최영락
휴레이포티지브 선임연구원 & 오픈플로우코리아 기술매니저

가상화와 컴퓨터 네트워크의 활용 3: 데이터센터와 네트워크 가상화

최영락 휴레이포티지브 선임연구원 & 오픈플로우코리아 기술매니저

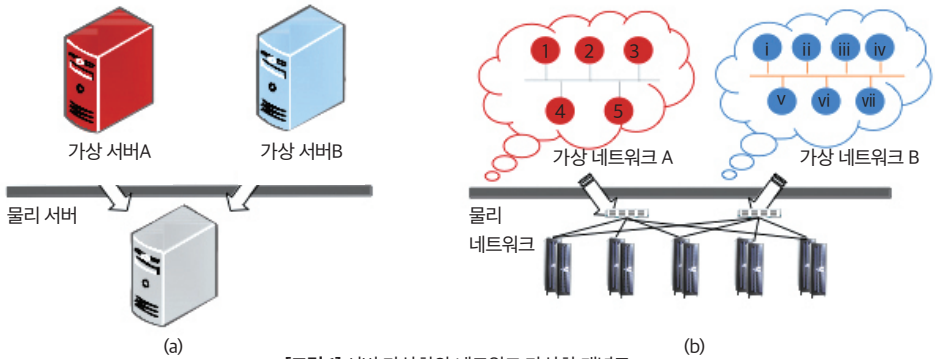
- 연재목록 -

지난 연재에서는 데이터센터 네트워크 스위치의 구분(Core, Aggregate, Access), TOR 스위치, 서버 랙 유형 등과 같은 데이터센터 네트워크 관련 여러 용어 및 데이터센터 네트워크에 사용 가능한 다양한 토폴로지 유형에 대해 살펴보았습니다. 이번 연재에서는 네트워크 가상화라는 개념 및 네트워크 가상화가 데이터센터 네트워크와 어떤 관련이 있는지를 중심으로 하여 살펴보고자 합니다.

네트워크 가상화란?

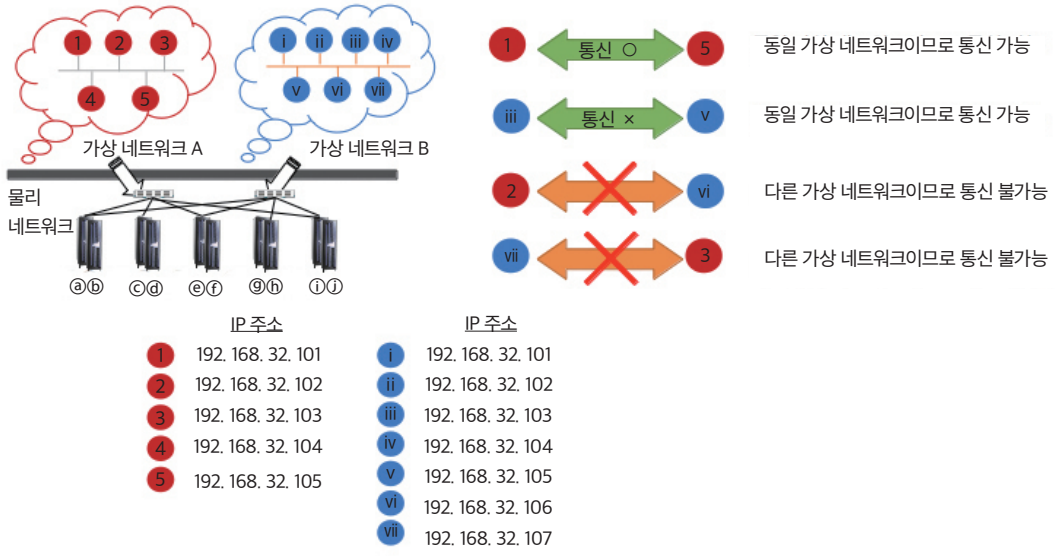
지난 4월 첫 연재에서는 가상화가 무엇인지 살펴보았었습니다. 가상화를 한 마디로 정리하자면, **'물리적, 논리적 자원을 추상화시켜 실제와 같은 자원으로 사용 및 관리 가능하도록 하는 기반 환경과 기술'**에 해당합니다. 일반적으로 가상화라고 하면 하나의 물리 서버 위에 여러 가상 서버들을 각각 마치 실제 물리 서버처럼 사용하는 서버 가상화를 많이 떠올립니다. 그런데, 서버 가상화가 물리 서버에 대한 가상화를 의미하듯이, 네트워크에서도 물리 네트워크를 가상화하여 사용한다는 '네트워크 가상화'라는 용어 또한 있습니다.

네트워크 가상화란 **하나의 물리 네트워크 위에서 여러 가상 네트워크를 생성하고, 각각의 가상 네트워크를 마치 실제 물리 네트워크와 같이 사용하는 기술을 통칭하는 용어**입니다. [그림 1]에서는 서버 가상화와 네트워크 가상화에 대한 개념도를 나타냅니다. 서버 가상화가 하나의 물리 서버에서 하이퍼바이저(Hypervisor)가 동작하여 논리적인 단위의 여러 가상 서버들을 생성하여 마치 실제 물리 서버인 것처럼 사용하는 기술인 반면, 네트워크 가상화는 여러 서버들 및 스위치, 라우터 등과 같은 네트워크 장비들과 함께 이루어진 물리 네트워크를 논리적인 여러 가상 네트워크로 쪼개어 각각을 마치 실제 물리 네트워크처럼 사용하는 기술을 이야기합니다.



[그림 1] 서버 가상화와 네트워크 가상화 개념도

네트워크 가상화에 대해 조금 더 구체적으로 [그림 1]의 개념도와 함께 살펴보겠습니다. [그림1 (b)]에서는 10대의 물리 서버와 2대의 스위치가 있으며, 각각의 물리 서버에는 모두 하이퍼바이저가 설치되어 있는 상태에서 총 12대의 가상 서버들이 실행 중입니다. 그리고 붉은색으로 도식화한 5개의 가상 서버들은 자체 네트워크를 통해 서로 연결되어 있으며, 파란색으로 도식화한 7개의 가상 서버들 역시 별도의 네트워크를 통해 서로 연결되어 있는 상태입니다. 이 때, 하나의 물리 네트워크 위에 2개의 가상 네트워크가 따로 존재하도록 구성이 된다면, [그림 2]와 같은 네트워크 구성이 가능합니다.



[그림 2] 네트워크 가상화 환경에서의 가상 네트워크

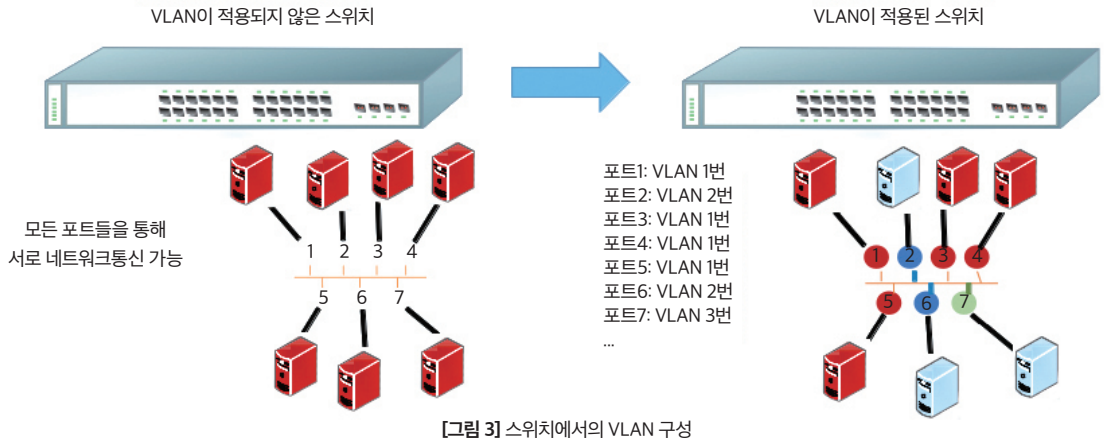
실제로 1개의 물리 네트워크가 존재함에도 네트워크 가상화를 통해 서로 다른 2개의 가상 네트워크를 만들었다면, 해당 가상 네트워크들은 서로 구분이 이루어지기에 IP 주소가 서로 중복되지 않습니다. 즉, 붉은색 가상 머신 1대와 파란색 가상 머신 1대의 IP 주소가 동일하게 192.168.32.101로 설정하더라도 IP 주소의 충돌 없이 두 가상 네트워크 모두 안정적으로 동작합니다. 즉, 별도의 네트워크로 간주하므로 같은 IP 대역을 사용해도 문제가 없습니다. 이와 같이 네트워크 가상화 기술이 잘 이루어진다면 가상 서버에 할당된 IP 주소들을 변경하지 않고도 가상 서버를 여러 가상 네트워크로 복제하여 IT 서비스를 준비하는 것도 가능할 것입니다. 반면, 별도의 추가 구성이 없다면 붉은색 네트워크와 파란색 네트워크는 서로 완벽히 격리되어 있어, 붉은색 가상 서버와 파란색 가상 서버들은 서로 통신이 불가능할 것입니다.

이때, 서버 가상화가 하이퍼바이저를 통해 가상 서버들을 지원하는 것과 달리, 네트워크 가상화는 하이퍼바이저와 같은 어떤 하나에 의해서 가상 네트워크를 지원한다고 이야기하기가 매우 어렵습니다. 이는 물리 네트워크를 이루고 있는 구성 요소들이 상대적으로 많기 때문이라 할 수 있습니다. 서버 가상화의 경우에는 물리 서버에서 동작하는 하이퍼바이저에 의해 가상 서버들을 관리하는 반면, 네트워크 가상화의 경우에는 네트워크 장비만 하더라도 여러 스위치, 라우터들로 구성되어 있는 경우가 많습니다. 즉, 하나의 물리 네트워크를 이루고 있는 모든 네트워크 장비들이 네트워크 가상화 기술을 지원하여야 네트워크 가상화가 이루어진다고 할 수 있을 것입니다. (이에 따라, 네트워크 가상화에서는 하이퍼바이저란 용어보다는 컨트롤러 등의 용어를 사용하여 통합/중앙 관리된다는 개념으로 접근하는 경우가 일반적입니다.) 그리고 네트워크 장비 제조사 또한 다양하다보니 네트워크 가상화와 관련된 기술의 종류가 다양하며, 네트워크 요구사항에 따라 적용하는 네트워크 가상화 기술 또한 달라집니다.

최영락
휴레이포티지브 선임연구원 & 오픈플로우코리아 기술매니저

VLAN 기술

본 연재에서는 여러 네트워크 가상화 기술 중 VLAN(가상 LAN, Virtual LAN)이라고 하는 기술을 살펴보고자 합니다. VLAN이라는 용어는 가상이라는 영단어인 Virtual의 앞 대문자 V와 뒤의 LAN이라는 단어로 이루어져 있습니다. 컴퓨터 네트워크를 규모에 따라 LAN(Local Area Network), MAN(Middle Area Network), WAN(Wide Area Network)로 구분하기도 하는데, LAN은 가정, 학교, 회사 내의 비교적 작은 규모의 환경에서 장비 간 통신에 사용되는 네트워크를 의미하는 반면, WAN은 학교와 학교, 회사와 회사 등의 두 개 이상의 LAN을 연결하는 네트워크를 이야기합니다. 따라서 VLAN이라는 용어에 LAN이 들어가는 만큼, VLAN은 LAN과 같은 소규모에서 적용되는 네트워크 가상화 기술에 해당합니다. (예를 들어, 미국과 한국 네트워크를 서로 연결하는데 있어 VLAN 네트워크 가상화 기술을 사용한다고 할 수는 없을 것입니다.)



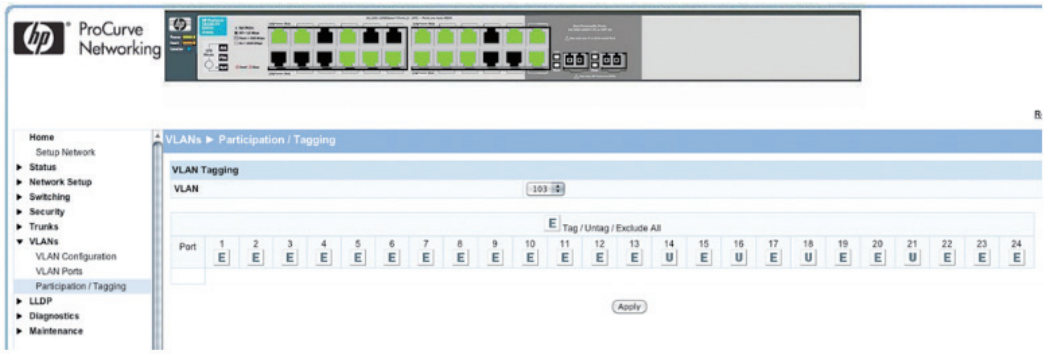
[그림 3] 스위치에서의 VLAN 구성

[그림 3]은 스위치에 VLAN을 적용하여 3개의 가상 네트워크로 구분한 것입니다. 스위치에는 각 포트별로 포트 번호가 할당되어 있는데, VLAN 기술이 지원되는 네트워크 스위치에서는 스위치에 있는 각 포트 번호에 VLAN 번호를 부여할 수 있습니다. 예를 들면, 포트 번호 1, 3, 4, 5번에는 VLAN 1번을 부여하고, 포트 번호 2와 6에는 VLAN 2번을, 그리고 포트 번호 7에는 VLAN 3번을 부여하는 식으로 설정한다면, [그림 3]의 오른쪽과 같이 3개의 가상 네트워크가 만들어지고 서로 다른 가상 네트워크에 할당되어 있는 컴퓨터들은 서로 네트워크 통신이 불가능하게 됩니다. 이 때, 스위치에 연결되어 있는 서버들은 VLAN 번호가 어떻게 부여되었는지 알지 못합니다. 즉, 네트워크 스위치에서 VLAN 번호를 설정하여 3개의 가상 네트워크가 생성되었으며, 3개의 스위치를 사용하고 각 스위치에 컴퓨터들을 연결된 것처럼 사용이 가능하다는 것입니다.

VLAN 설정 명령어 (예 : Cisco 장비)

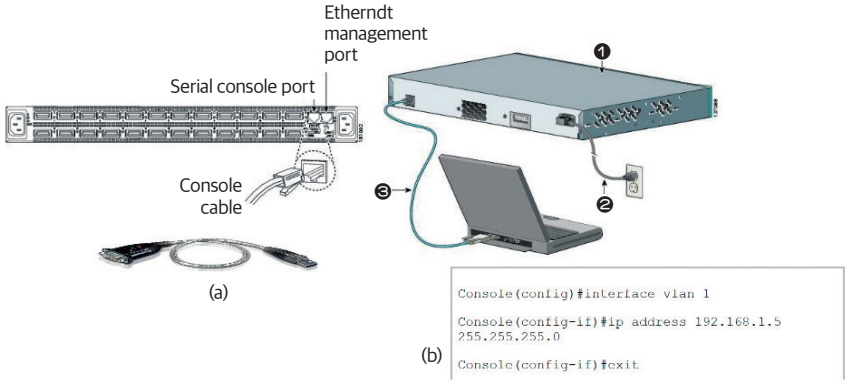
Switch(config)# vlan_id	VLAN 번호 생성 명령어
Switch(config - vlan)# name vlan_name	VLAN에 이름 부여
Switch(config - if)# switchport mode access	스위치 포트를 VLAN 사용 가능한 모드 (access 모드)로 변경
Switch(config - if)# switchport access vlan vlan_id	해당 스위치 포트에 VLAN 번호 부여

VLAN 설정 화면 (예 : HP 장비)



[그림 4] VLAN 구성 화면

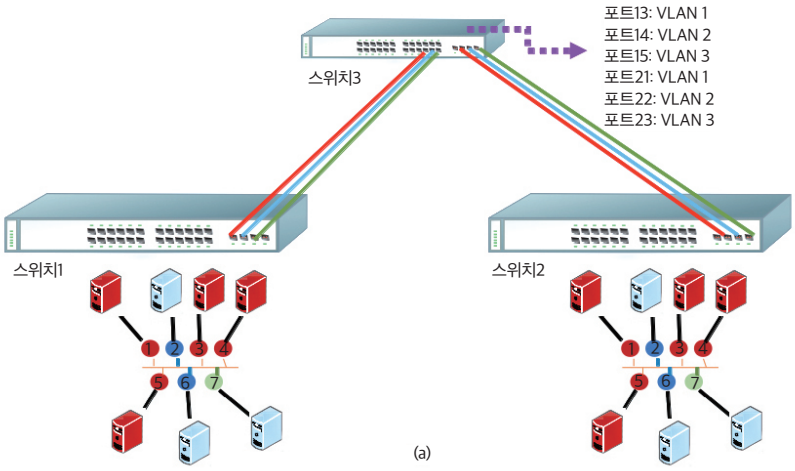
실제 스위치에 VLAN을 구성하는 방식은 [그림 4]와 같이 해당 스위치에 콘솔 모드로 접속하여 명령어를 실행하는 방식과 웹 브라우저를 통해 접속하여 클릭을 하여 설정하는 2가지 방식이 있습니다. 전자를 영어로는 CLI(명령어 라인 인터페이스, Command Line Interface) 방식이라 하고, 후자는 GUI(그래픽 사용자 인터페이스, Graphical User Interface) 방식이라고도 합니다. 웹 브라우저를 통해 접속하여 구성하는 GUI 방식은 [그림 4]와 같이 상대적으로 쉽게 알아볼 수 있으며, 구성 또한 매뉴얼(설명서)에 따라 단계별로 구성하기에 어렵지 않습니다. 그러나 대부분의 네트워크 엔지니어 분들께서는 CLI 방식을 보다 선호합니다. CLI 명령어들을 처음에 학습하는 데는 시간이 걸리지만, 명령어 내용들을 따로 저장해 두어 필요한 경우, 명령어 재확인 및 재사용이 가능합니다. 그리고 네트워크 구성에 어떤 문제가 생기는 경우에는 입력했던 명령어들을 확인하여 네트워크 구성에 어떤 문제가 있는지 확인 또한 가능합니다. 이와 같이 CLI 명령어 방식은 사용하기에는 GUI 방식보다 다소 불편하더라도 여러 장점을 가지고 있으며, 일부 네트워크 장비들의 경우 CLI 명령어 방식만 지원하는 경우도 있어 많은 네트워크 엔지니어 분들은 CLI 명령어 방식을 선호합니다. 참고로, VLAN 구성과 같은 명령어들을 실행하기 위해서는 일반 네트워크 장비에 접근하는 방식으로 설정하는 것이 아닌, 해당 네트워크 장비에 관리 모드(admin mode)로 접속해서 설정을 해야 합니다. 네트워크 장비의 특정 부분(보통 뒷 부분)에 관리 포트가 있어, 해당 포트에 컴퓨터를 연결 및 접속하여 네트워크 장비를 설정합니다. 이 관리 포트는 전통적으로 직렬(Serial) 콘솔 포트를 사용하였습니다. 9개의 핀으로 된 시리얼 포트를 통해 컴퓨터와 직접 연결하는데, 요즘 컴퓨터들에는 이 시리얼 포트가 없는 경우가 많아 USB-직렬포트 변환 잭을 사용하는 경우가 많습니다. 시리얼 콘솔 연결하는 프로그램을 사용하면 바로 CLI 명령어들을 입력 가능한 화면이 나타납니다. 최근에는 스위치에 관리 목적의 IP 주소를 부여하여 포트에 연결된 컴퓨터로부터 텔넷(telnet)이나 SSH(Secure Shell) 연결을 맺어 CLI 명령어들을 실행할 수 있습니다. 이때는 관리자만 접속 가능하도록 설정하기 위해 접속 가능한 IP 주소 등을 제한하는 경우가 많습니다.



[그림 5] 관리 콘솔 연결 및 네트워크 장비 관리 IP 주소 설정 / 출처 : Cisco

최영락
휴레이포티지브 선임연구원 & 오픈플로우코리아 기술매니저

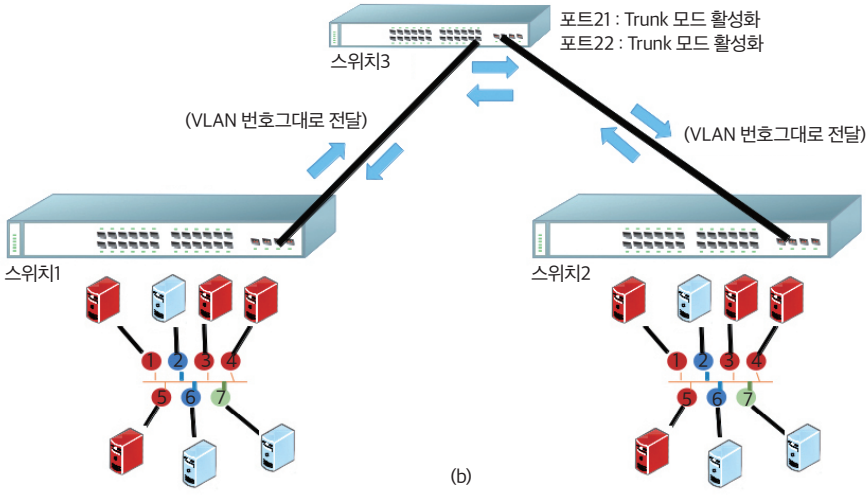
VLAN - 트렁크 모드



[그림 6] 2개의 스위치에 설정된 VLAN을 기반으로 서로 연결시키는 경우

[그림 6]과 같이 2개의 스위치(스위치 1, 스위치 2)가 있으며, 해당 스위치에는 여러 물리 서버들이 연결되어 있고, 각각 3개의 VLAN을 사용하고 있다고 가정합시다. 이때, 만약 스위치 1에 연결되어 있는 3번 컴퓨터가 스위치 2에 연결된 5번 컴퓨터와 통신을 하고 싶어하는 경우에는 스위치 1과 스위치 2가 서로 연결되어 있어야 할 것입니다. 스위치 1과 스위치 2를 직접 연결해도 무방하지만, 보다 쉽게 살펴보기 위해 스위치 3이 있다고 가정하는 경우, 빨간색 VLAN(VLAN 1번), 파란색 VLAN(VLAN 2번), 녹색 VLAN(VLAN 3번)이 모두 통신하기 위해서는 스위치 3에 총 6개의 포트를 필요로 합니다. 즉, 스위치 1에 있는 3번 컴퓨터는 스위치 3의 포트 13번으로 트래픽이 전송된 후, 해당 트래픽은 포트 21번을 통해 스위치 2에 전달되어 스위치 2에 있는 5번 컴퓨터로 잘 전달되는 것입니다.

그런데 이와 같이 구성을 하는 경우, VLAN을 사용해 여러 가상 네트워크를 만들어낼 수 있음에도 불구하고 가상 네트워크를 생성할 때마다 스위치 간 연결하는 선 작업을 별도로 해야 하는 문제가 생깁니다. (문제가 아니라고도 생각할 수 있지만, 여간 불편한 일임에는 분명할 것입니다.) 이를 위해 스위치에서는 특정 포트를 트렁크(Trunk) 모드로 설정이 가능합니다.



[그림 7] 트렁크 모드를 사용한 VLAN 통신

트렁크 모드를 사용하면 스위치 1에서 스위치 3으로 트래픽이 흐를 때, 네트워크로 해당 VLAN 번호를 그대로 전달시킵니다. 따라서 트렁크 모드로 설정되었다면, 스위치 1에 연결된 3번 컴퓨터에서 데이터를 전송하고, 해당 네트워크 데이터를 스위치 3에서 확인하면 'VLAN 1번'이 부여되었음을 확인할 수가 있습니다. 그리고 이 네트워크 데이터는 스위치 2에 그대로 전달되기에 스위치 2에서 5번 컴퓨터로 전달되는데 문제가 없는 것입니다. 이와 같이 트렁크 모드를 설정하면 여러 가상 네트워크를 생성하더라도 동일한 케이블을 통해 VLAN 번호가 그대로 전달되므로 추가로 케이블 작업을 하지 않고도 설정 가능하다는 장점이 있습니다. 그러나 하나의 케이블을 통해 트렁크 모드를 설정하는 경우에는 해당 포트로 모든 트래픽이 집중된다는 단점 또한 갖고 있습니다.

VLAN과 데이터센터 네트워크

이와 같은 VLAN을 사용하여 얻을 수 있는 가장 큰 장점으로는 한 물리 네트워크 내에서 전체적으로 퍼지던 브로드캐스트 트래픽이 감소한다는 장점이 있겠습니다. 특히, 데이터센터 네트워크에서는 하나의 브로드캐스트 트래픽이 전체 2계층(L2)으로 전달된다면 전달받을 필요가 없는 연결된 모든 스위치 및 물리 서버들에게 전달됩니다. 이 트래픽양이 전체적인 관점에서 볼 때는 굉장히 많아지며, 게다가 각 스위치들이 내부적으로 어떤 포트에 어떤 MAC 주소를 갖고 있는지에 대한 정보를 갖는데 이에 따른 불필요한 트래픽이 증가한다면 데이터센터 네트워크의 성능을 잡아먹는 주요 요인이 될 것입니다. 따라서 VLAN과 같은 네트워크 가상화 기술을 사용하면 하나의 네트워크를 작게 나눌 수 있게 있어 브로드캐스트 영역도 작아지고, 트래픽 또한 감소하여 대역폭의 낭비를 줄일 수 있습니다. 사실, 이러한 장점이 있어 VLAN은 데이터센터와 같은 대규모 환경이 아니더라도 적용 가능하지만, 소규모 환경의 경우 관리적인 이점이 주로 부각되는 반면, 네트워크 규모가 점차 커질수록 VLAN은 트래픽 감소의 장점 또한 갖습니다.

그러나 VLAN은 데이터센터 네트워크에 만능으로 적용할만한 해결책이라고 하기에는 사실상 어렵습니다. 대표적인 이유로, 대규모 데이터센터 네트워크에서는 많은 개수의 가상 네트워크를 필요로 하는데 VLAN은 이론상 최대 4,096개로 제한되어 있습니다. 특히, 물리 서버만을 고려하는 것이 아닌 가상 서버들을 고려하는 경우, 물리 서버 내부에서 여러 대의 가상 서버들이 VLAN을 사용하도록 설정할 수가 있는데, 이 경우 데이터센터 네트워크가 정말 복잡해집니다. 그리고 하나의 물리 서버에 있던 가상 서버가 다른 쪽 물리 서버로 옮겨지는 경우를 마이그레이션(Virtual Machine Migration)이라고 하는데, 이에 따른 VLAN 번호 이동 등을 같이 고려하면 데이터센터 네트워크 관리가 정말 복잡해집니다. 또한 VLAN은 사실 2계층(L2)에 해당하는 기술이기에, 한국과 미국을 연결하는 경우 등의 WAN 환경에서 가상 네트워크를 고려하는 경우에는 적합한 네트워크 가상화 솔루션이 되지를 못합니다. 본 연재에서는 네트워크 가상화를 설명하기 위해 실제 현업에서도 현재 많이 사용하는 VLAN을 살펴보았으나, 네트워크 가상화 기술은 VxLAN(Virtual eXtensible LAN), GRE(Generic Routing Encapsulation), NVGRE(Network Virtualization using GRE), STT(Stateless Transport Tunneling) 등의 다양한 오버레이 형태의 네트워크 가상화 기술 및 SDN(소프트웨어 정의 네트워킹, Software Defined Networking)을 활용한 해결책 등 다양한 방식이 있음을 참고하셨으면 합니다.

이와 같이 이번 연재에서는 네트워크 가상화 및 네트워크 가상화 중 VLAN 기술을 위주로 살펴보았습니다. 다음 연재에서는 가상화와 스토리지와 관련해 살펴볼 예정입니다.