품질차별화가 가능한 고신뢰도의 MPLS 기반 IP-VPN 서비스 모듈

(QoS Differentiated and Highly Reliable MPLS based IP-VPN Service Module)

윤 호 선 † 양 선 희 †† 이 유 경 ††
(HoSun Yoon) (SunHee Yang) (Yoo-Kyoung Lee)

요 약 본 논문에서는 ACE2000 MPLS 시스템의 핵심 응용 기능으로 개발된 MPLS 기반 IP-VPN 서비스 모듈의 설계와 구현에 대해서 기술한다. ACE2000 MPLS VPN 서비스 모듈은 BGP 확장 프로토콜을 이용해서 개발되었다. 이러한 IP-VPN 서비스 모듈은 MPLS 트래픽 엔지니어링을 이용해서 차별화된 QoS를 지원한다. 또한 고신뢰도 서비스 제공을 위해서 시스템 및 포워딩 엔진 재시동 기능과 경로 보호 기능을 지원한다.

키워드 : MPLS, IP-VPN, BGP/MPLS VPN, QoS, 경로보호, 트래픽 엔지니어링

Abstract *In this paper, we design and implement a MPLS based IP-VPN service module as an application for ACE2000 MPLS system. ACE2000 MPLS VPN service module has been developed using the BGP4 extension protocol. The IP-VPN service module supports differentiated QoS using the MPLS traffic engineering. In addition, it offers a path protection mechanism and the restart mechanism of MPLS system and forwarding engine for supporting a highly reliable service.*

Key words : MPLS, IP-VPN, BGP/MPLS VPN, QoS, path protection, traffic engineering

1. 서 론

VPN(Virtual Private Network) 기술은 기존의 전용선을 이용하여 기업간 정보 제공을 위한 통신망을 구축하는 것이 아니라, 공중망을 통해 기업 내부뿐만 아니라 기업 외부에 있는 직원이 기업 망으로 접근할 수 있도록 가상의 통신망을 구축하는 것이다. 이러한 기술은 전용선을 이용하는 것에 비해서 월등히 낮은 비용을 가지고 전용선 서비스와 유사한 서비스를 제공 받을 수 있다는 장점 때문에 그 수요가 크게 증가하고 있다.

VPN 서비스를 제공하는 기술은 전달망 기술에 따라 전용선, ISDN(Integrated Services Digital Network), 프레임 릴레이, ATM(Asynchronous Transfer Mode), IP 터널링 등의 다양한 기술이 사용되고 있다. 그 중에서 가장 널리 사용되고 있는 기술은 ATM이나 프레임 릴레이 PVC(Permanent Virtual Circuit)를 이용하는 계층 2 VPN과 IPSec을 이용하는 IP 터널링 VPN이다. 특히, IPSec 터널링을 이용한 VPN 기술은 인터넷이 기업 활동의 중요한 인프라로 확산됨에 따라 크게 각광받고 있다. 하지만 IPSec을 이용한 VPN은 품질 보장이 제한적이고, 가입자 사이트간 풀 메쉬 IP 터널을 구성해 주어야 하며, 키 분배, 인증 및 암/복호화와 같은 보안을 위한 많은 인프라가 요구된다. 이러한 많은 오버헤드 때문에 정보보호를 위한 또 다른 부가 장치가 필요한 단점을 갖게 된다.

이러한 문제점을 극복하기 위해서 MPLS(Multi Protocol Label Switching)에 기반을 둔 VPN 기술이 관심을 끌고 있다. MPLS 기반 VPN 서비스는 라우팅 정보를 선별적으로 전달함으로써 가입자를 그룹핑하며, MPLS LSP(Label Switched Path)를 이용해서 터널링을 제공한다. 이러한 MPLS 기반 IP-VPN 서비스는 IPSec을 이용한 VPN이 가지고 있는 많은 문제점들을

† 정 회 원 : 한국전자통신연구원 네트워크연구소 연구원
yhs@etri.re.kr
†† 비 회 원 : 한국전자통신연구원 네트워크연구소 연구원
shyang@etri.re.kr
leeyk@etri.re.kr
논문접수 : 2002년 2월 6일
심사완료 : 2002년 10월 8일

해결하고 있다. 즉, MPLS에서 제공되는 트래픽 엔지니어링 기술을 이용하여 차별화된 QoS(Quality of Service) 및 경로 보호 기능을 제공하기가 용이하며, MPLS 망의 에지에서만 VPN 기술을 제공하면 VPN 서비스가 가능하므로 확장성이 뛰어나며, 구현이 용이한 장점이 있다. 반면에 안전성(Security) 측면에서의 문제점 때문에 MPLS 기반 IP-VPN에 정보보호 기법을 도입하는 방법들이 논의되고 있다[1,2].

MPLS 기반 IP-VPN을 구현하는 방법은 BGP4 (Border Gateway Protocol) 확장 프로토콜을 이용하는 방법과 가상 라우터(Virtual Router)를 이용하는 방법이 있다. 가상 라우터를 이용하는 방법은 확장성에 문제가 있기 때문에 현재 BGP4 확장 프로토콜을 이용하는 방안이 주로 연구되고 있다.

본 논문에서는 ACE2000 MPLS 시스템에 탑재하기 위한 MPLS 기반 IP-VPN 서비스 모듈의 설계 및 구현에 관해서 기술한다. 본 논문에서 기술되는 ACE2000 MPLS 기반 VPN 서비스는 MPLS LSP를 이용하여 차별적인 QoS를 지원하고, MPLS의 트래픽 엔지니어링 기술을 이용하여 경로보호와 같은 고품질 서비스를 제공하며, 하나의 LSP를 하나나 그 이상의 VPN 그룹들이 공유할 수 있도록 설계되었다.

본 논문은 2장에서 ACE2000 MPLS 시스템에 대해서 기술하며, 3장에서 ACE2000 MPLS 시스템에서 VPN 서비스를 효율적으로 수행하기 위한 설계 방법과 각종 절차들에 대해서 기술한다. 그리고 4장에서는 차별적인 QoS를 지원하기 위한 절차와 시스템 및 망 장애 발생에 대한 고신뢰도의 서비스를 제공하기 위한 절차에 대해서 기술한다.

2. ACE2000 MPLS 시스템

ACE2000 MPLS 시스템은 ACE2000 스위치 시스템에 MPLS 모듈을 탑재한 ATM 기반 MPLS LER (Label Edge Router) 시스템이다. 그림 1의 시스템 구조에서 보듯이 시스템은 크게 ATM 스위치 모듈(SFM: Switch Fabric Module), 가입자 정합 모듈, 스위치 제어 모듈, 운용관리를 위한 MAS(Maintenance & Administration Server) 모듈, MPLS 제어 장치(MSC : MPLS Service Controller), 그리고 ATM 연결 제어 장치(ACC:ATM Call Controller)로 구성된다.

MSC 기능 블록에는 TCP/IP 프로토콜, RIP (Routing Information Protocol) / OSPF(Open Shorest Path First) / BGP4 / IS-IS(Intermediate System-to-Intermediate Sysytem) 라우팅 프로토콜, LDP(Label Distribution Protocol) / CR-LDP (Constraint-based Routing LDP) / RSVP-TE (Resource Reservation Protocol with Traffic Engineering) 시그널링 프로토콜, 트래픽 엔지니어링 및 VPN 분록 등의 응용 소프트웨어가 포함된다. 아울러 자원 관리 블록에서는 LSP 설정을 위한 자원관리와 포워딩 엔진내의 포워딩 엔트리 제어 기능을 담당한다. MSC의 라우팅 및 시그널링 프로토콜이 동작하여 만들어진 라우팅 및 포워딩 정보는 내부 IPC(Inter Processor Communication) 채널을 통해 각 포워딩 엔진으로 전달된다. 포워딩 엔진 기능은 가입자 채널을 통해 유입되는 IP 패킷을 MSC 블록에서 내려준 포워딩 정보를 이용하여 룩업하여 적절한 LSP로 매핑시켜주는 기능을 하며, 가입자 정합단에 위치한다.

MAS 기능 블록은 ACE2000 MPLS 시스템을 운용 및 관리하기 위한 제반 운용 기능을 처리한다.

MIM(MPLS Interface Module)은 MPLS를 위한 가입자 정합 기능을 갖는 MPLS 인터페이스 모듈로써 MPLS 패킷을 위한 포워딩 기능 및 VC 머징 기능을 가지고 있다. 또한 ATM 셀에 대해서는 AIM(ATM Interface Module)으로 통과(bypass)시킨다.

스위치 제어 모듈은 GSMP(General Switch Management Protocol) 슬레이브를 이용해서 스위치를 제어하며, MPLS를 위한 자원과 ATM을 위한 자원을 독립적인 영역으로 관리한다.

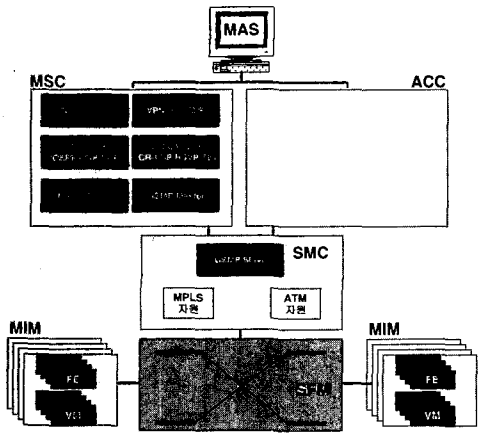

그림 1 ACE2000 MPLS 시스템 구조

3. ACE2000 MPLS VPN 서비스 모듈

이 장에서는 ACE2000 MPLS VPN에 대한 요구사항 및 VPN 서비스를 제공하기 위한 구조 및 설계에 대해

서 기술한다.

3.1 ACE2000 MPLS VPN 서비스 요구사항

ACE2000 MPLS 기반 IP-VPN 기술은 다음과 같은 요구사항을 만족하도록 설계 및 구현되었다.

먼저, 사설 주소를 지원해야만 한다. 사설 주소는 VPN 그룹 내에서만 유일하며, 이러한 사설 주소를 구분하기 위해서 RD(Route Distinguisher)라는 구분자를 사용한다[3,4,5].

기업 내에서의 기업 활동을 위한 인트라넷(Intranet) 뿐만 아니라, 협력 업체 및 기업 외부에서의 접속을 가능하게 하는 엑스트라넷(Extranet) 서비스를 지원해야만 한다. 이러한 요구사항을 만족하기 위해서 하나의 VPN 그룹에 여러 Import RT(Route Target) 및 Export RT를 할당할 수 있으며, 각 PE(Provider Edge)에서는 이러한 다수 개의 RT들을 처리할 수 있도록 설계되었다[3,4].

라우팅 프로토콜을 이용해서 VPN 그룹간 라우팅 정보를 제한적으로 분배해야만 한다. 이러한 요구사항을 만족하기 위해서 BGP4 라우팅 프로토콜을 확장하였다. BGP4 확장 프로토콜은 일반적인 라우팅 정보뿐만 아니라, VPN을 위한 라우팅 정보도 함께 전달하는 것이 가능하다. 실제로 BGP4 확장 프로토콜에서는 RD, Export RT, 그리고 VPN 레이블과 같은 VPN용 정보들을 분배한다[6,7,8,9].

VPN 그룹별로 차별화된 QoS 서비스를 제공할 수 있어야만 한다. 이러한 요구사항은 ACE2000 MPLS 시스템에서 제공하는 트래픽 엔지니어링 기술을 이용한다. 즉, CR-LDP나 RSVP-TE와 같은 시그널링 프로토콜을 이용해서 QoS를 지원하는 LSP를 설정하고, 설정된 LSP를 VPN 그룹별로 이용할 수 있도록 한다[10].

망 장애나 시스템 장애 발생 시 적절한 처리 절차가 있어야만 한다. 이러한 요구사항을 만족하기 위해서 망 장애를 극복하기 위한 경로 보호 기능과 시스템 장애 극복을 위한 시스템에 대한 재시동 및 이중화 기능을 가지고 있다. 재시동 기능에는 MSC 재시동 기능 및 VPN 블록의 재시동 기능, 그리고 포워딩 엔진의 재시동 기능을 모두 지원하며, 이러한 재시동 절차를 거치면 재시동 절차 이전의 상태로 복구가 가능하다. 또한 MSC 및 ACC 등의 이중화 기능을 적용함으로써 시스템 장애 발생 시 피해를 최소화 할 수 있도록 설계되었다.

VPN 서비스를 위한 설정 및 관리가 각 노드에서 MAS를 이용해서 가능해야만 하며, VPN 망을 위한 EMS(Element Management System)를 통해서도 가능해야 한다. 이러한 요구사항을 만족하기 위해서 ACE 2000 MPLS VPN에서는 SNMP(Simple Network Management Protocol)를 이용해서 EMS 기능을 제공하며, EMS에서 VPN 관련 정보를 설정할 수 있으며 현재 서비스중인 VPN 정보도 GUI(Graphic User Interface) 창을 통해서 운용자가 쉽게 이해할 수 있도록 구현하였다.

ACE2000 MPLS VPN 시스템은 다음과 같은 용량을 지원하도록 설계되었다. 먼저 10 기가당 16000개의 사이트 및 그룹을 관리할 수 있으며, 포워딩 엔진당 지원 가능한 포워딩 엔트리 수는 8000개이다. 만약 포워딩 엔진이 16개라면, 최대 지원 가능한 포워딩 엔진의 개수는 8K * 16이다. 이것은 ACE2000 MPLS VPN 시스템이 포워딩 엔트리를 포워딩 엔진별로 관리하기 때문에 가능하다.

3.2 ACE2000 MPLS VPN 기능 구조

ACE2000 MPLS VPN 서비스 모듈은 라우팅 정보 교환을 위한 BGP4 확장 블록, 가입자 인터페이스 설정 기능을 위한 블록, LSP 설정 및 관리를 위한 블록, 자원 관리 및 포워딩 엔진 관리를 위한 블록, 그리고 명령어 입력 부분 등으로 구성된다[11].

그림 2는 VPN 서비스 제공을 위한 VPN 기능 블록과 타 블록간의 관계를 나타낸 것이다. 그림 2의 VPN_CFB는 MPLS VPN 서비스를 제공하기 위한 블록이며, 이 블록에서 VPN 그룹 및 사이트 관리, VPN용 라우팅 테이블 관리, VPN용 LSP 관리 및 VPN 레이블 관리, 포워딩 엔트리 생성을 위한 정보 생성 및 전달과 같은 MPLS VPN 서비스를 제공하기 위한 기능을 수행한다.

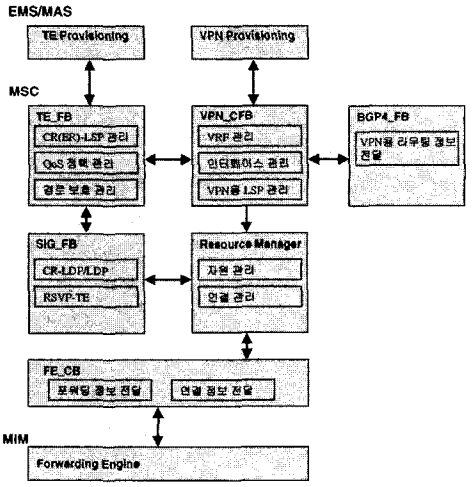

그림 2 MPLS VPN 기능 모듈 블록도

TE_FB는 LSP 설정을 위한 가입자 정보 및 LSP 정보와 경로보호를 위한 각종 정보들을 관리하는 블록이며, SIG_FB는 TE 기능 블록으로부터 수신된 LSP 설정 요청에 따라서 LSP를 설정하고 해제하기 위한 블록으로써 LDP/CR-LDP/RSVP-TE와 같은 시그널링 프로토콜을 갖는다. BGP4_FB는 BGP4 확장 블록으로써 일반적인 라우팅 정보와 VPN을 위한 확장 정보를 송/수신하기 위한 블록으로써, MPLS VPN에서 생성되거나 삭제되는 라우팅 정보와 VPN 관련 정보를 상대 피어들에게 전달하는 역할을 수행한다. 자원 관리 블록(Resource Manager)은 자원 관리 및 내부 채널 설정을 수행하며, FE_CB은 포워딩 엔진에 각종 채널 정보 및 포워딩 엔트리를 전달하기 위한 블록이다. 구체적인 동작 절차는 참고문헌을 참조하기 바란다.

3.3 MPLS VPN 서비스를 위한 기능

이 절에서는 rfc2547 모델을 바탕으로 실제 ACE2000 MPLS VPN 시스템에서 MPLS VPN 서비스를 제공하기 위한 절차들을 기술한다.

3.3.1 가입자 인터페이스 설정

CE(Customer Edge)로부터 입력되는 패킷은 수신되는 인터페이스에 따라서 VPN용 패킷인지 여부와 어느 VPN 그룹인지가 결정된다. 포워딩 엔진이 이러한 역할을 수행하도록 하기 위해서는 포워딩 엔진에 가입자측 정보를 전달하는 절차가 필요하다. 그림 3은 가입자 인터페이스를 설정하는 절차에 대해서 나타낸 것이다.

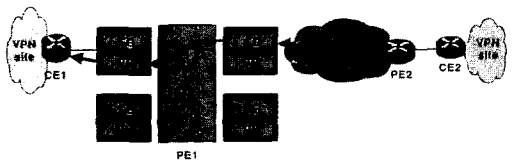

그림 3 가입자 인터페이스 설정 절차

가입자측과 망 사업자측 간에 VPN 서비스 여부를 결정짓기 위해서 각 사이트별로 논리적인 인터페이스(ATM인 경우, VPI/VCI로 구별)를 설정할 필요가 있다. ACE2000 MPLS VPN에서는 가입자측 인터페이스를 설정하는 과정을 통해서 두 가지 일을 수행한다. 하나는 해당 인터페이스를 VPN용 인터페이스로 설정하고, 그 인터페이스를 이용하는 VPN 그룹을 결정한다. 또한 이러한 정보들을 실제로 포워딩 작업을 수행하는 포워딩 엔진에 전달한다. 다른 하나는 MPLS 망으로부터 수신되는 데이타를 VPN 레이블을 이용해서 룩업할 수 있도록 해당 정보를 포워딩 엔진에 전달하고, 룩업된 데이타를 가입자측까지 전달하기 위한 시스템 내부 채널을 설정한다.

예를 들어서, CE1으로부터 데이타가 입력되는 경우, 포워딩 엔진에서는 해당 인터페이스를 통해서 수신된 데이타가 VPN용 데이타이며, 이 데이타가 어느 VPN 그룹을 위한 것인지 결정하기 위한 정보들을 가입자 인터페이스 설정 절차를 통해서 포워딩 엔진에 전달한다. 또한 CE2의 호스트로부터 CE1의 호스트까지 데이타를 전송하는 경우, PE1으로 입력되는 데이타로부터 VPN 레이블을 얻고, 이러한 레이블 값을 이용해서 시스템 내부 및 CE1까지의 경로를 결정하기 위한 정보를 가입자 인터페이스 설정 절차를 통해서 포워딩 엔진에 반영한다.

또한 QoS 파라미터를 이용해서 PE에서 CE로 전달되는 데이타에 대해서 QoS를 보장할 수 있다. 이때 입력되는 파라미터 값은 PCR(Peak Cell Rate), SCR(Sustained Cell Rate), MBS(Maximum Burst Size), CDVT(Cell Delay Variation Tolerance) 등이다.

3.3.2 VPN 사이트간 멤버쉽 정보 분배

MPLS 기반 VPN 기술은 라우팅 정보를 VPN 그룹별로 관리함으로써 사용자의 그룹을 형성하도록 한다. 라우팅 정보를 선별적으로 분배하기 위해서 RT를 사용하며, RT 및 VPN 관련 정보와 라우팅 정보를 전달하기 위해서 BGP4 라우팅 프로토콜을 확장한다. 구체적인 절차는 rfc 2547 및 BGP4 확장 프로토콜 표준안을 참조한다[3,4,6,7,8,9].

3.3.3 VPN용 LSP 설정

VPN용 LSP는 QoS를 지원하는 LSP와 QoS를 지원하지 않는 LSP 두 종류가 있다.

QoS를 지원하지 않는 LSP를 설정하는 방법은 다시 두 종류로 나눌 수 있다. 먼저, CR-LDP/RSVP-TE와 같은 시그널링 프로토콜을 이용해서 설정하는 경우로써, 이 경우에는 모든 QoS 파라미터를 디폴트로 설정한다. 다른 방법은 LDP를 이용해서 LSP를 설정하는 것이다.

QoS를 지원하는 LSP 설정은 TE 기능 블록의 운용자 명령어를 이용한다. 설정하고자 하는 LSP 정보, 제공하고자 하는 LSP의 QoS 정보, 가입자 정보, 그리고 필요하다면 경로보호를 위한 정보 등을 입력하고, 시그널링 프로토콜을 이용해서 해당하는 LSP를 설정한다. 구체적인 설정 방법은 4장에서 다룬다.

가입자 인터페이스 설정 절차(3.3.1절 참조)에서와 유사하게 LSP를 설정하면 시스템 내부 채널이 설정된다.

3.3.4 VPN용 패킷 포워딩

이 장에서는 VPN용 패킷을 포워딩하는 절차를 나타낸다[12].

(가) Ingress PE에서의 메시지 포워딩 절차

CE로부터 IP 패킷이 입력되면 포워딩 엔진에서는 패킷이 수신된 인터페이스를 가지고 VPN용 패킷인지 여부를 판별한다. 만약 VPN용 패킷이면 해당 인터페이스에 할당된 RD 값과 패킷에 포함된 목적지 주소를 이용해서 VPN용 포워딩 테이블을 룩업한다.

포워딩 테이블 룩업을 통해서 LSP에 대한 레이블과 도착지 PE에서 목적지 CE까지의 경로를 나타내는 VPN 레이블을 얻게 된다. 즉, 포워딩 테이블 룩업을 통해서 데이타 패킷이 이용할 LSP가 결정되며, 이 LSP가 어느 QoS를 지원하는지에 따라서 VPN 서비스에서 지원하는 QoS가 결정된다.

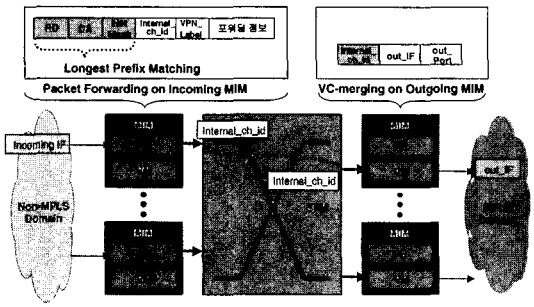

그림 4 Ingress PE에서의 패킷 포워딩 절차

(나) Egress PE에서의 메시지 포워딩 절차

MPLS 망 내부에서는 MPLS 레이블을 이용해서 Egress PE까지 패킷이 전달된다. 이때 이용하는 LSP의 QoS 특성에 따라서 VPN 서비스의 품질을 차별화하는 것이 가능하다.

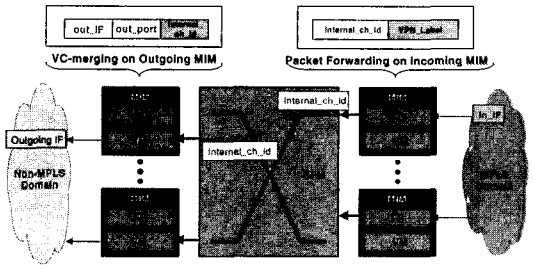

그림 5 Egress PE에서의 패킷 포워딩

Egress PE에서는 먼저 MPLS 레이블을 팝(pop)하고, VPN 레이블을 이용해서 CE까지의 경로를 찾는다[3,4, 13]. 이러한 경로는 3.3.1절에서 언급한 절차를 통해서 이미 설정되어 있으며, 이때 QoS 파라미터를 설정함으로써 가입자까지 QoS를 지원할 수 있다. 그림 5는 Egress PE에서의 패킷 포워딩 절차를 나타낸다.

3.4 EMS 기능

ACE2000 MPLS 시스템에서는 망 관리 기능을 제공하고 있으며, 이러한 기능에 VPN을 위한 기능도 포함되어있다. 각 노드에서 MAS를 통해서 입력하는 명령어를 EMS의 GUI 창을 이용해서 설정할 수 있다. 또한 설정된 결과 및 현재 제공중인 VPN 서비스에 대한 망 정보 및 노드 정보등을 GUI 창을 통해서 운용자가 쉽게 이해할 수 있도록 출력하고 있다.

SNMP를 위해서 사용한 MIB(Management Information Base)은 draft-ietf-ppvpn-mpls-vpn-mib-00이다. 하지만 이 MIB에서는 VPN의 기본적인 서비스 제공을 위한 MIB만을 정의하고 있다. 실제로 QoS를 지원하는 LSP를 이용하는 경우나 엑스트라넷 서비스를 지원하는 경우 등에 대한 정의는 미흡하다. 실제 구현에서는 [16]의 MIB을 바탕으로 사설 MIB을 설정해서 QoS 및 엑스트라넷 서비스를 지원하도록 구성하였다. 사설 MIB에는 QoS를 지원하는 LSP 정보 및 LSP를 이용하는 그룹 정보들, 그리고 하나의 그룹에 여러 RT를 입력할 수 있도록 구성되었다. 또한 가입자와 망 사업자간의 인터페이스에 대한 정보도 QoS 부분을 확장하였다.

4. 고신뢰도의 품질 차별화 서비스 지원을 위한 주요 메커니즘

ACE2000 MPLS VPN 서비스는 망 사업자가 다양하게 QoS 정책을 만들 수 있도록 설계되었으며, VPN 서비스를 위한 LSP의 개수를 줄이기 위해서 하나의 LSP를 여러 그룹들이 동시에 사용할 수 있도록 설계되었다. 또한 망 내에서 발생한 장애나 시스템 내에서 발생한 장애를 극복할 수 있도록 경로 보호 기능 및 각종 재시동 기능을 갖고 있다.

이 장에서는 QoS를 보장하는 VPN용 LSP를 설정하는 절차와 고신뢰도 서비스를 위한 경로 보호 기능 및 재시동 절차에 대해서 기술한다.

4.1 QoS를 지원하는 VPN용 LSP 설정

CR-LDP는 QoS 지원을 위해서 트래픽 파라미터(Traffic Parameters) TLV를 이용하며, 이때 사용되는 파라미터는 PDR(Peak Data Rate), PBS(Peak Burst Size), CDR(Committed Data Rate), CBS(Committed Burst Size), EBS(Excess Burst Size) 등이다. 이러한 파라미터들과 ATM에서 사용되는 파라미터들 사이의 관계는 LDP 표준에서 제안하고 있다. 즉, 서비스 유형

별로 ATM에서 사용되는 파라미터를 CR-LDP의 트래픽 파라미터 TLV에서 사용되는 파라미터로 변환하는 기준을 제시하고 있다[15].

ACE2000 MPLS 시스템에서는 TE 기능 블록의 운용자 명령어를 통해서 설정할 LSP의 QoS 특성, 경유할 홉, 그리고 FEC 등의 정보를 입력한다. 입력할 QoS 정보는 CBR(Constant Bit Rate), VBR(Variable Bit Rate), UBR(Unspecified Bit Rate) 등과 같은 서비스 유형과 각 유형별로 입력되는 PCR, SCR, MBS, CDVT와 같은 QoS 파라미터 값들이 있다. 또한 TE 기능 블록의 운용자 명령어를 통해서 CR-LDP에게 LSP 설정을 요구하고, CR-LDP는 자원 예약을 위해서 이러한 파라미터 값들을 각 노드로 전달한다. 노드로 전달된 값들은 ATM의 QoS 파라미터에 적합한 형태로 변경되고, 변환된 QoS 파라미터에 의해서 ATM에서 제공하는 대역폭, 지연, 전달 우선 순위(transmission priority) 등과 같은 ATM에서 지원할 수 있는 QoS 특성들을 제공한다.

CR-LDP를 통해서 LSP가 설정되면, 그 결과가 TE 블록으로 전달되며, TE 기능 블록에서는 해당 LSP의 QoS 파라미터 및 LSP ID 등의 정보를 VPN 기능 블록에 전달한다. VPN 기능 블록은 설정된 LSP를 위한 시스템 내부 연결 설정을 자원 관리 블록에 요청하며, 자원 관리 블록에서는 요청한 LSP에 대한 시스템 내부 연결 설정을 수행한다.

VPN용으로 설정된 LSP를 효율적으로 활용하기 위해서, 어느 그룹이 해당 LSP를 이용할 것인지 결정하는 과정을 수행한다. 즉, 하나의 LSP를 어느 그룹이 이용할 것인지, 또는 하나의 LSP를 어떤 여러 그룹이 공유할 것인지 여부를 결정한다. 이러한 절차는 VPN용 운용자 명령어를 통해서 수행된다.

QoS를 지원하는 LSP를 먼저 설정하고, 설정된 LSP를 이용할 그룹을 결정하는 방식은 다양한 QoS 정책을 수용하는 것을 가능하도록 하며, 가입자가 요구하는 QoS에 대한 다양한 요구사항을 탄력적으로 제공할 수 있다. 또한 망 내에서 하나의 LSP를 여러 VPN 그룹들이 공유할 수 있도록 설계함으로써, VPN 서비스를 위해서 요구되는 LSP의 개수를 크게 줄이는 것이 가능하다.

그림 6에서 보듯이, 그룹 A에서 사이트별로 대역폭이 'a'이면서 경로보호 기능을 지원하지 않는 LSP를 이용할 수도 있고, 대역폭이 "a"이면서 경로보호 기능을 지원하는 LSP를 이용할 수도 있으며, 대역폭이 'a'이면서 경로보호 기능을 지원하지 않는 LSP를 그룹 B와 공유해서 사용할 수도 있다. 즉, 망 사업자는 같은 그룹 내에서도 서로 다른 QoS 정책을 적용하는 것이 가능하다. 또한 가입자 입장에서도 각 사이트별로 다른 품질을 제공받음으로써, 사이트간 트래픽 특성 및 중요도에 따라서 차별화된 품질을 요구하는 것이 가능하다.

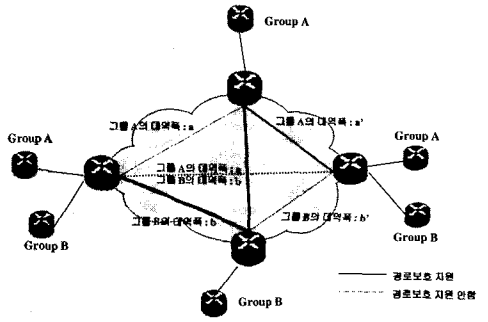

그림 6 VPN용 LSP 매핑 방법

매핑 정보에 대한 설정 절차를 마무리한 후에, 해당하는 VPN 그룹에 대해서 라우팅 테이블을 검색한다. 검색된 라우팅 정보와 해당 LSP 정보를 이용해서 포워딩 정보를 생성하고, 생성된 포워딩 정보는 자원 관리 블록에서 포워딩 엔트리를 생성하는데 이용된다. 포워딩 엔트리는 포워딩 엔진에 전달되서, 패킷을 포워딩 하는데 이용된다. 포워딩 엔진에 전달되는 포워딩 정보에는 VPN 레이블과 LSP에 대한 레이블 정보들이 포함되어 있다.

그림 7은 LSP 설정 및 포워딩 엔트리 생성 절차를 나타낸다.

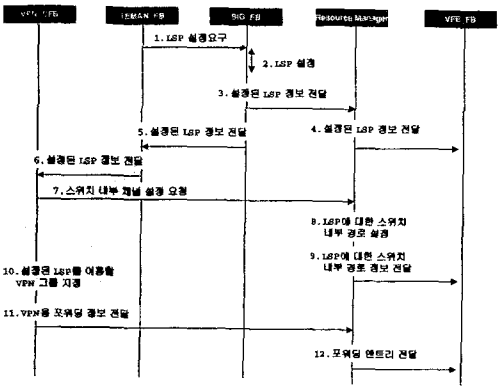

그림 7 포워딩 엔트리 생성 절차

4.2 망 장애시의 고신뢰도 서비스 제공 기능

ACE2000 MPLS 시스템에서 지원하는 경로 보호 기

능은 TE 기능 블록에서 제공하고 있다. TE 기능 블록에서는 CR-LDP나 RSVP-TE와 같은 시그널링 프로토콜을 이용해서 주 경로를 설정하며, 주 경로에 대한 대체 경로는 LSP 관련 정보를 입력만 하고 실제로 LSP 설정은 하지 않는 방법과 LSP를 실제로 설정하는 방법이 있다. 만약 주 경로에 장애가 발생하면, 시그널링 프로토콜을 통해서 장애 사실을 인지하고, 주 경로에 대한 포워딩 정보를 대체 경로에 대한 포워딩 정보로 수정해서 포워딩 엔진에 반영함으로써 대체 경로로 트래픽을 우회한다. ACE2000 MPLS 시스템의 TE 기능 블록에서는 하나의 주 경로에 대해서 네 개의 대체 경로를 설정하는 것이 가능하다.

VPN 서비스를 위한 경로 보호 기능은 위의 방식을 그대로 활용한다. 주 경로에 대한 장애 발생이 시그널링 프로토콜을 통해서 TE 기능 블록에 전달되면, TE 기능 블록은 장애가 발생한 주 경로가 VPN용 경로인지를 검사한다. 만약 VPN용 경로에 장애가 발생했다면 TE 기능 블록이 관리하고 있는 주 경로에 대한 대체 경로 정보를 VPN 기능 블록에게 전달한다. 물론 대체 경로가 미리 설정되어 있지 않다면 대체 경로를 실제로 설정한 후에 VPN 기능 블록에 대체 경로 정보를 전달한다. 주 경로에 대한 대체 경로 정보를 수신한 VPN 기능 블록은 그림 8과 같은 절차를 통해서 대체 경로에 대한 포워딩 정보를 포워딩 엔진에 반영함으로써 트래픽을 대체 경로로 우회시킨다.

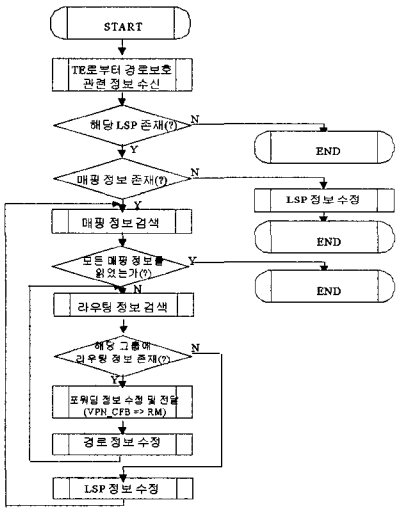

그림 8 경로 보호 기능 처리 절차

그림 8에서 보듯이 장애가 발생한 주 경로에 대한 라우팅 정보를 검색해서 기존의 주 경로에 대한 포워딩 정보를 대체 경로에 대한 포워딩 정보로 수정하고, 그 결과를 자원 관리 블록을 통해서 포워딩 엔진에 반영한다. 하나의 LSP를 여러 그룹이 이용하고 있는 경우에는 해당 LSP를 이용하는 모든 그룹의 라우팅 정보를 검색해서 포워딩 정보를 수정해야만 한다. 하나의 LSP를 여러 그룹이 공유하는 경우, 해당 LSP가 경로 보호 기능을 제공한다면 그 LSP를 이용하는 모든 그룹들도 경로 보호 서비스를 제공받는다.

4.3 시스템 장애시의 고신뢰도 서비스 제공 기능

ACE2000 시스템은 장애 극복을 위해서 스위치, IPC, 각종 메인 프로세서 및 장치 제어기(device controller)에 대한 이중화를 지원하고 있으며, MPLS 시스템에 대한 이중화도 지원하고 있다. 이 절에서는 ACE2000 MPLS 시스템에서 VPN 기능 블록이 지원하는 장애 극복을 위한 기능들을 기술한다.

4.3.1 MSC 재시동 절차

ACE2000 MPLS 시스템이 재시동 되었을 경우, 이전에 운영자에 의해서 입력된 정보는 모두 복구가 되어야만 하며, 프로토콜에 의한 정보도 프로토콜이 동작해서 모두 복구가 됨으로써 재시동 이전의 상태와 동일하게 VPN 서비스가 제공되어야만 한다. 이러한 요구사항을 만족하기 위해서 VPN 기능 블록은 운영자에 의해서 입력되는 모든 정보들을 데이타베이스에 관리하고 있다. 시스템이 재시동 되는 경우, 데이타베이스로부터 VPN 그룹 정보, 가입자 인터페이스 정보, LSP 및 매핑 정보, 그리고 정적 라우팅(static routing) 정보 등을 읽어서 처리한다. 또한 원격지 라우팅 정보는 BGP4+를 이용해서 재시동 이전 상태로 복구한다. 그림 9는 MSC가 재시동되는 경우 복구되는 정보 및 절차를 나타낸다.

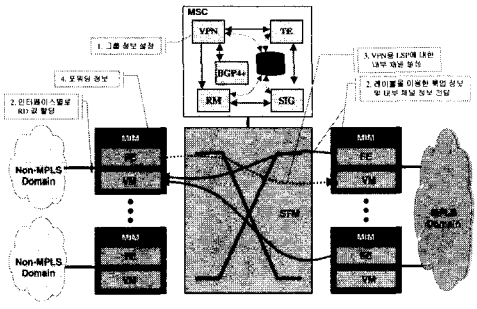

그림 9 MSC 재시동 절차

그림 9의 1번 절차는 데이타베이스로부터 VPN 그룹 정보를 읽어서 해당 테이블에 반영한다. 2번 절차는 가

입자 인터페이스를 설정하는 절차로서, 운용자에 의해서 명령어를 입력하는 경우의 처리 절차와 유사하다. 단지, 룩업 정보 및 내부 채널 정보를 포워딩 엔진에 전달할 때, 포워딩 엔진이 아직 정상적인 동작을 하지 않는 경우에는 데이타베이스로부터 읽은 정보들을 테이블에 반영하고 상태를 비정상 상태로 표시한다. 비정상 상태는 해당 인터페이스를 사용할 수 없으며, 관련 정보가 포워딩 엔진에 반영되지 않은 것을 의미한다. 추후에 포워딩 엔진이 정상적인 상태로 동작하면 GSMP가 VPN 블록에게 포워딩 엔진이 정상 상태임을 알려준다. VPN 기능 블록이 이러한 정보를 수신하면, 해당 포워딩 엔진에 관련된 가입자 인터페이스 설정 절차를 수행한다. 성공적으로 수행되면 상태는 다시 정상 상태로 수정되고, 이후에는 해당 정보를 정상적으로 활용할 수 있게 된다.

그림 9의 3번 절차는 기존에 사용되던 LSP를 복구하는 절차를 나타낸다. VPN 기능 블록은 데이타베이스로부터 LSP 정보 및 매핑 정보를 읽고, 해당 정보를 테이블에 반영하며 상태를 비정상 상태로 표시한다. 또한 TE 기능 블록은 데이타베이스로부터 LSP 관련 정보를 얻은 후, 시그널링 프로토콜에게 LSP 설정을 요청하고, 시그널링 프로토콜은 이전에 설정되었던 LSP를 다시 설정한다. 설정된 LSP 정보는 TE 기능 블록을 통해서 VPN 기능 블록으로 전달되고, VPN 기능 블록은 새롭게 설정된 LSP와 기존에 운영자에 의해서 정의된 매핑 정보의 상태를 비정상 상태에서 정상 상태로 수정한다. 이전에 사용되고 있던 LSP 중에서 일부가 다시 설정되지 않는 경우에는 VPN 블록에서는 해당 LSP를 계속 비정상 상태로 관리한다. 비정상 상태는 VPN용 LSP 정보를 관리하는 테이블에는 존재하지만 실제로 VPN 서비스를 위해서는 사용되지 않는다. 만약 추후에 TE 기능 블록과 시그널링 기능 블록에서 LSP를 성공적으로 설정하면, 해당 LSP의 상태는 정상 상태가 되고 유효한 정보로서 사용된다.

그림 9의 4번 절차는 운용자에 의해서 입력된 정적 라우팅 정보를 처리하는 절차를 나타낸다. 운영자에 의해서 입력된 정적 라우팅 정보와 새롭게 설정된 LSP 정보를 이용해서 포워딩 엔트리를 생성하는 것이 가능하다. 또한 BGP4 확장 프로토콜을 이용해서 수신되는 원격지 라우팅 정보도 같은 절차를 통해서 포워딩 엔진에 반영된다. 만약 라우팅 정보가 생성된 후에 LSP가 설정되는 경우에도 해당 포워딩 정보들은 포워딩 엔진에 반영된다.

만약 VPN 기능 블록만 재시동되는 경우에는 시스템 재시동 절차와 약간의 차이가 있다. VPN 기능 블록에서 관리하는 VPN 관련 정보들은 모두 데이타베이스에서 받아오고, VPN 기능 블록 및 타 블록들은 재시동 이전에 사용하던 정보들을 그대로 활용한다. 만약, LSP 설정 정보 및 가입자 인터페이스 설정 정보 등과 같이 타 블록과 연관성이 많은 정보들은 VPN 기능 블록이 다운된 상태에서 변경되는 경우에도 별도의 라이브러리를 통해서 데이타베이스 및 각 블록에서 관리하는 테이블에 정상적으로 반영된다.

4.3.2 포워딩 엔진 재시동 절차

하나나 그 이상의 포워딩 엔진이 재시동 되는 경우에는 해당되는 포워딩 엔진에만 정보들을 전달한다. 즉, 각종 시스템 내부 채널 연결 정보 및 포워딩 엔트리 정보 등을 포워딩 엔진에 전달하며, 이러한 기능은 자원 관리 블록이나 각 응용 블록에서 처리할 수 있다.

ACE2000 MPLS VPN에서는 각종 시스템 내부 연결 정보는 자원 관리 블록에서 복구하며 포워딩 정보는 VPN 기능 블록에서 포워딩 엔진별로 복구한다.

예를 들어서, LSP와 연관된 포워딩 엔진이 다운되면 해당 LSP들에 대해서 장애 발생을 위한 삭제 절차를 수행하며, VPN 기능 블록에서도 해당 LSP 정보 및 LSP와 연관된 포워딩 정보들을 삭제한다. 추후에 포워딩 엔진이 정상 상태가 되면 삭제된 LSP를 다시 설정하고, VPN 기능 블록에서는 다시 설정된 LSP 정보를 기반으로 새로운 포워딩 정보를 전달한다. 가입자측 인터페이스가 설정된 포워딩 엔진이 재시동되는 경우에는 가입자측 인터페이스 설정 절차와 동일한 과정을 통해서 해당 정보를 복구한다.

5. 결 론

본 논문에서는 ACE2000 MPLS VPN 서비스를 위한 설계 및 구현에 대해서 기술하였다. 본 논문에서 언급한 MPLS 기반 VPN 기술은 VPN 그룹별로 차별화된 서비스, 즉, QoS 및 경로 보호 기능을 제공할 수 있으며, 하나의 LSP를 여러 VPN 그룹이 이용할 수 있도록 설계함으로써 확장성이 뛰어나도록 하였다. 또한 망 내의 장애 및 시스템 내의 장애를 극복할 수 있도록 설계되었다.

추후에는 응용이나 가입자 특성에 따라 VPN 패킷의 CoS 등급을 구분하는 패킷 룩업 기술, MPLS 망에서의 모니터링 및 망 관리 기술, 그리고 VPN 서비스에서 제공할 수 있는 멀티캐스팅과 같은 각종 응용 기술들에 관련된 연구가 지속될 것이다.

참 고 문 헌

[1] De Clercq et. al, "BGP/IPSEC VPN," draft-declercq-bgp-ipsec-vpn-01, Feb. 2000.

[2] E.Rosen et. al, "Use of PE-PE IPsec in RFC2547 VPNs," draft-rosen-ppvpn-ipsec-2547-00, Jun. 2001.

[3] E.Rosen, Y.Rekhter, "BGP/MPLS VPNs," RFC 2547, Mar. 1999.

[4] E.Rosen, et al, "BGP/MPLS VPNs," draft-rosen-rfc2547bis-01, May. 2000.

[5] Y. Rekhter, et al, "Address Allocation for Private Internets," RFC1918, Feb. 1996.

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

[7] T.Bates, R.Chandra, D.Katz, Y.Rekhter, "Multiprotocol Extensions for BGP-4," RFC 2283, Feb. 1998.

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

[9] Y.Rekhter, E.Rosen, "Carrying Label Information in BGP-4," draft-ietf-mpls-bgp4-mpls-04, Jul. 2000.

[10] 양선희, 윤호선, 이유경, "품질보장이 가능한 MPLS 기반의 IP-VPN 기술", 한국통신학회 학회지, 제 18권 9호, 2001년 9월.

[11] 윤호선, 윤현식, 양선희, 강민수, "ACE2000 BGP/MPLS VPN 서비스 개발", Proc. of 한국정보처리학회 추계학술대회논문집, 제8권 2호, 2001년 10월.

[12] 윤호선, 정민영, 최병철, 양선희, "MPLS-VPN을 위한 Forwarding Engine의 설계", Proc. of 한국통신학회 추계학술대회논문집, 제22권 2호, 2000년 11월.

[13] E.Rosen, Y.Rekhter, D.Tappan, D.Farinacci, G.Fedorkow, T.Li, A.Conta, "MPLS Label Stack Encoding," draft-ietf-mpls-label-encaps-07, Sep. 1999.

[14] Thomas D. Nadeau et. al, "MPLS/BGP Virtual Private Network Management Information Base Using SMIv2," draft-ietf-ppvpn-mpls-vpn-mib-00, Jul. 2001.

[15] B. Jamoussi et. al, "Constraint-Based LSP Setup using LDP," RFC3212, Jan. 2002.

윤 호 선

1997년 순천향대학교 전자공학과(학사) 1999년 순천향대학교 전자공학과(석사) 2000년 3월 ~ 현재 한국전자통신연구원 네트워크연구소 연구원. 관심분야는 MPLS 기술, 통신보안, VPN 기술

양 선 희

1984년 경북대학교 전자공학과(학사) 1986년 한국과학기술원 전기및전자공학과(석사). 1986 2월 ~ 1988년 7월 한국과학기술원 통신공학연구실 연구원. 1988년 8월 ~ 현재 한국전자통신연구원 네트워크연구소 책임연구원, 현 차세대프로토콜팀 팀장. 관심분야는 인터넷 QoS 기술, MPLS 기술, 고속통신망구조, 고속통신프로토콜, 라우팅프로토콜

이 유 경

1978년 한국항공대학 전자공학과(학사) 1980년 2월 연세대 대학원 전자공학과(석사). 1980년 8월 ~ 1984년 3월 공군 제2사관학교 교관. 1984년 4월 ~ 현재 한국전자통신연구원 네트워크연구소 책임연구원. 1990년 12월 전기통신기술사 관심분야는 고속통신 시스템, 네트워크 구조, MPLS 기술