MPLS를 이용한 IP VPN의 기술 동향

Technology Trend of IP VPN Using MPLS

김숙연(S.Y. Kim) MPLS 응용팅 선임연구원
양선희(S.H. Yang) MPLS 응용팀 선임연구원, 팀장
이유경(Y.K. Lee) 인터넷기술연구부 책임연구원, 부장

MPLS(Multiprotocol Label Switching)를 이용한 IP 기반의 VPN은 고수익을 원하는 서비스제공자들과 저비용을 원하는 기업들에게 인트라넷(intranet)과 익스트라넷(extranet)의 해결책으로서 많은 관심을 끌고 있다. MPLS VPN에 대한 표준화는 IETF에서 추진되고 있는데, BGP multiprotocol extension(BGP-E)이라는 프로토콜을 이용하는 구조와 Virtual Router(VR)라는 개념을 이용하는 구조가 제안되었다. BGP-E 방식은 시스코에 의해 제안되어 RFC2547로 채택되었다. 이 방식에서는 BGP-E를 이용하여 도달성과 멤버쉽 정보를 PE간에 교환한다. VR 방식은 노텔과 루슨트를 중심으로 여러 기업들이 지지하고 있고 드래프트 형태로 작업중이다. 이 방식에서는 PE들에 VPN별로 VR들을 배치하고 같은 VPN에 속하는 VR들끼리 기존의 라우팅 프로토콜을 이용하여 라우팅 정보를 교환한다. 두 방식의 근본적 차이는 도달성과 멤버쉽 메커니즘의 분리 여부이다. 세계적으로 이름 있는 통신 회사들이 경쟁적으로 MPLS 시스템을 개발하고 있는 상황에서 MPLS VPN 기술도 빠르게 시장에 확산될 것으로 전망된다. 그러나 서로 다른 기술적 접근을 하고 있는 서비스제공자들간의 MPLS VPN에 대한 호환성은 시급히 풀어야 할 숙제로 남아 있다.

I. 서 론

VPN(Virtual Private Network)이란 공중망을 기반으로 구현된 가상의 사설망(private network)이다. VPN은 보안성, 신뢰성, 관리 편이성, 사설 주소 지원, 우선순위 설정과 같은 사설망의 기능을 제공하면서도 사설망에 비해 매우 경제적이다. 따라서 VPN은 대규모 기업의 분산된 사이트들을 연결하는 인트라넷, 혹은 협력 업체 사이트들 간의 익스트라넷을 구현하는 핵심 기술로 자리잡고 있다.

VPN 중 고객 기업 사이트의 VPN 데이터가 IP 패킷 형태로 전달되는 것을 IP VPN이라고 한다. IP VPN은 일반적으로 기반이 되는 백본망이 인터넷이므로 광범위한 지역에 구축 가능하고 접속비용이 저렴할 뿐 아니라 TCP/IP 데이터 어플리케이션의 급속한 확산에 따라 수용가능 어플리케이션도 풍부하다. 인터넷이 빠른 속도로 팽창하고 있는 상황에서 IP VPN은 이러한 장점들을 가지고 있으므로 차세대 VPN 기술의 주류가 될 것이 확실시 된다.

IP VPN은 크게 CPE(Customer Premises Equipment)-based VPN과 NBVPN(Network-based VPN)으로 나뉜다[1]. CPE-based VPN에서는 VPN을 위한 동작 메커니즘이 각 CPE에 구현되어야 하므로 고객의 부담이 큰 반면 NBVPN에서는 서비스 제공자의 백본망에 구현되므로 경제적으로 아웃소스(outsource)될 수 있다. 따라서 NBVPN은 고수익을 원하는 서비스제공자들과 저비용을 원하는 기업들에게 모두 환영받는 IP VPN의 해결책이 되고 있다.

NBVPN은 같은 VPN에 속하는 사이트 간을 백본망을 통하여 안전하게 연결하기 위하여 터널링 메커니즘을 필요로 한다. NBVPN의 터널링 메커니즘으로 쓸 수 있는 것은 IPSec, GRE(Generic Routing Encapsulation), IP/IP, L2TP(Layer 2 Tunneling Protocol), MPLS 등 다양하다. 그러나 이중 MPLS는 IP만을 지원하는 IPsec에 비해 다양한 프로토콜을 지원할 수 있을 뿐만 아니라 멀티캐스트(multi-cast)를 지원하기에도 용이한 구조를 가지고 있다. 뿐만 아니라 ATM이나 Frame Relay, IP를 포함하는 다양한 하부구조상에서 구현 가능하며 백본망 내에서의 패킷 포워딩이 단순 신속하다. 또한 명시 라우팅(explicit routing)이나 QoS 및 트래픽 엔지니어링(traffic engineering)과 같은 고급 기능 지원이 용이하다는 장점도 지닌다. 원래 MPLS는 비연결형으로 동작하는 IP 망 내에 논리 채널인 LSP(Label Switched Path)를 구성하여 연결형으로 동작하도록 함으로써 IP 트래픽의 흐름을 제어할 수 있게 한 기술이다. MPLS는 기존의 hop-by-hop 라우팅에 의해 전달되는 IP 패킷을 망 입출력 시에만 라우팅 처리를 하고, 코어에서는 레이블을 이용한 고속 스위칭을 하여 IP 라우팅의 성능을 개선한 차세대 IP 망 기술이다. MPLS를 NBVPN을 위한 터널링 메커니즘으로 사용한다는 것은 NBVPN의 백본망을 MPLS 망으로 하며 같은 VPN에 속하는 사이트 간을 LSP를 활용하여 연결함을 의미한다.

MPLS VPN을 위한 기본적 구조로서 제안된 것은 크게 두 가지이다. 하나는 BGP-E를 활용하는 방식이고 다른 하나는 VR이라는 개념을 이용하는 방식이다. 본 고에서는 MPLS VPN의 구조를 밝힌 후 두 방식을 소개하고 차이점 및 장·단점을 분석한다. 또한 이 두 방식을 중심으로 MPLS VPN과 관련한 IETF(Internet Engineering Task Force)의 표준화 동향을 조사 분석한다.

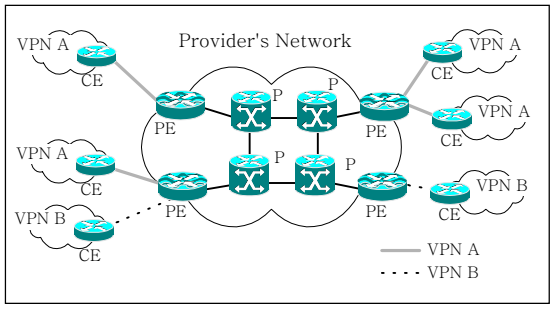
II. MPLS VPN 구조 분석

이 절에서는 MPLS VPN의 구조를 밝힌 후 BGP-E 방식과 VR 방식을 차례로 소개하고 두 방식의 공통점과 차이점 및 장·단점을 분석한다.

1. MPLS VPN 기술 개요

이 절에서는 MPLS VPN의 구성요소와 서비스 요구사항을 정리하고 MPLS 터널의 공유 메커니즘을 설명한다.

MPLS VPN은 (그림 1)과 같이 PE(Provider's Edge device), P(Provider's device), CE(Customer's Edge device) 등의 요소로 구성된다. P와 PE는 서비스제공자의 백본망에 속해 있고 CE는 고객 사이트에 속해 있다. CE는 하나의 호스트일 수도 있고 스위치나 라우터일 수도 있다. 고객 사이트의 백본망에 대한 접속은 CE와 PE간의 링크를 통해서만 이루어진다. P는 VPN을 위한 별도의 기능을 가지지 않을 뿐만 아니라 VPN에 관한 정보도 따로 유지하지 않는데 이는 MPLS VPN의 확장성을 위한 핵심적 요소이다. PE에는 입력되는 패킷을 VPN에 따라 구분하여 포워딩하는 기능이 탑재되어야 한다. 이 기능은 백본망 내에 VPN별로 폐쇄 사용자 그룹을 정의하기 위해 필수적이다.



(그림 1) Network-based VPN의 구조

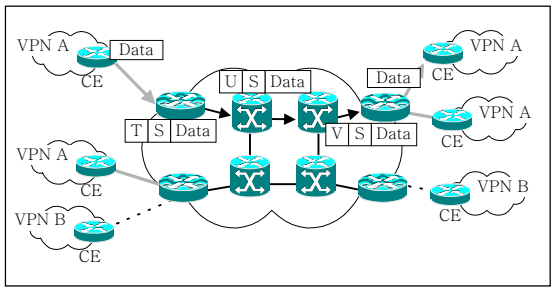
MPLS VPN의 서비스 요구사항은 다음과 같다.

- 통신 보안성을 보장해야 한다. 즉 같은 VPN에 속하는 고객 사이트들끼리 안전하게 연결되어야 한다.
- 사설주소체계를 지원해야 한다.
- QoS를 지원해야 한다.
- 하나의 고객 사이트가 여러 VPN에 공통적으로

속할 수 있어야 한다.

- 완전 메쉬나 hub-and-spoke와 같은 다양한 VPN 토폴로지를 지원해야 한다.
- CE와 PE간의 도달성 정보(reachability information) 교환은 기존의 라우팅 프로토콜 혹은 정적 라우팅 지정에 의해서도 가능해야 한다. 아울러 PE와 CE간의 라우팅 프로토콜은 백본망에서의 것과는 상관이 없어야 한다.
- CE와 PE를 연결하는 데이터 링크는 PPP, ATM, Ethernet, Frame Relay, GRE 터널 등 어떤 것이라도 상관없다.
- 서비스 확장성을 위하여 PE가 유지 관리하는 라우팅 정보량은 전체 VPN의 개수나 VPN 사이트 수와 상관이 없어야 한다. 즉 PE는 자신과 직접 연결된 VPN 수나 사이트 수에 비례하는 정보량만 유지 관리해야 한다.
- 고객 사이트는 VPN 서비스 뿐 아니라 인터넷 서비스도 받을 수 있어야 한다.
- IPv4나 IPv6 혹은 유니캐스트(unicast)나 멀티캐스트와 같은 여러 종류의 트래픽을 처리할 수 있어야 한다.
- 여러 AS(Autonomous System)를 거치거나 여러 서비스제공자를 거치는 VPN을 구성할 수 있어야 한다.

MPLS VPN에서 보안성을 확보하기 위한 주요한 방법인 터널링 메커니즘은 LSP를 활용하는 것이다. 만약 두 개의 PE 사이에 n개의 터널이 필요하다면 n개의 LSP를 따로 설정할 수도 있지만 한 개의 LSP를 공유할 수도 있다. LSP 공유는 MPLS 망의 주요 자원인 LSP를 절약하게 하므로 MPLS 망의 확장성 뿐 아니라 VPN 서비스의 확장성도 증진시킨다. LSP의 공유 방법 중 대표적인 것이 MPLS의 주요 기능인 레이블 스테킹(label stacking)을 활용하는 것이다. VPN 지원을 위한 두 단계의 레이블 스테킹에서 최상위 레이블(top label)은 LSP를 결정하며 둘째 레이블(second label)은 그 LSP에 공유된 터널들을 구분시킨다. 다시 말해서 최상위 레이블은 MPLS



(그림 2) 두 단계 레이블 스테킹을 활용한 LSP의 공유

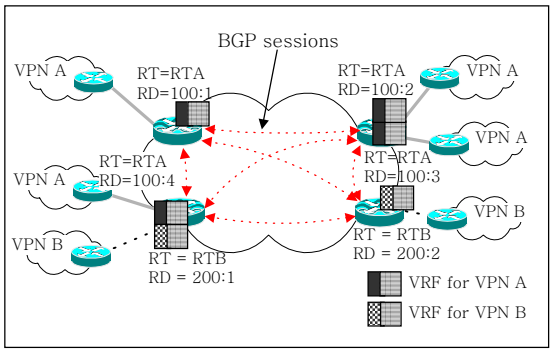
망 내에서의 라우팅 정보를 함축하고 둘째 레이블은 MPLS 망 출구에서의 라우팅 정보를 함축한다. (그림 2)는 레이블 스테킹에 의해서 데이터 패킷이 전달되는 예를 보여준다. IP 패킷 형태의 VPN 패킷은 VPN A의 고객 사이트에서 출발하여 입구 PE에 도착한다. 입구 PE에서는 T와 S를 최상위 레이블과 둘째 레이블로 각각 인코딩한다. 망을 통과하면서 최상위 레이블은 T에서 U와 V로 바뀌지만 둘째 레이블은 그대로 유지된다. 망의 출구 PE에 도착하면 데이터를 IP 패킷 형태로 복원하여 둘째 레이블에 의해 결정된 고객 사이트로 전달한다.

2. BGP-E 기반의 MPLS VPN의 구조

BGP-E 기반의 MPLS VPN은 VPN 사이트들에 대한 도달성 정보와 멤버쉽 정보를 BGP-E를 이용하여 PE간에 전달하는 방식이다[2]. 다시 말해서 VPN을 위한 라우팅 정보를 분배할 때 VPN 멤버쉽 정보도 함께 실어 보내는 피지백킹(piggybacking) 방식이다. BGP-E의 원조인 BGP4는 AS간에 라우팅 정보를 교환하기 위한 프로토콜로서 IPv4형태의 라우팅 정보만을 다룰 수 있다[3]. BGP4를 IPv6나 IPX를 비롯한 다양한 형태의 라우팅 정보도 교환할 수 있도록 확장한 것이 BGP-E인데, MPLS VPN에서는 "VPN-IPv4" 형태의 라우팅 정보를 교환한다.

가. 라우팅 정보의 분배 메커니즘

VPN 라우팅 정보는 (그림 3)과 같이 PE들간의



(그림 3) BGP-E 기반의 MPLS VPN

BGP 세션에 의해 분배된다. (그림 3)에서 P들과 그들에 인접한 링크들은 생략되었다. BGP-E가 분배하는 주소의 형태는 VPN-IPv4이다. VPN-IPv4 주소란 IPv4 주소 앞에 Route Distinguisher(RD)를 붙인 것이다. RD는 같은 IPv4 주소를 가지는 다른 시스템을 구분하기 위해서 필요하다. 왜냐하면 각 VPN은 사설주소체계를 가지기 때문이다. (그림 3)에서와 같이 RD는 CE로부터의 입력 인터페이스와 미리 연관되어 있어야 한다. 왜냐하면 CE로부터 온 IPv4 루트 앞에 PE가 RD를 붙여 분배할 수 있어야 하기 때문이다. 한편 PE가 BGP-E로 VPN-IPv4 루트를 분배할 때 VPN-IPv4에 대한 레이블도 함께 분배한다. VPN-IPv4에 대한 레이블은 1절의 레이블 스테킹을 위한 둘째 레이블이다.

한편 각 PE에는 (그림 3)에서와 같이 고객 사이트별로 VRF(VPN Routing and Forwarding instance)가 있다. 여러 VPN에 대한 포워딩 정보를 여러 VRF들에 적절히 나누어 저장해 놓는 것은 멤버쉽 기능에 의해 가능하다. VPN 멤버쉽 기능을 위한 핵심적 요소인 RT(Route Target)는 BGP-E 패킷의 에트리뷰트(attribute)로서 라우팅 정보 분배를 제어할 수 있게 한다. (그림 3)에서와 같이 모든 VFR은 하나 이상의 RT와 연관되어 있다. 한편 VPN-IPv4 루트도 하나 이상의 RT와 연관된다. VPN-IPv4 루트는 같은 RT와 연관된 VRF에만 분배되어야 한다. 다시 말해서, PE는 VPN-IPv4 루트를 받으면 같은 RT를 가지는 VRF들에 그 루트를 입력시킨다. RT를 import RT와 export RT로 세분화하여 활용하면 VPN 멤버쉽 기능을 더욱 세련되게 구현할 수 있다.

나. 데이터 패킷의 포워딩 메커니즘

BGP-E 방식에서의 패킷 포워딩은 1절에서 언급한 두 단계 레이블 스테킹에 의한 LSP 공유의 메커니즘에 따라 (그림 2)와 같이 이루어진다. 고객 사이트로부터 CE를 통하여 VPN 데이터 패킷이 PE에 도착하면 PE에서는 그 고객 사이트에 해당하는 VRF를 참조한다. VRF에는 그 데이터 패킷에 대한 두 개의 레이블과 다음 홉에 대한 정보가 적혀 있다. 두 개의 레이블 중 둘째 레이블은 위에서 언급한 대로 BGP-E에 의해서 분배된 것이다.

3. VR 기반의 MPLS VPN의 구조

VR을 이용한 MPLS VPN에서는 PE에 VPN별로 VR을 둠으로서 라우팅, 패킷 포워딩, QoS, 서비스 관리를 VPN별로 한다. VR이란 물리적인 실제 라우터와 똑같은 기능을 하는 가상의 라우터이다. VR은 설정(configuration), 연산(operation), 감시(monitoring), 과금(accounting), 유지보수(maitainance)를 위한 메커니즘과 도구(tool)를 가지고 있다[4].

VR은 다양한 VPN 설정을 지원할 수 있는 개념이다. VR간에 Layer-2 기반의 일 대 일 연결도 가능하고 여러 개의 VR을 하나의 VR에 뭉쳐넣음으로써 NBVPN에 활용하는 것도 가능하다. 여러 개의 VR을 하나의 VR에 뭉쳐넣는 것은 MPLS VPN에서 다음과 같이 활용된다. 하나의 PE에 백본 VR(backbone VR)이 들어있고 백본 VR에는 여러 개의 VPN용 VR이 들어 있다. 백본 VR은 기능적으로 다른 VR들과 같다. 백본 VR이 VPN용 VR들을 수용하므로 새로운 VPN 사이트의 추가로 인하여 백본망의 설정 상태가 변화될 필요가 없다. 백본 VR과 VPN용 VR들과의 관계는 오버레이(overlay) 관계이다. 따라서 백본 VR의 라우팅 도메인과 VPN용 VR들의 라우팅 도메인은 아무 관련이 없다. 더구나 백본 VR은 각 VPN VR에서 도는 라우팅 인스탄스에 대해서 알 필요가 없다.

가. 라우팅 정보의 분배 메커니즘

VPN 라우팅 정보는 MPLS에서 제공하는 터널(즉 LSP)을 통해 전달된다. 백본 VR은 한 VPN 내의 VR들이 마치 직접 연결된 것 같이 만들어 준다. 따라서 한 VPN 내의 VR들은 서로 직접 기존의 라우팅 프로토콜로 라우팅 정보를 교환한다. 이러한 라우팅 프로토콜은 VPN을 위해서 어떠한 확장이나 변형도 필요치 않다. RIP, OSPF, BGP4와 같은 동적 라우팅 프로토콜 뿐만 아니라 정적인 루트 지정도 가능하다. 뿐만 아니라 PIM(Protocol Independent Multicast) 또는 DVMRP(Distance Vector Multicast Routing Protocol)와 같은 기존의 멀티캐스트 라우팅 프로토콜들도 그대로 활용할 수 있다. (그림 4)는 VR 방식의 예를 보여주고 있다. 각 PE에는 VPN별로 VR이 있고 그들 사이는 터널로 연결되어 있다. 그림의 단순화를 위해서 백본 VR과 P들은 생략하였다.

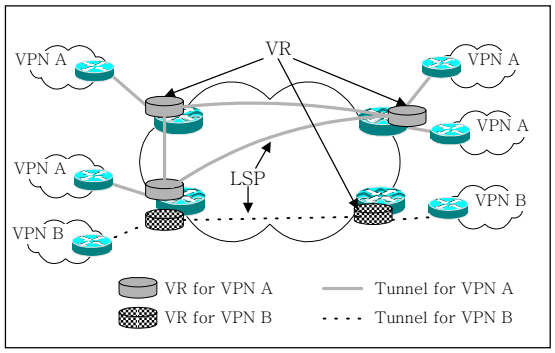
나. 데이터 패킷의 포워딩 메커니즘

VR 방식에서는 같은 VPN에 속하는 고객 사이트들이 VR들에 의하여 폐쇄적으로 연결되어 있다. 따라서 데이터 패킷 포워딩은 평범한 라우터를 사용하는 사설망과 같이 이루어진다. VR간의 터널은 1절에서 언급한 두 단계 레이블 스테킹에 의한 LSP 공유의 메커니즘을 활용할 수도 있다.

4. 구조 비교 • 분석

가. 공통점

두 방식은 NBVPN으로서 기본 모델이 같고 다음과 같은 공통점을 가진다. 첫째, CE에서 PE로 전달되는 VPN 데이터 패킷에는 VPN에 관한 정보가 실려 있지 않다. 둘째, 각 PE에서의 라우팅 정보와 패킷 포워딩 정보가 VPN별로 분리되어 유지 관리된다. BGP-E 방식에서는 고객 사이트별로 VRF가 존재하고 VR 방식에서는 VPN별로 VR이 존재한다. 셋째, CE에서 PE로 입력되는 VPN 데이터 패킷에



(그림 4) VR 기반의 MPLS VPN

대해서 그 PE의 어느 부분에서 처리할 지 미리 설정(preconfiguration)된다. BGP-E 방식에서는 입력 인터페이스마다 VRF가 연관되어 있고 VR 방식에서도 VR(들)이 연관되어 있다.

나. 차이점

두 방식의 가장 근본적인 차이는 VPN 도달성 기능과 멤버쉽 기능의 분리 여부이다. VR 방식에서는 VPN 도달성 기능과 멤버쉽 기능이 분리되어 다른 메커니즘으로 구현되는 반면 BGP-E 방식에서는 통일적으로 구현된다.

BGP-E 방식에서는 VPN 도달성 정보와 멤버쉽 정보가 BGP-E에 의해서 동시에 분배된다. VPN 도달성 정보는 VPN-IPv4 형태로 PE들간에 교환된다. VPN 멤버쉽 정보는 도달성 정보을 전송할 때 함께 전송되는 에트리뷰트인 RT에 의해 전송된다. RT는 해당 도달성 정보가 어떤 VRF에게 수신되어야 할지를 알려줌으로써 멤버쉽 기능을 수행한다.

VR 방식에서는 VPN 멤버쉽 기능과 도달성 기능이 분리된 메커니즘으로 구현된다. 도달성 정보는 한 VPN에 속하는 VR들간의 라우팅 프로토콜에 의해 분배된다. 멤버쉽 메커니즘은 각 PE가 어떤 VPN에 속하는 VR들을 가져야 할지를 결정할 뿐 아니라 여러 PE에 분산되어 있는 같은 VPN의 VR들간을 어떻게 LSP로 연결할 지를 결정한다. 멤버쉽 기능은 PE 관리 플랫폼(management platform)에서 명시적으로 설정하거나 서버를 따로 두어 VR이 서버에

게 물어 보는 식으로 구현할 수 있다고 알려져 있으나 구체적 기술은 표준화되어 있지 않다.

다. 장·단점

BGP-E 방식은 BGP-E라는 기존 프로토콜의 기본 메커니즘을 그대로 활용한다. 따라서 구현과 관련하여 상세 기술이 비교적 쉽게 명료화될 수 있었다. 이런 이유에서 이 방식은 MPLS VPN의 구현 기술로는 처음으로 RFC로 등록될 수 있었을 뿐 아니라 상품출시도 선진적이었다. 이 방식은 시장에 발빠르게 진출하여 시장을 점유함으로써 MPLS VPN의 표준으로 확고히 자리잡을 가능성이 크다.

그러나 BGP-E가 원래 라우팅 정보 교환에 목적을 두고 만들어진 프로토콜인 만큼 VPN을 위해 기술적으로 적합하지 않은 점들도 있다. 첫째 도달성 기능과 멤버쉽 기능의 미분리로 인하여 설정과 운용이 매우 복잡하다. 각 PE의 VRF마다 RT를 지정해야 할 뿐만 아니라 CE로부터의 입력 인터페이스마다 RD를 지정해야 한다. 모든 VPN의 정보가 한군데 모여 있지 않아 확장성이 좋다고 주장하지만 실제로 멤버쉽 기능을 위하여 각 PE마다 적절한 설정을 하는 것은 매우 복잡하고 소모적이다. 둘째, IPv6나 멀티캐스트와 같은 다른 종류의 트래픽을 처리하기 위하여 매번 BGP-E를 확장하고 표준화하여야 한다.

한편 VR 방식은 MPLS VPN을 포함하는 일반적인 NBVPN에 대해 적용될 수 있는 개념이다. 백본망이 MPLS 뿐 아니라 ATM, Frame Relay, IP 망일 때도 적용 가능하다. 이는 기술적으로 상이한 NBVPN (예를 들어, 여러 서비스제공자가 각자의 망에 다른 터널링 메커니즘을 도입했을 때 이 망들에 걸쳐 설치된 VPN)들 간을 연동시키는 기술적 기초가 될 수 있음을 의미한다. 하나의 PE가 여러 서비스제공자들의 백본망들에 동시에 연결되거나 같은 서비스제공자가 운영하는 다른 종류의 백본망들에 연결되는 상황에도 쉽게 적용된다. 이렇게 VR 방식은 확장성이 우수하며 다양한 VPN 설정을 수용한다. 뿐만 아니라 기존 라우팅 프로토콜을 그대로 활용하므로 IPv6나 멀티캐스트와 같은 다른 종류의 트래픽을 처리하기가 용이하다는 장점이 있다. 그러나 구체적인 구현 기술에 대해서는 아직 표준화가 매우 미흡한 상태이다. 예를 들어 백본 VR에 여러 개의 VPN VR들을 구현하는 방법이나 멤버쉽 기능 구현 방법 등이 구체적으로 명시되어 있지 않다.

<표 1>은 2절에 명시된 MPLS VPN의 요구사항에 대하여 두 방식을 비교한 것이다. 각 항목에 대하여 O는 관련 RFC나 드래프트에 구체적 기술이 명시되어 있음을 의미하고, Δ는 구체적으로 명시되어 있지 않았더라도 쉽게 확장 구현될 수 있음을 의미한다. X는 표준화가 미비하고 확장구현이 불투명함을 의미한다.

<표 1> MPLS VPN 서비스 요구사항에 대한 BGP-E 방식과 VR 방식의 비교

	BGP-E 방식	VR 방식
보안성[a]	O	O
사설주소체계 지원	O	O
QoS를 지원[b]	O	O
공유 고객 사이트[c]	O	Δ
다양한 VPN 토폴로지 지원[d]	O	O
CE-PE간의 라우팅 프로토콜 다양성	O	O
CE-PE간의 데이터 링크의 다양성	O	O
PE는 직접 연결된 VPN 수나 사이트 수에 비례하는 정보량만 유지 관리	O	O
고객 사이트는 VPN 서비스 뿐 아니라 인터넷 서비스도 받을 수 있어야 함.	O	Δ
IPv4/IPv6 및 유니캐스트/멀티캐스트와 같은 다양한 종류의 트래픽 처리 가능	X	O
여러 AS를 거치거나 여러 서비스제공자를 거치는 VPN 구성 용이[e]	X	X

a. MPLS 망 내에서 VPN의 보안성은 LSP에 의해 구현된다.
b. MPLS VPN의 QoS는 MPLS 망의 QoS 메커니즘에 의존한다.
c. VR 방식의 경우 공유 고객 사이트를 지원하기 위해서는 공유 고객 사이트의 데이터 패킷이 어느 VPN 서비스를 받을 것인지 PE가 결정하는 메커니즘이 필요하다.
d. VR 방식이 더욱 융통성 있게 다양한 VPN 토폴로지를 지원한다.
e. BGP 방식끼리 혹은 VR 방식끼리는 여러 AS를 거치거나 여러 서비스제공자를 거치는 VPN 구성이 용이하다.

III. MPLS VPN과 관련한 표준화 동향

이 절에서는 MPLS VPN과 관련하여 IETF에서의 표준화 동향을 살펴본다.

BGP-E를 이용하여 MPLS VPN을 구현하는 방식은 '99년에 처음 시스코에서 제안하여 informational RFC로 채택되었고, 기술적으로 불확실한 점들을 인터넷 드래프트 형태로 보완해 가고 있다[5, 6]. BGP-E 방식과 관련된 표준화 작업은 매우 활발히 이루어지고 있다. BGP4의 에트리뷰트인 커뮤니티를 확장한 확장 커뮤니티를 표준화하려는 시도가 진행되고 있고, BGP가 루트 정보를 분배할 때 그 루트에 대한 레이블을 함께 분배하도록 하는 방법에 대한 별도의 명시도 있다[7, 8]. 한편 PE와 CE간의 라우팅 프로토콜이 OSPF일 경우 PE에 구현되어야 할 구체적인 절차에 관한 작업도 있다[9]. NBVPN 중에 백본망의 터널링 메커니즘을 IPsec으로 하는 경우에 백본망에서의 VPN 루트 분배를 위해 BGP-E를 사용하는 것에 대한 작업도 진행중이다[10]. 이 모델은 백본망에서의 터널링 메커니즘이 IPsec이라는 것 외에는 BGP-E를 이용하여 MPLS VPN을 구현하는 방식과 같다.

한편 VR을 이용하여 MPLS VPN을 구현하는 방식은 노텔과 루슨트를 비롯한 여러 기업이 지지하고 있으나 IP VPN의 기반구조(framework)를 제시하는 표준 문서에서 BGP-E 방식과 비교하여 권장할 만하다고 나와 있을 뿐 아직 드래프트 형태로 진행중이다[11]. VR 방식에 대한 구체적 기술은 아직 명시되어 있지 않은 부분이 많고 개념적 정리가 이루어지고 있는 상태이다.

두 방식에 국한되지 않는 MPLS VPN에 관한 표준화 동향은 다음과 같다. 다른 구조를 가지는 MPLS VPN들 사이의 상호연동을 위해 필요한 요소들을 규정하고 기능들을 규격화하는 작업이 초보적으로 진행되고 있다[12]. 한편 NBVPN(VR 방식에서나 BGP-E 방식에서나 상관없이)에서 일반적으로 사용될 수 있는 일반적인 VPN 프로토콜로서 BGP를 사용하는 것에 대한 연구가 진행되고 있다[13]. 이렇게 일반적인 VPN 프로토콜을 사용함으로써 특정 VPN에 대한 노드를 자동으로 찾아내거나 도달성 메커니즘을 선택하거나 터널링 프로토콜을 선택할 수 있다.

MPLS VPN를 포함하는 일반적인 IP VPN에 대해서 연동을 위한 표준화 작업도 진행중이다. NBVPN에 대한 기반구조를 제시하는 드래프트가 있는데, 이 작업은 기술적으로 상이한 접근을 하고 있는 다양한 서비스제공자들의 NBVPN간의 연동(interoperation)을 지원하기 위한 메커니즘을 표준화하기 위한 시도이다[14]. 한편 노텔과 루슨트에서 다양한 IP VPN을 총망라하여 분류한 후 각각의 요구사항을 정리하여 기존의 규격을 만족하는 구현 메커니즘들을 제안한 문서가 informational RFC로 채택되었다. 이 문서의 목적은 연동 가능한(interoperable) VPN 개발을 위해 필수적인 논의의 기반구조를 제시하기 위함이다.

IV. 결 론

본 고에서는 MPLS VPN을 위한 두 가지 구조, 즉 BGP-E 방식과 VR 방식을 소개하고 두 방식의 공통점과 차이점 및 장·단점을 분석하였다. 또한 이 두 방식을 중심으로 MPLS VPN과 관련한 IETF의 표준화 동향을 조사 분석하였다.

세계적으로 이름있는 네트워크 및 통신 회사들(Cisco, Nortel, Lucent, Ericsson, 3Com, Alcatel, Avici, Juniper, Pluris, Nexabit)이 경쟁적으로 MPLS 시스템을 개발하고 있고 UUNet, 프랑스텔레콤, AT&T 등 대규모 서비스제공자들도 MPLS 기술 도입을 추진하고 있다. 또한 국내에서도 인터넷 백본망을 MPLS로 업그레이드 하는 것이 적극적으로 검토되고 있을 뿐만 아니라 벤처 기업인 미디어링크에서 최초로 MPLS 시스템을 개발하였고 한국전자통신연구원(ETRI)에서도 ATM 기반 MPLS를 개발중이다. 이러한 추세에 따라 MPLS VPN 기술도 빠르게 시장에 확산될 것으로 전망된다. 그러나 서로 다른 기술적 접근을 하고 있는 서비스제공자들의 MPLS VPN

간의 호환성은 시급히 풀어야 할 숙제로 남아 있다.

참 고 문 헌

[1] B. Gleeson *et al.*, "A Framework for IP Based Virtual Private Networks," RFC2764, Feb. 2000.

[2] T. Bates, R. Chandra and D. Katz, Y. Rekhter, "Multiprotocol Extensions for BGP-4," RFC2283, Feb. 1998.

[3] Y. Rekhter and T. Li, "A Border Gateway Protocol 4(BGP -4)," RFC1771, Mar. 1995.

[4] H. Ould-Brahim and B. Gleeson, "Network based IP VPN Architecture Using Virtual Routers," Internet-draft, Mar. 2000.

[5] E. Rosen and Y. Rekhter, "BGP/MPLS VPN," RFC 2547, Mar. 1999.

[6] E. Rosen *et al.*, "BGP/MPLS VPNs," Internet-draft, May 2000.

[7] S. Ramachandra and D. Tappan, "BGP Extended Communities Attribute," Internet-Draft, 2000.

[8] Y. Rekhter and E. Rosen, "Carrying La-bel Information in BGP-4," Internet-draft, Jan. 2000.

[9] E. Rosen, "OSPF as the PE/CE Protocol in BGP/MPLS VPNs," Internet-draft, July 2000.

[10] J. Clercq *et al.*, "BGP/IPsec VPN," Internet-draft, July 2000.

[11] K. Muthukrishnan and A. Malis, "A Core MPLS IP VPN Architecture," Internet-draft, June 2000.

[12] J. Sumimoto *et al.*, "MPLS VPN Interworking Internet-Draft," Feb. 2000.

[13] H. Ould-Brahim *et al.*, "BGP/VPN: Information Discovery for Network-based VPNs," Internet-draft, July 2000.

[14] M. Suzuki and J. Sumimoto "A Framework for Network-based VPNs," Internet-draft, July 2000.