

IPv6 홉-바이-홉 옵션 헤더 이용으로 멀티서비스의 QoS 개선을 위한 플로우 제어 방안

정회원 이인화, 김성조

A Flow Control Scheme for the QoS Improvement of Multi-Service using IPv6 Hop-by-Hop Option Header

In-Hwa Lee and Sung-Jo Kim

요 약

IPv6 환경에서는 인터넷 전화, 주문형 비디오 및 다자간의 대용량 파일 교환 서비스 등이 더욱 증가될 것이므로 단-대-단(End-to-End)기반의 엄격한 품질 보장 및 상대적으로 사용을 억제할 수 있는 차등화된 품질 제어 방안이 동시에 요구된다. 본 논문은 IPv6망에서 트래픽을 플로우 단위로 식별하고 IPv6 홉-바이-홉 옵션 헤더 내의 QoS 정보를 이용하여 멀티서비스의 QoS 개선을 위한 플로우 기반의 제어 방안을 제시한다. 플로우 제어 대상은 플로우 레이블 값을 이용하는 Non-default QoS 트래픽 뿐만 아니라 최선형 및 암호화 트래픽으로 확대 적용한다. 이를 통해 실시간 서비스에 대한 보장성은 강화하고 불필요하게 망 자원을 낭용하는 플로우는 효과적으로 제어한다. 또한, 기존 망 자원의 최소 변경과 통신사업자의 백본망 현황을 반영하여 플로우와 MPLS간 매핑 방안을 제시한다. 시뮬레이션 결과에서는 제안하는 플로우 품질 제어 방안이 실시간 서비스에 대한 QoS 제공 및 백본 자원의 활용 측면에서 효율적임을 확인한다.

국문키워드 : IPv6 홉-바이-홉 옵션 헤더, 플로우 제어, 플로우 레이블, P2P 제어, 품질

ABSTRACT

In IPv6 environment, the Internet Telephony, VoD(Video on Demand) and high capacity file exchange service will be more increased than IPv4. Therefore, the strict guarantee of QoS based on End-to-End and differentiated quality control schemes are simultaneously required. This paper proposes the flow control schemes on IPv6 network that the traffic is identified by flow and the QoS of multi-service is improved by QoS information in IPv6 hop-by-hop option header. The object of flow control includes not only non-default QoS traffic, which uses the flow label, but also best-effort or encrypted traffic. Therefore, the guarantee of real-time service is strengthened and the flow, which abuses unnecessarily the network resources, is effectively controlled. Also, this paper proposes the mapping scheme between the flow and MPLS by reflecting the minimum change of the existed network resource and the status of backbone network of ISP(Internet Service Provider). In the simulation result, It is shown that the proposed scheme is effective in the side of QoS on real-time services and utilization of backbone resources.

Keyword : IPv6 Hop-by-Hop Option Header, Flow Control, Flow Label, P2P Control, QoS(Quality of Service)

* (주) CST 상무이사/CTO(inhlee@cst.co.kr), 중앙대학교 공과대학 컴퓨터공학부 교수(sjkim@cau.ac.kr)
논문번호 : 030583-1226, 접수일자 : 2003년 12월 26일

1. 서 론

정보통신 기술의 발전으로 인터넷 환경이 광역화, 고속화되면서 이제까지는 불가능했던 다양한 멀티서비스들을 제공할 수 있게 되었다. 최근에는 P2P (Peer-to-Peer) 응용서비스(KaZaA, Napster, Morpheus, eDonkey 등)가 인터넷 트래픽의 약 50%를 차지할 정도로 성장하였다[1]. 이는 기존의 웹으로 대표되는 클라이언트/서버 기반의 수직적 정보획득체제가 P2P 기반의 수평적 정보공유체제로 변화하고 있음을 의미한다. 정보제공 주체가 중앙 서버에서 개인 단말로 이전되면서 서버의 정보 수집 및 관리의 부담은 감소되었으나 정보유통에 관한 제어는 상대적으로 어렵게 되었다. 이에 통신사업자들은 증가하는 P2P 트래픽을 수용하기 위한 망 증설 부담이 가중됨에 따라 포트번호 기반의 트래픽 제어로 부분적인 해결책을 강구하고 있다. 하지만, P2P 응용서비스가 가변 포트번호를 사용하는 등 점차 지능화되고 있어 기존 포트번호 기반의 트래픽 제어 방법으로는 한계가 있다.

차세대 인터넷 프로토콜인 IPv6는 풍부한 주소공간, 개선된 보안 및 이동성 등의 장점으로 단-대-단 (End-to-End) 통신의 투명성을 제공한다[2]. 따라서, IPv6 환경에서는 P2P와 같은 단-대-단 서비스가 더욱 활성화될 것으로 예상되며, 기존의 메시징 및 파일 교환용 P2P 외에 VoIP, VoD, 단-대-단 IPSec VPN 등 품질 보장을 기반으로 한 다양한 응용서비스(멀티서비스) 및 비즈니스 모델이 확대될 것으로 예상된다. 이에 따라 IPv6 환경에서는 다양한 응용서비스에 대해 보장 또는 억제기법을 차등적으로 적용할 수 있는 제어 방안이 요구되며, 이러한 트래픽 제어를 위해서는 적정 단위로 트래픽을 분류해야 한다. 이때 패킷 단위의 트래픽 제어는 제어 대상수가 방대하고 상태 기반의 처리가 불가능하므로 패킷의 연속된 집합인 플로우 단위의 트래픽 제어가 필요하다.

본 논문에서는 IPv6망에서 트래픽을 플로우 단위로 처리하기 위해 플로우 제어 대상을 기존 Non-Default QoS(또는 실시간 서비스) 트래픽 외에 최선형(Best Effort) 및 암호화 트래픽까지 확대 적용하였다. 또한, 실시간 플로우에 대한 품질 보장성을 강화하기 위해 IPv6의 홉-바이-홉 옵션 헤더 내의 QoS 정보를 활용하고, 남용 플로우는 플로우별 상태 관리를 통해 자원이용을 효과적으로 제어하였다.

그리고, 백본망의 코어라우터에서 플로우 처리 오버헤드를 감소시키기 위해 플로우와 MPLS QoS간 연계 모델을 제시하였다.

본 논문의 구성은 다음과 같다. 2장에서는 플로우 개념과 IPv6 기반 QoS 홉-바이-홉 옵션 헤더에 대해 살펴보고 3장에서는 본 논문에서 제안한 IPv6 QoS 홉-바이-홉 옵션 헤더를 이용한 플로우 기반 트래픽 제어 방안 및 효율적인 자원 활용방안을 기술하였다. 4장에서는 시뮬레이션 환경을 설명하고 시뮬레이션 결과를 통해 제안된 방식의 효율성을 확인하였다. 마지막으로 5장에서는 결론과 향후 연구 방향에 대하여 논의한다.

2. 관련 연구

IPv6는 실시간 응용서비스의 QoS 지원을 위해 IPv6 기본 헤더 내에 20비트의 플로우 레이블 필드를 정의하고 있으며[1], 이를 플로우 식별자로서 사용하는 방안에 대한 연구가 활발히 진행되고 있다. Schmid의 연구에서는 IPv4에서 발생되던 계층 위반 (Layer Violation) 문제를 해결하기 위해 IPv6 플로우 레이블의 활용방안을 제시하였다[3]. Rajahalme의 연구에서는 플로우 레이블의 부여와 플로우 상태 및 처리를 위한 요구사항을 정의하였다[4]. QoS를 요구하는 트래픽은 임의의 플로우 레이블 값을 할당하고 플로우 레이블 값이 0인 경우는 QoS를 요구하지 않는 일반 트래픽으로 처리된다. 송신지에서 플로우 레이블을 할당할 때 동일 송신지 및 수신지 주소를 갖는 플로우들에 대해 동일한 플로우 레이블이 부여되지 않도록 해야 하므로 송신지 노드는 현재 사용되고 있거나 최근에 사용된 플로우 레이블을 유지하고 있어야 한다. Banerjee의 연구에서는 하이브리드 방식을 이용하기 위한 IPv6의 플로우 레이블 포맷을 제시하였다[5]. 이 연구에서는 플로우 레이블 포맷을 랜덤 넘버, 홉-바이-홉 옵션 헤더, PHB ID, 포트번호/프로토콜, 하이브리드 타입 등 5가지로 분류하여 정의하였다.

Roberts 연구에서는 홉-바이-홉 옵션 헤더의 구체적인 포맷을 정의하여 IPv6망에서 플로우 단위의 QoS 시그널링을 제공하도록 제안하였다[6]. 현행 IPv6 표준에서는 CoS(Class of Service) 제공을 위해 TC(Traffic Class) 필드를 사용하도록 정의하고 있다[2]. 하지만, CoS는 패킷의 집합을 정해진 기준에 따라 분류된 클래스 단위로 QoS를 제공하므로 QoS를 보장하기에는 한계가 있다. 이에 Roberts 연

구에서는 QoS 정보에 대한 명세가 필요하거나 TCP 전송률에 대한 응답이 필요한 경우 IPv6 패킷 헤더에 8바이트의 홉-바이-홉 옵션필드를 추가적으로 정의하였다.

그림 1은 Roberts의 연구에서 정의한 QoS 홉-바이-홉 옵션필드와 QoS 홉-바이-홉 응답 옵션필드 포맷을 보여주고 있다. 여기서 CHG 필드는 AR(Available Rate) 또는 GR(Guaranteed Rate)이 변경될 경우 사용되며, 변경된 전송률은 응답 패킷에 표기되어야 한다. DIR 필드는 패킷의 방향성을 나타내며 순방향(Forward)인 경우 0, 역방향(Reverse)인 경우 1로 표기한다. TYP 필드는 플로우의 유형을 다음과 같이 4가지로 구분한다. 즉 유형 0은 AR(Available Rate)로 TCP형 서비스, 유형 1은 CR(Composite Rate)로 ATM VBR형 서비스, 유형 2는 MR(Maximum Rate)로 트래픽 손실이 없는 UDP형 서비스, 유형 3은 GR(Guaranteed Rate)로 GR 필드에 정의된 대역을 보장하도록 정의하고 있다.

Available Rate(AR) 필드는 망에서 수용 가능한 부동소수점 전송률을, Guaranteed Rate(GR) 필드는 송신지에서 요청한 부동소수점 보장 전송률을 나타낸다. AR과 GR의 부동소수점은 처음 5비트의 지수(Exponent) 부분과 다음 7비트의 가수(Mantissa) 부분으로 표기된다. AR 전송률은 $(1+M/32)*2^E$ kbps로 최대 4.278 Tbps의 전송률을 가진다. MLPP 필드는 다단계 선점 우선순위(Multi Level Preemption Priority)를 나타내는데 플로우의 우선순위를 8개의 레벨(0(최하위)~15(최상위))로 지정하고, 모든 플로우들이 이용할 수 있는 충분한 대역폭이 없는 경우 가장 낮은 MLPP 값을 가진 플로우들이 삭제된다. BT 필드는 Burst Tolerance로 플로우 전송률을 초과하여 패킷이 폐기되기 전에 허용되는 시간을 나타내며, $2^{-(BT-1)}$ 초(15 밀리초에서 500 밀리초)로

표기된다. PRI 필드는 16개 레벨(0(최하위)~15(최상위))의 지연 우선순위로 상위 레벨의 플로우는 전송시 우선적으로 처리된다. RFID 필드는 응답 플로우의 ID로 순방향 플로우의 플로우 ID를 나타낸다.

앞서 살펴본 바와 같이 QoS 홉-바이-홉 옵션 헤더는 IPv6망에서 플로우 단위의 QoS 시그널링을 제공하기 위한 용도로 제안되었다. 하지만, 정의된 이들 필드에 대해 망에서의 구체적인 수용방안이 제시되고 있지 못하며, 더욱이 AR 및 BT 필드 등의 정보를 실제적으로 활용하기 위해서는 현행 인터넷 모델의 대폭적인 변경이 필요하다. 따라서, 본 논문에서는 ITU-T의 Y.1541[7]에서 제시하는 IP QoS 클래스별 품질 수준을 제공하기 위해 QoS 홉-바이-홉 옵션 헤더의 일부 필드만을 제한적으로 활용한다. 이를 통해 기존 인터넷 모델의 변경을 최소화하면서 플로우별로 차등적인 QoS를 제공할 수 있다.

3. IPv6 홉-바이-홉 옵션 헤더를 이용한 플로우 품질 제어 방안

본 논문은 IPv6망에서 트래픽을 플로우 단위로 구분하고 IPv6의 QoS 홉-바이-홉 옵션 헤더 내의 플로우 특성 정보를 활용하여 실시간 서비스에 대한 보장성은 강화하고 남용 플로우의 자원이용을 효과적으로 제어할 수 있는 방안을 제시한다. 현행 통신사업자들은 서비스에 대한 투명성(Transparency)(즉, 단-대-단 응용서비스를 품질 저하없이 제공)[8]을 보장하기 위해 트래픽을 사전에 예측하여 망 용량을 설계하고 있다. 하지만, 장애, 부정확한 트래픽 예측, 일시적인 트래픽 폭주 등으로 요구된 트래픽이 설계된 용량을 초과할 수 있다. 또한, 최근 급격히 증가하고 있는 P2P 트래픽 예측의 어려움으로 인하여 서비스에 대한 투명성 제공을 더욱

• QoS 홉-바이-홉 옵션필드

Next Header	Hdr. Ext. Length=0	CHG	DIR	TYP	Available Rate (AR)	
Guaranteed Rate (GR)	MLPP	BT	PRI	Blank		

• QoS 홉-바이-홉 응답 옵션필드

Next Header	Hdr. Ext. Length=0	CHG	DIR	TYP	Available Rate (AR)	
Guaranteed Rate (GR)	Response Flow Identifier (RFID)					

그림 1. QoS 홉-바이-홉 옵션필드와 응답 옵션필드

어려워지고 있다. 이것은 결국 서비스에 대한 망 자원의 접근성(Accessibility)[8]을 보장하지 못한다는 것을 의미한다. 따라서, 서비스의 품질 특성에 따라 차등적인 접근성을 제공하는 방안이 중요시되고 있다.

인터넷 환경에서의 접근성 보장은 자원 예약(IntServ) 또는 서비스 클래스별 차등화(DiffServ)에 의해 제공된다. IntServ는 자원 예약 프로토콜인 RSVP(Resource Reservation Protocol) 시그널링을 이용하여 연결 수락 제어와 자원 예약을 수행하여 플로우의 QoS를 보장한다[9]. 하지만, 시그널링으로 인한 전송 지연 및 처리 오버헤드로 망 규모가 커질 경우 확장성 문제가 심각하다. DiffServ는 확장성의 문제점을 지닌 IntServ의 한계를 극복하고 인터넷 백본망에서 QoS를 제공하기 위해 플로우 단위로 QoS를 보장하지 않고 패킷을 정해진 기준에 따라 분류하고 서비스를 클래스별로 차등화하여 제공한다[10]. 하지만, 혼잡시에 동일 클래스내의 모든 트래픽에 대해 임의의 패킷 손실이 발생하게 되어 모든 트래픽의 품질이 저하되고 결국 망 자원이 비효율적으로 운용되는 문제점을 유발한다.

따라서, 본 논문에서는 플로우 기반으로 트래픽 특성을 분류하여 플로우별 차등화된 접근성 제공 방안을 제시한다. 이를 위해 플로우의 서비스 유형

을 하드(Hard) QoS, 소프트(Soft) QoS, 최선형(Best Effort), 남용(Abusive) 클래스로 분류하여 하드 또는 소프트 QoS를 요구하는 플로우에 대해서는 혼잡 시 CAC(Connection Admission Control)를 적용하여 기존에 형성된 플로우는 계속 보장하면서 신규 플로우에 대해서만 블러킹(Blocking)을 시행한다. 단, 하드 QoS를 요청하는 플로우에 대해서는 혼잡 시 MLPP를 적용하여 서비스 중인 낮은 우선순위의 플로우를 거절하는 대신 더 높은 우선순위의 신규 플로우를 수용하여 우선순위로 차등화된 접근성을 제공한다. 또한 자원의 효율적인 이용을 위해 남용 플로우를 플로우 상태 관리를 통해 식별하고 남용 클래스로 정의하여 이를 사전에 정의된 정책에 따라 처리한다.

3.1 시스템 모델

기존 인터넷 모델에서 플로우 단위의 품질 제어를 구현하기 위해서는 전체 IP 망자원의 증설 또는 교체로 인하여 상당한 비용과 시간이 필요하므로 본 논문에서는 MPLS망을 기반으로 Ingress 및 Egress LSR에 플로우 제어 메커니즘을 구현하였다. 플로우 제어를 통해 단말 트래픽을 간접적으로 제어하고 백본망에서는 서비스 클래스 기반으로 플로우 처리를 수행하여 단-대-단 트래픽 제어를 수행한

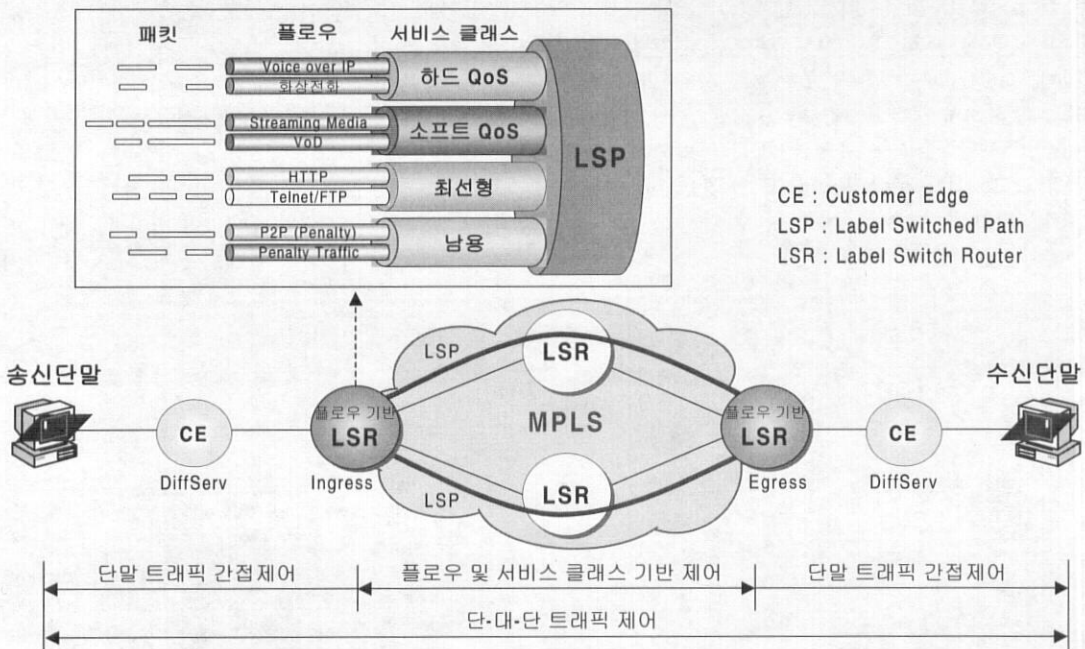


그림 2. 플로우 제어를 위한 제안 시스템 모델

다. CE에서 Ingress LSR 구간과 Egress LSR에서 CE 구간은 SLA(Service Level Agreement)[11] 범위 내에서 품질을 제공할 수 있도록 DiffServ 기능이 활용된다.

그림 2의 제안 시스템 모델에서 CE(Customer Edge)는 가입자망에서 사업자 또는 백본망과 접속되는 가입자 장비를 의미하고, 플로우 기반 LSR(Label Switch Router)은 MPLS 기능을 탑재하고 있는 라우터를 나타낸다. LSR 사이에는 MPLS 패킷 전달을 위해 LSP가 설정되고 IPv6 패킷은 MPLS 패킷에 캡슐화(Encapsulation)되어 교환된다. 송신 단말은 IPv6 QoS 홉-바이-홉 옵션 헤더에 QoS 정보가 표기된 트래픽을 발생시키고, Ingress LSR에서는 해당 트래픽을 플로우 단위로 식별하여 플로우별로 통계 처리를 수행하고 해당 서비스 클래스로 매핑한다.

본 논문에서는 Roberts가 제안한 IPv6 QoS 홉-바이-홉 옵션 헤더의 플로우 유형(GR, CR, AR), Guaranteed Rate(이하 요청 GR) 및 MLPP 필드를 사용하여 플로우 제어 메커니즘을 설계한다. 플로우 유형이 AR인 플로우는 예약되지 않은 대역을 플로우들이 공유하는 최선형 서비스며, GR인 플로우는 일정 대역폭의 보장을 필요로 하는 서비스, CR인 플로우는 GR과 AR이 결합된 형태로 최소한의 대역폭 보장을 필요로 하는 스트리밍 또는 최선형 서비스이다. 플로우의 서비스 클래스 타입은 하드(Hard) QoS, 소프트(Soft) QoS, 최선형(Best Effort), 남용(Abusive)으로 분류하고 각 서비스 클래스별로 플로우 유형을 매핑하였다. 표 1은 서비스 클래스별 해당 플로우 유형과 IETF Diffserv[10], ITU-T Y.1541[7]에서 정의한 IP QoS 클래스와의 관계 및 관련 응용서비스 예를 나타낸다.

표 1. 서비스 클래스 분류

서비스클래스	플로우 유형	IETF DiffServ	ITU-T Y.1541	응용서비스 예
하드 QoS	GR	EF	Class 0.1	VoIP, 화상전화
소프트 QoS	CR	AF	Class2, 3,4	주문형 비디오
최선형	AR	BE	Class 5	웹, FTP, E-mail
남용	AR	BE	Class 5	억제 대상 P2P

CE에서는 DiffServ를 처리하기 위해 하드 QoS는 EF(Expedited Forwarding), 소프트 QoS는 AF(Assured Forwarding), 그 외 플로우는 BE(Best-Effort)로 IPv6 헤더내의 TC(Traffic Class) 필드에 표기한다. DiffServ는 또한 IPv6 QoS 홉-바이-홉 옵션 헤더 내의 플로우 유형을 기반으로 한 클래스 분류 기능이 추가되어야 한다. 스케줄러(Scheduler)는 CBWFQ(Class-Based Weighted Fair Queuing)을 적용하여 플로우 특성에 따른 차등적인 QoS를 제공한다.

Ingress LSR에서는 그림 3과 같은 플로우 제어 메커니즘을 수행한다. 플로우 제어는 플로우 분류, 정책 및 혼잡 제어, FST(Flow State Table) 관리를 통한 남용 플로우 제어, 레이블 삽입 및 EXP 표기를 통한 서비스 클래스 할당, CBWFQ에 따른 스케줄링 및 LSP 매핑 과정을 통해 수행된다. 패킷이 입력되면 플로우 분류를 통해 FST에 해당 패킷의 플로우 상태 정보 존재 여부를 검색하여 플로우 정보가 없는 경우는 플로우의 첫 번째 패킷으로 간주한다. 이 경우 패킷의 QoS 홉-바이-홉 옵션 헤더 정보를 추출하여 정책 제어를 통한 SLA 준수 여부

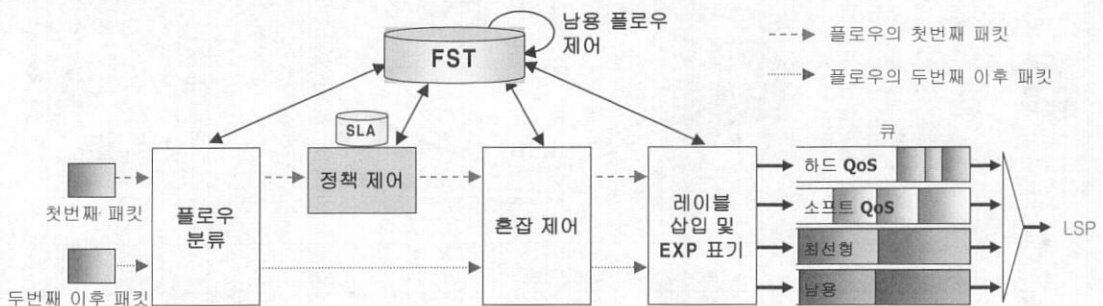


그림 3. Ingress LSR에서의 플로우 제어 메커니즘

와 혼잡 제어를 통한 망 자원의 접근 가능 여부에 따라 플로우의 수락을 결정한다. 플로우의 수락이 결정되면 FST에 해당 플로우에 대한 상태 정보를 생성하고, 패킷에 대해 서비스 클래스에 따른 MPLS 레이블 삽입 및 EXP 표기를 수행한다. 이후 패킷은 표기된 값에 따라 해당 서비스 클래스에 할당되어 CBWFQ 스케줄링을 통해 LSP로 매핑된다. 플로우의 두 번째 패킷부터는 FST에 따라 첫 번째 패킷과 동일한 경로와 동일한 서비스 클래스로 처리된다. 단, 혼잡 제어 과정에서 우선순위가 낮은 플로우가 제거되었거나 남은 플로우 제어 과정에서 서비스 클래스가 변경된 경우는 변경된 FST 정보에 따라 처리된다.

Egress LSR에서는 Ingress LSR과 유사하게 동작하나 정책 제어, 남은 플로우 제어, LSP 매핑을 위한 레이블 삽입 및 EXP 표기 과정은 생략된다. MPLS 레이블이 팝업된 패킷은 플로우 분류와 혼잡 제어에 따라 FST에 플로우 정보를 생성한 후, CE에서 표기된 패킷의 TC(Traffic Class) 값에 따라 패킷을 해당 서비스 클래스로 할당하여 처리한다.

3.2 플로우 분류

IPv6에서는 IPv6 헤더의 플로우 레이블 필드를 Non-Default QoS 또는 실시간 서비스와 같은 QoS가 요구되는 플로우를 식별하는 용도로 활용한다[2]. 하지만, 인터넷 환경은 P2P 트래픽의 폭발적인 증가, DDoS 및 Warm 등의 유해 트래픽이 확산됨에 따라 품질 보장 트래픽뿐만 아니라 일반 트래픽에 대한 제어의 필요성이 동시에 요구되고 있다. 따라서, 플로우 레이블 값을 이용하는 트래픽뿐만 아니라 플로우 레이블 값을 갖지 않는 일반 트래픽까지 플로우 기반 처리가 필요하다.

본 논문은 플로우 분류과정에서 패킷의 플로우 레이블 값이 표기된 경우는 3개 구성요소(플로우 레이블, 송신지/수신지 주소)에 의해 플로우를 분류하

고, 플로우 레이블 값을 갖지 않는 경우는 송신지/수신지 주소, 송신지/수신지 포트번호, 프로토콜 타입의 5개 구성요소에 의해 플로우를 분류한다. 이때 IPSec 프로토콜로 암호화된 플로우는 플로우 분류 과정에서 전송계층의 포트번호를 인식할 수 없으므로 플로우 레이블 값을 표기하여 플로우를 식별한다. 플로우 분류 후에는 FST(Flow State Table)에서 플로우 상태 정보의 존재 여부를 검색한다. 플로우 상태 정보가 FST에 존재하는 경우는 FST의 정보를 참조하여 바로 포워딩되며, 플로우 정보가 FST에 존재하지 않는 경우는 해당 플로우에 대한 정책 및 혼잡 제어를 수행하여 플로우 상태 정보의 생성여부를 결정한다.

3.3 플로우 제어를 위한 FST 관리

플로우의 전달 경로상에 있는 MPLS망의 Ingress LSR과 Egress LSR에서는 FST를 유지함으로써 플로우에 대한 처리 메커니즘을 제공한다. FST의 관리는 플로우 상태 정보의 생성(Add)과 삭제(Delete), 재설정(Refresh) 과정으로 이뤄지며 이를 위해 플로우 타이머 값(t)이 사용되는데, 본 논문에서는 "IPv6 Flow Label Specification"[4]을 참조하여 t값을 60초로 설정하였다. 패킷이 입력되었을 때, FST에 해당 패킷에 대한 플로우 상태 정보가 없는 경우(즉, 플로우의 첫 번째 패킷이 도착하는 경우)에는 정책 및 혼잡 제어를 통해 수락된 플로우에 한하여 FST에 새로운 플로우 상태 정보를 생성(Add)한다. FST에서의 플로우 상태 정보의 관리는 플로우 타이머 값에 의해 결정된다. 즉, 플로우 생성시에는 60초로 설정되며 시간이 경과함에 따라 감소되다가 해당 플로우에 속한 패킷이 도착할 경우 다시 60초로 설정된다. 플로우 타이머 값이 0이 된 경우, 해당 플로우는 FST에서 삭제(Delete)된다.

표 2는 LSR에서 관리되는 FST 구성을 보여준다. 플로우 레이블, 송신지/수신지 주소, 송신지/수신지

표 2. LSR에서의 플로우 상태 테이블(FST) 구성

플로우 식별자						QoS 홉-바이-홉 옵션 헤더 정보			남은 플로우 제어				
플로우 레이블	송신지 주소	수신지 주소	송신지 포트번호	수신지 포트번호	프로토콜	플로우 유형	요청 GR	MLPP	사용시간	평균 전송률	전송 바이트 수	서비스 클래스	타이머
Flow 11	XX	XX	179	XX	TCP	GR	144kbps	1	10	100kbps	100kB	하드 QoS	58
Flow 12	XX	XX	179	XX	TCP	GR	100kbps	2	12	80kbps	100kB	하드 QoS	55
Flow 21	XX	XX	25	XX	UDP	CR	1Mbps	-	8	1Mbps	1MB	소프트 QoS	52
-	XX	XX	1214	XX	TCP	AR	-	-	20	30kbps	1kB	최선형	58
-	XX	XX	6346	XX	TCP	AR	-	-	50	50kbps	5MB	남용	55

포트번호, 프로토콜은 플로우 식별자이며, 플로우 유형, 요청 GR, MLPP 값은 플로우에 대한 QoS 정보로 QoS 홈-비-홈 옵션 헤더 정보를 기반으로 생성된다. 이때, 플로우 유형은 GR, CR, AR로 구분되며, 요청 GR은 송신 단말에서 요청한 플로우의 보장대역폭을 나타낸다. MLPP는 GR 플로우의 우선순위에 따라 차등화된 접근성을 제공하는 용도로 사용된다. 플로우 사용시간, 평균 전송률 및 전송 바이트 수는 최선형 클래스의 플로우가 사전 정의된 임계값을 초과하는 경우 남용 클래스로 변경하기 위해 사용된다. 서비스 클래스는 플로우의 서비스 타입을 식별하여 해당 서비스 클래스로 플로우를 할당하기 위해 사용되며, 하드 QoS, 소프트 QoS, 최선형, 남용 타입으로 구성된다.

3.4 정책 및 혼잡 제어

첫 번째 입력되는 패킷의 플로우 상태 정보를 FST에 생성하기 위해서는 먼저 플로우에 대한 수락 여부를 결정해야 한다. 이 때, 플로우의 서비스 유형이 하드 및 소프트 QoS 서비스인 경우는 정책 제어와 혼잡 제어를 통해 플로우의 수락 여부를 결정하고 최선형 서비스인 경우는 설정된 최선형 클래스 대역폭을 플로우들이 공유하여 사용하므로 정책 및 혼잡 제어 과정없이 플로우의 요청을 수락한다.

정책 제어는 플로우의 요청 GR에 대해 가입자 SLA(Service Level Agreement)[11] 준수 여부를 판별하고 혼잡 제어는 LSR이 플로우의 요청 GR을 수용할 수 있는지를 판별한다. 플로우의 서비스 유형이 GR 및 CR인 경우에는 요청 GR에 대한 대역폭 예약이 필요한데 이를 예약 GR로 정의한다.

그림 4는 플로우의 첫 번째 패킷에 대한 정책 및 혼잡 제어 메커니즘으로 각 변수들의 정의는 다음과 같다.

- Fi : i 가입자 플로우
- C(Fi) : Fi가 속한 서비스 클래스
- Br(Fi) : i 가입자 플로우의 요청 GR
- Bs(i) : i 가입자 플로우들의 예약 GR 합
- Bsla(i) : i 가입자의 SLA 보장 GR
- Bc(Fi) : C(Fi)의 할당대역폭
- Ba(Fi) : C(Fi)의 예약 GR 합
- MFi : Fi의 MLPP 값
- Bp(Fi, k) : C(Fi)에서 MLPP 값이 k인 플로우들의 예약 GR 합

정책 제어 과정에서 하드 또는 소프트 QoS 플로우의 요청 GR(Br(Fi))은 SLA에 정의된 가입자별 보장 GR(Bsla(i))에서 FST에 있는 해당 가입자 플로우들의 예약 GR 합(Bs(i))을 뺀 값과 비교한다. 요청 GR을 수용할 수 있는 경우(즉, Br(Fi) ≤ Bsla(i) - Bs(i))는 혼잡 제어 과정을 수행하고, 그렇지 않을 경우는 패킷을 폐기(Drop)한다.

혼잡 제어 과정에서 플로우의 요청 GR(Br(Fi))은 플로우가 속한 서비스 클래스의 할당대역폭(Bc(Fi))에서 서비스 클래스의 예약 GR(Ba(Fi)) 합을 뺀 값과 비교한다. 요청 GR을 수용할 수 있는 경우(즉, Br(Fi) ≤ Bc(Fi) - Ba(Fi))는 플로우에 대한 FST를 생성하고, 그렇지 않은 경우는 플로우의 서비스 클래스가 소프트 QoS이면 패킷을 폐기하고 하드 QoS이면 MLPP 비교 과정을 수행한다. MLPP 비교 과정에서는 입력 플로우의 요청 GR(Br(Fi))과 입력 플로우의 MLPP 값보다 낮은 MLPP 값을 가지는

기존 플로우들의 예약 GR 합 즉, $\sum_{k=0}^{MFi-1} Bp(Fi, k)$

을 비교한다. 이때, Br(Fi) ≤ $\sum_{k=0}^{MFi-1} Bp(Fi, k)$

인 경우는 입력 플로우의 대역폭 선점(Preemption)을 위해서 입력 플로우보다 낮은 MLPP 값을 가지는 기존 플로우를 FST에서 삭제하고 새로운 입력 플로우 상태 정보를 FST에 생성한다.

이러한 정책 및 혼잡 제어 과정에서 발생하는 플로우의 첫 번째 패킷 손실은 중단간 MBAC(Measurement Based Admission Control)[12] 내의 프루브(probe)의 손실 또는 TCP 연결의 SYN나 SYN-

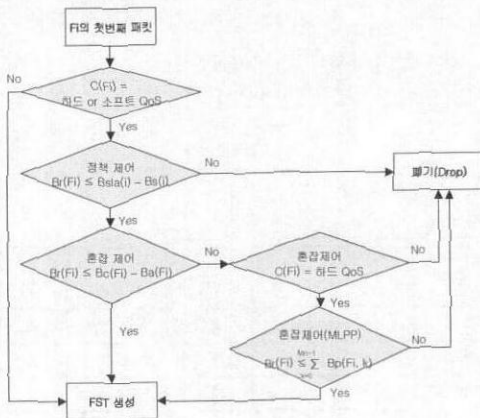


그림 4. 정책 및 혼잡 제어 메커니즘

ACK의 손실[13]을 의미한다. 이후 손실된 패킷에 대한 재전송 여부는 사용자의 선택에 따른다.

3.5 플로우의 품질 보장을 위한 LSP 매핑

백본망의 코어 라우터에서의 플로우 제어 오버헤드를 최소화하기 위해 MPLS 기술을 사용한 경우에는 Ingress LSR에서 각 서비스 클래스별 플로우들은 MPLS LSP와 적절하게 매핑되어야 한다. Ingress LSR에서 정책 제어와 혼잡 제어를 통해 수락된 플로우들은 해당 서비스 클래스로 할당되고 스케줄링을 통해 LSP로 매핑된다. 이때 하드 또는 소프트 QoS 서비스 클래스로 할당된 플로우들이 품질 저하없이 MPLS망을 통과하기 위해 MPLS DiffServ 기술이 사용된다[14].

Ingress LSR에서는 입력 패킷에 대해 FST를 참조하여 해당 패킷이 속한 플로우 유형에 따라 서비스 클래스를 결정하고 LFT(Label Forwarding Table)를 참조하여 LSP로 매핑되기 위한 MPLS 출력 레이블을 선택한다. LSP 타입이 E-LSP(EXP-Inferred-PSC LSP)이면 FEC(Forwarding Equivalence Class)에 따라 출력 레이블이 결정되고 서비스 클래스와 EXP 매핑 레이블을 참조하여 EXP 필드가 표기된다. L-LSP(Label-Only-Inferred LSP)의 경우에는 <FEC, 서비스 클래스>쌍에 해당하는 출력 레이블이 사용되며 패킷 패기의 우선순위에 따라 EXP 필드가 표기된다. 레이블이 푸쉬된(Labeled) 패킷은 EXP(E-LSP인 경우) 또는 레이블(L-LSP인 경우)을 참조하여 해당 서비스 클래스로 할당되어 CBWFQ(Class Based Weighted Fair Queuing) 방식에 따라 스케줄링을 받고 MPLS망을 통과한다.

3.6 남용 플로우 제어

본 논문에서는 망 자원을 남용하는 응용서비스를 남용 플로우로 정의하고 별도 서비스 클래스로 분류함으로써 자원 이용을 보다 효과적으로 제한한다. 남용 플로는 응용서비스 특성의 편별이 어렵거나 장시간 대용량의 트래픽을 발생하는 최선형 플로우로 정의한다. 남용 플로우 식별을 위해 FST에서는 플로우별 사용시간, 평균 전송률, 전송 바이트 수 정보를 유지하면서 사전 정의된 임계값을 초과하는 최선형 플로우를 남용 클래스로 변경한다. 남용 클래스로 변경된 플로는 남용 클래스에 할당된 대역폭을 다른 남용 플로우들과 공유한다. 이를 통해 남용 플로우에 의한 최선형 플로우들의 품질 저하

를 개선하고 전체 망 자원을 효율적으로 사용할 수 있게 된다.

4. 성능 평가

본 논문에서 제안한 IPv6 홉-바이-홉 옵션 헤더를 이용한 플로우 품질 제어 방안의 성능을 비교 분석하기 위하여 CAC, MLPP 및 남용 플로우 제어에 대해 시뮬레이션을 수행하였다. 시뮬레이션은 네트워크 시뮬레이터인 ns-2[15]를 사용하였고, TCL/TK 기반 도구인 nam[16]을 이용하여 시뮬레이션 결과를 보였다.

4.1 시뮬레이션 환경

그림 5는 본 시뮬레이션에 사용된 ns-2에서의 토폴로지를 나타낸 것으로 CE와 Ingress LSR사이의 액세스(Access) 구간은 DiffServ 메커니즘을 사용했고 백본 구간은 MPLS 기술을 적용하였다.

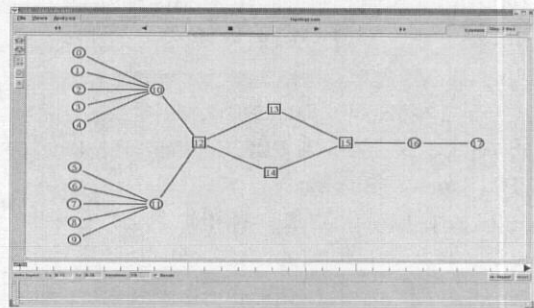


그림 5. ns-2 시뮬레이션 토폴로지

그 밖에 시뮬레이션을 위해 가정한 사항을 요약하면 아래와 같다.

- 트래픽을 발생하는 송신 노드는 0,1,2,3,4,5,6,7,8,9 이다.
- CE 노드는 10,11,16이며 DiffServ(WFQ) 기능을 통해 트래픽을 분류하여 해당 큐로 전송한다.
- MPLS 도메인은 노드 12,13,14,15 이며, 노드 12,15는 각각 Ingress LSR, Egress LSR 기능을 수행한다.
- MPLS 도메인에서 LSP(Label Switched Path)는 노드 12,13,15를 경유하여 형성한다.
- 노드 17은 트래픽이 전송되는 수신지이다.

본 논문에서는 혼잡 제어를 위한 CAC, MLPP

기능과 남용 플로우 제어를 시뮬레이션하기 위해 기존 ns-2의 기능을 확장하였다. CE에서는 트래픽의 종류에 따라 서로 다른 큐를 할당할 수 있도록 WFQ(Weighted Fair Queuing) 기능을 사용했고, Ingress LSR 에서는 플로우 분류, 혼잡 제어, FST 관리를 통한 남용 플로우 제어, WFQ 기능, LSP 매핑 기능 등을 구현하였다. 표 3은 본 시뮬레이션에 사용된 시스템 환경을 나타낸다.

표 3. 시뮬레이션 시스템 환경

하드웨어	Solaris Ultra 10
운영체제	Solaris 2.8
소프트웨어	NS-2 2.1b9
프로그래밍 언어	C++, OTcl

표 4와 5는 본 시뮬레이션에서 사용된 파라미터의 값을 나타낸다. 표 4에서 각 트래픽 타입별 특성을 반영하기 위해 하드 트래픽 타입은 VoIP 서비스, 소프트 트래픽 타입은 VoD(MPEG-2) 서비스, 최선형 트래픽 타입은 FTP 서비스로 가정한다. 일반적으로 VoIP 트래픽은 Exponential 분포를 따르므로 ns-2의 Exponential 트래픽 에이전트를 이용하고, MPEG-2 트래픽은 CBR(Constant Bit Rate)과 VBR(Variable Bit Rate)를 지원[17]하므로 ns-2의 CBR 트래픽 에이전트를 이용한다. FTP 트래픽은 ns-2의 TCP 트래픽 에이전트를 이용한다. 마지막으로, 각 트래픽 타입별 패킷 크기와 전송 속도 등의 파라미터 값은 서비스별 특성을 반영하여 설정하였다.

구간별 링크 구성은 시뮬레이션을 용이하게 하기 위해 표 5와 같이 링크 속성값 중에 대역폭과 링크 지연만을 고려하였다. 송신지에서 Ingress LSR 사이의 각 링크 대역폭은 송신지의 트래픽 전송 속도를 반영함으로써 패킷 손실이 발생하지 않도록 하기 위해 트래픽 송신지에서 CE구간은 1Mbps, CE에서 Ingress LSR 구간은 5Mbps로 대역폭을 설정하였다. Ingress LSR과 Egress LSR 사이의 각 링크 대역폭은 3Mbps로 설정하고 서비스 클래스별 대역폭을 설정하였다. 하드 QoS 클래스와 소프트 QoS 클래스는 각각 1Mbps, 최선형 클래스는 900kbps, 남용 클래스는 100kbps로 설정하였다.

본 논문은 시뮬레이션을 세 가지 성능 메트릭에 초점을 두어 수행하였다. 첫 번째로 CAC 기능 수행 여부에 따른 하드 플로우의 품질 변화를 비교하

표 4. 트래픽 발생 송신지와 유형

트래픽 송신지 노드	트래픽 타입	트래픽 파라미터
0, 1, 5, 6	하드 트래픽 (Exponential)	패킷 크기: 200byte Burst 시간: 1,000ms Idle 시간: 1,350ms 전송 속도: 300kbps
2, 7	소프트 트래픽 (CBR)	패킷 크기: 200byte 전송 속도: 500kbps
3, 8	최선형 트래픽 (TCP)	패킷 크기: 1,000byte 파일 사이즈: 5Mbyte
4, 9	최선형 트래픽 (TCP)	패킷 크기: 1,000byte 파일 사이즈: 20 Mbyte

표 5. 구간별 링크 대역폭 및 지연

구간	링크 대역폭	링크 지연
트래픽 송신지에서 CE	1Mbps	10ms
CE에서 Ingress LSR	5Mbps	10ms
MPLS 도메인의 각 링크	3Mbps	10ms
Egress LSR에서 수신지	3Mbps	10ms

표 6. 남용 플로우 식별 정책

구분	임계값
플로우별 사용시간	60초
전송 바이트 수	10Mbyte

였다. 이를 위해 송신지 노드 6은 노드 0,1,5의 트래픽 발생 이후 임의의 시간에 트래픽을 발생시키고, 노드 6 플로우의 CAC 적용 여부에 따른 하드 QoS 플로우의 성능을 측정하였다. 두 번째로 망 혼잡시 하드 QoS 플로우에 대한 MLPP기반 CAC 적용 여부에 따른 우선순위별 차별화된 접근성을 비교하였다. 이를 위해 송신지 노드 0,1,5,6에서는 우선순위가 각각 0,1,2,3인 트래픽을 발생시키고, 노드 6 플로우에 대해 우선순위가 낮은 노드 0 플로우의 CAC 적용 여부에 따른 성능을 측정하였다. 세 번째로 남용 플로우 식별 정책에 따라 임계값을 초과하는 최선형 플로우에 대한 남용 클래스로의 변경 처리 여부에 따른 플로우들의 품질 변화를 비교하였다. 이를 위해 표 4와 같이 송신지 노드 3과 8은 5Mbyte, 송신지 노드 4와 9는 20Mbyte 파일 크기의 트래픽을 발생시키고, 남용 플로우 식별 정책을 표 6과 같이 플로우별 사용시간과 전송 바이트 수에 대한 임계값으로 정의하였다.

4.2 시뮬레이션 결과 분석

그림 6과 7은 각각 CAC 적용 여부에 따라 노드 0의 하드 QoS 플로우에 대한 처리량 및 손실율을 나타낸다. CAC 기능이 미적용된 경우에는 4개의 트래픽 송신지가 동시에 트래픽을 발생시키는 혼잡 구간에서 하드 트래픽 전송량이 하드 QoS 클래스

대역폭인 1Mbps를 초과하게 되어 패킷 손실이 발생되므로 엄격한 QoS를 요구하는 하드 QoS 플로우의 전송을 보장할 수 없게 된다. CAC 기능이 적용된 경우에는 혼잡 제어 과정에서 하드 QoS 클래스 대역폭을 초과한 트래픽의 유입이 차단된다. 따라서, 노드 6의 하드 QoS 플로우에 대한 전송이 수락되지 않으므로 기존에 전송 중인 노드 0,1,5의 하

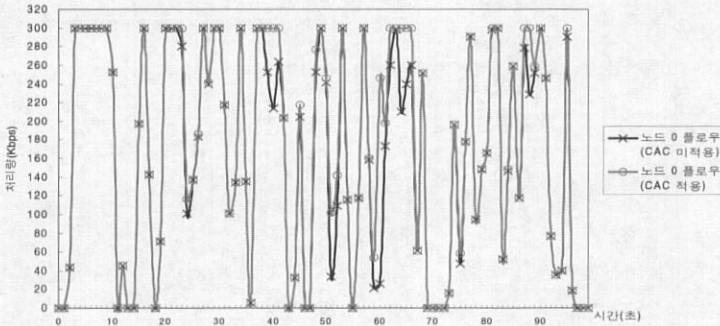


그림 6. CAC 적용 여부에 따른 노드 0 플로우의 처리량

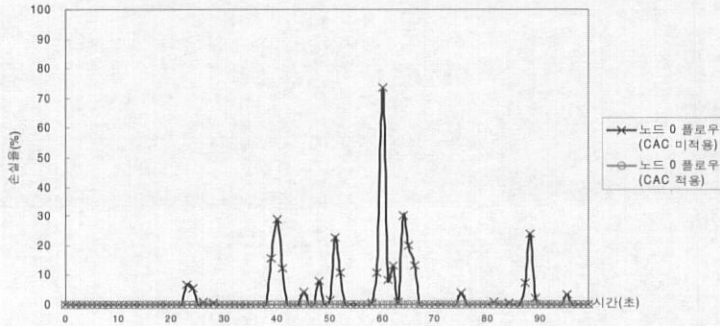


그림 7. CAC 적용 여부에 따른 노드 0 플로우의 손실율

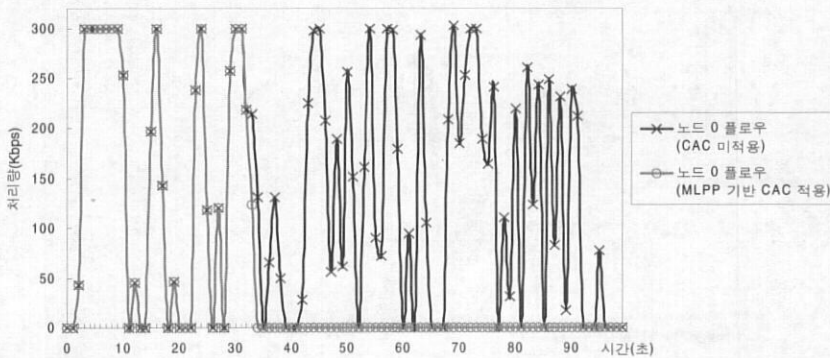


그림 8. MLPP기반 CAC 적용 여부에 따른 노드 0 플로우의 처리량

드 QoS 플로우에 대한 품질을 보장할 수 있다.

그림 8과 9는 각각 MLPP기반 CAC 적용 여부에 따른 노드 0과 6의 하드 QoS 플로우에 대한 처리량을 나타낸다. MLPP기반 CAC 기능이 적용된 경우에는 하드 QoS 플로우들 간의 MLPP 값 비교를 통해 플로우의 수락여부가 결정된다. 그림 8에서

노드 6의 하드 QoS 플로우가 생성되는 30초대 구간에서는 기존 전송중인 하드 QoS 플로우들 중에서 노드 6의 하드 QoS 플로우보다 우선순위가 낮은 노드 0의 하드 QoS 플로우가 거절된다. 또한 그림 9에서 노드 6의 하드 QoS 플로우가 노드 0의 점유 자원을 선점하므로 CAC가 미적용된 경우보다

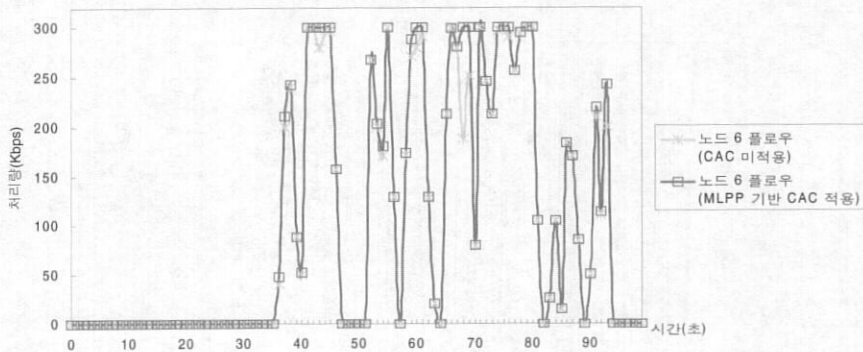


그림 9. MLPP기반 CAC 적용 여부에 따른 노드 6 플로우의 처리량

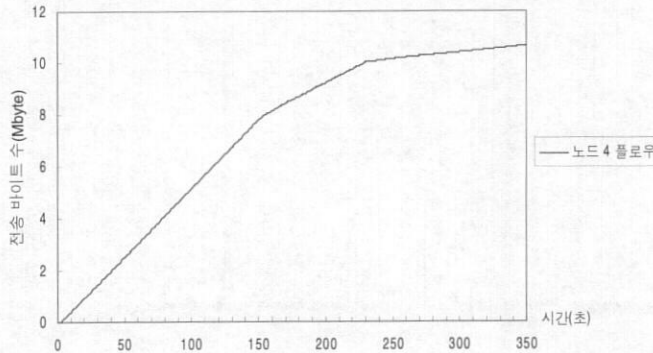


그림 10. 노드 4 플로우의 전송 바이트 수

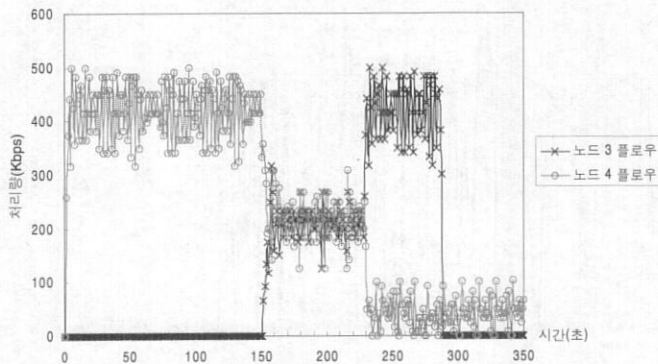


그림 11. 남용 플로우 제어에 따른 플로우 처리량

품질이 개선됨을 볼 수 있다.

그림 10과 11은 각각 남용 플로우 제어에 따른 노드 4 플로우의 전송 바이트 수 및 노드 3과 노드 4 플로우의 처리량 변화를 나타낸다. 그림 10에서 보면 노드 3 플로우는 전송 바이트 수가 10Mbps를 초과하는 시점인 230초대 구간에서 남용 플로우로 식별된다. 따라서, 그림 11에서와 같이 230초대에 노드 4 플로우의 서비스 클래스가 변경되며 이후 남용 클래스에 할당된 100kbps 대역폭 내에서 처리된다. 노드 3의 최선형 플로우는 노드 4,8,9의 플로우와 최선형 클래스에 할당된 900kbps 대역폭을 공유하다가 노드 4와 9 플로우가 남용 플로우로 식별되어 별도 클래스로 처리되는 230초대 이후부터는 처리량이 개선됨을 알 수 있다.

5. 결론 및 향후 과제

본 논문에서는 IPv6망에서 트래픽을 플로우 단위로 식별하고 IPv6 홈-바이-홈 옵션 헤더 내의 QoS 정보를 이용하여 멀티서비스의 QoS 개선을 위한 플로우 제어 방안을 제시하였다. 그 구현방법으로 IPv6 환경에서 플로우 레이블 값을 이용하는 Non-default QoS 트래픽 뿐만 아니라 최선형 및 암호화 트래픽으로 플로우 제어 대상이 확대 적용되었다. 혼잡 제어 과정에서는 신규 또는 우선순위가 낮은 플로우에 대해 CAC(Connection Admission Control)와 MLPP(Multi Level Preemption Priority)를 적용하였고, 남용 플로우 제어 과정에서는 플로우별 사용시간, 평균 전송률, 전송 바이트 수를 관리하여 남용 플로우를 식별하고 별도로 정의된 서비스 클래스로 분류하여 처리하였다. 또한, 기존 망 자원의 최소 변경과 통신사업자의 백본망 현황을 반영하여 제안된 플로우 제어 방안과 MPLS를 매핑하였다. 이를 통해 실시간 서비스에 대한 보장성은 강화하고 불필요하게 망 자원을 남용하는 플로우는 효과적으로 제어한다. 이를 검증하기 위해 시뮬레이션을 통하여 제안하는 플로우 제어 방안의 효율성을 확인하였다.

본 논문에서 제안한 IPv6 홈-바이-홈 옵션 헤더를 이용한 플로우 제어 방식은 향후 도입될 순수 IPv6망에서 실시간 트래픽에 대한 QoS 보장 및 남용 트래픽 제어를 통해 가입자에게 차등화된 프리미엄 서비스를 제공하고자 하는 사업자에게 유용할 것이다. 또한, 향후 개발될 IPv6 전용 장비에 플로우 제어 방식을 적용하기 위해서는 FST(Flow State

Table) 유지를 위한 DDR SDRAM(Double Date Rate Synchronous Dynamic RAM)등의 메모리 기술과 사용시간, 평균 전송률, 전송 바이트수의 효율적 계산을 위한 ASIC(Application-Specific Integrated Circuit) 기술의 수용이 필요하다. 향후 과제로는 IPv6 홈-바이-홈 옵션 헤더를 이용한 QoS 시그널링을 통해 단말의 전송률을 직접적으로 제어하여 플로우의 성능을 개선하고 BT(Burst Tolerance) 및 지연값 등을 활용하여 보다 엄격하고 정밀한 QoS를 제공하는 방안에 대한 연구가 진행되어야 한다.

참 고 문 헌

- [1] N. B. Azzouna and F. Guillemin. "Analysis of ADSL traffic on an IP backbone link," from in Proc. Globecom 2003, San Francisco, Dec. 2003.
- [2] S. Deering, and R. Hinden, et al., "Internet Protocol, Version 6 (IPv6) Specification," RFC 2460, Dec. 1998.
- [3] S. Schmid, et al., "QoS-based Real-time Audio Streaming in IPv6 Networks," from in Proc. of SPIE Vol. 3529, Internet Routing and Quality of Service, Boston, 1998.
- [4] J. Rajahalme, et al., "IPv6 Flow Label Specification," Work in Progress, Internet Draft, Oct. 2003.
- [5] R. Banerjee, et al., "A Modified Specification for Use of the IPv6 Flow Label for Providing an Efficient Quality of Service Using a Hybrid Approach," Work in Progress, Internet Draft, Apr. 2002.
- [6] L. G. Roberts, "Fast Setup QoS for IPv6," Work in Progress, TIA, Oct. 2003.
- [7] ITU-T Rec. Y.1541, "Network Performance Objectives for IP-Based Services," 2002.
- [8] T. Bonald, et al., "Flow-Aware Admission Control for a Commercially Viable Internet," EURESCOM Summit 2002, Heidelberg, Germany, Oct. 2002.
- [9] R. Braden, et al., "Resource ReSerVation Protocol (RSVP) - Version 1 Functional Specification," RFC 2205, Sep. 1997.
- [10] Y. Bernet, et al., "An Informal Management

Model for DiffServ Routers," RFC 3290, May 2002.

- [11] Walder, and Bob, "Service Level Agreements," Connections Newsletter from the NSS Group, Mar. 1998.
- [12] L. Breslau, et al., "Endpoint Admission Control: Architectural Issues and Performance," Proc ACM SIGCOMM, Stockholm, Sweden, Oct. 2000, pp. 57-9.
- [13] R. Mortier, et al., "Implicit Admission Control," IEEE Journal on Selected Areas in Communications, Dec. 2000.
- [14] F. Le Faucheur, et al., "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services," RFC 3270, May 2002.
- [15] "The ns-2 simulator," <http://www.isi.edu/nsnam/ns/>
- [16] "The nam animator," <http://www.isi.edu/nsnam/nam/>
- [17] A. Mehaoua and R. Boutaba, "The Impacts of Errors and Delays on the Performance of MPEG2 Video Communications," Proceedings of the IEEE International Conference On Acoustics, Speech, and Signal Processing, 1999.

이 인 화(In-Hwa Lee)

정회원



1987년 경북대학교 전자공학과
공학사
1994년 중앙대학교 정보대학원
공학석사
2000년 중앙대학교 컴퓨터공학과
박사수료
1987년 대신증권 전산센터
1992년 포스데이타 SI사업부
1992년 - 현재 (주) CST 상무이사/CTO

<관심분야> IPv6, NGI, VPN, MPLS, Mobile IP

김 성 조(Sung-Jo Kim)

정회원



1975년 서울대학교 응용수학과
(공학사)
1977년 한국과학기술원 전산과
(이학석사)
1977년 ~ 1980년 ADD(연구원)
1980년 ~ 현재 중앙대학교 컴퓨터
공학부(교수)
1987년 Univ. of Texas at
Austin (공학박사)
1987년 ~ 1988년 Univ. of Texas at Austin
(Research Fellow)
1996년 ~ 1997년 Univ. of California - Irvine
(Visiting Researcher)

<관심분야> 모바일 컴퓨팅, 임베디드 소프트웨어 및 유비쿼터스 컴퓨팅임.