CE 라우터 기반의 MPLS VPN
(A VPN controlled by CE Routers on MPLS Networks)

이 영 석 † 한 민 호 †† 전 우 직 ††† 최 훈 ††††
(Youngseok Lee) (Minho Han) (Woojik Chun) (Hoon Choi)

요 약 VPN이란 공중망에서의 물리적인 구성과 무관하게 논리적으로 폐쇄된 사용자 집단을 구성하여 각종 통신 서비스를 제공하는 기술이다. 이러한 VPN을 구성하기 위해 IP/IP, GRE, L2TP, MPLS 등 다양한 기술들이 제시되었고, 그 중에서 MPLS를 이용한 방식이 다른 기술에서는 제공하기 어려운 QoS, 보안, 관리 유지 등을 제공하는데 많은 장점을 갖고 있다.

본 논문에서는 기존의 라우터 제조업체들에서 제안된 Network 기반 VPN 즉, PE 라우터(Provider Edge Label Switch Router) 기반 MPLS VPN과는 달리 CE 라우터(Customer Edge LSR) 기반의 MPLS VPN 방식을 제시하였다. PE 라우터 기반 MPLS VPN에서의 단점을 보완하기 위해 CE 라우터 기반 MPLS VPN 제어 요소 및 동작 절차를 지역(Customer) 네트워과 망사업자(Provider) 네트워에서의 MPLS Edge 라우터에 기반하여 설계하였고, PE 라우터 기반의 MPLS VPN과 CE 라우터 기반의 MPLS VPN의 성능을 비교하였다.

키워드 : 가상사설망, 라우터, 엠피엘에스

Abstract The VPN(Virtual Private Network) is a private network constructed logically on a public network infrastructure. There have been numerous studies to support the VPN services by using different technologies such as IP in IP, GRE, L2TP, MPLS and so on. Among these technologies, MPLS has shown many merits in aspects of QoS, security, and management, compared with other technologies.

As an enhancement of the VPN that is controlled by MPLS PE(Provider Edge) routers, this paper presents the VPN controlled by MPLS CE(Customer Edge) routers. The functional architecture of the CE based VPN and operations of the CE routers are described along with the performance comparison of CE based MPLS VPN. It has been shown that the CE based VPN has more advantages than PE based VPN with respect to independency, scalability, security, and complexity.

Key words : VPN, Router, MPLS, LER

1. 서 론

근래 웹브라우저나 인터넷 서비스를 이용하여 업무를 처리하는 사설망인 인트라넷뿐만 아니라, 더 나아가 고객이나 공급업체, 협력업체를 상호 연결하는 엑스트라넷도 도입되고 있다. 이러한 인트라넷 혹은 엑스트라넷의 발전은 사설망의 구축요구를 증대시켜 왔다. 그러나 사설망의 구축은 전송로나 교환장비의 설치 등의 상당한 초기 투자 비용이 요구되기 때문에, 이런 문제를 해결하는 방안으로 제안된 것이 바로 가상사설망(VPN: Virtual Private Network)이다[1]. VPN은 교환설비, 전송장비 등은 직접 투자하지 않고 기존의 공중망 설비를 이용하여 실제 사설망에서 제공될 수 있는 서비스를 적은 초기 투자로 실현할 수 있다는 장점이 있다.

이러한 VPN을 구축하는 방안으로는 IP(Internet Protocol) 계층에서 IP 터널링 방식과 MPLS(Multi-protocol Label Switching)을 이용한 방식이 있다[2][3][4]. MPLS 기반의 VPN은 IP 터널링 기반의 VPN에서 제공하기 어려운 QoS나 보안등을 제공할 수 있다는

· 본 논문은 정보통신연구진흥원 1999 대학기초연구지원사업에 의해 지원된 과제의 결과물입니다.
† 비 회 원 : 충남대학교 컴퓨터공학과
yslee@ce.cnu.ac.kr
†† 비 회 원 한국전자통신연구원 정보보호기술연구본부 연구원
mhhan@etri.re.kr
††† 비 회 원 : 충남대학교 컴퓨터공학과 교수
chun@raonet.com
†††† 종신회원 : 충남대학교 컴퓨터공학과 교수
hchoi@ce.cnu.ac.kr
논문접수 : 2000년 8월 14일
심사완료 : 2001년 10월 23일

장점이 있고, 높은 확장성, 효과적인 비용, 그리고 사용자 요구의 광범위한 핸들링을 제공하여 IP 서비스를 낮은 비용으로 제공해 준다. MPLS는 이와 같은 잇점을 바탕으로 VPN을 구성하기 위한 최적의 방안으로 간주되고 있으며, IETF에서는 MPLS VPN을 표준화하기 위해 시도중이다. 현재 RFC2547 "BGP/MPLS VPN"이 MPLS VPN의 표준으로 정립되고 있지만, 이 모델은 망사업자 네트웍(Provider Network)에 기반한 MPLS VPN의 구성 방안으로서, PE(Provider Edge) 라우터가 VPN의 모든 정보를 유지 관리한다. 이것은 VPN 사이트의 추가 혹은 삭제에 의한 토폴로지(topology) 변화가 PE 라우터에게 많은 부담을 주게 되므로 VPN 시스템의 확장성(scalability)이 저하되는 단점을 갖는다.

이러한 단점을 해결하기 위하여, 본 논문에서는 CE(Customer Edge) 라우터 기반의 MPLS VPN을 구성하기 위한 기본 구조를 제시하고 그에 따른 제어요소 및 동작절차를 정의하였다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 VPN 구성 방안에 대해 기술하며, 3장에서는 CE 기반 MPLS VPN를 위해 제어 요소 및 동작 절차의 설계에 대해 기술한다. 4장에서는 구현 및 성능 분석을 다른 방식과 비교하여 설명하고, 5장에서는 결론을 기술한다.

2. 기존의 VPN 구성 방식

VPN이란 특정 사용자 집단 내에서 다른 사용자로부터 폐쇄된 통신서비스를 보장하는 기술이다. 이러한 통신서비스의 제공의 핵심기술은 터널링 기술과 암호화 기술이다. 터널링(tunneling)이란 특정 VPN에 가입된 사용자들 간에 공중망을 통한 연결을 제공하여 이들 연결을 통하여 VPN내의 정보가 유통되는 논리적 망을 형성하는 것이다. 특정 VPN에 속하지 않은 다른 사용자로부터의 보안을 위하여 터널을 통하여 유통되는 정보를 암호화하기도 한다.

VPN에서의 터널구성 기술은 크게 데이타 링크계층(L2)에서 연결을 이용하는 방식과 IP계층의 연결을 이용하는 방안으로 분류할 수 있다. 먼저 L2 계층(예: HDLC, PPP, SLIP)의 연결을 이용하는 방식으로는 L2F (Layer 2 Forwarding), PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol)가 있다[5][6]. 이 방식은 서비스 망사업자에 독립적으로 구현이 가능하므로 압축과 암호화는 단대단(end-to-end)간에 이루어진다. 두 번째로 IP계층에서 IP in IP 방식의 터널을 이용하는 방식으로는 IP/IP(IP in IP), GRE(General Routing Encasulation), IPSec (Internet Protocol Security)가 있다[7]. 이중에서 IP/IP는 IP패킷을 다른 IP패킷 안에 실어 보내는 방식이며, GRE는 멀티프로토콜 캡슐화를 위한 IETF 규격이다. IPSec은 IP 계층의 두 개체간의 통신에서 비밀(privacy)과 인증(authentication)을 위하여 암호화와 관련된 시스템 구조 및 키(key) 관리를 지원한다.

IP패킷을 다른 IP패킷에 실어 터널링하는 방식과 달리 MPLS를 기반으로 하는 방식에서는 LSP를 설정하여 터널로 이용한다. MPLS란 현재 IETF에서 표준화가 진행 중에 있는 IP패킷의 전송방식이다. MPLS 라우터는 IP패킷을 FEC(Forwarding Equivalence Class)로 분류하고 각 FEC에 짧고 고정된 길이의 레이블(label)을 부착하여 이후의 모든 라우터가 이 레이블을 기준으로 간단하고도 빠른 패킷전송을 지원하는 기술이다[8]. 이 MPLS라우터는 VPN의 가입자들 사이에서 LSP를 설정하고, 다른 VPN에 속한 LSP들은 서로 다른 정책으로 관리함으로써 기존의 IP 터널링 방식과 비교하여 향상된 성능뿐 아니라 FEC의 설정에 따라 QoS나 보안 등 다양한 서비스의 제공도 가능하게 된다[9].

그림 1은 기존의 대표적인 VPN 구축 기술들과 MPLS 기반 VPN의 기능상의 비교를 표로 나타낸 것이다[1].

기능 \ 프로토콜	IP/IP	GRE	L2TP	IPSec	MPLS
멀티플랙싱	no	y/n	yes	yes	yes
시그널링	no	no	yes	yes	yes
데이타 보호	no	no	y/n	yes	y/n
멀티프로토콜	no	yes	yes	yes	yes
패킷순서보장	no	no	yes	no	yes
관리 유지	no	yes	no	no	no
작업 부하	yes	yes	y/n	y/n	yes
QoS	no	no	no	no	yes

그림 1 기존의 VPN 구축기술과 MPLS VPN의 비교

MPLS는 위에서 언급한 다양한 잇점으로 인해 VPN을 구성하기 위한 최적의 방안으로 간주되고 있다. 이에 따라, IETF에서는 MPLS VPN을 표준화하기 위해 시도중이며, 현재 RFC2547 "BGP/MPLS VPN"이 MPLS VPN의 표준으로 정립되고 있다[10][11].

그러나, "BGP/MPLS VPN"에서 제시된 모델은 망사업자 네트웍(Provider Network)에 기반한 MPLS VPN의 구성방안으로서, PE 라우터가 VPN의 모든 정보를 유지 관리한다. 결국, VPN 사이트의 추가 혹은 삭제에 의한 토폴로지(topology) 변화가 PE 라우터에게 많은

부담을 주게 되므로 VPN 시스템의 확장성(scalability)이 상대적으로 떨어진다.

또한, VPN 사이트의 모든 정보를 PE 라우터에서 관리하기 때문에 보안에 관한 요구사항이 더 필요하게 된 것이며, 사용자의 다양한 요구사항을 수용하기 위한 유연성(flexibility)을 보장하기가 어렵다.

따라서, 본 논문에서는 Customer 사이트 내에 속한 CE 라우터(Customer Edge LER)에 기반한 MPLS VPN을 대안으로 제시하였고, Network 기반 MPLS VPN에서의 방식과 달리 CE 라우터 기반의 MPLS VPN 제어 요소 및 동작 절차를 Customer 네트웍과 망사업자 네트웍에서의 PE 라우터에 기반하여 설계하였다.

이 방식에서는 VPN 사이트에 속한 CE 라우터에 VPN을 수행하기 위한 기능이 추가되지만, PE 라우터는 VPN 서비스를 위한 최소한의 VPN 정보만을 갖고 있게 된다. 따라서, PE 라우터와는 별도로 같은 VPN 사이트에 속한 CE 라우터 간의 연결성이 제공되며 망사업자 네트웍 기반의 MPLS VPN에 비해 독립성(independence) 보장 등 많은 장점을 갖게 된다.

MPLS VPN의 구성 예가 그림 2에 보여진다. 그림 2에서 CE 라우터는 사설망에 속한 LER로서 PE 라우터와 스텁 링크(stub link)로 연결된다. CE 라우터는 자신의 VPN membership 정보만을 PE 라우터에게 전달하고 PE 라우터로부터 자신과 동일한 VPN 사이트의 정보를 전달받는다. PE 라우터는 망사업자 네트웍 내에 존재하는 LER로서 사설망을 위해 VPN 정보를 CE 라우터에게 제공해 주며, 다른 PE 라우터와도 VPN membership 정보를 주고 받는다. PE 라우터는 또한 자신과 연결된 다른 VPN 사이트의 CE 라우터로부터 VPN 정보를 수신한다.

망사업자 네트웍 내의 P 라우터(Core LSR)는 망사업자 네트웍에서 수송을 제공한다. P 라우터는 계층3 프로토콜과 MPLS를 수행하며, 직접 CE에 접속되지 않는다.

VPN 사이트 간의 데이타 패킷 전송은 3.5절에 기술된다.

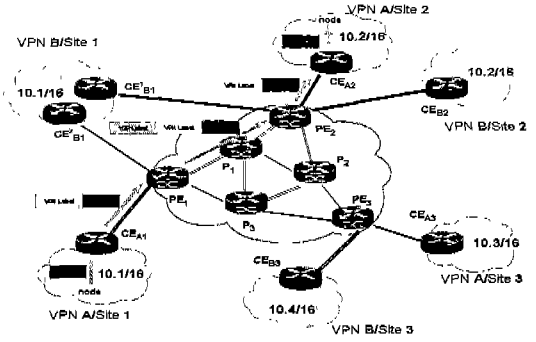

그림 2 VPN 구성 예

3. CE 기반 MPLS VPN

3.1 제어요소 및 동작 절차

CE 라우터 기반 MPLS VPN을 구성하기 위하여 CE/PE 라우터에서 제공되어야 할 기본적인 요구사항은 다음과 같다. 우선, 새로운 VPN 사이트가 생성되면 그 사이트에 속한 CE 라우터는 PE 라우터와 하나의 스텁 링크로 연결된다. 이 때 CE 라우터는 ISP(Internet Service Provider)로부터 유일한 IP 주소(예 : 168.188.46.147)를 할당받는다. 또한, CE 라우터는 자신이 속한 VPN 사이트의 VPN-ID(예 : A)를 알고 있다고 가정한다.

CE 라우터는 MPLS VPN을 구성하기 위하여 두 개의 테이블을 관리한다. 그림 3에서 보듯이, VPN member caching table에는 자신과 같은 VPN에 속해 있는 VPN 사이트의 CE 라우터 주소와 그 CE 라우터로 나가기 위한 자신의 interface 번호를 저장한다. VPN member caching table은 단순하게 VPN membership 정보만을 저장하며, 이 테이블을 참조하여 상대 CE 라우터와 편리하게 BGP(Border Gateway Protocol) peer를 유지하기 위해 사용된다[12][13][14]. VPN member caching table내에 저장된 자신과 같은 VPN에 속한 상대 CE 라우터의 주소를 사용하여 BGP를 수행하게 된다. BGP를 수행하면서 상대 CE 라우터로부터 전송된 VPN의 정보는 VPN routing table내에 저장하게 된다.

모든 PE 라우터는 VPN membership 정보를 관리하기 위해 VPN information table을 갖는다. VPN information table에는 PE 라우터와 stub link로 직접 연결된 CE 라우터로부터 받은 VPN 정보와 다른 PE 라우터로부터 받은 VPN membership 정보를 저장한다.

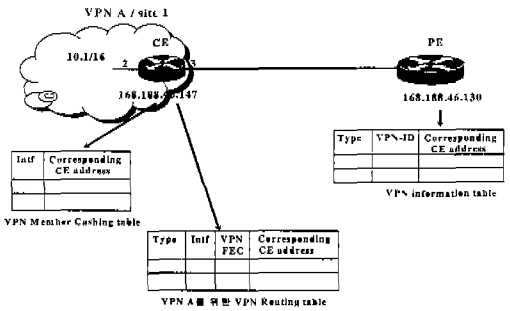

그림 3 MPLS VPN 지원을 위한 CE/PE 테이블 구성

PE 라우터에는 VPN membership 정보만을 저장하기 때문에, 망사업자 네트웍에서는 VPN을 지원하기 위한 단순한 메커니즘만이 필요하며 VPN 수행에 대한 부담을 덜 수 있게 된다.

3.2 새로운 VPN 사이트 생성 절차

새로운 VPN 사이트가 생성되는 경우, CE 라우터는 자신의 VPN membership 정보를 "Registration" 메시지에 실어 PE 라우터로 전송한다. 그림 4에서 보듯이 "Registration" 메시지에 전달되는 VPN membership 정보는 CE 라우터가 속한 VPN 사이트의 VPN-ID(예 : A)와 CE 라우터의 IP 주소(예 : 168.188.46.147)이다.

PE 라우터가 VPN membership 정보(VPN-ID, CE address)를 CE 라우터로부터 받은 경우 PE 라우터의 VPN information table내에 저장하고, Type 필드에는 자신과 직접 stub link로 연결되어 있다는 의미로 "Local"이라 한다. Remote는 자신과 직접 연결되지 않은 VPN 정보를 의미한다. PE 라우터가 CE 라우터로부터 VPN 정보를 받은 후, 자신의 VPN information table을 검색하여 이 라우터와 같은 VPN이 있는지를 확인한다.

만일 CE 라우터와 같은 VPN-ID(예 : A)가 VPN information table내에 존재한다면, PE 라우터는 해당 CE 라우터의 IP주소를 "Update" 메시지를 통하여 CE 라우터로 전송한다. 이 경우 "Update" 메세지내의 Tag 필드에 Addition 값이 들어간다. 이 때 CE 라우터는 PE 라우터로부터 수신한 VPN membership 정보를 자신의 VPN member caching table에 저장한다. 그림 4의 1번과 2번에는 이러한 과정을 보여주고 있다.

새로운 VPN 사이트의 등록을 수행한 후, PE 라우터는 새롭게 생성된 VPN membership 정보(VPN-ID, CE address)를 BGP에 실어 망사업자 네트웍 내에 속한 다른 모든 PE 라우터에게 전달한다. ISP내의 Edge 라우터인 PE 라우터들 사이에는 도달 정보(reachability information)를 교환하기 위하여 여러가지의 프로토콜이 사용될 수 있다. 하지만, 본 논문에서는 망사업자 네트웍내의 PE 라우터 사이에는 네트웍 도달 정보를 송수신하기 위해 BGP가 수행된다고 가정한다. 따라서, VPN membership 정보는 BGP에 piggybacking되어 다른 PE 라우터에게 전달되며, 이 VPN membership 정보는 수신된 모든 PE 라우터의 VPN information table에 저장된다. 이 때 Type 필드의 값은 "Remote"로 표시된다. 그림 5의 1번 과정이 이에 해당된다.

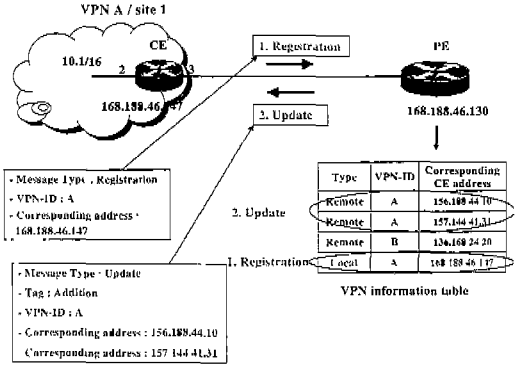

그림 4 새로운 VPN 사이트의 등록절차

그런 다음, VPN membership 정보를 수신한 PE 라우터는 자신의 VPN information table에서 Type 필드의 값이 "Local"인 엔트리 가운데 같은 VPN-ID가 있는지를 검사한다. 만일, 같은 VPN-ID가 있다면, 수신된 VPN membership 정보를 자신과 직접 연결된 즉, Type 필드의 값이 "Local"인 CE로 전송한다. 이 때 전송되는 VPN 정보는 "Update" 메시지를 사용하여 전달된다. 즉, "Update" 메시지 내에는 VPN-ID와 CE의 IP 주소가 포함된다.

VPN A/site2에 속한 CE가 VPN membership 정보를 수신한 후, 자신의 VPN member caching table에 수신된 정보를 저장한다. 그림 5의 2번에서는 이러한 동작 과정이 보여진다.

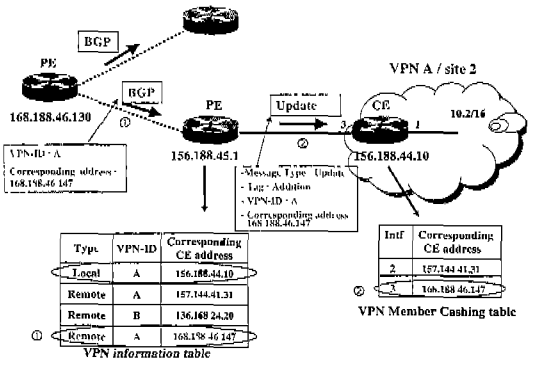

그림 5 VPN membership 정보의 전달 절차

위의 과정까지 수행된 이후에는, 각 VPN 사이트에 속한 CE 라우터는 자신과 같은 VPN 사이트 내 CE 라우터의 목적지 IP 주소를 알게된다. 이 때, 같은 VPN에 속해 있는 CE 라우터와 CE 라우터 사이에는 각 VPN 사이트의 도달 정보(reachability information) 등을 교

환해야 하는데, 이를 위해 다양한 프로토콜을 선택할 수 있으며, 본 논문에서는 그 중 BGP를 사용하였다. BGP를 통하여 전달되는 정보들은 CE 라우터 내의 VPN routing table에 VPN FEC 필드의 값으로 저장된다. CE 라우터와 CE 라우터 간에 BGP를 사용하여 도달정보를 교환하는 절차가 그림 6에 보여진다.

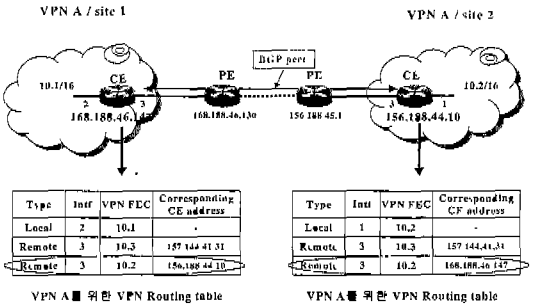

그림 6 CE와 CE간의 도달정보 교환

3.3 VPN 사이트간 데이타 전송 절차

VPN A/site1(10.1/16)에 속한 호스트에서 VPN A/site2(10.2/16)에 속한 호스트로 패킷을 전송하고자 하는 경우, VPN A/site1에 속한 CE 라우터(그림 7의 예 : 168.188.46.147)는 자신의 FIB(Forwarding Information Base) 테이블에 FEC(10.2)의 존재 여부를 검사한다. 만일 FEC(10.2)가 존재한다면 FIB 테이블 내에서 LIB(Label Information Base) 테이블로의 포인터가 존재하게 된다. 이 경우에는 LIB 테이블내의 레이블 정보에 기반하여 이미 설정된 LSP에 따라 패킷을 전송하게 된다.

그러나, FIB 테이블 내에 FEC(10.2)가 존재하지 않는다면, CE 라우터는 우선 VPN routing table을 조사한다. 여기서 FEC(10.2)는 VPN routing table내에서 Type 필드 "Remote"로서 존재하게 되며, FEC(10.2)에 해당하는 CE 라우터(그림 7의 예 : 156.188.44.10)에게 local address "10.2/16"에 해당하는 레이블을 요구한다. CE 라우터(156.188.44.10)로부터 "10.2/16"을 위한 레이블을 할당받으면 VPN A/site1에 속한 CE 라우터는 자신의 FIB 테이블과 LIB 테이블에 해당 정보를 삽입한다.

그런 다음, VPN A/site1에 속한 CE 라우터는 FIB 테이블을 다시 조사하여 PE 라우터의 FEC(156.188.46.130)가 존재하는 지를 검사한다. 만일 존재하면 VPN A/site1에 속한 CE 라우터의 LIB 테이블에서 FEC(10.2)의 레이블 값과 FEC(156.188.46.130)의 레이블 값을 포인터로 연결한다. 그렇지 않은 경우에는 PE 라우터(156.188.46.130)로 LSP를 설정한 후, LIB 테이블에서 FEC(10.2)와 FEC(156.188.46.130)의 레이블 값을 포인터로 연결한다.

MPLS VPN에서 레이블 정보가 LIB 테이블에 저장되어 있으므로 정해진 LSP를 따라 패킷을 전송한다.

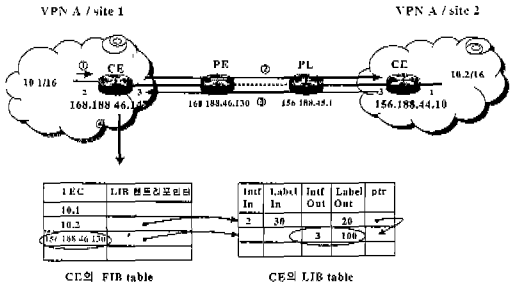

그림 7 CE의 FIB와 LIB 테이블 구성

3.4 기존 VPN 사이트 삭제 절차

VPN 사이트를 VPN에서 삭제하는 경우, 우선 삭제할 VPN 사이트에 속한 CE 라우터는 "Deregistration" 메시지를 자신과 stub link로 직접 연결된 PE 라우터에게 전송한다. 그런 다음, CE 라우터는 수행중인 프로토콜을 중지하고, VPN 구성 테이블들의 내용을 삭제한다.

PE 라우터는 stub link를 통해 "Deregistration" 메시지를 받은 뒤, 해당 VPN 사이트의 삭제 정보를 다른 모든 PE 라우터들에게 BGP에 piggybacking하여 전달한다. BGP에 piggybacking되어 전달되는 정보는 그림 8에 보여진 것처럼 VPN-ID와 VPN 사이트에 속한 CE의 IP 주소이다. 그 후, PE 라우터는 자신의 VPN information table에서 해당 VPN 사이트의 정보를 삭제한다.

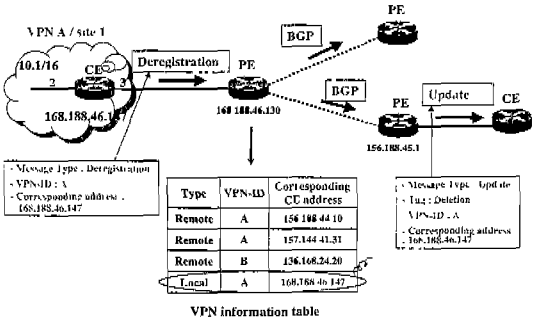

그림 8 VPN 사이트 삭제 절차

다른 PE 라우터로부터 VPN 사이트의 삭제 정보를 받은 PE 라우터는 VPN information table내에 Type 필드의 값이 "Local"인 엔트리중에서 삭제될 VPN과 같은 종류의 VPN-ID가 있는 지를 검사한다. 만일 같은 VPN-ID가 있다면, PE 라우터와 stub link로 연결된 CE 라우터에게 "Update" 메시지를 전송한 후, 자신의 VPN information table에서 해당 정보를 삭제한다. 이 경우 "Update" 메시지에는 삭제할 VPN 사이트의 VPN-ID와 CE 라우터 address가 포함되며, 메시지내의 Tag에는 Deletion 값이 삽입된다. 이 때, "Update" 메시지를 받은 CE 라우터는 자신의 VPN member caching table을 검색하여 메시지 내에 포함되어 있는 VPN 사이트에 해당되는 필드를 삭제하고, VPN routing table의 필드 역시 삭제한다.

3.5 라우팅

그림 2의 예제에서 VPN A/site1 내의 노드가 VPN A/site2 내의 노드와 통신하고자 한다면, VPN 프로토콜의 동작 완료 후에 데이타 패킷은 화살표에 따라 라우팅 된다.

VPN A/site1 내의 노드가 VPN A/site2 내의 노드 주소를 목적지로 하여 패킷을 전송하면, CE_{A1} 라우터는 CE_{A2} 라우터로 설정된 LSP를 통하여 레이블 패킷을 전달한다. 이 때 PE_1 라우터가 CE_{A1} 라우터로부터 레이블 패킷을 수신하고 IGP 레이블을 추가하여 PE_2 라우터로 패킷을 전달한다. PE2 라우터는 IGP 레이블을 삭제한 후, CE_{A2} 라우터에게 전달한다. CE_{A2} 라우터는 수신된 레이블 패킷의 레이블을 삭제하고 대응 노드에게 패킷을 전달한다. VPN A/site2 내의 노드가 VPN A/site1 내의 노드로 데이타 패킷을 전송하는 경우 역시 같은 방법으로 수행된다.

VPN A/site 1로부터 VPN A/site2까지의 경로에서 CE 라우터, PE 라우터 그리고 P 라우터의 프로토콜 구조를 그림 9에 보였다. CE_{A1}, PE_1, PE_2, CE_{A2} 라우터의 VPN 계층에서는 3.1-3.4 절에 기술된 절차를 수행한다.

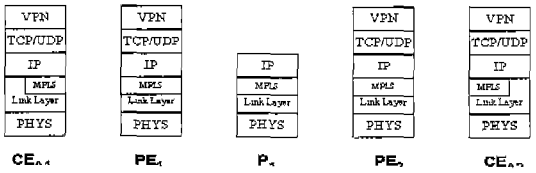

그림 9 CE/PE 라우터 프로토콜 구조

4. 구현 및 성능 평가

MPLS VPN 프로토콜은 Redhat Linux version 6.0, Linux Kernel version 2.2.9 상에서 C 언어를 이용하여 구현하였다. CE와 PE 라우터에서 VPN 서비스를 지원하기 위해 필요한 제어요소인 VPN member caching 테이블과 VPN 정보 테이블은 링크 리스트로 구현하였고, CE와 PE 사이의 메시지 전달을 위해 TCP (UDP)/IP Socket을 사용하였다. MPLS 계층은 LDP에 기반하여 연구실에서 개발한 부분을 이용하였다[15].

우선, 구현된 프로토콜을 이용하여 MPLS VPN 구성 방식들의 성능을 비교하였다. 성능 분석을 위해 Edge 라우터의 동작에 영향을 주는 중요한 요인 중에서, VPN 사이트 간에 데이타 패킷을 전송하는 경우 Edge 라우터에서 LSP를 설정하기 위해 필요한 VPN 관련 테이블들의 lookup 시간을 측정하였다.

Edge 라우터는 VPN 서비스를 지원하기 위해 VPN 계층에서 관련 정보를 검색한 후 LSP를 설정한다. 이 때, VPN 정보를 검색하기 위해 VPN 관련 테이블들을 lookup하는 시간은 CE와 PE 라우터의 수행 시간에 상당한 영향을 주는 요인이 될 것이다. 이러한 lookup 시간을 산출하기 위해 펜티엄 II 450 MHz 사양을 갖는 컴퓨터 상에서 MPLS VPN 프로토콜을 실행하여 시간을 측정하였다.

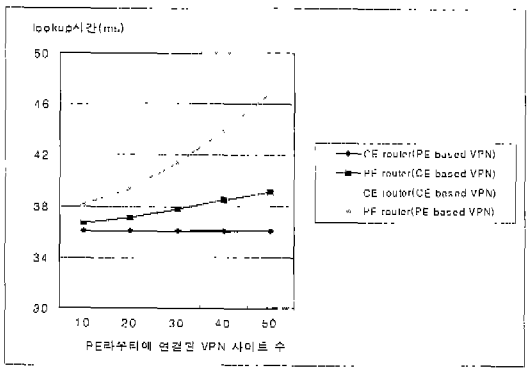

그림 10 CE/PE 라우터에서 LSP 설정을 위한 평균 수행 시간

그림 10은 두 가지 MPLS VPN 방식에서 PE 라우터에 연결된 VPN 사이트의 수가 증가함에 따라 Edge 라우터에서 요구되는 테이블 lookup 시간을 보여준다. 이 lookup 시간은 millisecond 단위로 측정하였다.

그림 10에 보여진 것처럼, PE 라우터 기반 MPLS VPN에서의 CE 라우터는 PE 라우터에 연결된 VPN 사이트의 수에 관계없이 항상 일정한 값을 갖으며 가장 수행 시간이 적다. 이것은 CE 라우터가 VPN 서비스를 지원하기 위해 어떠한 역할도 수행하지 않고, 단지

VPN 사이트 내의 노드에서 전송된 일반 데이타 패킷을 MPLS 레이블 패킷으로 변환하는 기능 및 그 역 기능만을 담당하기 때문이다.

그러나, PE 라우터는 자신에게 연결된 VPN 사이트의 수가 증가함에 따라 LSP 설정을 위한 수행 시간이 급격히 증가한다. 왜냐하면 PE 라우터에서 VPN에 관련된 모든 정보를 관리하기 때문이다.

CE 라우터 기반 MPLS VPN에서의 PE 라우터는 상대적으로 낮은 수행 시간을 갖는다. PE 라우터에서는 기본적으로 VPN 사이트의 연결 정보만을 관리하며 PE 라우터에 연결된 VPN 사이트의 수가 증가하더라도 관리하는 정보의 크기는 상대적으로 적게 증가한다.

이 방식에서 CE 라우터는 자신과 동일한 VPN의 모든 정보를 관리하게 되므로, PE 라우터에 비해 더 많은 VPN 정보를 갖게 된다. 따라서 VPN 사이트의 수가 증가함에 따라 PE 라우터보다 더 많은 검색 시간을 필요로 한다. 그렇지만, 이것은 PE 라우터 기반 방식의 PE 라우터보다는 상당히 적은 수행 시간이다.

다음으로, VPN 사이트의 추가 혹은 삭제 동작이 CE/PE 라우터에 미치는 영향을 살펴보았다. VPN 사이트 추가나 삭제와 같은 동작은 그 빈도가 증가함에 따라 CE/PE 라우터에서 처리하는 메시지의 수를 상당히 증가시키기 때문에 라우터의 성능에 영향을 주는 중요한 요인으로 간주할 수 있다. 그러나, VPN 사이트의 추가나 삭제는 실제 실험을 위해 VPN을 구축하는데 많은 어려움이 있기 때문에 성능 분석을 위해 본 논문에서는 COVERS라는 툴을 이용한 시뮬레이션 방법을 사용하였다. 또한, 시뮬레이션의 공정성을 보장하기 위해 실제 구현된 프로토콜에 기반하여 CE/PE 라우터에서의 메시지의 처리시간을 측정하였고, 해당 측정값을 시뮬레이션 모델에 적용하였다.

그림 2에 보여진 모델을 대상으로 시뮬레이션을 수행하기 위해 모두 6개의 VPN 사이트와 3개의 PE 라우터, 그리고 각 사이트 당 1개의 CE 라우터로 VPN을 구성하였다. 이와 같은 구성을 기반으로 3개의 PE 라우터에 새로운 VPN 사이트들이 추가되거나 삭제된다.

Customer 사이트 네트웍과 망사업자 네트웍 내에서 전송 오류는 없고, 각 네트웍 내에서의 전송 지연은 각각 평균 2의 값을 갖는 지수 분포를 따른다고 가정하였다. 두 가지 MPLS VPN 방식에서 CE 라우터와 PE 라우터가 VPN 계층에서 서비스를 지원하기 위해 수행되는 메시지의 처리 시간과 IP 계층에서의 메시지 처리 시간을 기준으로 각 라우터에 영향을 주는 작업 부하를 결정하였다.

이 작업 부하 역시 펜티엄 II 450 MHz 사양을 갖는 컴퓨터에 리눅스 커널 버전 2.2.9를 설치한 후, MPLS VPN 프로토콜을 직접 실행하여 VPN 계층과 IP 계층에서의 메시지 처리 시간으로 측정하였다. 측정값 중에서 가장 작은 시간을 갖는 CE 라우터에서 Deregistration 메시지의 전송 처리 시간을 작업 부하 1로 설정하고, 다른 동작들의 처리 시간의 작업 부하는 이에 대한 상대적 비율로 결정하였다.

-PE 라우터에서 VPN 사이트 Deregistration 메시지 수신 시의 작업 부하 : 1

-PE 라우터에서 VPN 사이트 Registration 메시지 수신 시의 작업 부하 : 1.3

-PE 라우터에서 VPN 사이트 Update 메시지 송신 시의 작업 부하 : 1.8

-CE 라우터에서 VPN 사이트 Deregistration 메시지 송신 시의 작업 부하 : 1.1

CE 라우터에서 VPN 사이트 Registration 메시지 송신 시의 작업 부하 : 1.2

-CE 라우터에서 VPN 사이트 Update 메시지 수신 시의 작업 부하 : 2.1

-CE/PE 라우터에서 메시지 송수신 시의 IP 계층 작업 부하 : 503

위에 제시된 작업 부하 값 중에서 IP 계층에서의 작업 부하가 가장 크다. 이것은 Linux 커널 내에서 VPN 메시지를 전송하는데 요구되는 시간뿐만 아니라 기타 다른 작업(예 : Context switch, Interrupt service 등)의 수행시간이 포함되기 때문이다.

그림 11은 VPN 사이트가 PE 라우터에 추가되는 평균 횟수에 따라 CE/PE 라우터에서 VPN 서비스를 지원하기 위해 필요한 작업 부하의 정도를 보여준다. VPN 사이트가 새로 등록되는 횟수가 증가함에 따라,

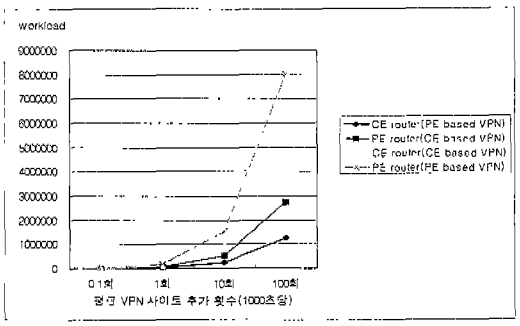

그림 11 VPN 사이트 추가에 의한 CE/PE 라우터의 평균 작업 부하

CE/PE 라우터에서는 더 많은 메시지를 처리해야 하므로 작업 부하의 값이 증가하게 된다.

PE 라우터 기반 MPLS VPN에서의 CE 라우터는 VPN 서비스를 직접 처리하지 않지만, 자신의 VPN 사이트를 PE 라우터에게 등록하는 과정은 수행하기 때문에 작업 부하의 값이 가장 작다. 두 가지 MPLS VPN 방식에서 CE/PE 라우터에 미치는 작업 부하는 그림 10과 동일한 순서를 갖는다.

그림 12는 VPN 사이트가 PE 라우터로부터 삭제되는 평균 횟수에 따라 CE/PE 라우터에서 이를 처리하기 위해 필요한 작업 부하의 정도를 보여준다. VPN 사이트가 삭제되는 횟수가 증가함에 따라, CE/PE 라우터에서는 더 많은 작업을 수행해야 하므로 작업 부하의 값이 증가하게 된다. 그러나, VPN 사이트를 등록하기 위해 요구되는 작업 부하에 비해 적은 값을 갖는다

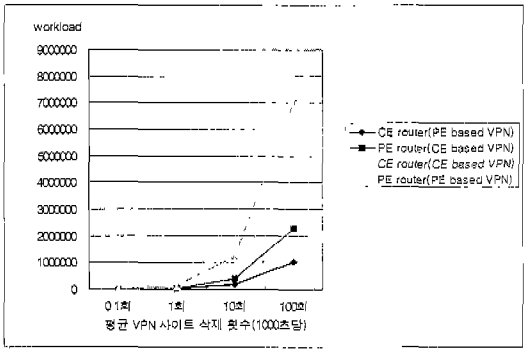

그림 12 VPN 사이트 삭제에 의한 CE/PE 라우터의 평균 작업 부하

본 논문에서 제시된 CE 라우터 기반 MPLS VPN에서는 VPN 시스템의 유연성을 보장하기 위하여 VPN 사이트 내의 CE 라우터에 VPN을 수행하기 위한 기능을 추가한 것이다. 이러한 결과로서 PE 라우터는 VPN 서비스를 위한 최소한의 VPN membership 정보만을 갖고 있게 된다. 따라서, PE 라우터는 단순한 형태의 메커니즘만으로 수행되기 때문에 서비스 망사업자내의 PE 라우터 성능에 부담을 주지 않게 된다.

PE 라우터의 성능에 크게 영향을 주지 않는 범위에서 같은 VPN 사이트에 속한 CE 라우터 간에 BGP가 수행 가능하므로 망사업자 네트웍으로부터의 영향을 최소화 할 수 있다. 이로 인하여 망사업자 기반의 MPLS VPN에 비해 VPN의 독립성이 상당히 보장된다.

또한, CE 라우터 기반 MPLS VPN은 VPN 사이트의 추가 혹은 삭제에 따른 topology 변화가 망사업자의 PE 라우터에게 큰 영향을 주지 않기 때문에 시스템의 확장성을 높일 수 있다. 망사업자에게 최소한의 VPN membership 정보만을 제공하므로 시스템의 보안 측면에서도 많은 장점을 갖는다.

PE 라우터 기반 MPLS VPN 구성 방식에서는 PE 라우터 내에 VPN의 모든 정보를 관리하므로 PE 라우터의 정보 분실이나 손실은 전체 VPN 서비스에 치명적이다. 반면에, CE 기반의 MPLS VPN 방식에서는 이러한 VPN 정보의 상당 부분을 CE 라우터에서 관리하게 되기 때문에 상대적으로 보안 측면에서 유리하다. 또한, PE 라우터에서 VPN 수행으로 인한 부담을 상당히 감소시킬 수 있게 된다. 그러나, 기존 PE 라우터에서 수행하는 VPN 기능을 CE 라우터에서 VPN 수행하기 때문에 CE 라우터의 부담이 커지게 된다.

표 1에는 MPLS VPN 구성 방식간의 장단점을 비교하였다.

표 1 MPLS VPN 구성 방식의 비교

	PE 기반의 MPLS VPN	CE 기반의 MPLS VPN
Independency	독립성 부족	우수
Scalability	확장 어려움	단순
Security	보안 어려움	우수
Complexity	PE 라우터 workload 많음	적음

5. 결 론

본 논문에서는 MPLS 도메인 내에서 VPN을 구성하기 위한 구조적 모델을 정의하였고, 제안된 모델의 제어 요소 및 동작절차를 설계하였다. 제시된 모델은 VPN을 구성하기 위한 단순한 메커니즘을 제공하며, Customer 사이트 내의 토폴로지 변화가 망사업자 네트웍의 라우터(PE)에 영향을 주지 않고 사용자의 다양한 요구사항을 수용할 수 있도록 유연성을 보장해 준다.

VPN 사이트에 속한 CE 라우터에는 VPN을 수행하기 위한 기능이 추가되는 단점이 있지만, 망사업자 네트웍에서는 VPN 서비스를 위한 최소한의 VPN membership 정보만을 갖고 있게 되므로 시스템 성능에 부담을 주지 않게 된다.

본 논문에서 제안한 방식은 CE/PE 라우터 내의 제어 요소들을 간단히 수정함으로써 MPLS 망에서 뿐만 아니라 기존의 IP 망에서도 VPN을 구현할 수 있으며, MPLS의 응용 서비스로서 VPN을 투명성있게 제공하

는 기반이 될 수 있을 것이다

CE 라우터 기반 MPLS VPN은 VPN 사이트의 수가 증가함에 따라, 네트웍 기반 MPLS VPN보다 PE 라우터의 성능을 향상시킨다. 따라서, 앞으로 MPLS VPN을 포함한 VPN의 시장이 급속히 확대될 것으로 많은 시장 조사 기관에서 예측한 것처럼, 제안된 모델의 적용 가능성은 VPN의 증가 속도에 따라 더욱 커질 것이다.

그러나, VPN 사이트의 지속적인 증가에 따라 보안의 문제점이 발생할 가능성이 높아지게 되며, 이러한 문제점의 해결방안으로서 CE/CE 라우터, CE/PE 라우터 사이에 높은 수준의 인증과 보안 기술 개발이 필요하다. 또한, VPN 사이트 내의 호스트가 다른 사이트로 이동할 때, 이동 호스트가 방문한 VPN 사이트에서도 계속 VPN 서비스를 제공받기 위한 이동성 지원 기술도 향후 연구되어야 한다.

이외에도, MPLS 망뿐만 아니라 ATM과 IP 등과 같은 다른 망에서 VPN을 구성하는 경우, 본 논문에서 제시된 방식과 연동 시의 문제점을 보다 구체적으로 분석해야 할 것이다.

참 고 문 헌

[1] Ferguson, P., Huston, G., "What is a VPN," The Internet Protocol Journal, Volume 1, Number 2, September 1998.

[2] Bleeson, B., et al, "A Framework for IP Based Virtual Private Networks," draft-gleeson-vpn-framewrok-01.txt, Fcbruary, 1999.

[3] Callon, R., et al, "A Framework for Multiprotocol Label Switching," draft-ietf-mpls-framework-05.txt, September 1999.

[4] Muthukrishnan, K., et al, "A Core MPLS IP VPN Architecturc", June, 2000.

[5] Hamzeh, K., et al, "Point-to-Point Tunncling Protocol," draft-ietf-pppext-pptp-10.txt, April, 1999.

[6] Townsley, W., et al, "Layer Two Tunneling Protocol," draft-ietf-pppext-l2tp-16.txt, Junc 1999.

[7] Perkins, C., "IP Encapsulation within IP", RFC2003, October 1996.

[8] Andersson L., et al, "LDP Specification," RFC 3036, Jan. 2001.

[9] Jamoussi, B., "Constraint-Based LSP Setup using LDP," draft-ietf-mpls-cr-ldp-03.txt, September, 1999.

[10] Rosen, E., Rekhter, Y., "BGP/MPLS VPNs," RFC2547, March 1999.

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

[12] Chandra, P., et al, " BGP Communities Attribute," RFC1997, August 1996.

[13] Rekhter, Y., et al, "A Border Gateway Protocol 4," draft-ietf-idr-bgp4-12.txt, Jan. 2001.

[14] Rekhter, Y., Rosen, E., "Carrying Label Information in BGP-4," draft-ietf-mpls-bgp4-mpls-03.txt, September 1999.

[15] Eunah Kim, Woojik Chun, "The LDP Implementation for a Linux-based LSR," ICOIN 14th Proceedings, pp. 4D-2.1~4D-2.7, Taipei Taiwan, Jan. 2000.

이 영 석

1992년 충남대학교 컴퓨터공학과(학사). 1994년 충남대학교 컴퓨터공학과(석사). 2000년 충남대학교 컴퓨터공학과 박사수료. 1994년 ~ 1997년 LG정보통신㈜중앙연구소 연구원. 관심분야는 가상사설망, 이동 컴퓨팅, 분산 시스템

한 민 호

1999년 충남대학교 컴퓨터공학과(학사). 2001년 충남대학교 컴퓨터공학과(석사). 2001년 ~ 현재 한국전자통신연구원 정보보호기술연구본부 연구원. 관심분야는 인터넷 프로토콜, 액티브 네트웍, 가상사설망

전 우 직

1982년 서울대 컴퓨터공학과(학사). 1984년 서울대 컴퓨터공학과(석사). 1989년 University of Delaware 전산학과(석사). 1992년 University of Delaware 전산학과(박사). 1984년 ~ 1993년 한국전자통신연구소 선임연구원. 1993년 ~ 현재 충남대학교 컴퓨터공학과 교수. 2000년 ~ 현재 ㈜라오넷 대표이사. 관심분야는 네트웍 프로토콜, 가상사설망, 트래픽 엔지니어링

최 훈

1983년 서울대학교 컴퓨터공학과 졸업. 1990년 듀크대학교 전산학 석사. 1993년 듀크대학교 전산학 박사. 1983년 ~ 1996년 한국전자통신연구원 선임연구원. 1996년 ~ 현재 충남대학교 컴퓨터공학과 조교수. 관심분야는 분산시스템, 컴퓨터네트워크, 이동컴퓨팅 등