

NETWORK 보안 실무

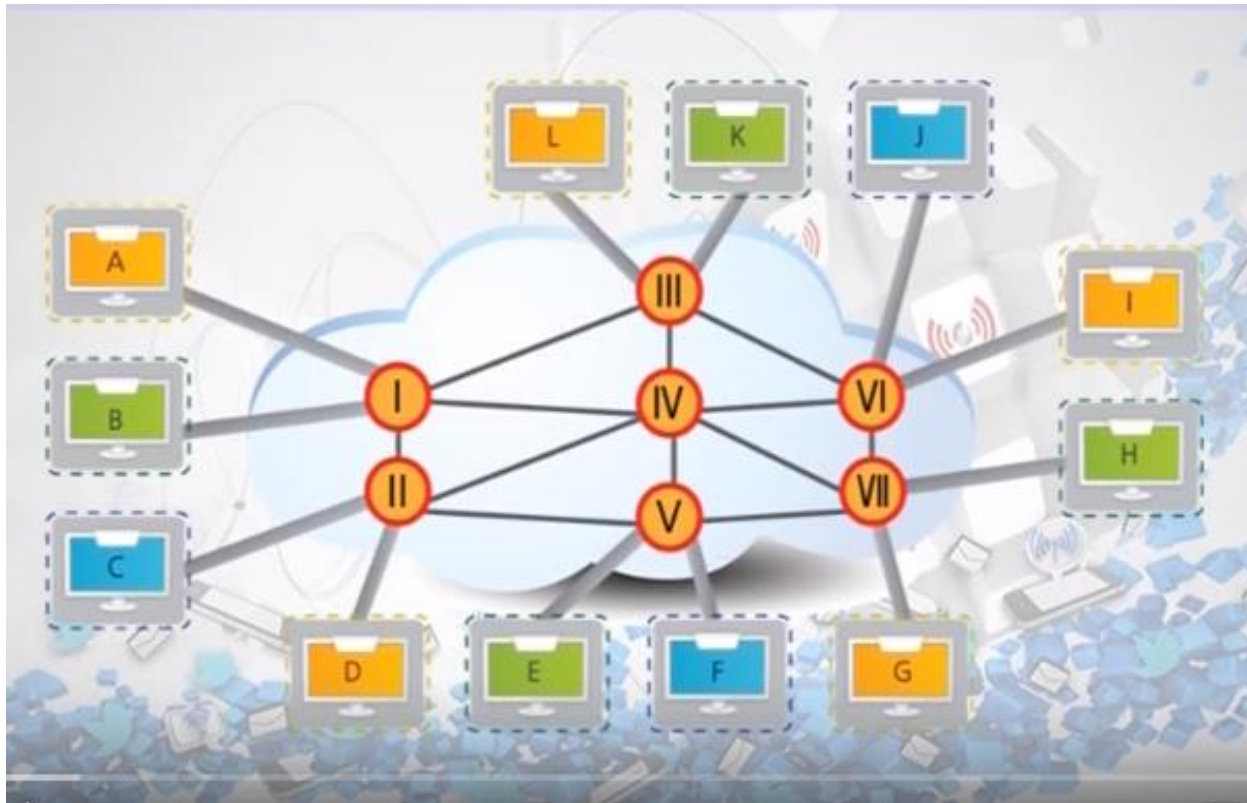
(사이버보안과 2학년)

2. 네트워크의 이해

2. 네트워크 의 이해

○ 네트워크 구성요소

- ✓ 장치 + 링크 (유선 & 무선)



○ 좋은 Network 의 조건

- 성능 : 처리량과 지연시간
- 신뢰성 : 장애발생에 대한 빈도 및 장애발생 후 회복시간 재난에 대한 견고성
- 보안성 : 송신한 데이터를 네트워크에서 정보유출이나 불법적인 침입으로부터 보안

○ Protocol

- ✓ 본래 의미는 외교에서 의례 또는 의정서
- ✓ 통신규약 (표준)
- ✓ 톰 마릴이 '컴퓨터와 컴퓨터 사이에서 메시지를 전달하는 과정'이라 정의

○ 프로토콜의 3가지 요소

- ✓ Syntax
- ✓ Semantics
- ✓ Timing

● 프로토콜의 종류

[HTTP](#) : Hyper Text Transfer Protocol

[HTTPS](#) : Hyper Text Transfer Protocol Secure

[FTP](#) : File Transfer Protocol

[SFTP](#) : Secure File Transfer Protocol

[Telnet](#) : Terminal Network

[POP3](#) : Post Office Protocol version 3

[SMTP](#) : Simple Mail Transfer Protocol

[SSH](#) : Secure Shell

[SSL](#) : Secure Socket Layer

[SOAP](#) : Simple Object Access Protocol

[ARP](#) : Address Resolution Protocol

○ 표준 프로토콜

✓ De facto 표준 프로토콜

✓ De Jure 표준 프로토콜

○ 대표적인 표준기관 : International Organization for Standardization (ISO)

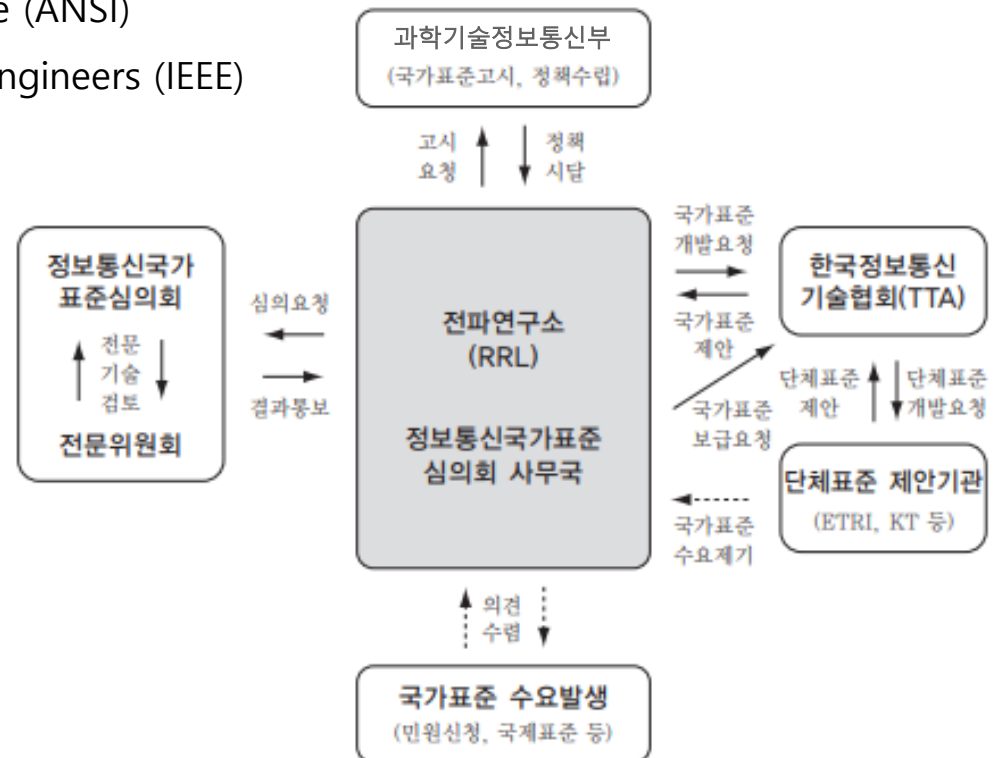
- ITU-T : International Telecommunication Union-Telecommunication Standards Sector (ITU-T)

cf. 예전에는 CCITT

- ANSI : American National Standards Institute (ANSI)

- IEEE : Institute of Electrical and Electronics Engineers (IEEE)

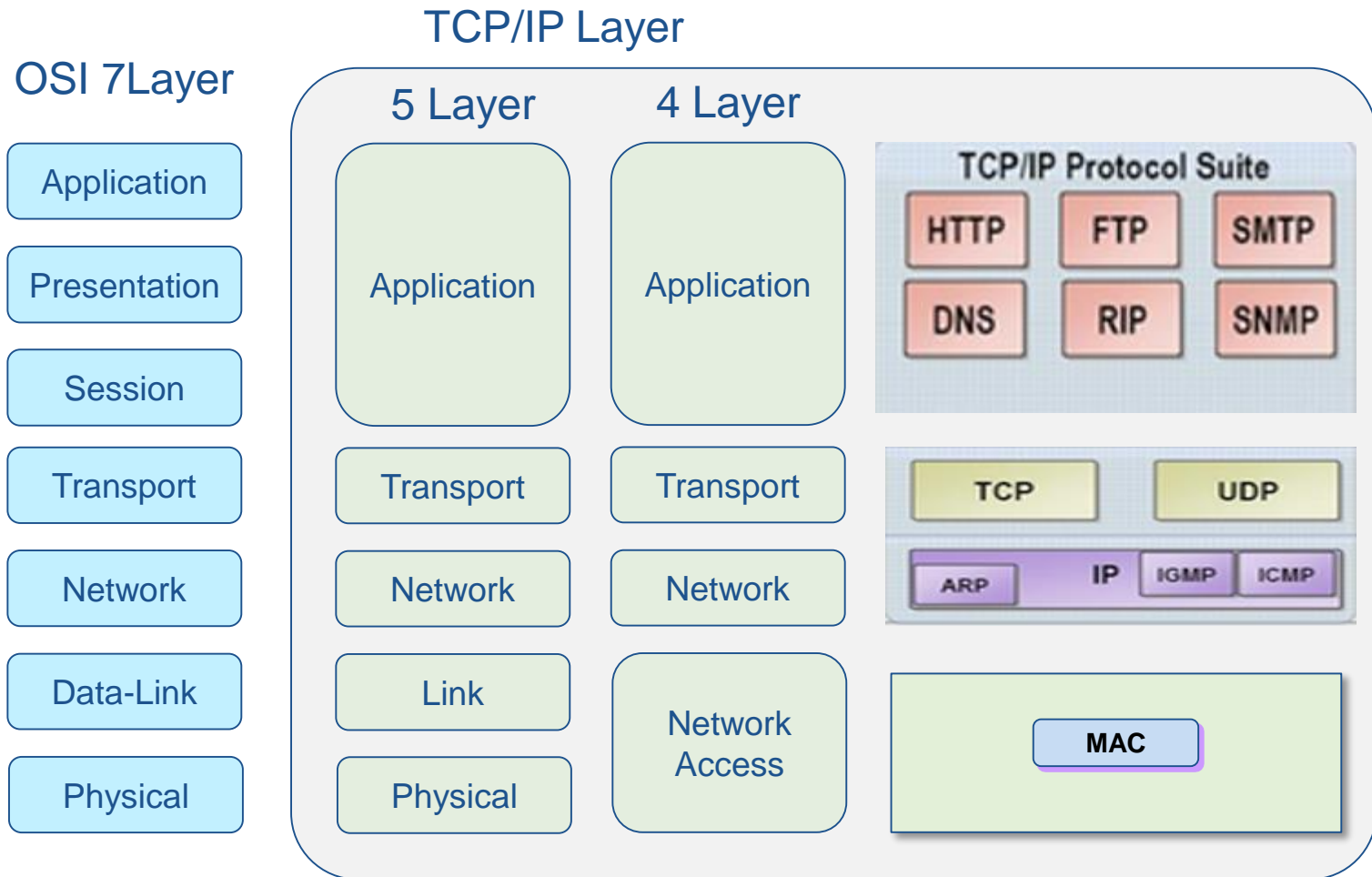
- EIA : Electronic Industries Association (EIA)



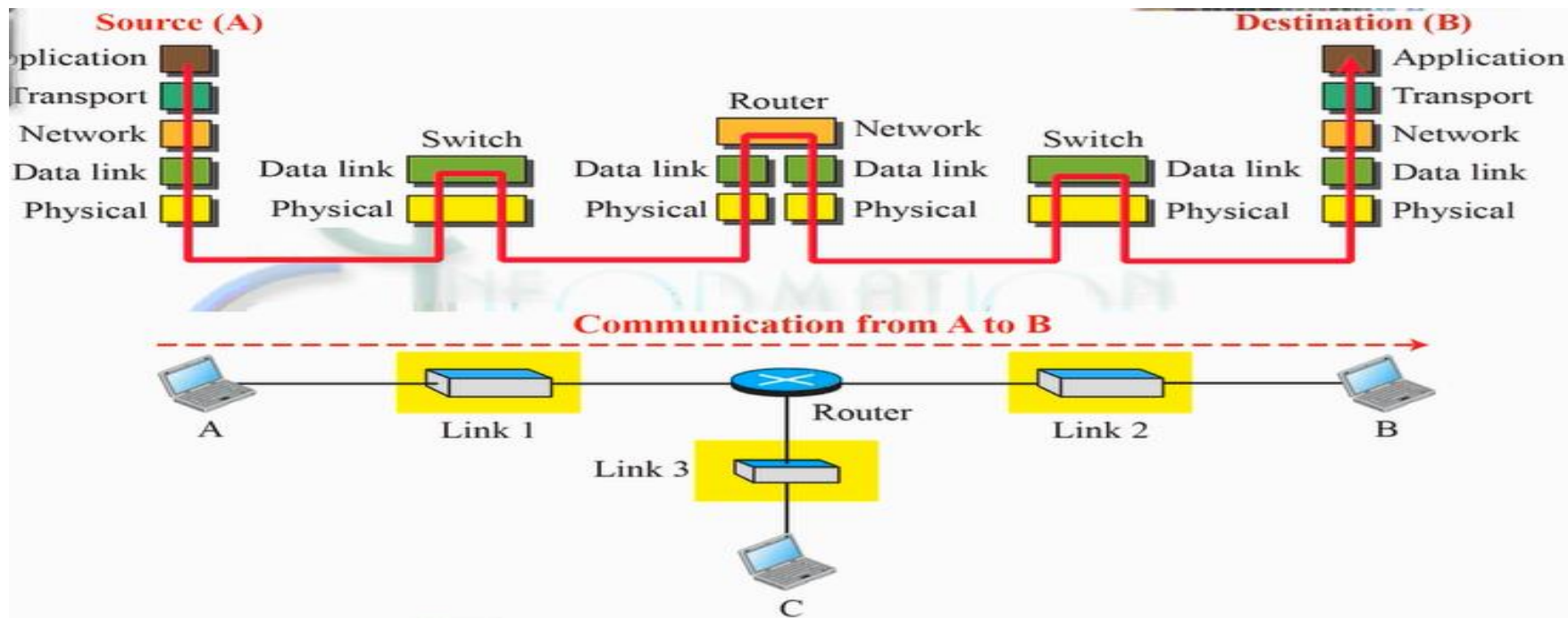
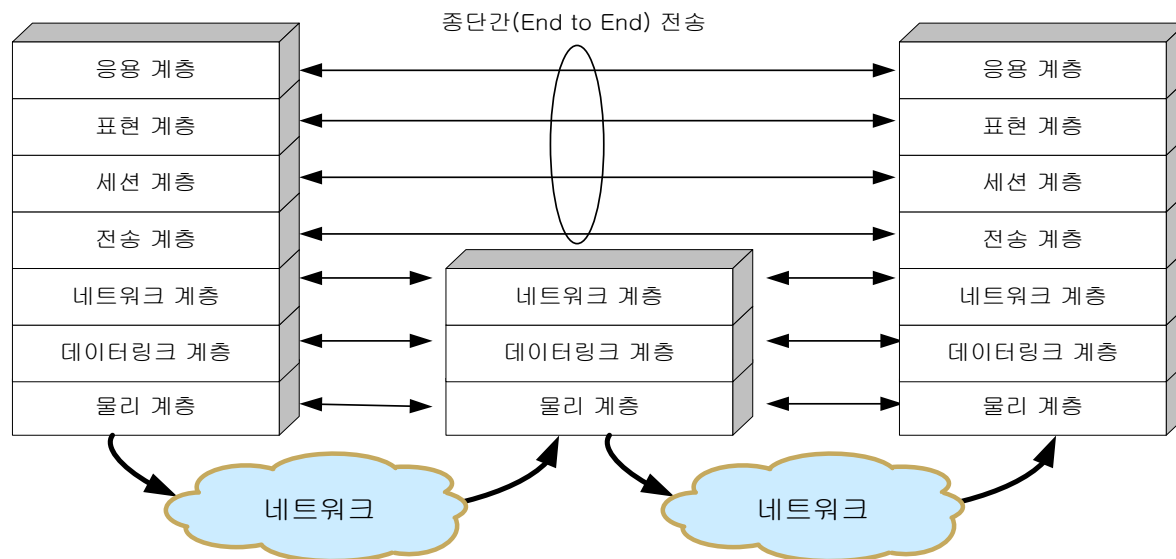
○ 프로토콜의 기능

- ✓ 주소설정(Addressing)
- ✓ 순서 제어(Sequence Control)
- ✓ 데이터 대열의 단편화 및 재조합(Fragmentation & Reassembly)
- ✓ 캡슐화(Encapsulation)
- ✓ 연결 제어(Connection Control)
- ✓ 흐름 제어(Flow Control)
- ✓ 오류 제어(Error Control)
- ✓ 동기화(Synchronization)
- ✓ 다중화(Multiplexing)
- ✓ 전송 서비스

- OSI 7Layer와 TCP/IP 5 or 4Layer



○ OSI 7Layer



○ 물리계층

- 데이터를 물리 매체 상으로 전송하는 역할
- 물리적 링크의 설정, 유지, 해제 담당
- 사용자 장비와 네트워크 종단 장비 간의 물리적, 전기적 인터페이스 규정
- 전송선로의 종류에 따른 전송 방식과 인코딩 방식 결정

표 2-1 CAT별 특성

카테고리	최대 속도	용도	
CAT 1	1Mbps 미만	• 아날로그 음성. 일반적인 전화 서비스 • ISDN 기본율 접속(Basic Rate Interface) • Doorbell wiring	
CAT 2	4Mbps	• IBM의 토큰 링 네트워크에 주로 사용	
CAT 3	16Mbps	• 10BASE-T 이더넷의 데이터 및 음성	
CAT 4	20Mbps	표 2-2 케이블의 구분	
CAT 5	100Mbps	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.
CAT 6	250Mbps	STP(Shielded Twisted Pair)	연선으로 된 케이블 겉에 외부 피복, 또는 차폐재가 추가(섀드 처리)된 것으로, 차폐재가 접지 역할을 하므로 외부 노이즈를 차단하거나 전기적 신호 간섭을 줄이는 데 탁월하다.
		• 155/622Mbps ATM • 기가비트 이더넷	

○ 물리계층

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.



그림 2-7 RJ-45



그림 2-6 RJ-11

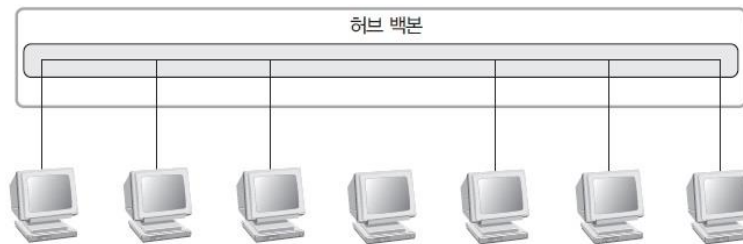


그림 2-9 더미 허브의 구조



그림 2-8 리피터



HUB

○ 데이터 링크 계층

- ✓ 물리 계층에서 전송하는 비트들에 대한 동기 및 식별 기능
- ✓ 원활한 데이터의 전송을 위한 흐름제어(Flow Control) 기능
- ✓ 안전한 데이터 전송을 위한 오류제어(Error Control) 기능
- ✓ 메시지 포맷 : 프레임
- ✓ 헤더와 트레일러 이용
 - 헤더필드에는 송신지/수신지 주소 포함
 - 트레일러에는 오류 검출 코드 포함

✓ 랜 카드나 네트워크 장비의 하드웨어 주소(MAC 주소)만으로 통신하는 계층

- ✓ 네트워크 카드의 MAC 주소는 윈도우 명령 창에서 'ipconfig /all' 명령을 실행 하면 'Physical Address'에서 확인 가능

MAC주소 확인 (16진수 표현)

```
이더넷 어댑터 Bluetooth 네트워크 연결:

   미디어 상태 . . . . . : 미디어 연결 끊김
   연결별 DNS 접미사 . . . . . :

C:\Users\이화정>ipconfig /all

Windows IP 구성

   호스트 이름 . . . . . : SeungIKYang
   주 DNS 접미사 . . . . . :
   노드 유형 . . . . . : 혼성
   IP 라우팅 사용 . . . . . : 아니요
   WINS 프록시 사용 . . . . . : 아니요

이더넷 어댑터 이더넷:

   미디어 상태 . . . . . : 미디어 연결 끊김
   연결별 DNS 접미사 . . . . . :
   설명 . . . . . : Realtek PCIe GBE Family Controller
   물리적 주소 . . . . . : 98-83-89-1E-45-B7
   DHCP 사용 . . . . . : 예
   자동 구성 사용 . . . . . : 예

이더넷 어댑터 Npcap Loopback Adapter:

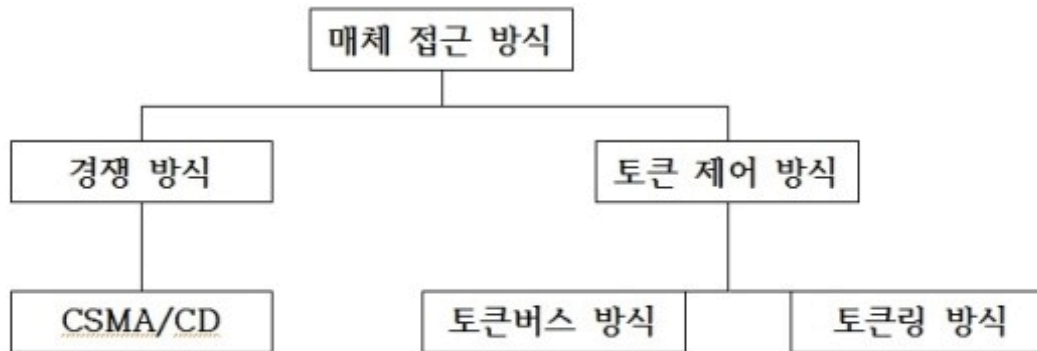
   연결별 DNS 접미사 . . . . . :
   설명 . . . . . : Npcap Loopback Adapter
   물리적 주소 . . . . . : 02-00-4C-4F-4F-50
   DHCP 사용 . . . . . : 예
```

○ 데이터 링크 계층

- ✓ X.25
- ✓ Frame Relay
- ✓ ATM(Asynchronous Transfer Mode)
- ✓ 이더넷

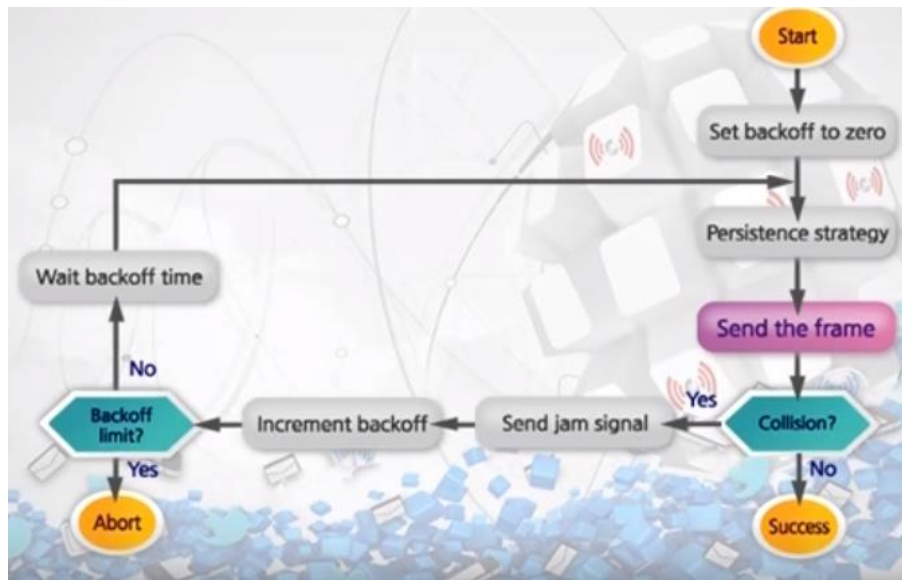
○ 데이터 링크 계층의 매체접근방식(물리계층)

- ✓ 공유하고 있는 전송매체에 대한 채널의 할당에 대한 문제를 해결하는 방식
- ✓ 방식 : CSMA/CD, 토큰 링, 토큰 버스

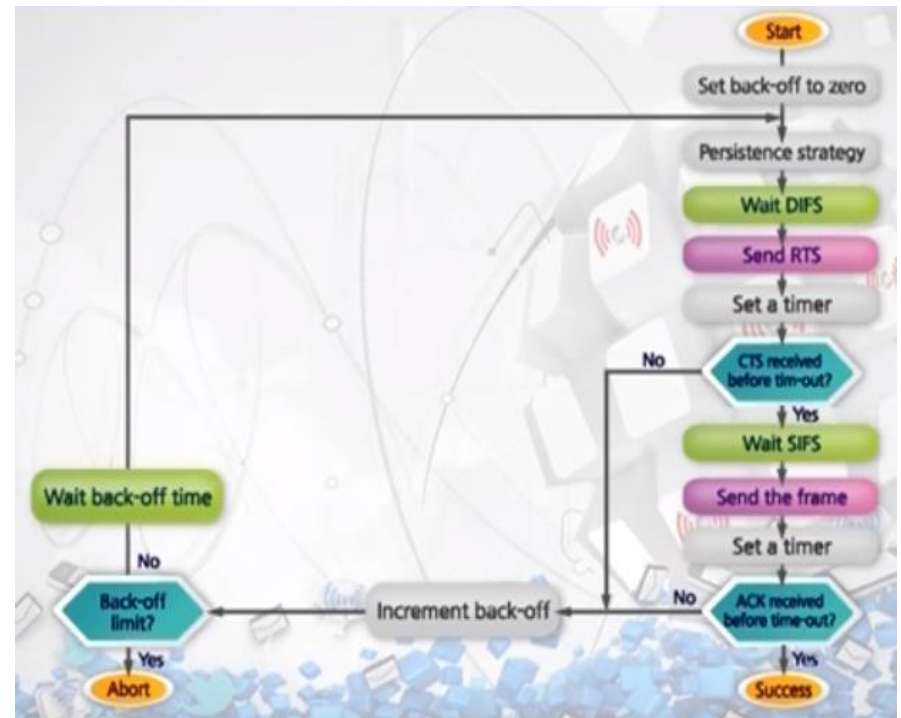


- 다중접속의 데이터 링크 계층에서 부계층
 - ✓ LLC(logical link control) or Data link control 계층
 - ✓ MAC(Media access control) 계층
- 데이터 링크 계층에서 다중접속 프로토콜 3가지 및 기능
 - ✓ 무작위 접근(Random Access Protocol)
 - CSMA / CD
 - CSMA / CA
 - ✓ 통제된 접근(controlled access Protocol)
 - 예약(Reservation)
 - 폴링(Polling)
 - 토큰전달(Token Passing)
 - ✓ 채널화(channelization Protocol)
 - FDMA(Frequency Division Multiple Access)
 - TDMA(Time Division Multiple Access)
 - CDMA(code Division Multiple Access)

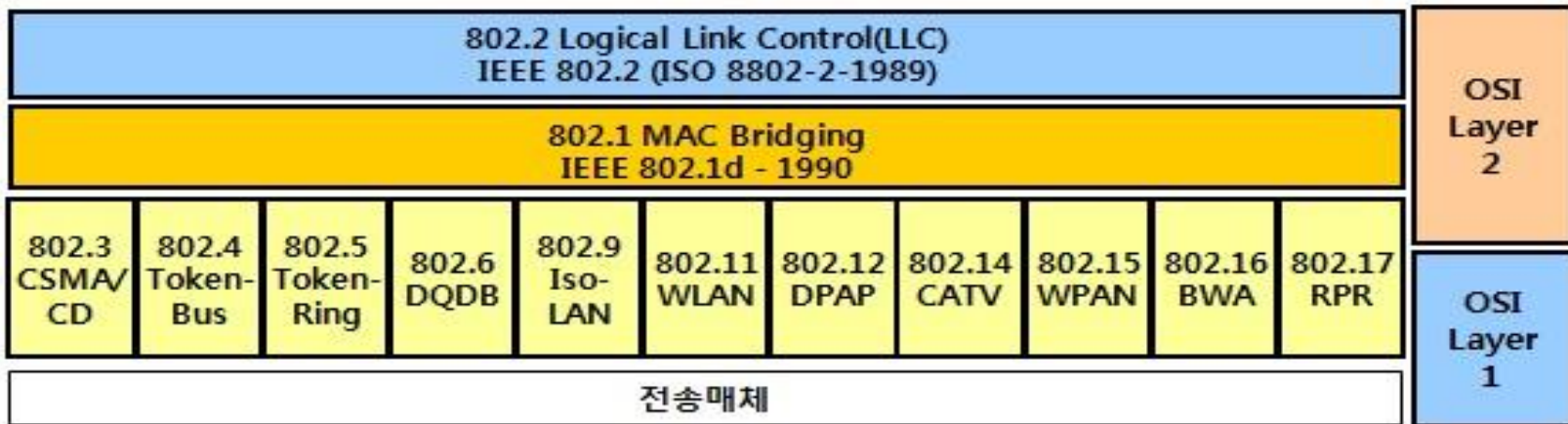
- CSMA / CD



- CSMA / CA



- 데이터 링크 계층에서 Ethernet
 - ✓ LLC(logical link control) or Data link control 계층
 - ✓ MAC(Media access control) 계층



- LLC(logical link control) 의 기능
 - ✓ 상위 계층인 네트워크 계층과 LAN의 MAC 계층을 연결해 주는 인터페이스
 - ✓ 어떤 매체를 사용하든 간에 공통으로 사용하고 있는 부분 즉 LAN에서 흐름제어, 에러제어 등 각종 제어에 대한 행위를 하는 부 계층
 - ✓ 모든 LAN에서 공통의 계층이다
- MAC (Medium Access Control)
 - ✓ 사용하는 매체를 어떤 것을 사용하느냐?
 - ✓ 매체의 특성, 운용방식에 따라 여러 개의 프로토콜이 존재하고 Ethernet, Token ring, Token bus등이 있다
 - ✓ 물리 네트워크에 대한 접근 제어를 담당

○ 데이터 링크 계층 장비

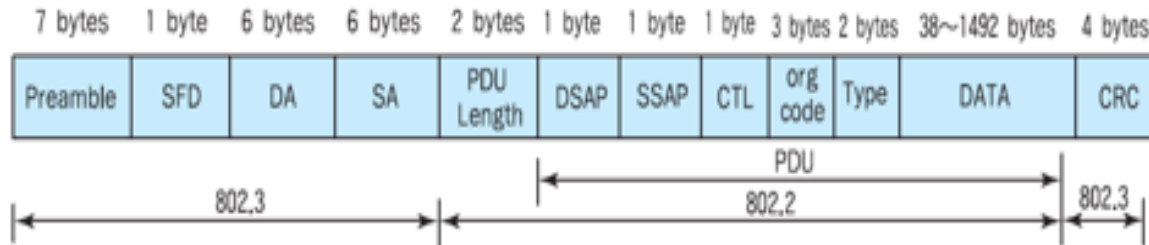
✓ 브릿지(Bridge)

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

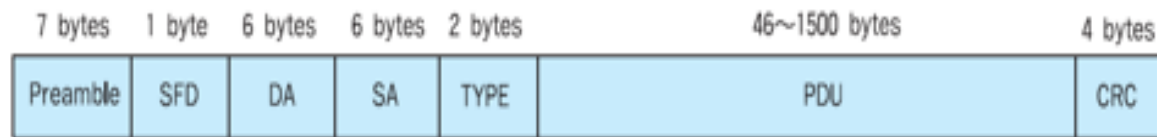
✓ 스위치(Switch)

- 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

❖ Ethernet의 MAC프레임 포맷
TCP/IP 총 7개의 필드로 구성



a. 802.2/802.3 프레임



b. 이더넷 프레임

- 프리엠블
- 시작 프레임 지시자
- DA(Destination Address) 목적지 주소 : 6바이트
- SA(Source Address) 송신지 주소 : 6바이트
- Length(랭스) 또는 타입(Type)은 데이터 필드의 길이와 위에 올라가는 프로토콜이 무엇이나
즉 네트워크 계층의 프로토콜을 명시하기 위하여 2바이트를 사용
- PDU 데이터부분으로 최소 46바이트에서 최대 1500바이트 사이
- CRC 에러를 검출하는 기능을 수행 4바이트(에러유무 검출)

❖ Ethernet의 MAC프레임 포맷 TCP/IP 총 7개의 필드로 구성

❖ 주소지정

- DA(Destination Address) 목적지 주소, SA(Source Address) 송신지 주소
- 송신자 6바이트, 수신자 6바이트, 이더넷 앞 부문에 포함되어 전송
- MAC주소(MAC address), Ethernet주소, 하드웨어 주소



- LAN카드는 주소가 설정되어 출고가 된다 6바이트(48비트)로 이루어 졌으며 보통 16진수로 표기가 된다
- 시스코 : 000C, 00067C, 00061C등, AT&T : 000055
- XEROX : 0000AA, DEC : 0000F8
- IBM : 0004AC 삼성 : 0000F0 삼보 : 004026 현대 : 00803F

○ 네트워크 계층

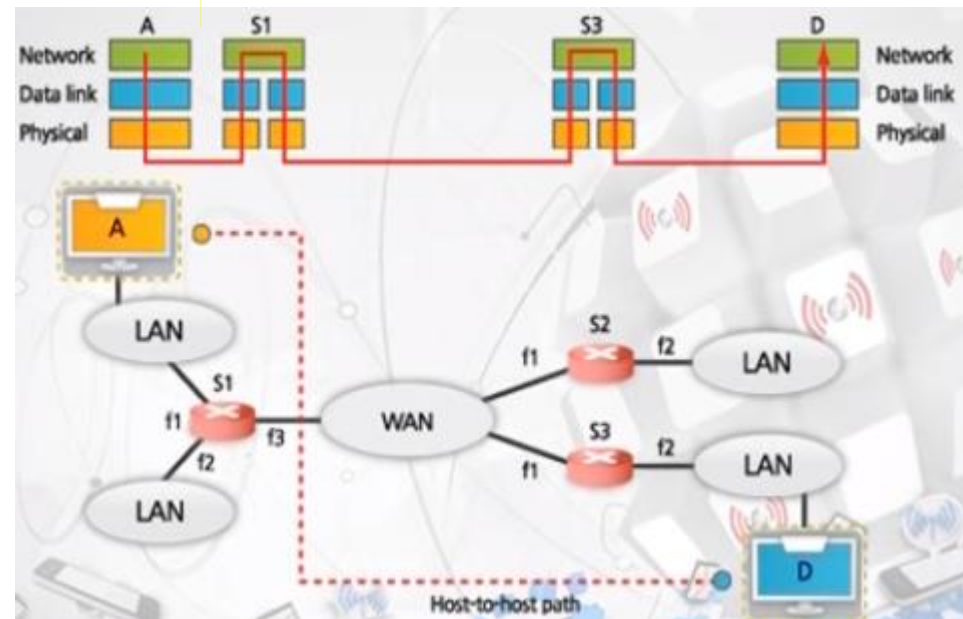
- ✓ 가장 중요한 기능은 라우팅이다
- ✓ 송신측과 수신측간의 논리적 링크 설정
- ✓ 상위 계층 데이터를 패킷으로 분할
- ✓ 메시지 포맷 : 패킷

❖ 라우터의 기능

- ✓ 최적 경로 선택
- ✓ 세그먼트의 분리
- ✓ 이종 네트워크간의 연결

○ Network 계층 Protocol

- ✓ ARP(Address Resolution Protocol)
- ✓ RARP(Reverse Address Resolution Protocol)
- ✓ IP(Internet Protocol)
- ✓ ICMP(Internet Control Message Protocol)
- ✓ IGMP(Internet Group Management Protocol)



○ Network 계층 Protocol

- ✓ 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
- ✓ 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)
- ✓ ICMP(Internet Control Message Protocol)
 - 호스트 서버와 인터넷 게이트웨이 사이에서 메시지를 제어하고 오류를 알려주는 프로토콜
 - 대표적인 툴은 ping
- ✓ IGMP(Internet Group Management Protocol)
 - 멀티캐스트에 관여하는 프로토콜로 멀티캐스트 그룹을 관리하는 역할

❖ 무선LAN의 표준

- 1970년 하와이 대학 알로하넷 개발
- 4개의 섬과 오후우섬 연결
- 1985년 CDMA를 이용한 무선 PABX시스템 개발 → 무선LAN 기반 마련
- 1991년 최초의 무선 LAN인 웨이브랜(Wave LAN) 상용화
- 전기 전자 기술자 협회(IEEE) 802.11 표준

❖ 무선LAN개요

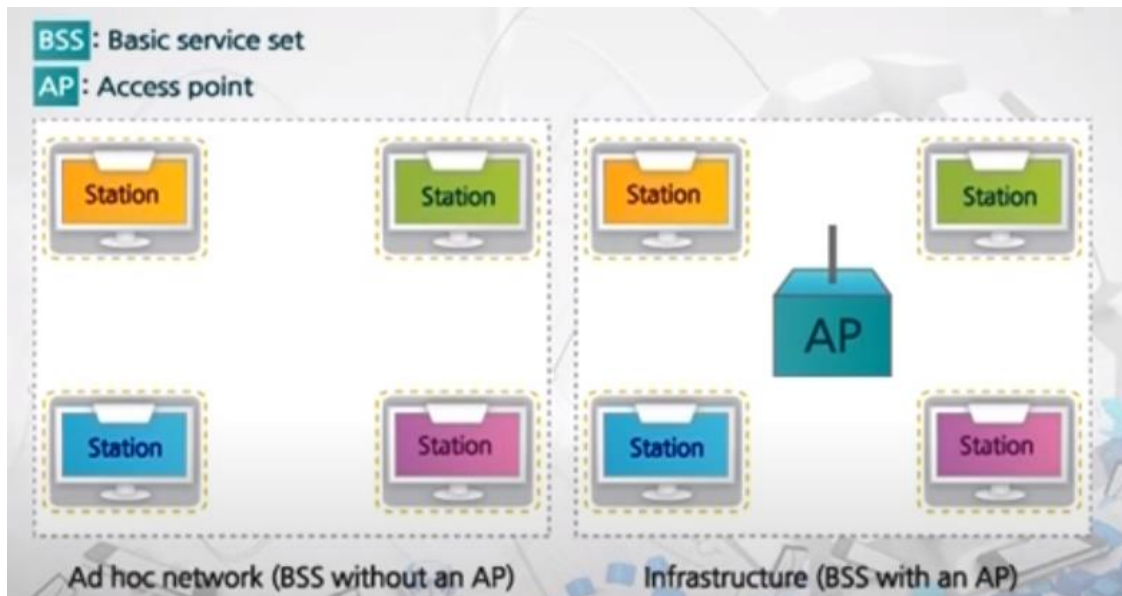
- 이동성, 확장성 그리고 편리성으로 확산 (모바일 네트워크와의 융합으로 확산 속도 증폭)
- 일반 기업, 공공장소, 학교 캠퍼스 및 가정까지 사용 범위 확대
- 관리 및 무관심과 정보 보호 마인드 부재로 일부 기관은 사용에 제한

❖ 무선LAN 지원서비스

- BSS(Basic Service Set)와 ESS (Extended Service Set) 서비스를 지원
- BSS는 Infrastructure Mode 와 Ad hoc 두 가지로 구분
- ESS(Extended Service Set) 여러 개의 BSS로 구성
- 각각의 BSS가 해당하는 AP의 관리

❖ 무선LAN의 서비스 지원

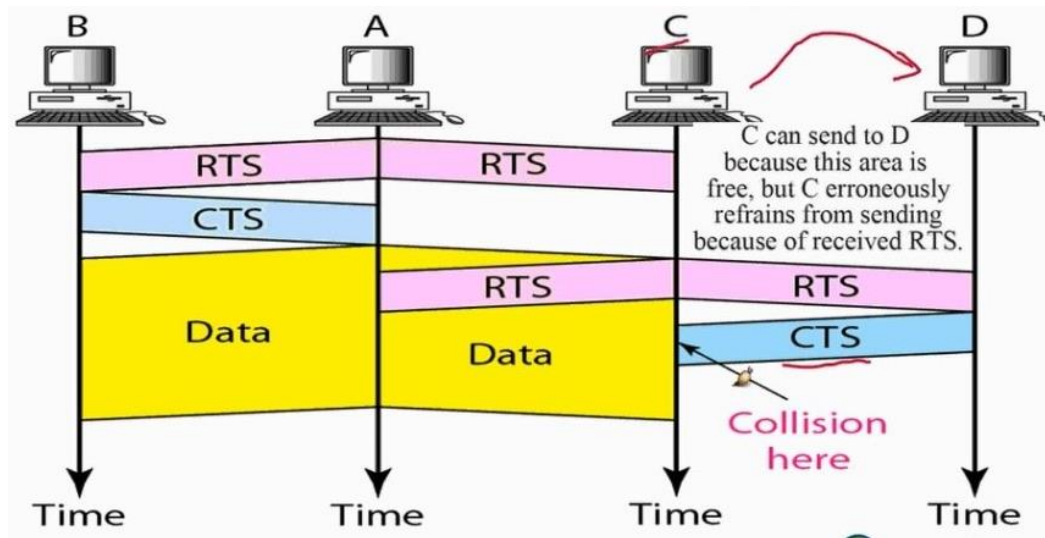
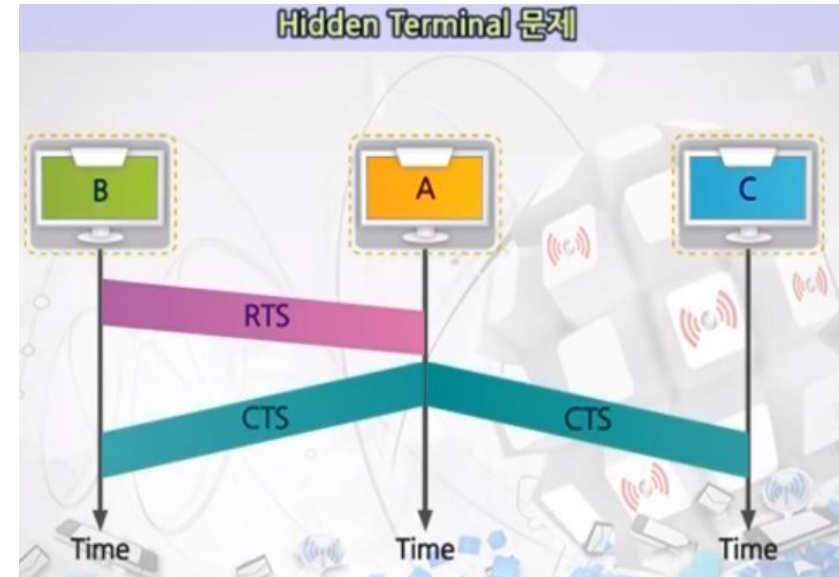
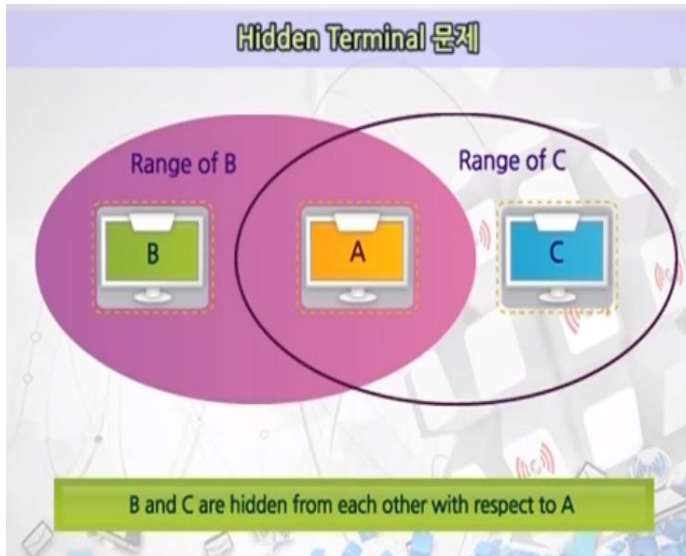
- 무선LAN은 BSS(Basic Service Set)와 ESS (Extended Service Set) 두 종류의 서비스를 지원한다
- ✓ BSS는 Infrastructure Mode 와 Ad hoc 두가지로 나눔



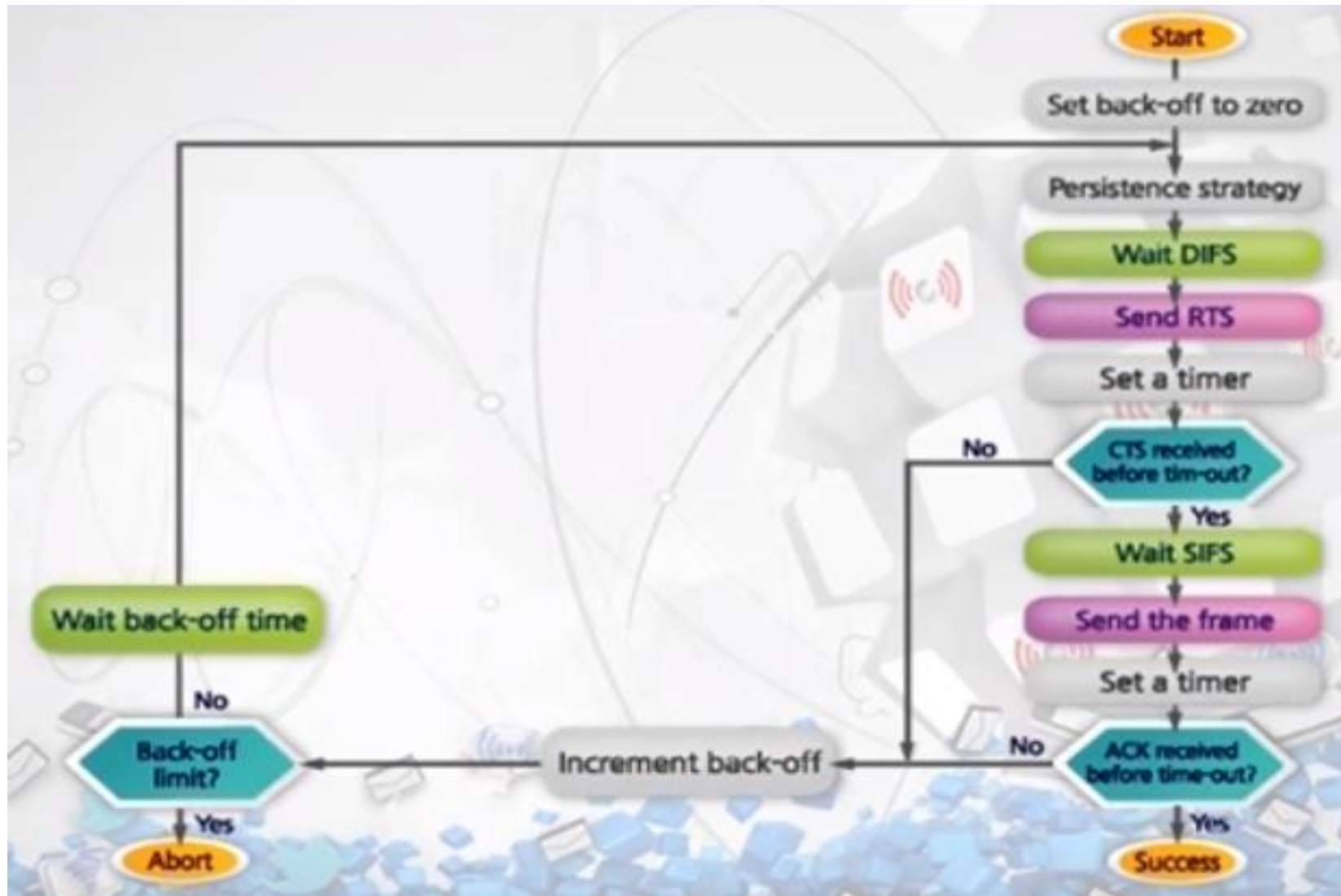
- ❖ 무선LAN 계층 (MAC의 부계층)
 - 무선LAN 표준 : IEEE 802.11
 - 무선LAN 표준(IEEE 802.11)의 정의
 - ✓ 2개의 MAC 부계층을 정의 (DCF와 PCF)
 - ✓ 데이터링크계층의 부계층(sub Layer) LLC와 MAC Layer 중 MAC Layer를 DCF와 PCF로 두 개로 나눈다
 - ✓ DCF : Distributed Coordination Function
 - ✓ PCF : Point Coordination Function
- ❖ 무선LAN에서 CSMA/CD를 사용하지 못하는 이유 (2가지)
 - Hidden Terminal Problem(숨겨진 단말기)
 - Signal Fading

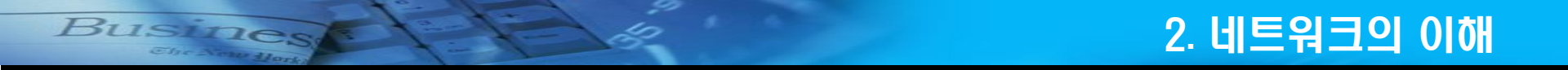
❖ 무선LAN에서 CSMA/CD를 사용하지 못하는 이유 (2가지)

- Hidden Terminal Problem(숨겨진 단말기)
- Hidden Terminal Problem(숨겨진 단말기) 해결방안



❖ 무선LAN에서 CSMA/CA





❖ 무선LAN에서 CSMA/CD를 사용하지 못하는 이유 (2가지)

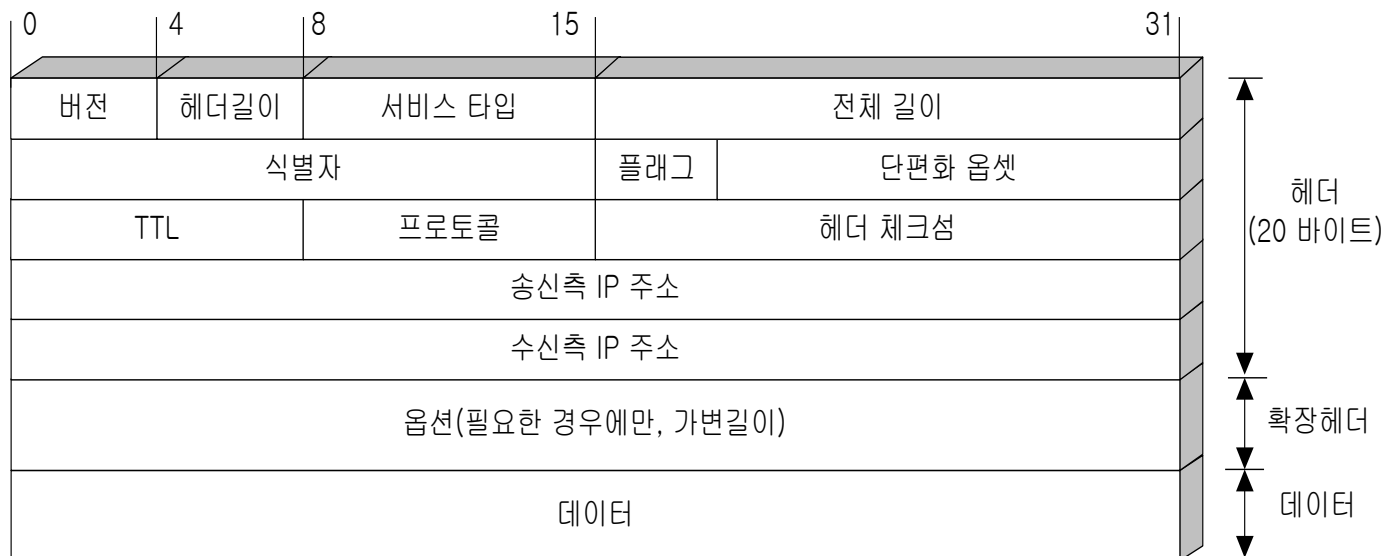
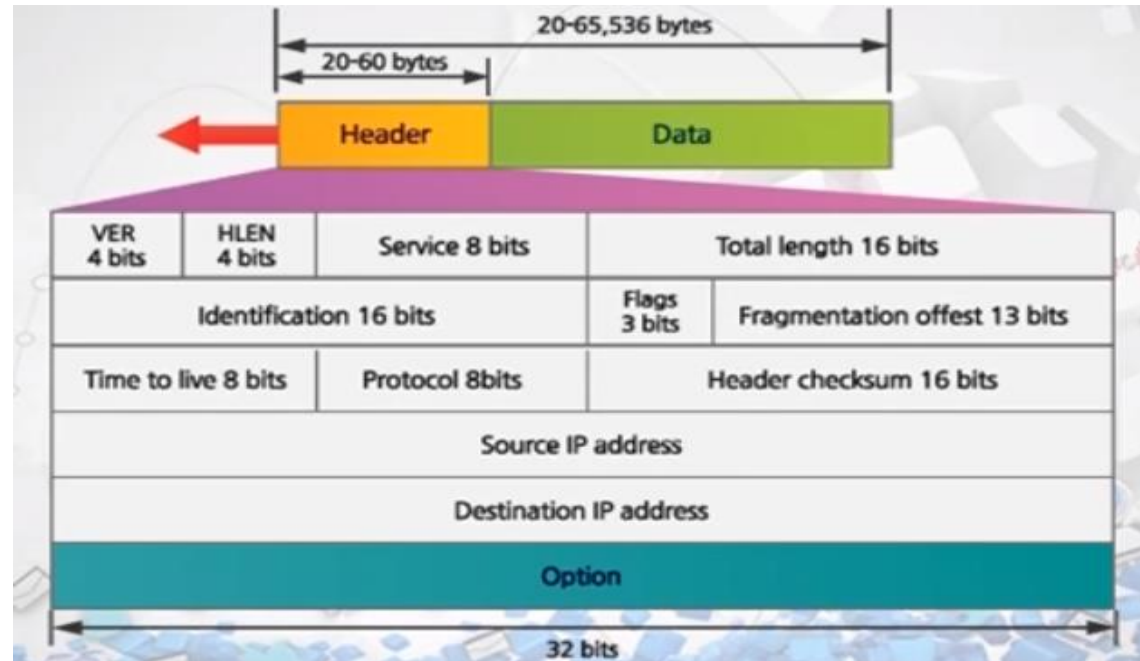
- Signal Fading
 - ✓ shadow fading(그림자 fading)
 - ✓ 선택적 fading (Frequency Selective Fading)
 - Frequency Selective Fading
 - Time selective fading

❖ IP(Internet protocol)

- IP의 특징
 - ✓ 비신뢰성(Unreliable)
 - 가능한 범위 내에서 패킷을 목적지까지 전달하는 최선형 서비스(Best Effort Service)
 - IP는 신뢰성이 없다
 - IP + TCP = 신뢰성 있는 전송
 - IP패킷 = IP데이터그램
 - ✓ 비접속형(Connectionless)
 - 연결(connection) 설정 없이 패킷을 전송
 - ✓ 주소 지정
 - 네트워크 내의 노드를 고유하게 지정하기 위한 수단으로 IP 주소를 사용
 - ✓ 경로 결정
 - 목적지 IP 주소를 기반으로 패킷 전달 경로를 판단

❖ IP(Internet protocol)

■ IP Packet 구성

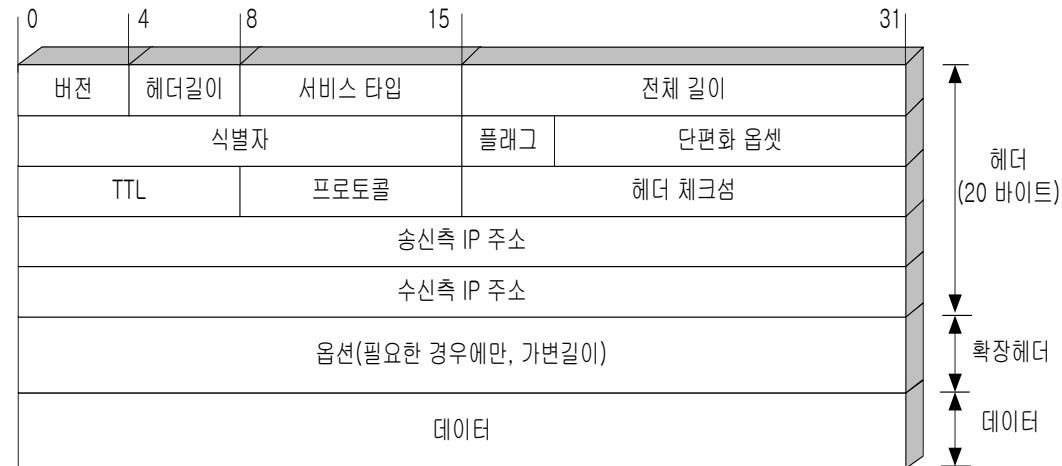


❖ IP(Internet protocol)

■ IP Packet 구성

✓ 헤더 전체적인 구조

- 기본 헤더 : 4byte * 5줄 = 20byte
- Option = 40byte
- Total = 60byte
- 헤더는 최소 20byte에서 60byte로 가변



✓ 헤더 필드의 역할

- 버전(VER : Version) : IP 프로토콜의 버전을 의미(값은 4 또는 6)
- 헤더 길이(HLEN : Header Length)
 - 옵션 필드를 포함한 헤더의 총 길이
 - 헤더의 크기를 나타내는 것으로 4바이트 단위로 나타낸 크기이며, 크기는 가변적
 - 헤더의 전체적인 구조에서 설명한 헤더의 총 길이(최소 20Byte~60byte까지 가변)
 - 표기는 4바이트 단위로 표기한다 (5라고 되어 있으면 4바이트 * 5 = 20byte, 6이면 24byte).
 - 표기할 수 있는 부문 : 5~15(5(20byte) ~15(60byte))

IP(Internet protocol)

IP Packet 구성

✓ 서비스 타입(Type-Of-Service)

- IP패킷이 가져야 하는 서비스의 형태
- 서비스는 응용 서비스별 주요하게 다루어져야 할 특성
- 지연시간, 신뢰성, 처리량 등
- 총 8비트(우선권(Precedence): 3비트, TOS(Type-Of-Service) :4 비트, 예약 : 1 비트
- Type Of Service (TOS) Flag (8 bits)구조

Precedence(우선순위)	D	T	R	C	0
0	1	2	3	4	5
6	7				

✓ 우선순위 설정 : Bit 0-2

- . 000 : Routine (Normal)
- . 001 : Priority(우선순위)
- . 010 : Immediate(즉시)
- . 011 : Flash(플래시)
- . 100 : Flash Override
- . 101 : Critical
- . 110 : Internetwork Control
(OSPF에서 셋팅됨)
- . 111 : Nnetwork Control

0	4	8	15	31
버전	헤더길이	서비스 타입	전체 길이	
식별자			플래그	단편화 옵션
TTL	프로토콜		헤더 체크섬	
송신측 IP 주소				
수신측 IP 주소				
옵션(필요한 경우에만, 가변길이)				
데이터				

IP(Internet protocol)

IP Packet 구성

- Type Of Service (TOS) Flag (8 bits)구조

Precedence(우선순위)	D	T	R	C	0		
0	1	2	3	4	5	6	7

✓ Bit 3 : Delay (지연)

. 0 : 보통의 지연, 1 : 높은 지연

✓ Bit 4 : Throughput (처리율)

. 0 : 보통 처리율, 1 : 높은 처리율

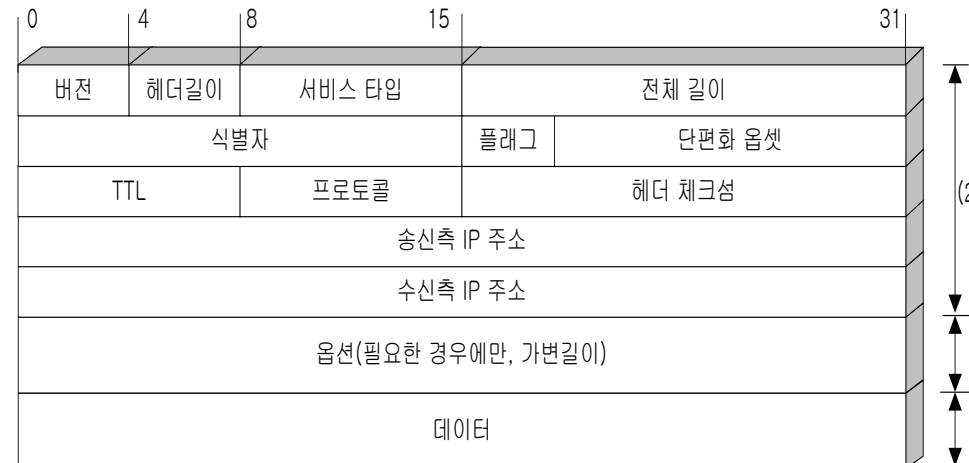
✓ Bit 5 : Reliability (신뢰성)

. 0 : 보통 신뢰성, 1 : 높은 신뢰성

✓ Bit 6 : Minimum Cost (최소비용)

✓ Bit 7 : 항상 0으로 셀팅됨

0 보통
1 저비용



❖ IP(Internet protocol)

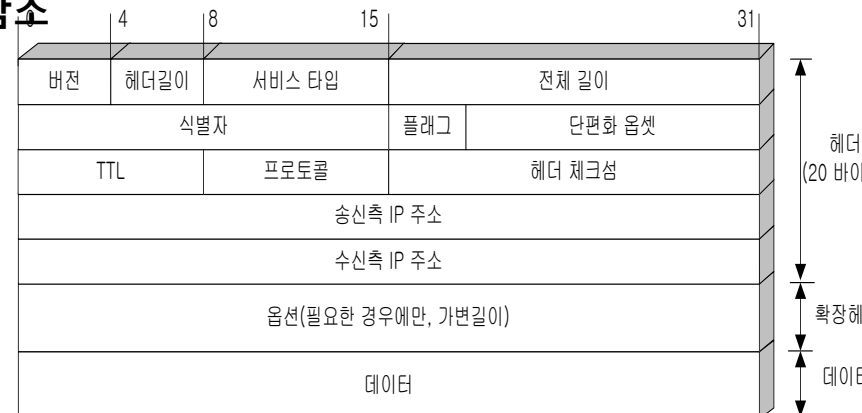
■ IP Packet 구성

• 전체 길이(Total Length)

- ✓ 헤더와 데이터를 포함한 IP 패킷의 전체 길이
- ✓ 바이트 단위로 표시
- ✓ 전체의 필드 크기(최대 길이)가 16비트로 이루어져 있기 때문에 IP 패킷의 총 가능한 길이를 표시할 수 있는 최대의 수는 2의 16제곱-1인 0~65535바이트 까지 가능하다
- ✓ IP패킷의 최대의 길이는 65,535byte 이다

• TTL (Time-To-Live) : 생존시간

- ✓ IP 데이터그램(IP 패킷)이 지나가는 최대 홉(hop)수
- ✓ 패킷이 라우터를 통과할 때마다 TTL 값은 1씩 감소
- ✓ TTL 값이 0이 되면 라우터는 해당 패킷은 폐기

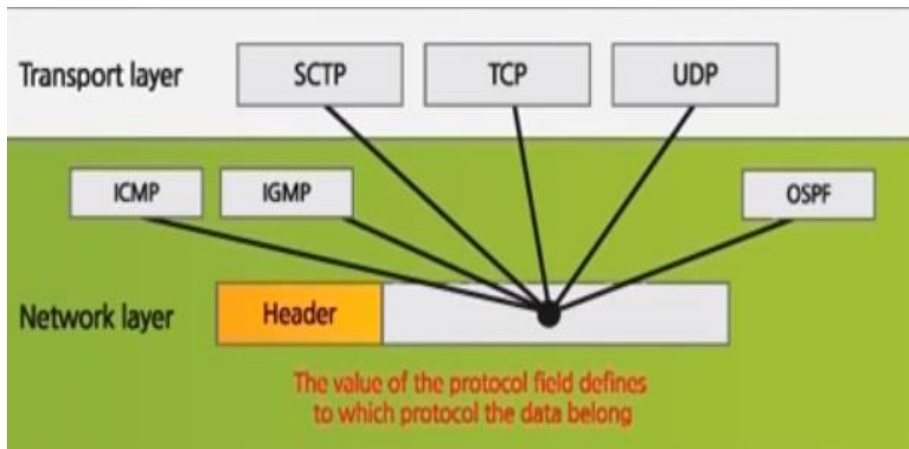


❖ IP(Internet protocol)

■ IP Packet 구성

• 프로토콜(Protocol)

- ✓ IP계층 위에서 존재하는 상위 프로토콜이 무엇인지 나타낸다
- ✓ 상위 프로토콜
 - 네트워크 계층 : ICMP, IGMP, OSPF
 - 전송계층 ; TCP, UDP 등
 - TCP는 6번, UDP는 17번, ICMP는 1번 값을 사용한다.
 - 그외 : IGMP 2번, IGRP 9번, GRE 47번, ESP 50번, EIGRP 88번, OSPF 89번 등



❖ IP(Internet protocol)

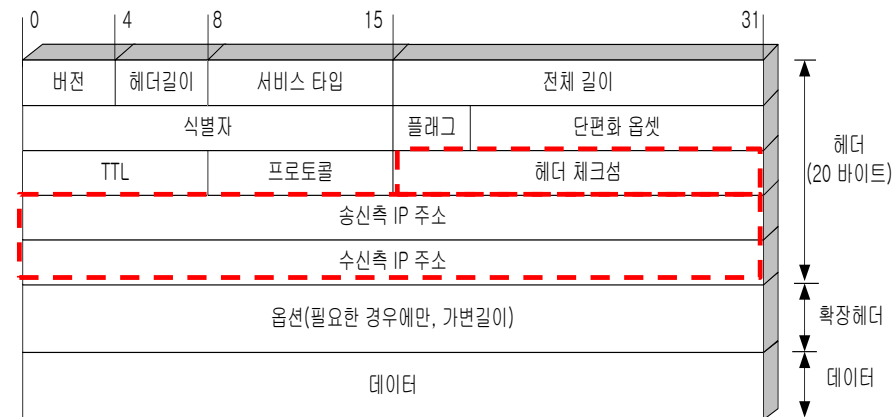
■ IP Packet 구성

• 헤더 체크섬(Header Checksum)

- ✓ IP 패킷 헤더의 오류 발생을 검사하기 위한 필드
- ✓ 헤더가 에러가 나면 폐기 시킨다
- ✓ 계산 방법
 - 전체의 헤더를 16비트 단위로 구분하여 1의 보수 덧셈연산을 수행
 - 그 결과값을 보수로 만들어서 체크섬 필드에 저장
 - 체크섬 필드를 포함해서 더 했을 때 0이 나오면 에러가 없다

• 송신자 주소와 목적지 주소

- ✓ 송신자와 수신자의 IP address



❖ IP(Internet protocol)

■ IP Packet 구성

• 단편화(Fragmentation) 옵션

- ✓ IP패킷을 잘라서 보내는 행위를 단편화 (Fragmentation)
- ✓ 어떤 네트워크에서 보낼 수 있는 최대의 크기 또는 최대로 보낼수 있는 메시지 단위를 MTU(Maximum transfer unit)

• 플래그(Flage)

✓ 3비트로 구성

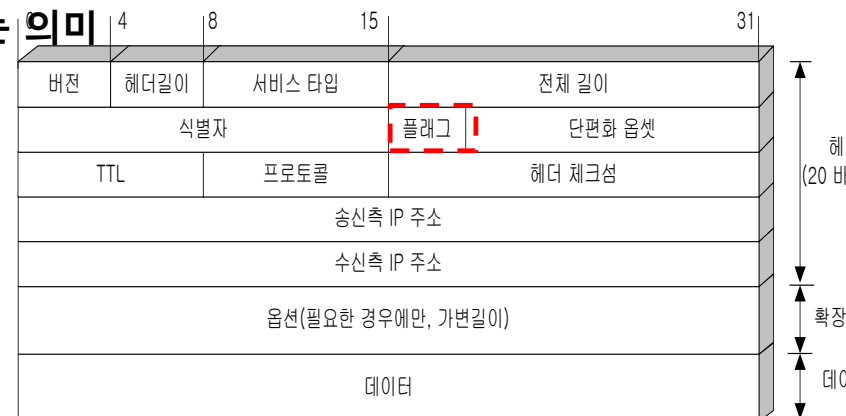
- 첫번째 비트 : 사용하지 않음(예약) 예약 비트 항상 "0"
- 두번째 비트 : DF bit(do not fragment) 단편화 금지

"1"이면 패킷을 자르지 못한다는 의미

- 세번째 비트 : MF bit(more fragment)

추가 단편화 비트

"1"이면 잘려진 패킷이 더 있다는 의미

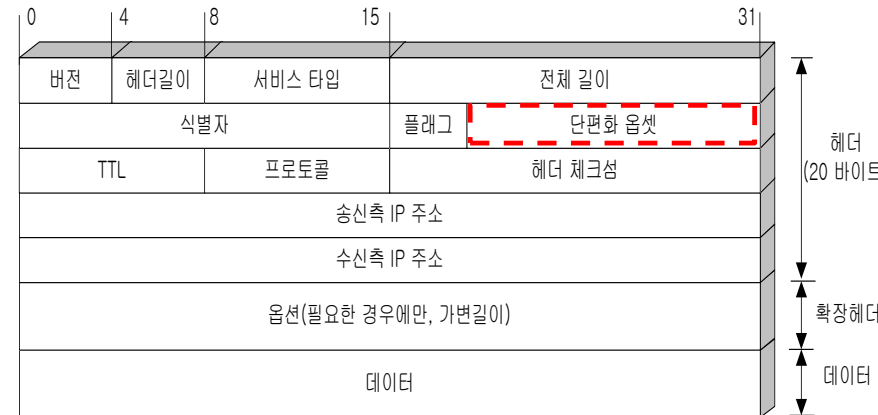
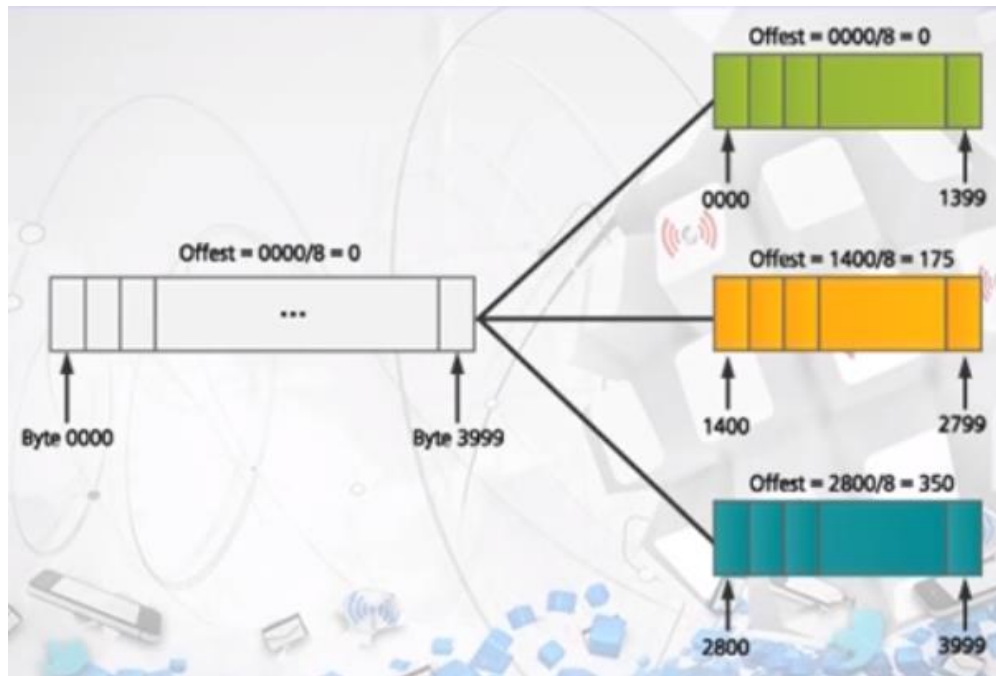


❖ IP(Internet protocol)

■ IP Packet 구성

• 단편화 위치(오프셋)(Fragmentation offset)

- ✓ 전체의 패킷에서 해당되는 단편이 차지하는 위치의 값을 의미
- ✓ 위치의 값은 첫번째 부터 시작하여 8비트 단위로 표시



❖ IP(Internet protocol)

■ IP Packet 구성

• 식별자(Identification)

- ✓ IP에서 링크의 최대 전달 유닛(MTU)보다 더 큰 데이터를 보내야 하는 경우 여러 개의 작은 패킷으로 전달 한다.
- ✓ 이 분할된 패킷이 목적지에서 다시 조립이 되는데 동일한 데이터로부터 분할된 패킷을 재조립할 수 있도록 분할된 패킷들은 같은 식별자를 가짐

✓ 옵션

- 옵션은 최대 40 바이트까지 사용할 수 있다
- 옵션은 4가지로 나눌 수 있다

. Record route(레코드 루트) : IP패킷이 가면서 경로를 기억하는 기능

. Strict source route(엄격한 소스루트) : Router의 경로를 정확하게 지정하는 것

. Loose source route(느슨한 소스루트) :

라우터를 지정한 곳만 경유, 그 외에는 지정하지 않음

. Timestamp(타임스탬프) :

패킷이 라우터에 도착하는 시간을 기록

1/1,000,000초 단위

0	4	8	15	31
버전	헤더 길이	서비스 타입	전체 길이	
식별자			플래그	단편화 옵션
TTL		프로토콜	헤더 체크섬	
송신측 IP 주소				
수신측 IP 주소				
옵션(필요한 경우에만, 가변길이)				
데이터				

○ Network 계층 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

명령 프롬프트

```
13...00 c2 c6 a9 e3 b9 .....Microsoft Wi-Fi Direct Virtual Adapter
18...02 c2 c6 a9 e3 b8 .....Microsoft Wi-Fi Direct Virtual Adapter #2
11...00 c2 c6 a9 e3 b8 .....Intel(R) Dual Band Wireless-AC 8260
9...00 c2 c6 a9 e3 bc .....Bluetooth Device (Personal Area Network)
1.....Software Loopback Interface 1
```

IPv4 경로 테이블

활성 경로:

네트워크 대상	네트워크 마스크	게이트웨이	인터페이스	메트릭
0.0.0.0	0.0.0.0	192.168.10.1	192.168.10.105	50
127.0.0.0	255.0.0.0		127.0.0.1	331
127.0.0.1	255.255.255.255		127.0.0.1	331
127.255.255.255	255.255.255.255		127.0.0.1	331
169.254.0.0	255.255.0.0		169.254.149.19	281
169.254.149.19	255.255.255.255		169.254.149.19	281
169.254.255.255	255.255.255.255		169.254.149.19	281
192.168.10.0	255.255.255.0		192.168.10.105	306
192.168.10.105	255.255.255.255		192.168.10.105	306
192.168.10.255	255.255.255.255		192.168.10.105	306
224.0.0.0	240.0.0.0		127.0.0.1	331
224.0.0.0	240.0.0.0		192.168.10.105	306
224.0.0.0	240.0.0.0		169.254.149.19	281
255.255.255.255	255.255.255.255		127.0.0.1	331
255.255.255.255	255.255.255.255		192.168.10.105	306
255.255.255.255	255.255.255.255		169.254.149.19	281

①

②

PC의 라우팅 테이블
명령어 : Route print

영구 경로:

없음

IPv4 경로 테이블

○ Network 계층 장비

✓ 정적라우팅

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

✓ 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

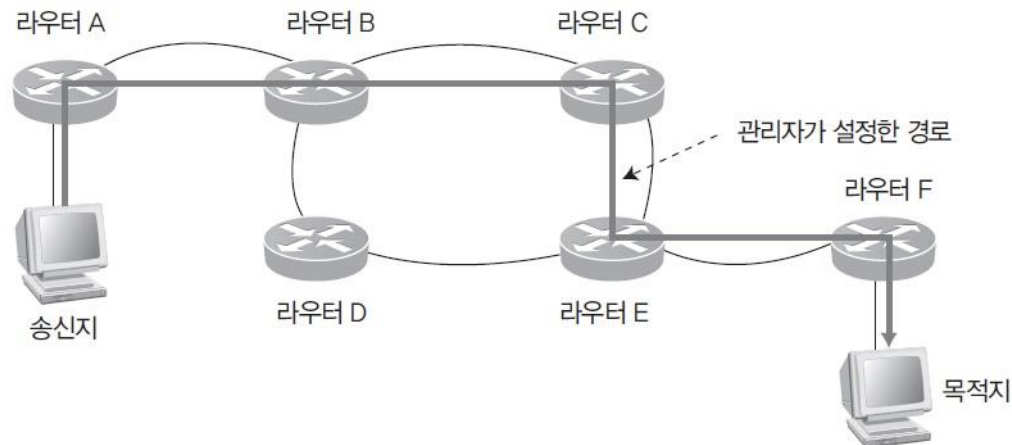


그림 2-26 정적 라우팅

○ Network 계층 장비

✓ 동적라우팅

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

✓ 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

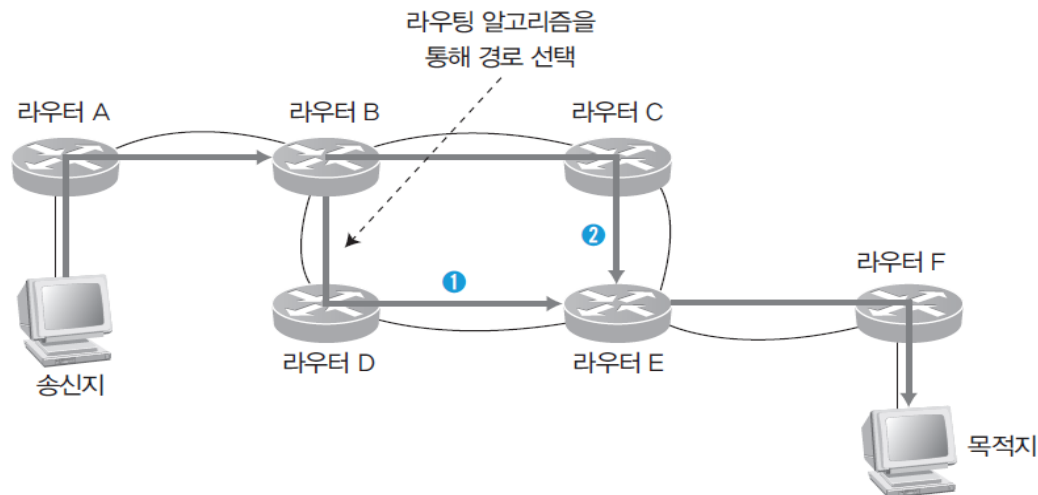


그림 2-27 동적 라우팅

○ Network 계층 장비

✓ 정적라우팅과 동적라우팅의 비교

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

○ 전송 계층 (Transport Layer)

- ✓ 전송 계층을 기점으로 네트워크 서비스와 상위 사용자 서비스 구분됨
- ✓ 전체 메시지의 종단간 전달
- ✓ 흐름 제어 및 오류 제어 기능
- ✓ 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).

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

- 전송 계층 (Transport Layer)
 - ❖ 클라이언트/서버의 구성
 - 프로세스간의 통신은 클라이언트와 서버 구성을 통하여 이루어 진다
 - 포트번호는 전송계층에서 사용되는 주소로서 특정 호스트에서 실행되는 프로세스를 구분하기 위하여 사용한다
 - 포트번호는 16비트 정수로 0에서 65535사이의 값을 갖는다
 - 포트 번호는 IP주소를 가진 컴퓨터 에서 여러 개의 프로세스를 구분하기 위한 역할
 - ❖ IANA(Internet Assigned Numbers Authority) 는 포트번호를 3개의 영역으로 구분
 - Well-Known Port : 0~1023까지 할당되며 인터넷 서비스를 위하여 사용
 - Registered Port : 1024~49151까지 할당되며, 특정응용을 위하여 기업이 사용한다
 - Dynamic Port : 49152 ~ 65535 까지 할당되며, 임시포트로 이용한다

○ 전송 계층 (Transport Layer)의 Protocol

- ✓ 대표적인 Protocol : TCP(Transmission Control Protocol), UDP(User Datagram Protocol)
- ✓ TCP(Transmission Control Protocol)
 - 연결 지향형 프로토콜
 - IP와 함께 통신을 하는 데 반드시 필요한 가장 기본적인 프로토콜
- ✓ TCP의 기능
 - TCP는 프로세스간의 통신, 스트림전달 서비스
 - 전이중, 연결지향 서비스,
 - 신뢰성 있는 서비스(데이터가 안전하게 도착확인 신호 ACK를 사용)
 - 프로세스간의 통신을 위하여 포트번호를 사용
- ✓ TCP의 특징
 - 높은 신뢰성
 - 가상 회선 연결 방식
 - 연결의 설정과 해제
 - 데이터 체크섬
 - 시간 초과와 재전송
 - 데이터 흐름 제어

○ 전송 계층 (Transport Layer)의 Protocol

✓ TCP(Transmission Control Protocol)



○ 전송 계층 (Transport Layer)의 Protocol

✓ 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.

○ 전송 계층 (Transport Layer)의 Protocol

✓ UDP(User Datagram Protocol)

- UDP의 헤더는 8바이트로 고정되어 있다
- UDP의 체크섬은 선택사항이며, 가상헤더의 중요한 필드는 한 번 더 검사를 위해 가상헤더를 붙여 메시지를 확인

✓ UDP의 헤더

송신 포트번호(16비트)	수신 포트번호(16비트)
전체 길이(16비트)	체크섬(16비트)
데이터(if any)	

○ 전송 계층 (Transport Layer)의 Protocol

✓ UDP(User Datagram Protocol)동작

- 비연결형 서비스를 제공
 - 데이터그램들 사이에 서로 관련이 없어 번호를 붙이지 않음
 - 연결설정, 종료과정이 없음
 - UDP의 각 데이터그램은 서로다른 경로로 전달 될 수 있다
- 흐름제어나 에러제어(오류제어)가 없다
 - 수신자는 수신 메시지로 오버플로우 될 수 있다
 - 송신자는 메시지가 유실 되거나 종료되는지 알 수 없다

✓ UDP(User Datagram Protocol)사용

- UDP는 간단한 요청-응답 서비스에 적합
 - 연결설정/해제 과정의 오버헤드가 없다
- UDP는 프로세스에서 내부 흐름제어와 에러제어를 갖는 경우에 적합
 - 응용프로그램의 자체적으로 가지고 있는 기능을 중복해서 가질 필요가 없다
- UDP는 멀티캐스팅에 적합
 - 그룹에 속한 모든 시스템과 연결 설정할 필요가 없다
- DNS, NFS, SNMP, RIP 같은 관리 시스템에 사용

- 전송 계층 (Transport Layer)의 Protocol
 - ✓ TCP(Transmission Control Protocol) 와 UDP(User Datagram Protocol) 동작비교

	TCP	UDP
연결 방식	연결형 프로토콜 연결 후 통신 1:1 통신 방식	비연결형 프로토콜 연결 없이 통신 1:1, 1:N, N:N 통신 방식
특징	<ul style="list-style-type: none">- 데이터의 경계를 구분 안함- 신뢰성 있는 데이터 전송- 데이터의 전송 순서 보장- 데이터의 수신 여부 확인- 패킷을 관리할 필요 없음- UDP보다 전송속도가 느림	<ul style="list-style-type: none">- 데이터의 경계를 구분함- 신뢰성 없는 데이터 전송- 데이터의 전송 순서가 바뀔 수 있음- 데이터의 수신 여부를 확인 안함- 패킷을 관리해야함- TCP보다 전송속도가 빠름
관련 클래스	.Socket .ServerSocket	.DatagramSocket .DatagramPacket .MulticastSocet

○ 응용 계층(Application Layer)

- ✓ 응용 프로세스에게 네트워크 접근 수단 제공
- ✓ 관련 응용 프로그램이 별도로 존재하며, 여러 가지 프로토콜에 대하여 사용자 인터페이스를 제공
- ✓ Application Layer Protocol
 - 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
 - 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

○ 응용 계층(Application Layer)

- ✓ 관련 응용 프로그램이 별도로 존재하며, 여러 가지 프로토콜에 대하여 사용자 인터페이스를 제공
- ✓ Application Layer Protocol
 - 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

○ 계층별 패킷 분석

- Wireshark를 이용하여 각 계층의 패킷을 분석
- 직접 Wireshark를 이용하여 패킷을 캡처하고 있는상태

Capturing from Npcap Loopback Adapter

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Poply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Time shift for this packet	Info
1	0.000000	fe80::a582:3313:d218:32c4	ff02::fb	ICMPv6	86	0.000000000	Multicast Listener Report
2	0.271259	fe80::a582:3313:d218:32c4	ff02::1:ff18:32c4	ICMPv6	86	0.000000000	Multicast Listener Report
3	0.271646	fe80::a582:3313:d218:32c4	ff02::1:3	ICMPv6	86	0.000000000	Multicast Listener Report
4	0.271903	fe80::a582:3313:d218:32c4	ff02::c	ICMPv6	86	0.000000000	Multicast Listener Report
5	28.921887	192.168.10.105	192.168.10.255	NBNS	92	0.000000000	Name query NB HPAF90CC<00>
6	28.922398	169.254.149.19	224.0.0.251	MDNS	74	0.000000000	Standard query 0x0000 A hpaf90cc.local, "QM" question
7	28.922702	192.168.10.105	224.0.0.251	MDNS	74	0.000000000	Standard query 0x0000 A hpaf90cc.local, "QM" question
8	28.923069	fe80::b8cc:a6c8:e6b8:9513	ff02::fb	MDNS	94	0.000000000	Standard query 0x0000 A hpaf90cc.local, "QM" question
9	28.923360	fe80::a582:3313:d218:32c4	ff02::fb	MDNS	94	0.000000000	Standard query 0x0000 A hpaf90cc.local, "QM" question
10	28.923835	169.254.149.19	224.0.0.251	MDNS	74	0.000000000	Standard query 0x0000 AAAA hpaf90cc.local, "QM" question
11	28.924058	192.168.10.105	224.0.0.251	MDNS	74	0.000000000	Standard query 0x0000 AAAA hpaf90cc.local, "QM" question
12	28.924321	fe80::b8cc:a6c8:e6b8:9513	ff02::fb	MDNS	94	0.000000000	Standard query 0x0000 AAAA hpaf90cc.local, "QM" question
13	28.924528	fe80::a582:3313:d218:32c4	ff02::fb	MDNS	94	0.000000000	Standard query 0x0000 AAAA hpaf90cc.local, "QM" question
14	28.925437	fe80::a582:3313:d218:32c4	ff02::1:3	LLMNR	88	0.000000000	Standard query 0x55ad A hpaf90cc
15	28.925687	192.168.10.105	224.0.0.252	LLMNR	68	0.000000000	Standard query 0x55ad A hpaf90cc
16	28.926204	fe80::a582:3313:d218:32c4	ff02::1:3	LLMNR	88	0.000000000	Standard query 0xabed AAAA hpaf90cc
17	28.926427	192.168.10.105	224.0.0.252	LLMNR	68	0.000000000	Standard query 0xabed AAAA hpaf90cc
18	28.927155	169.254.149.19	169.254.255.255	NBNS	92	0.000000000	Name query NB HPAF90CC<00>
19	28.927400	169.254.149.19	224.0.0.251	MDNS	74	0.000000000	Standard query 0x0000 A hpaf90cc.local, "QM" question
20	28.927588	192.168.10.105	224.0.0.251	MDNS	74	0.000000000	Standard query 0x0000 A hpaf90cc.local, "QM" question

< Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface \Device\NPF_{36F23396-43F1-41E5-9AB4-C03DCE069B5D}, id 0

> Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)

> Internet Protocol Version 6, Src: fe80::a582:3313:d218:32c4, Dst: ff02::fb

> Internet Control Message Protocol v6

```

0000  00 00 00 00 00 00 00 00 00 00 00 00 86 dd 60 00  .....
0010  00 00 00 20 00 01 fe 80 00 00 00 00 00 00 a5 82  ....
0020  33 13 d2 18 32 c4 ff 02 00 00 00 00 00 00 00 3...2...
0030  00 00 00 00 00 fb 3a 00 05 02 00 00 01 00 83 00  ....
0040  a0 bd 00 00 00 00 ff 02 00 00 00 00 00 00 00  ....
0050  00 00 00 00 00 fb  ....

```

○ 계층별 패킷 분석

✓ Wireshark 설치하고 실행하기

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

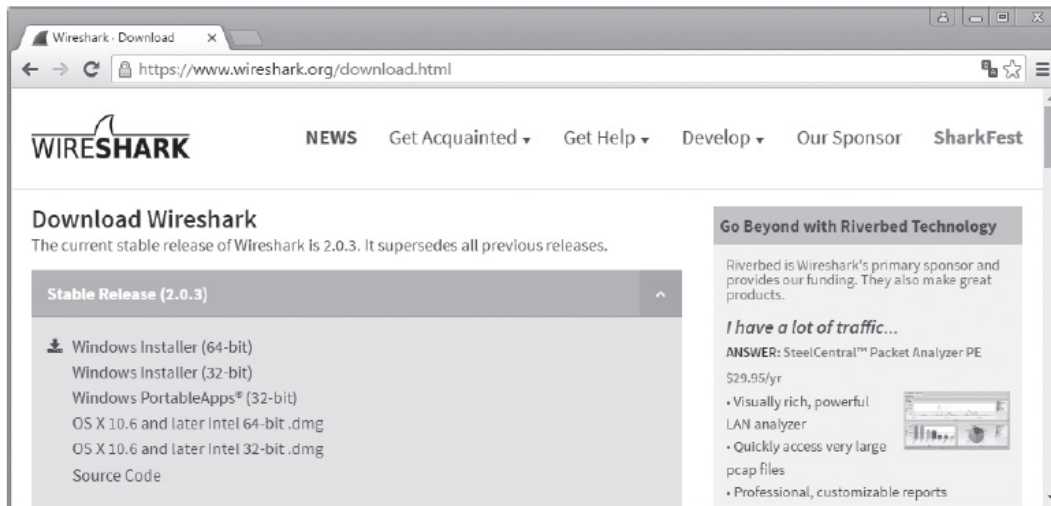


그림 2-33 Wireshark 다운로드 페이지

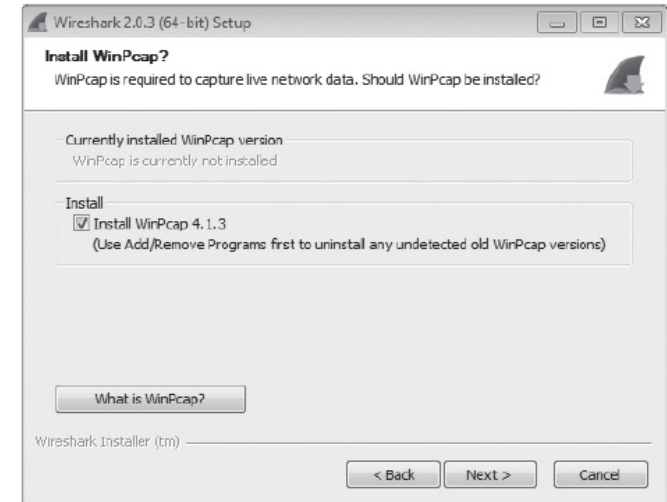


그림 2-34 설치 옵션에서 WinPcap 설치

Welcome to Wireshark

Capture

...using this filter:

All interfaces shown

Interface	Link Speed	Link Type	Link State
Npcap Loopback Adapter	1000 Mb/s	Loopback	Up
로컬 영역 연결* 12	1000 Mb/s	Ethernet	Up
Bluetooth 네트워크 연결	115.2 Kbps	Bluetooth	Up
Wi-Fi	1000 Mb/s	Wireless	Up
로컬 영역 연결* 3	1000 Mb/s	Ethernet	Up
로컬 영역 연결* 8	1000 Mb/s	Ethernet	Up
로컬 영역 연결* 10	1000 Mb/s	Ethernet	Up
로컬 영역 연결* 9	1000 Mb/s	Ethernet	Up
이더넷	1000 Mb/s	Ethernet	Up

○ 계층별 패킷 분석

✓ Wireshark 실행

■ 실제 실행되고 있는 Wireshark

Welcome to Wireshark

Capture

...using this filter:

Npcap Loopback Adapter

로컬 영역 연결* 12

Bluetooth 네트워크 연결

Wi-Fi

로컬 영역 연결* 3

로컬 영역 연결* 8

로컬 영역 연결* 10

로컬 영역 연결* 9

이더넷

Apply a display filter (Ctrl-F)

No.	Time	Source	Destination	Protocol	Length	Time shift for this packet	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	342	0.000000000	DHCP Discover - Transaction ID 0x92ebadb
2	0.000275	0.0.0.0	255.255.255.255	DHCP	342	0.000000000	DHCP Discover - Transaction ID 0x92ebadb
3	7.429671	192.168.10.105	192.168.10.255	NBNS	92	0.000000000	Name query NB HPAF90CC<00>
4	7.430343	169.254.149.19	224.0.0.251	MDNS	74	0.000000000	Standard query 0x0000 A hpaf90cc.local, "QM" question
5	7.430661	169.254.149.19	224.0.0.251	MDNS	74	0.000000000	Standard query 0x0000 A hpaf90cc.local, "QM" question
6	7.431081	192.168.10.105	224.0.0.251	MDNS	74	0.000000000	Standard query 0x0000 A hpaf90cc.local, "QM" question
7	7.431503	fe80::b8cc:a6c8:e6b8:9513	ff02::fb	MDNS	94	0.000000000	Standard query 0x0000 A hpaf90cc.local, "QM" question
8	7.431941	fe80::a582:3313:d218:32c4	ff02::fb	MDNS	94	0.000000000	Standard query 0x0000 A hpaf90cc.local, "QM" question
9	7.432670	169.254.149.19	224.0.0.251	MDNS	74	0.000000000	Standard query 0x0000 AAAA hpaf90cc.local, "QM" question
10	7.432917	169.254.149.19	224.0.0.251	MDNS	74	0.000000000	Standard query 0x0000 AAAA hpaf90cc.local, "QM" question
11	7.433137	192.168.10.105	224.0.0.251	MDNS	74	0.000000000	Standard query 0x0000 AAAA hpaf90cc.local, "QM" question
12	7.433531	fe80::b8cc:a6c8:e6b8:9513	ff02::fb	MDNS	94	0.000000000	Standard query 0x0000 AAAA hpaf90cc.local, "QM" question
13	7.433840	fe80::a582:3313:d218:32c4	ff02::fb	MDNS	94	0.000000000	Standard query 0x0000 AAAA hpaf90cc.local, "QM" question
14	7.434982	fe80::a582:3313:d218:32c4	ff02::1:3	LLMNR	88	0.000000000	Standard query 0xe4ea A hpaf90cc.local, "QM" question
15	7.435300	192.168.10.105	224.0.0.251	LLMNR	88	0.000000000	Standard query 0xe4ea A hpaf90cc.local, "QM" question

① 패킷목록 확인

6번 항목 클릭 → 결과 다음 페이지 참조

Frame 6: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{36F23396-43F1-41E5-9AB4-C03DCE8698D0}, id 0

Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: 00:00:00:00:00:00 (00:00:00:00:00:00)

Internet Protocol Version 4, Src: 192.168.10.105, Dst: 224.0.0.251

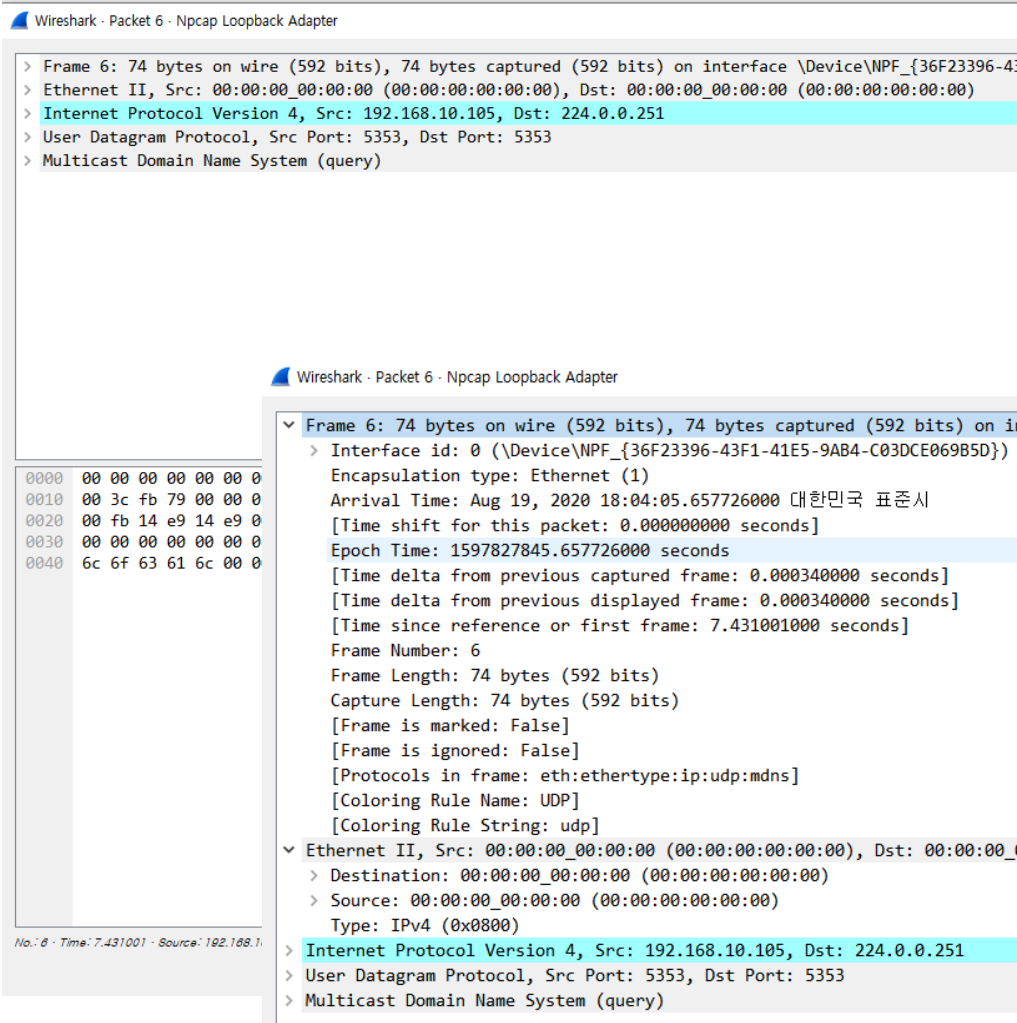
User Datagram Protocol, Src Port: 5353, Dst Port: 5353

Multicast Domain Name System (query)

```

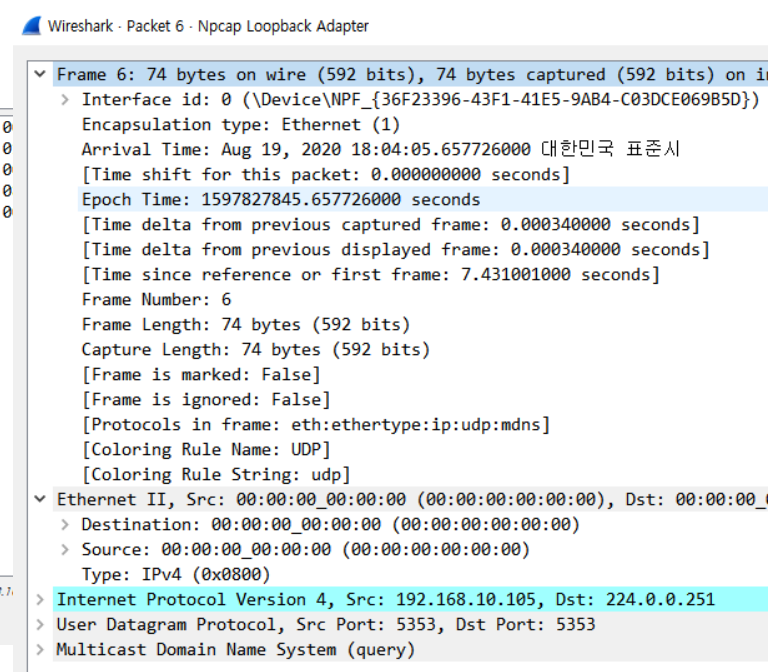
0000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....E-
0010  00 3c fb 79 00 00 01 11 00 00 c0 a8 0a 69 e0 00  .....<Y-.....i-
0020  00 fb 14 e9 14 e9 00 28 7b 7f 00 00 00 00 01  .....(.....{.....
0030  00 00 00 00 00 00 00 08 70 61 66 39 30 63 63 05  .....h paf90cc-
0040  6c 6f 63 61 6c 00 00 01 00 01  .....local...
  
```

- 계층별 패킷 분석
 - ✓ Wireshark 실행
 - 실제 실행되고 있는 Wireshark



각 계층별 패킷 정보 열람가능

- Frame정보
- Ethernet 정보
- IP 정보
- UDP 정보
- DNS정보



계층별 패킷 정보 클릭 시 세부정보 열람가능

- Frame 세부정보
- Ethernet 세부정보

- 계층별 패킷 분석
 - ✓ Wireshark 실행
 - 실제 실행되고 있는 Wireshark

```

▼ Frame 6: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{36F23396-43F1-41E5-9AB4-C03DCE069B5D}, id 0
  > Interface id: 0 (\Device\NPF_{36F23396-43F1-41E5-9AB4-C03DCE069B5D})
    Encapsulation type: Ethernet (1)
    Arrival Time: Aug 19, 2020 18:04:05.657726000 대한민국 표준시
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1597827845.657726000 seconds
    [Time delta from previous captured frame: 0.000340000 seconds]
    [Time delta from previous displayed frame: 0.000340000 seconds]
    [Time since reference or first frame: 7.431001000 seconds]
    Frame Number: 6
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:udp:mdns]
    [Coloring Rule Name: UDP]
    [Coloring Rule String: udp]
  ▼ Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
    > Destination: 00:00:00_00:00:00 (00:00:00:00:00:00)
    > Source: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Type: IPv4 (0x0800)
  > Internet Protocol Version 4, Src: 192.168.10.105, Dst: 224.0.0.251
  > User Datagram Protocol, Src Port: 5353, Dst Port: 5353
  > Multicast Domain Name System (query)

```

Frame 6 을 클릭을 하면 밑에 패킷에 대한 내용을
HEX와 ASCII 형식으로 보여 준다

```

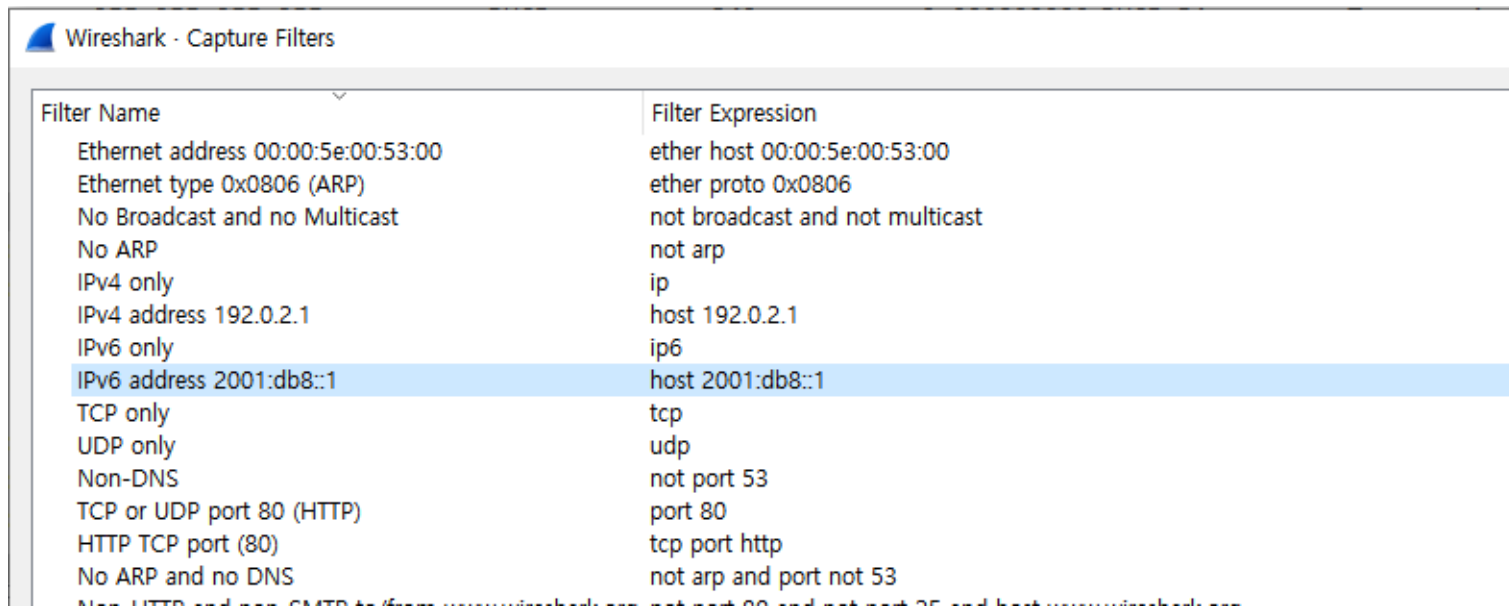
0000 00 00 00 00 00 00 00 00 00 00 00 08 00 45 00 .....E.
0010 00 3c fb 79 00 00 01 11 00 c0 a8 0a 69 e0 00 <.y....i..
0020 00 fb 14 e9 14 e9 00 28 7b 7f 00 00 00 00 01 .....( {.....
0030 00 00 00 00 00 00 08 68 70 61 66 39 30 63 63 05 .....h paf90cc-
0040 6c 6f 63 61 6c 00 00 01 00 01 local... ..

```

○ 계층별 패킷 분석

✓ Wireshark 실행

- Wireshark에서 Capture → Capture filters를 선택하면 특정프로토콜만 선택하여 캡처가 가능



The image shows the 'Wireshark - Capture Filters' dialog box. It contains a table with two columns: 'Filter Name' and 'Filter Expression'. The 'IPv6 address 2001:db8::1' filter is selected and highlighted in blue.

Filter Name	Filter Expression
Ethernet address 00:00:5e:00:53:00	ether host 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP)	ether proto 0x0806
No Broadcast and no Multicast	not broadcast and not multicast
No ARP	not arp
IPv4 only	ip
IPv4 address 192.0.2.1	host 192.0.2.1
IPv6 only	ip6
IPv6 address 2001:db8::1	host 2001:db8::1
TCP only	tcp
UDP only	udp
Non-DNS	not port 53
TCP or UDP port 80 (HTTP)	port 80
HTTP TCP port (80)	tcp port http
No ARP and no DNS	not arp and port not 53
Not HTTP and not SMTP to/from www.wireshark.org	not port 80 and not port 25 and host www.wireshark.org