# MPLS 망을 기반으로 하는 VPN의 성능에 관한 연구

# A Study on the Performance of VPN based on MPLS Networks

신 태 삼*, 김 영 범**

Tae-Sam Shin*, Young-Beom Kim**

## 요 약

본 논문에서는 MPLS VPN의 개념을 도입하고 이를 바탕으로 MPLS 망에서 VPN 서비스를 제공하는 방안을 제시하였다. 또한 MPLS VPN의 제어 요소와 동작절차를 설계하고, MPLS VPN과 종래의 VPN 구현 방식에 대하여 성능을 평가해 보았다. MPLS 기반 VPN은 VPN ID 부여 및 터널링이 없는 가상공간의 할당으로 IP VPN의 문제점들을 해결하고 효율적인 서비스 제공이 가능하다. 즉, MPLS VPN은 하나의 물리적 회선에서 고객별로 완벽한 트래픽 분리가 가능한 MPLS 기술과 공중망을 이용함으로써, 높은 신뢰성과 보안수준을 보장할 수 있다. 특히 고객의 입장에서는 장비도입 비용이나 관리비용을 절감할 수 있다는 장점이 있다. 반면에, MPLS 망에 기반을 두면 MPLS의 장점을 그대로 수용하여 효과적인 VPN 서비스를 제공할 수 있으나 동일한 ISP(Internet Service Provider)의 네트워크 내부에서만 구현이 가능하고, 자체적인 암호화 성능이 미약하므로 인터넷과 같은 공중망 경유 시 보안에 다소 취약하다는 단점이 있다.

## Abstract

In this paper we introduce the concept of MPLS-based VPN and propose a scheme for providing VPN services in MPLS networks. Furthermore, we design the control components and the operational procedures and evaluated the performance of traditional VPN implementation methods and MPLS-based VPN. In this scheme it is possible to solve several problems that IP-based VPN pertains via the allocation of VPN ID and virtual space without tunneling, thereby providing effective VPN services. In other words, the MPLS-based VPN scheme uses MPLS networking technology together with the PSTN which can achieve a perfect segregation of user traffic on per-customer basis in a physical link and can guarantee high reliability and security levels. Specially, in the perspective of customers, it can save networking facilities installation and maintenance costs considerably. On the contrary, it possesses some shortcomings in that its deployment tends to be restricted within an ISP's network boundary and it is vulnerable to external security break-ins when going through public networks such as the Internet due to its lack of data encryption capability.

***Keywords*** : Internet, MPLS, VPN, ATM, IPSec, LSP, QoS

## I. 서 론

인터넷은 세계를 연결하는 글로벌 네트워크로서 통신망의 발달 및 고성능 PC의 보급 등으로 인하여 보편적인 서비스로 발전되었으며 사용자 증가만큼이나 데이터 트래픽 또한 급증하였다. 하지만 기존의 인터넷은 고속의 멀티미디어 트래픽을 요구하는 현재의 인터넷 사용자들을 만족시켜 주기에는 확장성, IP (Internet Protocol) 전송능력, QoS (Quality of Service) 보장 등 근본적으로 개선되어야 할 문제점을 가지고 있다. 인터넷의 개방성과 확장성으로 인해 보안성이 취약하고, 네트워크 공유로 인한 속도저하 등이 발생한다. 다시 말해 해킹 등으로 인한 정보의 유출, 변조, 도용 등의 보안상 문제점이 심각하게 대두되었고, 네트워크를 공유함에 따라 자원의 독점이 불가능하여 원하는 시간에 원하는 만큼의 정보를 전송할 수 있는 능력을 보장 할 수 없게 된 것이다[1].

차세대 IP망 기술로서 각광받고 있는 MPLS (Multi-Protocol Label Switching)에 대한 표준화는 국제 표준화 기구인 IETF (Internet Engineering Task Force)를 중심으로 활발히 진행되고 있으며 MPLS는 QoS 및 VPN

*LG파워콤 네트웍 기술팀 **건국대학교 전자공학부
논문 번호 : 2006-4-15 접수 일자 : 2006.10.26
심사 완료 : 2007. 1.18

(Virtual Private Network)과 같은 고급 서비스를 제공하기에 쉬운 구조를 가지고 있다 [2,3,4].

VPN은 인터넷에서 사용자들에게 전용회선과 같은 서비스 품질을 보장해주고, 보안기능을 제공함으로써 저렴한 비용으로 전용회선을 이용하는 효과를 제공해 줄 수 있다. 공공의 네트워크를 마치 자신의 전용회선처럼 사용할 수가 있어 지사를 가지고 있는 기업의 네트워크를 구축하기 위한 방안으로서 주목을 받고 있다. 기업의 인트라넷이 WAN(Wide Area Network)을 통해 투명성 있게 확장되려면 경제적 효율성을 고려하여 IP VPN의 형태로 진화되어야 할 필요가 있으나 이를 위해서는 터널링(tunneling), 암호화에 따른 오버헤드, 그리고 관리면 복잡성 등의 문제가 뒤따르게 된다[5].

본 논문에서는 MPLS VPN의 개념을 설명하고 이를 바탕으로 MPLS 망에서 VPN 서비스를 제공하는 방안을 제시하였다. 또한 MPLS VPN의 제어 요소와 동작절차를 설계하고, MPLS VPN과 종래의 VPN 구현 방식에 대하여 성능을 평가해 보았다. MPLS 기반 VPN은 VPN ID 부여 및 터널링이 없는 가상공간의 할당으로 IP VPN의 문제점들을 해결하고 효율적인 서비스 제공이 가능하다. 즉, MPLS VPN은 하나의 물리적 회선에서 고객별로 완벽한 트래픽 분리가 가능한 MPLS 기술과 공중망을 이용함으로써, 높은 신뢰성과 보안수준을 보장할 수 있다. 특히 고객의 입장에서는 장비도입 비용이나 관리비용을 절감할 수 있다는 장점이 있다. 반면에, MPLS 망에 기반을 두면 MPLS의 장점을 그대로 수용하여 효과적인 VPN 서비스를 제공할 수 있으나 동일한 ISP(Internet Service Provider)의 네트워크 내부에서만 구현이 가능하고, 자체적인 암호화 성능이 미약하므로 인터넷과 같은 공중망 경유 시 보안에 다소 취약하다는 단점이 있다.

본 논문의 구성은 다음과 같다. 제2장에서는 종래의 VPN 구현 방안에 대해 소개하고, 제3장에서는 MPLS VPN의 제어요소와 동작절차에 대한 설계를 제시하고, 제4장에서는 기존의 여러 가지 VPN 구현방안과 MPLS VPN 방안간의 장단점을 비교하였다. 제5장에서는 여러 가지 방안의 성능을 Markov chain을 이용한 해석과 함께 시뮬레이션을 통하여 비교하였고 마지막으로 제6장에서 결론을 제시한다.

## II. 기존 VPN 구현방안에 대한 고찰

이 장에서는 ATM VPN[6]과 IPSec VPN[7]에 대해서 간단히 살펴보고 각각의 VPN 모델과 MPLS VPN의 장단점을 비교해 보기로 한다.

ATM은 LAN 백본이 FDDI (Fiber Distributed Data Interface)를 거쳐 고속 이더넷으로 진화하는 과정에서 새롭게 등장한 기술로서 데이터를 고정 길이의 셀(cell) 단위로 구분하여 전송하는 전용접속(dedicated) 방식 스위칭 기술이다. ATM 기반 VPN 기술은 ATM 인프라와 가상회선 (VC: Virtual Circuit) 기능을 이용하여 VPN을 구성하는 기술을 말하며, 전용 회선처럼 완전한 메시 (full-mesh) 형태로 양쪽 단말 간의 가상채널 및 가상경로를 설정한다. 그림 1은 ATM VPN의 구성 및 요소를 나타낸 것이다. ATM VPN은 ATM의 망관리 기능 및 보안성을 유지하면서 ATM 셀뿐만 아니라, IP 패킷 및 Non-IP 패킷을 모두 전송할 수 있으므로 음성 및 데이터망의 통합 관점에서도 강력한 기능을 제공할 수 있다. 또한 ATM 환경에서 기본적으로 제공하는 QoS 기능을 이용하여 멀티미디어 서비스와 같은 실시간 데이터를 수용할 수 있으므로 ISP 입장에서는 다른 방식에 비해 특화된 서비스를 제공할 수 있다는 장점이 있다.

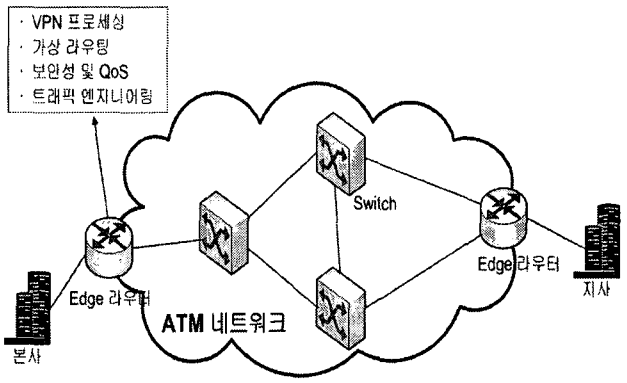


그림 1. ATM VPN의 구성 및 요소.
Fig. 1. The structure and components of ATM VPN.

그러나 ATM 장비 자체가 고가이며, 각 가입자 단말과의 접속을 위한 PVC (Permanent Virtual Circuit) 서비스 비용이 상대적으로 비싸다는 문제점이 있다. 또한 ATM VPN은 IP를 전송하기 위해 IP 주소와 라우팅을 ATM 주소와 라우팅으로 매핑시키는 복잡한 주소 변환 체계가 필요하며, 새로운 VPN 사이트를 추가시키기 위해 ATM VPN에서는 사이트별로 point-to-point VC 메시를 구성해야 하는 단점이 있다.

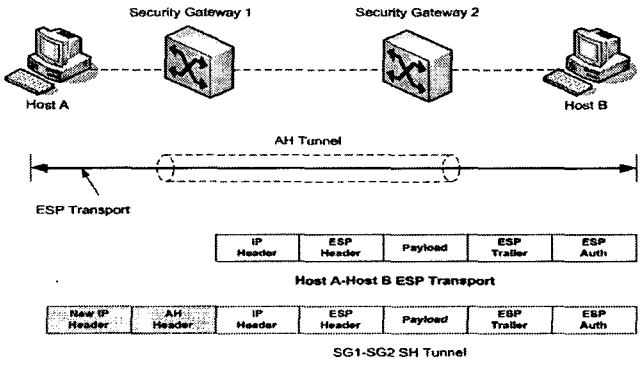


그림 2. IPSec 프로토콜 동작 과정.
Fig. 2. The operation of IPSec protocol.

IPSec은 IETF에 의해 표준화된 암호화와 관련된 시스템 구조 및 키 관리 프로토콜로서 IP 프로토콜의 보안상 문제점을 해결하고 네트워크 계층에서의 보안성을 보장하기 위해 개발되었다.

그림 2에서 주요 구성요소에 의한 처리과정을 살펴보면 IPSec은 시스템으로 하여금 보안 프로토콜을 선택하고, 암호화 알고리즘을 결정하며, 암호화 키를 결정할 수 있도록 함으로서 IP계층에서 보안 서비스를 제공할 수 있도록 하고 있다. IPSec은 암호화, 인증 및 키 관리 등 강력한 보안 기능을 탑재하고 있기 때문에 IP 환경에 있어서 최고의 터널링 프로토콜로 받아들여지고 있지만 오로지 IP 환경에서만 효과를 갖는다. 현재 사용되고 있는 IPSec 프로토콜은 인터넷상의 패킷들에 대한 보안 서비스 제공이라는 원래의 목적과는 달리 VPN의 구축에 주로 사용되고 있다. 그림 3은 이러한 IPSec VPN의 구조를 나타내었다. 그림에서와 같이 IPSec 프로토콜은 보안 게이트웨이에 탑재되며 보안 게이트웨이 사이에 IP 보안 터널을 형성하여 보안 서비스를 제공한다. IPSec은 네트워크 계층에서 암호화를 수행하기 때문에 원격지 VPN 구성뿐 아니라 원격 접속 VPN까지 완벽히 지원하며, 타 VPN 프로토콜과 달리 어플리케이션과는 독립적인 구현이 가능하다는 장점이 있다. 하지만 트래픽 제어 및 QoS 기능이 미약하고, 높은 초기 도입비용과 지속적인 관리비용이 발생하는 단점이 있다.

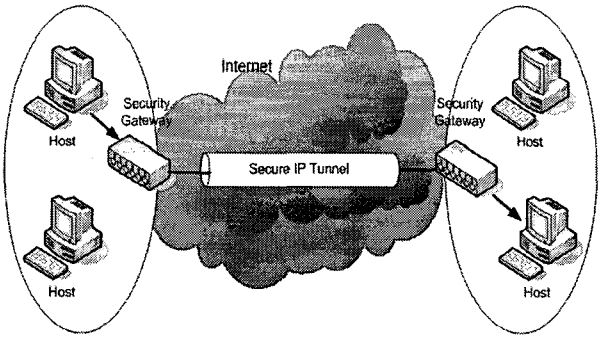


그림 3. IPSec VPN 구성 및 요소.
Fig. 3. The structure and components of IPSec VPN.

## Ⅲ. 제안된 MPLS 기반의 VPN 설계방안

MPLS VPN은 기존 라우팅 프로토콜인 BGP, OSPF를 이용하여 네트워크 노드들의 포워딩 정보인 FIB (Forwarding Information Base)를 생성하여 VPN의 연결 상태 정보를 얻게 되며, 이를 바탕으로 MPLS 망의 내부에서는 LDP 절차를 통해 레이블 할당 및 레이블 정보를 배포하게 된다.

### 3.1 MPLS VPN의 제어 요소 설계

그림 4는 ATM 인터페이스 상에서 동작하는 MPLS 프로토콜 제어 요소들이다. MPLS 망에서 라우팅 관리자는 호 설정을 위하여 BGP 등에 의하여 수집된 라우팅 정보를 LDP를 포함하는 레이블 관리자에게 알려준다. LDP는 이 라우팅 정보를 포워딩 정보로 재구성하여, FEC별로 레이블 할당을 요구한다. ATM 스위치 관리자는 레이블 제어 ATM 자원, 즉 VPI/VCI 값으로 연결 설정을 한다.

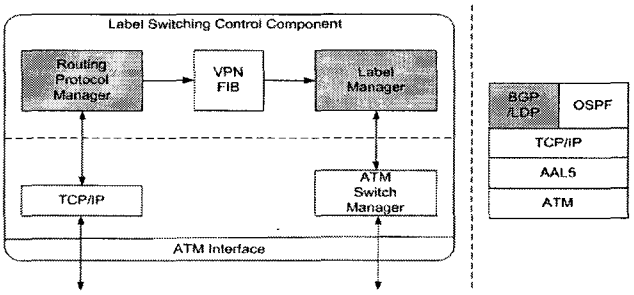


그림 4. MPLS VPN 프로토콜 제어요소.
Fig. 4. The control elements of MPLS VPN protocol.

### 3.2 MPLS VPN의 동작절차 설계

VPN을 지원하는 MPLS의 동작절차를 간단히 정리하면, VPN ID를 부여하여 VPN-IP 주소를 생성하고, VPN 라우팅 정보를 배포하고, 레이블과 VPN-IP 주소를 매핑하여 주소변환 (NAT : Network Address Translation)없이 망 제공자의 네트워크에서 유일한 주소를 생성한다. 이러한 라우팅 정보를 가지고 네트워크 포워딩 경로를 설정하여 VPN간에 통신을 설정하게 된다. 그림 5는 MPLS VPN의 동작절차 흐름도이다.

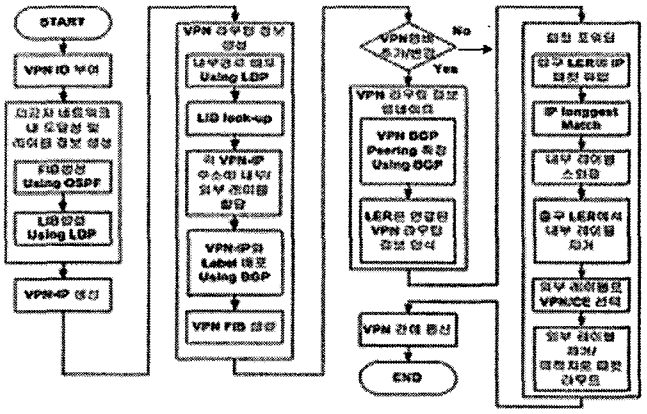


그림 5. MPLS VPN 동작절차 흐름도.
Fig. 5. The operational procedure of MPLS VPN.

## Ⅳ. 기존 VPN 구현방안과의 성능비교

이 장에서는 앞에서 검토한 내용을 바탕으로 MPLS VPN

과 기존의 VPN 구현방안과의 기능 및 장단점을 비교해 보고, 다음 장에서는 시뮬레이션을 통해 여러 가지 방안들의 성능을 비교해 보기로 한다.

VPN은 데이터 전송을 위한 백본상의 교환방식 관점에서 살펴보면, ATM 기반 VPN, IP 기반 VPN, 그리고 MPLS 기반 VPN으로 나눌 수 있다. 먼저 ATM 기반 VPN은 ATM의 QoS, 망관리의 편리성, 보안기능 등의 기술적인 장점을 가지면서 ATM 셀뿐만 아니라 IP 패킷, Non-IP 패킷을 모두 전송할 수 있으므로 음성, 데이터망, 인터넷망 등 통합의 관점에서 IP VPN에 비해서 유리하다. 이에 비해 IP 기반 VPN은 장비구입 비용이 적고 현재 기업체에서 사용되고 있는 단말과의 접속이 쉽다는 장점이 있으나, 트래픽이 급증할 경우의 QoS 제공과 트래픽 관리측면에서 인터넷이 가지고 있는 단점을 그대로 갖게 되어 추가적인 조치가 필요하다. 한편 MPLS 기반 VPN은 하나의 물리적인 회선에서 고객별로 완벽한 트래픽 분리가 가능한 MPLS 기술과 공중망을 이용하여 VPN을 구현하는 기술로, 높은 신뢰성과 보안수준을 보장할 수 있다. 또한 MPLS 기반 VPN은 레이블을 이용하여 데이터를 전송하므로 ATM 셀과 IP 패킷을 모두 처리할 수 있고, IP 라우터와 ATM 스위치 상에서 모두 구현할 수 있으며, 사용자 단말의 접속도 쉬운 장점을 가지고 있다. MPLS VPN은 가입자 측에 별도의 VPN 장비가 필요 없는 네트워크 서비스로 MPLS VPN 가입자들은 기존의 라우터를 업그레이드하거나 교체하지 않고 일반적인 라우팅 프로토콜을 사용하여 서비스 제공자의 VPN 네트워크에 연결하여 인트라넷 또는 엑스트라넷 VPN 서비스를 받을 수 있다. 반면 동일한 ISP 네트워크 내부에서만 구현이 가능하고, 자체적인 암호화 성능이 미약하여 인터넷과 같은 공중망 경유시 보안에 다소 취약하다는 단점이 있다.

### 4.1 MPLS VPN과 ATM VPN 비교

MPLS VPN을 ATM VPN과 비교해 볼 때, ATM VPN에서 IP 전송을 하려면 IP 주소와 라우팅을 ATM 주소와 라우팅으로 매핑시키는 복잡한 계층 구조의 변환 프로토콜이 있어야 하지만, MPLS VPN은 IP 주소와 라우팅 정보를 ATM 스위칭 테이블에 직접 매핑시켜서 복잡한 주소 변환 체계가 필요 없다는 장점을 가지고 있다. 특히, MPLS VPN은 고정된 길이의 레이블을 이용하여 데이터를 전송하므로 ATM 셀과 IP 패킷 모두를 수용할 수 있으며, 인터넷의 문제점인 대역폭 증가, 라우팅 증가, QoS 문제를 해결할 수 있는 현실적인 대안으로 인식되고 있다.

표 1. MPLS VPN과 ATM VPN의 성능 비교.
Table 1. Performance comparisons between MPLS VPN and ATM VPN.

| 구 분 | MPLS VPN | ATM VPN |
|---|---|---|
| IP 전송 | IP 주소와 라우팅 정보를 ATM 스위칭 테이블에 직접 매핑시킴 | IP 주소와 라우팅 정보를 ATM 주소와 라우팅 정보로 매핑하는 복잡한 구조의 프로토콜 필요 |
| 트래픽 구분 | 트래픽이 속한 VPN을 기초로 트래픽 구분용이 | 트래픽이 VC를 통해서 전송되므로 전달되는 트래픽의 종류 인식불가 |
| 프라이버시 구분 | VPN-IP 주소라고 하는 고유한 주소를 통하여 보안 확보 | PVC로 연결단위의 보안을 확보 |
| VPN 추가 | BGP가 모든 VPN 구성원을 자동으로 업데이트 | 새로운 사이트 별로 새로운 점대점 VC 메시 구성 필요 |

### 4.2 MPLS VPN과 IPSec VPN 비교

근래에 들어서는 인터넷이 기업 활동의 기반 인프라로 빠르게 확산됨 따라 IP 터널링 VPN 기술을 이용한 IPSec VPN이 각광을 받고 있는 추세이다. IPSec VPN은 IPsec 프로토콜을 이용하여 인터넷망 내에 정보보안이 가능한 터널을 제공하는 VPN 서비스를 제공한다. 따라서 뛰어난 보안성을 제공하지만, 키 관리 및 분배와 같은 여러 가지 기반 기술들이 필요하고, 가입자가 VPN 서비스를 직접 관리해 주어야 하며, QoS를 효과적으로 지원하지 못하는 등의 문제가 있다. 또한 IPSec 터널링시 Non-IPSec 터널링시보다 성능(throughput)이 상당히 떨어지며, 암호화 과정 등으로 인한 latency로 인해 음성 또는 영상 트래픽에는 적합하지 않으며, IKE (Internet Key Exchage) 프로토콜의 복잡성으로 인한 상호 연동성 문제도 단점으로 나타나고 있다.

표 2. MPLS VPN과 IPSec VPN 비교.
Table 2. Performance comparisons between MPLS VPN and IPSec VPN.

| 구분 | MPLS VPN | IPSec VPN |
|---|---|---|
| 장점 | -트래픽 제어, QoS 기능<br>-네트워크 레벨 VPN 기능<br>-낮은 장비도입 비용<br>-관리 편의성 및 비용 | -높은 보안수준과 암호화 기능<br>-고객 고유의 보안정책 적용<br>-다양한 인터넷 접속기술<br>-애플리케이션과 독립적 운용 |
| 단점 | -동일 ISP 내 운영 가능<br>-공중망 전송시 암호화 기능 취약<br>-대역폭에 비해 다소 고비용 | -높은 초기 도입비용<br>-트래픽 제어 및 QoS 기능미약<br>-지속적인 관리비용<br>-대규모 원격접속 환경에 다소 부적합 |

표 3에서는 앞에서 검토한 여러 가지 VPN의 기능을 비교해 보았다.

표 3. MPLS/ATM/IPSec VPN 기능 비교.
Table 3. Functional comparisons between

MPLS/ATM/IPSec VPNs.

| | MPLS VPN | ATM VPN | IPSec VPN |
|---|---|---|---|
| 확장성 | 매우 우수 | 우수 | 보통 |
| QoS | 매우 우수 | 매우 우수 | 보통 |
| 구축/유지 비용 | 저가 | 매우 고가 | 고가 |
| 보안성 | 보통 | 보통 | 우수 |

## V. 시뮬레이션 결과 및 검토

이 장에서는 여러 가지 VPN 구현방안의 성능 비교를 위해 컴퓨터 시뮬레이션을 통하여 얻어진 결과를 검토해 본다.

### 5.1 시뮬레이션을 위한 모델링

#### 5.1.1 MPLS VPN과 ATM VPN

네트워크를 통해 패킷이 전송되는 경로가 대기시간을 결정하는데, 라우팅 효율성에 영향을 미치는 중요한 요인으로 네트워크 처리율과 지연시간이 있다. 본 논문에서 성능평가를 위한 MPLS 및 ATM 기반의 VPN은 그림 6과 같은 모델을 갖는다.

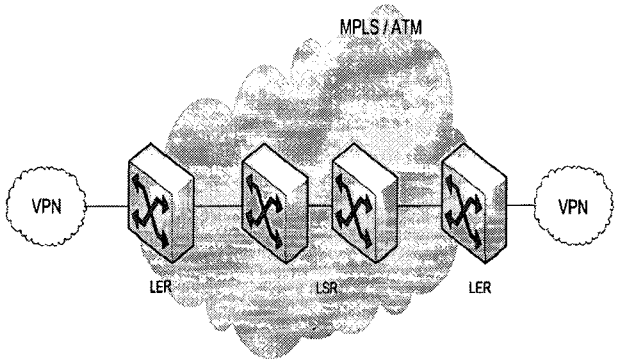


그림 6. 시뮬레이션을 위한 네트워크 모델링.
Fig. 6. The network model for computer simulation.

MPLS는 기존의 ATM과는 달리 FEC로 스트림을 병합하여 전송한다. 그림 7과 같이 VC 병합을 위해 변경된 스위치에서 각 흐름의 셀은 VC 리어셈블리 버퍼(RB : Reassembly Buffer)에 대기하고, 완전히 데이터그램을 수신한 후에는 출력 버퍼로 전송된다.

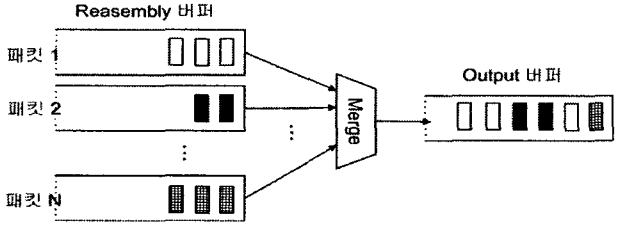


그림 7. MPLS 스위치의 VC 병합.
Fig. 7. A VC merging diagram in MPLS switches.

MPLS 도메인의 각 MPLS LER은 단일 FIFO (First In First Out) 출력버퍼에 완전하게 병합한다고 가정한다. 이는 주어진 패킷의 셀은 다른 패킷의 셀과 간섭하지 않는다는 의미이다. 출력포트의 도착 프로세스는 독립 ON-OFF 프로세스 N의 상태로 모델링 할 수 있다. 여기서 셀이 ON 주기 동안에 연속적으로 전송되고, ON과 OFF 주기 모두 각각의 입력 포트로부터 같은 파라미터로 기하학적 분배되는 것을 가정하면, 각 RB에 대한 도착 프로세스를 Interrupted Bernoulli Process (IBP)로 모델링할 수 있다. IBP는 다른 상태로 천이하는 확률(a와 b)과 현 상태에 머무르는 확률(1-a와 1-b)로 프로세스의 상태천이를 모델링한다. 여기서 OFF 주기일 때 RB의 값은 0이어야 하며, chain이 처음으로 ON 상태로 천이할 때 RB의 값은 1이 된다. 같은 ON 상태로 천이가 이어지는 동안, chain이 마침내 OFF 상태로 복귀하고 RB의 값이 순간적으로 0이 될 때까지 RB의 값은 1만큼씩 증가한다. 그림 8은 이와 같은 특징을 갖는 네트워크를 Markov 천이 다이어그램으로 나타낸 것이다.

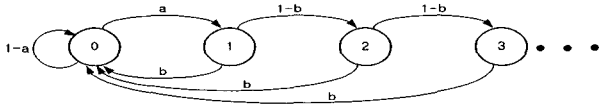


그림 8. Markov 천이 다이어그램.
Fig. 8. The Markov chain transition diagram.

이러한 규칙을 바탕으로, 상태($i$, $j$)에서 상태($i'$, $j'$)로 천이될 확률은, $N-j-i \le i' \le N-j$와 $N-i'-j \le j' \le N-i'$ 일 때

$$a_{i,j} = \binom{N-i}{j} \alpha^{j} (1-a)^{N-i-j}$$

이며, Markov chain의 상태 수는 $M=(N+1)(N+2)/2$이다. 여기에서 고려한 M/D/1 모델은 패킷 발생 확률로서 Poisson 분포를 따르고, 노드에서 패킷이 처리되는 서비스 시간은 10ms로 결정적(deterministic)이며, 노드에서 패킷이 출발하는 확률은 기하학적 분포를 따른다고 가정한다. 큐잉 시스템이 단일 노드로 구성되어 있다면, 활용률(ρ)은 노드가 busy한 시간적인 부분을 나타낸다. 단일 노드 큐에서 작업의 수에 제한이 없다면, 노드의 활용률은 다음과 같다. 패킷이 도착하는 시간 비율을 t라 하고, 서비스 시간을 x라 하면

$$\rho = ( 1 / t ) \cdot ( 1 / x ) = \lambda / \mu$$

이며, 시스템에서 n개의 패킷이 존재할 확률 Pn은

$$Pn = ( \rho )^{n} ( 1 - \rho )$$

이다. 그리고 시스템에서 평균 패킷의 수(L)는 다음과 같이 표현할 수 있다.

$$L = \rho / ( 1-\rho ) = \lambda / ( \mu - \lambda )$$

큐에서 대기하면서 소비되는 평균 시간 (Wq)은

$$Wq = ( \lambda ) / [ \mu ( \mu-\lambda ) ]$$

이며, 앞에서 가정한 모델에서의 전체 평균 시간(W)은

$$W = 1 / ( \mu - \lambda )$$

이다.

### 5.1.2 MPLS VPN과 IPSec VPN

VPN 모델들의 동작 및 특성을 관찰하고 성능을 분석하기 위해 다음과 같이 간단하면서도 유연성 있는 네트워크를 구성해 보았다.

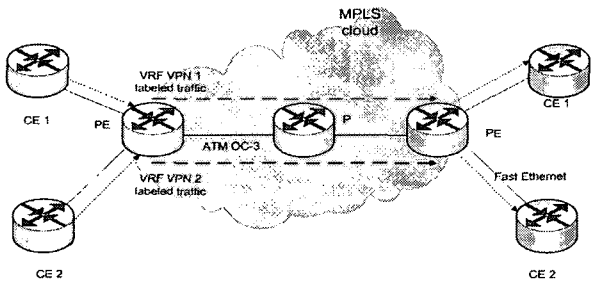


그림 9. 시뮬레이션을 위한 VPN 구성도.
Fig. 9. The VPN architecture for computer simulation.

그림 9에서 보면 코어는 OC-3 ATM 인터페이스로 연결된 3개의 라우터로 구성되어 있고, VPN의 단말이 되는 다른 라우터들)은 코어 라우터와 패스트 이더넷으로 연결되어 있다. 모든 연결에 있어서 고속의 인터페이스를 사용한 것은 광 통신망의 고성능 환경에 있어서 VPN의 동작과 확장성을 분석하기 위해서이다.

## 5.2 시뮬레이션 결과 및 검토

이 절에서는 MPLS VPN과 ATM VPN, MPLS VPN과 IPSec VPN으로 나누어서 성능평가 결과를 검토해 보기로 한다.

### 5.2.1 MPLS VPN과 ATM VPN

앞 절의 수학적 확률 모델을 컴퓨터 시뮬레이션하여 아래의 그림과 같이 MPLS 기반 VPN의 네트워크 성능에 대하여, 싱글 링크를 설정한 후 ABR(Available Bit Rate) 트래픽의 지연(delay)시간을 측정하여 ATM 기반 VPN의 측정치와 비교하여 네트워크의 효율성을 나타내었다.

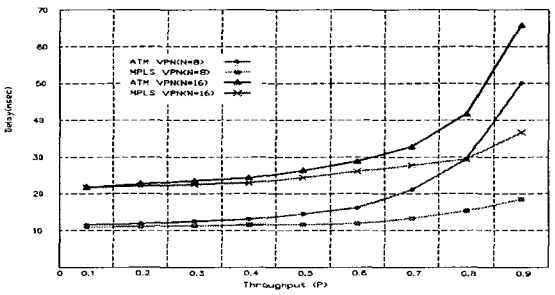


그림 10. MPLS VPN과 ATM VPN의 패킷 지연시간.
Fig. 10. Packet delay time for MPLS/ATM VPN.

그림 10은 네트워크 노드에서 입력 버퍼의 수(N)가 8, 16의 값을 갖는 경우에 대하여, 네트워크의 패킷 발생 비율을 나타내는 throughput(P)이 $0 \le P \le 1$의 범위를 가질 때, 이에 대한 지연시간을 나타내고 있다. 위의 성능평가 그래프를 살펴보면, N이 16인 경우, MPLS VPN과 ATM VPN 모두 throughput(P)이 0.6 이하일 때는 지연이 비슷하였으나, P가 0.6이상인 경우 즉, 네트워크 트래픽이 증가할수록 클래스 큐잉으로 우선순위가 높은 CBR 트래픽을 선행 처리하는 ATM VPN의 지연이 급증하는 반면에, FEC에 따른 VC 병합 기능을 가지고 우선순위가 낮은 ABR 트래픽에 대해서도 서비스 확률이 높아지는 MPLS VPN의 지연 값이 완만하게 증가함을 알 수 있다.

### 5.2.2 MPLS VPN과 IPSec VPN

그림 11와 그림 12은 여러 가지 크기의 패킷으로 ICMP(Internet Control Message Protocol) ping 테스트를 실시하여 RTT(Round Trip Time)와 패킷 손실을 측정한 결과이다.

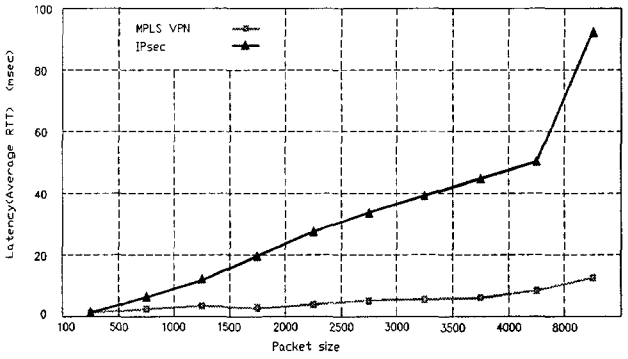


그림 11. 왕복전송시간.
Fig. 11. The round trip transmission time.

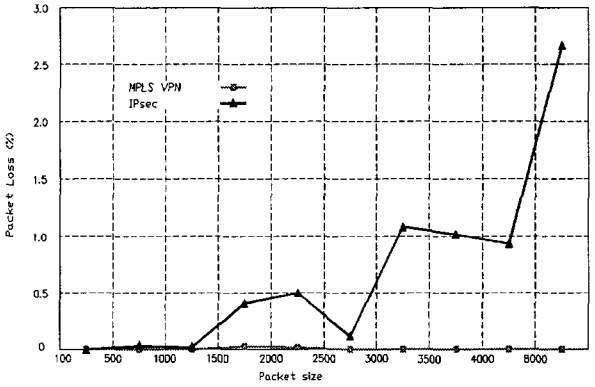


그림 12. 패킷 손실률.
Fig. 12. The packet loss ratio.

결과를 통하여 알 수 있듯이 MPLS VPN은 정상적인 패킷 라우팅과 같이 동작함을 알 수 있다. 이 것은 MPLS VPN의 경우 전송 메커니즘의 특성상 응답시간에 대해서는 오

버헤드가 없음을 나타내고 있다.

## Ⅵ. 결론 및 추후 연구과제

MPLS 망 기반의 VPN 제공 방안에서는 별도의 ID를 부여하여 터널링 없는 가상공간 할당으로 터널링이 주는 오버헤드와 네트워크 주소 변환이 필요 없기 때문에 인터넷 트래픽의 급증에 대응할 수 있는 효율적인 VPN 제공을 가능하게 한다. 본 논문에서는 MPLS 망의 동작을 위해 BGP를 이용하는 라우팅 프로토콜 관리부와 LDP를 이용하는 레이블 관리부를 포함하는 MPLS VPN의 동작 절차를 설계하였다. 이처럼 설계된 MPLS VPN은 라우팅 정보를 바탕으로 노드마다 주소 변환을 하지 않고 레이블 스와핑을 통해서 망제공자 네트워크의 경로를 설정하며, 확장성 및 IP 전송능력 등 MPLS의 장점을 그대로 수용할 수 있었다.

네트워크 노드(LSR)에서 입력 버퍼의 수 N을 변수로 하여 네트워크의 지연시간(delay)을 측정하여 성능을 분석한 결과, MPLS VPN은 네트워크의 트래픽이 많은 경우인 throughput(P)이 0.6이상일 때, 지연이 급격히 증가하는 ATM VPN에 비하여 상대적으로 지연이 완만하게 증가하였다, 따라서 성능평가를 통하여, MPLS VPN이 작은 버퍼로 셀 손실 없이 고속의 패킷 처리 능력을 갖으며 높은 네트워크 효율성을 갖는다는 것을 확인할 수 있었다. 더욱이 수요가 증가하고 있는 멀티미디어 서비스와 같이 트래픽이 상당한 경우 MPLS VPN의 라우팅 효율성이 우수함을 확인하였다. 또한 RTT, 패킷 손실, 처리율을 분석한 결과 MPLS VPN이 IPSec VPN에 비해서도 우수함을 알 수 있었다.

## 참 고 문 헌


[1] Jingdi Zeng, Nirwan Ansari, "Toward IP Virtual Private Network Quality of Service : A Service Provider Perspective", IEEE Communications Magazine, 2003

[2] Jeremy Lawrence, "Designing Multiprotocol Label Switching Networks", IEEE Communications Magazine, 2001

[3] Hosein F. Badran, "Service Provider Networking Infrastructures with MPLS", IEEE Communications Magazine, 2001

[4] I. Widjada, A. I. Elwalid, "Performance Issues in VC-Merge Capable Switches for Multiprotocol Label Switching", IEEE Journal on Selected Areas in Communications, 1999

[5] P. Knight, C. Lewis, "Layer 2 and 3 virtual private networks: taxonomy, technology, and standardization efforts", IEEE Communications Magazine, vol. 42, Jun. 2004



**신 태 삼**(Tae Sam Shin)
1995년 2월 건국대 전자공학과(공학사)
2004년 2월 건국대 대학원 전자공학과(공학석사)
2004년 ~ 현재 LG파워콤 네트웍 기술팀
관심분야 : 정보통신망, 차세대 인터넷, MPLS망

**김 영 범**(Young Beom Kim)
1984년 2월 서울대 전자공학과(공학사)
1986년 2월 서울대 전자공학과(공학석사)
1996년 8월 미 메릴랜드주립대(공학박사)
1997년 9월 ~ 현재 건국대학교 전자공학부 부교수
관심분야 : ATM, 통신망 트래픽 제어