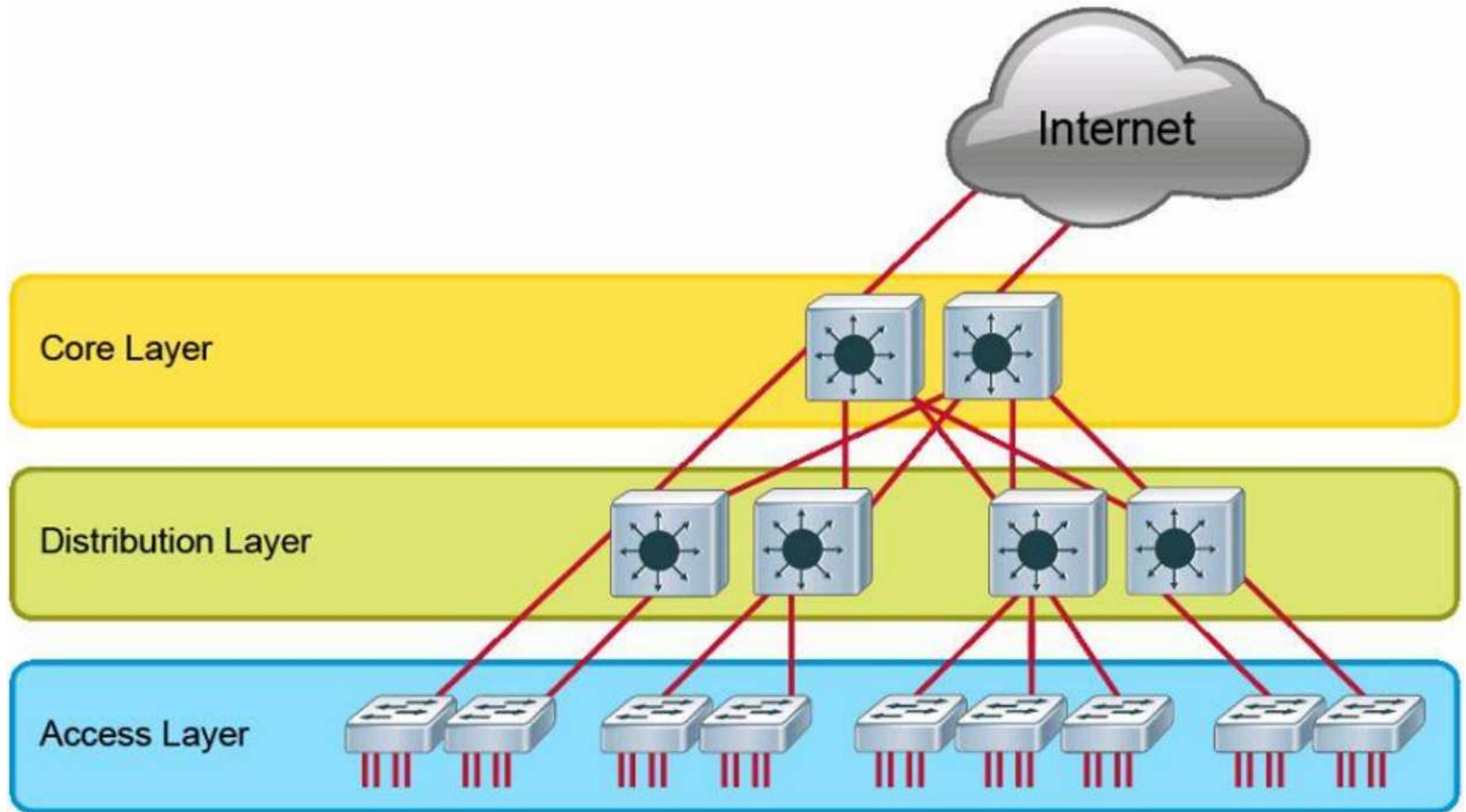

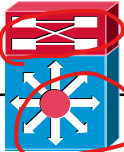
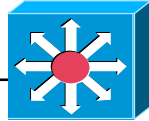



사내망 구성도



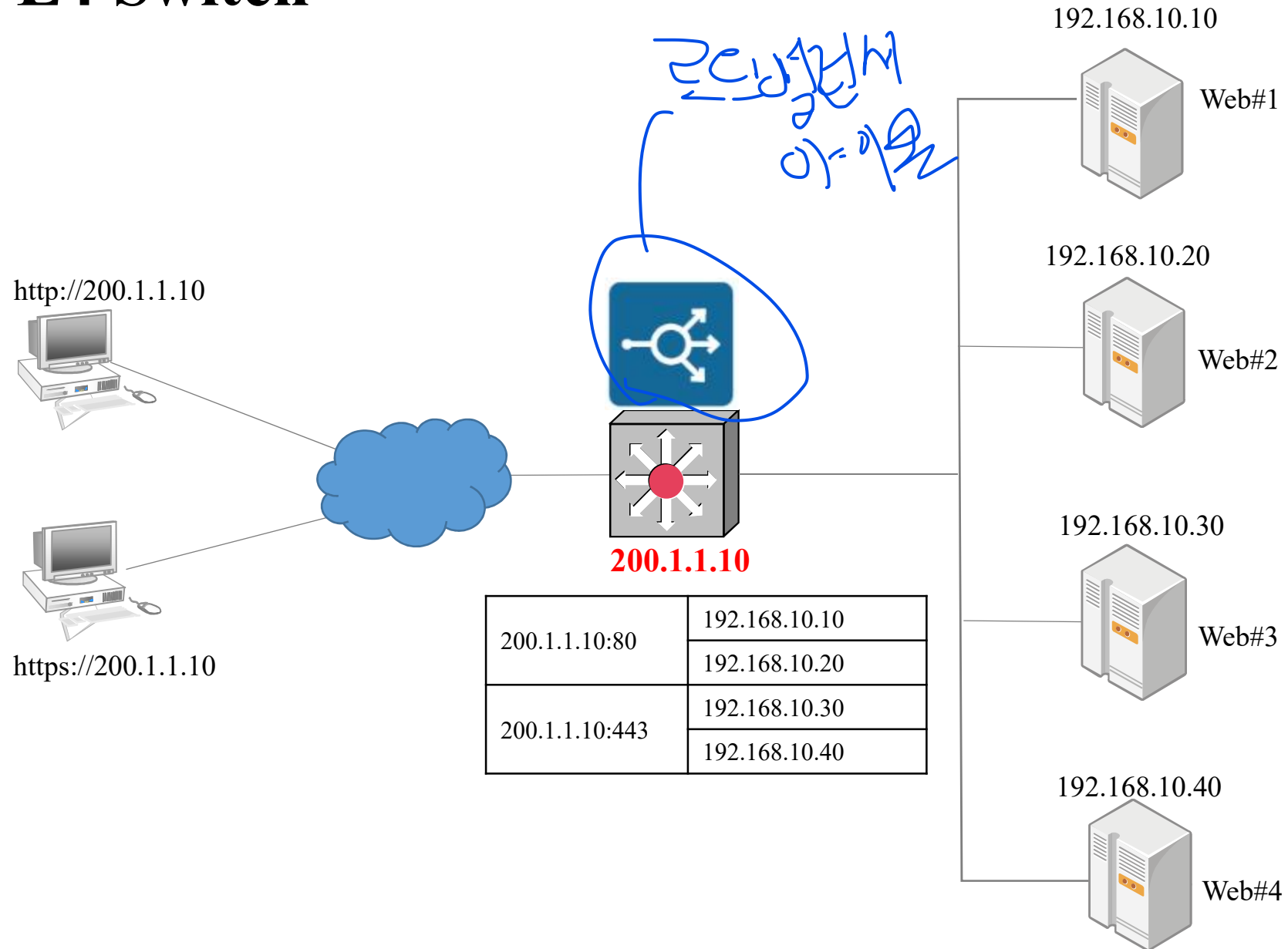
Multilayer Switch(다계층스위치)

구분	L2 Switch	L3 Switch	L4 Switch	L7 Switch
OSI 7계층	2계층 (MAC Address)	3계층 (Network 관리) <i>IP 관리</i>	4계층 (Session 관리) <i>IP + Port 관리</i>	7계층 (Content 관리) <i>IP + Port + Content</i>
기능	Switching Learning - Forwarding - Filtering 	Switching Routing 	L3 Switch Load Balance 	L4 Switch Security Content 인식 
주요 용도	Frame 전송	Packet 전송	FLB SLB	FLB SLB Security

*Server L3
Firewall L3*

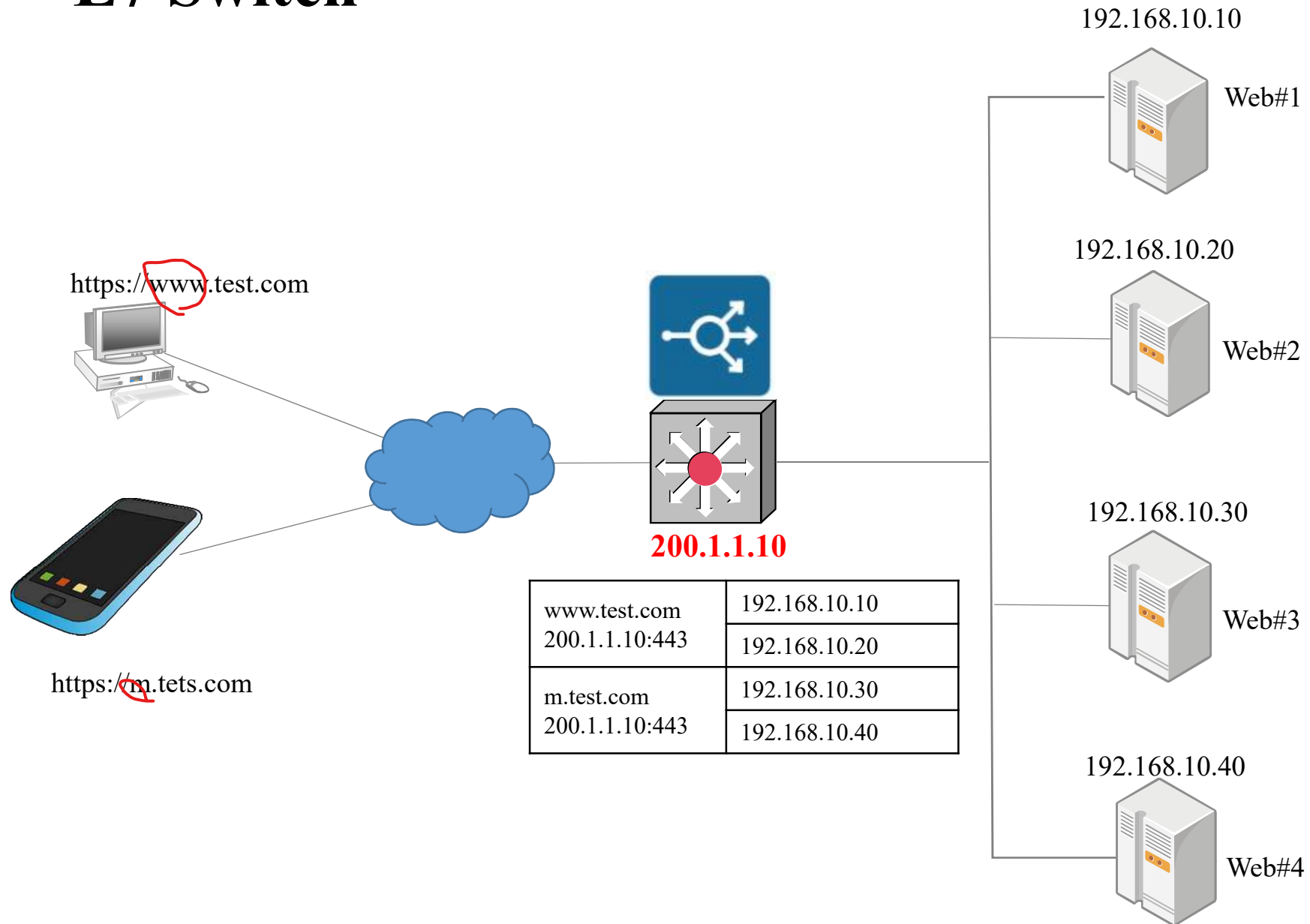
*2계층, 3계층: 동적 능력에
2차*

L4 Switch

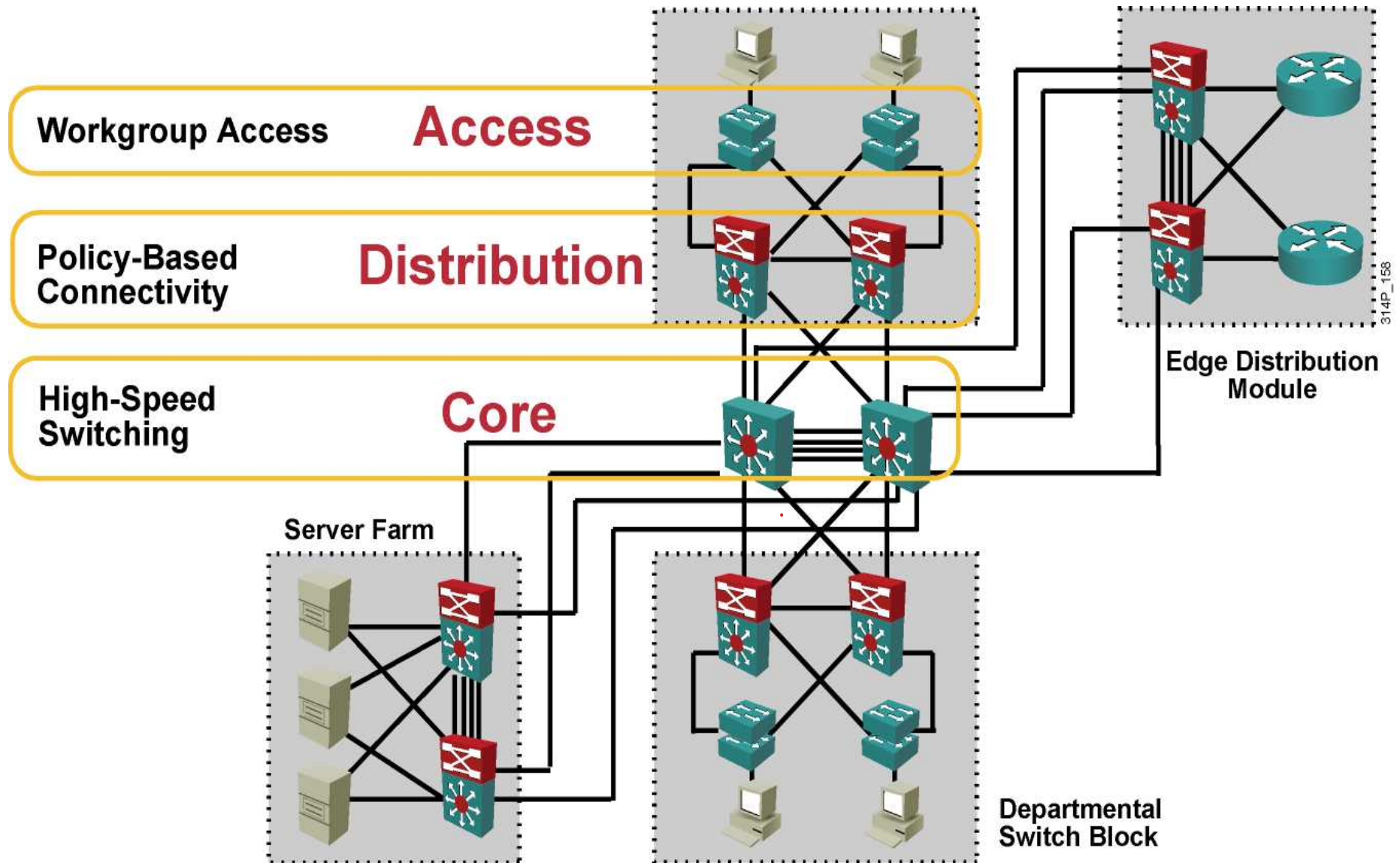


L7 Switch

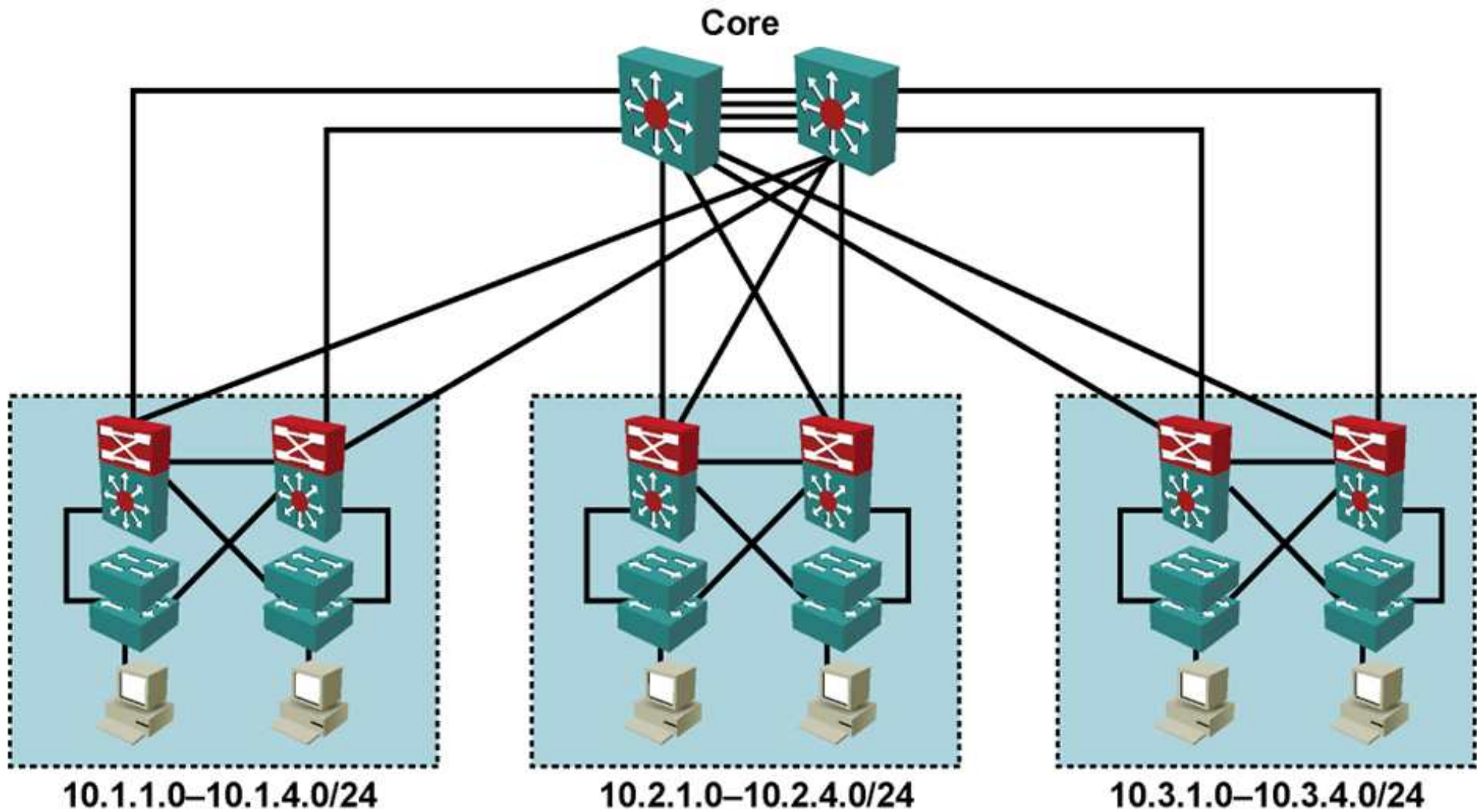
data



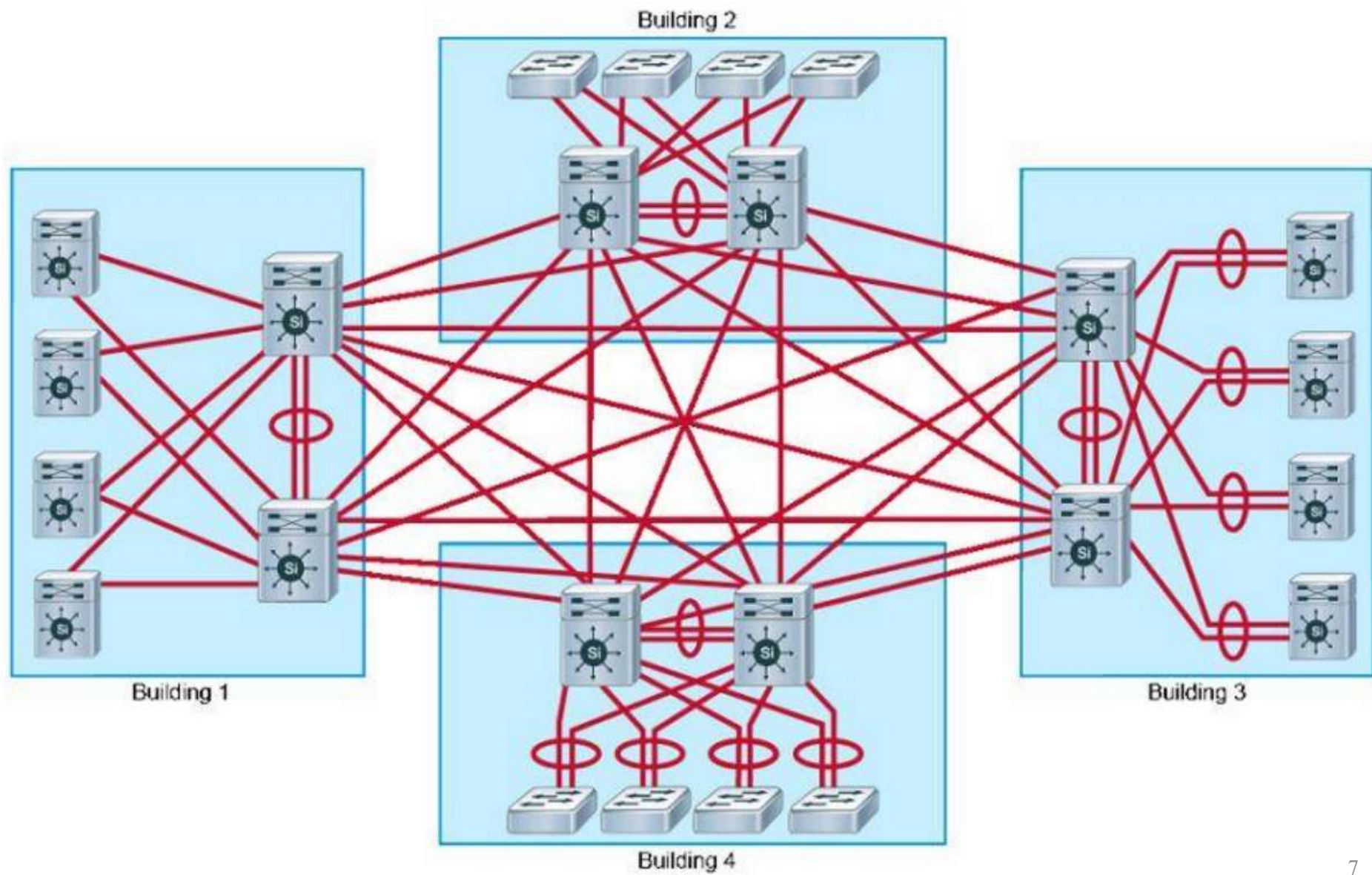
1 구성도



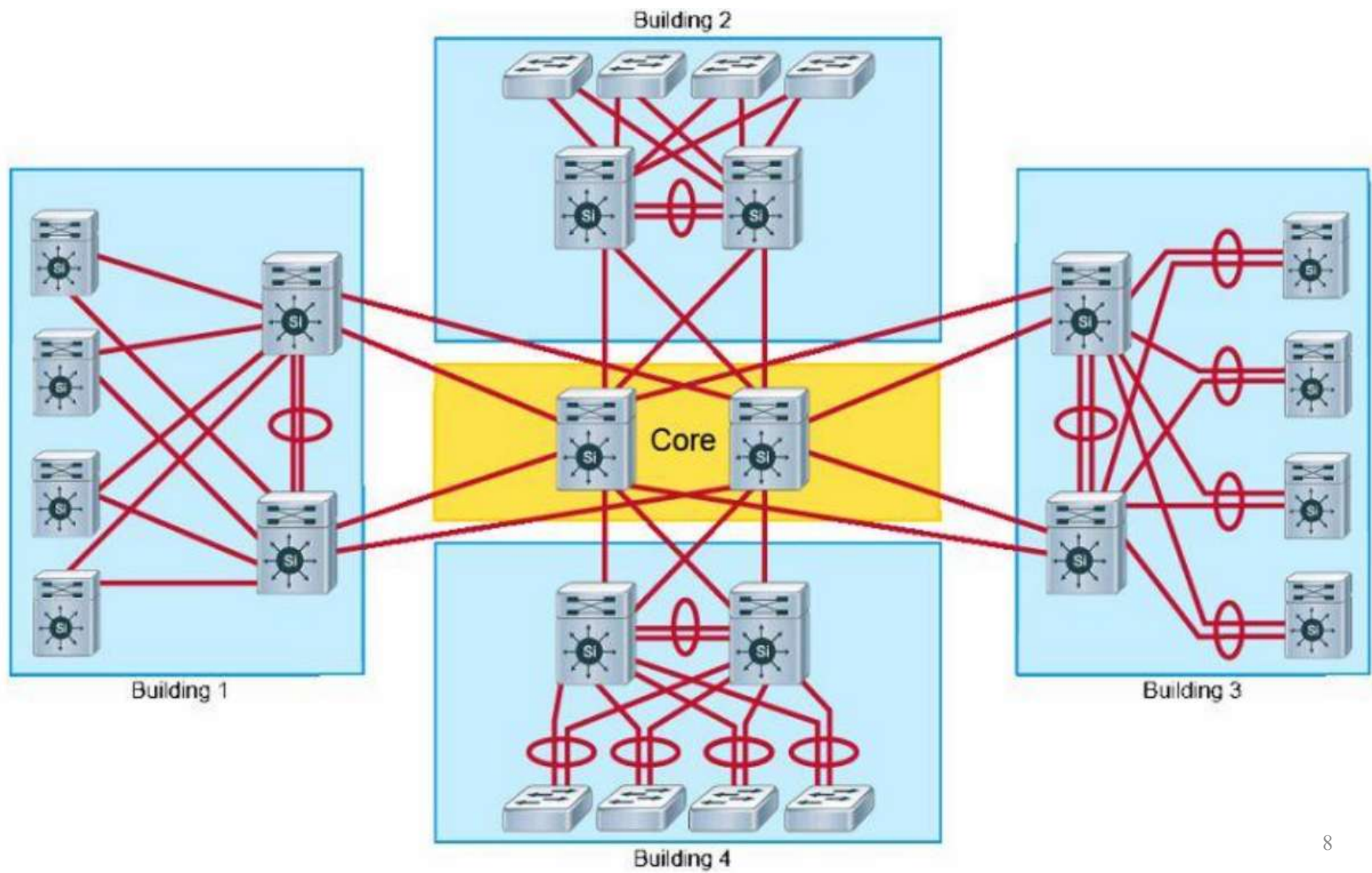
② 구성도



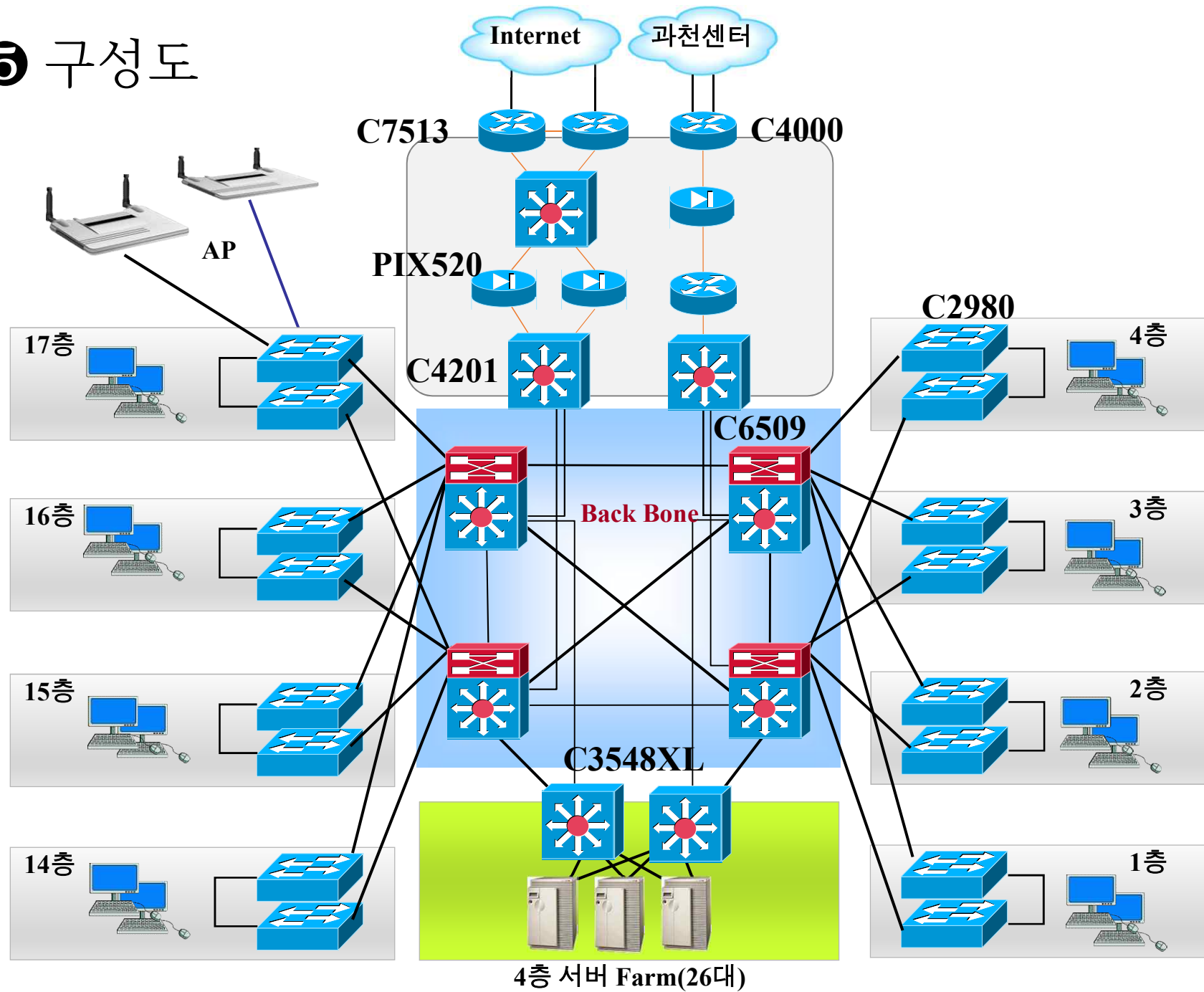
③ 구성도



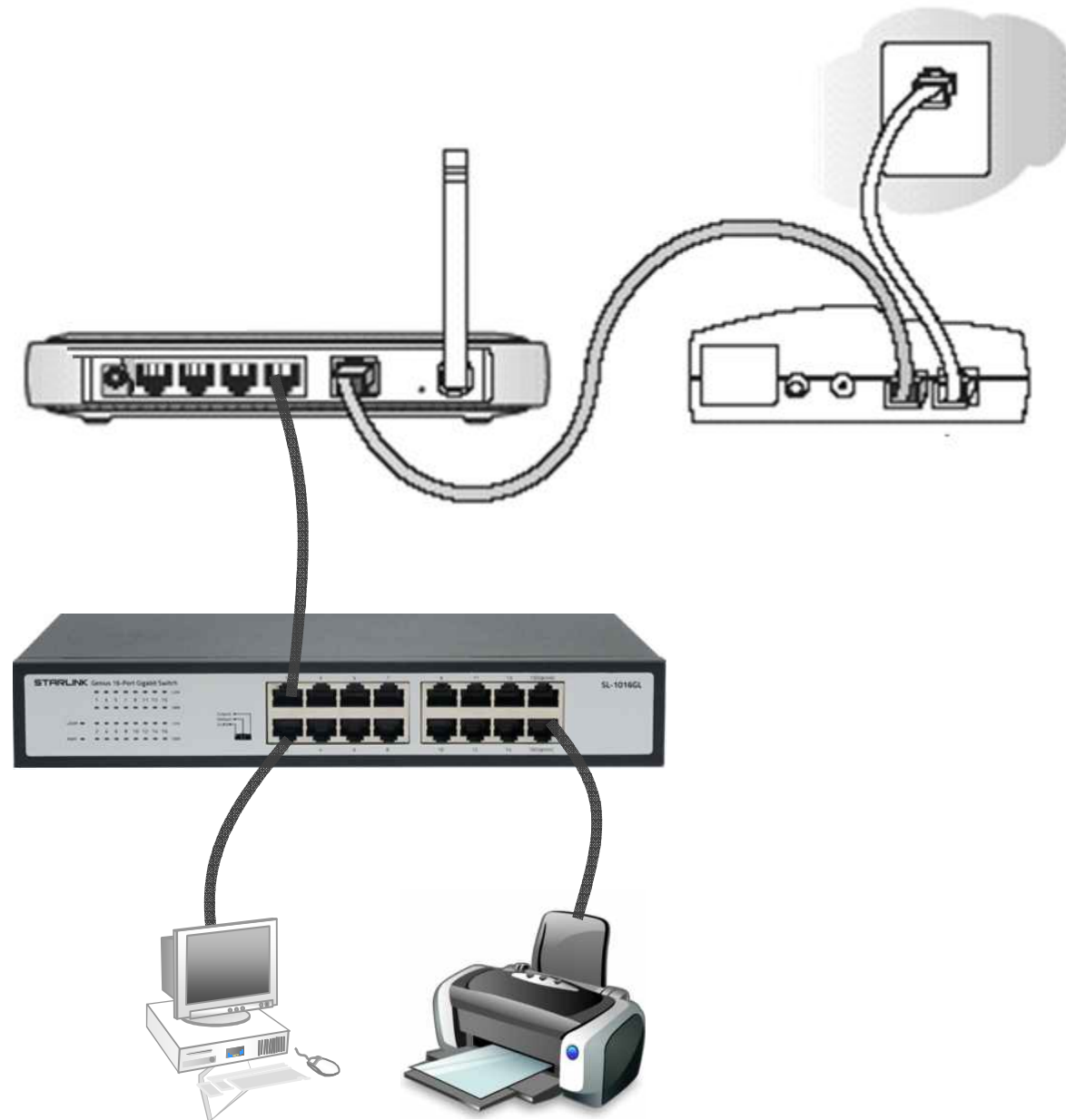
④ 구성도



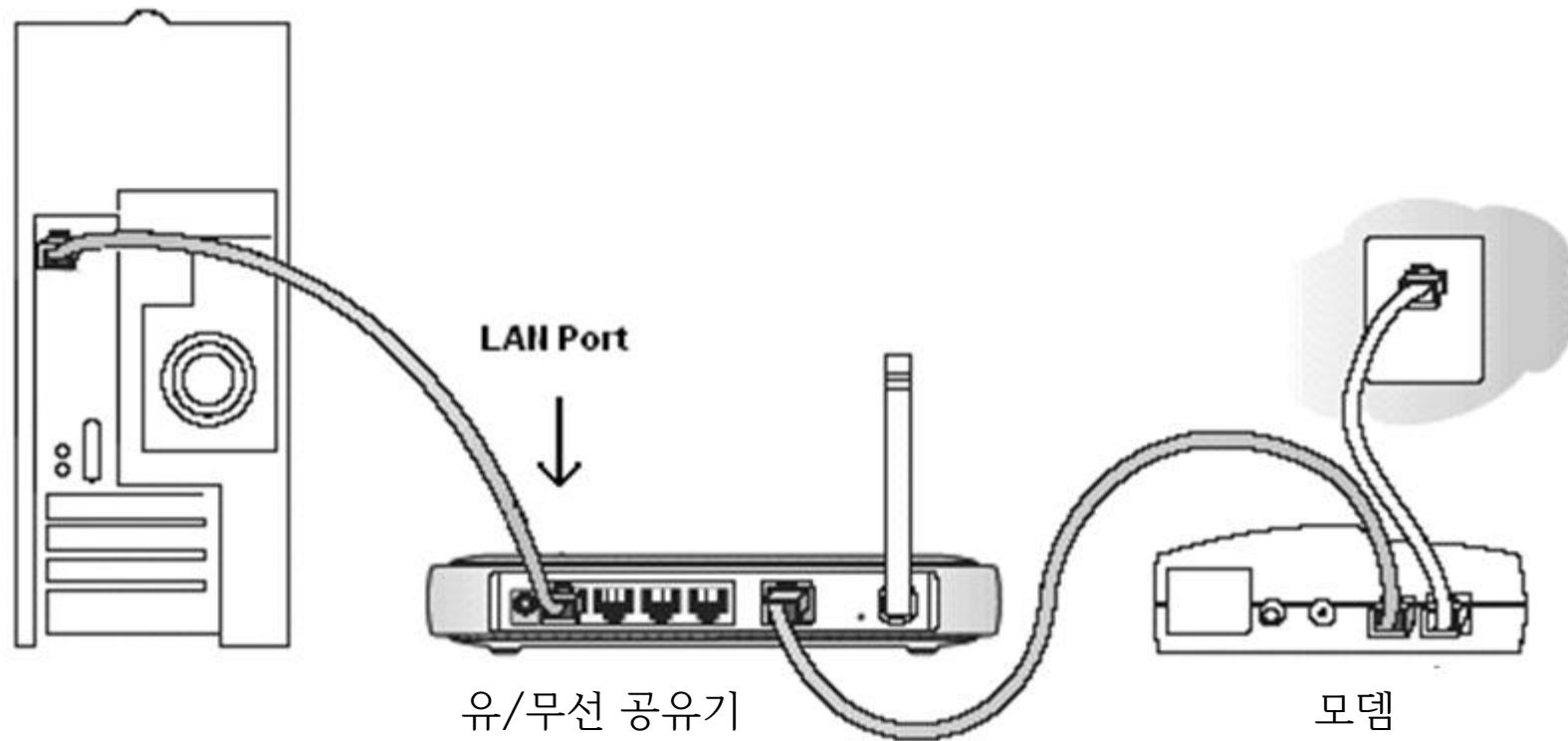
⑤ 구성도



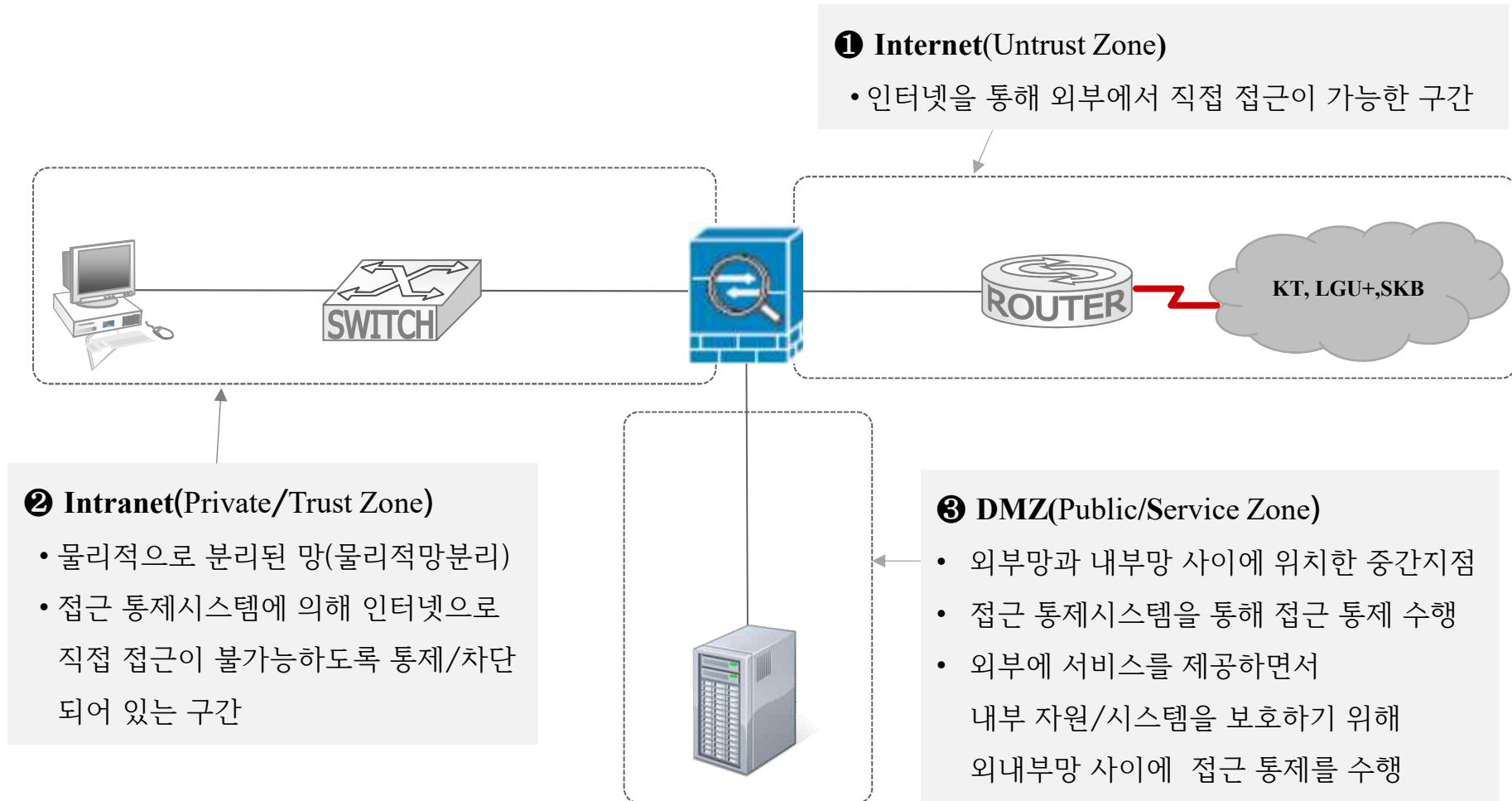
⑥ 구성도



⑦ 구성도

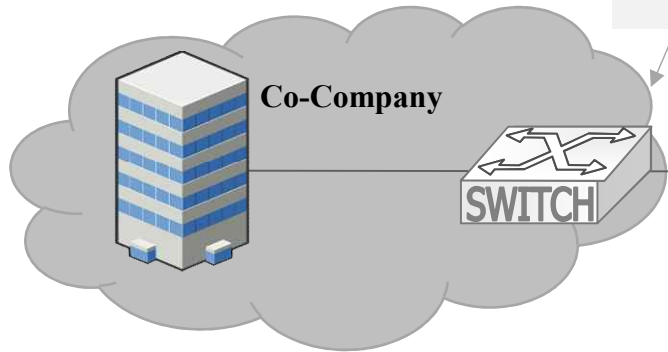


1.3 보안망 구성도



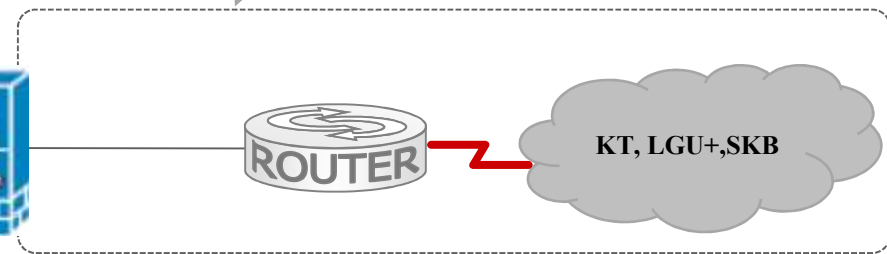
④ Extranet (대외망)

- 회사 대 회사로 서비스 연동이 필요한 경우 인터넷, 전용선, VPN등으로 연동



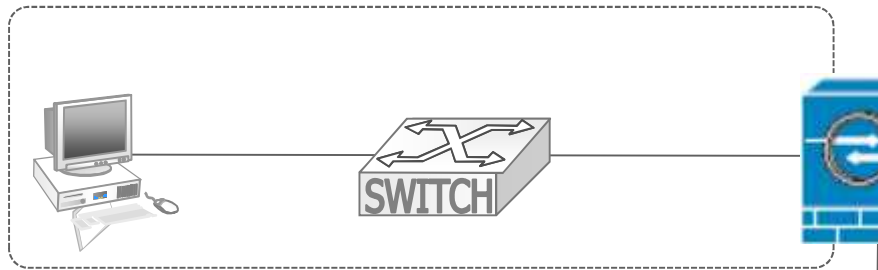
① Internet(Untrust Zone)

- 인터넷을 통해 외부에서 직접 접근이 가능한 구간



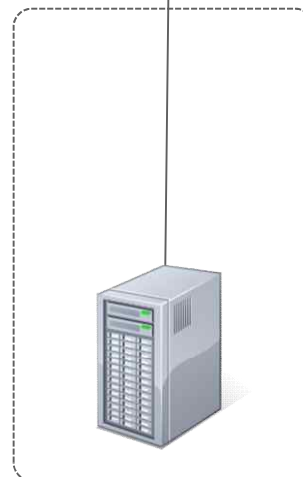
② Intranet (Private/Trust Zone)

- 물리적으로 분리된 망(물리적망분리)
- 접근 통제시스템에 의해 인터넷으로 직접 접근이 불가능하도록 통제/차단되어 있는 구간

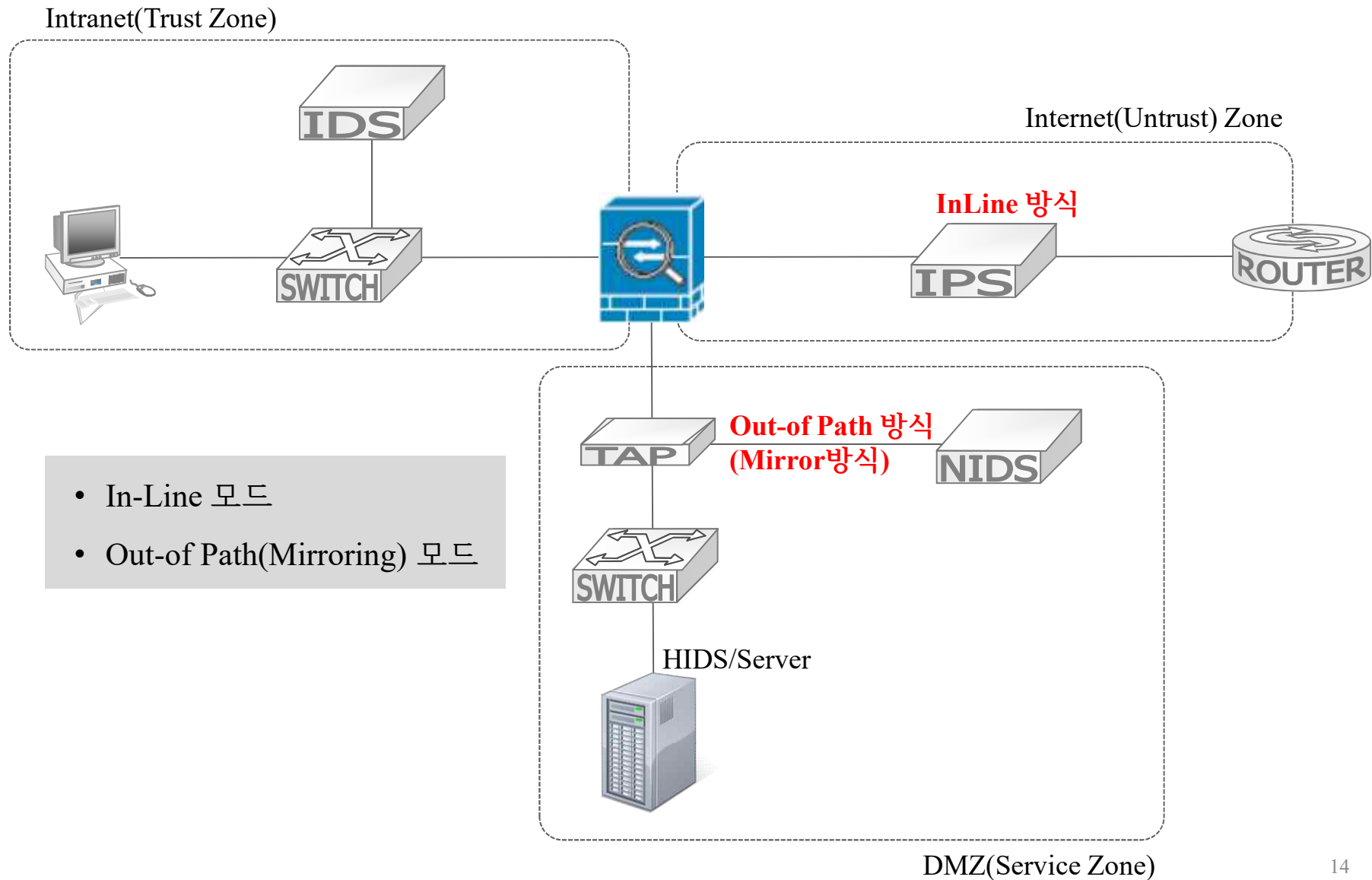


③ DMZ (Public/Service Zone)

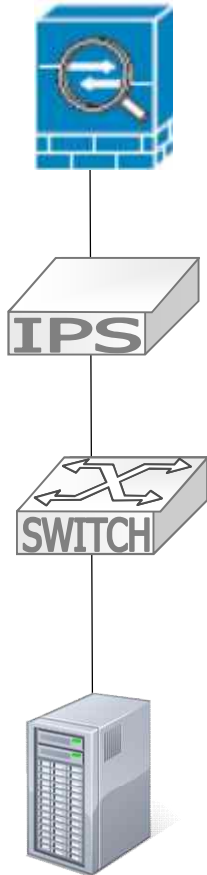
- 외부망과 내부망 사이에 위치한 중간지점
- 접근 통제시스템을 통해 접근 통제 수행
- 외부에 서비스를 제공하면서 내부 자원/시스템을 보호하기 위해 외내부망 사이에 접근 통제를 수행



보안 장비 설치 모드

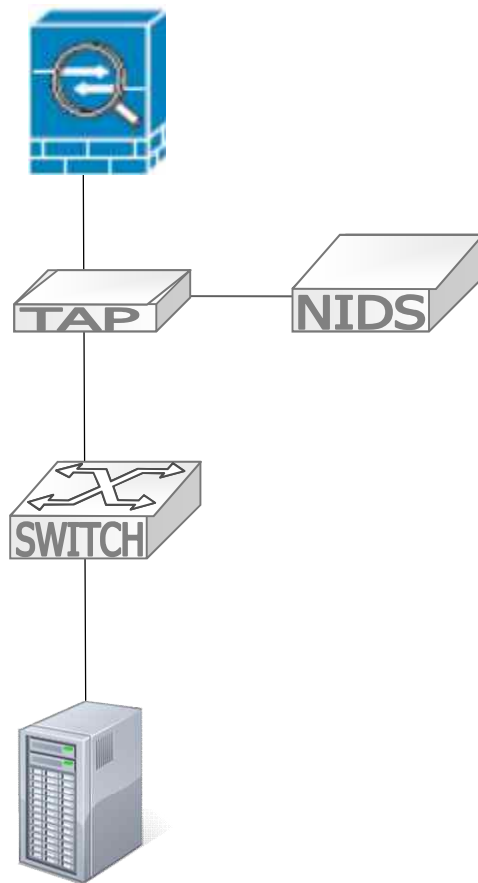


InLine 모드

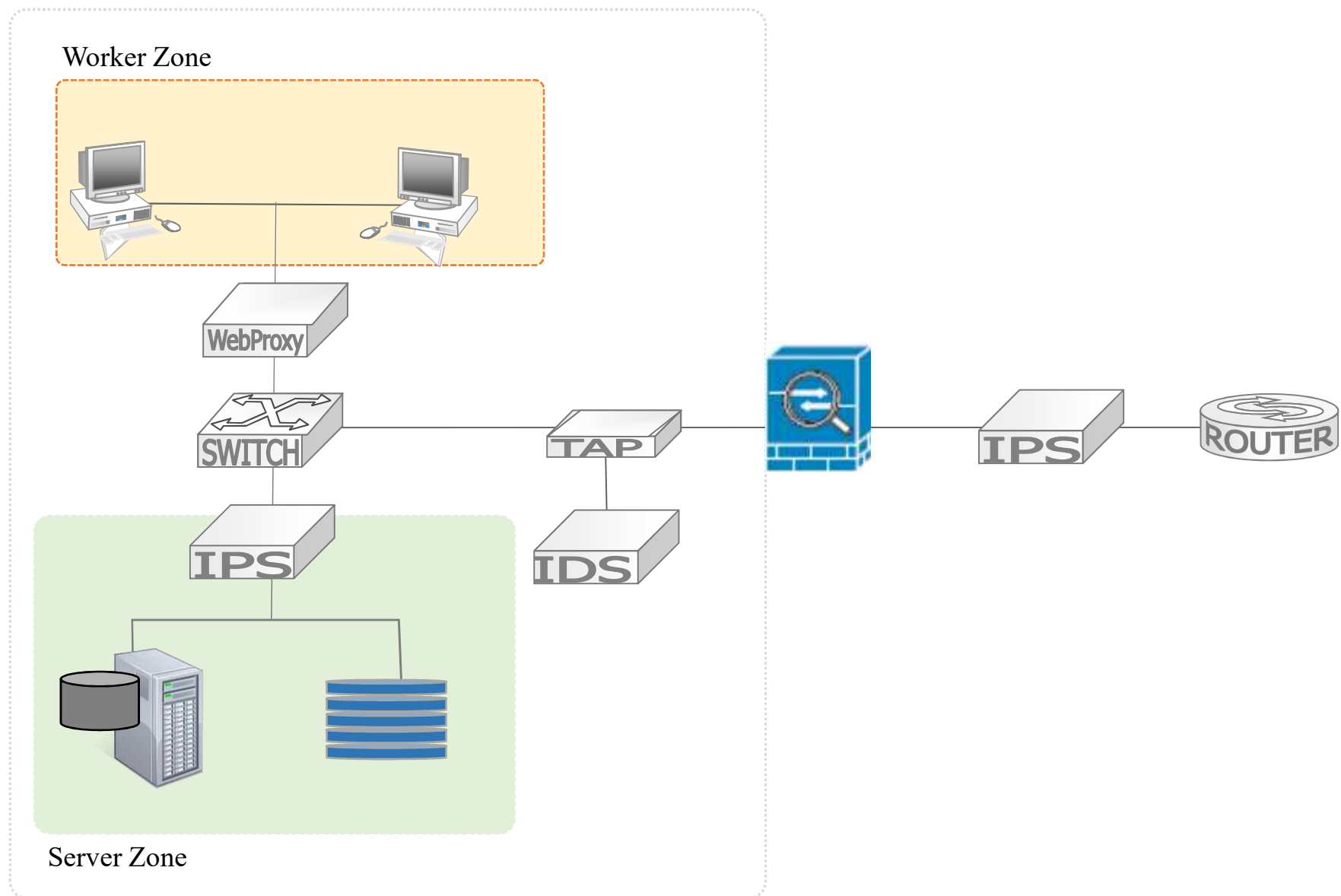


- 물리적 네트워크 경로 상에 보안장비를 설치
- 네트워크를 통과하는 모든 트래픽들이 보안장비를 거쳐 가도록 하는 모드
- 패킷 차단 목적의 장비에 적용 (예) Anti-DDoS, Firewall, IPS 등
- 장점 : 실시간 패킷을 탐지하고 차단
- 단점 : 장비에 장애가 발생 할 경우 전체 네트워크 장애로 확산 될 위험성
(전체 네트워크 가용성에 영향을 줄 수 있음)

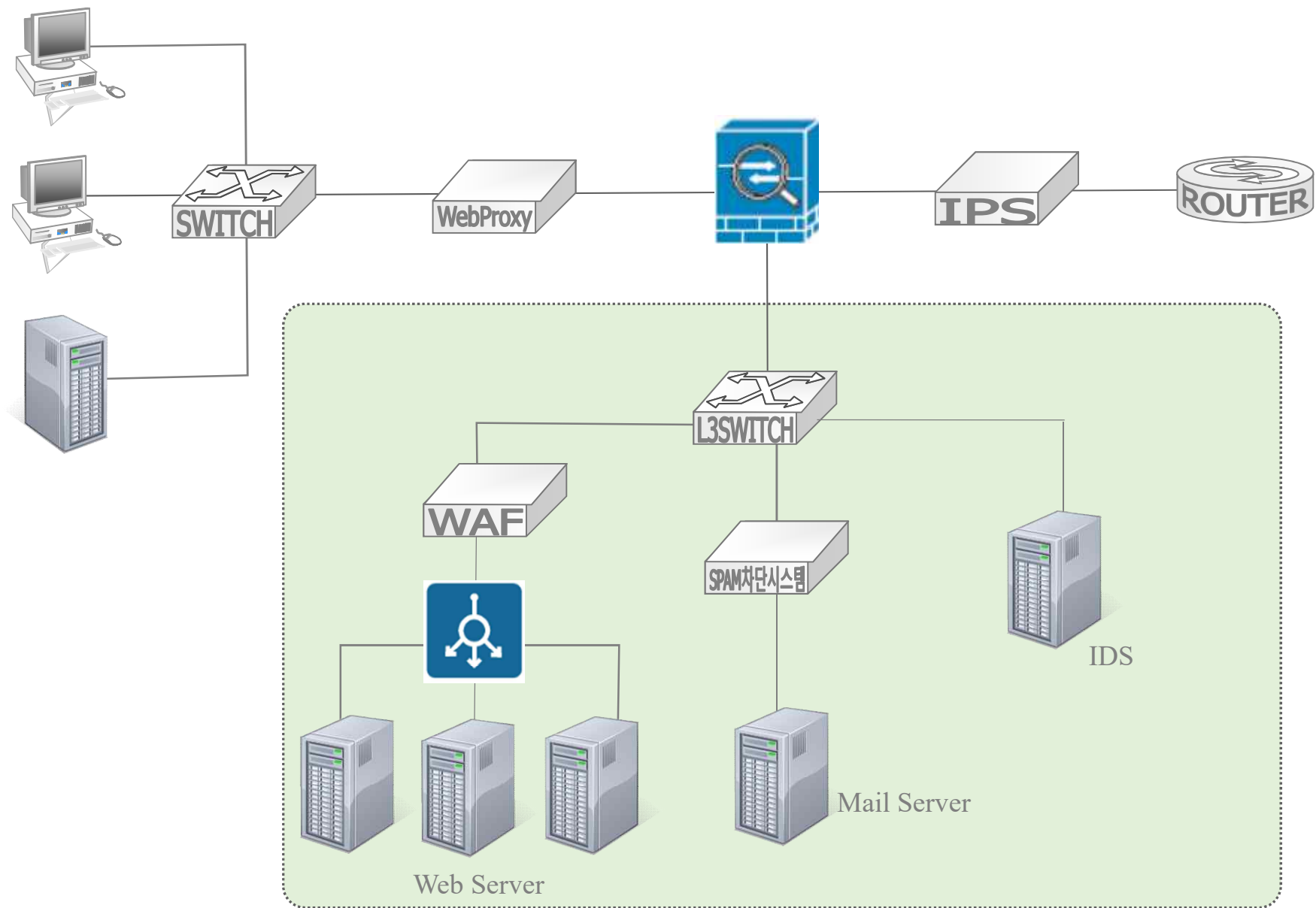
Out of Path(Mirror) 모드



- 미러링 장비(예. TAP)를 통해 복제된 패킷을 받아서 탐지하는 모드
- 패킷 차단 기능이 없는 탐지 목적의 장비에 적용
 - IDS, Anti-APT, Network Forensic 등
- 네트워크 경로를 벗어난 곳에 위치
- 장점 : 전체 네트워크 가용성에 영향을 주지 않으면서 패킷을 탐지할 수 있음
- 단점 : 복제(복사) 된 패킷을 탐지하기 때문에 실시간 패킷을 차단하기 어려움



Intranet Zone(Private/Trust)



DMZ Zone(Service/Public)

DataCenter Zone

