



# 네트워크 해킹과 보안

정보 보안 개론과 실습

개정3판



## Chapter 02 네트워크에 대한 이해

# 목차

- 01 프로토콜
- 02 네트워크 계층 구조
- 03 물리 계층
- 04 데이터 링크 계층
- 05 네트워크 계층
- 06 전송 계층
- 07 응용 계층
- 08 계층별 패킷 분석

# 학습목표

- 프로토콜의 필요성과 다양한 기능을 이해한다.
- TCP/IP를 구성하는 주요 프로토콜의 구조와 목적을 이해한다.
- 네트워크 계층 구조의 필요성을 이해한다.
- 네트워크 계층 구조인 OSI 7계층의 주요 동작 원리를 이해한다.
- 라우팅과 스위칭을 이해하고 패킷 분석 능력을 키운다.

# 1. 프로토콜

## 1.1 프로토콜에 대한 이해

### ■ 프로토콜(Protocol)

- 본래 의미는 외교에서 의례 또는 의정서
- 톰 마릴이 '컴퓨터와 컴퓨터 사이에서 메시지를 전달하는 과정'이라 정의



그림 2-1 프로토콜의 예 - 통역원을 통해 이야기를 나누는 두 대통령

## 1.1 프로토콜에 대한 이해

### ■ 프로토콜의 3가지 요소

- ① 구문(Syntax) : 데이터의 구조나 포맷을 의미
- ② 의미(Semantics) : 전송되는 데이터의 각 부분이 무엇을 뜻하는지를 알 수 있게 미리 정해둔 규칙(데이터 자체뿐만 아니라 오류 제어, 동기 제어, 흐름 제어를 포함)
- ③ 순서(Timing) : 어떤 데이터를 보낼 것인지와 얼마나 빠르게 데이터를 보낼 것인지 정의

## 1.1 프로토콜에 대한 이해

### ■ 프로토콜의 기능

- 주소 설정(Addressing)
  - 서로 다른 시스템의 두 개체가 통신을 하는 경우 필요
- 순서 제어(Sequence Control)
  - 프로토콜 데이터 단위를 전송할 때 보내는 순서를 명시하는 기능(연결 지향형(Connection-Oriented)에만 사용)
- 데이터 대열의 단편화 및 재조합(Fragmentation & Reassembly)
  - 대용량 파일을 전송할 때 전송 효율이 높은 작은 단위로 나누어 전송한 뒤 전송받은 시스템에서 이를 재조합해야 함.

# 1. 프로토콜

## 1.1 프로토콜에 대한 이해

### ■ 프로토콜의 기능

- 캡슐화(Encapsulation)
  - 데이터에 제어 정보를 덧붙이는 것

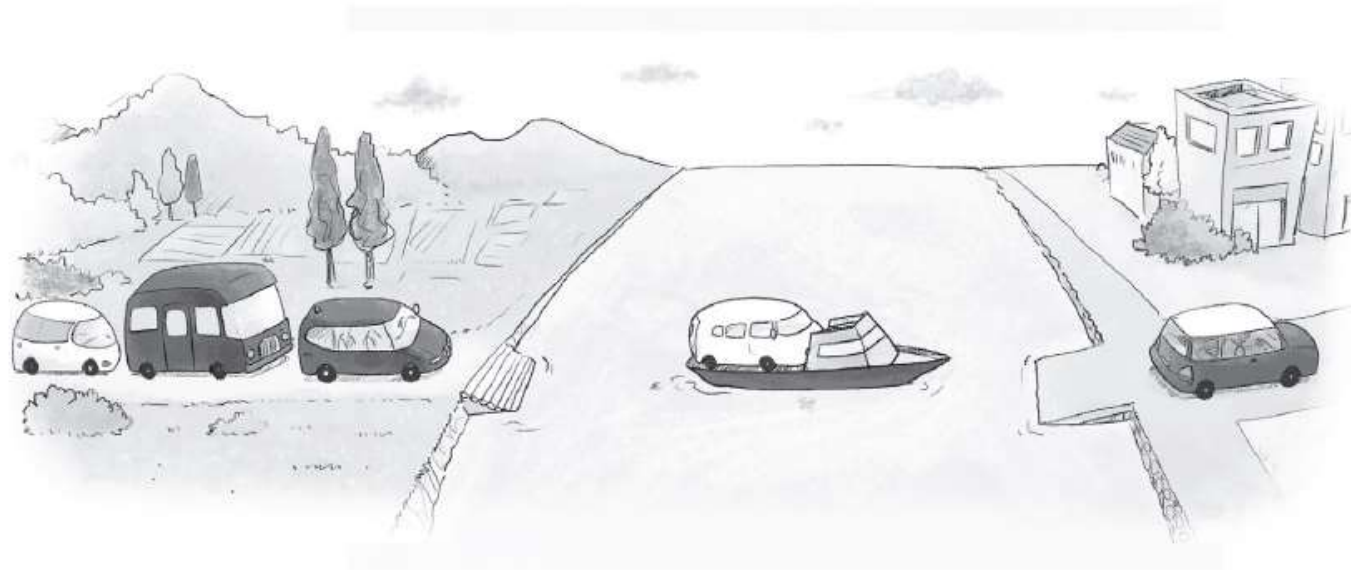


그림 2-2 캡슐화

- 연결 제어(Connection Control)
  - 연결 설정, 데이터 전송, 연결 해제에 대한 통제 수행

## 1.1 프로토콜에 대한 이해

### ■ 프로토콜의 기능

- 흐름 제어(Flow Control)
  - 송신측 개체로부터 오는 데이터의 양이나 속도를 조절하는 기능
  - 송신측과 수신측의 속도 차이 등으로 인한 정보 유실을 방지
- 오류 제어(Error Control)
  - 두 개체에서 데이터를 교환할 때 SDU나 PCI가 잘못되었을 경우, 이를 발견하는 기법
  - 순서를 검사하거나 특정 시간 안에 받지 못하면 재전송을 요구하는 방식으로 이루어짐.
- 동기화(Synchronization)
  - 두 개체 간에 데이터를 전송할 때 각 개체는 특정 타이머 값이나 윈도우 크기 등을 통해 동시에 정의된 인자 값을 공유하는 것
- 다중화(Multiplexing)
  - 통신 선로 하나에서 여러 시스템을 동시에 통신할 수 있는 기법
- 전송 서비스
  - 우선순위 결정, 서비스 등급과 보안 요구 등을 제어하는 서비스



## 2. 네트워크 계층 구조

### 2.1 네트워크 계층화에 대한 이해

#### ■ 네트워크 계층화에 대한 이해

- 1980년대 초 ISO는 여러 업체가 만든 시스템에 대해 상호연동이 가능한 표준 네트워크 모델을 제정할 필요성을 인식
- 1984년 OSI(Open System Interconnection) 네트워크 모델을 발표

7계층	응용 계층(Application Layer)
6계층	표현 계층(Presentation Layer)
5계층	세션 계층(Session Layer)
4계층	전송 계층(Transport Layer)
3계층	네트워크 계층(Network Layer)
2계층	데이터 링크 계층(Data Link Layer)
1계층	물리 계층(Physical Layer)

그림 2-3 OSI 7계층

### 2.1 네트워크 계층화에 대한 이해

#### ■ OSI 7계층

- 물리 계층 : 1계층
  - 실제 장치를 연결하는 데 필요한 전기적, 물리적 세부 사항을 정의
  - 물리 계층의 장치로는 허브나 리피터가 있음.
- 데이터 링크 계층 : 2계층
  - 점대점(Point-to-Point) 사이의 신뢰성 있는 전송을 보장하기 위한 계층
  - CRC 기반의 오류 제어와 흐름 제어가 필요
  - 가장 잘 알려진 예는 이더넷
- 네트워크 계층 : 3계층
  - 여러 노드를 거칠 때마다 경로를 찾아주는 역할
  - 라우팅, 흐름 제어, 단편화(Segmentation/Desegmentation), 오류 제어 등을 수행
  - 대표적인 예는 라우터로, 이 계층에서 동작하는 스위치를 흔히 L3 스위치라 함.

### 2.1 네트워크 계층화에 대한 이해

#### ■ OSI 7계층

##### ■ 전송 계층 : 4계층

- 양 끝단 사용자들이 신뢰성 있는 데이터를 주고받을 수 있게 하여 상위 계층이 데이터 전달의 유효성이나 효율성을 고려하지 않아도 되게 해줌.
- 전송 계층에서 동작하는 프로토콜 중 TCP는 연결 지향(Connection-Oriented) 프로토콜

##### ■ 세션 계층 : 5계층

- 양 끝단의 응용 프로세스가 통신을 관리하기 위한 방법을 제공
- 동시 송수신 방식(Duplex), 반이중 방식(Half-Duplex), 전이중 방식(Full-Duplex)의 통신과 함께 체크 포인팅과 유휴, 종료, 재시작 과정 등을 수행
- TCP/IP 세션을 만들고 없애는 책임을 짐.

### 2.1 네트워크 계층화에 대한 이해

#### ■ OSI 7계층

- 표현 계층 : 6계층
  - 시스템에서 사용되는 코드 간의 번역을 담당
  - 데이터 압축과 암호화 기능 수행
- 응용 계층 : 7계층
  - 사용자나 응용 프로그램 사이에 데이터 교환을 가능하게 하는 계층
  - HTTP, FTP, 터미널 서비스, 메일 프로그램, 디렉토리 서비스 등을 제공

## 2. 네트워크 계층 구조

### 2.1 네트워크 계층화에 대한 이해

#### ■ OSI 7계층

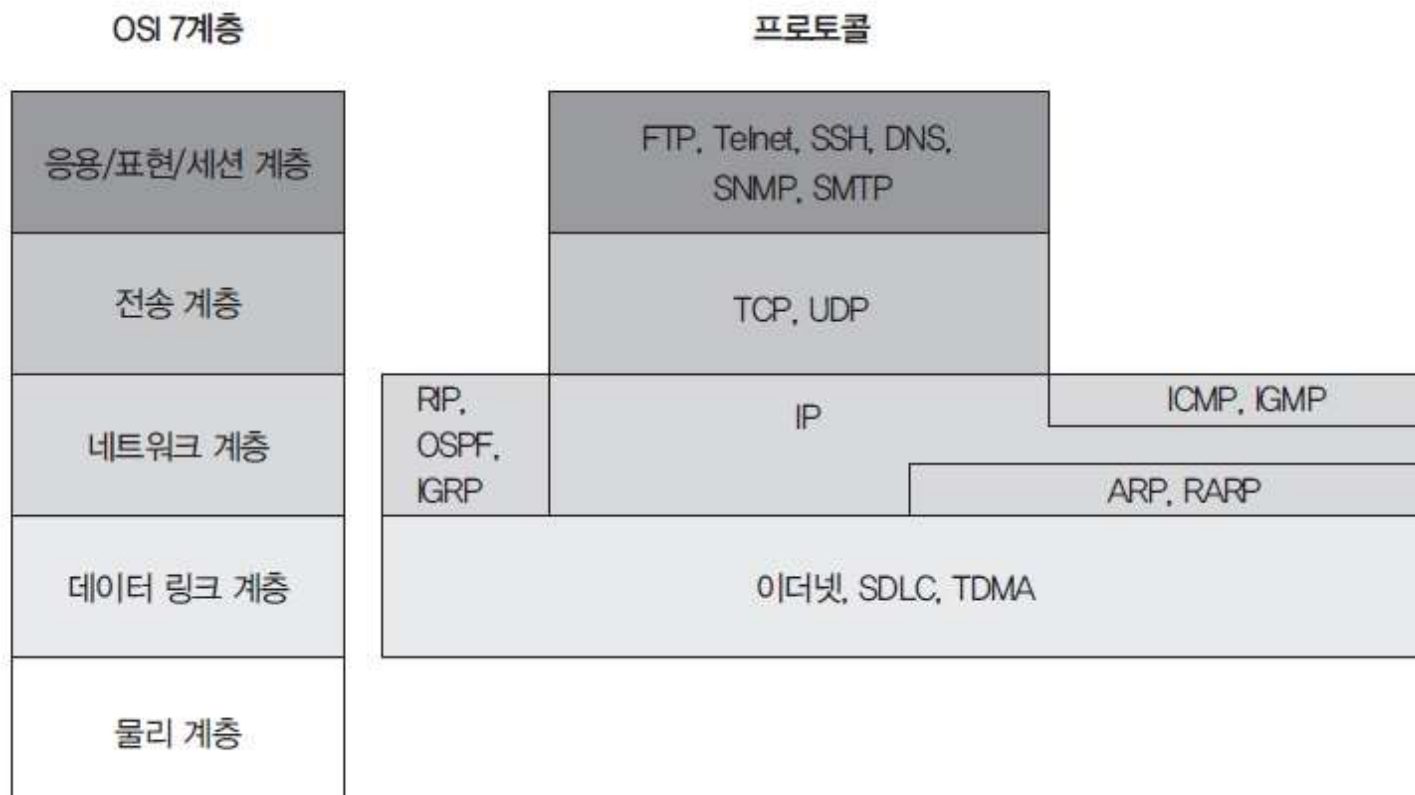


그림 2-4 OSI 7계층 구조에 대응하는 프로토콜

## 2. 네트워크 계층 구조

### 2.1 네트워크 계층화에 대한 이해

#### ■ TCP/IP 4계층



그림 2-5 OSI 7계층과 TCP/IP 4계층

### 3.1 물리 계층에 대한 이해

#### ■ 1계층 : 물리 계층(Physical Layer)

- 시스템 간의 연결선(흔히 랜(LAN)을 뜻함)
- 보통 랜 케이블은 CAT 5의 10/100 BASE-T(IEEE 802.3) 또는 CAT 6의 10/100/1000 BASE-T(IEEE 802.3) 선을 사용하고, 전화선은 CAT 1을 사용

## 3. 물리 계층

### 3.1 물리 계층에 대한 이해

#### ■ CAT별 특성

표 2-1 CAT별 특성

카테고리	최대 속도	용도
CAT 1	1Mbps 미만	<ul style="list-style-type: none"><li>• 아날로그 음성. 일반적인 전화 서비스</li><li>• ISDN 기본율 접속(Basic Rate Interface)</li><li>• Doorbell wiring</li></ul>
CAT 2	4Mbps	<ul style="list-style-type: none"><li>• IBM의 토큰 링 네트워크에 주로 사용</li></ul>
CAT 3	16Mbps	<ul style="list-style-type: none"><li>• 10BASE-T 이더넷의 데이터 및 음성</li></ul>
CAT 4	20Mbps	<ul style="list-style-type: none"><li>• 16Mbps 토큰 링에서 사용(많이 사용되지는 않음)</li></ul>
CAT 5	100Mbps	<ul style="list-style-type: none"><li>• 옥내 수평 및 간선 배선망(100MHz)</li><li>• 4/16Mbps 토큰 링(IEEE 802.5)</li><li>• 10/100 BASE-T(IEEE 802.3)</li><li>• 155Mbps ATM</li></ul>
CAT 6	250Mbps	<ul style="list-style-type: none"><li>• 옥내 수평 및 간선 배선망(250MHz)</li><li>• 4/16Mbps 토큰 링(IEEE 802.5)</li><li>• 10/100/1000 BASE-T(IEEE 802.3)</li><li>• 155/622Mbps ATM</li><li>• 기가비트 이더넷</li></ul>



## 3. 물리 계층

### 3.1 물리 계층에 대한 이해

#### ■ 케이블의 구분

- 일반적인 랜 케이블은 UTP를 사용

표 2-2 케이블의 구분

구분	내용
UTP(Unshielded Twisted Pair)	두 선 간의 전자기 유도를 줄이기 위해 절연의 구리선이 서로 꼬여 있는 것으로, 제품 전선과 피복만으로 구성된다.
FTP(Foil Screened Twisted Pair)	알루미늄 은박이 4가닥 선을 감싸고 있는 것으로, UTP보다 절연 기능이 탁월해 공장 배선용으로 많이 쓰인다.
STP(Shielded Twisted Pair)	연선으로 된 케이블 겉에 외부 피복, 또는 차폐재가 추가(실드 처리)된 것으로, 차폐재가 접지 역할을 하므로 외부 노이즈를 차단하거나 전기적 신호 간섭을 줄이는 데 탁월하다.

### 3.1 물리 계층에 대한 이해

#### ■ 커넥터

- 전화선 연결 커넥터 : RJ(Registered Jack-11)라고 부름.
- 랜 케이블의 연결 커넥터 : RJ-45라고 부름.
- 보통 쓰는 랜 케이블은 UTP 케이블 중 CAT 5 또는 CAT 6에 해당하는 10/100/1000 BASE-T(IEEE 802.3) 선과 RJ-45 커넥터



그림 2-7 RJ-45



그림 2-6 RJ-11

### 3.2 물리 계층 관련 장비

#### ■ 리피터(Repeater)

- 네트워크를 연장하기 위한 장비
- 불분명해진 신호 세기를 다시 증가시키는 역할
- 최근에는 리피터가 모든 네트워크 장비에 공통으로 들어가는 기능이 됨.



그림 2-8 리피터

### 3.2 물리 계층 관련 장비

#### ■ 허브(Hub)

- 요즘 쓰이는 스위치의 예전 형태
- 최근의 스위치를 스위칭 허브, 이전 허브를 더미 허브라 부름.
- 허브는 스위치와 형태나 사용 방법이 같지만 패킷을 모든 곳에 똑같이 복사해서 보내는 것이 다름(스위치는 목적지에만 데이터를 전송).



그림 2-9 더미 허브의 구조

## 4. 데이터 링크 계층

### 4.1 데이터 링크 계층에 대한 이해

#### ■ 2계층 : 데이터 링크 계층(Data Link Layer)

- 랜 카드나 네트워크 장비의 하드웨어 주소(MAC 주소)만으로 통신하는 계층
- 네트워크 카드의 MAC 주소는 윈도우 명령 창에서 'ipconfig /all' 명령을 실행하면 'Physical Address'에서 확인 가능

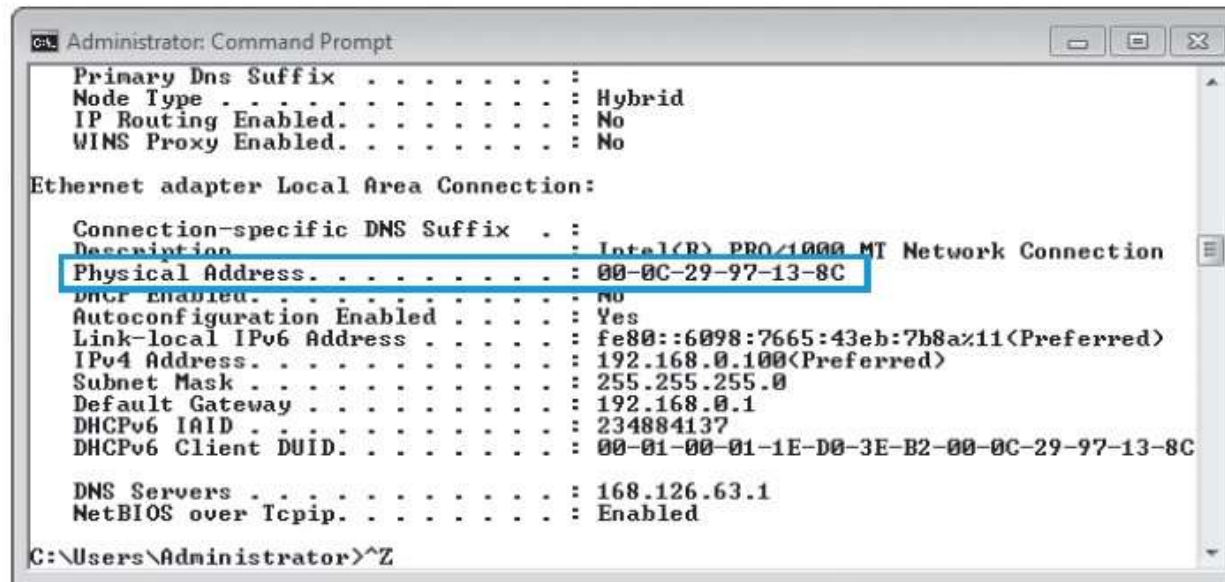


그림 2-10 MAC 주소 확인

### 4.1 데이터 링크 계층에 대한 이해

#### ■ MAC 주소

- 총 12개의 16진수로 구성
- 앞쪽 6개는 네트워크 카드를 만든 회사(OUI)를 뜻하고, 뒤쪽 6개는 호스트 식별자(Host Identifier)로 각 회사에서 임의로 붙이는 일종의 시리얼
- 같은 MAC 주소는 존재하지 않음.

OUI	Host Identifier
00-0C-29	97-13-8C

## 4. 데이터 링크 계층

### 4.1 데이터 링크 계층에 대한 이해

#### ■ X.25

- ITU-T(구 CCITT)에 의해 1980년경부터 규격화된 통신 규약
- 단말장치(DTE)와 회선종단장치(DCE)간의 통신 절차를 규정한 계층화된 프로토콜
- 가장 일반적인 회선종단장치는 모뎀, 단말장치는 컴퓨터
- X.25의 운용속도는 T1/E1급 정도



그림 2-11 X.25의 통신 구성 요소

### 4.1 데이터 링크 계층에 대한 이해

#### ■ 프레임 릴레이(Frame Relay)

- 불필요한 전송 오류 제어나 흐름 제어 등 복잡한 기능을 최소화하고, 망 종단 장치에서 처리하도록 하여 고속 전송을 실현하는 고속 데이터 전송 기술
- X.25 패킷 교환망의 10배까지 고속 데이터 전송이 가능

#### ■ ATM(Asynchronous Transfer Mode)

- 고속의 데이터를 53Byte 셀로 처리하는 VLSI 기술
- 실시간 영상 전송과 같은 고속 통신에 사용



### 4.2 데이터 링크 계층 프로토콜

#### ■ 이더넷

- 제록스의 PARC(Palo Alto Research Center)에서 1970년대에 개발한 데이터 링크 계층의 프로토콜
- 이더넷 패킷의 최소 길이는 64KBytes, 최대 길이는 1,518KBytes
- 이더넷은 1980년대에 발표된 IEEE 802.3이 규약의 기초가 됨.

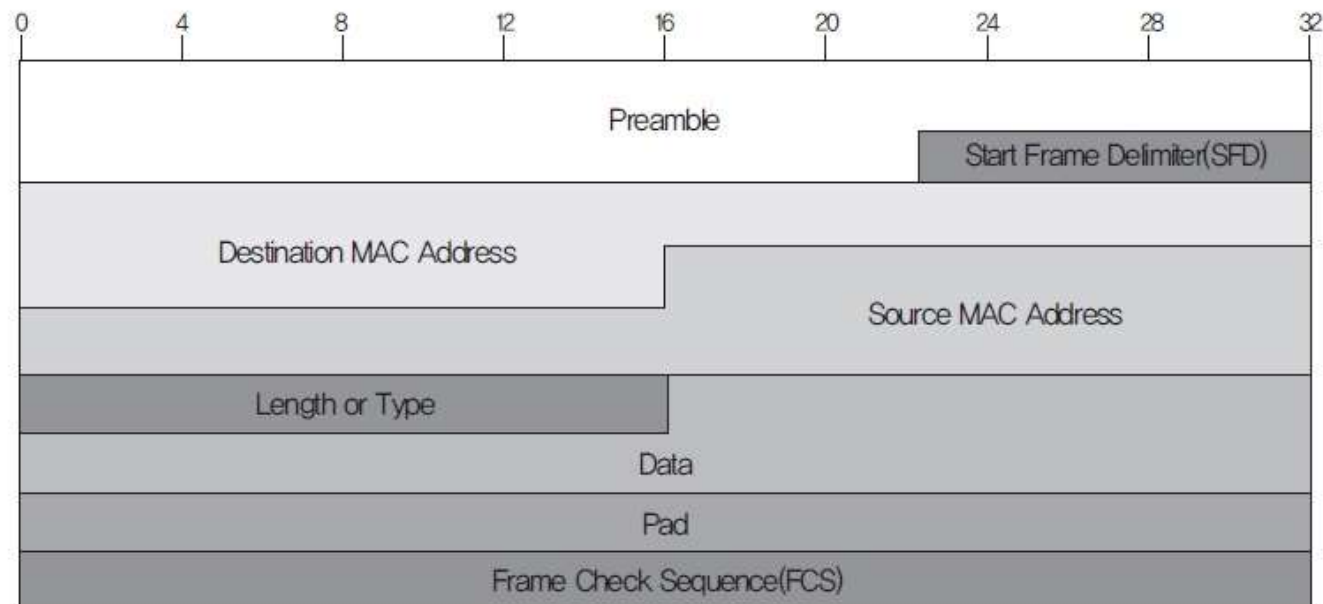


그림 2-12 이더넷 패킷 구조

## 4. 데이터 링크 계층

### 4.2 데이터 링크 계층 프로토콜

#### ■ 이더넷

표 2-3 이더넷 패킷의 내용

필드 이름	길이	내용
Preamble	7Bytes	패킷이 입력되고 있음을 네트워크 인터페이스에 알리기 위한 부분으로 1과 0이 번갈아 입력된다. 실제 데이터가 들어오니 '이제 정신차려!'라고 알려주는 것과 같다.
SFD	1Byte	Start Frame Delimiter. 통신을 위한 최초의 패킷에 10101011을 입력하여 해당 패킷이 최초 패킷임을 알려준다.
Destination MAC Address	6Bytes	패킷을 받을 네트워크 인터페이스에 대한 MAC 주소를 가리키는 것으로, 해당 주소가 모두 1(FF:FF:FF:FF:FF:FF)이면 브로드캐스팅 패킷이 된다.
Source MAC Address	6Bytes	패킷을 보내는 네트워크 인터페이스에 대한 MAC 주소를 가리킨다.
Length or Type	2Bytes	IEEE 802.3은 길이가 기록되는데 이더넷 버전 2 등의 프로토콜은 타입이 기록된다.
Data	0~1,500Bytes	전송 데이터가 저장되는 것으로, 최대 크기는 1,500Bytes다.
Pad	가변	전송하려는 데이터의 길이가 46Bytes보다 작으면 전체 패킷의 최소 길이인 64Bytes를 맞추기 위해 여기에 임의의 데이터를 쓴다.
FCS	4Bytes	Frame Check Sequence. 전송되는 패킷의 오류 등을 확인하기 위해 4Bytes의 CRC를 계산하여 입력한다.

### 4.3 데이터 링크 계층 관련 장비

#### ■ 브리지(Bridge)

- 랜과 랜을 연결하는 초기의 네트워크 장치
- 데이터 링크 계층에서 통신 선로를 따라서 한 네트워크에서 그 다음 네트워크로 데이터 프레임을 복사하는 역할

#### ■ 스위치(Switch)

- 기본적으로 데이터 링크 계층에서 작동하는 스위치를 뜻함.
- L2 스위치는 연결된 시스템이 늘어날수록 패킷 간 충돌 때문에 매우 낮은 속도로 동작하는 더미 허브의 문제점을 해결하는 획기적인 방안



그림 2-13 브리지



그림 2-14 스위치

### 4.4 스위칭

#### ■ 스위칭 방식

- 패킷 전송 방식에 따른 구분 : 컷스루 방식, 저장 후 전송 방식, 인텔리전트 스위칭 방식
- 제공하는 경로의 대역폭에 따른 구분 : 반이중 방식, 전이중 방식

#### ■ 컷스루(Cut-Through) 방식

- 수신한 프레임의 목적지 주소를 확인하고 목적지 주소의 포트로 프레임을 즉시 전송하여 지연 시간을 최소화
- 수신한 패킷에 오류가 발생할 때는 목적지 장치에서 해당 패킷을 폐기

### 4.4 스위칭

#### ■ 저장 후 전송 방식(Store & Forward)

- 전체 프레임을 수신하여 버퍼에 보관했다가 CRC 등의 오류를 확인하여 정상 프레임을 목적지 포트로 전송
- 패킷 길이에 비례해 전송 지연이 발생하지만 브리지나 라우터보다 신속
- 속도가 서로 다른 포트를 연결할 경우 반드시 사용해야 함.
- 최근에는 컷스루 방식과 저장 후 전송 방식을 동시에 지원하는 것이 일반적

#### ■ 인텔리전트 스위칭(Intelligent Switching) 방식

- 보통 컷스루 모드로 작동하다가 오류가 발생하면 저장 후 전송 모드로 자동 전환하여 오류 프레임 전송을 중지
- 오류율이 0이 되면 자동으로 다시 컷스루 방식으로 전환

### 4.4 스위칭

---

#### ■ 반이중(Half-Duplex) 방식

- 양방향 통신 기능을 제공하지만 한 번에 하나의 동작(수신 또는 송신)만 가능

#### ■ 전이중(Full-Duplex) 방식

- 송신 포트와 수신 포트를 분리해 반이중 방식보다 성능이 두 배로 뛰어나며, 충돌이 없어서 전송 거리의 제한을 연장할 수 있음.
- 기술적으로는 스위치에서만 전이중 방식을 지원할 수 있음.

### 4.4 스위칭

#### ■ 스위치 테이블

- 시스템 간의 원활한 통신을 위해 주소 테이블을 생성하고 관리하는 역할

스위치에 서버가 연결되어 있을 때 메모리 정보

1번 포트	
2번 포트	서버의 MAC 주소
3번 포트	
4번 포트	



클라이언트의 랜 케이블을 스위치의 3번 포트에 꽂음

1번 포트	
2번 포트	서버의 MAC 주소
3번 포트	클라이언트의 MAC 주소
4번 포트	

1번 포트	
192.168.0.100	서버의 MAC 주소
192.168.0.2	클라이언트의 MAC 주소
4번 포트	

### 5.1 네트워크 계층에 대한 이해

---

#### ■ 3계층 : 네트워크 계층(Network Layer)

- 랜을 벗어난 통신을 하기 위해 네트워크 계층에서 IP 주소를 사용



### 5.2 네트워크 계층 프로토콜

#### ■ ARP(Address Resolution Protocol)

- 데이터를 전달하려는 IP 주소와 통신에 필요한 물리적인 주소(MAC)를 알아내는 프로토콜
- 선택된 매체에 브로드캐스트를 통해 특정 IP 주소를 사용하는 호스트가 응답을 하도록 요구하는 방식을 사용

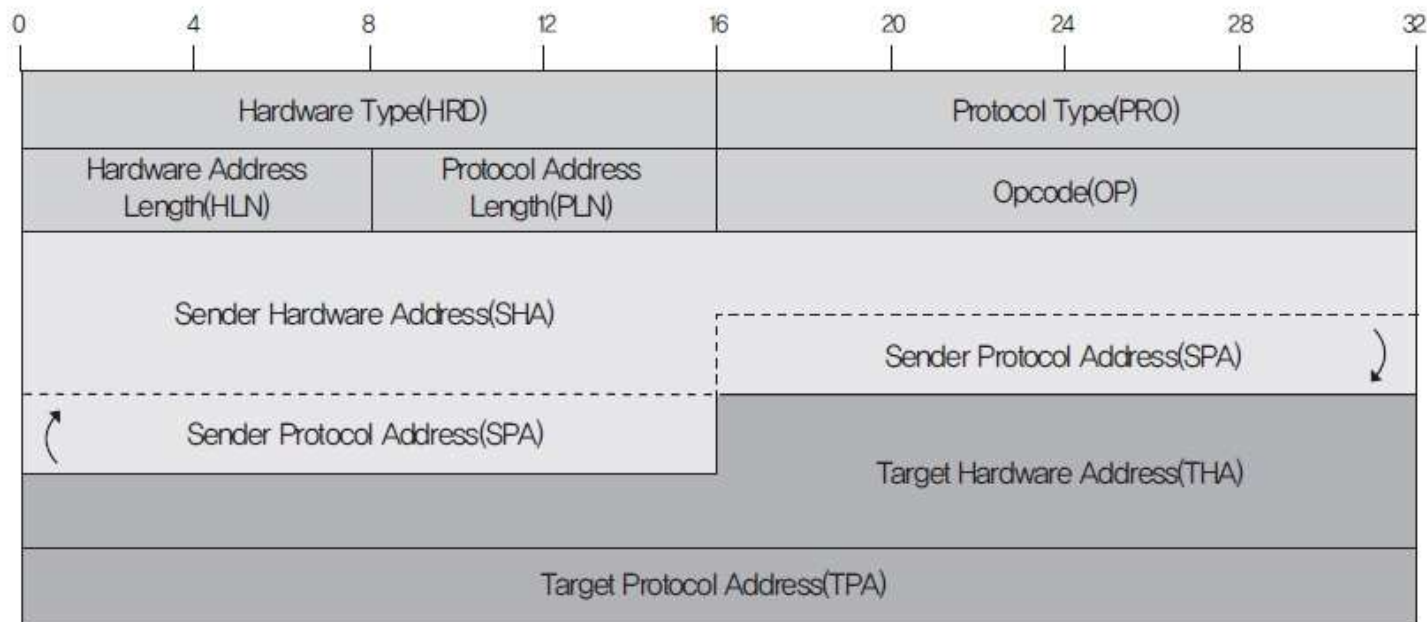


그림 2-15 ARP 패킷 구조

## ■ ARP(Address Resolution Protocol)

필드 이름	길이	내용
HRD	2Bytes	Hardware Type. ARP 패킷이 사용되는 물리 계층의 네트워크 유형을 정의한다. - 1 : 이더넷(10Mb)                      - 17 : HDLC - 6 : IEEE802 네트워크                - 18 : 광 채널 - 15 : 프레임 릴레이                  - 19 : ATM(Asynchronous Transfer Mode) - 16 : ATM                                  - 20 : 직렬 연결
PRO	2Bytes	Protocol Type. ARP를 위해 사용할 상위 계층 프로토콜의 종류를 지정한다. 일반적으로 IPv4를 사용하고, 그에 대한 값은 2048(0800 hex)이다.
HLN	1Byte	Hardware Address Length. 하드웨어 주소 값의 길이를 말하며 MAC 주소 값은 6이다.
PLN	1Byte	Protocol Address Length. 상위 계층 프로토콜의 주소 값의 길이로, IPv4의 주소 값 길이를 말한다. 당연히 4다.
OP	2Bytes	Opcode고, ARP 패킷 동작의 종류를 나타낸다. - 1 : ARP Request                      - 3 : RARP Request - 2 : ARP Reply                         - 4 : RARP Reply
SHA	=HLN	Sender Hardware Address. 패킷 송신자의 MAC 주소다.
SPA	=PLN	Sender Protocol Address. 패킷 송신자의 IP 주소다.
THA	=HLN	Target Hardware Address. 패킷 수신자의 MAC 주소다.
TPA	=PLN	Target Protocol Address. 패킷 수신자의 IP 주소다.

### 5.2 네트워크 계층 프로토콜

---

#### ■ RARP(Reverse Address Resolution Protocol)

- 디스크가 없는 호스트가 자신의 IP 주소를 서버로부터 확인하는 프로토콜
- 일반적으로 자체의 디스크 기억 장치가 없는 워크스테이션이나 지능형 단말기에서 사용

#### ■ IP(Internet Protocol)

- 가장 대표적인 네트워크 계층의 프로토콜
- 하위 계층의 서비스를 이용하여 두 노드 간의 데이터 전송 경로를 확립해주는 역할(단말장치 간 패킷 전송 서비스)

## 5. 네트워크 계층

### 5.2 네트워크 계층 프로토콜

#### ■ IP(Internet Protocol)

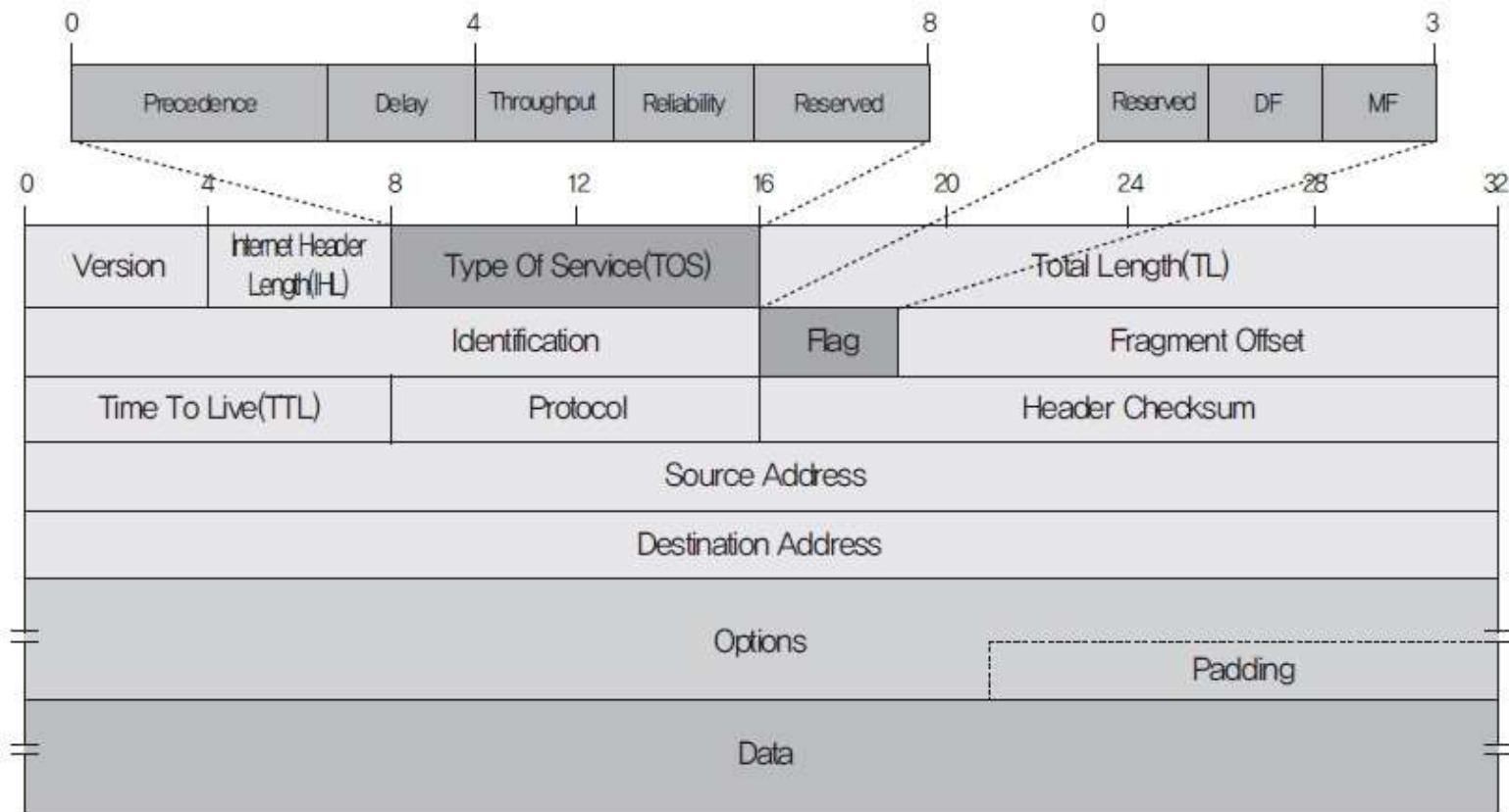


그림 2-16 IP 패킷 구조

### 5.2 네트워크 계층 프로토콜

#### ■ IP(Internet Protocol)

표 2-5 IP 패킷의 내용

필드 이름	길이	내용
Version	4bits	IP의 버전 정보로, 값이 0x4일 경우 IPv4를 의미한다.
IHL	4bits	Internet Header Length. IP 헤더의 길이로 이 필드 값에 4를 곱한 값이 실제 헤더의 바이트 길이이다.
TOS	1Byte	Type of Service. 라우터에서 IP 데이터그램을 처리할 때 우선순위를 정의한다. 우선순위로는 최소 지연(Delay), 최대 처리율(MTU), 최대 신뢰성(Reliability), 최소 비용(Cost)을 설정할 수 있고, 기본 값은 0이다.
TL	2Bytes	Total Length. 헤더를 포함한 데이터그램의 전체 길이를 의미한다.
Identification	2Bytes	데이터그램이 단편화(Fragmentation)될 때 모든 단편에 이 값이 복사되고, 단편화 된 데이터그램이 생성될 때마다 1씩 증가한다.
Flag	3bits	단편화 여부와 단편화된 조각이 첫 번째 조각인지, 중간 혹은 마지막 조각인지를 알려준다. - RF(Reserved Fragment) : 아직 사용하지 않으므로 항상 0이다. - DF(Don't Fragment) : 1이면 단편화되지 않았음을, 0이면 단편화되었음을 의미한다. - MF(More Fragment) : 0이면 마지막 단편이거나 유일한 단편이고, 1이면 마지막 단편이 아님을 의미한다.

## ■ IP(Internet Protocol)

필드 이름	길이	내용
Fragment Offset	13bits	기존 데이터그램 안에서 단편의 상대적 위치를 의미한다.
TTL	1Byte	Time To Live. 라우팅 과정에서 라우터를 몇 개 이상 통과하면 해당 패킷을 버릴 지를 입력한다. 라우터 하나를 지날 때마다 값이 1씩 줄어들고, 0이 되면 해당 패킷은 버려진다.
Protocol	1Byte	IP 계층의 서비스를 사용하는 상위 계층 프로토콜을 정의한다. - 1 : ICMP - 2 : IGMP - 6 : TCP - 17 : UDP
Header Checksum	2Bytes	패킷 전달 중 발생할 수 있는 오류 검사를 위해 사용하는 것으로, 송신측에서 체크섬을 계산하여 전송한다.
Source Address	4Bytes	송신측의 IP 주소다.
Destination Address	4Bytes	수신측의 IP 주소다.
Options	가변	해당 패킷에 대한 옵션 사항을 입력할 수 있다.
Padding	가변	옵션 내용이 입력될 경우 그 값이 32배수로 데이터가 마무리되도록 0으로 채운다.
Data	가변	IP 패킷을 통해 전송되는 데이터 부분이다.

### 5.2 네트워크 계층 프로토콜

#### ■ IP(Internet Protocol)

- 32자리 2진수로, 8자리마다 점을 찍어 구분
- A, B, C, D, E 클래스로 구분하는데 각 클래스는 네트워크 부분과 호스트 부분으로 구성
- A, B, C 클래스는 맨 앞부분에 시작하는 2진수 숫자에 따라 구분



그림 2-17 IP 주소 클래스



## 5. 네트워크 계층

### 5.2 네트워크 계층 프로토콜

#### ■ IP(Internet Protocol)

표 2-6 네트워크 클래스의 구분

시작 주소	구분	내용
0	A 클래스	<ul style="list-style-type: none"><li>• 00000000번~01111111(127)번 네트워크다.</li><li>• <math>2^7(128)</math>개가 가능하고, 하나의 A 클래스 안에 <math>256^3(16,777,216)</math>개 호스트가 존재할 수 있다.</li></ul>
10	B 클래스	<ul style="list-style-type: none"><li>• 10000000(128)번~10111111(191)번 네트워크다.</li><li>• <math>2^6 \times 256(16,384)</math>개가 가능하고, 하나의 B 클래스 안에 <math>256^2(65,536)</math>개 호스트가 존재할 수 있다.</li></ul>
110	C 클래스	<ul style="list-style-type: none"><li>• 11000000(192)번~11011111(223)번 네트워크다.</li><li>• <math>2^5 \times 256^2(2,097,152)</math>개가 가능하고, 하나의 C 클래스 안에 256개 호스트가 존재할 수 있다.</li></ul>
1110	D 클래스	<ul style="list-style-type: none"><li>• 11100000(224)번~11101111(239)번 네트워크다.</li><li>• 멀티미디어 방송을 할 때 자동으로 부여된다.</li></ul>
E 클래스		<ul style="list-style-type: none"><li>• 11110000(240)번~11111111(255)번 네트워크다.</li><li>• 테스트를 위한 주소 대역으로, 사용하지 않는다.</li></ul>



### 5.2 네트워크 계층 프로토콜

#### ■ IP(Internet Protocol)

- 사설 네트워크는 공인 네트워크 주소 부족 현상을 해결하기 위해 많이 사용

표 2-7 클래스별 사설 네트워크 범위

구분	지정된 사설 네트워크
A 클래스	10.0.0.0~10.255.255.255
B 클래스	172.16.0.0~172.31.255.255
C 클래스	192.168.0.0~192.168.255.255

### 5.2 네트워크 계층 프로토콜

#### ■ ICMP(Internet Control Message Protocol)

- 호스트 서버와 인터넷 게이트웨이 사이에서 메시지를 제어하고 오류를 알려주는 프로토콜
- 대표적인 툴은 ping

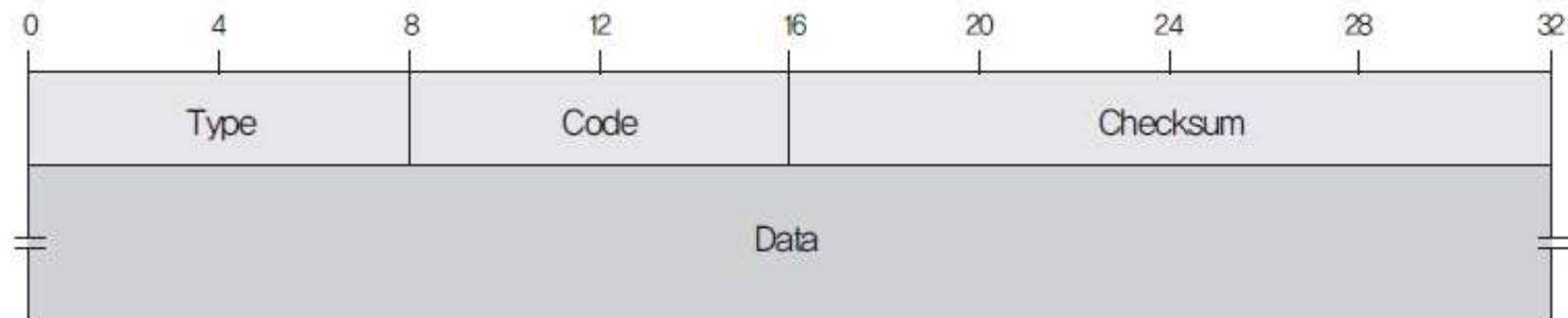


그림 2-18 ICMP 패킷 구조

### 5.2 네트워크 계층 프로토콜

#### ■ ICMP(Internet Control Message Protocol)

표 2-8 ICMP 패킷의 내용

필드 이름	길이	내용
Type	1Byte	ICMP 메시지의 타입을 가리키며, 다음과 같은 값이 있다. - 0 : Echo Reply - 4 : Source Quench - 5 : Redirect - 8 : Echo Request - 11 : Time Exceeded
Code	1Byte	각 타입별로 세부적인 값을 적는다.
Checksum	2Bytes	패킷의 무결성을 위한 오류 보정 값이다.
Data	가변	ICMP를 통해 보내는 데이터다. 보통 의미 없는 문자열로 채워진다.

### 5.2 네트워크 계층 프로토콜

#### ■ ICMP Echo Request 메시지

- 송신측의 전송 패킷이 목적이 노드나 라우터에 도착했는지를 확인하는 데 사용

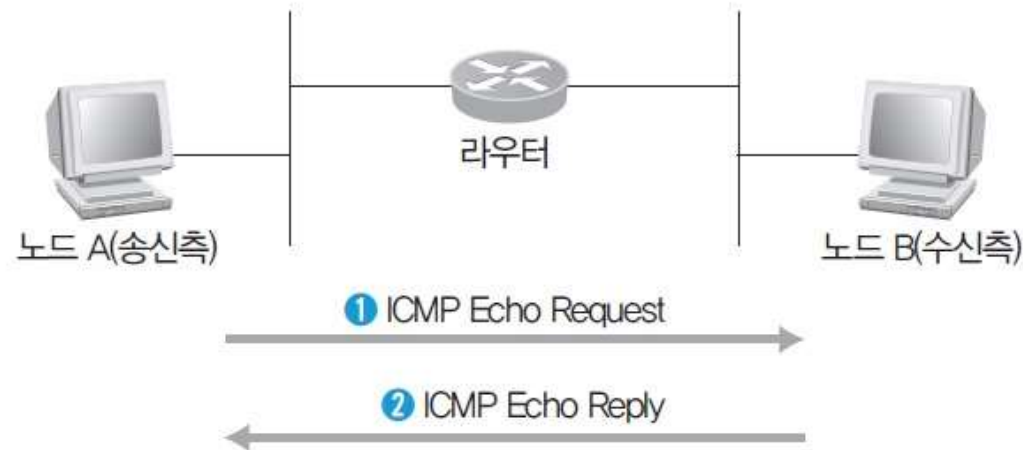


그림 2-19 ICMP Echo Request

#### ■ ICMP Destination Unreachable 메시지

- 라우터가 특정 노드의 패킷을 목적지에 보내지 못할 경우 보내는 메시지
- 목적지까지 전송되지 못한 이유를 나타내는 정보가 포함됨.

### 5.2 네트워크 계층 프로토콜

#### ■ ICMP Redirect 메시지

- 라우터가 송신측 노드에 적합하지 않은 경로로 설정되어 있을 경우 해당 노드에 대한 최적화된 경로를 다시 지정해주는 메시지

#### ■ ICMP Time Exceeded 메시지

- 패킷이 네트워크 사이에서 무한정 돌아가지 않도록 패킷을 처리할 때마다 TTL(Time to Live)을 감소시키다가 값이 '0'이 되면 보내는 메시지

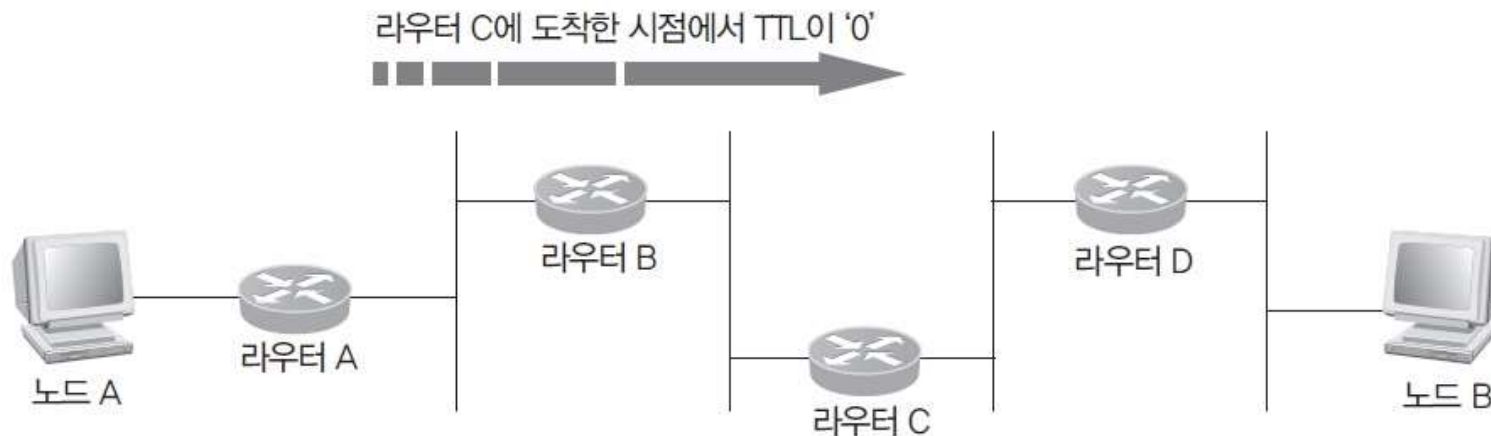


그림 2-20 ICMP Time Exceeded

### 5.2 네트워크 계층 프로토콜

#### ■ ICMP Source Quench 메시지

- IP 라우터의 WAN 쪽에 집중이 발생하여 송신 불능 상태가 되면 보내는 메시지
- 송신측은 이 메시지의 정보를 해석하여 송신 패킷의 양을 제어

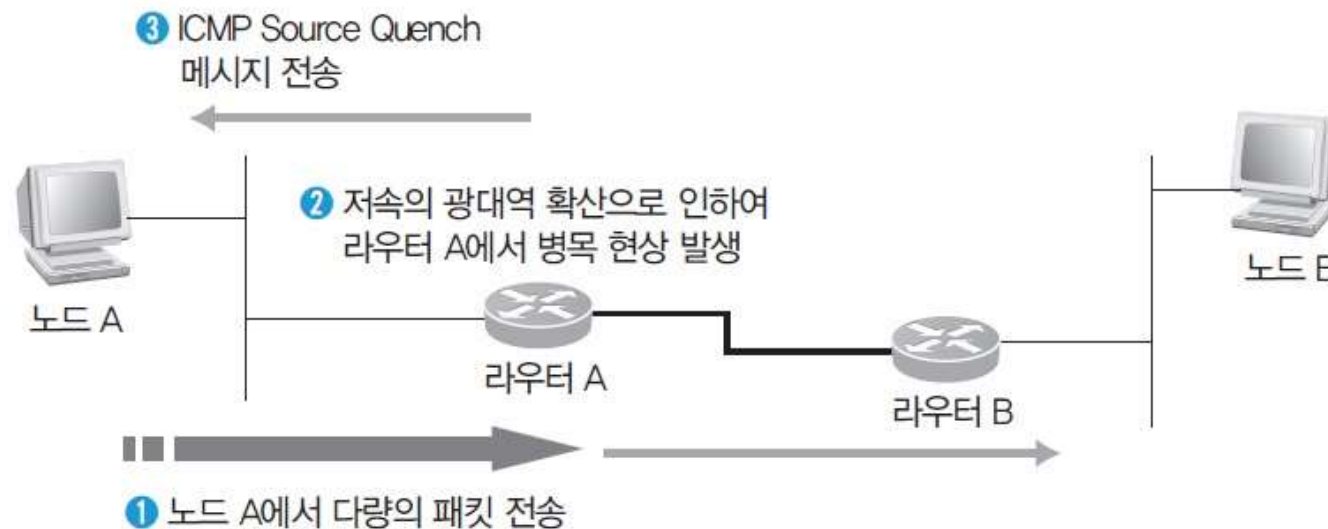


그림 2-21 ICMP Source Quench

### 5.2 네트워크 계층 프로토콜

#### ■ IGMP(Internet Group Management Protocol)

- 멀티캐스트에 관여하는 프로토콜로 멀티캐스트 그룹을 관리하는 역할
- 유니캐스트(Unicast)
  - 한 호스트에서 다른 호스트로 전송하는 것
  - 일반적인 IP 데이터의 전송은 유니캐스트를 사용
- 브로드캐스트(Broadcast)
  - 호스트에서 IP 네트워크에 있는 전체 호스트로 데이터를 전송하는 것
- 멀티캐스트(Multicast)
  - 유니캐스트와 브로드캐스트의 중간 형태
  - 송신하는 하나의 호스트에 특정한 호스트를 묶어서 전송하는 것
  - 지정한 주소로 패킷을 한 번만 전달하면 멀티캐스트 그룹에 속한 모든 호스트에 전달 되기 때문에 효율이 높음.
  - IP 멀티캐스트 주소는 D 클래스 주소 대역(244.0.0.1~239.255.255.255)으로 규정

### 5.3 네트워크 계층 관련 장비

#### ■ 라우터

- 네트워크의 대표적인 장비로, 게이트웨이라고도 함.
- 논리적으로 분리된 둘 이상의 네트워크를 연결
- 로컬 네트워크에서 브로드캐스트를 차단하여 네트워크를 분리
- 패킷의 최적 경로를 찾기 위한 라우팅 테이블 구성
- 패킷을 목적지까지 가장 빠르게 보내는 길잡이 역할 담당



(a) 소형 라우터



(b) 대형 라우터

그림 2-22 라우터



## 5. 네트워크 계층

### 5.4 라우팅

#### ■ 라우팅

```
Administrator: Command Prompt
C:\Users\Administrator>
C:\Users\Administrator>route PRINT
=====
Interface List
11...00 0c 29 97 13 8c .....Intel(R) PRO/1000 MT Network Connection
1.....Software Loopback Interface 1
=====

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
1 0.0.0.0                  0.0.0.0          192.168.0.1      192.168.0.100    266
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        306
127.0.0.1                  255.255.255.255  On-link          127.0.0.1        306
127 255.255.255.255        255.255.255.255  On-link          127.0.0.1        306
2 192.168.0.0              255.255.255.0    On-link          192.168.0.100    266
192.168.0.100              255.255.255.255  On-link          192.168.0.100    266
192.168.0.255              255.255.255.255  On-link          192.168.0.100    266
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        306
224.0.0.0                  240.0.0.0        On-link          192.168.0.100    266
255.255.255.255            255.255.255.255  On-link          127.0.0.1        306
255.255.255.255            255.255.255.255  On-link          192.168.0.100    266
=====
Persistent Routes:
Network Address            Netmask          Gateway Address  Metric
0.0.0.0                    0.0.0.0          192.168.0.1      Default
=====
```

그림 2-23 PC의 라우팅 테이블

### 5.4 라우팅

#### ■ 라우팅

- ① 라우팅 테이블에서 직접 구체적으로 지정한 주소 외의 모든 목적지 주소는 192.168.0.100 인터페이스를 통해 게이트웨이 192.168.0.1로 보내라는 의미
- 'tracert' 명령으로 200.200.200.200으로 시작하는 경로로 ICMP 패킷을 전송
- 200.200.200.200으로 목적지 IP가 설정된 패킷을 192.168.0.1로 보냄



```
Administrator: Command Prompt
C:\Users\Administrator>tracert 200.200.200.200

Tracing route to 200.200.200.200 over a maximum of 30 hops
  0  <1 ms  <1 ms  <1 ms  WindowsServer2012 [192.168.0.1]
  1  *      *      *      Request timed out.
```

그림 2-24 IP 주소 200.200.200.200에 대한 네트워크 경로 확인

### 5.4 라우팅

#### ■ 라우팅

- ② 로컬 네트워크에 있는 호스트이므로 192.168.0.1로 보내지 않고, 로컬 네트워크에서 상대방을 찾으라는 의미

- 넷마스크 값은 제어판의 네트워크 카드에서 설정하는 서브넷 마스크 값

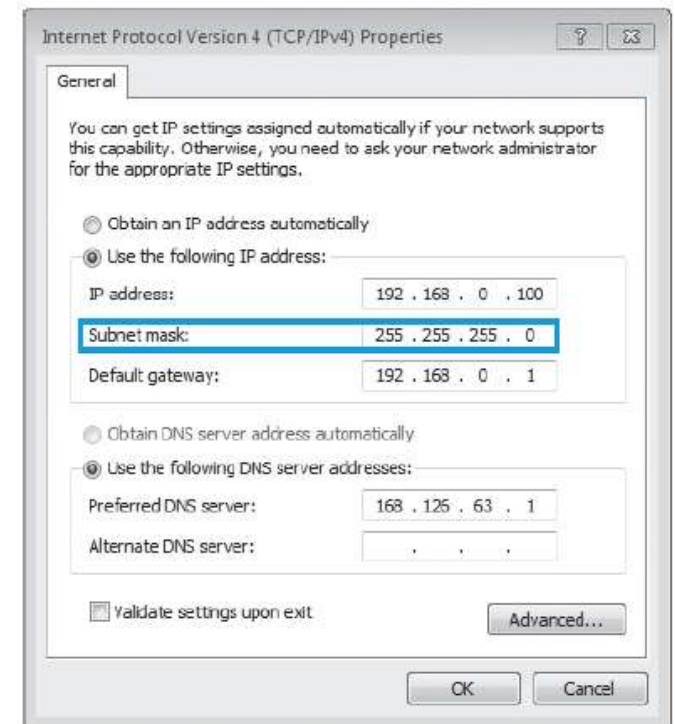


그림 2-25 LAN의 서브넷 마스크 설정

### 5.4 라우팅

#### ■ 정적 라우팅

- 관리자 권한으로 특정 경로를 통해서만 패킷이 지날 수 있도록 설정
- 네트워크 변경사항이 발생하면 라우팅 테이블을 수동으로 직접 고쳐야 함.
- 보안이 중요한 경우 선호

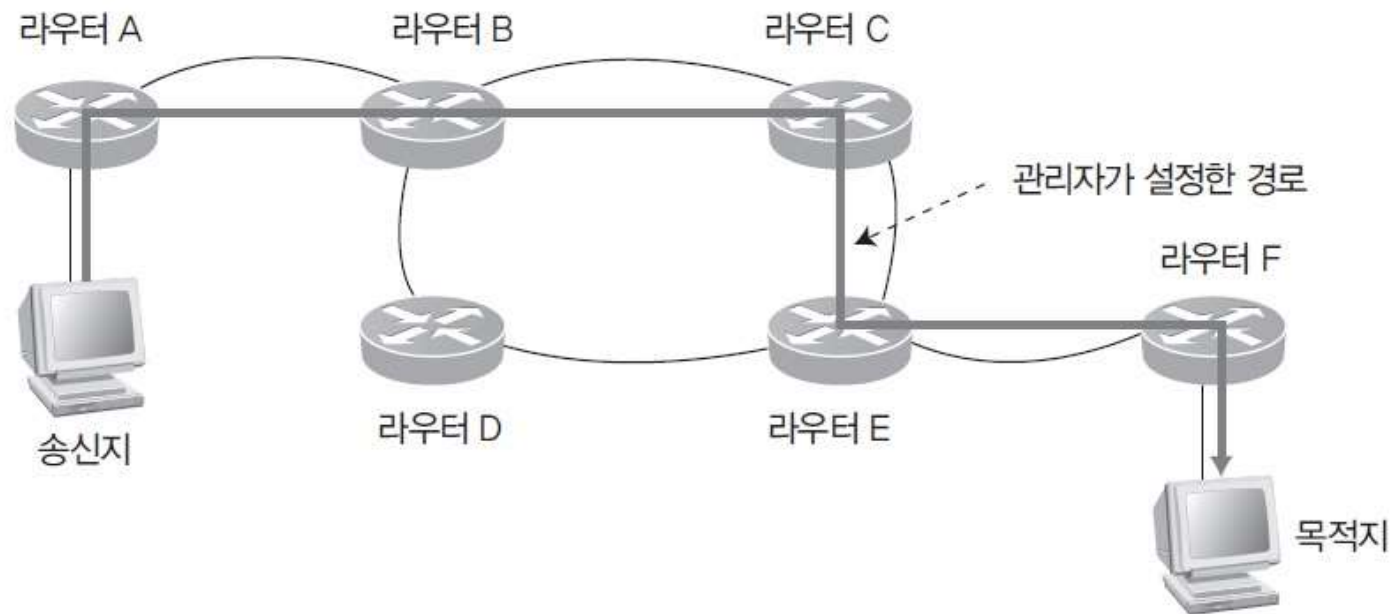


그림 2-26 정적 라우팅

### 5.4 라우팅

#### ■ 정적 라우팅의 특징

- 초기에 관리자가 다양한 라우팅 정보를 분석한 최적의 경로 설정 가능
- 라우팅 알고리즘을 통한 경로 설정이 이루어지지 않아 처리 부하 감소
- 네트워크 환경 변화에 대한 능동적인 대처가 어려움.
- 네트워크 환경 변화 시 관리자가 경로를 재산출하여 각 라우터에 제공해야 함.
- 비교적 환경 변화가 적은 형태의 네트워크에 적합

### 5.4 라우팅

#### ■ 동적 라우팅

- 라우터가 네트워크 연결 상태를 스스로 파악하여 최적의 경로를 선택해 전송
- 네트워크 연결 형태가 변경되어도 자동으로 문제를 해결

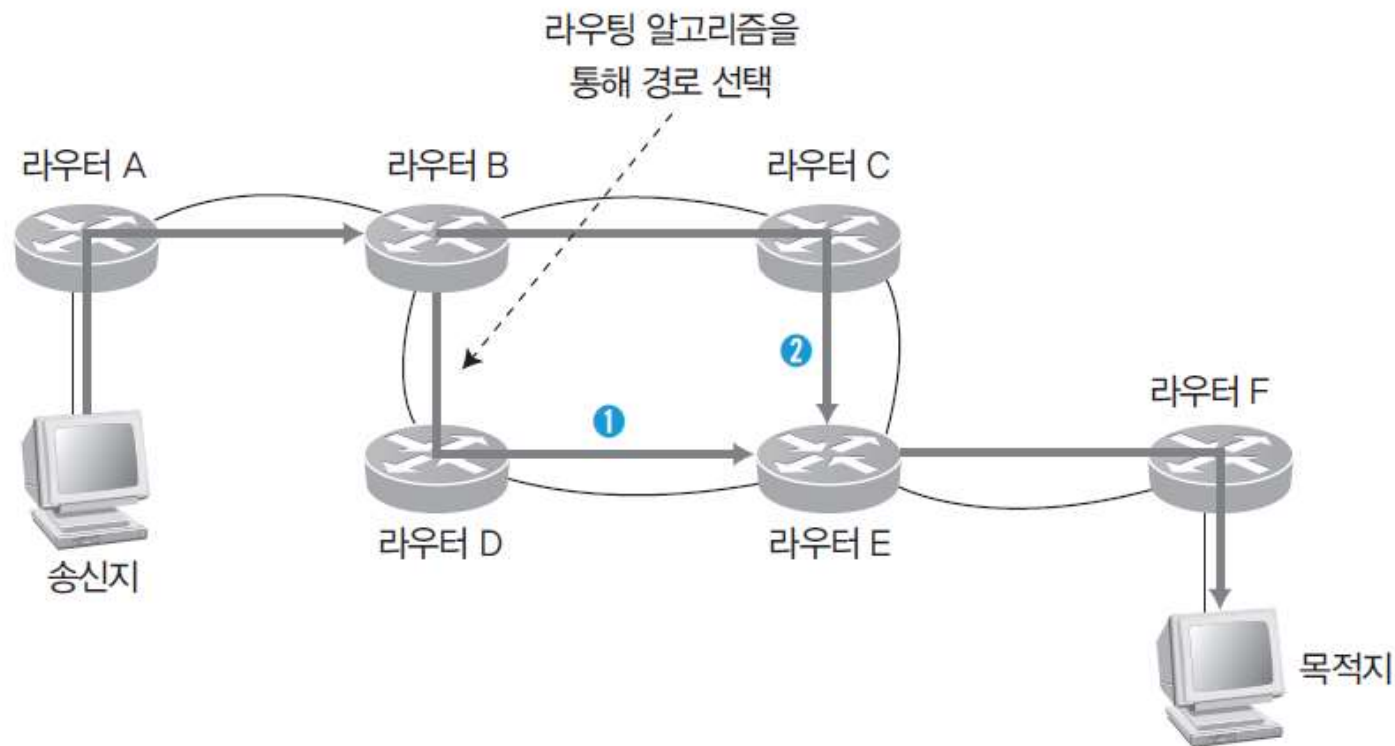


그림 2-27 동적 라우팅

### 5.4 라우팅

#### ■ 동적 라우팅의 특징

- 경로 설정이 실시간으로 이루어져 네트워크 환경 변화에 능동적으로 대처 가능
- 라우팅 알고리즘을 통해 자동으로 경로 설정이 이루어져 관리가 쉬움.
- 주기적인 라우팅 정보 송수신으로 인한 대역폭 낭비 초래
- 네트워크 환경 변화 시 라우터의 처리 부하 증가로 지연이 발생
- 수시로 환경이 변하는 형태의 네트워크에 적합

## 5.4 라우팅

### ■ 정적/동적 라우팅의 비교

표 2-9 정적/동적 라우팅의 비교

구분	정적 라우팅	동적 라우팅
라우팅 테이블 관리	<ul style="list-style-type: none"> <li>• 수동</li> <li>• 네트워크의 변화(라우터 추가/변경/회선 장애 등)에 대한 자동 인지 불가</li> </ul>	<ul style="list-style-type: none"> <li>• 자동</li> <li>• 네트워크의 변화를 자동으로 인지하여 정보 전송 경로를 재구성</li> </ul>
처리 부하	<ul style="list-style-type: none"> <li>• 라우팅 테이블의 갱신을 위한 별도의 부하 없음</li> <li>• CPU와 메모리에 부하 적음</li> <li>• 네트워크 장애의 실시간 관리를 위한 NMS와 각 라우터 간의 정보 전송이 많음(CPU에 부하 다소 발생)</li> </ul>	<ul style="list-style-type: none"> <li>• 라우팅 테이블의 갱신을 위해 라우터 간 정보 교환</li> <li>• CPU와 메모리에 부하 많음</li> <li>• 네트워크 장애를 실시간으로 관리할 필요가 없음</li> </ul>
백업 구성	<ul style="list-style-type: none"> <li>• 백업 구성이 곤란함</li> <li>• 별도의 네트워크 장비를 이용하여 회선 백업 가능</li> </ul>	<ul style="list-style-type: none"> <li>• 백업 구성이 쉬움(회선 장비)</li> </ul>
복구 기능	<ul style="list-style-type: none"> <li>• 백업 회선이 있는 경우, 회선 장애 시 수 초 내로 복구 가능</li> <li>• 기타 장애 시 최소 10분 이상의 복구 시간 필요(백본 라우터 장애 시 30분 이상 소요)</li> </ul>	<ul style="list-style-type: none"> <li>• 백업 회선이 있는 경우 수 초 내로 복구 가능</li> </ul>
인터페이스	<ul style="list-style-type: none"> <li>• 변경이 적을 때 유리</li> </ul>	<ul style="list-style-type: none"> <li>• 변경이 많을 때 유리</li> </ul>
노드 추가/변경/확대	<ul style="list-style-type: none"> <li>• 운영 요원이 라우팅 작업</li> </ul>	<ul style="list-style-type: none"> <li>• 대처 용이</li> </ul>
중간 경로	<ul style="list-style-type: none"> <li>• 단일 경로에 적합</li> </ul>	<ul style="list-style-type: none"> <li>• 다중 경로에 적합</li> </ul>



### 6.1 전송 계층에 대한 이해

#### ■ 4계층 : 전송 계층(Transport Layer)

- 대표 프로토콜은 TCP(Transmission Control Protocol)
- TCP가 가진 주소를 포트(Port)라 하며 0~65535( $2^{16}-1$ )번까지 존재
- 0~1023번(1,024)을 잘 알려진 포트(Well Known Port)라고 부름(보통 0번 포트는 사용하지 않음).

Registered port: 1024 ~ 49151  
Dynamic port : 49152 ~ 65535

표 2-10 주요 포트와 서비스

포트 번호	서비스	포트 번호	서비스
20	FTP-Data	80	HTTP
21	FTP	110	POP3
23	Telnet	111	RPC
25	SMTP	138	NetBIOS
53	DNS	143	IMAP
69	TFTP	161	SNMP

## 6. 전송 계층

### 6.1 전송 계층에 대한 이해

#### ■ 패킷 구조와 예

- 출발지 포트는 보통 1024번부터 65535번 사이에서 사용하지 않는 임의의 포트를 응용 프로그램별로 할당하여 사용
- 클라이언트가 웹 서버에 접속할 때 패킷 구조(서비스 포트는 보통 80번)

01001010101	출발지 포트	80	출발지 IP	목적지 IP	출발지 MAC	목적지 MAC
5계층까지의 패킷 정보	4계층 패킷 정보		3계층 패킷 정보		2계층 패킷 정보	

- 시스템에서 임의로 포트를 할당한 출발지 패킷 구조

01001010101	3405	80	출발지 IP	목적지 IP	출발지 MAC	목적지 MAC
5계층까지의 패킷 정보	4계층 패킷 정보		3계층 패킷 정보		2계층 패킷 정보	

### 6.2 전송 계층 프로토콜

---

#### ■ TCP(Transmission Control Protocol)

- 연결 지향형 프로토콜
- IP와 함께 통신을 하는 데 반드시 필요한 가장 기본적인 프로토콜

#### ■ TCP의 특징

- 높은 신뢰성
- 가상 회선 연결 방식
- 연결의 설정과 해제
- 데이터 체크섬
- 시간 초과와 재전송
- 데이터 흐름 제어

## 6. 전송 계층

### 6.2 전송 계층 프로토콜

#### ■ TCP 패킷의 구조

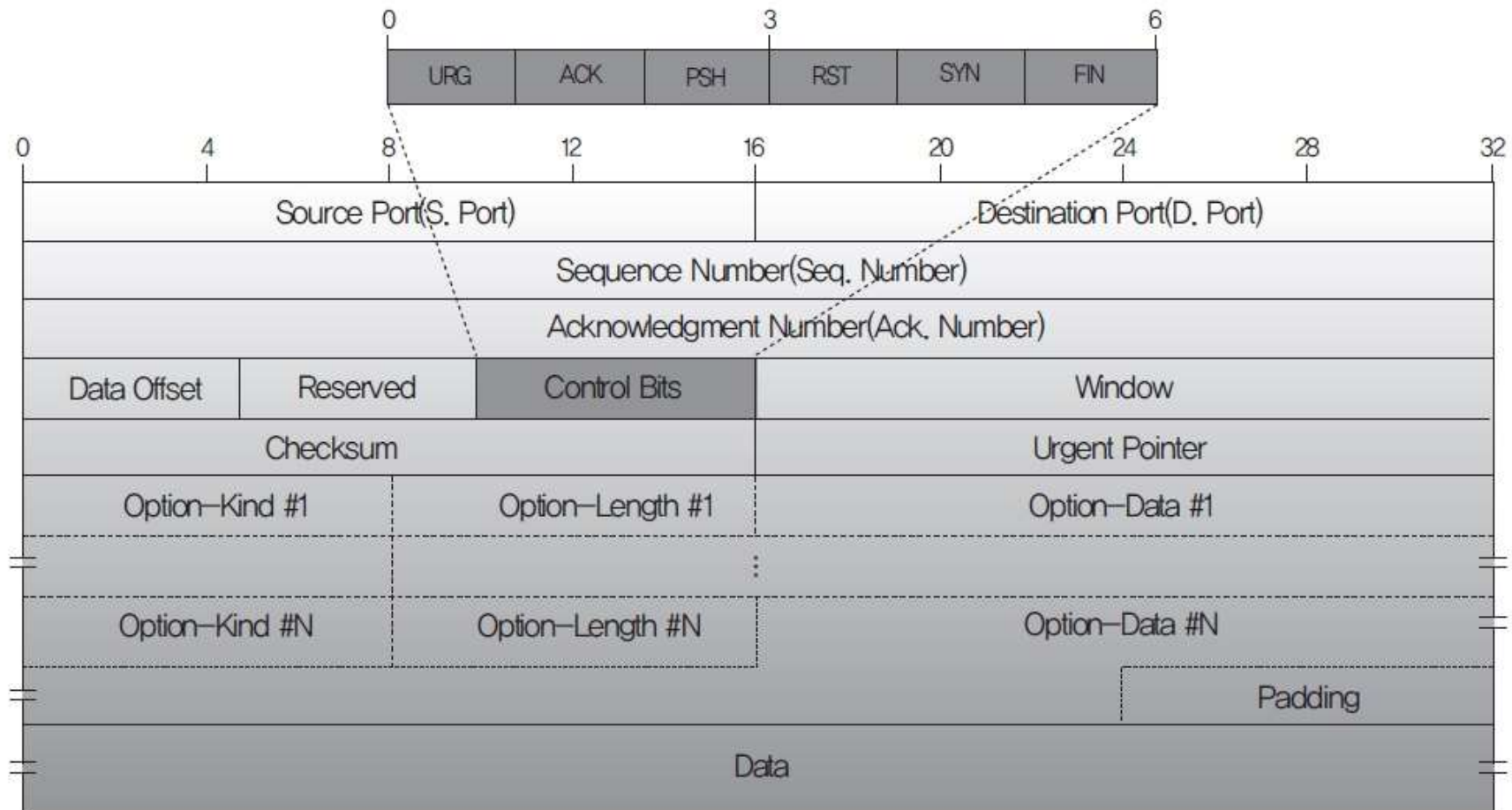


그림 2-29 TCP 헤더

### 6.2 전송 계층 프로토콜

#### ■ TCP 패킷의 내용

표 2-11 TCP 패킷의 내용

필드 이름	길이	내용
S.Port	2Bytes	Source Port. 패킷의 출발지 포트 번호를 가리키며 0~65535 값 중 하나이다.
D.Port	2Bytes	Destination Port. 패킷의 목적지 포트 번호다.
Seq. Number	4Bytes	Sequence Number. 패킷의 순서 값이다.
Ack. Number	4Bytes	Acknowledgment Number. 통신 상대의 패킷 순서 값이다.
Data Offset	4bits	TCP 패킷 헤더의 길이를 나타내는데, 32bits(4Bytes)가 몇 행인지를 가리킨다. 최소 값은 5다.
Reserved	6bits	나중에 필요할 때 사용하려고 남겨둔 공간이다.
Control Bits	6bits	6개의 비트는 각각 다음과 같이 TCP 패킷의 종류와 특성을 가리킨다. 예를 들어, ACK와 FIN 값이 1이면 Control Bits는 010001이 될 것이다. <ul style="list-style-type: none"><li>- URG(Urgent): 1이면 헤더의 마지막 필드인 긴급 포인터의 내용을 실행</li><li>- ACK(Acknowledgment): 1이면 확인 번호 필드가 유효</li><li>- PSH(Push): 1이면 송신자에게 높은 처리율을 요구</li><li>- RST(Reset): 1이면 TCP 연결을 다시 설정</li><li>- SYN(Synchronize): 1이면 연결 요청과 설정, 확인 응답에서 순서 번호를 동기화</li><li>- FIN(Finish): 1이면 TCP 연결을 종료</li></ul>

### 6.2 전송 계층 프로토콜

#### ■ TCP 패킷의 내용

표 2-11 TCP 패킷의 내용

필드 이름	길이	내용
Window	2Bytes	TCP에서는 흐름 제어를 할 때 슬라이딩 윈도우와 혼잡 윈도우 방법을 사용한다. - 슬라이딩 윈도우(Sliding Window) : 데이터를 한 번에 처리할 수 있는 버퍼의 용량을 의미하는 윈도우의 개념을 사용한다. 슬라이딩 윈도우는 송신 시스템이 전송한 전체 세그먼트에 대한 확인 메시지를 수신하기 전에 다른 세그먼트를 전송할 수 있게 해준다. - 혼잡 윈도우(Congestion Window) : 네트워크 혼잡 문제를 해결하기 위해 송신 시스템이 사용하는 방법이다. 네트워크 혼잡이 발견되면 보내는 데이터의 양을 조절하여 줄이고 혼잡이 줄어들면 다시 원래 보내던 만큼 데이터 양을 늘린다.
Checksum	2Bytes	데이터 오류 검출을 위한 값이다.
Urgent Pointer	2Bytes	Control Bits가 URG인 경우에 현재 전송되는 데이터와 관계없는 TCP 데이터를 보내 우선 처리할 때 사용한다. 이때 우선 처리하려는 긴급 데이터의 마지막 바이트 위치를 Urgent Pointer로 나타낸다.
Options	가변	옵션의 종류와 길이, 데이터를 저장한다.
Padding	가변	옵션이 32bits가 안 되면 나머지 비트를 0으로 채운다.
Data	가변	전송하고자 하는 데이터를 저장한다.

## 6. 전송 계층

### 6.2 전송 계층 프로토콜

#### ■ 연결 설정 과정(Three-Way Handshaking)

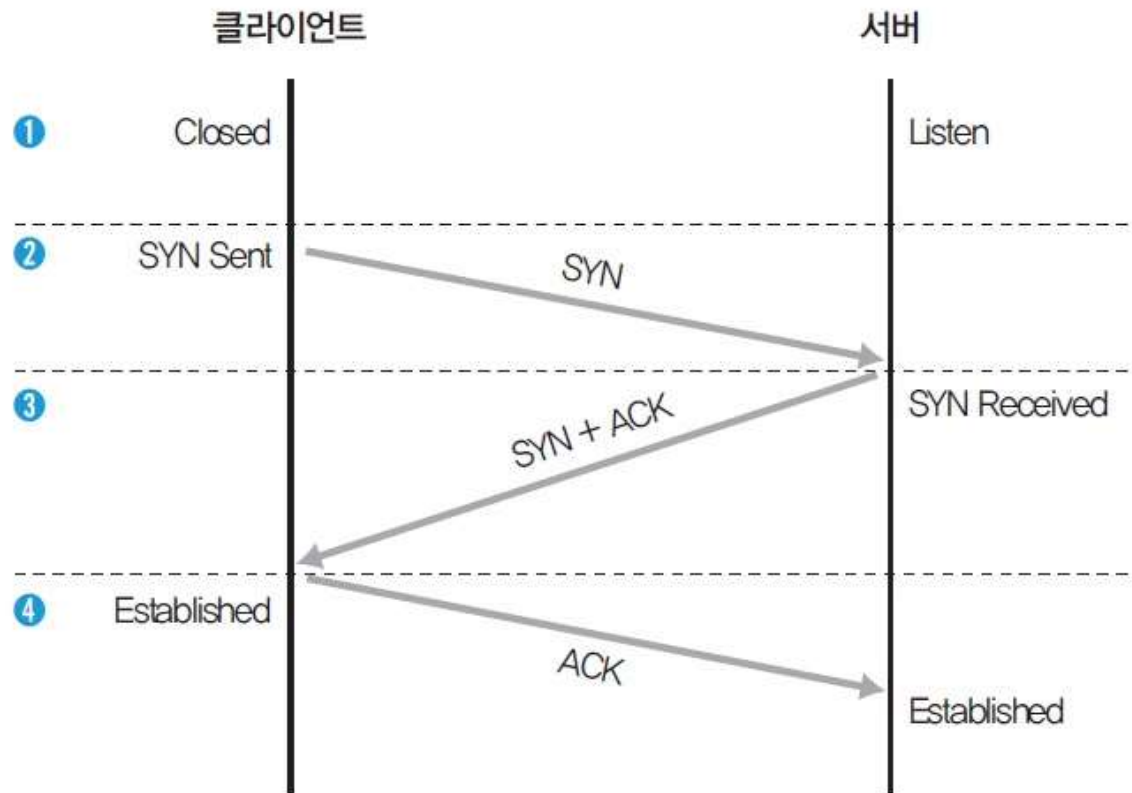


그림 2-30 TCP에서 연결 생성 과정



## 6. 전송 계층

### 6.2 전송 계층 프로토콜

#### ■ 연결 해제 과정

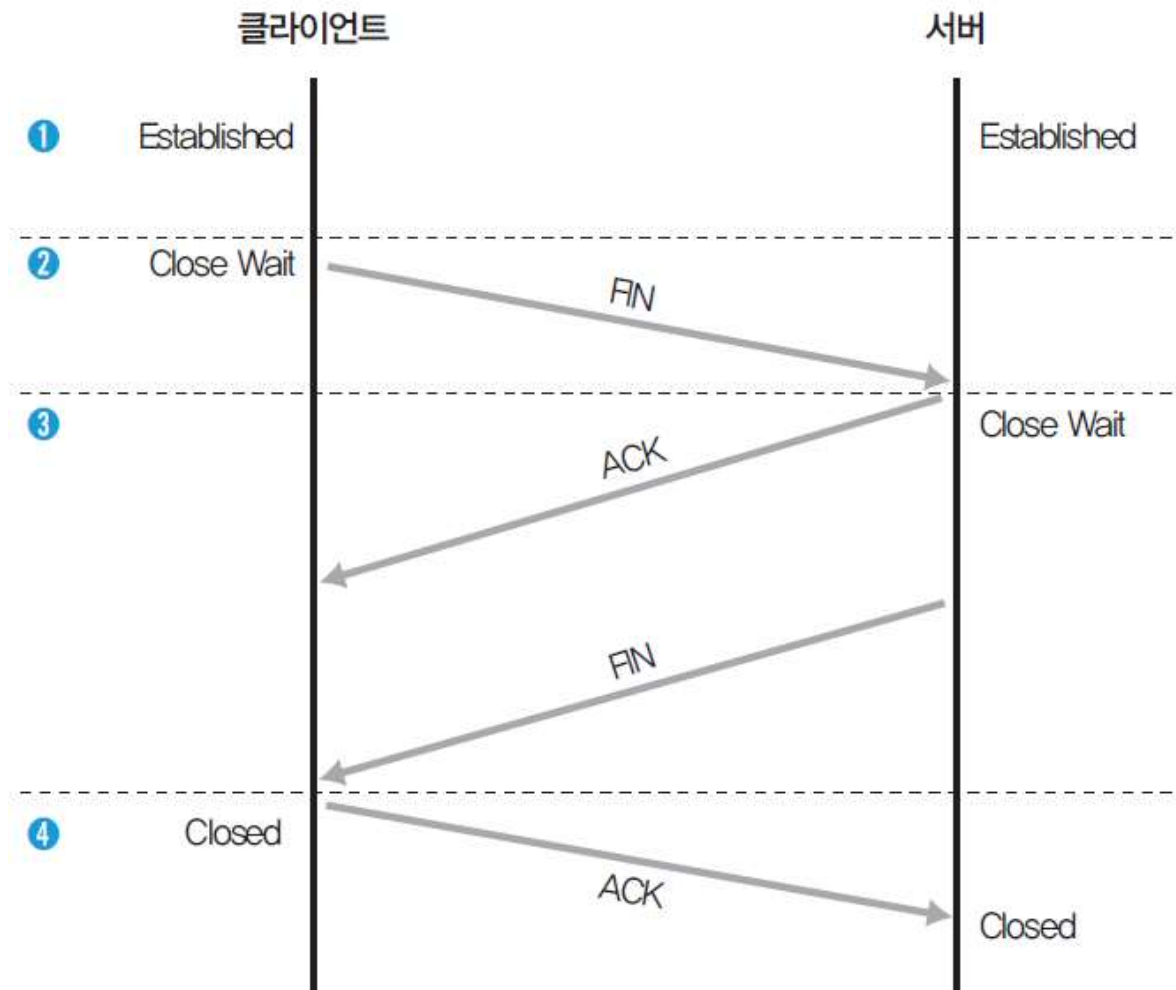


그림 2-31 TCP에서 연결 해제 과정



### 6.2 전송 계층 프로토콜

#### ■ UDP(User Datagram Protocol)

- 비연결 지향형 프로토콜
- 상대방이 보낸 응답을 확인하지 않아 네트워크에 부하를 주지 않음.
- 데이터 자체의 신뢰성이 없어 수신한 데이터의 무결성을 보장받지 못함.

#### ■ UDP의 특징

- 비연결 지향형
- 네트워크 부하 감소
- 비신뢰성
- 전송된 데이터의 일부가 손실됨.

### 6.2 전송 계층 프로토콜

#### ■ UDP 패킷의 구조

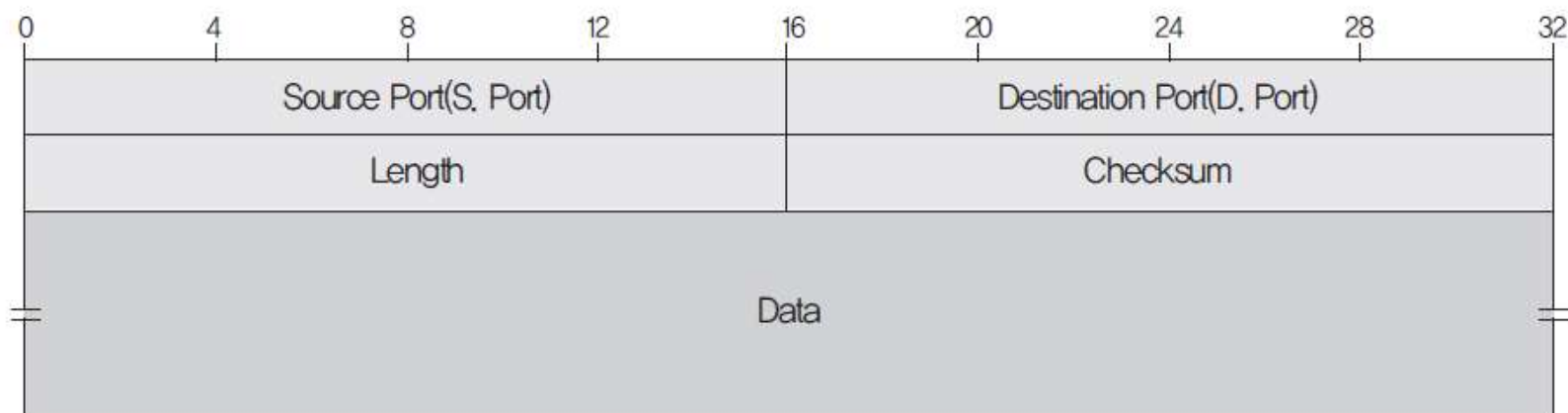


그림 2-32 UDP 패킷 구조

### 6.2 전송 계층 프로토콜

#### ■ UDP 패킷의 내용

표 2-12 UDP 패킷의 내용

필드 이름	길이	내용
S.Port	2Bytes	Source Port. 패킷의 출발지 포트 번호로, 0~65535 값 중 하나다.
D.Port	2Bytes	Destination Port. 패킷의 목적지 포트 번호다.
Length	2Bytes	UDP 헤더와 데이터 필드를 포함한 전체 패킷의 길이다.
Checksum	2Bytes	데이터 오류 검출을 위한 값이다.
Data	가변	전송하고자 하는 데이터를 저장한다.

### 7.1 응용 계층 프로토콜

#### ■ 7계층 : 응용 계층(Application Layer)

- 관련 응용 프로그램이 별도로 존재하며, 여러 가지 프로토콜에 대하여 사용자 인터페이스를 제공

#### ■ FTP(File Transfer Protocol, 20,21)

- 파일 전송을 위한 가장 기본적인 프로토콜
- 1972년 텔넷과 함께 표준으로 제정
- 클라이언트와 서버가 대화형으로 통신 가능

#### ■ Telnet(텔넷, 23)

- 사용자가 원격에 있는 서버에 로그인하도록 TCP 연결을 설정
- 단말기가 원격 컴퓨터 바로 옆에 있는 것처럼 직접 조작할 수 있게 해줌.

### 7.1 응용 계층 프로토콜

---

#### ■ SMTP(Simple Mail Transfer Protocol, 25)

- 메일 서비스

#### ■ DNS(Domain Name System, 53)

- 도메인 이름 주소를 통해 IP 주소를 확인할 수 있는 프로토콜

#### ■ TFTP(Trivial File Transfer Protocol, 69)

- 파일을 전송하는 프로토콜
- UDP 패킷을 사용하고, 인증 기능을 제공하지 않음.

#### ■ HTTP(HyperText Transfer Protocol, 80)

- 인터넷을 위해 사용하는 가장 기본적인 프로토콜

### 7.1 응용 계층 프로토콜

#### ■ POP3 & IMAP

- POP3(110) : 메일 서버로 전송된 메일을 확인할 때 사용하는 프로토콜
- IMAP(143) : POP3와 기본적으로 같으나, 메일을 읽은 후 메일이 서버에 남음.

#### ■ RPC(Remote Procedure Call, 111)

- 썬(Sun)의 Remote Procedure Call을 나타냄.

#### ■ NetBIOS(Network Basic Input/Output System, 138)

- 기본적인 사무기기와 윈도우 시스템 간의 파일 공유를 위한 것
- NBT(NetBIOS over TCP) 프로토콜을 사용하여 원격의 인터넷으로 전달이 가능

#### ■ SNMP(Simple Network Management Protocol, 161)

- 네트워크 관리와 모니터링을 위한 프로토콜

## 8. 계층별 패킷 분석

### 실습 2-1 Wireshark 설치하고 실행하기

실습환경 • 인터넷이 연결된 클라이언트 시스템(윈도우XP)

#### ① Wireshark 다운로드와 설치하기

- <http://www.wireshark.org>에서 다운로드
- 패킷을 스니핑하는 데 필요한 WinPcap 함께 설치

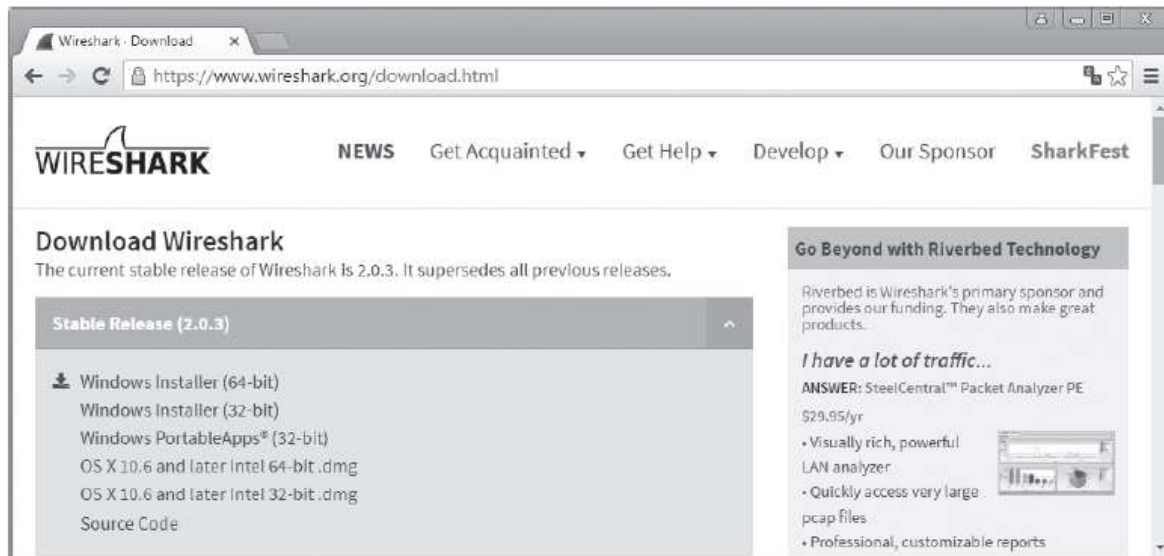


그림 2-33 Wireshark 다운로드 페이지

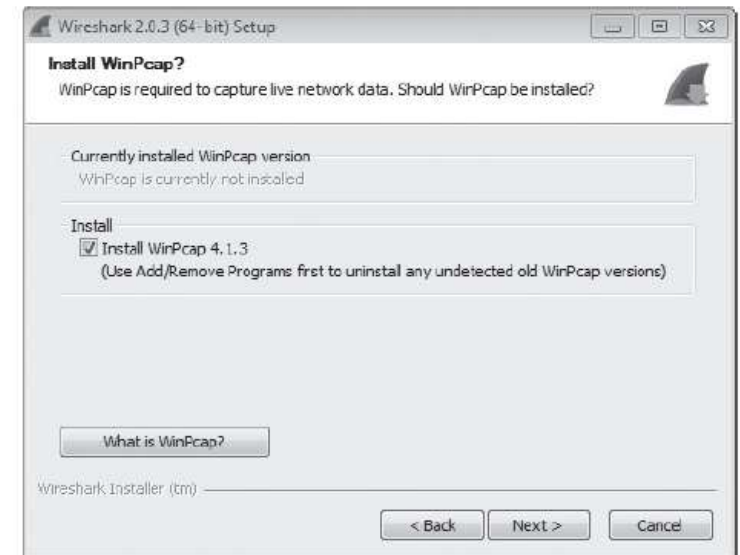


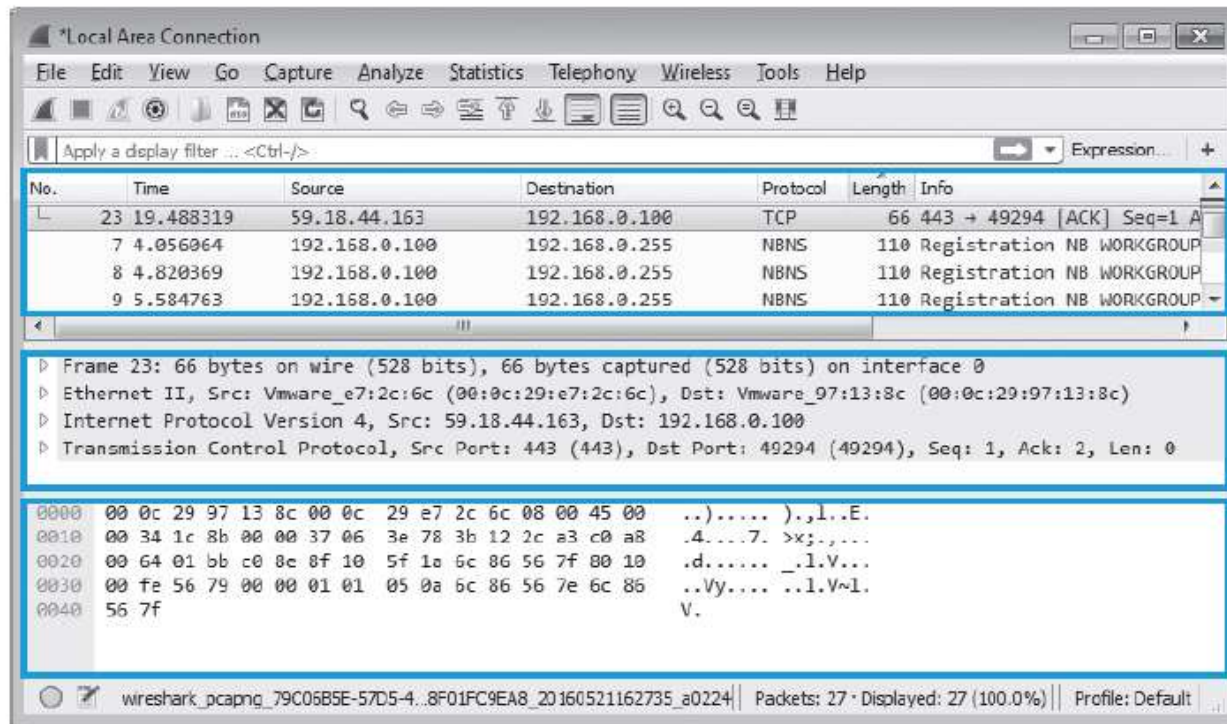
그림 2-34 설치 옵션에서 WinPcap 설치

## 8. 계층별 패킷 분석

### 실습 2-1 Wireshark 설치하고 실행하기

#### ② Wireshark 실행하기

- Wireshark를 실행한 후 [Capture]-[Options] 메뉴를 선택하여 아무 인터페이스 선택 후 패킷을 스니핑



① 패킷 선택

② 각 계층별 패킷 정보 열람

③ 해당 부분이 별도 표시됨.

그림 2-36 패킷을 캡처하고 있는 상태



## 8. 계층별 패킷 분석

### 실습 2-1 Wireshark 설치하고 실행하기

#### ② Wireshark 실행하기

- Wireshark에서 [Capture]-[Capture Filters] 메뉴를 사용하면 특정 프로토콜만 선택하여 캡처할 수 있음.

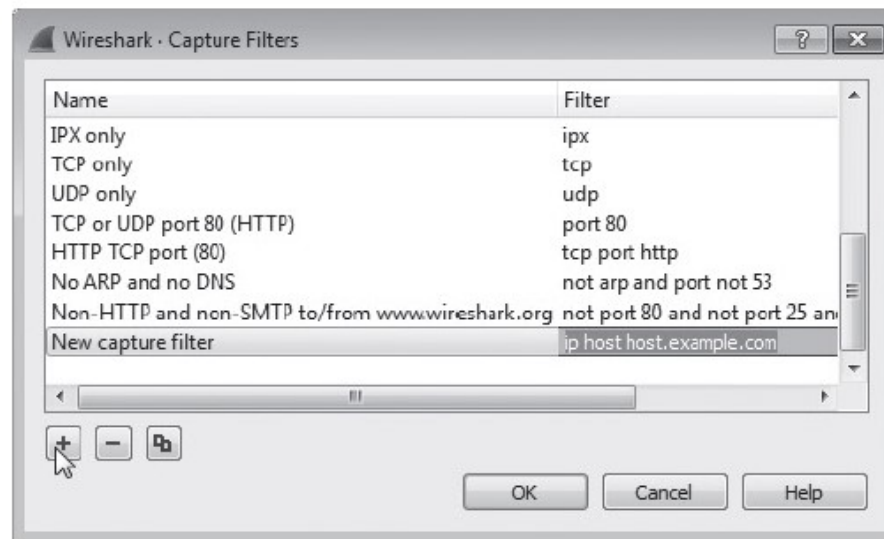


그림 2-37 특정 패킷만 캡처하기 위한 옵션

## 8. 계층별 패킷 분석

### 실습 2-2 데이터 링크 계층의 패킷 분석하기

- 실습환경**
- 스위치 또는 허브에 연결된 클라이언트(윈도우 7)와 서버 시스템(윈도우 서버 2012, IIS 설치)
  - 필요 프로그램 : Wireshark(서버와 클라이언트 각각에 설치)

#### ① 2계층에서 OSI 계층의 패킷 흐름 이해하기

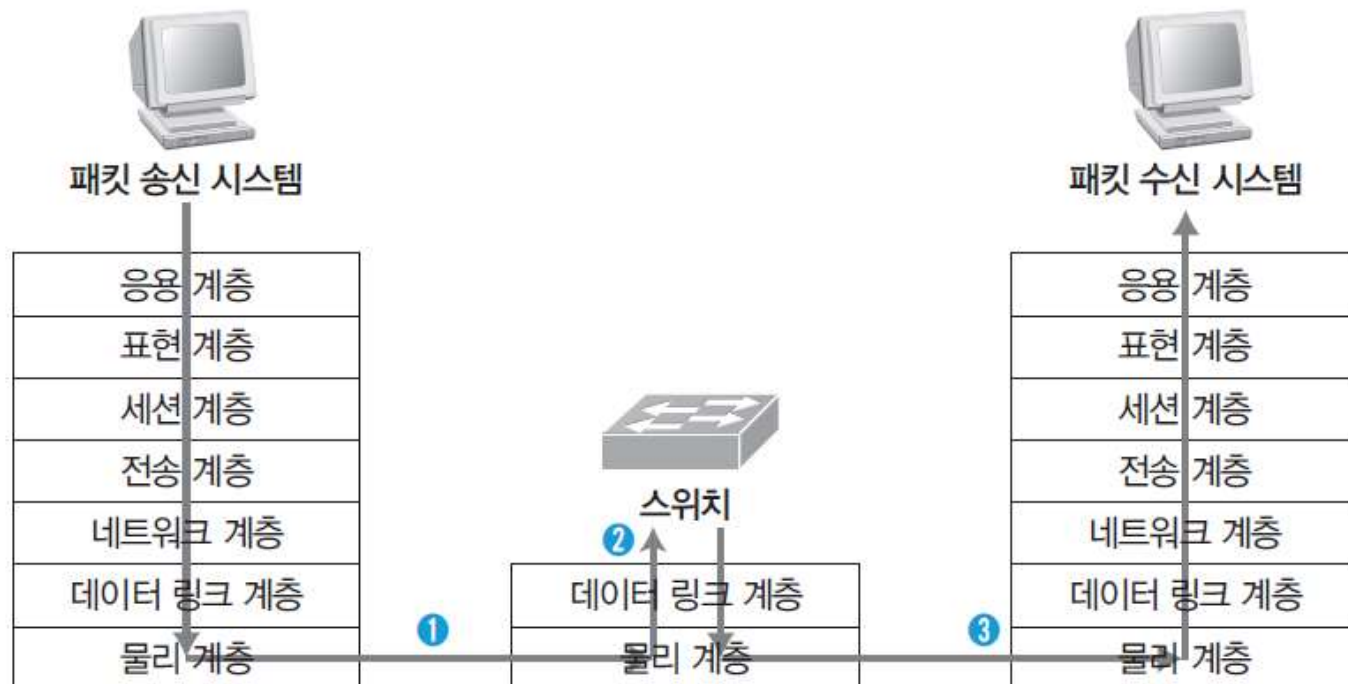


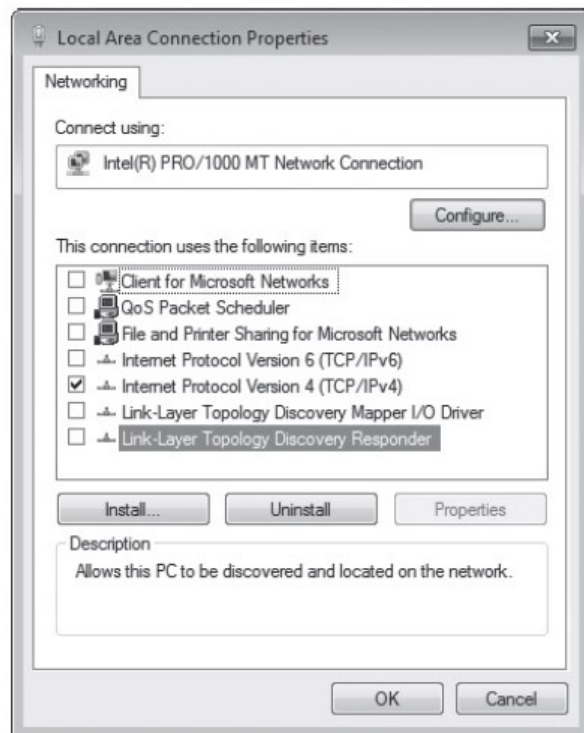
그림 2-39 2계층에서 OSI 계층의 패킷 흐름

## 8. 계층별 패킷 분석

### 실습 2-2 데이터 링크 계층의 패킷 분석하기

#### ② 패킷 캡처 준비하기

- 불필요한 패킷 생성을 막기 위해 [제어판]-[네트워크 연결]을 선택
- '인터넷 프로토콜(IP/TCP)'만 활성화하고, 다른 프로토콜은 모두 비활성화
- 클라이언트 IP, 서버 IP 설정 후 MAC 주소 확인



클라이언트 IP	192.168.0.101	서버 IP	192.168.0.100
클라이언트 MAC	00:16:D3:CA:85:67	서버 MAC	00:13:8F:53:2F:79

그림 2-40 Internet Protocol Version 4(TCP/IPv4)만 활성화

## 8. 계층별 패킷 분석

### 실습 2-2 데이터 링크 계층의 패킷 분석하기

#### ③ 패킷 캡처하기

- 서버와 클라이언트의 Wireshark를 실행시키고 클라이언트의 랜 선을 스위치에 연결한 후 웹 브라우저로 서버의 IIS에 접속
- 클라이언트로 IIS 서버에 접속하는 과정이 끝나면 Wireshark를 중단

#### ④ 패킷 분석하기

1	0.000000	Wistron_ca:85:67	Broadcast	ARP	who has 192.168.0.100? Tell 192.168.0.101
2	0.000384	Asiarock_53:2f:79	Wistron_ca:85:67	ARP	192.168.0.100 is at 00:13:8f:53:2f:79
3	0.000394	192.168.0.101	192.168.0.100	TCP	fpitp > http [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=2
4	0.000726	192.168.0.100	192.168.0.101	TCP	http > fpitp [SYN, ACK] Seq=0 Ack=1 win=16384 Len=0 MS
5	0.000767	192.168.0.101	192.168.0.100	TCP	fpitp > http [ACK] Seq=1 Ack=1 win=261340 [TCP CHECKSUM
6	0.000944	192.168.0.101	192.168.0.100	HTTP	GET / HTTP/1.1
7	0.002702	192.168.0.100	192.168.0.101	TCP	[TCP segment of a reassembled PDU]
8	0.002738	192.168.0.100	192.168.0.101	HTTP	HTTP/1.1 200 OK (text/html)
9	0.002767	192.168.0.101	192.168.0.100	TCP	fpitp > http [ACK] Seq=322 Ack=1604 win=261340 [TCP CH
10	0.040856	192.168.0.101	192.168.0.100	HTTP	GET /pagerror.gif HTTP/1.1
11	0.061877	192.168.0.100	192.168.0.101	TCP	[TCP segment of a reassembled PDU]
12	0.062265	192.168.0.100	192.168.0.101	TCP	[TCP segment of a reassembled PDU]
13	0.062285	192.168.0.100	192.168.0.101	HTTP	HTTP/1.1 200 OK (GIF89a)

그림 2-41 클라이언트의 Wireshark에 캡처된 패킷 목록

### 실습 2-2 데이터 링크 계층의 패킷 분석하기

#### ④ 패킷 분석하기

- 클라이언트는 랜에서 IP가 192.168.0.100인 시스템이 누구인지 브로드캐스팅

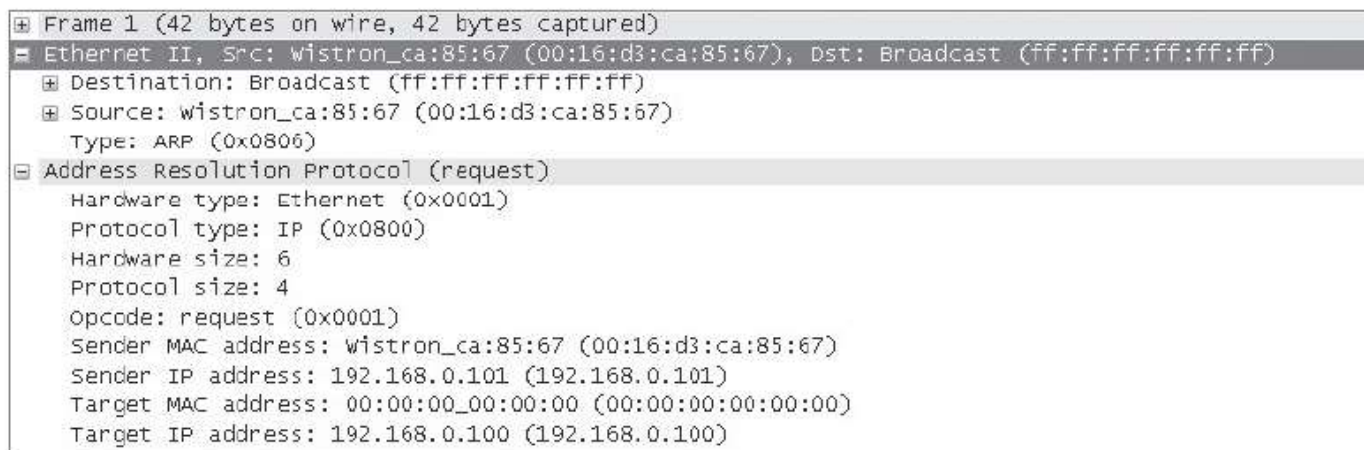


그림 2-42 ARP를 통한 MAC 주소 확인 요청 패킷

### 실습 2-2 데이터 링크 계층의 패킷 분석하기

#### ④ 패킷 분석하기

- 자신의 IP인 서버가 응답으로 자신의 MAC주소를 다음 패킷을 통해 시스템에 보냄.

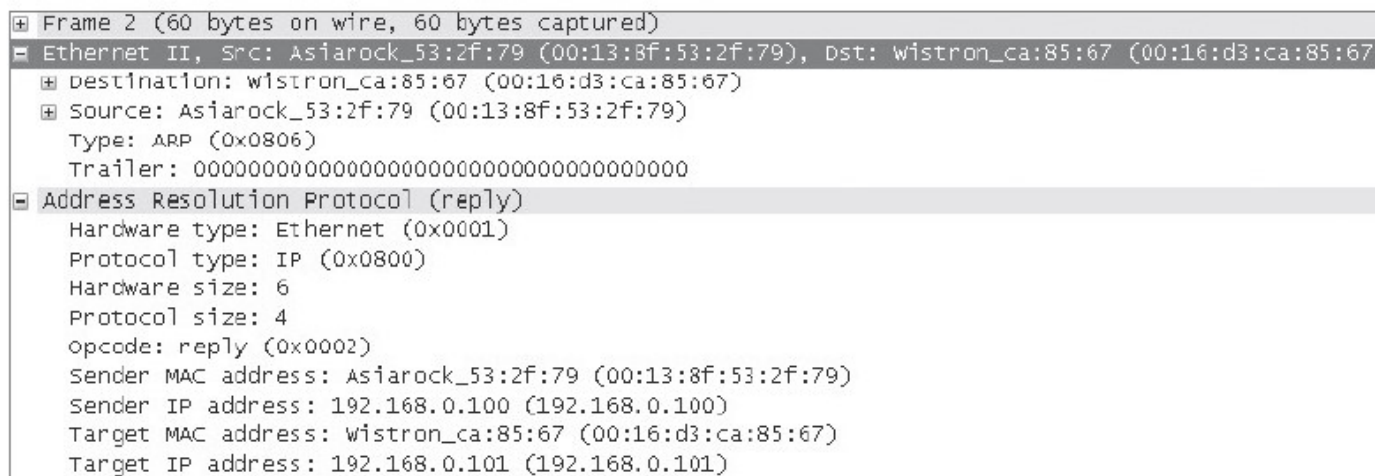
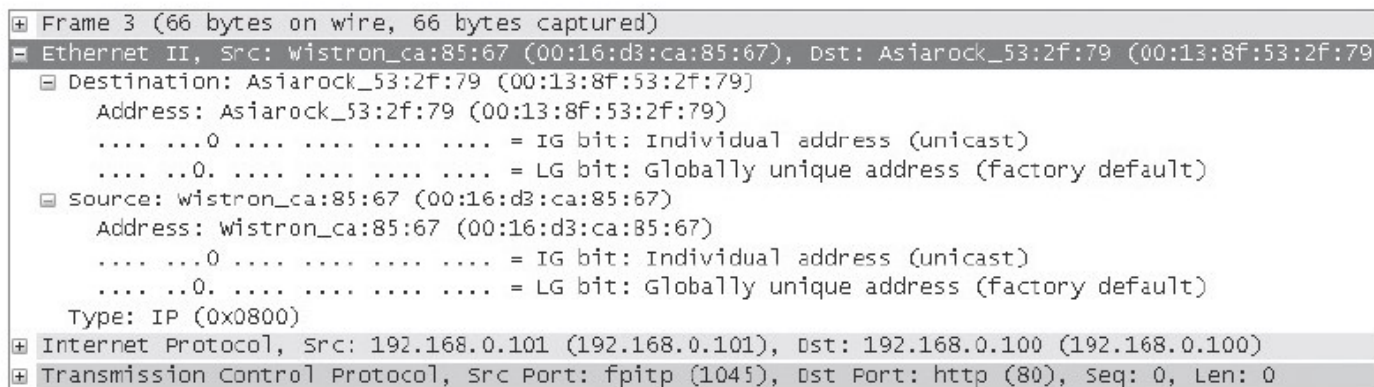


그림 2-43 ARP를 통한 MAC 주소 응답 패킷

### 실습 2-2 데이터 링크 계층의 패킷 분석하기

#### ④ 패킷 분석하기

- 서버와 클라이언트가 서로의 MAC 주소를 확인한 후, 클라이언트는 HTTP 연결을 위해 패킷을 보냄.



```
Frame 3 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: Wistron_ca:85:67 (00:16:d3:ca:85:67), Dst: Asiarock_53:2f:79 (00:13:8f:53:2f:79)
  Destination: Asiarock_53:2f:79 (00:13:8f:53:2f:79)
    Address: Asiarock_53:2f:79 (00:13:8f:53:2f:79)
      ....0.... = IG bit: Individual address (unicast)
      ....0.... = LG bit: Globally unique address (factory default)
  Source: Wistron_ca:85:67 (00:16:d3:ca:85:67)
    Address: Wistron_ca:85:67 (00:16:d3:ca:85:67)
      ....0.... = IG bit: Individual address (unicast)
      ....0.... = LG bit: Globally unique address (factory default)
  Type: IP (0x0800)
Internet Protocol, Src: 192.168.0.101 (192.168.0.101), Dst: 192.168.0.100 (192.168.0.100)
Transmission Control Protocol, Src Port: ftp (1045), Dst Port: http (80), Seq: 0, Len: 0
```

그림 2-44 서로의 MAC 주소 확인 후 최초로 전송되는 HTTP 패킷

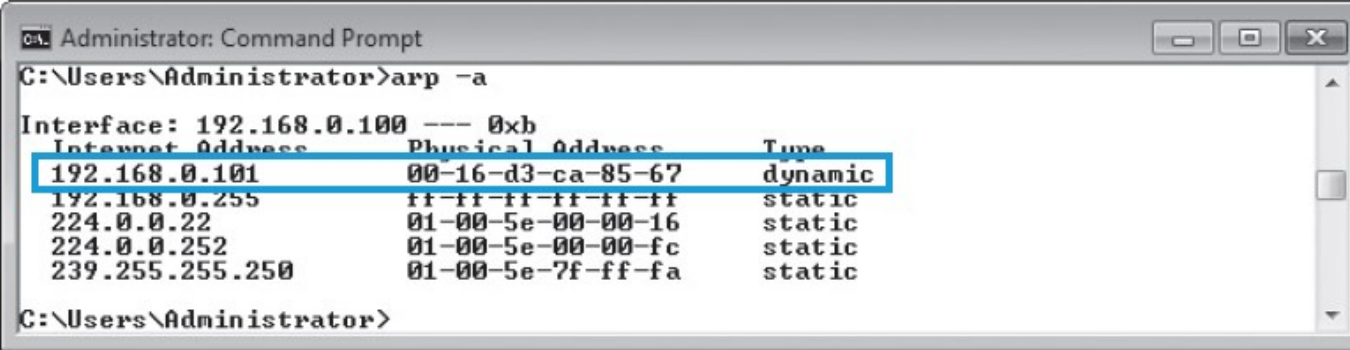


## 8. 계층별 패킷 분석

### 실습 2-2 데이터 링크 계층의 패킷 분석하기

#### ④ 패킷 분석하기

- 통신하는 사이 서버와 클라이언트는 상대방 MAC 주소를 각자의 ARP 테이블에 저장
- ARP 테이블의 내용은 arp -a 명령을 통해 확인



```
Administrator: Command Prompt
C:\Users\Administrator>arp -a

Interface: 192.168.0.100 --- 0xb
Internet Address      Physical Address      Type
192.168.0.101         00-16-d3-ca-85-67     dynamic
192.168.0.255         ff-ff-ff-ff-ff-ff     static
224.0.0.22            01-00-5e-00-00-16     static
224.0.0.252           01-00-5e-00-00-fc     static
239.255.255.250       01-00-5e-7f-ff-fa     static

C:\Users\Administrator>
```

그림 2-45 통신 중 서버측의 ARP 테이블



## 8. 계층별 패킷 분석

### 실습 2-3 네트워크 계층의 패킷 분석하기

**실습환경** • IP 공유기에 연결된 클라이언트(윈도우 7)와 서버 시스템(윈도우 서버 2012, IIS 설치)  
• 필요 프로그램 : Wireshark(서버와 클라이언트 각각에 설치)

#### ① 3계층에서 OSI 계층의 패킷 흐름 이해하기



그림 2-47 3계층에서 OSI 계층의 패킷 흐름

## 8. 계층별 패킷 분석

### 실습 2-3 네트워크 계층의 패킷 분석하기

#### ② 패킷 캡처하기

- 서버를 IP 공유기의 WAN 포트에 연결하고 클라이언트는 일반 포트에 연결
- 불필요한 프로토콜 제거
- 서버와 클라이언트의 Wireshark를 실행하고, 웹 브라우저로 서버의 IIS에 접속
- 클라이언트와 서버, 라우터 내·외부 포트의 MAC 주소와 IP 필요

클라이언트	클라이언트 IP	192.168.0.101
	클라이언트 MAC	00:16:D3:CA:85:67
라우터	IP 공유기 내부 인터페이스 IP	192.168.0.1
	IP 공유기 내부 인터페이스 MAC	00:08:9F:8A:39:9C
	IP 공유기 외부(WAN) 인터페이스 IP	200.200.200.1
	IP 공유기 외부(WAN) 인터페이스 MAC	00:08:9F:8B:39:9C
서버	서버 IP	200.200.200.2
	서버 MAC	00:13:8F:53:2F:79

## 8. 계층별 패킷 분석

### 실습 2-3 네트워크 계층의 패킷 분석하기

#### ③ 패킷 분석하기

1	0.000000	192.168.0.101	200.200.200.2	TCP	icmp > http [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=2
2	0.001076	200.200.200.2	192.168.0.101	TCP	http > icmp [SYN, ACK] Seq=0 Ack=1 win=16384 Len=0 MS
3	0.001114	192.168.0.101	200.200.200.2	TCP	icmp > http [ACK] Seq=1 Ack=1 win=261340 [TCP CHECKSU
4	0.001320	192.168.0.101	200.200.200.2	HTTP	GET / HTTP/1.1
5	0.129153	200.200.200.2	192.168.0.101	TCP	http > icmp [ACK] Seq=1 Ack=409 win=65127 Len=0
6	0.370280	200.200.200.2	192.168.0.101	TCP	[TCP segment of a reassembled PDU]
7	0.370321	200.200.200.2	192.168.0.101	HTTP	HTTP/1.1 200 OK (text/html)
8	0.370359	192.168.0.101	200.200.200.2	TCP	icmp > http [ACK] Seq=409 Ack=1604 win=261340 [TCP CH
9	0.370615	192.168.0.101	200.200.200.2	TCP	icmp > http [RST, ACK] Seq=409 Ack=1604 win=0 Len=0
10	0.372962	192.168.0.101	200.200.200.2	TCP	ltp-deepspace > http [SYN] Seq=0 win=65535 Len=0 MSS
11	0.373548	200.200.200.2	192.168.0.101	TCP	http > ltp-deepspace [SYN, ACK] Seq=0 Ack=1 win=1638
12	0.373579	192.168.0.101	200.200.200.2	TCP	ltp-deepspace > http [ACK] Seq=1 Ack=1 win=261340 [T

그림 2-48 클라이언트에서 캡처한 패킷 목록

1	0.000000	200.200.200.1	200.200.200.2	TCP	icmp > http [SYN] Seq=0 win=65535 Len=0 MSS=1460 WS=2
2	0.000059	200.200.200.2	200.200.200.1	TCP	http > icmp [SYN, ACK] Seq=0 Ack=1 win=16384 Len=0 MS
3	0.000755	200.200.200.1	200.200.200.2	TCP	icmp > http [ACK] Seq=1 Ack=1 win=261340 Len=0
4	0.001293	200.200.200.1	200.200.200.2	HTTP	GET / HTTP/1.1
5	0.128252	200.200.200.2	200.200.200.1	TCP	http > icmp [ACK] Seq=1 Ack=409 win=65127 Len=0
6	0.369048	200.200.200.2	200.200.200.1	TCP	[TCP segment of a reassembled PDU]
7	0.369068	200.200.200.2	200.200.200.1	HTTP	HTTP/1.1 200 OK (text/html)
8	0.370006	200.200.200.1	200.200.200.2	TCP	icmp > http [ACK] Seq=409 Ack=1604 win=261340 Len=0
9	0.370535	200.200.200.1	200.200.200.2	TCP	icmp > http [RST, ACK] Seq=409 Ack=1604 win=0 Len=0
10	0.372826	200.200.200.1	200.200.200.2	TCP	ltp-deepspace > http [SYN] Seq=0 win=65535 Len=0 MSS
11	0.372856	200.200.200.2	200.200.200.1	TCP	http > ltp-deepspace [SYN, ACK] Seq=0 Ack=1 win=1638
12	0.373222	200.200.200.1	200.200.200.2	TCP	ltp-deepspace > http [ACK] Seq=1 Ack=1 win=261340 Le

그림 2-49 서버에서 캡처한 패킷 목록

### 실습 2-3 네트워크 계층의 패킷 분석하기

#### ③ 패킷 분석하기

- ① 출발지 MAC 주소는 클라이언트의 MAC 주소며, 목적지 MAC 주소는 IP 공유기 내부 인터페이스 MAC 주소

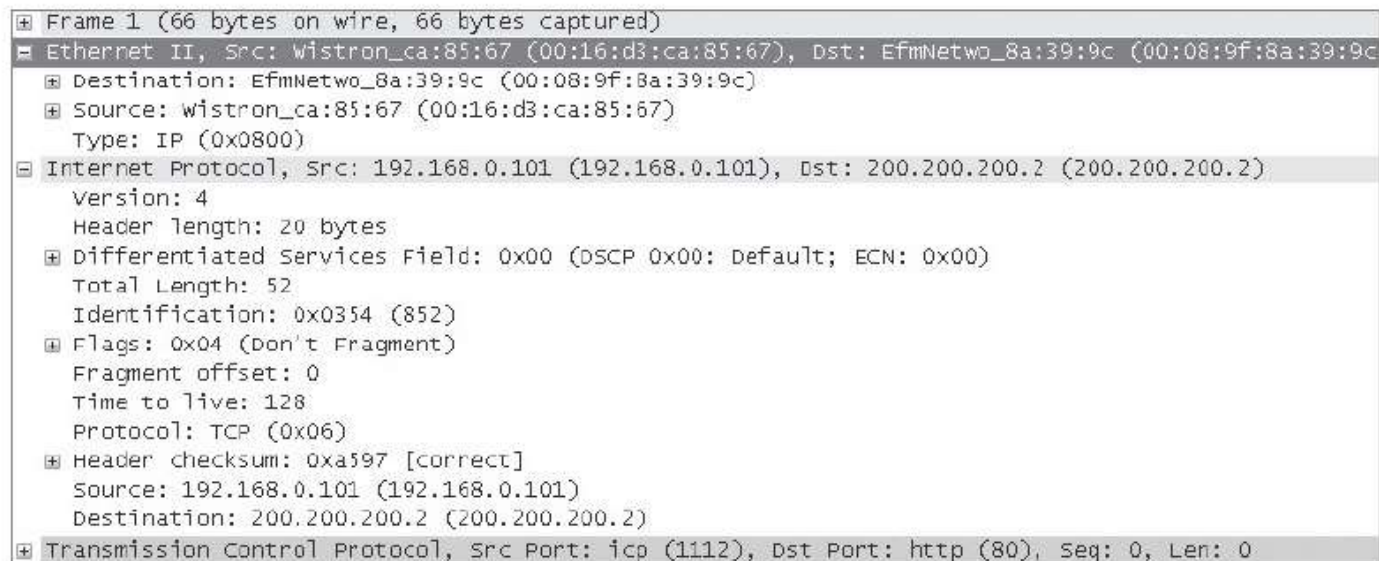


그림 2-50 클라이언트에서 라우터로 전송된 SYN 패킷

## 8. 계층별 패킷 분석

### 실습 2-3 네트워크 계층의 패킷 분석하기

#### ③ 패킷 분석하기

- ② 출발지 MAC 주소는 IP 공유기의 외부 인터페이스 MAC 주소며, 목적지 MAC 주소는 서버의 MAC 주소

```
Frame 1 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: EfmNetwo_8b:39:9c (00:08:9f:8b:39:9c), Dst: Asiarock_53:2f:79 (00:13:8f:53:2f:79)
  Destination: Asiarock_53:2f:79 (00:13:8f:53:2f:79)
    Address: Asiarock_53:2f:79 (00:13:8f:53:2f:79)
      ....0.... = IG bit: Individual address (unicast)
      ....0.... = LG bit: Globally unique address (factory default)
  Source: EfmNetwo_8b:39:9c (00:08:9f:8b:39:9c)
    Address: EfmNetwo_8b:39:9c (00:08:9f:8b:39:9c)
      ....0.... = IG bit: Individual address (unicast)
      ....0.... = LG bit: Globally unique address (factory default)
  Type: IP (0x0800)
Internet Protocol, Src: 200.200.200.1 (200.200.200.1), Dst: 200.200.200.2 (200.200.200.2)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  Total Length: 52
  Identification: 0x0354 (852)
  Flags: 0x04 (Don't Fragment)
  Fragment offset: 0
  Time to live: 127
  Protocol: TCP (0x06)
  Header checksum: 0xd6da [correct]
  Source: 200.200.200.1 (200.200.200.1)
  Destination: 200.200.200.2 (200.200.200.2)
Transmission Control Protocol, Src Port: icmp (1112), Dst Port: http (80), Seq: 0, Len: 0
```

그림 2-51 라우터에서 서버로 전송된 SYN 패킷



### 실습 2-3 네트워크 계층의 패킷 분석하기

#### ③ 패킷 분석하기

- ③ 클라이언트에서 서버로 SYN 패킷이 전송되면 서버는 클라이언트로 다시 SYN+ACK 패킷을 보냄(MAC 주소가 변경되는 과정은 똑같음).

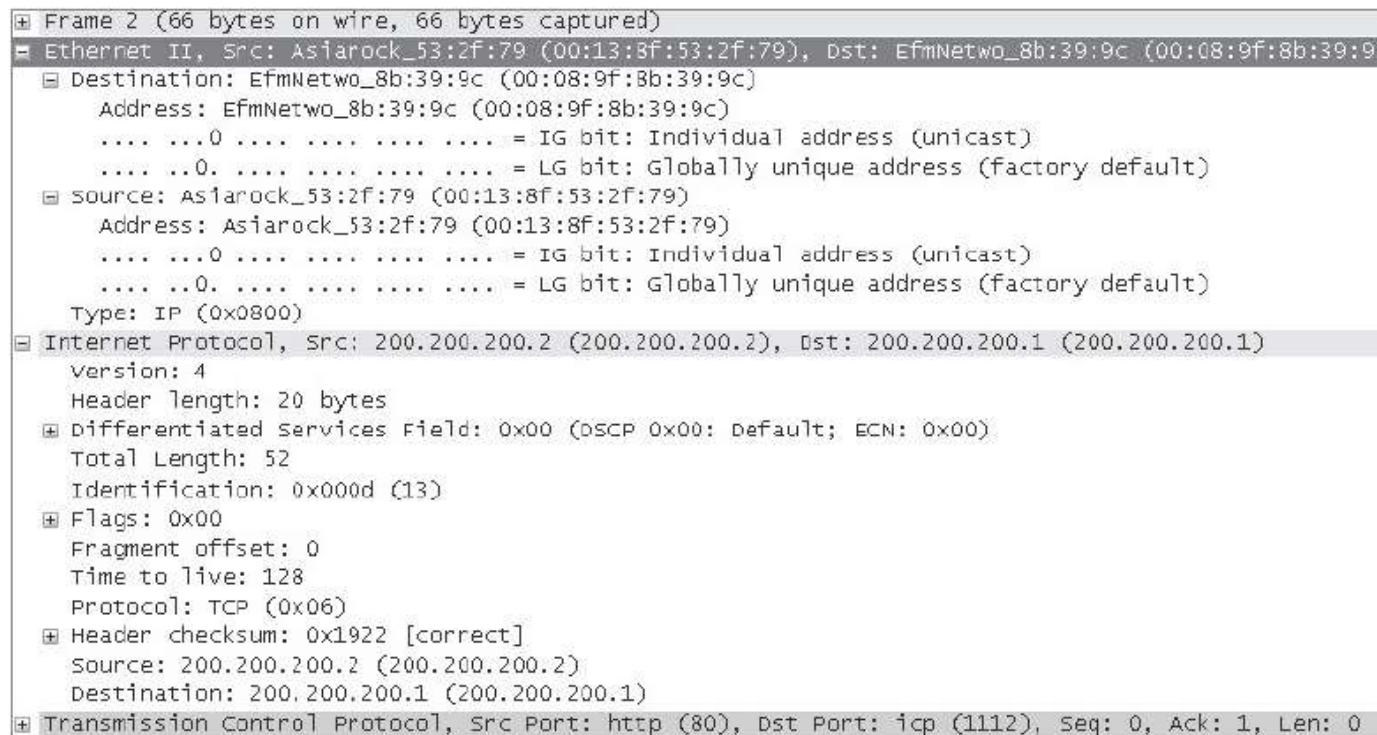


그림 2-52 서버에서 라우터로 전송된 SYN+ACK 패킷

### 실습 2-3 네트워크 계층의 패킷 분석하기

#### ③ 패킷 분석하기

The image shows a Wireshark packet capture analysis of a SYN+ACK packet. The packet list on the left shows 'Frame 2 (66 bytes on wire, 66 bytes captured)' and 'Ethernet II, Src: EfmNetwo\_8a:39:9c (00:08:9f:8a:39:9c), Dst: Wistron\_ca:85:67 (00:16:d3:ca:85:67)'. The packet details pane on the right shows the following structure:

- Destination: Wistron\_ca:85:67 (00:16:d3:ca:85:67)
  - Address: Wistron\_ca:85:67 (00:16:d3:ca:85:67)
    - .... ..0 .... = IG bit: Individual address (unicast)
    - .... ..0. .... = LG bit: Globally unique address (factory default)
- Source: EfmNetwo\_8a:39:9c (00:08:9f:8a:39:9c)
  - Address: EfmNetwo\_8a:39:9c (00:08:9f:8a:39:9c)
    - .... ..0 .... = IG bit: Individual address (unicast)
    - .... ..0. .... = LG bit: Globally unique address (factory default)
  - Type: IP (0x0800)
- Internet Protocol, Src: 200.200.200.2 (200.200.200.2), Dst: 192.168.0.101 (192.168.0.101)
  - Version: 4
  - Header length: 20 bytes
  - Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  - Total Length: 52
  - Identification: 0x000d (13)
  - Flags: 0x00
    - Fragment offset: 0
    - Time to live: 127
    - Protocol: TCP (0x06)
  - Header checksum: 0xe9de [correct]
  - Source: 200.200.200.2 (200.200.200.2)
  - Destination: 192.168.0.101 (192.168.0.101)
- Transmission Control Protocol, Src Port: http (80), Dst Port: tcp (1112), Seq: 0, Ack: 1, Len: 0

그림 2-53 라우터에서 클라이언트로 전송된 SYN+ACK 패킷

## 8. 계층별 패킷 분석

### 실습 2-4 계층별 패킷 구조 분석하기

**실습환경** • IP 공유기에 연결된 클라이언트(윈도우 7)와 서버 시스템(윈도우 서버 2012, IIS 설치)  
• 필요 프로그램 : Wireshark(서버와 클라이언트 각각에 설치)

#### ① 패킷 내용 확인하기

- 네트워크 계층에서 서버측 패킷을 보면 2,3,4 계층 정보의 실체 확인 가능

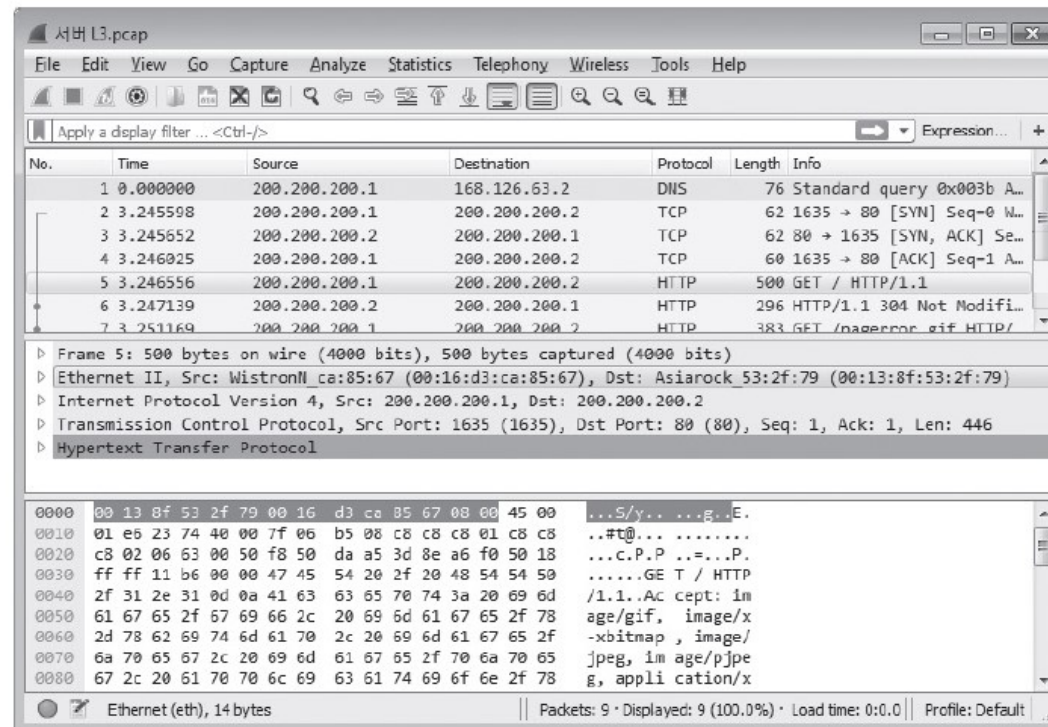


그림 2-54 클라이언트에서 서버로 웹 페이지를 요청한 패킷과 2계층 정보



## 8. 계층별 패킷 분석

### 실습 2-4 계층별 패킷 구조 분석하기

#### ① 패킷 내용 확인하기

0000	00 13 8f 53 2f 79 00 16 d3 ca 85 67 08 00 45 00	...S/y.. ...g..E.
0010	01 e6 23 74 40 00 7f 06 b5 08 c8 c8 c8 01 c8 c8	..#t@... .....
0020	c8 02 06 63 00 50 f8 50 da a5 3d 8e a6 f0 50 18	..c.P.P ..=...P.
0030	ff ff 11 b6 00 00 47 45 54 20 2f 20 48 54 54 50	.....GE T / HTTP
0040	2f 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 69 6d	/1.1..Ac cept: im
0050	61 67 65 2f 67 69 66 2c 20 69 6d 61 67 65 2f 78	age/gif, image/x
0060	2d 78 62 69 74 6d 61 70 2c 20 69 6d 61 67 65 2f	-xbitmap , image/
0070	6a 70 65 67 2c 20 69 6d 61 67 65 2f 70 6a 70 65	jpeg, im age/pjpe
0080	67 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78	g, appli cation/x
0090	2d 73 68 6f 63 6b 77 61 76 65 2d 66 6c 61 73 68	-shockwa ve-flash
00a0	2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 76 6e	, applic ation/vn
00b0	64 2e 6d 73 2d 65 78 63 65 6c 2c 20 61 70 70 6c	d.ms-exc el, appl

(a) 3계층 정보

0000	00 13 8f 53 2f 79 00 16 d3 ca 85 67 08 00 45 00	...S/y.. ...g..E.
0010	01 e6 23 74 40 00 7f 06 b5 08 c8 c8 c8 01 c8 c8	..#t@... .....
0020	c8 02 06 63 00 50 f8 50 da a5 3d 8e a6 f0 50 18	..c.P.P ..=...P.
0030	ff ff 11 b6 00 00 47 45 54 20 2f 20 48 54 54 50	.....GE T / HTTP
0040	2f 31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 69 6d	/1.1..Ac cept: im
0050	61 67 65 2f 67 69 66 2c 20 69 6d 61 67 65 2f 78	age/gif, image/x
0060	2d 78 62 69 74 6d 61 70 2c 20 69 6d 61 67 65 2f	-xbitmap , image/
0070	6a 70 65 67 2c 20 69 6d 61 67 65 2f 70 6a 70 65	jpeg, im age/pjpe
0080	67 2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 78	g, appli cation/x
0090	2d 73 68 6f 63 6b 77 61 76 65 2d 66 6c 61 73 68	-shockwa ve-flash
00a0	2c 20 61 70 70 6c 69 63 61 74 69 6f 6e 2f 76 6e	, applic ation/vn
00b0	64 2e 6d 73 2d 65 78 63 65 6c 2c 20 61 70 70 6c	d.ms-exc el, appl

(b) 4계층 정보

그림 2-55 클라이언트에서 서버로 웹 페이지를 요청한 패킷의 3계층과 4계층 정보

## 8. 계층별 패킷 분석

### 실습 2-4 계층별 패킷 구조 분석하기

#### ① 패킷 내용 확인하기

표 2-13 패킷 분석

구분	16진수(HEX)	2진수(Binary)
2계층 이더넷 패킷 헤더	00 13 8f 53	0000 0000 0001 0011 1000 1111 0101 0011
	2f 79 00 16	0010 1111 0111 1001 0000 0000 0001 0110
	d3 ca 85 67	1101 0011 1100 1010 1000 0101 0110 0111
	08 00	0000 1000 0000 0000
3계층 IP 패킷 헤더	45 00 01 e6	0100 0101 0000 0000 0000 0001 1110 0110
	23 74 40 00	0010 0011 0111 0100 0100 0000 0000 0000
	7f 06 b5 08	0111 1111 0000 0110 1011 0101 0000 1000
	c8 c8 c8 01	1100 1000 1100 1000 1100 1000 0000 0001
	c8 c8 c8 02	1100 1000 1100 1000 1100 1000 0000 0010
4계층 TCP 패킷 헤더	06 64 00 50	0000 0110 0110 0100 0000 0000 0101 0000
	f8 50 da a5	1111 1000 0101 0000 1101 1010 1010 0101
	3d 8e a6 f0	0011 1101 1000 1110 1010 0110 1111 0000
	50 18 ff ff	0101 0000 0001 1000 1111 1111 1111 1111
	11 b6 00 00	0001 0001 1011 0110 0000 0000 0000 0000
HTTP 데이터	47 45 54 ~	0100 0111 0100 0101 0101 0100 ~

## 8. 계층별 패킷 분석

### 실습 2-4 계층별 패킷 구조 분석하기

#### ② 2계층 이더넷 패킷 헤더 분석하기

Destination MAC Address	
0000 0000 0001 0011 1000 1111 0101 0011	
Destination MAC Address	Source MAC Address
0010 1111 0111 1001	0000 0000 0001 0110
Source MAC Address	
1101 0011 1100 1010 1000 0101 0110 0111	
Type	
0000 1000 0000 0000	

## 8. 계층별 패킷 분석

### 실습 2-4 계층별 패킷 구조 분석하기

#### ③ 3계층 IP 패킷 헤더 분석하기

Version	IHL	Type of Service(TOS)	Total Length(TL)	
0100	0101	0000 0000	0000 0001 1110 0110	
Identification			Flag	Fragment Offset
0010 0011 0111 0100			010	0 0000 0000 0000
Time To Live(TTL)		Protocol	Header Checksum	
0111 1111		0000 0110	1011 0101 0000 1000	
Source Address				
1100 1000 1100 1000 1100 1000 0000 0001				
Destination Address				
1100 1000 1100 1000 1100 1000 0000 0010				

## 8. 계층별 패킷 분석

### 실습 2-4 계층별 패킷 구조 분석하기

#### ④ 4계층 TCP 패킷 헤더 분석하기

Source Port(S.Port)			Destination Port(D.Port)
0000 0110 0110 0100			0000 0000 0101 0000
Sequence Number(Seq. Number)			
1111 1000 0101 0000 1101 1010 1010 0101			
Acknowledgment Number(Ack. Number)			
0011 1101 1000 1110 1010 0110 1111 0000			
Data Offset	Reserved	Control Bits	Window
0101	0000 00	01 1000	1111 1111 1111 1111
Checksum			Urgent Pointer
0001 0001 1011 0110			0000 0000 0000 0000

### 실습 2-4 계층별 패킷 구조 분석하기

---

#### ⑤ 7계층 HTTP 패킷 헤더 분석하기

- 그 뒤에 오는 데이터는 아스키 코드값 47 45 54로, 대문자로 GET
- 데이터 전송과 관련 없이 순수하게 응용 프로그램이 사용하는 데이터 부분





# 감사합니다.

## 네트워크 해킹과 보안 개정3판

정보 보안 개론과 실습

---