인터넷 VPN의 QoS에 대한 연구

최 용, 백승진, 박종태
경북대학교 대학원 정보통신학과
e-mail:antiself@knuicsvr1.knu.ac.kr

A Study on QoS of Internet VPN

Yong Choi, Seung-Jin Baek, Jong-Tae Park
Department of Information and Communication,
Kyungpook National University

요약

인터넷 VPN은 통신비용 절감과 접속 영역의 확장 및 신뢰적인 데이터 통신이 가능하도록 하는 기술이지만 최근 들어 인터넷 사용자의 급성장과 상업화로 인한 멀티미디어 서비스와 실시간성을 요구하는 인터넷 응용서비스를 지원하기 위한 QoS는 만족스럽지 못하다. 인터넷 QoS를 위해 IETF에 제출된 통합서비스는 확장성이 부족한 단점이 있다. 차등서비스 구조는 통합서비스 구조에 비해 확장성이 훨씬 좋아 QoS를 제공하기 위한, 인터넷 백본망에서 구현 가능한 방법으로 떠오르고 있다. MPLS는 라벨에 따라 패킷을 포워딩하는 혁신적인 기술로 확장성이 좋다. 특히 MPLS는 터널링 프로토콜로 사용 가능하고 패킷 캡슐화 기능등을 가지고 있어 VPN을 구성하기에 적합하다. MPLS 인터넷 VPN에서 QoS를 보장하기 위해서는 QoS가 지원되도록 디자인된 라우터나 IP 스위치와 트래픽 엔지니어링 알고리즘등을 사용해야만 최적으로 보장된다.

1. 서론

최근들어 각 기업들은 기존의 전용선이나 가상회선을 이용한 WAN 접속에 드는 비용을 줄이기 위해 인터넷을 이용하려 하고 있다. 또한 근무의 위치가 사무실에 국한되지 않고 집이나 업무 현장으로 확대되어 감에 따라 기업 내부에서의 정보 공유를 위한 LAN 구성뿐 아니라 기업 외부와의 네트워크 구성을 필요로 하게 되었다. 이런 다양한 요구조건을 수용할 수 있는 기술로 주목받고 있는 것이 인터넷을 이용한 VPN(Virtual Private Network)이다.

VPN은 공중망을 이용하여 사설망의 기능을 제공하는 가상의 사설 네트워크라 할 수 있다. 따라서 인터넷 VPN이란 IP 프로토콜로 구성되어 있는 공중 데이터망인 인터넷을 통해 사설망의 기능을 제공하는 것을 뜻한다. 현재, VPN 제공 기술은 통신의 시작점과 끝점에 터널링 프로토콜을 탑재하여 이들 사이에 터널이라는 가상 통신 선로를 구축하는 방안이 널리 사용되고 있다. 하지만 현재의 인터넷에서 터널링 기법을 이용하여 단대단(end-to-end) VPN을 제공하는 기술은 공중 인터넷 망을 수정하지 않고 VPN을 제공할 수 있는 장점이 있지만, 현재 인터넷이 최선형 서비스만을 지원하기 때문에 사용자에게 차별화된 VPN을 제공할 수 없으며, 망의 상태나 가입자의 요구사항에 따라 동적으로 VPN을 구성하지 못하는 단점이 있다. 또한 인터넷의 빠른 성장으로 등장한 멀티미디어 서비스와 VoIP(Voice over IP)등 실시간성을 필요로 하는 인터넷 응용서비스를 지원하기 위해 필수적인 QoS(Quality of Service)를 제대로 지원하지 못하는 단점도 있다. IETF(Internet Engineering Task Force)에는 위와 같은 인터넷의 단점들을 극복하기 위해 많은 서비스 모델과 메커니즘이 제출되고 있다.

본 논문에서는 인터넷에서 VPN을 구성할 때 QoS를 어떻게 적절하게 보장해 줄 수 있는지에 대해 연구해 본다. 2장에서는 인터넷 망 자체의 QoS 요구 사항을 만족시키키 위해 IETF에 제출된 통합

서비스(Integrated Services) 모델[1]과 차등서비스(Differential Services) 모델[2], 그리고 MPLS(Multi Protocol Label Switching)[3]등에 대해 살펴보고, 3장에서는 위에서 제안된 모델 중에서 VPN을 구성하기에 가장 적합한 방식이라고 알려진 MPLS 망에서 인터넷 VPN을 구성할 때 최적의 QoS를 어떻게 보장할 수 있는지에 대해 연구해 보기로 한다.

2. 인터넷 QoS

인터넷 QoS는 네트웍을 통해 전달되는 패킷 플로우의 성능을 나타내는 것으로서 서비스의 가용성, 지연, 지연 변이, 수율, 패킷 손실율 등 몇 가지 성능 인자로 표현된다. 인터넷 QoS의 주목적은 사용자 트래픽에 종단간 QoS를 제공하는 것이다. 인터넷 표준화 기구인 IETF는 인터넷에서 사용자의 요구사항에 따른 QoS를 제공하기 위해 여러 가지 서비스 모델과 메커니즘을 제시하고 있다. 그 중에서 특히 주목받고 있는 것은 통합서비스, 차등서비스, MPLS등인데 아래에서 각각에 대한 개념과 장단점을 살펴본다.

2.1 통합서비스(Integrated Services)

통합서비스 모델에서는 최선형(Best Effort) 서비스 외에 고정된 최대 지연을 요구하는 응용들을 위한 Guaranteed 서비스[4]와 최선형 서비스보다 향상된 성능과 신뢰성을 요구하는 Controlled Load 서비스[5]를 제안하고 있다. 이 모델의 기본은 특정 사용자의 패킷 스트림 즉, 플로우에 특별한 QoS를 제공하기 위해서는 라우터에서 자원 예약이 반드시 필요하며, 이를 위해 라우터에서 각 플로우별 상태(state)를 유지해야 한다는 것이다. 대표적인 자원 예약 신호 프로토콜로는 RSVP(ReSource reserVation Protocol)과 ST-II(STream protcol version II)가 있다.

RSVP는 실시간 서비스와 최선형 서비스를 갖는 다자간 통신을 위한 새로운 인터넷 구조의 한 부분으로, 미리 규정된 서비스를 지원할 수 있도록 송신측, 수신측 그리고 라우터간에 정보를 교환하는 프로토콜로써 ST-II보다 더 많은 주목을 받고 있다. 그 이유는 RSVP는 이질적인 특성을 갖는 수신자를 수용함으로써, 네트워크 자원을 효율적으로 사용하고, 그룹 멤버쉽의 동적 변화에 대응하는 프로토콜의 오버헤드가 작기 때문이다.
(그림 1)은 RSVP의 메시지 흐름을 보여주고 있다.

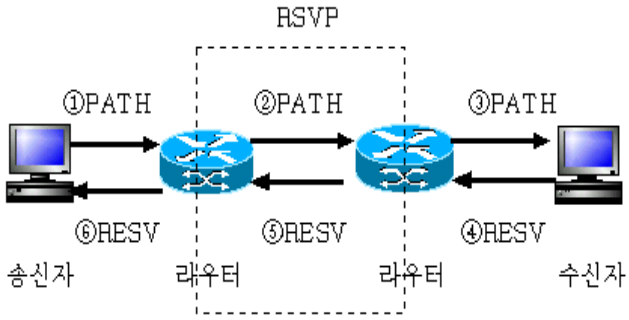

그림 1 : RSVP 신호절차

RSVP는 먼저 송신 호스트가 트래픽 특성을 명시한 PATH 메시지를 수신 호스트에 전송한다. 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 스케쥴과 패킷 분류 기능을 수행하여 사용자의 서비스 요구를 충족시키게 된다.

통합서비스는 크게 4가지 요소로 구성되어 있는데, 자원 요청을 수용할 지를 결정하는 수락제어, 패킷을 분류하여 그 결과에 따라 큐잉하는 분류자(Classifier), 패킷을 스케쥴링하는 스케쥴러(Scheduler), 그리고 자원을 예약하는 신호 프로토콜등이다. 패킷 분류자는 수신된 패킷의 헤더정보(수신자 주소, 프로토콜 타입, 포트번호)를 식별하고, 패킷 스케쥴러는 서비스될 클래스를 결정하며, 수락제어는 QoS 요구사항을 노드가 만족할 수 있을지를 판단하여 연결 여부를 결정한다.

최근 RSVP는 다중화된 플로우의 자원 예약, QoS 요구 사항을 가지는 Explicit Route(ER) 설정 및 다른 기능 등을 위해 여러 방법으로 수정되고 확장되었다. 이런 문제는 IETF에서 매우 활발하게 논의되어지고 있다.

통합 서비스 구조의 문제점은 첫째, 플로우 수가 증가하면 플로우 상태 정보량도 증가하므로, 상태

정보 저장을 위한 방대한 저장공간이 필요하며 이를 관리하기 위한 처리 부하가 증가하게 된다. 따라서 이와 같은 구조는 확장성에 심각한 문제를 야기한다. 둘째, 라우터의 기능 요구 사항이 높다. 모든 라우터는 RSVP, 수락제어, MF 분류(classification), 패킷 스케쥴링 기능을 모두 가지고 있어야 한다. 셋째, Guaranteed 서비스를 위해서는 통합 서비스를 제공하는 라우터가 망 전체에 설치되어야 한다. 이와 같은 단점 때문에 통합서비스는 전체 네트워크보다 지역 네트워크를 구성하는 네트워크 장비에 탑재되어 WAN으로의 대역폭 요청에 사용하는 방향으로 진행되고 있다.

2.2 차등서비스(Differential Services)

통합서비스에서 제안한 RSVP 기술은 단기간 내에 구현이 불가능하고, 공중망으로 도입하기에는 확장성이 부족해서 이를 보안하기 위해 차등서비스가 제안되었다. 차등서비스는 DSCP(Differentiated Service Code Point) 필드에 의해 서비스 수를 제한하고, 패킷의 분류, 마킹, 폴리싱과 쉐이핑을 망 경계 노드에서 수행하고, 코어노드는 BA(Behavior Aggregate) 분류만 수행하여 확장성 문제를 해결한다. 차등서비스는 상대적으로 우선 순위가 높은 패킷을 명시하여 다른 패킷에 비해 더 나은 서비스를 받게 하는 것으로 이를 위해 IP 패킷에 서비스 차등을 위한 우선순위 비트를 두어 네트워크 내의 라우터에서 이를 보고 패킷을 전달할 때 차별화하여 처리하는 개념이다. IPv4 헤더에는 TOS(Type of Service) 필드가 정의되어 있으며, 응용(application)은 작은 지연, 높은 수율, 낮은 손실율등을 나타내기 위해 TOS 필드를 사용하였다. 그러나 기존 라우터에서는 이와 같은 응용의 요구를 거의 무시하고 모든 패킷을 동일하게 처리하였다. 차등서비스는 TOS 필드의 이름을 DS 필드(Differentiated Services Field)로 재명명하여 이를 다시 정의하고, PHB (Per-Hop Behavior)라 불리는 일단의 기본적인 패킷 전송 방법을 정의하고 있다[6]. 차등서비스는 패킷의 DS 필드를 다르게 표시하고, 이 표시에 따라 패킷을 처리함으로써 몇 개의 차별화된 서비스 클래스를 생성하는 것으로써 기본적으로 상대적인 우선순위 기법이다.

차등서비스에서 ISP(Information Service Provider)는 사용자가 원하는 QoS를 제공하기 위해 도메인 내의 각 노드에 클래스별로 자원을 적절히 할당하고, 도메인간에는 종단간 QoS가 보장되도록 SLA(Service Level Agreement)를 맺어야 한다. 이의 기능을 수행하기 위해 BB(Bandwidth Broker) 기술이 제안되고 있다. BB는 도메인에 하나씩 존재한다. 인터 도메인에서는 이웃 도메인의 BB와 SLA를 체결하여 유지하는 기능을 수행하고, 인트라 도메인에서는 사용자나 응용으로부터의 QoS 요구를 받으면, 도메인 내의 자원 사용 정책에 따라 내부자원을 할당하는 기능을 수행한다. 특히 이웃 도메인과 협상된 SLA에 기반하여 경계 라우터의 자원 구성 정보를 제공한다. 정적인 SLA는 한달 혹은 일년 단위로 협상되며, 동적인 SLA를 체결한 가입자는 서비스를 요청하기 위해 신호 프로토콜(예: RSVP)을 사용해야 한다. 각 패킷의 DS 필드 값은 각 종단 호스트에서 가입자에 의해 표시되거나 혹은 MF 구분에 기초하여 leaf 라우터에서 표시 될 수 있다. ISP망의 입구측(ingress) 라우터에서 패킷 구분, 폴리싱, 쉐이핑이 이루어지며, 각 기능은 SLA에서 얻은 규칙에 따르고, 이를 위한 버퍼 크기 역시 SLA에서 유도된다. 한 도메인에서 다른 도메인으로 패킷이 전송되는 경우, 두 도메인간에 맺은 SLA에 따라 DS 필드 값은 재조정될 수 있다. 이와 같은 패킷 구분, 폴리싱, 쉐이핑, 스케줄링에 의해 다양한 서비스가 제공될 수 있으며 제안된 서비스로는 고정된 PBR(Peak Bit Rate) 트래픽을 생성하는 고객과의 SLA 계약을 통해 낮은 지연과 지연변이를 제공하는 Premium 서비스, 고객과 ISP 사이에 SLA 계약을 맺음으로써 ISP가 고객에게 계약된 만큼의 할당 대역폭을 제공하고 Best Effort 서비스보다 높은 신뢰성을 요하는 Assured 서비스, Gold, Silver, Bronze 세 종류의 서비스를 제공하는 Olympic 서비스가 있다. 중요한 사실은 차등서비스는 DS 필드와 PHB 만을 정의하고 있으며 어떤 서비스를 제공할 것인가는 ISP가 결정해야 할 몫이라는 것이다.

차등서비스 구조는 통합서비스 구조에 비해 확장성이 훨씬 좋아 QoS를 제공하기 위한, 인터넷 백본망에서 구현 가능한 방법으로 떠오르고 있다.

2.3 MPLS(Multi Protocol Label Switching)

전통적인 IP 라우팅에서, 각 라우터는 IP 헤더와 네트워크에 대해 라우터가 가진 정보를 바탕으로 포워딩 결정을 내린다. 라우터가 하나의 패킷을 처리하려면 먼저 패킷 헤더를 읽어 각 필드를 검사한 다음 패킷을 처리하는데 이는 라우터의 처리 기능인

라우팅과 포워딩이 각 패킷 단위로 처리됨으로써 많은 시간이 요구된다. 이러한 오버헤드를 줄이기 위해 도입된 방식이 MPLS이다. MPLS는 라벨에 따라 패킷을 포워딩한다. MPLS는 라벨을 사용하여 도메인 내의 한 종단간에 다수의 경로를 설정할 수 있으며, 설정된 경로는 서로 다르고 가변적인 대역폭을 가져, 트래픽의 지연 및 손실 민감도에 따라 차별화된 서비스를 제공할 수 있다.

MPLS는 기존의 라우팅에서 사용하는 longest prefix match 방식 대신 short label exact match 방식을 사용 때문에 간단하고 빠른 패킷의 전달이 가능하다. 기존에는 매 홉마다 패킷에 대한 포워딩 결정을 헤더의 내용과 라우팅 알고리즘에 기반을 두었지만 MPLS에서는 패킷이 망에 들어올 때 한번만 수행한다. MPLS에서 트래픽 전송은 다음과 같이 수행된다.

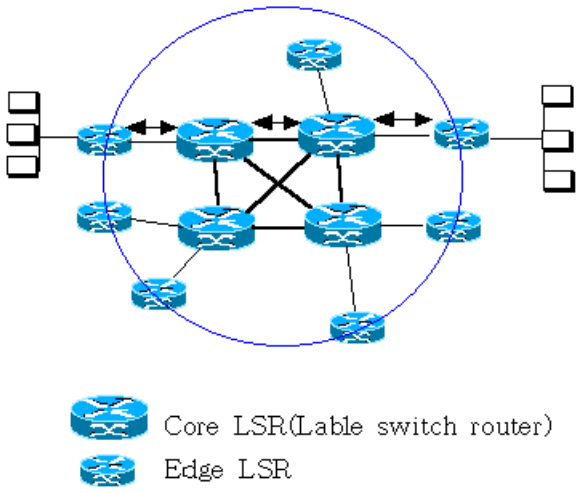

그림 2 : MPLS 작동 원리

서비스 제공자 네트워크 곳곳에 있는 라우터나 스위치가 OSPF, EIGRP, IS-IS와 같은 내부 게이트웨이 프로토콜을 사용하여 참여하는 동안, 네트워크가 자동으로 라우팅 테이블을 구축하게 된다. 에지 장치와 코어 장치 사이의 통신 수단인 LDP(Label Distribution Protocol)는 테이블의 라우팅 토폴로지를 사용하여 인접 장치 사이의 라벨 값을 설정한다. 이 과정에서 수신 엔드 포인트 사이에 LSP(Label Switched Path)가 만들어진다. 그 다음 진입하는 패킷이 에지 LSR(Label switch router)로 들어간다. 에지 LSR은 헤더 정보를 분석하여 사용할 경로를 결정하며, 일치하는 경로가 있으면 이를 패킷에 붙여 전송한다. 코어 LSR은 각 패킷의 라벨을 읽어서 테이블에 나오는 새 라벨로 바꾼 다음 라벨에 의해 지정된 경로를 따라 패킷을 단순히 전송한다. 출구측 Edge LSR이 라벨을 떼어버리고 패킷 헤더를 읽은 다음, 패킷을 최종 수신지로 전송한다. 이는 차등서비스와 유사한 구조를 갖지만, 차등서비스와의 차이는 입구측 노드는 MPLS 헤더를 추가하고, 코어 노드에서 DS필드가 아니라 라벨을 참조하며, 출구측 노드에서 MPLS 헤더를 제거한다는 점이다.

MPLS는 스위치에 의한 고속 IP 포워딩과 다양한 스위치에 적용이 가능하며 IP 멀티캐스팅 지원이 가능하다. 그리고 MPLS는 서로 다른 서비스 특성을 갖는 라벨 스위칭 경로를 생성하게 함으로써 QoS를 지원한다. 또한 MPLS에서 라벨은 국지적인 의미만을 가지므로 대형 네트워크에서는 여러 차례 사용되므로 라벨이 모자랄 가능성은 거의 없다. 이 특징은 규모가 큰 VPN, 트래픽 엔지니어링등과 같은 고급형 IP 서비스를 구현하는데 필수적이다.

3. MPLS 인터넷 VPN

앞에서 논의한 바와 같이 인터넷 백본망에서 QoS를 제공하기 위한 방법으로 차등서비스 모델과 MPLS가 주목을 받고 있는데, 이 두 모델을 이용하여 VPN을 구축하는 방안들이 많이 논의되고 있다. 특히 MPLS는 인터넷 VPN을 구축하는데 다음과 같은 장점들이 있어 이후에도 계속적으로 많은 연구가 이루어질 것으로 보인다. 첫째, MPLS는 주소와 무관하게 포워딩하므로 터널링 프로토콜로 사용할 수 있고, 둘째, ATM, 프레임 릴레이, SONET (Syncronous optical network), WDM(wavelength -division multiplexing)등과 같은 다양한 하부구조와 호환이 가능해서 망 토폴로지의 변화에 따라 VPN을 재구성하기 위한 프로토콜이 없어도 된다. 셋째, MPLS는 원래의 IP 헤더를 감추는 라벨을 쓰기 때문에 사설 어드레스를 쓰는 VPN에 적합하다. 넷째, MPLS 방식으로 구성된 IP(인터넷) VPN은 연결 장치가 없는 네트워크이며 프레임 릴레이나 ATM VC(Virtual Circuit)에 구축된 VPN과 동일한 프라이버시 보호 기능을 제공한다. 따라서, 이번 장에서는 기존에 제안된 MPLS망에서 인터넷 VPN을 제공하는 방식에 대해 간략히 살펴보고, MPLS 인터넷 VPN에서 어떻게 QoS를 보장할 수 있는지에 대해 논의해 보고자 한다.

3.1 MPLS VPN의 동작 방식[7],[8],[9]

기존에 제안된 MPLS VPN의 정보를 분배하는 방식은 다음과 같이 요약된다. 사용자 사이트와 코어망 사이의 VPN 정보 분배 방식은 사용자 사이트가 ISP의 MPLS에 참가하는 경우에는 바인딩된 라벨 및 VPN 전송 경로를 BGP(Border Gateway Protocol)에 실어 전송하게 되고, MPLS에 참여하지 않는 경우에는 라벨에 대한 정보없이 BGP에 실어 정적으로 분배하게 된다. 그리고 코어망에서의 VPN 정보 분배 방식은 OSPF와 LDP를 이용하게 되는데, OSPF는 라우팅 정보를 전송하고 LDP는 라벨을 전송하게 된다. BGP를 이용해서 라벨과 라우팅 정보를 동시에 전송할 수도 있다.

3.2 MPLS VPN의 QoS 보장 방법

아래 그림[10]은 MPLS망에서 구성된 IP(인터넷) VPN이다.

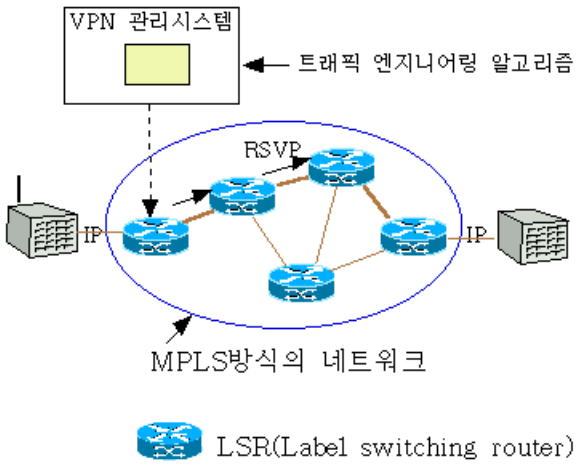

그림3 : MPLS 방식의 VPN

SLA에서 지정한 정책들과 DS-byte의 값들은 각각 IP 헤더에 들어 있는데 이들이 특정한 트래픽 스트림이 요구하는 QoS를 결정한다. VPN 관리 시스템의 트래픽 엔지니어링 알고리즘은 네트워크 자원을 적절히 사용해서 트래픽의 경로를 결정하는데 사용된다. VPN 관리 시스템은 입구나 출구 에지 노드에 설립할 경로와 요구된 QoS 파라미터들을 지시한다. 그 다음에 지정된 경로에 있는 모든 노드들은 요구된 QoS를 보장하기 위해 자원 예약(resource reservation)이 필요함을 알리는데 이때 MPLS 라우팅이 필요하다. 에지노드는 VPN 관리 시스템이 지정한 경로상의 다음 노드에 QoS 파라미터를 포함한 RSVP 메시지를 보내게 된다. MPLS 방식의 IP-VPN에서 각 노드들은 요구된 QoS가 보장되도록 디자인된 IP 스위치이거나 라우터여야 한다.

QoS는 장치 관련 기능이 아니라 완벽한 시스템 구조라 할 수 있다. MPLS 방식 IP VPN을 구성함에 있어서도 네트워크 전체에서 확장성이 있고 미디어 독립적인 서비스를 제공할 수 있도록 상호 작용을 하는 다양한 기술들과 전체 시스템 수준의 성능을 모니터할 수 있는 기능은 필수적이다. 위의 모델에서도 QoS가 보장되도록 디자인된 IP 스위치와 MPLS 라우팅, 트래픽 엔지니어링 알고리즘등을 적절히 사용해서 QoS가 보장되도록 했다.

4. 결론

본 논문에서는 인터넷을 이용해서 통신비용 절감과 접속 영역의 확장 및 신뢰적인 데이터 통신이 가능하도록 하는 IP(인터넷) VPN을 구축할 때 필수적으로 고려해야 하는 QoS에 대해 논의했다. IETF에서 인터넷 QoS를 위해 제안한 여러 모델과 메커니즘 중에서 통합서비스 모델과 차등서비스 모델 및 MPLS에 대해 살펴보았다. 그리고 마지막으로 VPN을 구축하기에 많은 장점을 가지는 MPLS 망에서 설계된 인터넷 VPN에서 QoS가 어떻게 보장되는지 검토해 보았고 QoS가 지원되도록 디자인된 라우터나 IP 스위치, 트래픽 엔지니어링 알고리즘등을 적절히 사용해야만 최적으로 보장됨을 논의했다.

이후에는 이상과 같은 연구를 바탕으로 QoS가 보장되는 MPLS VPN에 대한 설계 및 구현에 대한 연구를 할 것이다.

참고문헌

[1] R.Braden, D.Clark, and S.Shenker, "Intergrated Services in the internet Architecture: An Ovierview." RFC1633, June 1994.

[2] Y.Bernet, J.Binder, S.Blake, M.Carson, B.E.Carpenter, S.Keshav, E.Davies, B.Ohlman, D.Verma, Z.Wang, and W.Weiss, "A Framework for Differentiated Services," Internet Draft, February, 1999.

[3] Eric C. Rosen, "Multiprotocol Label Switching Architecture," Internet Draft, February 1999.

[4] S. Shenker, C. Partidge, and R. Guerin, "Specification of Guaranteed Quality of Service," RFC2212, September 1997.
[5] J. Wroclawski, "Specification of the Controlled-Load Network Element Service," RFC2211, September 1997.
[6] K. Nicholas, S. Blake, F. Barker, and D. Black, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers," RFC 2474, December 1998.
[7] D.jamieson, B.jamoussi, G.Wright, and P.Beaubien, "MPLS VPN Architecture," Internet Draft, August 1998.
[8] Juha Heinanen, "VPN support with MPLS," Internet Draft, March 1998.
[9] 정윤희, 최희숙, 손승원, "인터넷 VPN 제공 기술 및 동향에 대한 연구," ETRI 주간기술동향 918 호, 1999년 5월.
[10] Peter B.Busschbach, "Toward QoS-Capable Virtual Private Networks," Bell labs Technical Journal, October-December 1998.