

MPLmS기반의 Optical VPN 서비스를 위한 에지 라우터 설계

오홍석 · 김명희 · 이현태

목원대학교

Design of an Optical Edge LSR for MPLmS based VPN Service

Hong-seok Oh · Myung-hoi Kim · Hyeun-tae Lee

Mokwon University

E-mail : woon0710@hotmail.com Tel : 042)829-7798

요 약

본 논문에서는 MPLmS(Multiprotocol Lambda Switching) 기반의 Optical VPN 서비스를 제공하는 에지 라우터를 설계하기 위하여 MPLmS 기반의 VPN(Virtual Private Network) 모델과 동작 구조를 기반으로 에지 O-LSR(Optical Label Switching Router)의 기능적 블록을 설계하고 VPN 패킷 전달을 위한 라우팅 테이블을 설계한다.

1. 서 론

VPN은 인터넷과 같은 공중망을 이용하여 기존의 상호망과 같은 접근제어와 보안 기능을 제공하며 신뢰성, 확장성, 관리능력이 강화되고 비용측면에서 유리한 장점을 갖고 있다. 특히 광역의 공중망을 이용하여 비용측면에서 유리한 사설망을 구축할 수 있다는 점에서 서비스의 중요성이 강조되고 있다.

VPN 기술은 전달망 기술에 따라 Leased Line, ISDN, FR, ATM, IP 터널링 VPN 등의 다양한 형태의 기술이 사용되고 있다. 현재 가장 많이 사용되고 있는 기술은 ATM이나 FR를 이용한 L2-VPN (Layer2-VPN)과 IPsec과 같은 프로토콜을 이용한 IP 터널링 VPN이다[1]. VPN 서비스에 대해 이용자는 비용측면 뿐만 아니라 IP 서비스 지원, 정보에 대한 보안, 신뢰도, QoS 등을 고려하는 추세이다. 이에 따라 VPN 기술은 액세스망 기술에 의존적이고 확장성이 떨어지는 L2-VPN보다는 IP 기반의 IP-VPN으로, VPN의 제어기능에 대해 사용자 장치의 부담이 크고 CPE간에 네트워크 구성의 부담이 큰 CPE 기반의 VPN에서 망 차원의 VPN 서비스 제공 능력을 제공하는 PP(Provider Provisioned) 기반의 VPN기술로 발전되고 있다.

MPLS(MultiProtocol Label Switching) 기반의 VPN은 LSP(Label Switched Path)를 이용하여 VPN

사이트들간을 연결함으로써 서비스 품질을 차별화할 수 있고 확장성이 뛰어난 장점을 가진다. MPLS 기반의 VPN은 기존의 VPN의 단점, 즉, 품질보장의 제한적인 요소 및 확장성 제한, QoS의 지원 등을 개선하는 구조로서 관심을 끌고 있다[2].

기존의 라우터에서와 같이 매 패킷 단위로 수행되는 패킷 전달 기능은 수십 Gbps에 이르는 WDM (Wavelength Division Multiplexing) 기반의 광 네트워크 환경에서는 병목의 요인이 된다. MPLmS 기반의 광 네트워크 제어 기술은 IP 네트워크 내에 OXC (Optical Cross Connect) 기반의 연결형 광 네트워크를 구성하여 패킷 전달 기능의 고속화가 가능하도록 한다. 이러한 MPLmS 기반의 광 네트워크는 MPLS 기반의 VPN을 그대로 확장하여 광 네트워크에서의 VPN 서비스를 제공할 수 있다.[3][7]

본 논문에서 MPLmS 기반 광 네트워크에서의 VPN 서비스 제공을 위한 MPLmS VPN 네트워크 모델을 제시하고 이를 실현하기 위한 에지 O-LSR을 설계하였다. 제 2장에서는 MPLmS 기반의 VPN 서비스를 제공하는 에지 O-LSR의 모델과 설계 구조를 기술하였고, 제 3장에서는 에지 O-LSR 구조를 바탕으로 VRF(VPN Routing and Forwarding) 테이블을 설계하고 사이트가 하나 이상의 VPN에 속한 경우에 대하여 기술한다.

II. MPLmS 기반의 VPN 서비스를 제공하는 에지 O-LSR 구조 설계

1. MPLmS 기반의 VPN 모델

MPLmS 기반의 VPN은 기존의 MPLS 기반의 VPN 기술을 WDM기반의 네트워크에 적용하여 고속의 교환기능을 제공하고 MPLS의 제어기능을 통하여 서비스 제공 능력을 향상시킬 수 있다[3].

그림 1은 MPLmS 기반의 VPN 네트워크 모델이다. 각 CE 사이트는 일반 IP 라우터, MPLS 라우터, 혹은 Ethernet Switch등이 직접 접속될 수 있다.

본 논문에서는 일반 IP 라우터가 접속되는 모델을 기반으로 설계하였다.

에지 O-LSR은 각 인터페이스를 통해 들어오는 패킷의 목적지를 참조하여 목적지 에지 O-LSR를 통하여 해당 사이트로 패킷을 전달한다.

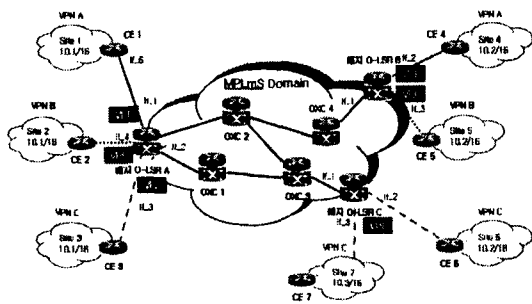


그림 1. MPLmS 기반의 VPN 모델

MPLmS기반의 VPN 사이트간 라우팅 정보의 분배 및 관리 방법에 따라 BGP(Border Gateway Protocol) 방식과 Virtual Router 방식이 있다.

MP-IBGP(MultiProtocol-interior BGP)방식의 MPLmS VPN은 VPN을 위한 라우팅 정보를 분배할 때 VPN정보도 함께 실어 보내는 피지백킹(Piggybacking)방식이다[4].

Virtual Router 방식은 에지 라우터에 VPN별로 Virtual Router를 둬으로써 라우팅, 패킷 포워딩, QoS, 서비스 관리를 VPN별로 하는 방식이다.

두 가지 방식에 있어 장,단점이 있지만 본 논문에서는 BGP방식의 MPLmS VPN에 관하여 논한다.

각 사이트는 각 인터페이스를 통하여 에지 O-LSR로 접속되고 각 사이트는 하나 혹은 하나 이상의 VPN 그룹에 속할 수 있다. VPN 서비스를 제공하는 에지 O-LSR은 각 인터페이스를 통하여 입력되는 패킷의 전달을 위하여 에지 O-LSR은 직접 접속된 사이트가 속한 VPN에 대한 라우팅 테이블만 갖고 있으면 된다.

VRF라고 부르는 각 VPN 단위의 라우팅 테이블은

해당 VPN에 속한 사이트의 패킷전달을 위해 참조된다. 에지 O-LSR은 CE 라우터로부터 경로 정보를 얻게 되면 MPLmS 도메인의 다른 에지 O-LSR과 MP-IBGP를 통하여 경로정보를 교환한다. RFC 2547bis에서는 서로 격리된 VPN내에서는 사설주소를 사용할 수 있도록 RD(Route Distinguisher)와 IPv4주소를 사용하여 중복주소의 사용을 허용하고 있다[5][12]. 에지 O-LSR에서 각 사이트로부터 입력되는 패킷을 목적지 사이트로 전달하기 위해서는 에지 O-LSR간에 Lambda SP(Lambda Switched Path)연결 설정이 되어야 한다.

본 논문에서 제시한 네트워크 모델은 기존의 MPLS기반의 VPN 기술을 최소화할 수 있도록 수정하여 제공할 수 있으면 앞으로의 연동문제 등을 쉽게 해결할 수 있다.

각각의 O-LSR 라우터에 대한 VRF 테이블은 3절에서 다룬다.

2. 에지 O-LSR의 물리적 패킷 교환 노드

에지 O-LSR에서는 Optical Switching Fabric을 기반으로 에지 O-LSR에 연결된 다양한 네트워크의 VPN 사이트에서 보내지는 패킷을 고려하여 그림 2와 같이 설계하였다.

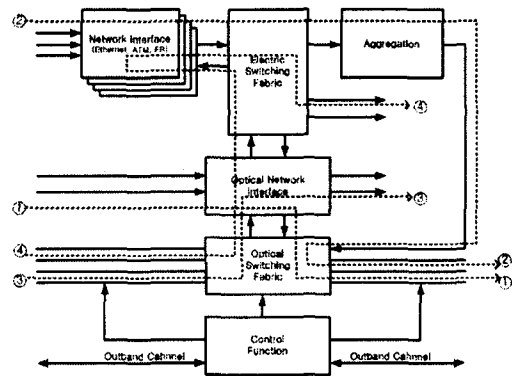


그림 2. 에지 O-LSR의 물리적 패킷 교환 노드

① VPN 사이트의 CE와 MPLmS 망의 O-LSR 간에 광 파이버로 연결되어 있는 경우 CE와 PE 간의 Optical 신호는 MPLmS망에서 LDP(Label Distribution Protocol)나 RSVP 같은 시그널링을 통해 Lambda label 경로를 할당하여 전송하는 것에 비해 이 링크에서는 단순히 대용량의 데이터를 고속의 Optical 신호로 전달하는 것이다[6][10]. 그래서, Ingress O-LSR에 전달된 Optical 신호는 Optical Network Interface로 입력되어 Egress O-LSR까지 설정된 Light Path에 따라 Lambda를 할당받고 Optical Switching Fabric에서 MPLmS 망으로 Optical 신호를 전송한다.

② Ingress O-LSR에 연결된 VPN 사이트가 일반 IP 도메인이나 MPLS 도메인으로 네트워크가 구성되어 있을 때, CE에서 보내진 Electric 신호는 Ethernet이나 ATM, FR등의 다양한 네트워크 인터페이스 카드를 통해 입력을 받아 Electric Switching Fabric에서 스위칭한다. Electric 신호를 스위칭한 패킷은 목적지 VPN 사이트가 동일한 패킷끼리 Aggreation 하여 Egress O-LSR까지 설정된 Light Path에 따라 Lambda를 할당하고 Optical Switching Fabric에서 MPLS 망으로 Optical 신호를 전송한다.

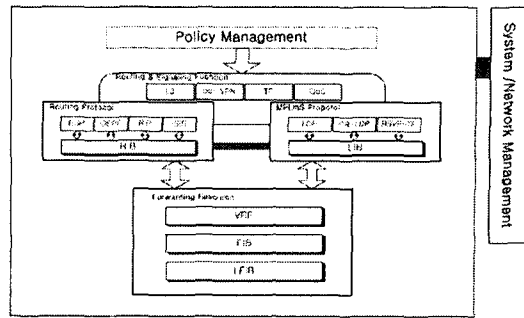


그림 3. Control Function의 기능 구성도

③ Egress O-LSR와 목적지 VPN 사이트의 CE가 ①의 경우와 같이 광 파이버로 연결되어 있을 때, MPLS망에서 들어오는 Optical 신호는 Lambda를 할당받아 Egress O-LSR까지 전송되었지만, Egress O-LSR에서 목적지 VPN 사이트의 CE 라우터로 Optical 신호를 전송할 때는 Optical Switching Fabric으로 입력된 신호를 Optical Network Interface를 통해 CE 라우터로 ①에서와 같은 형태의 Optical 신호로 전송한다.

④ MPLS망을 거쳐 Egress O-LSR로 들어온 Optical 신호를 목적지 VPN 사이트가 ②의 경우와 같은 CE 라우터로 전송할 때 Electric 신호로 변환한다. 이때, Optical Switching Fabric으로 들어온 Optical 신호를 Optical Network Interface를 통해 Electric 신호로 변환한 후 목적지 VPN 사이트의 네트워크의 종류에 따라 Ethernet이나 ATM, FR등의 다양한 네트워크 인터페이스 카드를 통해 적당한 패킷으로 재조립한 후 Electric Switching Fabric에서 스위칭하여 목적지 VPN 사이트의 CE 라우터로 전송한다[7][8].

3. 에지 O-LSR 제어 구조

에지 O-LSR의 물리적 패킷 교환은 VPN 사이트의 CE에서 보내진 패킷을 Optical 망으로 전송하기 위해 Lambda를 할당하여 스위칭한다[9]. 이때 MPLS망을 거쳐 목적지 O-LSR과 목적지 VPN CE 라우터까지 패킷을 전송하기 위해 망에 연결된 모든 에지 O-LSR들과 VPN CE 라우터들간에 Outband Channel로 서로의 라우팅 정보, 레이블 정보 및 VPN 정보를 교환해 에지 O-LSR의 포워딩 리소스를 만들어 패킷이 라우터에 들어오면 이들 테이블을 룩업하여 포워딩 동작을 수행한다.

그림 3은 에지 O-LSR의 제어 기능을 블록화하였다.

1) 라우팅과 신호 프로토콜 기능

MPLS 망의 모든 라우터들과 VPN 사이트의 CE 라우터들은 라우팅 프로토콜의 동작에 의해서 RIB (Routing Information Base)를 생성한다. RIB는 포워딩 리소스의 모든 테이블을 생성하는데 기본적인 경로 정보인 FIB(Forward Information Base) 정보를 생성한다. MPLS 망의 O-LSR는 VPN 사이트들에 대한 도달성 정보(라우팅 정보 분배 제어)인 RD(Route Distinguisher)와 멤버십 정보인 RT(Route Target)를 MP-IBGP를 이용하여 목적지 VPN 사이트와 연결된 PE 라우터에 전달한다[11]. VPN 패킷을 전달하기 위해서는 기존의 IPv4(4Byte)에 VPN 정보, 즉 RT와 RD(8Byte)가 추가된 12Byte의 VPN_IPv4의 패킷으로 변환하여 정보를 공유한다.

라우팅 프로토콜이 생성한 FIB 정보를 참조하여 LDP 및 CR-LDP, RSVP 등의 MPLS 프로토콜이 동작한다. 이 프로토콜은 MPLS망에서 목적지 VPN 사이트의 O-LSR까지 Lambda SP를 설정하는 레이블 정보인 LIB(Label Information Base)를 생성한다. LIB는 또한 트래픽 엔지니어링이나 QoS도 고려하여 레이블은 분배하고, FIB와 참조하여 레이블 정보로 포워딩을 할 수 있는 LFIB(Label Forwarding Information Base)정보를 생성한다. MPLS 망에서는 최종적으로 LFIB정보를 참조하여 포워딩된다.

2) 정책관리자(Policy Management)

에지 O-LSR에서는 들어오는 패킷의 네트워크의 종류와 인터페이스 정보를 보고 같은 목적지를 갖는 패킷을 구분하여 처리하기 위해 VPN, L3, 레이블 정보 등을 룩업한다. 이때, 정책 관리자는 테이블의 룩업과 사이트의 추가된 노드에 대한 새로운 테이블 생성을 제어하고, 이밖에 트래픽 엔지니어링이나 QoS등을 고려하여 시그널링 프로토콜들을 제어한다.

그리고 각각의 VPN 사이트에 대한 per-VPN 매니저가 VRF 테이블을 생성하고 분배하는 것에 대해 시

그널링 프로토콜을 정책적으로 관리한다.

3) 시스템 관리자(System Management)

Control Function의 시스템 관리자는 각 라우터들간 물리적인 패킷 전송을 위해서 Outband Channel로 시그널링 프로토콜을 동작시켜 포워딩 리소스를 생산하고 관리하여 라우터의 물리적인 패킷 전송을 제어한다.

4) 포워딩 리소스

시그널링 프로토콜의 동작에 의해 각각의 포워딩 정보인 FIB와 레이블 정보를 포함한 LFIB가 만들어진다. MPLmS 망에서는 LFIB정보에 의해 생성되는 LSP(Label Switched Path)에 대해 각각의 Lambda를 할당하여 VPN 패킷에 Bottom 레이블과 Top 레이블로 스테킹된 형태의 VRF 테이블을 형성한다.

MPLmS 기반의 VPN 서비스를 제공하는 망에서 PE 라우터는 모든 정보가 업데이트된 VRF 테이블을 록업하여 그림 2와 같은 절차로 포워딩 될 수 있다.

III. 에지 O-LSR의 VRF 테이블 구조

에지 O-LSR에서는 각각의 VPN 사이트에서 전송되는 패킷이 목적지 VPN 사이트까지 전송될 수 있도록 필요한 라우팅 정보와 포워딩 정보 즉, VRF 테이블을 가지고 있다.

이 절에서는 그림 1을 기반으로 하는 에지 O-LSR이 VRF 테이블을 생성하는 과정과 포워딩 과정에 대해 기술한다.

1) CE와 에지 라우터의 정보교환

에지 라우터는 VPN 패킷을 전달하기 위한 VRF 테이블을 생성한다. VRF 테이블은 RD, RT정보와 각 VRF에 해당하는 인터페이스가 바인딩 된다. 각 VRF 엔트리는 목적지 네트워크에 대한 BGP Next-Hop과 목적지 사이트 구별을 위한 Botton 레이블, 코어망 전달을 위한 Top 레이블을 포함한다. 에지 라우터에 생성된 VRF 테이블은 직접 연결된 VPN 사이트와 RIP, OSPF 같은 라우팅 프로토콜을 통해 CE라우터에 연결된 사이트의 라우팅 정보를 업데이트 한다.

2) 에지 라우터간의 정보 교환

에지에 연결된 각 VPN 사이트를 인터페이스로 구분한 Bottom 레이블과 Route target정보를 포함한 경로 정보를 MP-IBGP를 통하여 에지 라우터 간에 교환한다. 이때 에지 라우터는 자신과 직접 연결된 VPN 사이트에 대한 VRF 정보만을 가지고 있고, 같은 VPN 사이트

트의 에지 라우터간에는 MP-IBGP 세션이 설정되어 CE로부터 얻은 라우팅 정보를 서로 교환한다. 에지 라우터는 MP-IBGP를 통해 다른 PE에 연결된 같은 VPN 사이트의 CE에 대한 정보를 CE 라우터에게 전달한다.

3) 패킷전달에 대한 테이블 록업

에지 라우터에 CE 라우터로부터 패킷이 전달되면 입력 인터페이스에 대한 해당 사이트의 VRF 테이블을 록업하여 Bottom 레이블과 TOP 레이블을 할당받아 Egree 에지 라우터로 패킷을 전송한다. Bottom 레이블은 에지 라우터간 MP-IBGP를 통하여 정보를 교환해 VRF 테이블에 기록되어 있고, Top 레이블은 MPLmS망에서 LDP, RSVP등의 MPLmS 시그널링 프로토콜로 설정된 LSP에 해당하는 Lambda 레이블이다. Top 레이블로 Egree 에지 라우터에 전달된 패킷은 Bottom 레이블을 보고 해당 인터페이스를 찾아 IPv4패킷을 목적지 CE 라우터로 전달한다.

표 1, 2, 3에서는 그림 1에서 각각의 O-LSR에 대한 VRF 테이블의 예를 보여주고 있다.

<표 1> 에지 O-LSR A의 VRF 테이블

VRF Red				
Destination	BGP Next-Hop	Interface	Bottom Label (#)	Top Label (λ)
10.1/16	Direct	if_1	1001	-
10.2/16	에지 O-LSR B	if_2	1004	11

VRF Blue				
Destination	BGP Next-Hop	Interface	Bottom Label (#)	Top Label (λ)
10.1/16	Direct	if_4	1002	-
10.2/16	에지 O-LSR B	if_2	1006	22

VRF Green				
Destination	BGP Next-Hop	Interface	Bottom Label (#)	Top Label (λ)
10.1/16	Direct	if_3	1003	-
10.2/16	에지 O-LSR C	if_2	1006	33
10.3/16	에지 O-LSR C	if_2	1007	33

<표 2> 에지 O-LSR B의 VRF 테이블

VRF Red				
Destination	BGP Next-Hop	Interface	Bottom Label (#)	Top Label (λ)
10.1/16	에지 O-LSR A	if_1	1001	44
10.2/16	Direct	if_2	1004	-

VRF Blue				
Destination	BGP Next-Hop	Interface	Bottom Label (#)	Top Label (λ)
10.1/16	에지 O-LSR A	if_1	1002	55
10.2/16	Direct	if_3	1006	-

<표 3>에지 O-LSR C의 VRF 테이블

VRF Green				
Destination	BGP Next-Hop	Interface	Bottom Label (#)	Top Label (λ)
10.1/16	에지 O-LSR A	if_1	1003	66
10.2/16	Direct	if_2	1006	-
10.3/16	Direct	if_3	1007	-

표 1, 2, 3을 기반으로 하여 그림 1에서 VPN A 사이트에 속한 사이트 1에서 동일 VPN 사이트의 사이트 4로 패킷이 전송되는 과정을 그림 4와 같이 나타낼 수 있다.

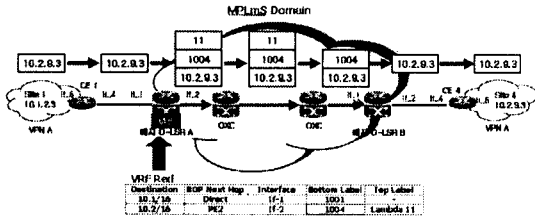


그림 4. Forwarding of Site 1 to Site 4

사이트 1에서 목적지 사이트 2까지 패킷을 전송하는 과정에 있어 에지 O-LSR까지의 전송은 CE1에서 1004라는 레이블 값이 스테킹되어 도달한다. 에지 O-LSR A에서는 사이트 4에 접속된 에지 O-LSR과 VRF 테이블의 정보를 교환한 상태이므로 Lambda 11을 스테킹하여 에지 O-LSR B로 전송할 수 있도록 한다.

IV. 결 론

RFC 2547bis로 표준화된 BGP/MPLS VPN을 기반으로 WDM 기반의 광 네트워크에 VPN 서비스 제공을 위한 네트워크 모델을 제시하고 에지 O-LSR를 중심으로 VPN서비스 제공을 위한 제어 구조를 설계하였다. 설계한 제어구조는 에지 라우터 장치로써 정책 기반 라우팅, 트래픽 관리 등을 고려하여 설계하였다.

제시된 네트워크 모델과 제어구조는 기존의 MPLS 기반의 VPN 기술을 최소한으로 수정하여 제공할 수 있으며 앞으로 MPLS망과 MPLMs망간의 연동 문제로 쉽게 제공할 수 있을 것이다.

제시된 제어구조를 기반으로 VPN 패킷 전달을 위한 VRF 테이블을 설계하고 광 네트워크에서 패킷 전달 시나리오를 제시하였다.

추후 연구 사항으로 정책기반 라우팅과 포워딩 제어구조에 대한 연구와 차별화된 VPN 서비스 제공을 위한 제어구조에 대한 연구가 필요하다.

참고문헌

[1] 양선희 · 윤호선 · 이유경, "품질보장이 가능한 MPLS 기반의 IP-VPN 기술", 한국통신학회지, 2001.
 [2] "Service Management of MPLS VPNs", White

Paper, digiquant, 2001.
 [3] Rameshbabu Prabagaran, Joseph B. Evans, "An architecture for scalable MPLMs VPNs", Optical Networks magazine, pp.66-72, April 2001.
 [4] T.Bates, R. Chandra and D.Katz, Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC2858, Feb 2000.
 [5] E.Rosen. et al. "rfc2547bit-02. txt:BGP/MPLS VPNs", July. 2000.
 [6] N. Ghani, Lambda-Labeling : A Framework for IP-over-WDM Using MPLS, Nokia Research Center Report, April 2000.
 [7] D. Awduche, R.Coltun, J. Drake and Rekhter, "Multi-Protocol Lambda Switching: Combining MPLS Traffic Engineering Control With Optical Cross Connects", work in progress, Feb 2000.
 [8] J. Anderson et al., "Protocols and Architectures for IP Optical Networking,"Bell Labs Tech. J., vol 4, no 1, Jan. 1999.
 [9] Bala Rajagopalan and Tellium et al., "IP over Optical Networks: A Framework", IETF Internet draft, draft-ietf-ip-framework-00.txt, July 2001.
 [10] Guangzhi Li, "Experiments in Fast Restoration Using GMPLS in Optical/Electronic Mesh Network", Optical Fiber Communication Conference and Exhibit, pp. PD34_1, PD34_3, 2001.
 [11] Bill St. Arnaud, Mike Weir, "BGP Optical switches and lightpath route arbiter", Optical Network Magazine, March/April. 2001.
 [12] C. Semeria, RFC 2547bis:BGP/MPLS VPN Fundamentals, Juniper.