네트워크 기초 정리

▼ 네트워크의 기본 규칙

▼ 네트워크 계층

네트워크 계층이란

송신자가 데이터를 상위계층에서 하위계층으로 보내고,

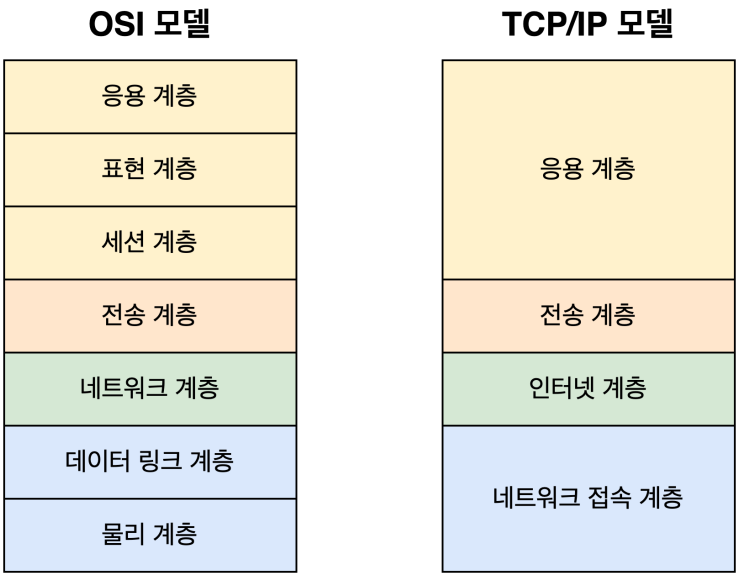
수신자는 하위계층에서 상위계층을 통해 올라온 데이터를 받게 된다.

네트워크 모델

OSI 모델

Aa 계층	이름	설명
7계층	응용계층	이메일 & 파일 전송, 웹사이트 조회 등 애플리케이션에 대한 서비스를 제공한다.
6계층	표현계층	문자 코드, 합축, 암호화 등의 데이터를 변환한다.
5계층	세션계층	세션 체결, 통신 방식을 결정한다.
4계층	전송계층	신뢰할 수 있는 통신을 구현한다.
3계층	네트워크계층	다른 네트워크와 통신하기 위한 경로 설정 및 논리 주소를 결정한다.
2계층	데이터링크계층	네트워크 기기 간의 데이터 전송 및 물리 주소를 결정한다.
1계층	물리계층	시스템 간의 물리적인 연결과 전기 신호를 변환 및 제어한다.

OSI 모델 vs TCP/IP 모델



▼ 캡슐화, 역캡슐화

캡슐화

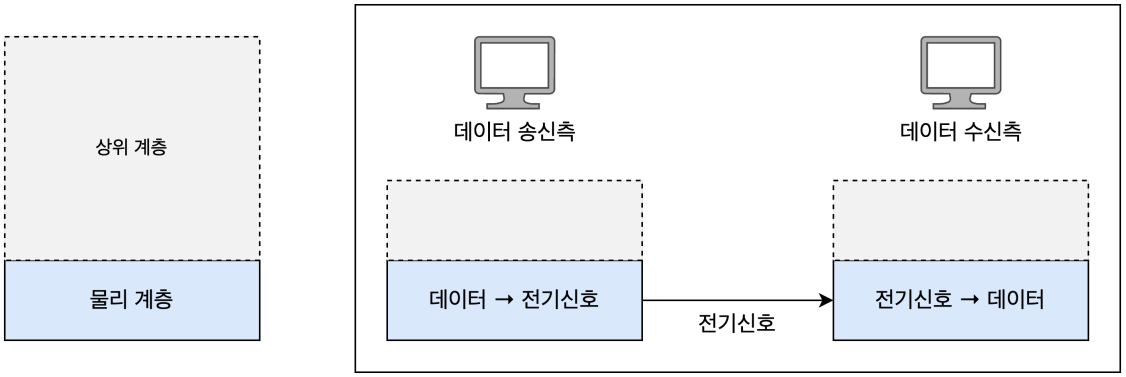
헤더(데이터를 전송하는데 필요한 정보)를 붙여서 다음 계층으로 보낸다.

이렇게 송신자가 계층마다 헤더를 붙여나가는 것을 '캡슐화'라고 한다.

역캡슐화

반대로 수신자가 하위계층에서부터 헤더를 하나씩 제거해나가는 것을 '역캡슐화'라고 한다.

▼ 물리 계층: 데이터를 전기 신호로 변환하기



물리계층

컴퓨터와 네트워크 장비를 연결하고, 컴퓨터와 네트워크 장비간에 전송되는 데이터를 전기신호로 변환하는 계층

어떻게?

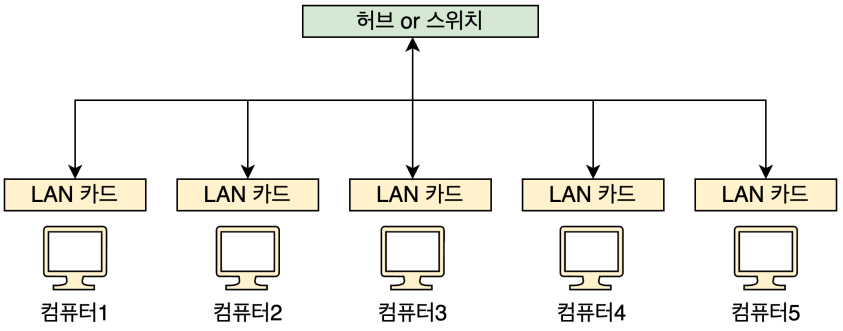
데이터 송신측 컴퓨터는 물리계층(=랜카드)에서 0과 1의 비트열 데이터를 전기신호로 변환하여,

네트워크를 통해 전기 신호를 전송한다.

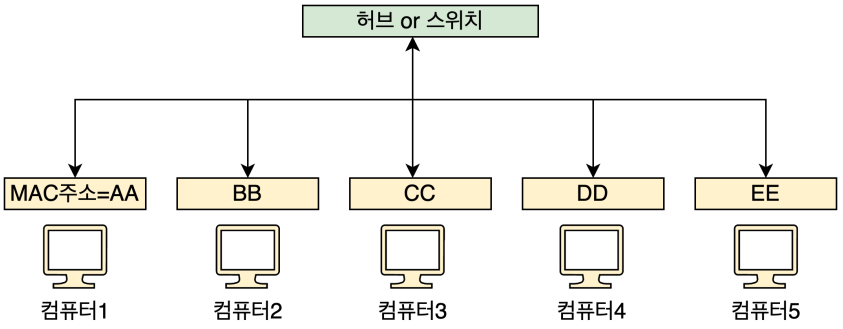
수신측 컴퓨터는 도착한 전기신호를 0과 1의 비트열 데이터로 복원한다.

▼ 데이터 링크 계층: 랜에서 데이터 전송하기

▼ 데이터 링크 계층 구조



LAN카드에는 MAC주소가 정해져 있다.



MAC주소는 LAN카드마다 할당된 주소로, 전세계에서 유일한 일련번호다.

▼ 데이터링크 계층 장비

컴퓨터간에 데이터를 전송할 수 있도록 하려면 장치가 필요한데, 이 장치가 바로 **스위치, 또는 허브**다.

둘은 데이터를 어떻게 목적지에 보내느냐에 차이가 있다.

허브

만약 컴퓨터1이 컴퓨터3으로 데이터를 보낼 경우, 허브는 컴퓨터2~5로 모두 보낸다.

단, 목적지가 아닌 컴퓨터에서는 이를 무시하도록 되어 있다.

스위치

MAC 주소 필터링 기능이 있어서, 만약 컴퓨터1이 컴퓨터3으로 데이터를 보낼 경우, 컴퓨터3으로만 보낸다. 최근에는 스위치를 사용하는 것이 표준이다.

- MAC주소 테이블

  스위치의 포트 번호와 해당 포트에 연결되어 있는 컴퓨터의 MAC주소가 등록되는 데이터베이스

- MAC주소 필터링

  데이터 헤더에 있는 목적지 MAC 주소를 기준으로, 해당 목적지 컴퓨터로만 보낼 수 있는 기능

스위치 vs 허브

Aa 속성	스위치	허브
데이터 전송 방식	컴퓨터1이 컴퓨터3으로 데이터를 보낼 경우, 허브는 컴퓨터2~5로 모두 보낸다.	만약 컴퓨터1이 컴퓨터3으로 데이터를 보낼 경우, 컴퓨터3으로만 보낸다.
데이터 통신 방식	전이중 통신 방식(효율↑)	반이중 통신 방식(효율↓)
충돌 도메인	각 컴퓨터로 한정됨	장치에 연결된 모든 컴퓨터

▼ 어떻게 데이터를 전송할까?

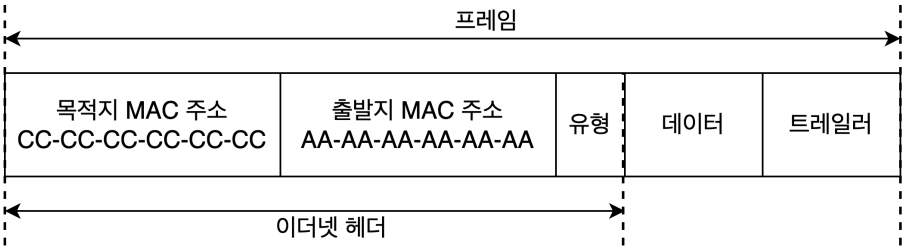
송신하는 컴퓨터는 데이터에 목적지MAC주소 등을 붙여 스위치로 데이터로 전송하고, 스위치는 목적지 주소를 가진 컴퓨터로 데이터를 전송한다.

데이터에 목적지MAC주소 등을 붙이는 것이 **데이터링크 계층의 캡슐화**다.

그리고 데이터를 전송할 때, 네트워크 장비 간에 신호를 주고받는 규칙이 **이더넷**이라 한다.

예를 들어, 여러 컴퓨터가 동시에 데이터를 전송하면, 데이터가 **충돌**할 수 있는데, 이 때 이더넷의 CSMA/CD를 통해 충돌을 방지하는 것이다.

▼ 데이터링크 계층의 캡슐화



프레임

프레임: 데이터링크 계층을 캡슐화한 것

유형: 이더넷으로 전송되는 상위 계층 프로토콜의 종류 ex) IPv4 → 0800

트레일러(Frame Check Sequence): 데이터 전송 도중에 오류가 발생하는 확인하는 용도

▼ 이더넷

네트워크 장비간에, 신호를 주고받는 가장 일반적인 규칙.

정확히는, 데이터링크 계층에서, MAC패킷과 프로토콜의 형식을 정의하는 방법.

이더넷에는 데이터간의 충돌을 막기 위한 방식을 사용한다.

CSMA/CD

CS : 데이터를 보내려고 하는 컴퓨터가 케이블에 신호가 흐르고 있는지 아닌지를 확인한다

MA : 케이블에 데이터가 흐르고 있지 않다면 데이터를 보내도 좋다

CD : 충돌이 발생하고 있는지를 확인한다

즉, 데이터가 흐르고 있지 않은지 확인한 후, 데이터를 보내고, 충돌이 발생하고 있는지를 확인하는 방식으로 데이터 간의 충돌을 방지하는 것이다.

이더넷 규격

▼ 어떻게 데이터 충돌을 방지할까?

컴퓨터 여러 대가 동시에 데이터를 보내면 데이터들이 서로 충돌할 수 있다. 그래서 이더넷은, 여러 컴퓨터가 동시에 데이터를 전송해도 충돌이 일어나지 않는 방식을 사용하는 것이다.(CSMA/CD)

▼ 기타

▼ 데이터 통신 방식

전이중 통신 방식

데이터의 송수신을 동시에 통신하는 방식

반이중 통신 방식

회선 하나로 송신과 수신을 번갈아가면서 통신하는 방식

스위치 vs 허브

허브는 반이중 통신 방식을 사용해서 충돌이 일어날 가능성이 높은 반면, 스위치는 송수신을 동시에 할 수 있기 때문에 효율이 높다

▼ 충돌 도메인

충돌 도메인

충돌이 발생할 때 그 영향이 미치는 범위

스위치 vs 허브

허브는 충돌이 발생할 때, 허브에 연결되어 있는 컴퓨터 전체가 충돌 도메인이 된다. 반면 스위치는 충돌 도메인은 각 컴퓨터 간에 충돌 도메인의 범위가 제한되어 있다.

▼ ARP(Address Resolution Protocol)

목적지 컴퓨터IP 주소를 이용하여 MAC주소를 찾기 위한 프로토콜

출발지 컴퓨터가 목적지 주소를 모를 경우, MAC주소를 알아내기 위해 네트워크에 브로드캐스트를 한다.(ARP 요청)

이 요청에 대해 지정된 IP주소를 가지고 있지 않은 컴퓨터는 응답하지 않지만, 지정된 IP주소를 가진 컴퓨터는 MAC주소를 응답으로 보낸다.(ARP 응답)

응답을 바탕으로, 출발지 컴퓨터는 MAC주소와 IP 주소의 매핑 정보를 메모리에 보관한다.(ARP 테이블)

But, 영원히 보관하는 것이 아니라, 일정 기간이 지나면 삭제하고 다시 ARP 요청을 한다.

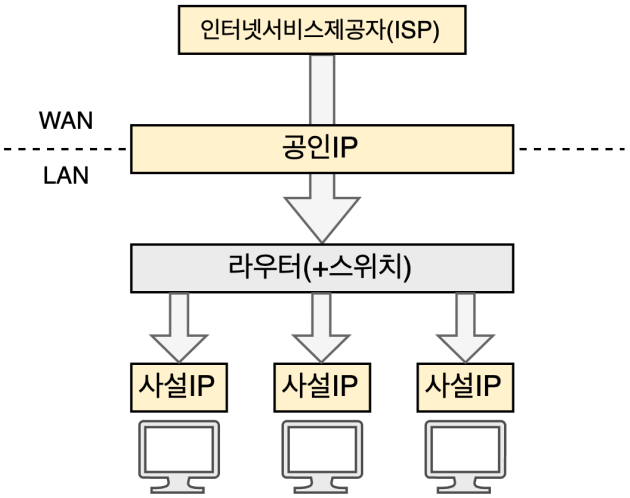
터미널에서 ARP캐시의 내용을 확인하고 삭제할 수 있다.

▼ 네트워크 계층: 목적지에 데이터 전달하기

▼ 네트워크 계층의 역할

네트워크 계층

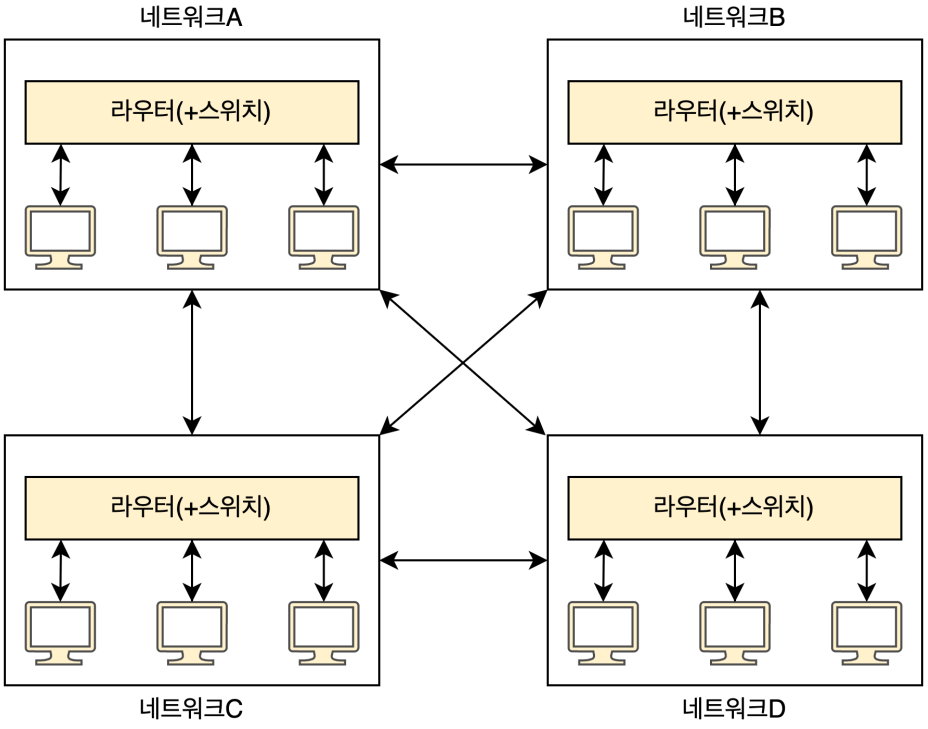
서로 다른 네트워크에 있는 목적지로 데이터를 전송하기 위해 필요한 계층



IP주소

다른 네트워크에 있는 컴퓨터로 데이터를 보내기 위해서는 목적지 주소=IP 주소가 필요하다

(같은 네트워크 안에서는 스위치만 있으면 되지만, 다른 네트워크로 보내기 위해서는 라우터가 필요하다.)



라우터

또한, 다른 네트워크에 있는 컴퓨터로 데이터를 보내기 위해서는 라우터가 필요하다.

라우터는 라우팅 역할(데이터를 어떤 경로로 보낼지, 결정하는 역할)을 한다.

▼ IP주소

IPv4 vs IPv6

IPv4는 32비트의 IP주소. 2의 32제곱인 약 43억개의 컴퓨터에 IP주소를 할당할 수 있다. 처음 IP주소를 만들 때 만들어진 주소로, 하지만 인터넷이 보급되면서 고갈되기 시작했고, 이에 IPv6이 생겨났다.

IPv6는 128비트로 확장하여 2의 128제곱의 IP주소. 즉 사실상 무제한의 IP주소를 사용할 수 있다.

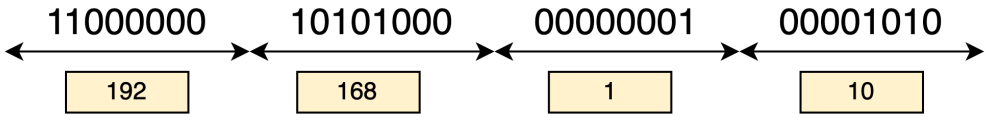
공인IP주소 & 사설IP주소

IPv4 주소가 고갈되고 있기 때문에, 공인IP주소와 사설IP주소를 할당하는 정책을 사용하고 있다.

인터넷에 직접 연결되는 컴퓨터나 라우터에는 공인IP주소를 할당하고, 회사나 가정의 랜에 있는 컴퓨터는 사설IP 주소를 할당한다.

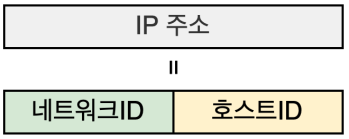
IP주소의 표기법

32비트를 10진수로 표기한다.

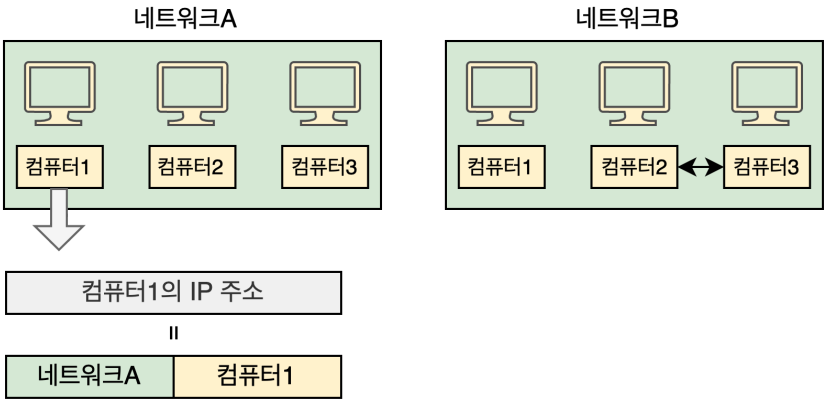


ex) 192.168.1.10

IP주소의 구조



IP주소는 네트워크ID와 호스트ID로 이루어져 있다.



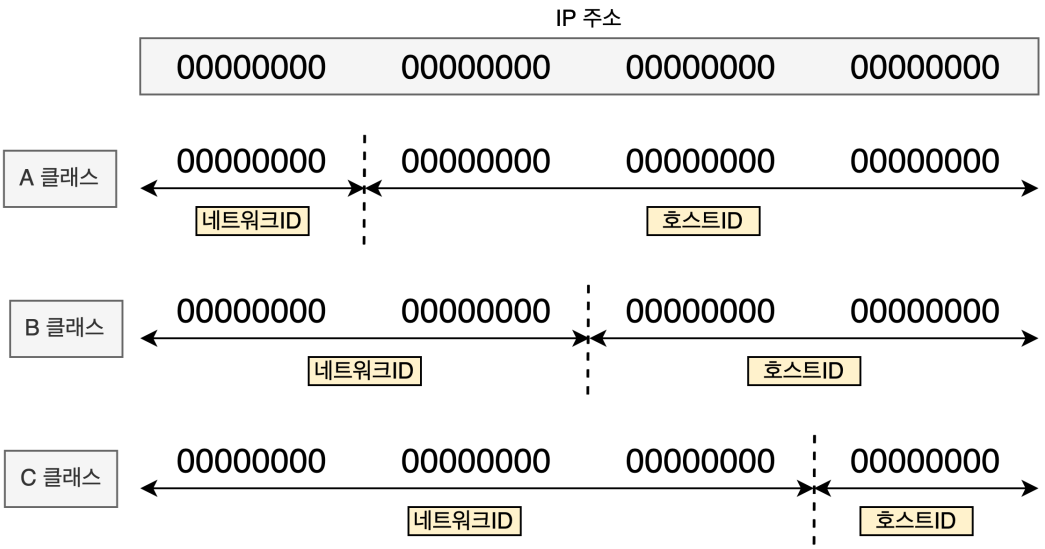
▼ IP주소의 클래스 구조

IP주소의 클래스

네트워크 크기는 클래스라는 개념으로 구분한다. 네트워크ID를 크게 만들거나, 호스트ID를 작게 만들어 네트워크 크기를 조정할 수 있다.

클래스 종류

Aa 이름	종류	주소의 범위
A클래스	대규모 네트워크 주소	1.0.0.0~127.255.255.255
B클래스	중형 네트워크 주소	128.0.0.0~191.255.255.255
C클래스	소규모 네트워크 주소	192.0.0.0~223.255.255.255
D클래스	멀티캐스트(multicast) 주소	
E클래스	연구 및 특수용도 주소	



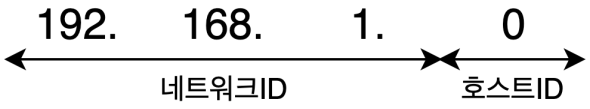
▼ 네트워크 주소, 브로드캐스트 구조

네트워크 주소

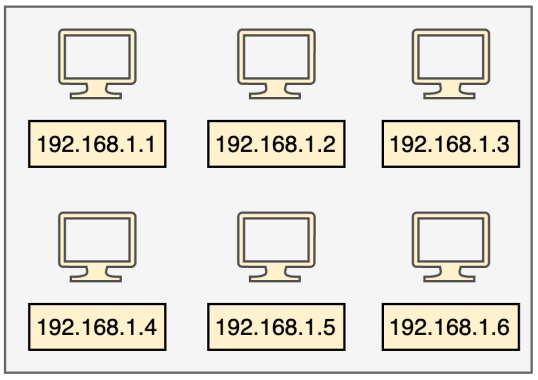
전체 네트워크에서 작은 네트워크를 식별하는데 사용되는,

해당 네트워크를 대표하는 주소.

ex)



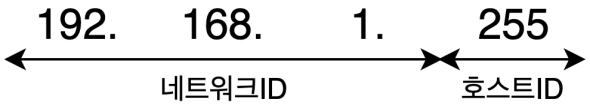
192.168.1.0 = 네트워크 주소



브로드캐스트 주소

네트워크에 있는 컴퓨터 장비 모두에게 한 번에 데이터를 전송하는데 사용되는 전용 IP 주소.

ex)



▼ 서브넷

▼ 전송 계층: 신뢰할 수 있는 데이터 전송하기

▼ 전송 계층의 역할

1. 오류를 점검해, 목적지에 신뢰할 수 있는 데이터를 전달하는 역할
2. 전송된 데이터의 목적지가 어떤 애플리케이션인지 식별하는 기능

▼ 연결형 통신 vs 비연결형 통신

연결형 통신

신뢰할 수 있고 정확한 데이터를 전달할 수 있는 통신

일반적으로 사용하는 통신으로, **TCP**가 있다.

비연결형 통신

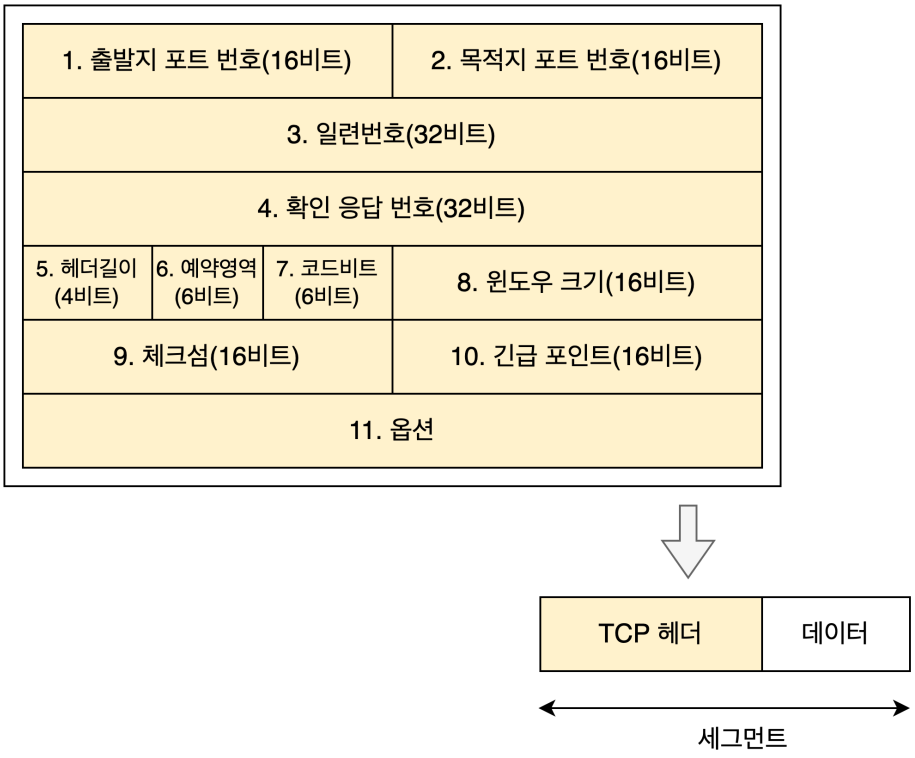
효율적으로 데이터를 전달하는 통신.

신뢰할 수 있고 정확한 통신보다는 빠른 전송이 필요한 경우에 사용한다. ex) 동영상 전송

비연결형 통신 프로토콜에는 **UDP**가 있다.

▼ 전송계층의 캡슐화

TCP를 사용할 경우, 전송계층에서는 TCP 헤더를 붙여 캡슐화한다.



▼ TCP

TCP(Transmission Control Protocol)

신뢰할 수 있고 정확한 데이터를 전달할 수 있는 통신 프로토콜.

연결확립, 재전송제어, 윈도우제어 역할을 통해 신뢰할 수 있고, 정확한 통신을 보장한다.

또한, 전송된 데이터의 목적지가 어떤 애플리케이션인지 구분하는 역할을 한다.

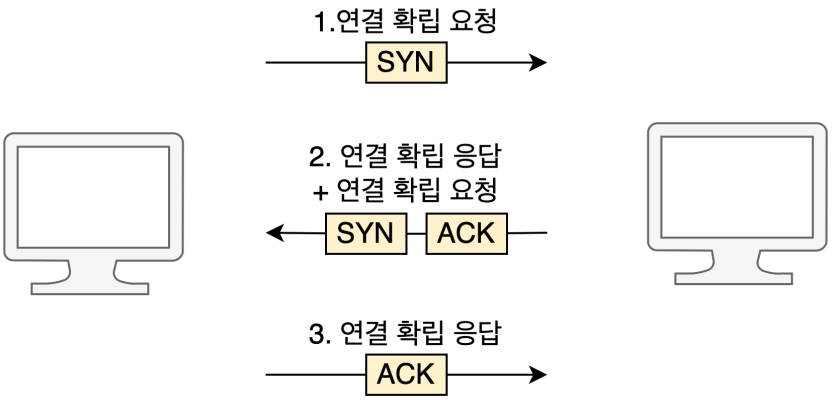
▼ **연결확립**

TCP는 3-way 핸드셰이크를 통해 신뢰할 수 있는 연결을 보장한다.

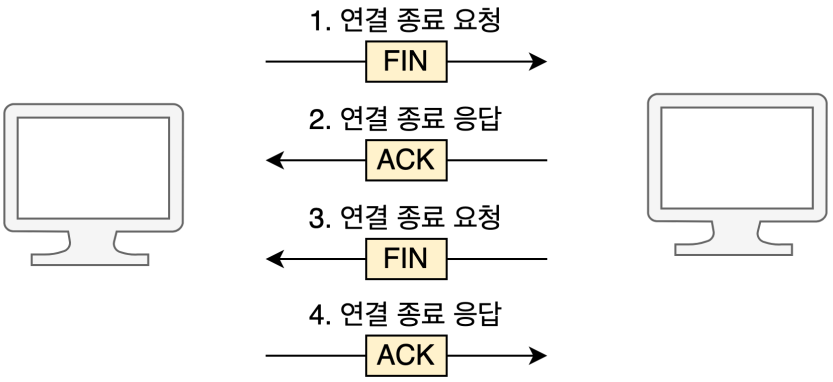
3-way 핸드셰이크를 통해, 신뢰할 수 있는 가상의 독점 통신로를 확립하고, 이를 통해 통신하는 것이다.

▼ **3-way 핸드셰이크**

1. **연결 확립**



2. **연결 종료**

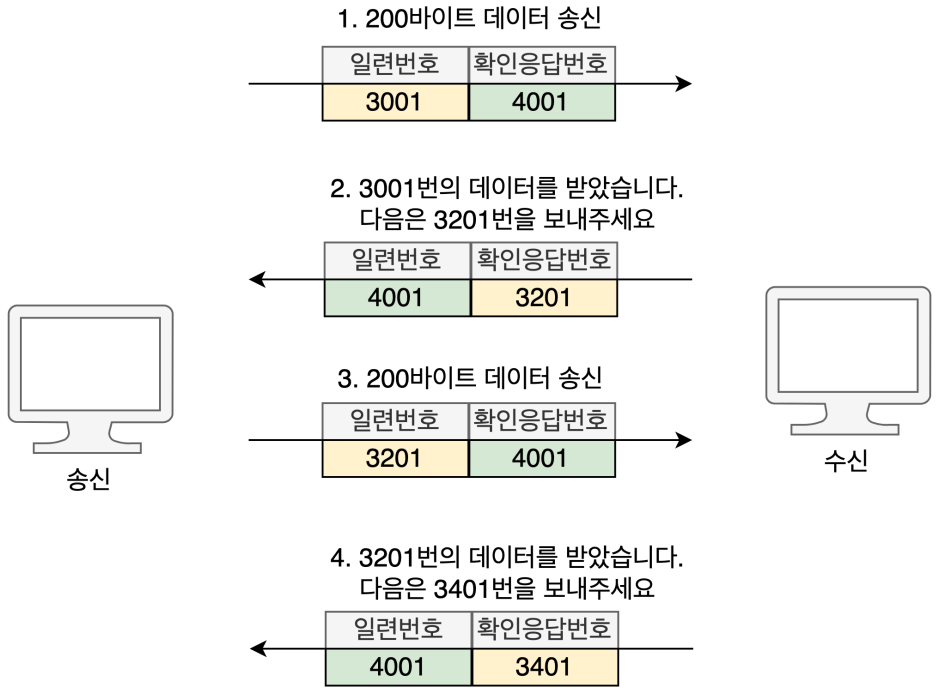


TCP 헤더 중 [7-코드 비트]가 이 3-way 핸드셰이크 역할을 수행한다.

▼ **재전송 제어**

TCP는 데이터에 일련 번호와, 확인 응답 번호를 붙여, 데이터가 제대로 전송 되었는 지 확인한다.

만약 확인응답번호를 통해 데이터가 손상되거나 유실된 것을 발견한 경우, 데이터를 다시 전송한다. 이를 '재전송 제어'라고 한다.



1. 송신측이 데이터와 함께 일련 번호와 확인 응답 번호를 보낸다.
2. 수신측은 데이터를 받고, 확인 응답 번호=다음 데이터 번호와, 일련 번호= 데이터를 받았다는 확인의 의미로 송신측이 보낸 확인 응답 번호를 보낸다.
3. 송신측은 다음 데이터와 함께 일련 번호와 확인 응답 번호를 보낸다.

▼ 윈도우 제어

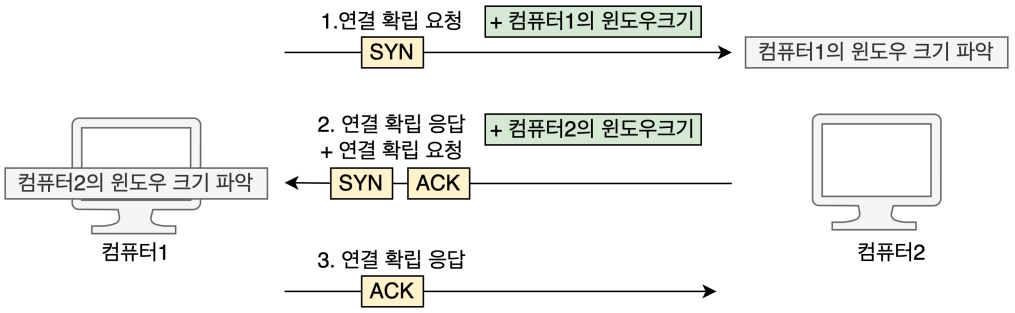
세그먼트(TCP헤더+데이터) 하나를 보낼 때마다 매번 확인 응답을 반환한다면, 비효율적이다. 때문에, 세그먼트를 연속해서 보낸 후, 확인 응답을 반환한다. 수신 측에서는, '버퍼'라는 보관소에 받은 세그먼트를 일시적으로 쌓아두었다가, 한 번에 처리한다.

다만, 버퍼가 보관할 수 있는 용량보다 대용량의 세그먼트를 받을 경우, 넘쳐버린다. '오버플로우'가 발생하는 것이다. 따라서, 오버플로우가 발생하지 않도록, 버퍼의 한계크기를 미리 알고 있어야 한다.

윈도우 크기 = 버퍼의 한계 용량

윈도우 크기를 파악하는 방법

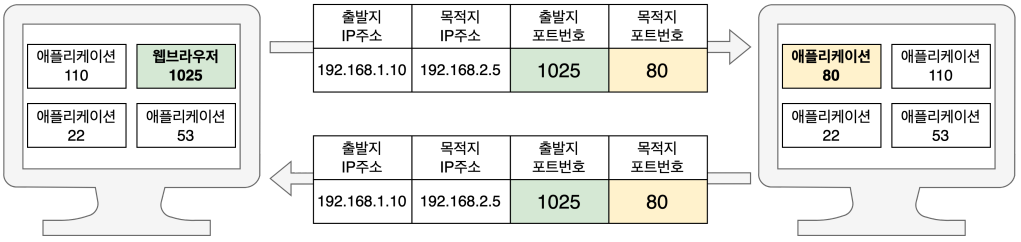
TCP헤더에 [8-윈도우크기]에 담아, 3-way 핸드셰이크를 할 때 판단한다.



▼ **데이터의 목적지를 구분하는 역할**

포트번호

컴퓨터가 데이터 통신을 할 때 통신하고자 하는 네트워크 서비스나 특정 프로세스를 식별하는 논리 단위.



포트를 통해 목적지를 찾는 방법

애플리케이션에는 각각 포트번호가 할당되어 있다. 데이터의 TCP헤더에 목적지 포트번호가 들어있어, 데이터의 최종 목적지를 찾아갈 수 있다.

주요 포트

0~1023번 포트는 주요 프로토콜이 사용하도록 예약되어 있다.(well-known port)

1024번은 예약되어 있지만 사용하지 않는 포트다.

1025번 이상은 랜덤 포트로, 클라이언트 측의 송신 포트로 사용된다.

웹브라우저의 포트

웹브라우저에 접속할 때는, 웹 브라우저에 임의로 포트가 자동으로 할당된다. 따라서 서버 측의 애플리케이션에는 포트 번호를 정해두어야 하지만, 클라에서는 정해두지 않아도 괜찮다.(임의로 할당된 포트번호를 그대로 사용하면 된다.)

▼ UDP

UDP(User Datagram Protocol)

비연결형 통신. 효율성을 우선으로 한다.

신뢰성과 정확성이 필요하지 않기 때문에, 헤더에도 신뢰 확보를 위한 데이터를 제외한 간단한 데이터만을 담고, 통신을 할 때도 확인 응답을 따로 하지 않고 빠르게 전송한다.

또한, 브로드캐스트를 할 때도, UDP를 사용한다. (TCP는 확인 응답을 하나씩 보내야 하기 때문에 브로드캐스트에 적합하지 않다.)

▼ 브로드캐스트

랜에 있는 컴퓨터나 네트워크 장비에 데이터를 일괄로 보내는 것

▼ 응용 계층: 애플리케이션에 데이터 전송하기

▼ 응용 계층의 역할

응용+표현 계층에서는 클라이언트의 요청을 전달하기 위해 통신 대상(서버 등)이 이해할 수 있는 메시지(데이터)로 변환하고 전송 계층으로 전달하는 역할을 한다.

▼ 응용계층의 프로토콜

클라이언트측 애플리케이션과, 서버측 애플리케이션이 통신하려면 프로토콜이 필요하다

주요 프로토콜

HTTP: 웹사이트를 볼 때

FTP: 파일을 전송할 때

SMTP: 메일을 보낼 때

POP3: 메일을 받을 때

▼ HTTP(웹브라우저의 프로토콜)

keepalive 기능

한 번 연결을 수립하면 데이터 교환을 마칠때까지 유지하고, 데이터 교환을 모두 끝내면 연결을 끊는 구조

HTTP/2 버전의 개선

요청을 보낸 순서대로 응답을 반환하지 않아도 된다. 그래서 콘텐츠를 빠르게 표시할 수 있다.

▼ SMTP, POP3(메일 서버 프로토콜)

▼ DNS

DNS

도메인 주소(= 웹사이트 URL)을 IP주소로 변환하는 시스템

1. 클라이언트가 웹사이트 URL을 입력하면
2. 컴퓨터는 DNS 서버에 URL의 IP주소를 알려달라고 요청한다.
3. DNS 서버가 IP를 알려주면, 클라이언트는 그 IP주소로 해당 웹사이트의 웹서버에 접속한다.

- 만약, DNS서버 1이 도메인 주소를 모를 경우, DNS 서버1이 DNS서버2로 요청을 보낸다. 이처럼, DNS 서버는 전세계에 흩어져 있고, 모두 계층적으로 연결되어 있다.