MPLS VPN 을 위한 BGP 확장 프로토콜 설계

박혜경*, 이숙영**, 유재호*
*한국전자통신연구원 인터넷기술연구부
**LG 정보통신 디지털 교환연구소
e-mail : {phk,jhyou}@etri.re.kr, jeny@lgic.co.kr

Design of BGP extension for MPLS VPN

Hae-Kyeong Park*, Sook-Young Lee**, Jae-Ho You*
*Internet Technology Department, ETRI
**Digital Switching System Research Institute, LGIC.

요 약

MPLS 망에서 VPN 기능을 제공하기 위한 방안 중 하나는 BGP 프로토콜을 이용하여 VPN 서비스를 위한 라우팅 정보를 전달하는 것이다. 본 논문에서는 BGP 을 이용한 MPLS/VPN 서비스를 위한 기능 모델을 제시하고, 이러한 기능을 위해 BGP 버전 4 로부터 확장되어야 할 기능들을 기술하고, 이러한 기능들을 구현하기 위한 확장 구조 및 인터페이스 구조를 제시하고자 한다.

1. 서론

인터넷이 전세계적으로 확산되고 사용자 층도 두터워짐에 따라 기업체들은 인터넷을 통해 고객들이나 협력 업체들 그리고 제공 업체들과 더욱 가까워지게 되었다. 이러한 추세에 따라 기업체들은 공중망을 통해 인트라 넷 및 엑스트라 넷을 구성하여 지사 사무실을 연결하거나 고객 및 관련 업체들과 연결할 수 있는 서비스를 요구하게 되었다. 이러한 요구에 의해 VPN 이 나타나게 되었다.

VPN(Virtual Private Network)은 공유 인프라에 구축되는 전사적인 규모의 연결 기능을 사설 망과 동일한 정책을 적용하여 제공하는 기술로 전용회선을 기반으로 구축된 사설 망보다 훨씬 저렴한 비용으로 인트라넷과 엑스트라 넷 서비스를 제공할 수 있으며, 사설 망과 동일한 수준의 보안성, 우선순위 제어, 신뢰성, 그리고 관리 편이성 등을 제공하여야 한다. VPN 은 엑세스 VPN, 인터라 넷 VPN, 엑스트라 넷 VPN 으로 분류될 수 있다. 엑세스 VPN 은 원격 액세스를 위해 종단간에 안전한 임시 연결 통로를 제공하는 기술로 암호화 기법과 함께 터널링 기능을 사용하거나 기존의 네트웍에 깔려 있는 다양한 액세스 테크놀러지를 이용하여 구현된다. 인터라 넷 VPN 과 엑스트라 넷 VPN 은 고객 네트웍과 동일한 정책을 적용하여, 공유형 서비스 제공자 네트웍에서 조직내의 여러 사무실들 간이나 이해관계가 있는 그룹들을 연결시켜 준다.

엑세스 VPN 솔루션들은 터널링 기술을 기반으로 VPN 을 제공하는 한 방법이 되지만 사용자가 많은 경우 확장성이 걸림돌이 된다. 또한 프레임 릴레이나 ATM VC(virtual circuit)기반 서비스 또한 많은 수의 VPN 을 구축하는 데는 적합하지 않다. 따라서 서비스 제공자들에게는 각 기업에게 차별화 된 IP 서비스를 제공해 주는 MPLS(Multiprotocol Label Switching)와 같이 확장성이 뛰어나고 표준을 기초로 구축된 인프라가 요구된다.

최근에 MPLS 를 기반으로 하는 다양한 VPN 구현 방안이 논의되고 있다[11,12,13]. MPLS 는 현재 IETF 에서 많은 관심을 끌고 있는 기술로, 기존 라우터에서 계층 3 라우팅 및 포워딩하는 방식과는 달리 계층 3 라우팅 정보를 이용하여 고정된 길이의 레이블로 메핑하여 계층 2 의 고속 포워딩을 가능하게 한 방식이다[1,2,3,14,15,16].

본 논문에서는 MPLS 망에서 BGP 프로토콜을 이용하여 VPN 관련 정보를 분배하는 BGP / MPLS VPN 방안에 대해 고려하고자 한다. 먼저 MPLS 기반 VPN 기능 모델을 제시하고, 이러한 기능을 제공하기 위해 기존의 BGP 프로토콜로부터 확장되어야 할 기능들을 기술하고, BGP 모듈의 소프트웨어 구조와 다른 모듈과의 인터페이스 구조 및 인터페이스 시나리오를 제시하고자 한다.

2. MPLS VPN 모델

MPLS 방식 VPN 에서는 각 VPN 마다 RD(route distinguisher)라고 하는 고유한 식별자를 할당하고, RD 와 고객 IP 주소를 연결하여 만든 고유한 VPN-IP 주소를 사용하여 라우팅 정보를 구성한다. BGP 는 다중 프로토콜 규약과 커뮤니티 속성(Community attribute)을 사용하여 같은 VPN 에 속한 가입자 들로 폐쇄된 사용자 그룹(Closed User Group)을 형성하여 그들 간에만 VPN 정보를 분배하도록 한다. VPN 라우팅 및 포워딩 테이블에는 각 VPN-IP 주소마다 레이블(label) 값을 가지는데, 이 값은 PE 가 어떤 가입자쪽으로 포워딩 할지 결정하기 위해 사용하는 VPN 레이블이다.

아래 그림 1 은 MPLS VPN 구성 모델을 보여주고 있다. PE(Provider Edge Router)는 공중망의 에지 라우터이며, VPN 가입자의 접속을 지원하는 MPLS 라우터이다. CE(Customer Edge Device)는 가입자 측의 공중망 접속 종단 시스템으로 라우터나 스위치 혹은 호스트 시스템들이 될 수 있다. 두 VPN 그룹 A, B 가 같은 MPLS 망에 연결되어 있고, 10.10.10.0/24, 10.10.20.0/24 IP 주소를 A, B 가입자들이 모두 사용하고 있다. 하지만 RD 값에 의해 서로 다른 주소로 식별될 수 있으며, MPLS 망에서 이러한 VPN 루트 정보들은 같은 VPN 그룹 간에만 전달된다. 예를 들어, CE2 의 임의의 호스트가 10.10.20.1 호스트로 패킷을 보내고자 할 경우, PE2 는 이 패킷이 VPN B 에 속한 패킷 임을 표시하는 식별자, 즉 VPN 레이블을 추가하여 PE3 로 포워딩 한다. PE3 는 VPN 레이블과 IP 주소를 보고 CE5 로 포워딩 하게 된다.

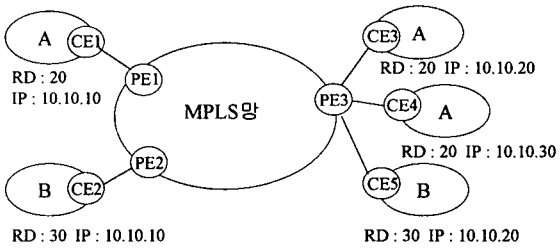


그림 1 MPLS VPN 모델

BGP 는 MPLS 망 내에서 VPN 루트 정보 및 포워딩을 위한 VPN 레이블 정보를 VPN 그룹들 간에 전달하기 위해 사용되는 프로토콜로 PE 들 간에 완전 메쉬(Full mesh) 형태로 연결되어 동작하는 것이 일반적이다.

3. BGP 프로토콜 확장

BGP 는 AS(Autonomous System)간에 라우팅 정보를 전달하기 위해 사용되는 프로토콜로 현재 가장 널리 사용되고 있는 외부 라우팅 프로토콜(Exterior Routing Protocol)이다. BGP 는 경로 벡터(Path Vector) 알고리즘을 기반으로 하여 루프 발생시키지 않으며, TCP 연결을 사용하는 프로토콜이다. BGP 버전 4 는 CIDR(Classless Inter Domain Routing)을 지원하며, AS 경로 및 라우팅 정보의 묶음(aggregation)을 허용한다.

그리고 BGP 는 확장이 용이한 프로토콜로, 최근 여러 가지 추가적인 요구에 따라 다양한 확장안 들이 제시되고 있다[5,6,7,8,9,10,11,12]. MPLS 도메인 내에서 VPN 정보를 전송하는 기능을 지원하기 위해 확장되어야 할 기능에는 다중 프로토콜 전송 기능, 레이블 정보 전송 기능, 확장된 커뮤니티 기능, 루트 정보 요청 기능, 그리고 이러한 기능 중 자신이 가진 능력을 상대 (peer or PE)에게 알려주는 기능 등이 있다.

다중 프로토콜 전송기능은 다양한 네트웍 계층 프로토콜을 전송하기 위해 UPDATE 메시지에 두 가지 속성 MP_REACH_NLRI, MP_UNREACH_NLRI 가 추가된 기능이다[6]. 이 속성은 AFI(Address Family Identifier) 필드를 가지는데, 이 필드에 의해 전송되는 라우팅 정보의 타입을 식별한다. 또한 두 BGP 피어간에 OPEN 메시지를 주고 받을 때, 이 필드 값에 의해 서로의 처리 능력을 알리게 된다.

레이블 정보 전송 기능은 다중 프로토콜 전송 기능을 이용하여 레이블을 가진 라우팅 정보를 전송하는 기능이다. NLRI 필드에 레이블 정보가 추가되어 <길이, 3 옥텟의 레이블, IP 프리픽스>로 구성되며, AFI 필드 값은 1, SAFI(Subsequent AFI)필드 값은 4 를 가진다[8]. 그리고 MPLS VPN 을 지원할 경우, 전송하는 정보가 레이블을 가진 VPN-IPv4 루트 정보가 되고, AFI 필드 값은 1, SAFI(Subsequent AFI)필드 값은 128 을 가지며, NLRI 필드는 <길이, 3 옥텟의 레이블, 12 옥텟의 VPN-IPv4 주소>로 구성된다[11,12].

확장된 커뮤니티 기능은 라우팅 정보를 분배하는데 있어 분배 대상을 제어 할 수 있도록 융통성을 제공하는 기능으로 VPN 서비스를 위해, Route Target 커뮤니티와 Route Origin 커뮤니티를 제공한다[5]. 확장 커뮤니티 속성 타입코드는 16 이다.

루트 정보 요청 기능은 ROUTE REFRESH 메시지를 추가하여 임의의 BGP 피어에게 라우팅 정보를 재전송하도록 요청하는 기능이다[10]. 메시지 포멧은 타입 필드(TBD), AFI 필드(2 옥텟), Reserved 필드(1 옥텟), SAFI 필드(1 옥텟)으로 구성된다. AFI 와 SAFI 필드 값은 재전송을 원하는 정보가 어떤 것인지를 표시한다. 이 기능은 VPN 기능 블록에서 피어 PE 들에게 VPN 루트정보의 재 전송을 요구할 때 사용된다.

BGP 가 가진 능력을 상대 PE 에게 알려주는 기능은 위의 여러 가지 확장된 기능 들 중 자신이 가진 능력을 BGP 가 세션을 맺을 때 미리 알림으로써 상대의 능력에 맞는 메시지를 전송하도록 한다[9]. 이 기능은 OPEN 메시지와 NOTIFICATION 메시지에 의해 수행된다. OPEN 메시지의 Capability Optional Parameter 필드에 자신의 능력을 싣어서 보내면, 같은 능력을 가진 경우 OPEN 메시지를 보내고 그렇지 않은 경우 NOTIFICATION 메시지에 에러코드와 지원되지 않는 Capability Code 들의 리스트를 싣어 보낸다. 현재 까지 결정된 Capability Optional Parameter 값은 표 1 과 같다.

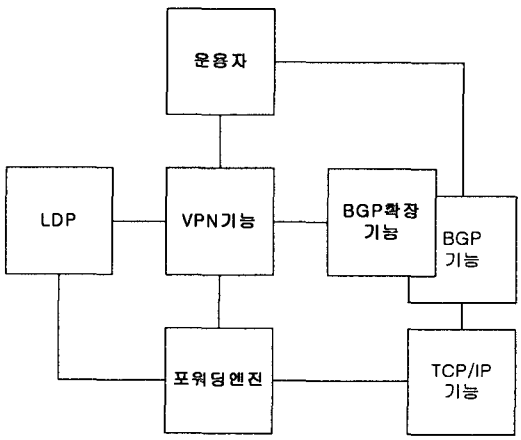
BGP 가 이러한 확장된 기능들을 가질 때, BGP 는 일반적인 IPv4 라우팅 정보들을 전달하기 위해서도

사용되고, 또한 VPN 기능 블록의 요구가 있을 경우 VPN 루트 정보도 전달하기 위한 기능도 수행하게 된다. 제안한 구조에서는 하나의 BGP 세션을 통해 두 가지 기능을 수행하고자 한다.

<표 1> Capability Optional Parameter 필드 내용

	Capability Code Field	Capability Length Field	Capability Value Field
BGP4 +	1	4	AFI = 1 SAFI = 1 (unicast), 2(multicast), 3(unicast and multicast)
Carry Label Info.	1	4	AFI = 1 SAFI = 4(TBD)
MPLS VPN	1	4	AFI = 1 SAFI = 128(Cisco)
Route Refresh	TBD	0	

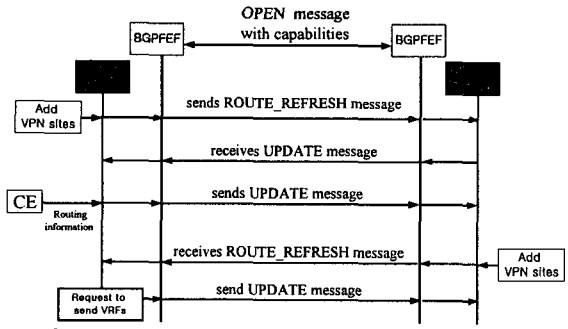
그림 2 는 MPLS VPN 을 지원하기 위한 기능 블록 구조이다. 제안한 구조에서 VPN 기능 블록은 VPN 관련 설정 기능, VPN 라우팅 및 포워딩 정보의 관리 기능, 포워딩엔진으로 VPN 포워딩 정보 전달 등의 기능을 수행하도록 하며, BGP 확장 기능블록에서는 VPN 기능 블록의 요구가 있을 경우, BGP 피어간에 VPN-IPv4 루트 정보를 전달해 준다. VPN 기능을 위해 BGP 블록은 다른 블록과는 인터페이스가 전혀 필요 없으며, 단지 VPN 블록과 인터페이스를 가진다.



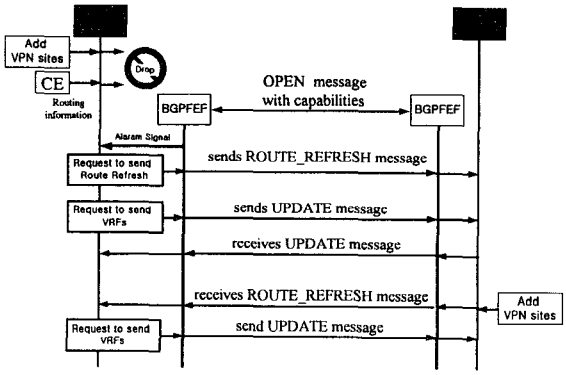
<그림 2> MPLS VPN 기능 블록 구조

다음은 BGP 기능 블록과 VPN 기능 블록간의 연동 시나리오이다. 그림 3 은 BGP 블록이 이미 세션을 맺은 후 VPN 블록이 시작되는 경우의 연동 시나리오이다. VPN 기능이 구동 될 경우 먼저 ROUTE REFRESH 메시지를 보낼 것을 BGP 에게 요구하게 되고 BGP 는 모든 피어 들에게 VPN 루트정보를 보낼 것을 요구하는 ROUTE REFRESH 메시지를 보낸다. BGP 는 UPDATE 메시지를 받았을 때, 이 정보가 VPN 루트 정보이면 VPN 블록으로 전송하고, 그렇지 않으면 BGP 블록 내에서 처리한다. VPN 블록에서 UPDATE 를 보낼 것을 요구할 경우, 그 루트정보가 전송되어야 하는 피어 들에게만 그 정보를 전송한다. 이것은 Route Target 확장 커뮤니티 기능에 의해 가능하다. BGP 피어로부터 ROUTE REFRESH 메시지를 받은 경우, VPN 블록에 알려주면 VPN 블록은 전송할 VPN 정보를 BGP 블록에게 보낼 것을 요구하게 된다.

그림 4 는 VPN 블록이 먼저 구동되고 BGP 블록이 세션을 맺는 경우의 연동 시나리오이다. 이 경우 VPN 블록이 구동되면 BGP 블록에게 ROUTE REFRESH 를 보낼 것을 요구하고, 사이트로부터 VPN 루트 정보가 생성될 경우 이를 보낼 것을 요구한다. 이런 메시지들은 BGP 블록이 구동 되어 BGP 세션이 맺어지기 전까지 무시되며, BGP 세션이 맺어지면 이 사실을 VPN 블록에 알려주고, VPN 블록에서는 그림 3 의 시나리오와 유사한 과정으로 동작한다. 일반적으로 그림 3 와 같은 시나리오를 가지고 동작하며, 예외적인 경우나 비정상적인 경우 그림 4 와 같은 시나리오로 동작하게 된다.



<그림 3> BGP 기능 블록이 먼저 구동되는 경우 BGP 블록과 VPN 블록 사이의 연동



<그림 4> VPN 기능 블록이 먼저 구동 되는 경우 BGP 블록과 VPN 블록 사이의 연동

이러한 시나리오에 따라 BGP 블록과 VPN 블록 간에 연동을 위한 인터페이스 기능들은 표 2 와 같으며, BGP 에서 VPN 기능을 위해 추가적으로 관리 해야 하는 데이터베이스에는 피어 Capability 테이블, Route Target 커뮤니티 테이블 등이 있다. 피어 Capability 테이블은 각 피어 들이 어떤 능력까지 가지고 있는지에

대한 정보를 관리하는 테이블로 이러한 정보는 BGP 세션을 열 때, 서로 주고 받는 메시지에 의해 알 수 있다. 그리고 Route Target 커뮤니티 테이블은 특정 VPN 라우팅 정보가 전달되어야 할 그룹들을 관리하는 테이블로, 피어 들의 Route Target 정보는 그 피어로부터 받은 UPDATE 메시지의 Route Target 속성을 보고 알 수 있으며 PE 에 직접 연결된 사이트의 Route Target 정보는 VPN 제어 블록의 설정정보를 참조하여 알 수 있다.

<표 2> BGP 블록과 VPN 블록 간의 인터페이스

인터페이스이름	기능	방향
Request_to_send_all	모든 VPN 루트정보를 전송하도록 요구	BGP 블록 → VPN 블록
Send_vrf	하나의 VPN 루트정보 전송요구	VPN 블록 → BGP 블록
Send_route_refresh	ROUTE REFRESH 메시지 전송 요구	VPN 블록 → BGP 블록
Receive_vrf	VPN 루트정보를 VPN 블럭으로 전송	BGP 블록 → VPN 블록

4. 결론

본 논문에서는 MPLS 상에서 VPN 을 지원하기 위해 필요한 BGP 의 확장 기능들을 정의하고 이러한 기능들이 어떻게 구현되며 VPN 기능 블록과 어떤 인터페이스를 가지면서 어떤 연동 시나리오로 수행되어야 하는 지를 제안하였다. 제안한 방법에서 BGP 는 하나의 세션으로 IPv4 라우팅 정보와 VPN 라우팅 정보를 전달하며, BGP 블록에서 받은 정보가 VPN 라우팅 정보라고 판단될 경우 VPN 기능블록으로 그 정보를 전달하며, VPN 블록이 VPN 루트 정보의 전송을 요구할 경우 해당 그룹으로 그 루트 정보를 전송해주는 역할을 한다.

본 논문에서 제시한 구조는 BGP 프로토콜의 확장 기능 들을 각각 독립적으로 설계하였으며, MPLS VPN 기능을 위해 4 개의 인터페이스 기능만으로 VPN 기능 블록에게 필요한 모든 기능을 지원하면서, 두 블록간의 독립성을 유지해주며, 하나의 세션으로 일반적인 d 인터넷 라우팅 정보와 VPN 라우팅 정보를 전송한다. 그리고 현재 구현된 BGP 의 확장된 기능들은 각각 독립적인 기능으로 다른 서비스를 위해 사용될 수 있도록 설계되었다.

참고문헌

[1] IETF, Multiprotocol Label Switching Architecture, draft-ietf-mpls-arch-07.txt, July 2000

[2] IETF, MPLS label stack encoding, draft-ietf-mpls-encaps-06.txt, September 1999.

[3] IETF, MPLS using ATM VC switching, draft-ietf-mpls-atm-02.txt, April 1999.

[4] Y. Rekhter and T. Li, "A Border Gateway Protocol 4(BGP-4)," RFC 1771, March 1995.

[5] IETF, BGP Extended Communities Attribute, draft-ramachandra-bgp-ext-communities-04.txt, December 2000

[6] T. Bates, R. Chandra, D. Katz and Y. Rekhter, "Multiprotocol Extensions for BGP-4," RFC 2858, June 2000.

[7] IETF, Multiprotocol Extensions for BGP-4, draft-ietf-edr-bgp4-multiprotocol-v2-05, March 2000

[8] IETF, Carrying Label Information in BGP-4, draft-ietf-mpls-bgp4-mpls-04.txt, January 2000.

[9] R. Chandra and J. Scudder, "Capability Advertisement with BGP-4," RFC 2842. May 2000

[10] IETF, Route Refresh Capability for BGP-4, dratf-chen-bgp-route-refresh-02.txt, September 1999.

[11] E. Rosen and Y. Rekhter, "BGP/MPLS VPN," RFC2547, March 1997.

[12] IETF, BGP/MPLS VPN, draft-rosen-rfc2547bis-00.txt, March 2000.

[13] IETF, A Core MPLS IP VPN Architecture, draft-muthukrishnan-mpls-corevpn-arch-03.txt, May 2000.

[14] 전병천, 정태수, 강선무, 이유경, "ATM 기반 고속 인터넷 구축 기술", 한국통신학회 정보통신지 제 16 권 2 호, pp.148-158, 1999.2.

[15] 유재호, 강선무, 이유경, "MPLS controller 소프트웨어 구조," COMSW'99 논문집, pp.517-520, 1999.7

[16] Sun Moo Kang and You Kyeong Lee, "Design Issues of MPLS for Public Internet Service," ICACT2000, pp.225-228, February 2000.