제 18 회 한국정보처리학회 추계학술발표대회 논문집 제 9 권 제 2 호 (2002.11)

MPLS 기반 L2/L3 VPN 서비스를 위한 QoS 지원 방안

윤호선, 김영희, 양선희
한국전자통신연구원 네트워크연구소 인터넷기술연구부
e-mail : {hsyoon,yhkim,shyang}@etri.re.kr

QoS Supporting Plan for MPLS based L2 & L3 VPN Service

Hosun Yoon, Yong Hee Kim, Sunhee Yang
Internet Technology Dept., Network Laboratory, ETRI

요 약

인터넷 사용의 급속한 증가와 다양한 서비스에 대한 요구사항을 수용하기 위해서 가입자망과 백본망 사이에 위치한 메트로망의 진화에 관심이 집중되고있다. 메트로망의 병목 현상을 해결하기 위한 방법중의 하나로 MPLS 를 이용하는 해결책이 제안되고 있으며 이에 대한 연구가 활발히 진행되고 있다. 메트로망에서 MPLS 를 활용하는 경우, 2 계층 VPN 서비스를 제공하기 위해서 Martini 가 제안한 방식이 사용될 수 있으며 , 3 계층 VPN 서비스를 제공하기 위해서는 RFC 2547 방식이 이용될 수 있다. 본 논문에서는 메트로망에서 VPN 서비스를 제공하기 위한 MPLS 기반 2 계층 및 3 계층 VPN 서비스를 위한 기능 모델과 QoS 모델을 정의하고, 정의된 QoS 모델을 지원하기 위한 포워딩 정보를 생성하는 절차에 대해서 기술한다.

1. 서론

인터넷 사용의 급속한 증가와 다양한 서비스에 대한 요구사항을 수용하기 위해서 망 사업자들은 전송 속도의 고속화와 다양한 서비스를 수용하기 위한 기술들을 망에 적용하여왔다. 이러한 노력으로 백본망의 트래픽 처리 용량은 크게 증가하였으며 MPLS (MultiProtocol Label Switching)와 같은 기술을 적용함으로써 다양한 서비스를 제공할 수 있게 되었다. 하지만 가입자망과 백본망 사이에 위치하는 메트로망의 진화 속도는 백본망이나 가입자 망의 진화 속도를 따라가지 못하고 있으며, 이러한 현상은 메트로망이 병목 현상을 일으키게 하는 원인이 되었다. 이러한 메트로망의 병목 현상을 해결하기 위해서 제안되고 있는 방법들 중의 하나가 MPLS 를 적용하는 것이다. MPLS 는 트래픽 엔지니어링 기술을 이용하여 망 자원을 효율적으로 사용할 수 있으며 다양한 서비스를 제공할 수 있다.

메트로망에 MPLS 가 적용되는 경우에 VPN(Virtual Private Network) 서비스를 제공하기 위해서 널리 사용되고 있는 방법이 Martini 가 제안한 방식이다. Martini 는 점대점(point to point)간에 2 계층 VPN 서비스를 제공하기 위해서 두 개의 규격을 발표하였다. 하나는 2 계층 VPN 과 관련된 정보를 전달하기 위해서 LDP(Label Distribution Protocol)를 확장하는 방법에 대해서 기술하고 있으며, 다른 하나는 데이터가 MPLS 망을 통과하기 위한 캡슐화 방법을 기술하고 있다.

메트로망에서 2 계층 VPN 뿐만 아니라, 3 계층 VPN 서비스도 제공할 필요가 있다. 3 계층 VPN 서비스는 RFC2547 방식이 널리 사용되고 있다.

본 논문에서는 메트로망에서 2 계층 및 3 계층 VPN 서비스를 제공하기 위한 VPN 서비스 모듈에 대해서 기술한다. 본 논문의 2 장에서는 MPLS 기반 VPN 기술의 개요를 서술하고, 3 장에서는 VPN 서비스를 제공하기 위한 기능 모델을 기술하며, 4 장에서는 VPN 서비스를 위한 QoS(Quality of Service) 모델을 정의하고, 5 장에서는 포워딩 정보를 생성하기 위한 절차에 대해서 기술하고 결론을 맺는다.

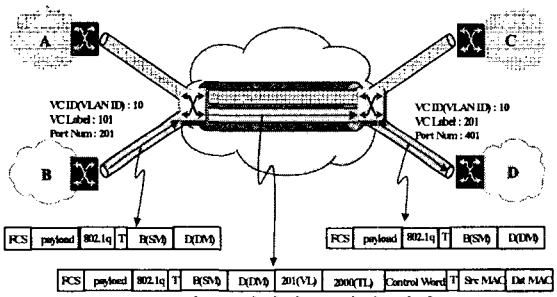
2. MPLS 기반 VPN 기술 개요

이 장에서는 MPLS 기반 2 계층 및 3 계층 VPN 기술에 대해서 살펴본다. 본 논문에서 기술하는 내용은 가입자와 망 사업자간의 인터페이스가 ePON(Ethernet Passive Optical Network) 및 이더넷인 경우를 가정하고 있다.

2.1 MPLS 기반 2 계층 VPN 기술

MPLS 기반 2 계층 VPN 기술에는 Martini 방식과 Kompella 방식이 있다. 현재 많은 업체들은 Martini 방식을 채택하고 있다. Martini 방식에는 데이터가 MPLS 망을 통과하기 위한 캡슐화 방법과 VPN 관련 정보를 전달하기 위해서 LDP 를 확장하는 방법을 기술한 두 종류의 규격서가 있다.

VPN 과 관련된 정보를 전달하기 위해서 LDP 는 VC(Virtual Circuit) FEC TLV 를 추가하였다. 이 TLV 에는 VC ID, Group ID, 그리고 인터페이스에 대한 각종 파라미터 값들이 포함되며, Label TLV 를 통해서 VC Label 을 전달한다. 가입자와의 인터페이스가 이더넷이고 VLAN 기능이 지원되는 경우, VC ID 는 VLAN ID 와 동일하게 사용할 수 있다.



[그림 1] 데이터 포워딩 절차

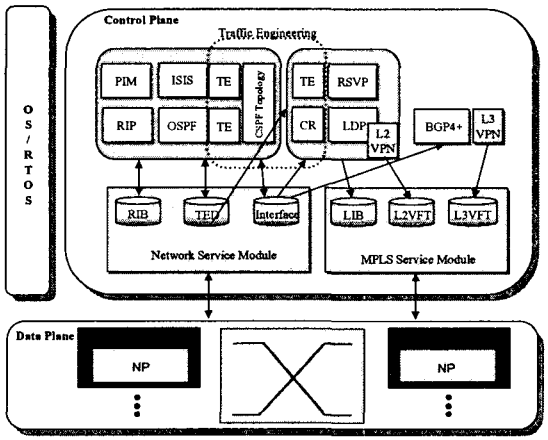
그림 1 은 LDP 를 통해서 전달된 정보를 이용해서 가입자로부터 입력되는 데이터를 목적지까지 전달하는 과정을 나타낸다. LER(Label Edge Router)과 LER 사이에는 Martini 가 제안한 캡슐화 방식에 따라서 인코딩된다. MPLS 망 내에서는 바깥쪽 VLAN 해더와 터널 레이블 값만 스와핑되고, Egress LER 에서는 VC 레이블을 이용해서 가입자까지 데이터를 전달한다. 가입자로부터 입력되는 데이터는 VLAN ID 를 이용해서 룩업하고, Egress 에서는 VC 레이블을 이용해서 목적지까지의 경로를 결정한다[1, 2].

2.2 MPLS 기반 3 계층 VPN 기술

일반적으로 널리 사용되고 있는 MPLS 기반 3 계층 VPN 기술은 RFC2547 방식이다. 이 방식은 BGP4 를 확장해서 VPN 관련 정보와 VPN 용 라우팅 정보를 전달한다. MPLS 기반 VPN 기술은 사설 주소를 지원해야만 하고, 이러한 사설 주소를 구분하기 위해서 RD(Route Distinguisher)를 이용하며, 라우팅 정보를 해당 그룹간에만 공유하기 위해서 Import/Export RT(Route Target)를 사용한다. 또한 MPLS 망으로부터 수신되는 데이터를 가입자측으로 전달하기 위해서 VPN 레이블을 사용한다[3, 4, 5].

3. MPLS VPN 기능 모델

이 장에서는 MPLS 기반 2 계층 및 3 계층 VPN 서비스를 제공하기 위한 구조에 대해서 기술한다. 이 장에서 기술하는 내용은 Zebra OS 에 기반을 두고 있다.



[그림 2] MPLS VPN 블록 구성도

그림 2 에서 NSM(Network Service Module)은 Zebra OS 에서 제공하는 모듈로서 라우팅 프로토콜 데몬들과 통신을 통해서 RIB(Routing Information Base) 정보를 관리하며, 각종 인터페이스 정보도 관리하고 있다.

그림 2 에서 보듯이 2 계층 VPN 은 확장된 LDP 를 통해서 VPN 과 관련된 정보들을 송신 및 수신하며, 이러한 정보를 바탕으로 포워딩 정보를 생성하고 MSM(MPLS Service Module)에 전달한다. MSM 에서는 생성된 포워딩 정보를 Data Plane 에 전달함으로써 가입자측으로부터 입력되는 데이터를 룩업할 수 있게 된다. 3 계층 VPN 은 확장된 BGP4 프로토콜을 통해서 가입자측의 라우팅 정보를 피어에게 전달하며, 상대 피어로부터 라우팅 정보를 수신한다. 수신된 라우팅 정보를 MSM 에 전달하며, MSM 에서는 수신된 정보와 LSP 정보를 이용해서 포워딩 정보를 생성하고 Data Plane 에 전달한다.

가입자측과의 인터페이스를 VPN 용으로 설정하는 경우에는 MPLS 망으로부터 수신되는 데이터를 가입자측으로 전달하기 위한 포워딩 정보를 생성해야만 한다. 3 계층 VPN 인 경우에는 VPN 레이블을 이용하며, 2 계층 VPN 인 경우에는 VC 레이블을 포워딩 정보의 키로 사용한다.

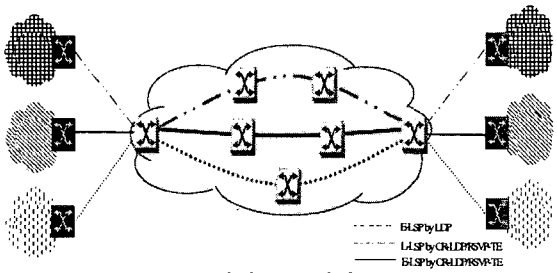
각종 레이블 값들은 레이블 pool 에서 할당받으며, 할당 받은 레이블들은 시스템 내에서 유일한 값이다. 또한 레이블 값을 사용하지 않는 경우에는 해당 레이블 값을 반환함으로써 레이블 값을 재사용할 수 있다. 단, 레이블 값을 반환하는 경우에는 반환되는 레이블 값이 MPLS 망 내에서 효력이 완전히 상실된 후에 반

환되어야만 한다.

Data Plane 은 여러 장의 LP(Line Processor)로 구성되어 있으며, 각 LP 에는 하나나 그 이상의 NP(Network Processor)로 구성된다. 이러한 LP 들은 가입자측과 망측으로 구분되며, 데이터는 NP 로 입력되서 스위치를 거쳐서 다시 NP 로 출력된다.

4. VPN 서비스를 위한 QoS 모델

MPLS 기반 VPN 서비스는 MPLS 에서 제공하는 트래픽 엔지니어링 기술을 이용해서 QoS 를 지원할 수 있으며, QoS 를 지원하기 위해서 CR-LDP(Constraint-based Routed LDP)와 RSVP-TE(Resource reSerVation Protocol Traffic Engineering)와 같은 프로토콜들이 사용된다.



[그림 3] VPN 서비스를 위한 QoS 모델

그림 3 은 VPN 서비스를 위한 QoS 모델을 나타낸다. 먼저, LDP 는 각 LER 간에 E-LSP(EXP inferred LSP)를 설정하고, CR-LDP 및 RSVP-TE 는 E-LSP 나 L-LSP(Label-only inferred LSP)를 설정한다. CR-LDP 나 RSVP-TE 에 의해서 설정되는 LSP 는 ER-LSP(Explicitly Routed LSP) 혹은 CR-LSP(Constraint-based Routed LSP) 모두를 포함한다.

각 가입자에서 Ingress LER 로 데이터를 전달할 때, DSCP(Differentiated Services Code Point)나 Priority 비트를 이용해서 서비스의 등급을 표시하고, Ingress LER 에서는 데이터에 표시된 서비스 등급을 VPN 레이블(2 계층 VPN 인 경우에는 VC 레이블)과 LSP 레이블(2 계층 VPN 인 경우에는 터널 레이블)의 EXP 필드에 표시한다. 각 LSR 에서는 레이블에 포함된 EXP 필드 값을 이용해서 큐잉 및 스케쥴링을 수행한다. 이러한 방법으로 CoS 를 제공하는 LSP 가 E-LSP 이다. 반면에 Label 자체가 QoS 특성을 나타내는 LSP 가 L-LSP 이다. 단, L-LSP 는 각종 QoS 파라미터들을 구체적으로 정의할 수 있으며, E-LSP 는 몇 가지 등급으로 QoS 를 정의할 수 있다.

VPN 서비스를 이용하는 가입자는 세 종류의 QoS 모델 중에서 하나를 선택할 수 있다. 먼저 LDP 가 설정한 LSP 를 이용하는 가입자는 자신의 서비스 종류에 따라서 데이터에 등급을 표시해서 망 사업자에게 전달한다. 이 경우에는 등급별로 CoS 를 제공하며, 경로 보호와 같은 망 장애를 극복할 수 있는 서비스를 제공 받지 못한다.

두 번째로 CR-LDP 나 RSVP-TE 가 설정한 E-LSP 를 이용하는 경우에는 망 상황에 따라서 다양한 경로를 이용할 수 있으며 망 장애를 처리할 수 있는 서비스를 제공 받을 수 있다. 또한 가입자측에서 데이터에 표시한 서비스 등급에 따라서 CoS 를 제공받을 수 있다.

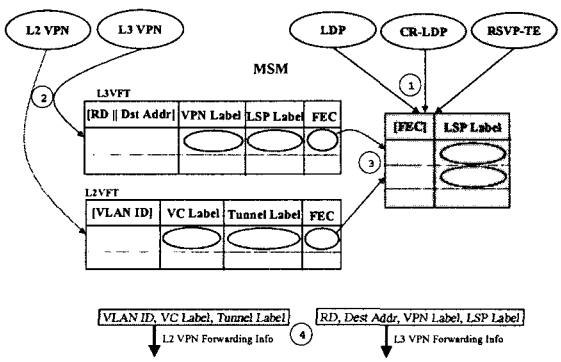
마지막으로 CR-LDP 나 RSVP-TE 로 설정한 L-LSP 를 이용하는 경우에는 망 상황에 따라서 다양한 경로를 이용할 수 있으며 망 장애를 처리할 수 있는 서비스를 제공받을 수 있다. 또한 가입자와 망 사업자간에 계약한 QoS 파라미터에 따라서 서비스를 제공한다. 이러한 경우에는 일반적으로 E-LSP 에서 제공할 수 있는 것보다 더욱 좋은 QoS 특성을 가지고 L-LSP 를 설정한다.

5. QoS 지원을 위한 포워딩 정보 생성 절차

이 장에서는 4 장에서 기술한 VPN 서비스를 위한 QoS 모델을 지원하기 위한 포워딩 정보를 생성하는 방법을 기술한다. MPLS 기반 2 계층 VPN 및 3 계층 VPN 서비스를 위한 포워딩 정보는 Ingress 를 위한 포워딩 정보와 Egress 를 위한 포워딩 정보가 있다.

5.1 Ingress 를 위한 포워딩 정보 생성 절차

MSM 은 VPN 서비스를 위한 포워딩 정보를 생성하고 전달하는 기능을 수행하기 위해서, 시그널링 프로토콜에서 생성된 LSP 설정 정보와 2 계층 VPN 에서 생성된 VPN 관련 정보 및 3 계층 VPN 에서 생성한 VPN 용 라우팅 정보를 관리한다.



[그림 4] Ingress 를 위한 포워딩 정보 생성 절차

그림 4 에서 보듯이 2 계층 VPN 과 3 계층 VPN 을 위한 포워딩 생성 절차는 동일하다. 먼저, 그림 4 의 1 번 절차를 통해서 각종 시그널링 프로토콜에서 설정한 LSP 관련 정보를 수신한다. 그림 4 의 2 번 절차는 VPN 블록으로부터 포워딩을 위한 정보를 수신하는 절차이다. 만약 가입자와 망 사업자간에 LDP 가 설정한 LSP 를 이용하도록 계약이 성립되었다면, 그리고 2 계층 VPN 서비스를 이용한다면 2 계층 VPN 으로부터 [VLAN ID, VC Label, FEC] 정보가 MSM 으로 전달되며, 3 계층 VPN 서비스를 이용한다면 3 계층 VPN 블록으로부터는 [RD, Dest Addr, VPN Label, FEC] 정보가 전달

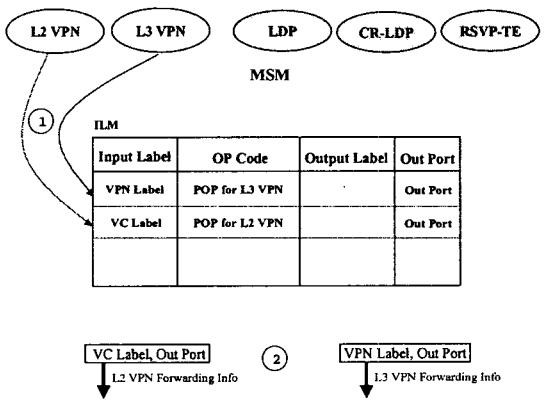
된다. 여기서, FEC 는 BGP4+의 Next Hop 주소(피어의 주소)가 된다. 이러한 정보를 수신한 MSM 은 FEC 를 키로 이용해서 LSP 관련 정보를 관리하는 테이블로부터 LSP Label 을 선택한다. 이러한 동작은 그림 4 의 3 번 절차를 통해서 수행된다. 그림 4 의 4 번 절차와 같이 생성된 포워딩 정보를 Data Plane 으로 전달한다. 그림 4 의 3 번 절차에서 FEC 를 이용해서 선택한 LSP 는 LDP 가 설정한 LSP 이며, 이러한 LSP 는 4 장에서 언급한 E-LSP 가 된다.

가입자가 CR-LDP 나 RSVP-TE 가 설정한 LSP 를 이용하기를 원하는 경우에는 운용자의 개입이 필요하다. 즉, 운용자는 VPN 그룹이 이용할 LSP 를 매핑시키고, 이러한 매핑 정보와 VPN 용 라우팅 정보를 이용해서 그림 4 의 2 번 절차를 통해서 MSM 으로 포워딩을 위한 정보를 전달한다. 2 번 절차를 통해서 전달되는 정보는 2 계층 VPN 인 경우에는 [VLAN ID, VC Label, Tunnel Label] 등이며, 3 계층 VPN 인 경우에는 [RD, Dest Addr, VPN Label, LSP Label] 등과 같다. 이러한 정보는 그림 4 의 4 번 절차를 통해서 Data Plane 으로 전달된다.

LSP 가 삭제되거나 장애가 발생하는 경우에는 MSM 에서 삭제를 위한 포워딩 정보를 생성해서 Data Plane 에 전달한다.

5.2 Egress 를 위한 포워딩 정보 생성 절차

MPLS 망으로부터 입력되는 VPN 용 데이터는 목적지 주소나 목적지 MAC 주소를 이용해서 룩업을 하지 않고, 레이블을 이용해서 목적지로 향하는 포트를 결정한다.



[그림 5] Egress 를 위한 포워딩 정보 생성 절차

그림 5 에서 보듯이, 레이블에 대해서 출력 포트가 결정되어 있으며, 이러한 정보는 인터페이스를 설정하는 과정에서 생성되는 정보이다. 물론 각 레이블에 대해서 결정된 가입자측과의 인터페이스에 따라서 데이터를 인코딩하는 과정이 필요하다.

이전 LSR 이 Penultimate Hop 인 경우에는 VPN 을 위한 레이블만 데이터에 포함되서 수신되며, 이러한 경우에는 ILM(Incoming Label Map)에서 해당 정보를 검색하고 레이블은 POP 한다. 반면에 Penultimate Hop 이 아닌 경우에는 LSP 를 위한 레이블과 VPN 을 위한 레이블 모두가 데이터에 포함되서 수신되며, LSP 를 위한 레이블은 POP 하고 VPN 에 관련된 레이블은 데이터를 출력할 포트를 결정하고 POP 한다.

6. 결론 및 추후 연구 과제

본 논문에서는 MPLS 기반 L2/L3 VPN 기능 모델을 정의하고, VPN 서비스를 위한 QoS 모델을 정의하였으며, 이러한 QoS 모델을 제공하기 위한 포워딩 정보 생성 절차를 기술하였다. 본 논문에서 기술한 설계 방식은 VPN 서비스를 위해서 다양한 QoS 를 제공할 수 있도록 한다.

추후에는 Data Plane 에서의 내부 채널 연결 절차 및 방법에 따라 포워딩 정보를 정의하고 Data Plane 과의 구체적인 API 를 정의할 필요가 있으며, LSP 설정 시 구체적인 QoS 파라미터와 등급에 따른 QoS 속성을 결정할 필요가 있다. 또한 시스템 장애 및 망 장애 발생에 대한 구체적인 처리 절차 및 API 를 정의할 필요가 있다.

참고문헌

[1] Luca Martini et al., "Transport of Layer 2 Frames over MPLS", draft-martini-l2circuit-trans-mpls-08, Nov 2001

[2] Luca Martini et al., "Encapsulation Methods for Transport of Layer 2 Frames over MPLS", draft-martini-l2circuit-encap-mpls-04, Nov 2001

[3] E. Rosen et al., "BGP/MPLS VPNs", rfc2547, Mar 1999

[4] Y.Rekhter, T.Li, "A Border Gateway Protocol 4 (BGP-4)", RFC 1771, Mar. 1995

[5] S.Ramachandra, D.Tappan, "BGP Extended Communities Attribute", draft-ramachandra-bgp-ext-communities-04, Dec. 2000

[6] 윤호선, 김숙연, 양선희, "MPLS 를 이용한 VPN 기능 모델 설계", Proc. of 한국정보처리학회, 제 7 권 2 호, 2000 년

[7] 윤호선, 윤현식, 양선희, 강민수, "ACE2000 BGP/MPLS VPN 서비스 개발", Proc. of 한국정보처리학회, 제 8 권 2 호, 2002 년 10 월