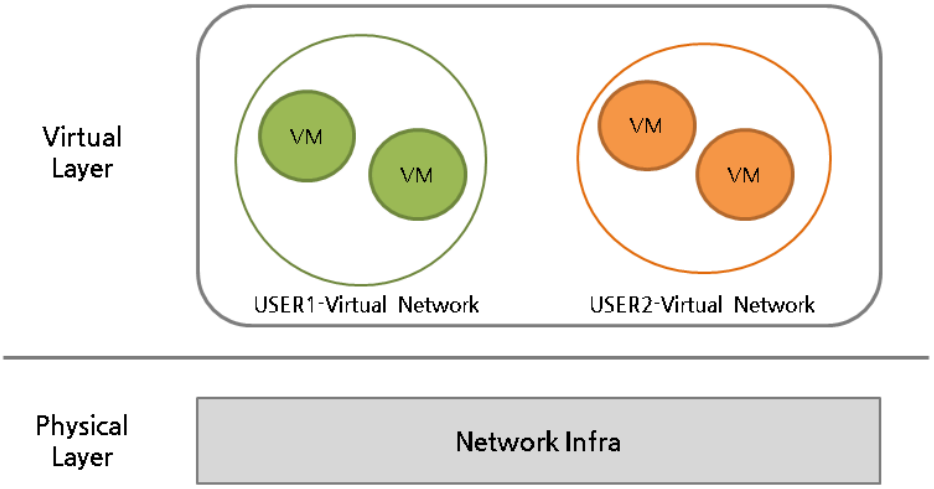
Openflow와 SDN

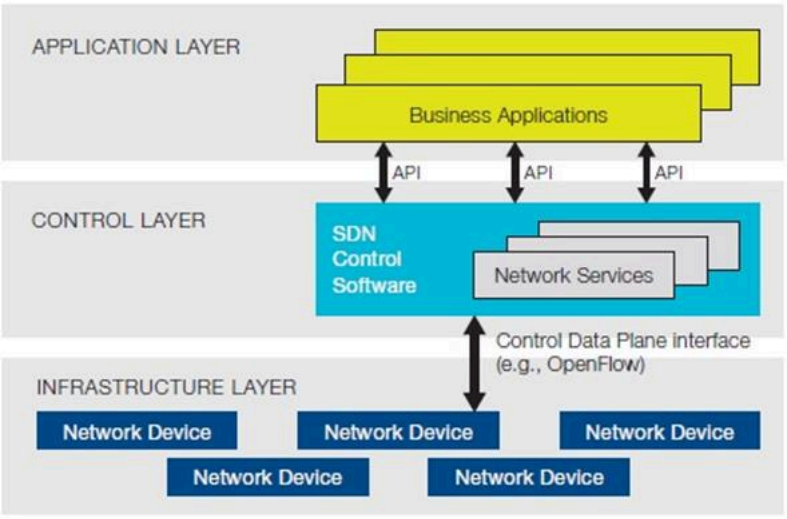
클라우드 환경의 네트워크 관리

- 클라우드 서비스는 하나의 물리 서버에 N개의 VM을 제공하는 서버 가상화 기술뿐만 아니라 물리 네트워크에서 가상의 네트워크 환경을 제공하는 네트워크 가상화 기술도 적용돼 있음



- 필요한 사항
  - 보안(security)
    - 공통의 물리 네트워크 인프라를 여러 명의 사용자가 공유해서 사용
    - 서로 다른 사용자의 VM 간에 보안이 보장돼야
  - 자동화(automation)
    - 클라우드 환경에서는 사용자가 간단히 조작해 네트워크를 설정하고 즉시 반영될 수 있어야 함
      - 일반적인 서비스 환경은 네트워크 설정 정보를 추가하거나 변경하려면 관리자에게 요청해야
    - 요청이 즉시 반영될 수 있도록 자동화해야 함
  - 확장성(scalability)
    - 클라우드 서비스의 장점은 필요한 VM을 빠른 시간 내에 투입할 수 있다는 것
    - 투입된 VM의 지역이나 국가가 다르거나, 그 수가 수천 대여도 쉽게 네트워크 환경을 구축할 수 있어야
- 위 3가지를 위한 네트워크 기술의 조건
  - 자유롭게 네트워크를 만들고 다양한 서비스를 제공할 수 있도록 유연성이 있어야
  - 네트워크를 동적으로 관리할 수 있도록 기능이 모듈화돼 있어야
  - 위 두 가지를 만족하기 위해 네트워크 요소들을 프로그래밍할 수 있어야

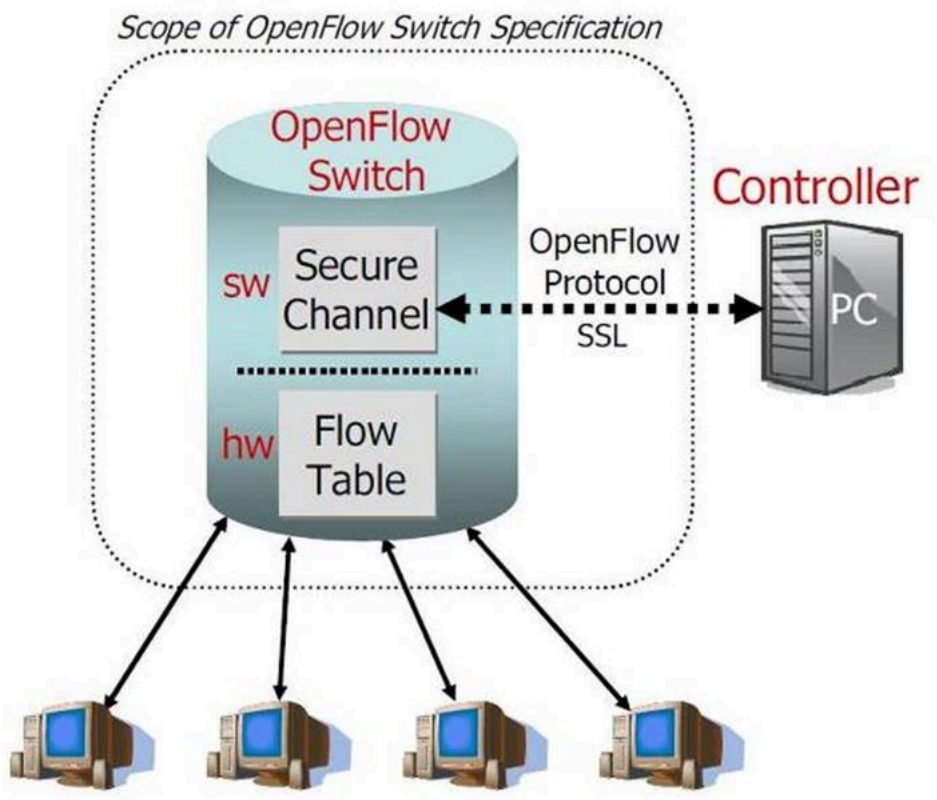
SDN(Software Defined Network)



- 하나의 물리 네트워크에서 다수의 가상 네트워크를 구축해 운영하는 이론적 개념
- 인프라 계층은 **단순히 패킷을 전달**
- SDN 제어 소프트웨어를 프로그래밍해 패킷 흐름 제어
  - 하나의 네트워크 인프라에서 다양한 네트워크 환경 구축
- 패킷 발생 → 네트워크 장비는 패킷을 어디로 전달할지 SDN 제어 SW에 물어봄 → 그 결과를 반영해 패킷 전송하는 경로와 방식 결정

OpenFlow

- SDN을 구현하기 위한 표준 인터페이스
  - OpenFlow 스위치, 컨트롤러로 구성되며 흐름(flow) 정보를 제어해 패킷의 전달 경로 및 방식 결정

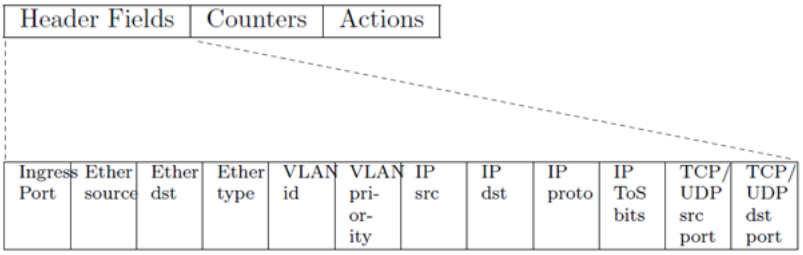


동작 방식

- 스위치는 패킷의 전달 경로와 방식에 대한 정보를 가진 **Flow Table** 존재
  - 패킷 발생 → Flow Table에 해당 패킷에 대한 정보가 있는지 확인
    - 정보가 존재하면 그에 맞춰 패킷 처리
    - 없으면 패킷에 대한 제어 정보를 컨트롤러에 요청
  - 제어 정보를 요청받은 컨트롤러는 내부에 존재하는 패킷 제어 정보 확인
  - → 해당 결과를 스위치에 전달
    - 컨트롤러 내의 패킷 제어 정보는 외부 프로그램에서 API로 입력
  - 스위치는 컨트롤러로부터 전달 받은 제어 정보를 Flow Table에 저장
    - 동일한 패킷이 발생하면 Table 활용해 패킷 전달

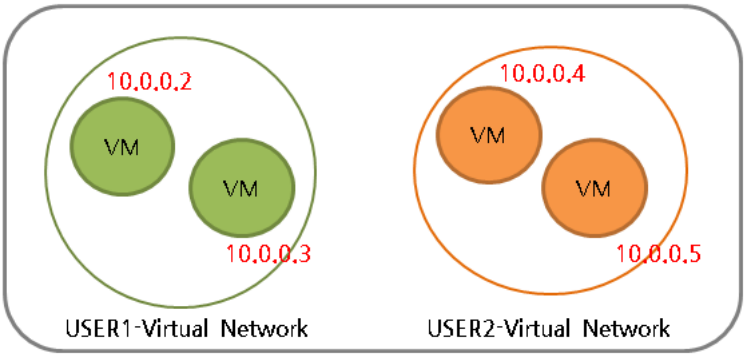
OpenFlow 패킷 제어 정보

- Header Fields, Counters, Actions



- Header Fields
  - 스위치 포트, 이더넷 및 프로토콜 정보, source/destination의 MAC/IP/PORT/우선순위
  - 헤더 필드 정보와 패킷의 정보 일치 여부에 따라, 패킷이 Flow Table에 존재하는지 결정
- Actions
  - 패킷 정보가 헤더 필드 정보와 일치할 때 어떻게 패킷을 처리할지에 대한 정보를 담고 있음
  - 처리 방식
    - 스위치에 정의돼 있는 경로로 패킷 전달
    - 정해진 하나의 포트 또는 여러 개의 포트로 패킷 전달(전달 경로 변경)
    - 패킷이 더 이상 전달되지 못하도록 차단(drop)
- Counters
  - Table에 제어 정보가 등록된 순간부터 현재까지의 시간을 측정하는 용도
  - 제어 정보는 영구적으로 저장 or 정해진 시간 동안만 유지
    - 카운터는 후자의 경우 생명 주기 관리에 사용

OpenFlow 적용 예



- 보안을 위해 각 사용자가 생성한 VM 끼리만 통신할 수 있어야 함
- 테이블 예시

SrcIp	DestIp	Protocol	SrcPort	DestPort	Priority	...	Action
10.0.0.2	10.0.0.3	*	*	*	0	*	NORMAL
10.0.0.3	10.0.0.2	*	*	*	0	*	NORMAL
10.0.0.4	10.0.0.5	*	*	*	0	*	NORMAL
10.0.0.5	10.0.0.4	*	*	*	0	*	NORMAL
*	*	*	*	*	65535	*	DROP

- 10.0.0.2 ↔ 10.0.0.3 과 10.0.0.4 ↔ 10.0.0.5 간의 패킷만 전달하고 나머지는 모두 drop
- 네트워크 설정을 자동화하려면 VM이 생성될 때마다 자동으로 위와 같이 구성돼야 함
  - 외부 프로그램에서 API로 컨트롤러에 정보를 입력할 수 있음
  - → 해당 VM이 생성될 때 관리 프로그램에서 API를 호출해 관련 정보를 설정
- 확장성을 보장하려면 네트워크 환경을 쉽게 구축할 수 있어야 함
  - 스위치를 추가할 때에는 기존의 컨트롤러와 연결하기만 하면 됨
  - 컨트롤러를 추가할 때에는 API로 패킷 제어 정보를 일괄 등록하고 스위치와 연결하기만 하면 됨