School of Electrical and Electronic of Enginnering
eee 4474-01 : Experiments on Communication Networks
2조 2016142096 **조윤신**, 2017142043 **김재민**

Pre Report Week6

Mininet(1) : SDN-based Switch and Hub

Topic 1 : SDN

1 - 1 SDN의 개념

SDN (Software Defined Network, 소프트웨어 정의 네트워크)은 소프트웨어 프로그래밍을 통해 네트워크 경로 설정과 제어 및 복잡한 운용관리를 편리하게 처리할 수 있는 차세대 네트워킹 기술을 말한다. SDN의 핵심은 네트워크 장비의 제어부(Control Plane)와 전송부(Data Plane)의 분리이다. 제어부는 네트워크 장비를 제어하는 'Routing' 역할을, 전송부는 데이터를 전송하는 'Forwarding' 역할을 한다.
기존의 개별 네트워크 장비는 제어부와 전송부 모두 가지고 있었다. 과거의 네트워크는 서버-클라이언트 중심 디자인이 대부분이었다. 인터넷 초창기에는 대부분의 통신이 클라이언트와 서버 간의 통신이었기 때문에 이런 단순한 구조가 문제되지 않았다. 하지만 모바일 기기가 급증하고, 클라우드 기반 가상화 서비스가 등장하면서 트래픽 패턴이 달라졌다.
과거의 서버-클라이언트 통신과 달리 애플리케이션은 다수의 가상머신(Virtual Machine)에 분산되어 다양한 트래픽을 생성한다. 기업은 폭발하는 비즈니스와 사용자 요구에 맞추어 네트워크 규모를 확대하려하면서 네트워크 관리가 더욱 복잡해졌다.
또, 기존의 제어부와 전송부 모두 가지고 있는 네트워크 장비는 빠르게 변화하는 네트워크 환경에 대응하기에 신속성이 부족했다. 네트워크 장비 제품의 수명주기는 3 4년에 불과했고, 표준 API나 개방된 인터페이스가 없었기 때문에 기업이 자사 네트워크 환경에 맞게 기능을 추가하는 것을 제한했다.
이러한 환경 속에서 SDN이 탄생했다. SDN은 제어부를 접근 가능한 컴퓨터 장치로 분리시켜 사용자가 소프트웨어로 네트워크를 관리하고 제어할 수 있도록 만드는 기술이다.

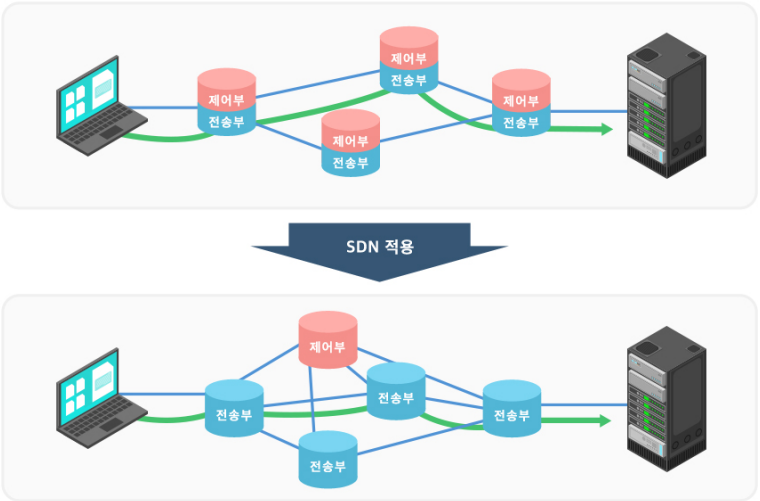

Figure 1: SDN Network

1 - 2 SDN의 장점

SDN은 네트워크 가상화를 통해 제어부를 하드웨어에서 소프트웨어로 전환해 물리적 리소스 한계에 구애받지 않는다. 시시각각 변하는 네트워크 환경에 맞게 네트워크 리소스를 유연하게 확장, 축소할 수 있다.

기존의 네트워크와 같이 스위치와 라우터를 개별적으로 설정할 필요 없이 사용자가 소프트웨어로 중앙화, 원격화된 네트워크를 간편하게 관리할 수 있다.
기존의 제어부가 포함된 값비싼 네트워크 장비와 달리 범용 스위치, 라우터 등의 저렴한 하드웨어를 사용할 수 있다.
또한 SDN은 소프트웨어로 여러 네트워크 장비를 제어하기 때문에 기존 네트워크보다 운영 비용이 적다.

1 - 3 SDN의 구성

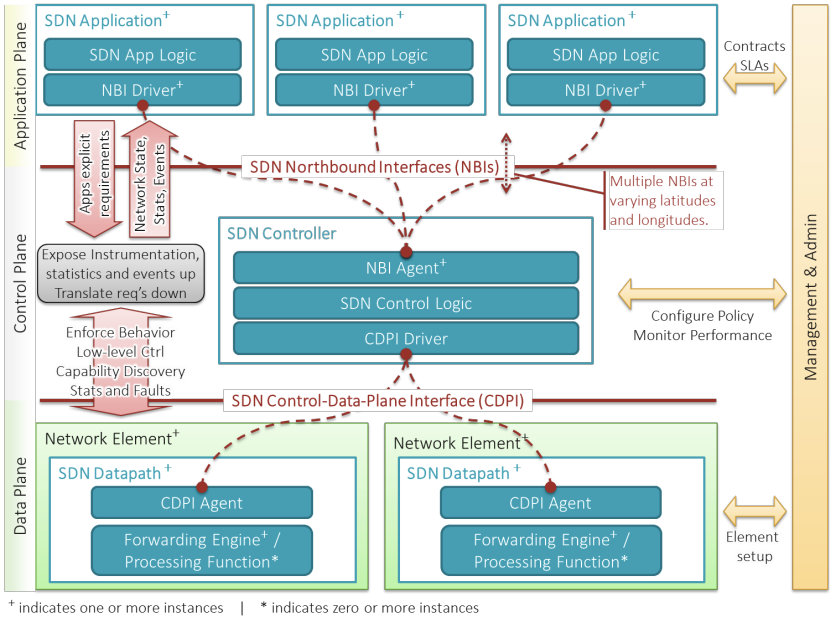

Figure 2: SDN Architecture

SDN 아키텍처는 Application Layer, Control Plane(SDN 컨트롤러), Data Plane(SDN 전송장비) 3계층 구조이다. 각 계층 사이에는 계층 간의 연동을 위한 Southbound Interface와 Northbound Interface가 존재한다.

Application Layer

소프트웨어 어플리케이션을 통해 사용자가 요구하는 네트워크 조건을 만족할수 있도록 Control Plane과 네트워크 관련 정보를 통신한다.

Control Plane

Control Plane은 전체 네트워크 자원에 대한 중앙 집중적 제어를 담당한다. 어플리케이션 정보를 활용하여 데이터 패킷 라우팅 방식을 결정하고, 각 네트워크 장비에게 포워딩 규칙을 전달한다. 또한 여러 네트워크 장비와 통신할 수 있도록 Southbound interface를 제공하거나 추가할 수 있으며, 여러 가지 기능의 애플리케이션을 개발하고 다른 운영 도구과 통신할 수 있게 해주는 Northbound interface도 제공한다.

Data Plane

Data Plane의 네트워크 장치는 Control Plane에서 정한 포워딩 규칙대로 각 데이터 패킷을 다음 장치로 수신한다.

Topic 2 : OpenFlow

2 - 1 OpenFlow의 개념

OpenFlow는 네트워크 장치의 Control Plane과 Data Plane 간의 인터페이스 위한 표준 통신 프로토콜이다. SDN을 실현하기 위한 가장 적합한 기술로 평가되었으며, 현재 SDN 컨트롤러와 네트워크 장치간의 인터페이스 규격으로 사용되고 있다.

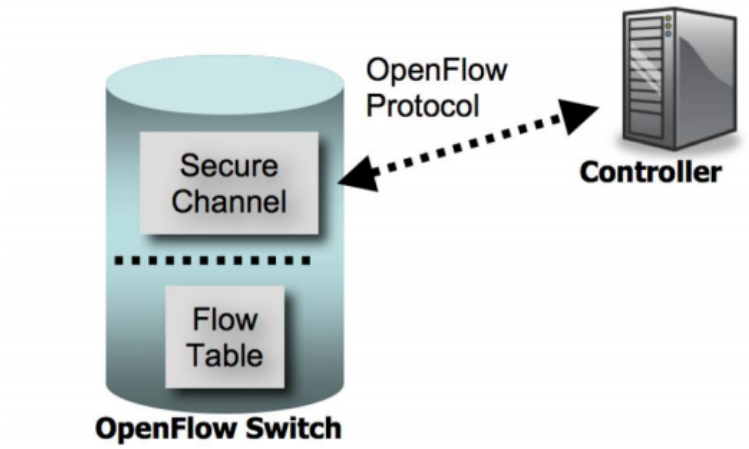

Figure 3: OpenFlow Structure

OpenFlow의 구성요소는 다음과 같다.

OpenFlow Controller

OpenFlow Protocol을 사용하여 네트워크 장치 설정 및 어플리케이션 최적 경로 설정하는 소프트웨어이다. 상위 응용이나 정책 요구에 따라 차별화된 포워딩 및 패킷 처리 룰을 결정하여 하위의 OpenFlow Switch에 전달한다.

OpenFlow Protocol

OpenFlow Controller와 Switch가 통신하기 위한 개방형 표준 인터페이스

OpenFlow Switch

OpenFlow Controller에서 받은 Flow Table대로 패킷 포워드와 조작, 통계 수집, 터널 캡슐화/비캡슐화 등의 기능을 수행한다.

Flow Table

OpenFlow Switch가 패킷을 제어하는 정보가 들어있는 테이블이다. Rule, Action, Stats로 구성된다. Rule은 플로우를 정의하는 패킷 헤더 정보를 갖는다. Action은 입력 패킷 정보가 Rule에 정의된 정보와 일치할 때 패킷을 어떻게 처리할지에 대한 정보를 담고 있다. Action에 따라 패킷을 경로에 맞게 전달하거나 전달 경로를 변경하거나, 더 이상 전달되지 않게 차단할 수 있다. Stats은 각 플로우별로 Rule이 일치하는 패킷이 얼마나 많이 입력되었는지를 보여준다.

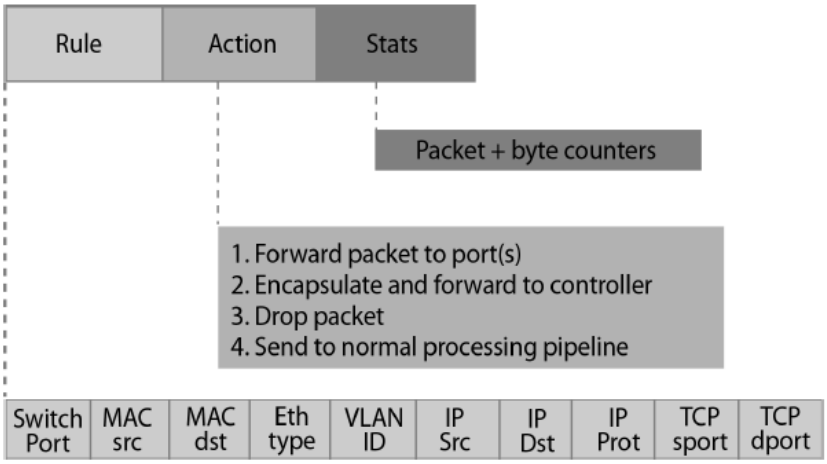

Figure 4: Flow Table

Secure Channel

OpenFlow Controller와 Switch간의 통신을 위한 보안 채널

2 - 2 OpenFlow 기반 SDN의 동작

패킷이 발생하면 제일 먼저 OpenFlow Switch의 Flow Table에 해당 패킷에 대한 정보가 있는지 확인한다. 일치하는 정보가 있다면 그에 맞추어 패킷을 처리하고, 정보가 없다면 해당 패킷에 대한 제어 정보를 OpenFlow Controller에 요청한다.
제어 정보 요청을 받은 OpenFlow Controller는 내부의 패킷 제어 정보를 확인하고, 그 결과를 OpenFlow Switch에 전달한다. 이 OpenFlow Controller 내부의 패킷 제어 정보는 외부 프로그램에서 API를 통해 입력할 수 있다.
패킷 제어 정보를 전달 받은 OpenFlow Switch는 전달 받은 정보를 Flow Table에 저장한다. 이후 동일한 패킷이 발생하면 OpenFlow Controller에 요청할 필요 없이 Flow Table 정보에 따라 패킷을 처리한다.

Topic 3 : Hub

3 - 1 Hub의 개념

Hub(허브)는 여러 대의 컴퓨터, 네트워크 장비를 연결하는 장치이다. 한대의 허브를 중심으로 여러대의 컴퓨터, 네트워크 장비가 성형 구조로 연결되며, 같은 허브에 연결된 컴퓨터와 네트워크 장비는 모두 상호 간에 통신할 수 있게 된다.
허브로 연결된 네트워크에서는 한 컴퓨터에서 주고받는 데이터가 같은 허브에 연결된 다른 모든 컴퓨터에 전달되는데, 이를 Flooding이라고 한다. 허브는 본래 OSI 7계층의 1계층 장비로, 2계층의 MAC 주소로 송수신지를 구분할 수 없기 때문에 Flooding 방식을 이용한다. 통신은 데이터 전송시 송신 측은 데이터를 보내고 수신 측은 오직 송신 측에서 보낸 데이터만 받는 반이중 방식(Half Duplex)을 사용한다.

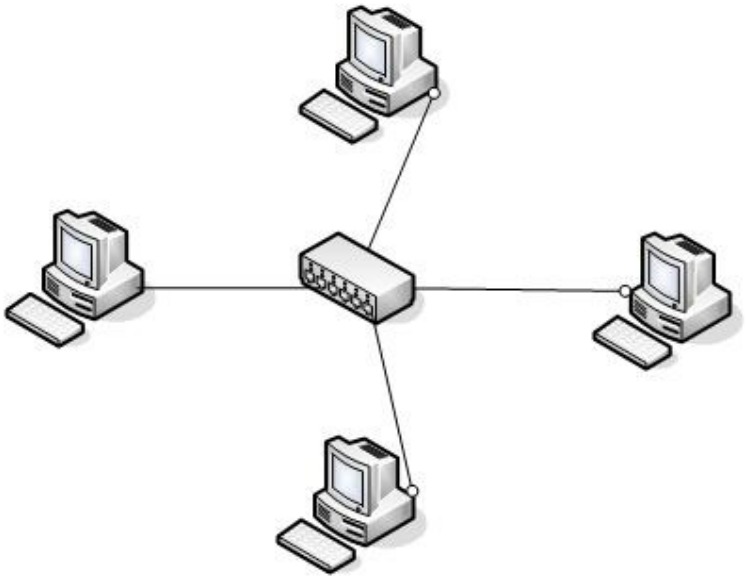

Figure 5: Hub

3 - 2 Hub의 동작

이더넷 허브의 전송방식은 CSMA/CD(Carrier Sense Multiple Access, Collision Detection)로, 이는 반송파를 감지하며 네트워크의 다중 접속을 지원하는 기술이다. CSMA/CD는 전송 전에 다른 노드가 전송 중인지 확인하는 작업을 거쳐 노드끼리의 충돌 가능성을 줄여주며 패킷의 충돌을 방지한다. 다음과 같은 방식으로 순차적으로 진행한다.

1. 컴퓨터가 네트워크를 사용하기 전에 현재 네트워크에서 흐르고 있는 데이터패킷이 있는지 확인한다.
2. 네트워크상에 다른 데이터 패킷이 전송되고 있다면 데이터 전송이 끝나는 시점까지 기다리고 그렇지 않을 때에는 전송을 바로 진행한다.
3. 여러 대의 PC가 동시에 데이터 패킷을 전송하여 데이터의 충돌이 발생하면 최소단위의 데이터 패킷을 다시 보내 다른 컴퓨터가 이를 알아차려 충돌을 방지 할 수 있게 한다.
4. 데이터가 처리될 때까지 임의의 시간 동안 기다리고 다시 반송파를 보내 네트워크에 사용자가 없으면 전송을 재개한다.
5. 원하는 전송을 클리어하면 상위계층에 이를 알리고 종료한다. 만약 이 과정을 여러 번 시도함에도 전송에 실패하면 이 역시도 상위 계층에 정보를 전송하고 종료한다.

Topic 4 : L2 Switch

4 - 1 L2 Switch의 개념

L2 Switch는 느리고 충돌이 발생하는 허브의 단점을 개선하기 위해 MAC 주소 정보를 보고 스위칭하는 일반적인 스위치 기능이다. Frame의 MAC 주소를 읽는 OSI 계층의 2계층 장비이기 때문에 Layer 2 Switch라고 부른다.

L2 Switch의 기능은 다음과 같다.

1. Learning: Frame의 출발지 주소가 MAC Table에 없다면, MAC Table에 주소를 저장한다.
2. Flooding: Frame의 목적지 주소가 MAC Table에 없으면 전체 포트에 Frame을 복사, 전달한다.
3. Filtering: 출발지, 목적지가 동일 네트워크 존재 시 다른 네트워크로 전파를 차단한다.
4. Aging: MAC 테이블의 주소는 일정 시간 후 삭제한다.

4 - 2 L2 Switch의 동작

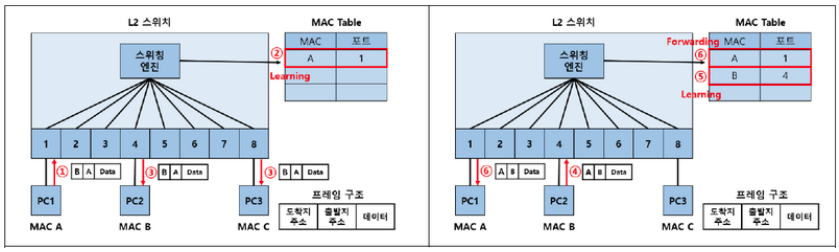

Figure 6: L2 Switch

위의 그림과 같이 MAC Table에 출발지/목적지 주소 정보가 없는 Frame이 들어왔을때의 동작을 알아보자.

1. 1번 포트에 연결된 PC1(MAC 주소 A)에서 MAC 주소 B로 Frame을 전송한다.
2. 출발지 PC1의 MAC 주소 A와 포트 번호 1을 매칭하여 MAC Table에 저장한다. (Learning)
3. 목적지 MAC 주소 B가 MAC Table에 없으므로 전체 포트에 Frame을 복사, 전송한다. (Flooding)
4. PC2(MAC 주소 B)에서 MAC 주소 A로 Frame을 전송한다.
5. 출발지 MAC 주소 B와 포트 번호 4를 매칭하여 MAC Table에 저장한다. (Learning)
6. 목적지 MAC 주소 A가 MAC Table에 있으므로, Frame을 Flooding 없이 포트 1로만 전달한다. (Forwarding)