한·미 SDN Testbed 구축 경험 및 현 상황

남 재 현 (박사과정)
한국과학기술원
namjh@kaist.ac.kr

SDN 테스트베드 구축

- 국외 SDN 테스트베드
  - NSF의 GENI (Global Environment for Network Innovations)
  - Internet2의 NDDI (100G OpenFlow/SDN Innovation Platform)
  - EU의 OFELIA (European project providing OpenFlow-based experimental facilities)
  - 일본의 JGN-X (Japan Gigabit Network–X)

- 국내 SDN 테스트베드
  - 광대역통합연구개발망(KOREN) → 고도화 사업의 일환으로 SDN 도입
  - 국가과학기술연구망(KREONET) → SDN 기반 KREONET-S

- 많은 기업들 역시 자체 SDN 테스트베드 구축

SDN 안전성 연구를 위한 테스트베드

- 지금까지의 SDN 테스트베드
  - 서비스 위주의 테스트베드
  - SDN 기술을 활용한 연구 및 검증을 위한 테스트베드

- SDN 안전성 연구를 위한 테스트베드의 부재
  - SDN 기술 연구와 SDN 안전성 연구를 목적 자체가 다름
  - 현 SDN 테스트베드는 SDN 내 각각의 구성요소에 대한 안전성 연구에는 부적합

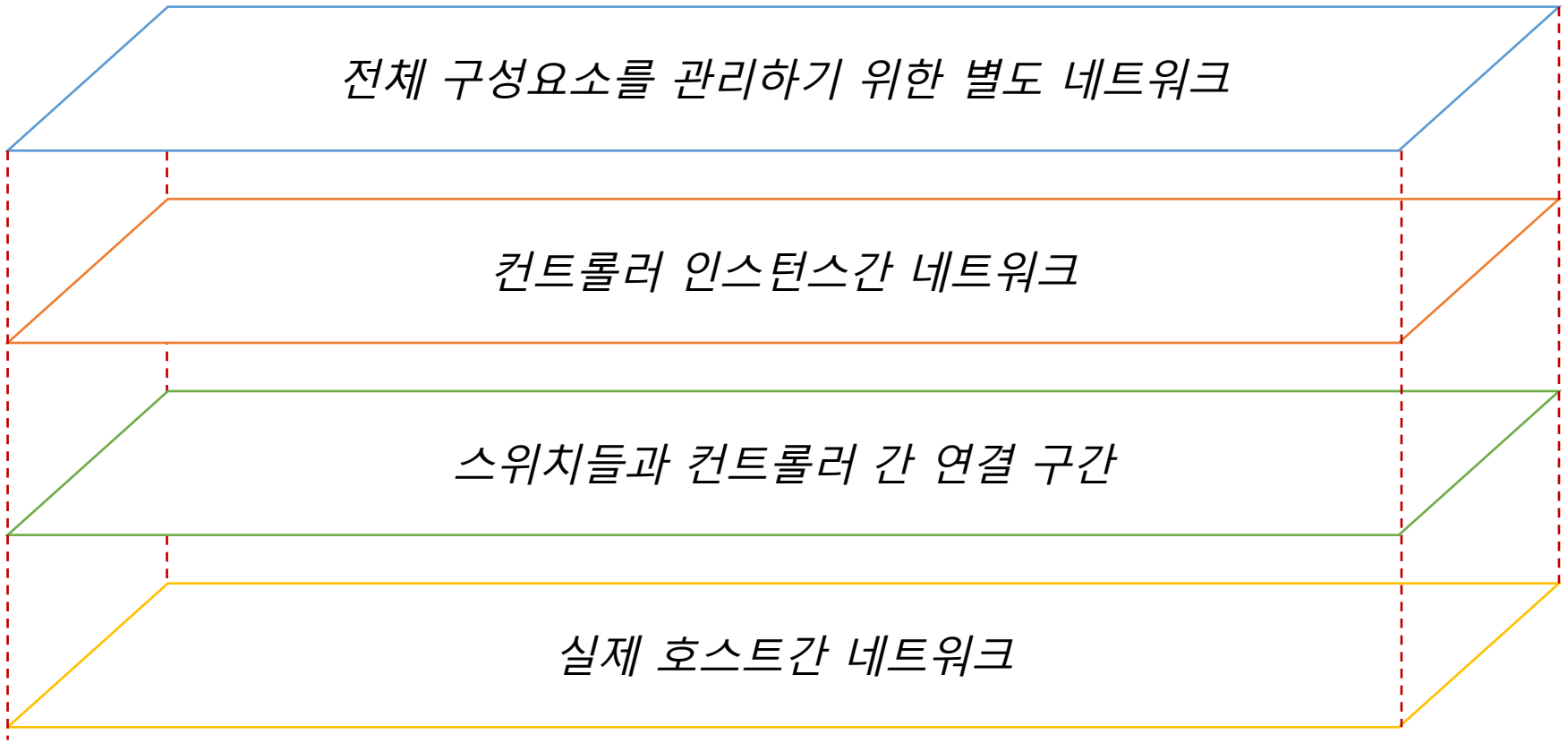
- SDN 자체의 안전성 연구를 위해서는 별도의 테스트베드가 필요함

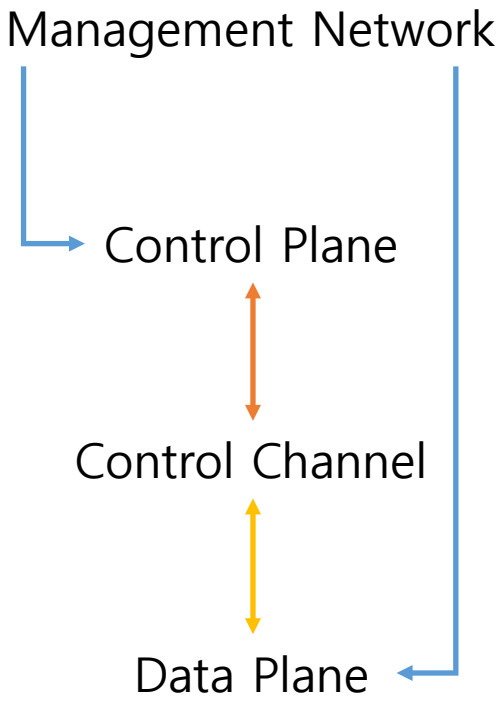
한·미 SDN 테스트베드 목적

- 독립적인 실험 환경
  - 실험 중 발생하는 내부 트래픽 격리(예: DoS 트래픽)
  - 실험 중 발생할 수 있는 네트워크 문제에 대한 복구
- 유연한 테스트베드 구성
  - 실험 목적에 따른 테스트베드 내부 구성 변경
- 물리 장비를 이용한 연구 수행
  - 실제 네트워크와 유사한 환경 재현
  - 가상 환경에서 확인할 수 없던 실제 네트워크 장비들로 인한 문제점 파악
- 다국간 테스트베드 연동
  - 지리적으로 분리된 네트워크 환경에 대한 다양한 연구 수행

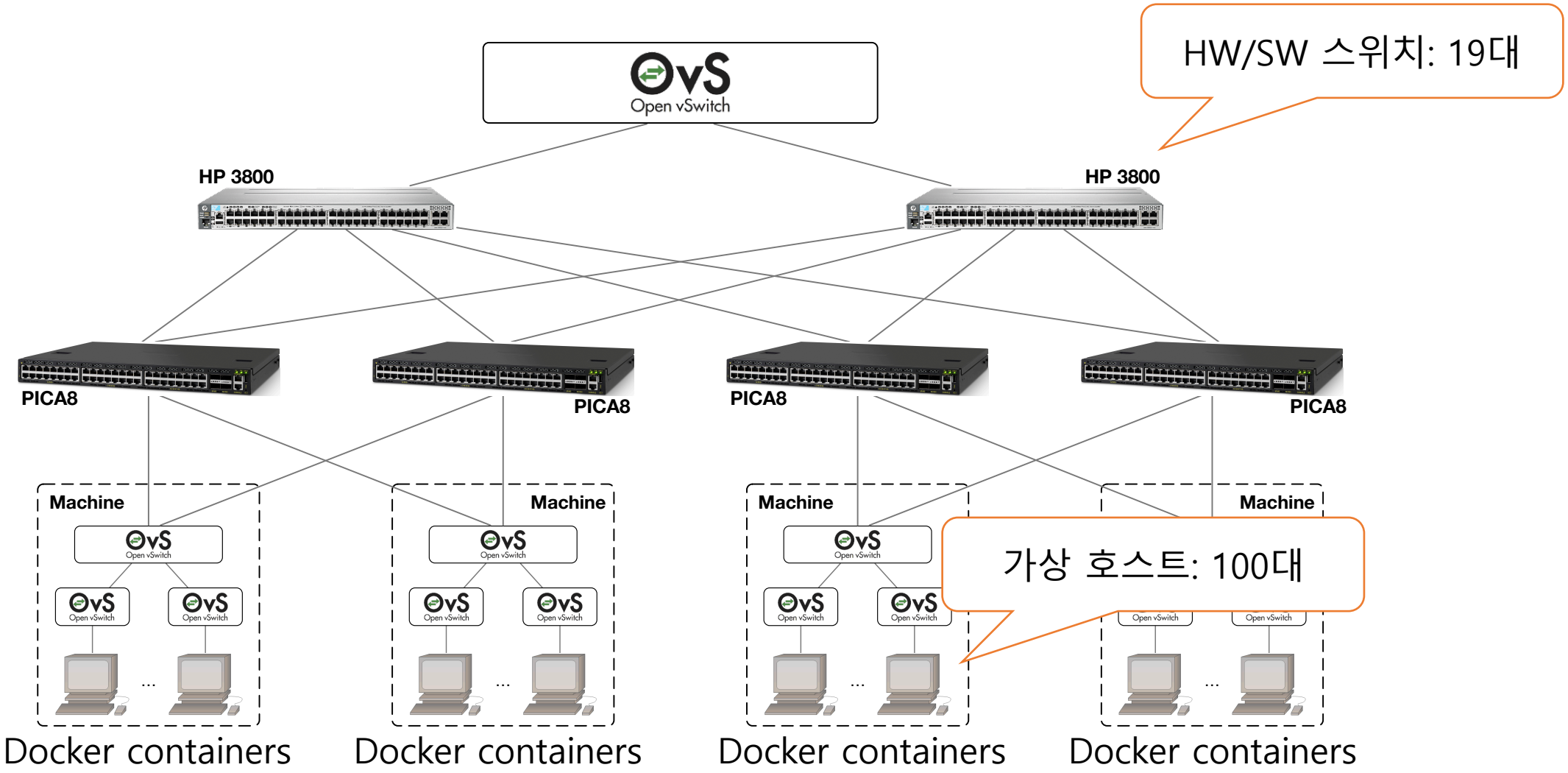
테스트베드 내 네트워크 구성

- 다양한 연구를 위해 4개의 레이어로 네트워크 구성함

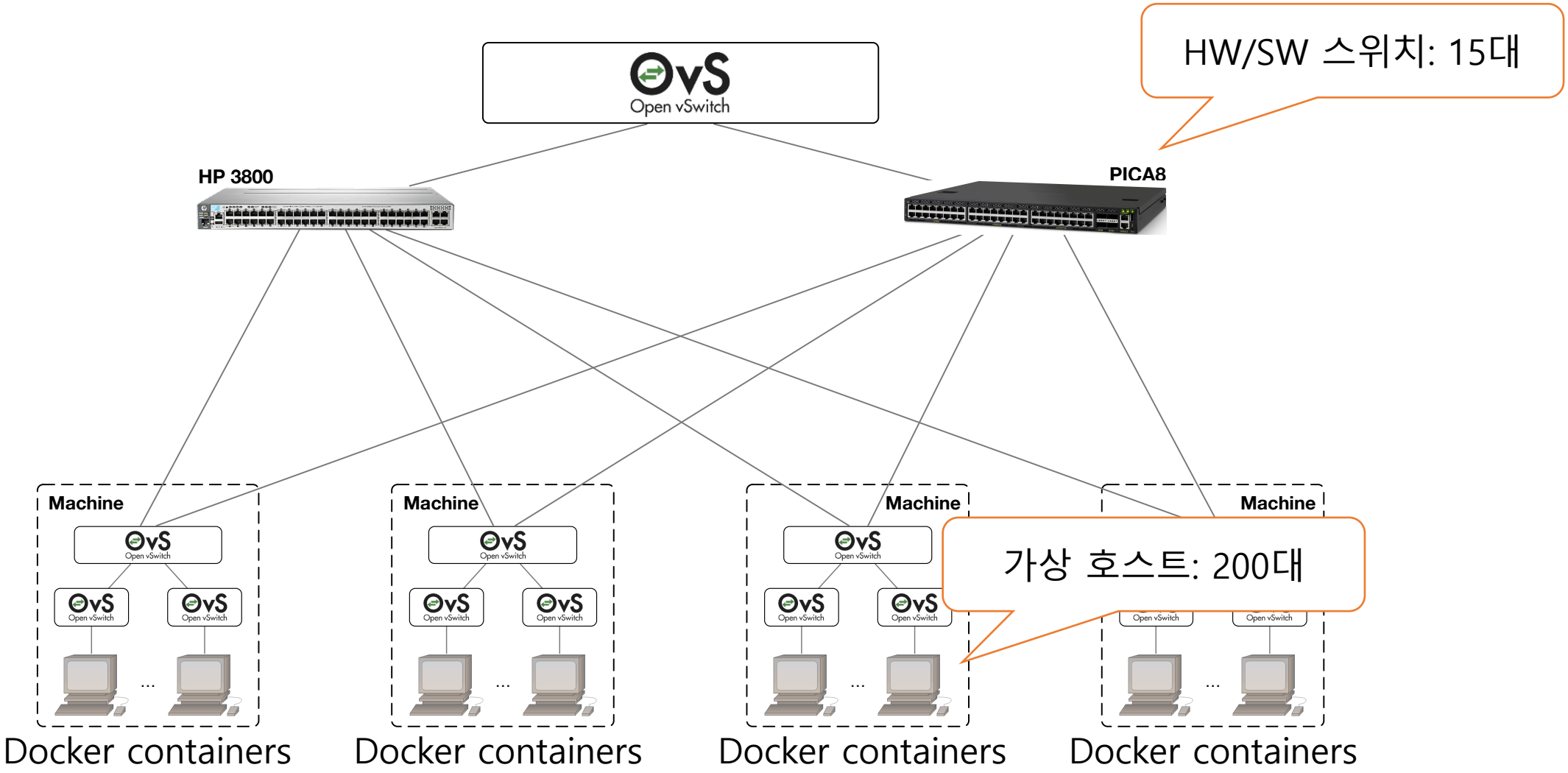




한국측 테스트베드 구성도

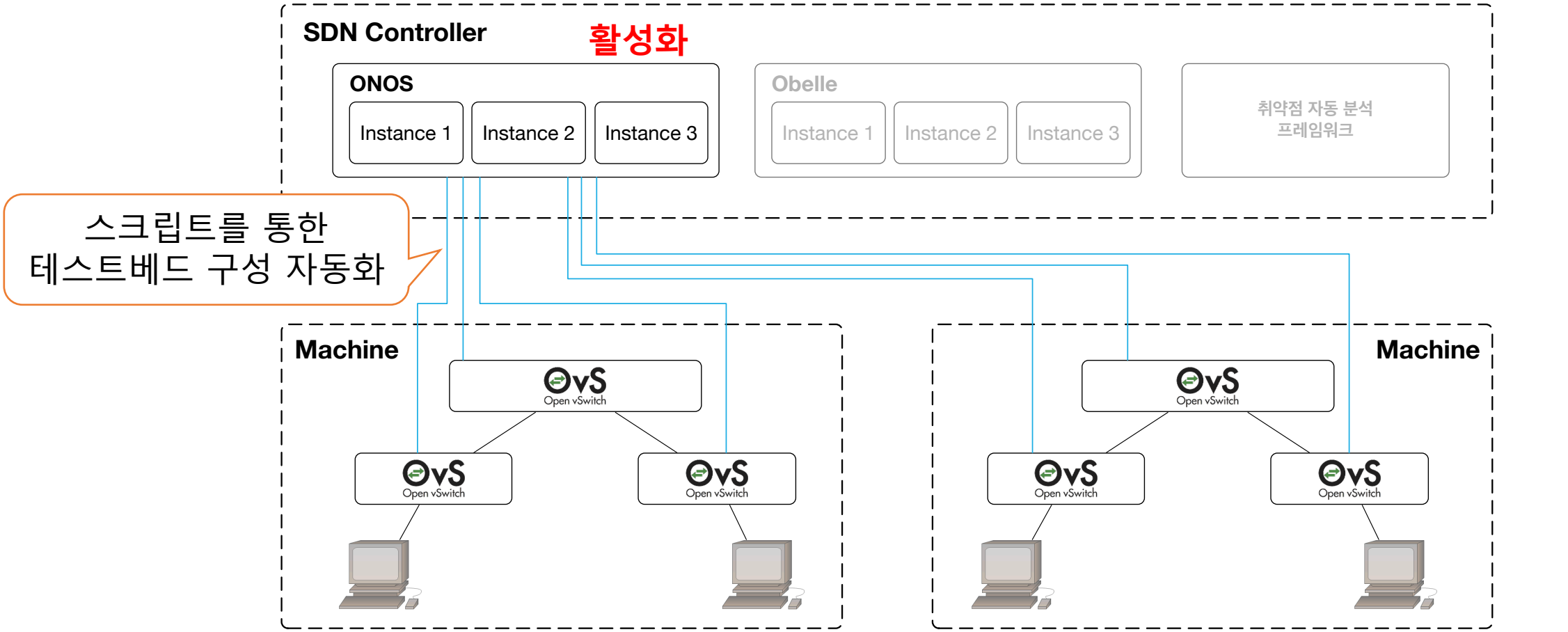


미국측 테스트베드 구성도

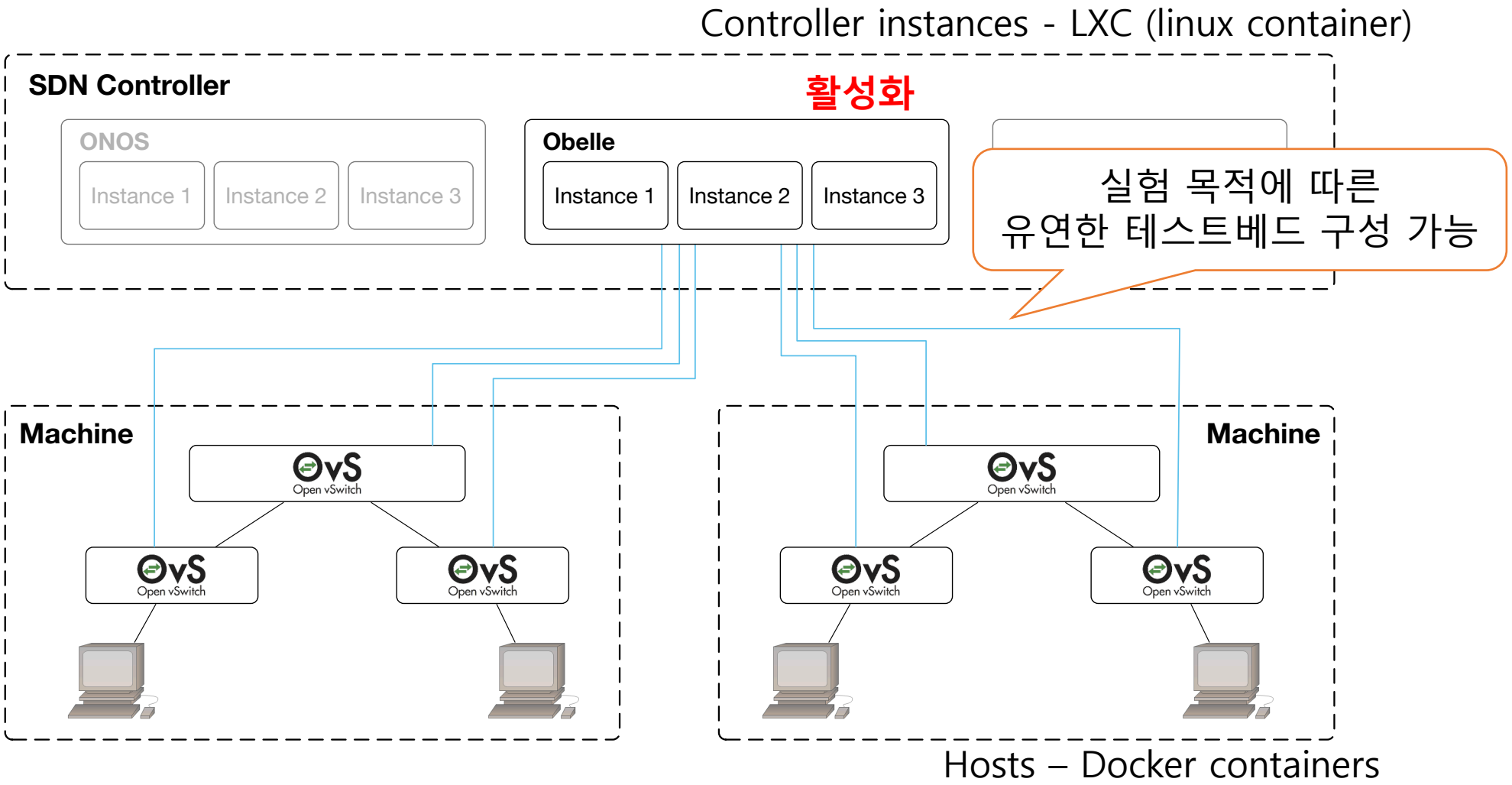


컨트롤러 머신 내부 구조

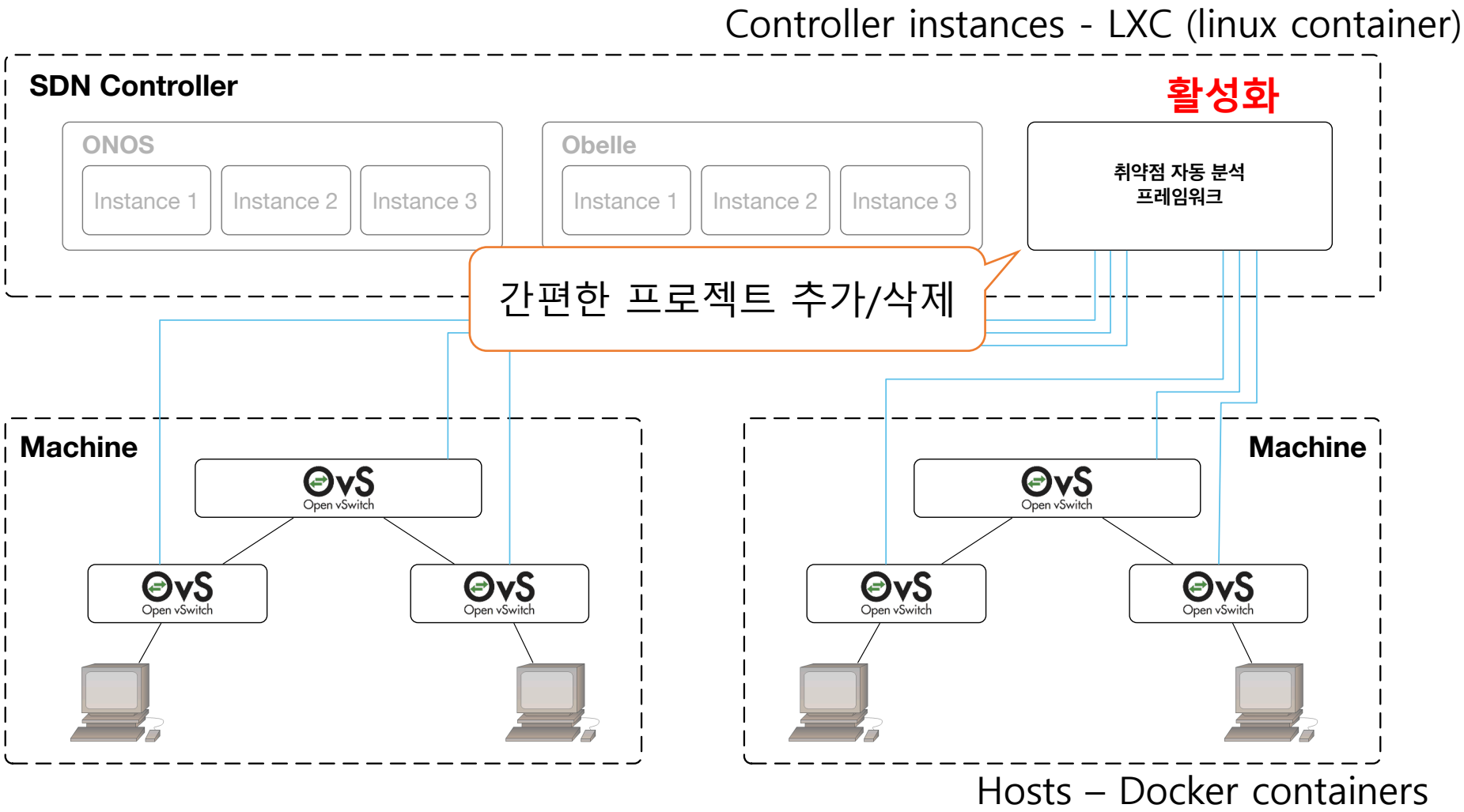
Controller instances - LXC (linux container)



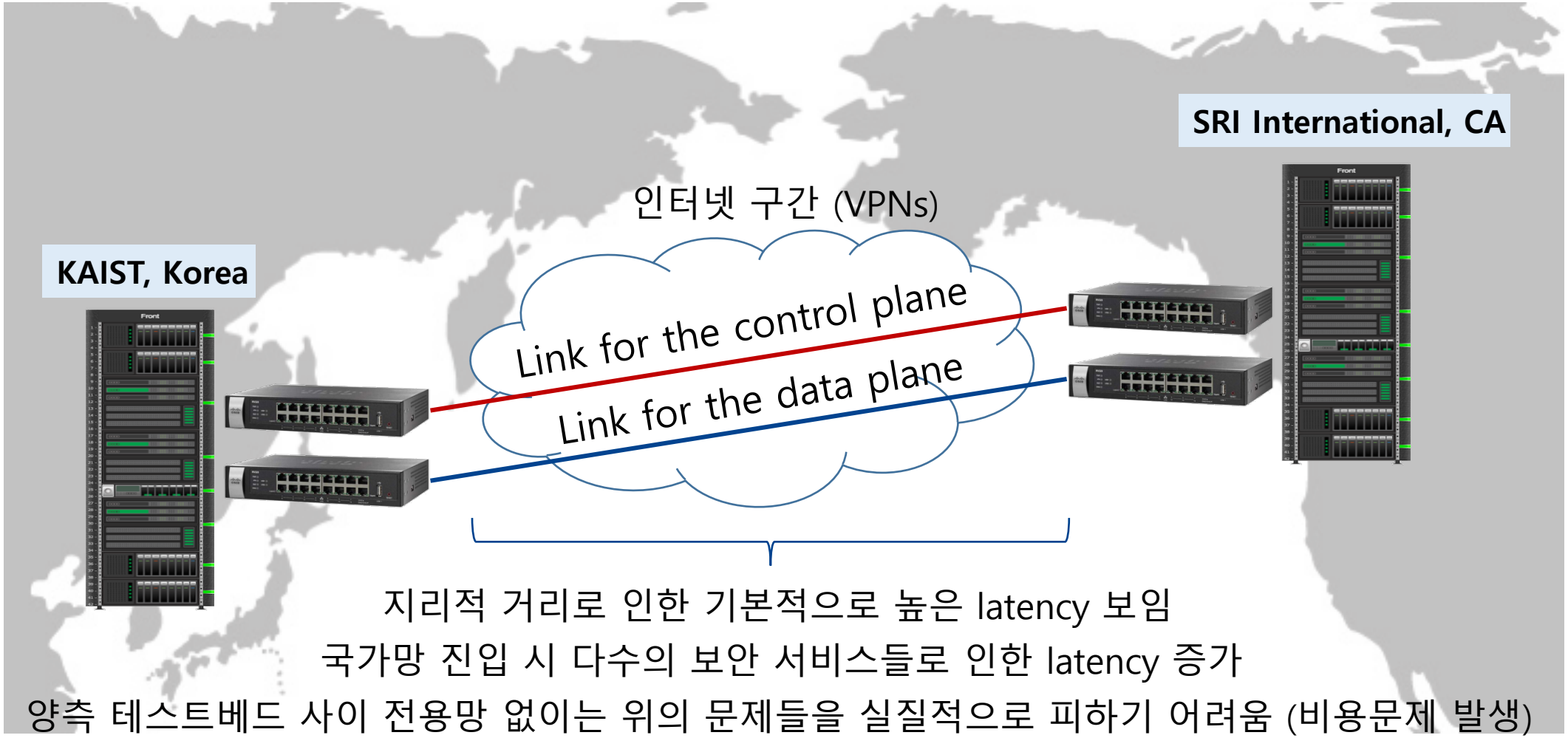
컨트롤러 머신 내부 구조


Controller instances - LXC (linux container)
SDN Controller
활성화
ONOS
Instance 1
Instance 2
Instance 3
Obelle
Instance 1
Instance 2
Instance 3
실험 목적에 따른
유연한 테스트베드 구성 가능
Machine
Machine
OvS
Open vSwitch
Hosts – Docker containers

컨트롤러 머신 내부 구조


Controller instances - LXC (linux container)
SDN Controller
활성화
ONOS
Instance 1
Instance 2
Instance 3
Obelle
Instance 1
Instance 2
Instance 3
취약점 자동 분석
프레임워크
간편한 프로젝트 추가/삭제
Machine
Machine
Open vSwitch
Hosts – Docker containers

한·미 SDN 테스트베드 연동



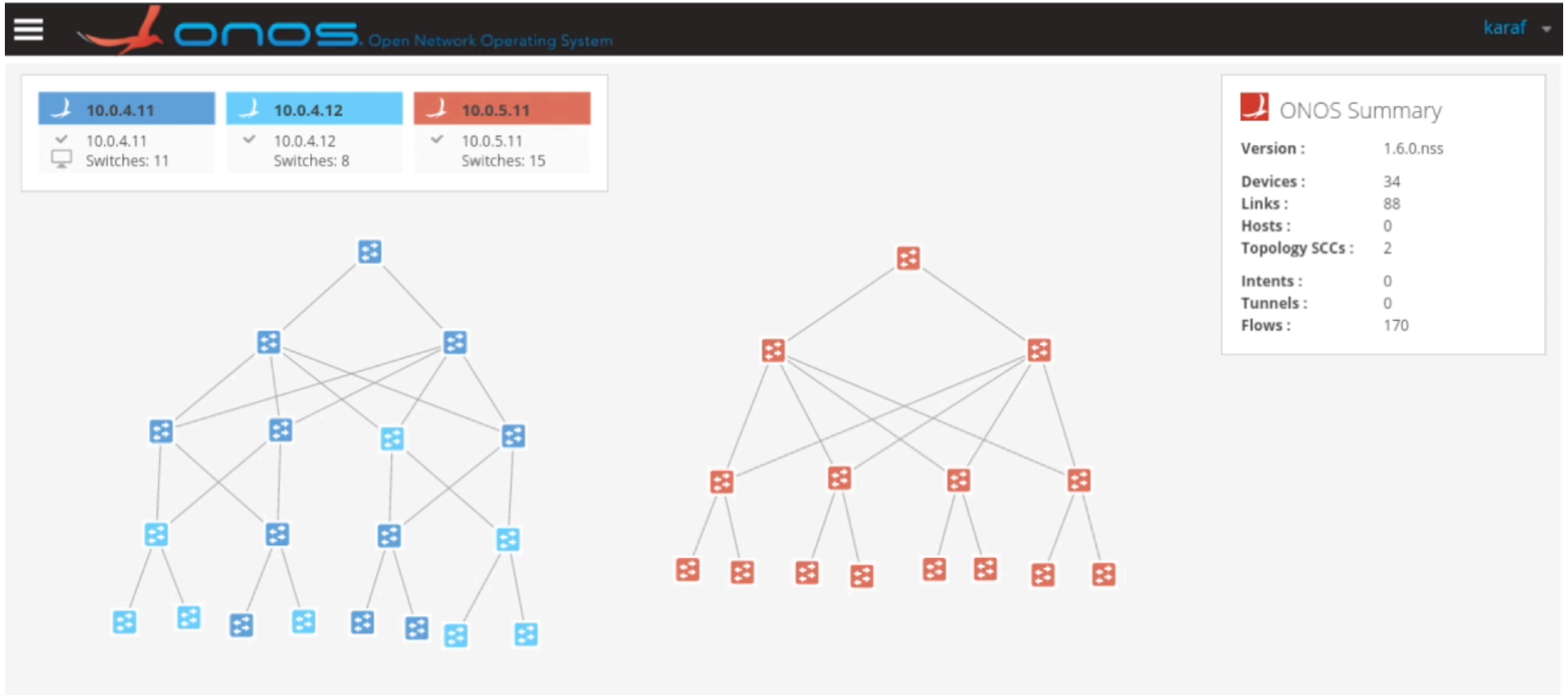
지리적 거리로 인한 기본적으로 높은 latency 보임

국가망 진입 시 다수의 보안 서비스들로 인한 latency 증가

양측 테스트베드 사이 전용망 없이는 위의 문제들을 실질적으로 피하기 어려움 (비용문제 발생)

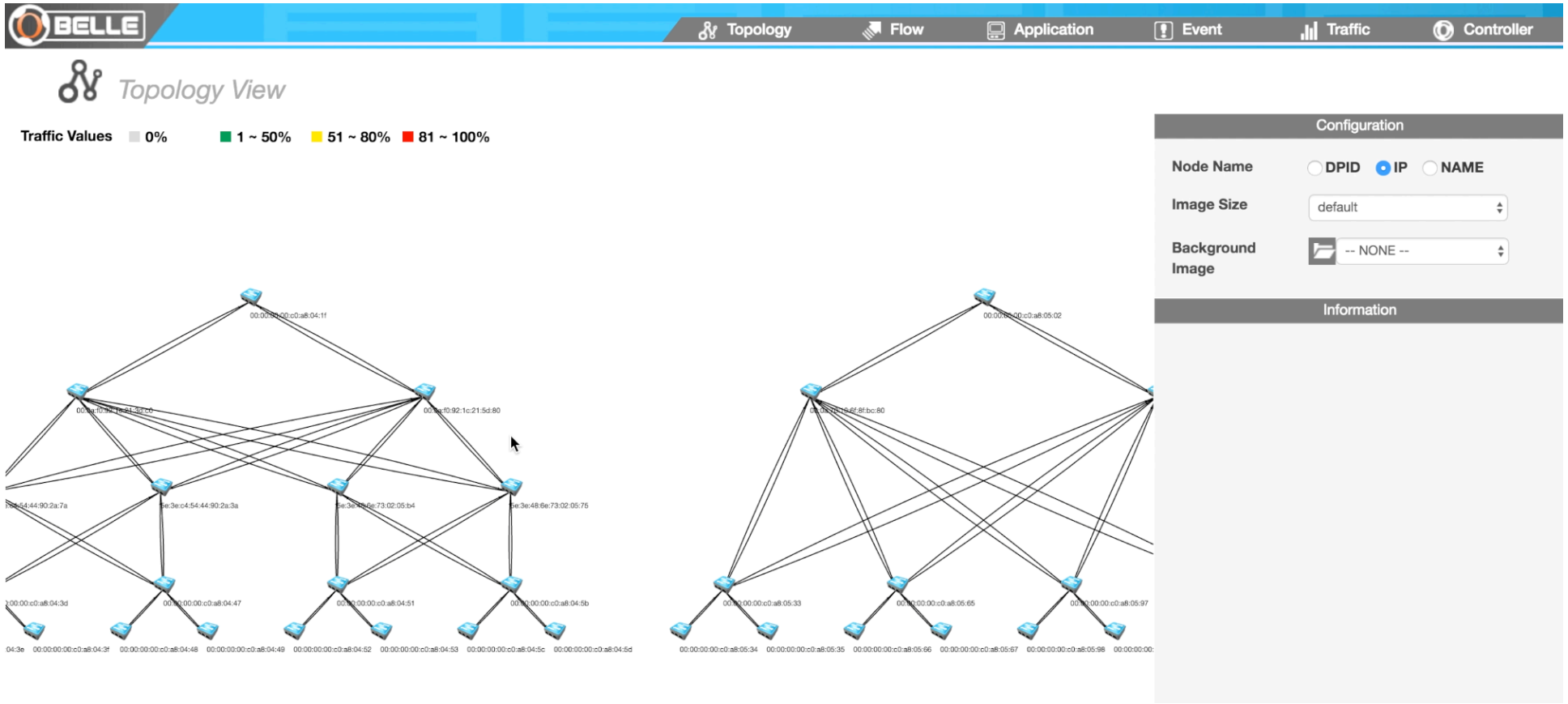
다양한 SDN 컨트롤러 적용

- 오픈소스 SDN 컨트롤러 (ONOS)



다양한 SDN 컨트롤러 적용

- 상용 SDN 컨트롤러 (Obelle)



테스트베드 구축 중 발생하는 다양한 이슈들

- 물리 스위치
  - 이기종 물리 스위치 간 연결 → 스위치별 OpenFlow 내부 구현 차이로 인하여 발생
  - 스위치 펌웨어 버그 → 펌웨어 버전에 따라 기능 상 문제 발견

- 컨트롤러
  - 토폴로지 링크 관리 → 스위치 재구동 시 내부 데이터 꼬임 현상 발생

- 한·미 SDN 테스트베드 연동
  - VPN 구간 내 패킷 drop → VPN 구간 트래픽 압축으로 인하여 실제 여러 패킷들이 drop
  - 분산 컨트롤러 인스턴스 간 동기화 깨짐 현상 → 높은 latency로 인하여 동기화 timeout 후 실제 데이터들이 전달됨

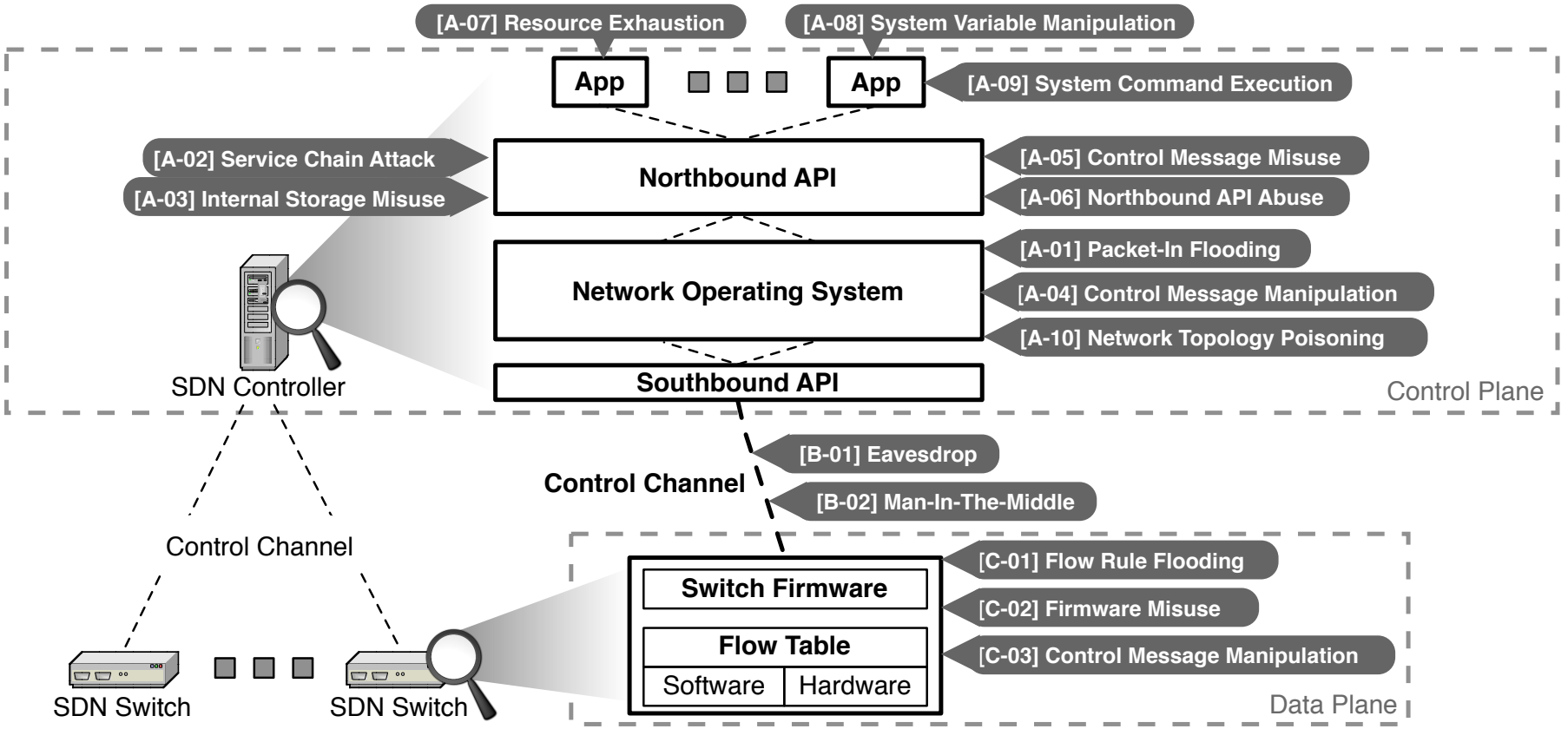
SDN 테스트베드를 활용한 연구 사례

- 네트워크 및 서비스 보안문제 분석 및 대응 기술 연구
  - SDN 취약점 자동 분석 프레임워크
  - TEE 가상 디바이스 간 암호화 모듈

- 효율적인 네트워크 및 서비스 관리기술 연구
  - 제어평면 모니터링 모듈
  - 트래픽 엔지니어링을 통한 부하분산

SDN 취약점 자동분석 프레임워크

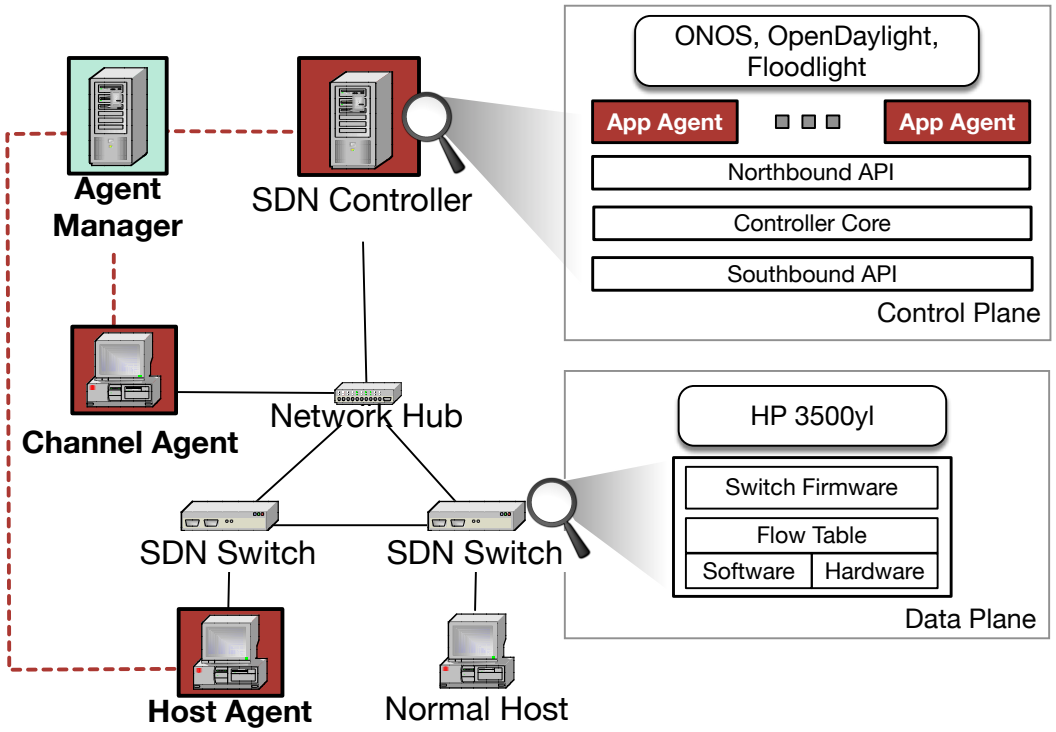
- SDN 취약점 계층별 분류



SDN 취약점 자동분석 프레임워크

- 필요성
  - 다수의 취약점 분석의 어려움
  - 테스트 환경 구축의 어려움

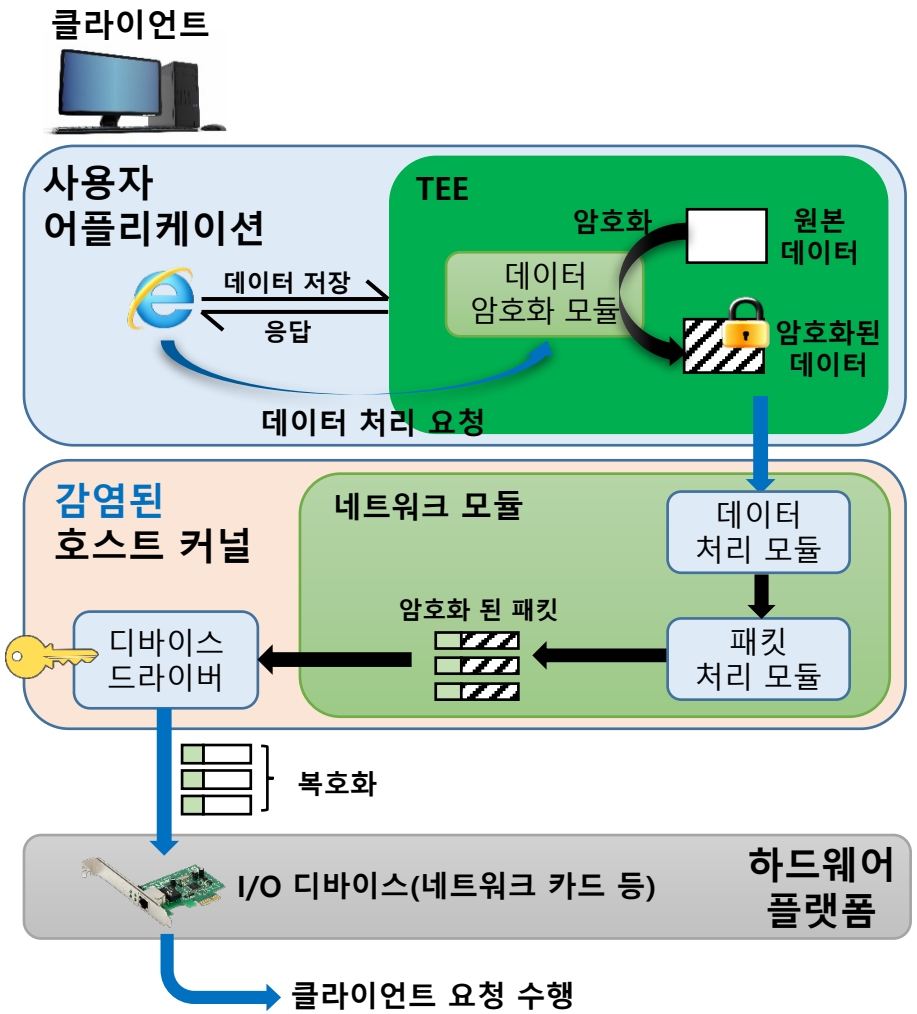
- 목적
  - 타켓 네트워크 내 각각의 요소에 대해서 자동적으로 분석 환경 설정 및 취약점 분석을 수행할 수 있는 프레임워크의 개발



- 구성요소
  - 에이전트 매니저
  - 어플리케이션 에이전트, 채널 에이전트, 호스트 에이전트

TEE 가상 디바이스 간 암호화 모듈

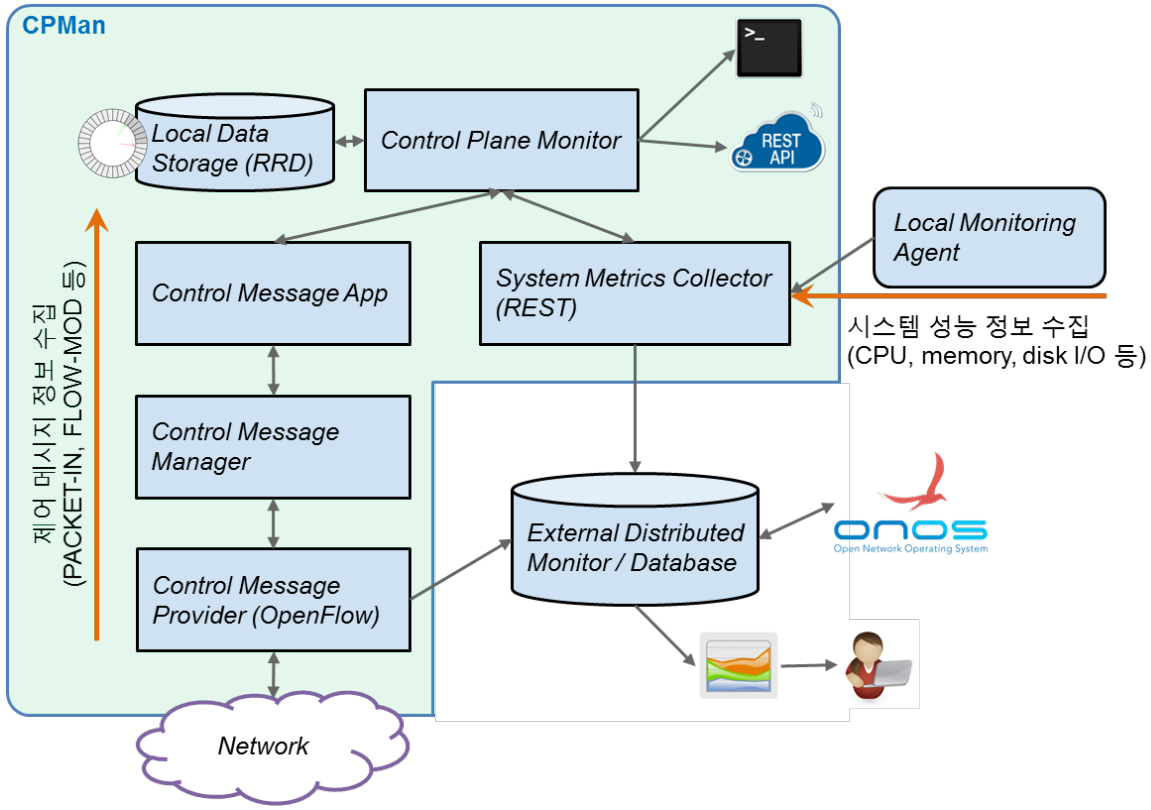
- 필요성
  - 호스트 내 악의적인 커널로 인하여 어플리케이션 데이터 변조/도청이 가능
- 목적
  - TEE(Intel SGX)를 이용하여 어플리케이션-네트워크 디바이스 간 데이터 채널의 보안상 취약점 개선
- 동작 방식
  - 클라이언트 어플리케이션 내 TEE 모듈을 통해 중요 데이터 암호화
  - 네트워크 디바이스 드라이버 내에서 데이터 복호화 후 데이터 전송



제어평면 모니터링 기술

- 목적
  - 제어 메시지 및 시스템 성능 모니터링 모듈 개발
  - 향후 컨트롤러 부하 감소 연구에 활용

- 모니터링 대상
  - 제어 메시지
    - PACKET_IN, PACKET_OUT, FLOW_MOD, FLOW_REMOVED, STATS_REQUEST, STATS_REPLY
  - 시스템 성능 요소
    - CPU 사용량, 메모리 사용량,
    - 디스크 I/O, 네트워크 I/O



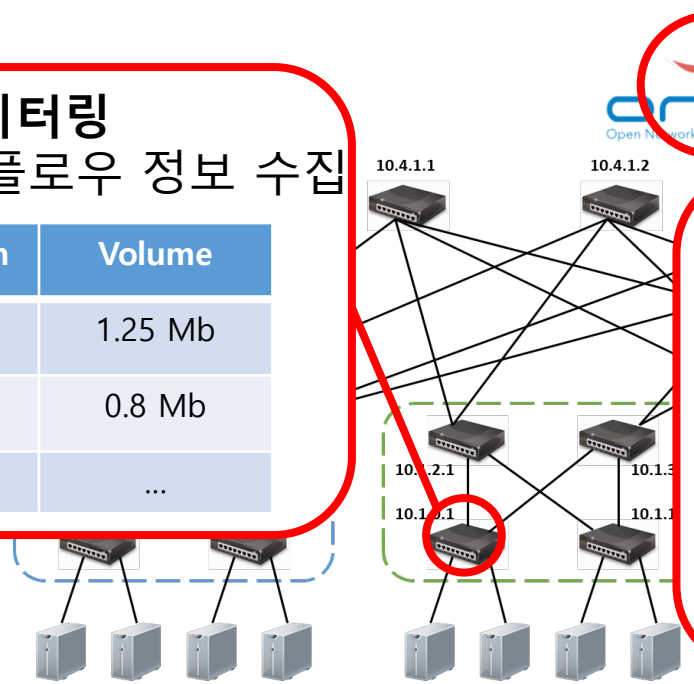
트래픽 엔지니어링을 통한 부하분산

- 목적
  - 소비 전력 감소, 최적의 토폴로지 구성을 통한 관리 복잡소 감소
  - 네트워크 혼잡 최소화
  - 네트워크 트래픽 모니터링 및 트래픽 예측을 통한 부하분산

네트워크 플로우 모니터링

- 스위치들로 부터 플로우 정보 수집

Origin	Destination	Volume
10.0.0.1	10.0.0.2	1.25 Mb
10.0.0.1	10.0.0.3	0.8 Mb
…	…	…

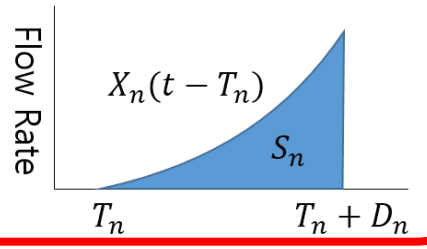


트래픽 예측을 위한 전처리

- 네트워크 토플로지 반영
- 플로우들을 종류별로 분류
- 각 플로우 그룹을 분석 (길이, 크기, 빈도)

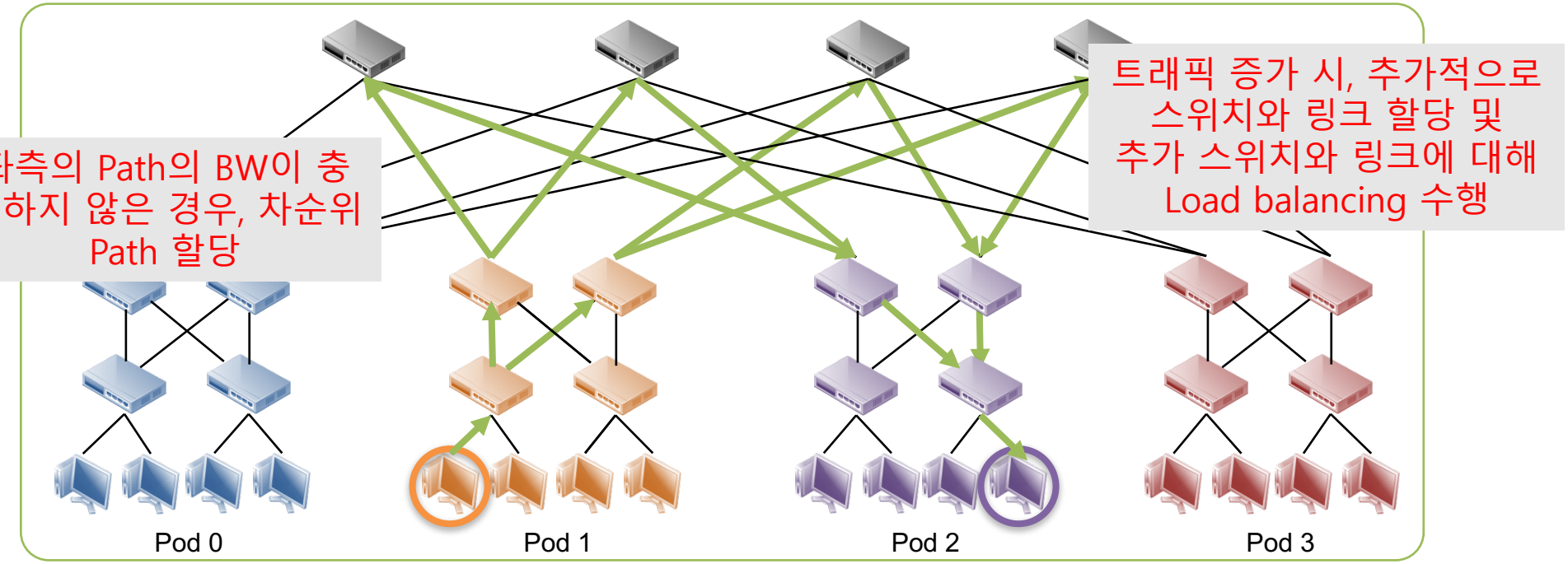
트래픽 매트릭스 예측

- 플로우 그룹의 특성 추출
  Poisson-Shot noise 기반
  트래픽 모델 설계 및 예측



트래픽 엔지니어링을 통한 부하분산

- 현재 트래픽 수준에서 최소의 링크와 스위치를 가지는 토폴로지 계산
- 예측된 모든 플로우에 대해서 알고리즘 적용
  - 동일한 비용을 같는 경로들(ECMPs)을 계산
  - 충분한 BW를 가지는 가장 좌측(우측)의 경로 할당 및 선택된 경로의 여유 BW 감소



맺음말

- SDN 안전성 연구를 위한 한·미 SDN 테스트베드 구축
  - SDN 기술을 활용한 서비스 연구 뿐만 아니라
    각각의 SDN 구성요소 실질적인 SDN 안전성 연구 수행 가능

- SDN 테스트베드를 통한 다양한 연구 수행
  - SDN 취약점 자동분석 프레임워크
  - TEE 가상 디바이스 간 암호화 모듈
  - 컨트롤러 모니터링 기술
  - 트래픽 엔지니어링을 통한 부하분산

- 안전한 SDN 네트워크 인프라 핵심 기술 확보를 위해 지속적인 연구 진행중

IITP 정보통신기술진흥센터
Institute for Information & communications Technology Promotion

KAIST POSTECH

감사합니다