

정보보호

-보안을 위한 네트워크이론-

컴퓨터공학과 장대희



경희대학교
KYUNG HEE UNIVERSITY



PWNJAB
@KYUNGHEE UNIVERSITY

01 Protocol

Concept of Protocol

■ Protocol

- The original meaning is ceremonial or protocol in diplomacy.
- Tom Marill defines it as "the process of communicating messages between computers and computers."



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

The three elements of a protocol

■ Syntax

- Data structure or format

■ Semantics

- Predetermined rules established to enable understanding of the meaning of each part of the transmitted data.
- Including error control, synchronization, and flow control, not only for the data itself but also for the interpretation of each part of the transmitted data.

■ Timing

- Defining what data will be sent and how quickly it will be sent.

Functions of a protocol

■ Addressing

- Required when two entities from different systems communicate with each other.

■ Sequence Control

- Specifies the order in which protocol data units are sent during transmission.
- Used only in connection-oriented communication.

■ Fragmentation & Reassembly

- When transmitting large files, it's efficient to divide them into smaller units for transmission, then reassemble them at the receiving system.

Functions of a protocol

■ Encapsulation

- Appending control information to data.

■ Connection Control

- Performing control over connection establishment, data transmission, and connection termination.

■ Flow Control

- Functionality to regulate the amount or speed of data coming from the transmitting entity, preventing information loss due to differences in speed between the transmitting and receiving entities, among other factors.

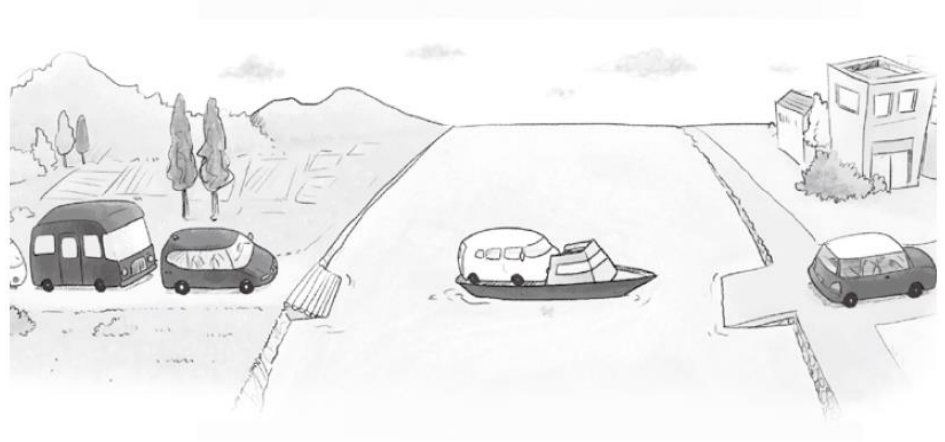


그림 2-2 캡슐화

Functions of a protocol

■ Error Control

- A technique for detecting errors in the Service Data Unit (SDU) or Protocol Control Information (PCI) when exchanging data between two entities. This is achieved by inspecting the sequence or requesting retransmission if not received within a specific timeframe.

■ Synchronization

- When transmitting data between two entities, each entity shares defined parameter values concurrently, such as specific timer values or window sizes.

■ Multiplexing

- A technique enabling multiple systems to communicate simultaneously over a single communication line.

■ Transmission Service

- A service that controls priority determination, service quality, security requirements, etc.

02 Network Layer Structure

The necessity of network layering

- In the early 1980s, ISO recognized the need for a standard network model that would allow interoperability between systems created by different vendors.
- In 1984, they published the OSI (Open Systems Interconnection) network model to address this need.

7 Layers of OSI

7계층	응용 프로그램 계층 (Application Layer)	응용 프로세스와 직접 관계해 일반적인 응용 서비스 수행
6계층	표현 계층 (Presentation Layer)	코드 간의 번역을 담당하는 계층. 사용자 시스템에서 데이터 구조를 통일해 응용 프로그램 계층에서 데이터 형식의 차이로 인해 발생하는 부담을 덜어줌
5계층	세션 계층 (Session Layer)	양 끝단의 응용 프로세스가 통신을 관리하는 방법 제공
4계층	전송 계층 (Transport Layer)	양 끝단의 사용자들이 신뢰성 있는 데이터를 주고받게 함으로써 상위 계층이 데이터 전달의 유효성이나 효율성을 신경 쓰지 않게 해줌
3계층	네트워크 계층 (Network Layer)	여러 개의 노드를 거칠 때마다 경로를 찾아주는 역할을 하는 계층. 다양한 길이의 데이터를 네트워크를 통해 전달하고, 전송 계층이 요구하는 서비스 품질(QoS)을 위해 기능적·절차적 수단 제공
2계층	데이터 링크 계층 (Data link Layer)	두 지점 간의 신뢰성 있는 전송을 보장하기 위한 계층. 16진수 12개로 구성된 MAC 주소 사용
1계층	물리 계층 (Physical Layer)	실제 장치를 연결하기 위한 전기적·물리적 세부 사항을 정의한 계층으로 랜선 등이 포함됨

그림 2-3 OSI 7계층



7 Layers of OSI

■ Physical Layer: Layer 1

- Defines the electrical and physical details required to connect actual devices. Devices in the physical layer include hubs or repeaters.

■ Data Link Layer: Layer 2

- Ensures reliable transmission between point-to-point connections. Requires error control and flow control based on CRC. The most well-known example is Ethernet. Devices in the data link layer include bridges or switches.

■ Network Layer: Layer 3

- Responsible for finding the path as data passes through multiple nodes. Performs routing, flow control, segmentation/desegmentation, and error control. Devices in the network layer include routers or switches (L3 switches).

7 Layers of OSI

■ Transport Layer: Layer 4

- Enables end-to-end users to exchange reliable data, allowing upper layers to transmit data without consideration for validity or efficiency of data delivery. TCP, a connection-oriented protocol, operates in the transport layer.

■ Session Layer: Layer 5

- Provides methods for managing communication between end-user applications. It handles communication modes such as duplex, half-duplex, and full-duplex, along with processes such as checkpointing, idle, termination, and restart. It is responsible for establishing and terminating TCP/IP sessions.

7 Layers of OSI

■ Presentation Layer: Layer 6

- Responsible for translating between codes used within the system, performing data compression, and encryption functions.

■ Application Layer: Layer 7

- Facilitates data exchange between users or applications. Provides services such as HTTP, FTP, terminal services, email programs, and directory services.

7 Layers of OSI

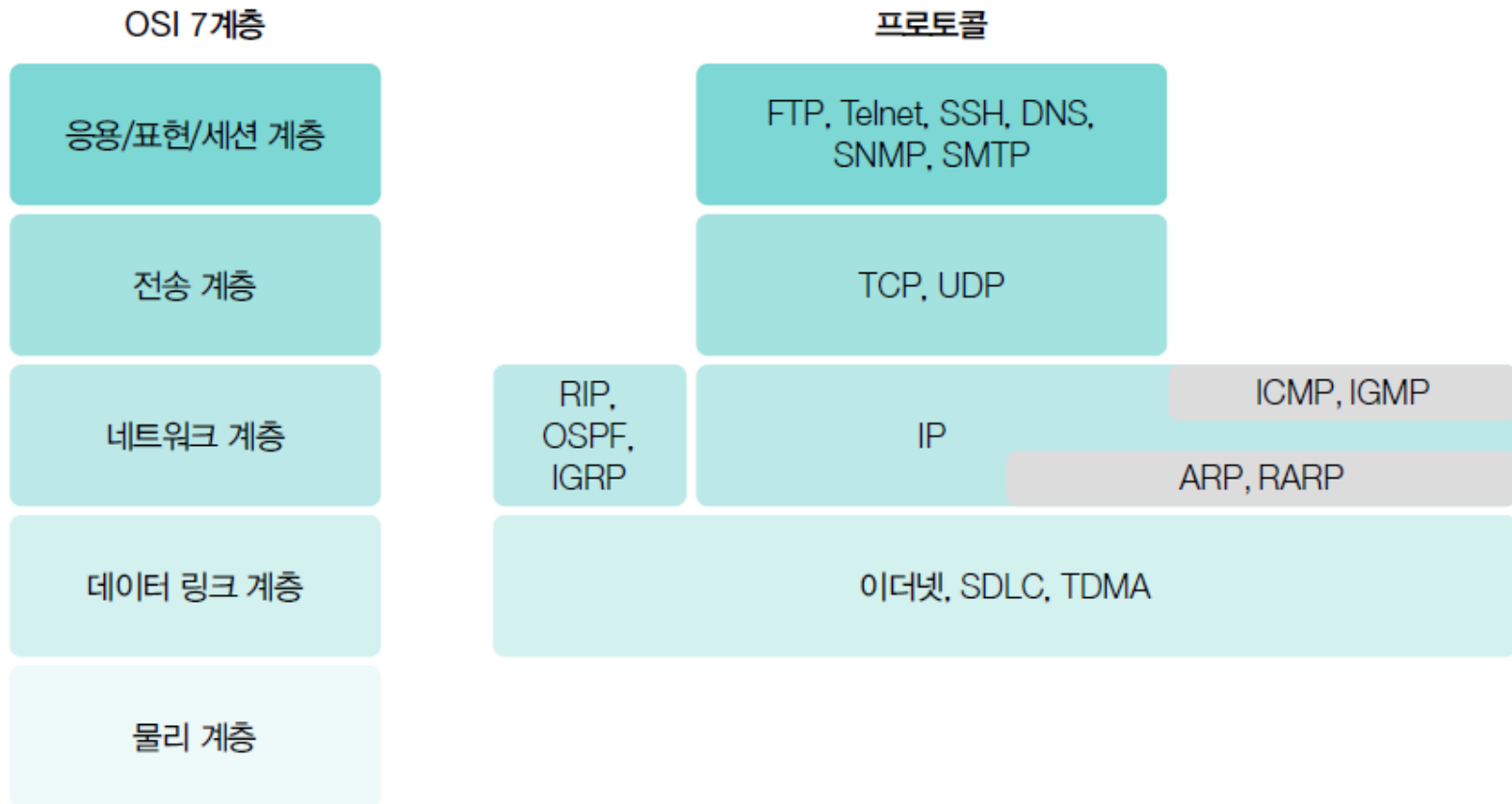


그림 2-4 OSI 7계층 구조에 대응하는 프로토콜

TCP/IP layer 4



NOTE OSI의 8계층

OSI 7계층 모델은 기술적이지 않은 문제나 이슈를 가리키는 농담에 이용되기도 한다. 예를 들어, 네트워크 기술자들이 '제8계층의 문제'라고 말하는 것은 실제로는 네트워크가 아닌 최종 사용자가 문제라는 것을 돌려서 말하는 것이다.

그림 2-5 OSI 7계층과 TCP/IP 4계층

03 Physical Layer

Physical Layer

■ Classification of cable wires

표 2-2 케이블 선의 분류

케이블 선	설명
UTPUnshielded Twisted Pair	제품 전선과 피복만으로 구성되어 있으며, 두 선 사이의 전자기 유도를 줄이기 위해 절연의 구리 선이 서로 꼬여 있다.
FTPShielded Twisted Pair Cable	알루미늄 은박이 네 가닥의 선을 감싸고 있으며, UTP보다 절연 기능이 탁월해 공장 배선용으로 많이 사용한다.
STPShielded Twisted Pair Cable	연선으로 된 전선 겉에 외부 피복 또는 차폐재가 추가된 케이블(실드 처리)이다. 차폐재는 접지 역할을 하므로 외부의 노이즈를 차단하거나 전기적 신호의 간섭에 탁월하다.

■ Connector

- Telephone line connector: RJ-11 (Registered Jack-11)
- LAN cable connector: RJ-45



(a) RJ-11



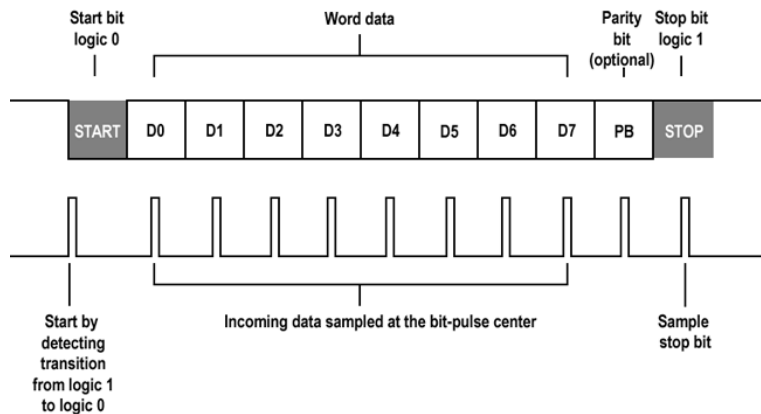
(b) RJ-45

그림 2-6 RJ-11과 RJ-45

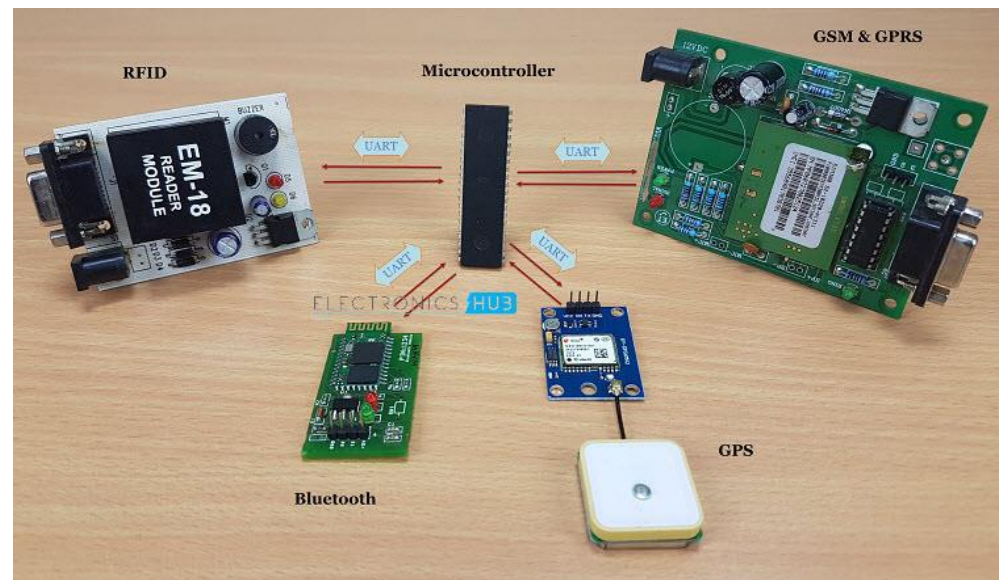
Physical Layer

Serial communication

- Communication at the hardware/radio frequency (HW/RF) level
- Existence of communication protocols such as modulation/demodulation of signals on antennas/wires



UART Signal Communication



Physical Layer

■ Repeater

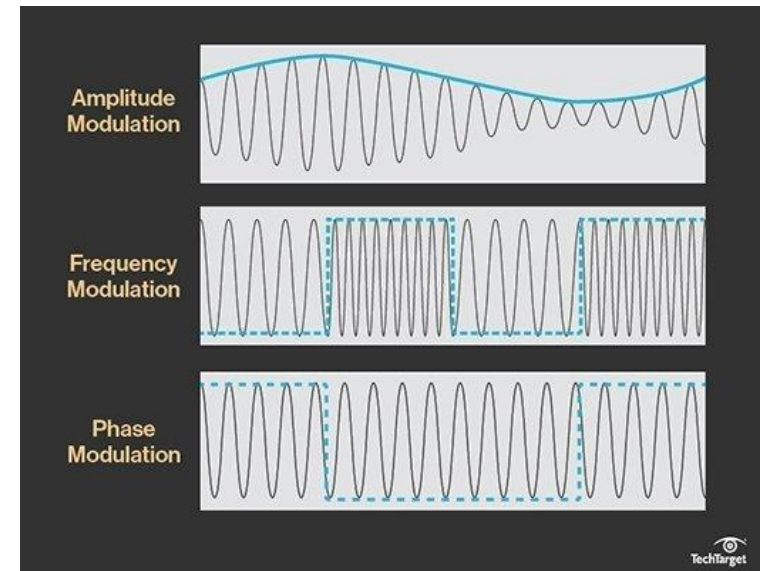
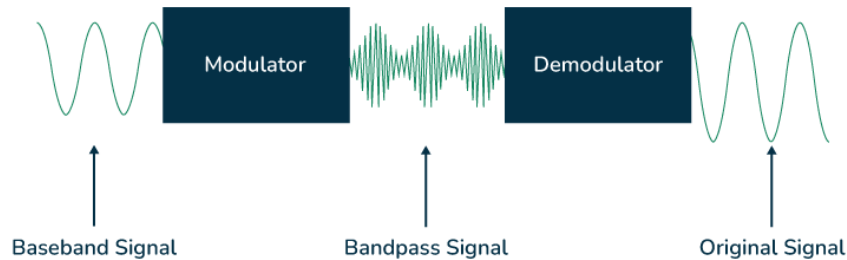
- A device used to extend a network
- Role: to amplify weakened signal strength
- Recently, repeaters have become a common feature in all network devices



그림 2-7 리피터

■ RF Communication

- Modulation / Demodulation



Physical Layer

Hub

- An earlier form of a switch; recent switches are switching hubs, while older ones are dummy hubs.
- Hubs and switches may appear and be used similarly, but they differ in whether they replicate packets equally to all destinations or only send them to the intended destination.

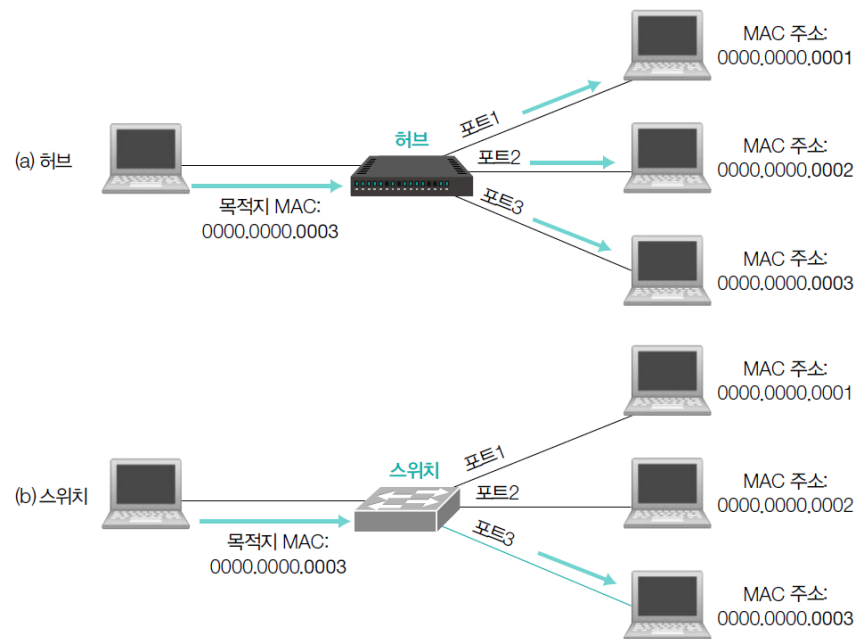


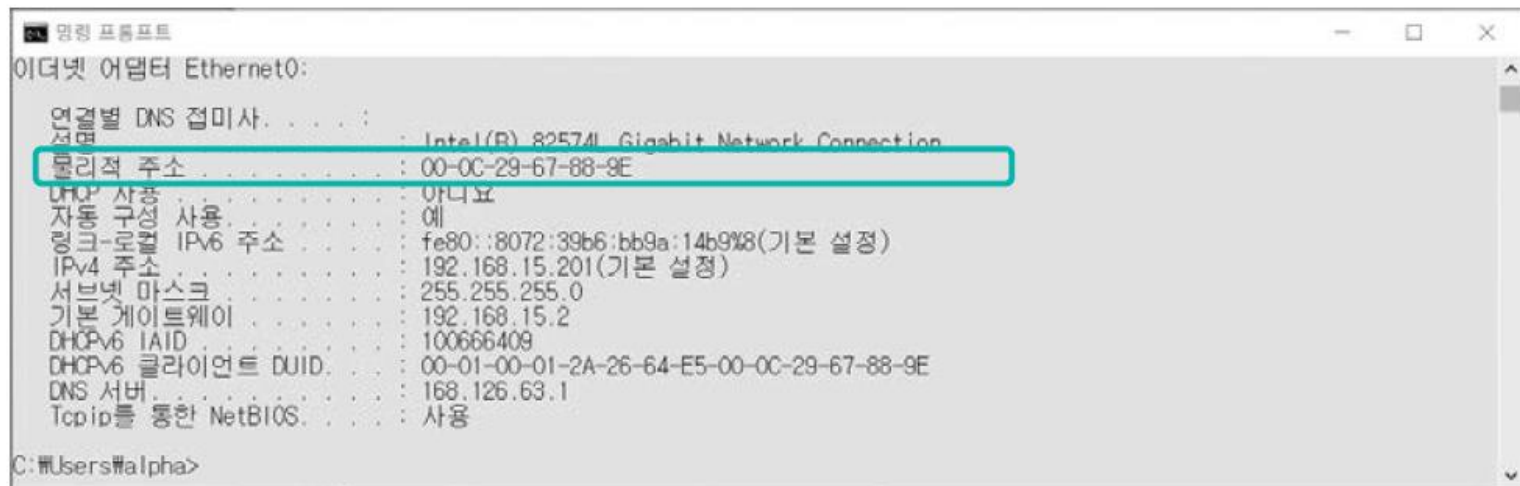
그림 2-8 허브와 스위치 비교

04 Data Link Layer

Data Link Layer

■ Layer 2: Data Link Layer (Data Link Layer)

- A layer that communicates solely based on hardware addresses (MAC addresses) of LAN cards or network devices.
- The MAC address of a network card can be checked by running the command "ipconfig /all" in the Windows command prompt.



```
명령 프롬프트
이더넷 어댑터 Ethernet0:

    연결별 DNS 접미사. . . . . : Intel(R) 82574L Gigabit Network Connection
    물리적 주소. . . . . : 00-0C-29-67-88-9E
    DHCP 사용. . . . . : 아니요
    자동 구성 사용. . . . . : 예
    링크-로컬 IPv6 주소. . . . . : fe80::8072:39b6:bb9a:14b9%8(기본 설정)
    IPv4 주소. . . . . : 192.168.15.201(기본 설정)
    서브넷 마스크. . . . . : 255.255.255.0
    기본 게이트웨이. . . . . : 192.168.15.2
    DHCPv6 IAID. . . . . : 100666409
    DHCPv6 클라이언트 DUID. . . . . : 00-01-00-01-2A-26-64-E5-00-0C-29-67-88-9E
    DNS 서버. . . . . : 168.126.63.1
    Tcpip를 통한 NetBIOS. . . . . : 사용

C:\Users\alpha>
```

그림 2-9 MAC 주소 확인

Data Link Layer and MAC Address

■ MAC address

- Consists of a total of 12 hexadecimal digits.
- The first 6 digits represent the company (OUI) that manufactured the network card, and the last 6 digits represent the host identifier, a kind of serial number assigned arbitrarily by each company.
- No two MAC addresses are the same.



그림 2-10 MAC 주소의 형태

Protocols of the Data Link Layer

■ Ethernet

- A Data Link Layer protocol developed by Xerox PARC in the 1970s.
- The minimum length of Ethernet packet is 64 bytes, maximum length is 1,518 bytes.
- Ethernet formed the basis of the IEEE 802.3 standard published in the 1980s.

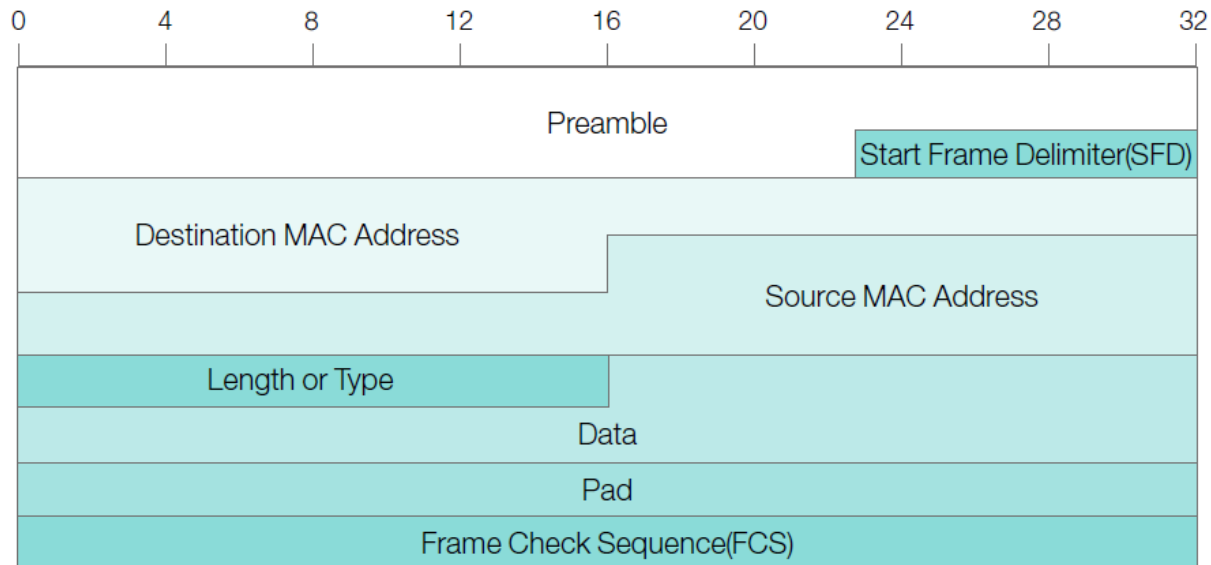


그림 2-11 이더넷의 패킷 구조

Protocols of the Data Link Layer

Ethernet

표 2-3 이더넷 패킷의 내용

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

Data Link Layer Devices

■ Bridge

- An early network device that connects LANs together.
- Operates at the Data Link Layer, copying data frames from one network to another along communication lines.

■ Switch

- Layer 2 Switch Refers to a switch that operates primarily at the Data Link Layer.
- L2 switches are a revolutionary solution to the problems of dummy hubs, which operate at very low speeds due to collisions between packets as the number of connected systems increases.



(a) 브리지



(b) 스위치

그림 2-13 브리지와 스위치

05 Network Layer

Network Layer Protocols

■ Layer 3: Network Layer

- Representative: Internet Protocol
- To communicate beyond LAN, IP addresses are used at the network layer.

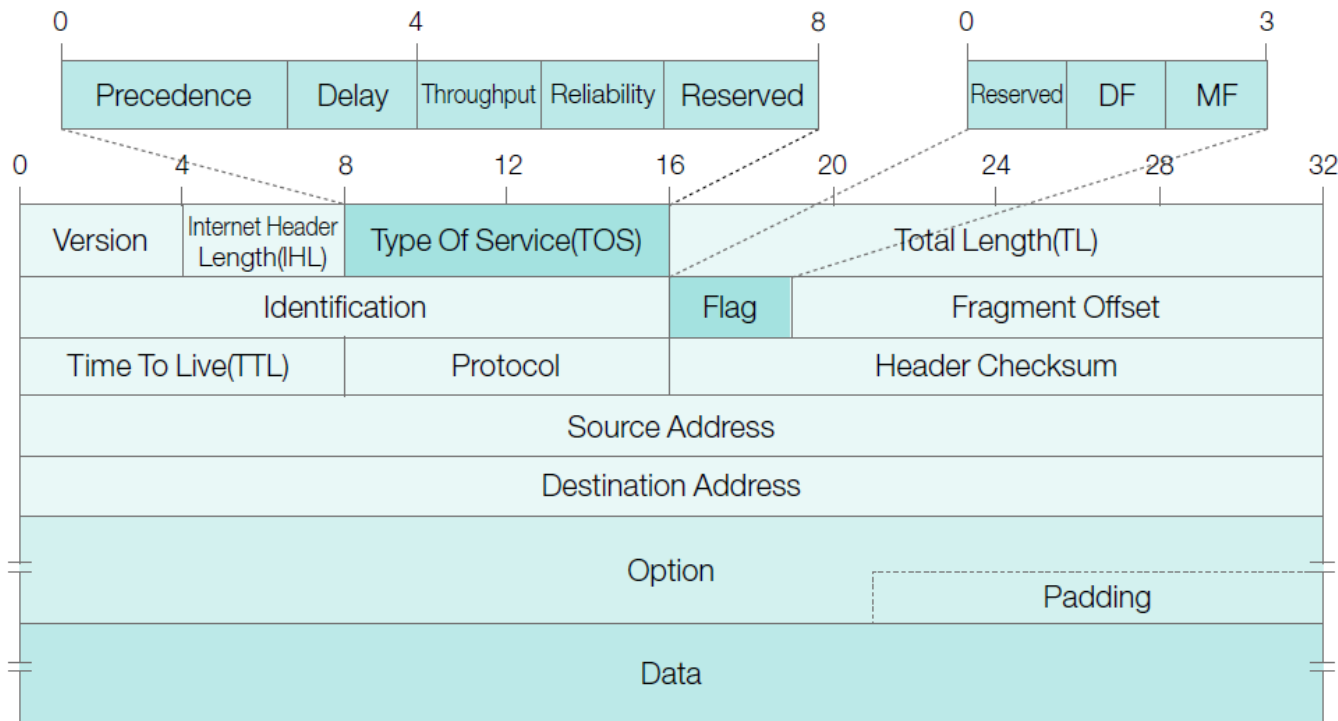


그림 2-15 IP 패킷 구조(IPv4)

Network Layer Protocols

■ IP(Internet Protocol)

표 2-4 IP 패킷의 내용

필드 이름	길이	내용
Version	4Bit	IP 프로토콜의 버전을 나타낸다. IPv4에서는 2진수로 0100(10진수로 4)이다.
IHL ^{Internet Header Length}	4Bit	IP 헤더의 길이로 이 필드 값에 4를 곱한 값이 실제 헤더의 바이트 길이이다.
TOS ^{Type of Service}	1Byte	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 ^{Total Length}	2Byte	헤더를 포함한 데이터그램의 전체 길이를 의미한다.
Identification	2Byte	데이터그램이 단편화 ^{Fragmentation} 될 때 모든 단편에 이 값이 복사되고, 단편화된 데이터그램이 생성될 때마다 1씩 증가하는 식별자다.
Flag	3Bit	단편화 여부와 단편화된 조각이 첫 번째 조각인지, 중간 혹은 마지막 조각인지를 알려주는 플래그다. <ul style="list-style-type: none">• 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.
Fragment Offset	13Bit	기존 데이터그램 안에서 단편의 상대적 위치를 의미하는 분할 오프셋이다.

Network Layer Protocols

TTL <small>Time To Live</small>	1Byte	라우팅 과정에서 라우터를 몇 개 이상 통과하면 해당 패킷을 버릴지를 입력한다. 라우터 하나를 지날 때마다 값이 1씩 줄어들고, 0이 되면 해당 패킷은 버려진다.
Protocol	1Byte	IP 계층의 서비스를 사용하는 상위 계층 프로토콜을 정의한다. <ul style="list-style-type: none"> • 1 : ICMP • 2 : IGMP • 6 : TCP • 17 : UDP
Header Checksum	2Byte	패킷 전달 중 발생할 수 있는 오류 검사를 위해 사용하는 것으로, 송신 측에서 체크섬을 계산해 전송한다.
Source Address	4Byte	송신 측의 IP 주소다.
Destination Address	4Byte	수신 측의 IP 주소다.
Option	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.

Network Layer Protocols

■ IP(Internet Protocol)

- 32-bit binary, separated by dots every 8 bits
- Classified into A, B, C, D, E classes, each consisting of network and host portions
- A, B, C classes are distinguished based on the binary digits at the beginning of the address



그림 2-16 IP 주소 클래스

Network Layer Protocols

■ IP(Internet Protocol)

표 2-5 네트워크 클래스의 구분

시작 주소	클래스	설명
0	A 클래스	<ul style="list-style-type: none">• 00000000번부터 01111111(127)번까지의 네트워크• A 클래스는 모두 $2^7(128)$개가 가능하고, 하나의 A 클래스 안에 $256^3(16,777,216)$개의 호스트가 존재할 수 있다.
10	B 클래스	<ul style="list-style-type: none">• 10000000(128)번부터 10111111(191)번까지의 네트워크• B 클래스는 $2^6 \times 256(16,384)$개가 가능하고, 하나의 B 클래스 안에 $256^2(66,536)$개의 호스트가 존재할 수 있다.
110	C 클래스	<ul style="list-style-type: none">• 11000000(192)번부터 11011111(223)번까지의 네트워크• C 클래스는 $2^5 \times 256^2(2,097,152)$개가 가능하고, 하나의 B 클래스 안에 256개의 호스트가 존재할 수 있다.
1110	D 클래스	<ul style="list-style-type: none">• 11100000(224)번부터 11101111(239)번까지의 네트워크• 멀티미디어 방송을 할 때 자동으로 부여된다.
E 클래스		<ul style="list-style-type: none">• 11110000(240)번부터 11111111(255)번까지의 네트워크• 테스트를 위한 주소 대역이며 사용하지 않는다.

Network Layer Protocols

■ IPv6(128bits)

- Introduced as an alternative to address the address exhaustion issue of IPv4 (32 bits)
- Comprises essential basic header and payload components

Ver	IHL	TOS	Length	
Identification			Flag	Fragment Offset
TTL		Protocol	Header Checksum	
Source Address				
Destination Address				
Option				Padding

□ IPv4에서 그대로 사용하거나 이름이 변경된 필드

■ 삭제 혹은 추가된 필드

그림 2-17 IPv4와 IPv6 헤더 비교

Ver	Traffic Class	Flow label	
Payload length		Next Header	Hop limit
Source Address			
Destination Address			

- 헤더의 길이가 고정되어 IHL 필드가 삭제되었다.
- TOS 필드가 삭제되고 이 기능을 Flow label 필드가 대신한다.
- TTL 필드가 Payload length 필드로 대체되었다.
- 기본 헤더에서 Identification, Flag, Fragment Offset 필드가 삭제되었다. 이 필드들은 단편화 확장 헤더에 포함되었다.
- TTL 필드를 Hop limit^{홉 제한} 필드로 부른다.
- Protocol 필드가 Next Header^{다음} 헤더 필드로 대체되었다.
- Header Checksum 필드가 삭제되었다. 체크섬은 상위 계층 프로토콜에서 계산한다.
- Options 필드를 확장 헤더로 구현한다.

Network Layer Protocols

■ ARP(Address Resolution Protocol) - Important

- A protocol that discovers the physical address (MAC) necessary for communication with a given IP address, to facilitate the transmission of data.
- It uses a method where a broadcast is sent on the selected medium, demanding a response from the host using a specific IP address.

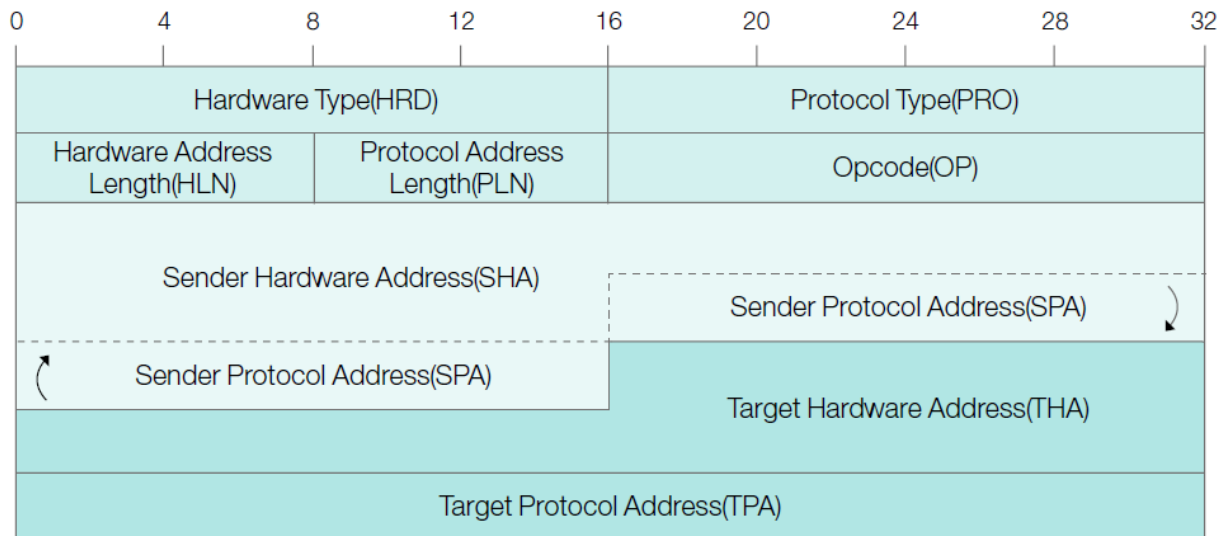


그림 2-18 ARP 패킷 구조

Network Layer Protocols

■ ARP(Address Resolution Protocol)

표 2-6 ARP 패킷의 내용

필드 이름	길이	내용
HRD ^{HaRdware Type}	2Byte	ARP 패킷이 사용되는 물리 계층의 네트워크 유형을 정의한다. <ul style="list-style-type: none"> • 1 : 이더넷(10Mb) • 6 : IEEE802 네트워크 • 15 : 프레임 릴레이 • 16 : ATM • 17 : HDLC • 18 : 광 채널 • 19 : ATM^{Asynchronous Transfer Mode} • 20 : 직렬 연결
PRO ^{Protocol Type}	2Byte	ARP를 위해 사용할 상위 계층 프로토콜의 종류를 지정한다. 일반적으로 IPv4를 사용하고, 그에 대한 값은 2048(0800 hex)이다.
HLN ^{Hardware Address Length}	1Byte	하드웨어 주소 값의 길이를 말하며 MAC 주소 값은 6이다.
PLN ^{Protocol address LeNgth}	1Byte	상위 계층 프로토콜의 주소 값의 길이로, IPv4의 주소 값 길이를 말한다. 당연히 4다.
OP	2Byte	Opcode이고, ARP 패킷 동작의 종류를 나타낸다. <ul style="list-style-type: none"> • 1 : ARP Request • 2 : ARP Reply • 3 : RARP Request • 4 : RARP Reply
SHA ^{Sender Hardware Address}	= HLN	패킷 송신자의 MAC 주소다.
SPA ^{Sender Protocol Address}	= PLN	패킷 송신자의 IP 주소다.
THA ^{Target Hardware Address}	= HLN	패킷 수신자의 MAC 주소다.
TPA ^{Target Protocol Address}	= PLN	패킷 수신자의 IP 주소다.

Network Layer Protocols

■ ICMP(Internet Control Message Protocol)

- A protocol that controls messages and notifies errors between host servers and internet gateways. A prominent tool associated with this protocol is ping.

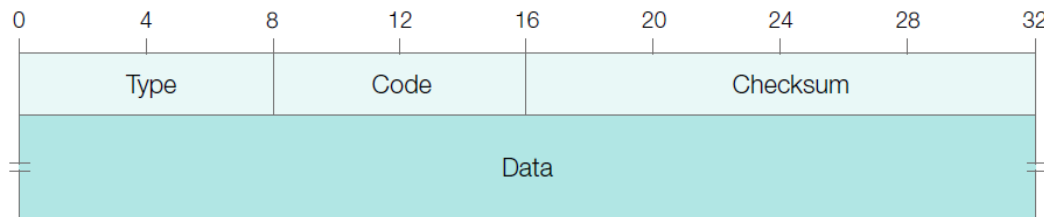


그림 2-19 ICMP 패킷 구조

표 2-7 ICMP 패킷의 내용

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

ICMP (Internet Control Message Protocol)

■ ICMP Echo Request/Reply Message

- Used to verify whether the transmitted packet from the sender has reached the intended node or router.

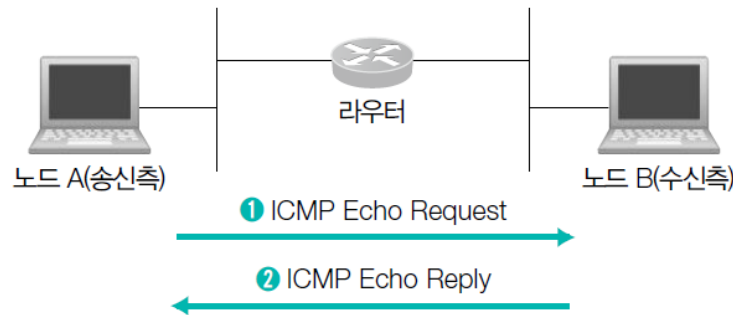


그림 2-20 ICMP Echo Request

■ ICMP Destination Unreachable Message

- Sent by a router when it cannot deliver a packet to the destination node.
- It includes information indicating the reason for the failure to reach the destination.

ICMP (Internet Control Message Protocol)

■ ICMP Redirect Message

- A message sent by a router to a transmitting node when it is determined that the current route set for that node is inappropriate, providing a new optimized route for that node.

■ ICMP Time Exceeded Message

- A message sent when a packet's Time to Live (TTL) value reaches zero as it is processed to prevent it from circulating indefinitely within the network.

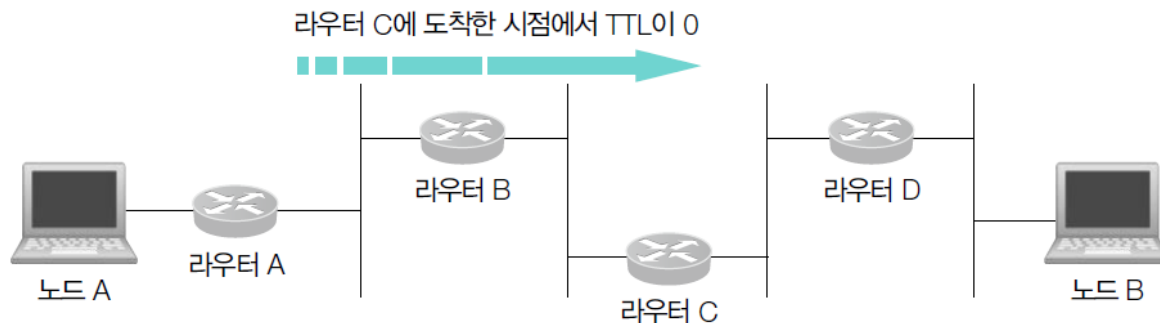


그림 2-21 ICMP Time Exceeded

Network Layer Equipment

■ Router

- A prominent device in a network, also referred to as a gateway.
- Connects two or more logically separated networks, blocking broadcasts from the local network to separate networks.
- Configures routing tables to find the optimal path for packet transmission and serves as a guide to send packets to their destination as quickly as possible.



(a) 소형 라우터



(b) 대형 라우터

그림 2-24 라우터

Routing Principles

■ Routing

- PC 등의 기본적 네트워크 단말기에도 라우팅 테이블이 존재함

라우팅 테이블에 지정한 주소 외의 모든 목적지 주소는
192.168.15.201 인터페이스를 통해 게이트웨이 192.168.15.2로 보내라는 의미

```
C:\Users\alpha>route PRINT

인터페이스 목록
8...00 0c 28 67 88 9e .....Intel(R) 82574L Gigabit Network Connection
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              192.168.15.2    192.168.15.201  281
127.0.0.0          255.0.0.0            127.0.0.1       127.0.0.1       331
127.0.0.1          255.255.255.255      127.0.0.1       127.0.0.1       331
127.255.255.255    255.255.255.255      127.0.0.1       127.0.0.1       331
192.168.15.0       255.255.255.0        192.168.15.201  192.168.15.201  281
192.168.15.201     255.255.255.255      192.168.15.201  192.168.15.201  281
192.168.15.255     255.255.255.255      192.168.15.201  192.168.15.201  281
224.0.0.0          240.0.0.0            127.0.0.1       127.0.0.1       331
224.0.0.0          240.0.0.0            192.168.15.201  192.168.15.201  281
255.255.255.255    255.255.255.255      127.0.0.1       127.0.0.1       331
255.255.255.255    255.255.255.255      192.168.15.201  192.168.15.201  281
```

그림 2-25 PC의 라우팅 테이블

255.255.255.0 의 마스크 (네트워크 마스크) 를 이해하려면?
32비트 IP 주소값과 네트워크 마스크 주소값을 AND 한 결과로 이해
255 -> 11111111 (2진수)
192.168.15.0 은 즉 하위 8비트를 상관하지 않는다는 의미

Routing Principles

■ Routing

- Tracing the route of ICMP packets to the destination starting with 200.200.200.200 using the `tracert` command.



```
명령 프롬프트 - tracert 200.200.200.200
C:\Users\alpha>tracert 200.200.200.200

최대 30홉 이상의 200.200.200.200(으)로 가는 경로 추적

 1      2 ms      1 ms      1 ms  192.168.15.2
 2     13 ms      8 ms      5 ms  192.168.1.1
 3      7 ms      *          *    222.96.18.254
 4      5 ms      3 ms      3 ms  112.189.155.181
 5      5 ms      6 ms      6 ms  112.189.145.5
 6      *          *          *    요청 시간이 만료되었습니다.
 7      *
```

그림 2-26 IP 주소 200.200.200.200에 대한 네트워크 경로 확인

Static Routing and Dynamic Routing

■ Static Routing

- Configuring specific paths for packets to travel with administrator privileges.
- In the case of network changes, the routing table needs to be manually updated.
- This method is preferred in situations where security is crucial.

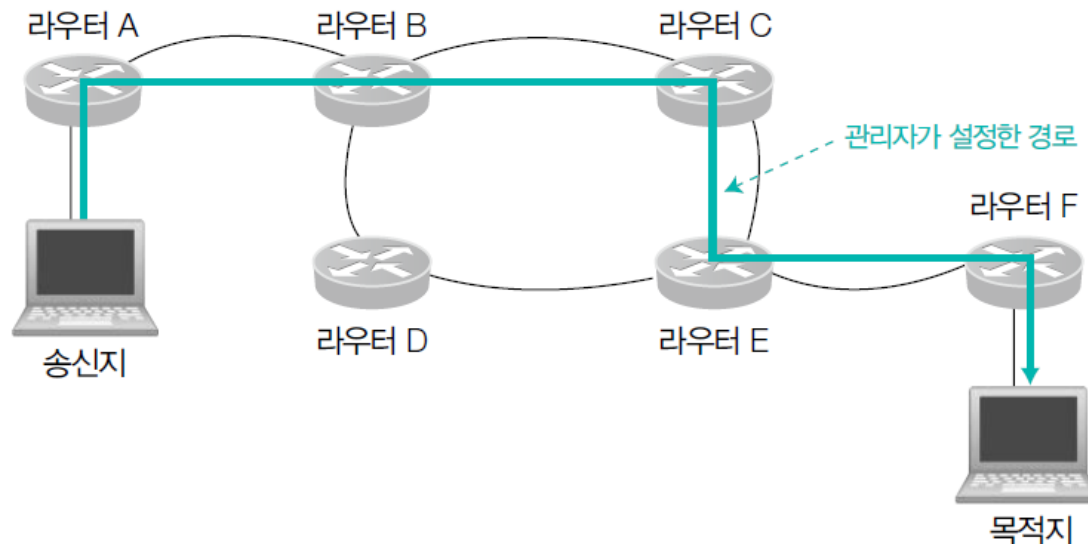


그림 2-28 정적 라우팅

Static Routing and Dynamic Routing

■ Dynamic Routing

- Routing where routers autonomously assess network connectivity and choose the optimal path for transmission.
- It automatically adapts to changes in network connectivity, resolving issues without manual intervention, even if the network topology changes.

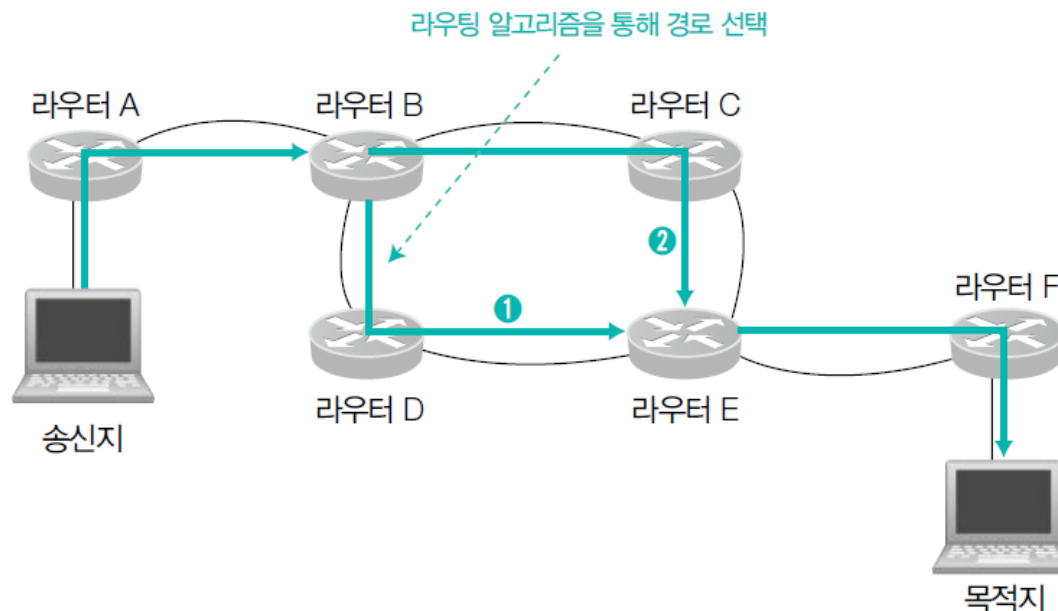


그림 2-29 동적 라우팅

06 Transport Layer

Transport Layer and Ports

Layer 4: Transport Layer

- The prominent protocol is TCP (Transmission Control Protocol). Ports, referred to as the addresses possessed by TCP, range from 0 to 65535 ($2^{16}-1$).

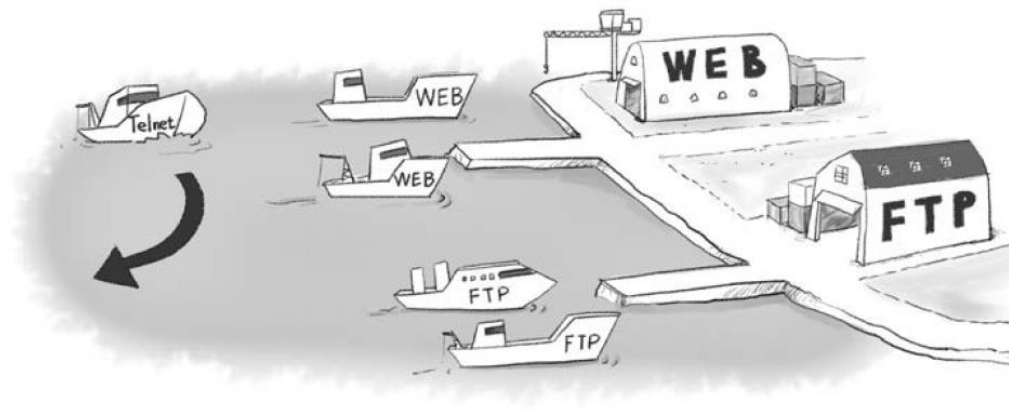


그림 2-30 포트별로 정해진 응용 프로그램

01001010101	출발지 포트	목적지 포트	출발지 IP	목적지 IP	출발지 MAC	목적지 MAC
← 세션 계층까지의 패킷 정보 →	← 전송 계층의 패킷 정보 →		← 네트워크 계층의 패킷 정보 →		← 데이터 링크 계층의 패킷 정보 →	

Port (중요 기본 개념)

- Ports in the range of 0 to 1023 (1,024) are known as Well-Known Ports (usually, port 0 is not used).

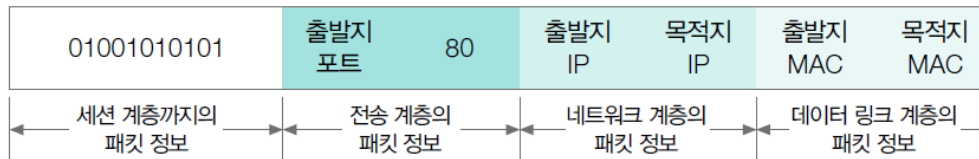
표 2-9 주요 포트와 서비스

포트	서비스	설명			
20	FTP Data	<ul style="list-style-type: none"> File Transfer Protocol-Datagram FTP 연결 시 실제로 데이터를 전송한다. 			
21	FTP	<ul style="list-style-type: none"> File Transfer Protocol-Control FTP 연결 시 인증과 제어를 한다. 			
23	Telnet	<ul style="list-style-type: none"> 텔넷 서비스로, 원격지 서버의 실행 창을 얻어낸다. 	80	HTTP	<ul style="list-style-type: none"> Hyper Text Transfer Protocol 웹 서비스를 제공한다.
25	SMTP	<ul style="list-style-type: none"> Simple Message Transfer Protocol 메일을 보낼 때 사용한다. 	110	POP3	<ul style="list-style-type: none"> Post Office Protocol 메일 서버로 전송된 메일을 읽을 때 사용한다.
53	DNS	<ul style="list-style-type: none"> Domain Name Service 이름을 해석하는 데 사용한다. 	111	RPC	<ul style="list-style-type: none"> Sun의 Remote Procedure Call 원격에서 서버의 프로세스를 실행할 수 있게 한다.
69	TFTP	<ul style="list-style-type: none"> Trivial File Transfer Protocol 인증이 존재하지 않는 단순한 파일 전송에 사용한다. 	138	NetBIOS	<ul style="list-style-type: none"> Network Basic Input Output Service 윈도우에서 파일을 공유할 수 있게 한다.
			143	IMAP	<ul style="list-style-type: none"> Internet Message Access Protocol POP3와 기본적으로 같지만 메일이 확인된 후에도 서버에 남는다는 것이 다르다.
			161	SNMP	<ul style="list-style-type: none"> Simple Network Management Protocol 네트워크 관리와 모니터링을 위해 사용한다.

Port

■ Packet Structure and Example

- The source port is typically assigned an arbitrary port between 1024 and 65535 for each application.
- When a client connects to a web server, the packet structure is as follows (the service port is usually 80)
- System-assigned source packet structure with an arbitrary port.



TCP (Transmission Control Protocol)

■ TCP(Transmission Control Protocol)

- A connection-oriented protocol that is essential for communication along with IP, serving as the fundamental protocol.

■ Characteristics of TCP

- Connection Oriented (3-way handshake)
- Sequence Numbering
- High reliability
- Virtual circuit connection method
- Establishment and termination of connections
- Data checksum
- Timeout and retransmission
- Data flow control

TCP (Transmission Control Protocol)

TCP (Transmission Control Protocol) packet structure

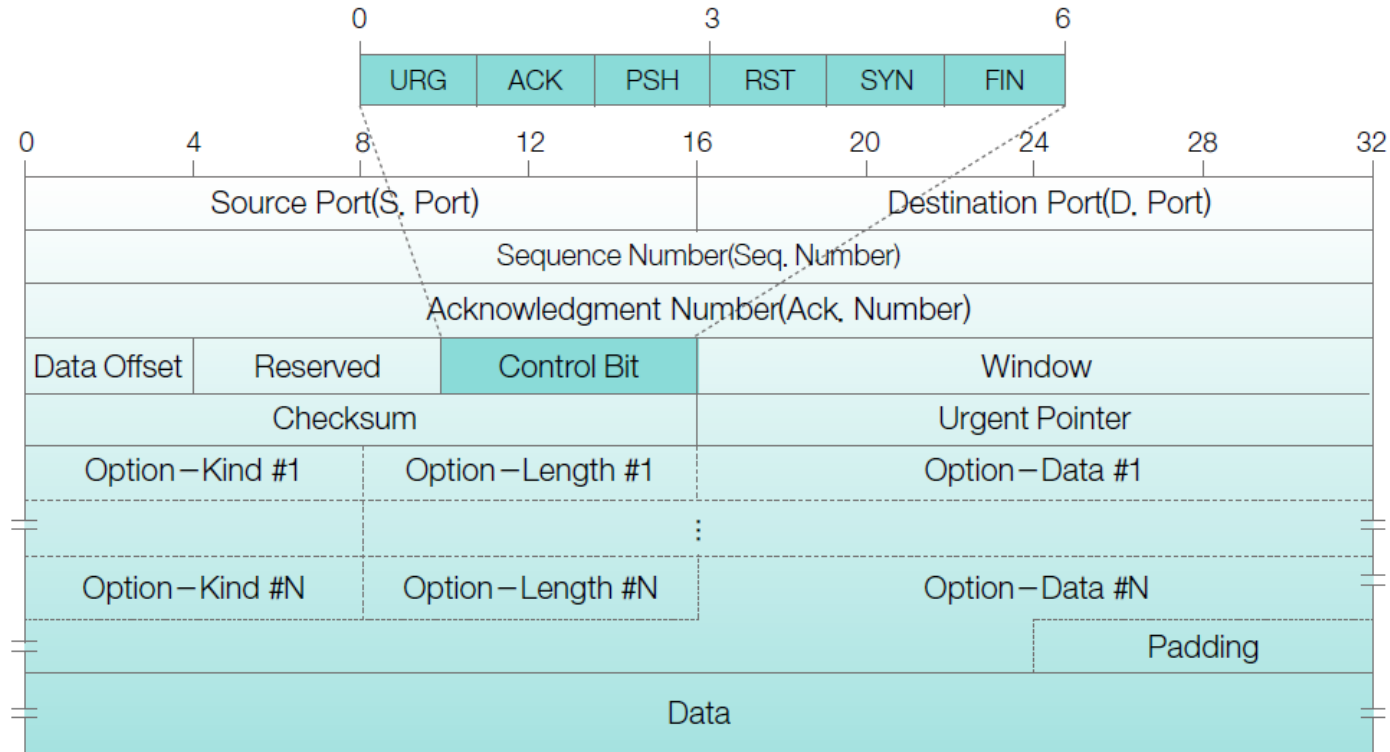


그림 2-31 TCP 패킷의 헤더 구조

TCP (Transmission Control Protocol)

표 2-10 TCP 패킷의 헤더 내용

필드 이름	길이	내용
S. Port ^{Source Port}	2Byte	패킷의 출발지 포트 번호를 가리키며 0~65535 값 중 하나다.
D. Port ^{Destination Port}	2Byte	패킷의 목적지 포트 번호다.
Seq. Number Sequence Number	4Byte	패킷의 순서 값이다.
Ack. Number Acknowledgment Number	4Byte	통신 상대의 패킷 순서 값이다.
Data Offset	4Bit	TCP 패킷 헤더의 길이를 나타내는데, 32Bit(4Byte)가 몇 행인지를 가리킨다. 최 솟값은 5다.
Reserved	6Bit	나중에 필요할 때 사용하려고 남겨둔 공간이다.
Control Bit	6Bit	6개의 비트는 각각 다음과 같이 TCP 패킷의 종류와 특성을 가리킨다. 예를 들어, ACK와 FIN 값이 1이면 Control Bit는 010001이 될 것이다. <ul style="list-style-type: none"> • URG^{URGent}: 1이면 헤더의 마지막 필드인 긴급 포인터의 내용을 실행 • ACK^{ACKnowledgment}: 1이면 확인 번호 필드가 유효 • PSH^{PSH}: 1이면 송신자에게 높은 처리율을 요구 • RST^{REseT}: 1이면 TCP 연결을 다시 설정 • SYN^{SYNchronize}: 1이면 연결 요청과 설정, 확인 응답에서 순서 번호를 동기화 • FIN^{FINish}: 1이면 TCP 연결을 종료

TCP (Transmission Control Protocol)

Window	2Byte	<p>TCP에서는 흐름 제어를 할 때 슬라이딩 윈도우와 혼잡 윈도우 방법을 사용한다.</p> <ul style="list-style-type: none"> • 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 있도록 해준다. • 혼잡 윈도우^{Congestion Window}: 네트워크 혼잡 문제를 해결하기 위해 송신 시스템이 사용하는 방법이다. 네트워크 혼잡이 발견되면 보내는 데이터의 양을 조절해 줄이고 혼잡이 줄어들면 다시 원래 보내던 만큼 데이터 양을 늘린다.
Checksum	2Byte	데이터 오류 검출을 위한 값이다.
Urgent Pointer	2Byte	Control Bit가 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 32Bit가 안 되면 나머지 비트를 0으로 채운다.
Data	가변	전송하고자 하는 데이터를 저장한다.

TCP (Transmission Control Protocol)

■ Three-Way Handshaking

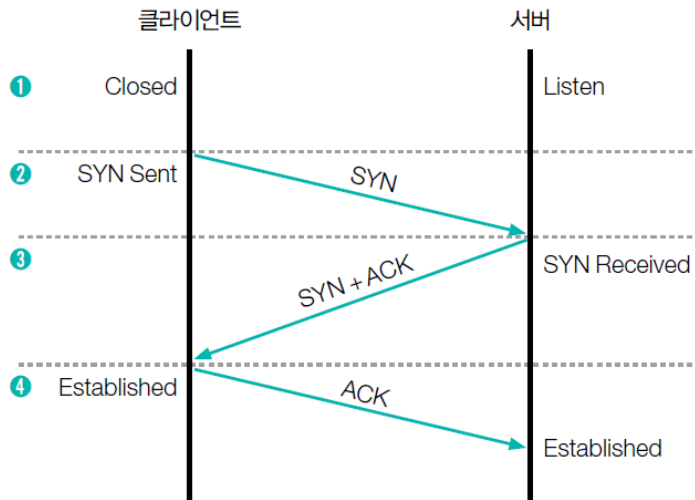


그림 2-32 TCP에서 연결 생성 과정

- 1 두 시스템이 통신을 하기 전에 클라이언트는 포트가 닫힌 Closed 상태이고, 서버는 해당 포트로 항상 서비스를 제공할 수 있는 Listen 상태다.
- 2 클라이언트가 처음 통신을 하려고 하면 임의의 포트 번호가 클라이언트 프로그램에 할당되고, 클라이언트는 서버에 연결하고 싶다는 의사 표시인 SYN Sent 상태가 된다.
- 3 클라이언트의 연결 요청을 받은 서버는 SYN Received 상태가 되고, 클라이언트에 연결을 해도 좋다는 의미로 SYN+ACK 패킷을 보낸다.
- 4 마지막으로 클라이언트는 연결 요청에 대한 서버의 응답을 확인했다는 표시로 ACK 패킷을 서버로 보낸다.

SYN: SYNchronize
ACK: ACKnowledge

TCP (Transmission Control Protocol)

■ Three-Way Handshaking

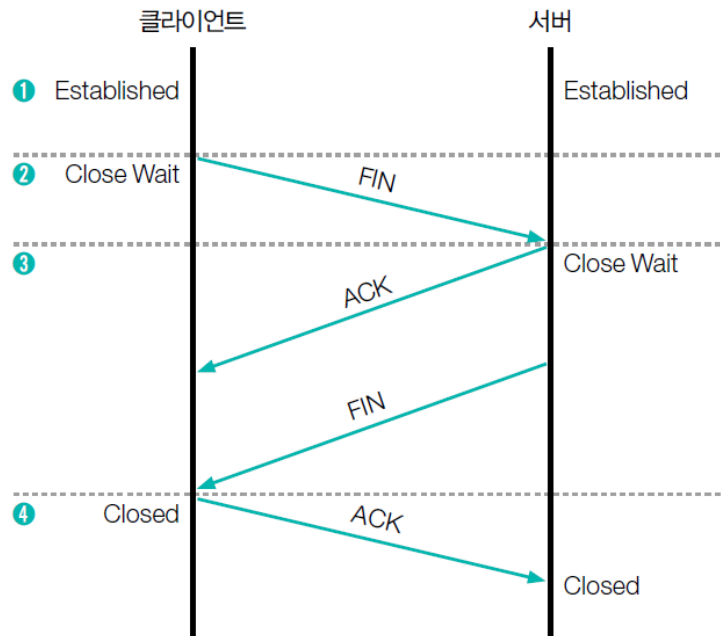


그림 2-33 TCP에서 연결 해제 과정

- 1 통신을 하는 동안에는 클라이언트와 서버 모두 Established 상태다.
- 2 통신을 끊으려는 클라이언트가 서버에 FIN^{FINish} 패킷을 보낸다. 이때 클라이언트는 Close Wait 상태가 된다(철수가 “영희야, 잘 자” 하는 과정이다).
- 3 서버는 클라이언트의 연결 종료 요청을 확인하고 응답으로 클라이언트에 ACK 패킷을 보낸다. 서버도 클라이언트의 연결을 종료하겠다는 의미로 FIN 패킷을 보내고 Close Wait 상태가 된다(영희가 “응, 너도 잘 자” 하는 과정이다).
- 4 클라이언트는 연결 종료 요청에 대한 서버의 응답을 확인했다는 표시로 ACK 패킷을 서버에 보낸다(철수가 “그래” 하고 전화를 끊는 과정이다).

SYN: SYNchronize
ACK: ACKnowledge
FIN: FINish

UDP (User Datagram Protocol)

■ UDP(User Datagram Protocol)

- A connectionless protocol that does not establish a connection before sending data.
- It does not confirm the receipt of responses from the other party, avoiding network overhead.
- However, it lacks the inherent reliability to ensure the integrity of received data.

■ Characteristics of UDP

- Connectionless
- Reduced network overhead
- Unreliable
- Some of the transmitted data may be lost.

UDP (User Datagram Protocol)

■ UDP (User Datagram Protocol) packet structure

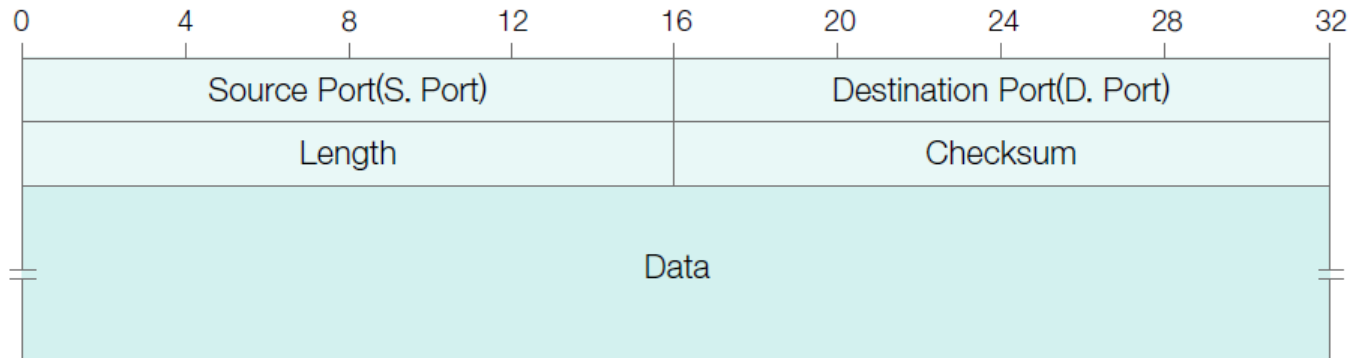


그림 2-34 UDP 패킷 구조

UDP (User Datagram Protocol)

■ UDP (User Datagram Protocol) packet content

표 2-11 UDP 패킷의 내용

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

07 Application Layer

Application Layer

■ Layer 7: Application Layer

- There are separate applications related to this layer, providing user interfaces for various protocols.

■ FTP(File Transfer Protocol, 20,21)

- The most fundamental protocol for file transfer, established as a standard in 1972 along with Telnet.
- Allows interactive communication between clients and servers.

■ Telnet(23)

- Establishes a TCP connection for users to log in to a remote server.
- It allows the terminal to operate as if it were directly manipulating the remote computer, as if it were right next to it.

Application Layer

■ SMTP(Simple Mail Transfer Protocol, 25)

- A mail service protocol.

■ DNS(Domain Name System, 53) - 중요

- A protocol that allows you to check IP addresses through domain name addresses.

■ TFTP(Trivial File Transfer Protocol, 69)

- A protocol for transferring files.
- It uses UDP packets and does not provide authentication.

■ HTTP(HyperText Transfer Protocol, 80) - 중요

- The most basic protocol used for the internet.

