MPLS를 이용한 CE 라우터 기반 VPN의 설계 및 구현

한민호○ 이영석 전우직 최훈
충 남 대 학 교 컴 퓨 터 공 학 과
{mhhan1, yslee, chun, hchoi}@ce.cnu.ac.kr

The Design and Implementation of VPN based on CE Router using MPLS

Min-Ho Han○ Young-Seok Lee Woo-Jik Chun Hoon Choi
Dept. of Computer Engineering, Chungnam National University

요 약

VPN이란 공중망에서 물리적인 구성과 무관하게 논리적으로 폐쇄된 사용자 집단을 구성하여 각종 통신 서비스를 제공하는 기술이다. 이러한 VPN을 구성하기 위한 다양한 기술들이 제시되었고, 그 중에서 MPLS를 이용한 방식이 다른 기술에서는 제공하기 어려운 QoS, 보안, 관리 유지 등을 제공하는데 많은 장점을 가지고 있다. 본 논문에서는 기존에 제안된 MPLS를 이용한 Network 기반, 즉 PE 라우터 기반 VPN의 단점을 보안하기 위해 제안된 MPLS를 사용하는 CE 라우터 기반 VPN의 설계 및 구현에 대해 기술하고자 한다.

1. 서론

근래 인터넷 서비스의 획기적인 발전은 기업들의 업무처리 방식에도 막대한 영향을 끼치고 있다. 기업의 업무 환경은 인터넷의 도입으로 인하여 근로자들의 근무 위치가 사무실에 국한되지 않고 집이나 업무현장으로 까지 넓혀지고 있고, 더 나아가 고객이나 협력업체를 연결하는 엑스트라넷도 도입되고 있다. 이러한 인트라넷 혹은 엑스트라넷의 발전은 기업이 내부에서의 정보 공유를 위한 LAN의 구성에서 벗어나 외부와의 네트워크 구성이 필요하게 된 것이다. 따라서 기업은 자신의 정보를 안전하게 전송하기 위하여 사설망을 구성하게 되는데 초기 네트워크 구성에 막대한 시설 투자비용이 요구되고 네트웍 운영과 관리에 많은 인적, 금전적 요소가 필요 하는 등의 문제점이 발생하게 된다. 이런 문제를 해결하는 방안으로 제안된 것이 바로 가상사설망(VPN: Virtual Private Network)이다[1].

본 논문에서는 기존의 라우터 제조업체들에게서 제안된 Network 기반 즉, PE(Provider Edge) 라우터 기반 VPN과는 달리 CE(Customer Edge) 라우터 기반 VPN을 구성하기 위한 기본 구조를 제시하였고, 그에 따른 제어요소 및 동작절차에 관한 설계 및 구현에 대해 다루고자 한다. 2장에서는 기존에 제안된 VPN 구성방법 및 본 논문에서 제시한 방법과의 차이점에 대해 설명하고 3장에서는 본 논문에서 제시한 MPLS를 이용한 CE 라우터 기반의 VPN의 설계 및 구현에 대해 설명하고자 한다. 마지막으로 4장에서는 결론 및 향후과제를 기술한다.

2. 관련연구

VPN에서의 터널 구성 기술은 크게 데이터 링크계층(L2)에서 연결을 이용하는 방식과 IP계층의 연결을 이용하는 방안으로 분류할 수 있다. 먼저 L2 계층 방식은 서비스 제공자에 독립적으로 구현이 가능하므로 압축과 암호화는 단대단(End-to-end)간에 이루어진다[1][2]. 두 번째로 IP계층에서 IP in IP 방식의 터널을 이용하는 방식으로는 IP/IP, GRE, IPSec 등이 있다[3].

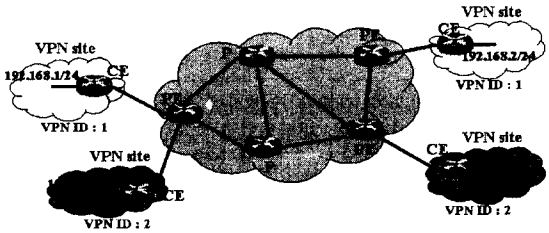
또한, IP패킷을 다른 터널링된 IP패킷에 실어 보내는 방식과 달리 MPLS를 기반으로 하는 방식에서는 LSP(Label Switch Path)를 설정하여 터널로 이용한다. MPLS 기능을 이용한 라우터는 VPN의 가입자들 사이에서 LSP를 설정하고, 다른 VPN에 속한 LSP들은 서로 다른 정책으로 관리함으로써 기존의 IP 터널링 방식과 비교하여 향상된 성능뿐 아니라 FEC의 설정에 따라 QoS나 보완 등 다양한 서비스의 제공도 가능하게 된다.

MPLS는 이러한 다양한 잇점을 바탕으로 VPN을 구성하기 위한 최적의 방안으로 고려되었으며, 현재 RFC2547 "BGP/MPLS VPN"이 MPLS VPN의 표준으로 정립되고 있다.

그러나, "BGP/MPLS VPN"[4]에서 제시된 모델은 제공자 네트웍에 기반한 MPLS VPN의 구성방안으로서, PE 라우터가

VPN의 모든 정보를 유지 관리한다. 결국, VPN site의 추가 혹은 삭제에 의한 topology 변화가 PE 라우터에게 많은 부담을 주게 되므로 VPN 시스템의 확장성(scalability)이 상대적으로 떨어진다. 또한, VPN site의 모든 정보를 PE 라우터에서 관리하기 때문에 보안에 관한 요구사항이 더 필요하게 될 것이며, 사용자의 다양한 요구사항을 수용하기 위한 유연성(flexibility)을 보장하기가 어렵게 된다.

따라서, 본 논문에서는 Customer site, 즉 VPN site내에 속한 CE 라우터에 기반한 MPLS VPN을 대안으로 제시하였고, Network 기반 MPLS VPN에서의 방식과 달리 CE 라우터 기반의 MPLS VPN 제어 요소 및 동작 절차를 지역망과 제공자 망에서의 MPLS Edge 라우터에 기반하여 설계하였다. [그림 1]에는 구성된 VPN의 예를 보여준다.



[그림 1] VPN 구성 예

결국, PE 라우터는 VPN 서비스를 위한 최소한의 VPN membership 정보, 즉 위치정보만을 갖고 있게 되므로 서비스 제공자내의 PE 라우터 성능에 부담을 주지 않게 된다. 따라서, 서비스 제공자 네트웍으로부터의 영향을 최소화 할 수 있기 때문에 Network 기반의 MPLS VPN에 비해 VPN의 독립성(independence)이 상당히 보장된다. 또한, 시스템의 확장성, 보안 등 다양한 측면에서도 많은 장점을 갖는다.

	PE 라우터 기반의 MPLS VPN	CE 라우터 기반의 MPLS VPN
독립성	부족	우수
확장성	복잡	용이
보안	어려움	우수
복잡도	제공자 네트웍 복잡	제공자 네트웍 단순

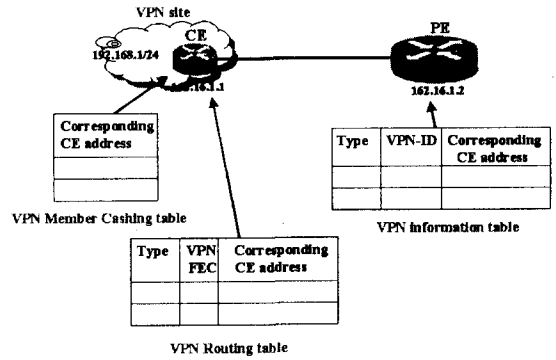
[표 1] MPLS VPN 구성방식의 비교

3. 설계 및 구현

3.1 요구사항 및 제어요소

VPN site를 대표하는 CE 라우터는 ISP로부터 공중망에서 사용되는 중복되지 않는 유일한 IP address를 할당받고, 자신이 속한 VPN site의 VPN ID를 알고 있어야 한다. 그리고 VPN site는 같은 VPN ID를 사용하는 site들 사이에 중복되지 않는 local IP address들을 사용한다. 또한 자신과 같은 VPN에 속한 VPN site의 CE 라우터의 주소, 즉 Corresponding CE address를 저장할 VPN Member Caching table과 Corresponding CE address로부터 받은 VPN site의 라우팅 정보를 저장 할 수 있는 VPN Routing table을 포함한다.

PE 라우터는 stub link로 연결된 CE 라우터 및 다른 PE 라우터로부터 받은 VPN ID 및 Corresponding CE address를 저장할 수 있는 VPN Information table을 갖는다. 각 라우터에 필요한 제어요소는 [그림 2]와 같다.

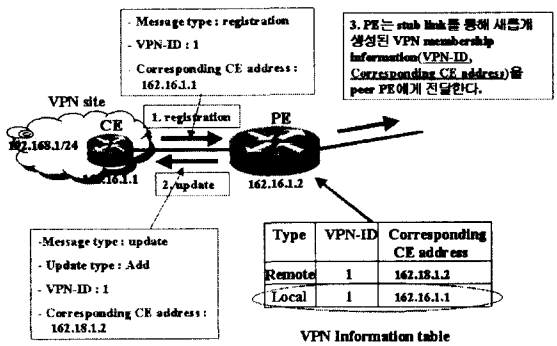


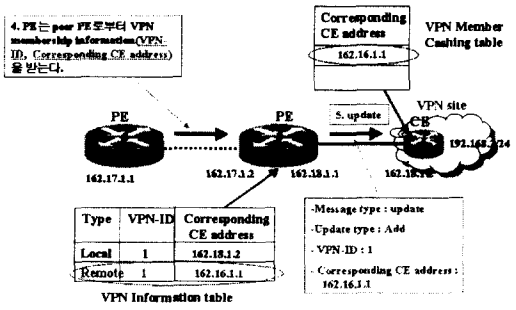
[그림 2] VPN 동작을 위한 CE/PE 라우터에서 테이블 구성

3.2 새로운 VPN site 생성

새로운 VPN site가 생성되면 CE 라우터는 VPN membership information(VPN ID, Corresponding CE address)을 stub link로 연결된 PE 라우터에게 전달한다. PE 라우터는 CE 라우터로부터 받은 VPN membership information을 VPN Information table에 저장한 뒤 VPN Information table을 검색해서 VPN ID가 같은 Corresponding CE address들을 찾아서 VPN membership information을 전송한 CE router에게 전달한다. 또한 PE 라우터는 새로 생성된 VPN site의 CE router로부터 받은 VPN membership information을 다른 모든 PE 라우터에게 전송한다.

PE 라우터가 다른 PE 라우터로부터 새로 생성된 VPN site에 대한 VPN membership information을 받으면 자신의 VPN





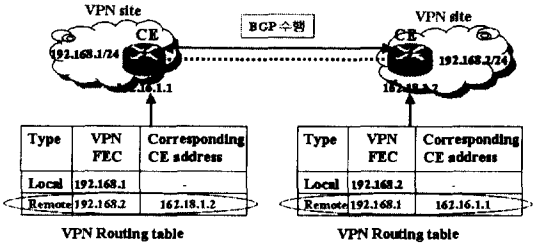
[그림 3] 새로운 VPN site 생성 시 등록 과정

Information table에 삽입하고 VPN Information table을 검색하여 같은 VPN ID를 가진 VPN site가 stub link로 연결되어 있으면 stub link로 연결된 CE 라우터에게 VPN membership information을 전송한다. CE 라우터는 PE 라우터로부터 받은 Corresponding CE address를 VPN Member Caching table에 삽입한다.

결국 [그림 3]과 같은 과정을 통하면 VPN site의 CE 라우터는 자신과 같은 VPN ID를 갖는 CE 라우터의 address, 즉 Corresponding CE address를 알 수 있다.

3.3 VPN site 간 데이터 전송

이렇게 해서 자신과 같은 VPN ID를 갖는 site를 대표하는 CE 라우터의 address들을 알게 되면 CE 라우터들 사이에 BGP를 수행하여 각 VPN site에 대한 도달정보를 알 수 있고 이러한 정보를 각 CE 라우터의 VPN Routing table에 삽입한다[5].

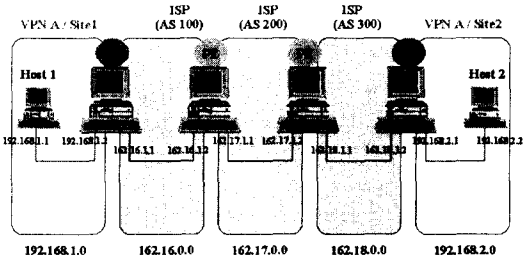


[그림 4] CE간 BGP를 이용하여 도달정보의 교환

CE 라우터는 VPN Routing table에 삽입된 새로운 라우팅 정보에 대해 LSP(Label Switch Path) 설정을 수행한다. 새로 삽입된 FEC에 대한 label을 할당받기 위해 라우팅 정보를 보낸 CE 라우터에게 label을 요청하여 할당받고 CE 라우터의 LIB 테이블에 삽입한다. 또한 CE 라우터는 새로운 라우팅 정보를 보낸 CE 라우터와 LSP의 설정이 필요하다. 이렇게 하여 LSP가 설정되면 각 VPN site사이에 MPLS 방법을 이용하여 데이터를 전송할 수 있다.

3.4 구현

CE 라우터 기반 MPLS VPN은 Redhat Linux version 6.0, Linux Kernel version 2.2.9 상에서 C 언어를 이용하여 구현하였다. CE와 PE 라우터에서 VPN을 서비스를 지원하기 위해 필요한 제어요소인 정보 테이블들은 링크 리스트를 이용하여 구현하였고, CE와 PE 사이의 메시지 전달을 위한 통신을 위해 TCP(UDP)/IP Socket을 이용하여 구현하였다. 구현된 MPLS VPN은 [그림 10]과 같은 환경에서 시험을 수행하였다.



또한, 다양한 시나리오에 따라 각 메시지의 송수신 및 VPN 서비스를 지원하기 위한 제어요소의 동작이 올바르게 동작하는 것의 여부를 확인하였으며, 최종적으로 Host 간의 데이터 전달 또한 정상적으로 수행되었다.

4. 결론 및 향후과제

본 논문에서는 MPLS 도메인 내에서 CE 라우터 기반 VPN을 구성하기 위한 구조적 모델을 정의하였고, 제안된 모델의 제어요소 및 동작절차를 설계하였다.

이 논문에 기술된 구조적인 구성은 MPLS VPN을 만들기 위해 유연하고 확장 가능한 기초을 제공할 것이다. 또한, 본 논문에서 설계 및 제안한 MPLS 망에서 VPN 제공 방안은 MPLS의 응용 서비스로서 가상사설망을 투명성있게 확장하기 위한 기반 자료로 활용될 수 있을 것이다.

향후 연구과제로는 공중망을 이용하여 구축되는 가상사설망에서 이용자에게 사설망과 동일한 서비스뿐만 아니라 QoS도 지원할 수 있도록 확장하는 것도 고려해야 한다.

[참고문헌]

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

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

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

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

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