2000년 한국정보처리학회 추계 학술발표논문집 제7권 제2호

# MPLS를 이용한 VPN 기능 모델 설계

윤호선, 김숙연, 양선희
한국전자통신연구원 교환.전송기술연구소
e-mail : yhs@etri.re.kr

# Functional Design for MPLS VPN Model

Ho-Sun Yoon, Sook-Yeon Kim, Sun-Hee Yang
Electronics and Telecommunications Research Institute
Switching & Transmission Technology Lab

**요 약**

VPN 서비스는 인터넷과 같은 공중망을 이용하여 사설 전용망이 갖는 사용자 폐역화와 같은 기능을 제공한다. 이러한 VPN 서비스는 기업 생산성과 비용 절감 측면에서 우수한 평가를 받고 있지만, 안전성을 위한 오버헤드의 증가 및 관리의 복잡성과 같은 문제점들이 대두되고 있다. 본 논문에서는 QoS(Quality of Service)를 보장하는 MPLS VPN 서비스를 구현하기위해 설계된 모델을 제시한다.

## 1. 서론

VPN 서비스는 공중망과 사설망이 갖는 장점을 고루 갖춤으로써, 그 수요가 크게 증가하고 있다. 반면에 데이터 암호화 및 사용자 인증과 같은 터널링 기법을 위한 오버헤드의 증가 및 관리의 복잡성과 같은 몇몇 단점들이 존재한다. 특히, IPSEC을 이용한 VPN 서비스인 경우, 암호화 기법을 이용함으로써 안전성은 크게 증가한 반면에 암호화 처리를 위한 오버헤드와 계산을 위한 부하의 증가가 큰 문제로 지적되고있다.

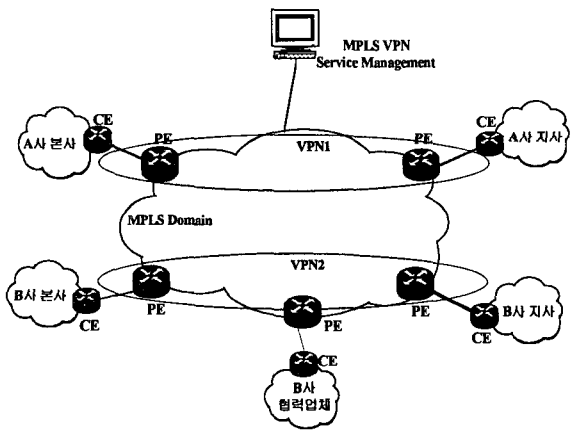
새롭게 대두되고 있는 MPLS VPN 서비스는 다양한 QoS 를 지원하면서 추가적인 오버헤드 없이 레이블 스와핑(Label Swapping)을 이용한다. MPLS VPN 은 사용자 폐역화를 위해서 라우팅 정보를 제한적으로 수용하는 방법을 사용한다. 이러한 방식의 사용은 사용자를 선택적으로 수용하면서 오버헤드에 대한 부담을 줄일 수 있다.

본 논문에서는 MPLS VPN 구현을 위한 기능 모델을 제시하고, 기능 블록별 역할 및 기능 블록간의 인터페이스에 대해서 기술한다. 본 논문에서 기술한 MPLS VPN 모델은 ACE 2000 교환기에 탑재하기 위한 것이다.

## 2. *MPLS VPN 개요*

MPLS 는 고속성뿐만 아니라 QoS 를 지원하는 큰 장점을 가지고 있다. QoS 를 지원하는 MPLS 의 장점을 VPN 서비스에 적용한 것이 MPLS VPN 의 큰 특징이다. 이러한 MPLS VPN 은 QoS 지원 및 효과적인 사용자 폐역화를 가능하게 한다.

그림 1 은 MPLS VPN 의 네트워크를 개략적으로 도식화한 것이다.




[그림 1] MPLS VPN Network

그림 1 에서, VPN1 과 같이 같은 기업체내의 VPN 을 Intranet VPN 이라 하며, VPN2 에서와 같이 동일한 기업체뿐만 아니라 협력 업체가 존재하는 경우에는 Extranet VPN 이라 한다. 또한 개개인들과 기업 인트라

넷 사이의 원격 액세스를 위한 VPN 을 Access VPN 이라 한다.

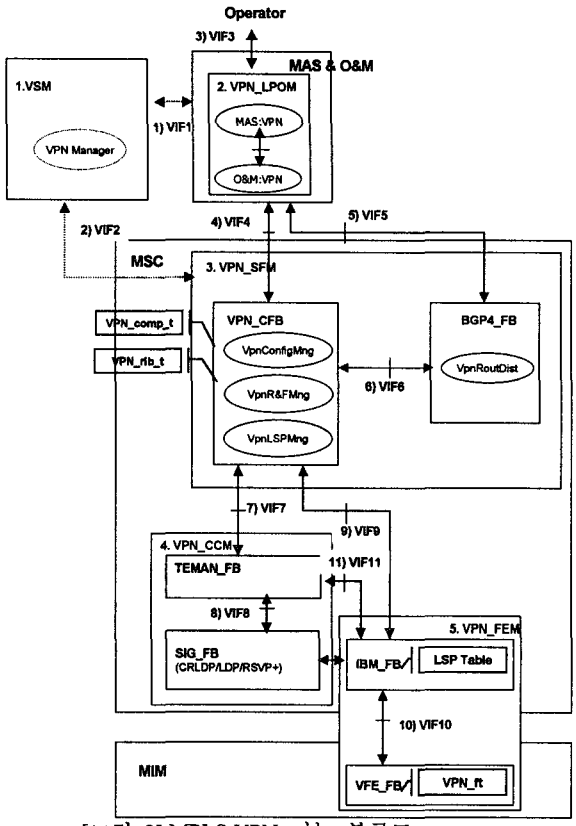
사설 주소 체계의 지원, VPN 별 라우팅 정보 관리, Egress PE 와 CE 사이의 경로 구분 등과 같은 기능을 제공하기 위해서 MPLS VPN 에서는 다음과 같은 데이터들을 정의한다.

- VPN ID(7 bytes) : VPN 그룹을 전역적으로 유일하게 구분하기 위한 구분자로써, VPN 관리 및 운용을 위해 사용된다[8].
- RD(Route Distinguisher)(8 bytes) : VPN 에서 사용되는 사설 주소를 전역적으로 유일하게 구분하기 위한 경로 구분자로 사용된다. 실제로 VPN 에서 사용되는 주소는 (RD ‖ 사설 IPv4 주소)이다[1,2,9].
- RT(Route Target)(8 bytes) : VPN 사이트들에 대한 라우팅 정보를 광고 및 업데이트 할 경우에 필터링을 위한 변수로 사용된다. 즉, LER 이 라우팅 정보를 수신할 경우, 수신된 라우팅 정보를 받아들일 것인지 아니면 무시할 것인지를 RT 를 통해 결정한다[2,5].
- VPN Label(3 bytes) : Egress PE 측에서 CE 측으로 VPN 패킷을 포워딩하기 위한 경로에 대한 정보를 나타낸다. VPN 레이블은 second label 로 스태킹된다[6,7].

### 3. MPLS VPN 기능 모델

MPLS VPN 서비스를 위한 기능 모듈은 크게 5 개의 모듈로 구성된다. 즉, VSM(VPN Service Manager Module), VPN_LPOM(VPN Local Provisioning and Operation Module), VPN_SFM(VPN Service Function Module), VPN_CCM(VPN Connection Control Module), 그리고 VPN_FEM(VPN Forwarding Engine Module)이다. 각 블록별 기능은 다음과 같다.

- VSM : VPN 서비스에 대한 SLA, Provisioning & Operation, VPN 서비스에 대한 품질 모니터링 및 과금 기능과 같은 서비스 운용 관리 기능을 처리한다.
- VPN_LPOM : VPN 서비스를 위한 주요 Configuration 데이터(VPN ID, RD, RT 등)의 할당 및 관리를 총괄하며, 운용자 명령어의 처리 및 모니터링, 가입자 정보의 관리를 담당한다.
- VPN_SFM : VPN 그룹 및 사이트를 관리하며 BGP4+ 기능 블록을 통해 라우팅 정보의 분배 및 수신 기능을 담당한다. 또한 LSP 설정을 위해서 VPN_CCM 모듈과 상호 동작하며, 포워딩 테이블의 관리를 위해서 VPN_FEM 과 상호 동작한다.
- VPN_CCM : VPN 서비스에 대한 LSP 설정 기능을 처리한다. VPN 사이트 간의 LSP 를 QoS 계약에 따라 설정하거나, 기존에 설정된 LSP 를 공유할 수 있다. 이 모듈은 TE 지원을 위한 TEMAN_FB 블록과 LSP 설정을 위한 SIG_FB 블록으로 구성된다. SIG_FB 은 CRLDP/LDP/E-RSVP 를 이용한다.
- VPN_FEM : VPN 을 위한 포워딩 테이블의 구성 및 포워딩 엔진의 동작을 제어한다. IBM_FB 은 VPN_CFB 로부터 포워딩에 관련된 정보를 수신하고, 수신된 정보를 이용해서 포워딩 테이블을 관리한다.




[그림 2] MPLS VPN 기능 블록도

그림 2 에서 보듯이 현재 MPLS VPN 에서는 모두 네 개의 테이블을 관리하고 있다. 각 테이블의 구성 정보 및 역할을 다음과 같다.

- VPN_comp_t : VPN 그룹 및 사이트에 관한 정보들이 포함된다. 즉, VPN 그룹의 ID, 패스 구성 정보, QoS 요구사항, RD, RT(Import RT, Export RT), 그리고 입력 인터페이스에 관련된 정보로 구성된다.
- VPN_rib_t : 라우팅 정보를 포함한다. 즉, VPN-IPv4 (RD‖IPv4), Next Hop, 그리고 출력 인터페이스 등의 정보로 구성된다. 또한 VPN 레이블과 LSP ID 도 이 테이블에서 관리한다. LSP ID 는 VPN_CCM 을 통해서 LSP 를 설정한 후에 수신하는 값이며, 나머지 정보들은 BGP4_FB 을 통해서 교환되는 라우팅 정보를 근간으로 해서 생성된다.
- LSP Table : LSP 에 관련된 정보들을 관리하는 테이블이다. 이 테이블은 CR-LDP/E-RSVP 를 이용해서 LSP 를 설정한 후에 SIG_FB 로부터 LSP 관련 정보

를 수신한 IBM_FB 에서 LSP 테이블에 관련 정보를 저장/삭제/수정한다.

- VPN_ft : VPN 사이트들에 대한 패킷 포워딩을 위한 정보를 포함한다. 즉, 목적지 VPN-IPv4, VPN 레이블, MPLS 레이블, 출력 포트, 그리고 Next Hop 등과 같은 정보들로 구성된다.

ACE 2000 시스템에서는 현재 VSM 모듈의 개발은 고려하고 있지 않으며, 추후 연구가 지속될 것이다.

## 4. 기능 블록간 인터페이스

이 장에서는 기능 블록간 인터페이스에 대해서 기술한다. ACE 2000 시스템에서의 VPN 개발 범위에 VSM 이 포함되지 않은 관계로 VIF1 과 VIF2 에 대해서는 정확히 정의되지 않은 상태이며, 추후 지속적인 연구가 필요하다. 다음은 각 인터페이스별 목적 및 메시지 종류에 대해서 기술한다.

### (가) VIF3

이 인터페이스의 정보는 주로 운용자가 운용 명령어를 통해서 전달하는 것들이다. 주로 이 인터페이스를 통해서 VPN 그룹 및 사이트의 구성 관리, VPN 사이트에 대한 연결 구성 제어, 서비스 사이트에 대한 라우팅 구성 및 제어, VPN 그룹에 대한 운용 정보의 검색 등과 같은 정보들이 교환된다.

실제 이 인터페이스를 통해서 전달되는 정보들은 그룹의 추가/삭제/변경 정보, 사이트의 추가/삭제/변경 정보, ER/CR LSP 설정/해제 정보, 그룹 및 사이트에 대한 운용 정보 등이 있다.

### (나) VIF4

이 인터페이스는 VIF3 를 통해서 전달 받은 정보를 VPN_CFB 에 전달하기 위한 것이다.

### (다) VIF5

현재 이 인터페이스를 통해서 전달되는 정보는 없다. 그 이유는 VPN 블록과 BGP 블록간의 역할을 명확히 구분하고 있기 때문이다. 즉, BGP 는 라우팅 정보와 VPN 에 관련된 정보들을 전달하는 기능만을 수행하며, 그 이외의 VPN 과 관련된 모든 기능 수행은 VPN 블록에서 수행한다.

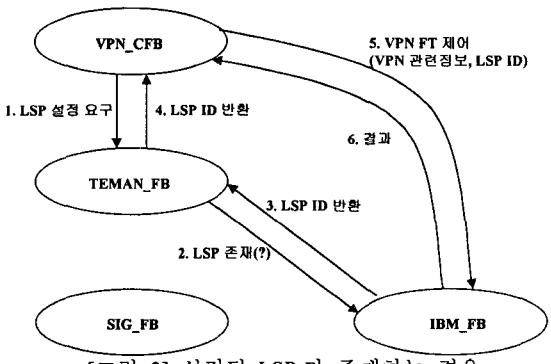
### (라) VIF6

이 인터페이스는 BGP4_FB 과 VPN_CFB 블록들 간의 정보 교환을 위한 것이다. ACE 2000 MPLS VPN 시스템에서는 VPN_CFB 와 BGP4_FB 의 기능을 명확히 구분한다. 즉, BGP4_FB 은 라우팅 정보의 분배 및 수신에 관련된 기능만 수행하며, VPN_CFB 에서는 VPN 에 관련된 모든 기능을 수행한다. 예를 들어서, BGP4_FB 이 라우팅 정보를 수신할 경우, BGP4_FB 은 수신된 라우팅 정보가 VPN 용인지 아닌지를 결정한 후에 VPN 용 라우팅 정보일 경우에 VPN_CFB 에 수신된 모든 라우팅 정보를 전달한다. 라우팅 정보를 수신한 VPN_CFB 은 VPN 용 라우팅 테이블에 라우팅 정보를 저장하고 필요에 따라 관련된 테이블들의 내용을 관리한다. 만약 수신된 라우팅 정보가 VPN 용이 아닌 일반 IP 용 라우팅 정보일 경우에는 BGP4_FB 이 라우팅 테이블을 관리한다.

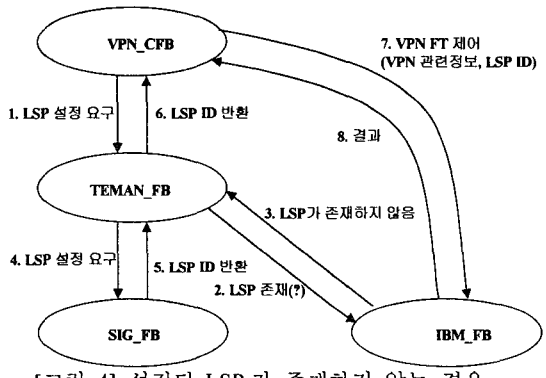
이 인터페이스를 통해서 BGP4+를 통해서 전달되거나 또는 수신된 정보들이 교환된다. 즉, VPN 용 라우팅 정보 및 VPN 레이블, RD, 그리고 RT 등과 같은 정보를 주고 받는다[3,4].

### (마) VIF7

이 인터페이스를 통해서는 LSP 설정을 위한 정보들이 전달된다. VPN_CFB 는 TEMAN_FB 에게 어느 정도의 QoS 를 보장하는 LSP 설정을 요구한다. VPN_CFB 로부터 수신된 LSP 설정 요구는 SIG_FB 으로 전달된다. SIG_FB 에서는 CRLDP 나 E-RSVP 를 이용해서 요구되는 LSP 를 설정한 후에 LSP ID 를 TEMAN_FB 에게 반환한다. TEMAN_FB 은 VPN_CFB 에게 LSP ID 를 반환한다. 만약 VPN_CFB 가 Best Effort 서비스를 요구할 경우에는 LDP 를 이용해서 설정된 LSP 가 존재하지 않으면 새로운 Best Effort 용 LSP 를 설정하고 LSP 가 존재하면 이미 설정된 LSP 를 공유한다. 그림 3 은 LSP 가 존재하는 경우의 LSP 설정 절차를 그림 4 는 LSP 가 존재하지 않을 경우의 LSP 설정 절차를 나타낸다.




[그림 3] 설정된 LSP 가 존재하는 경우




[그림 4] 설정된 LSP 가 존재하지 않는 경우

단, 기존에 설정된 LSP 는 CR-LDP/E-RSVP 를 이용해서 설정된 Best Effort 용 LSP 를 의미하며, 이러한 경우에 각 LSP 는 LSP ID 를 갖게 된다.

**(바) VIF8**

VPN_CFB 로부터 수신된 LSP 설정 요구를 SIG_FB 에 전달한다. 이때 VPN_CFB 로부터 수신된 정보이외에 TEMAN_FB 에서 필요한 정보를 추가할 수도 있다. SIG_FB 에서 LSP 를 설정한 후에 LSP ID 를 반환한다.

**(사) VIF9**

이 인터페이스는 포워딩 정보를 IBM_FB 에 전달하는 역할을 한다.

그림 3 과 그림 4 에서 보듯이 포워딩 정보에는 VPN 관련 정보와 LSP ID 가 있다. 이러한 정보를 수신한 IBM_FB 은 LSP ID 를 이용해서 LSP 관련 정보를 얻을 수 있으며 VPN 관련 정보와 함께 VPN 포워딩 테이블을 삽입/삭제/수정 기능을 수행한다. 이때 전달되는 정보는 VPN-IPv4, VPN 레이블, LSP ID 등이다.

**(아) VIF10**

이 인터페이스는 포워딩 정보를 IBM_FB 에서 VFE_FB 에 전달하기 위한 인터페이스이다. 이 인터페이스를 통해서 전달되는 정보는 VPN-IPv4(RD || private IP Address), VPN Label, MPLS Label, 출력측 정보 등이다.

**(자) VIF11**

이 인터페이스는 그림 3 과 그림 4 에 잘 나타나있다. 즉, VPN_CFB 가 Best Effort LSP 설정을 요구할 경우, TEMAN_FB 은 IBM_FB 에게 기존에 설정된 LSP 가 존재하는지 문의한다. 또한 이에 대한 응답을 수신한다. 수신된 결과를 이용해서 새롭게 Best Effort 용 LSP 를 설정할 것인지, 이미 존재하는 LSP 를 공유할 것인지를 결정한다.

## 5. 결론 및 추후 연구 사항

본 논문에서는 MPLS 에 기반한 VPN 서비스를 위한 기능 모델을 제시했다. MPLS VPN 에 관련된 전반적인 내용과 데이터 구조에 대해서 기술하였으며, 전체 기능 블록도를 바탕으로 각 블록의 기능과 각 블록간 인터페이스에 대해서 기술하였다.

추후에는 전체 VPN 서비스를 관리하기 위한 VPN 매니저에 관련된 연구가 지속될 것이며, VPN 서비스를 지원하기 위한 Traffic Engineering 에 대한 연구도 진행될 것이다.

본 논문의 결과를 이용해서 MPLS VPN 서비스가 구현되고 있으며, 구현된 결과는 ACE 2000 시스템에 탑재될 것이다.

## 참고문헌

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

[2] E.Rosen, et al, "BGP/MPLS VPNs", draft-rosen-rfc2547bis-01, May. 2000.

[3] Y.Rekhter, T.Li, "A Border Gateway Protocol 4 (BGP-4)", RFC 1771, Mar. 1995.

[4] T.Bates, R.Chandra, D.Katz, Y.Rekhter, "Multiprotocol Extensions for BGP-4", RFC 2283, Feb. 1998.

[5] S.Ramachandra, D.Tappan, "BGP Extended Communities Attribute", draft-ramachandra-bgp-ext-communities-04, Dec. 2000.

[6] Y.Rekhter, E.Rosen, "Carrying Label Information in BGP-4", draft-ietf-mpls-bgp4-mpls-04, Jul. 2000.

[7] E.Rosen, Y.Rekhter, D.Tappan, D.Farinacci, G.Fedorkow, T.Li, A.Conta, "MPLS Label Stack Encoding", draft-ietf-mpls-label-encaps-07, Sep. 1999.

[8] B.Fox, B.Gleeson, "Virtual Private Networks Identifier", RFC 2685, Sep. 1999.

[9] Y. Rekhter, et al, "Address Allocation for Private Internets", RFC1918, Feb. 1996.