정책기반 네트워킹 Policy Based Networking(PBN)

송 왕 철*

목 차

1. 서 론

근래 들어 인터넷은 모든 연구분야는 물론이고, 우리 생활 곳곳에서 중요한 역할을 하고 있다. 하지만, 이러한 인터넷 기술은 네트워크 상의 모든 데이터가 모두 동등하다는 가정 하에서 발전되어 왔으며, 네트워크상의 각 노드들은, 제어용 데이터와 일반 데이터만 구분하여 처리할 뿐, 실질적으로 모든 데이터를 동등하게 처리하고 전달하도록 하고 있다. 실제로 이러한 단순한 형태의 모델은 인터넷 기술의 비약적인 발전을 가져온 중요한 요인이 되어 왔다.

근래에 이르러 멀티미디어 서비스를 중심으로 하는 다양한 서비스들이 인터넷의 주요 트래픽 요인으로 자리잡으면서, 특히 실시간 응용들을 중심으로 하는 각종 서비스의 개발들로 인해, 모든 데이터가 같은 중요성을 가지며, 이들 데이터를 Best Effort 방식에 의해 전송한다는 전제는 수정이 필요하게 되었다. 즉, 네트워크가 혼잡할 때에, 특정 트래픽 플로우에 필요한 자원을 할당하고, 이에 대한 서비스가 보장되거나 다른 트래픽에 대해서 우선적으로 자원을 할당해 주는 QoS 메커니즘이 필요하게 되었다.

또한 일반적인 네트워크, 특히 학교 등과 같이 서로의 호스트들에 대한 신뢰성에 문제가 없는 네트워크와는 달리, 기업체들간의 네트워크상에서는 상대방, 특히 경쟁 업체들 사이에 데이터의 유출 및 오변조가 문제가 된다. 이러한 이유로 해서, 근래의 기업 네트워크에는 외부의 신뢰할 수 없는 사용자들로부터 내부 IP 네트워크를 격리시키는 방화벽 시스템이 도입되고 있다.

이제, 이러한 멀티미디어 응용들과 방화벽 시스템을 어떻게 제공하느냐는 중요한 문제가 되었다. 즉, 단순히 Web 서핑을 하는 사용자들에 대해, 특정한 IP나 특정한 사용자들에게 많은 자원을 할당 및 보장하거나, 특정 조직체 및 사용자들에게 특정 IP를 동적으로 할당하거나, 특정 사용자들이 사용하는 파일에 대해 다른 백업 스케줄을 제공하는 등의 방법들이 고려될 수 있을 것이다. 하지만, 이렇게 서비스를 특정 그룹 및 트래픽에 대해 서비스를 차별화 하려면, 이를 적절하게 관리해야 할 메커니즘이 필요하다. 실제로 많은 수의 인터넷 서비스 사업자(ISP)들은 높은 대역폭을 필요로 하는 사용자들의 접근을 효율적으로 통제할 수 있는 방법에 대해 고민하고 있다. 초고속 인터넷 기반 네트워크를 통해 고대역폭을 할당받은 사용자들이 네트워을 점령하고 있기 때문이다. 예를 들어, 45Mbps 전용회선을 통해 서울 부산간을 서비스하고 있는 한 ISP의 경우, ADSL 서비스를 사용하는 가입자가 서울 부산간 화상회의를 한다면 다른 사용자의 경우에 나머지 37Mbps로 회선을 나누어 사용해야 한다. 그러나, 이 가입자의 트래픽을 안정적으로 제공하면서, 다른 많은 사용자들에게도 ADSL이나 케이블 모뎀을 통해 고대역폭의 서비스를 제공하려면 ISP에는 큰 문제가 아닐 수 없다.

* 제주대학교 통신컴퓨터공학부 부교수

이러한 경우, ISP입장에서 문제를 해결할 수 있는 방법으로 정책기반 네트워킹이 주요한 방법으로 부각되고 있다. 큰 대역폭을 사용하는 사용자에게는 사용한 대역폭만큼의 비용을 부과하고, 많은 대역폭을 필요로 하지 사용자에게는 적정한 대역폭만 할당하면서, 특정 시간대에 특정 지역 사용자와 안정적인 대역폭을 할당받고 싶은 사용자에게도 원하는 만큼의 통신 대역폭을 배정할 수 있게 한다. 이처럼 네트웍 관리자가 중앙에서 회사의 정책에 따라 사용자나 특정 구간에 우선권이나 고용량의 대역폭을 할당할 수 있도록 총체적으로 관리하는 서비스가 정책기반 네트워킹이다.

이런 견지에서, 네트워크 정책은 연구분야에서 근래 주요하게 부각되는 주제이며, IETF(The Internet Engineering Task Force)와 DMTF(The Distributed Management Task Force)는 정책에 대한 표준화 작업을 수행하고 있다. 네트워킹을 위한 정책은 주로 QoS와 보안 분야, 망관리 분야에 대해서 연구가 이뤄지고 있으며, 네트워크 관리에 있어 지능성 및 역동성을 수용할 수 있는 방법이 될 것이다. 실제로 1999년부터 많은 장비제조업체에서 선을 보이기 시작한 정책기반 네트워크는, 수많은 회선 가입자들을 적정하게 통제하고 관리해야 하는 필요성 때문에, 대규모 통신 사업자들이 가장 반기고 있으며, 역동적인 변화에 대해 스스로 진단, 치유하는 지능성을 가진 네트워크 기술로서, 그 중요성은 크다 하겠다.

2. 네트워크 정책과 관리

네트워크 정책이란, 어떤 트래픽이 네트워크 상에서 차별화 되어서 다뤄져야 하며, 또한 어떻게 이뤄지는 가에 대하여 정의한 것이다. 이는 네트워크 관리자에 의해서 정의되며, 네트워크 내에 있는 여러 타입의 트래픽들을 어떻게 다룰 것인가에 대한 규칙을 정의하게 된다. 그 규칙들은 if condition then action의 형태를 취하여, 어떠한 사용자/응용/호스트가 어떠한 조건하에서 어떠한 자원에 접근할 수 있는 가를 제어할 수 있게 하는 것이다. 이러한 정책의 역할에 있어서 중요한 점은, 네트워크 관리를 간단하게 수행할 수 있게 해준다는 것이다. 오늘날의 기업체 네트워크들은 복잡하고 이기종의 시스템들로 이뤄져 있다. 이러한 환경에서 네트워크를 제대로 운영한다는 것은 쉬운 일이 아니며, QoS나 보안 기능을 추가한다면, 그 관리의 복잡성은 한층 커질 것이며, 이러한 기술들을 효과적으로 묶어줄 지능적인 관리 메커니즘이 필요하다.

따라서, 정책기반 네트워크는 복잡한 기술들을 채용하고 있는 여러 가지 기기들을 관리할 수 있는 간단한 방법을 제공할 수 있을 것이다. 기본적으로, 정책에 기초하는 네트워킹 역동적으로 변화하는 망의 상태에 대한 정보를 바탕으로 자원들을 효율적으로 배분함으로써 네트워크 상의 트래픽이 혼잡을 겪지 않도록 하고, 혼잡 상황에서도 특정한 사용자 및 그 그룹에 대해서는 일정한 양의 자원을 할당 및 보장하여 QoS를 제공할 수 있는 방법을 제공할 수 있을 것이다. 또한, 시간에 따라 특정 그룹이나 사용자의 대역폭 요구가 달라진다고 하더라도, 이를 위해 항상 최고 값의 대역폭을 할당하는 것이 아니라, 역동적으로 자원할당을 달리할 수 있을 것이다. 더구나, 이러한 네트워크 관리는 관리자가 지정한 규칙에 따라 자동적으로 이뤄지게 되므로, 결과적으로 관리자가 손쉽게 네트워크를 관리할 수 있게 하는 것이다.

정책 기반 접근법은 다음 두 가지 기법에 의해 이뤄질 수 있다[6].

◎ 중앙 집중식 구성관리 : 정책기반 네트워킹에서 네트워크 구성관리는, 각각의 장치를 개별적으로 구성하는 것에 의해 지정되는 것이 아니라, 중앙 지점에서 네트워크 전반에 대한 정책을 지정함으로써 이루어진다. 그 중앙 지점은 네트워크 운용자가 사용하고 있는 관리 도구의 콘솔이거나, 모든 정책이 저장되는 저장소가 될 것이다. 모든 장치의 구성을 알 수 있는 그 중앙 지점에서, 여러 가지 다른 구성들이 서로에게 모순되지 않은 지가 테스트되고, 점검될 수 있을 것이다. 또한, 응용들 사이의 우선권들도 이곳에서 지정될 수 있고, 여러 라우터들에서의 트래픽의 상대적인 우선권 역시 점검되고, 올바르게 셋업될 수 있을 것이다. 구성관리의 중앙집중화는 구성의 일관성을 점검하는 일을 간단하게 할 수 있게 해준다.

◎ 단순화된 추상화 : 실질적인 장치의 구성에 대한 것보다는 높은 계층에서의 단순화된 추상화를 제

공할 수 있게 함으로써 관리자의 임무를 단순화시켰다. 예를 들어, 응용들의 플로우에 정확한 마킹을 하게 한다든지, 전송률을 지정하도록 하기보다는 여러 응용들 사이의 우선권을 지정하거나 응답시간을 지정할 수 있도록 하여 단순화를 가져올 수 있다.

특정 기기 장치들에 최적화된 정책들은 정책기반 관리도구를 사용하여 발생시킬 수 있다. 단순화된 높은 계층 추상화는, 많은 다른 유형의 정책 구성 정보에 의해 충족될 수 있는데, 관리 도구는 이러한 가능성들 중에서 선택을 하고, 그 목적을 지원할 수 있도록 최적화된 구성방안을 결정하게 된다. 또한, 모든 정책이 모든 장치들에게 관련되어 있는 것은 아니므로, 관리 도구는 각 장치들에 관련된 정책들을 골라내어서 그 장치들을 적절하게 구성할 수 있도록 한다.

중앙 집중식 구성관리와 단순화된 추상화 둘 모두는 오버헤드를 가지고 있다. 중앙 집중식 구성 관리는, 보안 및 구성 정보에 대한 무결성에 대하여 고려해야 함은 물론 정책 저장소로부터 구성 정보를 가져오기 위한 프로토콜을 결정해야 함을 의미한다. 또한, 단순화된 추상화 기법은 사용하기 편리하게 끔 하는 목적에 있어서는 기여를 한다 해도, 단순화는 유연성의 감소라는 비용을 유발시킨다.

이러한 오버헤드에도 불구하고, 정책기반의 기법들은 네트워크 전체의 기준을 지정 및 실행을 자동화한다. 정책기반 환경에서 자동화된 도구란, 어떤 유형의 트래픽이 다른 유형의 것들에 비하여 높은 우선권을 가지고 있다는 간단한 네트워크 전체의 정책을 받아들이고, 그 정책을 네트워크 상의 다양한 라우터들에 적용될 수 있는 개별적인 구성의 정책으로 변환시키는 역할을 하는 것이다.

3. 정책의 특성

3.1 적용분야

정책 기반 네트워킹의 개념에서 정책을 적용하고 있는 분야는 다양할 수 있겠지만, 우리가 고려할 수 있는 분야들은 QoS와 보안 분야들이고, 네트워크 관리 분야는 이들 두 분야들과 연관되어 많은 연구가 진행 중에 있다.

3.1.1 QoS(Quality of Service)

인터넷상의 QoS 제공 기술은 크게 IntServ(Integrated Services)[1]와 DiffServ (Differentiated Services)[2] 기술로 나뉘어 진다. IntServ는 하나의 망 하부구조를 통해서 오디오, 비디오, 실시간, 기존의 데이터 트래픽을 한꺼번에 전송할 수 있는 메커니즘이다. 이 서비스는 IETF의 intserv WG(working group)가 권고안을 통하여 CL(Controlled Load) 서비스 클래스와 GS(Guaranteed Service) 클래스의 두 가지 QoS 제공 방식에 대해서 규정하고 있다. 이 IntServ 기술은 RSVP(Resource Reservation Setup Protocol) [3]을 근간으로 하고 있는데, 종단간의 플로우에 대한 QoS 보장을 위해 RSVP가 시그널링 메커니즘을 담당한다. 이 방식은, 중간 라우터들에 있어서의 효율적인 자원할당을 통해 각 전송 계층 플로우에 QoS를 제공해줄 수 있으나, 각 라우터에서 모든 플로우를 개별적으로 구분해야 하는 점 때문에 확장성에 문제점을 가지고 있어서, WAN 상황에 적용이 적절하지 못하다는 단점을 가지고 있다. 이러한 RSVP 프로토콜을 기반으로 하는 정책기반 프레임워크에 대한 논의는 주로 rap WG에서 이뤄지고 있다[4].

DiffServ는 IETF의 diffserv WG[5]에 의해 표준화가 주도되고 있으며, 다양한 응용들을 수용하고 인터넷 트래픽에 대해서 그 서비스의 차등 등급을 제공하자는 필요성에 의해서 연구가 이뤄지고 있다. DiffServ는 음성 등과 같이 데이터의 흐름이 끊어지면 안 되는 비교적 특별한 형식의 트래픽들에 대해, 다른 종류의 일반 트래픽에 비해 우선권을 갖도록 네트웍 트래픽을 등급별로 지정하고, 제어하기 위한 프로토콜이다. DiffServ는 서비스의 등급, 즉 CoS (Class of Service)라고 불리는 형태로 트래픽을 관리하는 가장 진보된 방식이다. DiffServ는 802.1p에서의 태그 이용 그리고 ToS (Type of Service) 등과 같은 초창기 방식과는 달리, 주어진 네트웍 패킷을 어떻게 전달할 것인지를 결정하기 위해 단순히 우선순위를 위한 태그를 붙이는 대신, 좀더 복잡한 정책이나 규칙 문을 사용한다. 주어진 패킷 이동 규칙에서 패킷은 홉 당 움직임, 즉 PHB (per hop behaviors)라고 불

리는 64개의 가능한 전달 움직임 중 하나가 적용된다. IP 헤더 내 DSCP (DiffServ code point)라는 여섯 비트 길이의 필드가 주어진 패킷의 흐름에 대해 홉 당 움직임을 지정한다. PHB그룹은 AF(Assured For-warding)와 EF(Expedited Forwarding)로 분류되는데 AF라 불리는 차등 서비스 PHB는 4개의 AF 클래스로 되어 있고 각 클래스에서 IP 패킷은 세 가지 가능한 버리는 우선순위(drop precedence)를 가지고 있다. EF PHB는 낮은 손실, 낮은 지연, 낮은 지터, 보장된 대역폭과 DS 영역을 통한 단대단 서비스를 제공하기 위해 사용된다. 복잡한 분류와 표시, 정책 등은 네트워크 경계 또는 호스트에서 이루어지며 트래픽이 어떻게 표시되어 있느냐에 따라서 네트워크 자원이 할당되어진다. 또한 네트워크 경계에서 트래픽이 진입 노드에 표시된 패킷들이 들어올 때 각 서비스 규칙 및 요구가 합당한지를 TCA(Traffic Conditioning Agreement)에 의해 확인된다.

3.1.2 IP 보안

IP 보안의 영역은 세 가지 기술방식에 의해 트래픽 필터링과 세션 계층 암호화, 네트워크 계층 암호화로서 구별된다. 인터넷으로 컴퓨터를 연결시킬 때, 그 보안 기법으로 다음의 기술들을 고려할 수 있다.

◎ 패킷 필터링 방화벽 : 이 방식은 OSI 모델에서 네트웍층(IP 프로토콜)과 전송층 (TCP 프로토콜)층에서 패킷의 출발지 및 목적지 IP 주소 정보, 각 서비스에 port번호, TCP Sync 비트를 이용한 접속제어를 한다. 방화벽은 인터넷으로부터 들어오는 트래픽에 대해 허락하도록 정해진 컴퓨터들에 대해서만 접속이 허용된다. 모든 기능은 외부와 내부 사이에 위치한 중간 컴퓨터에 의해서 이뤄진다.

◎ SSL(secure socket layer) 프로토콜을 이용한 데이터 암호화 : 방화벽이 들어오거나 나가는 트래픽에 대하여 제한을 가하지 않고, 전송 전에 SSL 기법을 이용하여 데이터를 암호화시킨다.

◎ IPsec(IP security protocol)을 이용한 네트워크 계층 암호화 : IPsec이 기계의 OS내에서 데이터를 암호화하고 상대방 기계에서 동작하고 있는 응용에 투명하게 전달한다.

3.2 정책에 대한 요건

정책이 네트워크에서 활성화되기 위해서 관리자는 이를 정의하고, 장치들은 이들을 실행시킬 수 있도록 해야 한다. 정책에 의해 네트워크의 운용이 제대로 이뤄지기 위해서는 정책이 다음의 요건들을 만족해야 할 것이다[6].

◎ 정확성(precision) : 정책은, 각 네트워크 요소들이 이해할 수 있을 만큼 자세한 레벨까지 정책의 실행에서 요구되는 필수 세부 항목들을 통하여 정확하게 지정되어야 한다. 그리고, 정책의 해석에 있어서도 애매함이 없어야 한다. 예를 들어, 트래픽 암호화에 대하여 지정한다면, 암호화 타입, 알고리즘, 키 값, 리프레쉬 시간 등의 세세한 것들 모두를 지정해야 한다.

◎ 일관성(consistency) : 네트워크 요소 하나에 주어지는 일련의 정책들이나 그 네트워크 상의 모든 요소들에게 주어지는 일련의 정책들이나 모두 일관되어야 한다. 트래픽이 특정한 우선권을 가지고 있다면 그 트래픽을 다루는 모든 라우터에서는 같은 우선권으로 그 트래픽을 처리할 수 있어야 한다.

◎ 호환성(compatibility) : 어떤 네트워크 요소에 주어지는 일련의 정책들은, 그 네트워크 요소가 지원하는 용량과 호환되어야 한다. 네트워크 상의 라우터들은 패킷에서 네트워크 계층 헤더만을 조사한다. 따라서 정책은 네트워크 계층 헤더 필드를 포함하는 형식으로 네트워크 요소에 지정되어야 한다. 라우터에서 해석될 수 없는 정책은 소용이 없다.

◎ 상호 일관성(mutual consistency) : 어떤 네트워크 요소에 다수의 정책이 지정된다고 하면, 그 정책들 모두는 서로 모순이 되지 말아야 한다. 네트워크 요소는 명백한 방법으로 이 정책들을 적용할 수 있어야 한다. 특히, 그 네트워크 요소를 통해 지나가는 각 패킷에 대하여, 그 패킷에 적용 가능한 일련의 정책들을 정확하게 식별하는 것이 가능해야 한다. 또한, 서로가 충돌이 일어나는 액션이 발생하지 않도록 정책들이 지정되어야 하며, 최소한 충돌하는 정책이 검출되었을 때, 가능한 정책들 중의 하나로 전환될 수 있는 명백한 방법이 제공되어야 한다.

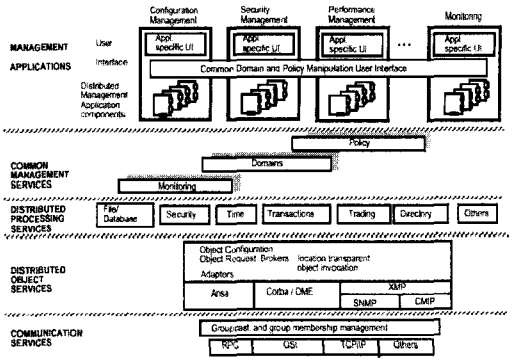
◎ 규정의 용이성(ease of specification) : 네트워크 관리자가 정책을 용이하게 지정할 수 있어야 한다.

◎ 직관(intuitiveness) : 네트워크 운용자가 정책을 지정하려면, 정책들이 네트워크 운용자에게 친숙한 항목으로 정의되어 있어야 한다. 이는 기업체 망인 경우 그 조직에서 쓰이는 용어를 기반으로 해서 정책들이 정의되어야 할 것이다. 즉, 이것은 정책이 지정되어 있는 경우 그 정의만으로 그 정책의 역할이나 의미를 직관적으로 파악하기 쉽게 하기 위함이다.

이러한 요건들을 제시하였지만, 이 요건들을 동시에 모두 충족시킬 수는 없다는 것은 명백하다. 실제로, 직관 에 대한 요건을 고려하여 기업체에서 쓰이는 용어를 기반으로 하는 경우, 이를 동시에 동일한 망에서 쓰이고 있는 모든 라우터가 이해할 수 있도록 호환성을 가질 수 있도록 하는 것은 어렵다고 볼 수 있다. 이러한 명백한 충돌 때문에, 정책은 최소한 두개의 레벨로 나뉘어야 할 것이다. 그 하나는 낮은 레벨의 정책으로서, 각 장치에서 실행 가능한 형태의 것이며, 또 다른 하나는 네트워크 운용자가 규정하기 용이하고 직관에 이해서 파악이 가능한 형태의 것인 높은 레벨의 정책이다. 물론, 이들 정책 레벨들은 필요에 따라서 더 많은 단계로 나뉠 수도 있으나, [7]은 비즈니스 레벨과 기술레벨의 두 가지 레벨로 나누고 있고, [8]는 네트워크 레벨, 역할 레벨, 구성 레벨의 세 단계로 나누어 놓고 있다.

4. 표준화 및 상용시스템

1990년대부터, 분산 시스템의 관리를 위한 정책 분야에서의 많은 연구가 이뤄져 왔는데, 이들 대부분은 Imperal College London에서 선도 되어왔다. [9]은 그림 1에서 보듯이 일반적 관리 구조에 있어서의 도메인과 정책의 개념을 보여주고 있다. 이들 연구로부터, 정책이란 주체(관리자들)와 목표점(관리대상)사이의 관계를 나타내는 객체로서 규정되어 있으며, 정책은 자동화된 관리자로부터 분리되어 있는 상태로서 역동적인 변화를 쉽게 하고, 재 구축 없이 새로운 요건에 쉽게 적응할 수 있게 하는 방법이다. 또한, 도메인을, 객체들을



(그림 1) 정책기반 분산 관리 시스템 구조[10]

그룹핑 함으로써 관리 책임을 나누기 위한 프레임웍을 제공하는 것으로 간주하고, 도메인 멤버 관리 객체들에 대한 참조 리스트들을 유지하는 객체로서 정의하고 있다. 정책에 대한 연구들을 바탕으로, IETF와 DMTF를 중심으로 하여 표준화 작업이 이뤄지고 있다.

4.1 DMTF(Distributed Management Task Force)

이 단체는 92년에 미국 IBM, 인텔, 썬소프트, 디지탈, 노벨, 휴렛팩커드, 마이크로소프트 등 8개 회사가 공동으로 만들었으며, 원래 Desktop 관리용 API의 표준화를 추진했던 단체로서, 원래 Desktop Management Task Force에서 1999년 Distributed Management Task Force로 이름을 바꾸면서, 객체지향 패러다임을 사용하여 분산된 통신망 구성장치의 정보를 획득하여 물리계층에서 응용계층, 운영체제까지의 관리를 할 수 있는 구현레벨의 표준화 규격을 제공하고 있다. DMTF에서 관리 객체를 정의하기 위해 제안한 CIM(Common Information Model)은 원래 컴퓨터의 특성을 나타내기 위한 것이었으나, 지금은 컴퓨터와 각종 기기로 이뤄진 네트워크로 확장되어서, 시스템과 네트워크 관리를 위한 규격으로 정의되고 있다.

정책을 통한 네트워킹에 전기를 마련하게 된 것은 1998년에 마이크로소프트와 시스코가 주도적으로 DEN (Directory Enabled Network)을 시도하면서 부터인데, 워크스테이션 OS 시장에서 마이크로소프트의 지배적인 위치와 인터넷 라우터 시장에서의 시스코의 위치

때문에, DEN의 시도는 산업체에서 많은 주목을 받았었다. 또한, DEN의 목적이 네트워킹 인프라를 구성하는 것으로서, 정책의 저장소로서 쓰이고, 관리의 용이성을 준다는 면에서, 정책기반 네트워킹의 초석이 된 것이다. 이러한 배경 때문에, DMTF는 DEN을 기조로 하여 X.500에 기초한 디렉터리 서비스와의 매핑 방식에 대한 표준화 작업에도 힘을 기울이고 있고, 또한 웹상에서의 통신망 관리를 방식인 WBEM (Web-Based Enterprise Management)에 대한 표준화도 진행시키고 있다.

정책 기반의 네트워킹을 위한 표준화 작업으로서, DMTF는 CIM 2.4와 CIM/LDAP(Lightweight Directory Access Protocol) 매핑, ASF(Alert Standard Format) pre-OS alert, CIM 2.5 이벤트들에 대한 강력한 규격과 스키마 집합을 개발하였다. 또한, CIM 2.4에 정책과 QoS 스키마를 추가하여 전통적인 장치, 시스템 및 네트워크에 대한 관리에 대해 CIM을 확장한 것을 바탕으로, 이어진 CIM 2.5 최종안에서는 이벤트 모델을 추가하였으며, 현재 CIM 2.6을 진행 중에 있다. 또한, CIM의 강화된 측면으로서, CIM 2.4부터 포함된 LDAP과의 매핑은, DEN 표준안을 통해 사용자들이 자신들의 디렉터리 정보들을 더욱 기업체 관리와 통합시키는 것이 가능하게 하였다.

최근에는 WBEM을 위한 xmlCIM이 개발되고 있으며, 개발된 객체를 이용하여 통신망을 관리하는 시범 프로젝트를 수행하여 표준화 검증에도 연구를 수행하고 있다.

4.2 IETF

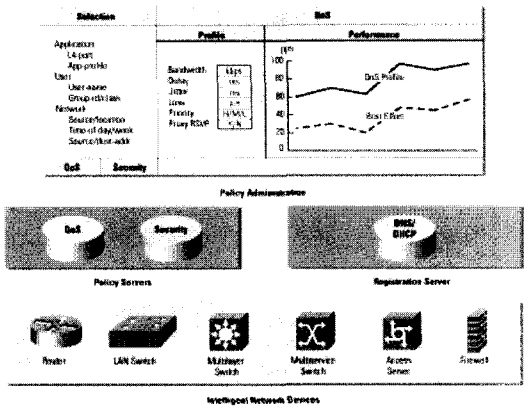
IETF는 정책기반 관련 WG으로서 policy WG과 rap (Resource Allocation Protocol) WG을 고려할 수 있다. RAP WG의 목적은 RSVP에 대한 확장 가능한 정책 제어 모델을 수립하는 것으로, RSVP를 인지 할 수 있는 네트워크 노드와 정책 서버사이에서 사용하기 위한 프로토콜을 규정하고 있다. Policy WG은 정책 자체, 특히 QoS에 대한 정책을 규정하는 표준화 작업을 수행한다. 즉, 정책을 나타내는 정보모델을 정의하고 이 모델을 QoS 관리에 알맞도록 확장하는 것은 물론, 업체들에 독립적이면서 상호운용가능하고 확장 가능한 방식으로 정책을 표시하고, 관리하고, 공유하고 재사용하기 위한 일반적인 프레임웍을 세우는 표준화 작업을 진하고 있다.

Rap WG은 두 주요 구조 요소인, PEP(Policy Enforcement Point)와 PDP(Policy Decision Point)를 규정함으로써 정책기반의 수락제어에 대한 프레임워크를 제시하고 있다. 근래 이르러, 세션계층에 대한 작업과 정책에 대한 작업을 결합시키면서, SIP (Session Initiation Protocol)과 결합된 형태의 working draft도 출간되고 있으나, 기본적으로 PDP가 정책에 근거한 결정을 내리고 PEP가 그 결정을 수행하는 메커니즘에 기초하고 있다. 이 그룹의 표준안들은 RSVP 프로토콜에 의한 자원 예약 시에 정책적 판단이 필요하게 되면, PEP는 그 요청을 PDP로 전송하여 정책 판단을 요구한다. PDP는 하나의 도메인에 하나의 호스트 특히 ingress point에 위치하면서, 그 도메인에서 flow의 자원예약에 대한 정책적 판단을 한다. 이러한 판단은 LDAP과 같은 저장소에 저장되어 있는 정책들을 참조하여 수행하게 된다. 또한, PEP는 정책기반한 결정을 내리기 위해 먼저 LPDP(Local Policy Decision Point)에 요청을 보내어 국지적으로 판단을 시도하고, PDP로의 추가적인 요청이 필요한 경우에 PDP로 요청하여 최종결정을 통보 받게 된다.

Policy WG은 정책을 정책 규칙들의 집합체로 정의하고 있다. 각 정책 규칙은 조건과 그에 따른, 장비와 업체에 독립적인 action의 집합으로 구성되어 있으며, if <condition> then <action>의 형식을 가진다. 이 그룹에서 정의하는 주요 기능 요소는 다음과 같이 4가지로 구성되어 있다 : 정책 관리 도구, 정책 저장소, 정책 타겟, 정책 소비자[11].

4.3 상용시스템

근래에 이르러 정책기반 네트워킹 기능을 가지고 있는 장비들은 가히 홍수처럼 쏟아져 나온다고 해도 과언이 아닐 정도이다. 대부분 업체들이 비슷비슷한 정책을 가지고 있고, 현재의 정책기반 시스템이라고 하는 기능들이 주로 QoS를 지원하고 있지만, 정책서버가 있느냐 없느냐 또는 정책서버가 한 개냐 두개냐 또는 DHCP, LDAP, 디렉터리 등을 지원하느냐 하지 않느냐에 따라 서로 상이하다.



(그림 2) CiscoAssure의 구조

4.3.1 시스코

시스코는 시스코어슈어 정책 네트워킹(CiscoAssure Policy Networking)을 내놓고 있다[12]. 시스코어슈어 정책 네트워킹은 관리자와 네트워크사이에 지능계층을 배치함으로써, 비즈니스 프로세스들을 지원하기 위해 개발된 직관적 정책들과 네트워크 장치들 사이에서 정책과 구현사이의 전환을 제공해준다. 또한, 견고한 종단간 보안 솔루션의 구현을 자동화하고 이들 관리를 디렉터리 서비스를 이용하여 중앙 집중화함으로써, 결과적으로 네트워크 관리자가 분산된 네트워크 지능을 이용하기 쉽도록 해주게 된다.

시스코어슈어 정책 네트워킹 아키텍처는 다음의 4가지 요소를 기반으로 이루어진다(그림 2).

◎ 지능형 네트워크 장치 : 네트워크 장치들은 정책의 지시 사항들을 해석하여, 각 사용자나 애플리케이션에 대해 정책에 기반하여 보안을 위한 제어를 적용할 수 있다.

◎ QoS(Quality of service)및 보안 정책 서비스 : 관리자와 네트워크 사이의 인터페이스를 제공하는 서버 기반의 제어 시스템이다. 해석 능력을 통해, 중앙의 콘솔에서 네트워크 전반에 거친 실제의 장치 구성을 자동화하며, 정책에 따라 해당 네트워크를 최적화한다. 모든 정책에 대한 지시는 PDP와 PEP사이의 표준 프로토콜인 COPS(Common Open Policy Service) 프로토콜을 통해 각 네트워크 요소로 전달된다.

◎ 등록 및 디렉터리 서비스 : 네트워크 주소, 사용자 프로파일, 그리고 적절한 정책의 구현과 이행에 있어 필수적인 정보와 정책 서비스 사이의 동적 바인딩을 제공한다. 이와 같은 서비스들은 DNS(Domain Name Server)및 DHCP(Dynamic Host Configuration Protocol) 서버 시스템과 LDAP(Lightweight Directory Access Protocol)v3 기반의 디렉터리들을 바탕으로 한다.

◎ 중앙 집중화된 정책 관리 : 관리자는 정책의 정의를 단순화시켜 주며, 중앙에서 비즈니스 규칙들을 구성하여 이 규칙들을 지능형 네트워크로 매핑할 수 있는 기능들을 제공하는 GUI(graphical user interface)를 통해CiscoAssure 정책 서버 시스템과 상호 작용한다. 실제로, 이 기능은 인지가 쉽도록 구성된 정책들이 각 장비로 적절하게 해석되어 이전됨으로써 상위 계층의 정책이 하위 계층의 정책으로 일관성 있게 매핑될 수 있는 것을 의미한다. 따라서, 다수의 Cisco security 요소들 전반에 걸쳐 일관성 있는 정책을 생성하고 이행할 수 있다.

4.3.2 3Com

3Com은 Policy Powered Networking 전략을 구사하고 있다. 이에 따라, 이미 97년에 트랜센드웨어(Transcend-Ware-TM) 소프트웨어를 발표하여, 3Com의 기본적인 네트워킹 시스템과 네트워크 인터페이스 카드에 내장되도록 했다. 트랜센드웨어 소프트웨어는 "정책기반 적용 또는 3차원 네트워킹"(policy-based adaptive or 3D networking)이라고 불리는 새로운 차원의 네트워킹을 제공한다. 이는 비즈니스 관리자에게 비즈니스 요구에 따라 네트워킹의 방식을 규정할 수 있으며, 개별 사용자나 부서, 그리고 응용이 특정 서비스 레벨이나 우선권을 제공받을 수 있도록 한다. 이는 핵심업무 정보가 항상 우선적으로 전달될 수 있도록 해 주는 것은 물론 보다 높은 대역폭을 요구하는 차세대 비디오 및 멀티미디어 응용이 네트웍 상에서 제대로 된 품질로 구현될 수 있도록 보장해 준다. "3차원"이란 3Com 네트워킹 프레임웍의 3대 요소인 성능향상, 성장관리, 원격접속 확대 등에 독창적인 정책기반 차원이 추가된 것을 의미한다.

트랜센드웨어 소프트웨어는 사용자가 글로벌 비즈

니스 정책 유형에 의해 명시된 특정 서비스 등급을 이용할 수 있도록 비용대비 효율성을 높여 놓았다. 이 소프트웨어는 최종 시스템 네트웍 인터페이스 카드의 인텔리전트 기능을 이용해 트래픽이 전달되는 네트웍 가장자리(network edge)와 네트웍 중심(network core)의 네트워킹 시스템에 신호를 전달해 주는 능력에 기반한다. 따라서 특정 사용자 또는 핵심 비즈니스 응용에 필요한 대역폭이나 우선적인 응답권 부여 등과 같은 글로벌하게 정의된 비즈니스 정책에 맞는 네트웍 서비스를 필요로 하는 사용자 및 응용 요구와 관련돼 있다. 네트웍에서 정체현상이 나타나면 3Com 장비에 탑재된 트랜센드웨어 네트웍 컨트롤 소프트웨어가 자동적으로 이 같은 정책을 실시하는 것이다. 트랜센드웨어는 업계 표준에 기반하고 있어 다른 업체 제품으로 이뤄진 네트웍에도 세밀한 관리, 제어, 정책 기능을 제공해 주며, 네트웍 성능을 향상시킬 수 있도록 했다.

4.3.3 노텔(Nortel)

노텔은 Optivity Policy Services라는 정책 기반 네트워킹 기술을 제시하고 있다. 이 서비스는 네트워크 관리자가 비즈니스에서 중요한 트래픽에 우선권을 줄 수 있도록 하는 정책관리에 대한 포괄적이면서 시스템 전반적인 관리 프레임웍을 제공한다. 또한, 이 서비스는 QoS가 장치별이 아닌 시스템 전체 레벨로 구성관리 될 수 있도록 한다. 통일된 관리 전략의 한 부분으로서, 비즈니스 목적에 따라 해당 조직이 네트워크 자원을 할당할 수 있게 함으로써 중요한 응용들이 가장 높은 우선권을 가지고 망을 이용할 수 있게 하는 메커니즘을 제공한다.

옵티비티 정책 서비스가 제공하는 기능들은 다음과 같다.

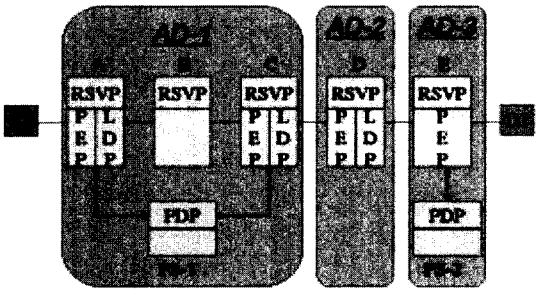
- 빠른 QoS 제공 : 비즈니스 응용에 맞춰 트래픽에 우선순위를 줄 수 있도록 한다.
- 정책 기반의 방화벽
- 비즈니스에 중요한 응용들을 위한 최적화된 성능
- 중앙집중식 QoS 구성 및 관리
- 스케줄링 기능 : 스케줄에 기초한 응용 트래픽의 우선순위 부여를 가능하게 한다.
- 사용이 편리한 자바기반의 관리 지원
- 트래픽 우선권 부여를 구현한 DiffServ
- 2계층, 3계층 양 계층에서의 트래픽 우선권 부여가능
- 다수의 망 관리자들 사이의 협동 작업
- SNMP 기반 보고

4.3.4 IBM

IBM은 네트워크의 정책관리를 단일화하면서 보안을 강화한 차세대 정책관리 아키텍처 ADN(Application Driven Networking)을 제시하고 있다. 이 아키텍처는 기존 네트워크에서 요구되던 수많은 정책 서버들이 필요 없으며, 정책결정 속도도 25배나 빨라져 사용자들은 이로 인해 연간 유지보수 비용을 절감할 수 있다는 장점을 가지고 있다. ADN은 사용자 인증 등을 통해 네트워크 보안을 유지하면서도 전송 효율성을 보장해주는 네트워크 아키텍처를 가지고 있으며, 기존에 설치된 정책의 복잡성을 단순화하면서 단일 시스템 레벨 인터페이스에서 모든 정책 결정이 가능하도록 설계된 것이 특징이다. 또한 응용 레벨과 네트워크 레벨에서 정책을 할당할 수 있어 성능 향상을 꾀할 수 있으며, 네트워크 보안에 대한 통제도 가능하다

5. 정책기반 네트워킹 구조

지금까지 살펴본 정책기반 네트워킹 시스템 구조는, IETF/DMTF에서 진행시키고 있는 표준화 작업의 구성요소들로 이뤄져 있다(그림 3). 이러한 요소들은 정책기반 시스템에 있어서의 필수적인 요소로서, 추가적인 요소들은 정책기반 시스템의 설계 필요요인에 따라



(그림 3) 정책기반 네트워킹 프레임웍

네트워크 감시, dimensioning, 트래픽 예측 등의 요소들로서 더해질 수 있을 것이다[13] .

◎ 정책 관리 도구 : 네트워크 관리자가 해당 네트워크에 대한 정책을 입력할 때, 이에 대한 일관성을 검사하고, 다른 정책과의 모순을 검사함으로써 관리자에게 관리의 용이성을 줄 수 있는 사용자 인터페이스를 제공하고, 높은 레벨의 정책을 낮은 레벨의 정책과 매핑시켜 변환시키는 기능을 제공한다.

◎ 정책 저장소 : 정책들이 저장되는 곳으로서 저장소는 중앙에 위치해서 네트워크 관리자가 중앙집중 방식으로 관리할 수 있게 한다. 이 저장소는 LDAP 디렉터리나 데이터베이스, 웹 서버 등이 될 수 있으나, IETF에서는 LDAP 디렉터리 서비스를 제시하고 있다.

◎ PEP : 네트워크로부터의 결정 요청에 대해 PDP로 전송하고, PDP에서 결정된 사항을 네트워크 요소에서 실행하게 된다. PDP사이의 통신 프로토콜은 COPS(Common Open Policy Service)가 쓰인다.

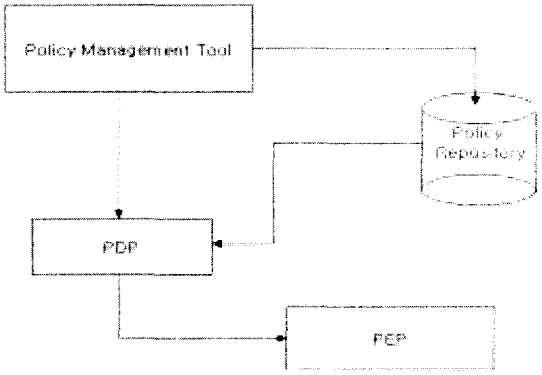
◎ PDP : 저장소에 저장되어 있는 정책을 기반으로 해서 PEP가 해석할 수 있는 적절한 형식과 문법으로 변환시켜 PEP로부터의 요청을 처리/결정한다. 또한, 현재 네트워크의 상태를 점검하여 네트워크 응용들에 대한 현재의 조건이 충족되는 가를 입증할 수 있도록 한다.

이러한 요소들은 정책기반 시스템에 있어서의 필수적인 요소로서, 추가적인 요소들은 정책기반 시스템의 설계 필요요인에 따라 네트워크 감시, dimensioning, 트래픽 예측 등의 요소들로서 더해질 수 있을 것이다[14].

또한, 그림 4에서와 같은 RSVP기반의 QoS 서비스 체계를 예로 살펴본다면, 각 PDP는 하나의 도메인에 하나 이상의 개수가 위치할 수 있고, PEP는 각 도메인 가장자리에 위치해서, 각 도메인에서 나가고 들어오는 트래픽에 대하여 결정할 수 있다. 각 도메인에서 PDP와 정책저장소가 정책서버로서 역할을 하게 된다.

6. 결 론

본 논문에서는 정책기반 네트워킹에 대한 정책에



(그림 4) 인터넷에서 정책 요소의 위치

대한 요소, 표준화 동향, 상용제품을 기초로 한 업체들의 동향에 대하여 살펴보았다. 최근에 많은 통신 장비들이 정책기반의 시스템으로 제작되어 출고되고 있고, 정책기반의 네트워킹 기법이 새로운 대안으로 떠오르고 있다. 이는 네트워크의 역동적인 변화에 망 관리자의 직접적인 대체 없이도 지능적으로 대처할 수 있는 방안을 정책기반의 시스템에서 찾을 수 있기 때문일 것이다.

지금까지 정책기반의 시스템들은 주로 QoS와 보안에 치중되어 개발되어 오고 있으며, 차후 다른 기능에 대한 부분까지 확장될 수 있을 것이다. 그렇지만 이러한 정책기반 시스템의 궁극적인 형태는 네트워크 관리와 통합된 형태로 나타날 것이다. 이러한 연구 경향에 따라서, SNMP 프로토콜을 이용한 관리 시스템과의 통합 및 이에 따른 계층적 구조의 설계 및 각 기능 모듈의 개발에 대한 노력이 활발하게 이뤄지고 있다.

참 고 문 헌

[1] R. Braden, et al, Integrated Services in the Internet Architecture: An Overview, RFC 1633, 1994.

[2] S. Blake, et al, An Architecture for Differentiated Services , RFC 2475, 1998.

[3] R. Braden et al, Resource Reservation Protocol Version 1 Functional Specification, RFC 2205, 1997.

[4] http://www.ietf.org/html.charters/rap-charter.html.

[5] http://www.ietf.org/html.charters/diffserv-charter. html.

[6] Dinesh C. Verma, "Policy-Based Networking-Architecture and Algorithms," New Riders Publishing, 2001.

[7] Dinesh Verma, "Simplifying Network Administration using Policy based Management", IEEE Network Magazine, March 2002.

[8] Raju Rajan, Dinesh Verma, Sanjay Kamat, Eyal Felstaine, and Shai Herzog. "A policy framework for integrated and differentiated services in the internet", IEEE Network, 13(5):36--41, September/October 1999.

[9] M. Sloman, Policy Driven Management For Distributed Systems, Journal of Network and Systems Management, Vol.2, No.4, pp.333-360, Plenum Publishing, December 1994.

[10] M. Sloman, Policy Driven Management For Distributed Systems, Journal of Network and Systems Management, Vol. 2, No. 4, pp. 333~360, Plenum Publishing, December 1994.

[11] M. Stevens et al., Policy Framework, Internet Draft, draft-ietf-policy-framework-00.txt, September 1999.

[12] http://www.cisco.com/warp/public/cc/pd/nemnsw/cap/tech/caqos_wp.htm.

[13] Paris Flegkas, Panos Trimintzios, and George Parvlou, A Policy-Based Quality of Service Management System for IP DiffServ Networks, IEEE Network Magazine, March 2002.

[14] The TEGUILA IST Project. http://www.isttequila.org/.

◐ 저 자 소 개 ◑

송 왕 철

1982년 2월~1986년 2월 연세대학교 식품공학과(공학사)
1987년 3월~1989년 2월 연세대학교 전자공학과(공학사)
1989년 3월~1991년 2월 연세대학교 전자공학과(공학석사)
1991년 9월~1995년 8월 연세대학교 전자공학과(공학박사)
2001년 2월~2002년 1월 University Of Western Ontario, Postdoctoral Fellow
1996년 3월~현재 : 제주대학교 통신컴퓨터 공학부(부교수)