# Assignment #5

| |
|---|
| ✓ ARP 프로토콜에 대해 조사하고, ARP Request/Reply 패킷을 와이어샤크를 통해 분석하시오. |
| ✓ 과제 copy 등 부정행위 발견시 모두 0점처리합니다. (웹사이트 단순 copy 포함) |
| ✓ **4 page 이내로 제출하시오.** |

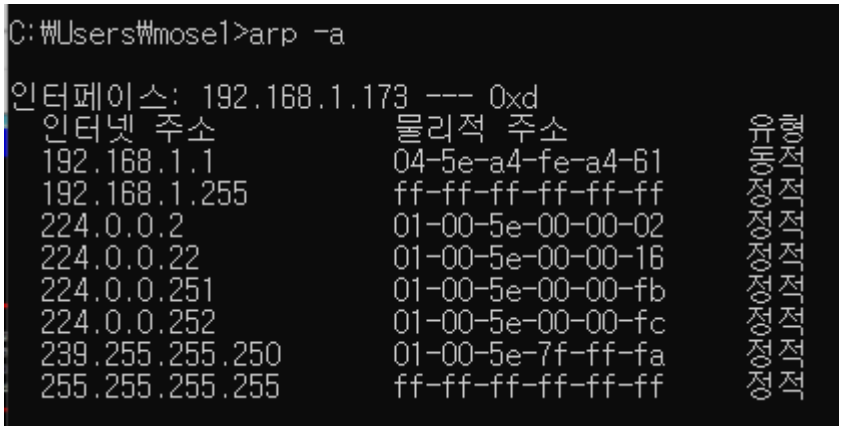
20201777 홍지훈

## 1. ARP 프로토콜이란?

ARP 프로토콜이란 Address Resolution Protocol의 약자로, 네트워크상의 IP주소를 물리적 네트워크 주소(MAC 주소)로 대응시키기 위해 사용되는 프로토콜이다. 반대로 물리적인 네트워크 주소에서 네트워크상의 IP 값을 알아내는 프로토콜에는 RARP(Reverse Address Resolution Protocol)이 있다.

IP주소와 MAC 주소를 1대1 매칭하여 테이블로 정리하는데 이것을 ARP Table이라고 한다.

윈도우에서는 CMD창에서 arp -a를 입력하면 arp table을 볼 수 있다.




### ARP 프로토콜 동작 순서 (같은 네트워크)

1. ARP Request
   송신 측에서 출발지 MAC, 출발지 IP, 목적지 IP 정보를 하나의 네트워크에 연결 되어있는 모든 기기로 ARP 요청을 Broadcast 시킨다.
2. 네트워크에 연결 되어있는 모든 PC는 이 프레임을 수신하고, 본인의 IP와 맞지 않는 PC는 수신 받은 프레임을 버리고, 맞는 PC는 응답을 보낸다.
3. ARP Reply
   IP가 맞는 PC는 송신자에게 본인의 MAC Address를 추가해서 응답한다. 응답을 보낼 땐 Broadcast가 아닌 Unicast를 사용한다.

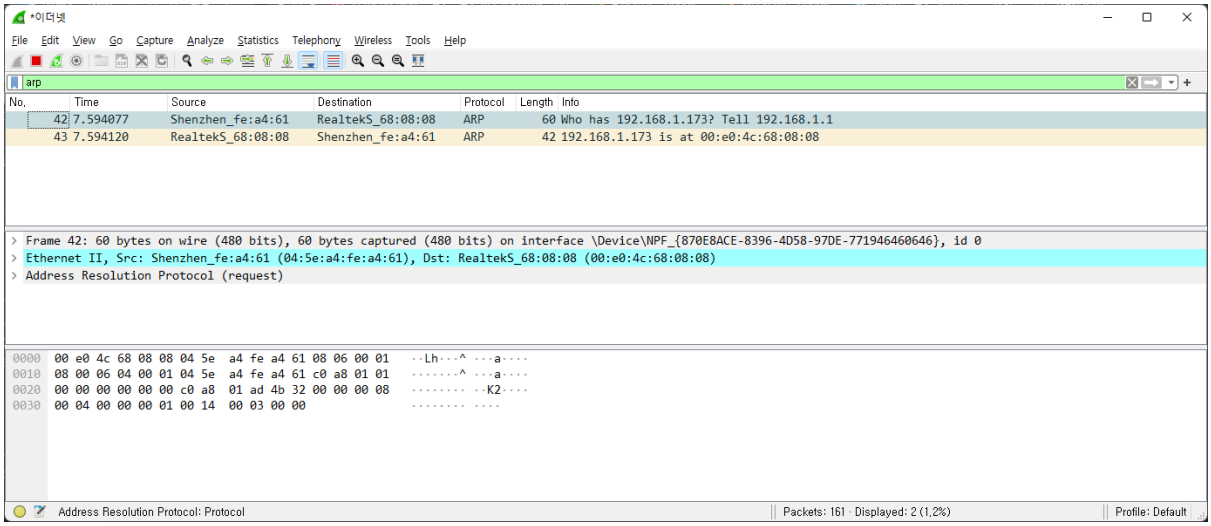
### ARP 프로토콜 동작 순서 (다른 네트워크)

1. 송신 측에서 출발지 MAC, 출발지 IP, 목적지 IP 정보를 하나의 네트워크에 연결 되어있는 모든 기기로 ARP 요청을 Broadcast 시킨다.
2. 라우터는 해당 ARP 요청을 받지만, 목적지의 IP주소가 같은 네트워크에 있지 않기

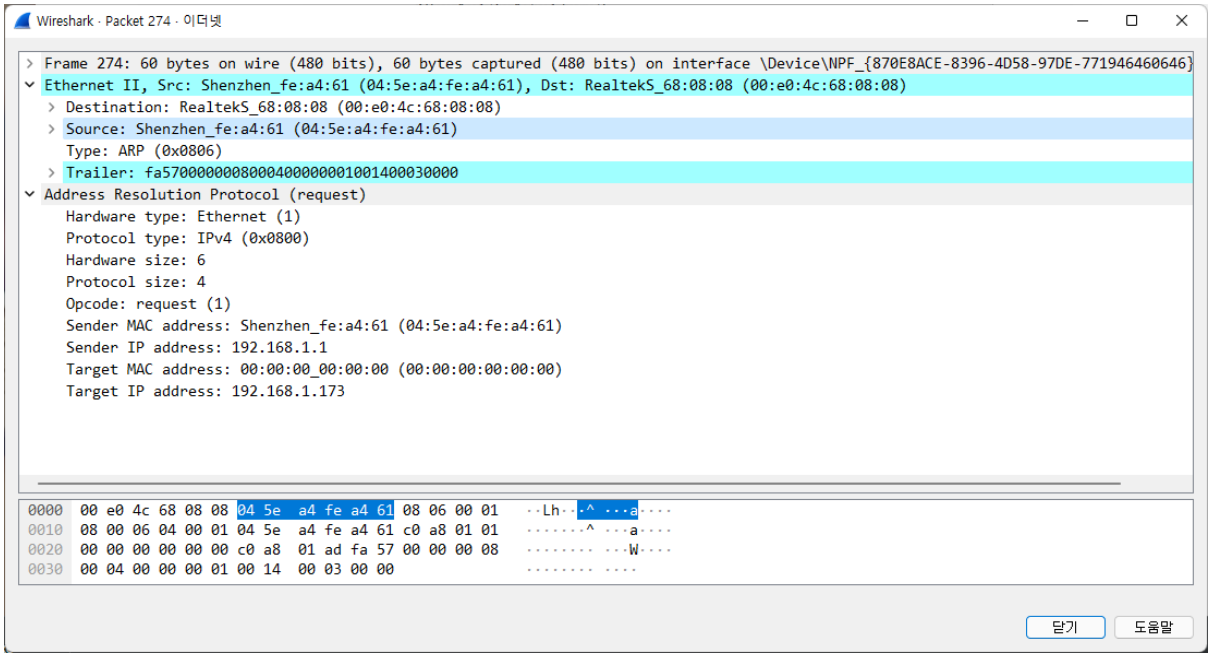
때문에 같은 네트워크에 있는 라우터의 MAC 주소로 응답한다.

3. 송신 측은 수신 측과 통신하기 위해 다시 같은 네트워크에 있는 라우터의 MAC 주소로 ARP 요청을 보낸다.
4. 라우터는 해당 네트워크에 대해서 Broadcast로 목적지 IP 정보를 가진 단말이 있는지 물어본다.
5. 받은 패킷의 목적지 IP가 맞는 기기가 있으면 라우터에 자신의 MAC주소를 포함한 상태로 보내서 응답한다.
6. 이후 수신 측과 송신 측은 서로 통신을 시작한다.

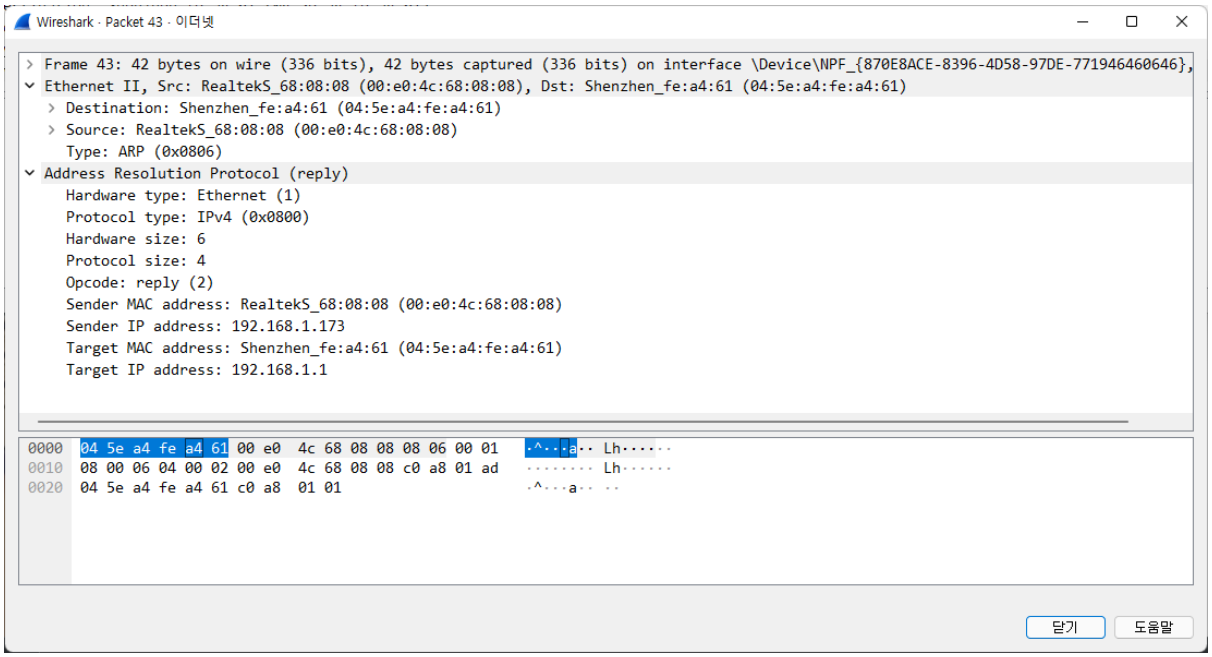
## 2. 와이어샤크를 통한 ARP Request/Reply 패킷 분석 결과 (스크린샷 포함 및 분석 대상 ARP패킷의 필드 소개 및 분석 내용을 정리함)




Request




Reply




송신 측인 Shenzhen_fe:a4:61은 집에서 사용하고 있는 Netis사의 공유기 주소이고, 수신 측인 RealtekS_68:08:08은 노트북의 LAN카드 주소이다.

**패킷 필드 분석**

- Hardware type: 사용 중인 네트워크의 하드웨어를 정의한다. 여기서는 이더넷을 사용하였다.
- Protocol type: 매핑 대상의 프로토콜 유형을 정의한다. IPv4이므로 0x0800으로 세팅되었다.
- Hardware Size: 하드웨어의 길이를 정의한다. Byte 단위이며 이더넷은 6으로 세팅한다.
- Protocol Size: 프로토콜 주소의 길이를 나타낸다. Byte 단위이며 IPv4는 4로 세팅한다.

- Opcode: Operation Code, ARP의 구체적인 동작을 나타낸다.
- Sender MAC address: 송신 측의 MAC 주소를  나타낸다.
- Sender IP address: 송신 측의 IP 주소를 나타낸다.
- Target Mac address: 수신 측의 MAC 주소를 나타낸다. (Request를 할 때 에는 수신 측의 MAC 주소를 아직 모르므로 0으로 설정된다)
- Target IP address: 수신 측의 IP 주소를 나타낸다.

위의 ARP 프로토콜을 보면 배운 것과 다르게 Request가 Broadcast가 아닌 Unicast를 사용하고 있다. 이에 대해 조사해본 결과 Arp Cache Validation을 하는 곳에서 Unicast Poll이라는 것을 발견하게 됐는데, 주기적으로 Point-to-point ARP Request를 보내서 ARP Reply가 되지 않으면 항목을 삭제하는 메커니즘이 있었다. 아마 계속해서 연결을 유지하기 위한 방법인 것 같고 위의 ARP 프로토콜은 Unicast Poll이 적용된 통신인 것으로 예상이 된다.

참조 문헌

Wikipedia. "Address Resolution Protocol". https://en.wikipedia.org/wiki/Address_Resolution_Protocol
(n. d.). "rfc1122". https://www.ietf.org/rfc/rfc1122.txt. 1989.