# 네트워크에 대한 이해

# 01_프로토콜에 대한 이해

## ❖ 프로토콜의 3가지 요소

- 구문(Syntax) : 데이터의 구조나 포맷을 의미

**0101001010111111**

| 0101 | 00101011 | 1111 |
|---|---|---|
| 목적지 주소 | 데이터 | 흐름제어(Flow control) |

- 의미(Semantics) : 전송되는 데이터의 각 부분이 무엇을 뜻하는지를 알 수 있게 미리 정해둔 규칙(데이터 자체뿐만 아니라 오류 제어, 동기 제어, 흐름 제어를 포함)

| 0101 | 00101011 | 1111 |
|---|---|---|
| 5번 방 | 짜장면 | 최대한 빨리 |

5번방에 짜장면 최대한 빨리

- 순서(Timing) : 어떤 데이터를 보낼 것인지와 얼마나 빠르게 데이터를 보낼 것인지 정의

# 01_프로토콜에 대한 이해

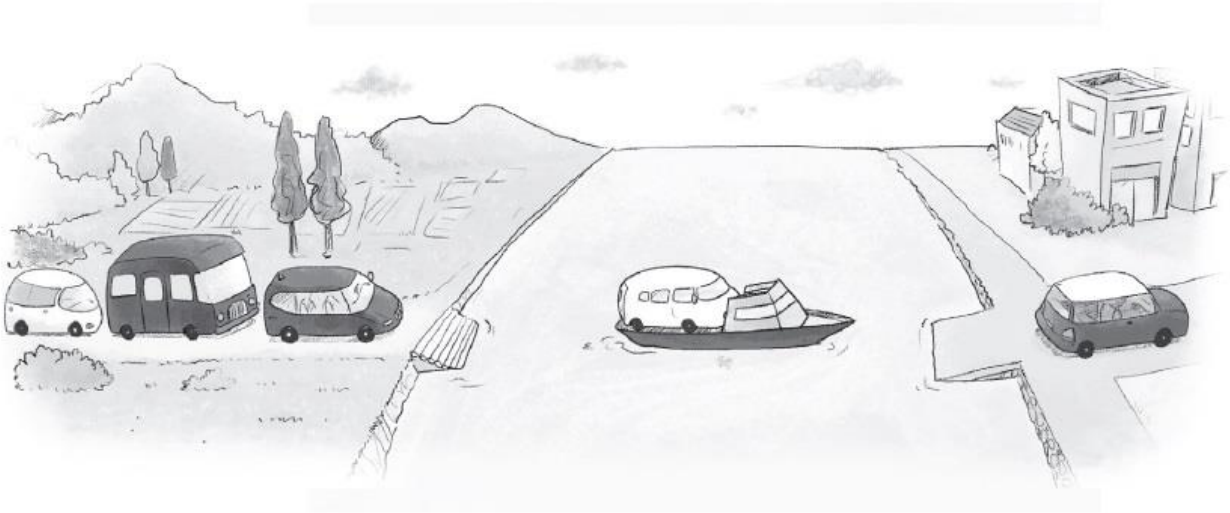
## 프로토콜의 기능

- 주소 설정(Addressing)
  - 서로 다른 시스템의 두 개체가 통신을 하는 경우 필요
  - 공격자는 정상이 아닌 변조된 주소 값을 이용하여 시스템에 혼란을 줌
- 순서 제어(Sequence Control)
  - 프로토콜 데이터 단위(PDU)를 전송할 때 보내는 순서를 명시하는 기능(연결 지향형(Connection-Oriented)에만 사용)
  - 공격자는 순서가 뒤바뀐 패킷을 보내 시스템을 과부하 걸리게 하기도 함
- 데이터 대열의 단편화 및 재조합(Fragmentation & Reassembly)
  - 대용량 파일을 전송할 때 전송 효율이 높은 작은 단위로 나누어 전송한 뒤 전송받은 시스템에서 이를 재조합해야 함.
  - 공격자는 데이터 분할 기능을 이용해 대량의 패킷을 전송하여, 재조합이 불가능 하도록 하여 혼란에 빠트리기도 함

# 01_프로토콜에 대한 이해

## ❖ 프로토콜의 기능

- 캡슐화(Encapsulation)
  - 데이터에 제어 정보를 덧붙이는 것



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

# 01_프로토콜에 대한 이해

## ❖ 프로토콜의 기능

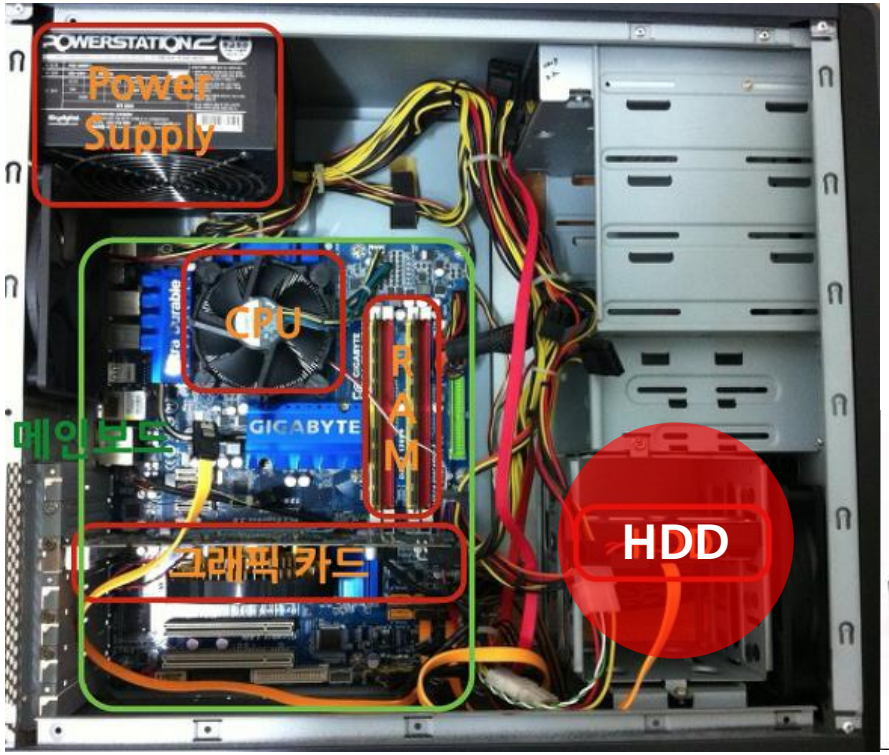
- 흐름 제어(Flow Control)
  - 송신측 개체로부터 오는 데이터의 양이나 속도를 조절하는 기능
  - 송신측과 수신측의 속도 차이 등으로 인한 정보 유실을 방지
- 오류 제어(Error Control)
  - 두 개체에서 데이터를 교환할 때 SDU(전송하려는 데이터)나 PCI(송신자와 수신자 주소, 오류 검출코드, 프로토콜 제어 정보 등)가 잘못되었을 경우, 이를 발견하는 기법
  - 순서를 검사하거나 특정 시간 안에 받지 못하면 재전송을 요구하는 방식으로 이루어짐.
- 동기화(Synchronization)
  - 두 개체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

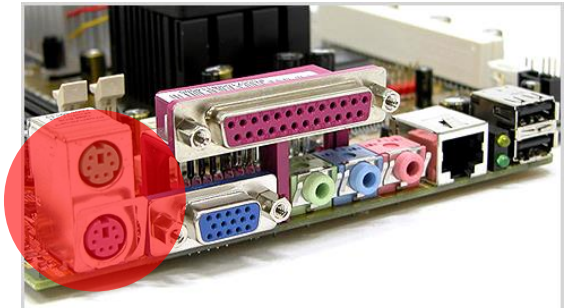
# 02_네트워크 계층 구조

## ❖ 네트워크 계층적 모듈 구조

CPU, 메모리, 하드디스크, 키보드, 마우스 등등 각자가 하는 역할이 다르지만 모두 적절한 상호작용을 하고 있다.

한 부분이 고장이 나도 그 도구만 고치게 되면 다른 도구들에게는 큰 영향을 끼치지 않는다. 대신에 도구를 바꿀 때에도 인턴페이스는 바뀌면 안 된다.



PS/2 커넥터

IDE 케이블

SATA 케이블

# 02_네트워크 계층 구조

## ❖ 네트워크 계층화에 대한 이해

- 1980년대 초 ISO(International Organization for Standardization)는 여러 업체가 만든 시스템에 대해 상호연동이 가능한 표준 네트워크 모델을 제정할 필요성을 인식
- 1984년 OSI(Open System Interconnection) 네트워크 모델을 발표

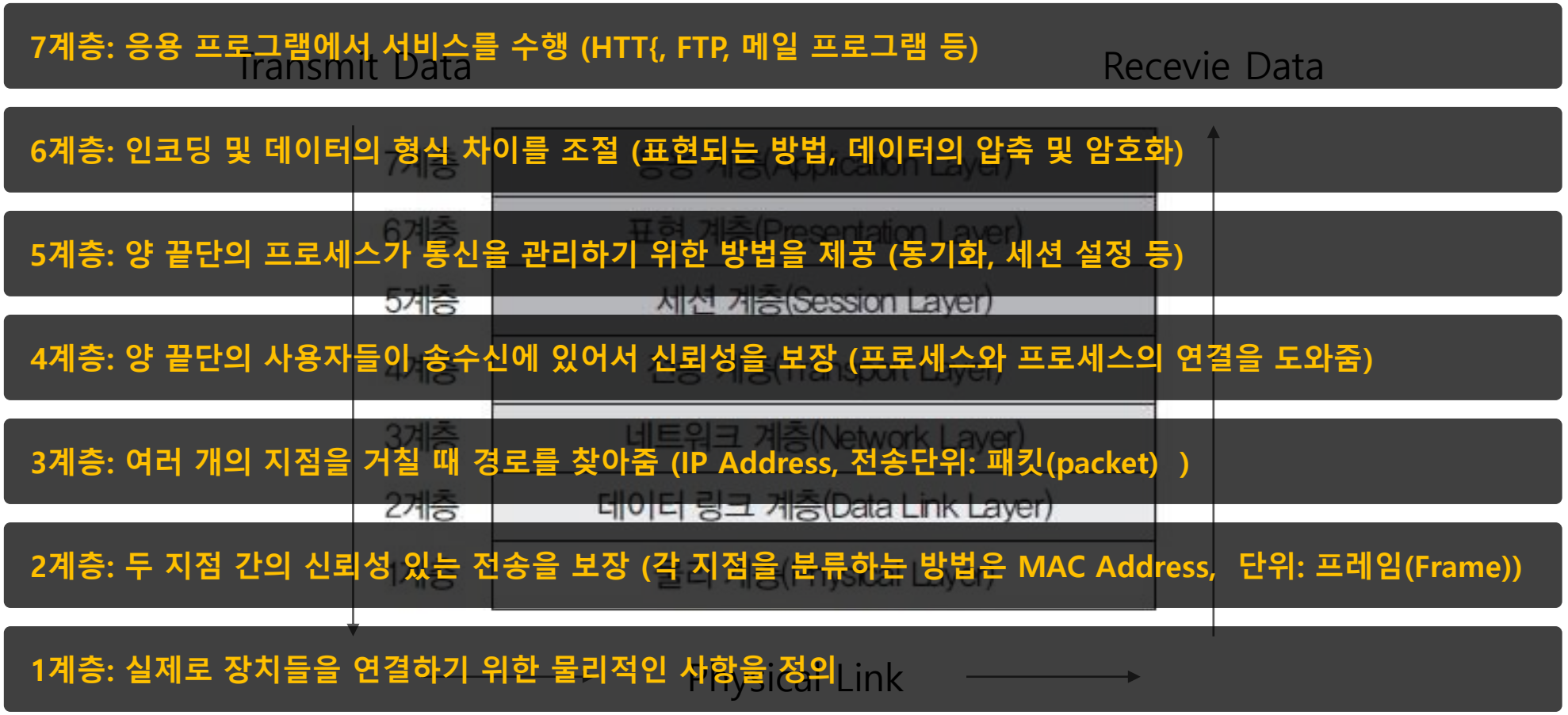
| | |
|---|---|
| 7계층 | 응용 계층(Application Layer) |
| 6계층 | 표현 계층(Presentation Layer) |
| 5계층 | 세션 계층(Session Layer) |
| 4계층 | 전송 계층(Transport Layer) |
| 3계층 | 네트워크 계층(Network Layer) |
| 2계층 | 데이터 링크 계층(Data Link Layer) |
| 1계층 | 물리 계층(Physical Layer) |

☞ OSI 7계층을 공부해야 하는 이유는 이 네트워크에 대해 전반적인 개념을 잡기 위한것 특히 보안과 관련해서는 이 네트워크가 정말 중요한 개념으로 작동

# 02_네트워크 계층 구조

## ❖ OSI(Open System Interconnection) 7계층 모델

- 네트워크 분야에서 가장 중요하게 다루는 것 중 하나로, 세계적으로 사용하고 있는 네트워크 표준모델 (이 안에 TCP/IP 및 네트워크 통신에 사용되는 전반적인 프로토콜이 포함)

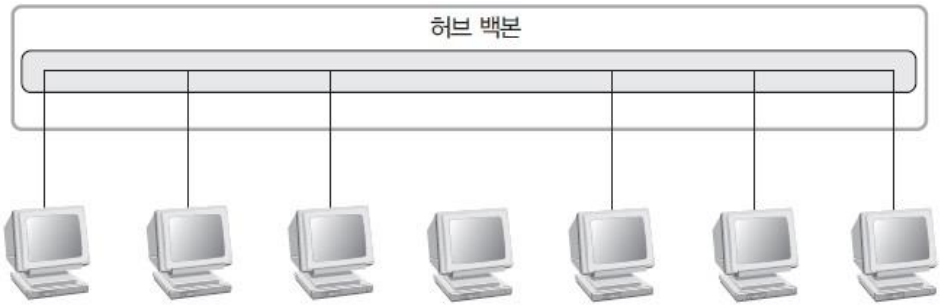


# 02_네트워크 계층 구조

## ❖ 물리 계층 관련 장비

- 리피터
  - 네트워크를 연장하기 위한 장비
  - 불분명해진 신호 세기를 다시 증가시키는 역할
  - 최근에는 리피터가 모든 네트워크 장비에 공통으로 들어가는 기능이 됨.
- 허브(Hub)
  - 요즘 쓰이는 스위치의 예전 형태
  - 최근의 스위치를 스위칭 허브, 이전 허브를 더미 허브라 부름.
  - 허브는 스위치와 형태나 사용 방법이 같지만 패킷을 모든 곳에 똑같이 복사해서 보내는 것이 다름(스위치는 목적지에만 데이터를 전송).

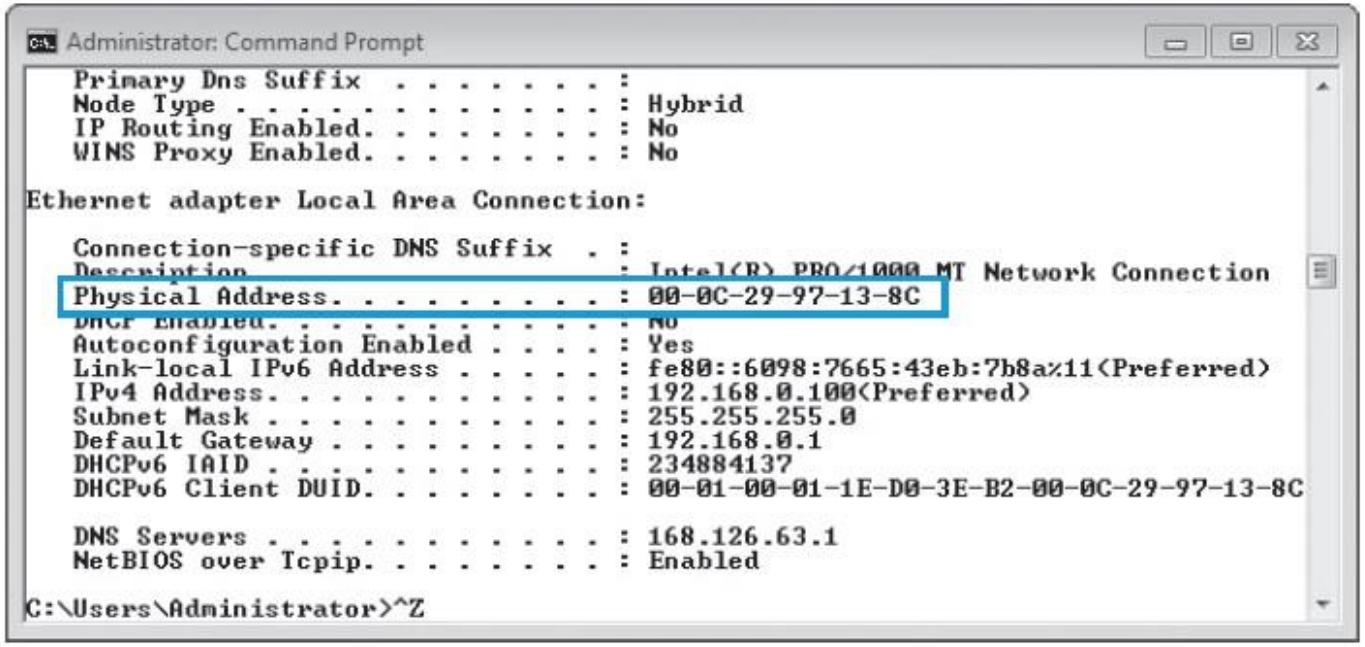
허브는 들어오는 신호의 송신지와 수신지를 구별하지 못해 허브를 통해 연결된 모든 컴퓨터에게 신호를 전달



# 02_네트워크 계층 구조

## ❖ 데이터 링크 계층(Data Link Layer)

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



# 02_네트워크 계층 구조

## MAC 주소

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

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

http://coffer.com/mac_find/

# 02_네트워크 계층 구조

## ❖ 데이터 링크 계층 관련 장비

- 브리지(Bridge)
  - 랜과 랜을 연결하는 초기의 네트워크 장치
  - 데이터 링크 계층에서 통신 선로를 따라서 한 네트워크에서 그 다음 네트워크로 데이터 프레임을 복사하는 역할
- 스위치(Switch)
  - 기본적으로 데이터 링크 계층에서 작동하는 스위치를 뜻함.
  - L2스위치는 연결된 시스템이 늘어날수록 패킷 간 충돌 때문에 매우 낮은 속도로 동작하는 더미 허브의 문제점을 해결하는 획기적인 방안


# 02_네트워크 계층 구조

## ❖ 스위치 테이블

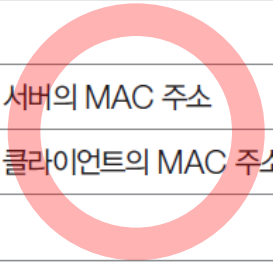
- 시스템 간의 원활한 통신을 위해 주소 테이블을 생성하고 관리하는 역할

스위치에 서버가 연결되어 있을 때 메모리 정보

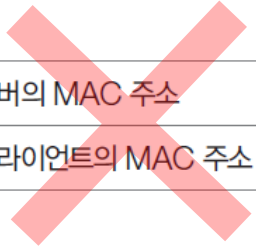
| | |
|---|---|
| 1번 포트 | |
| 2번 포트 | 서버의 MAC 주소 |
| 3번 포트 | |
| 4번 포트 | |

클라이언트의 랜 케이블을 스위치의 3번 포트에 꽂음

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



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



# 02_네트워크 계층 구조

## ICMP(Internet Control Message Protocol)

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

# 02_네트워크 계층 구조

## ❖ 네트워크 계층 관련 장비

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

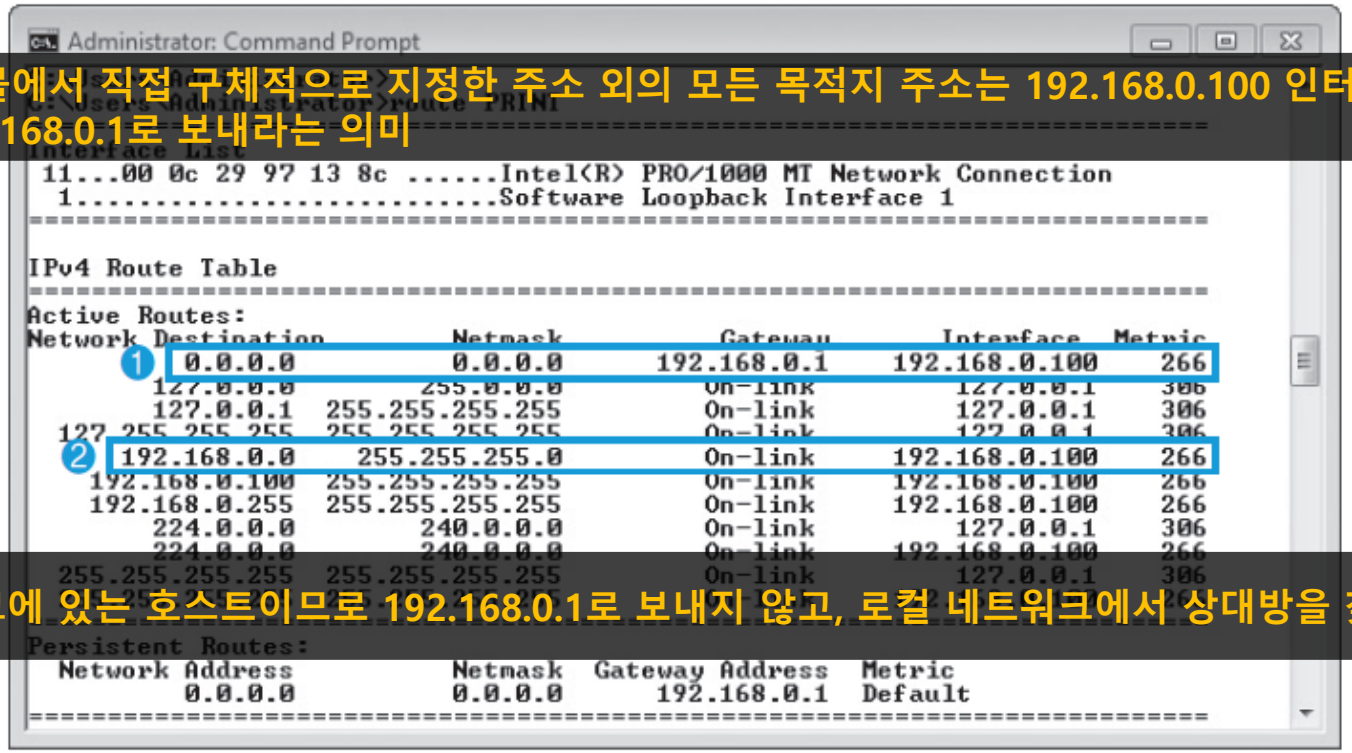
(a) 소형 라우터

(b) 대형 라우터

# 02_네트워크 계층 구조

## ❖ 라우팅

- 어떤 네트워크 안에서 통신 데이터를 보낼 경로를 선택하는 과정
- 'route print' 명령을 통해 라우팅테이블 출력



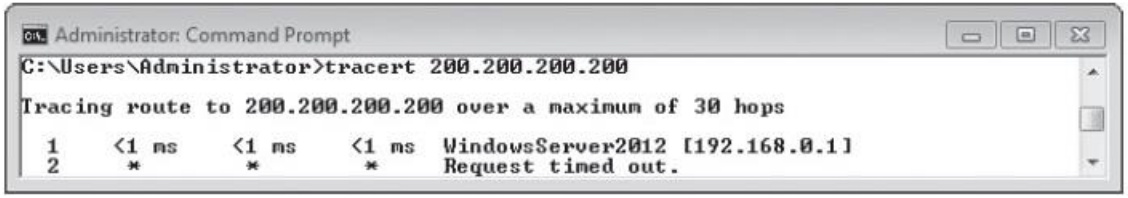

① 라우팅 테이블에서 직접 구체적으로 지정한 주소 외의 모든 목적지 주소는 192.168.0.100 인터페이스를 통해 게이트웨이 192.168.0.1로 보내라는 의미

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

# 02_네트워크 계층 구조

## ❖ 라우팅

- ‘tracert’ 명령으로 200.200.200.200으로 시작하는 경로로 ICMP 패킷을 전송
- 200.200.200.200으로 목적지 IP가 설정된 패킷을 192.168.0.1로 보냄



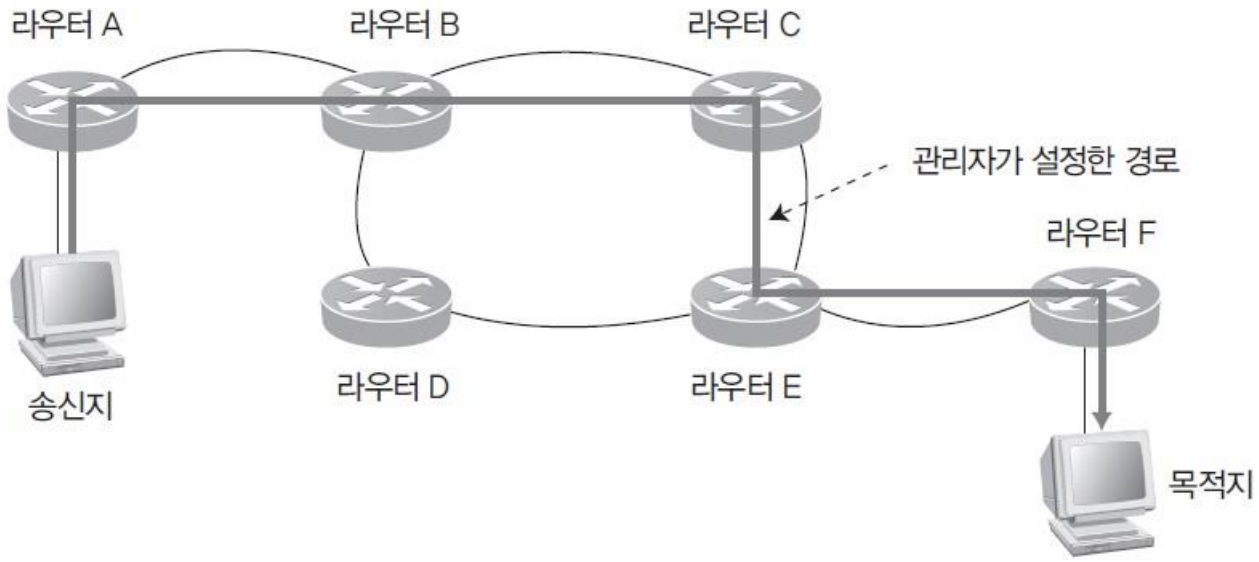

IP 주소 200.200.200.200에 대한 네트워크 경로 확인

☞ tracert : ICMP 패킷을 이용하여 tracert 명령의 매개변수로 지정한 목적지 IP 주소에 패킷이 도달할때 까지 거치는 중간 단계 네트워크 장비의 주소를 차례로 출력
윈도우에서는 tracert, 리눅스에서는 traceroute 명령으로 동작

# 02_네트워크 계층 구조

## ❖ 정적 라우팅

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



# 02_네트워크 계층 구조

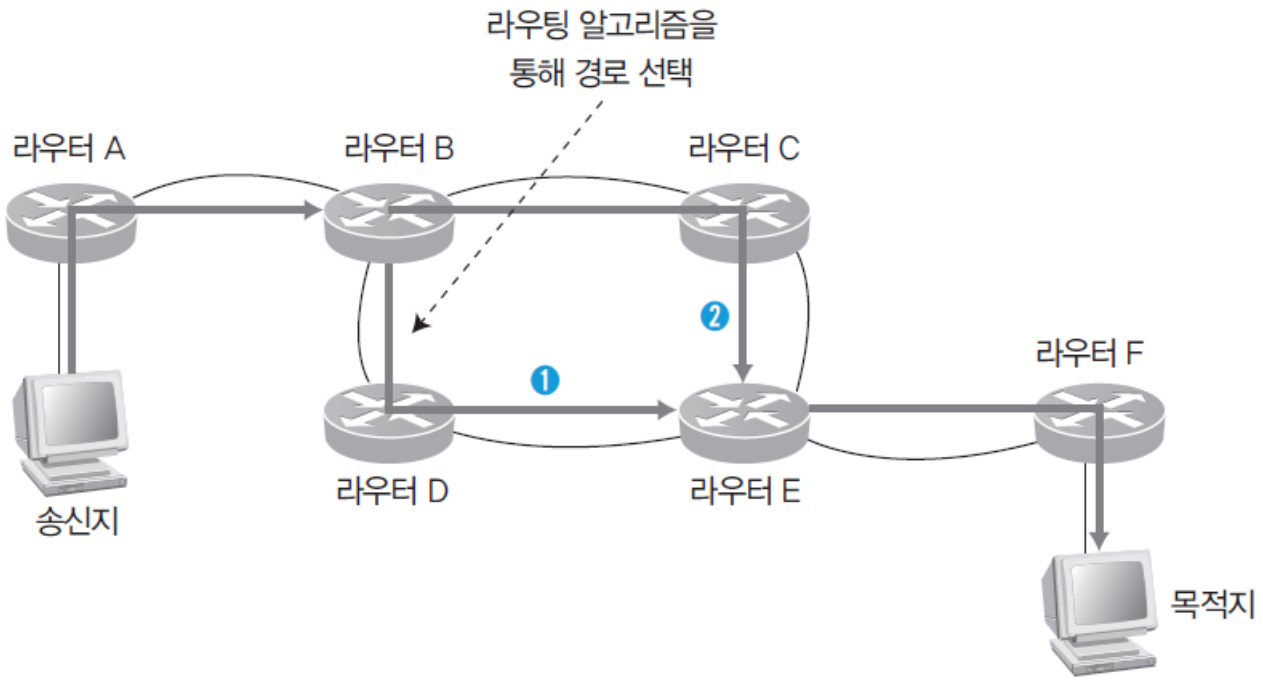
## 정적 라우팅의 특징

- 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

# 02_네트워크 계층 구조

## ❖ 동적 라우팅

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



# 02_네트워크 계층 구조

## ❖ 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

# 02_네트워크 계층 구조

## ❖ 4계층 : 전송 계층(Transport Layer)

- 대표 프로토콜은 TCP(Transmission Control Protocol)
- TCP가 가진 주소를 포트(Port)라 하며 0~65535(216-1)번까지 존재
- 0~1023번(1,024)을 잘 알려진 포트(Well Known Port)라고 부름 (보통 0번 포트는 사용하지 않음).

| 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 |

# 02_TEST

**다음 Port를 보고, 어떤 서비스 인지 맞춰보세요.**

| Port번호 | 서비스 |
| --- | --- |
| 22 | |
| 443 | |
| 389 | |

# 02_TEST (풀이)

**다음 Port를 보고, 어떤 서비스 인지 맞춰보세요.**

| Port번호 | 서비스 |
| --- | --- |
| 22 | SSH (Secure Shell) |
| 443 | HTTPS - HTTP over SSL (암호화 전송) |
| 389 | LDAP (Lightweight Directory Access Protocol) |

# 02_네트워크 계층 구조

## ❖ 패킷 구조와 예

- 출발지 포트는 보통 1024번부터 65535번 사이에서 사용하지 않는 임의의 포트를 응용 프로그램별로 할당하여 사용

- 클라이언트가 웹 서버에 접속할 때 패킷 구조(서비스 포트는 보통 80번)

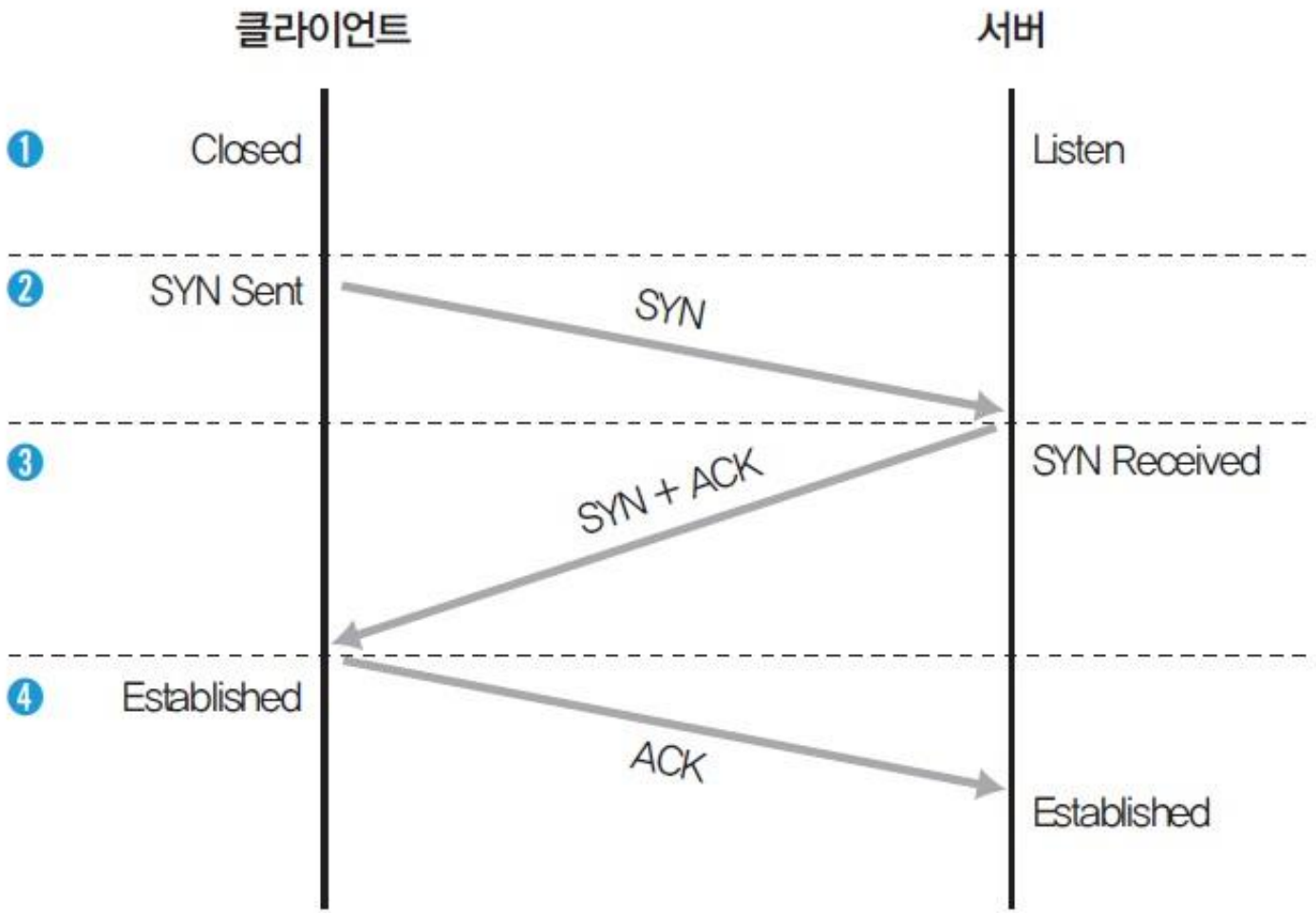
<table>
<tr><td>01001010101</td><td>출발지 포트</td><td>80</td><td>출발지 IP</td><td>목적지 IP</td><td>출발지 MAC</td><td>목적지 MAC</td></tr>
<tr><td>5계층까지의 패킷 정보</td><td colspan="2">4계층 패킷 정보</td><td colspan="2">3계층 패킷 정보</td><td colspan="2">2계층 패킷 정보</td></tr>
</table>

- 시스템에서 임의로 포트를 할당한 출발지 패킷 구조

<table>
<tr><td>01001010101</td><td>3405</td><td>80</td><td>출발지 IP</td><td>목적지 IP</td><td>출발지 MAC</td><td>목적지 MAC</td></tr>
<tr><td>5계층까지의 패킷 정보</td><td colspan="2">4계층 패킷 정보</td><td colspan="2">3계층 패킷 정보</td><td colspan="2">2계층 패킷 정보</td></tr>
</table>

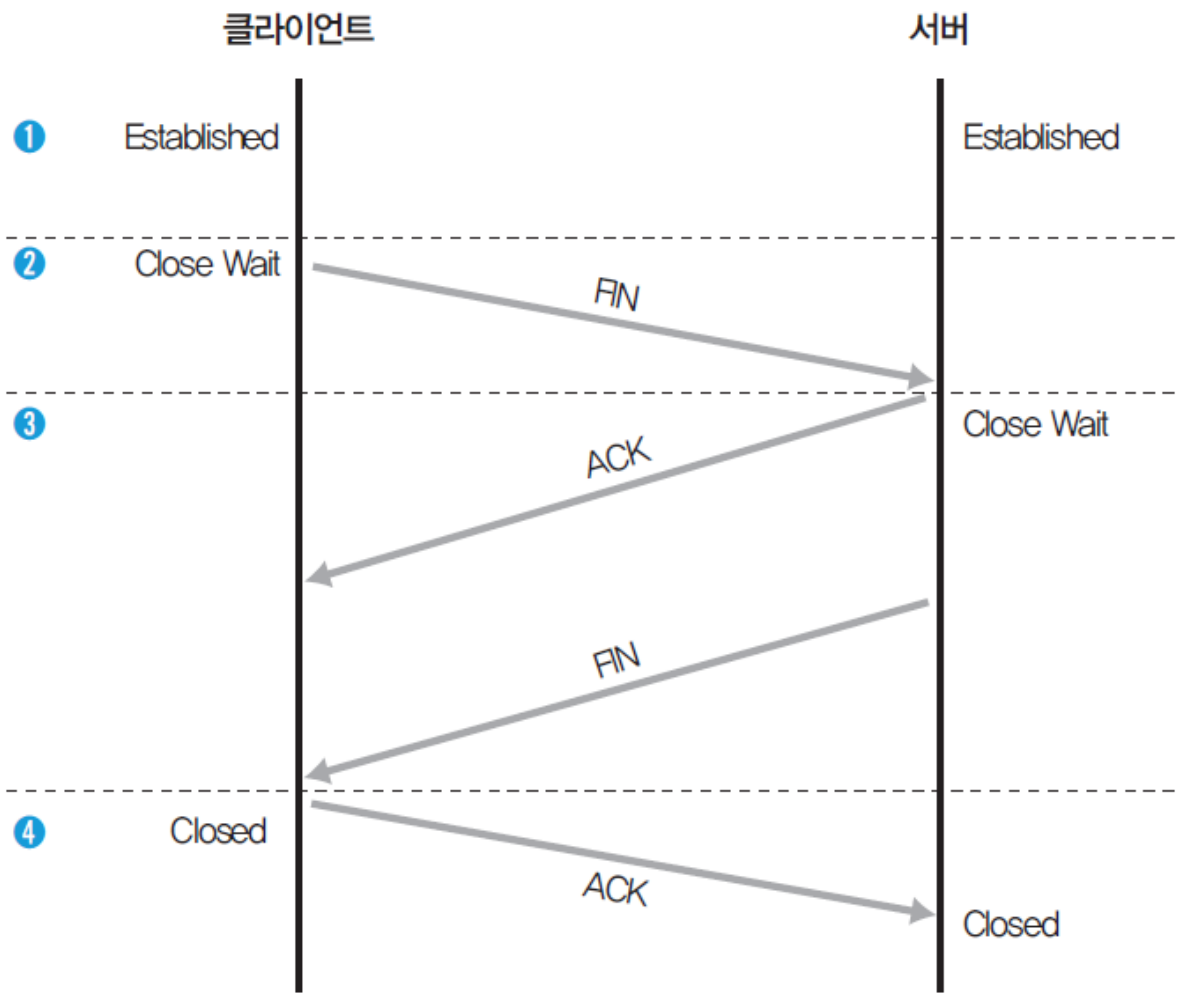
# 02_네트워크 계층 구조

## ❖ 연결 설정 과정(Three-Way Handshaking)



# 02_네트워크 계층 구조

## ❖ 연결 해제 과정



# 02_네트워크 계층 구조

## 7계층 : 응용 계층(Application Layer)

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

- FTP(File Transfer Protocol, 20,21)
  - 파일 전송을 위한 가장 기본적인 프로토콜
  - 1972년 텔넷과 함께 표준으로 제정
  - 클라이언트와 서버가 대화형으로 통신 가능
- Telnet(텔넷, 23)
  - 사용자가 원격에 있는 서버에 로그인하도록 TCP 연결을 설정
  - 단말기가 원격 컴퓨터 바로 옆에 있는 것처럼 직접 조작할 수 있게 해줌.