최영락
휴레이포지티브 선임연구원 & OVNC 기술매니저

가상화와 컴퓨터 네트워크의 활용 - 8 : 활용 사례 - (2)

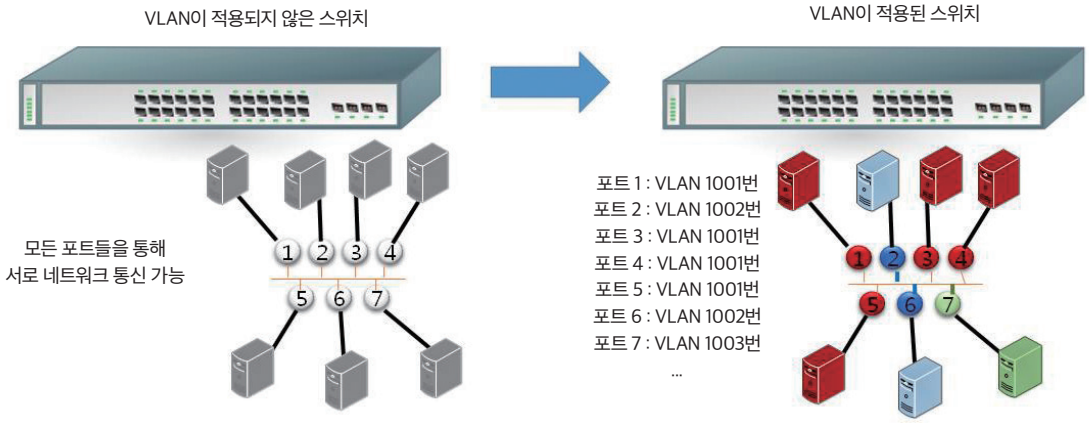
최영락 휴레이포지티브 선임연구원 & OVNC 기술매니저

- 연재목록 -

지난 연재에서는 가상화와 컴퓨터 네트워크와 관련된 활용 중 하나로, 방송 인코딩 및 전송을 사례로 하여 방송 인코딩 및 트랜스코딩 품질과 관련된 내용을 설명하였습니다. 이번 연재에서는 지난 6월 연재에서 살펴보았던 VLAN을 주제로 하여 관련된 활용 사례를 설명하고자 합니다.

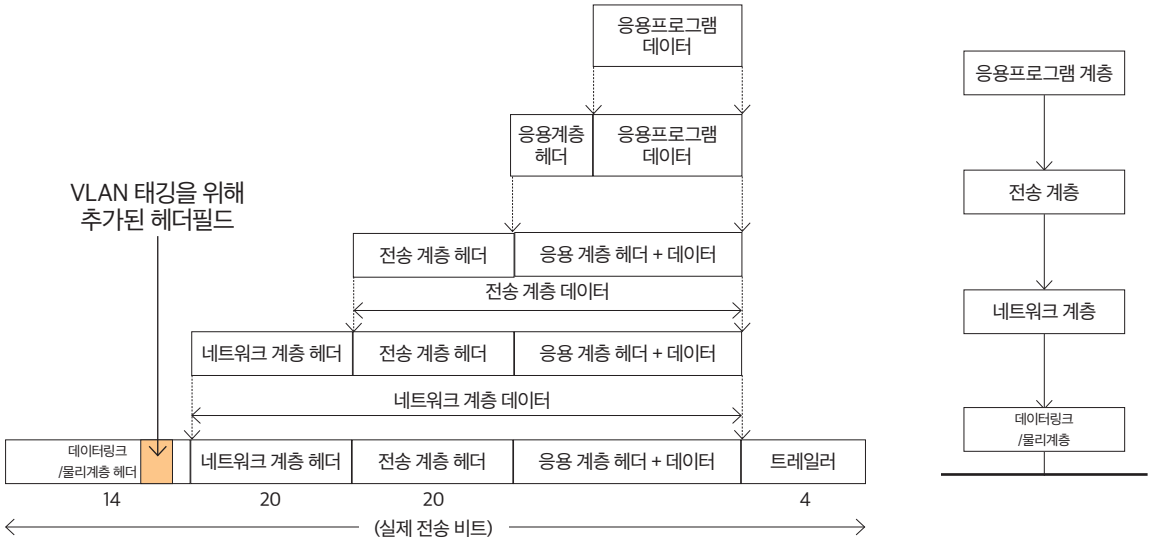
VLAN과 네트워크 2계층

지난 6월 연재에서는 VLAN(Virtual LAN)에 대해 살펴보았습니다. [그림 1]을 보면서 VLAN에 대해 잠시 복습해 보고자 합니다. [그림 1]은 스위치에 VLAN을 사용하여 3개(빨강, 파랑, 녹색)의 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 1001번을 부여하고, 포트 번호 2와 6에는 VLAN 1002번을, 그리고 포트 번호 7에는 VLAN 1003번을 부여하는 식으로 설정한다면, [그림 1]의 오른쪽과 같이 3개의 가상 네트워크가 만들어집니다. 이 때, 서로 다른 가상 네트워크에 할당되어 있는 컴퓨터들은 서로 다른 네트워크에 속한 컴퓨터와 통신이 불가능합니다. 포트1에 연결된 컴퓨터는 포트7에 연결된 컴퓨터와 통신이 불가능하다는 이야기입니다. 이 상황에서 스위치에 연결되어 있는 각 서버들은 VLAN 번호가 어떻게 부여되었는지 알지 못합니다. 네트워크 스위치에서 VLAN 번호를 설정하여 관리하므로 각 서버 입장에서는 마치 3개의 서로 다른 개별 스위치를 사용하는 것처럼 스위치 장비를 사용합니다. 이와 같이 물리 네트워크상에서 여러 개의 가상 네트워크를 사용하는 식으로 VLAN 기술을 사용하여 네트워크 가상화 구현이 가능합니다.



[그림 1] 스위치에서의 VLAN 구성

VLAN을 적용하는 대상은 일반적으로 [그림 1]과 같이 스위치에 해당하는 네트워크 장비에서 이루어집니다. (실제, 서버 가상화와 네트워크 가상화가 맞물려 복잡하게 적용되는 환경에서는 하나의 물리 서버에서 생성한 가상의 네트워크에 VLAN 적용 또한 이루어지지만, 이에 대해서는 뒤에서 살펴보고자 합니다.) 스위치는 TCP/IP 4계층을 기준으로 하면 '데이터링크/물리 계층'에서 동작하는 네트워크 장비로, OSI 7 계층을 기준으로 하면 2계층(L2, Layer 2)에서 동작하는 네트워크 장비입니다. 이를 통해 예상할 수 있듯이, VLAN 기술은 네트워크 스위치와 같은 L2 네트워크 장비에 적용 가능한 기술, 즉 L2에서 적용되는 네트워크 가상화 기술입니다. TCP/IP 4계층에 기반하여 살펴보면 [그림 2]와 같이 데이터링크/물리 계층 헤더 부분에 VLAN 헤더 필드 정보가 추가로 붙어 네트워크 가상화가 이루어집니다.

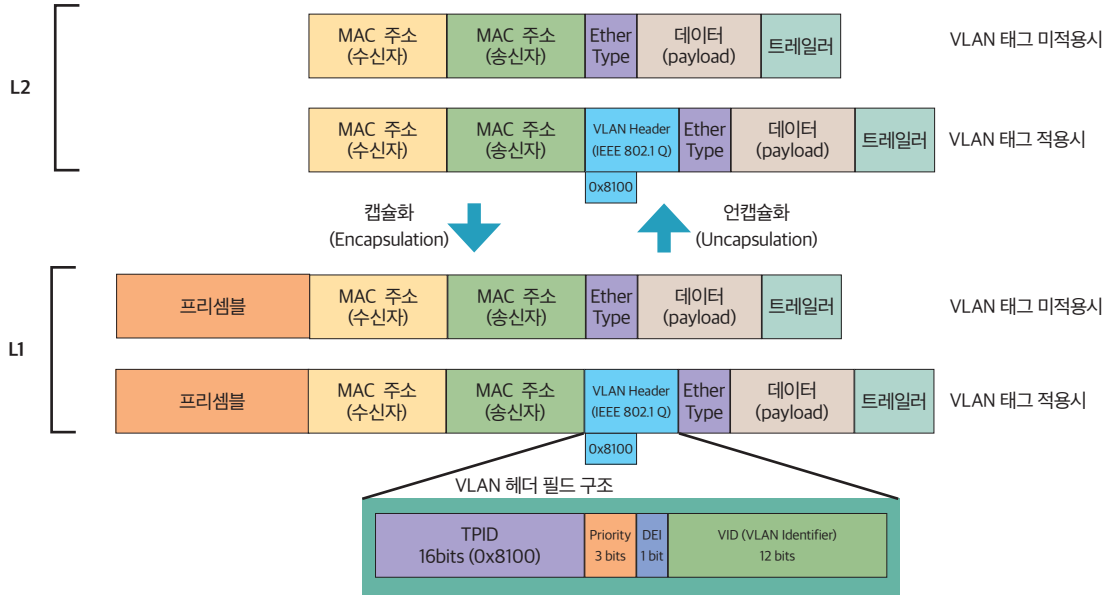


[그림 2] TCP/IP 4계층과 VLAN 헤더 필드

[그림 3]은 VLAN 헤더 필드 구조 및 OSI 7 계층을 기준으로 MAC 주소를 가지고 통신하는 이더넷(Ethernet)에 해당하는 1계층, 그리고 2계층에서 VLAN 태그가 적용되지 않았을 때와 적용되었을 때의 구조를 보여주고 있습니다. VLAN 태그가 적용되지 않았을 때의 부분에 보이는 EtherType 필드는 이더넷 프레임이 어떤 종류인지, 그리고 프레임 크기가 얼마나 될 것인지를 정하는 16비트 구조로 되어 있습니다. VLAN 기술이 사용되면 [그림 3]과 같이 VLAN 헤더가 추가로 붙는 구조로 적용됩니다. VLAN 헤더 각 필드에 대한 자세한 설명은 다음과 같습니다.

- **TPID(Tag Protocol Identifier) :** 16비트로 되어 있으며, 기존 VLAN이 적용되지 않았을 때의 프레임에서 같은 위치에 있는 EtherType 부분과 같은 위치에 있습니다. 기존 EtherType과 구분하기 위해 16진수로 8100(10진수: 33,024) 이라는 고정값을 사용합니다. 즉, TPID 부분에 8100이라는 값이 오면 VLAN이 적용된 프레임이며, 그렇지 않은 경우에는 기존 'VLAN 태그 미적용' 기준으로 프레임을 판단하고 분석하는 것입니다.
- **Priority :** 해당 프레임과 관련하여 우선순위를 지정 가능한 3비트로 된 헤더 필드입니다. 따라서 0~7 값을 사용하며, 값이 작을수록 낮은 우선순위를 나타냅니다.
- **DEI(Drop Eligible Identifier) :** 1비트 값으로, 예전에는 항상 0으로 설정하고, 토큰-링이라고 하는 환경과의 호환성을 위해서 두었는데, 현재는 트래픽이 혼잡해질 때 제거되기 적합한 프레임을 지정하는 데 사용되기도 합니다.
- **VID(VLAN Identifier) :** VLAN 번호가 지정되는 부분으로, 12비트로 되어 있습니다. 즉 값이 0~4095까지 지정 가능하며, 0으로 설정하면 해당 프레임은 VLAN에 속하지 않음을 의미합니다.

최영락
휴레이포지티브 선임연구원 & OVNC 기술매니저



[그림 3] VLAN 헤더 필드 구조 및 L2와 L1에서의 VLAN 태그 적용

VLAN의 활용

이러한 VLAN 기술은 2000년대 중후반으로 오면서 네트워크 인프라를 구성하는데 점차 활용되기 시작합니다. 여기서는 활용 예시로, VoD와 같은 IPTV 서비스를 기존 네트워크 인프라에 통합하는 예시를 살펴보고자 합니다. 이때 각 VLAN 번호에 대해 독립적인 L2에 대한 논리적 네트워크를 만들 수 있습니다. 각 논리 네트워크에 가입자별로 VLAN을 할당하게 되면, 기존 물리 네트워크에 대한 변경 없이 각 가입자별로 독립적인 네트워크가 생성될 뿐만 아니라, 각 가입자들은 마치 직접 접속된 것과 같은 네트워크 상태를 만들 수가 있습니다. 이렇게 VLAN을 활용하였을 때의 장점을 요약하면 다음과 같습니다.

- **기존 IP 서비스와의 간섭 최소화 :** IPTV 트래픽을 기존 IP 기반의 네트워크와 별도로 분리하므로 기존 사용하던 초고속 인터넷, VoIP 등과의 간섭을 줄일 수 있습니다. 특히, L2로 분리되어 브로드캐스트가 이루어지므로, 이에 따른 부담을 줄일 수 있으며, VLAN 태그에 포함된 Priority 필드를 활용해 우선순위를 기반으로 한 네트워크 관리가 가능해집니다.
- **많은 수의 VLAN 사용자를 지원하기 위한 확장성 :** 동일한 물리 인프라를 기반으로 하여 최대 2^{12}에 해당하는 4096개(실제로는 예약된 VLAN 번호 등이 있어 이보다 작아집니다)의 독립적인 개별 논리 네트워크를 생성할 수 있습니다.
- **분산 네트워크 관리 :** VLAN 번호를 할당 및 관리하기 위해서는 각 스위치에 관리자 모드로 접속하여 번호를 부여 및 관리해야 합니다. 실제, IPTV 망과 같이 대규모로 관리할 때에는 여러 대의 스위치에 대해 VLAN 번호를 통합 할당 및 관리가 가능한 별도의 분산 네트워크 관리 소프트웨어를 사용합니다. 해당 소프트웨어를 사용하여 개별 VLAN 번호에 대한 논리 네트워크에 필요한 DHCP, 라우터와 같은 장비를 사용하는 것이 가능해집니다.
- **유연성 :** 실제 VLAN 번호 변경 등은 별도의 관리 소프트웨어를 사용하여 이루어지기에, 기존에 현장에서 직접 작업하던 것들을 관리 소프트웨어로 대신할 수가 있습니다. 예를 들어, 기존에는 1명의 고객을 지원하기 위해 물리 네트워크를 점검하는 일이 필수였다면, VLAN에서는 소프트웨어를 통해 VLAN 할당 및 점검이 가능해지며, 실제 사용자 단에서만 VLAN이 잘 동작하는지만 점검하는 식으로 유연성이 향상되는 것입니다.

그리고 VLAN 번호는 일반적으로 다음과 같은 4가지 방식으로 지정하여 사용합니다.

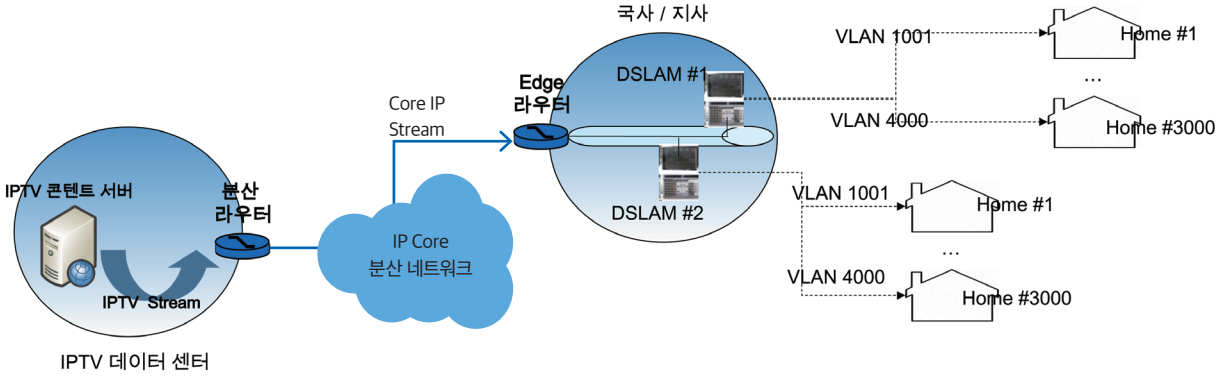
· **포트 기반 :** 여기서 말하는 포트란 스위치에서 물리적인 선을 연결 가능한 개별 포트를 이야기합니다. [그림 1]에서 설명한 VLAN 번호 할당을 살펴보면 스위치에 있는 각 포트를 기반으로 어떤 VLAN 번호를 사용할 것인지를 지정합니다. 이러한 방식을 포트 기반이라고 합니다.

· **MAC 기반 :** 실제 컴퓨터에서 사용하고 있는 물리 인터페이스의 MAC 주소를 기반으로 VLAN 번호를 할당하는 방식입니다. [그림 1]에서 포트1에 연결된 빨간 서버가 aa:bb:cc:dd:ee:ff 라는 MAC 주소를 가졌다고 하고, 스위치에서 MAC 주소 aa:bb:cc:dd:ee:ff에 대해서는 VLAN 번호 1001번을 사용하겠다고 지정하면, 해당 서버가 포트1에서 포트8로 바꾸어 연결하더라도 스위치의 다른 설정 없이 포트8에 연결된 빨간 서버에는 VLAN 번호 1001이 스위치에서 태깅됩니다.

· **프로토콜 기반 :** [그림 3]에서 설명했던 L2 헤더 부분을 살펴보면, 기존 VLAN이 태깅되지 않은 패킷에 EtherType이라는 부분이 있습니다. 해당 부분을 통해 이더넷 프레임의 종류를 파악 가능한데, 이 부분을 기반으로 VLAN 번호를 할당하는 방식을 프로토콜 기반이라고 합니다.

· **인증 기반 :** 추가로 인증 시스템을 사용하여 인증이 된 경우에만 특정 VLAN 번호를 할당하는 방식입니다. 인증 체계가 필수인 환경에서 결합되어 사용하는 방식입니다.

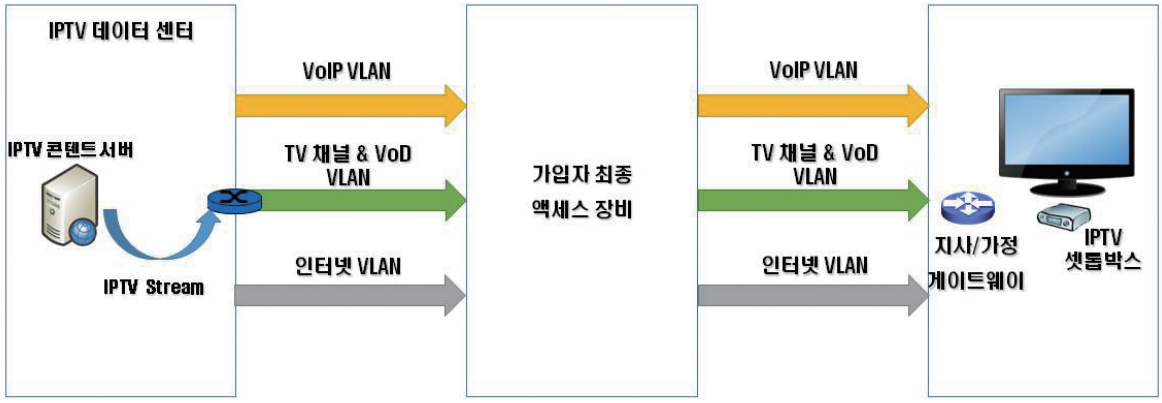
이러한 할당 방식을 기반으로, IPTV 망에 VLAN이 활용되는 경우로는 크게 가입자 중심의 망에 따라 VLAN 번호를 지정하는 활용 및 서비스 중심으로의 VLAN 번호 지정을 들 수 있습니다. 먼저, 가입자 중심의 망에 따른 VLAN 디자인 설계는 [그림 4]와 같이 간단히 살펴볼 수 있습니다. DSLAM이란 Digital Subscriber Line Access Multiplexer의 약자로, 여러 디지털 가입자 회선 접속과 고속 백본 회선에 다중화 기술을 사용하여 연결하는 장비를 말합니다. 일반적으로 통신사를 기준으로 지사나 지역 국사 또는 아파트의 경우 통신실에 설치되어 있습니다. 이때, 해당 DSLAM 장비부터 고객단까지를 VLAN 번호로 개별 지정하여 사용하는 것입니다. 이렇게 구성을 하는 경우 개별 고객단 VLAN 망이 DSLAM 장비를 기준으로 논리적으로 구분된다는 장점이 있습니다. 그러나 멀티캐스트와 같은 기술을 활용하고자 할 경우에는 개별 논리 네트워크로 구분되어 있어 사용이 불가능하다는 단점도 있습니다.



[그림 4] 가입자 중심 VLAN 설계

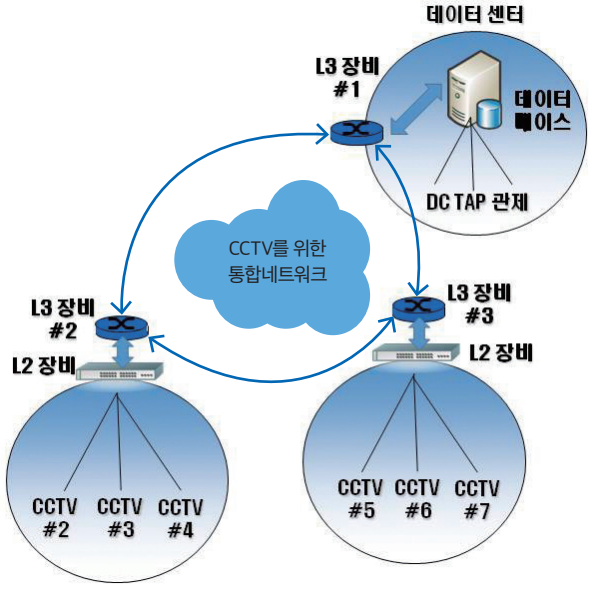
반면, [그림 5]는 서비스를 중심으로 VLAN 디자인을 설계한 예시입니다. 해당 설계에서는 각 VLAN은 개별 IP 서비스를 의미합니다. 해당 설계의 경우 동일한 물리 네트워크를 기반으로 하여 여러 서비스를 생성하는 것이 쉬워진다는 장점이 있습니다. 이때 모든 고객 사용자들이 VoIP와 IPTV를 사용하지 않을 수도 있는데, 이 경우에 대해서는 인증 기반으로 VLAN을 설정하도록 하여 특정 고객은 VoIP만, 또 다른 특정 고객은 IPTV만 사용하도록 지정하는 것이 가능합니다. 또한 이러한 두 디자인을 모두 활용하여 VLAN을 네트워크에 활용할 수 있습니다.

최영락
휴레이포지티브 선임연구원 & OVNC 기술매니저



[그림 5] 서비스 중심 VLAN 설계

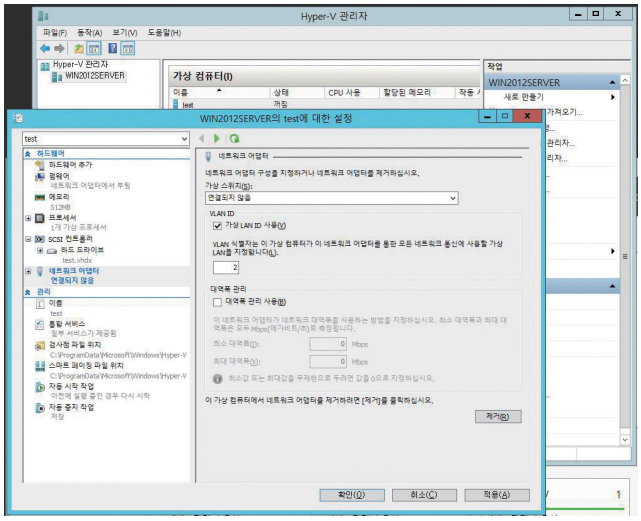
이러한 설계에서 한 가지 유념해야 하는 사항은, VLAN은 L2를 위한 네트워크 가상화 기술이기에, 라우터 등의 L3 장비에서 VLAN을 활용하기는 어렵습니다. [그림 4]에서 DSLAM을 기준으로 VLAN 번호를 부여한 이유가 이에 해당합니다. 다른 예로, 통합 CCTV 망을 구성한다고 가정한다면, [그림 6]과 같이 VLAN 번호는 L2 장비 이하에 부여를 하고, L3에서는 이를 라우팅하도록 구성해야 하는 것입니다. [그림 6]에서는 각 CCTV 모니터링하는 지점에 스위치와 같은 L2 장비를 두고, 해당 장비 하위에 VLAN 번호를 할당하는 식으로 설계를 합니다. (통합했을 때의 총 VLAN 개수가 4,096개보다 적다면 다른 지점이라 하더라도 다른 VLAN 번호를 할당하는 것이 추후 지점 통합 등을 고려할 때 좋은 이점도 있습니다.) 그리고 L3 장비에서 해당 L2 트래픽을 어떻게 라우팅할 것인지를 정합니다. [그림 6]에서 예를 들면, L3 장비 #1과 #2 사이의 물리 연결이 끊어지더라도 #3 장비를 거쳐 #2 장비로 가는 경로가 있기에 통신이 되는 것과 같이 안정적으로 구축하는 것이 일반적입니다.



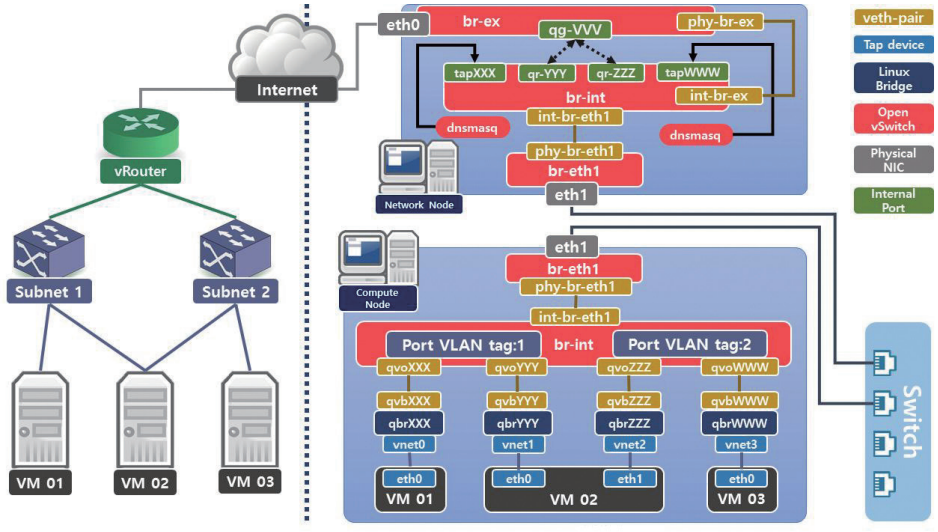
[그림 6] CCTV 통합망 구성 예시

최근에는 서버 가상화가 이루어지는 환경 안에서 스위치에서 물리 서버에 대한 VLAN 번호를 할당하는 것과 비슷하게, 각 가상 머신에 대해 VLAN 번호를 부여하는 것이 가능합니다. 상용 제품인 VMware vSphere 뿐만 아니라 Microsoft Hyper-V[그림 7], 그리고 오픈소스인 OpenStack[그림 8] 등에서 모두 가능합니다. 이렇게 필요로 하는 VLAN 번호 개수가 점차 증가하다보니 VLAN

기술만을 사용해서는 네트워크 가상화를 구현하는데 한계가 생겼습니다. 또한 L2의 기술이다보니 L3 이상에서도 적용 가능한 다양한 네트워크 가상화 기술이 고려되기 시작하였습니다. 최근 통합된 시설을 위한 네트워크망을 구축할 때에는 VLAN 뿐만 아니라 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 다양한 해결책이 고려되는 이유가 바로 여기에 있습니다.



[그림 7] Windows Server 2012 : Hyper-V에서의 VLAN ID 설정



[그림 8] OpenStack : VLAN을 사용한 네트워크 가상화 (Neutron) 구성도 예시

이와 같이 이번 연재에서는 VLAN을 중심으로 네트워크에서 어떻게 활용되는지를 살펴보았습니다. 다음 연재에서는 관련된 서버 / 네트워크 가상화와 관련된 활용 사례를 중심으로 살펴볼 예정입니다.

참고 문헌

[1] Gerard O'Driscoll, "Next Generation IPTV Services and Technologies", Wiley, 2008.
[2] 강효성 외 5인, "OpenStack Networking을 다시 살펴보자", 오픈스택한국커뮤니티, 2015년 7월.