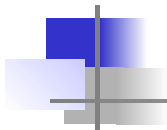
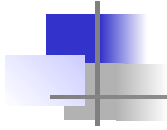


TCP/IP Protocol

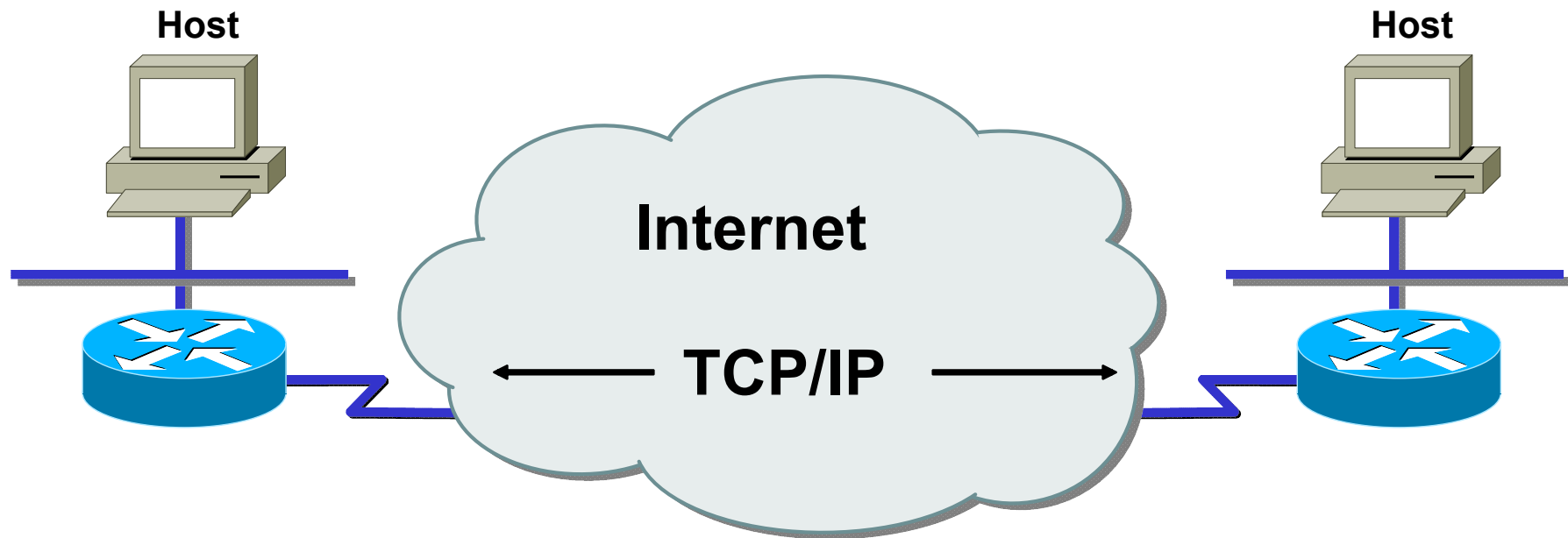


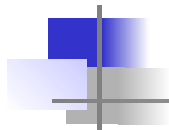
❖ TCP/IP Protocol

- TCP/IP의 특징과 기능을 이해한다.
- TCP 패킷을 분석할 줄 안다.
- UDP 패킷을 분석할 줄 안다.
- IP 패킷을 분석할 줄 안다.
- ARP, RARP, ICMP Protocol의 쓰임새를 안다.



TCP/IP Overview





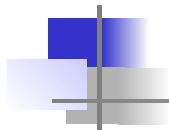
TCP/IP Overview

정의

- ISO/OSI 계층 4 Transport Protocol에 해당
- Transmission Control Protocol/Internet Protocol
- 미 국방성(DOD)에서 이기종 컴퓨터간의 통신 및 자원을 공유하기 위한 목적으로 개발된 미 국방성용 Protocol
- 신뢰할 수 없는 Network 환경에 접속된 컴퓨터간의 신뢰적인 통신을 위해 설계된 Program의 집단

배경

- 1969 : ARPANET 시작
- Advanced Research Projects Agency(미 국방성 고등연구 프로젝트국)
- 1972 : ARPANET의 Demo
- 1970 중반 : UNIX(DEC PDP-11)와 TCP/IP의 관계가 시작
- 1980 : 미 국방성의 Protocol로서 채택
- 1980 초반 : NCP와 TCP를 포함하는 Berkeley UNIX발표
- TCP/IP가 DOD(Department of Defense:미국방성)의 표준으로 확정
- 1983 : TCP/IP가 Military Standard Specification이 됨



TCP/IP Overview (Cont.)

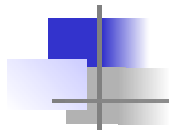
특징

가. TCP/IP와 OSI의 관계

- ISO/OSI의 계층 3,4에 해당
- 개방형 프로토콜의 표준
- 물리적 Media에 대한 독립성
- TCP/IP 주소 체계
- 일관성 있는 상위 layer의 프로토콜

나. 기능

- 신뢰성 있는 가상회로(Virtual Circuit)연결 기능을 제공
- 다수의 서로 다른 network으로 연결된 Host간의 통신을 지원
- 기본적인 데이터 전송(Basic Data Transfer)
- 신뢰성보장(Reliability) 보장



TCP/IP 프로토콜

TCP/IP Protocol Stack별 기능

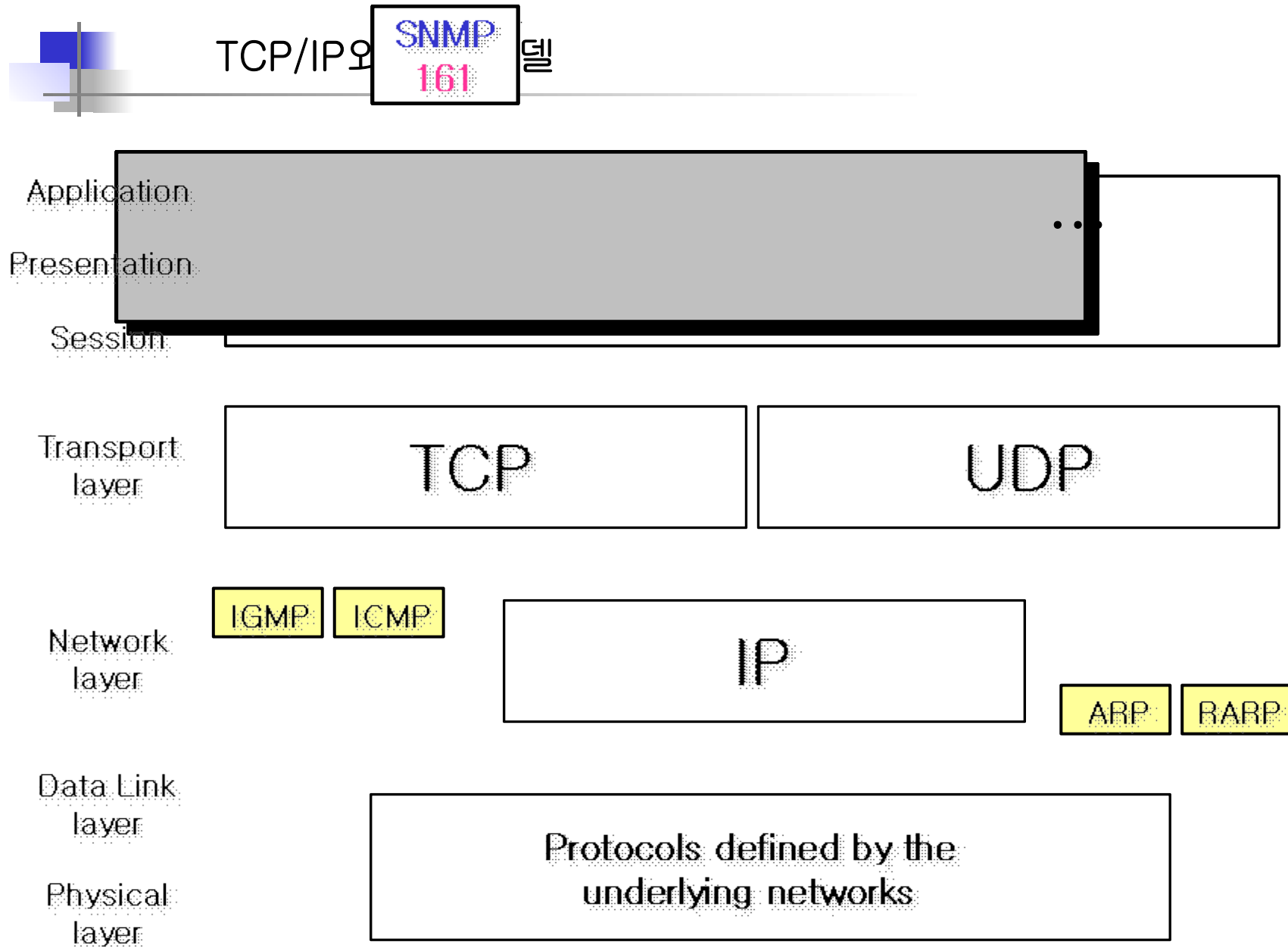
OSI 7 Layer Model

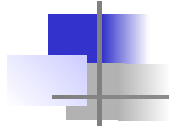
Application
Presentation
Session
Transport
Network
Data Link
Physical

TCP/IP Protocol

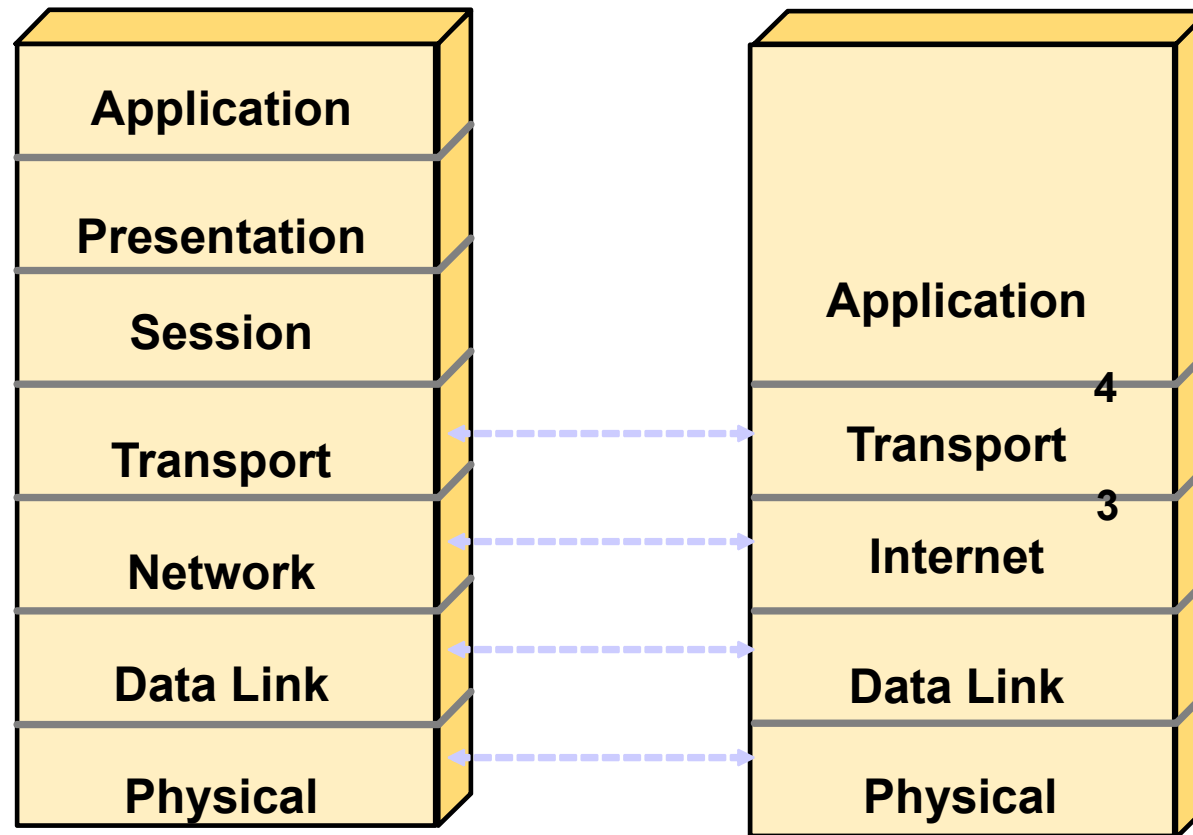
Port No.	Application	FTP 21	TELNET 23	SMTP 25	DNS 53	TFTP 69	SNMP 161
	Transport	TCP 6			UDP 17		
	Protocol No.	Internet	IP	ICMP	ARP	RARP	
	Network Interface	Network Interface					

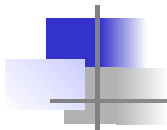
OSI 7계층 모델과 TCP/IP 프로토콜 모델의 비교





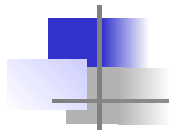
TCP/IP Protocol Stack





TCP/IP Protocol 구조

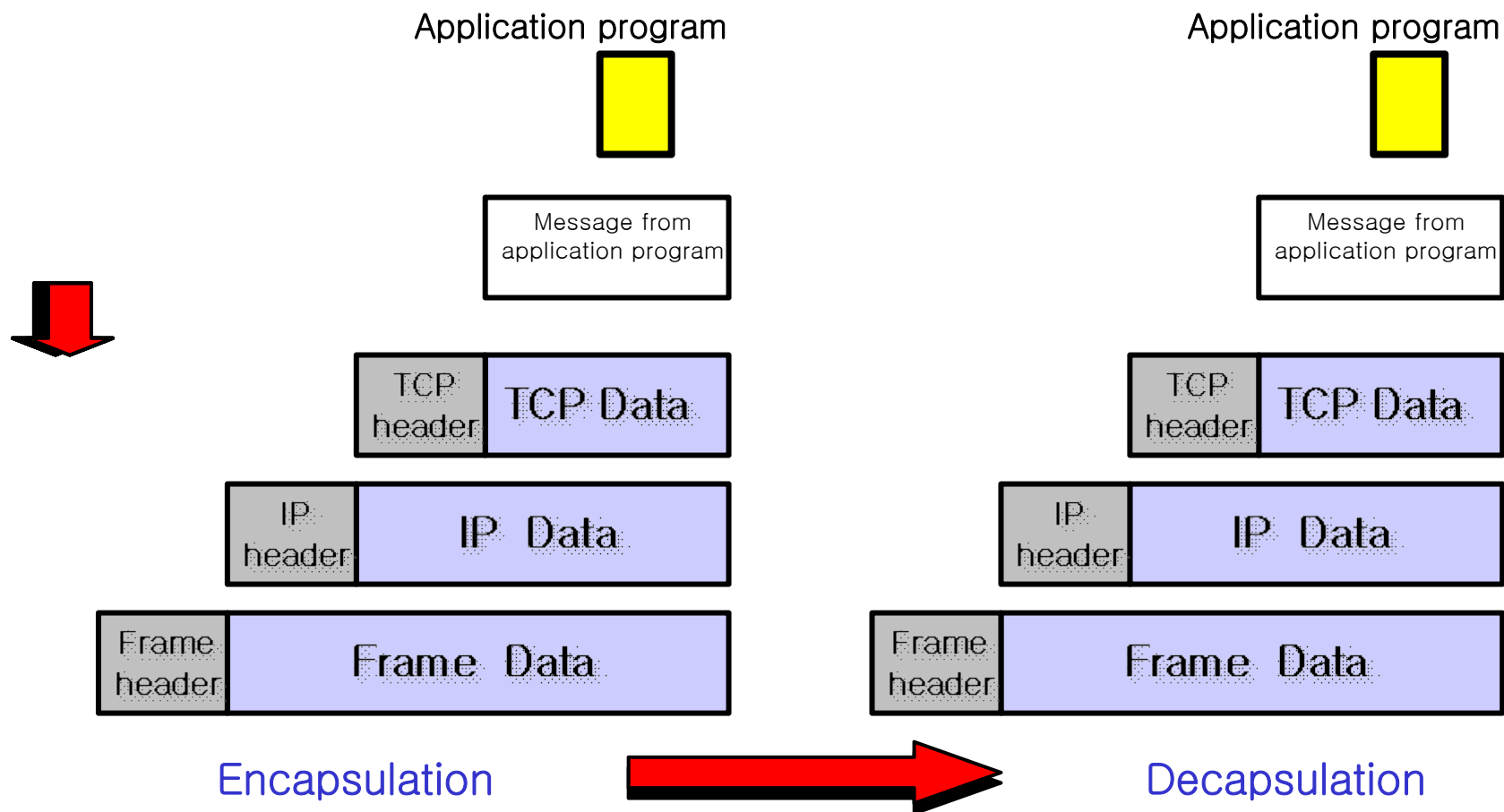
- TCP(Transmission Control Protocol)
 - ✓ 연결지향 프로토콜
 - ✓ 사용자 프로세스에게 신뢰성 있는 full-duplex, byte stream 서비스를 지원한다.
 - ✓ 대부분의 인터넷 응용들은 TCP를 사용한다.
- UDP(User Data Protocol)
 - ✓ 비연결 프로토콜
 - ✓ UDP datagram의 목적지 도달을 보장 못함
- ICMP(Internet Control Message Protocol)
 - ✓ 호스트와 게이트웨이간의 에러 및 제어 정보를 제어
- IP(Internet Protocol)
 - ✓ TCP, UDP, 및 ICMP를 위한 패킷 전달 서비스를 제공
- ARP(Address Resolution Protocol)
 - ✓ IP 주소를 Hardware 주소로 매핑
- RARP(Reverse ARP)
 - ✓ Hardware 주소를 IP 주소로 매핑

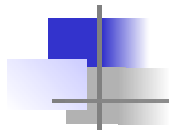


Data Encapsulation & Decapsulation

데이터에 제어 정보를 Header 형태로 추가

데이터에 제어 정보 기록한 Header 제거

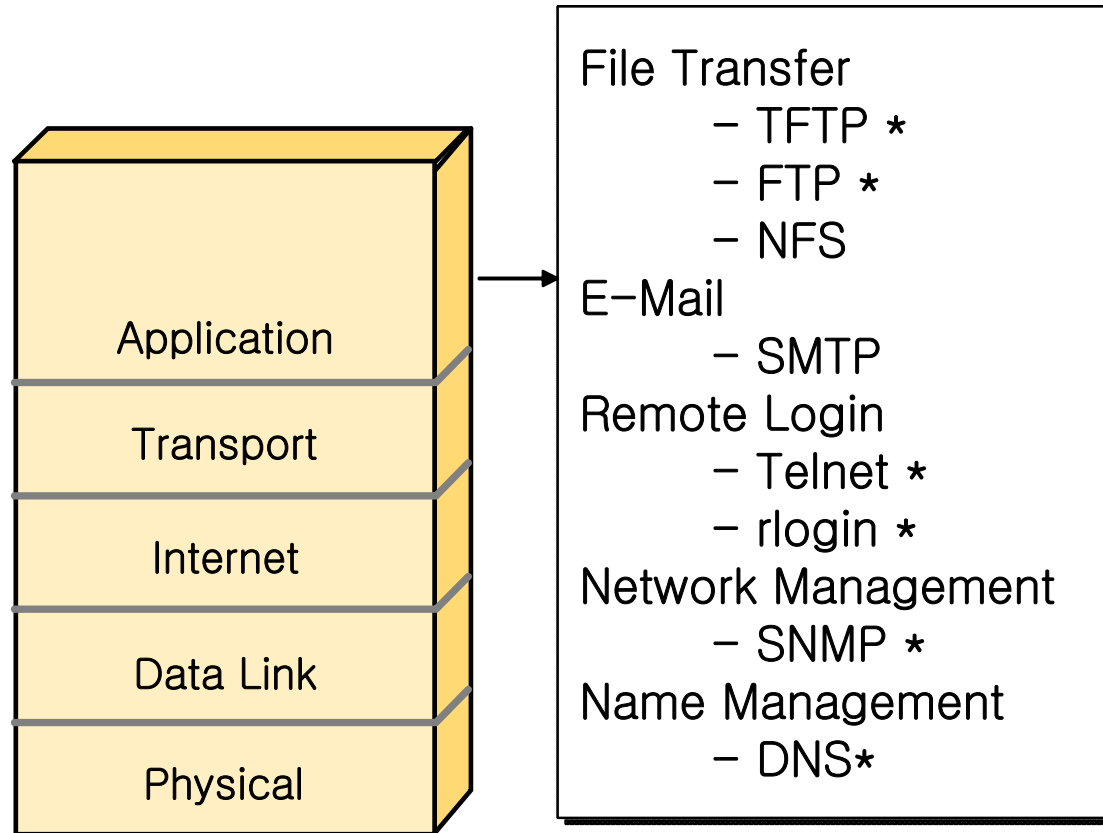




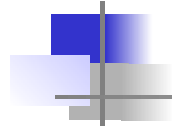
데이터의 계층별 데이터 명칭

Layer	TCP	UDP
Application Layer	stream	message
Transport Layer	segment	packet
Internet Layer	datagram	
Network Access Layer	frame	

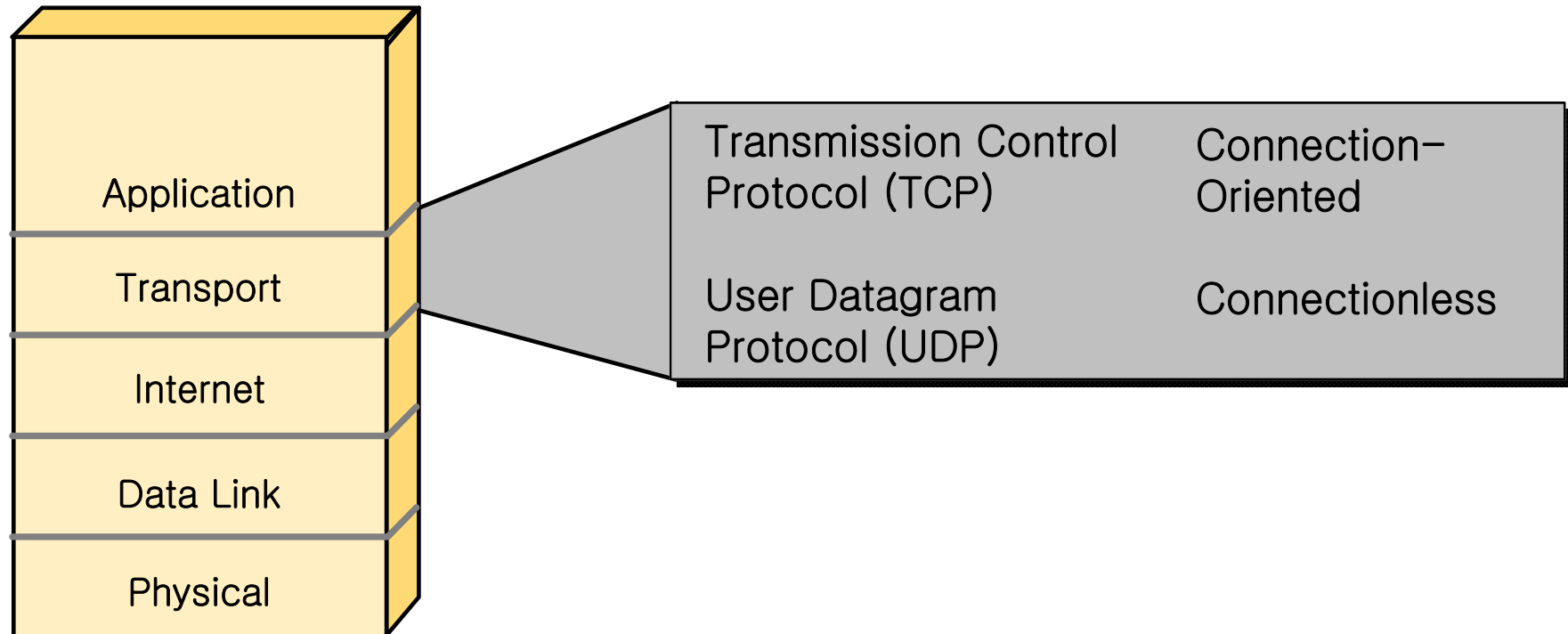
Application Layer

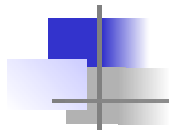


- Application Protocol사이의 데이터 교환을 책임지는 계층.



TCP/IP Transport Layer Overview





Transport Layer

기능

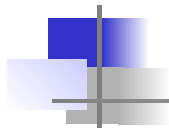
- Application 계층에서 세션과 Datagram 통신 서비스를 제공
- End-to-End간 통신 데이터의 무결성에 대한 역할을 담당하는 계층
- TCP와 UDP
- transport layer에서 application layer와 port번호를 이용해 통신을 한다. 가령 FTP에 의한 데이터를 전달 받았을 때 transport layer에서는 port 21번으로 해당 데이터를 전달한다

TCP

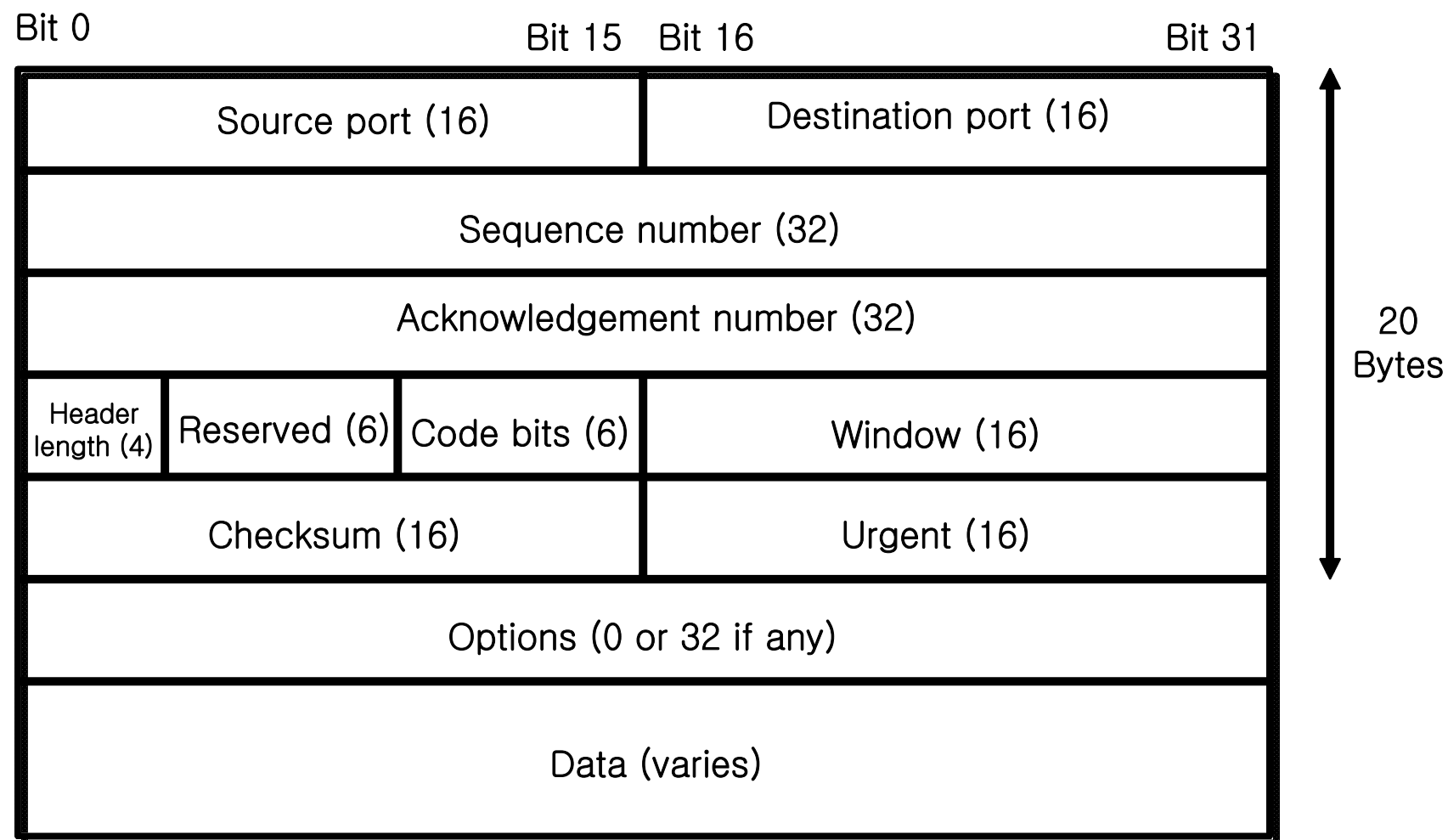
- 일대일의 Connection-oriented, 신뢰할 수 있는 통신 서비스를 제공하며 TCP는 TCP 연결 확립과 보내진 패킷의 확인, 순서화, 전달 중에 손상된 패킷을 복구하는 책임을 맡고 있다.

UDP

- 일대일, 일대 다의 connectionless, 신뢰할 수 없는 통신 서비스를 제공한다. UDP는 주로 전달할 데이터의 크기가 작거나 TCP 연결 확립에 의한 부하를 피할 때 혹은 상위 프로토콜이 신뢰할 수 있는 전달을 책임지는 경우에 사용된다.



TCP Segment Format



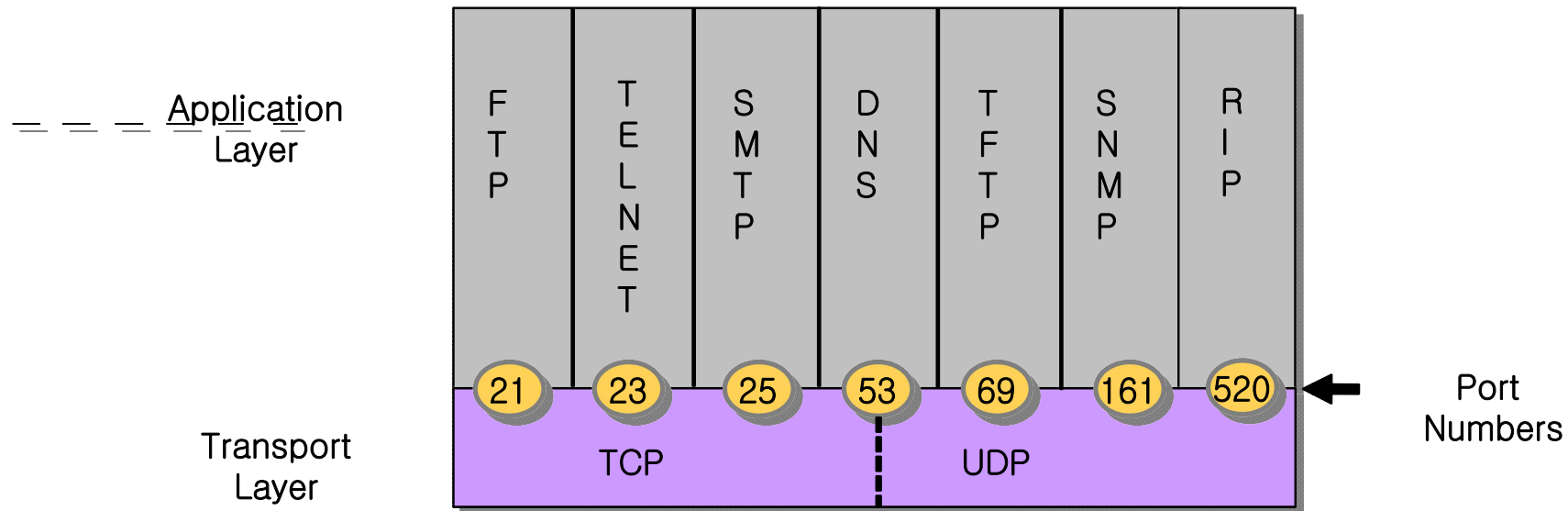


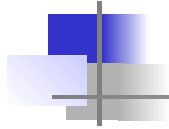
Fields in Datagram

- source와 destination 포트 번호
: TCP 연결의 양 종단에 있는 응용 프로그램을 나타내는 포트 번호
- sequence 번호
: 세그먼트에 들어 있는 데이터가 응용 프로그램의 byte stream에서 어느 위치에 있는지를 표시한다.
- ACK 번호 : 수신측에서 송신측으로부터 받은 세그먼트에 대한 응답
: 바로 다음에 받기를 기다리는 세그먼트의 byte 번호를 의미한다.
- 헤더 길이
: 32 bits의 정수배로 계산된 세그먼트 헤더 길이를 나타내는 정수값
- 예약(Reserved) : 차후 사용을 위해서 예약된 6-비트 필드
- 제어(Control) : 6 개의 서로 다른 제어 비트 또는 플래그를 나타냄
- 윈도우 크기(window size)
: receiver의 입장에서 현재 자신의 가용 버퍼(available buffer)의 크기를 알려 준다.
: 이것을 이용하여 양 종단 간의 flow control을 수행한다.
- Checksum

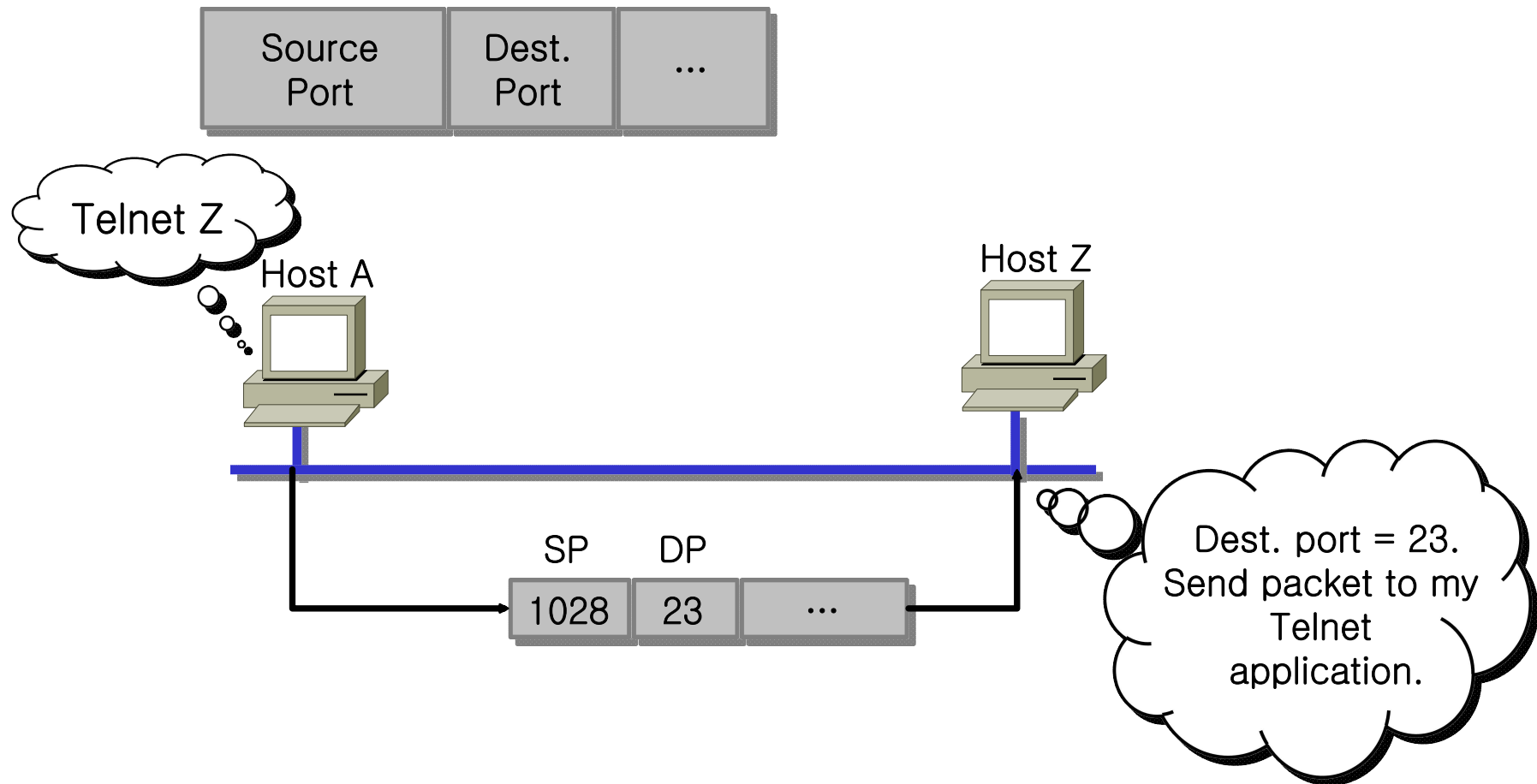
TCP Port Numbers

- Telnet Service(Daemon)의 TCP Port 23번이 Port Address로 할당되어 Telnet Service는 23번 포트를 Listening한다.
- 원격의 Telnet Client가 Telnet Server의 해당 IP Address와 23번 Destination Port Address로 Telnet Service를 요청하면 23번 포트를 Listening하던 Telnet Service가 응답하여 Telnet Service가 이루어지게 된다.
- Port Address 1 -65535까지의 할당이 가능
- 0- 1023번 까지의 Port Address는 Well-Known Port Address라 하여, 이미 특정 서비스로 정의된 Address 이다.



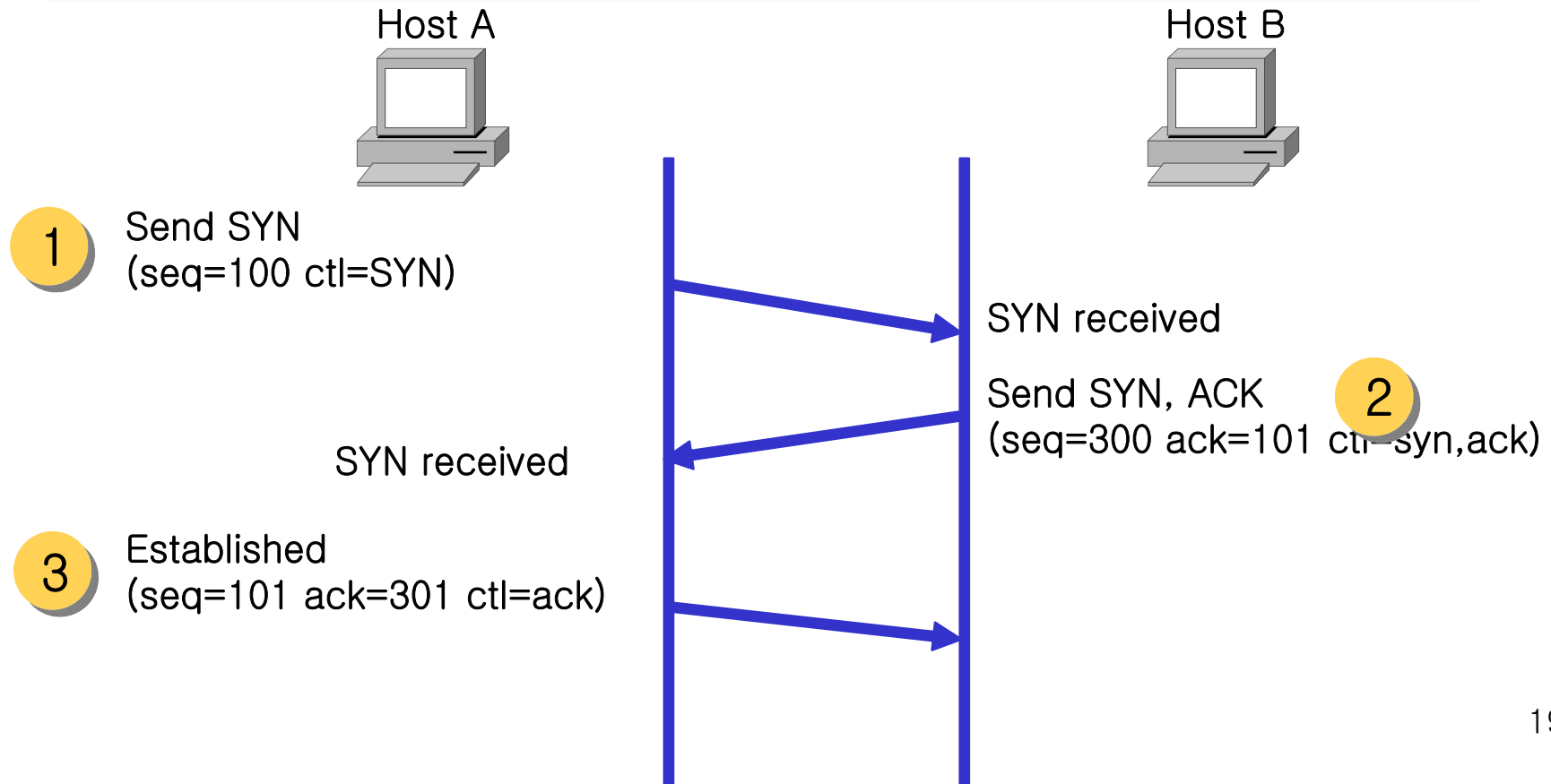


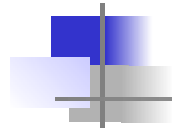
TCP Port Numbers



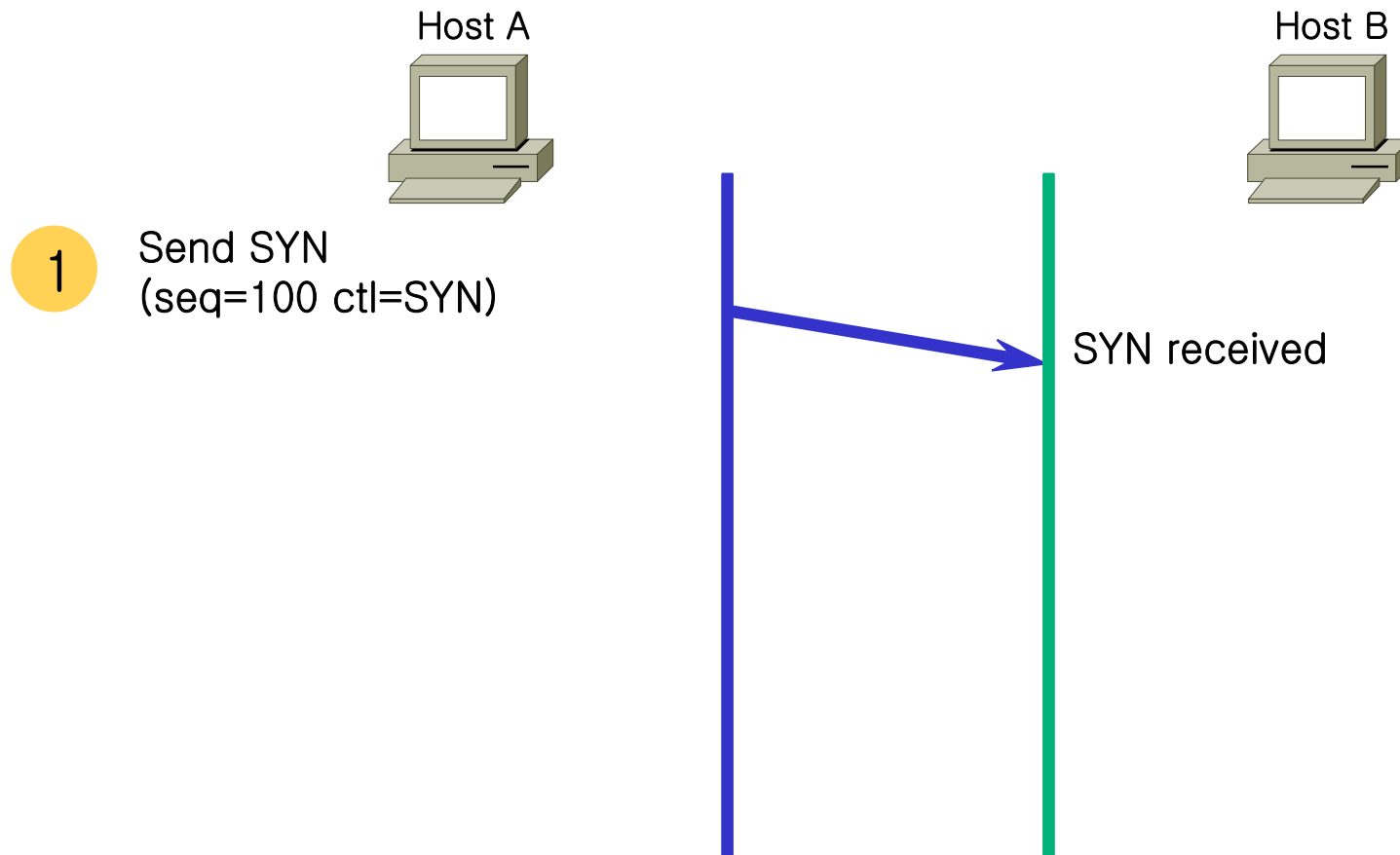
TCP 연결설정 및 연결종료

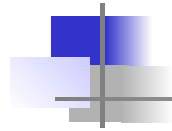
- TCP는 Connection Oriented Protocol로 노드간 데이터 교환 전에 세션을 형성한다. Three Hand-Shaking이라는 Process에 의해 두 노드간에 Virtual Circuit을 생성하고, 데이터를 교환한다. 데이터 교환이 끝나면 Two Hand-Shaking에 의해 Session을 종결한다.
- 연결설정을 통하여 초기 Sequence No, Window 사이즈, MTU 사이즈 등의 정보를 교환한다.



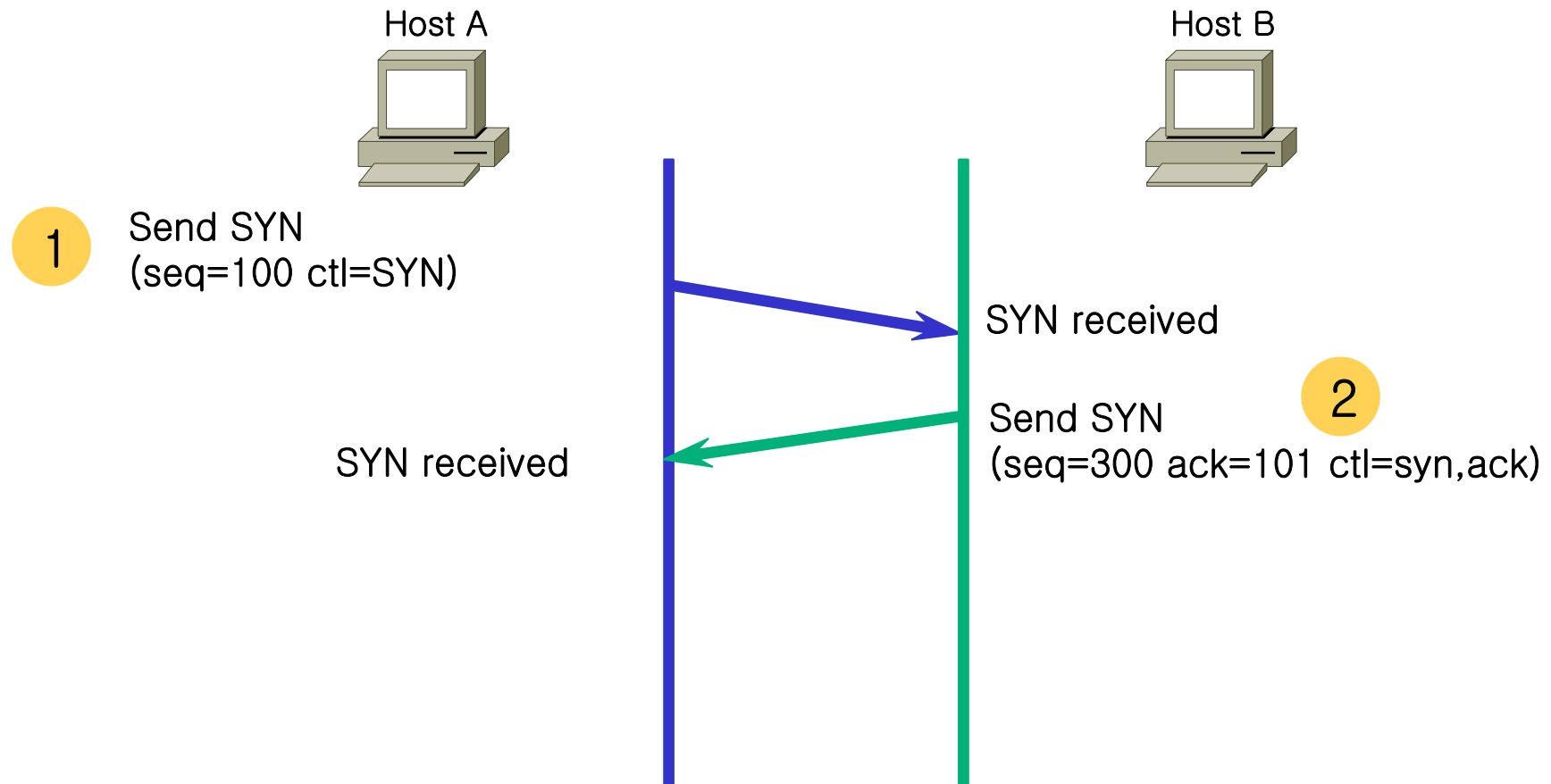


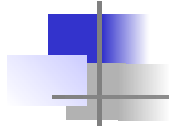
TCP Handshake/Open Connection



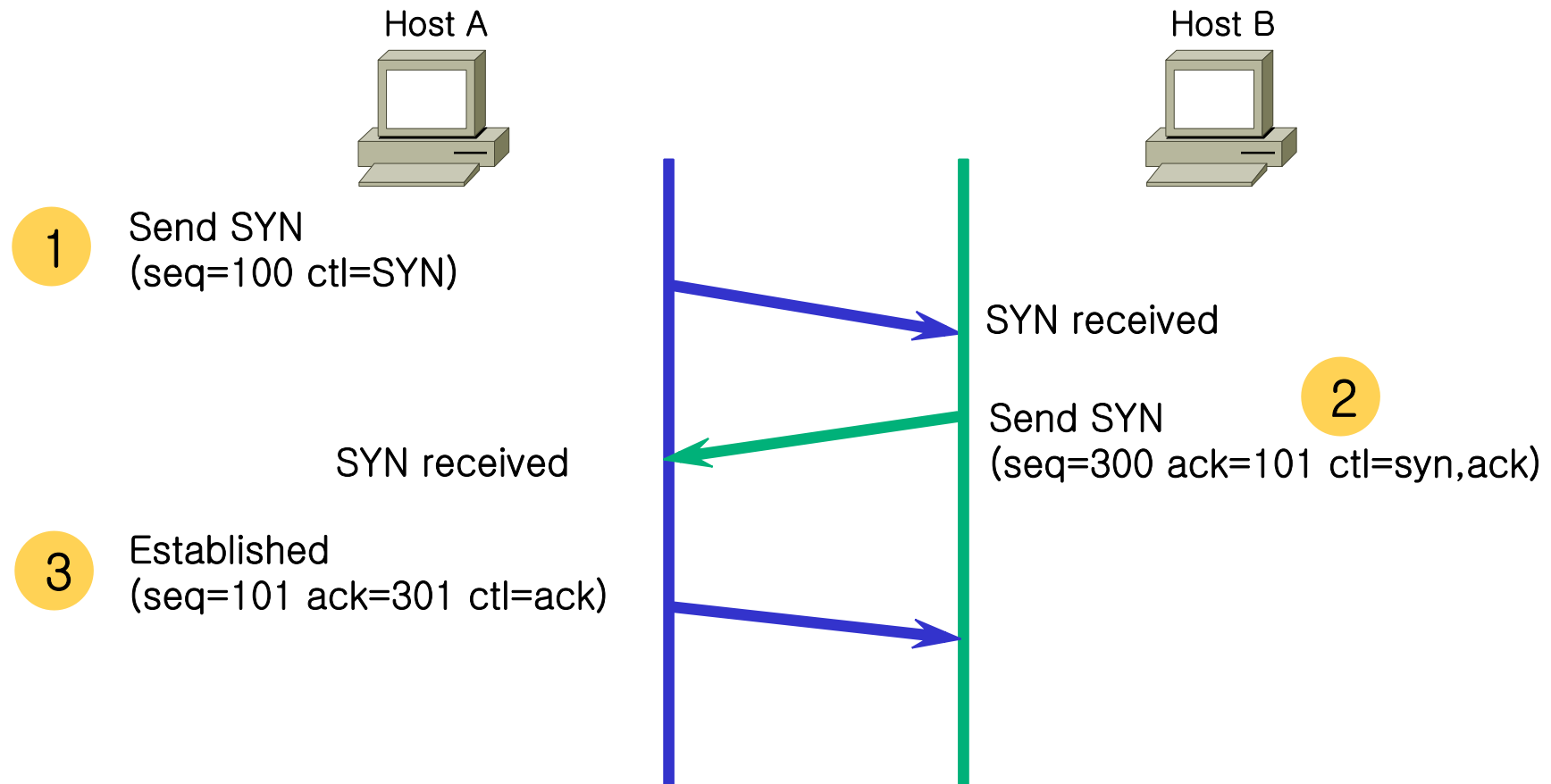


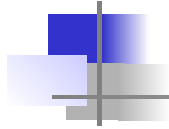
TCP Handshake/Open Connection



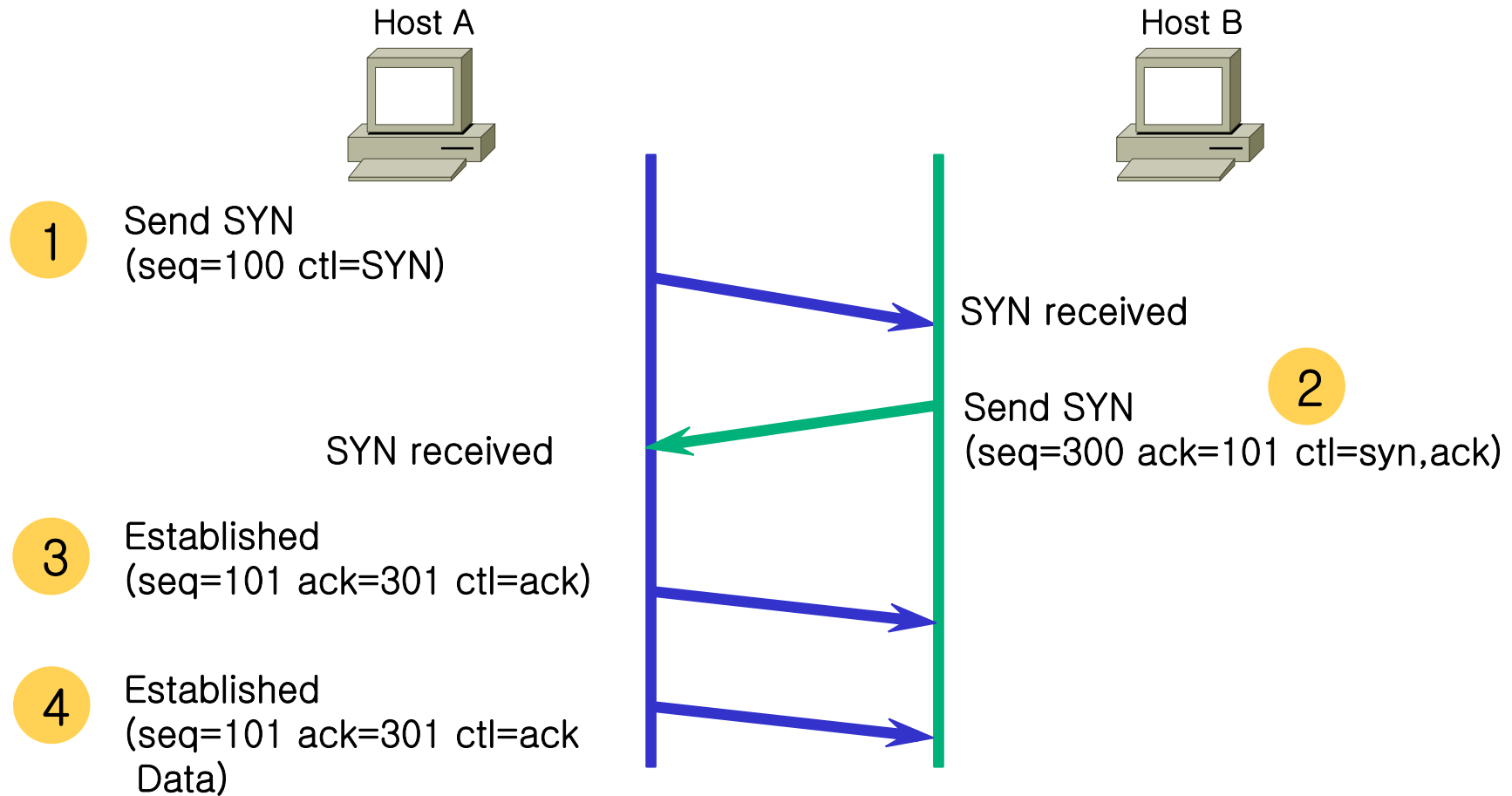


TCP Handshake/Open Connection

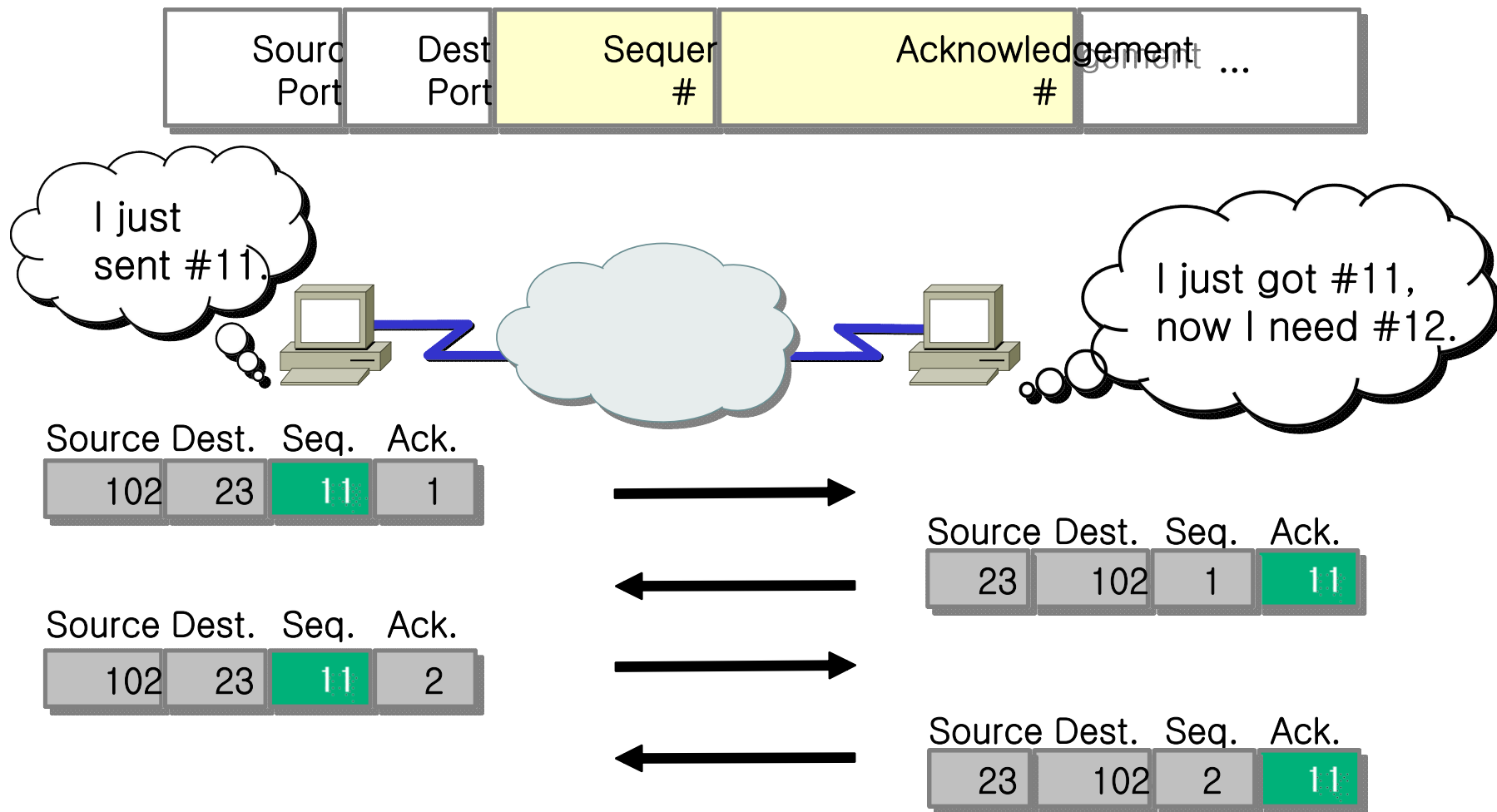




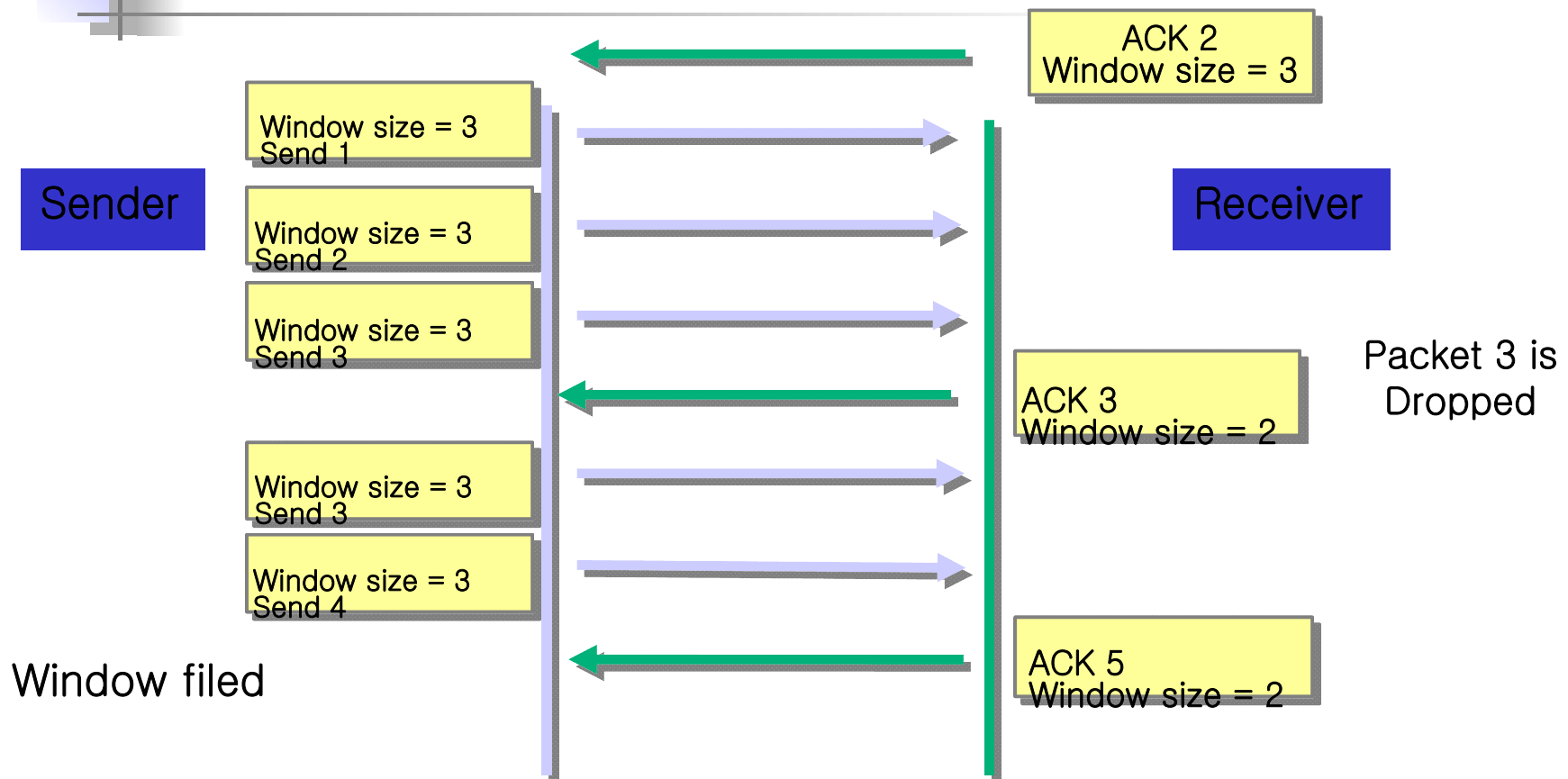
TCP Handshake/Open Connection



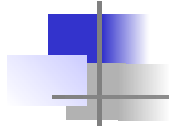
TCP Sequence & Acknowledgment



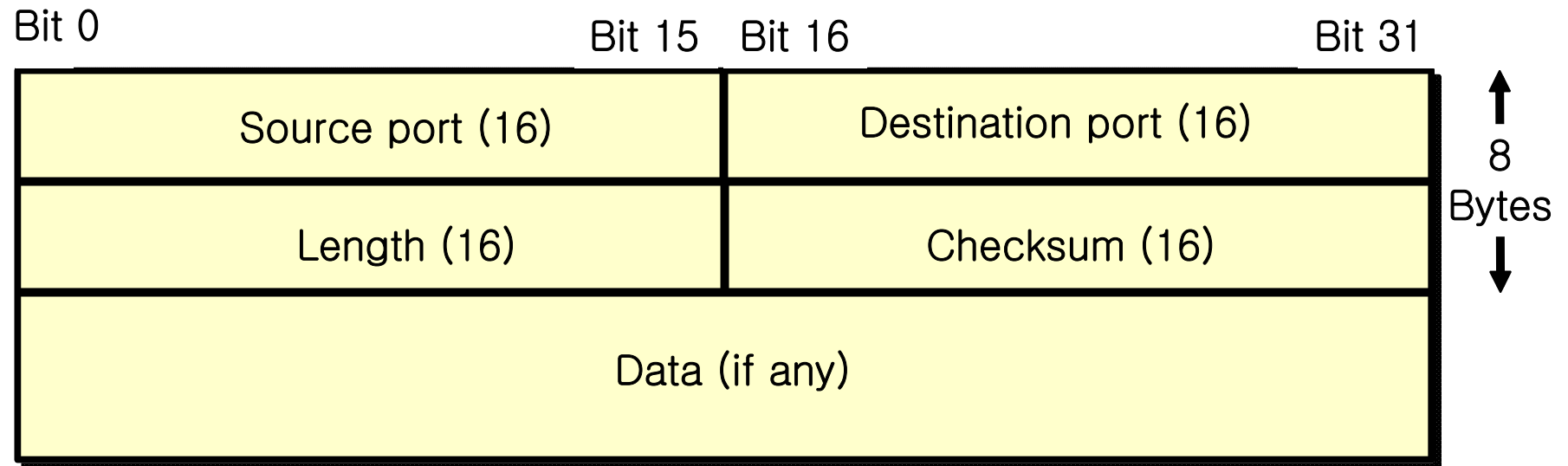
TCP Windowing



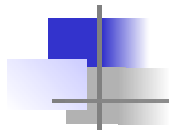
- 흐름제어를 위하여 수신 TCP는 자신이 준비해 놓은 Octet (1 Byte)수를 지정하여 알린다.
- 송신 TCP는 이를 참조하여, 슬라이딩 윈도우 수를 조절할 수 있다. 이 필드의 길이가 16bit이므로 윈도우의 최대 크기는 65,535 바이트이다.



UDP Segment Format

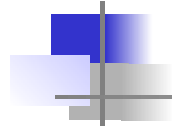


- No sequence or acknowledgment fields

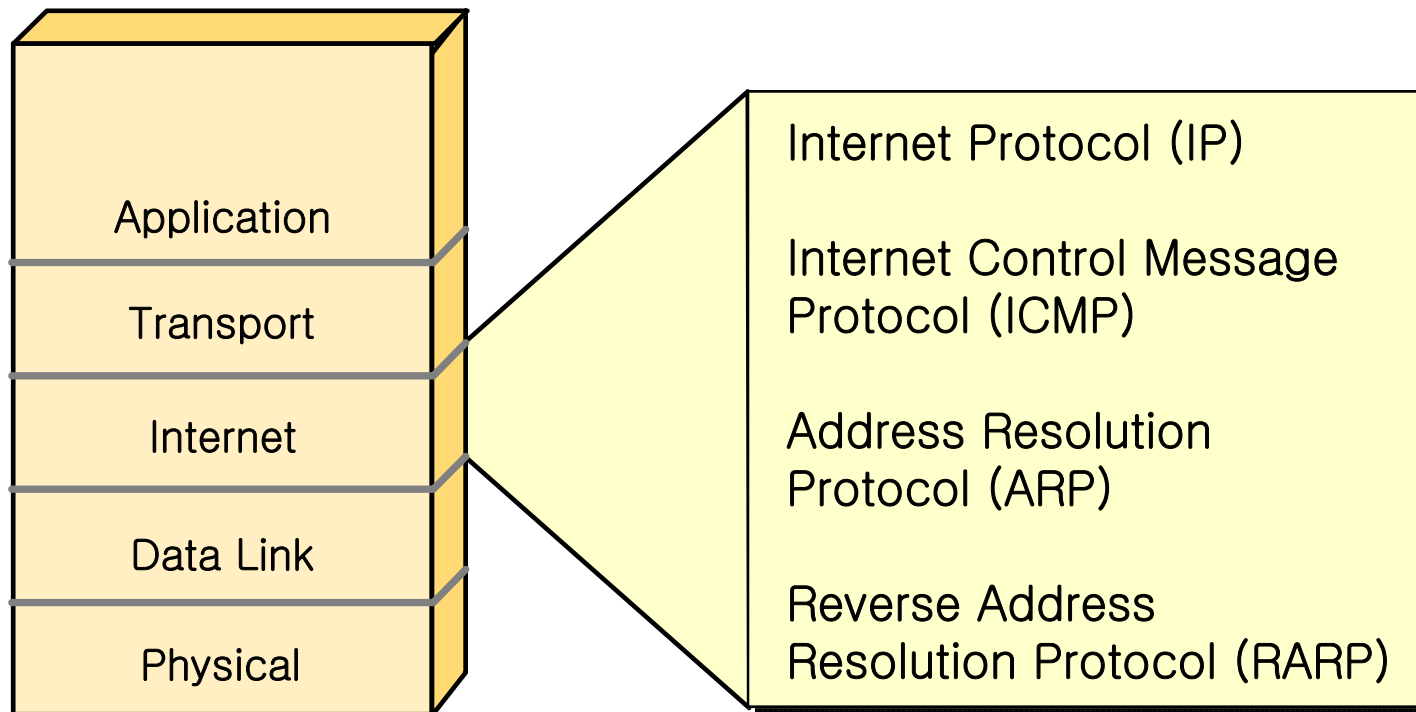


Fields in Datagram

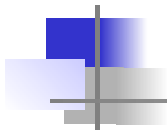
- **SOURCE PORT, DESTINATION PORT** : SOURCE PORT 는 응답을 받을 포트어드레스가 된다. Destination Port는 UDP 통신의 목적지 포트 어드레스로 UDP 서버인 경우 포트번호는 잘 대부분의 경우 알려진 포트번호이다.
- **LENGTH** : UDP datagram (header+data)의 Byte 수를 나타낸다. 최소 값은 8이다.
- **CHECKSUM** : 선택적인 필드로 0이 올 수도 있으며, 이 경우는 체크섬을 계산하지 않음을 의미한다. 수신 노드에서 검사합을 계산하여 맞지 않는 경우 UDP Datagram은 조용히 폐기된다.



Internet Layer Overview

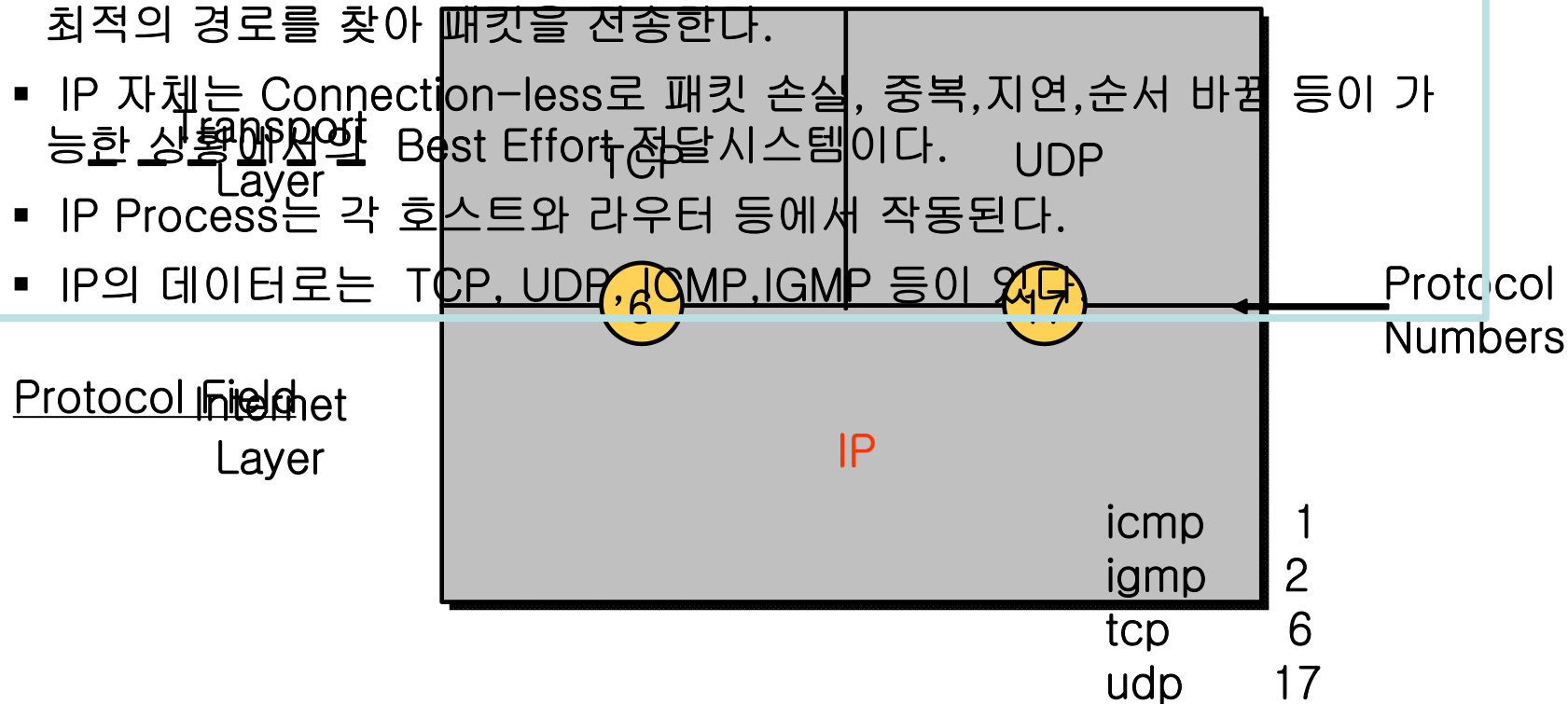


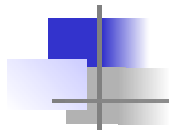
- OSI network layer corresponds to the TCP/IP internet layer



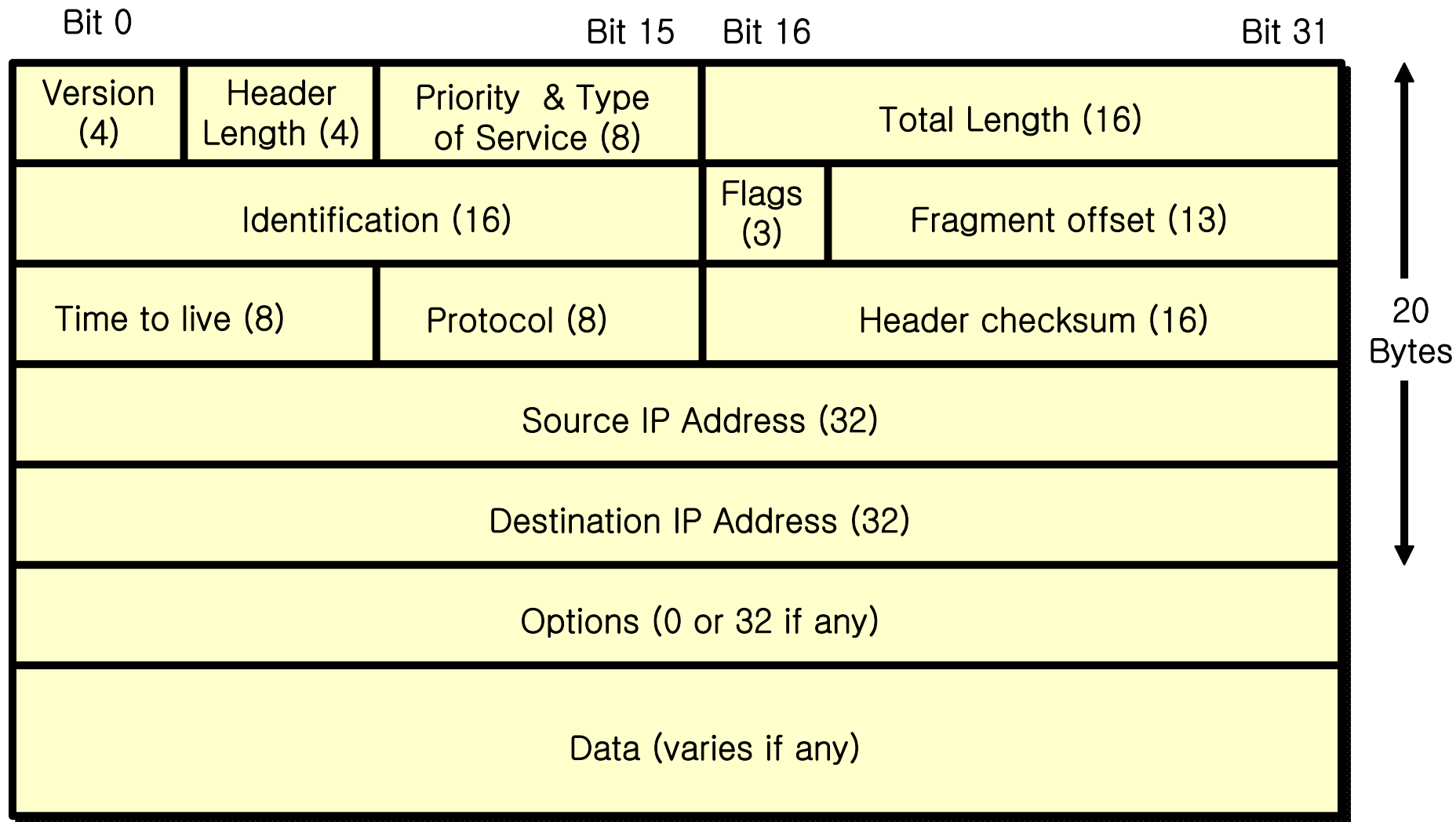
Internet Protocol Overview

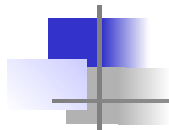
- 패킷의 목적지 주소(Destination IP Address)를 보고, 네트워크에 대한 최적의 경로를 찾아 패킷을 전송한다.
- IP 자체는 Connection-less로 패킷 손실, 중복, 지연, 순서 바뀔 등이 가능한 상황에서의 Best Effort 전달 시스템이다. UDP
- IP Process는 각 호스트와 라우터 등에서 작동된다.
- IP의 데이터로는 TCP, UDP, ICMP, IGMP 등이 있다.





IP Datagram Format





Fields in Datagram

- **VERS (Version)** : IP protocol version (Ipv4, IPv6)
- **HLEN (Header Length)** : 데이터그램의 헤더길이(통상 20바이트)를 표시한다. 데이터그램의 헤더는 60 바이트까지 가능하다. IP헤더의 길이를 32비트 단위로 나타낸다. 대부분의 IP 헤더의 길이는 20바이트이며, 이 필드의 값은 거의 항상 5다. ($5 \times 32 = 160$ 비트, 또는 20바이트)
- **Service Type** : 우선순위(3bit)와 서비스유형(4bit)의 서브필드로 구성되며, 현재 버전(Version 4)에서는 보통 우선순위는 사용되지 않는다. 응용 프로그램은 특정한 서비스 유형을 IP에 요청할 수 있다.
- **TOTAL LENGTH** : IP Header와 데이터 길이의 합계이며 16bit로 표현되므로 IP Packet의 최대길이는 65,536 바이트까지 가능하다.
- **Fragmentation Identifier** : 데이터그램의 식별자이다.
- **Fragmentation Flags** : Fragment된 패킷 인지, Fragment된 경우 마지막 Fragment인지를 표시한다.
- **Fragment Offset** : . Fragment된 패킷인 경우, 원래 패킷에서의 위치를 표시한다. 8 바이트 데이터 단위로 표시된다.



Fields in Datagram(Cont.)

- **TIME TO LIVE (TTL)** : 데이터그램의 수명을 나타낸다. 라우터를 경유시 1씩 감소한다.
- **PROTOCOL Identifier** : IP가 전송하는 프로토콜을 명시한다. (TCP=6, UDP=17, ICMP=1, OSPF=89)
- **Header Checksum** : IP Header의 체크섬 값을 저장한다. 경유지 및 도착지에서 헤더의 체크섬을 재계산하여 일치하지 않으면 데이터그램을 폐기한다.
- **SOURCE IP ADDRESS** : 보내는 노드의 32-bit IP address
- **DESTINATION ADDRESS** : 받는 노드의 32-bit IP address
- **IP OPTIONS** : 특별한 IP 추가 Option을 설정할 수 있으나, 대부분의 경우 사용하지 않으며, 사용하면 IP Header가 20Byte를 초과하는 유일한 사유가 된다. 최대 40Byte까지 가능하므로 IP Header의 크기는 최대 60Byte에 이를 수 있다.
- **PADDING** : Option이 추가되는 경우, IP Header가 32bit 단위로 끝날 수 있도록 채우는 부분이다.

Type of Service

우선순위(3bit)와 서비스유형(4bit)의 서브필드로 구성

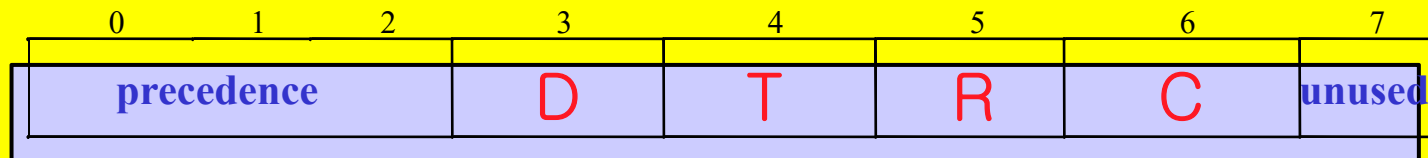
- **Precedence Field(3bit)** : 0-7까지의 패킷 전송 우선순위를 부여할 수 있다. 현재 사용 안 한다.
- **TOS field(4bit)**의 권장 값(통상 DTRC가 모두 0인 Normal Mode로 사용한다.) 응용프로그램은 특정한 서비스 유형을 IP에 요청할 수 있다.

D : Minimize Delay

T : Maximize Throughput

R : Maximize Reliability

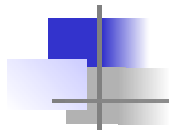
C : Minimize Cost



Type of Service

- **Minimize Delay**를 선택하면 IP가 빠른 응답을 위하여 정체가 적은 경로를 선택하며, **Maximize Throughput**을 선택하는 경우는 대역폭이 큰 경로를 우선적으로 선택, **Maximize Reliability**는 신뢰성이 높은 경로, **Minimize Cost**는 비용이 가장 적은 경로를 설정토록 요구한다.

Protocol	TOS Bits(DTRC)	Description
ICMP	0000	Normal
BOOTP	0000	Normal
NNTP	0001	Minimize Cost
IGP	0010	Maximize Reliability
SNMP	0010	Maximize Reliability
TELNET	1000	Minimize Delay
FTP(data)	0100	Maximize Throughput
FTP(control)	1000	Minimize Delay
TFTP	1000	Minimize Delay
SMTP(command)	1000	Minimize Delay
SMTP(data)	0100	Maximize Throughput
DNS(UDP query)	1000	Minimize Delay
DNS(TCP query)	0000	Normal
DNS(zone)	0100	Maximize Throughput



IP Fragmentation

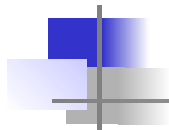
MTU (maximum transfer unit)와 Fragmentation

▪ MTU(Maximum Transport Unit)

- ✓ 두 노드간 물리적 네트워크에 대한 데이터 필드 최대 크기
- ✓ Ethernet 인 경우 최종 데이터 프레임이 1518 Byte까지 이다.
- ✓ IP 데이터그램의 최대 가능 크기는 65536 바이트이다.
- ✓ (Total Length Field가 16비트이므로 2의 16승의 크기까지 가능하다.)

Protocol	MTU	Protocol	MTU
HyperChannel	65,535byte	16Mbps Token Ring	17,914byte
FDDI	4,352byte	4Mbps Token Ring	4,464byte
DIX Ethernet	1,500byte	802.3	1,492byte
X.25	576byte	PPP	296byte

서로 다른 네트워크의 MTU



IP Fragmentation

MTU (maximum transfer unit)와 Fragmentation

▪ Fragmentation

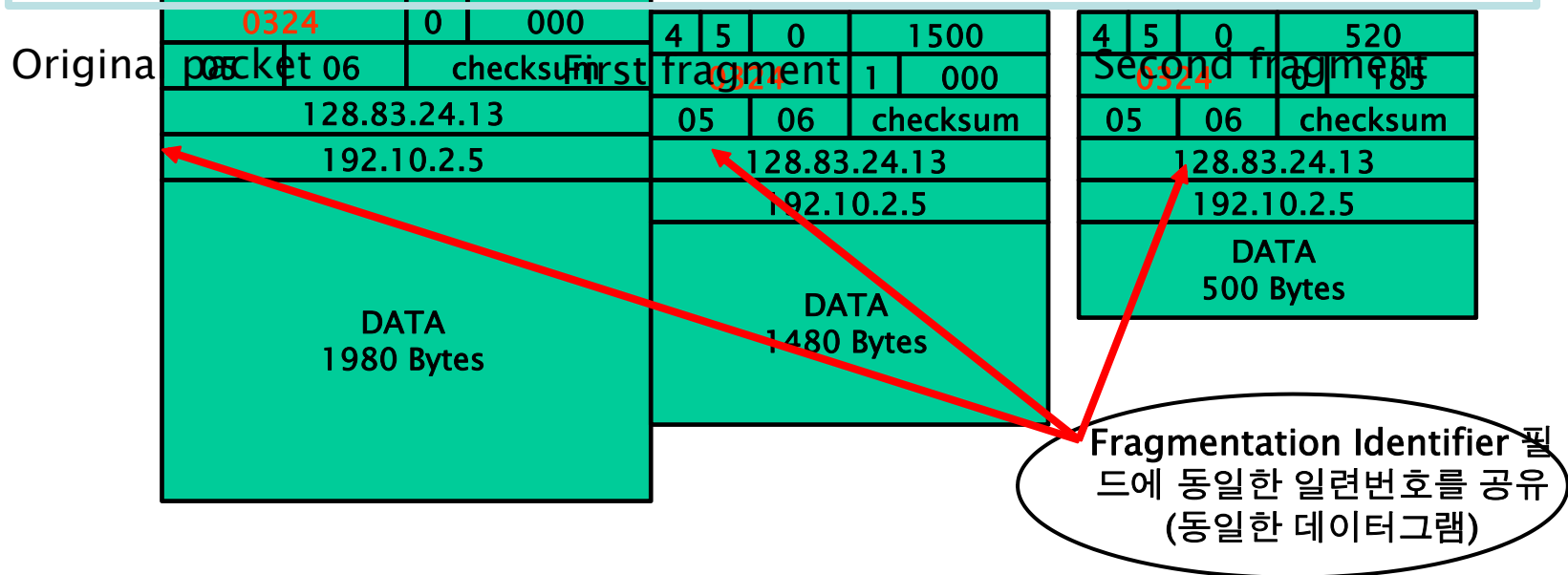
- ✓ IP는 전송 구간의 물리적 네트워크 MTU에 따라 Packet을 단편화 한다.
- ✓ Datagram이 MTU보다 클 경우, 각 데이터그램은 여러 개의 조각으로 분리된다.
- ✓ 경유 라우터는 단편들을 재 조립하지 않고, 목적지의 IP가 단편화된 패킷을 재조립한다.
- ✓ TCP 레벨에서는 메시지 관리의 효율성을 고려 대개 MTU 크기를 최대로 사용하여 세그먼트를 만들어 IP Layer로 내려 보낸다.
- ✓ UDP의 레벨에서는 Application이 제공하는 크기(65536Byte의 크기 까지 가능하다.)의 데이터그램을 IP Layer로 내려 보내면 IP가 필요시 Fragmentation

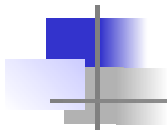
IP Fragmentation

단편화와 관련된 필드

■ 식별자(Identification) : 16비트 필드

- ✓ 발신지 호스트가 전송하는 데이터그램을 지정
- ✓ 보통 매번 값을 1씩 증가 시킨다.
- ✓ 식별자와 IP 주소의 조합은 데이터그램이 발신지를 떠날 때 유일하게 정의되어야 함
- ✓ 데이터그램이 단편화 될 때 식별자 필드값은 모든 단편에 복사됨



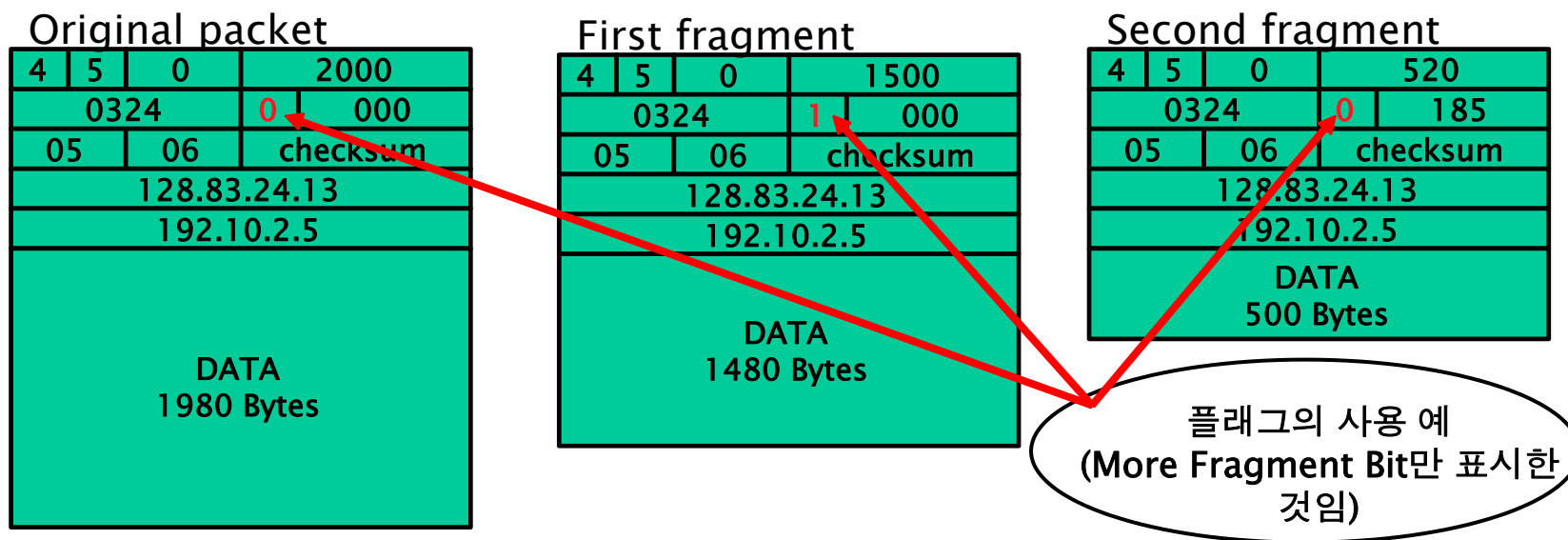


IP Fragmentation

단편화와 관련된 필드

■ 플래그(Flag) : 3비트 필드

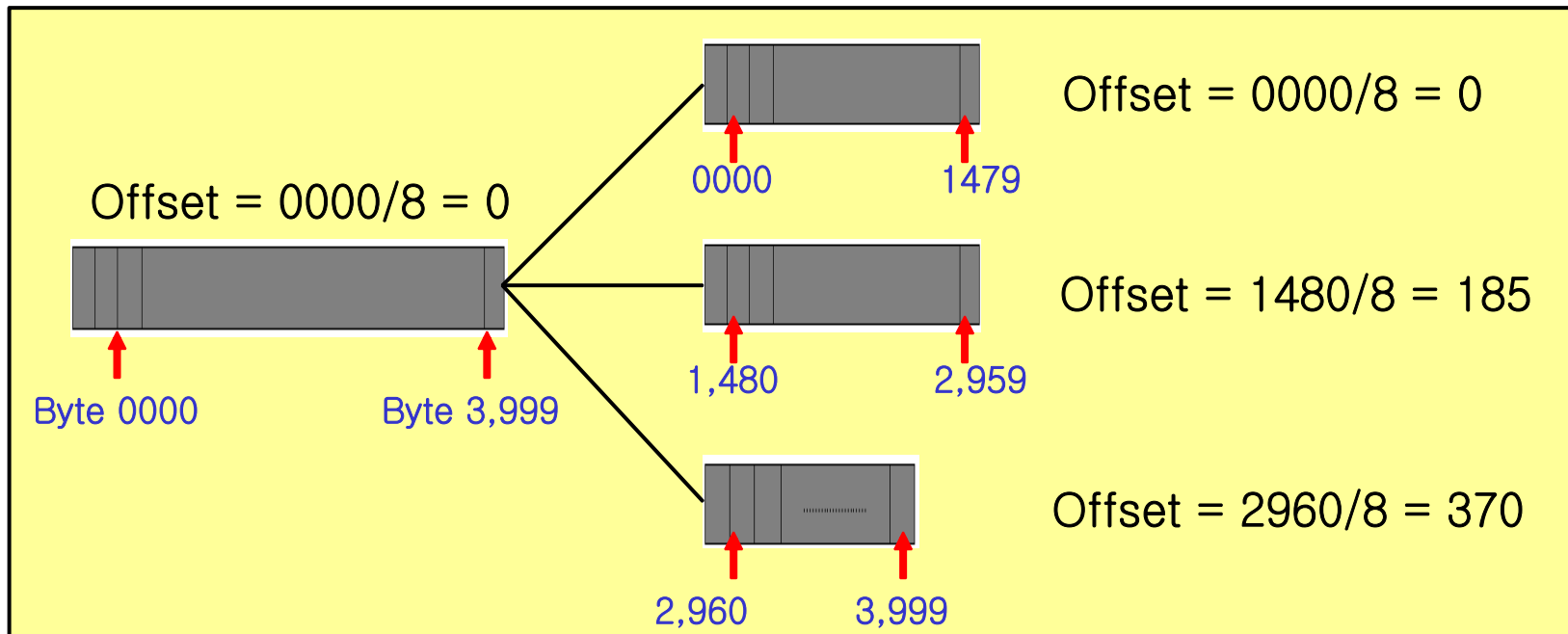
- ✓ 처음 비트 : 사용하지 않음(Reserved Flag) - 0
- ✓ 두 번째 비트 : Do not Fragment 비트. 1이면 단편화 해서는 안됨
- ✓ 세 번째 비트 : More Fragment 비트. 1이면 데이터그램이 마지막 단편이 아니라는 것을 의미. 0이면 마지막 단편이거나, 유일한 단편임



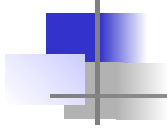
IP Fragmentation

단편화와 관련된 필드

- 단편화 오프셋(Fragmentation Offset) : 13비트 필드
 - ✓ 전체 데이터그램 내에서 단편의 상대적 위치
 - ✓ 원 데이터 그램 내에서 데이터의 오프셋을 8바이트 단위로 나타냄



4000Byte의 데이터그램 단편화의 예 (단편화의 크기는 MTU에 따라 다름, 여기서는 1480Byte)

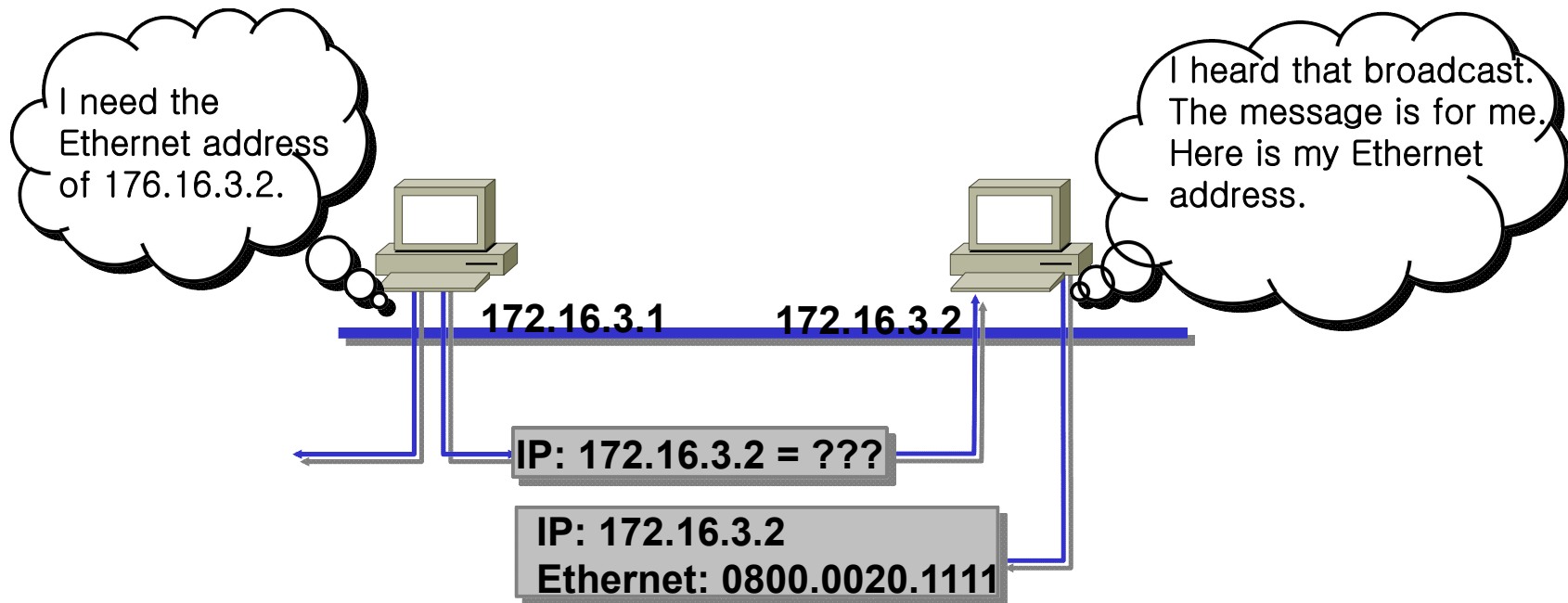


TTL(Time To Live)

- 라우터를 경유할 때 마다 수명필드가 1씩 감소한다. 수명필드가 0이 되면 데이터그램을 버리고 ICMP 오류메시지를 근원지에 발송한다. 데이터그램의 Looping을 방지하는 목적, 전달범위를 제한하는 목적 등으로 사용된다. 예를 들어 TTL이 1로 설정된 데이터그램은 LAN구간을 벗어날 수 없다.
- 단위는 sec로 물론 시간적인 경과에도 영향을 받을 수 있으나, 이를 위해서는 라우터간 시간동기화 등이 필요하므로 실제로 시간에는 영향을 받지 않는다.
- TTL 필드에 1에서 255사이의 값을 지정, 최종 목적지에 도달하기 이전에 이 값이 0이되면, 패킷이 전달될 수 없는 것으로 판단되어 즉시 소멸된다.
- 이 필드의 길이가 8비트이다.
- RFC 793에서는 TTL이 60

ARP(Address Resolution Protocol)

- IP Packet 전송을 위해서는 Destination의 MAC Address를 알아내어 Frame의 Header에 DA로 설정해야 Frame 형태로 전송할 수 있다. IP는 ARP 프로토콜에 요청하여 IP Address에 대한 Layer 2 Address(MAC Address)를 알아내도록 하는데 IP Address를 MAC Address로 변환해주는 Protocol을 ARP라 한다. ARP는 Local Broadcasting에 의존한다. ARP는 한번 찾은 Address는 ARP Cache에 일정 기간 IP Address-MAC Address형태로 보관한다.

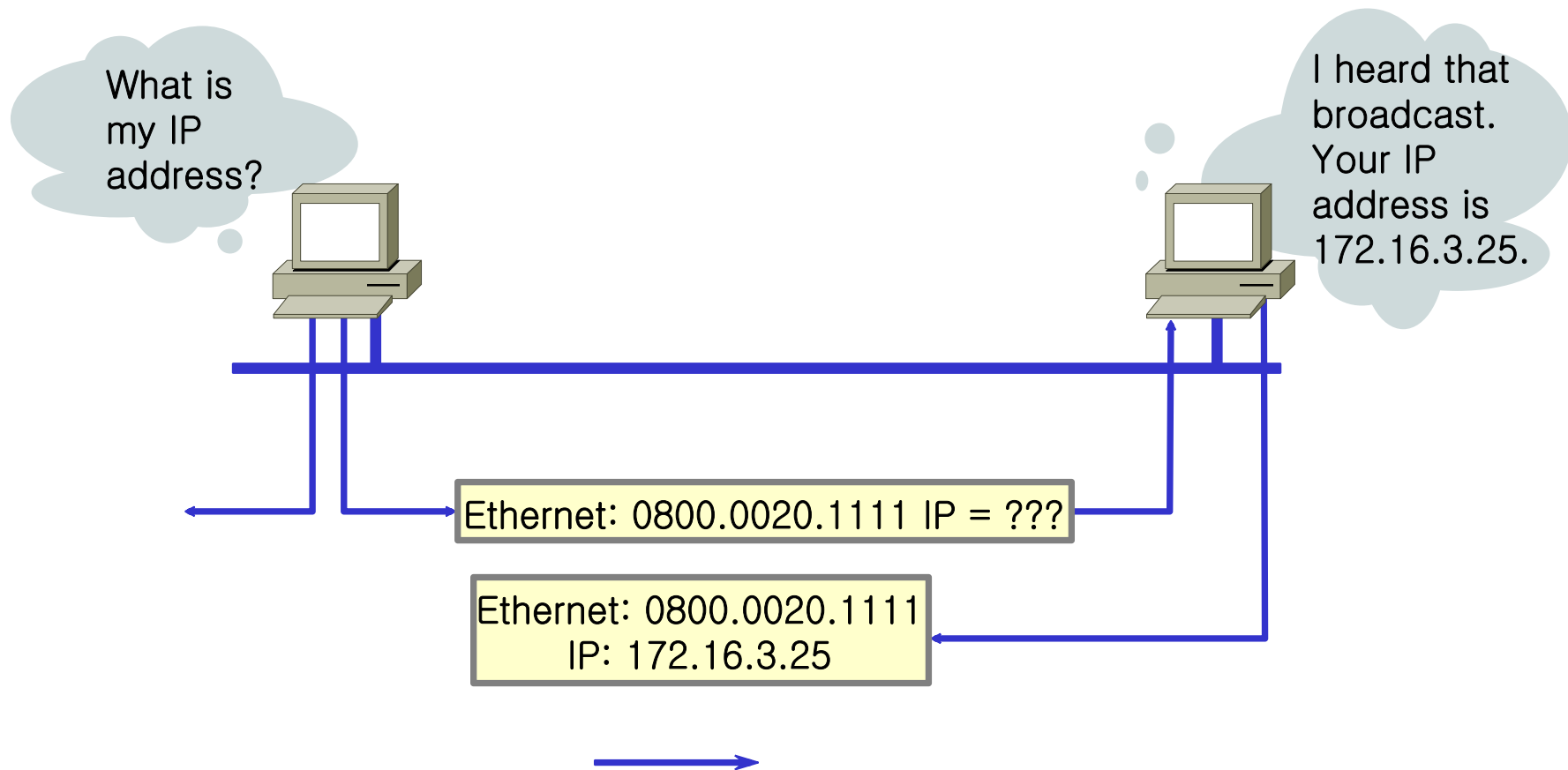




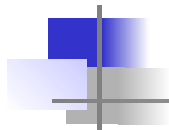
RARP(Reverse ARP) Protocol

- 디스크를 가지고 있지 않은 호스트가 자신의 IP 주소를 서버로부터 얻어내기 위해서는 RARP (Reverse Address Resolution Protocol)라는 TCP/IP 인터넷 프로토콜을 사용해야 한다. ARP와의 반대로 RARP 서버에 MAC Address 정보를 제시하여 IP Address를 요청한다. RARP 서버는 RARP 클라이언트의 하드웨어 주소와 IP 주소에 대한 Mapping DataBase를 보유한다.
- 송신 호스트는 RARP 메시지를 브로드캐스트한다. 네트워크상의 모든 호스트들이 이 요청을 받지만, RARP 서비스를 지원하도록 허가받은 호스트들만이 이 요청을 수행하고, 그 답신을 Unicast로 보낸다. RARP가 성공적으로 수행되기 위해서, 네트워크는 적어도 하나의 RARP 서버를 포함해야 한다.
- Operation 필드의 값 : 3(RARP Request), 4(RARP Response)
- RARP은 IP Address를 제공하나 Subnetmask나 Default Gateway 등의 정보를 제공하지 못하므로, 현재는 BootP나 DHCP를 주로 사용하며, 오래된 시스템간에서 사용되는 것을 종종 볼 수 있다. RARP Client는 ICMP Address Mask 요청 (ICMP Type 17, Code 0)을 통해 동일 네트워크 상의 라우터로부터 Subnet Mask정보를 얻고, ICMP Router Solicitation(ICMP Type 10, Code 0)을 통해 Default Gateway에 대한 정보를 얻게 할 수 있다.

RARP(Reverse ARP)



- Map Ethernet = IP
- ARP와 RARP는 데이터링크 계층과 직접 관여가 됨

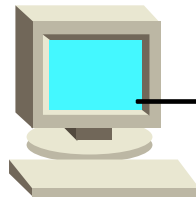


ICMP(Internet Control Message Protocol)

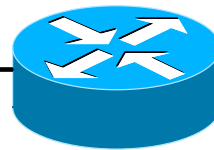
- 인터넷상의 라우터 및 호스트가 전송상의 에러를 송신 노드에 보고하고, 노드간 통신에 있어 제어를 위한 메시지를 보고하게 할 목적으로 만들어진 프로토콜을 Internet Control Message Protocol(ICMP)라고 한다. Error Reporting Message와 Query Message로 나눌 수 있다.
- IP 데이터그램이 목적지로 전달되는 것을 방해하는 문제가 발생시에 송신지에 해당 메시지를 전달하여, 특정문제를 피할 수 있도록 한다(Error Reporting).ICMP는 네트워크의 일반적인 정보를 교환하거나 네트워크의 상태를 조사하는데 사용될 수도 있다(Query). 예를 들어 ping 프로그램은 대상 호스트의 Alive 상태를 알아보기 위해 ICMP 프로토콜을 사용하는 프로그램이다.
- ICMP Message는 IP Datagram의 데이터에 실려 전송되며 Protocol ID가 1번으로 어떤 시스템에서 프로토콜이 1로 표시된 데이터그램을 수신하면 시스템은 이 데이터를 ICMP에 전달하게 된다.
- 다른 모든 전송과 같이, ICMP 메시지는 IP 데이터그램의 데이터부분에 실려 인터넷을 통해 전송된다. 따라서 ICMP Message 자체도 유실 될 수 있다.ICMP 메시지 전송관련 오류메시지는 생성되지 않는다.ICMP는 오류를 보고할 뿐 수정하지 않는다. 오류수정은 TCP등 상위프로토콜이 담당한다.

Network Unreachable

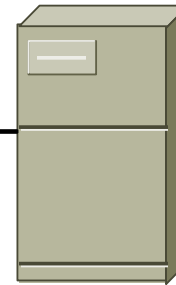
192.168.39.10 으로 전송되는 패킷



Bhkang
192.168.10.1



ROUTER
192.168.10.254
192.168.20.254



Server
192.168.20.1

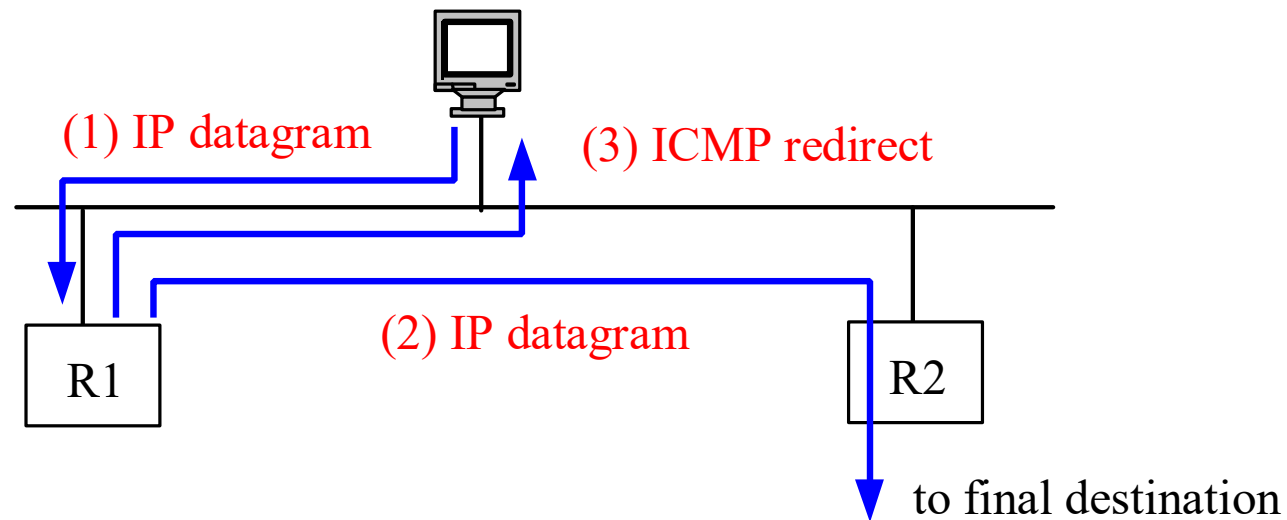


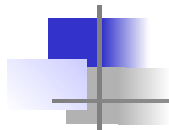
ICMP: Network Unreachable

- Destination Unreachable (Type 3, Code 0-15)
 - ✓ net/host/protocol/port가 unreachable 하는 등, 라우터가 데이터그램을 전송 할 수 없을 때 발생된다.

ICMP 경로 재지정

- ICMP 경로 재지정 (Type 5, Code 0)
 - ✓ 동일 서브넷 상에 두 개 이상의 라우터를 둔 경우, 통상 Default Gateway를 하나로 설정하는데 Default Gateway가 데이터그램을 받아 본 결과 다른 쪽의 라우터를 경유해서 나가야 하는 데이터그램인 경우, 다른 라우터로 데이터그램을 전송하고, ICMP가 경로 재지정을 요구하는 메시지를 발신호스트로 보낸다. 호스트는 이 메시지를 받아, 라우팅 테이블을 갱신한다. 일부 TCP/IP 구현은 ICMP 경로 재지정을 무시한다.



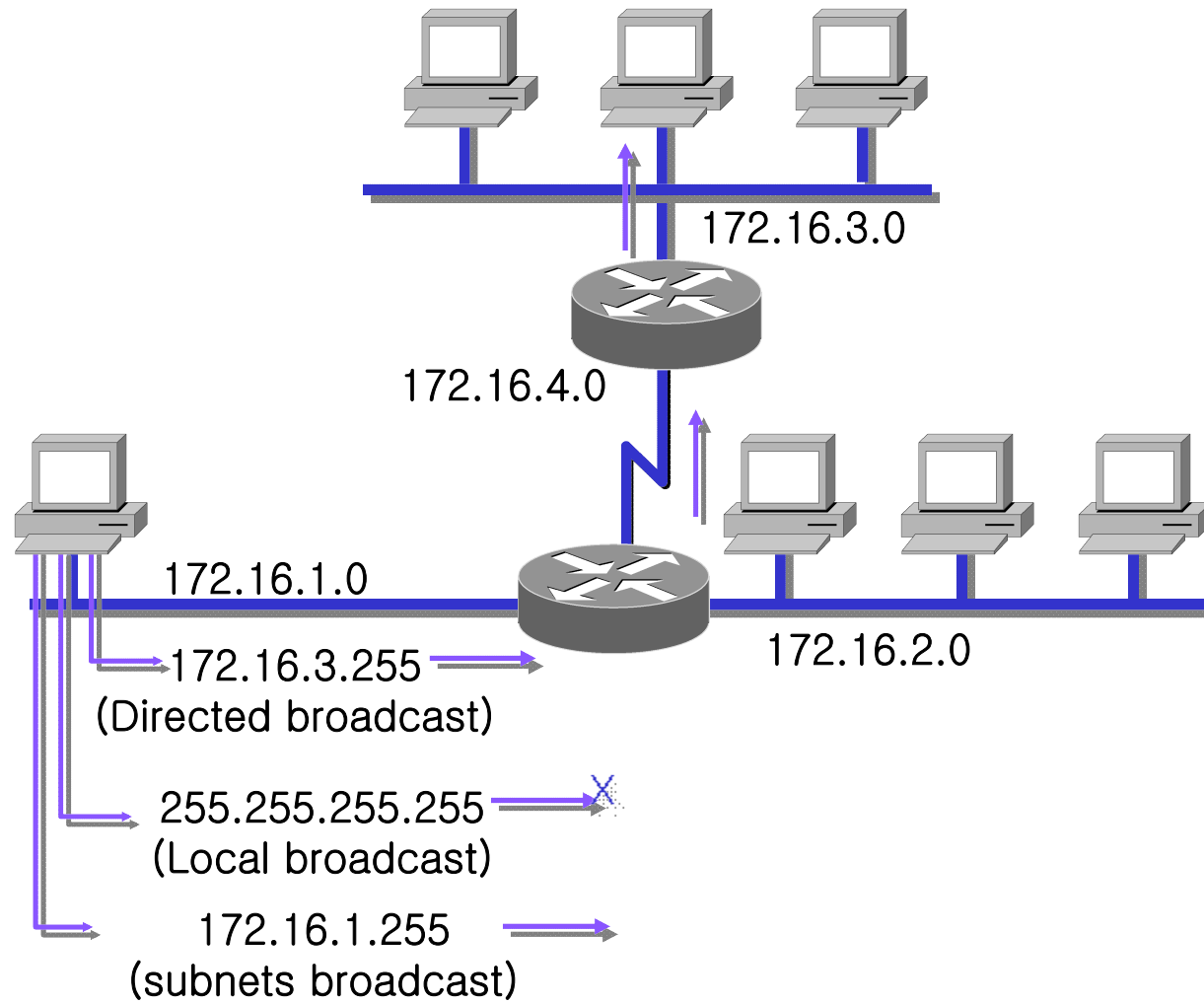


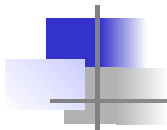
Multicast & IGMP

Unicast, Broadcast, Multicast

- **Unicast** : 하나의 호스트를 Destination으로 한다. Ethernet Frame Header의 DA가 하나의 MAC Address를 나타낸다. (예. 00-50-04-F2-A7-3B) Destination IP Address가 특정 IP Address이다. (예. 150.21.32.250)
- **Broadcast** : 모든 호스트가 Destination이다. Ethernet Frame Header의 DA가 모든 MAC Address를 나타낸다. (FF-FF-FF-FF-FF-FF) Destination IP Address가 Broadcast IP Address이다. (예. 150.21.255.255 또는 255.255.255.255)
- **Multicast** : 멀티캐스트 그룹에 속하는 호스트가 Destination이다. Ethernet Frame Header의 DA가 그룹 MAC Address를 나타낸다. Destination IP Address가 Multicast IP Address이다.

Broadcast Address



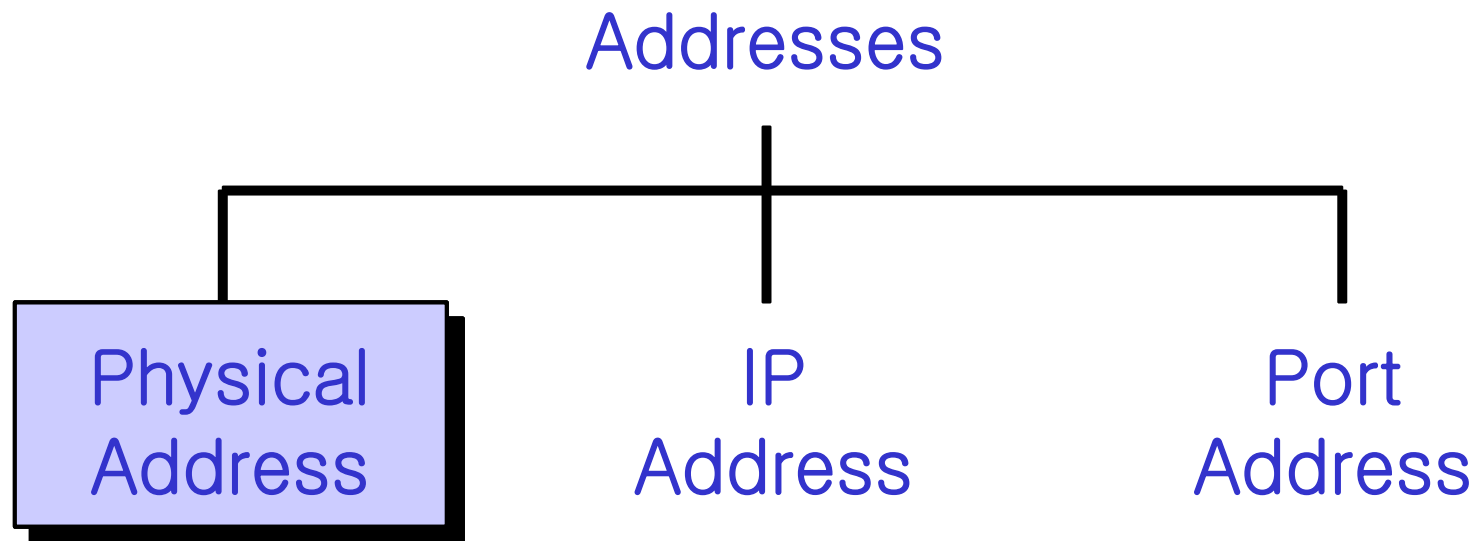


Muticast Address

- 하나의 프레임을 발행하여, 복수의 목적지로 전송하되, 브로드캐스트의 경우처럼 불필요한 시스템부하를 유발시키지 않는다. Unicast의 경우, 여러 개의 호스트에 동일한 프레임을 전달하려면 호스트 수만큼의 프레임을 발행해야 한다.
- 화상회의, VOD(Video On Demand)등의 경우에 사용할 수 있으며 UDP를 사용한다. TCP를 사용한다면 여러 번의 Unicast로 전송해야 한다.
- Multicast Group Ethernet Address
 - ✓ 01:00:5e:00:00:00 – 01:00:5e:7f:ff:ff
 - ✓ 01:00:5e는 동일하다.(상위 28Bit는 동일한 값을 사용한다.)
 - ✓ 01:00:5e + 그룹 Address의 하위 23bit를 Octet 단위로 16진수 값으로 변환한 값으로 산출된다.
- IP주소의 마지막 23비트가 단순히 01:00:5e:00:00:00 이더넷 그룹 주소 블록으로 복사된다.
- 224.128.64.32와 224.0.64.32는 01:00:5e:00:40:20으로 동일한 이더넷 주소를 갖게 된다. 이 경우, IP Level에서 구분될 것이다.

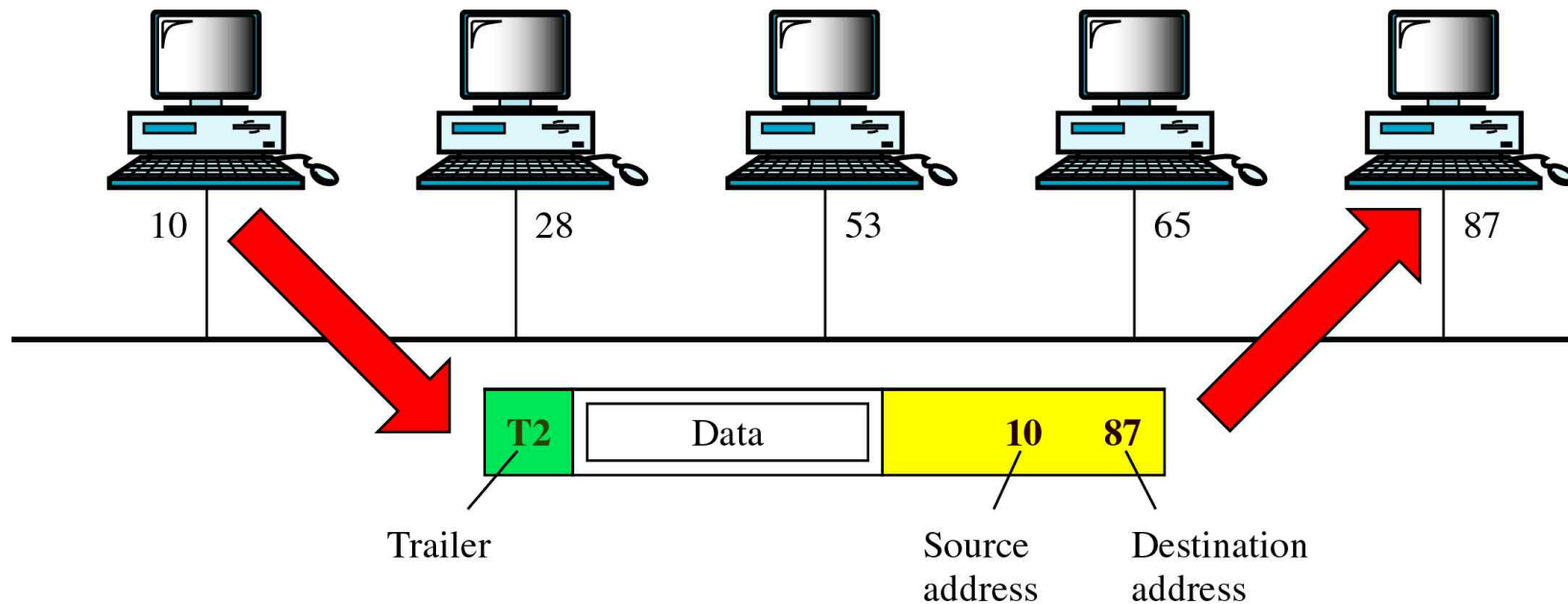
주소 지정

TCP/IP에서 사용하는 주소



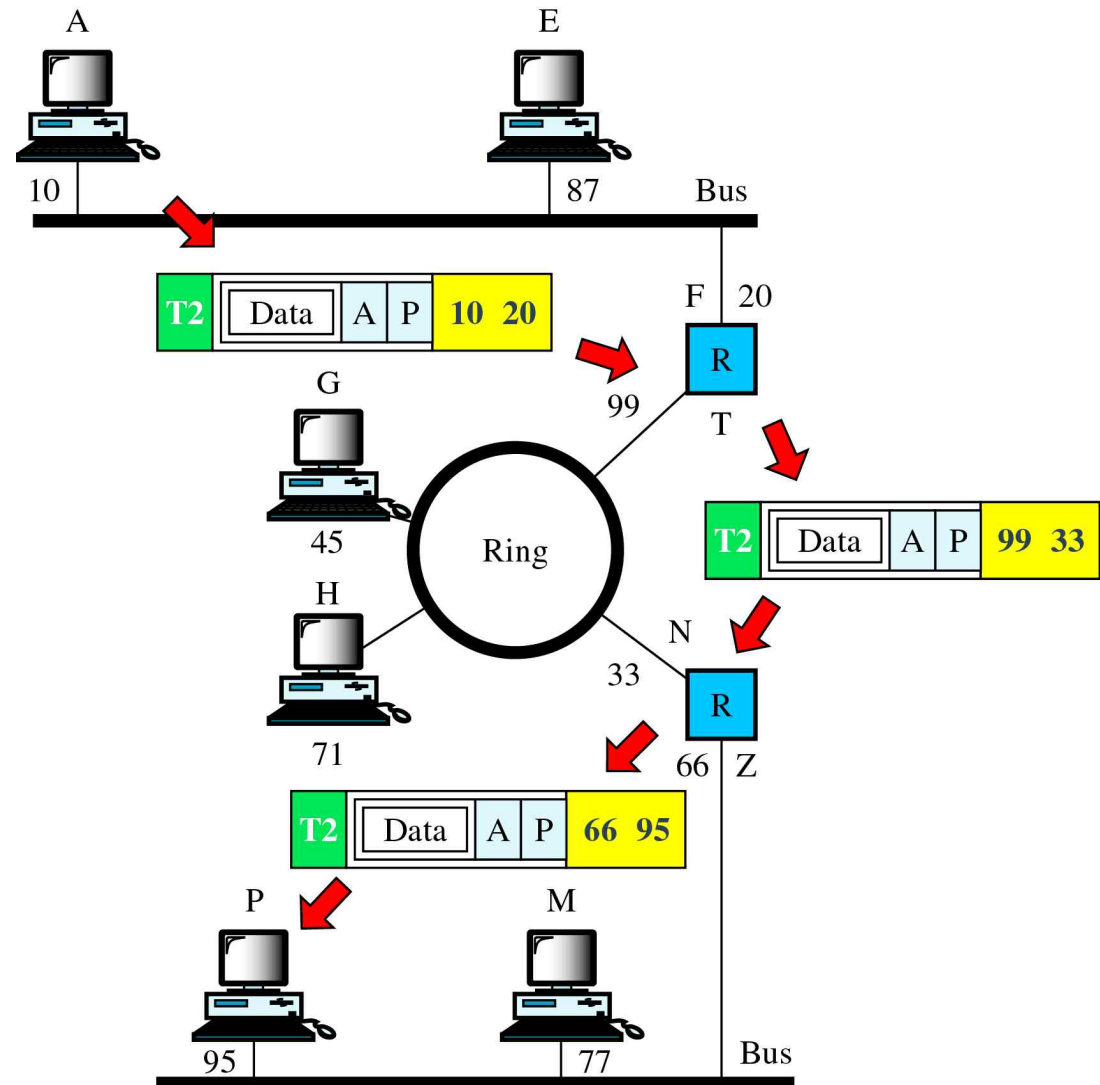
물리 주소(Physical Address)

- 링크 주소라고도 함
- LAN이나 WAN에서 정의된 노드의 주소이다.
- 이 주소의 크기와 형식은 네트워크에 의존하기 때문에 매우 다양함
예 - 이더넷 : 6바이트의 물리주소
- 대부분의 네트워크는 물리주소로 unicast, multicast, broadcast를 모두 지원하나 지원하지 않는 네트워크도 있다.



인터넷 주소(IP Address)

- 기존의 물리적인 네트워크와는 달리 독립적인 전 세계적인 통신 서비스를 위해 필요하다.
- 각 호스트를 유일하게 식별할 수 있는 전 세계적인 주소 지정 시스템
- 32비트 주소 체계 사용
- 인터넷 주소는 유니캐스트, 멀티캐스트, 브로드캐스트가 될 수 있다.



포트 주소(Port Address)

- 데이터를 발신지에서 목적지 호스트까지 전송하기 위해서는 물리 주소와 IP주소가 필요하다.
- 그러나 목적지 호스트에 도착하는 것이 최종 목표가 아니다.
- 단지 하나의 컴퓨터에 다른 컴퓨터로 데이터를 전송하는 시스템은 완전하지 못하다.
- 인터넷의 최종 목적은 한 프로세스가 다른 프로세스와 통신할 수 있도록 하는 것이다.
- TCP/IP 구조에서 프로세스에 할당된 레이블을 포트 주소라고 한다.
- TCP/IP에서 포트 주소 길이는 16비트이다.

