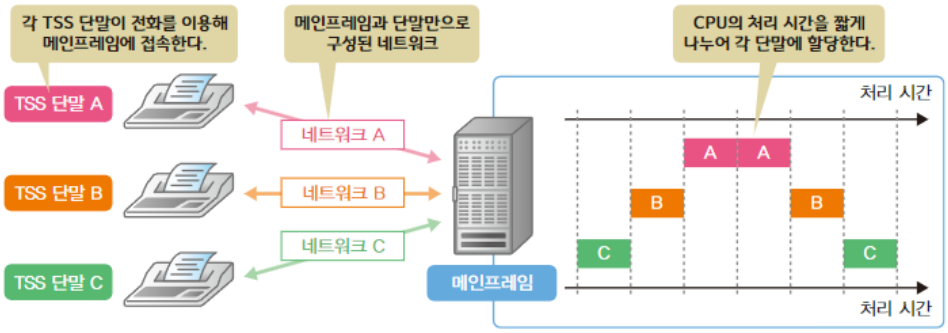
네트워크란

네트워크 역사

현대 네트워크의 원형은 1960년대~19870년대에 걸쳐 미국에서 연구되고 개발되었습니다. 1960년대에는 한 대의 대형 컴퓨터(mainframe, 메인프레임)의 처리를 짧은 시간으로 나누어서 여러 사람이 사용하는 TSS(Time Sharing System, 시분할 시스템) 방식으로 컴퓨터를 이용하였습니다.



1. 컴퓨터 네트워크의 탄생

- 패킷 교환 개념

1960년대에 미국의 폴 바란(Paul Baran)과 영국의 도널드 데이비스(Donald Davies)는 각각 독립적으로 '패킷 교환(packet switching)' 개념을 제안했습니다. 이는 데이터를 작은 단위(패킷)로 분할해 전송하고, 목적지에서 재조합하는 방식으로, 효율적이고 견고한 통신 방식을 가능하게 했습니다.

- ARPANET의 시작 (1969년)

미국 국방고등연구계획국(ARPA)이 주도한 ARPANET은 최초의 패킷 교환 네트워크로, UCLA, 스탠포드 연구소, 유타 대학교, 캘리포니아 대학교 산타바버라 캠퍼스 등이 연결되었습니다. ARPANET은 현대 인터넷의 전신으로 평가받으며, 초기 컴퓨터 네트워크 연구의 장이 되었습니다.

2. 프로토콜의 발전과 인터넷의 형성

- TCP/IP의 개발과 채택 (1970년대 ~ 1983년)

Vint Cerf와 Bob Kahn 등 연구자들이 여러 네트워크를 하나로 연결할 수 있는 표준 통신 프로토콜인 TCP/IP(Transmission Control Protocol/Internet Protocol)를 개발했습니다. 1983년 1월 1일, ARPANET은 기존의 통신 프로토콜에서 TCP/IP로 전환하며, 다양한 네트워크 간 상호운용성을 확보하게 되었습니다.

- DNS와 네트워크 인프라의 확장 (1980년대)

도메인 네임 시스템(DNS)이 도입되면서 숫자로 된 IP 주소 대신 사람이 이해하기 쉬운 도메인 이름으로 네트워크 상의 컴퓨터를 식별할 수 있게 되었습니다. 이 시기에 대학, 연구소, 정부 기관 등으로 네트워크 인프라가 확장되었습니다.

3. 월드 와이드 웹의 혁명과 인터넷의 대중화

- 월드 와이드 웹(WWW)의 발명 (1989 ~ 1991년)

CERN의 팀 버너스 리(Tim Berners-Lee)는 월드 와이드 웹을 개발하여, 하이퍼텍스트(Hypertext)를 기반으로 문서와 정보를 손쉽게 연결하고 공유할 수 있는 시스템을 만들었습니다. 이로 인해 인터넷이 연구기관뿐만 아니라 일반 대중에게도 빠르게 확산되었습니다.

- 상업화와 대중화 (1990년대)

1990년대에는 인터넷 서비스 제공업체(ISP)가 등장하면서, 인터넷이 상업적으로도 크게 성장하기 시작했습니다. 웹 브라우저의 발전, 전자상거래의 등장, 그리고 전 세계적으로 네트워크 인프라의 확충으로 인터넷은 일상생활의 필수 요소로 자리잡았습니다.

4. 현대의 네트워크와 미래 전망

- 고속 인터넷과 무선 네트워크

2000년대 이후 초고속 인터넷, Wi-Fi, 그리고 모바일 데이터 네트워크의 발전은 언제 어디서나 인터넷에 접속할 수 있는 환경을 만들었습니다. 스마트폰과 태블릿 등 모바일 기기의 보급은 네트워크 사용의 패러다임을 변화시켰습니다.

- 클라우드 컴퓨팅과 사물인터넷(IoT)

클라우드 컴퓨팅은 데이터를 중앙 집중형 서버에서 관리하고 다양한 기기에서 접근할 수 있도록 지원하며, IoT는 일상 용품들이 네트워크에 연결되어 데이터를 주고받는 환경을 조성하고 있습니다.

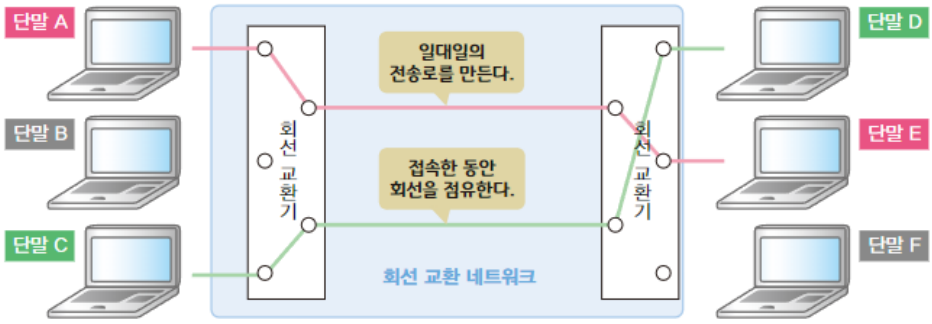
- 5G와 미래 네트워크 기술

최신 5G 기술은 더욱 빠른 속도와 낮은 지연 시간을 제공함으로써, 자율주행차, 스마트 시티, 증강 현실(AR) 등 미래 기술의 기반을 마련하고 있습니다. 또한, 향후 양자 네트워크와 같은 차세대 기술 연구도 활발히 진행 중입니다.

회선 교환 방식과 패킷 교환 방식

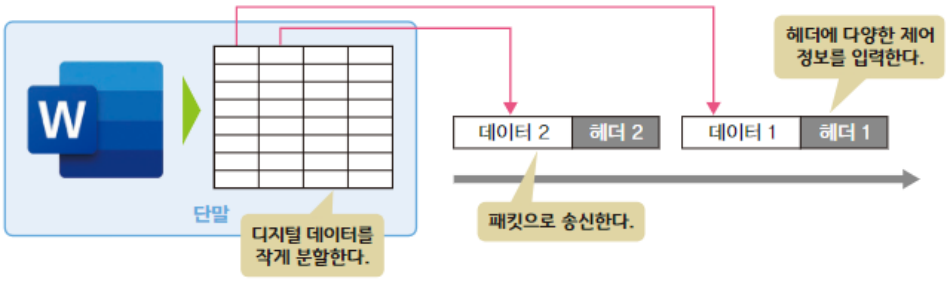
데이터 전송방식에는 **회선 교환 방식**(circuit exchange method)과 **패킷 교환 방식**(packet exchange methord)의 두 가지 방식이 있습니다.

회선 교환 방식은 데이터를 교환하기 전에 일대일의 전송로(데이터 통로)를 만들고, 교환을 마칠때까지 전송로를 계속 사용하는 방식입니다.



패킷 교환 방식은 데이터를 **패킷**(packet)이라 부르는 작은 단위로 나누어 네트워크로 보내는 방식입니다. **헤더**(header)라는 정보를 붙여 패킷 교환기(네트워크 기기)로 구성된 패킷 교환 네트워크로 패킷을 보냅니다. 헤더에는 수신 컴퓨터 정보, 데이터 중 몇 변째에 해당하는 패킷인지에 관한 정보등 다양한 정보가 포함되어 있습니다.

패킷 교환 네트워크는 헤더 정보를 보고 수신 컴퓨터로 패킷을 전달합니다. 그리고 수신 컴퓨터의 헤더의 정보를 보고 원 데이터로 복원합니다.



차이점

구분	회선 교환 방식	패킷 교환 방식
연결 방식	통신 시작전에 고정된 경로를 설정	데이터 패킷을 개별적으로 전송하며 경로 설정 없음
데이터 전송	연속적인 흐름으로 전송	패킷 단위로 분할하여 전송
효율성	비효율적(사용하지 않는 시간에도 회선을 독점)	효율적(여러 사용자가 자원 공유)
지연(latency)	낮음(일단 연결되면 빠름)	다소 발생 가능(패킷별 경로가 다름)

구분	회선 교환 방식	패킷 교환 방식
적합한 용도	음성 통화, 비디오 회의 등 실시간 서비스	인터넷, 메일, 웹 서핑, 데이터 통신
대표적 예시	전화통신망(PSTN)	인터넷(TCP/IP), VoIP, 온라인 스트리밍

통신을 위한 규칙, 프로토콜

네트워크 세계에서는 패킷을 처리하기 위한 규칙이 존해합니다. 이 규칙을 **프로토콜(통신 프로토콜)**(protocol, communication protocol)이라 부릅니다. 이 프로토콜이 통신에 필요한 기능별로 명확하게 규정되어 있기 때문에 PC 제조사나 운영체제(OS)가 다르더라도, 유무선에 관계없이 동일하게 패킷을 교환할 수 있습니다.

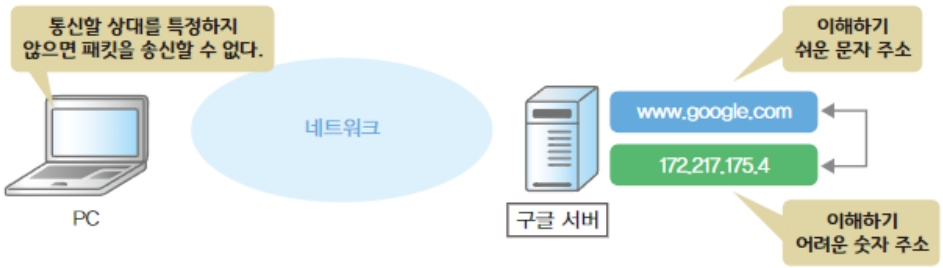
프로토콜에 결정되어 있는 것

- 물리적 사양

LAN 케이블 소재나 커넥터 형태 그 핀 할당(핀 배열)에 이르기까지 네트워크에서 눈에 보이는 것들은 모두 프로토콜로 정의되어 있습니다. 그리고 와이파이 환경에서 전파의 주파수는 물론, 패킷을 전파로 변환(변조)하는 방식도 프로토콜에 정의되어 있습니다. PC의 NIC(Network Interface Card)는 프로토콜에 정의된 내용에 기반해 케이블이나 전파 등의 전송 매체에 패킷을 보냅니다.

- 송신상태 특정

주소를 할당해서 송신 상대를 구별합니다.

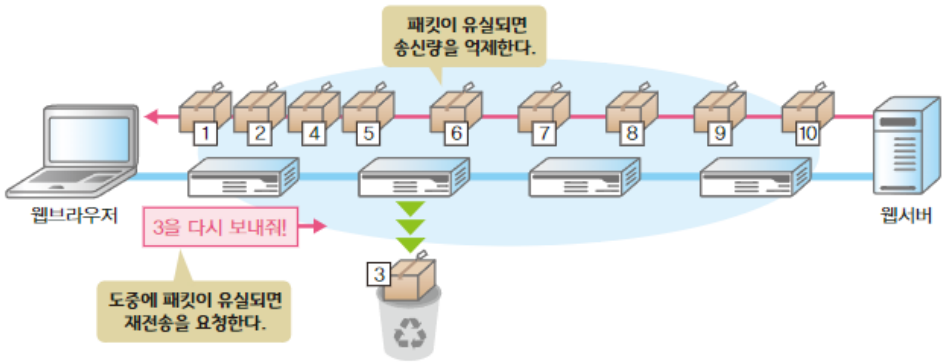


- 패킷 전송

송신 상대를 특정한 뒤에는 패킷을 상대에게 전달해야 합니다. 프로토콜에는 헤더의 어디에서 어디까지(몇 번째 비트에서 몇 번째 비트까지) 어떤 정보를 포함하고 어떤 순서로 교환하는 지 등이 정의 되어 있습니다.

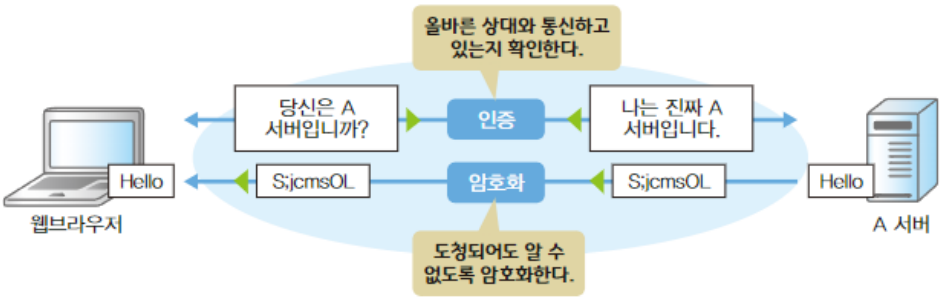
- 신뢰성 확립

프로토콜은 어떤 상황에서 패킷이 손상되거나 사라질 수 있습니다. 그런 상황이 발생해도 이상이 없도록 에러를 알리거나 데이터를 재전송하는 구조를 제공합니다. 또한, 유한한 네트워크 자원이 패킷으로 가득차서 잠기지 않도록 하기 위한 구조도 제공합니다.



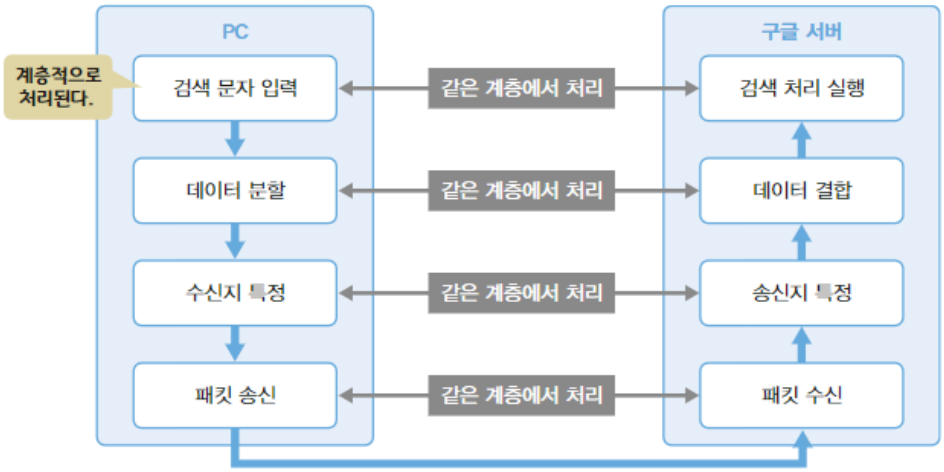
- 보안 확보

프로토콜은 중요한 정보를 안심하고 교환할 수 있도록 올바른 통신 상대인지 인증하고 통신을 암호화 하는 구조를 제공합니다.



프로토콜은 계층으로 정리한다.

프로토콜로 정의된 다양한 통신 기능은 그 처리에 맞춰 계층 구조로 되어 있습니다. 데이터 송신지가 되는 컴퓨터는 계층별로 준비된 프로토콜에 걸쳐 상위 계층부터 순서대로 데이터를 처리해 패킷 상태로 전송 매체로 보냅니다. 그 패킷을 받은 컴퓨터는 반대로 하위 계층에서 순서대로 계층별로 송신지 컴퓨터와 동일한 프로토콜을 따라 데이터를 처리하고, 최종적으로 원 데이터를 복원합니다.



두 가지 계층 구조 모델

- TCP/IP 참조 모델

계층	계층 이름	프로토콜
4계층	애플리케이션 계층	HTTP DNS FTP HTTP FTP SSL/TLS QUIC DNS Syslog SNMP NTP
3계층	트랜스포트 계층	TCP UDP
2계층	인터넷 계층	IP ICMP ARP
1계층	링크 계층	IEEE 802.3 IEEE 802.11

- OSI 참조 모델

계층	계층 이름	역할
7계층	애플리케이션 계층	사용자에게 애플리케이션을 제공한다.
6계층	프레젠테이션 계층	애플리케이션 데이터를 통신 가능한 방식으로 변환한다.
5계층	세션 계층	애플리케이션 데이터를 송신하기 위한 논리적 통신로(세션)를 관리한다.
4계층	트랜스포트 계층	애플리케이션 식별 및 그에 따라 통신 제어한다.
3계층	네트워크 계층	다른 네트워크에 있는 단말과의 연결성을 확보한다.
2계층	데이터링크 계층	물리 계층의 신뢰성을 확보하고, 같은 네트워크에 있는 단말과의 연결성을 확보한다.
1계층	물리 계층	디지털 데이터를 전기 신호나 광 신호, 전파로 변환해 네트워크로 보낸다.

각 계층마다 역할을 가진다.

자신의 처리를 완료하면 인접 계층으로 전달한다.

- PDU

네트워크에서 데이터는 하나의 큰 덩어리 그대로 처리되지는 않습니다. 각 계층에서 처리 할 수 있도록 작게 분할해서 처리합니다. 계층에서 처리하는 한 덩어리의 데이터, 즉 데이터 단위를 PDU(Protocol Data Unit)라 부릅니다. PDU는 제어 정보를 포함한 헤더, 데이터 자체인 페이로드(payload)로 구성되어 있으며, 처리되는 계층에 따라 명칭이 다릅니다.

계층	계층 이름	PDU 이름
7계층	애플리케이션 계층	메시지
4계층	트랜스포트 계층	세그먼트(TCP), 데이터그램(UDP)
3계층	네트워크 계층	패킷
2계층	데이터링크 계층	프레임
1계층	물리 계층	비트

> 네트워크 데이터를 부르는 이름 중 자주 혼란을 일으키는 것이 '패킷' 입니다. 넓은 의미의 패킷과 좁은 의키의 패킷이 있습니다. 전자는 네트워크를 통해 흐르는 데이터 그 자체를 의미합니다. 후자는 네트워크 계층의 PDU를 의미합니다.

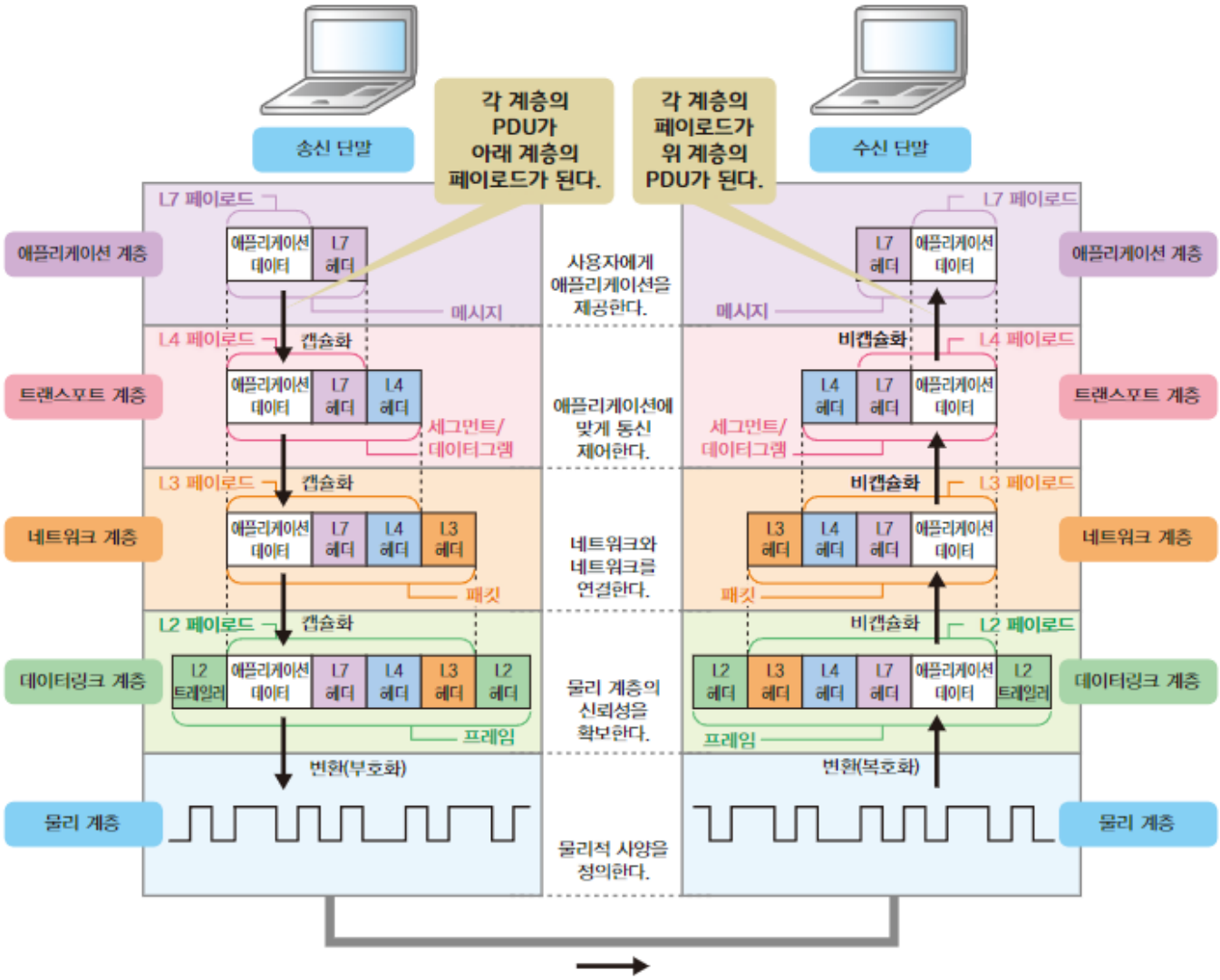
- 대표적인 RFC(Request For Comments, 프로토콜의 표준) 및 프로토콜

RFC	제안 이름	대상 프로토콜
768	User Datagram Protocol	UDP
791	INTERNET PROTOCOL	IP(IPv4)
792	INTERNET CONTROL MESSAGE PROTOCOL	ICMP
793	TRANSMISSION CONTROL PROTOCOL	TCP
826	An Ethernet Address Resolution Protocol	ARP
1034	DOMAIN NAMES - CONCETPS AND FACILITIES	DNS
1035	DOMAIN NAEMS - IMPLEMENTATION AND SPECIFICATION	DNS
2131	Dynamic Host Configuration Protocol	DHCP
2460	Internet Protocol, Version 6(IPv6) Specification	IPv6
2616	Hypertext Transfer Protocol -- HTTP/1.1	HTTP/1.1
4346	The Transport Layer Security(TLS) Protocol Version 1.1	TLS
5246	The Transport Layer Security(TLS) Protocol Version 1.2	TLS 1.2
7540	Hypertext Transfer Protocol Version 2(HTTP/2)	HTTP/2
8446	The Transport Layer Security(TLS) Protocol Version 1.3	TLS 1.3

각 계층이 연계하여 동작하는 구조

- 캡슐화와 비캡슐화

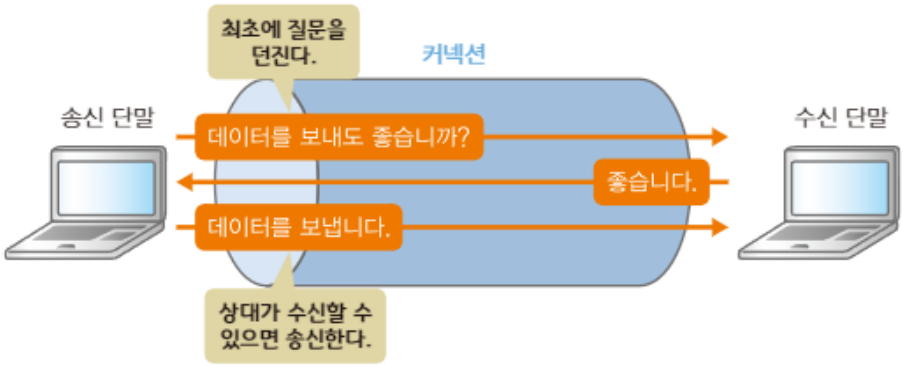
송신 단말은 애플리케이션 계층에서 순서대로 각 계층에서 페이로드에 헤더를 붙여 PDU로 만들어 한 단계 아래 계층으로 전달합니다. 헤더를 추가하는 처리를 **캡슐화**(encapsulation)라고 합니다.



- 커넥션 타입과 커넥션리스 타입

각 계층의 프로토콜은 **커넥션 타입**(connection type, 연결형) 또는 **커넥션리스 타입**(connectionless type, 비연결형)이라는 상이한 두 종류의 데이터 전송 서비스를 상위 계층에 제공합니다.

커넥션 타입은 확실하게 정해진 순서를 따르므로 전송에는 다소 시간이 걸리지만 데이터를 확실하게 전송할 수 있습니다.



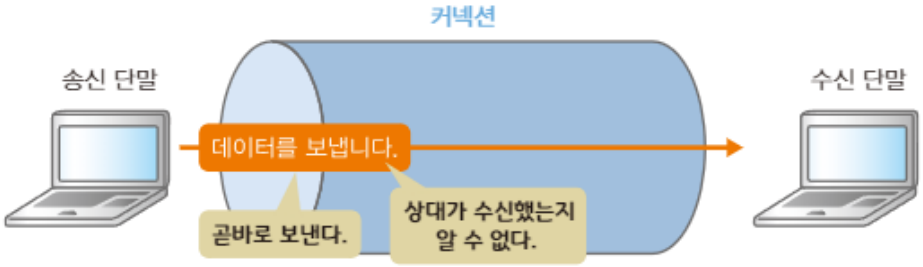

```
* 특징
    - 데이터 전송 전에 반드시 **세션(Session) 또는 연결(Connection)**을 설정해야 함.
    - 전송되는 데이터의 순서가 보장됨.
    - 신뢰성이 높음 (데이터 손실 시 재전송 메커니즘을 제공).
    - 데이터 전송이 끝나면 연결을 해제하여 네트워크 자원을 해방함.
    - 지연 시간이 비교적 큼 (연결 설정과 종료 과정이 필요하기 때문).

* 사용 예시
    * TCP (Transmission Control Protocol)
        - 웹 브라우징 (HTTP, HTTPS) → 웹 페이지 요청 및 응답 처리
        - 파일 전송 (FTP, SFTP) → 안정적인 파일 전송
        - 이메일 송수신 (SMTP, IMAP, POP3) → 메일 전송 시 데이터 손실 없이 정확히 전달
        - 화상회의, 온라인 게임 (QoS 적용) → 데이터 순서 보장과 신뢰성이 중요한 경우

    * 전화 통화 (VoIP, PSTN 등)
        - 전화 통화를 시작하면 통화가 끝날 때까지 지속적으로 연결 유지

    * 은행 거래 (온라인 뱅킹, 결제 시스템)
        - 신뢰성이 중요한 금융 거래에서 데이터의 정확한 전송을 보장
```

커넥션리스 타입은 곧바로 데이터를 보내면서 커넥션을 확립한 뒤 마음대로 종료합니다.




```
* 특징
    - 연결 설정 없이 데이터를 독립적인 패킷(데이터그램) 단위로 전송합니다.
    - 빠르고 가벼움: 연결 설정 과정이 없어서 속도가 빠르고 오버헤드가 적습니다.
    - 신뢰성이 낮음: 패킷이 손실될 수 있으며, 도착 순서를 보장하지 않습니다.
    - 대표적인 프로토콜: UDP (User Datagram Protocol)

* 사용 예시
```

```
    - 실시간 스트리밍 (YouTube, Netflix)
    - 온라인 게임 (LoL, 배틀그라운드)
    - VoIP (인터넷 전화, Zoom, Skype)
```

네트워크 구성 기기

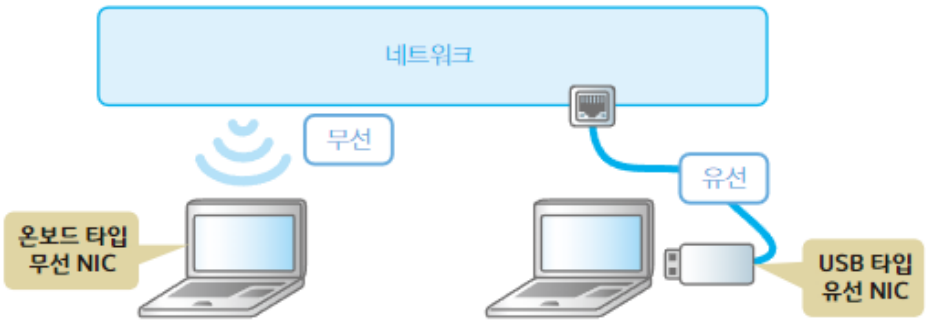
계층	계층 이름	NIC	리피터	리피터 허브	미디어 컨버터	액세스 포인트	브리지	L2 스위치	라우터	L3 스위치	방화벽	차세대 방화벽	WAF	부하 분산 장치
7계층	애플리케이션 계층													
4계층	트랜스포트 계층													
3계층	네트워크 계층													
2계층	데이터링크 계층													
1계층	물리 계층													

물리 계층에서 동작하는 기기

물리 계층은 케이블이나 커넥터 형태, 핀 할당(핀 배열) 등 물리적인 사양에 관해 모두 정의되어 있는 계층입니다.

- NIC (Network Interface Card)

NIC는 PC나 서버 등 컴퓨터를 네트워크에 연결하기 위해 필요한 하드웨어입니다. 모든 네트워크 단말은 애플리케이션과 운영체제가 처리한 패킷을 NIC를 이용해 LAN 케이블이나 전파로 보냅니다.

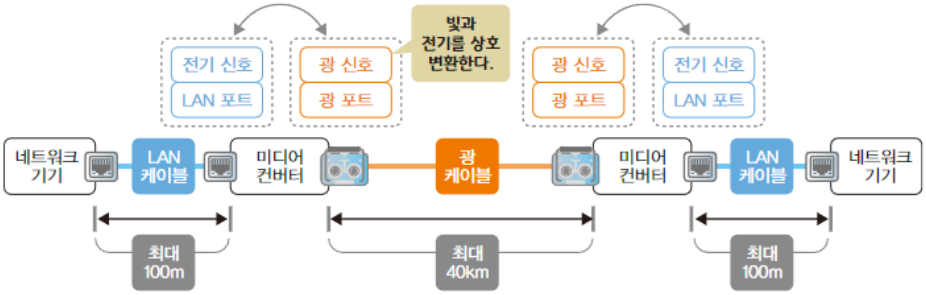


- 리피터

LAN 케이블에 흐르는 전기 신호는 전송 거리가 길수록 감쇠하며, 100m 정도 되면 파형이 깨집니다. **리피터**(repeater)는 파형을 한 번 더 증폭해서 정돈한 뒤 다른 쪽으로 전송합니다. 이렇게 함으로써 전송 거리를 늘려 패킷이 더 멀리까지 도달하게 합니다.

- 미디어 컨버터

미디어 컨버터(media converter)는 전기 신호와 광 신호를 서로 교환하는 기기입니다. 광섬유 케이블을 연결하지 못하는 기기만 있는 상황에서 네트워크를 연장하고자 할 때 사용합니다. 전기 신호는 감쇠가 심하고, LAN 케이블은 100m 이상 늘릴 수 없습니다. 그렇게 되면 광섬유 케이블을 이용해야만 하나, 광섬유 케이블과 함께 이용하는 기기는 가격이 높기 때문에 섣불리 사용할 수 없습니다.



데이터링크 계층에서 동작하는 기기

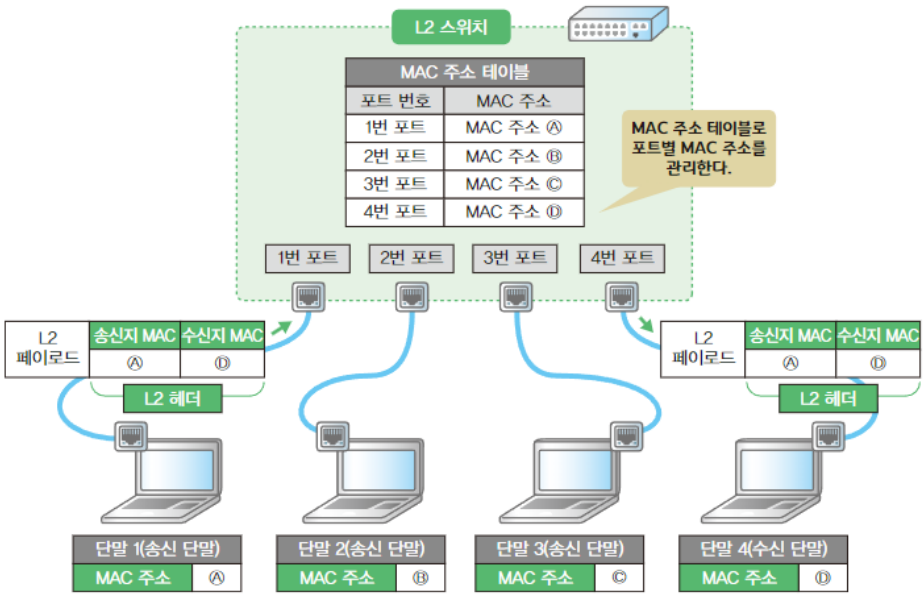
데이터링크 계층은 물리 계층의 신뢰성을 확보하고, 같은 네트워크에 있는 단말과 연결할 수 있도록 하는 계층입니다. 데이터링크 계층에서 동작하는 기기는 프레임 헤더에 포함된 **MAC 주소**(MAC address)의 정보에 기반해 프레임을 전송합니다.

- 브리지

브리지(bridge)는 이름 그대로 포트와 포트 사이의 '다리' 역할을 담당합니다. 단말에서 받아들인 MAC 어드레스를 MAC 주소 테이블(MAC address table)이라는 테이블로 관리하고, 전송 처리 합니다. 이 전송 처리를 브리징(bridging)이라 부릅니다.

- L2 스위치

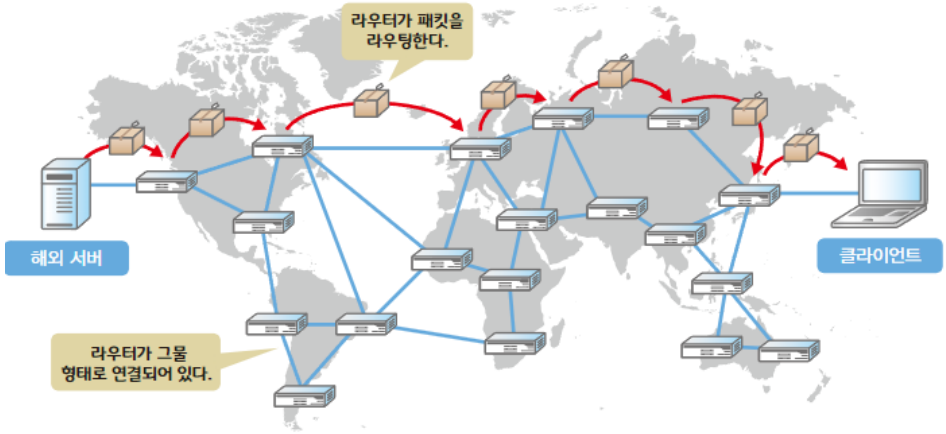
L2 스위치(L2 switch)는 많은 포트를 가진 브리지 입니다. 스위칭 허브(switching hub) 혹은 간단히 스위치(switch)라 부르기도 합니다. L2 스위치의 기본 기능은 브리지와 같습니다. 단말에서 받아 들인 프레임의 MAC 주소를 MAC 주소 테이블로 관리하고, 전송 처리합니다.



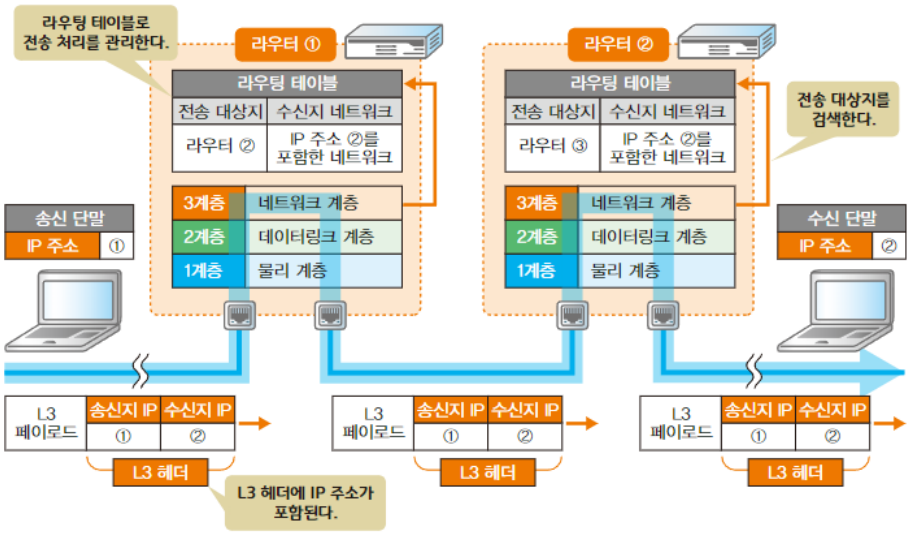
네트워크 계층에서 동작하는 기기

네트워크 계층은 네트워크와 네트워크를 연결하는 계층입니다. 네트워크 계층에서 동작하는 기기는 IP 패킷의 헤더에 포함된 IP 주소의 정보에 기반해 패킷을 전송합니다. IP 주소는 네트워크 계층에서의 주소, 즉 식별자에 해당합니다.

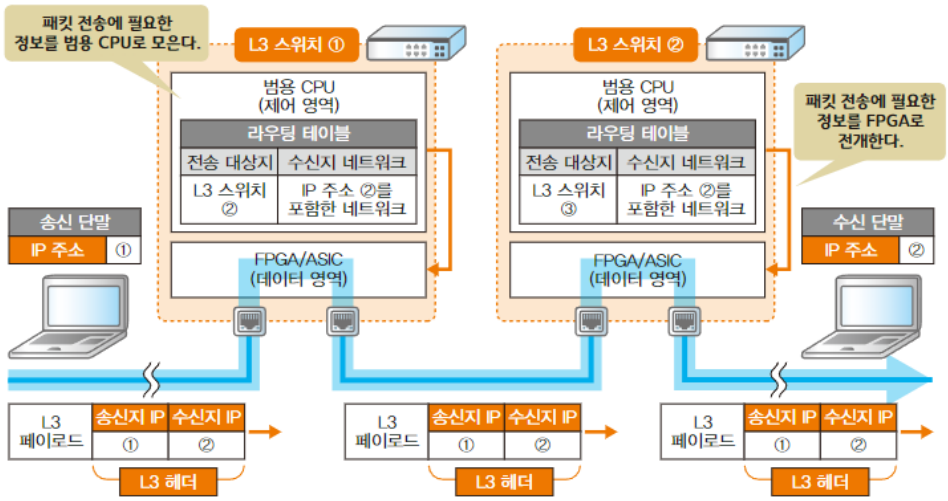
- 라우터 라우터(router)는 단말로부터 받아들인 IP 패킷의 IP 주소를 보고, 자신이 속한 네트워크를 넘은 범위에 있는 단말로 전달하는 역할을 담당합니다.



라우터는 라우팅 테이블(routing table)이라는 테이블에 기반해서 패킷을 전송할 대상지를 관리합니다.



- L3 스위치 L3 스위치(L3 switch)는 간단히 말하면 라우터에 L2 스위치를 추가한 기기입니다.L3 스위치는 MAC 주소 테이블과 라우팅 테이블을 조합한 정보를 FPGA(Field Programmable Gate Array)나 ASIC(Application Specific Intergrated Circuit)등의 패킷 전송 처리 전용 하드웨에 기록하고, 그 정보를 기반으로 스위칭 혹은 라우팅 합니다.

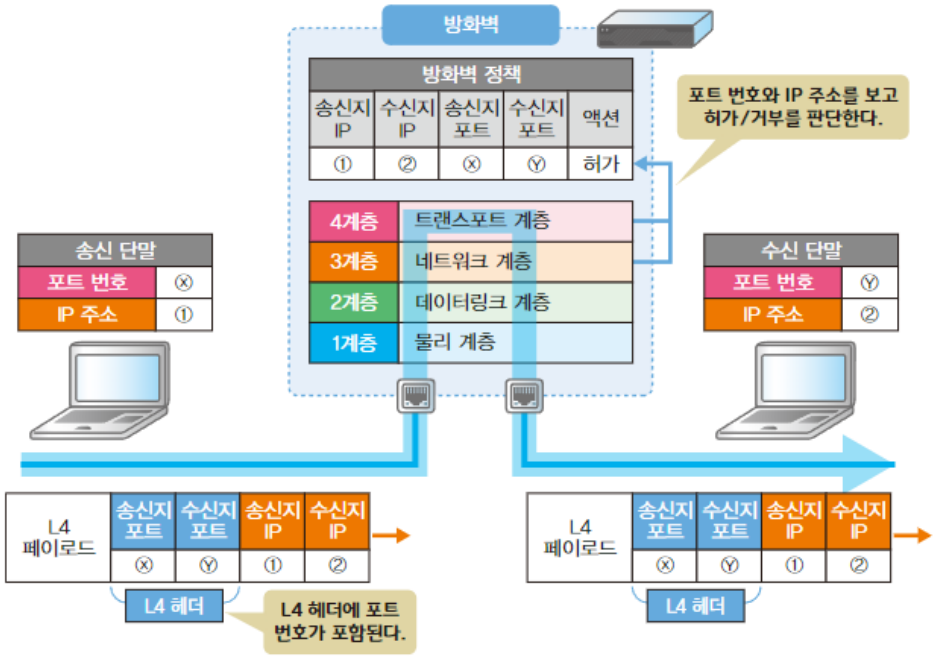


트랜스포트 계층에서 동작하는 기기

트랜스포트 계층은 애플리케이션을 식별하고, 그 요건에 맞게 통신제어하는 계층입니다. 트랜스포트 계층에서 동작하는 기기는 세그먼트(TCP) 또는 데이터그램(UDP)의 헤더를 포함한 '포트번호'에 기반하여 패킷 전송합니다. 포트 번호는 서비스를 식별하기 위한 번호입니다.

- 방화벽

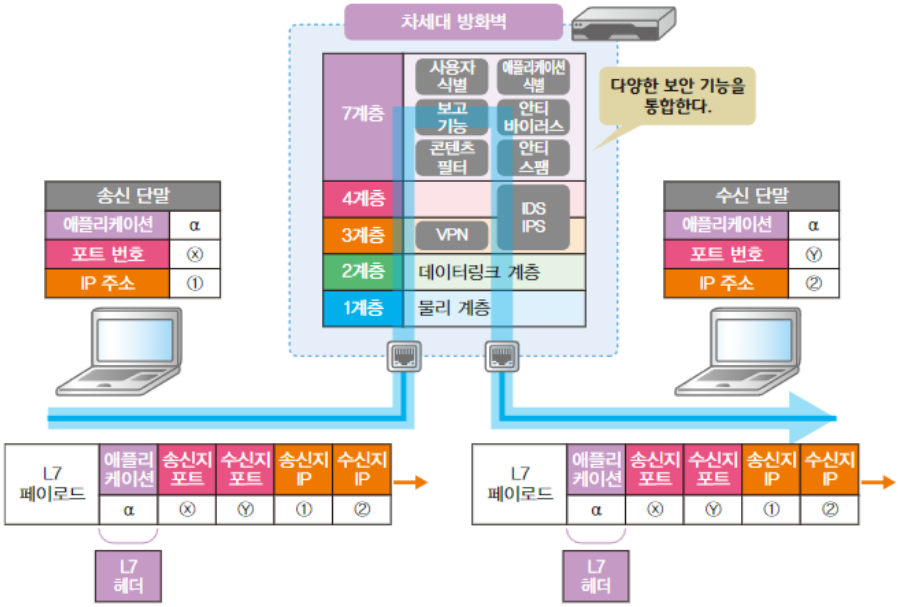
방화벽(firewall)은 네트워크의 안전을 지키기 위해 이용하는 기기입니다.방화벽은 단말 사이에서 교화되는 패킷의 IP 주소나 포트번호를 보고, 통신을 허가하거나 차단합니다.이 통신 제어 기술을 스테이트풀 인스펙션(stateful inspection, 상태 추적 기반 방화벽)이라 부릅니다.



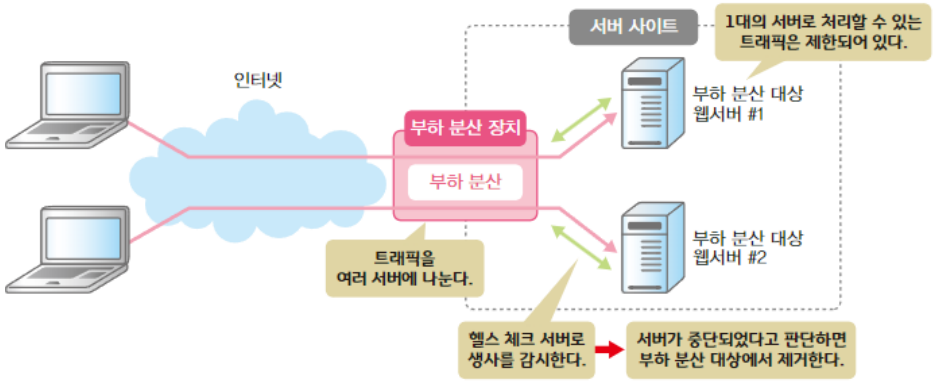
애플리케이션 계층에서 동작하는 기기

- 차세대 방화벽

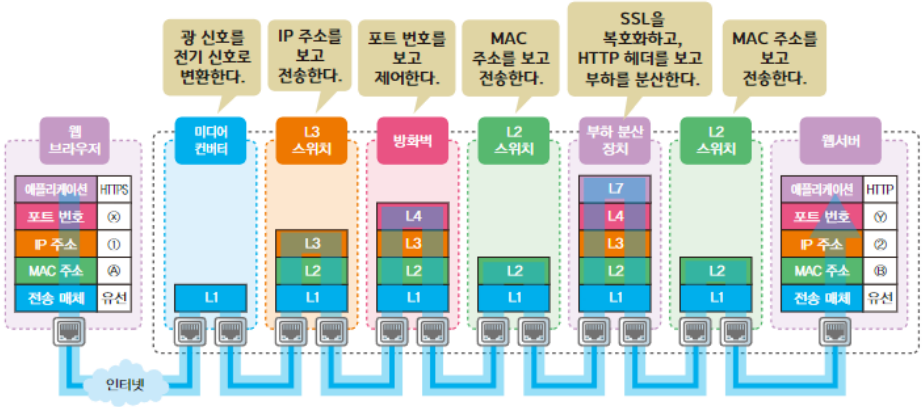
차세대 방화벽(next-generation firewall)은 앞서 설명한 방화벽(전통적 방화벽)이 진화한 버전입니다. 스테이트풀 인스펙션과 함께 VPN이나 IDS(Intrusion Detection System, 침입 탐지 시스템)/IPS(Intrusion Prevention System, 침입 차단 시스템) 등 다양한 보안기능을 넣은 통합화를 추구합니다.



- 부하 분산 장치 (L7 스위치) 부하 분산 장치는 이름 그대로 서버의 부하를 분산하는 기기입니다. 서버 1대로 처리할 수 있는 트래픽(traffic, 통신 데이터)의 양은 제한이 있습니다. 부하 분산 장치는 클라이언트로부터 받아들인 패킷을 부하 분산 방식(load balancing, 로드 밸런싱)이라는 방법에 근거해, 뒤쪽에 있는 여러 서버들로 나눔으로써 시스템 전체적으로 처리 가능한 트래픽 양을 확장하는 것을 목표로 합니다. 또한 헬스 체크(HC, Health Check)를 통해 정기적으로 서버를 감시함으로써, 장애가 발생한 서버를 부하 분산 대상에서 제외해 서비스의 가용성을 향상함을 목표로 합니다.

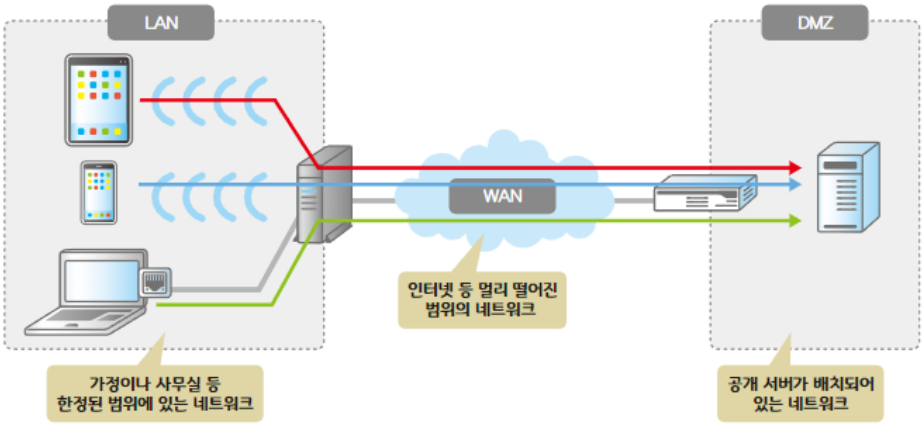


모든 기기 연결



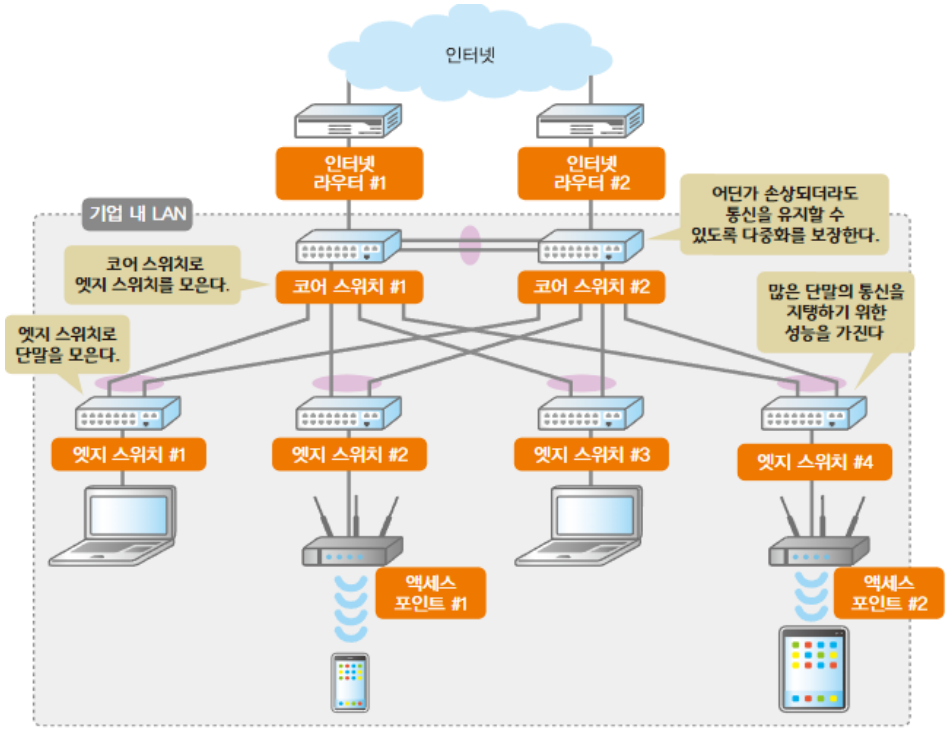
네트워크 형태

'네트워크'는 매우 다양하며, 이를 구성하는 네트워크 기기 또한 여러 가지 입니다.



LAN

LAN은 'Local Area Network'의 약자로, 가정이나 기업 등 한정된 범위의 네트워크를 의미합니다. 기업의 LAN 역시, 기본적으로 크게 다르지 않지만 구성하는 네트워크 기기의 성능과 기능이 크게 다릅니다.

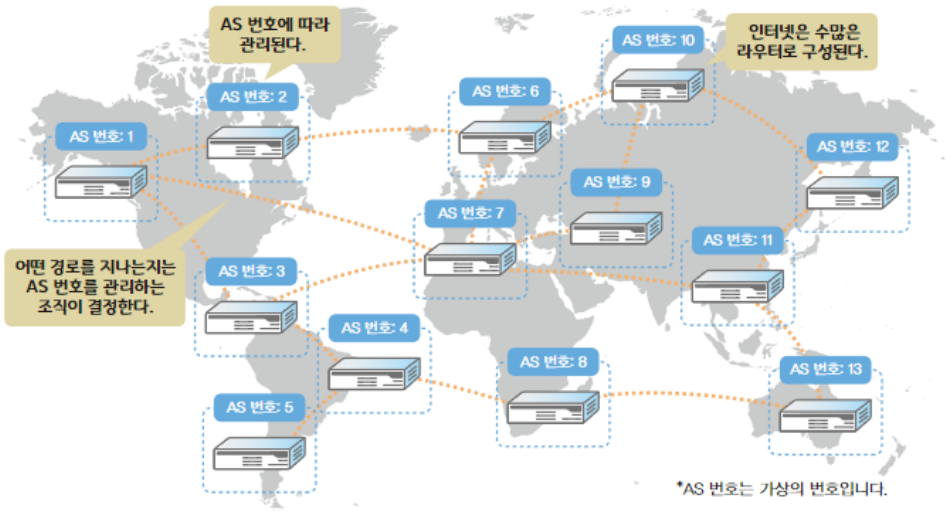


WAN

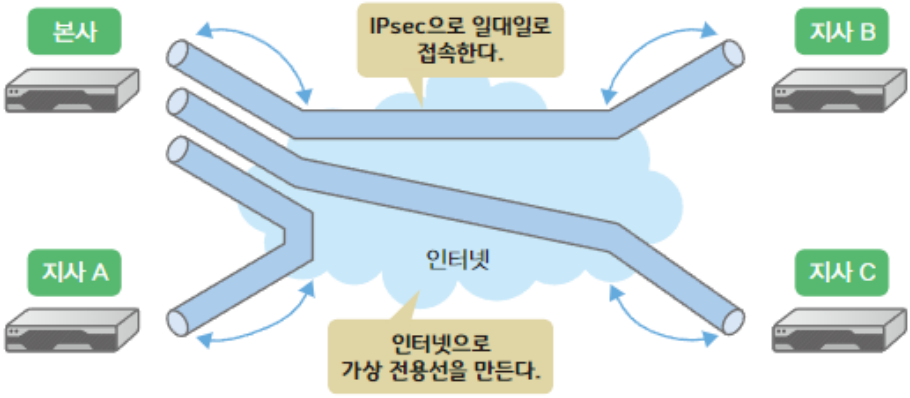
WAN은 'Wide Area Network' 의 약자로 거리상 멀리 떨어진 범위의 네트워크를 의미합니다. WAN은 크게 인터넷(internet)과 VPN을 사용한 내부망(closed-area VPN network)으로 나뉠 수 있으며, 그 용도가 크게 다릅니다.

- 인터넷

인터넷는 공중 WAN을 의미합니다. 인터넷은 간단히 말하면 라우터의 집합입니다. 인터넷 서비스 제공자(Internet Service Provider, ISP)나 연구 기관, 기업 등이 가진 수많은 라우터가 산과 계곡을 넘고, 바다를 건너고, 국경을 넘어 연결되어 셀 수 없는 많은 패킷을 운반하고 있습니다.



- 폐역 VPN망 폐역 VPN망은 LAN과 LAN을 연결하는 네트워크를 의미합니다. VPN은 'Virtual Private Network'의 약자로 인터넷상에 가상의 전용선(터널)을 만드는 기능입니다. IPsec이라는 프로토콜을 이용해 거점 사이를 피어-투-피어(peer-to-peer), 즉 일대일로 연결하고 해당 통신을 암호화 합니다.



DMZ

DMZ는 'DeMilitarized Zone'의 약자로, 인터넷에 공개하는 서버를 설치한 네트워크를 의미합니다. DMZ의 기본은 서버가 제공하는 서비스를 안정적으로 가동하는 것입니다. 그리고 그 안정적인 가동을 위해 반드시 필요한 기능이 다중화(redundancy)입니다. DMZ에서는 어떤 기기가 고장나더라도, 어떤 케이블이 끊어지더라도 경로가 즉시 전환되어 서비스를 계속 제공할 수 있도록 동일한 종류의 네트워크 기기를 병렬로 배치합니다.