오늘날 기업의 주요한 비즈니스 프로세스는 네트워크라는 인프라에 의해 인체의 혈관처럼 유기적으로 작동하고 있어 이제 네트워크 관리는 단순 장비 중심이 아니라 데이터 플로우 관리라는 새로운 과제를 안게 됐다. 이에 이번호에는 최근 SNMP의 한계를 넘어선 관리 솔루션으로 새롭게 주목받고 있는 RMON에 대해 살펴보고, 다음 2회에 걸쳐 RMON의 구체적인 구현 사례를 소개한다.

김형태 | htkim@f-net.co.kr
에프네트 네트워크 컨설팅 사업부 대리

RMON으로 데이터 플로우 관리하기

「과」거 전형적인 네트워크 관리는 라우터나 스위치 등의 장비에 대한 가동 여부를 모니터하고, 네트워크 자원에 대한 연결성을 유지하며, 사용자가 네트워크에 정상적으로 연결됐는지를 파악하는 것이었다. 하지만 최근 네트워크 관리는 이같은 장비 중심에서 연결성 중심으로, 그리고 다시금 애플리케이션 중심으로 그 개념이 변화하고 있다.

더구나 애플리케이션과 네트워크를 별개의 것으로 단절시켜서 생각하던 것에서 이제는 유기적으로 연결돼 있음을 인식하기 시작한 것은 네트워크 관리에 있어 주요한 변환점으로 작용하고 있다. 유기적인 결합을 인정하지 못했던 과거에는 비즈니스 사업부에서는 비즈니스 프로세스와 애플리케이션만을, 네트워크 사업부에서는 장비와 장비간의 연결성만을 고려했기 때문에 사용자가 네트워크 애플리케이션의 응답 속도에 불만을 호소할 경우, 네트워크와 애플리케이션 사업부는 각각 자신의 사업부에는 문제가 없다고 주장하기 바빴던 것이다.

이제는 하나의 비즈니스 프로세스를 인식함에 있어, 이들을 상호 연계해서 모니터링하고 이해하려하는 인식이 증대되고 있다.

데이터 플로우를 감당하기에 역부족인 SNMP

현재 네트워크 관리를 위해 가장 많이 사용되고 있는 것은 SNMP 시스템이지만 SNMP는 아래와 같은 한계를 보이고 있다.

✓ 장비 중심의 제한적 관리

SNMP를 지원하는 에이전트들에 대한 관리 정보의 수집 및 분석은 가능하나, 장비의 확장 가능 여부를 결정하기 위한 필요한 단위 세그먼트의 부하 등의 모니터링을 할 수가 없다.

✓ 데이터 흐름 정보의 필요성

일반적으로 장비에서 제공하는 SNMP 기능은 장비의 인터페이스나 자원 상황만을 모니터링하고 정보를 수집한다. 하지만 장비의 특정 인터페이스에 과다한 부하가 걸릴 경우, 대역폭 잠식 원인이 무엇이며, 어떤 호스트에 부하가 걸렸는지 해명하지 못하는 문제가 있다.

✓ 대역폭의 과다 소요

대부분의 관리 시스템은 데이터 수집을 위해 정기적으로 SNMP 폴링을 하는데, 이 트래픽이 WAN을 경유하는 경우 네트워크 속도를 느리게 만드는 주요 요인이 된다. 따라서 관리자는 에이전트의 수나 폴링 간격을 제한할 수밖에 없는데 이 경우, 지속적으로 확장되고 있는 네트워크 환경에서 더욱 빨리 그 한계에 달하게 돼 많은 장비를 관리하기가 곤란하다.

✓ **장비 기능의 저하**

SNMP 에이전트를 갖고 있는 장비는 장비 본연의 임무를 수행하는 동안 에이전트가 트래픽 정보를 분석하는 경우 그 자원의 왜곡이 있을 수 있으며, 충분한 성능을 확보하지 못할 수 있다.

위와 같은 이유로 SNMP만으로는 오늘날의 네트워크를 감당한다는 것은 무리다. 21세기의 비즈니스 백본은 기업 내에서는 부서 간, 그리고 기업 외부로는 공급자와 수요자간의 네트워크 애플리케이션이 상호 연결돼 있다. 단순한 업무 파일 공유로부터 메일 시스템, ERP, e-비즈니스에 이르기까지 다양한 네트워크 애플리케이션이 기업의 경쟁력을 증대시키고 있는 것이다. 이제는 바야흐로 '네트워크는 비즈니스다' 라는 말을 새삼 되새겨볼 필요가 있다.

모든 애플리케이션 데이터는 네트워크를 통해 흐르며, 이는 곧 기업의 비즈니스 플로우와 직접 연계돼 있다. 따라서 아래와 같은 공식이 성립된다.

애플리케이션 데이터 플로우 = 비즈니스 플로우

단기적으로 데이터 플로우 관리는 즉각적인 네트워크 애플리케이션의 성능을 향상하고, 중요한 애플리케이션의 네트워크 사용율을 최적화하는 것이다. 장기적으로는 애플리케이션의 흐름 경향을 분석하고, 기준 정립 및 투자 계획과 효율적인 장비의 운용을 가능케 한다. 데이터 플로우 관리의 주요 사안들은 다음과 같이 네트워크에서 무엇을 언제 어디서 누가 사용하는가를 분석하는 것이다.

- 애플리케이션 모니터링
- 실시간 장애 분리
- 성능 모니터링 및 분석
- 성능 및 용량 계획
- 서비스 레벨 관리
- 정책 입증

복잡하고 기능이 강화된 네트워크를 관리하기 위해서는 전체 네트워크로부터 정보를 수집할 필요가 있다. 여기서 핵심이 되는 것은 컴퓨터나 애플리케이션, 라우터, 브리지, 허브, 모뎀에서부터 이들을 연결시켜주는 네트워크 프로토콜까지 '모든 네트워크 구성요소의 상태와 활동 상황에 대한 정보' 이다.

이 같은 정보를 제공하기 위해 등장한 것이 SNMP(Simple Network Management Protocol)를 표준 프로토콜로 하는 RMON(Remote Monitoring) 장비다.

IETF(Internal Engineering Task Force)는 1990년에 RMON 워킹 그룹을 만들었고, 1991년 11월에 이더넷에 초점을 맞춘 'Remote Network Monitoring Management Information Base' 라는 RFC 1271 표준을 제정했다.

RMON의 핵심은 에이전트와 콘솔

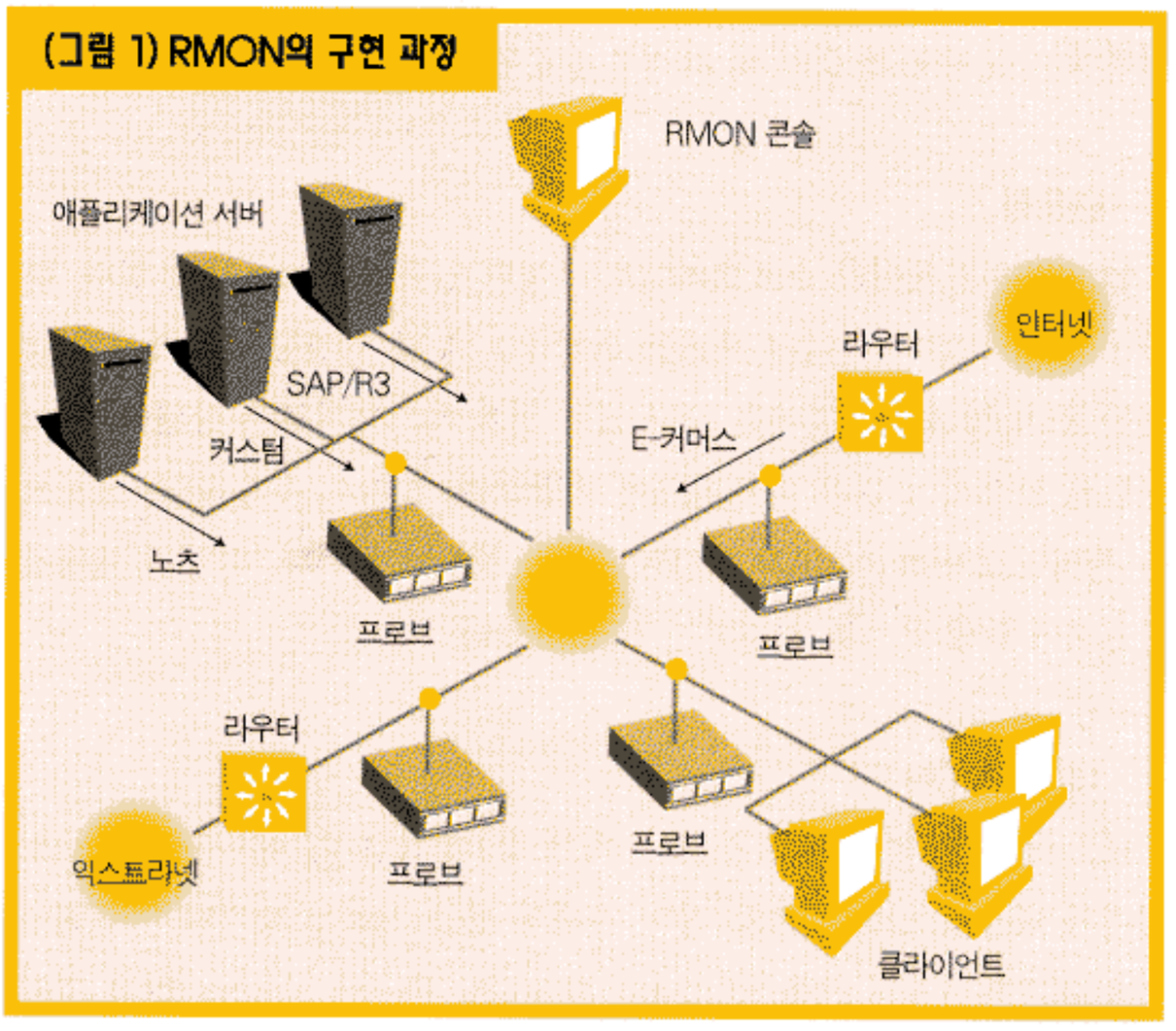
이더넷에 근간을 둔 RFC 1757은 93년 9월에 토큰링을 지원하는 RFC 1513을 포함시켰고, 1995년 2월에 RFC 1271은 RFC 1757로 대체됐다. 이후 94년 7월에 RMON 2 워킹 그룹이 결성, 95년 6월에 RMON 2 초안을 제안했고 97년 1월에 표준으로 제정됐다.

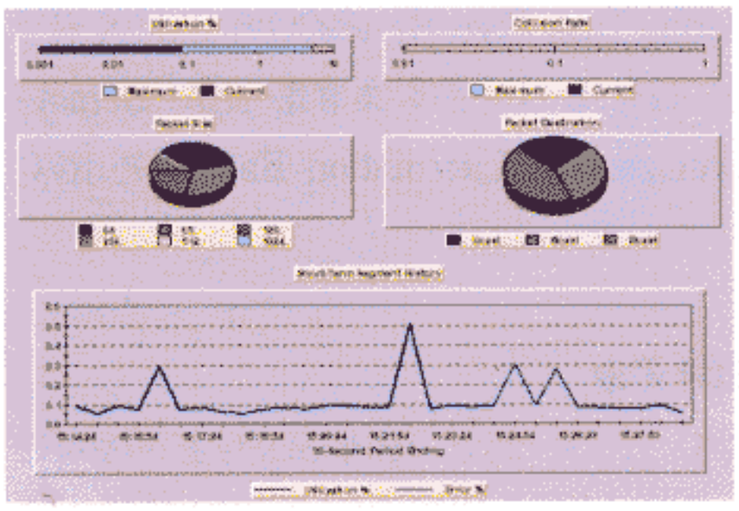
RMON은 표준 SNMP 전송 메커니즘과 명령을 이용해 분산 LAN 환경에 위치한 원격 모니터링 장비가 어떻게 네트워크 데이터를 수집, 저장할 것인지를 규정한 표준이다. 기존의 MIB II는 실제 각 네트워크 장비의 인터페이스에 초점을 맞추고 있기 때문에 LAN 환경의 트래픽 패턴, 애플리케이션 경향 등의 정보를 얻을 수 없다. RMON은 이런 기능을 보강하면서 LAN 프로토콜 분석기의 개념을 확대 발전시킨 것이다.

데이터 플로우 관리를 통한 해결책

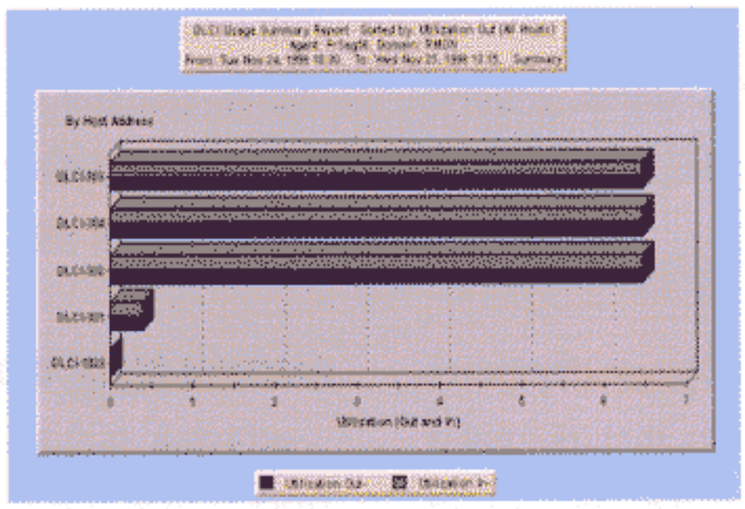
당면 과제	전형적인 관리 측면	데이터 플로우 관리 측면
성능 튜닝	장비 업그레이드	어떤 비즈니스 프로세스가 용량을 필요로 하는가
애플리케이션 응답성	서버로의 핑(ping)	애플리케이션 트래픽 직접적 성능 분석
과금	포트당 산정	사용자, 부서, 애플리케이션, 서버별 산정
용량 계획	더 많은 CIR 확보, 대역폭 확장	사용율 분석 및 대역폭 재할당
서비스 저하	재시도&장애	잘못 설정된 네트워크 애플리케이션 격리
정책 부여	주소별 블로킹	네트워크의 불필요한 사용 방지

(그림 1) RMON의 구현 과정





(화면 1) RMON 통해 실시간 트래픽 경향 분석



(화면 2) RMON로 DLCI 사용량에 대한 보고서를 작성할 수 있다

RMON은 NMS와는 다르게 네트워크에 흐르는 데이터를 측정하는 장비다. 다시 말해, NMS는 네트워크 장비를 대상으로 하는 반면 RMON은 네트워크 트래픽을 대상으로 한다는 것이다. RMON은 네트워크에 어떤 통신 프로토콜들이 있고, 어떤 애플리케이션 데이터들이 흘러다니는지 알려준다.

RMON의 핵심은 RMON 에이전트와 RMON 콘솔이다. RMON 에이전트에서는 요청에 따라 네트워크 상에서 수집한 정보를 RMON 표준에 따라 RMON 콘솔로 전송해 네트워크의 상황을 알려준다.

네트워크 정보를 수집하는 RMON 에이전트는 독자적인 하드웨어로 구성된 프로브(Probe), 네트워크 장비에 내장된 RMON 에이전트, 소프트웨어 RMON 에이전트 등으로 나뉘며, RMON 에이전트를 관리하고 수집된 데이터를 통계 처리해 보여주는 RMON 콘솔 시스템과의 상호 작용을 통해 동작한다(그림 1). 보다 세부적으로 RMON의 구성 요소를 살펴보면 다음과 같다.

먼저 RMON 에이전트는 네트워크 정보를 수집하는 독립 장비인 프로브 또는 라우터, 브리지, 호스트 시스템, 워크스테이션, 허브 등 관리 대상 장비 안에 존재하는 소프트웨어 프로그램을 말한다. 프로브는 일반적으로 RMON 전용 하드웨어를 의미한다. RMON 에이전트는 구현 형태에 따라 다음과 같이 몇 가지로 구분된다.

· 단독형

별도의 하드웨어와 소프트웨어로 구성돼 있으며 프로브로 불린다. 하나 이상의 NIC와 데이터 보관을 위한 RAM 및 고성능 프로세서를 장착한 RMON 소프트웨어를 갖고 있는 전용 하드웨어로 구성된다. 세그먼트의 트래픽이 많은 네트워크에 적합하며, 성능이 우수하다. 프로브는 관리하고자 하는 LAN 세그먼트마다 설치되게 된다. 다양한 매체를 지원하며 다중 포트를 지원하는 제품도 있다.

· 내장 RMON

네트워크 장비(라우터, 스위치, 허브 등)에 RMON 에이전트 소프트웨어가 내장돼 있는 것으로 장비 자체의 성능 저하를 방지하기 위해서 RMON 1의 4개의 그룹(Statistic, History, Event, Alarm)만을 지원한다. Mini-RMON이라고도 불린다.

· 모듈형

네트워크 장비에 삽입하는 형태로 가격은 저렴하나 네트워크 장비 고유의 기능 수행에 영향을 줄 수 있다.

· 소프트웨어 에이전트

네트워크 상에 존재하는 시스템(PC 또는 워크스테이션)에 RMON 에이전트 소프트웨어를 설치해 사용한다. 세그먼트에서 발생하는 트래픽이 적은 네트워크에 적당하다.

관리 시스템인 RMON 콘솔은 RMON 에이전트를 구성하고 수집한 데이터를 처리해 표현한다. SNMP 통신을 이용해 RMON 에이전트로부터 데이터를 수집하고, 이를 처리하고 표현하며 수집된 데이터를 저장한다.

네트워크 계획 수립을 돕는 RMON

RMON 에이전트와 콘솔은 네트워크 상황을 정확히 이해하고 효율적으로 계획을 수립하기 위한 여러 가지 기반 정보를 제공해준다. RMON의 활용으로 아래와 같은 장점을 얻을 수 있다.

· 경향 분석 및 사전예방 감시

특정 세그먼트와 노드 성능에 관한 정보를 얻을 수 있어 경향 분석을 할 수 있다. 이런 분석을 통해서 네트워크의 특정 세그먼트에 존재하는 잠재적 문제를 인지할 수 있다. 네트워크의 성능을 지속적으로 감시하고 기록함으로서 문제 발생시 이를 활용할 수 있고, 이를 발생한 문제의 유형에 연계시켜 이력 자료로 기록, 관리함으로써 유사 문제 발생시 진

(그림 2) RMON 지원 계층

단용 자료로 활용이 가능하다.

· 멀티 프로토콜/멀티 토폴로지 지원

RMON은 프로토폴 계층 구조에 따른 멀티 네트워크 프로토콜 및 애플리케이션을 지원함으로써 다양한 사용자 환경에 즉각적으로 적용 및 구현이 가능하다. RMON 벤더들은 이더넷, 토큰링뿐만 아니라, 프레임 릴레이, WAN, ATM, 기가비트 이더넷 등의 다양한 토폴로지를 지원하고 있다.

· 장애 검출 및 보고 기능

장애 조건을 설정해 이에 대한 조건이 만족되면 해당하는 이벤트를 저장하고 여러가지 방법으로 관리자에게 경보를 전달한다. 예를 들면, 해당 세그먼트의 장애 횟수나 사용율이 일정 수준을 초과하면 관리자에게 경보를 전달한다.

· 네트워크의 재배치 및 확장에 도움

네트워크 성능의 변화 및 병목 발생을 조기에 감지함으로써 네트워크의 재구성 필요 여부를 판단할 수 있으며, 분산된 세그먼트에서 장비를 효율적으로 재배치하는데 도움을 준다. 또한 신규 장비의 추가 확장 시 해당 세그먼트의 대역폭 소요량을 계산하고 신규 장비의 추가로 인한 영향을 파악하는데 도움을 준다.

· 네트워크 계획 수립

네트워크 성능의 변화를 사전에 인식함으로써 네트워크의 구성 변경이 필요한 지 결정할 수 있다. RMON은 또한 분산된 세그먼트에서 장비를 효율적으로 재배치하는데도 도움이 된다. RMON은 최적의 서버를 결정하거나, WAN 대역의 소요량을 파악하고, 신규 네트워크 애플리케이션의 추가로 인한 영향을 파악하는 데 도움을 준다.

RMON 1 MIB의 세부 사양

IETF는 MIB의 표준화를 통해 RMON MIB을 개발했으며, 이더넷과 토큰링에 대한 표준을 제공하고 있다. 현재 19개의 RMON MIB 그룹을 통해서 RMON 에이전트는 이더넷과 토큰링 세그먼트 상의 패킷과 트래픽 정보를 수집하고, 이 정보를 RMON 콘솔로 전송하게 된다.

RMON MIB에서는 정보수집에 대한 표준을 정의하지만, 수집된 정보의 표현 방법은 규정하지 않고 있다. RFC 1757(이더넷)과 RFC 1513(토큰링), RFC2021(RMON 2)을 OSI 참조 모델과 비교해서 구분해 보면 RMON 1 그룹은 2계층까지만 지원을 하며, RMON 2 그룹이 3계층 이상을 지원한다. RMON 1 MIB의 주요 내용을 살펴보면 다음과 같다.

· 통계(Statistics)

한 세그먼트 내에서 발생한 패킷/바이트 수, 브로드캐스트/멀티캐스트 수, 충돌(collision) 수, 패킷 길이별, 각종 오류(프레그먼트, CRC-Alignment, jabber, 길이 미달, 길이 초과)에 대한 통계를 제공한다.

· 이력(History)

관리자가 설정한 시간 간격 내에 발생한 각종 트래픽 및 오류에 대한 정보를 제공한다. 기본적으로 단기/장기적으로 간격을 설정가능하고 정해진 시간 간격으로 샘플링한다. 이 자료를 통해 시간대별 이용 현황 및 다른 세그먼트와 비교가 가능하다.

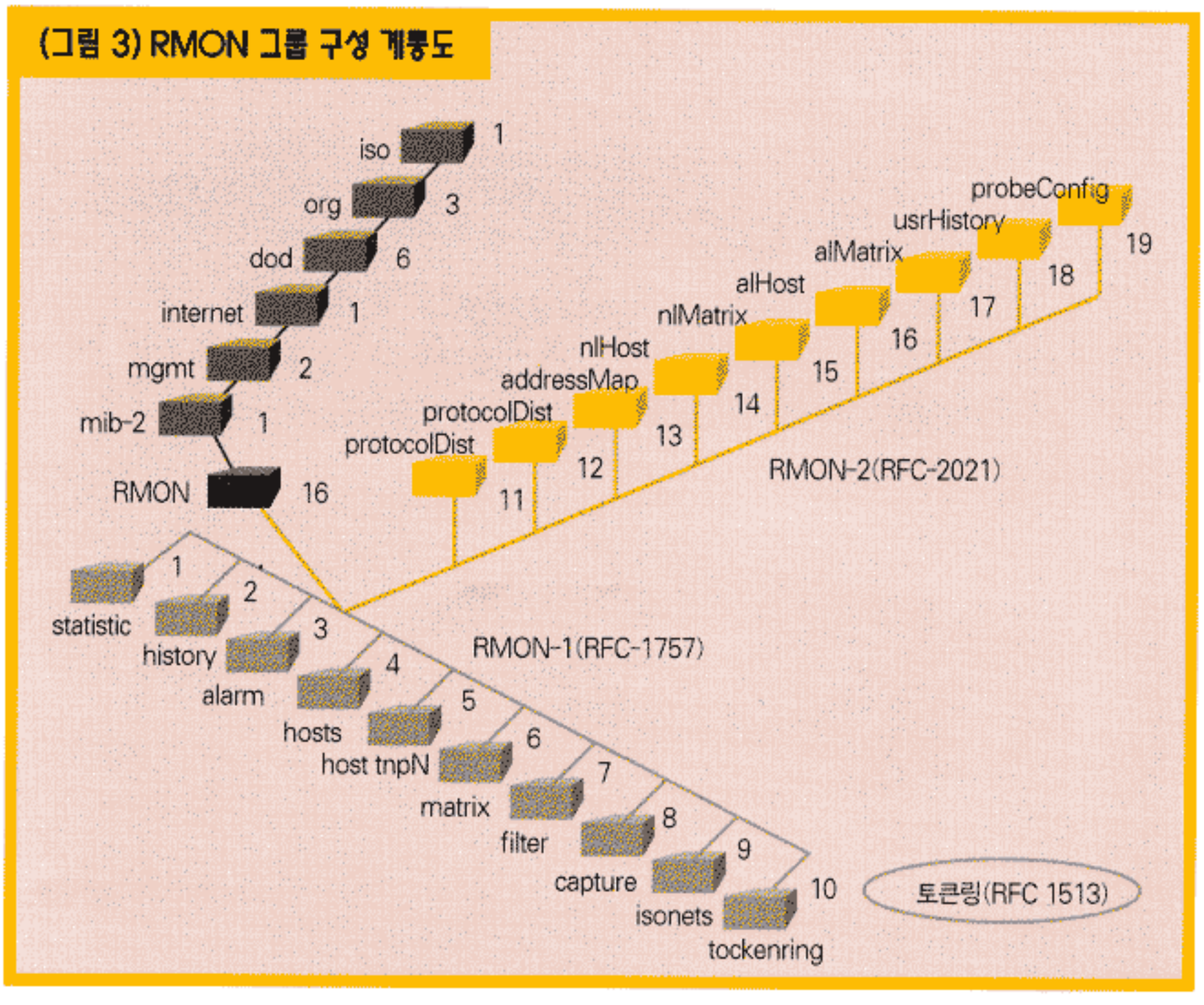
· 경보(Alarm)

에이전트는 주기적으로 특정한 값을 체크해서 기준치(임계치)에 도달하면 관리자에 보고한다. 기준치는 절대값 및 상대값으로 설정이 가능하며, 계속적인 경보 발생을 막기 위해서 상/하한치를 설정해서 넘나드는 경우에만 경보가 발생한다.

· 호스트(Host)

세그먼트에 연결된 각 장비가 발생시킨 트래픽, 오류수를 호스트별로 관리한다. RMON 1에서의 호스트는 MAC 주소로 표시된다.

(그림 3) RMON 그룹 구성 계통도



· **상위 N개의 호스트(Host Top N)**

호스트 테이블에 발견된 호스트 중에서 일정시간 동안 가장 많은 트래픽을 발생시킨 호스트를 상위 N개로 찾는다. 관리자는 원하는 종류의 자료(입/출력 패킷, 바이트, 오류, 브로트캐스트/멀티캐스트 패킷)와 시간 간격 및 원하는 호스트의 개수를 설정해서 정보를 얻을 수 있다.

· **매트릭스(Matrix)**

데이터 링크 계층, 즉 MAC 어드레스를 기준으로 두 호스트 간에 발생한 트래픽 및 오류에 대한 정보를 수집한다. 이 정보를 이용해서 특정 호스트에 가장 많은 이용자가 누구인지를 어느 정도는 알 수 있다. 다른 세그먼트에 있는 호스트가 가장 많이 이용했다면 이것은 주로 라우터를 통과하는 것으로 실제 이용자는 알 수 없다.

· **필터(Filter)**

관리자가 특정한 패킷의 동향을 감시하기 위해서 이용한다. 이를 이용해서 특정패킷의 발생여부를 알 수 있고 경보와 사건 기능을 이용해서 한계치 이상 발생을 알 수가 있다.

· **패킷 수집(Capture)**

세그먼트에 발생한 패킷을 수집해서 관리자가 분석할 수 있도록 한다. 관리자는 수집/추적할 패킷의 형태와 버퍼 사이즈를 지정할 수 있으며, 수집한 패킷의 전부 또는 일정한 길이만 보관하고 읽을 수 있도록 설정이 가능하다.

RMON으로 무엇을 할 수 있는가

1. 요구사항 분석

▶토폴로지 분석 : 주요 WAN 백본 체계, 주요 LAN 백본 체계, 데이터 센터의 네트워크 체계

▶지역적 분석 : 사이트 수와 가용한 보유 기술 수준, 각 사이트마다의 가용한 관리 자원

▶애플리케이션 적용 분석 : 어떤 애플리케이션들에 대해서 콜이 많은가

2. 우선 순위 선정

토폴로지가 다양하므로, 항상 우선 순위를 분류해 진행한다.

▶1순위 : WAN 백본, LAN 백본, 서버 밀집 지역

▶2순위 : 중요한 지역 거점 및 사이트

▶3순위 : 소규모 지역 사무소나 지점

3. 문제해결을 위한 운영

▶목적 : 사전 장애 검출 및 빠른 복구

▶대상 : 업무 중대 트래픽을 전송하는 회선, 많은 컨버세이션 수를 갖는 회선, 적합한 지원 인력이 부족한 사이트, 장애 이력이 있는 회선이나 사이트, 적용 후에 임계치를 설정하거나 보정

4. 용량 산정을 위한 운영

▶목적 : 현재와 미래의 투자를 정당화

▶대상 : 최고의 대역폭을 사용하는 회선, 많은 컨버세이션 수를 갖는 회선, 응답 지연 요구가 있는 사이트나 서버, 장애 이력이 있는 회선이나 사이트

5. WAN 서비스 레벨 관리를 위한 운영

▶목적 : 실제 사용값을 근거한 서비스 사전 관리

▶대상 : 외부 서비스(업무상 중요한 트래픽을 전송하며 서비스 제공자로 연결돼 있는 회선, 많은 컨버세이션 수를 갖는 회선), 내부 서비스(비즈니스 기반의 애플리케이션이 집중화되는 사이트,주요한 서버들이 있는 백본, 적합한 네트워크 지원 인력이 부족한 사이트, 장애 이력이 있는 회선이나 사이트)

6. 애플리케이션 모니터링을 위한 운영

▶목적 : 애플리케이션 성능 사용자 관점에서 적용

▶대상 : 중요 애플리케이션 및 데이터베이스 서버로 연결된 회선, 사용자 사이트(중요도, 사용자 밀집도, 지리적 위치에 따라 선택, 서버와 사용자에서의 애플리케이션 응답 측정 적용), 중요 업무 애플리케이션 트래픽을 전송하는 회선(서비스 사용자 수에 따라 선택), 장애 이력이 있는 회선이나 사이트

7. 데이터 플로우 관리에 있어 RMON의 계층적 운용(그림)

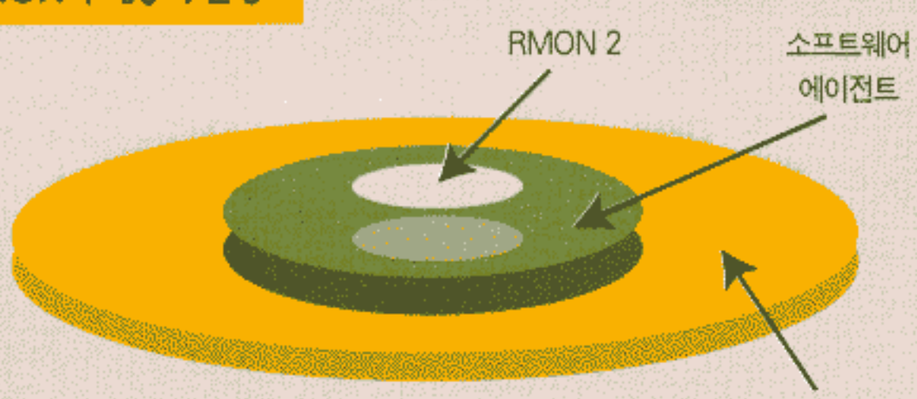
▶업무 중요 요소에 대한 기준 적용

▶RMON2는 프로브를 통해 업무상 중요하거나 최우선 회선에 적용해 상세한 트래픽 데이터를 산출

▶소프트웨어 에이전트는 2, 3순위에 적용하며, 원거리 지점 경우에 경제적으로 운용이 가능하다.

▶임베디드 RMON은 네트워크 장비에 내장돼 있는 기능을 사용하는 것으로, 장비 성능에 영향을 주지 않은 범위내에서 효과적으로 운영이 가능하며, 모든 순위에 적용이 가능하다.

RMON의 계층적 운영



· 사건(Event)

일정한 사건이 발생하면 그 기록을 보관하고 관리자에게 경고 메시지를 보낸다. 트랩 발생 및 기록 보관은 선택 사항. 경보와 연관돼서 사건이 발생하면 사건 기록 및 트랩 발생은 관리자가 사전 설정할 수 있다.

RMON 2 MIB의 세부 사양

기존의 RMON1은 문제 해결과 성능 감시를 위해 데이터 링크 계층의 상태와 성능 정보를 제공하는 반면, RMON 2는 네트워크 계층 이상의 데이터를 관리함으로써 관리 범위를 단위 세그먼트에서 엔터프라이즈 네트워크까지 확장해 전체 네트워크를 살펴볼 수 있게 한다. IETF는 RMON 2표준을 RFC 2021에 정의했으며, 모두 9개의 그룹으로 구성돼 있다. 세부 항목은 다음과 같다.

· 프로토콜 디렉토리

프로토콜들의 목록을 리스트하고, 이들의 상관관계를 정의한다. 이 리스트내의 엔트리들을 프로브에서 감시할 수 있으며 추가, 삭제, 구성이 가능하다. 예를 들면, HTTP 프로토콜은 RMON〉IP〉TCP의 상위 객체로 존재한다.

· 프로토콜 분포

네트워크 세그먼트의 트래픽을 상위의 프로토콜 디렉토리에 근거해 수집한다. 주어진 세그멘트내에서 네트워크 및 애플리케이션 프로토콜별로 트래픽 비율을 추적할 수 있다.

· 주소 매핑

MAC 주소를 네트워크 주소로 매핑하고 해당 주소들의 최종 인터페이스가 무엇인가를 알려준다.

· 네트워크 계층 호스트

네트워크 주소별 송/수신한 트래픽 양을 계산한다. 네트워크 계층 차원의 호스트별 패킷, 에러, 바이트 수를 추적한다.

· 네트워크 계층 매트릭스 테이블

각 쌍별 네트워크 주소 사이에서 전송된 트래픽을 산출한다. 네트워크 계층 프로토콜에서 서로 통신하고 있는 호스트의 다른 한 쌍(예를 들어 IP로 통신하는 두 호스트간의 대화)을 추적해 통계를 제공한다.

· 애플리케이션 계층 호스트

애플리케이션별로 각 네트워크 주소에서 송/수신한 트래픽 양을 계산한다. 애플리케이션 계층(HTTP, 텔넷, 노츠 등)에서의 호스트별 패킷, 에러, 바이트 수를 추적한다.

· 애플리케이션 계층 매트릭스

애플리케이션별로 각 쌍의 네트워크 주소 사이에서 전송된 트래픽 양을 계산한다. 애플리케이션 계층에서 호스트간의 쌍(예를 들어, HTTP 정보를 교환하는 두 노드간의 대화)을 추적해 통계를 제공한다.

· 프로브 구성

원격으로 프로브를 구성하기 위한 운용값(에러 트랩 전송, 프로브 통신 방법, 프로브에 의한 데이터 로드 방법 등)을 정의한다.

· 사용자 이력

경고(Alarm)와 이력(History) 기법을 결부시켜 사용자가 정의한 이력을 수집한다. 사용자가 정의한 RMON 2 변수에 대해 일정시간 동안의 통계를 수집해 저장한다.

용어설명

● **SNMP**
Simple Network Management Protocol. TCP/IP 환경에서의 네트워크 관리 프로토콜. SNMP는 SNMP 에이전트와 SNMP 매니저로 구성돼 있는데, SNMP 에이전트는 SNMP 매니저에 관리 장비에 대한 MIB(Management Information Basement) 정보를 제공한다. SNMP 에이전트는 모두 관리 대상 시스템 상에 있으면서 매니저에 MIB에 대한 정보를 제공하게 된다.

● **RMON**
Remote Network Monitoring. 원격지에서 네트워크 상의 트래픽 정보를 수집, 분석하기 위해 제안된 표준. RMON은 SNMP에 의해 획득되고 사용되는 관리 정보를 보충하기 위해 설계됐으며, 정보를 수집하는 에이전트와 분석 관리를 담당하는 매니저로 구성돼 있다.

● **RMON 2**
Remote Network Monitoring 2. 네트워크 계층의 패킷을 추적할 수 있는 등 기능을 향상한 RMON. MAC층을 넘어 네트워크 애플리케이션 계층까지 적용 범위를 넓힘으로써 인터네트워크 장비의 물리적 연결과 프로토콜 애플리케이션 또한 트래킹할 수 있다. 네트워크 관리자들은 RMON 2를 통해 트래픽을 TCP/IP나 SNA 같은 프로토콜과 전자우편 애플리케이션으로 분리할 수 있어 전송을 정지하고 네트워크 성능에 장애가 되는 요인을 알아낼 수 있다.

● **CIR**
Committed Information Rate. 프레임 릴레이 서비스 업체가 서비스 사용자에게 제공하는 최대한의 대역폭 보장값.

● **console**
콘솔. 컴퓨터 시스템의 관리자가 시스템의 상태를 알아보거나, 각종 업무를 처리하기 위해 사용하는 단말 장치. 이는 보통의 단말기와 유사하나 CPU에 직결돼 여러 특수 기능을 수행하며, 대개 컴퓨터의 본체와 가까운 곳에 설치된다.

● **MIB**
Management Information Base. RAID 기술을 기반 등장한 스토리지 표준 중 하나. EMC의 후원을 받는 광섬유 연맹에서 제안했으며 IETF에 제출됐다. MIB는 이기종 스토리지 장비 간에 정보를 모으는 방법을 제공하며, 이들을 단일 관리 콘솔에서 관리할 수 있다.