

Chapter 04. IP 통신과 라우팅

ICMP

목차

- ICMP의 정의
- ICMP의 기능

ICMP의 정의

- **ICMP(Internet Control Message Protocol)**
인터넷 제어 메시지 프로토콜

IP 통신은 목적지에 패킷을 정상적으로 전달하는 방법은 있지만 에러 발생시 처리 불가

ICMP는 IP 통신의 에러 상황을 출발지에 전달 & 메시지 제어 역할

RFC 792, 1981년 소개됨

ICMP는 IPv4 패킷으로 캡슐화

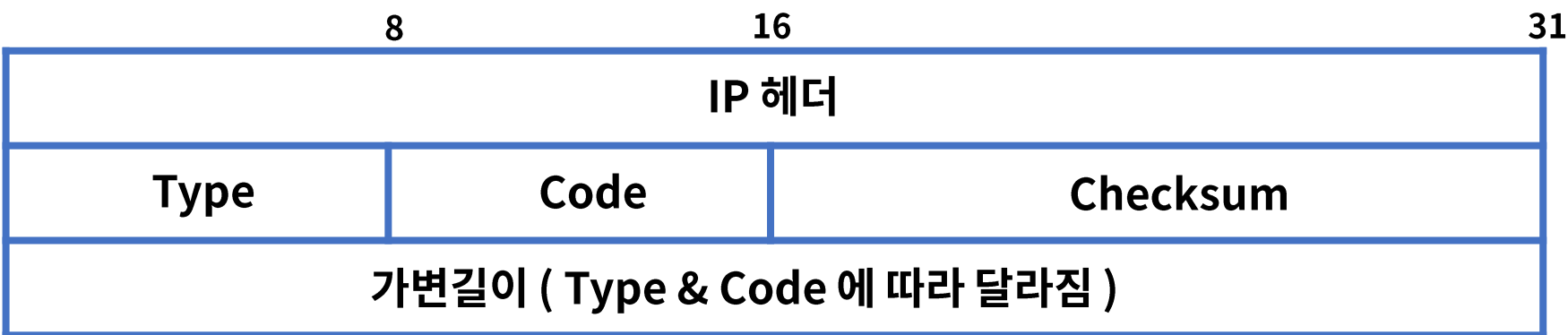
Protocol ID = 1

Ping & Traceroute 명령어를 사용

ICMP의 기능

- ICMP 포맷 구조

IP 패킷에 포함



Type: ICMP 메시지 종류

Code: 메시지 Type 별 세부 코드 정보

Checksum: ICMP 헤더 손상 여부 확인

ICMP의 기능

- ICMP Type

<https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml>

0 ~ 254 까지 정의

주로 쓰이는 타입은 아래와 같으며 오류 보고 & 정보성으로 나눈다

정보용: 8, 0, 9, 10

오류 보고용: 3, 5, 11, 12

Type	Name	Reference
0	Echo Reply	[RFC792]
3	Destination Unreachable	[RFC792]
5	Redirect	[RFC792]
8	Echo	[RFC792]
9	Router Advertisement	[RFC1256]
10	Router Solicitation	[RFC1256]
11	Time Exceeded	[RFC792]
12	Parameter Problem	[RFC792]

ICMP의 기능

- Type 8 & 0 Echo Request & Reply

네트워크 문제 진단시 사용

출발지에서 목적지 IP로 ICMP Echo Request 메시지를 보내면 목적지는 Echo Reply로 응답

목적지 도달 여부, RTT(Round-Trip delay Time), hop count 확인

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

Ping 8.8.8.8 32바이트 데이터 사용:
8.8.8.8의 응답: 바이트=32 시간=161ms TTL=114
8.8.8.8의 응답: 바이트=32 시간=76ms TTL=114
8.8.8.8의 응답: 바이트=32 시간=70ms TTL=114

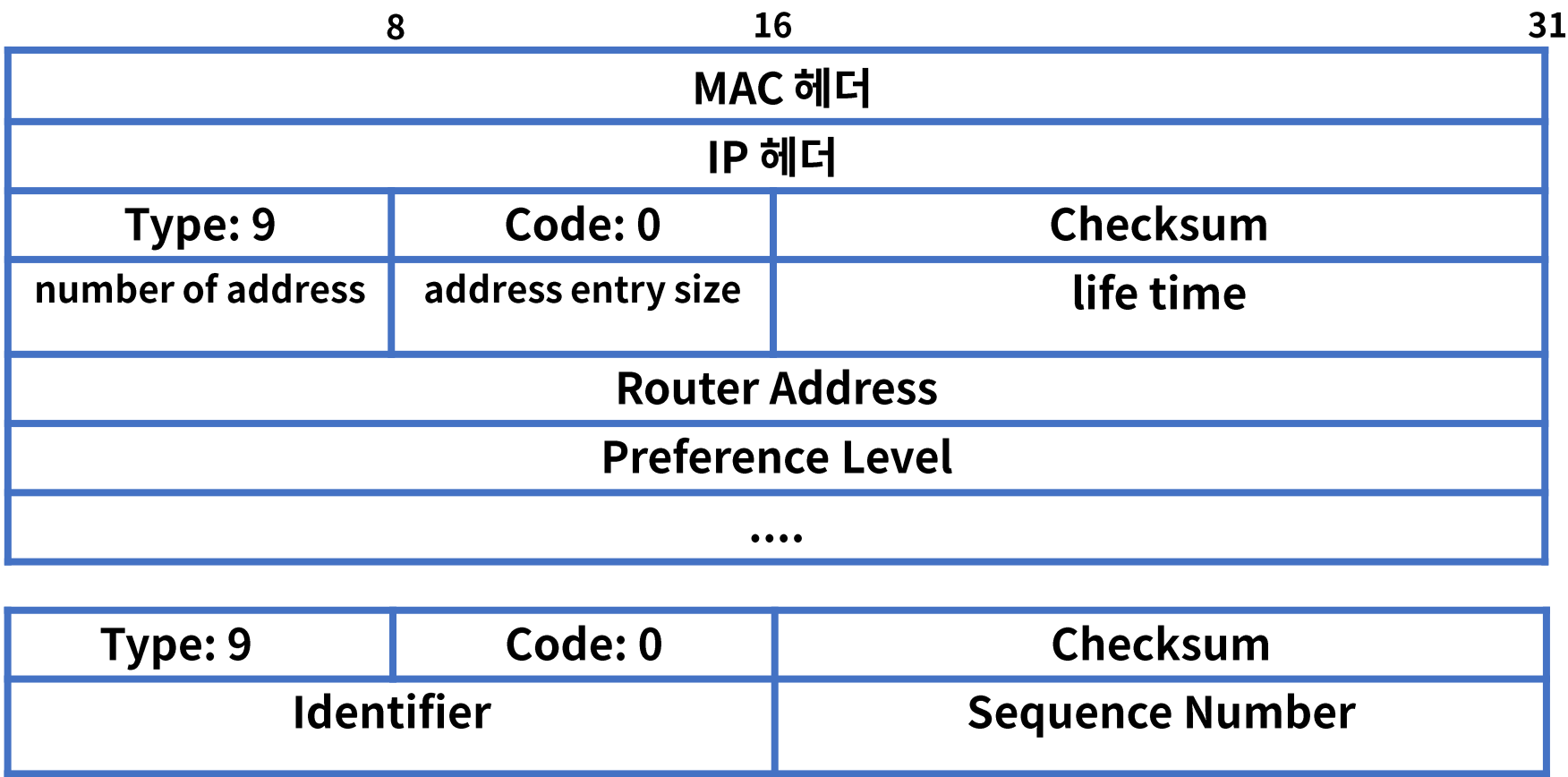
8.8.8.8에 대한 Ping 통계:
    패킷: 보냄 = 3, 받음 = 3, 손실 = 0 (0% 손실),
    왕복 시간(밀리초):
        최소 = 70ms, 최대 = 161ms, 평균 = 102ms
```

TTL값에 따라서 일반적인 OS 종류를 알수 있다
Windows 계열 128, linux 계열 64

ICMP의 기능

- Type 9 & 10 라우터 광고 & 정보 요청

자신이 라우터 임을 응답 & 네트워크 진입시 라우터 정보 요청



ICMP의 기능

- Type 3 Destination Unreachable & 5 Redirect

라우터가 IP 패킷을 라우팅 하지 못하는 경우에 발생

0 = net unreachable

1 = host unreachable

2 = protocol unreachable

3 = port unreachable

4 = fragmentation needed and DF set

5 = source route failed

Type 5 Redirect: 로컬 네트워크에 2개 이상의 경로가 있을때 더 좋은 경로를 알려줌

```
Pinging [redacted] with 32 bytes of data:  
Reply from [redacted]: Destination host unreachable.  
Reply from [redacted]: Destination host unreachable.  
Reply from [redacted]: Destination host unreachable.  
Reply from [redacted]: Destination host unreachable.
```

```
Redirect Host(New addr: [redacted])
```

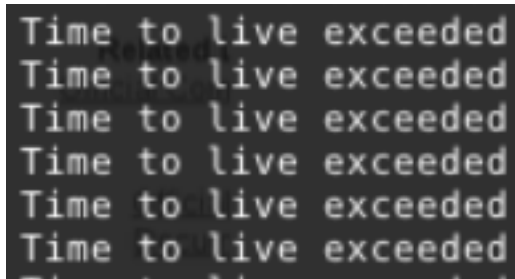

ICMP의 기능

- **Type 11 Time Exceeded & 12 Parameter Problem**

시간 초과, TTL 값이 “0”이 되면 출발지에게 응답

0 = Time to Live Exceeded

1 = Fragment Reassembly Time Exceeded



```
Time to live exceeded  
Time to live exceeded  
Time to live exceeded  
Time to live exceeded  
Time to live exceeded  
Time to live exceeded
```

IP Fragmentation : IP 패킷을 작은 패킷으로 나누어서 전송하고 목적지에서 재조합

MTU(Maximum Transmission Unit): IP 패킷을 전송할 수 있는 최대 크기

Type 12 Parameter Problem: IP 옵션을 잘못 사용하여 라우터에 패킷 폐기

ICMP의 기능

- Ping Type 8 echo Request & Type 0 echo reply

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
19	5.537868	172.20.10.2	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=95/24320, ttl=128 (reply in 20)
20	5.610267	8.8.8.8	172.20.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=95/24320, ttl=114 (request in 19)

> Frame 19: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{B7158E2F-587B-4D49-AFAA-BA995AC18FAB}, id 0
 > Ethernet II, Src: 76:b5:87:57:3a:20 (76:b5:87:57:3a:20), Dst: 76:b5:87:75:83:64 (76:b5:87:75:83:64)
 > Internet Protocol Version 4, Src: 172.20.10.2, Dst: 8.8.8.8
 > Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0x4cfc [correct]
 [Checksum Status: Good]
 Identifier (BE): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence number (BE): 95 (0x005f)
 Sequence number (LE): 24320 (0x5f00)
 [Response frame: 20]

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
19	5.537868	172.20.10.2	8.8.8.8	ICMP	74	Echo (ping) request id=0x0001, seq=95/24320, ttl=128 (reply in 20)
20	5.610267	8.8.8.8	172.20.10.2	ICMP	74	Echo (ping) reply id=0x0001, seq=95/24320, ttl=114 (request in 19)

> Frame 20: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{B7158E2F-587B-4D49-AFAA-BA995AC18FAB}, id 0
 > Ethernet II, Src: 76:b5:87:75:83:64 (76:b5:87:75:83:64), Dst: 76:b5:87:57:3a:20 (76:b5:87:57:3a:20)
 > Internet Protocol Version 4, Src: 8.8.8.8, Dst: 172.20.10.2
 > Internet Control Message Protocol
 Type: 0 (Echo (ping) reply)
 Code: 0
 Checksum: 0x54fc [correct]
 [Checksum Status: Good]
 Identifier (BE): 1 (0x0001)
 Identifier (LE): 256 (0x0100)
 Sequence number (BE): 95 (0x005f)
 Sequence number (LE): 24320 (0x5f00)
 [Request frame: 19]

ICMP의 기능

- Traceroute

Type 11 Time Exceeded

icmp						
No.	Time	Source	Destination	Protocol	Length	Info
20	12.692059	172.27.147.114	172.20.10.2	ICMP	134	Time-to-live exceeded (Time to live exceeded in transit)
21	12.693888	172.20.10.2	168.126.63.1	ICMP	106	Echo (ping) request id=0x0001, seq=107/27392, ttl=3 (no response found!)

> Frame 18: 134 bytes on wire (1072 bits), 134 bytes captured (1072 bits) on interface \Device\NPF_{B7158E2F-587B-4D49-AFAA-BA995AC18FAB}, id 0

> Ethernet II, Src: 76:b5:87:75:83:64 (76:b5:87:75:83:64), Dst: 76:b5:87:57:3a:20 (76:b5:87:57:3a:20)

> Internet Protocol Version 4, Src: 172.27.147.114, Dst: 172.20.10.2

▼ Internet Control Message Protocol

Type: 11 (Time-to-live exceeded)

Code: 0 (Time to live exceeded in transit)

Checksum: 0xc2bf [correct]

[Checksum Status: Good]

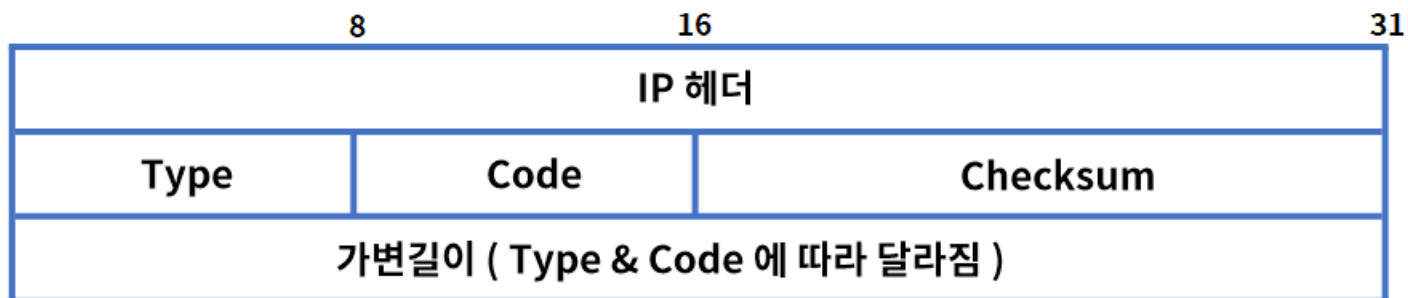
Unused: 00000000

> Internet Protocol Version 4, Src: 172.20.10.2, Dst: 168.126.63.1

> Internet Control Message Protocol

Wrap up

- ICMP(Internet Control Message Protocol)
- IP 통신의 에러 상황을 출발지에 전달 또는 메시지 제어 역할
- 포맷



- 주 타입은 정보용(8, 0, 9, 10)과 오류 보고용(3, 5, 11,12)으로 구분
- Ping & Traceroute 명령어를 통해서 사용된다