Chapter 6

주소 변환 프로토콜(ARP)

학습목표(OBJECTIVES):

- 논리 주소 (IP 주소)와 물리 주소 (MAC 주소)간의 차이점을 이해
- ARP (address resolution protocol)에 의하여 논리 주소가 동적으로 물리 주소로 변환하는 방법 설명
- 서브넷팅 효과를 얻기 위해 프록시(proxy) ARP(디폴트 게이트웨이인 라우터)를 사용하는 방법

6-1 주소 변환(ADDRESS MAPPING)

호스트나 라우터로 패킷을 전달하기 위해서는 두 레벨의 주소지정이 필요하다: 논리(logical)와 물리(physical). 따라서, 논리 주소를 대응하는 물리 주소로 또는 그 반대로 변환하는 기능이 필요하다.

인터넷에서 사용하는 주소

1. 논리 주소(logical address)

- 호스트나 라우터가 사용하는 네트워크 레벨 주소
- 전세계적으로 유일한 주소
- IP 주소
- 32 비트 길이

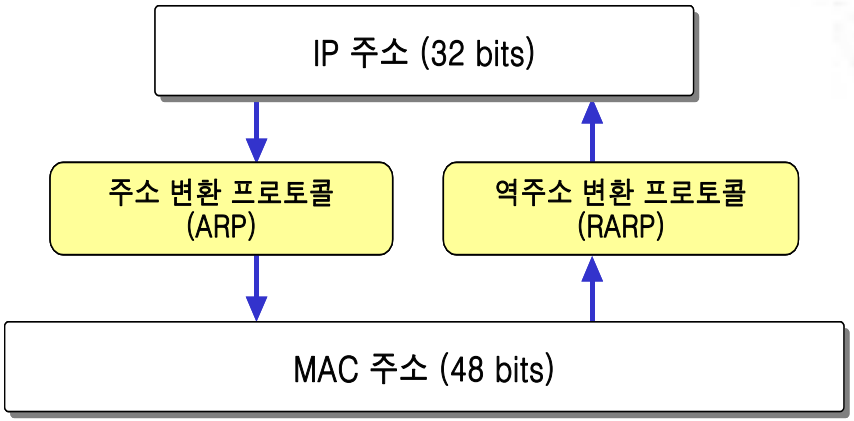
2. 물리 주소(physical address)

- 로컬 네트워크에서 유효한 주소
- 로컬 주소(local address)
- 로컬에서만 유일하면 됨
- 보통 하드웨어로 구현
- 호스트나 라우터내에 설치된 NIC에 들어 있음

인터넷에서 사용하는 주소

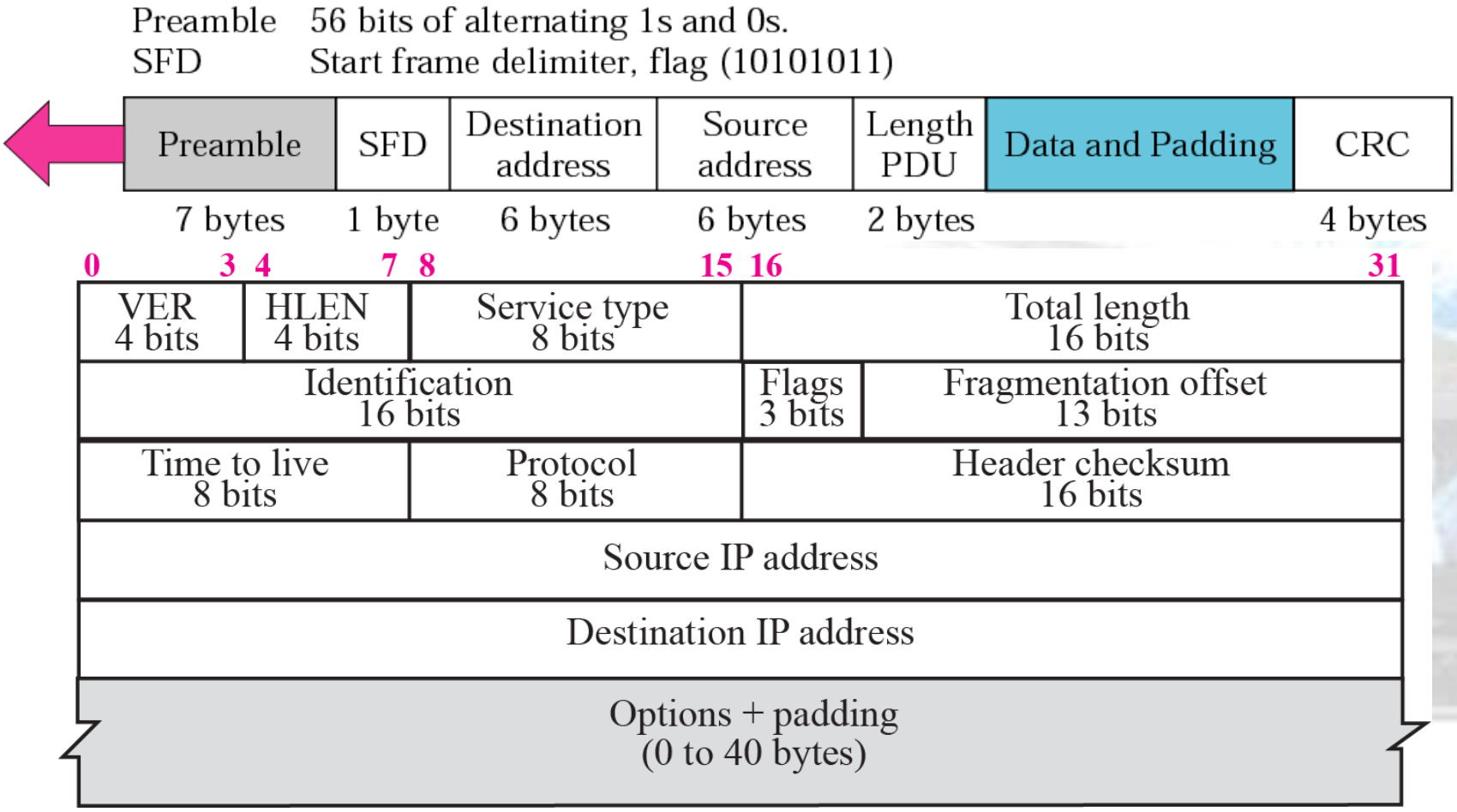
ARP와 RARP

- Address Resolution Protocol
- Reverse Address Resolution Protocol: 현재 사용하지 않음



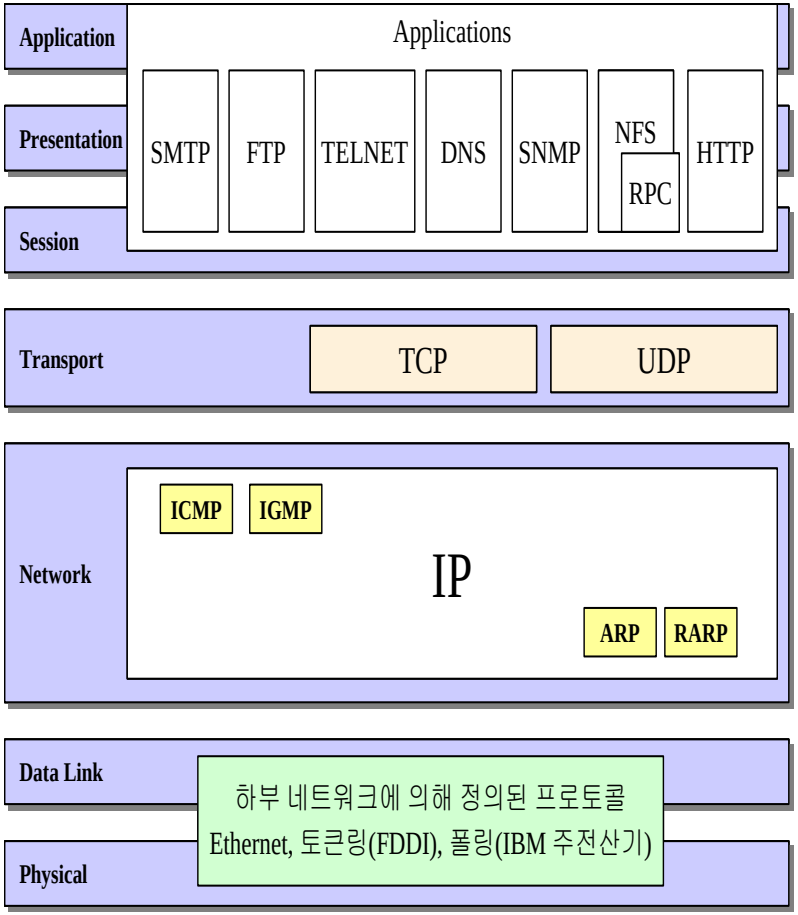
6-2 ARP 프로토콜

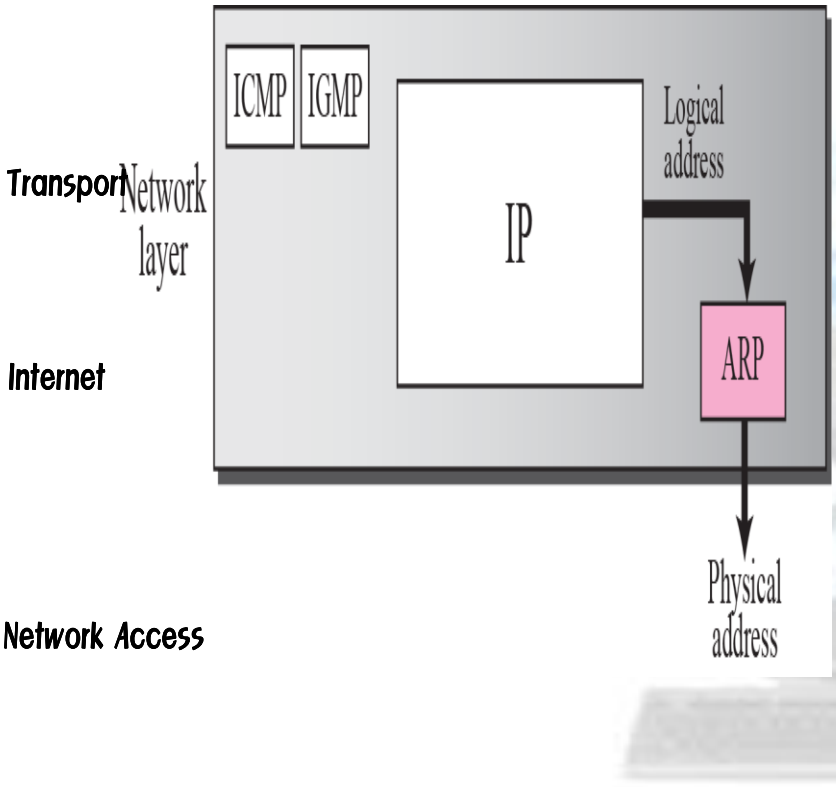
논리 주소에 대응하는 물리 주소를 찾음 : 이더넷의 헤더를 보면 프레임 형성시 필요.



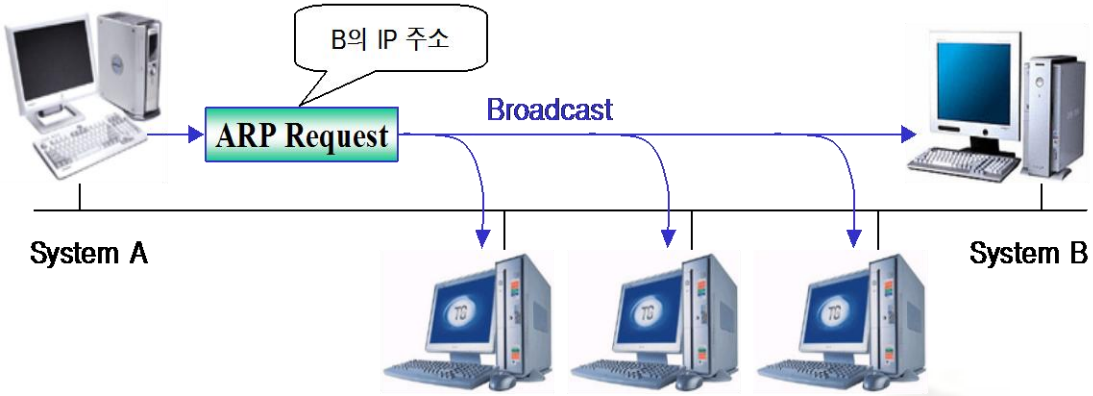
b. Header format

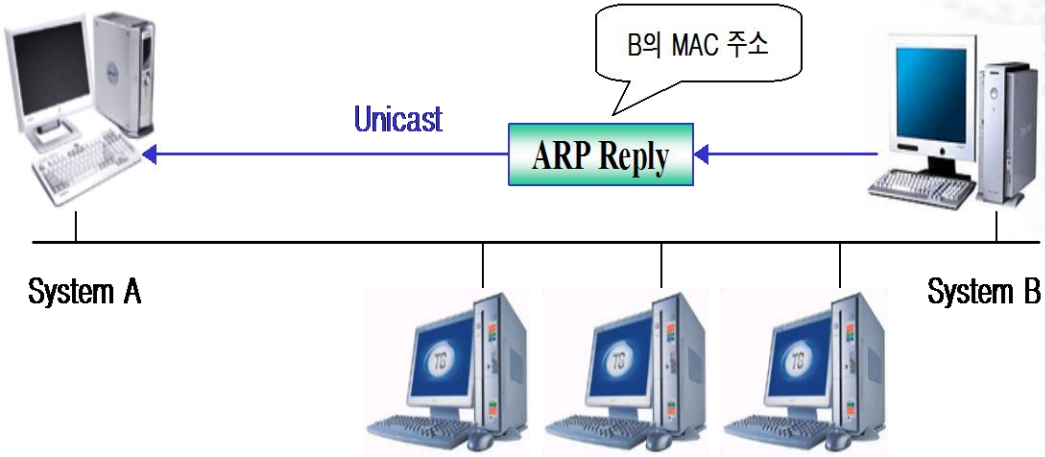
TCP/IP 프로토콜에서 ARP의 위치





ARP 동작


B의 IP 주소
ARP Request
Broadcast
System A
System B


B의 MAC 주소
Unicast
ARP Reply
System A
System B

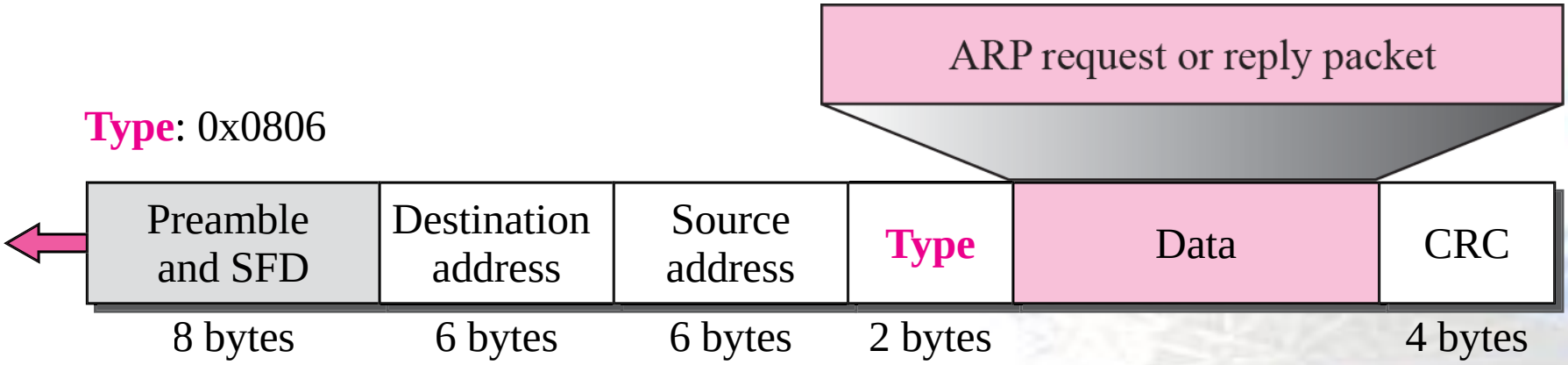
ARP 패킷


0
1
2
3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
Hardware Type(2)
Protocol Type(2)
Hardware Length(1)
Protocol Length(1)
Operation(2)
(request 1, reply 2)
Sender Hardware Address(6)
Sender Protocol Address(4)
Target Hardware Address(6)
Target Protocol Address(4)

ARP 패킷 파라메터

- **Hardware type** : 네트워크 유형 정의(이더넷 : **1**)
- **Protocol type** : 프로토콜 정의(**IPv4** : 0800_{16})
- **Hardware length** : 물리 주소의 바이트 단위 길이
- **Protocol length** : 논리 주소의 바이트 단위 길이
- **Operation** : 패킷 유형–**ARP** 요청(**1**), **ARP** 응답(**2**)
- **Sender hardware address** : 송신자 물리 주소
- **Sender protocol address** : 송신자 논리 주소
- **Target hardware address** : 타깃 물리 주소
- **Target protocol address** : 타깃 논리 주소

ARP 패킷 캡슐화


ARP request or reply packet
Type: 0x0806
Preamble and SFD
Destination address
Source address
Type
Data
CRC
8 bytes
6 bytes
6 bytes
2 bytes
4 bytes

ARP 동작

ARP 프로세스의 캡슐화 동작 과정

1. 송신자는 타깃 IP 주소를 알고 있다
2. IP가 ARP에게 ARP 요청 메시지 생성 요청
   (송신자 물리 주소, IP 주소; 타깃 IP 주소, 물리 주소(O))
3. 데이터링크층에 전달되면 발신지 주소는 송신자의 물리주소, 목적지 주소는 물리 브로드캐스트 주소로 하는 프레임에 캡슐화
4. 모든 호스트나 라우터가 프레임을 수신하여 자신의 ARP에 전달

ARP 동작

5. 타겟 시스템을 자신의 물리 주소를 포함한 ARP 응답 메시지 송신(유니케스트)

6. 송신자는 응답 메시지를 받고 타겟 시스템의 물리 주소를 알게 된다

7. IP 데이터그램은 프레임으로 캡슐화 되어 목적지에 유니캐스트

ARP가 사용되는 case

1. 송신자가 호스트로서 같은 네트워크상에 다른 호스트에 패킷 전송(논리주소는 목적지 IP주소)

2. 송신자가 호스트이고 다른 네트워크상에 있는 다른 호스트에게 패킷 전송(논리 주소는 라우터의 IP 주소)

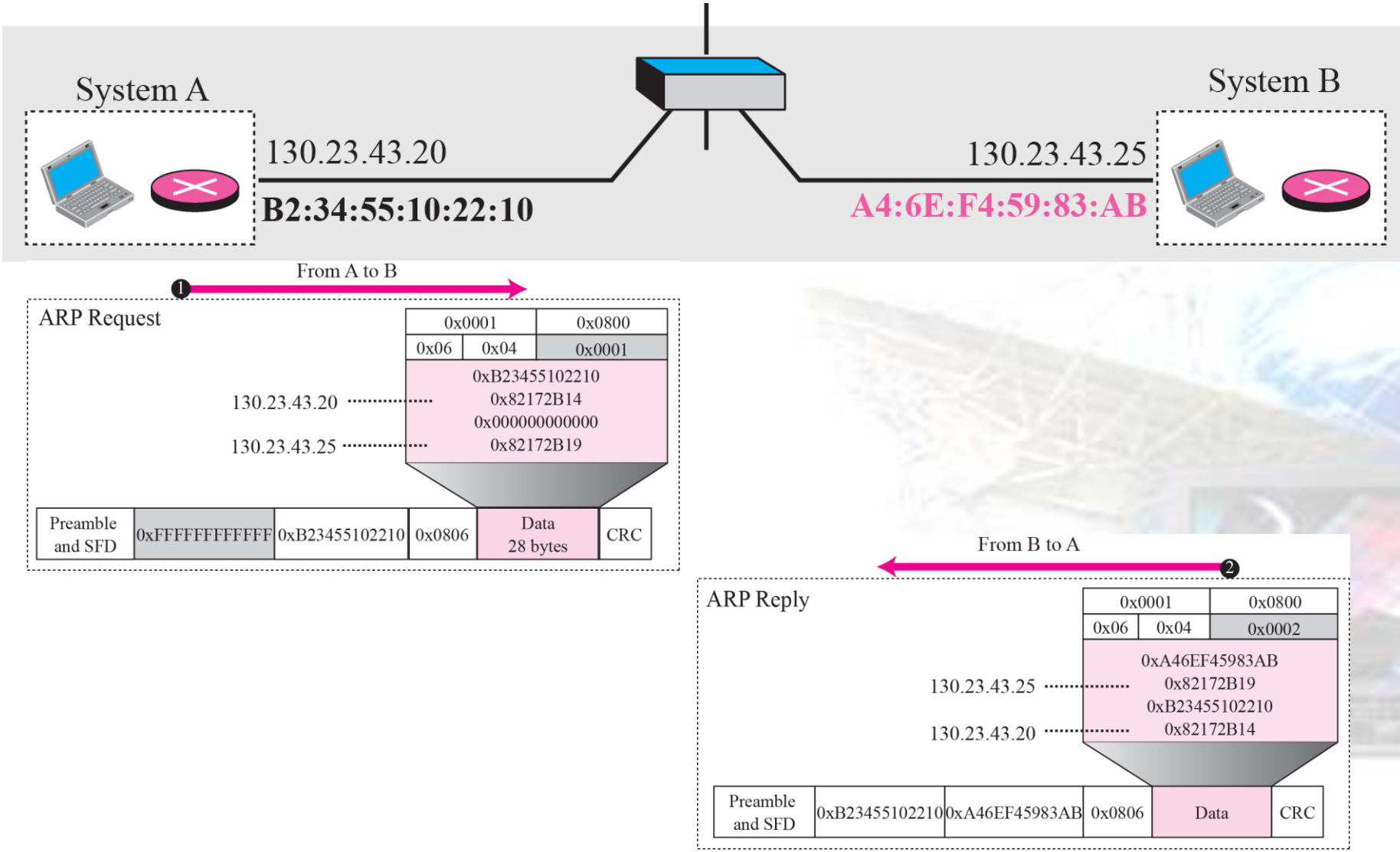
예제 8.1

IP 주소가 130.23.43.20이고 물리주소가 B2:34:55:10:22:10인 호스트가 IP 주소가 130.23.43.25이고 물리 주소가 A4:6E:F4:59:83:AB인 호스트에게 보낼 패킷을 가지고 있다. 두 호스트는 같은 이더넷 네트워크에 있다. 이더넷 프레임에 캡슐화된 ARP 요청(request)과 응답(reply) 패킷을 보여라.

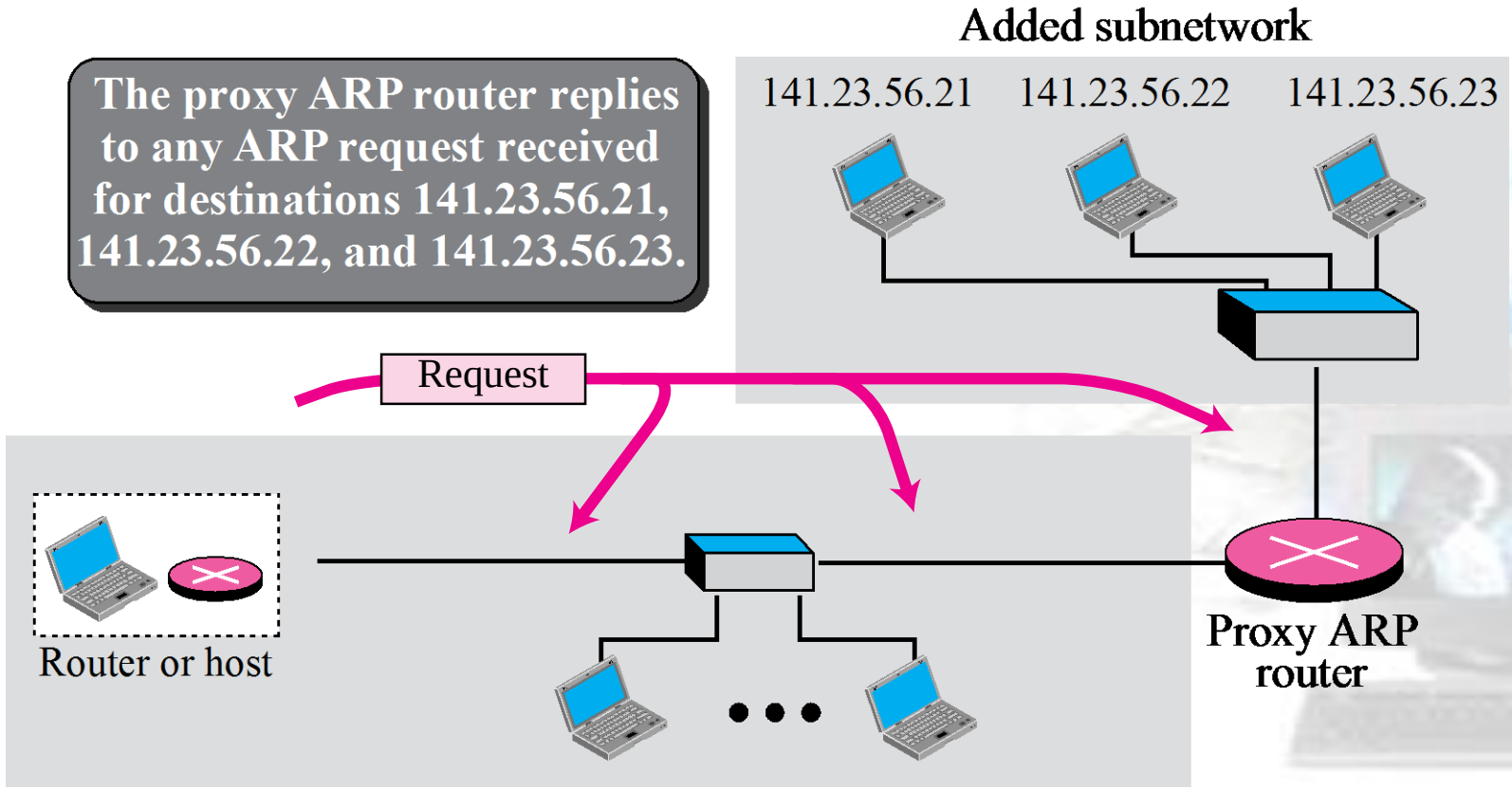
Solution

다음 쪽 그림은 ARP 요청과 응답 패킷을 보여준다. 이 경우 ARP 데이터 필드는 28 바이트이고 각 주소는 4 바이트 경계에 맞지 않는다. 이것이 주소를 위한 4 바이트 경계에 맞지 않는 이유이다. IP 주소는 16 진수로 나타나 있다.

Example 8.1


System A
System B
130.23.43.20
B2:34:55:10:22:10
130.23.43.25
A4:6E:F4:59:83:AB
From A to B
1
ARP Request
0x0001
0x0800
0x06
0x04
0x0001
0xB23455102210
0x82172B14
0x000000000000
0x82172B19
130.23.43.20
130.23.43.25
Preamble and SFD
0xFFFFFFFFFFFF
0xB23455102210
0x0806
Data 28 bytes
CRC
From B to A
2
ARP Reply
0x0001
0x0800
0x06
0x04
0x0002
0xA46EF45983AB
0x82172B19
0xB23455102210
0x82172B14
130.23.43.25
130.23.43.20
Preamble and SFD
0xB23455102210
0xA46EF45983AB
0x0806
Data
CRC

Proxy ARP: 라우터를 지난 다른 네트워크와 통신시



ARP 테이블 확인법: ARP 캐쉬가 있음

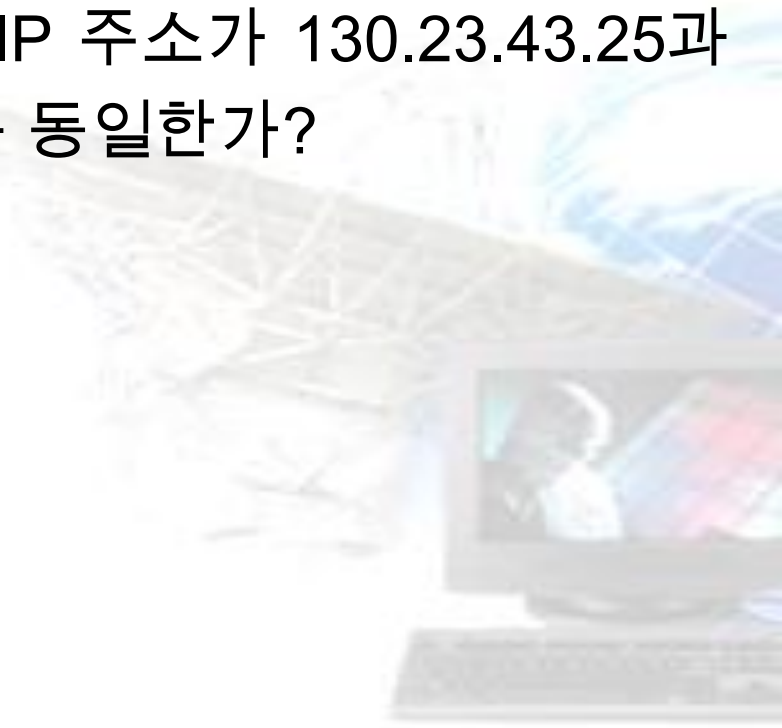
```
C:₩Documents and Settings₩user>arp -a

Interface: 220.68.139.28 --- 0x3
  Internet Address      Physical Address      Type
  220.68.139.12         a4-ba-db-fc-2a-a5     dynamic
  220.68.139.126        30-e4-db-9b-bb-c1     dynamic

C:₩Documents and Settings₩user>arp -d
```

```
C:₩Documents and Settings₩user>arp -a
No ARP Entries Found
```

예제 8.2

IP 주소가 220.68.139.28이고 물리주소가 00:13:77:C8:E5:0D인 호스트가 다른 네트웨크에 접속된 IP 주소가 130.23.43.25(예: www.daum.net)과 IP 주소가 180.23.43.24(예: www.naver.com)로 패킷 송신시 와이어샥에서 캡쳐된 IP 주소가 130.23.43.25과 IP 주소가 130.23.43.24의 MAC 주소는 동일한가?

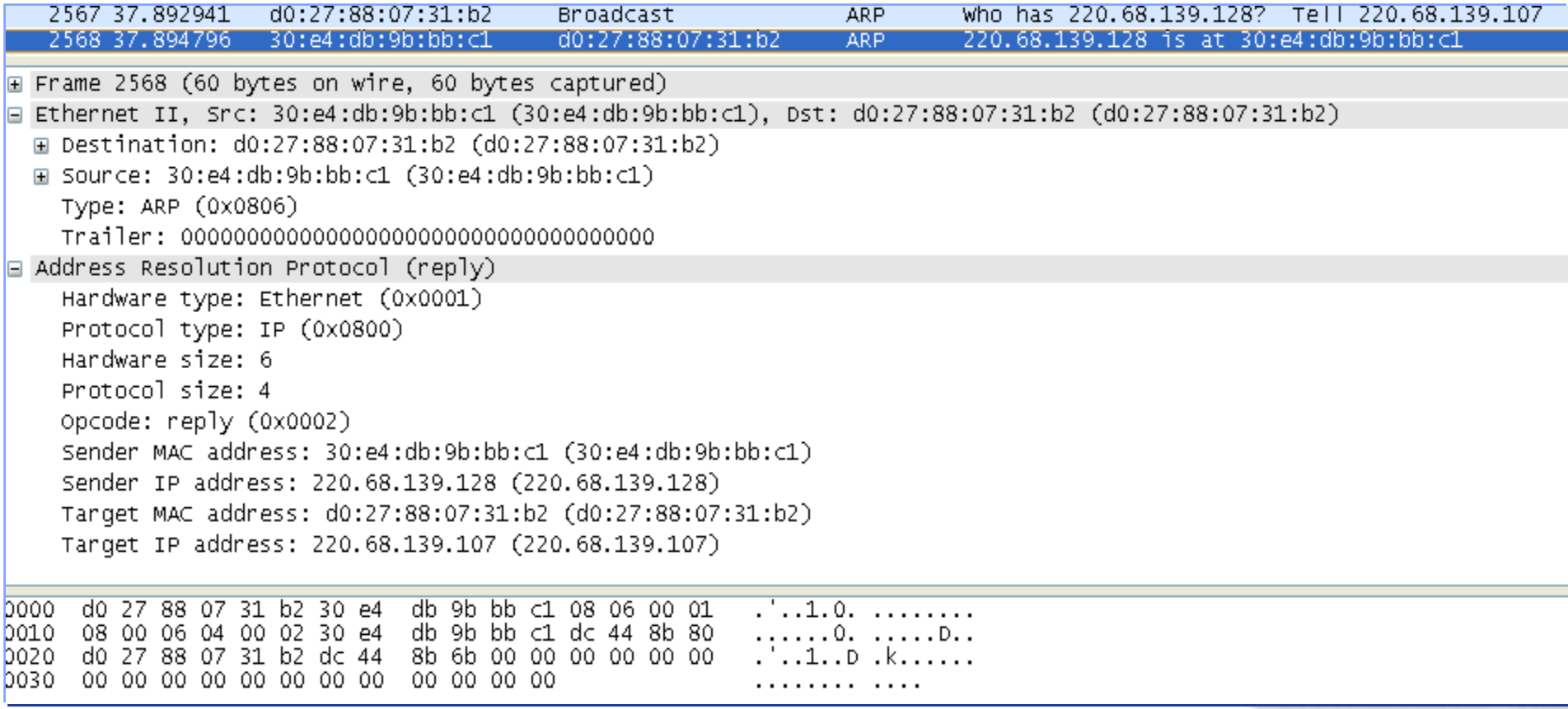
Solution 동일



예제 8.3 아래 그림의 응답 패킷을 서술하라

```
  2567 37.892941   d0:27:88:07:31:b2   Broadcast           ARP     Who has 220.68.139.128?  Tell 220.68.139.107
  2568 37.894796   30:e4:db:9b:bb:c1   d0:27:88:07:31:b2   ARP     220.68.139.128 is at 30:e4:db:9b:bb:c1

⊞ Frame 2567 (60 bytes on wire, 60 bytes captured)
⊟ Ethernet II, Src: d0:27:88:07:31:b2 (d0:27:88:07:31:b2), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ⊞ Source: d0:27:88:07:31:b2 (d0:27:88:07:31:b2)
    Type: ARP (0x0806)
    Trailer: 00000000000000000000000000000000000000
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: d0:27:88:07:31:b2 (d0:27:88:07:31:b2)
    Sender IP address: 220.68.139.107 (220.68.139.107)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 220.68.139.128 (220.68.139.128)

0000  ff ff ff ff ff ff d0 27  88 07 31 b2 08 06 00 01   .......' ..1.....
0010  08 00 06 04 00 01 d0 27  88 07 31 b2 dc 44 8b 6b   .......' ..1..D.k
0020  00 00 00 00 00 00 dc 44  8b 80 00 00 00 00 00 00   .......D ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

Solution


2567 37.892941 d0:27:88:07:31:b2 Broadcast ARP Who has 220.68.139.128? Tell 220.68.139.107
2568 37.894796 30:e4:db:9b:bb:c1 d0:27:88:07:31:b2 ARP 220.68.139.128 is at 30:e4:db:9b:bb:c1
Frame 2568 (60 bytes on wire, 60 bytes captured)
Ethernet II, Src: 30:e4:db:9b:bb:c1 (30:e4:db:9b:bb:c1), Dst: d0:27:88:07:31:b2 (d0:27:88:07:31:b2)
Destination: d0:27:88:07:31:b2 (d0:27:88:07:31:b2)
Source: 30:e4:db:9b:bb:c1 (30:e4:db:9b:bb:c1)
Type: ARP (0x0806)
Trailer: 00000000000000000000000000000000000000
Address Resolution Protocol (reply)
Hardware type: Ethernet (0x0001)
Protocol type: IP (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: reply (0x0002)
Sender MAC address: 30:e4:db:9b:bb:c1 (30:e4:db:9b:bb:c1)
Sender IP address: 220.68.139.128 (220.68.139.128)
Target MAC address: d0:27:88:07:31:b2 (d0:27:88:07:31:b2)
Target IP address: 220.68.139.107 (220.68.139.107)
0000 d0 27 88 07 31 b2 30 e4 db 9b bb c1 08 06 00 01 .'..1.0. ....
0010 08 00 06 04 00 02 30 e4 db 9b bb c1 dc 44 8b 80 ......0. .....D..
0020 d0 27 88 07 31 b2 dc 44 8b 6b 00 00 00 00 00 00 .'..1..D .k......
0030 00 00 00 00 00 00 00 00 00 00 00 00 ....

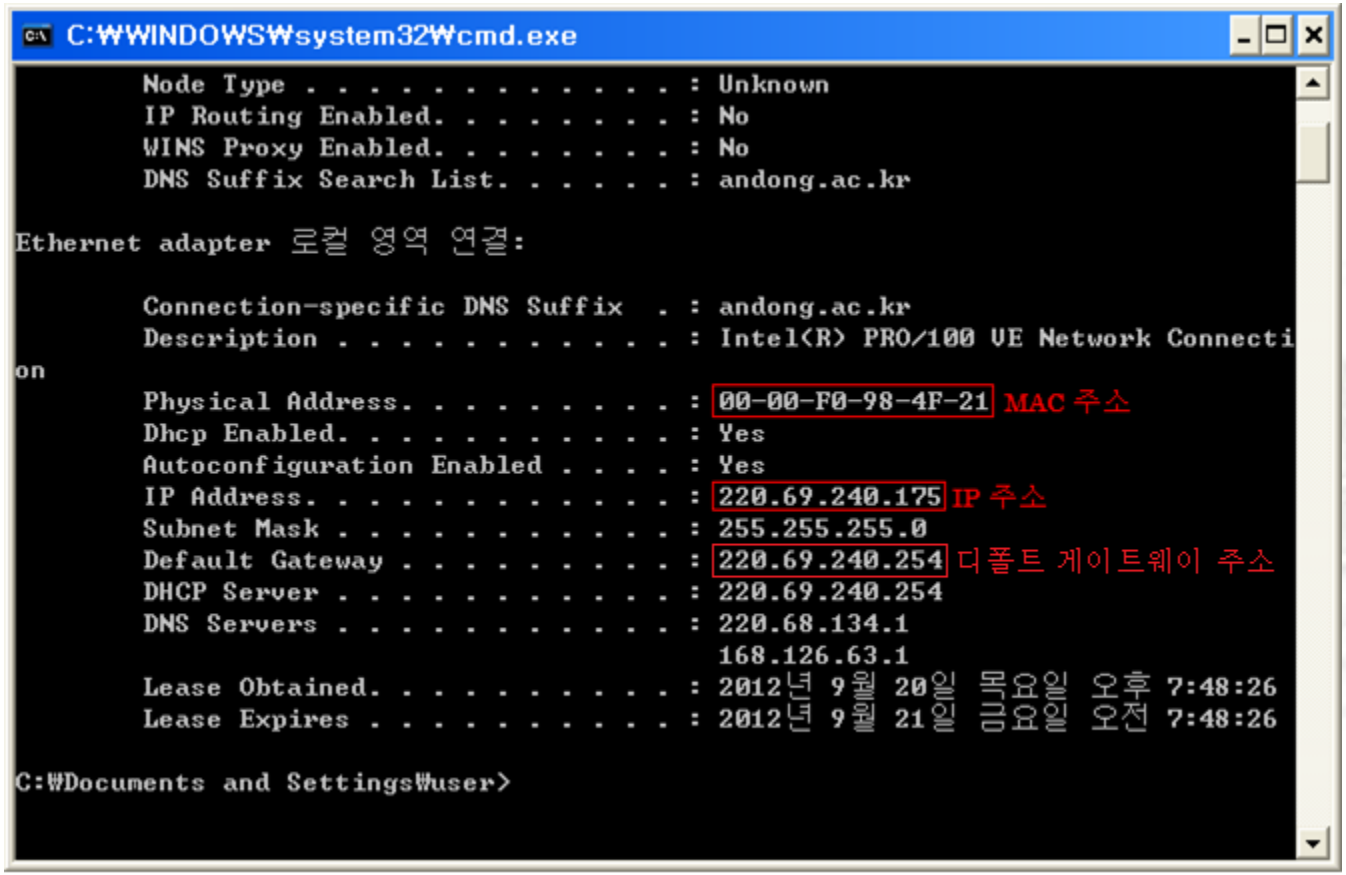
종합문제: 이 문제는 반드시 풀고 갈것

1. IP 주소가 220.69.240.175이고 물리주소가 00:00:00:F0:98:21인 호스트가 다른 네트웨크에 접속된 IP 주소가 202.131.30.11(예: www.naver.com)과 IP 주소가 61.111.62.35(예: www.daum.net) 의 MAC 주소를 구하는 ARP 요구와 응답패킷을 분석하라. ➔동일한가? 동일하면 그 이유는?

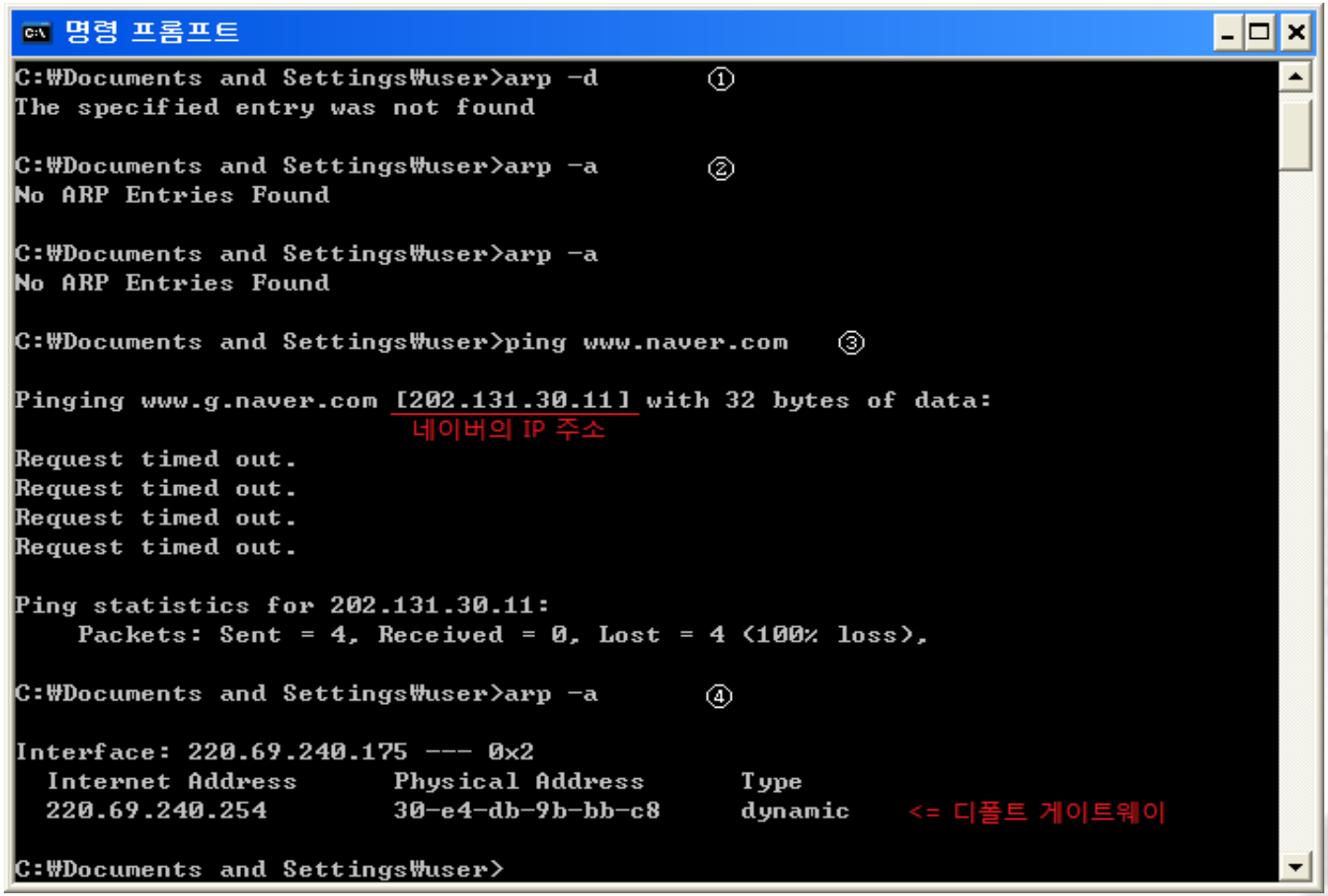
2. IP 주소가 220.69.240.175이고 물리주소가 00:00:00:F0:98:21인 호스트가 다른 네트웨크에 접속된 IP 주소가 202.131.30.11(예: www.naver.com)과 IP 주소가 61.111.62.35(예: www.daum.net) 에 IP 패킷 송신시 IP 패킷을 분석하라.
➔MAC 주소는 동일하고 IP 헤더의 IP주소는 왜 다른가?

정답: 1 문제

220.69.240.175 호스트 IP 주소와 MAC 주소, 디폴트 게이트웨이의 IP 주소



다른 네트워크의 MAC 주소 찾기 – NAVER



① 먼저 명령 프롬프트로 arp를 지운다. (명령어 : arp -d)

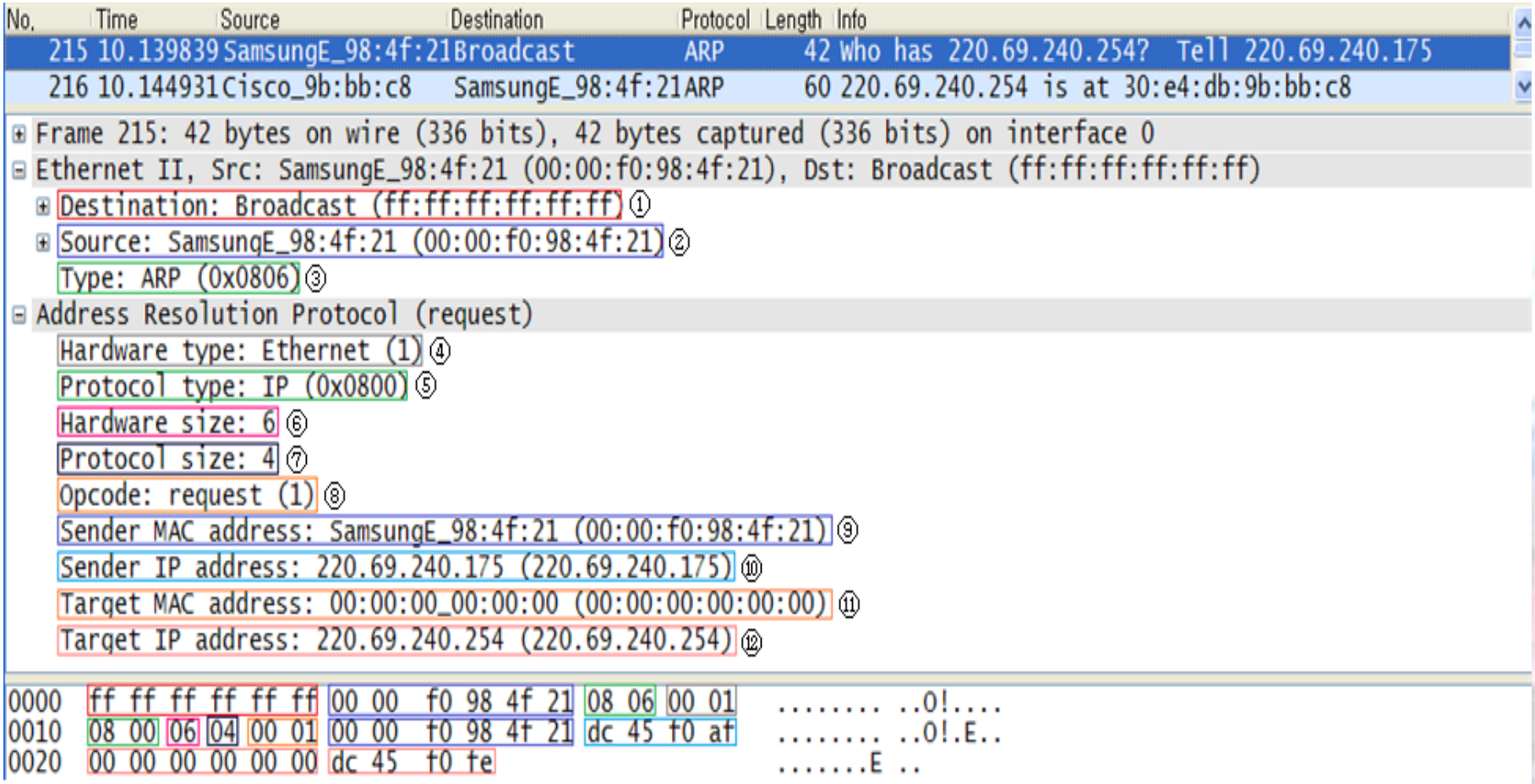
② ARP가 지워졌는지 확인한다. (명령어 : arp -a)

③ Wireshark를 구동한 후, NAVER에 접속한다.
(명령어 : ping www.naver.com / 또는 NAVER 홈페이지 띄우기)

④ Wireshark을 멈추고 명령 프롬프트에서 ARP를 다시 확인해본다.
(명령어 : arp -a)IP 주소가 누구의 IP주소인지 알아본다.
(NAVER인지 디폴트 게이트웨이인지)
∴ 디폴트 게이트웨이 (naver는 다른 네트워크 상에 있기 때문)

이로서 사실상 naver의 MAC 주소를 알기 위해 시도했지만 다른 네트워크 상에 있으므로 디폴트 게이트웨이의 MAC 주소를 먼저 알아야 한다는 것을 알게 되었다.
이제 Wireshark으로 디폴트 게이트웨이의 MAC 주소를 알아내는 ARP 패킷을 찾으면 된다.
아래와 같다.

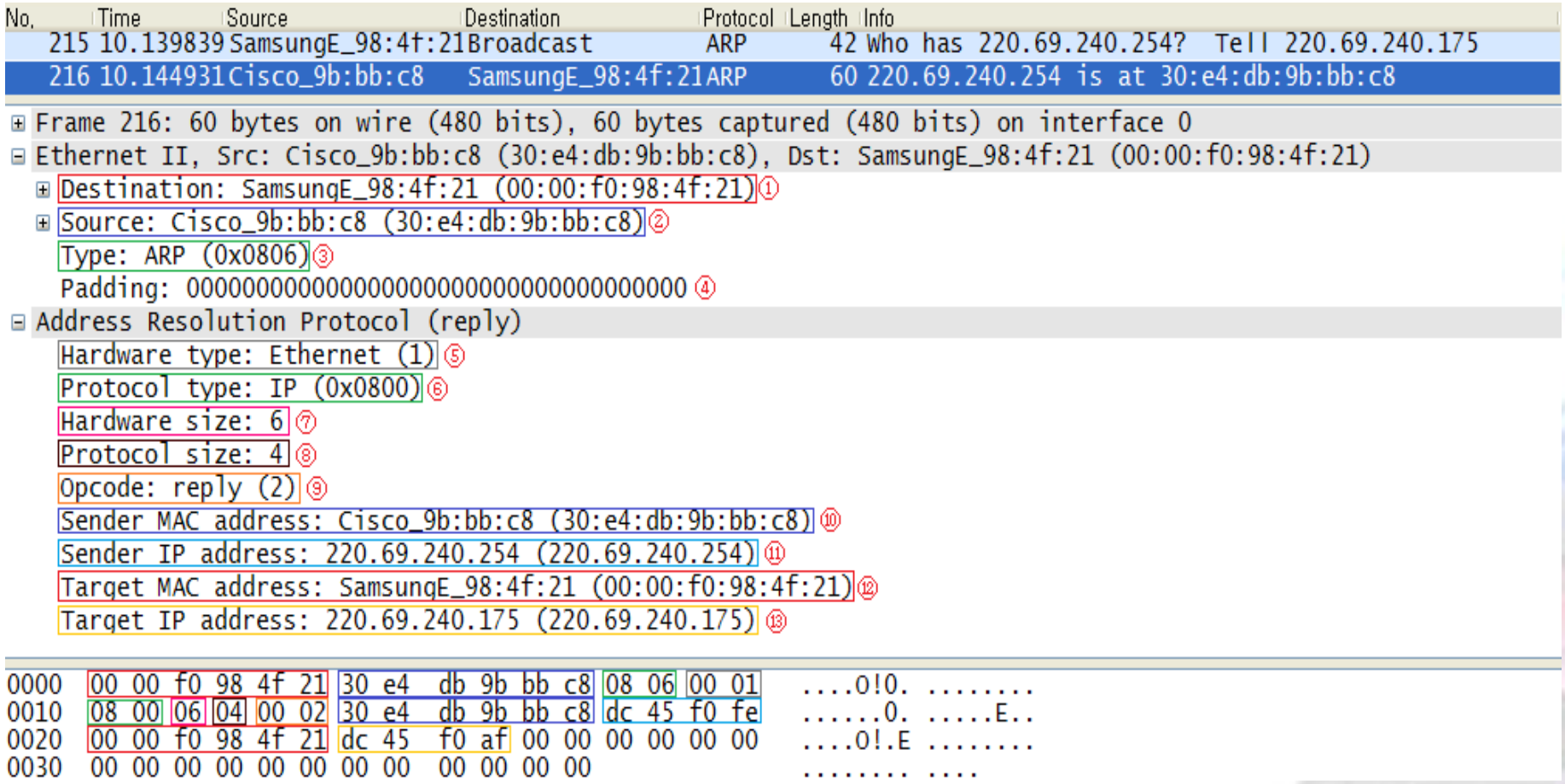
1) NAVER에 접속했을 때 ARP 요청 패킷



① Destination(목적지 MAC 주소, 6 bytes) : 목적지의 MAC 주소를 모르기 때문에 모든 사람에게 프레임을 보낸다. 그 방법이 브로드캐스트다.
② Source(발신지 MAC 주소, 6 bytes) : 내가 발신자이므로 나의 MAC 주소인 00:00:f0:98:4f:21이 이 자리에 위치한다.
③ Type(타입, 2 bytes) : 목적지 IP 주소로 목적지 MAC 주소를 구해야하므로 주소변환프로토콜 즉, ARP 타입이다.
④ Hardware type(MAC 주소의 타입?, 2 bytes) : 현재 MAC 주소는 이더넷 프레임 위에 있으며 이더넷을 나타내는 수는 1이다.
⑤ Protocol type(프로토콜 타입, 2 bytes) : 이더넷 프레임 위에서 타입이 무엇이었는지 담는 공간이다. IP였으므로 08 00이 들어간다.
⑥ Hardware size(MAC 주소의 크기, 1 byte) : MAC 주소 크기에 관한 정보다. MAC 주소는 6 bytes로 구성되어 있다.
⑦ Protocol size(IP 주소의 크기, 1 byte) : IP 주소 크기에 관한 정보다. IP 주소는 4 bytes로 구성되어 있다.
⑧ Opcode(ARP 유형?, 2 bytes) : 내가 목적지 MAC 주소를 알기 위해 가르쳐달라고 요청하는 과정이다. 요청을 1로 표현한다.
⑨ Sender MAC address(발신지 MAC 주소, 6 bytes) : 나의 MAC 주소가 들어갈 자리. 00:00:f0:98:4f:21이므로 6 bytes를 차지한다.
⑩ Sender IP address(발신지 IP 주소, 4 bytes) : 나의 IP 주소가 들어갈 자리. 220.69.240.175이므로 4 bytes를 차지한다.
⑪ Target MAC address(타겟 MAC 주소, 6 bytes) : 목적지 MAC 주소가 들어갈 자리. 모르므로 전부 0이 들어간다. (00:00:00:00:00:00)
⑫ Target IP address(타겟 IP 주소, 4 bytes) : 현재 디폴트 게이트웨이가 목적지이므로 디폴트 게이트웨이의 IP 주소 220.69.240.254가 들어감)

명령 프롬프트에서 NAVER를 접속했을 때 NAVER MAC 주소가 아닌 디폴트 게이트웨이의 MAC 주소를 알아냈듯이 Wireshark에서도 NAVER가 아닌 디폴트 게이트웨이에게 MAC 주소를 알려달라고 요청을 하고 있다.

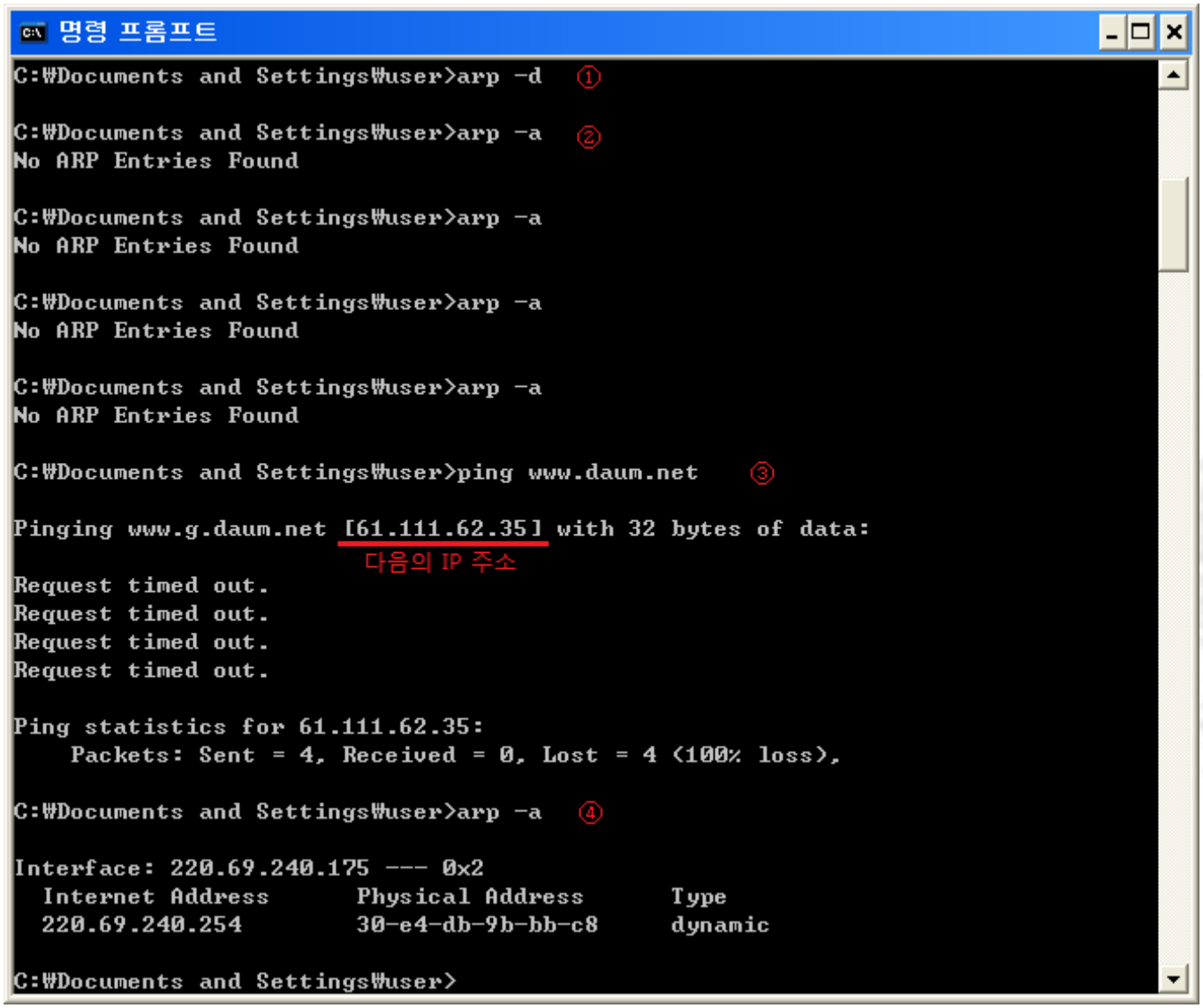
2) NAVER에 접속했을 때 ARP 응답 패킷



```
No.     Time        Source                Destination           Protocol Length Info
    215 10.139839   SamsungE_98:4f:21     Broadcast             ARP      42 Who has 220.69.240.254?  Tell 220.69.240.175
    216 10.144931   Cisco_9b:bb:c8        SamsungE_98:4f:21     ARP      60 220.69.240.254 is at 30:e4:db:9b:bb:c8

⊞ Frame 216: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
⊟ Ethernet II, Src: Cisco_9b:bb:c8 (30:e4:db:9b:bb:c8), Dst: SamsungE_98:4f:21 (00:00:f0:98:4f:21)
  ⊞ Destination: SamsungE_98:4f:21 (00:00:f0:98:4f:21) ①
  ⊞ Source: Cisco_9b:bb:c8 (30:e4:db:9b:bb:c8) ②
    Type: ARP (0x0806) ③
    Padding: 000000000000000000000000000000000000 ④
⊟ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1) ⑤
    Protocol type: IP (0x0800) ⑥
    Hardware size: 6 ⑦
    Protocol size: 4 ⑧
    Opcode: reply (2) ⑨
    Sender MAC address: Cisco_9b:bb:c8 (30:e4:db:9b:bb:c8) ⑩
    Sender IP address: 220.69.240.254 (220.69.240.254) ⑪
    Target MAC address: SamsungE_98:4f:21 (00:00:f0:98:4f:21) ⑫
    Target IP address: 220.69.240.175 (220.69.240.175) ⑬

0000  00 00 f0 98 4f 21 30 e4  db 9b bb c8 08 06 00 01   ....O!0. ........
0010  08 00 06 04 00 02 30 e4  db 9b bb c8 dc 45 f0 fe   ......0. .....E..
0020  00 00 f0 98 4f 21 dc 45  f0 af 00 00 00 00 00 00   ....O!.E ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

① Destination(목적지 MAC 주소, 6 bytes) : 응답과정 이므로 발신지는 게이트웨이 목적지는 내가 된다. 따라서 나의 MAC 주소가 온다.
② Source(발신지 MAC 주소, 6 bytes) : 게이트웨이의 MAC 주소가 온다.
③ Type(타입, 2 bytes) : MAC 주소를 알기 위한 패킷 유형은 ARP이다.
④ Padding : 이더넷의 최소길이 유지 (데이터 46-1500 바이트)
⑤ Hardware type(MAC 주소의 타입?, 2 bytes) : 현재 MAC 주소는 이더넷 프레임 위에 있으며 이더넷을 나타내는 수는 1이다.
⑥ Protocol type(프로토콜 타입, 2 bytes) : 이더넷 프레임 위에서 타입이 무엇이었는지 담는 공간이다. IP였으므로 08 00이 들어간다.
⑦ Hardware size(MAC 주소의 크기, 1 byte) : MAC 주소 크기에 관한 정보다. MAC 주소는 6 bytes로 구성되어 있다.
⑧ Protocol size(IP 주소의 크기, 1 byte) : IP 주소 크기에 관한 정보다. IP 주소는 4 bytes로 구성되어 있다.
⑨ Opcode(ARP 유형?, 2 bytes) : 게이트웨이가 자신의 MAC 주소를 나(목적지)에게 알려주는 과정 즉, 응답패킷을 2로 표현한다.
⑩ Sender MAC address(발신지 MAC 주소, 6 bytes) : 게이트웨이의 MAC 주소가 들어갈 자리. 30-e4-db-9b-bb-c8이므로 6 bytes를 차지한다.
⑪ Sender IP address(발신지 IP 주소, 4 bytes) : 게이트웨이의 IP 주소가 들어갈 자리. 220.69.240.254이므로 4 bytes를 차지한다.
⑫ Target MAC address(타겟 MAC 주소, 6 bytes) : 나의 MAC 주소가 들어갈 자리. 00-00-f0-98-4f-21이고 6 bytes를 차지한다.
⑬ Target IP address(타겟 IP 주소, 4 bytes) : 나의 IP 주소가 들어갈 자리. 220.69.240.175이고 4 bytes를 차지한다.
이로써 NAVER는 내 컴퓨터와 다른 네트워크에 있으므로 NAVER의 MAC 주소를 바로 알 수 있는 것이 아니라 디폴트 게이트웨이의 MAC 주소가 온다는 것을 알게 되었다.

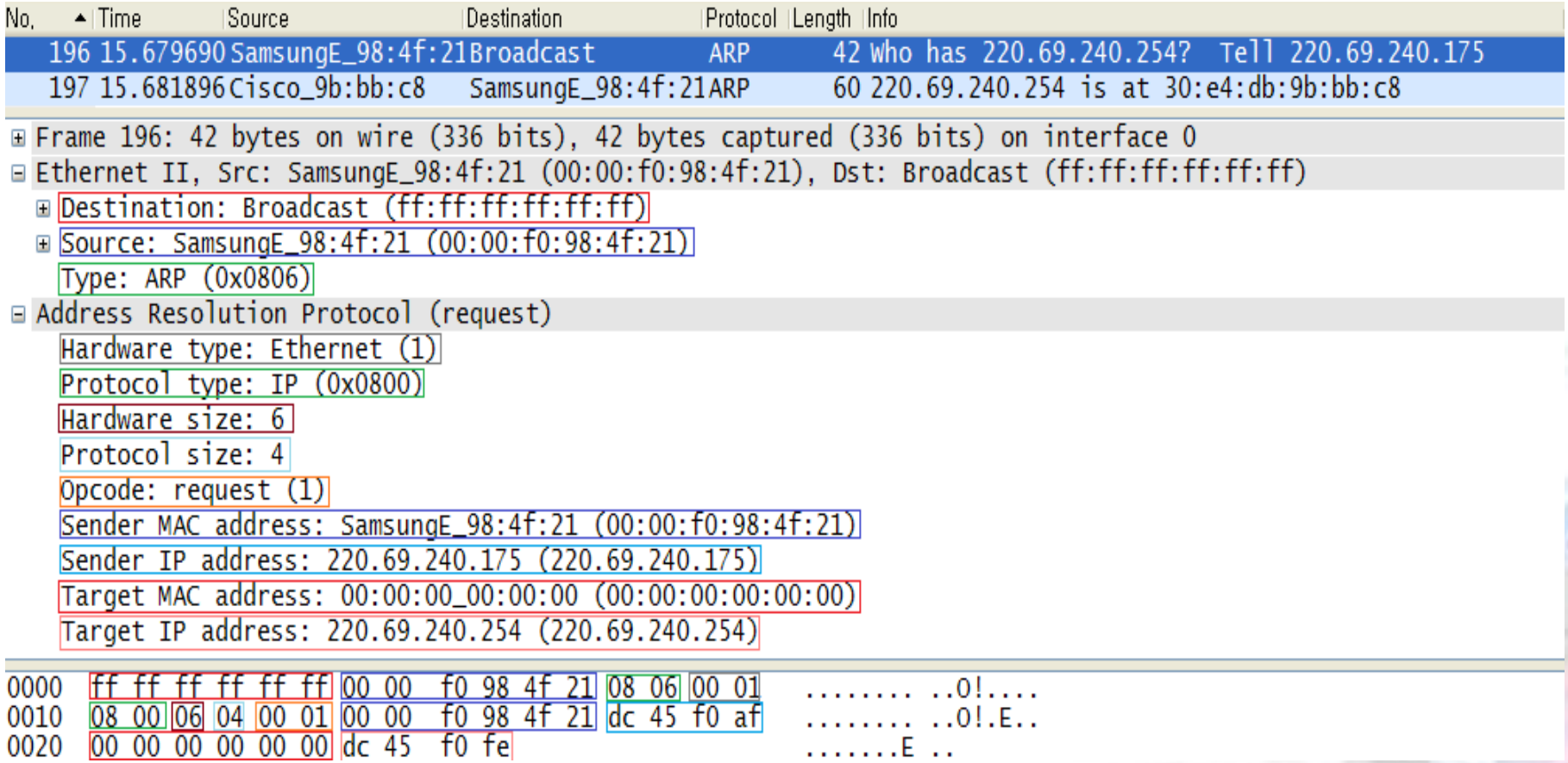
다른 네트워크의 MAC 주소 찾기 – DAUM



① 먼저 명령 프롬프트로 arp를 지운다. (명령어 : arp –d)
② ARP가 지워졌는지 확인한다. (명령어 : arp –a)
③ Wireshark를 구동한 후, DAUM에 접속한다.
(명령어 : ping www.daum.net / 또는 DAUM 홈페이지 띄우기)
④ Wireshark을 멈추고 명령 프롬프트에서 ARP를 다시 확인해본다.
(명령어 : arp –a)IP 주소가 누구의 IP주소인지 알아본다.
(DAUM인지 디폴트 게이트웨이인지)
∴ 디폴트 게이트웨이 (DAUM는 다른 네트워크 상에 있기 때문)

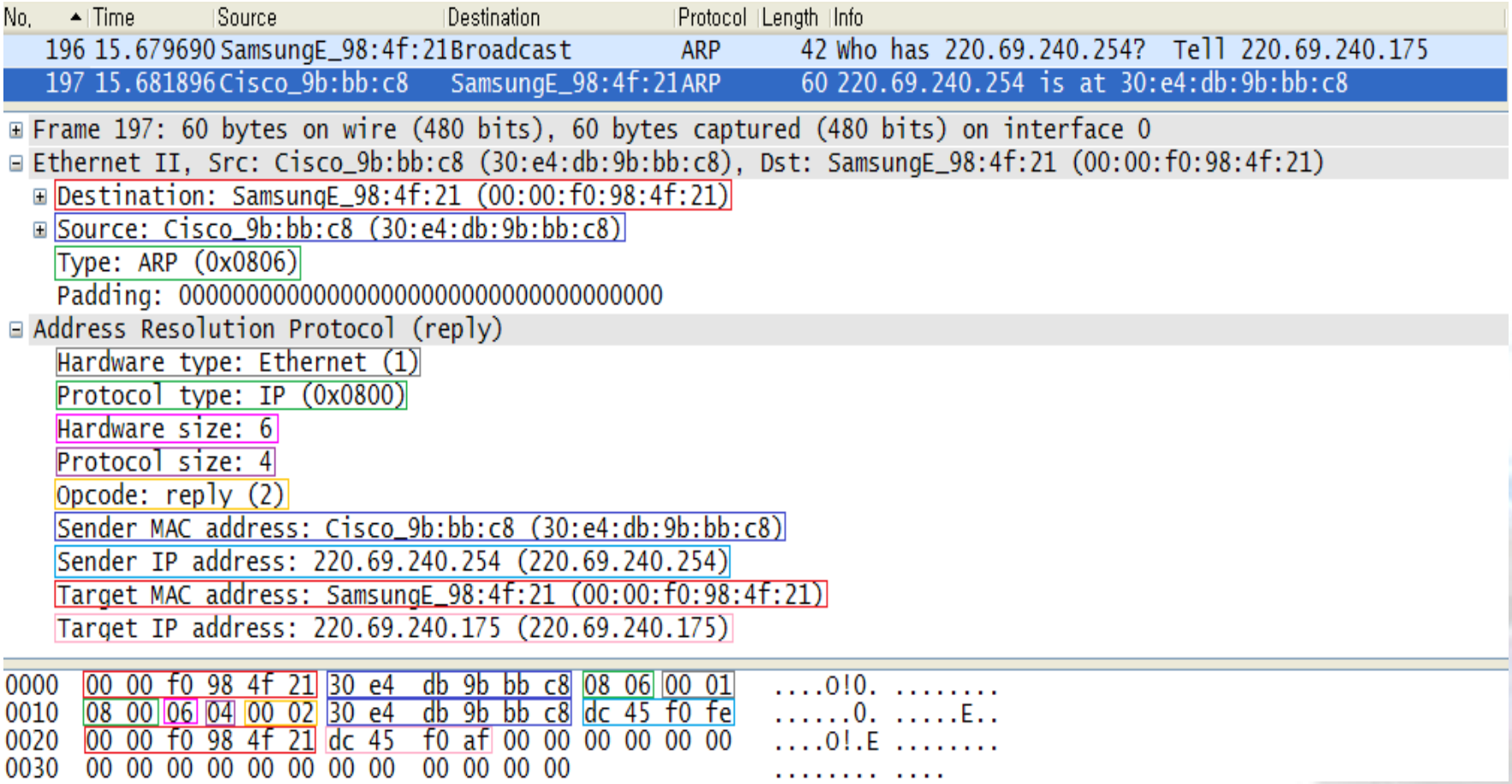
DAUM도 NAVER와 마찬가지로 게이트웨이의 정보가 나왔다. Wireshark에서 ARP 패킷을 살펴보자.

1) DAUM에 접속했을 때 ARP 요청 패킷: NAVER접속과 동일



명령 프롬프트에서 DAUM를 접속했을 때 DAUM MAC 주소가 아닌 디폴트 게이트웨이의 MAC 주소를 알아냈듯이 Wireshark에서도 DAUM이 아닌 디폴트 게이트웨이에게 MAC 주소를 알려달라고 요청을 하고 있다. NAVER 접속했을 때와 동일한 패킷이다.

2) DAUM에 접속했을 때 ARP 응답 패킷



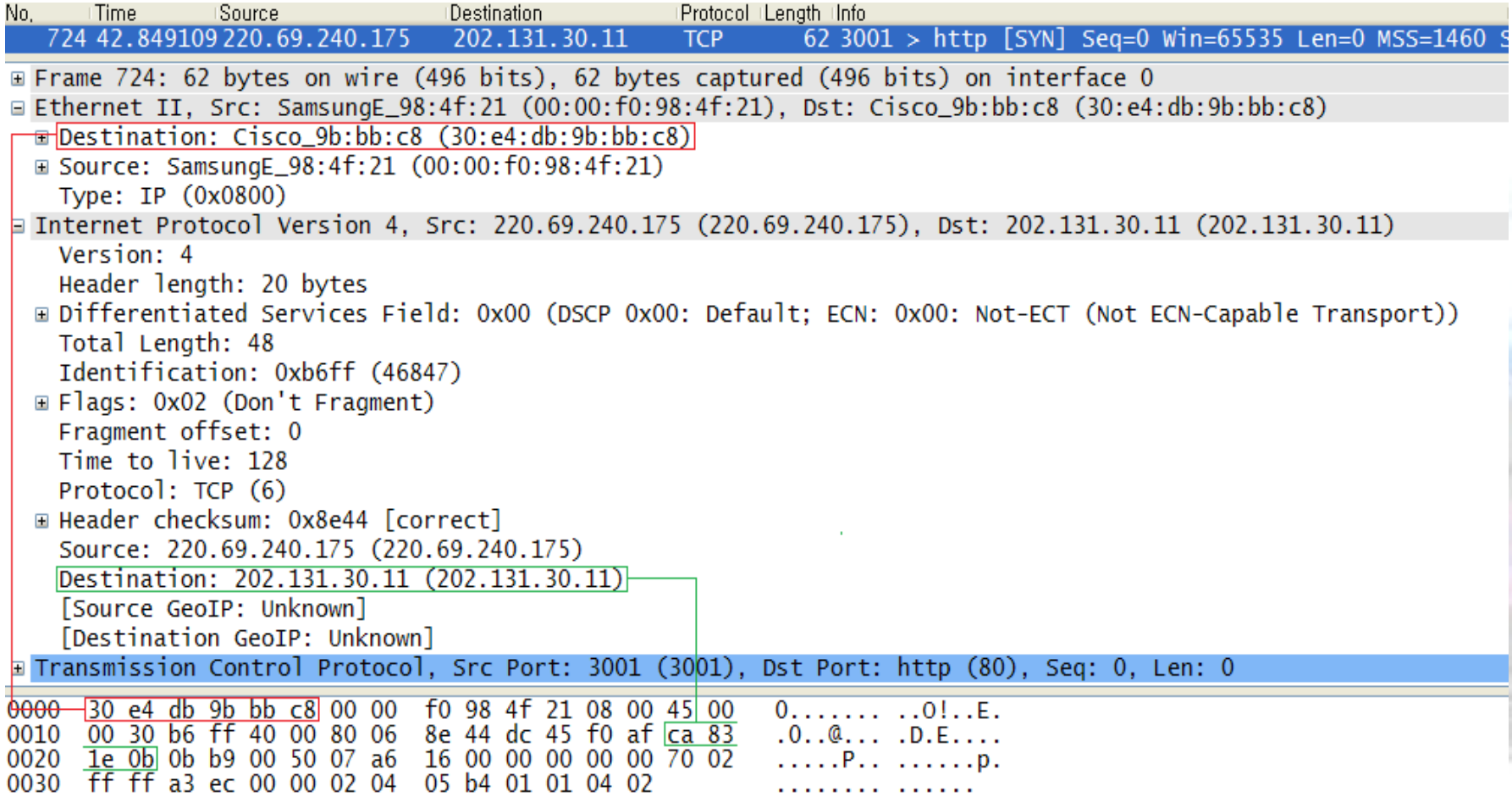
```
No.   Time        Source              Destination         Protocol Length Info
  196 15.679690   SamsungE_98:4f:21   Broadcast           ARP      42 Who has 220.69.240.254?  Tell 220.69.240.175
  197 15.681896   Cisco_9b:bb:c8      SamsungE_98:4f:21   ARP      60 220.69.240.254 is at 30:e4:db:9b:bb:c8

⊞ Frame 197: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
⊟ Ethernet II, Src: Cisco_9b:bb:c8 (30:e4:db:9b:bb:c8), Dst: SamsungE_98:4f:21 (00:00:f0:98:4f:21)
  ⊞ Destination: SamsungE_98:4f:21 (00:00:f0:98:4f:21)
  ⊞ Source: Cisco_9b:bb:c8 (30:e4:db:9b:bb:c8)
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000000000
⊟ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: Cisco_9b:bb:c8 (30:e4:db:9b:bb:c8)
    Sender IP address: 220.69.240.254 (220.69.240.254)
    Target MAC address: SamsungE_98:4f:21 (00:00:f0:98:4f:21)
    Target IP address: 220.69.240.175 (220.69.240.175)

0000  00 00 f0 98 4f 21 30 e4  db 9b bb c8 08 06 00 01   ....O!0. ........
0010  08 00 06 04 00 02 30 e4  db 9b bb c8 dc 45 f0 fe   ......0. .....E..
0020  00 00 f0 98 4f 21 dc 45  f0 af 00 00 00 00 00 00   ....O!.E ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

응답 패킷도 역시 NAVER 접속 경우와 같다.

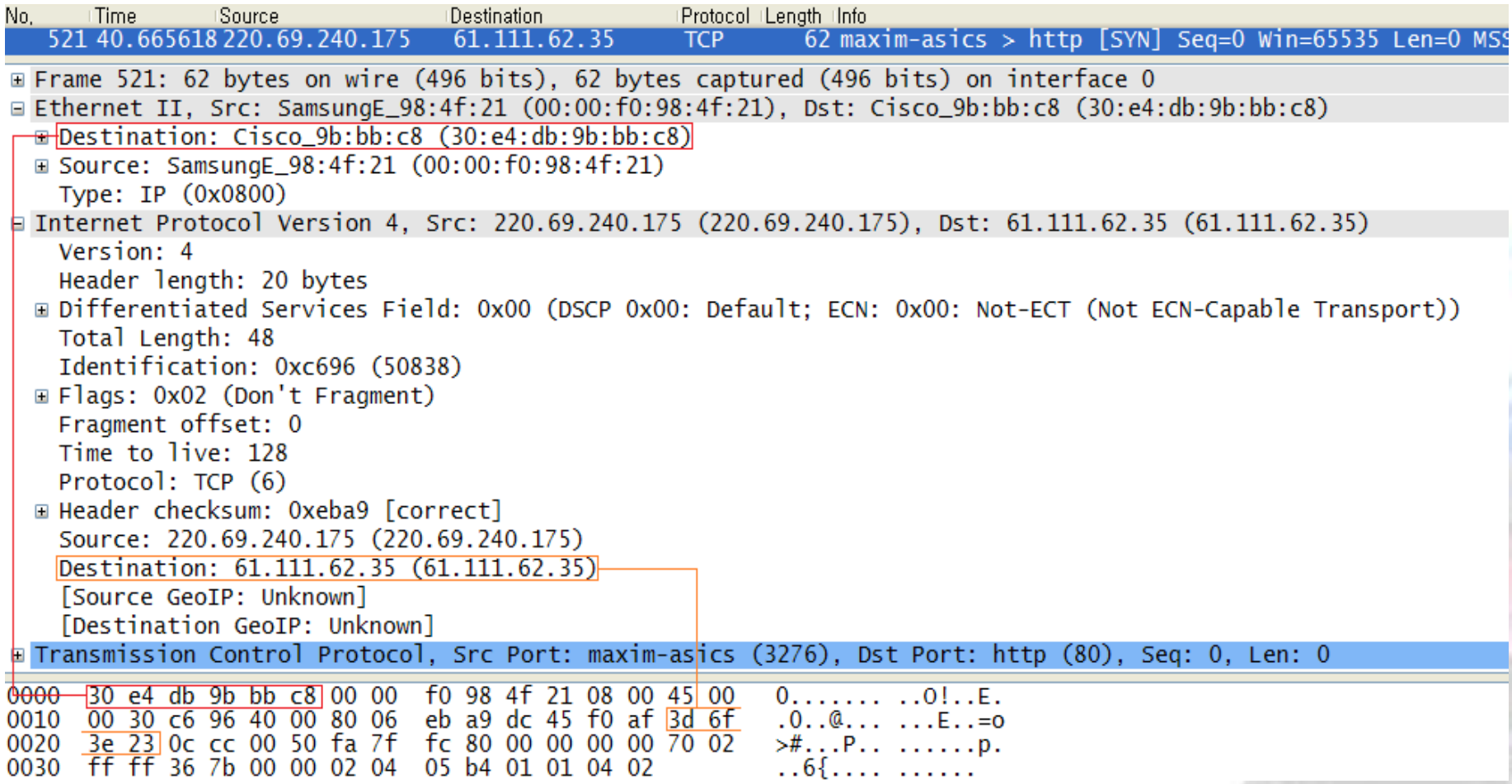
따라서 **다른 네트워크 접속 시(NAVER, DAUM 등) 항상 디폴트 게이트웨이의 MAC 주소를 알아야 한다는 것을 알 수 있다.**

정답: 2 문제

1) NAVER 접속한 경우 (발신지 : 내 컴퓨터, 목적지 : NAVER)



1) DAUM 접속한 경우 (발신지 : 내 컴퓨터, 목적지 : DAUM)



∴ NAVER와 DAUM을 비교한 결과 이더넷 헤더의 목적지 주소(MAC 주소) 30-e4-db-9b-bb-c8로 동일하고 IP 헤더의 목적지 주소(IP 주소)는 달랐다. 1번 ARP 분석 결과처럼 목적지 MAC 주소는 NAVER와 DAUM의 MAC주소가 아니라 디폴트 게이트웨이의 MAC 주소임을 알 수 있다. 즉, 다른 네트워크(NAVER, DAUM 등)에 접속하려면 항상 디폴트 게이트웨이를 지나야 접속할 수 있으므로 게이트웨이의 MAC 주소를 먼저 알아야 한다.