최영락
나임네트웍스 SDN기술팀 매니저

컴퓨터 네트워크의 이해 및 활용 ❽

주요 상위 계층 (L4/L7) 네트워크 장비

+ **최영락** 나임네트웍스 SDN기술팀 매니저

지난 연재에서는 TCP/IP의 가장 상위 계층인 응용프로그램 계층 및 프로토콜을 살펴보고, 대표적인 응용프로그램 계층 프로토콜인 DNS를 통해 응용프로그램 계층 프로토콜이 어떻게 동작하는지 살펴보았습니다. 이번 연재에서는 먼저 지난 7월 연재에서 살펴보았던 OSI 7 계층을 리뷰하고자 합니다. 이후, 전송 계층 및 응용프로그램 계층을 활용하는 주요 네트워크 장비들을 구분하여 살펴보고자 합니다.

I. OSI 7 계층 및 L1-L3 네트워크 장비

지난 7월 연재에서는 TCP/IP의 4개 계층 및 국제 표준화 기구인 ISO에서 제정한 OSI 7 계층을 살펴보았습니다. 컴퓨터 네트워크에서 쓰는 TCP/IP 계층은 여러 연재를 통해 살펴보았던 데이터 물리 계층, 네트워크 계층, 전송 계층, 그리고 응용프로그램 계층, 이렇게 총 4개의 계층을 말합니다. 반면, OSI 7 계층은 1계층부터 7계층까지 총 7개의 계층이 있고, 영어로 계층 용어에 해당하는 Layer의 첫 대문자 L을 사용해 L1~L7 계층으로 줄여서 표현하고 있습니다.

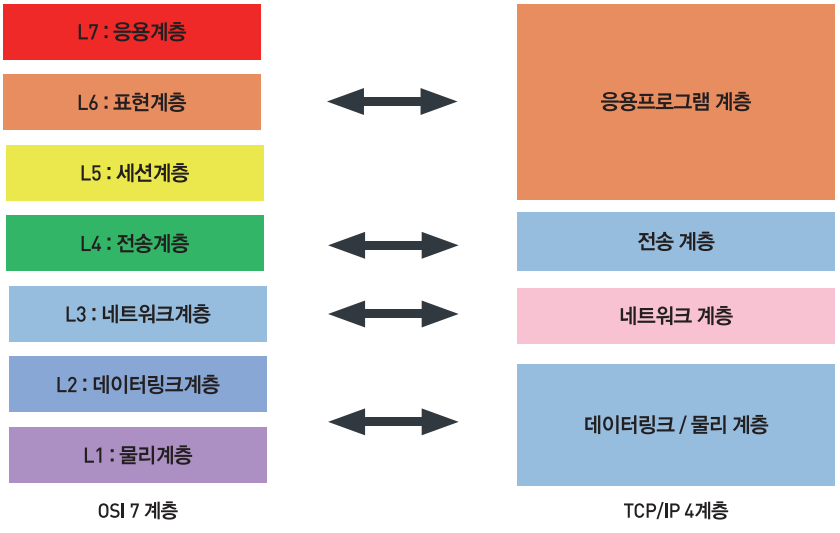

그림 1. OSI 7계층과 TCP/IP 4계층

[그림 1]에서는 OSI 7계층 및 TCP/IP 4계층의 관계를 나타냅니다. L1~L7 용어 및 TCP/IP 4계층 용어 모두 사용되기에 서로 다른 두 계층이 서로 관련이 있음을 잘 알아두면 좋을 것입니다. OSI 7 계층에서의 L1~L7 용어는 컴퓨터 네트워크 장비들이 어떤 계층에 해당하는 장비인지 이야기할 때 많이 사용되는 용어이므로 잘 알아둘 필요가 있습니다. 그렇다고 TCP/IP 4계층의 중요성이 떨어지는 것은 아닙니다. 우리가 사용하는 현재의 인터넷은 TCP/IP 4계층을 기반으로 하여 전체적인 구조가 이루어져 있습니다. 그런데 네트워크 하드웨어 장비 제조업체들은 TCP/IP 4계층을 위한 장비만을 생산하는 것이 아니기에 국제 표준에 해당하는 L1~L7 용어를 더 많이 사용하는 경향이 있습니다. TCP/IP 4계층 및 OSI 7 계층의 차이에 대해 다음과 같이 이해하시면 쉬울 것 같습니다.

- TCP/IP 4계층 : IP 주소를 사용하여 통신하는 경우에 한해 4계층으로 구분하여 사용
- OSI 7 계층 : IP 주소를 사용하지 않고 통신하는 경우에도 7계층으로 구분하여 사용

그렇다면 IP 주소를 사용하지 않고 통신하는 경우는 언제가 있을까요? 예를 들어, 규모가 큰 통신사들은 내부에서 보다 빠른 인터넷 데이터를 주고받도록 성능을 높이기 위해 MPLS(Multi-Protocol Label Switch) 프로토콜 및 이를 지원하는 하드웨어 장비를 사용합니다. 이때 사용하는 통신 방식은 IP 주소를 이용한 통신 방식은 아니기에, OSI 7계층의 L1~L7 유형으로 장비를 분류합니다. 또한 해당 장비들에서 통신할 때, IP 주소를 이용하는 데이터들을 보내고 받는 경우가 많은데, 이때 IP 주소를 사용하는 스위치, 라우터 등의 장비와도 연동되어야 하는 경우가 많습니다. 이러한 다양한 경우가 있어, 아무래도 네트워크 장비들을 이야기할 때는 L1~L7 장비라는 용어가 더 많이 사용되고 있지 않나 추측해 봅니다.

그림 2. MPLS 스위치/라우터 네트워크 장비 / 출처 : Cisco

실제 이동 통신 또는 방송 등에서 특히 L1~L3 장비들은 네트워크 설비를 구축하는 데 많이 사용됩니다. 지난 8월, 프란치스코 교황께서 한국에 도착하여 광화문 광장, 음성 꽃동네, 서산 해미성지 등 짧은 일정 동안 여러 곳을 방문하였습니다. 이때 교황 방문 현장을 실시간으로 중계하기 위해서는 방송에서 촬영하는 데이터가 실시간으로 별도의 방송/통신망에 연결되어 중계되어야 할 것입니다. 광화문 광장이

최영락
나임네트웍스 SDN기술팀 매니저

야, 여러 행사들이 있으니 통신 시설 등을 비교적 빠르게 준비할 수 있겠지만, 음성 꽃동네나 서산 해미성지 등에서는 실시간으로 여러 방송사들에 트래픽을 전송할 수 있는 네트워크 관련 시설들을 준비해야 할 것입니다.

이런 상황에서, 주로 L2-L3 계열 스위칭 관련 장비들이 준비되어, 충분한 양의 방송 트래픽이 통신망을 통해 잘 전달될 수 있도록 구축을 해야 실제 교황께서 방문하였을 때 실시간으로 촬영하는 트래픽을 잘 전달할 수 있습니다. 특히, 이런 상황에서는 각 장비들이 순간 트래픽 폭증 또는 장애로 인해 서비스되지 않는 현상을 미리 방지하기 위해 장비에 대한 이중화, 삼중화도 고려하여 준비합니다. 그러다 보니 위와 같은 행사를 위해 L2-L3 계열의 장비들이 때에 따라서 10대 이상 준비하고, 한 장비가 순간 장애를 일으키더라도 다른 장비에서 잘 처리가 될 수 있도록 장비를 세팅해야 합니다. 이렇게, 장애가 발생했을 때 다른 장비에서 서비스 가능하도록 하는 기능이 있는 네트워크 장비는 해당 기능이 없는 장비보다 가격이 많이 비싸지겠죠. 이러한 기능 및 장비의 안정성 등에 따라 다양한 회사에서 L2-L3 장비를 생산하고, 이 장비들을 이용해 네트워크가 구축 및 서비스가 이루어집니다. [그림 3]은 L3 스위치를 이중화하여 구성한 예시입니다.

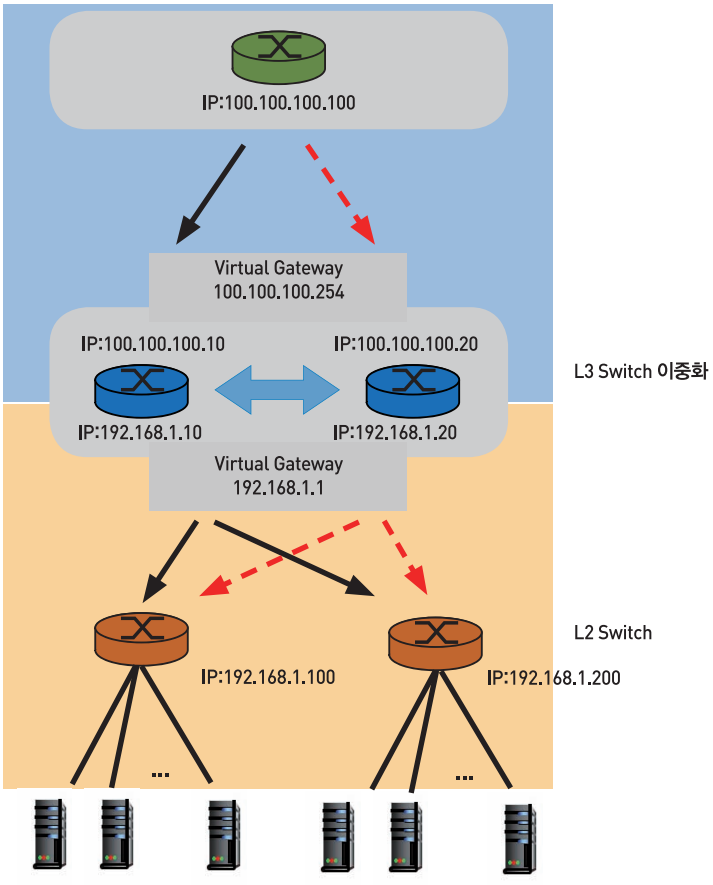

그림 3. L3 이중화 구성 예시

II. L5 및 L6 계층

주요 L4~L7 계층에서의 주요 네트워크 장비들을 소개하기 전에, [그림 1]에서와 같이 L4 계층은 TCP/IP 계층에서 전송 계층과 그리고 L5~L7 계층은 응용프로그램 계층과 매칭됩니다. 그런데 실제로는 L5 세션 계층과 L6 표현 계층 네트워크 장비란 용어는 거의 쓰이지 않습니다. OSI 7 계층 표준에서 L5 계층과 L6 계층은 다음과 같이 정의되어 있습니다.

계층(숫자)	계층명	계층명(영문)	설명
L5	세션 계층	Session Layer	응용프로그램 계층 간의 통신에 대한 제어 구조를 제공하기 위해 응용프로그램 사이의 접속을 설정, 유지, 종료시켜주는 역할을 하는 계층. 데이터를 교환함에 있어 동기화, 점검 및 복구 기능을 제공
L6	표현 계층	Presentation Layer	데이터 표현의 차이를 해결하기 위하여 서로 다른 형식을 변환해 주거나 공통 형식을 제공하는 계층. 암호화, 압축, 특정 기계에서 사용되는 표현과 관련된 구분을 해결하는 기능을 제공

표 1. L5-L6 계층 설명

그런데 실제 TCP/IP 계층에서 전송 계층 이상은 응용프로그램 계층 하나인 데다, OSI 7 계층에서 L4 이상의 계층을 실제 쓰는 쪽은 거의 인터넷이라고 봐도 무방하기에 L4 이상의 계층을 L5, L6, L7 이렇게 복잡하게 굳이 구분할 필요가 없습니다. 그리고 L5, L6 계층에서 수행하는 역할 비중이 상대적으로 다른 계층들에 비해 적은 면도 있어, L5~L6 네트워크 장비를 거의 찾아보기 어렵습니다.

III. 주요 L4/L7 네트워크 장비

네트워크 관련 장비는 크게 기능 관련 장비와 활용 관련 장비로 구분됩니다. 기능 관련 장비는 컴퓨터 네트워크 자체에 대한 특정 기능을 목적으로 만들어진 장비입니다. 반면, 네트워크 활용 장비는 주로 응용프로그램 계층에서 컴퓨터 네트워크를 활용하고자 하는 목적으로 만들어진 장비로, NAS, SAN, 그리고 NPS 등이 있습니다. 본 연재에서는 L4~L7 계층에서 동작하는 네트워크 기능 관련 장비인 방화벽, DPI, 그리고 로드밸런서를 살펴보고자 합니다.

1) 방화벽

방화벽을 영어로는 Firewall이라 하는데, 이를 해석하면 불(Fire)을 막는 벽(wall)이 됩니다. Firewall의 원래 의미는 건물에서 발생한 화재가 더 이상 번지는 것을 막는다는 의미였는데, 컴퓨터 네트워크 보안에서 특정 트래픽이 외부에서 내부로 들어올 때, 또는 내부에서 외부로 나갈 때 해당 트래픽만 막아낸다는 의미로 '방화벽'이라는 용어가 사용되기 시작하였습니다.

컴퓨터 네트워크에서 특정 트래픽을 차단할 때, 방화벽에서는 어디로부터 트래픽이 오는지를 판단하기 위해 발송지 IP 주소를, 그리고 어떤 컴퓨터로 트래픽이 가는지 판단하기 위한 도착지 IP 주소를, 그리고 어떤 포트 번호를 통해 트래픽을 주고받는지에 대한 송·수신 포트 번호, 또한 트래픽이 TCP인지 UDP인지를 살펴보고 트래픽을 차단합니다. 이 정보들은 TCP/IP 계층에 따르면 TCP/UDP인지와 포트 번호를 살펴보기에 '전송 계층'에 해당하고, 이는 OSI 7 계층에 따르면 L4 계층에 해당합니다. 따라서 방화벽 기능을 포함하는 네트워크 장비는 L4 장비라 할 수 있습니다.

이런 방화벽은 응용프로그램 계층의 기능을 합쳐 보다 나은 기능을 제공하는 L7 계층의 장비로 활용되기도 합니다. 대표적인 예로, 네트워크 보안에서 많이 언급하는 침입 탐지 시스템(IDS : Intrusion Detection System)이 있습니다. 이 장비는 기존의 방화벽의 기능뿐만 아니라 응용프로그램 데이터를 살펴보고, 보안에 영향을 미치는 공격 내용이 포함되어 있으면 해당 트래픽을 탐지합니다. 이 장비는 실제 데이터를 살펴보아야 하기에, L7 네트워크 장비에 해당합니다. 또한, 관리자에게 공격이 발생했을 때 이에 대한 적극적인 알림 및 차단 등 보다 포괄적인 기능을 제공하는 네트워크 장비에 대해서는 침입 예방 시스템(IPS : Intrusion Prevention System)이라고 불립니다.

최영락
나임네트웍스 SDN기술팀 매니저

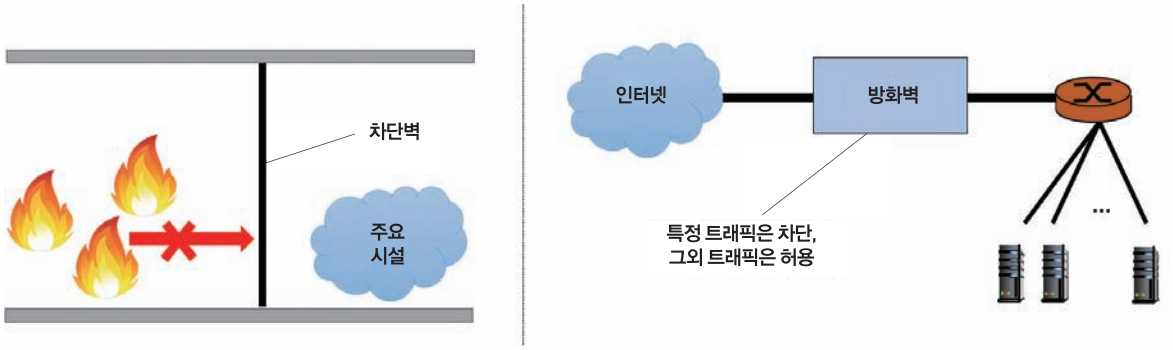

그림 4. Firewall 원 의미 및 컴퓨터 네트워크에서의 방화벽

2) DPI 장비

위에서 설명할 때, 침입 탐지 시스템에서 수행하는 기능으로 보안에 영향을 미치는 공격 내용이 포함되어 있는지를 살펴본다고 하였는데, 이러한 기능을 전문 용어로는 '심층 패킷 분석 (DPI : Deep Packet Inspection)이라고 합니다.' 침입 탐지 시스템에서는 이 DPI라는 기능을 보안을 위해 사용하고 있는데, 이 심층 패킷 분석 자체를 전문으로 수행하는 네트워크 장비도 있습니다. 이를 DPI 장비라고 합니다. DPI 장비는 특정 지점에 설치되어, 해당 지점을 오가는 인터넷 트래픽 중 어떤 응용프로그램 데이터가 많은지 판단을 하는 데 사용됩니다. 예를 들어, 특정 지점을 기준으로 YouTube와 같은 동영상 트래픽이 많은지, 스마트TV를 시청하는 방송 트래픽이 많은지, 또는 파일 전송과 같은 P2P 트래픽이 많은지 등을 응용프로그램 계층 레벨에서 데이터를 직접 보고 판단을 합니다. 인터넷 초창기에는 송 · 수신 포트를 사용하는 방식이 거의 정형화되어 있어 전송 계층에 해당하는 L4 계층까지만 살펴보더라도, DPI라는 기능 없이 어떤 응용프로그램에 대한 트래픽인지 식별이 가능했지만, 현재는 송 · 수신 포트 번호를 임의로 변경하는 경우도 있어 응용프로그램 데이터를 직접 보고 식별합니다. 단, 특정 지점에 설치되더라도 이렇게 인터넷에서 오가는 모든 트래픽을 직접 보고 식별하려면 성능이 매우 좋아야 하기 때문에 아무래도 해당 장비 가격은 다른 장비에 비해 많이 비싼 편입니다.

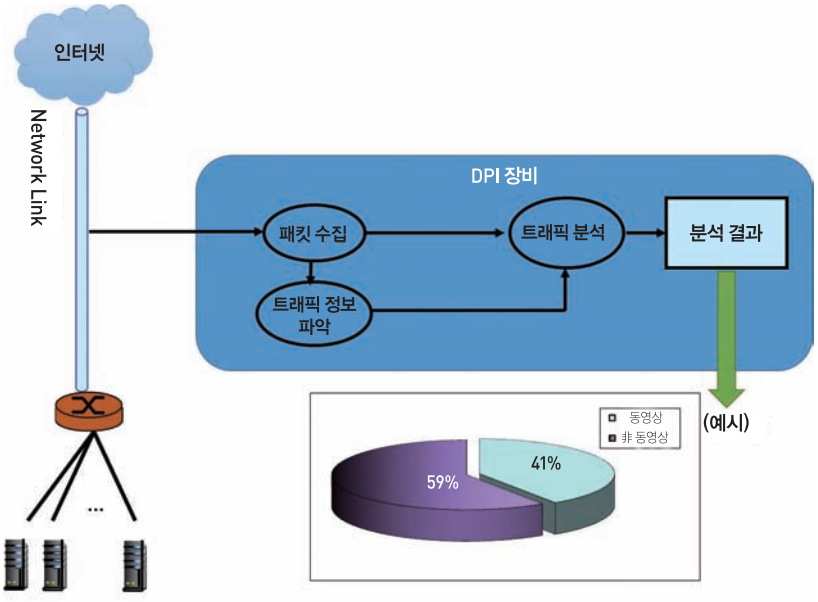

그림 5. DPI 장비

3) 로드밸런서

로드밸런서는 특히, 방송 스트리밍과 같은 서비스를 대규모로 서비스할 때 필요한 장비 중 하나입니다. 스트리밍 서비스는 사용하는 전송 계층 유형에 따라 TCP 또는 UDP로 서비스가 이루어질 텐데, 어떤 것이든 둘 중 하나를 선택했다 하더라도 이론상 서버 1대에서는 최대 65,536개의 접속만을 수행할 수 있습니다. 이는 포트 번호가 TCP와 UDP 각각 0~65,535까지로 규정되어 있기 때문입니다. 이 65,536개라는 것은 단순히 포트 번호로 볼 때 계산되는 숫자입니다. 실제로는 해당 서버에서 다른 서버 등과의 통신, 또는 내부적으로 사용하고 있는 포트 번호를 제외해야 하며, 이렇게 해서 60,000개의 접속이 실제 오더라도 해당 접속을 모두 처리하기 위해서는 서버 CPU, 메모리 등 사양이 매우 좋아야 하며, 스트리밍 프로그램 자체에서 이 모든 접속들을 수용하기 어렵습니다. 특히, 방송 스트리밍과 같은 경우에는 대량의 트래픽을 전송해야 하므로 서버당 지원 가능한 접속 수가 몇백 개를 넘어가기가 힘든 것이 현실이고, 각 접속 당 오가는 대역폭을 제한하기도 합니다.

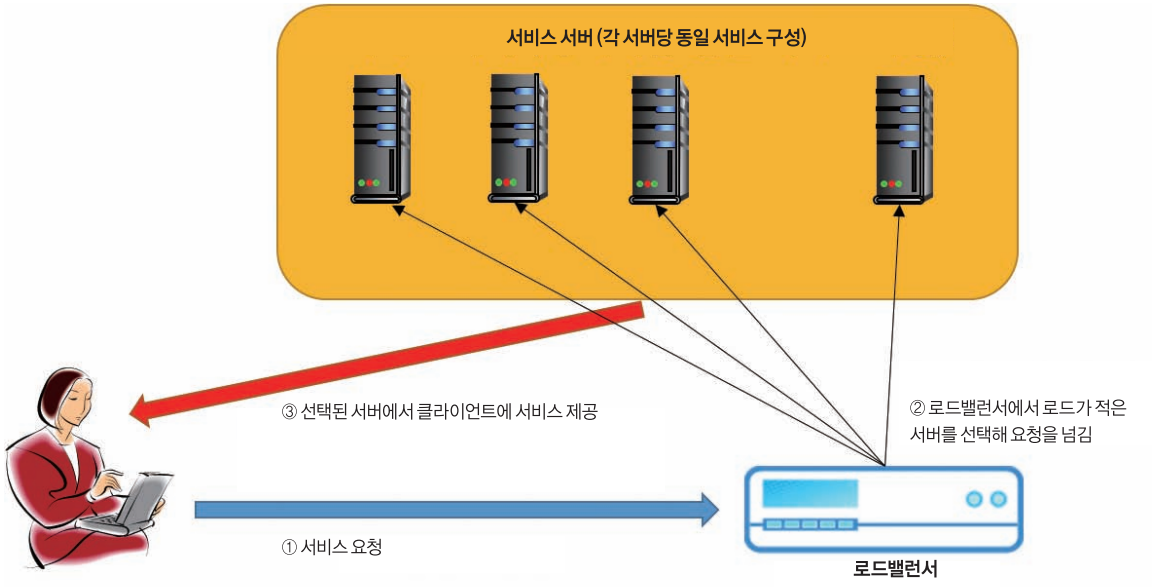

그림 6. 로드밸런서

따라서 대규모 스트리밍 서비스를 구축할 때에는 여러 대의 서버를 설치하는데, 이때 내부적으로는 다른 IP 주소를 사용하더라도, 외부에서는 같은 IP 주소를 사용하도록 설정이 되어 있어야 스트리밍 서비스가 갖추어졌다고 이야기할 수 있습니다. 예를 들어, 스트리밍 서비스를 제공하는데, 첫 번째에서 100번째까지 접속하는 사용자는 A라는 IP 주소를 사용하도록 하고, 101번째에서 200번째까지의 사용자는 B라는 IP 주소를 사용하는 식으로 서비스를 만들 수는 없을 것입니다. 따라서 로드밸런서 장비는 특정 IP 주소를 가지고 있고, 해당 로드밸런서 장비에 실제 서비스하는 서버들이 연결되도록 구성합니다. 이때 로드밸런서 장비로 접속을 하면 이 장비에서 각 서버로 접속을 연결시켜주는 방식으로 사용하는 장비가 로드밸런서입니다.

로드밸런서는 일반적으로 IP 주소와 포트 번호, 그리고 TCP인지 UDP인지까지 살펴보고 동작하기에 L4 장비에 해당합니다만, 일부 로드밸런서의 경우 응용프로그램 계층까지 고려하는 L7 로드밸런서 장비도 있음을 참고하였으면 합니다.

이번 연재에서는 OSI 7계층에 따른 용어들을 다시 살펴보고, 주요 L4/L7 네트워크 장비들을 살펴보았습니다.
다음 호에서는 스트리밍 및 멀티캐스트와 관련된 용어에 대해 알아보는 시간을 가지고자 합니다.