DOI: 10.3745/KIPSTC.2008.15-C.2.093

SNMP를 이용한 엔터프라이즈 Network Weather Map 시스템

김 명 섭[†] · 김 성 윤[††] · 박 준 상[†††] · 최 경 준[††]

요 약

네트워크사업자, 인터넷 사업자, 및 엔터프라이즈 네트워크의 트래픽 현황을 파악하기 위한 방법으로 Network Weather Map (NWM)과 대역폭 시간추이 그래프를 많이 사용한다. 이들은 라우터나 스위치장비 내에 동작하는 SNMP 에이전트가 제공하는 MIB정보를 주기적으로 수집하여 DB에 저장하고, 사용자가 언제 어디서나 볼 수 있도록 웹으로 결과를 보여주는 형태로 구축된다. 현재의 엔터프라이즈 네트워크는 multi-Gbps를 지원하는 이더넷 스위치 중심의 트리 토폴로지 형태로 구축되고 있다. 본 논문은 현재의 엔터프라이즈 네트워크에 적합한 SNMP 기반의 Network Weather Map 구축에 있어 고려되어야 할 사항을 점검하고, 이를 바탕으로 엔터프라이즈 Network Weather Map 시스템을 설계하고 구현한 내용을 기술한다. 특히 엔터프라이즈 네트워크와 Core 네트워크의 토폴로지 상의 차이를 고려하여 효율적인 Network Weather Map 디자인을 제시하고, multi-Gbps 고속 링크를 지원하는 현재의 라우터/스위치장비에 SNMP MIB-II 사용의 문제점을 확인하고 이의 해결방안을 제시한다. 또한 SNMP의 사용에 따른 트래픽 발생량, 그리고 네트워크 장비의 부하를 조사함으로써 SNMP의 효율적 사용방법을 제시한다. 본 논문에서는 학교 캠퍼스 네트워크를 대상으로 Network Weather Map 시스템을 구축하였다.

키워드 : Network Weather Map, 시간 추이 그래프, 엔터프라이즈 네트워크, Passive Monitoring, SNMP, MIB

Enterprise Network Weather Map System using SNMP

Myung-Sup Kim[†] · Sung-Yun Kim[††] · Jun-Sang Park[†††] · Kyung-Jun Choi[††]

ABSTRACT

The network weather map and bandwidth time-series graph are popularly used to understand the current and past traffic condition of NSP, ISP, and enterprise networks. These systems collect traffic performance data from a SNMP agent running on the network devices such as routers and switches, store the gathered information into a DB, and display the network performance status in the form of a time-series graph or a network weather map using Web user interface. Most of current enterprise networks are constructed in the form of a hierarchical tree-like structure with multi-Gbps Ethernet links, which is quietly different from the national or world-wide backbone network structure. This paper focuses on the network weather map for current enterprise network. We start with the considering points in developing a network weather map system suitable for enterprise network. Based on these considerings, this paper proposes the best way of using SNMP in constructing a network weather map system. To prove our idea, we designed and developed a network weather map system for our campus network, which is also described in detail.

Key Words : Network Weather Map, Time-series graph, Enterprise Network, Passive Monitoring, SNMP, MIB

1. 서 론

현재 엔터프라이즈 네트워크는 multi-Gbps를 지원하는 이더넷 스위치 기반의 트리 토폴로지의 형태로 구축되고 있고 이러한 추세는 앞으로도 계속될 것이다.[1] 이러한 계층적 트리 구조의 최 상단에는 라우터가 있어 인터넷과의 연결을 담당하고, 각 건물에는 상단에서부터 Building 스위치, Floor 스위치, Room 스위치, 종단에는 컴퓨터들이 위치하며, 각 건물의 Building 스위치들과 라우터 사이를 연결하는 코어스위치가 위치한다. 또한 링크들은 하단은 100 Mbps Fast 이더넷으로, 상단은 1 Gbps 이상의 Gbit 이더넷으로 구성된다.

네트워크 사업자 (NSP)나 인터넷 사업자 (ISP)의 코어 네트워크 및 회사, 학교, 기관의 엔터프라이즈 네트워크의 트래픽 현황을 파악하기 위한 방법으로 SNMP 프로토콜을 이용한 네트워크 모니터링 시스템[2]이 많이 구축되고 있다. SNMP 기반의 네트워크 모니터링 시스템은 라우터

※ 이 논문은 2007년 정부(교육인적자원부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임(KRF-2007-331-D00387)
† 정 회 원 : 고려대학교 컴퓨터정보학과 조교수
†† 준 회 원 : 고려대학교 컴퓨터정보학과 학사과정
††† 준 회 원 : 고려대학교 컴퓨터정보학과 석사과정
논문접수 : 2007년 7월 11일, 심사완료 : 2008년 3월 3일

나 스위치에 내재된 SNMP 에이전트로부터 트래픽 통계 정보를 주기적으로 수집하여 과거와 현재의 네트워크 트래픽 발생현황을 다양한 형태로 보여준다. SNMP 에이전트가 제공하는 트래픽 통계정보는 표준화된 혹은 개별적으로 정의된 MIB 구조에 따라 구축되고, SNMP 매니저에 해당하는 모니터링 시스템은 SNMP 프로토콜을 이용하여 MIB 정보를 수집한다.

모니터링 시스템에서 네트워크 트래픽 현황을 표현하는 방법으로는 현재의 트래픽 현황을 네트워크 토폴로지 정보와 함께 보여주는 Network Weather Map (NWM) [3, 4, 5, 6]과 각 링크의 시간 추이에 따른 트래픽 변화를 그래프로 보여주는 시간추이 그래프[7]의 형태가 대표적이다. 사용자 인터페이스 또한 독립된 응용프로그램으로 구축되기도 하고, 사용자의 이동성, 편재성을 고려하여 웹 기반의 시스템으로 구축되기도 한다.

본 논문은 현재의 엔터프라이즈 네트워크에 적합한 SNMP 기반의 Network Weather Map 및 시간추이 그래프 시스템 구축에 있어 고려되어야 할 사항을 점검하고, 이를 바탕으로 엔터프라이즈 Network Weather Map 시스템을 설계하고 구현한 내용을 기술한다. 특히 엔터프라이즈 네트워크와 코어네트워크의 토폴로지 상의 차이를 고려하여 효율적인 Network Weather Map 디자인을 제시하고, multi-Gbps 고속 링크를 지원하는 현재의 라우터/스위치장비에 SNMP MIB-II 사용의 문제점을 확인하고 이의 해결방안을 제시한다. 또한 SNMP의 사용에 따른 네트워크 트래픽의 발생량, 그리고 네트워크 장비의 부하를 조사함으로써 SNMP의 효율적 사용방법을 제시한다. 본 논문에서 구축한 Network Weather Map 시스템은 학교 캠퍼스 네트워크를 대상으로 구축되었다.

본 논문은 다음과 같은 순서로 기술한다. SNMP 기반의 네트워크 모니터링 시스템에 대한 관련연구가 2장에서, Network Weather Map 시스템 구축 고려사항이 3장에 기술한다. 4장에서는 고려사항을 바탕으로 한 시스템 설계에 대하여 5장은 시스템 구현 및 구현 결과에 대하여 기술한다. 마지막으로 6장에서는 결론을 맺고 향후 보완점과 연구과제에 대하여 언급한다.

2. 관련 연구

SNMP [2]는 네트워크[8]뿐만 아니라 시스템[9] 및 서비스[10]의 성능을 모니터링 하기 위한 표준화된 가장 일반적인 도구이다. 본 장에서는 Network Weather Map (이하 NWM) 시스템 구축에 대한 관련 연구를 기술한다.

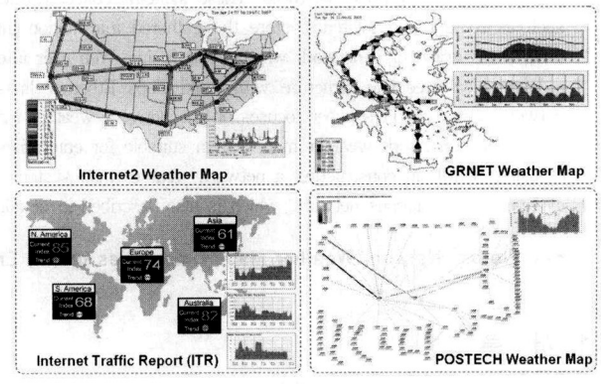
〈표 1〉 Network Weather Map 시스템의 내용에 따른 분류

Target Network	Core Network, Enterprise Network
What to monitor	Bandwidth, Utilization, Response Time, Packet Loss
Data Gathering Method	SNMP-based, Proprietary protocol-based
How to show	Arrow and Color in the geographical map
User Interface	Window-based, Web-based

<표 1>은 네트워크의 현황을 나타내는 NWM 시스템의 구축 내용에 따른 분류이다. 우선 NWM시스템은 보여주는 내용에 따라 특화된 데이터 수집체계를 통하여 구축된 시스템[11]도 있지만 일반적으로 많은 시스템들은 SNMP를 이용하여 네트워크 장비로부터 트래픽 정보를 수집하여 보여준다[12, 13]. SNMP 기반의 NWM 시스템의 구축은 대상 네트워크에 따라 코어 네트워크를 위한 NWM 시스템, 엔터프라이즈 네트워크를 대상으로 한 NWM 시스템으로 나누어 볼 수 있고, 구축된 형태에 따라 웹 기반 사용자 인터페이스를 제공하는 웹 기반 NWM 시스템, 독립된 컴퓨터에서 윈도우즈 사용자 인터페이스 위주로 구현된 윈도우즈 기반 시스템으로 나누어 볼 수 있다. 많은 경우 NWM 시스템들은 위의 항목들을 목적에 따라서 적절히 혼용하여 구축되고 있다.

NWM 시스템의 관점에서 본 윈도우즈사용자 인터페이스의 장점으로는 네트워크 장비의 연결정보 자동 검색[12, 13]을 통한 자동화된 네트워크 토폴로지 구축 및 다양한 토폴로지 표현 방법을 제공하며, 목적에 따라 다양한 기능을 추가 삭제 할 수 있는 시스템 운영의 유연성을 제공하지만, 사용자의 이동성 및 다수 사용자의 지원이 어려운 단점이 있다. 그러나 웹 기반 사용자 인터페이스는 반대로 사용자의 이동성과 동시성에 대한 장점은 있지만 정해진 범위 내에서의 분석 및 정보표현으로 유연성이 부족한 단점이 있다. 본 논문에서 개발한 NWM 시스템은 엔터프라이즈 네트워크를 대상으로 구축하고 웹 기반의 사용자 인터페이스를 제공하는 구조로 설계되고 구현되었다.

(그림 1)은 현재 운영되고 또한 공개되고 있는 대표적인 NWM 시스템의 구축 사례들이다. <표 2>은 그들의



(그림 1) NWM관련연구

〈표 2〉 NWM 관련 연구 비교

	Internet2 [3]	GRNET [5]	ITR [4]	POSTECH [6]
Origination	NOC at Indiana Univ.	Ministry of Development in Greece	AnalogX.com	DPNM at POSTECH
Target Network	Abilene Core Network	Greece Core Network	World Internet	POSTECH Campus Network
What to monitor	Bandwidth Utilization	Utilization	Response Time Packet Loss	Bandwidth
Data gathering	SNMP	SNMP	Ping	SNMP
How to show	Two colored arrow on geographical map	Two colored arrow on geographical map	Traffic Index on world map	Two gray arrow
User Interface	Web-based	Web-based	Web-based	Web-based

NWM 시스템 구축에 있어 특징들을 비교한 것이다.

먼저 가장 대표적인 NWM 시스템[3]으로 미국 Indiana Univ.의 Network Operation Center (NOC)에서 Internet2 (Abilene Network)을 모니터링 하는 시스템이다. 이 시스템은 미국 내 Internet2를 구성하는 Point of Presence (POP) 12개 사이의 트래픽 현황을 실시간으로 측정하여 웹으로 그 결과를 보여준다. 이 NWM의 특징은 미국 지도상에 각 POP의 위치를 표시하고, POP과 POP사이의 양방향 트래픽을 화살표로 분리하고, 각각의 트래픽 양을 색깔을 달리하여 표현하고 각 연결 별 트래픽의 시간추이 그래프도 보여주고 있다. 이러한 방법은 코어네트워크를 대상으로 한 NWM 시스템의 가장 대표적인 구축 사례이다.

Internet Traffic Report[4]은 전 세계 트래픽의 흐름 현황을 취합하여 대륙 별 트래픽 상황을 숫자 값(traffic index: 0-100)으로 표현한다. 이 시스템은 각 링크의 현황 보다는 대륙단위의 전반적인 트래픽 현황을 PING을 이용하여 RTT와 패킷 손실률을 트래픽 인덱스의 값으로 표현하고 있다. 5분 주기의 실시간 정보를 웹을 통하여 확인할 수 있다.

GRNET NWM 시스템[5]은 그리스 국내 네트워크의 트래픽 현황을 NWM과 각 링크의 시간추이 그래프를 통하여 표현하고 웹을 통하여 정보를 제공한다. 이 역시 코어네트워크를 대상으로 구축된 시스템으로 화살표와 색깔로 트래픽의 방향과 양을 표현하며, 시간 추이 그래프를 통하여 시간 흐름에 따른 각 링크의 트래픽양의 변화를 확인할 수 있게 해 준다.

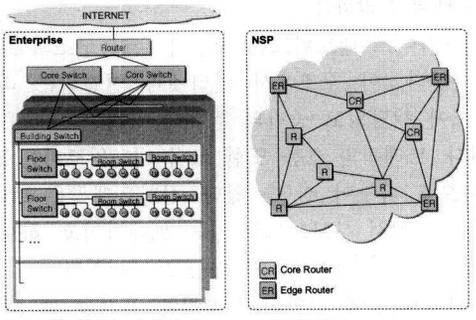
엔터프라이즈 네트워크를 대상으로 한 NWM 시스템은 네트워크의 보안과 관리의 면에서 공개된 것을 찾아보기 쉽지 않다. 국내의 포항공대 NWM 시스템[6]은 대표적인 엔터프라이즈 네트워크를 대상으로 한 시스템으로 코어네트워크 NWM 시스템과는 다른 몇 가지 특징이 있다. NWM상에 네트워크 토폴로지 구성에 있어 지도를 사용하지 않고, 각 네트워크 장비와 장비들 사이의 링크를 중심으로 구성되었다. 각 링크 별 트래픽 정보는 코어네트워크 NWM과 비슷하게 화살표와 색깔로 트래픽 양을 표현하고 있다. 또한 관리자의 입장에서 주요한 네트워크 장비, 링크를 제한하여 NWM에 표시하고 있다. 단점으로는 관심대상이 늘어나게 되면 복잡한 구조로 표현되어 효과적인 표현방법의 개발이 요구된다. 엔터프라이즈네트워크 NWM역시 각 링크 별 트래픽 변화를 파악하기 위해 시간추이 그래프를 제공하고 있다.

3. 엔터프라이즈 NWM시스템 구축 고려사항

3.1 엔터프라이즈 네트워크 토폴로지

엔터프라이즈 네트워크 토폴로지는 코어네트워크 토폴로지와 다르다. 따라서 NWM 시스템의 구축에 있어 엔터프라이즈 네트워크 토폴로지 특성을 최대한 고려하여 구축하여야 한다.

엔터프라이즈 네트워크 토폴로지는 (그림 2)에 나타난



(a) 전형적인 Enterprise Network (b) 전형적인 Core Network

(그림 2) Enterprise 네트워크 vs. Core 네트워크

바와 같이 최 상단에 라우터가 있어 인터넷과 연결되고, 라우터로부터 들어온 인터넷 트래픽을 각 건물로 분산하는 코어스위치, 각 건물에서 트래픽을 취합/분산하는 Building 스위치, 건물의 각 층에서 트래픽을 분산하는 Floor 스위치, 그리고 하단에 컴퓨터가 직접 연결되거나 Room 스위치를 거쳐 각종 컴퓨터 장비로 연결되는 계층적 트리 구조 (Hierarchical Tree-like Structure)를 형성한다. 이는 (그림 2)에서 나타난 일반 그래프 구조의 코어네트워크의 구조와는 다른 형태를 띠고 있다. (그림 2)에서 나타난 계층적 트리 구조의 엔터프라이즈 네트워크 토폴로지 정보가 NWM의 디자인에 고려되어야 한다.

3.2 엔터프라이즈 네트워크 모니터링 범위

엔터프라이즈 NWM은 코어 네트워크의 NWM과는 달리 구성하는 네트워크장비와 링크의 세부적인 연결정보를 중심으로 구축되기 때문에 네트워크 장비, 링크의 선택이 중요하다. 계층적 트리 구조로 이루어진 엔터프라이즈 네트워크의 네트워크장비들은 네트워크 관리자 관리와 사용자 관리로 나눌 수 있다. 이는 NWM 디자인에 있어 트리 구조에서 표현범위를 결정하는 중요한 요소가 된다.

일반적으로 상위 라우터에서 하위 Floor 스위치까지는 네트워크 관리자의 관리 범위에 속하고, Room 스위치 이하는 사용자가 관리하고 있다. NWM의 디자인에 있어 모니터링 범위는 관리자 관리의 네트워크 장비들로 정하는 것이 관리의 일관성과 시스템 운용의 효율성을 위해 타당하다. 또한 관리자 관리 범위의 네트워크 장비는 IP 주소가 할당되어야 하고, SNMP 에이전트가 동작되어야 한다.

장비의 선택 다음으로 고려되어야 하는 것이 선택된 장비의 링크들 중에서 NWM 표현에 필요한 링크를 선택하는 일이다. NWM을 위한 네트워크 토폴로지 구성에 필요한 링크들은 링크 단위로 트래픽 정보가 표현되어야 하고, 나머지 링크들은 목적에 따라 NWM에 제외 될 수도 있고, 그룹별로 통합되거나 전체로 통합되어 표현될 수 있다. 본 NWM의 구축에 있어서는 장비의 모든 링크의 정보를 표현하는 것을 목표로 한다. 단지 링크 별로 트래픽 정보를 표현하는 감시 링크들, 무선 Access Point (AP)가 연결된 Wireless Link 그룹, 나머지 링크들인 The Others 링크 그룹으로 나누고, 이들을 NWM에 표현한다.

3.3 트래픽의 방향성

엔터프라이즈 네트워크는 계층적 트리 구조의 토폴로지를 형성한다. 이 구조에서 인터넷과 연결되는 라우터는 root노드에 해당되고 종단의 컴퓨터 장비들은 leaf 노드에 해당된다. 트래픽의 흐름 또한 코어 네트워크와는 달리 상향/하향으로 나누어 질 수 있다. 상향트래픽은 트리 구조상 자식노드에서 부모노드로 가는 트래픽이고, 하향트래픽은 부모노드에서 자식노드로 가는 트래픽이다.

NWM 디자인에 있어서 트래픽을 표시할 때 MRTG에서와 같이 트래픽을 장비를 기준으로 수신 트래픽(inbound) / 송신 트래픽(outbound)로 나누어 색깔을 정하는 것 보다는 토폴로지상의 상향트래픽과 하향트래픽으로 구분하여 색깔을 분리하는 것이 좋다. 이는 방향성에 따른 트래픽 표현의 통일성을 유지할 수 있고, 그 양을 색의 농도로 표시하는 방법은 전체적인 트래픽의 흐름을 파악하는데 도움된다.

3.4 모니터링 지점의 선택

타깃 링크의 트래픽 정보를 측정할 때 계층적 트리 구조에서 링크의 상위 또는 하위 네트워크 장비 중 하나를 선택해야 한다. 링크를 통해 지나간 트래픽은 링크 양단 네트워크 장비의 SNMP 에이전트로부터 모두 수집할 수 있기 때문이다. 이러한 선택에 있어서 일관성의 유지가 NWM 시스템의 사후 관리를 위해 중요하다.

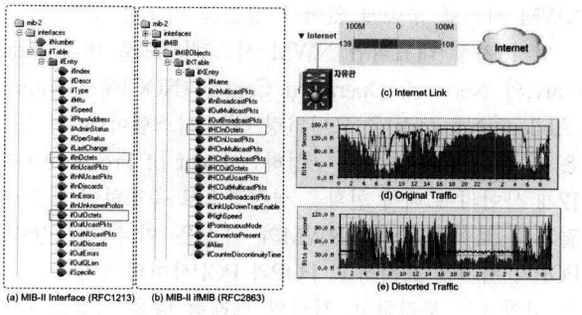
본 논문에서는 엔터프라이즈 네트워크의 계층적 트리 구조에서 타깃 링크의 트래픽 정보는 상위 네트워크 장비에서 수집하는 것을 제안한다. 이유는 각 링크의 상단 네트워크 장비에서 트래픽 정보를 수집하면 관리 범위를 한 단계 더 확장 할 수 있기 때문이다. 즉 Room 스위치 및 각 호스트 별 트래픽 발생 정보를 NWM에 표현 가능하게 된다. 단 라우터에서 인터넷으로 오가는 트래픽 정보는 라우터와 연결된 상단 네트워크장비가 관리 범위를 벗어나기 때문에 라우터에서 잡아야 하는 예외가 생긴다.

3.5 트래픽 정보 표현 주기

트래픽 정보 표현 주기는 대부분의 시스템에서5분을 사용한다. 이는 대표적인 트래픽 시간추이 그래프를 제공하는 MRTG[7]에서 트래픽 수집 주기를 5분을 최소 값으로 제공하고 있고, CISCO Enterprise MIB[14]에서도 5분을 최소 단위로 하여 트래픽 평균값 정보를 제공하고 있다. NWM 시스템을 구축함에 있어서 수집 주기를 변경함으로써 표현 주기를 변경 가능하지만, 일반적으로 사용되는 5분 단위의 NWM 정보 갱신을 사용하는 것이 타당하다고 본다.

3.6 고속 링크에서 트래픽 정보 수집 주기

트래픽 정보 수집 주기는 3.5절에서의 이유로 대부분의 시스템에서5분을 사용한다. 이는 고속 네트워크 트래픽 수집에 있어 치명적인 문제를 가지고 있다. 5분간 대역폭 평균값을 계산하기 위해 대부분의 경우 (그림 3-(a))와 같이 MIB-II [15]의 interfaces 그룹에 정의된 mib-2.2.2.1.16 (ifOutOctets)와 mib-2.2.2.1.10 (ifInOctets) MIB정보를 사용하는데, 이 MIB 오브젝트들은 Counter (32 bit) 타입으로 정의 되어 있어 (그림 3-(e))와 같이5분 동안 약 110 Mbps 이상의 트래픽이 발생하면 ifOutOctets/ifInOctets 값의 오버플로우가 발생하여 오류 값을 발생시킨다.



(그림 3) 링크 In/Out 대역폭 시간 추이그래프

(그림 3-(e))에서 보는 바와 같이 저녁18시에서 다음날 6시 사이에 파란색 그래프가 급격히 떨어지는 것을 확인할 수 있다. 이는 그 시간에 트래픽이 적은 것이 아니라 110 Mbps 이상 발생했기 때문이다. 이러한 현상은 현재 많은 엔터프라이즈 네트워크가 100 Mbps 이상의 고속 링크로 인터넷에 연결되어 있고, 라우터와 Building스위치 사이가 Gbps 고속 링크로 구축되어 있어 빈번히 나타날 수 있다.

이에 대한 해결책으로 두 가지 방법이 있다. 먼저 트래픽 정보의 수집 주기를 5분 보다 짧게 하는 방법이다. 단순 계산으로 1분 단위 수집은 550 Mbps까지 정확한 값을 얻을 수 있고, 30초 단위 수집은 1.1 Gbps까지 정확한 값을 얻을 수 있다. 이 방법은 수집 주기가 짧아짐에 따라 많은 트래픽을 발생시켜 네트워크에 부담을 줄 여지가 있다. 두 번째 방법은 MIB-II 인터페이스 그룹의 ifOutOctets이 아닌 다른 MIB으로부터 정보를 가져오는 것이다. (그림 3-(a)(b))에서 보는 바와 같이ifOutOctets 의 경우는 RFC2863 [16]에 정의된 IF-MIB의 ifHCOutOctets MIB 오브젝트가 Counter (64 bit)로 정의되어 있어 대체가 가능하다. 이와 같은 방법으로 여러 RFC 1213[15]의 MIB-II 오브젝트들은 나중에 정의된 MIB들로 대체될 수 있다. 그러나 이 방법의 사용에 있어 고려해야 할 점은 해당 네트워크 장비들이 IF-MIB 정보를 제공하는지 확인해야 하고, SNMP v2c[2] 이상의 프로토콜에서만 동작한다는 것이다. 본 논문에서는 NWM 시스템의 구축에 있어서 IF-MIB의 사용을 추천한다. 이는 현재 대부분의 네트워크장비들이 IF-MIB과 SNMP v2c을 기본적으로 지원하고 있어 5분 주기 표현과 5분주기 수집의 일관성을 유지할 수 있고 트래픽 및 시스템의 부하를 줄일 수 있기 때문이다.

본 장에서는 고속 링크로 구성된 엔터프라이즈 네트워크를 위한 NWM 시스템을 구축함에 있어서 고려되어야

할 사항들을 기술하고, 각각에 대한 타당한 해결 방안들을 제시하였다. 본 장에서 기술한 내용은 시스템을 설계하기 전에 고려해야 할 사항들을 중점으로 기술되었고, 시스템의 설계에 있어서 고려사항과 본 논문에서 선택한 방법은 4장에서 상세하게 기술한다.

4. 엔터프라이즈 NWM시스템 설계

4.1 NWM 시스템 요구사항

본 절에서는 캠퍼스 NWM 시스템 개발에 필요한 요구사항들을 기술한다.

첫째, NWM 시스템은 캠퍼스 네트워크의 관리자 관리 범위의 모든 네트워크 장비 및 모든 링크들을 모니터링 할 수 있어야 한다.

둘째, NWM 표현에 있어 캠퍼스 네트워크의 계층적 트리 구조가 잘 표현 되어야 하며, 각 계층의 링크에서 발생하는 트래픽 양에 대한 비교를 쉽게 할 수 있어야 한다.

셋째, NWM 시스템은 현재 캠퍼스 네트워크에서 발생하는 트래픽의 정보를 실시간으로 보여주어야 하며, 각 링크의 트래픽 발생량에 대한 시간 추이그래프도 볼 수 있어야 한다.

넷째, 수집된 트래픽 정보는 시간이 지남에 따라 효과적으로 저장 관리되어야 하고, 제한된 저장공간을 효율적으로 사용할 수 있어야 한다.

다섯째, 네트워크 장비로부터 트래픽 정보의 수집에 있어 네트워크 및 네트워크 장비의 부하를 최소화하여야 하고, 최단시간에 필요한 트래픽 정보를 수집할 수 있어야 한다.

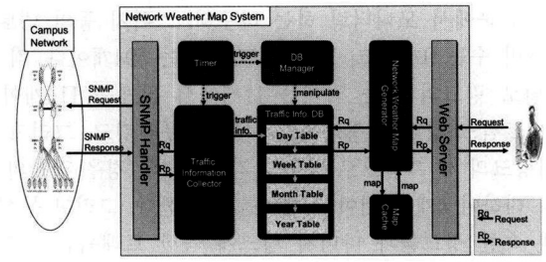
여섯째, 사용자의 NWM요구는 언제 어디서나 이루어질 수 있어야 하고, 요구에 의해 NWM 정보를 즉시 보여줄 수 있어야 하며, 사용자의 요구 폭증을 효율적으로 처리할 수 있어야 한다.

본 논문에서 개발한 캠퍼스 NWM 시스템은 위의 여섯 가지 요구사항을 바탕으로 개발되었다.

4.2 NWM 시스템 전체 구조

(그림 4)는 캠퍼스 NWM 시스템의 전체적인 구조를 표현한 것이다. 캠퍼스 NWM 시스템은 기본적으로 SNMP를 이용하여 캠퍼스 네트워크의 각 네트워크 장비로부터 트래픽 정보를 수집하여 Traffic Info. DB에 저장하고, 사용자의 요청에 의해 DB에 저장된 정보를 바탕으로 현재 시점의Network Weather Map을 생성한다. 사용자 요청은 웹을 통해 이루어지며 사용자는 언제 어디서나 네트워크를 통해 캠퍼스 네트워크 트래픽 현황을 파악할 수 있다.

NWM 시스템은 양단에 사용자와 HTTP 통신을 담당하는 웹 서버, 네트워크 장비와의 SNMP 통신을 담당하는 SNMP Handler가 존재하고, 그 사이에 타이머, Traffic Info. Collector, DB Manager, Traffic Info. DB, NWM Generator, Map Cache의 6개의 모듈이 있다. 6개의 모듈은 DB를 중심으로 DB에 트래픽 정보를 수집하여 저장하



(그림 4) NWM 시스템 전체 구조

는 Traffic Info. Collector와 DB에 저장된 데이터를 주, 월, 년 단위로 압축 저장하는 DB Manager가 있고, 타이머는 주기적인 시간 간격으로 Traffic Info. Collector와 DB Manager를 실행시킨다. 웹 서버를 통해 사용자 요청이 들어오면 NWM Generator는 DB에 저장된 트래픽 정보를 읽어 NWM을 생성하고, 생성된 NWM은 Map 캐쉬에 저장한다. NWM Generator는 DB가 새롭게 갱신되기 전까지 Map 캐쉬에 있는 map을 사용자에게 제공한다. 다음은 NWM 시스템의 각 모듈에 대한 상세 설명이다.

4.3 Traffic Information DB

Traffic Info. DB는 MRTG와 RRDTool [17]에서 시간추이 그래프를 표현하기 위한 데이터 저장방법인 Round-Robin DB의 형태로 테이블을 구축하였다. 이는 시간의 흐름에 관계없이 저장공간의 크기를 일정하게 유지하면서 다양한 시간추이 그래프 (일간, 주간, 월간, 연간)를 보여줄 수 있는 장점이 있다.

Traffic Info. DB는 (그림 5)에서 보는 바와 같이 5분 단위로 각 링크의 양방향 대역폭 정보를 저장하는 day_table, 30분 단위 대역폭 평균을 저장하는 week_table, 2시간 단위 평균값을 저장하는 month_table, 1일 단위 평균값을 저장하는 year_table의 4 종류의 table이 각 모니터링 링크 별로 별도로 구성된다. 4 종류의 table이 하나의 set을 이루어 장비의 각 링크별로 구축된다.

각 DB테이블에 저장되는 레코드의 수는 (그림 5)와 같이 day_table은 7일간 2016 개, week_table은 14일간 672 개, month_table은 60일간 720 개, year_table은 400일간 400개의 레코드를 갖게 되고, 한 링크를 모니터링 하기 위해 필요한 저장공간은 DB 사용에 따른 시스템 공간을 제외하고 순수한 데이터 저장공간은 위의 네 테이블에 필요한 공간의 합인 90.288 Kbytes이다.

day_table (# of record = 7 day x 24 hour x 12 (5 min) = 2016, (2016x28 = 54.448 Kbytes)

Time (4 byte)	InOctets (8byte)	5min_avg_InBw (4 byte)	OutOctets 8 byte	5min_avg_OutBw (4 byte)

week_table (# of record = 14 day x 24 hour x 2 (30 min) = 672, (672x20 = 13.440 Kbytes)

Time (4 byte)	30min_avg_InBw (4byte)	30min_max_InBw (4 byte)	30min_avg_OutBw (4 byte)	30min_max_OutBw (4 byte)

month_table (# of record = 60 day x 12 (2 hour) = 720, (720x20 = 14.400 Kbytes)

Time (4 byte)	2hr_avg_InBw (4byte)	2hr_max_InBw (4 byte)	2hr_avg_OutBw (4 byte)	2hr_max_OutBw (4 byte)

year_table (# of record = 400 day = 400, (400x20 = 8.000 Kbytes)

Time (4 byte)	1day_avg_InBw (4byte)	1day_max_InBw (4 byte)	1day_avg_OutBw (4 byte)	1day_max_OutBw (4 byte)

(그림 5) Traffic Info. DB의 테이블 스키마

본 논문에서 모니터링 하는 라우터, 스위치 등의 네트워크 장비 수는 9개이고, 모든 링크의 수는 594개이다. 각 장비 별로 링크의 수는 적게는 11개에서 많게는 114개이다. 각 네트워크 장비의 링크는 감시링크, 무선링크, 그리고 나머지링크의 세 그룹으로 나누고 감시링크의 경우 각각의 링크에 대하여 4개의 테이블 세트를 생성한다. 그리고 무선링크에 속한 링크들과 나머지 링크에 속한 트래픽은 각각 1세트의 테이블로 트래픽 정보를 표현한다. 따라서 전체 필요한 테이블 세트의 수는 63개 (감시링크: 49, 무선링크: 6, 나머지링크:8)로 필요한 전체 저장공간은 5.688 Mbytes (= 90.280 Kbytes x 63)이다. 이 사이즈는 캠퍼스 NWM 시스템을 구축하는데 필요한 최소한의 저장공간이다. 물론 링크의 수가 늘어나게 되면, 그리고 수집해야 할 정보의 종류가 늘어나 테이블의 스키마가 확장되게 되면 저장공간의 크기는 늘어나게 되겠지만, 수백 기가의 저장공간이 흔한 현재의 컴퓨터환경에서는 충분하다고 여겨진다.

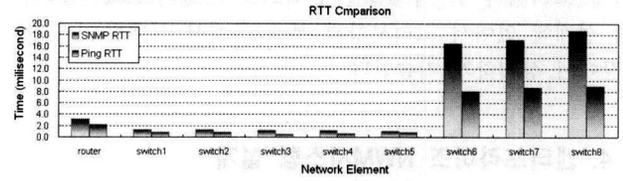
4.4 Traffic Information Collector

Traffic Info. Collector는 일정한 시간 주기로 타이머 이벤트를 받아 지정된 네트워크 장비로부터 SNMP 프로토콜 모듈을 이용하여 트래픽 정보를 수집하는 기능을 수행한다. 각 링크 별로 수집된 트래픽 정보는 DB의 day_table에 저장된다.

여기에서 고려해야 할 사항은 어떤 MIB 오브젝트로부터 어떤 시간 주기로 어떠한 방식으로 트래픽 정보를 수집할 것인가 이다. 본 논문에서 구현하는 캠퍼스 NWM 시스템은 고속 링크의 대역폭정보를 수집해야 하기 때문에 IF-MIB[16]에 정의된 ifHCOutOctets (mib-2. 31.1.1.1.10)와 ifHCInOctets (mib-2. 31.1.1.1.16)에서 SNMP v2c 프로토콜을 이용하여 5분 단위로 트래픽 정보를 수집한다. 또한 지정된 네트워크 장비의 모든 링크에 대하여 트래픽 정보를 수집하는데, 본 캠퍼스 NWM 시스템의 구축에 있어 각 장비의 링크수는 최고 114개였다.

(그림 6)은 캠퍼스 NWM시스템 구축에 사용된 장비의 종류, 각 장비당 모니터링 해야 하는 링크의 수, 그리고 NWM 시스템으로부터 각 장비로의 SNMP RTT 및 Ping RTT를 나타낸 것이다. NWM 시스템으로부터 각 장비로는 모두 3홉(Hop) 이하의 링크로 연결되어 있다. Ping RTT와 SNMP RTT는 장비에 따라서 1.5배에서 2배 정도의 차이를 보이는데 이는 SNMP 에이전트의 데이터 처리시간이 Ping 메시지 처리시간 보다 오래 걸린다는 것을 알 수 있다. SNMP RTT는 한 개의 MIB 오브젝트 값을 가져오는 시간으로 MIB 오브젝트 개수가 증가하면 SNMP 에이전트의 처리시간 또한 증가한다. 네트워크 장비의 타입에 따라 SNMP RTT는 CISCO 7507라우터의 경우 평균3.2 msec, CISCO6509 스위치 평균 1.3 msec, CISCO 6507 스위치 평균 1.2 msec, 그리고 CISCO 4006 스위치 17.5 msec의 값을 나타내었고, 장비의 타입에 따라 SNMP RTT는 최고 15배의 차이가 났다. 이러한 사실은

	router	switch1	switch2	switch3	switch4	switch5	switch6	switch7	switch8
number of links	11	70	70	114	69	13	92	59	93
Device Type (CISCO)	7507	6509	6509	6506	6506	6506	4006	4006	4006

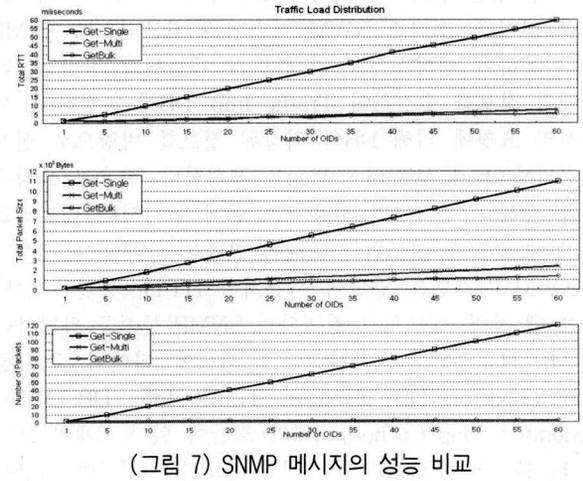


(그림 6) 캠퍼스 NWM에 사용된 네트워크 장비

SNMP를 이용하는 트래픽 정보를 가져오는데 시간을 줄이기 위한 효율적인 방법을 찾아야 함을 의미한다.

MIB 데이터를 수집하는데 있어 사용할 수 있는 SNMP 메시지는 SNMP Get (또는 GetNext) 메시지와 SNMP GetBulk 메시지가 사용된다. SNMP Get 메시지는 MIB 오브젝트 하나씩 가져오는 방법(Get-Single)과 여러 MIB 오브젝트를 한꺼번에 가져오는 방법(Get-Multi)의 두 가지 방법을 생각할 수 있다. (그림 7)은 CISCO 6506 장비로부터 MIB 오브젝트 1개에서 60개의 값을 가져오는데, Get-Single, Get-Multi, GetBulk SNMP 메시지 사용의 성능을 비교한 것이다. Get-Single은 Get 메시지를 이용하여 MIB 오브젝트를 하나씩 가져오는 경우이고, Get-Multi는 Get 메시지를 이용하여 여러 개의 MIB 오브젝트를 한꺼번에 가져오는 경우이다. GetBulk는 GetBulk 메시지를 사용하는 경우이다. SNMP는 UDP 기반으로 동작하기 때문에 하나의 SNMP request로 가져올 수 있는 MIB 오브젝트의 개수는 UDP 패킷의 최대 값(1500 byte, IP, UDP header size 포함)이내로 결정되고, 그 값은 대략 60개의 MIB 오브젝트이다.

성능 평가는 수집해야 하는 SNMP MIB 오브젝트의 수의변화에 따른 SNMP RTT값, SNMP 메시지의 크기, 그리고 SNMP 메시지의 수를 Get-Single, Get-Multi, 그리고 GetBulk에 대하여 비교하였다. (그림 7)에서 나타난 바와 같이 Get-Single의 경우, 수집되는 MIB 오브젝트의 수가 증가함에 따라 RTT, 메시지 크기, 메시지 수는



(그림 7) SNMP 메시지의 성능 비교

〈표 3〉 60개 MIB 오브젝트 수집시 성능 비교

60 MIB objects	Total RTT		Total Packet Size		Number of packets	
	msec	ratio	bytes	ratio	count	ratio
Get-Single	59.84	10.93	10,956	8.15	120	60
Get-Multi	7.65	1.38	2,354	1.75	2	1
GetBulk	5.47	1	1,344	1	2	1

Get-Multi와 GetBulk에 비해 급격히 증가함을 알 수 있다. 따라서 하나의 장비로부터 다수의 MIB 오브젝트 값을 수집해야 하는 경우 Get-Single의 방법은 지양해야 하며, Get-Multi 또는 GetBulk를 사용해야 함을 알 수 있다. Get-Multi와 GetBulk의 경우 SNMP 메시지의 수는 2개로 동일하지만, RTT와 메시지의 크기의 면에서 GetBulk가 더 효과적임을 알 수 있다.

<표 3>에 나타난 바와 같이 MIB 오브젝트 60개를 추출할 경우 Get-Multi의 경우 GetBulk에 비해 RTT는 1.38배, 메시지 크기는 1.75배의 차이를 보였다. UDP기반의 SNMP 메시지의 특성상, 60 MIB 오브젝트는 하나의 UDP 패킷으로 보낼 수 있는 최대 MIB 오브젝트 값으로 볼 수 있기 때문에 이 차이는 Get-Multi와 GetBulk의 최대 차이라고 볼 수 있다. (그림 7)의 그래프에서 나타난 바와 같이 MIB 오브젝트의 수가 줄어들면 그 차이는 줄어들게 되고, MIB 오브젝트의 수가 60 이상으로 늘어나더라도 SNMP 메시지의 수가 증가하게 되기 때문에 그 차이는 다시 조금씩 줄어들게 된다.

캠퍼스 NWM 시스템의 구축에 있어 모니터링 되는 링크는 한 네트워크 장비에 최고 114개이고 각 링크 당 2개의 MIB 오브젝트 (ifHCOutOctets, ifHCInOctets) 값을 추출하므로 Get-Multi나 Get-Bulk를 사용하고 한번에 60개씩의 MIB 오브젝트 값을 가져온다면 4개의 SNMP 메시지 쌍으로 트래픽 정보를 수집할 수 있다. 트래픽 정보 수집 시간 역시40 msec내에 모든 수행이 가능하다는 것을 알 수 있다.

여기서 한가지 더 고려해야 할 사항은 모든 경우에 GetBulk가 최상은 아니라는 점이다. 즉 GetBulk의 특성상 SNMP MIB을 순차적으로 가져올 경우에는 GetBulk가 최상의 성능을 발휘하지만, MIB 트리상에 산발적으로 분포된 MIB 오브젝트의 값을 가져 올 경우에는 GetBulk는 사용할 수 없게 된다. 이 경우 Get-Multi를 사용하는 것이 더 효과적이다. 예를 들어 114개의 링크를 가진 네트워크 장비의 모든 링크의 ifHCOutOctets, ifHCInOctets 값을 가져와야 한다면 GetBulk가 효과적이지만, 일부 사용되지 않는 링크를 제외한 링크의 ifHCOutOctets, ifHCInOctets 값을 가져온 다면 Get-Multi를 사용하는 것이 더 효과적이다. 그리고 SNMP 결과 메시지를 처리하는 데 있어서도 Get-Multi가 GetBulk보다 더 쉽기 때문에 Get-Multi와 GetBulk의 선택에 있어서 RTT 와 메시지 사이즈뿐만 아니라 어떤 MIB 오브젝트 값을 수집해야 하는 지, 그리고 수집된 MIB 오브젝트 값의 처리 방법 등의 요인도 동일한 수준으로 고려되어야 한다.

본 논문에서 구현한 캠퍼스 NWM 시스템에 있어서는 Get-Multi 방법을 이용하여 구현하였다. 네트워크 연결 특성상 한 장비에서 모든 링크에 대한 MIB 오브젝트 정보를 가져올 필요가 없기 때문이다. 또한 Get-Multi의 방법은 RTT와 메시지 크기의 증가가 있지만, 그것은 전체 링크용량 (100 Mbps or 1Gbps)에 비하여 충분히 작고, 시간 또한 1초 이내에 원하는 데이터를 수집할 수 있어 요구사항을 충분히 만족시킬 수 있으며, 캠퍼스 NWM 시스템의 분석 구조를 단순화하고, 다른 MIB 오브젝트의 수집 필요에 따른 확장성의 장점이 있기 때문이다. 또한 네트워크 장비의 부하는 어떤 방법을 사용하든 거의 일정한 수준을 유지하였고, SNMP 오퍼레이션이 네트워크 장비의 성능에 대한 영향은 거의 없는 것으로 나타났다.

엔터프라이즈 네트워크에 문제가 발생하지 않는다면 Traffic Info. Collector는 Get-Multi나 GetBulk를 이용한 순차적인 링크 트래픽 정보의 수집을 하여도 네트워크 부하나 수집 시간에 있어 충분히 요구사항을 만족시킬 수 있다. 여기에 효율성을 더하기 위하여 SNMP 메시지를 비동기화 기법을 이용하여 사용하거나, 쓰레드/멀티프로그래밍의 병렬적 수행 기법을 이용한 동시 수집을 고려할 수 있으며 이는 엔터프라이즈 네트워크의 크기와 수집해야 할 네트워크 장비의 수 및 링크의 수 등을 고려하여 적절히 결정되어야 할 사항이다.

다음으로 고려해야 될 사항은 네트워크와 네트워크 장비에 장애가 발생한 경우 NWM 시스템의 안정적 동작이다. 트래픽 정보 수집 시간은 어떠한 경우라도 다음 수집 시간 전에 끝나야 한다. SNMP는 UDP를 사용하기 때문에 SNMP 패킷의 손실, SNMP 에이전트의 장애, 네트워크 장비의 장애 등의 경우에 Traffic Info. Collector는 적절히 대처하여야 한다. 본 논문에서 구축한 Traffic Info. Collector는 SNMP 메시지를 보내고 난 후에 일정시간 동안 답변이 없으면 문제가 생겼음을 인식하고 다시 SNMP 메시지를 보낼지, 장애로 여길지 판단하는데, 이 경우 타임아웃의 값과 재시도(retrial) 횟수가 Traffic Info. Collector의 안정적 동작에 큰 영향을 미친다.

본 논문의 캠퍼스 NWM 시스템에서는 타임아웃 값을 2 sec, 재시도(retrial) 횟수를 2회로 정하였다. 이는 NWM 시스템 및 타깃 장비들이 모두 캠퍼스 네트워크 내에 존재하고, 3 홉(Hop)이하의 링크로 연결되어 있기 때문이다. 또한 한 네트워크 장비에 5 개의 SNMP 메시지의 응답이 연속적으로 돌아오지 않을 경우 해당 네트워크 장비의 장애로 판단하고 그 장비로의 SNMP 메시지는 해당 시간에 더 이상 보내지 않게 된다. 최악의 경우(예, 스위치 장비 다운) 해당 장비로 5개의 SNMP 메시지를 보내게 되고 각 메시지당 소요되는 시간은 4초 (2회 x 2초)로 20 초 정도에 해당 네트워크 장비로의 요청이 끝나게 된다. 이는 트래픽 수집 주기가 5분이기 때문에 충분한 시간이다.

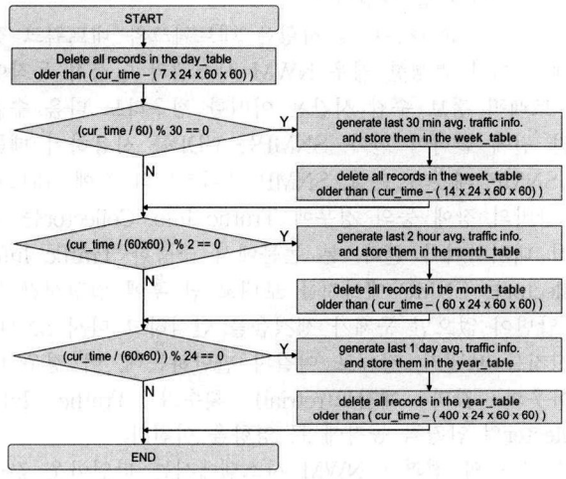
또한 네트워크 장비 별로 Traffic Info. Collector를 독립된 프로세스로 실행시킴으로써 트래픽정보 수집을 병렬적으로 수행한다. 라우터에서부터 Building 스위치 레벨까지 9개의 네트워크 장비에 대하여 각각 독립된 프로세스

가 트래픽 정보를 수집한다. 한 장비에 대하여 최악의 경우 20 초의 시간이 소요된다. 그러나 장애가 발생하지 않은 경우는 1초 내에 모든 수집이 끝나게 된다.

4.5 DB Manager

DB Manager의 역할은 각 링크의 day_table에 저장된 5 분 평균 트래픽 정보를 4.3절에서 정의한 내용에 맞춰 week_table, month_table, year_table을 구성하는 역할을 수행한다. (그림 8)은 5 분 마다 타이머에 의해 이벤트를 받은 DB Manager의 작업 내용을 순서도로 그린 것이다.

먼저 각 링크의 day_table에 저장된 레코드들 중에 7일 이전의 데이터를 지운다. 다음으로 현재 시각이 0분, 30분일 경우 day_table에 저장된 지난 30분 간의 트래픽 정보를 바탕으로 수신 및 송신 트래픽의 평균 대역폭, 최대 대역폭을 계산하여 week_table에 저장하고 14일 이전의 데이터는 지운다. 다음으로 매 2시간 마다 지난 2시간 동안의 트래픽 양의 평균값, 최대값을 계산하여 month_table에 저장하고 60일 이전의 데이터는 month_table에서 지운다. 마지막으로 매 24 시간 마다 지난 1일 동안의 트래픽 양을 계산하여 year_table에 저장하고 400일 이전의 데이터를 지운다.

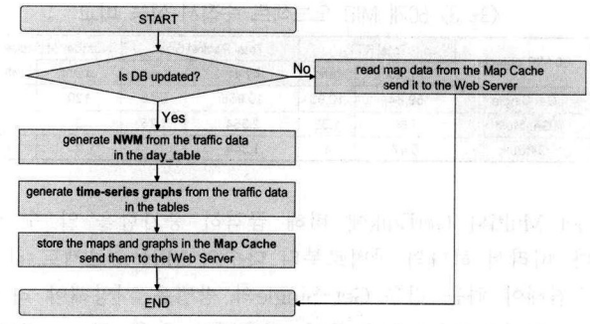


(그림 8) DB Manager 순서도

4.6 NWM Generator

NWM Generator의 역할은 사용자의 요청에 의해 현재 MAP정보를 웹 페이지 형식으로 생성하고 웹서버를 통하여 사용자에게 전달하는 역할을 수행한다. 캠퍼스 NWM 시스템은 5분 주기로 트래픽 정보를 갱신하고 map 데이타를 생성하고, 웹 UI의 특성상 여러 사용자로부터 동시 다발적인 요청이 이루어질 수 있기 때문에 map 캐쉬를 두어 시스템의 부하를 최소화 하였다.

(그림 9)은 사용자 요청에 따른 NWM Generator의 동작을 나타내는 순서도이다. 우선 사용자의 요청이 들어오면 최근 요청 이후 DB의 트래픽 정보가 갱신 되었는지 검사한다. 갱신되지 않았다면 Map 캐쉬에 저장된 map 데이터를 보내주고, 갱신되었다면 새로운 map 데이터와 시



(그림 9) NWM Generator 순서도

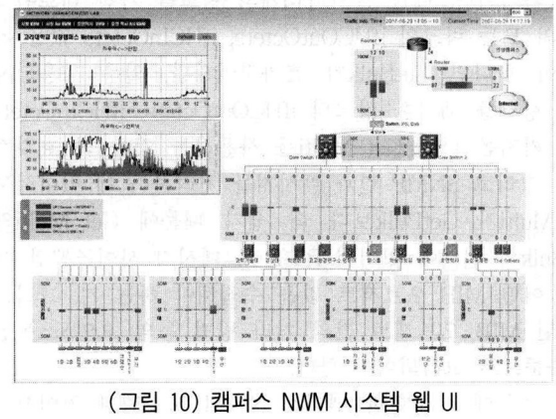
간 추이 그래프를 생성하여 Map 캐쉬에 저장하고 웹서버에 보내준다. 이러한 방법으로 NWM Generator의 부하를 최소화하고, 많은 사용자의 동시 요청을 처리할 수 있다.

5. 시스템 구현

4장의 NWM 시스템 설계를 바탕으로 캠퍼스 네트워크의 트래픽 현황을 한 눈에 파악할 수 있는 캠퍼스 NWM 시스템을 개발 하였다. (그림 10)은 NWM 시스템이 보여주는 map 내용이다.

캠퍼스 네트워크는 최상위의 라우터가 인터넷과 다른 캠퍼스로 연결되어 있고, 라우터는 하위에 두 대의 코어 스위치와 연결되어 있다. 두 대의 코어 스위치는 각 빌딩의 Building 스위치와 동시에 연결되어 있어 장애 발생을 최소화 한 구조로 되어 있다. 각 Building 스위치와 연결된 Floor 스위치까지 캠퍼스 네트워크의 계층적 트리 구조를 map으로 표현하였다.

각 계층별 링크를 그룹화 하고, 링크에서 발생하는 트래픽 양을 막대 그래프로 표현하여 같은 계층의 링크에서 발생하는 트래픽의 양을 쉽게 비교할 수 있도록 하였다. 캠퍼스 내에서 인터넷으로 발생하는 상향트래픽(Outbound)은 상단 막대 그래프로, 인터넷에서 캠퍼스 내로 들어오는 하향트래픽(Inbound)은 하단 막대 그래프로 표현하여 두 종류의 트래픽 양을 쉽게 비교할 수 있도록 하였다. 또한 상향트래픽, 하향트래픽 양의 표시에 있어 그래프의 색깔을 통일함으로써 쉽게 구분할 수 있도록 하였다. 상향트래픽은 초



(그림 10) 캠퍼스 NWM 시스템 웹 UI

〈표 4〉 캠퍼스 NWM 시스템 개발 환경

Hardware	P4-2.0 GHz, 786 MB, 80 G HD, 100 Mbps Ethernet
OS	Linux Fedora 6
Web Server	Apache 2.2.3
DB	MySql 5.0.22
SNMP	Net-SNMP library 5.3.1
Tool	MRTG, RRDTool, cron
Language	C, PHP, Perl

록색으로, 하향트래픽은 파란색으로 지정하였고, 이는 막대그래프, 시간추이 그래프에 모두 적용된다. 또한 각 링크를 선택하면 타깃 링크의 트래픽 시간추이 그래프를 보여줌으로써 지난 하루 동안 트래픽 발생양의 변화를 확인 할 수 있게 하였다. 또한 네트워크장비의 현재 CPU 사용량을 표시함으로써 트래픽에 따른 장비의 성능도 함께 파악할 수 있게 하였다.

본 논문에서 개발한 캠퍼스 NWM 시스템은 <표 4>와 같은 개발 환경에서 개발되었다. Fedora 6 Linux 환경에서 아파치(Apache) 웹 서버를 사용하였고, DB는 MySQL을 사용하였다. 그리고 NWM Generator로 PHP를 사용하였으며, DB Manager와 Traffic Info. Collector는 C를 이용하여 구현하였다. 타이머는 리눅스에서 제공하는 크론 서비스를, 시간추이 그래프를 생성하기 위해서는 RRDTool을 이용하였다. 구축된 시스템은 현재 캠퍼스 네트워크 관리팀에 제공되어 학내 트래픽 현황을 파악하는데 운영되고 있으며 아래의 URL을 통하여 웹으로 확인할 수 있다. http://kumon.korea.ac.kr

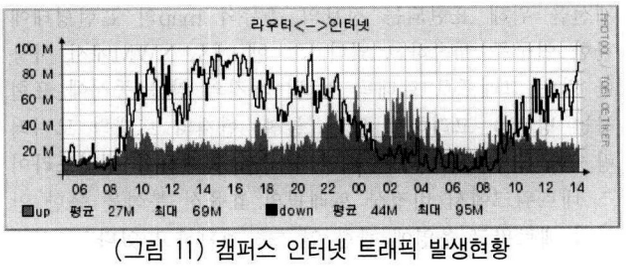
5.1 캠퍼스 네트워크 트래픽의 특징

본 절에서는 캠퍼스 NWM 시스템 개발을 통하여 관찰된 캠퍼스 네트워크의 트래픽 현황에 대하여 설명한다. (그림 11)는 하루 동안 발생한 인터넷 트래픽의 양을 나타낸 시간추이 그래프이다.

첫째, 하향트래픽 (Inbound)의 양 (1일 평균 27 Mbps)이 상향트래픽 (Outbound)의 양 (1 일 평균 44 Mbps)보다 1.6배정도 많은 양을 차지하고 있다.

둘째, 하루 동안 트래픽 양의 변화는 하향트래픽이 상향트래픽에 비해 변화가 심하고, 상향트래픽은 완만한 변화를 보여주고 있다. 또한 수업이 진행되는 낮 시간에 트래픽 양이 급격히 증가하여 최대치 (100 Mbps)까지 올라가며, 저녁과 밤 시간에는 반대로 급격히 떨어지는 현상을 보여주고 있다. 이는 학교 학생들의 활동에 대한 특성을 잘 나타내주는 것이다. 상향트래픽의 경우 변화가 심하지 않지만 밤시간의 경우 하향트래픽과 역전되는 현상이 나타났다.

셋째, 하향트래픽의 최대치는 100 Mbps인데 하루 중 오전 10시부터 오후7시까지 대부분의 시간에 최대치를 보여주고 있다. 이는 하향트래픽 대역폭에 대한 SLA를 재협상하여 높일 필요가 있음을 보여준다. 또한 하향트래픽과 상향트래픽 대역폭을 달리 정하는 대역폭 협정의 필요성도 갖게 한다. 또한 하향트래픽 대역폭이 최대치를 나타낼 때 응용 별 대역폭 할당 문제에 대한 연구의 필요성도



(그림 11) 캠퍼스 인터넷 트래픽 발생현황

생각해 볼 수 있다.

넷째, 캠퍼스 트래픽 흐름을 분석해 보면 건물 내에서 발생한 트래픽은 대부분 인터넷으로 나가거나 들어오는 트래픽이고, 건물과 건물 사이에 오가는 트래픽은 거의 없는 것으로 나타났다. 그리고 건물 내의 경우 층별로 설치되어 Floor 스위치 간의 트래픽 교환은 빌딩간의 트래픽 교환보다는 많아 보이지만, 대부분 인터넷으로 오가는 트래픽인 것으로 보여진다. 따라서 캠퍼스 내에서 발생하는 대부분의 트래픽은 인터넷 트래픽 위주이고, 캠퍼스 내 컴퓨터간 통신은 소수인 것으로 보여진다. 이러한 현상이 대부분의 엔터프라이즈 네트워크에서의 일반적인 현상인지에 대해서는 좀 더 많은 연구가 필요할 것이다. 이러한 현상이 일반적인 경우라면 네트워크 관리자는 이러한 트래픽의 특성을 고려하여 엔터프라이즈 네트워크를 관리하여야 할 것이다.

6. 결 론

본 논문은 multi-Gbps를 지원하는 이더넷 스위치 중심의 트리 토폴로지 형태로 구축되고 있는 현재의 엔터프라이즈 네트워크의 트래픽 현황을 실시간으로 파악하기 위한 Network Weather Map시스템의 설계와 구축에 관한 내용을 기술하였다. 본 연구에서는 관리자가 트래픽 현황을 효율적으로 파악하기 위하여 엔터프라이즈 네트워크가 가지는 계층적 트리 구조의 특징을 NWM의 구축에 적용하였고, 각 계층 링크에서 발생하는 트래픽을 쉽게 비교할 수 있도록 막대그래프 표현방법을 이용하였다. 또한 Gbps 이상의 고속 링크로 구축되는 엔터프라이즈 네트워크의 모니터링에 SNMP의 사용에 있어 MIB 정보 선택의 문제점과 해결점을 제시하였고, 시스템 및 네트워크의 부하에 대한 분석을 통하여 NWM 시스템이 네트워크에 미치는 영향을 연구하였다. 또한 시스템 체계와 효율성을 위하여 모니터링 지점의 선택, 트래픽 정보의 수집 주기 등 NWM 시스템의 설계와 구축에 있어 여러 가지 고려사항을 제시하고, 각각에 대한 해결책을 제시함으로써 본 논문은 향후 NWM 시스템을 구축하려는 연구에 도움을 줄 것으로 기대한다. 본 연구의 결과물인 캠퍼스 NWM 시스템은 상시 운영함으로써 네트워크 관리자의 네트워크 관리에 도움을 주고 있다.

향후 연구로는 현재의 시스템 성능 개선과 개발된 시스템을 바탕으로 엔터프라이즈 네트워크 관리에 관한 다양한 연구를 추진 중에 있다. 첫째, 시스템 성능 및 효율성

개선을 위해 표현되는 정보의 종류와 map의 표현형태에 관한 연구를 계속하고 있다. 그 한 예로 NWM에서 사용한 막대 그래프로 트래픽 양 및 패킷의 양을 동시에 표현하는 방법을 고려하고 있다. 둘째, 현재의 트래픽 모니터링 연구를 SNMP 기반 보안 연구로 확대하여 엔터프라이즈 네트워크에서 비정상 트래픽의 효율적 분석을 통한 안정적 네트워크 운영에 관한 연구를 계획하고 있다.

참 고 문 헌

[1] N. Jovanovic, D. Sorgic, Tianying Ji, Shaowen Song, "An overview of metropolitan and enterprise networks -current and future," Canadian Conference on Electrical and Computer Engineering, May 1-4, pp.160-163, 2005.

[2] William Stallings, "SNMP, SNMPv2, SNMPv3 and RMON 1 and 2, Third Edition," Addison-Wesley, ISBN:201485346, 1999

[3] Internet2 Network Weather Map, http://www.abilene.iu.edu/abilene/maps-graphs2/weather-map.html.

[4] Internt Traffic Report, http://www.internettrafficreport.com.

[5] GRNET Network Map, http://netmon.grnet.gr.

[6] POSTECH Network Weather Map, http://ngmon.postech.ac.kr/NG-MON.

[7] Tobi Oetiker, "Monitoring your IT gear: the MRTG story,", IT Professional, Vol.3, No.6, Nov-Dec, pp.44-48, 2001. http://oss.oetiker.ch/mrtg/.

[8] You-Sun Hwang, Eung-Bae Kim, "The management of the broadband wireless access system with SNMP," Proc. of the 10th International Conference on Telecommunications(ICT 2003), Tahiti, Papeete, French Polynesia, Feb. 23 - Mar. 1, pp.225-228, 2003.

[9] Myung-Sup Kim and James Won-Ki Hong, "Highly Available and Efficient Load Cluster Management System using SNMP and Web," Proc. of the IEEE/IFIP Network Operations and Management Symposium (NOMS) 2002, Florence, Italy, Apri. 15-19, pp.619-632. 2002.

[10] Jae-Young Kim, Myung-Sup Kim, and James Won-Ki Hong, "Management of Differentiated Services Using the SNMP Framework," Proc. of the International Conference on Advanced Communication Technology (ICACT) 2000, Muju, Korea, Feb. 16-18, pp.624-629. 2000.

[11] Rich Wolski, Neil Spring, and Jim Hayes,"The Network Weather Service: A Distributed Resource Performance Forecasting Service for Metacomputing," Journal of Future Generation Computing Systems,Vol. 15, No.5-6, October, pp.757-768, 1999.

[12] HP Openview, http://www.openview.hp.com.

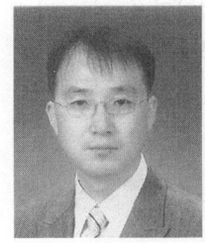
[13] IMB Tivoli, http://www.tivolie.com.

[14] CISCO, CISCO Enterprise MIB, http://www.cisco.com/univercd/cc/td/doc/product/wanbu/8850px45/release3/snmp/axsm1.htm.

[15] K. McCloghrie, M. Rose, "Management Information Base for Network Management of TCP/IP-based internets: MIB-II," FRC1213, IETF, Mar. 1991, http://www.ietf.org/rfc/rfc1213.txt.

[16] K. McCloghrie, F. Kastenholz, "The Interfaces Group MIB," FRC2863, IETF, Jun. 2000, http://www.ietf.org/rfc/rfc2863.txt.

[17] RRDtool, "Round Robin Database Tool," http://oss.oetiker.ch/rrdtool/.



김 명 섭

e-mail : tmskim@korea.ac.kr

1998년 포항공과대학교 전자계산학과 (학사)

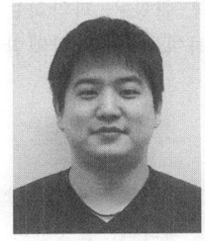
1998년~2000년 포항공과대학교 컴퓨터공학과(석사)

2000년~2004년 포항공과대학교 컴퓨터공학과 (박사)

2004년~2006년 Post-Doc., Dept. of ECE, Univ. of Toronto, Canada.

2006년~현 재 고려대학교 컴퓨터정보학과 조교수

관심분야 : 네트워크 관리 및 보안, 트래픽 모니터링 및 분석, 멀티미디어 네트워크

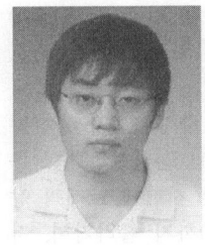


김 성 윤

e-mail : adayslife@korea.ac.kr

1999년~현 재 고려대학교 컴퓨터정보학과 (학사과정)

관심분야 : 네트워크 관리 및 보안, 트래픽 모니터링 및 분석



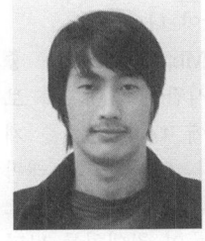
박 준 상

e-mail : runtoyou@korea.ac.kr

2008년 고려대학교 컴퓨터정보학과 (학사)

2008년~현 재 고려대학교 컴퓨터정보학과 (석사과정)

관심분야 : 네트워크 관리 및 보안, 트래픽 모니터링 및 분석



최 경 준

e-mail : mashow@korea.ac.kr

2002년~현 재 고려대학교 컴퓨터정보학과 (학사과정)

관심분야 : 네트워크 관리 및 보안