2001 년 한국정보처리학회 추계 학술발표논문집 제 8 권 제 2 호

KREONET 에서의 네트워크 분석 인프라 구축 연구

김국한*, 이만희*, 곽재승*, 변옥환*, 진용옥**
* 한국과학기술정보연구원 초고속연구망부
** 경희대학교 정보통신대학원
e-mail : ghkim@kisti.re.kr

Network Analysis Infrastructure for KREONET

Kook-Han Kim*, Man-Hee Lee*, Jai-Seung Kwak*,
Ok-Hwan Byeon*, Yong-Ohk Chin**

* Div. of High Performance Networking Korea Institute of Science & Technology Information (KISTI)
** Kyung Hee Graduate School of Information & Communication

요 약

네트워크에 흐르는 트래픽 측정을 효율적으로 함으로서 트래픽의 종류와 양을 알 수 있고, 이를 기반으로 측정 네트워크의 트래픽 특성과 상태를 파악할 수 있다. 본 고에서는 초고속 연구망 환경에 적합한 네트워크 분석 인프라(NAI) 구축을 제시한다. NAI 구성은 네트워크 링크를 모니터링하는 수동적 측정 방법 MRTG 와 NAVI, 그리고 인위적으로 트래픽을 발생시켜 그 결과를 분석하는 능동적 측정 밥벙 PingER 와 AMP 두 가지 종류로 나뉜다. 현재 초고속 연구망에서 적용중인 네트워크 트래픽 분석 측정 도구 하나씩 알아보고, 국내\외로 링크된 네트워크 트래픽의 특성과 상태를 균형적으로 분석 할 도구에 대한 모델을 알아본다.

1. 서론

인터넷 사용인구의 급증에 따른 트래픽 사용량의 발생이 증가하고 있으며, 효율적인 인터넷 이용을 위해서는 트래픽 측정과 분석이 필요하다. 인터넷 트래픽에 관한 정확한 측정은 트래픽 특성과 상태를 파악하는데 큰 도움이 된다.

초고속연구망[1]은 대부분 대학, 기관, 연구소가 사용자 그룹을 이루고 있고 슈퍼컴퓨팅 연구환경을 제공하기위한 고성능 네트워크를 지향하고있다. 따라서 기존의 인터넷 트래픽과는 다른 성격의 트래픽을 발생시킨다는 점을 고려해야 하고, 이런 사용자들에게 이용환경의 최적화와 네트워크 기술지원 등을 보장하기 위해서는 효율적인 트래픽 분석 인프라가 구축되어야 한다.

본 고는 한국과학기술정보연구원 초고속연구망부 개발실(이하 개발실)에서 구축 중인 네트워크 분석 인프라 (NAI : Network Analysis Infrastructure)를 제시하고, 초고속 연구망 환경에서 적합한 네트워크 트래픽 분석 도구의 모델을 제시한다.

트래픽 측정방법에는 트래픽 특성을 파악하는 수동적인 측정 (Passive Measurement: PM)법과 트래픽 상태를 파악하는 능동적인 측정(Active Measurement: AM) 법이 있다. PM 법은 네트워크 노드사이의 링크에 분리기 (splitter)를 연결하여 모니터링함으로써, 두 네트워크 노드 사이를 통과하는 트래픽 종류와 양을 파악할 수 있고, AM 법은 종단 호스트들간에 임의로 트래픽을 발생시켜 네트워크 내에서 전송이 어떻게 이루어지는지를 파악하여 네트워크 상태를 진단한다[5]. 일반적으로 사용되는 PM 법으로는 Tcpdump, Coral Reef, NetFlow, Cflowd, Flowscan, MRTG 등이 있고, AM 법은 PingER, Skitter, Surveyor, ping, AMT, AMP 등이 있다.

연구전산망에서 구축중인 NAI 의 PM 측정법으로 는 MTRG (Multi Router Traffic Grapher) 와 NAVI[2] Project (Network traffic monitoring, Analysis & Visualization)가 있다. AM 측정법으로는 PingER (Ping End-to-end Reporting)와, AMP (Active Measurement Project)를 사용한다.

본 고의 구성은 다음과 같다. 2 장에서 NAI 모델을 살펴보고, 개발실에서 사용중인 측정도구 MRTG, NAVI, PingER, AMP 를 3 ~ 6 장에서 소개하고, 마지막 7 장에서 결론과 앞으로의 방향을 제시한다.

2. NAI

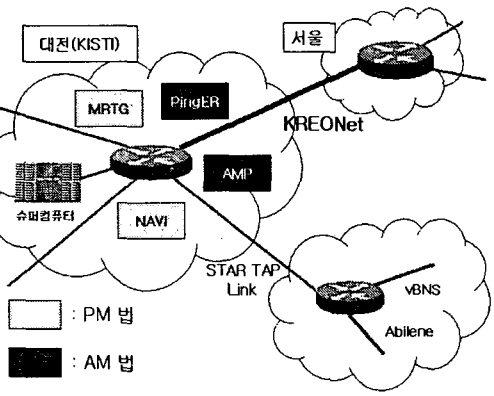
개발실에서 사용중인 기존의 네트워크 트래픽 분석 도구는 일반적인 인터넷 트래픽 분석으로 개략적인 네트워크 상태와

[1] 초고속연구망(KREONet : Korea Research Environment Open Network)은 국가 기간전산망의 하나로서 300 여 국내 정부 정부출연 연구소, 대학 및 산업체 연구인력 에게 첨단 과학기술 인프라를 제공한다.

[2] 카이스트 전길남 교수 System Architecture lab.과 공동으로 개발실 과제로 진행중인 프로젝트이다.

특성을 보여주고 있다. 따라서 초고속 연구망 환경에 적합하게 기관별, 응용별, 국가별[3] 등의 내용을 분석하여 장기간(long-term), 실시간(real-time), 쉽고 편한(easy-to-ues) 그리고 웹 기반으로 보여주는 네트워크 트래픽 분석 인프라의 모델이 필요하다 [4].

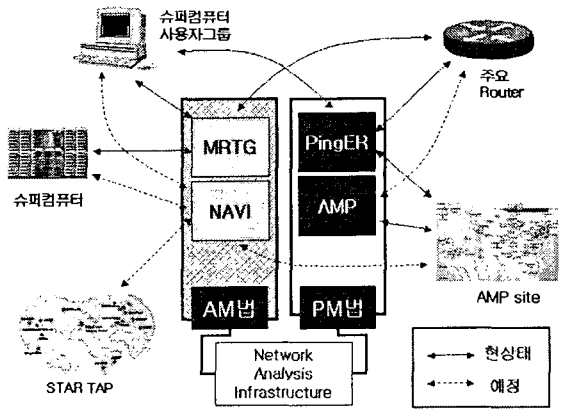
[그림 1]은 현재 초고속 연구망의 연동상태를 간략하게 나타낸 것이다.



[그림 1] 초고속연구망 링크 개략도

우선 NAI 를 살펴보기 위해서 연구중인 트래픽 측정 도구들의 적용 범위를 알아보겠다. 우선 PM 법인 MRTG 는 슈퍼컴퓨터 입\출력 되는 트래픽을 인터페이스별로 나타내고, NAVI 는 STAR TAP 링크에 흐르는 트래픽을 측정하고 분석할 예정이다. AM 법인 PingER 는 초고속연구망 사용자 그룹과 링크를 KISTI 간 RTT(Round Trip Time), Packet loss 를 구하며 AMP 는 130 여개 미국내 주요 대학, 연구소 등과 Full Mesh 형태로 이루어져 ping, traceroute 결과를 분석하고있다.

이와 같이 개발 예정인 NAVI 와 적용중인 PM, AM 법으로 국내\외 네트워크의 상태와 특성을 분석할 수 있는 NAI 를 구성할 수 있다.



[그림 2] 초고속연구망에서의 NAI Architecture (안)

[그림 2]는 제시된 NAI 가 어떤 트래픽을 목적으로 모니터링 하고 있는지, 앞으로 어떤 트래픽을 어떤 측정도구로 분석을 할 것인지 나타내서 보여준다. 그림과 같이 개발 예정인 NAVI 시스템은 일차적으로는 STAR TAP 링크 트래픽을 분석하지만 장기적으로는 초고속연구망에 도입될 AMP 시스템과 함께 국내외 네트워크 트래픽 분석 도구로서 중요한 역할을 하게 된다.

모니터링을 통해서 수집되어진 내용들은 Server 에서 분석되며, 웹을 통해 원하는 DB(Data Base)나 Query 를 기반으로 원하는 정보를 얻기에 용이하고, 분석되어 얻어진 정보를 기반으로 네트워크의 특성과 상태가 파악이 되면 차후의 발전된 NAI 구축에 중요한 자료가 된다.

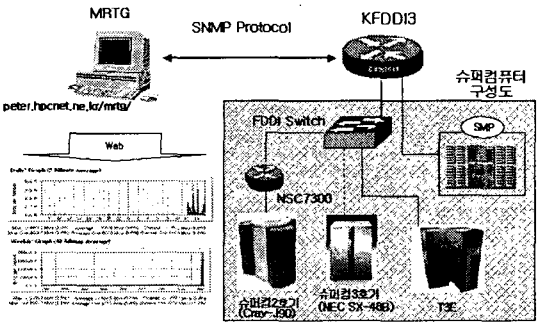
3. MRTG

MRTG 는 현 네트워크 상태에서 인터페이스별로 사용률을 HTML(Hyper Text Makeup Language)을 이용하여 사용자가 보기 쉽게 모니터에 나타내 준다. 대부분의 UNIX 와 Windows NT 에서 작동하며, SNMP(Simple Network Management Protocol)를 이용하는 펄 스크립트와 프로그래밍 C 언어를 사용하여 트래픽 데이터를 수집하고 이를 그래픽으로 나태내어 분석이 용이하게 하도록 구성되어 있다[1].

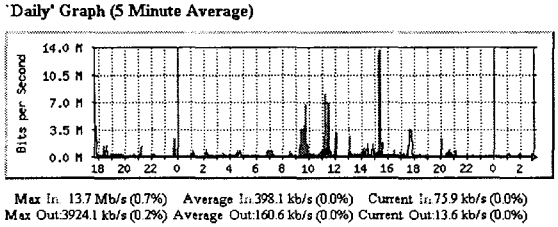
웹사이트나 시스템을 구축한 후, 네트워크 내외부로 전송되는 트래픽 통계를 그래픽 형식으로 용이하게 나타내고자 할 경우에 MRTG 가 적합하다. 통계 그래프는 일간, 주간, 월간, 연간으로 구분하여 보여준다.

개발실에서는 MRTG 를 이용하여 슈퍼컴퓨터 트래픽과 연구원 내부 트래픽을 측정하는데 적용한다. 측정된 결과는 슈퍼컴퓨터 트래픽 측정 홈페이지에서 확인할 수 있다[2].

슈퍼 컴퓨터(CRAYC90, CRAYT3E, CRAYJ90, SMP) 의 인터넷 traffic 측정환경



[그림 3] 슈퍼컴퓨터 MRTG 측정환경



[그림 4] 슈퍼컴퓨터 트래픽을 측정한 일간 MRTG 그래프

[그림 3]은 슈퍼컴퓨터 트래픽 측정환경으로 입\출력되는 슈퍼컴퓨터 트래픽이 모두 모이는 라우터에서 MRTG 를 실행하고 있음을 보여주고 있다. [그림 4]는 2001-09-04 일 슈퍼 컴퓨터 MRTG 그래프로 하루 중 최고 16 시경에 14Mb/s 의 트래픽 이 흘렀음을 보기 쉽게 알 수 있도록 나타낸다

4. NAVI

초고속연구망은 대학, 정부출연기관, 연구소 등이 대부분의 사용자 그룹을 이루고 있다. 사용중인 측정 도구들은 기존의 인터넷 트래픽을 측정하여 네트워크 상태와 특징을 알 수 있는데 유용한 방법들이다. 따라서 보다 더욱 초고속연구망 환경에

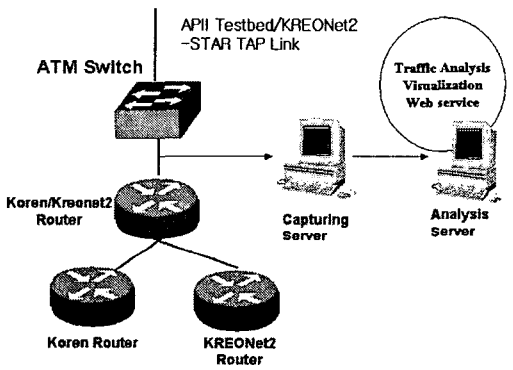
[3] KREONET- STAR TAP(미국 차세대 과학기술 연구망)링크가 5 월부터 45Mbps 로 연동되어지고 본 기관은 네트워크 운영센터의 기능을 한다.

적합한 측정도구 개발이 필요하다. 그 해결책으로 기존의 측정 도구를 비교 분석하는 단계를 거쳐 NAVI 라는 PM 법 측정 도구를 개발 진행 중이며, 개발되는 측정도구는 일차적으로 STAR TAP 링크를 분석하는 목표를 가진다.

NAVI 는 우리 네트워크에 필요한 특성을 가지고 개발되어지므로 본 고에서 제시되어지는 초고속연구망에서의 NAI 구축하는데 있어 중요한 의미를 지닌다. 또, 우리가 직접 초고속연구망에 유용한 네트워크 트래픽 분석 도구를 개발한다는데 있어 그 의미가 새롭다 할 수 있다.

NAVI 의 특성은 우선 STAR TAP 링크에서 네트워크 트래픽 모니터링이 목적이므로 국가별, 기관별, 응용별로 세분하여 정확한 트래픽 특성을 분석해야 하며, 장기(long-term), 실시간(real-time) 그리고 웹 기반의 트래픽 측정 분석 용이한 도구의 개발이 필요하다.

[그림 5]는 개발도구의 예상 구축 환경이다. AMT 스위치를 거쳐 STAR TAP 으로 나가는 트래픽을 모니터링하여 서버에서 분석하는 것을 보여준다.



[그림 5] 초고속연구망과 STAR TAP 링크에서
NAVI 구축 예정 환경

개발도구의 기대효과는 다음과 같다[3].

1) 기술적인 측면
- 네트워크 트래픽 측정, 성능분석, 가시화에 관한 통합 적인 모델 제시와 기술 보유
- 효율적인 망 관리를 위한 기반 기술과 시스템 구축, 확보
- 차세대 인터넷에서의 다양한 응용서비스 트래픽 패턴분석을 통한 향후 네트워크 인프라에 필요 요구조건 도출

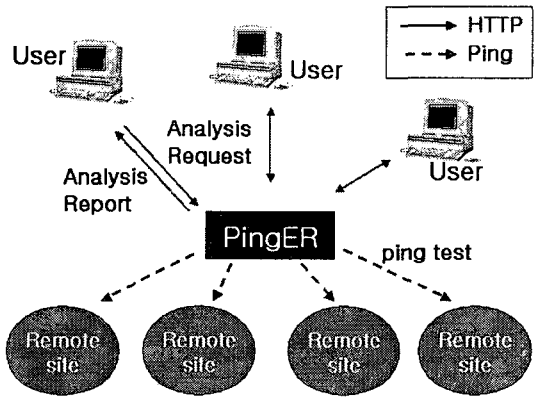
2) 경제 산업적인 측면
- 인터넷 망 설계와 구축, 업그레이드에 대한 투자비용 계획을 위한 근거자료 제공
- 현 시점에서 개념정립 단계인 네트워크 트래픽 측정, 성능분석, 가시화에 관한 기술 보유

5. PingER

PingER 는 Ping 을 이용하여 말단간의 호스트의 트래픽 상태를 측정하는 도구이며, SLAC(The Stanford Linear Accelerator Center)의 IEPM(The Internet End-to-end Performance Monitoring) 그룹이 개발했다[10]. PingER 는 한 사이트에서 여러 사이트로 주기적으로 ping 테스트 한 결과를 수집하고, 각종 Perl CGI 프로그램을 제공하여 트래픽 분석 데이터와 그래프 작성을 용이하게 한다. 즉 인위적으로 트래픽을 발생시켜 그 결과를 분석하는 AM 법 중의 하나이다.

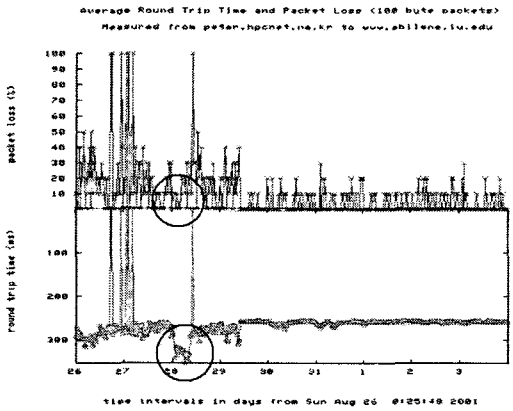
다음은 PingER 모니터 구조의 3 가지 구성 요소이다[9].

1) Remote monitoring sites : 간단하게 말단 호스트 상태를 알려준다.
2) Monitoring sites : 각각의 호스트에 PingER 가 설치되야 하고, 수집되어진 Ping 정보는 웹서버를 통해 제공될 수 있도록 유용하게 만들어져야 하며, 수집된 정보의 Short Term 분석과 결과를 local cache 에 저장하고 제공해야 한다.
3) Archive and analysis sites : 적어도 하나 이상의 서버가 Archive 와 analysis 로 운영되어져야 한다. Archive 는 HTTP(Hypertext Transfer Protocol)를 이용하여 규칙적으로 Monitoring site 으로부터 정보를 수집하여 Analysis site 로 보내면 여기에서 분석하여 웹 형식으로 결과를 볼 수 있다.



[그림 6] 초고속연구망에서의 PingER Architecture

위의[그림 6]은 초고속연구망의 물리적인 링크는 대전을 중심으로 성상(star-like)을 이루고있다. 중심에서 하나의 PingER 를 이용하여 멀리 떨어진 링크의 상태를 측정하는데 유용하다 할 수 있다.



[그림 7] PingER 결과 그래프(KREONet-인디아나 대학)[6].

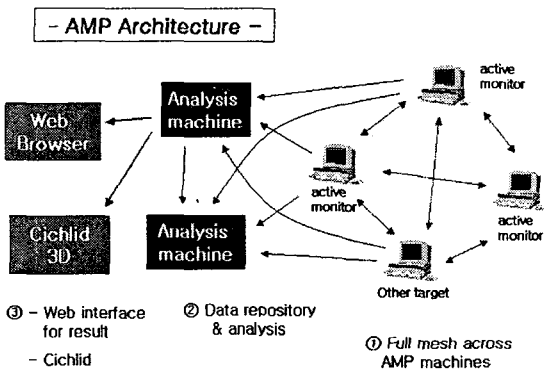
아래 [그림 7]은 인디아나대학(美)과 PingER 측정결과를 나타내는 것인데, 동그라미 부분을 보면 RTT 는 더욱 느려진 반면 패킷 손실률은 오히려 양호하게 나왔음을 알 수 있다. 그리고 PingER 를 사용하여 국내 초고속연구망 사용자들 뿐 아니라 STAR TAP 링크의 기관과도 성능 측정을 할 수 있음을 봤다. 그러나 PingER 는 네트워크 상태에 대한 많은 정보를 제공하지는 않는다. 그래서 AMP 를 도입을 했으며, 두 시스템을 이용해서 더욱 효율적인 성능 측정을 할 수 있다.

6. AMP

AMP 는 NLANR (The National Laboratory for Applied Network Research) 팀에 의해서 연구 개발되는 프로젝트이다. 현재 미국의 주요 대학과 연구소 등 130 여 개의 사이트에 AMP 모니터가 설치되어 있으며, 대부분은 미과학재단(NSF: The National Science Foundation)의 보조를 받는 HPC(High Performance Computer)의 사이트이다[8].

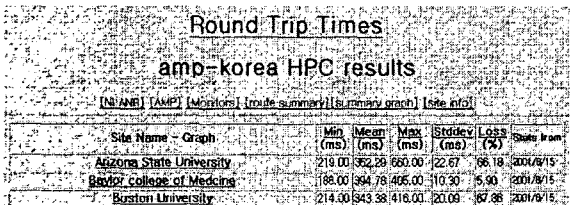
AMP 는 매분 마다 다른 시스템과의 RTT 를 측정하고, 10 분마다 Traceroute 를 수행하여 Ping 의 경로를 측정한다. AMP 에서는 단 방향이 아닌 양방향으로 시간을 측정하는데, 이는 RTT 측정이 130 여 개의 모니터링 사이트 모두를 GPS(Global Position System)로 상호 동시성을 맞추고 측정 해야 하는 어려움이 있는 단 방향 측정보다 용이하기 때문이다. RTT 측정은 ICMP(Internet Control Message Protocol) 패킷을 이용하는 fping 프로그램을 사용한다[11].

현재 개발실은 미국의 NLANAR 로부터 AMP 장비를 제공받아 국내에서는 처음으로 KREONET-STAR TAP 링크간의 트래픽 측정을 위해 설치되어있다.



[그림 8] AMP Architecture

[그림 8]은 AMP 의 측정 구조를 설명 한 것이다. PingER 와 유사한 형태이지만 PingER 에서는 하나의 시스템이 중심에 자리하고 AMP 는 Full-mesh 형태로 각각의 사이트에서 다른 AMP 사이트간의 네트워크 성능을 측정할 수 있다.


Round Trip Times

amp-korea HPC results

[NLANR] [AMP] [Monitors] [route summary] [summary graph] [site info]

Site Name - Graph	Min (ms)	Mean (ms)	Max (ms)	Stddev (ms)	Loss (%)	Starts from
Arizona State University	219.00	352.29	660.00	22.67	66.18	2001/8/15
Baylor college of Medicine	188.00	364.78	406.00	10.30	5.90	2001/8/15
Boston University	214.00	343.38	416.00	20.09	67.36	2001/8/15
CSU - San Bernardino	168.00	276.49	543.00	12.42	64.17	2001/8/15
California Institute of Technology	147.00	363.55	481.00	11.33	7.57	2001/8/15
California State University, Pomona	160.00	269.97	322.00	11.12	64.17	2001/8/15
Canarie CA-net3-ARDNOC	228.00	323.87	359.00	5.61	66.04	2001/8/15
Case Western Reserve University	223.00	327.44	390.00	7.70	66.25	2001/8/15
Clemson University	241.00	334.16	367.00	15.67	10.76	2001/8/15
Colorado State University - AMP	244.00	331.74	339.00	5.63	65.42	2001/8/15
Columbia University	227.00	326.76	333.00	7.62	65.90	2001/8/15
Cornell University	248.00	325.52	328.00	5.77	65.36	2001/8/15

[그림 9] Korea - AMP 사이트(다른 기관들)[7].

[그림 9]는 NLANR 홈페이지에 올려진 내용으로 개발실과 연결된 다른 AMP 사이트를 확인할 수 있고, 이 외에도 각 링크간의 RTT 와 loss 그리고 Ping 이 거치는 Trace 를 확인할 수 있다. 그림 내용은 2001-08-15 이고 보스턴 대학 같은 경우 평균 RTT 가 343.38 (ms) 이며 loss 율은 67.36 으로 나타나고있다. 이와 같은 내용은 그래프로도 나타내므로 STAR TAP 링크상태를 AM 법으로 측정하는데 도움이 된다.

7. 결론

본 고에서는 네트워크 트래픽 분석 방법을 PM 법과 AM 법으로 구분하여 살펴보았고, 초고속연구망 환경에서의 NAI 를 구축하기 위한 내용들을 제시하였다.

NAI 를 구성하는 PM 법인 MRTG 는 각각의 인터페이스별로 슈퍼컴퓨터에 입, 출력되는 트래픽 특성을 쉽게 확인할 수 있었고, 진행중인 NAVI 시스템은 우선 STAR TAP 링크에서 네트워크 트래픽 모니터링이 목적이므로 국가별, 기관별, 응용별로 세분하여 정확한 트래픽 특성을 분석해야 하며, 장기(long-term), 실시간(real-time) 그리고 웹 기반의 트래픽 측정 분석 용이한 도구이다. 그리고 AM 법인 PingER 는 개발실 중심인 물리적인 구조에서 End-to-end 에 주기적인 Ping test 를 통해 네트워크 상태를 확인할 수 있는 도구로 사용 중이고, AMP 는 미국내 130 여 AMP 사이트로 이루어진 R&D 테스트베드 상의 트래픽을 링크간의 Full mesh 로 효율적인 측정 분석할 수 있다.

특히 NAVI 시스템은 초고속연구망에 적합한 트래픽 측정 도구를 개발 운영함으로써 초고속연구망 특성에 맞는 분석과 정보 축적이 가능하며, 사용자 그룹에게 사용환경 최적화와 유용한 정보를 제공할 수 있다. 또한 초고속연부망을 모니터링하는 대표적인 도구를 개발했다는데 의의를 가질 수 있다.

NAI 를 통해서 얻어지는 정보는 분석을 통해서 사용자들과 초고속연구망 링크 특성을 알 수 있고, 이를 기반으로 초고속연구망 환경에 적합한 NAI 구축에 필요한 효율적인 정책 수립이 제시된다.

향후에는 KREONet 의 전반적인 트래픽 성능측정을 위해서 AMP mesh 를 초고속연구망에 도입 할 예정이며, 더 나아가 Application level 에서의 네트워크 성능 파악할 수 있는 도구를 NAI 에 추가함으로써 보다 효율적이고 체계적으로 KREONet 의 성능을 측정할 수 있는 NAI 를 만들 예정이다

8. 참고문헌

[1] 문태준, "MRTG 를 이용한 네트웍 트래픽 모니터링" http://tunelinux.pe.kr/bbs/read.php?table=linuxinfo&no=18

[2] 슈퍼컴퓨터 트래픽 홈페이지, http://peter.hpcnet.ne.kr/mrtg/

[3] 이만희, "고성능 연구망에서의 네트워크 트래픽 측정, 성능 분석 및 데이터 가시화에 관한 연구 위탁연구 제안요청서"

[4] 이만희, "NAVI project & AMP project", 2001.5.21, APAN-KR Measurement W/G Meeting

[5] 정재훈, "인터넷 트래픽 측정 방법과 측정시스템", ETRI 월간지 (전자통신동향분석)

[6] 초고속연구망 PingER 홈페이지, http://peter.hpcnet.ne.kr/

[7] AMP 측정결과 홈페이지, http://watt.nlanr.net/active/

[8] AMP 홈페이지, http://watt.nlanr.net/

[9] Les Cottrell, Warren Matthews, and Connie Logg ,"Tutorial on Internet Monitoring & PingER at SLAC", http://www.slac.stanford.edu/comp/net/wan-mon/tutorial. html

[10] PingER 홈페이지, http://www-iepm.slac.stanford.edu/

[11] Todd Hansen, Jose Otero, Tony McGregor, Hans-Werner Braun, "Active Measurement Data Analysis Techniques", http://moat.nlanr.net/Papers/AMP_case_studies/case_ studies.pdf