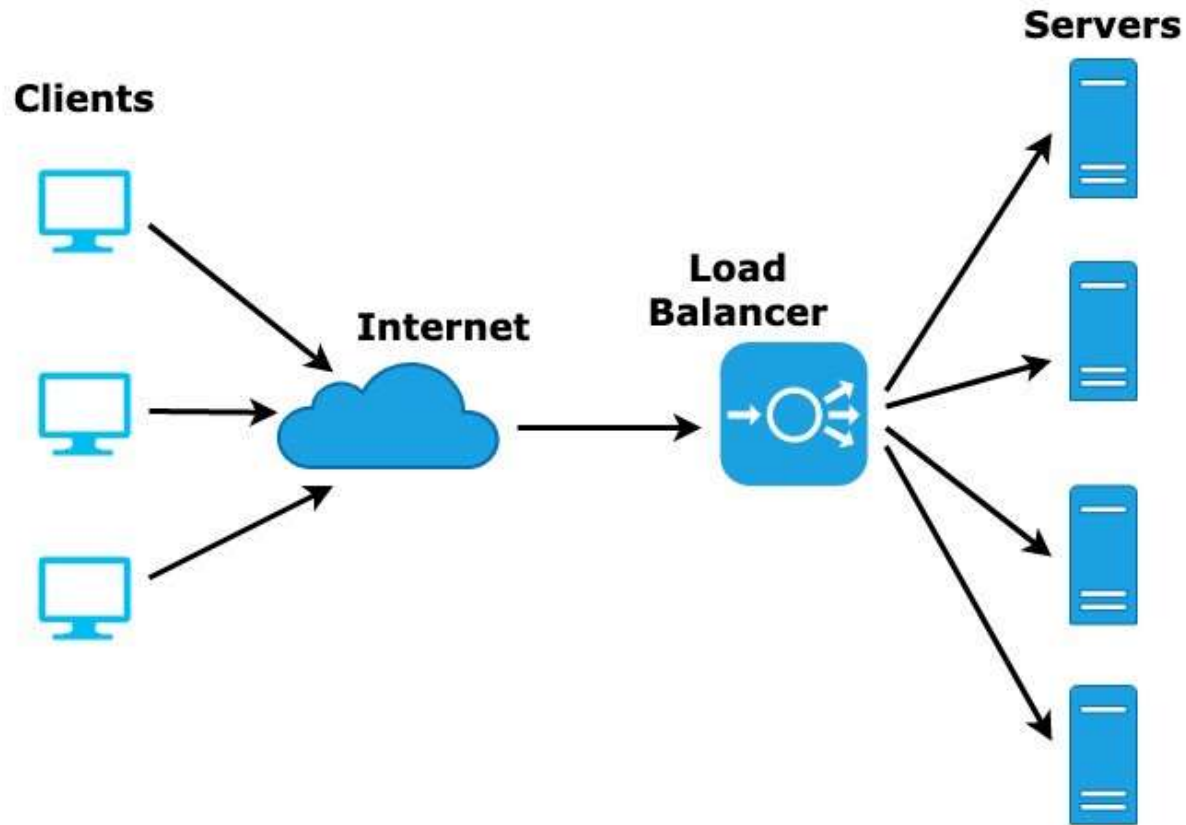


L4/L7 스위치 & 로드밸런싱

발표자료

로드밸런싱이란



여러 서버에 트래픽, 부하
분산 처리 시키는 것

Virtual IP 가진 가상 서버
로 동작

클라이언트 요청 전달 받음

클라이언트와 실제 서버
중계 역할

로드밸런서 장점

1.부하 분산:

트래픽 여러 서버로 균등하게 분산해 서버의 과부하 방지, 시스템 전체의 성능 향상

2.고가용성:

여러 대의 서버 관리해 한 대의 서버에 장애 발생해도 다른 서버로 요청 전달 가능

3.확장성:

서버 추가 or 제거 경우 로드밸런서가 자동으로 감지해 트래픽 분배

로드밸런서 주요 기능

1. 헬스 체크:

- 서버에 대한 주기적인 상태확인 통해 장애 여부 판단
- 정상 동작 중인 서버로만 트래픽 배분

2. 터널링:

- 데이터 스트림을 인터넷 상에서 가상의 파이프 통해 전달 시키는 기술
- 연결된 상호 간에만 캡슐화 된 패킷 구별해 캡슐화 해제하게 함

3. NAT:

- IP주소 변환해주는 기술
- 내부에서 외부로 나가는 경우에는 SNAT
- 외부에서 내부로 트래픽이 들어오는 경우에는 DNAT

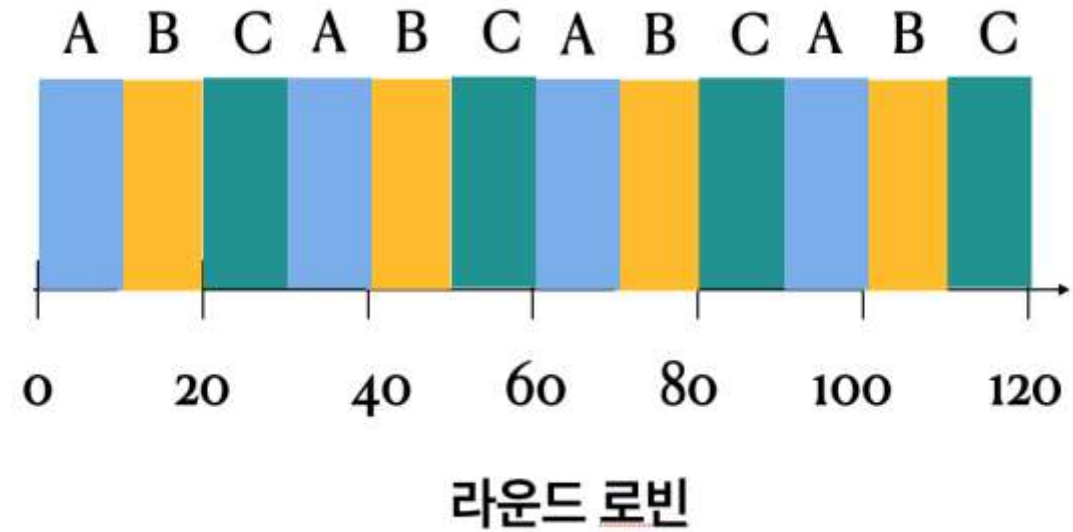
4. DSR:

- 서버에서 클라이언트로 갈 때 네트워크 장비나 로드밸런서 거치지 않고 바로 클라이언트 찾아가는 방식
- 로드밸런서의 부하 줄여줌

로드밸런서 알고리즘

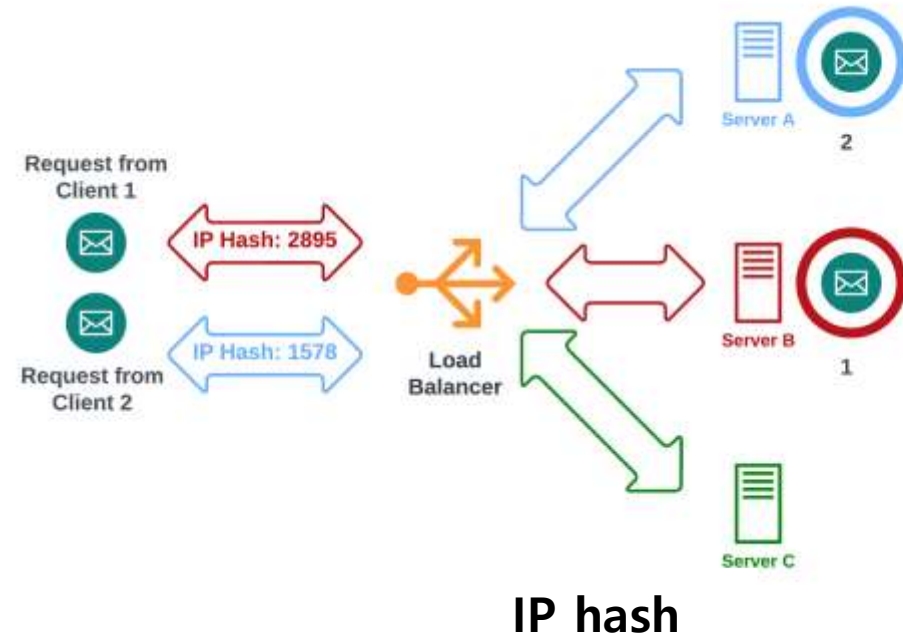
- 정적 로드밸런싱

- 라운드 로빈 방식
- 가중치 기반 라운드 로빈 방식
- IP 해시 방식

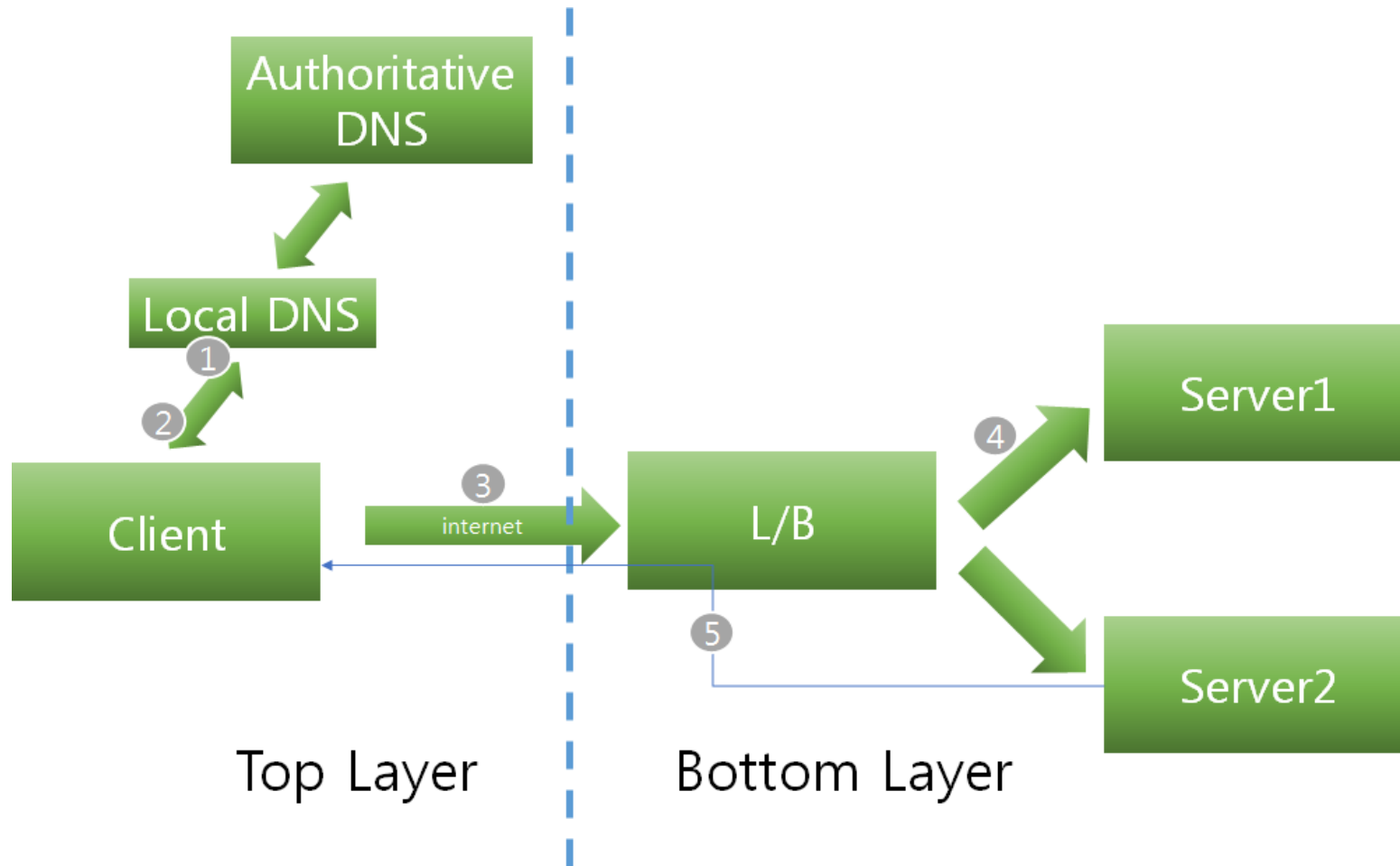


- 동적 로드밸런싱

- 최소 연결 방법
- 가중치 기반 최소 연결 방법
- 최소 응답 시간 방법
- 리소스 기반 방법



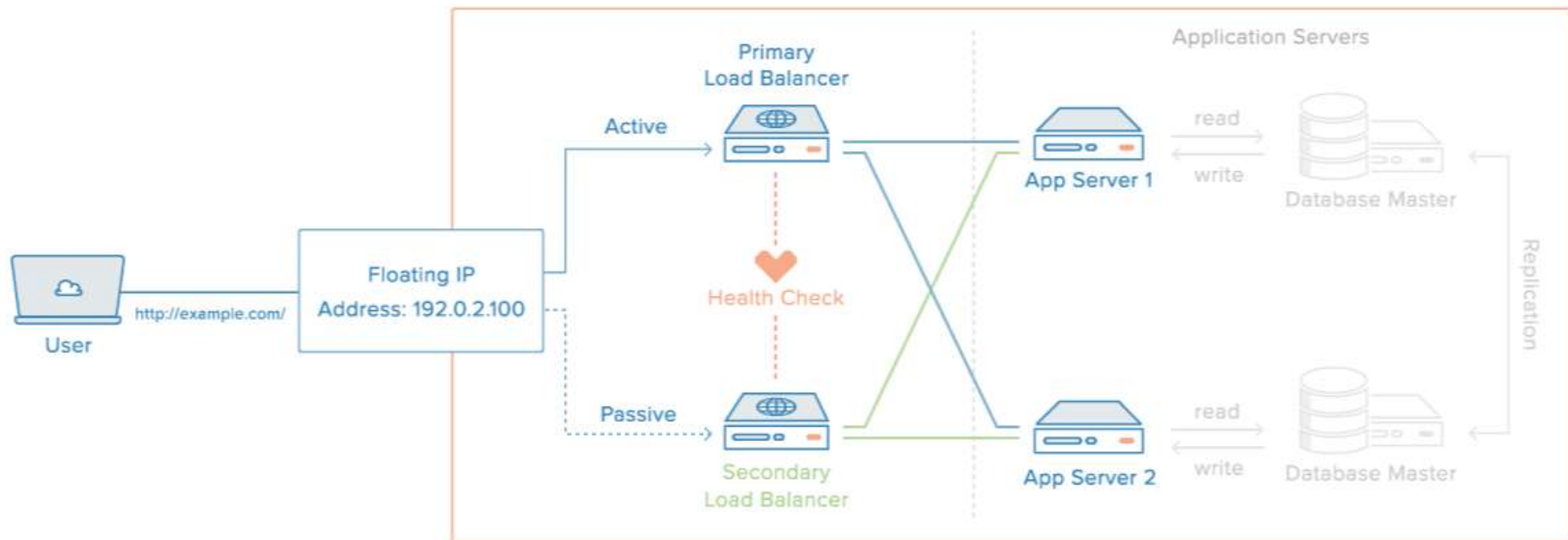
로드밸런서 동작 방식



Mode

1. Bridge/Transparent mode
2. Router mode
3. One Arm mode
4. DSR (Direct Server Return) mode

로드밸런서 장애 대비



- 1 Active/Passive Cluster is healthy
- 2 Primary node fails
- 3 Floating IP is assigned to Secondary node

L4 스위치

- L4 스위치는 Transport Layer에서 동작하는 기능을 제공하며 로드밸런싱 역할을 하는 스위치
- 클라이언트 요청의 TCP/UDP 프로토콜 패킷 헤더(IP, PORT) 기반으로 Source, Destination IP 변조해 다중화된 서버와 중계해주는 역할
- 애플리케이션의 트래픽 패턴 분석해 QoS(Quality Of Service) 정책을 적용하거나, 특정 IP주소 혹은 포트로의 접근을 제어 가능
- 주로 Round Robin 방식 사용

L7 스위치

- L7 스위치는 L4 스위치의 기능을 포함하는 것뿐만 아니라 애플리케이션 계층(HTTP, SMTP, FTP)의 정보 바탕으로도 분산 처리 가능
- 트래픽 내용(URI, Payload, Cookie, HTTP 헤더 등) 직접 분석할 수 있어 L4 스위치보다 정교한 로드밸런싱에 사용
- L4 스위치에 비해 자원의 소모가 큼
- 특정한 패턴 지닌 바이러스 감지해 네트워크 보호할 수 있음
- DoS/DDoS와 같은 비정상적인 트래픽을 필터링할 수 있어 네트워크 보안 분야에서도 활용됨

L4 스위치 VS L7 스위치

	L4 로드밸런서	L7 로드밸런서
네트워크 계층	Layer 4 전송계층(Transport layer)	Layer 7 응용계층(Application layer)
특징	> TCP/UDP 포트 정보를 바탕으로 함	> TCP/UDP 정보는 물론 HTTP의 URI, FTP의 파일명, 쿠키 정보 등을 바탕으로 함
장점	> 데이터 안을 들여다보지 않고 패킷 레벨에서만 로드를 분산하기 때문에 속도가 빠르고 효율이 높음 > 데이터의 내용을 복호화할 필요가 없기에 안전함 > L7 로드밸런서보다 가격이 저렴함	> 상위 계층에서 로드를 분산하기 때문에 훨씬 더 섬세한 라우팅이 가능함 > 캐싱 기능을 제공함 > 비정상적인 트래픽을 사전에 필터링할 수 있어 서비스 안정성이 높음
단점	> 패킷의 내용을 살펴볼 수 없기 때문에 섬세한 라우팅이 불가능함 > 사용자의 IP가 수시로 바뀌는 경우라면 연속적인 서비스를 제공하기 어려움	> 패킷의 내용을 복호화해야 하기에 더 높은 비용을 지불해야 함 > 클라이언트가 로드밸런서와 인증서를 공유해야하기 때문에 공격자가 로드밸런서를 통해서 클라이언트에 데이터에 접근할 보안 상의 위험성이 존재함