

主題

인터넷상의 주요 QoS 관리 기술 동향

한국전자통신연구원 정태수, 최태상, 이유경

차 례

- I. 서 론
- II. QoS 관리 핵심요소 기술
- III. QoS 관리 기술 연구 및 표준화동향
- IV. QoS 관리 제품 동향
- V. 결 론

요 약

지난 몇 년간 인터넷망은 세계 도처를 연결하면서 인터넷 사용자의 수를 기하급수적으로 늘렸으며, 비디오 텔레컨퍼런스, Video-on-Demand(VoD), 가상현실 등과 같은 새로운 응용들 뿐 아니라 기존의 전화, 라디오 및 TV서비스까지 제공하면서 엄청난 트래픽 증가를 가져왔다. 이는 인터넷 망의 대역폭 확대를 요구하고 있으며, 단순한 대역폭의 증가만으로 이러한 엄청난 수요를 충족시킬 수 없다는 것이 대다수의 공통된 의견이다. 왜냐하면 인터넷 트래픽이 단순히 양적으로 증가할 뿐만 아니라 트래픽 특성상의 다양한 변화가 일어나고 있으며 mobile 환경을 수용해야되는 분제 등 다양한 새로운 요구에 부응하기 위한 변화가 동반되어야 한다. 본 고에서는 이러한 변화가 왜 일어나고 있으며 어떻게 대처해야 되는가에 대한 기술적인 해답을 찾기 위해서 전 세계적으로 활발히 진행되고 있는 인

터넷 QoS 관리 기술의 연구 및 표준화 동향에 대해 논하고자 한다.

I. 서 론

인터넷의 IP 기술은 끝없이 많은 시스템과 통신 매체들을 연결하는 글로벌 네트워크의 형성을 가능하게 만들었다. 전세계적으로 전자 우편과 웹 항해가 업무, 연구, 학업 그리고 레저 등을 수행하는 일상생활의 수단이 되었다. 또한 라디오, 텔레비전과 같은 방송망과 일상생활에서 빠져서는 안될 전화망이 편리성, 보편성, 융통성을 확장하기 위해서 IP와 통합을 시도하고 있으며, 이러한 새로운 네트워크의 출현이 새로운 응용과 나아가서는 새로운 사용자들을 창출하는 견인차 역할을 하고 있다.

이 추세의 가장 큰 원인은 IP 기술의 단순성에 근거한다. 즉, 인터넷은 대부분의 지능을 네트워크의

종단으로 몰고 네트워크 내부에서는 목적지 주소를 바탕으로 단순하게 정보를 전달하기만 하는 단순한 구조를 가지고 있다. 따라서 인터넷은 네트워크 전달 장치인 라우터의 자원의 여부에 따라 데이터의 전달이 지연되거나 혹은 손실될 수도 있는 최선형 서비스로의 특성만 가지게 되었다. 사용자 수요의 폭발적인 증가와 요구의 다양성은 이러한 최선형 서비스에 자원만 늘리면 해결되는 단순한 문제가 더 이상 아니게 되었다. 멀티미디어 서비스와 IP 전화와 같은 응용은 대용량의 대역폭 뿐만 아니라 엄격한 시간적인 전달 요구 사항 및 일대다/다대다의 전달 요구사항을 갖게 되었다. 즉, 근본 인터넷의 철학인 네트워크의 단순성을 탈피하고 지능을 첨가해야 하는 상황이 된 것이다. <표 1>은 인터넷 응용을 전송율, 전송방식 및 지연성에 따라 분류하고 있다.

<표 1>의 다양한 요구사항을 가진 응용들을 지원하기 위해서는 대역폭의 증대뿐만 아니라 전송 신뢰

성, 실시간성 등 충족 시켜야 될 많은 기술들이 필요하다. 이러한 기술들을 간단히 표현하면 서비스/응용의 QoS 관리 기술이라고 통칭할 수 있다. 즉, 최선형 서비스 형태에서 탈피해서 차세대 인터넷의 상업용 QoS 서비스를 제공하기 위해서는 QoS 관리 기술이 필수 불가결한 요소이다.

QoS는 크게 사용자가 실제로 서비스 QoS를 느끼는 표현 및 체감 QoS와 사용자의 서비스 이용 및 제어의 편리성을 보장하는 이용 및 제어 QoS로 나눌 수 있다. (그림 1)은 이들간의 관계를 보여주고 있다.

종단 사용자간의 서비스 QoS는 사용자 단말, 전달 링크, 스위치나 라우터 같은 망장치에서의 지연 및 Throughput, 손실 특성 등에 의해 복합적으로 영향을 받게 되므로, 종단간 QoS 보장형 서비스를 지원하기 위해서는 이들 QoS 요소 변수들을 제어할 수 있는 네트워크 서비스 측면의 제어 메커니즘이

표 1. 네트워크 응용 분류표 (출처: iBAND 2백서)⁽¹⁾

	최 선 형		동 제 형	보 장 형
다방향 (many-to-many bidirectional)	Asynchronous Burst - News - Session announcement	Interactive Stream - Distance learning - Multi-Player games Interactive Burst - Chat (IRC) - Resource discovery - Shared editing	Isochronous Stream - A/V Conferencing - Distributed simulation - Real-time modeling	Mission-Critical Stream - Distributed process Mission-Critical Burst - Auction
양방향 (one-to-one bindirectional)		Interactive Stream - Thin client - X-windows Interactive Burst - Web browsing - Resource sharing - Database access - POS transactions - Remote login - Chat(text-based)	Isochronous Stream - Telephone Isochronous Burst - Database updates	Mission-Critical Stream - Telemedicine - Remote control Mission-Critical Burst - Financial X-actions
단방향 (one-to-one or one-to-many unidirectional)	Asynchronous Burst - E-mail - File Transfer - Push Media	Synchronous Stream - Streaming media - Data collection - Push media	- Isochronous Stream - Data collection - Process monitoring - Push media	Mission-Critical Stream - Data collection - Process monitoring - Push media

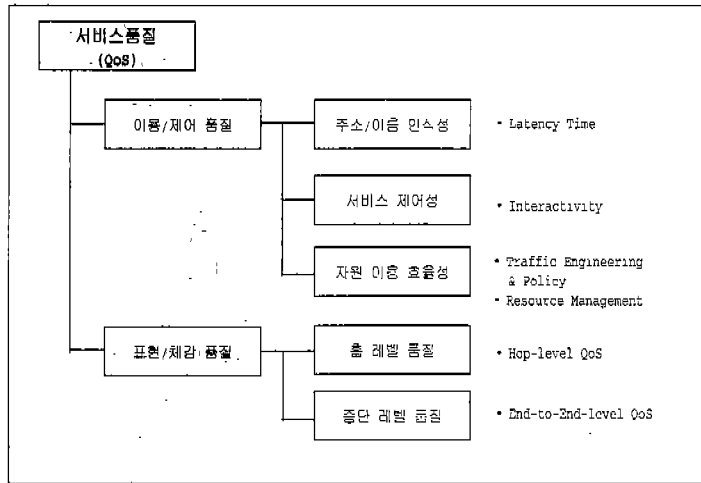


그림 1. QoS의 정의

필요하다. 예를 들면 망에서 실시간 서비스를 지원하기 위해서는 요구되는 자원을 미리 예약하거나 망 내의 트래픽 부하를 반영하여 라우터의 큐잉 기능을 적절히 설정하거나 혹은 설정된 트래픽 특성이 제대로 운영되는지를 모니터링하는 기능 등이 이에 해당한다. 이와 같이 네트워크 서비스 레벨에서 사용자의 QoS 보장을 위한 기술이 바로 QoS 관리 기술로 정의할 수 있다.

본 고에서는 QoS 관리 기술을 소개하기 위하여 다음 장에서 핵심 요소 기술들에 관해 간단히 설명을 하고 현재 진행 중인 관련 기술의 연구 및 표준화 동향을 살펴본 뒤 아직 초보 단계이기는 하나 시험 중이거나 발표 되고 있는 제품들을 소개하면서 인터넷 상에서의 QoS 보장의 가능성에 대해 정리하고자 한다.

II. QoS 관리 핵심요소 기술

QoS 관리 기술은 크게 QoS 보장 기술과 제공된 QoS의 상태를 측정하기 위한 QoS 모니터링 기술로 나뉘어 진다. QoS 보장 기술은 다시 각 네트워

크 장비에서 제공되어야 될 트래픽 관리 기술, 네트워크 전체 입장에서 QoS의 보장 기술 및 이를 관리할 수 있는 정책기반의 QoS 관리 기술로 나뉘어 진다. 또한 QoS 모니터링 기술은 프로토콜 모니터링, 네트워크 모니터링, 종단간 QoS 모니터링 기술로 세분된다.

1. 트래픽 관리 기술

트래픽 관리 기술은 다양한 세부 기술들이 소개되어 있으며 크게 큐관리(Queue management), 트래픽 셰이핑(Traffic shaping), 수락제어(Admission control), 폴리싱(Policing), 혼잡 관리(Congestion management)의 분야로 나누고 각 분야별 세부적 알고리즘이나 방법들은 아래에서 설명한다. 이들 각각은 독립적으로 사용될 수도 있지만 대표적인 QoS 관리 모델로 알려진 인터넷의 통합서비스(Integrated Service)⁽²⁾ 모델과 차등서비스(Differentiated Service) 모델⁽³⁾에 서와 같이 복합적으로 사용되기도 한다.

가. 큐 관리(Queue management)

큐잉(Queuing)은 라우터 구조에서 핵심 부분으로서, 프레임들이 입력 프로세스를 거쳐 패킷으로 합쳐지고 무결성을 검사 받은 뒤 포워딩 프로세스에 의해 출력될 인터페이스가 결정되고 출력 프로세스에 의해 다시 프레임화 되어 다음 라우터로 전달되는 과정을 포함한다. 큐관리는 이 과정에서 프로세스간의 연결 역할을 하게 된다. 따라서 큐잉이 지금까지, 현재, 그리고 미래의 서비스 차별화를 위해 해 오거나 할 역할을 이해하는 것이 매우 중요하다. 다음은 큐관리를 위해 제안된 대표적인 방법들이다.^[4]

• FIFO Queuing

트래픽을 Store-and-forward 방식으로 처리하는 가장 대표적인 방법이다. 네트워크의 대역폭이 충분히 크고 스위칭/포워딩 성능이 뛰어난 버스트 트래픽만 처리하면 되는 경우가 대부분이므로 FIFO 큐잉방식이 적절하지만, 실제 상황에서는 트래픽의 양이 FIFO 큐가 처리할 수 없을 만큼 발생할 경우가 많이 생기고 있다. FIFO 큐가 채워질 경우 서비스의 종류와 무관하게 패킷이 버려지는 상황이 발생하여, 차별적인 서비스를 제공해야 할 경우에 한계에 부딪히게 된다. 따라서 아래에서 설명될 다른 형태의 방법이 필요하게 된다.

• Priority Queuing

Priority 큐잉은 FIFO 큐잉 방식을 변형한 것으로서 특정 유형의 트래픽을 구분하여 출력 Queue의 앞부분으로 보내 먼저 처리될 수 있도록 한 방식이다. 이 방식은 가장 초보적인 서비스 차별화를 가능하게 하지만 여러 가지 단점을 가지고 있다. 서비스 차별화 단계를 많이 만들수록 처리 부담을 가중시키고 패킷 포워딩 성능을 저하시키게 된다. 그리고 가장 높은 우선순위 트래픽의 양이 많을 경우 순위가 낮은 트래픽은 버퍼 고갈로 인해 손실이 높아지게 되고, 지연에 민감한 응용의 경우에

는 제대로 작동을 하지 않을 수도 있게 된다. 점차 고속화 되는 네트워크 환경에서 이 큐잉방식은 확장성을 지원하기가 힘들다.

• Class-Based Queuing (CBQ)^[5]

Priority 큐잉 방식의 단점인 우선권이 있는 클래스를 제외한 타 클래스 트래픽의 자원을 완전히 거부하는 경우를 방지하기 위해서 최근에 제안된 방식으로 동류의 알고리즘이 이미 운영체제에서 많이 활용되고 있다. CBQ는 Priority 큐잉방식의 변형으로써 하나의 출력 큐 대신에 여러 개의 출력 큐를 클래스 별로 두어서 우선 순위를 정하고 각 큐별로 서비스 되는 트래픽의 양을 조절할 수 있는 방식이다. 이렇게 함으로써 어느 특정 클래스의 트래픽이 전 시스템 자원을 모두 독점하는 것을 방지한다. CBQ는 각 클래스별로 정해진 양의 대역폭을 보장할 수 있는 방식으로 알려져 있지만, 실제로는 완전 보장이라기 보다는 Priority 큐잉 방식보다는 약간 더 완화된, 클래스별로 자원이 완전 고갈되는 것을 막으면서도 각 클래스에 적절한 서비스를 제공할 수 있는 방식이다. 그러나, 이 방식도 여전히 복잡한 큐 관리에 소요되는 계산 부담 때문에 고속의 네트워크의 경우에는 확장성이 부족하게 된다.

• Weighted Fair Queuing (WFQ)^[6]

WFQ는 소량의 트래픽이 대량의 트래픽에 의해서 피해를 보지 않도록 플로우 별로 큐를 두어 트래픽을 조절하는 공정성 측면과 특정 기준에 따라 가중치(Weight)를 정하고 이에 따라 같은 양의 트래픽을 가진 플로우 간에도 차별을 두는 가중치 측면을 복합적으로 적용한 큐잉 방식이다. 이때 가중치를 결정하는 방식은 구현 방식 의존적이며 한가지 예로 IP 헤더의 Type of Service(TOS) 필드 중 IP precedence 비트를 사용하는 구현이 소개되었다. WFQ 방식도 priority 큐잉 혹은 CBQ와 비슷한 특성을 가지고 있는 관계로 고속의 네트워크

환경에서 확장성을 가지기가 어렵다. 또한, 트래픽 플로우 간을 차별 할 수 있는 메커니즘의 부재로 인한 granularity 부족이 이 방식의 큰 단점이다.

나. 트래픽 셰이핑

트래픽 셰이핑은 네트워크 내부로 유입되고 유출되는 트래픽의 양과 유출되는 트래픽의 속도를 조절하는 메커니즘이다. 또한 Ingress 포인트에서 유입되는 트래픽의 플로우를 구분하여 플로우별로 셰이핑하는 기능도 포함한다. 대표되는 방법으로, leaky-bucket 방법과 token-bucket 방법 그리고 이들을 통합한 복합 방법이 있다.

● Leaky-Bucket 방식

Leaky-Bucket은 일정하지 않은 트래픽을 일정하게 유지시켜 네트워크에 전송시키기 위한 방식으로 ATM 네트워크에서 셀트래픽의 속도를 조절하기 위해 제안되었으나 패킷 네트워크의 제3계층에서도 사용되고 있다. Bucket(FIFO Queue)의 깊이(크기)와 전송율은 일반적으로 사용자가 조절할 수 있으며 바이트 단위로 표시한다. 이 방식은 네트워크로 전송되는 트래픽을 아주 단순히 제어하고 조절할 수 있으며 구현 또한 비교적 쉽고, 네트워크 내의 한 종류의 트래픽 양을 조절하는 임의의 임계치(threshold)로 사용할 수 있는 방식인 반면, 여러 종류의 트래픽 속도를 지원해야 하는 경우에는 비 효과적이며, leak rate이 고정된 값을 가지므로 네트워크 자원의 여유가 많을 때에도 충분히 활용할 수 있는 적용성을 가지지 못하는 단점을 가지고 있다.

● Token-Bucket 방식

Token-Bucket은 Leaky-Bucket과는 달리 Bucket 자체를 FIFO 큐로 사용하지 않고 트래픽을 제어하기 위한 제어용 토큰을 관리하는 용도로 사용한다. 트래픽은 토큰의 유무에 따라 흐름의 제

어를 받게 되는데, 고속도로의 톨게이트에서 통행료를 지불하는 차량들이 통과하듯이 트래픽은 토큰이 있을 경우 통과 하게 된다. 또한 항상 정해진 일정량만 통과하도록 되어있는 Leaky-Bucket과는 달리 트래픽이 버스티한 경우에도 정해진 한계치 범위 내에서는 통과가 가능하다. 따라서 네트워크의 자원 활용을 보다 효율적으로 할 수 있는 장점을 가진다. 또한 하나의 토큰과 한계치 값을 갖는 방식에서 다수 개를 허용하는 변형된 방식들도 소개되었는데 이를 통해 서로 다른 클래스 트래픽의 개별적인 조절이 가능하다.

● 복합 방식

위 두 가지 방식의 장점을 활용한 복합 방식도 제안되었는데, 먼저 Token-Bucket으로 트래픽 양의 버스트를 허용하면서 조절한 후, Leaky-Bucket을 이용해서 특정 한계치의 값만큼 일정하게 트래픽을 전송하는 방식이 복합 방식이다. 이 방식을 이용하면 다수의 Token-Bucket 방식이 가질 수 있는 특정 클래스의 자원 독점 혹은 경쟁을 막을 수 있을 뿐만 아니라 트래픽 클래스의 차별화를 훨씬 용이하게 구현할 수 있게 된다.

다. 수락제어

수락제어는 어떤 종류의 트래픽을 네트워크로 받아 들일 것인가를 결정하는 정책이다. 이러한 정책 없이 네트워크를 운영할 경우 네트워크 내부에서 발생할 수 있는 다양한 문제점들에 대해 해결책을 제시할 수 없게 되어 QoS 보장이 불가능하게 된다. 즉, 수락제어는 QoS를 제공하는데 필수적인 요소이며, 이를 제공하기 위해 Leaky-Bucket 혹은 Token-Bucket을 이용한 단순한 방법에서부터 복잡한 QoS 변수를 적용하여 수락제어를 하는 통합서비스 모델. 그리고 자원의 유무와 별도로 네트워크 자체의 정책에 따른 수락제어에 이르기까지 다양한 방법들이 적용될 수 있다.

라. 혼잡관리

엄격한 수락제어와 큐관리에도 불구하고 다양한 트래픽을 수용하다 보면 혼잡상황을 완전히 피할 수는 없게 된다. 혼잡은 네트워크의 작동을 예상하기 힘들게 만들고, 시스템 버퍼들을 채워서 데이터 손실율을 높이며, 다시 재 전송율을 증가시켜 악순환을 반복하게 하는 주범이 된다. 다음은 혼잡 관리의 두 가지 대표적인 방식을 소개한다.

• Random Early Detection (RED)⁽⁷⁾

수천/만 개의 플로우가 동시에 네트워크에 존재할 때, 어느 한 부분에서 혼잡 상황이 발생하면, 각 플로우가 거의 동시에 데이터 손실을 겪게 되는 글로벌 동기화 현상을 방지하기 위하여 임의로 플로우를 선택하여 탈락(drop)시키는 방식을 RED라고 한다. 이를 위하여 RED는 큐 길이를 측정하여, 시스템 관리자가 설정해 둔 한계치 값에 접근하면 임의로 특정 플로우를 선택하여 패킷을 탈락시켜 송신측에서 송신 속도를 낮출 수 있도록 한다. 따라서 앞에서 설명된 비 FIFO 큐잉방식들의 단점인 패킷 순서 조정 및 큐 관리에 소요되는 계산 부담없이 혼잡 제어를 할 수 있는 장점이 있다. 그러나 이 방식은 혼잡 발생시 탈락시키는 플로우의 선택을 임의로 하기 때문에 서비스의 차별성을 두어야 하는 환경에서는 공정성을 유지하기가 쉽지 않다.

• Weighted Random Early Detection (WRED)

WRED는 RED의 단점을 보완, 서비스 차별성을 유지하면서도 혼잡을 제어 할 수 있는 방법으로 혼잡발생 시 탈락시킬 플로우를 특정 기준(정책)에 준하는 값에 따라 우선순위를 두고 선택하도록 한 방법이다. 이와 유사한 방식으로 Enhanced RED (ERED)⁽⁸⁾도 제안되었다.

2. 인터넷에서의 QoS 보장 기술

상기에 기술한 트래픽 관리 기술들을 사용하여, 인터넷 표준화 기구인 Internet Engineering Task Force(IETF)는 인터넷에서 사용자의 요구 사항에 따른 QoS를 제공하기 위해 여러가지 서비스 모델과 메커니즘을 제시하고 있다. 그 중에서 주목받고 있는 것은 크게 통합서비스, 차등서비스, Multi Protocol Label Switch(MPLS)라 할 수 있다. 다음은 각각의 QoS 보장 방법에 대해 살펴본다.

가. 통합서비스에서의 QoS 보장 방법

통합서비스는 크게 자원 요청을 수용할 지를 결정하는 수락제어, 패킷을 분류하여 그 결과에 따라 큐잉하는 분류자(Classifier), 패킷을 스케줄링하는 스케줄러(Scheduler), 그리고 자원을 예약하는 신

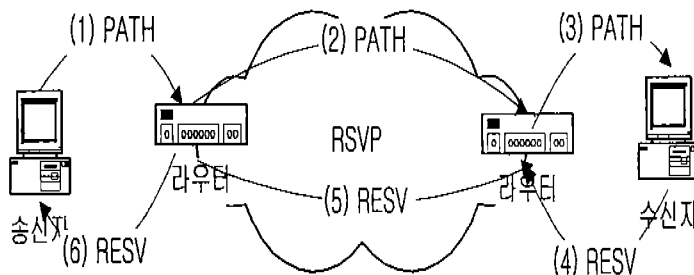


그림 2. RSVP 신호 절차

호 프로토콜의 4가지 요소로 구성된다. 패킷 분류자는 수신된 패킷의 헤더정보(수신자 주소, 프로토콜 타입, 포트번호)를 식별하고, 패킷 스케줄러는 서비스될 클래스를 결정하며, 수락제어는 QoS 요구사항을 노드가 만족할 수 있을 지를 판단하여 연결 여부를 결정한다.

대표적인 자원 예약 신호 프로토콜로는 ReSource reSeVation Protocol(RSVP)과 Stream protocol version II(ST-II)가 있으며, ST-II보다는 RSVP가 더 많은 주목을 받고 있다. 그 이유는 RSVP는 이질적인 특성을 갖는 수신자를 수용함으로써, 네트워크 자원을 효율적으로 사용하고, 그룹멤버십의 동적 변화에 대응하는 프로토콜의 오버헤드가 작기 때문이다.

(그림 2)는 RSVP의 메시지 흐름을 보여주고 있다. RSVP는 먼저 송신 호스트가 PATH 메시지를 통해 자신의 트래픽 요구사항을 수신 호스트에게 알려준다. PATH 메시지가 지나가는 경로의 망 노드 즉, 라우터는 경로 상태(PATH state)를 기록한다. PATH 메시지를 받은 수신호스트는 송신 호스트가 보내고자 하는 흐름의 특성을 보고 자신이 원하는 대역폭을 결정하여 RESV 메시지를 PATH 메시지가 전달된 반대방향의 경로를 따라 전송된다. 수신 호스트로부터 RESV 메시지를 받은 망노드는 메시지에 기록된 서비스 요구사항을 보고 현재의 망 자원으로 제공이 가능한지를 결정한다. 만약 요구를 수락한다면, 망 노드는 흐름 특성을 링크계층에 전달하고, 링크 계층은 주어진 특성에 따라 패킷 스케줄링과 패킷 분류 기능을 수행하여 사용자의 서비스 요구를 충족시키게 된다.

RSVP는 기존의 IP 네트워크와 장비를 그대로 사용하여 중단간 QoS를 보장할 수 있으나, 모든 라우터에서 흐름마다 자원을 예약하므로, 라우터가 유지해야 하는 상태 정보의 양이 많고, 이로 인해 프로세싱의 오버헤드를 가져오며, 모든 라우터가 RSVP, Multi-Field(MF) 분류, 패킷 스케줄링

등의 기능을 가져야 하는 단점이 있다.

통합서비스에서 망노드는 노드내의 의사 결정에 따라 호 요구에 대한 수락 제어를 수행하거나, 또는 도메인 내의 의사 결정을 하는 서버가 있다면 이로부터 자문을 얻어 호 수락 여부를 결정한다. 후자의 경우는 호 수락제어를 중앙집중적으로 관리할 수 있는 장점을 가지며, 단순히 통합 서비스의 호 수락 제어 기능 외에 정책 기반의 QoS 관리를 수행할 수 있게 한다.

나. 차등서비스에서의 QoS 제공 방법

앞에서 언급한 바와 같이 통합서비스에서 제안한 RSVP기술은 공중망으로 도입하기에는 확장성이 부족하다. 이를 보완하기 위해 제안된 차등서비스는 Differentiated Service Code Point(DSCP) 필드에 의해 서비스 수를 제한하고, 패킷의 분류, 마킹, 폴리싱과 웨이핑을 망 경계 노드에서 수행하고, 코아노드는 Behavior Aggregate(BA)분류만 수행하여 확장성 문제를 해결한다.

일종의 우선권 방식이라 할 수 있는 차등서비스는 최선형 서비스 외에 Assured Forwarding(AF) 서비스와 Expedited Forwarding(EF) 서비스를 제공한다. AF 서비스는 망이 혼잡할 때 사용자에게 일정수준의 서비스 품질을 보장하는 서비스로서, 실제 트래픽을 Service Level Agreement(SLA) 준수여부에 따라 트래픽을 in 또는 out 프로파일로 분류하여, Assured Queue에 넣고, RED 또는 RED with In and Out(RIO)로 스케줄링한다. EF 서비스는 사용자에게 낮은 지연과 지터를 제공하는 서비스로서, 사용자가 실제 트래픽을 EF 클래스로 세팅하여 전송하면, 망 제공자는 호수락 제어를 통해 프리미엄 서비스를 제공 가능할 지를 결정하여 다른 트래픽보다 더 빨리 전송한다. SLA를 초과한 트래픽은 드롭하며, egress 라우터는 SLA에 따라 리웨이핑 기능을 수행한다. 차등서비스에서 QoS를 제공하기 위해 망제공자는 사용

자가 원하는 QoS를 제공하기 위해 도메인 내의 각 노드에 클래스 별로 자원을 적절히 할당하고, 도메인 간에는 중단간 QoS가 보장되도록 SLA를 체결하여야 한다. 이의 기능을 수행하기 위해 대역폭 브로커(Bandwidth Broker) 기술이 제안되고 있다. 대역폭브로커는 도메인에 하나씩 존재하여, 인터-도메인에서는 이웃 도메인의 대역폭 브로커와 SLA를 체결하여 유지하는 기능을 수행하며, 인트라-도메인에서는 사용자나 응용으로부터의 QoS 요구를 받으면, 도메인 내의 자원 사용 정책에 따라 내부 자원을 할당하는 기능을 수행한다. 특히 이웃 도메인과 협상된 SLA에 기반하여 경계 라우터의 자원 구성 정보를 제공한다. 즉, 대역폭 브로커는 인터넷에서 QoS를 제공함에 있어서 정책 기반 QoS 관리 기능 중에서 자원사용량에 기반한 QoS관리를 수행하는 시스템이라고 할 수 있다.

다. MPLS에서의 QoS 제공 방법

MPLS는 라벨에 따라 패킷을 포워딩한다. MPLS는 라벨을 사용하여 도메인 내의 한 중단간에 다수의 경로를 설정할 수 있으며, 설정된 경로는 서로 다르고 가변적인 대역폭을 가져, 트래픽의 지연 및 손실 민감도에 따라 차별화된 서비스를 제공할 수 있다.

MPLS에서 트래픽 전송은 다음과 같이 수행된다. 에지 라우터는 헤더 정보를 분석하여 사용할 경로를 결정하며, 일치하는 경로가 있으면 이를 패킷에 붙여 전송한다. 코어 라우터는 라벨에 의해 지정된 경로를 따라 패킷을 단순히 전송한다. 이는 차등 서비스와 유사한 구조를 갖지만, 차등서비스와의 차이는 ingress 노드는 MPLS 헤더를 추가하고, 코어 노드에서 DSCP 필드가 아니라 라벨을 참조하며, egress노드에서 MPLS 헤더를 제거한다는 점이다.

MPLS에서 QoS를 제공하기 위해서는 설정된 경로에 대역폭을 할당할 필요가 있으며, 이를 위해 대역폭 정보와 명확한 경로를 명시하여 경로를 요청

하는 Explicitly Routed Label Switch Path (ER-LSP)가 제안되고 있다. ER-LSP를 구현하는 방법은 Constraint-based Routed Label Distributed Protocol(CR-LDP)를 사용하거나 RSVP를 확장하여 이용하는 방법이 IETF에서 논의 중에 있다. 기술적인 관점에서는 비슷한 신호 기능을 가지며, CR-LDP는 구현이 용이하고, 상호 운용성이 보장되며, 여러 벤더가 참여하고 있는 장점을 가지고, RSVP를 사용하는 방법은 RSVP 메시지에 explicit-route 객체만 추가하는 약간의 수정으로 이미 구현/설치된 RSVP를 사용할 수 있는 장점이 있다.

라. 기 타

인터넷에서 QoS제공과 관련된 또 다른 연구분야로 트래픽 엔지니어링, QoS 라우팅과 Constraints-Based Routing(CBR)을 들 수 있다. 트래픽 엔지니어링기술은 망에서 혼잡이 발생하지 않도록 망을 구성하는 기술이다. 통합서비스, 차등서비스, 그리고 최선형 서비스는 트래픽이 많지 않을 경우 별 차이가 없을 수 있다. 그러나 트래픽이 많을 경우 통합서비스와 차등서비스 메카니즘은 현저한 성능 저하를 가져온다. 따라서 망에서 QoS를 제공하기 위해서는 트래픽 엔지니어링 기술은 중요한 역할을 수행한다.

혼잡은 망자원이 부족한 경우와 망에서 트래픽이 고르게 분배되지 못한 경우에 발생한다. 전자의 경우 망자원을 업그레이드하는 것이 필수적이며, 후자의 경우는 라우팅 프로토콜이 무조건 최단 경로를 선택함으로 발생한다. 따라서 OSPF의 Equal Cost Multi-Path(ECMP)선택사항등을 사용하면 어느 정도 트래픽을 고르게 분배할 수 있으나, 경로가 하나 존재하면 소용없다. 따라서 망 관리자는 같은 비용의 여러 경로가 존재하도록 망을 구성하여야 한다.

QoS 라우팅과 CBR은 QoS 요구에 따라 가장

만족하는 경로를 찾는 반면에 CBR은 QoS 라우팅의 확장으로서, 망의 토폴로지, 흐름의 요구사항, 링크의 가용자원, 정책 등을 고려하여 경로를 찾는다. 따라서 로드가 큰 최단경로보다는 로드가 작은 더 긴 경로를 계산하여, 망에서 트래픽을 고르게 분배한다.

QoS 라우팅을 지원하기 위해서는 새로운 링크 상태 정보를 분배하고 이를 사용하여 계산하는 알고리즘이 요구된다. 라우팅 프로토콜은 링크 상태 정보 분배 주기가 문제시 되므로, 중요한 변화 있을 때 분배하도록 한다. CBR에서 제약식에 따라 경로를 계산하는 알고리즘은 일반적으로 NP-complete 문제이지만, 대역폭과 홉 수를 제약식으로 하는 경로를 찾는 알고리즘은 간단하고 Dijkstra 또는 Bellman-Ford의 알고리즘을 사용할 수 있다.

3. 정책기반 QoS 관리 기술

위에서 언급된 트래픽 관리 기술들은 각 네트워크의 요소들에서 개별적으로 제공되는 기능들이며, QoS 보장 기술은 인터넷에서 QoS를 제공하기 위해 해당 응용 서비스 마다 자원을 예약하거나 할당하는 기능을 수행하며, 이 경우 일관성 있고 효율적인 종단간의 QoS 보장을 위해서는 네트워크 도메인 내부와 도메인간 전반적인 입장에서 자원관리를 할 필요가 있는데, 정책기반의 관리를 통해서 이 역할을 수행할 수 있다. 먼저 네트워크 도메인 내부에서는 도메인 특성에 맞는 정책에 따라 QoS 관리를 수행하며 도메인 간에는 서로의 협상을 통해서 종단간의 QoS를 보장하여야 한다.

정책 기반의 QoS 관리는 크게 정책 편집, 정책 충돌 방지, 정책 생성, 정책 분배, 정책 진화 기능으로 구성되어 있다. 정책 편집 기능을 통해서 네트워크 관리자는 네트워크와 사용자의 정책을 생성한다. 생성된 정책은 일단 기존의 정책과 충돌이 일어나는가를 정책 충돌 방지 기능을 통해서 검토한다. 그 후

정책 생성 기능은 네트워크 장비가 이해할 수 있는 형태로 정책을 변경 생성 한다. 변경 생성된 정책 정보는 필요한 네트워크 장비에 분배되며 각 장비는 받은 정책을 적용하여 트래픽을 제어한다. 일단 분배된 정책은 네트워크의 상태나 특정 일시 등과 같은 영향으로 변경을 요하게 되기도 하는데 정책 진화 기능을 이러한 변화를 감지하는데 필요한 기능을 한다.

정책 기반 관리 기술은 단순히 QoS 관리 뿐만 아니라 보안, 경로 제어 등을 위한 용도로 광범위하게 사용되므로, 정책 기반 관리 기술은 확장성 있는 구조를 가지는 것이 매우 중요하다.

가. 정책기반 QoS 관리 시스템 구조

정책 기반의 QoS 관리를 위해서 IETF, Distributed Management Task Force (DMTF)^[9] 등에서는 공통된 시스템 구조를 정의하기 위해 상호 협력 중에 있으며, 현재까지 정의된 구조를 (그림 3)에서 보여 주고 있다.

정책 기반 QoS 관리 시스템은 크게 정책을 생성, 수정, 편집, 제거하거나 기존의 정책과의 충돌여부를 확인하고 해결하는 기능을 하는 정책 톨, 정책 저장 및 검색을 위한 디렉토리 시스템, 정책 결정을 책임지는 정책 사용자(Policy Consumer or Policy Decision Point(PDP))와 실제 정책이 수행되어지는 장치 (Policy Target or Policy Enforcement Point(PEP)), PDP Proxy로 구성되어 있다. (그림 3)에서 보듯이 PDP와 PEP는 통합된 시스템이거나 분산된 형태로 존재할 수 있으며, 분산 시스템이 확장성 면에서 유리하다. PDP, PEP 및 디렉토리 간에는 통신을 위한 프로토콜이 필요한데, 현재 거론되고 있는 대표적인 프로토콜로 Common Open Policy Service (COPS)^[10]와 Light Weight Directory Access Protocol(LDAP)^[11]이 있다. COPS는 PDP와 PEP 사이에 정책 정보를 전달하기 위해 필

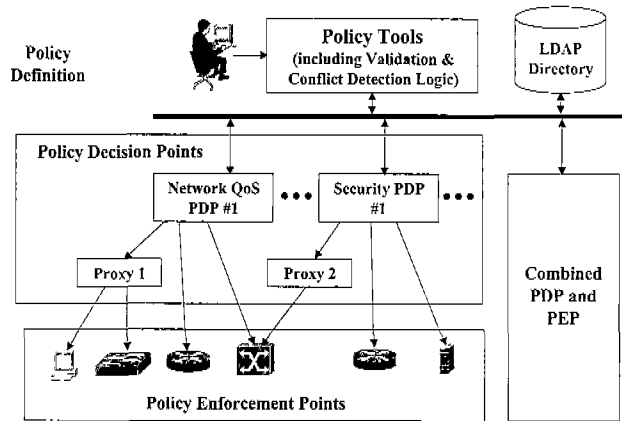


그림 3. 정책기반 QoS관리 시스템 구조

요하며, LDAP은 PDP나 PEP가 정책 정보를 저장, 검색, 획득하는데 필요한 프로토콜이다. 이 외에 정책기반 QoS 관리에 필요한 프로토콜에 대한 보다 상세한 내용을 요약하면 다음과 같다.

나. 정책기반 QoS관리 시스템 프로토콜

정책프로토콜은 각 라우팅 시스템에서 사용자 데이터 전달 요구를 수신하였을 때 사용자에게 적용할 수 있는 정책에 따라 사용자를 받아들이거나 거절하는 기능을 수행하기 위하여 라우터와 서버간에 동작하는 프로토콜이다. 이러한 정책 프로토콜에 대하여 다음과 같은 사항들이 요구되어진다.

- 신뢰성
- 작은 지연
- Opaque objects 전송 기능-PEP-initiated, two-way Transactions 기능
- Asynchronous notification 기능-Mmulticast groups 처리 기능
- QoS Specification 기능

기존에 정책 프로토콜로 이용되어 왔던 프로토콜로는 RADIUS^[12], LDAP, Simple Network Management Protocol(SNMP)등이 있으나

이들은 신뢰성이 부족하고 서버가 시작하는 메시지 전달 기능 등을 제공하지 못하고 있다. 이러한 단점을 보완하고 위에 기술한 정책 프로토콜 요구를 만족시키기 위하여 제안된 정책프로토콜로는 IETF의 Resource Allocation Protocol (RAP)^[13] 워킹그룹에서 제안한 COPS와 RADIUS를 기반으로 만들어진 DIAMETER^[14]가 있다. 서버에서 정책프로토콜 기능을 가지는 것을 고려해본다면 현재 정책 프로토콜에 대한 완전한 표준 규격이 나오지 않은 상태이기 때문에 COPS나 DIAMETER와 같은 프로토콜의 사전 도입 방안보다는 기존 프로토콜을 이용하는 단계적 접근 및 통합적인 접근 방안이 필요하다. 즉, 초기에는 RADIUS, SNMP, Common Line Interface(CLI) 등과 같이 기존 라우터들이 이용하는 프로토콜을 이용하여 정책 프로토콜로 이용하고 추후 정책 프로토콜에 대한 국제 표준이 결정된 후 그것을 수용하도록 하는 단계적 접근과 PDP는 다양한 라우터를 수용할 수 있는 능력을 가지고 있어야 하므로 기존의 다양한 프로토콜들을 대부분 수용할 수 있어야 할 것이다.

4. QoS 모니터링 기술^[15]

QoS 보장이 된 후 사용자들이 가장 궁금해 하는

것은 제공 중인 QoS가 요구사항에 따라 제대로 지켜지고 있는지를 하는 것이다. 이를 위해 네트워크 장비 및 네트워크 상태 정보를 규칙적으로 측정하여 분석하고 정책 관리 기능에 피드백하여 QoS 관리에 활용하며, 또한 이를 사용자가 이해할 수 있는 형태의 정보로 변경하여 분배함으로써 요구한 조건이 잘 지켜지고 있는지를 확인 시킬 필요가 있다.

QoS 모니터링 기술은 트래픽 측정, 분석, 표현 기술로 나뉘어 지며 적용할 범위에 따라 프로토콜 모니터링, 네트워크 모니터링, 종단간 QoS 모니터링 기술로 세분된다. 프로토콜 모니터링은 특정 QoS 구조를 가지는 네트워크 도메인에서 사용되고 있는 프로토콜이 제대로 작동되고 있는지를 점검하는데 필요한 기술로서 특정 QoS 관리 구조의 완결성을 확인할 수 있는 좋은 기준이 된다. QoS 모니터링을 위한 기술로는 먼저 프로토콜의 경우에는 모니터링을 하려는 목표 프로토콜이 동작되고 있는 호스트나 네트워크 장비에서 요구된 형태로 프로토콜이 잘 동작하는지를 시험할 수 있는 툴이 필요한데, 주로 프로토콜이나 장비에 의존적으로 개발이 된다. 예로 RSVP 프로토콜의 동작상태를 모니터링 할 수 있는 RSVP Diagnostics 툴^[16]과 같은 것이 있을 수 있다.

네트워크 모니터링 기술은 네트워크 자원의 사용 정도나 소비정도를 측정하여 전반적인 상태를 모니터링함으로써 네트워크 엔지니어링과 관리에 도움을 준다. 네트워크 모니터링을 위해서는 기존의 SNMP 기반의 네트워크 관리 툴을 활용하여 현재 표준화가 진행 중인 QoS 보장 관련 기술용 MIB을 구현, 네트워크의 QoS 보장 상태를 모니터링 할 수 있다. 예로 Realtime Traffic Flow Measurement(RTFM) 구조^[17]를 기반으로 한 모니터링 툴이 있다. 이 구조의 주요 구성요소로는 meter, meter reader, meter manager, analysis applications이 있다. 모니터링 포인트에 SNMP agent인 meter를 설치하여 수집된 자료를

RTFM MIB에 저장하면, meter reader는 분산되어 있는 meter에서 필요한 자료를 수집한다. 이때 meter manager는 meter와 meter reader를 관리하는데, 어떠한 자료를 어떻게 수집할 것인가를 결정하는 역할을 한다. 이렇게 수집된 자료는 분석 응용이 분석하게 된다. RTFM 외에 환경에 적절한 툴들을 개발할 필요가 있으면 이에 대한 연구 및 개발이 요구된다. 프로토콜 모니터링과 네트워크 모니터링 만으로는 사용자가 요구한 QoS를 만족하고 있는지를 확인하기가 어렵다. 즉, 가장 복잡하면서 또한 가장 중요한 종단간의 QoS 모니터링을 통해서 이 문제를 풀어야 한다. 또한 종단간의 모니터링은 이질적인 QoS 관리 구조를 가지는 네트워크 도메인 간의 QoS 보장의 제공 여부를 점검하는데 중요한 기능을 한다. 먼저 종단간 QoS 모니터링을 위해 원하는 트래픽 생성을 원하는 시점에 원하는 양 만큼을 할 수 있는 툴과 그 결과를 모니터링하기 위한 툴이 필요하다. 다양한 종류의 트래픽으로 정확한 모니터링이 상당히 어렵는데 아주 치밀하게 사전 설계 및 구조의 정의가 요구된다.

지금까지는 QoS 보장 모니터링 기술 자체에 대해서만 언급했으나 이 기술의 사용자 입장에서 고려해 보면 네트워크 관리자만이 아니라 차등 QoS 서비스를 사용하는 고객들도 주요 사용자이다. 초기에는 이 기술이 QoS 보장 모니터링 자체에만 치중을 하겠지만, 장기적으로는 QoS 상태에 대한 다양한 형태의 분석 자료를 원하는 고객들에게 실시간으로 전달할 수 있는 형태로 발전함으로써 진정한 고객 지향의 차등 QoS 서비스의 초석이 될 수 있는 중요한 기술이다.

III. QoS 관리기술 연구 및 표준화 동향

인터넷에서 실시간 서비스를 지원하는 새로운 서비스가 도입됨에 따라 서비스 QoS를 제공하는 방안

이 요구되고 있으며, IETF에서는 이에 대한 기술들을 표준화하고 있고, 벤더들은 QoS를 지원하는 제품을 개발하고 있다. 이에 발맞추어 대두되는 인터넷 기술을 시장에서 빠르게 수용하고 표준화 기구, 벤더 및 IT와의 협력을 촉진하기 위해 정보 및 이벤트 제공을 목적으로 1994년에 미국의 Stardust Forum Inc.이 창설되었으며, 인터넷에서 QoS, IP Multicast, 차등서비스, RSVP, Policy, COPS와 같은 새로운 IP 대역폭 관리 기술을 토론할 수 있는 iBAND 라는 컨퍼런스를 주최하고, QoS 기술을 시장으로 확산하기 위해 QoS Forum을 설립하였다.

또한 Internet2는 차등서비스 기술을 시험할 수 있는 테스트베드인 Qbone^[18]을 구축하고, 종단간 QoS를 보장하기 위해 자원을 관리하고 제어하는 기능을 수행하는 대역폭브로커에 대한 연구를 수행하고 있다.

그리고 유럽에서는 새로운 기술 또는 서비스를 상용화하기 이전에 유럽 16개국의 연구망을 155 Mbps로 연결하는 범 유럽 초고속망인 TEN-155 망에서 이를 시험하고 확인하는 것을 목적으로 설립된 TF-TANT 프로젝트를 통해 차등서비스, RSVP를 ATM SVC로의 매핑, QoS 모니터링 및 policy server등에 대한 연구를 수행하고 있다. 본

절에서는 IETF의 표준화 동향, Qbone의 대역폭브로커 및 TF-TANT의 QoS 관리 연구동향에 대해 살펴본다.

1. IETF의 표준화 동향

IETF에서는 QoS 관리를 위해 QoS Management/Traffic Engineering 그룹, 정책 그룹, QoS 라우팅 그룹 등 세 가지 그룹으로 나누어서 표준화 작업을 진행하고 있다. QoS Management/Traffic Engineering 그룹은 다시 차등서비스, 통합서비스, RSVP, MPLS, Traffic Engineering, IP over Optical 워킹 그룹으로 세분화 하여 작업이 진행 중이며, 정책 그룹은 Policy, RAP, Authentication, Authorization, Accounting(AAA), IP Security Policy(IPSP) 워킹 그룹으로 나누어지며, QoS 라우팅 그룹은 기존의 IP 라우팅 프로토콜에 QoS 정보를 포함한 QoS 기반 라우팅을 위한 표준 작업을 하고 있으나 기술적으로 난관에 봉착한 상태여서 라우팅 프로토콜 자체를 수정하여 QoS를 해결하려는 시도보다는 위에서 언급된 다양한 타 방식을 상황에 따라 혼용하여 처리하는 쪽으로 기울고 있다.

QoS 그룹 활동은 비교적 장기적으로 작업을 진

표 2. Qbone의 단계별 대역폭브로커 개발 추진 전략

단 계	시 기	특 징	비 고
0단계 : Local Admission	99.4	로컬 도메인에서 호가 수락되면 목적지까지 자원의 가용여부와 무관하게 호 수락	- SLA 수동으로 설정 - 대역폭브로커간 통신 없음
1단계 : Informed Admission	미정	업스트림 대역폭브로커로부터의 정보에 따라 호 수락 단, 자원의 재협상 없음.	- SLA 수동으로 설정 - 대역폭브로커 간은 가용자원 정보만 제공
2단계 : Guaranteed Admission	미정	초과로 예약하는 자원의 양을 제한하고 버스트한 데이터 처리 방안	- 2단계와 동일
3단계 : Dynamic SLA Admission	미정	SLA를 동적으로 협상	- SLA 동적으로 설정

행하여 상당한 부분에서 표준작업이 마무리 단계에 있으며 많은 산업체들이 이들 표준을 따르는 제품들을 개발하여 상용화 했거나 개발 중에 있다. 정책 그룹은 현재 많은 부분이 진행 중인 상태여서 정책기반 QoS관리를 위한 프레임워크 및 핵심 정보 모델 문서는 거의 마지막 수정과정을 거치고 있는 상태이다. 이 중 일부 워킹 그룹에서는 Common Open Policy Service(COPS)와 같은 정책관리를 위한 표준을 완성 하였다. 최근에는 MPLS와 Optical 기술을 이용한 Traffic Engineering 측면의 QoS 관리 솔루션을 찾기위한 노력이 시작되고 있는 상태이다.

2. Internet2:Qbone의 대역폭브로커 연구동향⁽¹⁹⁾

Qbone에서는 대역폭브로커의 기능을 4 단계로

나누어 개발하고 있다. <표 2>는 대역폭브로커 개발의 단계별 추진 전략을 나타낸다. Qbone에서 대역폭브로커의 개발은 Merit, British Columbia Institute of Technology(BCIT), UCLA가 주도하고 있으며, 그 외 참가 기관으로는 Telia, Globus를 들 수 있다. 다음은 각 기관의 대역폭브로커의 개발 동향이다.

가. Merit의 대역폭브로커 개발 동향

Merit는 인터-도메인(BB간)과 인트라-도메인(BB-라우터사이)에서 자원 할당을 요구하기 위한 신호 프로토콜 및 협상 엔진으로 DIAMETER 사용 방안을 제안하고 이를 개발하고 있다. 여기서 대역폭브로커는 미리 정의된 토폴로지 정보를 이용하여 대역폭을 할당하고, OSPF를 사용하여 도메인 내의 라우팅 정보를 얻는다.

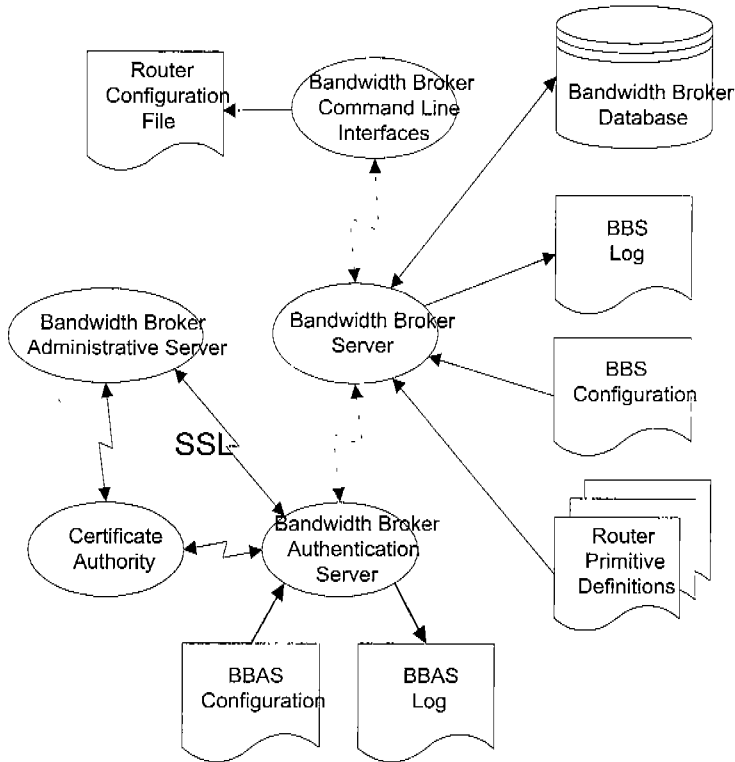


그림 4. BCIT의 대역폭브로커 시스템 구조

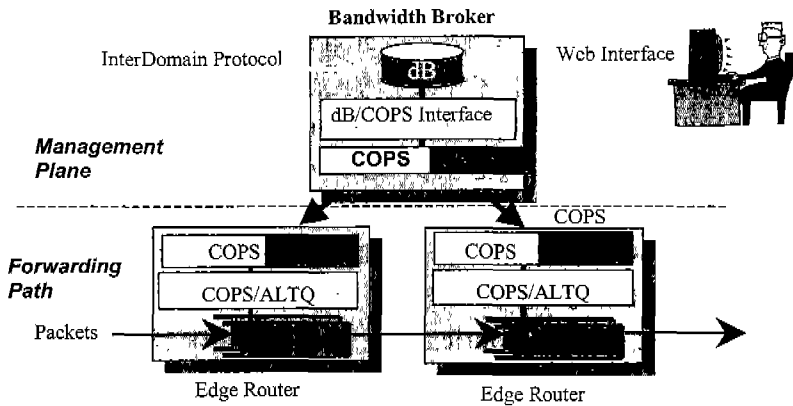


그림 5. UCLA의 대역폭브로커 및 에지 디바이스의 개요

나. BCIT의 대역폭브로커 개발 동향
 BCIT는 망 운용자와 대역폭브로커 서버 사이의 기능을 주로 구현하고 있으며, 대역폭브로커와 라우터간의 프로토콜인 BB Transport Protocol (BBTP)을 제안하고 있다. BCIT에서 개발된 대역폭브로커는 CA*Net II에 배치될 예정이다. (그림 4)은 BCIT의 대역폭브로커 시스템 구조를 나타낸다.

다. UCLA의 대역폭브로커 연구 동향
 UCLA에서 제안한 대역폭브로커는 대역폭브로커와 에지 라우터간에 COPS 프로토콜을 사용하고 대역폭브로커 간의 통신은 정적으로 구성한다. (그

림 5)는 UCLA의 대역폭브로커 대역폭브로커 및 에지 디바이스의 개요를 나타낸다.

라. 기타

Telia는 Olov Schelen(스웨덴)의 논문에서 제안한 QoS service agent라는 대역폭브로커와 유사 기능을 수행하는 에이전트에 대해 연구하고 있으며, 이 에이전트는 OSPF를 이용하여 도메인내의 토폴로지 정보를 얻고 라우터와 SNMP를 통해 통신하며, 사전에 미리 자원을 예약하는 것을 주요 내용으로 하고 있다.

Globus는 멀티미디어 서비스를 제공하기 위해

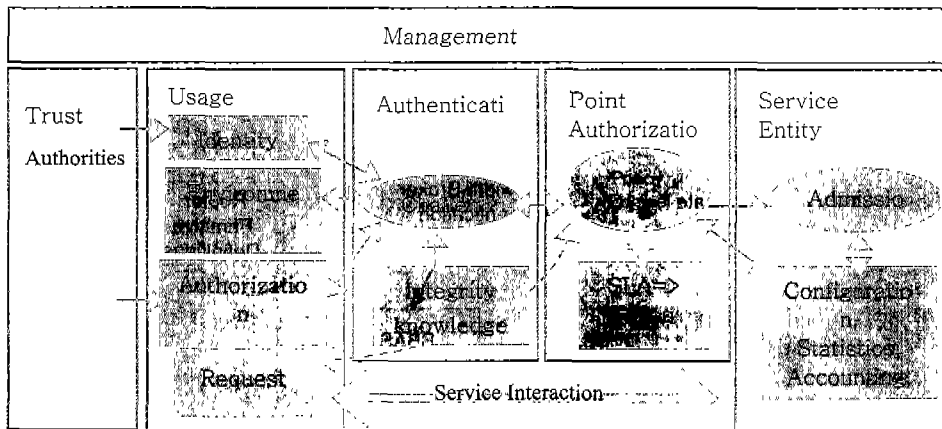


그림 6. TF-TANT프로젝트에서 개발하는 policy server의 구조

분산되어 있는 메모리 및 CPU 등의 자원을 관리하고 제어하는 스케줄러에 대해 연구하는 프로젝트이며, Qbone은 이 개념을 대역폭브로커에 활용하려고 하고 있다.

3. 유럽: TF-TANT에서의 policy server에 대한 연구 및 개발 동향

TF-TANT 프로젝트는 새로운 기술 또는 서비스를 제공하기 전에 이를 시험하고 확인하는 것을 목적으로 설립된 것으로써, 여기서는 차등서비스, RSVP를 ATM SVC로의 매핑, QoS 모니터링 및 대역폭브로커와 유사한 기능을 수행하는 policy server 등에 대한 연구를 수행하고 있다. (그림 6)는 TF-TANT 프로젝트에서 개발하는 policy server의 구조를 보이고 있다. 여기서 Request, Policy engine, SLA rule, configuration이 대역폭브로커의 역할을 수행할 수 있다.

IV. QoS 관리 제품 동향

앞 장에서는 QoS 관리 기술의 연구 및 표준화 동향에 대해서 살펴보았다. 이 분야의 중요성은 정부, 학계, 표준단체 뿐만 아니라 새로운 기술을 주도하기를 희망하는 일부 산업체들로 하여금 상용 제품 개발 및 발표를 서두르게 하고 있다. 본 장에서는 이러한 QoS 관리 기술 분야를 선도해 가는 대표되는 기업들의 제품을 간략히 소개한다.

현재 개발된 제품은 크게 두 종류로 구분할 수 있다. 하나는 라우터 스위치와 같은 네트워크 장비 업체들이 기존 및 새롭게 개발되는 모델에 QoS 관리 기능을 첨가하는 형태이며, 두 번째는 이들 네트워크 장비를 제어하고 관리하기 위해 정책을 기반으로 한 정책 서버 형태의 제품이다. 특히 정책 서버는 장비 업체가 직접 자체 장비의 관리를 위해 개발한 정

책 서버 형태와 제 3자가 여러 가지 네트워크 장비와 호환성을 가지고 사용할 수 있게 개발한 정책 서버 형태로 다시 세분할 수 있다. 현재 전자에 속하는 제품의 출하를 발표한 업체는 11개사 정도가 있으며, 후자의 경우는 3개 정도로 알려져 있다. 이 외에 하드웨어 기반의 트랙픽 셰이핑이나 튜닝을 담당하는 제품을 개발한 업체들도 있다.

〈표 3〉은 전자의 11개의 정책 서버 제품에 관한 사양을 사용자 인터페이스, 정책 서버 유형, 정책 전달 메커니즘, 정책 지원 장비, 우선순위, 보안 정책 등을 기준으로 비교 분석한 표이다.

〈표 3〉에서 보듯이 11개의 업체들 모두 네트워크 장비를 직접 개발 판매하는 업체들로서 QoS 관리 기능을 첨가하는 것은 차후 인터넷 QoS 시장에서 우위를 확보하기 위한 중요한 투자임을 확인할 수 있다.

아직은 제품들이 초보 단계이며 상호운용성, 확장성 등 많은 문제점들을 안고 있으나 시장의 요구가 증가하고 성숙되어 감에 따라 제품의 수준도 증가해 갈 것임은 의심할 여지가 없다.

그리고 이들 네트워크 장비 업체와는 별도로 독립형 정책 서버 솔루션을 발표하고 있는 벤처 업체들이 있다. 대표적인 업체로 IP Highway⁽²⁰⁾, Orchestream⁽²¹⁾, Ukia⁽²²⁾를 들 수 있다. 이들 제품의 특징은 이중의 스위치와 라우터로 구축된 네트워크에서 정책을 수행하는 데 사용될 수 있는데, 최근 발표된 Orchestream Enterprise 1.0은 소프트웨어 대행자(프록시)를 이용해 시스코와, 익스트림, 노텔 및 제디아의 캠퍼스 장비로 정책을 다운로드 시킬 수 있으며, 사용 프로토콜은 LDAP, COPS, IOS CLI 에 상관 없이 모두 수용할 수 있게 설계되어 있다. IP Highway와 Ukia 제품도 비슷한 지원을 약속하고 있다. 이미 대형 네트워크 장비 업체들이 각자의 정책 서버 솔루션을 제공하고 있음에도 불구하고 이들이 이 분야에 뛰어 들고 있는 이유는 QoS 정책 관리에서 가장 중요한 부분이

표 3. 정책 서버 제품 사양 비교표 (출처: Data Communications Magazine, 1999)

업체명	제품명/ 출하시기	사용자 인터페이스	정책서버 유형	정책 전달 메커니즘	정책 지원 장비	우선 순위	보안 정책
Cabletron	Smart Networking Services/ 1999. 5	그래픽	독립형	SNMP, IOS CLI via Telnet	워크그룹, 부서용 및 백본 스위치	802.1p, QoS	접근 제어 목록
Cisco	Cisco Sure Policy Networking/ 1999. 4	그래픽	독립형	COPS	라우터 8500, 백본스위치의 웹 인터페이스	TOS, DS	없음
EXtreme Networks	Extreme Enterprise Policy Manager/ 1999. 8	그래픽	탑재형	COPS: IOS CLI with Telnet	모든 스위치	802.1p	없음
Fore	Application aware Networking	그래픽	탑재형	LDAP	캠퍼스 백본, 스위 치 및 모듈러 부서 용 스위치	802.1p	방화벽
HP/Intel	Policy Expert/ 1999. 6	그래픽	독립형	COPS: IOS CLI with Telnet	이더넷 어댑터, 라우터, 부서용 스위치	802.1p, TOS	방화벽
IBM	Application Virtual Networking/ 1999. 6	텍스트	탑재형	LDAP	서버 및 라우터	DS	패킷 필터링, Ipssec
Lucent	Multinet/ 1999. 8	그래픽	독립형	LDAP, SNMP, IOS CLI with Telnet	라우터, 캠퍼스 백본 스위치	802.1p, TOS	비밀번호
Newbridge Networks	Newbridge Management Executive/1994	그래픽	독립형	MPOA 및 전용	ATM 백본 스위치, ATM/ LAN 혼용 부서용 스위치	DS (WAN only)	없음
Northern Telecom	Optivity Policy 1.0/ 1999. 7	그래픽	독립형	호텔용 COPS, IOS CLI with Telnet	라우터	802.1p, TOS	비밀번호, 암호화
3Com	Policy-powered Networks/ 1999. 4	그래픽	탑재형	LDAP	XL 라인 이더넷 어댑터, 코어빌더 및 페스빌더 캠퍼 스 백본 스위치	802.1p, DS	비밀번호, 암호화
Xylan	Switched Network Services/ 1999. 5	그래픽	탑재형	LDAP	모든 스위치	없음	비밀번호

서버의 성능, 상호 운용성, 확장성 등 때문이다. 이들은 오랜 경험 및 소규모의 효율적인 조직을 기반으로 보다 확장성 있고 성능이 우수한 정책 기반 QoS 관리 서버를 개발함으로써 이 분야에서 우위를 점한다는 전략을 세워 두고 있는 것이다.

이들 제품의 성공 여부를 평가하기에는 아직은 너무 이른 시기이다. 그러나 중요한 것은 의외로 많은 사용자들이 QoS 관리를 통한 생산 및 정보 인프라의 효율을 증대하기 위한 관심을 가지고 있다는 사실이다. 예로, 최근 Data Communications Magazine에서 행한 QoS 관련 설문 조사 중 QoS가 필요하다고 응답한 78%의 절반 이상이 이미 Orchestream Enterprise 1.0과 같은 정책 기반 QoS 관리 틀을 시험하고 있다는 것으로 판명되었다. 아직 국내의 ISP나 기업들의 요구사항에 대한 설문이 발표되지는 않았으나, 사용자 내부의 효율성 증대 및 국제 경쟁력을 생각한다면 심각히 고려해 보아야 될 문제가 아닌가 생각된다.

되고 있는 분야가 되고있다.

안타깝게도 국내에서는 아직 가시적인 연구 개발의 열기가 나타나고 있지 않고 있다. 차세대 인터넷이 가까운 장래의 세계 정치 및 경제를 이끌어 갈 핵심 정보 허부 구조가 될 것이라는 것을 잘 알고 있는 우리로서는 보다 적극적인 자세로 산, 학, 연이 공히 서로 유기적으로 관련 기술의 연구 및 개발에 많은 관심을 쏟아야 할 때이다. QoS 보장은 인터넷 상에서 가능할 것으로 예상되어 진다. 그러나 결코 단순히 저절로 얻어지는 것은 아니다. 비록 완벽한 QoS를 보장하는 기술이 바로 가까운 장래에는 실현되지 않을지 모르나 현재의 최선형 인터넷 서비스보다 훨씬 예측가능하고, 비교적 일관성 있는 차별 서비스를 QoS 관리 기술은 가능하게 할 것이며, 아직 초보 연구 개발 단계에 있는 시점에서 국내의 기술력을 확보하는 것은 국제 경쟁력을 비롯한 모든 부분에서 매우 중요한 포석이 될 것이다.

※ 참고문헌

V. 결론

본 고에서는 향후 인터넷 상에서 차별 서비스를 상업화 하기 위해서 반드시 해결해야 되는 문제인 QoS 관리 기술의 정의, 핵심 요소 기술의 연구 및 표준화 동향, 그리고 제품 동향에 대해 살펴보았다. 이 분야의 기술은 아직 연구 단계에 있으며 그 성공 가능성에 대해서 누구도 자신 있게 대답할 수 없는 입장이다. 왜냐하면 단순히 기술적으로만 해결될 문제가 아니라 경제적, 정치적, 문화적, 사회적으로 모두 매우 신중히 검토되어야 될 복잡한 문제이기 때문이다. 그러나 중요한 것은 불확실한 미래에도 불구하고 전세계 정보 선진국에서는 모두 나름대로의 QoS 관리 기술을 활발히 연구 개발 시험 중에 있다는 사실이다. 심지어 상용 제품이 이미 출시되고 있으며 차세대 인터넷 분야에서 가장 관심의 초점이

- [1] Stardust Forum, Internet Bandwidth Management 2(iBAND2) Conference., San Francisco, May 1999.
- [2] R. Braden, D. Clark, S. Shenker, Integrated Services in the Internet Architecture: An Overview, RFC1633, June 1994.
- [3] Y. Bernet, J. Binder, S. Blake, M. Carson, et. Al., A Framework for Differentiated Services, Internet Draft, October 1998.
- [4] Paul Ferguson, and Geoff Huston, Quality of Service: Delivering QoS on the Internet and in Corporate Networks, John Wiley & Sons, Inc.

- 1998.
- [5] Floyd, S., and Jacobson, V., Link-sharing and Resource Management Models for Packet Networks, IEEE/ACM Transactions on Networking, Vol. 3 No. 4, pp. 365-386, August 1995.
- [6] Demers, Keshav, and Shenker, Analysis and Simulation of a Fair Queuing Algorithm, Internetwork: Research and Experience, Volume 1, Number 1, John Wiley & Sons, September 1990, pages 3-26.
- [7] S. Floyd, and V. Jacobson, Random Early Detection Gateways for Congestion Avoidance, IEEE/ACM Transactions on Networking, V.1, N.4, August 1993.
- [8] D. Kandlur, D. Saha, and K. Shin, Understanding TCP Dynamics in an Integrated Services Internet, NOSSDAV 97, May 1997.
- [9] DMTF, Distributed Management Task Force,.
- [10] J. Boyle, R. Cohen, D. Duram, S. Herzog, R. Rajan, and A. Sastry, The COPS (Common Open Policy Service) Protocol, Internet Draft, December 1998.
- [11] Wahl, M., Howes, T. and S. Kille, "Lightweight Directory Access Protocol (Version 3)", RFC 2251, December 1997.
- [12] Rigney C., Rubens A., Simpson W., and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2138, April 1997.
- [13] Calhoun, and Ruebens, "DIAMETER User Base Protocol", Internet draft, November 1998.
- [14] UCLA Internet Research Lab., RSVP Diagnostics Tool.
- [15] Realtime Traffic Flow Measurement (rtfm) Working group, /qbone/



최태상

1988년 계명대학교 건축공학과(학사)
1991년 미주리-캔사스 주립대학교 컴퓨터통신(석사)
1995년 미주리-캔사스 주립대학교 컴퓨터통신(박사)
1996년~현재 한국전자통신연구원, 선임연구원
관심분야: 인터넷 품질관리/트래픽엔지니어링, 서비스
및 망 관리



정태수

1981년 경북대학교 전자공학과(학사)
1983년 경북대학교 전자공학과(석사)
1983년~현재 한국전자통신연구원, 책임연구원, 팀장
1991년~1992년 미국 UMass 대학 방문연구원
관심분야: 통신망구조, 인터넷 시스템, LAN 시스템,
망관리



이유경

1978년 한국항공대학교 항공전자공학과(학사)
1980년 연세대학교 전자공학과(석사)
1980년~1984년공군제2사관학교 전자공학과 교관
1984년~현재 한국전자통신연구원, 책임연구원, 부장
1995년~1996년 일본 NTT연구소 방문연구원
관심분야: 광통신시스템, ATM 네트워크, ATM LAN