

1. 패킷의 기본

TCP담당 부분은 접속, 송수신, 연결 끊기의 각 단계에서 통신 상대와 대화할 때 **IP담당 부분**에 의뢰하여 데이터를 패킷의 모습으로 만들어 상대방에게 도착한다.

여기에서는 **의뢰를 받은 IP 담당 부분**이 어떻게 패킷을 상대방에게 송신하는지 살펴본다.

패킷은 '헤더'와 '데이터'의 두 부분으로 구성된다.

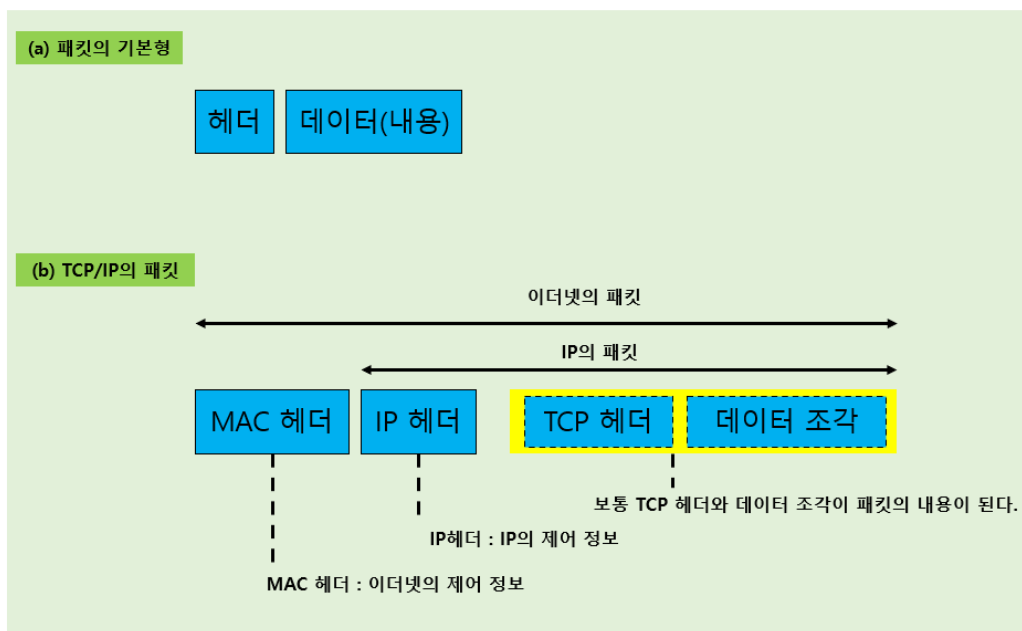


그림 1. 패킷의 모습

헤더에는 수신처를 나타내는 주소 등의 정보가 들어있고, 데이터에는 의뢰처에서 의뢰한 데이터가 담겨 있다.

허브는 이더넷의 규칙에 따라 패킷을 운반하고, 라우터는 IP의 규칙에 따라 패킷을 운반한다.

- ➔ IP가 목적지를 확인하여 다음 IP의 중계장치를 나타낸다.
- ➔ 서브넷 안에 있는 이더넷이 중계 장치까지 패킷을 운반한다.
- 헤더 : MAC헤더(이더넷용), IP헤더(IP용 헤더)

패킷 전송 과정

- ➔ 먼저 송신처에서 패킷의 목적지가 되는 액세스 대상 서버의 IP 주소를 IP헤더의 수신처에 기록한다.
- 패킷의 목적지가 분명해지므로 IP는 이 수신처가 어느 방향으로 있는지 조사하고 그 방향에 있는 다음 라우터를 찾는다.

- 다음 라우터에 패킷이 도착하도록 이더넷에 의뢰할 때 다음 라우터에 할당된 이더넷의 주소(MAC주소)를 조사하고, 그것을 MAC 헤더에 기록한다.
- 이렇게 하여 의뢰 받은 이더넷에게 어느 라우터에 패킷이 도착하면 좋은지를 전달한다.
- ➔ 클라이언트 다음에 놓여있는 허브에서는 패킷의 목적지를 판단하기 위한 표(이더넷용 표)와 같은 것이 있어 이더넷의 헤더의 수신처 정보와 표를 결합하여 패킷의 목적지를 판단하여 중계한다.
 - 허브가 여러 개일 경우 순차적으로 경유하여 패킷이 전달된다.
- ➔ 허브를 통과하면 패킷은 다음 라우터에 도착한다.
 - 라우터에는 IP용 표가 있으므로 이것과 IP헤더의 수신처를 결합하면 다음에 어느 라우터에 패킷을 중계하면 좋을지가 결정된다.
 - 이후 다음 라우터에 패킷을 건네 주기 위해 라우터의 MAC주소를 조사하고 이것을 MAC헤더에 바꾸어 쓰고 다음 라우터에 송신한다.
- ➔ 이와 같은 과정을 반복하여 라우터를 이동하면서 최종으로 서버에 도착하게 된다.

2. 패킷 송수신 동작의 개요

여기에서는 프로토콜 스택의 IP 담당 부분의 패킷 송신 동작에 대해 알아본다.

IP담당 부분은 다음 두개의 헤더를 덧붙인다.

- ➔ MAC 헤더 : 이더넷용 헤더, MAC주소를 쓴다.
- ➔ IP헤더 : IP용 헤더, IP 주소를 쓴다.

이제 만든 패킷을 네트워크용 하드웨어에 건네 준다. 하드웨어는 이더넷이나 무선 LAN등 이다.

- ➔ 이 부분은 PC의 확장 슬롯에 장착해서 사용하는 보드형과 노트북에 사용하는 PC 카드형, PC의 마더보드에 내장된 유형 등 다양하다.
- ➔ 여기에서는 "LAN 어댑터"로 부른다.

LAN어댑터에 건네 줄 때 패킷의 모습은 0 또는 1의 디지털 데이터이고, 이것이 LAN 어댑터에 의해 전기나 빛의 신호로 바뀌어 케이블에 송출된다.

상대에게 패킷이 도착하면 회답을 하는 수신 동작도 송신 동작과 같다.

IP가 패킷을 송 수신하는 동작은 제어 패킷이든지, 데이터 패킷이든지 패킷의 역할에 상관 없이 모두 같다.

3. 수신처 IP 주소를 기록한 IP헤더 만들기

필드의 명칭	길이 (비트)	설명
버전	4	IP 프로토콜의 버전. 현재 사용하는 것은 버전 4입니다.
헤더 길이(IHL)	4	IP 헤더의 길이. 프로토콜 옵션의 유무에 따라 헤더 길이가 달라지므로 헤더 길이를 알도록 하기 위한 것입니다.
서비스 유형 (ToS)	8	패킷을 운반할 때의 우선 순위 등을 나타냅니다. 처음의 사양이 모호했기 때문에 최근에 DiffServ라는 사양으로 이 필드의 사용법을 재정의했습니다.
전체 길이	16	IP 메시지 전체의 길이를 나타냅니다.
ID 정보 (Identification)	16	각 패킷을 식별하는 번호. 보통 패킷의 참조 번호가 여기에 기록됩니다. 단 IP 클라이언트에 따라 분할된 패킷은 모두 값이 같습니다.
플래그	3	이 필드는 3비트인데, 유효한 것은 2비트입니다. 이 중에서 하나로 조각 나누기(fragmentation, 프래그먼테이션)가 가능한지 나타내고, 또 하나로 이 패킷이 조각으로 나는 것인지 나타냅니다.
프래그먼트 오프셋	13	이 패킷에 저장되어 있는 부분이 IP 메시지의 맨 앞부분부터 몇 번째 바이트에 위치하는지를 기록합니다.
생존 기간(TTL)	8	네트워크에 루프를 만들 수 있을 때 패킷이 영구적으로 순환되지 않도록 생존 기간을 지정한 것으로, 라우터를 경유할 때마다 이 값이 1씩 감소하여 0이 되면 패킷이 폐기됩니다.
프로토콜 번호	8	프로토콜의 번호가 기록됩니다. • TCP : 06(16진수 표기) • UDP : 11(16진수 표기) • ICMP : 01(16진수 표기)
헤더 체크섬	16	오류 검사용 데이터로, 현재는 사용하지 않습니다.
송신처 IP 주소	32	이 패킷을 발신한 쪽의 IP 주소
수신처 IP 주소	32	이 패킷을 전달할 상대의 IP 주소
옵션	가변 길이	위의 헤더 필드 이외의 제어 정보를 기록할 때는 헤더에 옵션 필드를 추가하지만 옵션 필드를 사용하는 일은 거의 없습니다.

그림 2. IP헤더의 포맷

(이미지 출처 : “성공과 실패를 결정하는 1%의 네트워크 원리”)

그림 2 여기에서 송신처 IP주소는 컴퓨터에 할당된 IP주소라기보다 클라이언트 PC에 장착된 LAN 어댑터의 주소라고 볼 수 있다. 만약 여러 개의 LAN 어댑터를 장착하면 각 LAN 어댑터에 서로 다른 IP 주소가 할당된다.

정리하면

- ➔ 헤더의 수신처 IP 주소에는 통신 상대의 주소를 설정한다.
- ➔ IP 주소는 송신처가 되는 LAN 어댑터를 판단하여 주소를 설정한다.

4. 이더넷용 MAC 헤더 생성

이더넷은 TCP/IP와 다른 구조로 패킷의 수신처를 판단하며, 이 구조를 따르지 않으면 이더넷 패킷을 운반할 수 없다.

- ➔ IP 담당 부분은 IP헤더를 붙였으면 그 앞에 MAC 헤더를 붙인다. MAC 헤더는 이더넷에서 사용하는 헤더로서 수신처나 송신처의 MAC 주소 등이 기록되어 있다.

MAC 헤더에 기록되는 항목은 수신처 MAC 주소, 송신처 MAC 주소, 이더 타입(Ether Type)이 있다.

- ➔ 수신처 MAC 주소와 송신처 MAC 주소는 각각 패킷을 전달하는 상대와 패킷을 송신한 송신처의 MAC 주소를 나타낸다.
- ➔ IP의 주소와 같은 역할을 하지만 IP주소는 32비트이고 MAC 주소는 48비트이다.

이더 타입이라는 항목은 IP헤더의 프로토콜 번호와 비슷하다.

- ➔ 이더넷의 경우 이더 타입까지가 MAC헤더이고, 그 뒤에 이어지는 것이 패킷의 내용물로 생각된다.

MAC헤더를 만들 때는 위의 3가지 항목에 값을 설정하기만 하면 된다.

- ➔ 이더 타입 : IP프로토콜을 나타내는 0800(16진 표기)라는 값을 설정한다.
- ➔ 송신처 MAC주소 : 자체의 LAN 어댑터의 MAC주소를 설정한다.
 - MAC주소는 LAN어댑터를 제조할 때 그 안에 있는 ROM에 기록되어 있으므로 여기에 기록되어 있는 값을 읽어와 MAC 헤더로 설정한다.
 - 여러 개의 LAN이 있을 경우 판단한 후 설정해야 한다.
- ➔ 수신처 MAC주소 : 여기에는 패킷을 건네 줄 상대의 MAC 주소를 기록해야 한다.
 - 단 누구에게 건네 주어야 할지 모를 시점에서는 상대가 누구인지 조사해야 하는데 이것은 경로표에 기록되어 있다.
 - 경로 표에서 찾은 일치하는 행의 'Gateway'항목에 기록되어 있는 IP주소의 기기가 패킷을 건네 줄 상대가 된다.
 - 여전히 상대의 MAC 주소는 모르기 때문에 IP주소에서 MAC주소를 조사하는 동작을 실행한다.

IP담당 부분은 경로표의 'Gateway'항목의 값에서 패킷을 건네 줄 상대를 판단한다.

5. ARP로 수신처 라우터의 MAC주소 조사

다음 상대를 찾은 후 상대의 MAC주소를 알기 위해 ARP를 사용하게 된다.

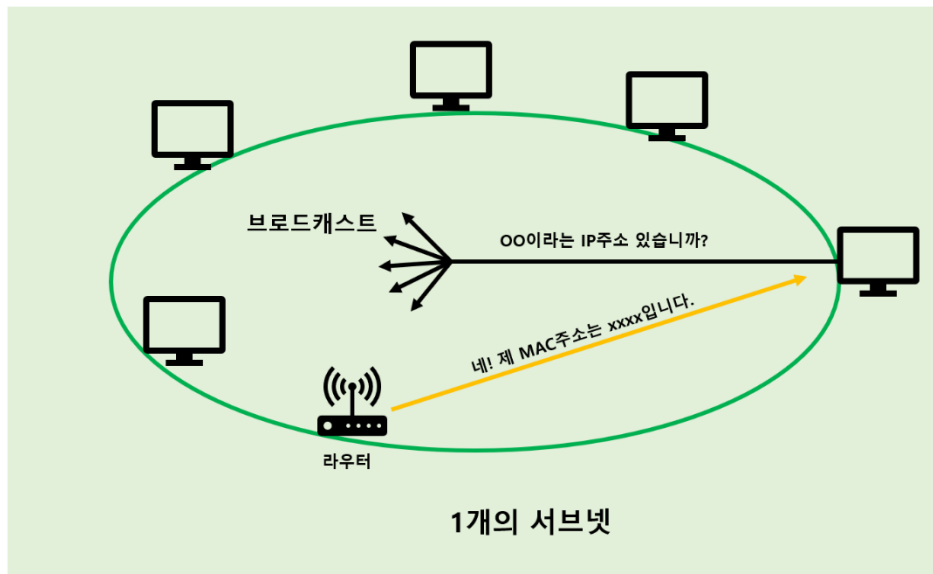


그림 3. ARP로 MAC주소 조사

ARP 개념 :

- ➔ 브로드캐스트를 통해 연결된 노드들에 OO이라는 IP주소를 가진 노드를 찾는다고 질문한다. 해당 IP를 가진 노드가 있을 경우 자신의 MAC주소를 수신한다.
- ➔ 만약 상대가 같은 네트워크에 존재하면 이것으로 MAC주소를 알 수 있고 MAC헤더에 설정하여 만들 수 있다.

패킷을 보낼 때마다 이 동작을 하면 ARP의 패킷이 불어나기 때문에 한번 조사한 결과는 ARP 캐시라는 메모리 영역에 보존하여 다시 이용한다.

ARP캐시를 사용하여 ARP 패킷을 줄일 수 있지만, ARP캐시에 저장된 MAC 주소를 계속 사용할 경우 문제가 발생할 수 있다.

- ➔ IP주소를 설정하여 고쳐진 경우 등 ARP캐시의 내용과 현실 사이에 일치하지 않는 문제가 발생할 수 있기 때문이다.
- ➔ 이를 해결하기 위해 ARP캐시에 저장된 값은 시간이 지나면 삭제하게 되어 있다.
 - 삭제 동작은 ARP 캐시의 내용이 유효한지 여부에 관계 없이 OS에 따라 시간은 다르지만 보통 몇 분 정도 경과하면 무조건 삭제한다.

MAC 주소 표기 방법 : 00-80-C8-2D-82-EA, 00:80:C8:2D:82:EA

6. 이더넷의 기본

IP담당 부분이 패킷을 완성하면 LAN어댑터가 다음 단계를 실행한다.

이더넷 변형 과정

(a) 10BASE5(이더넷의 원형)

➔ 네트워크의 실체는 케이블만 있다. "트랜시버"라는 기기가 있지만 이것은 연결한 케이블 사이에 신호를 흘리는 역할만 하며 케이블과 같다. 그러므로 컴퓨터가 신호를 송신하면 케이블을 통해 네트워크 전체에 신호가 흐르고 전원에게 신호가 도착하게 된다. 이때 누구에게 갈 것인지 나타내기 위해 MAC헤더를 사용하게 된다.

(b) 리피터 허브를 이용한 파생형(10BASE-T)

➔ 기존 방식에서 트렁크 케이블이 리피터허브로 바뀌고, 트랜시버 케이블이 트위스트 페어 케이블로 바뀌었다.

(c) 스위칭 허브를 이용한 형태

➔ 이후에는 스위칭 허브를 사용한 형태가 보급되었고, 현재는 이더넷을 말하면 이 형태를 가리킨다. 기존 방식과 달리 여기에서는 MAC 주소로 나타내는 원하는 기기가 존재하는 부분에만 신호가 흐른다.

이와 같은 변화 과정이 있었지만 MAC 헤더의 수신처 MAC주소에 기억된 상대에게 패킷을 전달하고, 송신처 MAC 주소로 송신처를 나타낸 후 이더 타입으로 패킷의 내용물을 나타낸다는 세 가지 성질은 변하지 않았다.

7. IP패킷을 전기나 빛의 신호로 변환 후 송신

여기에서는 이더넷 패킷의 송수신 동작에 대해 설명한다.

IP가 만든 패킷은 디지털 데이터이므로 그대로 상대에게 보낼 수 없다. 따라서 이것을 전기나 빛의 신호로 변환하여 네트워크 케이블에 송출하는데 이것을 송수신 동작의 본질이라고 할 수 있다.

그리고 이 동작을 실행하는 것이 **LAN 어댑터**이다. 단 LAN 어댑터는 단독으로 동작하는 것이 아니라 LAN드라이버 소프트웨어가 필요하다.

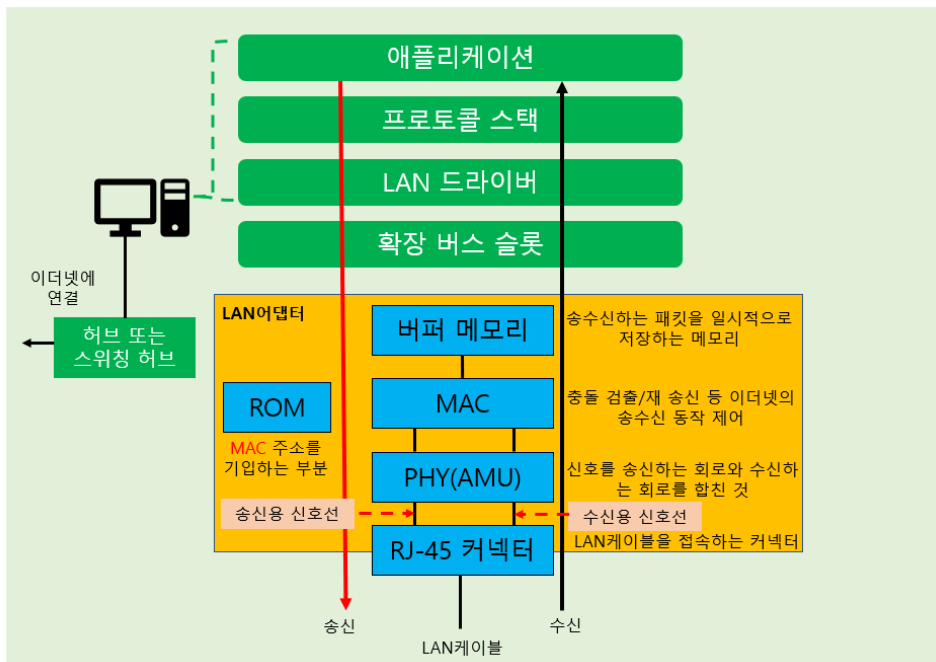


그림 4. LAN 어댑터

LAN어댑터는 전원을 공급하면 즉시 사용할 수 있는 것이 아니라 다른 하드웨어와 마찬가지로 초기화 작업이 필요하다.

LAN어댑터의 ROM에는 전 세계적으로 중복되지 않도록 일원화하여 관리하는 MAC주소를 기록하므로 이것을 읽어 LAN드라이버가 MAC회로에 설정한다.

8. 패킷에 3개의 제어용 데이터 추가

여기서는 패킷을 전기신호로 변환하여 실제로 케이블에 송출하는 부분을 설명한다.

LAN드라이버는 IP 담당 부분에서 패킷을 받으면 그것을 LAN 어댑터의 버퍼 메모리에 복사한다. 복사를 마친 후 패킷을 송신하도록 MAC 회로에 명령을 보내면 MAC 회로의 작업이 시작된다.

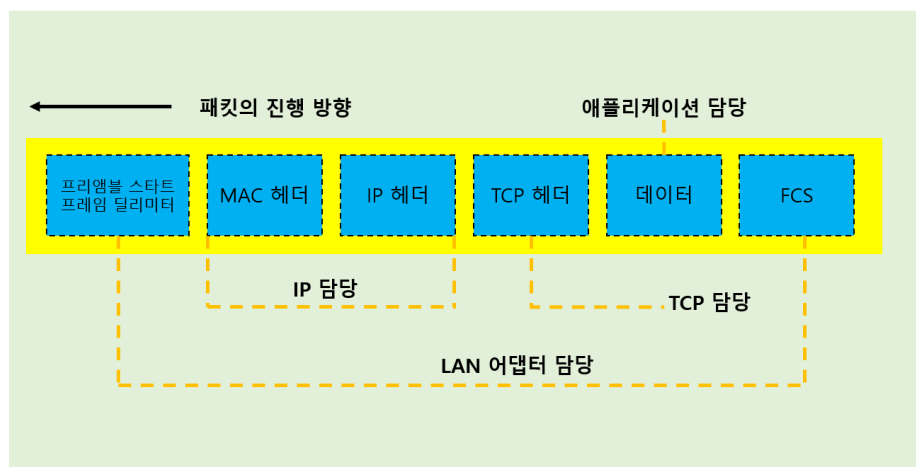


그림 5. LAN어댑터에서 송출하는 패킷

MAC회로는 먼저 송신 패킷을 버퍼 메모리에서 추출하고 맨 앞에는 **프리앰블**과 **스타트 프레임 딜리미터**라는 두개의 데이터를, 맨 끝에는 **프레임 체크 시퀀스**라는 오류 검출용 데이터를 부가한다.

- ➔ **프리앰블** : 송신하는 패킷을 읽을 때의 타이밍을 잡기 위한 것으로, '101010...'과 같은 비트열이 56비트 이어진 것이다. 0과 1은 파형처럼 나타난다.
- ➔ 디지털 데이터를 전기 신호로 나타낼 때에는 0과 1의 비트 값을 전압이나 전류의 값에 대응시킨다.
- ➔ 신호에서 데이터를 읽을 때의 동작은 위의 대응을 반대로 실행한다.
- ➔ 0과 1의 신호변환 과정에 1과 0이 이어져 신호의 변화가 없어질 때 비트 구분을 판단하기 어려운 상황이 발생하며, 이를 해결하기 위해 **클록**이라는 신호를 추가로 사용한다.
- ➔ 하지만 이것도 신호가 길어지면 클록에 오차가 생기기에 **데이터 신호와 클록 신호를 합성**하여 한 개로 전송한다.
- ➔ 이후 클록 신호의 타이밍을 판단해야 하는데 이것을 잡기 위한 특별한 신호를 패킷의앞에 부가하게 되고 이것이 프리앰블의 역할이 된다.
- ➔ **스타트 프레임 딜리미터** : 패킷의 시작을 나타내는 표시
- ➔ **FCS**: 패킷 운반 과정에 잡음 등의 영향으로 파형이 흐트러져 데이터가 변한 경우 이것을 검출하기 위한 용도이다. FCS는 32비트의 비트 열이며 어떠한 계산에 의해 쓰여진다.

9. 허브를 향해 패킷 송신

앞서 프리앰블, 스타트 프레임 딜리미터, FCS의 세가지를 부가하면 케이블에 송출하는 패킷이 완성된다.

여기에서는 신호를 송신하는 동작을 설명하는데 여기에는 **반이중 모드**와 **전이중 모드**가 있다.

- 반이중 모드 (리피터 허브)
 - ➔ 먼저 케이블에 다른 기기가 송신한 신호가 흐르고 있는지 조사하고, 신호가 흐르고 있으면 끝날 때까지 기다린다.
 - 이유는 신호가 흐를 때 송신하면 충돌하기 때문이다.
 - ➔ 이후 신호가 흐르지 않으면 송신동작을 시작하는데 먼저 MAC 회로가 프리앰블의 맨 앞부터 1비트씩 차례로 디지털 데이터를 전기신호로 변환한다.
 - ➔ 이것을 PHY 또는 MAU라는 송수신 신호 부분에 보낸다. 이때 디지털 데이터를 신호로

변환하는 속도가 전송속도이다.

➔ PHY(MAU)회로는 이 신호를 케이블에 송출하는 형식으로 변환하여 송신한다.

정리 : LAN 어댑터의 MAC회로가 공통 형식의 신호를 만들고 PHY회로가 케이블에 송출하는 형식으로 변환하여 케이블에 송신한다.

- 전이중 모드 (스위칭 허브)

➔ 송신과 수신을 동시에 실행하면서 충돌이 일어나지 않는다.

10. 돌아온 패킷 받기

수신동작 순서

➔ 신호의 맨 앞에는 프리앰블이 있어 파형에서 타이밍을 계산하여 스타트 프레임 딜리미터가 나오면 그 다음 비터부터 디지털 데이터로 변환하여 동작을 개시한다.

➔ 이후 송신과 반대로 먼저 PHY회로에서 신호를 공통 형식으로 변환하여 MAC회로에 보내고, MAC회로에서 신호를 맨 앞부터 차례대로 디지털 데이터로 변환하여 버퍼 메모리에 저장한다.

➔ 그리고 패킷의 맨 앞부터 계산식에 적용하여 FCS 값을 계산하고 패킷 끝의 FCS와 비교한다. 정상이 아닐 경우 두개가 일치하고 아닐 경우 오류 패킷으로 간주하고 폐기한다.

➔ FCS를 정상으로 통과하면 MAC헤더의 수신처에 MAC 주소를 조사하여 자신에게 오는 패킷인지 판단한다.

➔ 주소가 맞을 경우 패킷을 받아 버퍼 메모리에 저장한다.

➔ 이렇게 MAC 회로가 할 일이 끝나면 이 사실을 컴퓨터 본체에 통지한다.

■ 이 통지는 **인터럽트**라는 구조를 사용한다.

- 인터럽트 동작 과정

➔ 먼저 LAN어댑터가 확장 서브 슬롯 부분에 있는 인터럽트용 신호선에 신호를 보낸다.

➔ 이 신호 선은 CPU에 연결되어 있으며, 신호가 들어오면 CPU는 실행하던 작업을 일시적으로 보류하고 OS 내부의 인터럽트 처리용 프로그램 쪽으로 전환한다.

➔ 여기에서 LAN드라이버가 호출되어 LAN어댑터를 제어하면서 송수신 동작을 한다.

■ 인터럽트에는 번호가 할당되어 있어 LAN 어댑터를 설치할 때 번호를 하드웨어로 설

정한다.

- 인터럽트 처리용 프로그램 쪽은 하드웨어의 인터럽트 번호에 대응하도록 드라이버 소프트웨어를 등록하게 되어 있다.

11. 서버의 응답 패킷을 IP에서 TCP로 넘기기

여기서는 웹 서버에 패킷이 돌아온 것으로 간주하고 다음 프로토콜 스택의 동작을 추적해 본다.

- 프로토콜 스택 동작

- ➔ 서버에서 반송된 패킷의 타입은 0080이므로 LAN드라이버는 TCP/IP의 프로토콜 스택에 패킷을 건넨다.
- ➔ IP 담당 부분은 IP 헤더 부분부터 조사하여 포맷에 문제가 없는지 확인하고, 수신처 IP를 조사한다.
 - 만약 IP주소가 다를 경우 ICMP라는 메시지를 이용하여 통신 상대방에게 오류 통지를 하게 된다.
- ➔ 이후 패킷이 분할되어 수신되면 하나의 덩어리가 완성될 때까지 받고 확인 한 후 다시 조립하여 TCP 담당 부분에 건네 준다.
- ➔ TCP담당 부분은 IP 헤더에 기록된 수신처 IP 주소와 송신처 IP주소, TCP 헤더에 기록된 수신처 포트 번호 및 송신처 포트 번호의 네 가지 항목을 조사하여 해당하는 소켓을 찾는다.
- ➔ 소켓을 찾으면 통신의 진행 상태가 기록되어 있으므로 상황에 따라 적절한 동작을 실행한다.