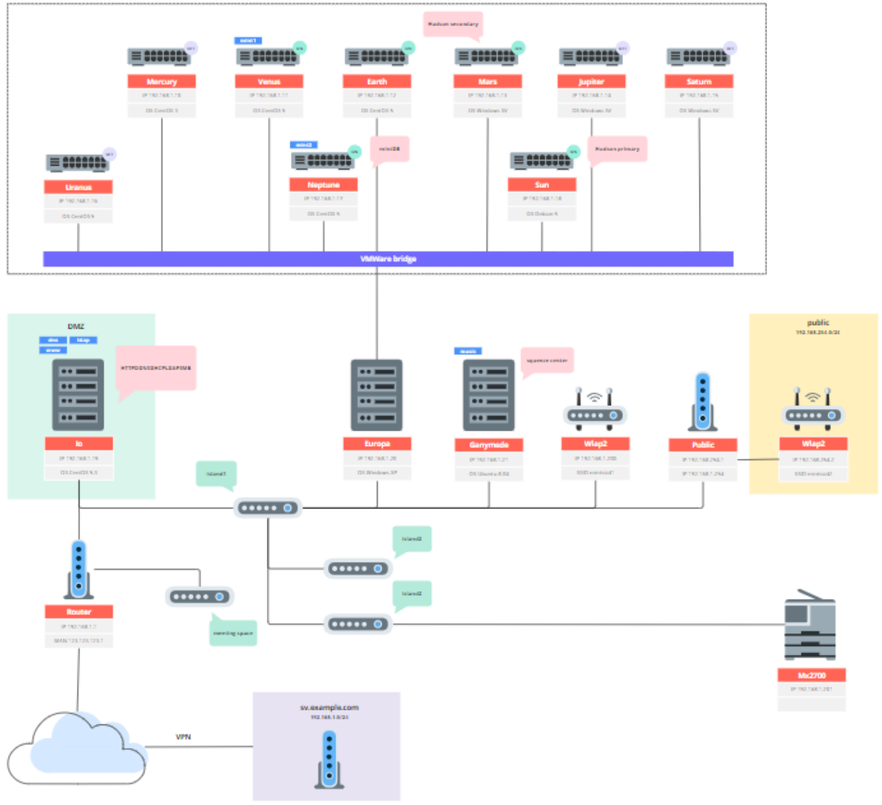
인터넷, 네트워크 그리고 서버

네트워크 시작

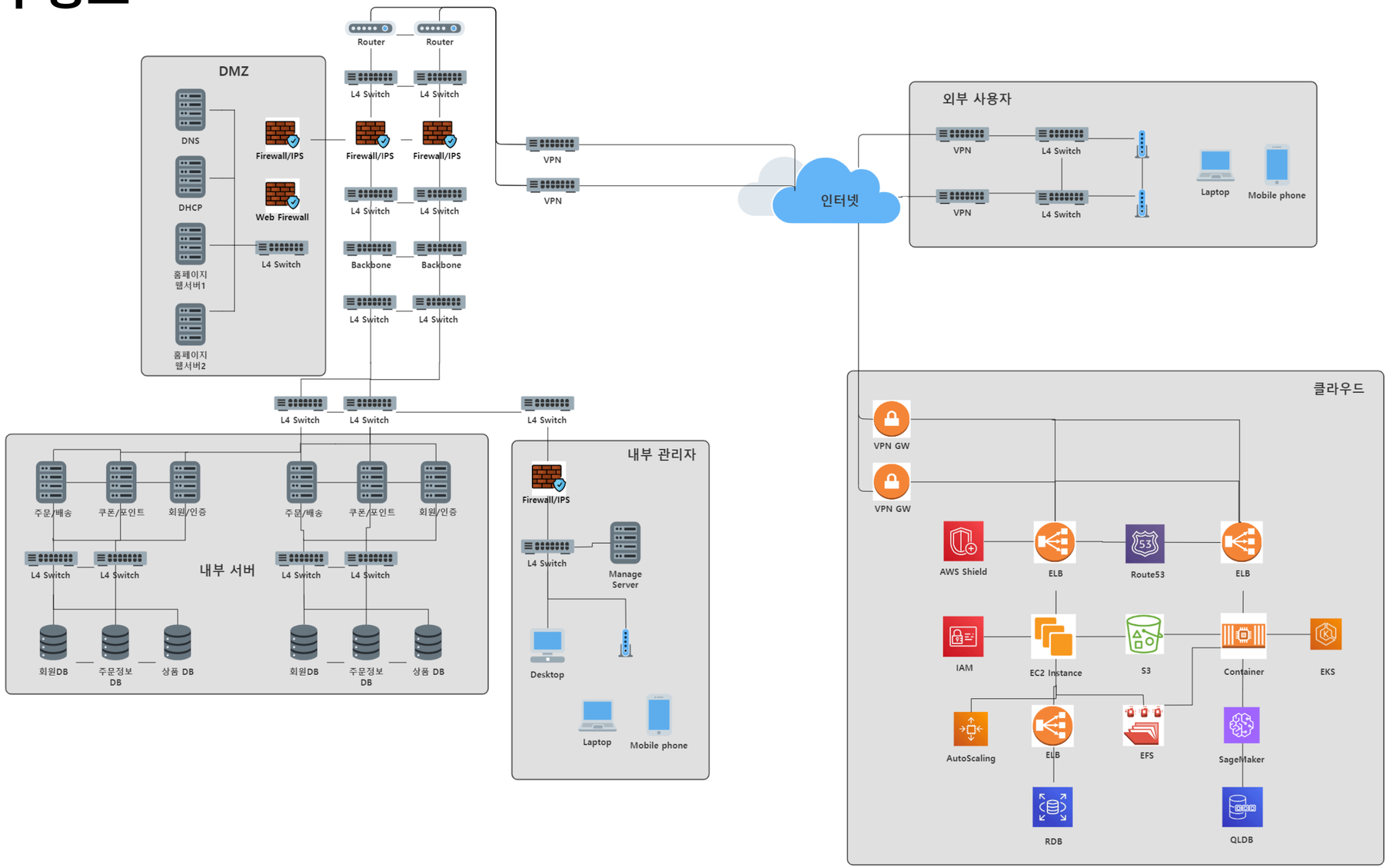
네트워크 기본 개념

IT 인프라 구성도란?

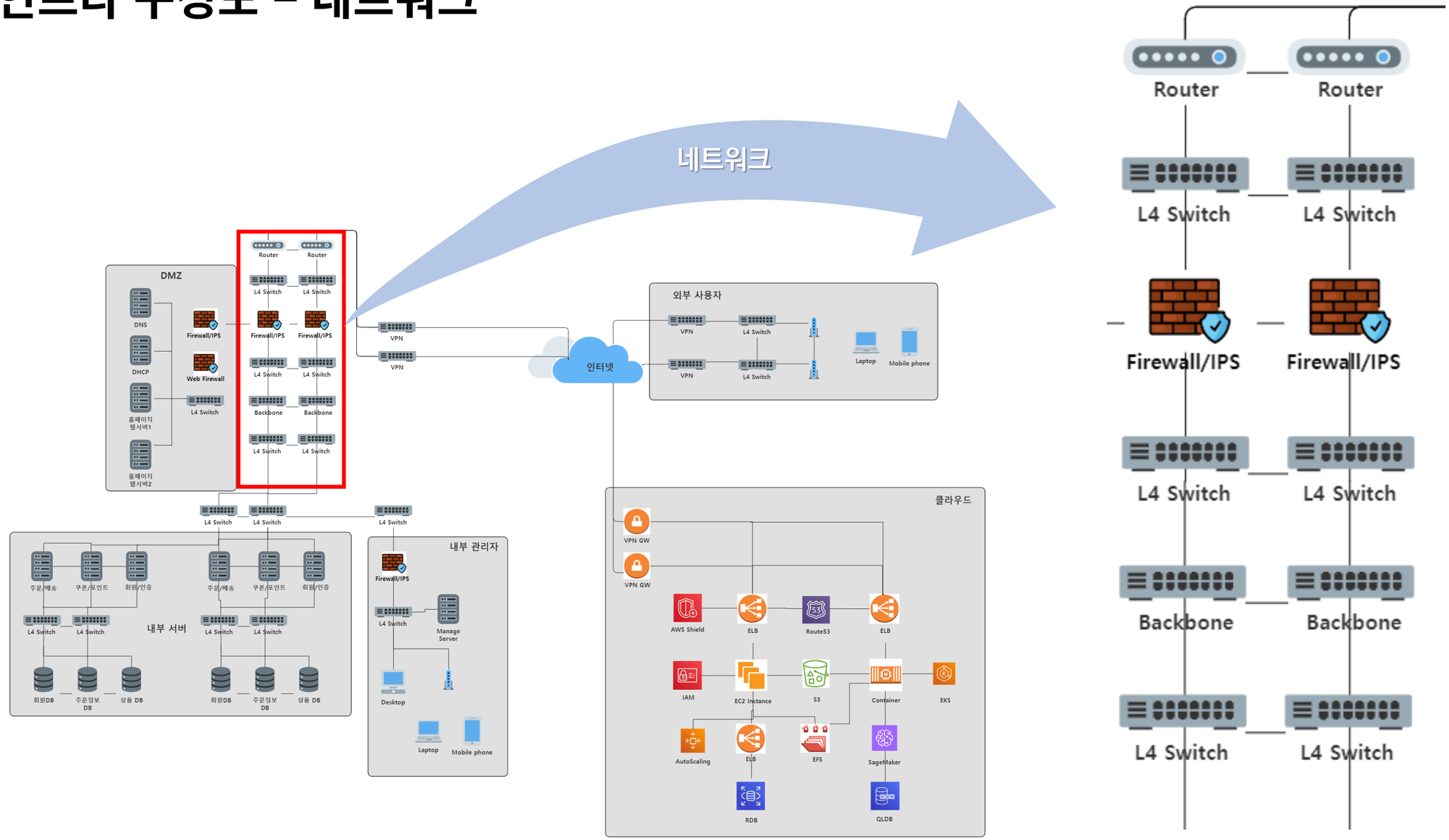
- IT 인프라 구성 등을 한 눈에 알아볼 수 있는 다이어그램 또는 구성도
- 시스템의 배치 연결관계를 아이콘, 선으로 구조화



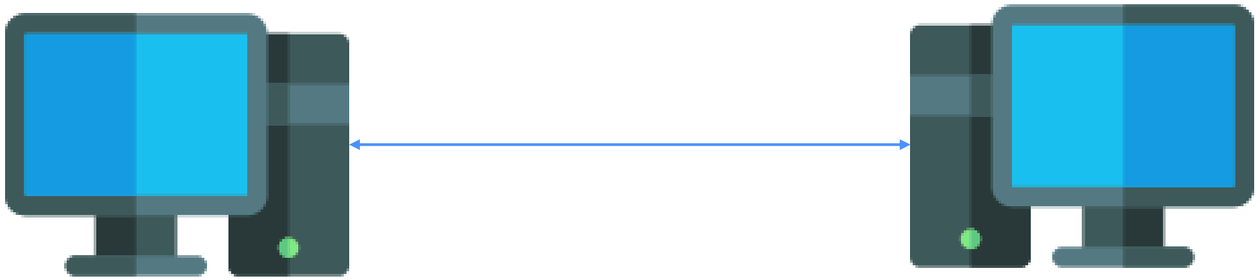
IT 인프라 구성도


DMZ
DNS
DHCP
홈페이지 웹서버1
홈페이지 웹서버2
Firewall/IPS
Web Firewall
L4 Switch
Router
Router
L4 Switch
L4 Switch
Firewall/IPS
Firewall/IPS
Firewall/IPS
L4 Switch
L4 Switch
L4 Switch
L4 Switch
Backbone
Backbone
L4 Switch
L4 Switch
VPN
VPN
인터넷
외부 사용자
VPN
VPN
L4 Switch
L4 Switch
Laptop
Mobile phone
L4 Switch
L4 Switch
L4 Switch
주문/배송
쿠폰/포인트
회원/인증
주문/배송
쿠폰/포인트
회원/인증
L4 Switch
L4 Switch
L4 Switch
L4 Switch
내부 서버
회원DB
주문정보 DB
상품 DB
회원DB
주문정보 DB
상품 DB
내부 관리자
Firewall/IPS
L4 Switch
Manage Server
Desktop
Laptop
Mobile phone
클라우드
VPN GW
VPN GW
AWS Shield
ELB
Route53
ELB
IAM
EC2 Instance
S3
Container
EKS
AutoScaling
ELB
EFS
SageMaker
RDB
QLDB

IT 인프라 구성도 – 네트워크



네트워크란 무엇인가?



- 가장 간단한 형태의 네트워크는 "서로 연결된 두 대의 컴퓨터가 자원을 공유하는 것"입니다.

- 네트워크는 두 가지 주요 측면으로 구성됩니다:
    - 물리적 연결 (선, 케이블, 무선 매체)
    - 논리적 연결 (물리적 매체를 통해 데이터가 전송됨)

네트워크의 구성요소

- 전송 단말기 (노드)
  - 정보를 주고 받는 장치
  - PC, 휴대폰, 노트북, 서버 등
- 전송 매체
  - 정보를 전달할 수 있는 수단
  - 유선케이블 : 동축케이블, 광케이블, LAN 케이블 등
  - 무선기술: Wifi, 5G, LTE, 블루투스 등
- 네트워크 장비
  - 정보를 전달하기 위해 목적지를 찾고 길을 결정하는 장비 (허브, 스위치, 라우터 등)

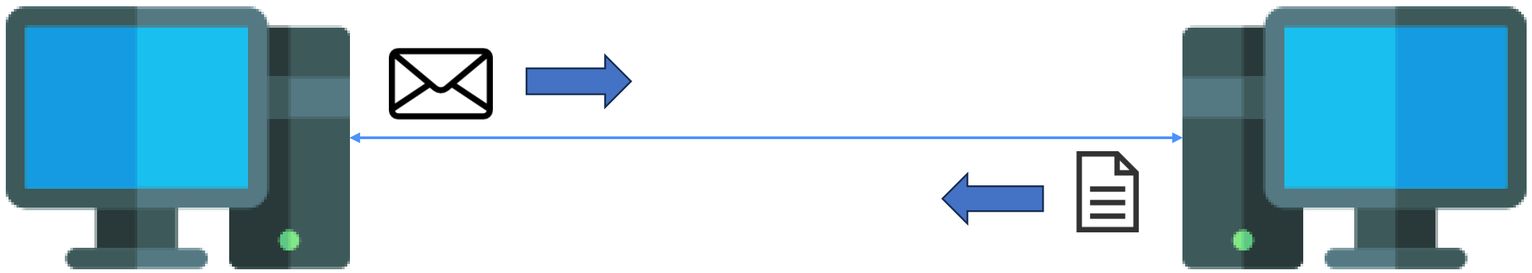
네트워킹 기본 개념

- "네트워크의 컴퓨터들은 데이터를 전송하고 수신하기 위해 동일한 절차를 사용해야 합니다. 이를 **통신 프로토콜**이라고 부릅니다."

- "데이터는 손상되지 않고 전달되어야 합니다. 손상되면 쓸모가 없습니다. (예외가 있을 수 있습니다.)"

- "네트워크의 컴퓨터는 정보의 **출처**와 **목적지**를 결정할 수 있어야 합니다. 예를 들어, 각각의 **IP 주소**와 **MAC 주소**를 알아야 합니다."

컴퓨터 네트워킹 프로토콜



- "컴퓨터들은 네트워크 프로토콜을 사용하여 서로 통신합니다.“
- "프로토콜은 기계가 데이터를 교환하고 효과적인 통신을 가능하게 하는 규칙입니다."
- 일상적인 예시:
  - "누군가에게 전화를 걸 때, 전화를 들고 신호음이 있는지 확인한 후, 번호를 누릅니다.“
  - "차를 운전할 때 도로의 규칙을 준수합니다."

프로토콜

- 물리적 프로토콜: 매체(배선), 연결(RJ-45 포트) 및 신호(전선의 전압 수준)를 설명합니다.
- 논리적 프로토콜: 데이터가 언제 어떻게 컴퓨터로 전송되고 수신되는지를 제어하는 소프트웨어로, 물리적 프로토콜을 지원합니다.
- "컴퓨터 네트워크는 제대로 작동하기 위해 여러 가지 다른 유형의 프로토콜에 의존합니다."
- 일반적인 TCP/IP 프로토콜 예시:
  - 웹 통신: HTTP
  - 이메일: POP3, SMTP, IMAP
  - 파일 전송: FTP

계층구조 개요

계층구조

- OSI(Open Systems Interconnection) 모델
  - 개념적 프레임워크로, 네트워크 프로토콜이 통신하는 구조를 7개의 계층으로 분리하여 각 계층간 상호 작동하는 방식을 정한 모델
  - 1977년에 국제 표준화 기구(ISO)에 의해 개발

- 목적
  - 통신이 일어나는 과정을 7단계로 크게 구분하여 한 눈에 들어올 수 있도록 정의

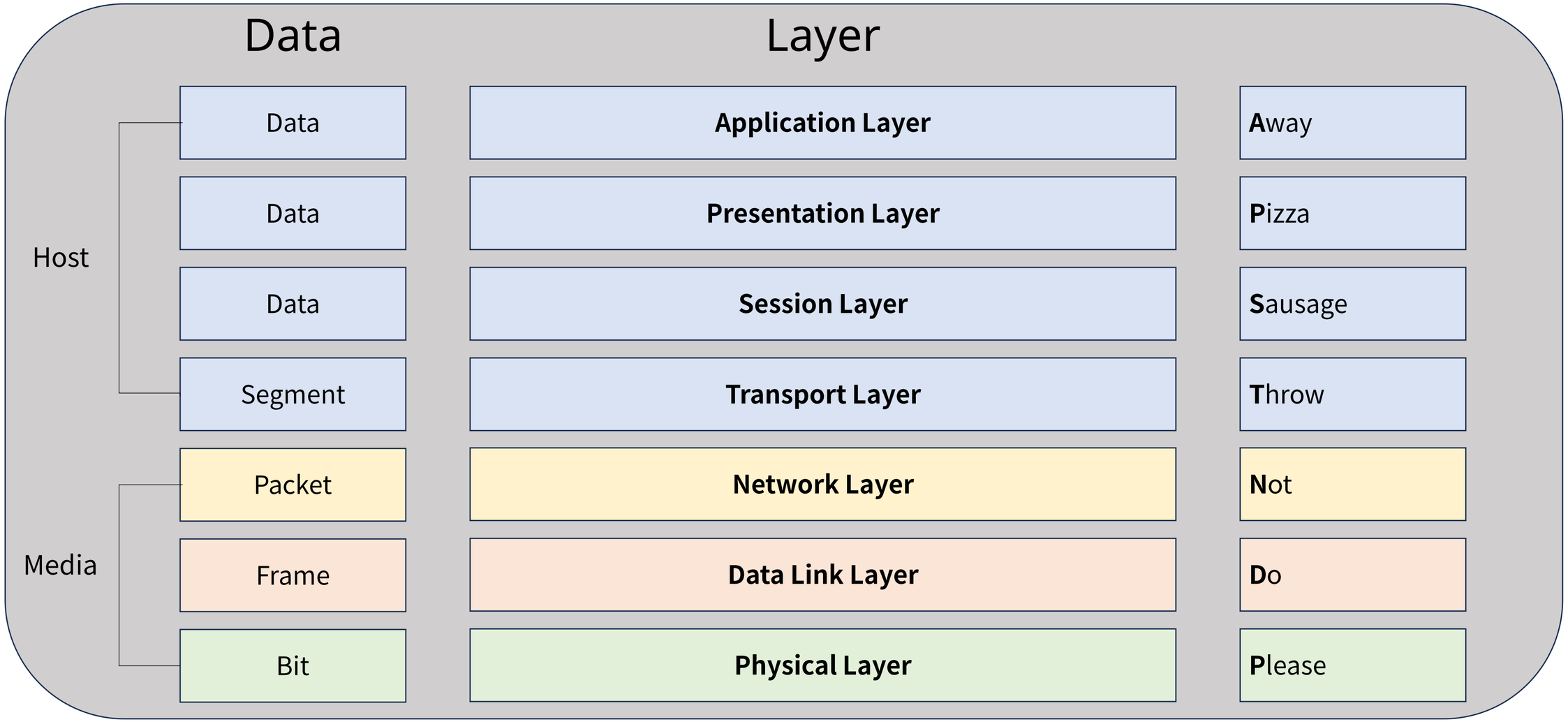
OSI 모델 스택

- OSI 모델은 컴퓨터 간의 네트워크 통신을 7개의 계층으로 나누어 복잡한 작업을 분해합니다.

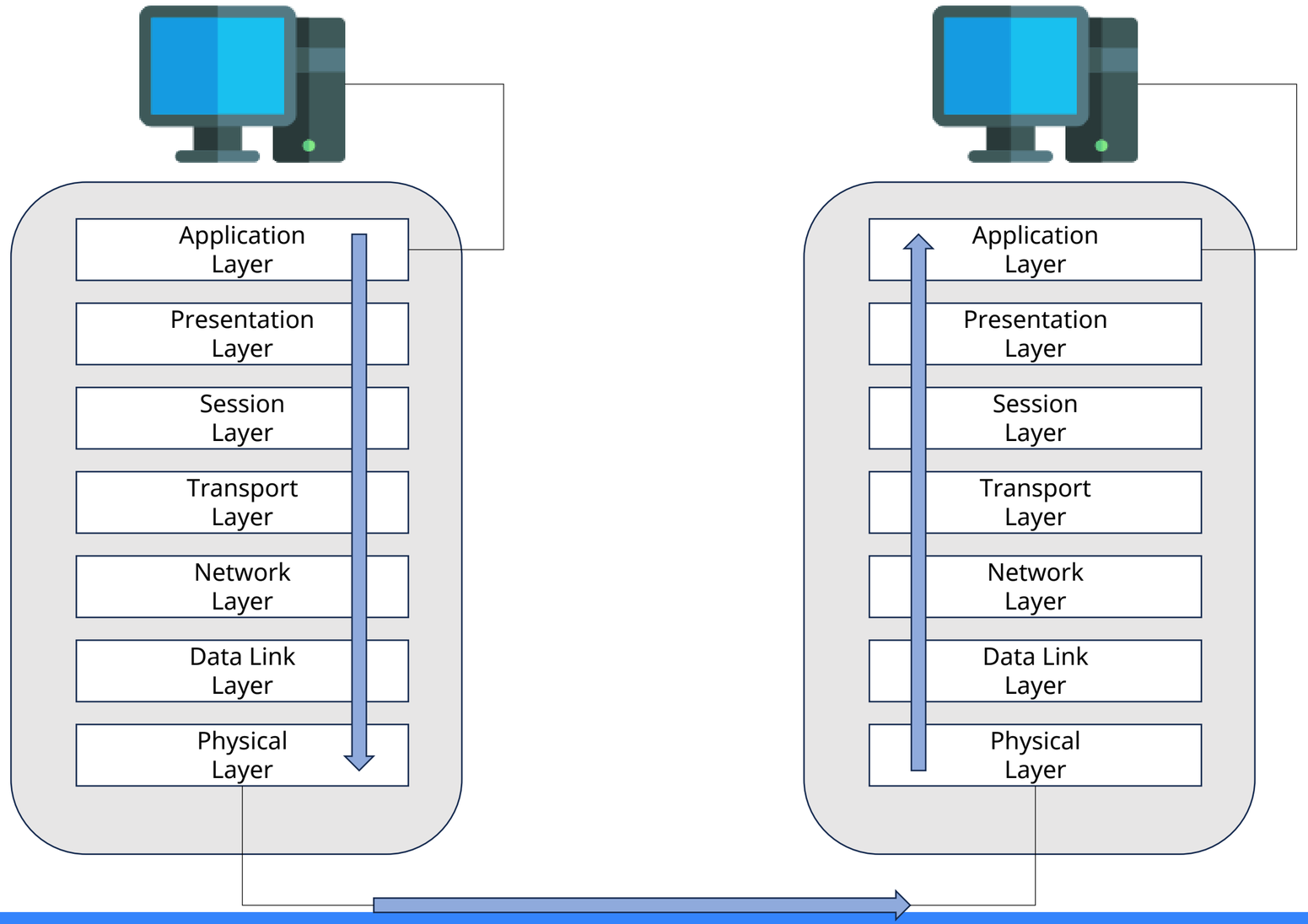
- 상위 계층 (호스트 계층)
    - 호스트 컴퓨터가 처리하며, 데이터 포맷팅, 암호화 및 연결 관리와 같은 애플리케이션 특정 기능을 수행합니다.

- 하위 계층 (미디어 계층)
    - 라우팅, 주소 지정 및 흐름 제어와 같은 네트워크 특정 기능을 제공합니다.

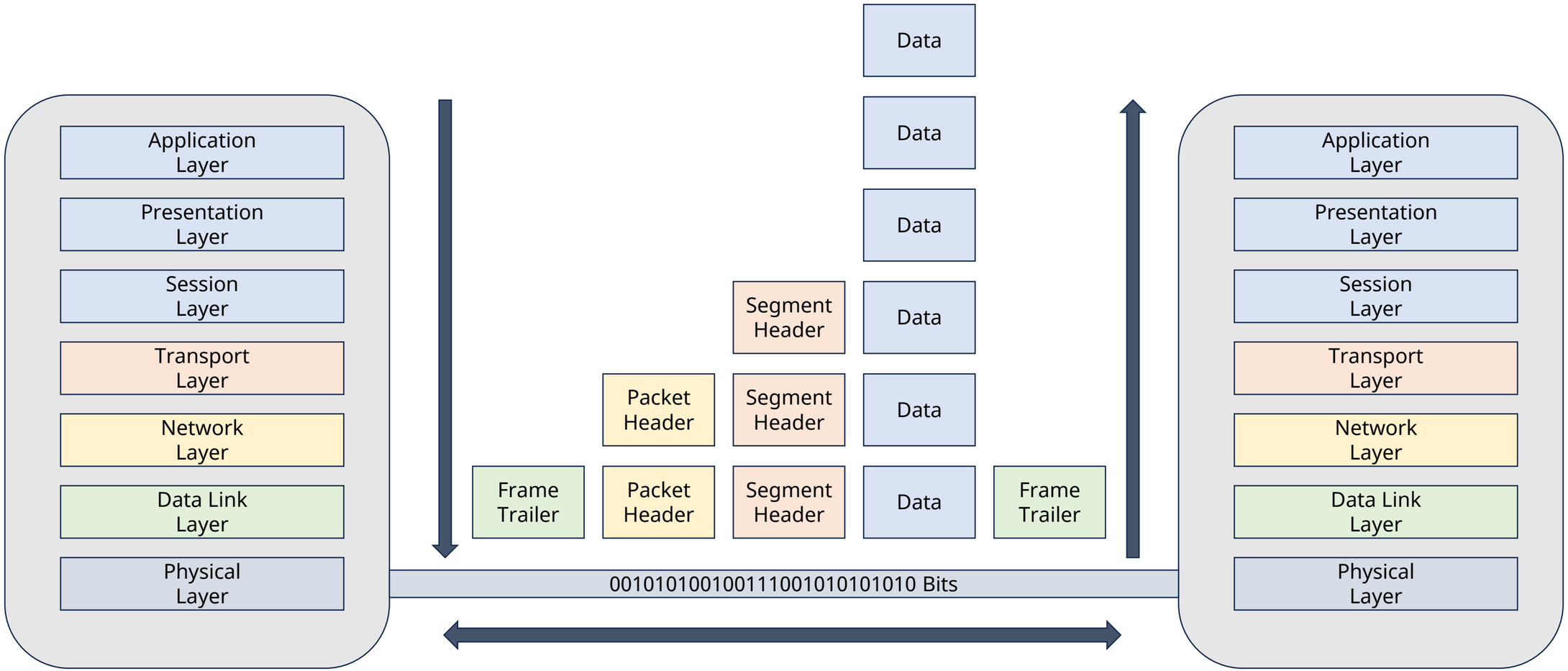
OSI 모델 시각화


Data
Layer
Data
Application Layer
Away
Data
Presentation Layer
Pizza
Host
Data
Session Layer
Sausage
Segment
Transport Layer
Throw
Packet
Network Layer
Not
Media
Frame
Data Link Layer
Do
Bit
Physical Layer
Please

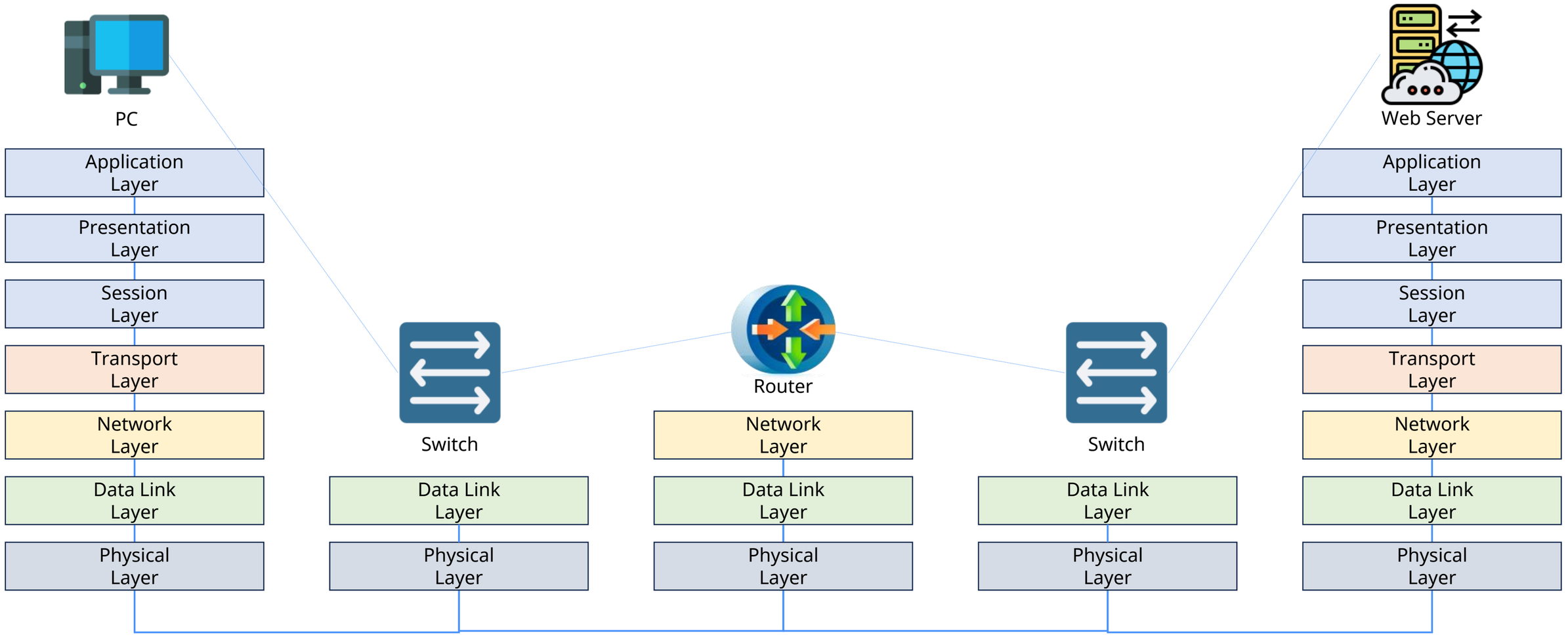
OSI 커뮤니케이션


Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer
Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

OSI Encapsulation & De - Encapsulation



OSI Encapsulation & De - Encapsulation



데이터 이동하는 경로 LAN과 WAN 구별

네트워크의 종류

- 개인 영역 네트워크 (PAN - Personal Area Network)
- 로컬 영역 네트워크 (LAN - Local Area Network)
- 무선 로컬 영역 네트워크 (WLAN - Wireless Local Area Network)
- 캠퍼스 영역 네트워크 (CAN - Campus Area Network)
- 대도시 지역 네트워크 (MAN - Metropolitan Area Network)
- 광역 네트워크 (WAN - Wide Area Network)

개인 영역 네트워크 (PAN - Personal Area Network)

- "데이터를 한 장치에서 다른 장치로 공유하기 위해 개인 용도로 사용되는 초소형 네트워크입니다.“

- 유선(PAN) 또는 무선(WPAN)일 수 있습니다
  - USB
  - 블루투스
  - NFC
  - ANT+

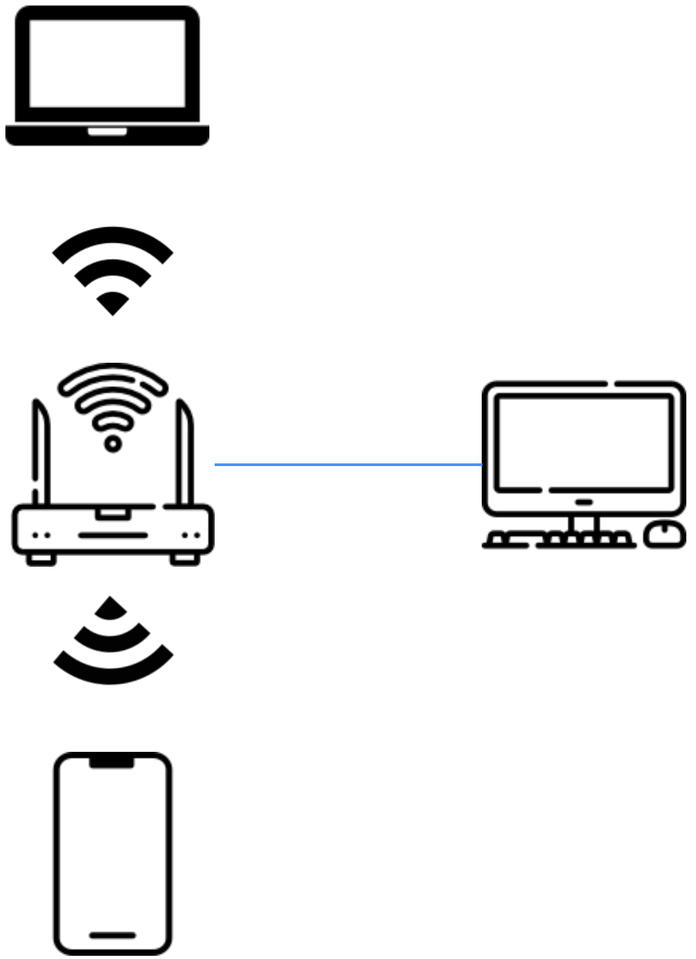
- 예시:
  - 스마트폰과 노트북 간의 연결
  - 스마트 워치와 스마트폰 간의 연결
  - 스마트폰 핸즈 프리 자동차 통화
  - 심박수 모니터와 스마트폰 간의 연결

로컬 영역 네트워크 (LAN - Local Area Network)

- "단일 방, 건물 또는 여러 건물과 같은 작은 지리적 영역 내의 컴퓨터 네트워크입니다.“

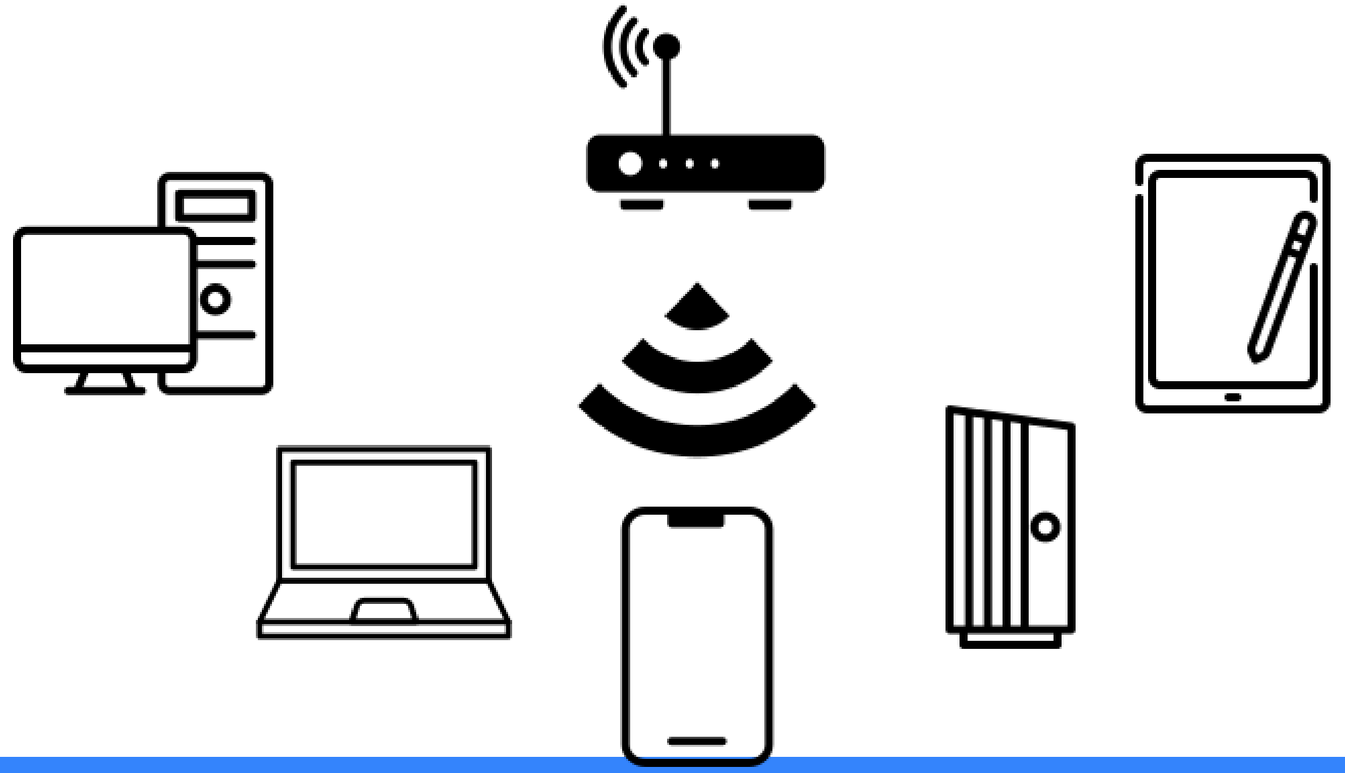
- "자급자족(Self-contained)으로 간주됩니다:
  - 모든 장치는 케이블 및/또는 단거리 무선 기술을 통해 직접 연결됩니다
  - 인터넷 서비스 제공업체(ISP)로부터 임대된 통신 회선이 필요하지 않습니다.

- "예시:
  - 가정용 네트워크
  - 소규모 비즈니스 또는 사무실 네트워크



무선 로컬 영역 네트워크 (WLAN - Wireless Local Area Network)

- "무선 연결에 의존하는 LAN이거나 기존의 유선 LAN을 무선 LAN으로 확장하는 네트워크입니다.“
- "대부분의 가정용 네트워크는 WLAN입니다."



캠퍼스 영역 네트워크 (CAN - Campus Area Network)

- "기업 비즈니스 파크, 정부 기관 또는 대학 캠퍼스와 같은 제한된 지리적 영역에서 여러 개의 LAN이 상호 연결된 컴퓨터 네트워크입니다.“
- "일반적으로 단일 주체에 의해 소유되거나 사용됩니다."

대도시 지역 네트워크 (MAN - Metropolitan Area Network)

- "도시 내에서 사용자와 컴퓨터 자원을 상호 연결하는 컴퓨터 네트워크입니다.“
- "캠퍼스 영역 네트워크보다 크지만, 광역 네트워크보다는 작은 규모입니다."

광역 네트워크 (WAN - Wide Area Network)

- "대규모 지리적 거리를 넘어 여러 도시와 국가에 걸쳐 확장되는 컴퓨터 네트워크입니다.“
- "WAN은 지리적으로 먼 LAN을 연결합니다.“
- "일반적으로 ISP로부터 임대된 통신 회선을 사용합니다.

- "예시:
    - 인터넷
    - 서로 다른 주에 있는 기업 사무실

네트워크의 종류

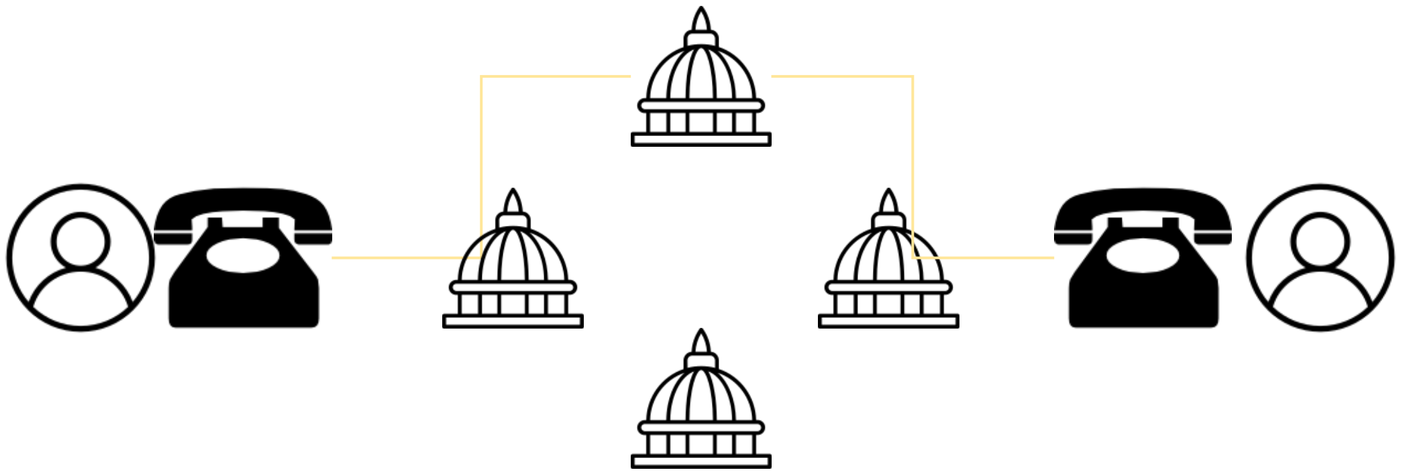
- 개인 영역 네트워크 (PAN - Personal Area Network)
- 로컬 영역 네트워크 (LAN - Local Area Network)
- 무선 로컬 영역 네트워크 (WLAN - Wireless Local Area Network)
- 캠퍼스 영역 네트워크 (CAN - Campus Area Network)
- 대도시 지역 네트워크 (MAN - Metropolitan Area Network)
- 광역 네트워크 (WAN - Wide Area Network)

WAN 연결 유형

- WAN 연결은 세 가지 범주로 나눌 수 있습니다:
    - 회선 교환 연결(Circuit Switched Connections)
    - 패킷 교환 연결(Packet Switched Connections)
    - 전용 임대 회선(Dedicated Leased Lines)

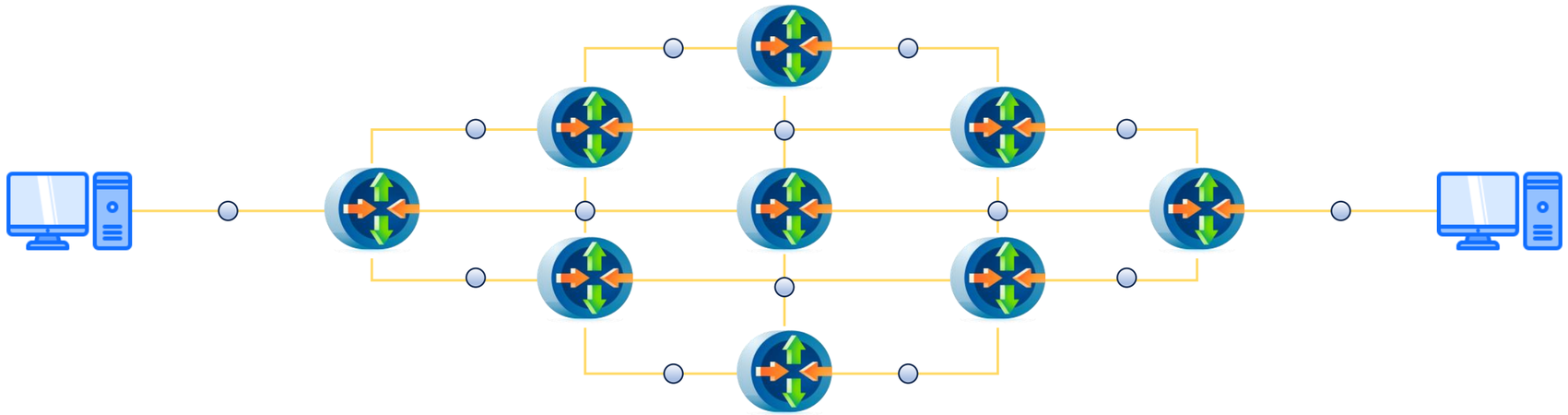
회선 교환 연결(Circuit Switched Connections)

- 1878년에 설계되었으며, 원래는 전화 통화를 위해 만들어졌습니다.
- 통신망을 이용하여 전용 점대점 연결(회선)을 사용합니다.
    - 통신하는 노드 간에 고정된 대역폭을 갖춘 전용 링크를 생성합니다.
    - 연결 중 다른 사용자는 회선을 이용할 수 없어 대역폭이 낭비될 수 있습니다.
    - 전송은 순서대로 송수신되며, 패킷 교환과 달리 전송 순서가 어긋나지 않습니다.
- 예시:
    - 전용 임대 회선 및 다이얼업



패킷 교환 연결(Packet Switched Connections)

- 데이터는 패킷으로 나누어지며, 각 패킷은 다른 링크를 통해 목적지로 전송됩니다.
- 데이터가 전송되는 시점에 가장 최적의 경로를 따라 전송 경로가 달라집니다.
    - 패킷이 순서 없이 도착할 수 있으며 올바른 순서로 재조립해야 합니다.
- 회선 교환과 달리, 패킷 교환은 대역폭과 연결을 다른 사용자와 공유합니다.
- 이 데이터 전송 방식은 인터넷과 대부분의 LAN에 사용되는 핵심 기술입니다.
- 패킷 교환 연결은 가상 회선을 생성할 수 있으며, 이에 대해서는 다음 슬라이드에서 다루겠습니다.

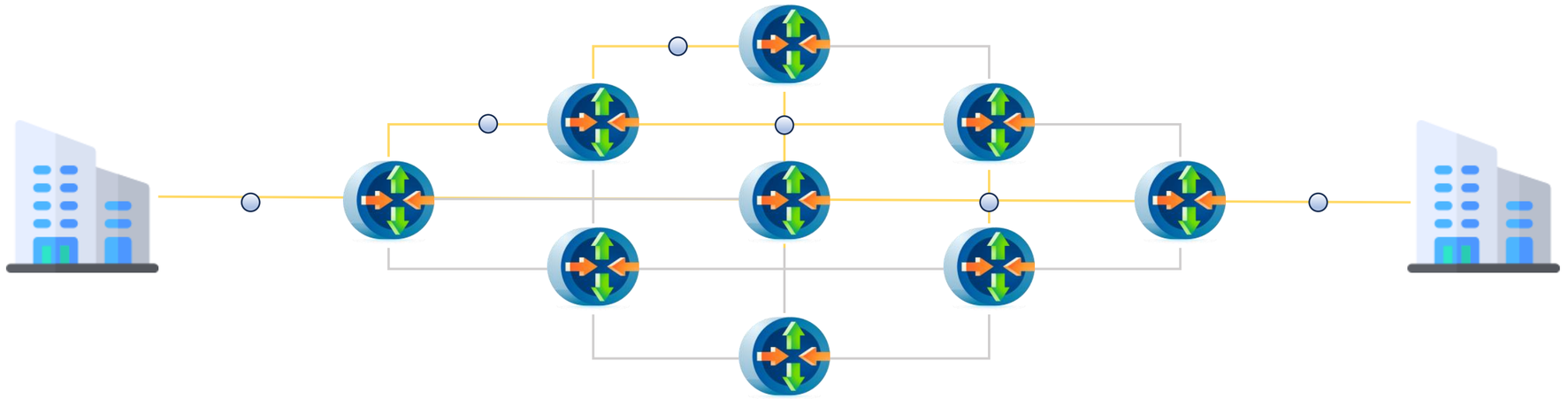


가상 회선(Virtual Circuit)

- 연결 지향 패킷 교환 연결은 가상 회선을 생성합니다.
    - 송신지와 수신지 간에 전용 물리적 연결(회선)이 있는 것처럼 데이터 패킷을 전달하는 방법입니다.

- 가상 회선은 서비스 제공자가 서비스 수준 협약(SLA)에 따라 더 나은 QoS(서비스 품질)을 제공할 수 있도록 합니다.

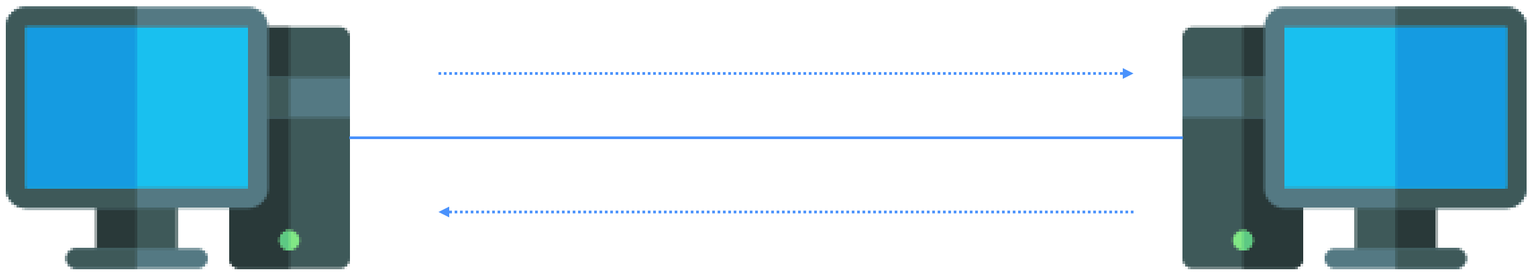
- 가상 회선의 종류는 두 가지입니다:
    - 상설 가상 회선(PVC): 항상 존재합니다.
    - 스위치드 가상 회선(SVC): 필요에 따라 생성됩니다.



전용 임대 회선(Dedicated Leased Line)

- 이름에서 알 수 있듯이, 이는 전용 임대 회선입니다.
- 일반적으로 점대점(Point-to-Point) 링크라고 불립니다.
- 두 사무실 간에 고정된 대역폭을 제공하는 전용 회선으로, 항상 활성 상태로 고정 대역폭을 보장하며 월 정액 요금으로 이용할 수 있습니다.
- 임대 회선은 전용 물리 회선이거나 상설 가상 회선(PVC)일 수 있습니다.

Half Duplex vs Full Duplex



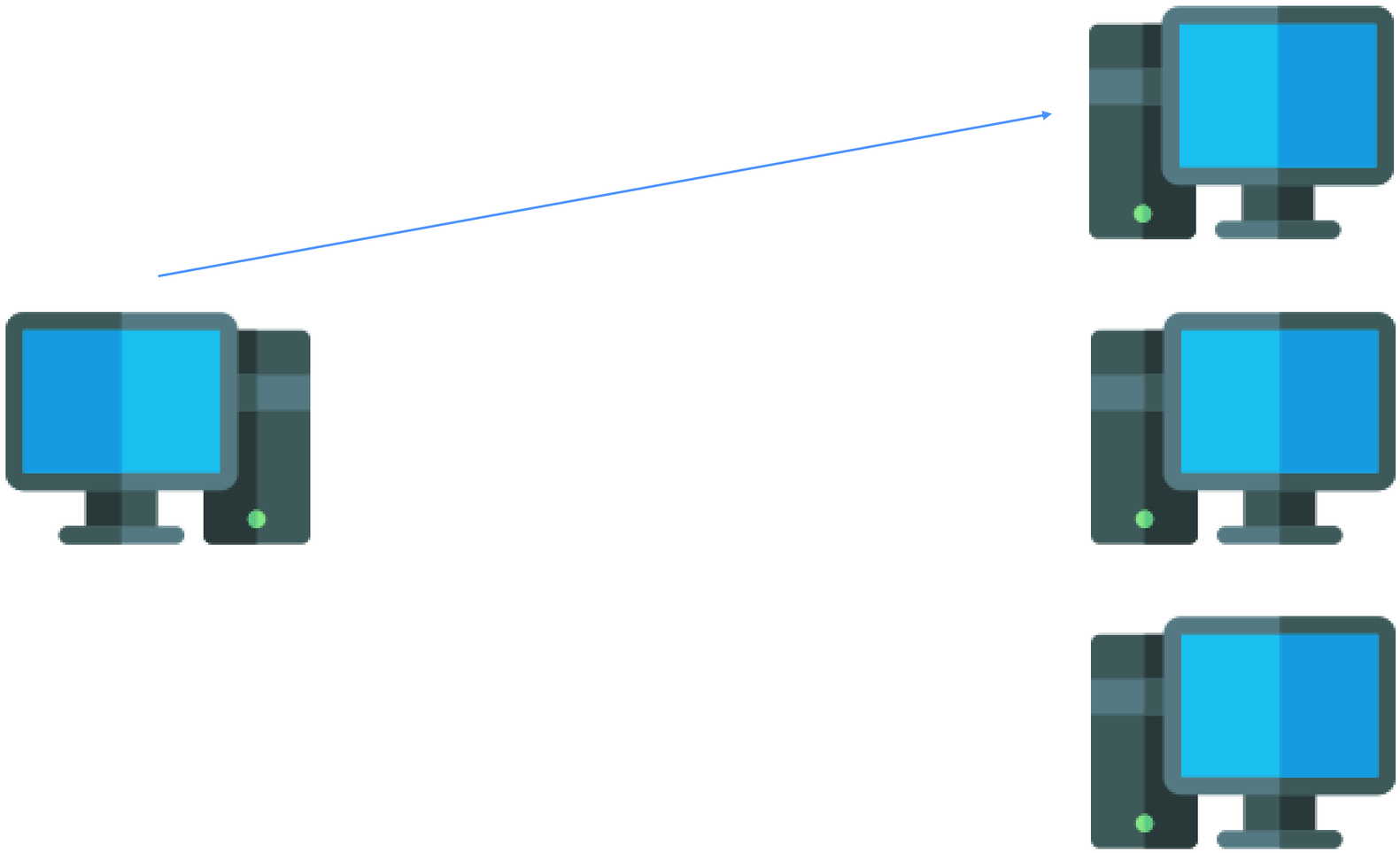
네트워크 통신은 반이중 모드 또는 전이중 모드로 이루어질 수 있습니다:

- 반이중 (Half Duplex): 데이터를 송신하고 수신할 수 있으나, 동시에 할 수는 없습니다.
- 전이중 (Full Duplex): 데이터를 송신하고 수신을 동시에 할 수 있습니다.

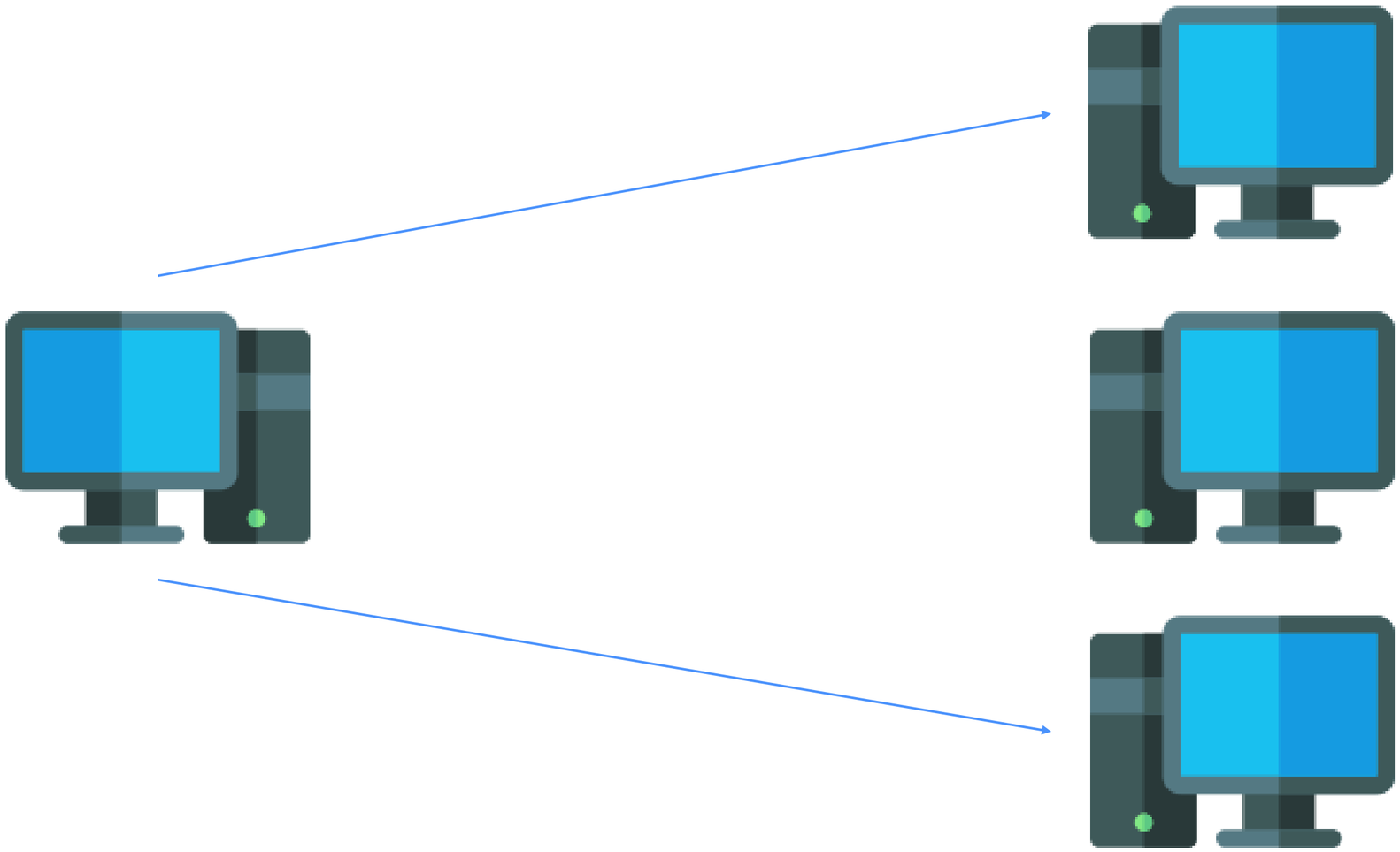
네트워크 전송 유형

- Unicast
- Multicast
- Broadcast

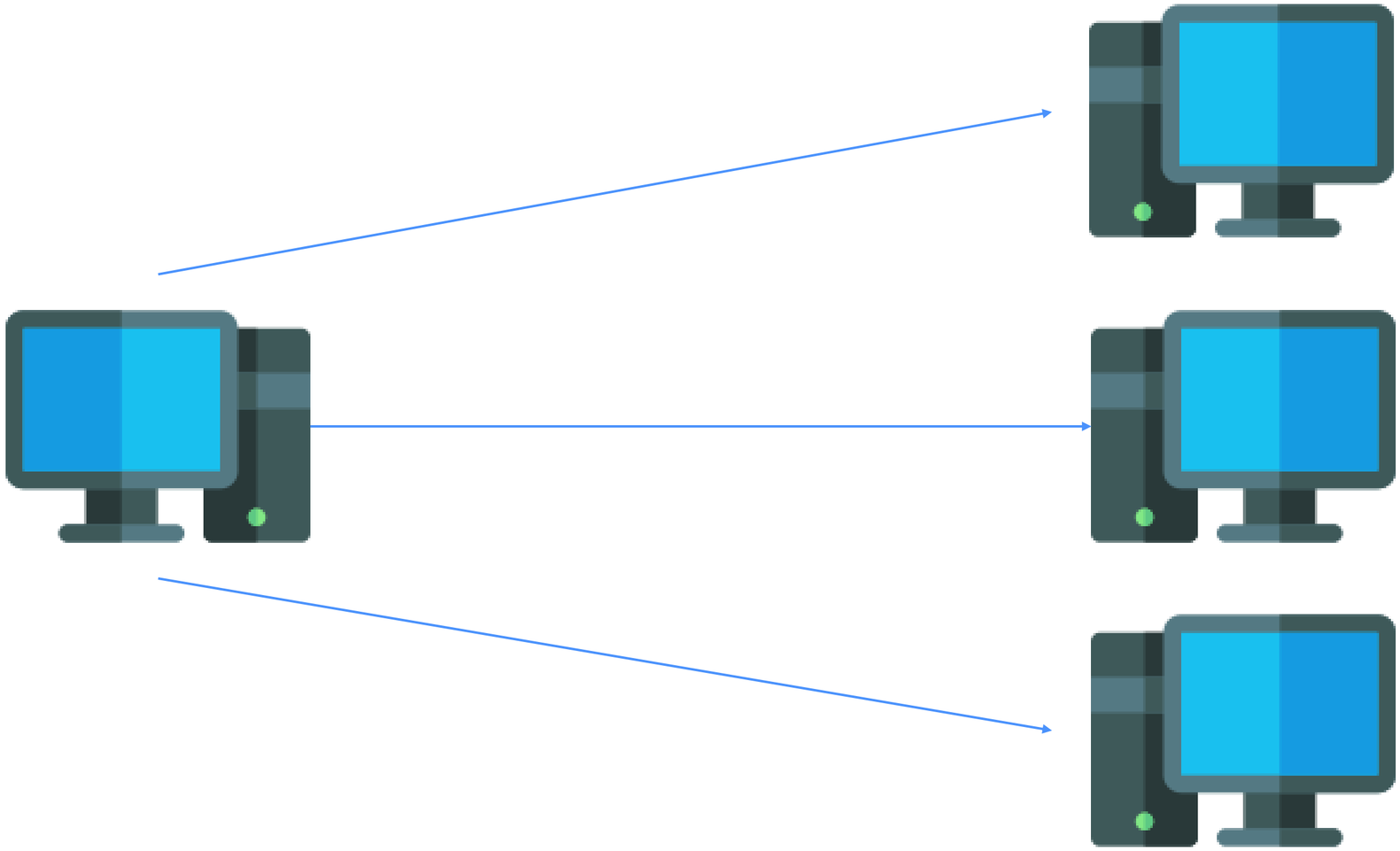
Unicast (One-to-One)



Multicast (One-to-Many)



Broadcast (One-to-All)



OSI 7계층 모델

OSI 7계층 모델

- ISO(국제표준화기구)가 네트워크 프로토콜이 통신하는 구조를
  7개의 계층으로 분리하여
  각 계층간 상호 작동하는 방식을 정한 모델

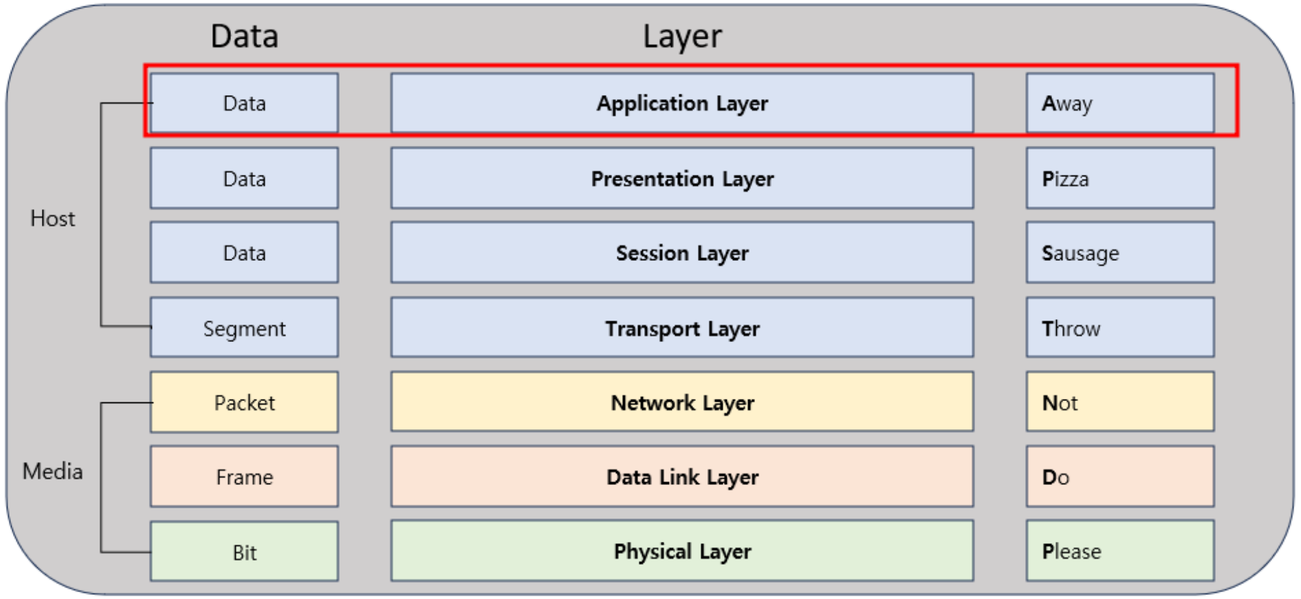
- 통신이 일어나는 과정을 7단계로 크게 구분하여
  한 눈에 들어올 수 있도록 정의

L7 - Application 계층

- 사용자에게 다양한 Network 서비스 제공
  (email - SMTP, FTP, 가상터미널...)
- 사용자 인증

Layer 7 - Application Layer

- 사용자가 컴퓨터와 상호작용하는 계층입니다.
- 응용 프로그램과 최종 사용자 프로토콜 사이의 인터페이스 역할을 합니다.
- 네트워크와 통신하기 위한 인터페이스를 제공합니다(예: Outlook, Chrome 등).
- 응용 프로그램은 응용 계층에 직접 존재하지 않으며, 대신 응용 계층 프로토콜과 인터페이스합니다.
- 예시 응용 계층 프로토콜:
    - 이메일: IMAP4, POP3, SMTP
    - 웹 브라우저: HTTP, HTTPS
    - 원격 접속: SSH, Telnet

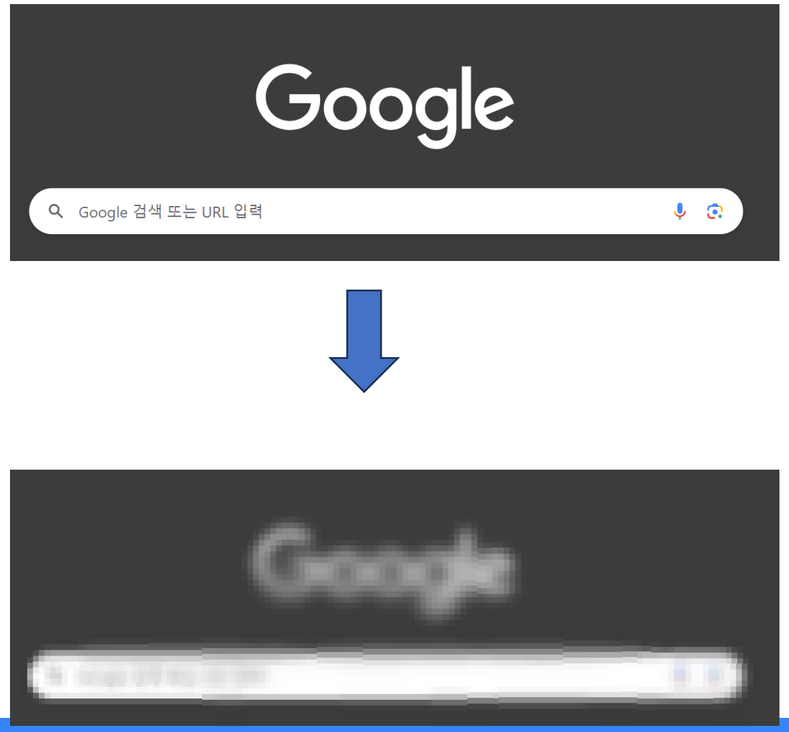


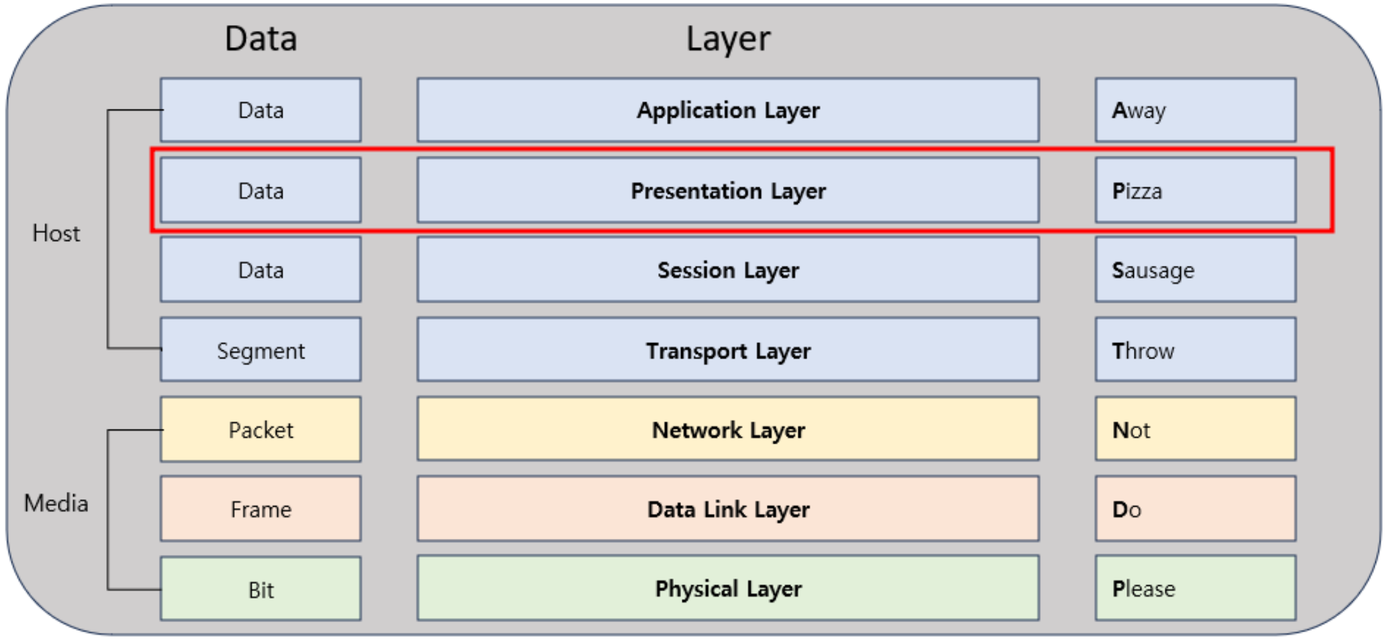
L6 - Presentation 계층

- App, Layer에 대한 Data 전송, Syntax 협의
- Data Format 결정, 구성
- Code 변환
- 구축변환
- 압축
- 암호화

Layer 6 - Presentation Layer

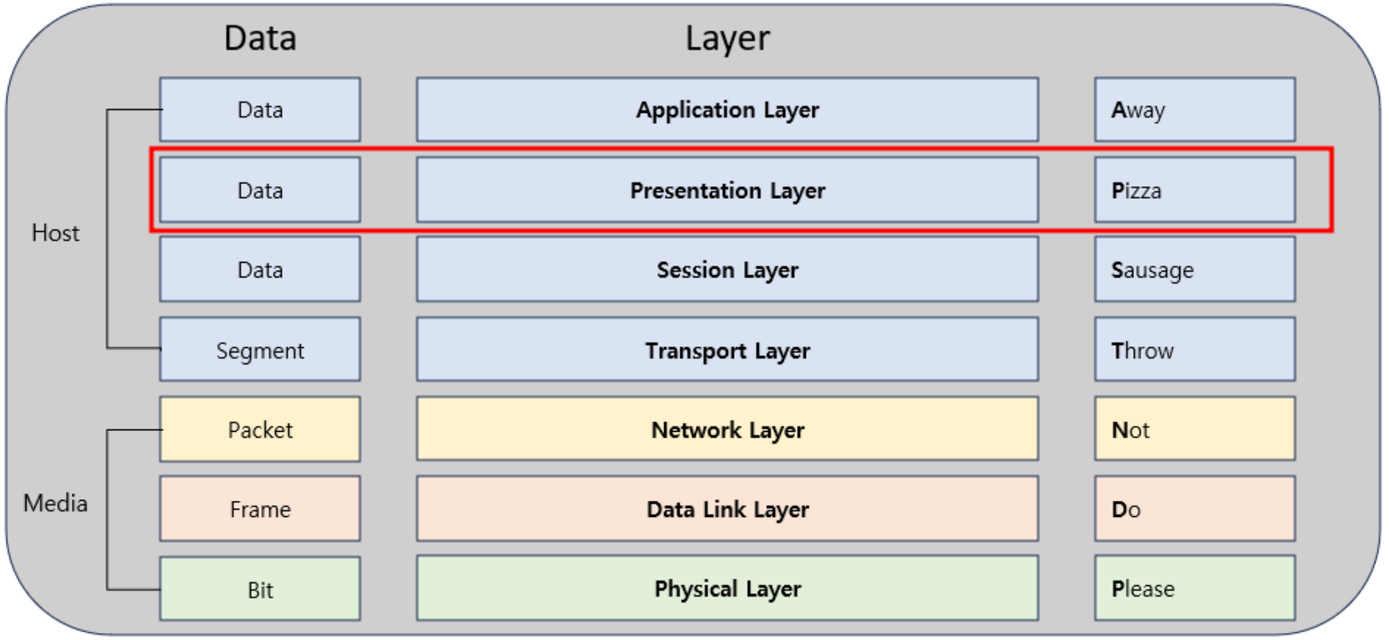
- 한 시스템의 응용 계층에서 전송된 데이터를 다른 시스템의 응용 계층에서 읽을 수 있도록 보장합니다.
- 문자 코드 변환, 데이터 압축, 데이터 암호화/복호화를 제공합니다.
- 예시: Google Chrome의 HTML이 ASCII 형식으로 변환되는 과정.

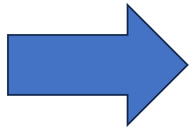




Layer 6 - Presentation Layer

- 6계층 파일 형식의 예:
  - 웹 브라우저: HTML, XML, JavaScript
  - 그래픽 파일: JPEG, GIF, PNG
  - 오디오/비디오: MPEG, MP3
  - 암호화: TLS, SSL
  - 텍스트/데이터: ASCII, EBCDIC



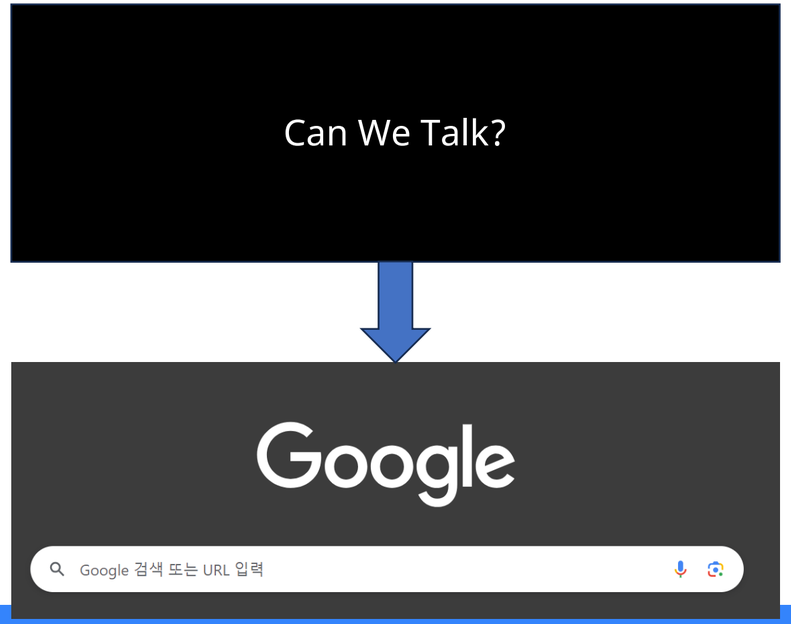


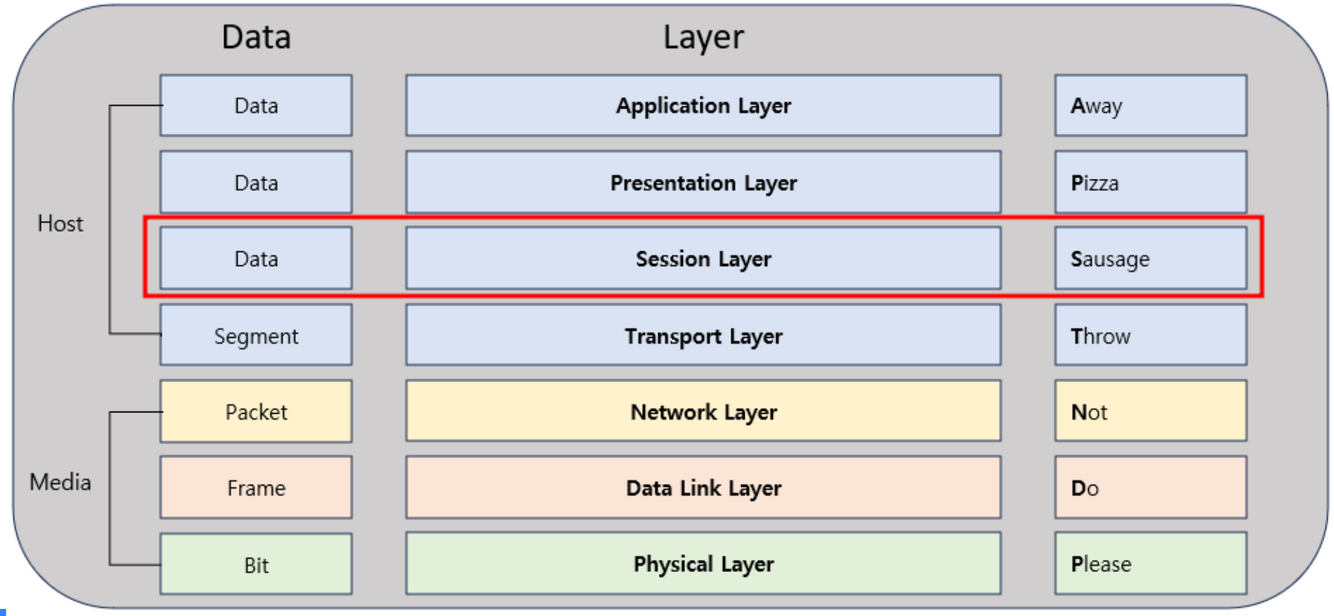
L5 - Session 계층

- Interhost Communication
- Application 사이의 대화 Start, Maintain, Stop

Layer 5 - Session Layer

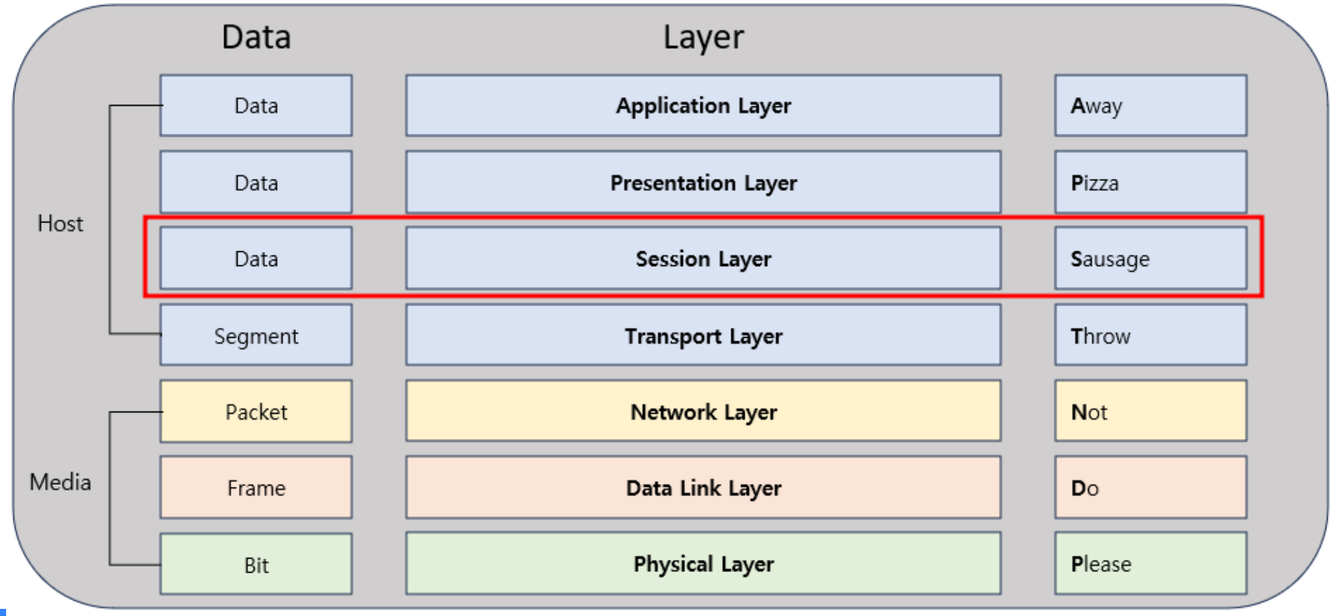
- 네트워크 장치 간 세션을 설정하고 관리하며, 세션을 종료하는 역할을 담당합니다.
- 다른 애플리케이션 세션의 데이터가 분리되도록 보장합니다.
- TCP/IP 프로토콜과 통신하기 위해 API(애플리케이션 프로그래밍 인터페이스)를 활용합니다.
- 시스템 간 통신을 조정합니다.
    - 시작, 정지, 재시작





Layer 5 - Session Layer

- 장치 간 통신을 위한 세 가지 방법을 제공합니다:
    - 단방향(Simplex): 두 장치 간의 일방향 통신으로, 라디오 방송을 듣는 것과 같습니다.
    - 반이중(Half Duplex): 두 장치 간의 양방향 통신이 가능하지만, 한 번에 한 장치만 통신할 수 있습니다.
    - 전이중(Full Duplex): 두 장치 간의 양방향 통신이 가능하며, 두 장치가 동시에 통신할 수 있습니다.

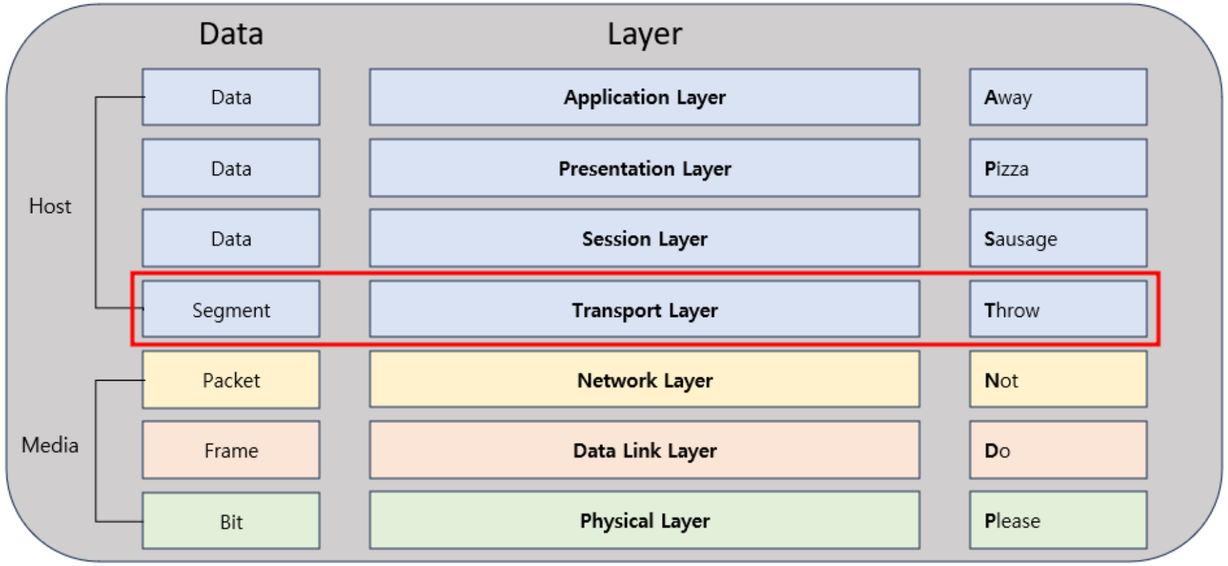


L4 - Transport 계층

- End to End Connection
- Application 사이의 논리적인 통로 제공
- 전송 문제 관리
- 신뢰성 있는 전송 보장

Layer 4 - Transport Layer

- 데이터를 오류 없이 순서대로 전달되도록 보장합니다.
- 데이터를 세그먼트로 나누고 올바르게 재조립합니다.
- 연결 지향적일 수도 있고, 비연결 지향적일 수도 있습니다.
- "우체국" 계층으로 간주됩니다.
    - TCP(전송 제어 프로토콜)
    - UDP(사용자 데이터그램 프로토콜)

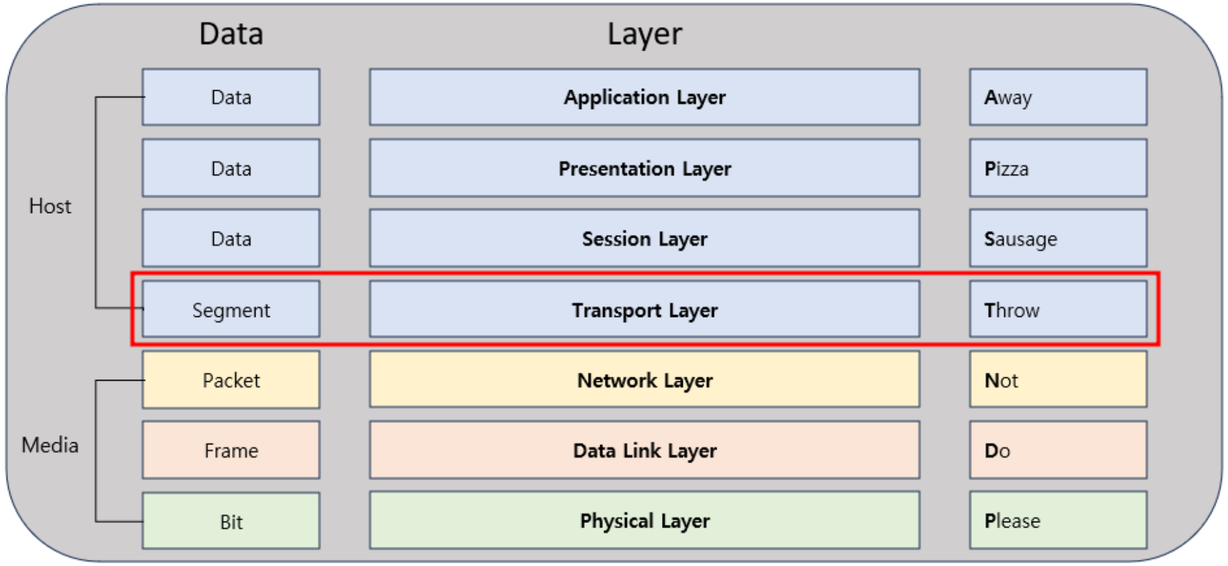


Layer 4 - Transport Layer

- 두 가지 데이터 흐름 제어 방법을 담당합니다:

- 버퍼링
    - 목적지 장치가 준비될 때까지 데이터를 메모리 버퍼에 저장합니다.

- 윈도잉
    - 세션 중인 장치들이 전송할 데이터 세그먼트의 "윈도우" 크기를 결정할 수 있게 합니다.

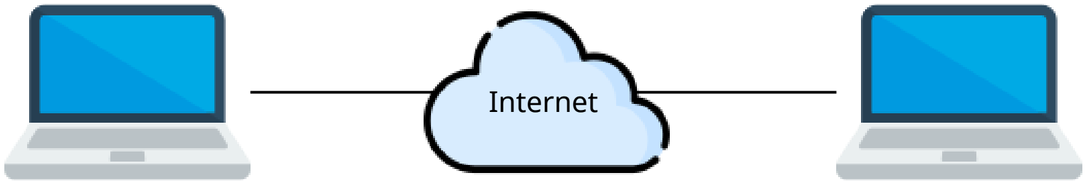


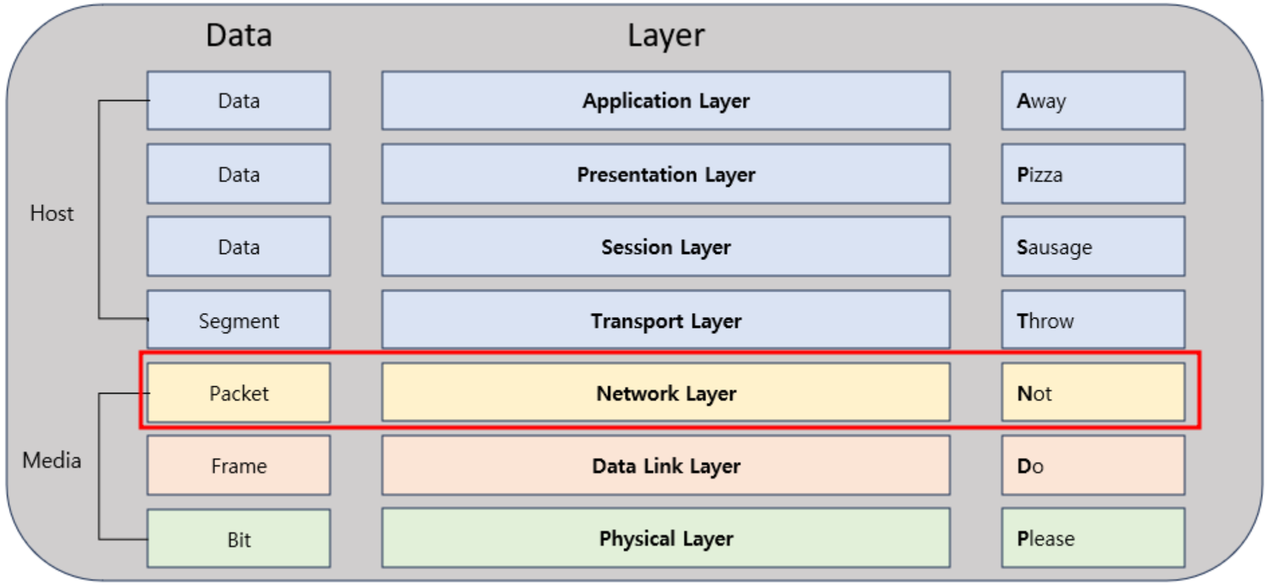
L3 - Network 계층

- 논리적인 주소를 사용
- 경로 관리, 최적 경로 선정
- 사용자 Data (Packet) 전송

Layer 3 - Network Layer

- "라우팅" 계층이라고도 불립니다.
- 논리적 주소(IP 주소) 및 라우팅 서비스를 제공합니다.
- 두 개의 IP 주소를 패킷에 넣습니다:
    - 출발지 주소와 목적지 IP 주소
- 인터넷 프로토콜(IP)
    - 인터넷에서 사용되는 기본 네트워크 프로토콜로, IPv4, IPv6 논리적 주소를 사용합니다.





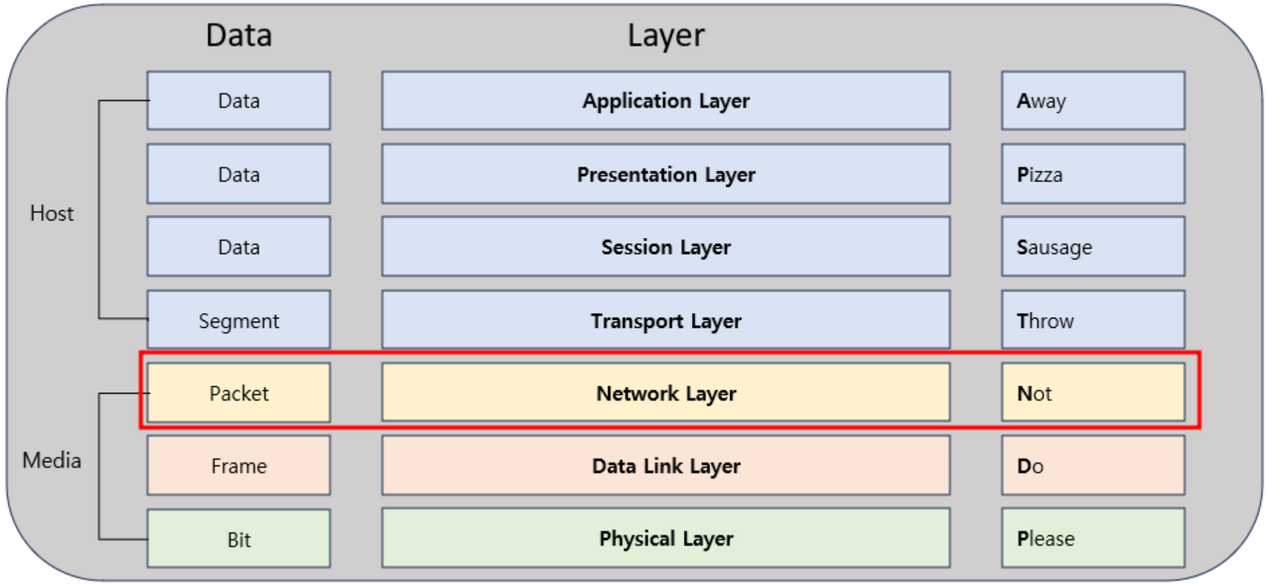
Layer 3 - Network Layer

- 네트워크 계층에서의 패킷 종류:

- 데이터 패킷
  - 라우팅된 인터넷 프로토콜(IP) 데이터 패킷.
  - IPv4 & IPv6

- 라우트-업데이트 패킷
  - 경로 결정 정보를 제공하기 위해 이웃 라우터에 업데이트를 전송하는 라우팅 프로토콜.
  - RIP, OSPF, EIGRP 등.

- 3계층 장비 및 프로토콜:
  - 라우터 & 다계층 스위치
  - IPv4 & IPv6
  - 인터넷 제어 메시지 프로토콜(ICMP), 예: Ping

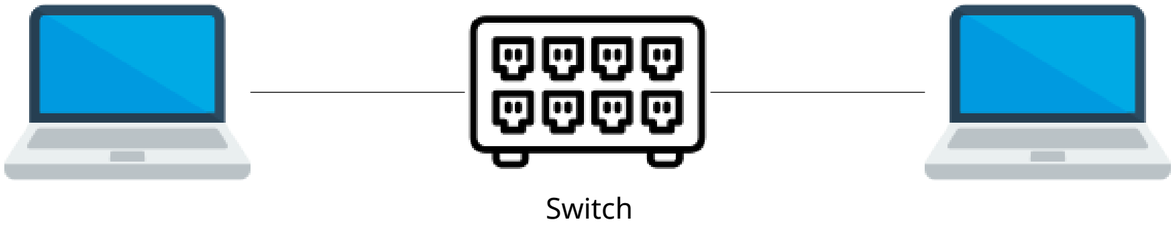


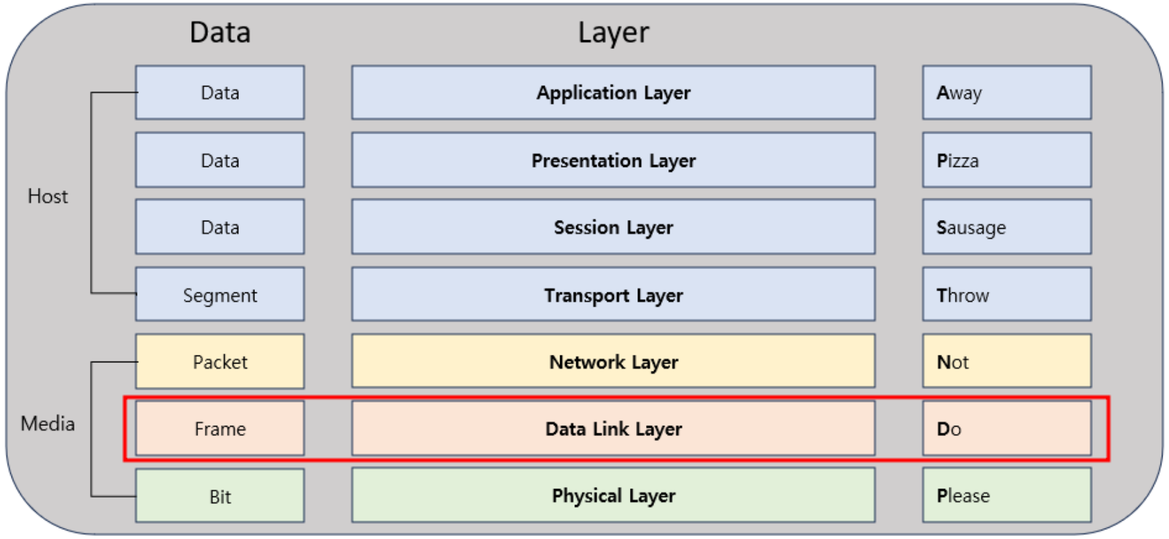
L2 - Data Link 계층

- Data 전송을 위한 Format 결정
- Data 전송을 위하여 Media 에 접근하는 방법 제공
- 물리적인 주소(MAC) 사용
- Error Detection 기능 제공

Layer 2 – Data Link Layer

- "스위칭" 계층
- LAN에서 하드웨어 주소를 사용하여 올바른 장치에 메시지를 전달하는 것을 보장합니다.
  - MAC(매체 접근 제어) 주소
  - 같은 네트워크 내에서 프레임을 로컬로 전달하는 데만 관여합니다.
- 물리 계층을 위한 프레임으로 데이터를 패키징하는 역할을 합니다.
- 네트워크 계층에서 오는 메시지를 물리 계층을 위한 비트로 변환합니다.



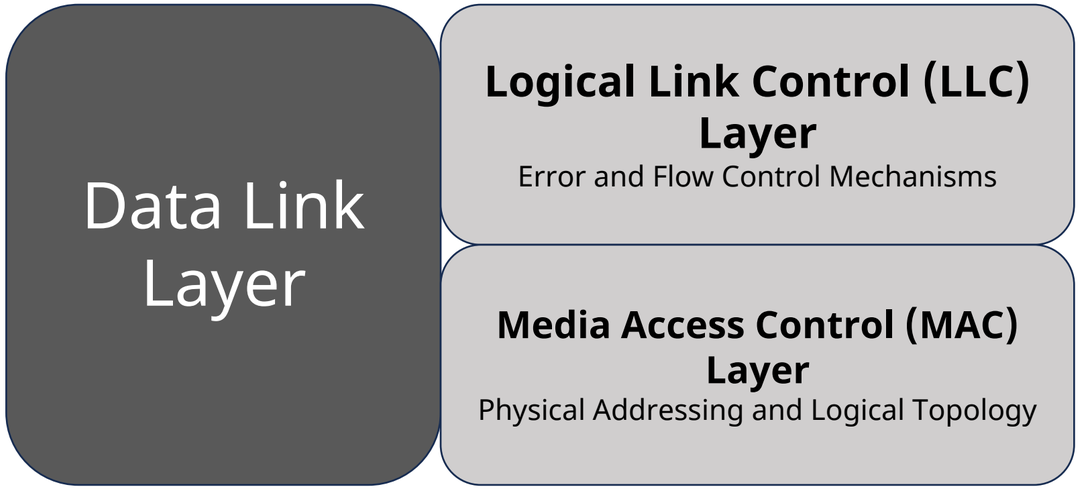


Layer 2 – Data Link Layer

- 두 개의 하위 계층을 가집니다.

- 논리 링크 제어(LLC) 계층
    - 오류 제어 및 흐름 제어
        - 손상된 데이터 프레임을 감지하고 수정합니다.
        - 장치가 과부하되지 않도록 전송되는 데이터 양을 제한합니다.

- 매체 접근 제어(MAC) 계층
    - 물리적 주소 지정(MAC 주소)
        - NIC에 기록된 48비트 MAC 주소
    - 논리적 토폴로지 및 매체 접근
        - 이더넷, 토큰 링 등
        - CSMA/CD & CSMA/CA

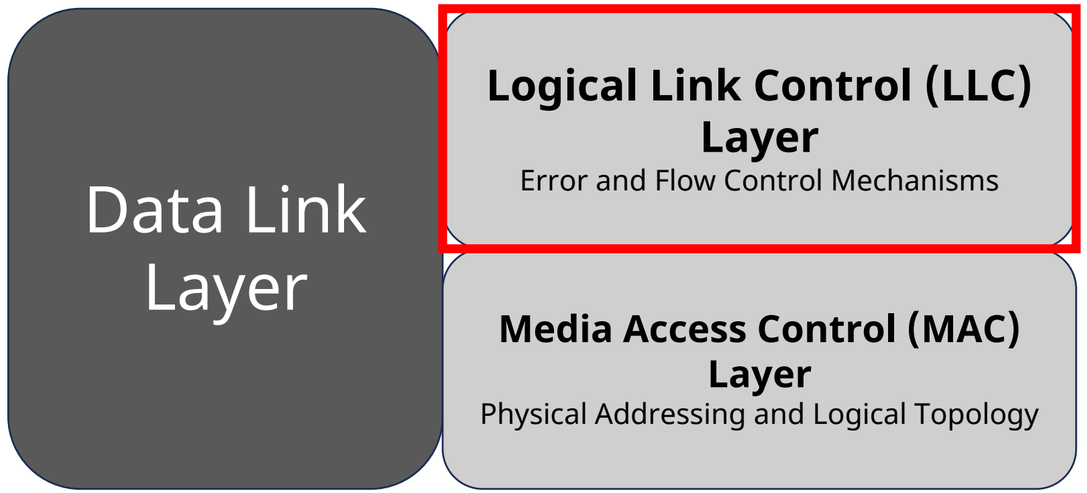


Layer 2 – Data Link Layer

- 두 개의 하위 계층을 가집니다.

- 논리 링크 제어(LLC) 계층
  - 오류 제어 및 흐름 제어
    - 손상된 데이터 프레임을 감지하고 수정합니다.
    - 장치가 과부하되지 않도록 전송되는 데이터 양을 제한합니다.

- 매체 접근 제어(MAC) 계층
  - 물리적 주소 지정(MAC 주소)
    - NIC에 기록된 48비트 MAC 주소
  - 논리적 토폴로지 및 매체 접근
    - 이더넷, 토큰 링 등
    - CSMA/CD & CSMA/CA

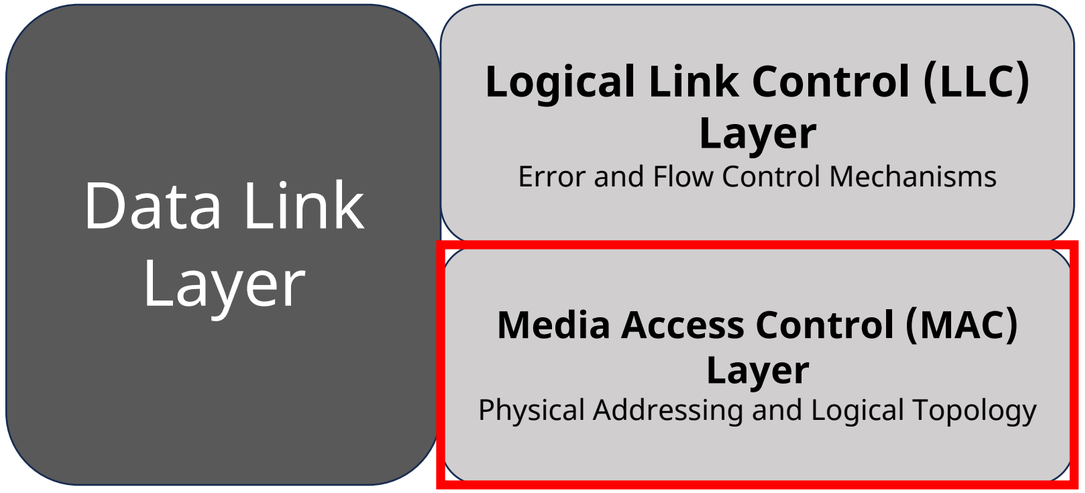


Layer 2 – Data Link Layer

- 두 개의 하위 계층을 가집니다.

- 논리 링크 제어(LLC) 계층
    - 오류 제어 및 흐름 제어
        - 손상된 데이터 프레임을 감지하고 수정합니다.
        - 장치가 과부하되지 않도록 전송되는 데이터 양을 제한합니다.

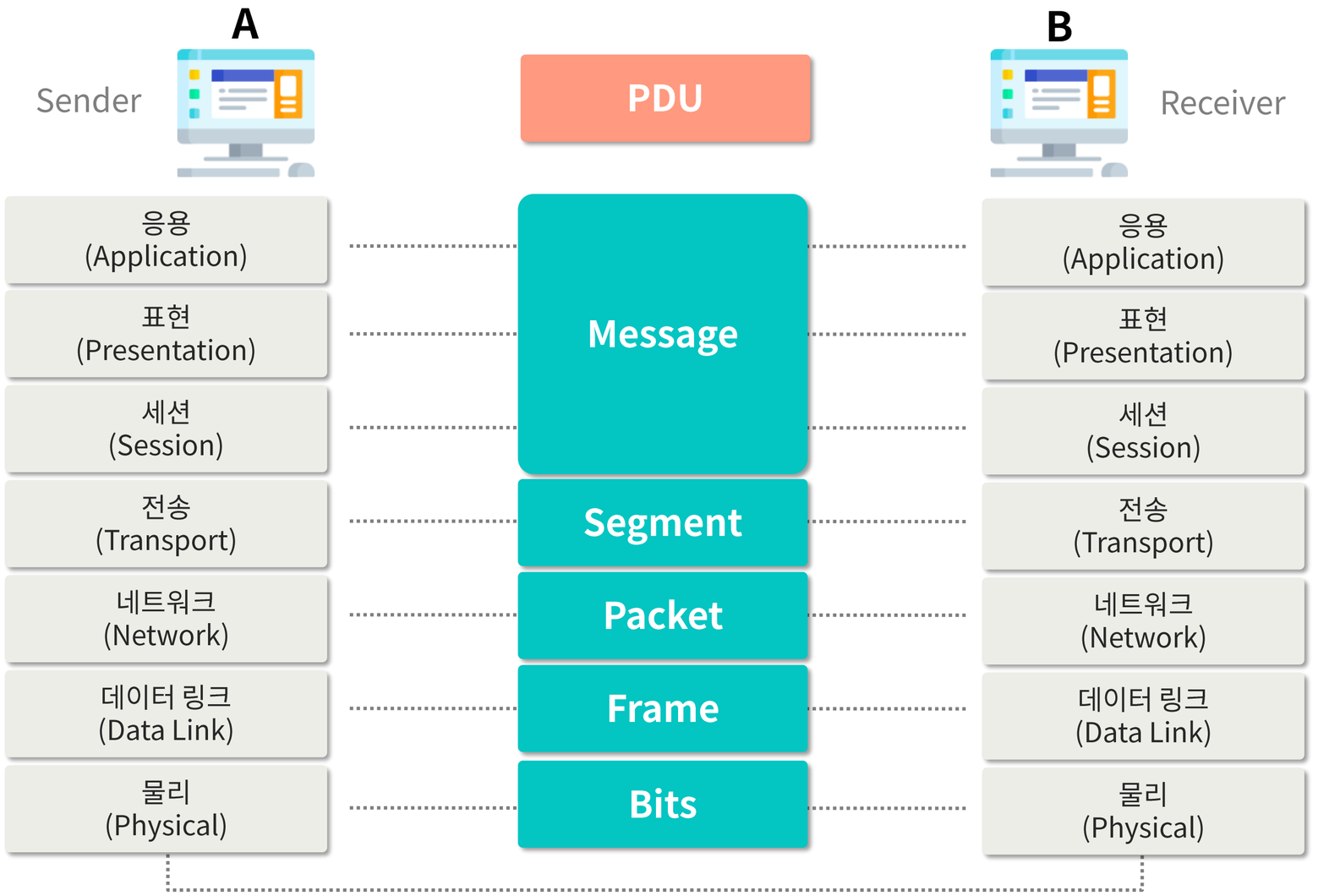
- 매체 접근 제어(MAC) 계층
    - 물리적 주소 지정(MAC 주소)
        - NIC에 기록된 48비트 MAC 주소
    - 논리적 토폴로지 및 매체 접근
        - 이더넷, 토큰 링 등
        - CSMA/CD & CSMA/CA



L1 - Physical 계층

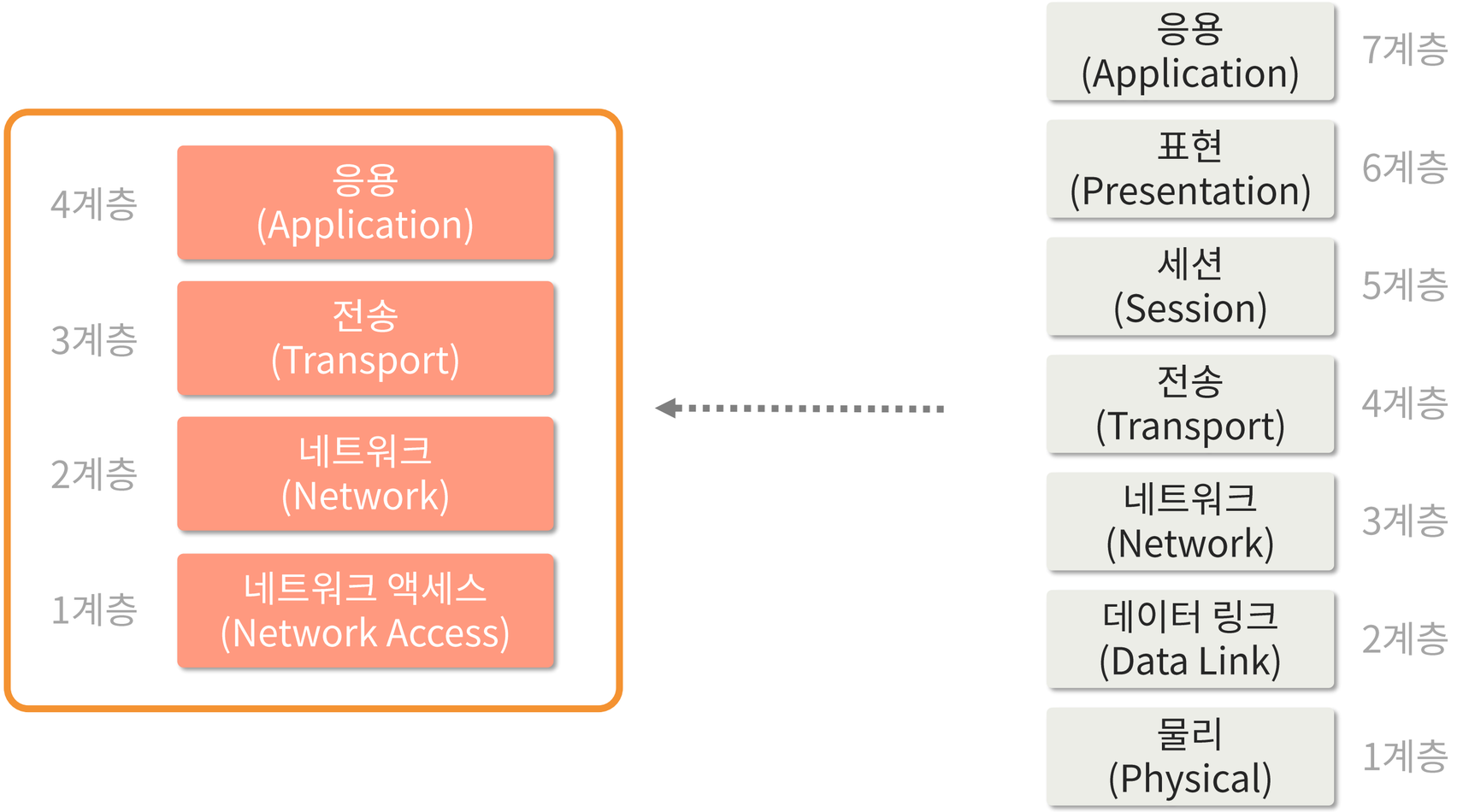
- 물리적인 연결
- 전기적, 기계적, 기능적 절차적인 수단 제공

계층별 데이터 형태

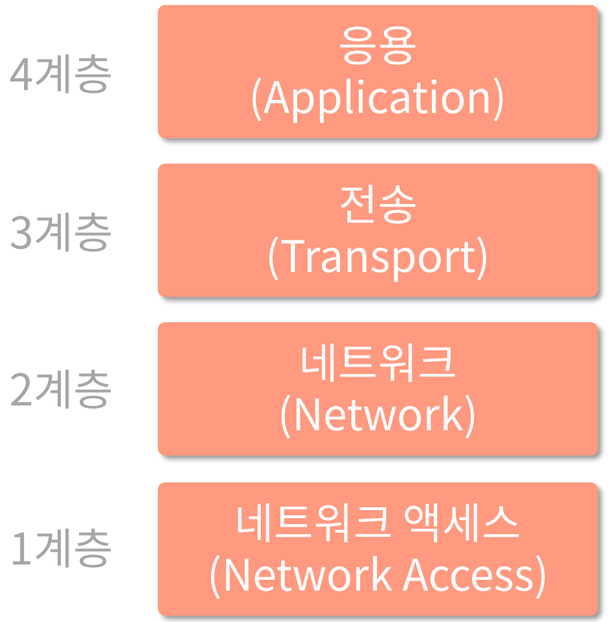

A
Sender
PDU
B
Receiver
응용 (Application)
표현 (Presentation)
세션 (Session)
전송 (Transport)
네트워크 (Network)
데이터 링크 (Data Link)
물리 (Physical)
Message
Segment
Packet
Frame
Bits
응용 (Application)
표현 (Presentation)
세션 (Session)
전송 (Transport)
네트워크 (Network)
데이터 링크 (Data Link)
물리 (Physical)

TCP/IP 4계층 모델

- OSI 7계층 모델을 기반으로 실제 업무에서 이용될 수 있도록 단순화 된 모형



Network Access 계층

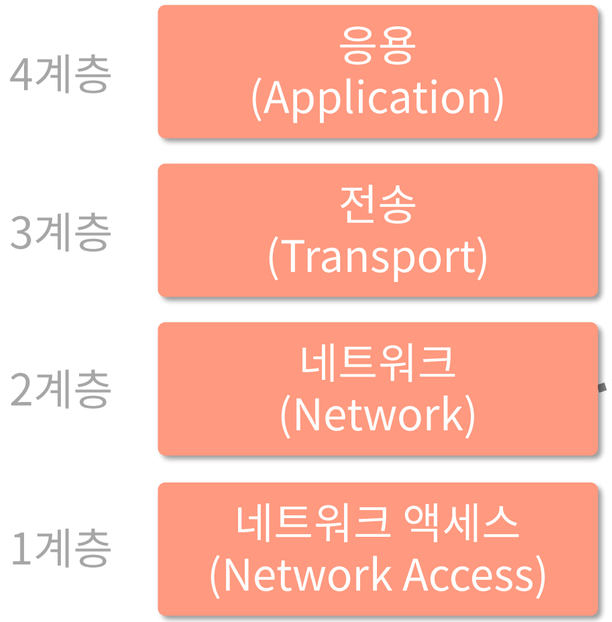


- OSI 7계층의 데이터링크, 물리 계층
- MAC 주소를 통해 장비간 데이터 전송
- 프레임(Frame) 단위의 데이터 구성

- 데이터 단위 :
  Frame

- 프로토콜 :
  Ethernet, Token Ring 등

Network 계층

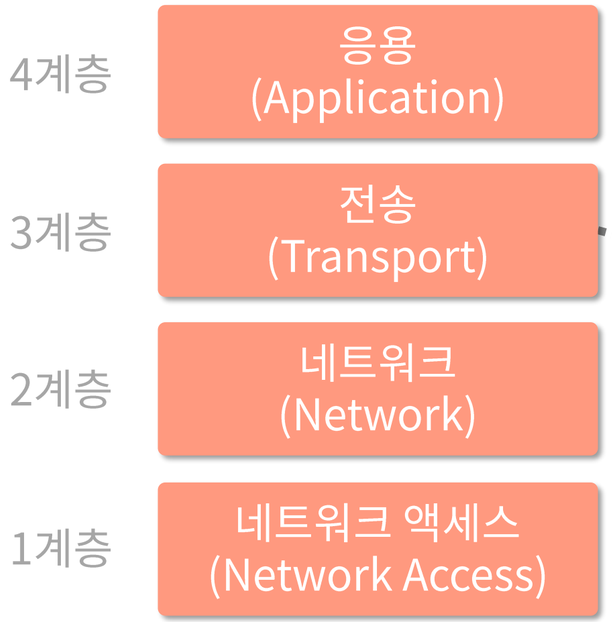


- OSI 7계층의 네트워크 계층
- 네트워크상 목적지까지 연결
- IP 할당, 경로(Route) 설정
- 패킷(Packet) 단위의 데이터 구성

- 데이터 단위 :
  Packet

- 프로토콜 :
  IP, ARP, ICMP, RARP, OSPF 등

Transport 계층

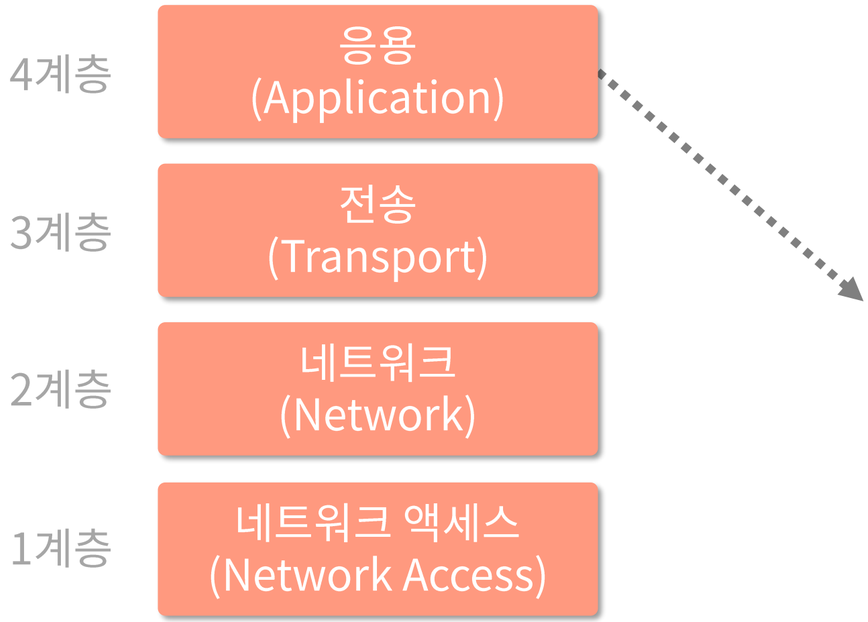


- OSI 7계층의 전송 계층
- 통신 노드 간 연결
- Port 기반 데이터 전송
- 세그먼트(Segment)단위의 데이터 구성

- 데이터 단위 :
  Segment

- 프로토콜 :
  TCP, UDP 등

Application 계층



- OSI 7계층의 세션, 표현, 응용 계층
- 사용자와 가장 가까운 계층으로
  사용자가 Application 과 소통할 수 있게 지원

- 데이터 단위 :
  Message

- 프로토콜 :
  FTP, HTTP, SSH, Telnet, DNS, SMTP 등

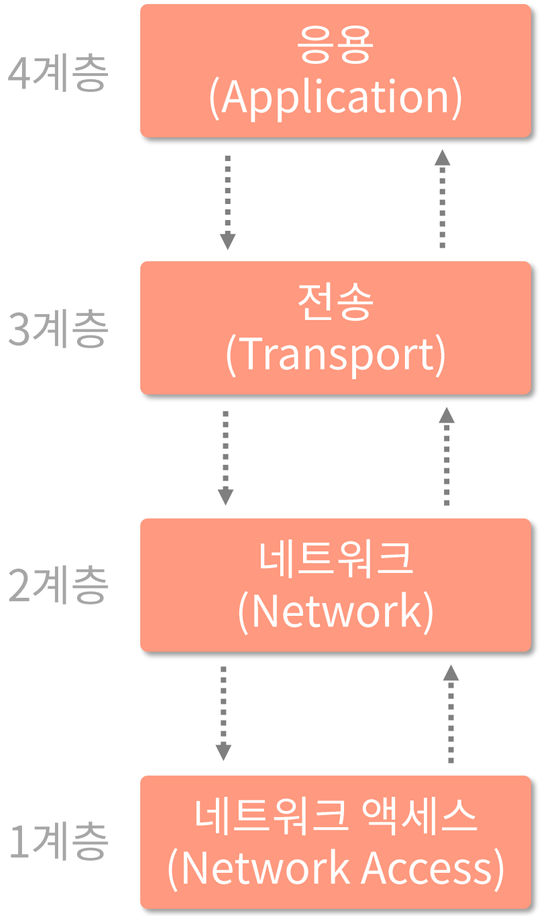
헤더란

- 데이터 전송이 이루어질 때, 계층 이동별로 필요한 정보
- 목적지 정보, 출발지 정보, 에러 체크 등

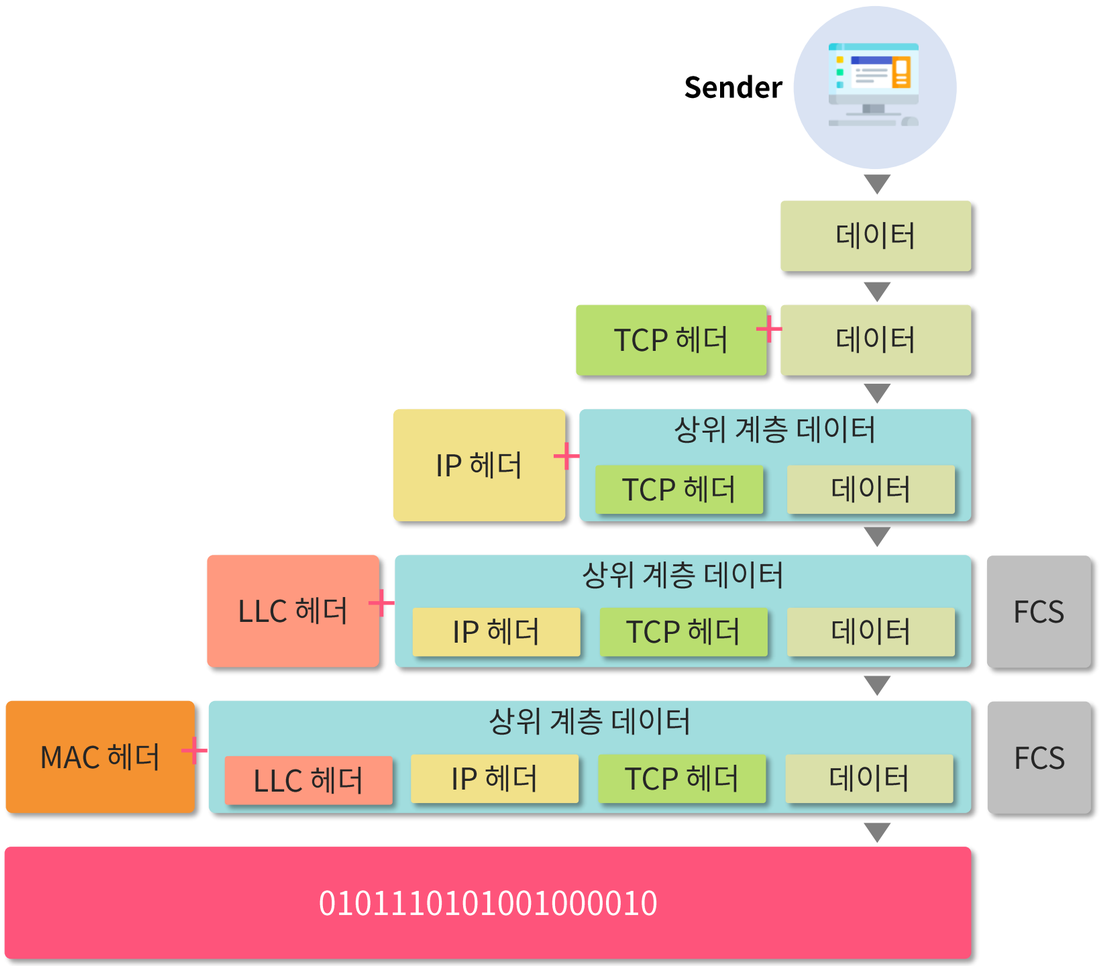
- 예시
  - HTTP 헤더, TCP 헤더, IP 헤더, 이더넷 헤더

- 헤더 하나하나 붙이는 것 : 캡슐화

- 헤더 하나하나 제거하는 것 : 역캡슐화



헤더 - Sender (Encapsulation)



응용
(Application)

표현
(Presentation)

세션
(Session)

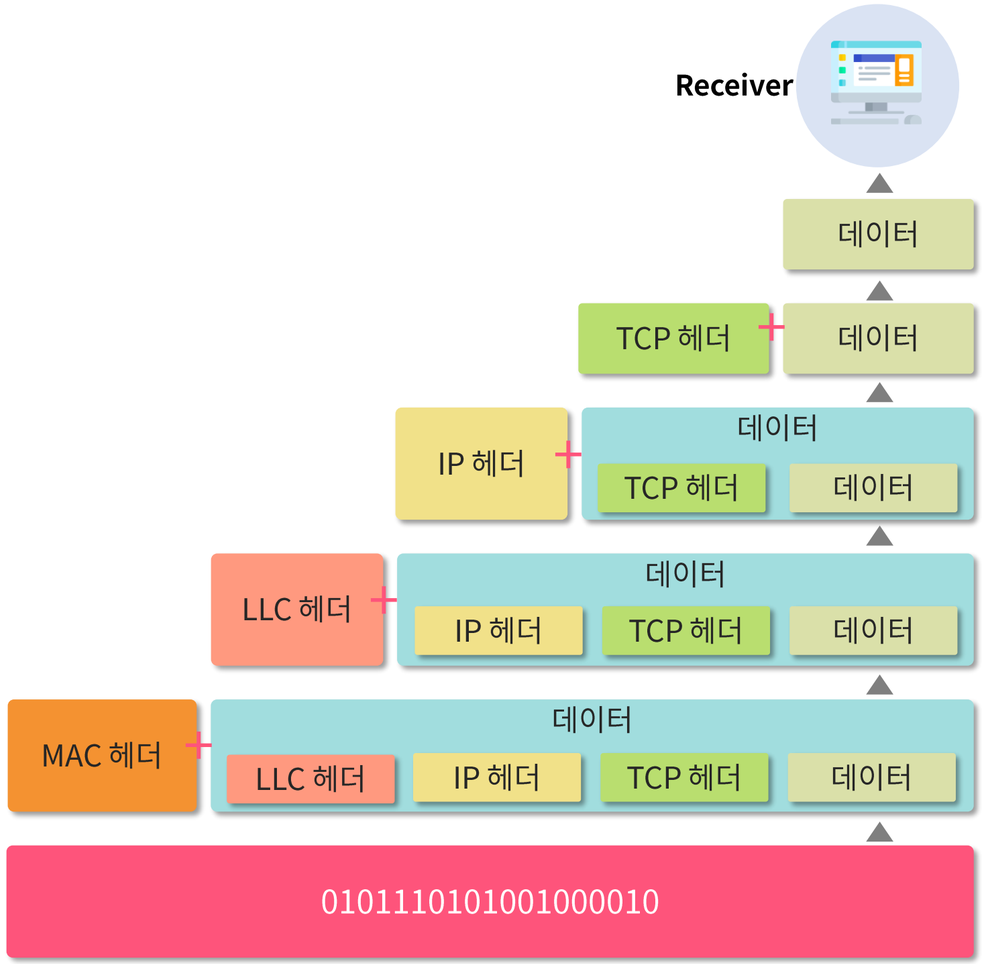
전송
(Transport)

네트워크
(Network)

데이터 링크
(Data Link)

물리
(Physical)

헤더 - Receiver (Decapsulation)



응용
(Application)

표현
(Presentation)

세션
(Session)

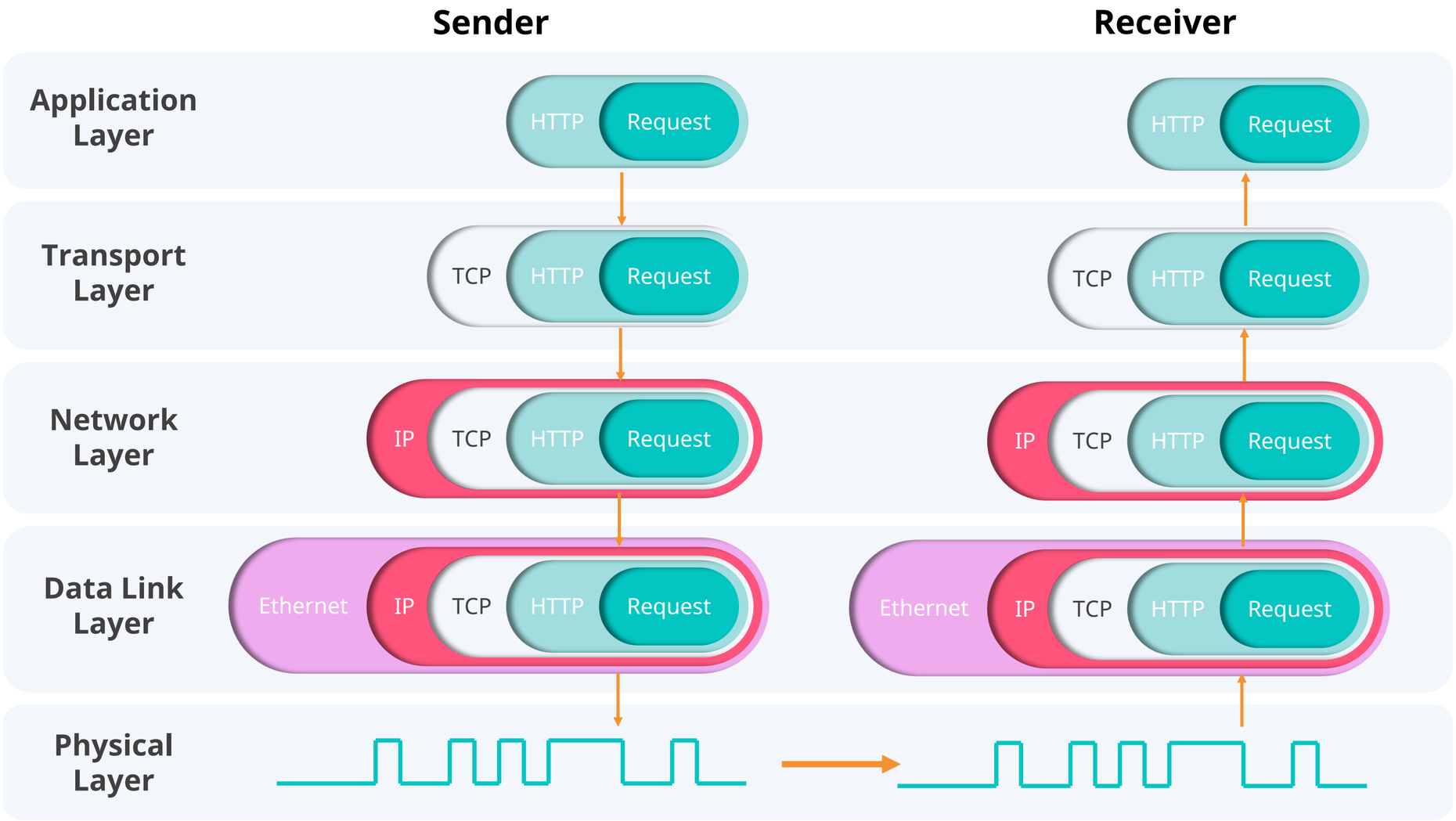
전송
(Transport)

네트워크
(Network)

데이터 링크
(Data Link)

물리
(Physical)

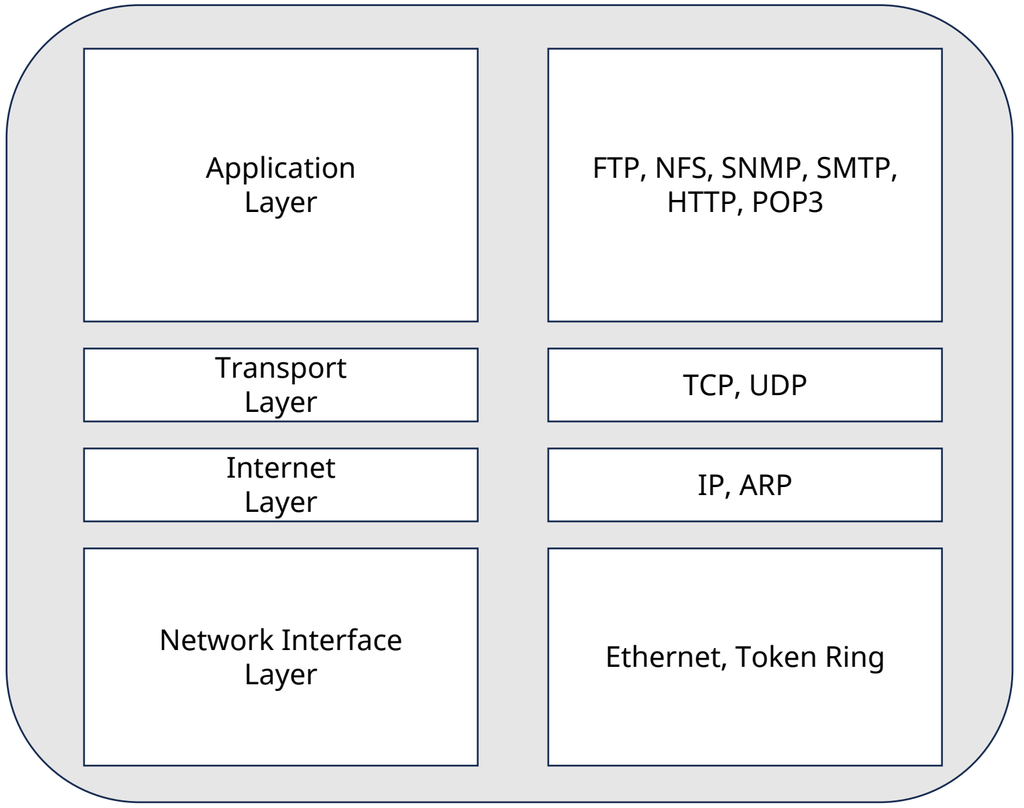
Data Encapsulation 및 Decapsulation



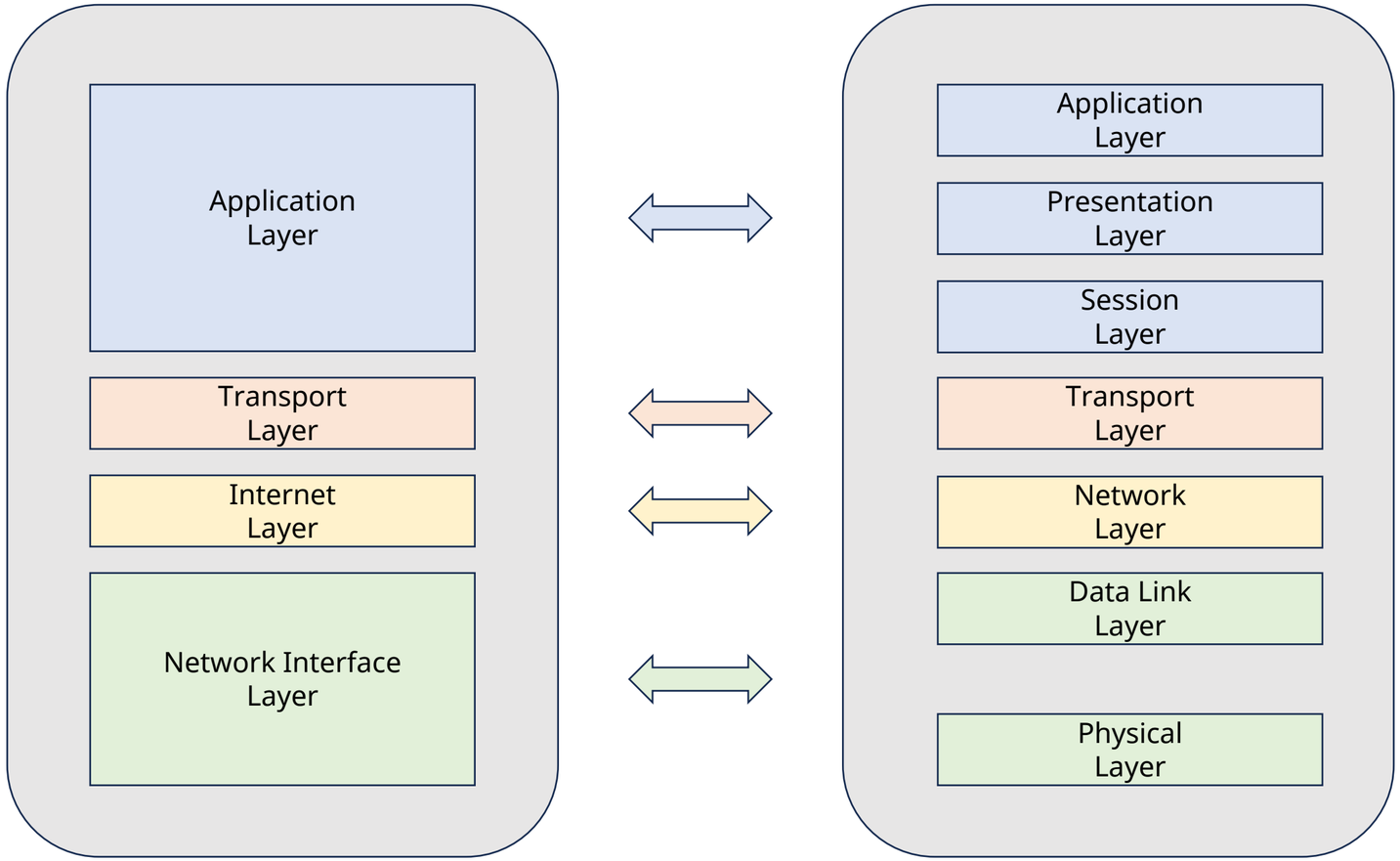
네트워크 주요 용어

TCP/IP 모델

- TCP/IP 스위트는 네트워킹 분야에서 가장 널리 사용되는 프로토콜 스위트입니다.
- 이는 인터넷을 구축하는 데 사용된 프로토콜 스위트이기도 합니다.
- 컴퓨터 네트워킹의 표준으로 자리잡고 있습니다.OSI 모델과 유사한 4계층 모델을 기반으로 합니다.
- TCP/IP의 역사:
    - 1970년대 초 미국 국방부(DoD)에 의해 개발되었습니다.
    - 1982년, 국방부는 모든 군사 컴퓨터 네트워킹의 표준으로 TCP/IP를 선언했습니다.
    - 1984년에 IBM, AT&T 등에서 TCP/IP의 광범위한 채택이 시작되었습니다.



TCP/IP 모델과 OSI 모델



MAC 주소

- Media Access Control (MAC)
  - 네트워크 어댑터 카드의 물리적 주소
  - OSI 2계층 (데이터 링크) 계층 주소
  - TCP/IP 1계층 (네트워크 인터페이스) 계층 주소

- 6바이트 (48비트), 일반적으로 16진수로 표현
  - 처음 3바이트 (24비트)는 제조사에 대해 IEEE가 할당함조직
  - 고유 식별자 (OUI) - 예: Dell 또는 HP

  - 마지막 3바이트 (24비트)는 일반적으로 순차적으로 할당됨고유 번호

00:21:70:6f:06:f2 00-21-70-6F-06-F2

2^{24} = 약 1,670만 개의 고유 주소

IP 주소

- IP 주소는 IP 네트워크에서 장치를 고유하게 식별하기 위해 사용되는 논리적 주소입니다.

- 이는 라우팅과 관련된 네트워크 계층 주소입니다.
    - OSI 3계층: 네트워크 계층
    - TCP/IP 2계층: 인터넷 계층

- 두 가지 버전이 있습니다:
    - IP 버전 4 (IPv4)
        - 예: 192.168.0.1
    - IP 버전 6 (IPv6)
        - 예: 2001:DB8:85A3:0:0:8A2E:370:7334

IP vs MAC

IP 주소

- 네트워크 (OSI 3계층) 주소
- 논리적 주소
- 운영 체제에서 할당
- 라우터를 통한 네트워크 간 통신 가능
- WAN 통신

MAC 주소

- 데이터 링크 (OSI 2계층) 주소
- 물리적 주소
- NIC에 물리적으로 저장됨
- 허브, 스위치, 라우터를 통한 네트워크 내 통신 가능
- 로컬 LAN 통신

Ethernet (이더넷)

- 세계에서 가장 널리 사용되는 네트워크 기술입니다!
- LAN의 물리적 및 논리적 측면을 정의하는 표준군을 나타냅니다.
- 로컬 네트워크(LAN)를 구축하기 위한 표준 통신 프로토콜입니다.
    - 물리적(Physical)
        - 케이블링, 커넥터, 장비 등
    - 논리적(Logical)
        - 네트워크 액세스 방법, 즉 캐리어 감지 다중 접속(CSMA)

계층별 장비 - 1계층 (물리 계층)

- 리피터
  - 전송 신호를 증폭
  - 단순히 신호만을 증폭하여 전달
- 허브
  - 여러 노드를 연결하여 데이터 통신
  - 작은 네트워크에 사용

리피터

허브

계층별 장비 - 2계층 (데이터링크 계층)

- 스위치
  - 여러 노드를 연결, MAC 주소 기반으로 통신
- NIC(네트워크 인터페이스 카드)
  - 컴퓨터 등 노드가 네트워크에 연결할 수 있도록 하는 장치
  - MAC 주소를 보유
- 모뎀
  - 디지털 신호와 아날로그 신호간 변환을 수행
  - 인터넷 연결의 케이블 모뎀, DSL 모뎀으로 활용

스위치

네트워크 인터페이스 카드

모뎀

계층별 장비 - 3계층 (네트워크 계층)

- 라우터
  - 데이터 패킷을 네트워크 간 라우팅
  - 최적의 경로를 선택하여 네트워크 전송
  - IP 주소를 사용하여 통신 관리
  - 서로 다른 네트워크 연결
- L3 스위치
  - 2계층 장비 스위치에 라우팅 기능을 추가
  - 대규모 LAN 네트워크 환경에 사용

라우터

L3 스위치

계층별 장비 - 4계층 (전송 계층)

- 로드밸런서
  - 트래픽을 여러 서버에 분산
  - TCP/UDP 포트를 기반으로 분산
- L4 스위치
  - TCP/UDP 포트번호와 IP주소 기반으로 트래픽 분산

로드밸런서

L4 스위치

계층별 장비 - 7계층 (응용프로그램 계층)

- WAF (웹 애플리케이션 방화벽)
  - 웹 애플리케이션을 공격으로부터 보호
  - SQL 인젝션, XSS 등 웹 기반 공격을 탐지 및 차단
- L7 로드밸런서
  - L7 계층에서 트래픽을 분산
  - HTTP/S 트래픽 기반으로 로드밸런싱 수행
- L7 스위치
  - L7 계층 로드밸런싱, 콘텐츠 기반 라우팅, WAF 기능 등 L7 계층의 역할 수행

WAF

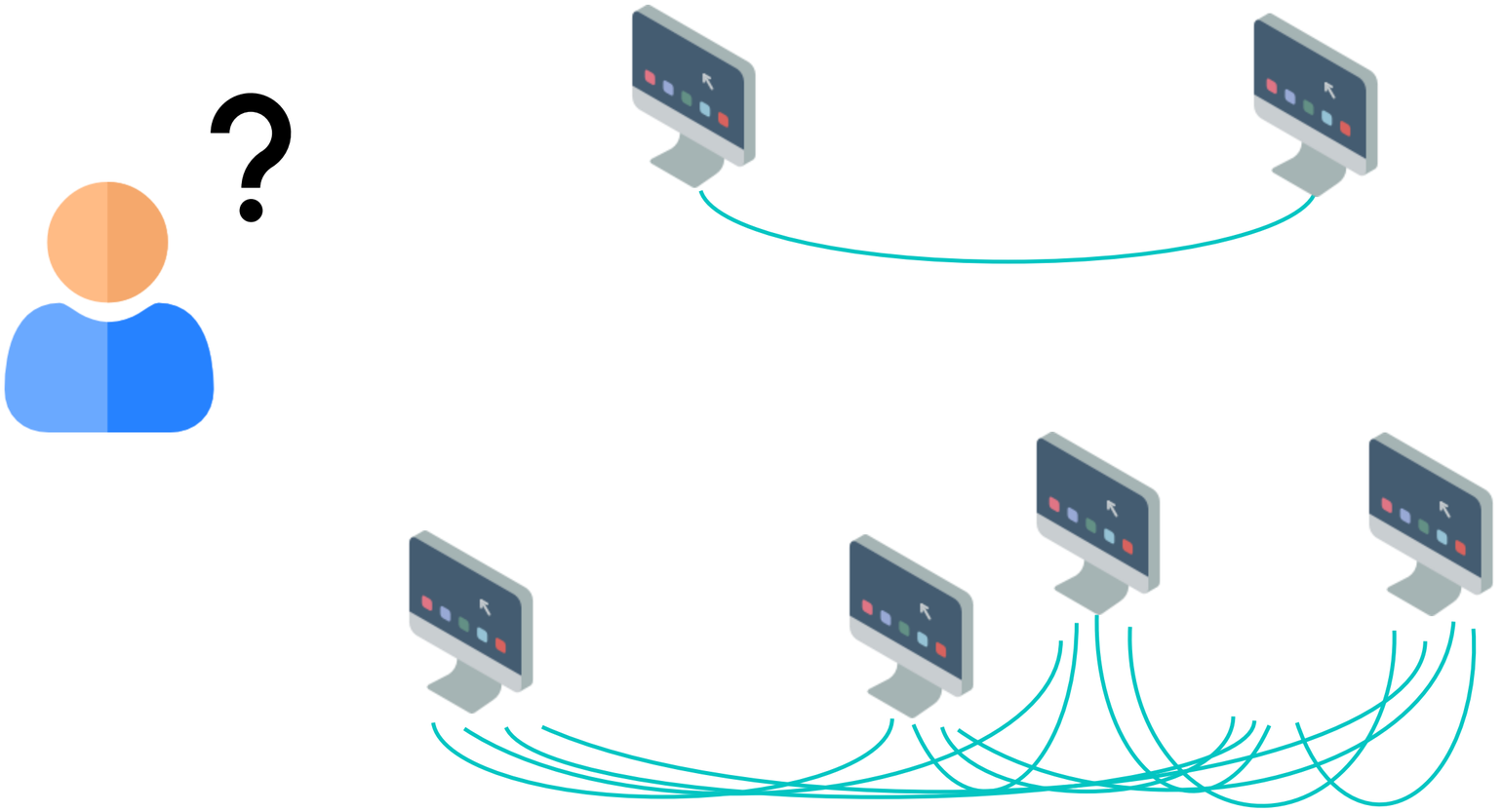
L7 스위치

스위치 개요 및 특징

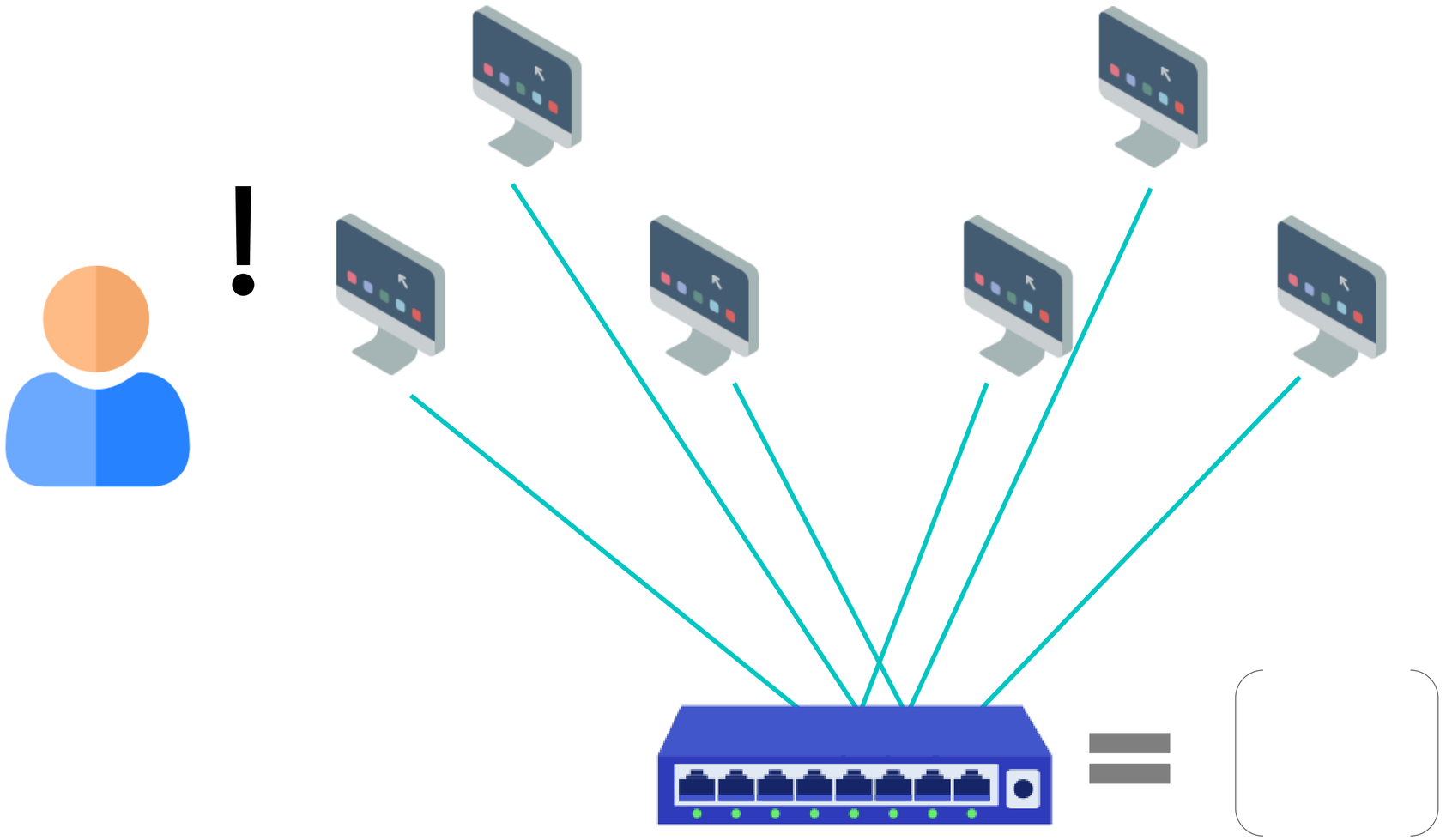
스위치

- MAC 주소를 기반으로 스위칭을 하는 2계층 장비
- 스위칭 : 노드와 노드간 연결을 중개해주는 것

장비 간 연결?

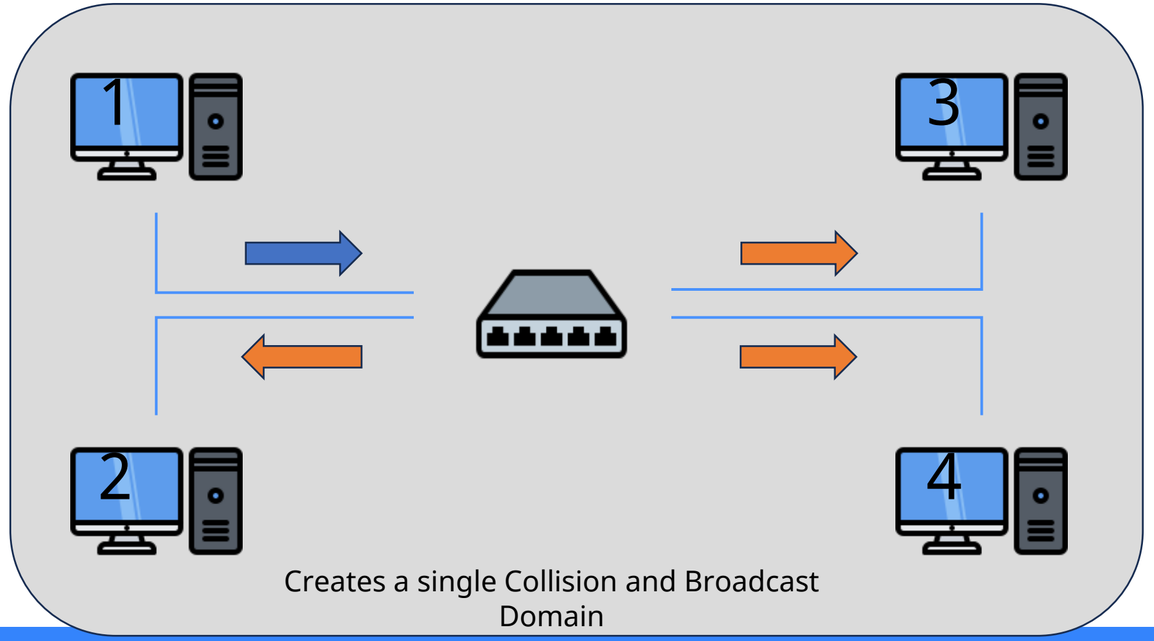


장비 간 연결!



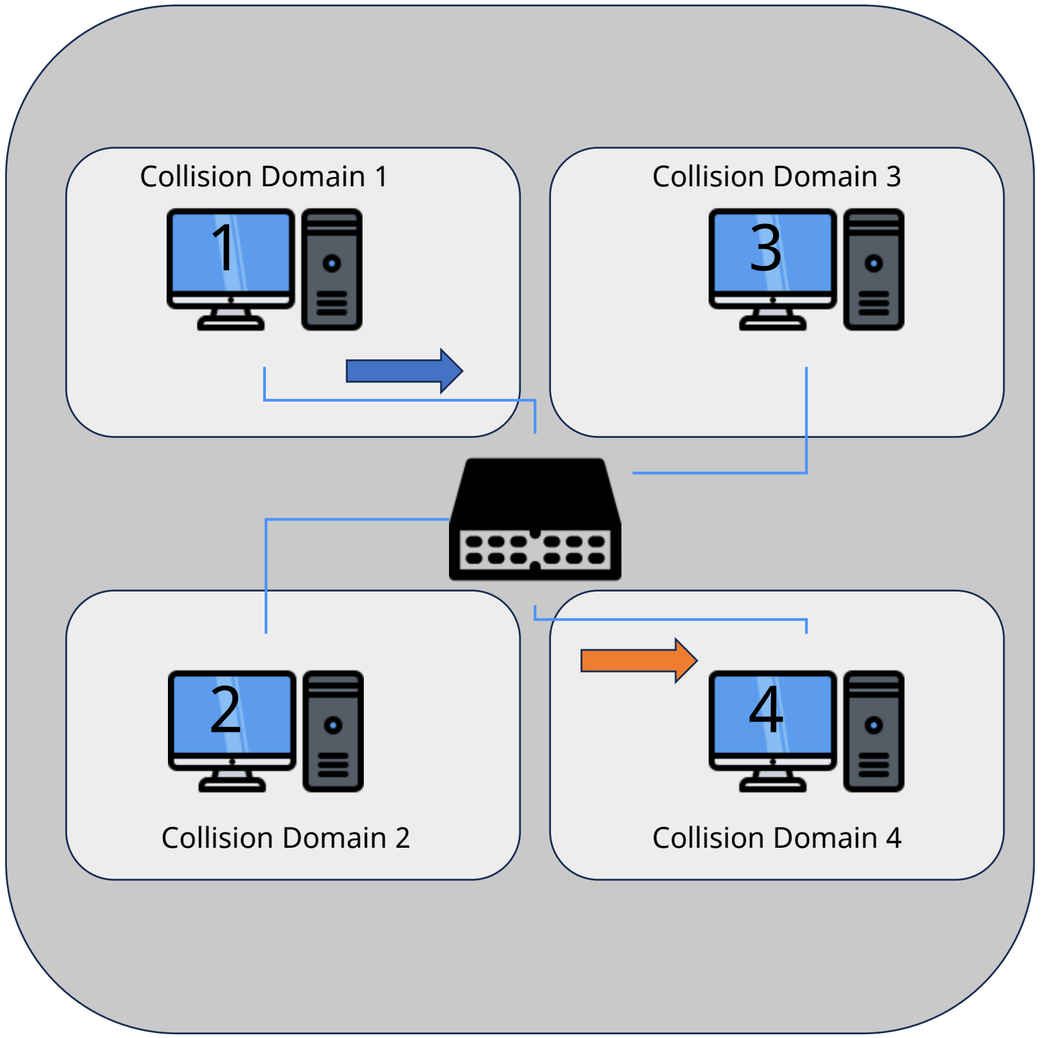
허브 (Hubs)

- 네트워크 내에서 장치들을 연결하는 데 사용됨
- 초기 네트워크에서 사용되었으며, 스위치로 대체됨
- "멀티 포트 리피터“
  - 트래픽이 한 포트로 들어오면 다른 모든 포트로 반복(브로드캐스트)됨
  - OSI 1계층 장치
  - 비지능형 네트워크 장치
  - 네트워크 충돌 오류 증가를 유발함
- 스위치보다 효율성이 훨씬 낮음
- 현재는 사용되지 않는 구형 장비



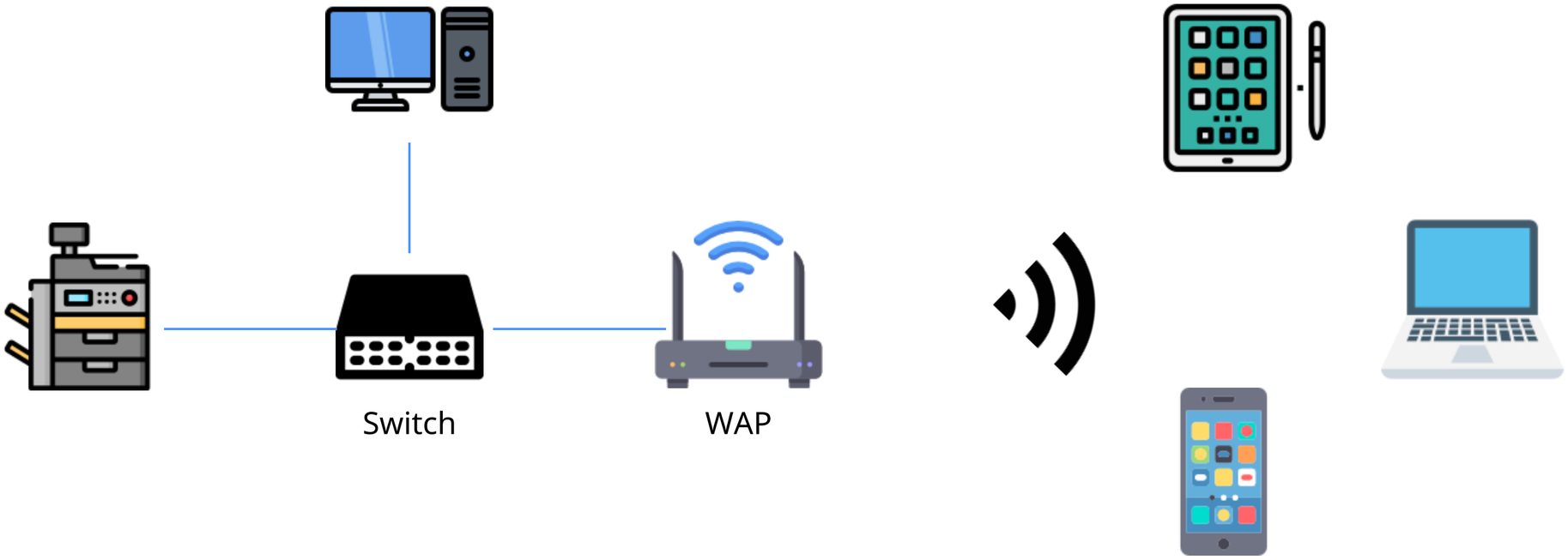
스위치 (Switches)

- 허브와 마찬가지로 장치들을 서로 연결함
- 지능형 네트워크 장치 (OSI 2계층)
- 연결된 각 장치의 MAC 주소를 기억함. 이를 위해 MAC 주소 테이블 또는 콘텐츠 주소 지정 메모리 (CAM) 테이블을 사용
- 통신 과정에서 출발지와 목적지 MAC 주소를 주목함
- 매우 빠른 속도를 제공하는 ASIC (응용 전용 집적 회로)를 사용
- 충돌 도메인을 분리함
    - 트래픽이 한 포트로 들어오면 해당 목적지 포트로만 전달됨
    - 높은 대역폭을 위해 설계됨
    - 오늘날의 네트워크 인프라에서 표준으로 사용됨



무선 액세스 포인트 (Wireless Access Point (WAP))

- 무선 액세스 포인트(WAP)는 유선 네트워크를 무선 네트워크로 확장하는 브리지 역할을 합니다.
- 스위치와 마찬가지로, 데이터 링크 계층(2계층) 장치입니다.
- 참고: WAP는 라우터가 아닙니다.



스위치의 데이터 전달 방법

충돌 도메인 이해하기

- 충돌 도메인은 데이터 충돌이 발생할 수 있는 네트워크 세그먼트를 의미합니다.

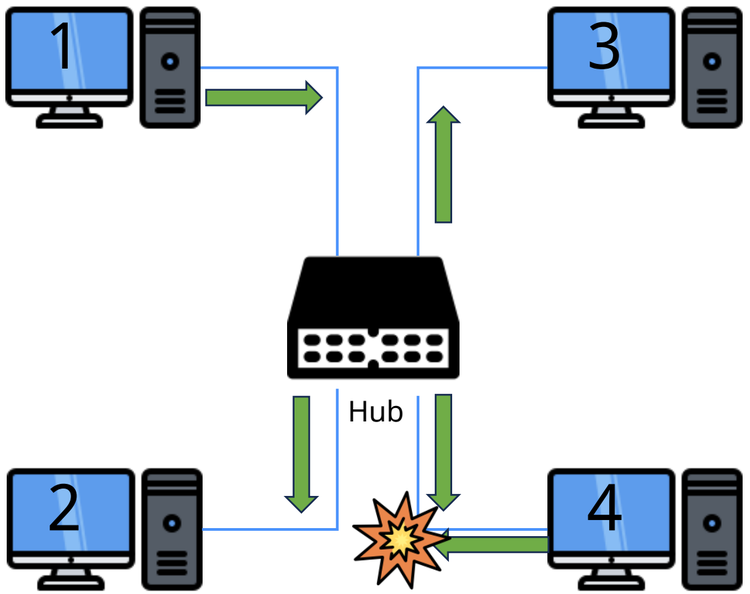
- 이더넷 네트워크에서는 다음과 같은 장치를 사용할 때 충돌이 발생할 수 있습니다:
    - 허브
    - 반이중(Half-Duplex) 모드의 스위치

- CSMA/CD를 활용하여 충돌을 최소화합니다.
    - CSMA/CD: 충돌 감지 다중 접속 (Carrier Sense Multiple Access with Collision Detection)
        - 충돌 감지 기능이 있는 반송파 감지 다중 액세스
        - 데이터 충돌을 줄이기 위해 공유 네트워크 매체에서 사용됩니다.
        - 호스트가 데이터를 언제 전송할지 결정하고 충돌을 감지하도록 돕습니다.
        - 하나의 큰 충돌 도메인을 갖는 허브(다중 포트 리피터)와 함께 사용됩니다.
        - 반이중 모드에서만 스위치와 함께 사용됩니다

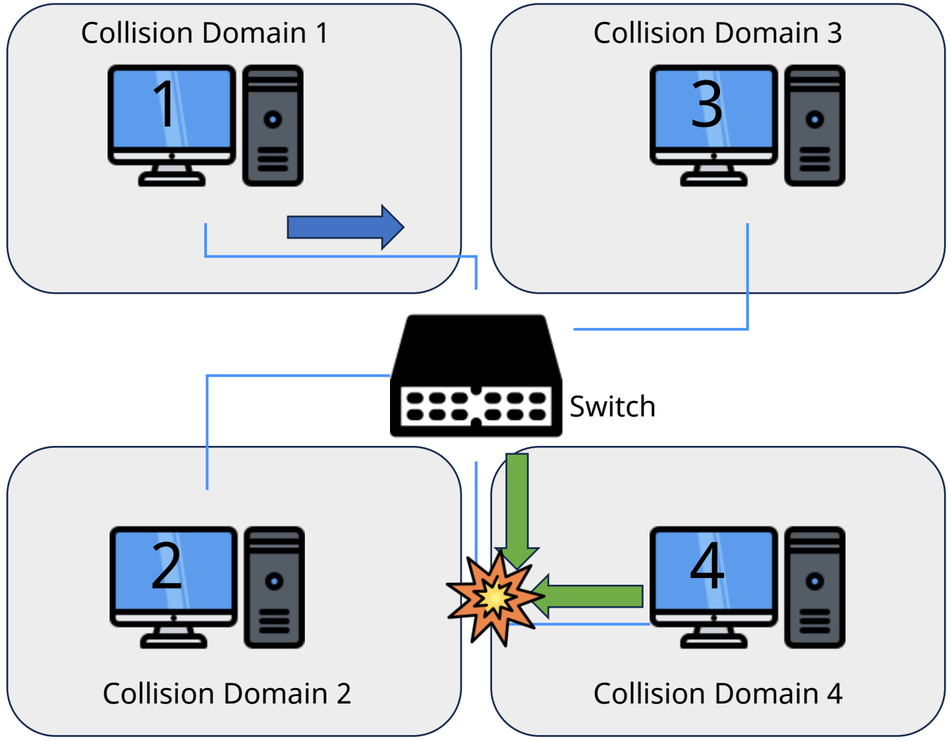
ⓒ Codinghub,2023

충돌 도메인 이해하기

- **허브(Hubs)**
  - 하나의 큰 충돌 도메인(Collision Domain)을 생성합니다.



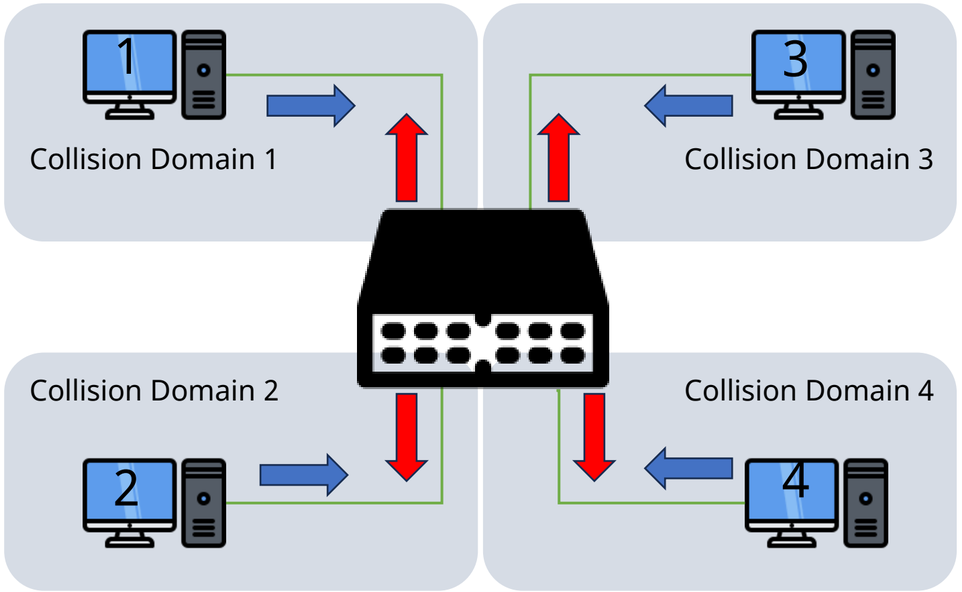
- **스위치(반이중 모드)(Switches in Half-Duplex)**
  - **충돌 도메인을 더 작은 단위로 분할합니다.**

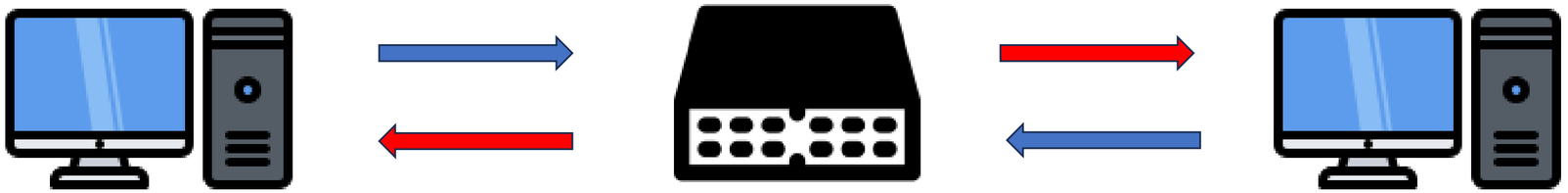


ⓒ Codinghub,2023

전이중 모드 스위치는 충돌을 제거

- **전이중 모드를 사용하는 스위치에서는 충돌이 발생하지 않습니다:**
    - 데이터 전송과 수신을 동시에 처리할 수 있는 전용 채널이 제공됩니다.



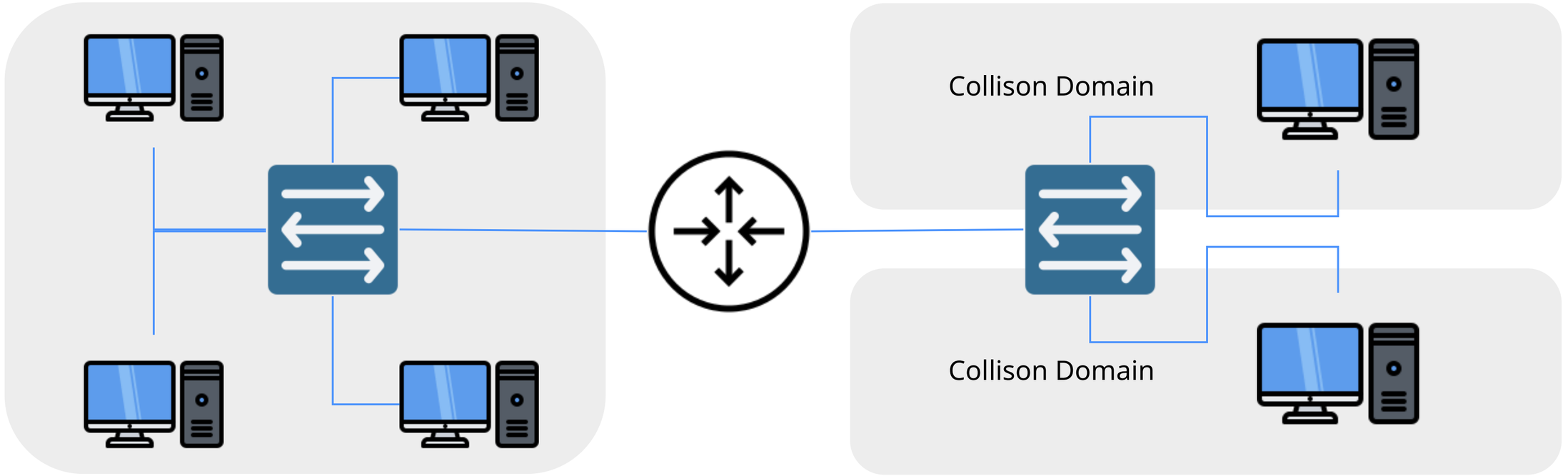


ⓒ Codinghub,2023

브로드캐스트 도메인 이해

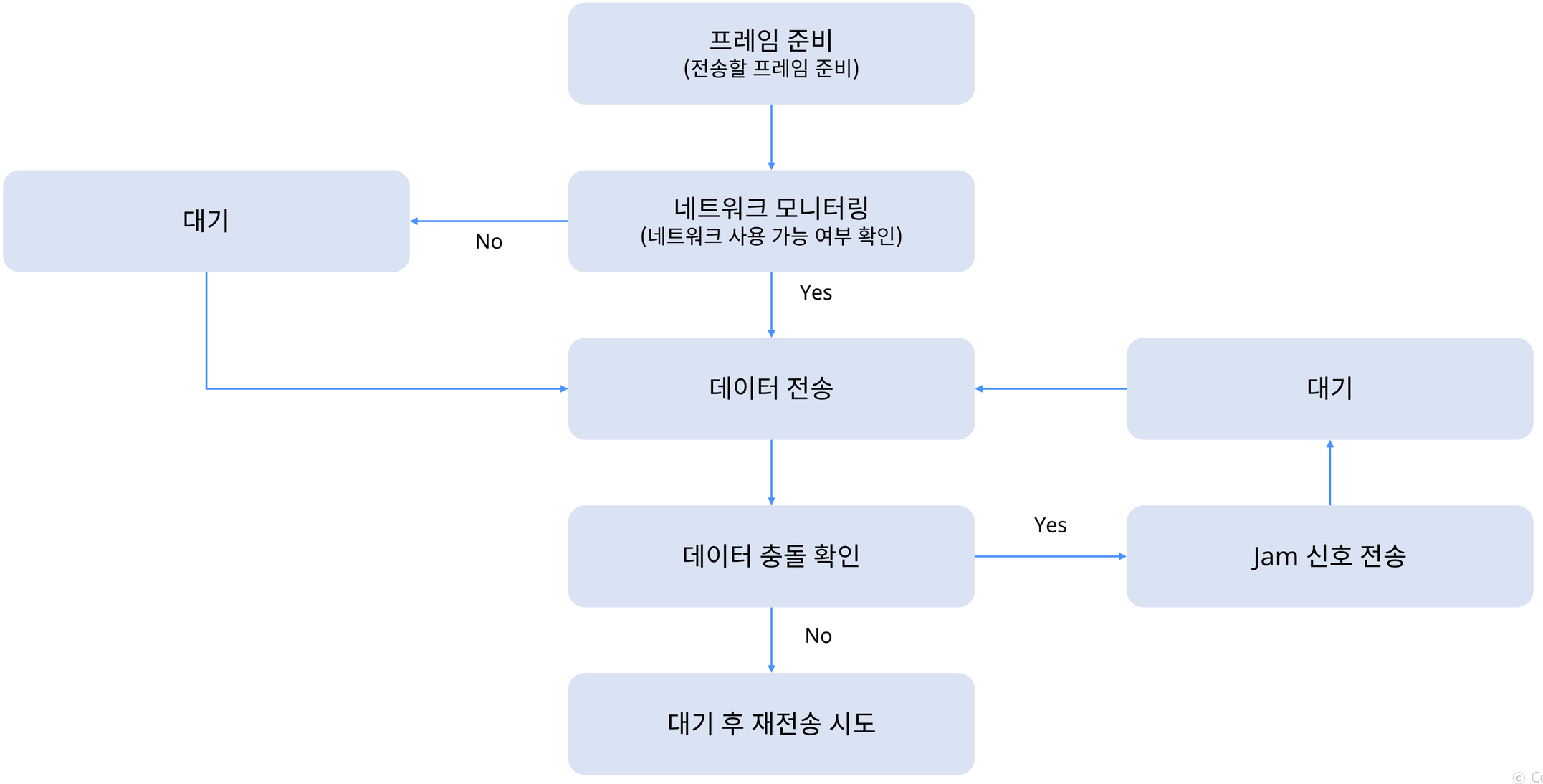
- 브로드캐스트 도메인은 네트워크 내 모든 장치가 서로 이더넷 브로드캐스트 메시지(일대다 메시지)를 수신할 수 있는 네트워크 세그먼트입니다.
    - 예시 브로드캐스트 프로토콜: ARP, DHCP

- 허브와 스위치는 브로드캐스트 메시지를 전달하지만 라우터는 그렇지 않습니다.
    - 브로드캐스트 메시지는 매우 비효율적이고 리소스를 많이 소모합니다.
    - 만약 라우터가 브로드캐스트를 허용한다면, WAN 및 인터넷 성능이 브로드캐스트 폭주로 인해 크게 저하될 수 있습니다.



ⓒ Codinghub,2023

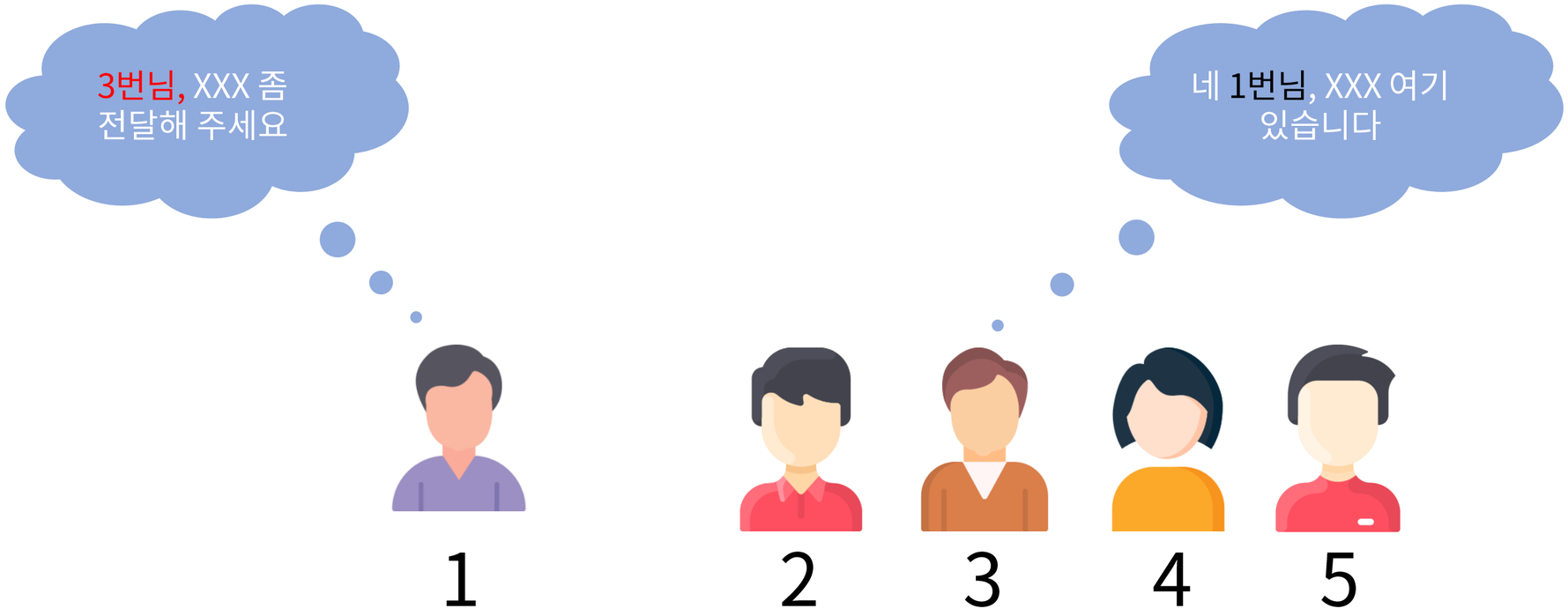
CSMA/CD 프로세스



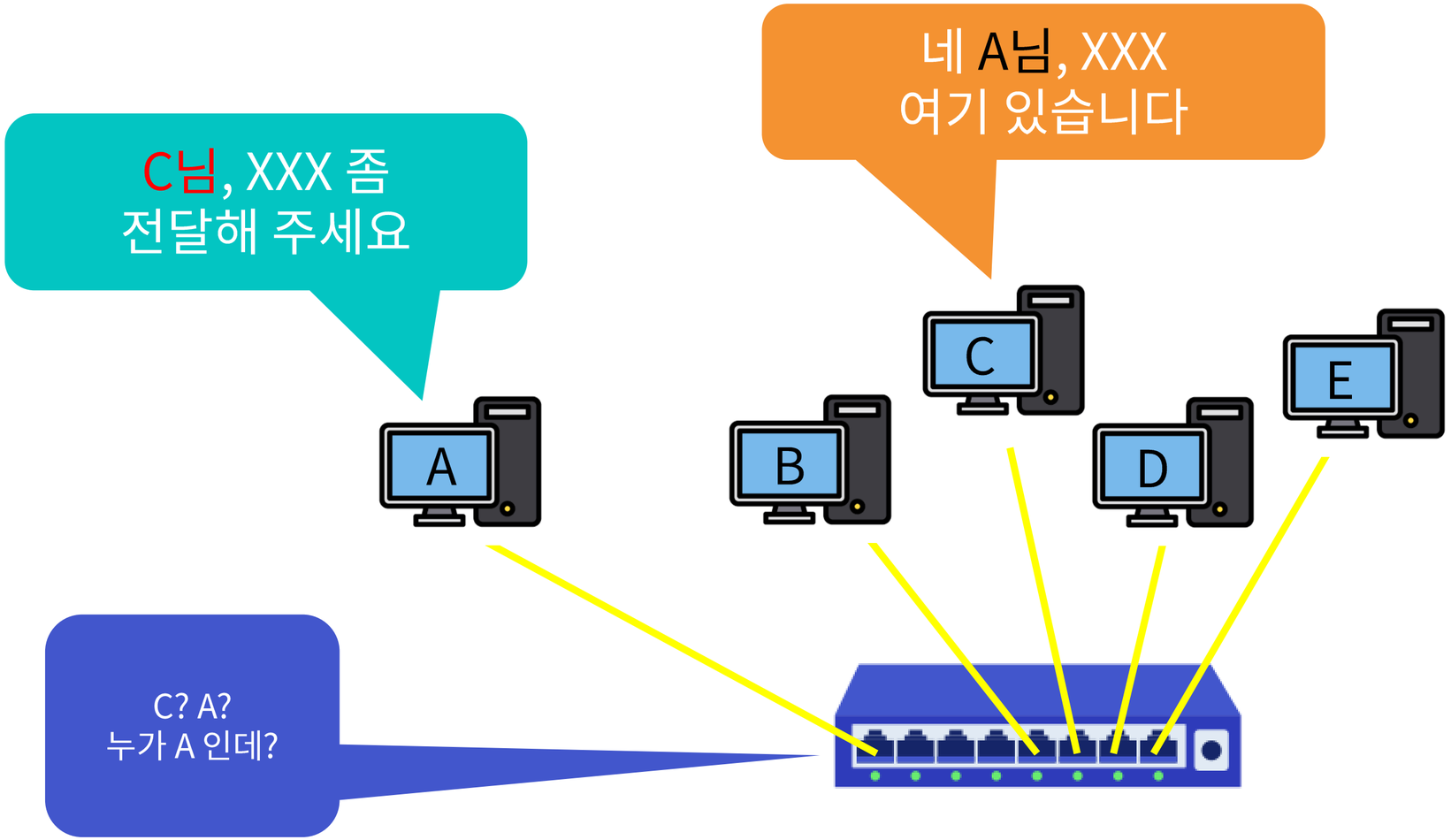
ⓒ Codinghub,2023

스위치 동작방식 이해

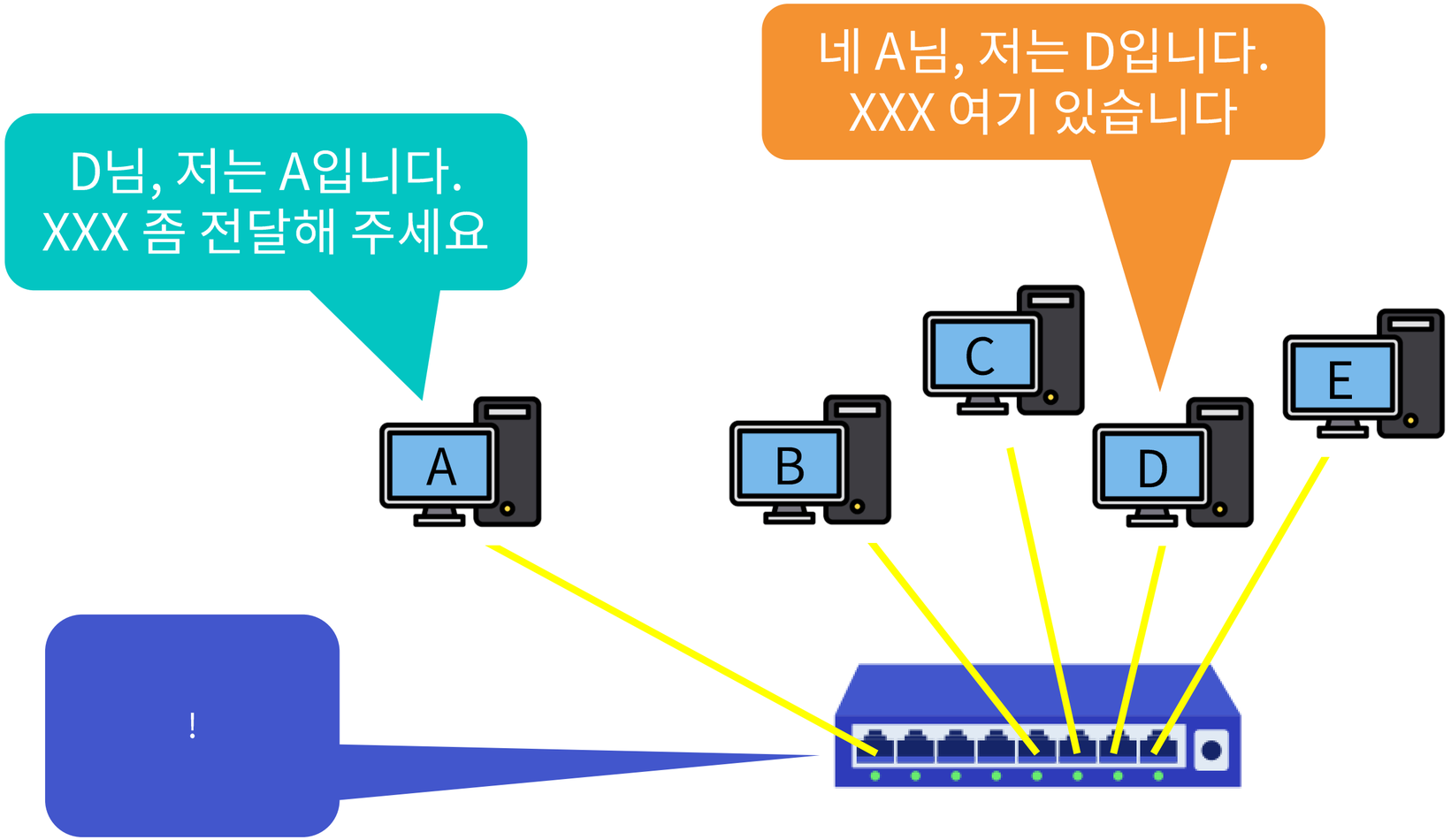
스위치 동작방식 이해



스위치 동작방식 이해 – 장비 간 통신



스위치 동작방식 이해



MAC Address

- 네트워크 상의 장비 구분을 위하여 각 장비의 인터페이스 마다 할당된 주소
- MAC 주소 형식 (48 비트) : D0-3C-1F-9C-FA-F9
- MAC 주소는 일반적으로 네트워크 인터페이스 카드(NIC)의 제조사가 할당하여 하드웨어 저장

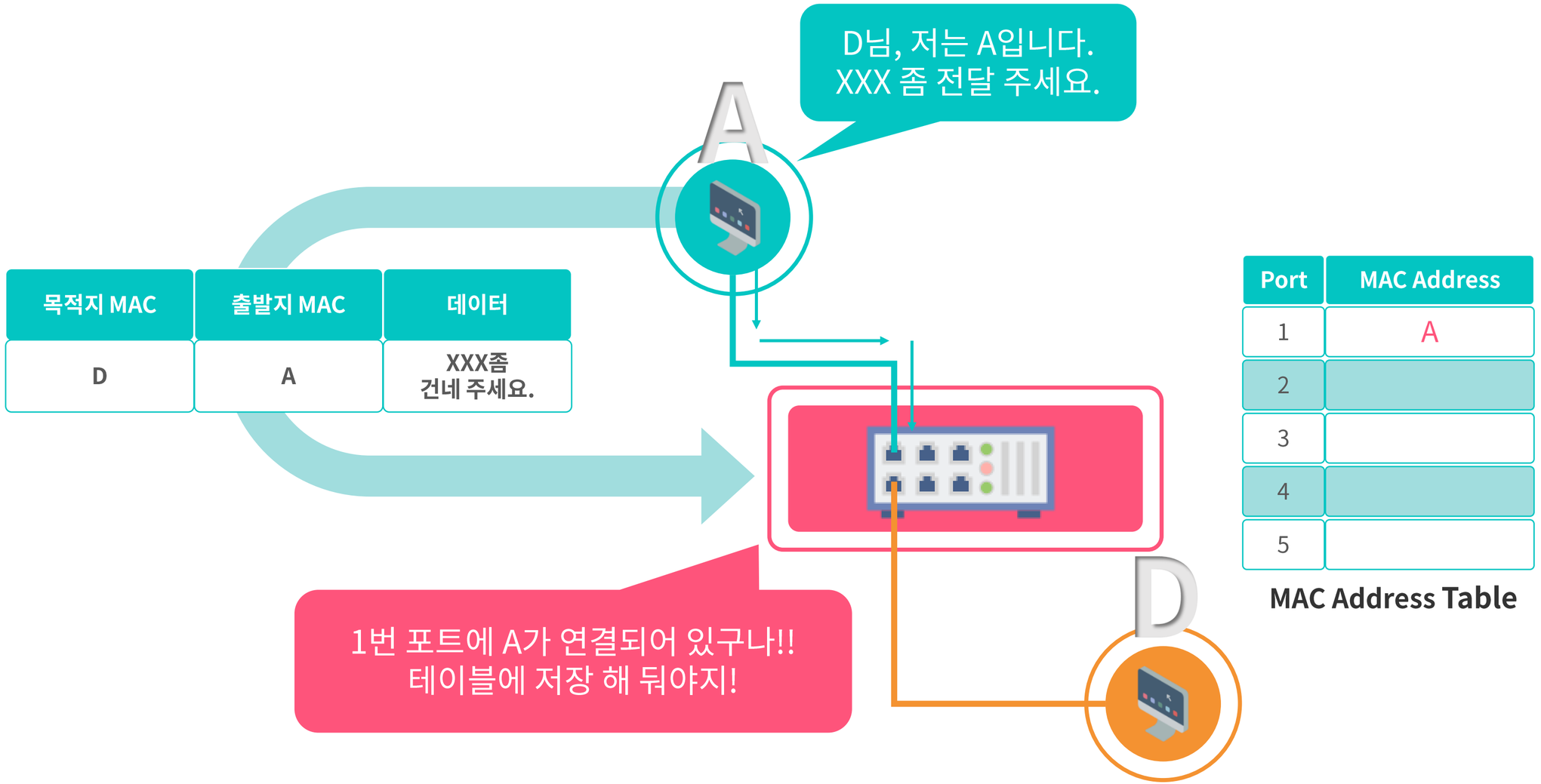
MAC Address Tables

- 스위치가 스위칭 하기 위해 관리하는 테이블

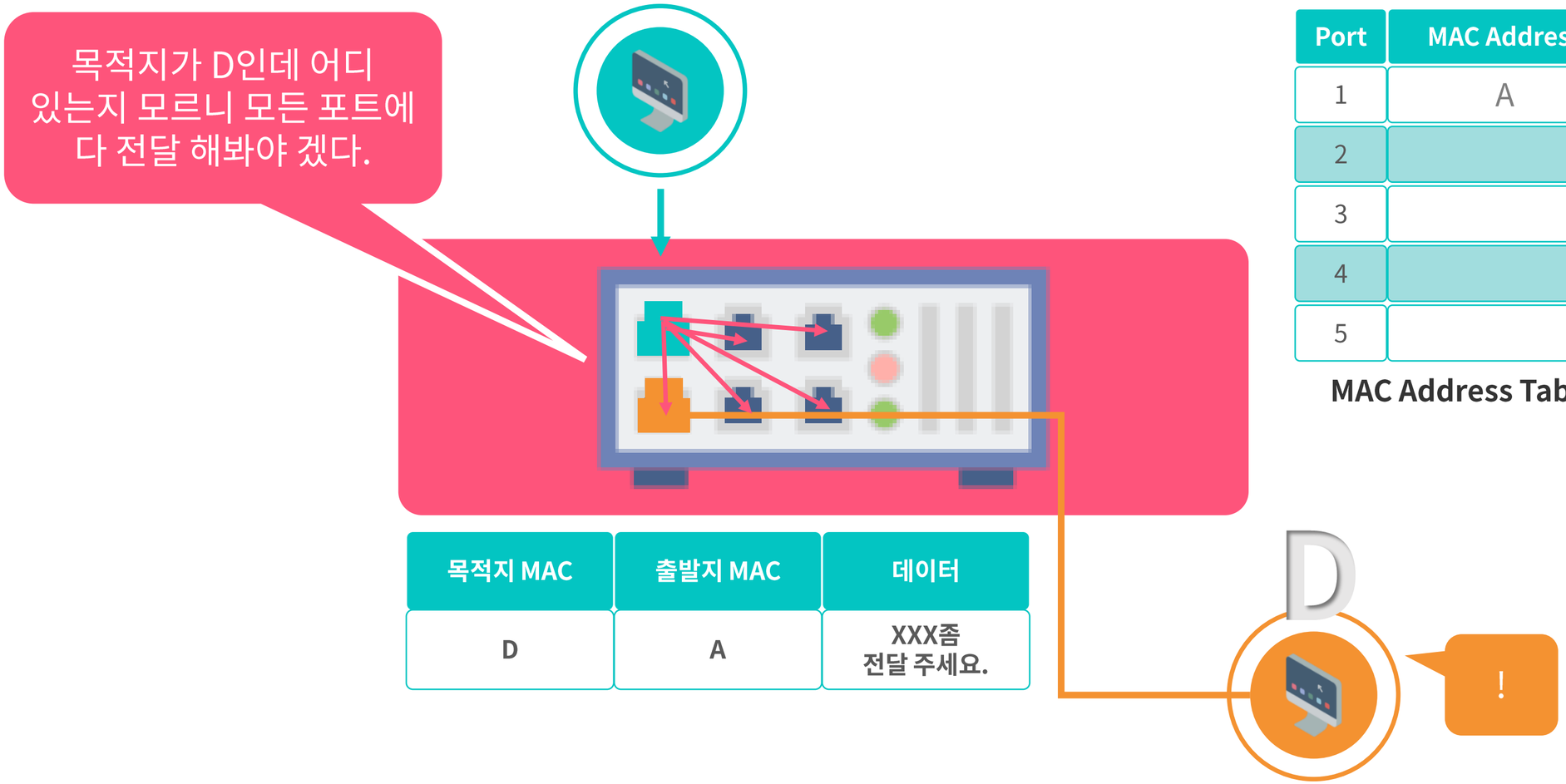
- 예시

MAC Address	Port
00:AB:CD:09:10:20	i0/1
00:AB:CD:60:E3:23	i0/2
00:AB:CD:00:FF:FF	i0/2
00:AB:CD:11:D3:6C	i0/3

스위치 동작 방식 – 명시적 대상 MAC 주소가 있는 프레임 전달



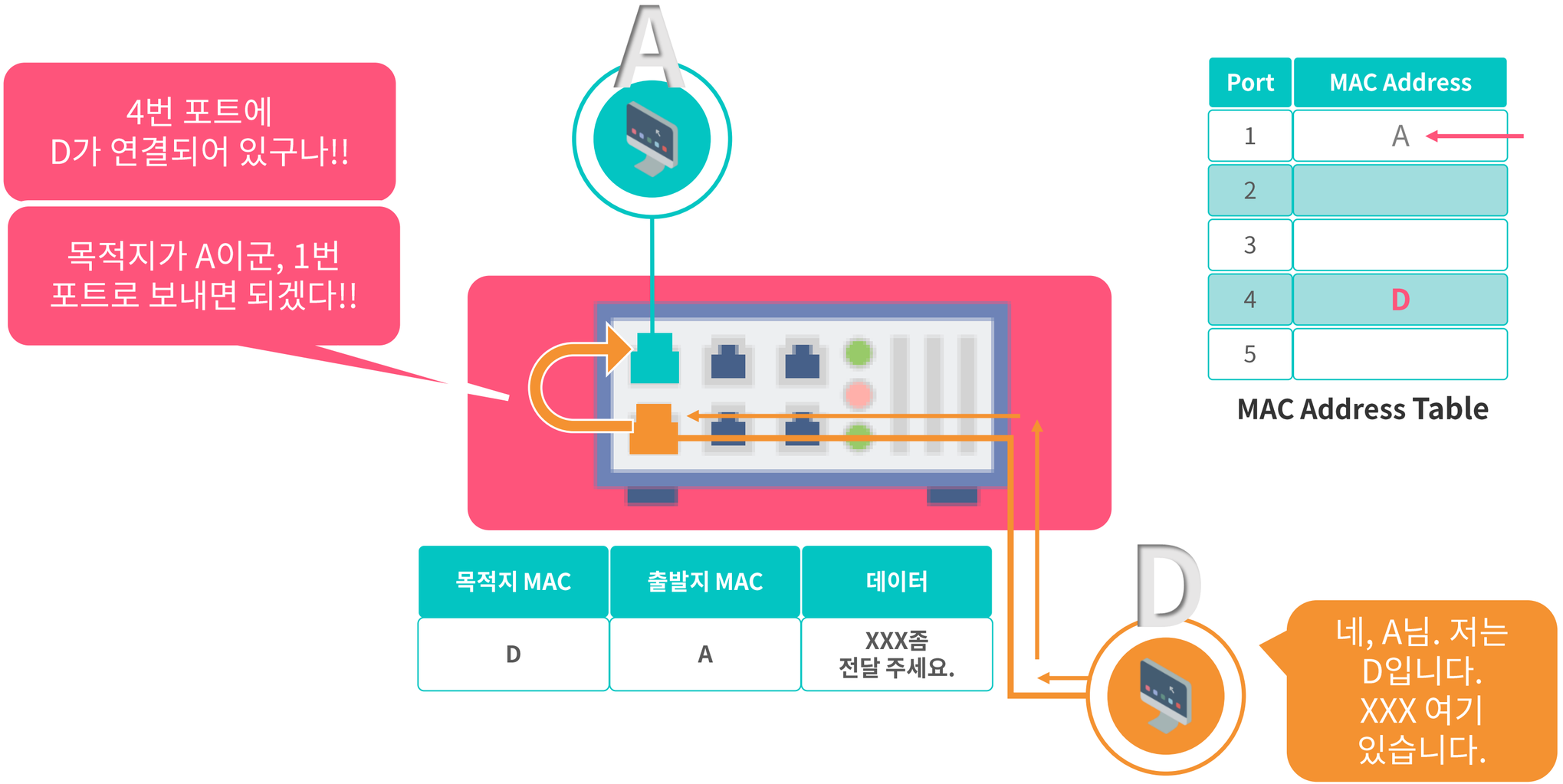
스위치 동작 방식 – 대상 MAC 주소가 MAC 테이블에 없는 경우



Port	MAC Address
1	A
2	
3	
4	
5	

MAC Address Table

스위치 동작 방식 – 대상 MAC 주소가 MAC 테이블에 있는 경우



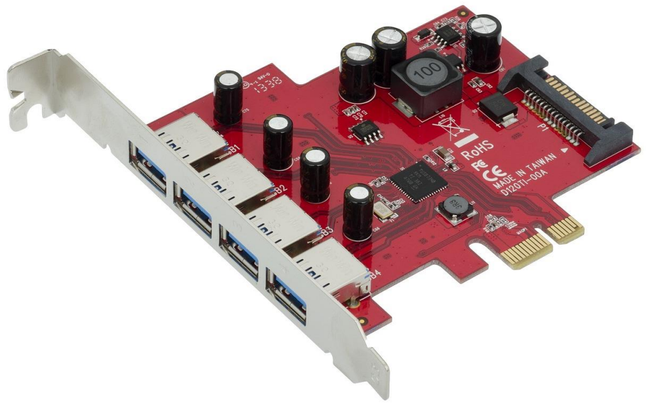
Port	MAC Address
1	A
2	
3	
4	D
5	

MAC Address Table

네트워크 카드(NIC)와 MAC 주소의 역할

네트워크 인터페이스 카드 (NIC)

- 네트워크 장치에 설치된 네트워크 어댑터입니다.
- 네트워크 매체와의 물리적 및 전기적, 광 또는 무선 주파수 연결을 제공합니다.
- 확장 카드, USB 장치, 또는 메인보드에 직접 내장될 수 있습니다.

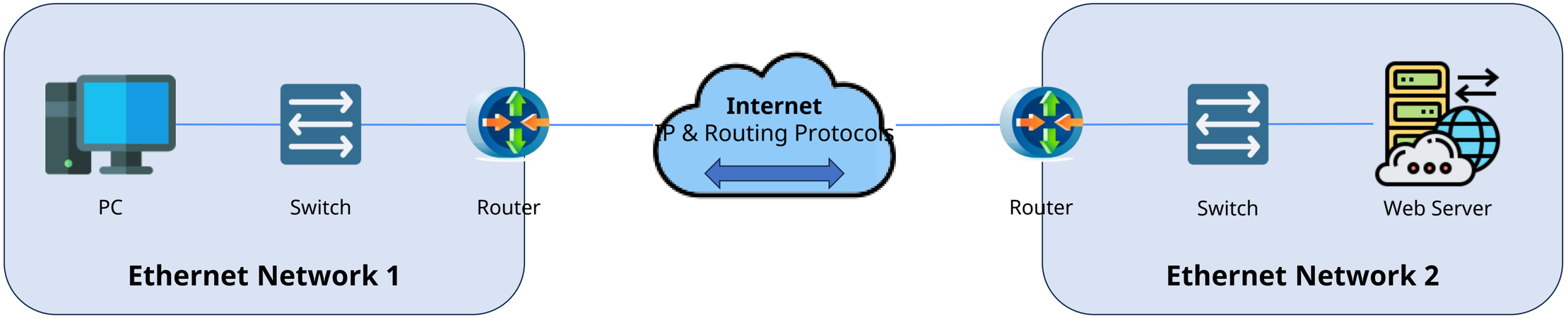


ⓒ Codinghub,2023

IP 주소체계

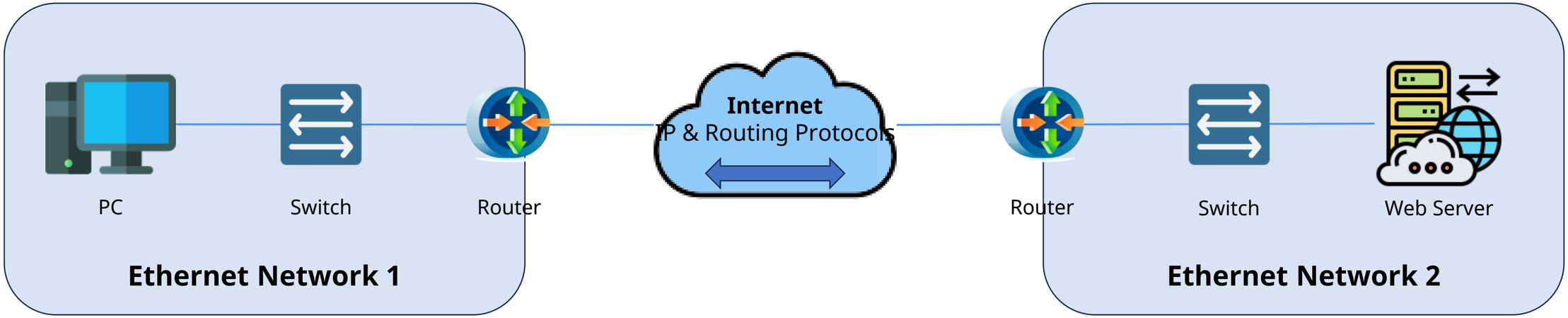
인터넷 프로토콜 (IP)

- OSI 계층 3 프로토콜로, WAN과 인터넷을 통해 데이터를 전달할 수 있도록 패킷의 라우팅 및 논리적 주소 지정을 정의합니다.
- 패킷의 형식과 논리적 주소 체계를 명시합니다.
    - IP 주소: IPv4와 IPv6
- 서로 다른 OSI 계층 2(스위치된) 네트워크를 연결하는 역할을 합니다.
- 라우터를 통해 하나의 계층 2 네트워크에서 다른 계층 2 네트워크로 끝단 연결을 제공합니다.

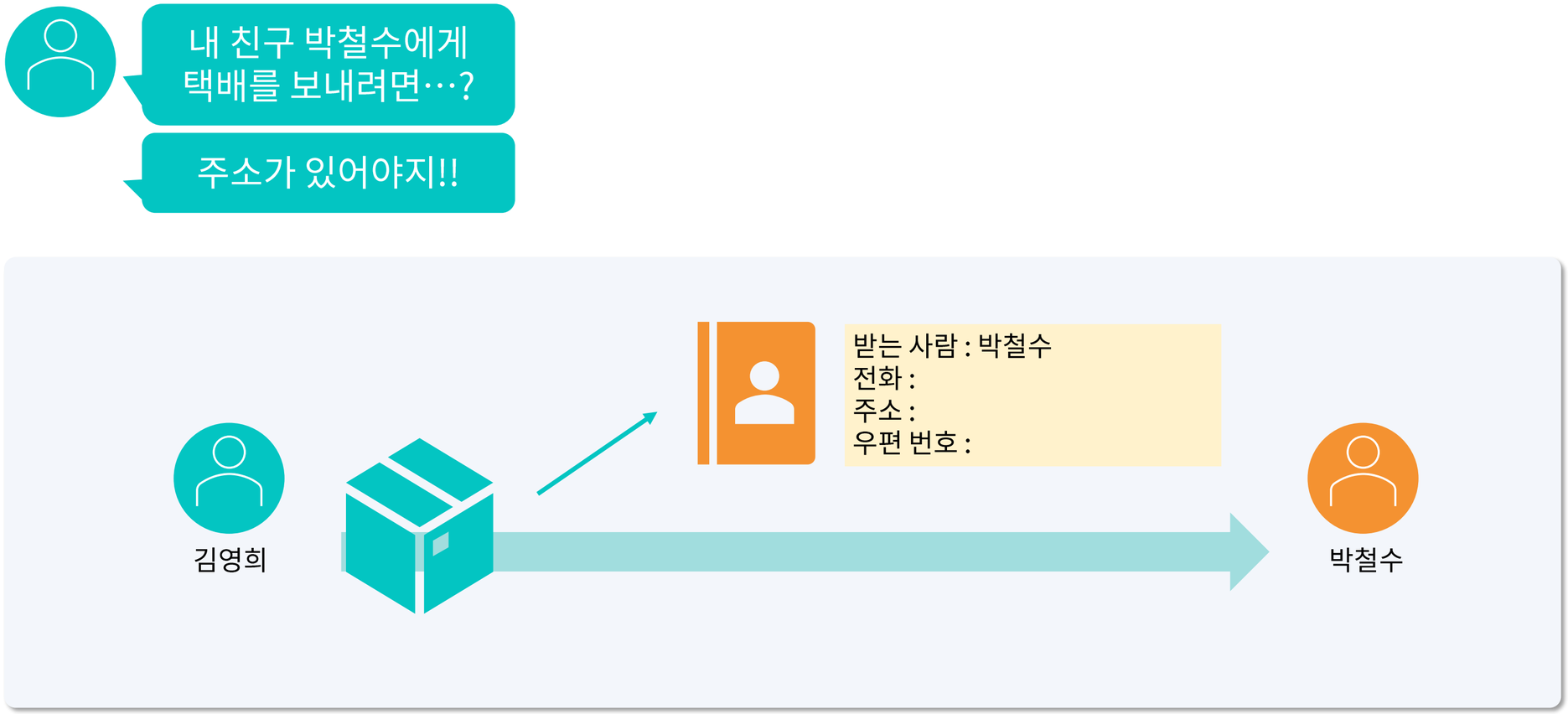


인터넷 프로토콜 (IP)

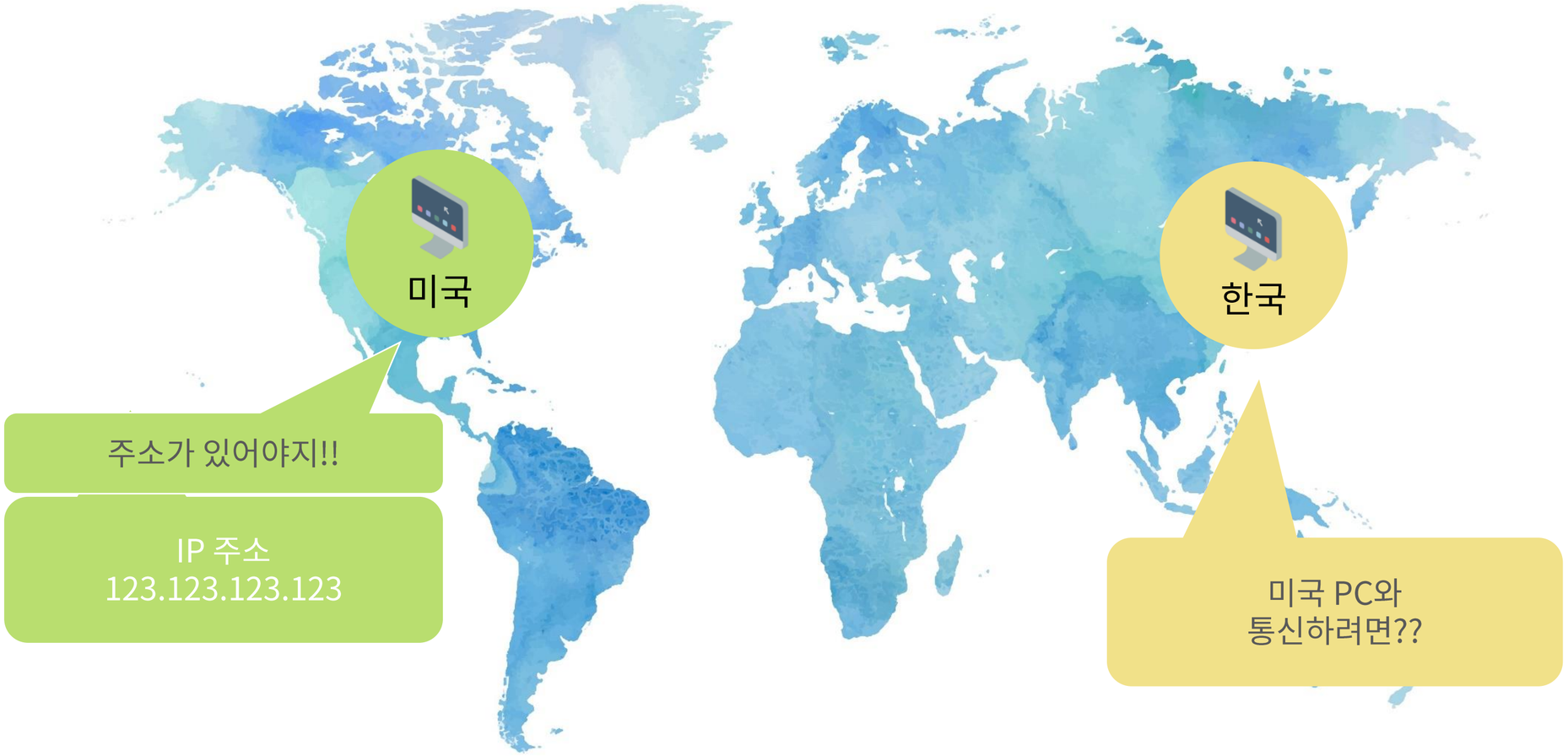
- 연결을 유지하지 않으므로 신뢰할 수 없으며(UDP와 유사), 지속적인 연결이 없습니다.
- 전송되는 각 패킷은 서로 독립적입니다.
  - TCP 및 기타 프로토콜이 이를 올바르게 재조립할 수 있는 수단을 제공합니다.
- 패킷이 항상 같은 경로로 목적지에 도달하지는 않습니다.
  - 가장 효율적인 경로로 전송됩니다.
- 오류 복구나 순서 지정 기능을 제공하지 않습니다.
  - 이는 다른 프로토콜의 역할입니다.



주소의 필요성



서로를 식별하기 위한 방법, 주소 체계 - IP 주소체계



IP 주소 구성

- IP 네트워크에서 장치를 고유하게 식별하기 위해 사용되는 논리적 주소

- IP 주소는 32bit의 2진수로 구성
  - 10101100000100001000000000010001

- 이를 아래와 같은 단계를 거쳐 익숙한 10진수로 바꾸어 표현
  1. 32bit를 4개의 octet으로 나눈 후

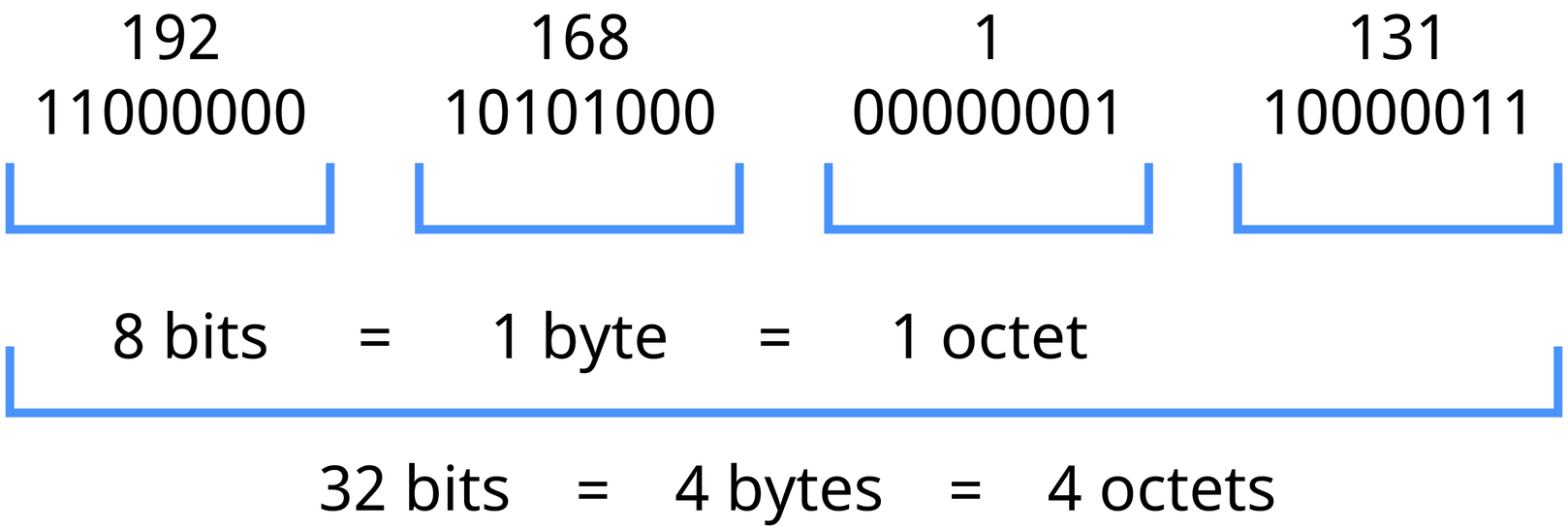
     10101100 00010000 10000000 00010001
  2. 각 octet(1 byte)을 이루는 이진수를 십진수로 변환

     172 16 128 17
  3. 각 십진수를 점을 통해 구분(Dotted-decimal notation)

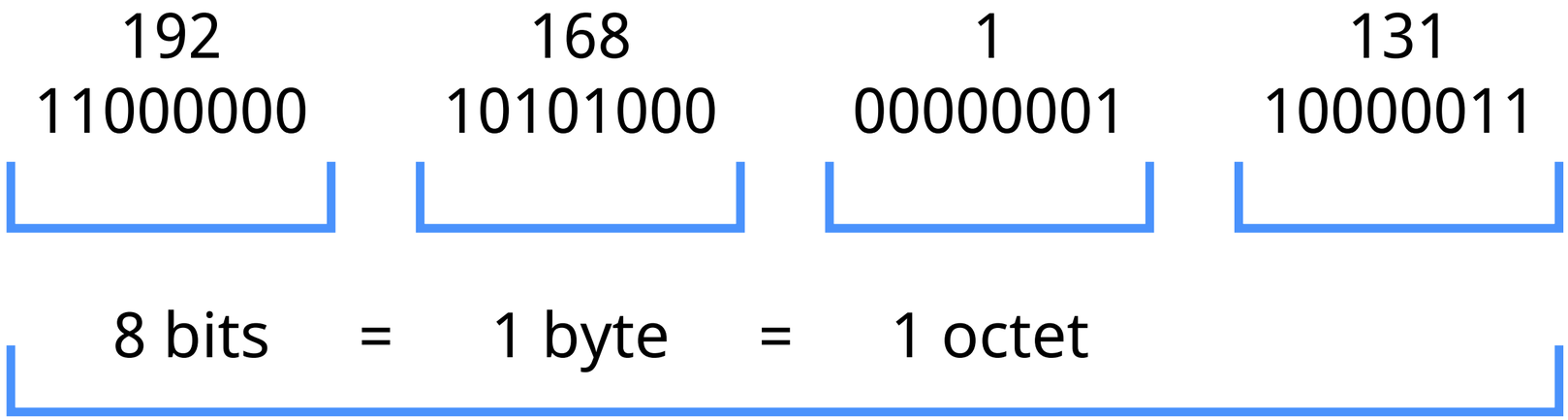
     172.16.128.17

IPv4 주소 구조

- IPv4 주소는 32비트의 이진수로 구성되며, 네트워크 부분과 호스트 부분으로 나눌 수 있습니다. 이 부분은 서브넷 마스크를 통해 구분됩니다.
    - 32비트의 이진수는 4개의 octet(1 octet = 8 bits)으로 나뉩니다.
    - 각 octet은 10진수로 변환되며, 점(.)으로 구분됩니다.
    - 이러한 이유로, IP 주소는 점 분리 10진수 표기법으로 표현됩니다.



IPv4 주소 구조



32 bits = 4 bytes = 4 octets

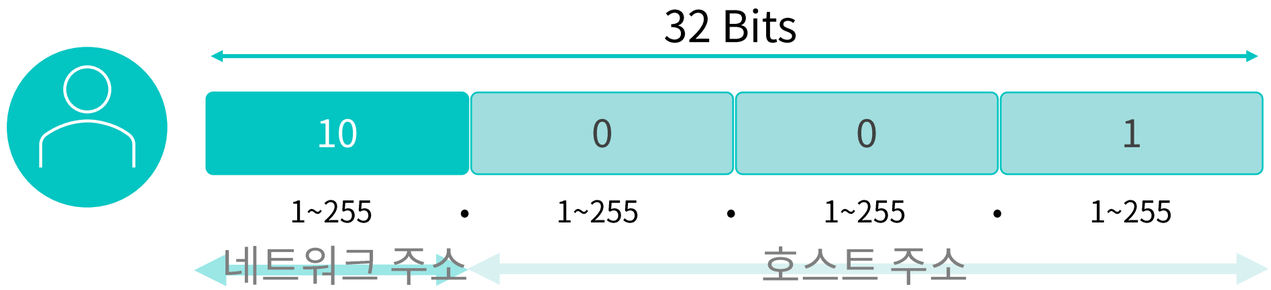
First Octet	Second Octet	Third Octet	Fourth Octet
192	168	1	131
11000000	10101000	00000001	10000011
8 bits	8 bits	8 bits	8 bits

네트워크 및 호스트 부분

- IP 주소는 두 부분으로 나뉩니다:
    - 네트워크 주소 (Network Address)
        - 인터넷의 수많은 네트워크 중에서 특정 네트워크를 식별해 주는 역할
        - 예시: 당신의 거리 이름: 언주로 425

    - 호스트 주소 (Host Address)
        - 같은 네트워크의 수많은 호스트들 중에서 특정 호스트를 식별해 주는 역할
        - 예시: 당신의 집 주소: OO 빌딩

- 네트워크 주소 + 호스트 주소 = IP 주소
    - 예시: 언주로 425 OO 빌딩



IPv4 주소 구성 요소

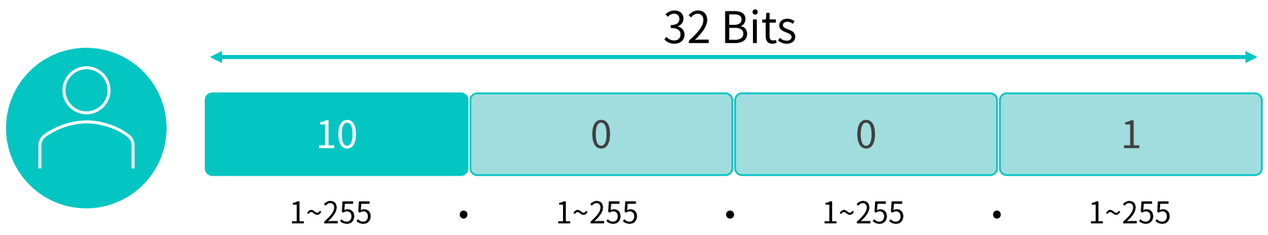
- 네트워크에 있는 각 장치는 IP 주소, 서브넷 마스크 및 기본 게이트웨이를 할당받습니다:
    - IP 주소: 네트워크에 있는 각 장치에 할당된 고유한 논리적 주소.
    - 서브넷 마스크: 장치가 어떤 서브넷에 속해 있는지, 특히 IP 주소의 네트워크와 호스트 부분을 결정하는 데 사용됨.
    - 기본 게이트웨이: 네트워크 라우터의 IP 주소로, 로컬 네트워크에 있는 장치들이 다른 네트워크와 통신할 수 있게 해 줌.

네트워크 크기와 네트워크 클래스

첫번째 옥탯으로
네트워크 주소를 표현하고
나머지 옥탯으로
Host 주소를 표시 해야겠다.

+

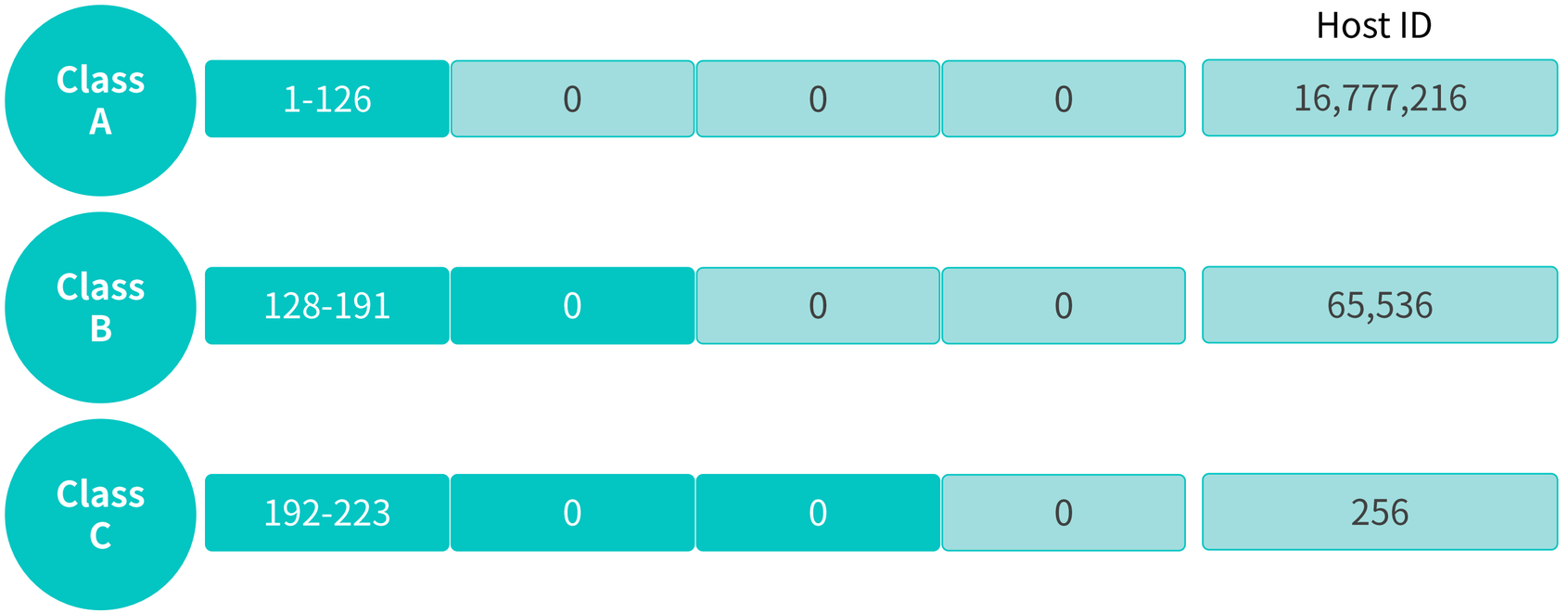
이정도면 충분하겠지?



네트워크 크기와 네트워크 클래스

쓰다보니 네트워크 개수가 부족하군,
네트워크를 표현하는 옥탯 수를 늘려서
네트워크 수를 늘려야겠다.

각 클래스의 구분은
첫번째 옥탯의 범위에 따라 나누자



네트워크 크기와 네트워크 클래스

IP 주소 Class	IP 주소 영역 (첫번째 octet의 십진수 값)
Class A	1-126 (00000001-01111110)
Class B	128-191 (10000000-10111111)
Class C	192-223 (11000000-11011111)
Class D	224-239 (11100000-11101111)
Class E	240-255 (11110000-11111111)

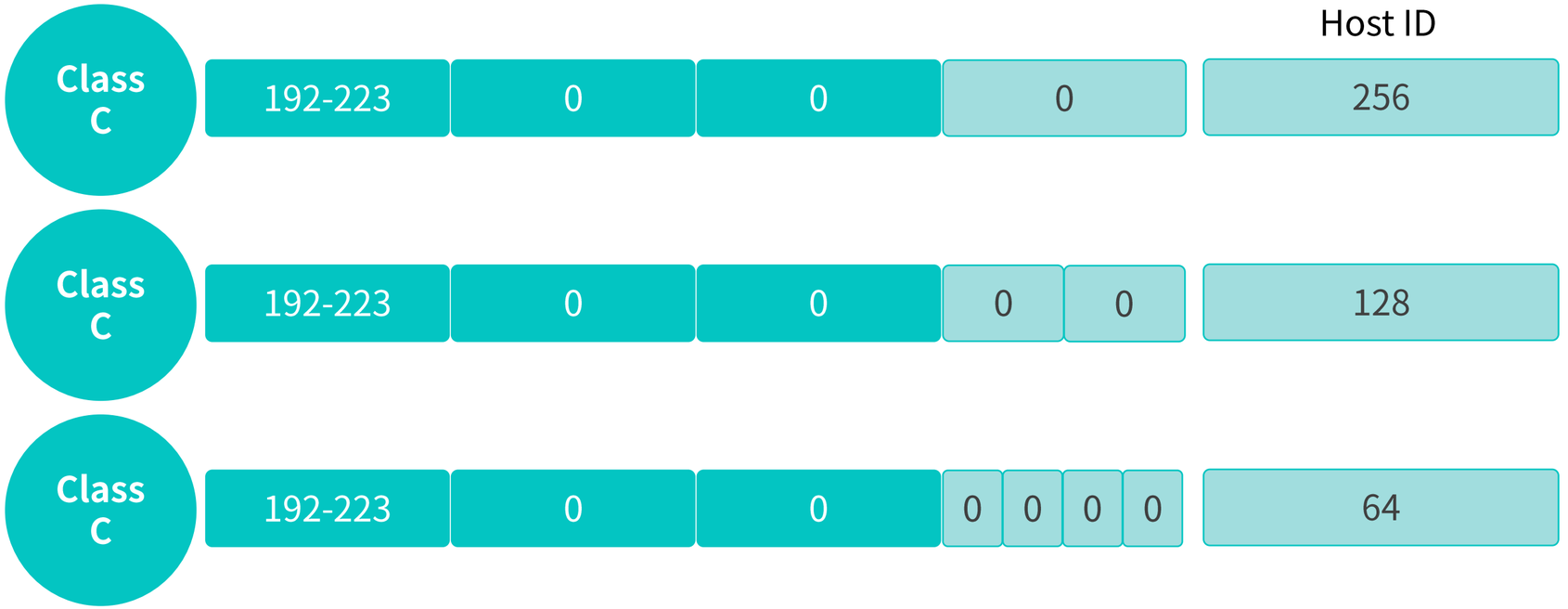
첫번째 octet의 십진수 값을 통해
Class가 구분되어 진다.

- Class A 주소 중 127 (011111111)은 Loopback 테스트(Local Host)을 위해 예약되어 있기 때문에 네트웍 주소로는 사용 불가
- Class D 는 multicast groups을 위해 사용되며, 이때 Network과 Host 주소로 구분 X
- Class E 영역은 오직 연구용으로만 예약되어 사용 불가

네트워크 크기와 서브넷 마스크

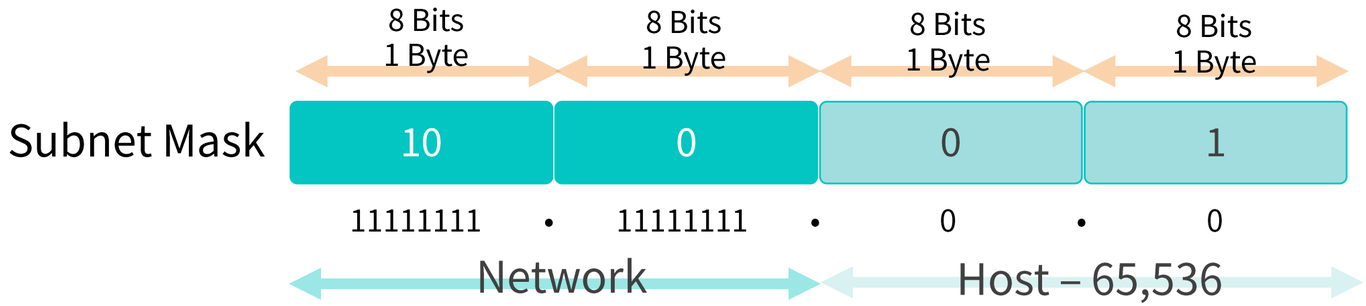
네트워크를 옥탯(8bit) 단위로 구분하여
사용했는데도 개수가 부족하니,
옥탯(8bit) 말고 bit 단위로 구분하자

클래스 별로 나누던 방식 말고
네트워크 크기를 알기 위한
방법을 만들어야겠다



네트워크 크기와 서브넷 마스크

- 서브넷 마스크(Subnet Mask)
  - IP 주소 중 네트워크 주소와 호스트 주소를 구분하기 위하여 만든 32bit의 2진수



서브넷팅(subnetting)

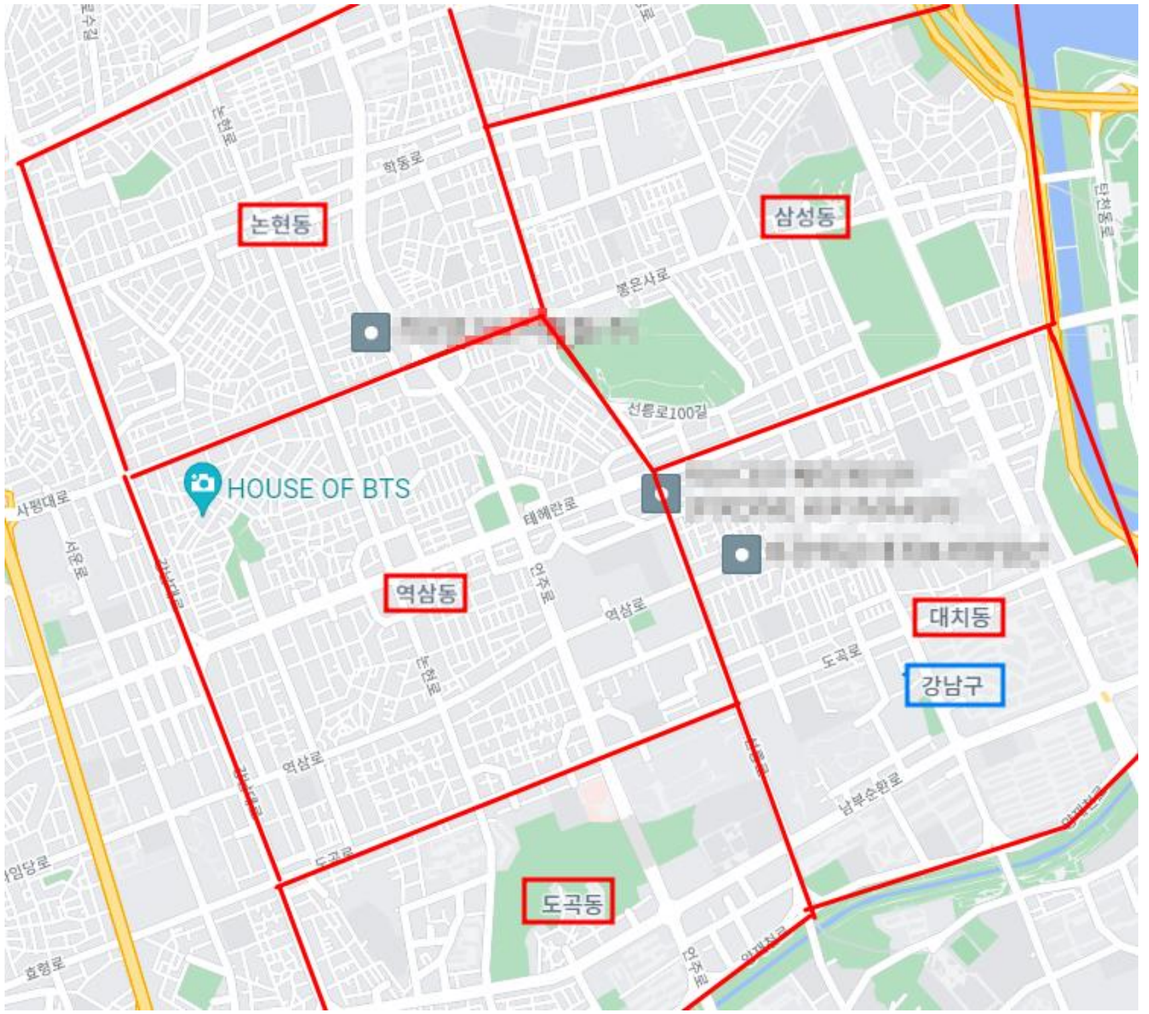
- 서브넷팅이란?
  - 네트워크를 더 작은 단위의 네트워크로 분할
  - 네트워크 부족 현상 해결, 브로드캐스트 도메인 분할, 관리 용이성 등 여러가지 목적에 따라 작은 네트워크로 나누어 사용

*브로드캐스트 : 연결된 모든 호스트에 데이터를 전송하는 방식

- 서브네트워크란?
  - 큰 네트워크에서 분할되어 만들어진 더 작은 단위의 네트워크

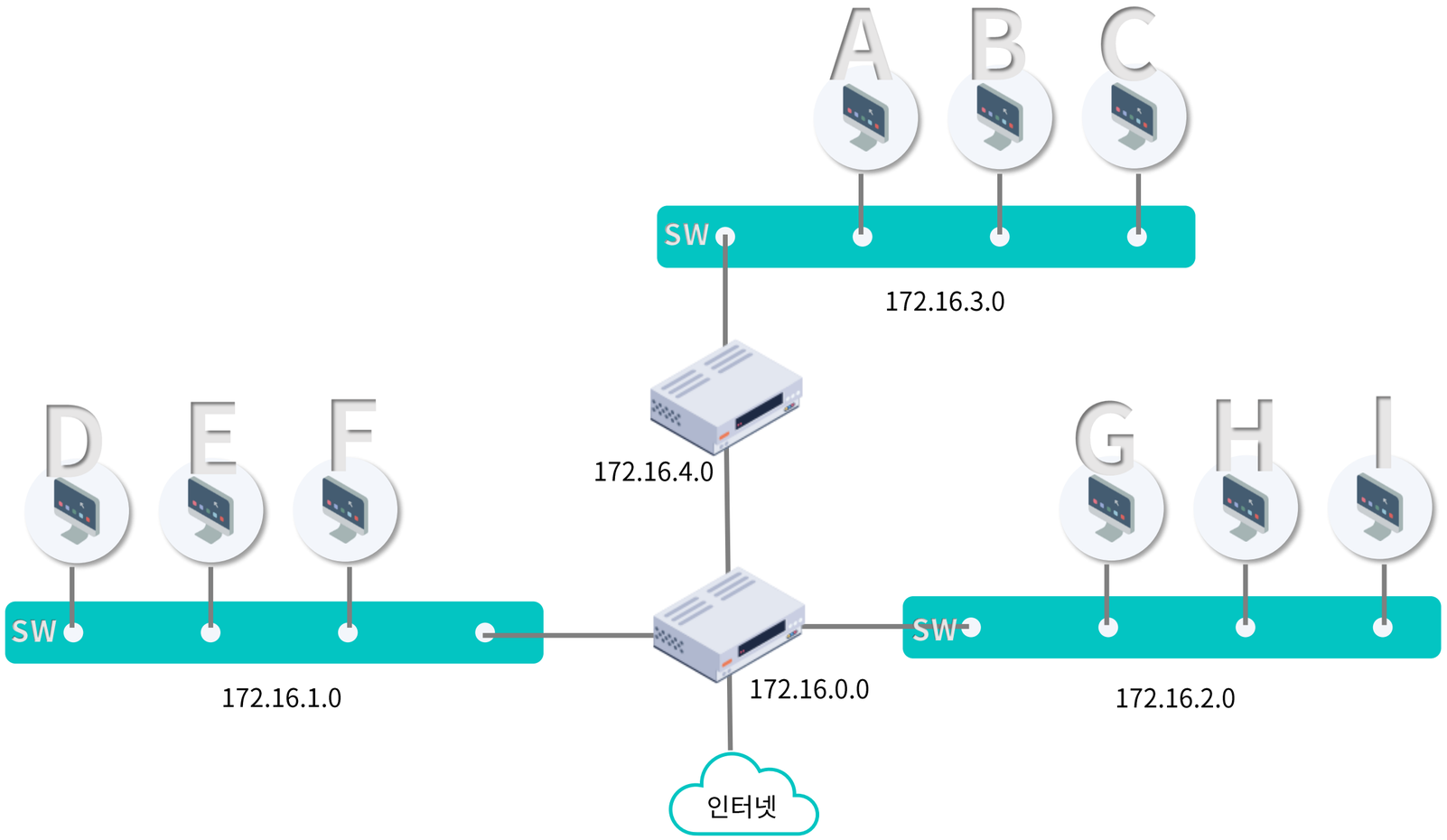
서브 네트워크(Subnetwork)

- 강남구
  - 논현동
  - 삼성동
  - 역삼동



서브 네트워크(Subnetwork)

- 172.16.0.0
  - 172.16.1.0
  - 172.16.2.0
  - 172.16.3.0
  - 172.16.4.0



공인(Public) IP와 사설(Private) IP

- 공인(Public) IP
  - IP주소를 관리하는 기관에 사용권을 요청하여 할당 받아 사용하는 IP
  - IANA(internet Assigned Names Authority)에서 관리하며
    한국의 경우 한국인터넷 진흥원(KISA)에서 IP를 할당 받아 관리
- 사설(Private) IP
  - IP주소 중 특수 목적으로 예약된 IP주소로 같은 네트워크 내에서만 통신 가능
  - 인터넷상의 누군가와 통신하려면 공인 IP 필요

Class	RFC 1918 Internal 주소 영역
Class A	10.0.0.0 to 10.255.255.255
Class B	172.16.0.0 to 172.31.255.255
Class C	192.168.0.0 to 192.168.255.255

CIDR 표기법

- CIDR : 클래스 없는 도메인 간 라우팅
    - 서브넷팅을 위한 방법론
    - "슬래시" 표기법은 서브넷 마스크와 연관된 비트 수를 나타냅니다.

- 서브넷 마스크를 간단하게 표현하는 방법:
    - /8 = 11111111.00000000.00000000.00000000
    - /8 = 255.0.0.0

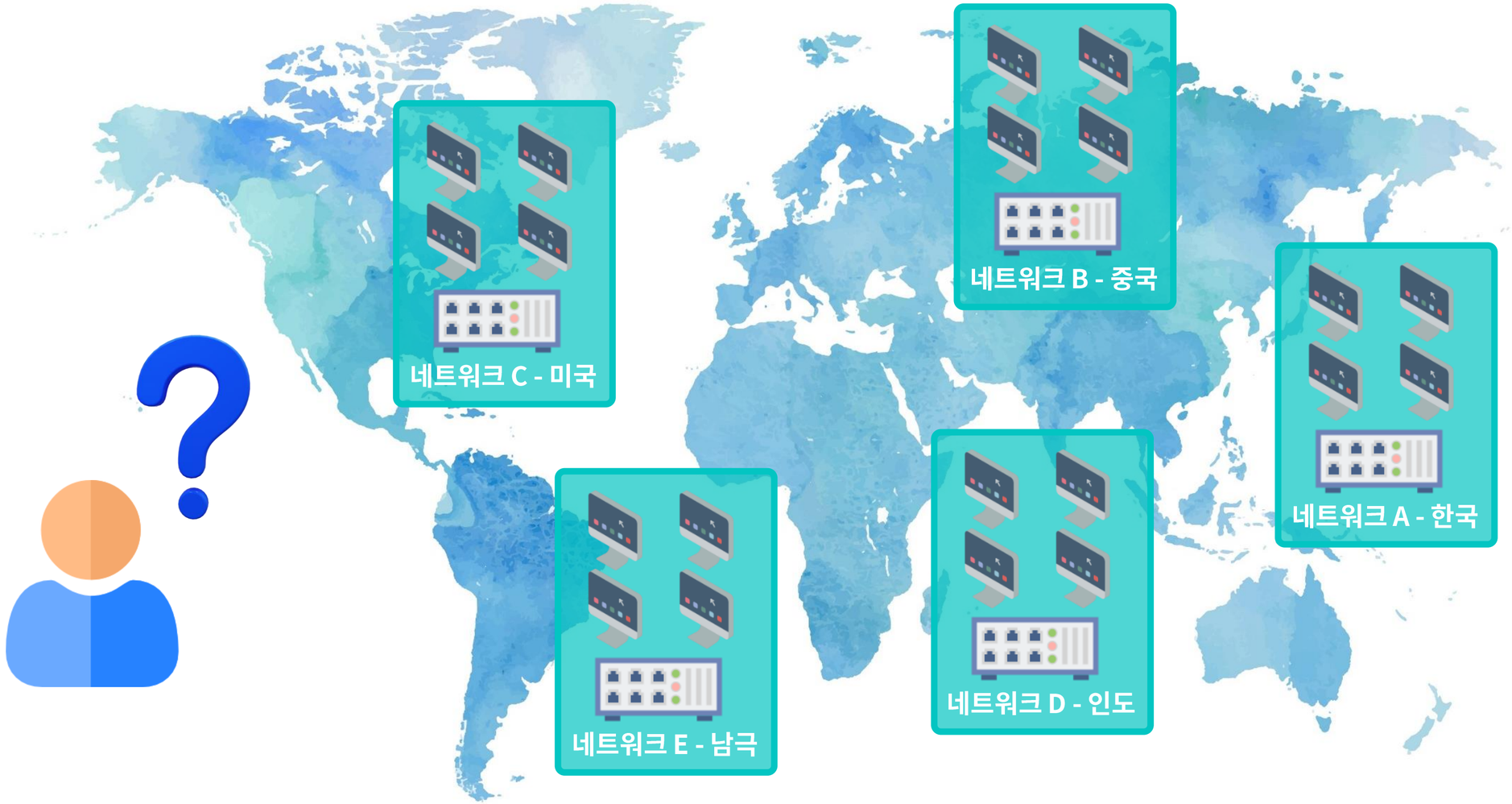
- 192.168.1.0 /24 = 255.255.255.0
- 10.1.0.0 /16 = 255.255.0.0
- 196.10.10.0/25 = 255.255.255.128

라우터 개요 및 특징

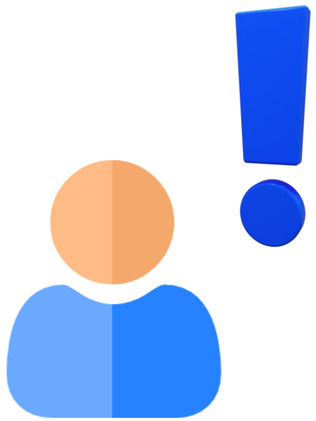
라우터

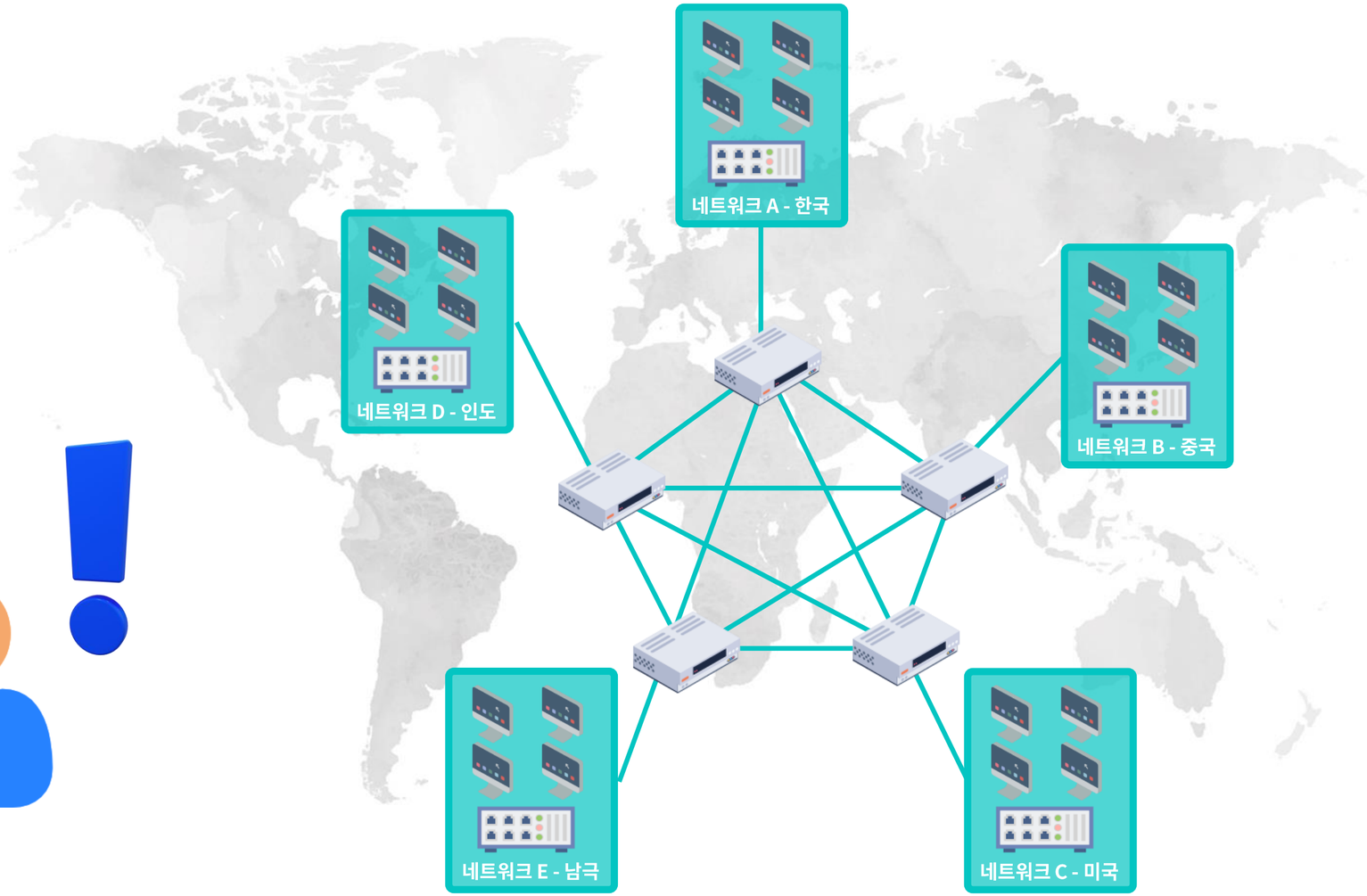
- IP 주소를 기반으로 라우팅을 하는 3계층 장비
- 라우팅은 최적의 경로를 선택하는 프로세스

서로 다른 네트워크 연결?



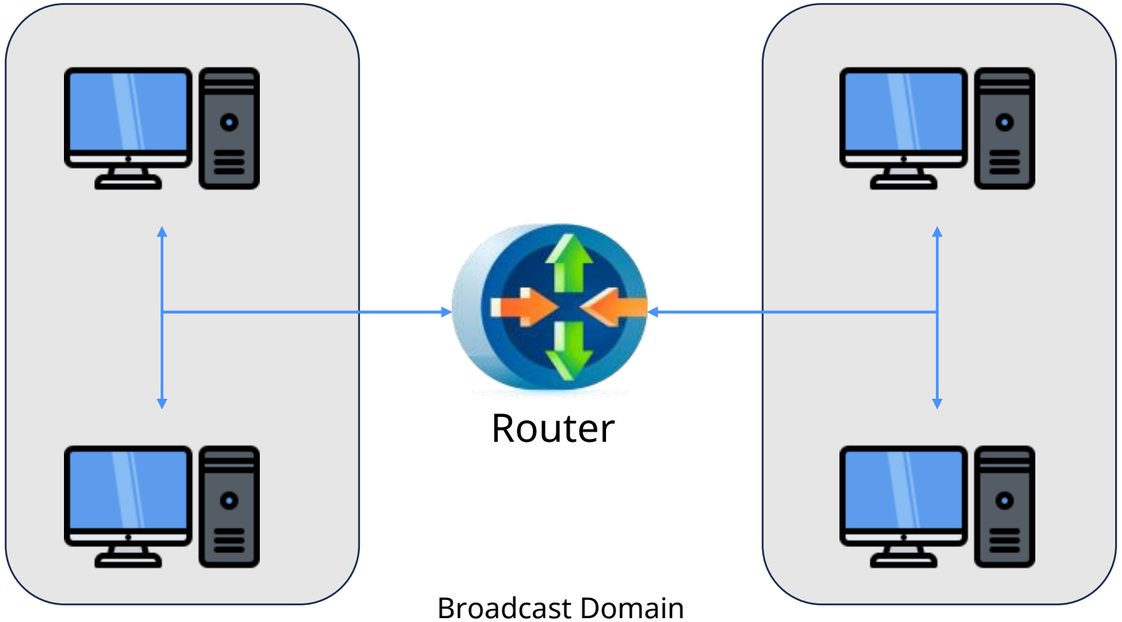
서로 다른 네트워크 연결!





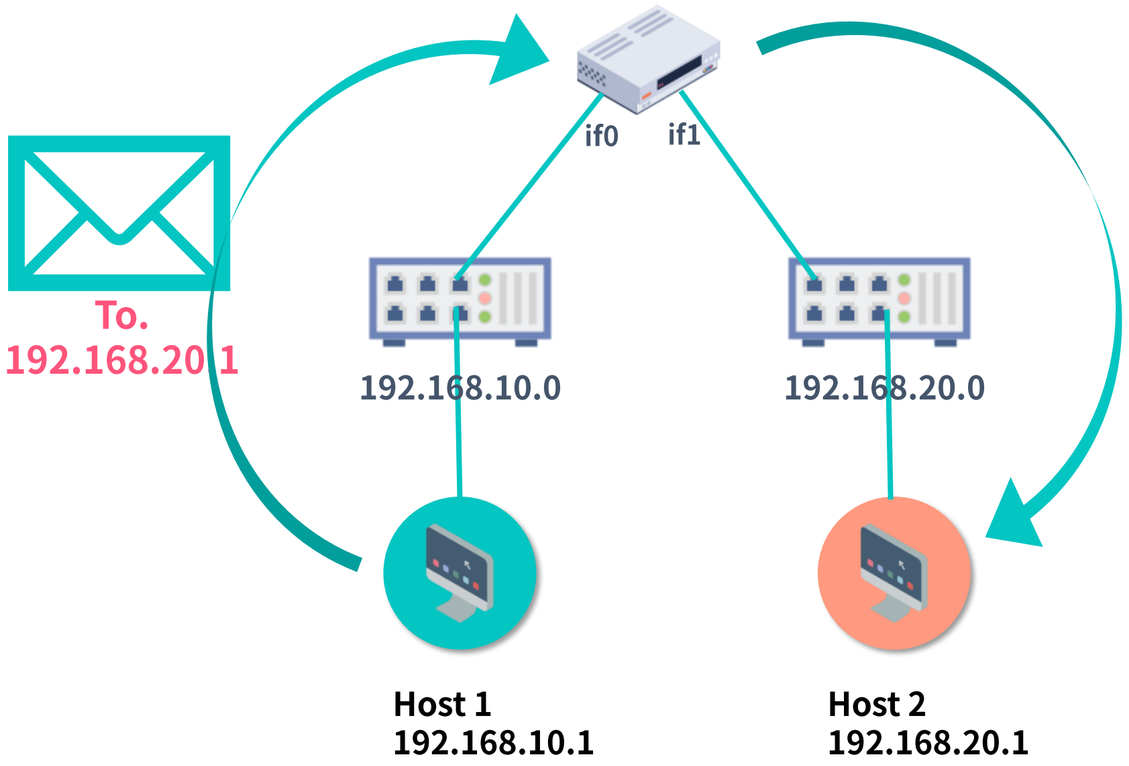
라우터 (Routers)

- 서로 다른 네트워크를 연결하는 데 사용됩니다.
- IP 주소를 사용하여 네트워크 간의 트래픽을 라우팅합니다.
- 라우팅 프로토콜을 통해 네트워크 간의 정보를 전달하기 위한 최적의 경로를 찾는 지능적인 결정을 내립니다.
- 브로드캐스트 도메인을 분할합니다.
- OSI 3계층 장치
    - 3계층 = 라우터
    - 2계층 = 스위치
    - 1계층 = 허브



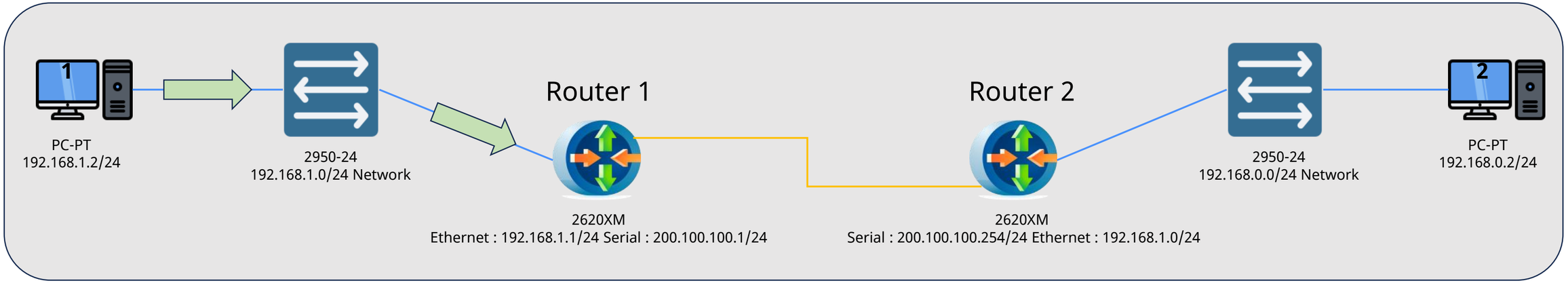
라우팅(Routing)

- 서로 다른 IP 네트워크 간에 패킷을 전달하는 프로세스
- 라우터는 라우팅 테이블에 저장된 정보를 사용하여 라우팅을 수행



if	Network
if0	192.168.10.0
if1	**192.168.20.0**

1단계 : 라우터 (Routers) 프로세스

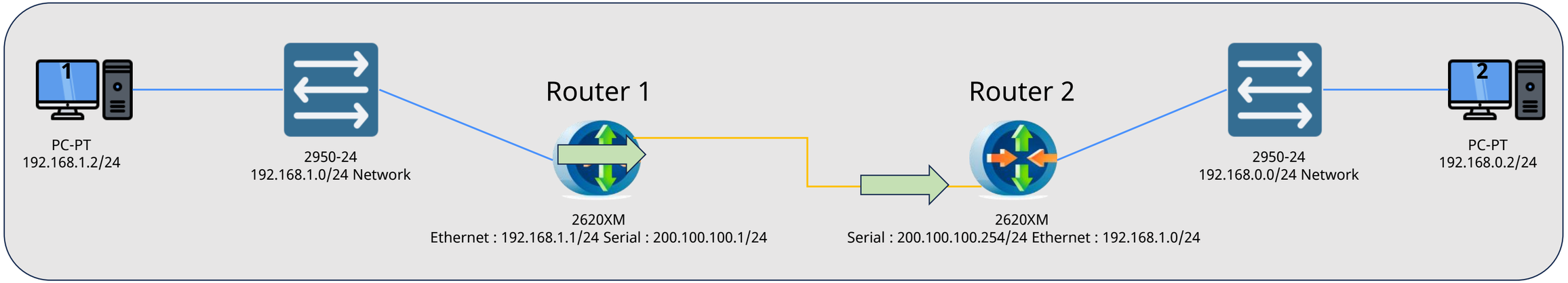


- PC 1은 PC 2로 향하는 패킷을 생성합니다.
  - 출발 IP: 192.168.1.2/24
  - 도착 IP: 192.168.0.2/24

- 패킷이 다른 네트워크로 가야 하기 때문에 PC 1의 기본 게이트웨이인 라우터 1의 이더넷 인터페이스(192.168.1.1/24)로 전송됩니다.

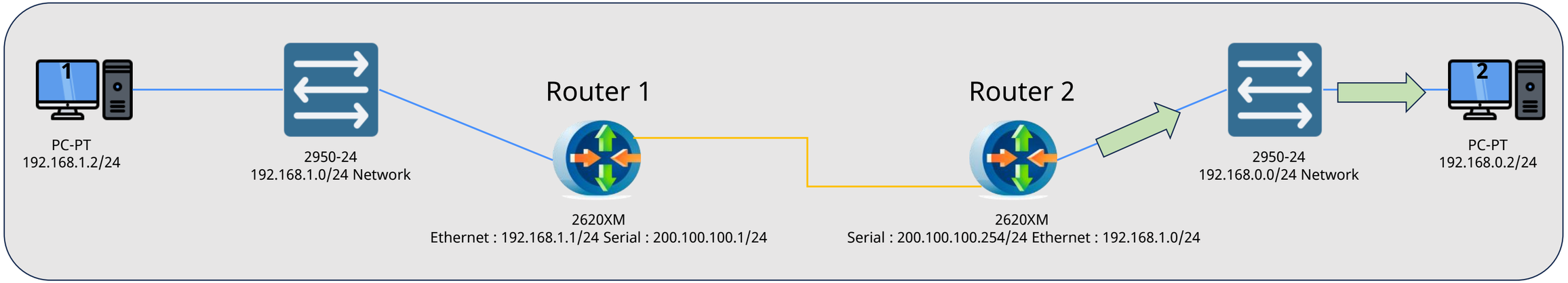
- PC 1이 라우터 1의 MAC 주소를 모르는 경우, ARP 요청을 통해 MAC 주소를 요청하게 됩니다.

2단계 : 라우터 (Routers) 프로세스



- 라우터 1이 패킷을 받으면, 도착지 IP 주소를 확인한 후 라우팅 테이블을 참조하여 패킷을 어느 경로로 보낼지 결정합니다.
- 이 경우, 라우터 1의 시리얼 인터페이스 IP 주소는 200.100.100.1/24입니다.

3단계 : 라우터 (Routers) 프로세스



- 라우터 2가 패킷을 수신하면, 목적지 IP 주소를 확인하고 라우팅 테이블을 바탕으로 전송할 경로를 결정합니다.
- 이 경우, 라우터 2의 직접 연결된 Ethernet 인터페이스는 192.168.0.1/24 IP 주소를 갖고 있습니다.

라우팅 테이블(Routing Table)

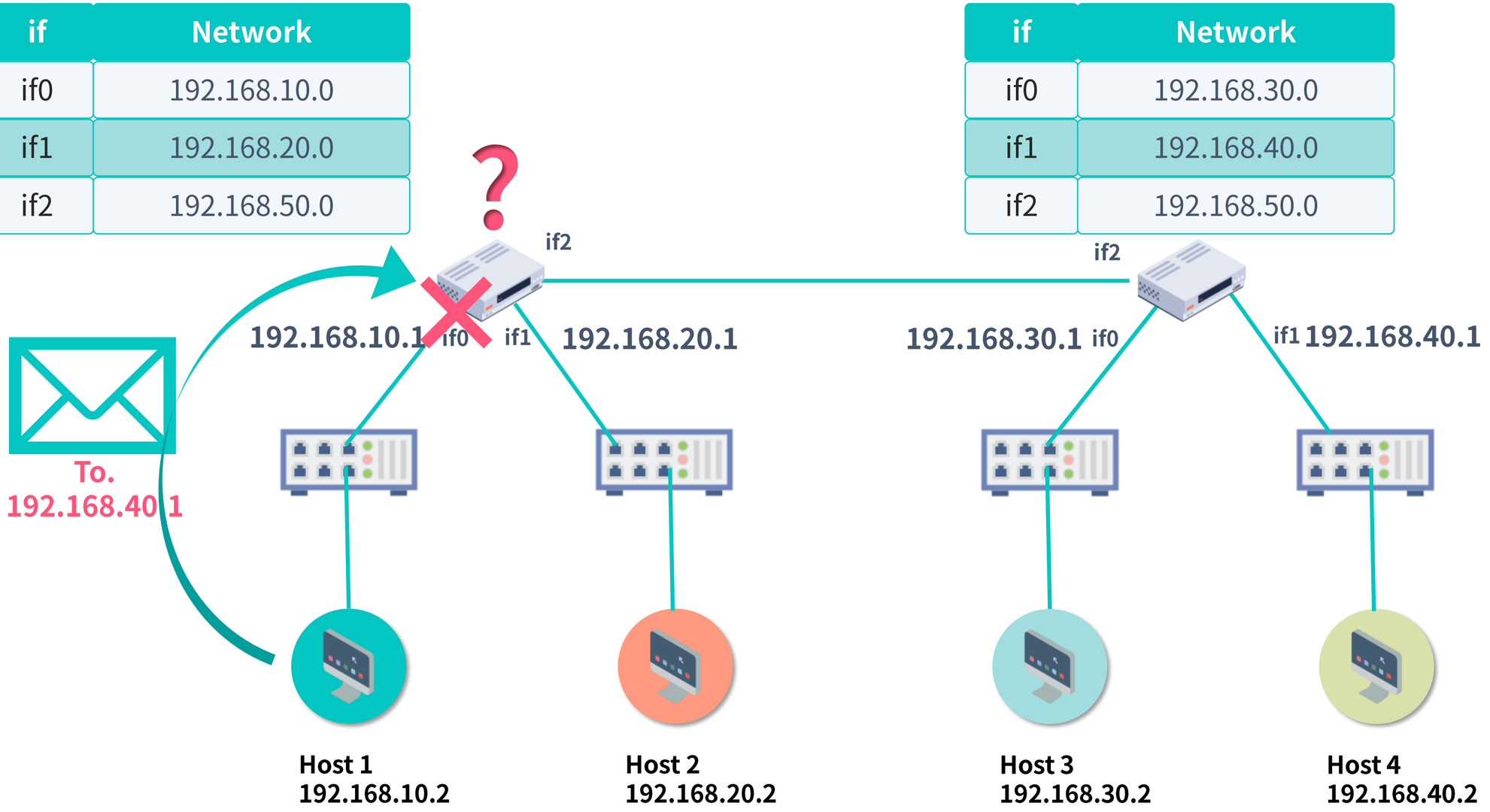
- 라우터가 라우팅을 할 때 사용하는 테이블

if	Network
if0	192.168.10.0
if1	192.168.20.0
if2	192.168.30.0
if3	192.168.40.0

라우터 동작 방식 – 대상 네트워크가 라우팅 테이블에 없는 경우

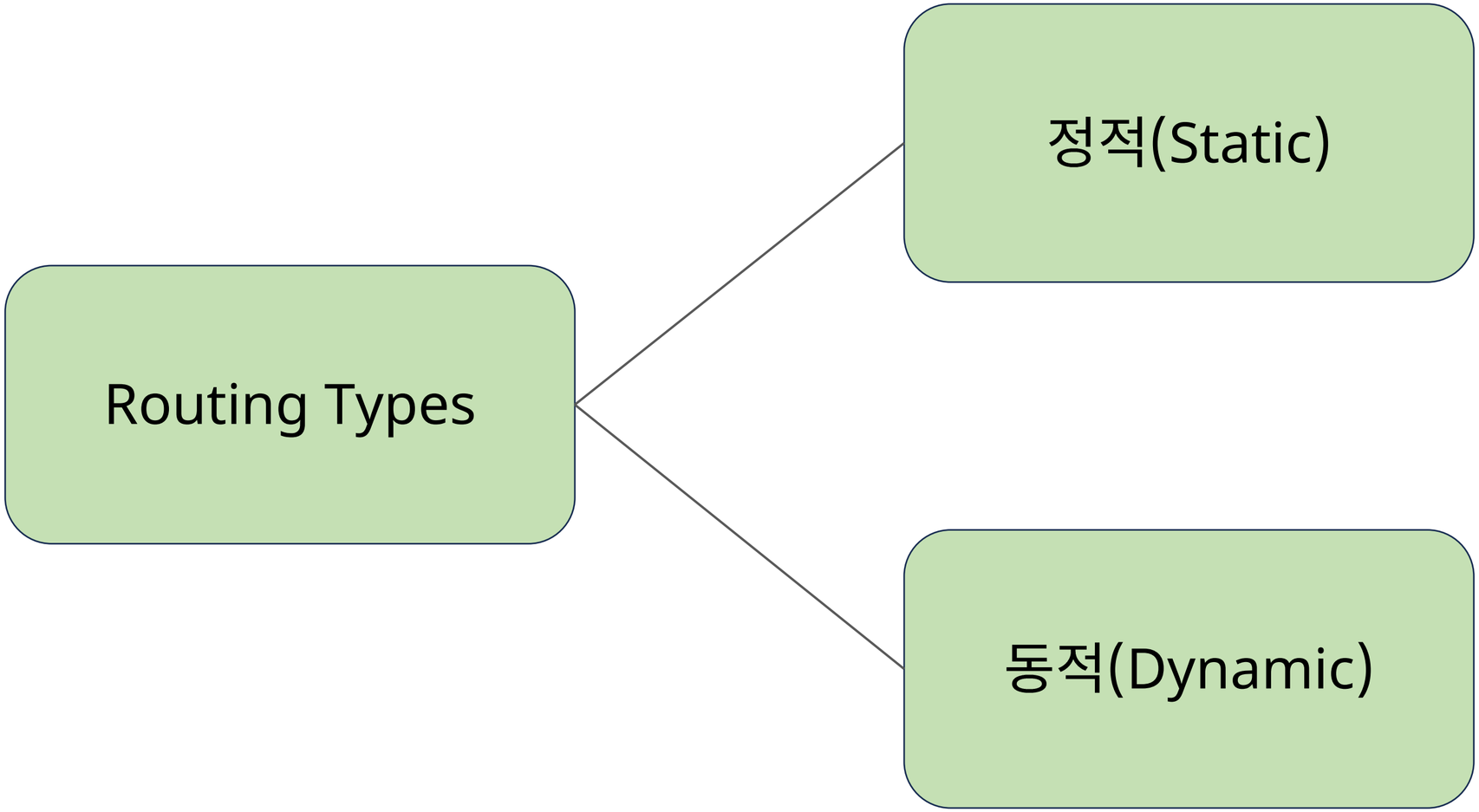
if	Network
if0	192.168.10.0
if1	192.168.20.0
if2	192.168.50.0

if	Network
if0	192.168.30.0
if1	192.168.40.0
if2	192.168.50.0



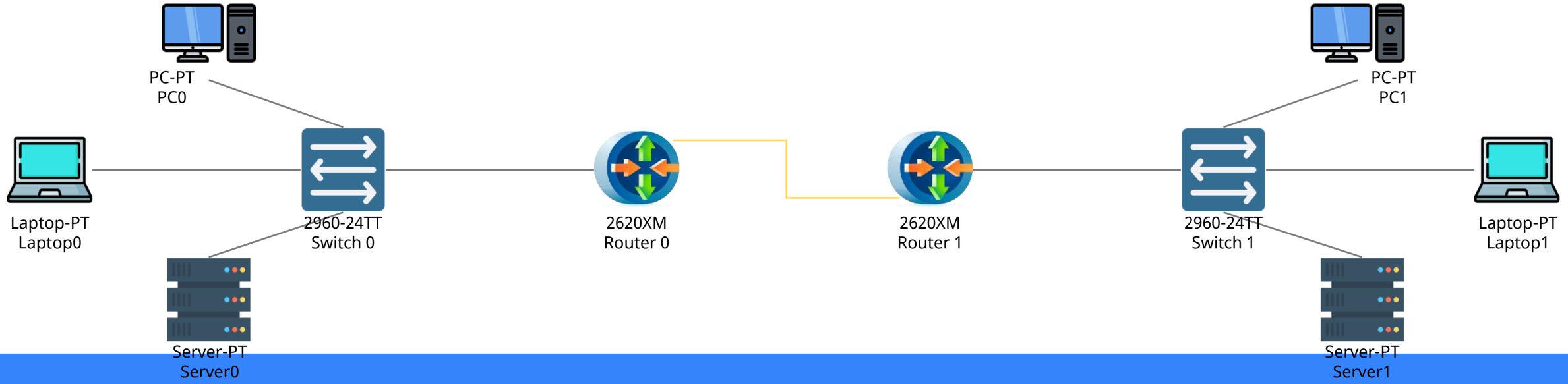
정적 vs. 동적 라우팅

- 라우팅은 두 가지 주요 범주로 나눌 수 있습니다:



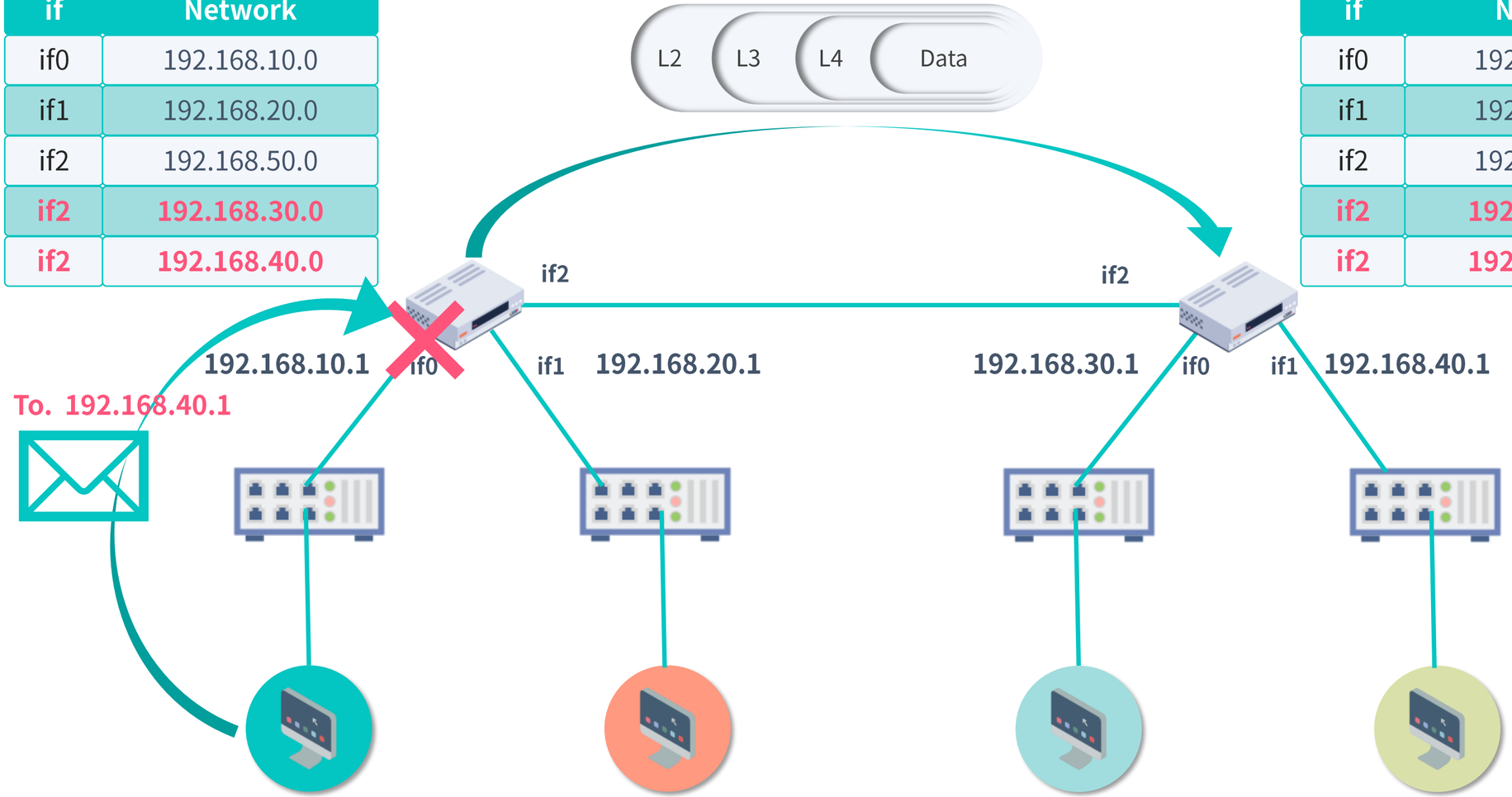
정적 라우팅

- 가장 간단한 형태의 라우팅
- 네트워크 관리자가 수동으로 입력한 정적 경로 사용
- 경로 변경이 거의 없는 소규모 네트워크에 이상적
    - 동적 라우팅처럼 부하가 없음
- 대규모 네트워크나 자주 변경되는 네트워크에서는 문제 발생 가능
    - 모든 변경 사항을 수동으로 적용해야 하므로 시간 소모가 크고 오류가 발생할 수 있음



라우터 동작 방식 – 대상 네트워크가 라우팅 테이블에 있는 경우

if	Network
if0	192.168.10.0
if1	192.168.20.0
if2	192.168.50.0
if2	192.168.30.0
if2	192.168.40.0



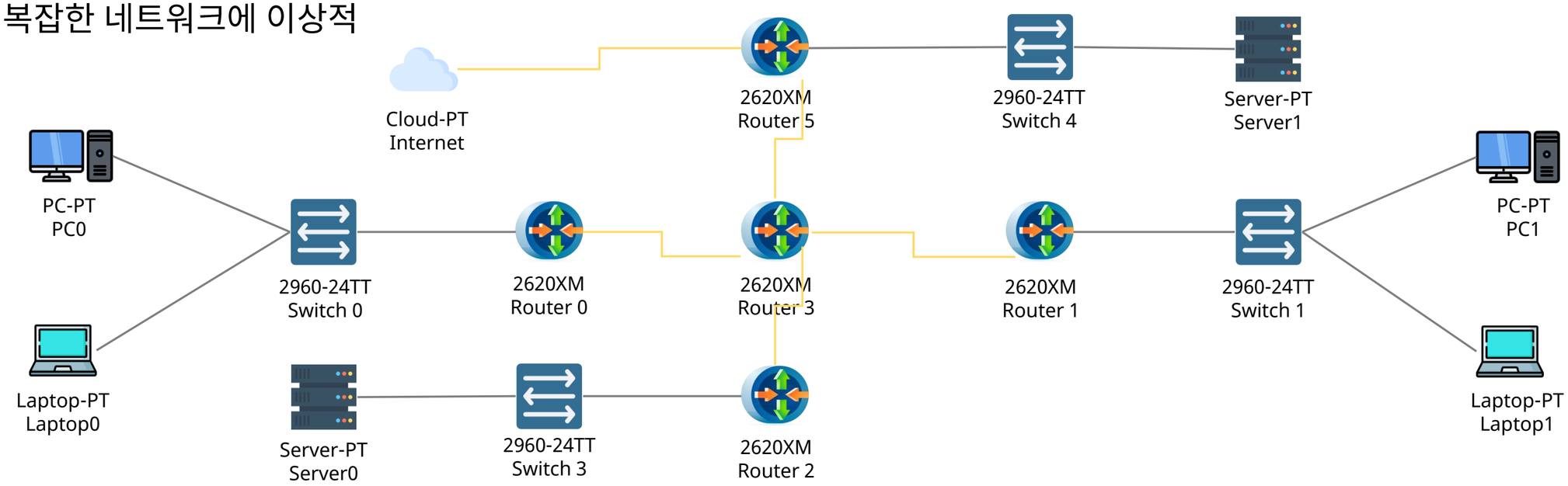
if	Network
if0	192.168.30.0
if1	192.168.40.0
if2	192.168.50.0
if2	192.168.10.0
if2	192.168.20.0

동적 라우팅

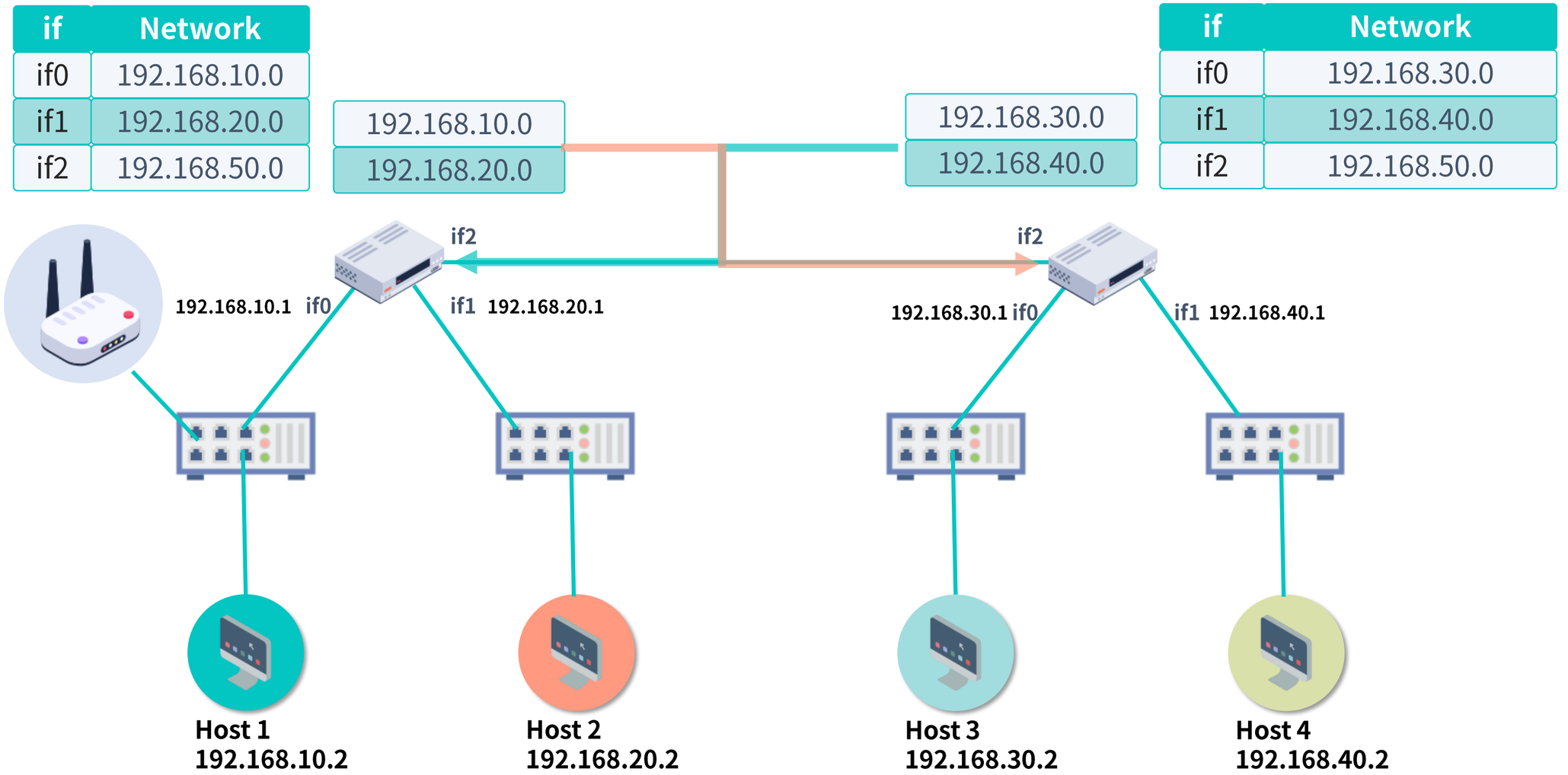
- 라우팅 프로토콜을 사용하여 자동으로 라우팅을 수행하는 방식
  - 라우터의 라우팅 테이블을 자동으로 채움
  - 가장 효율적인 라우팅 결정을 내림
  - 네트워크가 변경될 때마다 라우팅 테이블을 업데이트

- 자동화 및 비관리 방식
  - 모든 라우팅 결정이 프로토콜에 의해 처리됨

- 더 크고 복잡한 네트워크에 이상적

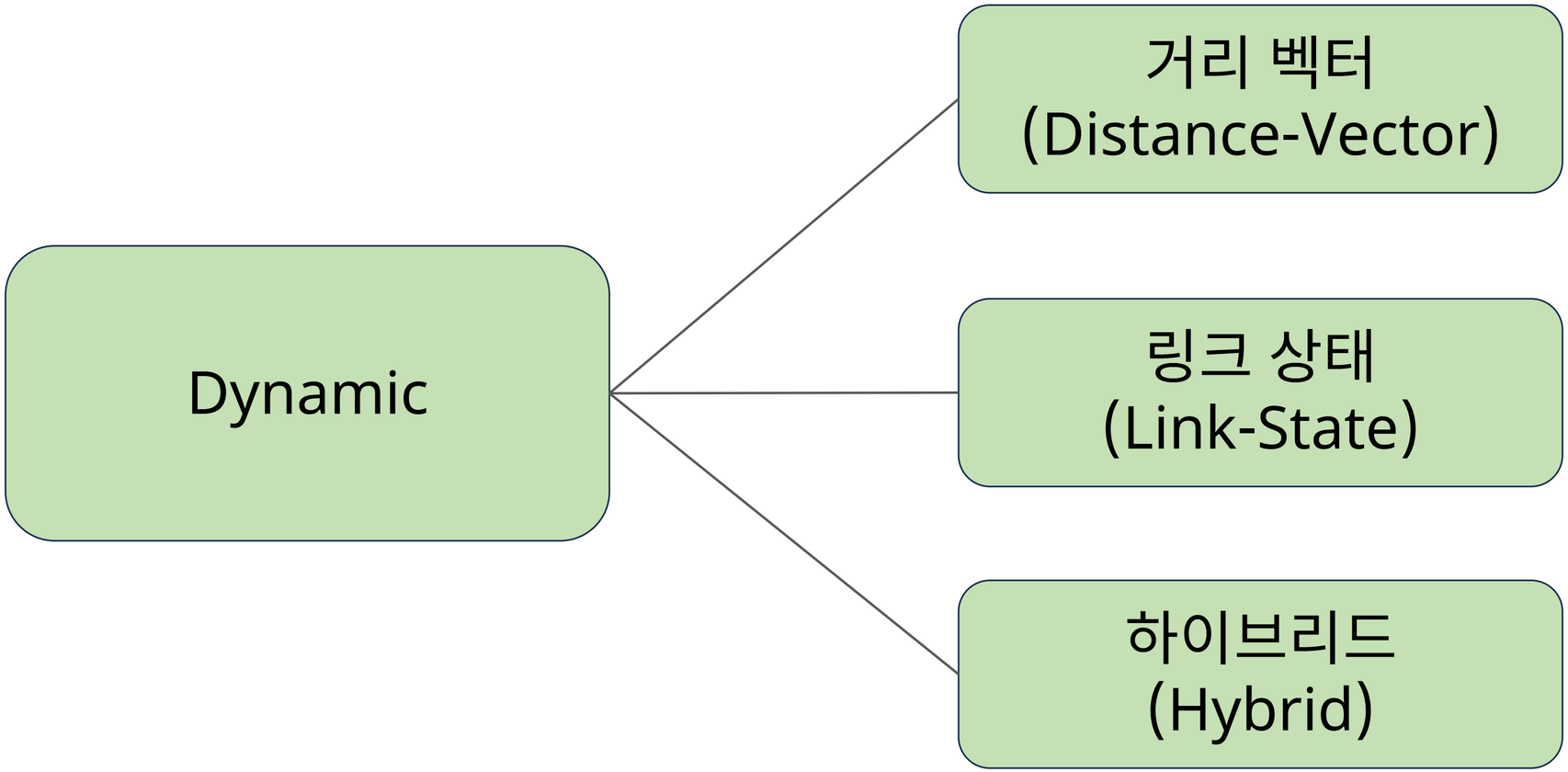


라우팅 테이블 업데이트


if
Network
if0
192.168.10.0
if1
192.168.20.0
if2
192.168.50.0
192.168.10.0
192.168.20.0
192.168.30.0
192.168.40.0
if
Network
if0
192.168.30.0
if1
192.168.40.0
if2
192.168.50.0
if2
if2
192.168.10.1
if0
if1
192.168.20.1
192.168.30.1
if0
if1
192.168.40.1
Host 1
192.168.10.2
Host 2
192.168.20.2
Host 3
192.168.30.2
Host 4
192.168.40.2

동적 라우팅 프로토콜의 유형

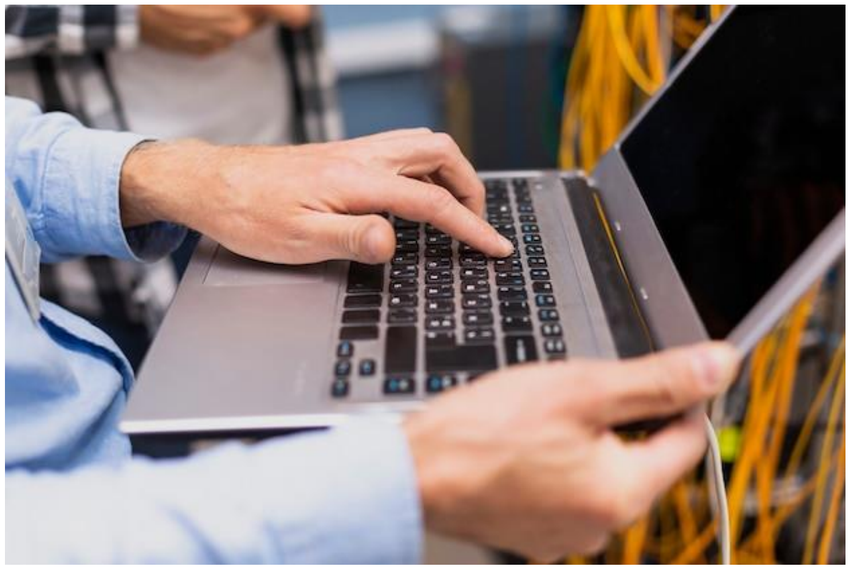
- 세 가지 유형의 동적 라우팅 프로토콜이 있으며, 이 섹션에서 자세히 다룰 예정입니다.



라우팅 테이블 업데이트 방식

- 정적 라우팅 (Static Routing)
  - 네트워크 관리자가 수동으로 라우팅 테이블에 경로를 설정
  - 변경사항에 따라 자동으로 업데이트 되지 않고, 수동에 의해서만 업데이트
  - 대규모 네트워크에는 설정이나 관리가 복잡

- 동적 라우팅 (Dynamic Routing)
  - 라우팅 프로토콜을 사용하여 네트워크 경로를 자동으로 학습하여 라우팅 테이블 업데이트
  - 라우터간 서로 라우팅 정보를 교환
  - 주요 라우팅 프로토콜 : RIP, OSPF, RIGRP 등



자동 IP 설정 기술

Static vs Dynamic IP 주소 할당

- 정적 (Static)
  - IP 주소가 수동으로 설정됩니다.
  - 변경되지 않습니다.
  - 주로 사용되는 경우:
    - DNS 서버
    - 웹 서버
    - 네트워크 프린터
    - 기본 게이트웨이(라우터)

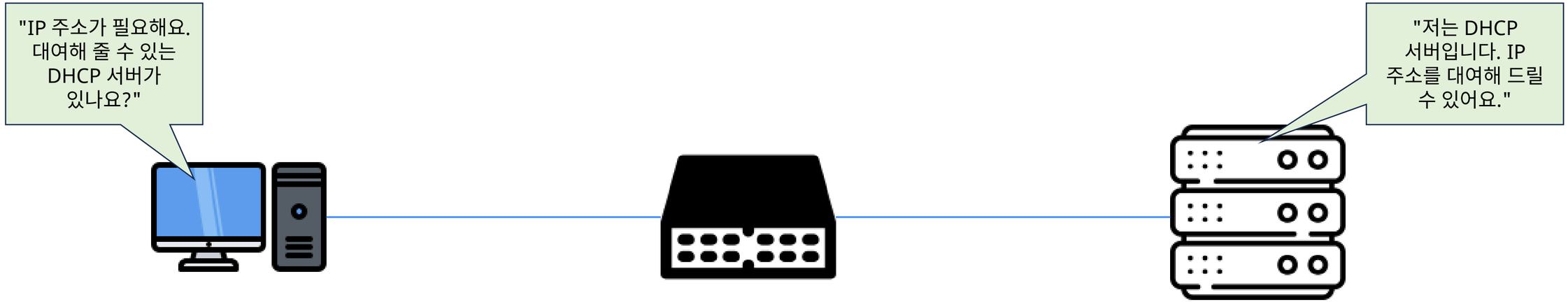
- 동적 (Dynamic)
  - IP 주소가 동적으로 설정됩니다.
    - DHCP 서버
    - APIPA
    - 상태 비저장 자동 구성
  - 주로 정적 IP 주소가 필요하지 않은 최종 사용자 장치에 사용됩니다.

IPv4 Dynamic IP 주소 할당

- 종류
  - Dynamic Host Configuration Protocol (DHCP)
  - Automatic Private IP Addressing (APIPA)

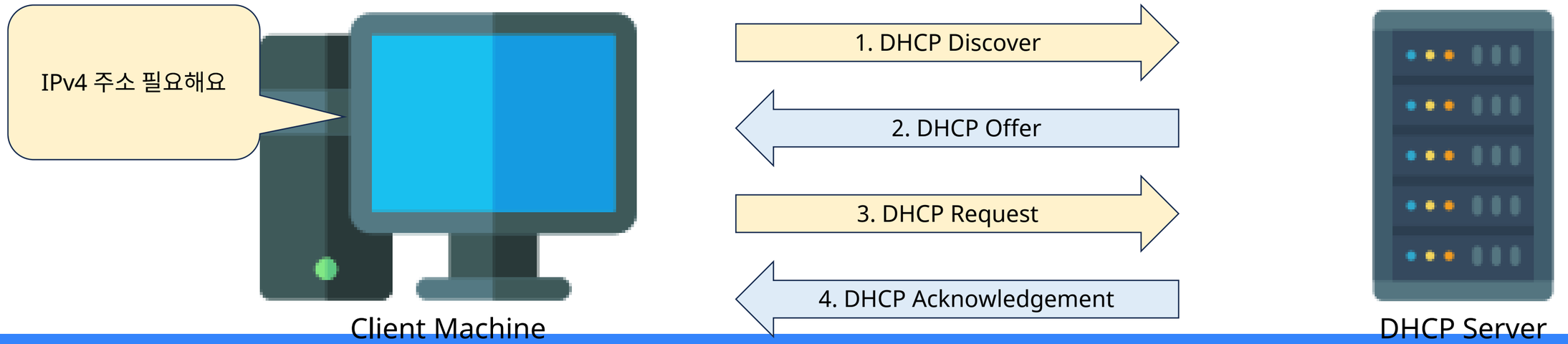
DHCP 서버

- 동적 호스트 구성 프로토콜(DHCP) 서버
- 호스트에 IP 주소를 자동으로 할당
- 네트워크 관리가 훨씬 쉬워
- 짐정적 IP 할당이 대안임
- DHCP에 대해서는 이후 과정에서 더 자세히 다룰 예정



DHCP DORA 프로세스 이해하기

1. 클라이언트가 로컬 서브넷에 "DHCP Discover" 메시지를 브로드캐스트하여 IP 주소를 요청합니다.
2. DHCP 서버가 요청을 받으면 IP 주소와 임대 정보를 포함한 "DHCP Offer" 메시지로 응답합니다.
3. DHCP 서버가 없을 경우, 클라이언트는 자동 사설 IP 주소 지정(APIPA) 대체 구성을 사용합니다.
4. 클라이언트는 "DHCP Offer"를 수락하고 DHCP 서버에 "DHCP Request" 메시지로 응답합니다.
5. DHCP 서버는 클라이언트에게 주소를 할당하고 "DHCP Acknowledgement" 메시지로 응답하여 DHCP IP 주소 임대를 완료합니다.

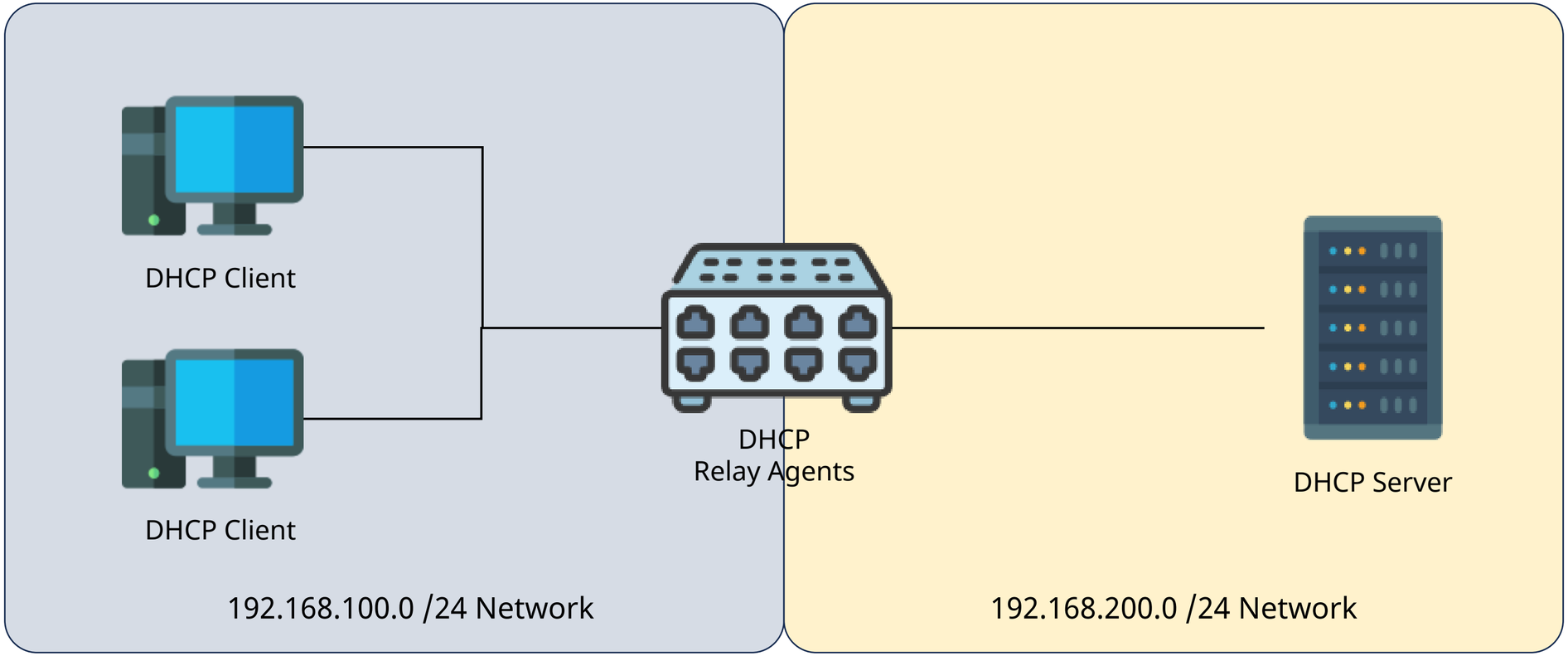


Additional DHCP Details

- DHCP를 구성할 때, 일반적으로 다음 항목을 구성할 수 있는 옵션이 제공됩니다:
    - IP 주소 범위 / 풀
    - 기본 게이트웨이 (라우터)
    - DNS 서버
    - IP 주소 제외 항목
    - MAC 주소 예약
    - 임대 기간

DHCP Relay Agents

- DHCP 서버가 다른 네트워크에 있을 때, DHCP 서버와 클라이언트 간의 DHCP 요청과 응답을 전달하는 시스템입니다.
- 이를 통해 각 네트워크에 DHCP 서버를 두지 않아도 됩니다.



Automatic Private IP Addressing (APIPA)

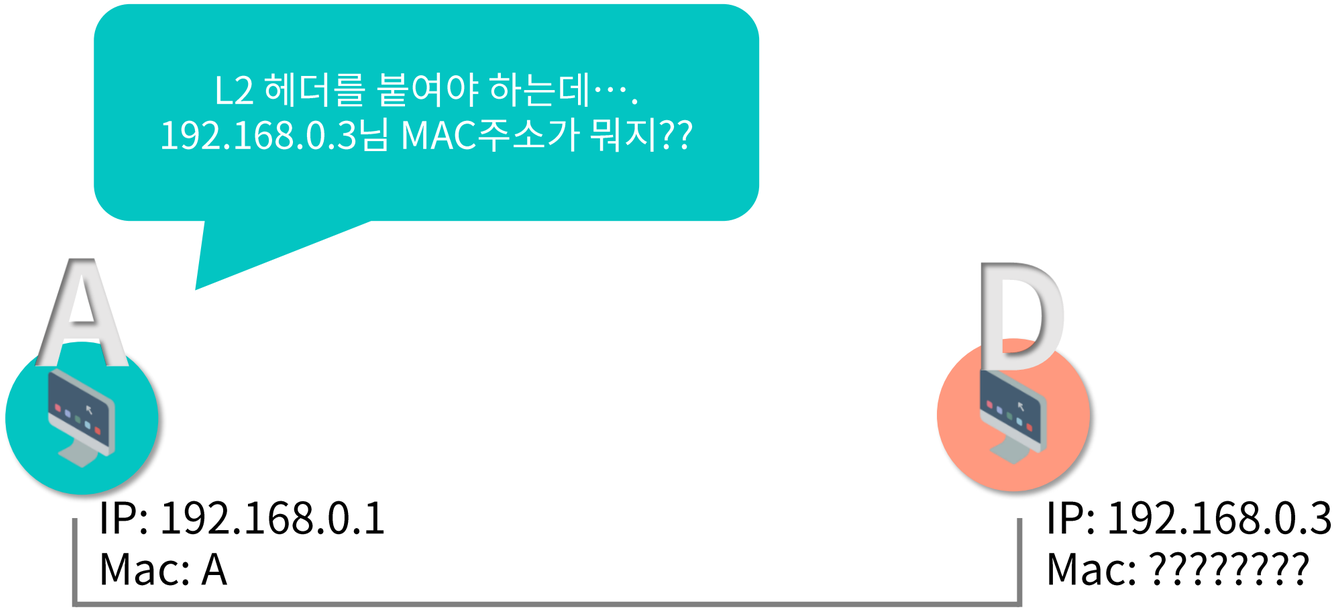
- Windows 운영 체제 기능
    - DHCP로 설정된 클라이언트가 네트워크에 DHCP 서버가 없을 경우, 스스로 IP 주소를 설정할 수 있게 합니다.
    - 만약 DHCP 서버가 IP 주소 요청에 응답하지 않으면, Windows 운영 체제가 APIPA IP 주소와 서브넷 마스크를 자동으로 설정할 수 있습니다.
        - 클래스 B IP 주소 범위: 169.254.0.1 ~ 169.254.255.254
        - 서브넷 마스크: 255.255.0.0

    - 같은 네트워크의 클라이언트들은 169.254.x.x 범위 내의 IP 주소를 스스로 할당하고 서로 통신할 수 있습니다.

- 참고: APIPA 주소는 링크 로컬 주소로, 라우팅되지 않습니다.

ARP(Address Resolution Protocol)

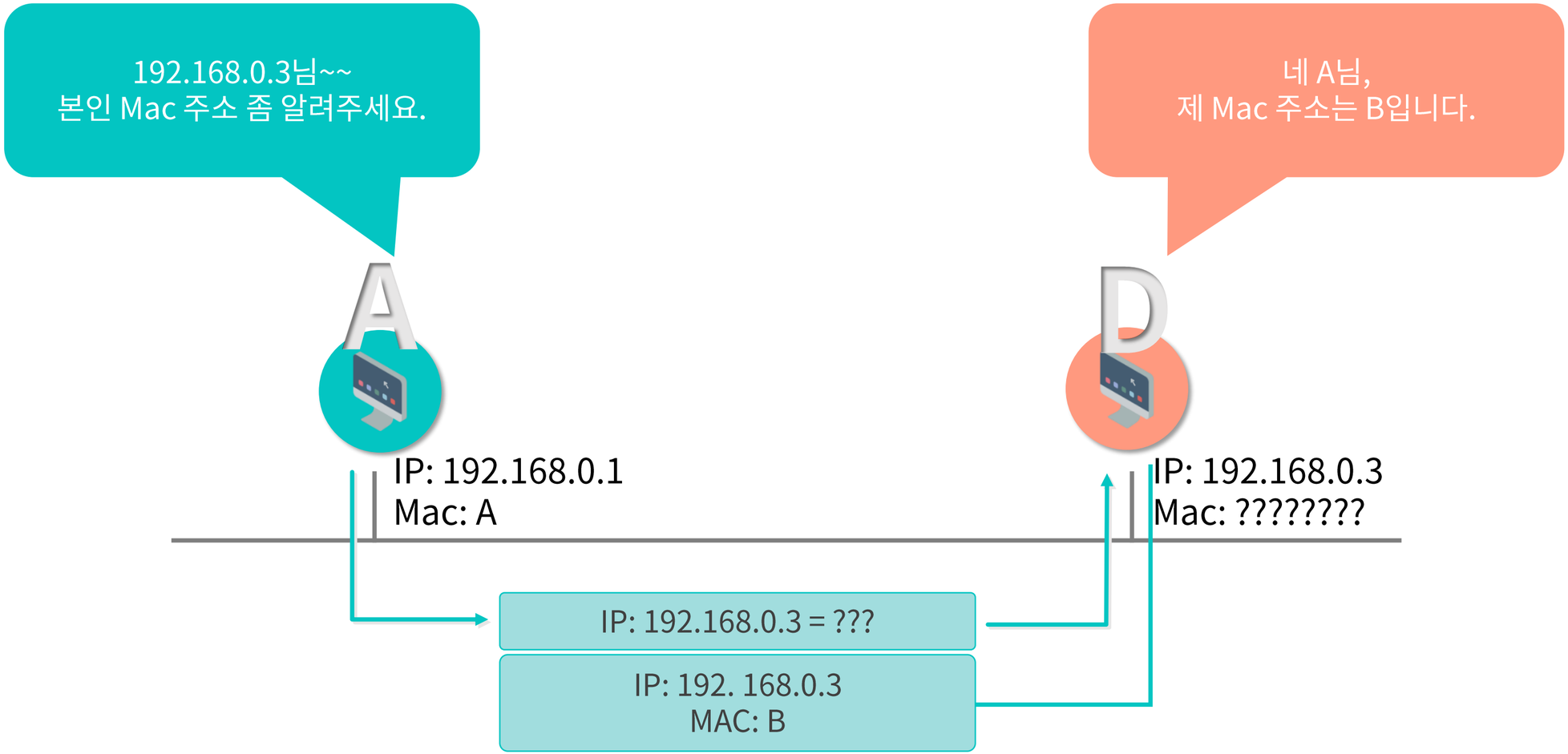
- IP 만 알고 있을 때 Mac 주소를 확인 할 수 있도록 해주는 프로토콜
  - 2계층 환경에서 사용하는 주소 = MAC address
  - 3계층 환경에서 사용하는 주소 = IP address



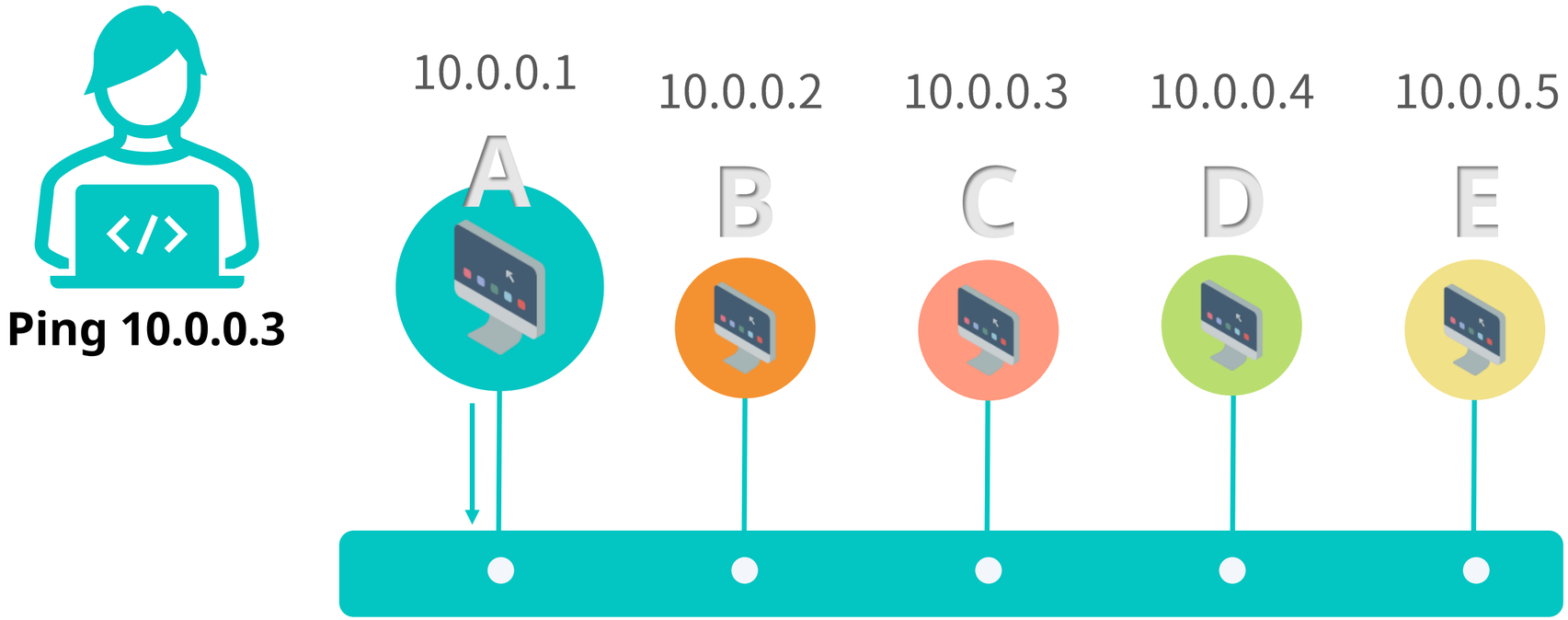
ARP 필요성

- IP 주소만으로는 데이터를, 네트워크 통해 전달 불가
- 데이터 링크 계층 (2계층) 에서는 패킷이 MAC 주소를 통해 전달되기에,
  ARP를 통해 IP주소를 MAC주소로 변환하는 과정이 필요

ARP(Address Resolution Protocol)

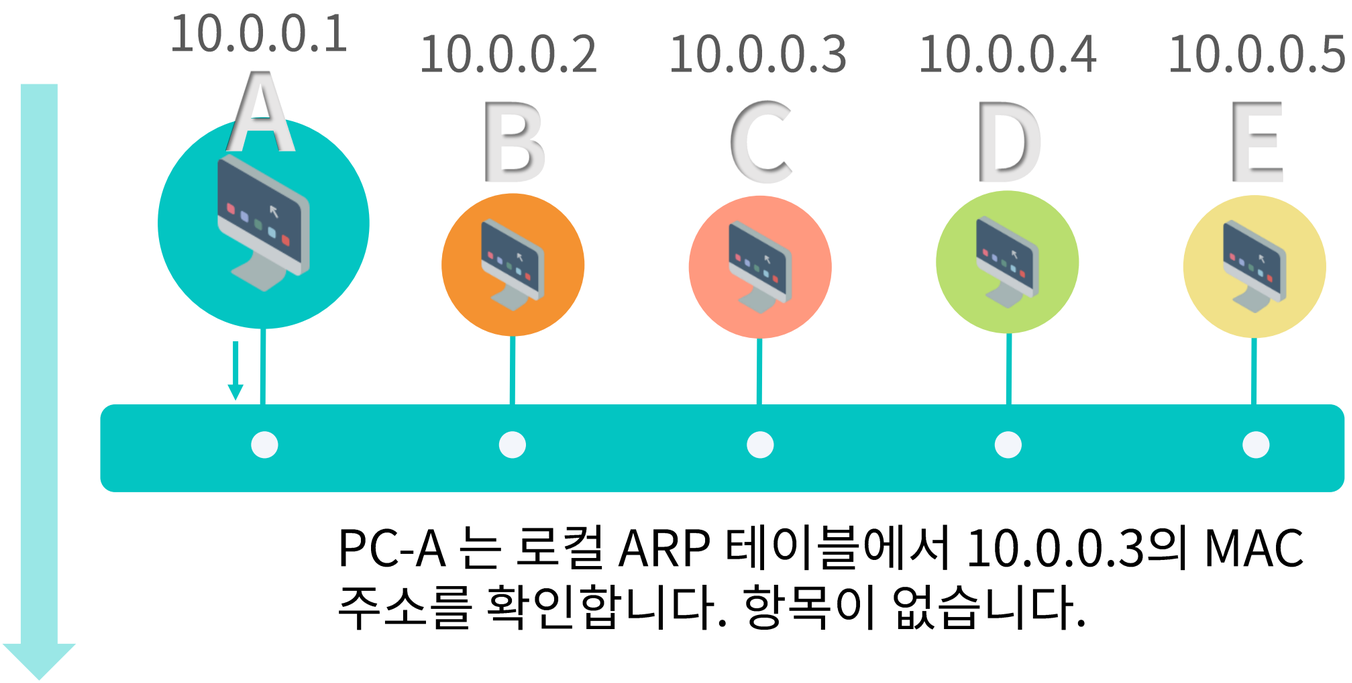


ARP 동작 방식 - ARP Request (1)



ARP는 요청 시 IP 주소와 데이터 링크 계층 주소 연결을 확인합니다.

ARP Request (2)

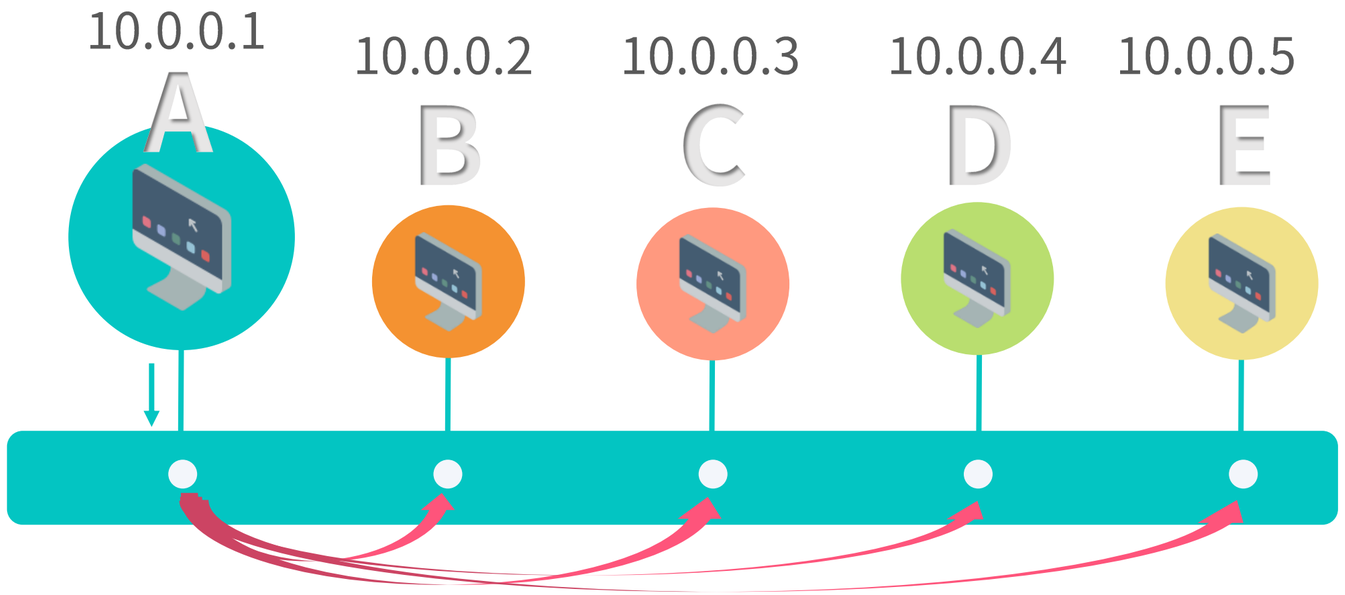


PC-A 는 로컬 ARP 테이블에서 10.0.0.3의 MAC 주소를 확인합니다. 항목이 없습니다.

PC-A ARP Table

IPv4 Address	MAC Address
10.0.0.1	0000:0000:AAAA
10.0.0.3	????

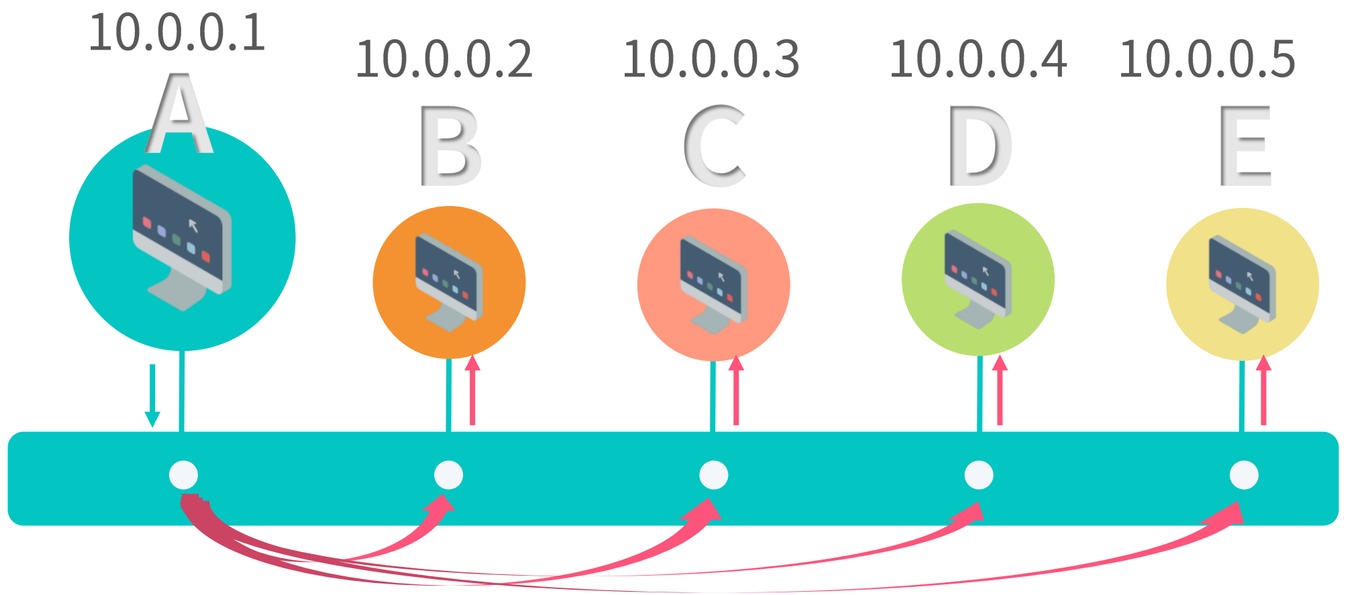
ARP Request (3)



PC-A는 이더넷 네트워크에 ARP 요청을 브로드캐스트합니다.

D MAC	S MAC	S IP	D IP	Payload
FFFF:FFFF:FFFF	0000:0000:AAAA	10.0.0.1	10.0.0.3	ARP request

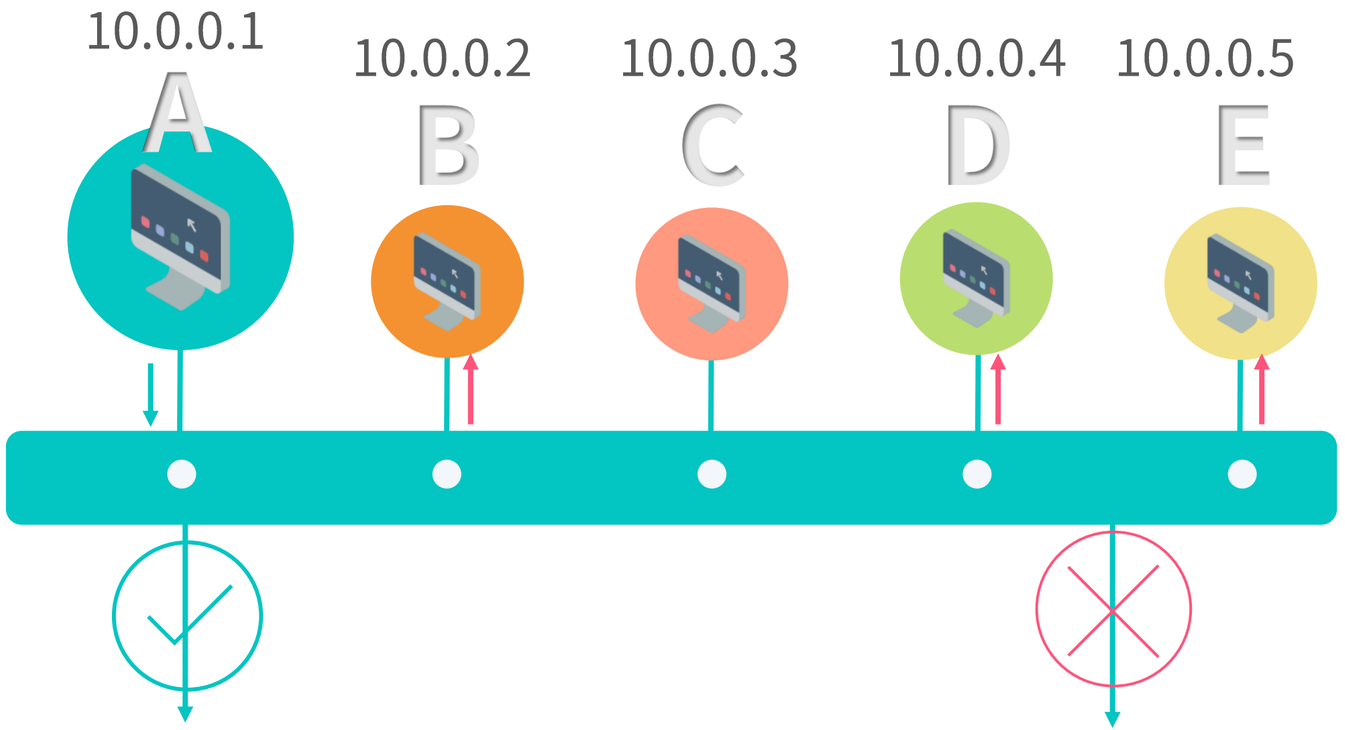
ARP Request (4)



모든 PC 들이 ARP 요청을 수신합니다.

D MAC	S MAC	S IP	D IP	Payload
FFFF:FFFF:FFFF	0000:0000:AAAA	10.0.0.1	10.0.0.3	ARP request

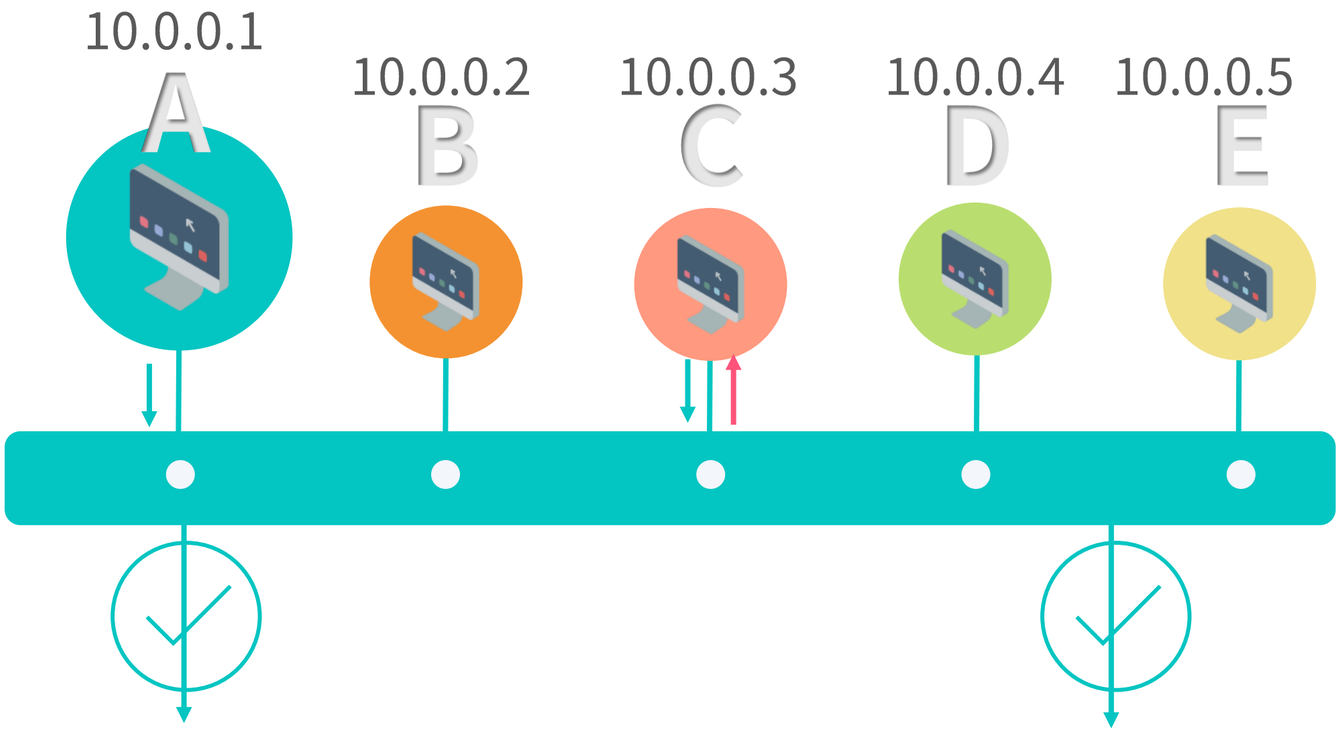
ARP Reply (1)



B,D,E는 목적지 IP 주소가
본인과 일치하지 않는 것을
확인 후 답변하지 않습니다.

D MAC	S MAC	S IP	D IP	Payload
FFFF:FFFF:FFFF	0000:0000:AAAA	10.0.0.1	10.0.0.3	ARP request

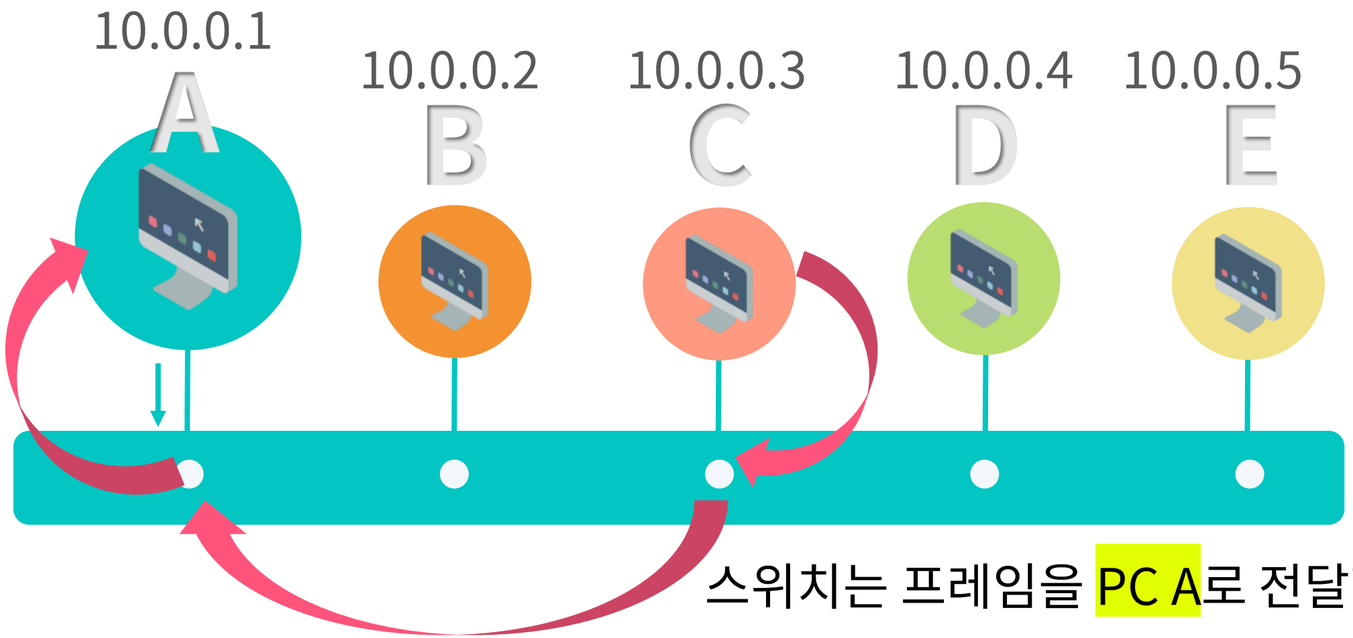
ARP Reply (2)



C는 목적지 IP 주소가 본인과 일치됨을 확인하고 응답합니다.

D MAC	S MAC	S IP	D IP	Payload
FFFF:FFFF:FFFF	0000:0000:AAAA	10.0.0.1	10.0.0.3	ARP request

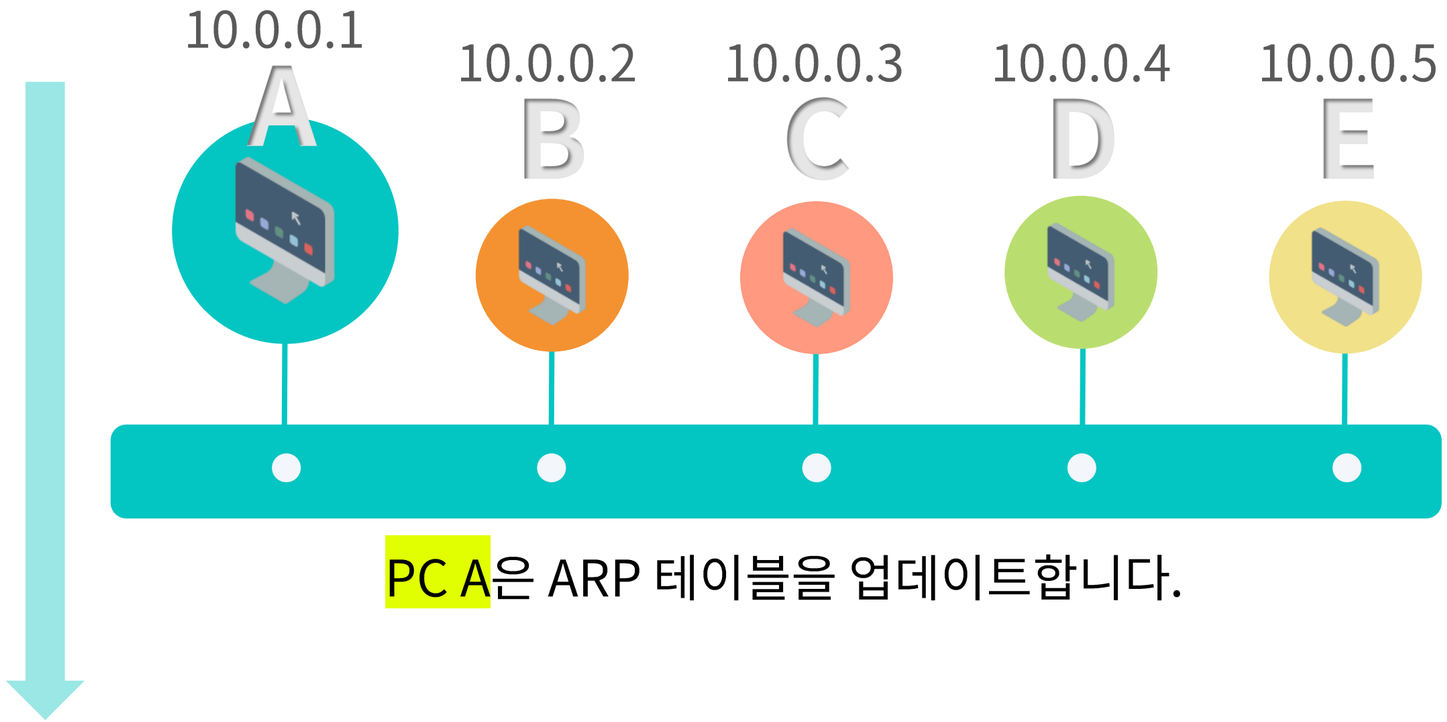
ARP Reply (3)



스위치는 프레임을 PC A로 전달합니다.

D MAC	S MAC	S IP	D IP	Payload
0000:0000:AAAA	0000:0000:CCCC	10.0.0.3	10.0.0.1	ARP reply

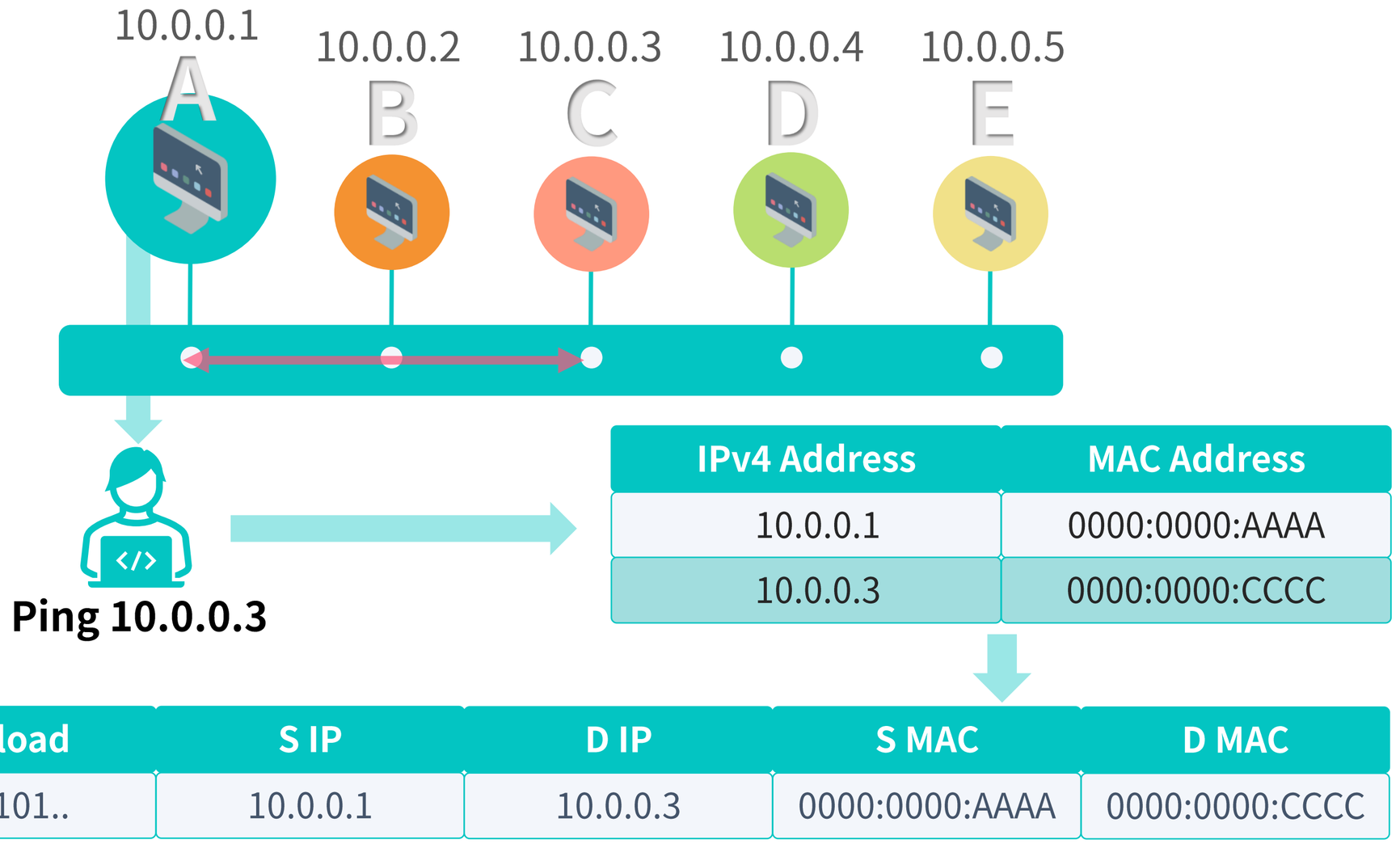
ARP 테이블 업데이트 완료



PC A은 ARP 테이블을 업데이트합니다.

IPv4 Address	MAC Address
10.0.0.1	0000:0000:AAAA
10.0.0.3	0000:0000:CCCC

실제 데이터 통신 시작


10.0.0.1
A
10.0.0.2
B
10.0.0.3
C
10.0.0.4
D
10.0.0.5
E
Ping 10.0.0.3
IPv4 Address
MAC Address
10.0.0.1
0000:0000:AAAA
10.0.0.3
0000:0000:CCCC
Payload
S IP
D IP
S MAC
D MAC
..10101..
10.0.0.1
10.0.0.3
0000:0000:AAAA
0000:0000:CCCC