

---

# 이동 MPLS VPN에서의 QoS 지원 방안

이영석\* · 양해권\*

## QoS Support Mechanisms in Mobile MPLS VPN

Young-seok Lee\* · Hae-kwon Yang\*

---

이 논문은 2004년도 군산대학교 학술연구비의 지원에 의하여 연구되었음

---

### 요 약

MPLS(Multiprotocol Label Switching)를 이용한 네트워크 기반 VPN(Virtual Private Network)은 PE(Provider Edge router) 기반 MPLS VPN으로도 불리우며, 고수익을 원하는 사업자와 저비용을 요구하는 고객 모두에게 인트라넷(Intranet)과 엑스트라넷(Extranet)을 위한 해결 방안으로서 도입되고 있다. 본 연구에서는 BGP-E(BGP multiprotocol Extension)를 이용한 PE 기반 MPLS VPN을 대상으로, VPN 사이트 내에 속한 단말이 다른 사이트로 이동하더라도 계속 VPN 서비스를 받을 수 있게 하는 MPLS VPN 구성 방안과 QoS를 지속적으로 제공할 수 있는 방안을 제안한다. MPLS VPN 서비스와 Mobile IP에 의한 이동서비스를 지원하기 위한 메커니즘을 백본 네트워크 내의 PE(Provider Edge) 라우터 상에 설계한다. VPN 사이트 내에 속하는 어떤 노드가 기존의 통신을 유지한 상태로 다른 사이트로 이동할 때, 이동 노드와 통신하고자 하는 대응 노드가 속한 VPN 사이트와 연결된 PE 라우터는 이동을 통보 받고 단말이 이동한 곳으로 새로운 MPLS 경로를 설정한다. PE 라우터에 Mobile IP 프로토콜과 연동하는 VPN 관리 방식 및 라우터 제어 기능의 성능 분석을 위해 COVER 도구를 이용하여 시뮬레이션을 수행하고 결과를 분석한다.

### ABSTRACT

Network based VPN(Virtual Private Network) using MPLS(Multiprotocol Label Switching) technology, called PE(Provider Edge router) based MPLS VPN, is regarded as a good solution for intranets or extranets because of the low cost and the flexibility of the service provision. In this paper, we describe a mechanism that allows the VPN users to move from one site to another site of the VPN network based on the BGP-E MPLS technology. This mechanism is designed for PE(Provider Edge) routers of the backbone network. PE routers connected to the VPN sites establish a new MPLS path to the mobile node after they detect movement of the mobile VPN node. The new location may belong to the same VPN or to different VPN. We designed VPN management and control functions of the PE routers in order to interface with the Mobile IP protocol and support the QoS mechanism. The pilot implementation and performance measurement were carried out on a simulation using COVERS tool.

### 키워드

MPLS, VPN, Mobile IP, QoS

## I. 서론

지금까지의 기업들은 지사나 영업소 또는 이동근무자가 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 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 핵심이다. MPLS VPN은 기존의 IP VPN(Internet Protocol VPN) 방식의 단점인 터널링(tunneling)이 주는 추가의 오버헤드, 암호화기법, 복잡한 관리 등과 같은 문제점들을 VPN ID(identification)를 부여하여 터널링 없는 가상공간 할당으로 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 [2][3][4].

본 논문에서는 MPLS VPN에서의 이동성 지원 및 QoS 제공 방안에 관한 연구로서 다양한 MPLS VPN 구성 방식 가운데 네트워크 기반 MPLS VPN 혹은 PE 기반 MPLS VPN으로 불리우는 MPLS VPN을 대상으로 하여 VPN 사이트내의 어떤 노드가 다른 사이트로 이동하는 경우 기존의 VPN 서비스를 지속하기 위해 Mobile IP 및 경로 최적화(route optimization) 프로토콜을 확장하여 이동 엔티티 기능을 설계하였고 MPLS VPN에서 이동 노드에 대한 QoS를 제공하기 위한 새로운 모델을 제시한다.

현재 인터넷은 QoS보장과 확장성에 그 초점이 맞춰져 있으며, 그 중에 QoS보장은 트래픽 엔지니어링(Traffic Engineering)과 관련이 있다. 기존의 라우팅 관점에서는 사용자의 서비스 요구가 있을 때 가장 최적의 경로(Shortest Path)를 검색하는 것이 목적이었지만 QoS를 보장하는 라우팅은 사용자의 요구에 적합한 경로를 검색하

여 연결한다. 즉, QoS보장은 망의 활용도를 높이고 망의 효율적인 사용을 지원하는 것이다.

본 논문의 구성은 다음과 같다. 2장에서는 MPLS VPN의 기본적인 구조와 그에 따른 제공방안과 제어요소 및 동작절차를 간단히 설명하였고, 3장에서는 PE 기반 MPLS VPN에서의 이동 서비스를 제공하기 위한 메커니즘을 기술하였다. 4장에서는 이동성을 지원하는 PE 기반 MPLS VPN에서의 QoS 지원을 위한 기술적인 내용을 다루었다. 5장에서는 시뮬레이션 도구인 COVERS를 이용하여 이동성을 지원하는 PE 라우터 기반 MPLS VPN에서의 QoS 지원을 위한 모델의 구현 및 성능 분석을 하였고, 6장에서는 결론을 기술한다.

## II. MPLS VPN의 구성

MPLS 기반의 VPN은 IP 터널링 기반의 VPN에서 제공하기 어려운 QoS나 보안 등을 제공하는 장점이 있다. 또한, MPLS VPN은 높은 확장성, 효과적인 비용, 그리고 사용자 요구의 광범위한 핸들링을 제공하여 IP 서비스를 낮은 비용으로 제공해 준다. MPLS는 이와 같은 이점을 바탕으로 VPN을 구성하기 위한 최적의 방안으로 간주되고 있다.

VPN은 크게 CPE(Customer Premise Equipment)-based VPN과 Network-based VPN으로 나뉜다[5]. CPE 기반 VPN에서는 VPN을 위한 동작 메커니즘이 각 CPE에 구현되는 방식이며, Network 기반 VPN에서는 서비스 제공자의 백본 네트워크에 구현된다. 만일 MPLS를 Network 기반 VPN을 위한 터널링 메커니즘으로 사용한다면, Network 기반 VPN의 백본 네트워크를 MPLS 네트워크로 하여 같은 VPN에 속하는 사이트 간에 LSP를 활용하여 연결하는 것을 의미한다.

MPLS VPN은 그림 1과 같이 PE(Provider's Edge device), P(Provider's device), CE(Customer site's Edge device) 등의 요소로 구성된다. P와 PE는 서비스 제공자의 백본 네트워크에 속해 있고 CE는 고객 사이트 내에 속해 있다. CE는 스위치나 라우터일 수도 있다. 고객 사이트의 백본 네트워크 접속은 CE와 PE 간의 링크를 통해서만 가능하다. P는 VPN을 위한 별도의 기능을 갖지 않고 VPN에 관한 정보도 따로 유지하지 않는데, 이는 MPLS VPN의 확장성을 위한 핵심적 요소이다. PE에는 입력되는 패킷을

VPN에 따라 구분하여 포워딩하는 기능이 포함된다. 이 기능은 백본 네트워크 내에 VPN 별로 폐쇄 사용자 그룹(Closed User Group)을 정의하기 위해 필수적이다.

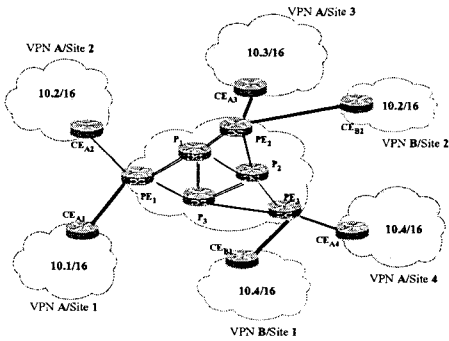


그림 1. MPLS VPN의 구조  
Fig. 1 MPLS VPN Architecture

네트워크 기반 MPLS VPN은 PE 간에 VPN 사이트들의 도달성 정보와 멤버십(membership) 정보를 전달하여 VPN을 구성하는 방식이다. 이에 반해 CPE 기반 MPLS VPN은 CE와 PE 간에 도달성 정보를 전달하고 CE 간에 멤버십 정보를 교환하여 VPN을 구성하는 방식이다. 본 논문에서는 네트워크 기반 MPLS VPN을 PE 기반 MPLS VPN이라 칭하고, CPE 기반 MPLS VPN을 CE 기반 MPLS VPN이라 부르기로 한다.

PE 기반 MPLS VPN은 BGP-E를 이용하여 VPN 사이트들에 대한 도달성 정보와 멤버십 정보를 전달하는 방식이다[6]. 다시 말해서, PE 간에 VPN을 위한 라우팅 정보를 분배할 때 VPN 멤버십 정보도 함께 실어 보내는 piggybacking 방식이다. BGP-E의 원조인 BGP4는 AS (Autonomous System) 간에 라우팅 정보를 교환하기 위한 프로토콜로서 IPv4 형태의 라우팅 정보만을 다룰 수 있다. BGP4를 IPv6 혹은 IPX를 비롯한 다양한 형태의 라우팅 정보도 교환할 수 있도록 확장한 것이 BGP-E이며, PE 기반 MPLS VPN에서는 "VPN-IPv4" 형태의 라우팅 정보를 교환한다.

CE 라우터 기반의 MPLS VPN[7]에서는 VPN 사이트에 속한 CE 라우터에 VPN을 수행하기 위한 기능이 추가되지만, PE 라우터는 VPN 서비스를 위한 최소한의 VPN 정보만을 갖고 있게 된다. 따라서, PE 라우터와는 별도로 같은 VPN 사이트에 속한 CE 라우터 간의 연결성이 제공되며 망사업자 네트워크 기반의 MPLS VPN에 비해 독립성 보장 등 많은 장점을 갖게 된다.

### III. MPLS VPN에서의 이동서비스 지원

본 논문에서는 현재 활발히 상용화 작업이 진행된 PE 기반 MPLS VPN을 대상으로 하여 VPN 사이트 내의 노드에 대한 이동 서비스 지원 방안과 QoS 제공 방안을 고려한다. VPN 사이트 내의 어떤 노드가 같은 VPN 내의 다른 사이트로 이동하는 경우와 다른 VPN 내의 사이트로 이동하는 경우에서 모두 기존의 VPN 서비스를 지속하면서 QoS를 제공하는 프로토콜을 제안하고 구현한다.

PE 기반 MPLS VPN에서 이동 서비스 지원을 위해 Mobile IP[8][9]에서 제시된 이동 엔티티, 즉 홈 에이전트(HA: Home Agent), 외부 에이전트(FA: Foreign Agent) 이외에 경로 최적화[10]를 위해 참고문헌[11]에서 제안된 새로운 형태의 이동 엔티티(대응 에이전트)를 도입한다. 대응 에이전트(CA: Correspondent Agent)는 이동 노드와 통신하고자 하는 대응 노드(Correspondent Node)가 위치한 VPN 사이트에 연결된 PE 라우터 상에서 수행된다. 망사업자의 Edge 라우터인 PE 라우터는 VPN 서비스를 지원하기 위한 구성 요소와 이동 서비스(Mobile IP) 지원을 위한 에이전트 기능(홈 에이전트, 외부 에이전트, 대응 에이전트)을 모두 포함해야 한다.

#### 3.1 동일 VPN 내의 사이트로 이동

그림 2에 보여진 것처럼 Mobile IP 프로토콜은 가입자 네트워크에 속한 CE 라우터 상에서 수행된다. 만일 Mobile IP 프로토콜이 그림 2의 PE 라우터 상에서 수행된다면, PE 라우터는 홈 에이전트와 외부 에이전트 기능을 함께 수행하게 된다[12].

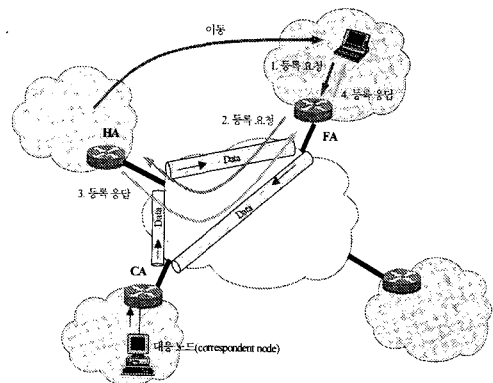


그림 2. Mobile IP 등록 및 데이터 전달  
Fig. 2 Mobile IP Registration and Data Transmission

예를 들어 그림 3의 PE<sub>1</sub> 라우터 상에서 수행되는 외부 에이전트는 앞서 기술된 Mobile IP 프로토콜과 달리 자신과 연결된 두 개의 VPN 사이트로 동일한 'ICMP Agent Advertisement' 메시지를 전송하게 된다. 만일 그림 4에서 VPN A/site 1에 속해 있는 이동 노드가 VPN A/site 2로 이동한다면, 이동 노드는 자신이 이동했는지를 파악할 수 없게 된다. 이것은 이동 노드가 이동한 이후에도 PE<sub>1</sub> 라우터에서 수행되는 외부 에이전트로부터 동일한 'ICMP Agent Advertisement' 메시지를 받기 때문이다.

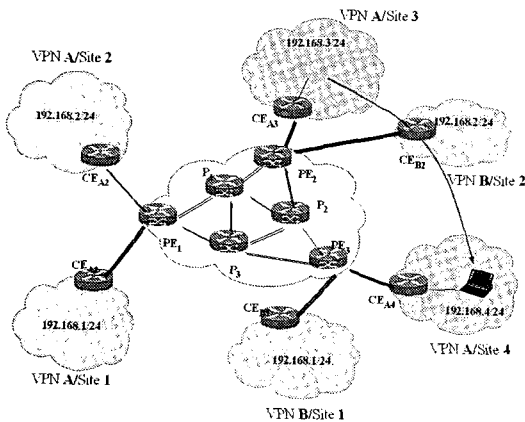


그림 3. PE 기반 MPLS VPN 구성 및 이동 예  
Fig. 3 PE based MPLS VPN Configuration and Moving Example

따라서, 이동 노드가 이동을 인식할 수 있도록 PE<sub>1</sub> 라우터에서 수행되는 외부 에이전트는 자신과 연결된 VPN 사이트마다 서로 다른 'ICMP Agent Advertisement' 메시지를 전송해야만 한다. 만일 PE<sub>1</sub> 라우터에 다른 종류의 VPN들이 연결되어 있다면, 'ICMP Agent Advertisement' 메시지에는 VPN 식별정보도 추가로 포함되어야 한다. 이 정보를 기반으로 이동 노드는 자신이 동일한 VPN으로 이동했는지 다른 VPN으로 이동했는지를 파악할 수 있게 된다. 그러므로, 'ICMP Agent Advertisement' 메시지에는 'VPN Information' Extension을 추가되어야 한다. 이동 노드는 'VPN Information' Extension을 통하여 같은 VPN 내로 이동했는지 다른 VPN으로 이동했는지 알 수 있게 된다. 또한, 이동 노드가 다른 VPN의 사이트 내로 이동한 경우라면, 이동 노드는 'VPN Information' Extension을 이용하여 이동한 사이트 내의 주소 영역이 이동 노드와 동일한 주소 영역을 사용하는 지를 알 수 있다. 'VPN

Information' Extension에는 VPN-ID 및 VPN 사이트 관련 정보가 포함된다.

### 3.2 다른 VPN 내의 사이트로 이동

그림 3에서 어떤 VPN(VPN A/site 2) 내에 속한 노드가 다른 VPN(VPN B/site 2)으로 이동한다면, 이동 노드는 방문한 VPN 사이트의 외부 에이전트(PE2)로부터 'ICMP Agent Advertisement' 메시지를 수신하게 된다. 이 메시지를 통하여 이동 노드는 이동을 확인한다. 이 때, 외부 에이전트는 'ICMP Agent Advertisement' 메시지 내에 'VPN Information' Extension을 추가하여 전송해야 한다[12].

'VPN Information' Extension이 추가된 'ICMP Agent Advertisement' 메시지를 수신한 이후에, 이동 노드는 이동한 사이트의 주소 영역이 자신의 주소 영역과 동일한지를 검사한다. 동일하다면, 'ICMP Agent Advertisement' 메시지에 포함된 외부 에이전트의 Care-of-Address를 사용하여 등록 절차를 수행할 수 없다. 왜냐하면 이동한 사이트 내에서 이동 노드와 같은 주소를 사용하는 노드가 존재하여 주소 충돌이 발생할 수 있기 때문이다. 이러한 경우, 이동 노드는 방문 사이트에서 Co-located Care-of-Address를 할당 받은 후에 등록 절차를 수행한다. 만일 동일하지 않다면, 이동 노드는 'ICMP Agent Advertisement' 메시지에 포함된 외부 에이전트의 Care-of-Address를 사용하여 등록 절차를 수행한다.

### 3.3 라우팅

그림 3의 예에서 VPN A/site 3에 있던 이동 노드가 VPN A/site 4로 이동하는 경우를 가정해 보자. 그림 4는 VPN A/site 1에 있는 대응 노드가 VPN A/site 3에 있던 이동 노드로 데이터 패킷의 전달 과정을 보여준다. 우선, 이동 노드는 PE<sub>3</sub> 라우터에서 수행되는 외부 에이전트 및 PE<sub>1</sub>의 홈 에이전트를 통하여 등록 과정을 수행한다. 등록 과정이 끝난 이후, VPN A/site 1에 있는 대응 노드가 이동 노드에게 데이터를 전달하고자 한다. 먼저, 대응 노드가 전송한 패킷은 CE<sub>1A1</sub> 라우터를 거쳐 PE<sub>1</sub>에게 전달된다. PE<sub>1</sub>은 CE<sub>1A1</sub> 라우터로부터 수신된 패킷이 VPN A라는 것을 이미 알고 있다. PE<sub>1</sub>은 수신된 패킷의 목적지 주소를 갖고 VPN A에 해당하는 VRF(VPN Routing and Forwarding)를 검색하여 이동 노드의 홈 네트워크 라우터인 PE<sub>2</sub>에게 두 단계 스택킹된 레이블 패킷을 전달한다. 두 단계 레이블의 바깥(outer) 레이블은 PE<sub>1</sub>과 PE<sub>2</sub> 사이에 설정된 LSP를

의미하며, 안(inner) 레이블은 VPN 종류를 의미한다. VPN 종류를 의미하는 VPN 레이블은 PE<sub>1</sub>의 VRF를 통해 얻어진다. PE<sub>2</sub>에서는 패킷을 수신한 후, VPN A/site 3으로 패킷을 전달하기 이전에 VPN A/site 3에 있던 목적지 노드가 이동했는지를 검사한다. 이동 확인은 PE<sub>2</sub>의 홈 에이전트에 의해 수행된다.

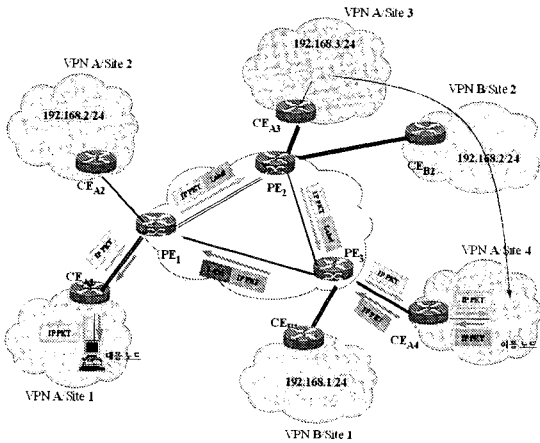


그림 4. 이동 서비스 이후의 패킷 라우팅  
Fig. 4 Packet Routing after mobility service

홈 에이전트는 각 VPN 별로 구성된 "Binding Entry"에서 이동 노드의 정보를 추출한다. 홈 에이전트에 의해 목적지 노드가 PE<sub>3</sub>로 이동했다는 것을 파악한 후, PE<sub>2</sub>는 PE<sub>3</sub>로 패킷을 전달한다. PE<sub>3</sub>에서는 패킷을 수신하고, 외부 에이전트를 통해 목적지 노드가 어느 사이트로 이동했는지를 파악한다. PE<sub>3</sub>는 외부 에이전트에서 관리하는 VPN A에 해당하는 "Visitor List Entry" 정보에 따라 CE A4 사이트 내에 목적지 노드가 존재함을 알게 된다. 그런 다음 PE<sub>3</sub>는 CE A4로 패킷을 전달한다. CE A4는 수신된 패킷을 자신의 사이트로 브로드캐스팅(broadcasting)하고 이동 노드는 자신의 패킷을 수신한다.

이동 노드가 대응 노드로 응답 패킷을 전송하는 과정을 살펴보자. 우선 PE<sub>3</sub>가 CE A4로부터 패킷을 수신한다면, PE<sub>3</sub>는 VPN A에 해당하는 VRF를 검색할 것이다. 그런 다음 수신된 패킷의 목적지 주소에 따라 PE<sub>1</sub>으로 레이블 패킷을 전달한다. PE<sub>1</sub>은 패킷을 수신한 후, CE A1에게 전달한다. 그림 4에서 보듯이, 패킷 전달에서 삼각 라우팅 현상이 발생한다. 삼각 라우팅(triangle routing)은 Mobile IP 프로토콜의 문제점이며, 이것을 보완하기 위해

경로 최적화(Route Optimization) 방안이 도입되었다. 본 연구에서도 경로 최적화 방안을 도입하여 삼각 라우팅 문제를 해결하고자 한다. 그 방법은 PE 라우터(예: 그림 4의 PE<sub>1</sub>)에 대응 에이전트(Correspondent Agent)를 두어 홈 에이전트로부터 "Binding Update" 메시지를 받아 이동 노드의 정보를 기록하는 것이다. 대응 노드에서 이동 노드로 전달되는 패킷은 PE 라우터 상에서 수행되는 대응 에이전트에 의해, 홈 에이전트로 전달되지 않고 직접 외부 에이전트로 전달된다. 따라서, 대응 노드는 Mobile IP 혹은 VPN에 무관하게 이동 노드로 데이터를 전달할 수 있다. 이러한 과정이 그림 5에 보여진다.

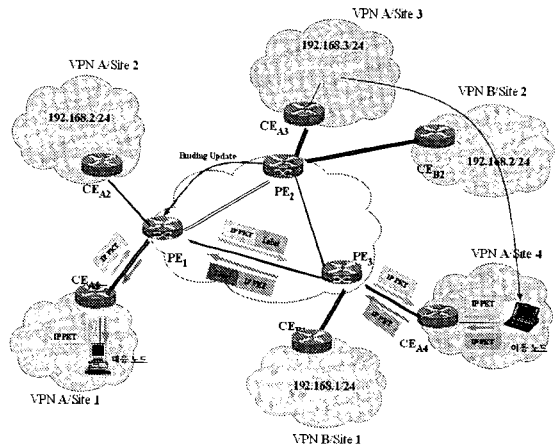


그림 5. 경로최적화에서의 패킷 라우팅  
Fig. 5 Packet Routing in Route Optimization

#### IV. 이동 MPLS VPN에서의 QoS 지원

현재의 인터넷은 최단 경로(shortest Path) 알고리즘에 기반한 RIP(Routing Information Protocol), OSPF(Open Shortest Path First), IS-IS(Intermediate System to Intermediate System)와 같은 IGP(Interior Gateway Protocol) 프로토콜들을 사용하고 있다. 이러한 인터넷 IGP 프로토콜들은 네트워크의 자원 상태에 관계없이 최단 경로만으로 집중하여 혼잡 상황을 발생시킬 수 있다. 이러한 혼잡 문제를 해결하기 위하여 등장한 기술이 바로 트래픽 엔지니어링이다.

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 매커니즘을 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.

트래픽 엔지니어링의 목적은 망 자원의 효율성을 극대화 시키고 트래픽 스트림의 서비스 품질을 높이는 것이다. MPLS는 명시적 라우팅, 트래픽 모음, 제약 기반 라우팅, 부하 분산과 같은 트래픽 엔지니어링 기술을 손쉽게 지원할 수 있기 때문에 트래픽 엔지니어링을 적용하기에 적합한 기술로써 알려져 있다.

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.

트래픽 제어 서버는 SLA 프로파일, QoS 정책, LSP별 품질정보, QoS 매트릭(metric)과 같은 트래픽 엔지니어링 데이터베이스를 총괄 관리하고, 이를 이용하여 경로 계산, 부하 분산, 재 라우팅 등의 엔지니어링 제어 기능을 네트워크 전반에 대해 수행한다. LSR은 Traffic Engineered MPLS 기능을 위해 추가적으로 QoS 라우팅 프로토콜, MPLS 시그널링 프로토콜이 추가되며, 입력단에는 패킷 분류 및 전송 기능이 추가된다.

Constrained 라우트를 찾아내기 위해서는 온라인 경로 계산 방법을 이용한다. 온라인 경로계산은 QoS 라우팅

프로토콜을 이용하여 QoS 매트릭을 수집 분배하고, 이를 이용하여 특정 제한 사상을 만족시키는 경로를 찾는 알고리즘으로 구성된다. QoS 매트릭은 링크 총 대역폭, 예약된 대역폭, 예약 가능한 대역폭, 전달지연 등 네트워크의 최신 상태에 대한 정보로 구성된다. 사용자 제한 사항은 요구 대역폭, 허용 가능 최대 홉수, 설정 및 유지 우선 순위, 링크 운용 관리 정보 등 가입자나 운용자의 자원사용에 대한 제한 사상을 포함한다.

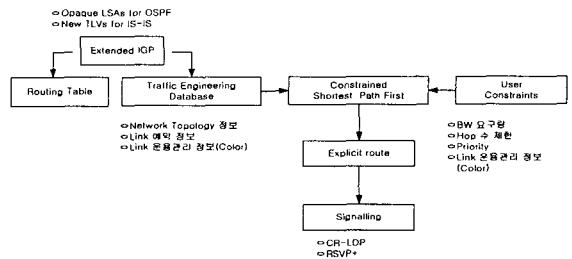


그림 6. Constrained-based Routing 기능  
Fig. 6 Constrained-based Routing Function

그림 6은 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.

시그널링 프로토콜로써 CR-LDP는 LSP 설정 메시지 내에 explicit 라우트 정보와 트래픽 파라미터를 전달할 수 있도록 LDP를 확장한 프로토콜로서, TCP를 이용하여 시그널링 메시지를 교환한다.

ER-LSP 설정은 그림 7에서처럼 미리 결정된 경로를 따라 레이블 요구 및 레이블 매핑 메시지를 한 바퀴 교환함에 따라 이루어진다. 일단 ER-LSP 경로가 결정되면 시그널링 프로토콜을 이용하여 해당되는 노드들 간에 연결을 설정한다.

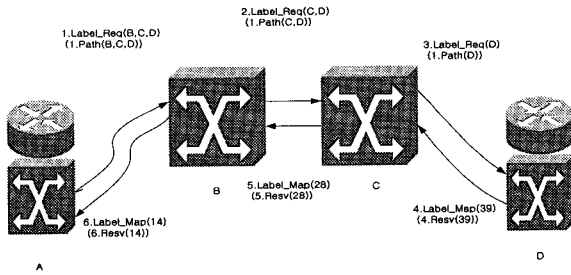


그림 7. CR-LDP 및 RSVP-TE 연결 설정 과정  
Fig. 7 CR-LDP and RSVP-TE Connection Establishment

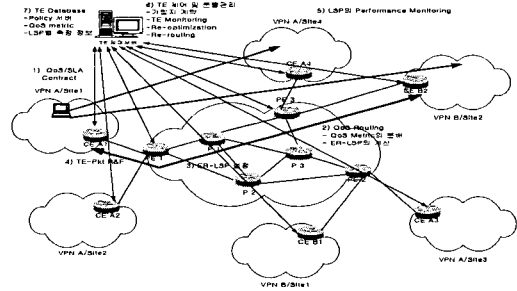


그림 9. 트래픽 엔지니어링을 이용한 QoS 지원  
Fig. 9 QoS Support using Traffic Engineering

MPLS 시그널링 프로토콜은 레이블의 분배, explicit 라우트 정보의 전달, 대역폭을 포함한 트래픽 파라미터의 전달 및 우선순위와 같은 연결 설정에 필요한 부가적인 정보들을 인접 노드들 간에 전달하는 역할을 한다[13].

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 운전자 정책을 고려하여, 계약 범위 안에서 트래픽 특성에 따라 레이블과 PHB(per hop behavior)가 결정되고, 버퍼링을 거쳐서 다음 노드로 전송한다. 그림 8에서 QoS 패킷의 분류 및 분배 기능을 나타낸다.

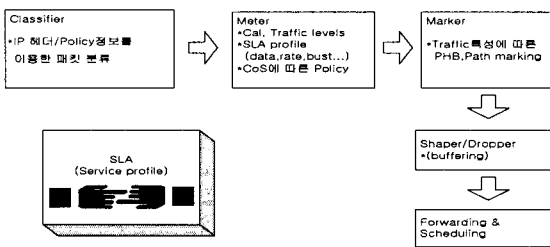


그림 8. QoS 패킷으로의 분류 및 분배 기능  
Fig. 8 QoS Packet Classifying and Distribution

이동성을 지원하는 MPLS VPN에서의 QoS 지원을 위해 MPLS 트래픽 엔지니어링을 이용하였고 전체적인 구성은 그림 9와 같다.

### V. 실험 및 성능 평가

본 논문에서는 PE 기반 MPLS VPN에서 이동 노드가 같은 VPN 내의 다른 사이트로 이동하는 경우와 다른 VPN 내의 사이트로 이동하는 경우에서 이동 엔티티들 간의 메시지 교환과 대응 노드에서 이동 노드로의 데이터 패킷 및 QoS 패킷 전송을 시뮬레이션 도구 COVERS를 이용하여 구현하였다.

이동성을 갖는 MPLS VPN에서의 QoS 지원의 시뮬레이션은 그림 3의 VPN 구성 모델을 대상으로 하였다. 이동성 지원 서비스의 시뮬레이션을 수행하기 위해 모두 6개의 VPN 사이트와 3개의 PE 라우터, 그리고 각 사이트당 1개의 CE 라우터로 구성하였고, 이에 따라 6개의 VPN 사이트가 생성된다.

이와 같은 구성을 기반으로 그림 10과 같이 VPN 사이트에서 다른 VPN 사이트로 이동하는 경우를 가정하여 시뮬레이션이 수행된다. 이동 노드가 VPN 사이트로 이동하는 것은 시뮬레이션 수행 시간 동안 랜덤(random)하게 계속 반복된다.

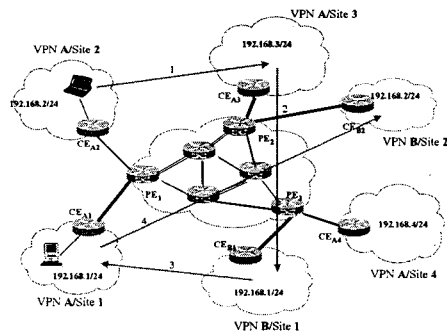


그림 10. 시뮬레이션에서의 이동 노드 시나리오  
Fig. 10 Mobile Node Scenarios on the Simulation

본 연구에서 제안한 이동성을 갖는 MPLS VPN에서의 QoS 지원의 성능을 평가하기 위해 QoS를 제공하는 LSP와 QoS를 제공하지 않는 LSP의 데이터 패킷 손실율을 측정하였다.

네트워크 내에서 이동 엔티티 사이에 전송되는 메시지의 손실은 QoS를 제공하는 LSP의 경우 적고, QoS를 제공하지 않는 LSP의 경우 이 보다 조금 더 크다고 가정하였다. QoS를 제공하는 LSP와 QoS를 제공하지 않는 LSP의 전송 지연은 각각 평균 2초, 5초 값을 갖는 지수 분포를 따른다고 가정한다. 또한, 대응 노드는 rate 1.2(데이터 패킷/초)의 포아송 분포로 이동 노드에게 데이터를 전송한다고 가정한다.

그림 10의 시나리오에 따라 COVERS를 이용하여 시뮬레이션을 수행하는 과정이 그림 11에서 보여진다. PE 기반 MPLS VPN에서 이동 노드가 이동 이후에, 등록 절차를 시작하는 과정과 이동 노드가 방문한 VPN 사이트 내의 외부 에이전트가 홈 에이전트로 등록 요청을 전달하는 과정들이 예시되어 있다. 우측 그림은 PE 라우터들의 상태를 보여주며, 다른 PE 라우터들은 'Normal' 상태에 있지만 세 번째 PE 라우터가 이동 노드의 방문으로 등록 과정에 있음 알 수 있다. 좌측 하단에는 이동 노드가 다른 사이트로 이동하여 등록을 시작하고 있는 과정이다.

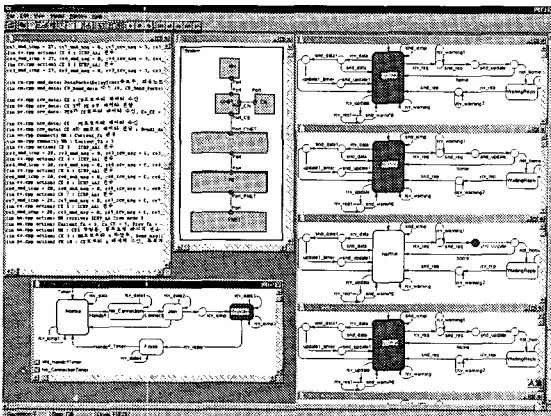


그림 11. 시뮬레이션 수행 과정  
Fig. 11 Example of Simulation Operations

그림 12는 이동 노드의 핸드오프 비율에 따라 대응 노드에서 전송된 데이터 패킷의 수와 이동 노드에서 수신한 패킷의 수를 백분율로 표시하였다. 이동 노드의 핸드오프 비율이 증가하면 이동 노드가 더 자주 비연결 상태

에 놓이기 때문에, 이동 노드에서 데이터 패킷의 수신율이 저하됨을 알 수 있다. 또한, QoS를 보장하는 LSP와 QoS를 보장하지 않는 LSP에서의 이동 노드 데이터 패킷 수신율은 핸드오프 비율이 커짐에 따라 그 차이가 커짐을 볼 수 있다.

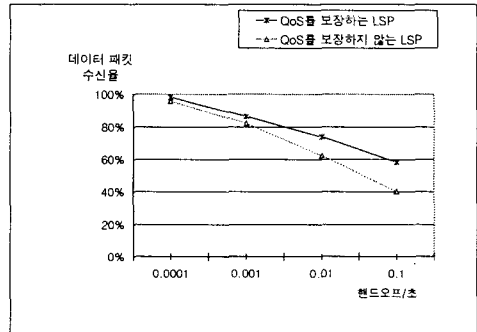


그림 12. 이동 노드의 핸드오프율에 따른 데이터 패킷 수신율

Fig. 12 Receiving Rate of Data Packet based on Handoff-Rate of Mobile Node

## VI. 결론

VPN은 기업들이 많은 비용을 들여 별도의 사설 전용 망을 구축하지 않고 국내의 지사는 물론 협력사 및 고객과 일반 인터넷 망을 통해 전용선으로 통신하는 것처럼 빠르고 안전하게 정보를 주고받을 수 있는 시스템으로 최근 기업들의 요구 증가로 인하여 시장 확대가 급속히 이루어지고 있는 솔루션이다.

그러나, 기존 VPN은 터널링(tunneling)이 주는 추가의 오버헤드, 암호화 기법, 복잡한 관리 등과 같은 문제점을 내포하고 있다. 또한 사용자에게 차별화된 VPN 망을 제공하지 못하고, 자동으로 터널을 구성 및 관리하는 프로토콜이 없으며, 신뢰성 있는 VPN 서비스를 제공하기 위한 기술적인 측면에서 많은 문제점을 갖고 있다.

본 논문에서는 이동성을 지원하는 PE 라우터 기반 MPLS VPN에서의 트래픽 엔지니어링을 이용한 QoS 지원 방안을 설계 제시하였으며, PE 라우터 기반 MPLS VPN을 대상으로 하여 라우터 내의 기능과 프로토콜을 구현하였다. 성능 검증을 위해 시뮬레이션 도구인 COVERS를 이용하여 시뮬레이션을 수행하였다.



시뮬레이션을 수행한 결과, 이동 노드의 핸드오프 비율이 증가하면 이동 노드가 더 자주 비연결 상태에 놓이기 때문에 이동 노드에서 데이터 패킷의 수신율이 저하됨을 확인할 수 있었다. 또한 QoS를 보장하는 LSP에서의 데이터 패킷 수신율의 경우 핸드오프 비율이 증가할수록 QoS를 보장하지 않는 LSP에서의 데이터 패킷 수신율의 경우에 비교하여 상대적으로 더 적은 패킷 손실을 가짐을 확인하였다.

이동성을 지원하는 MPLS VPN에 트래픽 엔지니어링 기술을 이용함으로써 가입자는 고품질의 VPN 서비스를 경제적인 비용에 이용할 수 있고 사업자는 서비스 운용관리를 포함한 다양한 부가서비스의 지원, 수익성 그리고 한정된 네트워크 자원을 효율적으로 운용할 수 있다는 점에서 앞으로 많이 응용될 것으로 전망된다.

현실적으로 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.

### 참고문헌

[ 1 ] Hamzeh K., et al, "Point-to-Point Tunneling Protocol," draft-ietf-pppext-12tp-16.txt, Apr. 1999.  
 [ 2 ] Townsley, W., et al, "Layer Two Tunneling Protocol," draft-ietf-pppext-12tp-16.txt, Jun. 1999.  
 [ 3 ] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", RFC 1825, Jul. 1998.  
 [ 4 ] D. Farincci, T. Li, A. Conta, Y. Rekhter, D. Tappan, E. Rosen, G. Fedrokov, "MPLS Label Stack Encoding," Internet Draft draft-ietf-mpls-label-encaps-07.txt, Oct. 1999.  
 [ 5 ] B. Gleeson, et al, "A framework for IP based Virtual Private Network," RFC2764, Feb. 2000.  
 [ 6 ] Eric Rosen, Yakov Rekhter, "BGP/MPLS VPNs", RFC 2547, Mar. 1999.  
 [ 7 ] 이영석, 오명환, 최 훈, "MPLS VPN에서의 Mobile IP", 한국통신학회논문지, Vol. 28, No. 8B,

pp.738-749, 2003년 8월  
 [ 8 ] C. Perkins, "IP Mobility Support," Proposed Standard, RFC2002, Oct. 1996.  
 [ 9 ] C. Perkins, "Mobile IP," IEEE Communications Magazine, May 1997.  
 [ 10 ] C. Perkins, D. Johnson, "Route Optimization in Mobile IP," Internet Draft, draft-ietf-mobileip-optim-09.txt, Feb. 2000.  
 [ 11 ] Cheng-Yin Lee, Glenn Morrow, Fayaz Kadri, "Intercepting Location Updates," Internet-Draft, Nov. 2000.  
 [ 12 ] 이영석, 임형택, 최훈, "이동 서비스를 지원하는 BGP-E 방식 MPLS VPN 설계 및 구현," 한국통신학회논문지, Vol. 28, No. 10B, pp.927-937, 2003년 10월  
 [ 13 ] 양선희, 정민영, 이유경, "MPLS 트래픽 엔지니어링에 의한 인터넷 품질제어기술," 한국통신학회지 Vol. 17, No. 9, pp. 66-76, 2000년 9월

### 저자소개

#### 이 영 석(Young-seok Lee)



1992년 충남대학교 컴퓨터공학과 공학사  
 1994년 충남대학교 컴퓨터공학과 공학석사  
 2002년 충남대학교 컴퓨터공학과 공학박사

1994년~1997년 LG전자정보통신연구소 연구원  
 2002년~2004년 한국전자통신연구원 선임연구원  
 2004년~현재 군산대학교 전자정보공학부 교수  
 ※관심분야: 정보보호, 이동컴퓨팅, 컴퓨터네트워크

#### 양 해 권(Hae-Kwon Yang)



1976년 서울대학교 전기공학과 공학사  
 1983년 울산대학교 전기공학과 공학석사  
 1992년 전북대학교 전기공학과 공학박사

1985년~1987년 호원대학교 전자계산학과 전임강사  
 1987년~현재 군산대학교 전자정보공학부 교수  
 ※관심분야: 광대역통합망(BcN), 인터넷