제 19 회 한국정보처리학회 춘계학술발표대회 논문집 제 10 권 제 1 호 (2003. 5)

MPLS VPN 에서의 이동성 지원에 관한 연구

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

A Study on mobility support on MPLS VPN

Myounghwan Oh*, Hyoungteak Lim*, Youngseok Lee**, Hoon Choi*
*Dept. of Computer Engineering, ChungNam National University
**Electronics and Telecommunications Research Institute

요 약

인터넷 서비스의 발전에 따라 보안성이 높고 경제적인 VPN 의 필요성이 대두되었다. 여러 방식의 VPN 구성 방법중 향후 멀티미디어 실시간 서비스 등에 필요한 QoS 및 트래픽 엔지니어링에 장점을 갖는 MPLS 기반의 VPN 기술이 활발히 논의되고 있으며 현재 BGP/MPLS VPN 이 표준으로 정립되고 있다. 본 연구팀은 현재 활성화 되고 있는 Mobile computing 기술과 이러한 VPN 기술을 접목시켜 MPLS VPN 망에서의 이동성을 지원을 위한 방안을 제시 및 구현한 바 있으며 본 연구에서 기제안한 방식에서 추가적으로 고려해줘야 할 문제점 및 해결방안에 대해 연구하였다.

1. 서론

근래 인터넷 서비스의 획기적 발전은 서비스 영역의 확장을 불러왔고 기업들은 이러한 추세에 맞추어 초기 망 구성 비용 및 기업정보 전송에 따르는 보안성 측면을 고려한 가상 사설망[1]을 구성하게 되었다. 현재까지 제안된 가상사설망의 구성을 위한 여러 방식들 중 향후 멀티미디어 실시간 전송등에 적합한 QoS 및 보안측면에서 많은 장점을 갖는 MPLS(Multi Protocol Label Switching)[3]가 새로운 VPN 기반 기술로 활발히 논의되고 있다. 한편 이동 컴퓨팅의 보편화와 함께, VPN 도 VPN 이용자가 이동하는 경우에 위치에 구애 받지 않고 지속적인 서비스를 제공할 필요가 있다. 이에 따라 본 연구팀은 기존의 Mobile IP[7]를 확장하여 MPLS 기반 VPN 에서 VPN 이용자 노드가 이동하더라도 지속적으로 VPN 서비스를 받을 수 있는 방안을 제시하고 구현한 바 있다[9][10].

인터넷상의 일반 노드의 이동성 지원을 위한 Mobile IP 와는 달리 VPN 하에서 노드의 이동성을 지원을 위해서 몇가지 추가적으로 고려해 줘야 할 사항이 있다. VPN 이용자 노드의 이동이 있더라도 이동한 VPN 사용자 노드의 위치에 관계없이 지속적으로 VPN 서비스는 받을 수 있도록 지원해야 하나, VPN 의 근본 구성 목적 중 하나인 보안성을 침해해서는 안되며, VPN 망 내부에서는 각자 독립적인 사설 주소를 사용하여 네트웍을 구성할 수 있으므로 이에 따라 터널의 종단점 및 패킷의 전송 등 여러가지 추가적인 대처방안이 필요하다. 이에 따라 본 연구팀은 MPLS 기반 VPN 에서 VPN 사용자 노드의 이동성을 지원하기 위한 방안에서 위와 같은 추가적인 고려사항을 반영하여 이미 제안한 Mobile MPLS VPN 프로토콜[9][10]을 보완하여 설계, 구현하였다.

다음은 본 연구팀이 제안한 Mobile MPLS VPN 프로토콜에 대하여 간략히 소개하고 일반 인터넷 노드의 이동과 달리 VPN 노드의 이동을 지원함에 있어 추가적으로 고려해 줄 사항 및 문제점과 이에대한 해결방안을 제시한다.

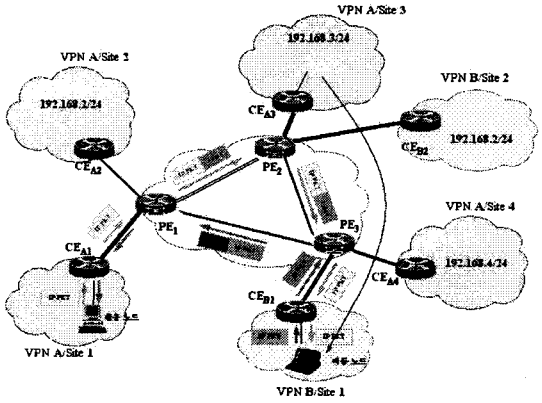
2. MPLS VPN 에서의 이동성 지원

MPLS 를 이용한 VPN 서비스를 제공하기 위해 BGP-E 를 사용하는 방식(IETF RFC 2547)에서는 PE 라우터 즉, LER(Label Edge Router : 레이블 경계 라우터) 내의 VRF(VPN Routing Forwarding instance)를 이용하여

* 본 연구는 한국과학재단 산학협력연구의 지원과 BK21 충남대학교 정보통신 인력 양성 사업단의 지원을 받음.

각 VPN 별로 라우팅/포워딩 정보를 기록한다[6]. 그런데, VPN 사용자가 다른 위치로 이동하는 경우 해당 VPN 이용자는 이동한 위치에서 VPN 서비스를 받지 못하게 된다. 따라서, VPN 이용자가 자신의 위치를 이동하더라도 계속적으로 VPN 서비스를 제공하기 위해서는 LER 내의 VRF 와 Mobile IP 프로토콜[7]에서 정의된 이동 에이전트(Mobility Agent)들이 결합되어 이동 서비스를 제공해야 한다. PE 에는 입력되는 패킷을 VPN 에 따라 구분하여 포워딩하는 기능이 포함된다[9].

[그림 1]은 MPLS VPN 망에서 이동 서비스 지원 후의 패킷 전달과정을 보여 준다.



[그림 1] MPLS VPN 이동서비스 지원 후 패킷전달

MPLS VPN 에서 이동성 지원을 위한 패킷전송의 개략적인 동작 절차는 다음과 같다.

① LER 은 처음 VPN 사용자의 데이터그램을 받아 VRF 를 검색하여 목적지 VPN 사이트로 전송한다.

② 목적지 VPN 에 연결된 LER 은 홈 에이전트(home agent)[7]에 의해 기록된 이동 정보를 이용하여 목적지 VPN 사이트 내의 목적지 노드가 이동되었는지를 파악한다.

③ 목적지 노드가 이동한 경우에는 이동지 VPN 사이트가 연결된 LER 로 두단계 레이블 스태킹을 이용하여 데이터를 전달한다.

④ 이동지 VPN 사이트에 연결된 LER 은 외부 에이전트(foreign agent)에 의해 기록된 방문자 정보를 이용하여 이동 노드가 방문했는지를 파악한다.

⑤ 방문한 경우 수신된 데이터를 해당 VPN 사이트로 전달한다.

PE 라우터 기반 MPLS VPN 에서 CE 라우터는 자신의 VPN 사이트로부터 같은 VPN 식별자를 갖는 다른 VPN 사이트로 데이터 전송을 위한 디폴트 게이트웨이에 불과하다. 즉, CE 라우터는 자신과 같은 VPN 식별자를 갖는 VPN 사이트의 위치 정보 뿐만 아니라 자신과 같은 VPN 식별자를 갖는 VPN 사이트의 도달 정보를 알 필요가 없다. 모든 VPN 사이트의 위치 정보와 도달 정보는 PE 라우터에서 관리하며 CE 라우터는 Mobile IP 에 관련하여 패킷의 전송에만 일부 관여한다.

2.1. Mobile MPLS VPN 프로토콜

(1) 노드의 이동 및 등록

이동한 Mobile Node 가 외부 에이전트로부터 VPN information extension 이 포함된 ICMP Agent Advertisement 메시지를 받으면 자신이 이동했음을 알게 되고 홈 에이전트에게 등록을 시도한다. 등록 과정은 RFC 2002 Mobile IP[7]의 과정을 따르지만 현재 방문한 VPN 으로 패킷을 포워딩 할 수 있도록 하기 위하여 등록 메시지에 추가적인 Registration VPN information extension[10]이 추가되어 전송된다.

홈 에이전트는 이동 노드의 등록을 받은 후, 등록 메시지에 추가된 VPN information extension 을 확인한다. 그런 다음, 이동 노드의 현재 위치(care-of address)와 VPN 정보를 의 홈 에이전트가 관리하는 VPN 이동 바인딩(home agent VPN Mobility Binding[10])에 각 VPN 별로 구분하여 저장하고 등록 응답을 이동 노드가 현재 위치하는 외부 에이전트에게 보낸다. 이때에도 Mobile IP[7]에 정의된 등록 응답 메시지 외에 이동 노드가 등록 요청 시 추가하였던 Registration VPN information extension 과 동일한 extension 이 추가된다. 외부 에이전트가 등록 응답을 받으면 이동 노드의 현재 방문 기록을 의 외부 에이전트가 관리하는 VPN 방문자 리스트(foreign agent VPN Visitor List[10])에 각 VPN 별로 구분하여 저장하고 이동 노드로의 패킷 전달 경로를 설정한다.

(2) 라우팅

임의의 대응 노드가 이동 노드를 목적지로 하는 패킷을 전송하면 이 패킷은 이동 노드의 홈 에이전트를 거치게 된다. 이때 홈 에이전트는 자신의 VRF 테이블[9]중에 local 로 기록된 항목에 대해 의 홈 에이전트 이동 바인딩을 검색한다. 만일 전송할 패킷의 목적지인 이동 노드의 항목이 홈 에이전트 이동 바인딩에 존재하면 노드는 이동한 것이므로 두단계 레이블 스태킹을 이용하여 이동 노드가 현재 위치한 외부 에이전트로 터널링한다. 외부 에이전트는 홈 에이전트가 두단계 레이블 스태킹을 이용하여 터널링한 패킷을 받아 외부 에이전트 방문자 리스트를 검색한다. 수신 패킷의 목적지인 이동노드의 항목이 외부 에이전트 방문자 리스트에 존재하면 이동 노드가 현재 자신의 영역에 들어와 있는 것이므로 등록 과정에서 설정한 패킷 전달 경로에 따라 이동 노드에게 전달한다.

(3) 경로최적화

MPLS VPN 망에서의 Mobile IP 에서는 이동노드의 현재 위치에 대한 바인딩 정보를 각 노드가 개별적으로 관리하지 않고 백본 네트웍에 위치한 PE 라우터(correspondent agent)가 모든 바인딩 정보를 캐싱하고 관리한다. 임의의 노드가 보낸 이동노드로 향하는 패킷은 홈 에이전트가 인터셉트하여 이동노드의 현재 위치로 터널링하는 동시에 Binding Update VPN information extension[10]이 추가된 바인딩 업데이트 메

시지를 보낸다. 이후 대응 에이전트는 의 Binding Cache[10] 정보에 기반하여 패킷을 직접 이동노드의 현재 위치로 전송하게 된다. 만일 이동 노드가 현재의 외부 에이전트에서 또 다른 외부 에이전트로 이동을 하게 된다면 이전 외부 에이전트(Previous foreign agent)로 바인딩 업데이트 메시지를 전송하며, 이때도 VPN information extension 을 함께 추가해 보낸다. 이전 외부 에이전트는 새로운 외부 에이전트가 보낸 바인딩 업데이트 메시지에서 재 터널링에 필요한 정보들을 대응 에이전트가 갖는 의 VPN Binding Cache 와 동일한 자료 구조에 저장한다. 만일 대응 에이전트가 예전의 바인딩 정보를 가지고 있어 이전 외부 에이전트에게 패킷을 보내면 이전 외부 에이전트는 의 VPN Binding Cache 에 따라 새로운 외부 에이전트로 재 터널링을 하여 패킷을 전달함으로써 smooth handoff 가 달성된다.

3. 기 제안 방식의 문제점 및 해결 방안

연구팀이 참고문헌 [9],[10]에서 제안하였던 위와 같은 Mobile MPLS VPN 프로토콜은 다음과 같은 사항의 몇가지 문제점 및 추가적인 고려사항이 존재한다. 우선 한 VPN(VPN A)에 속한 VPN 사용자 노드가 다른 VPN(VPN B)의 영역으로 이동하였을 경우에 VPN 간 격리성을 침해하는 문제가 발생한다. VPN 사이트 내부적으로는 사설주소를 사용할 수 있으므로 이동해 간 VPN(VPN B)의 다른 사이트에도 이동노드가 액세스 하고자 하는 home VPN(VPN A)과 같은 주소 영역을 가진 VPN 사이트가 존재할 가능성이 있다. 이동노드로부터 전송된 패킷은 Mobility Agent 로 전달된 후 VRF 를 참조하여 전달된다. [그림 2]는 각 이동 에이전트가 관리하는 VRF 의 구조이다.

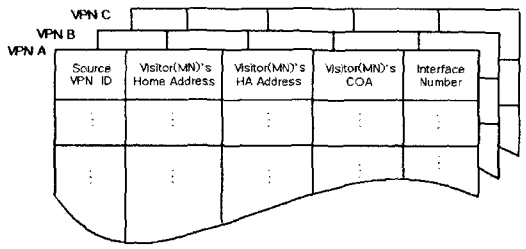
Type	Site	Intf	PE address	CE address	VPN FEC
Local	1	1	168.188.1.1	168.188.1.5	202.188.1.x
Remote	2	x	168.189.2.1	168.189.2.9	202.188.2.x
Remote	3	x	168.190.3.1	168.190.3.4	202.188.3.x

[그림 2] VRF(VPN Routing & Forwarding Table)

다른 VPN 영역으로 이동한 VPN 이용자 노드가 자신의 home VPN 과 같은 식별자를 갖는 동일 VPN 의 다른 사이트로 데이터 패킷을 전송하는 경우를 고려해 보자. 참고문헌 [9],[10]에서 제안된 방식은 이동노드가 패킷을 전송하면 Mobility Agent 의 한 인터페이스로 유입되고 Mobility Agent 는 인터페이스별로 VPN 의 사이트를 인식하게 되므로 이동노드의 home VPN(VPN A)에 대한 VRF 가 아닌 이동지 VPN(VPN B)의 VRF 를 우선적으로 참조하게 된다.

이때 우연히 이동한 VPN 의 다른 사이트에 이동노드와 같은 주소영역을 사용하는 VPN 사이트가 존재하게 된다면 패킷은 이동지 VPN 의 VRF 에 따라 우선적으로 이동해 간 VPN(VPN B)의 다른 사이트로 전송될 것이다. 이는 패킷이 전달되어야 할 의도된 목적지와 다르게 의도하지 않은 곳으로 잘못 전달 될 가능성이 존재하는 것으로, VPN 간 보안성을 침해하며 악의적인 액세스 가능성이 존재하므로 바람직 하지 않다. 따라서 본 연구팀은 외부 에이전트가 커널 내에 관리하는 VPN 방문자 리스트에 이동 노드의 home VPN 식별자를 기록하고 패킷 전송시 참조하게 될 VRF 의 선택에 이 식별자를 참조함으로써 VPN 간 보안성을 유지하도록 개선하였다. 외부 에이전트는이동노드로부터 전송된 패킷을 전달할 때 의 VPN 방문자 리스트에 기록된 이동노드의 home VPN 의 사이트에게만 패킷을 전송하게 되어 VPN 간 보안성을 유지할 수 있다.

[그림 3]은 외부 에이전트가 에 관리하는 VPN 방문자 리스트에 이동 노드의 home VPN 식별자 항목이 추가된 테이블 구조이다.

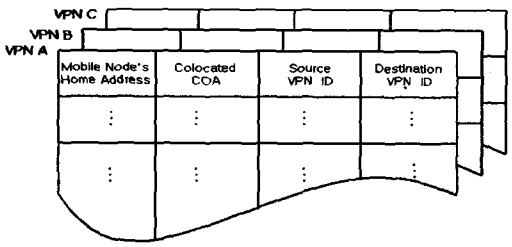


[그림 3] 외부에이전트 VPN Visitor List 의 구조

또 다른 문제점은, 이동지에서의 주소 충돌 가능성으로 인하여 DHCP 서버에서 할당받은 주소를 Care-of Address 로 사용하는 Colocated COA 동작 방식[10]에서, 터널링의 종단점이 VPN 이동노드가 될 수 없는 점이다. 본 연구팀이 제안한 MPLS VPN 에서의 이동성 지원 프로토콜은 PE 라우터 기반의 MPLS VPN 에서 동작하도록 설계,구현 되었으므로 백본의 LER(PE)을 넘어 그 이후의 단까지 두 단계 레이블 스태킹을 통한 터널링이 불가능하다. 다시말해 백본이 MPLS 망으로 이루어져 있는 PE 라우터 기반의 MPLS VPN 은 백본 내의 LER(PE) 간에 BGP-E 프로토콜로 VPN 멤버십 정보와 도달 정보를 교환한다. 반면 PE 라우터 이후의 네트웍 구성은 각각 독자적인 전송 프로토콜을 사용하는 네트웍으로 구성될 수 있으므로 두 단계 레이블 스태킹을 이용한 터널의 종단점이 백본의 LER 을 벗어나는 것은 바람직하지 않다.

따라서 본 연구팀은 외부 에이전트 역할을 수행하는 PE 라우터가 DHCP 서버 기능을 겸비하여, 이동노드에 할당한 주소 목록을 커널내에 유지하게 함으로써 터널의 종단점을 LER(PE)로 제한하도록 보완하였다. 이동 노드의 home address 와 같은 주소영역을 사용하는 다른 VPN 의 사이트로 이동한 경우 주소영역 충돌의 가능성이 존재하므로 DHCP 서버에 새로운 주소를 요청한다. 외부 에이전트 역할의 PE 에서 수행되는 DHCP 서버는 이동노드에게 주소를 할당하고 커널내에 할당한 주소들에 대한 목록을 유지한다.

[그림 4]는 외부 에이전트에서 수행되는 DHCP 서버가 커널 내에 관리하는 Address Allocation Table 의 구조이다.



[그림 4] 외부 에이전트의 Address Allocation Table

터널의 종단점이 외부 에이전트(PE)가 되도록 수정한 Mobile MPLS VPN 프로토콜의 등록 과정은 다음과 같다.

① 이동노드가 Colocated COA 로 등록요청 메시지를 전송한다.

② 외부 에이전트는 등록 메시지의 COA 와 일치하는 항목이 커널 내 주소할당 테이블에 존재하는지 검사한다.

③ 일치하는 경우 이동 노드의 주소 및 VPN 식별자 등 테이블의 나머지 항목을 저장하고 등록요청 메시지를 홈 에이전트에게 전송한다. 이때 COA 항목을 PE 주소(FA-COA)로 바꾸어 전송한다.

④ 홈 에이전트는 등록 요청 메시지를 받아 바인딩 정보를 기록한 후 외부 에이전트로 등록응답을 보낸다.

⑤ 외부 에이전트는 수신한 등록 응답 메시지의 이동노드 home address 와 커널 내 주소할당 테이블의 이동노드 home address 항목을 비교한다.

⑥ 일치하는 경우 이동노드에게 테이블 내의 Colocated COA 주소로 등록 응답 메시지를 전송한다.

즉 외부 에이전트는 DHCP 서버가 할당한 주소에 대한 사항을 커널 내에 기록하여 유지하고 이동노드로부터의 등록을 의도적으로 FA COA 의 방법으로 바꾸어 수행함으로써 터널의 종단점을 외부 에이전트(PE)로 고정한다.

임의의 대응노드가 위의 방법으로 등록된 이동노드에게 패킷을 전송하면 FA COA 를 사용하는 동작과정과 동일하게 외부 에이전트까지 터널링되어 전달된다. 외부 에이전트는 레이블을 떼어낸 후 데이터 패킷을 이동노드에게 전달하기 위해 등록과정 중에 기록된 Address Allocation Table 을 참조하여 목적주소를 할당받은 주소로 변경하여 재 전송한다.

4. 결론

본 연구에서 PE 라우터 기반 MPLS VPN 을 대상으로 하여 라우터 내의 기능과 프로토콜을 설계하고 구현하였다. 또한 본 연구팀이 제안하였던 기 제안 방식에서 추가적으로 고려해야할 사항과 보완 방법에 대해 연구하였다. VPN 사이트 내의 어떤 노드가 같은 VPN 내의 다른 사이트로 이동하는 경우, 다른 VPN 내의 사이트로 이동하는 경우에 이동성 방안을 제시하고 이동시 발생할 수 있는 VPN 간 보안성 침해 문제의 해결 방안과 Colocated COA 를 통한 동작과정시 발생할 수 있는 터널의 종단점 문제에 대한 해결 방안을 제시하고 구현하였다 본 연구를 수행함으로써, 최근 중요성이 부각되고 있는 MPLS VPN 기술과 이동 컴퓨팅 기술을 접목시킨 새로운 기술을 확보할 수 있었으며, 추후 MPLS VPN 의 활성화에 기여할 것으로 기대한다.

참고문헌

[1] Paul Ferguson, Geoff Huston, "What is VPN", The Internet Protocol Journal, Vol 1, No 2, June 1998.

[2] Bryan Gleeson, Juha Heinanen, Arthur Lin, Grenville Armitage, Andrew G. Malis, "A Framework for IP Based Virtual Private Networks", RFC2764, Feb. 2000

[3] Eric Rosen, Arun Viswanathan, Ross Callon,"Multiprotocol Label Switching Architecture", RFC3031, Jan. 2001

[4] Andersson, Doolan, Feldman, Fredette, Thomas, "LDP Specification", RFC 3036, Jan. 2001

[5] 이영석, 최 훈, 전우직, "MPLS 를 이용한 가상 사설망 실현 연구", 대학기초연구지원사업 연구개발결과보고서, 2000 년 8 월.

[6] Eric Rosen, Yakov Rekhter, "BGP/MPLS VPNs", RFC 2547, Mar. 1999.

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

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

[9] 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.

[10] 오명환, 이영석, 최훈, "MPLS VPN 망에서의 Mobile IP 설계 및 구현" , 한국 통신학회 추계 종합 학술발표 논문 초록집 vol.26 p.191, Nov. 2002