컴네 7주차 - ARP 공부 자료

▼ **Table of contents**

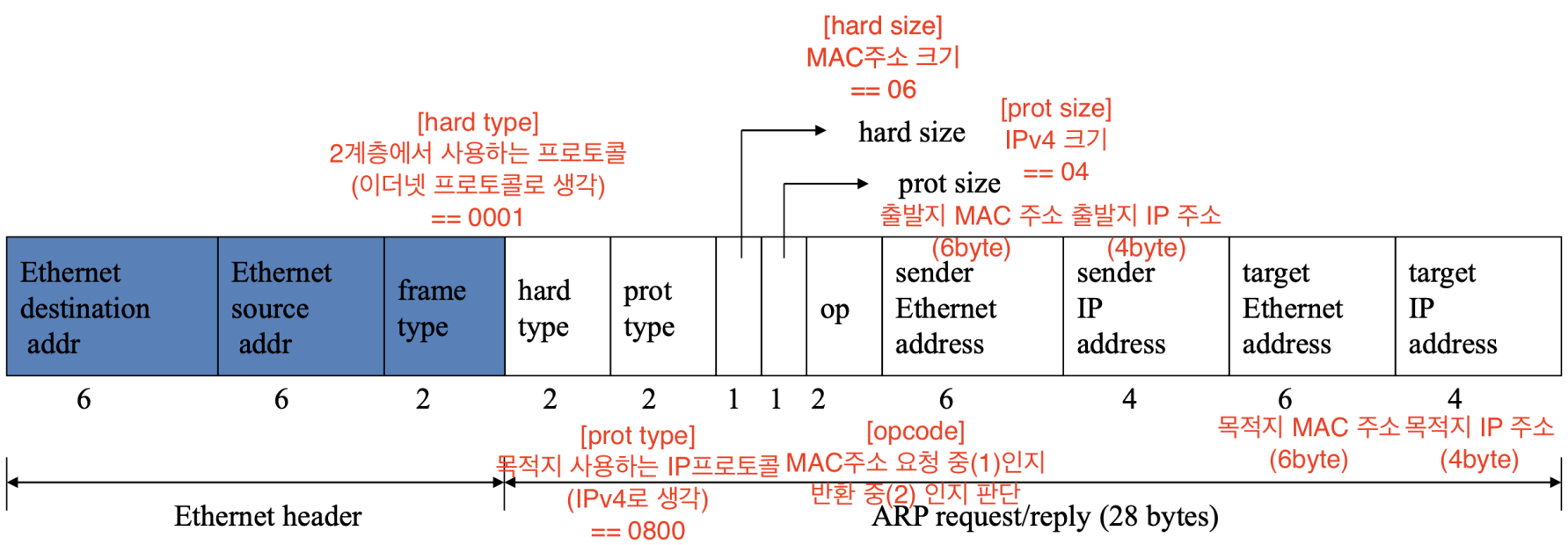
ARP Protocol이란?

ARP 프로토콜은 같은 네트워크 대역에서 통신을 하기 위해 필요한 MAC 주소를 IP 주소를 이용해서 알아오는 프로토콜이다.

같은 네트워크 대역에서 통신을 한다고 하더라도 데이터를 보내기 위해서는 7계층부터 캡슐화를 통해 데이터를 보내기 때문에 IP주소와 MAC 주소가 모두 필요하다. 이때, IP 주소는 알고 MAC 주소는 모르더라도 ARP를 통해 통신이 가능하다.

(평상 시에는 컴퓨터가 자동으로 ARP를 해주기 때문에 IP주소만 알아도 통신할 수 있다.)

ARP 패킷 구조



Ethernet Frame

[Ethernet destination address Field]

Broadcast 주소

[Ethernet source address Field]

출발지의 MAC 주소

[frame type Field]

ARP 요청과 반환 시, 이 값은 0x0806으로 고정

ARP Frame

[hard type Field]

2계층에서 사용하는 프로토콜

이더넷 프로토콜만 있는 건 아니지만 이더넷 프로토콜이라고 생각하면 됨

0001 또는 1로 표기(이더넷 프로토콜일 경우)

[prot type Field]

목적지에서 사용하는 IP 프로토콜 (IPv4로 생각)

0800으로 표기

[hard size Field]

MAC 주소 크기

06 또는 6으로 표기

[prot size Field]

IPv4 크기

04 또는 4로 표기

[op(opertion) Field]

MAC 주소 요청 중 == ARP request(1로 표기)

MAC 주소 반환 중 == ARP reply(2로 표기)

IP 주소 요청 중 == RARP request(3으로 표기)

IP 주소 반환 중 == RARP reply(4로 표기)

[sender Ethernet address Field]

출발지 MAC 주소 (6byte)

[sender IP address Field]

출발지 IP 주소 (4btye)

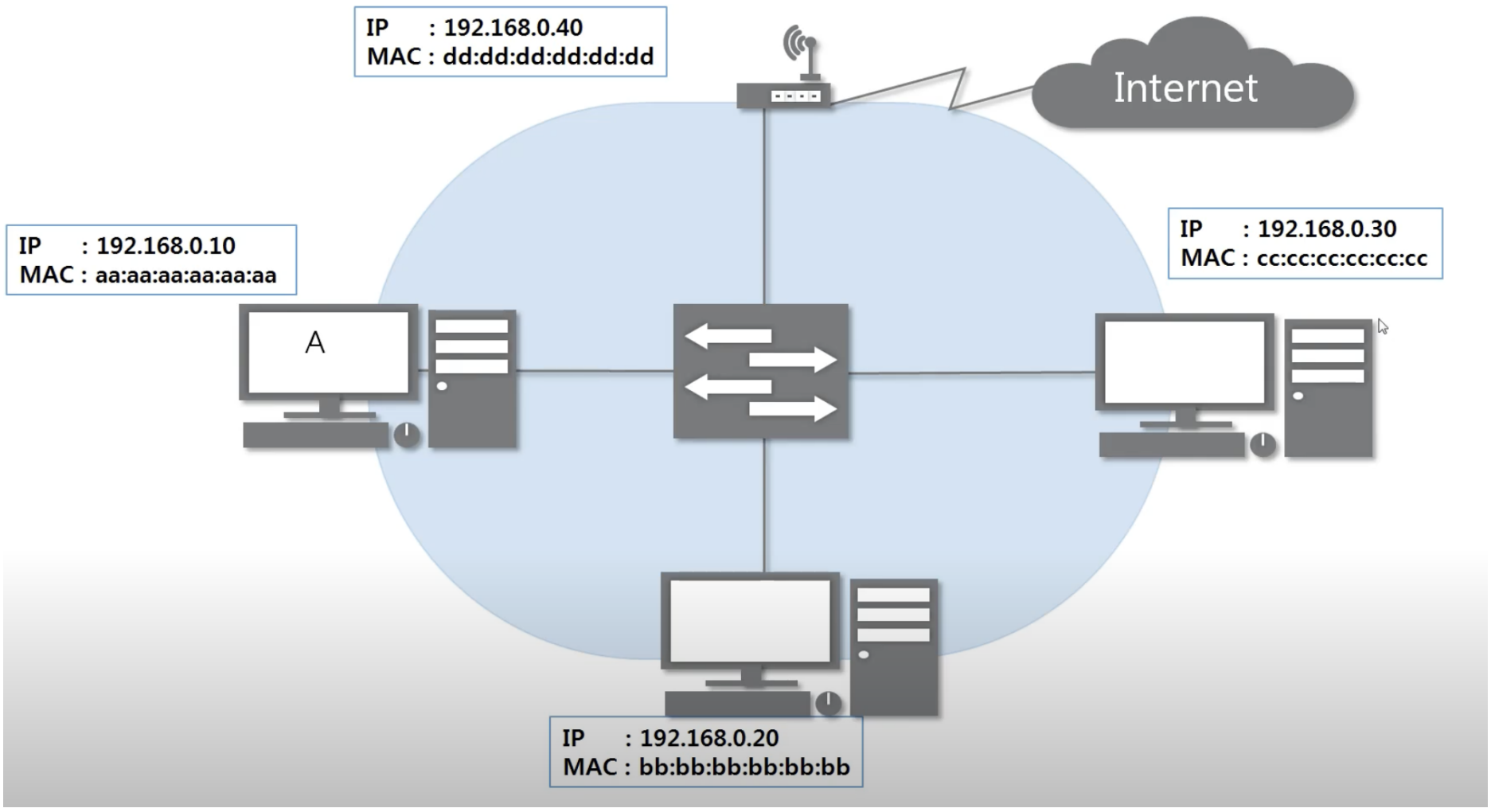
[target Ethernet address Field]

목적지 MAC 주소 (6byte)

[target IP address Field]

목적지 IP 주소 (4byte)

ARP 데이터 flow



같은 LAN 대역(같은 네트워크 대역)에 있는 컴퓨터 A가 컴퓨터 C와 통신하고싶지만 IP주소만 알고있는 상황이라고 가정

1. 컴퓨터 A가 ARP요청 프로토콜을 작성

ARP 요청 패킷에 이더넷 헤더를 붙여서 작성한다.

근데, ARP 패킷에도 목적지 MAC 주소를 써야하고 이더넷 헤더에도 목적지 MAC 주소를 써야하는데 모르지 않나?

먼저 ARP Frame을 살펴보자

[request - ARP Frame]

00	01	08	00
06	04	00	01
aa	aa	aa	aa
aa	aa	c0	a8
00	0a	00	00
00	00	00	00
c0	a8	00	1e

출발지 IP 주소는 16진수로 변환한 것이다.

목적지 MAC 주소는 모르니까 00 00 00 00 00 00 으로 비워둔다.

목적지 IP 주소도 16진수로 변환하여 적는다.

그렇다면 이더넷 헤더는 어떨까?

[request - Ethernet Frame]

FF FF	FF FF
FF FF	aa aa
aa aa aa aa	
08 06	

목적지의 MAC 주소를 모르기때문에 FF FF FF FF FF FF로 작성한다. 이진수로 생각하면 1로 꽉채운 것이다.

== broadcast라는 뜻

이렇게 이더넷 헤더를 broadcast로 지정하면 스위치로 연결된(== 같은 네트워크 대역) 모든 장비에게 프레임 전송

2. 컴퓨터 A가 스위치(L2 장비)한테 프레임 전송
3. 스위치는 L2장비니까 이더넷 헤더만 까서 확인
4. broadcast니까 스위치에 연결된 모든 장비에 프레임 재전송
5. 프레임을 받은 장비들(컴퓨터 C 포함)은 이더넷 헤더를 까고 이더넷 헤더에 적힌 MAC주소를 확인, broadcast임을 확인하고 ARP 프레임을 까봄(L3 장비니까)
6. 각 컴퓨터는 목적지 IP주소를 확인하고 자신의 IP 주소와 다르면 discard, 같으면 출발지 MAC 주소에 자신의 MAC 주소(컴퓨터 C의 MAC 주소)를 넣어서 ARP reply 패킷의 ARP Frame 작성

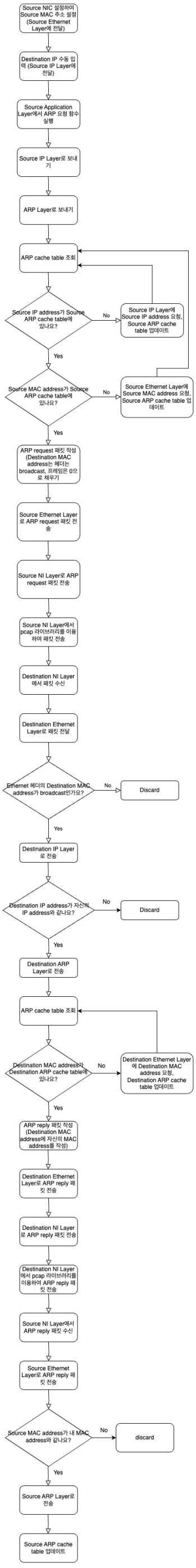
00 01	08 00
06 04	00 02
cc cc cc cc	
cc cc	c0 a8
00 1e	aa aa
aa aa aa aa	
c0 a8 00 0a	

7. ARP reply 패킷의 Ethernet Frame에서도 어디서 온 프레임인지 알기 때문에 도착지 MAC 주소(컴퓨터 A의 MAC 주소)를 잘 쓸 수 있음

aa aa aa aa	
aa aa	cc cc
cc cc cc cc	
08 06	

8. ARP - reply 패킷을 받은 컴퓨터 A는 다 까서 컴퓨터 C의 MAC 주소를 확인하고 자신의 ARP cache table을 갱신

순서도


Source NIC 설정하여 Source MAC 주소 설정 (Source Ethernet Layer에 전달)
Destination IP 수동 입력 (Source IP Layer에 전달)
Source Application Layer에서 ARP 요청 함수 실행
Source IP Layer로 보내기
ARP Layer로 보내기
ARP cache table 조회
Source IP address가 Source ARP cache table에 있나요?
No
Source IP Layer에 Source IP address 요청, Source ARP cache table 업데이트
Yes
Source MAC address가 Source ARP cache table에 있나요?
No
Source Ethernet Layer에 Source MAC address 요청, Source ARP cache table 업데이트
Yes
ARP request 패킷 작성 (Destination MAC address는 헤더는 broadcast, 프레임은 0으로 채우기
Source Ethernet Layer로 ARP request 패킷 전송
Source NI Layer로 ARP request 패킷 전송
Source NI Layer에서 pcap 라이브러리를 이용하여 패킷 전송
Destination NI Layer에서 패킷 수신
Destination Ethernet Layer로 패킷 전달
Ethernet 헤더의 Destination MAC address가 broadcast인가요?
No
Discard
Yes
Destination IP Layer로 전송
Destination IP address가 자신의 IP address와 같나요?
No
Discard
Yes
Destination ARP Layer로 전송
ARP cache table 조회
Destination MAC address가 Destination ARP cache table에 있나요?
No
Destination Ethernet Layer에 Destination MAC address 요청, Destination ARP cache table 업데이트
Yes
ARP reply 패킷 작성 (Destination MAC address에 자신의 MAC address를 작성)
Destination Ethernet Layer로 ARP reply 패킷 전송
Destination NI Layer로 ARP reply 패킷 전송
Destination NI Layer에서 pcap 라이브러리를 이용하여 ARP reply 패킷 전송
Source NI Layer에서 ARP reply 패킷 수신
Source Ethernet Layer로 ARP reply 패킷 전송
Source MAC address가 내 MAC address와 같나요?
No
discard
Yes
Source ARP Layer로 전송
Source ARP cache table 업데이트

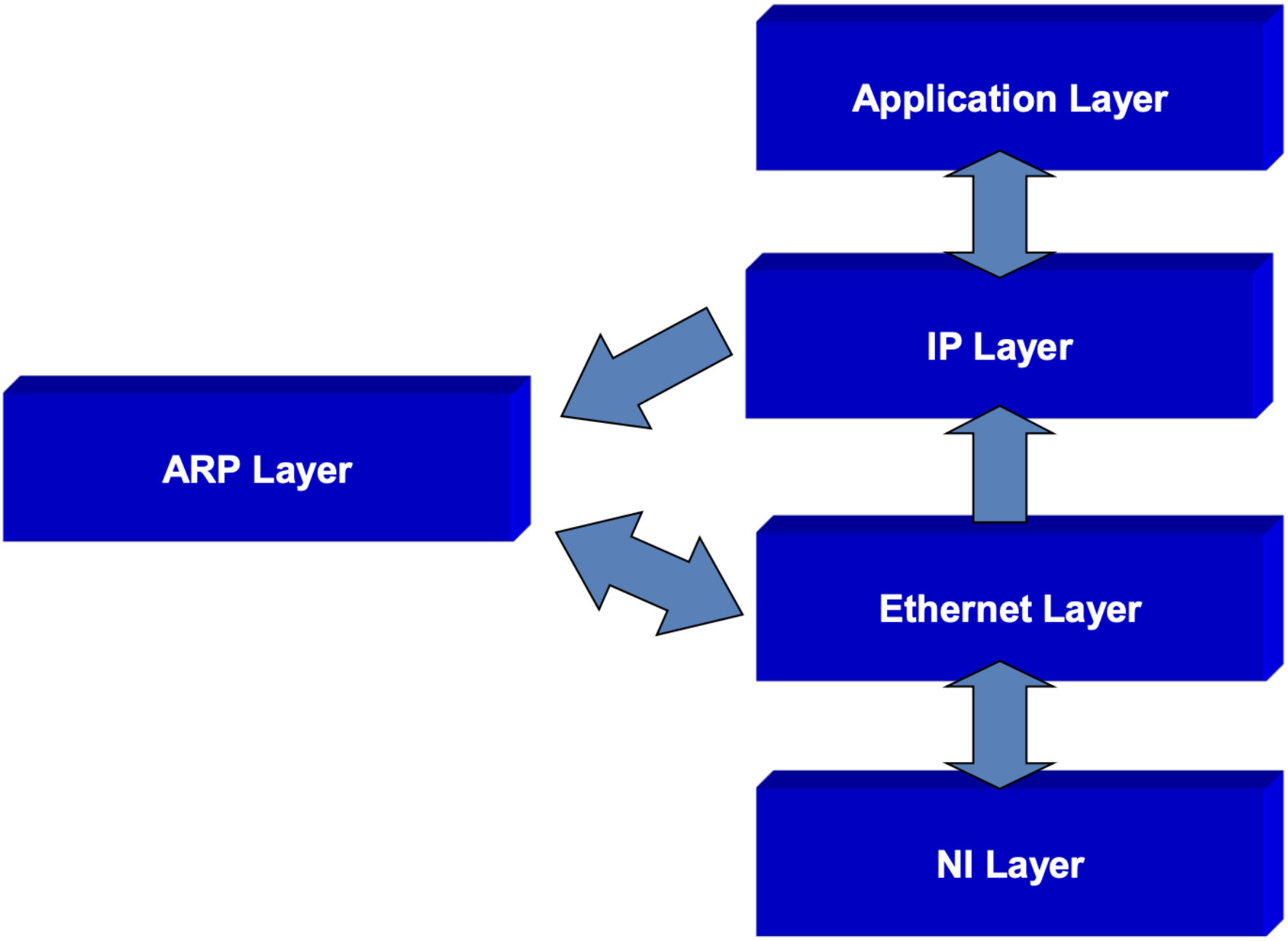
ARP cache table이란?

나(내 컴퓨터)와 통신했던 컴퓨터들의 MAC 주소와 IP 주소들을 하나씩 맵핑 시켜놓은 것

하지만, cache table이기에 일정 시간이 지나면 사라진다. 사라지고 나서 다시 그 컴퓨터와 통신하려면 ARP를 통해 cache table을 채워넣고 통신한다. (수동으로 등록해서 영구적으로 사용하는 방법도 있음)

complete는 20분마다 incomplete는 3분마다 삭제

ARP 레이어 분석



레이어 별 구현 함수

Dlg

1. ARP 요청 함수
2. Source IP 주소를 받아서 IP Layer에 넣어주는 함수
3. 타이머 start 함수
4. status를 incomplete로 만드는 함수

IP Layer

Source IP address 저장 변수

Destination IP address 저장 변수

1. Source IP address 조회 함수
2. 하위 레이어(Ethernet Layer)에서 payload를 받는 함수
    - Destination IP 주소가 자신의 IP address와 같은지 확인
        - 아니면 discard
        - 맞으면 ARP Layer로 payload 전송

ARP Layer

1. ARP cache table 조회 함수(Source일 때 사용)

- Source IP address가 있는 지
    - 없다면 IP Layer에 Source IP address 요청해서 ARP cache table 업데이트
- Source MAC address가 있는 지
    - 없다면 Ethernet Layer에 Source MAC address 요청해서 ARP cache table 업데이트

2. ARP request 패킷 작성 함수
3. Ethernet Layer로 ARP 패킷(request, reply) 전송
4. IP Layer에서 payload 받는 함수
5. ARP cache table 조회 함수(Destination일 때 사용)
    - Destination MAC 주소가 ARP cache table에 있는 지
        - 없다면 Ethernet Layer에 Destination MAC address 요청(MAC 주소 추철 함수 그대로 사용), ARP cache table 업데이트
        - 있다면 ARP reply 패킷 작성
6. ARP reply 패킷 작성 함수
7. Ethernet Layer에서 payload 받는 함수
    - ARP cache table에 Destination MAC 주소 업데이트
    - Dlg에 업데이트하는 함수
    - 타이머 stop 함수
    - status를 complete로 바꾸는 함수

Ethernet Layer

1. MAC 주소 추출 함수 (pcap쓰나?)
2. 상위 레이어(ARP Layer)에서 패킷 받는 함수
3. NI Layer로 패킷 전송 함수
4. 하위 레이어(NI Layer)에서 패킷 받는 함수

- 이더넷 헤더를 까서 MAC 주소가 broadcast 또는 내 MAC 주소와 같은 지 확인
    - 아니면 discard
    - broadcast면 상위 레이어(IP Layer)로 payload(헤더 떼고)전송
    - 내 MAC 주소면 상위 레이어(ARP Layer)로 payload(헤더 떼고) 전송

NI Layer

pcap 라이브러리를 이용하여 패킷 전송

패킷 수신 함수

상위 레이어(Ethernet Layer)에 패킷 전송 함수