MPLS VPN에서의 Mobile IP

정회원 이 영 석*, 오 명 환**, 최 훈**

Mobile IP on MPLS VPN

Young-Seok Lee*, Myoung-Hwan Oh**, Hoon Choi**

요 약

단말의 이동성을 지원하기 위한 방안으로 RFC3344에서는 Mobile IP(Mobile IPv4) 프로토콜을 제시하고 있다. 제시된 Mobile IP 프로토콜은 IP 네트워크에서 IP 터널링을 통해 단말의 이동성을 지원한다. 본 논문에서는 MPLS(Multiprotocol Label Switching) 네트워크에서 VPN(Virtual Private Network) 서비스를 제공받고 있는 단말에 대한 이동 서비스를 제공하는 방안을 다룬다. 이동 서비스를 제공하기 위해 고려된 MPLS VPN은 RFC2547에서 제시된 "BGP/MPLS VPNs" 방식을 기반으로 한다. MPLS VPN 서비스를 제공하는 PE(Provider's Edge) 라우터에 단말의 이동 서비스를 제공하기 위해 Mobile IP 프로토콜을 결합함하고, MPLS VPN 내의 단말이 동일한 VPN 내의 다른 사이트로 이동하는 경우, 다른 VPN 내의 사이트로 이동하는 경우, 일반 인터넷 지역으로 이동하는 경우로 구분하여 이동성 지원 메커니즘을 제시한다. PE 라우터 상에 메커니즘을 구현하고, 시범 환경을 구성하여 제안된 방식의 성능을 분석한다..

Key Words : VPN, MPLS, Mobile IP

ABSTRACT

Mobile IP protocol introduced in RFC3344 provides a node of the mobility service through IP tunneling mechanism in the IP networks. In this paper, we describe a method to provide a mobility service for VPN(Virtual Private Network) nodes on the MPLS(Multiprotocol Label Switching) network. The MPLS VPN considered here is based on "BGP/MPLS VPNs" presented in RFC2547. PE(Provider's Edge) routers, which are able to provide VPN services on the MPLS network, are associated with mobility agents to support Mobile IP. This proposed mechanism applies when a VPN node moves to other site of the same VPN, or when it moves to other site of a different VPN, or to the ordinary Internet site. We implemented this mechanism in PE routers and analyzed the performance of the MPLS VPN with mobility support on the testbed.

* 한국전자통신연구원(yslee@etri.re.kr), ** 충남대학교 컴퓨터공학과(mhoh@ce.cnu.ac.kr; hchoi@ce.cnu.ac.kr)
논문번호 : 030169-0424, 접수일자 : 2003년 4월 28일
※ 본 연구는 산업자원부의 지역전략산업 석·박사 연구인력 양성사업의 지원으로 수행된 것임.

Ⅰ. 서 론

VPN(Virtual Private Network)은 공중망이 사설망과 동일한 서비스를 제공하여, VPN 이용자들에게 마치 자신들만 연결된 사설망을 이용하는 것처럼 느끼도록 하는 것이다[1]. 이러한 VPN 기술의 구현을 통하여 낮은 비용으로 실제 사설망에서 제공될 수 있는 서비스를 지원하는 것이 가능하다.

VPN 구성 방식 가운데 IP(Internet Protocol) 터널링 기술을 이용한 VPN은 기존의 공중 인터넷 망에서 특정 VPN에 가입된 사용자들 사이에 IP 터널을 구성하여 VPN을 구성하는 방식으로서[2], 손쉬운 접속, 구축비용 절감 등 많은 장점을 가지고 있지만, 향후 실시간 멀티미디어 전송을 위하여 요구되는 QoS(Quality of Service) 및 트래픽 엔지니어링 능력을 지원하지 못하는 한계를 가지고 있다. 이에 반하여 MPLS(Multiprotocol Label Switching)[3]를 기반으로 하는 방식은 최근에 IETF(Internet Engineering Task Force)에서 활발하게 논의되고 있는 MPLS 라우터의 기능을 이용한 방식으로서, 같은 VPN에 속하는 가입자들 사이에 LSP(Label Switched Path)[4]를 설정하여 VPN 서비스를 제공하는 방안이다.

현재 IETF의 MPLS 위원회는 MPLS의 가장 유력한 응용분야를 VPN으로 간주하고 MPLS 기반 VPN 연구를 활발하게 진행하고 있다. 이에 따라, IETF에서는 MPLS VPN을 표준화하기 위해 시도중이며, 현재 RFC 2547 "BGP/MPLS VPNs"[5]이 유력한 산업계 표준으로 정립되고 있다.

한편, 이동통신망이나 무선 LAN을 통해 휴대형 단말기나 노트북 컴퓨터 등을 이용하여 언제, 어디서나 네트워크를 통해 업무를 처리하는 이동 컴퓨팅이 보편화되고 있다. 따라서, VPN 사업자도 VPN 이용자가 이동하는 경우에도 위치에 구애받지 않고 지속적으로 VPN 서비스를 제공할 필요가 있다.

본 논문에서는 VPN 사이트 내의 어떤 노드가 같은 VPN 내의 다른 장소로 이동하는 경우 또는 다른 VPN 내의 장소로 이동하는 경우에서 모두 VPN 서비스를 지속하게 하는 이동성 지원 프로토콜을 제안한다. 본 논문에서 기술된 VPN은 RFC 2547 "BGP/MPLS VPNs" 방식을 기반으로 하며, 이동성 서비스를 제공하기 위한 방안으로 기존의 Mobile IPv4 및 경로 최적화(Route Optimization)[6,7] 프로토콜을 확장하였다. Mobile IPv4는 RFC3344 표준으로 정립되어 있지만, Mobile IPv6는 현재 표준화가 진행중이다. 본 논문에서는 표준으로 정립된 Mobile IPv4를 확장하여 VPN에서의 이동 서비스 지원 방안을 제시한다.

MPLS VPN 서비스 기능을 제공하는 PE 라우터가 이동 엔티티(홈 에이전트, 외부 에이전트)의 기능을 수행하며, 이동 엔티티들을 통하여 이동 서비스를 제공한다. 또한, 효율적인 이동 서비스 지원을 위해 Mobile IP에서 제시된 이동 엔티티(홈 에이전트, 외부 에이전트) 이외에 경로 최적화를 위해 참고문헌 [8]에서 제안된 새로운 형태의 이동 엔티티인 대응 에이전트를 도입한다.

본 연구와 유사한 연구들로서 [9,10]이 발표된 바 있다. 참고문헌 [9]에서는 CE(Customer Edge) 라우터에 이동성 지원 기능을 구현하는 방식을 제시하고 그 방식의 성능을 시뮬레이션을 통해 분석하였다. 그러나, 본 연구는 PE 라우터에서 이동 서비스를 제공하는 방식으로서, 실제로 제안된 내용을 구현하여 성능을 분석하였다. 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 지원하는 것을 목적으로 하고 있다.

본 논문은 다음과 같이 구성된다. 2장에서는 기존 네트워크 기반의 MPLS VPN 구성 방식을 살펴보고, 3장에서는 MPLS VPN에서 이동 서비스를 제공하기 위해 확장된 Mobile IP 프로토콜과 동작 절차를 기술한다. 4장에서는 이동 서비스 지원을 위해 설계된 자료구조와 실험 결과를 기술하며 5장에서 결론을 맺는다.

Ⅱ. MPLS VPN 구성 방식

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, 다른 하나는 VR(Virtual Router) 개념을 이용하는 방식이다. BGP-E 방식은 시스코에 의해 제안되어 RFC2547로 채택되었고[5], 현재 다양한 상용 라우터 제품들이 출시되고 있다. 이 방식에서는 BGP-E를 이용하여 VPN 도달 정보와 멤버쉽 정보를 PE 라우터 간에 교환한다. VPN 라우팅 정보는 그림 1과

같이 PE들 간의 BGP 세션에 의해 분배된다. 각 PE에는 고객 사이트 별로 VRF(VPN Routing and Forwarding instance)가 있다. 여러 VPN에 대한 포워딩 정보를 여러 VRF들에 적절히 나누어 저장해 놓는 것은 멤버쉽 기능에 의해 가능하다.

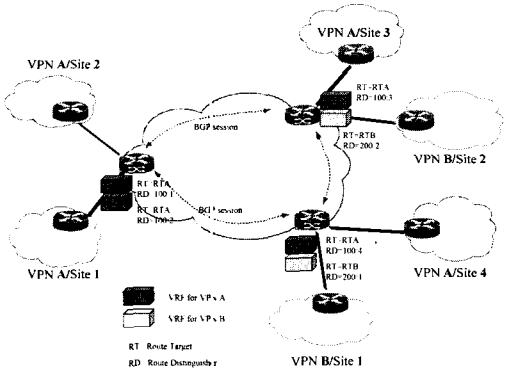


그림 1. BGP-E를 이용한 네트워크 기반 MPLS VPN

VR 방식은 루슨트와 바바체 네트워크를 중심으로 여러 기업들이 지지하고 있으며 IETF 기고서 형태로 추진 중에 있는 것[11]과 RFC2917로 채택된 것[12]이 있다. [11]에서 추진 중인 기고서는 현재 더 이상 구체적인 진행은 없는 상태이며, RFC2917[12] 기반의 MPLS 라우터에 대한 상용화 작업도 현재 활발히 이루어지지 않고 있다. VR 방식은 PE 들 사이에 VPN 별로 VR을 배치하고 같은 VPN에 속하는 VR 사이에 기존 라우팅 프로토콜을 이용하여 라우팅 정보를 교환한다. VR 방식에서는 같은 VPN에 속한 고객 사이트들이 VR에 의해 폐쇄적으로 연결된다. 따라서, 데이터 패킷 포워딩은 일반 라우터를 사용하는 사설망과 동일하게 수행된다. VR 간의 터널은 두 단계 레이블 스태킹에 의한 LSP 공유 메커니즘을 활용할 수 있다.

이 두 방식의 차이점은 도달성(Reachability)과 멤버쉽(Membership) 메커니즘의 분리 여부이다. BGP-E 방식은 도달성 정보와 멤버쉽 정보를 BGP-E를 이용하여 PE 간에 전달하는 방식이며, VR 방식은 도달성 정보를 VR 간에 전달하는 방식이다.

본 논문에서는 현재 활발히 상용화 작업이 이루어지고 있는 BGP-E를 이용한 MPLS VPN을 대상으로 하여 VPN 사이트 내의 노드에 대한 이동 서비스 지원 방안을 고려한다. VPN 사이트 내의 어떤 노드가 같은 VPN 내의 다른 사이트로 이동하는 경우와 다른 VPN 내의 사이트로 이동하는 경우에서 모두 기존의 VPN 서비스를 지속하기 위한 이동성 지원 프로토콜을 제안하고 구현한다.

Ⅲ. MPLS VPN에서의 Mobile IP 프로토콜 지원

MPLS VPN에서 이동성 지원을 제공하기 위해 고려되어야 할 사항들과 MPLS VPN 방식에서 이동 서비스 제공 방안에 대해 기술한다. 우선, 이동 서비스는 VPN 사이트 내의 어떤 노드가 같은 VPN 내의 다른 사이트로 이동하는 경우, 다른 VPN 내의 사이트로 이동하는 경우에서도 모두 VPN 서비스를 지속하게 하는 이동성 지원 프로토콜을 제시하였다. 본 방식은 인터넷에서 이동성 서비스를 제공하는 Mobile IP[6] 및 경로 최적화[7] 프로토콜을 확장하였다.

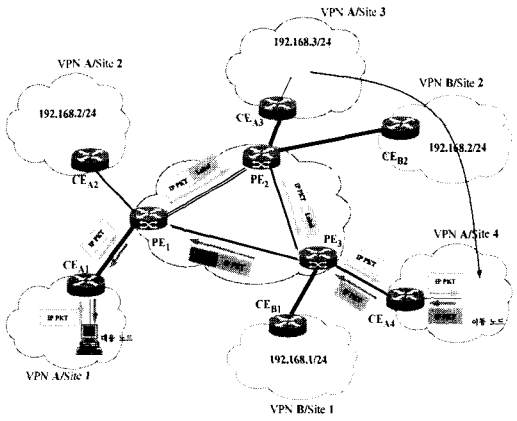


그림 2 . MPLS VPN 구성 및 노드 이동 예

MPLS VPN에서 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 [8]에서 제안된 새로운 형태의 이동 엔티티인 대응 에이전트(CA: Correspondent Agent) 개념을 도입한다. 대응 에이전트는 이동 노드와 통신하고자 하는 대응 노드(Correspondent Node)가 위치한 VPN 사이트에 연결된 PE 라우터 상에서 수행된다. 망사업자의 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. PE 라

우터 기반 MPLS VPN에서 CE 라우터는 PE 라우터와는 달리 VPN 서비스 및 이동 서비스에 대해 투명하게 동작한다. 그림 2는 네트워크 기반 MPLS VPN에서 노드의 이동 예를 보여준다.

3.1 동일 VPN 내의 사이트로 이동

그림 2의 예에서, 이동 노드가 이동을 인식할 수 있도록 PE_1 라우터에서 수행되는 외부 에이전트는 자신과 연결된 VPN 사이트마다 서로 다른 "ICMP Agent Advertisement" 메시지를 전송해야만 한다. 만일 PE_1 라우터에 다른 종류의 VPN들이 연결되어 있다면, "ICMP Agent Advertisement" 메시지에는 VPN 식별정보인 "VPN Information Extension"도 추가로 포함되어야 한다. 이 정보를 기반으로 이동 노드는 자신이 동일한 VPN으로 이동했는지 다른 VPN으로 이동했는지를 파악할 수 있게 된다. 예를 들어, 그림 2의 PE_1 라우터 상에서 수행되는 외부 에이전트가 자신과 연결된 두 개의 VPN 사이트로 동일한 "ICMP Agent Advertisement" 메시지를 전송하고 VPN A/site 1에 속해 있는 이동 노드가 VPN A/site 2로 이동한다면, 이동 노드는 자신이 이동했는지를 파악할 수 없게 된다. 이것은 이동 노드가 이동한 이후에도 PE_1 라우터에서 수행되는 외부 에이전트로부터 동일한 "ICMP Agent Advertisement" 메시지를 받기 때문이다.

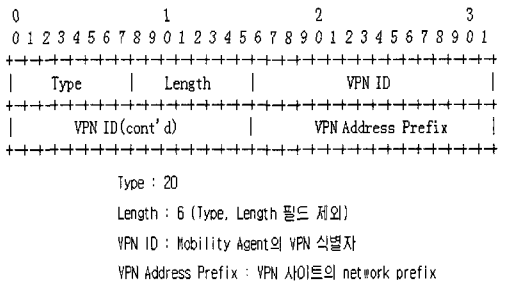


그림 3. ICMP Agent Advertisement 메시지 내의 VPN Information Extension

이동 노드가 다른 VPN의 사이트 내로 이동한 경우, 이동 노드는 "VPN Information Extension"을 이용하여 이동한 사이트 내의 주소 영역이 이동 노드와 동일한 주소 영역을 사용하는지를 알 수 있다. "VPN Information Extension"에는 VPN 식별자 및 VPN 사이트 관련 정보가 포함된다. "VPN Information Extension"의 완전한 구조는 그림 3과 같이 정의한다.

이동 노드가 이동을 확인한 이후의 등록 과정은 Mobile IP 프로토콜[6]과 유사하다. 그러나, 기존 Mobile IP 프로토콜의 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 이동했는지를 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.

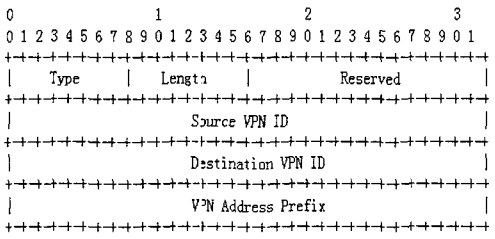
BGP-E 프로토콜을 사용하는 MPLS VPN 방식에서의 패킷 포워딩은 두 단계 레이블 스태킹에 의한 LSP 공유 메커니즘에 따라 수행된다. 고객 사이트로부터 CE를 통하여 VPN 데이터 패킷이 PE에 도착하면 PE에서는 그 고객 사이트에 해당하는 VRF(VPN Routing and Forwarding)를 참조한다. VRF에서 그 데이터 패킷에 대한 두개의 레이블과 다음 홉에 대한 정보가 포함되어 있다. 두개의 레이블 중 둘째 레이블은 앞에서 언급한 것처럼 BGP-E에 의해서 분배된 VPN 레이블이다.

3.1.1 등 록

이동한 이동 노드가 외부 에이전트로부터 위와 같은 "VPN Information Extension"이 포함된 "ICMP Agent Advertisement"메시지를 받으면 자신이 이동했음을 알게 되고 홈 에이전트에게 등록을 시도한다. 등록과정은 Mobile IP[6]의 과정을 따르지만 현재 방문한 VPN으로 패킷을 전달 할 수 있도록 하기 위하여 등록 메시지에 "VPN Information Extension" 이 추가되어 전송된다. 그림 4는 등록 요청 메시지에 추가적으로 확장되는 "VPN Information Extension"의 구조이다.

홈 에이전트는 이동 노드의 등록 요청을 받은 후, 등록 요청 메시지 내의 "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 저장한 후, 등록 응답을 이동 노드가 현재 위치해 있는 외부 에이전트에게 보낸다. 이 경우에도 Mobile IP에 정의된 등록 응답 메시지 외에 이동 노드가 등록 요청시 추가하였던 "VPN Information Extension" 과 동일한 확장이 추가된다. 등록 요청 메시지의 VPN 정보 확장과 등록 응답 메시지의 VPN 정보 확장은 "Type" 값만 다를 뿐 동일한 형태를 취한다.



Type : 55 (Registration Request VPN information extension)
56 (Registration Reply VPN informaion extension)
Length : 14
Source VPN ID : 이동노드의 홈 네트웍의 VPN 식별자
Destination VPN ID : 이동 노드가 이동하여 받은 AA내의 VPN 식별자
VPN Address Prefix : 이동 노드의 홈 네트웍의 VPN address prefix

그림 4. 등록 메시지 내의 VPN Information Extension

"Authentication Extension"은 Mobile IP에 정의된 것으로 구성되며 패킷의 무결성을 보호하기 위해 사용된다. 이동 노드가 등록 요청에 추가할 기본 확장은 Mobile IP에 정의된 것과 같은 순서를 따른다. 패킷의 무결성과 인증을 증명한 후에 홈 에이전트는 [6]에 정의된 등록 응답 메시지를 갖고 외부 에이전트에게 응답한다. 그런 다음 외부 에이전트는 등록 요청을 보낸 이동 노드에게 등록 응답을 반환한다.

3.1.2 핸드오버(Handover)

그림 2에서 이동 노드가 방문 사이트(VPN A/site 3)에서 다른 사이트(VPN A/site 4)로 다시 이동하는 경우를 고려하자.

이전 VPN 사이트에서 새로운 VPN 사이트로 이동한 이동 노드는 새로운 외부 에이전트(PE_3)를 통하여 앞서 기술된 것과 같은 등록 절차를 시작한다. 홈 에이전트는 새로운 외부 에이전트로부터 등록 요청을 받는다. 이 때, 홈 에이전트는 VPN A에 대해 이동 노드의 바인딩(Binding) 정보를 새로운 외부 에이전트에 의해 보내진 내용에 따라 변경한다.

이동 노드가 핸드오버를 실행할 때, 새로운 외부 에이전트에 의한 등록이 완료되지 않았다면, 이동 노드로의 패킷은 이전 외부 에이전트로 전해진다. 이 경우 패킷의 손실이 발생하며, 이러한 문제를 최소화하기 위해 외부 에이전트 사이에는 Smooth 핸드오버가 제공되어야한다. Smooth 핸드오버의 절차와 사용되는 메시지에 대한 내용은 3.5절에 기술된다.

3.2 다른 VPN 내의 사이트로 이동

그림 2에서 어떤 VPN(VPN A/site 2) 내에 속한 노드가 다른 VPN(VPN B/site 2)으로 이동한다면, 이동 노드는 방문한 VPN 사이트의 외부 에이전트(PE_2)로부터 "ICMP Agent Advertisement" 메시지를 수신하게 된다. 이 메시지를 통하여 이동 노드는 다른 VPN지역으로의 이동을 확인한다. "VPN Information Extension"이 추가된 "ICMP Agent Advertisement" 메시지를 수신한 이후에, 이동 노드는 이동한 사이트의 주소 영역이 자신의 주소 영역과 동일한 지를 검사한다. 동일하다면, "ICMP Agent Advertisement" 메시지에 포함된 외부 에이전트의 "Care-of-Address"를 사용하여 등록 절차를 수행할 수 없다. 왜냐하면 이동한 사이트 내에서 이동 노드와 같은 주소를 사용하는 노드가 존재하여 주소 충돌이 발생할 수 있기 때문이다. 이러한 경우, 이동 노드는 방문 사이트에서 "Co-located Care-of-Address"를 할당받은 후에 등록 절차를 수행한다. 만일 동일하지 않다면, 이동 노드는 "ICMP Agent Advertisement" 메시지에 포함된 외부 에이전트의 "Care-of-Address"를 사용하여 등록 절차를 수행한다. 따라서, 모든 VPN의 외부에이전트는 3.1절에 기술된 것처럼 "ICMP Agent Advertisement" 메시지에 "VPN Information Extension" 을 추가하여 전송한다. 이동 노드는 "VPN Information Extension"을 포함한 "ICMP Agent Advertisement" 메시지를 수신 한 후에, 외부 에이전트에 등록 요청 메시지를 전달한다.

VPN 간 이동에서도 등록 과정 동안에 교환된 모든 메시지를 인증하는 것이 요구된다. 그러나, 이동 에이전트가 수행되는 PE 라우터들은 동일한 망 사업자에서 관리되기 때문에, PE 라우터들 간에는

미리 구성된 보안 결합(Security Association)이 존재한다고 가정한다. 또한, VPN 간 이동에서는 이동 노드가 속한 VPN과 방문한 다른 VPN 사이에도 보안 결합이 존재한다고 가정한다.

3.3 일반 인터넷 지역으로 이동

일반 인터넷 지역으로 이동하는 경우에는 그 지역 라우터가 VPN 제공기능이 없으므로 "ICMP Agent Advertisement" 메시지에 "VPN Information Extension"을 추가하는 것이 불가능하다. 따라서, 이 경우에 이동 노드는 외부 에이전트로부터 추가적인 확장이 없는 "ICMP Agent Advertisement" 메시지만을 수신한다. 이동 노드는 기존의 VPN 서비스를 지속할 수는 없지만, 외부 에이전트를 통해 단순히 이동성만을 갖게 된다. 일반적으로, 사설 주소를 사용하게 되는 이동 노드는 방문 지역의 DHCP(dynamic Host Configuration Protocol) 서버를 통해 IP 주소를 할당받아야 한다. 따라서, 이동 노드는 "Co-located Care-of-Address"를 이용하여 직접 등록 절차를 수행할 것이다.

이동 확인 이후에, 이동 노드의 등록 과정은 3.1절의 내용과 동일하게 수행된다. 그렇지만, 등록 이후에, 이동 노드는 MPLS VPN 서비스를 제공받지 못하는 일반 노드로 동작할 것이다.

3.4 라우팅

그림 2의 예에서 VPN A/site 3에 있던 이동 노드가 VPN A/site 4로 이동하는 경우를 가정해 보자. 이 그림은 또한 VPN A/site 1에 있는 대응 노드가 VPN A/site 3에 있던 이동 노드로 데이터 패킷의 전달 과정을 보여준다.

우선, 이동 노드는 PE_3 라우터에서 수행되는 외부 에이전트 및 PE_2의 홈 에이전트를 통하여 등록 과정을 수행한다. 등록 과정이 끝난 이후, VPN A/site 1에 있는 대응 노드가 이동 노드에게 데이터를 전달하고자 한다. 먼저, 대응 노드가 전송한 패킷은 CE_{A1} 라우터를 거쳐 PE_1에게 전달된다. PE_1은 CE_{A1} 라우터로부터 수신된 패킷이 VPN A라는 것을 이미 알고 있다. PE_1은 수신된 패킷의 목적지 주소를 갖고 VPN A에 해당하는 VRF를 검색하여 이동 노드의 홈 네트워크 라우터인 PE_2에게 두 단계 스태킹된 레이블 패킷을 전달한다. 두 단계 레이블의 바깥(outer) 레이블은 PE_1과 PE_2 사이에 설정된 LSP를 의미하며, 안(inner) 레이블은 VPN 종류를 의미한다. VPN 종류를 의미하는 VPN 레이블은 PE_1의 VRF를 통해 얻어진다. PE_2에서는 패킷을 수신한 후, VPN A/site 3으로 패킷을 전달하기 이전에 VPN A/site 3에 있던 목적지 노드가 이동했는지를 검사한다. 이동 확인은 PE_2의 홈 에이전트에 의해 수행된다.

홈 에이전트는 각 VPN 별로 구성된 "Mobility Binding"에서 이동 노드의 정보를 추출한다. 홈 에이전트에 의해 목적지 노드가 PE_3으로 이동했다는 것을 파악한 후, PE_2는 PE_3으로 패킷을 전달한다. PE_3에서는 패킷을 수신하고, 외부 에이전트를 통해 목적지 노드가 어느 사이트로 이동했는지를 파악한다. PE_3은 외부 에이전트에서 관리하는 VPN A에 해당하는 "Visitor List" 정보에 따라 CE_{A4} 사이트 내에 목적지 노드가 존재함을 알게 된다. 그런 다음 PE_3은 CE_{A4}로 패킷을 전달한다. CE_{A4}는 수신된 패킷을 자신의 사이트로 방송(broadcasting)하고 이동 노드는 자신의 패킷을 수신한다.

이동 노드가 대응 노드로 응답 패킷을 전송하는 과정을 살펴보자. 우선 PE_3이 CE_{A4}로부터 패킷을 수신한다면, PE_3은 VPN A에 해당하는 VRF를 검색할 것이다. 그런 다음 수신된 패킷의 목적지 주소에 따라 PE_1으로 레이블 패킷을 전달한다. PE_1은 패킷을 수신한 후, CE_{A4}에게 전달한다. 그림 2에서 보듯이, 패킷 전달에서 삼각 라우팅(Triangle Routing) 현상이 발생한다. 삼각 라우팅은 Mobile IP 프로토콜의 문제점이며, 이것을 보완하기 위해 경로 최적화(Route Optimization) 방안[7]이 도입되었다. 본 연구에서도 경로 최적화 방안을 도입하여 삼각 라우팅 문제를 해결하고자 한다. 그 방법은 PE 라우터(예 : 그림 2의 PE_1)에 대응 에이전트(Correspondent Agent)를 두어 홈 에이전트로부터 "Binding Update" 메시지를 받아 이동 노드의 정보를 기록하는 것이다. 대응 노드에서 이동 노드로 전달되는 패킷은 PE 라우터 상에서 수행되는 대응 에이전트에 의해, 홈 에이전트로 전달되지 않고 직접 외부 에이전트로 전달된다. 따라서, 대응 노드는 Mobile IP 혹은 VPN에 무관하게 이동 노드로 데이터를 전달할 수 있다. 이러한 과정이 그림 5에 보여진다.

참고문헌 [7]의 경로 최적화 방안은 먼저, 홈 에이전트가 대응 노드에게 "Binding Update" 메

시지를 통해 이동 노드의 바인딩 정보를 전달한다. 그런 다음 대응 노드가 이동 노드의 바인딩 정보를 가지고 직접 이동 노드에게 패킷을 전달하는 것이다. 이것은 대응 노드가 VPN 서비스와 Mobile IP 서비스에 투명하게 동작하는 것을 방해한다.

따라서, 본 연구에서는 참고문헌 [8]에서 제안한 라우터에서 바인딩 정보를 유지하는 방식을 사용한다. 홈 에이전트는 대응 노드에게 "Binding Update" 메시지를 전달하는 것이 아니라, 대응 노드가 속한 VPN 사이트와 연결된 PE 라우터 즉, 대응 에이전트에게 전달하게 된다. 대응 에이전트는 라우팅을 변경하여 이동 노드가 속한 외부 에이전트로 미리 설정된 LSP 터널을 이용한다. 결국, 대응 노드는 이동 노드와의 통신에 있어 투명하게 동작한다. 경로 최적화 이후의 패킷 라우팅이 그림 5와 같이 이루어진다.

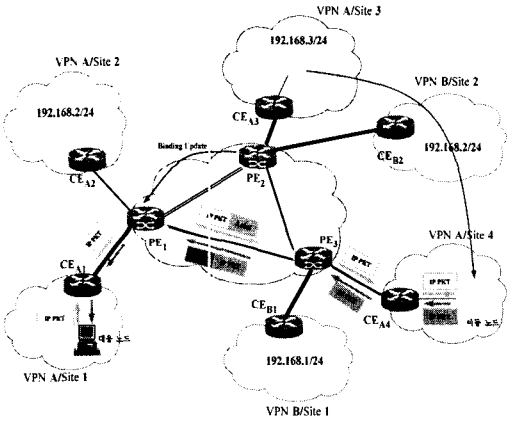


그림 5. 경로 최적화에서의 패킷 라우팅

3.5 Smooth 핸드오버

그림 6의 예처럼, 홈 VPN 사이트를 떠나 다른 사이트로 이동한 이동 노드가 다시 새로운 VPN 사이트로 이동한다면, 그 이동 노드는 새로운 외부 에이전트를 통하여 홈 에이전트로 등록을 요청한다. 그러나, 등록이 완료되기 이전에 홈 에이전트 혹은 이전 외부 에이전트로 보내진 패킷은 이동 노드로 전달되지 못하기 때문에 손실된다.

이런 문제점을 해결하기 위해 참고문헌 [6,7]에서는 이전 외부 에이전트에게 이동 노드의 새로운 바인딩 정보를 알려준다. 이렇게 함으로써, 이동 노드로 전송된 패킷은 이전 외부 에이전트가 새로운 외부 에이전트로 다시 전달(re-tunneling)한다.

이러한 과정은 우선, 이동 노드가 새로운 외부 에이전트에게 등록 요청을 전달하면, 새로운 외부 에이전트는 등록 요청 메시지를 이동 노드의 홈 에이전트로 보낸다. 그런 다음 등록 요청 메시지에서 추출한 정보를 기반으로 이전 외부 에이전트에게 "Binding Update" 메시지를 전달한다. 이전 외부 에이전트는 "Binding Update" 메시지를 받게 되면 새로운 외부 에이전트로 패킷을 터널링한다.

홈 에이전트는 등록 요청 메시지를 수신 후, 인증 절차 수행한다. 그런 다음 새로운 외부 에이전트로 등록 응답 메시지를 보낸다. 그러나 이 때, 홈 에이전트는 이동 노드와 통신을 하고 있는 대응 노드가 무엇인지 알지 못한다. 따라서, 대응 에이전트에게 이동 노드의 새로운 외부 에이전트의 주소를 알려주지 못하는 결과를 낳는다.

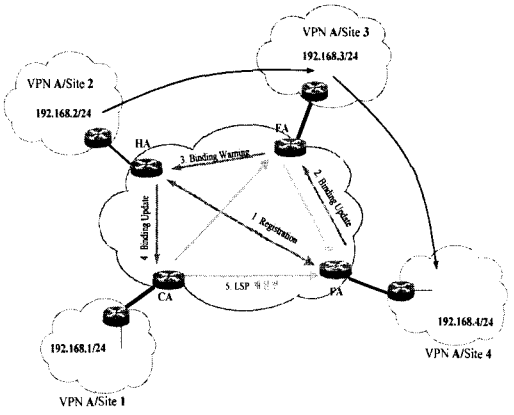


그림 6. Smooth 핸드오버

이러한 단점을 보완하기 위해, 이전 외부 에이전트는 새로운 외부 에이전트에게 "Binding Update" 메시지를 받은 후에, 홈 에이전트에게 "Binding Warning" 메시지를 전송한다. 이 메시지를 통해 홈 에이전트는 이동 노드와 통신을 하고 있는 대응 에이전트를 알 수 있게 된다. 홈 에이전트는 대응 에이전트에게 "Binding Update" 메시지를 전달하고, 대응 에이전트는 새로운 외부 에이전트로 LSP 터널을 설정한다. 이러한 과정이 그림 6에 보여진다.

라우팅 관점에서 살펴볼 때, 이동 노드와 통신을 지속하고자 하는 대응 노드가 속한 사이트의 대응 에이전트에서 이전 외부 에이전트로 설정된 LSP가 새로운 외부 에이전트까지 확장될 수도 있고,

이전 외부 에이전트로의 LSP 대신에 새로운 외부 에이전트로 LSP가 설정될 수도 있다.

Ⅳ. 구현 및 실험

본 연구에서는 MPLS VPN에 Mobile IP 프로토콜을 적용하기 위해 SUN의 Mobile IP 구현(version 1.2 beta)을 확장하였다. SUN의 Mobile IP 구현은 백본 네트워크를 IP 기반으로 하여 이동 에이전트 사이에 "IP in IP" 터널링 방식을 사용하고 있다. 그러나, 본 연구에서는 MPLS 네트워크를 사용하기 때문에, IP 기반의 터널링 방식이 아니라 MPLS의 고유 기능인 레이블 스태킹을 이용하여 두 단계 레이블 스태킹으로 LSP를 공유하는 터널링 방법을 사용하였다. 따라서, MPLS 라우터로 동작하는 PE 라우터는 리눅스 커널 2.4.x 버전의 MPLS 커널 패치(mpls-linux version 1.170)[13]를 이용하여 MPLS 기능을 수행하도록 C 언어를 이용하여 구현하였다.

4.1 이동성 지원을 위한 VPN 자료구조

각 이동 에이전트(홈 에이전트, 외부 에이전트, 대응 에이전트)들은 이동성 지원을 위해 VPN별로 구분된 자료구조를 가지며, 각 자료구조는 Linked List로 구성하여 레코드의 추가와 삭제 시에 동적으로 메모리를 사용하는 구조로 설계하였다. 홈 에이전트가 이동 노드의 등록 정보를 관리하는 "VPN Mobility Binding" 테이블 및 구조체가그림 7과 그림 8에 보여진다. 홈 에이전트가 관리하는 "VPN Mobility Binding" 에는 이동 노드의 홈 주소, "Care of Address", 근원지 VPN 식별자, 목적지 VPN 식별자가 포함된다. PE 라우터 상에서 수행되는 홈 에이전트는 자신과 연결된 VPN 수만큼의 바인딩 테이블을 유지한다.

VPN C

MN's Home Address	MN's Care of Address	Source VPN ID	Destination VPN ID

VPN B

MN's Home Address	MN's Care of Address	Source VPN ID	Destination VPN ID

VPN A

MN's Home Address	MN's Care of Address	Source VPN ID	Destination VPN ID
192.168.2.2	168.188.20.1	A	A
192.168.2.3	202.188.20.1	A	B
192.168.2.4	211.149.52.1	A	C

그림 7. 홈 에이전트의 VPN 바인딩 구성

```
struct KHABE{
        int srcVPN;
        unsigned int MnHomeAddr;
        unsigned int COA;
        int dstVPN;
        struct KHABE *next;
};
```

그림 8. 홈 에이전트 VPN 바인딩 구조체

외부 에이전트는 자신과 연결된 VPN 사이트 내에 방문하는 이동 노드에 대한 정보를 관리하기 위해 VPN 방문자 리스트를 구성한다. VPN 방문자 리스트에는 근원지 VPN 식별자, 이동 노드 홈 주소, HA 주소, "Care of Address", 인터페이스 식별자가 포함된다. 그림 9과 그림 10에 외부 에이전트 VPN 방문자 리스트 구성 형태와 자료구조를 보였다.

VPN C

Source VPN ID	MN's Home Address	MN's HA Address	MN's Care of Address	Interface Number

VPN B

Source VPN ID	MN's Home Address	MN's HA Address	MN's Care of Address	Interface Number

VPN A

Source VPN ID	MN's Home Address	MN's HA Address	MN's Care of Address	Interface Number
A	192.168.2.2	168.188.10.1	168.188.20.1	1
A	192.168.2.5	168.188.10.1	168.188.20.1	1
C	192.168.5.7	168.188.32.1	168.188.20.1	2

그림 9. 외부 에이전트의 VPN 방문자 리스트 구성

```
struct KFAVE {
        int srcVPN;
        unsigned int VisitorAddr;
        unsigned int VisitorHomeAddr;
        unsigned int VisitorCOAddr;
        int IfaceNo;
        struct KFAVE *next;
};
```

그림 10. 외부 에이전트 VPN 방문자 리스트 구조체

대응 에이전트는 자신과 연결된 VPN 사이트 내의 대응 노드와 통신하는 이동 노드에 대한 이동 정보를 관리하기 위해 바인딩 캐쉬를 구성한다. VPN 바인딩 캐쉬에는 이동 노드 홈 주소, Care of Address, 목적지 VPN 식별자가 포함된다. 그림 11과 그림 12는 대응 에이전트 VPN 바인딩 캐쉬 구성과 구조체 형식이다.

VPN C

MN's Home Address	MN's Care of Address	Destination VPN ID
192.168.2.2	168.188.10.1	A
192.168.2.3	202.188.10.1	B
192.168.2.4	211.149.12.1	C

VPN B

MN's Home Address	MN's Care of Address	Destination VPN ID

VPN A

MN's Home Address	MN's Care of Address	Destination VPN ID

그림 11. 대응 에이전트 VPN 바인딩 캐시 구성

```
struct KBC {
        unsigned int MnHomeAddress;
        unsigned int COAddress;
        unsigned int DstVPN;
        struct KBC *next;
};
```

그림 12. 대응 에이전트 VPN 바인딩 캐쉬 구조체

4.2 실험 결과 및 분석

그림 13은 본 논문에서 제안한 방식의 시범 구현을 위해 구성한 실험 환경이다. LDP를 이용하여 PE 라우터 사이에 설정된 LSP가 보여진다. 각 PE 라우터는 LER(Label Edge Router)로서 MPLS VPN 서비스뿐만 아니라 이동 에이전트(HA, FA, CA)의 역할을 수행하게 된다. LSR 역할을 담당하는 P 라우터는 홈 에이전트와 외부 에이전트간의 패킷 전송 시 레이블 스와핑을 수행하며, 리눅스 시스템 상에서 동작한다. 홈 에이전트와 외부 에이전트는 각각 두 개의 VPN 사이트를 갖도록 구성하였고, 이동 노드가 동일 VPN 내 다른 사이트로 이동하는 경우 및 다른 VPN의 다른 사이트로 이동하는 경우를 대상으로 실험하였다.

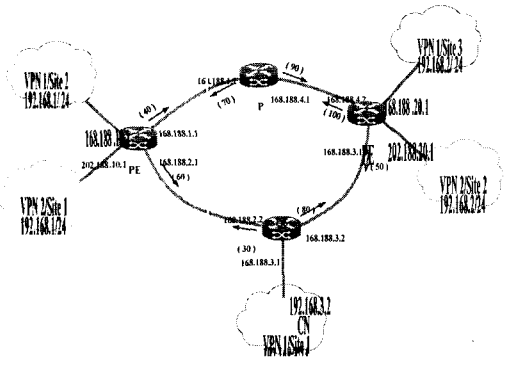


그림 13. 실험환경 및 레이블 분배 과정

그림 14는 대응 노드(CN)에서 "ping" 프로그램을 이용하여 이동 노드(MN)에게 패킷을 전송하고 이동 노드는 패킷 수신 후, 응답 패킷을 전송하는 것을 보여준다. 대응 노드가 이동 노드의 이전 위치로 패킷을 전달하지만, 홈 에이전트에서 이동 노드의 현재 위치로 LSP를 확장하여 패킷을 전달한다. 그런 다음, 대응 에이전트에게 이동 노드의 현재 위치를 "Binding Update" 메시지를 이용하여 알려주고, 대응 에이전트는 이동 노드가 속한 사이트의 PE(FA) 라우터 즉, 외부 에이전트로 패킷을 직접 전송한다. 이동 노드는 패킷 수신 후, 송신 주소를 목적 주소로 하여 응답 패킷을 전송한다. 경로 최적화 이후에, PE(CA)와 PE(FA) 사이에 전달되는 2단계 MPLS 레이블 패킷이 보여진다. 2단계 레이블 패킷의 바깥쪽 레이블은 PE 라우터 사이의 LSP를 의미하며, 안쪽 레이블은 VPN 식별자를 의미한다.

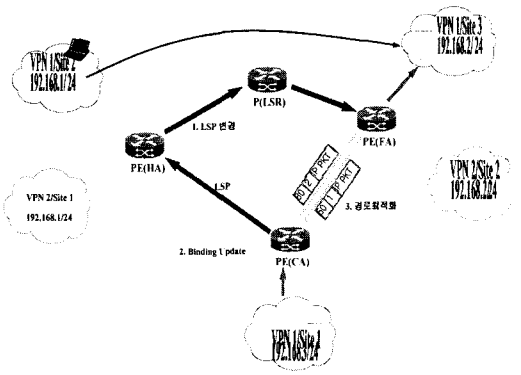


그림 14. 경로 최적화 이후의 패킷 라우팅

본 연구에서 제안한 이동성 지원 방식을 MPLS VPN에 적용한 경우, 대응 노드에서 이동 노드로 전송된 데이터 패킷의 손실률과 대응 노드를 기준으로 이동 노드로부터 반환되는 RTT(Round Trip Time)를 측정하였다. 네트워크 내에서 전송도중 메시지의 손실은 없고, 가입자 네트워크에서의 전송 지연과 사업자 네트워에서의 전송 지연은 실험 결과의 평균값으로서 각각 0.022, 0.05초로 가정하였다. 또한, 대응 노드는 이동 노드에게 데이터를 전송하기 위해 "ping" 프로그램을 이용하여 전송하며, ICMP ping 패킷은 3초 간격으로 전송된다.

MPLS VPN에서 이동 노드의 등록과정에 가장 큰 영향을 미치는 요소는 외부 에이전트로부터 주기적으로 전송되는 "ICMP Agent Advertisement" 메시지이다. 표 1은 "ICMP

Agent Advertisement" 메시지의 전송 간격이 증가함에 따라 대응 노드에서 이동 노드로 전송한 패킷의 손실률을 보여준다. 이 메시지의 전송 간격이 길어짐에 따라 이동 노드에서 수신되는 패킷의 손실이 증가함을 알 수 있다. 이동 노드는 외부 에이전트의 "ICMP Agent Advertisement" 메시지를 이용하여 이동을 인식하고 등록을 수행하기 때문에, 이 메시지의 전송 간격이 짧을수록 더 빠른 등록 과정이 이루어진다. 이동 후에 신속한 등록 과정은 이동 노드로 전송되는 패킷의 손실을 줄일 것이다.

표 1. ICMP AA 메시지 전송 간격에 따른 이동 노드의 패킷 손실율

	3sec	6sec	9sec	15sec	20sec	25sec
패킷 손실율	5.4 %	6.6 %	9.6 %	12.1 %	17.2 %	22.5 %

표 2는 이동 노드가 핸드오프에 소요된 시간 간격이 증가함에 따라 대응 노드에서 이동 노드로 전송한 패킷의 손실률을 보여준다. 이동 노드가 VPN 사이트에서 다른 VPN 사이트로 이동하는데 걸리는 시간이 증가함에 따라 대응 노드에서 이동 노드로 전송되는 패킷의 손실이 증가하게 된다. 이러한 핸드오프에 소요되는 시간은 이동 노드가 어떠한 VPN 서비스도 받을 수 없는 상태이기 때문이다. 무선랜이나 셀룰러 네트워크와 결합된 VPN 환경에서는 이러한 요인에 의한 패킷 손실률은 상당히 감소할 것이다.

표 2. 이동 노드의 핸드오프 시간 간격에 따른 패킷 손실율

	3sec	5sec	10sec	15sec
패킷 손실율	6.3%	7.9%	13.7%	17.9%

그림 15는 이동노드(MN)가 홈 VPN 사이트에서 이동하기 이전의 경우(HA-MN), 외부 사이트로 이동한 경우(HA-FA-MN), 그리고 외부 사이트에서 다시 이동한 경우(HA-FA-FA-MN)에, 대응 노드에서 이동 노드로 전송된 "ping" 패킷이 다시 이동 노드에서 대응 노드로 수신될 때까지 소요된 RTT(Round Trip Time)를 보여준다. 위 3가지는 삼각 라우팅 방식을 사용하는 경우와 경로 최적화 라우팅을 사용하는 경우로 구분하여 측정하였다. 경로 최적화 라우팅에서는 초기 패킷들은 홈 에이전트를 경유하여 이동 노드로 전송되지만, 그 이후의 패킷들은 대응 에이전트로 전송된 바인딩 갱신 메시지에 의해 직접 이동 노드로 전송된다. 따라서, 삼각 라우팅에 비해 경로 최적화 라우팅은 대응 노드로부터 전송된 패킷을 다시 대응 노드가 수신할 때까지 소요된 시간을 크게 줄일 수 있게 된다.

그러나, 본 논문에서 제안된 PE 라우터 기반의 이동 서비스 지원 방식과 참고문헌 [9]에서 제안된 CE 라우터 기반의 이동 서비스 지원 방식의 성능 비교는 [9]에서 수행한 시뮬레이션 결과를 참고할 때, CE 라우터 기반의 이동 서비스 방식이 약간 우수함을 알 수 있다.

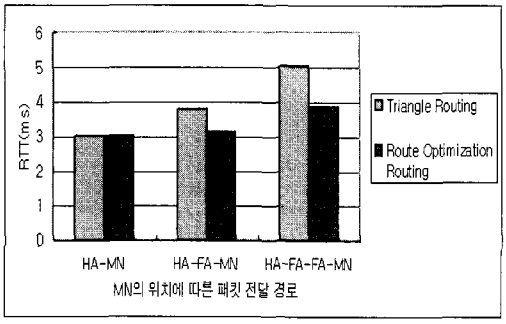


그림 15. 삼각 라우팅과 경로 최적화 라우팅에서의 RTT 비교

V. 결 론

본 논문에서는 VPN 사이트 내의 어떤 노드가 같은 VPN 내의 다른 장소로 이동하는 경우와 다른 VPN 내의 장소로 이동하는 경우, 그리고 일반 인터넷 지역으로 이동하는 경우 모두 VPN 서비스를 지속하게 하는 이동성 지원 프로토콜을 제시하였다. 이를 위해, 인터넷에서 이동성 서비스를 제공하는 Mobile IPv4 및 경로 최적화 프로토콜을 확장하였고, MPLS VPN 서비스 기능을 제공하는 PE 라우터가 이동 엔티티의 기능을 수행하며, 이동 엔티티들을 통하여 이동 서비스를 제공할 수 있도록 MPLS VPN 라우터를 구현하였다.

특히, 실험 환경에서 구현 결과를 기반으로 VPN 노드에 대한 이동 서비스 지원을 실제 확인하였고, VPN 노드의 이동에 따라 이동 노드로 전송되는 패킷의 손실률과 RTT를 측정하였다. 이러

한 결과들은 향후 네트워크 사업자가 MPLS VPN 네트워크에서 이동 서비스를 지원하고자 하는 경우에 기초 자료로서 활용될 수 있을 것이다.

다른 VPN으로 이동하는 경우, 이동 노드의 인증과 권한 검증을 위해 VPN 사이에 보안 결합이 제공되어야 하며, 이것은 VPN 간에 미리 설정된 보안 결합을 요구한다. 그러나, VPN 사이에 미리 설정된 보안 결합이 없는 경우, 이동 노드의 인증과 권한 검증을 위해 기존 "Internet Key Exchange" 프로토콜[14]을 이용하는 방안이 고려될 수 있다.

이 외에도, MPLS 네트워크뿐만 아니라 ATM과 IP 등과 같은 다른 네트워크에서 VPN을 구성하여 이동 서비스를 제공하는 경우, 본 논문에서 제안된 방식의 적용성과 연동 시의 문제점을 연구할 필요가 있다.

참 고 문 헌

[1] Paul Ferguson, Geoff Huston, "What is VPN," The Internet Protocol Journal, Volume 1, Number 2, June 1998.

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

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

[4] Loa Anderssor., et al., "LDP Specification," IETF RFC 3036, Jan. 2001.

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

[6] Charles Perkins, "IP Mobility Support for IPv4," IETF RFC 3344, Jan. 2002.

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

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

[9] 이영석, 최 훈, "이동성 지원을 고려한 MPLS 방식 가상사설망", 한국통신학회 논문지, Vol. 26, No. 12C, pp. 225-232, 2001.12.

[10] Zhong Ren, et al., "Integration of Mobile IP and Multi-Protocol Label Switching,"The International Computer Congress 2001, Hong Kong, Nov. 2001.

[11] H. Ould-Brahim and B. Gleeson, "Network based IP VPN Architecture Using Virtual Router,"IETF Draft, Mar. 2000.

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

[13] http://www.sourceforge.net

[14] D. Harkins, D. Carrel, "The Internet Key Exchange," IETF RFC2409, Nov. 1998.

이 영 석(Young-Seok Lee) 정회원

1992년 2월 : 충남대학교 컴퓨터공학과 학사

1994년 2월 : 충남대학교 컴퓨터공학과 석사

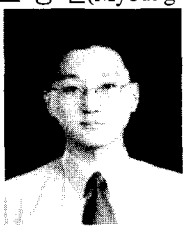
2002년 2월 :충남대학교 컴퓨터공학과 박사

1994년~1997년 : LG전자 연구원

2002년~현재 : 한국전자통신연구원 선임연구원

<주관심분야> 분산시스템, 가상사설망, 이동컴퓨팅

오 명 환(Myoung-Hwan Oh) 준회원

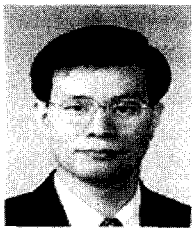


2002년 2월 : 충남대학교 컴퓨터공학과 학사

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