2023/03/09, 2023 보안기초 세미나

TCP/IP 완벽 가이드

- II-6부 IP 지원 프로토콜-

손 우 영(wooyoung@pel.sejong.ac.kr)

세종대학교 프로토콜공학연구실

목 차

- 보충
- ICMP 개념과 일반 동작
- ICMPv4 오류 메시지 유형
- ICMPv4 정보 제공 메시지 유형

목 차

- 보충
- ICMP 개념과 일반 동작
- ICMPv4 오류 메시지 유형
- ICMPv4 정보 제공 메시지 유형

보충

- 멀티호밍(Multihoming)
  - 하나의 통신 장비가 여러 IP 주소를 가지게 하는 것
  - 다중 인터페이스를 갖는 경우
    - 두 개 이상의 인터페이스를 동일한 네트워크에 연결
      - 동일한 네트워크 ID를 갖는 두 개의 IP 주소를 가짐
      - 대역폭 확장 가능
        - e.g., 서버, 고성능 워크스테이션 등

보충

- 클래스 단위 주소지정
  - 멀티캐스트 주소 지정

범위 시작 주소	범위 끝 주소	설명
224.0.0.0	224.0.0.255	유명한 특수 멀티캐스트 주소로 예약됨

  - 유명 멀티캐스트 주소

범위 시작 주소	설명
224.0.0.1	서브넷의 모든 장비
224.0.0.2	서브넷의 모든 라우터
224.0.0.4	DVMRP를 사용하는 모든 라우터

보충

- IP 클래스 비사용 주소지정
  - 클래스 비사용 도메인간 라우팅(CIDR, Classless Internet-Domain Routing)
    - 슈퍼네팅(Supernetting)
      - 특정 네트워크를 서브넷으로 분해하는 대신 네트워크를 병합하여 더 큰 슈퍼넷을 만드는 기법
      - 주소 공간의 낭비를 줄이고 라우터의 부담을 줄이기 위한 기법
        - 슈퍼넷: 여러 네트워크를 하나의 형태로 합친 네트워크
        - 라우팅 테이블 항목 수를 줄일 수 있음

보충

- IP 서브넷 주소지정
  - 서브넷 ID 비트 수 결정 방법
    - 네트워크에서 사용해야 할 서브넷의 수, 각 서브넷별로 사용 가능한 최대 호스트의 수에 따라 결정됨
    - 예시
      1. 클래스 B 네트워크에서 10개의 서브넷이 필요하다고 파악
      2. 서브넷 ID에 4비트를 할당
         - $2^4 = 16, 2^3 = 8$이기 때문에 만약 3비트를 할당한다면 원하는 서브넷의 개수를 충족시키지 못할 것임
      3. 위와 같은 과정으로 호스트 ID에 12비트가 남고 이것은 각 서브넷별로 4,094개의 호스트 포함 가능을 의미

보충

- 재조합
  - 수신된 IP 데이터그램을 헤더필드의 정보를 이용하여 조합하는 과정
    - 과정
      1. 단편 인식과 단편화 된 메시지 식별
         - MF값과 오프셋 값으로 단편을 인식하고 식별자 필드 등을 통해 메시지를 식별
      2. 버퍼 초기화
         - 단편을 받아 저장할 공간 확보
         - 만약 버퍼가 다 채워진 경우 ICMP 송신 속도 낮춤 메시지 전송 후 송신율을 낮춤
      3. 타이머 초기화
         - 재조합을 위한 타이머 설정
         - 만약 모든 단편을 수신하기 전에 타이머가 만료되면 장비는 단편들을 모두 버리고 ICMP 시간 초과 메시지를 송신함
      4. 단편 수신과 처리
         - 버퍼에 단편화 오프셋 값을 보고 순서에 맞게 단편 삽입

목 차

- 보충
- ICMP 개념과 일반 동작
- ICMPv4 오류 메시지 유형
- ICMPv4 정보 제공 메시지 유형

ICMP 개념과 일반 동작

- ICMP(Internet Control Message Protocol)
  - 정의
    - IP 패킷을 처리할 때 여러 정보를 전달하거나 제어하는 IP 지원 프로토콜
  - IP와 ICMP의 관계
    - IP는 연결을 수립하지 않고 데이터그램이 목적지에 도달한다는 보장 없이 전달하는 신뢰성 없는 프로토콜
      - ICMP는 이러한 IP의 특징을 보완하기 위한 프로토콜

ICMP 개념과 일반 동작

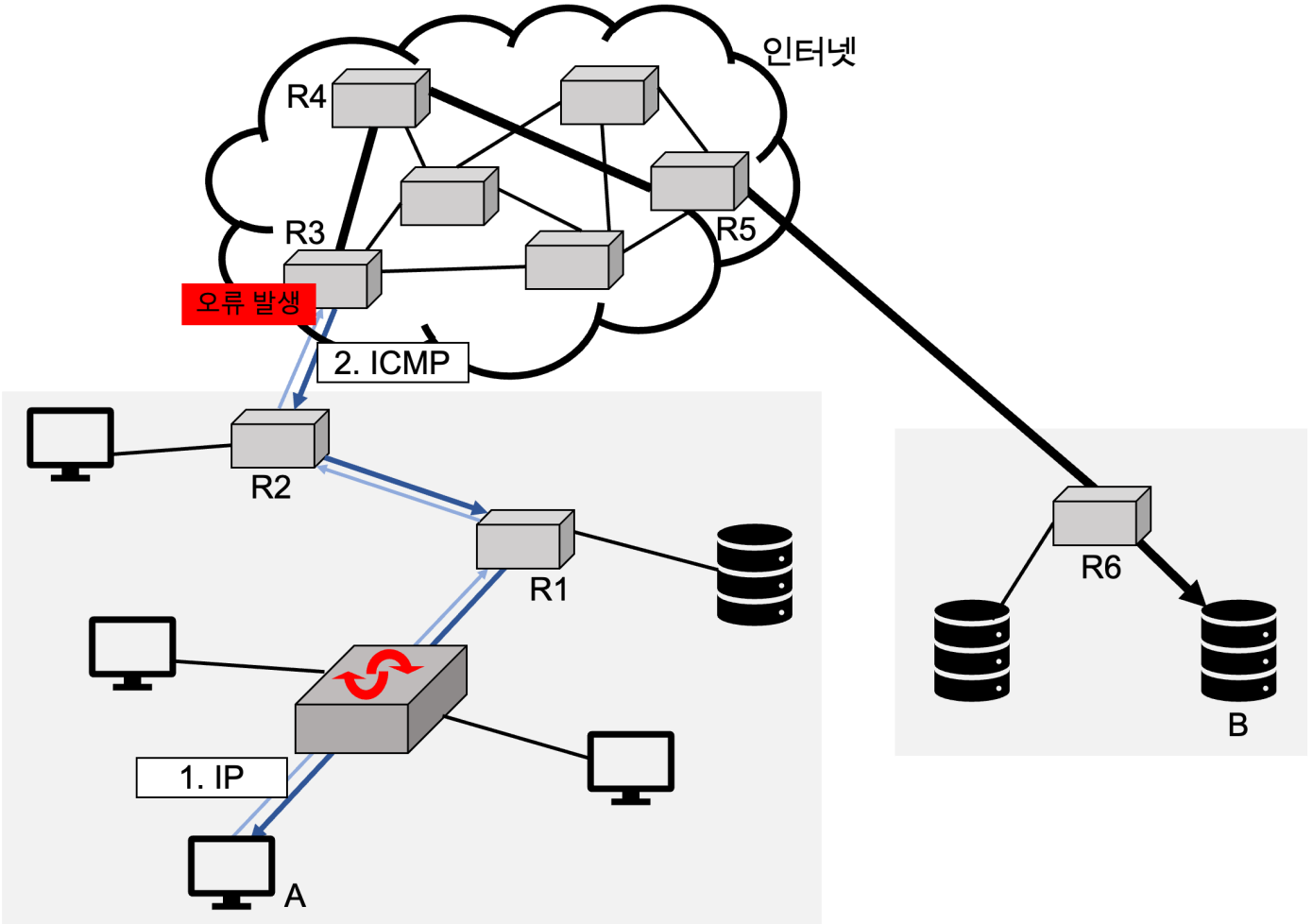
- ICMP(Internet Control Message Protocol)
  - 특징
    - IP 데이터그램의 문제로 발생한 ICMP 메시지는 최초 송신 장비에게만 전달 가능
      - IP 데이터그램의 헤더에는 오직 최초 송신 장비의 주소만 존재하기 때문
    - ICMP를 수신 장비가 반드시 처리해야 하는 것은 아님
      - 한 쌍으로 동작하는 정보 제공 메시지에서는 처리해야 함

ICMP 개념과 일반 동작

- 일반 동작
  - IP 장비가 다른 장비에게 제어 메시지를 보낼 수 있는 방법을 제공함
  - TCP/IP 메시지와 동일한 방법으로 캡슐화되고 수신 장비의 IP 계층으로 송신
  - 유형에 따라 송신 주체가 달라짐
    - 라우터만 송신 가능한 메시지
      - e.g., 리다이렉트 메시지
    - 라우터와 호스트 모두 송신 가능한 메시지
      - e.g., 에코 요청과 에코 응답 메시지, 라우터 광고와 라우터 정보 요청 메시지

ICMP 개념과 일반 동작

- 일반 동작
  - 오류 보고 과정

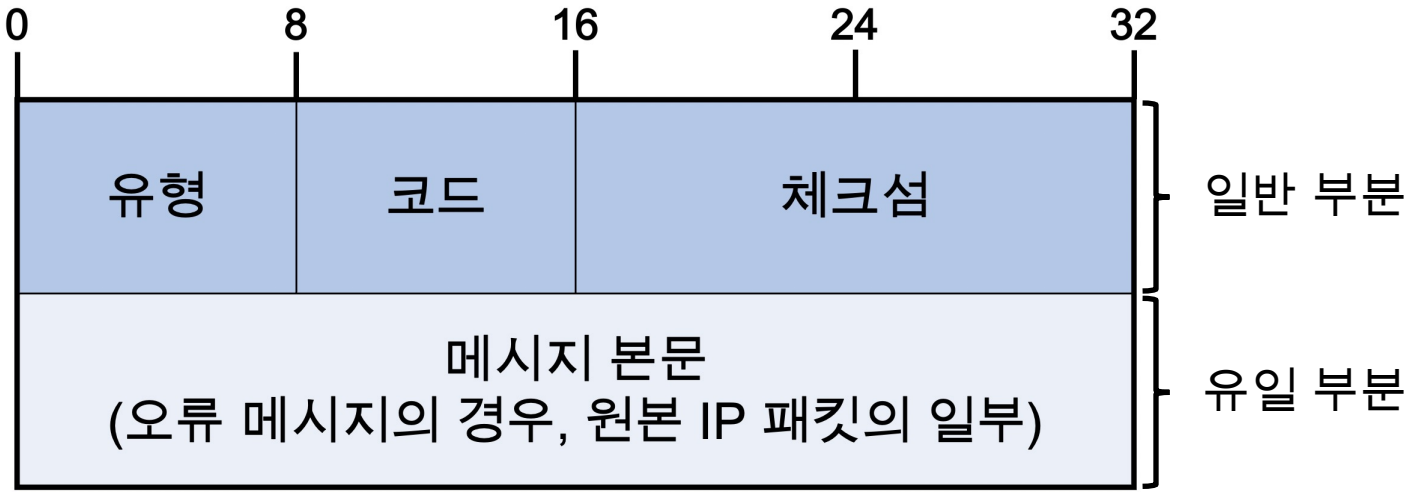


ICMP 개념과 일반 동작

- ICMP 메시지 클래스
  - 오류 메시지
    - 에러가 발생했다는 것을 출발지 장비에게 알림
    - 일반적으로 어떤 행위에 의한 응답으로 생성
      - e.g., 데이터그램의 전송
  - 정보 제공/요청 메시지
    - 네트워크의 문제를 테스트, 진단 등에 사용되는 정보 제공
    - 메시지 쌍으로 구성됨
      - e.g., 에코 요청/응답 메시지, 타임스탬프 요청/응답 메시지

ICMP 개념과 일반 동작

- ICMP 일반 메시지 포멧



필드 이름	크기(바이트)	설명
유형	1	ICMP 메시지 유형 식별
코드	1	각 ICMP 메시지 유형 내에서의 하위 유형 식별, 256개의 하위 유형 정의 가능
체크섬	2	전체 ICMP 메시지의 에러 검출
메시지 본문	가변적	에러가 발생하거나 정보를 제공하기 위한 메시지 원문

ICMP 개념과 일반 동작

- ICMP 메시지 생성
  - IP를 이용하여 캡슐화 됨
    - IP 대역폭의 일부분 사용
      - 필요한 경우에만 ICMP 사용
  - 오류 메시지
    - 여러 오류 상황에 대한 응답으로 메시지 생성
  - 정보 제공 메시지
    - 메시지를 사용하는 프로토콜에 정의되어 있는 규칙에 따라 메시지 생성

ICMP 개념과 일반 동작

- ICMP 메시지 한계
  - 메시지 생성 루프가 생길 경우
  - 브로드/멀티캐스트로 패킷을 여러 개 송신했는데 모든 목적지 호스트가 출발지 장비로 에러 보고를 보내는 경우
  - 패킷이 단편화 되고 여러 단편들이 동일한 오류를 발생시키는 경우
  - 패킷이 유니캐스트 장비 주소가 아닌 출발지 주소를 갖는 경우

ICMP 개념과 일반 동작

- ICMP 메시지 처리
  - ICMP 메시지를 수신한 장비는 메시지 유형에 맞게 처리
    - e.g., 에코 요청 메시지를 수신한 경우, 에코 응답 메시지로 응답함으로써, 통신 여부를 테스트 함
    - e.g., 송신 속도 낮춤 메시지를 수신한 경우, 송신율을 낮춤
  - 알 수 없는 유형값을 갖는 ICMP 메시지가 수신되면 자동으로 버림
  - 응답을 필수적으로 요구하지 않는다면 반드시 처리할 필요는 없음

목 차

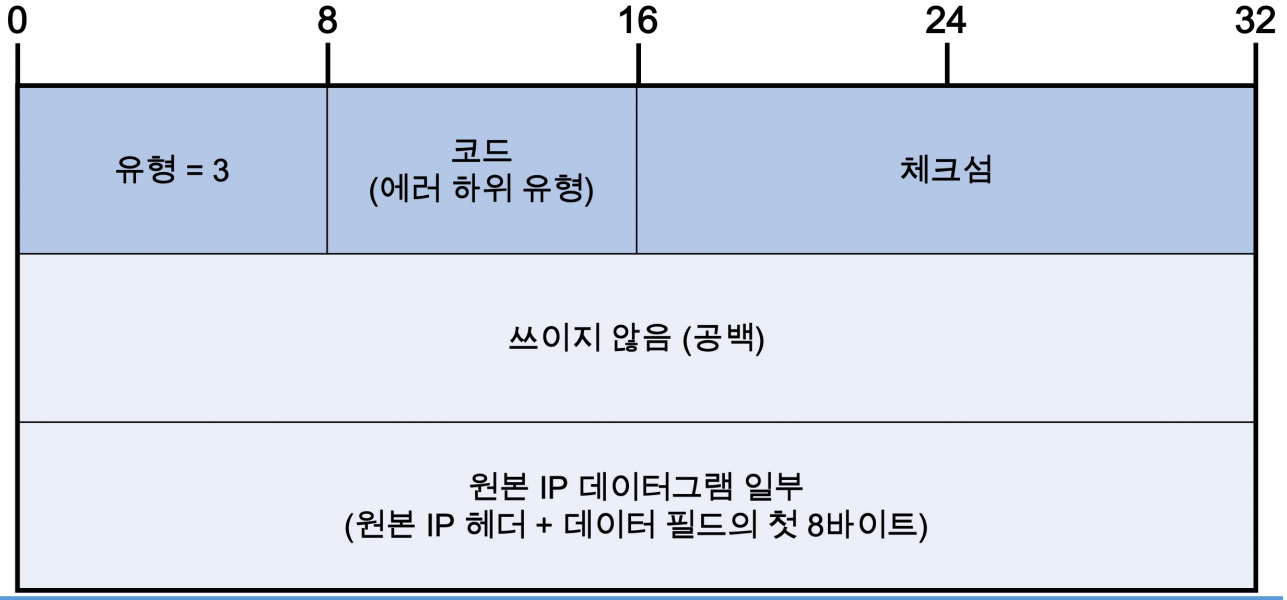
- 보충
- ICMP 개념과 일반 동작
- ICMPv4 오류 메시지 유형
- ICMPv4 정보 제공 메시지 유형

ICMPv4 오류 메시지 유형

- ICMPv4 목적지 접근 불가 메시지
  - 정의
    - 송신 장비에게 IP 데이터그램 전달 실패를 알려주는 메시지
  - 특징
    - 전달 불가능한 데이터그램의 일부를 포함
      - IP 헤더 전체와 페이로드의 처음 8바이트 포함
      - 메시지 수신자가 문제의 원인을 파악하는 데 도움을 줌

ICMPv4 오류 메시지 유형

- ICMPv4 목적지 접근 불가 메시지
  - 메시지 포맷



필드 이름	크기(바이트)	설명
유형	1	ICMP 메시지 유형 식별, 이 메시지의 경우 이 필드값은 3
코드	1	메시지 하위 유형 식별
체크섬	2	ICMP 메시지를 위한 오류 탐지 기능 제공
쓰이지 않음	4	공백으로 남아 있고 쓰이지 않는 4바이트
원본 데이터그램 일부	가변적	오류 메시지를 유발시킨 데이터그램의 전체 IP 헤더와 페이로드의 첫 8바이트

ICMPv4 오류 메시지 유형

- ICMPv4 목적지 접근 불가 메시지
  - ICMPv4 목적지 접근 불가 메시지 하위 유형(1/2)

코드 값	메시지 하위 유형	설명
0	네트워크 접근 불가	목적지 네트워크로 가는 경로가 없는 경우 발생 (e.g., 목적지 주소가 라우팅 테이블에 없을 경우 및 잘못된 주소인 경우)
1	호스트 접근 불가	패킷이 IP 주소의 지정된 네트워크로는 전달되었지만, 실제 호스트에 전달되지 못한 경우 발생
2	프로토콜 접근 불가	IP 프로토콜의 상위 계층인 UDP, TCP 등에 전달되지 못한 경우 발생
3	포트 접근 불가	수신 측 애플리케이션(프로세스)에 전달하지 못한 경우 발생
4	단편화가 필요하지만 DF(Don't Fragment)가 있음	단편화 불가 옵션이 설정되었으나, 단편화가 필요한 경우 발생
5	소스 라우팅 실패	송신 측에서 설정한 라우팅 옵션대로 라우터를 방문할 수 없을 경우 발생
6	알려지지 않은 목적지 네트워크	지정된 호스트가 속한 네트워크가 알려지지 않은 경우 발생
7	알려지지 않은 목적지 호스트	지정된 호스트가 알려지지 않은 경우 발생

ICMPv4 오류 메시지 유형

- ICMPv4 목적지 접근 불가 메시지
  - ICMPv4 목적지 접근 불가 메시지 하위 유형(2/2)

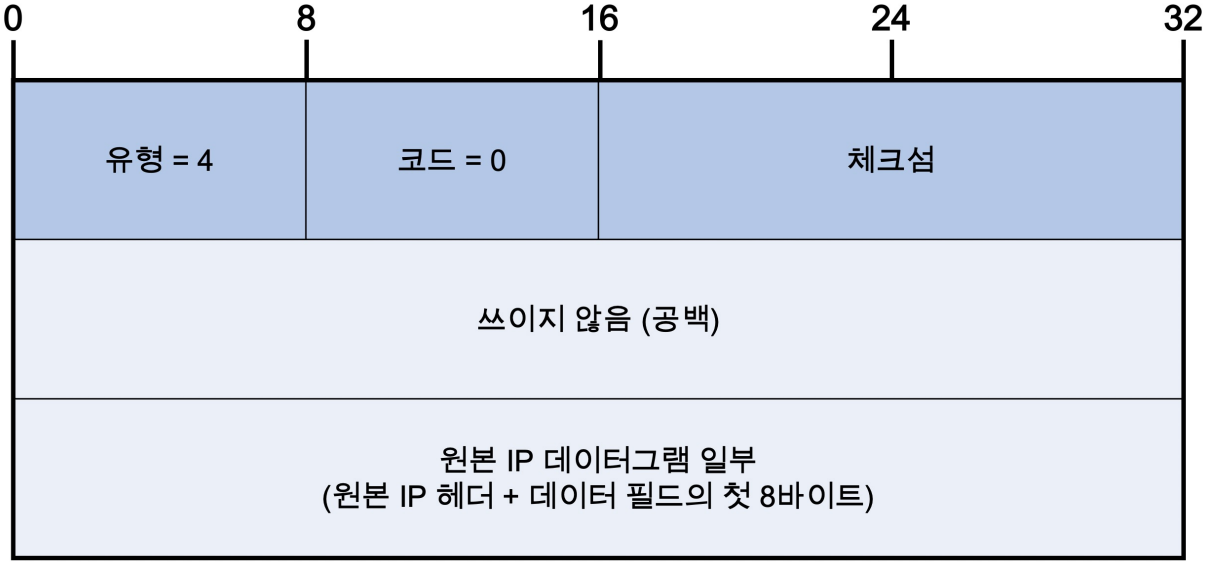
코드 값	메시지 하위 유형	설명
8	출발지 호스트 고립	쓰이지 않음
9	목적지 네트워크로의 통신이 관리상 금지됨	출발지 장비로의 목적지 장비가 위치한 네트워크로 통신이 허용되지 않음
10	목적지 호스트로의 통신이 관리상 금지됨	출발지 장비로부터 목적지 장비가 위치한 네트워크로 송신할 수 있지만 특정 장비로 송신할 수 없음
11	서비스 유형에 대한 목적지 네트워크 접근 불가	패킷 헤더의 서비스 유형 필드에 명시된 서비스를 제공할 수 없어서 IP 주소에 지정된 목적지 네트워크에 접근할 수 없음
12	서비스 유형에 대한 목적지 호스트 접근 불가	패킷 헤더의 서비스 유형 필드에 명시된 서비스를 제공할 수 없어서 IP 주소에 지정된 목적지 호스트에 접근할 수 없음
13	관리상 통신이 금지됨	패킷이 메시지 내용에 의한 차단을 수행하는 필터링 때문에 전달될 수 없음
14	호스트 우선 순위 위반	서비스 유형 필드의 우선 순위 값이 허용되지 않을 때 첫 번째 홉 라우터에 의해 송신
15	우선 순위 차단	받은 패킷의 우선 순위 값이 그 네트워크에서 허용된 최소값보다 작을 때 라우터가 송신

ICMPv4 오류 메시지 유형

- ICMPv4 송신 속도 낮춤 메시지
  - 정의
    - 수신 장비의 버퍼가 모두 채워진 경우 송신 장비에게 송신 속도를 낮춰 달라고 요청하는 메시지
  - 수신 버퍼의 혼잡 상황
    - 하나의 목적지 장비가 여러 출발지 장비에서 온 데이터그램을 받는 경우
    - 수신 장비의 처리 속도보다 송신 장비의 송신 속도가 더 빠른 경우
    - 데이터그램이 장비에서 처리되지 못한 채로 남아 있는 경우

ICMPv4 오류 메시지 유형

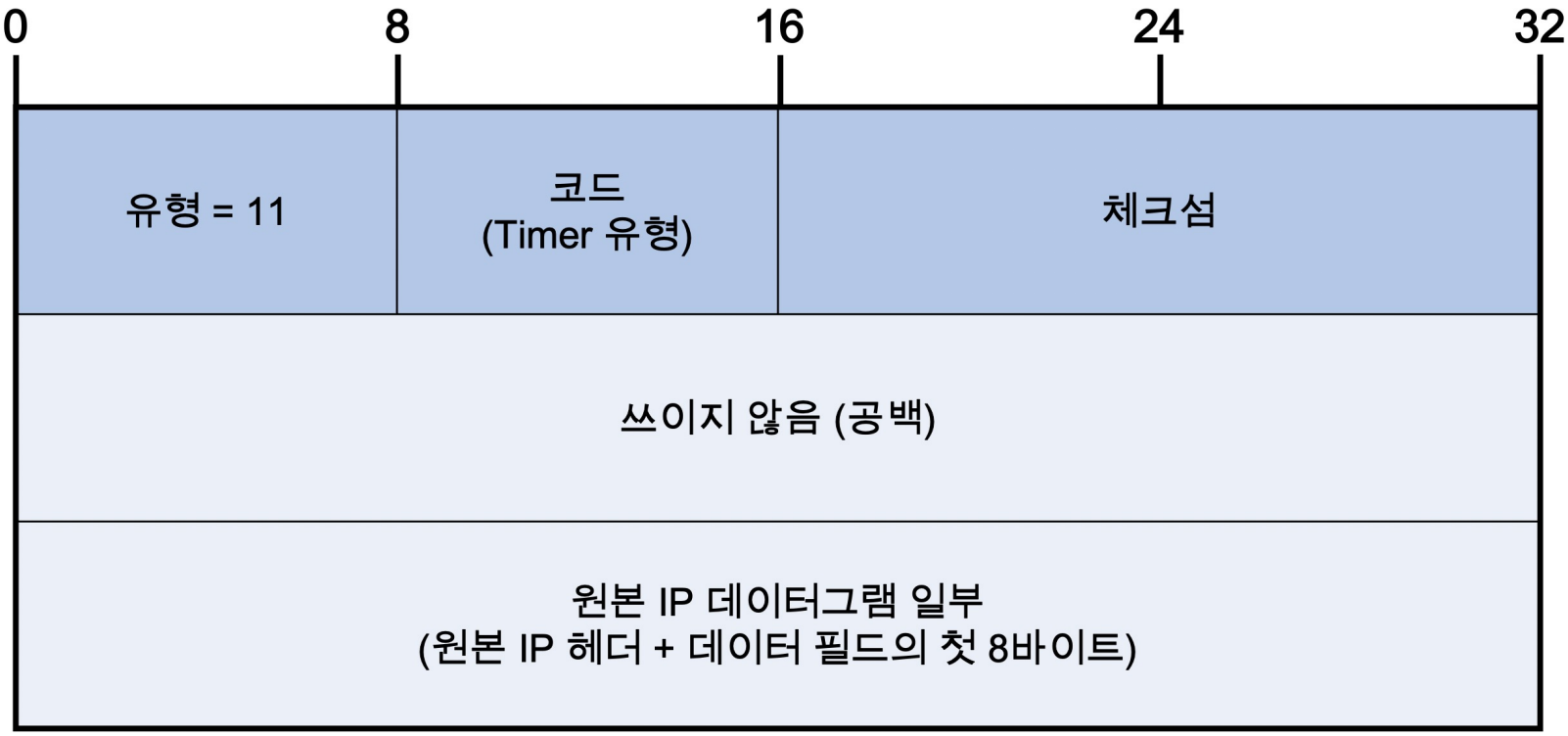
- ICMPv4 송신 속도 낮춤 메시지
  - 메시지 포맷



  - 한계
    - 출발지 장비에게 혼잡 상태가 해제되었다는 사실을 알려줄 방법이 존재하지 않음
      - 낮춘 송신율을 계속 사용함
  - 해결 방안
    - 출발지 장비는 메시지가 오지 않을 때까지 전송률을 낮추고, 이후에 천천히 전송률을 올림

ICMPv4 오류 메시지 유형

- ICMPv4 시간 초과 메시지
  - 정의
    - 송신 장비에게 데이터그램의 수명이 만료되었다고 알리는 메시지
  - 포맷



ICMPv4 오류 메시지 유형

- ICMPv4 시간 초과 메시지
  - ICMPv4 시간 초과 메시지 하위 유형

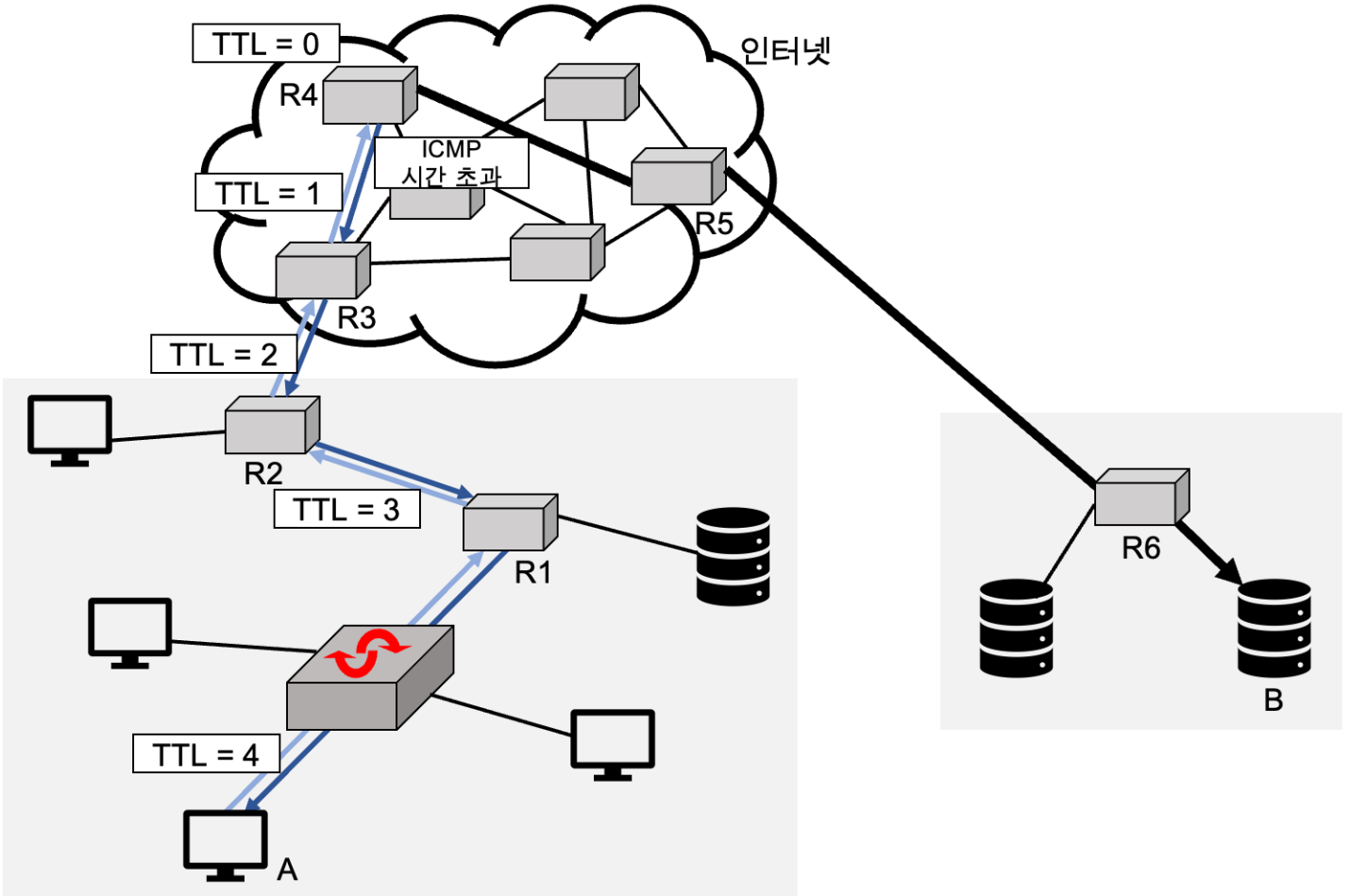
코드 값	메시지 하위 유형	설명
0	TTL 필드 만료	TTL(Time to Live) 필드 만료에 의해 패킷을 버린 경우, 출발지 장비에게 보내는 메시지
1	재조합 타이머 만료	수신 장비가 단편화된 메시지의 첫 단편을 받은 후 재조합 타이머의 만료에 의한 전송

- TTL(Time to Live) 필드
  - 패킷이 한 장비에서 다른 장비로 전달될 수 있는 횟수에 따라서 패킷의 수명을 제한
  - 각 라우터가 데이터그램을 라우팅하는 경우, 1씩 감소

- 재조합 타이머
  - 단편화 된 데이터그램이 재조합하기 위해 지정된 시간

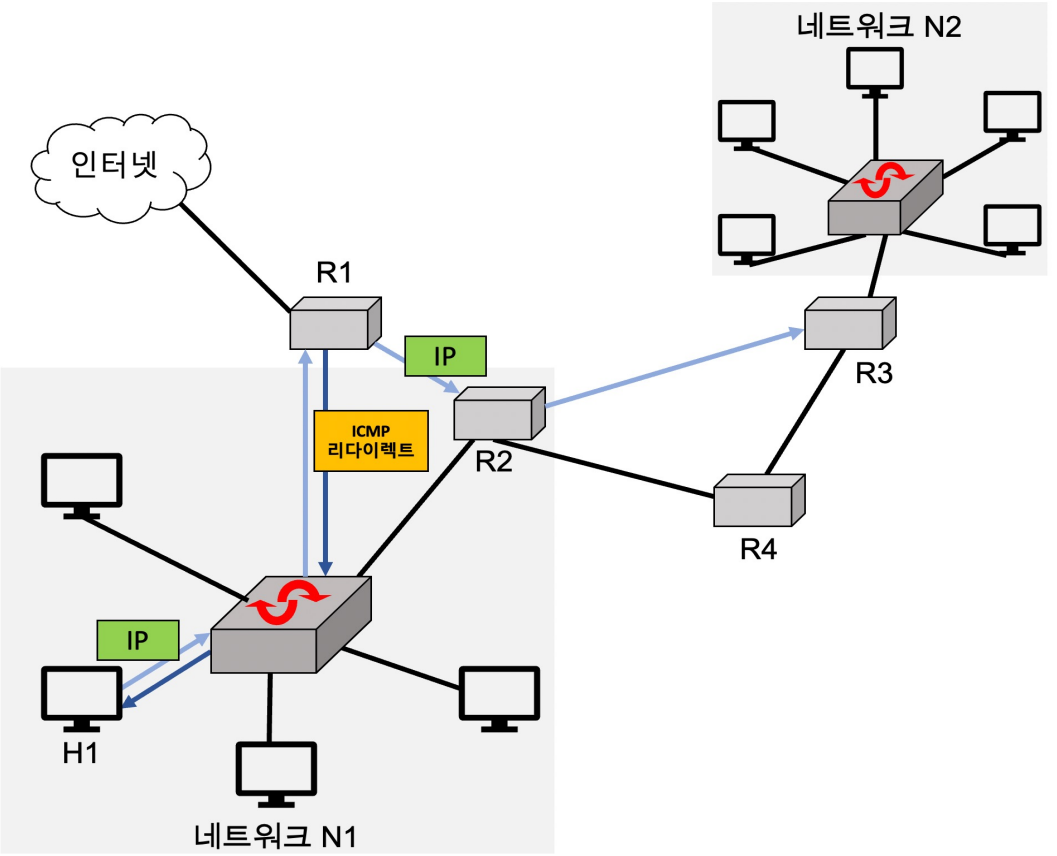
ICMPv4 오류 메시지 유형

- ICMPv4 시간 초과 메시지
  - TTL 만료 과정



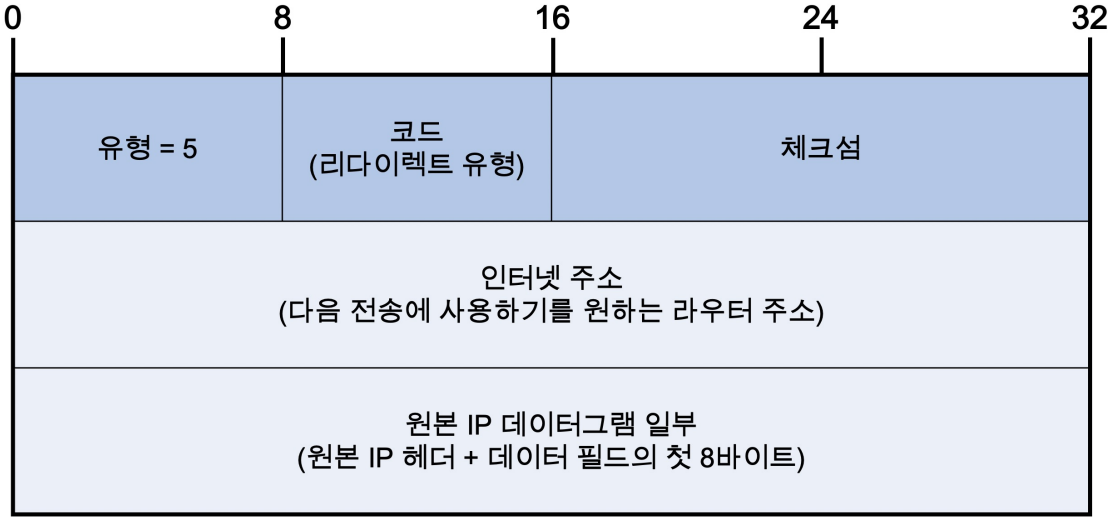
ICMPv4 오류 메시지 유형

- ICMPv4 리다이렉트 메시지
  - 정의
    - 로컬 네트워크 내에서의 통신인 경우, 더 나은 경로 정보를 제공하는 메시지



ICMPv4 오류 메시지 유형

- ICMPv4 리다이렉트 메시지
  - 메시지 포맷과 하위 유형



코드 값	메시지 하위 유형	설명
0	네트워크 또는 서브넷에 대한 리다이렉트	목적지 주소가 위치한 네트워크로 향하는 모든 패킷을 리다이렉트
1	호스트에 대한 리다이렉트	목적지 주소로 향하는 모든 패킷을 리다이렉트
2	서비스 유형(ToS)과 네트워크 또는 서브넷에 대한 리다이렉트	원본 패킷과 같은 ToS(Type of Service) 값을 갖는 패킷만을 리다이렉트
3	ToS와 호스트에 대한 리다이렉트	

ICMPv4 오류 메시지 유형

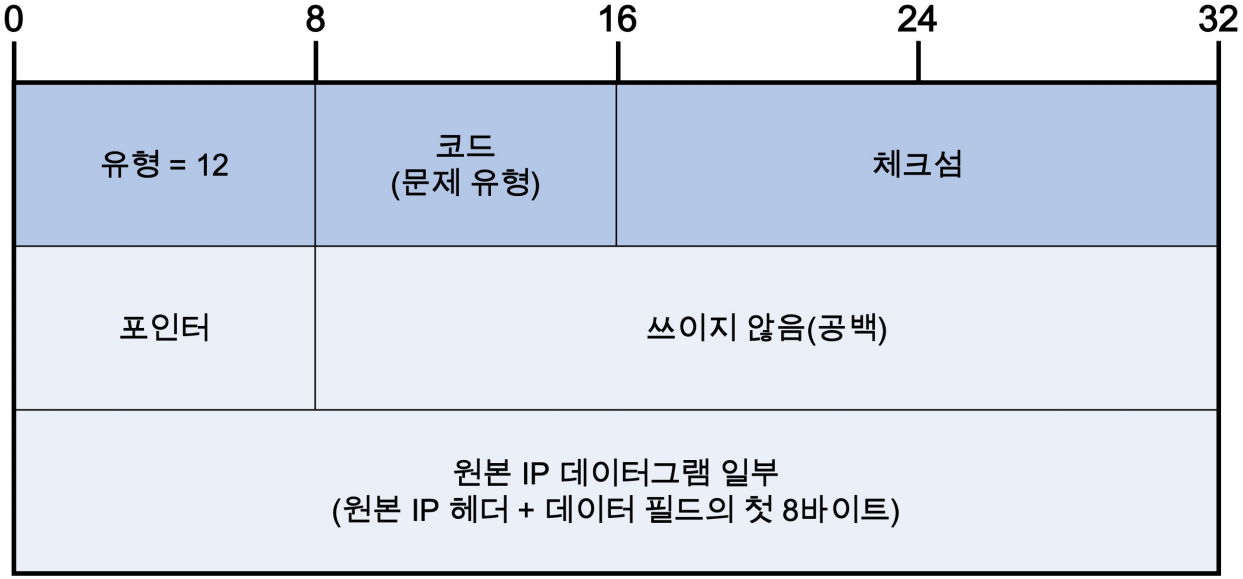
- ICMPv4 리다이렉트 메시지
  - 한계
    - 라우터 간 경로 정보 교환에 사용되지 않음
      - 로컬 라우터가 호스트에게 경로 정보를 제공하기 위한 방법임
  - 해결 방안
    - 라우팅 프로토콜 사용
      - 라우팅 테이블을 만들어 패킷이 목적지까지 가는 방법을 결정해주는 프로토콜

ICMPv4 오류 메시지 유형

- ICMPv4 인자 문제 메시지
  - 정의
    - 데이터그램의 헤더 필드에서 발생하는 오류에 대해 송신 장비에게 보내는 메시지
  - 포인터 필드
    - IP 헤더의 어떤 필드가 오류인지 나타냄

ICMPv4 오류 메시지 유형

- ICMPv4 인자 문제 메시지
  - 메시지 포맷



  - ICMPv4 인자 문제 메시지 하위 유형

코드 값	메시지 하위 유형	설명
0	포인터가 에러를 가리킴	가장 일반적인 인자 문제 메시지, 문제가 발생한 위치를 가리킴
1	필요한 옵션의 부재	IP 패킷이 가지고 있어야 할 옵션이 빠진 경우 사용
2	잘못된 길이	IP 패킷 전체의 길이가 잘못된 경우 사용

목 차

- 보충
- ICMP 개념과 일반 동작
- ICMPv4 오류 메시지 유형
- ICMPv4 정보 제공 메시지 유형

ICMPv4 정보 제공 메시지 유형

- ICMPv4 에코 요청과 응답 메시지
  - 정의
    - 장비 간 서로 통신 여부를 테스트하고 확인하는 메시지
  - 특징
    - PING(Packet Internet Groper) 테스트에서 사용
      - 컴퓨터 네트워크 상태를 점검, 진단하는 테스트
      - ping 명령어를 전송하면, 에코 요청 메시지가 지정된 주소로 전송됨
      - 호스트가 요청을 수신하면 에코 응답 메시지를 전송
      - 에코 응답 메시지를 수신, 분석하여 컴퓨터가 잘 작동하는지, 또는 네트워크 상태는 어떠한지 확인 가능
        - e.g., ping을 날려 주고받은 패킷의 손실률을 파악하여 인터넷 연결 상태 진단 가능

ICMPv4 정보 제공 메시지 유형

- ICMPv4 에코 요청과 응답 메시지
  - 메시지 포맷

필드 이름	크기 (바이트)	설명
유형	1	ICMP 메시지 유형을 식별 (에코 요청의 경우, 필드 값 8 / 에코 응답의 경우, 필드 값 0)
코드	1	에코 요청과 에코 응답 메시지에는 쓰이지 않음
체크섬	2	에러 검출
식별자	2	에코 요청과 에코 응답 메시지를 대응시키는 데 도움을 줌
순서 번호	2	
선택적 데이터	가변적	메시지와 함께 송신할 추가 데이터

ICMPv4 정보 제공 메시지 유형

- ICMPv4 타임스탬프 요청과 응답 메시지
  - 정의
    - 장비 간 메시지가 왕복하는 데 필요한 시간을 알아내고, 시간 정보를 교환할 수 있도록 하는 메시지
  - 특징
    - 메시지를 통해 두 장비들이 시간 동기화 가능
    - 세 개의 타임스탬프 필드 존재
      - 응답 장비가 요청 메시지를 수신하고 응답 메시지를 생성할 때 별도의 타임스탬프를 기록하기 때문

ICMPv4 정보 제공 메시지 유형

- ICMPv4 타임스탬프 요청과 응답 메시지
  - 메시지 포맷

필드 이름	크기 (바이트)	설명
유형	1	ICMP 메시지 유형을 식별 (타임스탬프 요청의 경우, 필드 값 13 / 타임스탬프 응답의 경우, 필드 값 14)
요청 송신 타임스탬프	4	송신 장비가 타임스탬프 요청을 송신하기 바로 전 시간
요청 수신 타임스탬프	4	수신 장비가 타임스탬프 요청을 수신한 시간
응답 송신 타임스탬프	4	타임스탬프 응답 메시지를 돌려 보내기 바로 전 시간

ICMPv4 정보 제공 메시지 유형

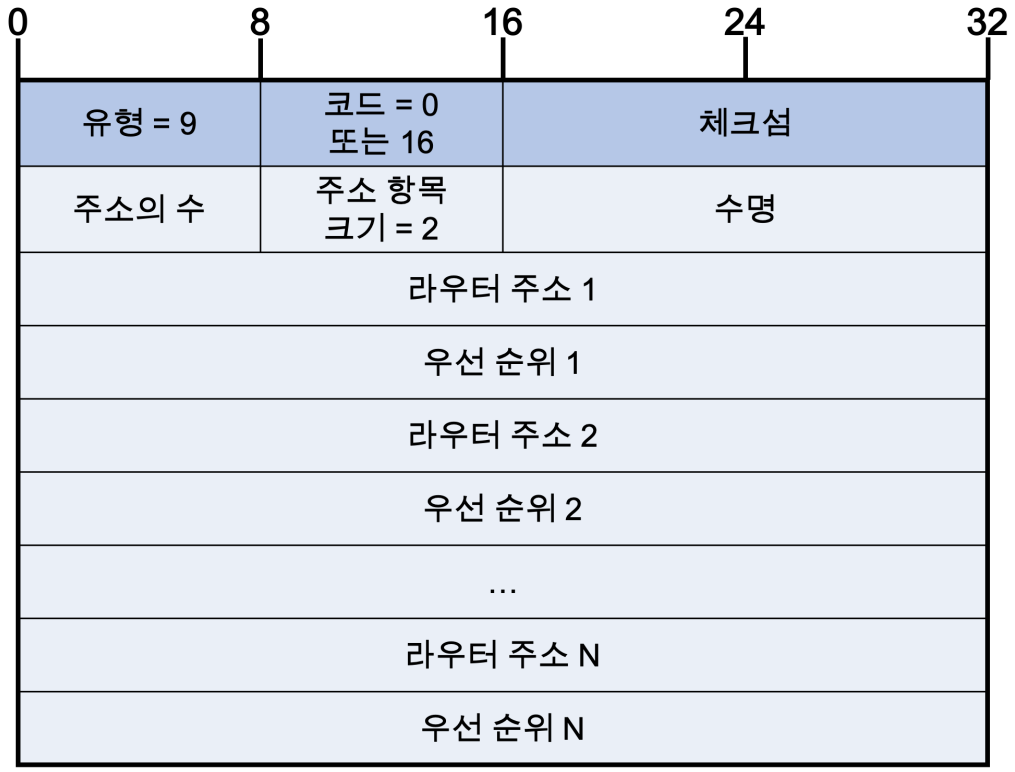
- ICMPv4 타임스탬프 요청과 응답 메시지
  - 한계
    - 타임스탬프 필드를 사용해도 시간 동기화가 어려움
      - 각 데이터그램별로 송신하는 데 걸리는 시간이 다름
      - 데이터그램을 수신하는 데 시간이 무한정 소모될 수 있음
      - 중간에서 라우터가 데이터그램을 버릴 수도 있음
  - 해결 방안
    - 네트워크 시간 프로토콜(NTP, Network Time Protocol) 사용
      - 네트워크로 연결된 모든 장비 간의 시간을 동기화 하기 위해 사용되는 프로토콜

ICMPv4 정보 제공 메시지 유형

- ICMPv4 라우터 광고와 라우터 정보 요청 메시지
  - 정의
    - 호스트가 네트워크에 연결하기 위해 하나 이상의 로컬 라우터를 알기 위해 사용되는 메시지
  - 라우터 발견(Router Discovery) 과정
    - 라우터가 정기적으로 광고 메시지를 송신
      - 7~10분 간격
    - 호스트는 라우터 광고 메시지를 받으면 라우팅 테이블에 추가
    - 라우터 정보가 없는 호스트는 라우터 광고를 요청하여 라우터 정보를 얻음

ICMPv4 정보 제공 메시지 유형

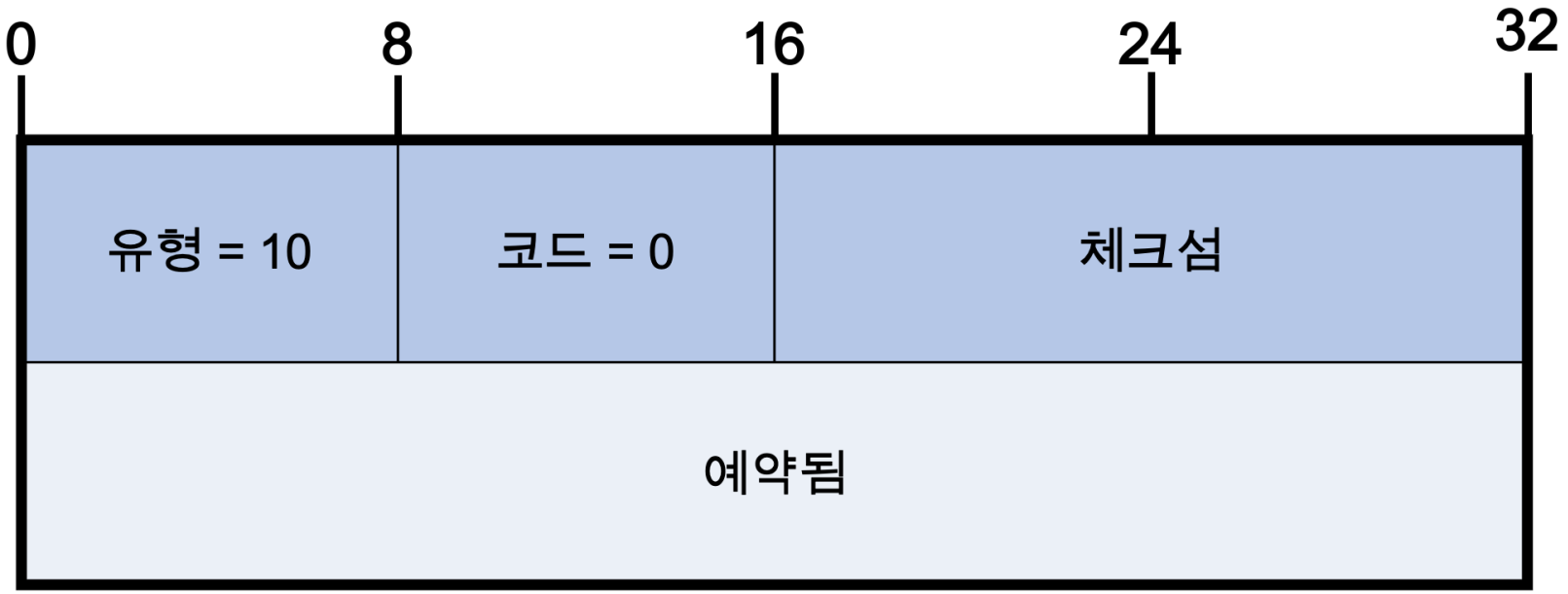
- ICMPv4 라우터 광고와 라우터 정보 요청 메시지
  - 라우터 광고 메시지 포맷



필드 이름	크기 (바이트)	설명
주소 수	1	광고 메시지에 포함된 라우터의 주소 수
주소 항목 크기	1	라우터 주소 항목과 우선 순위 값이 32비트라는 것을 나타냄 (필드 값 2)
수명	2	메시지의 유효 시간을 나타냄 (단위: 초)
라우터 주소 항목	주소 수 필드 값 X 8	주소 수 필드만큼의 라우터 주소 항목

ICMPv4 정보 제공 메시지 유형

- ICMPv4 라우터 광고와 라우터 정보 요청 메시지
  - 라우터 정보 요청 메시지 포맷



필드 이름	크기 (바이트)	설명
예약	4	예약된 필드로, 0으로 설정됨

ICMPv4 정보 제공 메시지 유형

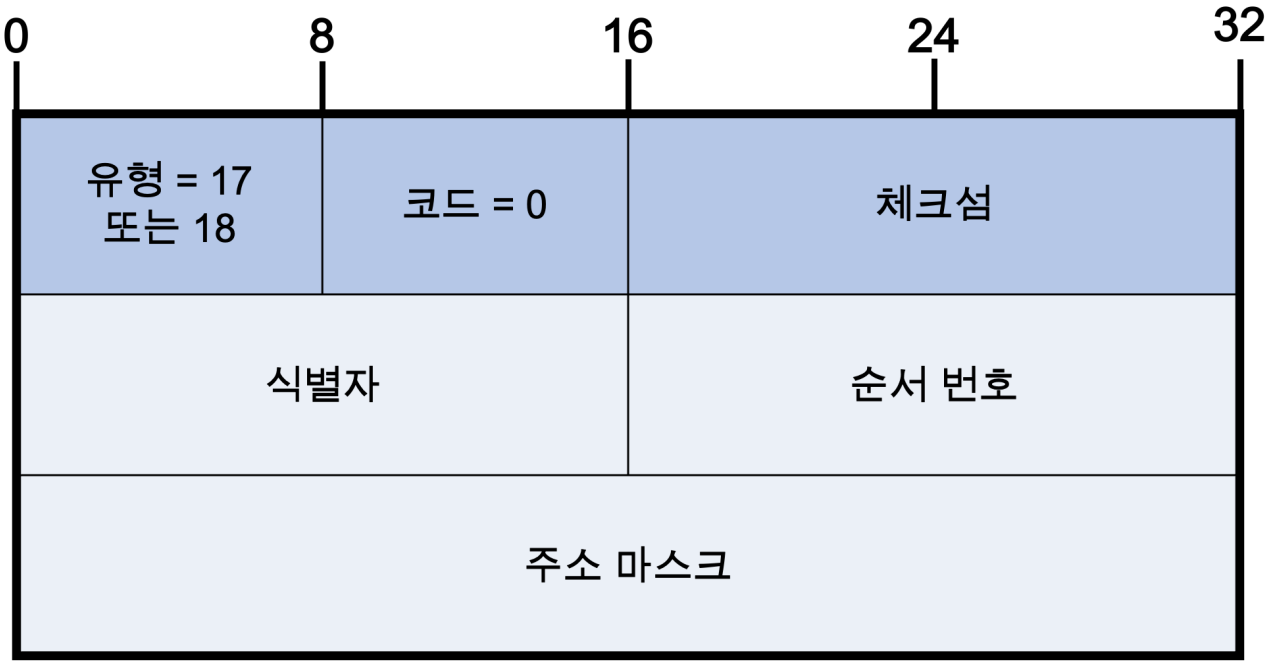
- ICMPv4 라우터 광고와 라우터 정보 요청 메시지
  - 메시지 주소 지정
    - 라우터 광고 메시지
      - 모든 장비 멀티캐스트 주소(224.0.0.1) 사용
    - 라우터 정보 요청 메시지
      - 모든 라우터 멀티캐스트 주소(224.0.0.2) 사용
    - 로컬 네트워크가 멀티캐스트를 지원하지 않는 경우
      - 브로드캐스트 주소(255.255.255.255) 사용

ICMPv4 정보 제공 메시지 유형

- ICMPv4 주소 마스크 요청과 응답 메시지
  - 정의
    - 로컬 네트워크에서 서브네팅을 사용할 때 호스트에게 서브넷 마스크 정보를 알려주는 메시지
  - 호스트의 서브넷 마스크 정보 식별 방법
    - 수동 방법
      - 각 호스트에 수동으로 서브넷 마스크 할당
    - 자동 방법
      - 호스트는 로컬 네트워크에 주소 마스크 요청 메시지 보냄
      - 라우터는 메시지를 수신한 후 호스트에게 주소 마스크 응답 메시지 보냄

ICMPv4 정보 제공 메시지 유형

- ICMPv4 주소 마스크 요청과 응답 메시지
  - 포맷 설명



필드 이름	크기 (바이트)	설명
유형	1	ICMP 메시지 유형을 식별 (주소 마스크 요청의 경우, 필드 값 17 / 주소 마스크 응답의 경우, 필드 값 18)
주소 마스크	4	로컬 네트워크의 서브넷 마스크

ICMPv4 정보 제공 메시지 유형

- ICMPv4 경로 추적 메시지
  - 정의
    - 시간 초과 메시지를 응용하여 목적지까지의 라우터의 경로를 파악하기 위한 메시지
  - 동작 과정
    - 송신 장비가 수신 장비에게 Traceroute IP 옵션을 포함한 패킷을 TTL을 증가시키며 전송
    - 두 장비 사이의 각 라우터는 옵션 확인 후, 송신 장비에게 ICMP 경로 추적 메시지 송신

ICMPv4 정보 제공 메시지 유형

- ICMPv4 경로 추적 메시지
  - 포맷 설명

필드 이름	크기 (바이트)	설명
코드	1	송신한 데이터그램이 성공적으로 전달된 경우, 코드 값이 0 / 데이터그램이 버려진 경우, 코드 값 1
ID 번호	2	송신 장비 원본 메시지를 구분하기 위한 식별자 필드
아웃바운드 홉 수	2	원본 메시지가 지금까지 거쳐 온 라우터 수
리턴 홉 수	2	리턴 메시지가 거쳐 온 라우터 수
출력 링크 속도	4	경로 추적 메시지가 송신되는 링크의 속도 (단위: B/s)
출력 링크 MTU	4	메시지가 송신되는 링크의 최대 전송 단위를 바이트 수로 나타냄

Thanks!

손 우 영 (wooyoung@pel.sejong.ac.kr)