대용량 클라우드 네트워크 관리를 위한 OpenFlow 활용

NHN ▌정 소 영

1. 서 론

OpenFlow[1]는 switch의 data path와 control path를 분리하여, control path를 OpenFlow controller에서 처리하고, switch는 controller의 처리 결과에 따라 flow 처리를 수행할 수 있도록 함으로써 switch들을 제어하는 표준 기술이다. OpenFlow 네트워크를 구축하면 네트워크 관리자들은 controller를 통해서 switch의 flow table을 원하는 대로 제어할 수 있게 되며, 이로 인해 관리자의 관리 정책에 맞게 동적으로 네트워크를 관리할 수 있다. 이런 장점들로 인해 OpenFlow는 최근 화두가 되고 있는 SDN의 핵심 요소 기술로 활용되고 있다.

OpenFlow는 전통적인 Traffic Engineering 영역에서 관장하는 WAN 구간 최적화, 데이터 센터 관리를 위한 IT Fabric, 클라우드 네트워크의 Virtual Overlay Network 구현 등 다양한 용도로 사용되고 있다. 본 고에서는 주로 클라우드 네트워크에서의 활용 사례를 살펴 보도록 한다. 먼저 2장에서는 클라우드 네트워크가 전통적인 IT 인프라의 네트워크와 어떻게 다른지 살펴 보고, 3장에서는 클라우드 네트워크에서 OpenFlow가 어떻게 활용될 수 있는지 살펴 본다. 4장에서는 네이버의 Ncloud에서 OpenFlow를 활용하는 원칙에 대해 간단히 살펴보고, 5장에서는 OpenFlow의 기술 활성화를 위해 좀 더 연구되어야 할 항목들에 대해 고민해 본다. 이를 통해 OpenFlow/SDN을 연구하는 분들께 보다 현실성 있고 실질적인 연구 주제를 고민할 수 있는 기회를 제공해 보고자 한다.

2. 클라우드 네트워크의 특성

IaaS(Infrastructure As a Service) 기반의 클라우드 네트워크는 여러 가지 측면에서 전통적인 IT 네트워크와 다른 특징을 가지고 있다.

2.1 운영 관점 – 자동화

클라우드 네트워크는 자동화가 필수 구성 요소이다. 전통적인 IT 네트워크의 경우 사용자가 필요한 인프라 변경 작업(인프라의 생성/반납/구조 변경 등)을 요청하면 전담 관리자가 작업 완료 후 사용자에게 인프라를 제공하고 이를 이용하는 형태로 이루어 진다. 따라서 명백히 사용자와 관리자 개념이 분리되어 있으며, ITSM (IT Service Management)과 같이 사용자의 인프라 관련 작업 요청에 대해 체계적으로 제공할 수 있는 방법론 및 관리 시스템이 중요한 역할을 수행해 왔다. 그러나 클라우드 인프라를 사용하는 고객은 필요할 경우 언제든지 직접 인프라를 생성/반납/변경 하는 작업이 가능하므로 필요한 작업을 고객이 직접 수행하는 경우가 많다. 따라서 전통적인 IT 인프라와는 다른 접근 방법이 필요하며, 이를 위해서 필요한 작업들이 자동화 되어 있지 않을 경우 효과적인 서비스 제공이 불가능해진다.

2.2 서비스 제공 관점 – 확장성

클라우드 네트워크는 확장성(scalability)이 인프라 설계에 있어서 아주 중요한 역할을 차지한다. 기본적으로 IT 인프라는 데이터 센터 내 상면의 물리적인 제약, 네트워크 연결 구조에 있어서의 계층적 구조 등의 제약으로 인해 확장성 있는 서비스를 제공하기가 쉽지 않다. 특히 네트워크 관점에서 보면 전통적인 IT 인프라에서의 네트워크는 특정한 서비스 구축을 위한 전용 서비스 형태로 제공되는 경우가 많아서 소위 사일로(silo)화한 구조를 지니는 경우가 많다. 그러나 클라우드에서는 고객이 언제/어디서나 원하는 만큼의 인프라를 제공할 수 있어야 하므로 확장성 있는 구조를 지니는 인프라 설계가 아주 중요하게 된다. 특히 아마존 AWS와 같이 전 세계에 존재하는 고객을 대상으로 클라우드 서비스를 제공하기 위해서는 필요한 만큼 인프라를 추가로 공급할 수 있는 유연한 구조를 지니고 있어야 한다. 특히 네트워크는 'Infrastructure of IT infrastructure' 역할을 수행하고 있으므로 확장성은 더더욱 중요하다고 할 수 있다.

3. UseCase in Large-Scale Cloud Network

본 장에서는 대용량 클라우드 환경에서 OpenFlow가 어떻게 사용될 수 있는지 살펴 본다.

3.1 ACL 관리

ACL(Access Control List) 관리는 기술적으로 도전적인 과제는 아니다. 그러나 실제로 대규모 클라우드/데이터 센터 네트워크 관리에 있어서 ACL 구현 및 운영은 굉장한 부담을 야기할 수 있는데, 대부분의 기업들은 ACL 관련 작업을 수작업으로 대응하는 경우가 많아서 유지/보수에 상당한 어려움을 겪고 있기 때문이다. 특히 최근에 발생한 일련의 개인 정보 유출 사고로 인해서 정부는 개인 정보를 다루는 다수의 IT 기업들로 하여금 망 분리를 지원하는 것을 법제화하고 있어서 ACL 관리는 한층 더 중요하게 다루어 지고 있다.

만일 OpenFlow를 지원하는 switch를 이용할 경우 이와 같은 ACL을 쉽고 편리하게 지원할 수 있다. 특히 많은 종류의 OpenFlow Controller들은 ACL 관리 기능을 기본 기능으로 제공하고 있는데 ACL rule을 OpenFlow switch에서 인식할 수 있도록 flow entry로 변환해 주는 것이 핵심이다. OpenFlow switch의 flow entry에는 L2~L4 layer의 정보를 이용하여 flow를 정의할 수 있으며, 해당 정보를 통해 정의된 flow의 forward/drop action을 ACL rule의 allow/deny에 매핑하는 형태로 구현하고 있다[2].

이러한 OpenFlow 기반의 ACL 관리 메커니즘을 도식화 하면 다음과 같다(그림 1).

ACL 정보는 DB에 저장되어 있으며, 해당 정보를 OpenFlow 네트워크에서 필요한 로직으로 변경하여 적용하는 것은 OpenFlow controller에서 담당한다. 이를 위해서 OpenFlow controller는 Northbound API(일반적으로 REST API)를 지원하고 있으며, 해당 API를 이용하여 ACL 정보를 OpenFlow에서 이해할 수 있는 정보로 변환하여 전달한다.

OpenFlow를 이용한 ACL 메커니즘은 OpenFlow switch에 ACL rule을 어떻게 전달하느냐에 따라서 크게 두 가지 방식으로 나눌 수 있다.

- **Proactive 방식:** ACL에 대응되는 OpenFlow flow entry를 해당 switch에 static 하게 설정하는 방식이다. 이를 위해서는 특정 switch에 존재하는 디바이스 정보마다 적합한 ACL rule을 flow entry로 변환하여 해당 switch에 직접 지정함으로써 ACL을 관리하는 방식이다. Proactive 방식으로 설정된 flow entry는 일반적으로 timeout이 설정되지 않는 경우가 많아 영구적으로 적용 가능하다. 따라서 전통적인 네트워크 기반의 ACL 정책을 관리/적용하는 것과 유사한 방식이어서 쉽고 편리하게 적용할 수 있다는 장점이 있는 반면, 클라우드 네트워크와 같이 네트워크 토폴로지가 동적으로 변화할 수 있는 경우에 적합하지 않을 수 있다.
- **Reactive 방식:** switch에 새로운 flow가 정의되면 해당 flow에 대한 최초의 패킷에 대해서 OpenFlow switch가 Packet-In event를 발생시켜 이를 controller로 전송하고, controller는 Packet-In event에

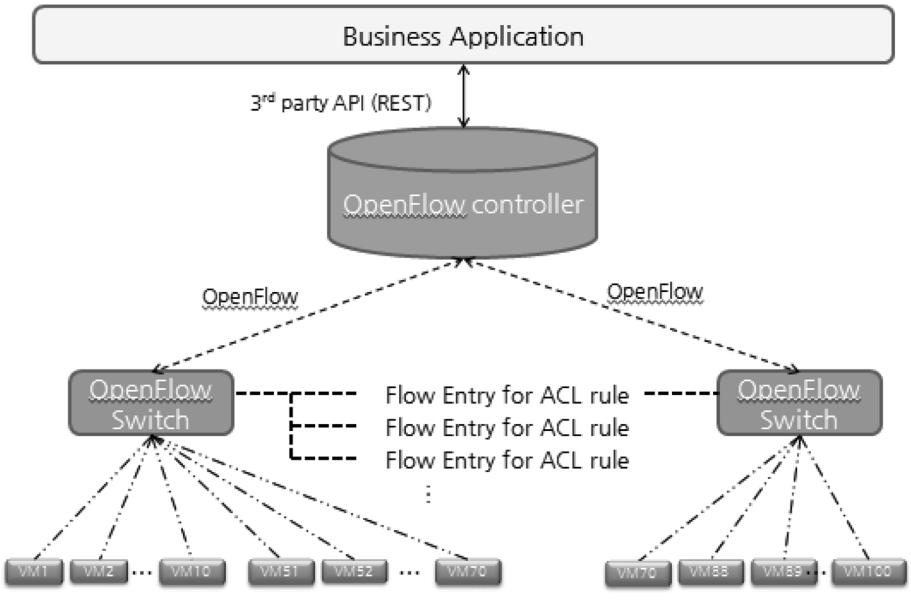

그림 1 ACL 관리를 위한 OpenFlow 메커니즘

대응되는 flow 정보를 찾아서 switch에 ACL rule에 대응되는 flow entry를 전송하는 방식이다. Reactive 방식으로 적용되는 ACL rule은 flow entry에 soft timeout이 설정되어 있는 경우가 많다. 이는 네트워크 토폴로지 변화에 유동적으로 대처할 수 있다는 면에서는 장점이 될 수 있으나, 트래픽 양이 늘어날 경우 controller 부하가 증가할 수 있으며 만일 controller가 감당할 수 없는 수준의 Packet-In event가 발생할 경우 네트워크 품질 저하 및 가용성 저하와 같은 위험 부담을 안을 수 있다는 단점이 있다.

3.2 Anti-ARP spoofing

ARP spoofing은 ARP[3] response 패킷을 조작하여 정상적인 통신을 방해하는 일종의 man-in-the-middle 공격 방식이다. ARP에는 인증 메커니즘이 존재하지 않기 때문에 전통적인 네트워크 구조에서는 ARP spoofing 공격을 근본적으로 차단하는 방법은 존재하지 않으며, ARP spoofing을 대응하기 위해서는 static ARP table을 사용함으로써 ARP spoofing을 원천적으로 차단한다든지, DHCP 서버 등의 3rd party entity를 활용하여 ARP 패킷에 대한 인증을 처리하도록 하는 방식 등이 가능하다. 전통적인 IT 네트워크에서는 많은 기업이 ARP spoofing에 대한 특별한 대응 없이 망을 구축하고 있으나 클라우드 네트워크에서는 내부 공격이 빈번히 발생하므로 이에 대한 대비가 반드시 필요하다. 가장 단순한 방법으로는 고객 별 VLAN을 할당해 줌으로써 서브넷 내에 특정 고객의 서버만 호스팅하여 ARP spoofing을 원천적으로 방지하는 방법이 있으나, VLAN tag는 1~4K 만 할당 가능하므로 확장성 면에서 단점이 있다. 만일 OpenFlow 네트워크를 구축한다면 ARP 패킷에 대한 인증을 OpenFlow controller를 통해서 제공함으로써 ARP spoofing을 방지할 수 있다(그림 2).

먼저 OpenFlow controller에 해당 네트워크에 존재하는 IP/Mac 정보를 미리 등록해 둔다. 등록된 정보는 ARP 패킷 인증의 기본 데이터로 활용된다. 그리고 controller에 연동된 OpenFlow switch에는 ARP response 메시지를 모두 controller로 전달하도록 설정한다. 이렇게 되면 해당 네트워크에 ARP response 메시지가 전송될 때 switch의 flow table을 참조하는 대신 OpenFlow Controller에 해당 메시지를 Packet-In event로 전달하게 된다. ARP response 패킷에 대한 Packet-In event를 받은 controller는 미리 등록된 IP/MAC 정보를 이용해서 정상적인 ARP 패킷인지 확인한다. 만일 비정상적인 패킷일 경우 해당 패킷을 drop하는 명령을 switch에 전달하여 ARP spoofing 공격을 차단할 수 있다.

3.3 Virtual Overylay Network 구현

Virtual Overlay Network은 클라우드 네트워크에서 멀티테넌시를 지원하기 위해 주로 사용되는 기술이다. 예를 들어 아마존의 VPC(Virtual Private Cloud)[4]에서 사용자는 클라우드 네트워크에서 자신만의 가상 네트워크를 생성하고, ip를 부여하고 라우팅 정보를 설정하는 등의 작업을 수행할 수 있다. 이와 같은 기능을 위해서는 클라우드 인프라 내에서 특정 사용자의 리소스들을 가상적으로 연결할 수 있는 Virtual Overlay Network 구성이 필요하게 된다. Virtual Overlay Network는 다양한 방식으로 구현할 수 있는데 OpenFlow를 이용하여 필요한 리소스 간에 터널을 구성한다던지, 패킷 접근 제어 기능을 통해서 특정 리소스 간에만 통신을 제공하는 등의 방식으로 구현하는 기술들이 등장하고 있다[5,6].

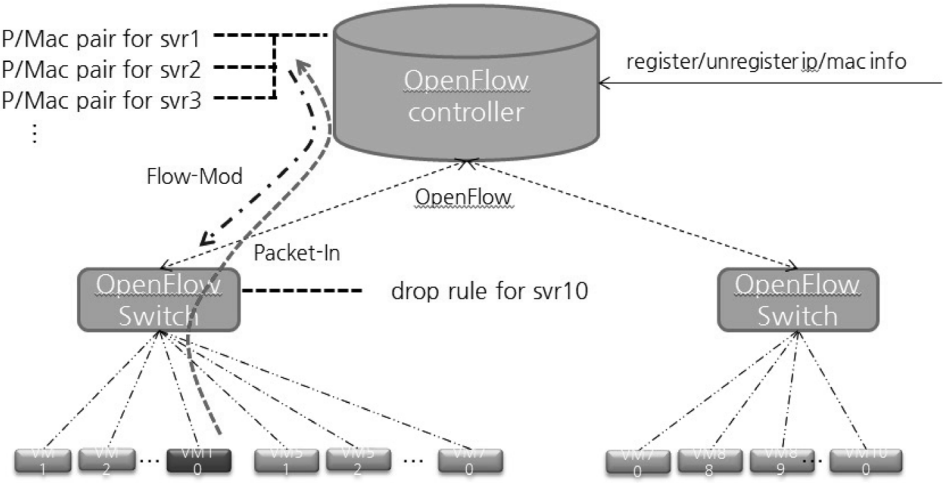

그림 2 OpenFlow 네트워크에서 ARP spoofing 방지 메커니즘

4. OpenFlow in Ncloud

네이버는 2008년부터 클라우드 인프라를 구축하여 운영하고 있으며 2012년부터 Ncloud라는 플랫폼을 구축하고 그 서비스 영역을 확대하여 다양한 내/외부 고객을 위한 클라우드 서비스를 운영하고 있다. 초기 클라우드 인프라 구축 시 많은 시행 착오도 경험하였으나 몇 번의 진화를 거듭한 끝에 현재 네이버의 클라우드 네트워크는 다음과 같은 기본 철학을 가지도록 설계되어 있다.

1) 물리적인 네트워크 구성은 최대한 단순하게 구축할 것: 사일로(silo) 화한 네트워크 대신 확장성 있는 네트워크 구성을 위해서는 물리적인 네트워크는 최대한 단순하게 구축하여야 한다.
2) 복잡한 비즈니스 로직은 애플리케이션/소프트웨어를 이용하여 제공할 것: 전통적인 IT 인프라의 경우 필요한 네트워크 기능을 제공하기 위해서는 해당 기능을 제공하는 네트워크 장비를 인프라에 어떻게 연동할 것인지가 네트워크 설계 및 운영에 중요한 역할을 수행하였다. 그러나 이와 같은 방식은 확장성 있는 네트워크 제공에 많은 걸림돌이 될 수 있다. 이를 극복하기 위해서 많은 네트워킹 기능을 애플리케이션/소프트웨어 방식으로 변환함으로써 보다 유연하고 확장성 있는 구조를 제공할 수 있도록 하고 있다.
3) 다양한 클라우드 솔루션을 자유롭게 연동할 수 있을 것: IaaS 기반의 클라우드 인프라는 인프라 자체에 대한 제공뿐만 아니라 해당 인프라를 기반으로 PaaS(Platform As a Service), SaaS(Software As a Service) 등의 추가적인 클라우드 솔루션을 연동하는 용도로 사용될 수 있어야 한다. 이를 위해서 각각의 기능들을 모듈화 하고 재사용할 수 있도록 설계/구현하고 있다.

이러한 원칙을 통해 Ncloud의 클라우드 네트워크는 다양한 요소 기술을 활용하여 자동화, 확장성을 지원할 수 있도록 설계/구축되었다. OpenFlow는 이러한 요소 기술 중 하나로 이용되고 있는데, Ncloud에서 OpenFlow를 활용하는 기본 철학은 다음과 같다.

1) End-to-End Flow Control용도로 사용하지 않음: OpenFlow는 기본적으로 switch의 forwarding table 제어를 통해 효율적으로 flow 관리를 수행할 수 있는 기능을 갖고 있다. 예를 들어 Google은 효율적인 WAN 구간의 트래픽 관리를 위해 OpenFlow를 활용한 사례를 발표한 바 있다[7]. 다만, 클라우드 네트워크 관리에 있어서는 이와 같은 기능이 효과적으로 적용될 수 있는 영역이 상대적으로 적다. 따라서 Ncloud에서는 End-to-End Flow Control 용도로 OpenFlow를 활용하지 않으며, OpenFlow를 활용한 보안 관리(Security Management) 및 IT 거버넌스 관리(Governance Management) 용도로 사용하고 있다.
2) 가상 인프라 관리용으로만 사용: OpenFlow 기술 자체의 성숙도는 충분히 이루어 졌으나 네트워크 운영적인 관점에서 필요한 운영 노하우는 아직 확보되지 않았다. 따라서 일차적으로 클라우드 네트워크 운영을 통해 안정성을 확보하고 운영 노하우를 축적하여 향후 사용 대상을 확대해 나갈 수 있는지 검토하고자 한다.
3) OpenFlow Controller에 대한 customization: 현재 FloodLight[8], NOX[9], Beacon[10] 등 다양한 OpenFlow controller들이 오픈 소스로 공개되어 있다. 그러나 이러한 솔루션들은 실제 상업적인 용도로 사용하기에 어려운 점들이 많다. 예를 들어 어떤 네트워킹 기능을 위해 구현을 모듈의 소스를 분석해 보면 범용적인 클라우드 서비스 지원을 위해서 필요한 확장성이 부족한 경우들이 상당 부분 존재한다. 이를 개선하기 위해서 기능적/성능적으로 튜닝하고 개선한 버전의 OpenFlow controller를 사용하고 있다.

5. Challenges

OpenFlow는 네이버 뿐만 아니라 세계 다수의 기업에서 많이 사용하고 있는, 이미 검증된 기술이다. 다만, 내부적으로 적용을 위해 검토한 결과 다음과 같은 기술적 이슈들이 산재해 있음을 확인할 수 있었다.

5.1 효율적인 deployment architecture

OpenFlow 도입의 핵심은 도입 전략에 맞는 효과적인 deployment architecture를 도출하는 것이다. 현재 이용 가능한 OpenFlow controller나 OpenFlow switch들이 확장성 면에서 제한적이기 때문에 어떠한 목적으로 OpenFlow 네트워크를 도입하느냐에 따라 전혀 다른 deployment architecture가 도출될 수 있기 때문이다. 또한 OpenFlow 네트워크 구축에 복수 개의 controller가 이용될 경우 controller들이 동일한 비즈니스 로직 하에서 원활하게 동작하도록 하기 위한 메커니즘 등도 여전히 숙제로 남아 있다.

5.2 보안 이슈

클라우드 네트워크에서는 전통적인 네트워크와는 다르게 네트워크 내부에서의 공격 가능성이 훨씬 높을 수밖에 없다. 따라서 OpenFlow 기반의 네트워크를 구축할 경우 이에 대한 대비도 보다 철저히 이루어 져야 하는데, 아직까지 이에 대한 연구가 상대적으로 부족한 것이 사실이다. 보안 이슈는 OpenFlow 네트워크를 도입하려는 많은 기업들이 가장 조심스럽게 접근하는 분야이므로 해당 분야에 대한 연구가 더욱 더 활발히 진행되는 것이 OpenFlow 네트워크의 보급에 많은 도움이 될 것으로 기대한다.

6. 맺음말

전통적인 IT 인프라의 네트워크 관리는 상당 수의 작업들이 수작업으로 이루어 지고 있었으며, IT 인프라의 기반 인프라 역할을 한다는 인식으로 인해서 상당히 보수적으로 업무가 수행되는 영역이다. 반면, 최근 SDN이 각광을 받는 이유 중의 하나는 이와 같이 전통적으로 수작업으로 이루어 져 온 네트워크 관리에 있어서 완전히 새로운 패러다임의 전환이 가능하기 때문이다. 즉, 네트워크 노드들은 단순히 패킷 처리만 수행하고, 실제 패킷 처리에 대한 로직은 별도의 controller에서만 수행하면 되기 때문에 관리자는 자신이 관리하고 싶은 비즈니스 로직을 controller를 통해 제어하기만 하면 네트워크가 원하는 대로 동작하도록 구현할 수 있다는 가능성이 높아지고 있다. 이러한 SDN의 핵심 기술로서 OpenFlow가 주목받고 있으며 다양한 연구를 통해서 적용 사례들을 지속적으로 생산해 내고 있다.

다만 OpenFlow가 보다 더 활성화 되기 위해서는 controller에서 지원할 수 있는 기능이 보다 다양하게 제공되어야 할 것이며, 이를 지원할 수 있는 효율적인 deployment architecture에 대한 연구도 필요하다. 아울러 OpenFlow 관련 보안 관련 연구가 한층 더 심도 깊게 진행되어 기업들이 믿고 안심하게 사용할 수 있는 환경 조성이 필요하다.

참고문헌

[1] Nick Mckeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, OpenFlow: Enabling Innovation in Campus Networks, March 14, 2008, OpenFlow.org

[2] OpenFlow Specification 1.0, OpenFlow.org

[3] David C. Plummer, ARP: An Ethernet Address Resolution Protocol, RFC 826, IETF

[4] Amazon VPC, http://aws.amazon.com/vpc/

[5] Nicira, Network Virtualization Platform(NVP), http://nicira.com/

[6] BigSwitch, Big Virtual Switch(BVS) http://www.bigswitch.com/

[7] Google G-scale, http://www.eecs.berkeley.edu/~rcs/research/google-onrc-slides.pdf

[8] Floodlight, http://www.projectfloodlight.org/floodlight/

[9] NOX, http://www.noxrepo.org/

[10] Beacon, https://openflow.stanford.edu/display/Beacon/Home

약 력

정 소 영

1994~1998 서울대학교 계산통계학과 전산과학 전공
1998~2000 서울대학교 대학원 전산과학과 석사
2000~2004 타오네트웍스
2004~2006 SK 텔레텍
2006~현재 NHN
관심분야 : 가상화, x86 서버 기술, 대용량 클라우드 아키텍쳐 설계
E-mail : jeong.soyoung@nhn.com