이동성을 갖는 MPLS VPN에서의 QoS

송영필* · 양해권**
*군산대학교 대학원 정보통신공학과, **군산대학교 정보통신공학과 교수

QoS for Mobile MPLS VPN

Youngpil Song* · Haekwon Yang*
School of Electronic & Information Eng., Kunsan National Univ.*

요 약

가상사설망(VPN)은 공공 네트워크를 자신의 사설망처럼 사용할 수 있다. 생산성 향상과 비용절감 효과를 기대할 수 있지만 네트워크 제공자는 관리가 복잡하고 터널링 및 암호화에 따른 오버헤드를 감수해야 한다. 그러나 MPLS VPN은 각 VPN에 별도의 ID를 부여하여 터널링이 주는 추가의 오버헤드와 네트워크 주소 변환이 필요 없는 효율적인 VPN을 제공할 수 있다. 본 논문에서는 CE(customer edge) 라우터를 기반으로 노드가 이동하는 경우에 따른 프로토콜을 기술하고 이에 대한 QoS 지원방안을 제시한다.

ABSTRACT

The term "VPN", or Virtual Private Network, generally means the public network of vendors which is *providing a communication net and other network using WWW as a backbone of its WAN.* the existing VPN is expected to reduce expenses and will improve the productivity, however, the network provider should accept the management complexity and the overhead after tunneling and encryption. But MPLS VPN can provide efficient VPN which would not need the address transformation and the additional overhead made by tunneling after giving separately ID. This paper describes the protocol for MPLS VPN which is about a node that moves based on Customer Edge (CE) router and supports a scheme for QoS.

키워드
MPLS VPN, QoS, SLA, CR-LSP, ER-LSP

Ⅰ. 서 론

지금까지의 기업들은 지사나 영업소 또는 이동 근무자가 지역에 관계없이 업무를 수행할 수 있도록 통신사업자에게 점대점 기반의 전용회선을 임대하여 원격지까지 연결하는 방식으로 사설망을 확대하였다. 이렇게 구성하는 사설망은 각종 통신망 장비와 소프트웨어 투자에 초기비용이 많이 소요될 뿐만 아니라 회선 요금도 비싸고 통신망을 운영하고 관리하는 데에도 많은 인적·물적 자원이 필요하다. 이와 같은 기존 사설망의 고비용과 비효율적인 관리를 해결하기 위한 방법으로 인터넷 망을 마치 전용선으로 사설망을 구축한 것처럼 사용하는 방식이 대두하게 되었는데 이를 가상 사설망(Virtual Private Network, VPN)이라 한다.[1]

이러한 VPN을 제공하기 위한 기술 중에서 최근 각광을 받고 있는 기술 중에 하나가 MPLS (MultiProtocol Label Switching) VPN이다. MPLS의 레이블(label)을 이용하여 서로 다른 VPN 간에 트래픽을 격리시켜 효율적인 패킷 전송을 하는 것이 MPLS VPN 기술의 핵심이며, 이를 간단히 MPLS VPN이라 한다. MPLS VPN은 기존의 IP VPN(internet protocol VPN) 방식의 단점인 터널링(turnneling)이 주는 추가의 오버헤드, 암호화 기법, 복잡한 관리 등과 같은 문제점을 VPN ID(identification)를 부여하여 터널링 없는 가상공간 할당으로 IP VPN의 이러한 문제점들을 해결하고 높은 확장성, 효율적인 비용, 그리고 사용자가 요구한 다양한 QoS(Quality of Service)를 제공하여 IP VPN에 비해 낮은 비용으로 서비스를 제공하게 된다.

본 논문에서는 VPN의 모든 정보를 PE(provider edge) 라우터가 유지 관리하여 VPN 사이트의 추가 혹은 삭제가 PE 라우터에게 많은 부담을 주게 되어 상대적으로 확장성이 떨어지고 보안에 관한 요구사항이 많은 PE 라우터 기반 MPLS VPN이 아닌 사용자의 다양한 요구사항을 만족할 수 있는 CE(customer edge) 라우터 기반 MPLS VPN에서 이동성을 지원하는 프로토콜을 기술하고 QoS 지원방안을 다루고자 한다. 2장에서는 이동성을 지원하는 MPLS VPN의 전체적인 구조와 인터페이스를 기술하였으며, 3장에서는 MPLS 트래픽 엔지니어링을 이용한 MPLS VPN에서의 QoS 지원방안을 제시하였다. 끝으로 4장에서는 결론 및 향후과제를 기술하였다.

II. 이동성을 지원하는 MPLS VPN

1. 기존의 VPN 방식

VPN이란 특정 사용자 집단 내에서 다른 사용자로부터 폐쇄된 통신서비스를 보장하는 기술이다.[2] VPN 서비스의 핵심은 완벽한 보안 환경을 제공하는데 있으며 이를 제공하지 못한다면 VPN 서비스로서의 의미를 가질 수 없다. 이처럼 보안 기능은 VPN 서비스의 가장 중요한 요소이다. VPN의 보안 기능을 가능케 해주는 기술로는 크게 터널링 기술과 암호화 기술을 꼽을 수 있다. 터널링은 시작지점에서 목표지점까지 터널을 형성한다는 의미로서 인터넷 네트워크 상에서 외부의 영향을 받지 않는 가상적인 터널을 형성해 정보를 주고받는다는 뜻이고 이를 기술적으로 풀어보면 네트워크상의 터널과 관련해 상호 약속된 프로토콜로 세션을 구성하고 이 터널은 다른 사용자로부터 보호를 받는다는 것이 터널을 구성하는 중요한 목적이다.

이러한 터널링 기법은 다시 터널이 형성되는 계층과 터널이 시작되는 포인트에 따라 구분할 수 있다. 터널이 형성되는 계층은 크게 2계층 터널링과 3계층 터널링으로 구분할 수 있다. L2F(Layer 2 Forwarding), PPTP(Point-to-Point Tunneling Protocol), L2TP(Layer 2 Tunneling Protocol)는 2계층의 연결을 이용하는 방식이고 IP/IP(IP in IP), GRE(General Routing Encapsulation), IPSec (Internet Protocol Security)는 3계층의 연결을 이용하는 방식이다.[3]

이러한 기존의 VPN 방식은 터널링이 주는 추가의 오버헤드, 암호화 기법, 복잡한 관리 등과 같은 문제점을 내포하고 있지만 MPLS VPN 방식에서는 LSP(Label Switched Path)를 설정하고 VPN ID를 부여하여 터널링없는 가상공간 할당으로 레이블 처리되므로 기존의 VPN 방식의 단점인 터널링이 주는 추가의 오버헤드 없이 원격지 사용자들과 사무소가 마치 본사의 네트워크에 직접 연결되듯이 시내 전화로 ISP(Internet Service Provider)의 네트워크에 연결할 수 있으며, 네트워크 관리자의 복잡한 관리도 해결할 수 있고 FEC (Forwarding Equivalence Class)의 설정에 따라 QoS나 보안 등 다양한 서비스의 제공도 가능하게 된다.

2. CE 라우터 기반 MPLS VPN

MPLS란 현재 IETF에서 표준화가 진행 중에 있는 IP패킷의 전송방식이다. MPLS라우터는 IP패킷을 FEC로 분류하고 각 FEC에 짧고 고정된 길이의 레이블을 부착하여 이후의 모든 라우터가 이 레이블을 기준으로 간단하고도 빠른 패킷전송을 지원하는 기술이다.[4]

현재 MPLS VPN 중에서 RFC2574 "BGP/MPLS VPN"이 MPLS VPN의 표준으로 정립되고 있지만 "BGP/MPLS VPN"에서 제시된 모델은 ISP의 네트워크에 기반한 MPLS VPN의 구성방안으로서, PE 라우터가 VPN의 모든 정보를 유지 관리함에 따라 VPN 사이트의 추가 혹은 삭제에 의한 토폴로지(topology) 변화가 PE 라우터에게 많은 부담을 주게 되므로 VPN 시스템의 확장성이 상대적으로 떨어지고 보안에 관한 요구사항이 늘어나 유연성을 보장하기가 어렵다.

CE 라우터 기반 MPLS VPN에서 CE 라우터는 두 개의 테이블을 관리하는데 하나는 VPN mem -ber caching 테이블로써 VPN 멤버쉽 정보만을 저장한 이 테이블은 같은 VPN에 속한 상대 CE 라우터와 편리하게 BGP(Border Gateway Protocol) peer를 유지하기 위해 사용되고, BGP는 이 테이블에 저장된 상대 CE 라우터의 주소를 사용하여 수행한다. BGP를 수행하면서 상대 CE 라우터로부터 전송된 VPN의 정보는 CE 라우터에서 관리하는 또 하나의 테이블인 VPN 라우팅 테이블에 저장된다.[5]

PE 라우터의 경우는 VPN 멤버쉽 정보를 관리하기 위한 VPN 정보 테이블을 갖는데 이 테이블에는 CE 라우터로부터 받은 VPN 정보와 다른 PE 라우터로부터 받은 VPN 멤버쉽 정보만을 저장하여 ISP(internet service provider) 네트워크에서의 VPN 수행 부담을 덜어준다.

3. 이동성을 지원하는 CE 라우터 기반 MPLS VPN

CE 라우터 기반 MPLS VPN에서 이동성을 지원하기 위해서 CE 라우터는 VPN 서비스를 지원하기 위한 구성요소와 이동 서비스 지원을 위한 에이전트 기능(홈 에이전트, 외부 에이전트, 대응 에이전트)을 포함해야 한다. 참고문헌[6]에서는 이동 노드가 동일 VPN 내의 사이트로 이동하는 경우, 다른 VPN 내의 사이트로 이동하는 경우 그리고 일반 인터넷 지역으로 이동하는 경우에 따른 프로토콜을 제안하였다.

이동 노드가 처음으로 외부 에이전트에 의해 관리되는 MPLS VPN 사이트를 방문할 때, 이동 노

드는 외부 에이전트가 실행되는 라우터로부터 AA(Agent Advertisement) 메시지를 최초로 수신한다. AA 메시지에 'VPN Information' Extension을 추가하여 전송하고 이동 노드는 'VPN Infor-mation' Extension을 통하여 이동 지역을 판별한다. 만일, 이동 노드가 수신한 AA 메시지에 'VPN Information' Extension이 포함되지 않았다면 이는 일반 인터넷 지역으로 이동했음을 의미한다.

AA 메시지를 수신한 이후에, 이동 노드는 이동한 사이트의 주소영역이 자신의 주소영역과 동일한지를 검사하고 동일하다면 주소 충돌을 방지하기 위해 Co-located Care-of-Address를 할당받은 후에 등록 절차를 수행하고 동일하지 않다면 외부 에이전트의 Care-of-Address를 사용하여 등록 절차를 수행한다. 등록 절차는 이동 노드가 등록 요청 메시지를 외부 에이전트에 보내면 외부 에이전트는 홈 에이전트로 이 등록 요청 메시지를 전달한다. 패킷의 무결성과 인증을 거친 후에 홈 에이전트는 등록 응답 메시지를 갖고 외부 에이전트에게 응답한다. 그런 다음 외부 에이전트는 등록 요청을 보낸 이동 노드에게 등록 응답을 반환한다.

III. QoS 지원 방안

1. MPLS 트래픽 엔지니어링

MPLS 트래픽 엔지니어링 기술은 MPLS 망 내에 서비스 요구나 망 사업자의 자원 사용 정책을 반영한 traffic-engineered path를 설정하고, 입력단에서 MPLS 망으로 유입되는 트래픽을 특성에 따라 분류하여 적절한 LSP로 분배해 주는 메커니즘을 바탕으로 한다. MPLS 트래픽 엔지니어링의 핵심기술은 크게 서비스 품질 요구사항을 만족하는 경로를 찾는 경로 선택(Constraint-based routing) 기능, 찾아낸 경로를 따라 자원을 예약하기 위한 시그널링 기능, 패킷 입력단에서의 트래픽의 종류에 따라 트래픽 흐름을 최적으로 분류 및 적정 경로로의 패킷 분배, 각 노드에서의 트래픽 전달시의 큐잉 제어, 네트워크 상태 변화에 따른 지속적인 re-optimization 기능 등으로 구성된다.[7]

2. QoS 지원 메커니즘

QoS를 지원하기 위해서 우선 가입자는 망 사업자와 서비스 사용 등급에 대한 계약(SLA, Service Level Agreement)을 맺는다. 계약 내용에는 서비스의 종류, 서비스별 요구 품질(요구대역, 지연, 지연변이, 손실 등)을 포함한다. 서비스 계약이 이루어지면 SLA와 망사업자의 자원 사용 정책을 고려하여, 계약 내용을 만족시킬 수 있는 경로(Constraint Routed Path)를 찾는다. CR-LDP나 RSVP-TE와 같은 시그널링 프로토콜을 이용하여 Explicit Routed LSP를 설정한다. MPLS 망으로 유입되는 트래픽에 대해 트래픽 특성과 SLA를 고려하여 IP 패킷을 분류한 다음 적합한 LSP 혹은 ER-LSP로 분배한다. Traffic engineered path에 대해서는 지속적으로 계약된 성능을 만족시키는 지를 감시하고, 필요시에는 재라우팅이나 대역폭 증감과 같은 re-optimization을 지속적으로 수행한다.[7]

트래픽 제어 서버는 SLA 프로파일, QoS 정책, LSP별 품질정보, QoS 메트릭(metric)과 같은 트래픽 엔지니어링 데이터베이스를 총괄 관리하고, 이를 이용하여 경로 계산, 부하 분산, 재 라우팅 등의 엔지니어링 제어 기능을 네트워크 전반에 대해 수행한다.

LSR(Label Switching Router)은 Traffic Engi-neered MPLS 기능을 위해 추가적으로 QoS 라우팅 프로토콜, MPLS 시그널링 프로토콜이 추가되며, 입력단에는 패킷 분류 및 전송 기능이 추가된다.

Constrained 라우트를 찾아내기 위해서는 온라인 경로계산 방법을 이용한다. 온라인 경로계산은 QoS 라우팅 프로토콜을 이용하여 QoS 메트릭을 수집 분배하고, 이를 이용하여 특정 제한 사상을 만족시키는 경로를 찾는 알고리즘으로 구성된다. QoS 메트릭은 링크 총 대역폭, 예약된 대역폭, 예약 가능한 대역폭, 전달지연 등 네트워크의 최신 상태에 대한 정보로 구성된다. 사용자 제한 사항은 요구 대역폭, 허용 가능 최대 홉 수, 설정 및 유지 우선순위, 링크 운용 관리 정보 등 가입자나 운용자의 자원사용에 대한 제한 사상을 포함한다.[8]

그림1은 온라인 Constrained-based 라우팅 기능의 동작을 전체적으로 보여준다. 확장 IGP 프로토콜은 기존의 네트워크 토폴로지 정보와 확장된 트래픽 엔지니어링 데이터베이스를 수집, 분배하고, CSPF 알고리즘은 사용자 제한 사상을 반영하여 최적 경로를 명시적으로 결정한다. 경로가 결정되면 ER-LSP 설정을 지원하는 시그널링 프로토콜을 이용하여 입력단 LSR에서 출력단 LSR까지 경로가 설정된다.

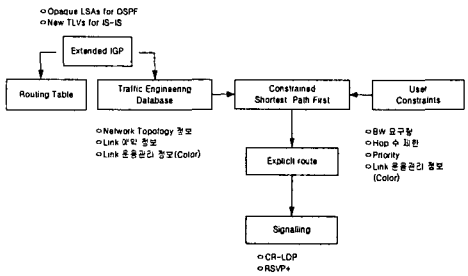

그림 1. Constrained-based Routing 기능

시그널링 프로토콜로써 CR-LDP는 LSP 설정 메시지 내에 explicit 라우트 정보와 트래픽 파라메터를 전달할 수 있도록 LDP를 확장한 프로토콜로서, TCP를 이용하여 시그널링 메시지를 교환한다. ER-LSP 설정은 그림2에서처럼 미리 결정된 경로

를 따라 레이블 요구 및 레이블 매핑 메시지를 한 바퀴 교환함에 따라 이루어진다. 일단 ER-LSP 경로가 결정되면 시그널링 프로토콜을 이용하여 해당되는 노드들간에 연결을 설정한다. MPLS 시그널링 프로토콜은 레이블의 분배, explicit 라우트 정보의 전달, 대역폭을 포함한 트래픽 파라메터의 전달 및 우선순위와 같은 연결 설정에 필요한 부가적인 정보들을 인접 노드들간에 전달하는 역할을 한다.[9]

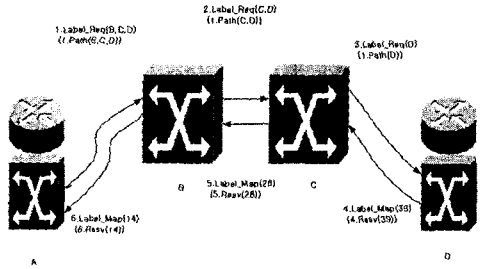

그림 2. CR-LDP 및 RSVP-TE의 연결설정과정

QoS 패킷의 분류 및 전달 기능은 입력단 LSR의 전송 엔진에서 이루어진다. 입력단 LSR의 전송 엔진에서는 유입되는 IP 패킷 헤더의 정보를 이용하여 가입자와 서비스 종류에 따라 FEC(Forwarding Equivalence Class)로 세분화한다. 분류된 트래픽은 종류별로 측정되고, SLA와 운용자 정책을 고려하여, 계약 범위 안에서 트래픽 특성에 따라 레이블과 PHB(per hop behavior)가 결정되고, 버퍼링을 거쳐서 다음 노드로 전송한다. 그림3에서 QoS 패킷의 분류 및 분배 기능을 나타낸다.

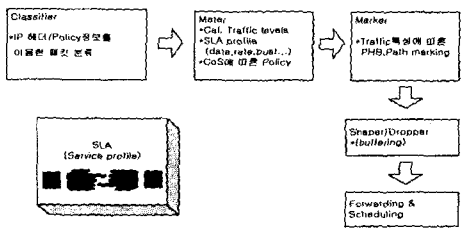

그림 3. QoS 패킷으로의 분류 및 분배 기능

3. 적용

이동성을 지원하는 MPLS VPN에서의 QoS 지원을 위해 MPLS 트래픽 엔지니어링을 이용하였고 전체적인 구성은 그림4와 같다.

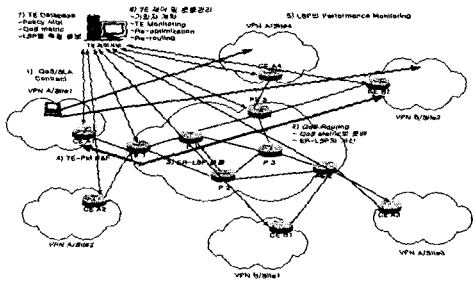

그림 4. 트래픽 엔지니어링을 이용한 QoS 지원

Ⅳ. 결 론

본 논문에서는 이동성을 지원하는 MPLS VPN에서의 트래픽 엔지니어링을 이용한 QoS 지원 방안을 제시하였다. 트래픽 엔지니어링 기술을 이동성을 지원하는 MPLS VPN에 이용함으로써 가입자는 고품질의 VPN 서비스를 제공받을 수 있고 사업자는 수익성과 한정된 네트워크 자원을 효율적으로 운용할 수 있을 것으로 전망된다. 하지만 실제 망에 이를 적용하기 위해선 트래픽 엔지니어링 기술에 대한 기술적 보완이 필요하다. 즉, QoS 지원이 가능한 CR-LSP를 찾기 위한 QoS 라우팅 및 알고리즘, Policy Server, 응용이나 가입자 특성에 따라 VPN 패킷의 CoS(class of service) 등급을 구분하는 패킷 룩업 기술 및 MPLS 망에 대한 모니터링과 최적화 기술 등에 대해 좀 더 많은 연구가 있어야 할 것이다.

참고 문헌

[1] Hamzeh K., et al, "Point-to-Point Tunneling Protocol," draft-ietf-pppext-12tp-16.txt, Apr., 1999.

[2] Ferguson P., Huston G., "What is a VPN," The Internet Protocol Journal, Vol. 1, No. 2, Sep., 1998.

[3] Perkins E., "IP Encapsulation within IP", RFC 2003, Oct., 1996

[4] Eric C. Rosen, Arun Viswanathan, Ross Ca -llon, "Multiprotocol Label Switching Archi -tecture," draft-ietf-mpls-arch-02.txt, IETF, Jul., 1998.

[5] 한민호, 이영석, 최 훈, 전우직, "CE 라우터 기반 MPLS VPN 설계 및 구현," 제 27회 한국정보과학회 추계학술대회, Vol. 21, No. 2, pp.251-253, 2000년 10월

[6] 이영석, 최훈, "이동성을 지원하는 MPLS 방식 가상사설망," 한국통신학회논문지, Vol. 26, No. 12C, pp.225-232, 2001년 7월

[7] Daniel O. Awduche, "MPLS and Traffic Engineering in IP Networks Using," IEEE

Communications Magazine, Dec., 1999
[8] 양선희, 정민영, 이유경, "MPLS 트래픽 엔지니어링에 의한 인터넷 품질제어기술," 한국통신학회지 Vol. 17, No. 9, pp. 66- 76, 2000년 9월
[9] Ash J., Girish M., Gray E., Jamoussi,B. and G. Wright, "Applicability Statement for CR-LDP", RFC 3213, Jan., 2002.