BGP/MPLS VPN 과 가상 라우터 VPN 을 이용한 기업 네트워크 구성 방안

전정훈*, 우미애**
*하나로텔레콤
**세종대학교
e-mail : jhjun@hanaro.com

An Enterprise Network Configuration Method using BGP/MPLS VPN and Virtual Router VPN

Jung-Hoon Jun* and Miae Woo**
*Hanaro Telecom
**Sejong University

요 약

VPN(Virtual Private Network)은 물리적인 장비나 회선을 논리적으로 구분하여 기존 전용회선을 기반으로 하는 사설 네트워크에 비해 상대적으로 적은 구축 비용, 융통성 있는 확장성, 저렴한 운용비용의 장점을 보유한 별도의 사설 네트워크를 구성하는 기술이다. 다양한 VPN 기술 중에서도 MPLS VPN 은 확장성, QoS 제공을 용이하게 해주는 장점을 가지고 있어 차세대 네트워크 기술로 부각되고 있다. 일반적으로 MPLS VPN 은 ISP 에서 제공하는 서비스로 인식되나 규모가 크고 다양한 사설 네트워크를 필요로 하는 기업의 네트워크 모델로도 적합하다. 또한 Virtual Router VPN 은 Customer Edge(CE) 장비로서 활용성이 큰 Switch 장비에 적용하여, CE 를 MPLS VPN 과 쉽게 연동하게 한다. 본 논문에서는 MPLS VPN 및 Virtual Router VPN 을 이용하여 기업 네트워크를 효과적으로 구성하는 방안을 기술한다.

1. 서론

VPN 이란 공중망에서 물리적인 구성과는 별도로 여러 지역의 분산된 site 들을 상호접속하기 위한 논리적인 별도의 망을 구성하기 위해 이용된다. VPN 은 전용회선을 이용한 물리적인 망에 비해 비용 및 망 구성의 유연성 측면에서 많은 장점을 가지며, 근래에는 근간 기술 및 활용 범위가 더욱 다양해지고 확대되고 있다.

VPN 은 크게 Layer2 와 Layer3 방식으로 분류할 수 있으며, 세부적으로는 VPLS(Virtual Private LAN Service), L2TP(Layer2 Tunneling Protocol), IPSec, MPLS(Multi-Protocol Label Switching), Virtual Router 등의 기술 방식들이 있다. 이 중에서 MPLS VPN 은 타 방식들에 대비하여 확장성이나 Traffic Engineering, QoS 에서 장점을 가지고 있다. 이 같은 장점을 활용하여 ISP(Internet Service Provider)가 아닌 일반 기업에서 직접 MPLS VPN 을 이용하여 비용, 성능, 확장성 측면에서 효과적인 네트워크를 구성할 수 있다.

일반적으로 기업에서의 MPLS VPN 사용은 서비스 사업자(ISP)가 제공하고 사용자인 고객은 제공된 망을 적정 대가를 지불하고 사용하는 모델이 알려져 있다. 하지만 대기업이나 그룹 계열사 네트워크 또는 대규모의 네트워크를 구축, 운영해야 하는 기업에서는 MPLS VPN 이 ISP 의 전유물이 아닌 자체적으로 기업망에 적합한 모델이 될 수 있다. 즉 기업 전산망 자체를 MPLS 네트워크의 Core 인 P(Provider), PE(Provider edge)로 구성하며, 각 계열사, 지사, Intranet/Extranet 또는 다른 용도의 네트워크(CE)를 VPN 으로 구성하는 것이다. 이 과정에서 Virtual Router VPN 이 CE 구현 기술로서 사용된다. 만일 VPN 을 사용하지 않고 다른 용도의 네트워크를 물리적으로 각각 구성한다면 더 많은 비용과 공간의 낭비가 될 것이다.

본 논문에서는 BGP/MPLS VPN 및 Virtual Router VPN 에 대한 설명과 이를 이용하여 상기와 같은 용도의 기업망을 비용 및 성능 효과적으로 구성하는 방안 및 주요 특징을 MPLS 구조, 라우팅 방안, QoS 적용 방법 등에 대해 기술한다.

2. BGP/MPLS VPN(RFC2547bis) 개요

MPLS 은 패킷에 Label 을 표시하여 고속으로 스위칭하는 기술이며, Label Stacking 기술에서 VPN 기능이 파생되었다. 그림 1 과 같이 RFC2547bis VPN 은 VPN 라우팅 정보를 분배하는데 BGP 를 이용하며, 망 별 완벽한 보안을 유지하여 망 별로 분리된 사설 네트워크처럼 동작이 가능하기 때문에 장비의 별도 구성없이 하나의 장비에서 분리된 서비스를 구현할 수 있다[1][2].

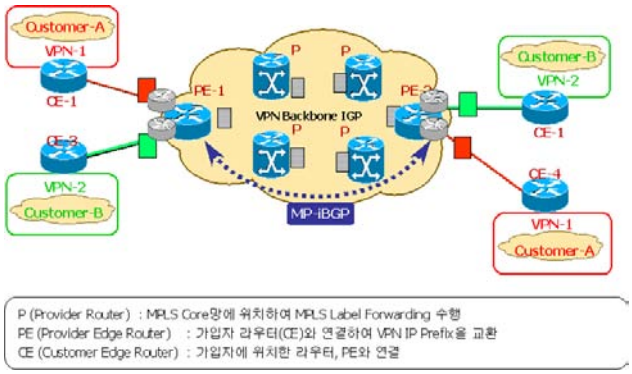


그림 1. MPLS VPN 개요

3. Virtual Router VPN 개요

Virtual Router(VR)란 하나의 장비내에서 논리적으로 여러 개의 라우팅 프로세서가 독립적으로 운영되어 각 망 별로 가상의 독립된 라우터를 구성하는 기술이다. 망 별 장비는 통합하면서 하단의 독립된 망으로부터 유입되는 트래픽은 해당 망 라우팅 테이블만을 참조하게 되는 형태이다[3].

대부분의 L3 VPN 에서 CE 로서 라우터를 이용하지만, 이 논문에서는 VR 이 구현되는 L3 Routing Switch 를 이용하며 CE 의 역할을 수행한다. 그 이유는 기업망의 물리적인 하나의 장소에서 다수의 VPN 을 구현 시 인터페이스 제약이 큰 라우터보다 물리적인 LAN 포트수가 많은 스위치가 확장성에서 유리하기 때문이다. 또한 최근에 Metro Ethernet 의 확대로 상대적으로 비싼 전용회선보다 비용 효과적으로 구성할 수 있으며, 아직까지는 MPLS VPN 을 구현하는 Switch 가 상용화되지 않았기 때문이기도 하다. 이와 같이 CE 에서는 Virtual Router 를 이용하여 PE 의 해당 VRF(VPN Routing & Forwarding)와 Mapping 하여 연동하는 것이 많은 장점을 갖는다.

4. 네트워크 구성 방안

4.1 기본 요소 및 구성

4.1.1 P Router (LSR: Label Switch Router)

MPLS Core 망에 위치하여 Label 정보를 교환하며 PE Router 로부터 MPLS VPN Packet 을 받아서 Label Switching 을 수행한다. 요구되는 기능으로는 MPLS Label Adding, Swapping, Popping 과 LDP(Label Distribution Protocol), LSP(Label Switched Path) Setup, Fast Reroute, QoS over MPLS 등이 있다[1][2].

4.1.2 PE Router (LER: Label Edge Router)

CE 라우터와 연결되어 서비스망에 대한 VPN 을 정의한다. 요구 기능은 MP-iBGP(MultiProtocol iBGP), Route Reflect, VPN 별 Routing & Forwarding Table(VRF Table) 등이 있다[1][2].

4.1.3 CE Router (or Switch)

PE 와 연결되어 서비스망의 Normal IP 트래픽을 전달한다. MPLS 구성을 지원하지 않으며, 많은 인터페이스가 제공되는 Switch 장비에서는 VPN 별 Virtual Router 를 활성화시켜 상위 PE Router 와 VPN 별로 연결한다. 이중화를 위해 VRRP(Virtual Router Redundancy Protocol)를 이용하기도 한다[4].

4.1.4 MPLS L3 VPN

앞의 각 요소들을 이용하여 표 1 과 같은 기본적인 구성을 구현한다.

표 1. MPLS VPN 기본 구성

CE-PE 구간	- CE 라우터(스위치) ✓ PE 라우터를 향하여 Default-Route 생성 - PE 라우터 ✓ 연결된 CE 라우터가 보유하고 있는 VPN을 정의 ✓ PE-CE 구간을 VPN 영역으로 설정 ✓ VPN Network 에 대한 Routing Table 생성
MPLS Core 구간	- VPN Network에 대한 Routing Table 을 교환하고자 하는 PE간에 MP-iBGP Session 형성 ✓ Route-Reflector를 사용하여 PE 라우터간의 MP-iBGP Session 감소 - MP-iBGP Session이 형성된 PE-라우터간 VPN Network Routing Table 교환 ✓ VPNv4-Address (Route Distinguisher + IP Prefix)를 사용하여 VPN 별로 Unique한 주소체계 사용 - VPN Network의 IP Prefix에 대한 VPN 전용 Label 생성/ 교환
Packet Forwarding	- CE -> PE 구간에서는 Normal IP Packet Forwarding - PE 라우터는 IP Packet에 대한 VPN Forwarding Table 참조하여 ✓ MPLS Label / VPN 전용 Label 2개를 Encapsulation - Label Packet을 받은 PE 라우터는 VPN Forwarding Table 을 참조하여 Label 제거 후 목적지 VPN 으로 Packet을 Forwarding

4.2 라우팅 방안

MPLS 망에서의 라우팅을 위한 MP-iBGP 는 VPN-IPv4 정보, MPLS Label 정보, Standard/ extended BGP Community 를 VPN 간 공유하기 위한 목적으로 사용된다[1][5]. Standard iBGP 의 선언과 동일한 절차에 의거

IPv4 대신 VPN-IPv4 Address Family 를 규정하여 PE 간의 iBGP Neighborship 을 형성시킨다. 동일한 VPN 그룹에 속한 PE 간에는 MP-iBGP 가 Full Mesh 로 구성되어야 하지만, 구현 복잡성 및 리소스 보호를 위한 모든 MP-iBGP 라우터간의 Full Mesh neighborship 을 방지하기 위하여 iBGP 개념에서 도입된 Route Reflector 를 적용하고, 각 PE 는 Route Reflector 로 정의된 PE 하고만 MP-iBGP 관계를 형성한다. VPN 끼리의 정보 공유는 MPLS VPN Network Prefix Advertisement 를 위하여 MP-iBGP 프로토콜로 VRF 라우팅 정보들을 유입 시킨다. 이 때, MP-iBGP 내로 유입되는 각 Prefix 는 Static 으로 선언되고 Static 선언 부는 자동으로 MP-iBGP 프로토콜로 유입되며, VPN-IPv4 Address Family 가 규정되어서 neighborship 이 형성된 경우 동일 VRF Address Family 간에는 정보가 공유된다. 이에 각 PE 의 VRF Routing Table 은 각기 동일 망에 대한 Prefix 정보만 보유한다. 그림 2 는 Full Mesh 와 Route Reflect 를 각각 사용할 때의 iBGP Neighborship 상태를 나타낸다[2].

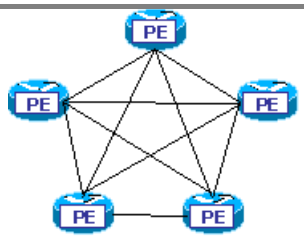
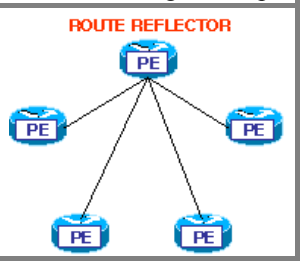
구분	FULL MESH 상태의 iBGP Neighborship	Route Reflector 사용시의 iBGP Neighborship
구성		

그림 2. Full Mesh vs. Route Reflect 방식 비교

그림 3 의 MPLS 내부 라우팅을 위한 프로토콜은 사용상 제약이 없으나, LDP(Label Distributed Protocol) 및 TE(Traffic Engineering)을 위하여 LSA Type 1, 2 의 교환을 보장하는 IGP(Internal Gateway Protocol)인 OSPF(또는 ISIS) Single Area 로 구성한다. End-to-End Traffic Engineering 구현을 위해서는 Single Area 를 반드시 사용하여야 하며, Interarea TE Tunnel 등의 기법을 사용하여 적용하는 것이 불가능한 것은 아니지만, 라우팅 프로토콜의 원천적인 Area 분리의 한계가 있다. Single Area Domain 내에는 MPLS P Router, PE Router 로 사용될 장비의 Interface 부분이 포함된다[6].

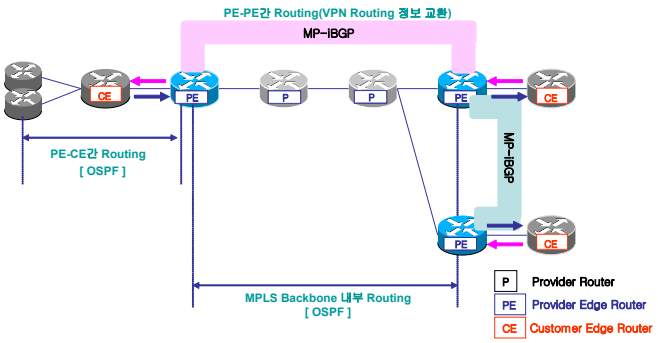


그림 3. MPLS 라우팅

그림 4 에서처럼 CE 와 PE 간의 라우팅은 Static 또는 OSPF 와 같은 Dynamic IGP 를 사용한다. 동일 VPN 내부에서만 MPLS VPN 을 통하여 Routing Update 가 수행되며, MPLS VPN 망이 OSPF Backbone Area 역할을 수행한다. 또한 OSPF 를 사용하지만 PE Router 에서 다른 Routing 정보를 전파하는 대신 Default Route 만 전파함으로써 CE 라우터에는 Dynamic 하게 OSPF Default Route 만 존재하게 되어 라우팅에 따른 CE 의 부담이 거의 없다.

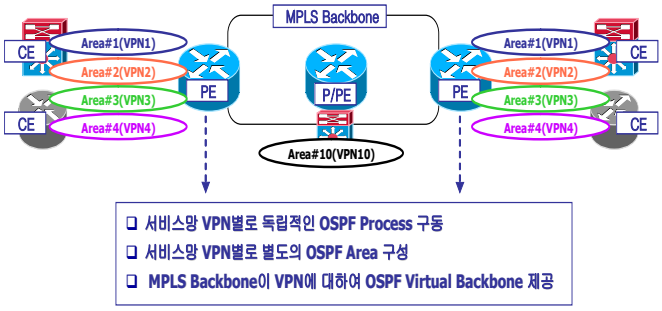


그림 4. PE~CE Routing

4.3 VPN 간 통신 (Overlapping)

MPLS L3 VPN 에서는 동일 VPN 간의 통신만이 가능하다. 그러나 기업망에서 VPN 간의 통신이 요구되는 경우가 있으며, 이를 위한 기술이 VPN Overlapping 이다[2]. 예를 들어 VPN1 과 VPN2 가 VPN10 이라는 하나의 VPN 과 통신을 수행하려면 VPN10 은 VPN1 과 VPN2 에 대한 IP Prefix Table 을 보유하고, VPN1 과 VPN2 는 VPN10 에 대한 IP Prefix Table 을 보유해야 한다. 이것은 Route-Target 을 이용하여 구현 가능하며, VPN1 & VPN2 와 VPN10 간의 통신을 수행하여 준다.

4.4 이중화 (Redundancy)

중요한 구간의 네트워크 가용성 증대를 위해 P, PE 의 MPLS Backbone 구간은 그림 2 에서의 Route Reflector 를 이중화하여 Dual RR 시스템으로 구현한다. CE~PE 구간의 이중화는 VRRP(Virtual Router Redundancy Protocol)과 Dynamic Routing Protocol 을 함께 이용한다[4]. 그림 5 와 같은 구성으로 장비 및 회선 장애 시 우회 경로를 마련한다. 첫번째, CE 에서의 VRRP 구현으로 Active-Active 방식으로 장비 이중화를 하였으며, 두번째, VPN 별 OSPF 에 의한 CE~PE 간 Dynamic 경로 이중화. 세번째, MPLS 망의 OSPF 구현으로 PE~P 구간의 경로 이중화가 가능하다.

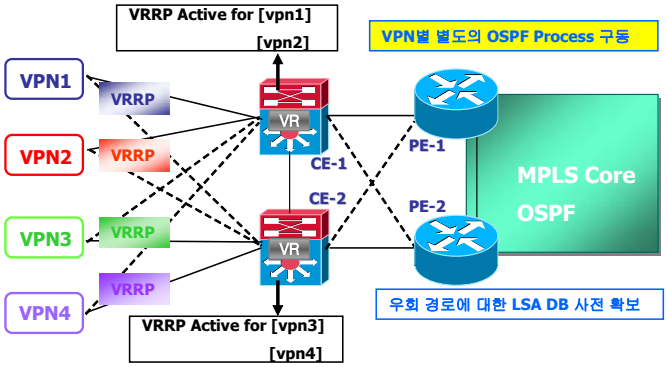


그림 5. 이중화 구성

4.5 Quality of Service

각 VPN 의 원활한 통신의 Congestion 관리를 위해 Differentiated Service 기반의 QoS 를 적용한다. 이를 위해 먼저 CE 단의 Outbound 트래픽에 대하여 IP 레벨의 Traffic Classification & DSCP(Diff-Serv Code Point) Marking 을 하여 Source, Destination, Application, 대역폭에 따라서 Class 를 분류한다. 그 다음으로 CE 와 대응하는 PE 의 Inbound 트래픽에 대해 IP 망에서 분류된 DSCP Code Class 를 MPLS 망에서도 식별하기 위해서 DSCP Code 를 MPLS EXP Bit 로 변경한다. 다음 구간의 P/PE 에서는 MPLS EXP Bit 를 읽어서 Class 를 인식하고 Class 별 Queue Scheduling 을 수행한다. Queuing 은 최우선순위 Class 에 LLQ(Low Latency Queuing, Priority Queuing)을 사용하여 우선적인 대역폭을 할당받고, 나머지 Class 들은 WFQ(Weighted Fair Queuing)으로 상위 Class 에서 사용하고 남은 대역폭의 일정 비율을 할당받는다[7][8].

최근 바이러스나 웜과 같은 비정상 트래픽으로 인한 네트워크 장애가 발생하고, P2P 나 비업무용 트래픽으로 업무용 트래픽 속도 저하 및 대역폭 낭비가 빈번히 발생하고 있다. 이러한 상황 시 DiffServ MPLS QoS 를 적용하여 업무용이나 중요한 트래픽에 상위 Class 를 부여하고 비업무용 트래픽에 낮은 순위의 Class 를 부여한다면 효율적인 네트워크 구성이 이루어질 수 있다.

5. 결론 및 향후 고려 사항

본 논문에서는 대규모 기업이나 서비스 용도에 따른 개별 네트워크가 요구되는 기업을 위한 네트워크 모델로서의 MPLS VPN 및 Virtual Router VPN 을 제안하고 그 구현 방법을 제시하였다. 제시된 방법은 ISP 에서 제공하는 MPLS 서비스의 제한된 한계에서 벗어나 직접 MPLS VPN 구축을 통해 각 기업의 특성에 맞는 MPLS 의 특징들을 적용할 수 있는 장점이 있다. 특히 Virtual Router Switch 를 이용하여 비용 효과적인 CE 를 구성하는 방법과 Active-Active 이중화 기법은 중요 네트워크의 가용성을 향상시킬 것이다. 또한 MPLS 의 특징중 하나인 QoS 적용을 통해 기업 내부 네트워크의 성능, 가용성 향상 및 대역폭 적정 활용을 통한 비용 절감의 효과도 가져올 수 있다.

추가적으로 보다 나은 QoS 를 위해 IntServ(RSVP)를 이용한 Traffic Engineering 적용이 필요하며, IPv6 로의 전이에 대한 고려가 있어야 하겠다.

참고문헌

[1] Rosen, E., Rekhter, Y., “BGP/MPLS IP VPNs”, RFC2547bis, May 2003.

[2] Pepelnjak, I., Guichard, J., “MPLS and VPN Architectures”, Cisco Press, October 2000.

[3] Knight, Paul, et al, “Network based IP VPN Architecture using Virtual Routers”, draft-ietf-l3vpn-vr-02.txt, April 2004.

[4] Hinden, R., “Virtual Router Redundancy Protocol”, RFC3768, April 2004.

[5] Bates, Chandra, Katz, and Rekhter, “Multiprotocol Extensions for BGP4”, RFC2858, June 2000.

[6] Rosen, Psenak and Pillay-Esnault, “OSPF as the PE/CE Protocol in BGP/MPLS VPNs”, draft-ietf-l3vpn-ospf-2547-00.txt, June 2003.

[7] Weiss, W., “QoS with Differentiated Service”, Bell Labs Technical Journal, October-December 1998.

[8] Vegesna, S., “IP Quality of Service”, Cisco Press, January 2003.