

TCP/IP 프로토콜

- 9장 ICMPv4, 10장 모바일 IP -

이 성 현(seonghyeon@pel.sejong.ac.kr)

세종대학교 프로토콜공학연구실

목 차

- 보충
- ICMPv4
- 모바일 IP

목 차

- 보충
- ICMPv4
- 모바일 IP

보충

- ICMPv4 (1/4)

- 질의 메시지

- 라우터 간청(Router Solicitation) 메시지

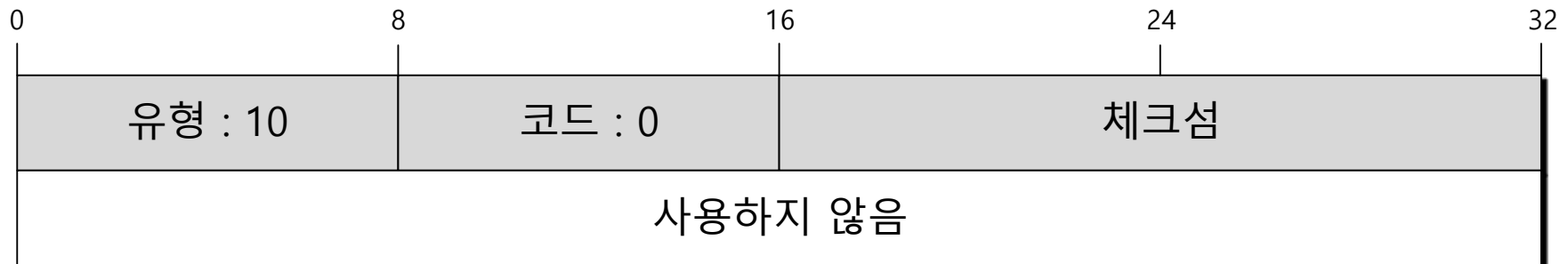
- 정의

- 호스트가 네트워크에 처음 연결되었을 때 주변 라우터에게 라우터 광고 메시지를 요청하기 위해 보내는 메시지

- 특징

- 호스트가 브로드캐스트 등을 통해 라우터 간청 메시지를 전송하면 해당 메시지를 수신한 라우터가 라우터 광고 메시지를 호스트에게 전송함
 - 현재는 DHCP가 네트워크 정보를 할당하여, DHCPDISCOVER 메시지를 사용하여 DHCP 서버에게 네트워크 정보 할당을 요청함

- 포맷



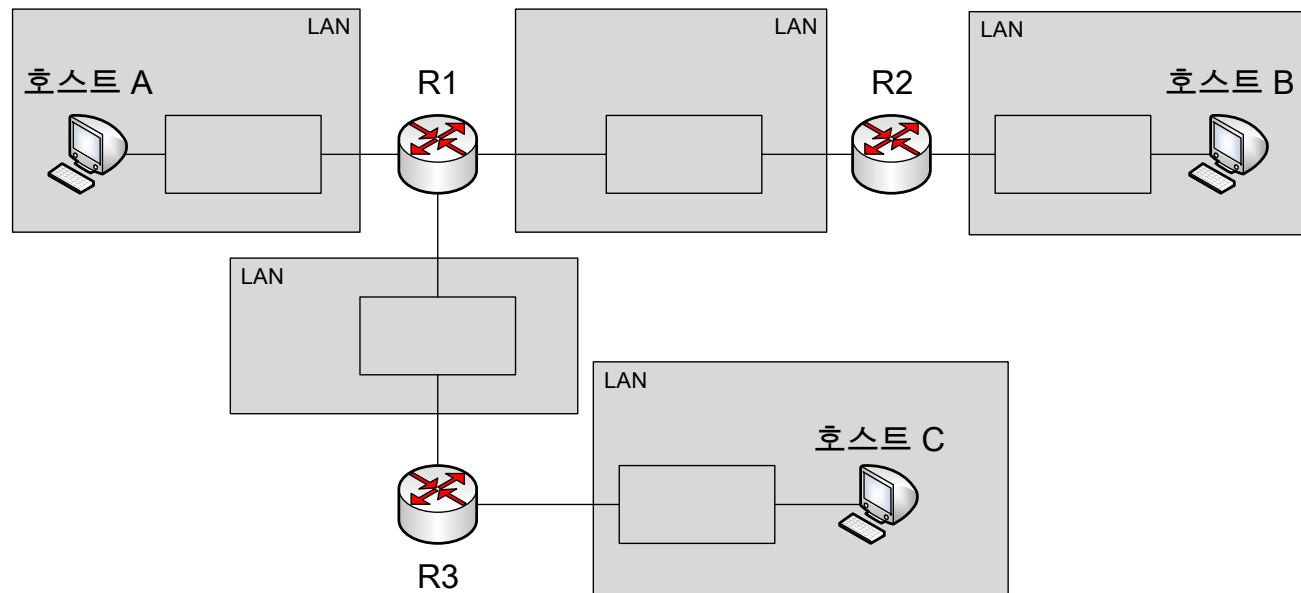
보충

- ICMPv4 (2/4)

- 디버깅 도구 (1/3)

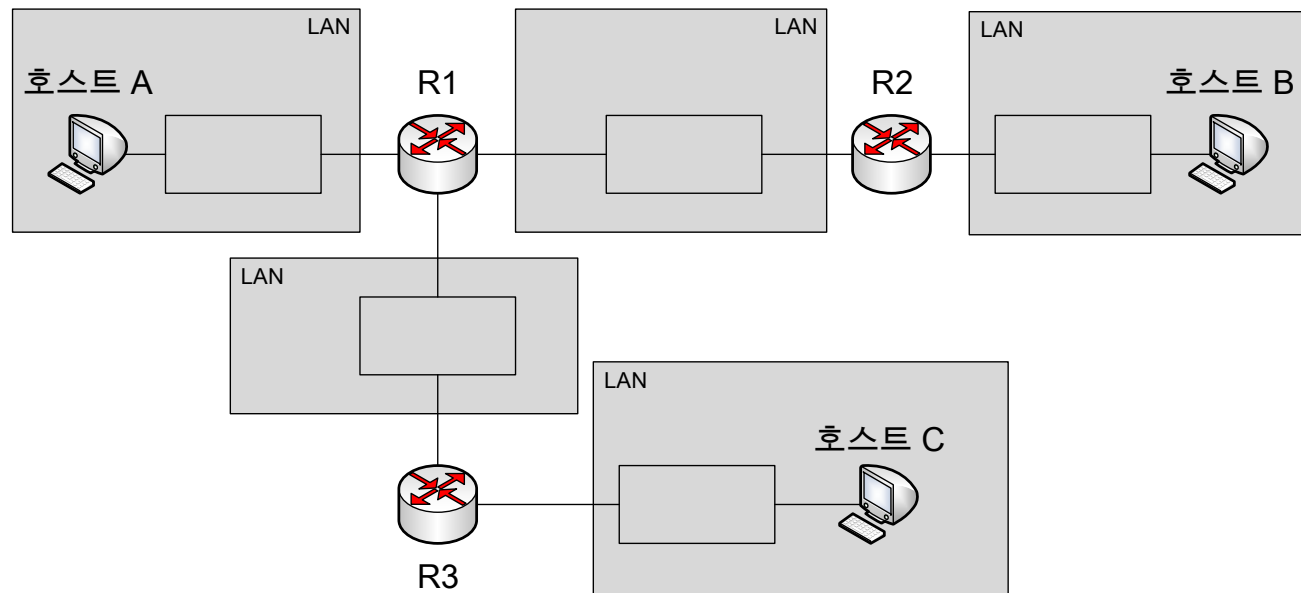
- Traceroute (1/3)

- 패킷이 발신지 호스트에서 목적지 호스트까지 가는 경로를 추적할 수 있음
 - 패킷의 TTL을 늘려가며 수신하는 ICMP 시간 초과 메시지를 통해 경로가 거쳐간 라우터의 주소와 왕복 시간을 얻음



보충

- ICMPv4 (3/4)
- 디버깅 도구 (2/3)
 - Traceroute (2/3)
 - UDP가 지원하지 않는 포트 번호를 사용하여 UDP 패킷을 보내어 목적지에서 ICMP 목적지 도달 불가 메시지를 발생시켜 목적지에 패킷이 도착했음을 확인함



보충

- ICMPv4 (4/4)
- 디버깅 도구 (3/3)
 - Traceroute (3/3)
 - 응답 메시지를 보내오지 않는 라우터에 대해서는 정보를 나타내지 않음

```
C:\Users\admin>tracert 8.8.8.8

최대 30홉 이상의
dns.google [8.8.8.8](으)로 가는 경로 추적:

  1      8 ms      14 ms      1 ms  GT-AX11000-7480 [192.168.50.1]
  2     15 ms       3 ms       4 ms  223.195.34.1
  3      6 ms       6 ms      10 ms  210.107.239.13
  4      *         *         *     요청 시간이 만료되었습니다.
  5      8 ms       4 ms       6 ms  210.107.239.1
  6      6 ms      13 ms       4 ms  211.168.5.117
  7      7 ms       3 ms      12 ms  1.213.140.17
  8      6 ms       4 ms       4 ms  1.208.140.5
  9     10 ms       5 ms       4 ms  1.208.144.13
 10      *         *         *     요청 시간이 만료되었습니다.
 11      8 ms       4 ms       5 ms  100.65.51.13
 12     39 ms      38 ms      39 ms  100.67.30.38
 13     42 ms      37 ms      38 ms  61.43.220.22
 14    231 ms     202 ms     209 ms  142.250.168.244
 15    198 ms     205 ms     206 ms  72.14.233.125
 16    245 ms     223 ms     204 ms  216.239.47.17
 17    205 ms     203 ms     202 ms  dns.google [8.8.8.8]

추적을 완료했습니다.
```

```
C:\Users\admin>curl ipinfo.io/223.195.34.1
{
  "ip": "223.195.34.1",
  "city": "Seoul",
  "region": "Seoul",
  "country": "KR",
  "loc": "37.5660,126.9784",
  "org": "AS9769 Sejong University",
  "postal": "03141",
  "timezone": "Asia/Seoul",
  "readme": "https://ipinfo.io/missingauth"
}
```

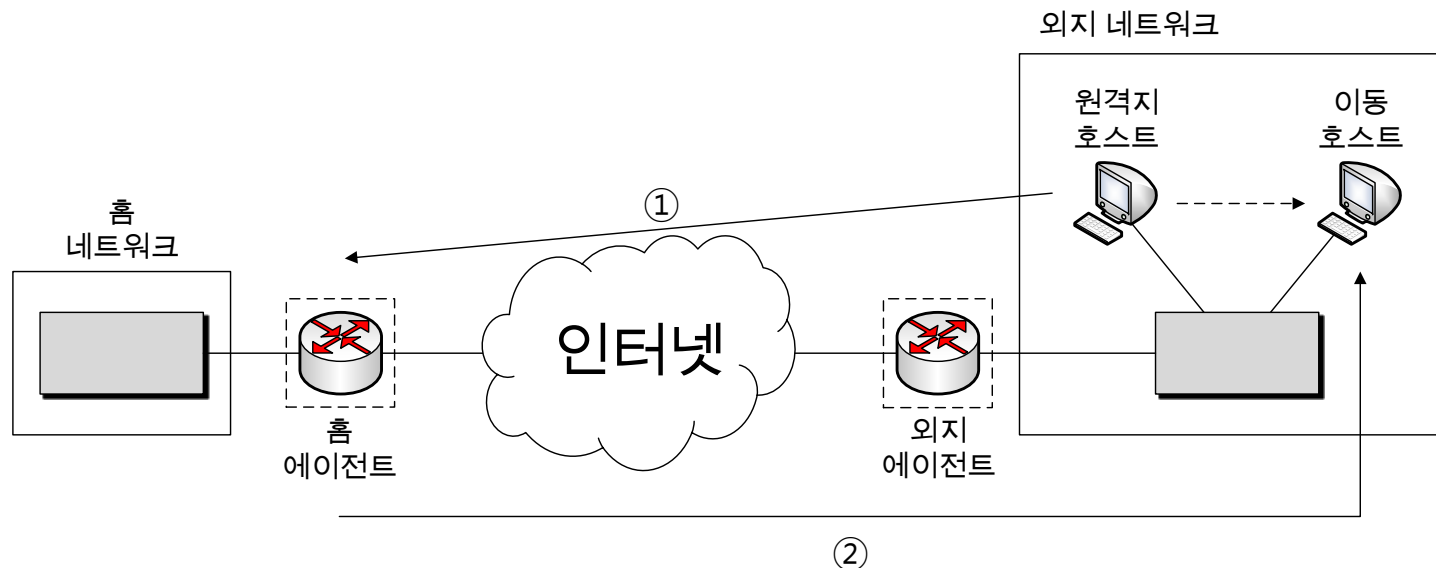
보충

• 모바일 IP

• 비효율성 문제 (1/3)

• 더블 크로싱(Double Crossing)

- 원격지 호스트가 자신과 같은 네트워크로 이동한 이동 호스트와 통신할 때 발생함
- 원격지 호스트가 같은 네트워크 내의 이동 호스트에게 패킷을 보낼 때 이동 호스트에게 바로 보내지 않고 홈 에이전트를 거쳐서 보냄



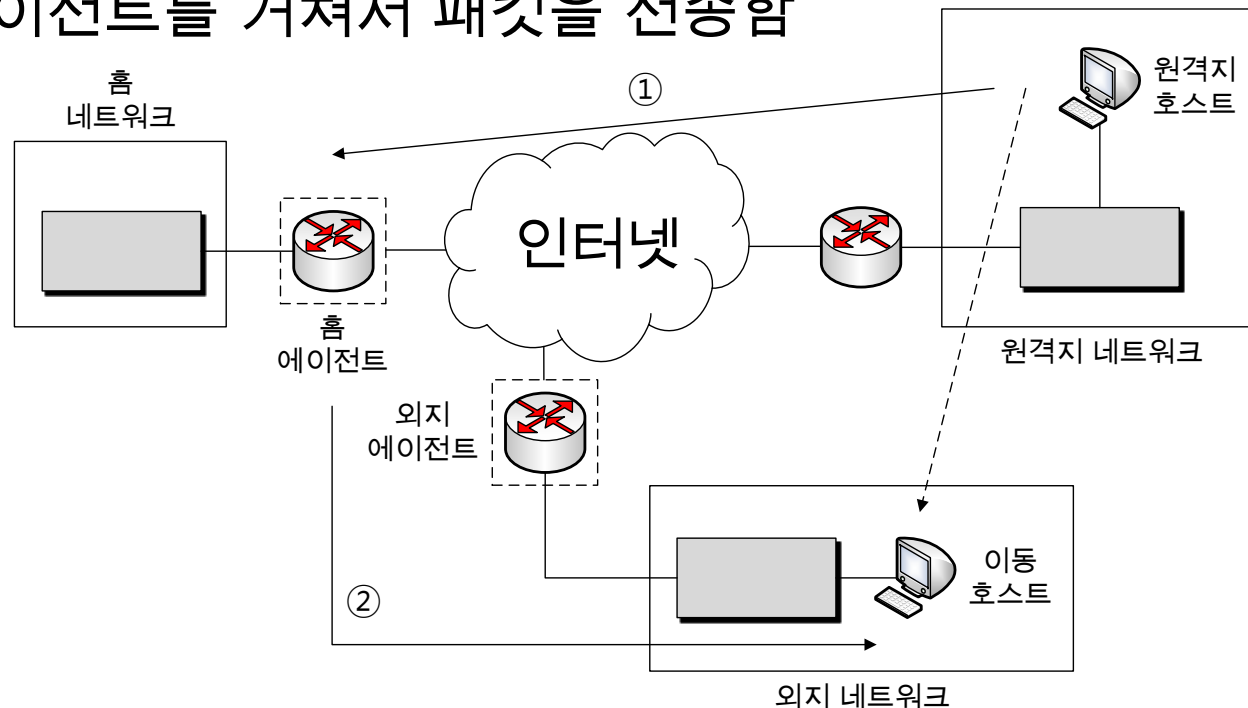
보충

• 모바일 IP

• 비효율성 문제 (2/3)

• 삼각형 라우팅(Triangle Routing)

- 원격지 호스트가 자신과 다른 네트워크에 연결되어 있는 이동 호스트와 통신할 때 발생함
- 원격지 호스트에서 이동 호스트까지의 경로가 존재함에도 홈 에이전트를 거쳐서 패킷을 전송함



보충

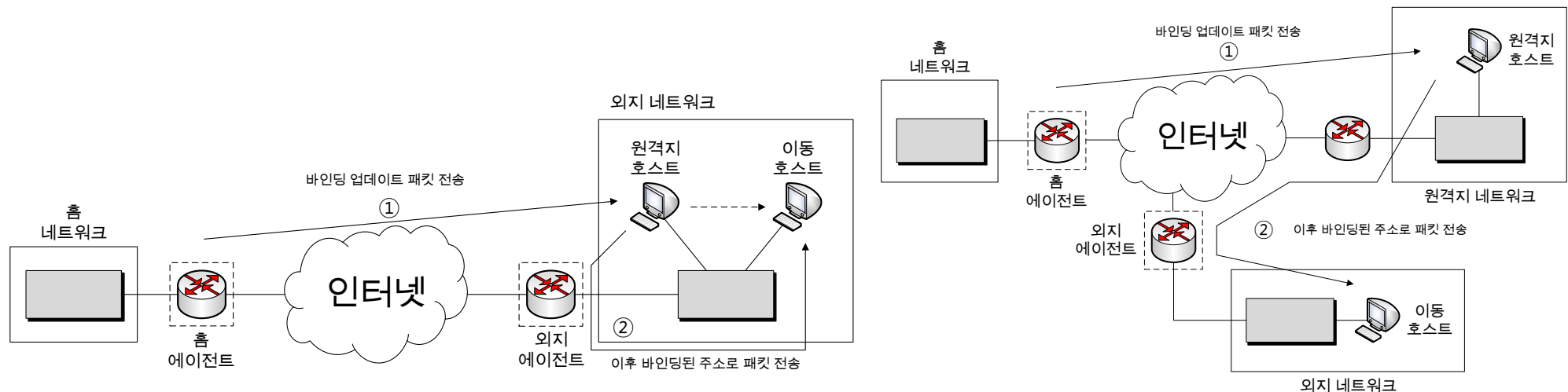
• 모바일 IP

• 비효율성 문제 (3/3)

• 해결 방안

- 원격지 호스트가 의탁 주소로 이동 호스트의 홈 주소에 바인드함

- 홈 에이전트가 보낸 바인딩 갱신(Binding Update) 메시지를 이용하여 이동 호스트로 가는 패킷이 의탁 주소로 바로 가게 함
- 이동 호스트가 이동하여 네트워크가 변경되면 캐시 정보가 무효화되므로 네트워크가 변경될 때마다 바인딩 갱신 메시지를 보내야 함
- 인증 등의 보안 기능을 추가하여 모바일 IPv6에서 공식적으로 정의됨



목 차

- 보충
- ICMPv4
- 모바일 IP

ICMPv4

- 개요

- IPv4는 최선형 전달(Best-effort Delivery)을 제공함
 - 전달 과정에서 손실되거나 지연, 경로 문제 등을 이유로 폐기되어도 이에 대한 피드백을 제공하지 않음
- ICMP (Internet Control Message Protocol)는 IP 프로토콜을 보조하기 위해 설계됨
 - 오류 보고, 네트워크 상태 및 정보 요청 기능을 제공함

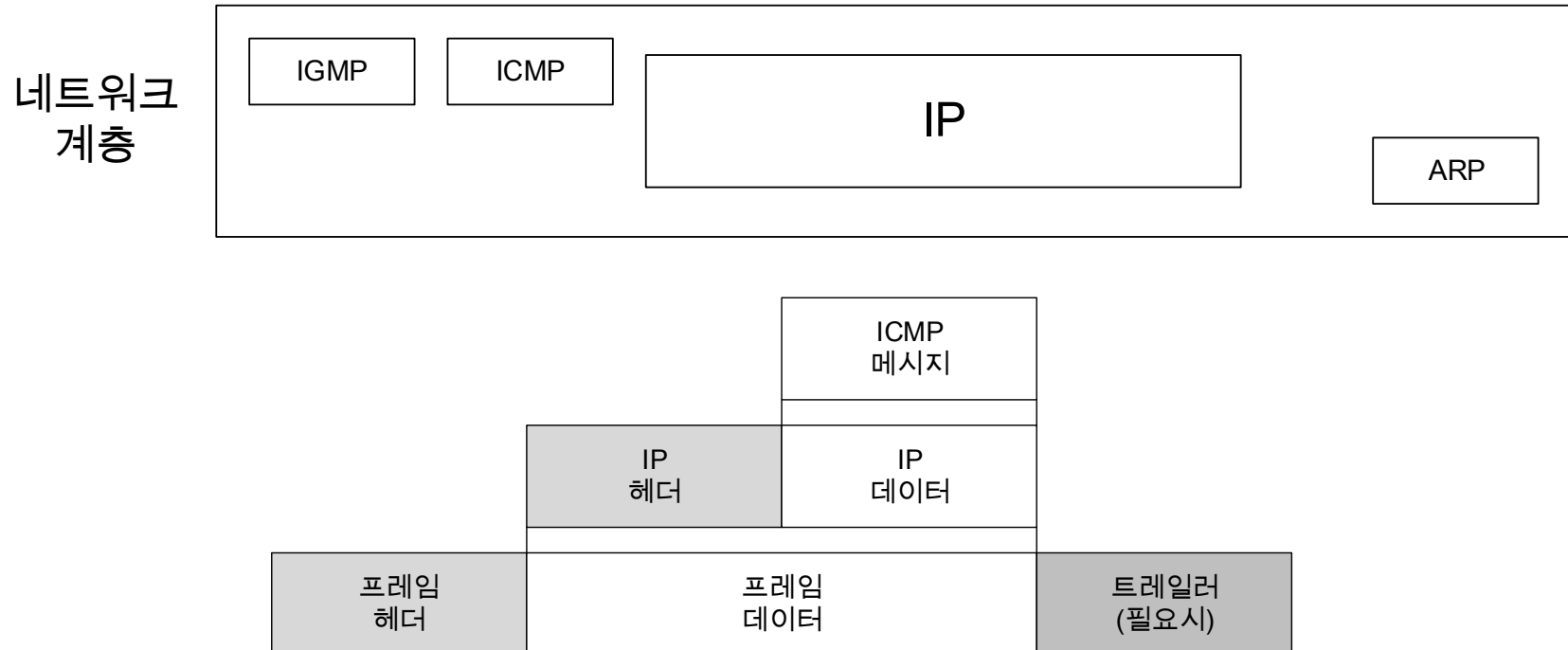
- 정의

- 오류 보고와 정보 요청 / 응답을 위한 메시지를 규정하는 네트워크 계층 프로토콜

ICMPv4

• 특징

- IP와 함께 동작하는 네트워크 계층 프로토콜임
- 메시지는 IP 패킷 내에 캡슐화(Encapsulation) 되어 전달됨
 - 해당 IP 패킷 헤더의 프로토콜 필드 값을 1로 하여 ICMP 메시지임을 나타냄



ICMPv4

• 메시지 유형

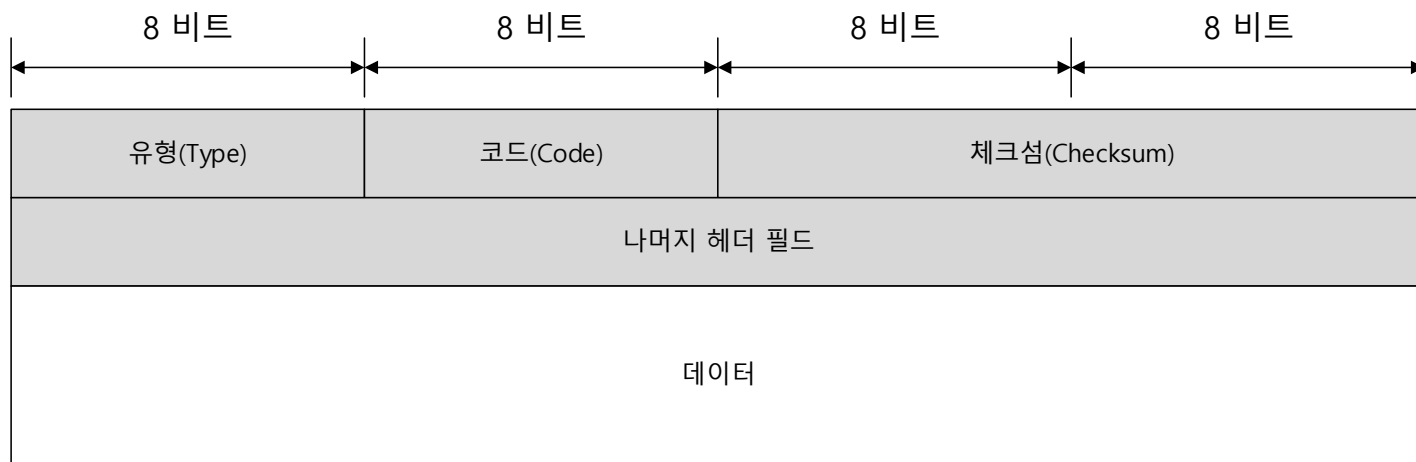
- 오류 보고 메시지는 라우터나 목적지 호스트가 IP 패킷을 처리하는 도중 탐지하는 문제를 보고함
- 질의 메시지는 호스트나 네트워크 관리자가 라우터나 다른 호스트로부터 특정 정보를 획득하기 위해 사용함

분류	유형	메시지
오류 보고 메시지 (Error-reporting)	3	목적지 도달 불가
	4	발신지 억제
	11	시간 경과
	12	매개변수 문제
	5	재지정
질의 메시지 (Query)	8 / 0	에코 요청 / 응답
	13 / 14	타임스탬프 요청 / 응답
	10 / 9	라우터 간청 / 광고
	15 / 16	정보 요청 / 응답
	17 / 18	주소 마스크 요청 / 응답

ICMPv4

- 메시지 포맷(Format)

- 8 바이트 헤더와 가변 길이의 데이터 부분을 가짐
- 첫 4 바이트는 1 바이트의 유형(Type), 1 바이트의 코드(Code), 2 바이트의 체크섬(Checksum)으로 공통임
- 오류 보고 메시지에서는 오류를 발생시킨 패킷의 정보가 데이터 부분에 들어감
- 질의 메시지에서는 질의 유형에 따른 추가 정보가 데이터 부분에 들어감



ICMPv4

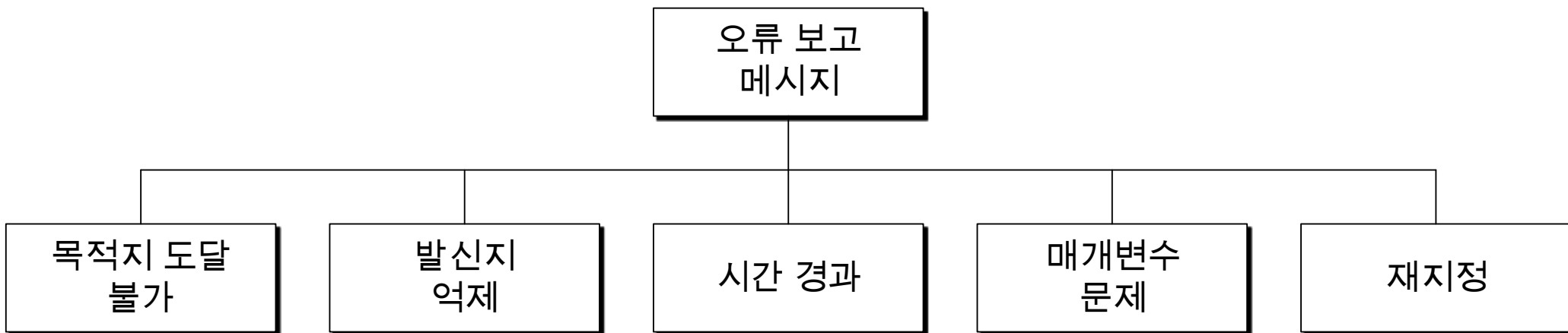
- 오류 보고 메시지 (1/10)

- 정의

- IP 패킷 전달 중 오류가 발생했음을 알리는 메시지

- 특징 (1/2)

- 오류를 수정하지 않고 상위 계층에 보고하기만 함
- 항상 최초 발신지로 전송됨
- ICMP 오류 보고 메시지에 대해서는 오류 보고 메시지가 생성되지 않음

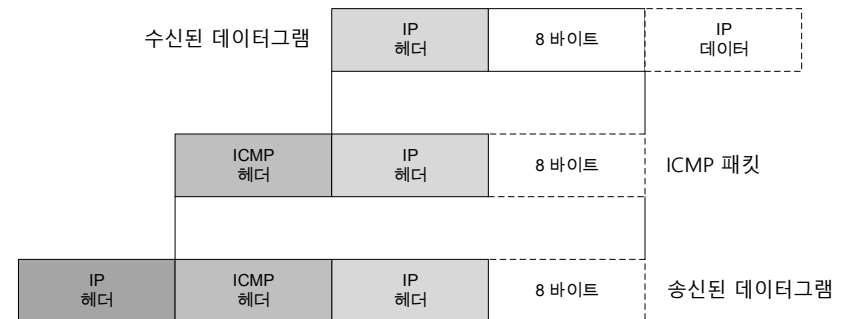
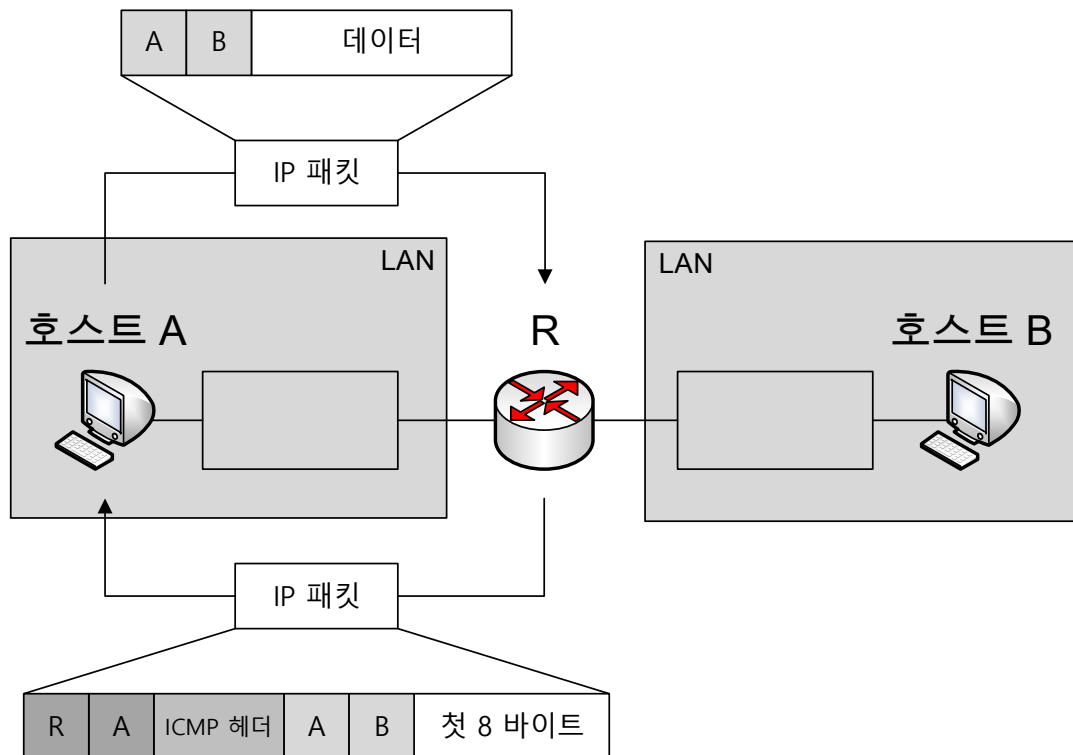


ICMPv4

- 오류 보고 메시지 (2/10)

- 특징 (2/2)

- 오류 보고 메시지의 데이터 부분에는 원본 데이터그램의 IP 헤더와 데이터그램 데이터의 첫 8 바이트가 포함됨



ICMPv4

- 오류 보고 메시지 (3/10)

- 목적지 도달 불가(Destination Unreachable) 메시지 (1/3)

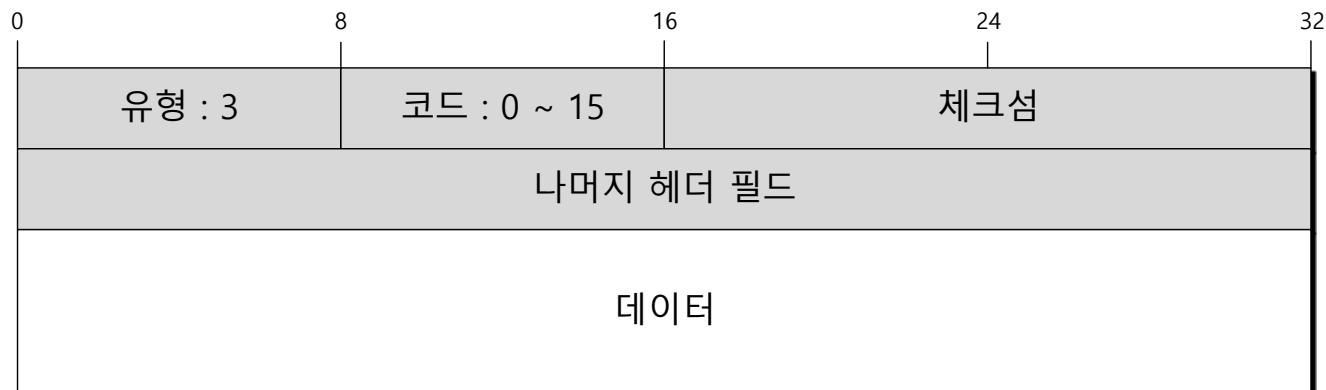
- 정의

- IP 패킷이 목적지에 도달할 수 없을 때 이를 알리기 위해 생성되는 메시지

- 특징

- 목적지에 도달하지 못한 데이터그램은 폐기되고 라우터나 호스트가 코드 필드에 폐기 이유를 표기하여 목적지 도달 불가 메시지를 전송함
 - 목적지 도달 불가 메시지를 받지 않았다고 해서 데이터그램의 전송이 보장되는 것은 아님

- 포맷



ICMPv4

- 오류 보고 메시지 (4/10)
 - 목적지 도달 불가 메시지 (2/3)
 - 코드 (1/2)
 - 코드 2, 3은 목적지 호스트에 의해서 생성되고 나머지 코드는 라우터에 의해 생성됨

코드 값	의미	설명
0	네트워크 도달 불가	지정된 네트워크로의 전달 경로가 사용 불가함
1	호스트 도달 불가	지정된 호스트로의 전달 경로가 사용 불가함
2	프로토콜 도달 불가	지정된 전송 프로토콜이 목적지 호스트의 전송 계층에서 지원되지 않음
3	포트 도달 불가	지정된 포트에서 실행되는 응용 프로그램이 없음
4	DF 설정으로 인한 단편화 불가	데이터그램을 단편화 해야하지만 DF(Do not Fragment) 필드가 설정되어 있어 단편화 할 수 없음
5	발신지 경로 실패	지정된 경로가 유효하지 않음
6	알려지지 않은 목적지 네트워크	목적지 네트워크에 대한 정보를 찾을 수 없음
7	알려지지 않은 목적지 호스트	목적지 호스트에 대한 정보를 찾을 수 없음

ICMPv4

- 오류 보고 메시지 (5/10)
- 목적지 도달 불가 메시지 (3/3)
 - 코드 (2/2)
 - 코드 2,3은 목적지 호스트에 의해서 생성되고 나머지 코드는 라우터에 의해 생성됨

코드 값	의미	설명
8	격리된 발신지 호스트	발신지 호스트가 네트워크에서 격리되어 통신할 수 없음
9	네트워크 차단	관리상의 이유로 네트워크에 대한 접근이 차단됨
10	호스트 차단	관리상의 이유로 목적지 호스트와의 통신이 차단됨
11	서비스 유형에 대해 네트워크 도달 불가	지정한 서비스 유형이 네트워크로의 전달 경로를 사용할 수 없음
12	서비스 유형에 대해 호스트 도달 불가	지정한 서비스 유형이 호스트로의 전달 경로를 사용할 수 없음
13	관리상의 이유로 차단	라우터가 관리 필터링으로 인해 패킷을 전달할 수 없음
14	호스트 우선순위 위반	요청된 우선순위가 목적지 호스트에 대해 허용되지 않음
15	우선순위 차단	네트워크 관리자가 설정한 최소 우선순위를 만족하지 못함

ICMPv4

- 오류 보고 메시지 (6/10)

- 발신지 억제(Source Quench) 메시지

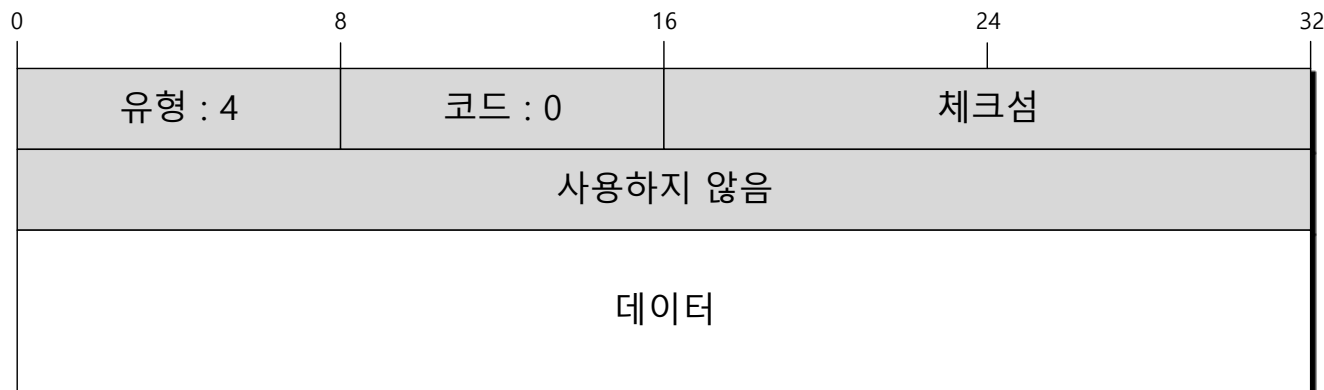
- 정의

- 혼잡으로 인해 데이터그램을 폐기할 때 송신 과정을 억제 해야함을 알리기 위해 생성되는 메시지

- 특징

- 폐기되는 데이터그램 하나 당 발신지 억제 메시지를 하나 생성하여 전송함
 - 혼잡이 해소 되었을 때 송신 속도를 회복할 수 있음을 알리는 메커니즘은 없음

- 포맷



ICMPv4

- 오류 보고 메시지 (7/10)

- 시간 경과(Time Exceeded) 메시지

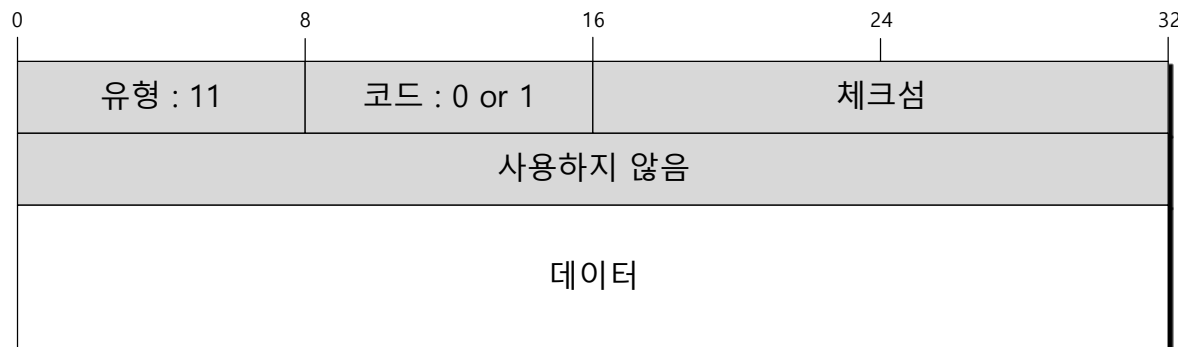
- 정의

- 수명(TTL, Time To Live) 필드 값이 0이 되었을 때 패킷의 수명이 만료되었음을 알리기 위해 생성되는 메시지

- 특징

- TTL이 0이 된 경우에는 코드 값을 0으로 하여 시간 경과 메시지를 전송함
 - 패킷이 단편화가 이루어진 경우, 단편 일부가 정해진 시간 내에 도착하지 않아서 이미 도착한 단편을 폐기할 때 코드 값을 1로 하여 시간 경과 메시지를 전송함

- 포맷



ICMPv4

- 오류 보고 메시지 (8/10)

- 매개변수 문제(Parameter Problem) 메시지

- 정의

- IP 헤더의 필드에 오류가 있어 패킷을 정상적으로 처리할 수 없음을 알리기 위해서 생성되는 메시지

- 특징

- 헤더 필드에 오류가 있을 경우, 문제가 발생한 바이트의 위치를 포인터 필드에 담아 코드 값 0으로 메시지를 전송함
 - 라우터나 호스트가 요구하는 필수 옵션이 없는 경우, 포인터 필드를 사용하지 않고 코드 값 1로 메시지를 전송함

- 포맷



ICMPv4

- 오류 보고 메시지 (9/10)

게이트웨이(Gateway)
다른 네트워크로 나가기 위한 출입구 노드

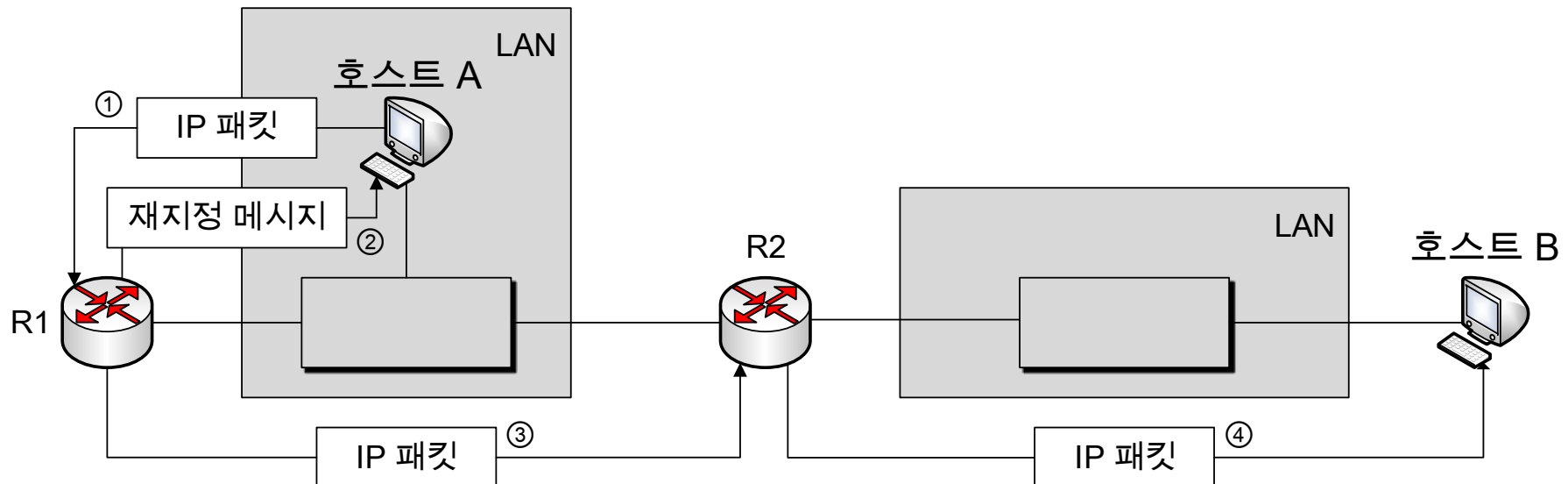
- 재지정(Redirect) 메시지 (1/2)

- 정의

- 발신지 호스트가 지정한 게이트웨이를 통한 경로가 최적이지 아닐 때 최적의 게이트웨이를 알리기 위해 생성되는 메시지

- 특징

- 라우터가 데이터그램을 폐기하지 않고 적절한 라우터에게 보낸 후 최적의 게이트웨이 정보를 재지정 메시지에 담아 전송함



ICMPv4

- 오류 보고 메시지 (10/10)
- 재지정 메시지 (2/2)
 - 포맷
 - 코드 값을 통해 재지정 유형을 나타냄



코드 값	의미	설명
0	네트워크 경로 재지정	목적지 네트워크에 대해 최적의 게이트웨이가 존재함
1	호스트 경로 재지정	목적지 호스트에 대해 최적의 게이트웨이가 존재함
2	특정 서비스 유형에 대한 네트워크 경로 재지정	특정 서비스 유형에 대해 목적지 네트워크로 가기 위한 최적의 게이트웨이가 존재함
3	특정 서비스 유형에 대한 호스트 경로 재지정	특정 서비스 유형에 대해 목적지 호스트로 가기 위한 최적의 게이트웨이가 존재함

ICMPv4

- 질의 메시지 (1/13)

- 정의

- 네트워크의 상태나 정보를 요청하거나 요청에 대해 응답하기 위해 생성되는 메시지

- 특징

- 대부분 요청에 따른 응답 메시지가 쌍으로 존재함
- 네트워크 진단 및 관리 용도로 사용됨
- 오류 발생 시 오류 보고 메시지가 생성될 수 있음

ICMPv4

- 질의 메시지 (2/13)

- 에코 요청 / 응답(Echo Request / Reply) 메시지

- 정의

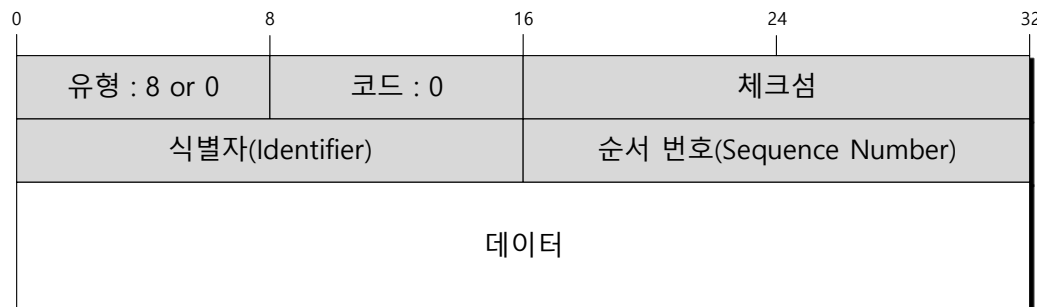
- 네트워크의 상태를 확인하기 위하여 주고 받는 메시지

- 특징

- 호스트의 도달 가능성(Reachability)을 검사할 수 있음
 - PING (Packet Internet Groper) 프로그램에서 주로 사용함

- 포맷

- 요청 메시지는 유형 8, 응답 메시지는 유형 0을 사용함
 - 식별자와 순서 번호를 사용하여 요청에 따른 응답 메시지를 구분함
 - 요청 메시지가 보낸 메시지 본문은 응답 메시지의 본문으로 사용됨



ICMPv4

- 질의 메시지 (3/13)
- 타임스탬프 요청 / 응답(Timestamp Request / Reply) 메시지 (1/4)
 - 정의
 - 네트워크의 시간 동기화와 지연 시간 측정을 위해 주고 받는 메시지
 - 특징
 - 세계 표준시를 기준으로 Milliseconds 단위로 시간을 기입하여 전송함
 - 메시지 내 타임스탬프 필드들의 값을 이용하여 시간 오차나 왕복 지연을 계산할 수 있음

ICMPv4

- 질의 메시지 (4/13)

- 타임스탬프 요청 / 응답 메시지 (2/4)

- 포맷

- 요청 메시지는 유형 13, 응답 메시지는 유형 14를 사용함
 - 식별자와 순서 번호를 사용하여 요청에 따른 응답 메시지를 구분함
 - 오리지널 타임스탬프에는 요청을 보낸 시각을 삽입함
 - 수신 타임스탬프에는 요청을 받은 시각을 삽입함
 - 전송 타임스탬프에는 응답을 보낸 시각을 삽입함

0	8	16	24	32
유형 : 13 or 14		코드 : 0	체크섬	
식별자			순서 번호	
오리지널 타임스탬프(Original Timestamp)				
수신 타임스탬프(Receive Timestamp)				
전송 타임스탬프(Transmit Timestamp)				

ICMPv4

- 질의 메시지 (5/13)
- 타임스탬프 요청 / 응답 메시지 (3/4)
 - 계산 (1/2)
 - 송신 시간 = 수신 타임스탬프 - 오리지널 타임스탬프
 - 수신 시간 = 패킷이 돌아온 시간 - 전송 타임스탬프
 - 왕복 시간 = 송신 시간 + 수신 시간

타임스탬프 요청 / 응답 메시지를 통해 다음과 같은 정보를 얻었을 때, 왕복 시간을 구하여라

- 오리지널 타임스탬프 : 46, 수신 타임스탬프 : 59, 전송 타임스탬프 : 60, 패킷 도착 시간 : 67

- 송신 시간 = 수신 타임스탬프 - 오리지널 타임스탬프 = $59 - 46 = 13\text{ms}$
- 수신 시간 = 패킷이 돌아온 시간 - 전송 타임스탬프 = $67 - 60 = 7\text{ms}$
- 왕복 시간 = 송신 시간 + 수신 시간 = $13 + 7 = 20\text{ms}$

∴ 왕복 시간 = 20ms

ICMPv4

- 질의 메시지 (6/13)
- 타임스탬프 요청 / 응답 메시지 (4/4)
 - 계산 (2/2)
 - 시간 오차 = 수신 타임스탬프 - (오리지널 타임스탬프 + 편도 시간)
 - 편도 시간 = 왕복 시간 / 2

타임스탬프 요청 / 응답 메시지를 통해 다음과 같은 정보를 얻었을 때, 시간 오차를 구하여라

- 오리지널 타임스탬프 : 46, 수신 타임스탬프 : 59, 전송 타임스탬프 : 60, 패킷 도착 시간 : 67
- 편도 시간 = 왕복 시간 / 2 = 20 / 2 = 10ms
- 시간 오차 = 수신 타임스탬프 - (오리지널 타임스탬프 + 편도 시간)
= 59 - (46 + 10) = 3ms

∴ 시간 오차 = 3ms

ICMPv4

- 질의 메시지 (7/13)

DHCP (Dynamic Host Configuration Protocol)
호스트에게 네트워크 설정 정보를 할당하는 프로토콜

- 라우터 광고(Router Advertisement) 메시지 (1/2)

- 정의

- 라우터가 자신의 네트워크 정보를 알려주기 위해 보내는 메시지

- 특징

- 라우터는 같은 네트워크 내 호스트들에게 주기적으로 라우터 광고 메시지를 전송함
 - 호스트가 어떤 라우터를 게이트웨이로 사용할지 알기 위해 사용된 메시지 였으나 현재는 DHCP가 자동으로 게이트웨이를 할당함
 - 공격자가 가짜 라우터 광고 메시지를 보내 중간자 공격이나 서비스 거부 공격에 악용할 가능성이 있기 때문에 거의 사용되지 않음

ICMPv4

- 질의 메시지 (8/13)
- 라우터 광고 메시지 (2/2)
 - 포맷

0	8	16	24	32
유형 : 9		코드 : 0		체크섬
주소 수 (Numbers of Addresses)		주소 크기 (Address Entry Size)		수명(Lifetime)
라우터 주소 1				
우선 순위 1				
라우터 주소 2				
우선 순위 2				
...				
라우터 주소 N				
우선 순위 N				

ICMPv4

- 질의 메시지 (9/13)

- 라우터 간청(Router Solicitation) 메시지

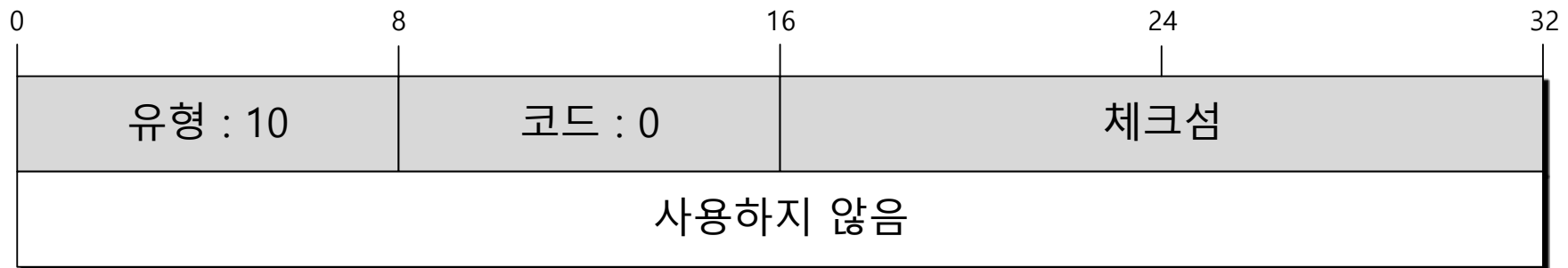
- 정의

- 호스트가 네트워크에 처음 연결되었을 때 주변 라우터에게 라우터 광고 메시지를 요청하기 위해 보내는 메시지

- 특징

- 호스트가 브로드캐스트 등을 통해 라우터 간청 메시지를 전송하면 해당 메시지를 수신한 라우터가 라우터 광고 메시지를 호스트에게 전송함
 - 현재는 DHCP가 네트워크 정보를 할당하여, DHCPDISCOVER 메시지를 사용하여 DHCP 서버에게 네트워크 정보 할당을 요청함

- 포맷



ICMPv4

- 질의 메시지 (10/13)
- 정보 요청 / 응답 (Information Request / Reply) 메시지 (1/2)
 - 정의
 - 요청자가 네트워크에 처음 연결되었을 때 자신의 네트워크 정보를 알아내기 위해 주고 받는 메시지
 - 특징
 - 요청자가 브로드캐스트로 요청을 보내면 IP를 할당해줄 수 있는 네트워크 장비가 IP 주소를 할당하여 요청자에게 응답 메시지를 전송
 - 현재는 DHCP가 자동으로 네트워크 설정 정보를 할당함
 - 충돌 관리, 인증 및 검증 등의 부재로 관리가 어렵고 가짜 정보 응답 메시지를 통해 서비스 거부 공격에 악용할 가능성이 있기 때문에 거의 사용하지 않음

ICMPv4

- 질의 메시지 (11/13)

- 정보 요청 / 응답 메시지 (2/2)

- 포맷

- 요청 메시지는 유형 15, 응답 메시지는 유형 16을 사용함
 - 식별자와 순서 번호를 사용하여 요청에 따른 응답 메시지를 구분함



ICMPv4

- 질의 메시지 (12/13)
- 주소 마스크 요청 / 응답(Address Mask Request / Reply) 메시지 (1/2)
 - 정의
 - 요청자가 응답자의 서브넷 마스크를 알아내기 위해 주고 받는 메시지
 - 특징
 - 요청자가 같은 네트워크 내의 호스트에게 전송하여 자신의 서브넷 마스크를 유추하는 데에 사용할 수 있음
 - 현재는 DHCP가 자동으로 네트워크 설정 정보를 할당함
 - 인증 및 검증의 부재로 가짜 주소 마스크 응답 메시지를 통해 중간자 공격이나 서비스 거부 공격에 악용할 가능성이 있기 때문에 거의 사용되지 않음

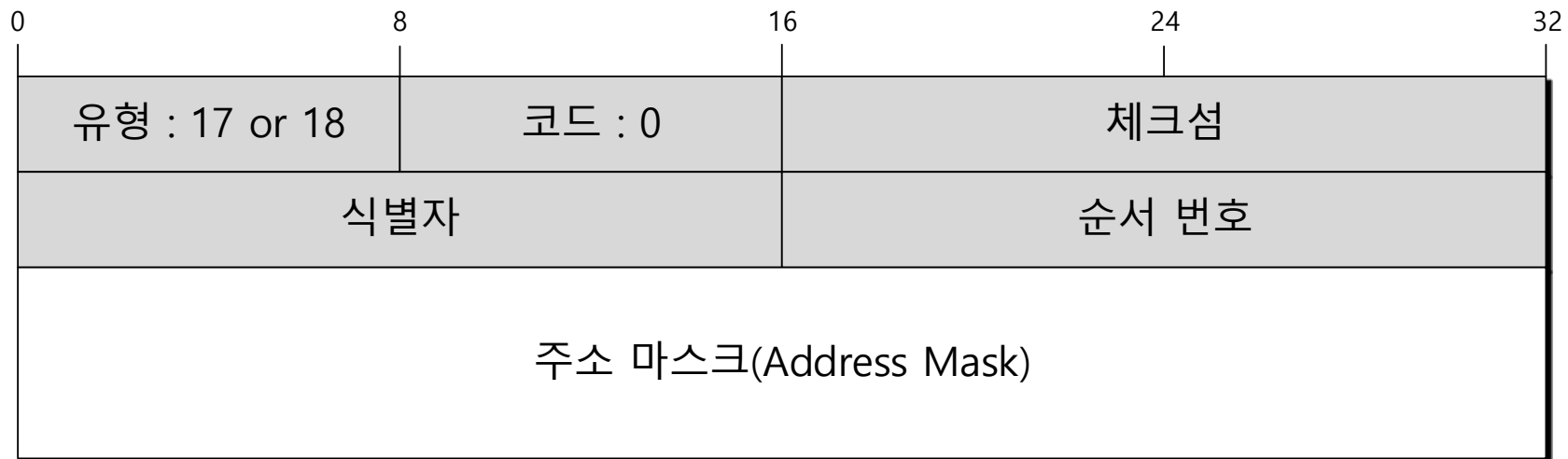
ICMPv4

- 질의 메시지 (13/13)

- 주소 마스크 요청 / 응답 메시지 (2/2)

- 포맷

- 요청 메시지는 유형 17, 응답 메시지는 유형 18을 사용함
 - 식별자와 순서 번호를 사용하여 요청에 따른 응답 메시지를 구분함
 - 응답 메시지는 메시지 본문에 응답자의 서브넷 마스크가 삽입되어 전송됨



ICMPv4

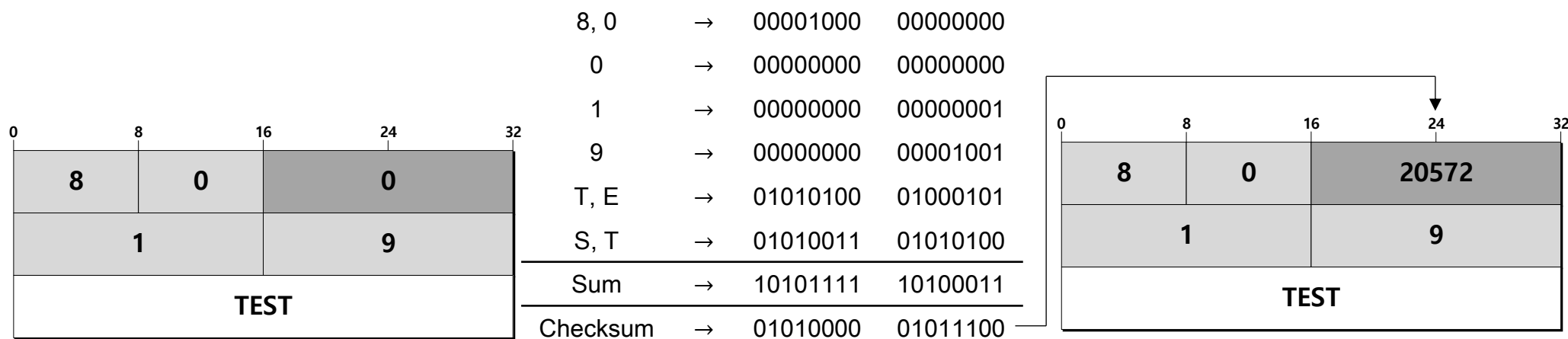
• 체크섬 (1/2)

• 정의

- 패킷의 오류 여부를 확인하기 위한 오류 검출 필드

• 계산 과정

1. 체크섬 필드를 0으로 만듦
2. 헤더와 데이터에 대해 16 비트 단위 값의 합을 구함
3. 합에 1의 보수를 취하여 체크섬을 구함
4. 구한 체크섬을 체크섬 필드에 저장함



ICMPv4

• 체크섬 (2/2)

• 검사 과정

1. 헤더와 데이터에 대해 16 비트 단위 값의 합을 구함
2. 합에 1의 보수를 취한 결과값을 구함
3. 결과값이 0 비트로만 이루어져 있으면 메시지를 수락하고 그렇지 않으면 메시지를 폐기함

0	8	16	24	32
8		0	20572	
1		9		
TEST				

8, 0	→	00001000	00000000
20572	→	01010000	01011100
1	→	00000000	00000001
9	→	00000000	00001001
T, E	→	01010100	01000101
S, T	→	01010011	01010100
Sum	→	11111111	11111111
Result	→	00000000	00000000

← 전부 0 비트이므로 검사를 통과함

ICMPv4

- 디버깅 도구 (1/5)

- PING (1/2)

- 상대 호스트와의 네트워크 연결 가능 여부를 확인하기 위해 사용함
- ICMP 에코 요청 메시지를 보내고 그에 따라 에코 응답 메시지를 받아서 왕복 지연 시간, 패킷 손실률 등을 측정함

```
C:\Users\admin>ping 8.8.8.8
```

```
Ping 8.8.8.8 32바이트 데이터 사용 :
```

```
8.8.8.8의 응답 : 바이트=32 시간=45ms TTL=114
```

```
8.8.8.8의 응답 : 바이트=32 시간=46ms TTL=114
```

```
8.8.8.8의 응답 : 바이트=32 시간=41ms TTL=114
```

```
8.8.8.8의 응답 : 바이트=32 시간=39ms TTL=114
```

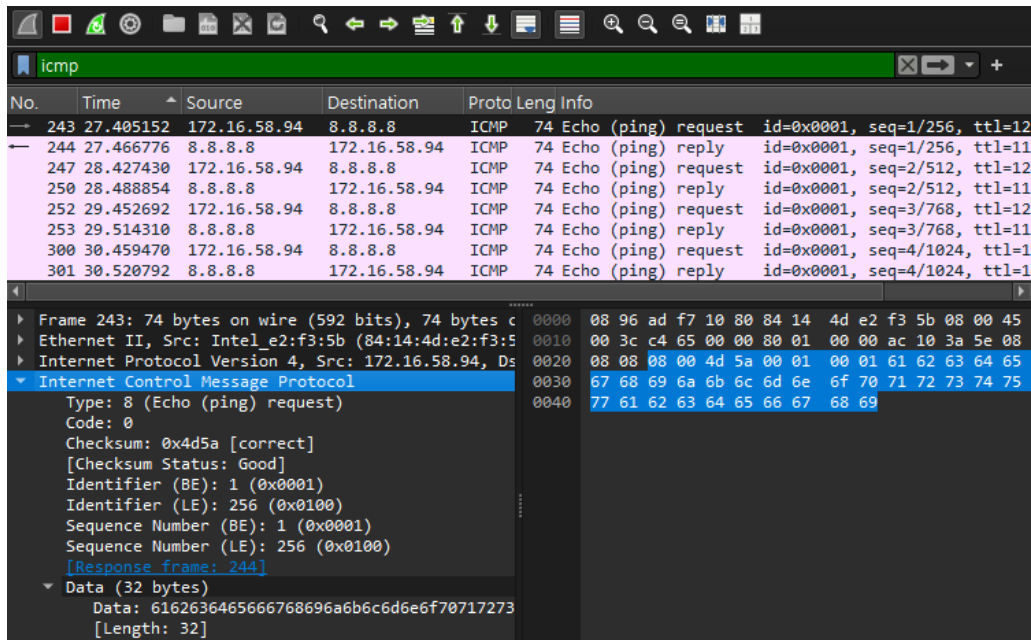
```
8.8.8.8에 대한 Ping 통계 :
```

```
패킷 : 보냄 = 4, 받음 = 4, 손실 = 0 (0% 손실),  
왕복 시간(밀리초):
```

```
최소 = 39ms, 최대 = 46ms, 평균 = 42ms
```

ICMPv4

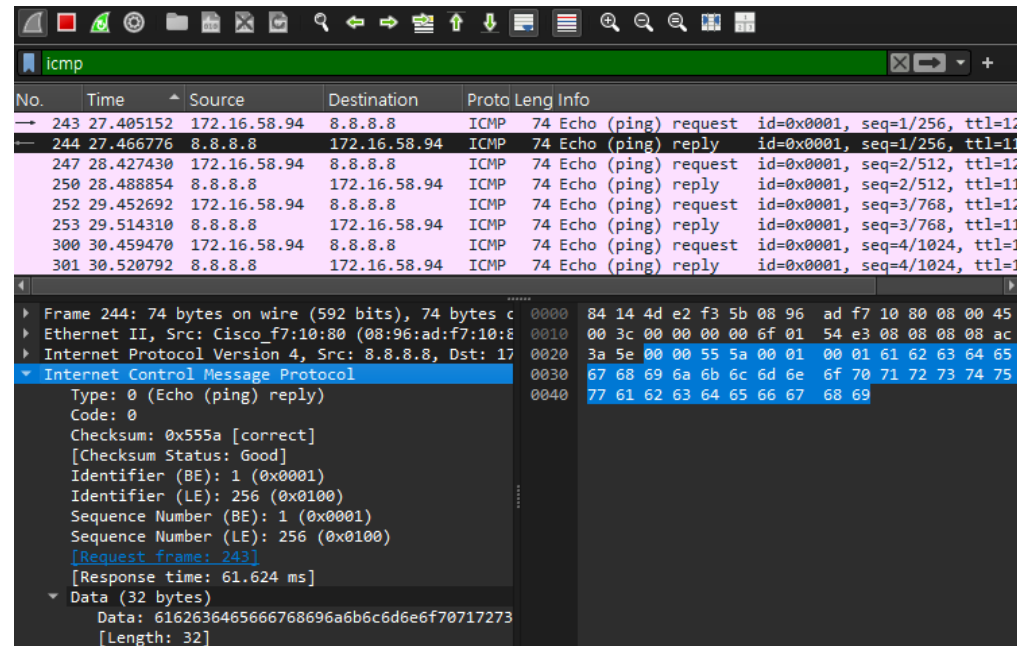
- 디버깅 도구 (2/5)
- PING (2/2)



Wireshark packet capture showing ICMP Echo (ping) request and reply. The packet list shows a request from 172.16.58.94 to 8.8.8.8 (No. 243) and a reply from 8.8.8.8 to 172.16.58.94 (No. 244). The packet details pane shows the structure of the ICMP Echo (ping) request and reply, including the type, code, checksum, identifier, sequence number, and data.

No.	Time	Source	Destination	Proto	Leng	Info
243	27.405152	172.16.58.94	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=12
244	27.466776	8.8.8.8	172.16.58.94	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=11
247	28.427430	172.16.58.94	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=12
250	28.488854	8.8.8.8	172.16.58.94	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=11
252	29.452692	172.16.58.94	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=12
253	29.514310	8.8.8.8	172.16.58.94	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=11
300	30.459470	172.16.58.94	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=12
301	30.520792	8.8.8.8	172.16.58.94	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=11

Frame 243: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: Intel_e2:f3:5b (84:14:4d:e2:f3:5b), Dst: 08:00:27:00:00:00
Internet Protocol Version 4, Src: 172.16.58.94, Destination: 8.8.8.8
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x4d5a [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 1 (0x0001)
Sequence Number (LE): 256 (0x0100)
[Response frame: 244]
Data (32 bytes)
Data: 6162636465666768696a6b6c6d6e6f70717273
[Length: 32]



Wireshark packet capture showing ICMP Echo (ping) request and reply. The packet list shows a request from 172.16.58.94 to 8.8.8.8 (No. 243) and a reply from 8.8.8.8 to 172.16.58.94 (No. 244). The packet details pane shows the structure of the ICMP Echo (ping) request and reply, including the type, code, checksum, identifier, sequence number, and data.

No.	Time	Source	Destination	Proto	Leng	Info
243	27.405152	172.16.58.94	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=12
244	27.466776	8.8.8.8	172.16.58.94	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=11
247	28.427430	172.16.58.94	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=12
250	28.488854	8.8.8.8	172.16.58.94	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=11
252	29.452692	172.16.58.94	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=12
253	29.514310	8.8.8.8	172.16.58.94	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=11
300	30.459470	172.16.58.94	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=12
301	30.520792	8.8.8.8	172.16.58.94	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=11

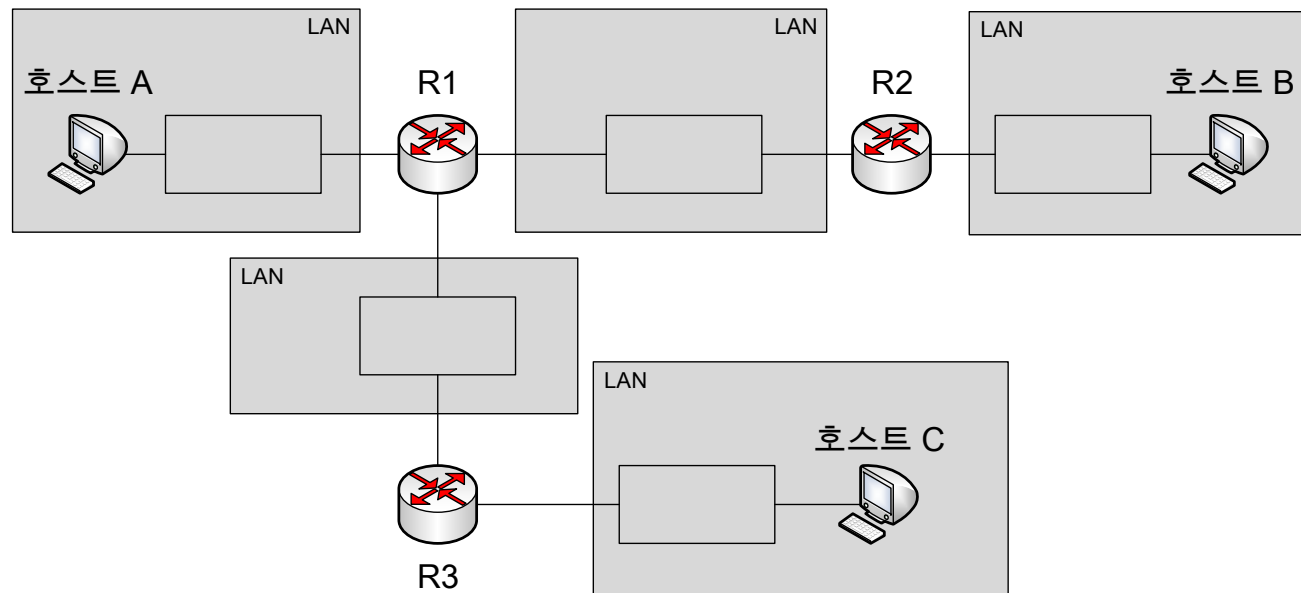
Frame 244: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
Ethernet II, Src: Cisco_f7:10:80 (08:96:ad:f7:10:80), Dst: 84:14:4d:e2:f3:5b
Internet Protocol Version 4, Src: 8.8.8.8, Destination: 172.16.58.94
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x555a [correct]
[Checksum Status: Good]
Identifier (BE): 1 (0x0001)
Identifier (LE): 256 (0x0100)
Sequence Number (BE): 1 (0x0001)
Sequence Number (LE): 256 (0x0100)
[Request frame: 243]
[Response time: 61.624 ms]
Data (32 bytes)
Data: 6162636465666768696a6b6c6d6e6f70717273
[Length: 32]

ICMPv4

- 디버깅 도구 (3/5)

- Traceroute (1/3)

- 패킷이 발신지 호스트에서 목적지 호스트까지 가는 경로를 추적할 수 있음
- 패킷의 TTL을 늘려가며 수신하는 ICMP 시간 초과 메시지를 통해 경로가 거쳐간 라우터의 주소와 왕복 시간을 얻음

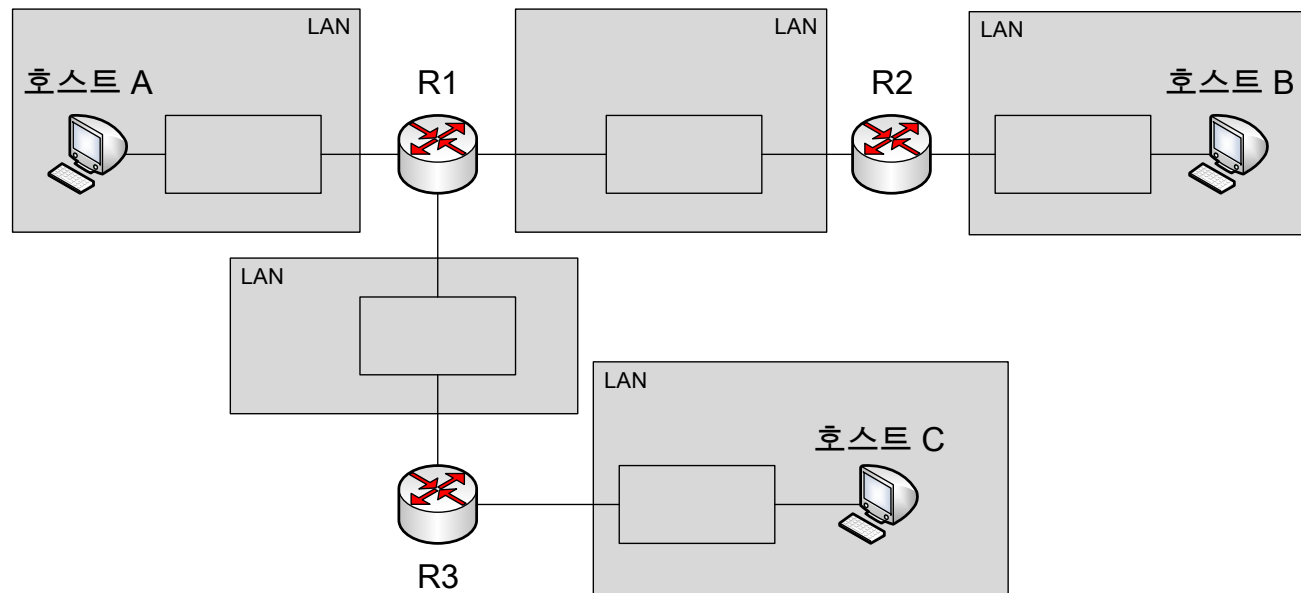


ICMPv4

- 디버깅 도구 (4/5)

- Traceroute (2/3)

- UDP가 지원하지 않는 포트 번호를 사용하여 UDP 패킷을 보내어 목적지에서 ICMP 목적지 도달 불가 메시지를 발생시켜 목적지에 패킷이 도착했음을 확인함



ICMPv4

- 디버깅 도구 (5/5)

- Traceroute (3/3)

- 응답 메시지를 보내오지 않는 라우터에 대해서는 정보를 나타내지 않음

```
C:\Users\admin>tracert 8.8.8.8

최대 30홉 이상의
dns.google [8.8.8.8](으)로 가는 경로 추적:

 1    8 ms    14 ms    1 ms    GT-AX11000-7480 [192.168.50.1]
 2   15 ms     3 ms     4 ms    223.195.34.1
 3    6 ms     6 ms    10 ms    210.107.239.13
 4     *      *      *      요청 시간이 만료되었습니다.
 5    8 ms     4 ms     6 ms    210.107.239.1
 6    6 ms    13 ms     4 ms    211.168.5.117
 7    7 ms     3 ms    12 ms    1.213.140.17
 8    6 ms     4 ms     4 ms    1.208.140.5
 9   10 ms     5 ms     4 ms    1.208.144.13
10     *      *      *      요청 시간이 만료되었습니다.
11    8 ms     4 ms     5 ms    100.65.51.13
12   39 ms    38 ms    39 ms    100.67.30.38
13   42 ms    37 ms    38 ms    61.43.220.22
14  231 ms   202 ms   209 ms   142.250.168.244
15  198 ms   205 ms   206 ms    72.14.233.125
16  245 ms   223 ms   204 ms   216.239.47.17
17  205 ms   203 ms   202 ms   dns.google [8.8.8.8]

추적을 완료했습니다.
```

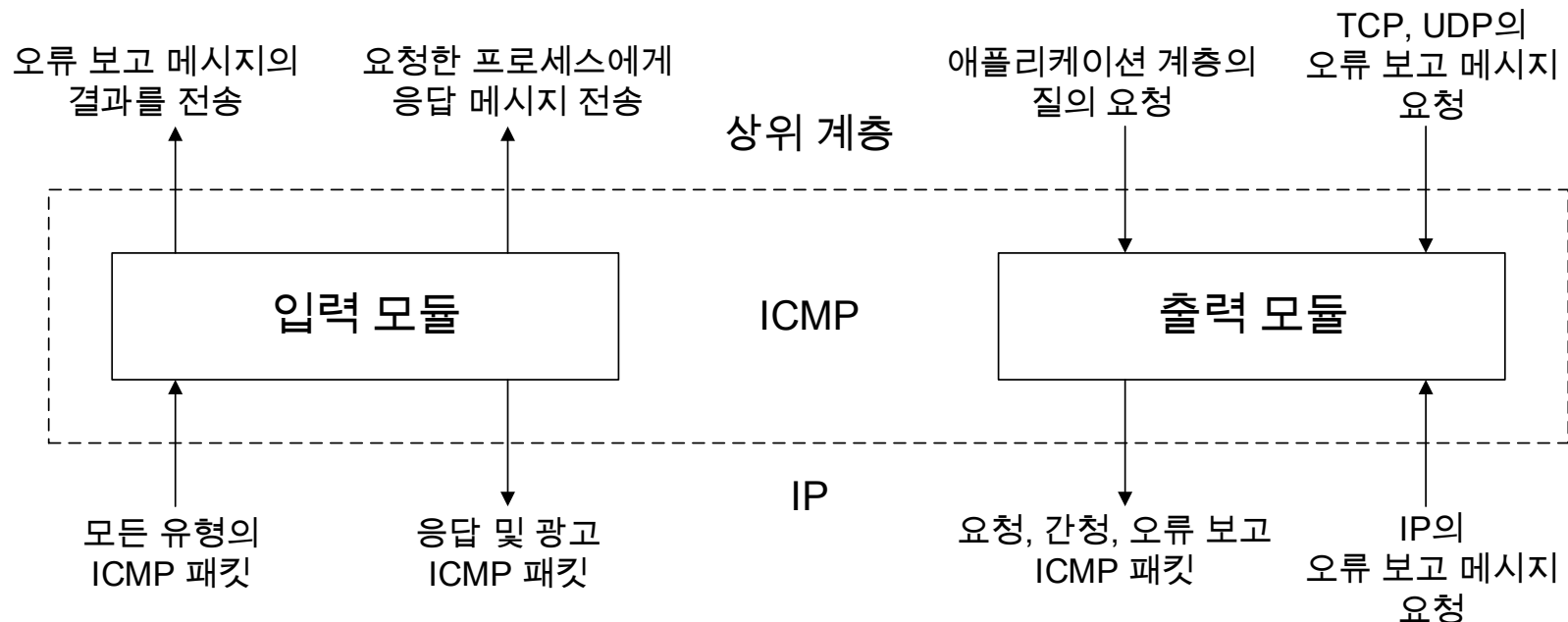
```
C:\Users\admin>curl ipinfo.io/223.195.34.1
{
  "ip": "223.195.34.1",
  "city": "Seoul",
  "region": "Seoul",
  "country": "KR",
  "loc": "37.5660,126.9784",
  "org": "AS9769 Sejong University",
  "postal": "03141",
  "timezone": "Asia/Seoul",
  "readme": "https://ipinfo.io/missingauth"
}
```

ICMPv4

• ICMP 패키지 (1/3)

• 개요

- ICMP 메시지는 입력 모듈에 의해 수신되고 상황에 맞게 처리됨
- 출력 모듈은 수신한 요구에 맞춰 ICMP 메시지를 생성함



ICMPv4

• ICMP 패키지 (2/3)

• 입력 모듈

- 수신된 모든 ICMP 메시지를 유형에 따라 처리함
- 요청 메시지를 수신하면 그에 맞는 응답 메시지를 생성하고 전송함
- 재지정 메시지를 수신하면 라우팅 테이블을 수정하도록 함
- 오류 보고 메시지를 수신하면 관련 프로토콜에게 오류 정보를 알림

```
ICMP_input_module(ICMP_Packet)
{
    if (the type is a request)
    {
        create a reply
        send the reply
    }
    if (the type defines a redirection)
    {
        modify the routing table
    }
    if (the type defines other error messages)
    {
        inform the appropriate source protocol
    }
    return
}
```

ICMPv4

• ICMP 패키지 (3/3)

• 출력 모듈

- 상위 계층이나 IP로부터 요구를 받으면 그에 맞는 ICMP 메시지를 생성함
- 오류 보고 메시지를 생성할 수 없는 경우나 유효한 재지정 메시지의 경우에는 오류 보고 메시지를 생성하지 않음
- 요청 메시지를 요구 받으면 그에 맞는 요청 메시지를 생성함

ICMP_Output_module(*demand*)

```
{  
    if (the demand defines an error message)  
    {  
        if (demand comes from IP AND is forbidden)  
        {  
            return  
        }  
        if (demand is a valid redirection message)  
        {  
            return  
        }  
        create an error message  
    }  
    if (demand defines a request)  
    {  
        create a request message  
    }  
    send the message  
    return  
}
```


목 차

- 보충
- ICMPv4
- 모바일 IP

모바일 IP

- 개요 (1/2)
 - 정지 호스트(Stationary Hosts)
 - 고정된 위치에서 하나의 네트워크에 연결되어 있는 호스트
 - 프리픽스(Prefix)를 기반으로 하는 기존의 IP 라우팅 규칙을 따라서 작동함
 - 이동 호스트(Mobile Hosts)
 - 위치를 변경하며 연결되는 네트워크가 바뀌는 호스트
 - 호스트가 한 네트워크에서 다른 네트워크로 이동하면 IP 주소 구조도 변경 되어야 함

모바일 IP

- 개요 (2/2)

- 이동 호스트 주소 지정 방법

- 주소 변경

- 호스트가 새로운 네트워크로 갈 때마다 새 주소로 변경하여 사용하는 방법
 - 변경할 때마다 네트워크 설정 변경, 재부팅, 데이터 전송 중단 등을 해야하는 문제점이 있음

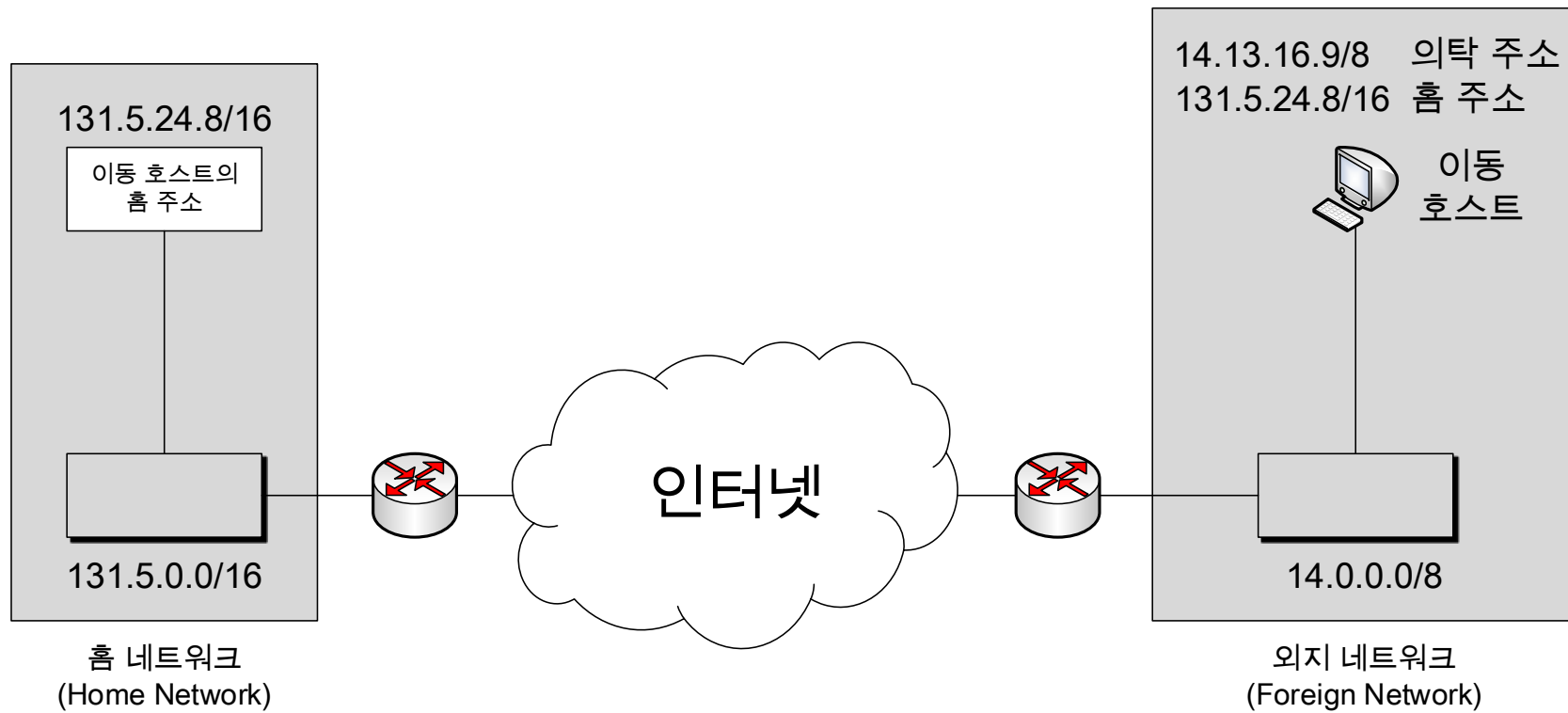
- 이중 주소 사용

- 호스트가 홈 주소(Home Address)라는 원 주소와 의탁 주소(Care-of Address)라는 임시 주소를 가지는 방법
 - 홈 주소는 고정되어 있고, 호스트가 새로운 네트워크로 이동할 때마다 의탁 주소를 받아 쓰게 됨

모바일 IP

- 정의

- 이동 호스트가 이동하여 네트워크가 바뀌어도 기존의 IP를 유지하면서 통신할 수 있도록 하는 프로토콜

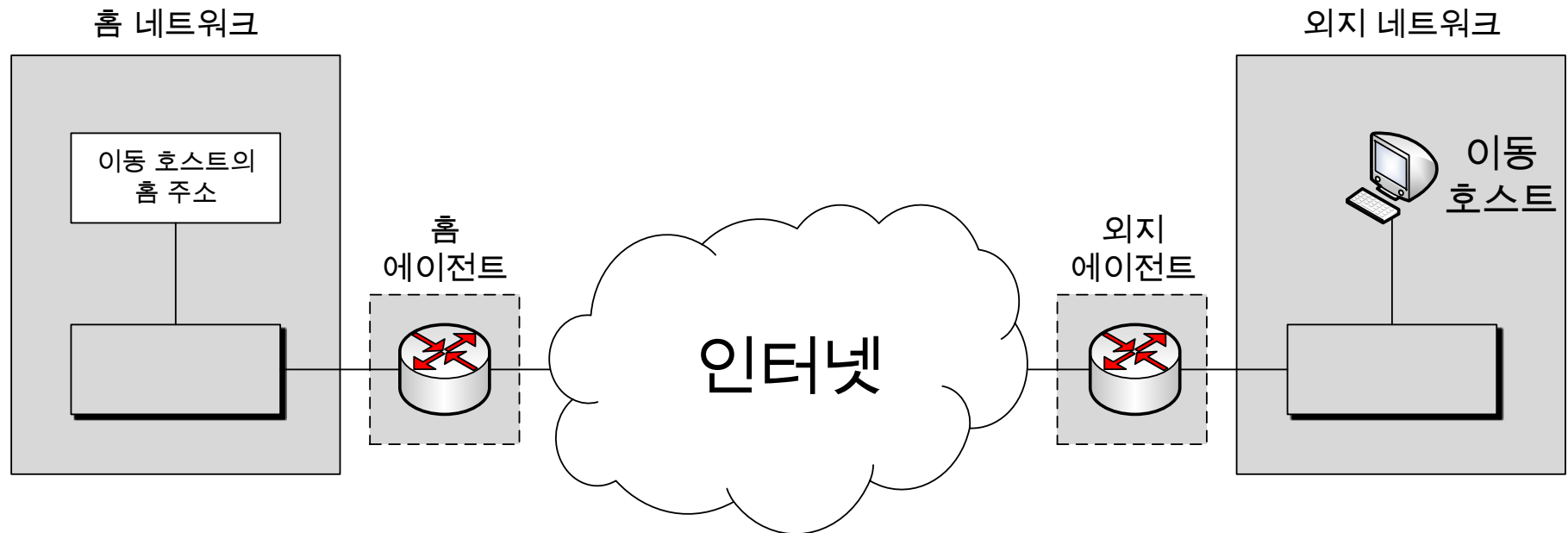


모바일 IP

- 에이전트(Agent) (1/4)

- 정의

- 이동 호스트의 이동성을 지원하기 위한 기능을 수행하는 라우터

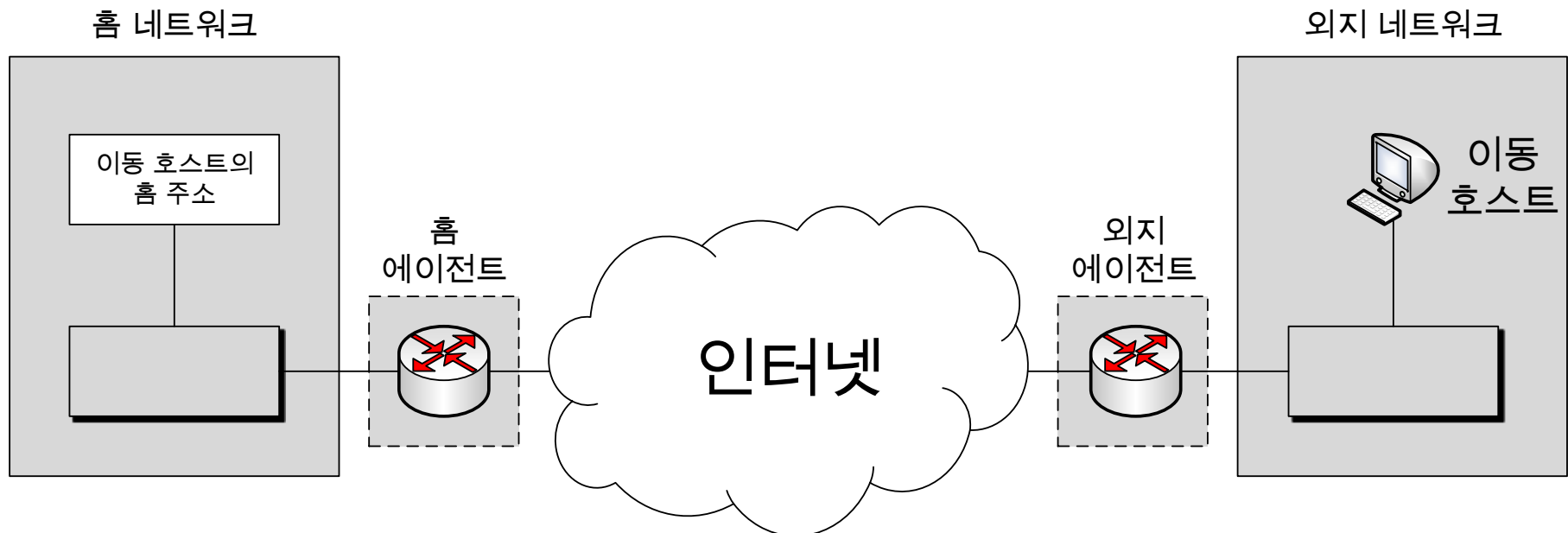


모바일 IP

- 에이전트 (2/4)

- 홈 에이전트(Home Agent)

- 이동 호스트의 홈 네트워크에 연결된 라우터
- 이동 호스트에게 보내진 패킷은 홈 에이전트가 수신하여
외지 에이전트(Foreign Agent)에게 전송



모바일 IP

- 에이전트 (3/4)

- 외지 에이전트 (1/2)

- 외지 네트워크에 연결된 라우터
- 홈 에이전트로부터 받은 패킷을 이동 호스트에게 전송

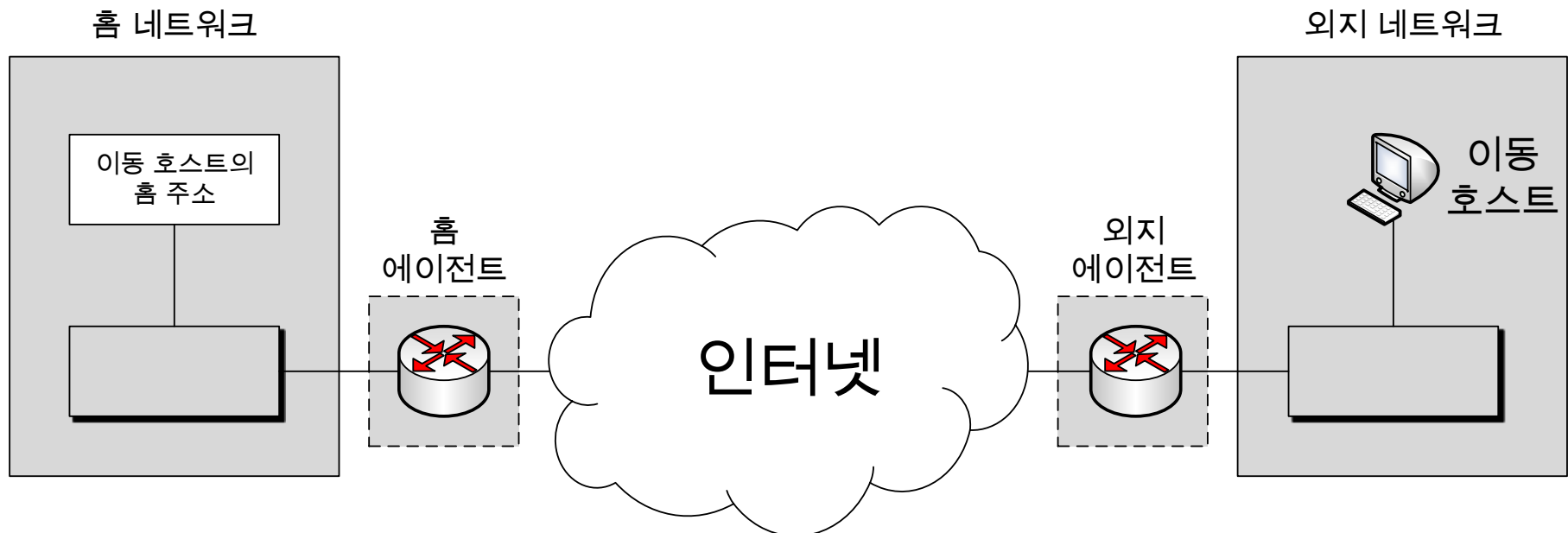


모바일 IP

- 에이전트 (4/4)

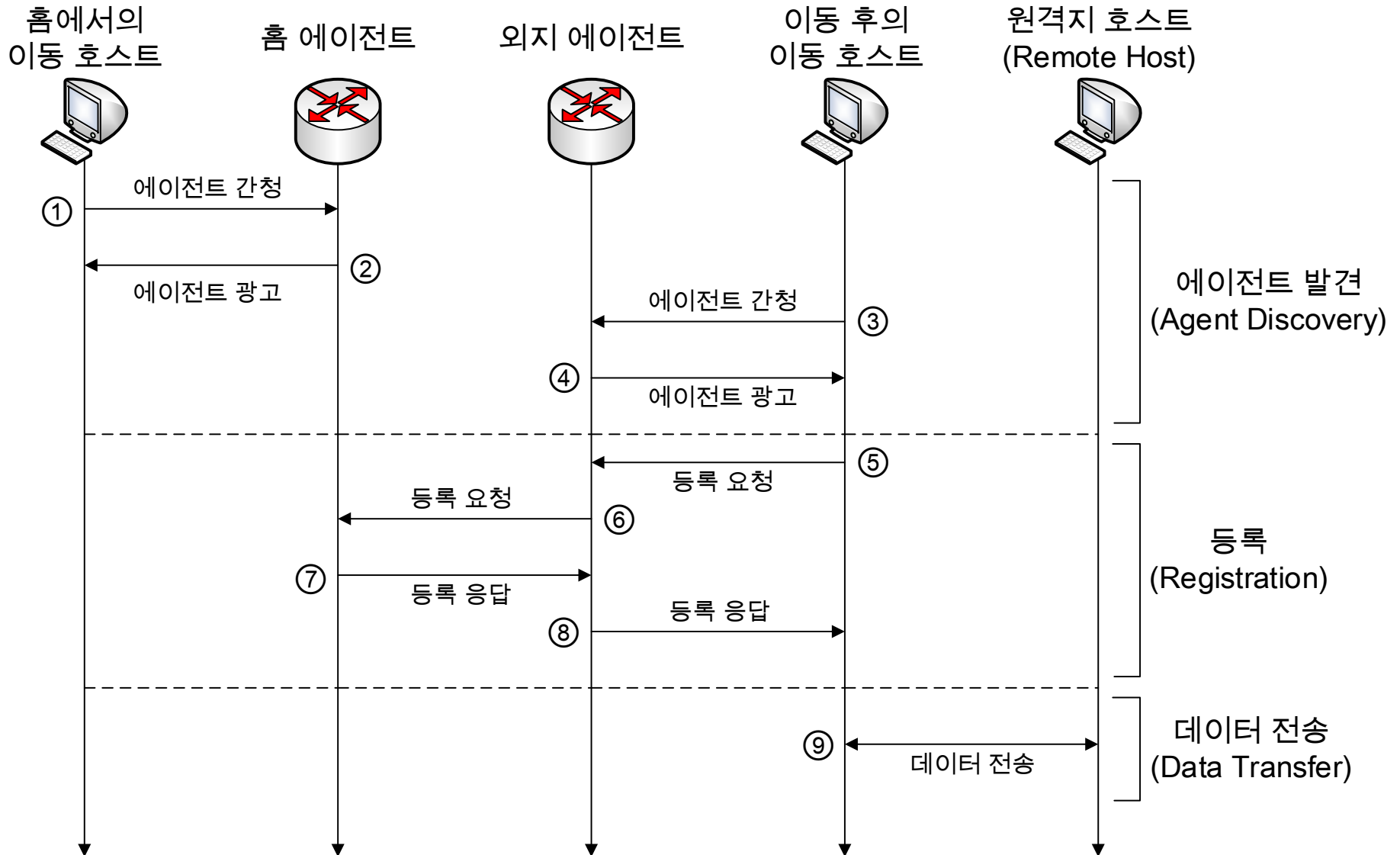
- 외지 에이전트 (2/2)

- 이동 호스트가 직접 외지 에이전트의 역할을 수행하여 외지 에이전트로서 작동할 수 있고, 이때의 위탁 주소는 동위치 위탁 주소(Colocated Care-of Address)라고 함



모바일 IP

• 과정 (1/12)

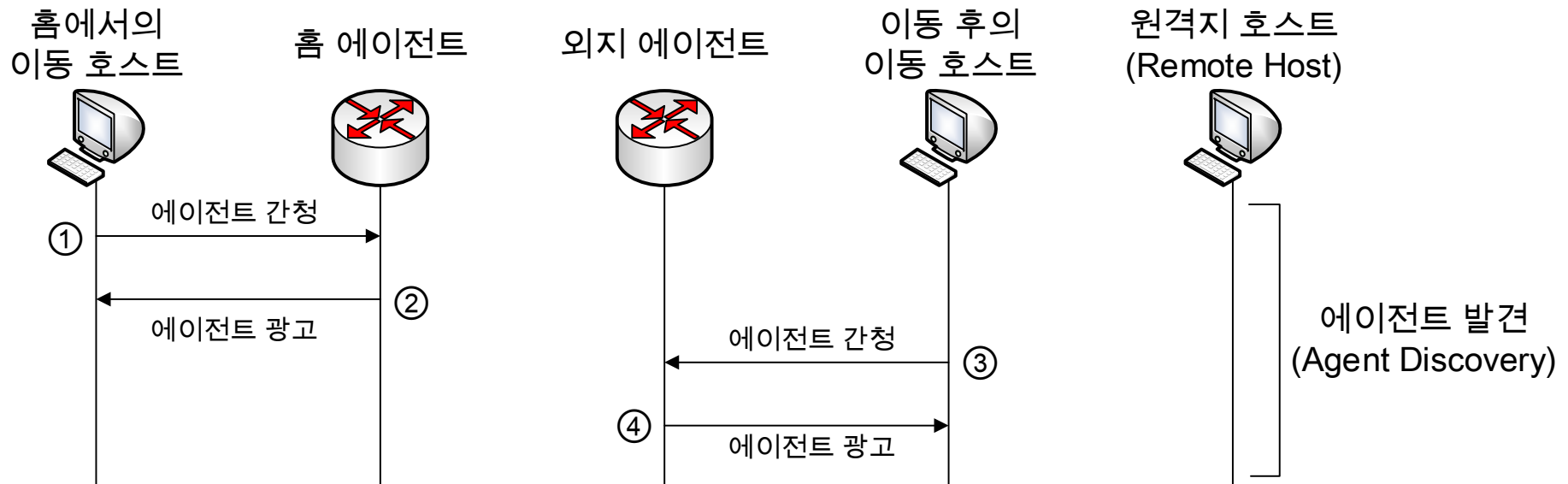


모바일 IP

• 과정 (2/12)

• 에이전트 발견(Agent Discovery)

- 이동 호스트는 홈 네트워크를 떠나기 전 홈 에이전트의 주소를 알아야 함
- 이동 호스트가 외지 네트워크에 들어간 후에는 외지 에이전트를 발견하고 의탁 주소를 얻어야 함
- 에이전트 발견은 에이전트 광고 / 간청을 통해 이루어짐



모바일 IP

- 과정 (3/12)

- 에이전트 발견 - 광고(Advertisement) (1/2)

- 에이전트로서 작동하는 라우터는 ICMP 라우터 광고 메시지를 보낼 때 에이전트 광고 메시지를 추가하여 전송함



모바일 IP

- 과정 (4/12)

터널링(Tunneling)

한 프로토콜의 데이터 단위를 다른 프로토콜의 데이터 단위 안에 캡슐화하여 전송하는 기법

- 에이전트 발견 - 광고 (2/2)

- 플래그 필드의 비트로 에이전트의 정보를 나타냄

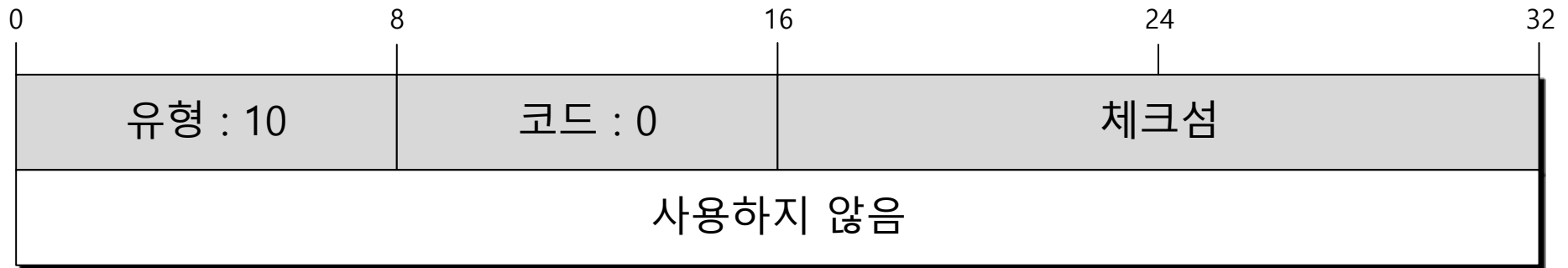
플래그 비트 위치	설명
0(10000000)	등록이 필요함
1(01000000)	추가적인 등록을 받지 않음
2(00100000)	홈 에이전트의 기능을 제공함
3(00010000)	외지 에이전트의 기능을 제공함
4(00001000)	최소(Minimal) 캡슐화를 사용함
5(00000100)	GRE (Generic Routing Encapsulation) 캡슐화를 사용함
6(00000010)	사용하지 않음
7(00000001)	역터널링을 지원함

모바일 IP

- 과정 (5/12)

- 에이전트 발견 - 간청(Solicitation)

- 에이전트 간청은 ICMP 라우터 간청 메시지를 그대로 사용하고 에이전트 간청을 받은 에이전트는 에이전트 광고 메시지를 보냄

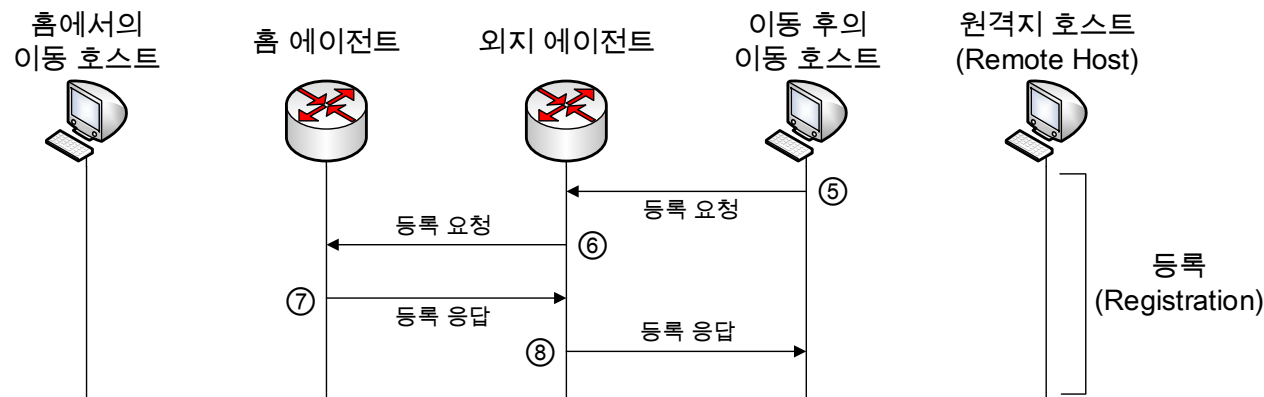


모바일 IP

• 과정 (6/12)

• 등록(Registration)

- 이동 호스트는 외지 네트워크 접속 후 외지 에이전트에 자신을 등록해야 함
- 이동 호스트는 등록 이후 홈 에이전트에 자신을 등록해야 함
- 등록을 지속하려는 경우, 등록이 만료되기 전까지 다시 등록해야 함
- 홈 네트워크로 돌아온 이후에는 홈 에이전트에게 수명을 0으로 하여 등록 요청을 보냄으로써 등록을 취소해야 함
- 등록은 UDP를 이용한 등록 요청 / 응답을 통해 이루어짐

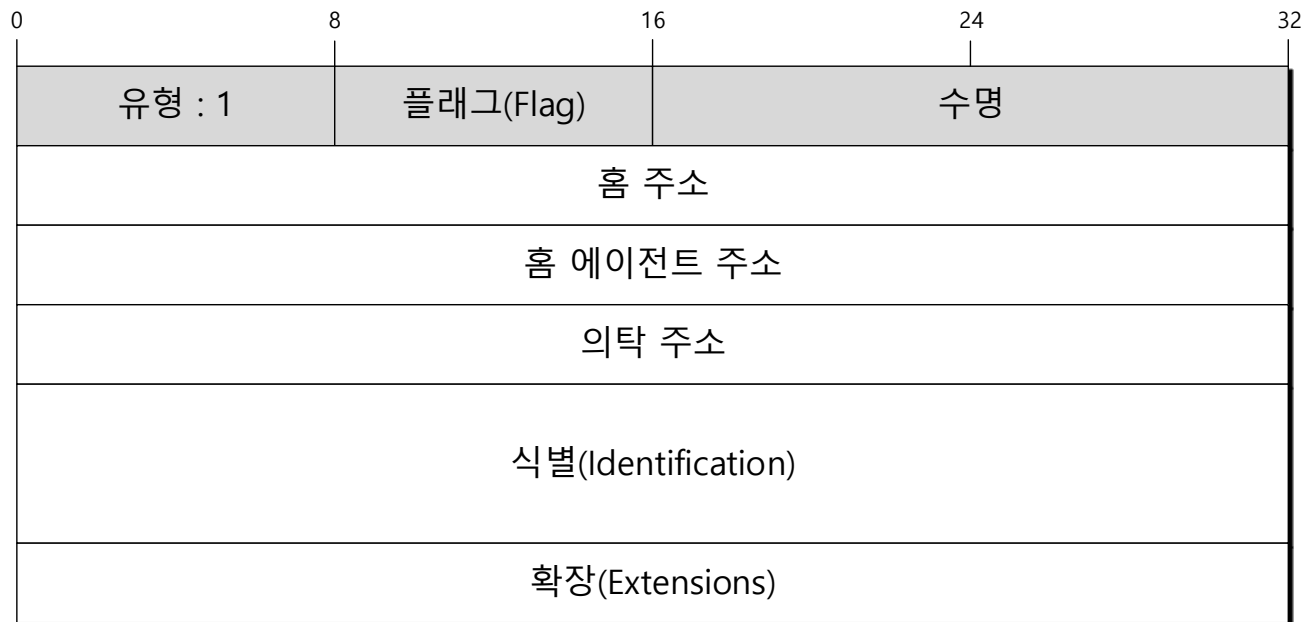


모바일 IP

- 과정 (7/12)

- 등록 - 요청 (1/2)

- 이동 호스트는 등록 요청 메시지를 통해 외지 에이전트에게 등록 요청을 보냄
- 외지 에이전트는 해당 메시지를 확인한 후 홈 에이전트에게 보내고 홈 에이전트는 해당 패킷의 IP 헤더를 통해 외지 에이전트의 주소를 알게 됨



모바일 IP

- 과정 (8/12)
 - 등록 - 요청 (2/2)
 - 플래그 필드의 비트로 요청에 대한 정보를 나타냄

플래그 비트 위치	설명
0(10000000)	홈 에이전트에게 이전 바인딩을 유지하도록 요청함
1(01000000)	홈 에이전트에게 홈 네트워크에서 수신하는 모든 브로드캐스트 메시지를 터널링 하도록 요청함
2(00100000)	동위치 의탁 주소를 사용함
3(00010000)	홈 에이전트에게 최소 캡슐화를 사용하도록 요청함
4(00001000)	홈 에이전트에게 GRE 캡슐화를 사용하도록 요청함
6(00000010)	역터널링을 요청함
5(00000100) 7(00000001)	예비 비트

모바일 IP

- 과정 (9/12)

- 등록 - 응답

- 홈 에이전트는 등록 요청을 확인한 후 수락 여부를 코드 필드에 삽입하여 등록 응답 메시지를 이동 호스트에게 보냄
- 요청과 응답을 매칭시키기 위해 응답 메시지의 식별 필드는 요청 메시지와 동일한 값이 삽입됨

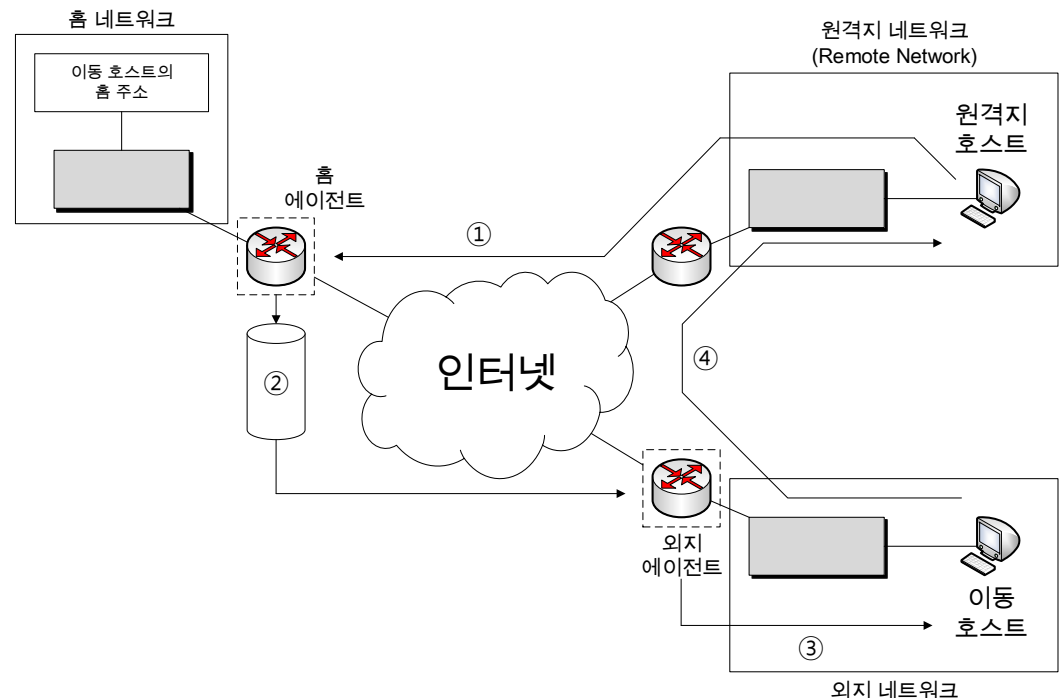


모바일 IP

- 과정 (10/12)

- 데이터 전송(Data Transfer) (1/3)

1. 원격지 호스트가 홈 주소로 패킷을 보내면 홈 에이전트가 해당 패킷을 가로챈
2. 홈 에이전트는 해당 패킷을 터널링을 통해 외지 에이전트로 전송함

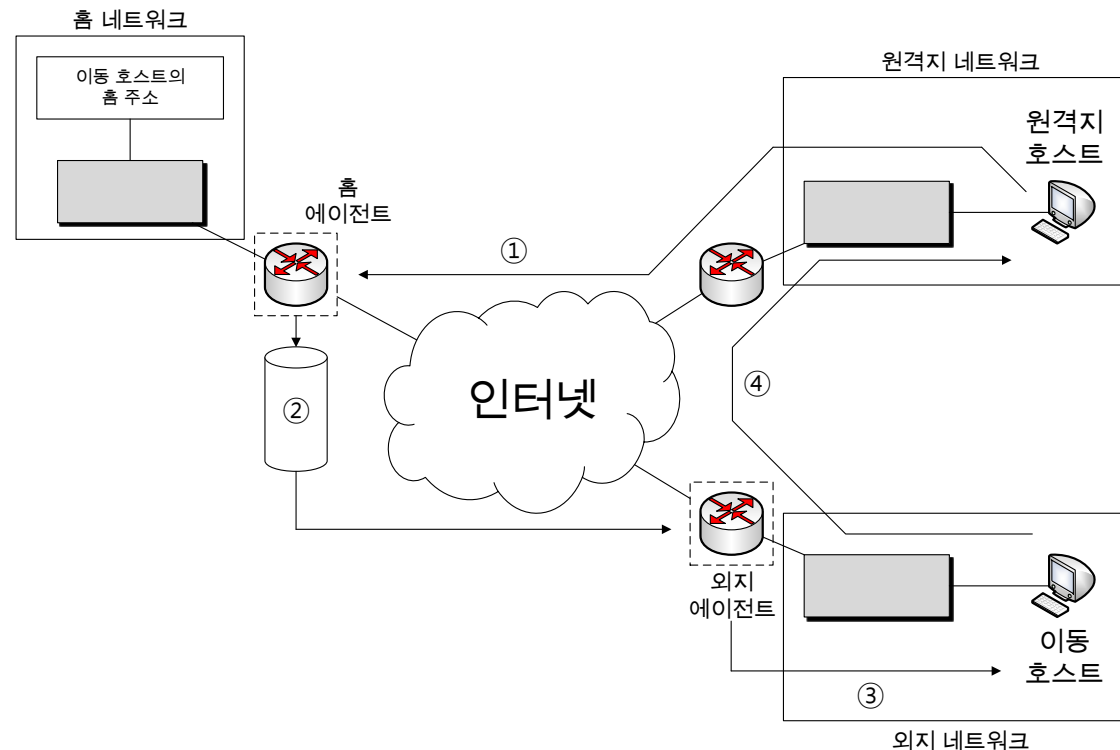


모바일 IP

- 과정 (11/12)

- 데이터 전송 (2/3)

3. 외지 에이전트는 받은 패킷을 역캡슐화(Decapsulation)하고 목적지 주소에 적힌 이동 호스트의 홈 주소를 등록 테이블에서 참조하여 이동 호스트의 의탁 주소로 전송함

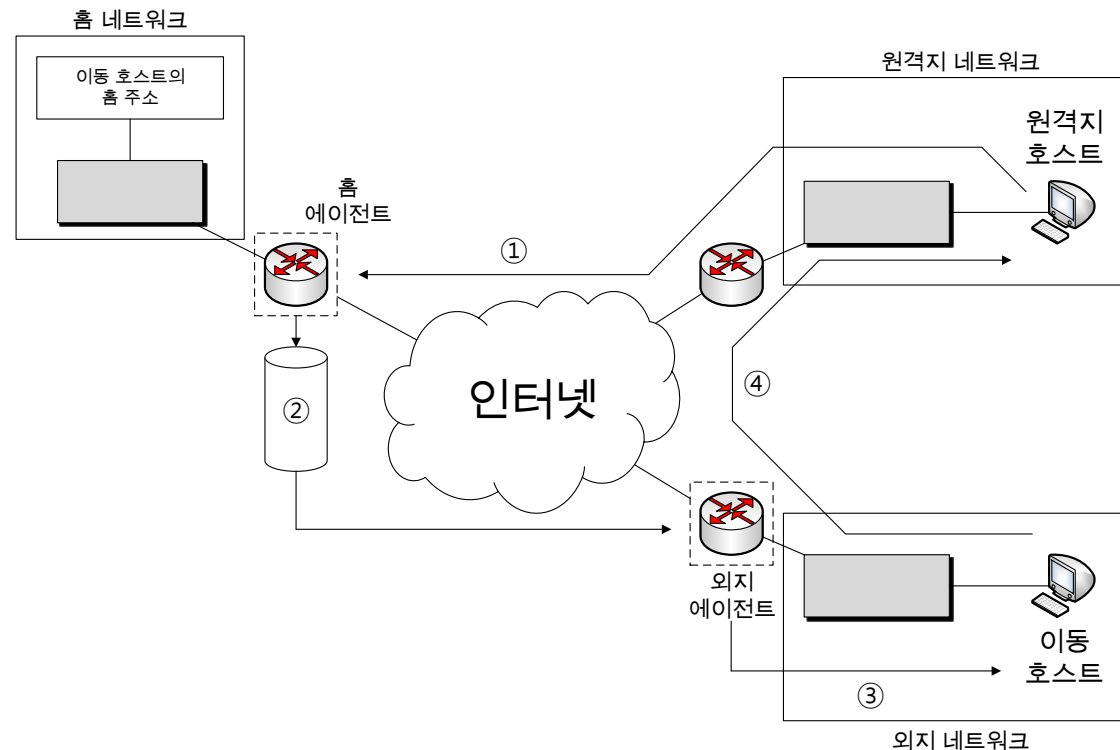


모바일 IP

- 과정 (12/12)

- 데이터 전송 (3/3)

4. 이동 호스트가 원격지 호스트로 패킷을 보낼 때엔 홈 주소를 발신지 주소로, 원격지 주소를 목적지 주소로 하여 원격지 호스트로 바로 전송함

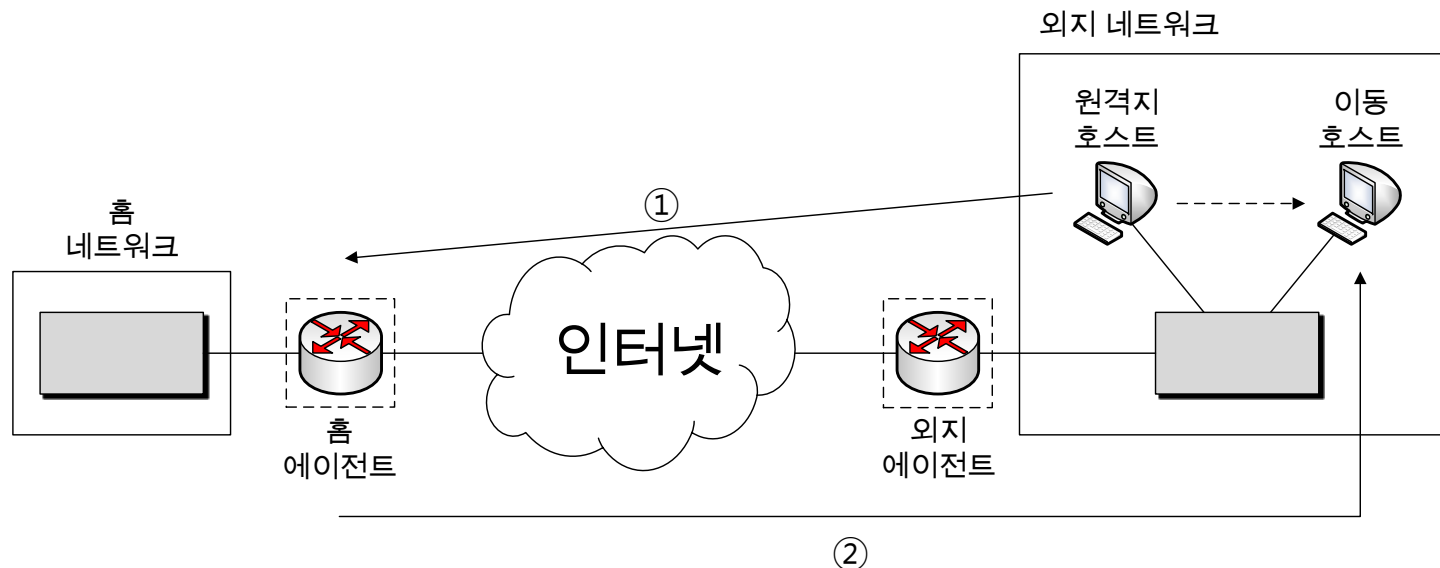


모바일 IP

- 비효율성 문제 (1/3)

- 더블 크로싱(Double Crossing)

- 원격지 호스트가 자신과 같은 네트워크로 이동한 이동 호스트와 통신할 때 발생함
- 원격지 호스트가 같은 네트워크 내의 이동 호스트에게 패킷을 보낼 때 이동 호스트에게 바로 보내지 않고 홈 에이전트를 거쳐서 보냄

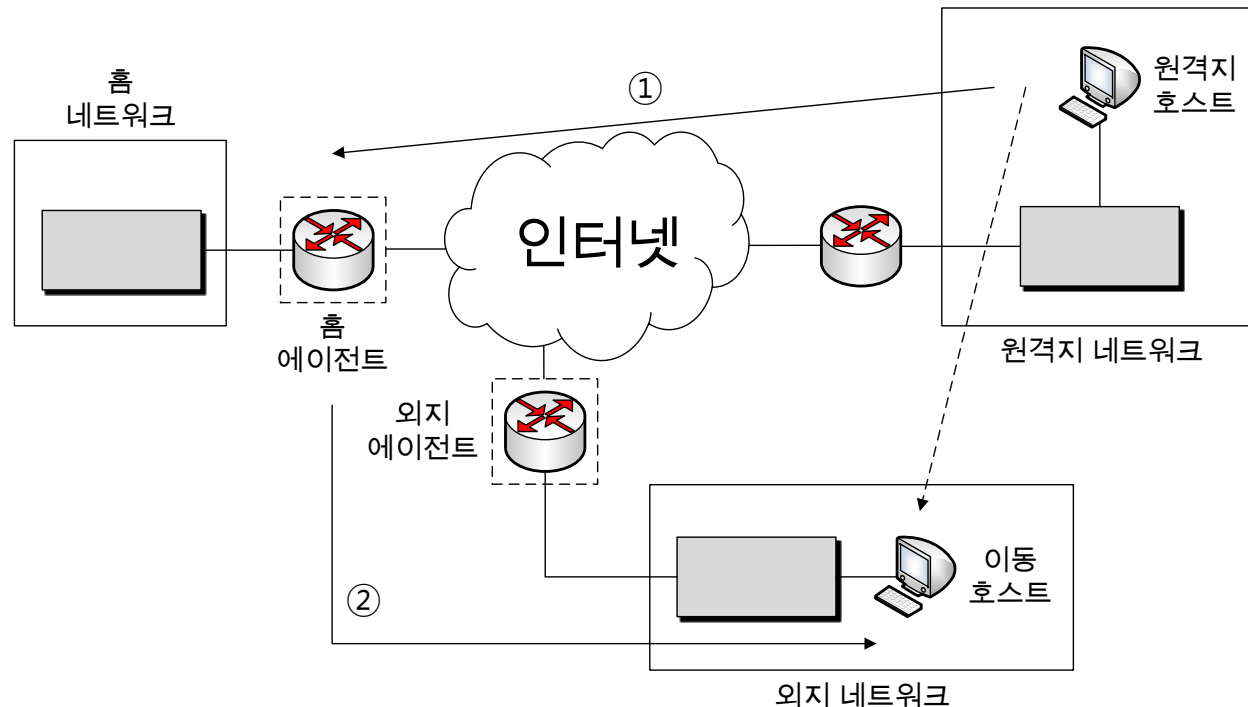


모바일 IP

- 비효율성 문제 (2/3)

- 삼각형 라우팅(Triangle Routing)

- 원격지 호스트가 자신과 다른 네트워크에 연결되어 있는 이동 호스트와 통신할 때 발생함
- 원격지 호스트에서 이동 호스트까지의 경로가 존재함에도 홈 에이전트를 거쳐서 패킷을 전송함



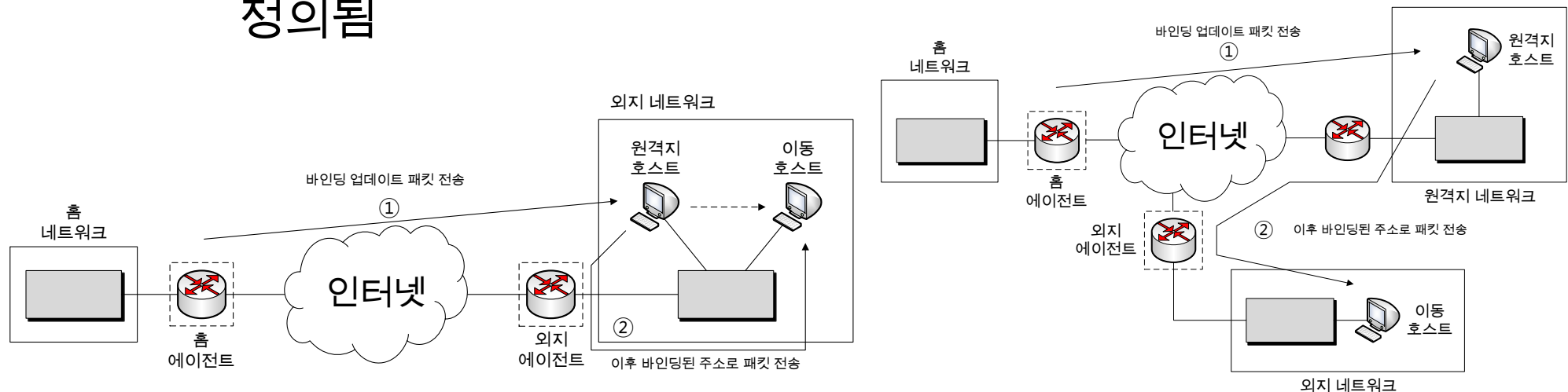
모바일 IP

• 비효율성 문제 (3/3)

구분	라우팅(Routing)	포워딩(Forwarding)	바인딩(Binding)
설명	패킷의 전송 경로를 결정	패킷을 실제로 어디로 전달할지 결정	두 주소의 매핑 관계를 결정

• 해결 방안

- 원격지 호스트가 의탁 주소를 이동 호스트의 홈 주소에 바인드함
 - 홈 에이전트가 보낸 바인딩 갱신(Binding Update) 메시지를 이용하여 이동 호스트로 가는 패킷이 의탁 주소로 바로 가게 함
 - 이동 호스트가 이동하여 네트워크가 변경되면 캐시 정보가 무효화 되므로 네트워크가 변경될 때마다 바인딩 갱신 메시지를 보내야 함
 - 인증 등의 보안 기능을 추가하여 모바일 IPv6에서 공식적으로 정의됨



Thanks!

이 성 현(seonghyeon@pel.sejong.ac.kr)