최영락
나임네트웍스 SDN기술팀 매니저

컴퓨터 네트워크의 이해 및 활용 11

네트워크 관리와 SDN

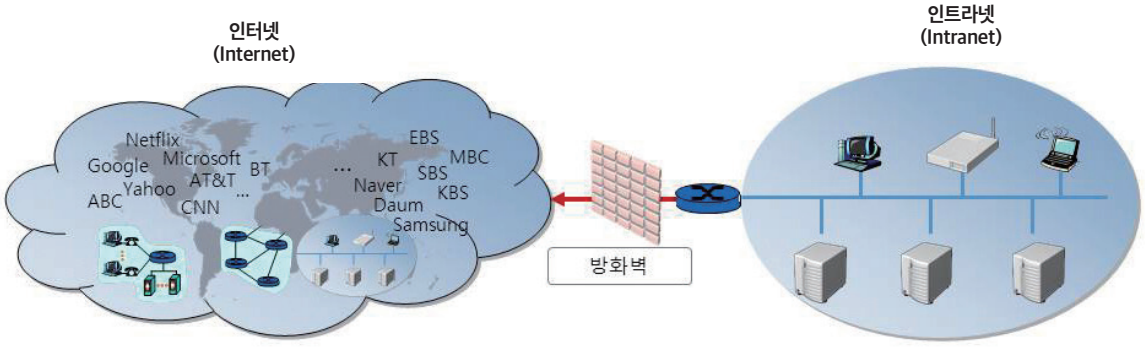
최영락 나임네트웍스 SDN기술팀 매니저

지난 연재에서는 인터넷 역사와 함께 차세대 IP 주소에 해당하는 IPv6에 대한 개요 및 동향에 대해 살펴보았습니다. 방송 시설에 대해 구축뿐만 아니라 관리 및 운영도 중요하듯이, 네트워크 관리 또한 컴퓨터 네트워크의 이해 및 활용에 있어서 필수적인 부분입니다. 마지막 본 연재에서는 네트워크 관리를 설명하기 전에, 잠시 인터넷과 인트라넷이라는 용어를 먼저 알아보고, 네트워크 관리 및 소프트웨어 정의 네트워킹이라고 부르는 SDN에 대해 살펴보면서 마무리하고자 합니다.

I. 인터넷과 인트라넷

지난 여러 연재에 걸쳐, 컴퓨터 네트워크와 관련해 서버와 클라이언트에 대한 설명을 시작으로 프로토콜, IP 주소, TCP/IP 4계층 및 관련 장비들, 스트리밍 및 멀티캐스트, 그리고 현 IP 주소 체계(IPv4)를 대체할 차세대 IP 주소 체계인 IPv6에 대해 살펴보았습니다. 이러한 여러 개념은 PC 및 노트북, 그리고 서버와 같은 여러 장치가 하나의 네트워크로 묶여 서로 연결되어 "인터넷"이라는 이름으로 현재 많은 사람이 사용하고 있습니다.

인터넷과 대비되는 용어로, 인트라넷이라는 용어가 있습니다. 인트라넷은 영어로 '안쪽, 내부'를 뜻하는 intra라는 접두어와 네트워크의 앞 세 글자인 net이 합쳐진 단어로, 특정 기업 또는 조직의 내부적인 목적으로 활용하기 위해 구성한 네트워크를 의미합니다. 일반적으로, 인터넷과 인트라넷 사이에, 기업 또는 조직에서는 방화벽을 설치하고, 인터넷상의 임의의 외부 사용자가 허락 없이 인트라넷에 접근하지 못하도록 제한하여 보안을 유지합니다. 반면, 인터넷은 '서로 간, 상호 간'을 의미하는 inter라는 접두어와 net이 합쳐진 단어로, 폐쇄적인 인상을 주는 인트라넷이라는 용어와 달리 여러 개의 네트워크가 서로 연결을 맺고 있는 인상을 주는 용어입니다. 이렇듯, "인터넷"은 오늘날 전 세계인이 공용으로 서로 연결되어 있고, 많은 방송사를 포함하여 IT 서비스 회사, 통신사, 그리고 통신사에 가입하여 사용하는 모든 컴퓨터가 연결되어 있는 하나의 망을 의미합니다.

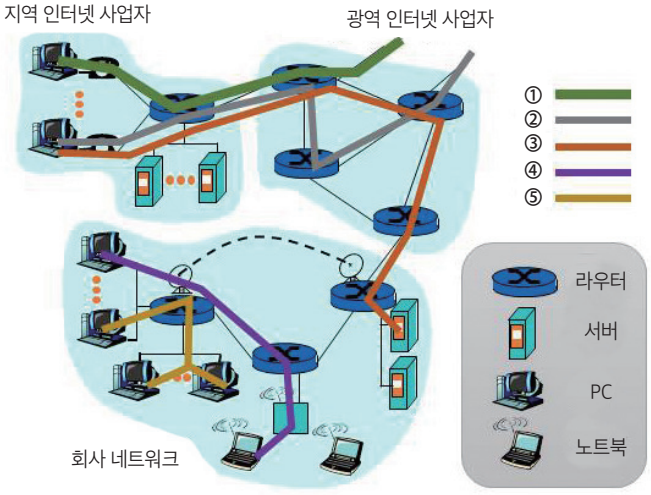


[그림 1] 인터넷과 인트라넷

이때, 인트라넷 구성은 인트라넷을 사용하고자 하는 조직 또는 기업의 사용 목적에 따라 내부 구성이 달라집니다. 소프트웨어 개발 회사에서 인트라넷을 구성하는 경우에는 사내에 개발을 위한 서버를 먼저 구축하고자 할 것입니다. 반면, 금융사의 경우에는 외부로부터의 네트워크 침입을 막기 위해 보안이 강력한 방화벽 및 여러 보안 장비(예 : 침입탐지 / 예방 시스템)들을 추가하면서, 안정적인 내부 인트라넷 망을 구성하고자 할 것입니다. 방송사의 경우 안정성도 중요하겠지만 예를 들자면, 사내에서 빠르고 안정적인 방송 데이터 실시간 편집/전송이 가능하도록 구성되어야 하는 등의 부가적인 목적에 따른 인트라넷 설계 및 구축이 필요할 것입니다.

II. 네트워크 관리의 중요성

네트워크 관리란 컴퓨터 네트워크를 구성하는 각 요소가 올바르게 동작하는지 각 요소에 대해 모니터링 등을 통해 지속적으로 확인하는 작업, 서버와 같은 장비를 추가할 때 이에 따른 네트워크 구성을 제어하고 네트워크 장애와 같은 문제가 발생하였을 때 대응하는 관리를 말합니다. [그림 2]에서, 몇 가지 발생 가능한 상황을 가정하고, 이에 따른 어떤 네트워크 관리를 필요로 하는지 나누어 살펴보고자 합니다.



[그림 2] 컴퓨터 네트워크와 네트워크 관리

1. 지역 인터넷 사업자에 속한 1대의 컴퓨터가 P2P를 통해 용량이 큰 동영상을 다운로드 하고 있는데, 속도가 느린 상황
   → ①, ②, ③이 모두 공통된 네트워크 장비를 통과하기에 상대적으로 느릴 수 있습니다. 해당 네트워크 장비에 많은 부하가 있는지를 살펴보아야 할 것입니다.
2. 지역 인터넷 사업자에 속한 다른 1대의 컴퓨터가 인터넷을 느리게 이용하는 상황
   → ①과 동일한 이유일 수도 있겠지만, 그림에서와 같이 불필요하게 1개의 네트워크 장비를 추가로 거치고 있기에 해당 원인을 파악해야 할 것입니다.
3. 회사원이 회사 네트워크에 접속하여 재택근무를 하였는데, 다음 날 다른 회사 내부 자료가 유출된 것으로 확인됨
   → 보안이 잘 유지되어 안전한 네트워크 접속이 유지되는지, 그리고 해당 접속이 있었을 때 네트워크 공격이 있었는지 확인할 필요가 있습니다.
4. 회사 내에서 노트북 사용자가 다른 PC 사용자와 파일을 주고받다가 접속이 끊어짐
   → 회사 내 Wi-Fi가 잘 동작하고 있는지 확인할 필요가 있습니다.
5. 회사 내에서 한 PC로부터 다른 2대의 PC에 자료를 전송하였는데, 2대 중 1대에서 자료를 받지 못하였다고 함
   → 관련 네트워크 장비에서 패킷이 다른 2대의 PC에 모두 성공적으로 전송되었는지 확인할 필요가 있습니다.

최영락
나임네트웍스 SDN기술팀 매니저

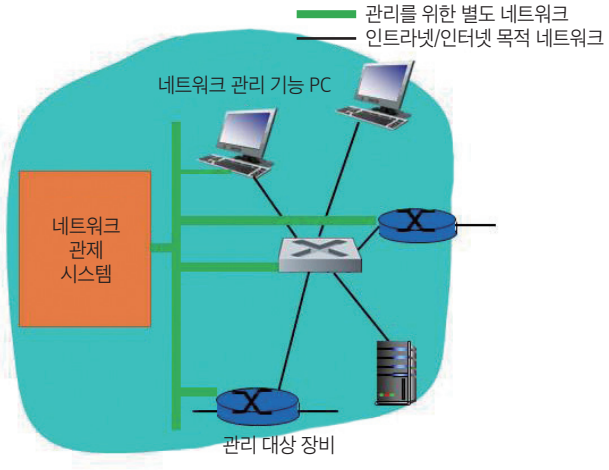
이와 같이, 네트워크 관리는 네트워크가 올바르게 동작하는지 점검(모니터링)하고 이에 따른 대처를 포함한 전반적인 관리를 의미합니다. 실제, 컴퓨터 네트워크 관리는 앞에서 언급한 5가지의 상황을 비롯해 관리해야 할 많은 사항이 있습니다. 특정 서버에 장애가 발생하였을 때에도 계속 서비스가 가능하도록 안정성 있는 네트워크를 구성하는 경우가 많습니다. 이를 네트워크 이중화라고 하는데, 이때 해당 네트워크 장비에 장애가 발생하는 경우 장애를 빠르게 감지하고 발 빠르게 대처하는 것 또한 중요합니다. 따라서 규모가 큰 회사 및 금융사, 방송사 등과 같이 안정적인 네트워크를 매우 중요하게 생각하는 회사 및 조직에서는 별도의 네트워크 관제 역할을 하는 기능 또는 시스템을 두어 네트워크 장비에 문제가 없는지 지속적으로 확인하는 일을 합니다.

네트워크 관리에 대해 이러한 중요성에 대해 가장 먼저 인지한 곳은 아무래도 네트워크 자체를 서비스로 만들어 개인 및 기업 고객에게 제공하는 통신사가 아닐까 생각합니다. 1980년대에, 통신사에서는 네트워크 관리 요소에 대해 ISO 규정으로 FCAPS라는 것을 규정하였습니다. 이 FCAPS는 장애(Fault) 관리, 구성(Configuration) 관리, 어카운팅(Accounting) 관리, 성능(Performance) 관리, 보안(Security) 관리, 이렇게 5가지 관리 요소에 대해 각 영어 첫 글자를 차례대로 나열한 것입니다. 자세한 설명은 [표 1]과 같습니다.

FCAPS 요소	설명
장애(Fault)	네트워크 장비에 장애가 발생하였을 때, 이를 감지하고 대처하는 관리 요소로, 장애 판단을 위한 테스트도 포함
구성(Configuration)	장비 추가 및 삭제, 그리고 네트워크 구성이 변경되었을 때에 따른 각 네트워크 장비 설정을 구성하는 관리
어카운팅(Accounting)	통신사의 경우, 망을 사용하는 개인 및 기업 고객이 가입하여 사용하므로, 각 고객에 따른 계정 정보 관리 및 사용한 네트워크에 따른 과금 정보 수집
성능(Performance)	네트워크 성능이 정상적인지 감시, 트래픽 및 통계 관리
보안(Security)	안전한 네트워크 사용을 위한 보안 관리

[표 1] FCAPS 각 요소 및 설명

III. SNMP와 네트워크 관리의 어려움



[그림 3] 네트워크 관리를 위한 관리 네트워크 구성 예시

[그림 3]과 같이 네트워크 관제 시스템을 갖추고 있는 경우, 안정적으로 네트워크를 관리하기 위해 별도의 관리 네트워크를 구성합니다. 해당 네트워크는 데이터 통신을 위한 인트라넷 또는 인터넷과는 달리 각 네트워크 장비가 올바르게 동작하는지 확인하고 네트워크 구성 요청 및 응답을 주고받기 위한 목적으로 사용하는 관리 목적의 별도 네트워크입니다. 해당 네트워크 관제 시스템에 접속하기 위해서 네트워크 관제 시스템에 접근 가능한 PC를 설치하거나, 또는 네트워크 관제 시스템을 인트라넷 또는 인터넷에 연결하여 허가된 사람만 접속 가능하도록 설정합니다.

SNMP(Simple Network Management Protocol)란 네트워크를 관리하기 위해 네트워크 관제 시스템과 각 네트워크 장비 사이에 어떤

식으로 관리 요청을 하고 응답을 받을 것인지를 규정한 프로토콜입니다. SNMP는 앞 연재에서 설명했던 TCP/IP 4계층에서 응용프로그램 계층에 해당하는 프로토콜로, 관리를 위한 별도 네트워크가 따로 구성되었기에 안정적이라고 가정하고 UDP를 사용하여 관제 시스템과 각 네트워크 장비 사이에서 빠르게 통신이 이루어집니다. 언뜻 보면 각 네트워크 장비를 관리하기 위한 목적이 있기에 위에서 설명한 FCAPS를 모두 고려하여 관리가 되어야 한다면, SNMP가 복잡할 수도 있다고 생각할 수도 있을 것 같습니다. 그러나 SNMP는 첫 대문자 S가 단순함을 의미하는 Simple이라는 단어에 걸맞게 생각보다 단순하게 [표 2]에서 설명하는 3가지 유형만을 규정하고 있습니다. (실제, SNMP는 GetNextRequest, GetBulkRequest, Response 등 여러 유형의 메시지가 더 있으나 [표 2]에서 언급되는 주요 3개의 메시지 유형의 주목적과 거의 들어맞기에 생략하였습니다.)

주요 SNMP 메시지 유형	설명
GetRequest	관제 시스템에서 특정 네트워크 장비에 정보를 요청함
SetRequest	관제 시스템에서 특정 네트워크 장비에 구성을 설정함
Trap	긴급/예외 상황일 때 관제 시스템에서 요청하지 않아도 네트워크 장비에서 정보를 관제 시스템에 보냄

[표 2] SNMP 주요 메시지 유형과 설명

네트워크 관제 시스템은 SNMP GetRequest 메시지를 사용하여 각 네트워크 장비로부터 정보를 가져와 네트워크 관리자 및 엔지니어가 쉽게 알아볼 수 있도록 화면에 나타내고, 새로운 장비가 추가되거나 네트워크 구성 변경 시 관제 시스템 화면에서 명령을 내리면 SNMP SetRequest 메시지를 사용하여 네트워크 장비 설정을 구성합니다. 또한, Trap을 사용하여 네트워크 장비로부터 긴급한 알림(예 : 여유 대역폭 부족)을 받기도 합니다. 그런데, SNMP만을 사용하여 네트워크 관제 시스템을 사용하는 것만으로는 다음과 같은 어려움이 있습니다.

1. 기본적으로, SNMP는 네트워크 관제 시스템에서 1대의 네트워크 장비를 대상으로 관리합니다. 복합적인 요인에 의해 네트워크가 느린 경우에는 관제 시스템에서 여러 네트워크 장비로부터 정보를 가져와 직접 판단해야 하는데 여러 대의 네트워크 장비 정보를 한 번에 보고 결정을 내리기가 쉽지 않습니다.
2. 네트워크 장비마다 SNMP를 사용해 정보를 가져오는 방법, 설정하는 방법 등이 제각각입니다. SNMP는 위와 같은 네트워크 관리를 위한 주요 3가지 목적의 메시지 유형만 규정되어 있고 대역폭 조회, 패킷 수 조회 등과 같은 구체적인 관리 대상 메시지는 MIB (Management Information Base)라는 것으로 규정합니다. 해당 MIB는 각 네트워크 장비 제조사마다 서로 다르게 정해져 있기에 이를 네트워크 관제 시스템에서 모두 확인하여 네트워크 관리를 수행해야 합니다.
3. 네트워크 관제 시스템에서 관리하고자 하는 기능이 때로는 각 네트워크 장비 제조사들에서 SNMP로는 지원하지 않는 경우가 있습니다. 각 네트워크 장비 제조사들에서도 자체 네트워크 관제 시스템을 출시하는 경우가 있는데, 표준 SNMP를 사용하지 않고 공개되지 않은 방식으로 관리되는 경우가 많아, 여러 제조사의 네트워크 장비를 사용하는 인트라넷을 관리하는 안정적인 네트워크 관제 시스템을 만들기가 쉽지 않습니다.

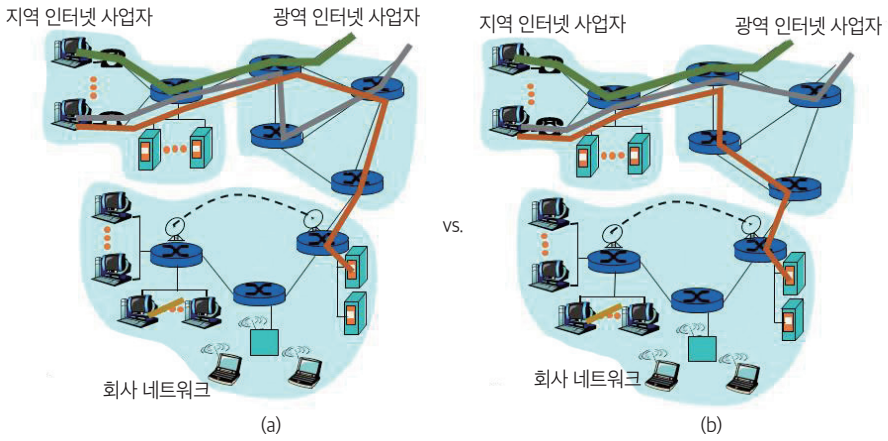
이와 같은 SNMP를 사용한 네트워크 관리에 어려움이 있어, 특정 네트워크 제조사 또는 기술력 있는 회사에서 개발한 네트워크 관리 소프트웨어를 활용한 네트워크 관제 시스템을 사용하는 경우가 많으며, 해당 시스템은 SNMP만을 이용하지 않고 여러 기술을 활용하여 안정적인 네트워크를 보장하고자 합니다.

IV. SDN의 등장과 네트워크 관리

SDN은 Software-Defined Networking, 즉 소프트웨어 정의 네트워킹의 약어로, 해당 용어를 풀어쓰면 '소프트웨어로 네트워크를 정의한다'는 의미가 됩니다. 그렇다면, 소프트웨어로 네트워크를 정의한다는 것이 어떤 의미를 담고 있는지 살펴보고자 합니다.

최영락
나임네트웍스 SDN기술팀 매니저

이전 연재에서, 네트워크 계층에 대해 이야기하고 '패킷의 경로를 결정하고 보내는 역할'을 수행하는 라우터라는 네트워크 장비에 대해 언급한 적이 있습니다. [그림 4]와 같이 총 3개의 네트워크 연결이 이루어져 있는 두 상황이 있을 때 왼쪽보다 오른쪽이 더 최적화된 네트워크 연결임을 우리는 쉽게 알 수 있을 것입니다. 회색으로 된 네트워크 연결의 경우, 광역 인터넷 사업자 망에서 왼쪽 아래 라우터를 거치지 않고도 바로 경로 설정이 되는 상황, 그리고 주황색으로 된 네트워크 연결은 경로가 변경된 회색 연결과 덜 겹치도록 경로가 설정되는 것이 왼쪽 그림보다 더 최적화된 결과를 보여줄 것입니다.



[그림 4] 여러 네트워크에 걸쳐 있는 두 네트워크 연결 상태

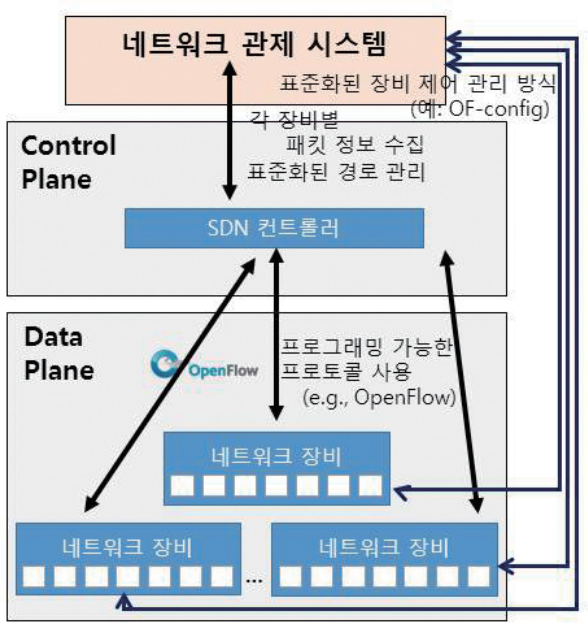
라우터는 패킷의 경로를 설정할 때, 해당 장비에서 얻은 정보만을 사용하기에 왼쪽과 같은 최적화되지 않은 결과를 가져올 수 있습니다. 반면, 우리가 왼쪽보다 오른쪽 상태가 더 최적화된 상태임을 쉽게 알 수 있는 것처럼, 각 라우터에서 얻은 정보들을 모두 보고 네트워크 경로를 판단한다면 가장 최적화된 경로를 계산하기 더욱 쉬울 것입니다. 앞에서 설명했던 네트워크 관리의 어려움과 포함하여 관련된 필요성을 정리하면 다음과 같습니다.

1. 가장 최적화된 경로를 계산하기 위해서는 중앙화된 경로 관리가 가능한 체계가 필요
2. 각 네트워크 장비 제조사에 의존적이지 않은 관리 체계 필요
3. 패킷 경로를 변경하고자 할 때, 프로그래밍 등으로 유연성 있게 변경 가능한 체계 필요

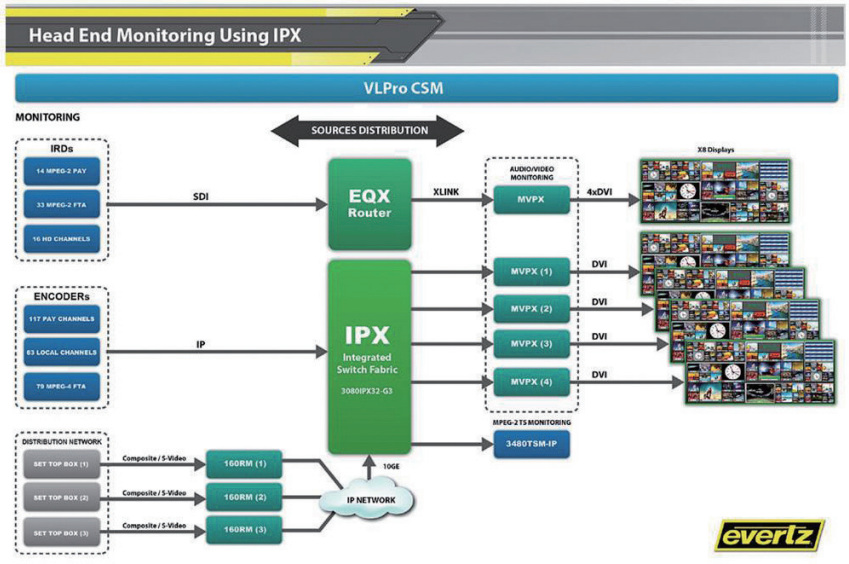
이러한 필요성들을 충족하게 하는 SDN은 네트워크를 관리하는 영역인 제어 평면과 데이터를 처리하는 영역인 데이터 평면으로 구분하고, 네트워크 경로 설정을 'SDN 컨트롤러'라는 곳에서 중앙 관리하여, 각 네트워크 장비에서 경로를 결정해야 할 때, SDN 컨트롤러에 묻고 경로를 정하거나, 또는 SDN 컨트롤러에서 최적화된 경로를 각 네트워크 장비에 설정하는 방식 등을 통해 최적화된 경로를 사용합니다. 이때, 오픈플로우(OpenFlow)라고 하는 표준화된 방식을 사용하여, 각 네트워크 장비 제조사에 의존되지 않은 방식으로 관리하고, 경로 설정 또한 프로그래밍을 통해 유연하게 변경 가능하도록, 일종의 소프트웨어를 통해 네트워크를 유연성 있게 변화한다고 하여, 소프트웨어 정의 네트워킹, 즉 SDN이라는 용어가 등장하였습니다.
[그림 5]는 SDN을 사용한 제어 평면과 데이터 평면의 분리와 함께 네트워크 관제 시스템을 활용한 네트워크 관리 구성도를 나타낸 것입니다. SDN 컨트롤러의 주목적은 각 네트워크 장비를 통과하는 패킷 정보를 지속적으로 저장 및 관리를 하고, 각 네트워크 장비에서 SDN 컨트롤러로 최적화된 경로를 물어볼 때 알려주거나, 또는 직접 SDN 컨트롤러에서 경로를 지정하는 역할을 수행합니다. 이때, 네트워크 관제 시스템은 SDN 컨트롤러로부터 각 네트워크 장비별로 수집된 패킷 정보 및 경로 정보를 가져와 보여주고, 사용자에게 경로 관리에 필요한 정보를 입력하도록 지원합니다. 뿐만 아니라, 기존 SNMP에서 패킷 이외의 장비에 대해 필요한 관리에 대해서는 OF-Config

라는 표준화된 방식을 통해 각 네트워크 장비를 모니터링 및 제어, 관리가 가능해집니다.

여러 서버 컴퓨터와 네트워크 회선 등을 제공하는 대규모 시설을 데이터센터라고 하는데, 구글은 SDN을 사용하여 전 세계에 걸친 구글 데이터센터 간 트래픽을 최적화하여 회선 비용을 대폭 절감한 사례를 선보였습니다. 이후, SDN은 네트워크 분야에서 '파괴적 기술'이라고 부를 정도로 큰 화두가 되었고, 이에 기존 네트워크 장비 제조사들은 표준화된 방식 사용에 따른 자사 장비 이용률 저하 등으로 인한 수익 감소를 우려하여 오픈플로우와 같은 표준화된 방식은 아니지만 자체적인 SDN 역할을 하는 방식 및 제품을 출시하기도 합니다. 또한, 네트워크 분야에서 '소프트웨어 정의'라는 개념이 성공적으로 이루어져, 소프트웨어 정의 스토리지, 소프트웨어 정의 데이터 센터와 같은 SDS, SDDC 용어가 등장하고, 심지어는 데이터 센터 내 모든 것을 정의한다는 SDx(Software Defined Anything/Everything)이라는 용어 또한 등장하였습니다. 그리고 [그림 6]과 같이 이를 비디오 네트워크 등 구체적인 분야에 소프트웨어 정의 개념을 활용하여 대용량의 비디오 데이터에 대해 복잡한 네트워크 환경에서 최적화된 고성능을 제공하는 솔루션 또한 출시되기도 하였습니다.



[그림 5] OpenFlow, OF-Config를 사용한 표준화된 SDN과 네트워크 관리



[그림 6] 소프트웨어 정의 비디오 네트워크(SDVN), 출처 : http://www.evertz.com

이번 연재에서는 인터넷과 이에 대비되는 용어인 인트라넷을 설명하고, 네트워크 관리의 중요성 및 네트워크 관리 프로토콜에 해당하는 SNMP, 그리고 소프트웨어 정의 네트워킹에 해당하는 SDN에 대해 살펴보았습니다. 그동안 총 11편의 연재에 걸쳐, '컴퓨터 네트워크의 이해 및 활용'을 주제로 다양한 내용을 살펴보았는데, 방송에 점차 많이 활용되고 있는 컴퓨터 네트워크에 대해 보다 친숙해지셨기를 바랍니다. 감사합니다.