지난호에는 RMON의 기본 개념과 기술에 대해 소개했다. 이번호에는 RMON을 LAN 환경에서 활용하는 방안에 대해 소개한다. 특히 이해를 돕기 위해 두 가지 활용 사례를 통해 상황별로 RMON을 적용하는 과정과 방법, 적용 결과를 알아본다.

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

사례로 본 LAN 환경에서 RMON의 활용

「현」재 기업 네트워크에는 다양한 토폴로지가 공존하고 있으며, 대역폭, 네트워크 및 애플리케이션 응답시간 증대를 위해 스위치 장비의 적용이 보편화됐다. 스위치는 네트워크 세그먼트 수를 증가시키고, 세그먼트 당 사용자 수를 감소시키고, 각 사용자별로 가용 대역폭을 증대시키는 역할을 한다.

근래의 LAN 모니터링은 스위치 환경 하에서의 모니터링이라 해도 과언이 아니다. 우선 네트워크 토폴로지별로 어떻게 모니터링할 것인가를 알아보자.

· 공유 LAN에서 네트워크 모니터링

공유 매체 LAN에서 데이터 플로우 모니터링은 해당 세그먼트에 RMON 프로브(Probe)를 연결함으로써 간단히 구현될 수 있다. 프로브와 매니저 콘솔 간의 관리 데이터가 실제 데이터 플로우에 섞이지 않도록 별도의 관리 네트워크를 운영할 수 있다.

· 스위치 LAN에서 네트워크 모니터링

스위치 네트워크의 주요한 두 가지 이점인 마이크로 세그먼테이션과 가상 LAN 기능들은 문제해결을 위한 네트워크 모니터링과 계획 목적에 필수적이다.

· 마이크로 세그먼테이션에서의 모니터링

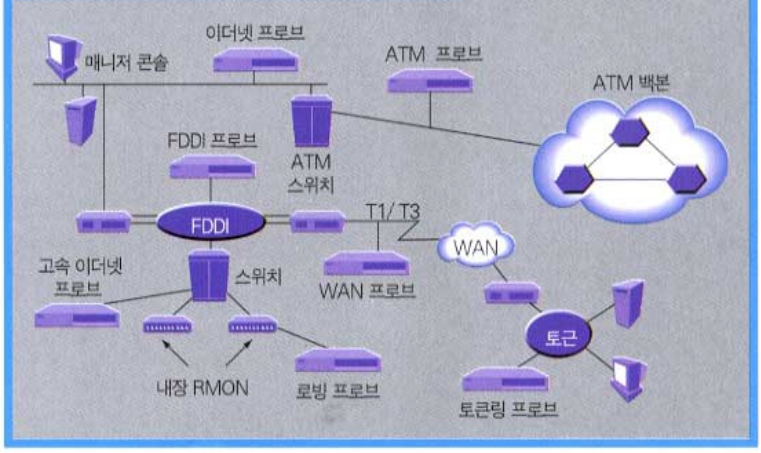
스위치 LAN에서는 각 스위치 포트가 독립적인 브릿지로 작동하기 때문에 세그먼트 수는 훨씬 많아지게 되고, 스위치와 서버들은 고속의 포트에 위치하게 된다. 서버들은 전이중 포인트 투 포인트로 연결이 되고, 고성능의 프로브를 필요로 하게 된다. 이를 위해 미니-RMON(Mini-RMON), 로빙(Roving), 전이중 모니터링을 효율적으로 활용할 수 있다.

· 가상 LAN에서의 모니터링

가상 LAN은 네트워크 토폴로지를 간단하게 통합하는 기술이다. 소프트웨어 제어를 통해 가상 LAN은 동일 가상 LAN 사용자들에게 브로드캐스트를 제한하지만, 다른 가상 LAN과의 통신을 위해서 라우터가 필요하다.

연재순서
1. RMON 기본 개념과 기능 (2001년 4월)
2. 사례로 본 RMON 활용 I LAN 진단(2001년 5월)
3. 사례로 본 RMON 활용 II WAN 진단(2001년 6월)

다양한 LAN 토폴로지에서의 모니터링 장비 구성



최근 가상 LAN의 사용이 증대되면서 트래픽 분석의 필요성이 증가하고 있다. 가상 LAN 구성의 튜닝을 위해 가상 LAN 트래픽 패턴을 아는 것은 중요하다. 예를 들어, 네트워크를 구성하고 관리하는 데 있어 가상 LAN 호스트 리스트와 사용률은 아주 중요한 툴이라는 것이다.

가상 LAN에 의한 트래픽을 수집하기 위해서 RMOM 프로브는 현재의 가상 LAN 그룹을 확인하기 해야 하며 또 스위치간 트래픽을 모니터링 할 수 있어야 한다.

고속 스위치와 서버간 연결시 RMON의 적용

스위치간의 연결은 스위치 LAN 네트워크의 백본이 된다. 백본은 업무상 아주 중요하며 대량의 데이터 트래픽이 집중된다. 백본의 효과적인 운영은 분산 컴퓨팅 환경의 주요 초석의 하나다. 스위치간의 연결은 전형적으로 고가이며, 고속/대량 데이터 전송을 지원한다. 빠른 네트워크 응답과 유연한 네트워크 성능을 위해 스위치간을 모니터링하는 것은 필수적이다. 만약, 백본에 장애가 발생한다면 네트워크 전체가 영향을 받을 것이다.

대부분의 스위치 장비는 고속의 포트를 서버나 백본에 연결하기 위해 사용된다. 따라서 대부분의 서버들은 스위치에 직접 연결돼 있으며, 서버 링크에 장애가 발생했을 때 분산환경에서는 영향이 적지만, 실질적으로는 네트워크에서 전체적으로 서버의 연결이 단절되게 된다. 다시 말해 서버가 중앙에 위치한 경우는 서버의 연결성은 전사적으로 영향을 미친다는 것이다.

스위치간의 연결이나 서버 연결은 모든 문제를 발견하고 해결하는 것으로는 부족하다. 공유 환경에서는 네트워크 전체에 영향을 미칠 수 있는 높은 사용률의 세그먼트 문제는 예방할 수 있으며, 잠재적 문제는 RMON을 통해 발견할 수 있다.

스위치간이나 서버 연결에서 RMON2의 분석은 어떤 네트워크 애플리케이션이 사용되며, 어느 정도의 대역폭을 사용하고 있으며, 누가 사용하고 있는지 알 수 있다. 전용의 RMON2 프로브는 와이어 스피드에서 전이중 전송을 모니터링할 수 있다.

전이중의 고성능 RMON2 프로브는 트래픽 부하를 수용하며, 트래픽 패턴을 송수신으로 구분한다.

예를 들어, 네트워크 관리자는 전체 사용량을 볼 수 있으며, 관심에 따라 송신 트래픽만 볼 수도 있다. 이것은 스위치간을 연결할 경우 혼잡 발생시 어떤 스위치로부터 발생된 트래픽인지 알 수 있는 장점이 있다. 그러한 정보로부터 네트워크 관리자와 사용자들은 다른 스위치나 가상 LAN으로 재설정할 수 있다.

RMON 솔루션은 스위치 LAN 환경에서 관리와 모니터링을 위한 경제적인 전략을 제공하고 있다. 스위치 내장 미니i-RMON, 로빙 RMON, 전용 프로브, 고속의 전이중 프로브, 확장된 관리 소프트웨어는 광범위한 기업 네트워크의 가시성을 제공한다.

(사례 1) 네트워크의 콜리전 장애 발생

국내 한 의료 기관에서 노후한 네트워크를 업그레이드해야 할 필요성은 느끼지만, 어떤 문제점 때문에 업그레이드해야 하는지를 정확하게 파악하지 못하고 있었다. 이를 RMON 장비를 이용해 네트워크의 정확한 상황을 알아내고, 현재의 문제점을 이해하고 발전 방향을 모색할 수 있었다.

각종 장애 내역이나, 부족한 대역폭 수준과 지점, 엔터프라이즈 RMON을 통한 추가적인 객관적인 자료를 수집함으로써 업그레이드 방향과 필요한 장비를 적정하게 산정할 수 있었다.

A. 상황

백본은 FDDI로 구성돼 있으며, FDDI는 전산실과 사용자층 사이가 라우터로 연결돼 있다. 사용자편 라우터는 층내 메인 허브로 연결됐고, 증설된 사용자들을 위해 추가의 허브를 메인 허브에 스택해서 서비스를 하고 있다. 사용자들은 때때로 늦은 네트워크 응답을 호소하며, 네트워크 관리자는 네트워크 장비의 업그레이드나 교체를 고려하고 있지만, 이를 입증할 명백한 객관적인 데이터가 필요했으며, 필요한 장비의 성능이 고려의 대상이었다.

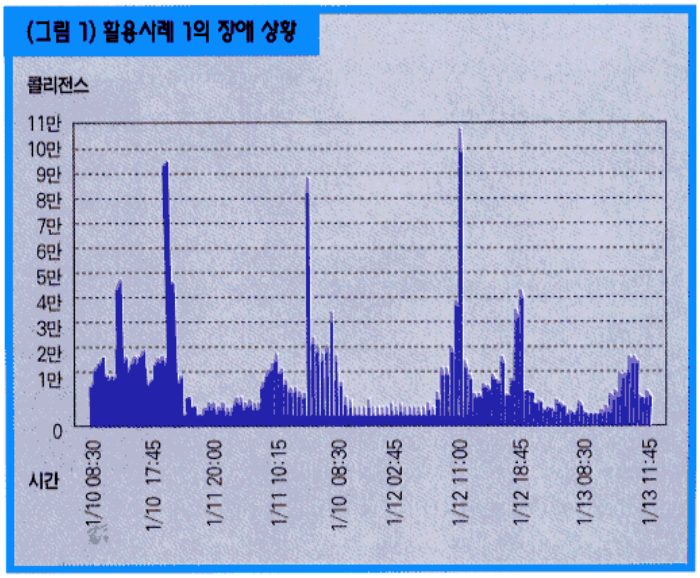
B. 당면 과제

- 네트워크의 현 상태 파악 및 발전방향 제시
- 네트워크 업그레이드시, 고려사항 제시

C. RMON의 적용

공유 이더넷에서의 RMON 적용은 간단하게 구현됐다. 네트워크 관리자의 관심은 사용자 네트워크였으며, 우려되는 사용자 네트워크 세그먼트를 선정했다. 해당 세그먼트에 프로브를 설치하고, RMON 설치로 인한 추가의 트래픽 발생 방지를 위해 프로브와 매니저 콘솔을 직접 연결했다.

(그림 1) 활용사례 1의 장애 상황



D. 결과

네트워크 상태

· 대역폭 사용률

10Mbps 공유 이더넷의 사용률은 업무시간대 평균 10~15% 수준이며, 가장 혼잡할 때 50%를 상회하고 있다. 이것은 통상적인 이더넷의 사용률 권고치를 평균 40% 이하 수준으로 본다면 사용률은 그다지 많지 않다고 볼 수 있다. 다만 매일 일정시간대에 피크가 발생하므로, 호스트 보고서나 애플리케이션 보고서를 통해 어떤 호스트들이 어떤 애플리케이션으로 대역폭을 많이 사용했는지 추적함으로써, 이들에 대한 네트워크 서비스를 보장해 줄 수 있다.

· 장애 상황

주요 네트워크 장애는 콜리전(Collision) 발생이었으며, 업무 시간에 대략 1만~2만개/15분당 발생했다. 피크시에는 11만개/15분을 상회했다. 콜리전(Collision)은 LAN의 CSMA/CD 메커니즘에 기반한 공유 매체를 여러 호스트가 동시에 사용했을 때 발생하는 데이터 충돌을 의미한다.

해당 세그먼트에서는 평균 40만 패킷/15분이 발생했으며, 40개 프레임이 전송될 때, 대략 1~2개는 충돌이 발생돼 재전송 된다.

통상적인 콜리전 권고치가 전체 트래픽의 0.1% 이하 수준을 기준으로 본다면 상당히 높은 콜리전이 발생한다고 볼 수 있다.

· 호스트 상황

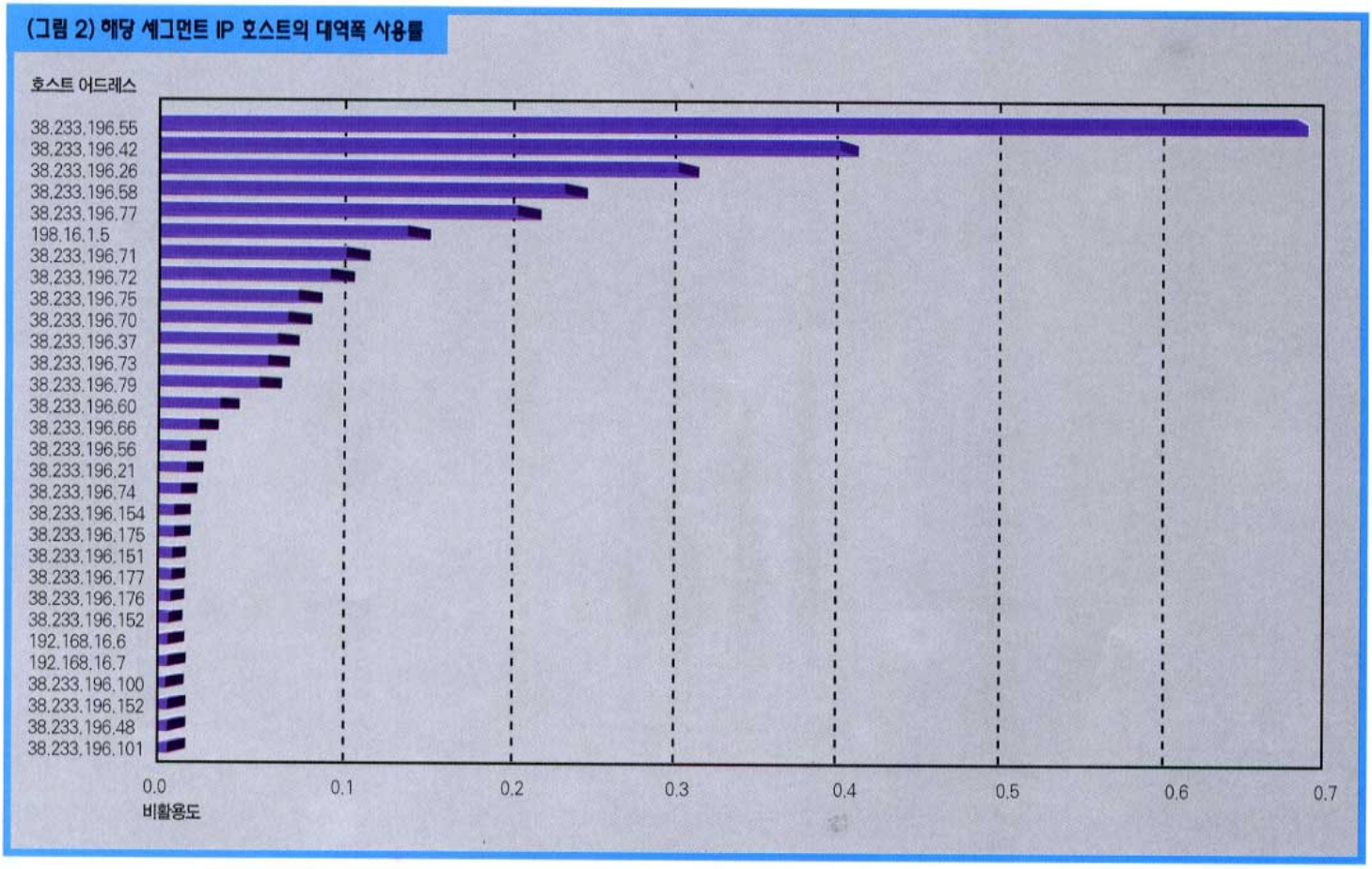
(그림 2)는 해당 세그먼트의 IP 호스트를 대역폭 사용률 순으로 정리한 것이다. 대부분의 네트워크 데이터가 몇몇의 특정 호스트가 점유하고 있다는 것을 파악할 수 있다. 해당 IP 호스트는 업무 서버거나 사용률이 많은 단말일 것이다.

이들 호스트들이 업무 관련 트래픽의 발생 여부는 애플리케이션별 호스트 보고서나 호스트 매트릭스 보고서를 통해 재검증할 수 있다. 이들 정보를 통해 향후, 네트워크를 구성함에 있어 우선 순위의 네트워크 서비스가 가능해 질 것이다.

관리자는 데이터 플로우를 인식함으로써 네트워크의 상황을 선명히 이해할 수 있다. 현재 네트워크의 사용률 및 에러 경향, 호스트별 경향, 애플리케이션별 사용률과 호스트 경향 등의 정보를 이해함으로써 네트워크 서비스의 어떤 부분에 초점을 둬야 할지 판단 자료가 생기게 된 것이다.

우선 네트워크에서 발생하는 대부분의 에러인 콜리전을 줄이기 위해

(그림 2) 해당 세그먼트 IP 호스트의 대역폭 사용률



서는 콜리전 도메인을 시급히 축소해야 했고, 네트워크 담당자는 공유 이더넷을 스위치 이더넷으로 전환함에 있어 당위성을 갖게 됐다. 대역폭 사용률이 이더넷 기준으로 10~15% 수준이고, 특성 호스트나 애플리케이션이 많은 트래픽을 유발하기 때문에, 향후 애플리케이션 도입을 감안해 신규 장비 선정 및 도입, 장비 재배치 계획의 수립이 가능하게 됐다.

(사례 2) 네트워크의 성능 저하

북미 금융권의 한 업체에서 사옥 이전이 예정돼 있었는데, 금융권 업무의 특성상 네트워크 전체가 한꺼번에 정지돼서는 안되기 때문에 서버나 PC를 단계적으로 이전하기 위한 방법을 RMON 장비를 통해 계획했다. 즉, 특정 사용자들이 주로 사용하는 서버를 하나로 묶어서 옮기고 그 그룹이 기존의 본사 네트워크와 연동되면서 작업을 진행하고 또다른 그룹이 다시 이전했다. 이때 신 사옥과 구 사옥간의 WAN 대역폭도 조절하면서 진행하게 됐다.

A. 상황

주요 조직(1000명의 컴퓨터 사용자와 100개의 FDDI 기반 서버)을 신사옥으로 이전 계획 수립시, IT 부서가 직면한 과제는 명백했다. 4단계에 걸쳐 일어나는 이전동안 새로운 장소로 이전한 사용자나 이전을 기다리는 사용자들 모두

RMON이 정의하는 4가지 핵심 요소

광범위하고 경제적이며 자원 효과적인 방법으로 데이터 플로우의 모니터링과 문제해결, 네트워크에 대한 전반적인 리포트를 제공하기 위한 RMON 기술은 아래의 4가지 요소를 정의하고 있다.

· 미니-RMON

RMON1 표준의 통계(Statistics), 이력(History), 경보(Alarm), 이벤트 그룹은 스위치의 각 포트에 내장돼 있다. 미니-RMON은 지속적으로 스위치의 모든 포트에 대해 비정상적 상태에 대한 알람을 포함한 네트워크 상태를 모니터링한다. 미니-RMON은 풀-RMON(Full-RMON)과는 달리 스위치의 자원에 영향을 주지 않는 범위 내에서 작동하도록 축소돼 구현됐다. (그림 1)은 RMON 매니저 콘솔을 통해 스위치 에이전트를 포트별로 모니터링하는 것을 보여주고 있다.

· 로빙 RMON

스위치가 프로브와 연결돼 있는 분석 포트로 모니터링 포트의 패킷을 복제하는 기능을 말한다. 로빙 RMON은 미니-RMON 기반의 MAC 계층 이상을 프로브를 통해 7계층을 자세히 분석할 수 있는 장점을 제공한다. 로빙 RMON을 이용해 네트워크 관리자는 스위치의 어느 포트라도 스위치에 연결돼 있는 외부의 RMON2 프로브를 제어할 수 있다.

이것은 알람의 소스 포트를 필요할 때만 풀-RMON을 사용하기 때문에 리소스, 메모리, CPU 등의 자원의 효율적인 사용을 가능하게 한다. 연결된 외장의 RMON 프로브는 강력한 풀-RMON 기능을 통해 수준 높은 분석 가용성을 제공하게 된다.

· 풀-RMON2 프로브

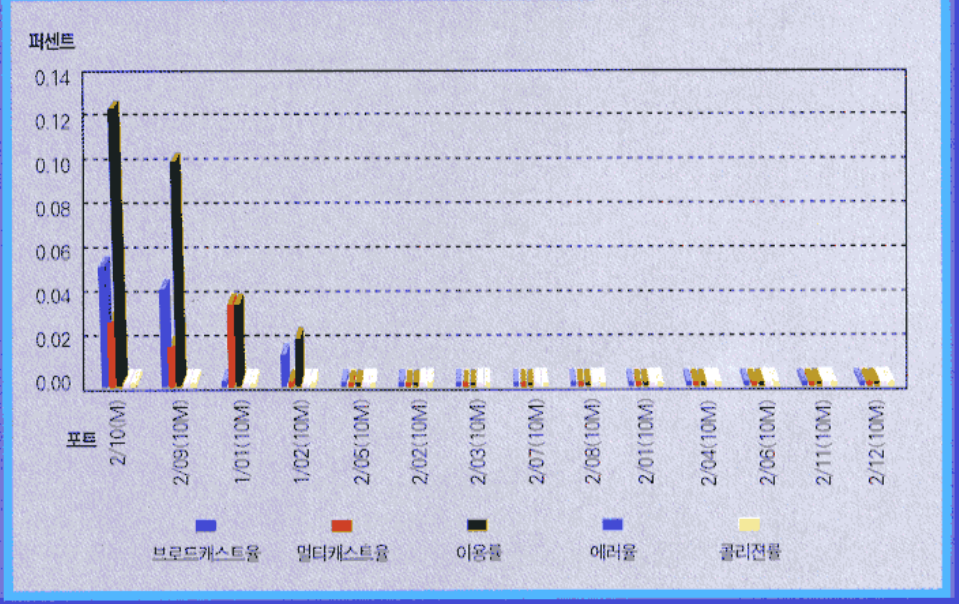
이더넷은 18개의 그룹과 토큰링은 19개의 RMON2 MIB 그룹을 지원한다. 이것은 미니-RMON의 4개 그룹보다 현저히 증가된 능력이다. 이런 그룹들은 풍부한 데이터 리소스를 제공한다. 프로브는 와이어 스피드로 패킷의 손실 없이 프로토콜을 분류하고, 호스트 주소를 호스트나 호스트 매트릭스 테이블을 만들기 위해 출발지/목적지별로 인식할 수 있어야 한다. 대부분의 스위치 장비에서 이런 작업은 프로세서나 메모리 자원을 과도하게 사용하게 된다. 고속의 RMON2 프로브는 대부분의 사용자 트래픽이 집중하는 중요한 스위치간이나 서버의 연결을 모니터링 한다. 높은 대역폭 수준이나 중요한 연결성으로 인해, 이런 링크들은 100Base-T나 FDDI, 기가비트 이더넷으로 구현된다. 고속의 RMON2 프로브는 가상 LAN 트래픽의 데이터를 수집할 수 있다.

· RMON 매니저 콘솔

확장 네트워크 관리 애플리케이션으로, 다음과 같은 요소들이 구현된다.

- 미니-RMON 에이전트로부터 알람 경고 수신
- 스위치에 패킷 미러링(Roving RMON) 설정
- 프로브에 수신된 패킷 분석을 위한 설정
- 사용자로 하여금 명확한 보고서 산출

미니-RMON의 스위치 에이전트를 포트별로 모니터링한다.



네트워크의 성능 저하를 용납하지 않는다는 것이다. 뉴욕을 근거로 한 시장 중개인들은 매일 정해진 시간 내에 수백만 달러를 처리하는 거래에 있어 네트워크로부터의 응답시간 지연은 묵인할 수 없는 일이었다.

B. 당면 과제

- 네트워크 중단 없이 새로운 건물로의 이전
- 현존 트래픽의 빠른 측정과 고대역폭 사용자를 쉽게 구분하는 것

C. 해결책

RMON 기술

D. 결과

사옥 이전간 네트워크는 최고치의 성능을 수용하고, 네트워크 관리자는 건물간의 대역폭 투자를 최소화했다.

· 이전 방법 결정

관리자는 두 가지 상대적 방법을 고려했다. 첫 번째 선택은 서버를 제외한 사용자들을 이동하는 것이다. 이 경우 재배치된 사용자들의 모든 트래픽은 이전 지역의 FDDI 서버 링으로 되돌아 갈 것이므로, 그 만큼의 WAN 대역폭을 두 지역간에 필요로 할 것이다.

두 번째 선택은 사용자들을 관련된 파일 및 부트 서버를 따라 이동시키는 것이다. 모든 사용자들이 애플리케이션 서버를 사용하는 동안 특정 소규모 사용자 그룹은 파일과 부트 서버들을 사용했다. 이 경우 요구되는 WAN 대역폭의 양은 얼마나 많은 트래픽이 재배치된 사용자에게 나타나는가에 기인하고, 파일과 부트 서버는 애플리케이션 서버로 다시 보내지게 된다.

최고의 선택을 결정하기 위해 관리자는 현존하는 트래픽을 빠르고 쉽게 평가해야만 했다. 이런 측정은 클라이언트/서버 통신간의 평균 및 최고치를 구하고, 많은 양의 대역폭을 사용하는 클라이언트를 정확히 찾아내는 것을 의미했다. 이런 클라이언트는 그들의 결합된 서버들과 함께 이동하기 위한 잠정적인 후보자일 것이다. 서버간의 트래픽을 아는 것은 동시에 이동해야 할 서버 조합을 확인하는데 도움을 줄 수 있었다.

· 해결책 조사

IT 부서의 분석가들이 이런 자료를 수집하려고 할 때, 프로토콜 분석기가 고려 대상이 됐는데, 이 자료들은 뛰어난 기능성을 보여주었으나, 상위 호스트를 인식할 수 있는 반면, 프로토콜, 애플리케이션 또는 호스트에 의한 경향을 보고하지는 못했다. 다시 말해 이것은 많은 수의 호스트 매트릭스에는 실용적인 접근이 아니었다.

관리자는 네트워크의 거시적 수준뿐만 아니라 트래픽 부하와 이의 주요 분류를 가시적으로 볼 수 있기를 원했다. 특별한 호스트 매트릭스를 찾을 수 있고, 필요한 세부 수준까지 모니터링 할 수 있어야 했다. 다행히 관리자는 모니터링과 진단에 유용한 솔루션이 RMON 기술로 간단하고 강력하다는 것을 들은 적이 있었다.

RMON 분석 시작 24시간 안에, IT 관리자는 신 사옥과 구 사옥 사이에 단지 5MB 연결만이 요구된다는 것을 깨달았다. 그는 기존에 염려했던 100MB연결은 필요가 없었던 것이다.

· 서버-서버 트래픽 레벨 정의

IT 관리자는 처음에 전반적인 서버-서버 트래픽 레벨을 정의했다. 프로브는 FDDI 서버 링에 연결됐고, 간단히 RMON 매니저 콘솔에서 IP 주소, 서브넷 마스크(Subnet Mask), 디폴트 게이트웨이 (Default Gateway)를 기입함으로써 설치됐다. 다음에 소스/도착지 주소(FDDI 링은 하나의 IP 서브넷)를 포함하는 커스텀 도메인(Custom Domain)을 만들었다. 프로브는 즉시 사용자가 정의한 시간간격으로 자료를 수집하고 요약하기 시작했다. 그 결과 분석을 위해 매니저 콘솔로 전송됐다. 트래픽 수준은 시간에 따라 추적되고 그래프로 보여주었고, 완벽하고 정확한 활용 경향 보고를 제공했다. 이 경향보고는 비록 서버가 무작위로 움직이더라도 필요한 대역폭은 일정하다는 것을 보여주었다.

· 클라이언트/서버 트래픽 구분

그 다음으로 관리자는 모든 클라이언트/서버 트래픽을 구분해야 했다. 모든 애플리케이션을 구성하는 또 다른 사용자 도메인이 만들어졌고, 애플리케이션 서버 도메인에서 분석가는 호스트 매트릭스의 분류된 (호스트 IP 주소에 의해) 목록을 간단히 출력해 어떤 사용자 호스트가 어떤 애플리케이션 서버와 통신되는지 볼 수 있었다. 네트워크 사용률 순서로 재분류된 목록은 높은 대역폭을 사용하는 호스트 매트릭스를 재빠르게 지적했다. 클라이언트/서버 트래픽은 올바르고 균일하게 분류됐으며, 24시간 안에 분석은 완성됐다.

주마다 일괄 작업 또는 애플리케이션의 오버랩 같은 예외 데이터가 근본 데이터를 왜곡하지 않았다는 것을 확신하기 위해 RMON 프로브는 FDDI와 WAN 트래픽을 모니터링하기 위해 추가적으로 2주간 더 운영됐다.

· 예상치 않던 정보 수집

예상치 않게, RMON 솔루션은 소수의 클라이언트가 최적의 경로를 거쳐 애플리케이션에 통신하지 않는다고 보여주었다. 클라이언트와 서버간의 통신은 클라이언트로 가는 라우팅과 클라이언트로부터 오는 다른 라우팅을 사용했고, 이런 불균형의 사건이 정확히 파악되면, 애플리케이션 그룹은 애플리케이션을 재구성할 수 있고 더 이상의 하드웨어 비용 없이 성능을 향상시킬 수 있었으며, RMON은 IT 부서의 분석 활동을 위한 주요 협력자가 됐다.