**IP and ICMP**

**1. 실험**

1) Wireshark 실행하고 Capture 준비

2) 관리자 권한으로 Console 창을 열고, “arp –d \*”을 타이핑하여, ARP 캐쉬를 비운다.

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

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 ARP, IP, 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.

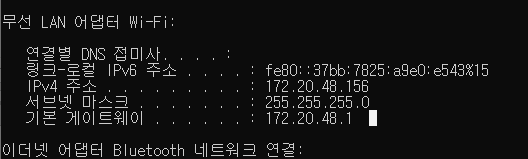
3) 라우터의 한 물리적인 포트에 복수의 서브넷이 할당될 수 있다.

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

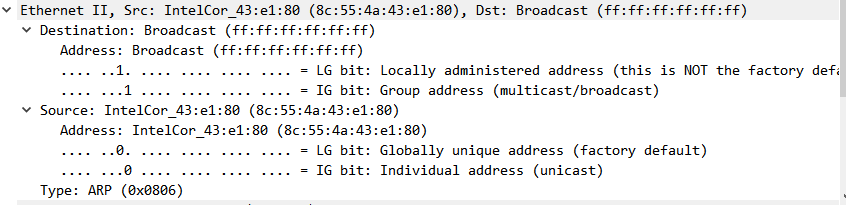
**3. 문제**

Capture된 packets 중에서 ARP request packet을 찾아, 화면 캡쳐하라.





Q1) 그 packet의 Ethernet source address와 destination address를 16진수로 표기하라.



Ethernet source address (8c:55:4a:43:e1:80)

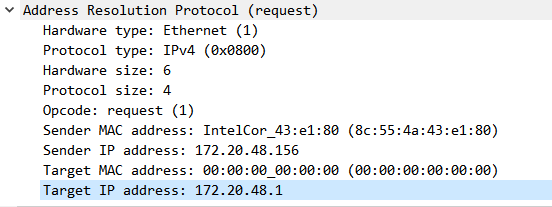
destination address (ff:ff:ff:ff:ff:ff)

Q2) 그 packet의 Ethernet header의 “Frame Type” field 값은 (16진수로 표기)? 해당 “Frame Type”이 의미하는 바는?



프레임 타입이 ARP타입인 패킷이다.

Q3) 그 packet은 어떤 IP address에 대한 Ethernet address를 묻고 있는가?

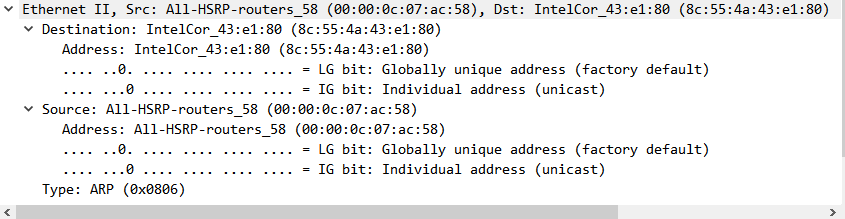


172.20.48.1인 ip address에 대한 ethernet address를 묻고 있다.

Capture된 packets 중에서 해당 ARP request에 대응하는 ARP response packet을 찾아, 화면 캡쳐하라.



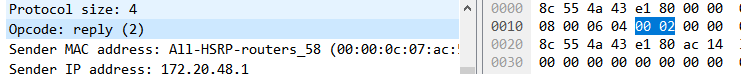
Q4) 그 packet의 Ethernet source address와 destination address를 16진수로 표기하라.



Ethernet source address (00:00:0c:07:ac:58)

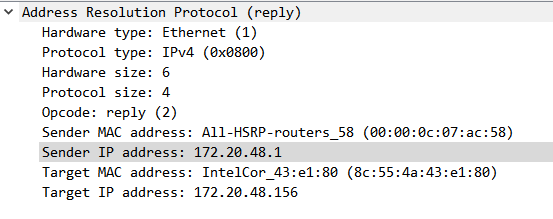
destination address (8c:55:4a:43:e1:80)

Q5) 그 packet의 “Operation” field 값은 (16진수로 표기)?



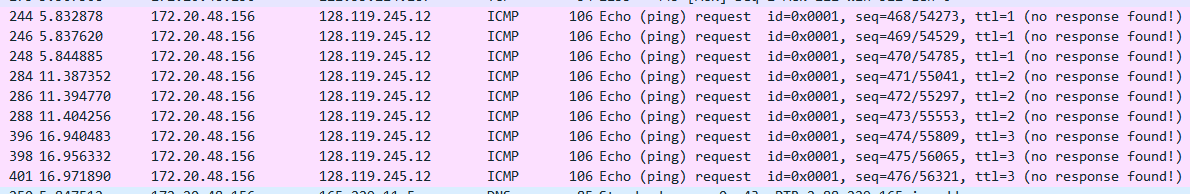
* 0x0002

Q6) ARP request의 “Target IP address”에 대응되는 Ethernet address는 ARP response packet의 어느 부분에 명시되어 있는가?

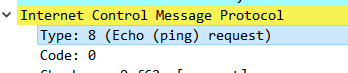


Sender ip address에 명시되어있다.

자기 PC의 IP address를 확인한 후, 송신한 일련의 ICMP 패킷들을 찾는다.



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



Type: echo request 타입 (사용되는 프로그램 도구는 ping)

Code: 타입에 대한 상세한 설명. 0이므로 네트워크 도달불가

Q8) 첫 번째 packet의 Source IP address와 Destination IP address는? 해당 Source IP address와 Destination IP address는 각각 누구를 가리키는가?



각각 사용자의 컴퓨터와 gaia.cs.umass.edu

Q9) 첫 번째 packet의 IP header 크기는 몇 바이트인가? 또한, payload 크기는 몇 바이트인가?

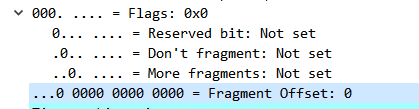


Ip header의 크기는 20 바이트이고,



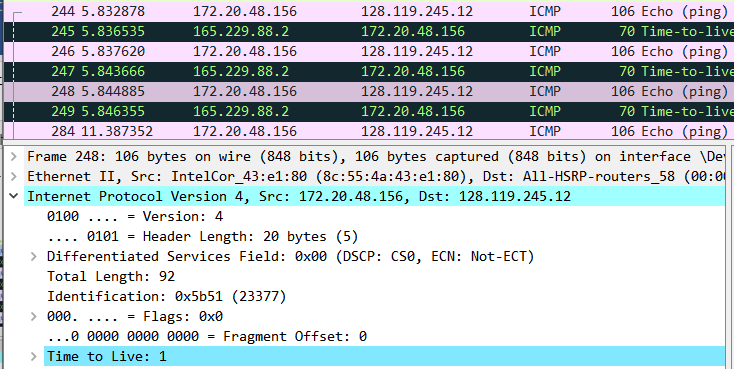
Payload의 크기는 64바이트이다.

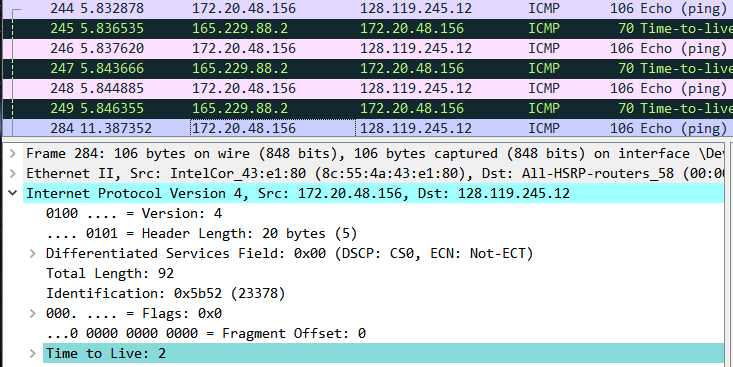
Q10) 첫 번째 packet은 fragmented되었는가, 그렇지 않은가?



fragmented되지 않았다.

Q11) 일련의 ICMP 패킷들의 IP header를 관찰하라. 매 패킷마다 “Time-To-Live” field의 값이 어떻게 변하는지 확인하고, 그렇게 달라지는 이유를 설명하라





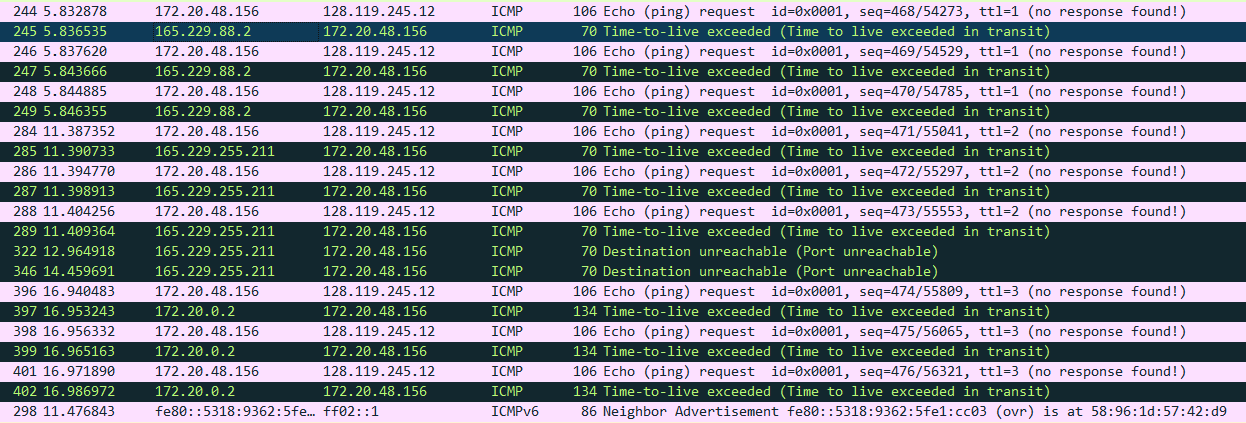
1부터 시작해서 세 패킷마다 Time to live가 1씩 증가하는 것을 확인할 수 있다.

즉, time to live는 한 홉을 거칠 때 마다 1씩 증가하며 경로를 체크하도록 한다.

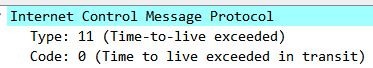
Q12) 내 디폴트 라우터(default router or gateway)의 IP address는 무엇이라고 생각하는가?

172.20.48.1

수신한 일련의 ICMP 패킷들을 찾는다.



Q13) 해당 ICMP 패킷들의 ICMP header에서 “type”과 “code”의 값은”? 해당 값이 의미하는 바는?



Type: Time to live 초과되었음을 의미

Code: 타입에 대한 상세한 설명. 0이므로 네트워크 도달불가 즉, 패킷이 gaia에 도착하기 전에 Time to live 필드값이 0이 됨

Q14) 해당 ICMP 패킷들 중에서 첫 번째 packet의 Source IP address? 이 packet은 누가 보낸 것이라고 생각하는가?



Source ip address : 172.20.48.156

Gaia로 보내는 패킷 경로 중에 첫번째 라우터가 보낸 것

Q15) 해당 ICMP 패킷들 중에서 네 번째 packet의 Source IP address? 이 packet은 누가 보낸 것이라고 생각하는가?



Source ip address : 172.20.48.156

Gaia로 보내는 패킷 경로 중에 두번째 라우터가 보낸 것