재미있는 어플리케이션 이야기

황 규 언 차장

2009. 9. 19

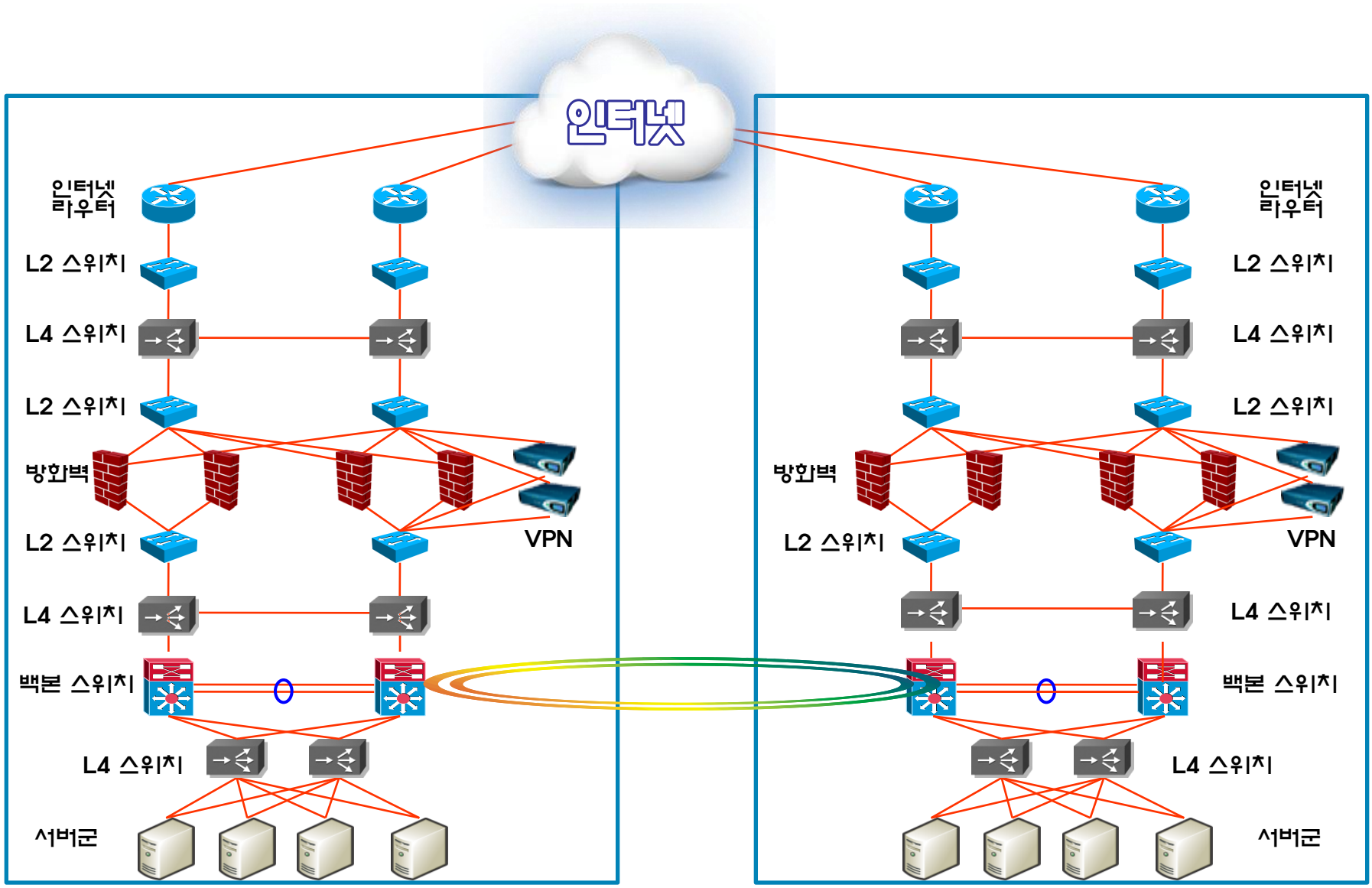
오늘 세션은

- 어플리케이션 스위치를 이해 함으로써, 네트워크 구성 나타나도 두렵지 않습니다.
- 향후, 네트워크 관점이 아닌, 전체적인 서비스 관점의 이해가 한결 편해 집니다.
- 이론적인 OSI 7 Layer 가 실무적인 OSI 7 Layer로 여러분에게 다가 옵니다.

발표 순서

- 제 1부
  - 어플리케이션 스위치가 없을 때는 어떻게 했나 ?
  - L4 스위치의 기본 기능은 이렇습니다.
- 제2부
  - 이제 좀 더 고급 기능 어플리케이션 스위치?
  - 아무리 강조해도 지나 치지 않는 보안!
- 마지막 정리

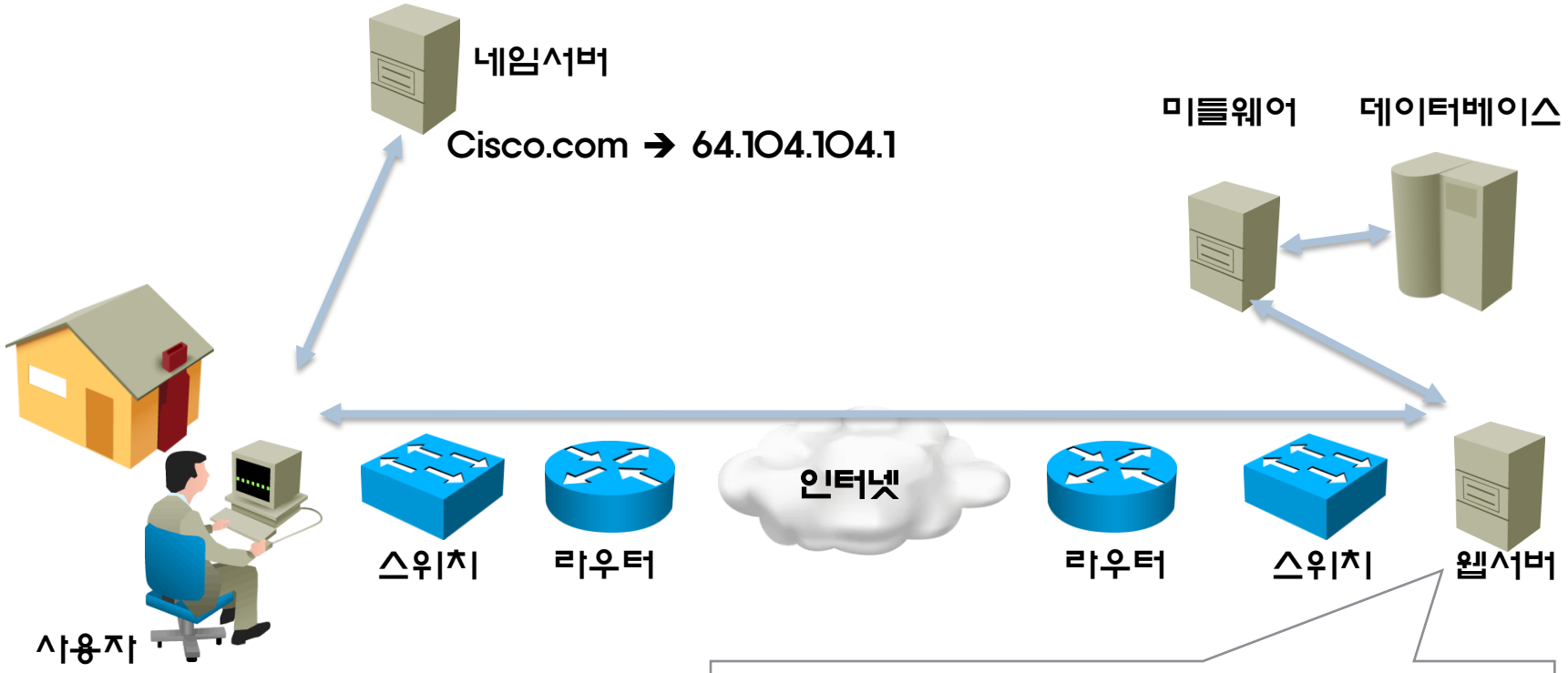
조금 복잡한 네트워크 구성 현황

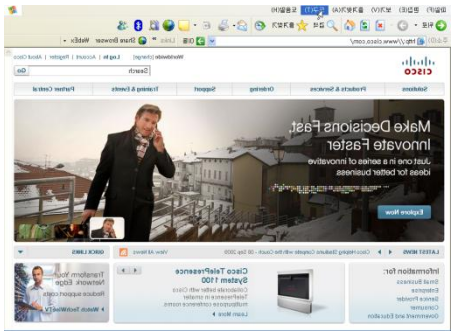


제1부

어플리케이션 스위치가 없을 때는 어떻게 했나?

재미있는 패킷 여행(1/2)

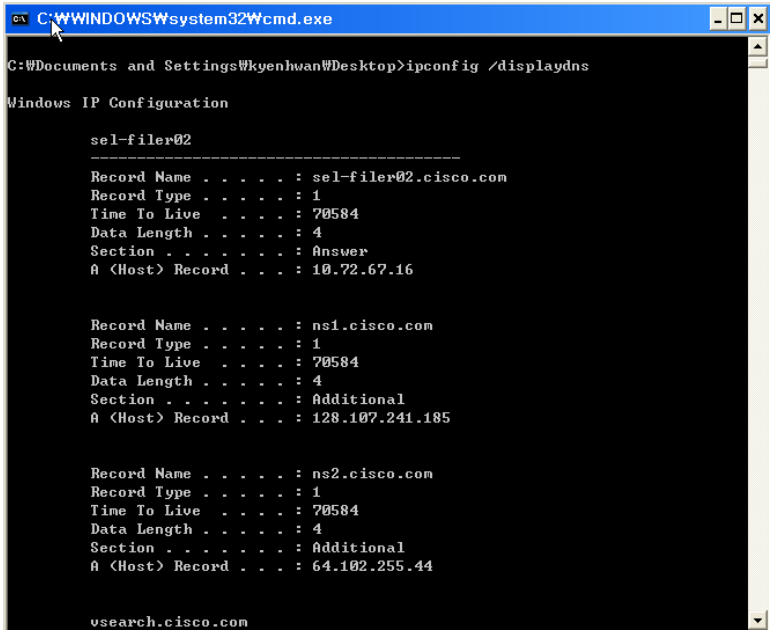

네임서버
Cisco.com ➔ 64.104.104.1
미들웨어
데이터베이스
인터넷
스위치
라우터
라우터
스위치
웹서버
사용자
Tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN



재미있는 패킷 여행(2/2)

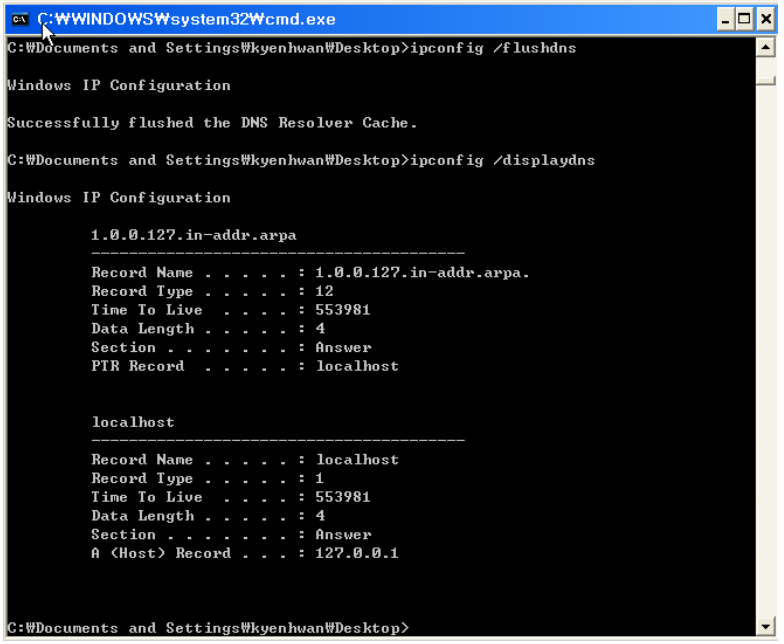
PC내의 cache 정보 먼저 확인 한다.

ipconfig /displaydns 명령어



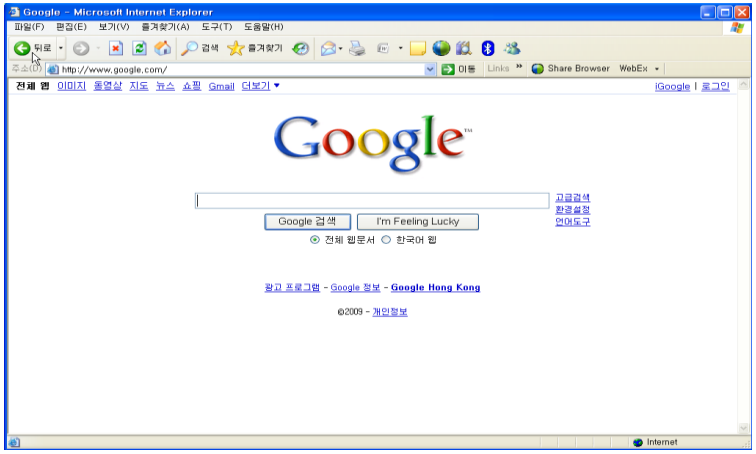
사용자

ipconfig /flushdns 명령어

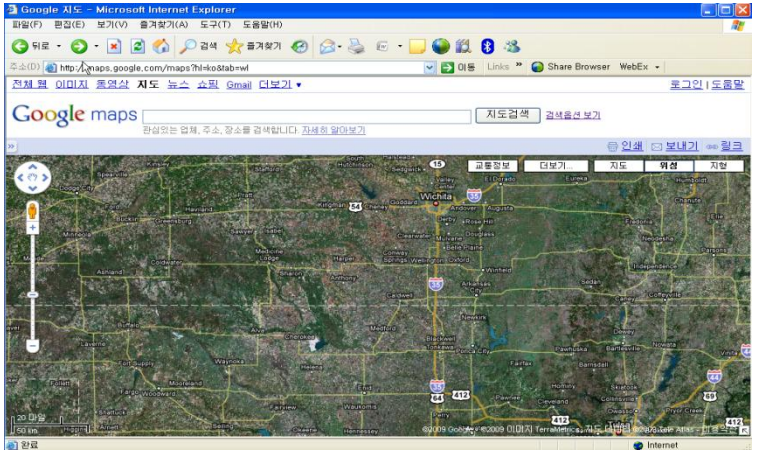


트래픽 성격 참 많이 변했습니다.

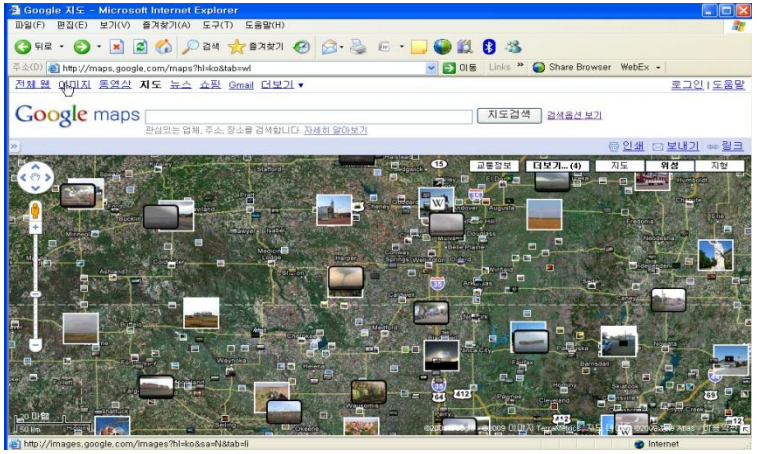
텍스트 기반



그래픽 기반



동영상

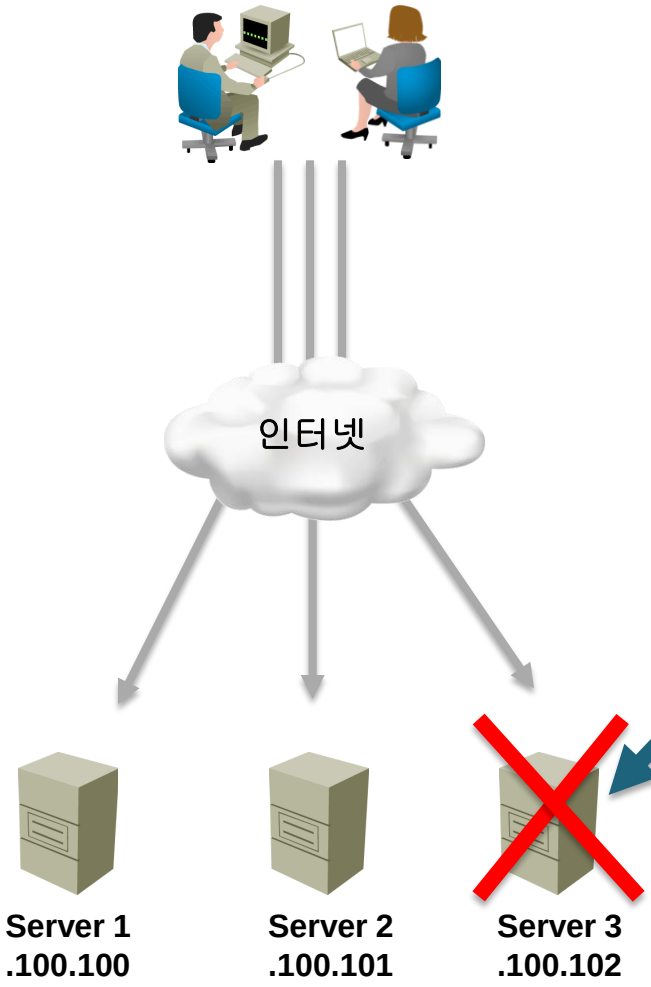


수많은 동적 컨텐츠

생각지 못한 문제점들.

복잡화, 응답속도, 안정성

DNS로 부하분산을 ?



일반적인 DNS Zone File

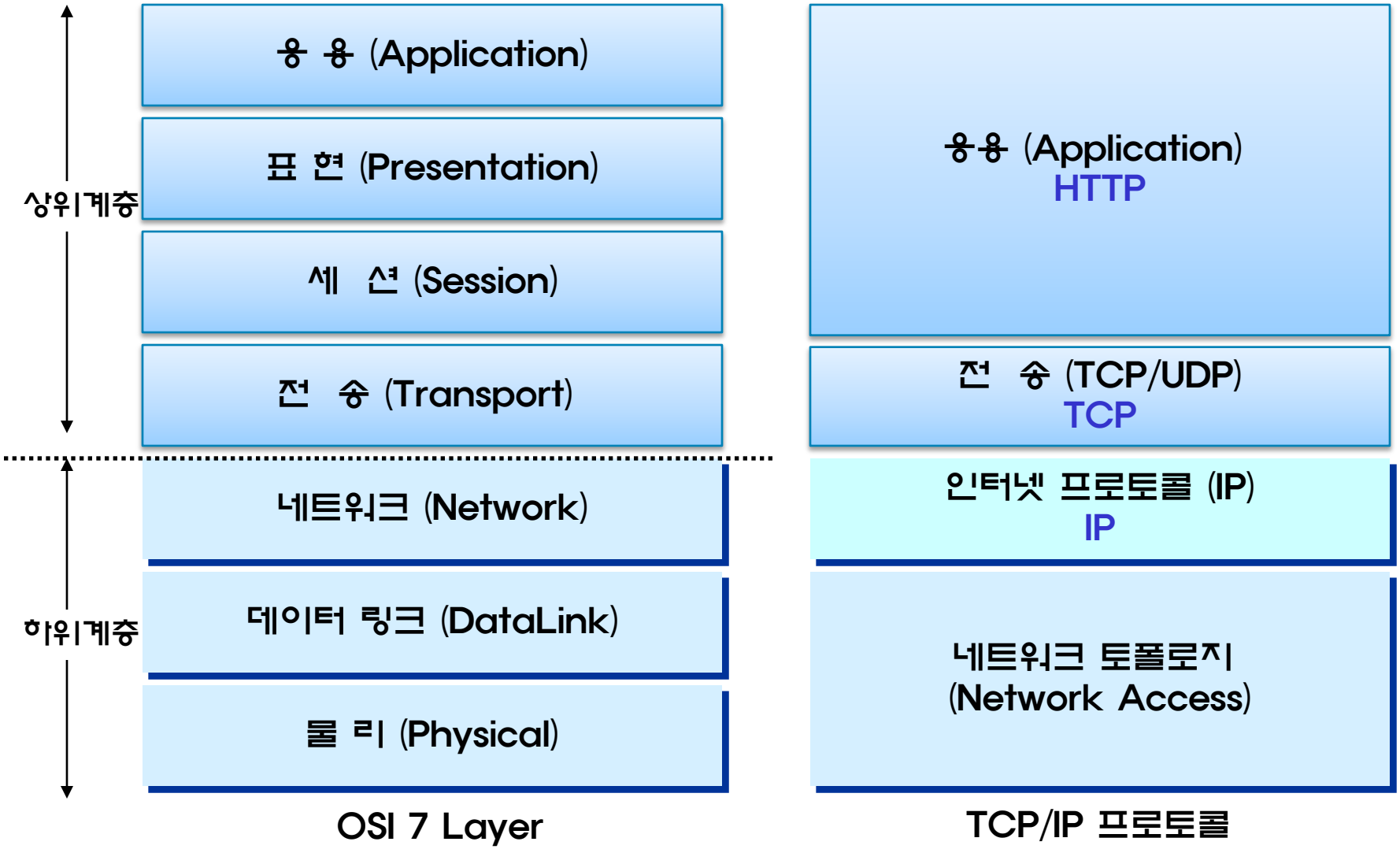
▪ www.yahoo.com	IN	A	200.100.100.100

DNS 기반의 로드 밸런싱

▪ www.yahoo.com	IN	A	200.100.100.100
	IN	A	200.100.100.101
	IN	A	200.100.100.102

- DNS 캐쉬등으로 DNS 변경 적용이 바로 안됨
- 로드 분배 형태의 단순
- 서버 장애에 대한 인지 할 수 없음

OSI 7 Layer 와 TCP/IP의 기본에 충실



실제 패킷에서 참조되는 영역은?

실제 패킷 정보

Source	Destination	Protocol	Info
121.170.68.94	64.244.14.162	TCP	tcoregagent > http [SYN] Seq=0 Win=65535 Len=0 MSS=1260 WS=1
64.244.14.162	121.170.68.94	TCP	http > tcoregagent [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS
121.170.68.94	64.244.14.162	TCP	tcoregagent > http [ACK] Seq=1 Ack=1 Win=65536 Len=0
121.170.68.94	64.244.14.162	HTTP	GET /WebIQ/DataServer/DataServer.dll?Handler=AuthorizeOptInRe
64.244.14.162	121.170.68.94	TCP	[TCP segment of a reassembled PDU]
64.244.14.162	121.170.68.94	HTTP	HTTP/1.1 200 OK (PNG)
121.170.68.94	64.244.14.162	TCP	tcoregagent > http [ACK] Seq=681 Ack=778 Win=64758 Len=0
64.244.14.162	121.170.68.94	TCP	http > tcoregagent [FIN, ACK] Seq=778 Ack=681 Win=64855 Len=0
121.170.68.94	64.244.14.162	TCP	tcoregagent > http [ACK] Seq=681 Ack=779 Win=64758 Len=0
121.170.68.94	64.244.14.162	TCP	tcoregagent > http [FIN, ACK] Seq=681 Ack=779 Win=64758 Len=0
64.244.14.162	121.170.68.94	TCP	http > tcoregagent [ACK] Seq=779 Ack=682 Win=64855 Len=0

제1부

L4 스위치의 기본 기능은 이렇습니다.

기본 개념부터 충실히.

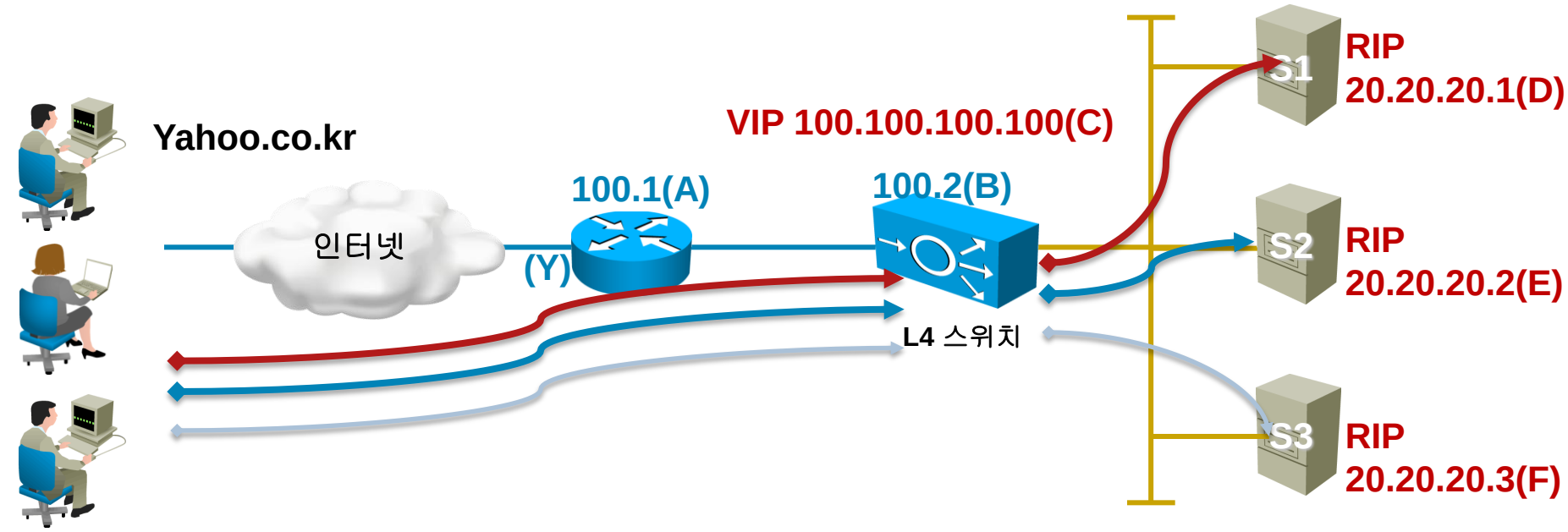
- 일반적으로 OSI 7 Layer의 4번째 전송(Transport)계층에서 정의되어지는 TCP/UDP 트래픽의 관리가 가능한 장비
- 기본적으로 DNS 라운드 로빈 방식의 서버 로드밸런싱의 확장 개념
- 현재는 웹 서버뿐만 아니라 TCP, UDP를 사용하는 대부분의 서비스 지원(HTTP, Telnet, FTP, SSL, Firewall, VPN, VoIP 등)
- Fault Tolerant에 대비한 다양한 Active-Standby, Active-Active 환경 제공
- 부하분산은 VIP(virtual Server)를 향하는 트래픽에 대해서만 작동함
- Virtual server = IP address & L4 protocol & port

용어만은 꼭 알고 갑시다.

- VIP (Virtual IP) : 외부 클라이언트들이 접속을 위해 사용되어지는 가상의 IP
- Real Server (실제서버) : VIP 로 접속되어진 클라이언트들의 서비스를 받아주는 실제 물리적인 서버
- Service Farm : Real Server들을 모여 있는 그룹
- Policy(정책) : 스위치로 들어온 트래픽을 어떤 서버로 보낼것인가를 결정하는 정책 (Weighted Round-Robin(Weighted) Least Connection, Hash etc)
- Persistence : 한 클라이언트의 브라우져가 같은 서버로 지속적으로 연동될 수 있게 함(Source IP, Sessoin ID)

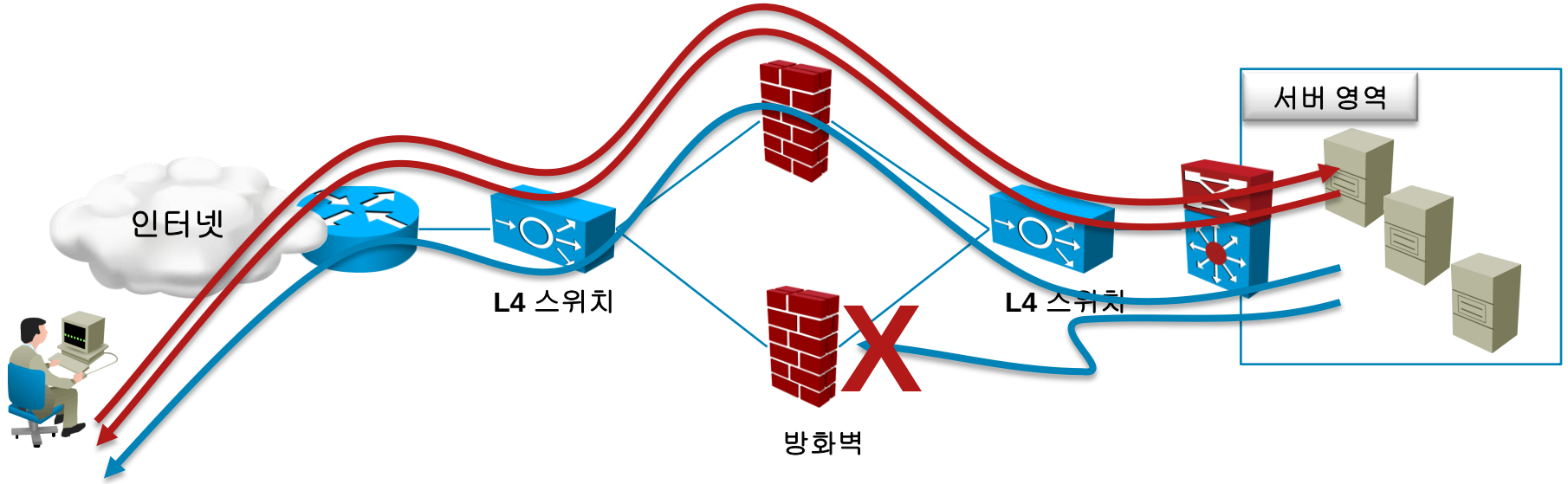
SLB(Server Load Balancing), 부하분산 ?

- 트래픽이 지나간 정보에 대해서 IP, Port 정보의 Session Table 작성



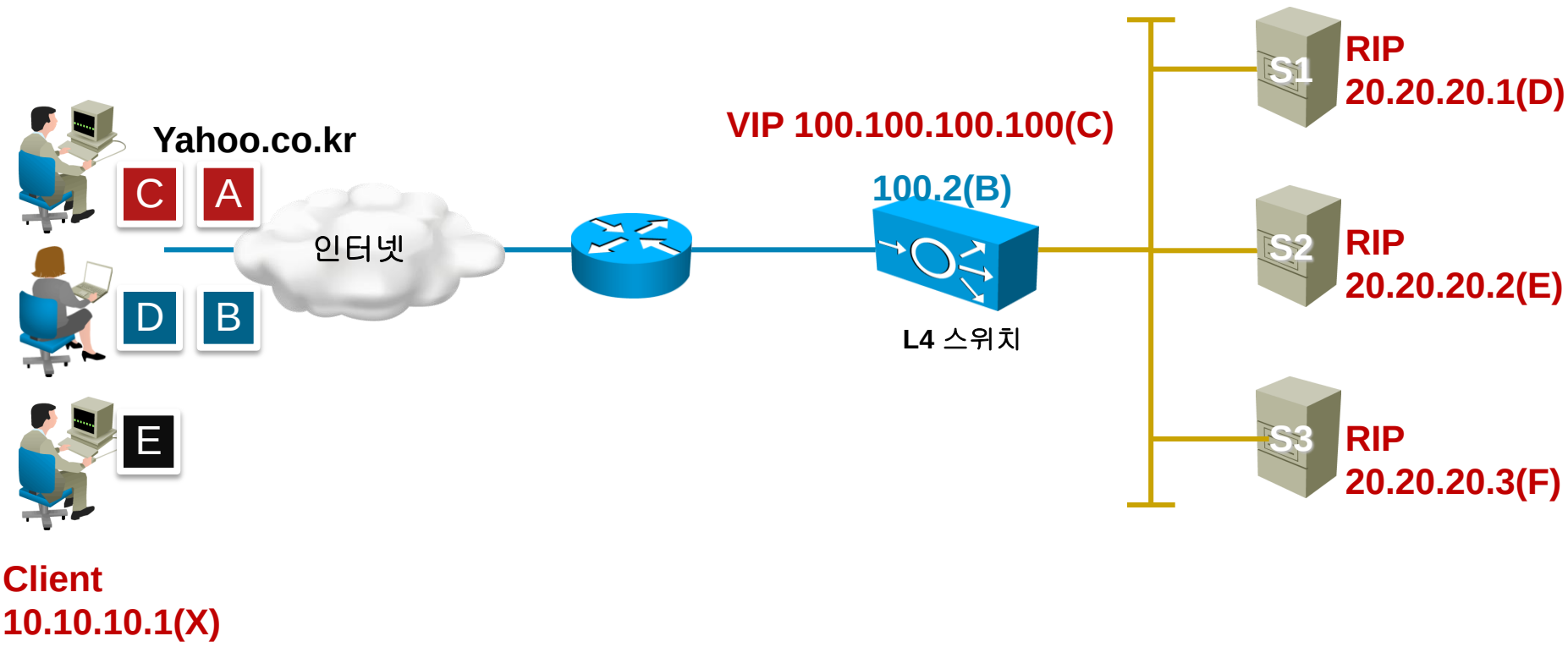
FLB(Firewall Load Balancing), 부하분산 ?

- 부하분산 알고리즘에 의해서, 트래픽의 동일 경로 유지가 필수



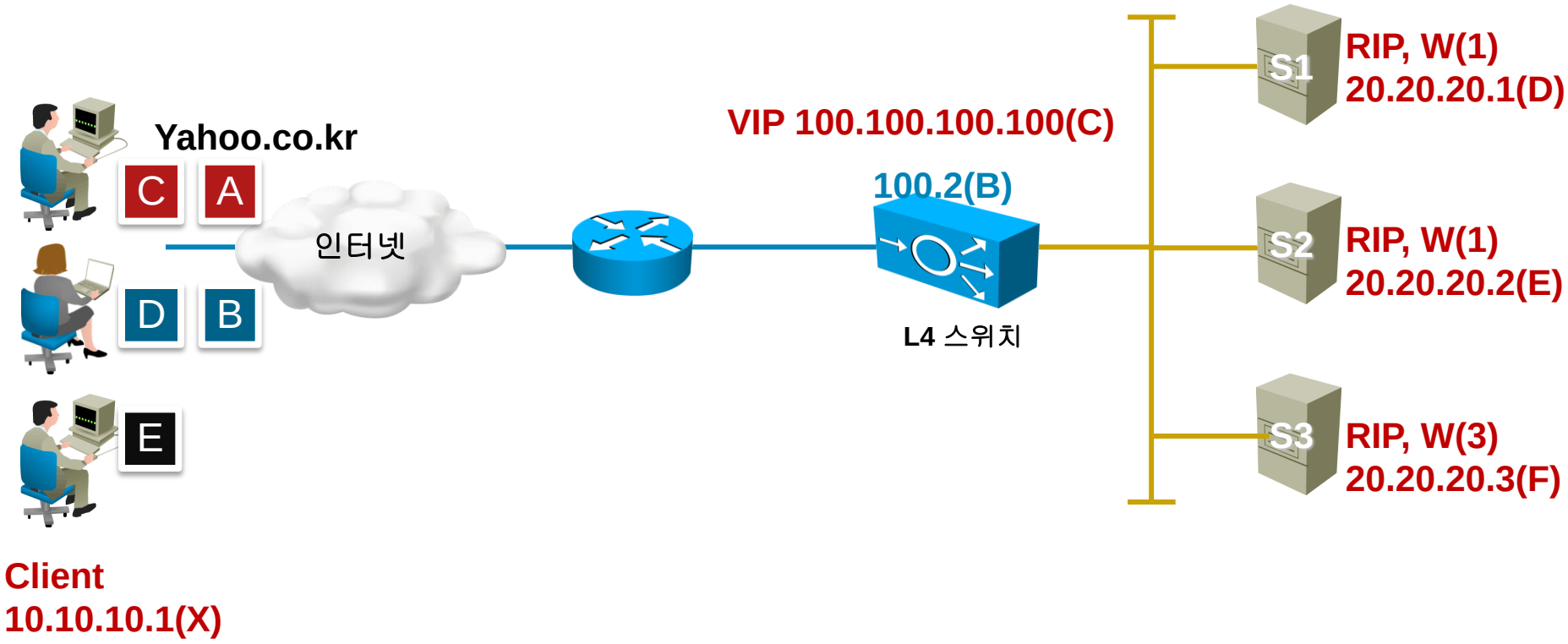
부하분산 정책 – Round Robin

- 단순 무식하게 동작, VIP로 접속하는 순서대로



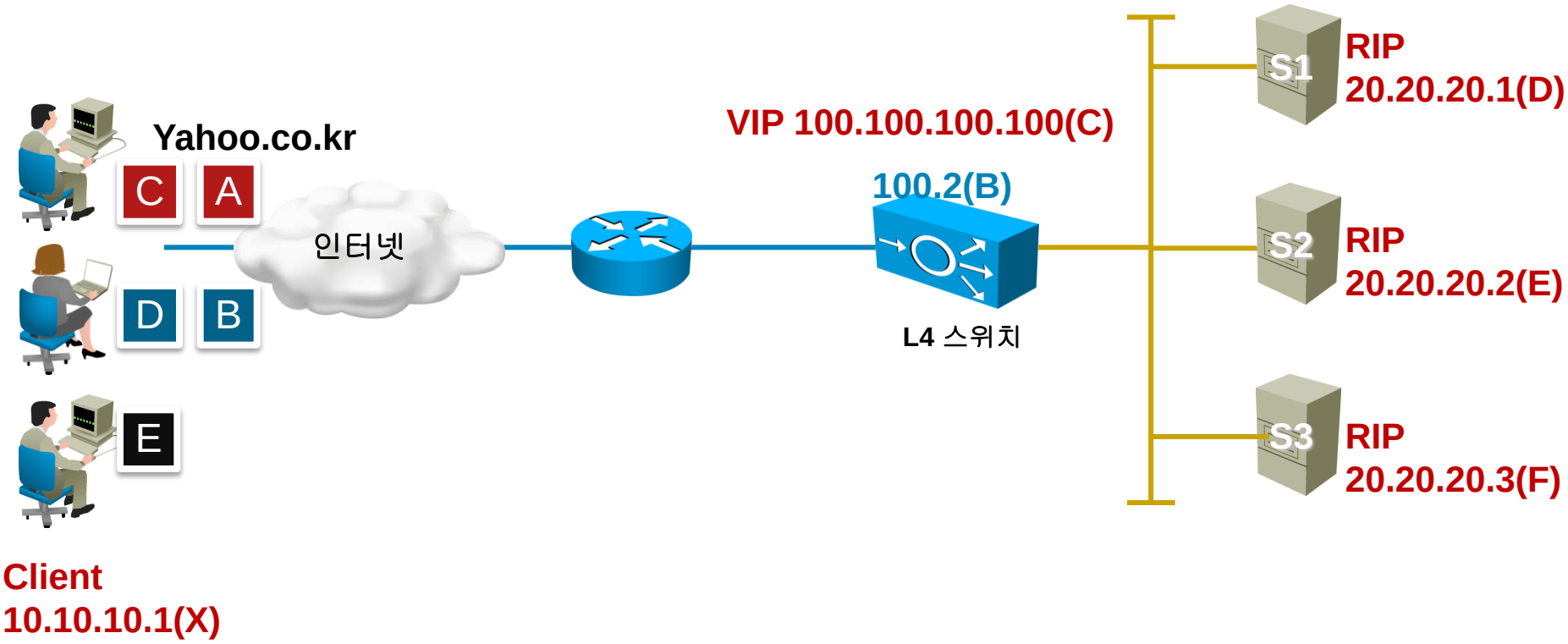
부하분산 정책 – Weighted Round Robin

- 서버의 성능에 따라, 가중치를 부여, 고민한 흔적이 보임



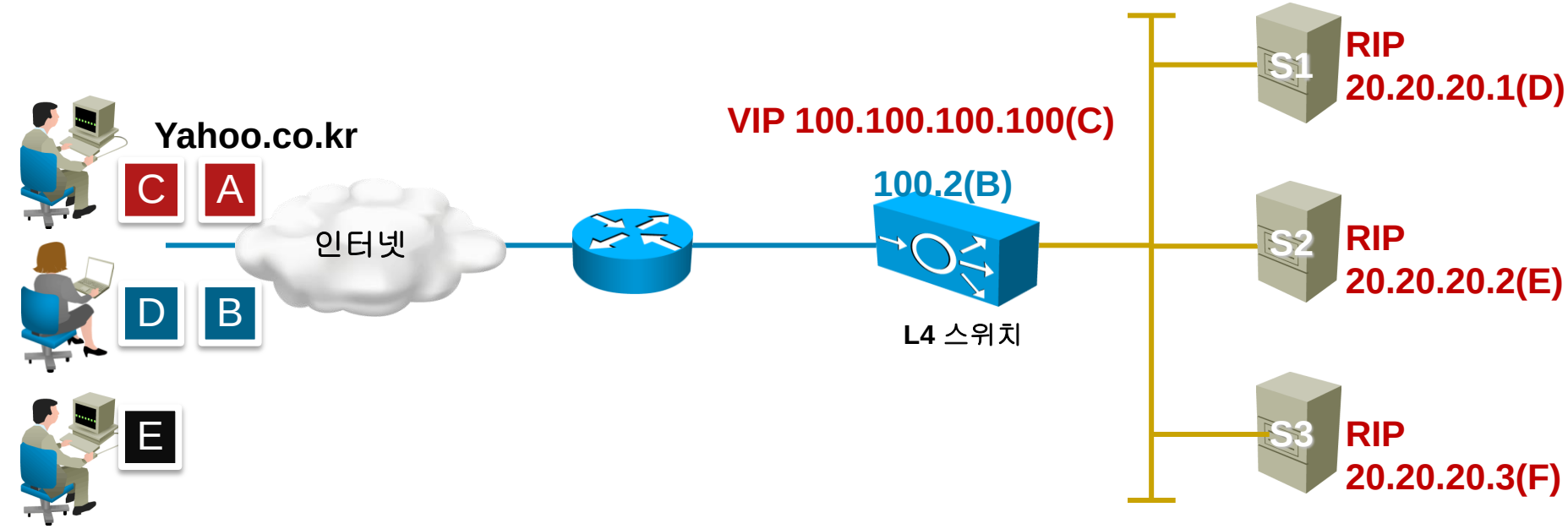
부하분산 정책 – Least Connection

- 현재 Connection이 제일 작은 서버로 부하분산
- Round Robin과는 다른 동작 하나, 서버와의 Connection 검사



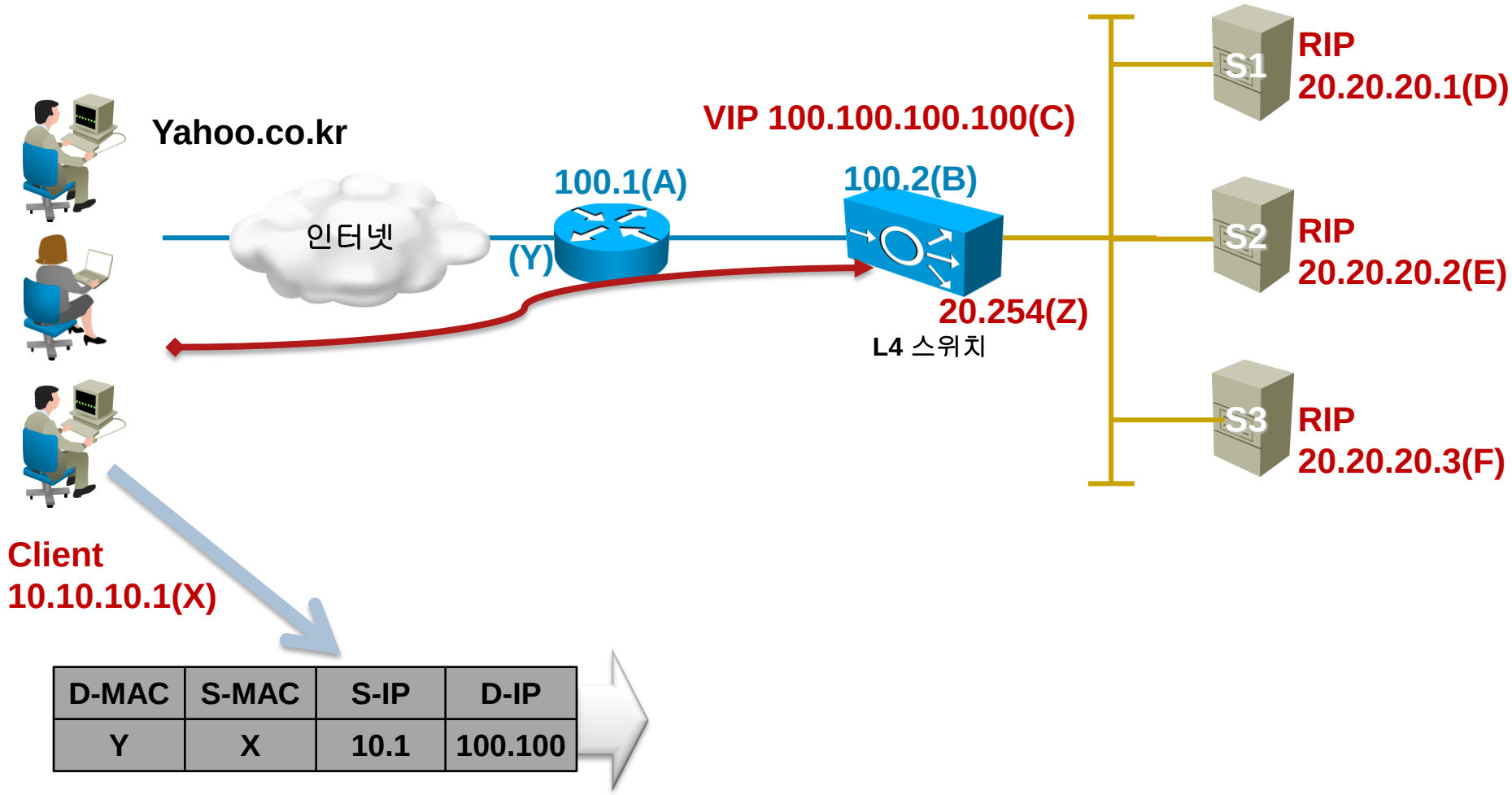
부하분산 정책 – Hash

- 한번 선택하면, 끝까지…
- “내 장바구니 찾아내…”
- Source IP or Source IP + Destination IP 조합의 Hash 계산

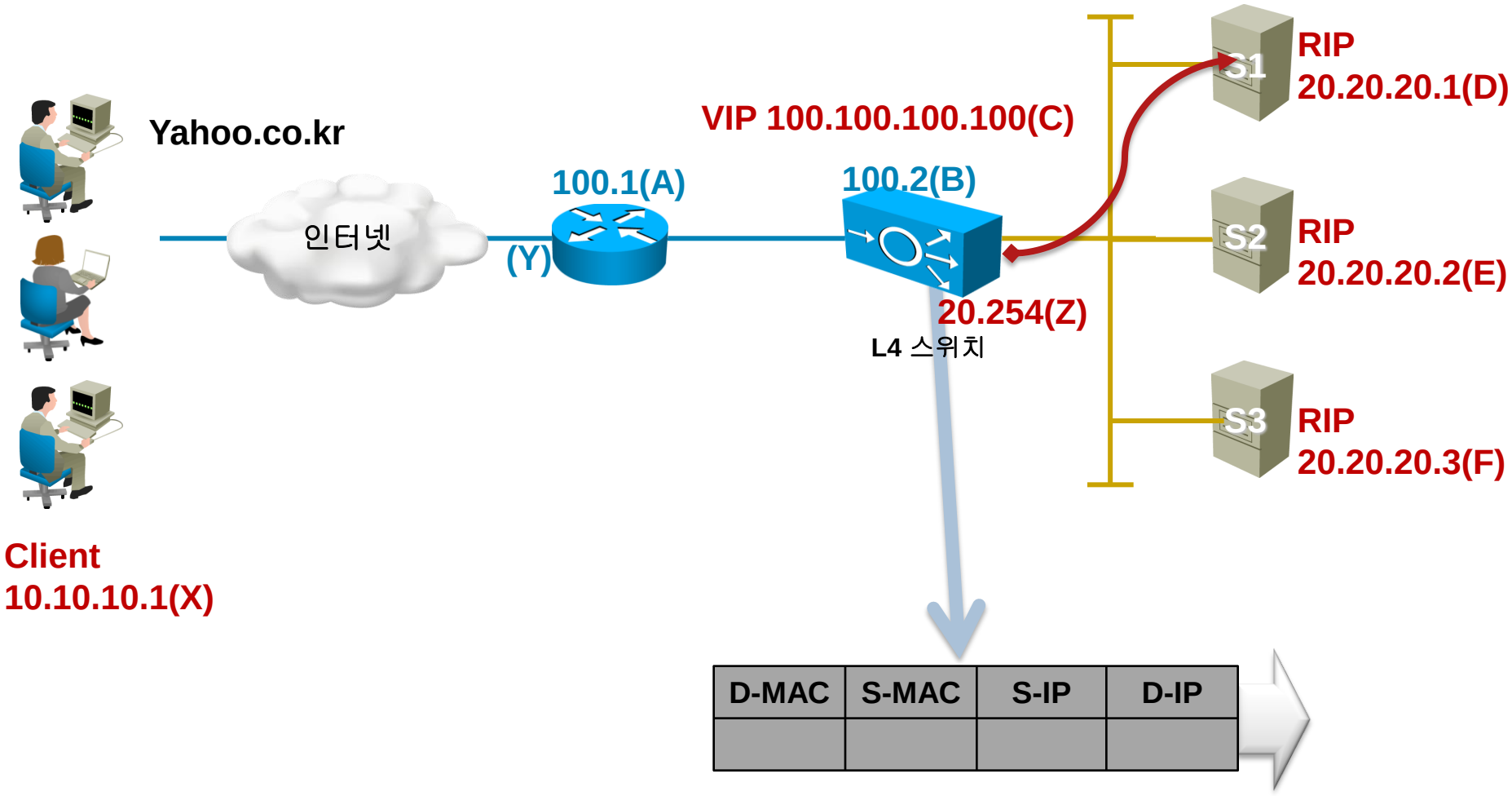


Client
10.10.10.1(X)

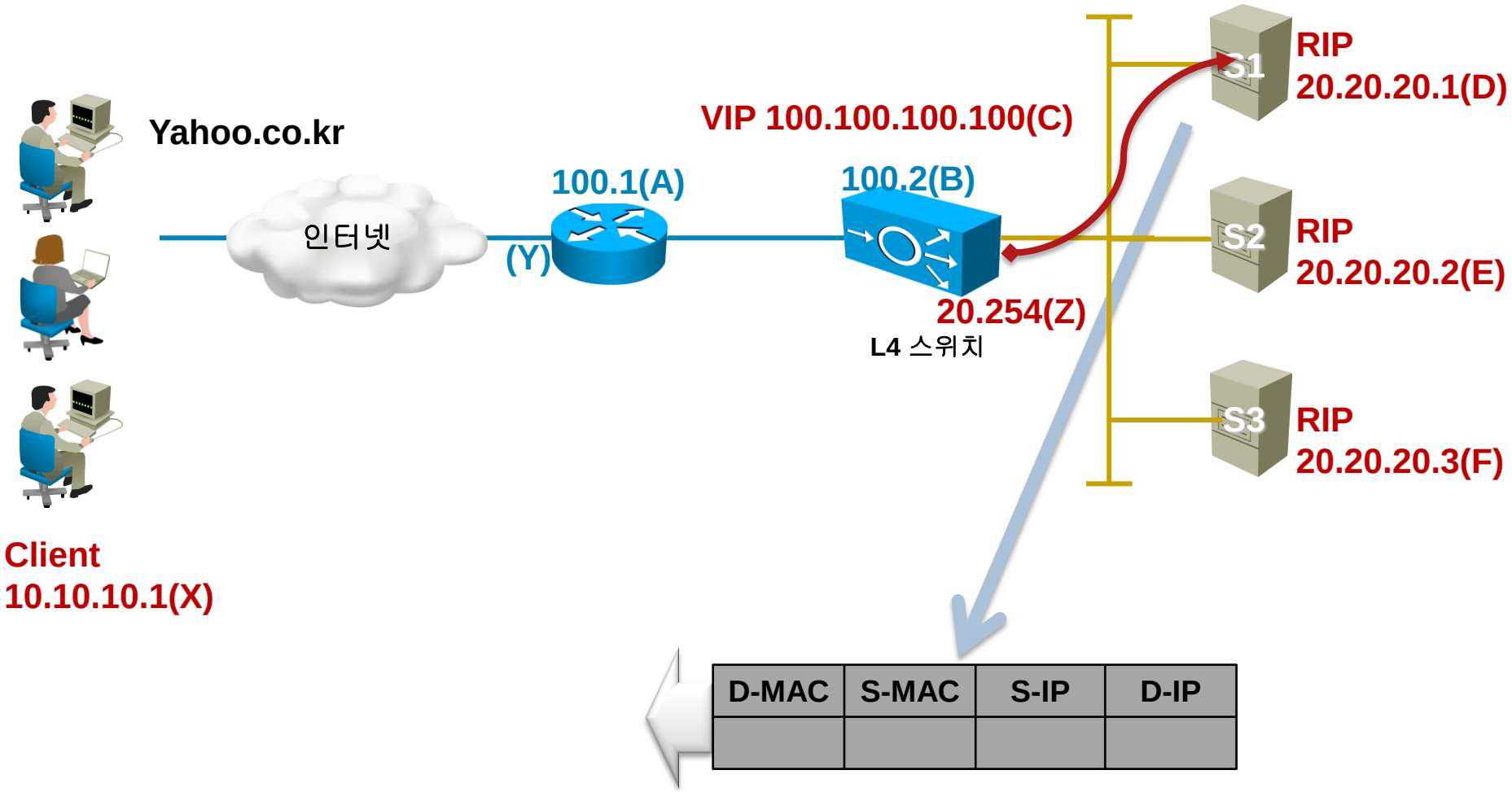
SLB(Server Load Balancing), 부하분산 ?



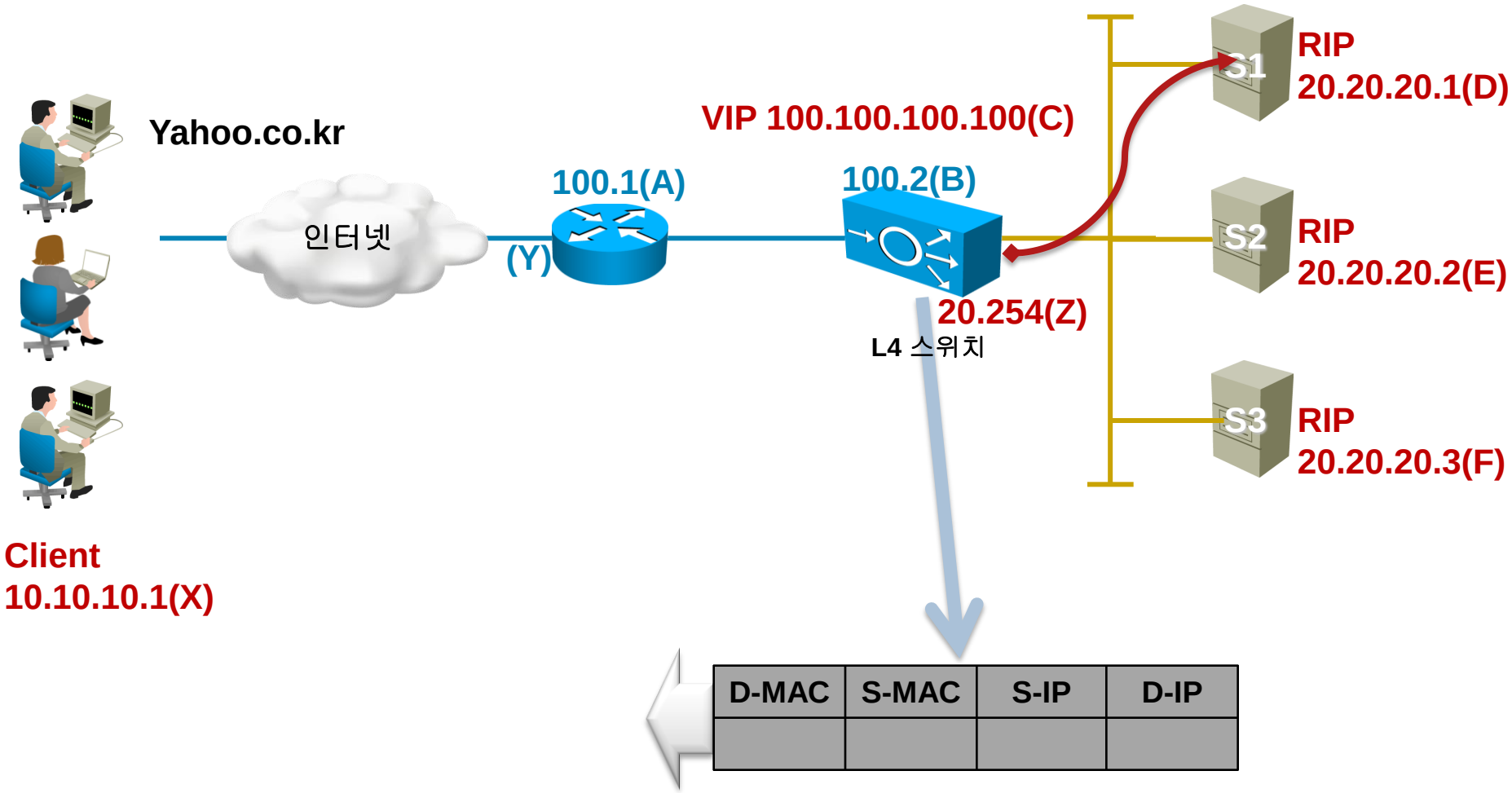
SLB(Server Load Balancing), 부하분산 ?



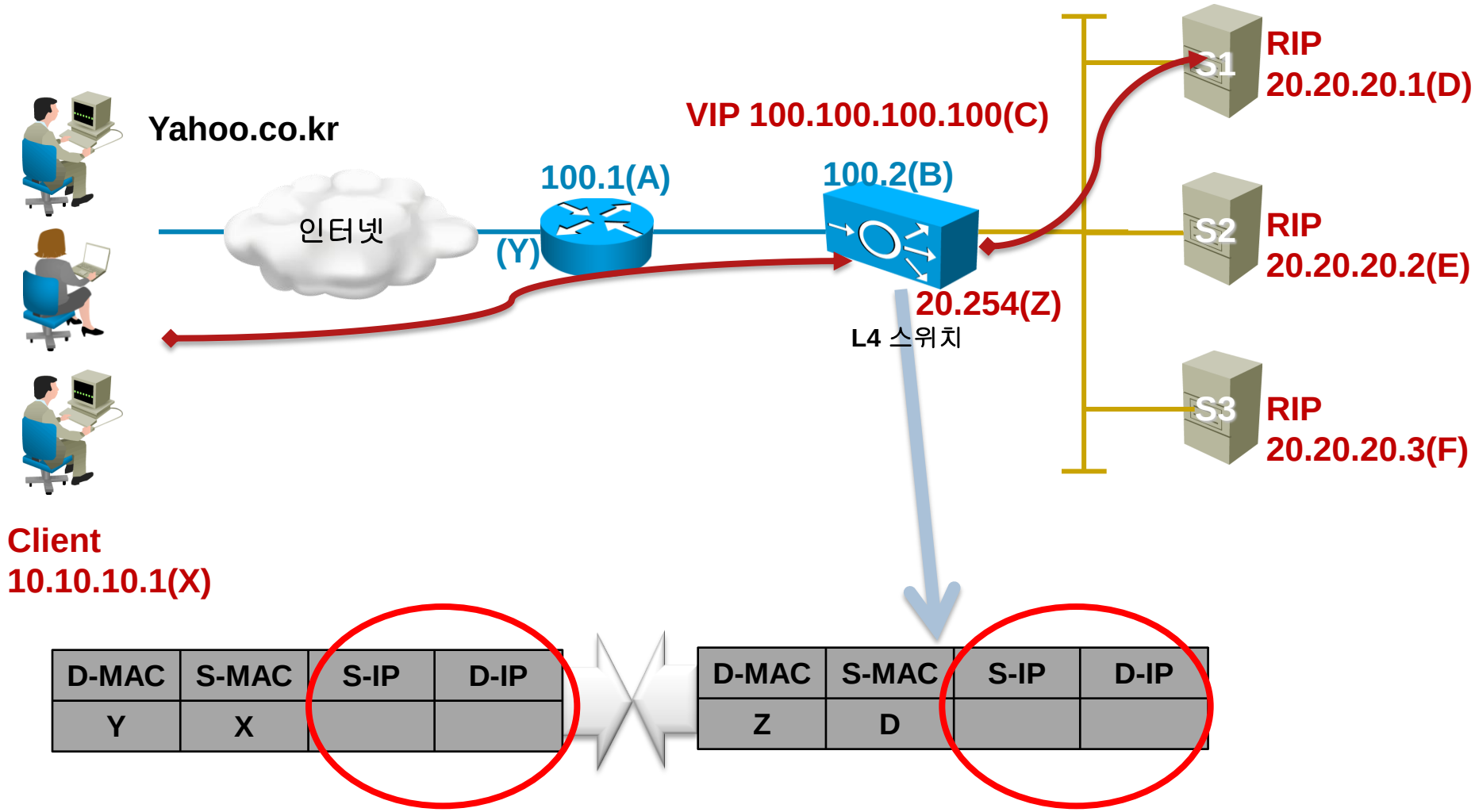
SLB(Server Load Balancing), 부하분산 ?



SLB(Server Load Balancing), 부하분산 ?



SLB(Server Load Balancing), 부하분산 ?

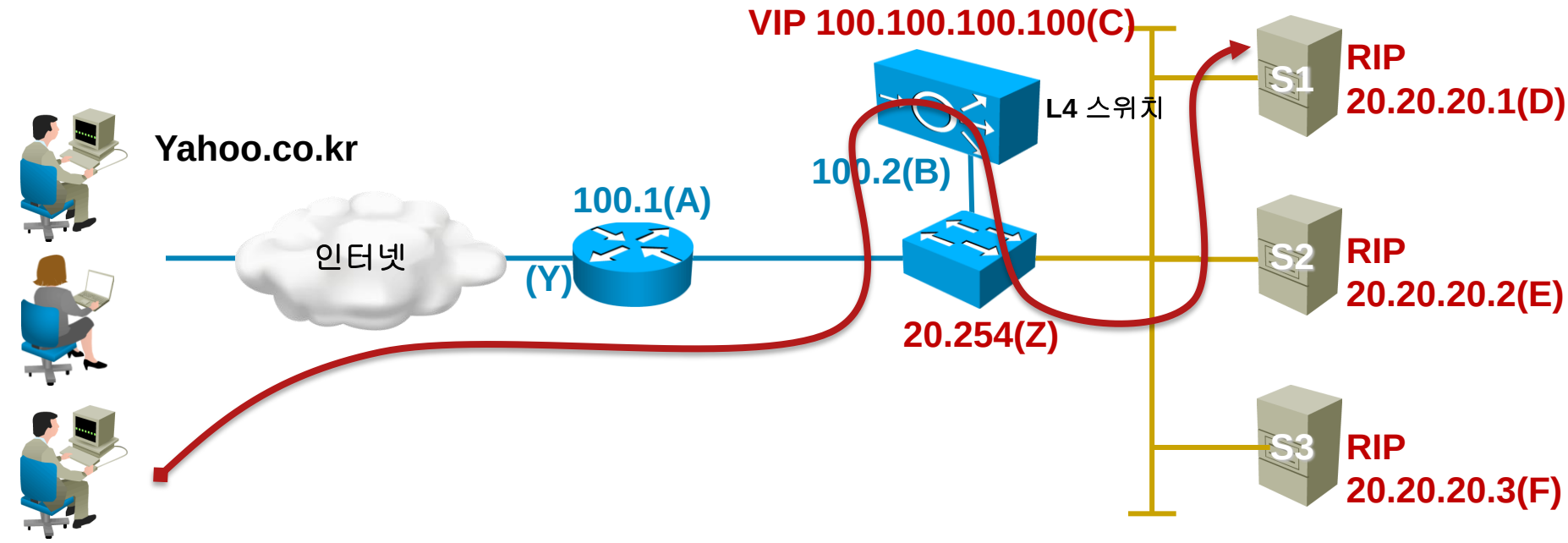


제2부

이제 좀 더 고급 기능 어플리케이션 스위치?

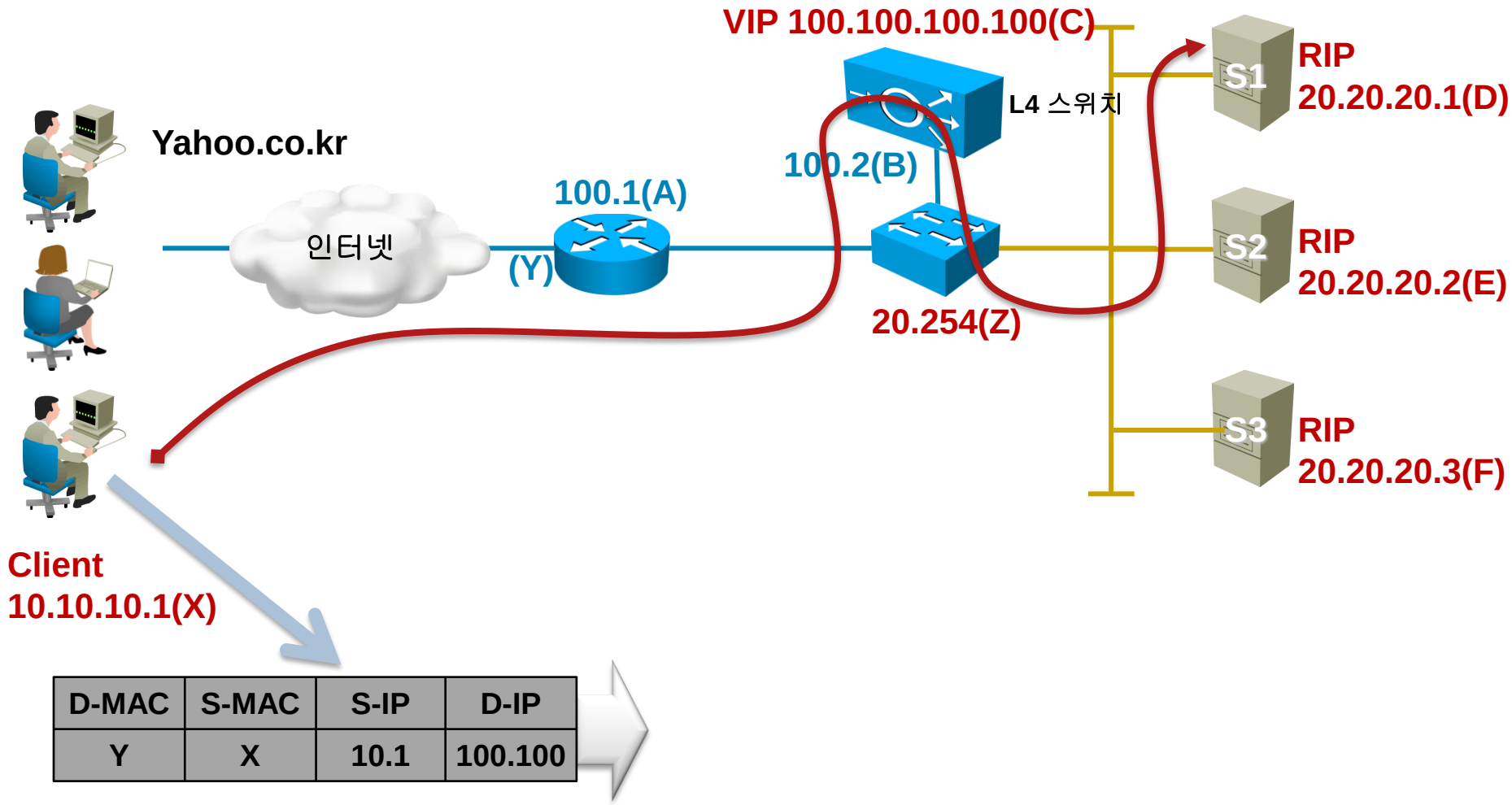
One - Arm 모드

- VIP로 들어 오는 패킷만을 관리함으로써, 네트워크 부하감소



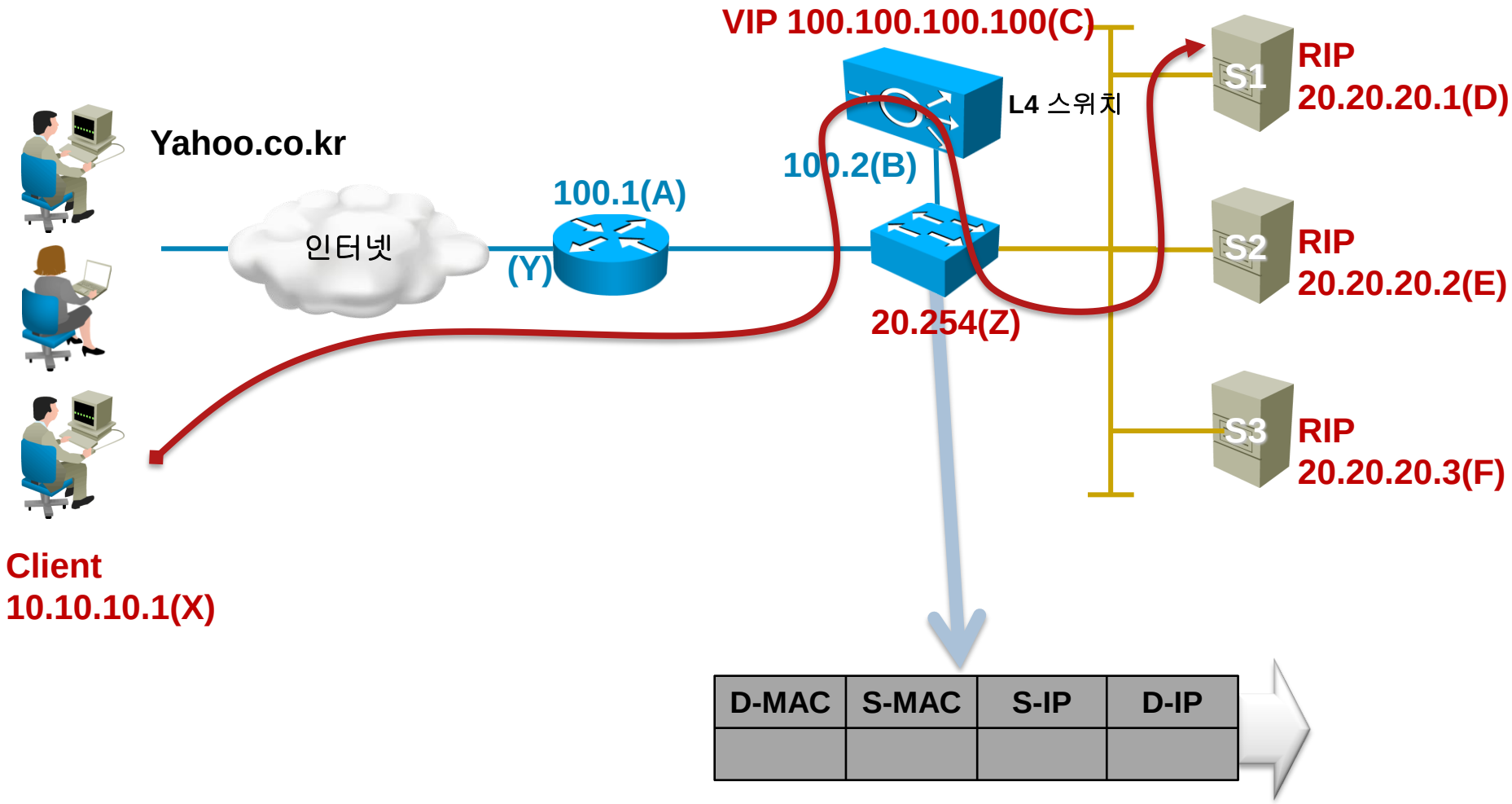
One - Arm 모드

- VIP로 들어 오는 패킷만을 관리함으로써, 네트워크 부하감소



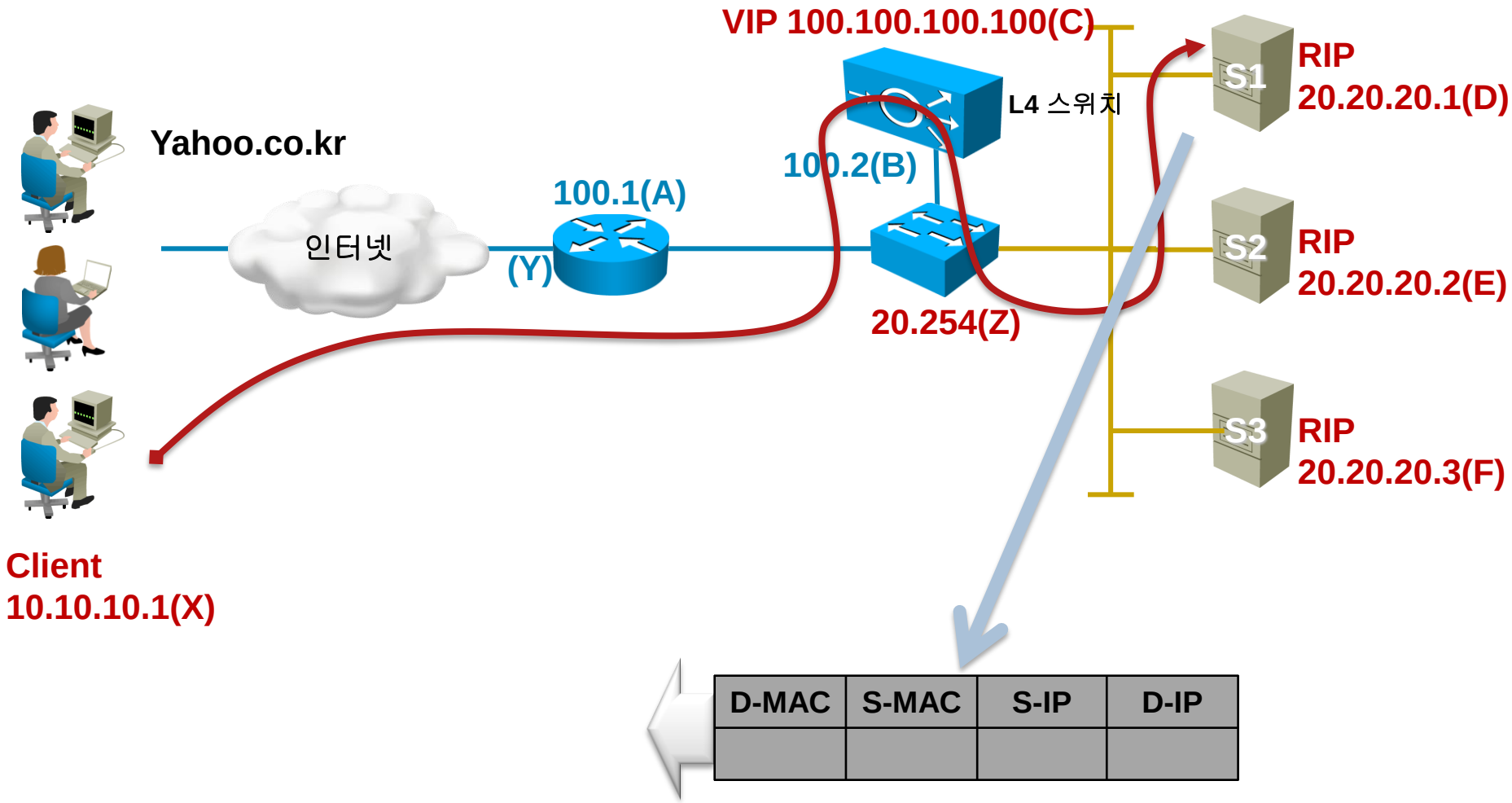
One - Arm 모드

- VIP로 들어 오는 패킷만을 관리함으로써, 네트워크 부하감소



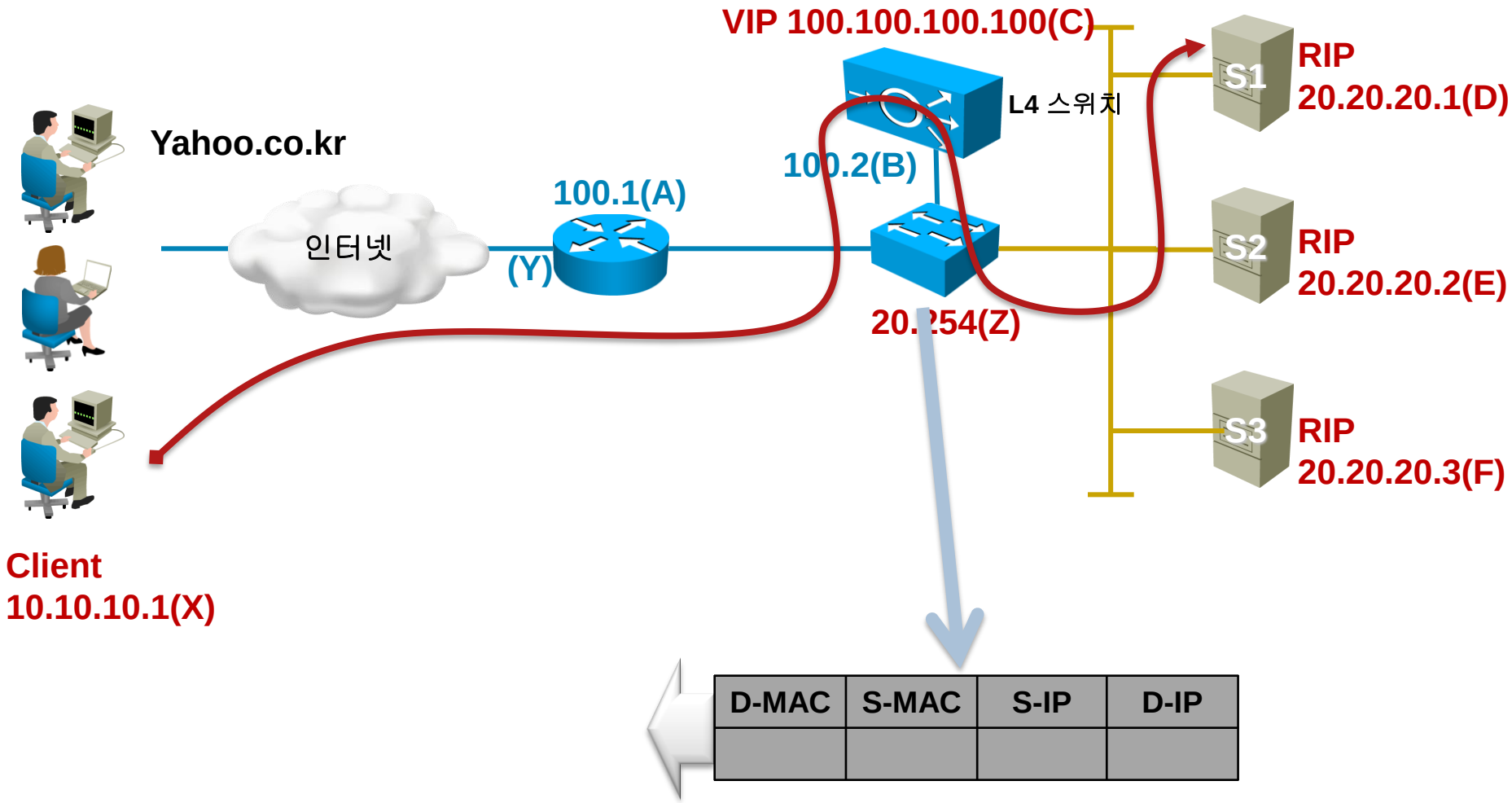
One - Arm 모드

- VIP로 들어 오는 패킷만을 관리함으로써, 네트워크 부하감소



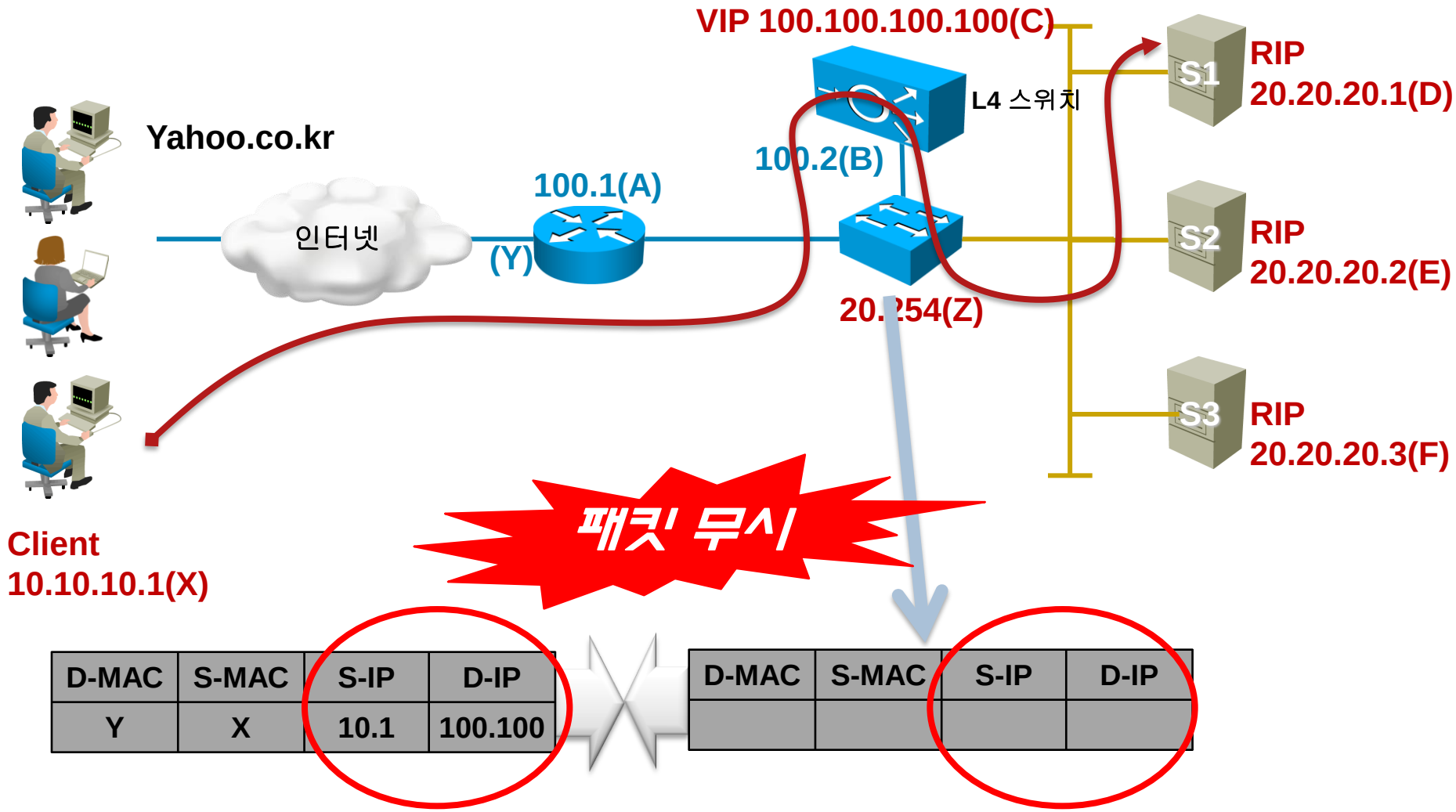
One - Arm 모드

- VIP로 들어 오는 패킷만을 관리함으로써, 네트워크 부하감소



One - Arm 모드

- 처음 보낸 패킷의 IP를 그대로 가져와야 정상 패킷 이라고 판단

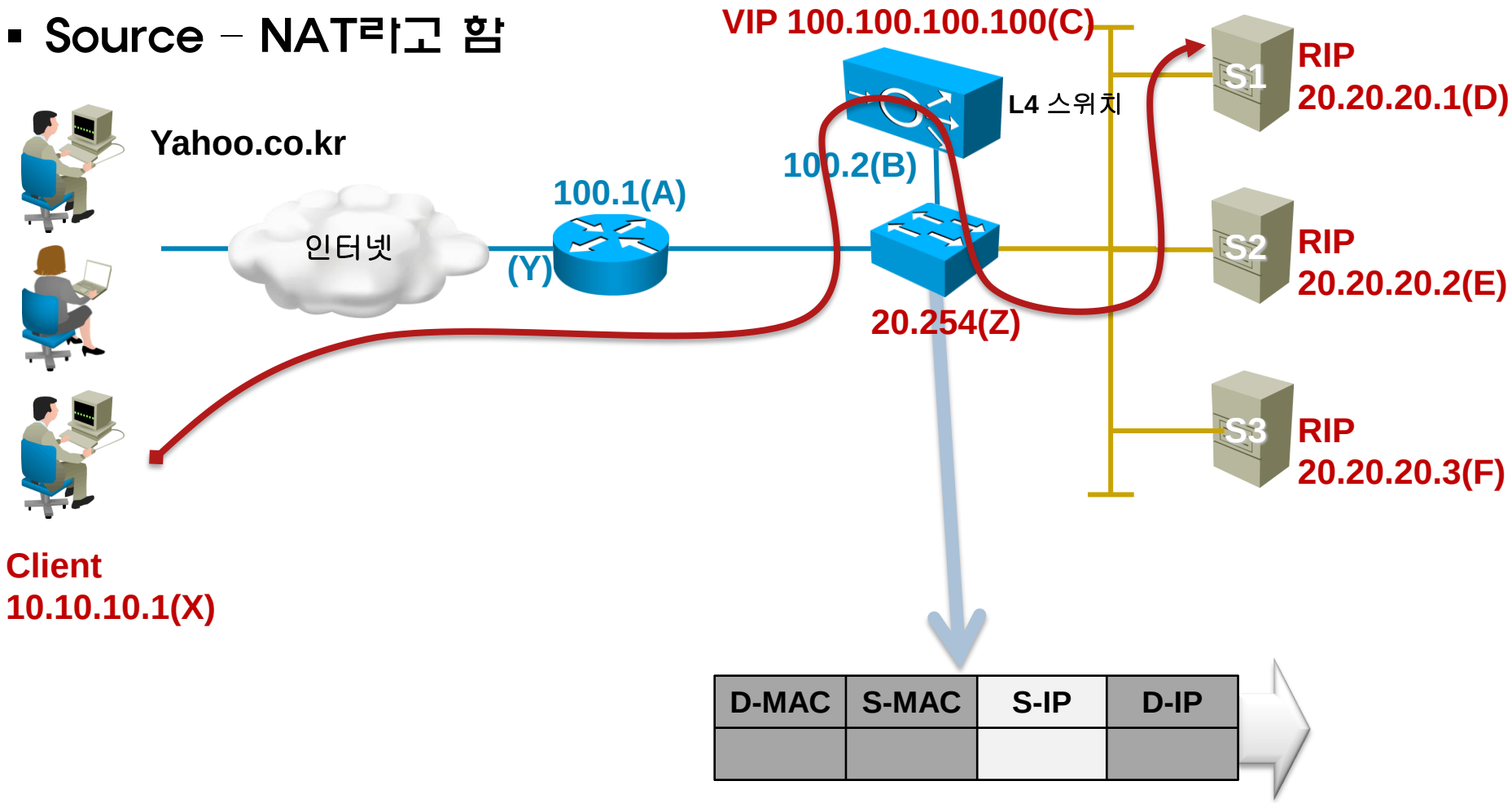


D-MAC	S-MAC	S-IP	D-IP
Y	X	10.1	100.100

D-MAC	S-MAC	S-IP	D-IP

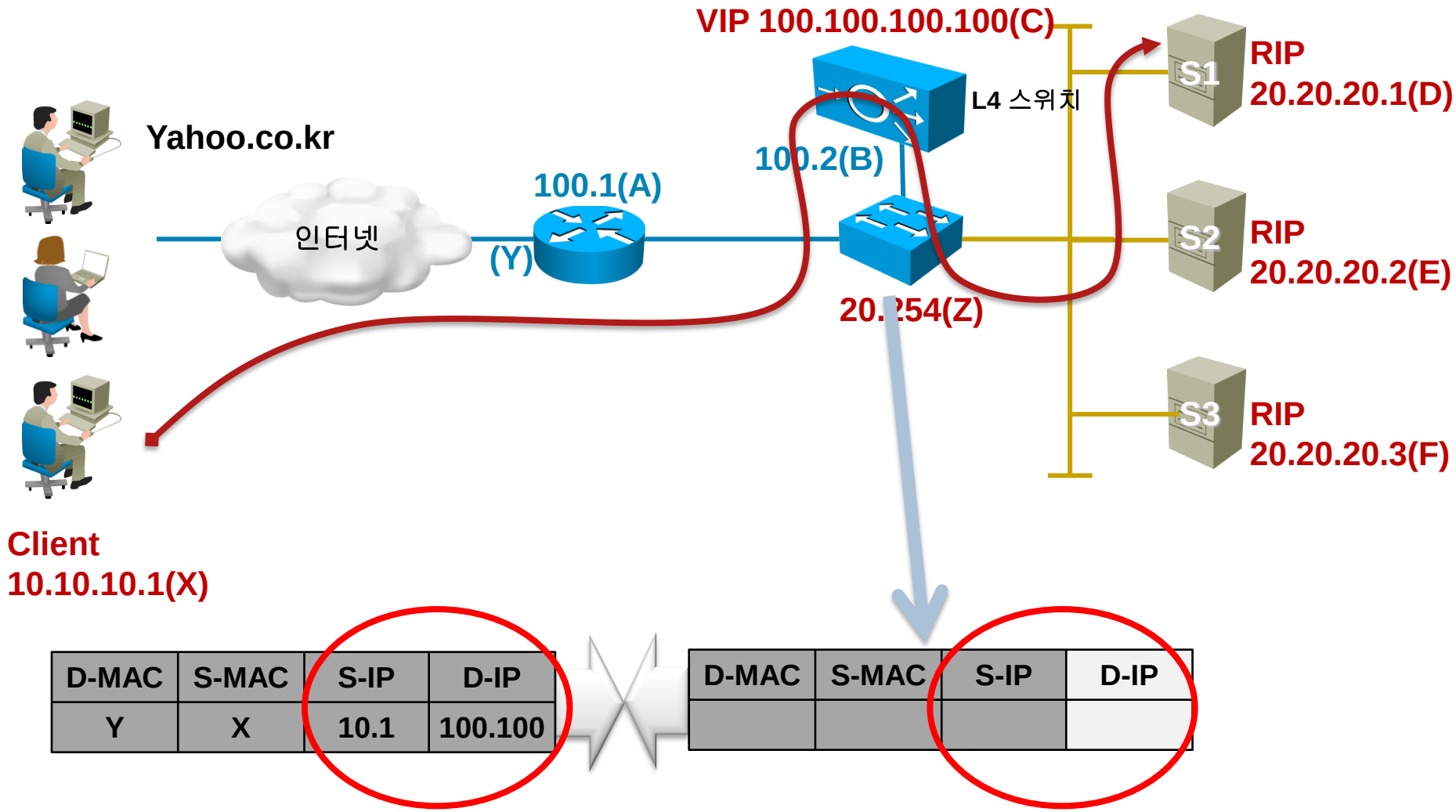
One - Arm 모드

- 그래서, 소스 IP를 변경해서 VIP로 변경해서 보낸다.
- Source – NAT라고 함



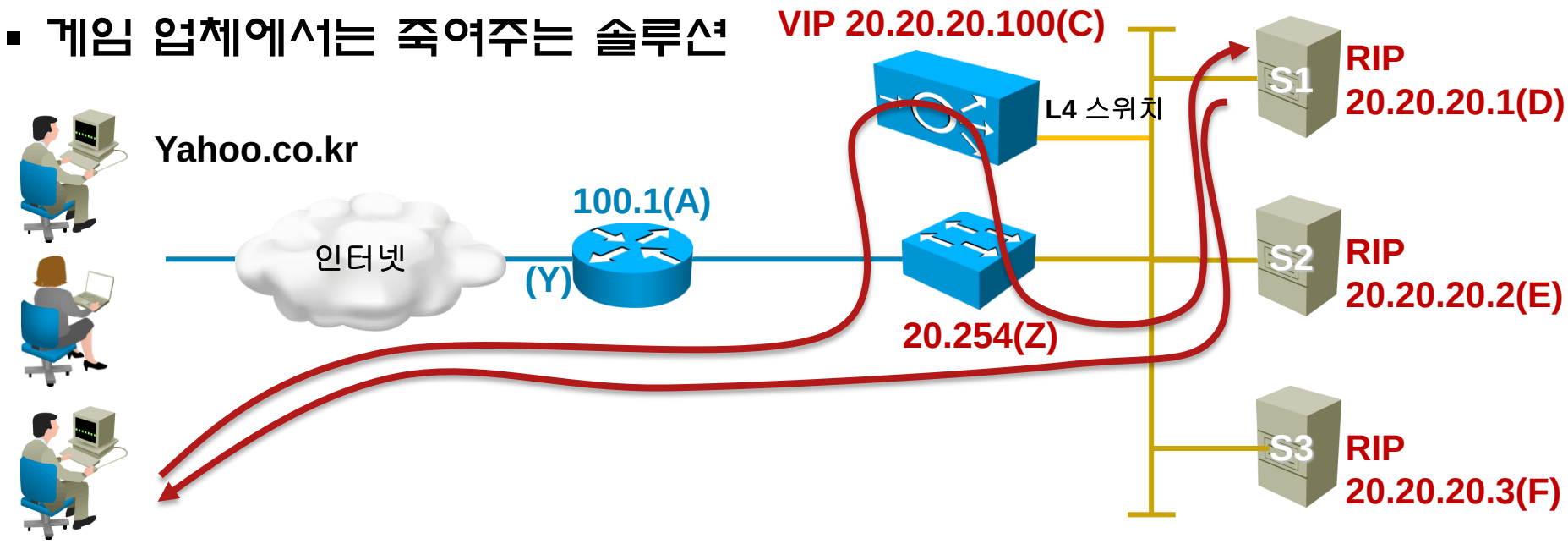
One - Arm 모드

- 처음 보낸 패킷의 IP를 그대로 가져와야 정상 패킷 이라고 판단



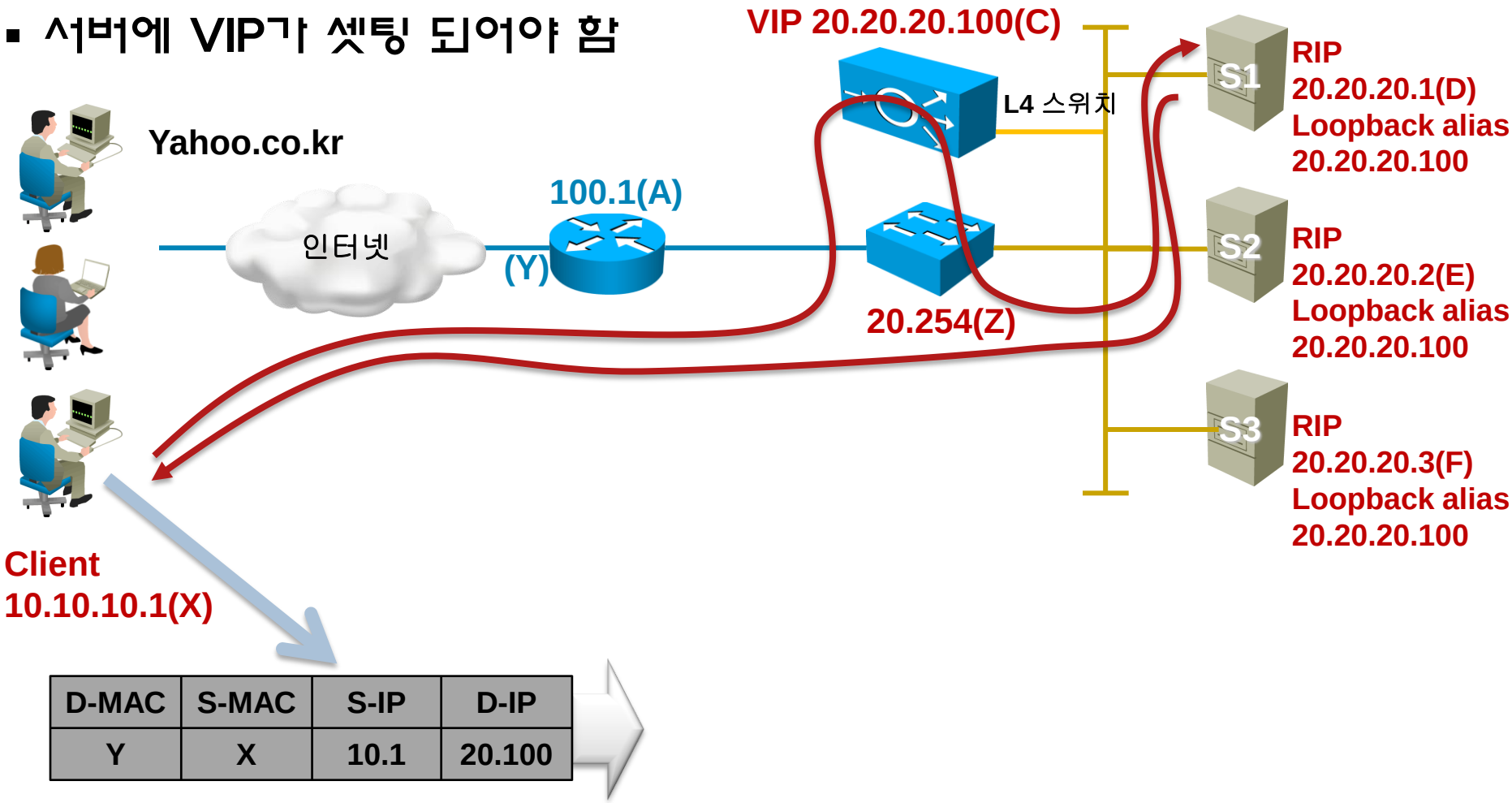
DSR (Direct Server Return)모드

- 클라이언트 응답하는 트래픽에 대해서 L4 스위치를 거치지 않음
- 게임 업체에서는 죽여주는 솔루션



DSR (Direct Server Return)모드

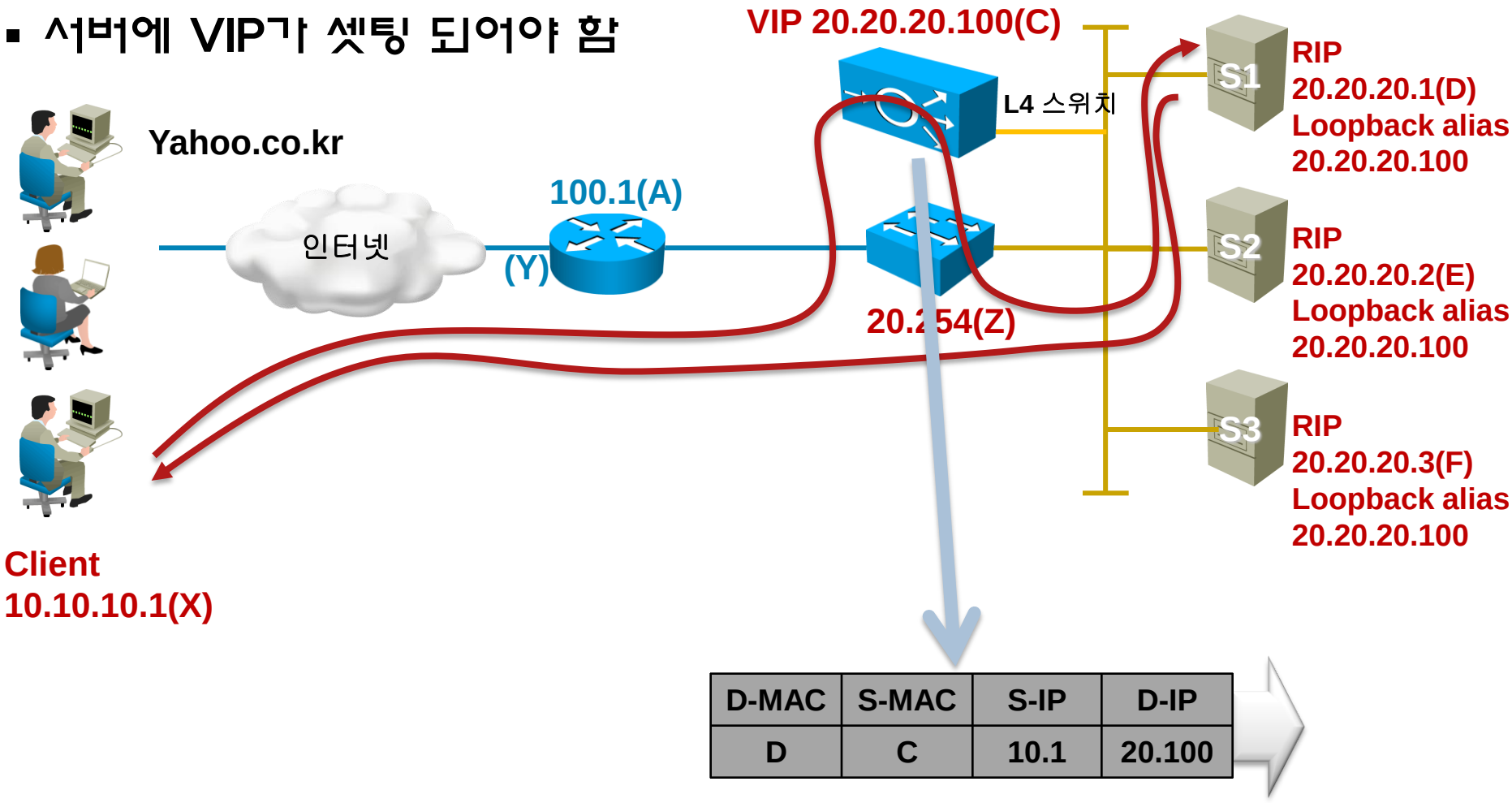
- Destination IP가 변화지 않는다.
- 서버에 VIP가 셋팅 되어야 함



D-MAC	S-MAC	S-IP	D-IP
Y	X	10.1	20.100

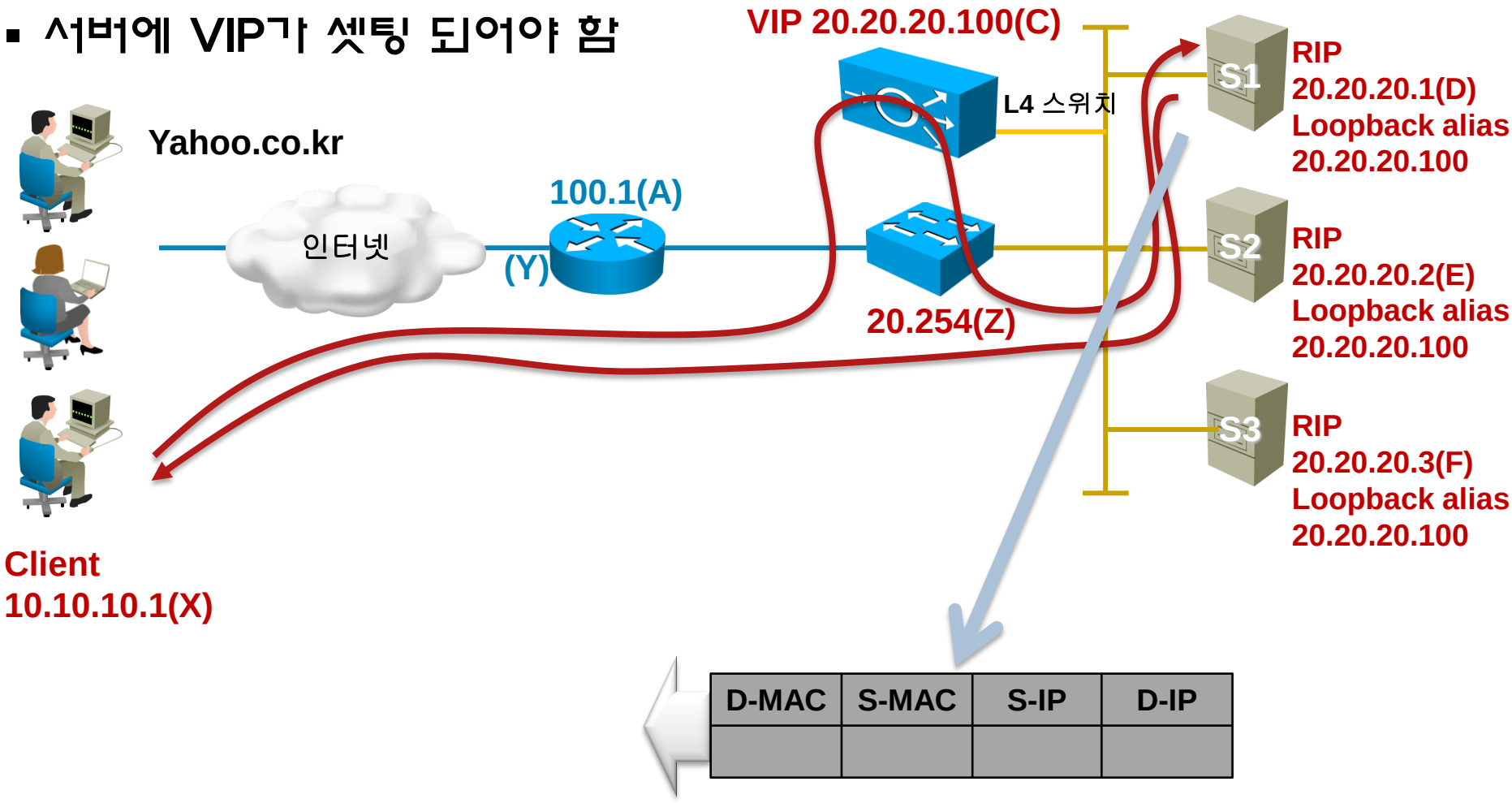
DSR (Direct Server Return)모드

- Destination IP가 변화지 않는다.
- 서버에 VIP가 셋팅 되어야 함



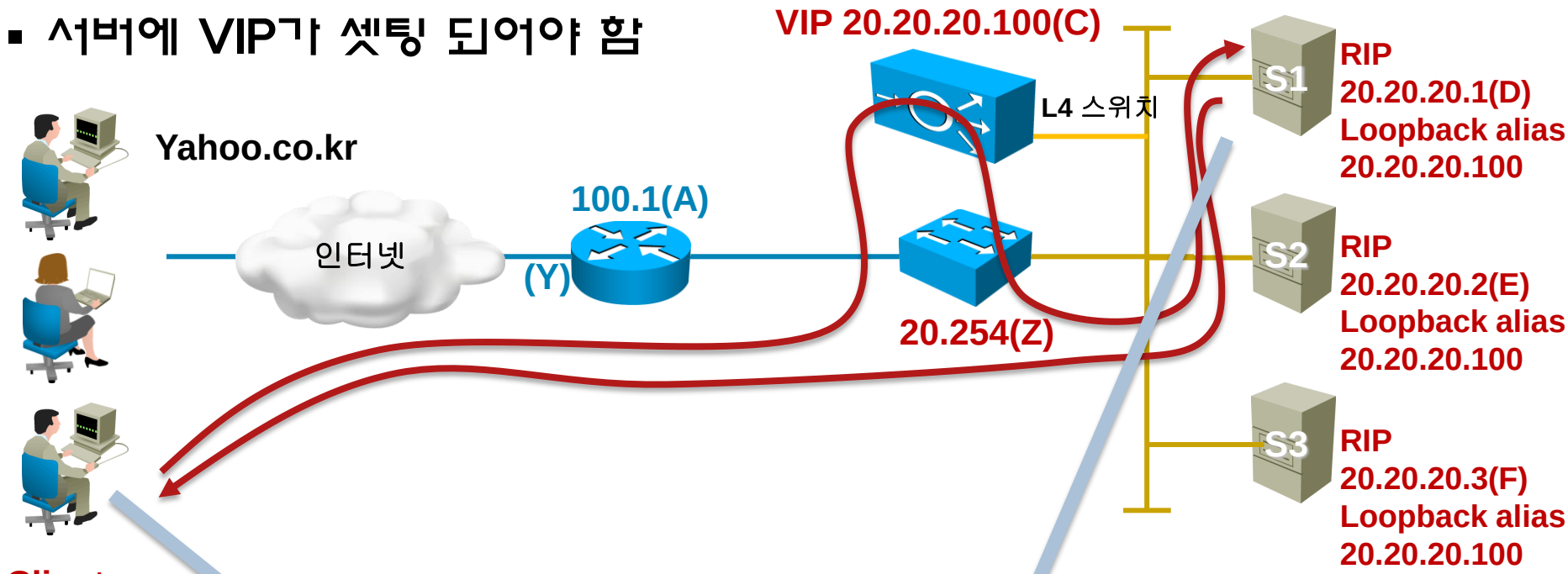
DSR (Direct Server Return)모드

- Destination IP가 변화지 않는다.
- 서버에 VIP가 셋팅 되어야 함



DSR (Direct Server Return)모드

- Destination IP가 변화지 않는다.
- 서버에 VIP가 셋팅 되어야 함

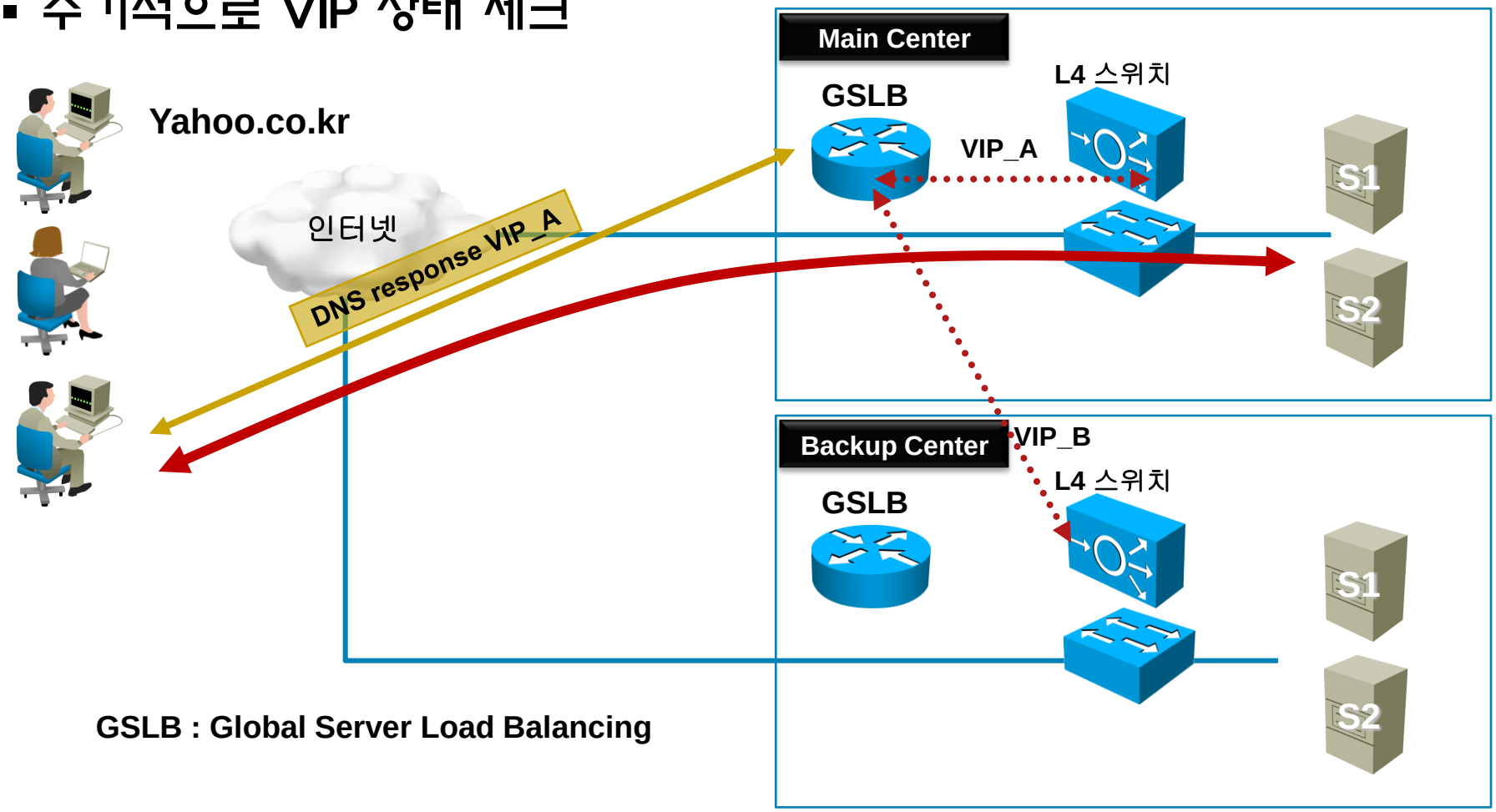


D-MAC	S-MAC	S-IP	D-IP
Y	X	10.1	20.100

D-MAC	S-MAC	S-IP	D-IP
Z	D		

Data Center 이중화 구성

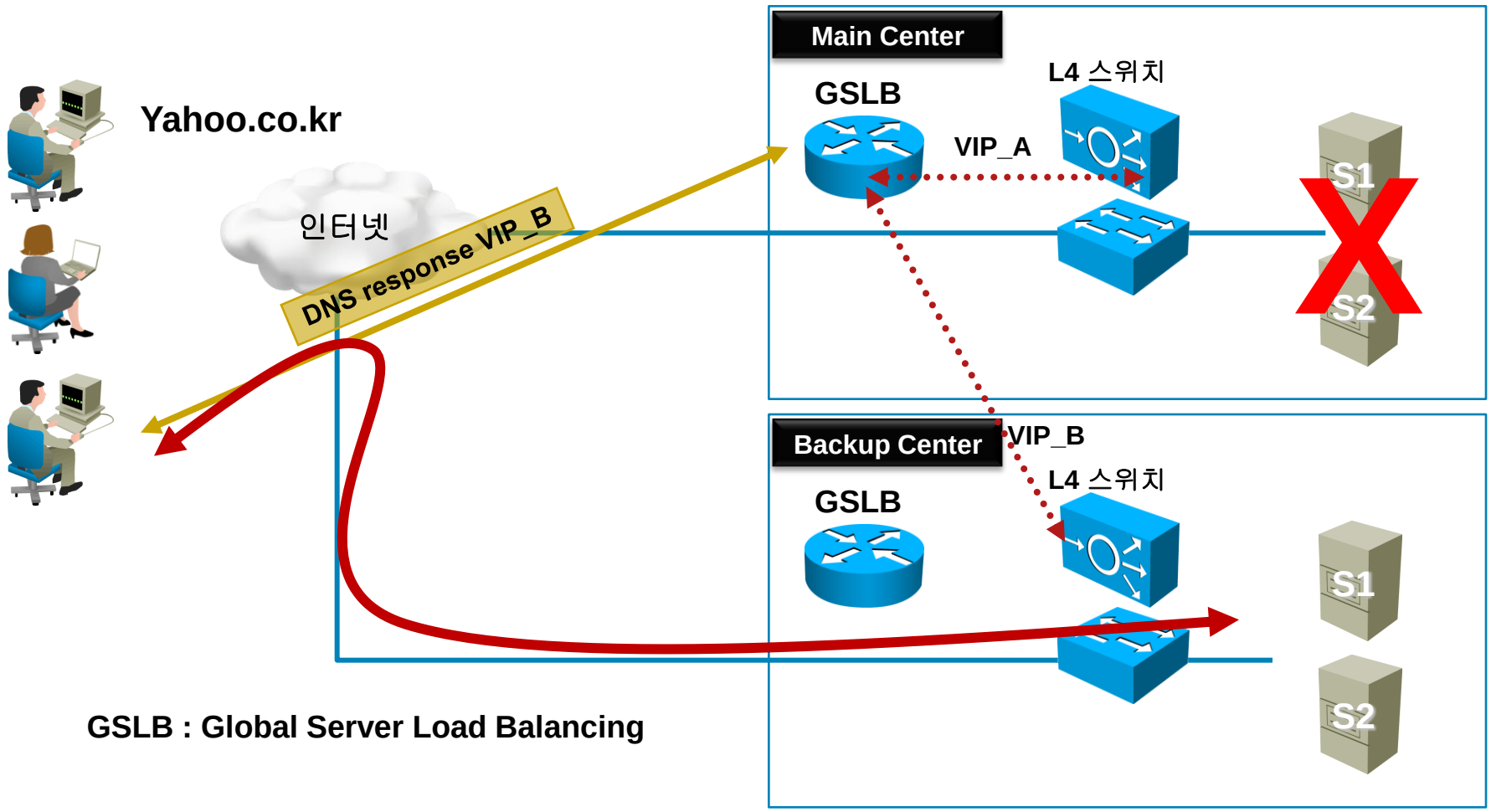
- 클라이언트 요청에 대해서 VIP_1으로 DNS Query에 대한 응답 수행.
- 주기적으로 VIP 상태 체크



GSLB : Global Server Load Balancing

Data Center 이중화 구성

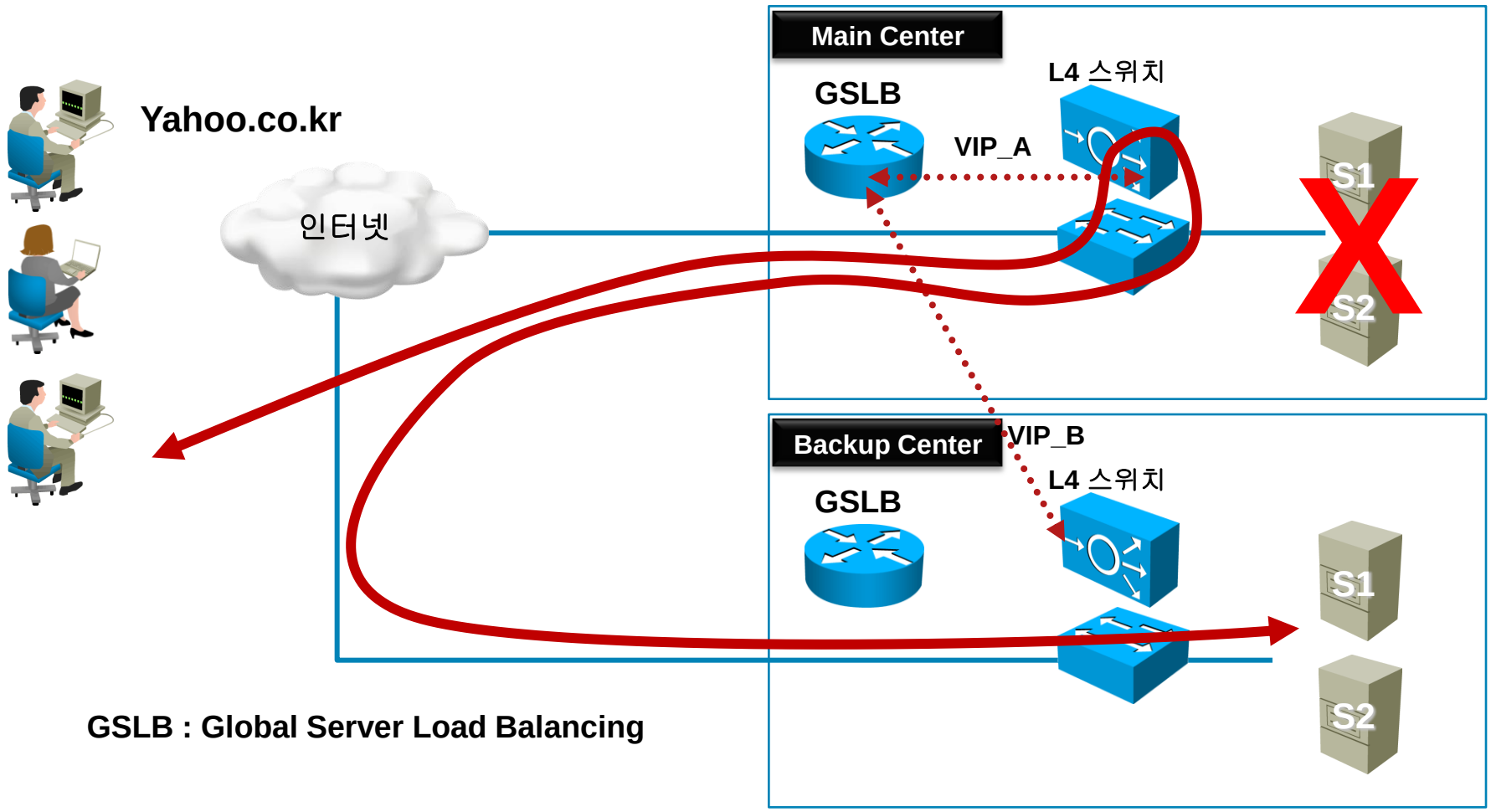
- 새로운 사용자 – VIP_2으로 DNS Query에 대한 응답 수행



GSLB : Global Server Load Balancing

Data Center 이중화 구성

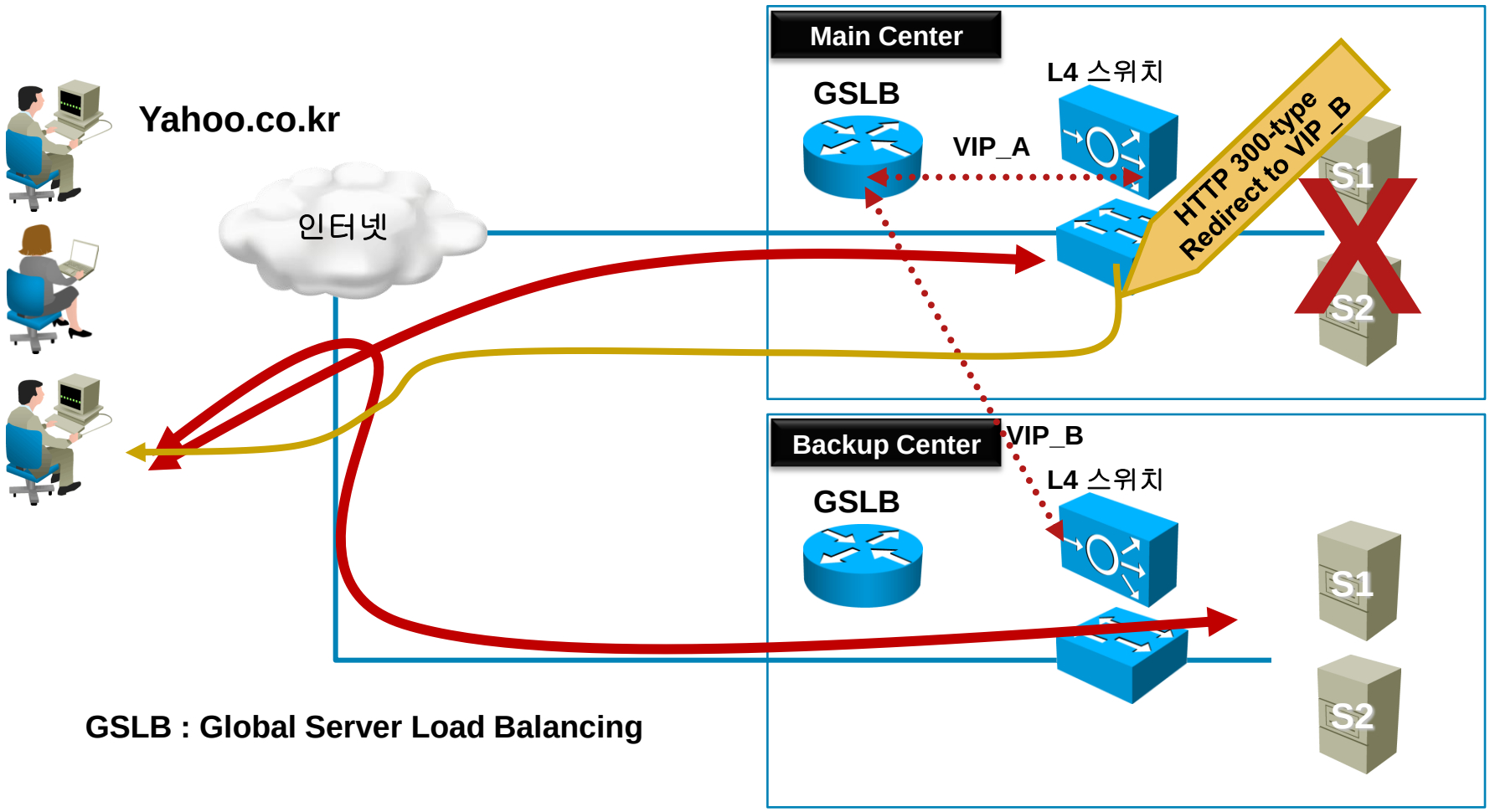
- 기존 사용자 – L4스위치에서 Source NAT 후 VIP_2 패킷 전송



GSLB : Global Server Load Balancing

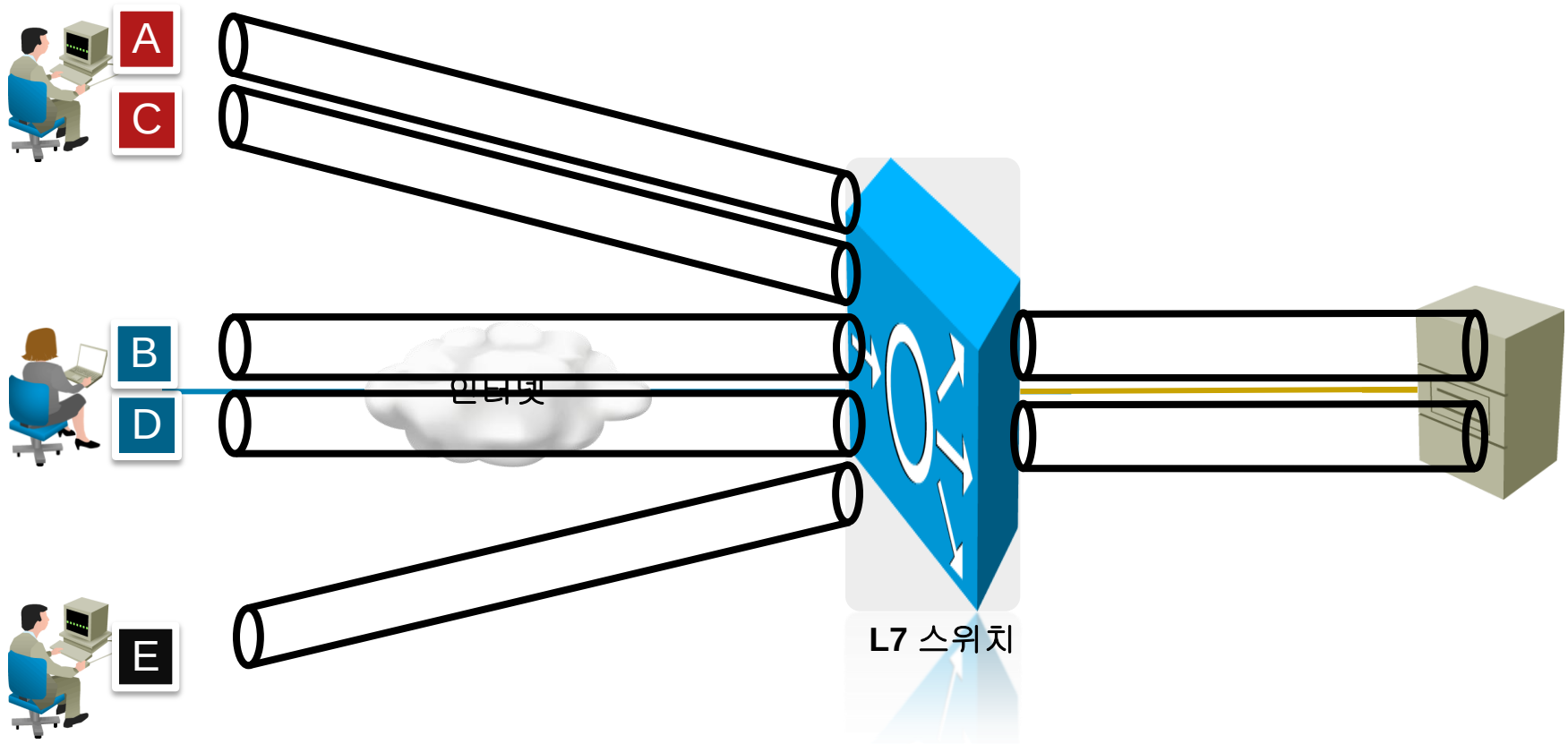
Data Center 이중화 구성

- 기존 사용자 – HTTP Redirect to VIP_B 기능 이용해서 서비스



TCP Offload

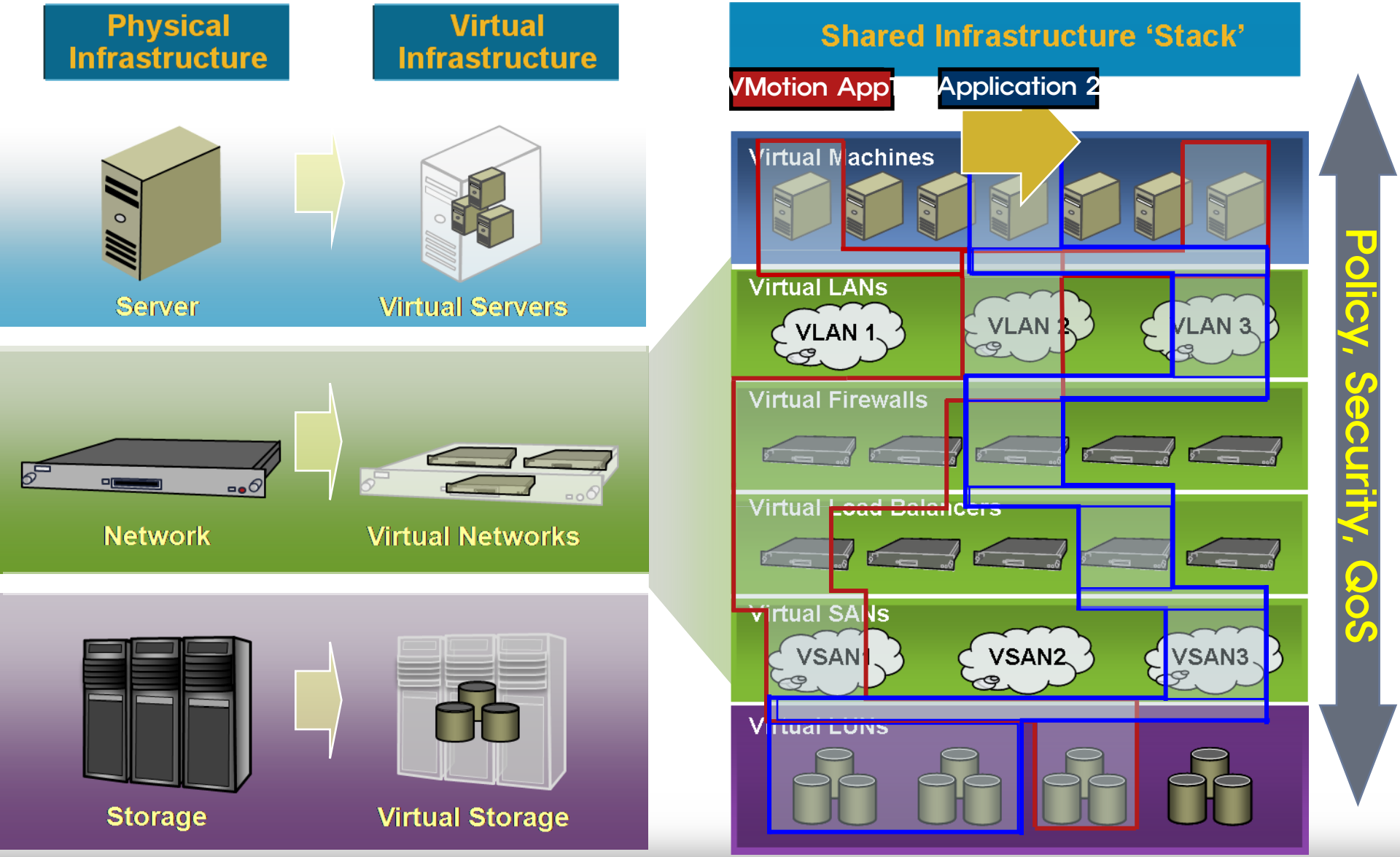
- TCP Connection 재활용을 통한 서버의 부하를 줄여보자



TCP Offload

- 테스트 결과 서버 자원의 놀라운 절약

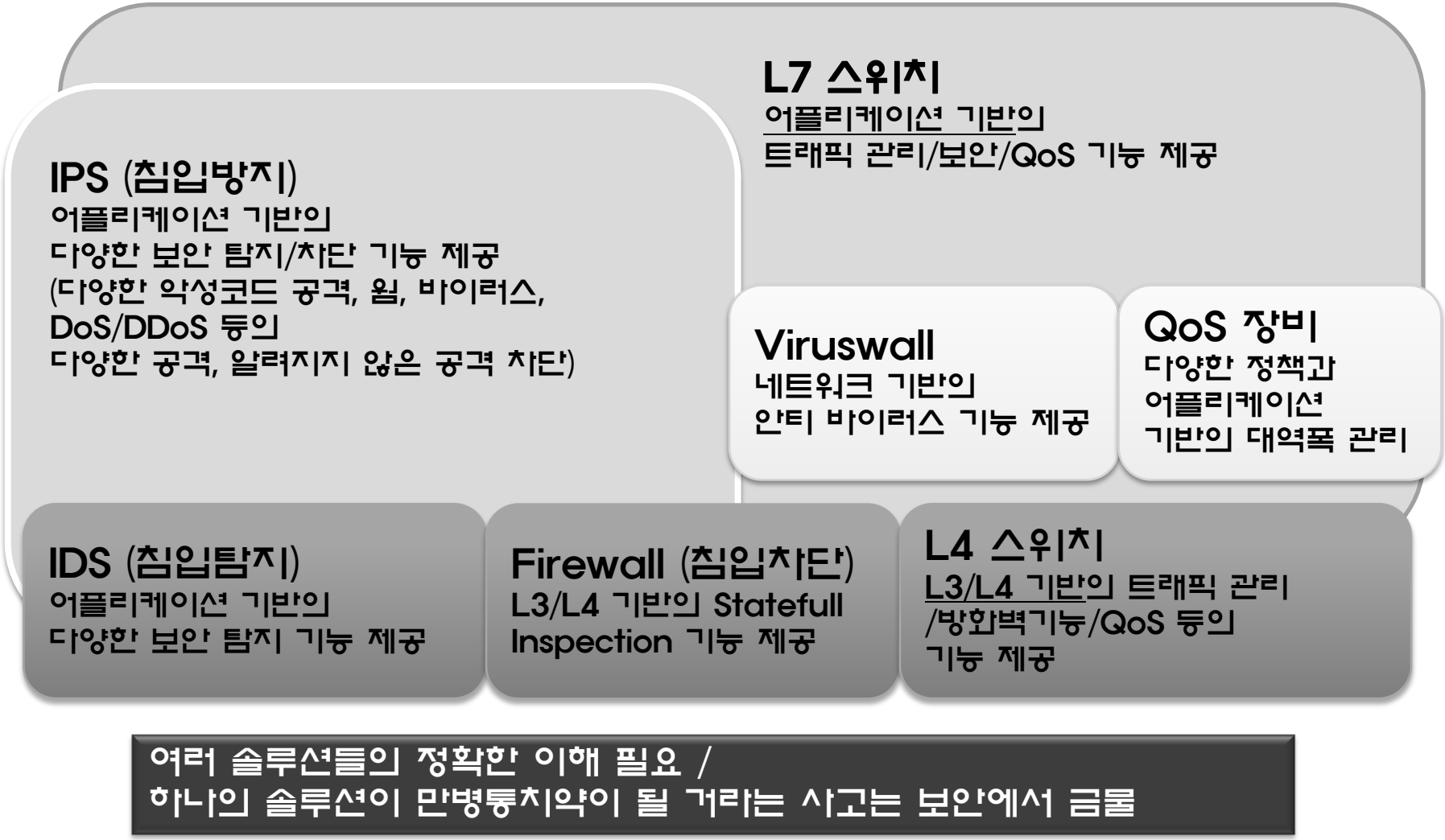
가상화(Virtualization)



제2부

아무리 강조해도 지나 치지 않는 보안!

L7 스위치와 만나는 보안 솔루션



여러 솔루션들의 정확한 이해 필요 /
하나의 솔루션이 만병통치약이 될 거라는 사고는 보안에서 금물

최근 DDoS 공격 특징

어떻게 방어 할 것인가 ?

참고_보안 솔루션 정리

구 분	주요기능	보안 기능	장/단점	비고
L3 스위치				
라우터				
L4 스위치				
방화벽				

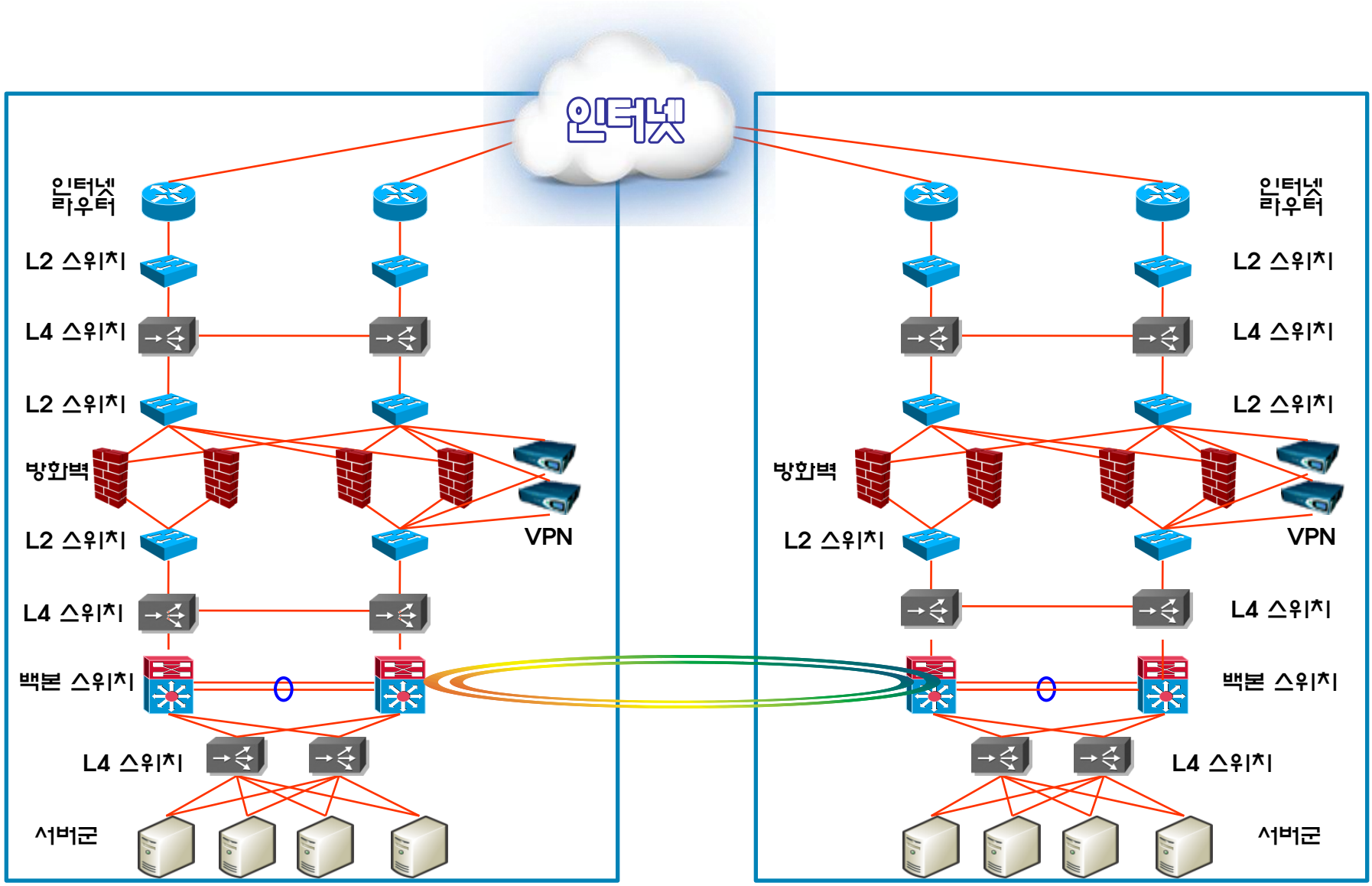
참고_보안 솔루션 정리

구 분	주요기능	보안 기능	장/단점	비고
IDS				
IPS				
Viruswall				
L7 스위치				
QoS				

제2부

마지막 정리

이제 단순해 보이시죠


인터넷
인터넷 라우터
L2 스위치
L4 스위치
L2 스위치
방화벽
VPN
L2 스위치
L4 스위치
백본 스위치
L4 스위치
서버군
인터넷 라우터
L2 스위치
L4 스위치
L2 스위치
방화벽
VPN
L2 스위치
L4 스위치
백본 스위치
L4 스위치
서버군

마지막 정리

돈 벼락 맞으세요 !!!