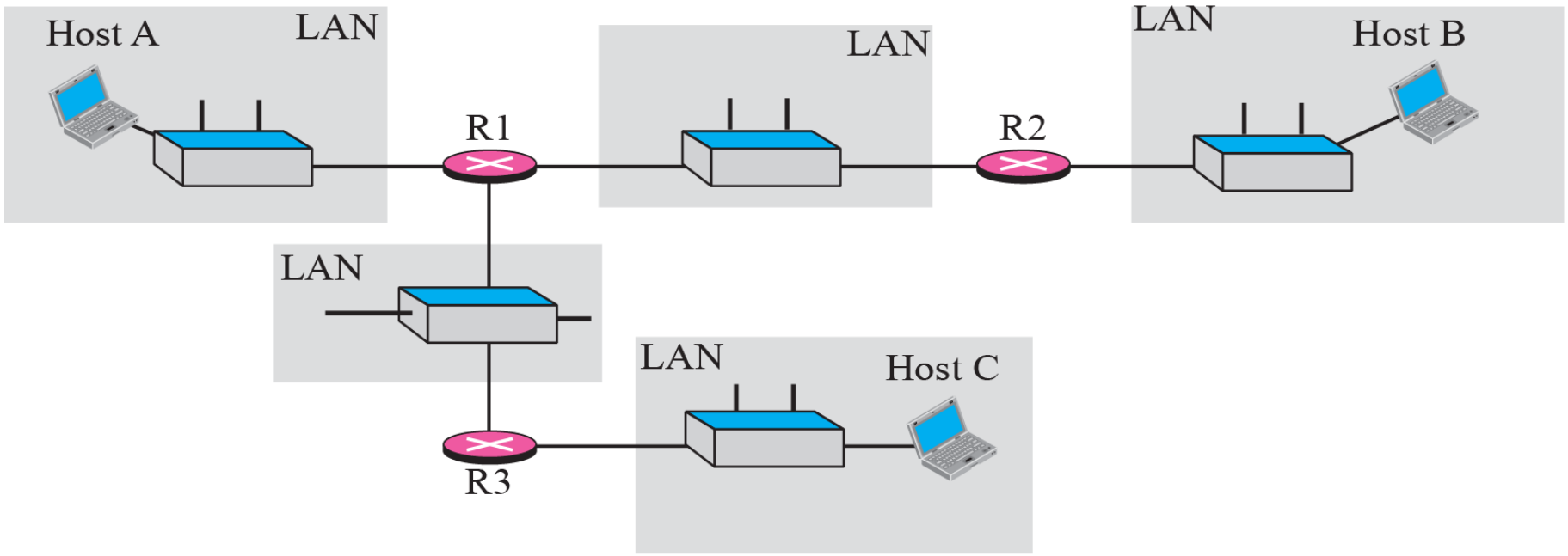


그림 9.15 traceroute 프로그램의 동작 (The traceroute program operation)

[from TCP/IP Protocol Suite Fourth Edition]

9.3 디버깅 도구 – traceroute – Example 9.4

✓ traceroute 프로그램을 사용하여, **voyager.deanza.edu** 컴퓨터와 **fhda.edu** 서버 사이의 **경로 (route)를 찾은 결과**는 다음과 같음

```
$ traceroute fhda.edu
traceroute to fhda.edu      (153.18.8.1), 30 hops max, 38 byte packets
1 Dcore.fhda.edu            (153.18.31.25)      0.995 ms      0.899 ms      0.878 ms
2 Dbackup.fhda.edu          (153.18.251.4)      1.039 ms      1.064 ms      1.083 ms
3  tiptoe.fhda.edu          (153.18.8.1)        1.797 ms      1.642 ms      1.757 ms
```


[from TCP/IP Protocol Suite Fourth Edition]

9.3 디버깅 도구 – traceroute – Example 9.5

✓ 이 예제에서는 **xerox.com** 까지의 더 긴 경로 (**longer route**)를 추적함

✓ 다음은 전체 경로의 일부를 보여줌

```
$ traceroute xerox.com
traceroute to xerox.com (13.1.64.93), 30 hops max, 38 byte packets
1  Dcore.fhda.edu      (153.18.31.254)     0.622 ms    0.891 ms    0.875 ms
2  Ddmz.fhda.edu       (153.18.251.40)     2.132 ms    2.266 ms    2.094 ms
3  Cinic.fhda.edu      (153.18.253.126)    2.110 ms    2.145 ms    1.763 ms
4  cenic.net           (137.164.32.140)    3.069 ms    2.875 ms    2.930 ms
5  cenic.net           (137.164.22.31)     4.205 ms    4.870 ms    4.197 ms
6  cenic.net           (137.164.22.167)    4.250 ms    4.159 ms    4.078 ms
7  cogentco.com        (38.112.6.225)      5.062 ms    4.825 ms    5.020 ms
8  cogentco.com        (66.28.4.69)        6.070 ms    6.207 ms    5.653 ms
9  cogentco.com        (66.28.4.94)        6.070 ms    5.928 ms    5.499 ms
```


[from TCP/IP Protocol Suite Fourth Edition]

9.3 디버깅 도구 – traceroute – Example 9.6

- ✓ 흥미로운 점은 **호스트가 자신에게 traceroute를 보낼 수 있다는 것**임
- ✓ 자신을 목적지 (destination)로 지정함으로써 가능함
- ✓ 예상하는 것과 같이, 패킷은 **루프백 주소 (loopback address)**로의 경로를 찾음

```
$ traceroute voyager.deanza.edu
traceroute to voyager.deanza.edu   (127.0.0.1), 30 hops max, 38 byte packets
1  voyager          (127.0.0.1)          0.178 ms          0.086 ms          0.055 ms
```


[from TCP/IP Protocol Suite Fourth Edition]

9.3 디버깅 도구 – traceroute – Example 9.7

- ✓ 마지막으로, traceroute 프로그램을 사용하여, **fhda.edu**와 **mhhe.com** (McGraw-Hill server) **사이의 경로**를 찾는 예제
- ✓ 이 경우, **전체 경로 (whole route)를 찾을 수 없음**.
- ✓ traceroute가 **5초 내에 응답을 받지 못하면**, 문제가 있음을 알리기 위하여 *** (asterisk)**를 **프린트**하고 다음 홉을 시도함

```
$ traceroute mhhe.com
traceroute to mhhe.com (198.45.24.104), 30 hops max, 38 byte packets
```

1	Dcore.fhda.edu	(153.18.31.254)	1.025 ms	0.892 ms	0.880 ms
2	Ddmz.fhda.edu	(153.18.251.40)	2.141 ms	2.159 ms	2.103 ms
3	Cinic.fhda.edu	(153.18.253.126)	2.159 ms	2.050 ms	1.992 ms
4	cenic.net	(137.164.32.140)	3.220 ms	2.929 ms	2.943 ms
5	cenic.net	(137.164.22.59)	3.217 ms	2.998 ms	2.755 ms
6	SanJose1.net	(209.247.159.109)	10.653 ms	10.639 ms	10.618 ms
7	SanJose2.net	(64.159.2.1)	10.804 ms	10.798 ms	10.634 ms
8	Denver1.Level3.net	(64.159.1.114)	43.404 ms	43.367 ms	43.414 ms
9	Denver2.Level3.net	(4.68.112.162)	43.533 ms	43.290 ms	43.347 ms
10	unknown	(64.156.40.134)	55.509 ms	55.462 ms	55.647 ms
11	mcleodusa1.net	(64.198.100.2)	60.961 ms	55.681 ms	55.461 ms
12	mcleodusa2.net	(64.198.101.202)	55.692 ms	55.617 ms	55.505 ms
13	mcleodusa3.net	(64.198.101.142)	56.059 ms	55.623 ms	56.333 ms
14	mcleodusa4.net	(209.253.101.178)	297.199 ms	192.790 ms	250.594 ms
15	eppg.com	(198.45.24.246)	71.213 ms	70.536 ms	70.663 ms
16	…	…	…	…	…

[from TCP/IP Protocol Suite Fourth Edition]

9.4 ICMP 패키지

✓ ICMP가 ICMP 메시지의 송신과 수신을 어떻게 처리하는지 설명하기 위하여, 다음의 **두 가지 모듈 (two modules)**로 구성된 **ICMP 패키지 (ICMP package)**를 살펴봄

- **입력 모듈 (input module)**
- **출력 모듈 (output module)**

[from TCP/IP Protocol Suite Fourth Edition]

9.4 ICMP 패키지

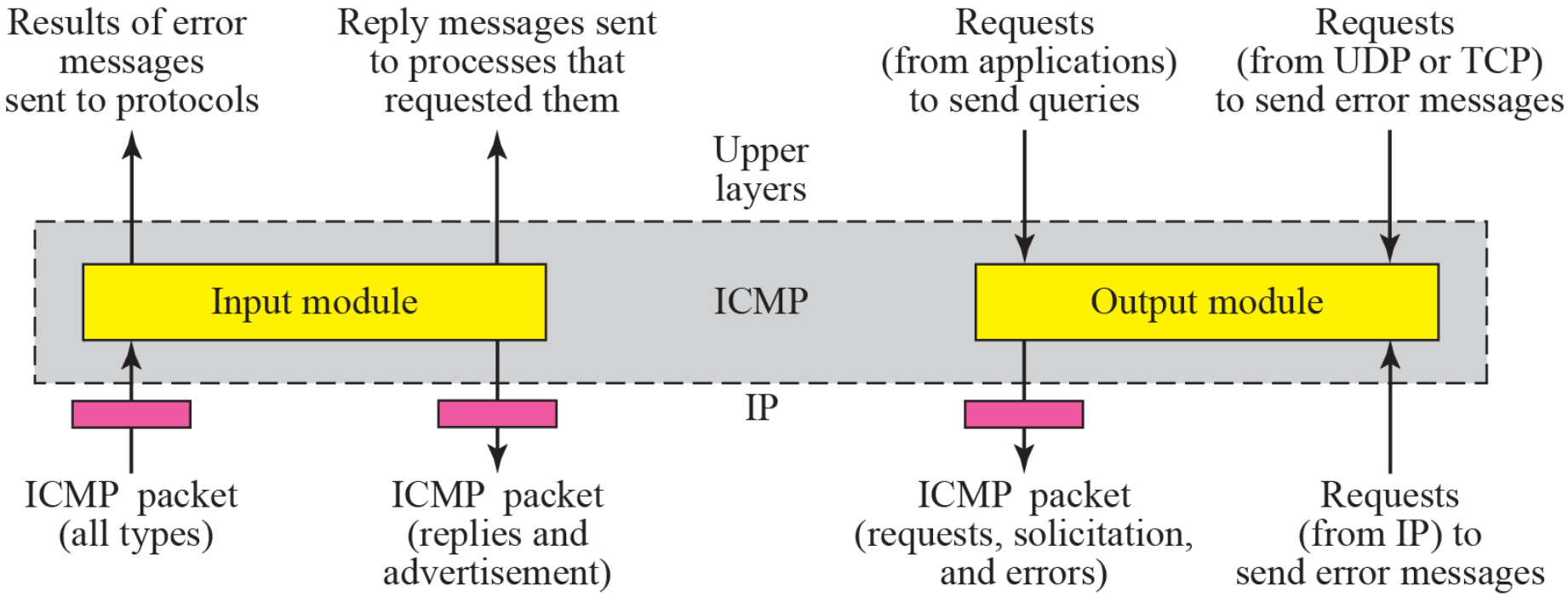


그림 9.16 ICMP 패키지 (ICMP package)

[from TCP/IP Protocol Suite Fourth Edition]