2001 년 한국정보처리학회 추계 학술발표논문집 제 8 권 제 2 호

ACE2000 BGP/MPLS VPN 서비스 개발

윤호선*, 윤현식*, 양선희*, 강민수**
*한국전자통신연구원
**LG 전자
e-mail : yhs@etri.re.kr

Development of ACE2000 MPLS based IP-VPN

Ho-Sun Yoon*, Hyun-Sik Yoon*, Sunhee Yang*, Min-Soo Kang**
*Electronics and Telecommunications Research Institute
** LG Electronics

요 약

본 논문에서는 ACE2000 MPLS 시스템의 핵심 응용 기능으로 개발된 BGP/MPLS VPN 의 기능블럭 구성과 주요 특성을 기술하였다. BGP/MPLS VPN 은 VPN 사이트들간을 MPLS LSP 를 이용하여 터널링 시키는 서비스로서 VPN 사이트들에 대한 라우팅 정보가 BGP4 확장 프로토콜을 이용해서 전달되고, VPN 사이트간의 트래픽은 MPLS LSP 를 통해서 전달된다. ACE2000 BGP/MPLS VPN 은 품질의 차별적 지원이 가능하고 확장성이 뛰어난 구조로 개발되었다.

1. 서론

VPN 기술은 전달망 기술에 따라 Leased Line, ISDN, FR, ATM, IP 터널링 VPN 등의 다양한 기술이 사용되고 있다. 근래들어 인터넷이 기업활동의 기반 인프라로 빠르게 확산됨에 따라 IP 터널링 VPN 기술이 각광을 받고 있는 추세이다. 그러나 IP 터널링 VPN 은 품질보장이 제한적이며, 가입자 사이트간 풀메쉬 IP 터널을 구성해 주어야 하는 구조적 단점을 갖는다.

이러한 문제를 개선한 구조로서 최근 관심을 끌고 있는 기술이 MPLS 기반 IP-VPN 기술이다. MPLS 기반 IP-VPN 은 MPLS LSP(Label Switched Path)를 이용하여 VPN 사이트들간을 연결함으로써 가상의 사설망 서비스를 제공하는 서비스이다. MPLS-VPN 은 가입자 관점에서는 IP 프로토콜로 접속되고, MPLS 트래픽 엔지니어링 기능을 이용하여 서비스 품질의 차별적 지원이 가능하며, LSP 공유에 의해 확장성이 뛰어 나다는 장점을 갖고 있다.

MPLS 기반 IP-VPN 에 대한 표준화는 IETF 에서 완료되어 RFC 로 승인되었으며, 올해들어 AT&T, GlobalOne 등 대규모 ISP 들이 서비스 도입을 서두르고 있다. 우리나라에서도 MPLS 기반으로의 인터넷 백본망 업그레이드가 긍정적으로 검토되고 있으며, 이에 따라 ACE2000 시스템 기반 MPLS 기술 개발이 ETRI 를 중심으로 추진되고 있다.

본 논문에서는 ACE2000 MPLS 시스템에 탑재하기 위해 설계 개발된 MPLS 기반 IP-VPN 서비스 모듈의 구현 내용에 대해 기술한다. ACE2000 MPLS 시스템 기반 IP-VPN 서비스 모듈은 RFC 2547 규격에 준하여 설계 개발되었다. 2 장에서는 BGP/MPLS VPN 의 기술 개요를 간단히 정리하였다. 3 장에서는 서비스 모듈의 기능블럭 구성과 특성을 소개하고, 4 장에서 결론을 맺는다.

2. BGP/MPLS VPN 기술

MPLS 기반 IP-VPN 은 VPN 사이트들간을 MPLS LSP 를 이용하여 터널링시키는 서비스로서, 가입자 사이트들간의 라우팅 정보는 기존의 라우팅 혹은 시그널링 프로토콜을 이용하여 Piggy-backing 되고, VPN 트래픽은 MPLS LSP 를 통해서 전달된다.

MPLS-VPN 은 VPN 사이트간의 라우팅 정보의 분배 및 관리 방법에 따라 BGP/MPLS VPN 구조와 Virtual Router 의 두가지 구조가 있다.

Virtual Router 방식은 각 VPN 그룹마다 라우팅 프로토콜 인스턴스와 라우팅 테이블이 다 따로 동작하

는 구조로서 하나의 물리적 라우터 안에 논리적으로 구분되는 VPN 그룹별 전용 라우터가 여러 개 있는 것 처럼 동작한다.

BGP/MPLS VPN 구조는 망측 에지 장비들간에 iBGP 피어링을 맺고, 확장된 BGP4 어트리뷰트들을 이용해서 VPN 루트 정보를 전달한다. 망측 에지 장비들은 각 VPN 그룹별로 VPN 용 라우팅 테이블(VPN Routing & Forwarding Table)을 따로 유지한다. 따라서 BGP4/MPLS VPN 구조는 라우팅 인스턴스가 하나만 동작하므로 성능면에서 Virtual Router 구조에 비해 유리한 대신에 BGP4 프로토콜의 확장이 필요하다. 현재 MPLS 기반 VPN 은 주로 BGP/MPLS VPN 구조가 주도하고 있다.

BGP4/MPLS VPN 서비스는 VPN 사이트 접속이 이루어지는 PE 시스템 내에만 VPN 서비스 모듈을 탑재하게 된다. PE 는 VPN 사이트가 연결되어 있는 LER 시스템으로서 VPN 사이트에 대한 라우팅 정보의 제한적 분배 및 관리 기능과 VPN 패킷의 인식 및 포워딩 기능, VPN 을 위한 LSP 설정 기능 등을 처리한다. 아울러 PE 는 각 VPN 사이트별로 폐쇄사용자그룹에 대한 라우팅 및 포워딩 정보 테이블(VPN Routing & Forwarding Table, VRF)을 유지하며, PE 간의 VPN 루트 정보 교환은 BGP4 확장 프로토콜을 통해 전달된다. 망내 코어 시스템이나 가입자 장비는 VPN 기능과 무관하다

PE 에 의해서 이루어지는 VPN 서비스 동작은 크게 VPN 사이트간 라우팅 정보의 분배, VPN 사이트간 LSP 의 설정, VPN 패킷의 포워딩 절차로 구성된다.

○ VPN 사이트간 라우팅 정보의 분배 기능

PE 는 각 폐쇄사용자그룹에 대해 따로 분리된 VRF 테이블을 유지하며, 각 VRF 테이블에는 로컬 및 원격의 VPN 사이트들에 대한 경로정보(VPN 주소 정보, 원격의 PE 주소, VPN Label) 가 저장 관리된다.

VPN 사이트의 로컬 루트 정보가 갱신되면 이 정보가 RIP/OSPF/EBGP 프로토콜이나 혹은 매뉴얼 셋팅에 의해 로컬 PE 측으로 전달 된다. 로컬 PE 에서는 로컬 루트 정보를 해당되는 VRF 테이블에 저장하고, BGP4 확장 프로토콜을 이용해서 원격의 PE 측으로 전달한다. 이때 PE 간에는 iBGP 피어링이 맺어진 상태이며, VPN 루트 정보는 iBGP 에 의해 piggy-backing 된다.

BGP 가 실어 나르는 VPN 루트 정보에는 VPN-Ipv4 주소, VPN Label 및 Export Route Target 등이 포함된다. VPN-Ipv4 는 사설망 주소를 지원할 수 있도록 확장된 VPN 주소 체계로서 4 바이트의 Ipv4 주소 앞에 8 바이트의 Route Distinguisher 를 부착하여 12 바이트의 유일한 주소 체계로 확장한 것이다. VPN Label 은 각 인터페이스에 할당된 레이블로서 Egress PE 에서 출력 인터페이스를 결정하기 위한 레이블이다. VPN label 은 새로운 VPN 사이트 인터페이스가 추가될 때 각 인터페이스에 대해 할당되게 되며, 이 값은 VPN 루트 정보 분배시에 BGP4 확장 프로토콜에 의해 원격의 PE 로 전달되어 VRF 테이블에 기록된다. Export RT 값은 분배되고 있는 루트 정보가 원격 PE 의 어느 VRF 에 반영되어야 하는 지를 나타내는 일종의 루트 필터이다.

원격 PE 에서는 BGP4 를 통해 VPN 루트 정보를 접수하게 되면 Export 및 Import RT 값을 비교하여 해당되는 VRF 테이블에만 반영시킴으로서 폐쇄사용자그룹별로 논리적으로 분리된 VRF 테이블이 만들어진다.

○ VPN 용 LSP 의 설정 기능

VPN 을 위한 LSP 는 Ingress PE 에서 Egress PE 까지 설정되며, 가입자의 요구 서비스 품질에 따라 LDP 를 이용해서 설정한 백본 LSP 를 공유하거나 혹은 CR-LDP 나 RSVP-TE 를 이용해서 특정 VPN 가입자 전용의 CR-LSP 를 설정할 수 있다.

○ VPN 패킷의 포워딩 기능

VPN 을 위한 데이터 경로는 Ingress PE 에서 Egress PE 까지의 LSP 와 Egress PE 에서 데스티네이션 VPN 사이트까지의 출력 경로로 구성되며, 이를 위해서 VPN 패킷 전달에는 2-레벨 스태킹이 사용된다.

CE 측으로부터 PE 측으로 패킷이 입력되면 PE 는 인터페이스 정보를 이용하여 VPN 패킷임을 인식한다. 그리고 해당 인터페이스에 설정한 RD 값을 참조하여 해당 VRF 테이블을 결정하고, 목적지 주소를 룩업하여 원격의 PE 측까지의 백본 LSP 를 구분하는 top label 과 Egress 측에 서의 출력 인터페이스를 구분하기 위한 VPN label 을 찾아낸다. 그 다음 찾아낸 레이블을 2 레벨 스택킹으로 부착하여 포워딩한다. VPN 패킷이 Egress PE 측에 도착하면 두번째 레이블이 부착되어 있는 점으로부터 VPN 패킷임을 인식하고 VPN 레이블로부터 출력 인터페이스를 룩업하여 최종 CE 사이트로 포워딩된다.

3. ACE2000 BGP/MPLS VPN 서비스 모듈 구조

3.1 시스템 개요

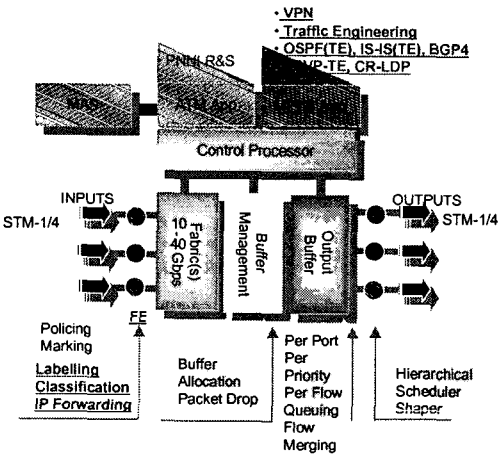
ACE2000 MPLS 시스템은 ACE2000 스위치 시스템에 MPLS 모듈을 탑재한 ATM 기반 MPLS LER 시스템이다. (그림 1)의 기능구조에서 보듯이 시스템은 크게 ATM 스위치모듈, 가입자 정합 모듈, 제어모듈 및 운용관리를 위한 MAS 모듈로 구성된다. 스위치 모듈과 가입자 정합 모듈은 기본적인 ATM 기능을 처리한다. ATM 서비스 가입자의 경우 ATM 제어모듈에 탑재된 PNNI 라우팅 및 시그널링 프로토콜에 의해 가입자 정합 모듈의 연결 정보가 제어된다.

MPLS 서비스 모듈은 제어기능을 담당하는 MPLS Service Control 기능(MSC)과 사용자평면의 IP 패킷 처

리를 담당하는 포워딩 엔진 기능(FE), 그리고 운용관리 기능(M-MAS)으로 구성된다. FE 은 가입자 정합 모듈 내에 탑재되며, MSC 블록은 제어모듈에 탑재되어 FE 을 GSMP 를 통해 제어한다.

MSC 기능블럭에는 TCP/IP 프로토콜 Suit 와 RIP/OSPF/BGP4 라우팅 프로토콜 그리고 LDP/CR-LDP/RSVP-TE 시그널링 프로토콜, 트래픽 엔지니어링 및 VPN 블록 등의 응용 소프트웨어가 포함된다. 아울러 LSP 설정을 위한 자원관리와 포워딩 엔진내의 포워딩 엔트리 제어 기능을 담당한다. MSC 의 라우팅 및 시그널링 프로토콜이 동작하여 만들어진 라우팅 및 포워딩 정보는 내부 IPC 채널을 통해 각 FE 으로 다운로드된다. FE 기능은 가입자 채널을 통해 유입되는 IP 패킷을 MSC 블록에서 내려준 포워딩 정보를 이용하여 룩업하여 FEC 로 분류하여 적절한 LSP 로 맵핑해주는 기능을 하며, 가입자정합단에 위치한다. M-MAS 기능은 MPLS 모듈을 구성하고, 운용하기 위한 제반 운용기능을 처리한다.

VPN 서비스 모듈는 MSC 기능블럭의 최상위에 위치하는 응용 소프트웨어로서 크게 VPN 서비스 구성관리, VRF 제어 기능, VPN-LSP 구성관리, VPN-FE 기능, BGP4+ 기능 등으로 구성된다. VPN 서비스 모듈은 TE 기능과 시그널링 블록의 도움을 받아 VPN 사이트에 대한 LSP 를 설정한다. 그리고 BGP4+ 기능을 통해 분배받은 VPN 루트 정보와 LSP 정보 및 VPN 패킷에 대한 FEC 분류 정책 정보를 종합하여 각 폐쇄사용자 그룹별 VRF 테이블을 구성하여 이를 VPN 사이트가 접속되는 FE 으로 내려준다.



(그림 1) ACE2000 MPLS 시스템의 기능구조

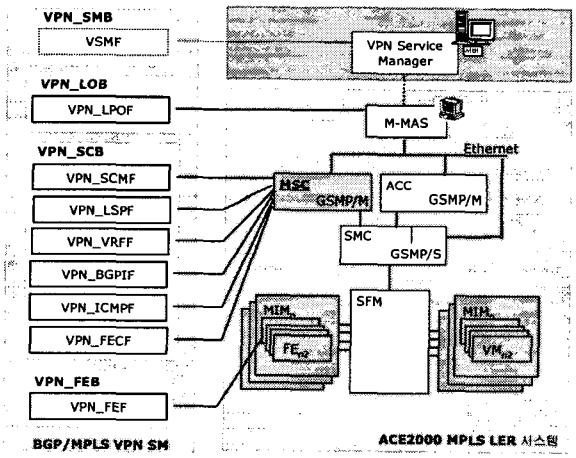
3.2 서비스 요구사항 및 설계 고려사항

ACE2000 BGP/MPLS VPN 서비스 모듈 설계를 위한 서비스 요구사항은 다음과 같다.

- 목표서비스는 인터라넷 및 엑스터라넷 서비스 (비즈니스-to-비즈니스)를 지원한다.
- 주소체계는 Public 및 Private IPv4 주소를 제한없이 사용할 수 있어야 한다.
- QoS 지원은 VPN 사이트간 대역보장형 고품질 VPN 과 최선형의 저가 VPN 서비스를 지원한다.
- VPN 라우팅 제어는 매뉴얼 셋팅 및 BGP4 확장 프로토콜을 이용한 자동구성을 지원한다.
- 서비스 Provisioning 은 각 LER 시스템의 운용관리 시스템(M-MAS)을 통해 구성한다.

3.3 기능블럭 구성

ACE2000 BGP/MPLS VPN 서비스 모듈은 (그림 2)와 같이 크게 VPN_SMB, VPN_LOB, VPN_SCB, VPN_FEB 의 네 블록으로 구성되며, 이들은 각기(그림 2)의 물리 시스템 컴포넌트에 탑재된다.



(그림 2) ACE2000 BGP/MPLS VPN 기능블럭 구성

○ VPN_SMB(VPN Service Manager Block)

VPN_SMB 은 VPN 서비스에 대한 SLA, Provisioning & Operation, VPN 서비스에 대한 품질 모니터링 및 과금 기능과 같은 서비스 운용관리 기능을 네트워크 차원에서 처리한다. 이 블록은 서비스 관리 서버에 위치하며, VPN_LOB 및 VPN_SCB 과는 SNMP 나 COPS 프로토콜을 이용하여 접속된다.

○ VPN_LOB(VPN Local Operation Block)

VPN_LOB 는 ACE2000 MPLS 시스템의 운용관리 시스템(M-MAS)에 위치하며, VPN 서비스의 Provisioning(구성관리) & Operation 을 위한 운용자 명령어의 처리 및 모니터링, 가입자 정보의 관리를 담당한다. VPN_LOB 는 VPN 서비스를 위해 요구되는 주요 구성 데이터(VPN 그룹 구성, 사이트 정보구성, 가입자 인터페이스 정보 구성, VRF 구성 데이터)의 할당 및 관리를 총괄한다.

○ VPN_SCB(VPN Service Control Block)

VPN_SCB 는 LER 의 MSC 에 위치하며, VPN 가입자 및 그룹, 사이트, 인터페이스에 대한 구성관리(VPN_SCMF), VPN 을 위한 품질보장형 LSP 의 설정관리(VPN_LSPF), VRF 테이블 구성 및 관리(VPN_VRFF), BGP4 확장 프로토콜과의 인터페이스(VPN_BGPIF) 및 VPN 을 위한 ICMP 프로토콜의 처리(VPN_ICMPF) 등을 수행한다. 아울러 VPN 라우팅 정보와 VPN LSP 정보 그리고 VRF 에 셋팅된 가입자 플로우 구분 정책 정보를 종합하여 VPN FE 모듈로 VPN 포워딩 엔트리 정보를 내려주는 포워딩 엔진 제어 기능(VPN_FECF)을 수행한다.

○ VPN_FEB(VPN Forwarding Engine Block)

VPN_FEB 은 가입자 정합 모듈(MIM)에 위치하며, VPN_SCB 의 제어를 받아 VPN 을 위한 포워딩 테이블의 엔트리들을 구성 관리한다. 입력되는 패킷에 대해 인터페이스 정보를 이용하여 VPN 패킷임을 인식하고 VRF 테이블을 참조하여 LSP 를 룩업하고 레이블을 스태킹하여 LSP 로 맵핑하는 사용자 평면 기능을 수행한다. Egress 의 경우에도 VPN 레이블의 스태킹 여부를 판단하여 VPN 패킷을 VPN 사이트측으로 포워딩시키는 기능을 수행하게 된다.

3.4 ACE2000 BGP/MPLS VPN 의 주요 특성

ACE2000 BGP/MPLS VPN 은 품질의 차별적 지원이 가능하고 확장성이 뛰어나다.

품질 차별화 측면에서는 1 차 모델에서는 VPN 그룹별로 품질 보장형 혹은 최선형 품질을 지원할 수 있도록 차별화하였다. 그러나 추후 FE 블록의 패킷 분류 기능이 업그레이드되는 경우에는 단일 VPN 그룹 내에서도 응용의 특성에 따라 품질의 차별화가 가능하도록 하고, 각 VPN 사이트별 QoS 계약에 대한 SLA 에 따라 패킷을 분류하고 계약 내용의 준수 여부를 검사하는 SLA 기능을 연구 중이다.

또한 확장성 측면에서는 VPN 그룹간에 LSP 를 공유할 수 있도록 하되, 품질 요구 기준에 따라 QoS 특성을 달리하는 ER-LSP 를 지원함으로써 품질 차별화와 확장성을 동시에 지원할 수 있도록 개발하였다.

4. 결론

본 논문에서는 ACE2000 MPLS 시스템의 핵심 응용 기능으로 개발되고 있는 BGP/MPLS VPN 의 기능블럭 구성과 주요 특성을 기술하였다.

BGP/MPLS VPN 은 VPN 사이트들간을 MPLS LSP 를 이용하여 터널링시키는 서비스로서 VPN 사이트들에 대한 라우팅 정보가 BGP4 확장 프로토콜을 이용해서 전달되고, VPN 사이트간의 트래픽은 MPLS LSP 를 통해서 전달된다.

ACE2000 BGP/MPLS VPN 은 품질의 차별적 지원이 가능하고 확장성이 뛰어나도록 설계하였다. LSP 공유 메커니즘과 품질보장형 CR-LSP 및 최선형 LSP 를 제한없이 사용하도록 하여 품질의 차별화와 확장성 사이에 트레이드업이 가능하다.

현재 기본 기능에 대한 개발이 마무리되어 시험 중이다. 이를 바탕으로 앞으로 품질보장이 가능한 CR-LSP 를 찾기 위한 QoS 라우팅 및 알고리즘, 응용이나 가입자 특성에 따라 VPN 패킷의 CoS 등급을 구분하는 패킷 룩업 기술 및 MPLS 망에 대한 모니터링과 최적화 기술, SLA 기술에 대한 연구를 계속할 것이다.

참고문헌

[1] IETF Draft, "draft-rosen-rfc2547bis-02.txt:BGP/MPLS VPNs," July.2000.

[2] Chuck Semeria, "RFC 2547bis:BGP/MPLS VPNs VPN Fundmentals," White Paper, Juniper Networks, 2001.

[3] "Implementing Carrier-Grade IP-VPN Solutions," White Paper, Ericsson, 2001.

[4] "Service Management of MPLS VPNs," White Paper, digiquant, 2001.

[5] "MPLS-Based Traffic Engineering and VPNs," White Paper, Unisphere Networks, 2001.

[6] IETF Draft, "draft-ietf-mpls-framework-05.txt: A Framework for Multiprotocol Label Switching," Sep. 1999.

[7] IETF Draft, " draft-ietf-mpls-arch-06.txt: Multiprotocol Label Switching Architecture," Aug. 1999.

[8] Anoop Ghawani 외, "Traffic Engineering Standards in IP Metwork Using MPLS," IEEE Communications Magazine, Dec. 1999.

[9] Daniel O. Awduche, "MPLS and Traffic Engineering in IP Networks," IEEE Communications Magazine, Dec. 1999.

[10] Nancy Feldman, "Traffic Engineering Standards in IP Networks Using," IEEE Communications Magazine, Dec. 1999.

[11] 윤호선, 김숙연, 양선희, "MPLS 를 이용한 VPN 기능모덜 설계," Proc. of 한국정보처리학회, 제 7 권 2 호, 2000.