論文2002-39TC-7-1

MPLS 기반 VPN 제공을 위한 설계 및 성능 분석

(Design and Performance Evaluation for VPNs based MPLS)

柳 泳 一 *, 田 炳 實 **

(Young-Eel Yu and Byoung-Sil Chon)

요 약

MPLS(Multi-Protocol Label Switching) 도메인의 경계에 위치하는 MPLS LER(Label Edge Router) 시스템은Ingress 또는 Egress 라우터로 동작하여 기존의 인터넷 망과의 접속 역할을 담당하는데, MPLS LER 시스템의 구성요소 중 포워딩 엔진(Forwarding Engine) 장치는 MPLS LER 시스템의 IP 패킷 처리 능력을 좌우하는 핵심적인 역할을 담당한다. MPLS 도메인 위에서 서비스가 이루어지는 가상 사설망(VPN)은 공공의 네트워크를 마치 자신의 사설망처럼 사용할 수 있고, MPLS LER 시스템의 성능에 따라 고 신뢰성 및 QoS 보장 등의 장점으로 인해 인트라넷 구축을 위한 최적의 수단으로 주목받고 있다. 본 논문에서는 전체 MPLS 도메인의 핵심적인 역할을 담당하는 MPLS LER 시스템의 라우팅 컨트롤러와 포워딩 엔진 장치 사이에서 효율적인 라우팅&포워딩 엔트리 제공 방안을 제안하고, 이를 기반으로 MPLS 망에서 IP VPN 지원 방안을 제안한다. 또한 제안한 방안에 따라 MPLS-VPN 서비스를 위해 MPLS-VPN 서비스 제어 기능부와 MPLS-VPN 동작 절차, VPN 그룹 구성 및 LSP 설정 절차를 설계한다.

Abstract

This paper proposes that an efficient routing entry sending method between routing controller FE. based on this method, we organize IP VPN support method based on MPLS network and design MPLS-VPN service control module, MPLS-VPN processing, VPN group configuration and LSP setup processing. We evaluate the performance about the VPN based on proposed MPLS, at the result of evaluation. We figure out that based on proposed IPC method, lost packets number reduces and delay increases more slowly in case of VPN based on MPLS comparing with the VPN based on ATM which has rapid delay increasement. Therefore we confirm that the VPN based on MPLS has high speed of packet processing and high utilization of buffers through the performance evaluation.

Keywords : VPN, MPLS, Label, 포워딩엔진, LER

* 正會員, 서울通信技術(주) 通信硏究所
(SEOUL COMMTECH CO., LTD.)
** 正會員, 全北大學校 工科大學 電子情報工學部
(Division of Electronic and Information Eng., Chonbuk Nat'l Univ.)
接受日字:2002年4月24日, 수정완료일:2002年5月30日

I. 서 론

인터넷은 세계를 연결하는 글로벌 네트워크로서 WWW 및 고성능 PC의 보급, 그리고 통신망의 발달로 보편적인 서비스로 형성되어 그 사용자만큼이나 데이터

트래픽 또한 급증하고 있다. 하지만 기존의 인터넷은 고속의 멀티미디어 트래픽의 사용자 요구를 만족시켜 주기에는 IP 전송 능력, 확장성, QoS 보장 등의 근본적으로 개선해야 할 문제점을 가지고 있다.

초기에 IP 제공의 기술로IPOA(IP Over ATM)의 오버레이 모델인 MPOA(Multi-Protocol Over ATM)이라는 기술을 표준화하였으나, 이 기술은 그 구현이 복잡하고 대형 네트워크로의 확장성 문제로 인하여 솔루션의 관심은 오버레이 모델에서 통합 모델로 옮겨가게 되었고, IETF에서 MPLS(Multi-Protocol Label Switching)라는 표준화된 기술을 완성하였다[1]. 또한 VPN(Virtual Private Network)은 공공의 네트워크를 마치 자신의 전용선처럼 사용할 수 있어 생산성 향상과 비용절감 효과를 얻을 수 있기 때문에 분산된 지사를 가지고 있는 기업의 네트워크를 구축하는데 있어 주목을 받고 있다.

기업의 인트라넷이 WAN을 통해 투명성 있게 확장하려면 경제적 효율성을 고려하여 IP VAN으로 진화되어야 하는데, 이는 터널링과 암호화 기법에 따른 오버헤드를 가져오며, 네트워크 제공자는 IP VAN의 단점인 복잡한 관리와 높은 오버헤드 문제를 안고 있어야 한다. 그러나 MPLS 기반의 VPN은 VPN ID를 부여하여 터널링 없는 가상 공간 할당으로 IP VPN의 문제점들을 해결하고 효율적인 서비스를 제공한다.

본 논문에서는 전체 MPLS 도메인의 핵심적인 역할을 담당하는 MPLS LER 시스템의 포워딩 엔진 장치에서 효율적인 라우팅&포워딩 엔트리 제공 방안을 제안하고, 이를 기반으로 MPLS 망에서 VPN 지원 방안을 제안한다. 또한 제안한 방안에 따라 MPLS-VPN 서비스를 위해 MPLS-VPN 서비스 제어 기능부와 MPLS- VPN 동작절차 및 VPN 가입자측에 대한 인터페이스를 설계하고 제안한 방안에 대하여 성능 평가를 수행하였다.

Ⅱ. MPLS와 VPN 연구

1. MPLS(Multi-Protocol Label Switching)

그림 1은 MPLS 망의 개념도를 보여주고 있는데, MPLS 포워딩 엔진에서는 일단 패킷이 MPLS 망에 들어올 때, "레이블(Label)"이라는 고정된 짧은 길이의 값으로 코딩된 FEC(Forwarding Equivalence Class)에 한 번만 할당되면 MPLS 망 내에서의 다음 경로는 이 레이블을 인덱스로 이용하여 간단히 설정될 수 있다. 그러므로 라우터에서 매번 패킷 헤더를 해석해야 하는 기존

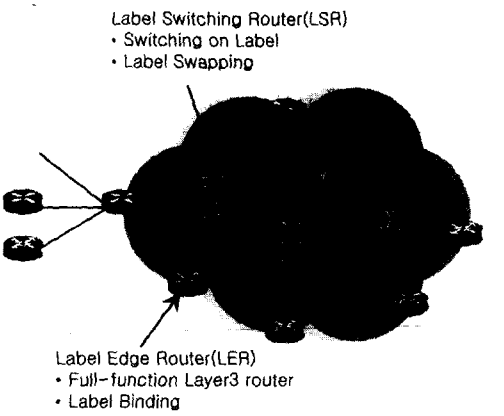


그림 1. MPLS 망의 개념도
Fig. 1. Concept of MPLS network.

의 인터넷 포워딩 방법에 비해 MPLS 포워딩 기술은 포워딩의 단순화, 서비스 품질 보장, 효율적인 라우팅 및 트래픽 엔지니어링 등의 장점이 있다.

1.1 포워딩 엔진의 구조 및 기능

MPLS LER 시스템에서 포워딩 엔진 장치는 IP 패킷을 처리하기 위해 가장 중요한 역할을 하는 부분으로 그림 2에서 보는 것처럼 크게 스위치 인터페이스부(SWIC), 셀 송/수신부(SARC_rx/tx), 패킷 메모리 및 제어부(PM/PMC/CMC), IP Lookup 제어부(IPLC) 및 Lookup 테이블을 저장하기 위한 데이터베이스(FIB/LIB)로 구성되어 있다.

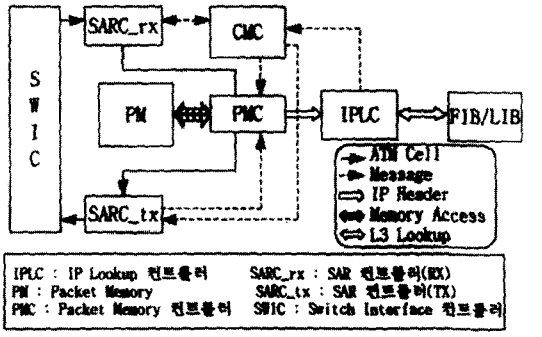


그림 2. 포워딩 엔진의 구조
Fig. 2. Forwarding Engine structure.

포워딩 엔진 장치의 주기능은 라인정합 장치를 통하여 입력되는 ATM 셀을 재조립하여 IP 패킷을 만들고, IP 패킷 헤더를 해석하여 목적지 주소에 따라 MPLS 망으로 전달하기 위한 레이블(VPI/VCI)을 할당한 후, 할당한 레이블을 이용하여 IP 패킷을 다시 ATM 셀로

분해하여 해당 출력포트로 송신한다. 한편 non-MPLS 망으로 송신되는 IP 패킷에 대하여 MPLS 망 영역에서 사용되던 레이블을 제거하고 다음 홉(Hop)으로 전달되기 위한 출력 포트를 결정하여 전달한다. 포워딩 엔진 장치는 라우팅 제어 프로세서와의 제어 메시지에 대하여 기본적으로 IPC(InterProcessor Communication) 형태로 송수신하여 포워딩 테이블을 생성, 유지하게 된다. MPLS LER로 수신되는 패킷의 목적지 주소를 분석한 후, 포워딩 테이블 Lookup에 의해 유입된 패킷을 다음 홉으로 포워딩하게 된다[2].

2. VPN(Virtual Private Network)

VPN은 기존의 인터넷 서비스에, 전송되는 data의 보안과 안전을 위한 Firewall/Authentication 장치/암호화 장치 등을 부착하여 외부사용자의 침입을 차단함으로써 기업의 전용사설 통신망처럼 사용하는 기술로서, 전송되는 Data는 기본적으로는 인터넷을 통하여 전송되어지나 그 외에도 전용회선, Frame Relay/ATM 링크 또는 ISDN 등의 망을 통해서 전송될 수도 있다. 현재VPN을 도입하는 주요한 이유는 다음과 같다.

① 통신 비용의 절감

② 익스트라넷을 위한 최적의 수단

③ 인터넷 이용과 WAN 접속과의 통합

그림 3은 VPN의 일반적인 서비스 요구 사항을 보이고 있다.

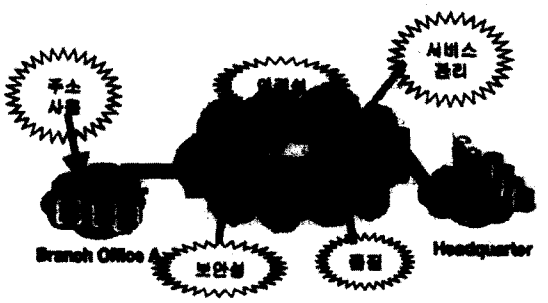


그림 3. VPN의 일반적인 서비스 요구 사항
Fig. 3. General VPN service.

Ⅲ. 효율적인 라우팅/포워딩 엔트리 제공 방안

1. MPLS LER 시스템의 라우팅 컨트롤러와 포워딩 엔진 사이의 IPC 방식

MPLS LER(Label Edge Router) 시스템에서 포워딩 엔진 장치는 라우팅 제어 프로세서와의 제어 메시지에 대하여 기본적으로IPC(InterProcessor Communication) 형태로 송수신하여 포워딩 테이블을 생성, 유지하게 된다[2].

Non-MPLS 망이 새로이 생성되거나 또는 기존의 망이 제거될 경우, 이에 대한 정보가 MPLS LER 시스템의 라우팅 제어 프로세서를 통해 포워딩 엔진에 업데이트 되어야 한다. 그러나 라우팅 제어 프로세서와 포워딩 엔진 사이의 IPC 통신 수단으로 인하여 방대한 양의 라우팅 정보가 수신될 경우, 모든 라우팅 정보를 포워딩 엔진에 전송하는데 상당한 시간이 걸리게 되어, 수신된 패킷의 목적지 주소를 Lookup하지 못하여 패킷을 폐기해야 하는 문제점이 발생하게 된다. 만약 프로세서가 새로이 유입된 라우팅 정보를 추가/삭제하는 과정에만 관여한다면, 포워딩 엔진에 라우팅 정보가 갱신되는 시간은 단축되지만, 스케줄링에 의해 수행되는 프로세싱이 하나의 특정 프로세서에게만 유지되어 다른 프로세서들이 수행되지 못한다. 결국 수신된 패킷에 대한 패킷 포워딩이 제대로 수행될 수 없게 된다. 이는 망의 효율성을 저하시키며 MPLS 망의 신뢰성을 떨어뜨리는 결과를 초래하게 된다.

아래 그림 4에 일반적인 IPC 전송 방식에 의한 라우팅 엔트리 송수신 과정을 보여주고 있다.

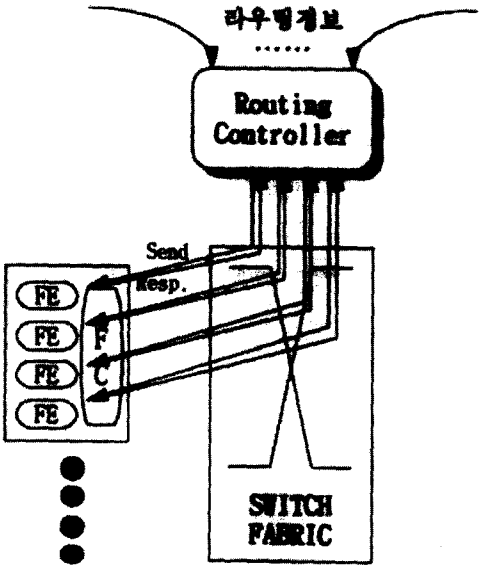


그림 4. MPLS LER 시스템의 라우팅 컨트롤러와 포워딩 엔진 사이의 라우팅 엔트리 제공
Fig. 4. MPLS LER's routing entry sending method between routing controller and FE.

2. 제안된라우팅 컨트롤러와 포워딩 엔진 사이의 IPC 방식

그림 4와는 달리 그림 5에서는 라우팅 컨트롤러의 부하를 줄이기 위해서 자원관리 모듈을 두어 라우팅 컨트롤러에서는 단순히 라우팅 정보를 수집하는 역할만하고, 자원관리 모듈이 이 라우팅 정보를 받아서 채널 정보와 레이블을 할당하여 포워딩 엔진에 IPC를 통해 송수신하게 된다.

일반적으로 라우팅 프로세서와 포워딩 엔진 사이에 라우팅 정보를 송수신하기 위하여 IPC를 보내고 이에 대한 응답을 받은 과정을 계속해서 반복하였다. 새로운 VPN Site가 추가 또는 제거되어 방대한 양의 라우팅 정보가 유입된다면, 라우팅 컨트롤러는 라우팅 테이블에 새로 추가해야 할 정보인지, 삭제해야할 정보인지를 구분하고, 포워딩 엔진에 송신하기 위해서 이 라우팅 정보를 가공하여 각각의 포워딩 엔진에 IPC를 통해 전송해야 한다. 따라서 라우팅 컨트롤러는 과부하 상태가 되고, 짧은 시간 동안에 모든 포워딩 엔진에 라우팅 정보를 내려주기 위한 IPC 송신 횟수도 많아져서 프로세서 독점 현상도 발생하게 된다.

제안된 IPC 송수신 방안에서는 라우팅 컨트롤러에서 라우팅 정보를 수신하면, 먼저 수신 정보가 새로운 라우팅 정보인지를 확인한다. 라우팅 엔트리 추가인 경우, 이 정보를 Total Entry Table에 저장하여 전체 라우팅 정보를 유지하고, 또한 추가 또는 삭제할 라우팅 정보를 저장하며 이를 포워딩 엔진에 내려주기 위하여 New

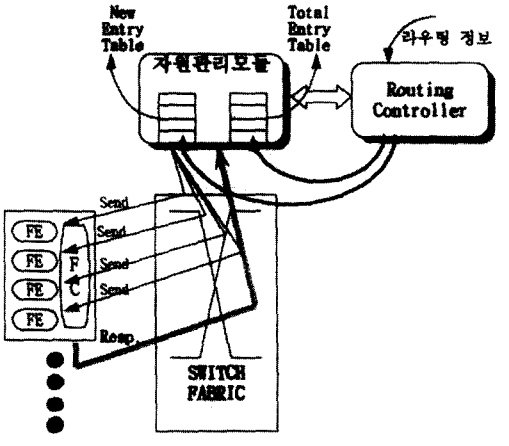


그림 5. 제안된 라우팅 컨트롤러와 포워딩 엔진 사이의 라우팅 엔트리 제공 방안

Fig. 5. Proposed routing entry sending method between routing controller and FE.

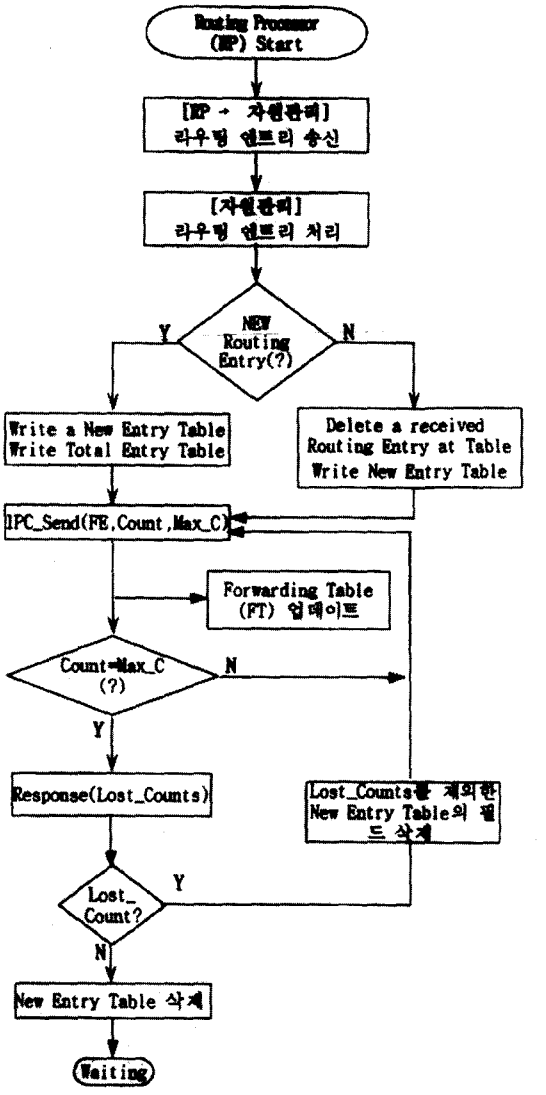


그림 6. 제안된 라우팅 컨트롤러와 포워딩 엔진 사이의 IPC 방식의 흐름도

Fig. 6. Flowchart of proposed IPC method between routing controller and FE.

Entry Table에 기록한다. IPC 메시지를 통해 라우팅 엔트리를 포워딩 엔진에 내려주기 위해 Max_C 파라미터와 Count 파라미터를 사용하였다. Max_C는 송신하고자 하는 전체 라우팅 엔트리의 수이고, Count는 Max_C 중에서 현재 송신하고 있는 라우팅 엔트리의 번호이다. 자원관리모듈에서 FE로 IPC 메시지를 통해서 라우팅 엔트리를 송신하게 되는데, Max_C와 Count 값이 같을 때까지 계속해서 IPC를 보내고 이에 따라 포워딩 엔진에 존재하는 포워딩 테이블을 업데이트 한다. Max_C와 Count 값이 같게 되면, 즉 새로이 추가된 모든 라우팅

엔트리 정보를 송신하게 되면 FE에서 자원관리모듈로 응답 메시를 보낸다. 이 응답 메시지 안에 손실된 IPC 번호를 나타내는 Lost_Counts 값을 실어 보내고, Lost_Counts에 해당하는 New Entry Table의 필드를 다시 IPC로 포워딩 엔진에 재전송한다. 이 때 Lost_Count에 해당하지 않는 New Entry Table의 모든 필드를 삭제한다.

라우팅 컨트롤러에서 보낸 정보가 라우팅 엔트리 삭제인 경우, 자원관리모듈의 Total Entry Table의 엔트리를 삭제하는 것을 제외하고는 라우팅 엔트리 추가의 경우와 동일하다.

Ⅳ. MPLS 기반 VPN 서비스 제공 방안

본 절에서는 VPN과 MPLS의 개념 및 동작을 분석하고, 이를 기반으로 MPLS 망에서 IP VPN 지원 방안을 제안한다. 또한 제안한 방안에 따라 MPLS-VPN 서비스를 위해 MPLS-VPN 서비스 제어 기능 블록과 MPLS-VPN 동작절차 및 VPN 그룹 구성 및 LSP 설정 절차를 설계한다.

1. MPLS-VPN 서비스를 위한 제어 기능부의 설계

MPLS에서 VPN 서비스가 제공되기 위해서는 LER (Label Edge Router) 시스템 내에 VPN 서비스를 지원할 수 있는 기능이 탑재되어야 하는데, MPLS-VPN 서비스 기능은 서비스/가입자 관리 및 제어 기능, VPN 사이트간 라우팅 기능, VPN LSP 제어기능, VPN FE 제어 기능, VPN Label 제어기능, VPN 패킷의 포워딩 기능의 여섯 종류의 기능으로 크게 구분된다. 이중 VPN 사이트간 라우팅 기능은 라우팅 기능 블록에서 제공되며, VPN 패킷의 포워딩 기능은 하드웨어로 실현된다.

그림 7은 VPN 서비스 제어 기능부의 구성도를 보여주고 있다. 이 VPN 서비스 제어 기능부는 크게 Operation Layer, Control Layer, Interface Layer로 나뉘며, Control Layer는 두 개의 Sublayer로 나누어진다.

첫째, Operation Layer의 MPLS 운용/관리부는 VPN 서비스의 Provisioning(구성관리)&Operation을 위한 운용자 명령어의 처리 및 모니터링, 가입자 정보의 관리와 VPN 서비스를 위해 요구되는 주요 Configuration 데이터(VPN Name, RD, RT 등)의 할당 및 관리를 총괄한다.

둘째, Control Layer의 상위에 위치하는 VPN 서비스 제어부는 VPN 그룹에 대한 구성관리, VPN 그룹에 대한 라우팅&포워딩 테이블의 구성 기능을 처리한다. 이를 위해서 VPN 서비스에 대한 제어 기능 블록(VPN Control Function Block)과 VPN 사이트의 라우팅 정보 분배를 위한 BGP4+ 기능 블록(BGP4 Function Block)으로 구성된다. 그리고 하위에 위치하는 VPN 연결 제어부는 VPN 그룹에 대한 LSP의 설정 기능을 처리한다.

셋째, Interface Layer에 위치하는 VPN 전송부는 VPN을 위한 포워딩 테이블의 구성과 포워딩 엔진의 동작을 제어한다. VPN 전송부는상위의 VPN 연결 제어부로부터 VPN 사이트에 대한 라우팅 및 포워딩 정보를 받아서 이를 포워딩 테이블에 반영하는 제어 기능을 수행하고, 데이터를 포워딩하기 위해서 VPN용 포워딩 테이블을 하드웨어 단에 직접 작성하는 절차를 처리한다.

아래 그림 7은 MPLS-VPN 서비스를 위한 제어 기능 구성도와 흐름도를 나타낸다.

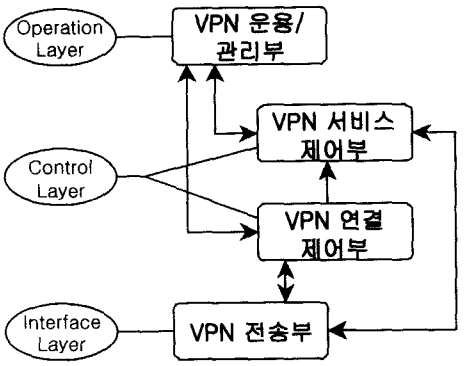


그림 7. VPN 서비스 제어 기능부의 구성도
Fig. 7. Configuration of VPN service control module.

2. MPLS-VPN 동작 절차 설계

MPLS에 기반하는 VPN 지원 방안은 MPLS 에지 라우터에 연결된 VPN에 VPN ID를 할당하고 이를 라우팅 정보에 포함시켜 MPLS내에서 유일한 주소를 가지고 각 노드마다 네트워크 주소 변환(NAT : Network Address Translation)을 하지 않고 목적지로 레이블을 스와핑을 통하여 패킷을 전달하는 동작을 수행한다.

VPN을 지원하는 MPLS의 동작 절차를 간략히 정리하면, VPN ID를 부여하여 VPN-IP 주소를 생성하고, VPN 라우팅 정보를 배포하고, 레이블과 VPN-IP 주소를 맵핑하여 NAT 없이 제공자 네트워크에서 유일한 주소를 제공한다. 이러한 라우팅 정보를 가지고 네트워크 내 포워딩 경로를 설정하여 VPN 간에 통신을 설정하게 된다. 그림 8은 MPLS 망에서 VPN을 지원하는 동작 절차의 흐름도이다.

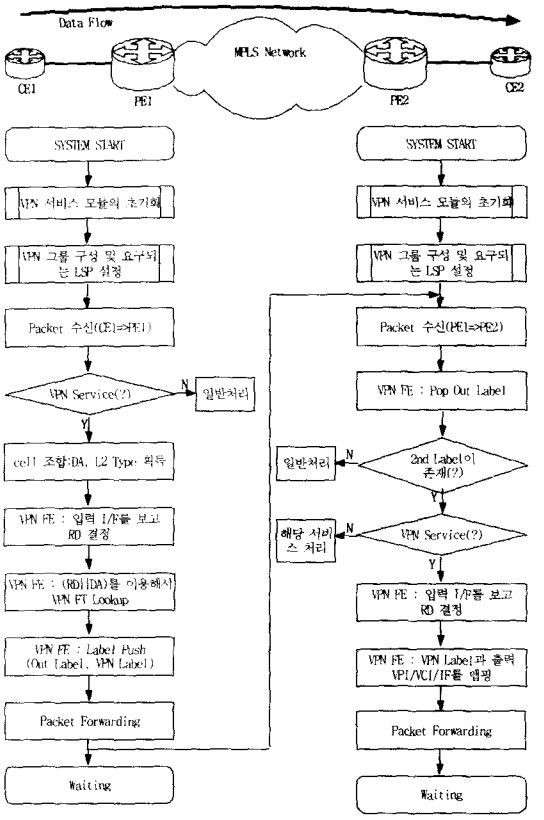


그림 8. MPLS-VPN의 동작 절차 흐름도
Fig. 8. Flowchart of MPLS-VPN process.

그림 8에서 패킷을 수신한 Ingress LER은 수신된 패킷이 VPN용인지 검사를 한다. VPN용 패킷인 경우, 입력되는 인터페이스를 이용해서 RD(Route Distinguisher)를 결정하고, (RD(1) || IPv4(3))를 이용해서 VPN 포워딩 테이블을 lookup한다. 포워딩 테이블의 lookup을 통해서, MPLS 망 내에서 경로를 나타내는 MPLS Label과 Egress LER에서 CE(Customer Edge Router)까지의 경로를 결정하는 VPN Label을 얻을 수 있다. MPLS 레이블을 이용해서 Egress LER(PE2)까지 도달한 패킷들은 VPN 레이블을 통해서 CE까지의 경로를 결정한다.

3. VPN 그룹의 구성 및 LSP 설정 절차

그림 9는 VPN 그룹 구성 및 LSP 설정 절차를 보여주고 있는데, 새롭게 VPN에 가입하는 가입자에 대해서 VPN 그룹에 대한 정보를 입력하고, VPN에 속하는 사이트에 대한 정보를 입력한다. 이때 각 사이트간의 QoS를 지정하고, RD 및 RT에 관한 정보를 각각 입력한다. 또한 라우팅 프로토콜(BGP4+)은 라우팅 정보를 바탕으로 라우팅 테이블을 작성한다. VPN 가입자가 어떤 서

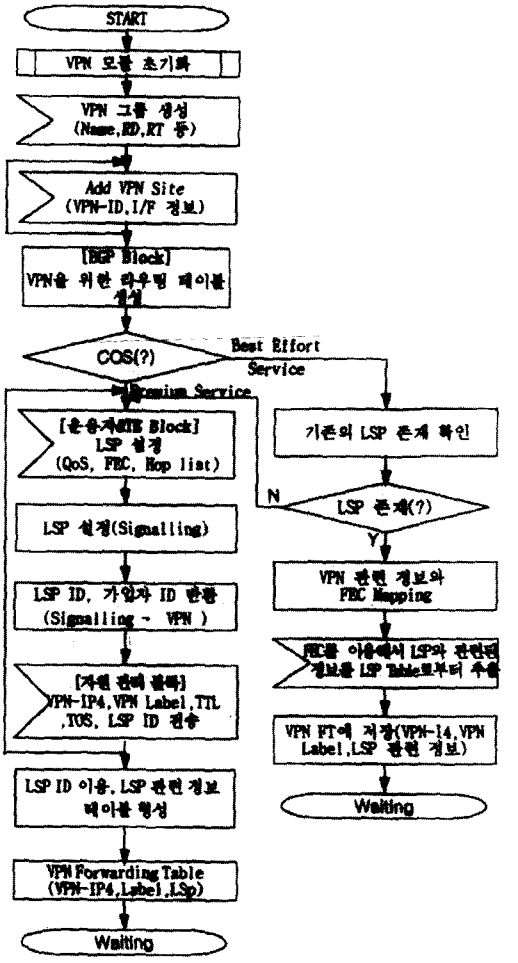


그림 9. VPN 그룹 구성 및 LSP 설정 절차 흐름도
Fig. 9. Flowchart of VPN Group and LSP process configuration.

비스에 가입했는가에 따라서 Best Effort용 LSP를 설정할 것인지, 아니면 Premium 서비스용 LSP를 설정할 것인지를 결정한다. Best Effort Service를 요구하는 경우에는 기존에 설정된 Best Effort용 LSP를 공유할 수도 있다.

V. 성능평가

패킷이 인터넷을 통해 가는 경로가 대기 시간을 결정하는데, 라우팅 효율성에 영향을 미치는 중요한 요인으로 네트워크 성능(Throughput)과 지연(Delay)등이 있다. 본 논문에서는 MPLS-VPN을 모델링 한 후, 네트워크 성능에 따른 지연 시간과 VC-Merging에 요구되는 버퍼 크기를 수학적 모델링을 통해서 분석하고, 또한 시험

장비와 MPLS LER 시스템으로 시험망을 구성하여 제안한 IPC 방식과 일반적인 방식의 성능을 비교 분석하였다.

1. 성능 평가를 위한 모델링과 수학적 분석

본 논문에서 성능 평가를 위한 MPLS 기반의 VPN은 그림 10과 같은 모델을 갖는다.

MPLS 도메인의 각 MPLS LER은 싱글 FIFO(First In First Out) 출력 버퍼에 풀 머지 한다고 가정한다. 이는 주어진 패킷의 셀은 다른 패킷의 셀과는 간섭하지 않는다는 의미이다. 출력 포트의 셀 도착 프로세스는 독립 ON-OFF 프로세스 N 상태로 모델링 할 수 있으며, N개의 입력 포트로부터 각각 들어온다. 입력 셀은 싱글 패킷으로 ON 주기 안에 있으며, OFF 주기 동안 슬롯은 휴지상태이다. 즉 ON 주기 동안에 셀인 연속적으로 전송되고 OFF 주기 동안에는 어떠한 셀도 발생하지 않는다. 그리고 ON과 OFF 주기 모두 각 입력 포트로부터 같은 트래픽 파라미터들이 기하학적 분배되는 것을 가정하며 그림 11과 같이 도착 프로세스를 각 버퍼에 IBP (Interrupted Bernoulli Process)로 모델링 할 수 있다.

IBP는 On 주기 동안 생성되는 셀들은 슬롯당 평균이 λ인 Bernoulli Process를 따른다.

P매 단위 시간마다 OFF에서 ON로 옮겨갈 확률 = α.

P매 단위 시간마다 ON에서 OFF로 옮겨갈 확률 = β.

P매 단위 시간마다 ON 상태에 머무를 확률 = $1-\alpha$.

그림 10. 성능 평가를 위한 네트워크 모델링
Fig. 10. Network modeling for performance evaluation.

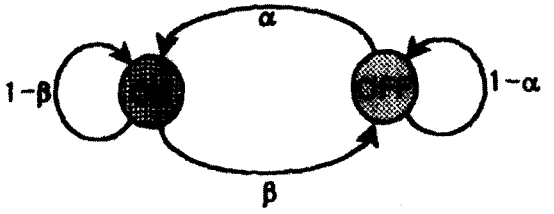


그림 11. ON-OFF 도착 프로세스 모델
Fig. 11. ON-OFF Process Model.

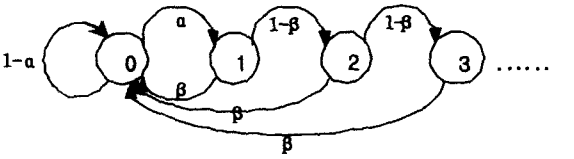


그림 12. Markov 천이 다이어그램
Fig. 12. Markov chain Diagram.

P매 단위 시간마다 OFF 상태에 머무를 확률 = $1-\beta$.

본 논문에서는 Markov chain을 근거로 수학적 함수를 도출하여 네트워크 성능 평가를 수행하였다. 여기서 OFF 주기일 때는 버퍼의 내용은 0 이어야 하며, chain이 처음 ON 상태로 변화할 때 버퍼의 내용은 1이 된다. 그림 12는 위와 같은 특징을 갖는 네트워크를 Markov 천이 다이어그램으로 나타낸 것이다.

IBP와 Markov 모델링을 바탕으로 아래와 같은 확률을 얻게 된다.

$$P_n = P\{N\text{개의 입력 트래픽 중에서 n개가 ON일 확률}\} = \binom{N}{n}\left(\frac{\alpha}{\alpha+\beta}\right)^n\left(\frac{\beta}{\alpha+\beta}\right)^{N-n}$$

$$P_{i,j} = P\{\text{상태}(i, j \rightarrow i', j')\text{로의 천이 확률}\} = \binom{N-i}{j}\alpha^j(1-\alpha)^{N-i-j}$$

X를 Cell들의 도착 시간 간격이라 하고, X_{off}는 OFF 상태에 있는 기간이라 하면,

$$X^d = \begin{cases} 1 \\ 1+X \\ 1+X_{off}+X \end{cases} \qquad X_{off} = \begin{cases} 1 \\ 2 \\ \vdots \\ K(=\text{상수}) \end{cases}, \quad \text{이다.}$$

따라서 평균 소비 시간은

$$E(X) = (1-\beta)\lambda + (1+E(X))(1-\beta)(1-\lambda) + (1+\frac{1}{\alpha}+E(X)\beta = \frac{\alpha+\beta}{\lambda\alpha(1-\beta)} \quad \text{이다.}$$

G/M/C(C=1)은 서비스 시간이 지수 분포를 갖고, 도착 과정은 갱신 과정을 따르는 대기 체제의 모델로서, C=1인 1개의 서버를 나타내고 있다. 이 모델은 n개의 패킷이 서비스를 받고 있을 때, 도착한 패킷이 서비스를 받기 위해 큐에서 대기하는 시간의 확률 밀도 함수를 이용해서 패킷 스위칭 망이나 셀 릴레이 스트림을 제공하는 망에서 응용되고 있다. 본 논문에서 고려한 G/M/C(C=1) 모델은 패킷 발생 확률로서 포아송 분포를 따르

고, 노드에서 출발하는 확률은 기하분포를 따른다고 가정한다. 또한 도착하는 패킷들에 FIFO Queuing 방법을 적용한다.

위와 같은 조건 아래에서 패킷이 도착하는 시간 간격을 t라 하고, $\lambda = 1/t$를 도착률, μ을 서비스율, 서비스 시간을 x 라 하면, 활용률($\rho = E$[도착간격 시간 동안에 서비스 되는 패킷의 수]

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

평행 상태에서 임의 시각에 시스템 내에 n개의 패킷이 존재할 확률은 $P_n = (\rho)^n(1-\rho)$ 이다.

G/M/1 대기 체제에서 도착 시점에서의 시스템의 크기의 분포는 기하분포이므로 큐 내에서 대기시간 W_q의 분포함수 $W_q(x)$는 다음과 같이 얻는다.

$$W_q(x) \equiv P\{W_q \le x\} = \begin{cases} 1-\rho, & t = 0 \\ 1-\rho e^{-\mu(1-\rho)t}, & t \ge 0 \end{cases}$$

또한 큐 내에서 대기하면서 소비되는 평균 시간은 다음과 같이 얻을 수 있다.

$$E(W_q) = \sum_{k=0}^{\infty} E\{\text{큐 내에있는 시간} \mid \text{도착 순간에 시스템 내에 k개의 패킷}\} \cdot P\{\text{도착 순간에 시스템내에 k개의 패킷}\}$$

$$= \sum_{K=0}^{\infty} \frac{K}{\mu}(1-\rho)\rho^K = \frac{\rho}{\mu(1-\rho)}$$

$$= \lambda/[\mu(\mu-\lambda)] \qquad \text{식(1)}$$

따라서 전제 평균 소비 시간은 $W=1/(\mu-\lambda)$ 이다. 여기서 $E(W_q)$(평균대기 시간)을 최소화시키는 도착 과정은 Folk의 정리에 의해서 도착간격분포가 상수일 때이다.

셀이 큐에서 대기해야한다는 가정 하에서 큐 내에서의 조건부 대기 시간의 확률분포 $W_q(y \mid$ 큐에서 기다려야 함)을 구하여 보면, 셀이 대기해야한다는 가정 하에서 셀이 도착하여 시스템의 크기가 (n+c)일 확률은 $(1-\sigma)\sigma^n$로 주어지고, 이 때 도착한 셀이 서비스를 받으러 들어갈 때까지는 (n+1)개의 셀이 서비스를 받고 시스템을 빠져나가야 한다. 따라서 큐 내에서의 조건부 대기 시간은 매개변수 $c\mu$를 갖는 지수분포가 (n+1)개의 독립적인 합으로 나타난다.

$\tilde{W}_q(s|n)$를 큐의 길이가 n이라는 가정 하에 W_q의 Laplace 변환으로 정의하면 $\tilde{W}_q(s/n) = (\frac{c\mu}{s+c\mu})^{n+1}$, $\sum_{n=0}^{\infty} \tilde{W}_q(s/n)(1-\sigma)\sigma^n = (1-\sigma\frac{c\mu}{s+c\mu+c\mu\sigma})$이 되고, 역 Laplace 변환을 취하면, 기다려야 한다는 조건 하에서 큐 내에서의 조건부 확률밀도함수는 다음과 같이 구해진다.

$$\tilde{W}_q(s|\text{기다려야 함}) = (1-\sigma)c\mu e^{-c\mu(1-\sigma)y}.$$

그리고 G/M/C(=1) 대기 체제에 관한 중요한 성능 중에 하나인 큐의 길이에 관한 식을 구해보면, 셀이 도착했을 때 큐에서 기다릴 확률은

$P\{\text{도착한 셀이 큐내에 기다림}\} = \sum_{k=c}^{\infty} K\rho^k = \frac{K\rho^c}{1-\rho}$ 이며, 셀이 큐 내에 기다려야 한다는 가정 하에서 큐의 길이가 n일 조건부 확률은

$$P = \{\text{큐의 길이} = n \mid \text{고객이 큐내에 기다려야 함}\} = \frac{r_{c+n}}{P\{\text{고객이 기다려야 함}\}} = \frac{K\rho^{n+c}}{\frac{K\sigma^c}{1-\rho}} = (1-\rho)\rho^n, \quad n \ge 0. \qquad (2)$$

이다. 따라서 G/M/C 대기체제에서 셀이 기다려야 한다는 가정 하에서 조건부 큐의 길이 분포는 기하분포를 따른다.

2. 성능 분석 및 검토

1절에서 식(1)을 바탕으로 수학적 확률 모델링을 컴퓨터 시뮬레이션하여 MPLS 기반 VPN의 네트워크 성능(Throughput)에 대하여, Single Link를 설정한 후 CBR과 ABR 트래픽이 폭주 상태의 링크를 통과할 때, ABR 트래픽의 지연(Delay) 시간을 측정한 참고문헌 7의 ATM 기반 VPN의 측정치[7]와 동일 조건 하에 네트워크 효율성을 그래프로 비교하였다.

그림 13은 네트워크 노드에서 입력 버퍼의 수(N)가 8, 16를 갖는 경우에 대하여, 네트워크 패킷 발생 비율을

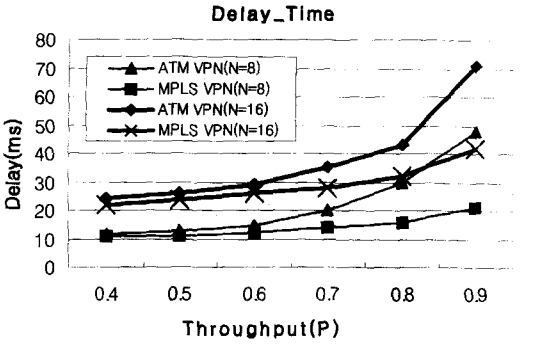


그림 13. 부하에 따른 MPLS VPN과 ATM VPN의 패킷 지연시간

Fig. 13. Delay time of MPLS VPN and ATM VPN packet for load.

나타내는 Throughput(P)이 0.4≤P≤1의 범위를 가질 때, 이에 대한 지연 시간을 나타내고 있다. 위의 성능 평가 그래프를 보면, N=8/16인 경우, MPLS VPN과 ATM VPN 모두 Throughput(P)이 0.6이하일때는 지연이 비슷하였으나 P가 0.6이상인 경우 즉 네트워크 트래픽이 증가할수록 Class Queueing으로 우선순위가 높은 CBR 트래픽을 선행 처리하는 ATM VPN의 지연이 상당히 급증하는 반면에, FEC에 따른 Merging으로 우선순위가 낮은 ABR 트래픽도 서비스 확률이 높아지는 MPLS VPN의 지연 값이 완만히 증가하고 있음을 알 수 있다. 따라서 음성 및 비디오 스트림 등의 멀티미디어 서비스와 같이 네트워크의 트래픽이 상당한 경우 트래픽의 큐 대기 시간이 증가하여 셀 손실이 발생할 확률이 커지게 되어 네트워크의 처리량을 감소시키게 된다.

오른쪽 그림 14는 5.1절의 식(2)에서 P=0.5, 평균 도착 시간 간격=4.24[μs], μ(서비스율)= 150 Mbps, N=8/16인 경우에 부하에 대한 큐의 길이(n)를 보이고 있다.

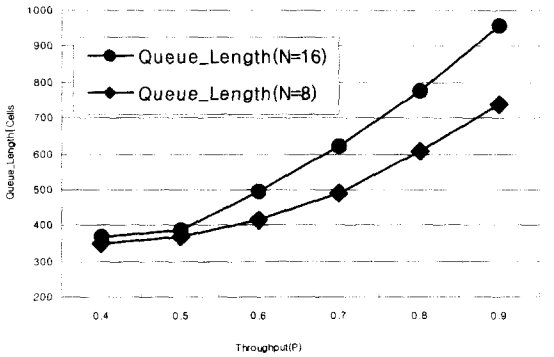


그림 14. 부하에 따른 MPLS VPN에 대한 버퍼의 길이
Fig. 14. Buffer length of MPLS VPN for load.

위 결과에서 알 수 있듯이 MPLS 기반 VPN은 부하가 0.9일 때, 버퍼의 크기가 약 1000이면 셀 손실 없이 모든 셀들을 서비스할 수 있다. 일반적으로 VC Merging을 위해 필요한 메모리가 수 Mbyte임을 감안할 때, 결론적으로 MPLS 기반의 VPN은 상대적으로 작은 지연과 버퍼로 고속의 라우팅 효율성을 갖음을 확인할 수 있다.

2. 시험 장비와 MPLS LER 시스템으로 구성된 시험망에 대한 성능 분석 및 검토

본 논문에서 라우팅 컨트롤러와 FE 사이의 라우팅 엔트리 제공에 대한 성능 평가를 위한 MPLS 기반의 VPN에 그림 16과 같은 환경을 구축하였다. 그림 16에서

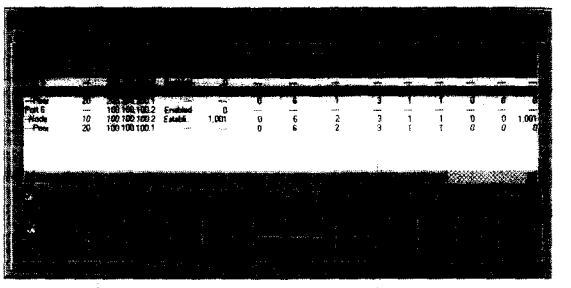


그림 15. AX-4000 시험 장비를 사용하여 BGP 라우팅 엔트리 생성
Fig. 15. BGP routing entry generation using AX-4000 generator.

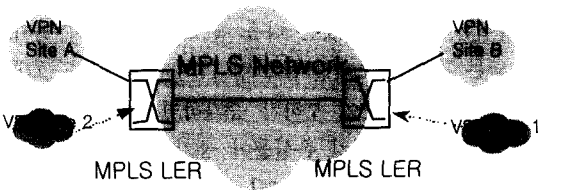


그림 16. MPLS LER과 시험 장비를 이용한 시험망 구성도
Fig. 16. MPLS-VPN network using MPLS LER and AX-4000.

MPLS LER 시스템은 ACE2000 SYSTEM이고, VPN Site는 ADTEC사의 AX-4000이라는 시험 장비를 사용하였다. AX-4000 시험 장비에서 그림 15와 같이 BGP 라우팅 엔트리 2000개를 발생한다. 또한 시험 장비에서 부하(0.4≤P≤1)에 따른 데이터 패킷을 발생시켜 VPN Site A에서 VPN Site B로 데이터를 보낼 때, MPLS LER에서 손실된 패킷의 수를 측정하였다.

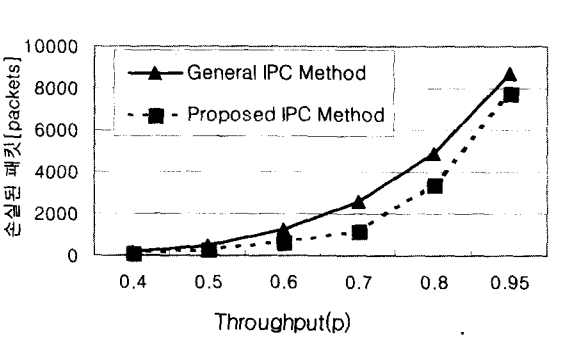


그림 17. 부하에 따른 제안된 IPC 기법과 일반적이 IPC 기법에서 손실된 패킷의 수
Fig. 17. Lost packet of proposed IPC method and general IPC method for load.

위의 그림 16과 같이 VPN Site 1, 2가 추가되고 VPN Site A와 B의 패킷 발생 비율을 나타내는 Throughput(P)이 $0.4 \le P \le 1$의 범위를 가질 때, MPLS LER 시스템에서 제안된 라우팅 엔트리 제공 방안과 일반적인 라우팅 엔트리 제공 방안을 적용한 경우, 이에 대한 패킷 손실률을 그림 17에서 나타내고 있다.

그림 16과 같이 VPN Site가 추가되었을 때, 이 Site에 대한 모든 라우팅 정보가 MPLS LER 시스템의 포워딩 엔진에 전송되면서 실제 데이터 패킷을 처리하는 과정에 새로운 Site에 대한 라우팅 정보가 미쳐 포워딩 엔진에 내려오지 않아서 데이터 패킷에 대한 라우팅 Lookup을 하지 못하게 된다. 즉 MPLS LER 시스템으로 들어온 데이터 패킷은 다음 홉으로 전송되지 못하고 폐기되는 결과를 초래한다. 그림 17의 성능 평가 그래프에서도 알 수 있듯이 부하가 증가하면서 일반적인 IPC 송수신 기법에서 패킷 손실률이 증가한다. 하지만 과부하(P=0.95) 상태에서는 데이터 처리에 대부분의 프로세싱이 이루어져서 제안된 기법에서도 월등한 성능 향상을 보이지 못하고 있다.

네트워크 부하가 $0.6 \le P \le 0.8$ 일 때, 제안된 기법의 성능 향상이 두드러짐을 확인할 수 있는데, 이는 데이터 패킷을 전송하면서도 포워딩 엔진에 라우팅 엔트리를 송수신하는 프로세서를 스케쥴링할 수 있는 기회가 많기 때문이다.

VI. 결론 및 향후 과제

본 논문에서는 MPLS LER 시스템에서 라우팅 컨트롤러와 포워딩 엔진 간에 IPC 통신 방식을 제안하였으며, 이를 바탕으로 MPLS 망에서 VPN을 지원하는 방안을 제시하였다. 제안한 방안에 대해 MPLS VPN 서비스를 지원하기 위한 서비스 제어 기능부의 구성도, VPN 그룹 구성 및 LSP 설정 절차, 가입자 인터페이스를 설계하고, 이를 토대로 MPLS 망에서 VPN 지원 방안의 동작 절차를 설계하였다.

제안한 MPLS LER 시스템의 IPC 통신 방식에 대해 시험장비(AX-4000)와 ACE2000 교환기로 시험망을 구성하여 VPN Site 추가에 따른 성능평가를 수행하였는데, 부하가 증가할수록 제안된 방식에서 손실된 패킷의 수가 현저히 줄어들었음을 확인할 수 있었다. 또한 MPLS 기반의 VPN 제공을 위한 네트워크 모델에 대해 수학적 모델링과 분석을 한 후, 컴퓨터 네트워크 성능 평가를 수행하여, 네트워크 노드에서 입력 큐의 수 N을 변수로 하여 네트워크 처리 지연시간과 버퍼의 길이를 측정하였다. 성능 분석 결과 기 제안된 ATM 기반 VPN[7]에 비하여 상대적으로 완만하게 지연이 증가하였고, 작은 버퍼로 셀 손실없이 고속의 패킷 처리 능력과 높은 네트워크 효율성을 갖는다는 것을 확인할 수 있었다.

본 논문에서 설계 및 제안한MPLS 망 기반 VPN 제공 방안은 국내에서도 인터넷 솔루션으로 도입한 MPLS의 응용 서비스로써, 현재 진행 중인 초고속 국가망 위에 신뢰성이 높고 확장성 있는 가상 사설망의 기초 자료로 활용 될 수 있을 것이다. 또한 향후 과제로 멀티 캐스트 지원 및 트래픽 엔지니어링에 대하여 MPLS VPN에서 해결해야 할 연구가 계속되어야 할 것이다.

참 고 문 헌

[1] R.Callon, P.Doolan, N.Feldman, A.Rfrdette, G.Swallow, A.Viswanathan, "A Framework for MultiProtocol Label Switching", draftietf-mpls-framework-02.txt, IETF, Nov. 1997.

[2] 류호용, 이재섭, 임준목, 서재준, "MPLS망에서의 포워딩 엔진에 대한 성능 분석", IE Interface, Vol.14, No.3, pp.263-271, Sep. 2001.

[3] 정윤희, 최희숙, 손승원, "인터넷에서 VPN 제공 기술 및 동향에 대한 연구" 주간기술동향 제 898 호, 1999.6.

[4] Juha Heinanen, Telia Finland, "VPN support with MPLS", draft-heinanen-mpls-vpn-01.txt, IETF, Sep. 1998.

[5] D.Jamieson, B.Jamoussi, G.Wright, P.Beaubien, "MPLS VPN architecture", draft-jamieson-mpls-vpn-00.txt, MPLS Working Group, Aug.2000.

[6] E. Rosen, Y. Rekhter, RFC 2547, "BGP/MPLS VPNs", March, 1999.

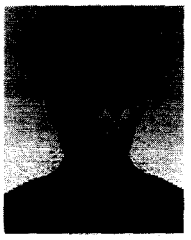
[7] Carols M.Pazos, Mario Gerla, "ATM Virtual Private Networks for Internet Multimedia Traffic", IEEE International Conference on Comm., ICC'98, 1998.

[8] Gary N. Higginbottom, "Performance Evaluation of Communication Networks", Artech House, 1998.

[9] 박석천, "MPLS 망에서 인터넷 VPN 제공 방안", 멀티미디어학회 논문지 제3권 제 2호, 2000.4

[10] 홍현석, 이동원, 김영철, 이귀상, 최덕재, "ATM 기반 MPLS 망에서 실시간 서비스를 제공하기 위한 레이블 통합에 관한 연구", 전자통신기술 논문지 제 3권 제 1호, 2000. 12

저 자 소 개



柳 泳 一(正會員)

1993~1999년 : 전북대학교 전자공학과 졸업(공학학사). 1999~2001년 : 전북대학교 전자공학과 졸업(공학석사). 2001.4~현재 : 서울통신기술(주) 통신연구소 연구원. <주관심분야 : ATM 중계호처리/트래픽 제어, MPLS LDP/VPN>

田 炳 實(正會員) 第39卷 TC編 第4號 參照