# 인터넷 트래픽 측정 방법 및 시스템

**Methodology and Systems for Internet Traffic Measurement**


정재훈(J.H. Jeong) 차세대인터넷표준연구팀 연구원
이승윤(S.Y. Lee) 차세대인터넷표준연구팀 선임연구원
김용진(Y.J. Kim) 차세대인터넷표준연구팀 책임연구원, 팀장



원활한 인터넷 서비스를 제공하기 위해서는 인터넷 트래픽을 효율적으로 관리할 수 있어야 하며, 이를 위해 가장 먼저 해야 할 것은 인터넷 트래픽을 측정하는 것이다. 인터넷 트래픽의 측정은 수동적인 측정과 능동적인 측정으로 분류된다. 수동적인 측정은 라우터나 ATM 스위치를 통해 흘러 다니는 트래픽 종류와 트래픽 양을 측정하여 측정네트워크의 트래픽 특성을 파악하는 것이고, 능동적인 측정은 측정네트워크 종단에 위치한 두 호스트 사이에 측정패킷을 투입하여 측정네트워크의 상태를 파악하는 것이다. 본 고는 현재 알려진 인터넷 트래픽 측정 방법과 현재 구현된 측정 시스템을 소개한다.


## I. 서 론

인터넷은 현재 세계의 정보망을 이루고 있는 중요한 네트워크이다. 인터넷의 네트워크 프로토콜은 Internet Protocol(IP)로써 현재는 IPv4가 주로 사용되고 있으나, 최근 IP 주소고갈문제를 포함하여 차세대인터넷을 위한 다양한 요구사항을 수용하기 위하여 차세대 IP로 등장한 IPv6가 점진적으로 적용되고 있는 추세다. 이러한 IP를 통해 전송되는 주요 인터넷 트래픽으로는 TCP, UDP, ICMP 등이 있으며, 응용 관점의 트래픽으로는 TELNET, FTP, HTTP, SMTP, SNMP, RPC, RTP, RTCP 등이 있다. 사용자들의 정보를 담고 있는 IP 패킷은 사용자의 호스트를 떠나 라우터를 통해서 목적지로 이동하게 된다. 인터넷 트래픽이 라우터를 통해 지나가는 것을 측정할 수 있다면 유용한 정보를 만들 수 있다.

트래픽 측정은 크게 두 가지로 나눌 수 있는데, 네트워크의 트래픽 특성을 파악하는 수동적인 측정(passive measurement)과 네트워크의 상태를 파악하는 능동적인 측정(active measurement)으로 구분된다[1],[2]. 예를 들면, 수동적인 측정은 인터넷 서비스를 제공하는 ISP에서 사용자의 과금을 책정할 때 이용될 수 있다. ISP의 과금 정책은 허용 대역에 따라 사용료를 책정하고 있지만, 사용 트랙픽의 종류와 양을 파악하면 실제 네트워크 이용률을 계산해서 보다 공평한 과금을 책정할 수 있다. 또한 수동적인 측정은 어떤 네트워크에서 발생되는 트래픽 종류와 양을 파악하여 현재 가장 많이 사용되는 서비스 종류를 파악할 수 있다. 최근 조사의 의하면 넵스터와 웹 트래픽이 가장 많이 발생되었고, 또한 비교적 작은 크기의 패킷이 많이 사용되고 있는데, 대부분 게임관련 트래픽으로 밝혀졌다. 이처럼 네트워크에 발생되는 트래픽의 종류와 양을 정량적으로 측정하여 네트워크 특성을 정확히 파악한다면 효율적인 네트워크 서비스를 할 수 있을 것이다. 즉, 현재 발생되는 트래픽을 최적으로 서비스 할 수 있는 라우팅 정책, 라우터의 스케줄링 기법 그리고 라우터의 버퍼 관리 기법 등을 선택할 수 있다.

능동적인 측정은 네트워크 종단 호스트들간의 인터넷 데이터 패킷이 중간에 여러 라우터를 통해 목적지로 어떻게 서비스를 받으며 이동을 하고 있는지를 파악하여 네트워크 상태를 진단할 수 있게 한다. 패킷은 경로상의 네트워크 상태에 따라 전송 처리율이나 손실률이 결정된다. 즉, 중간 라우터에 체증이 발생하면 라우터의 버퍼 관리 기법에 의해 패킷들이 버려지게 되어 종단 호스트들에게는 손실되는 패킷으로 간주된다. 한 호스트에서 다른 호스트로 가는 경로는 RIP, OSPF 그리고 BGP 등의 라우팅 프로토콜에 의해 결정이 된다. 특히 OSPF는 링크 상태에 따라 로드 밸런스를 하여 보다 효과적으로 패킷을 라우팅 할 수 있다. 네트워크 종단간의 경로에 측정 패킷을 투입하여 서비스 받는 것을 장시간 관찰하면 이 경로상의 네트워크의 상태를 파악할 수 있다. 패킷전송 시간과 손실률이 증대되고, 지터가 커지면 경로상의 특정 네트워크에 문제가 발생했음을 알 수 있다. 이러한 경우에는 문제가 되는 경로의 네트워크를 발견하여 적절한 조치를 취함으로써 호스트 종단간의 네트워크가 원활한 서비스를 할 수 있다. 취할 수 있는 조치로는 라우터의 라우팅 테이블의 수정, 보다 우수한 성능의 라우터로의 교체, 링크 용량의 증대 등이 있다.

위와 같이 수동적 측정을 통해 네트워크의 트랙픽 특성을 파악할 수 있고, 능동적 측정을 통해 네트워크의 상태를 진단할 수 있다. 따라서, 트래픽 측정은 효율적인 네트워크 관리에 필수적인 역할을 한다. 본 고는 트래픽 측정에 관련된 연구동향과 개발된 시스템을 소개하는 데 그 목적이 있다.

본 고의 구성은 다음과 같다. II장에서는 트래픽 측정에 관련된 표준화 활동을 IETF의 IP Performance Metrics(IPPM) 워킹 그룹(WG)을 중심으로 소개하고, III장에서 트래픽 측정의 전반적인 구조를 설명한다. IV장에서 수동적 측정의 방법과 개발된 시스템을 설명하고, V장에서는 능동적 측정의 방법과 개발된 시스템을 설명한다. VI장에서 결론과 앞으로의 동향을 제시한다.

## II. IETF의 IPPM WG

IPPM WG의 임무는 인터넷 데이터 전송 서비스에 관련된 표준 메트릭을 개발하는 것이다[3]. 표준 메트릭이 다루는 것은 품질(Quality), 성능(Performance) 그리고 안정성(Reliability)이다. 이러한 메트릭은 네트워크 오퍼레이터나 종단 사용자 그리고 독립적인 테스트 그룹에 의해 사용될 수 있다. 메트릭이 제공하는 것은 측정값의 좋고 나쁨이 아니라 편중되지 않은 정량적인 측정량이다. 이처럼 IPPM WG은 특정 메트릭을 정의하고 그 메트릭을 정확하게 측정할 수 있는 측정방법 및 기술을 연구하고 측정 도구의 개발 및 공유를 증대하는 데 목적을 두고 있다. 하지만, 실제적인 측정 도구의 구현과 응용 프로그램은 다루지 않는다. <표 1>은 지금까지 발표한 RFC를 나타내고 있고, <표 2>는 IP 성능 측정에 관련된 인터넷 작업 문서들(Internet-draft)을 나타내고 있다.

IPPM에서 만든 표준 문서는 IP 성능 측정에 관련된 측정도구를 만드는 데 기초가 된다. 특히 능동적 측정 도구를 만드는 데 중요한 정보를 제공하고 있다.

<표 1> IETF의 IPPM WG이 발표한 RFC

| RFC 번호 | 제목 | 설명 |
|---|---|---|
| 2330 | Framework for IP Performance Metrics | IP 성능 메트릭을 측정하기 위한 측정 방법과 측정 구조를 기술 |
| 2678 | IPPM Metrics for Measuring Connectivity | 네트워크의 연결을 측정하기 위한 IPPM 메트릭을 정의 |
| 2679 | A One-Way Delay Metric for IPPM | IPPM의 단방향성 지연 메트릭을 정의 |
| 2680 | A One-Way Packet Loss Metric for IPPM | IPPM의 단방향성 패킷 손실 메트릭을 정의 |
| 2681 | A Round-Trip Delay Metric for IPPM | IPPM의 양방향성 지연 메트릭을 정의 |

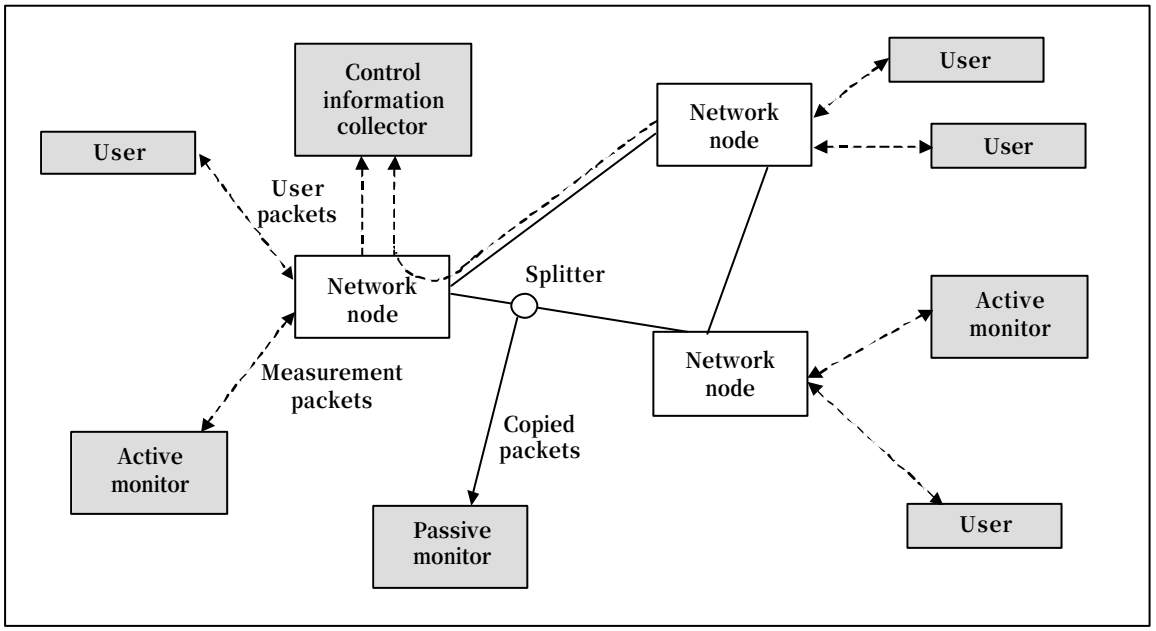
<표 2> IETF의 IPPM WG이 발표한 Internet-Draft

| 제목 | 설명 |
|---|---|
| IP Packet Delay Variation Metric for IPPM | IP 패킷의 지연 변화량의 정의를 기술 |
| A Framework for Defining Empirical Bulk Transfer Capacity Metrics | 대량 전송 용량 메트릭을 측정하는 구조를 기술 |
| One-Way Loss Pattern Sample Metrics | 단방향성 손실 패턴 메트릭을 정의 |
| Network Performance Measurement for Periodic Streams | 주기적 스트림의 네트워크 성능 측정을 기술 |
| A One-Way Delay Measurement Protocol | OWDP라는 단방향성 지연을 측정하는 구조를 기술 |
| A Bulk Transfer Capacity Methodology for Cooperating Hosts | 상호 작용하는 호스트간의 대량 전송 용량을 측정하는 방법을 기술 |

## III. 트래픽 측정 구조

인터넷 트래픽을 측정하기 위해서는 측정도구가 필요하다. 측정도구는 측정을 하고자 하는 네트워크에 배치되어 원하는 측정 메트릭을 수집하고 수집된 메트릭을 측정 데이터로 가공하여 분석가에게 제공한다. (그림 1)은 인터넷 트래픽을 측정하기 위한 일반적인 측정 구조를 나타내고 있다[4].

(그림 1)은 수동적인 측정과 능동적인 측정을 동시에 나타내고 있다. 수동적인 측정은 두 가지로 나눌 수 있는데, 첫째는 분리기(Splitter)를 이용하는 방법으로 ATM 스위치 같은 네트워크 노드(Network node) 사이의 링크에 분리기를 연결시켜서 두 네트워크 노드 사이를 통과하는 패킷을 복사해서 Passive monitor에게 넘겨주어 그 네트워크 노드 사이를 통과하는 트래픽 종류와 양을 파악할 수 있다. 둘째는 라우터 같은 네트워크 노드를 통해 지나간 패킷들의 종류와 양에 대한 통계적인 정보를 제공하는 패킷을 이용하는 방법으로 이 패킷을 주기적으로 Control Information Collector에게 전달하고, Collector는 전달받은 통계 정보를 통해 네트워크 노드의 특정 네트워크 인터페이스를 통해 출입한




(그림 1) 일반적인 측정 구조

트래픽의 종류와 양을 파악할 수 있게 한다. 능동적인 측정은 종단 호스트인 Active monitor가 측정 패킷(Measurement packet)을 주기적이거나 랜덤하게 네트워크에 투입하여 그 측정 패킷이 측정구간의 두 Active monitor 사이에서 지연되는 시간과 손실되는 정도를 측정하여 그 구간의 네트워크 상태를 파악할 수 있게 한다.

## Ⅳ. 수동적 측정 도구

수동적 측정은 네트워크에 유통되는 패킷 정보를 수집하고 분석함으로써 이용자별, 시간대별, 프로토콜별, 응용별로 특정 네트워크를 출입한 패킷을 파악하여 그 네트워크의 트래픽 특성을 파악할 수 있게 한다. 인터넷 백본에서의 트래픽 유통량이나 사용 패턴의 분석은 그 백본 네트워크의 성능 파악은 물론 앞으로의 네트워크 링크 용량 증대에 유용한 정보를 제공한다[1].

기존에 수행되었던 인터넷 트래픽 패턴 분석의 연구에 의하면 대부분의 인터넷 패킷은 송신자와 수신자 사이의 연속적인 데이터 흐름을 이루고 있음이 밝혀졌다. 이러한 연구의 결과로 등장한 MPLS(Multi-Protocol Label Switching)는 인터넷 트래픽을 연속적인 패킷 흐름인 플로우(Flow)로 모델링하여 고정된 레이블(Label)을 이용하여 고속으로 패킷을 스위칭함으로써 IP 라우팅의 성능을 향상시킬 수 있다. IP 플로우는 다음과 같이 정의될 수 있다. IP 플로우는 응용의 주소 쌍(송신자 주소, 송신자 포트 번호, 수신자 주소, 수신자 포트 번호), 호스트 쌍(송신자 네트워크 주소, 수신자 네트워크 주소), AS 번호 쌍(송신자 AS 번호, 수신자 AS 번호) 등으로 명세되는 제한된 시간 내에 도착하는 IP 패킷들의 흐름이다. 이러한 플로우 모델은 패킷 트레인 모델로 처음 제안되었다[5]. 플로우의 정의는 사람마다 다르다. 플로우 정의의 한 예를 들면, TCP 연결에서 송신자와 수신자의 주소와 포트 쌍으로 이루어진 플로우는 SYN과 ACK로 플로우의 시작과 끝을 구분할 수 있다. 플로우의 길이는 다양한데, 전자메일은 대부분 몇 개의 IP 패킷으로 플로우를 구성하지만, VOD와 같은 멀티미디어 서비스의 플로우는 많은 IP 패킷으로 플로우를 구성한다.

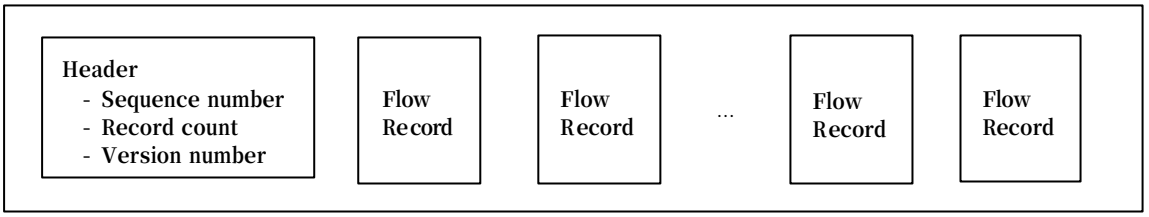
이러한 플로우 측정을 포함하는 대표적이고 수동적인 측정은 Cisco의 NetFlow와 CAIDA(Cooperative Association for Internet Data Analysis) 그룹의 Cflowd를 이용한 구조인데, 서울대의 CINERA와 FlowScan이 대표적인 측정도구이다. 이 장에서는 수동적 측정 구조와 수동적 측정을 위해 구현되어 있는 시스템들을 소개한다.

### 1. NetFlow

Cisco의 네트워크 플로우는 송신자에서 수신자로의 일련의 단방향성 패킷의 흐름으로 정의된다[6]. Cisco의 NetFlow는 Cisco 라우터가 각 네트워크 인터페이스를 통해 지나가는 트래픽의 플로우 정보를 제공하는 기능이다. 플로우의 구분은 IP 주소와 포트 번호로 되는데, Cisco의 NetFlow는 플로우의 구분을 위해 IP Protocol type, Type of Service(TOS) 그리고 Input interface identifier도 같이 사용하면서 플로우의 정보를 제공한다. NetFlow는 NetFlow Cache를 이용하여 동작하는데, NetFlow Cache Software는 특정 패킷이 기존에 존재하는 플로우에 속하는지 여부에 따라 Cache에 새로운 플로우 엔트리를 생성할지를 결정한다. 또한 플로우 해제시간(expire time)이 지난 플로우들의 정보를 (그림 2)의 'NetFlow Export' UDP 데이터그램의 페이로드에 담아서 플로우 정보 Export 네트워크 인터페이스로 전송한다. (그림 3)은 Cisco NetFlow Version 5 Flow Header를 기술하고 있고, (그림 4)는 Cisco NetFlow Version 5의 Flow Entry를 기술하고 있다.

### 2. Cflowd

Cflowd는 Cisco의 NetFlow를 이용한 스위칭 방법을 분석하기 위해 현재 사용되고 있는 플로우 분석 도구이다[7]. 현재 릴리스 버전은 수집, 저장, 기본적인 분석 모듈을 포함하고 있다. arts++ 라이브




(그림 2) NetFlow Export UDP 데이터그램의 페이로드 구조

| version | count |
|---|---|
| sysUpTime | |
| unix seconds | |
| unix nano seconds | |
| flow sequence number | |
| engine type | engine ID | reserved |

(그림 3) Cisco NetFlow Version 5 Flow Header

| source IP address | | | |
|---|---|---|---|
| destination IP address | | | |
| next hop IP address | | | |
| input interface index | | output interface index | |
| packets | | | |
| bytes | | | |
| start time of flow | | | |
| end time of flow | | | |
| source port | | destination port | |
| pad | TCP flags | IP protocol | TOS |
| source port | | destination port | |
| src netmask len | dst netmask len | | padding |

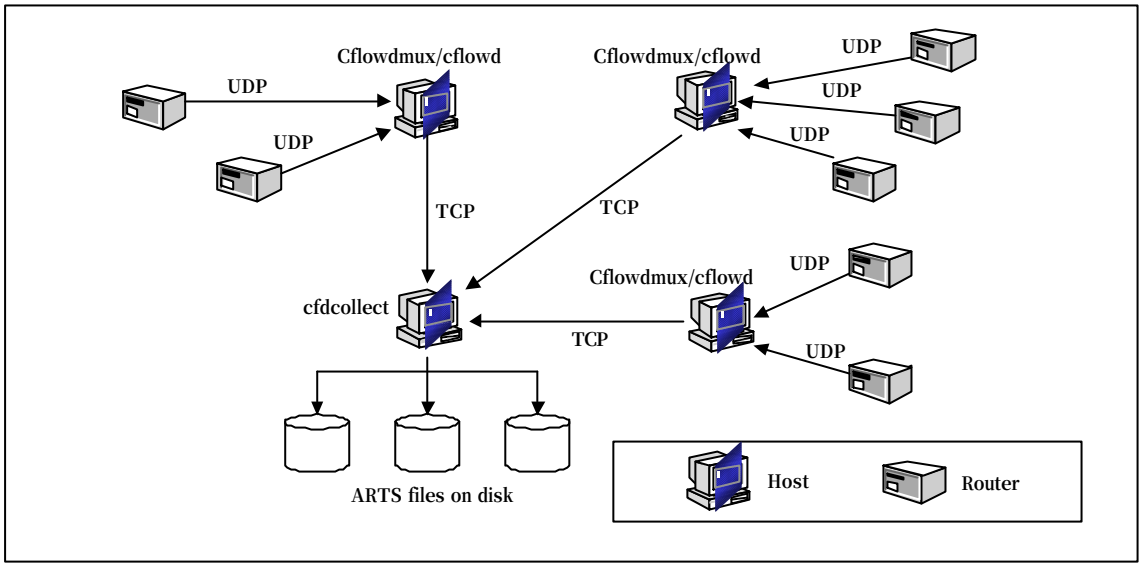
(그림 4) Cisco NetFlow Version 5 Flow Entry

러리를 이용하여 기본적인 분석 모듈을 만들었다[8]. 위의 분석 패키지는 ISP나 네트워크 엔지니어가 Capacity planning, Trends analysis 그리고 네트워크 서비스 환경에서 워크로드의 특성을 파악할 수 있도록 데이터 수집과 분석 기능을 제공하고 있다. 그밖에도 Web hosting, Billing, Network planning, Network monitoring 그리고 Data warehousing/mining 등을 할 수 있게 한다. (그림 5)는 Cflowd의 데이터 흐름을 나타내고 있다.

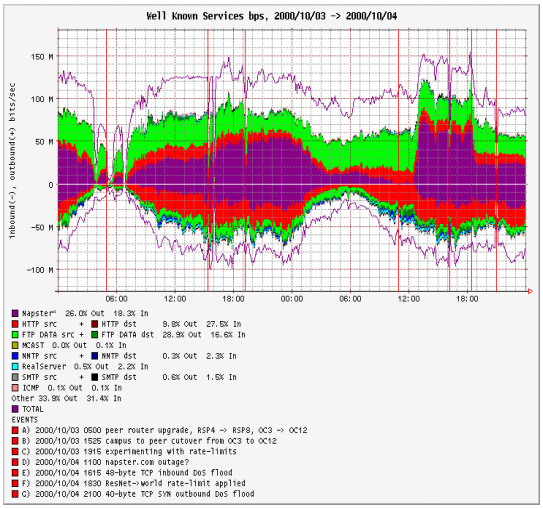
(그림 5)와 같이 각 Cisco 라우터는 Flow-export 패킷을 cflowdmux와 cflowd를 실행하고 있는 호스트에 보낸다. 호스트의 cflowdmux는 UDP 데이터그램인 Flow-export 패킷을 수신하여 공유메모리 버퍼에 쓰고, 호스트의 cflowd는 공유메모리에 쓰여진 패킷을 읽어서 로컬 테이블에 저장한다. 최종 데이터 수집은 호스트의 cfdcollect에 의해 수행되는데, cfdcollect는 주기적으로 한 번에 하나의 cflowd와 TCP 연결을 맺고 cflowd의 로컬 테이블로부터 테이블 데이터를 수집하여 ARTS라는 바이너리 파일로 저장한다. arts++ 패키지를 통해 ARTS 파일로부터 AS matrix. Net matrix 같은 여러 가지 통계정보를 얻을 수 있는데, 이 통계정보를 가지고 데이터를 수집한 네트워크의 트래픽을 분석할 수 있다.

## 3. FlowScan

CAIDA 그룹의 FlowScan은 라우터들에 의해 전달된 IP 플로우 데이터를 분석하여 그래프와 텍스트로 결합된 이미지를 만들므로 웹 인터페이스를 통해 결과 이미지를 보고 트래픽 분석을 쉽게 할 수 있게 한다[9]. FlowScan은 Perl 스크립트와 모듈로 구성되어 있고, 다음의 패키지를 통합하여 동작한다. (1) Flow collection engine(cflowd의 패치된 버전), (2) High performance database(Round Robin Database - RRD) 그리고 (3) Visualization tool(RRDtool)[10],[11]. (그림 6)은 FlowScan의 이미지 그래프를 나타내고 있다. 이 그림은 연속적인 시간으로 네트워크 트래픽을 보여주고 있는데,




(그림 5) Cflowd의 데이터 흐름



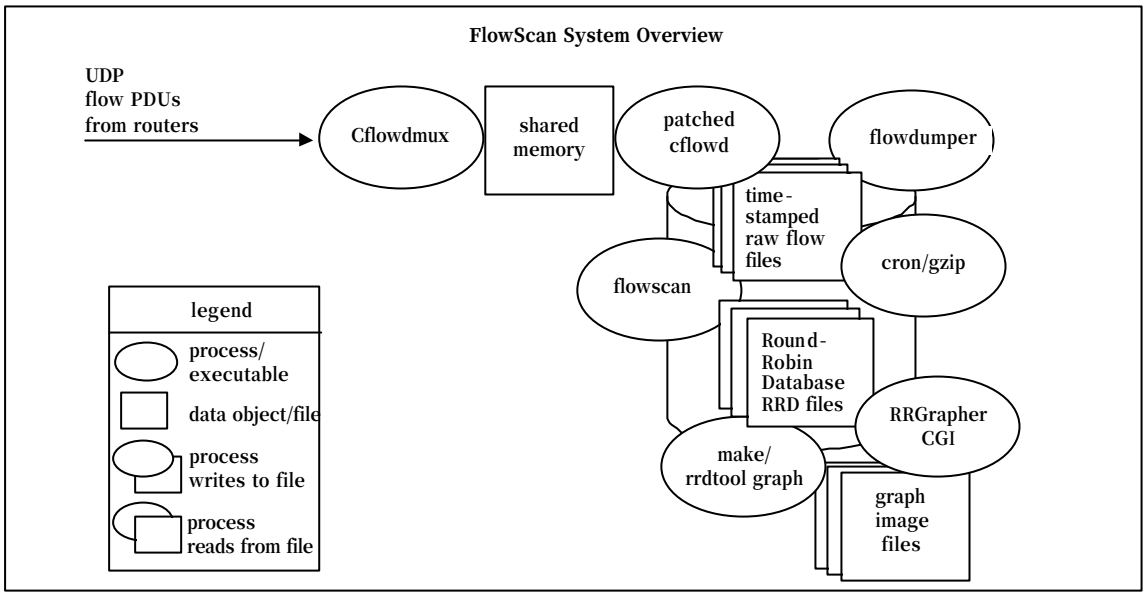

(그림 6) FlowScan의 그래프 이미지

넷스터 트래픽이 인바운드와 아웃바운드에서 가장 많은 부분을 차지하고 있다. 다음으로 많은 트래픽은 웹 트래픽(HTTP)과 FTP 트래픽이다. 또한 전체 인바운드 트래픽보다 전체 아웃바운드 트래픽이 많음을 알 수 있는데, 이 결과를 통해 이 네트워크의 기관이 외부로부터 사용하는 인터넷 컨텐츠 보다 자신이 제공하는 인터넷 컨텐츠가 더 많음을 유추할수있다.

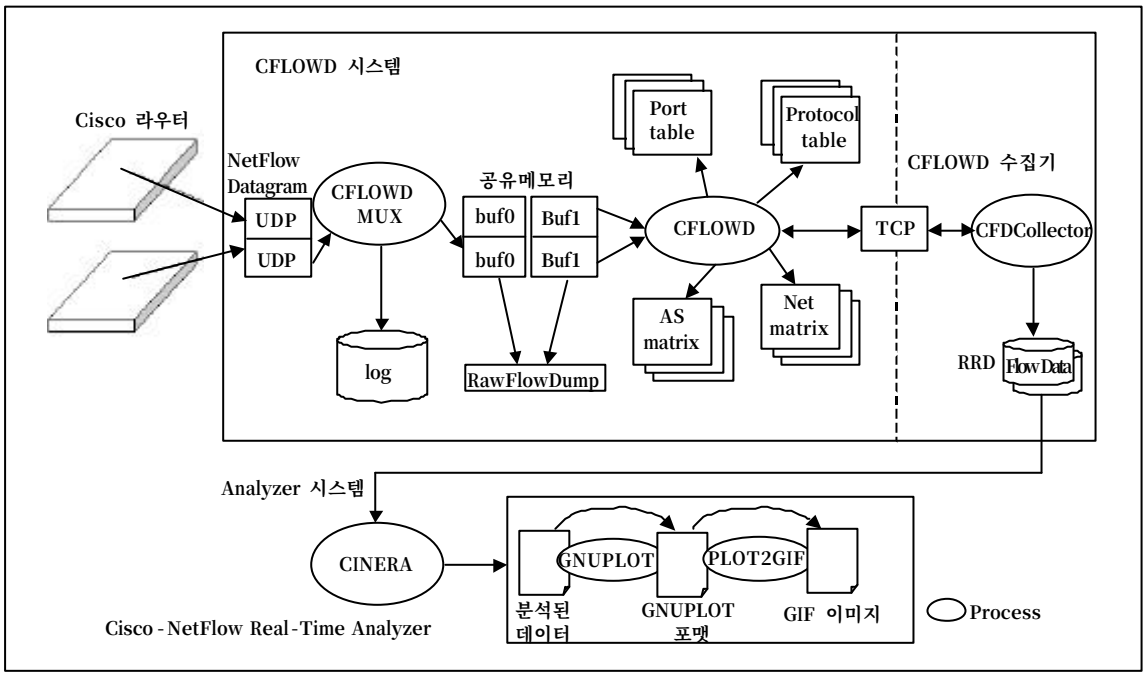
(그림 7)은 FlowScan 시스템 구조를 나타내고 있다. FlowScan은 여러 개의 소프트웨어 컴포넌트로 구성되어 있다. 첫번째 컴포넌트는 패치된 cflowd인데, 기존의 cflowd에 5분마다 Flow file에 타임스탬프를 찍는 기능이 추가되었다. 두번째 컴포넌트는 flowscan이라는 Perl 스크립트이다. 이것은 네트워크 관리자에 의해 선택된 Report module들을 로드하여 실행한다. 세번째 컴포넌트는 RRDtool이다. 이것은 Numeric time-series data를 저장하고 이 데이터를 시간축으로 통합(aggregate)한 뒤에 RRD 파일로 저장한다. RRDtool과 RRGrapher는 .gif나 .png 형태의 파일로 그래프 이미지를 생성한다. FlowScan은 사용하는 운영체제 유틸리티들이 있는데, 다음과 같다. (1) make 명령어, (2) cron job-scheduling facility 그리고 (3) gzip compressor. 마지막으로 flowdumper라는 유틸리티가 있는데, 이것은 Raw flow를 조사하는 데 사용된다.

## 4. CINERA

CINERA(Cisco-NetFlow Real-Time Analizer)는 서울대학교 멀티미디어 통신 연구실에서 개발한 것으로 FlowScan과 같은 기능을 수행한




(그림 7) FlowScan 시스템 구조




(그림 8) CINERA 시스템 구조

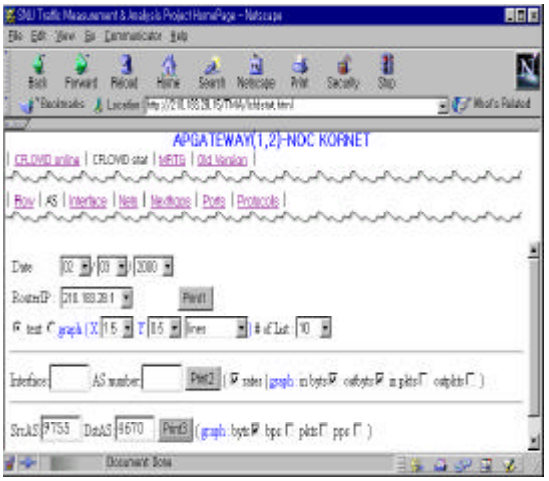
다[1]. 즉 웹을 통해 트래픽 분석을 쉽게 할 수 있게 하는 측정도구인데, Perl 스크립트로 구현되어 있다. (그림 8)은 CINERA 시스템 구조이다. CINERA는 RRD에 저장된 플로우 데이터를 읽어와서 .gif의 그래프 이미지를 만든다.

CINERA의 웹 인터페이스는 두 가지 기능으로 구성되어 있다. 하나는 시간축으로 갱신되는 측정결과를 계속적으로 보여주는 실시간 분석기

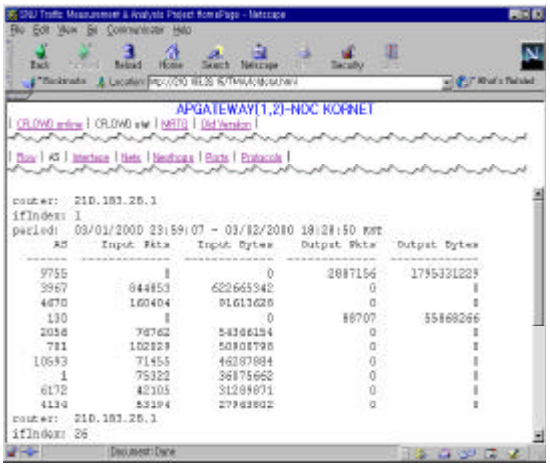
능(CFLOWD online)이고 다른 하나는 과거의 측정결과를 텍스트나 그래프 이미지 형태의 요약 정보로 출력하는 통계 분석기능(CFLOWD stat)이다.

실시간 분석기능은 (그림 9)와 같이 5분 단위로 통합된 트래픽 정보를 실시간으로 보여준다. 통계 분석기능은 (그림 10)과 같이 특정 라우터의 특정 네트워크 인터페이스를 통해 출입한 트래픽에 대한 통계 분석을 하기 위한 것으로, 쿼리를 입력하고 그 쿼리를 처리하게 하면, (그림 11)처럼 해당 쿼리의 결과가 출력된다.


(그림 9) CINERA의 실시간 분석기능(CFLOWD online)




(그림 10) CINERA의 통계 분석기능(CFLOWD stat)




(그림 11) 통계 분석기능의 쿼리에 대한 출력

## V. 능동적 측정 도구

인터넷이 비대칭적인 구조라는 사실은 많은 논문에서 밝혀졌다[12]. 비대칭성을 갖고 있는 인터넷의 현재 상황을 잘 측정하기 위해 단방향 측정이 필요하게 되었다. IETF의 IPPM 워킹 그룹은 단방향 메트릭과 단방향 측정구조를 제시하고 있다[13]. 측정 메트릭으로는 단방향 지연시간(one way delay), 지연시간 편차(delay variation), 단방향 패킷 손실(one way packet loss), 패킷 손실 패턴(packet loss pattern) 등이 있다[14] - [16]. 단방향 측정은 능동적인 트래픽 측정에 속한다. 측정 메트릭을 얻기 위해서는 측정패킷을 측정할 구간에 능동적으로 투입하여 그것이 그 경로 상에서 서비스를 어떻게 받는지를 관찰하기 때문이다[17]. 이러한 능동적인 측정을 통해 얻은 단방향 메트릭을 가지고 네트워크 관리를 효율적으로 할 수 있다. 예를 들면, 단방향 측정시스템 종단간의 경로상에서 측정되는 단방향 지연시간을 지속적으로 관찰하여 평소보다 지연시간이 급증한다면 네트워크에 어떤 문제가 발생했다고 추측할 수 있다. 또한 장기간 네트워크를 관찰하여 얻은 측정 결과를 통해 병목 현상이 발생한 경로를 찾아서 자원의 재배치, 링크 용량 증대 그리고 라우터의 성능 개선 등을 통해 네트워크 전체 성능을 향상시킬 수 있을 것이다. 이처럼 네트워크 관리에 필수적인

능동적인 측정시스템은 정확한 측정과 측정 데이터의 효과적인 관리 그리고 운영자가 쉽게 이용할 수 있는 사용자 인터페이스를 제공하는 것이 중요하다. 또한 안정적으로 측정을 할 수 있는 시스템이어야 한다. 이 장에서는 능동적 측정 구조와 능동적 측정을 위해 구현되어 있는 시스템들을 소개한다.

## 1. Skitter

Skitter는 CAIDA 그룹에서 제시한 측정시스템으로 인터넷 토폴리지와 성능을 분석하기 위해 인터넷에 측정패킷을 투입하여 그 패킷을 관찰한다[18]. Skitter의 중요 기능은 다음과 같다. Forward IP Path 측정, RTT 측정, 라우팅 변화의 지속적인 추적 그리고 네트워크 연결도의 도식화 기능 등이 있다. 사용자 인터페이스가 사용하기 쉽게 잘 구성되어 있으나 측정 메트릭으로 양방향 인자인 RTT만을 지원하고 있으므로 단방향 메트릭을 구할 수 없는 단점이 있다.

## 2. Surveyor

Surveyor는 Advanced Network & Services 그룹에서 제시한 시스템으로 단방향 메트릭을 측정할 수 있다[19],[20]. 이 시스템은 IETF의 IPPM WG에서 제시하는 표준들을 기초로 한 측정 메트릭을 측정한다. 측정구조는 다음과 같다. GPS 위성의 시간 정보로 동기화된 측정시스템들과 측정시스템을 제어하여 측정 결과를 수집하는 중앙 제어시스템으로 구성되어 있다. 측정시스템간의 시간 동기화를 이루기 위해 GPS 보드를 이용하는데, GPS 수신기로 받은 시간 정보를 PCI 버스를 통해 PC로 읽어 들여서 측정시스템의 하드웨어 시간을 GPS로부터 받은 시간과 동기화 시킨다. 측정시스템은 BSD 4.4 UNIX를 탑재한 PC이고 측정 프로그램은 OWDP(One - Way Delay and Packet loss protocol)에 따라 구현되었다[21],[22]. 정확한 단방향 지연을 측정하기 위해 측정패킷의 타임스탬프를 네트워크 디바이스 드라이버에서 찍고 있다. 현재 가장 많이 사용되는 있는 시스템이지만, 중앙 관리적 측정 구조의 운용이 대단히 경직되어 있어 측정 대상의 확장이 어렵고, 단반향 지연시간과 단방향 패킷 손실만 측정하므로 측정 메트릭이 적은 단점이 있다.

## 3. RIPE

유럽의 ISP들을 지원하기 위한 RIPE(Réseaux IP Européens)라는 곳에서도 단방향 지연시간을 측정하기 위한 구조를 만들어 운용하고 있다[23]. 여기서는 Surveyor와 동일하게 종단간 시간 동기화를 위해 GPS 수신기를 이용하였으나, Surveyor가 GPS 시간 정보를 읽어 오기 위해서 하드웨어적으로 문제를 해결한 반면, NTP에서 제공하는 디바이스 드라이버와 운영체제의 시스템 함수를 이용하여 소프트웨어적으로 운영체제 시간과 GPS 시간이 동기화 되게 한다. GPS 수신기에서 PC 안으로 시간 정보를 읽어 들이는 과정에서 다른 방법을 사용한 이 두 구조를 이용해서 동일한 환경에서 측정을 실시하고 결과를 비교해 본 결과, 그 차이가 거의 없음을 입증하는 실험 결과도 발표되었다. 그러나, 이 RIPE의 단방향 메트릭 측정 구조 역시 유럽내 ISP들간의 운용을 목적으로 만들어진 것으로 구조의 운용이 외부적으로는 매우 폐쇄적이고 이용이 제한적인 단점이 있다. 또한, 단반향 지연시간과 단방향 패킷 손실만 측정하므로 측정 메트릭이 적은 단점이 있다.

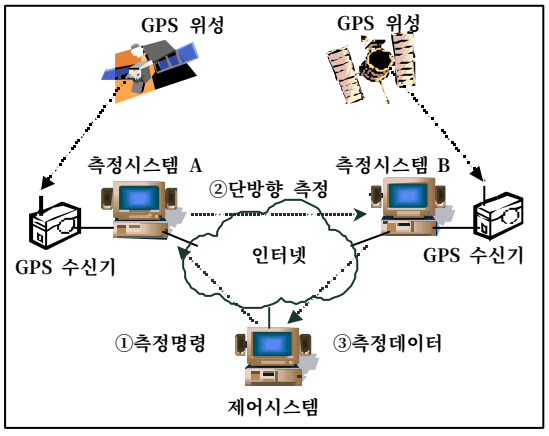
## 4. AMT

Active Measurement Tool(AMT)은 서울대학교 멀티미디어 통신 연구실에서 개발한 단방향성 IP 성능 측정을 위한 도구이다[2],[24]. AMT는 인터넷상의 특정 경로상에서 IETF의 IPPM WG에서 제시한 단방향 메트릭을 측정할 수 있다. 위의 Surveyor나 RIPE 보다 측정 메트릭이 많고, 확장성을 고려한 설계를 통해서 구현되었다. AMT는 FreeBSD UNIX를 운영체제로 하는 PC 기반의 시스템으로서, 데이터베이스 시스템으로는 MySQL을 사용한다.

### 가. GPS 위성을 이용한 측정시스템의 동기화

두 시스템간의 양방향 지연인 RTT를 측정하기 위해서는 두 시스템의 시간이 동기화될 필요가 없지만, 단방향 지연을 측정하기 위해서는 두 측정시스템간의 시스템 시간이 동기화 되어야 한다. (그림 12)는 GPS 위성을 이용한 측정시스템간의 동기화를 보여 주고 있다. 시스템간의 동기화를 쉽게 할 수 있는 방법으로써 GPS 위성의 시간 정보를 수신하여 그 시간을 가지고 주기적으로 측정시스템의 커널 시간을 보정하면 된다. GPS 위성의 시간 정보를 얻기 위해서 사용된 하드웨어는 다음과 같다. Motorola사의 Oncore Remote Antenna, Oncore GPS Receiver(UT)를 이용하여 GPS 시간 정보와 위성의 위치 정보를 수신한다[25].

수신된 시간 정보를 가지고 커널 시간을 보정하는 것은 Network Time Protocol을 운영하는 ntpd 데몬이다[26],[27]. 직렬 포트(serial port)와 병렬 포트(parallel port)에 수신되는 시간 정보는 PPS(Pulse Per Second)라는 신호로 부호화되어 있다. 각 포트의 디바이스 드라이버는 이 신호를 바이너리 정보로 변환하여 ntpd 데몬에게 전달한다. ntpd 데몬은 포트 디바이스의 파일을 통해 들어오는 시간 정보를 수신하고, NTP 커널 시간 보정 알고리즘을 통해 주기적으로 커널 시간을 정정하여 GPS 위성과 측정시스템을 동기화 시킨다.



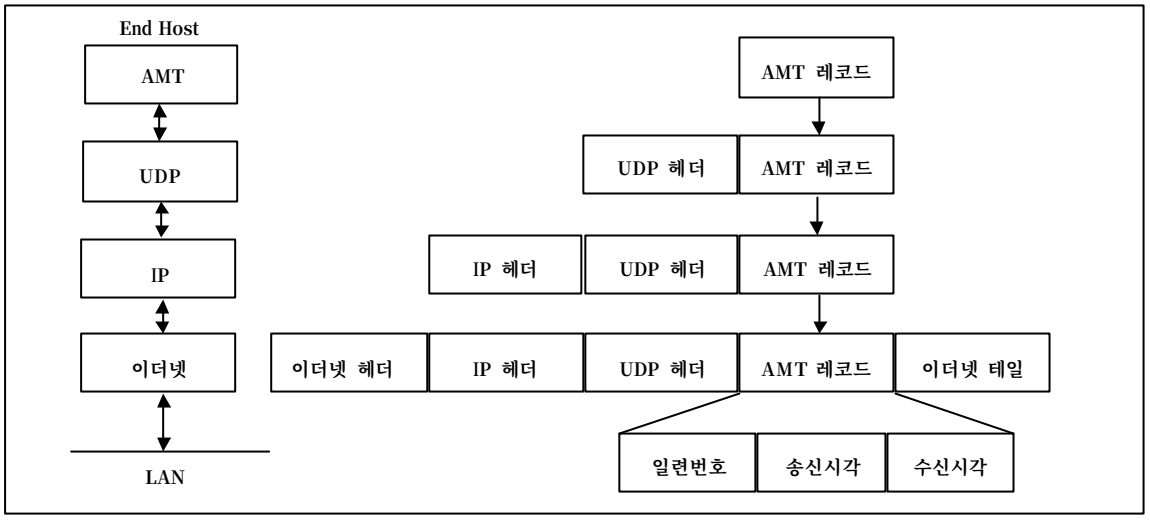

(그림 12) 측정시스템의 동기화와 측정 과정

### 나. 타임스탬프

정확한 지연시간을 측정하기 위해서는 송신자가 IP 패킷을 이더넷 프레임에 캡슐화하기 직전에 시간 정보를 기록해야 한다. 왜냐하면 응용 계층에서 타임스탬프를 기록하면, 계층간의 이동 지연이 발생하여 정확한 경로 지연 시간을 측정할 수 없게 된다. (그림 13)과 같이 송신 타임스탬프는 이더넷 계층에서 네트워크 인터페이스를 나가기 직전에 찍고, 수신 타임스탬프도 이더넷 계층에서 네트워크 인터페이스에서 받자마자 찍도록 이더넷 디바이스 드라이버를 수정하였다[20],[28].

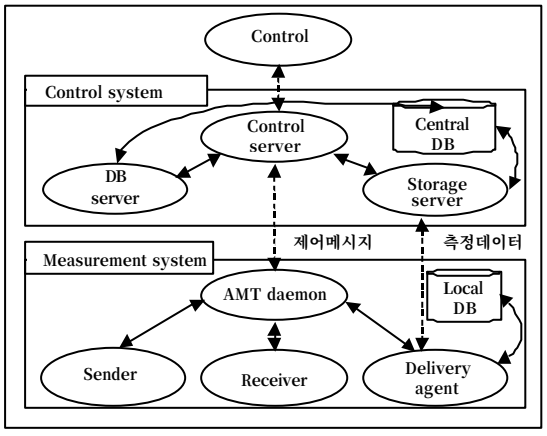
### 다. AMT 시스템 구조

AMT 시스템은 두 가지 종류의 시스템으로 이루어져 있다. 측정 네트워크에 측정패킷을 투입하여 측정을 담당하는 측정시스템(Measurement System)과 이러한 측정시스템을 제어하고 측정데이터를 관리하는 제어시스템(Control System)이 있다. (그림 14)는 제어시스템과 측정시스템으로 이루어진 AMT 시스템 구조를 나타내고 있다. 사용자는 Control shell을 통해 측정에 관련된 작업을 한다. 제어시스템은 세 개의 프로세스(Control server, Storage server 그리고 DB server)로 구성되어 있다. Control server는 Control shell이 보내는 명령을 처리하는 AMT의 핵심 프로세스로써 측정시스템을 제어하여 측정에 관련된 모든 일을 관리한다. Storage server는 측정시스템에 저장된 측정데이터를 중앙 데이터베이스(Central DB)로 수집하는 역할을 한다. DB-server는 측정결과를 분석하여 분석된 결과를 데이터베이스에 저장한다. 측정시스템은 네 개의 프로세스(AMT daemon, Sender, Receiver 그리고 Delivery Agent)로 구성되어 있다. AMT 데몬은 Control server의 제어메시지를 처리하여 실제적인 단방향 메트릭 측정을 하는 Sender와 Receiver를 제어한다. Sender는 측정패킷을 생성하여 송신시각 타임스탬프를 찍어서 다른 측정시스템의 Receiver들에게 전달한다. Re-




(그림 13) 타임스탬프를 기록하는 위치

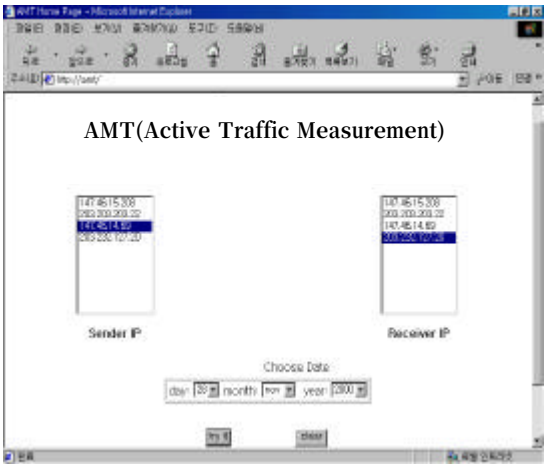
ceiver는 측정패킷을 수신하여 수신시각 타임스탬프를 찍고 측정시스템 내의 지역 데이터베이스(Local DB)에 저장한다. Delivery Agent는 측정이 종료되었을 때, 측정데이터를 제어시스템의 Storage server에게 전달하는 역할을 수행한다. (그림 14)는 AMT 시스템을 이용한 측정과정을 기술하고 있다.




(그림 14) AMT 시스템 구조

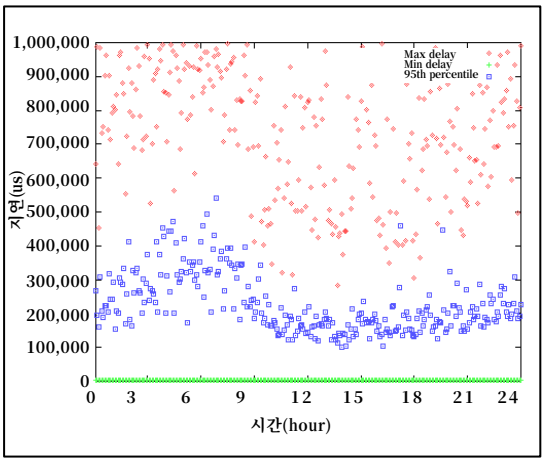
라. AMT Visualizer

(그림 15)는 AMT Visualizer(AMTV)를 보여준다. AMTV는 다음의 입력을 받는다; (a) 송신자 IP 주소,(b) 수신자 IP 주소, (c) 날짜. 세 개의 입력이 의미하는 것은 다음과 같다. 주어진 날짜에 송신자 IP

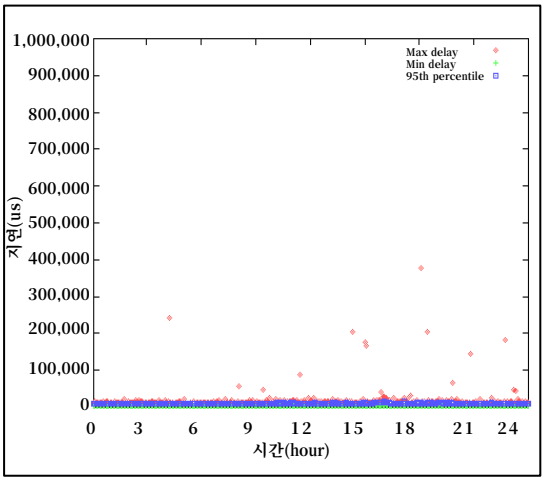



(그림 15) AMT Visualizer(AMTV)

주소를 갖는 측정시스템이 수신자 IP를 갖는 측정시스템에 측정패킷을 보내어 측정된 결과를 얻기를 원한다. (그림 16)과 (그림 17)은 AMTV를 통해 쿼리를 입력하여 얻은 결과를 나타내고 있다. 그 쿼리는 2000년 11월 26일 하루동안 IP 주소 147.46.14.69를 갖고 있는 호스트(MS1)와 IP 주소 203.232.127.20을 갖는 호스트(MS2) 사이에서 측정된 단방향 지연을 요구하는 것이다. (그림 16)은 MS1에서 MS2로의 단방향 지연을 나타내고, (그림 17)은 MS2에서 MS1으로의 단방향 지연을 나타낸다. 두 그림에서 볼 수 있듯이 하루동안에 측정된 단방향 지연의 패




(그림 16) MS1에서 MS2로의 단방향 지연




(그림 17) MS2에서 MS1으로의 단방향 지연

턴이 다름을 알 수 있다.

이 결과로 인터넷 경로의 비대칭적인 성향을 알 수 있다[12]. 즉 두 종단 호스트가 패킷을 주고 받을 때, 한 호스트가 보낸 패킷과 다른 호스트가 보낸 패킷이 방향만 다르고 경로는 같은 네트워크를 통과할 때도 단방향 지연시간과 단방향 손실률이 다를 수 있다는 것이다. (그림 16)과 (그림 17)의 측정결과도 방향에 따른 단방향 지연 시간의 다름을 제시하고 있다.

이와 같이 단방향 측정결과의 분석을 통해 얻은 정보를 네트워크 서비스에 이용할 수 있다. 참고로 Ping 같은 RTT를 측정하는 도구로써는 위의 측정결과를 이끌어 낼 수 없다. 따라서, 능동적 측정은 대부분 단방향 측정도구를 통해 이루어지고 있다.

## VI. 결 론

본 고에서는 인터넷 트래픽을 측정하고 분석하기 위한 방법과 현재 구현되어 있는 시스템을 소개하였다. 인터넷 트래픽 측정을 하는 방법은 크게 두 가지로 나누어진다. 하나는 수동적 측정으로 네트워크상의 트래픽의 종류와 양을 파악하여 그 네트워크 트래픽의 특성을 파악하는 것이다. 다른 하나는 능동적 측정으로 측정 패킷을 측정하고자 하는 네트워크에 투입하여 그 패킷이 서비스되는 것을 관찰하여 네트워크의 상태를 파악하는 것이다.

수동적 측정은 인터넷 서비스를 제공하는 ISP에서 사용자의 과금을 책정할 때 이용될 수 있다. ISP의 과금 정책은 허용 대역에 따라 사용료를 책정하고 있지만, 사용 트랙픽의 종류와 양을 파악하면 실제 네트워크 이용률을 계산해서 보다 공평한 과금을 책정할 수 있다. 그밖에도 Web hosting, Billing, Network planning, Network monitoring 그리고 Data warehousing/mining 등에 사용될 수 있다. 대표적인 수동적 측정 도구로는 Cisco의 NetFlow를 이용하여 수동적 측정을 하는 Cflowd와 측정된 결과를 가공하는 그래프 이미지로 출력하는 FlowScan과 CINERA 등이 있다.

능동적인 측정은 장기간 네트워크를 관찰하여 얻은 측정 결과를 통해 병목 현상이 발생한 경로를 찾아서 라우팅 테이블의 변경, 라우터의 성능 개선, 자원의 재배치 그리고 링크 용량 증대 등을 통해 네트워크 전체 성능의 향상을 기할 수 있다. 대표적인 능동적 측정 도구로는 인터넷 토폴리지와 성능을 분석하는 Skitter와 단방향 측정을 위해 GPS 위성을 이용하는 Surveyor, RIPE 그리고 AMT 등이 있다.

따라서, 수동적인 측정과 능동적인 측정은 네트워크 트래픽의 파악과 분석에 필수적인 역할을 한다. ISP나 네트워크 관리자 등이 두 측정을 적절히 이용

한다면, 네트워크 트래픽과 네트워크 상태를 잘 파악하여 효율적인 네트워크 관리를 할 수 있을 뿐만 아니라, 네트워크 플래닝과 같은 네트워크 확장에 좋은 지침서로 얻을 수 있다. 참고로 현재의 측정시스템은 IPv4 인터넷을 위해 구현되어 있으나, 차세대인터넷 프로토콜인 IPv6를 위한 측정시스템으로 업그레이드 되고 있다. 네트워크를 진단할 수 있는 측정시스템은 차세대인터넷의 VoD나 인터넷 방송과 같은 높은 대역의 멀티미디어 서비스와 지연에 민감한 인터넷 텔레포니 같은 응용을 개발하는 데 필수적인 도구가 될 것이다. 이러한 측정시스템의 개발과 적용에 적극적으로 참여한다면, 차세대인터넷 기술 개발에 선도적인 역할을 할 수 있을 것이다.

## 참고문헌


[1] 옥도민, "플로우 분류기를 이용한 인터넷 트래픽 측정 및 특성 분석," 서울대학교 컴퓨터공학 석사논문, 2000. 2.

[2] 정재훈, "단방향 IP 성능 측정 도구의 설계 및 구현," 서울대학교 컴퓨터공학 석사논문, 2001. 2.

[3] IETF IPPM(IP Performance Metrics) WG, http://www.ietf.org/html.charters/ippm-charter.html

[4] Tony McGregor, "The NLANR Network Analysis Infrastructure," *IEEE Comm. Magazine*, May 2000.

[5] R. Jain and S.A. Routhier, "Packet Trains – Measurements and a New Model for Computer Network Traffic," *IEEE JSAC*, Sep. 1986.

[6] NetFlow, http://www.cisco.com/warp/public/cc/pd/iosw/ioft/neflct/tech/napps_wp.htm

[7] Cflowd, http://www.caida.org/tools/measurement/cflowd/

[8] arts++Library, http://www.caida.org/tools/utilities/arts/

[9] FlowScan, http://www.caida.org/tools/utilities/flowscan/

[10] Flow collection engine, http://net.doit.wisc.edu/~plonka/cflowd/

[11] Visualization tool(RRDtool), http://www.caida.org/tools/utilities/rrdtool/

[12] V. Paxson, "End-to-End Internet Packet Dynamics," *IEEE/ACM Transactions on Networking*, Vol. 7, No. 3, June 1999, pp. 277 - 292.

[13] V. Paxson, "Framework for IP Performance Metrics," RFC 2330, May 1998.

[14] G. Almes *et al.*, "A One-way Delay Metric for IPPM," RFC 2679, Sep. 1999.

[15] C. Demichelis and P. Chimento, "Instantaneous Packet Delay Variation Metric for IPPM," Internet-Draft, Oct. 1999.

[16] R. Koodli and R. Ravikanth, "One-way Loss Pattern Sample Metrics," Internet-Draft, July 2000.

[17] Tony McGregor *et al.*, "The NLANR Network Analysis Infrastructure," *IEEE Communications Magazine*, May 2000.

[18] Skitter, http://www.caida.org/tools/measurement/skitter/

[19] Surveyor, http://www.advanced.org/surveyor/

[20] Sunil Kalidindi *et al.*, "Surveyor: An Infrastructure for Internet Performance Measurements," *presented at INET'99*, San Jose, June 1999.

[21] Sunil Kalidindi, "OWDP: A Protocol to Measure One-Way Delay and Packet Loss," *Surveyor Technical Report 001*.

[22] Sunil Kalidindi, "OWDP Implementation, v1.0," *Surveyor Technical Report 002*.

[23] Henk Uijterwaal and Olaf Kolkman, "Internet Delay Measurements Using Test Traffic," RIPE NCC, June 2, 1997.

[24] AMT, http://mmlab.snu.ac.kr/~traffic/

[25] Motorola Oncore GPS Receiver, http://www.motorola.com/ies/GPS/products/

[26] NTP, http://www.eecis.udel.edu/~ntp/

[27] D.L. Mills, "Network Time Protocol(Version 3), Specification, Implementation and Analysis," RFC 1305, Mar. 1992.

[28] Richard Stevens, "TCP/IP Illustrated, Volume 2: Implementation," Addison Wesley.