MPLS 기반 VPN의 설계

이준호°, 서동운, 강성용, 박석천
경원대학교 전자계산학과
scpark@mail.kyungwon.ac.kr

Design of VPN based on MPLS

Joon-Ho Lee°, Dong-Woon Seo, Sung-Yong Kang, Seok-Cheon Park
Dept. of Computer Science, Kyungwon University

요 약

통신 사업자는 많은 상호 독립적인 보이지 않는 네트워크를 제공하기 위해 가상의 네트워크를 운영한다. 기업 입장에서는 인트라넷이 주로 웹과 기타 IP 기술에 기초하는데, 이를 투명성 있게 확장하기 위해 IP VPN의 요구가 증가했었다.

VPN은 사용자의 요구에 따라 WWW 및 멀티미디어 서비스 등의 IP 서비스를 수용하는 방향으로 전개되고 있다. 그러나 IP VPN으로 가는데 있어서의 단점인 터널링과 암호화에 따른 오버헤드 문제를 해결해야 하는데, 이를 위하여 인터넷 솔루션으로 도입하고 있는 MPLS 망을 기반으로 하여 VPN을 제공하면 터널링이 주는 오버헤드 없이 서비스를 제공할 수 있다.

본 논문에서는 MPLS 망에서 VPN을 지원하는 방안을 제안하고, MPLS VPN 제어 요소 및 동작 절차를 설계하였다.

1. 서 론

MPLS 기술을 VPN에 적용하게 되면 터널링이 주는 추가의 오버헤드 없이 원격지 사용자들과 사무소가 마치 본사의 네트워크에 직접 연결되듯이 시내 전화로 ISP의 네트워크에 연결할 수 있게된다. 따라서 VPN과 동일한 프라이버시 기능을 제공할 수 있으며, 연결장치가 필요없는 네트워크를 구축할 수 있다. VoIP(Voice over IP)나 비디오 스트리밍 등의 멀티미디어 데이터가 전송되기 위해서는 QoS를 제공하는 진보한 트래픽 관리가 필수적이다. MPLS는 하나의 IP 세션 내에 있는 패킷들을 네트워크 계층에서 하나의 흐름으로 묶은 다음 경로를 따라 라우터를 쉽게 통과할 수 있도록 각각의 세션에 레이블을 달아준다. 일단 흐름이 이루어지면 MPLS는 전달을 위해 전용 데이터 회선에 그 흐름을 맵핑한다. MPLS의 레이블을 이용하여 서로 다른 VPN간에 트래픽을 격리시켜 효율적인 패킷 전송을 하는 것이 MPLS 기반 VPN 기술의 핵심이며, 이를 간단히 MPLS VPN이라 한다.

본 논문에서는 MPLS VPN 구조와 그에 따른 제공방안과 제어요소 및 동작절차를 설계하였다.

2. MPLS 기반 VPN의 제공 방안

기본적인 MPLS VPN의 구조는 그림 1과 같이 사설 네트워크의 PNL과 제공자 네트워크의 PEL, 코어 LSR, 그리고 PNL과 PEL을 물리적으로 연결하는 공유 엑세스 링크(SAL)로 구성되어 있다.

MPLS VPN은 높은 확장성, 효과적인 비용, 그리고 사용자 요구의 광범위한 핸들링을 제공하여 IP 서비스를 낮은 비용으로 제공해 준다.

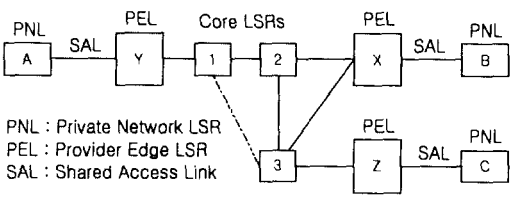

그림 1. MPLS 기반 VPN 구조

MPLS 기반의 VPN을 기존의 오버레이 솔루션과 비교하면 터널링이나 암호화 없이도 트래픽을 분리하고 프라이버시를 제공한다는 것이다. MPLS 망에서 VPN을 지원하기 위한 MPLS 프로토콜로 BGP 및 LDP를 이용하여 라우팅 정보의 분배 및 레이블 할당을 통한 경로설정의 절차를 수행한다.

그림 2에 MPLS 기반의 VPN이 동작하는 원리를 나타내었다. 트래픽은 각 VPN을 위한 논리적으로 명확한 포워딩 테이블을 사용하여 VPN들 간에 분리된다. 입력 인터페이스에 기초하여 스위치는 BGP의 도움을 받아 특정 포워딩 테이블을 선택하여 그 VPN에서 유효한 목적지만을 리스트한다. 익스트라넷의 생성으로 제공자는 VPN들 사이에 도달성을 명확히 형성한다.

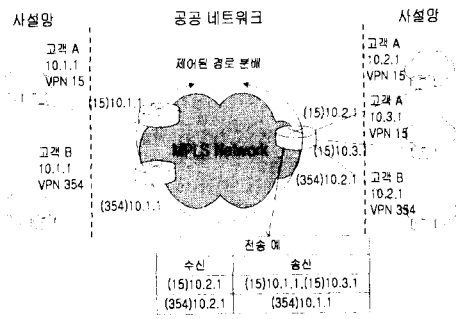

그림 2. MPLS 기반 VPN의 원리

VPN과 MPLS망 사이에 라우팅 정보의 배포 방안과 MPLS에서 VPN 바인딩의 배포 방안은 다음과 같다.

(1) VPN 라우팅 정보 배포

고객 측을 서비스 제공자 네트워크로 연결하는 서비스 제공자 LSR은 고객 측에 속한 VPN이 VPN ID를 리스트 함으로써 구성된다. 고객 라우터가 서비스 제공자 LSR을 갖는 MPLS에 관여할 때, BGP는 IP 도달성 정보와 레이블 바인딩을 고객 측과 서비스 제공자 네트워크 사이에 배포하기 위해 사용된다.

(2) MPLS 망에서 VPN 바인딩의 배포

서비스 제공자 LSR이 고객 사이트로부터 VPN ID와 도달성 정보의 바인딩을 인식할 때, 이 연결된 정보는 어떻게해서든지 같은 VPN의 멤버들인 다른 고객 사이트에게 알려야 한다. OSPF와 LDP, 혹은 BGP가 서비스 제공자 네트워크 내의 도달성 정보와 레이블 바인딩을 배포한다.

3. MPLS VPN 제어 요소의 설계

레이블 스위칭은 기존 라우팅 프로토콜인 BGP, OSPF를 이용하여 네트워크 노드들의 라우팅 정보를 생성하는 MPLS의 기본 기능을 포함하며, 또한 BGP를 통하여 네트워크 에지 부분에서 VPN의 라우팅 정보인 VPN FIB 생성하게 된다. 네트워크 내에서는 LDP 절차를 통해 레이블 할당 및 레이블 정보를 배포하게 된다. ATM 인터페이스 상에서 동작하는 MPLS VPN 프로토콜 제어 요소들을 정의하면 그림 3과 같다.

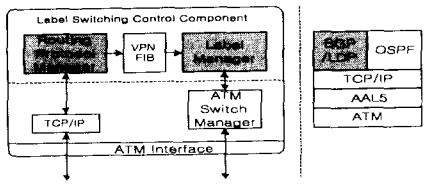

그림 3. ATM 기반 MPLS VPN 프로토콜

- 라우팅 프로토콜 관리 : BGP를 이용한 VPN 라우팅 정보의 배포
- 레이블 관리 : LDP를 이용한 제공자 네트워트에서 패킷 포워딩

ATM 기반의 MPLS 망에서도 결국 ATM 스위치를 이용하여 IP 패킷을 전송하여야 하기 때문에 LDP 프로토콜의 요구에 따라서 ATM 스위치 레벨의 접속을 설정/해제 및 관리하는 GSMP(General Switched Management Protocol)를 사용한다.

4. MPLS VPN 동작 절차의 설계

MPLS에 기반하는 VPN 지원 방안은 MPLS 에지 라우터에 연결된 VPN에 VPN ID를 할당하고 이를 라우팅 정보에 포함시켜 MPLS 내에서 유일한 주소를 가지고 각 노드마다 네트워크 주소 변환(NAT : Network Address Translation)을 하지 않고 목적지로 레이블 스와핑을 통하여 패킷을 전달하는 동작을 수행한다.

독립적인 LSP 설정방법은 초기화 메시지에 옵션 파라미터를 정의하는 순차적인 LSP 설정 방법과는 달리,초기화 메시지의 옵션 파라미터에 DOD 모드로 정의되어 있으며, 각 LSR이 독립적인 분배 방식을 사용하여 LSP를 설정하는 절차는 그림 4와 같다.

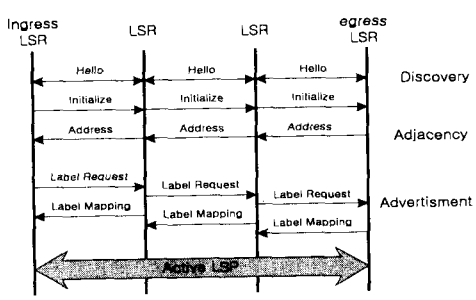

그림 4. MPLS VPN의 LSP 설정 절차(독립적)

VPN을 지원하는 MPLS의 동작 절차를 간단히 설명하면 VPN ID를 부여하여 VPN-IP 주소를 생성하고, VPN 라우팅 정보를 배포하고, 레이블과 VPN-IP 주소를 맵핑하여 NAT 없이 제공자 네트워크에서 유일한 주소를 제공한다. 이러한 라우팅 정보를 가지고 네트워크내 포워딩 경로를 설정하여 VPN 간에 통신을 설정하게 된다.

본 논문에서 설계한 MPLS 망에서 VPN을 지원하는 동작 절차는 그림 5와 같다.

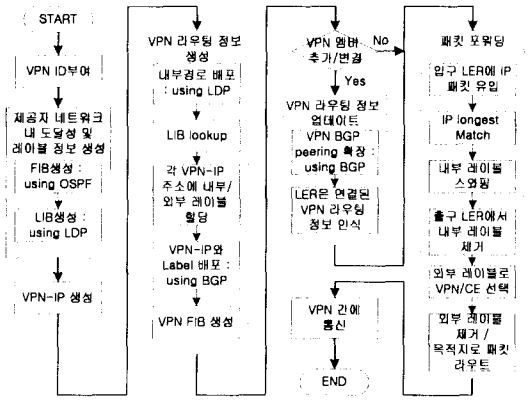

그림 5. MPLS VPN의 동작 절차 흐름도

(1) VPN ID의 부여

VPN마다 고유한 ID로 RD(Route Distinguisher)를 부여하며, VPN 안에서 IP 주소는 유일하다. VPN ID를 통하여 같은 VPN인지 알 수 있는 정보를 갖게 된다.

(2) 내부 도달성 및 레이블 배포

각 코어 LSR은 내부 경로 도달성과 내부 레이블 바인딩을 유지하는 에지 LSR을 포함한다. 기존 라우팅 프로토콜인 OSPF를 통하여 FIB를 생성하고, LDP를 통하여 LIB를 생성한다.

(3) VPN-IP 주소의 생성

입구 에지 LSR은 정적인 라우팅, BGP, RIP를 이용하여 경로를 인식한다. 여기서 고객 주소는 유일성을 보증할 수 없는데, 에지 LSR에서는 IP(v4) 주소를 전체적으로 유일한 VPN-IP 주소로 변환한다. VPN-IP 주소는 64 비트의 RD와 고객 IP 주소가 결합한 것으로 BGP를 통하여 출구 에지 LSR로 전송된다.

(4) VPN 도달성 정보 생성

VPN-IP 주소는 관련된 레이블과 함께 BGP 멀티 프로토콜 확장의 NLRI 필드로 전송된다. 64 비트 확장된 속성으로 부가 필드는 VPN-IP와 결합되며, VPN FIB를 구축한다.

(5) 레이블과 VPN-IP 주소와 맵핑

BGP는 VPN-IP와 결합된 레이블을 배포하고, 필터는 통신 속성을 확장하는데 적용된다. LDP는 내부 레이블과 결합된 레이블을 배포하며 BGP next hop을 추가한다. 각 고객의 주소를 위해 에지 라우터는 순환 탐색(recursive lookup)으로 'BGP next hop'의 경로를 찾으며, LIB를 생성한다. 각 VPN-IP 주소는 내부 레이블과 외부 레이블을 할당받는다.

(6) 트래픽 분리를 통한 포워딩

모든 다음의 코어 라우터는 내부 레이블만으로 패킷을 스위치한다. 출구 LER은 내부 레이블을 제거하고, 외부 레이블을 이용하여 VPN 및 고객 LER을 선택하여 패킷을 전송한다. 외부 레이블은 고객 LER에 패킷이 라우트되면서 제거된다.

(7) VPN 간 통신

소스 VPN과 목적 VPN 간에 통신은 '통신 필터링'에 의하여 제어된다. 외부 VPN은 중추 방화벽 제어에 의하여 내부 VPN이 동작하는 동안에 any-to-any 접속을 할 수 있다.

4. 결 론

MPLS 기반 VPN 기술은 MPLS 표준과 함께 BGP 표준을 지원한다. 레이블에 부속된 패킷에 대한 우선전달 경로 정보와 같은 QoS 요구사항을 레이블에 포함시킬 수 있도록 MPLS에 대한 확장 기능을 제공하며, 서비스 공급업체는 이 정보를 이용해 수많은 내부 네트워크 경로 중에서 특정 네트워크 경로를 구분할 수 있다. 또한, MPLS 확장 기능을 통해 VPN ID를 부여해 터널링 없이 가상 공간을 제공하며, PVC/SVC에 따른 콜 셋업 절차가 복잡하지 않아 관리가 쉬우며, 확장성을 확보할 수 있는 것이 특징이다.

본 논문에서는 VPN과 MPLS의 개요 및 동작을 분석하였으며, 이를 바탕으로 MPLS 망에서 VPN을 지원하는 방안을 제시하였다. MPLS 망의 동작을 위해 BGP를 이용하는 라우팅 프로토콜 관리부와 LDP를 이용하는 레이블 관리부를 포함하는 MPLS VPN 제어 요소를 설계하고, 이를 토대로 MPLS 망에서 VPN 지원 방안의 동작 절차를 설계하였다. 또한, 본 논문에서 설계 및 제안한 MPLS 망에서 VPN 제공 방안은 국내에서도 인터넷 솔루션으로 도입한 MPLS의 응용 서비스로서, 가상 사설망을 투명성있게 확장하기 위한 기초 기반 자료로 활용될 수 있을 것으로 사료된다.

참고문헌

[1] R. Callon, P. Doolan, N. Feldman, A, Fredette, G. Swallow, A. Viswanathan, "A Framework for Multiprotocol Label Switching," draft-ietf-mpls-framework -02.txt, IETF, Nov. 1997.

[2] Eric C. Rosen, Arun Viswanathan, Ross Callon, "Multiprotocol Label Switching architecture," draft-ietf-mpls-arch-04.txt, IETF, Feb. 1999.

[3] Juha Heinanen, Telia Finland, "VPN support with MPLS," draft- heinanen -mpls-vpn-01.txt, IETF, Sep. 1998.

[4] Jerry Ryan, "Multiprotocol Label Switcing (MPLS)," Technology Guide Techguide .com, 1998.

[5] Jhon Amoss, Daniel Minoli, "IP Applications with ATM," McGraw-Hill, 1998.

[6] E. Rosen, Y. Rekhter, "BGP/MPLS VPN," RFC 2547, Net Working Group, Mar. 1999