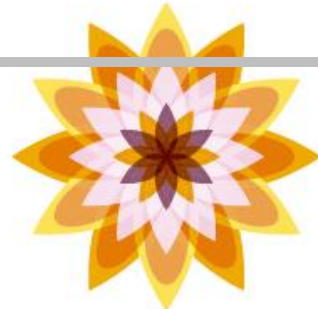
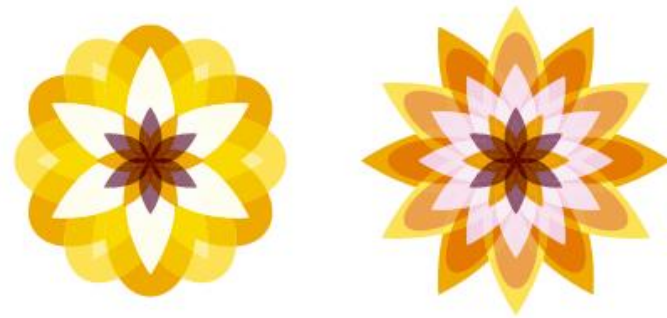


*Chapter 07*

# 주소 변환 프로토콜 (ARP)



# 1. 주소 변환

- 인터넷은 라우터나 게이트웨이와 같은 네트워크를 연결하는 장치들이 서로 연결된 네트워크들로 구성된다.
- 따라서 발신지 호스트가 보낸 패킷은 목적지 호스트에 도달하기 전에 서로 다른 물리적인 네트워크를 지나갈 수 있다.
- 호스트와 라우터는 네트워크 레벨에서 자신의 논리 주소(logical address)로 인식된다.
- 이 논리 주소는 전 세계적으로 유일한 주소로서 실제로 소프트웨어로 구현되므로 논리 주소라고 한다.
- 네트워크를 연결하기 위해 사용되는 모든 프로토콜은 논리 주소가 필요하다.
- TCP/IP 프로토콜 그룹에서 논리 주소는 IP 주소라고 하며 32bit(IPv4) 또는 128bit(IPv6)길이를 가지고 있다.

# 1. 주소 변환

- 그러나 패킷은 호스트와 라우터에 도달하기 위해 물리적인 네트워크를 통과하게 된다.
- 물리적인 레벨에서 호스트와 라우터들은 물리 주소에 의해 인식된다.
- 물리 주소는 로컬 주소(local address)이다.
- 이 주소는 로컬 네트워크 내에서만 유효하다.
- 따라서 이 주소는 로컬에서만 유일하면 되고 전 세계적으로 유일할 필요는 없다.
- 물리 주소라고 부르는 이유는 이 주소가 보통 하드웨어로 구현되기 때문이다.
- 물리 주소의 예는 이더넷이나 토큰 링의 48bit MAC 주소가 있으며 이 주소는 호스트나 라우터 내에 설치된 NIC(네트워크 인터페이스 카드)에 들어있다.
- 물리 주소와 논리 주소는 서로 다른 식별자이다.

# 1. 주소 변환

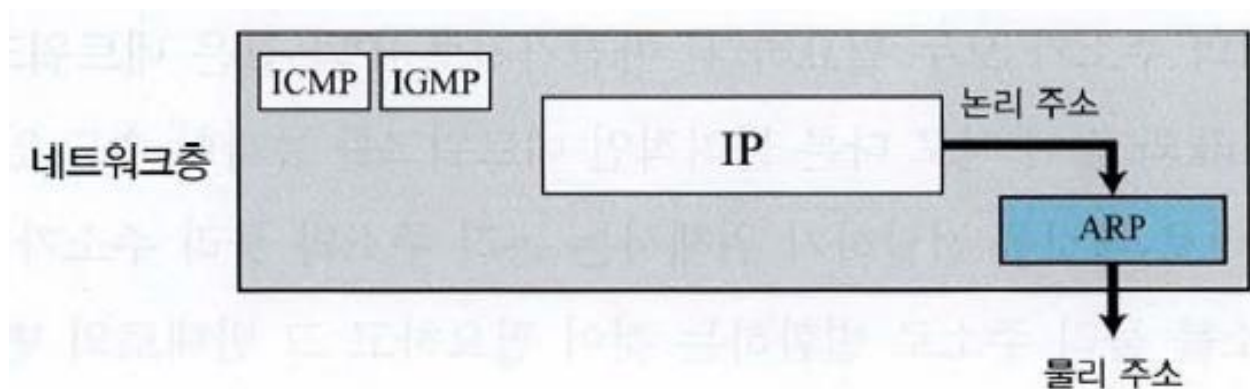
- 호스트나 라우터로 패킷을 전달하기 위해서는 논리 주소와 물리 주소가 모두 필요하다.
- 따라서, 논리 주소를 물리 주소로 변환하는 것이 필요하고 그 반대로의 변환도 필요하다.
- 이 변환은 정적이나 동적으로 가능하다.
- 정적 변환은 몇 가지 문제점 때문에 사용되지 않고 있고 동적 변환을 이용하고 있다.
- 동적 변환(dynamic mapping)에서는 물리 주소와 논리 주소 쌍 중 하나만을 알고 있을 때 프로토콜을 사용하여 다른 하나를 알 수 있다.
- 이러한 동적 변환을 수행하기 위해 주소 변환 프로토콜(Address Resolution Protocol; ARP)과 역 주소 변환 프로토콜(Reverse Address Resolution Protocol; RARP)이 설계되었다.
- ARP는 논리 주소를 물리 주소로 변환하고 RARP는 물리 주소를 논리 주소로 변환한다.

# 1. 주소 변환

- ARP의 역할을 그림으로 나타내면 그림과 같다.



- ARP는 유니캐스트와 브로드캐스트 물리 주소를 사용한다.
- 그림은 TCP/IP 프로토콜 모음에서 ARP의 위치를 보여준다.

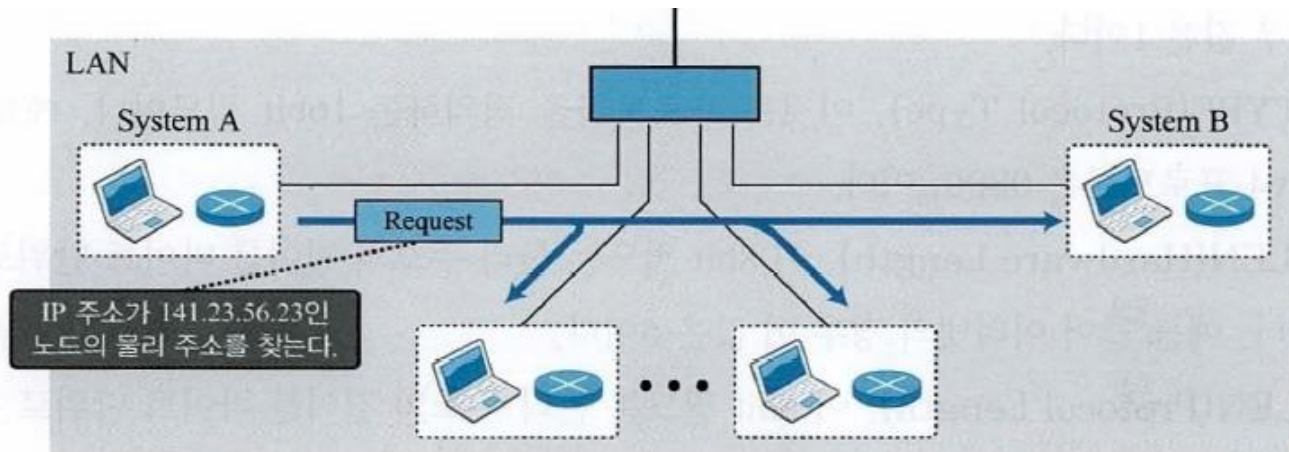


## 2. 주소 변환 프로토콜(ARP)

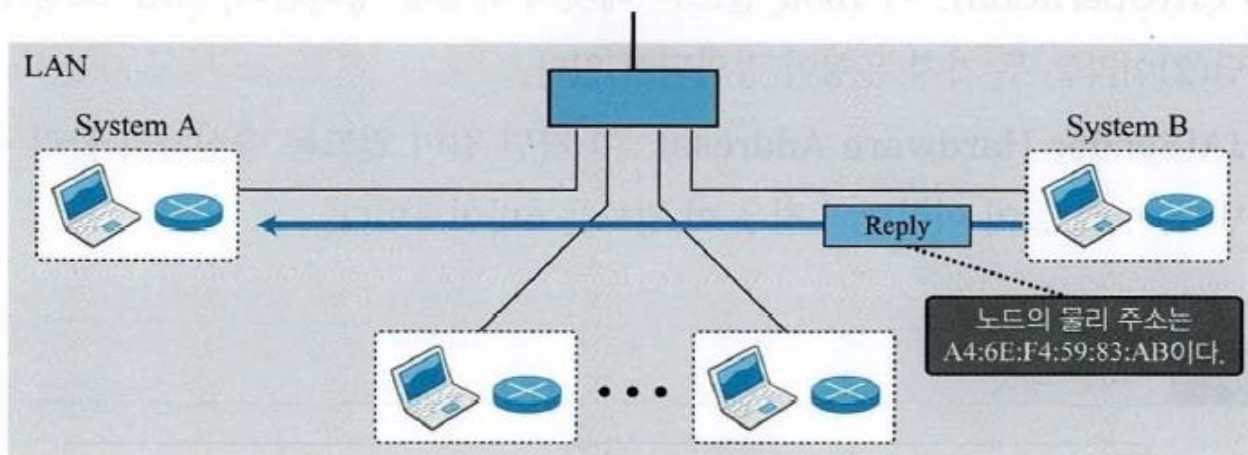
- 어떤 호스트나 라우터가 다른 호스트나 라우터에 보낼 IP 데이터그램을 가지고 있다면 송신자는 수신자의 논리 주소인 IP 주소를 가지고 있다.
- 그러나 IP 데이터그램은 물리적인 네트워크를 통과하기 위해 프레임에 캡슐화되어야 한다.
- 그러기 위해서 송신자는 수신자의 물리 주소를 알아야 한다.
- ARP는 이러한 변환을 동적으로 수행하기 위해 설계되었다.
- ARP는 IP 주소를 물리 주소와 연관시킨다.
- LAN과 같은 전형적인 물리적인 네트워크에서 각 링크 상의 장치는 NIC 내에 저장된 물리 주소에 의해 식별된다.
- 하나의 호스트나 라우터가 같은 네트워크에 있는 다른 호스트나 라우터의 물리 주소가 필요하다면, ARP 요청(request) 패킷을 보낸다.

## 2. 주소 변환 프로토콜(ARP)

- 송신자는 수신자의 물리 주소를 모르기 때문에 요청 패킷을 네트워크상에 브로드캐스트한다.



a. ARP 요청은 브로드캐스트



b. ARP 응답은 유니캐스트

## 2. 주소 변환 프로토콜(ARP)

### ■ ARP 패킷 형식

- 그림은 ARP 패킷 형식을 보여준다.

Hardware Type		Protocol Type
Hardware length	Protocol length	Operation Request 1, Reply 2
Sender hardware address (예, 이더넷은 6바이트)		
Sender protocol address (예, IP는 4바이트)		
Target hardware address (예, 이더넷은 6바이트) (request인 경우는 비어있음)		
Target protocol address (예, IP는 4바이트)		



## 2. 주소 변환 프로토콜(ARP)

### ■ ARP 패킷 형식

#### ■ ARP 패킷의 필드들은 다음과 같다.

- HTYPE(Hardware Type)
  - 이것은 ARP가 수행되고 있는 네트워크 유형을 나타내는 16bit 필드이다. 각 LAN은 유형에 따라 정수로 할당되어 있다.
  - 예를 들어 이더넷의 경우 값은 1이다.
- PTYPE(Protocol Type)
  - 이것은 프로토콜을 정의하는 16bit 필드이다.
  - 예를 들어 IPv4 프로토콜은 0800<sub>16</sub>이다.
- HLEN(Hardware Length)
  - 이 8bit 필드는 물리 주소의 길이를 바이트 단위로 정의한다.
  - 예를 들어 이더넷의 경우 이 값은 6이다.
- PLEN(Protocol Length)
  - 이 8bit 필드는 논리 주소의 길이를 바이트 단위로 정의한다.
  - 예를 들어 IPv4의 경우 이 값은 4이다.

## 2. 주소 변환 프로토콜(ARP)

### ■ ARP 패킷 형식

- ARP 패킷의 필드들은 다음과 같다.
  - OPER(Operation)
    - 이 16bit 필드는 패킷의 유형을 정의한다.
    - ARP 요청(1)과 ARP 응답(2) 이라는 두 가지 유형이 정의되어 있다.
  - SHA(Sender Hardware Address)
    - 이 가변 길이 필드는 송신자의 물리 주소를 나타낸다.
    - 예를 들어 이더넷의 경우 이 필드는 6바이트이다.
  - SPA(Sender Protocol Address)
    - 이 가변 길이 필드는 IP 주소와 같은 송신자의 논리 주소를 나타낸다.
    - IP 프로토콜의 경우 이 필드는 4바이트이다.

## 2. 주소 변환 프로토콜(ARP)

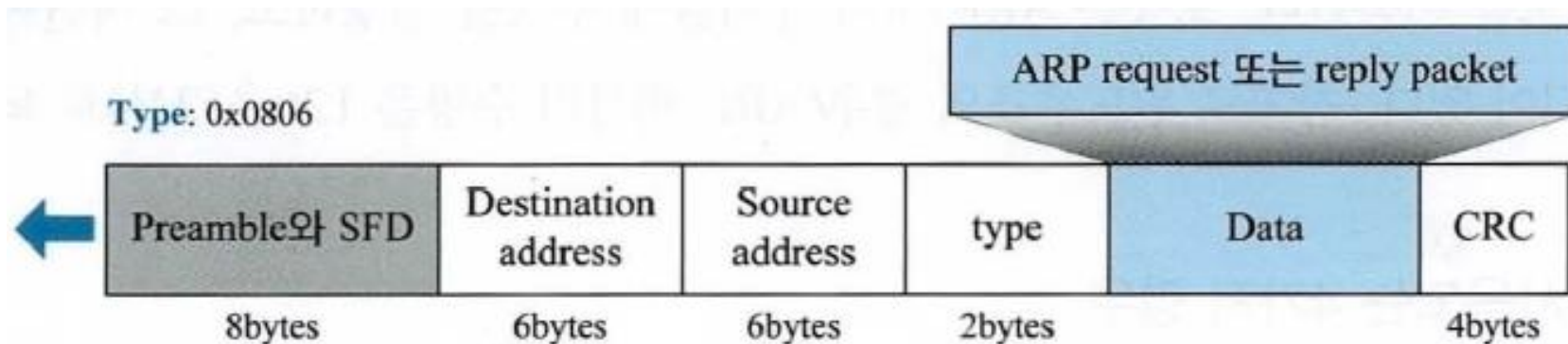
### ■ ARP 패킷 형식

- ARP 패킷의 필드들은 다음과 같다.
  - THA(Target Hardware Address)
    - 이 가변 길이 필드는 타겟의 물리 주소를 나타낸다.
    - 예를 들어 이더넷의 경우 이 필드는 6바이트이다.
    - ARP 요청의 경우 송신자는 타겟의 물리 주소를 모르므로 이 필드는 0 이다.
  - TPA(Target Protocol Address)
    - 이 가변 길이 필드는 P 주소와 같은 타겟의 논리 주소이다.
    - IPv4의 경우 이 필드는 4바이트이다.

## 2. 주소 변환 프로토콜(ARP)

### ■ 캡슐화

- ARP 패킷은 데이터 링크층 프레임으로 캡슐화된다.
- 예를 들어 그림에서 ARP 패킷은 이더넷 프레임에 의해 캡슐화되어 있다.
- 유형(Type) 필드는 프레임에 의해 전달되는 데이터가 ARP 패킷임을 나타내고 있다.



## 2. 주소 변환 프로토콜(ARP)

### ■ 동작

#### ■ 과정

- 송신자는 타겟(Target)의 IP 주소를 알고 있다.
- IP가 ARP에게 ARP 요청 메시지 생성을 요청한다.
- 이 메시지가 데이터 링크층에 전달되고 여기서 송신자의 물리 주소를 발신지 주소로, 그리고 물리 브로드캐스트 주소를 목적지 주소로 하는 프레임에 의해 캡슐화된다.
- 모든 호스트나 라우터는 이 프레임을 수신한다. 프레임은 브로드캐스트 목적지 주소를 가지고 있으므로 모든 지국은 이 메시지를 자신의 ARP에게 전달한다.
- 타겟 장치는 자신의 물리 주소를 포함하는 ARP 응답 메시지를 보낸다.
- 송신자는 응답 메시지를 받고 타겟의 물리 주소를 알게 된다.
- 타겟에게 보낼 데이터를 포함하고 있는 IP 데이터그램은 이 물리 주소를 갖는 프레임으로 캡슐화되어 목적지에 유니캐스트된다.

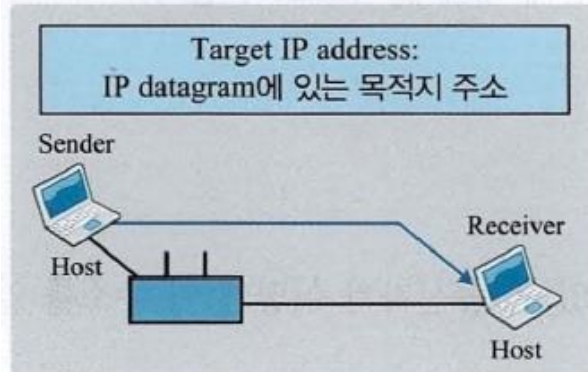
## 2. 주소 변환 프로토콜(ARP)

### ■ 동작

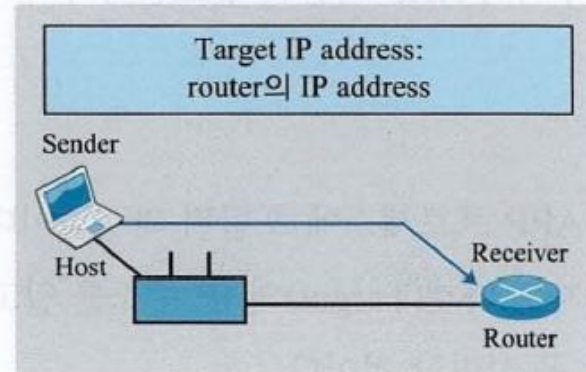
#### ▪ ARP가 사용되는 4가지 경우

- 다음은 ARP 서비스가 사용될 수 있는 네 가지 경우이다.

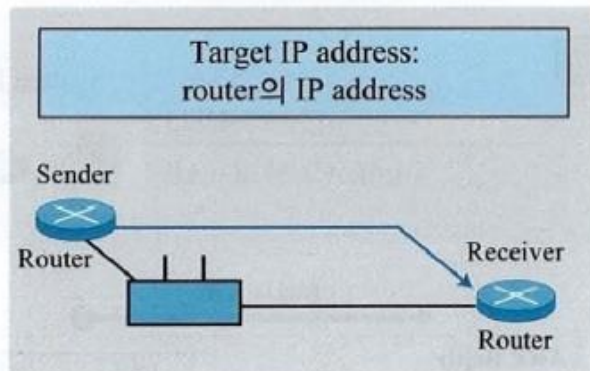
경우 1: 호스트가 같은 네트워크에 있는 호스트에게 패킷을 보내는 경우



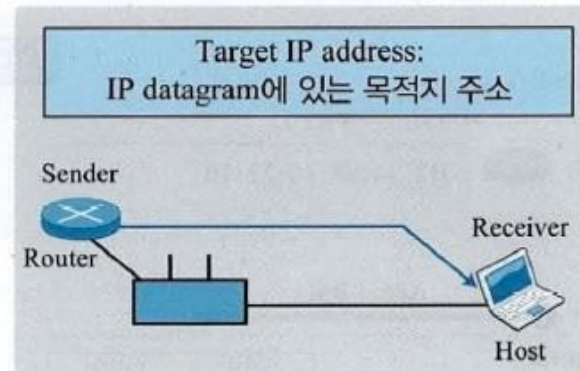
경우 2: 호스트가 다른 네트워크에 있는 호스트에게 패킷을 보내는 경우



경우 3: 라우터가 다른 네트워크에 있는 호스트에게 패킷을 보내는 경우



경우 4: 라우터가 같은 네트워크에 있는 호스트에게 패킷을 보내는 경우

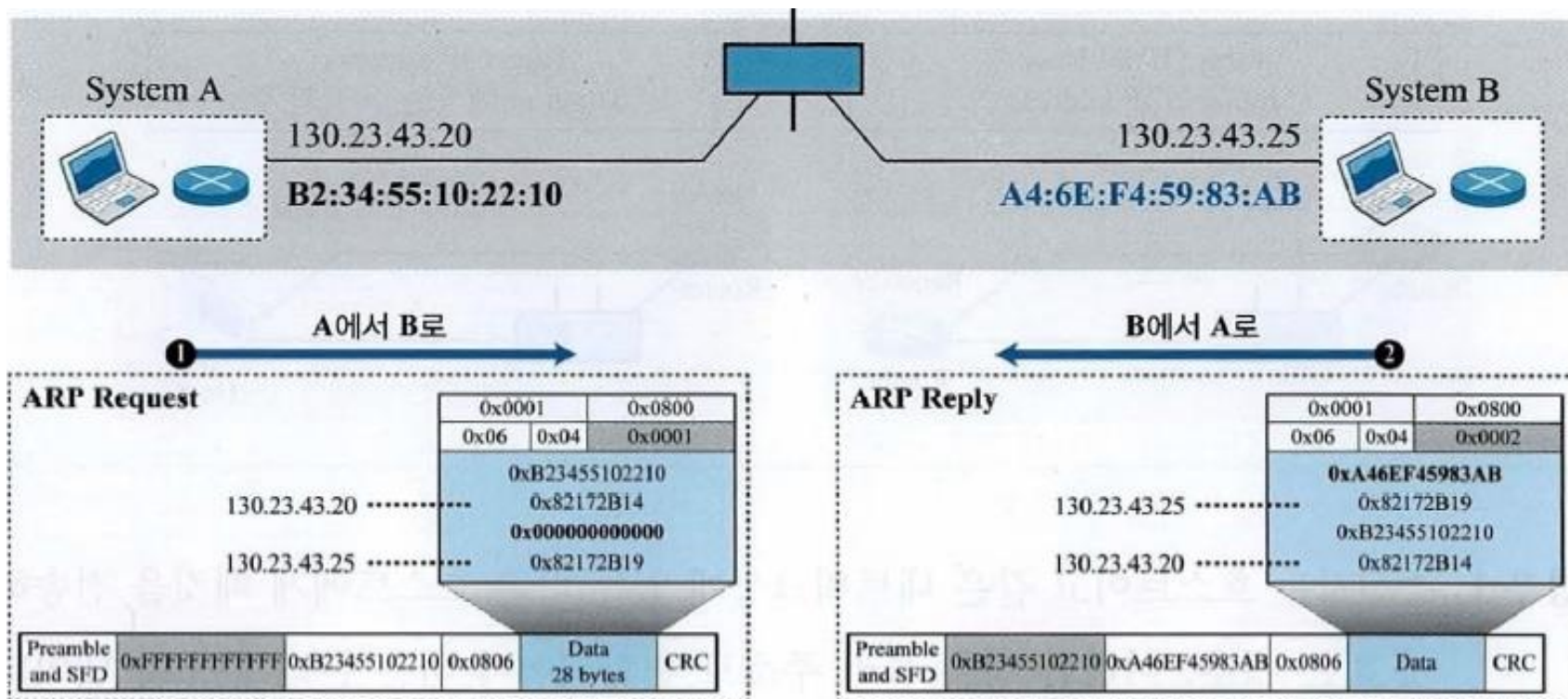


## 2. 주소 변환 프로토콜(ARP)

### ■ 동작

#### ▪ ARP가 사용되는 4가지 경우

- 예제 1. ARP 과정

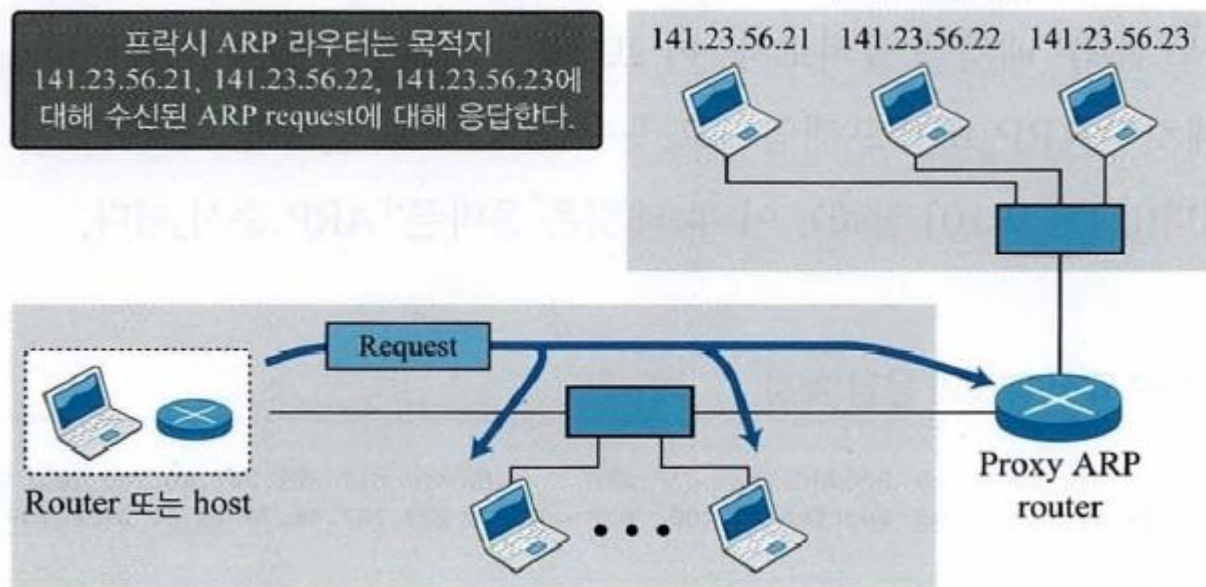




## 2. 주소 변환 프로토콜(ARP)

### ■ 프락시 ARP

- 프락시(proxy) ARP라는 기술은 서브네팅 효과를 만드는 데 사용된다.
- 프락시 ARP는 호스트 집합을 대행하여 수행하는 ARP이다.
- 프락시 ARP를 수행하는 라우터가 이 집합 중에 한 호스트의 물리 주소를 찾는 ARP 요청을 받으면 라우터는 자신의 물리 주소를 ARP 응답 메시지를 통해 알려준다.
- 그런 뒤에 라우터가 실제 IP 패킷을 받으면 라우터는 이 패킷을 적절한 호스트나 라우터에게 보낸다.
- 그림에서 오른쪽 호스트에 설치된 ARP는 타겟 주소가 141.23.56.23 인 ARP 요청에 대해서만 응답을 한다.

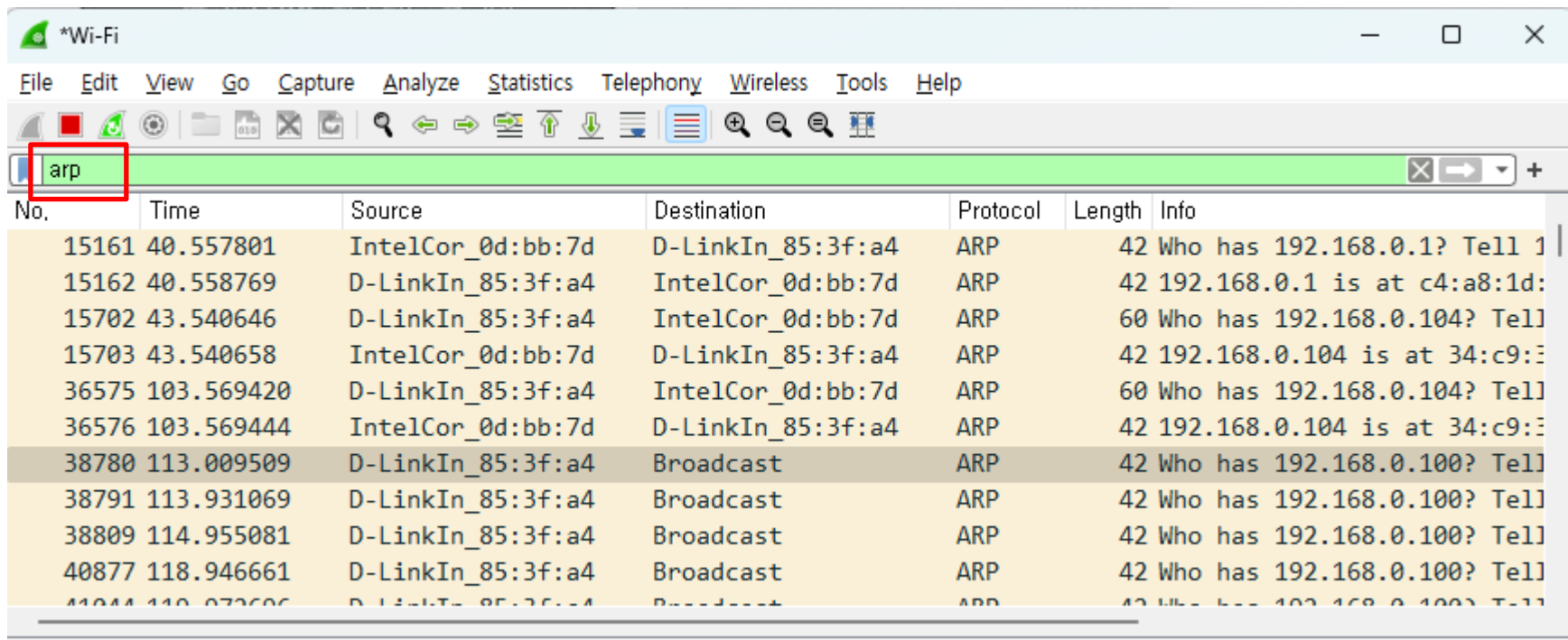




## 2. 주소 변환 프로토콜(ARP)

### ■ ARP 덤프 분석

- 이제 와이어샤크를 이용하여 ARP 덤프 분석을 해보자.
- 먼저 와이어샤크를 실행한 다음 패킷을 캡처한다.
- 어느 정도 패킷이 캡처되었다고 판단되면 캡처 정지 버튼을 누른다.
- 그런 다음 디스플레이 필터에 “arp”를 입력하고 엔터키를 친다.
- 그러면 패킷 목록 정보에 ARP 패킷만 나타난다.



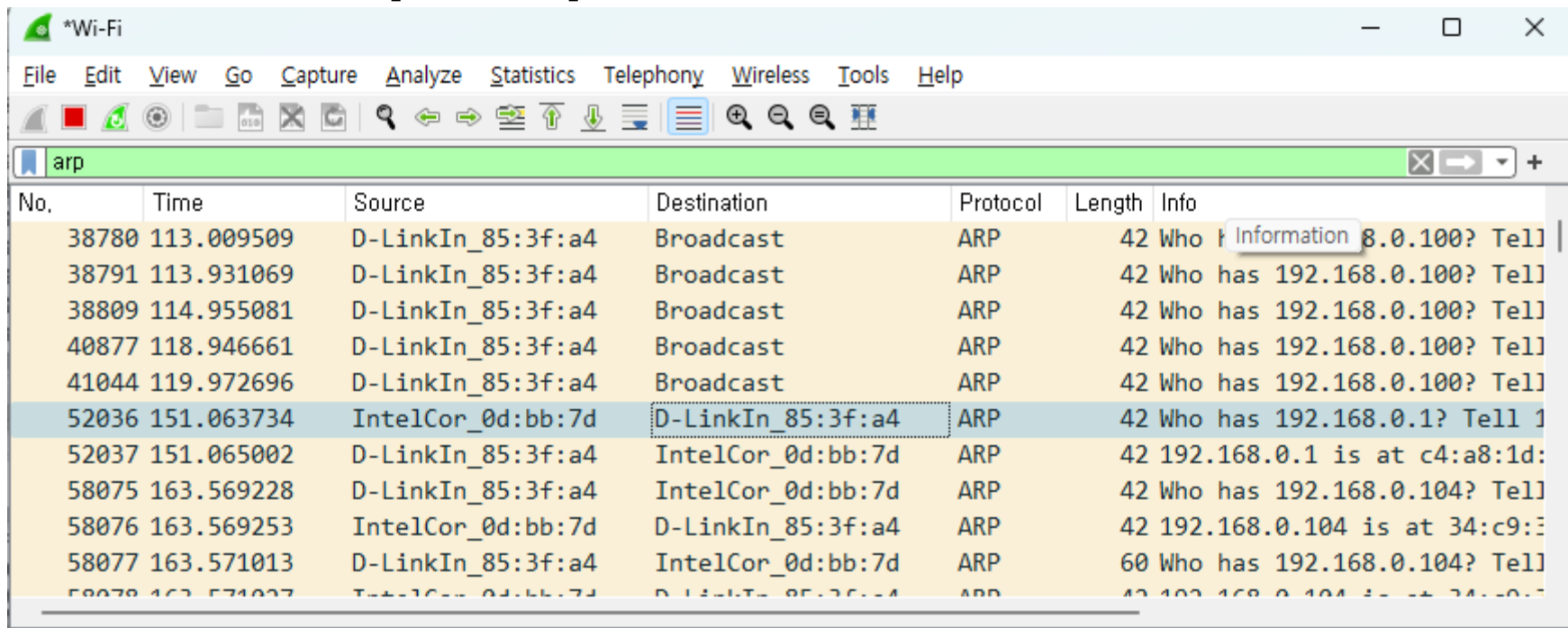
The image shows the Wireshark network protocol analyzer interface. The title bar indicates the capture is on the \*Wi-Fi interface. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The display filter bar at the top shows the filter 'arp' in a green box. Below the filter bar is a table of captured packets. The table has columns for No., Time, Source, Destination, Protocol, Length, and Info. The packets listed are all ARP requests and responses between IntelCor\_0d:bb:7d and D-LinkIn\_85:3f:a4, as well as broadcast requests. The packet list is truncated at the bottom.

No.	Time	Source	Destination	Protocol	Length	Info
15161	40.557801	IntelCor_0d:bb:7d	D-LinkIn_85:3f:a4	ARP	42	Who has 192.168.0.1? Tell 1
15162	40.558769	D-LinkIn_85:3f:a4	IntelCor_0d:bb:7d	ARP	42	192.168.0.1 is at c4:a8:1d:
15702	43.540646	D-LinkIn_85:3f:a4	IntelCor_0d:bb:7d	ARP	60	Who has 192.168.0.104? Tell
15703	43.540658	IntelCor_0d:bb:7d	D-LinkIn_85:3f:a4	ARP	42	192.168.0.104 is at 34:c9:3
36575	103.569420	D-LinkIn_85:3f:a4	IntelCor_0d:bb:7d	ARP	60	Who has 192.168.0.104? Tell
36576	103.569444	IntelCor_0d:bb:7d	D-LinkIn_85:3f:a4	ARP	42	192.168.0.104 is at 34:c9:3
38780	113.009509	D-LinkIn_85:3f:a4	Broadcast	ARP	42	Who has 192.168.0.100? Tell
38791	113.931069	D-LinkIn_85:3f:a4	Broadcast	ARP	42	Who has 192.168.0.100? Tell
38809	114.955081	D-LinkIn_85:3f:a4	Broadcast	ARP	42	Who has 192.168.0.100? Tell
40877	118.946661	D-LinkIn_85:3f:a4	Broadcast	ARP	42	Who has 192.168.0.100? Tell
41044	119.073606	D-LinkIn_85:3f:a4	Broadcast	ARP	42	Who has 192.168.0.100? Tell

## 2. 주소 변환 프로토콜(ARP)

### ■ ARP 덤프 분석

- 여기서 [Info] 열에 [Who has ....]와 [.....is at .....]이 연속해서 나타난 패킷을 살펴본다.
- 예를 들어 그림에 나타난 패킷 목록 정보 중에서 52036번 프레임과 52037번 프레임에 나타난 ARP 패킷을 살펴보자.
- 이 프레임들의 [Info] 열을 보면 [Who has ..... ]라고 되어있는 패킷이 ARP 요청 프레임이고 [..... is at ..... ]이라고 되어있는 패킷이 ARP 응답 프레임이다.
- 이 두 패킷은 올바른 [ARP 순서]이다.



No.	Time	Source	Destination	Protocol	Length	Info
38780	113.009509	D-LinkIn_85:3f:a4	Broadcast	ARP	42	Who has 192.168.0.100? Tell
38791	113.931069	D-LinkIn_85:3f:a4	Broadcast	ARP	42	Who has 192.168.0.100? Tell
38809	114.955081	D-LinkIn_85:3f:a4	Broadcast	ARP	42	Who has 192.168.0.100? Tell
40877	118.946661	D-LinkIn_85:3f:a4	Broadcast	ARP	42	Who has 192.168.0.100? Tell
41044	119.972696	D-LinkIn_85:3f:a4	Broadcast	ARP	42	Who has 192.168.0.100? Tell
52036	151.063734	IntelCor_0d:bb:7d	D-LinkIn_85:3f:a4	ARP	42	Who has 192.168.0.1? Tell 1
52037	151.065002	D-LinkIn_85:3f:a4	IntelCor_0d:bb:7d	ARP	42	192.168.0.1 is at c4:a8:1d:
58075	163.569228	D-LinkIn_85:3f:a4	IntelCor_0d:bb:7d	ARP	42	Who has 192.168.0.104? Tell
58076	163.569253	IntelCor_0d:bb:7d	D-LinkIn_85:3f:a4	ARP	42	192.168.0.104 is at 34:c9:3
58077	163.571013	D-LinkIn_85:3f:a4	IntelCor_0d:bb:7d	ARP	60	Who has 192.168.0.104? Tell
58078	163.571027	IntelCor_0d:bb:7d	D-LinkIn_85:3f:a4	ARP	42	192.168.0.104 is at 34:c9:3

## 2. 주소 변환 프로토콜(ARP)

### ■ ARP 덤프 분석

- 먼저 그림에 나타나 있는 52036번 프레임인 ARP 요청(request)을 확인해 보기 위해 [Info] 옆에 [Who has ....]라고 되어있는 패킷을 선택하여 패킷 상세 정보에서 이 패킷의 [Address Resolution Protocol] 앞의 [>]를 클릭하면 Address Resolution Protocol의 헤더가 전개되어 나타난다.

```
> Frame 52036: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on inter-
> Ethernet II, Src: IntelCor_0d:bb:7d (34:c9:3d:0d:bb:7d), Dst: D-LinkIn_85:3f:a4
✓ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: IntelCor_0d:bb:7d (34:c9:3d:0d:bb:7d)
    Sender IP address: 192.168.0.104
    Target MAC address: D-LinkIn_85:3f:a4 (c4:a8:1d:85:3f:a4)
    Target IP address: 192.168.0.1
```

## 2. 주소 변환 프로토콜(ARP)

### ■ ARP 덤프 분석

#### ■ Hardware type

- 데이터 링크층의 프로토콜 유형을 지정하는 필드이다.
- 그림에는 "1"이란 값이 나타나 있는데, 이것은 Ethernet II 를 사용함을 의미한다.

#### ■ Protocol type

- 이 필드는 네트워크층 프로토콜이 2바이트로 지정된다.
- 여기서는 0x0800이란 값이 들어있고 IPv4로 지정되어 있다.

#### ■ Hardware size

- 이 필드는 데이터 링크층의 주소 길이를 나타내는 필드로서 MAC 주소 길이인 "6"이 지정되어 있다.

#### ■ Protocol size

- 이 필드는 네트워크층의 프로토콜 주소 길이를 나타내는데 IPv4 주소 길이인 "4"가 지정되어 있다.

## 2. 주소 변환 프로토콜(ARP)

### ■ ARP 덤프 분석

#### ■ Opcode

- 이 필드는 2바이트 필드로서 ARP 처리 유형을 지정한다.
- 여기에는 "1"이 들어있고 request(요청)라고 되어있다.
- 이것은 IP 주소를 이용하여 MAC 주소를 조회하는 ARP 요청 브로드캐스트를 의미한다.

#### ■ Sender MAC address

- 이 필드에는 ARP 요청을 보낸 발신지 호스트의 MAC 주소를 지정하는 6바이트 필드이다.
- 여기에는 송신자 호스트의 MAC 주소가 들어있다.

#### ■ Sender IP address

- 이 필드는 ARP 요청을 보낸 발신지 호스트의 IP 주소를 지정하는 4바이트 필드이다.

## 2. 주소 변환 프로토콜(ARP)

### ■ ARP 덤프 분석

#### ■ Target MAC address

- 이 필드는 통신 상대방 호스트의 MAC 주소를 지정하는 6바이트 필드이다. LAN을 통하여 통신하려면 상대방 호스트의 MAC 주소를 알아야 한다.
- 그러나 지금은 통신 상대방 호스트의 MAC 주소를 모르는 상태이다.
- 따라서 ARP 요청에는 [Target MAC address] 필드에는 아무것도 지정하지 않고, 모두 0으로 채워져서 LAN 전체에 브로드캐스트 된다.
- 그래서 [00 00 00 00 00 00]이 들어가 있음을 알 수 있다.

#### ■ Target IP address

- 이 필드는 통신하고자 하는 상대방 호스트의 IP 주소를 지정하는 4바이트 필드이다.
- 따라서, 통신 상대방 호스트의 IP 주소가 들어가 있다.

## 2. 주소 변환 프로토콜(ARP)

### ■ ARP 덤프 분석

- [Target IP address]는 통신하고자 하는 상대방 호스트의 IP 주소를 지정하는 4바이트 필드이다.
- 따라서, 통신 상대방 호스트의 IP 주소가 들어가 있다.
- 패킷 상세 정보의 Ethernet II 앞의 [>]를 클릭하면 그림과 같이 전개되어 나타난다.

```
> Frame 52037: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface 0
  0:0 Ethernet II, Src: D-LinkIn_85:3f:a4 (c4:a8:1d:85:3f:a4), Dst: IntelCor_0d:bb:7d:11:11:11
    0:0 Destination: IntelCor_0d:bb:7d (34:c9:3d:0d:bb:7d)
    0:0 Source: D-LinkIn_85:3f:a4 (c4:a8:1d:85:3f:a4)
    0:0 Type: ARP (0x0806)
  0:0 Address Resolution Protocol (reply)
```

## 2. 주소 변환 프로토콜(ARP)

### ■ ARP 덤프 분석

- 이어서 패킷 상세 정보의 [Address Resolution Protocol] 앞의 [>]를 클릭하여 전개해 보면 그림과 같이 나타난다.

```
> Frame 52037: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface
> Ethernet II, Src: D-LinkIn_85:3f:a4 (c4:a8:1d:85:3f:a4), Dst: IntelCor_0d:bb:7d
  ▾ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: D-LinkIn_85:3f:a4 (c4:a8:1d:85:3f:a4)
    Sender IP address: 192.168.0.1
    Target MAC address: IntelCor_0d:bb:7d (34:c9:3d:0d:bb:7d)
    Target IP address: 192.168.0.104
```



## 2. 주소 변환 프로토콜(ARP)

### ■ ARP 덤프 분석

- 그림에서 맨 앞에 있는 [Hardware type:], [Protocol type:], [Hardware size:], [Protocol size:]의 각 필드의 값은 ARP 요청과 같다.
- 다른 것은 [Opcode: ]라는 2바이트 필드로서 여기에는 [reply (2)]라고 되어있다.
- 이것은 이 패킷이 ARP 응답 유니캐스트 패킷임을 알 수 있다.
- 구체적으로 ARP 요청 메시지를 받은 IP 주소를 사용하고 있는 시스템의 MAC 주소를 응답하는 패킷이다.
- ARP 요청과 응답의 흐름을 살펴보자.
- [Sender MAC address:] 필드에는 ARP 응답을 보낸 라우터나 호스트의 MAC 주소가 6바이트로 지정되어 있다.
- 같은 근거리 통신망에 있는 호스트와 통신하는 것이 아니라 라우터를 경유하여 통신망 외부와 통신하기 위한 경우에는 외부 네트워크로 나가는 출구인 디폴트 라우터의 MAC 주소가 된다.
- 또한 [Sender IP address:] 필드에는 ARP 응답을 보낸 발신지의 IP 주소가 4바이트로 지정된다.
- 여기에 라우터의 IP 주소가 지정된다.
- 이처럼 LAN 내에서는 직접 통신하는 장치가 ARP 응답을 하며 LAN 외부에 대해서는 디폴트 라우터 장치가 ARP 응답을 하게 된다.

## 2. 주소 변환 프로토콜(ARP)

### ■ ARP 덤프 분석

- 여기서 ARP 캐시 테이블을 확인해 보자.
- ARP 요청과 응답 결과는 요청한 호스트와 응답한 호스트 모두 ARP 캐시에 저장된다
- 윈도우즈에서는 ARP 캐시 테이블에 120초간(2분간) IP 주소와 MAC 주소가 저장된다.
- 명령 프롬프트에서 ARP 명령에 테이블을 보여주는 옵션 [-a]를 붙임으로써 이 ARP 캐시 테이블을 확인할 수 있다.
- 또한, arp 명령을 사용할 때는 기존의 ARP 캐시(임시 저장소)를 미리 삭제해 둘 필요가 있다.
- ARP 캐시를 삭제하는 옵션 명령은 [-d]이다.

```
C:\Windows\System32>arp -a
```

인터페이스: 192.168.0.104 --- 0xa	인터넷 주소	물리적 주소	유형
192.168.0.1	c4-a8-1d-85-3f-a4	정적	
192.168.0.100	3c-f7-a4-1f-ac-03	정적	
192.168.0.255	ff-ff-ff-ff-ff-ff	정적	
224.0.0.22	01-00-5e-00-00-16	정적	
224.0.0.251	01-00-5e-00-00-fb	정적	
224.0.0.252	01-00-5e-00-00-fc	정적	
239.255.255.250	01-00-5e-7f-ff-fa	정적	
255.255.255.255	ff-ff-ff-ff-ff-ff	정적	

인터페이스: 172.28.64.1 --- 0x34	인터넷 주소	물리적 주소	유형
172.28.79.255	ff-ff-ff-ff-ff-ff	정적	
224.0.0.22	01-00-5e-00-00-16	정적	
224.0.0.251	01-00-5e-00-00-fb	정적	
224.0.0.252	01-00-5e-00-00-fc	정적	
239.255.255.250	01-00-5e-7f-ff-fa	정적	
255.255.255.255	ff-ff-ff-ff-ff-ff	정적	

## 2. 주소 변환 프로토콜(ARP)

### ■ ARP 덤프 분석

- ARP 명령에는 [arp -s IP 주소 MAC 주소]라는 옵션도 있다.
- 이 옵션을 이용하면 ARP의 정적 항목을 수동으로 추가할 수 있다.
- 예를 들어 [arp -s 192.168.0.100 00-10-db-11-11-11]과 같은 명령을 실행하면 IP 주소 [192.168.0.100]에 대해서 항상 MAC 주소가 [00-10-db-11-11-11]이란 조합을 ARP 캐시 테이블에 등록한다.
- 원래 ARP 항목이 있으면 호스트는 ARP 요청을 보내지 않는다.
- 따라서 ARP에 대응되지 않는 기기와 통신할 경우나 의도적으로 APR 패킷을 보내고 싶지 않은 경우에는 정적 항목을 이용하면 된다.



**Thank You**

---