

클라우드컴퓨팅

김태운

네트워크 기본 & 복습

Computer Networks.

클라우드 컴퓨팅의 핵심기술 중 하나인 네트워크에 대해 간략하게 복습하겠습니다. 통신/네트워크 관련 상세 내용은 [데이터 통신] 또는 [컴퓨터 네트워크] 과목에서 배울 수 있습니다!



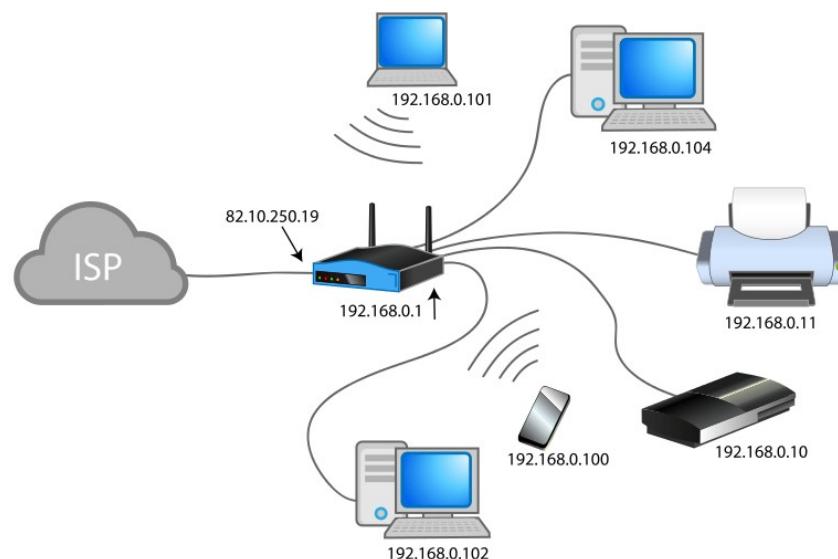
네트워크

초기 네트워크 장비는 서로 호환이 되지 않았으나, OSI 7계층 개념을 기반으로 통신 기술의 표준화가 진행되었고, 이후로는 서로 다른 제조사 장비간 상호 운용/호환이 가능해졌습니다.



• 네트워크

- 전송매체(transmission media)를 매개로 서로 연결되어 데이터를 교환하는 시스템의 모음
- 일반적인 컴퓨터 네트워크에서는 물리적인 통신 매체(유선 또는 무선)로 연결된 컴퓨터들이 동일한 프로토콜을 이용해 서로 데이터를 주고 받음
- L2 스위치로 연결된 소규모 네트워크가 모여 더 큰 네트워크를 구성할 수 있는데, 서로 다른 네트워크를 연결하는 목적으로 라우터(Layer-3)라는 중개 장비를 사용



Cisco Small Business RV Series Router

네트워크 : 용어

- 인터페이스 :

- 시스템과 전송 매체의 연결 지점에 대한 규격
- 데이터 단말 장치와 데이터 통신 장치간의 접속에 관한 규격
- 대표적인 네트워크 인터페이스 카드 (NIC, network interface card):
 - 일반적으로, NIC는 MAC/PHY 계층을 구현함



유선 통신 (이더넷)
인터페이스 카드



무선 통신 (WiFi)
인터페이스 카드

- 프로토콜 :

네트워크에는 규격/규칙이 많은데, 서로 다른 제조사에서 생산한 기기/부품들이 서로 연동되어 동작하기 위해서는 공통의 규칙이 필요합니다.

- 시스템간 데이터를 교환할 때 사용하는 통신 규칙/규약
- 무엇을, 언제, 어떻게, 어떤 방식으로 통신 할지를 정의 해 놓은 것
- 예: 전송 계층 프로토콜 TCP, UDP

TCP 프로토콜은 3-way handshake 및 ACK 메시지를 이용해서 구현 로직이 복잡하지만 안정적인 데이터 전송을 보장하고, 이와 반대인 UDP는 로직 복잡도는 낮지만 신뢰성/안전성이 보장되지 않는 전송 프로토콜입니다.

네트워크 : 주소



- 두 단말 간 통신을 하기 위한 조건

- 1) 두개의 단말이 네트워크에 연결되어 있고, 공통의 프로토콜을 사용함
- 2) 두 단말은 서로 상대방의 고유한 주소를 알고, 접근이 허용됨(방화벽 등...)
- 예: NAVER 웹 페이지 접속하기
 - 웹 브라우저의 주소창에 www.naver.com 입력
= "www.naver.com"이라는 이름(hostname)을 가진 서버의 첫 화면을 가져와서, 웹 브라우저에 보여줘"
 - 웹 브라우저는 DNS 서버를 통해 www.naver.com라는 (사람이 이해할 수 있는) 영문 주소를, (네트워크가 이해할 수 있는) 숫자 주소로 변환 => 23.50.3.12
 - 23.50.3.12 주소를 가진 서버에게 웹 페이지 요청 전송 (예: GET Request)
 - 네이버 서버는 응답 웹 페이지를 내 컴퓨터로 전송
 - 네이버 웹 페이지를 다운 받은 후, 웹 브라우저에 표시

```
PS C:\Users\User> nslookup www.naver.com
서버:  ns.ns1.uhost.co.kr
Address: 210.115.225.11

권한 없는 응답:
이름:  e6030.a.akamaiedge.net
Address: 23.50.3.12
Aliases: www.naver.com
          www.naver.com.phos.com
          www.naver.com.ekey.net
```

‘nslookup’ 명령으로
숫자 주소(IP주소)를 알아낼 수 있음

간단히 생각하면, IP 주소는 컴퓨터에 주소이고, MAC 주소는 컴퓨터에 장착된 인터페이스 카드에 할당된 주소입니다.



네트워크 : 주소

- 주소 (Address)

- 일반적인 주소 : 사람이 사는 곳이나 기관, 회사 따위가 자리 잡고 있는 위치
- 네트워크에서 주소 : 컴퓨터, 서버 등의 논리적인 위치를 설명하고, 서로 다른 단말을 고유하게 구별할 수 있기 위해 부여한 식별자

- 네트워크에서의 주소:

- **IP 주소** : IP 주소는 컴퓨터 네트워크에서 장치들이 서로를 인식하고 통신을 하기 위해서 사용하는 특수한 번호 (변할 수 있는 주소)
- MAC 주소 : 네트워크 인터페이스에 할당된 고유 식별자 (변하지 않는 주소)
- 포트번호 : 단일 머신 내에서 서비스를 구분하기 위한 고유 식별자 (HTTP 80 등)

MAC 주소도 변경할 수 있지만,
이는 극히 드문 경우임.

```
daniel@Ubuntu22Desk:~$ ifconfig  
enp0s3: flags=4163<UP,BROADCAST,RUNNING,  
        inet 10.0.2.15 brd 255.255.0.0 netmask 255.255.0.0  
          MAC 주소  
          inet6 fe80::78cc:8bda:864d:1bdf  
            ether 08:00:27:cd:89:d9 MAC 주소  
              RX packets 148279 bytes 148279  
              RX errors 0 dropped 0 overruns 0
```

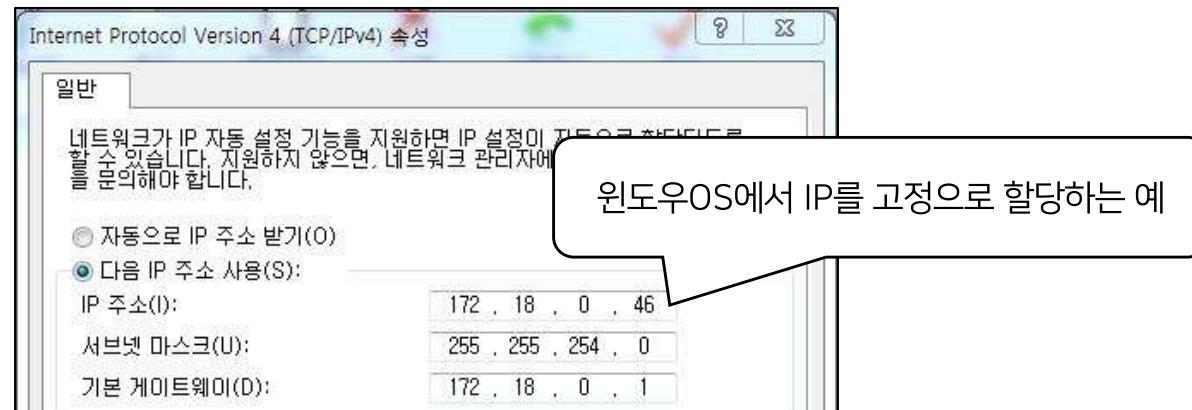
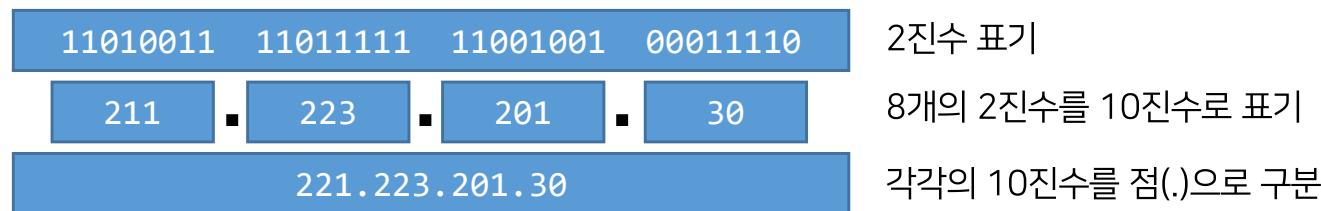
tacacs	49/udp
domain	53/tcp
domain	53/udp
bootps	67/udp
bootpc	68/udp
tftp	69/udp
gopher	70/tcp
finger	79/tcp
http	80/tcp
kerberos	88/tcp
kerberos	88/udp
iso-tsap	102/tcp
acr-nema	104/tcp
pop3	110/tcp
sunrpc	111/tcp
--More--	

\$ cat /etc/services 출력 결과
(well-known 포트 번호 목록 조회)

네트워크 : IP 주소

- IP 주소 (IP Address)

- 네트워크 계층의 기능을 수행하는 IP 프로토콜이 호스트(= 통신이 가능한 기기/머신)를 구분하기 위해 사용하는 숫자 주소
- 임의의 호스트/머신을 인터넷에 연결하려면, 반드시 해당 머신에 IP 주소를 할당 해야 함
- IP 주소는 32비트의 이진 숫자로 구성 (IPv4)
 - 표기 할 때에는 8비트씩 끊어서 0~255의 10진수 숫자를 사용, 각 숫자는 점(.)으로 구분



네트워크 : IP 주소

- IP 주소 (IP Address)

- 유일성을 보장하기 위해 국제 표준화 기구가 전체 주소를 관리하고 할당함
 - 유일성(즉, 주소가 고유함)이 보장 되어야 혼란 없이 원하는 호스트에 접근 할 수 있다.



- IP 주소 부족으로 인해(2^{32}), IPv6를 점차 사용하는 추세 (2^{128} 주소 공간)

```
이더넷 어댑터 이더넷:  
연결별 DNS 접미사...:.  
설명...: Intel(R) Ethernet Connection (5) I219-LM  
물리적 주소...: 10-00-04-81-D9-97  
DHCP 사용...: IPv6 주소 (128 비트)  
자동 구성 사용...: 예  
링크-로컬 IPv6 주소...: fe80::ef:d955:b461:1bbd%15(기본 설정)  
IPv4 주소...: 192.168.0.2(기본 설정)
```

네트워크 : IP 주소

- IP 주소

- 공인(public) IP 주소

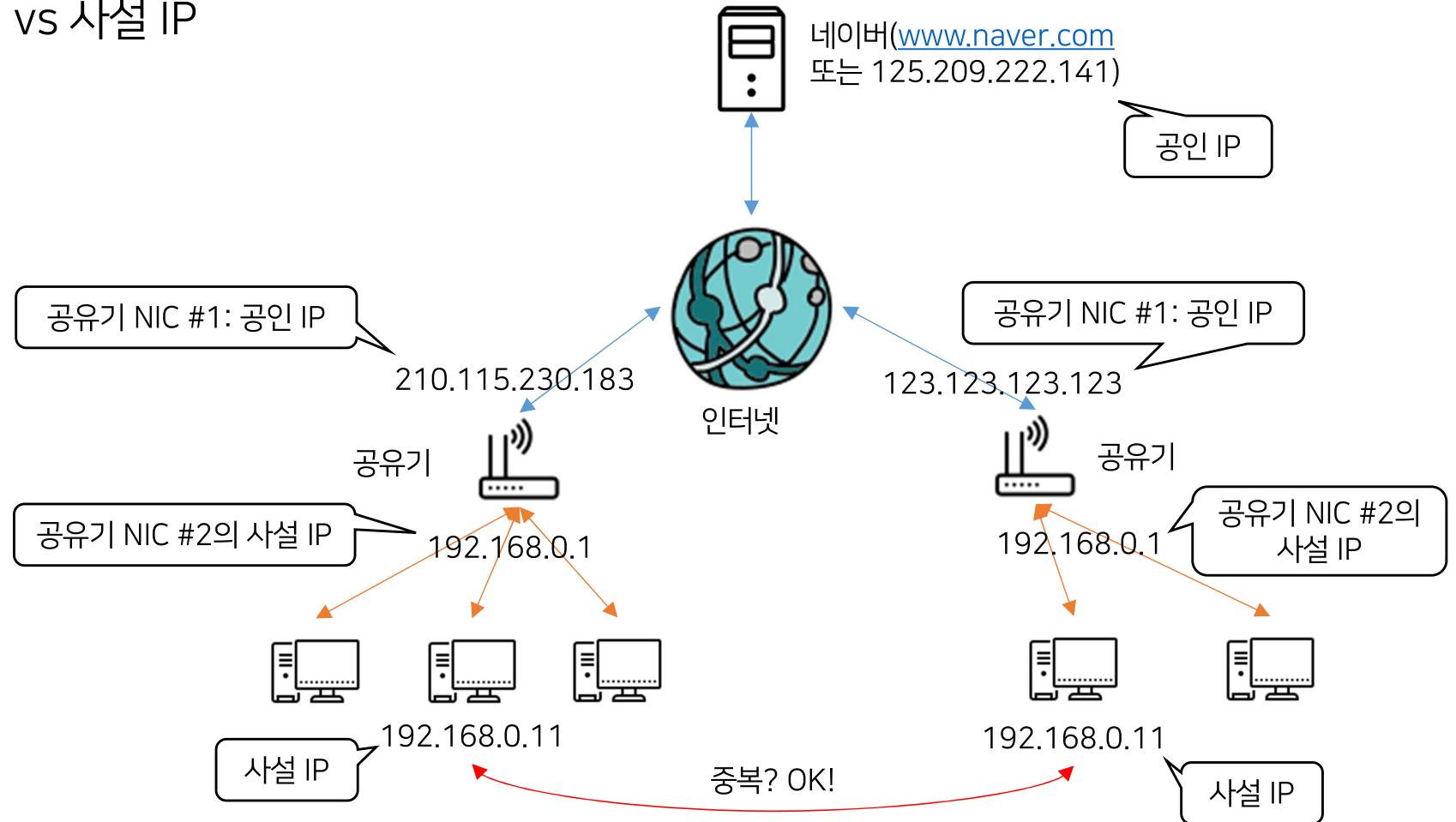
- 전 세계적으로 고유한 주소이며 한국내의 공인 IP 주소는 인터넷 진흥원에서 관리
 - 예: 부산시 금정구 부산대학교 자연대연구실험동 302호 (전국적으로 고유한 주소)
 - IPv4 주소 공간은 32비트로 제한되어 있으며, 따라서 사용 가능한 IP 주소도 제한됨

- 사설(private) IP 주소

- 서로 다른 컴퓨터가 동일한 주소를 중복해서 사용 가능(즉, 주소가 고유하지 않음)
 - 예: 1116-1 호 (공학관 외부인은 목적지가 어디인지 알 수 없음)
 - IP 주소 부족 문제를 해결하기 위해 특정 주소 대역을 사설 IP 대역으로 지정
 - 사용 예: 공유기에 공인 IP 할당 후, 공유기에 연결된 다수의 컴퓨터에 사설 IP를 DHCP로 자동 할당
 - RFC 1918에 의해 정의된 사설 IP 주소 범위
 - 10.0.0.0 ~ 10.255.255.255 (10.0.0.0/8) : 1개의 A 클래스
 - 172.16.0.0 ~ 172.31.255.255 (172.16.0.0/12) : 16개의 B 클래스
 - 192.168.0.0 ~ 192.168.255.255 (192.168.0.0/16) : 256개의 C 클래스

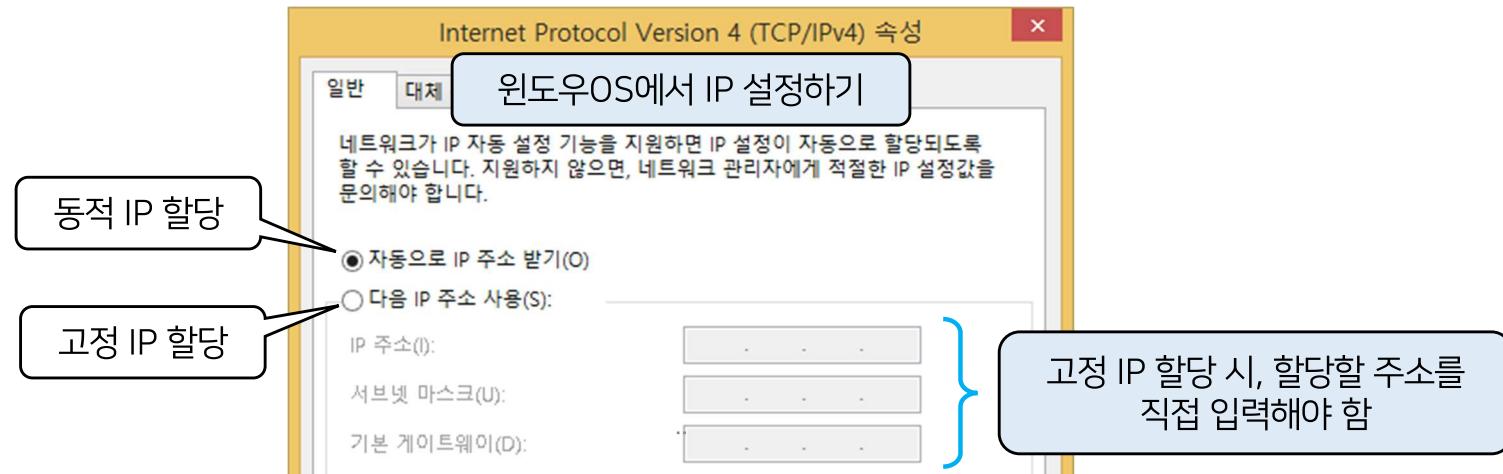
네트워크 : IP 주소

- 공인 IP vs 사설 IP



네트워크 : IP 주소

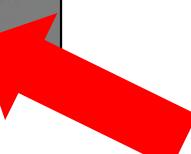
- IP 주소를 할당하는 방법
 - 고정 IP 할당
 - 고정된 IP 주소를 고정적으로 할당하는 것 (공인 IP를 사용할 때 주로 사용)
 - 머신(예: 컴퓨터 등)이 재부팅 되어도 항상 동일한 IP 주소를 사용함
 - 동적 IP 할당
 - DHCP (Dynamic Host Configuration Protocol) 프로토콜을 사용하여, 동적으로 가용한 IP 주소를 할당하는 방식
 - 사설 IP를 사용할 때 주로 사용
 - 예: 공유기는 가용 IP주소를 풀링하여 관리하고, 사용자 요청에 따라 IP주소를 할당 (단, 일정 시간이 지나거나, 더 이상 사용되지 않는 주소는 자동으로 수거하여 다시 풀링으로 관리함)



네트워크 구성: IP 주소

- 우분투 리눅스에서 IP 설정하기
 - 참고: 우분투 v18 부터는 netplan 툴을 사용하여 IP 주소를 설정함
 - /etc/netplan 디렉토리 아래의 *.yaml 파일을 수정하여 IP를 직접 부여하거나 동적 할당으로 설정
 - 동적 IP 설정하기: *.yaml 파일을 아래와 같이 수정 (관리자 권한 필요)

```
network:  
  ethernets:  
    eno1: 인터페이스 이름 ($ifconfig로 확인)  
      addresses: []  
      dhcp4: true  
  version: 2
```



네트워크 구성: IP 주소

- 우분투 리눅스에서 IP 설정하기
 - 참고: 우분투 v18 부터는 netplan 툴을 사용하여 IP 주소를 설정함
 - /etc/netplan 디렉토리 아래의 *.yaml 파일을 수정하여 IP를 부여하거나 동적할당으로 설정
 - 고정 IP 설정하기: *.yaml 파일을 아래와 같이 수정 (관리자 권한 필요)

```
network:
  ethernets:
    eno1: 인터페이스 이름 ($ifconfig로 확인)
      dhcp4: no
      addresses: [210.115.230.183/24]
      gateway4: 210.115.230.1
      nameservers:
        addresses: [210.115.225.11, 168.126.63.1]
version: 2
```

네트워크 구성: IP 주소

- 우분투 리눅스에서 IP 설정하기
 - 참고: 우분투 v18 부터는 netplan 툴을 사용하여 IP 주소를 설정함
 - /etc/netplan 디렉토리 아래의 *.yaml 파일을 수정하여 IP를 부여하거나 동적할당으로 설정
 - 고정/동적 IP 설정하기: *.yaml 파일을 수정한 후 변경 내용을 적용

```
$sudo netplan apply
```

네트워크 : IP 주소

네트워크 주소
(24비트)호스트 주소
(8비트)

- IP 주소 클래스 (IP Class)

- IP 주소는 클래스 단위로 관리하고, 클래스 내에서 각 호스트에 주소를 할당함
- IP 주소 클래스의 종류 : A, B, C, (D, E) 클래스

이름	범위	서브넷마스크/CIDR	호스트 bit 수	사용 가능 호스트 수
A 클래스	1.0.0.0 ~ 126.0.0.0	255.0.0.0/8	32	약 1,600만 개
B 클래스	128.0.0.0 ~ 191.0.0.0	255.255.0.0/16	16	약 65,000개
C 클래스	192.0.0.0 ~ 223.0.0.0	255.255.255.0/24	8	254개

- 일반 사용자 입장에서 가장 많이 사용하는 클래스는 C 클래스

- 예: 192.168.0.X 인 C 클래스 = 192.168.0.X/24 (CIDR 표기)

하나의 서브 네트워크의 규모
(= 사용 가능한 호스트 수)는
A > B > C 순서임

- 앞의 3자리(24비트) 192.168.0 은 호스트가 속한 네트워크의 주소를 의미하고

- 뒤의 1자리 X는, 해당 네트워크에 연결된 호스트 번호를 의미

```

연결별 DNS 접미사.....:
링크-로컬 IPv6 주소.....: fe80::ef:d955:b461:1hhhd%15
IPv4 주소.....: 192.168.0.2
서브넷 마스크.....: 255.255.255.0
기본 게이트웨이.....: 192.168.0.1

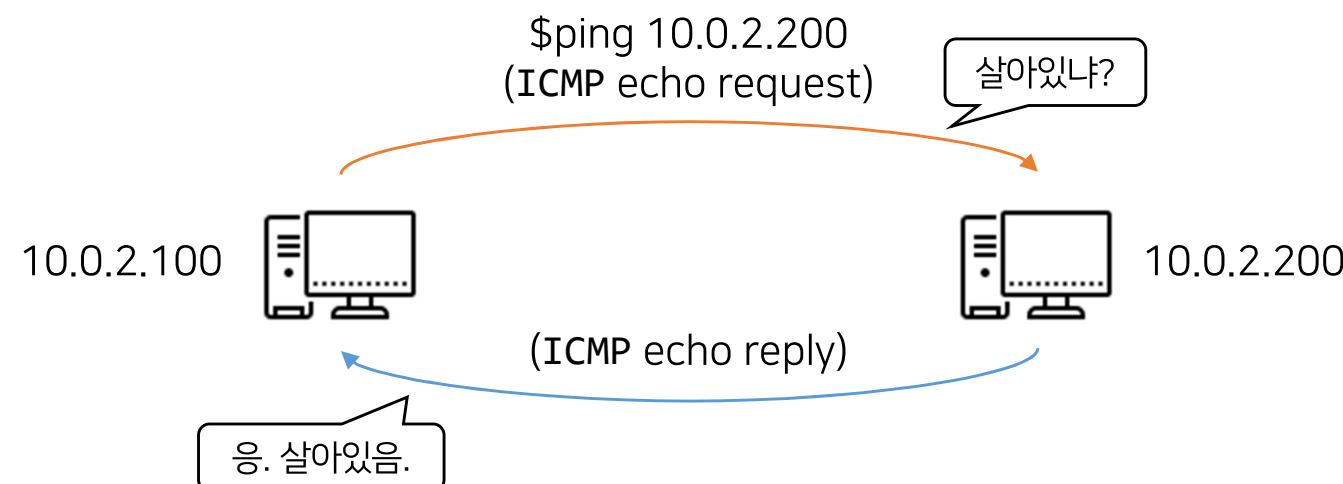
```

192.168.0 네트워크에 연결된
2번 호스트에서 ipconfig 결과

네트워크 : 리눅스 명령어

- **\$ifconfig** : 네트워크 인터페이스 카드 설정 정보 확인
 - IPv4, IPv6 주소
 - MAC 주소
 - Netmask 정보 등 조회
- **\$ping <원격 호스트 URL 또는 IP 주소>** : 네트워크 연결 및 호스트 상태 확인
 - 예: \$ping www.google.com
 - 예: \$ping 123.123.123.123

\$ifconfig 명령어가 없다면,
'net-tools' 패키지를 먼저 설치하세요!



윈도우에서 SSH 접속 시, PuTTY와 같은 전용 터미널 프로그램을 주로 사용합니다.



네트워크 : 리눅스 명령어

- \$ssh <아이디>@<서버주소> : 원격 서버에 터미널 접속 // 다음 페이지 참고

- 예:

- 210.115.229.76 서버에 daniel이라는 아이디로 접속하기
 - \$ssh daniel@210.115.229.76 (윈도우, 리눅스 사용방법 동일)

```
daniel@danpc3: ~  
PS C:\Users\User> ssh daniel@210.115.229.76  
daniel@210.115.229.76's password:  
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux)  패스워드 입력 시, 화면에 보여지지 않습니다.
```

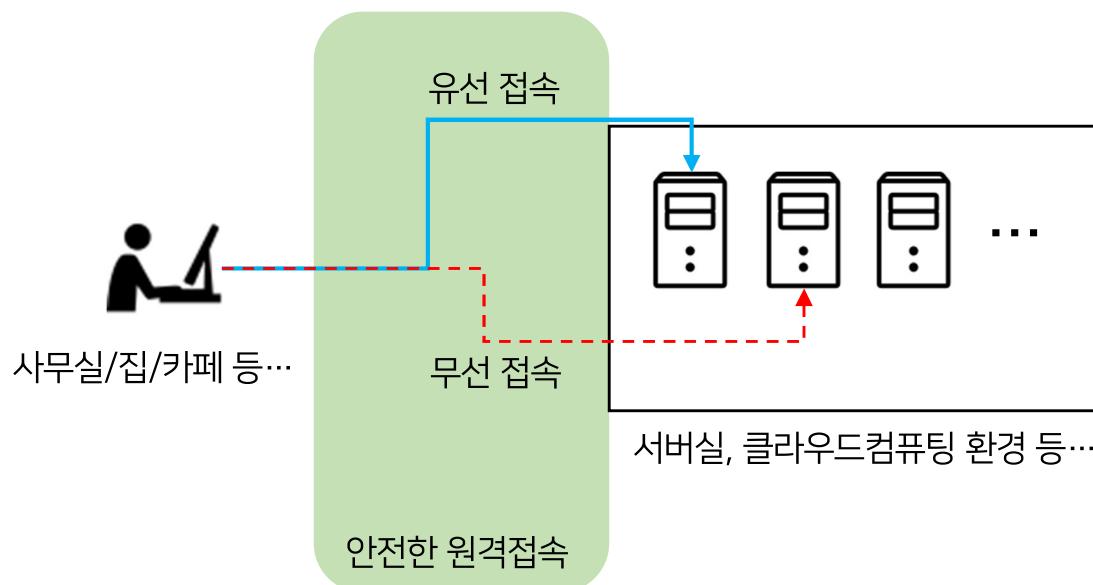
- \$wget <원격지 파일 명> : 웹 상의 파일을 다운로드

- 예:

- 위키피디아(영문)에서 “Computer program” 웹 페이지 다운 받기
 - \$wget https://en.wikipedia.org/wiki/Computer_program

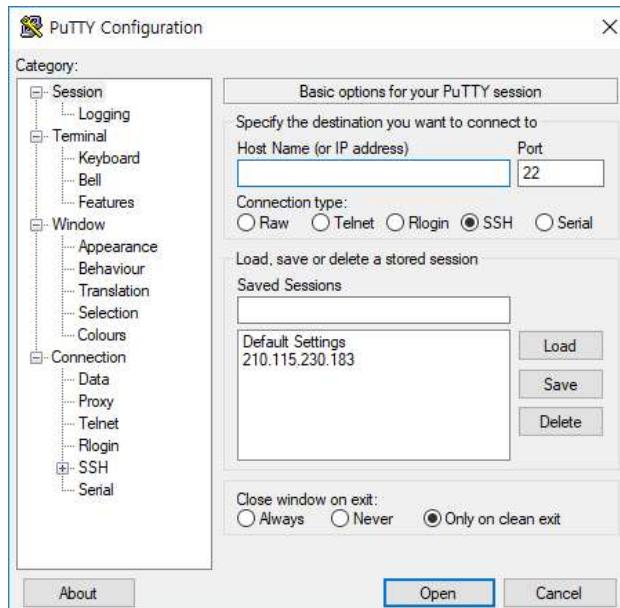
네트워크 구성: SSH 접속

- 시큐어 셸 (SSH, Secure Shell)
 - 네트워크 상의 다른 컴퓨터에 로그인하거나 원격 시스템에서 명령을 실행하고 다른 시스템으로 파일을 복사할 수 있도록 해 주는 응용 프로그램 또는 프로토콜 (기본적으로 22번 포트 사용)
 - 암호화 기법을 사용하기 때문에, 통신이 노출되어도 이해할 수 없는 암호화된 문자로 보임
 - 사용 예:



네트워크 구성: SSH 접속

- 터미널 에뮬레이터 프로그램 : SSH, 텔넷 등의 접속을 위한 터미널 프로그램
- PuTTY
 - 가장 많이 사용하는 오픈 소스 터미널 에뮬레이터 프로그램
 - SCP, SSH, Telnet, rlogin 등 다양한 프로토콜 지원
 - 1999년 윈도우 운영체제에서 동작하도록 최초 개발. 이후, 다양한 운영체제 지원
 - 다운로드 링크 : <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>



윈도우의 경우 PowerShell을 이용해도 충분합니다.

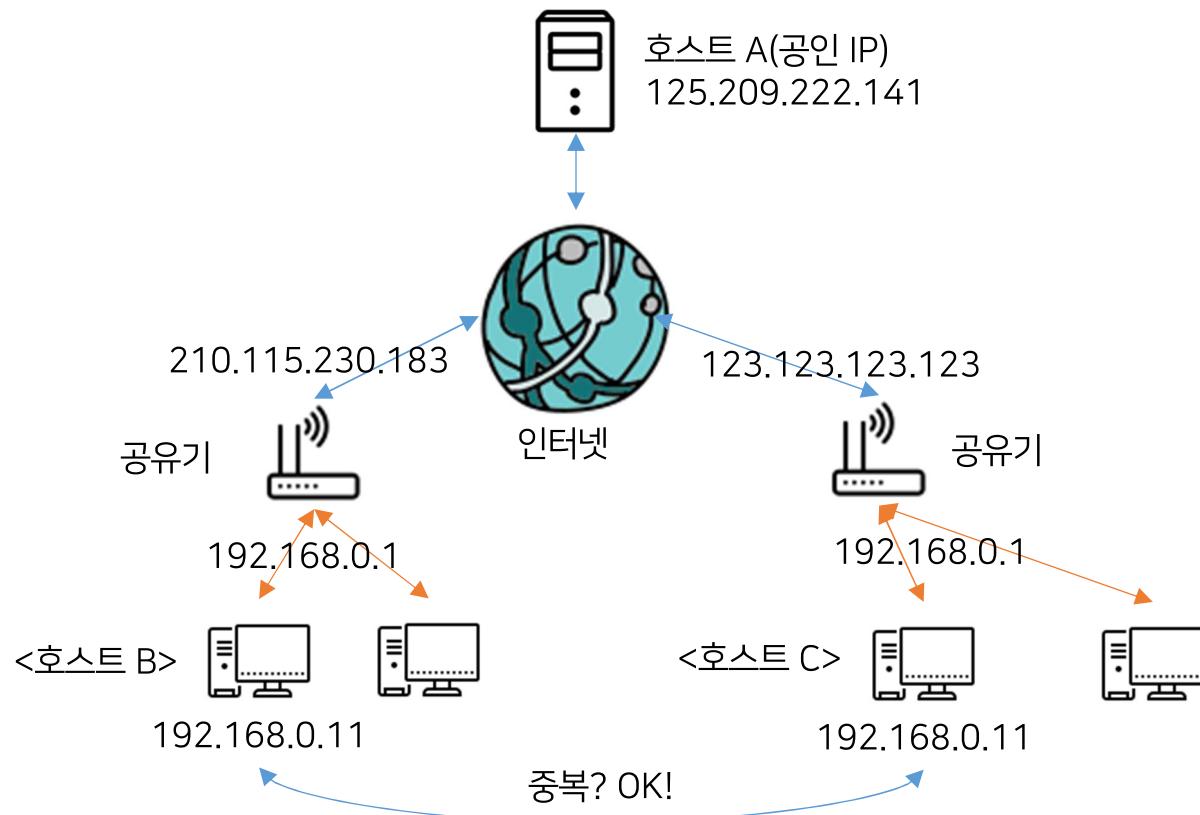


네트워크 : NAT, 포트 포워딩

(복습) IPv4 주소 체계에서, IP 주소의 부족 문제를 해결하기 위해 '사설 IP'가 도입되었습니다.



- 사설 IP 사용시 문제점
 - IP 주소가 중복 될 수 있어서, 목적지를 명확히 구분하기 어려움



[B가 A에 데이터 요청 시]

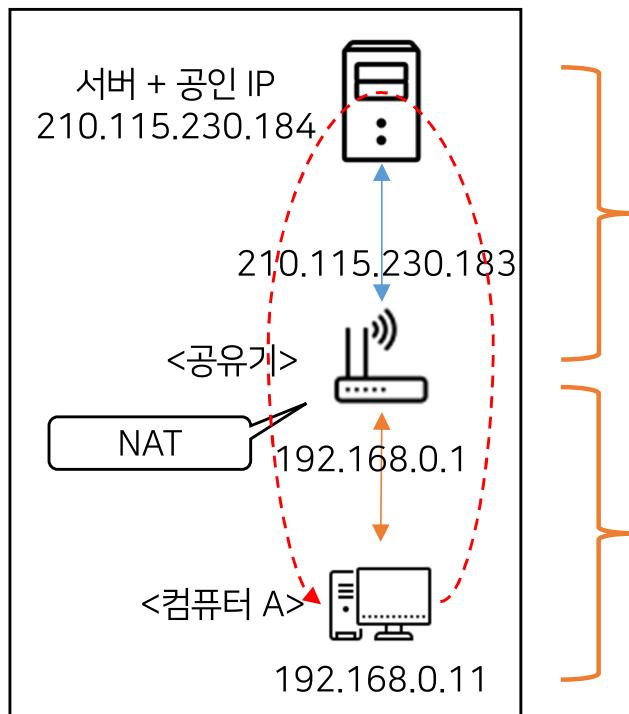
B에서 A의 주소(고유한 주소)로 요청 메시지 전송 가능. 하지만, A가 B로 데이터(=응답) 전송 시, B의 주소는 중복이어서 어떤 컴퓨터로 데이터를 보내야 할지 알 수 없음.

[A가 B로 데이터 요청 시]

B의 주소가 중복으로 사용 되어서, 어떤 컴퓨터에 요청 메시지를 보내야 하는지 알 수 없음.

네트워크 : NAT, 포트 포워딩

- 사설 IP(=중복 IP)를 공인 IP(=고유한 IP) **처럼** 활용하는 방법



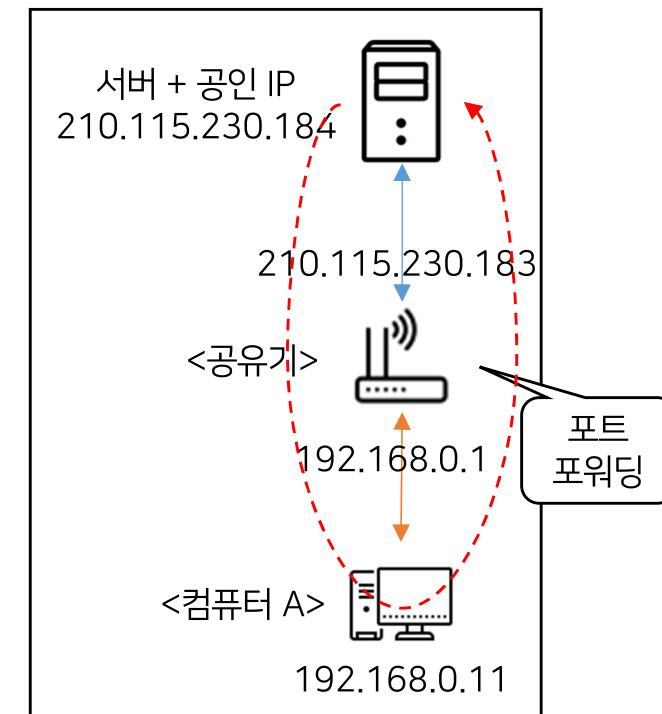
(공유기를
기준으로...)

외부 망

내부 망

(공유기를
기준으로...)

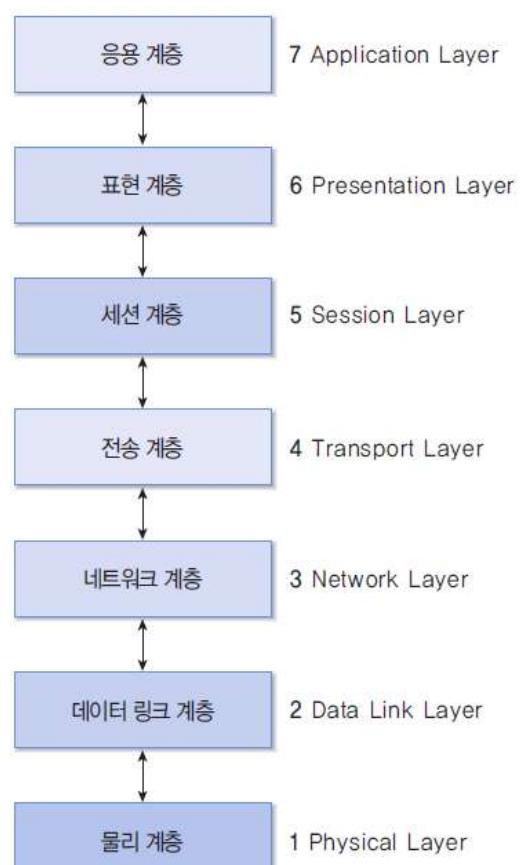
사설 네트워크에서 외부 네트워크를 접근하고,
응답을 받을 때 발생하는 IP 중복 문제를 해결



외부 네트워크에서 사설 네트워크를 접근할 때
발생하는 IP 중복 문제 해결

네트워크 : 계층 모델

- 서로 다른 호스트를 서로 연결하고 통신하려면 통신 방식을 표준화해야 함
 - 국제 표준단체 ISO는 OSI (Open System Interconnection) 7계층 모델을 제안하고, 네트워크에 연결된 시스템이 갖추어야 할 기능을 정의함
 - ISO의 OSI(Open System Interconnection) 7계층 모델 [그림 1-4]

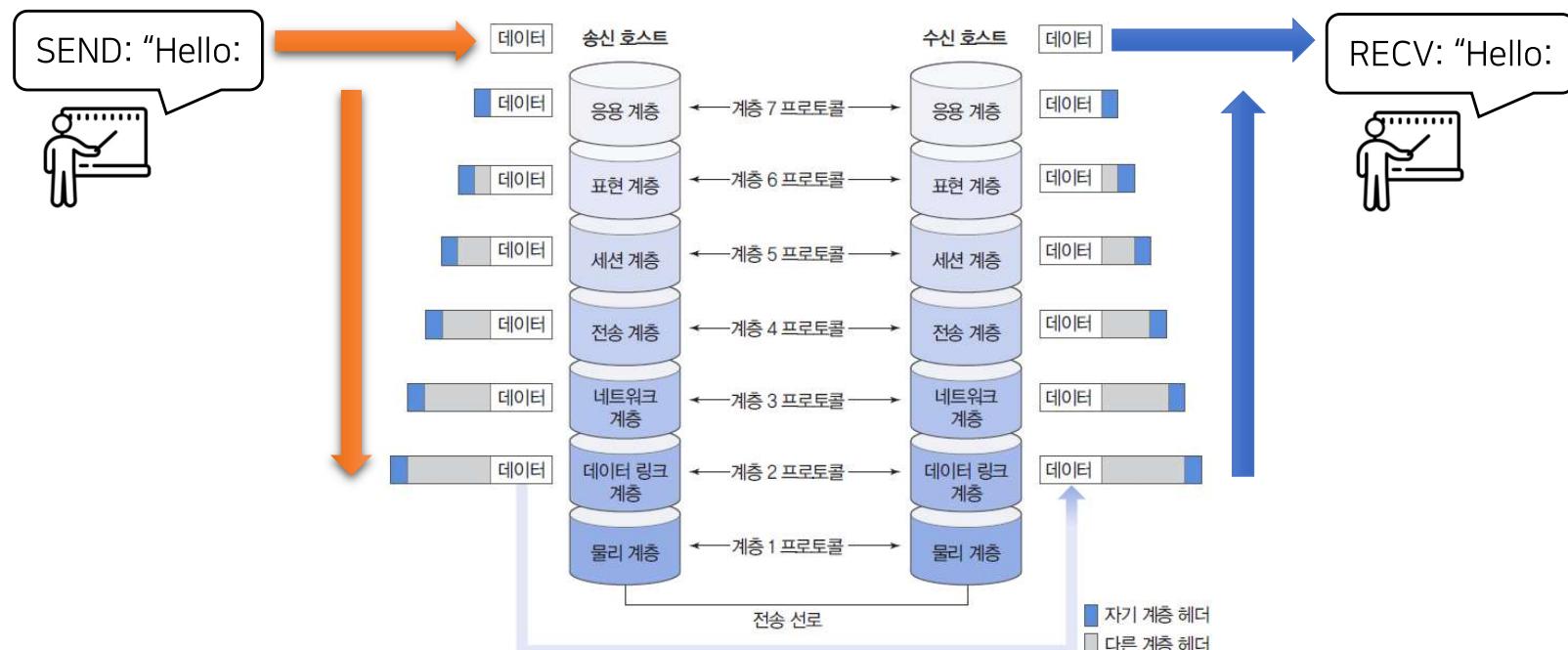


응용 계층	다양한 응용 환경/응용 프로그램을 지원
표현 계층	데이터의 표현 방법, 즉 데이터를 서로 다른 호스트가 인식할 수 있도록 하는 기능 제공 (+ 압축, 암호화)
세션 계층	대화 개념을 지원하는 상위의 논리적 연결을 지원 * 세션 연결을 지원
전송 계층	송수신 프로세스 사이의 연결 기능을 지원
네트워크 계층	올바른 전송 경로를 선택 (혼잡 제어 포함) * 보통은 라우터에서 수행
데이터 링크 계층	물리적 전송 오류를 해결 (오류 감지 / 재전송 기능) * 물리 계층에서 데이터 전송 시 noise 등으로 인해 전송 오류 발생 가능 및 네트워크 혼잡으로 인해 데이터가 유실 될 수도 있음
물리 계층	물리적으로 데이터/신호를 전송하는 역할을 수행

그림 1-4 OSI 7계층 모델

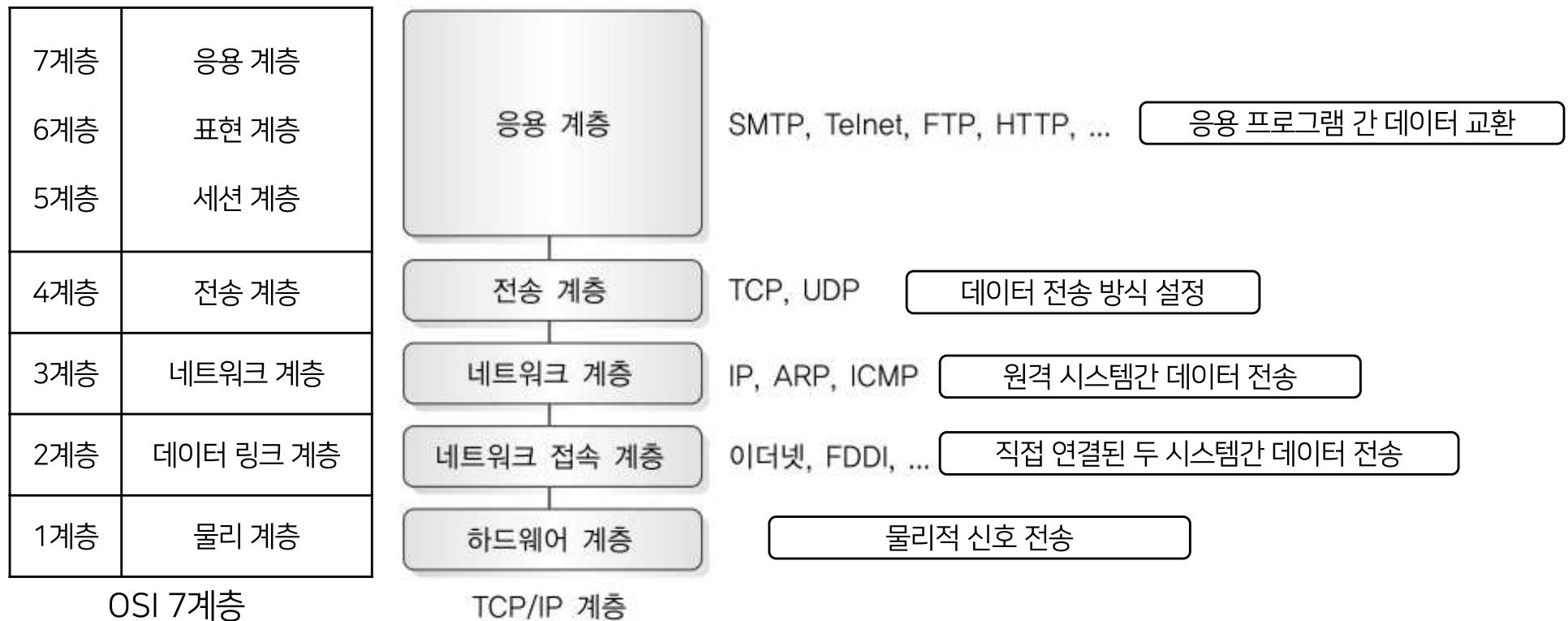
네트워크 : 계층 모델

- 네트워크에 연결된 호스트는 7개 계층으로 모듈화된 통신 기능을 갖춰야 함
 - 일반 사용자는 최상위 계층(응용 계층)을 통해 데이터 송수신을 요청
 - 이 요청은 하위 계층에 순차적으로 전달되고, 물리 계층을 통해 상대방에 전달됨
 - 상대방에 도달한 데이터는 반대방향으로 전달됨 (물리 계층 => 응용 계층)
 - 단, 실제 구현 시, 7개보다 더 적은 수의 계층으로 구현될 수 있음
 - 인터넷의 경우 TCP/IP라고 하는 4계층 (또는 5계층) 구조를 가짐



네트워크 : 인터넷 TCP/IP 계층 모델

- 인터넷 계층 구조 (인터넷 프로토콜 = TCP/IP)
 - 인터넷 표준 프로토콜은 OSI 7계층을 5계층(또는 4계층)으로 줄여서 사용



네트워크 : 인터넷 TCP/IP 계층 모델

- 인터넷 계층 구조 (인터넷 프로토콜 = TCP/IP)
 - 인터넷 표준 프로토콜은 OSI 7계층을 5계층으로 줄여서 사용
 - 또는, 하위 1,2 계층을 합쳐서 4계층으로 표현하기도 함

OSI 7 Layer

L7	응용 계층 (Application Layer)
L6	표현 계층 (Presentation Layer)
L5	세션 계층 (Session Layer)
L4	전송 계층 (Transport Layer)
L3	네트워크 계층 (Network Layer)
L2	데이터 링크 계층 (Data Link Layer)
L1	물리 계층 (Physical Layer)

TCP/IP 4 Layer

L4	응용 계층 (Application Layer)
L3	전송 계층 (Transport Layer)
L2	인터넷 계층 (Internet Layer)
L1	네트워크 액세스 (Network Access Layer)

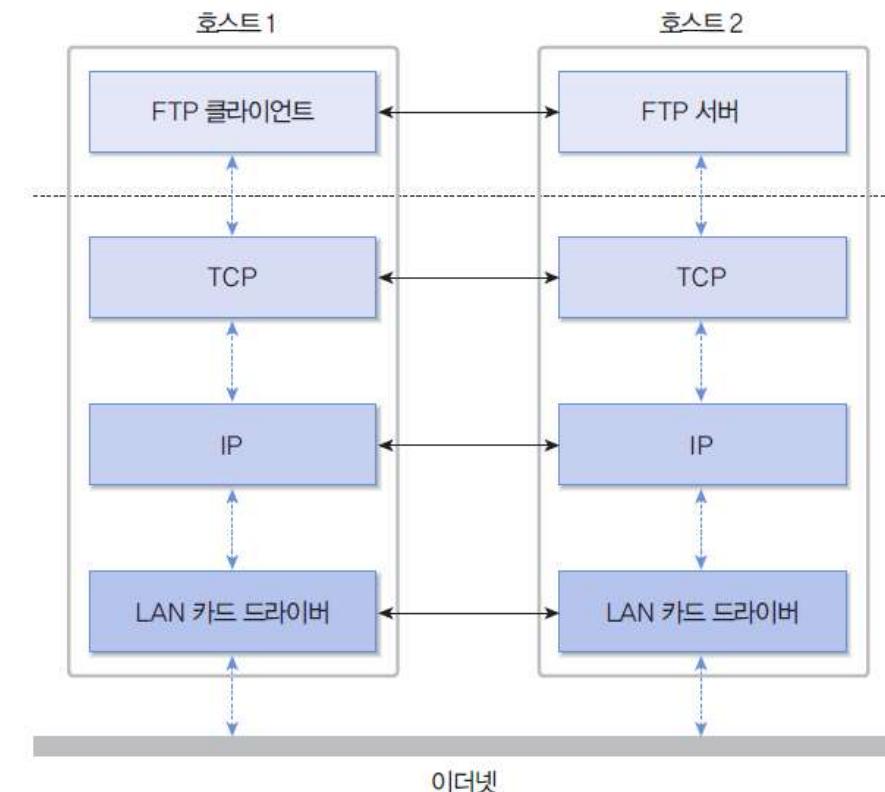


그림 1-6 FTP의 계층 구조

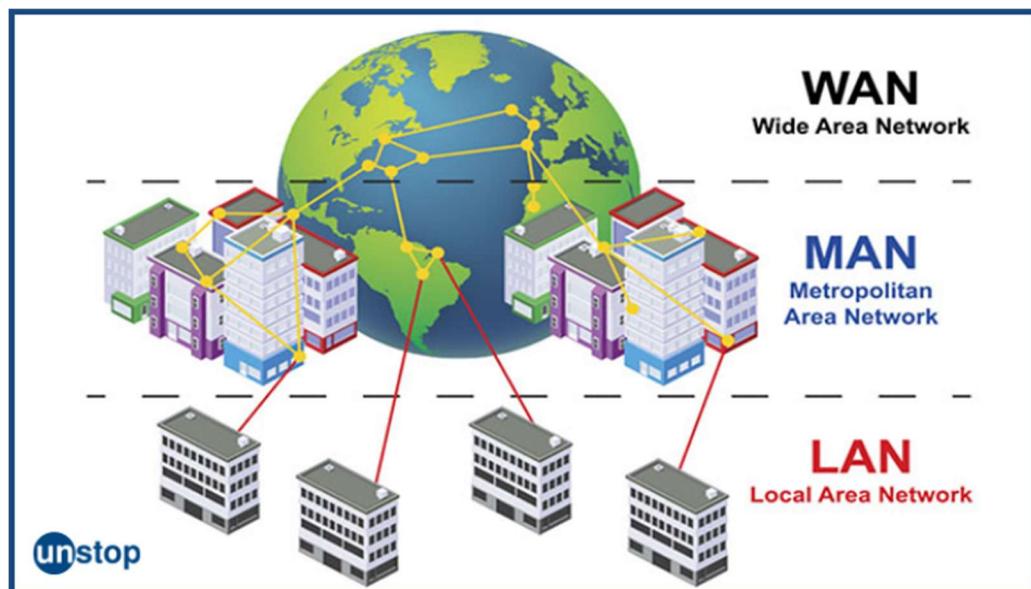
네트워크 : 교환 시스템

- 교환 시스템(Switching System)

- 현대의 네트워크는 대부분 Packet Switching 기반으로 동작함
 - 송신 호스트는 전송 데이터를 패킷으로 나누어 전송
 - 각 패킷은 독립적 경로 설정(라우팅) 과정을 거쳐 목적지에 도착
 - 장점 :
 - 전송 대역의 효율적 이용 : 동적으로 회선을 결정하여 패킷을 전달
 - 호스트의 무제한 수용 : 회선 교환 방식은 고정 대역을 할당해야 하므로, 연결 수가 제한됨
 - 단점:
 - 패킷 별로 서로 다른 경로로 전송될 수 있어, 패킷의 도착 지연 시간이 가변적
 - * 참고: 지터(jitter)는 각 패킷들의 지연 시간 분포를 의미. 네트워크 상황에 따라 지터가 커질 수 있음

네트워크 : 규모에 따른 분류

- 네트워크의 크기/규모에 따른 분류
 - 네트워크는 물리적으로 떨어진 독립적인 호스트간 데이터 교환 환경을 지원함
 - 호스트 사이의 연결 거리를 기준으로 네트워크를 LAN, MAN, WAN으로 구분



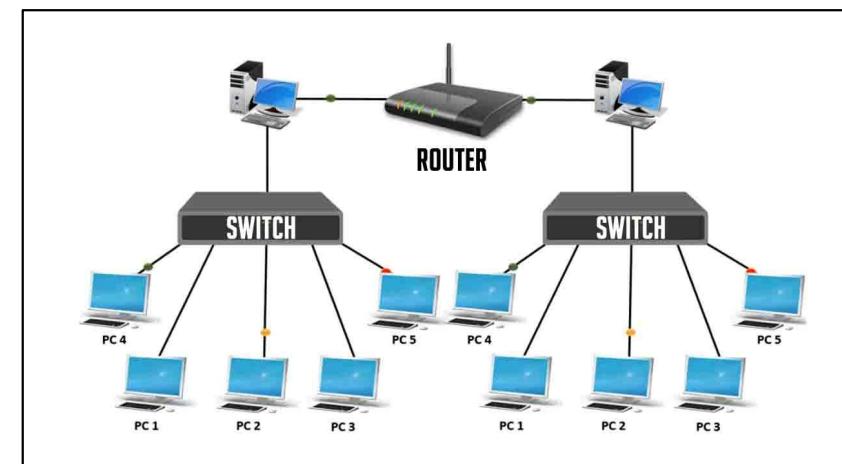
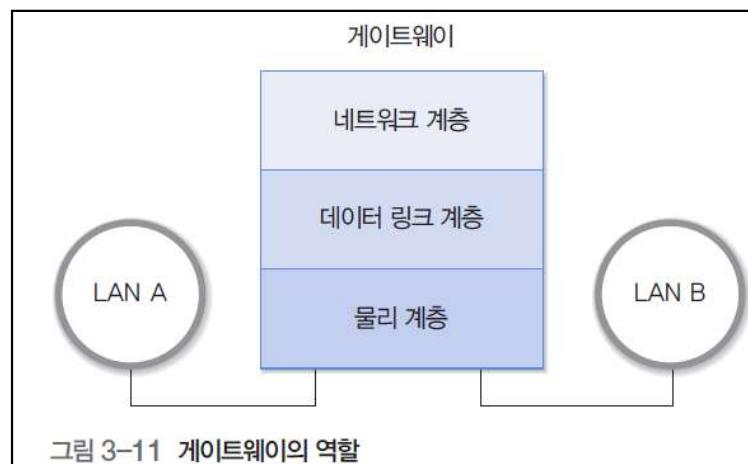
WAN, Wide Area Network (광역 통신망): 국가 이상의 넓은 지역을 지원하는 네트워크 구조

MAN, Metropolitan Area Network (도시권 통신망): LAN보다 큰 지역을 지원 (도시 규모)

LAN, Local Area Network (근거리 통신망): 소규모 지역 내에 위치하는 호스트로 구성된 네트워크 (집, 사무실, 건물, 학교 등)

네트워크 : 인터네트워킹

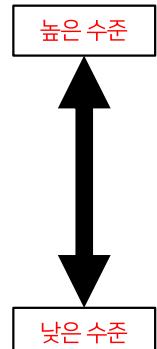
- 인터네트워킹: 둘 이상의 서로 다른 네트워크를 연결하는 것 또는 기술
 - 네트워크 연결을 위해서는 전용의 장비가 필요하며, 일반적으로 게이트웨이라 함
 - 게이트웨이 (GW): GW는 일반적인/개념적인/포괄적인 용어이며, 세부 기능에 따라 아래와 같이 분류
 - L1 리피터: 계층 1 기능 지원 (단순히 물리적인 신호를 증폭 & 전달)
 - L2 스위치: 계층 2 기능 지원 (MAC 주소 기반 프레임 전달 기능)
 - L3 라우터: 계층 3 기능 지원(IP 주소 기반의 라우팅/경로 기능 등) & 서로 다른 네트워크를 연결



스위치와 라우터를 이용한 네트워크 구성 예

네트워크 : 서비스 품질 (QoS)

- QoS (Quality of Service) : 통신/네트워크 서비스 품질을 의미
 - QoS는 포괄적이고 추상적으로 사용하는 개념이며, 구체적인 지표로 정의하여 사용 해야함
 - 예: 데이터 전송 속도, 데이터 전송 시간 또는 서비스 응답시간, 데이터 전송 신뢰성 등
 - 예: ITU-T(국제전기통신연합 전기통신표준화부문)에서 권고한 서비스 품질 등급



〈애플리케이션별 서비스 품질 등급〉		
QoS 등급	애플리케이션 예	시스템 메커니즘
0	실시간, 지연변이 민감형, 하이 인터액티브 애플리케이션 (고품질 VoIP, 고품질 비디오 회의등)	차별화 서비스를 위한 분리형 큐, 트래픽 관리
1	실시간, 지연변이 민감형, 인터액티브 애플리케이션 (VoIP, VTC)	
2	트랜잭션 데이터, 하이 인터액티브 애플리케이션 (시그널 링등)	분리형 큐, 폐기 우선순위
3	트랜잭션형 데이터, 인터액티브 애플리케이션	
4	에러민감형 애플리케이션 (짧은 트랜잭션, 벌크 데이터, 비디오 스트리밍등)	큰 사이즈의 큐, 폐기 우선순위
5	인터넷의 전통적 비보장형 애플리케이션	분리형 큐

〈IP QoS 등급 및 성능 목표값〉						
망 성능 파라미터	서비스 품질 등급					
	Class 0	Class 1	Class 2	Class 3	Class 4	Class 5
패킷 지연	100ms	400ms	100ms	400ms	1 s	미규정
패킷 지연변이	50ms	50ms	미규정	미규정	미규정	미규정
패킷 손실	1×10^{-3}	미규정				
패킷 에러			1×10^{-4}			미규정

네트워크 : 계층 별 주요 기능

- IEEE 802 시리즈
 - IEEE는 국제 표준화 단체로, 데이터 링크 계층과 관련된 다양한 LAN 표준안을 IEEE 802 시리즈로 발표 함
 - IEEE 802.1 : 표준안 전체 소개
 - IEEE 802.2 : (데이터 링크 계층의 상위 sub-layer인) LLC 계층을 소개
 - IEEE 802.3 부터 : 다양한 환경의 물리 계층과 MAC 계층을 소개
 - 802.3 : 이더넷으로 잘 알려진 CSMA/CD 방식 정의(공유 버스 기반)
 - 802.4 : 토큰 버스 방식 정의
 - 802.5 : 토큰 링 방식 정의

네트워크 : 계층 별 주요 기능

- L2 계층의 두 sub-layers
 - IEEE 802 표준은 L2 계층의 기능을 구분하고, 두 개의 sub-layer 구조를 제시함

Sublayer	Role
LLC (Logical Link Control)	<ul style="list-style-type: none">- Provides a consistent interface to the Network Layer (Layer 3), no matter what physical network is underneath.- Handles framing, error control, flow control (when needed), and addressing for higher layers.
MAC (Media Access Control)	<ul style="list-style-type: none">- Responsible for the actual addressing (MAC addresses) and controlling how devices access the physical transmission medium.- This part varies depending on whether the network is wired (Ethernet) or wireless (Wi-Fi), etc.

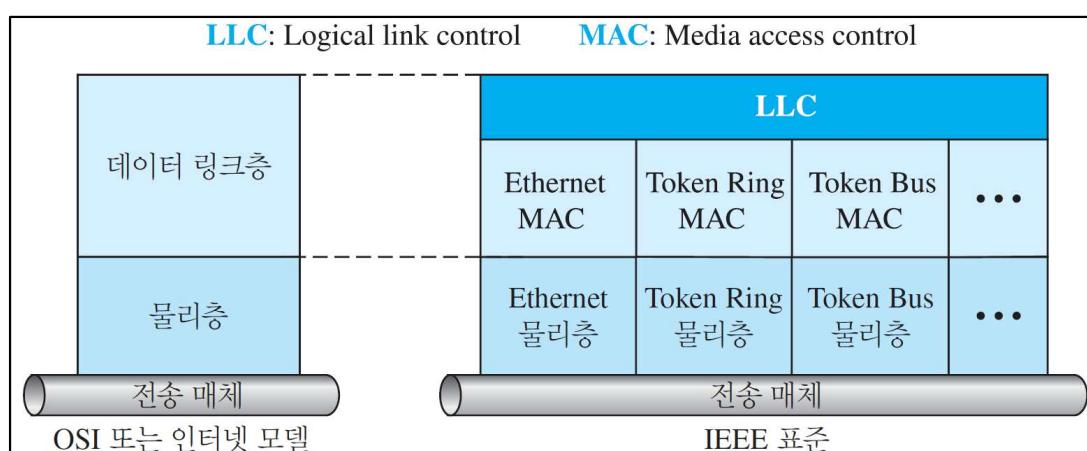
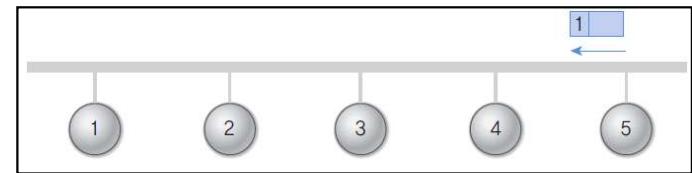


그림 5-2 IEEE 802 시리즈의 계층 구조

네트워크 : 계층 별 주요 기능

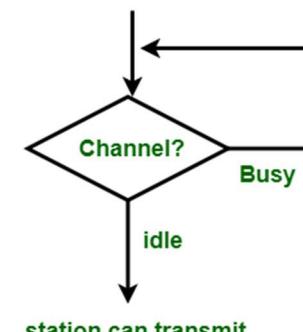
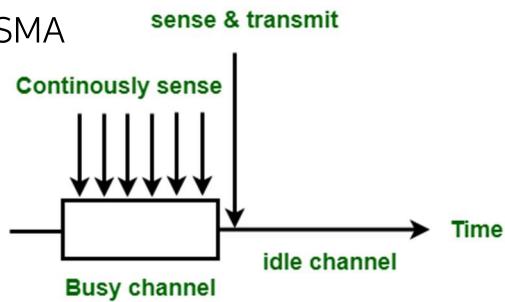
- L2 계층의 두 sub-layers
 - LLC (Link Layer Control) 계층 : IEEE 802.2 프로토콜
 - 데이터링크 계층(2계층)의 상위 sub-layer로, 하위 MAC 계층과 상위 네트워크 계층간 인터페이스 기능
 - (LLC 탑 2, 탑 3) ACK 전송, 흐름 제어, ARQ 기반의 오류 제어 기능 등을 수행함
 - (LLC 탑 1) ACK 전송, 흐름 제어 등. 단, 오류 제어 기능은 없음 // Ethernet은 LLC 탑 1을 사용함
 - MAC (Medium Access Control) 계층 : IEEE 802.3 계열 프로토콜(Ethernet)
 - MAC 주소 관리 및 매체 접근 방식을 제어
 - IEEE 802.3은 Ethernet으로 알려진 CSMA/CD 방식의 매체 접근 제어 기법을 정의하며, 공유 버스 기반의 네트워크에서 사용됨

네트워크 : 계층 별 주요 기능



- IEEE 802.3(Ethernet) MAC: CSMA/CD Carrier Sense Multiple Access/Collision Detection
 - 공유버스 토폴로지에서 매체에 접근하는 방법 및 충돌 해결 방법을 정의
 - 참고) 매체 접근 방법을 정의 = 언제 전송을 할 것인지에 대한 알고리즘을 정의하는 것
 - Carrier Sensing (높은 에너지 수준 센싱을 통해, 매체가 사용 중인지를 판단)
 - 공유 버스를 사용하고, de-centralized channel access를 수행하므로, 충돌 가능성은 항상 존재함
 - Collision Detection 기능을 통해, 충돌 발생 시 오류 복구(재전송)를 수행
 - Ethernet은 full-duplex 통신이 가능한 케이블을 사용하여, 전송 중에 collision 탐지가 가능
 - CSMA 방식은 1/non/p-persistent 방식으로 구분할 수 있는데, IEEE 802.3은 1-persistent 기법을 사용함

- 1-persistent CSMA



- 채널이 idle 상태가 될 때까지 지속적으로 센싱
- 채널이 idle 상태이면, 즉시 전송

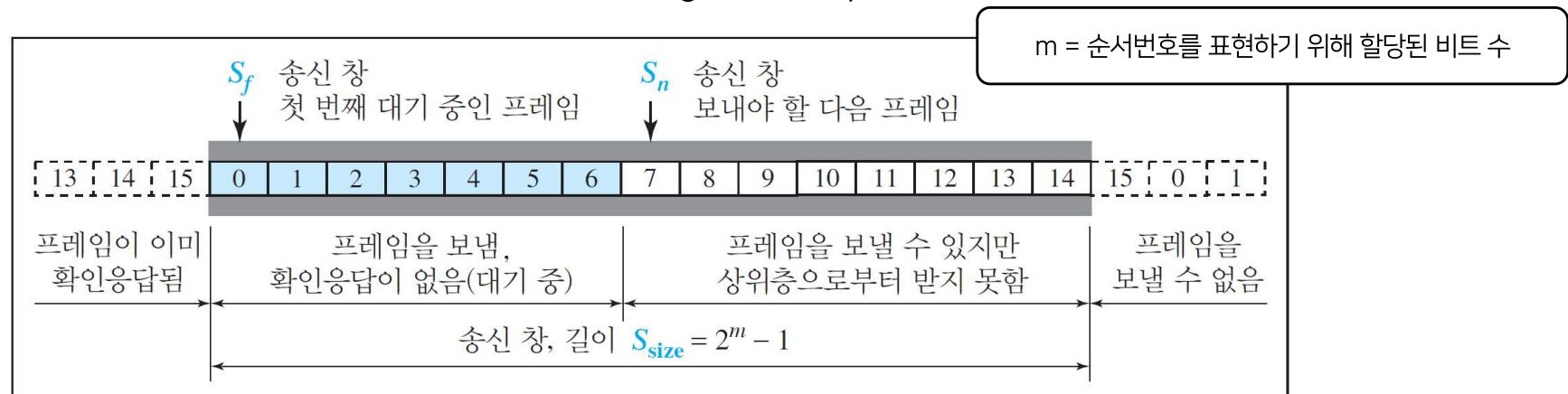
- non-persistent CSMA

- 채널이 IDLE이면 즉시 전송
 - 단, 채널이 BUSY이면 랜덤 한 시간동안 대기한 후 다시 센싱함 (1-pers. 대비, 충돌 확률이 감소함)

네트워크 : 계층 별 주요 기능

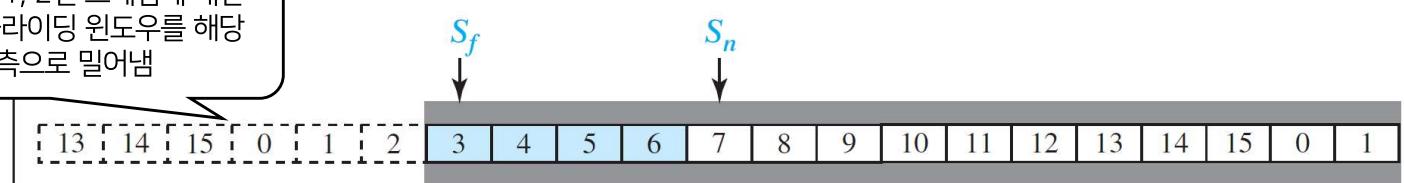
- LLC 계층의 흐름 제어

- 흐름 제어: 송신 단말의 데이터 프레임 전송 속도를 조절하는 것
 - 즉, 수신 단말에서 buffer overflow가 발생하지 않도록 송신 단말의 frame sending rate를 조절하는 것
 - 흐름 제어를 구현하기 위한 핵심 기능은 sliding window protocol



a. 밀어내기 전 송신 창

전송한 데이터 중, 0, 1, 2번 프레임에 대한 ACK를 받은 경우, 슬라이딩 윈도우를 해당하는 만큼 우측으로 밀어냄



b. 밀어낸 후 송신 창

슬라이딩 윈도우가 3칸 밀려나면서, 추가로 전송할 수 있는 3개 프레임을 확보함

네트워크 : 계층 별 주요 기능

- LLC 계층의 흐름 제어 : 대표적인 흐름 제어 알고리즘 소개
 - SW(Stop-and-Wait)
 - 하나의 프레임을 전송한 후, ACK를 받아야 다음 프레임을 전송할 수 있음
 - 구현이 간단하지만, 성능이 매우 떨어짐
 - GBN(Go-Back-N)
 - 슬라이딩 윈도우 프로토콜을 사용하여 N개의 프레임을 연속적으로 보낼 수 있음
 - 단, 수신 단말의 윈도우 크기가 1이어서, 전송 오류가 발생할 경우, 해당 프레임부터 뒤따르는 모든 프레임을 재전송
 - SR(Selective Repeat)
 - GBN을 개선하여, 수신 단말의 윈도우 크기를 송신 단말의 윈도우 크기와 같게 설정함
 - 전송 중간에 전송 실패한 프레임이 있으면 해당 프레임만 재전송
 - HARQ(Hybrid ARQ)
 - Forward Error Correction (FEC) 와 ARQ(자동 재전송)를 결합한 형태
 - 간단한 프레임 변형 오류는 수신 단말이 처리하고, 복잡한 오류는 재전송을 요청

네트워크 : 계층 별 주요 기능

- L3 계층의 주요 기능 : 라우팅(Routing)
 - 라우팅 : 패킷의 전송 경로를 지정하는 것
 - 정적 라우팅
 - 관리자가 사전에 설정한 라우팅 테이블에 따라 전송 경로를 설정
 - 단, 실시간으로 변화하는 네트워크 상황을 반영하지 못함
 - 동적 라우팅
 - 동적으로 변화하는 네트워크 상황에 따라 라우팅 테이블을 지속적으로 업데이트
 - 소스 라우팅
 - 송신 단말이 라우팅 경로를 계산한 뒤, 라우팅 경로 정보를 패킷에 담아서 보냄
 - 센서 네트워크 환경에서 사용됨

네트워크 : 계층 별 주요 기능

- L4 계층 (Transport Layer)
 - 대표적인 프로토콜 : TCP, UDP

구분	TCP	UDP
연결 지향?	연결지향형 프로토콜(사전에 연결을 맺고 데이터 송수신을 수행)	비 연결지향형 프로토콜 (사전에 연결을 맺지 않고 데이터 송수신)
안정성?	안정적 연결(혼잡 제어, 흐름 제어 기능 지원)	비 안정적 연결
신뢰성?	재전송 기반의 신뢰성 있는 전송 (오류 발생 시 재전송)	신뢰성을 보장하지 않음
패킷 단위 명칭?	패킷 단위를 세그먼트라고 함	패킷 단위를 데이터그램이라고 함
서비스 구분?	바이트 스트림 서비스 (데이터의 경계를 구분하지 않음. 즉, 하나의 연결에서 전송되는 패킷들은 연속적인 바이트처럼 취급)	메시지 스트림 서비스 (메시지 단위로, 경계가 구분된 단위의 데이터를 전송함)
장단점?	신뢰성을 보장하지만 UDP 보다는 처리 속도가 느림 (연결 수립에 시간이 소요되고, 다양한 기능 지원을 위해 수행해야 하는 기능이 많음)	신뢰성을 보장하지는 않지만 신속하게 처리하며 프로토콜 오버헤드가 적음 (지원하는 기능이 많지 않아, 빠르게 처리 가능)
활용분야?	이메일, 온라인뱅킹, 파일 다운로드 등 데이터 전송에 신뢰성 보장이 필요한 분야	VoIP(음성 채팅), 시간 조회(단발성 서비스), 게임 컨트롤 정보 전송(실시간성 확보가 중요한 서비스)

네트워크 : 계층 별 주요 기능

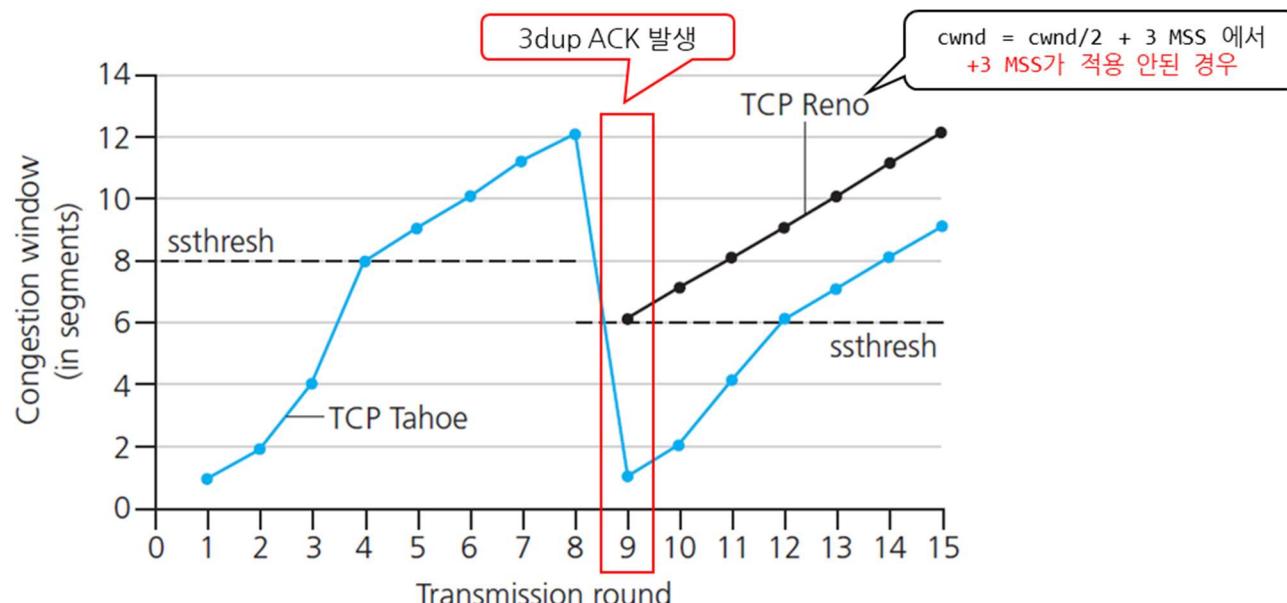
- TCP Congestion Control Algorithm (혼잡제어 알고리즘)
 - 종단간 혼잡 제어 (end-to-end congestion control) 방식의 일종
 - 혼잡이 감지되면, 송신 호스트는 전송 속도를 낮춤, 그리고 혼잡이 없거나 또는 해소 되었다고 판단되면, 송신 호스트는 전송 속도를 높임 (모든 결정은 end-host가 스스로 결정함)
 - 용어 설명
 - 'cwnd' : congestion window (혼잡 윈도우)
 - 송신 호스트가 ACK 없이 전송 가능한 최대 바이트 수 (= 송신 호스트의 전송 속도/transmission rate로 볼 수 있음)
 - $\text{LastByteSent} - \text{LastByteAcked} \leq \text{cwnd}$
 - 즉, ACK 없이 보낸 바이트 수는 cwnd를 초과할 수 없음
 - MSS (Maximum Segment Size)
 - 한 개의 세그먼트의 최대 크기(바이트 수)
 - RTT (Round Trip Time) : (송신 호스트 입장에서) 세그먼트를 보낸 시간부터 ACK를 수신한 시간의 차이
 - 혼잡을 탐지(=예상)하는 두 가지 방법
 - [Timeout] 전송한 세그먼트에 대해 타임아웃 발생
 - [3 dup(=duplicate) ACK] 동일한 ACK를 3번 수신 (= 즉, 동일한 순서 번호에 대한 ACK를 3번 수신)
 - 참고: ACK는 누적 ACK임 (=즉, ACK의 순서 번호가 N 이면, N번 이전까지의 데이터는 정상 수신 했고, N번 부터의 데이터를 받기를 기다린다는 것을 의미)

네트워크 : 계층 별 주요 기능

- TCP Congestion Control Algorithm (혼잡제어 알고리즘)
 - 혼잡 제어 알고리즘 (참고: 혼잡의 징후는 Timeout 및 3dup ACK이 있음)
 - TCP Tahoe 버전 혼잡 제어 알고리즘 동작 방식
 - 타임 아웃 발생 시: cwnd=1 MSS로 초기화 한 후, Slow Start에 따라서 cwnd 값을 증가
 - 3번의 중복 ACK 발생 시 (= 동일한 순서 번호에 대해 3개의 ACK 도착 시): 타임 아웃과 동일하게 cwnd=1 MSS로 설정 (Fast Recovery 없음).
 - TCP Reno 버전 혼잡 제어 알고리즘 동작 방식
 - Timeout은 혼잡이 명확하다고 판단하여 매우 조심하지만, 3dup ACK는 혼잡이 아닐 수 있으니까 전송 속도를 조금만 낮추는 방식으로 동작
 - Timeout 발생 시, cwnd=1 MSS로 초기화 한 후, Slow Start에 따라서 cwnd 값을 증가
 - 3dup ACK 발생 시, Fast Recovery 수행
 - Fast Recovery
 - 3번의 중복 ACK 발생 시 (= 동일한 순서 번호에 대해 3개의 ACK 도착 시):
 - (극심한 혼잡은 아니라고 판단하여) $cwnd = cwnd/2$ 로 설정하고, 3번의 중복 ACK 각각에 대해 $cwnd += 1 \text{ MSS}$ 동작을 수행
 - 결국, $cwnd = cwnd/2 + 3 \text{ MSS}$ 가 됨

네트워크 : 계층 별 주요 기능

- TCP Congestion Control Algorithm (혼잡제어 알고리즘)
 - Congestion Avoidance : 혼잡 상황 예방하기
 - Slow Start 방식으로 $cwnd$ 값을 계속 증가시키다가, $cwnd \geq ssthresh$ 가 되면, 매 RTT마다 $cwnd$ 를 1 MSS 만큼만 증가시킴 ($cwnd$ 를 무작정 키우면 혼잡이 발생할 수 있으니까, 일정 수준 이상으로 $cwnd$ 가 커지면, 증가 속도를 낮춤)
 - 'ssthresh'는 slow start threshold (임계치)를 의미하며, 타임아웃으로 인해 $cwnd = 1 MSS$ 가 되기 직전의 $cwnd$ 값의 $\frac{1}{2}$ 를 $ssthresh$ 값으로 설정.



끝