방송 네트워크 트래픽 모니터링과 분석

조준호
KBS 미디어송출부
MNC(Media Network Center)팀

들어가며

대규모의 네트워크 시스템을 효율적으로 운영하기 위해서는 대상 장비의 상태 정보를 수집하고 장애 발생 시 즉시 인지할 수 있도록 네트워크 관제시스템(Network Management System, 이하 NMS)을 활용합니다. 이를 통해 트래픽 병목구간이 어디서 발생하는지, 원인은 무엇인지를 분석하여 네트워크 성능을 최적화할 수 있습니다.
이 글에서는 네트워크 트래픽 모니터링과 분석 방법인 SNMP와 FLOW 기술을 설명하고 KBS 미디어 네트워크에서 어떻게 활용하고 있는지 소개하고자 합니다.

KBS 미디어 네트워크

KBS 네트워크는 ERP, 그룹웨어, 인사정보 등 직원들의 업무용 시스템을 처리하기 위한 사내 OA망과 라디오(DRS), 제작 부조(TS), 제작/편집(NPS), 뉴스(KDNS), 송출 주조(DMCR), 아카이브(KDAS) 등 파일 기반 방송시스템들로 구성된 미디어 네트워크(이하 MNC망)로 구성되어 있습니다.

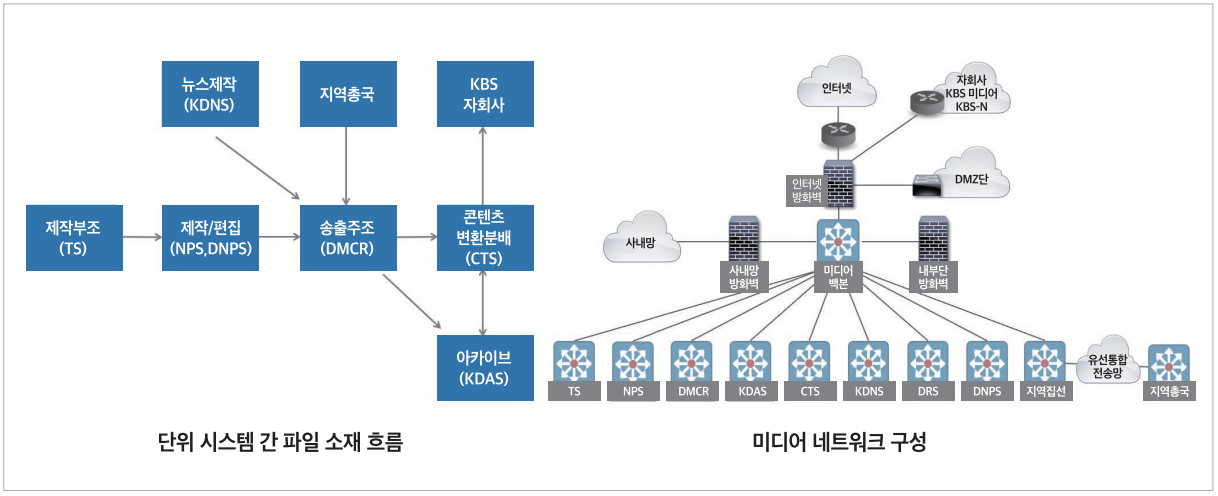

그림 1. 파일 기반 워크플로우와 미디어 네트워크

MNC망에서의 파일 기반 워크플로우는 프로그램 '제작-송출-분배-아카이브' 과정으로 구성됩니다. 제작 부조에서 녹화된 촬영본은 NPS로 인제스트되고, 편집과정을 거쳐 완성된 방송본 파일은 주조로 입고됩니다. 방송본 파일은 CTS를 통해 자회사 및 아카이브시스템으로 분배됩니다.

MNC망은 각각의 단위 파일 기반 방송시스템들이 미디어 백본 스위치를 중심으로 서로 연결되어 있고, 시스템 간의 대용량 미디어 파일을 송수신하는 네트워크 트래픽을 모니터링하고 분석하기 위해 SNMP, FLOW 등의 기술들을 활용하고 있습니다.

네트워크 트래픽 모니터링을 위한 SNMP

Simple Network Management Protocol(이하 SNMP)은 네트워크상에서 동작하는 서버, 스토리지, 스위치 등 장비들의 상태 및 성능 정보를 수집하고 관리하기 위해 사용되는 프로토콜입니다. SNMP를 활용하여 대상 장비 내부의 리소스 점유율뿐만 아니라 장비와 장비 사이에 연결된 네트워크 구간의 트래픽 사용량, 패킷 손실률 등을 모니터링할 수 있습니다.

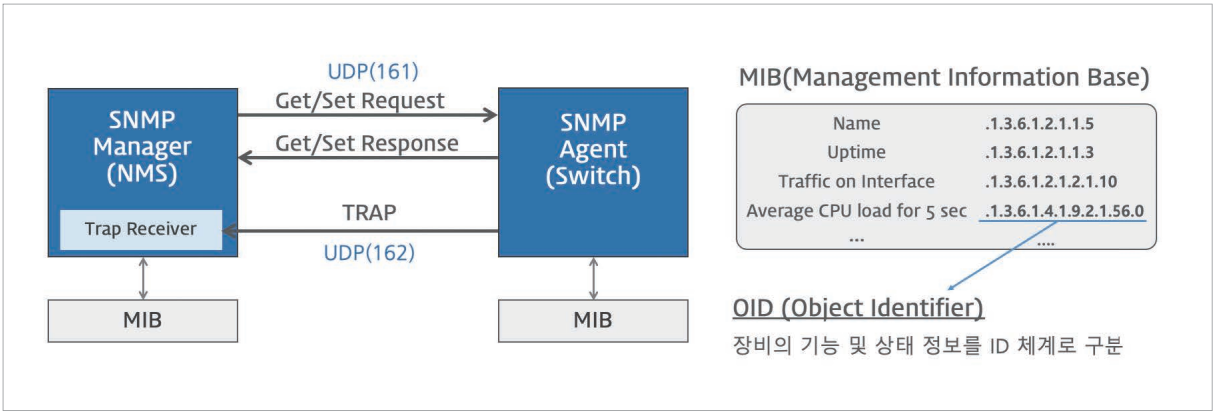

그림 2. SNMP 동작 원리

SNMP는 서버 역할을 하는 매니저와 관제 대상 장비에 포함된 에이전트 간의 통신으로 이루어지고, 메시지 타입은 SNMP GET, SET, TRAP 방식으로 구성됩니다.

SNMP GET은 매니저가 에이전트에게 필요한 정보를 주기적으로 요청(Get Request)하고 에이전트는 관리 대상 장비의 상태 정보 등을 수집하여 매니저에게 응답(Get Response)하는 폴링(Polling) 방식으로 동작하며, UDP 161번 포트를 사용합니다. 그리고 SNMP TRAP은 대상 장비의 메모리 증가 및 네트워크 인터페이스 다운 등과 같은 이상 징후가 생긴 상황에서 매니저의 요청 없이도 에이전트에서 먼저 해당 정보를 즉시 전달하는 메시지로 UDP 162번 포트를 사용합니다. SNMP SET은 매니저가 에이전트에게 대상 기기의 설정 변경을 요청하는 메시지 타입입니다. 다만, 관리자가 직접 장비에 접속해서 설정 변경하는 방식을 선호하기에 SNMP SET 메시지 타입은 거의 사용하지 않습니다.

매니저와 에이전트 간의 SNMP 통신을 위해서 요청하고 응답하는 정보가 무엇인지 동일하게 정의되어야 합니다. 즉, 대상 장비의 상태를 외부에 알릴 수 있도록 공개한 정보가 무엇인지 매니저에서 알 수 있어야 하고, 이는 MIB이라는 트리 구조 형식으로 정의되어 있습니다. MIB를

구성하는 각각의 노드는 번호를 붙여서 장치명, 인터페이스의 상태, 트래픽 등의 상세 정보로 구분되어 번호 열로 표현되는데 이러한 객체 정보가 OID(Object Identifier)입니다.
정리하면, SNMP는 MIB에 정의된 객체들의 OID 값을 이용하여 요청하고 응답하는 방식으로 해당 장비의 상태를 모니터링할 수 있습니다.

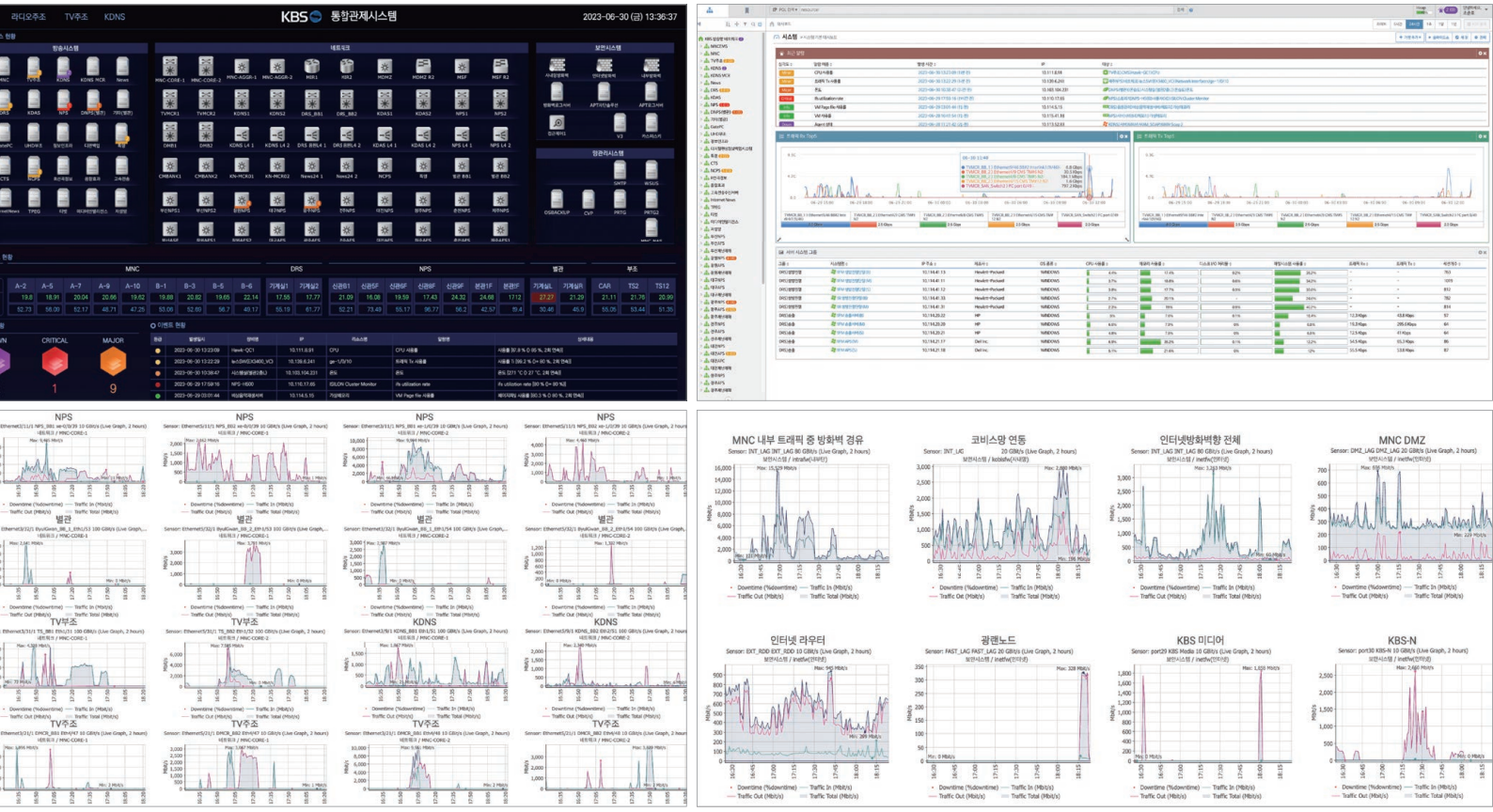

그림 3. SNMP를 활용한 네트워크 트래픽 모니터링

[그림 3]은 MNC망 내 약 350여 대의 네트워크 장비를 SNMP 감시 등록하여 모니터링하는 NMS 구성화면으로 장애 발생 및 장비의 CPU, 메모리 등 리소스 점유율이 임계치 초과하는 경우 관리자가 즉시 인지하고 조치할 수 있도록 하였습니다. 또한 미디어 백본을 중심으로 주요 네트워크 구간의 트래픽 처리량을 실시간으로 모니터링할 수 있도록 구성하여 어디에서 병목현상이 발생하고 있는지 확인할 수 있습니다.

SNMP로 획득한 결과 데이터는 NMS에 장기간 보관하여 트래픽 사용량의 추이를 분석하기 위해 활용할 수 있습니다. [그림 4]는 미디어 백본 스위치와 주조 백본 스위치 구간의 22년 6월과 23년 4월 한 달 동안의 트래픽 사용량을 측정한 결과로써 1년 전에 비해 약 45% 증가한 것을 확인할 수 있습니다. 이와 같이 SNMP를 활용하면 특정 구간의 트래픽 양과 추이 등을 쉽게 파악할 수 있는 반면에 증가한 트래픽 양이 어디에서 발생하는지 구체적으로 원인을 분석하기에는 한계가 있습니다. 따라서, 네트워크 트래픽 사용량을 세분화해서 파악할 수 있는 흐름(Flow) 분석 기술의 활용이 증가하고 있습니다.

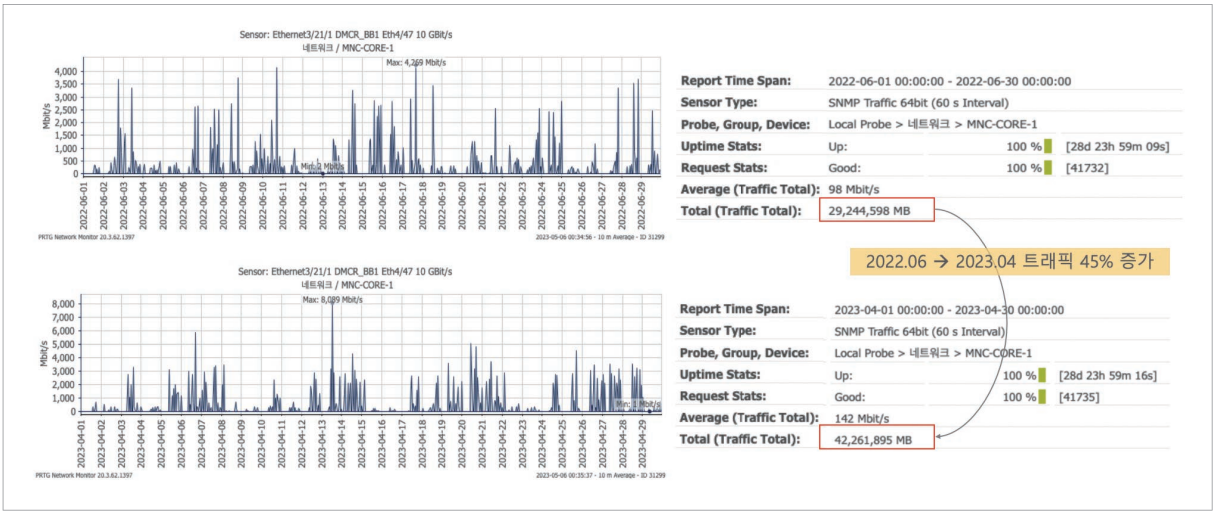

그림 4. 네트워크 트래픽 추이

네트워크 트래픽 분석을 위한 FLOW

흐름(flow)이란 특정 시간 동안 패킷의 출발지와 목적지 정보 등을 가진 데이터라고 정의할 수 있습니다. Flow 관련 기술은 제조사 별로 다양하게 존재하지만, 근본적으로 출발지와 목적지를 기준으로 패킷데이터를 하나의 흐름으로 집계하는 원리는 같습니다.

대표적인 흐름 분석 기술 중 하나인 시스코에서 개발한 넷플로우(NetFlow)를 예를 들어 설명하겠습니다.

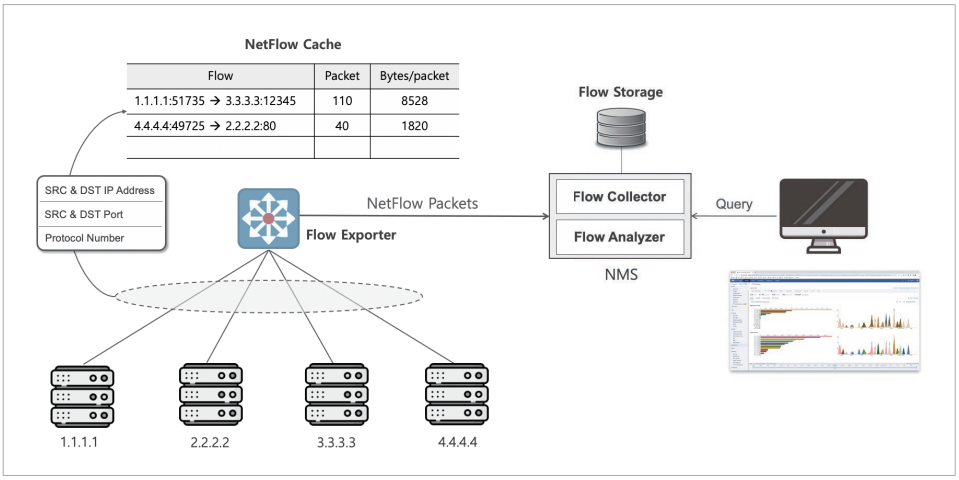

그림 5. NetFlow 동작 원리

NetFlow가 활성화된 네트워크 장비는 인터페이스를 통과하는 패킷 헤더 정보를 확인하여 5-tuple 정보(출발지/목적지 IP 주소, 출발지/목적지 포트, 프로토콜)가 동일한 패킷들을 하나의 흐름으로 규정하고 NetFlow 캐시라고 불리는 데이터베이스에 저장합니다. 동일 흐름의 패킷이 관찰될 때마다 NetFlow 캐시에 패킷과 바이트를 더하여 흐름 정보를 업데이트합니다. TCP FIN 플래그에 의해 통신이 종료했다고 판단되는 흐름 정보는 NetFlow 캐시에서 NetFlow 수집 장치(Collector)로 전달합니다.

네트워크 관리자는 NetFlow 수집 장치에 저장된 흐름 정보를 분석하여 특정 시간 동안 발생

한 트래픽이 어디서 시작된 것인지(출발지 IP), 어디로 도착하는지(목적지 IP), 어떤 애플리케이션이 트래픽을 사용하는지(포트 정보), 트래픽은 얼마나 발생했는지(누적된 패킷과 바이트 수) 등을 확인할 수 있습니다.

구분	NetFlow v5	NetFlow v9	IPFIX	sFlow
표준 여부	비표준 (Cisco)	비표준 (Cisco)	개방형 표준 (IETF)	개방형 표준 (제조사 컨소시엄)
흐름 정보 (Flow Cache)	고정필드 (5-tuple)	템플릿 기반 (사용자 정의)	템플릿 기반 (사용자 정의)	흐름 캐시 없음
흐름 추적 (Flow Tracking)	상태저장 (Stateful)	상태저장 (Stateful)	상태저장 (Stateful)	패킷 샘플링 방식 (Packet Sampling)
입/출력 모니터링	단방향(입력)	양방향	양방향	양방향

표 1. 흐름 분석 기술 비교

최근 가장 많이 활용되는 흐름 분석 기술은 NetFlow, IPFIX, sFlow가 있고 차이점은 다음과 같습니다.

NetFlow v5는 패킷 헤더에서 NetFlow 캐시로 내보내는 필드 정보가 고정되어 있고 모니터링은 인터페이스 입력 방향으로만 지원되는 반면에 v9는 입출력 양방향 지원과 각 흐름 레코드에 포함된 필드를 사용자가 정의해서 템플릿을 구성할 수 있도록 유연성을 제공합니다.
IPFIX(Internet Protocol Flow Information eXport)는 NetFlow v9를 기반으로 IETF에서 표준화된 프로토콜로 다양한 제조사 장비 및 NMS에서 지원되고 있습니다.
sFlow는 Sampled Flow의 줄임말로 다른 Flow 기술과는 다른 접근 방식을 취합니다. NetFlow가 흐름 캐시에 의해 흐름을 상태별로 추적하는 반면에 sFlow는 미리 정해진 간격으로 지정된 흐름의 전체 패킷 헤더를 무작위로 샘플링하는 패킷 샘플링에 기반하여 작동합니다. 따라서 sFlow는 샘플링된 패킷을 거의 실시간으로 내보내기만 하므로 흐름 정보를 캡처하는 네트워크 장비의 CPU, 메모리 등 리소스 부하가 작다는 장점이 있습니다. 또한 주요 제조사들이 컨소시엄을 구성해서 만들어진 개방형 프로토콜이기 때문에 IPFIX와 더불어 대부분의 NMS에서 지원하고 있습니다.

그림 6. 미디어 백본 ↔ 주조 백본 네트워크 구간 FLOW 분석

[그림 6]은 MNC망에서 미디어 백본과 주조 백본 스위치 구간에서 24시간 동안의 네트워크 트래픽을 FLOW 분석한 결과입니다.
먼저, 주조로 전달되는 트래픽은 제작/편집시스템(NPS, DNPS)으로부터 대부분 발생하는 것을 알 수 있습니다. 그리고 지역국 및 자회사의 IP 대역에서 출발지 정보를 가지는 흐름 정보가 관찰되는데 이는 UHD 제작 완료 후 주조로 전송할 수 있도록 본사와 지역국, 자회사 간의 네트워크 연계 기능이 개선되면서 발생하는 트래픽인 것으로 파악할 수 있습니다.
주조에서 나가는 트래픽은 CTS를 통해 분배되는 트래픽 사용량이 가장 많고, 추가로 아카이브를 목적지로 하는 흐름 정보가 관찰되는데, 이는 주조에서 UHD 생방송 프로그램에 대해 인코딩하고 아카이브로 전송하는 연계 기능이 구현됨에 따라 발생하는 트래픽임을 확인할 수 있습니다.

이와 같이 Flow 분석을 활용하여 주조 업링크 구간의 트래픽을 흐름의 출발지/목적지 별로 세분화해서 확인함으로써 시스템 간 네트워크 연계 기능 추가 및 UHD 편성 비율 확대 등이 트래픽 사용량 증가의 주요 요인인 것을 파악할 수 있습니다.

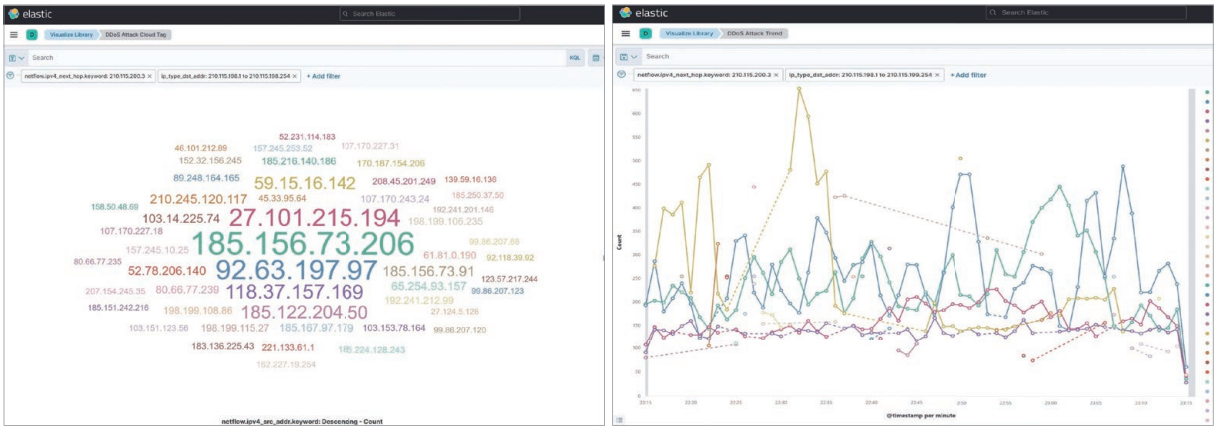

그림 7. ELK를 활용한 NetFlow 트래픽 모니터링

외부에서의 과도한 트래픽을 유발하는 유해 트래픽의 경우, 네트워크 자원 낭비뿐 아니라 시스템 오동작 유발과 다른 시스템 감염 등을 통해 전체 네트워크 장애로 이어질 수 있습니다. [그림 7]은 엘라스틱 스택(이하 ELK)을 활용하여 외부 인터넷에서 MNC 방송망으로 유입되는 트래픽에 대한 흐름 정보를 모니터링하는 화면입니다. 패킷 수를 기준으로 외부 출발지 IP를 크기순, 시간순으로 시각화하여 비정상 트래픽 여부를 쉽게 인지할 수 있으며 과도한 트래픽을 유발하는 특정 호스트를 검색하고 전체 트래픽에서 특정 서비스/애플리케이션 같은 세부적인 정보를 분석하는데 활용되고 있습니다.

마치며

네트워크 모니터링 및 분석을 통해 현재의 네트워크 상황을 명확하게 이해하고 향후 변화요인을 예측하여 대역폭 설계를 하는 것이 중요합니다. 본 글에서 소개된 네트워크 모니터링 분석 기술들을 이해하고 활용하는데 조금이나마 도움이 되었으면 합니다.