

TCP/IP 4계층 (TCP/IP 4 Layer)

□ OSI 7계층

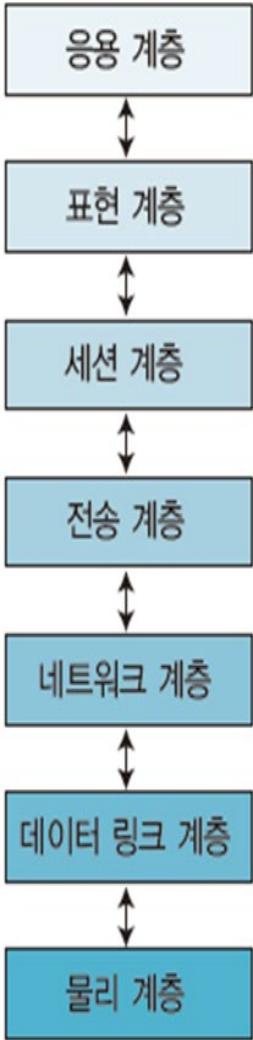
- 표준이 정립되기 전 여러 정보 통신 업체 장비들은 자신의 업체 장비 사이에서의 연결만 지원하고 다른 업체 장비와의 호환성은 지원하지 않음
- 위 이유로 ISO에서 1984년에 OSI모델을 발표하게 됨
- 모든 시스템들의 상호 연결에 있어 문제가 없도록 표준을 만든 것이며 7개의 계층으로 구분

□ TCP/IP 4계층

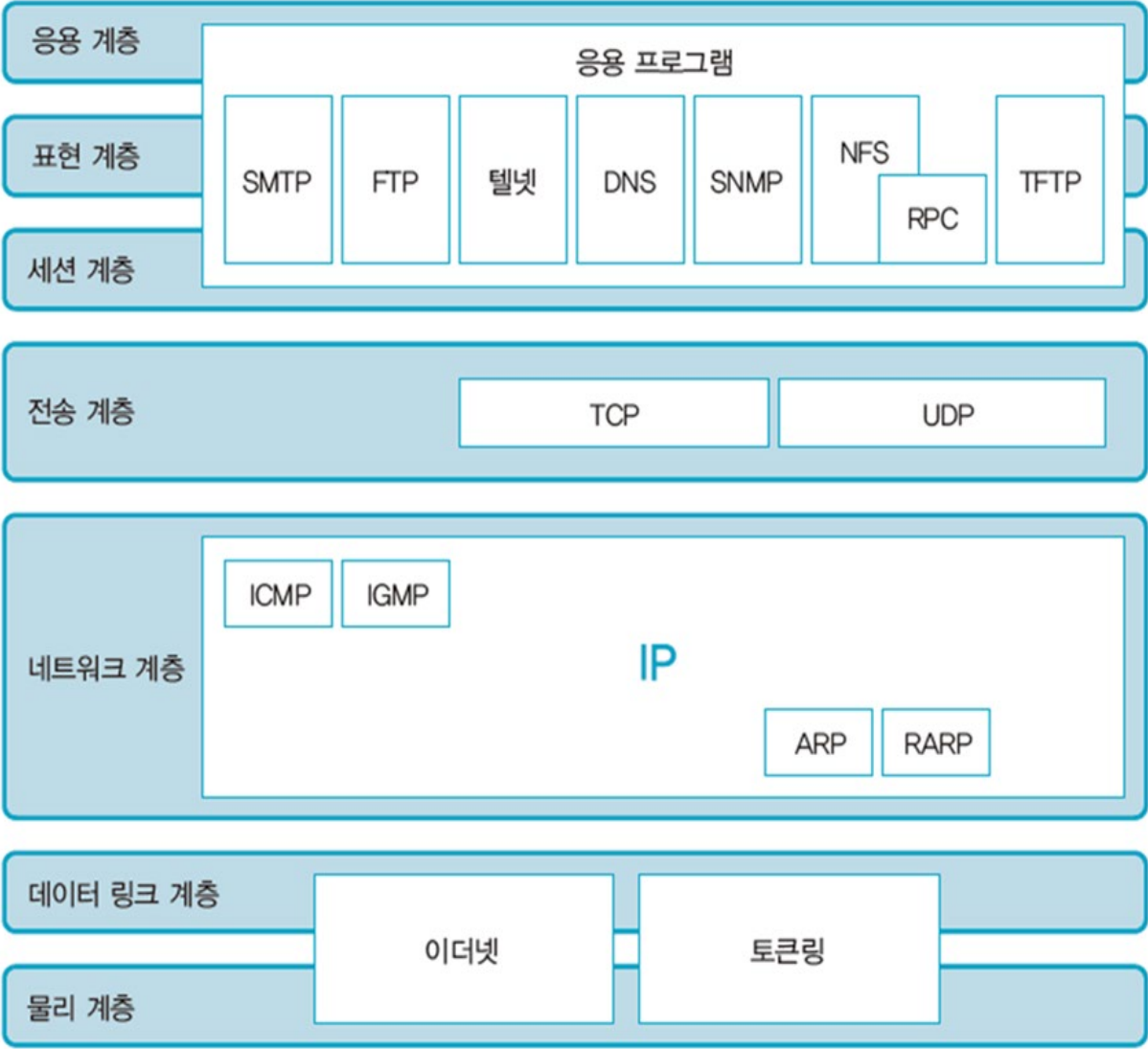
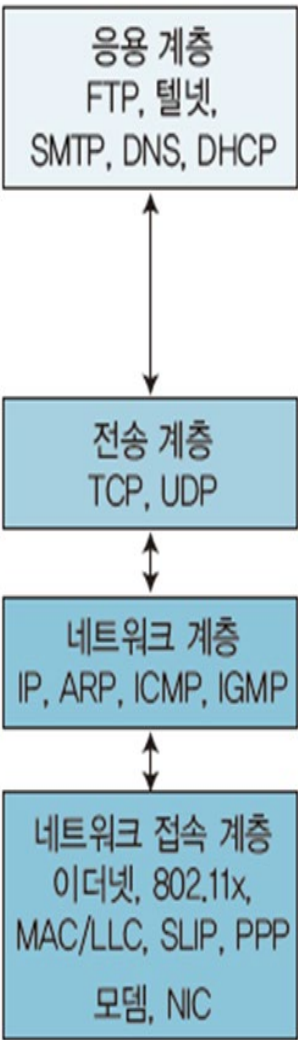
- 1960년대 말 방위고등연구계획국(DARPA)이 수행한 연구개발의 결과로 탄생하였으며 군사적 목적으로 사용하기 위한 통신규약(프로토콜)의 모음
- 이런 통신규약을 모아둔 것을 스위트 또는 슈트(Suite)라고 하며 프로토콜의 모음으로 Protocol Suite라고 부름
- 군사적 목적으로 사용하기 위해 만들어졌지만 민간에 개방이 되면서 네트워크와 네트워크 사이를 연결하면서 internet protocol suite(인터넷 프로토콜 스위트)라고 하였으나 이중 TCP와 IP가 가장 많이 사용되어 TCP/IP 프로토콜 스위트라고 불림
- 현재는 우리가 사용하는 인터넷의 표준이 되어 인터넷 모델이라고도 한다.

OSI 7계층과 TCP/IP 계층 비교

OSI 참조 모델 7계층



TCP/IP 프로토콜 계층



OSI 7계층과 TCP/IP 계층 비교표

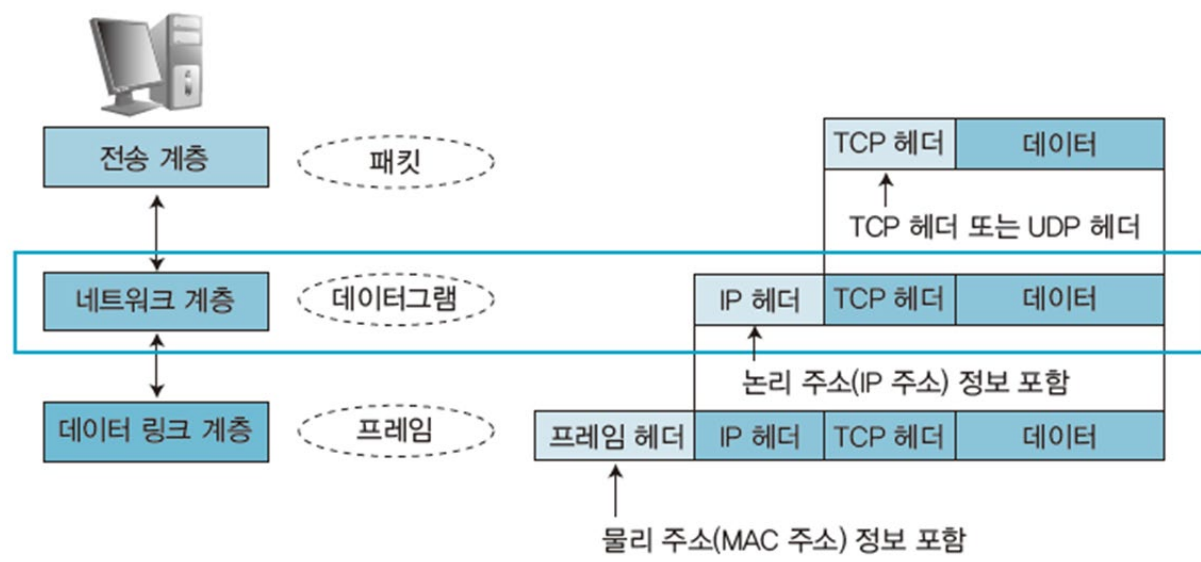
항목	OSI 모델	TCP/IP 모델
계층	- 7계층 구조	- 4계층 구조
구현	- 모델을 만들고 실제 구현을 진행함	- 이미 실제로 구현된 기술을 바탕으로 만들
문제점	- 너무 복잡하여 여러 계층에 중복된 기능이 존재함	- 프로토콜간의 경계나 기능들이 확실히 구분되어 있지 않음
공통점	<div>- 두 모델 모두 계층적 구조를 가짐</div> <div>- 다양한 서비스를 가진 응용프로그램 계층이 존재함</div> <div>- 전송계층/네트워크 계층과 호환되는 계층이 존재함</div> <div>- 패킷 스위칭 기술을 기반으로 함</div>	
차이점	<div>- TCP/IP 프로토콜은 인터넷 표준이며 높은 신뢰성 보장</div> <div>- 현실 네트워크는 구체적인 OSI 프로토콜로 만들어지지 않음</div>	

- ❑ 인터넷 모델의 응용 계층에 포함되어 있는 프로토콜과 프로그램은 원격으로 컴퓨터 자원에 접속하는 데 사용
- ❑ 응용 프로그램들로 제공되는 서비스는 표현 계층과 세션 계층에서 정의



TCP/IP – Internet Layer (인터넷 계층)

- OSI 참조 모델의 네트워크 계층과 비슷하여 '네트워크 계층'이라고도 함
- 네트워크의 패킷 전송을 제어하며, 데이터를 전송할 때 경로를 선택
- IP와 ARP, ICMP, IGMP 프로토콜로 구성
- TCP/IP에서 가장 중요한 프로토콜 중 하나인 IP는 네트워크의 주소 체계 관리, 데이터그램을 정의, 전송에 필요한 경로를 결정
 - 송신 측 컴퓨터 : 상위 계층에서 전달받은 패킷에 논리적 주소인 IP주소를 포함하는 헤더를 추가하여 하위 계층인 데이터 링크 계층으로 전달
 - 수신 측 컴퓨터 : 하위 계층에서 전달받은 패킷의 헤더 정보를 확인한 후 송신 측 컴퓨터의 인터넷 계층에서 추가한 헤더를 제거하여 상위 계층인 전송 계층으로 전달

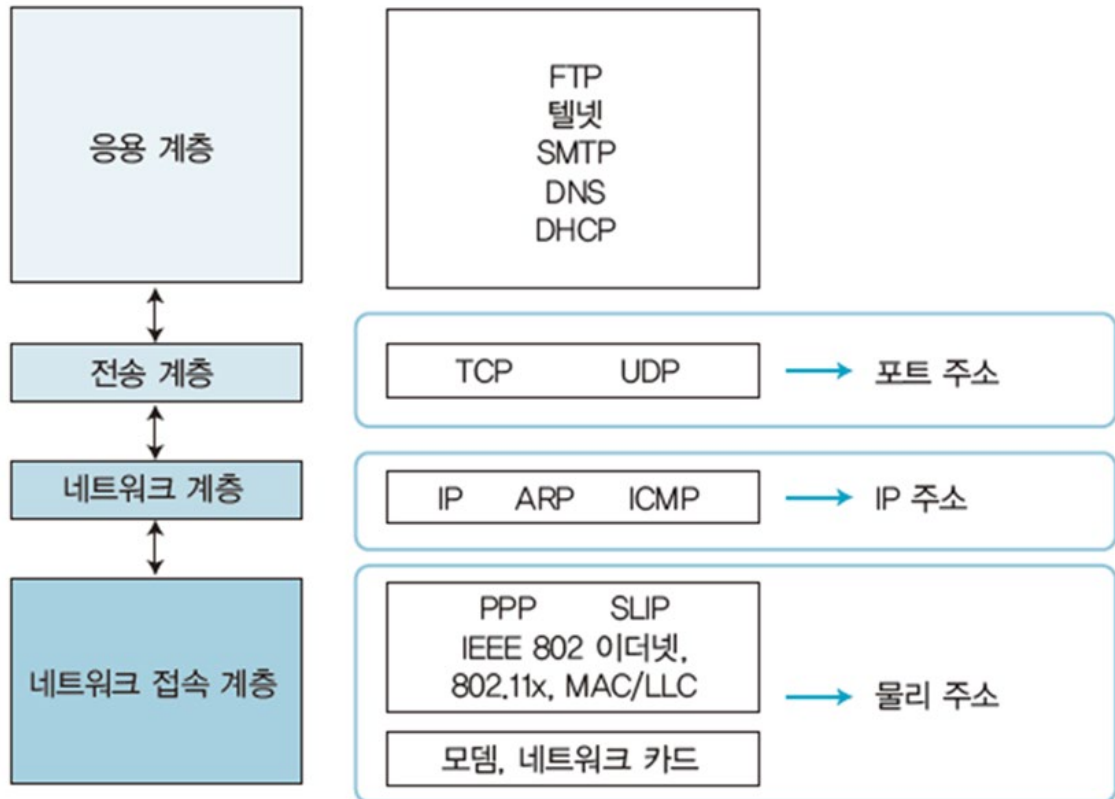


TCP/IP – Network Interface Layer (네트워크 인터페이스 계층)

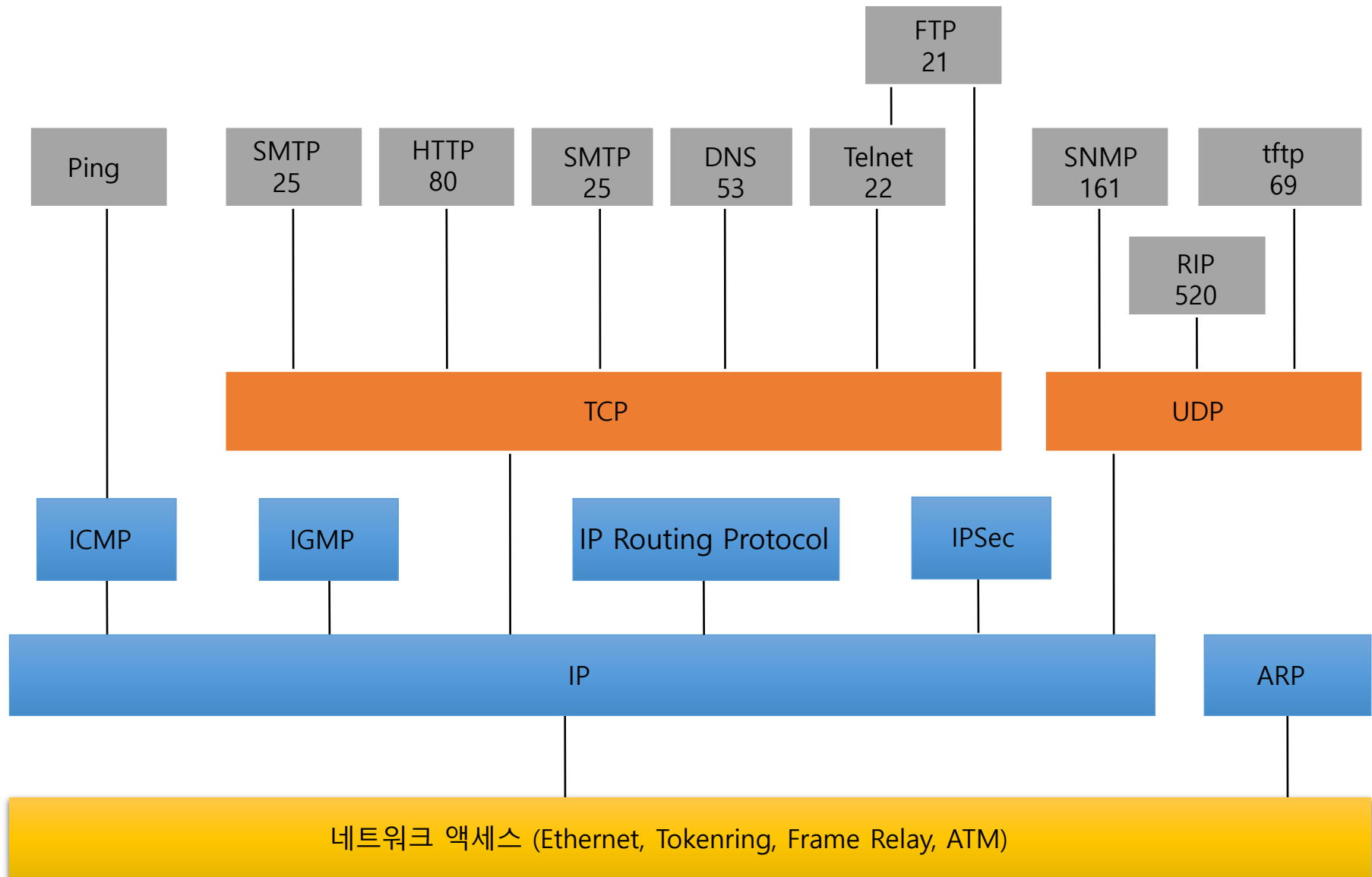
- ❑ TCP/IP에서는 하위 계층인 물리 계층과 데이터 링크 계층을 특별히 정의하지 않았으며, 단지 모든 표준 및 임의의 네트워크를 지원할 수 있도록 하고 있다.
- ❑ 데이터 링크 계층의 역할을 하는 TCP/IP 프로토콜에는 ethernet, 802.11x, MAC/LLC, SLIP, PPP 등이 있다.
- ❑ 송신 측 컴퓨터에서는 상위 계층에서 전달받은 패킷에 물리적 주소인 MAC 주소 정보가 있는 헤더를 추가하여 프레임을 만든 후 그 프레임을 물리 계층에 전달
- ❑ 수신 측 컴퓨터에서는 데이터 링크 계층에서 추가한 헤더를 제거하여 상위 계층인 네트워크 계층으로 전달
- ❑ Network Access Layer (네트워크 접속 계층)이라고도 한다.



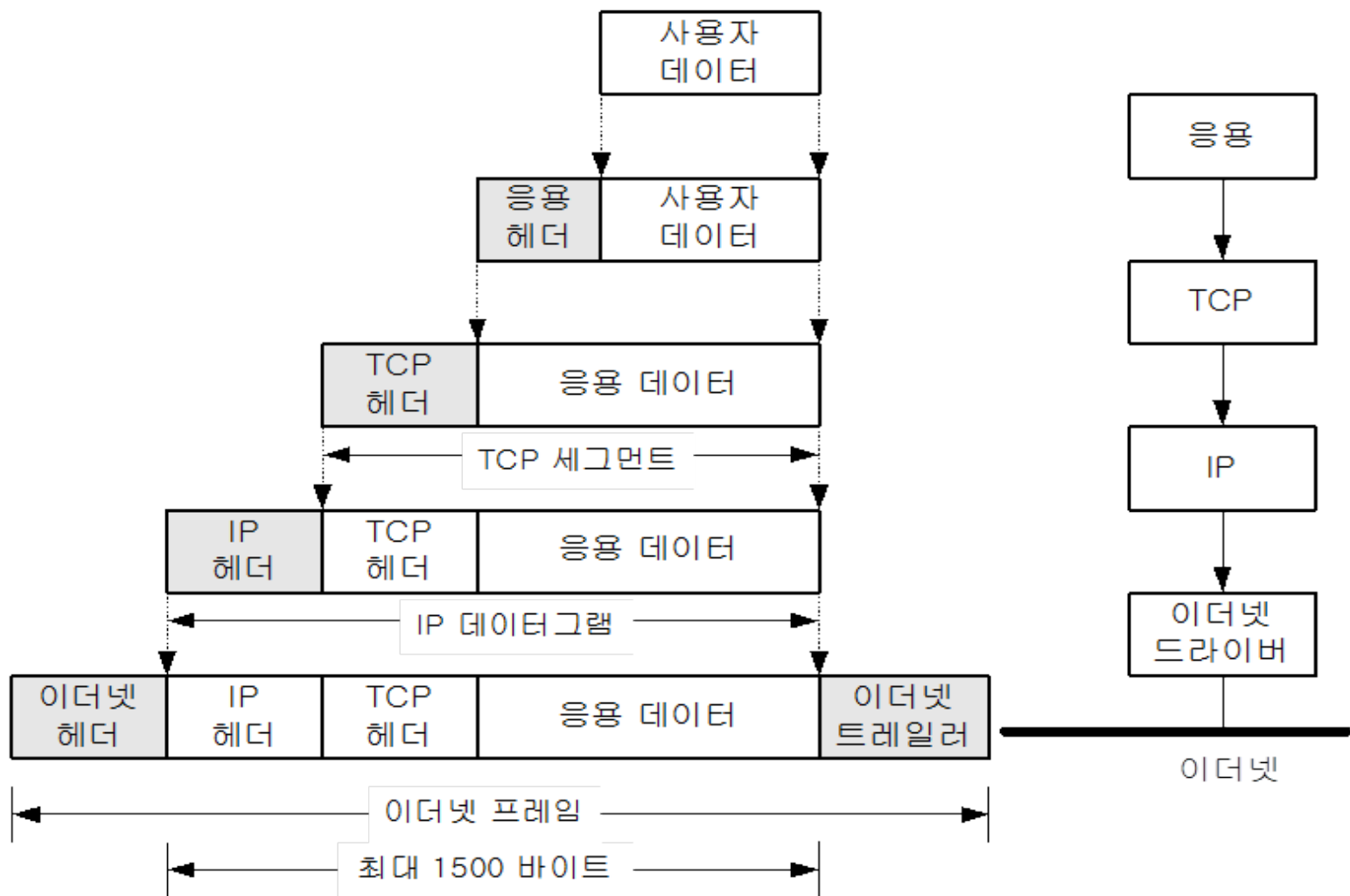
- 물리 주소(MAC 주소)
 - 링크 주소 또는 통신망에서 정의된 노드의 주소
 - 이더넷 네트워크인터페이스 카드(NIC) 6바이트(48비트) 주소 등
 - 물리주소 (Physical Address)
- 인터넷 주소
 - 기존 물리 주소와는 별도로 각 호스트를 식별할 수 있는 유일한 주소
 - 논리주소 (Logical Address)
- 포트 주소
 - 수신지 컴퓨터의 응용계층과 통신하기 위해 필요한 주소



TCP/IP Protocol Suite



TCP/IP Frame 구성 흐름도

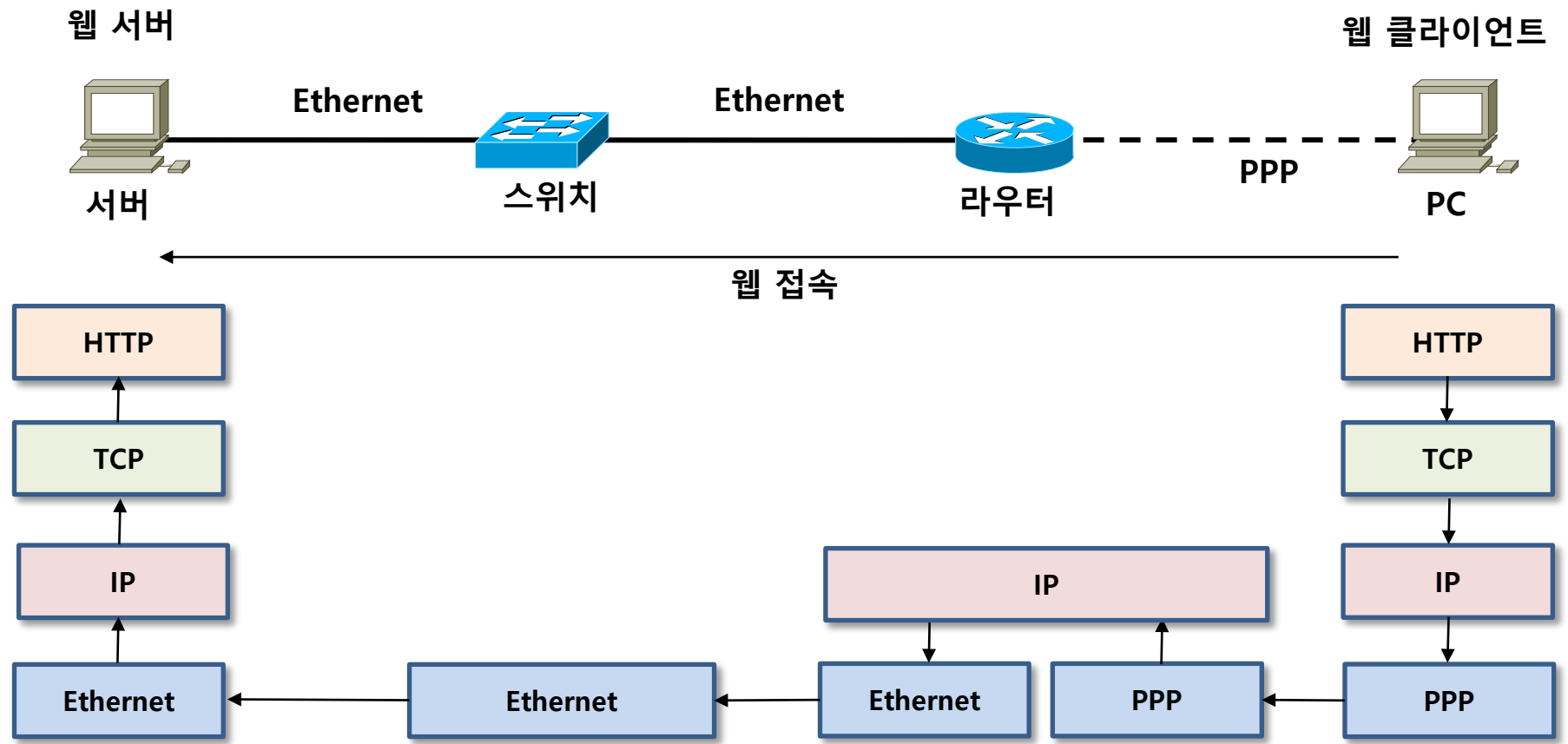


MTU

(Maximum Transfer Unit)

윈도우에서 MTU 확인 : netsh interface ipv4 show interfaces

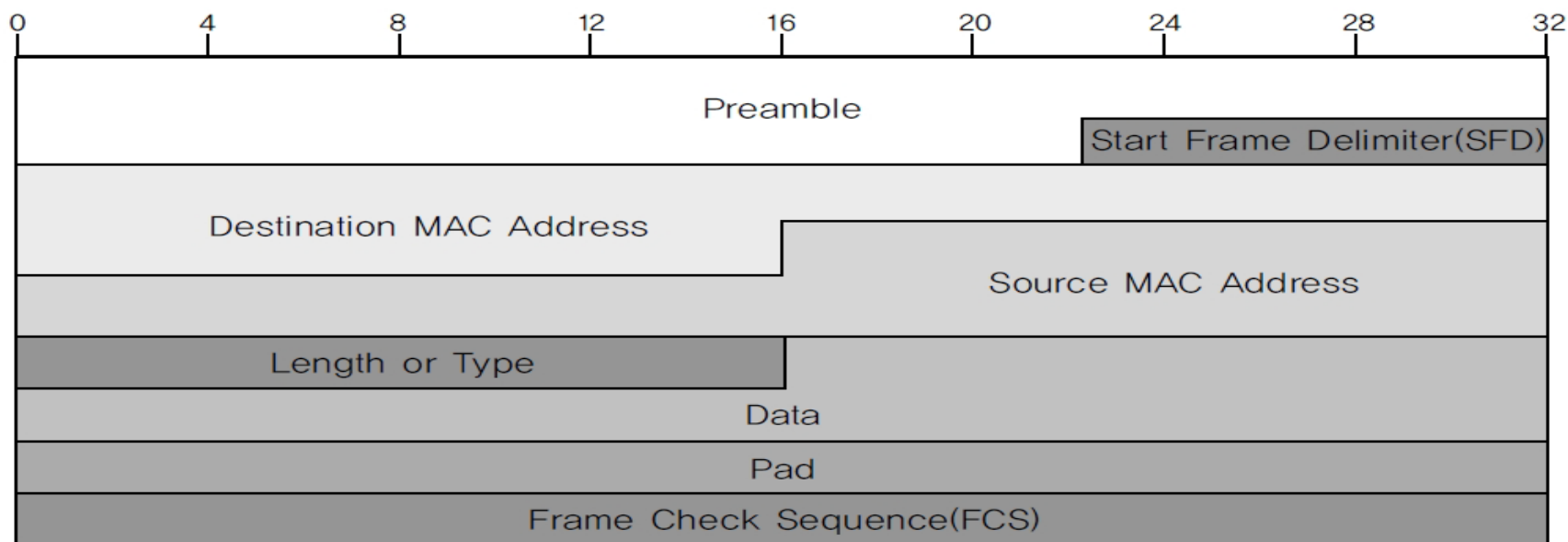
TCP/IP 장치들의 프로토콜 흐름도



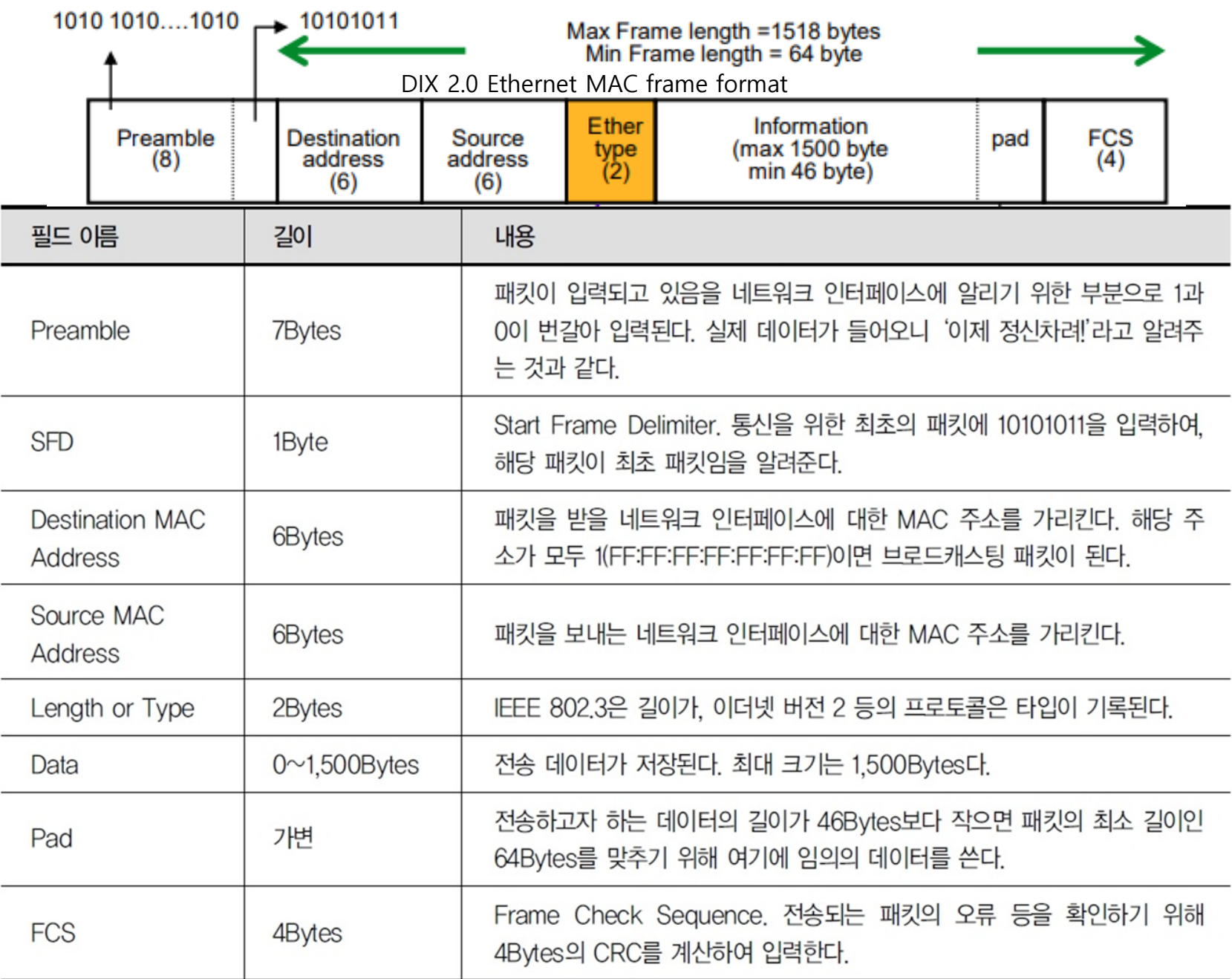
- ❑ TCP/IP에서는 네트워크 인터페이스 계층인 물리 계층과 데이터 링크 계층을 특별히 정의하지 않았으며 현재 우리가 가장 많이 사용하는 것이 Ethernet Protocol임
- ❑ 하드웨어에 대한 주소인 MAC(Media Access Control) 주소를 기반으로 하드웨어 간 통신을 위한 프로토콜
- ❑ 주요기능
 - ❑ 정보전달 : 인접 노드간 데이터 전송
 - ❑ 회선제어 : 신호간 충돌이 발생하지 않도록 제어 (ENQ/ACK기법, 폴링기법)
 - ❑ 흐름제어 : 송신자와 수신자간의 속도차 보상 (Stop and Wait, Sliding Window)
 - ❑ 오류제어 : 물리 전송 특성상 발생하는 오류와 잡음에 대한 보정 (FEC, BEC, ARQ)
 - ❑ 주소지정 : 송신자와 수신자의 물리주소 삽입 (MAC Address)
 - ❑ 접근제어 : 여러 시스템 연결 시, 링크 점유 시 사용 (CSMA/CD, CSMA/CA)

□ Ethernet Protocol

- 흔히 랜이라고 부르는 네트워크 구간 또는 네트워크 하드웨어 사이에서 MAC 주소를 기반으로 통신을 위한 프로토콜
- 이더넷 패킷의 최소 길이는 64KBytes, 최대 길이는 1,518KBytes



Ethernet Protocol



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 가리킨다. 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, 이더넷 버전 2 등의 프로토콜은 타입이 기록된다.
Data	0~1,500Bytes	전송 데이터가 저장된다. 최대 크기는 1,500Bytes다.
Pad	가변	전송하고자 하는 데이터의 길이가 46Bytes보다 작으면 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.

IP (Internet Protocol)

- ❑ 인터넷 프로토콜(IP, Internet Protocol)은 송신 호스트와 수신 호스트가 패킷 교환 네트워크(패킷 스위칭 네트워크, Packet Switching Network)에서 정보를 주고받는 데 사용하는 정보 위주의 규약(프로토콜, Protocol)
- ❑ TCP/IP 기반의 인터넷 망을 통하여 데이터그램의 전달을 담당하는 프로토콜
- ❑ IP의 정보는 패킷 혹은 데이터그램이라고 하는 덩어리로 나뉘어 전송
- ❑ IP 네트워크란 IP 기반으로 구축된 네트워크를 말하며, 주로 현재의 인터넷을 지칭
- ❑ OSI 네트워크 계층(TCP/IP 인터넷 계층)에서 호스트의 주소지정과 패킷 분할 및 조립 기능을 담당
- ❑ IPv4 IEN54 : <http://www.rfc-editor.org/ien/ien54.pdf>
 - ❑ IEN(Internet Experiment Note)
- ❑ IPv4 : RFC 791
- ❑ IPv6 : RFC 2640으로부터 시작하는 여러 규격들이 있음

□ IP 주요기능

- IP 계층에서 IP 패킷의 라우팅 대상이 됨 (Routing)
- IP 주소 지정 (Addressing)
- Fragmentation (단편화) Defragmentation(재결합)
- Capsulation (캡슐화)

□ IP 특징

- 신뢰성(에러제어)및 흐름제어 기능이 전혀 없음 (Best-Effort Service)
- 신뢰성을 확보하려면 IP 계층 위의 TCP와 같은 상위 전송 계층에 의존
- 비연결성 데이터그램 방식으로 전달되는 프로토콜 (Connectionless)
- 패킷의 완전한 전달(소실,중복,지연,순서바뀜 등이 없게함)을 보장 않음 (Unreliable)
- IP 헤더 내 수신 및 발신 주소를 포함 : IPv4 헤더, IPv6 헤더, IP 주소
- IP 헤더 내 바이트 전달 순서 : 최상위 바이트(MSB)를 먼저 보냄 (Big-endian)
- 경우에 따라 단편화가 필요함 (MTU 사이즈보다 클 경우)
- TCP, UDP, ICMP, IGMP 등이 IP 데이터 그램에 실려서 전송
- 현재 사용 IP는 IPv4와 IPv6

IP (Internet Protocol)

□ IPv4 Header와 IPv6 Header

IPv4 Header

Version	IHL	Type of Service	Total Length	
Identification			Flags	Fragment Offset
Time to Live	Protocol		Header Checksum	
Source Address				
Destination Address				
Options				Padding

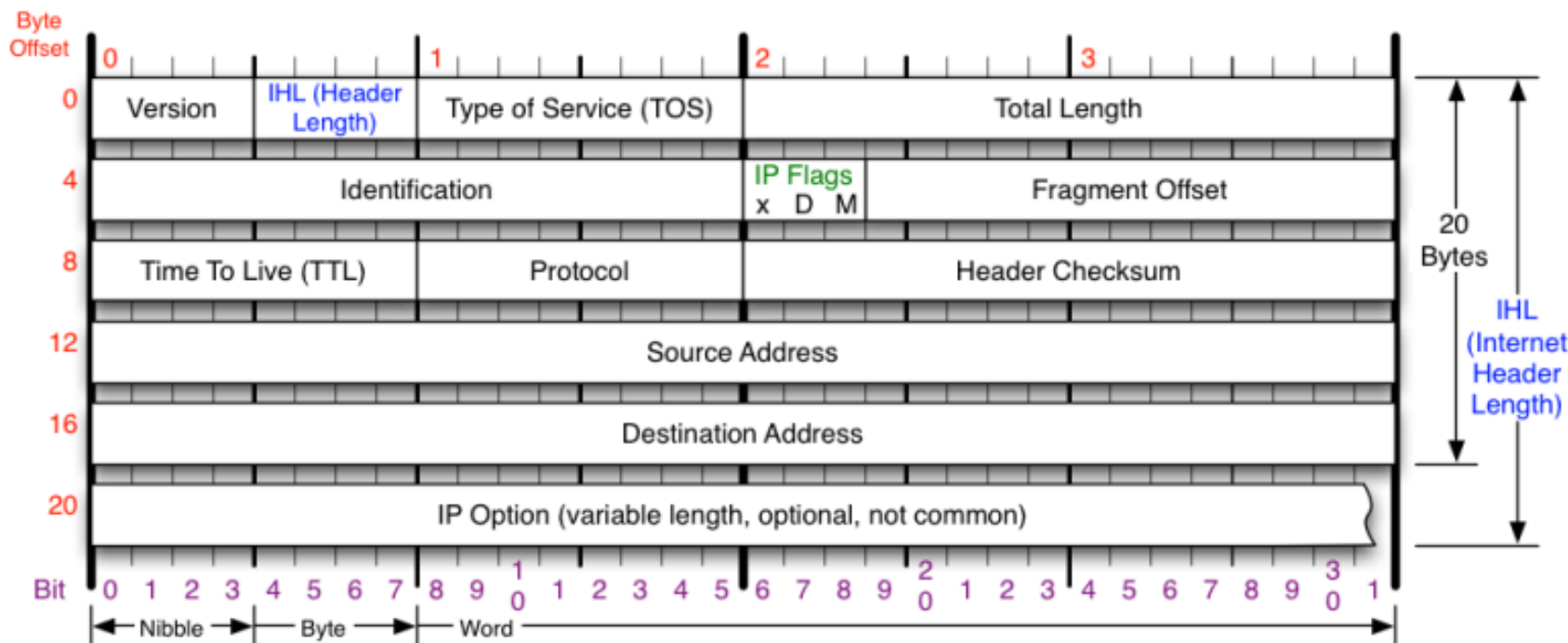
IPv6 Header

Version	Traffic Class	Flow Label		
Payload Length			Next Header	Hop Limit
Source Address				
Destination Address				

Legend

- Field's name kept from IPv4 to IPv6
- Field not kept in IPv6
- Name and position changed in IPv6
- New field in IPv6

IPv4 헤더 구조



Version

Version of IP Protocol. 4 and 6 are valid. This diagram represents version 4 structure only.

Header Length

Number of 32-bit words in TCP header, minimum value of 5. Multiply by 4 to get byte count.

Protocol

IP Protocol ID. Including (but not limited to):

1 ICMP	17 UDP	57 SKIP
2 IGMP	47 GRE	88 EIGRP
6 TCP	50 ESP	89 OSPF
9 IGRP	51 AH	115 L2TP

Total Length

Total length of IP datagram, or IP fragment if fragmented. Measured in Bytes.

Fragment Offset

Fragment offset from start of IP datagram. Measured in 8 byte (2 words, 64 bits) increments. If IP datagram is fragmented, fragment size (Total Length) must be a multiple of 8 bytes.

Header Checksum

Checksum of entire IP header

IP Flags

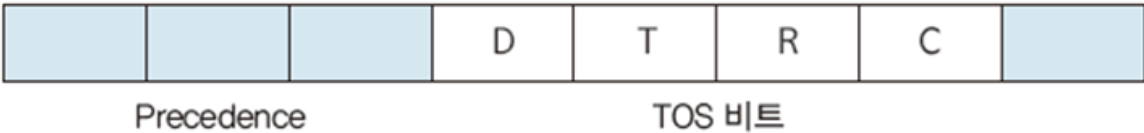
x D M

x 0x80 reserved (evil bit)
D 0x40 Do Not Fragment
M 0x20 More Fragments follow

RFC 791

Please refer to RFC 791 for the complete Internet Protocol (IP) Specification.

- Type-of-Service Flags : 서비스의 우선 순위를 제공
 - 인터넷에서 서비스의 품질(QoS: Quality of Service)을 보장하려는 방법 중의 하나
- 과거 (ToS)
- 현재 (Diffserv 차등서비스 : DSCP 값을 사용)

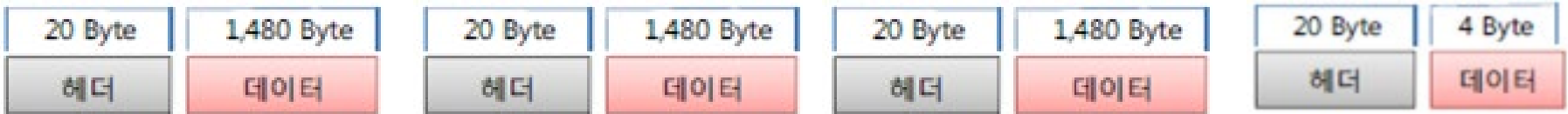
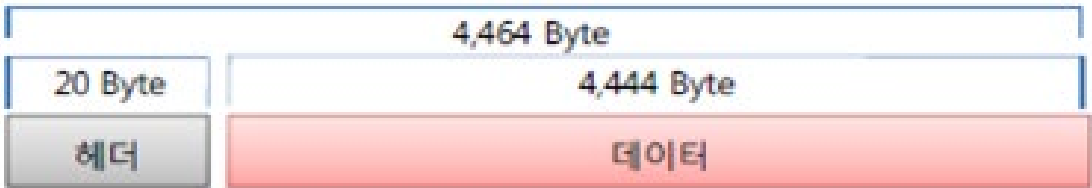


D : 지연 비트(Delay bit) – 1로 설정되면 최소한의 지연으로 데이터 전송을 요청
T : 처리량 비트(Throughput bit) – 1로 설정되면 IP 라우터는 가장 처리량이 큰 경로를 따라 데이터그램을 전송
R : 신뢰성 비트(Reliability bit) – 1로 설정되면 데이터그램 손실 없이 전송
C : 비용 비트(Cost bit) – 1로 설정되면 데이터가 최소 비용으로 수신지에 전송

Delay	Throughput	Reliability	Cost
1	0	0	0
0	1	0	0
0	0	1	0
0	0	0	1
0	0	0	0

IPv4 헤더 구조

- ❑ Total Packet Length 필드 (16bit): 전체 IP 패킷의 길이를 바이트 단위로 나타냄
- ❑ Fragment identifier 필드 (16bit): Fragmentation 이 발생한 경우, 조각을 다시 결합하기 원래의 데이터를 식별하기 위해서 사용
- ❑ Fragmentation Flags 필드 (3bit): 처음 1bit는 항상 0으로 설정, 나머지 2bit
 - ❑ May Fragment : IP 라우터에 의해 fragmentation되는 여부를 나타낸다.
플래그 0 - fragmentation 가능 1 - fragmentation 방지
 - ❑ More Fragments : 원래 데이터의 fragmentation된 조각이 더 있는지 여부 판단.
 - ❑ 플래그 0 - 마지막 조각 기본값 1- 조각이 더 있음
- ❑ Fragmentation Offset 필드 (13bit): 8바이트 오프셋으로 조각에 저장된 원래 데이터의 바이트 범위



IPv4 헤더 구조

- ❑ Protocol Identifier 필드(8bit): 상위계층 프로토콜의 번호
 - ❑ 1 - ICMP, 2 - IGMP, 6 - TCP, 17 - UDP
- ❑ Header Checksum 필드(16bit): IP 헤더의 체크섬을 저장, 라우터를 지나갈때 마다 재계산을 하기 때문에 속도가 떨어진다.
- ❑ Source IP Address 필드(32bit): 출발지 IP 주소
- ❑ Destination IP Address 필드(32bit): 목적지 IP 주소
- ❑ Options(선택적) 필드(가변적): Type-of-Service 플래그 처럼 특별한 처리 옵션을 추가로 정의 할 수 있다.

IP(인터넷 프로토콜) 주소

- ❑ IP 주소 : 공인으로 되어있는 인터넷에 연결된 모든 컴퓨터에 부여된 고유의 주소
 - ❑ 현재 사용하는 IP 주소 체계는 IP Ver. 4
 - ❑ 8비트 크기의 필드 네 개를 모아서 구성한 32비트(4바이트) 논리 주소
 - ❑ xxx.xxx.xxx.xxx, 즉 163.152.19.114처럼 .(점)으로 구분한 10진수 형태 네 개로 구성
 - ❑ 한 바이트가 가질 수 있는 10진수는 0~255이므로, IP 주소의 값은 0.0.0.0에서 255.255.255.255

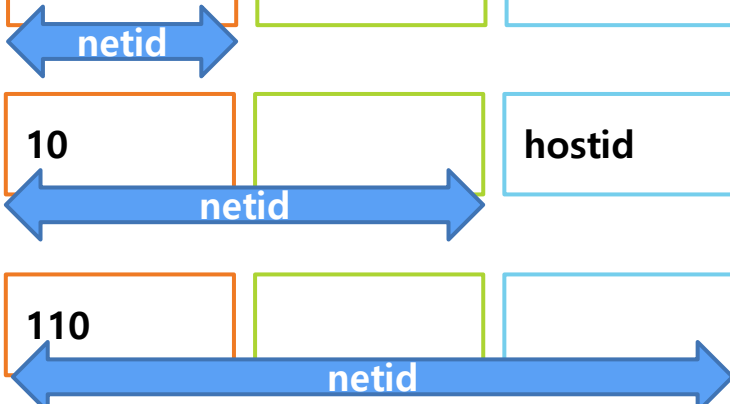
- ❑ IP 주소의 구성
 - ❑ 일반 우편 주소를 시, 동, 번지 등으로 구분하는 것처럼 IP 주소도 네트워크 주소(Net ID)와 호스트 주소(Host ID)로 구분
 - ❑ 네트워크 주소 : 전체 네트워크를 좀 더 작은 네트워크로 분할하여 각 호스트가 속한 네트워크를 대표
 - ❑ 호스트 주소 : 네트워크 주소로 표현하는 네트워크 내부에서 각 호스트의 주소를 표현하는 역할을 하며, 전체 32비트에서 네트워크 주소를 제외한 나머지에 해당

□ IPv4 주소 체계

- IP 주소를 효율적으로 배정하기 위해 클래스라는 개념 도입(A, B, C, D, E 다섯 종류)
- A 클래스 : IP 주소의 맨 처음 바이트의 시작 1비트가 0으로 시작
- B 클래스 : 시작 2비트가 10으로 시작
- C 클래스 : 시작 3비트가 110으로 시작
- D 클래스 : 시작 4비트가 1110으로 시작, IP 멀티 캐스팅용으로 사용
- E 클래스 : 시작 4비트가 1111로 시작, 자원 확보를 위해 예비용으로 분류

IPv4 주소 체계

Class	첫번째 Byte	두번째 Byte	세번째 Byte	네번째 Byte	
A Class	0	hostid	hostid	hostid	0.0.0.0 ~ 127.255.255.255
B Class	10		hostid	hosid	128.0.0.0 ~ 191.255.255.255
C Class	110			hostid	192.0.0.0 ~ 223..255.255.255
D Class	1110				224.0.0.0 ~ 239.255.255.255
E Class	1111				240.0.0.0 ~ 255.255.255.255



TCP (Transport Control Protocol)

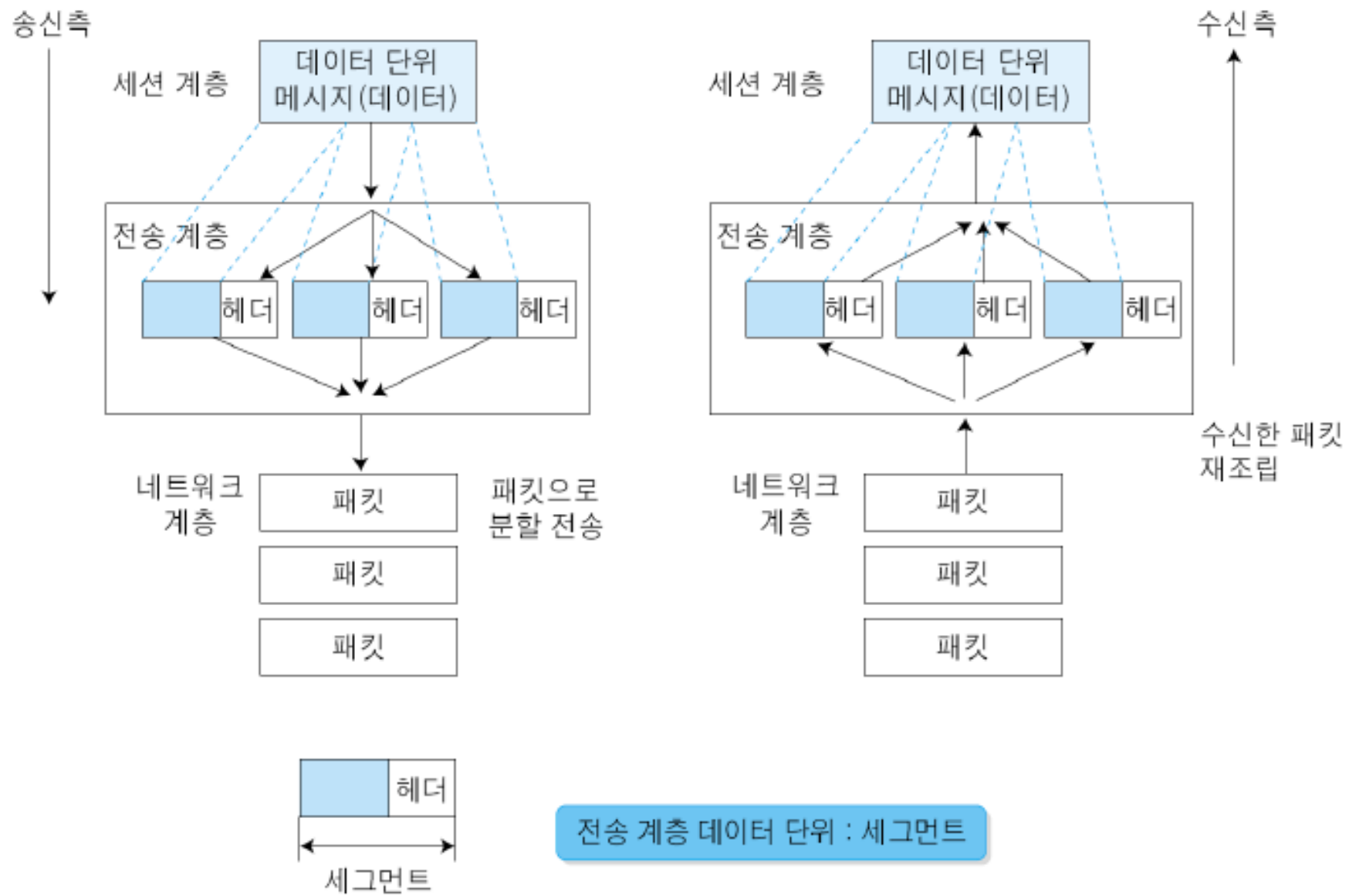
□ TCP (전송 제어 프로토콜)

- 송신 측 TCP 포트에서 수신 측 TCP 포트로 바이트의 스트림을 전송하는 연결형 데이터 전달 서비스 제공
- 연결 지향형 프로토콜
 - 송신 측 컴퓨터와 수신 측 컴퓨터가 데이터를 전송하기 전에 먼저 데이터를 송수신할 수 있는 연결 통로를 만들고 데이터를 전송하는 프로토콜

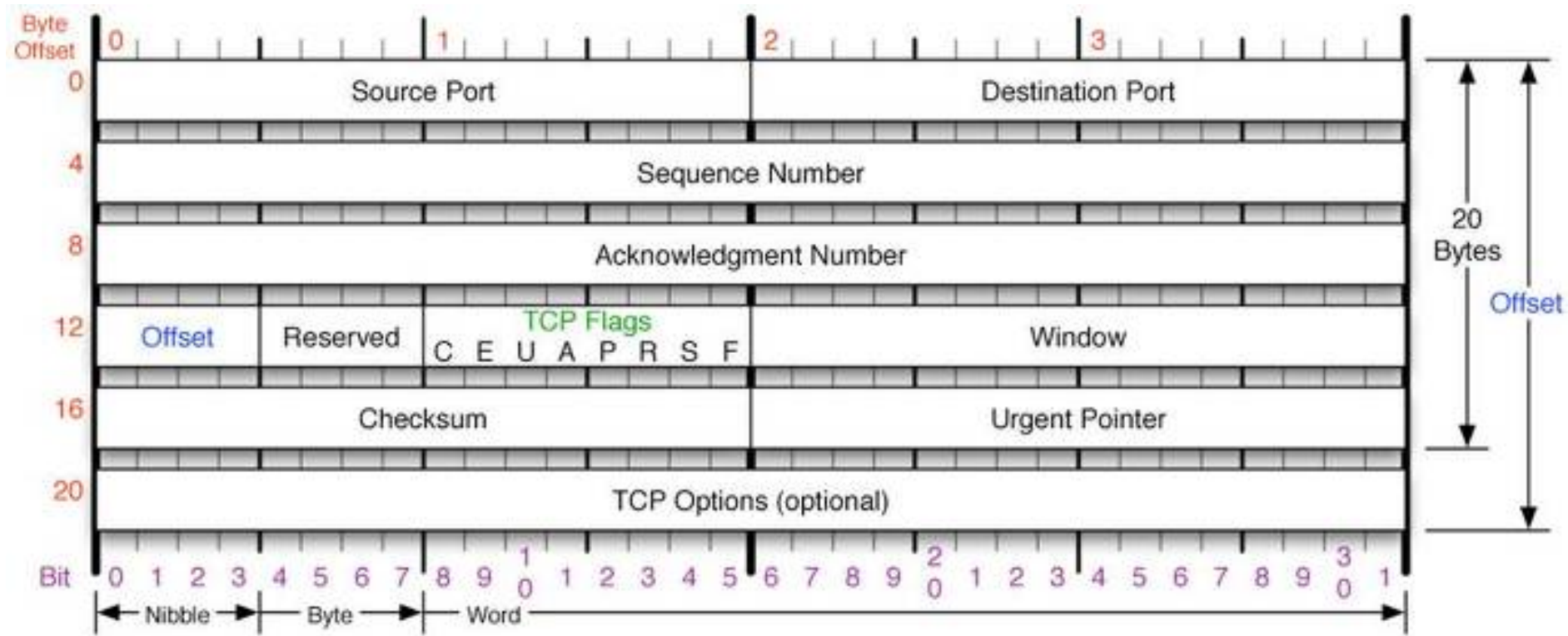
□ TCP 주요기능

- 서비스 지점 주소 지정
 - 전송층 헤더는 서비스 지점 주소(포트번호)를 포함
- 분할 및 재조립
 - 송신 시 세그먼트 단위로 나누고 목적지에서는 세그먼트를 재조립하여 메시지 형성
- 연결제어
 - 비연결지향: 각 세그먼트를 독립된 패킷으로 나누어 전송 (UDP)
 - 연결지향: 패킷을 전달하기 전 먼저 목적지 시스템의 전송층과 연결 설정(TCP)
- 흐름제어
 - 단일 링크가 아닌 종단간 흐름제어
- 오류제어
 - 종단간 오류제어, 재전송을 통한 오류 정정

TCP (Transport Control Protocol)



TCP 헤더 구조



- Port 주소 : 16bit 주소로 되어 있으며 0 ~ 65,535의 주소를 가질 수 있음
 - Well-known ports(0~1,023): IANA에 의해 지정되고 제어된다.
 - Registered port(1,024~49,151): IANA에 의해 지정되거나 제어되지 않는다. 하지만, 중복을 피하기 위해 IANA에 등록 될 수는 있다.
 - Dynamic Ports(49,152~65,535): IANA에 의해 제어되거나 등록되지 않는다.

TCP 헤더 구조

❑ Source Port address 필드(16bit)

데이터를 생성한 애플리케이션에서 사용하는 포트번호를 나타낸다.

❑ Destination Port address 필드(16bit)

목적지 애플리케이션이 수행하는 프로세스가 사용하는 포트 번호

❑ Sequence number 필드(32bit)

- ❑ 전송되는 데이터의 가상 회선을 통해 전송되는 데이터의 모든 바이트에는 고유한 일련 번호가 부여된다.
- ❑ 네트워크가 불안하여 패킷을 분실, 지연 등으로 세그먼트가 순서가 어긋나게 도착 할 수 있기 때문에 sequence number를 이용하여 데이터를 올바른 순서로 재배열할 수 있다.

❑ Acknowledgement number 필드(32bit)

- ❑ 다음 세그먼트를 수신할 준비가 되었다는 사실을 알린다.
- ❑ 성공적으로 수신한 마지막 바이트의 순서 번호 + 1

❑ Header Length 필드 (4bit)

- ❑ 헤더의 길이를 32비트 단위로 나타낸다. 최소 필드 값은 5 ($5 * 32 = 160\text{bit}$ or 20Byte)
- ❑ 최대 값 15 ($15 * 32 = 480\text{bit}$ or 60byte)

❑ Reserved 필드(6bit): 차후의 사용을 위해서 예약된 6 비트 필드이다.

TCP 헤더 구조

- ❑ CWR : Congestion Window Reduced – 혼잡 윈도우 크기 감소
- ❑ ECN : Explicit Congestion Notification – 혼잡을 알림
- ❑ Control Flags (6bit)
 - ❑ 6개의 서로 다른 제어 비트 또는 플래그를 나타내고 TCP Flags 8bit 중 처음 C,E를 제외
 - ❑ 동시에 여러 개의 비트가 1로 설정될 수 있다.
 - ❑ SYN(Synchronization) - S : 연결요청 플래그
 - ❑ TCP에서 세션을 성립할 때 가장먼저 보내는 패킷, 시퀀스 번호를 임의적으로 설정하여 세션을 연결하는 데에 사용되며 초기에 시퀀스 번호를 보내게 된다.
 - ❑ ACK(Acknowledgement) - ACK : 응답
 - ❑ 상대방으로부터 패킷을 받았다는 걸 알려주는 패킷, 다른 플래그와 같이 출력되는 경우도 있다.
 - ❑ 받는 사람이 보낸 사람 시퀀스 번호에 TCP 계층에서 길이 또는 데이터 양 을 더한 것과 같은 ACK를 보낸다.
 - ❑ RST(Reset) - R : 커넥션 리셋
 - ❑ 재설정을 하는 과정이며 양방향에서 동시에 일어나는 중단 작업이다. 비정상적인 세션 연결 끊기에 해당한다. 이 패킷을 보내는 곳이 현재 접속하고 있는 곳과 즉시 연결을 끊고자 할 때 사용한다.

❑ Control Flags (6bit)

❑ PSH(Push) - P : 밀어 넣기

- ❑ 텔넷 과 같은 상호작용이 중요한 프로토콜의 경우 빠른 응답이 중요한데, 이 때 받은 데이터를 즉시 목적지인 Application 계층으로 전송하도록 하는 Flag이다. 버퍼가 채워지기를 기다리지 않고 데이터를 전달한다.

❑ URG(Urgent) - U : 긴급 데이터

- ❑ 전송하는 데이터 중에서 긴급히 전달해야 할 내용이 있을 경우에 사용한다.

❑ FIN(Finish) - F : 연결 종료 요청

- ❑ 세션 연결을 종료시킬 때 사용되며 더 이상 전송할 데이터가 없음을 나타낸다.

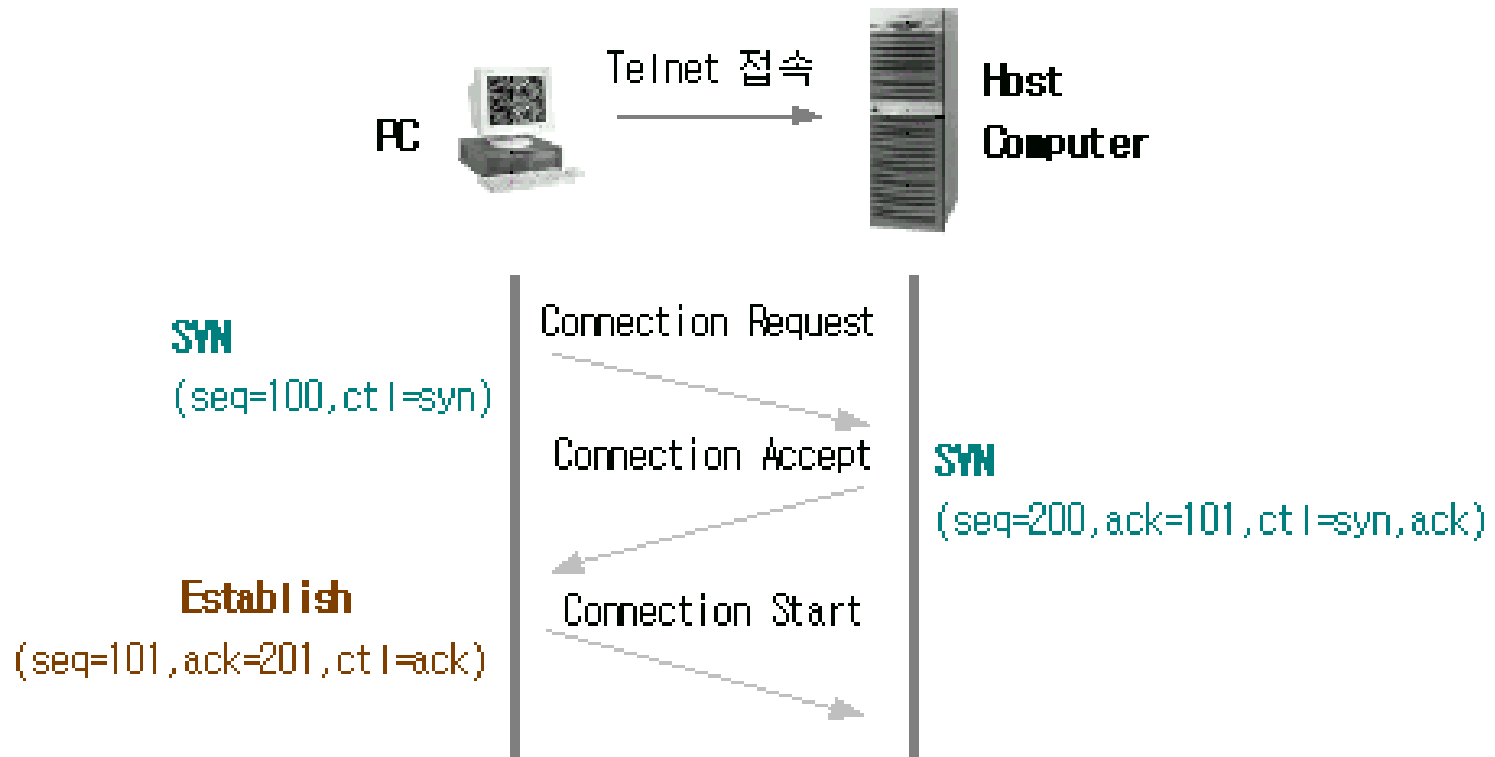
❑ Window size 필드(16bit): 송신 시스템의 가용 수신 버퍼의 크기로 바이트 단위 사용

❑ 최대크기는 $2^{16}\text{Byte} = 65,536\text{Byte} = 64\text{KB}$

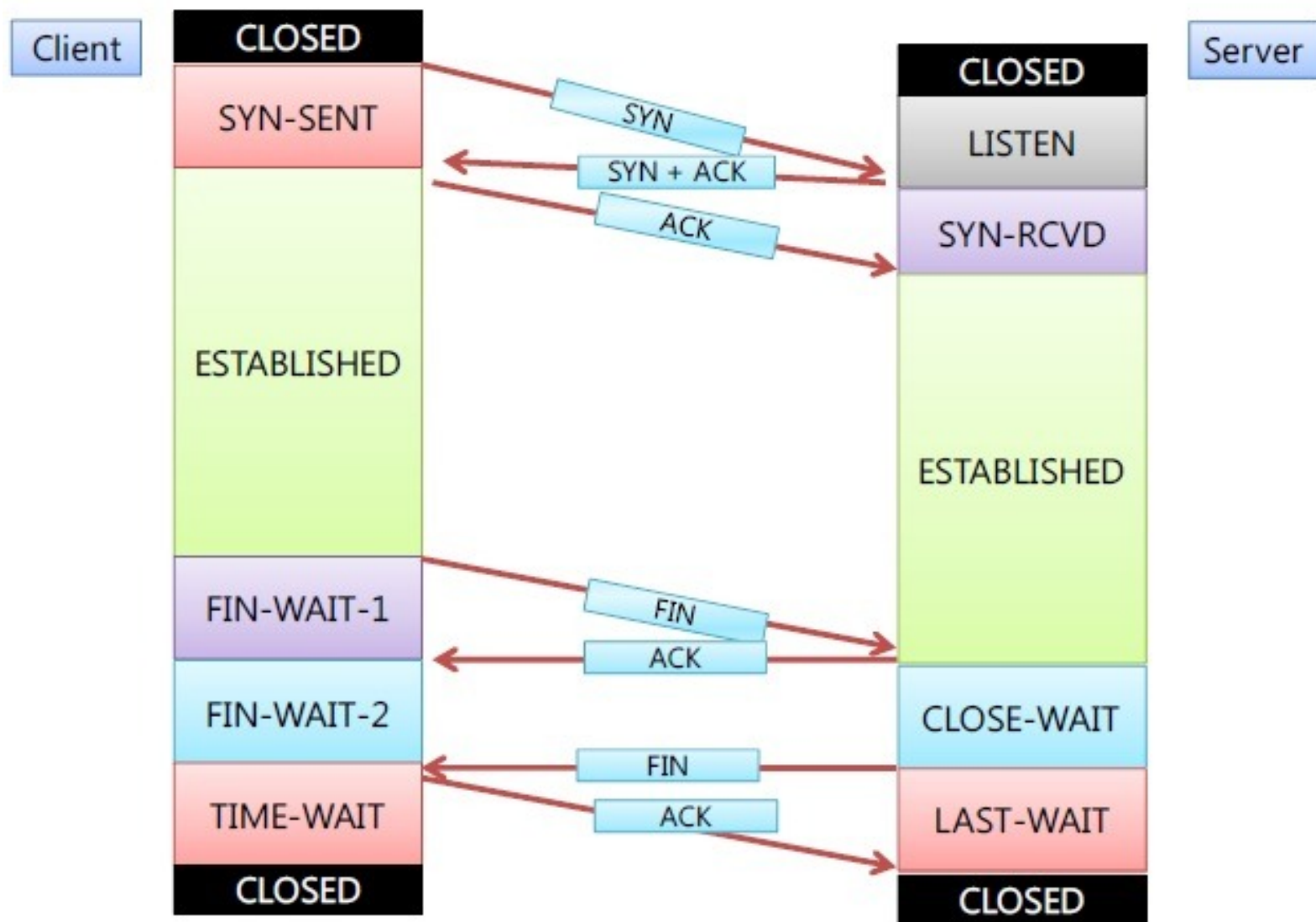
❑ Checksum 필드(16bit): TCP 세그먼트의 내용이 유효한지 검증하고 손상 여부를 검사

□ 3-Way Hand Shaking

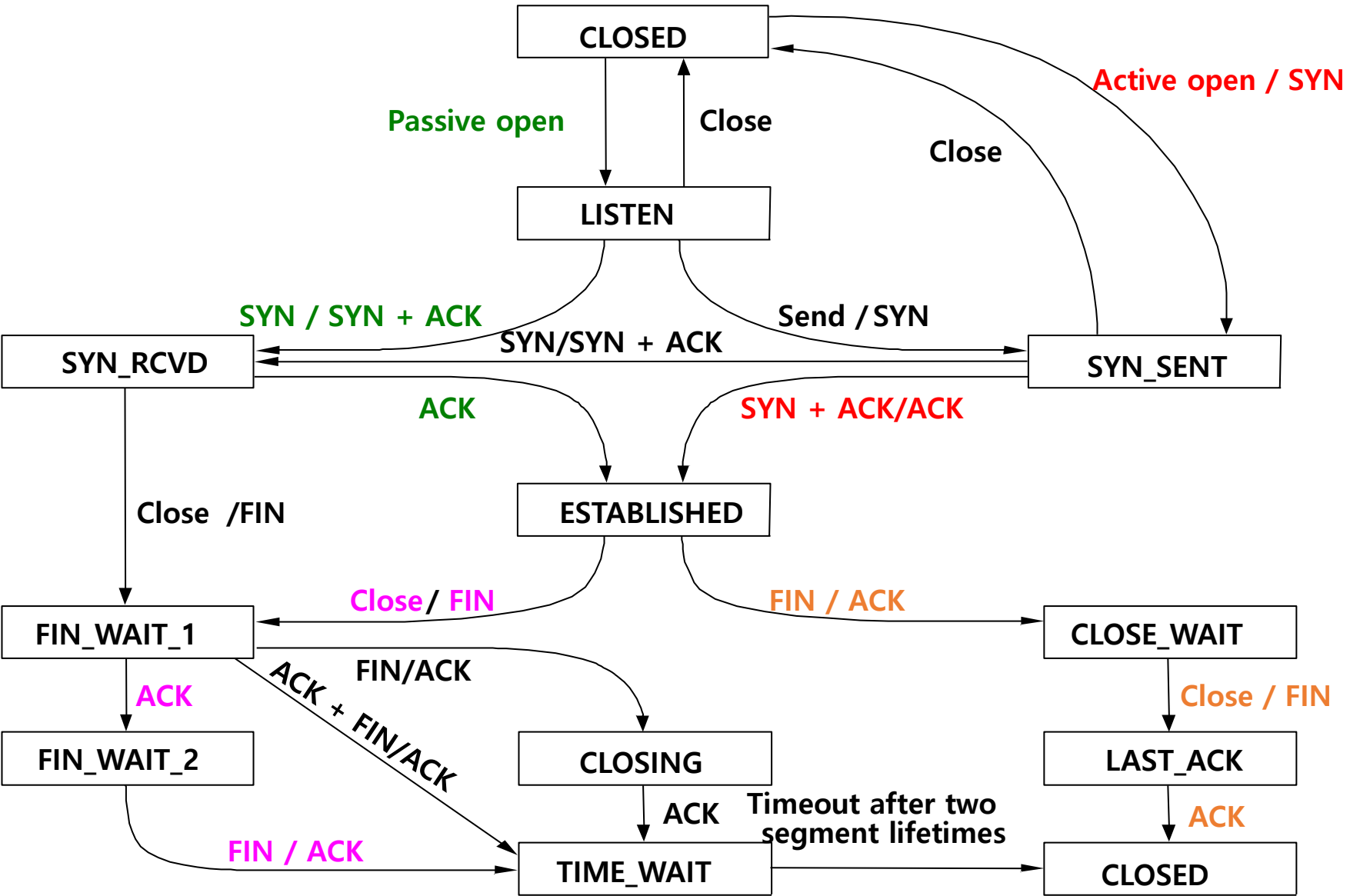
- 포트 번호만 사용하여 응용 프로그램을 식별하는 UDP와는 달리 TCP는 연결을 사용하여 응용 프로그램을 식별한다.
- 연결 설정 (3-Way 핸드 셰이킹)
- 연결 해제 (4-Way 핸드 셰이킹)



TCP 통신 구조



TCP 상태 전이도



□ 흐름제어 (Flow Control)

- 송신측이 수신측의 처리속도 보다 더 빨리 데이터를 보내지 못하도록 제어해 주는 것
- 수신측에서 송신측 발송 데이터의 양이나 속도를 제한 (송신측을 억제하는 형태)
- 이를위해 수신측에서 데이터 넘침을 송신측에 통보하는 피드백 메커니즘 필요

□ 흐름제어 방식 구분

- 정지 대기 방식 (Stop and Wait)
 - 한번에 1개씩 수신확인하며 프레임을 전송하는 방식
 - 링크상에서 보내고자하는 데이터가 프레임 길이 보다 긴 경우에는 비효율적임
- 전송률 기반 흐름제어 (Rate-based)
 - 데이터 송신률에 대한 임계값 관리에 의한 흐름제어
- 윈도우 기반 흐름제어 (Windows based => Sliding Windows)
 - 여러 개의 프레임을 동시에 보내고자하는 기법
 - 기타 윈도우 방식 : 크레딧(Credit) 윈도우 방식, 페이징(paging) 윈도우 방식

- ❑ 데이터링크(OSI 7 L2 , TCP/IP 1계층)계층에서 흐름제어
 - ❑ 데이터 링크의 송수신 양단 간에 송신율 및 수신율의 균형을 맞춤
- ❑ 네트워크 계층 (OSI 7 L3 , TCP/IP 2계층)에서 흐름제어
 - ❑ 통신망 종류에 따라, 흐름제어 기능 제공을 할 수도 안할 수도 있음
 - ❑ IP계층에서 흐름제어 방식
 - ❑ IP계층에서는 명시적인 흐름제어 기능이 없음
 - ❑ 그 상위계층(즉, 전송계층)에서 흐름제어 기능을 제공함
 - ❑ 다만, IP계층에서는 송수신 버퍼 정도의 기능은 제공하게됨
- ❑ 전송 계층(OSI 7 L4 , TCP/IP 3계층) 에서 흐름제어
 - ❑ 단일 데이터 링크 간이 아닌, 전송계층 종단-대-종단 간에 흐름제어 기능을 수행함
 - ❑ 전송계층 상에서의 흐름제어는 구현이 복잡
 - ❑ 전송지연이 매우 가변적이므로 링크계층처럼 단순한 재전송(시간만료) 메커니즘을 사용하기 어려움

❑ Sliding Window 방식 (연속적 ARQ(Continuous ARQ) = Go Back n ARQ)

- ❑ 흐름제어를 위한 검출 후 재전송 방식(ARQ)의 일종 (혼잡제어도 가능)
- ❑ 일정한 윈도우 크기 이내에서 한번에 여러 패킷을 송신하고,
- ❑ 이들 패킷에 대하여 단지 한 번의 ACK 로써 수신 확인을 하며,
- ❑ 윈도우 크기를 변경시키며 흐름제어(혼잡제어도 가능)를 하는 기법

❑ TCP의 Sliding Windows

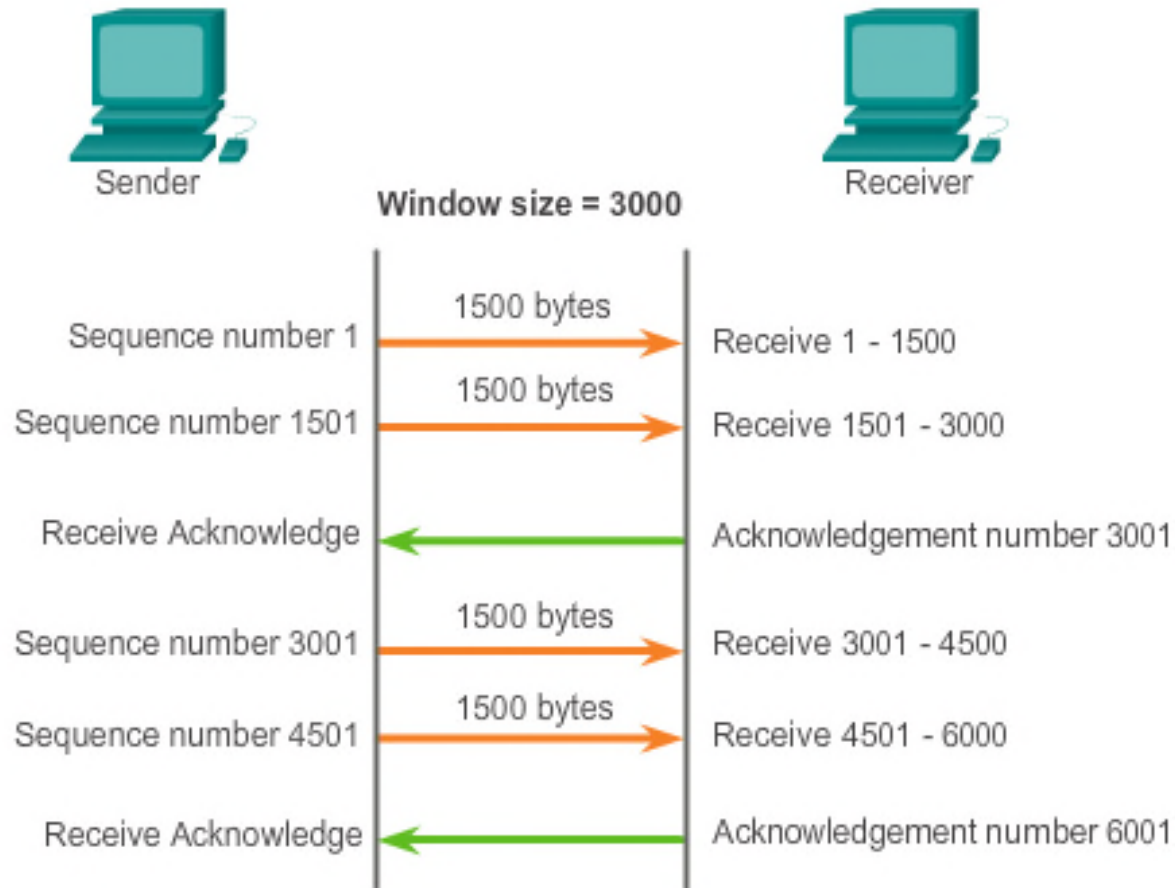
- ❑ TCP 슬라이딩 윈도우 기법은 수신 측에서 설정한 윈도우 크기만큼 송신 측에서 확인 응답 없이 세그먼트를 전송할 수 있게 하여 데이터 흐름을 동적으로 조절하는 제어 기법이다.
- ❑ 이처럼 슬라이딩 윈도우를 통하여 송신 버퍼의 범위는 수신 측의 여유 버퍼 공간을 반영하여 동적으로 바뀜으로써 흐름제어를 수행하게 된다.
- ❑ 슬라이딩 윈도우는 일단 윈도우에 포함되는 모든 패킷을 전송하고, 그 패킷들의 전달이 확인되는대로 이 윈도우를 옆으로 옮김(Slide)으로서 그 다음 패킷들을 전송하는 방식이다.
- ❑ 윈도우의 크기 만큼은 수신 쪽의 확인(응답)을 받지 않고도 보내는 것이 가능하므로 매번 전송한 패킷에 대해 확인을 받아야만 그 다음 패킷을 전송하는 방법(stop-and-wait)를 사용하는 것보다 훨씬 네트워크를 효율적으로 사용할 수 있다.

□ TCP Window Size (윈도우 크기)

- TCP/IP를 사용하는 모든 호스트들은 각각 2개의 window를 가지고 있다. 하나는 보내기 위한 window이며 또 다른 하나는 받기 위한 window이다.
- 호스트들은 실제 데이터를 보내기 전에 먼저 "TCP-3-way handshaking"을 통하여 수신컴퓨터의 receive window size에 자신의 send window size를 맞추게 된다. 즉 상대방이 받을 수 있는 크기에 맞추어 전송을 하겠다는 것이다.
- 즉 TCP 송신 윈도우 크기는 수신 측으로부터 확인응답 없이 전송할 수 있는 데이터의 개수를 의미한다. 윈도우 크기는 전송했으나 아직 확인 응답 받지 못한 데이터와 지연 없이 전송할 수 있는 데이터 크기를 합한 값이 된다.TCP의 Sliding Windows
- TCP 슬라이딩 윈도우 기법은 수신 측에서 설정한 윈도우 크기만큼 송신 측에서 확인 응답 없이 세그먼트를 전송할 수 있게 하여 데이터 흐름을 동적으로 조절하는 제어 기법이다.
- 이처럼 슬라이딩 윈도우를 통하여 송신 버퍼의 범위는 수신 측의 여유 버퍼 공간을 반영하여 동적으로 바뀜으로써 흐름제어를 수행하게 된다.
- 슬라이딩 윈도우는 일단 윈도우에 포함되는 모든 패킷을 전송하고, 그 패킷들의 전달이 확인되는대로 이 윈도우를 옆으로 옮김(Slide)으로서 그 다음 패킷들을 전송하는 방식이다.
- 윈도우의 크기 만큼은 수신 쪽의 확인(응답)을 받지 않고도 보내는 것이 가능하므로 매번 전송한 패킷에 대해 확인을 받아야만 그 다음 패킷을 전송하는 방법(stop-and-wait)를 사용하는 것보다 훨씬 네트워크를 효율적으로 사용할 수 있다.

TCP Windows Size & TCP Congestion

TCP Segment Acknowledgement and Window Size

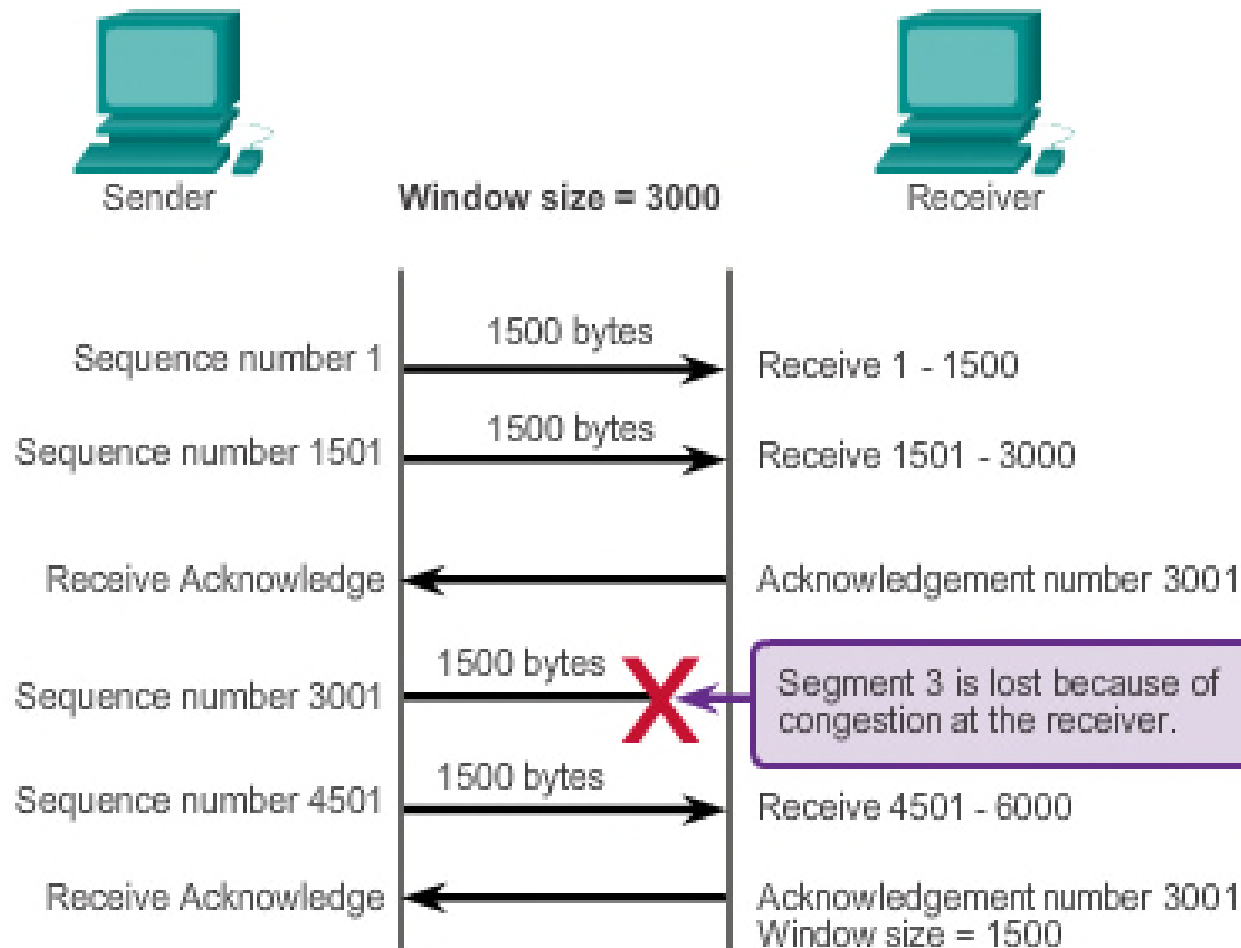


The **window size** determines the number of bytes sent before an acknowledgment is expected.

The **acknowledgement** number is the number of the next expected byte.

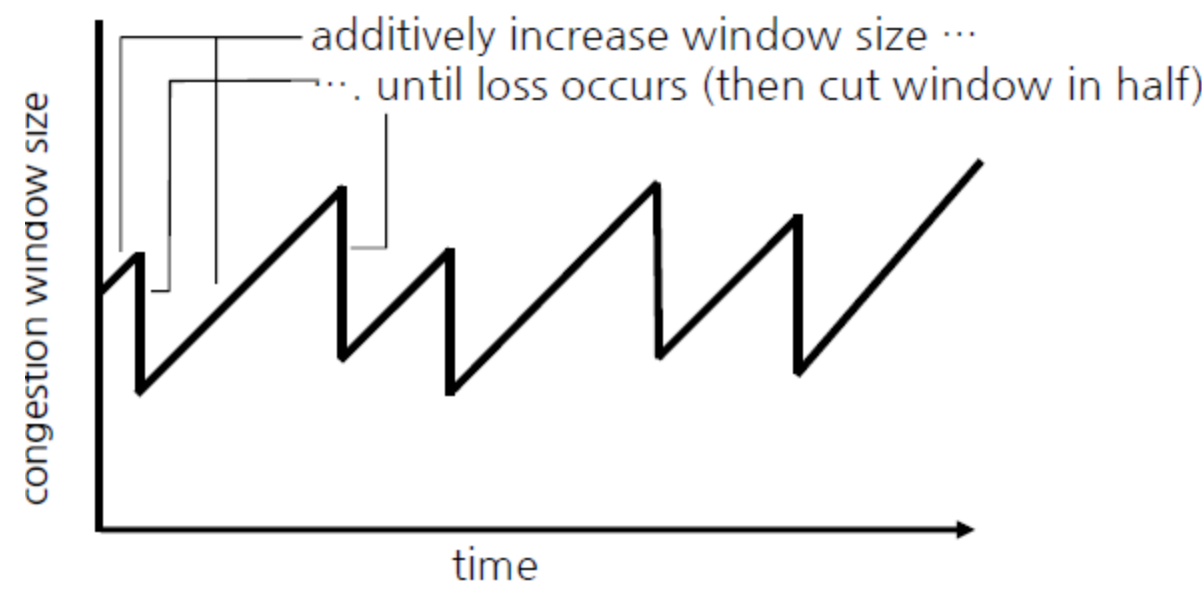
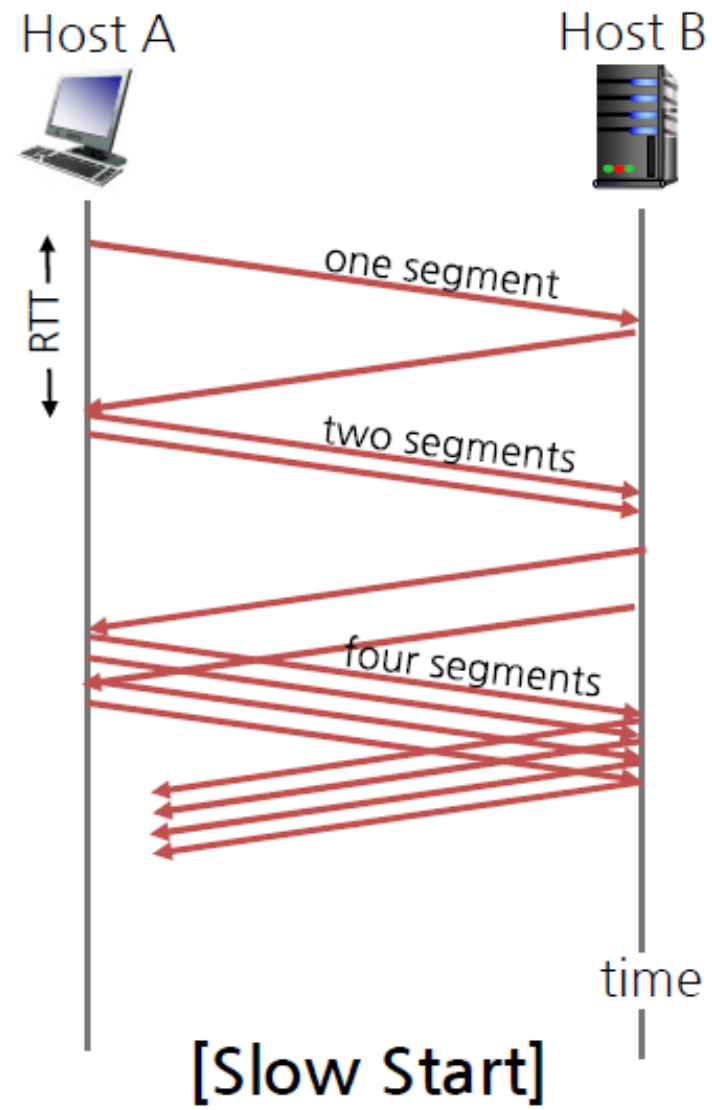
TCP Windows Size & TCP Congestion

TCP Congestion and Flow Control



If segments are lost because of congestion, the Receiver will acknowledge the last received sequential segment and reply with a reduced window size.

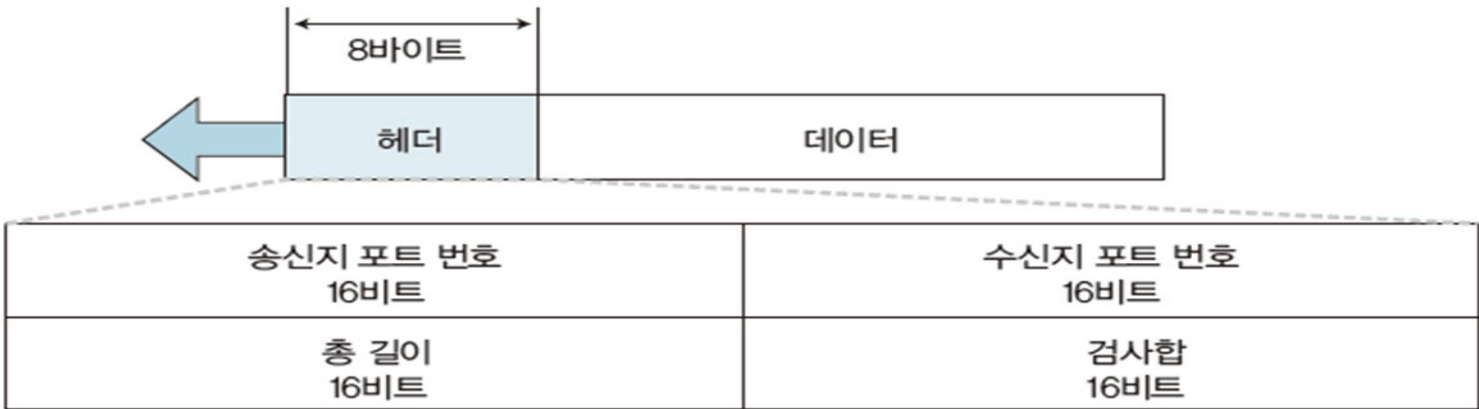
TCP Slow Start & Congestion Flow Control



[Flow Control]

UDP (User Datagram Protocol)

- ❑ UDP (User Datagram Protocol): 사용자 데이터그램 프로토콜
 - ❑ 최선 형 (best-effort) 비연결형 전달 프로토콜
 - ❑ 연결 지향 프로토콜과 달리 패킷이나 흐름 제어, 단편화 및 전송 보장 등의 기능은 제공하지 않는다.
 - ❑ TCP 헤더에 비해 간단하므로 상대적으로 통신 과부하가 적다
 - ❑ UDP 헤더의 크기(8바이트)는 TCP 헤더의 크기(20바이트)보다 작다
 - ❑ UDP를 사용하는 대표적인 응용 계층 프로토콜
 - ❑ DNS(Domain Name System)
 - ❑ DHCP(Dynamic Host Configuration Protocol)
 - ❑ SNMP 등



❑ Transmission Control Protocol (TCP)

- ❑ RFC 793
- ❑ Connection-oriented
- ❑ Reliable delivery
- ❑ Ordered data reconstruction
- ❑ Error control
- ❑ Flow control
- ❑ Stateful protocol
- ❑ Overhead 많이 발생
- ❑ 일반적인 통신에 사용

❑ User Datagram Protocol (UDP)

- ❑ RFC 768
- ❑ Connectionless
- ❑ Unreliable delivery
- ❑ No ordered data reconstruction
- ❑ No error control (Option)
- ❑ No flow control
- ❑ Stateless protocol
- ❑ Overhead 적게 발생
- ❑ Real-time service에 많이 활용

OSI 7 Layer와 TCP/IP 4 Layer 비교표

Layer	OSI 7 Layer	기능	장비	주요소	PDU	TCP/IP Layer
L7	Application	사용자가 네트워크에 접속 가능하게 해주는 계층 사용자인터페이스, 전자우편, 데이터베이스 관리등의 서비스 제공	IDS, IPS (L7 스위치)		DATA	Application
L6	Presentation	운영체제의 한 부분으로 입력 또는 출력되는 데이터를 하나의 표현 형태로 변환 필요한 번역을 수행하여 두 장치가 일관되게 전송데이터를 서로 이해할 수 있도록 함 제어코드나 문자 및 그래픽등의 확장자를 생각하면 쉬움				
L5	Session	통신 세션을 구성하는 계층으로 포트(port)연결이라고 할 수 있음 통신 장치간의 상호작용을 설정하고 유지하며 동기화 함 사용자 간의 포트 연결(세션)이 유효한지 확인하고 설정함				
L4	Transport	전체 메시지를 발신지:목적지(종단:종단)간 제어와 에러를 관리 패킷들의 전송이 유효한지 확인하고 실패한 패킷은 재전송 요청 등 신뢰성 있는 통신을 보장	Firewall (L4 스위치)	Port 번호	Segment	Transport
L3	Network	다중 네트워크 링크에서 패킷을 발신지로부터 목적지로 전달할 책임을 가짐 2계층은 노드대 노드 전달을 감독하고 3계층은 각 패킷의 시작 지점에서 최종 목적지까지 성공적이고 효과적으로 전달되도록 함	Router (L3 스위치)	IP주소	Packet	Internet
L2	Data Link	오류없이 한 장치에서 다른 장치로 프레임을 전달하는 역할 스위치와 같은 장비의 경우 MAC 주소를 이용하여 정확한 장치로 정보 전달 3계층에서 정보를 받아 주소와 제어 정보를 Header와 Tail(FCS)에 추가	Bridge (L2 스위치)	MAC 주소	Frame	Network Interface
L1	Physical	물리적 매체를 통해 비트의 흐름을 전송하기 위해 요구되는 기능들을 조정 케이블, 연결장치 등과 같은 기본적인 물리적 연결기의 전지적 규격을 정하고 네트워크의 두 노드를 물리적으로 연결시켜주는 신호방식을 다룸	Hub Repeater Cable		Bit	