OSI 7 Layer 각 계층별 기능

- **Layer 1 : Physical Layer**
  - 시스템 간의 물리적 링크를 동작시키거나 유지
  - 전기, 기계, 절차, 기능적 측면을 정의

- **Layer 2 : Data-Link Layer**
  - 물리적인 연결을 통하여 두 장치간의 신뢰성 있는 전송을 보장
  - 물리적인 주소를 지정 **(MAC Address)**
  - 회선 사용 규칙, 오류검출, **Frame** 전달, 흐름제어

- **Layer 3 : Network Layer**
  - 다른 장소에 위치한 두 시스템 간의 연결성과 경로 선택을 제공
  - 라우팅 프로토콜을 사용하여 최적 경로를 선택 후 선택된 경로를 통해 정보를 전달
  - 장비를 구분하기 위한 논리적 주소를 사용 **(IP Address)**

OSI 7 Layer 각 계층별 기능

- **Layer 4 : Transport Layer**
  - 데이터 전송 서비스를 제공
  - 통신에 참가하는 개체(Application)간의 메시지 전달 책임
  - 데이터 흐름제어, 에러 복구, 신뢰성 보장

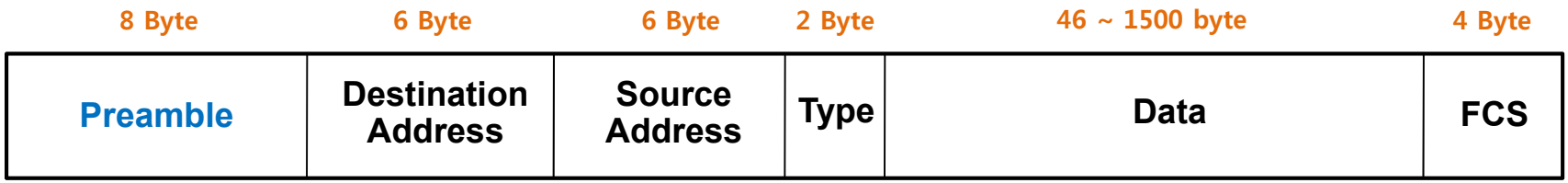
- **Layer 5 : Session Layer**
  - 세션 설정, 유지, 종료, 전송방향 변경

- **Layer 6 : Presentation Layer**
  - 전송 데이터 형태(format)를 결정

- **Layer 7 : Application Layer**
  - 사용자의 접근을 제공 or 서비스를 지칭
  - 파일전송, DB, 원격 접속, 전자메일 등

Ethernet Frame (Layer 2)

▪ Ethernet II Frame (DIX II)

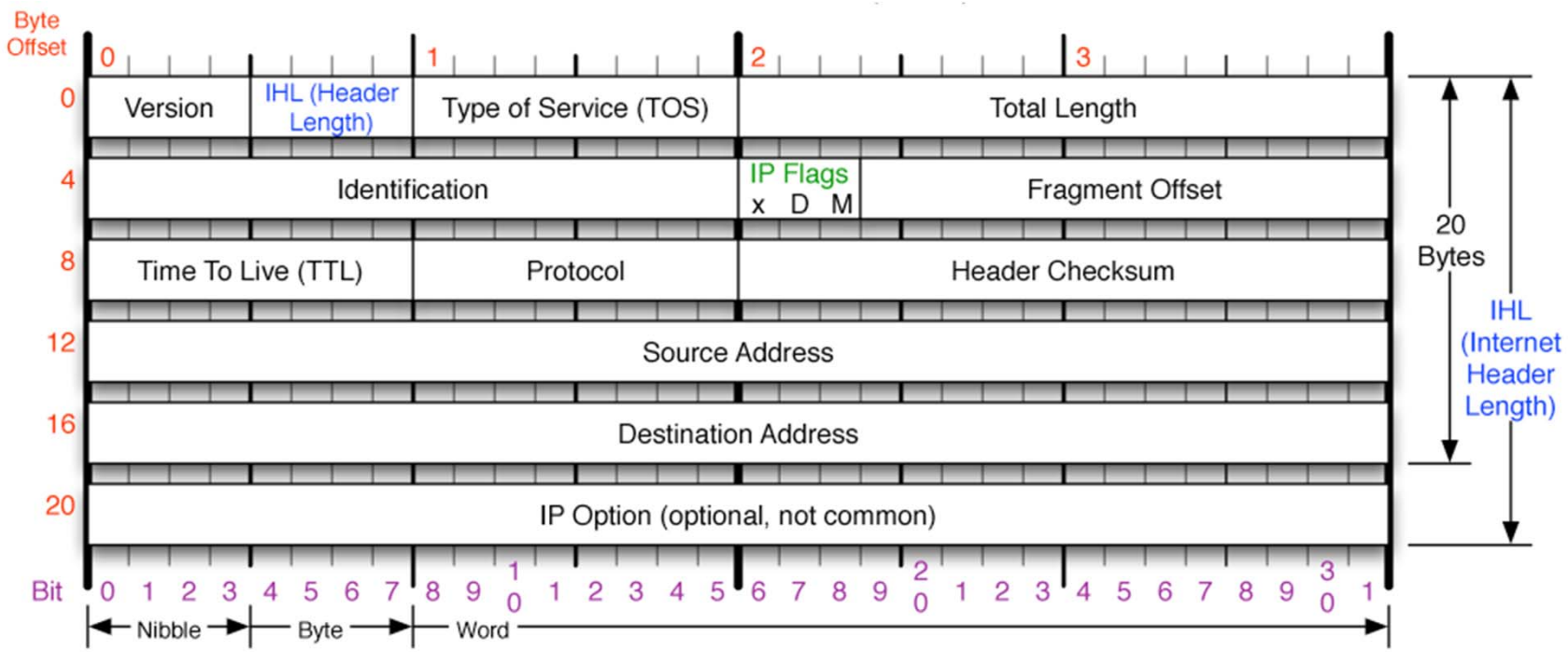


- **Preamble** : 송신측과 수신측의 bit 동기화 및 Frame의 시작을 알림
  - 상위 7byte : 비트 동기화를 위해 10101010....10으로 된 bit열을 전달
  - 하위 1byte : Frame의 시작을 알리는 10101011을 전달
- **Destination Address** : 목적지의 2계층 주소를 표시 (MAC Address)
- **Source Address** : 출발지의 2계층 주소를 표시 (MAC Address)
- **Type** : MAC Frame의 데이터 부분에 실려있는 상위 계층 프로토콜 종류를 표시
- **Data** : 상위 계층으로부터 받은 데이터 or 상위 계층에 전달해야 할 데이터
- **FCS** : Preamble과 FCS를 제외한 유요한 MAC Frame의 bit열에서 오류를 검사

Internet Protocol

- **Internet Protocol (IP)**
  - **OSI 7 Layer**의 **3**계층에 해당하는 프로토콜
  - **TCP/IP**에서 전송을 담당하는 프로토콜
  - 신뢰성이 없고 비 연결 지향적이다
  - **IP**주소에 따라 네트워크간 전송 경로를 제어한다
  - **IP**의 **Version**은 **IPv4**와 **IPv6**가 존재
  - **Router**
    - 네트워크 프로토콜의 주소에 따라 네트워크간 전송 경로를 제어한다.
    - 라우팅 알고리즘에 의해 최적의 경로를 배정함.
    - **Broadcast Domain**을 분리시킨다.

IP Header (Layer 3)



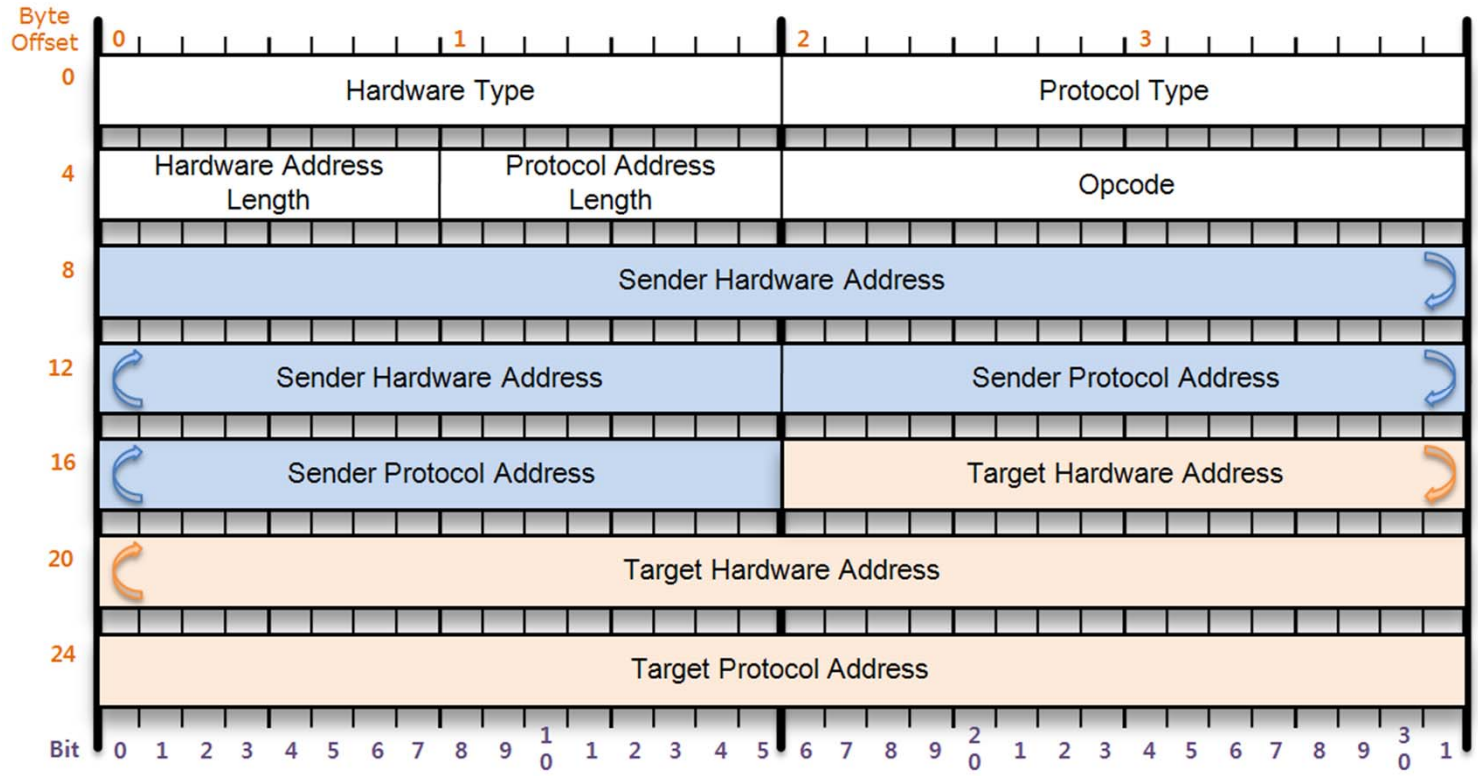
IP Header Field

- Version : IP Protocol Version 정보(IPv4, IPv6)
- IHL(Internet Header Length) : IP Header의 길이를 32bit단위로 표시
- TOS(Type of Service) : Internet의 Application, Host, Router의 우선순위 서비스를 제공
- Total Length : IP Packet의 전체 길이를 바이트 단위로 표시
- Identification : IP Packet을 구분하기 위한 번호. IP Packet이 Fragmentation되었을 경우 목적지에서 결합을 위해 사용한다
- IP Flags : IP Packet의 Fragmentation 정보를 표시
- Fragmentation Offset : Fragmentation되어진 IP Packet의 시작 위치를 표시
- TTL(Time-to-Live) : IP Packet이 이동할 수 있는 최대 라우터의 개수
- Protocol : IP Data에 포함되어 있는 Next-Header를 표시
- Source IP Address : IP Packet을 전달한 출발지 시스템의 IP 주소
- Destination IP Address : IP Packet을 수신할 목적지 시스템의 IP주소
- Option : 특별한 처리 옵션을 정의
- Padding : Option이 추가되는 경우 32bit단위로 끝날 수 있도록 추가되는 부분

ARP (Address Resolution Protocol)

- **Address Resolution Protocol**
  - IP 주소 변환 표준 프로토콜
  - IP 장비가 통신을 하기 위해서는 해당 망에 특화된 2계층 주소를 먼저 알아와야 한다
  - IP장비가 통신하는 경우 해당 네트워크에서 정의된 2계층 주소를 알아오기 위한 프로토콜
    - Ethernet 망에서는 2계층 주소로 MAC Address를 사용
  - ARP는 Request(요청), Reply(응답)으로 구성

ARP Header (Layer 3)



ARP Header Field

- **Hardware Type** : 요청된 하드웨어 주소의 종류
- **Protocol** : 다루고 있는 상위계층 Protocol 정보
- **Hardware Address Length** : 물리매체의 하드웨어 주소의 크기를 byte단위로 표시
- **Protocol Address Length** : 상위 계층의 프로토콜 주소의 크기를 byte단위로 표시
- **Operation** : ARP packet의 목적을 표시(Request, Reply)
- **Sender Hardware Address** : ARP packet을 전송하는 시스템의 하드웨어 주소
- **Sender Internet Address** : ARP packet을 전송하는 시스템의 상위계층 프로토콜 주소
- **Target Hardware Address** : ARP packet을 수신하는 시스템의 하드웨어 주소
- **Target Internet Address** : ARP Packet을 수신하는 시스템의 상위계층 프로토콜 주소

ARP의 동작방식

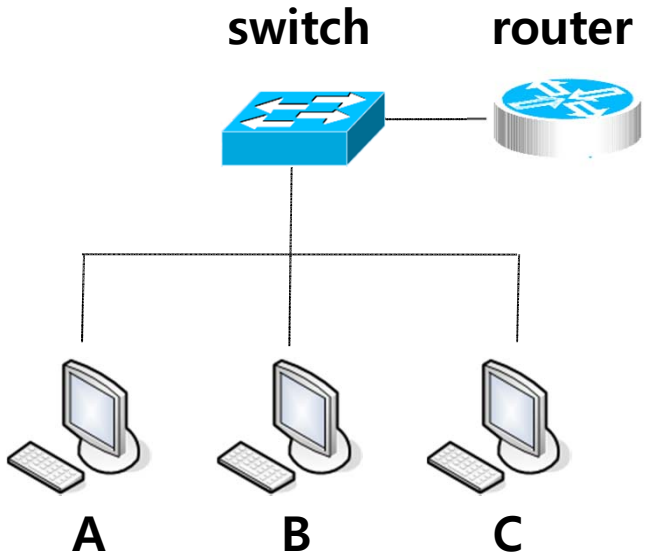
❖ARP는 Request와 Response로 이루어져있다.

A 컴퓨터가 C로 데이터를 전송하는 경우

1. **A는 IP(C)를 누가 사용하고 있는지 ARP Request를 Broadcasting한다.**

2. **C는 ARP Reply를 A에게 보낸다.**

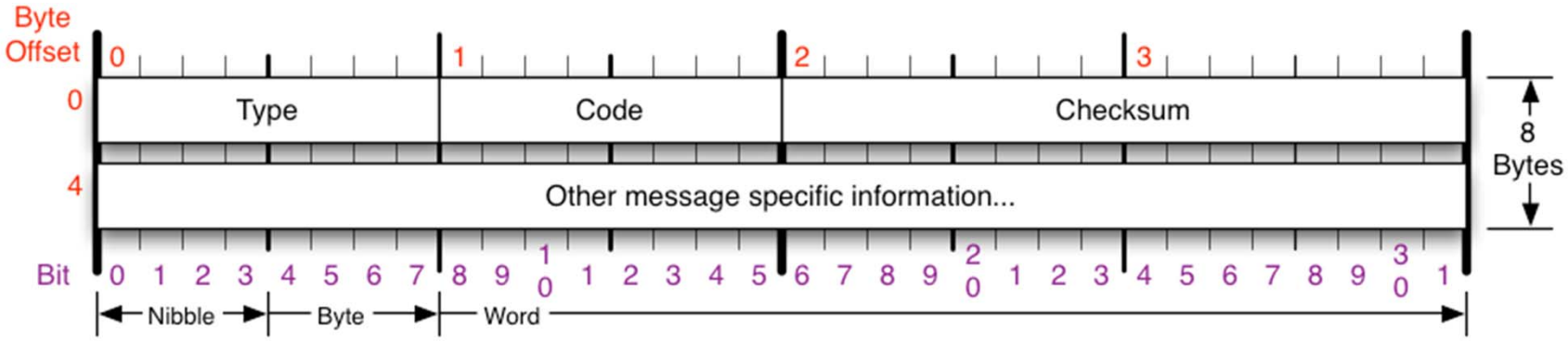
3. **A는 C의 MAC주소로 데이터를 전송한다.**



ICMP (Internet Control Message Protocol)

- **Internet Control Message Protocol**
  - **Layer 3 Protocol**
  - 다양한 유형의 정보를 교환할 수 있도록 다양한 메시지 유형을 정의
  - 호스트와 게이트웨이(라우터) 사이에서 메시지를 제어
  - 네트워크의 테스트와 진단을 위해 사용
  - **IP**를 지원하기 위한 프로토콜로 정의

ICMP Header (Layer 3)



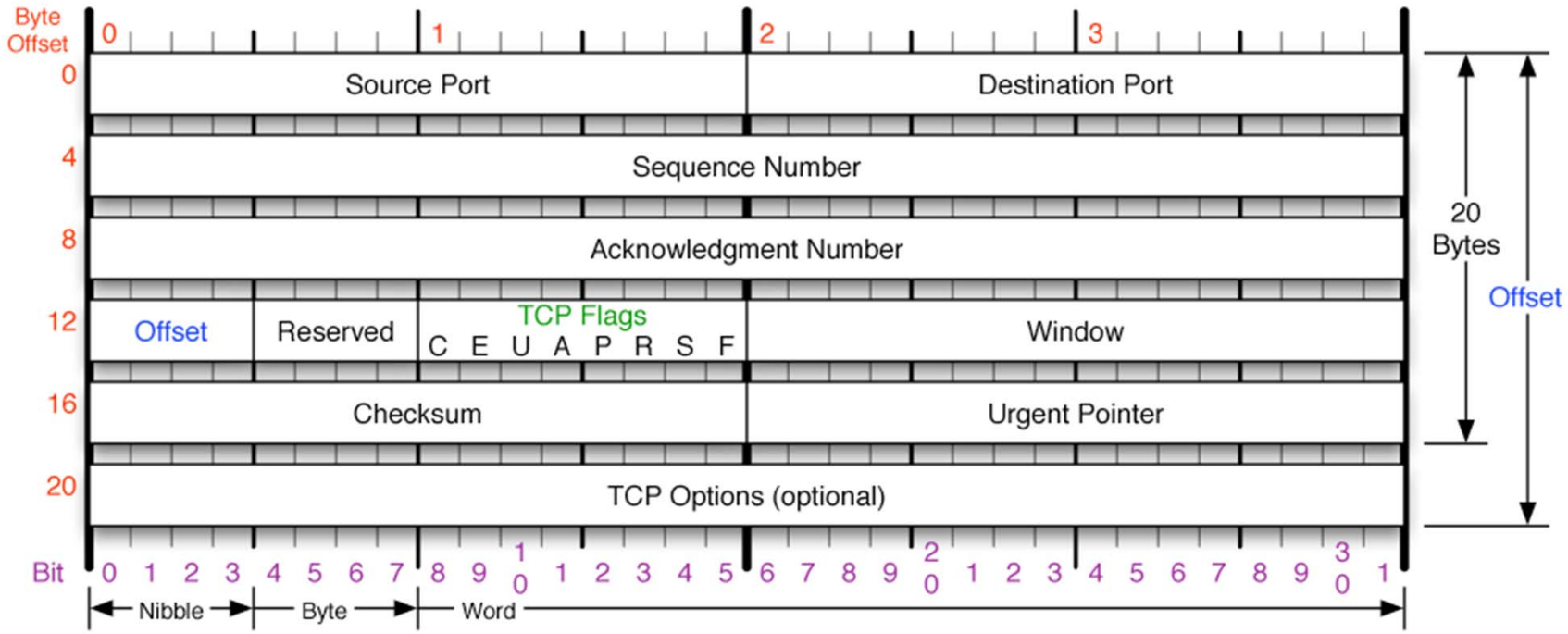
Type	Message
0	에코 응답 (Echo Reply)
3	수신처 도달 불가 (Destination Unreachable)
4	발신제한 (Source Quench)
5	라우트 변경 (redirect)
8	에코 요청 (Echo Request)
11	시간 초과 (Time Exceeded)
12	파라미터 불량 (Parameter Problem)
13	타임 스탬프 요청 (Timestamp Request)
14	타임 스탬프 응답 (Timestamp reply)

Code	Message
0	Network Unreachable
1	Host Unreachable
2	Protocol Unreachable
3	Port Unreachable
5	Source Route Failed
6	Destination Network Unknown
7	Destination Host Unknown

TCP(Transmission Control Protocol)

- **Transmission Control Protocol**
  - 연결지향 형 프로토콜
    - 출발지와 목적지간의 연결 설정과정을 통해 연결을 맺은 후 데이터를 전송한다 **(Three-way Handshake)**
  - 데이터의 신뢰성을 제공
    - **Sequence Number**를 사용하여 데이터를 전달하고 전달할 데이터의 확인을 **Acknowledge Number**로 확인 한다. 만약 전달한 데이터에 문제가 발생했을 경우 재 전송을 시도한다
  - 흐름제어
    - **TCP Header**의 **Window** 필드를 사용하여 해당 시스템의 **buffer** 크기를 송신 시스템(또는 수신시스템)에게 알려준다
  - 오류제어
    - **Checksum**값을 이용

TCP Header (Layer 3)



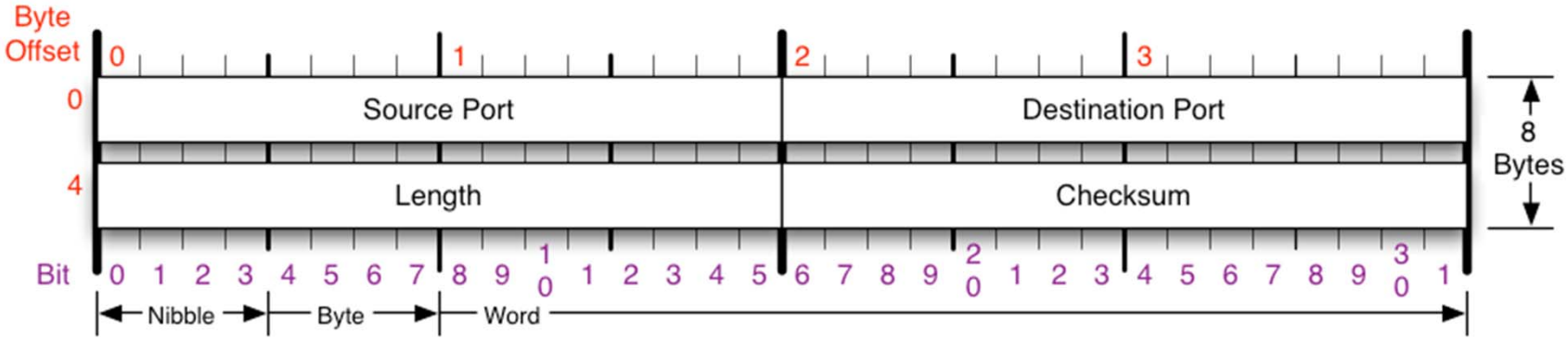
TCP Header Field

- Source Port: 출발지 Port 번호
- Destination Port : 목적지 Port 번호
- Sequence Number : 스트림을 유지하기 위한 순차번호
  - syn flag가 1인 경우 초기 순서번호를 의미
  - syn flag가 0인 경우 segment의 순서번호를 의미
- Acknowledge Number : 응답 번호
- Offset : TCP Header의 크기 (기본 20byte)
- TCP Flags : TCP Segment의 목적을 의미
  - URG : 긴급 데이터 Urgent 항목의 값이 유효함
  - ACK : 응답 Segment임을 표시. Acknowledge Number가 유효함
  - PSH : 해당 segment의 데이터를 Application 계층으로 즉시 전달해야 함
  - RST : 연결을 재 설정, 또는 유효하지 않은 Segment를 받았을 경우 응답으로 전달
  - SYN : 연결 요청
  - FIN : 연결 종료
- Window : 수신측이 받을 수 있는 buffer의 크기
- Checksum : TCP Header를 포함한 Segment전체의 오류 검사를 위해 사용
- Urgent Pointer : 긴급한 처리해야 할 데이터의 마지막 바이트
- Option : 최대 40byte (32bit단위로 처리해야 하므로 길이가 안 맞는 경우 Padding)

UDP(User Datagram Protocol)

- **User Datagram Protocol**
  - IP를 기반으로 데이터를 전송
  - 데이터 전달을 보장 받지 못함 (신뢰성이 없음)
  - 연결 설정 및 연결 종료 과정이 존재하지 않음
  - 연결 상태가 존재하지 않음
  - 속도가 TCP보다 빠르다

UDP Header (Layer 3)

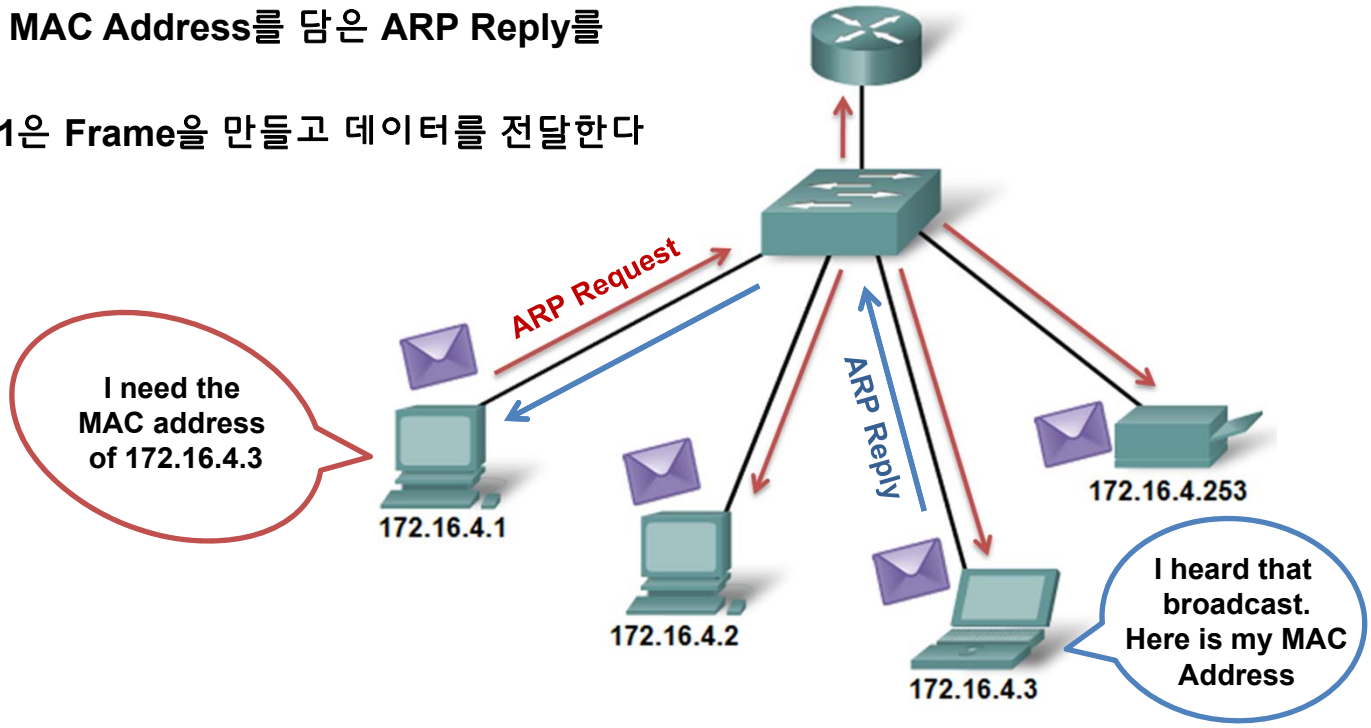


- **Source Port** : 출발지 **Port** 번호
- **Destination Port** : 목적지 **Port** 번호
- **Length** : **UDP Header**를 포함한 **UDP Segment**의 전체 크기
- **Checksum** : **UDP Header**를 포함한 **UDP Segment** 전체의 오류 검사

ARP Operation

- **ARP는 Request와 Reply로 구성**
  - **172.16.4.1이 172.16.4.3에게 데이터를 전송하는 경우**

1. **172.16.4.1은 172.16.4.3 IP Address를 사용하는 PC의 MAC Address를 찾기 위해 ARP Request를 Broadcast 한다**
2. **ARP Request를 받은 172.16.4.3은 172.16.4.1에게 자신의 MAC Address를 담은 ARP Reply를 전달한다**
3. **172.16.4.1은 Frame을 만들고 데이터를 전달한다**



ARP 문제점

- **ARP Vulnerability**
  - ARP는 Stateless한 Protocol
  - 인증 매커니즘의 부재
    - 응답자가 보낸 MAC의 진위 여부를 확인할 수 없음
  - ARP Request는 Broadcast 방식으로 Packet을 전달
    - Broadcast Traffic을 줄이가 위한 방법
      - ✓ARP Cache Table을 사용
      - ✓ARP Request Packet 안의 정보를 학습 (일부 OS)

ARP Spoofing Attack

- **ARP Spoofing Attack**
  - ARP Cache poisoning이라고도 함
  - Victim의 ARP Cache Table의 내용을 공격자의 의도대로 변경
  - Packet의 이동 경로 변경 가능
    - **Victim은 공격자에게 packet을 전달하게된다**

- **공격 원리**
  - Attacker
    - **Victim에게 공격자가 임의로 생성한 ARP Reply 패킷을 지속적으로 전송**
  - Target
    - **ARP는 자시이 받은 ARP Reply Packet을 인증하는 매커니즘이 없으므로 공격자가 보내는 ARP Reply를 받아들여 자신의 Cache Table을 변경한다**

ARP Spoofing Attack

- **주의사항**
  - Target의 ARP cache table을 조작하여 Packet을 공격자를 경유하도록 공격했다면 공격자는 반드시 해당 Packet을 forwarding해주어야 한다
  - 공격자의 NIC가 Packet을 받은 후 IP를 확인하게 되는데 이때 자신의 IP가 아니므로 Forwarding이 설정되어 있지 않으면 패킷을 Drop하게 된다. 따라서 Data를 전달한 송신자는 응답을 받을 수 없게 된다

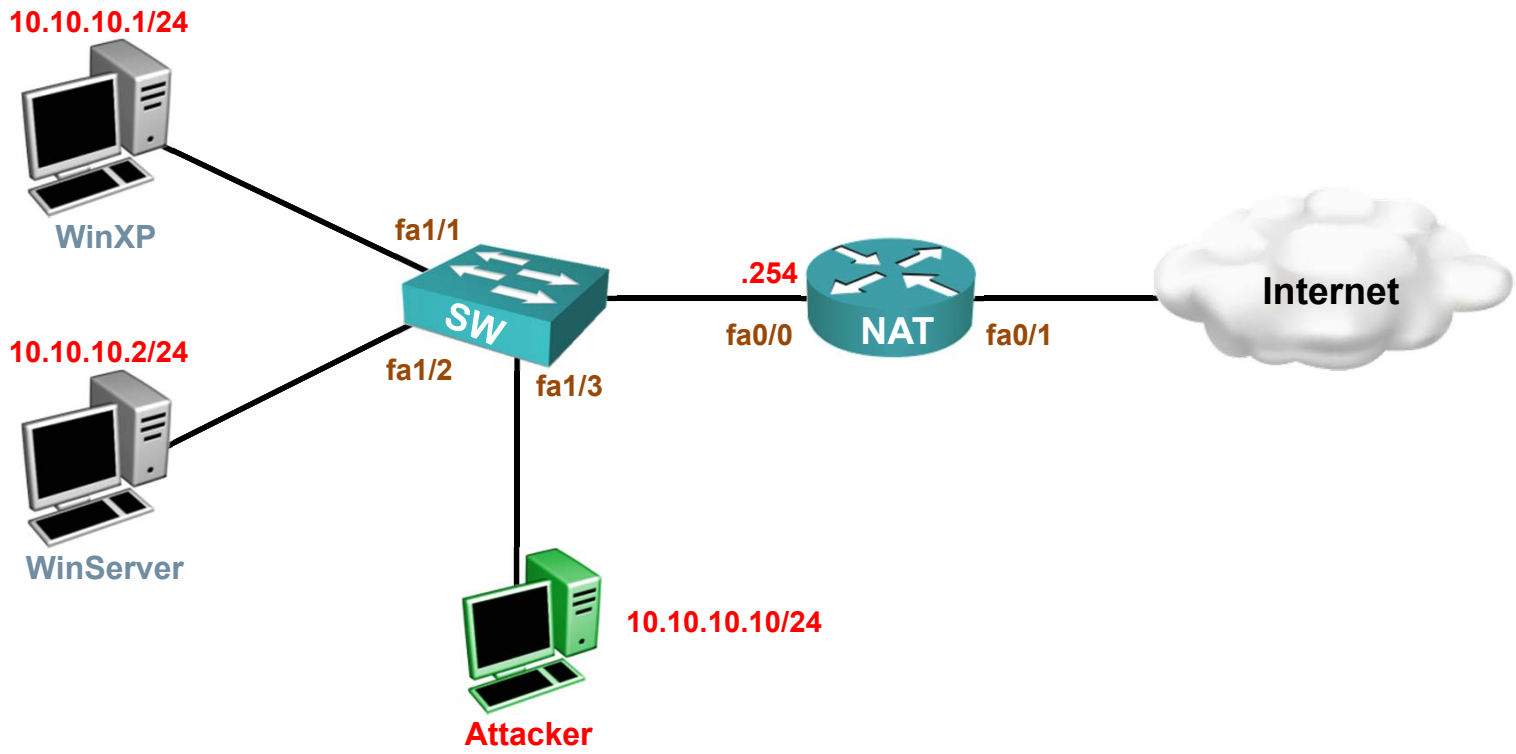
IP Forwarding 방법

- **Packet Forwarding 방법**
  - Kernel에서 지원하는 방법
    - **Unix 계열**
      - /proc/sys/net/ipv4/ip_forwarding의 내용을 1로 설정
    - **Windows 계열**
      - \HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\IPEnableRouter를 1로 설정
  - Application을 사용하는 방법
    - **fragrouter –B1**

- **두 방법의 차이점**
  - Kernel방식 : 해당 시스템을 라우터처럼 동작 시키기 때문에 Traceroute로 확인 가능
  - fragrouter를 이용할 때는 traceroute로 확인 안됨

ARP Spoofing Attack Lab

- **Topology**



ARP Spoofing

- **ARP Spoofing 공격**
  - Sniffing하고자 하는 두 개의 System을 선택한 후 서로의 MAC 주소를 공격자의 MAC 주소로 위조하여 보냄
  - 두 시스템이 통신할 때 공격자를 경유하여 통신하게 됨
  - MiTM(Man In The Middle) 형태가 됨
- 서로에게 공격자가 상대방인 것처럼 속이기 위해 **ARP Spoofing**을 한다
  - arpspoof –t 10.10.10.1 10.10.10.254
  - arpspoof –t 10.10.10.254 10.10.10.1