# 15 네트워크

## Section 1. 네트워크 기본

### 1. 네트워크

#### (1) 네트워크 개념

- Net + Work 의 합성어
- 컴퓨터와 같은 노드들이 통신 기술을 이용하여 그물망처럼 연결된 통신 이용 형태
- 2대 이상의 컴퓨터들을 연결하고 서로 통신할 수 있는 환경

#### (2) 네트워크의 장/단점

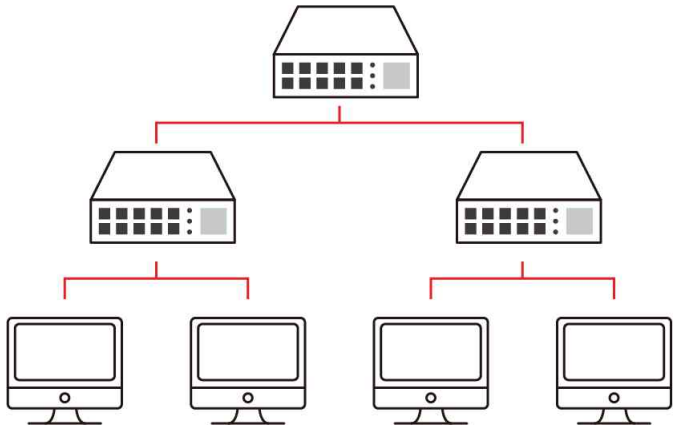
- 장점
  - 네트워크의 데이터 통신을 통해 많은 정보를 서로서로 공유할 수 있음
- 단점
  - 바이러스나 악성코드, 원치 않는 정보를 받게 될 수 있음
  - 해킹으로 인한 개인 정보 유출 등 네트워크가 다양하고 많은 단말기와 접속함으로 인해서 보안상의 문제점이 점점 커지고 있음
  - 데이터의 변조 가능

#### (3) 거리 기반 네트워크

- PAN(Personal Area Network)
  - 5m 전후의 인접 통신
- LAN(Local Area Network)
  - 근거리 네트워크로 사무실과 같은 소규모 공간 내의 고속 통신 회선
- MAN(Metropolitan Area Network)
  - LAN과 WAN의 중간 형태
- WAN(Wide Area Network)
  - 광대역 네트워크망으로 유관한 LAN간의 연결

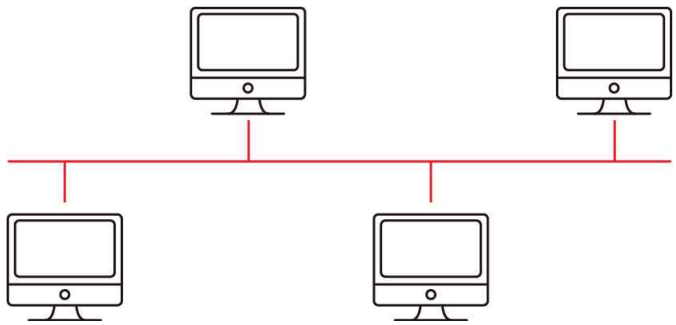
## 2. 네트워크 토폴리지(Network Topology)

### (1) 계층형(Tree)



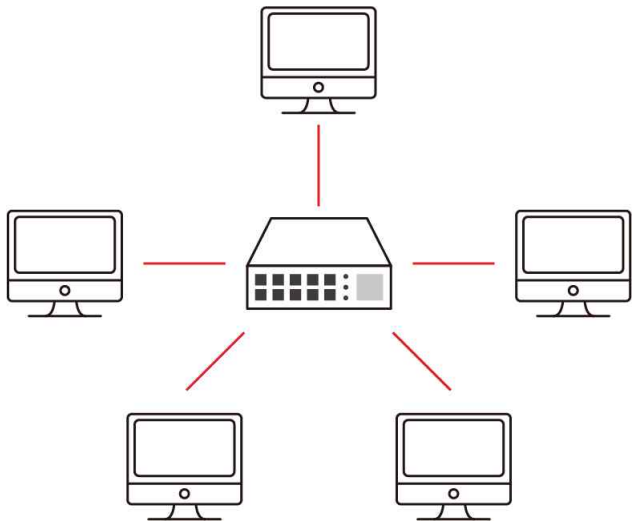
| | |
|---|---|
| 장점 | - 네트워크 관리가 쉽고, 새로운 장치를 추가하기 쉬움<br>- 네트워크의 신뢰도가 높음 |
| 단점 | - 트래픽 집중에 따른 속도 저하현상(병목현상)이 발생하기 쉬움<br>- 상위 노드 고장시 상위 네트워크와의 통신이 불가능 |

### (2) 버스형(Bus)



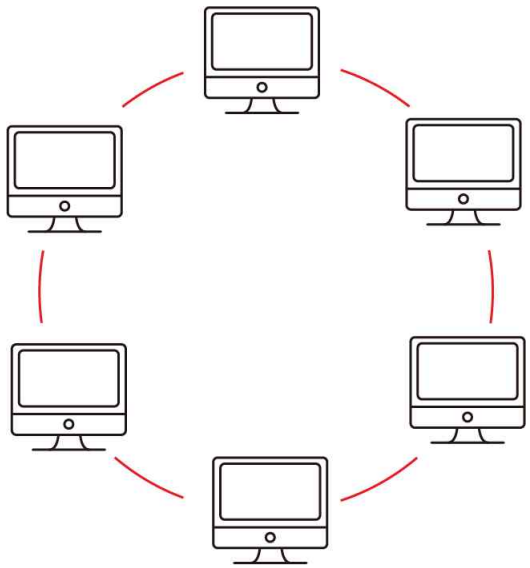
| | |
|---|---|
| 장점 | - 설치비용이 적고, 신뢰성 우수<br>- 구조가 간단하고, 새로운 노드 추가가 쉬움 |
| 단점 | - 네트워크 병목현상 발생이 쉬움<br>- 장애 발생시 전체 네트워크 마비 |

### (3) 성형(Star)



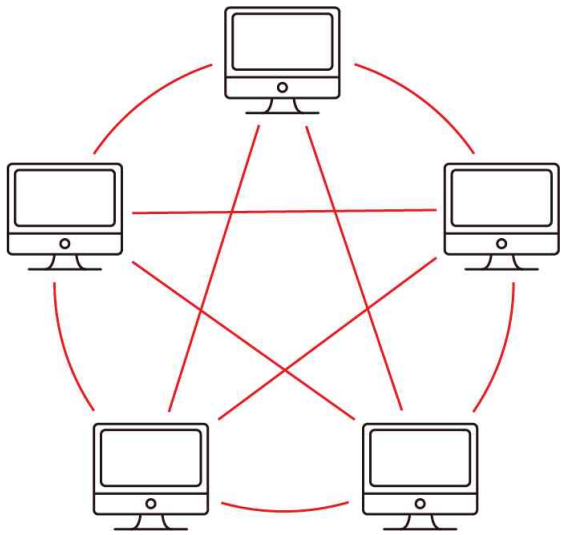
| | |
|---|---|
| 장점 | - 고속 네트워크에 적합<br>- 노드 추가가 쉬움<br>- 개별 링크 장애시에도 네트워크에 영향이 없음 |
| 단점 | - 중앙 노드 장애시 전체 네트워크 불통<br>- 노드 증가에 따라 네트워크의 복잡도 증가함 |

### (4) 링형(Ring)



| | |
|---|---|
| 장점 | - 저렴한 네트워크 구성이 가능함<br>- 충돌 현상이 발생하지 않음 |
| 단점 | - 네트워크의 구성을 변경하기 힘듦<br>- 링크 장애시 전체 네트워크 불통 |

### ⑸ 망형(Mesh)



| | |
|---|---|
| 장점 | - 완벽하게 이중화 되어 있으므로 장애에 강함<br>- 많은 양의 데이터 처리에도 문제 없음<br>- 회선수 : n(n-1) / 2<br>- 각 장치당 포트 수 : n-1 |
| 단점 | - 구축과 운영 비용이 고가 |

## 3. 데이터 전송

### (1) 아날로그/디지털 전송

#### ① 아날로그 전송

- 전송 매체를 통해 전달되는 신호가 아날로그 형태인 것
- 신호 감쇠 현상이 심하고, 오류의 확률이 높음

#### ② 디지털 전송

- 전송 매체를 통해 전달되는 신호가 디지털 형태인 것
- 제한된 거리에서의 감쇄 현상은 없으나 전송거리의 제한을 극복하기 위해 리피터(Repeater) 사용
- 신호 왜곡이 적기 때문에 정확한 데이터 전송이 가능
- 리피터에 의해 잡음을 제외한 원래의 신호만 복원 가능
- 장거리 전송이 가능

### (2) 방향에 따른 구분

#### ① 단방향 통신(Simplex)

- 일방적으로 'A → B' 의 통신만 가능한 전송 방식(ex. 라디오, TV)


#### ② 반이중 통신(Half Duplex)

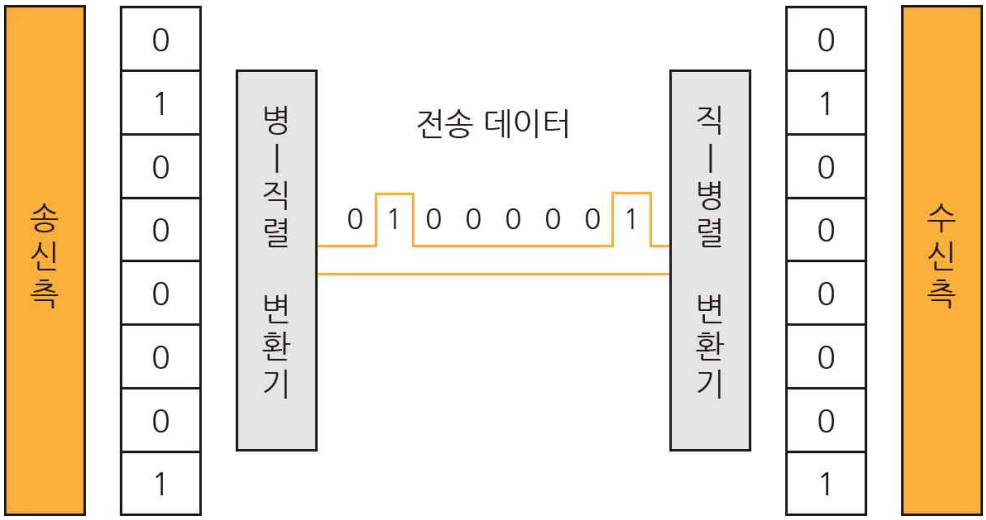
- 서로 데이터를 전송할 수 있지만, 하나의 회선을 사용하기 때문에 동시에 전송은 불가능(ex. 무전기)


#### ③ 전이중 통신(Full Duplex)

- 서로 언제나 필요한 데이터를 동시에 송수신 할 수 있는 전송(ex. 전화)

### (3) 직렬전송/병렬전송

#### ① 직렬전송(Serial Transmission)




- 한 번에 한 비트씩 순서대로 전송
- 데이터 전송 속도 느림
- 구축이 쉽고 경제적

#### ② 병렬전송(Parallel Transmission)


- 문자 단위 등 여러 비트를 동시에 전송하는 방식
- 데이터 전송 속도 빠름
- 흐름제어 필요

## (4) 동기 전송/비동기 전송

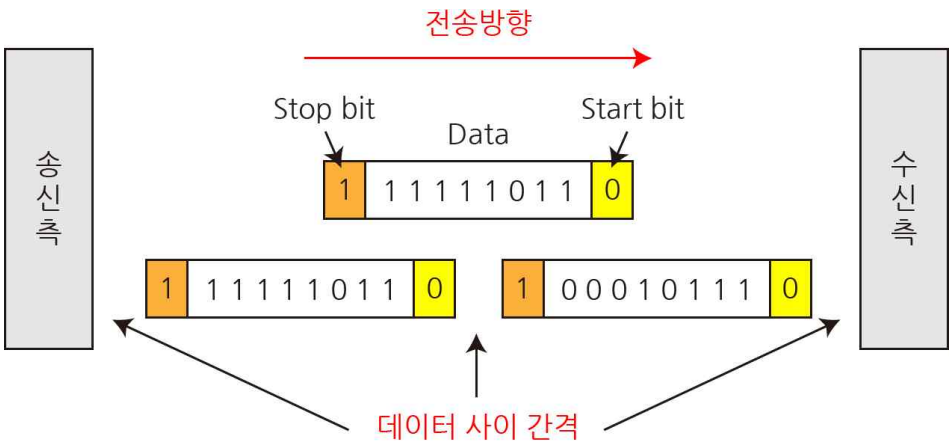
### ① 동기식 전송 방식(Synchronous Transmission)

- 한 문자단위가 아니라 여러 문자를 수용하는 데이타블럭 단위로서 전송하는 방식
- 양측에 설치된 모뎀이나 다중화기 등과 같은 기기에 의해 타이밍 조정
- 동기문자나 플래그 등을 사용하여 송수신측간의 데이타블럭을 수신해야 하기 때문에 터미널에는 버퍼장치가 요구됨
- 전송 효율이 높아 대부분의 통신 프로토콜에서 이용
- 문자 동기 방식과 비트 동기 방식이 있음
- 문자 동기 방식
  - SYN : 동기 맞춤 문자
  - STX(Start of Text) : 실제 전송할 데이터의 시작
  - ETX(End of Text) : 데이터의 종료


- 비트 동기 방식


### ② 비동기식 전송 방식(Asynchronous Transmission)

- 작은 비트블럭의 앞뒤에 각각 start bit와 stop bit를 삽입하여 동기화하는 방식
- start-stop 전송이라고 불리기도 한다.
- 각 문자와 문자의 전송사이에는 휴지기간이 존재하여, 스톱비트를 계속 전송
- 단순하고 저렴하지만 전송 효율이 낮다.
- 300bps ~ 1200bps 정도의 저속 전송에 사용



### ③ 동기/비동기 비교

| 구분 | 동기식 전송 방식 | 비동기식 전송 방식 |
|---|---|---|
| 통신 속도 | 고속 | 저속 |
| 회로 복잡도 | 복잡 | 단순 |
| 구축 비용 | 고가 | 저가 |
| 동기 제어 방식 | 클럭 동기 | Start bit, Stop bit |
| 전송 단위 | 블록 단위 전송 | 문자 단위 전송 |
| 적용 예 | 전화 교환망, ATM, 데이터 통신망 | RS-232C |

# Section 2. 근거리 통신망(LAN, Local Area Network)

## 1. LAN

### ⑴ LAN의 개념

- 여러 대의 컴퓨터와 주변장치 등이 통신 네트워크를 구성하여 통신하는 망
- 학교, 건물, 사무실 등과 같이 비교적 가까운 거리에 한정되어 있는 망

### ⑵ LAN의 특징

- 제한된 지역 안에서 다양한 장치들 사이에서의 통신
- 빠른 전송속도 및 높은 신뢰도
- 네트워크 구성의 최소 단위
- 다양한 통신장치와의 연결
- 네트워크 확장 및 재배치 용이

### ⑶ LAN의 구성요소

- NIC(Network Interface Card)
  - LAN CARD라고 불림
  - 컴퓨터를 전송매체에 연결해주는 장치
- 리피터(Repeater)
  - 거리가 길어질수록 감쇄되는 신호를 재생시키는 증폭기
- 허브(Hub)
  - 네트워크 케이블 집중 장치
- 브리지(Bridge)
  - LAN과 LAN을 연결하여 신호를 교환해주는 역할
- 라우터(Router)
  - 다른 망을 연결하기 위한 장치
  - 원거리의 연결(LAN, MAN, WAN) 가능
  - 라우팅 테이블을 만들어서 데이터 이동
- 게이트웨이(Gateway)
  - 다른 종류의 통신망 사이에 메시지를 전달할 수 있도록 해주는 장치

### ⑷ LAN의 전송방식

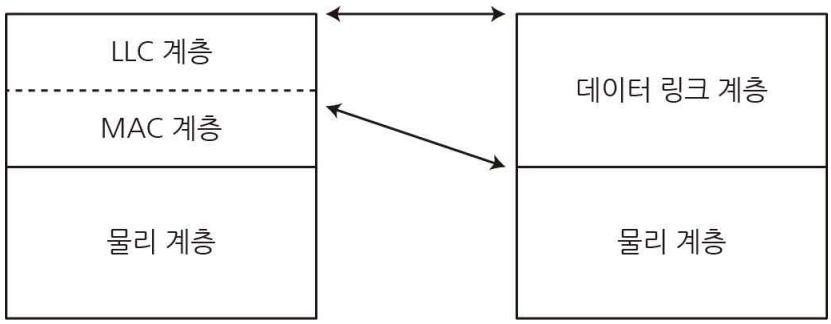
#### ① 베이스밴드(Base Band)

- 컴퓨터나 통신장치의 디지털 신호를 변조하지 않고 전송로를 이용하여 그대로 전송하는 방식
- 송수신 장치가 간단하고, 비용이 저렴
- 1~2Km 정도로 거리가 제한되어 있고, 그 이상 거리는 리피터를 사용
- 전송매체는 트위스트 페어 케이블, 동축 케이블을 많이 사용함

#### ② 브로드 밴드(Broad Band)

- 디지털 데이터를 모뎀을 이용하여 아날로그 데이터로 변조하여 전송하는 방식
- 주파수 분할 다중화(FDM) 방식을 이용
- 동시에 여러 정보 전송 가능

### (5) LAN의 프로토콜

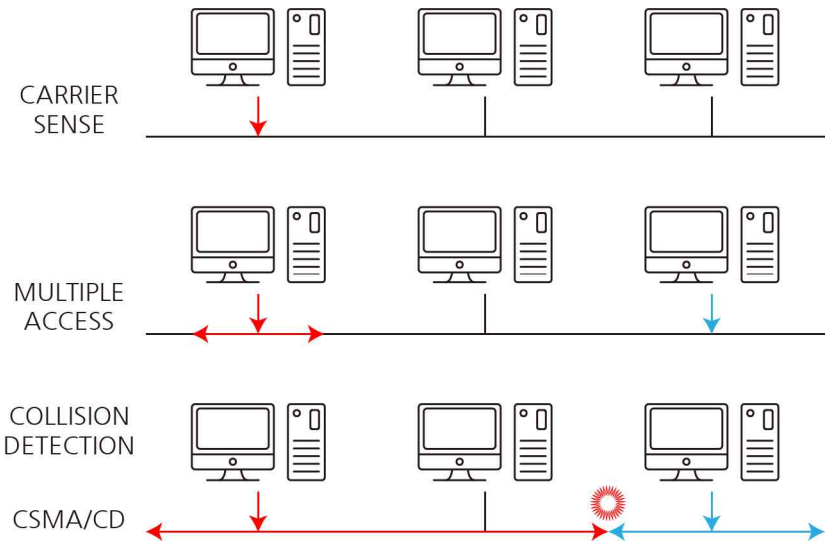



- LLC(Logical Link Control)
  - OSI에서 데이터 링크 계층 기능 담당 (흐름제어, 오류처리 등)
- MAC(Medium Access Control)
  - 물리적 전송 선로의 특징과 매체 간 연결 방식 제어
  - CSMA/CD, 토큰 링, 토큰 버스

## 2. LAN의 표준 802.X 시리즈

| 표준 | 설명 |
|---|---|
| 802.1 | - 전체의 구성, OSI 참조 모델과의 관계, 표준 규약 |
| 802.2 | - 논리링크제어(LLC)에 관한 규약 |
| 802.3 | - CSMA/CD에 관한 규약 |
| 802.4 | - 토큰 버스에 관한 규약 |
| 802.5 | - 토큰 링에 관한 규약 |
| 802.11 | - 무선 LAN에 관한 규약 |
| 802.15 | - 블루투스에 관한 규약 |

### (1) CSMA/CD(Carrier Sense Multiple Access with Collision Detection)



### ① CSMA/CD 개념

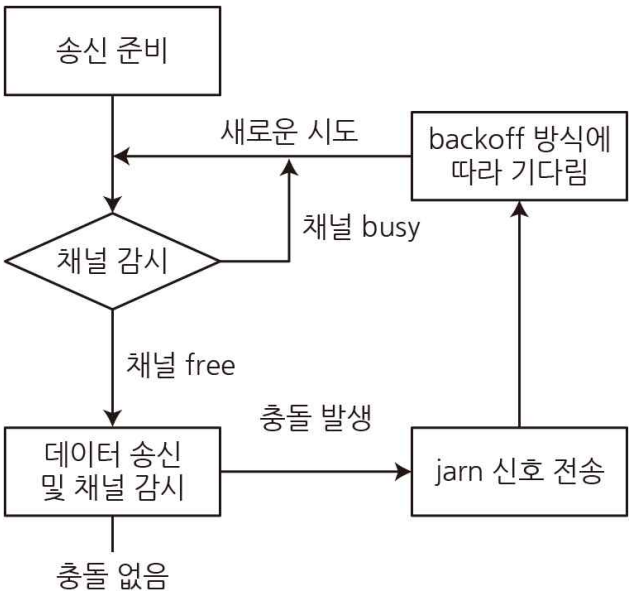
- IEEE 802.3 이더넷 LAN에서 사용되는 매체접근방식
- 유선 네트워크에서 충돌을 확인할 수 있는 방식

### ② 용어의 의미

- CS(Carrier Sense Multiple Access)
  - 채널 사용 전 다른 이용자가 있는지 확인하는 방식
- MA(Multiple Access)
  - 누구든 동시에 접근할 수 있는 방식
- CD(Collision Detection)
  - 충돌을 검사하여 제어하는 통신 방식

### ③ 주요 절차

- 네트워크를 사용하려는 컴퓨터는 현재 네트워크 상에 통신이 일어나고 있는지 확인한다.
- 현재 다른 데이터가 전송 중이면 사용할 수 있을 때까지 기다리고, 아니면 전송을 시작한다.
- 여러 컴퓨터에서 동시에 전송을 시작해 충돌이 발생하면 잼 신호를 브로드 캐스트 한다.
- 충돌 발생시 임의 시간 동안 기다린 뒤 다시 신호를 감지하고, 재전송한다.




### ④ 이더넷(Ethernet) 시스템 규격

- 10 BASE 2 : 얇은 동축 케이블을 이용하며, 2는 세그먼트의 최장거리가 200m
- 10 BASE 5 : 굵은 동축 케이블을 이용하며, 5는 세그먼트의 최장거리가 500m
- 10 BASE F : 광섬유 케이블을 이용하는 이더넷
- 10 BASE T : 10MBps의 전송 속도, 베이스 밴드 방식, Twisted Pair Wire 케이블 사용
- 고속 이더넷(Fast Ethernet) : 100 Base T 라고 불리는 이더넷의 고속 버전
- 기가비트 이더넷(Gigabit Ethernet) : 1GBps 의 전송속도를 지원

## ⑵ CSMA/CA(Carrier Sense Multiple Access with Collision Avoidance)

### ① CSMA/CA 개념

- IEEE 802.11 무선 LAN에서 사용되는 매체접근방식
- 무선 네트워크에서 충돌을 감지하기 힘들기 때문에 CSMA/CD대신 CSMA/CA 사용
- CSMA 방식에 충돌 회피 기능 추가
- 다른 컴퓨터가 네트워크를 사용중인지 판단하여, 사용중이라면 일정시간 동안 대기한다.

### ② 용어의 의미

- CS(Carrier Sense Multiple Access)
  - 채널 사용 전 다른 이용자가 있는지 확인하는 방식
- MA(Multiple Access)
  - 누구든 동시에 접근할 수 있는 방식
- CA(Collision Avoidance)
  - 충돌을 검사하여 피하는 통신 방식

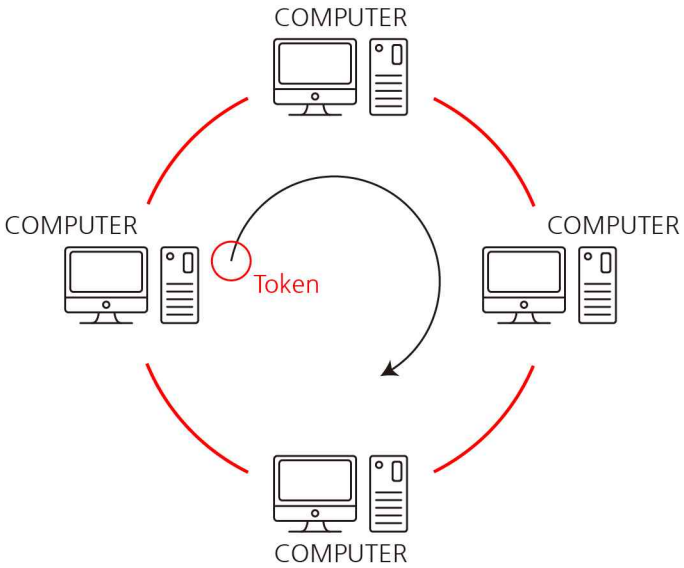
### ③ 802.11의 버전

| 버전 | 내용 |
|---|---|
| 802.11a | - 5GHz 대역에서, 802.11의 속도를 최대 54 Mbps까지 동작하는 확장 표준 |
| 802.11b | - 2.4GHz 대역에서 최대 11Mbps의 데이터 전송 속도를 지원 |
| 802.11e | - 무선 LAN 표준에 QoS 및 트래픽관리 기능을 추가 |
| 802.11g | - 802.11b의 뒤를 잇는 후속 표준<br>- 2.4GHz 대역에서 54Mbps 속도를 지원한다. |
| 802.11n | - 2.4GHz와 5GHz 두 주파수를 지원하며 최대 속도는 600Mbps |

## ⑶ 토큰 버스(Token Bus)

- 버스형(Bus) LAN에서 사용하는 방식으로, 토큰이 논리적으로 형성된 링(Ring)을 따라 각 노드들을 차례로 옮겨 다니는 방식
- 토큰은 논리적인 링을 따라 순서대로 전달되며, 토큰을 점유한 노드는 정보를 전송할 수 있고, 전송을 끝낸 후 토큰을 다음 노드로 전달
- 각 노드가 공평한 송신 권한을 가지며, 전송 시간을 가변적으로 조절할 수 있다.
- 전송량이 많을 때에도 안정적이고 액세스 시간이 일정하다.
- CSMA/CD방식보다 장치가 복잡하고 평균 대기 시간이 길다.
- 일부 노드나 통신 회선에 장애가 발생하면 전체적인 장애 발생

### (4) 토큰 링(Token Ring)




- 링형(Ring) LAN에서 사용하는 방식으로, 물리적으로 연결된 링(Ring)을 따라 순환하는 토큰(Token)을 이용하여 송신 권리를 제어
- 토큰 상태
  - 프리 토큰(Free Token) : 회선을 사용할 수 있는 상태
  - 비지 토큰(Busy Token) : 회선이 데이터 전송에 사용 중

### (5) 블루투스 규약(802.15)

| 버전 | 내용 |
|---|---|
| 802.15.1 | - 'Bluetooth'를 기반으로한 WPAN(Wireless Personal Area Network) 규격 |
| 802.15.2 | - WPAN 및 WLAN을 동시에 사용, 상호 간섭 해소 등 공존 |
| 802.15.3 | - 20Mbps 이상의 고속의 WPAN 규격 |
| 802.15.4 | - 저속의,저전력,저가형 WPAN 규격 |
| 802.15.5 | - WPAN에 의한 `Mesh Network` 구성 |
| 802.15.6 | - Body Area Network (체온, 심전도, 맥박, 삼축 가속도 등의 측정 기능) |
| 802.15.7 | - 가시광선 통신 (Visible Light Communication) |

# Section 3. 데이터 교환 방식과 다중화

## 1. 데이터 교환 방식

### (1) 회선망의 종류

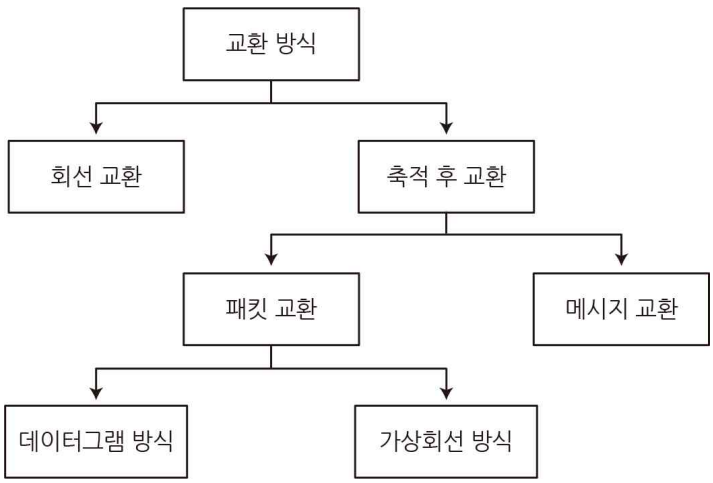
#### ① 전용회선

- 통신회선이 항상 고정되어 있는 방식
- 송수신 측을 일대일로 연결
- 전송 속도가 빠르고 전송 오류가 적다.
- 전송 데이터, 사용 시간이 많을 때 효율적
- 고장 발생 시 유지보수가 유리함
- 고가의 비용이 발생

#### ② 교환회선

- 교환기에 의해 송/수신 상호간이 연결되는 방식
- 전용회선에 비해 전송 속도가 느림
- 정보 보안을 위해 기밀성, 무결성을 고려해야 함
- 통신 장치와 회선 비용을 줄일 수 있다.

### (2) 데이터 교환 방식




#### ① 회선 교환 방식

- 두 지점을 교환기를 이용하여 물리적으로 접속시키는 방식
- 접속이 이루어지면 접속을 해제할 때까지 전용선처럼 사용 가능
- 고정 대역폭을 사용하고 동일한 전송 속도 유지

#### ② 메시지 교환 방식

- 축적 교환 방식으로 논리적 단위인 메시지를 교환하는 방식
- 교환기가 메시지를 모두 받고 저장하고 있다가 메시지와 주소를 확인 후 전송해주는 방식
- 응답시간이 빨라야 하는 데이터 전송에는 부적합한 방식

### ③ 데이터그램 교환 방식

- 데이터를 전송하기 전에 논리적 연결이 설정되지 않으며, 패킷이 독립적으로 전송된다.
- 각각의 패킷을 순서에 무관하게 독립적으로 전송
- 짧은 메세지의 패킷들을 전송할 때 효과적이고, 재정렬이 필요하다.

### ④ 가상회선 교환 방식

- 회선교환 방식과 데이터그램 방식의 장점을 결합한 기술
- 패킷을 전송하기 전에 논리적인 연결을 먼저 수행한다.
- 경로가 고정되면 다른 패킷을 나누어 전송한다.
- 데이터그램 보다 빠르고 안정적으로 통신할 수 있지만, 많은 사용자가 동시에 사용하기에는 한계가 있다.

## 2. 다중화(Multiplexing)

### (1) 다중화의 개념

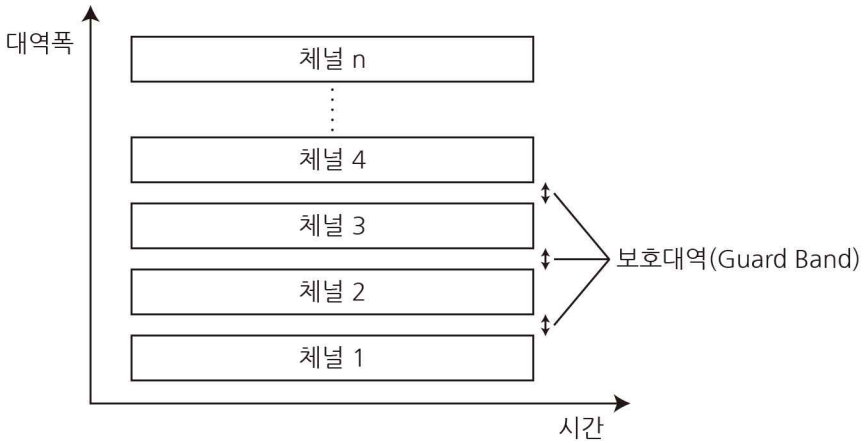
- 하나의 통신 회선을 여러 가입자들이 동시에 사용하도록 하는 기능
- 하나의 통신 회선에 다수의 터미널이 공유할 수 있도록 하는 기능
- 선로의 공동 이용이 가능하므로 전송 효율이 높아진다.

### (2) 다중화기(MUX, MultipleXer)

- 여러 개의 터미널 신호를 하나의 통신 회선을 통해 전송할 수 있도록 하는 장치

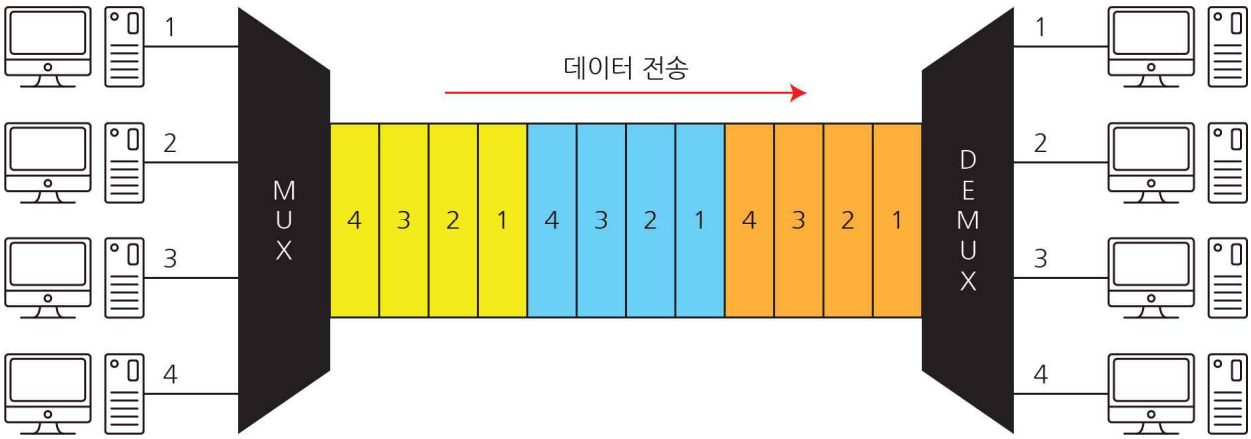
### (3) 다중화기 종류

### ① 주파수 분할 다중화기 (FDM, Frequency Division Multiplexer)




- 하나의 물리적 통신 채널을 여러 주파수 채널로 나누어 사용하는 다중화 방식
- 저속의 데이터를 각기 다른 주파수로 변조하여 통신 선로에 내보내는 방식
- 주파수 분할 다중화 자체가 변복조의 역할을 하므로 별도의 변복조기가 필요없음
- 저속도(1,200bps 이하) 아날로그 전송에 적합하며, 비동기 전송에 이용
- 각 채널 간의 완충 지역으로 Guard Band를 주어야 하므로 대역폭의 낭비가 발생
- 시분할 다중화기TDM)에 비해 비교적 구조가 간단하고 가격이 저렴
- 라디오나 TV 방송, CATV 등에서와 같이 여러 채널들을 동시에 전송하는 곳에서 활용된다.

### ② 시분할 다중화기 (TDM, Time Division Multiplexer)




- 한 전송로의 데이터 전송 시간을 일정한 시간 폭으로 나누어 차례로 분배하는 방식
- 디지털 전송에 적합(아날로그 신호를 디지털 신호로 변환할 때 PCM 방식 사용)
- 각 채널이 고속 채널을 점유하고 있는 것으로 보이나 실제로는 배정된 시간만 사용
- 고속 전송이 가능하며 포인트 투 포인트 방식에 주로 이용
- 다중화 방식

| | |
|---|---|
| 동기식 시분할 다중화<br>(Synchronous TDM) | - 실제 송신할 데이터의 존재 유무에 관계없이 타임슬롯을 할당하여 전송<br>- 전송할 데이터가 없는 장치도 타임슬롯이 할당되므로 효율성이 떨어진다. |
| 비동기식 시분할 다중화<br>(Asynchronous TDM) | - 실제로 전송할 데이터가 있는 장치에만 타임슬롯을 할당<br>- 동기식 다중화에 비해 전송 효율이 높다.<br>- 통계적 시분할 다중화 방식, 지능형 다중화 방식이라고도 한다. |

### ③ 코드 분할 다중화 (Code Division Multiplexer, CDM)

- 고유의 코드를 이용한 다중화 방식
- 공통 주파수 대역을 통한 동시 전송을 위해 여러 데이터 신호를 결합하는 네트워킹 기술
- 여러 사용자가 단일 통신 채널을 공유 할 수 있는 경우, 이 기술을 코드 분할 다중 액세스(CDMA)라고 한다.
- 2차 세계 대전에서 개발 된 기술인 확산 스펙트럼을 사용하여 전송을 가로채거나 방해하지 않도록 한다.

### ④ 파장 분할 다중화 (Wavelength Division Multiplexing, WDM)

- 여러 파장대역을 통해, 동시에 전송하는 광 다중화 방식
- 레이저 빛의 다른 파장(다른 색)을 사용하여 여러 반송파 신호를 단일 광섬유에 적용하는 기술
- FDM 방식의 일종인 파장 다중화 방식
- 중장거리 통신에 주로 활용

### ⑤ 공간 분할 다중화 (Space-Division Multiplexing, SDM)

- 시간(TDM) 또는 주파수(FDM)가 아닌 공간 차원(SDM)에서 다중화하는 기술

### ⑷ 역다중화기와 집중화기

#### ① 역다중화기 (Inverse MUX)

- 하나의 고속회선으로부터 데이터를 받아 여러 개의 저속회원으로 쪼개어 전송하는 것
- 여러 개의 저속회선을 사용해 광대역의 전송속도를 얻을 수 있고, 하나의 채널에 장애가 발생해도 다른 채널로 계속 전송이 가능하다.

#### ② 집중화기(Concentrator)

- 여러 개의 저속회선으로부터 전송된 데이터를 버퍼에 축적한 후 이를 모아서 고속회선으로 전송하는 것
- 여러 개의 저속회선을 고속회선을 사용하여 전송하고자 할 때 사용한다.

# Section 4. 인터넷

## 1. 인터넷

### (1) 인터넷(Internet)의 개념

- TCP/IP 프로토콜을 기반으로 하여 전 세계 수많은 컴퓨터와 네트워크들이 연결된 광범위한 컴퓨터 통신망
- 인터넷은 1960년대 미국 국방성에서 군사적인 목적으로 구축한 알파넷(ARPANET)으로부터 시작되었다.
- 특징
  - 서로 동시에 참여할 수 있는 쌍방향 통신 제공
  - 인터넷은 유닉스 운영체제를 기반으로 한다.
  - 통신망과 컴퓨터만 있으면 시간과 장소에 관계없이 정보를 교환할 수 있다.
  - 인터넷에 연결된 모든 컴퓨터는 고유한 IP를 가진다.

### (2) 인터넷 서비스

- WWW (Wold Wide Web)
  - 텍스트, 그림, 동영상, 음성 등 인터넷에 존재하는 다양한 정보를 거미줄처럼 연결해 놓은 종합 정보 서비스를 말하며 HTTP프로토콜을 사용하는 하이퍼텍스트 기반으로 되어있다.
  - WWW를 효과적으로 검색할 수 있도록 도와주는 프로그램을 웹브라우저라고 한다.
- 전자우편 (E-MAIL)
  - 인터넷을 통해 다른 사람과 편지뿐만 아니라 그림, 동영상 등 다양한 형식의 데이터들을 주고받을 수 있도록 해주는 서비스
  - SMTP, POP3, MIME 프로토콜을 사용
- 텔넷 (Telnet)
  - 멀리 떨어져 있는 컴퓨터에 접속하여 자신의 컴퓨터처럼 사용할 수 있도록 해주는 서비스
- HTTP (Hyper Text Transfer Protocol)
  - 하이퍼 텍스트 문서를 전송하기 위해 사용되는 프로토콜
- FTP (File Transfer Protocol)
  - 파일 전송 프로토콜
- 아키 (Archie)
  - 익명의 FTP 사이트에 있는 FTP 서버와 그 안의 파일 정보를 데이터베이스에 저장해 두었다가 FTP서버의 리스트와 파일을 제공함으로써 정보를 쉽게 검색할 수 있도록 하는 서비스
- 고퍼 (Gopher)
  - 메뉴 방식을 이용해 손쉽게 정보 검색을 할 수 있도록 하는 서비스
- 유즈넷(USENET)
  - 분야별로 공통의 관심사를 가진 인터넷 사용자들이 서로의 의견을 주고받을 수 있게 하는 서비스

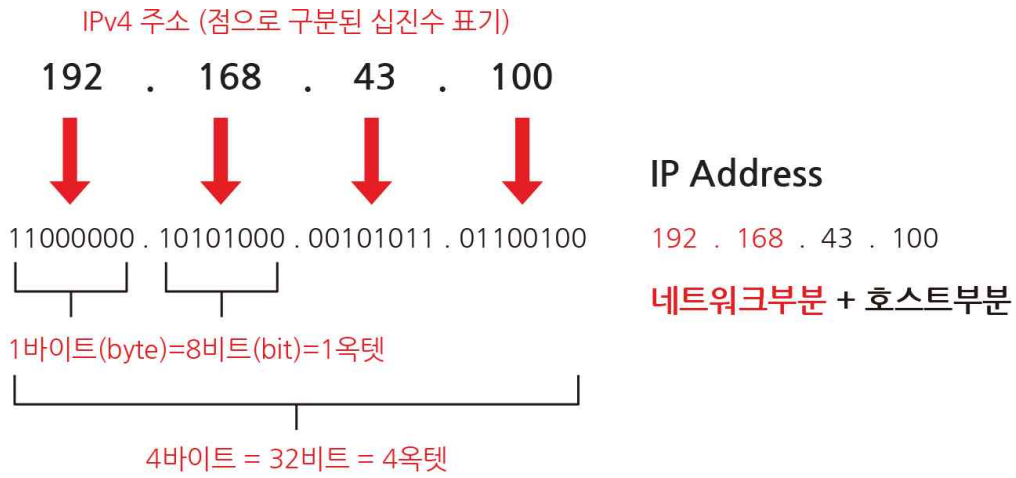
## 2. IP

### (1) IP(Internet Protocol address) 주소

#### ① IP의 개념

- 인터넷에서 컴퓨터를 식별할 수 있는 고유한 번호
- IPv4, IPv6 방식으로 나누어져 있고, 우리가 보통 사용하는 IP는 IPv4를 의미한다.
- 8비트씩 4부분, 총 32비트로 구성되어 있다.
- 패킷 크기는 64킬로바이트로 제한
- 네트워크 부분과 호스트 부분을 구분하기 위해 서브넷 마스크(Subnet Mask)를 사용한다.
- IPv4는 Class A ~ E, 5개 클래스로 분류하며 용도가 다르다.
- IPv4는 공인주소(Public Address)와 사설주소(Private Address)가 있다.

#### ② 표시형식




#### ③ 주소분류

- 유니캐스트(Unicast)
  - 단일 송신자와 단일 수신자 간의 통신
- 멀티캐스트(Multicast)
  - 단일 송신자와 다중 수신자 간의 통신
- 브로드캐스트(Anycast)
  - 같은 네트워크에 있는 모든 장비들에게 보내는 통신

#### ④ IP 주소 클래스

| 클래스 | 옥텟 IP | 최상비트 | 호스트 수 | 네트워크 수 | 용도 |
|---|---|---|---|---|---|
| A Class | 0 ~ 127 | 0 | 16,777,216 | 128 | 국가/대형 통신망 |
| B Class | 128 ~ 191 | 10 | 65,536 | 16,384 | 중대형 통신망 |
| C Class | 192 ~ 223 | 110 | 256 | 2,097,152 | 소규모 통신망 |
| D Class | 224 ~ 239 | 1110 | | | 멀티캐스트용 |
| E Class | 240 ~ 255 | 1111 | | | 실험용 |

## (2) IPv6

### ① IPv6의 개념

- IPv4의 주소 고갈 문제를 해결하기 위하여 기존의 IPv4주소 체계를 128비트 크기로 확장한 차세대 인터넷 프로토콜 주소

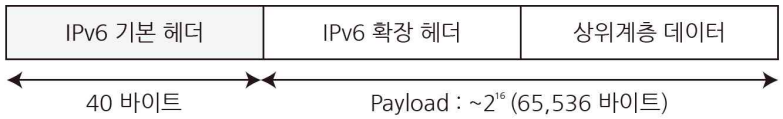
### ② 특징

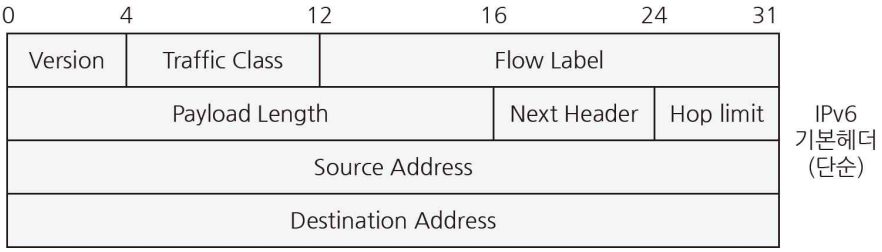
- 헤더의 내용을 확인하는 데 소요되는 오버헤드를 최소화하도록 설계
- 주소를 128비트로 표현한 확장된 주소 공간
- 계층적 주소 할당 체계
- 자동화된 주소 설정
- 기본으로 제공되는 보안기능
- 개선된 QoS 지원
- 헤더를 추가할 수 있는 확장성
- 패킷 크기 확장

### ③ 표시형식

- 16비트씩 8부분, 128비트로 구성되며, 콜론(:)으로 구분한다.
- EX) 2001:0DB8:1000:0000:0000:0000:1111:2222

### ④ IPv6 헤더




- IPv6 기본 헤더
  - 확장 헤더를 포함하지 않은 경우의 기본 헤더(40 바이트)
- IPv6 확장 헤더
  - 기본 고정 헤더 뒤 페이로드 내에 선택적인 확장 헤더들이 뒤따라옴

### ⑤ 주소분류

- 유니캐스트(Unicast)
  - 단일 송신자와 단일 수신자 간의 통신
- 멀티캐스트(Multicast)
  - 단일 송신자와 다중 수신자 간의 통신
- 애니캐스트(Anycast)
  - 그룹 내 가장 가까운 수신자에게 전달

#### ⑥ IPv4/IPv6 전환기술

- 듀얼 스택(Dual Stack)
  - 장비들이 IPv4 및 IPv6 모두 지원, 동시 처리 가능
- 터널링(Tunneling)
  - IPv6 패킷을 IPv4 패킷 속에 캡슐화하여 사용하는 기술
- 주소 변환(Address Translation)
  - IPv6 시스템이 IPv4 수신자가 이해할 수 있는, 또는 그 반대로 헤더 변환하는 기술

### (3) IPv4 와 IPv6 비교

| 구분 | IPv4 | IPv6 |
|---|---|---|
| 주소길이 | 32비트 | 128비트 |
| 표시방법 | 8비트씩 4부분, 10진수로 표시 | 16비트씩 8부분, 16진수로 표시 |
| 주소개수 | 약 43억개 | 43억 * 43억 * 43억 * 43억 |
| 주소할당 | 비 순차적 할당 | 순차적 할당 |
| 품질제어 | 지원 수단 없음 | 품질보장이 용이 |
| 보안기능 | IPSec 프로토콜 별도 설치 | 확장기능에서 기본으로 제공 |
| 플로그앤플레이 | 지원 수단 없음 | 지원 수단 있음 |
| 모바일 IP | 곤란 | 용이 |
| 주소 유형 | 유니캐스트, 멀티캐스트, 브로드캐스트 | 유니캐스트, 멀티캐스트, 애니캐스트 |

## 3. 서브넷

### (1) 서브넷, 서브넷 마스크

#### ① 서브넷(Subnet)

- 하나의 네트워크가 분할되어 나눠진 작은 네트워크

#### ② 서브네팅(Subnetting)

- 네트워크 성능 보장, 자원을 효율적으로 분배하기 위해 네트워크 영역과 호스트 영역을 쪼개는 작업

#### ③ 서브넷 마스크(Subnet Mask)

- IP 주소에 대한 네트워크 아이디와 호스트 아이디를 구분하기 위해서 사용
- Mask 연산(AND 연산)을 활용하여 구분

## ⑵ 서브네팅 예

### ① 200.1.1.0 / 24 를 7개의 subnet 으로 나눌 경우

| 번호 | 구분 | 범위 | 네트워크 주소 | 브로드캐스트 주소 |
|---|---|---|---|---|
| 1 | 000 | 200.1.1.0~200.1.1.31 | 200.1.1.0 | 200.1.1.31 |
| 2 | 001 | 200.1.1.32~200.1.1.63 | 200.1.1.32 | 200.1.1.63 |
| 3 | 010 | 200.1.1.64~200.1.1.95 | 200.1.1.64 | 200.1.1.95 |
| 4 | 011 | 200.1.1.96~200.1.1.127 | 200.1.1.96 | 200.1.1.127 |
| 5 | 100 | 200.1.1.128~200.1.1.159 | 200.1.1.128 | 200.1.1.159 |
| 6 | 101 | 200.1.1.160~200.1.1.191 | 200.1.1.160 | 200.1.1.191 |
| 7 | 110 | 200.1.1.192~200.1.1.223 | 200.1.1.192 | 200.1.1.223 |
| 8 | 111 | 200.1.1.224~200.1.1.255 | 200.1.1.224 | 200.1.1.255 |

### ② 200.1.1.65/27의 서브넷 마스크

- 호스트 주소 중 3비트를 네트워크 아이디로 사용하여, 255.255.255.224 이 서브넷 마스크가 됨

### ③ 같은 네트워크 영역인지 확인

| 범위 | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 65 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1 |
| 224 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| AND | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |

| 범위 | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 94 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 0 |
| 224 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| AND | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |

| 범위 | 128 | 64 | 32 | 16 | 8 | 4 | 2 | 1 |
|---|---|---|---|---|---|---|---|---|
| 97 | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| 224 | 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |
| AND | 0 | 1 | 1 | 0 | 0 | 0 | 0 | 0 |

## 4. IP 기타기술

### (1) NAT(Network Address Translation)

#### ① NAT의 개념

- 외부서 알려진 공인 IP 주소와 사설 IP 주소를 사용하는 내부 네트워크에서 IP 주소를 변환
- 제한된 수의 인터넷 IPv4 주소 문제를 해결하기 위해 개발

#### ② 사용목적

- 인터넷의 공인 IP 주소를 절약할 수 있다.
- 사용자들의 고유한 사설망을 침입자들로부터 보호할 수 있다.

#### ③ 주소 할당 방식에 따른 NAT 종류

- Static NAT
  - 공인 IP주소와 사설 IP주소가 1:1로 매칭되는 방식
- Dynamic NAT
  - 여러 개의 공인 IP 주소 대비 사설 IP 개수가 많을 경우 사용하는 방식
- PAT(Port Address Translation)
  - 공인 IP 주소 1개에 사설 IP 주소 여러 개가 매칭되는 방식

### (2) DNS(Domain Name System)

- Domain Name을 IP Address로 바꾸어 주거나, 그 반대의 작업을 처리하는 시스템
- DNS 서버는 도메인 이름과 이에 대응하는 IP 주소에 관한 데이터베이스를 유지하고 있다가 원하는 컴퓨터에게 제공한다.

# Section 5. 프로토콜

## 1. 프로토콜

### (1) 프로토콜의 개념

- 컴퓨터나 통신장비들 사이에서 원활한 데이터 교환을 수행하기 위해 표준화한 통신 규약
- 통신을 제어하기 위한 표준 규칙과 절차의 집합으로 하드웨어와 소프트웨어, 문서를 모두 규정한다.

### (2) 통신 프로토콜의 기본요소

- 구문(Syntax)
  - 전송하고자 하는 데이터의 형식, 부호화, 신호 레벨 등을 규정
- 의미(Semantics)
  - 두 기기 간의 효율적이고 정확한 정보 전송을 위한 협조 사항과 오류 관리를 위한 제어 정보를 규정
- 타이밍(Timing)
  - 두 기기 간의 통신 속도, 메시지의 순서 제어 등을 규정

### (3) 프로토콜의 기능

- 단편화와 재결합
  - 단편화(Fragmentation) : 송신 측에서 전송할 데이터를 전송에 알맞은 일정 크기의 작은 블록으로 자르는 작업
  - 재결합(Reassembly) : 수신 측에서 단편화된 블록을 원래의 데이터로 모으는 작업
- 캡슐화(Encapsulation)
  - 단편화된 데이터에 송/수신지 주소, 오류 검출 코드, 프로토콜 제어 정보 등의 정보를 부가하는 작업
  - 데이터를 오류 없이 정확하게 전송하기 위해 캡슐화를 수행한다.
- 흐름제어(Flow Control)
  - 수신 측의 처리 능력에 따라 송신 측에서 송신하는 데이터의 전송량이나 전송 속도를 조절하는 기능
- 오류제어(Error Control)
  - 전송중에 발생하는 오류를 검출하고 정정하여 데이터나 제어 정보의 파손에 대비하는 기능
- 혼잡제어(Congestion Control)
  - 네트워크의 혼잡을 피하기 위해 송신측에서 보내는 데이터의 전송속도를 강제로 줄이는 기능
- 동기화(Synchronization)
  - 송, 수신 측이 같은 상태를 유지하도록 타이밍(Timing)을 맞추는 기능
- 순서 제어(Sequencing)
  - 전송되는 데이터 블록(PDU)에 전송 순서를 부여하는 기능
  - 연결 위주의 데이터 전송 방식에만 사용
- 주소 지정(Addressing)
  - 데이터가 목적지까지 정확하게 전송될 수 있도록 목적지 이름, 주소, 경로를 부여하는 기능
- 다중화(Multiplexing)
  - 한 개의 통신 회선을 여러 가입자들이 동시에 사용하도록 하는 기능
- 경로 제어(Routing)
  - 송/수신 측간의 송신 경로 중에서 최적의 패킷 교환 경로를 설정하는 기능

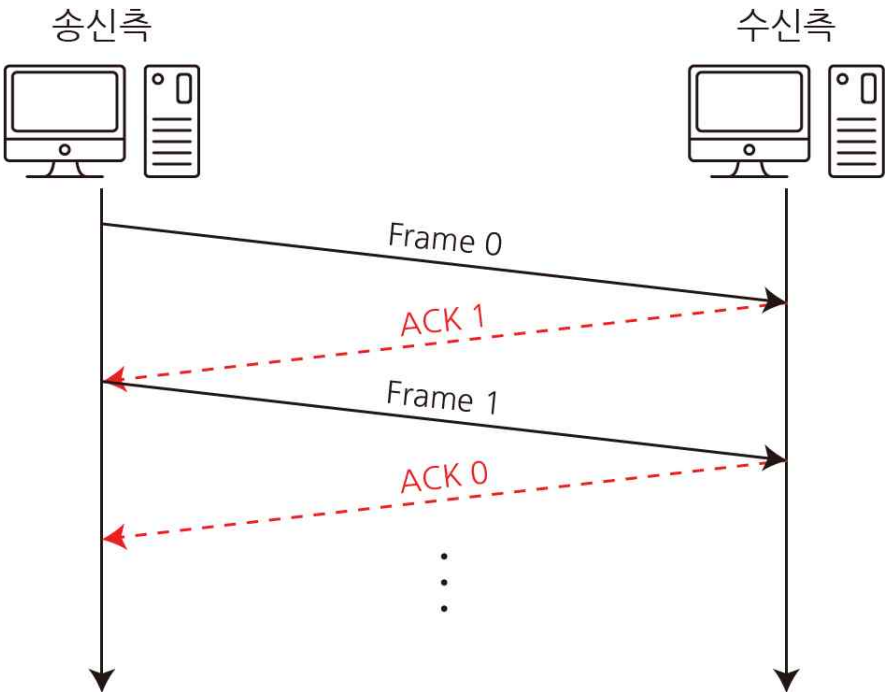
## 2. 흐름제어와 오류제어

### (1) 흐름제어

#### ① 흐름제어의 개념

- 수신 측의 처리 능력에 따라 송신 측에서 송신하는 데이터의 전송량이나 전송 속도를 조절하는 기능
- 송신측과 수신측의 데이터 처리 속도 차이를 해결하기 위한 기법
- Stop and Wait 방식, Sliding Window 방식

#### ② Stop and Wait 방식

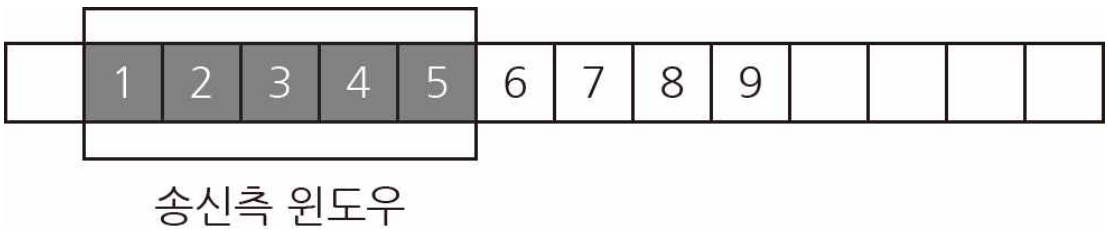



- 매번 패킷을 보낼 때마다, 확인을 한 후, 다음 패킷을 전송하는 방법
- 오버플로우가 일어날 수 없지만, 너무 느리다는 단점이 있다.
- Stop and Wait는 거의 사용되고 있지 않다.

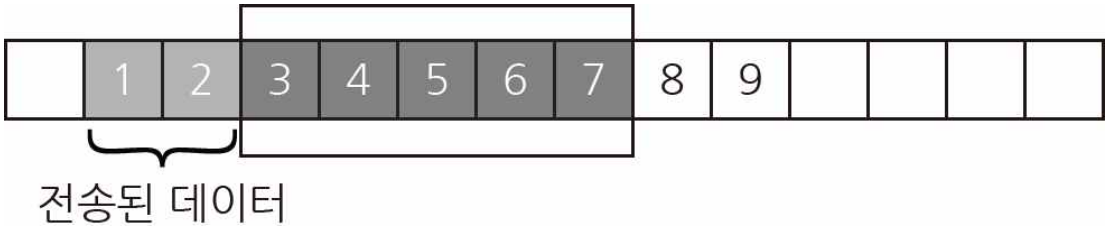
#### ③ Sliding Window 방식

- 수신측에서 설정한 윈도우 크기만큼 송신측에서 확인응답없이 세그먼트를 전송할 수 있게 하여 데이터 흐름을 동적으로 조절하는 제어기법
- 윈도우에 포함되는 모든 패킷을 전송하고, 전송이 확인되는 대로 윈도우를 옆으로 옮겨(slide) 다음 패킷들을 전송하는 방식
- Sliding Window 처리 방식(5개 윈도우 설정시)

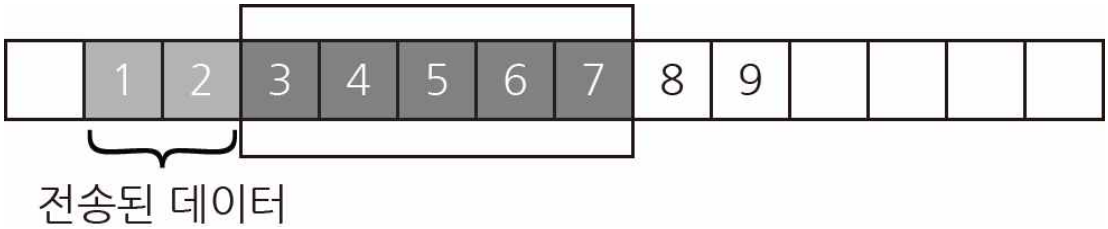
㉠ 송신측에서 1~5까지의 프레임 전송 가능



㉡ 데이터 1과 2를 전송하고, 3~5 데이터는 전송하지 않은 상태




㉢ 전송된 데이터에 대한 ACK 프레임 수신 후, ACK된 프레임만큼 윈도우 이동




#### ④ 피기배킹(piggybacking)

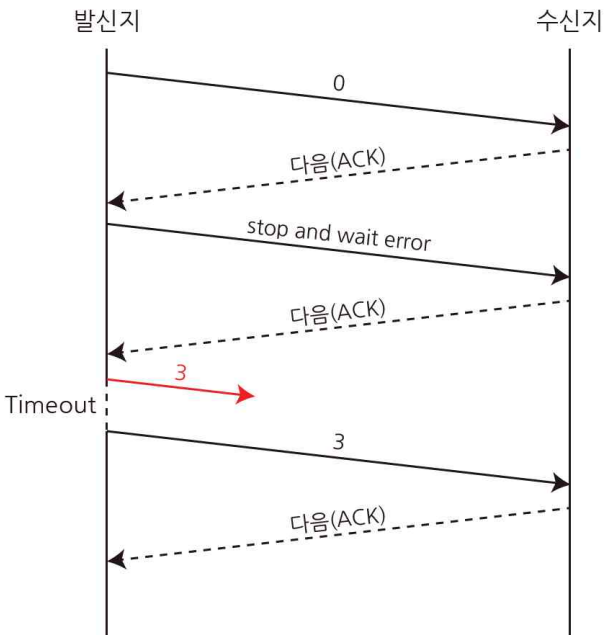
- 양방향으로 동시에 정보 프레임과 응답 프레임을 교차하여 전송하는 경우를 사용하는 방식
- 정보 프레임을 전송하면서 응답 기능까지 동시에 수행하도록 프레임 구조를 변형시킨 것
- 응답 프레임의 전송 횟수를 줄이는 효과가 있어 전송 효율을 높일 수 있다.

### (2) 오류제어

#### ① 오류제어의 개념

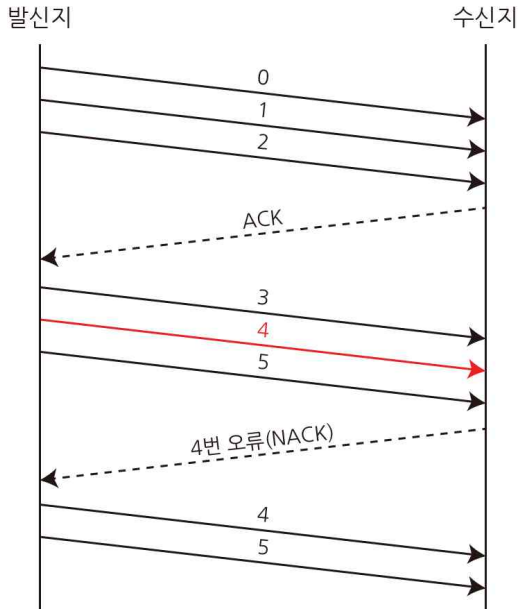
- 전송중에 발생하는 오류를 검출하고 정정하여 데이터나 제어 정보의 파손에 대비하는 기능
- TCP는 기본적으로 ARQ(Automatic Repeat Request), 재전송 기반 오류 제어를 사용한다.
- Stop and Wait 방식, Go Back N 방식, Selective Repeat, Adaptive ARQ 방식

#### ② Stop and Wait ARQ



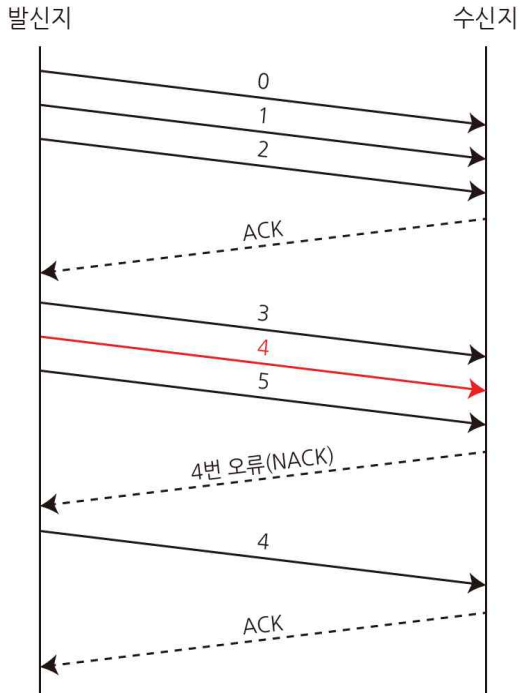

- 한 번 데이터를 보내면 제대로 받았다라는 응답이 올 때까지 대기하고 있다가 다음 데이터를 보내는 방식

### ③ Go Back N ARQ




- 오류가 난 지점부터 전송한 지점까지 모두 재전송하는 기법
- 데이터에서 에러가 발생했음을 감지하면 NACK 신호를 보내고, 오류 발생 이후 데이터를 모두 폐기한다.
- 중복전송의 단점이 있다.

### ④ Selective Repeat ARQ




- 여러 프레임을 연속적으로 전송하고, 수신측에서 NACK을 보내면 송신측에서는 오류가 난 부분의 프레임만 재전송
- 별도의 데이터 재정렬을 수행해야 하며, 별도의 버퍼를 필요로 한다.

#### ⑤ Adaptive ARQ

- 전송 효율을 최대로 하기위해 데이터 프레임의 길이를 동적으로 변경
- 전송 효율이 제일 좋으나, 제어 회로가 복잡하고 비용이 많이 든다.

### (3) 오류 발생 원인

#### ① 감쇠(Attenuation)

- 전송 신호가 전송 매체를 통과하는 과정에서 거리에 따라 점차 약해지는 현상
- 주파수가 높을수록 감쇠 현상이 심해진다.
- 중계기를 이용하여 감쇠현상을 해결한다.

#### ② 지연 왜곡(Delay Distortion)

- 주로 유선 전송 매체에서 발생
- 하나의 전송 매체를 통해 여러 신호를 전달했을 경우 주파수에 따라서 속도가 틀려져 생기는 오류

#### ③ 상호 변조 잡음(Intermodulation Noise)

- 서로 다른 주파수들이 하나의 전송 매체를 공유할 때 주파수 간의 합이나 차로 새로운 주파수가 생성된다.

#### ④ 충격 잡음(Impluse Noise)

- 순간적으로 높은 진폭이 발생하는 잡음
- 번개와 같이 외부적인 충격이나 기계적인 통신 시스템에서의 결함이 원인이다.

### (4) 전송 오류 제어 방식

#### ① 전진 오류 수정(Forward Error Correction, FEC)

- 재전송 요구 없이 수신 측에서 스스로 오류 검출 및 수정하는 방식
- 에러 발생할 경우 송신측에 통보하지 않음
- 오류정정을 위한 제어비트가 추가되어 효율이 떨어짐
- 해밍코드, 상승코드 방식

#### ② 후진 오류 수정(Backward Error Correction, BEC)

- 송신 측에 재전송을 요구하는 방식
- 패리티 검사, CRC, 블록 합 방식으로 오류를 검출하고, 오류 제어는 ARQ에 의해 이루어진다.

### (5) 오류 검출

#### ① 패리티(Parity) 검사

- 데이터 한 블록 끝에 1비트의 검사 비트인 패리티 비트를 추가하여 전송 에러를 검출하는 방식
- 홀수 개의 오류만 검출할 수 있고, 짝수 개의 오류는 검출하지 못하는 문제점이 발생
- 이를 해결하기 위해 Two-dimensional Parity Check(2차원 패리티 검사)가 있다.

#### ② 순환 중복 검사(Cyclic Redundancy Chcek, CRC)

- 데이터에 오류가 발생했는지 확인하는 코드를 데이터 뒤에 확장 데이터를 덧붙여 보내는 방식
- 프레임 단위로 오류 검출을 위한 코드를 계산하여 프레임 끝에 FCS(Frame Check Sequence)를 추가
- 집단적으로 발생하는 오류에 대해 신뢰성 있는 오류검출

### ③ 체크섬(Checksum)

- 간단하게 에러검출을 하는 방법
- 간단한 방식이기는 하나, 워드의 순서가 바꾸어지는 오류에 대한 검출은 하지 못함

### ④ 해밍코드(Hamming code)

- 수신측에서 직접 자기 정정 부호의 하나로 오류를 검출하고 수정까지 함
- 1Bit 의 오류만 수정가능
- 검출 가능한 최대 오류의 수 : 해밍거리 - 1
- 정정 가능한 최대 오류의 수 : (해밍거리 - 1) / 2

### ⑤ 상승코드

- 순차적 디코딩과 한계값 디코딩을 사용하여 오류수정
- 해밍코드처럼 검출과 정정 가능
- 여러 비트의 오류도 수정 가능

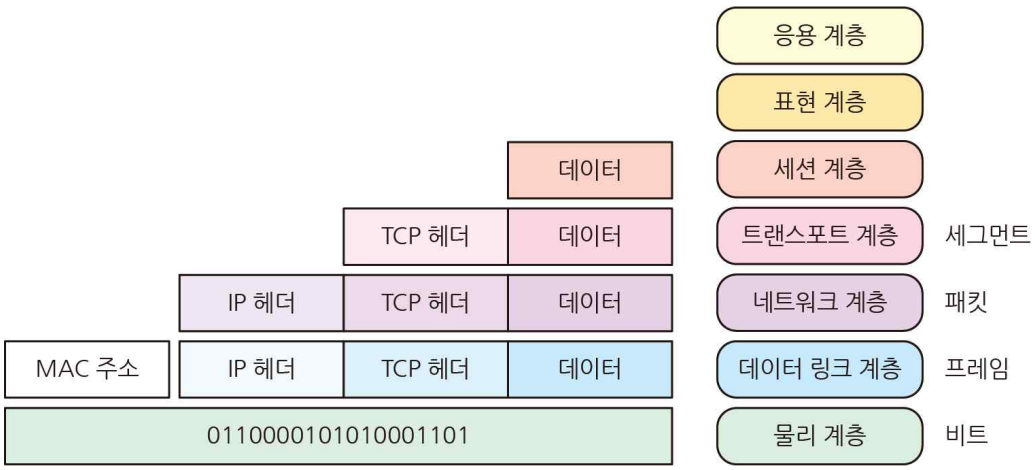
# Section 6. OSI 7계층

## 1. OSI (Open System Interconnection) 7계층

### (1) OSI 7계층 개념

- 네트워크 프로토콜 디자인, 통신을 7개의 계층으로 나누어 설명한 모델
- 국제표준화기구(ISO)에 의해 정립되었다.
- 통신이 일어나는 과정이 단계별로 파악할 수 있다.

### (2) OSI 7계층 구조




## 2. 계층별 특징

### (1) 물리계층(Physical Layer)

- 전기적, 기계적, 기능적인 특성을 이용해서 통신 케이블로 데이터를 전송
- 통신 단위는 비트이며 이것은 1과 0으로 나타내어지는, 즉 전기적으로 On, Off 상태이다.
- 데이터를 전달할 뿐, 데이터가 무엇인지 어떤 에러가 있는지 신경쓰지 않는다.
- 장비 : 통신 케이블, 리피터, 허브

### (2) 데이터 링크계층(DataLink Layer)

- 포인트 투 포인트(Point to Point) 간 신뢰성 있는 전송을 보장하기 위한 계층
- CRC 기반의 오류 제어와 흐름 제어가 필요
- 물리 계층에서 발생할 수 있는 오류를 찾아내고, 수정하는 데 필요한 기능적, 절차적 수단을 제공
- 물리주소인 MAC주소가 이 계층에 해당한다.
- 장비 : 스위치, 브리지

### (3) 네트워크 계층(Network Layer)

- 데이터를 목적지까지 가장 안전하고 빠르게 전달하는 기능(라우팅)
- 여러 개의 노드를 거칠 때마다 경로를 찾아주는 역할을 하는 계층
- 주소부여(IP), 경로설정(Route)
- 장비 : 라우터, L3 스위치

### (4) 전송 계층(Transport Layer)

- 양 종단간(End to end)의 사용자들이 신뢰성있는 데이터를 주고받을 수 있도록 해준다.
- 시퀀스 넘버 기반의 오류 제어 방식을 사용
- TCP, UDP 프로토콜이 있는 계층
- 패킷들의 전송이 유효한지 확인하고 전송 실패한 패킷들을 다시 전송한다.
- 오류검출 및 복구와 흐름제어, 중복검사 등을 수행한다.

### (5) 세션 계층(Session Layer)

- 양 끝단의 응용 프로세스가 통신을 관리하기 위한 방법을 제공
- 이 계층은 TCP/IP 세션을 만들고 없애는 책임을 진다.

### (6) 표현 계층(Presentation Layer)

- 데이터 표현이 상이한 응용 프로세스의 독립성을 제공하고, 암호화 한다.
- MIME 인코딩이나 암호화 등의 동작이 이 계층에서 이루어진다.

### (7) 응용 계층(Application Layer)

- 데이터의 최종 목적지로서 HTTP, FTP, SMTP, POP3, IMAP, Telnet 등과 같은 프로토콜이 있다.
- 브라우저나, 메일 프로그램은 프로토콜을 보다 쉽게 사용하게 해주는 응용프로그램이다.

## 3. 네트워크 장비

- Lan 카드
  - PC 혹은 네트워크에서 전달되어 오는 정보를 상호 교환할 수 있도록 만들어준다.
  - 랜 카드에 맥 주소(MAC Address)가 들어가는데, 랜 카드에 할당된 48비트 물리적 주소이다.
- 허브(Hub)
  - 집중화 장비라고도 하며, 단순히 노드들을 연결시켜주는 역할
  - 네트워크에 붙어 있는 PC들을 한곳으로 모아주는 역할
- 리피터(Repeter)
  - 디지털 신호를 증폭시켜주는 역할
  - 신호가 약해지지 않고, 컴퓨터로 수신되도록 하는 장비
- 브리지(Bridge)
  - 두 개의 근거리 통신망을 서로 연결해주는 장치
- 스위칭허브
  - 스위치 기능을 가진 허브
- 라우터(Router)
  - 패킷의 위치를 추출하여, 그 위치에 대한 최적의 경로 지정
  - 원하는 목적지까지 지정된 데이터가 안전하게 전달되도록 하는 역할
- 게이트웨이
  - 프로토콜을 서로 다른 통신망에 접속할 수 있게 해주는 장치

## 4. 백본(BackBone)

### (1) 백본 네트워크

- 기간망으로 불리는 대규모 패킷 통신망이다.
- 빠르게 전송할 수 있는 대규모 전송회선
- 보통의 백본은 Internet Backbone Network 를 의미한다.

### (2) 백본 스위치

- 네트워크 중심에 위치하며 모든 패킷이 지나가는 역할
- 많은 트래픽을 처리해야 하므로 기가급 장비를 사용한다.

### (3) 스위치의 종류

#### ① L2 스위치

- 데이터 링크 계층에서 운용되는 스위치
- Mac 주소를 기반으로 스위칭한다.

#### ② L3 스위치

- 인터넷 계층에서 운용되는 스위치
- IP 주소 기반으로 스위칭 한다.
- 라우팅 기능이 탑재되어 있다.

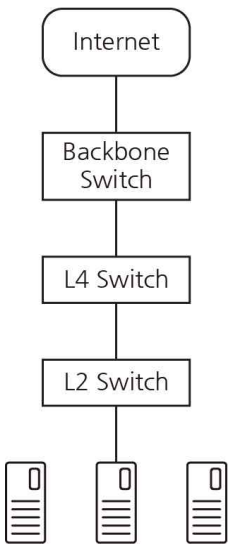
#### ③ L4 스위치

- 전송 계층에서 운용되는 스위치
- QoS 설정 등 다양한 기능을 가지고 있어 효율적인 네트워크를 구성할 수 있다.
- 서버나 네트워크의 트래픽을 로드밸런싱 한다.

#### ④ L7 스위치

- 응용 계층까지 운용되는 스위치
- 응용 계층 패킷까지 분석하여 보안 장비에 주로 사용된다.

### (4) 네트워크 구성



# Section 7. TCP/IP

## 1. TCP/IP(Transmission Control Protocol / Internet Protocol)

### (1) TCP/IP 개념

- 현재 인터넷에서 사용되는 프로토콜로 시스템간 네트워크 연결과, 데이터를 전송하는데 사용하는 모델
- 현재 대부분의 통신 프로토콜이 TCP/IP 가 사용되고 있다.
- TCP/IP는 단순히 인터넷 통신을 위한 표준 프로토콜, 모델을 가리키는 용어

### (2) TCP/IP 4계층 구조

| OSI 7계층 | TCP/IP 4계층 | 프로토콜 |
|---|---|---|
| 응용계층 | 응용 계층 | HTTP, FTP, SMTP,<br>DNS, RIP, SNMP, DHCP |
| 표현계층 | | |
| 세션계층 | | |
| 전송계층 | 전송 계층 | TCP, UDP |
| 네트워크 계층 | 인터넷 계층 | IP, ICMP, IGMP, ARP, RARP |
| 데이터 링크 계층 | 네트워크 엑세스 계층 | Ethernet, X.25, RS-232C |
| 물리 계층 | | |

## 2. 계층별 특징

### (1) 네트워크 액세스 계층(Network Access Layer)

- OSI 7계층의 물리계층과 데이터 링크 계층에 해당함
- 물리적인 주소로 MAC을 사용한다.
- 프로토콜

| 프로토콜 | 설명 |
|---|---|
| Ethernet | - 물리 계층과 데이터 링크 계층의 통신 회선의 접근 제어를 정의하는 IEEE 표준 |
| X.25 | - DTE와 DCE간의 인터페이스를 제공, 패킷 교환망을 통해 패킷을 원활히 전달하기 위한 통신 프로토콜<br>- TCP/IP보다 느리지만 안정성과 보안성은 더 뛰어나다. |
| RS-232C | - 공중전화 교환망(PSTN)을 통한 DTE/DCE 접속 규격 |

### ⑵ 인터넷 계층(Internet Layer)

- OSI 7계층의 네트워크 계층에 해당함
- 여러 개의 패킷 교환망들의 상호 연결을 위한 비연결성 프로토콜
- 통신 노드 간의 IP패킷을 전송하는 기능과 라우팅 기능을 담당한다.
- 프로토콜

| 프로토콜 | 설명 |
|---|---|
| IP | - 여러 개의 패킷 교환망들의 상호 연결을 위한 비연결성 프로토콜 |
| ICMP | - 인터넷 제어 메시지 프로토콜<br>- IP 패킷 전송 중 에러 발생 시, 에러 발생 원인을 알려주거나 네트워크 상태를 진단해주는 기능 제공 |
| IGMP | - 호스트가 멀티캐스트 그룹 구성원을 인접한 라우터에게 알리는 프로토콜 |
| ARP | - IP 주소를 MAC 주소로 변환한다.<br>- 네트워크 상에서 IP주소를 물리적 네트워크 주소(MAC)로 대응시키기 위해 사용되는 프로토콜 |
| RARP | - 호스트의 물리적 주소로부터 IP 주소를 구할 수 있도록 하는 프로토콜 |

### ⑶ 전송 계층(Transport Layer)

- OSI 7계층의 전송 계층에 해당함
- 통신 노드 간의 연결을 제어하고, 신뢰성 있는 데이터 전송을 담당한다.
- 프로토콜

| 프로토콜 | 설명 |
|---|---|
| TCP | - 클라이언트와 서버가 연결된 상태에서 데이터를 주고받는 프로토콜<br>- TCP는 데이터를 정확하고 안정적으로 전달할 수 있다.<br>- 데이터의 전송 순서를 보장한다.<br>- 연결의 설정 (3-way handshaking)<br>- 연결의 해제 (4-way handshaking)<br>- UDP 보다 전송 속도가 느리다.<br>- 헤더정보 : 송수신자의 포트번호, 시퀀스 번호, 응답번호, 데이터 오프셋, 예약필드, 제어비트, 윈도우 크기, 체크섬, 긴급위치 |
| UDP | - 데이터를 주고받을 때 연결 절차를 거치지 않고 발신자가 일방적으로 데이터를 발신하는 프로토콜<br>- TCP보다는 빠른 전송을 할 수 있지만 데이터 전달의 신뢰성은 떨어진다.<br>- 중간에 패킷이 유실이나 변조가 되어도 재전송을 하지 않는다.<br>- 헤더정보 : 송수신자의 포트번호, 데이터의 길이, 체크섬 |

### (4) 응용 계층(Application Layer)

- 사용자와 가장 가까운 계층으로 사용자가 소프트웨어 application과 소통할 수 있게 해준다.
- 응용프로그램(application)들이 데이터를 교환하기 위해 사용되는 프로토콜
- 프로토콜

| 프로토콜 | | 설명 |
|---|---|---|
| TCP 프로토콜 | HTTP | - 서버와 클라이언트 간에 하이퍼텍스트 문서를 송수신하는 프로토콜<br>- 80 포트 사용 |
| | FTP | - 인터넷에서 파일을 전송하는 기본 프로토콜<br>- Data 전달 시 : 20 포트, 제어정보 전달 시 : 21 포트 |
| | SMTP | - 이메일 전송에 사용되는 네트워크 프로토콜<br>- 25 포트 사용 |
| UDP 프로토콜 | DNS | - 호스트의 도메인 이름을 네트워크 주소로 바꿔주는 프로토콜<br>- 53 포트 사용 |
| | SNMP | - 네트워크에 있는 장비들을 관리하기 위한 프로토콜 |
| | DHCP | - IP 자동 할당과 분배 기능 |

## 3. TCP/IP 헤더

### (1) IP(Internet Protocol)

#### ① IP의 특징

- 호스트간의 통신만을 담당
- 송신 호스트와 수신 호스트가 패킷 교환 네트워크에서 정보를 주고받는 데 사용하는 정보 위주의 규약
- 비신뢰성(unreliability)과 비연결성(connectionlessness)
- 흐름제어, 오류 복구 기능은 없음

#### ② IP 헤더

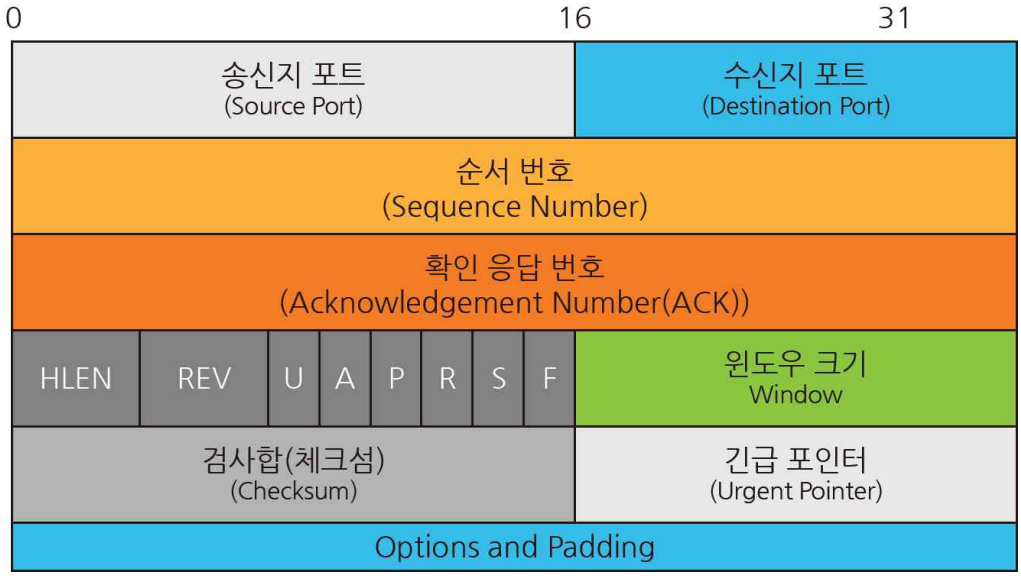
- 버전(Version)
  - IP 프로토콜의 버전
- 헤더길이(Header Length)
  - IP 헤더의 길이
  - 헤더의 길이 20Byte ~ 60Byte
- 서비스 유형(Type of Service, TOS)
  - 요구되는 서비스 품질
- 전체길이(Total Packet Length)
  - IP 헤더 및 데이터를 포함한 IP 패킷 전체의 길이를 바이트 단위로 길이를 표시
- 식별자(Identifier)
  - 각 데이터 그램을 식별한다.
  - 데이터그램이 단편화되었을 때 단편화된 데이터그램이 원래 어떤 데이터그램에 속해 있는지를 확인한다.
- 플래그(Flags)
  - IP 데이터그램이 단편화됬는지를 나타내는 필드
- 단편 오프셋(Fragmentation offset)
  - 단편화된 데이터그램의 순서
- 수명(Time to live)
  - 패킷이 라우터를 최대 몇 번 거쳐서까지 살아 남을 것인지를 나타내는 필드
  - 패킷이 라우터를 거칠 때마다 이 필드의 값이 1씩 감소되며 0이 되면 버려진다.
- 프로토콜(Protocol)
  - IP 데이터그램의 데이터(페이로드)에 담겨져 있는 상위 계층의 프로토콜을 알려준다.
  - ICMP가 1번, IGMP가 2번, TCP가 6번, UDP가 17번
- 체크섬(Header checksum)
  - Header 필드의 오류를 검출할 수 있는 정보가 담긴 필드
- 발신지 주소(Source IP address)
  - 패킷을 보낸 노드의 IP 주소
- 목적지 주소(Destination IP address)
  - 패킷이 도착해야하는 목적지의 IP 주소

## ⑵ TCP(Transmission Control Protocol)

### ① TCP의 특징

- 연결형 서비스를 지원하는 전송 계층 프로토콜
- 양 종단간 신뢰성 있는 데이터 전달과 흐름제어를 한다.
- 인터넷상에서 데이터를 메시지의 형태로 보내기 위해 IP와 함께 사용하는 프로토콜
- IP가 데이터의 배달을 처리한다면, TCP는 패킷을 추적 및 관리한다.

## ② TCP 헤더




- 송신지 포트(Source Port)
  - 출발지 포트
- 수신지 포트(Destination Port)
  - 수신지 포트
- 순서 번호(Sequence Number)
  - 바이트 단위로 순서화되는 번호
  - 이것을 통해 신뢰성(3-Way Handshake) 및 흐름제어(sliding Window) 기능 제공
- 확인 응답 번호(Acknowledgment Number)
  - 수신하기를 기대하는 다음 byte 번호 (마지막으로 수신에 성공한 번호의 +1)
- 헤더 길이(Header length)
  - TCP 헤더 길이
- 예약된 필드(Reserved)
  - 예약된 필드, 현재 사용되지 않음
- 윈도우 크기(Window)
  - 자신의 수신 버퍼 여유용량
- 검사합(Checksum)
- 긴급포인터(Urgent Pointer)
  - 어디서부터 긴급 값인지 알려주는 플래그(TCP Flags의 U와 세트)
- TCP Flags
  - U (Urgent) : 긴급 비트, 내가 지금 보내는 데이터가 우선순위가 높음. Urgnet Pointer와 세트
  - A (Ack) : 승인 비트, 물어본 것에 대한 응답을 해줄 때 사용됨
  - P (Push) : 밀어넣기 비트, 데이터를 계속 밀어 넣겠다.
  - R (Reset) : 초기화 비트, 연결 상태를 리셋하게 됨
  - S (Syn) : 동기화 비트, 상대방과 연결을 시작할 때 무조건 사용되는 플레그
  - F (Fin) : 종료 비트

# Section 8. 라우팅 프로토콜

## 1. 라우팅 프로토콜

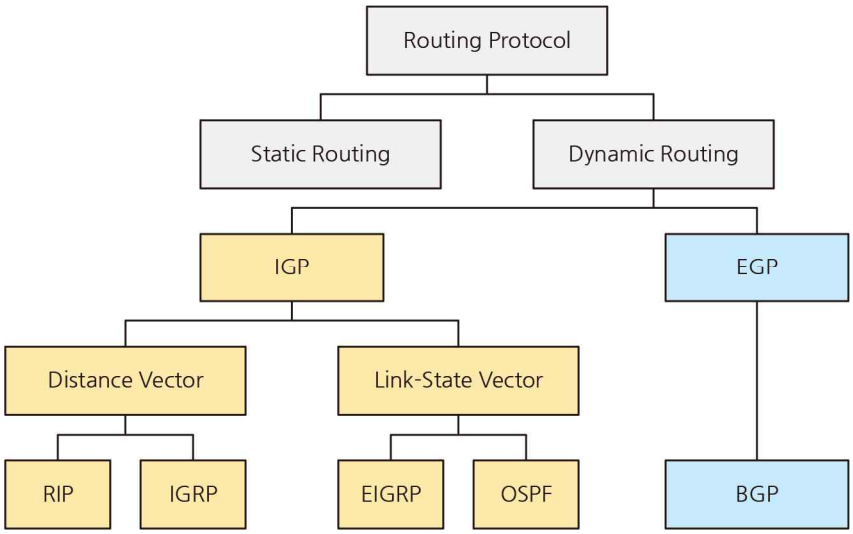
### (1) 라우터(Router)

- Path Determination(경로설정)과 Switching(스위칭)을 하는 장비
- 데이터 패킷이 목적지까지 이동할 때 최적의 경로를 판단하는 장비

### (2) 라우팅 프로토콜

- 패킷이 목적지까지 가는 방법을 결정해주는 프로토콜
- RIP, OSPF, IGRP, BGP 등이 있다.

## 2. 라우팅 프로토콜의 종류




### (1) 라우팅 경로 고정 여부

#### ① 정적 라우팅 프로토콜(Static Routing Protocol)

- 관리자가 경로를 직접 지정하는 수동형 방식
- 라우터 부하경감
- 고속 라우팅 가능
- 관리자의 관리부담 증가
- 정해진 경로 문제 발생시 라우팅 불가능

#### ② 동적 라우팅 프로토콜(Dynamic Routing Protocol)

- 라우터가 스스로 라우팅 경로를 동적으로 결정
- 종류 : RIP, IGRP, OSPF, EIGRP

### ⑵ 내/외부 라우팅

#### ① IGP(Interior Gateway Protocol)

- AS(Autonomous System) 내에서의 라우팅을 담당하는 라우팅 프로토콜
- 종류 : RIP, IGRP, OSPF, EIGRP

#### ② EGP(Exterior Gateway Protocol)

- 서로 다른 AS 사이에서 사용되는 라우팅 프로토콜
- 종류 : BGP, EGP

### ⑶ 라우팅 테이블 관리

#### ① 거리 벡터 알고리즘(Distance Vector Algorithm)

- 라우팅 Table에 목적지까지 가는데 필요한 거리와 방향만을 기록(인접 라우터)
- 종류 : RIP, IGRP

#### ② 링크 상태 알고리즘(Link State Algorithm)

- 라우터가 목적지까지 가는 경로를 SPF(Shortest Path First) 알고리즘을 통해 모든 라우팅 테이블에 기록해 두는 것 (모든 라우터)
- 종류 : OSPF

## 3. 주요 라우팅 프로토콜

### ⑴ RIP(Routing Information Protocol)

- 벨만 포드 거리벡터 알고리즘을 사용한 HOP 수 기반 라우팅 프로토콜
- 최대 15홉을 지원하며, 소규모망에 적합
- 30초마다 라우팅 테이블을 이웃 라우터들과 공유
- 네트워크 속도나 안정성을 고려하지 않고, HOP 수만을 고려하여 설계

### ⑵ OSPF(Open Shortest Path First)

- 다익스트라 알고리즘기반 방식
- 최적 경로 선택을 위해 홉수, 대역폭, 지연시간 등을 고려
- 링크상태 변화시에만 라우팅정보전송

### ⑶ BGP(Border Gateway Protocol)

- RIP나 OSPF 등의 라우팅 방식에 비해 규모가 큰 망을 지원할 수 있는 Path Vector기반 라우팅 프로토콜