초고속연구망에서의 성능 관리

글 _ 이원혁 | 초고속연구망사업실 연구원 | livezone@kisti.re.kr

초고속연구망 운영센터는 기업기관의 사용자들에게 R&D목적의 원활한 네트워크 사용을 지원하기 위하여 이용 트래픽에 대한 성능 관리를 수행하고 있다.

이를 지원하기 위하여 KREONET은 백본을 구성하는 11개 지역, 12개 지역망센터에 설치되어 있는 네트워크 장비들에 대한 물리적인 관리와 백본의 각 구간별 트래픽, 성능에 대한 모니터링을 수행하여 사용자들의 연구목적에 맞는 네트워크 성능을 유지하고 있다. 다음 〈표 1〉은 네트워크 운영자와 사용자의 네트워크 사용에 있어서 주요 관심 분야이다.

〈표 1〉 네트워크 운영자와 사용자의 주요 관심분야

네트워크 운영자	네트워크 사용자
▷ Network Reliability	▷ Network Bandwidth
▷ Network Utilization	▷ Network Performance
▷ Network Capacity	▷ SLA

따라서 사용자에게 안정적이고 고품질의 서비스를 제공하기 위하여 사용현황을 꾸준히 모니터링하고 성능을 관리하여 네트워크 신뢰도를 높이기 위한 노력이 필요하다. 또한 이를 바탕으로 네트워크 자체의 신뢰성과 사용량을 꾸준히 분석하여 네트워크의 이상 유무를 검사하고 트래픽의 특성에 대한 분석을 수행해야 한다.

지속적인 분석결과를 바탕으로 네트워크 자원 사용의 적절성을 유지하며, 사용자에게는 네트워크 사용현황과 성능정보를 제공하고 운영자는 네트워크 용량과 전체적인 topology의 구성을 위한 기초 자료로 사용할 수 있다.

사용자들에게 안정적인 서비스를 제공하기 위하여 기본적으로 네트워크 상에 유출입되는 트래픽에 대한 모니터링과 분석을 수행해야 한다. 트래픽은 데이터의 흐름이다. 이것은 마치 강물이 흘러가듯이 강의 폭은 변하지 않는데, 태풍이나 홍수와 같은 주위 환경에 의해 변화되는 물살로 비유할 수 있다. 이와 같이 네트워크의 대역폭은 일정한데 사용자에 의한 트래픽의 양은 기본적으로 변화하며, 특히 웜이나 DDoS와 같은 비정상 트래픽으로 인하여 트래픽의 변화량이 매우 큰 폭으로 변화하기도 한다. 네트워크 성능을 일정하게 유지하기 위해서는 이러한 트래픽의 변화량을 모니터링하고 특성을 분석해야 하기 때문에 상당히 어려운 작업이며, 중요한 작업이다.

과거 네트워크 관리에 대한 인식은 대부분 IP주소를 설정하고, 장비를 configuration하는 등의 구성관리와

네트워크를 감시하고 통제하는 장애관리에 많은 비중을 두었다. 초고속연구망에서는 구성, 장애, 성능에 대한 관리를 모두 정적(static)인 부분에만 초점을 맞추고 있었던 관점에서 벗어나 능동적인 트래픽 측정을 이용하여, 현재 네트워크의 성능을 측정하고 수동적인 측정을 이용하여 네트워크 상에 유·출입되는 트래픽의 양적인 모니터링과 함께 세부 특성까지도 파악하여 정상적인 트래픽의 사용 패턴 분석은 물론 웜과 DDoS와 같은 유해 트래픽까지의 관리를 수행하고 있다.

네트워크 트래픽 측정 및 분석을 위한 방법은 크게 다음과 같이 능동적 측정방법(Active Measurement)과 수동적 측정방법(Passive Measurement)이 사용되고 있다. 다음은 초고속연구망에서 수행하고 있는 트래픽 측정 및 분석을 위한 툴과 시스템들에 대해서 소개한다.

1. 능동적 트래픽 측정방법 (Active Measurement)

능동적 측정방법은 네트워크 내에 인위적인 트래픽을 발생시켜 성능을 측정하는 방법이다. 이때 측정을 위한 데이터 전송 및 측정방법 선택이 중요한 요인이 되는데, IETF IPPM WG(Internet Engineering Task Force IP Performance Metrics Working Group)의 측정인자들을 위주로 연구가 수행중이며, 현재 초고속연구망에서는 미국 NLANR(The National Laboratory for Applied Network Research)의 'Measurement and Network Analysis Group'에서 고성능 네트워크 상에서의 성능측정 프로젝트로 연구·개발한 AMP(Active Measurement Project)를 도입하여 성능측정 중에 있다.

1) AMP (Active Measurement Project)

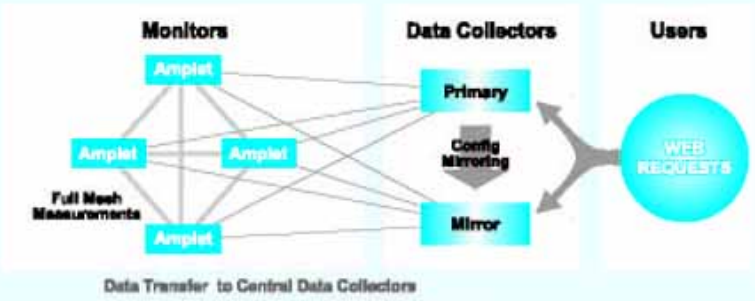
■ 소개

NLANR/MOAT에서 개발된 Active Measurement Infrastructure를 의미함

북미 vBNS, Abilene, STAR TAP에 연동된 연구소 및 대학교 간의 네트워크 성능 측정에 사용되고 있음

국제적으로 120여개 사이트에 AMP 모니터가 설치되어 있으며, 국내에는 초고속연구망가입기관을 중심으로 지역망센터 및 R&D연구 기관을 중심으로 설치

측정방법(1분에 한번씩 RTT(Round Trip Time)를 측정), 정보저장(각 AMPlet들이 AMP 서버로 이 정보를 전송하고, 서버는 데이터를 저장함)



〈그림 1〉 AMP 동작 구성도

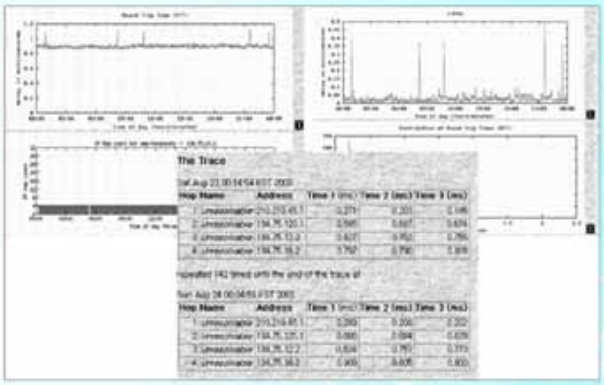
■ 특성

사용자간 또는 사용자와 슈퍼컴퓨터 간의 네트워크 성능을 측정함

Round Trip Time, Packet Loss, Traceroute를 성능 측정인자로 사용함

장시간 또는 시간별 그래프가 자동으로 생성됨

슈퍼컴퓨터 사용자 및 KREONET 사용자의 네트워크 성능을 측정함



〈그림 2〉 AMP를 이용한 성능 측정 화면

■ 성능 측정대상

- 고성능 슈퍼컴퓨팅 자원을 활용하는 이용자(포항공대 외 4개 기관)
- 국가 그리드 응용 연구개발자(서울시립대 외 4개 기관)
- 지역망센터(한국전산원 외 5개 기관)
- 초고속과학기술연구망(SuperSIReN)

■ 성능 측정 인자

- RTT(Round Trip Time), Packet Loss, Topology

■ 제공 URL 및 인터페이스

- http://amp.kreonet2.net을 통하여 국내 사용자간 성능 측정결과 조회
- http://watt.nlanr.net/active/amp-korea/international/body.html을 통하여 국제간 AMPlet노드와 성능 측정결과 조회

2. 수동적 트래픽 측정 방법 (Passive Measurement)

수동적 트래픽 측정방법은 네트워크 내의 스위치/라우터를 경유하는 트래픽을 수집·분석하여 네트워크 트래픽을 실시간으로 보여주고, 측정된 데이터를 저장하여 오프라인으로 다양한 분석도구를 이용하여 분석하는 방법이다. 이 방식의 특징은 인위적인 트래픽을 유발하지 않고 트래픽을 모니터링하거나 캡쳐하여 실제 사용되고 있는 트래픽을 분석한다는 것이다. 초고속연구망에서는 라우터/스위치의 netflow 정보를 이용하여 트래픽을 flow단위로 분석하는 FlowScan+, SNMP(Simple Network Management Protocol)를 이용하는 SysMon, Visual-Netmon, MRTG, NetMax를 구축 운영중이다.

1) FlowScan+

■ 특성

- 네트워크 트래픽의 flow 레포팅, visualization tool
- CAIDA에 의해 개발된 FlowScan을 KISTI와 KAIST의 협업연구로 업그레이드
- 라우터/스위치에서 제공되는 netflow 정보이용
- Component : flow 수집 엔진(cflowd의 패치판)

: 고성능 DB(RRD-Round Robin Database)

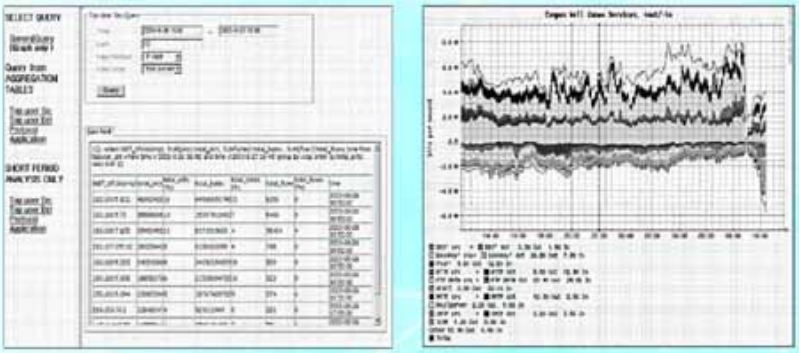
: visualization tool(RRDTool)

■ 성능 측정대상

- 국제 R&D 연구망 (StarTAP)을 중심으로 트래픽 특성 분석

■ 제공 URL 및 인터페이스

- http://flowscan.kreonet2.net을 통하여 트래픽 특성 실시간 모니터링 가능

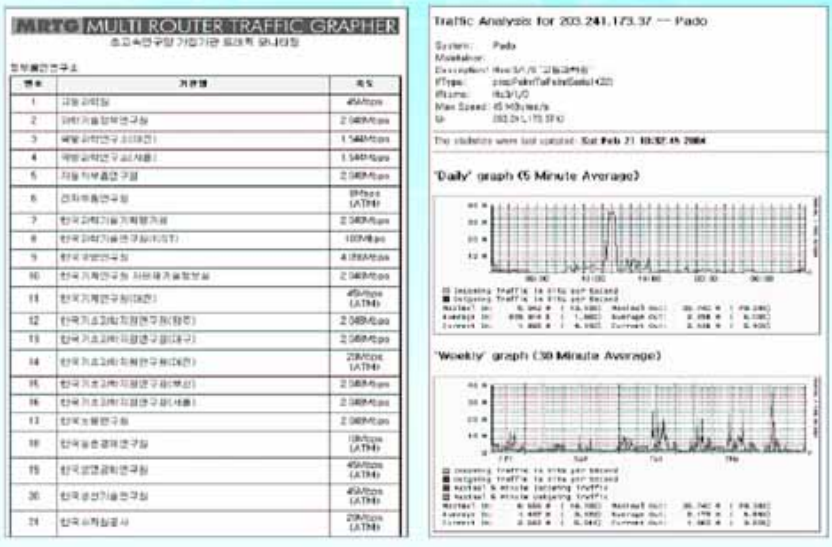


〈그림 3〉 FlowScan+을 이용한 트래픽 특성 분석

2) MRTG(Multi Router Traffic Grapher)

■ 특성

- 네트워크 링크상에서의 Traffic Load를 모니터링하는 툴
- SNMP를 이용하여 라우터/스위치로부터 트래픽 정보 수집
- PNG이미지화일을 포함하는 HTML 페이지를 생성
- UNIX, WindowsNT 상에서 동작하며 Perl과 C로 작성



〈그림 4〉 MRTG를 이용한 각 기관별 트래픽 현황 분석

■ 성능 측정대상
- 해외망 연동 Link(R&D를 위한 StarTAP과 일반 인터넷 사용자를 위한 Link)
- 타 ISP와 연동하는 IX구간(KIX, KT IX, Dacom IX 등 5개 IX구간)
- 회원기관(교육 및 연구기관, 학회 등 초고속연구망 사용 171개 기관)
- 지역망센터(전국 11개지역, 12개 지역망센터의 백본)

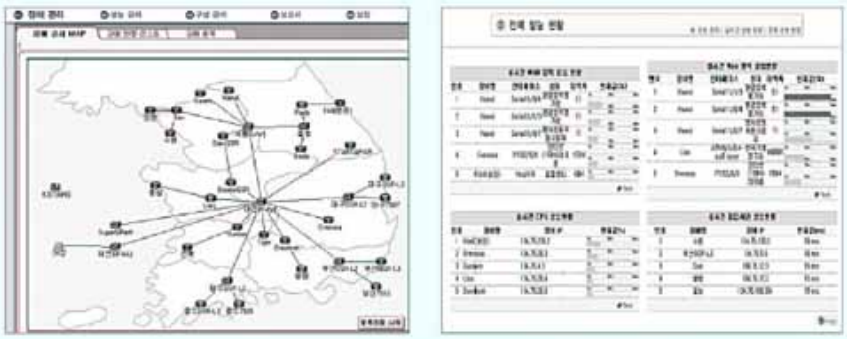
■ 제공 URL 및 인터페이스
- http://www.kreonet.net/noc/mt.html을 통하여 모든 측정기관의 트래픽 정보조회

3) 백본 성능 및 장애관리 시스템 (NetMax)

■ 특성
- 초고속연구망 백본의 성능 및 장애 관리를 위한 네트워크 관리 시스템
- SNMP를 이용하여 백본 장비별 인터페이스 트래픽 현황을 실시간적으로 탐지
- 주요 백본 네트워크를 중심으로 SubMap을 활용하여 Map Touring 수행
- 장애 발생시 SMS 발송, 맵으로 시스템에 대한 실시간 상황파악
- 구성 장비들에 대한 성능 분석 및 장애요인 분석 수행

■ 성능 측정대상
- 초고속연구망 백본 네트워크 중심의 장애 및 성능 관리

■ 제공 URL 및 인터페이스
- http://150.183.95.27:1004을 통하여 인증된 관리자만이 백본 현황을 모니터링



〈그림 5〉 NetMax를 이용한 초고속연구망 백본장비 성능 분석

4) SysMon(System Monitoring tool)

■ 특성
- 비정상적인 트래픽 감지를 위하여 시스템 자원(CPU, Memory)의 이용 상태를 실시간 모니터링
- SNMP를 이용한 스위치 장비 트래픽 분석

- 급격한 패킷의 증가로 인한 트래픽 탐지로 웜바이러스의 사전 탐지 가능

■ 성능 측정대상

- 원내 네트워크의 스위칭 장비를 중점으로 모니터링

■ 제공 인터페이스

- 현재 자체 구축 Ver. 1로서 웹이 아닌 운영자에 의한 Application 조회 가능

〈그림 6〉 SysMon을 이용한 원내 통신망 자원 분석현황 분석

5) Visual-NetMon(Visual-Network Monitoring tool)

■ 특성

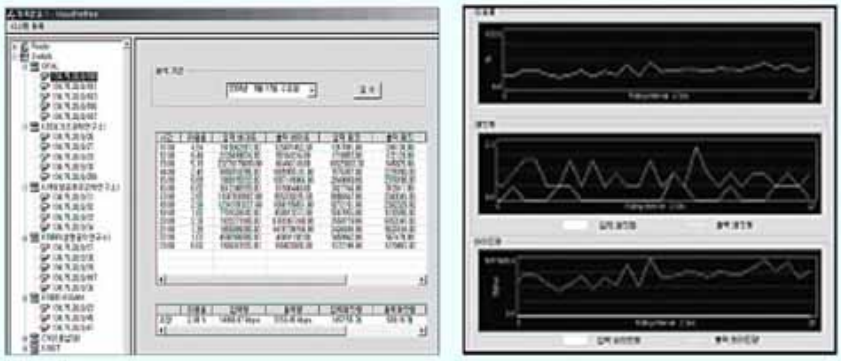
- 네트워크 중심의 트래픽 이용현황 분석 및 모니터링
- SNMP를 이용한 라우터/스위치 장비 트래픽 분석
- 원내 및 주요 백본 구간 네트워크 장비의 지속적 분석으로 baseline 초과시 대책을 위한 기본 자료로 활용

■ 성능 측정대상

- 원내 네트워크 라우터/스위치 및 프로젝트 중심의 백본 네트워크 장비

■ 제공 인터페이스

- 현재 자체 구축 Ver. 1로서 웹이 아닌 운영자에 의한 Application 조회 가능



〈그림 7〉 Visual-NetMon을 이용한 네트워크 중심의 트래픽 현황 분석