이동성 지원을 위한 MPLS VPN 에서의 Smooth Hand-off 의 설계 및 구현

임형택 0*, 오명환*, 이영석**, 최 훈*
*충남대학교 컴퓨터공학과
** 한국전자통신연구원
e-mail : {htlim,mhoh, hchoi}@ce.cnu.ac.kr, yslee@etri.re.kr

The Smooth Hand-off Scheme on MPLS-VPN

Hyoung-Taek Lim 0*,Myoung-Hwan Oh*, Young-suk Lee**, Hoon Choi*
*Dept. of Computer Engineering, Chungnam National University
** Electronics and Telecommunications Research Institute

요 약

많은 기업들이 사설망과 같은 수준의 기능을 제공하면서 사설망에 비해 매우 경제적인 VPN 을 기업 네트웍의 인프라로 채택하고 있다. VPN 을 구성하는데 있어 우수한 QoS 나 보안 기능을 제공하는 MPLS VPN 이 VPN 을 구성하기 위한 최적의 방법으로 간주되고 있다. 또한 모바일 컴퓨팅의 보편화와 이동 환경에서의 인터넷 서비스에 대한 요구의 증가로 VPN 에서도 이동 인터넷 서비스를 제공할 필요가 있게 되었다. 본 논문에서는 IP 의 이동성을 제공하는 Mobile IP 와 MPLS VPN 을 결합하여 VPN 이용자에게 이동 인터넷 서비스를 제공하는 방법을 설명하고 이동 노드의 핸드오프시 발생하는 패킷 손실을 최소하기 위해 Smooth handoff 를 지원하는 MPLS VPN 을 Linux 에서 구현하고 테스트를 수행하였다.

1. 서론

최근 기업별로 자신의 정보를 안전하게 전송하기 위하여 사설망(private network)을 구성해야 할 필요성이 대두되었다. 그러나 이러한 사설망은 초기 네트웍 구성에 막대한 시설 투자비용이 요구되고 네트웍 운영과 관리적인 측면에서 많은 소요 인원과 경제적 부담이 따르는 문제점으로 인해 기업은 VPN(Virtual Private Network)에 많은 관심을 가지게 되었다.

VPN 은 보안성, 신뢰성, 관리 편이성, 사설주소 지원, 정보 전달 성능 등에서 사설망과 같은 수준의 기능을 제공하면서도 사설망에 비해 매우 경제적이다[1]. VPN 을 구축하는 방안으로는 IP(Internet Protocol) 터널링 방식과 MPLS(Multi-Protocol Label Switching)를 이용한 방식이 있다. MPLS 기반의 VPN 은 IP 터널링 기반의 VPN 에서 제공하기 어려운 QoS(Quality of Service)나 보안등을 제공할 수 있다는 장점이 있고, LSP(Label Switched Path) 공유를 통한 높은 확장성, 효과적인 비용, 그리고 사용자 요구의 광범위한 핸들링을 제공하여 IP 서비스를 낮은 비용으로 제공해 준다[2][3]. MPLS 는 이와 같은 이점을 바탕으로 VPN 을 구성하기 위한 최적의 방안으로 간주되고 있으며, IETF(Internet Engineering Task Force)에서는 MPLS VPN 을 표준화하고 있고 RFC2547 "BGP/MPLS VPN"이 MPLS VPN 의 표준으로 정립되고 있다[4].

한편 모바일 컴퓨팅의 보편화와 이동 환경에서의 인터넷 서비스에 대한 요구가 증가하면서 VPN 에서도 이동 인터넷 서비스를 제공할 필요가 있게 되었다. 이를 위해 IP 의 이동성을 제공하는 Mobile IP 의 지원과 MPLS 의 2 계층 터널링을 사용해 VPN 이용자가 이동하는 경우에도 위치에 구애받지 않고 지속적으로(seamless) VPN 서비스를 제공 받을 수 있다.

본 논문에서는 MPLS-VPN 을 구성하는 방안 가운데 PE(Provider Edge) 라우터에 기반한 MPLS VPN 을 대상으로 VPN 노드에게 이동 인터넷 서비스를 제공함으로써 VPN 사이트에 속하는 어떤 노드가 기존의 통신을 유지한 상태로 다른 사이트로 이동하더라도 계속적으로 VPN 서비스를 제공받을 수 있는 모바일 MPLS-VPN 모델을 소개하고 더 나아가 VPN 노드의 핸드오프시 발생할 수 있는 많은 패킷 손실을 최소화 하기 위해 Smooth Handoff 를 지원하는 모바일 MPLS VPN 모델을 제시한다.

본 논문은 다음과 같이 구성되어 있다. 2 장에서는 본 연구에서 구현한 이동성 지원을 위한 MPLS VPN 에 대해 설명하며 3 장에서는 Smooth Handoff 를 지원하는 모바일 MPLS VPN 의 구현에 대해 기술하고 4 장에서는 결론을 맺는다.

2. 이동성 지원을 위한 MPLS-VPN

2.1 VRF 의 구현

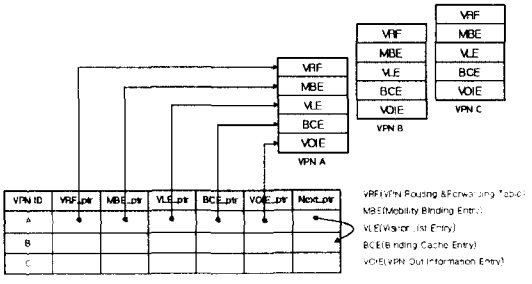
PE 라우터는 VPN 서비스를 제공하기 위해 [그림 1]과 같이 각 VPN 그룹별로 분리된 VRF(VPN Routing & Forwarding Table)를 유지하고 각 VRF 에는 로컬 및 원격의 VPN 사이트에 대한 경로 정보를 저장하였다. 이러한 VPN 라우팅 정보는 PE 들 간의 BGP 세션에 의해 분배된다[5][6].

o 본 연구는 충남대학교 소프트웨어 연구센터의 부분 지원을 받았음.

Type	Site	Intf	PE address	CE address	VPN FEC
Local	1	1	168.188.1.1	168.188.1.5	202.188.1.x
Remote	2	x	168.189.2.1	168.189.2.9	202.188.2.x
Remote	3	x	168.190.3.1	168.190.3.4	202.188.3.x

[그림 1] VRF(VPN Routing & Fowarding Table)

Type 필드는 자신과 *stub link* 로 연결되어 있는 CE(Customer Edge) 라우터로부터 위치 정보를 받았을 경우와 이웃 PE 라우터로부터 받았을 경우에 따라 "Local" 이나 "Remote" 값이 저장되고 Site 필드는 동일 VPN 그룹의 분산된 사이트를 나타낸다. Intf 필드는 Type 값이 "Local" 일 경우에 CE 라우터로 나가기 위한 출력 interface 번호를 나타낸다. PE address 와 CE address 필드는 VPN FEC(Forwarding Equivalence Classes)에 해당하는 VPN 사이트에 도달하기 위한 PE 라우터와 CE 라우터의 IP 주소가 들어가며 VPN FEC 필드에는 도달 정보의 FEC 가 들어간다[7][8].



[그림 2] VPN 인덱스 테이블

[그림 2]는 VPN 인덱스 테이블의 구성이다. VPN 그룹별로 VPN 서비스를 제공하기 위해 VPN 라우팅 테이블인 VRF 와 IP 이동성 지원 기술인 Mobile IP[9][10]의 이동성 바인딩 엔트리, 방문자 리스트 엔트리, 바인딩 캐쉬 엔트리 그리고 Egress PE 라우터에서 인접 CE 라우터로 패킷을 전송하기 위한 VPN 출력 정보가 저장되어 있는 VPN Out Information Entry 를 가리키는 하나의 VPN 인덱스 테이블을 구현하였다.

2.2 동작 절차

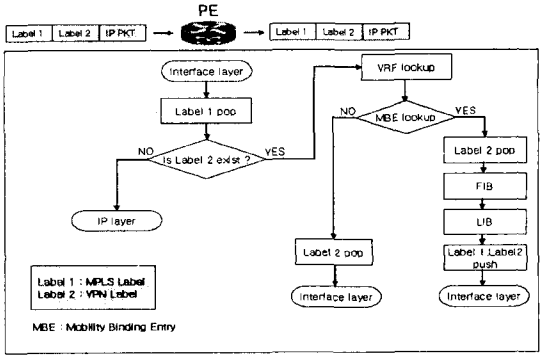
PE 라우터는 VPN 노드에게 이동 인터넷 서비스를 제공하기 위해 VPN 을 고려하여 확장된 Mobile IP 의 이동성 에이전트의 지원을 받는다.

다음은 외부 네트웍으로 이동한 VPN 노드에게 패킷을 전달하는 PE 라우터의 동작 과정이다.

① CE 라우터로부터 패킷이 유입되면 PE 라우터는 인터페이스 정보에 따라 VPN 을 식별하고 해당 VRF 를 결정한 후 VRF 에서 목적지 주소와 일치하는 VPN FEC 의 존재 여부를 검사한다. 만일 VPN FEC 가 존재한다면 이동 VPN 노드에게 도달하기 위한 PE address 을 획득하여 이 PE address 에 대해 맵핑 되어있는 FIB(Forwarding Information Base)와 LIB(Label Information Base)를 참조하여 백본 LSP 를 위한 외부 레이블(MPLS Label) 과 Egress PE 라우터에서 출력 인터페이스를 구분하기 위한 내부 레이블(VPN label)을 2-레벨 스태킹으로 추가하여 다음 홉으로 전송한다.

② 다음의 코어 라우터는 외부 레이블만으로 패킷을 스위치하며 VPN 에 투명하게 동작한다.

③ VPN 이동 노드의 홈 네트웍인 Egress PE 라우터에 패킷이 유입되면 PE 라우터는 외부 레이블(MPLS Lable)을 제거하고 내부 레이블(VPN Label)로 VRF 를 결정해 룩업을 한다. 룩업을 통해 알아낸 Type 은 "Local"이고 목적 노드의 이동을 판별하기 위해 이동성 바인딩 엔트리를 참조하게 된다. 이동성 바인딩 엔트리에서 목적지 주소와 일치하는 엔트리가 존재한다면 PE 라우터는 이동성 바인딩 엔트리의 외부 에이전트의 주소와 이동한 VPN 사이트의 VPN ID 에 따라 외부 레이블과 내부 레이블을 추가하여 2 계층 터널링 과정을 수행하게 된다. [그림 3]은 HA 역할을 수행 하는 Egress PE 라우터의 동작 절차에 대한 흐름도이다.



[그림 3] PE(HA) 라우터의 흐름도

④ 패킷이 2 계층 터널링으로 터널링되어 외부 에이전트인 Egress PE 라우터에 도착하게 되면 MPLS 계층에서 VRF 와 방문자 리스트 엔트리를 참조하여 방문자 리스트의 출력 interface 로 목적 노드에게 패킷을 전달한다.

3. Smooth Hand-off

VPN 이동 노드가 외부 망으로 이동하여 서비스를 받던 도중 다시 임의의 다른 망으로 이동하였을 경우, 호스트가 위치 변경을 감지하기 위한 지연이 존재하게 되고 감지 후 새로운 CoA(Care of Address)를 획득하여 바인딩 업데이트가 일어나 정상적으로 서비스를 받게 되기까지 기간, 즉 handoff 동안에 VPN 이동 노드로 패킷을 보내는 CN(Correspondent Node)은 이동 노드가 아직 이전의 외부 망에 있는 것으로 인식하기 때문에 패킷을 이전의 외부 망으로 전송한다. 이 때 이전의 외부 에이전트가 이 패킷들을 버리지 않고 VPN 이동 노드까지 전송해 주어 패킷 손실을 줄이는 것이 Smooth handoff 이다. 그렇게 하기 위해서 Route Optimization in Mobile IP[11] 에서와 같이 이전의 외부 에이전트로 BU(Binding Update)를 전송하여 이전 외부에이전트가 임시의 홈 에이전트 역할을 수행하도록 한다.

3.1 바인딩 캐쉬 엔트리 (Binding Cache Entry)

바인딩 캐쉬는 VPN 이동 노드의 홈 주소와 CoA 사이의 연결 관계 즉, 이동성 결합을 위한 정보로서 CoA 로의 2 계층 터널링을 위해 사용된다. 본 연구에서 구현한 바인딩 캐쉬 엔트리는 VPN 을 고려하여 아래 [그림 4]와 같이 설계하였다.

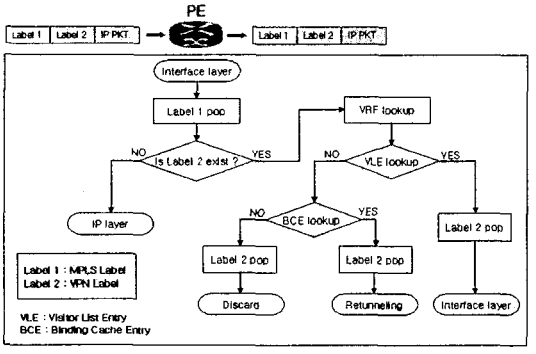
MN Address	COA	Dst VPN ID

[그림 4] 바인딩 캐쉬 엔트리의 구조

새로운 외부 에이전트는 BU 메시지에 Binding Update VPN extension 을 추가로 확장하여 이동 노드에 대한 VPN 정보까지 알려준다. VPN 정보에는 이동 노드가 속한 VPN 의 VPN ID(Src VPN ID)와 노드가 이동한 VPN 사이트의 VPN ID(Dst VPN ID)를 포함한다. 이전 외부 에이전트는 Src VPN ID 를 인덱스로 VPN 별로 구분된 바인딩 캐쉬 엔트리를 결정한 후 이동 노드의 바인딩 정보를 바인딩 캐쉬에 기록한다. [그림 4]의 Dst VPN ID 는 VPN 이동 노드가 이동한 VPN 사이트를 나타내고 IP 패킷에 부착되는 내부 레이블(VPN Label)로 사용된다.

3.2 동작 절차

VPN 이동 노드가 핸드오프 한 경우 이전의 외부 에이전트는 자신의 방문자 리스트에서 VPN 이동 노드의 엔트리를 삭제한다. 새로운 외부 에이전트는 이전의 외부 에이전트에게 VPN 이동 노드의 새로운 바인딩 정보를 BU 메시지에 실어 전송한다. [그림 5]는 Smooth handoff 를 지원하는 PE 라우터의 동작 절차에 대한 흐름도이다.



[그림 5] Smooth Handoff 를 위한 PE 라우터의 흐름도

홈 에이전트로부터 이전의 외부 에이전트인 PE 라우터에 유입된 패킷에 대해 PE 라우터는 내부 레이블(VPN Label)로 VRF 를 결정하고 룩업을 수행한다. 룩업한 결과 Type 필드 값은 "Remote" 이고 이때 해당 VPN 그룹의 방문자 리스트 엔트리를 참조 한다. 그러나 방문자 리스트에는 VPN 이동 노드의 엔트리가 존재하지 않게 되고 Smooth handoff 동작을 위해 새로운 외부 에이전트에게 받은 바인딩 정보를 참조한다. 바인딩 캐쉬에 목적 노드에 대한 엔트리가 존재하면 바인딩 정보에 따라 2 계층 터널링을 수행하게 된다. 터널링은 Ingress PE 와 마찬가지로 출력 인터페이스를 구분하기 위한 내부 레이블을 부착하고 새로운 외부 에이전트 주소인 CoA 에 대해 미리 설정된 레이블 교환 경로로 터널링하여 패킷을 전송하게 된다.

본 논문에서 제시한 Smooth handoff 를 테스트하기 위해 Linux 머신으로 테스트 베드를 구성하고 MPLS VPN 과 확장된 Mobile IP 를 연동하여 테스트를 수행하였다.

구현 환경: Linux Kernel Version - 2.4.12
구현 언어: C 언어
Code Size : 148 Kbyte

4. 결론

본 논문에서는 MPLS 망에서 VPN 을 구성하기 위한 구조적 모델과 MPLS 프로토콜 상에 Mobile IP 를 연동시켜 VPN 이용자에게 이동 인터넷 서비스를 제공하는 메커니즘을 제시하였다. 또한 이동 환경에서 향후 멀티미디어 서비스나 실시간 서비스 등에 필요한 QoS 를 보장하기 위해 이용자의 핸드오프 시 발생할 수 있는 패킷 손실을 최소화 하는 Smooth handoff 를 PE 라우터에 설계하고 구현하였다. 본 연구 결과가 MPLS VPN 의 활성화에 기여할 것으로 기대한다.

참고 문헌

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

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

[3] Eric Rosen, Arun Viswanathan, Ross Callon, "Multiprotocol Label Switching Architecture", RFC 3031, Jan. 2001.

[4] Eric Rosen and Y.Pekhter, "BGP/MPLS VPNs," RFC2547, Mar. 1999.

[5] T.Bates, R. Chandra, D. Katz, Y. Pekhter, "Multi-protocol Extention for BGP-4," RFC2283, Feb. 1998.

[6] Y.Pekhter and T. Li, "A Border Gateway Protocol 4(BGP-4)," RFC1771, Mar. 1995.

[7] 한민호, 이영석, 최 훈, 전우직, "CE 라우터기반 MPLS VPN 설계 및 구현", 제 27 회 한국정보과학회 추계학술대회, Vol. 21, No. 2, pp.251-253, 2000 년 10 월.

[8] 임형택, 이영석, 최 훈 "이동성 지원을 위한 MPLS VPN 의 설계 및 구현", 한국 통신학회 추계 종합 학술발표 논문 초록집 vol.26 p.88, Nov. 2002

[9] Charles Perkins, "Mobile IP," IEEE Communications Magazine, May 1997.

[10] Charles Perkins, "IP Mobility Support", Proposed Standard, RFC 2002, Oct. 1996.

[11] Charles Perkins, David Johnson, "Route Optimization in Mobile IP", Internet-Draft, Nov. 2000.