MPLS-VPN 기술과 엔터프라이즈 망에서의 적용 사례

김철용°, 오석희, 이성호
LG CNS 사업지원본부 인프라솔루션사업부 네트웍서비스센터 통신기술연구소
{cyoungkim,shoh,shlee}@lgcns.com

MPLS-VPN architectures and Transition Instances of Enterprise Network

Cheulyoung Kim°, Seokhee Oh, Seongho Lee
Telecommunication Technology Institute.
Network Service Center Infra Solution Division LG CNS

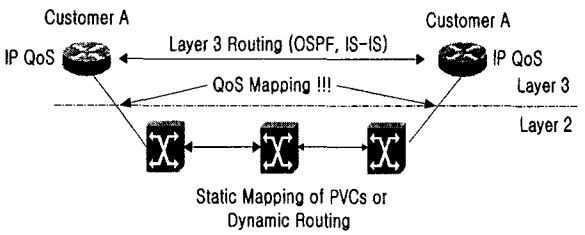
요 약

대부분 기업들의 본사와 지사처럼 위치상으로 멀리 떨어져 있는 소속 네트웍들의 연결은 Service Provider를 통한 VPN을 이용한다. 트래픽이 대용량화 되고 서로 다른 네트웍 간에 보안도 중요한 문제로 부상하는 상황에서 기존의 Layer 2 또는 Layer 3 VPN의 단점을 보안한 MPLS-VPN의 적용은 Service Provider로서는 한 가지 해결책이 될 수 있다. Service Provider 측면에서 MPLS-VPN 기술에 대해 요약하고, Service Provider로서 백본을 제공, 운영하는 LG CNS에서 기존 고객사 네트웍을 MPLS-VPN으로 전환한 사례를 들어 실제 적용 방법을 소개하고자 한다.

1.MPLS-VPN

1.1 Layer2 vs Layer3 VPN

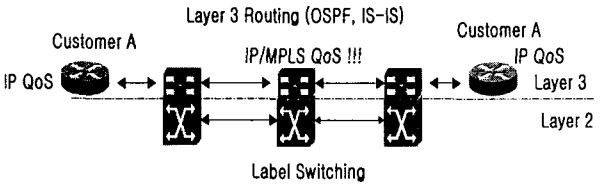
VPN은 리모트에 위치해 있는 네트웍을 Service Provider가 제공하는 공유망을 이용하여 사설 백본처럼 사용하는 서비스 이다. MPLS-VPN은 layer3 VPN 기술 중 하나로 [그림 1]에서 보이는 기존의 layer2 VPN의 단점인 IP-QoS mapping문제, 새로운 고객사 추가 시 VC 설정문제 등과 [그림 2]의 layer3 VPN의 단점인 core provider router가 customer route 정보를 모두 가져야 하는 등의 단점들을 해결하여 layer 2의 장점인 빠른 traffic forwarding, core device들이 customer routes에 관여하지 않는 점들과 layer 3의 장점인 간단한 새 customer 네트웍 추가, IP QoS mapping 들을 얻을 수 있는 VPN에 활용도가 높은 기술이다[1][2].



[그림 1] Layer 2 VPN Architecture

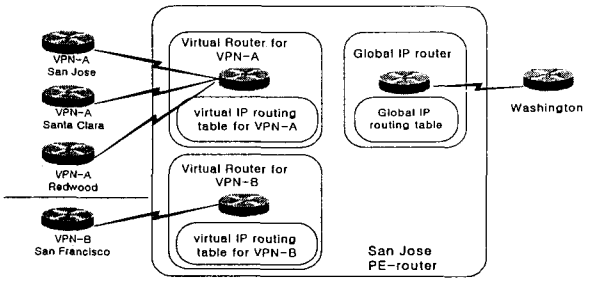
1.2 MPLS-VPN의 Routing

[그림 3]과 같이 customer network에 MPLS-VPN을 제공하는 경우 하나의 Provider Edge router(PE)는 각각의 VPN customer sites의 routes 정보를 가지고 있는 Customer Edge Router(CE)과 routing peer로 동작한다. 또한, 중간의 P (core) router는 이러한 routing 정보 전송에 관여하지 않고,PE-router 만 customer routes 정보를 주고 받는다.



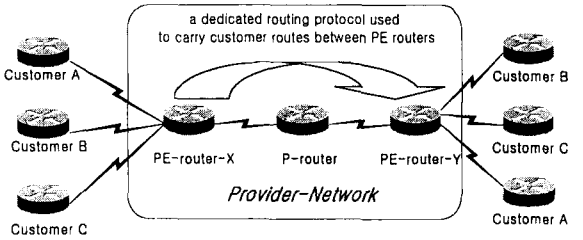
[그림 2] Layer 3 VPN Architecture

각 VPN site의 routes 정보를 논리적으로 분리된 VRF(Virtual Routing and Forwarding Table)에 따로 관리한다. 또, provider network 내부의 routes 정보는 global routing table을 사용하여 저장하고 인접 router들과 IGP로 OSPF와 IS-IS 등을 이용한다. CE router와 PE router 사이에는 Static, RIP version 2, OSPF, eBGP 등의 routing protocol을 사용하여 routes 정보를 수집한다.



[그림 3] PE router의 논리적인 구성

MPLS-VPN에서는 PE router와 리모트의 PE router간에 [그림 4]처럼 iBGP4를 MPLS-VPN에 적합하게 확장한 MP-BGP (MultiProtocol-BGP)를 사용한다[1][2][3].



[그림 4] PE-routers 간 MP-BGP protocol 사용

PE router의 논리적 구성과 MP-BGP와 관련된 동작을 좀 더 세부적으로 설명하면 하나의 PE router는 연결된 VPN customer network를 관리하는 하나의 VRF를 정의하고, 각 VRF에는 customer의 private IPv4 address를 unique하게 만드는 64bit 길이의 RD (Route Distinguisher)와 리모트 PE router로부터의 MP-BGP update 정보를 import/export할지 결정하기 위한 64bit RT(*Route Target*)을 정의 한다. 즉, 하나의 VPN site가 여러 VPN에 속할 수 있으므로 MP-BGP 정보와 함께 전달되는 RT을 보고 VRF별로 customer route 업데이트를 판단하게 된다[1]

1.3 PE-CE router 간의 Routing 설정

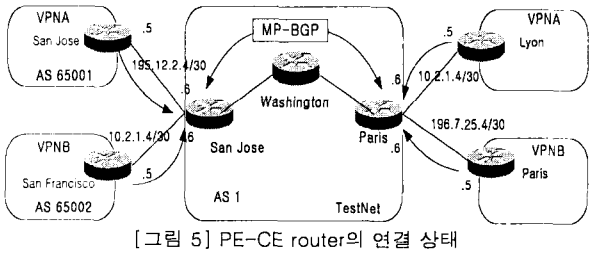
MPLS-VPN을 적용하기 위해서 기존 Service Provider의 PE router에 다음과 같은 과정의 설정이 필요하다.

① VRF를 구성하고 정의 한다.
② Route Distinguisher를 정의하고 구성한다.
③ import and export policy를 정의 하고 구성한다.
④ 앞에서 정의한 VRF에 CE-interface를 연결시킨다.
⑤ PE-CE links를 configure한다.
⑥ MP-BGP protocol을 configure한다.

위의 PE-CE link 구성 중 여러 routing protocol에 따른 *configuration*을 다음에서 보인다[1].

1.3.1 Static Routing

PE router에서 customer route를 static하게 지정하고 이 정적 route 정보를 같은 router내의 BGP protocol로 redistribute 시킨다. 이 구성은 [표 1]과 같은 설정을 필요로 한다[1].



[그림 5] PE-CE router의 연결 상태

1.3.2 RIPv2 Routing

[그림 5]와 같은 구성에서 PE-CE router 간의 RIPv2 protocol을 사용하여 customer routes를 PE-router와 송수신하는 설정을 [표 2]에서 보인다[1]. 그 외에 OSPF, eBGP 등의 routing protocol을 이용한 CE-PE router간 routing update 설정이 가능하다.

1.4 PE router 사이의 Label allocation and Distribution

동일한 목적지 customer routes 정보를 FEC (Forwarding Equivalent Class)로 구분하고 같은 FEC에 대해 SP내의 device

[표 1] Paris PE-router의 static configuration

```
paris (config)# ip route vrf VPNA 10.2.1.0 255.255.255.0 serial0
paris (config)# ip route vrf VPNB 196.7.25.0 255.255.255.0 serial1
```

```
router bgp 1
!
address-family ipv4 vrf VPNB
 redistribute static
 no autosummary
 no synchronization
exit-address-family
!
address-family ipv4 vrf VPNA
 redistribute static
 no autosummary
 no synchronization
exit-address-family
```

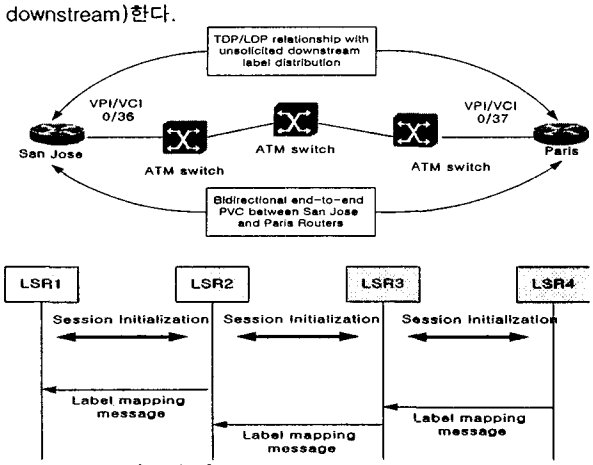
[표 2] San Jose PE-router의 RIPv2 configuration

```
hostname San Jose
!
ip vrf VPNB
 rd 1:27
 route-target export 100:27
 route-target import 100:27
!
ip vrf VPNA
 rd 1:26
 route-target export 100:26
 route-target import 100:26
!
interface loopback0
 ip address 194.22.15.2 255.255.255.255
!
interface serial0
 description **interface to VPNB San Francisco **
 ip vrf forwarding VPNB
 ip address 10.2.1.5 255.255.255.252
!
interface serial1
 description **interface to VPNA San Jose **
 ip vrf forwarding VPNA
 ip address 195.12.2.5 255.255.255.252
!
router rip
 version 2
!
address-family ipv4 vrf VPNB
 version 2
 redistribute bgp 1 metric 1
 network 10.0.0.0
 no auto-summary
exit-address-family
!
address-family ipv4 vrf VPNA
 version 2
 redistribute bgp 1 metric 1
 network 195.12.2.0
 no auto-summary
exit-address-family
```

```
router bgp 1
!
 no bgp default ipv4-unicast
 neighbor 194.22.15.3 remote-as 1
 neighbor 194.22.15.3 update-source loopback0
 neighbor 194.22.15.3 activate
 neighbor 194.22.15.1 remote-as 1
 neighbor 194.22.15.1 update-source loopback0
!
address-family ipv4 vrf VPNB
 redistribute rip metric 1
 no auto-summary
 no synchronization
exit-address-family
!
address-family ipv4 vrf VPNA
 redistribute rip metric 1
 no auto-summary
 no synchronization
exit-address-family
!
address-family vpnv4
 neighbor 194.22.15.3 activate
 neighbor 194.22.15.3 send-community extended
 neighbor 194.22.15.1 activate
 neighbor 194.22.15.1 send-community extended
exit-address-family
```

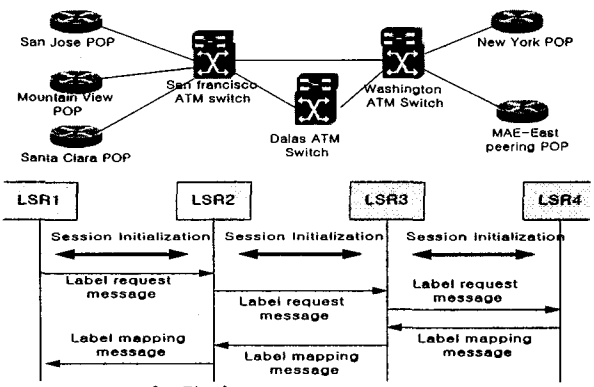
간에는 LDP(Label Distribution Protocol) 또는 TDP(Tag Distribution Protocol)를 이용하여 label을 할당하고 서로 교환한다[4].

[그림 6]과 같은 Pure router-based network 혹은 frame-mode ATM network의 SP는 모든 내부 router 들에서 IGP를 통해 core network의 routes들에 대해 독립적으로 label 할당(independent label allocation)과 label request 수신 없이도 upstream node에 label mapping을 임의로 전달(unsolicited downstream)한다.



[그림 6] Frame-mode MPLS-VPN

반면 [그림 7]과 같은 cell-mode ATM network은 label request message가 최종 egress-router까지 전달된 후 label이 할당(downstream on demand)되고 원래 요청 PE-router까지 label binding이 순서대로 이뤄지는 방법으로 FEC-to-Label binding이 이뤄진다(ordered control). 이 정보들은 SP의 모든 router 내에 LFIB(Label Forwarding Information Base)로 저장되어 label swapping에 사용된다[4].



[그림 7] Cell-mode MPLS-VPN

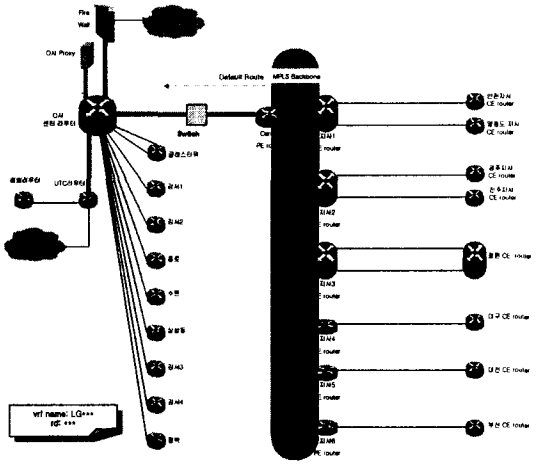
2. MPLS-VPN 전환사례

2.1 Enterprise Network topology

ATM switch로 구성된 LGCNS backbone은 [그림 6]과 같은 PE-router 간 point-to-point connection으로 설정된 Frame-mode MPLS로 전환하였다. 고객사의 지역 site와 트윈타워의 센터 사이트의 PE-router에는 다른 고객사 VPN간 통신을 제공하는 VRF를 가지고 있고 Internet 접근이나 서버 존에 접근을 제공하는 Central service zone으로 구성되어 있다[5].

2.2 고객사 망의 MPLS-VPN 전환

ATM backbone으로 VPN을 사용했던 한 고객사 망을 MPLS-VPN으로 전환한 사례이다. PE-CE간에 Static Routing으로 configuration을 설정하였고, 인터넷 접근은 센터 사이트에서 제공하는 경로를 사용한다[6].



[그림 8] LG 고객사의 MPLS-VPN 전환 망

3.결론

ATM B/B의 layer 2 VPN은 빠른 packet switching의 이점 대신 customer site 추가 시 여러 스위치에서 PVC 설정이 필요하며 IP packet을 layer 2 frame으로의 QoS mapping 문제가 발생한다.

MPLS-VPN으로 전환함으로써 layer 2 VPN의 빠른 switching과 함께 customer site 추가 시 단순한 구성, customer routes 전달의 효율성, IP packets의 QoS mapping 문제가 생기지 않는 등의 장점을 가진다. 또한 다수의 고객사에 VPN을 통한 Internet access를 제공하는 현재 enterprise 망 상황에서 PE-router내 완전히 분리된 고객사 routes tables을 사용함으로써 다른 고객사로부터의 해킹이나 바이러스, 웜 등을 피해를 원천적으로 차단할 수 있다는 점들과 같은 기존의 VPN에서 구현할 수 없었던 서비스가 가능해 졌다.

4. 참고문헌

[1]Jim Guichard, Ivan Pepelnjak, " MPLS and VPN Architectures" , Cisco Press.

[2]Peter Tomsu, Gerhard Wieser, " MPLS-Based VPNs: Designing Advanced Virtual Networks" , Prentice Hall, 2002.

[3]Ivan Pepelnjak, " MPLS VPN Technology" , World Wide Training Word Templates v1, Cisco Systems Inc, 1999.

[4]Cisco Systems Inc, " MPLS Label Distribution Protocol (LDP)" , Cisco IOS Release 12.0(22)S.

[5]오석희, " MPLS VPN Routing Scheme" , presentation 자료, LG*Net팀 NSC LGCNS, 6.2002.

[6]이성호, " MPLS VPN 전환-LG 0사" , presentation 자료, LG*Net팀 NSC LGCNS, 10.2002.

etc