Virtual Router VPN과 BGP/MPLS VPN의 비교분석

김성한* · 이계상*

*동의대학교 정보통신공학과

A Comparison of Virtual Router and BGP/MPLS VPN

Sung-Han Kim* · Kye-Sang Lee*

*Dong-eui University

E-mail : shksh@hananet.net

요 약

정보기술의 급속한 발달로 멀티미디어 및 인터넷 환경이 확산되어 사용자의 네트워크 대역폭 또한 증가하였다. 이런 환경에서 VPN은 공중망을 이용하여 사설망을 꾸미는 기술로 통신비용 및 관리비용을 줄이는 것을 목적으로 현재 사용되는 기술이다. VPN은 접속방법, 이용회선, 서비스 제공방식, 응용방식, 구현방법 등에 따라 여러 형태로 분류된다. 본 논문에서는 서비스 제공방식의 분류에서 네트워크기반의 VPN중 현재 제안되고 있는 두 방식인 Virtual Router구성 방식과 BGP/MPLS구성 방식을 비교분석 한다.

Ⅰ. 서 론

정보기술이 급격히 발달하면서 멀티미디어의 발달과 인터넷 환경의 확산으로 대용량의 대역폭이 사용되게 되었다. 따라서 기업들도 대용량의 대역폭이 필요로 하게 되었고 이에 따른 통신비용 및 관리비용이 증가하게 되었다. 이 통신비용과 관리비용을 줄이는 것이 VPN의 최대 매력이다. 초기 VPN은 전용회선에 사용되었으나 최근 공중망을 이용한 VPN의 구성이 이슈로 등장하면서 각종 기술들이 나오고 있다. 공중망을 이용한 VPN을 구성하는데는 중요한 두 가지 기술이 있는데 암호기술과 터널링 기술이다. 암호기술에는 여러 가지 암호화 알고리즘(DES, 3DES, IDEA, CAST등)을 VPN에 도입하였고 터널링 기술에는 IPSec, PPTP, L2TP, L2F등이 사용되고 있다. 또, VPN은 여러 기준으로 분류되는데 첫째, 접속 범위에 따라 Intranet VPN, Remote access VPN, Extranet VPN으로 나뉜다. 둘째, 이용회선에 따라 전용회선기반 VPN, Dial-Up을 이용한 VDPN, 인터넷 기반 VPN으로 분류 될 수도 있다. 셋째, 서비스 제공방식에 따라 원격접속 VPN, LAN-to-LAN VPN등으로 분류되기도 한다. 특히, 서비스 제공방식에 따른 분류에서는 터널의 형태와 접속을 제공하는 기능에 따라 사용자 기반 VPN, 종단장치 기반 VPN, 네트워크 기반 VPN으로 세분화된다.[1] 본 논문에서는 네트워크 기반 VPN을 바탕으로 한 Layer 3 VPN 기술인 Virtual Router와 BGP/MPLS VPN의 구성방식을 기술하고, 이 두 방식의 비교 및 향후 전망을 결론으로 맺는다.

Ⅱ.구성요소

Virtual Router(VR)네트워크는 VR을 포함하여 Customer Site(CS), Customer Edge(CE)장치, Provider Edge(PE)장치, Provider(P)가 기본 구성요소이다. CS는 CE와 VR의 연결로 P의 백본에 연결되어 있다. CE장치는 하나 이상의 VR에 연결될 수 있으며 미리 설정되어 있다. VR은 한 Service Provider(SP)의 PE장치에 다중으로 존재하고 어떤 접속링크(ATM, FR, Ethernet, PPP이나 각종 터널링 프로토콜)라도 사용할 수 있으며 라우팅 테이블은 각 VPN의 Site-to-Site Reachability information을 가지고 있다.[2]

BGP/MPLS VPN은 CE 장치(라우터), PE 라우터, P 라우터로 기본 구성을 이룬다. CE 장치는

하나이상의 PE 라우터의 데이터 링크를 통해 SP 네트워크에 고객이 접속할 수 있도록 하고 Host 나 Layer 2 Switch임과 동시에 직접 연결된 PE 라우터와 인접성을 수립하는 IP 라우터가 되며 PE 라우터와 PE 라우터에서 전용으로 사용되는 원격 VPN 경로로 지역 VPN의 경로를 알려주는 역할을 한다. PE 라우터는 정적 라우팅, RIPv2, OSPF, EBGP등의 라우팅 프로토콜이 사용된 CE 라우터와 라우팅 정보를 교환한다. 또, PE 라우터는 직접 연결된 VPN 사이트들의 라우팅 테이블인 VPN Routing and Forwarding(VRF)을 각각 유지한다(VRF는 PE 라우터의 포트이다.). 데이터를 백본을 통하여 전송할 때 MPLS를 사용하면 PE 라우터는 Label Switch Router(LSR)의 기능을 한다. P 라우터는 CE장치에 연결되지 않은 P 네트워크의 라우터이고, 트래픽 포워딩이 MPLS를 이용해 백본의 PE와 PE사이를 통과할 때 LSR의 기능을 하고, P와 PE사이의 경로 유지를 요구하지만 CS 까지의 VPN 라우팅정보를 유지하는 것은 요구하지 않는다.[3]

III. VR 구성모델

VPN CS는 CE와 VR의 연결에 의해 P의 백본에 연결된다. 또, CE는 하나 이상의 VR에 미리 설정된 상태로 연결되어 있다. 다중 VR은 같은 PE에 공존하고 VR은 어떤 형태의 접속링크라도 사용 가능하며 CE 사이트는 전용회선 또는 dial-up 링크도 연결 가능하다. VR의 라우팅 테이블은 각 VPN의 Reachability information을 갖고 있다. 내부 백본의 P 라우터들은 VPN을 알지도 못하고 VPN 형태를 유지하지도 않는다. 그림 1은 VR이 사용된 참조모델이다.

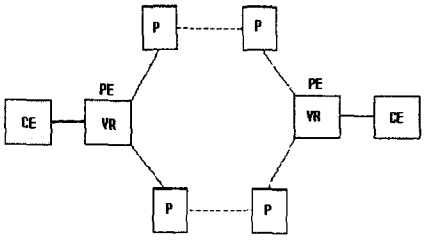

그림 1. VPN 참조모델

VR을 이용한 VPN은 2개의 주요 구축 시나리오를 가지고 있다. 첫 번째는 Layer 2로 연결된 PE사이에서 연결되는 VR이고 두 번째는 같은 PE에서 하나의 VR에 다른 VR이 다중으로 연결되는 것이다. 그림 2와 그림 3은 이 형태를 보여주고 있다.

첫 번째 시나리오에서는 Layer 2에서 사용되는 FR이나 ATM 혹은 다른 기술들이 사용되는 가운데 VR이 설치되고 이것은 VPN에 직접 연결된 형태로 서비스의 품질을 조절하고 이 연결은 정적 또는 동적인 설정이 가능하다.

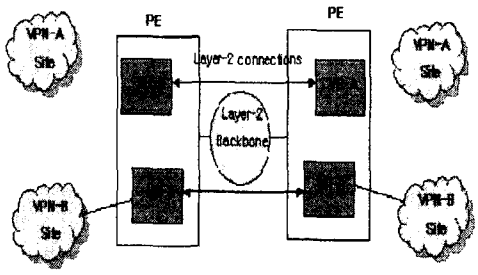

그림 2. Layer2 백본에 의한 VR간 연결

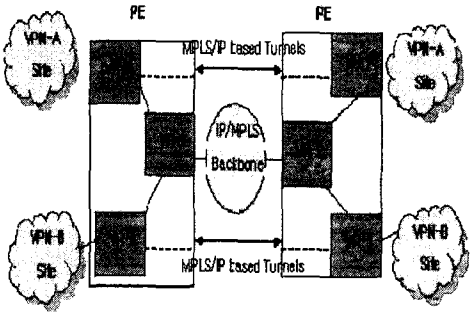

그림 3. 백본 VR을 통한 VR간 연결

두 번째 시나리오에서는 다른 형태의 VPN 설정이 단일 VR의 사용을 통해 다중 VR로 연결된다. 이때 단일 VR을 백본 VR이라고 하며 이것은 기능적으로 VR과 다르지 않다. 백본 VR은 공유된 백본을 이용해 PE사이를 연결하며 또, VPN VR의 집합을 허용해서 다른 VPN사이트가 부가되는 것의 영향을 받지 않는다. 이 시나리오에서 VR은 ATM, FR, IP, MPLS 사이에 설치될 수 있다.

VR 구성을 하는데는 터널링과 라우팅이 관계된다. 터널링에서 VPN 데이터와 라우팅 정보는 IP 또는 MPLS기반의 터널(IPSec, GRE, MPLS 등)을 사용하여 터널을 구성하고 있다. 또, 사용하는 터널기술에 따라 정적 혹은 동적 터널구성이 가능하고 이 터널들은 Point-to-Point의 형태로 VR구성에 나타난다. 백본 VR에서 보내어져 터널을 통과하는 트래픽은 기존의 백본 기술

(ATM, FR, Fast Ethernet 등)에서 분명하지 않다. 터널은 VPN 혹은 VR들 사이에서 공유되어 성립되고 VR이나 백본 VR에서부터 구성된다. 백본 VR은 VPN내부의 VR에 터널을 직접 연결한 것처럼 보이게 한다. 여기서 VR은 다른 VPN의 VR과 라우팅 정보를 직접 교환한다. 주목할 것은 터널의 형성은 VPN의 내부 연결성을 위해 서로 다른 형태로 구성될 수 있고 실제로 두 사이트에서는 MPLS와 IPSec을 선택적으로 사용한다.

라우팅에서는 서로 다른 백본 엔트리사이에서 백본 VR이 라우팅 정보를 교환하며 VR은 local VPN domain을 통해 동작하고 VPN 사이트들은 백본을 통한 터널을 이용해 라우팅 정보를 교환한다. 이 라우팅에서는 정적 혹은 동적 라우팅 프로토콜, 즉 기존에 사용되는 어떠한 라우팅 프로토콜이라도 사용이 가능하다.

마지막으로 VR과 백본VR의 관계를 살펴보면, 한 VPN에 관여하는 VR들의 라우팅 도메인의 구성은 백본 라우팅 도메인과는 관계가 없다. 따라서 백본 VR은 각 사설 VR에서 작동하는 라우팅에 대하여 알 필요가 없다. 그러나 백본 VR역시 VR이므로 사설 VR들이 필요로 한다면 관계성을 만들 수 있다.[2][4]

IV. BGP/MPLS 구성모델

그림 4에서는 단일 SP가 서로 다른 기업 고객끼리 BGP/MPLS VPN서비스를 전송하는 토폴로지를 보여준다. 여기서 두 PE 라우터는 네 개의 서로 다른 고객사이트에 연결되어 있는데 내부 사이트의 연결은 사이트 1과 사이트 2 사이에서 각 사이트의 어떤 호스트 간에 상호간 통신이 가능하고 사이트 3과 사이트 4사이에서도 역시 각 사이트간 동일한 동작을 할 수 있다.

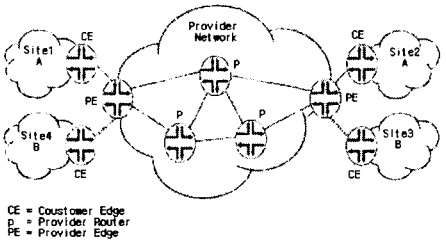

그림 4 네트워크 구성요소

BGP/MPLS모델에서는 기본적으로 일어나는 두 가지 트래픽의 흐름이 있다. VPN 경로의 분배와 LSP수립을 위해 사용되는 flow control과 고객의 데이터 트래픽을 forwarding하기 위해 사용되는 data flow이다.

flow control은 두 subflow로 다시 나누어지는데, 첫째, P 백본의 Edge에서 CE 라우터와 PE 라우터 사이의 라우팅 정보를 교환하고 P 백본을 통과하는 PE 라우터 사이에서 일어나는 라우팅 정보의 교환을 책임지고 있는 것과 둘째, PE 라우터 사이에서 P 백본을 지나는 LSP를 수립하기 위한 책임을 가지는 것이다. [5]

라우팅 정보의 교환에서는 RD와 VPN-IPv4 address family의 사용으로 주소공간을 중복해 사용하는 것을 허용하며 유사 속성을 확장한 BGP에 기반한 경로 필터링의 사용으로 PE 라우터들 사이의 라우팅 정보의 분배를 억제한다. LSP의 수립에서는 P의 백본을 통과하는 VPN 트래픽이 전송되는데 MPLS를 이용하기 위해서 LSP는 경로를 받아들이는 쪽의 PE 라우터와 경로를 알려주는 쪽의 PE 라우터 사이에서 수립되어야 한다. 또 LSP는 LDP나 RSVP를 사용하는 SP의 네트워크를 통과하여 수립될 수도 있다.[6][7]

data flow는 한 고객사이트로부터 다른 고객사이트로 SP의 백본을 통과하는 VPN 데이터 트래픽의 흐름이고 그림 5는 이것을 보여준다.

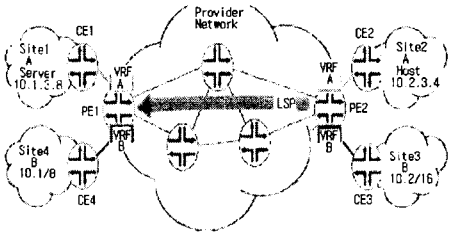

그림 5. BGP/MPLS 데이터 흐름

만약 사이트 2의 호스트 10.2.3.4가 사이트 1의 서버 10.1.3.8과 통신하려고 한다면 호스트 10.2.3.4는 자신의 default g/w에서 서버 10.1.3.8와 통신할 데이터(패킷)를 전송한다. CE2에 데이터가 도착해서 가장 알맞은 정보를 찾고 PE2로 IPv4패킷을 전송한다. PE2는 데이터를 받으면 VRF A에서 경로 찾기를 시작한다. 이때 PE2는 레이블 222인 경로 및 PE1에 의해 알게되는 MPLS 레이블, PE1의 경로를 위한 BGP의 다음 홉, LSP수립을 위한 최초의 MPLS 레이블 등의 정보를 포함한다. 사용자 트래픽은 레이블 222와 최초의 MPLS 레이블을 포함하는 레이블 스택으로 MPLS를 통해 PE2에서 PE1으로 전송된다.

이때 PE2는 LSP를 위한 내부로 들어오는 쪽의 LSR이 되고 PE1은 외부로 나가는 쪽의 LSR이 된다. PE2는 데이터를 전송하기 전에 하위 레이블을 만들기 위한 레이블 스택에 레이블 222를 포함하는데 이것은 PE2가 경로 10.1/16을 위해 PE1의 IBGP의 알림을 받은 후에 실제로 VRF A

에 설치된다. 다음으로 PE2는 상위 레이블을 만드는 레이블 스택을 통해 LDP나 RSVP에 기반한 LSP와 결합된 레이블을 PE1에 포함시킨다. 레이블 스택을 만든 후에 PE2는 PE1으로 향하는 LSP의 첫 번째 P 라우터에서 외부로 나가는 인터페이스를 통해 MPLS 패킷을 보낸다. P 라우터는 상위 레이블에 근거하여 P 백본 네트워크의 Core를 통과하는 패킷을 교환한다. PE1에서 패킷을 받았을 때 만들어진 IPv4레이블을 읽어들이고 PE1은 10.1/16에서 다음 홉인 CE에 직접 연결되는 것을 확인하는 하위 레이블 222를 사용하고 최종적으로 PE1은 사이트 1의 서버 10.1.3.8로 패킷을 보내는 역할을 하는 CE1으로 IPv4패킷을 보낸다.[8]

V. 비교 및 전망

VR과 BGP/MPLS의 구조는 단독으로 사용될 수도 있고 복합적으로 사용될 수 도 있다. VR은 PE에 존재하며 기존의 물리적 라우터와 하드웨어적이나 소프트웨어적으로 같은 역할을 한다. 따라서 모든 구성, 동작, 문제해결, 모니터링 등의 설정은 기존의 라우팅 프로토콜의 메커니즘을 따른다. VR구조는 VPN-ID를 이용하여 각 VPN을 확인하고 라우팅을 하는데 있어서 기존의 라우팅 프로토콜을 사용할 수 있다. 백본 VR을 통해 다중 VR의 형태를 지닐 수 있다. 내부의 VPN은 각각의 VR을 가지며 백본 VR을 통해서 P의 백본을 통과한다. VR의 연결은 백본을 통할 때 VR대 VR연결을 하고 이후 VR대 CE의 연결구조를 가진다.

BGP/MPLS는 PE 라우터 VRF라는 라우팅 테이블을 가지고 있고 VRF는 다중 CE 라우터와 결합 될 수 있다. CE 라우터를 기준으로 내부 VPN이 구성된다. VRF는 PE의 포트이기 때문에 다중으로 존재한다. 연결구조는 P의 백본을 통과하여 PE 라우터와 PE 라우터 사이를 연결하는 LSP를 수립한다. 이때 각 PE 라우터는 LSR이 된다. PE 라우터의 VRF는 각 CE 라우터를 구분하며 CE 라우터에서 내부 VPN의 호스트를 구별한다. 이 구조에서는 RD와 VPN-IPv4가 사용된다.

최종적으로 네트워크 기반 VPN은 IP VPN 서비스는 크게 공중망을 사용하고 IP address를 사용한다는 관점에서 볼 때 일맥 상통한다. 따라서, 현재 VR과 BGP/MPLS의 보안, Scalability, QoS 등에 관해 RFC문서와 Internet Draft에서 계속 제안되고 있으며 VPN에 대한 관심 역시 고조되고 있을 뿐만 아니라 일부 상용화 되어있으며 향후 계속 발전될 전망이다.

참고문헌

[1] Gleeson, B., et al., A Framework for IP based Virtual Private Networks, RFC 2764, February 2000

[2] Ould-Brahim, Gleeson., et al, Network based IP VPN Architecture using Virtual Router,<draft-ietf-ppvpn-vpn-vr-oo.txt>, July 2001

[3] Rosen E., et al, BGP/MPLS VPNs, <draft-ietf-ppvpn-rfc2547bis-00-txt>, July 2001

[4] ITU-T, Draft Recommendation Y.IPVPN, Study Group 13, Q20/13, May 2000

[5] Ramachandra, Tappan, and Rekhter, BGP Extended Communities Attribute,<draft-ramachandra-bgp-ext-communities-08.txt>, January 2001

[6] Jamoussi, B., et al, Constraint-based LSP Setup using LDP, Work in Progress.

[7] Chen and Rekhter, Cooperative Route Filtering Capability for BGP4,<draft-ietf-idr-route-filter-02.txt>,November 2000

[8] Rosen E., et al, BGP/MPLS VPNs,<draft-rosen-rfc2547bis-02.txt>, July 2000