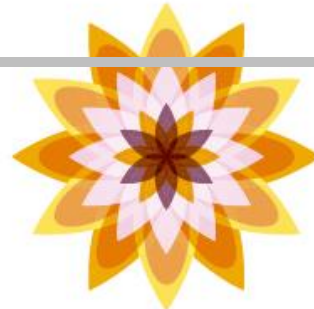
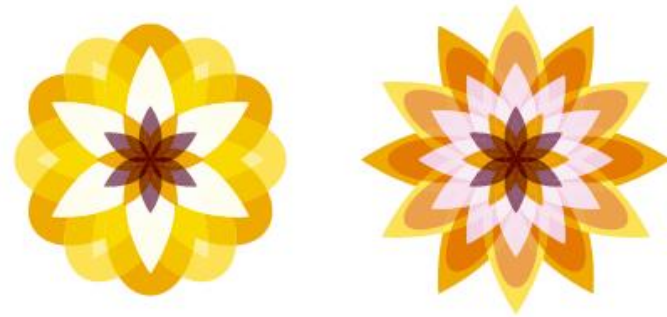


Chapter 06

근거리 통신망: 유선 이더넷



1. IEEE 표준 이더넷

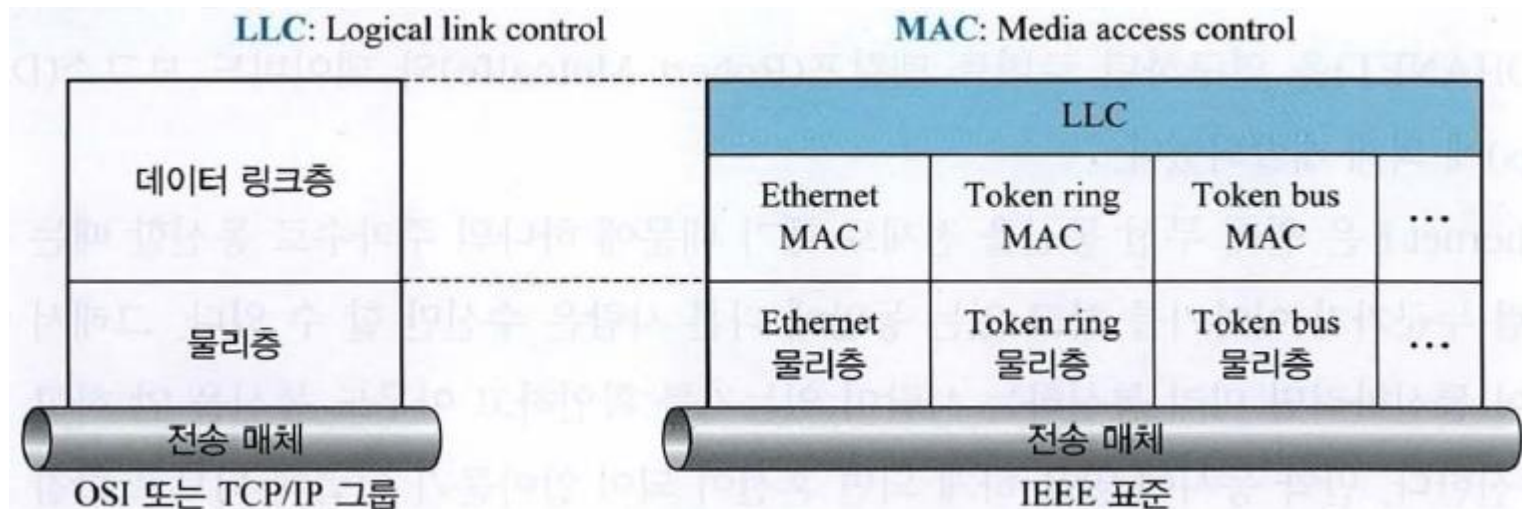
- Ethernet II은 원래 무선 통신을 전제로 했기 때문에 하나의 주파수로 통신할 때는 무전기처럼 누군가가 이야기를 하고 있는 동안에 다른 사람은 수신만 할 수 있다.
- 그래서 여러 사람이 통신하려면 미리 통신하는 사람이 있는지를 확인하고 아무도 통신을 안 하고 있으면 송신한다.
- 만약 동시에 말을 하게 되면 혼선이 되어 알아듣기 어렵게 되므로 한참 기다렸다 다시 통신을 시도한다.
- 이것은 CSMA/CD(반송파 탐지 다중 접속/충돌 검출)방식이라 불리며, 송신 또는 수신을 한쪽만 하는 반이중 데이터 통신에서 이용되고 있다.

1. IEEE 표준 이더넷

- Ethernet II는 원래 약 2.7Mbps 속도로 통신하는 규격으로 설계되었다.
- 그 후 제록스사, DEC사(현재의 휴렛패커드사)와 인텔사를 비롯한 파트너 기업과 제휴하여 전송 속도를 10 Mbps로 올린 Ethernet II를 발표하였다.
- 또한, Ethernet II를 TCP/IP와 마찬가지로 공개하기로 하고 미국 전기전자공학 회(IEEE)에서 표준으로 제정하였다.
- 1980년 2월에 탄생했기 때문에 LAN에 관한 표준화를 제정하는 위원회를 IEEE 802 위원회라고 한다.
- IEEE 802 위원회는 근거리 통신망(LAN)에 관한 표준화 작업을 하고 있으며 작업 분과(Working Group)도 여러 가지가 있다.
- 분과에는 숫자가 매겨 있어, 예를 들면 CSMA/CD 방식 분과는 IEEE 802.3 WG으로 표준화 작업을 하고 있다.

1. IEEE 표준 이더넷

- 또 분과 밑에는 분야별로 Task Group이 형성되어 있다.
- Task Group에는 분과마다 알파벳이 a에서부터 순서대로 매겨져 구별된다.
- 예를 들어 우리가 사용하고 있는 무선 LAN 규격 중 하나인 IEEE 802.11b란 이름이 있다.
- 이것은 무선 LAN 규격을 제정하는 IEEE 802.11 분과에서 2.4GHz 대역을 이용하여 11Mbps 전송속도로 통신을 하는 Task Group 이름이다.
- IEEE 802 표준과 TCP/IP 프로토콜 그룹 사이의 관계는 그림에 나타나 있다.



■ 논리 링크 제어 (LLC)

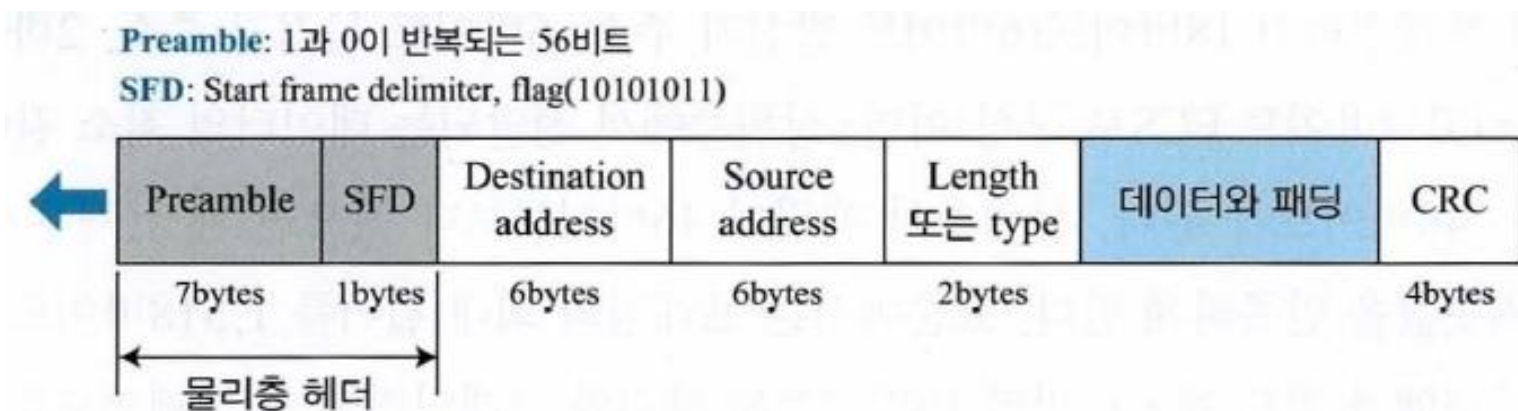
- IEEE 프로젝트 802에서는 흐름 제어, 오류 제어와 프레임 생성 일부분에 대한 역할을 논리 링크 제어(logical link control)라는 하나의 부계층에서 처리한다.
- 즉, 프레임 생성은 LLC 부계층과 MAC 부계층 양쪽에서 모두 처리된다.
- LLC는 모든 IEEE LAN을 위해 하나의 데이터 링크 제어 프로토콜을 제공한다.
- LLC 프로토콜은 서로 다른 LAN들 사이에 연결성을 제공할 수 있는데 이것은 LLC가 MAC 부계층을 투명하게 만들기 때문이다.

■ 매체 접근 제어 (MAC)

- IEEE 프로젝트 802는 각각의 LAN을 위해 특별한 접근 방법인 매체 접근 제어 (MAC; Medium Access Control)라 불리는 부계층을 만들었다.
- 예를 들어, 이더넷 LAN을 위한 매체 접근 방식으로써 CSMA/CD를 정의하였고 토큰 링이나 토큰 버스 LAN을 위해 토큰 패싱 방식을 정의하였다.
- 앞에서 설명했듯이 프레임을 만드는 기능의 일부도 MAC 층에서 다루어진다.

2. Ethernet II 프레임 형식

- Ethernet II는 데이터 링크층 프로토콜이다.
- LAN 프레임 형식에는 IEEE가 정한 IEEE 802.3 형식이 있지만 TCP/IP 모델에서는 Ethernet II 프레임 형식인 RFC 894가 사실상 표준으로 사용되고 있다.
- 또한 Ethernet II 프레임 형식은 DEC사, Intel사, Xerox사 등이 중심이 되어 규정했기 때문에 이들 3사의 머리글자를 따서 [DIX 규격]이라고도 한다.
- Ethernet II의 프레임 형식을 그림으로 나타내면 그림과 같다.



2. Ethernet II 프레임 형식

■ 각 필드의 기능은 다음과 같다.

■ 프리엠블(preamble)

- 0과 1이 반복되는 8바이트(64bit)가 들어있는 프레임의 첫 번째 필드로서 시스템에 들어오는 프레임을 수신하게 하고 입력 타이밍을 맞추게 한다.
- 패턴은 단지 경고와 타이밍 펄스를 제공한다.
- 64bit 패턴은 프레임의 시작을 나타낸다.
- 실제로 프리엠블은 물리 계층에서 추가되므로 프레임 일부가 아니다.

■ 목적지 주소(DA: Destination Address)

- DA 필드는 6바이트이고, 패킷을 수신하는 목적지 지국 또는 지국들의 물리(MAC) 주소가 들어있다.

■ 발신지 주소(SA: Source Address)

- SA 필드도 6바이트이고, 패킷 송신자의 물리(MAC) 주소가 들어있다.

2. Ethernet II 프레임 형식

■ 각 필드의 기능은 다음과 같다.

■ 이더넷 유형 (ether type)

- 이 필드는 유형 필드를 나타낸다.
- 원래의 이더넷은 이 필드를 MAC 프레임을 이용한 상위 계층 프로토콜을 나타내는 유형 필드로 사용한다.

■ 데이터(data)

- 데이터 필드는 상위 계층 프로토콜로부터 캡슐화된 데이터를 전달한다.
- 데이터 필드는 최소 46바이트에서 최대 1,500바이트의 크기를 갖는다.
- 따라서, 상위층에서 오는 데이터가 1,500 바이트 이상인 경우 이것은 하나 이상의 프레임으로 단면화 및 캡슐화되어야 한다.
- 46바이트 미만인 경우 여분의 공간에 0으로 패딩해야 한다.
- 패딩된 데이터 프레임은 상위 계층 프로토콜로 그대로(패딩을 제거하지 않은 채로) 전달되어도, 이는 상위 계층이 패딩을 제거하거나(발신자의 경우) 추가해야 한다는 것을 의미한다.
- 상위층 프로토콜은 그 데이터의 길이를 알아야 한다.
- 예를 들어, 데이터 그램은 데이터의 길이를 정의하는 필드가 있다.

2. Ethernet II 프레임 형식

■ 각 필드의 기능은 다음과 같다.

■ 데이터(data)

- Ethernet II 프레임은 최소 길이가 512bit, 즉 64바이트가 되어야 한다.
- 이 길이의 일부분이 헤더와 트레일러이다.
- 헤더와 트레일러가 18바이트(6바이트 발신지 주소, 6바이트 목적지 주소, 2바이트 유형, 그리고 4바이트 FCS로 구성)이면, 상위층에서 전달되는 데이터의 최소 길이는 $64 - 18 = 46$ 바이트가 된다.
- 상위층의 패킷이 46바이트보다 작으면 패딩(채우기)을 통해서 최소값을 만족하게 한다.
- 표준에서는 프레임의 최대 길이를 1,518바이트로 정의한다(프리앰블 필드 제외).
- 만약 18바이트의 헤더와 트레일러를 빼면 페이로드의 최대 길이는 1,500바이트이다.

■ 프레임 확인 순서 (FCS; Frame Check Sequence)

- 마지막 필드에는 4바이트 길이로 오류 검출 정보가 포함된다.

2. Ethernet II 프레임 형식

- 앞서 설명한 것처럼 와이어샤크에서는 확인할 수 없지만, 프레임의 맨 앞에 [프리엠블]이라는 동기를 맞추기 위해 10101010 ... 10 형태의 8바이트(64bit) 동기 신호가 들어간다.
- 또 트레일러에는 [FCS(프레임 확인 순서)]라는 패킷의 내용을 확인하기 위해 4바이트 오류 확인 데이터가 붙게 된다.
- 프리엠블을 제외한 패킷의 길이는 FCS를 포함하면 64바이트가 되며 이것이 Ethernet II 패킷의 최소 길이가 된다.
- 이 길이보다 작으면 [패딩(Padding)] 데이터를 넣어서 최소 길이를 맞추고 있다.
- 송신자와 수신자에 이용하는 주소를 [MAC 주소]라고 한다.
- MAC 주소는 각각의 LAN 카드를 나타내는 6바이트 주소로 모든 LAN 카드(무선 LAN 카드 포함)마다 서로 다른 유일한 주소가 부여되어 있다.
- 그래서 MAC 주소는 물리 주소, 지국 주소라고 불리기도 한다.

2. Ethernet II 프레임 형식

- MAC 주소가 무선 LAN 카드를 포함한 모든 LAN 카드에 제대로 할당되었는지 궁금할 수 있다.
- 그러나 다행히 MAC 주소는 6바이트이므로 IP 주소인 4바이트에 비하면 여유가 있다.
- 그렇지만 제조사나 회사가 멋대로 MAC 주소를 부여하면 중복이 발생할 수 있다.
- 따라서 MAC 주소에는 일정한 규칙이 있다.
- 6바이트 길이인 MAC 주소 중에서 처음 3바이트를 [OUI(Organizationally Unique Identifier)]라 하며 어느 제조 회사가 LAN 카드를 만들었는지를 식별하기 위한 필드이다.
- 이 OUI는 IEEE 802 위원회에서 관리되고 있으며 웹 페이지 (<http://standards.ieee.org/regauth/oui/index.html>)에서 최신 목록을 확인할 수 있다.
- 또 MAC 주소의 뒤쪽 3바이트는 제조 회사에서 부여한 일련번호를 나타낸다.

2. Ethernet II 프레임 형식

- MAC 주소에는 지국을 나타내는 주소 외에 특정 그룹에 대해 송신하는 [멀티캐스트 MAC 주소]나 LAN에 접속하고 있는 모든 지국에 동시에 전달하는 [브로드캐스트 MAC 주소]가 있다.
- 멀티캐스트 MAC 주소는 처음 25bit가 00000001 00000000 01011110 0 이 되며 16진수로 나타내면 이 부분은 01-00-5E가 된다.
- 이 뒤에 이어지는 후반부 23bit는 멀티캐스트 MAC 주소 그룹 번호의 하위 bit 내용으로부터 할당된다.
- 또한 멀티캐스트 MAC 주소는 IP 주소를 기반으로 자동적으로 작성된다.
- 한편 브로드캐스트 MAC 주소는 모든 bit가 1로 구성되어 FF-FF-FF-FF-FF-FF로 나타낸다.

IT COOKBOOK

-
- The image shows a Wireshark packet capture window titled "*Wi-Fi". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar with various icons for packet capture and analysis. The packet list pane on the left shows a list of captured packets, with packet 38780 selected. The packet details pane on the right shows the structure of the selected packet, which is an ARP request. The packet bytes pane at the bottom shows the raw data of the packet, with the Ethernet II header highlighted in blue.
- | 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 |
- Packet 38780 details:
- > Frame 38780: 42 bytes on wire (336 bits), 42 bytes captured on interface (336 bits) on Wi-Fi
 - > Ethernet II, Src: D-LinkIn_85:3f:a4 (c4:a8:1d:85:3f:a4), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 - > Address Resolution Protocol (request)
- Packet 38780 bytes:
- ```

0000 ff ff ff ff ff ff c4 a8 1d 85 3f a4 08
0010 08 00 06 04 00 01 c4 a8 1d 85 3f a4 c0
0020 00 00 00 00 00 00 c0 a8 00 64

```

### 3. Ethernet II 덤프 분석

- [Ethernet II] 앞에 있는 [>]를 클릭하면 Ethernet II 프로토콜에 대한 설명이 전개되어 그림과 같이 나타난다.

```
> Frame 38780: 42 bytes on wire (336 bits), 42 bytes captured
 ▾ Ethernet II, Src: D-LinkIn_85:3f:a4 (c4:a8:1d:85:3f:a4), D
 > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 > Source: D-LinkIn_85:3f:a4 (c4:a8:1d:85:3f:a4)
 Type: ARP (0x0806)
 > Address Resolution Protocol (request)
```

- 이때 맨 먼저 [Destination](수신자 MAC 주소) 필드가 나타난다.
- 또한, 이후 [Destination]을 비롯한 패킷 헤더의 각 부분을 [필드]라고 한다.
- [Destination] 필드에는 Ethernet II의 수신자를 나타내는 MAC 주소가 들어간다.
- 여기에는 수신자 MAC 주소가 [Broadcast]로 되어있다.
- Broadcast(브로드캐스트)란 LAN에 접속된 모든 송신자에게 프레임을 보낸다는 의미이다.

### 3. Ethernet II 덤프 분석

- 이 [Destination] 필드를 클릭하여 반전 표시를 하고 패킷 바이트 정보를 확인해 보라.
- 그러면 패킷 바이트 정보에는 [ff ff ff ff ff ff] 부분이 선택된 상태가 되어 있을 것이다.
- 이는 수신자 MAC 주소는 6바이트이며 [Broadcast]의 경우에는 [ff:ff:ff:ff:ff:ff]란 브로드캐스트 주소가 사용되고 있음을 알 수 있다.
- 이어서 패킷 상세 정보의 [Source] 필드를 확인해 보라.
- 이 필드에는 송신자를 나타내는 MAC 주소가 지정되어 있다.
- 나타난 내용을 보면 먼저 앞부분 3바이트는 LAN 카드 제조사명(D-LinkIn)이 있고, 뒷부분 3바이트는 LAN 카드마다 부여된 제조 일련번호가 지정되어 있다.
- 화면에는 이들이 D-LinkIn\_85:3f:a4라고 나타나 있다.
- 그리고 다음으로 실제 MAC 주소를 괄호 안에 16진수 6바이트로 나타나 있다.

### 3. Ethernet II 덤프 분석

- 다음에는 [Type] 필드를 확인해 보자.
- 이 필드는 Ethernet II 헤더 다음에 이어지는 캡슐화 형식을 2바이트로 지정하는 부분이다.
- [Type] 필드는 Ethertype 필드라고도 불리며 Ethernet II 다음에 이어지는 프로토콜을 2바이트로 나타낸다.
- 주요 이더넷 유형 값과 캡슐화되는 프로토콜의 대응 관계는 표와 같다.

| 이더넷 유형 값       | 프로토콜                     |
|----------------|--------------------------|
| 0x0800         | IPv4                     |
| 0x86dd         | IPv6                     |
| 0x0806         | ARP                      |
| 0x089b         | Apple Talk               |
| 0x8137, 0x8138 | Novell IPX               |
| 0x80d5         | IBM SNA Service on Ether |



### 3. Ethernet II 덤프 분석

- 예를 들어 그림에 나타나 있는 38780번째 ARP 패킷(패킷 목록 정보의 [Info] 열에 [Who has ... ]라고 나타나 있는 패킷이다)에는 [0806]이 들어가며 ARP가 지정되어 있다.
- 만약 DNS 패킷([Info] 열에서 [Standard query ...]라고 표시되어 있는 패킷)인 경우에는 [0800]이 들어가며 IPv4가 지정되어 있다.
- 이처럼 이더넷 유형 값을 지정하여 Ethernet II 는 여러 가지 패킷을 캡슐화할 수 있다.
- 이더넷 유형 필드 값과 의미는 인터넷 표준화 조직인 IANA(Internet Assigned Number Authority)에 의해 결정된다.
- 최신 이더넷 유형 할당에 대해서는 URL(<http://www.iana.org/assignments/ethernet-numbers>)을 참고하기 바란다.
- 인터넷에서 사용하는 기술에 대한 표준화 작업은 IETF(Internet Engineering Task Force) 에서 이루지고 있다.

### 3. Ethernet II 덤프 분석

- 다시 화면으로 되돌아가 보자.
- MAC 주소는 OUI(Organizational Unique Identifier)나 헤더마다 ID 외에 특별한 의미를 갖는 비트를 포함하고 있다.
- Ethernet II 헤더의 [Destination] 필드와 [Source] 필드 앞에 있는 [>]를 클릭하면 그림과 같이 나타난다.

```
▼ Ethernet II, Src: D-LinkIn_85:3f:a4 (c4:a8:1d:85:3f:a4)
 ▼ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
 Address: Broadcast (ff:ff:ff:ff:ff:ff)
 ①1. = LG bit: Locally administered address
 ②1 = IG bit: Group address
 ▼ Source: D-LinkIn_85:3f:a4 (c4:a8:1d:85:3f:a4)
 Address: D-LinkIn_85:3f:a4 (c4:a8:1d:85:3f:a4)
 0. = LG bit: Globally unique address
 0 = IG bit: Individual address
 Type: ARP (0x0806)
```

### 3. Ethernet II 덤프 분석

- MAC 주소의 8 번째 비트 ②는 멀티캐스트 또는 유니캐스트를 나타내기 위해 이용된다.
- 8 번째 비트가 "1"(ON) 인 경우 멀티캐스트 통신(또는 브로드캐스트 통신)을 의미한다.
- 멀티캐스트 통신은 하나의 패킷을 한 번에 복수 단말에 송신할 수 있으므로 통신 효율성이 좋고 라우터 간 통신이나 멀티미디어 파일 배포 등에 이용되고 있다.
- 또한 8 번째 비트가 "0"(OFF)인 경우에는 통상적인 유니캐스트 통신을 의미한다.
- 멀티캐스트나 유니캐스트 이외의 통신 방법으로 브로드캐스트가 있다.
- 브로드캐스트를 할 경우 MAC 주소는 48bit가 모두 1 인 [FF-FF-FF-FF-FF-FF]를 주소로 사용한다.
- 브로드캐스트 주소를 수신하거나 중계기 허브와 스위칭 허브인 경우는 접속하고 있는 모든 포트에 패킷을 전송한다.
- 브로드캐스트 통신은 네트워크 상의 기기를 탐색하는 경우와 같이 한꺼번에 모두에게 정보를 보내기 위해 이용되고 있다.

### 3. Ethernet II 덤프 분석

- 또한 MAC 주소의 7 번째 비트 ①은 MAC 주소의 종류를 나타내기 위하여 이용된다.
- 7번째 비트가 “1”(ON)인 경우는 LAN 내에서 네트워크 관리자가 다시 부여한 관리 MAC 주소임을 의미한다.
- 이 경우 원칙적으로 MAC 주소는 변경되지 않는다.
- 또한, 이 비트가 “0”(OFF)이면 MAC 주소가 통상적으로 제조사가 출하 시에 부여된 유일한 주소임을 의미한다.



**Thank You**

---