NetFlow 기반 IPv6 사용자 Flow traffic 모니터링

NetFlow based IPv6 user's Flow traffic monitoring

김성수, 송왕철*, 오용택, 최덕재**
제주 대학교*, 전남 대학교**

KIM Sung-Su, SONG Wang-Cheol*, OH Yong-Taek, Choi Deok-Jai**
Cheju National Univ.*, Chonnam National Univ.**

요약

Gbps급의 대역폭을 지원하는 차세대 인터넷이 등장함에 따라 다양한 초고속 응용 서비스들이 개발 되어 시험 운용되고 있다. 이런 초고속 응용 서비스를 이용하는 도중에 문제가 발생하면 그 원인을 파악하기 어렵다. 하지만 특정 사용자 flow traffic에 대한 정보(종단 간 라우팅 경로, 구간별 패킷과 데이터 전송률과 라우터 상태정보)를 실시간으로 확인 할 수 있다면 문제 원인을 파악, 개선하기가 수월 해질 것이다. 현재 한 지점에서 flow traffic을 모니터링 하는 시스템은 개발되어 있으나 사용자 flow traffic의 종단 간 흐름을 모니터링 할 수 있는 시스템은 개발되어 있지 않다. 따라서 본 연구에서는 사용자 flow data의 종단 간 라우팅 경로와 각 구간별 패킷 전송률과 데이터 전송률을 수치로 제공함으로써 데이터 소실 구간을 실시간으로 파악 가능한 종단 간 Flow 모니터링 시스템을 제안하고 구현하였다. 또한 IPv6을 사용하는 사용자 flow traffic에 대해서도 flow traffic 모니터링이 가능 하도록 구현 하였다.

Abstract

As the next generation internet (NGI) is supporting High-speed in Gbps rate with the appearance of advanced network technologies, various applications that require high data rates. have been experimented and operated. By using high speed application services, many kinds of problems can be generated but we cannot easily grasp their reasons. However, if the user monitors the end-to-end one's flow data information (path and data rate in each router, state of each router) he can find them more accurately Until now, we have found out the fact that systems which can network-widely monitor end-to-end flow have not be developed yet, only simple systems which can monitor user's indivisual flow data at just one node are developed In this study, we suggest and materialize a system which can analyze bandwidth in real time by searching routing paths and measuring packet transfer rate between end-to-end flow data and supported flow traffic of using IPv6.

I. 서 론

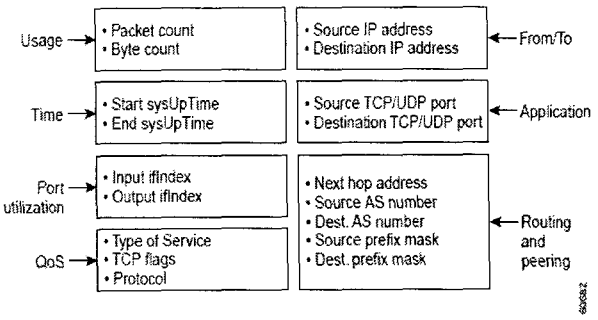
최근 Internet2[1], KOREN[2]와 같은 Gpbs급의 대역폭을 지원하는 차세대 인터넷이 등장으로 기존에 인터넷 방송이나 화상 회의와 같은 실시간 온라인 서비스가 높은 서비스의 질을 제공 할 수 있게 되었고 더불어 높은 데이터 전송률을 요구하는 많은 초고속 응용 서비스들이 개발되어 시험 운용되어지고 있다. 하지만 원격 진료 서비스와 같은 몇 몇 실시간 초고속 응용 서비스들은 지연시간에 민감하게 반응 하며 많은 트래픽을 발생 시키더라도 높은 서비스의 질을 제공 하려 한다. 따라서 최소한의 트래픽을 발생시키면서 고화질의 서비스를 제공하기 위해 ABR, UBR, VBR, CBR등 여러 기술들이 개발 되어 왔다. 하지만 이런 노력에도 불구하고 이런 응용 서비스를 이용하다 보면 여러 가지 네트워크 원인에 의해 비디오 데이터가 완전 실시간이 아닌 이전 데이터일 경우 이거나 전송 트래픽의 전송률을 떨어뜨려 음성 데이터는 출력이 되나 비디오 데이터는 출력이 되지 않거나 비디오 화면과 소리가 서로 싱크가 맞지 않는 등 많은 문제가 발생 할 수 있다. 현재까지는 이런 문제가 발생하게 되면 엔지니어의 경험에 의존하여 문제를 해결 할 수밖에 없었고 많은 초고속 응용 서비스를 모두 해결하기에는 숙련된 엔지니어 수는 극히 적다. 하지만 본 연구에서 개발한 시스템에서 제공하는 사용자 traffic에 대해서 실시간으로 정보를 사용자 또는 망 관리자에게 제공하게 된다면 사용자에게는 자신의 traffic에 대한 정보를 실시간으로 제공 받을 수 있어 망 관리자 또는 서비스 제공자에게 네트워크의질 개선을 요구 할 수 있고 망 관리자에게는 숙련된 엔지니어가 아닐지라도 신속하게 장애요인을 파악하고 해결 하여 네트워크 사용자에게 높은 질의 서비스를 제공 할 수 있게 된다. 현재 PMACCT[3], NFDUMP[4] 등 많은 flow data 모니터링이 가능한 시스템이 개발되어 있으나 어느 한 지점에서만의 현재 이용 상태와 특정 시간동안 이용량에 대한 통계를 나타낼 뿐이지 특정 사용자 flow data에 대한 정보를 제공

하여 주지 않는 것으로 조사 되었다. 따라서 본 연구에서는 사용자 flow data가 이동하는 종단 간 라우팅 경로 상에 있는 라우터들로부터 사용자의 flow data를 수집하여 사용자의 종단 간 라우팅 경로를 찾고 각 구간별 패킷 전송률과 데이터 전송률을 측정 수치로 제공하여 사용자 flow data의 종단 간 흐름을 모니터링 할 수 있는 시스템을 제안 하고 구현 하였다. 또한 사용자 flow data가 이동하는 각 이동 경로상의 라우터들의 현재 상태를 모니터링 할 수 있도록 하였고 IPv4뿐만 아니라 IPv6를 사용하는 사용자 traffic에 대해서도 서비스를 가능 하도록 하였다.

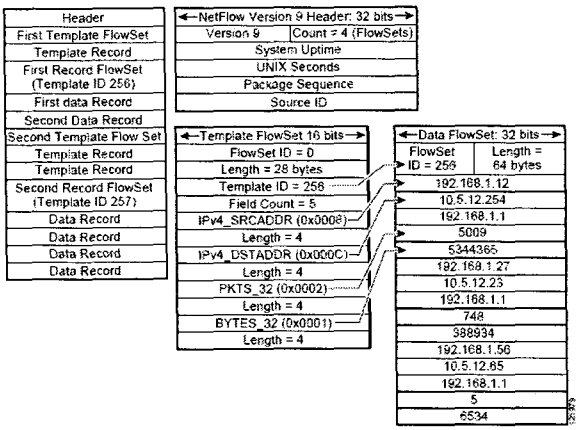
이 시스템은 Informational Traffic Flow Measurement Architecture[5]를 기반으로 설계되었으며 Meter, Reader로 구성된다. Meter는 각 라우터에서 flow data를 수집하여 Reader로 전송하고 Reader는 Meter에서 수집된 정보를 바탕으로 사용자가 자신의 flow data에 대한 정보를 요청 할 시 사용자의 flow data의 종단 간 라우팅 경로와 각 구간별 성능 요소로써 패킷 전송률과 데이터 전송률을 측정하여 사용자의 flow data 정보를 실시간으로 응답 할 수 있는 시스템을 구축 하였다. 또한 각 이동 경로 상의 라우터의 실시간 전송량 상태를 사용자가 볼 수 있도록 하였다. 우리는 Meter로 Cisco Netflow[6]을 사용하였고 Reader는 Java로 프로그래밍 한 서버를 사용 하였다. Netflow data collector로써 JNCA[7] 프로그램을 사용하여 NetFlow data를 MySQL 데이터 베이스에 저장하도록 하였다. 마지막으로 이 시스템을 KOREN 망에서 구축하여 실험 하였다.

1. NetFlow

데이터 통신에서 발생하는 일련의 패킷들을 NetFlow라고 정의할 수 있으며 NetFlow버전에 따라 다양한 정보를 포함하고 있다. NetFlow로부터 현재 우리 네트워크에 존재하는 트래픽에 대한 정보를 얻을 수 있으며 이 정보를 통해 현재 발생하고 있는 이벤트에 대한 추적이 가능하다. 기존의 MRTG(The Multi Router Traffic Grapher)가 실제 트래픽 사용률에 대한 정보를 보여 주었다면, NetFlow 데이터는 과다한 트래픽을 발생시키는 IP나, 바이러스에 감염된 PC, 그리고 현재 우리 네트워크에서 존재 하는 트래픽에 대해서 분석할 수 있게 한다. NetFlow 는 1996년 Cisco Systems[8].에서 개발이 되어 사용되고 있지만 현재는 다른 벤더 Enterasys, Juniper, extreme등 에서도 도입하여 사용되고 있다. Flow 규격은 현재 v1 부터 시작하여 v9 까지 존재하는데 그 중 라우터에서 BGP AS가 지원되기 시작한 v5가 현재 가장 많이 사용되고 있으며 Version 9 기반은 IPv6, MPLS, Multicast 등의 다양한 Flow 포맷들을 실어 보낼 수 있다. 또한 기존의 UDP 기반의 전송을 TCP 또는 SCTP 전송계층을 이용하도록 하여 신뢰성을 강화 시켰다.



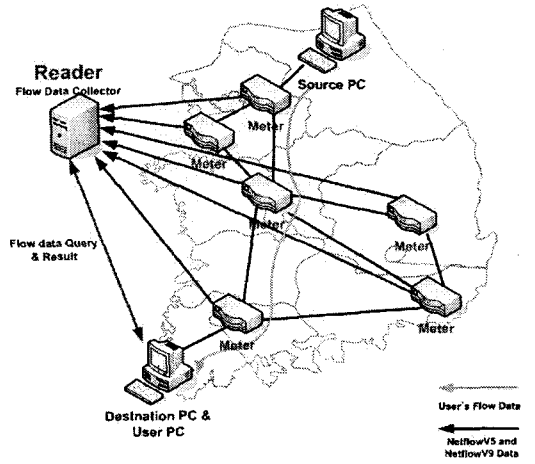
▶▶ 그림 1 Cisco NetFlow V5



▶▶ 그림 2 Cisco NetFlow V9

2. 시스템 구성

종단 간 Flow data 모니터링 시스템의 구조는 그림3과 같이 각 라우터에서 flow data를 수집하여 Reader로 전송하는 Meter, Meter로부터 모여진 flow data를 바탕으로 사용자 flow data의 종단 간 라우팅 경로를 찾고 각 구간별 성능을 측정하는 Reader, 그리고 사용자가 Reader에게 사용자의 flow data의 정보를 요청하면 Reader는 그 결과를 사용자에게 보여 주는 구조로 되어 있다.



▶▶ 그림 3. NetFlow monitoring 시스템

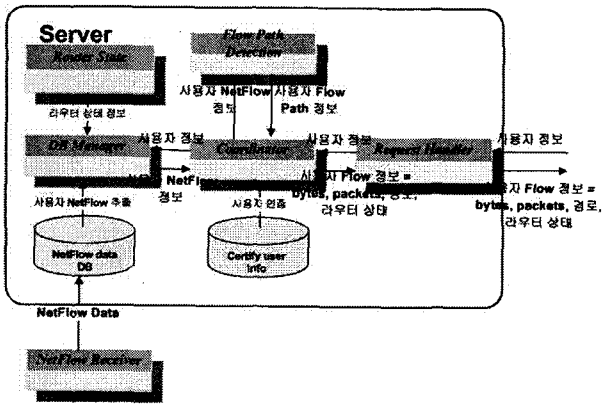
1) Meter

Meter는 망 안에서 정해진 지점에서 트래픽 flow에 대한 데이터를 수집하는 장치이다. 일반적으로 Meter는 라우터에 설치되며 Meter의 동작은 다음과 같다. Meter에 들어온 packet header는 PACKET PROCESSOR로 보내진다. PACKET PROCESS는 packet header에서 source_ip, destination_ip 등의 속성을 추출하여 matching key를 생성한다. 그 후 PACKET PROCESSOR는 특정 rule set이 정의된 Packet Matching Engine(PME)를 호출하여 matching key와 PME의 rule set을 비교한다. matching key와 rule이 일치하면 flow key를 생성하고 flow key는 flow table에 저장된다. Reader는 flow table에서 flow를 항상 수집할 수 있다[4].

우리가 제안한 시스템에서는 Meter로 Cisco Netflow를 사용하여 라우터를 지나가는 패킷들을1/10의 비율로 샘플링 하여 flow data를 생성하고 생성된 flow data를 Reader로 실시간으로 전송한다.

2) Reader(server)

Reader(server)는 그림4와 같이 Netflow data DB, Certify UserDB, Request Handler, DBManager, , Flow Path Detection, Router State 그리고 Coordinator로 구성하였다.



▶▶ 그림 4. Reader 시스템 구조

• NetFlow Receiver(JNCA)

Netflow Receiver는 각 Meter가 보내온 NetFlow 데이터를 MySQL DB로 저장하는 역할을 한다. NetFlow collector 프로그램으로 JNCA[6]을 사용하였고 MySQL DB는 heap memory를 사용하여 최소한의 NetFlow 데이터 drop이 발생하도록 하였다.

• Reuest Handler

Request Handler는 사용자 클라이언트와 통신을 담당하는 역할을 수행한다. 사용자가 요청한 사용자 flow data의 정보를 받아 Coodinator에게 보내고 해당 사용자의 flow data에 대한 패킷 전송률과 데이터 전송률, 현재 라우터 상태 그리고 라우팅 Path정보를 Coodinator로부터 받아 사용자에게로 보내는 기능을 한다. 이때 받는 사용자 flow data의 정보는 source_ip, source_port, destination_ip, destination_port, 그리고 period로 구성되어 있으며 여기서 period는 Reader에게 사용자가 모니터링 하기를 원하는 현재 시간부터 일정 시간 주기를 의미한다. 사용자는 자신의 flow data의 종단 간 라우팅 경로와 각 구간별 패킷 전송 율과 데이터 전송 율, 그리고 현재 이동 경로 상의 각 라우터의 현재 사용량에 대한 상태를 확인할 수 있다.

• Coodinator & Certify User

Coodinator는 먼저 사용자의 ip 주소를 이용하여 Certify User를 통한 Reader의 서비스를 이용할 수 있는 사용자인지 구별하여 주고 사용자가 요청한 period 마다 DBManager에게 사용자의 NetFlow Data 정보를 얻고 Flow Path Detection 모듈을 호출하여 사용자의 최신 라우팅 경로를 찾고 각 구간별 패킷 전송 율과 데이터 전송 율을 측정하여 Request Handler를 통해 사용자에게 전송하게 하는 역할을 한다. 이외에 Coodinator는 위에서 언급한 각 모듈들을 필요에 따라 호출 하고 각 모듈에서 반환한 값들을 다른 모듈로 넘겨주는 중계자 역할을 한다.

• NetFlow Data DB & DB Manager

Netflow data DB는 JNCA 프로그램을 이용하여 Meter가 수집하여 보내준 flow data를 그림 5와 같이 NetFlow Data Record 형태로 저장한다.

Field	Version 5	*Version 5 Catalyst 65k	Version 9	*Version 7 Catalyst 65k
source IP address	Y	Y	Y	Y
destination IP address	Y	Y	Y	Y
source TCP/UDP application port	Y	Y	Y	Y
destination TCP/UDP application port	Y	Y	Y	Y
next hop router IP address	Y	Y 12.1(13)E	Y	Y
input physical interface index	Y	Y	Y	Y
output physical interface index	Y	Y 12.1(13)E	Y	Y
packet count for this flow	Y	Y	Y	Y
byte count for this flow	Y	Y	Y	Y
start of flow timestamp	Y	Y	Y	Y
end of flow timestamp	Y	Y	Y	Y
IP Protocol (for example, TCP=6; UDP=17)	Y	Y	Y	Y
Type of Service (ToS) byte	Y	***PFC3b Only	Y	***PFC3b Only
TCP Flags (cumulative OR of TCP flags)	Y	N	Y	N
source AS number	Y	Y 12.1(13)E	Y	Y 12.1(13)E
destination AS number	Y	Y 12.1(13)E	Y	Y 12.1(13)E

▶▶ 그림 5. NetFlowV5 & V9 data field

DBManager는 Cordinator가 넘겨주는 사용자 Flow Data 정보를 받아 NetFlow Data DB에서 사용자의 NetFlow Data를 검색 · 추출한 후 Cordinator에게 최신 사용자의 NetFlow Data(경로, 패킷 전송률, 데이터 전송률)와 라우터의 상태 정보(데이터 전송량)를 넘겨준다.

• Flow Path Detection

Flow Path Detection은 Cordinator에게서 받은 사용자 Netflow data를 이용하여 사용자 Netflow data의 정보에 해당하는 flow data들을 추출하여 종단 간 라우팅 경로를 찾는다.

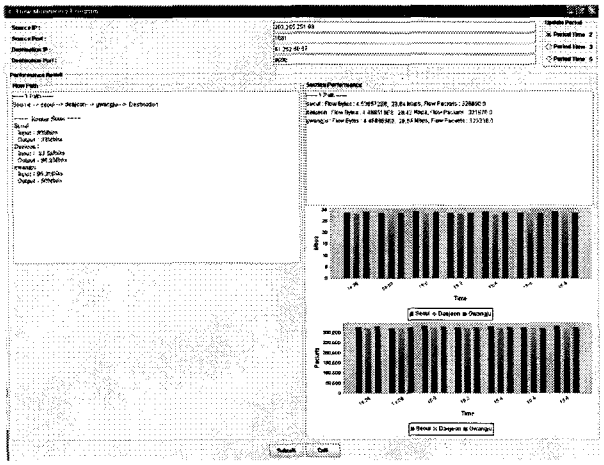
flow data의 종단 간 라우팅 경로는 다음과 같은 알고리즘을 통해 찾는다.

```
FindPath(){
  // 다음 라우터 찾기 & 설정
  for(int i=0; i<C_Router.length; i++){
    if(!C_Router[i].getPkts().equals("0")){
      C_Router.FindHoc(C_Router[i]);
    }
  }
  // 사용자 data path 찾기
  for(int k=0; k<C_Router.length; k++){
    for(int i=0; i<C_Router.length - 1; i++){
      if( C_Router[i].getcurRName().equals(
C_Router[i+1].getnxtRName()) ){
        TC_Router = C_Router[i];
        C_Router[i] = C_Router[i+1];
        C_Router[i+1] = TC_Router;
      }
    }
  }
}
```

먼저 추출한 라우터의 이름을 찾고 다음 목적지 라우터를 찾기 위해 후위 추적법을 사용하여 목적지가 연결된 목적지 라우터를 먼저 찾은 후 목적지 라우터를 next hop으로 하는 라우터를 찾고, 찾은 라우터를 다시 next hop으로 하는 라우터를 찾는 재귀적인 방법을 사용하여 종단 간 라우팅 경로를 찾는다.

3. 실 험

우리는 시스템을 KOREAN 상에서 각 각 Meter가 설치된 6개 라우터와 1개의 Reader 그리고 송(서울).수신(제주) 호스트를 구성하고 테스트를 하였다. 각 라우터는 flow data를 수집하여 NetFlowV5 와 V9를 Reader에게 전송하게 되고 Reader는 NetFlow Collector JNCA를 이용하여 NetFlow data를 MySQL 데이터 베이스에 저장을 한다. Server는 MySQL에 저장된 NetFlow를 이용하여 사용자 Flow data정보 요청에 대해서 응답을 한다. 클라이언트는 사용자PC에서 동작하며 Server에게 현재 자신이 사용하는 트래픽에 대한 정보를 요청할 수 있다.



▶▶ 그림 4. Client 동작 화면

4. 결론 및 향후 과제

본 논문에서 제안한 종단 간 Flow data 모니터링 시스템은 사용자의 요청 시 사용자 flow data의 종단 간 라우팅 경로를 찾고 각 구간별 패킷 전송 율과 데이터 전송 율을 측정함으로써 사용자 flow data의 종단 간 흐름을 모니터링 할 수 있다. 또한 현재 각 라우터의 전송량 상태를 알 수 있다. 이 시스템을 통해 사용자는 사용자 flow data의 흐름에 문제 발생 시 망 관리자에게 문제 발생 구간과 정도를 객관적인 수치로 제시하여 서비스의 질 향상을 요구 할 수 있으며 망 관리자는 제시된 자료를 바탕으로 사용자 flow data 흐름을 개선함으로써 서비스의 질을 높일 수 있을 것으로 기대된다.

향후 과제로 NetFlow v9에 대한 측정요소를 다양화를 위하여 여러 기능을 추가하고 NetFlow data drop를 최소화 할 수 있도록 NetFlow data 저장 모듈을 강화하여 모니터링 결과의 정확성과 객관성을 더욱 높일 것이다. 또한 종단 간 Flow data 모니터링 시스템을 트래픽 엔지니어링 기술과 결합하여 특정 사용자 flow data흐름에 문제 발생 시 망 관리자가 직접 문제를 해결 하지 않고 자동으로 문제를 해결하는 시스템을 추가할 계획이다.

▌참 고 문 헌▐

[1] http://www.internet2.edu
[2] http://www.koren21.net
[3] http://www.pmacct.net/
[4] http://nfdump.sourceforge.net/
[5] RFC2722, "Traffic Flow Measurement: Architecture"
[6] Cisco System, "NetFlow Services and Applications"White Papers, http://www.cisco.com/warp/public/cc/pd/iosw/ioft/neflct/tech/napps_wp.htm
[7] http://jnca.sourceforge.net/
[8]http://www.cisco.com/en/US/tech/tk812/tsd_technology_support_protocol_home.html