NAT&ICMP

네트워크프로그래밍

휴먼지능정보공학과
201810776 소재휘

Lab. ICMP

- Questions with Ping activities
  1. Examine one of the ping request packets sent by your host. What are the ICMP type and code numbers? What other fields does this ICMP packet have?
  2. Examine the corresponding ping reply packet. What are the ICMP type and code numbers? What other fields does this ICMP packet have?
- Questions with Traceroute activities
  1. Examine the ICMP echo packet in your screenshot. Is this different from the ICMP ping query packets in the first half of this lab? If yes, how so?
  2. Examine the ICMP error packet in your screenshot. It has more fields than the ICMP echo packet. What is included in those fields?
  3. Examine the last three ICMP packets received by the source host. How are these packets different from the ICMP error packets? Why are they different?
  4. 강의노트에서 배운 내용과 다른 점을 찾아라.

#2 ICMP

Network programming

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x4282 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 2777 (0x0ad9)
    Sequence number (LE): 55562 (0xd90a)
    [Response frame: 35]
  > Data (32 bytes)
```

PING 명령을 내린 후 관찰한 패킷이다.
ICMP 패킷의 타입은 8(Echo(ping))이었다

코드 번호는 0이다.
Type 8 Code 0은 Echo reply or request, Network unreachable이다.

헤더의 필드의 종류에는 Type, Code, Checksum, Identifier(BE, LE), Sequence number(BE, LE)가 있고 데이터 필드가 있다.

Ping을 사용하면 Echo request를 여러 개 보내게 되며 Identifier은 프로세스를 식별하기 위해 프로세스 ID를 사용하며
Sequence number은 순서를 나타내고 하나씩 증가시키며 사용하며 Request time을 같이 적어서 보내면 RTT를 계산하게 된다.

Response frame을 통해 라우터가 응답하는 것을 확인할 수 있었다.

#2 ICMP

Network programming

```
C:₩Users₩asd>traceRT www.mitedu.com

최대 30홉 이상의
www.mitedu.com [45.33.23.183](으)로 가는 경로 추적:

  1     *        *        *     요청 시간이 만료되었습니다.
  2     *        *        *     요청 시간이 만료되었습니다.
  3     6 ms     1 ms     1 ms  61.254.6.77
  4     2 ms     1 ms     2 ms  10.47.254.154
  5     4 ms    42 ms    28 ms  10.222.15.180
  6     4 ms     3 ms     3 ms  118.217.96.147
  7   138 ms   138 ms   139 ms  118.221.7.125
  8   135 ms   135 ms   140 ms  ix-xe-0-1-0-2-0.tcore1.eql-los-angeles.as6453.net [206.82.129.121]
  9   187 ms   185 ms   215 ms  if-ae-30-2.tcore1.lvw-los-angeles.as6453.net [206.82.129.19]
 10   176 ms   176 ms   177 ms  if-ae-34-2.tcore2.dt8-dallas.as6453.net [66.110.57.20]
 11   181 ms   180 ms   179 ms  if-ae-11-2.tcore1.xz3-dallas.as6453.net [66.110.57.102]
 12   176 ms   173 ms   172 ms  64.86.188.35
 13   180 ms   181 ms   179 ms  45.79.12.5
 14   171 ms   171 ms   172 ms  li977-183.members.linode.com [45.33.23.183]

추적을 완료했습니다.
```

TraceRT 명령을 내렸다.

#2 ICMP

Network programming

```
Internet Protocol Version 4, Src: 172.16.25.233, Dst: 45.33.23.183
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 92
    Identification: 0x3983 (14723)
  > Flags: 0x0000
  > Time to live: 1
    Protocol: ICMP (1)
    Header checksum: 0x754d [validation disabled]
    [Header checksum status: Unverified]
    Source: 172.16.25.233
    Destination: 45.33.23.183
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xed1c [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 2786 (0x0ae2)
    Sequence number (LE): 57866 (0xe20a)
  v [No response seen]
      > [Expert Info (Warning/Sequence): No response seen to ICMP request]
  > Data (64 bytes)
```

TraceRT 명령을 내렸다.
다음 패킷을 보면 Echo request에 대해서 응답을 하지 않는 라우터가 존재하는 것도 확인할 수 있었다. 또한 데이터의 byte 또한 64byte로 차이가 나는 것을 알 수 있다.

#2 ICMP

Network programming

10	0.814472	172.16.25.233	45.33.23.183	ICMP	106	Echo (ping) request id=0x0001, seq=2786/57866, ttl=1 (no response found…
69	4.631617	172.16.25.233	45.33.23.183	ICMP	106	Echo (ping) request id=0x0001, seq=2787/58122, ttl=1 (no response found…
128	8.631566	172.16.25.233	45.33.23.183	ICMP	106	Echo (ping) request id=0x0001, seq=2788/58378, ttl=1 (no response found…
166	12.632421	172.16.25.233	45.33.23.183	ICMP	106	Echo (ping) request id=0x0001, seq=2789/58634, ttl=2 (no response found…
217	16.633314	172.16.25.233	45.33.23.183	ICMP	106	Echo (ping) request id=0x0001, seq=2790/58890, ttl=2 (no response found…
284	20.687534	172.16.25.233	45.33.23.183	ICMP	106	Echo (ping) request id=0x0001, seq=2791/59146, ttl=2 (no response found…
380	24.634270	172.16.25.233	45.33.23.183	ICMP	106	Echo (ping) request id=0x0001, seq=2792/59402, ttl=3 (no response found…

다음과 같이 라우터에 패킷이 도착할 때 마다 ttl을 1씩 증가시키는 것을 확인할 수 있다.

#2 ICMP

Network programming

```
Internet Control Message Protocol
Type: 11 (Time-to-live exceeded)
Code: 0 (Time to live exceeded in transit)
Checksum: 0xf4ff [correct]
[Checksum Status: Good]
Unused: 00000000
Internet Protocol Version 4, Src: 172.16.25.233, Dst: 45.33.23.183
   0100 .... = Version: 4
   .... 0101 = Header Length: 20 bytes (5)
> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
   Total Length: 92
   Identification: 0x3989 (14729)
> Flags: 0x0000
> Time to live: 1
   Protocol: ICMP (1)
   Header checksum: 0x7547 [validation disabled]
   [Header checksum status: Unverified]
   Source: 172.16.25.233
   Destination: 45.33.23.183
Internet Control Message Protocol
   Type: 8 (Echo (ping) request)
   Code: 0
   Checksum: 0xed16 [unverified] [in ICMP error packet]
   [Checksum Status: Unverified]
   Identifier (BE): 1 (0x0001)
```

ICMP 에러 패킷을 검사하였다. 여기에는 더 많은 필드가 포함되어 있었다 . 우선 오류의 타입은 11(Time-to-live exceeded)로 TTL동안 전달되지 못하였다. 이는 라우터를 거칠 때 마다 TTL을 1씩 감소시키는데 0이 되어서 Error에 대한 reply가 전달된 것이다.

이 에러 난 패킷에 대해 정보를 전달해 주는 방법은
에러 난 패킷의 앞부분을 잘라서 보내주는 것 이다.
(Error난부분의 IP header부분과 추가적인 8byte(transport layer의 헤더 정보))

여기에는 IPV4 프로토콜의 정보와 원래 보내려고 했던 ICMP의 정보가 담겨 있다.

#2 ICMP

Network programming

```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xf4f4 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 2826 (0x0b0a)
    Sequence number (LE): 2571 (0x0a0b)
    [Request frame: 1415]
    [Response time: 171.742 ms]
```

```
Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0xecf3 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 2827 (0x0b0b)
    Sequence number (LE): 2827 (0x0b0b)
    [Response frame: 1422]
  > Data (64 bytes)
```

```
Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0xf4f3 [correct]
    [Checksum Status: Good]
    Identifier (BE): 1 (0x0001)
    Identifier (LE): 256 (0x0100)
    Sequence number (BE): 2827 (0x0b0b)
    Sequence number (LE): 2827 (0x0b0b)
    [Request frame: 1417]
    [Response time: 172.029 ms]
```

마지막 3개의 ICMP 패킷이다. 이는 오류 패킷과 다르다. 에러가 난 패킷이 아니기 때문에 IP header부분에 대한 정보가 존재하지 않는다. 또한 Type이 reply에 해당하는 0이나 request에 해당하는 8이 되어 에러가 나지 않았음을 알 수 있다. 또한 error패킷과 다르게 ttl을 1씩 정상적으로 증가시키는 것을 확인할 수 있다.

강의 내용과 다른 점은 랜덤한 포트 number로 보내서 그에 대해서 열리지 않았다는 reply를 통해서 해당 포트를 사용할 수 있음을 확인하는데 해당 와이어 샤크 캡처에서는 Code와 Type를 일정하게 한다는 점에서 차이점이 있다.