

네트워크

(3)

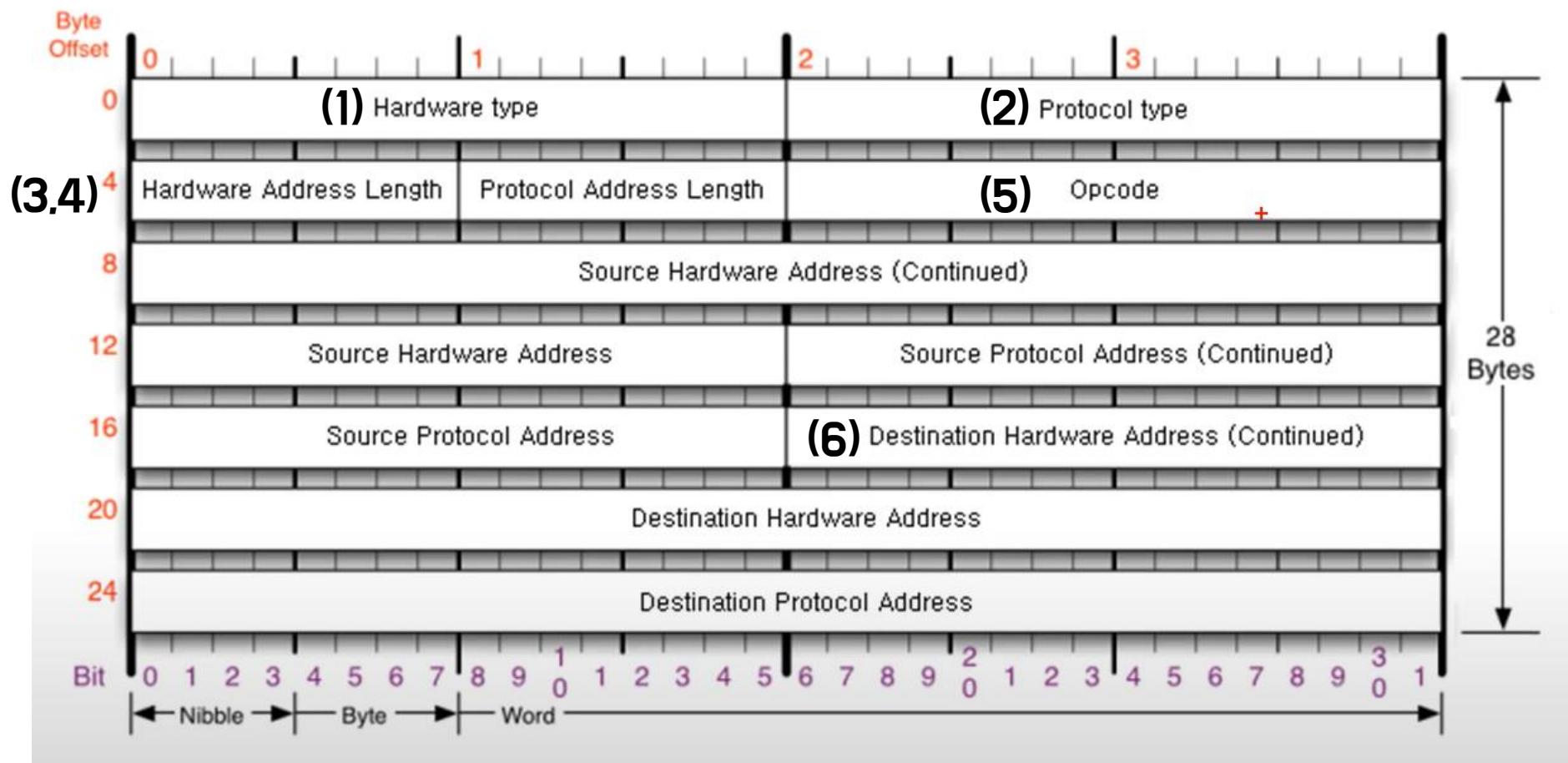


ARP 프로토콜?

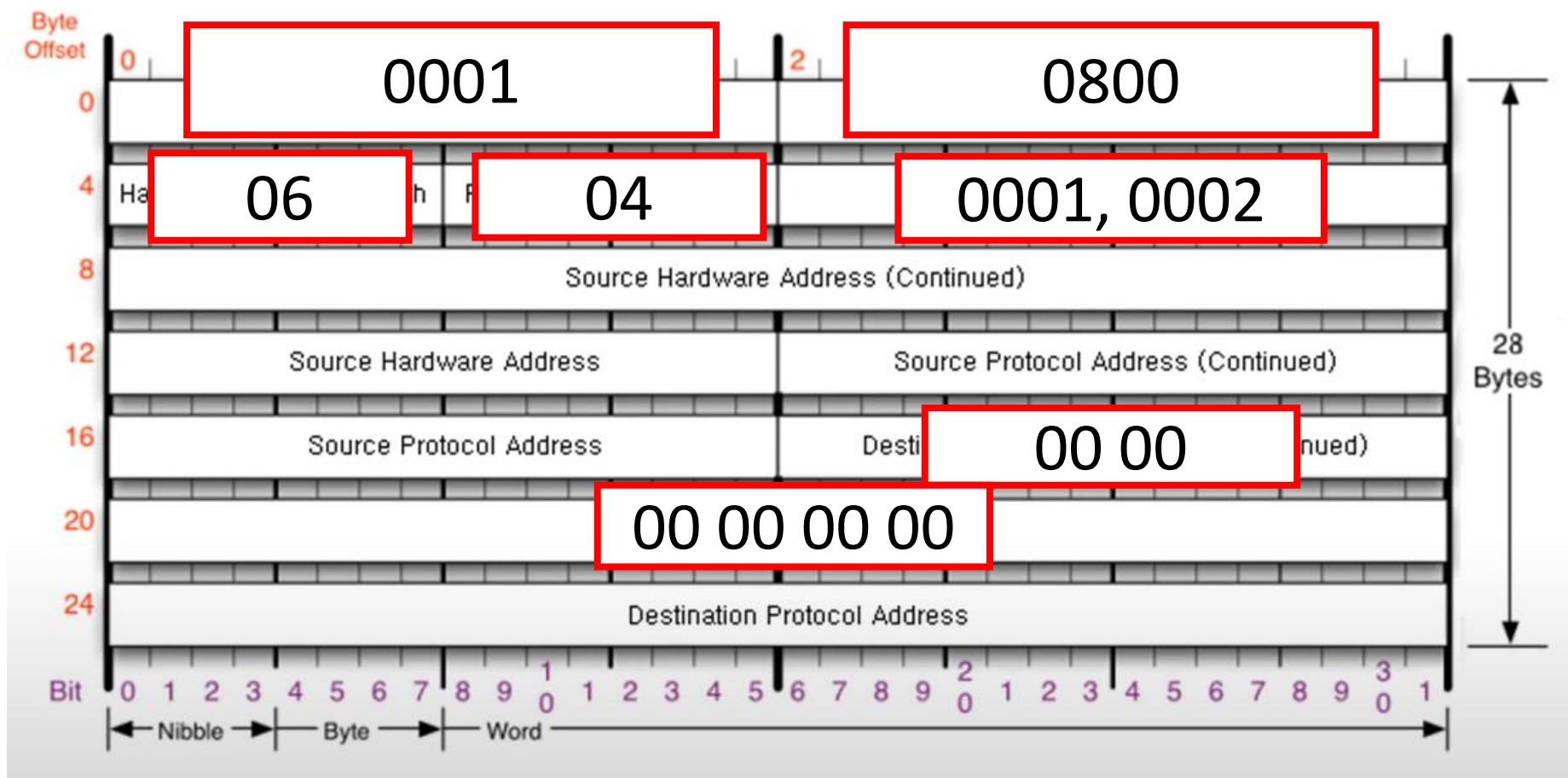
IP주소를 알지만
MAC주소를 모를 때 사용

28Bytes 형태로 이더넷 프로토콜보다
조금 더 복잡하다

기본적으로 브로드캐스트 형태의 통신
(같은 네트워크 대역의)



- 1) Hardware Type: 2계층 프로토콜 타입
- 2) Protocol Type: 현재 프로토콜 타입
- 3) Hardware Address Length: MAC주소 길이
- 4) Protocol Address Length: IPv4주소 길이
- 5) Opcode: 요청 시 (0001)로 응답 시 (0002)로
- 6) 목적지의 MAC주소는 모르기 때문에 비워서 요청
(이더넷 프로토콜에서 1로 채워 브로드캐스트 통신)



이더넷 프로토콜 (브로드캐스트)

- 각 통신 장비에서 ARP 프로토콜 디캡슐화 후
- IPv4주소 확인 (다른 IP주소면 요청 무시)
- 해당하는 IP주소의 장비는 본인의 MAC주소로

ARP 응답 프로토콜 전송

- ARP 캐시 테이블에 기록

```

C:\Windows\system32\cmd.exe
C:\#>arp -a

인터페이스: 192.168.0.189 --- 0xc
인터넷 주소      물리적 주소
192.168.0.1      90-9f-33-df-14-e8
192.168.0.4      e8-03-9a-68-98-21
192.168.0.7      e8-11-32-34-7a-9f
192.168.0.8      e8-11-32-33-01-b5
192.168.0.11     e8-11-32-34-d4-58
192.168.0.12     e8-11-32-34-5f-ad
192.168.0.15     e8-11-32-34-60-a9
192.168.0.16     e8-03-9a-65-da-c1
192.168.0.17     e8-11-32-34-61-7e
192.168.0.18     14-c2-13-e7-34-14
  
```

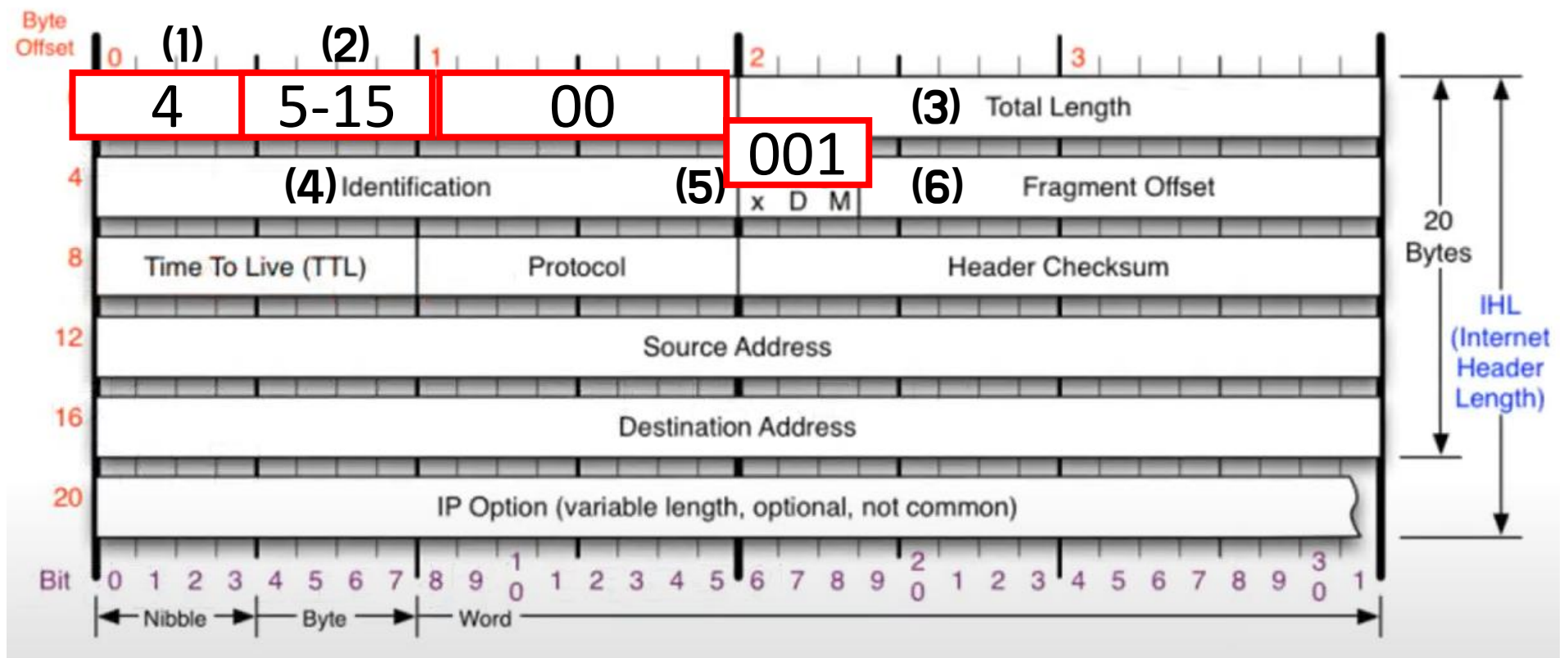
IPv4프로토콜?

**다른 네트워크끼리의
통신 프로토콜**

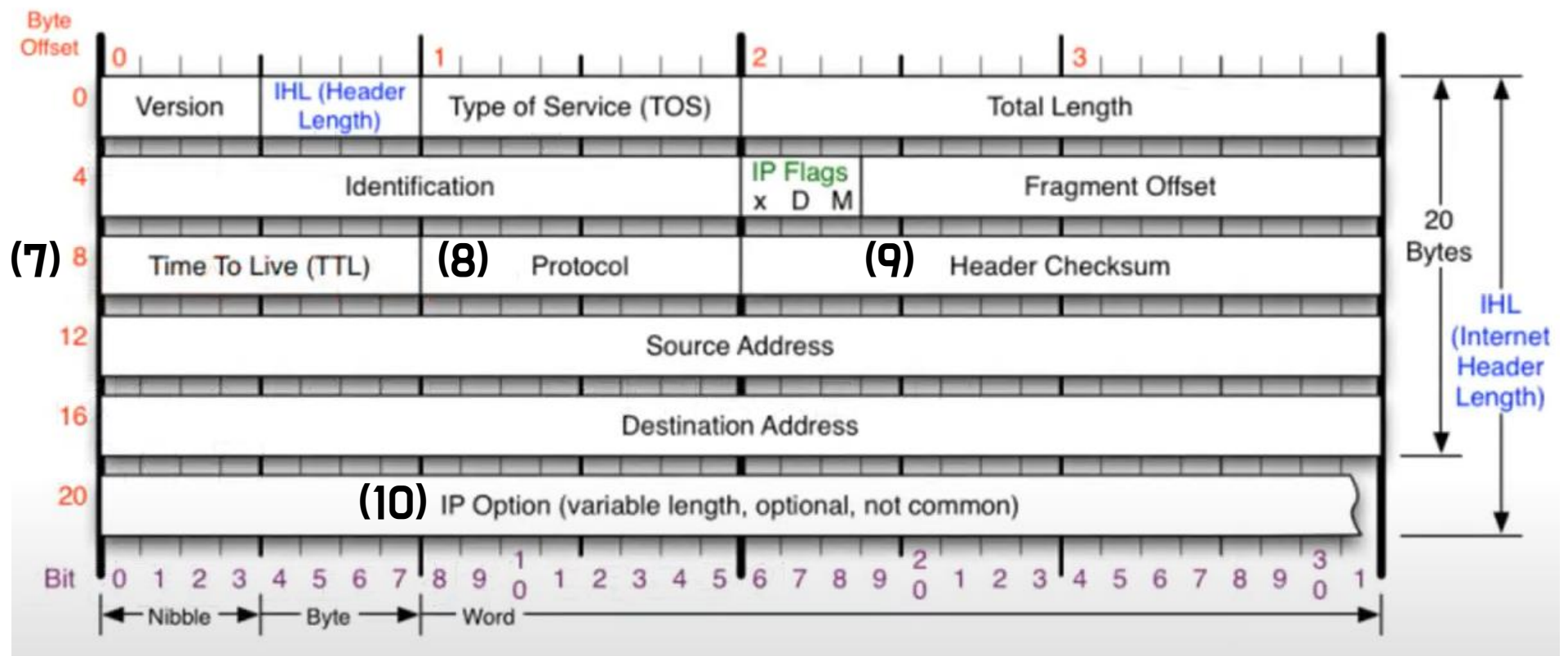
데이터가 정확하게 전달될 것을 보장 X

데이터의 신뢰성은 4계층 (TCP/UDP)

악의적으로 사용하면 DDOS 공격 가능



- 1) Version: 프로토콜의 버전
- 2) IHL: IP헤더의 길이 (총 Bytes에 4로 나눠서 표현)
- 3) Total Length: Payload까지 합쳐진 전체 길이
- 4) Identification: 패킷이 조각났을 때의 ID값
- 5) IP Flags: 패킷을 조각할지 말지 결정하는 값 (D/M)
- 6) Fragment Offset: 조각 패킷의 위치를 알려줌
(패킷이 처음 시작하는 위치로부터 얼마나 떨어져 있는 지)



7) Time To Live: Loop 네트워크에 들어가는 경우를 대비
(통신 장비를 통과할 때마다 -1 → 0에 따라서 128(W), 64(L)로 설정)

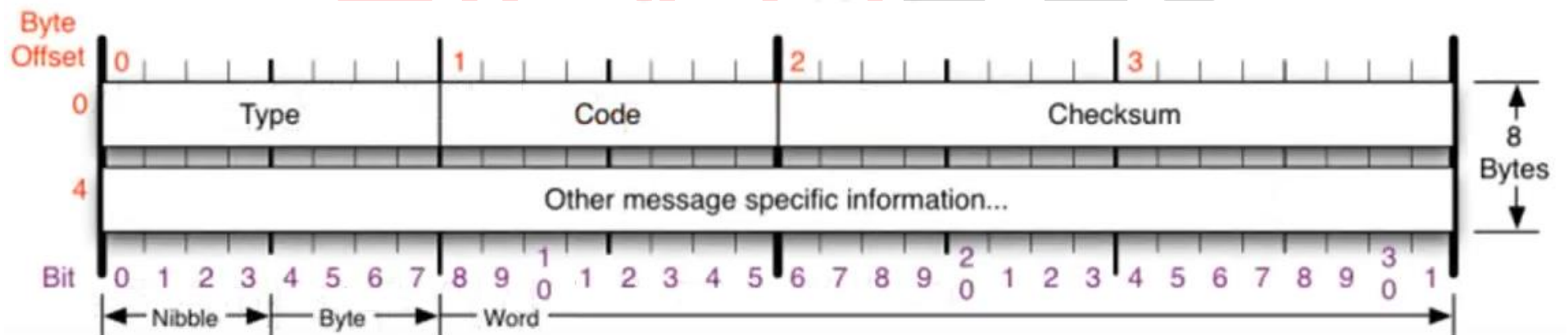
8) Protocol: 상위 프로토콜의 정보를 줌
(ex/ ICMP[1], TCP[6], UDP[17])

9) Header Checksum: 오류 체크 필드

10) IP Option: 통신에 Option추가 (4 Bytes씩 증가)
(→ 최대 10개까지 가능하기 때문에 IPv4프로토콜은 60 Bytes까지 가능)

ICMP 프로토콜?

메시지 프로토콜로
오류 메시지를 전송



〈ICMP Message Types〉

0: Echo Reply → 응답

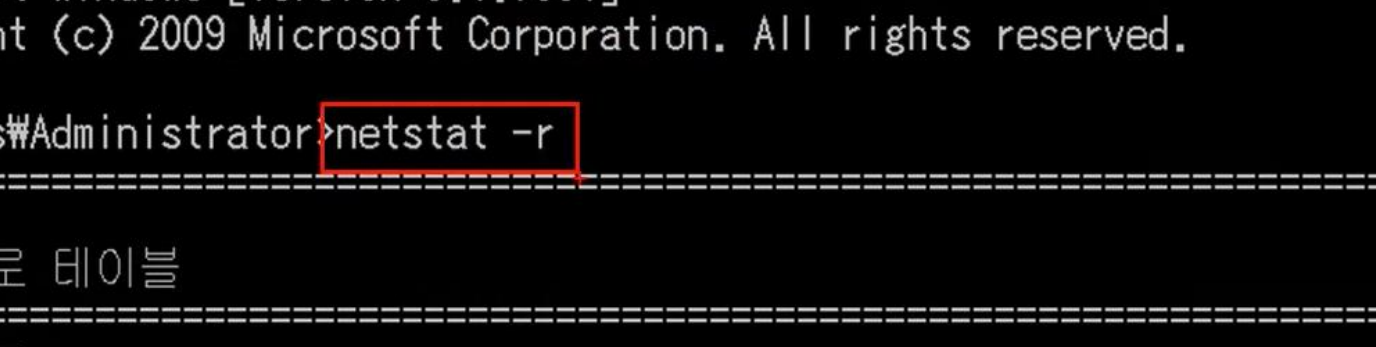
3: Destination Unreachable → 요청이 목적지에 도달하지 못함

5: Redirect → 상대방의 라우터 테이블의 수정 (보안 관련)

8: Echo → 요청

11: Time Exceded → 목적지에 도달 했지만 응답이 없음 (방화벽)

라우팅 테이블?



```
관리자: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

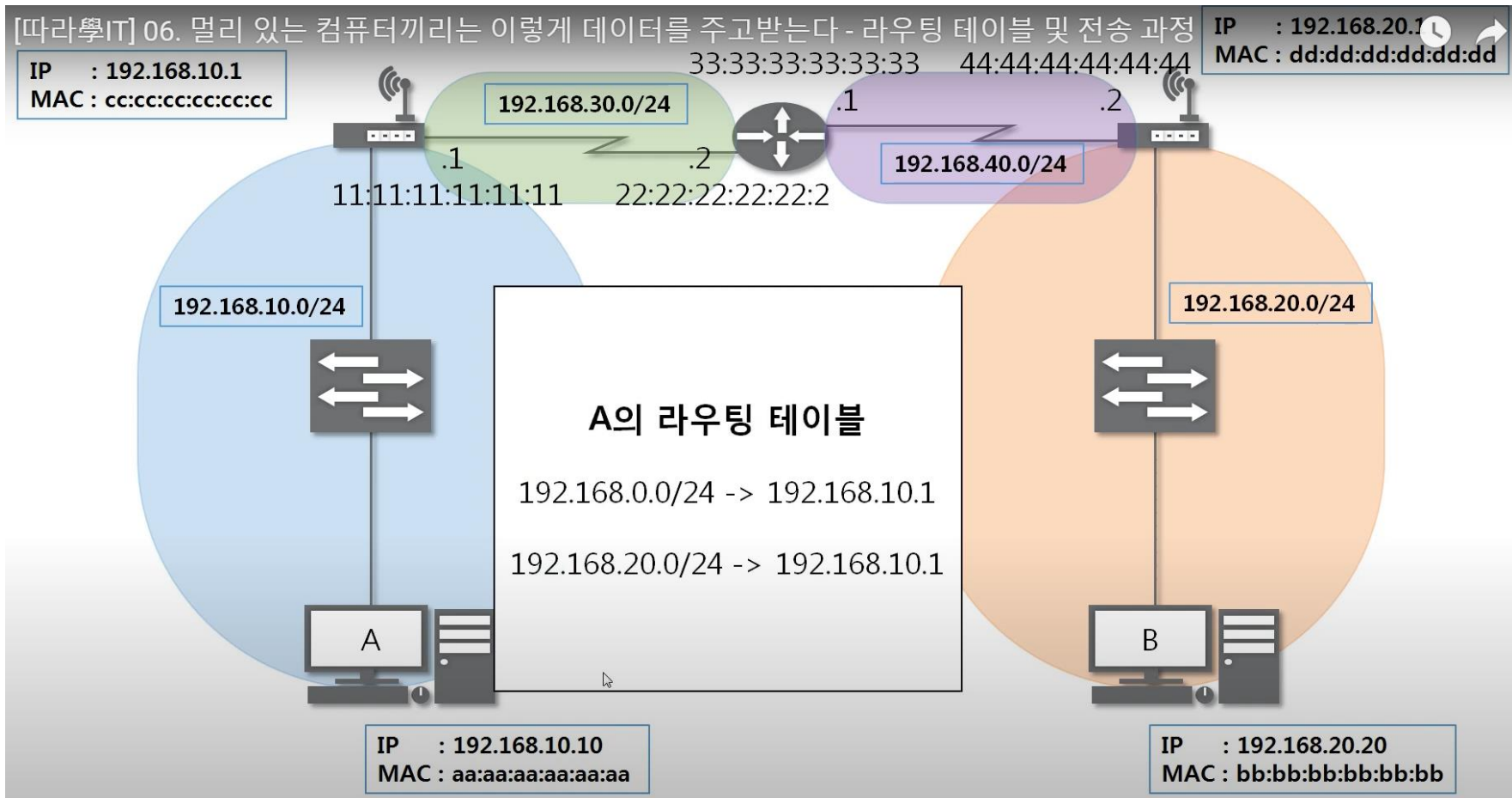
C:\Users\Administrator>netstat -r

=====

IPv4 경로 테이블
=====

활성 경로:
네트워크 대상      네트워크 마스크      게이트웨이      인터페이스      메트릭
0.0.0.0            0.0.0.0            192.168.0.1      192.168.0.189      276
127.0.0.0          255.0.0.0          연결됨           127.0.0.1          306
127.0.0.1          255.255.255.255    연결됨           127.0.0.1          306
127.255.255.255    255.255.255.255    연결됨           127.0.0.1          306
192.168.0.0        255.255.255.0      연결됨           192.168.0.189      276
192.168.0.189      255.255.255.255    연결됨           192.168.0.189      276
192.168.0.255      255.255.255.255    연결됨           192.168.0.189      276
192.168.199.0      255.255.255.0      연결됨           192.168.199.1      276
```

- 통신을 보내야하는 위치를 알려주는 테이블 (캐시 테이블과 비슷하다)
- 통신을 하기 전에 라우팅 테이블을 확인하고 목적지로 통신을 보냄
- 라우팅 테이블에 없다면 ARP를 이용하여 MAC주소를 알아낸다



A에서 테이블에 맞는 목적지로 통신

→ IPv4를 확인 후 (일치 X)

→ 이더넷 프로토콜을 수정하고

→ 다시 테이블에 맞는 목적지로 통신

→ 반복

→ ICMP응답 작성 후, 위 반복

→ 테이블에 없으면 ARP도 시도

공유기의 라우팅 테이블

192.168.10.0/24 -> 192.168.10.1

192.168.20.0/24 -> 192.168.30.2

라우터의 라우팅 테이블

192.168.30.0/24 -> 192.168.30.1

192.168.20.0/24 -> 192.168.40.2

192.168.40.0/24 -> 192.168.40.2