**IP and ICMP**

**1. 실험**

1) Wireshark 실행하고 Capture 준비

2) Console 창을 연다.

3) Wireshark에서 capture 시작하자마자, console 창에 “tracert gaia.cs.umass.edu”를 타이핑하고 실행

- PATH가 설정되어 있지 않은 경우, “c:\windows\system32” 디렉토리로 이동한 후 실행

4) “tracert” 프로그램의 실행이 종료되자마자, Wireshark의 capture 중단

- 세 번째 라우터로부터 적어도 한번의 응답을 받은 후 중단해도 무방함

**2. 참고사항**

1) Internet에서 IP와 ICMP 프로토콜을 검색하여 header format과 각 field의 의미를 참고하라.

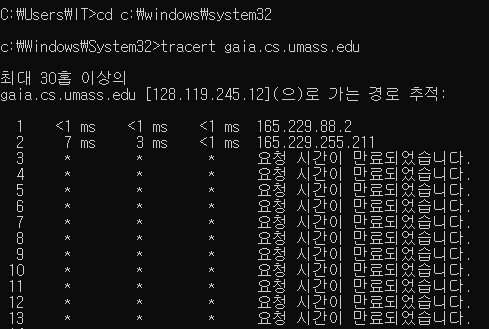
2) HSRP 프로토콜이 동작하는 라우터에서 ICMP 패킷을 생성할 때, source IP 주소로 virtual IP 대신 실제 IP가 사용된다.

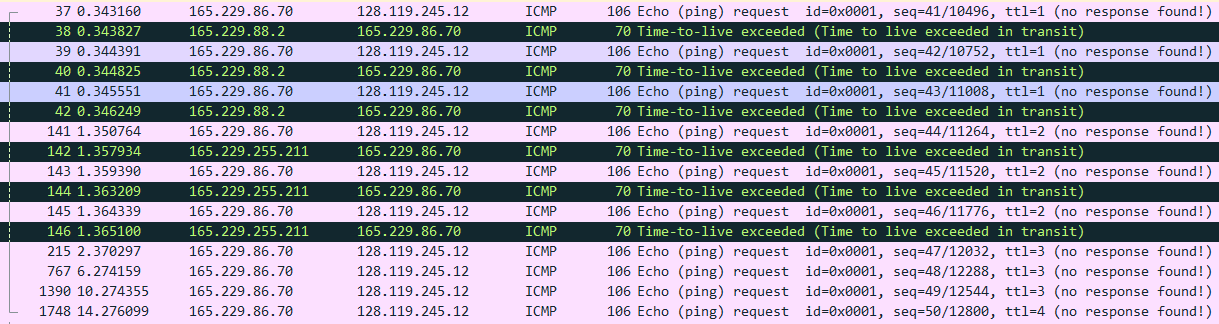
3) 라우터의 한 물리적인 포트에 복수의 서브넷이 할당될 수 있다.

- 예) 165.229.187.5/24와 165.229.125.7/24가 동일 라우터의 동일 포트에 있을 수 있음

**3. 문제**

먼저, 자기 PC의 IP address를 확인하고, 송신한 일련의 ICMP 패킷들을 찾는다.





Q1) 해당 ICMP 패킷들 중에서 첫 번째 packet의 Source IP address와 Destination IP address는?

Source IP address : 165.229.86.70

Destination IP address : 128.119.245.12

Q2) 해당 ICMP 패킷들 중에서 첫 번째 packet의 IP header에서 “Protocol” field의 값은? 해당 “Protocol”의 값이 의미하는 바는?



-> Protocol의 field는 ICMP이며, 1의 값을 가진다.

Field의 값은 1이고, 해당 protocol은 ICMP이다.

Q3) 첫 번째 packet의 IP header 크기는 몇 바이트인가? 또한, payload 크기는 몇 바이트인가?





-> IP Hedaer : 20byte, payload(= Data) : 64bytes

.Q4) 첫 번째 packet은 fragmented되었는가, 그렇지 않은가?



->fragment offset의 값이 0으로 설정되어 있기때문에, fragmented가 되어있지 않은 것을 확인할 수 있다.

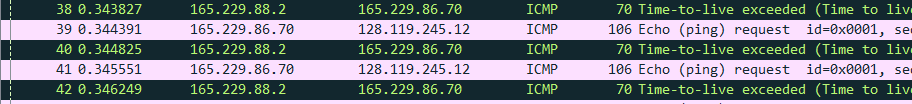
Q5) 일련의 ICMP 패킷들의 IP header를 관찰하라. 매 패킷마다 “Time-To-Live” field의 값이 어떻게 변하는지 확인하고, 그렇게 달라지는 이유를 설명하라





-> 3개의 패킷마다 “Time-To-Live” field의 값이 1씩 증가한다. 왜냐하면 전달되는 패킷이 라우터에 들어갈 때 “Time-to-live의 값이 1개씩 줄이는데, 해당 값이 0으로 바뀌는 것을 방지하고자 해당 값을 1씩 증가시킨다.

Q6) 디폴트 라우터(default router or gateway)의 IP address는 무엇이라고 생각하는가?



-> 검은색의 기록에서 알수 있듯이 첫 3개의 IP주소인 165.229.88.2이다.

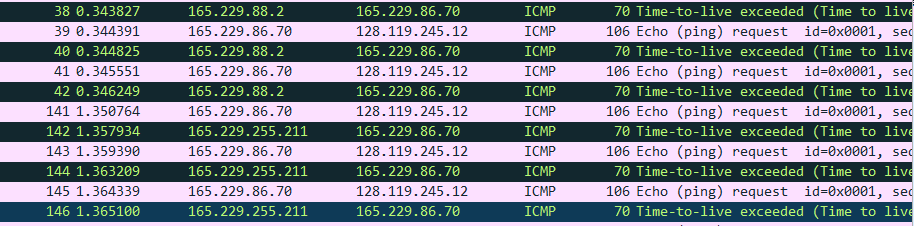
Q7) ICMP header에서 “type”과 “code”의 값은”? 해당 값이 의미하는 바는?



-> type : Echo request 값을 나타내준다. / code : subtype

해당 값들에서 수신받은 ICMP 패킷의 type을 나타내준다.

수신한 일련의 ICMP 패킷들을 찾는다

.

-> 이 가운데 검은색 패킷이 수신한 ICMP 패킷들이다.

Q8) 해당 ICMP 패킷들 중에서 첫 번째 packet의 Source IP address? 이 packet은 누가 보낸 것이라고 생각하는가?



-> 165.229.88.2

Q9) 해당 ICMP 패킷들 중에서 네 번째 packet의 Source IP address? 이 packet은 누가 보낸 것이라고 생각하는가?



-> 연결된 링크 중에서 내 PC쪽에서 2번째로 연결된 라우터가 1번째로 연결된 라우터에게 전송하였다.

Q10) 해당 ICMP 패킷들의 ICMP header에서 “type”과 “code”의 값은”? 해당 값이 의미하는 바는?



-> type : Time-to-live의 값(초과되었다고 표시), Code : Time-to-live의 값이 초과 되었는 것을 나타낸다.