MPLS 네트워크 상에서의 CUG 서비스 제공을 위한 구조 설계

권 민 희, *백 승 진
경북대학교 전자공학과, *경북대학교 정보통신학과
전화 : 053-940-8898 / 핸드폰 : 011-9950-6724

Structure Design for CUG(Closed User Group) Services provision at the MPLS network

Min Hee Kwon, Seung Jin Baek
Dept. of Electrical Engineering, Kyungpook National University
E-mail : minhi@intizen.com

Abstract

This paper is proposed structure which it sees currently the problem point which it follows in the independent space for work which the members who do a same work from the environment which is to fall the at distance, therefore the MPLS based VPN necessary to follow, it forms the small-scale group which is closed again with the CUG(Closed User Group) it will be able to own jointly information to present a structure, the individual small-scale groups are closed from outside and the group members are the CUG authentication process for the security maintenance the model which is possible.

I. 서론

인터넷의 고속화로 인해 네트워크의 사용자가 점차 늘어남에 따라 네트워크의 크기도 기하급수적으로 커졌으며, 이에 인터넷 서비스 제공자들은 광대한 네트워크를 관리, 유지하기에 점차 많은 비용과 노력이 들이게 되었다. 이러하므로 네트워크를 효율적으로 관리할 수 있는 방법이 필요하게 되었다. 또한 현재는 과거에 비해 멀티미디어 서비스가 증가됨에 따라 그만큼 데이터의 양도 커졌으므로 이에 대응할 수 있는 방안으로 MPLS데이터의 양도 커졌으므로 이에 대응할 수 있는 방안을 들 수 있다. MPLS의 대표적인 특징으로 특정한 경로의 폭주를 방지하고 IP 트래픽을 전달하는데 효율성을 높일 수 있는 트래픽 엔지니어링기술과 VPN(Virtual Private Network)의 제공이 용이하다는 것이다. 그리고 VPN에서 문제가 될 수 있는 QoS(Quality of Service)를 MPLS와 연동해서 사용함으로써 안정적이고 효율적으로 구현할 수 있다.

본 논문은 현재 거리상으로 떨어져 있는 환경에서 같은 작업을 하는 구성원들끼리의 독립된 작업 공간 확보에 따른 문제점이 제기되고 있으므로, MPLS를 기반으로 하는 VPN에서 필요에 따라 다시 폐쇄된 소규모의 그룹을 형성함으로써 정보를 공유할 수 있는 CUG(Closed User Group)의 구조를 제시하며, 이에 개별적인 소규모 그룹들은 외부로부터 폐쇄되어 있으며 그룹 구성원들은 CUG인증과정을 거치므로 그룹들간에도 보안이 유지 가능한 모델을 설계하고자 한다.

II. MPLS 네트워크 기반의 VPN

2.1 MPLS 네트워크 기반의 VPN 구조

MPLS 네트워크는 가입자들과 망을 연결하는 기능을 하는 LER(Label Edge Router)를 통과하는 모든 데이터들은 목적지까지의 정보를 가진 작은 레이블(Label)을 달게 된다. 이 레이블은 라우터마다 헤더를 분석하여 다음 목적지를 정하는 것에 비해 LSR(Label Switched Router)을 거쳐 최적의 경로(LSP(Label Switched Path))를 통해 최종 목적지로 전송하게 되므로 빠른 라우팅이 가능하다.

또한 ATM이나 Frame Relay를 기반으로 하는 VPN에서는 가입자가 속한 VPN에 연결된 ATM이나 Frame Relay등의 링크 계층에서 PVC(Permanent Virtual Circuit)를 통해 서로 분리되는 방식으로 QoS를 보장하게 된다. 그러나 MPLS VPN에서는 PVC로 연결하는 것이 아니라 Ingress LSR로부터 Egress LSR까지 정해진 경로인 LSP로 연결함으로 다른 트래픽의 암호화 과정 없이 각 VPN의 데이터를 분리함으로 QoS를 제공할 수 있다. 즉 IP계층의 비연결형 네트워크의 장점을 포함하면서, 미리 정의된 VC(Virtual Circuit)없이 QoS를 제공하는 것이다.

2.1 BGP/MPLS VPN의 운영 모델

이 절에서는 제안된 여러 VPN 모델중의 하나로 RFC 2547bis에서 제안한 VPN 서비스 모델인 BGP/MPLS VPN을 이해하는데 중점을 둘 것이다.

BGP/MPLS VPN은 네트워크 계층에서 제공되는 것으로 BGP를 이용하여 라우팅의 정보와 VPN의 사용자들의 정보를 서로 교환함으로써 VPN을 구성한다. 그러므로 데이터 링크 계층의 터널링 기법이나 IPSec 같은 트래픽의 인증이나 암호과 과정 없이도 각 트래픽에 레이블을 할당하게 되므로 VPN의 트래픽은 서로 분리가능하다.

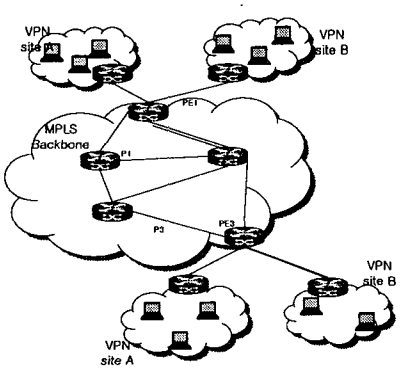

그림1. MPLS/VPN 네트워크 토폴로지

그림 1은 단일 서비스 사업자가 BGP/MPLS VPN 서비스를 여러 사용자에게 제공하는 네트워크 토폴로지의 예이다.

위 그림에서 사이트A에 있는 모든 호스트들은 다른 편의 사이트A의 모든 호스트들과 통신이 가능하며, 사이트B 또한 다른 사이트B에 있는 모든 사이트들과 통신할 수 있다. 서비스 제공자의 백본망을 통해 VPN 라우팅 정보를 분배하는데 BGP를 사용하고 한 VPN 사이트에서 다른 VPN 사이트로 VPN 트래픽을 전달하는데 MPLS를 사용한다. 이에 BGP/MPLS VPN에서의 두 가지의 제어흐름으로 구성되는데, 첫번째는 호스트들 간의 데이터 트래픽을 포워딩하는데 사용되는 데이터의 흐름이며, 두번째는 VPN의 경로 분배와 레이블 스위치 경로인 LSP를 설정하는 제어흐름이다.

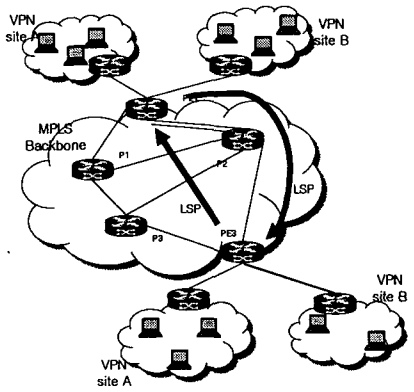

그림2. 사이트A에서 사이트B로의 데이터이동과 LSP

위의 그림은 사이트A에서 사이트B로의 데이터의 흐름의 방향과, PE1에서 PE2로의 두 PE간의 LSP방향을 나타내고 있다. LSP의 설정은 MPLS를 백본으로 사용하여 VPN 트래픽을 전달하려면 경로를 탐색하는 PE 라우터와 트래픽을 전달하는 라우터간의 LSP를 설정해야 한다.

레이블은 BGP를 통해서 각각의 서비스제공자들의 라우터에 분배된 후 패킷 두 가지 레벨의 레이블을 덧붙여져 전송된다.

그림3에와 같이 패킷이 들어오면 먼저 포워딩 테이블에 의해 어느 VPN에 속한 패킷인지 판별한 후 도착지에 따라서 BGP를 통해 분배된 레이블이 먼저 붙여지고, MPLS 내부의 네트워크 안에서 전송될 수 있도록 해주는 레이블이 나중에 붙여지게 된다.

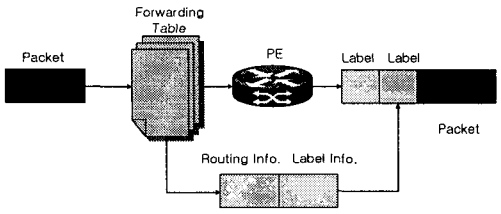

그림3. BGP/MPLS VPN에서의 레이블 스택

이와 같이 LSP가 결정되면 트래픽은 정해진 경로로만 전송되므로 중간에서의 침입이 어려워진다. 또한 MPLS 네트워크 안에서의 서로 다른 VPN에 속한 사용자들 사이에는 LSP가 존재하지 않으므로 서로 구분되는 것이다.

III. CUG 서비스 제공을 위한 구조설계

본 장에서는 CUG 서비스를 하기위한 레이블이 붙여지는 과정과 실제 레이블이 붙여진 패킷들이 목적지가 결정된 후 정해진 경로로 전달될 수 있도록 설계하였다.

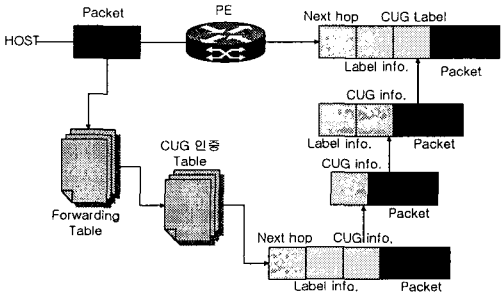

그림4. BGP/MPLS VPN에서의 CUG 서비스를 하기 위한 레이블 스택

그림4에서와 같이 레이블은 BGP를 통해서 각각의 서비스제공자들의 라우터에 분배된 후 CUG 인증과정을 거쳐 패킷은 세 가지 레벨의 레이블을 덧붙여져 전송된다. 먼저 패킷이 들어오면 VPN 포워딩 테이블에 의해 어느 VPN에 속한 패킷인지 판별한 후 도착지에 따라서 BGP를 통해 분배된 레이블이 붙여지고, MPLS 내부의 네트워크 안에서 전송될 수 있도록 레이블이 붙여지며 마지막으로 어느 CUG에 속한 HOST인지 판별하여 적확한 HOST에게 전달 될 수 있도록 한다.

다음 그림은 패킷이 실제 호스트에서 시작하여 포워딩 테이블과 CUG 인증테이블을 거쳐 붙여진 레이블에 따라 정해진 경로로 전송되는 것이다.

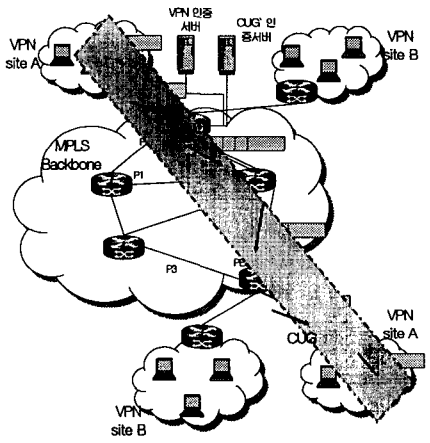

그림5. CUG 서비스에서의 패킷 포워딩

그림5는 구성된 VPN안에서 다시 소규모 CUG서비스를 하려면, 필요에 따라 호스트들은 CUG를 형성하기 위해 호스트 자신의 정보를 CUG 인증서버에 보내고 인증과정을 거쳐서 소규모의 그룹을 형성할 수 있다. 이렇게 구성된 CUG간에는 특정 호스트로부터 다른 같은 그룹에 속한 호스트로 데이터를 보낼 수 있으며, 이는 포워딩 테이블을 거쳐 다시 CUG 인증 테이블의 정보와의 검증이 후 정해진 호스트로 데이터를 전송될 수 있다. 패킷에 붙여진 레이블들은 들어온 IP나 다른 정보들에 의해서 패킷이 속한 VPN이 정해지게 되고 다음 내부 네트워크로 전송되면서 레이블은 제거되며, 마지막으로 특정 IP를 가진 호스트에게 전달된다.

IV. MPLS 네트워크 상에서의 CUG 서비스 구성

본 장에서는 앞서 구성한 BGP/MPLS 네트워크 기반의 VPN에서 사용자들의 요구에 따른 보다 소규모 그룹인 CUG 서비스를 제공할 수 있도록 설계하여 다음 그림에 전체 시스템의 구성도를 나타내었다.

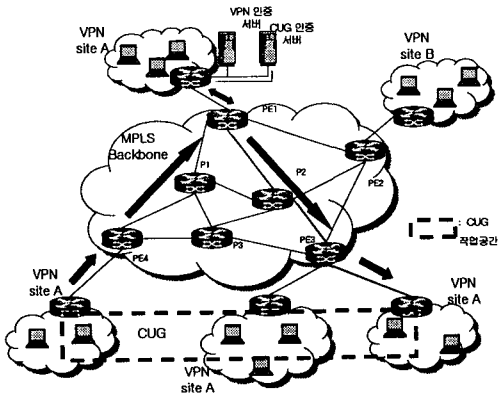

그림 2. MPLS 네트워크 상에서의 CUG서비스 제공을 위한 구조

위 그림과 같이 각 그룹의 가입자들은 VPN 그룹간의 정보를 관리하는 서버 외에 소그룹을 형성하기위해서는 CUG 인증 서버를 거쳐 한번의 인증과정을 더 거친 다음 인터넷상에 공동의 작업공간을 형성할 수 있게 된다. 이는 MPLS 네트워크 상의 VPN 환경에서 CUG 서비스를 제공함으로써 현재 구성원들 간의 필요에 따라 보안성 유지되는 작은 그룹을 운영할 수 있으므로 자료 공유에 대한 부담을 줄일 수 있으며, 거리가 떨어진 곳에서 같은 작업을 하는 구성원들끼리 장소에 제약받지 않는 네트워크상에 독립된 작업공간을 확보할 수 있게 되는 것이다. 예를 들어, 본사와 하나 이상의 지사들이 VPN을 구성하고, 그 안에서 다시 본사와 지사에서 같은 업무를 하는 팀들 중 특정 팀의 기밀문서를 서로 공유하고자할 때 이들은 전체 그룹 내 다른 구성원들과 무관하게 하나의 팀이 CUG를 구성함으로써 특정 구성원들 간에 독립적인 공간을 마련할 수 있으며, 신뢰성 있는 통신이 가능하게 된다.

V. 결론

본 논문은 MPLS 네트워크 상에서의 CUG 서비스 제공을 위한 구조를 제시함으로써 서비스 제공자 입장에선 가입자들의 요구조건에 따른 차별화된 서비스를 제공할 수 있으며, 가입자들은 그룹들간의 공유에서 좀더 세부적으로 환경에 적합한 VPN을 구성할 수 있다. 또한 BGP/MPL VPN 또한 MPLS의 내부망 자체가 안전하다고 가정한다면, MPLS 네트워크 안에서 각각의 패킷들은 레이블의 LSR에 의해 서로 분리가 되므로 안정성을 보장해 줄 수 있다. 그러나 CE와 PE 라우터 사이의 트래픽들은 보호되지 않으므로, IPSec이나 다른 암호와 알고리즘을 함께 적용한다면, 좀 더 안전한 통신이 가능할 것이다. 앞으로 이에 더하여 구성원들 간의 모든 구간에서의 보안문제를 좀더 보완하여 무선 인터넷 환경으로의 확장에도 적용할 수 있을 것이다

참고문헌(또는 Reference)

[1] Jim Guichard, Ivan Pepelnjak, "MPLS and VPN Architectures," 2001 Cisco.

[2] Chuck Semeria, "RFC 2547bis : BGP/MPLS VPN Fundamentals," 2001 Juniper Networks.

[3] RFC 2401, "Security Architecture for the Internet Protocol," Nov. 1998.

[4] RFC 3031, "Multiprotocol Label Switching Architecture," Jan. 2001

[5] 이동훈, 임채훈, "MPLS와 MPLS 기반 VPN," Dec. 2001.

[6] 인터넷 보안 기술포럼 ISTF-003, "Implementation Technology for secure VPN in IP Layers," May. 2001.