

# 이동서비스를 지원하는 BGP-E 방식 MPLS VPN의 설계 및 구현

정회원 이영석\*, 임형택\*\*, 최훈\*\*

## Network based MPLS VPN using BGP-E for Mobility Support

Young-Seok Lee\*, Hyoung-Taek Lim\*\*, Hoon Choi\*\*

### 요 약

MPLS(Multiprotocol Label Switching)를 이용한 네트워크 기반 VPN(Virtual Private Network)은 고수익을 원하는 사업자와 저비용을 요구하는 고객 모두에게 인트라넷(Intranet)과 엑스트라넷(Extranet)을 위한 해결 방안으로서 도입되고 있다. 네트워크 기반 MPLS VPN은 BGP-E(BGP multiprotocol Extension) 프로토콜을 이용하는 구조와 VR(Virtual Router) 개념을 이용하는 구조로 구분된다. 본 연구에서는 BGP-E를 이용한 네트워크 기반 MPLS VPN을 대상으로, VPN 사이트 내에 속한 단말이 다른 사이트로 이동하더라도 계속 VPN서비스를 받을 수 있게 하는 MPLS 라우터 구현 방안을 제안한다. MPLS VPN 서비스와 Mobile IP에 의한 이동서비스를 지원하기 위한 메커니즘을 백본 네트워크 내의 PE(Provider Edge) 라우터 상에 설계하고 구현한다. VPN 사이트 내에 속하는 어떤 노드가 기존의 통신을 유지한 상태로 다른 사이트로 이동할 때, 이동 노드와 통신하고자 하는 대응 노드가 속한 VPN 사이트와 연결된 PE 라우터는 이동을 통보 받고 단말이 이동한 곳으로 새로운 MPLS 경로를 설정한다. 단말의 이동 서비스 지원을 위해 PE 라우터에 Mobile IP 프로토콜과 연동하는 VPN 관리 방식 및 라우터 제어 기능을 구현하고 시범 환경에서 시험하였다.

Key Words : VPN, MPLS, Mobile IP, BGP-E

### ABSTRACT

Network based VPN(Virtual Private Network) using MPLS(Multiprotocol Label Switching) technology is regarded as a good solution for intranets or extranets because of the low cost and the flexibility of the service provision. In this paper, we describe a mechanism that allows the VPN users to move from one site to another site of the VPN network based on the BGP-E MPLS technology. This mechanism is designed for and implemented on PE(Provider Edge) routers of the backbone network. PE routers connected to the VPN sites establish a new MPLS path to the mobile node after they detect movement of the mobile VPN node. The new location may belong to the same VPN or to different VPN. We designed VPN management and control functions of the PE routers in order to interface with the Mobile IP protocol. The pilot implementation and performance measurement were carried out on a testbed.

\* 한국전자통신연구원(yslee@etri.re.kr), \*\* 충남대학교 컴퓨터공학과(hilim@ce.cnu.ac.kr; hchoi@ce.cnu.ac.kr)

논문번호 : 030184-0602

※ 본 연구는 산업자원부의 지역전력산업 석·박사 연구인력 양성사업의 지원으로 수행된 것임.

## I. 서론

VPN(Virtual Private Network)은 공중망의 물리적인 구성과 별도로 논리적으로 한정된 가상의 그룹을 설정하여 다양한 통신 서비스를 제공하는 기술이다. VPN 데이터가 IP 패킷 형태로 전달되는 것을 IP VPN이라고 하며, IP VPN은 인터넷과 같은 광범위한 지역에 구축이 가능하고, 접속 비용이 저렴하며 IP 기반 응용이 풍부한 장점을 갖고 있다. IP VPN은 크게 CPE(Customer Premise Equipment) 기반 VPN과 네트워크 기반 VPN으로 나뉜다<sup>[1]</sup>. CPE 기반 VPN에서는 VPN을 위한 동작 메커니즘이 가입자 네트워크 내의 각 CPE에 구현되기 때문에 가입자의 부담이 큰 반면에, 네트워크 기반 VPN에서는 VPN 서비스 기능이 백본 네트워크 경계(edge) 라우터에 구현되므로 고수익을 원하는 네트워크 사업자와 저비용을 원하는 가입자들 모두에게 해결책이 되고 있다.

이러한 네트워크 기반 VPN은 같은 VPN에 속하는 사이트들을 백본 네트워크를 통하여 안전하게 연결하기 위해 터널링 메커니즘을 사용한다. 터널링 메커니즘으로 사용되는 것은 IPsec, GRE(Generic Routing Encapsulation), IP/IP, L2TP(Layer 2 Tunneling Protocol), MPLS 등 다양하다. 이 중에서 MPLS<sup>[2]</sup>는 IPsec<sup>[3]</sup>에 비해 다양한 프로토콜을 지원할 수 있을 뿐 아니라 ATM, Frame Relay, IP를 포함하는 다양한 하부구조 상에서 구현이 가능하다. 또한, 명시 라우팅(explicit routing), QoS, 트래픽 엔지니어링<sup>[4]</sup>과 같은 기능 지원도 용이하다는 장점을 갖는다. MPLS의 레이블을 이용하여 같은 VPN에 속하는 가입자들 사이에 LSP(Label Switched Path)<sup>[5]</sup>를 설정하여 VPN 서비스를 제공하는 것이 MPLS 기반 VPN 기술의 핵심이며, 이를 간단히 MPLS VPN이라 한다. 결과적으로, MPLS VPN은 높은 확장성, 효율적인 비용, 그리고 사용자가 요구한 다양한 QoS를 제공하여 IP 터널링 방식을 이용한 VPN에 비해 낮은 비용으로 서비스를 제공해 준다. MPLS는 이와 같은 이점을 바탕으로 VPN을 구성하기 위한 최적의 방안으로 간주되고 있다.

MPLS VPN에 대한 표준화가 IETF에서 추진되고 있으며, 두 가지의 기본적인 구조가 제안되고 있다. 그 중 하나는 BGP-E(Border Gateway Protocol multiprotocol Extension)를 이용하는 방식이고, 다

른 하나는 VR(Virtual Router) 개념을 이용하는 방식이다. BGP-E 방식은 시스코에 의해 제안되어 RFC2547로 채택되었다<sup>[6]</sup>. 이 방식에서는 BGP-E를 이용하여 VPN 도달 정보와 멤버십 정보를 PE(Provider's Edge device) 라우터 간에 교환한다.

VR 방식은 루슨트와 비바체네트워크를 중심으로 여러 기업들이 지지하고 있으며, PE 라우터 상에 VPN 별로 VR을 배치하고 같은 VPN에 속하는 VR 사이에 기존 라우팅 프로토콜을 이용하여 라우팅 정보를 교환한다. 이 방식은 RFC2917로 채택되었다<sup>[7]</sup>.

MPLS VPN에서의 이동성 지원에 관한 연구로서 참고문헌[8]에서 VPN 사이트 내의 어떤 노드가 다른 사이트로 이동하는 경우 기존의 VPN 서비스를 지속하기 위해 Mobile IP 및 경로 최적화(route optimization) 프로토콜을 확장하고 이동 엔티티 기능을 구현하였다. 그렇지만, 본 논문에서는 현재 활발히 상용화 작업이 이루어지고 있는 BGP-E를 이용한 MPLS VPN을 대상으로 하여 VPN 서비스 지원 기능과 VPN 사이트 내의 노드에 대한 이동 서비스 지원을 위한 라우터 구현 방안을 제시한다. 또한, 참고문헌[8]에서 제안된 방식에 따라, PE 라우터가 이동 엔티티(홈 에이전트, 외부 에이전트, 대응 에이전트)의 기능을 수행하도록 MPLS 라우터 제어 기능을 구현한다. 참고문헌[9]에서는 CE(Customer Edge)라우터에 이동성 지원 기능을 구현하는 방식을 제시하고, 제안된 방식의 성능을 시뮬레이션을 통해 분석하였다. 그러나, 본 연구는 PE 라우터에서 이동 서비스를 제공하는 방식이며 제안된 방식을 실제로 구현하여 성능을 측정하였다. 참고문헌[10]에서는 MPLS 기반의 백본 네트워크 내의 PE 라우터에서 Mobile IP 프로토콜과 MPLS 기능을 통합하는 방식을 제안하였다. 이 연구는 VPN 서비스를 제공하는 MPLS 라우터가 아니라 일반 MPLS 라우터에서 Mobile IP 프로토콜을 지원한 것이다.

본 논문은 다음과 같이 구성된다. 2장에서는 MPLS VPN 구성 방식을 분석하고, 3장에서는 BGP-E를 이용한 MPLS VPN의 설계 및 구현에 대해 기술한다. 4장에서는 구현된 MPLS VPN 라우터에 대해 다양한 시나리오에 따라 시험 환경에서 수행한 결과를 분석한다. 5장에서 결론을 맺는다.

## II. MPLS VPN 구조

이 절에서는 MPLS VPN의 구성 방식을 기술하

고, BGP-E 방식과 VR 방식을 소개하며 두 방식의 차이점을 기술한다.

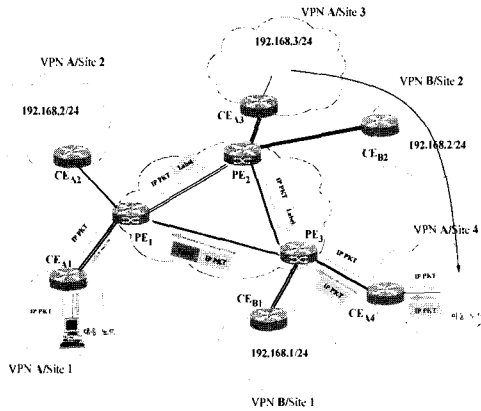


그림 1. MPLS VPN 구성 및 노드 이동 예

MPLS VPN은 그림 1과 같이 PE, P(Provider's device), CE(Customer site's Edge device) 등의 요소로 구성된다. P와 PE는 서비스 제공자의 백본 네트워크에 속해 있고 CE는 고객 사이트 내에 속해 있다. CE는 스위치나 라우터일 수도 있다. 고객 사이트의 백본 네트워크 접속은 CE와 PE 간의 링크를 통해서만 가능하다. P는 VPN을 위한 별도의 기능을 갖지 않고 VPN에 관한 정보도 따로 유지하지 않는다. PE에는 입력되는 패킷을 VPN에 따라 구분하여 포워딩하는 기능이 포함된다. 이 기능은 백본 네트워크 내에 VPN 별로 폐쇄 사용자 그룹(Closed User Group)을 정의하기 위해 필수적이다. 그림 1에서, 대응 노드와 이동 노드 사이의 패킷 전달 과정은 3.1 절에서 기술한다

### 2.1 BGP-E 기반의 MPLS VPN 구조

BGP-E 기반의 MPLS VPN은 그림 2에서 보듯이, PE 간에 VPN 사이트들의 도달 정보와 멤버십 정보를 전달하여 VPN을 구성하는 방식이다. 즉, PE 간에 VPN을 위한 라우팅 정보를 분배할 때, VPN 멤버십 정보도 함께 실어 보내는 piggybacking 방식이다<sup>16)</sup>. BGP-E의 원조인 BGP4는 AS(Autonomous System) 간에 라우팅 정보를 교환하기 위한 프로토콜로서 IPv4 형태의 라우팅 정보만을 다룰 수 있다. BGP4를 IPv6 혹은 IPX를 비롯한 다양한 형태의 라우팅 정보도 교환할 수 있도록 확장한 것이 BGP-E이며<sup>11)</sup>, BGP-E 기반의 MPLS VPN에서는 "VPN-IPv4" 형태의 라우팅 정보를 교환한다.

VPN 라우팅 정보는 PE들 간의 BGP 세션에 의해 분배된다. BGP-E가 분배하는 주소의 형태는 VPN-IPv4이다. VPN-IPv4 주소란 IPv4 앞에 경로 식별자(RD : Route Distinguisher)를 붙인 것이다. 각 VPN은 사실 주소 체계를 가지기 때문에, RD는 동일한 IPv4 주소 영역을 갖고 있는 다른 VPN을 구분하기 위해서 필요하다. RD는 CE로부터의 입력 인터페이스와 미리 연관되어 있어야 한다. 왜냐하면, CE로부터 온 IPv4 경로 앞에 PE가 RD를 붙여 분배할 수 있어야 하기 때문이다. 한편 PE가 BGP-E로 VPN-IPv4 경로를 분배할 때, VPN-IPv4에 대한 레이블도 함께 분배한다. VPN-IPv4에 대한 레이블은 레이블 스택에서 둘째 레이블, 즉 안쪽을 구성한다.

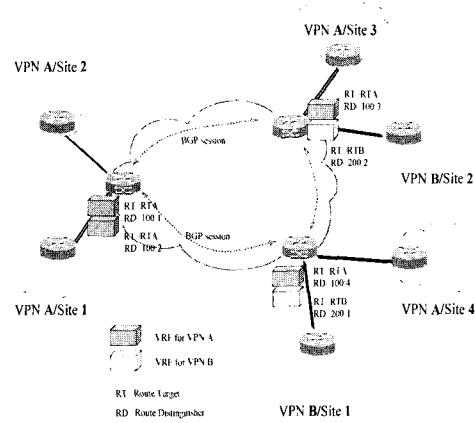


그림 2. BGP-E를 이용한 네트워크 기반 MPLS VPN

한편, 각 PE에는 고객 사이트 별로 VRF(VPN Routing and Forwarding) 테이블이 존재한다. 여러 VPN에 대한 포워딩 정보를 여러 VRF들에 적절히 나누어 저장하는 것은 멤버십 기능에 의해 가능하다. VPN 멤버십 기능을 위한 핵심적 요소인 RT(Route Target)는 BGP-E 패킷의 애트리뷰트(attribute)로서 라우팅 정보 분배를 제어할 수 있게 한다. 그림 2에서 보듯이 모든 VRF는 하나 이상의 RT와 연관된다. 또한, VPN-IPv4 경로도 하나 이상의 RT와 연관된다. VPN-IPv4 경로는 같은 RT와 연관된 VRF에만 분배되어야 한다. 즉, PE는 VPN-IPv4 경로를 받으면 같은 RT를 갖고 있는 VRF들에 그 경로를 입력시킨다. 고객 사이트로부터 CE를 통하여 VPN 데이터 패킷이 PE에 도착하면 PE에서는 그 고객 사이트에 해당하는 VRF를

참조한다. VRF에서 그 데이터 패킷에 대한 두개의 레이블과 다음 홉에 대한 정보가 포함되어 있다. 두개의 레이블 중 안쪽 레이블은 앞에서 언급한 대로 BGP-E에 의해서 분배된 것으로서 멤버 VPN에 대한 정보이다.

## 2.2 VR 기반의 MPLS VPN 구조

VR을 이용한 MPLS VPN에서는 PE에 VPN 별로 VR을 두어 라우팅, 패킷 포워딩, QoS, 서비스 관리를 VPN별로 수행한다<sup>[7]</sup>. VR이란 물리적인 실제 라우터와 같은 기능을 수행하는 가상의 라우터를 일컫는다. VR은 다양한 VPN 설정을 지원할 수 있는 개념으로서, VR 간에 계층 2 기반의 일대일 연결도 가능하며, 여러 개의 VR을 하나의 VR로 합쳐서 네트워크 기반 VPN에 활용할 수 있다. 하나의 PE에 백본 VR이 있고, 백본 VR에는 여러 개의 VPN용 VR이 있다. 백본 VR은 기능적으로 다른 VR과 같다. 백본 VR이 VPN용 VR들을 수용하므로 새로운 VPN 사이트의 추가로 인하여 백본 네트워크의 설정 상태가 변화되지는 않는다.

VPN 라우팅 정보는 MPLS에서 제공하는 터널 즉, LSP를 통해 전달된다. 백본 VR은 한 VPN 내의 VR들이 마치 직접 연결된 것처럼 수행될 수 있도록 해준다. 따라서, 한 VPN 내의 VR들은 서로 직접 기존의 라우팅 프로토콜로 라우팅 정보를 교환한다. 이러한 라우팅 프로토콜은 VPN을 위해서 어떠한 확장이나 변경도 요구하지 않는다. RIP, OSPF, BGP4 등과 같은 동적 라우팅 프로토콜 뿐만 아니라 정적인 경로 지정도 가능하다. 또한, PIM(Protocol Independent Multicast)과 DVMRP(Distance Vector Multicast Routing Protocol)와 같은 기존의 멀티캐스트 라우팅 프로토콜도 활용될 수 있다. 그림 3에서는 VR 기반의 MPLS VPN 예를 보여준다. 각 PE에는 VPN별로 VR이 존재하며 VR 사이에는 터널로 연결된다.

VR 방식에서는 같은 VPN에 속한 고객 사이트들이 VR에 의해 폐쇄적으로 연결된다. 따라서, 데이터 패킷 전달은 일반 라우터를 사용하는 사실망과 동일하게 수행된다. VR 간의 터널은 2.1절에서 언급된 것처럼 두 단계 레이블 스택킹에 의한 LSP 공유 메커니즘을 활용할 수 있다.

VR 방식에서는 VPN 멤버십 기능과 도달성 기능이 분리된 메커니즘으로 구현된다. 도달성 정보는 한 VPN에 속하는 VR들 사이의 라우팅 프로토콜에 의해 분배된다. 멤버십 메커니즘은 각 PE가 어떤

VPN에 속하는 VR들을 가져야 할 지를 결정할 뿐만 아니라 어떻게 LSP를 연결할 지를 결정한다. 이 방식은 확장성이 우수하며, 다양한 VPN 설정을 수용할 뿐만 아니라 기존 라우팅 프로토콜을 활용하므로 IPv6 혹은 멀티캐스트와 같은 다른 종류의 트래픽을 처리하기 쉽다는 장점을 갖고 있다. 그러나, BGP-E 방식에 비해 구체적인 상용화 작업은 아직 미흡하다.

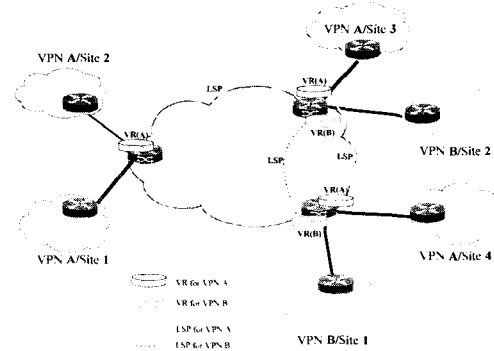


그림 3. VR을 이용한 네트워크 기반 MPLS VPN

반면에, BGP-E 방식에서는 VPN 도달성 정보와 멤버십 정보가 BGP-E에 의해서 동시에 분배된다. VPN 도달성 정보는 VPN-IPv4 형태로 PE들 간에 교환된다. VPN 멤버십 정보는 도달성 정보를 전송할 때, 함께 전송되는 애트리뷰트인 RT(Route Target)에 의해 전송된다. RT는 해당 도달성 정보가 어떤 VRF에 의해 수신되어야 할 것인지를 알려주는 방식으로 멤버십 기능을 수행한다. 또한, BGP-E라는 기존 프로토콜을 그대로 활용함으로써, 구현과 관련하여 상세 기술이 비교적 쉽게 명료화될 수 있다. 이런 이유로 MPLS VPN의 구현 기술로는 처음으로 RFC로 등록되었고, 상용화 제품도 먼저 출시되었다. 따라서, BGP-E 방식이 향후 MPLS VPN의 정식 표준으로 확립될 가능성이 매우 크다.

## III. BGP-E를 이용한 MPLS VPN 설계 및 구현

### 3.1 이동성 지원 방식

2장에서 소개된 MPLS VPN에서 이동성 지원을 제공하기 위해 참고문헌[8]에서는 Mobile IP<sup>[12]</sup> 및 Route Optimization<sup>[13]</sup> 프로토콜을 확장하였다. 또

한, 이동 서비스 지원을 위해 Mobile IP에서 제시된 이동 엔티티, 즉 홈 에이전트(HA: Home Agent), 외부 에이전트(FA: Foreign Agent) 이외에 경로 최적화를 위해 참고문헌[15]에서 제안된 새로운 형태의 이동 엔티티인 대응 에이전트(CA, Correspondent Agent) 개념을 도입하고 있다. 본 논문에서는 참고문헌[8]에서 제안된 이동 서비스 방식을 BGP-E 기반 MPLS VPN에 적용하기 위해 PE 라우터를 설계하고 구현하였다.

대응 에이전트는 이동 노드와 통신하고자 하는 대응 노드(Correspondent Node)가 위치한 VPN 사이트에 연결된 PE 라우터 상에서 수행된다. 네트워크 사업자의 경계 라우터인 PE 라우터는 VPN 서비스를 지원하기 위한 구성 요소와 이동 서비스(Mobile IP) 지원을 위한 에이전트 기능(홈 에이전트, 외부 에이전트, 대응 에이전트)을 모두 포함해야 한다. BGP-E를 이용한 MPLS VPN에서 CE 라우터는 PE 라우터와는 달리 VPN 서비스 및 이동 서비스에 대해 투명하게 동작한다. MPLS VPN에서 이동 서비스를 제공하기 위한 기본 요구사항은 Mobile IP와 같다. 다만 이동 노드가 이동을 인식할 수 있도록 모든 PE 라우터에서 수행되는 외부 에이전트는 자신과 연결된 각 VPN별로 사이트마다 그림 4와 같은 VPN 식별정보를 추가하여 서로 다른 "ICMP Agent Advertisement" 메시지를 전송해야만 한다.

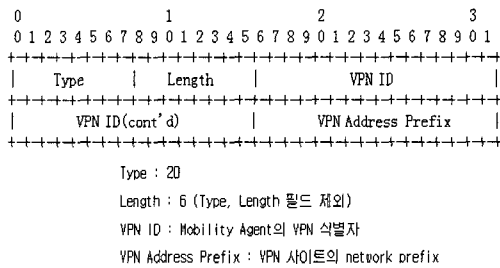


그림 4. ICMP Agent Advertisement 메시지 내의 VPN Information Extension

이동 노드가 이동을 확인한 이후의 등록 과정도 Mobile IP 프로토콜과 유사하다. 그러나, 기존 홈 에이전트에서 관리하는 이동 노드 관리 정보인 "Mobility Binding"에는 MPLS VPN 서비스를 위해 VPN 정보(근원지 VPN 식별자, 목적지 VPN 식별자)가 추가되어야 한다. 이 정보를 기반으로 홈 에이전트는 이동 노드가 어떤 VPN으로 이동했는지 파악하게 된다. 또한, PE 라우터에서 수행되는

홈 에이전트는 각 VPN 별로 "Mobility Binding"을 유지해야 하며, 외부 에이전트 역시 각 VPN 별로 "Visitor List"를 유지해야 한다.

홈 에이전트는 이동 노드의 등록이 받은 후, 등록 메시지에 'VPN Information Extension'을 확인한다. 그런 다음, 이동 노드의 "Care-of Address"와 VPN 정보를 커널 내에서 홈 에이전트가 관리하는 VPN 이동 바인딩(VPN Mobility Binding)에 각 VPN별로 구분하여 저장하고, 등록 응답을 이동 노드가 현재 위치하는 외부 에이전트에게 보낸다.

그림 1의 이동 예에서, 대응 노드가 전송한 패킷을 받은 홈 에이전트는 각 VPN 별로 구성된 "Mobility Binding"에서 이동 노드의 정보를 추출한다. 홈 에이전트에 의해 목적지 노드가 PE<sub>3</sub>로 이동했다는 것을 파악한 후, PE<sub>2</sub>는 PE<sub>3</sub>로 패킷을 전달한다. PE<sub>3</sub>에서는 패킷을 수신하고, 외부 에이전트를 통해 목적지 노드가 어느 사이트로 이동했는지 파악한다. PE<sub>3</sub>는 외부 에이전트에서 관리하는 VPN A에 해당하는 "Visitor List" 정보에 따라 CE<sub>A4</sub> 사이트 내에 목적지 노드가 존재함을 알게 된다. 그런 다음 PE<sub>3</sub>는 CE<sub>A4</sub>로 패킷을 전달한다. CE<sub>A4</sub>는 수신된 패킷을 자신의 사이트로 브로드캐스팅(broadcasting)하고 이동 노드는 자신의 패킷을 수신한다.

이동 노드가 대응 노드로 응답 패킷을 전송하는 과정을 살펴보자. 우선 PE<sub>3</sub>가 CE<sub>A4</sub>로부터 패킷을 수신한다면, PE<sub>3</sub>는 VPN A에 해당하는 VRF를 검색할 것이다. 그런 다음, 수신된 패킷의 목적지 주소에 따라 PE<sub>1</sub>으로 레이블 패킷을 전달한다. PE<sub>1</sub>은 패킷을 수신한 후, CE<sub>A1</sub>에게 전달한다. 그림 1에서 보듯이, 패킷 전달에서 삼각 라우팅(triangle routing) 현상이 발생한다. 삼각 라우팅은 Mobile IP 프로토콜의 문제점이며, 이것을 보완하기 위해 경로 최적화(route optimization) 방안<sup>[13]</sup>을 적용한다. 참고문헌[13]의 경로 최적화 방안은 먼저, 홈 에이전트가 대응 노드에게 "Binding Update" 메시지를 통해 이동 노드의 바인딩 정보를 전달한다. 그런 다음 대응 노드가 이동 노드의 바인딩 정보를 가지고 직접 이동 노드에게 패킷을 전달하는 것이다. 이 방법은 대응 노드가 VPN 서비스와 Mobile IP 서비스에 투명하게 동작하지 못하게 하기 때문에 좋은 방법이 아니다.

따라서, 홈 에이전트는 대응 노드에게 "Binding Update" 메시지를 전달하는 것이 아니라, 대응 노드가 속한 VPN 사이트의 PE 라우터 즉, 대응 에이

전트에게 전달하게 한다. 대응 에이전트는 라우팅을 변경하여 이동 노드가 속한 외부 에이전트로 설정된 LSP 터널을 이용한다. 이렇게 하면 대응 노드는 이동 노드의 이동성 여부에 투명하게 동작한다.

### 3.2 PE 라우터 상의 VRF 구현

본 연구에서 구현한 MPLS VPN 라우터는 다수의 VPN 그룹에게 VPN 서비스와 VPN 노드의 이동성을 제공하며 VPN 그룹들을 효율적으로 관리하기 위해 하나의 VPN 인덱스 테이블을 가지고 있다. 그림 5의 VPN 인덱스 테이블은 각 VPN 그룹별로 관리되는 테이블들의 인덱스를 저장한다. VPN 인덱스 테이블의 구성은 VPN 그룹을 식별하는 VPN ID, VRF 테이블, VPN 사용자의 이동성 지원을 위해 홈 에이전트에서 사용되는 “Mobility Binding Entry”, 외부 에이전트에서 사용되는 “Visitor List Entry”, 대응 에이전트에서 사용되는 “Binding Cache Entry”, 그리고 VPN 가입자인 CE 라우터로 패킷을 전송하기 위한 “VPN Out Information Entry”의 헤더 포인터로 이루어진다. 이와 같이 설계된 VPN 인덱스 테이블은 VPN ID 값을 통해 여러 VPN 그룹의 라우팅 정보와 이동성 정보를 효율적으로 검색, 관리하는 것을 가능하게 한다. VPN ID는 입구(Ingress) PE 라우터의 경우에 입력 인터페이스 정보에 따라 식별되며, 출구(Egress) PE 라우터의 경우 수신된 VPN 패킷 내의 VPN 레이블 정보에 의해 식별된다.

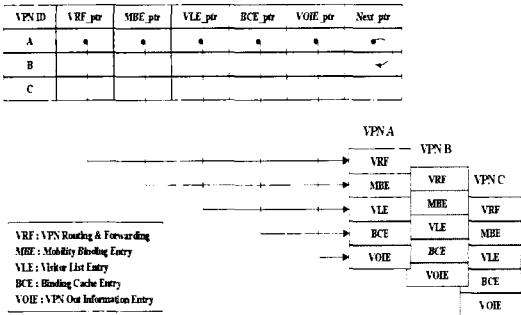


그림 5. VPN 인덱스 테이블

MPLS VPN은 VPN 사이트들간을 MPLS LSP를 이용하여 터널링하는 서비스이다. VPN 가입자 사이트들간의 라우팅 정보를 관리하기 위해 PE 라우터 내에 VPN용 라우팅 테이블인 VRF를 연결리스트(linked list)로 구현하였다. VRF 테이블을 위한 자료구조는 리스트 구현을 위해 그림 6과 같이 설

계되었고, 테이블 내의 각 필드들은 VPN 서비스를 제공하기 위해 필요한 정보들을 저장한다. 각 필드의 사용 목적은 다음과 같다.

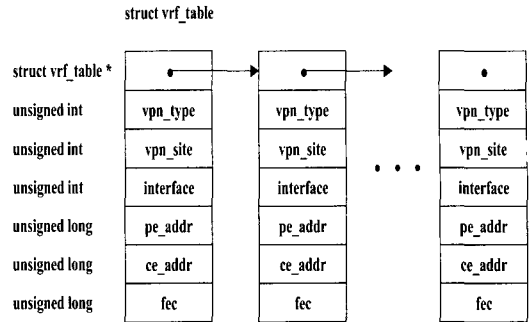


그림 6. /include/net/mpls.h 파일에 정의된 vrf\_table 구조체

VRF 테이블에서 ‘vpn\_type’ 필드는 자신과 stub 링크로 연결되어 있는 CE 라우터로부터 위치 정보를 받았을 경우와 이웃 PE 라우터로부터 받았을 경우를 구분하기 위해 사용되는 필드로서 Local이나 Remote를 값으로 사용한다. ‘vpn\_site’ 필드는 동일 VPN의 사이트인지를 의미한다. ‘interface’ 필드는 VPN 사이트의 출력 인터페이스를 가리킨다. 또한, ‘pe\_addr(PE address)’ 필드는 VPN FEC (Forwarding Equivalence Classes)에 해당하는 VPN 사이트에 도달하기 위한 PE 라우터의 IP 주소가 들어가고 ‘ce\_addr(CE address)’ 필드는 위치정보를 전달한 CE 라우터의 IP 주소가 들어가며, fec 필드에는 각 도달 정보의 VPN FEC가 들어간다.

### 3.3 입구(Ingress) PE 라우터 기능 구현

이동성을 지원하는 MPLS 라우터의 동작은 입구 라우터와 출구 라우터로 구분할 수 있다. 우선, 입구 라우터로 동작하는 PE 라우터의 구현 내용과 동작 과정을 설명한다.

VPN 사이트로부터 데이터 패킷을 받은 입구 PE 라우터는 패킷을 목적지로 전송하기 위한 절차를 시작한다. 수신된 패킷의 목적지 IP 주소와 헤더 정보를 검사하고, 목적지 IP 주소와 패킷 형식이 올바른 경우 수신한 패킷이 VPN 패킷인지를 식별한다. 이미 각 인터페이스마다 특정 VPN 그룹이 맵핑되어 있으므로 수신한 패킷의 인터페이스 정보를 통해 VPN 패킷을 식별한 후, 해당 VPN 사이트의 VPN ID를 얻는다.

VPN ID는 VPN을 구분하기 위한 식별자이다. PE 라우터는 VPN ID를 통해 해당 VRF 테이블을

결정한다. 결정된 VRF 테이블에서 패킷의 목적지 주소와 일치하는 VPN FEC를 검색한다. 일치하는 VPN FEC가 존재하면 목적지에 도달하기 위한 원격의 PE 라우터 주소를 알 수 있고 이 주소를 통해 이미 백본(backbone)에 설정된 LSP(Label Switched Path)를 위한 MPLS 레이블 정보를 FIB(Forwarding Information Base)에서 액세스 할 수 있다.

PE 라우터에 LSP가 설정된 경우, FIB에는 FEC에 대한 MPLS 레이블 정보가 존재한다. FIB에 MPLS 레이블 정보가 존재할 경우 MPLS 처리 모듈로 패킷을 전달하게 된다. 패킷을 수신한 출구 PE 라우터에서는 VPN 레이블을 통해 출력 인터페이스를 구분한다. 그리고 VRF의 검색을 통해 알아낸 목적지 PE 라우터 주소를 이용하여 입구 PE에서 출구 PE까지의 백본(backbone) LSP를 통해 MPLS 레이블 패킷을 전송한다.

Out 레이블이 부착된 MPLS 패킷은 2 계층에 패킷을 전달함으로써 출력 인터페이스를 통해 다음 홉(LER 또는 LSR)으로 패킷을 전송한다.

### 3.4 출구(Egress) PE 라우터 기능 구현

출구 라우터의 동작은 크게 1) stub 링크로 연결된 VPN 노드로의 패킷 처리, 2) 이동 노드를 위한 LSP의 변경, 3) 이동 노드가 PE 라우터의 관리 영역으로 이동해왔을 때의 패킷을 처리하는 세 가지로 동작으로 구분할 수 있다.

1) stub 링크로 연결된 VPN 노드로의 패킷 처리  
출구 PE 라우터는 수신한 패킷의 바깥쪽 MPLS 레이블을 제거하고 패킷으로부터 안쪽 레이블 즉, VPN 레이블이 존재하는지를 판별한다. 패킷에 VPN 레이블이 존재하면 출구 PE 라우터는 VPN 패킷으로 인식하게 되고 VPN 서비스를 제공하기 위한 처리를 수행하게 된다.

네트워크 인터페이스로부터 패킷을 수신한 후, 바깥쪽 레이블에 대한 처리를 수행한다. 출구 PE에서 바깥쪽 MPLS 레이블의 처리는 레이블과 맵핑되어 있는 명령어 정보에 따라 수행된다.

그런 다음, 출구 PE 라우터는 안쪽 VPN 레이블의 존재를 식별한다. VPN 레이블이 부착된 패킷을 확인한 출구 PE 라우터는 Shim 헤더로부터 VPN 레이블 값(VPN ID)을 얻어 해당 VPN의 VRF 테이블을 검색한다. VRF에서 목적지 주소와 일치하는

VPN FEC 필드가 존재하면 동일 레코드의 Type(local) 과 Intf를 반환한다. 그리고 “Mobility Binding” 테이블을 검색하여, 목적지 VPN 노드가 이동하지 않았을 경우 VPN 레이블을 제거하고, 목적 노드가 속한 VPN 가입자 CE 라우터로 패킷을 전달한다.

### 2) 이동 노드를 위한 LSP의 변경

VPN 노드가 이동했을 경우, 홈 에이전트는 수신된 패킷을 이동 노드에게 전달하기 위해 이동 노드가 방문한 네트워크의 라우팅 정보를 가지고 있는 “Mobility Binding Entry”를 검색한다. “Mobility Binding Entry”에 목적지 VPN 노드의 주소 항목이 존재하면 출구 PE 라우터는 해당 노드가 다른 라우터로 이동했음을 판단하고 이동 노드가 속한 외부 에이전트로 패킷 전달을 위한 처리를 수행하게 된다. 그림 7은 이동 노드를 위해 LSP를 변경하는 PE(HA) 라우터의 패킷 처리 흐름도 이다.

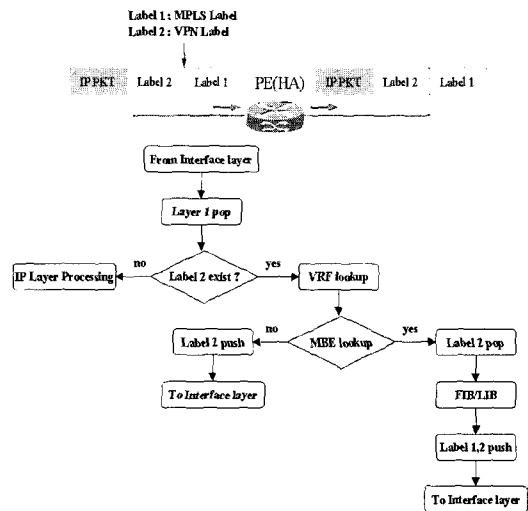


그림 7. 이동 노드를 위해 LSP를 변경하는 PE(HA) 라우터의 흐름도

### 3) 이동 노드가 PE 라우터의 관리 영역으로 이동해 왔을 때의 패킷 처리

변경된 LSP를 통해 패킷을 수신한 출구 PE 라우터(외부 에이전트)는 바깥쪽 레이블인 MPLS 레이블을 제거하고 VPN 레이블에 의해 VRF를 결정한다. 그런 다음, PE 라우터는 이동 노드가 자신이 관리하는 지역으로 이동해 왔는지를 확인하기 위해 “Visitor List”를 검색한다. “Visitor List Entry”에 이동 노드의 주소가 존재하면 PE 라우터는 이동 노

드의 방문을 확인하고 VPN 레이블을 제거한 후, "Visitor List Entry"의 출력 인터페이스를 통해 VPN 정보를 획득하여 이동 노드에게 패킷을 전달한다.

#### IV. 시범 구현 및 분석

##### 4.1 시험 환경 구성

그림 8은 본 논문에서 제안한 방식의 시범 구현을 위해 구성한 시험 환경 및 PE 라우터 사이에 분배된 MPLS 레이블을 보여준다. LDP(Label Distribution Protocol) 시그널링을 통해 동적으로 LSP(Label Switched Path)가 구성되며, 분배된 레이블 값(30, 60, 40, 70, 90, 100, 80, 50)은 FEC(Forwarding Equivalence Class)가 192.168.x/24로 설정되고 백본 네트워크에서 데이터를 전달하기 위한 레이블이다. 또한, 레이블 값(31, 21, 32, 22)은 FEC가 168.188.x/24로 레이블 값(51, 41, 52, 42)은 FEC가 202.188.x/24로 설정되고 Mobile IP 에이전트간의 메시지 전송을 위한 레이블이다.

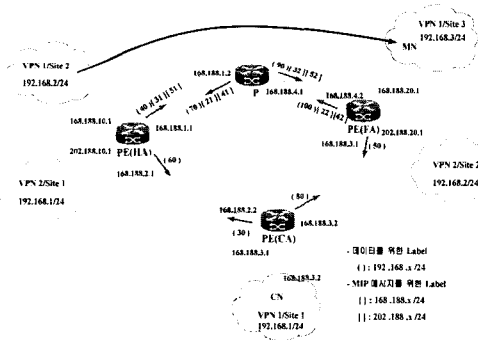


그림 8. 시험 환경 구성 및 레이블 분배 과정

백본 네트워크의 구성에서 PE 라우터는 리눅스 시스템을 이용하였고, 각 PE 라우터는 LER(Label Edge Router)로서 MPLS VPN 서비스 뿐만 아니라 이동 에이전트(HA, FA, CA)의 역할을 수행하게 된다. LSR 역할을 담당하는 P 라우터는 홈 에이전트와 외부 에이전트간의 패킷 전송시 레이블 스위핑을 수행하며, 리눅스 시스템 상에서 동작하도록 구현하였다. 홈 에이전트와 외부 에이전트는 각각 두 개의 VPN 사이트를 갖도록 구성하였고, 이동 노드가 동일 VPN 내 다른 사이트로 이동하는 경우를 대상으로 실험하였다.

본 연구에서는 mpls-linux 버전 0.996을 이용하

였고 이에 대응하는 kernel 2.4.12를 사용하였다<sup>[13]</sup>. mpls-linux는 커널 패치를 통해 설치되고, static한 방식과 LDP(Label Distribution Protocol) 시그널링을 통한 LSP의 설정이 모두 가능하다. mpls-linux는 MPLS 패킷의 처리를 위해 In/Out 레이블과 인스트럭션을 매핑시킴으로써 전체적인 MPLS의 동작을 수행하고 있다. 본 연구에서는 이동성 지원을 위한 BGP-E 기반 MPLS VPN을 구현하기 위해, 수정된 Mobile IP 프로토콜<sup>[8]</sup>을 이용하여 기존의 mpls-linux를 확장하였다.

##### 4.2 결과 분석

백본 네트워크 상의 PE 라우터는 BGP-E를 이용하여 VPN 도달성 정보를 분배하고, 이 분배된 정보를 이용하여 각 PE 라우터들은 VRF를 구성한다.

그림 9는 제안한 방식의 구현 및 실험 결과 대응 에이전트의 역할을 수행하는 PE 라우터에 생성된 VRF 테이블을 보여준다. 'Type' 값이 '1'일 때는 local을 '2'일 때는 remote를 의미한다. 아래 그림에서 VPN1의 VRF 내의 두번째 엔트리는 VPN 1의 FEC가 192.168.2/24인 사이트는 2번 사이트로서 이 사이트에 도달하기 위한 PE 주소는 168.188.2.1이고 CE 주소는 192.168.2.1 라는 것을 나타내고 있다. 또한 'Type' 값은 2로서 대응 에이전트 역할의 PE 라우터와 다른 네트워크에 연결된 사이트임을 나타내고, 'Intf' 값은 패킷을 원격의 PE (168.188.2.1)로 내보내기 위한 출력 인터페이스 0(eth0)을 나타낸다. 아래 그림에서 "Don't care"는 PE 라우터 자신의 IP 주소인 이 값은 참조되지 않는다는 것을 의미한다

VPN 1의 VRF

Type	Site	Interface	PE_Address	CE_Address	VPN FEC
2	3	1	168.188.3.1	192.168.3.1	192.168.3.0
2	2	0	168.188.2.1	192.168.2.1	192.168.2.0
1	1	2	Don't Care	192.168.1.1	192.168.1.0

VPN 2의 VRF

Type	Site	Interface	PE_Address	CE_Address	VPN FEC
2	1	0	168.188.2.1	192.168.1.1	192.168.1.0
2	2	1	168.188.3.1	192.168.2.1	192.168.2.0

그림 9. 대응 에이전트 역할의 PE 라우터에 생성되는 VRF 테이블 로그

그림 10은 홈 에이전트의 역할을 수행하는 PE 라우터에 생성된 VRF 테이블을 보여준다. VPN1의 VRF 내의 두번째 엔트리의 예에서, VPN 1의 FEC가 192.168.1/24인 사이트는 1번 사이트로서 이 사



이트에 도달하기 위한 PE 주소는 168.188.2.2 이고 CE 주소는 192.168.1.1 라는 것을 의미한다. 또한 'Type' 값은 2로서 홈 에이전트 역할의 PE 라우터와 다른 네트워크에 연결된 사이트임을 나타내고, 'Intf' 값은 패킷을 원격의 PE(168.188.2.2) 라우터로 내보내기 위한 출력 인터페이스 2(eth2)을 나타낸다

VPN 1의 VRF

Type	Site	Interface	PE_Address	CE_Address	VPN_FEC
2	2	3	168.188.4.2	168.188.20.1	168.188.20.0
2	3	2	168.188.2.2	168.188.30.1	168.188.30.0
1	1	0	168.188.1.1	168.188.1.1	168.188.1.0

VPN 2의 VRF

Type	Site	Interface	PE_Address	CE_Address	VPN_FEC
1	1	1	168.188.2.1	202.188.10.1	202.188.10.0
2	2	3	168.188.4.2	202.188.20.1	202.188.20.0

그림 10. 홈 에이전트 역할의 PE 라우터에 생성되는 VRF 테이블 로그

외부 에이전트의 역할을 수행하는 PE 라우터에 VRF 테이블 생성 결과 역시 위의 예와 유사하다. 이와 같이, MPLS 라우터 내 VPN 및 이동성 지원용 각종 테이블들에 해당 정보가 이상 없이 생성, 관리되며, 이 결과 MPLS 패킷이 제대로 라우팅 되는 것을 확인하였다.

본 연구에서 제안한 이동성 지원 방식을 MPLS VPN에 적용한 경우, 대응 노드에서 이동 노드로 전송된 데이터 패킷의 손실율과 PE 라우터 작업 부하(workload)를 측정하였다. 이때 네트워크 내에서 이동 엔티티 사이에 전송되는 메시지의 손실은 없고, 가입자 네트워크에서의 전송 지연과 사업자 네트워크에서의 전송 지연은 실험 결과의 평균값으로서 각각 0.022, 0.05초로 가정하였다. 또한, 대응 노드는 이동 노드에게 데이터를 전송하기 위해 ping 프로그램을 이용하여 전송하며, ping 패킷은 3초 간격으로 전송하였다.

그림 11의 "Case A"는 "ICMP Agent Advertisement" 메시지의 전송 간격이 증가함에 따라 대응 노드에서 이동 노드로 전송한 패킷의 손실률을 보여주고, "Case B"는 이동 노드가 핸드오프에 소요된 시간 간격이 증가함에 따라 대응 노드에서 이동 노드로 전송한 패킷의 손실율을 보여준다. "Case A"에서 보듯이, 메시지의 전송 간격이 길어짐에 따라 이동 노드에서 수신되는 패킷의 손실이 증가함을 알 수 있다. 메시지의 전송 간격이 짧을수록 더 빠른 등록 과정이 이루어지며, 이동 노드로 전송되는 패킷의 손실은 감소된다. "Case B"는 이

동 노드가 VPN 사이트에서 다른 VPN 사이트로 이동하는 시간이 증가함에 따라 대응 노드에서 이동 노드로 전송되는 패킷의 손실이 증가하는 것을 나타낸다. 핸드오프에 소요되는 시간은 이동 노드가 어떠한 VPN 서비스도 받을 수 없는 상태이기 때문에, 무선랜과 같은 무선 네트워크를 이용하는 경우 이러한 요인에 의한 패킷 손실율은 상당히 감소할 것이다.

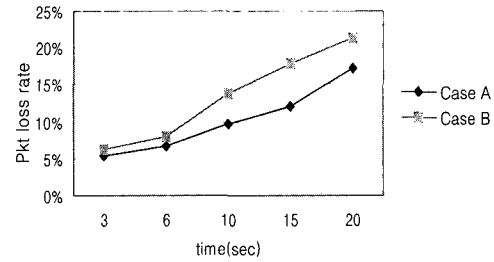


그림 11. 이동 노드 패킷 손실율

이동성 지원을 위한 MPLS VPN 기능은 PE 라우터 상에서 수행되기 때문에, PE 라우터의 성능에 상당한 부담을 준다. MPLS VPN 서비스를 제공하는 PE 라우터는 이동 서비스 제공을 위해 이동 엔티티 기능을 수행하며, 서로 다른 이동 엔티티로 동작하는 PE 라우터들은 서로 다른 작업부하를 갖는다.

표 1은 PE 라우터가 홈 에이전트, 외부 에이전트, 대응 에이전트로 동작하는 경우에, 대응 노드와 이동 노드 사이에 송수신되는 패킷에 따라 PE 라우터의 작업 부하를 처리 시간으로 측정된 결과를 보여준다. 이동 에이전트용 PE 라우터는 데스크탑 PC를 사용하였다.

표 1. PE 라우터의 작업 부하

단위 : micro second

	PE(HA)*	PE(FA)	PE(CA)
CN→MN	698.3	769.5	128.5
MN→CN	637.5	654.1	485.2

\* : "CN→MN과 MN→CN의 경우 모두 홈 에이전트와 연결된 MN(이동노드)은 이동하기 이전의 작업 부하이다.

표 1에서 "CN→MN"은 PE 라우터 관점에서 발신지 PE 라우터로부터 패킷을 수신하여 자신과 연결된 VPN 사이트로 패킷을 전달하는 것을 의미하고, "MN→CN"은 PE 라우터가 자신과 연결된

VPN 사이트로부터 패킷을 수신하여 목적지 PE 라우터로 패킷을 전달하는 것을 의미한다. 또한, 각 측정 시간은 본 연구에서 구현한 PE 라우터에서 MPLS 및 VPN 모듈이 처리되는데 걸리는 시간이다.

표 1에서 보듯이, 대응 에이전트(CA)가 수행되는 PE 라우터의 작업 부하는 홈/외부 에이전트(HA, FA)가 수행되는 PE 라우터보다 패킷 처리를 위한 작업 부하보다 작다. 홈 에이전트에서는 외부 에이전트로 패킷을 "Re-tunneling"하는 기능을 수행하며, 외부 에이전트에서는 이동 노드를 위한 "Smooth Handover" 기능을 수행한다. 또한, 홈 및 외부 에이전트는 이동 노드의 등록 과정에서 발생하는 Mobile IP 메시지를 일반 데이터 패킷과 구별하고 등록 과정을 처리해야 한다. 이러한 부하로 인하여 홈 및 외부 에이전트는 대응 에이전트에 비해 작업 부하가 크다.

또한, PE 라우터 상의 외부 에이전트 수행 부하가 홈 에이전트 수행 부하보다 약간 크다. "CN→MN"의 경우에서, 홈 에이전트는 발신지 PE 라우터로부터 입력되는 패킷의 VPN 레이블을 기반으로 VRF를 선택한다. 표 1에서 언급된 것처럼 이동 노드는 이동하지 않았기 때문에, 해당 VRF 내의 'VPN Type'의 값은 Local(노드가 이동하지 않음을 의미)이며 홈 에이전트는 MBE(Mobility Binding Entry)를 검색한다. 그러나, 노드의 이동 전이므로 MBE에는 해당 엔트리가 존재하지 않기 때문에, 이전에 선택된 VRF를 검색하여 얻은 출력 인터페이스로 패킷을 전달한다. 반면에, 외부 에이전트는 상대 PE 라우터로부터 입력되는 패킷의 VPN 레이블에 기반하여 VRF를 선택한다. 홈 에이전트의 경우와 달리, 이동 노드가 이동한 경우이므로 선택된 VRF 내의 'VPN Type'의 값은 노드의 이동을 의미하는 Remote이다. 외부 에이전트는 VLE(Visitor List Entry)를 검색하여 이동 노드와 일치하는 엔트리를 찾아 VLE에 저장된 출력 인터페이스로 패킷을 전달하게 된다. 따라서, 외부 에이전트에서는 홈 에이전트에 비해 추가적인 검색 과정이 더 요구되므로 작업 부하가 크게 된다.

"MN→CN"의 경우에서, PE 라우터 상의 홈 에이전트는 대응 노드(CN)로 패킷을 전달하기 위해 VLE를 검색하지만 이동 노드에 대한 항목이 존재하지 않기 때문에, 인터페이스 식별을 통해 얻은 VPN ID를 갖고 VRF를 찾아 목적지 VPN 사이트로 전송한다. 그러나, 외부 에이전트는 인터

페이스 식별을 통해 VPN ID를 얻을 지라도 이동 노드의 등록 이후에는 VLE에 이동 노드에 대한 항목이 존재하기 때문에, VLE 내의 'Source VPN ID'를 다시 검색하여 이동 노드가 속해 있는 VRF를 찾고 CN이 속한 목적지 PE 라우터로 전송한다. 이 경우에서도 외부 에이전트에서는 홈 에이전트에 비해 추가적인 검색 과정이 더 요구되기 때문에, 외부 에이전트의 작업 부하가 조금 더 큰 것으로 분석되었다.

## V. 결론

본 논문에서는 MPLS VPN을 구성하는 방안 가운데 PE라우터에 기반한 MPLS VPN을 대상으로 VPN 노드의 이동성을 지원하기 위한 MPLS 라우터 처리 기능과 관련 자료구조 모델을 제안하였다. 새로 제안된 모델을 이용하여 VPN 사용자는 이동 후에도 지속적인 VPN 서비스를 제공할 수 있다. 제안된 모델은 이동 노드가 동일 VPN 내에서 이동하는 경우뿐만 아니라, 다른 VPN 내의 사이트로 이동하는 경우, 혹은 일반 인터넷 지역으로 이동하는 경우에서도 모두 이용 가능하다.

본 연구를 수행함으로써, 최근 중요성이 부각되고 있는 MPLS VPN 기술과 이동 컴퓨팅 기술을 접목시킨 새로운 기초 기술을 확보할 수 있는 계기가 되었다. 이 기술은 향후 산업계에서 상용화될 가능성이 크며, 아직까지 개념 도입과 표준 정립 단계에 있는 MPLS VPN 분야에서 기술적 우위를 점하는 역할을 할 것으로 기대된다.

특히, 실험 환경에서 구현 결과를 기반으로 VPN 노드에 대한 이동 서비스 지원을 실제 확인하였고, VPN 노드의 이동에 따라 이동 노드로 전송되는 패킷의 손실율과 PE 라우터의 작업 부하를 측정하였다. 이러한 결과들은 향후 네트워크 사업자가 MPLS VPN 네트워크에서 이동 서비스를 지원하고자 하는 경우에 기초 자료로서 활용될 수 있을 것이다.

그러나, 실제 네트워크에 적용되기 위해서는 본 논문에서 구현한 이동성 지원 방식의 성능을 개선하기 위한 구현 코드의 최적화 과정이 필요하며, Mobile IP와 연동하는 VPN 관리 프로토콜의 최적화 기술 등에 대해 깊이 있는 연구가 필요하다. 또한, 향후 차세대 IP 주소인 IPv6에서의 이동성 지원 방안도 고려되어야 할 것이다.

참 고 문 헌

[1] B. Gleenson, et al., "A framework for IP based Virtual Private Network," IETF RFC2764, Feb. 2000.

[2] Eric Rosen, Arun Viswannathan, Ross Callon, "Multi-protocol Label Switching Architecture," IETF RFC3031, Jan. 2001.

[3] S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol," IETF RFC2401, Nov. 1998.

[4] D.Awduche, et al., "Requirements for Traffic Engineering over MPLS," IETF RFC2702, Sep. 1999.

[5] Loa Anderson, Paul Doolan, Nancy Feldman, Andre Fredette, Bob Thomas, "LDP Specification," IETF RFC3036, Jan. 2001.

[6] Eric Rosen, Yakov Rekhter, "BGP/MPLS VPNs," IETF RFC2547, Mar. 1999.

[7] K. Muthukrishnan, A. Malis, "A Core MPLS IP VPN Architecture," IETF RFC2917, Sep. 2000.

[8] 이영석, 오명환, 최 훈, "MPLS VPN에서의 Mobile IP", 한국통신학회논문지, Vol. 28, No 8, 2003. 8.

[9] 이영석, 최 훈, "이동성 지원을 고려한 MPLS 방식 가상사설망", 한국통신학회논문지, Vol 26., No.12C, p. 225-232, 2001. 12.

[10] Zong Ren, et al., "Integration of Mobile IP and Multi-protocol Label Switching," The International Computer Congress 2001, Hongkong, Nov. 2001.

[11] Yakov Rekhter, Eric Rosen, "Carrying Label Information in BGP-4," IETF Draft, Sep. 2001.

[12] Charles Perkins, "IP Mobility Support for IPv4," IETF RFC3344, Aug. 2002.

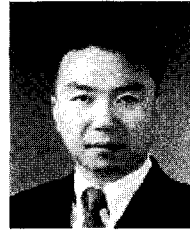
[13] Charles Perkins, David Hohnson, "Route Optimization in Mobile IP," IETF Draft, Nov. 2001.

[14] Cheng-Yin Lee, Glenn Morrow, Fayaz Kadri, "Intercepting Location Update," IETF Draft, Nov. 2000.

[15] <http://www.sourceforge.net>

이 영 석(Young-Seok Lee)

정회원



1992년 2월 : 충남대학교  
컴퓨터공학과 학사  
1994년 2월 : 충남대학교  
컴퓨터공학과 석사  
2002년 2월 : 충남대학교  
컴퓨터공학과 박사

1994년~1997년 : LG전자 연구원

2002년~현재 : 한국전자통신연구원 선임연구원

<주관심분야> 분산시스템, 가상사설망, 이동컴퓨팅

임 형 택(Hyoung-Taek Lim)

준회원



2002년 2월 : 충남대학교  
컴퓨터공학과 학사  
2002년 3월~현재 : 충남대학교  
컴퓨터공학과 석사과정

<주관심분야> 분산시스템, 이동컴퓨팅, 무선인터넷

최 훈(Hoon Choi)

정회원



1983년 2월 : 서울대학교  
컴퓨터공학과 학사  
1990년 12월 : Duke University  
전산학과 석사  
1993년 5월 : Duke University  
전산학과 박사

1983년~1996년 : 한국전자통신연구원 광대역  
통신망 연구부 선임연구원

1996년~현재 : 충남대학교 컴퓨터공학과 교수

2000년 : 미국 NIST(National Institute of Standards  
and Technologies) 객원연구원

<주관심분야> 분산시스템, 이동컴퓨팅, 컴퓨터통신,  
Fault-tolerant 시스템