Cisco 7609s에서 VPLS 구성 및 QoS

작성자: 김민아, 공정욱, 홍원택

연구망개발팀, 고성능연구망사업단, 한국과학기술정보연구원
{petimina, kju, wthong}@kisti.re.kr

최종수정일: 2007년 11월 28일

Abstract

협업연구가 활성화됨에 따라 연구망 사용자들은 연구데이터의 교환이나 화상회의 화상 교육을 위한 연구 그룹끼리의 가상 사설망에 대한 요구가 높아지고 있다. 본문에서는 이러한 원거리에 있는 연구자 그룹 통신이 가능한 가상 사설망 서비스를 제공할 수 있는 VPLS 기술에 대해 알아보고, 연구망을 구성하고 있는 주요 장비인 시스코 장비 중 VPLS를 지원하는 7609s 에서 VPLS 기능을 시험해 봄으로써 연구망상에서 VPLS를 이용한 가상 사설망 서비스의 가능성에 대해 알아본다.

Topics

1. 서론

연구망의 주요 사용자들은 지리적으로 떨어져 있으나 데이터 공유가 필요한 협업 연구자들이다. 이들의 요구를 크게 분류하면, 먼저 1:1 통신을 통한 대용량 데이터 전송에 대한 요구로 고에너지 물리, 천문, 기상 분야 등이 있다. 두 번째는 지리적으로 떨어진 연구자 그룹 간 데이터 교환에 있어 다른 데이터의 침입을 받지 않는 연구자 그룹 VPN에 대한 요구이다. 첫 번째 요구의 경우 현재 연구망에서는 고 대역폭의 백본망과 UCLP를 사용한 전

용 lambda를 특정 응용에 할당해 줌으로써 이를 만족시킬 수 있는 서비스를 제공하고 있다. 그러나, 현재 두 번째 요구에 대해 연구망은 특별한 서비스를 제공하고 있지 않다.

VPLS는 원거리에 있는 사용자에게 하나의 가상 LAN 을 제공함으로써, 다자간 통신 기능을 제공한다. 현재 북미와 유럽 시장을 중심으로 해외 통신시장에서는 VPLS를 이용한 트리플 플레이 서비스를 제공하고 있다.

본 문서에서는 이러한 VPLS 를 이용하여, 지리적으로 떨어져 있는 연구자 그룹에 하나의 VPN을 제공해 주는 프리미엄 VPN 서비스를 위해 VPLS를 KREONET에 도입하고자, KREONET의 주요구성 장비인 cisco router 7609상에서 다양한 연구 그룹 구성을 위한 VPLS를 시험하고 그 가능성을 살펴본다.

2. VPN 기술

IP 백본들은 전통적으로 인터넷 액세스를 제공하기 위해 사용되어져 왔으며, 최근에는 VPN 액세스를 제공하기 위해 사용되어지고 있다. 최근 가장 많이 사용되고 있는 VPN 기술들은 크게 세 가지로 나눌 수 있다.

2.1 IP VPN

IP VPN 은 BGP VPN을 기본으로 한 Layer3 MPLS VPN기술이라 할 수 있다. 고객의 사이트는 공유하는 IP 백본 상에서 사설망을 구성할 수 있는 IP router 들을 통해서 연결된다. 현재 80 개 이상의 캐리어들이 다양한 사이트들 사이에 IP VPN을 운영하고 있다. IP VPN은 동적이고 유연하며, 확장성을 보장해 준다. 또한 전용선과 같은 기존 서비스 상에서도 동작할 수 있다. 그러나, IP VPN은 multi-protocol LAN 을 지원하지 않으며, IP로 encapsulate되지 않은 SNA나 IPX같은 기존의 트래픽을 지원하지 않는다. 또한, 관리하기 힘들고, 고비용이라 새로운 이더넷 환경에서 단순성과 효율성 비용 측면을 고려할 때, 최선의 선택이라 할 수 없다.

2.2 Ethernet Virtual Private Line

Ethernet Virtual Private Line 서비스는 Pseudo-wires, Martini Tunnel 로 알려져 있는 Layer2 MPLS VPN 기술을 사용한다. 이들 프로토콜은 이더넷, ATM, Frame Relay, SDH, TDM 등 어떤 트래픽도 운반할 수 있다. Martini tunnel 로 고객은 하나의 전용선을 가진 것처럼 point-to-point circuit으로 통신할 수 있다. 그러나, Martini의 접근은 하나의 meshed network을 만들 때 사용되는 Frame Relay 나 ATM 과 유사한 문제를 가지고 있다. 즉 n개의 지역을 연결할 때, n*(n-1)개의 연결을 가져야 한다.

2.3 Virtual Private LAN Service(VPLS)

IP VPN 이나 Ethernet Virtual Private Line 서비스의 문제를 해결하기 위해 보다 나은 확장성을 제공함과 동시에 multipoint-to-multipoint 서비스를 제공하는 MPLS Layer2 기술인 VPLS가 등장하였다.

VPLS 서비스의 주목적은 지리적으로 떨어져 있는 여러 사이트들이 하나의 LAN switch (L2)에 연결되어 있는 것과 동일한 효과를 제공해주는 것이다. 즉, 각 site의 CE(Custimer Edge)에서 VPLS망으로 유입된 이더넷 프레임은 변형되지 않고 그대로 해당 사이트로 전달된다. 따라서, 사용자는 마치 하나의 private LAN에 연결된 것처럼 느낀다.

하나의 VPLS를 생성하기 위해서는 VPLS instance를 생성하여 각 라우터에서 그 VPLS를 통해 데이터를 보낼 때 사용할 레이블인 vc-label(Virtual Circuit)을 서로 주고 받아야 한다. 이렇게 레이블 교환이 있은 후, vc-lsp 가 생성되면, 데이터를 주고 받을 수 있게 된다. 이 때 point-to-point circuit 과 달리 VPLS 서비스에서는 도착한 프레임의 목적지가 여러 개이다. 따라서, 어느 사이트로 프레임을 전달해야 할 지 알아내야 하는 데, 이를 위해 각 PE는 vc-lsp별로 MAC address를 관리/학습하고 있어야 한다. 즉, VPLS에 참여하는 PE는 VPLS별로 configuration 정보를 가지고 있어야 하며, 각 인터페이스별로 MAC address를 학습하고 있어야 한다. MAC learning 을 통해 FIB(forwarding information base)를 생성하여 하나의 포워딩 테이블을 만듦으로써, VPLS를 통한 데이터 통신이 가능하게 된다.

3. Virtual Private LAN Service

Virtual Private LAN Service(VPLS)는 MPLS 기술을 이용해 이더넷 VPN을 제공하는 것으로 보다 나은 확장성, 단순성, 관리성, 품질성, 안정성을 목표로 하고 있다. 이 때문에, 향후 통신 사업들의 수익 창출에 있어 주요한 서비스가 될 프리미엄 이더넷 VPN, 트리플 플레이 서비스, 모바일 백홀을 가장 잘 지원할 수 있는 기술로 여겨진다. 연구망에서 VPLS는 대역폭과 보안을 보장해 주는 프리미엄 이더넷 VPN 서비스를 위해 도입을 고려하고 있다. 본 절에서는 이러한 VPLS로 하나의 VPN 이 생성되는 과정을 살펴봄으로써, VPLS의 상세 기술에 대해 알아본다.

3.1 VPLS instance 의 생성과 vs-lsp의 생성

먼저, 하나의 VPLS 를 만들기 위해, 운영자가 PE1, PE2, PE3 에 각각 VPLS instance를 생성하면, 이 VPLS instance에는 unique 한 VCID가 할당된다. 이후 각 PE들은 동일한 VPLS instance 에 속하는 PE 들을 찾아 이들에게 signaling 을 통해 vc-lsp를 위한 label을 배포하여야 한다. 이 과정을 위한 표준은 크게 draft-ietf-ppvpn-vpls-ldp와 draft-ietf-ppvpn-vpls-bgp 가 있으며, draft-ietf-ppvpn-vpls-ldp 는 알카텔-루슨트 진영에서, draft-ietf-ppvpn-vpls-bgp 는 주니퍼 진영에서 표준화를 주도하고 있다.

Figure 1은 PE들이 동일한 VPLS instance 에 속하는 PE들을 찾은 후, LDP로 vc-lsp 생성을 위해 label을 주고 받는 과정을 보여준다. 각 PE들은 Label Mapping Message를 통해 이러한 작업을 수행한다. 먼저, PE1은 PE2에게, VCID 17로 데이터를 보낼 때는 vc-label 200을 써서 보내달라고 요청한다. PE3에게는 VCID 17로 데이터를 보낼 때, vc-label 500을 써서 보내달라고 요청한다. PE2와 PE3도 이러한 과정을 거친다.

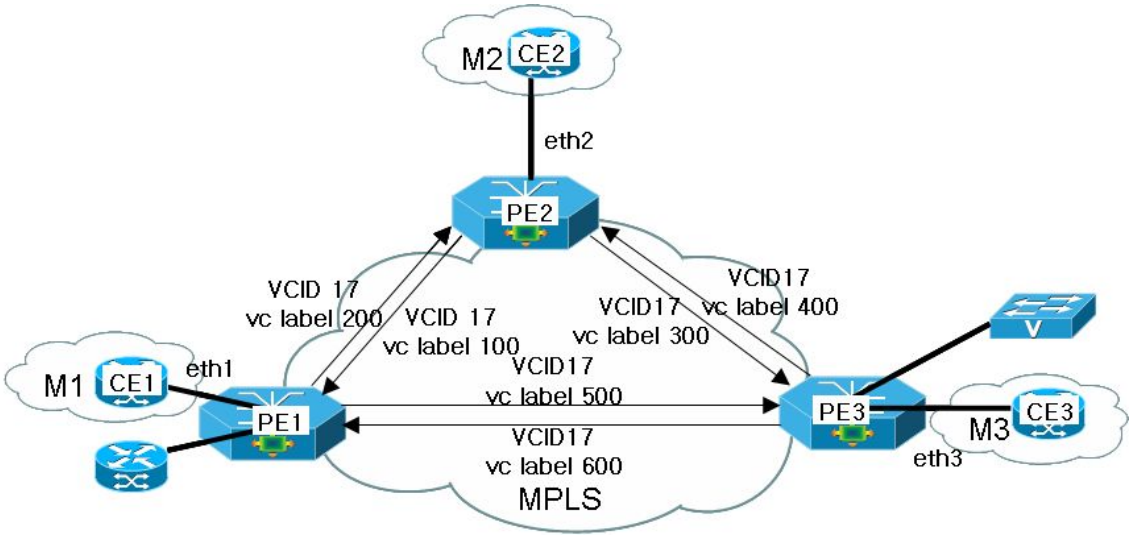

Figure 1. VPLS Signaling

이러한 과정이 끝나면 PE1, PE2, PE3 사이에는 vc-lsp 가 생성되고, 각 PE에서, 이 VPLS를 사용할 CE가 연결된 인터페이스(eth1, eth2, eth3)를 설정해주면 하나의 VPLS domain이 생성된다.

3.2 FIB 와 MAC learning

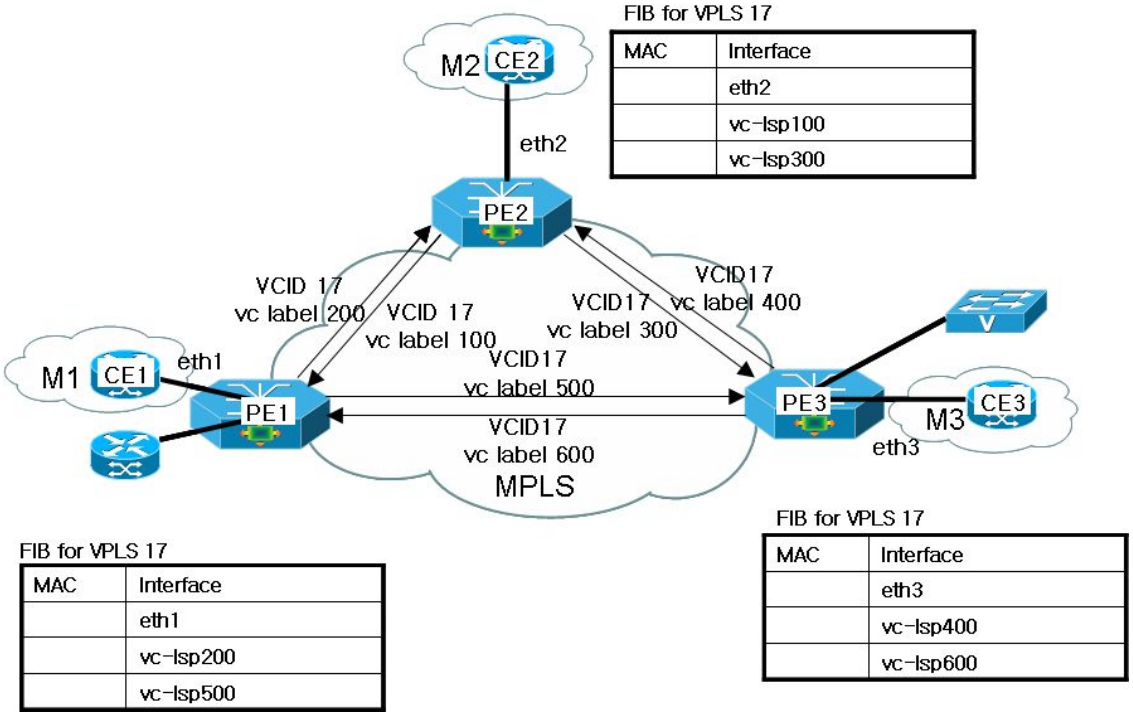

Figure 2. FIB Creation for a VPLS instance

하나의 VPLS domain 이 생성되면, 각 PE들은 이제 데이터를 보낼 준비가 끝났다. 그러

나, 이것은 아직 완전하지 않다. 이를 테면, PE1에 CE3 로 보내는 데이터가 왔을 때, PE2 로 포워딩해야 할 지 PE3 로 포워딩해야 할 지에 대한 정보가 아직 없기 때문이다. 이러한 정보를 담고 있는 테이블이 Forwarding Information Table(FIB)로 이 FIB 는 실제 데이터가 보내지는 시점에서 채워진다. VPLS의 생성이 끝나면, 각 PE 들은 Figure 2와 같이 아직 비어 있는 FIB를 가지게 된다.

CE1에서 데이터를 보내기 시작하면 첫 번째 데이터 프레임이 도착했을 때, PE1은 eth1 으로 들어온 source MAC address M1 을 보고 eth1 에 M1을 채운다. 아직 PE1 은 destination 인 M2가 어디에 있는지 모르므로 VCID17에 속한 PE2와 연결된 vc-lsp200 과 PE3와 연결된 vc-lsp500에 도착한 프레임을 복사하여(replication) 하여 전달(flooding)한다. 이때, PE2에는 vc-lsp200을 통해 label 200과 tunnel label 그리고 L2 header 들을 붙인 MPLS 프레임을 전송한다.

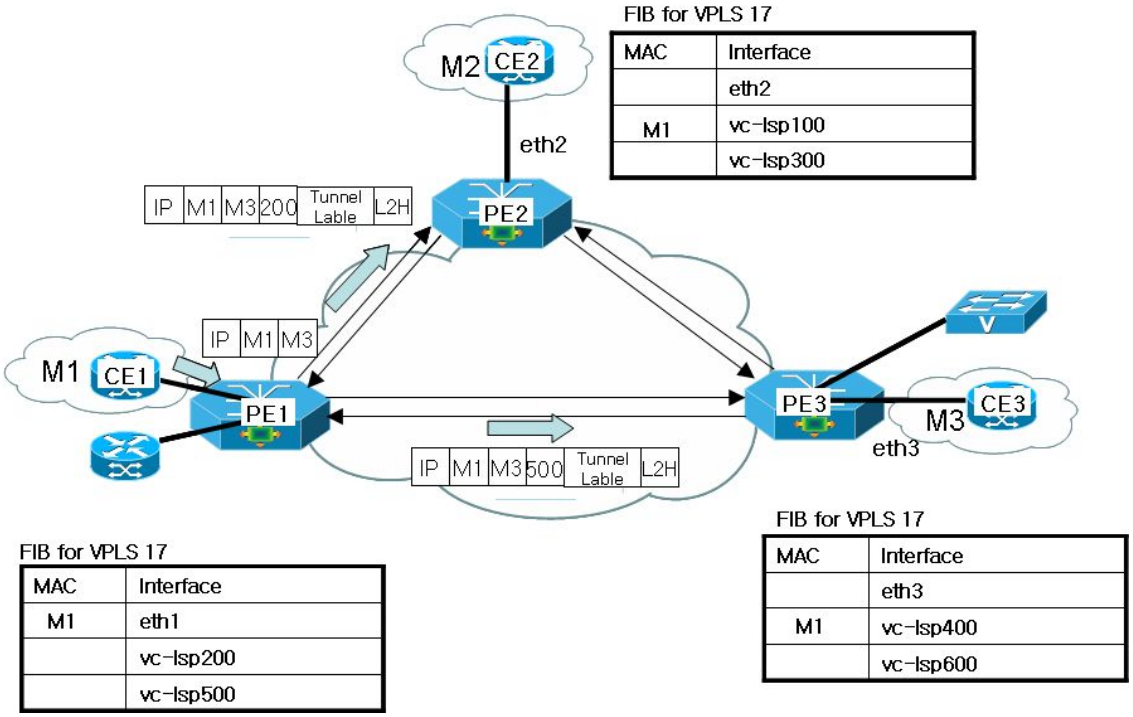

Figure 3. Step 1: Filling FIB table step

PE3에는 vc-lsp500을 통해 label 500 과 tunnel label 그리고 L2 header 들을 붙여 전송한다. MPLS 프레임을 받은 PE2는 도착한 프레임의 vc-label 값을 참조하여 그 프레임이 어느 PE로부터 왔는지 알 수 있으며, 그 PE 뒤에 source MAC address M1이 있음을 알 수 있다. 따라서, PE1과 연결된 vc-lsp100에 M1을 채운다. PE3 도 이와 동일한 과정을 거쳐 vc-lsp400에 M1을 채운다.

PE2는 FIB에서 아직 destination 인 M2를 찾을 수 없으므로, 이를 다시 복제하여 전달한다. 이 때, loop을 방지하기 위해 vc-lsp 들로는 전달하지 않고 연결된 이더넷 포트로만 전달한다. 따라서, Figure 3 에서 PE2는 eth2 로만 프레임을 전달한다. PE3 역시 마찬가지

로 eth3 으로만 프레임을 전달한다. CE2와 CE3는 자신의 MAC address를 확인하고, destination MAC 이 일치하는 M3 많이 PE3로 eth3를 통해 프레임을 전송한다. 이를 받은 PE3는 eth3를 통해 들어온 source MAC address M3를 FIB에 채우고, 이를 다시 vc-lsp400과 vc-lsp600으로 전송한다.

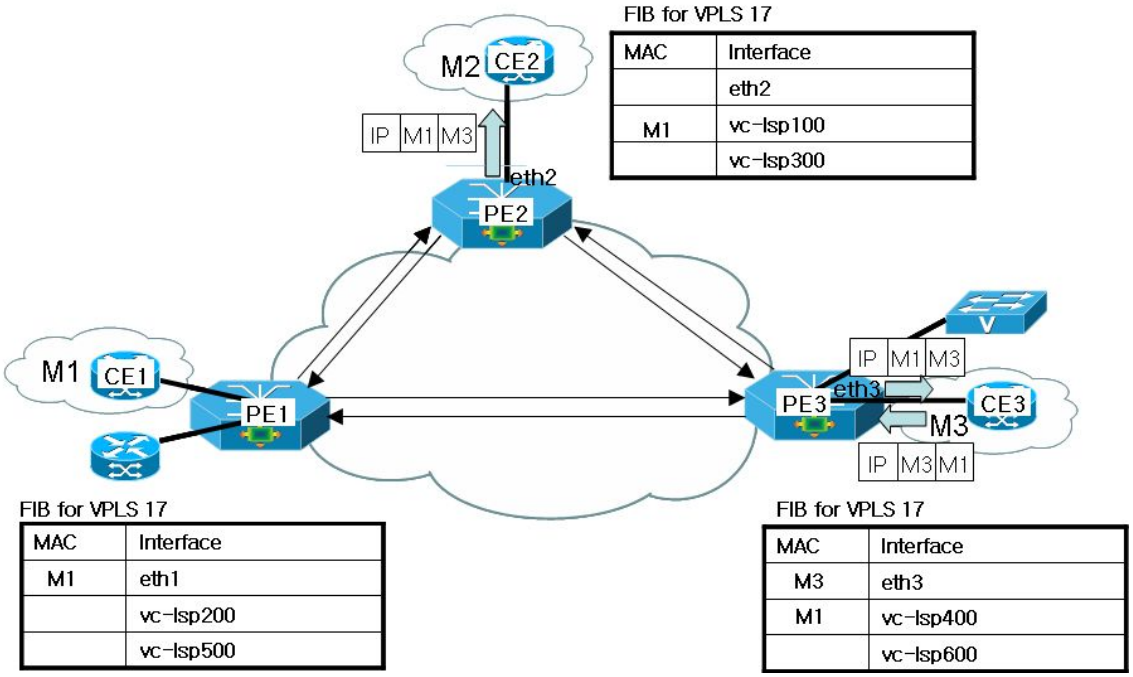

Figure 4. Step 2: Filling FIB table step

Figure5 에서 이를 받은 PE2와 PE1은 vc-lsp 정보를 통해 이 프레임이 어느 PE로부터 왔으며, 그 PE 뒤에 M3가 위치함을 알고 PE3와 관련된 vc-lsp500과 vc-lsp300에

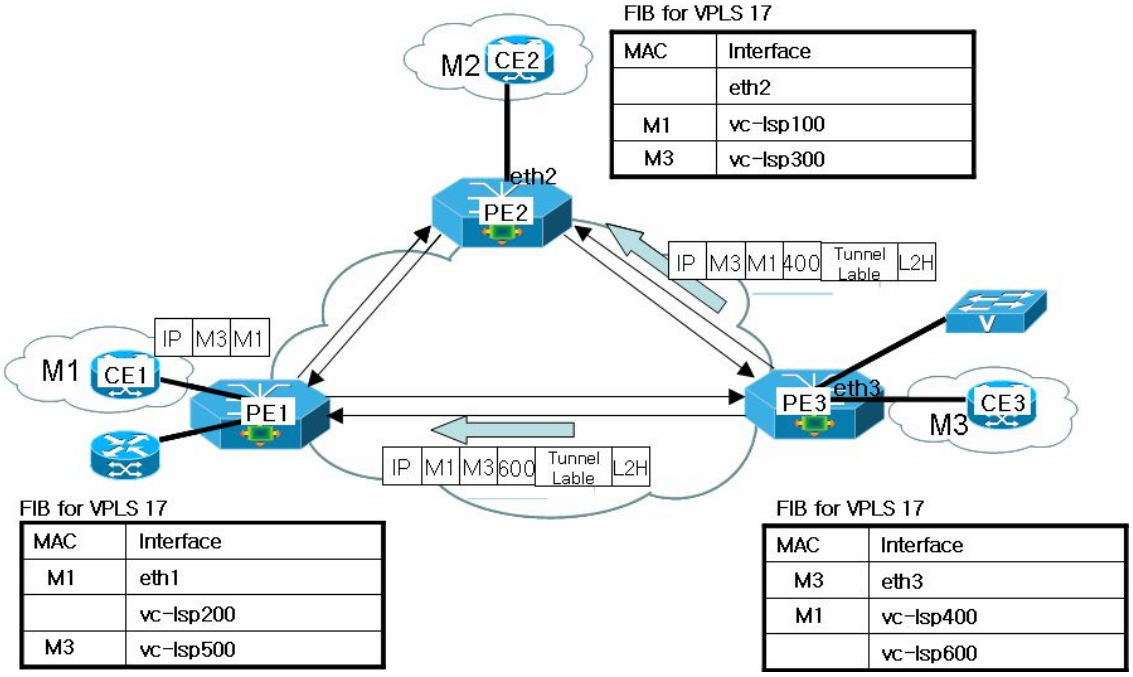

Figure 5. Step 3: Filling FIB table step

source MAC M3를 채운다. 다음으로 프레임을 전송할 detination MAC 이 FIB에 존재하는지 확인한 다음 존재할 경우 그 인터페이스로 프레임을 포워딩한다. Figure에서 PE1은 eth1 으로 이를 전송하고, M1 이 FIB에 있으나, vc-lsp 에 있으므로 PE2는 어떤 데이터도 전송하지 않게 된다.

CE1이나 CE3 가 CE2 에 데이터를 보내게 될 경우, 동일한 과정을 통해 FIB는 모두 채워지게 된다. 이러한 과정을 거친 후 FIB가 모두 채워지게 되면, 이 후에 보내지는 데이터들은 FIB를 참조하여 정확한 destination으로만 포워딩할 수 있게 된다.

4. 시스코 장비에서 VPLS 가상 사설망 시험

현재 연구망은 시스코 장비로 구성되어 있으므로 시스코 장비에서 VPLS를 적용함으로써, 연구망에서의 VPLS 적용 가능성을 살펴보기로 한다. 시험은 KREONET상에 광 장비 시험을 위해 구축된 테스트 베드인 ONLab(Optical Network Laboratory)에서 진행되었다.

ONLab은 Cisco 7609 장비의 ONS 15600, ONS 15454 로 구성되어 있으며, 대전의 ONS 15600과 광주의 ONS 15454를 통해 대전 광주 간을 연결하고 있다.

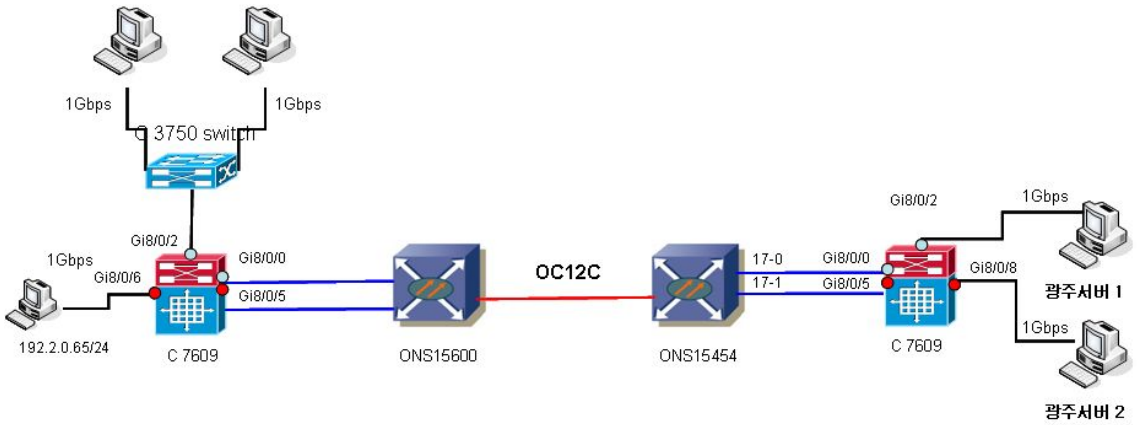

Figure 6. VPLS test network topology

ONS15600과 ONS 15454 상의 link 는 OC12C 로 각 서버들의 네트워크 카드와 라우터 스위치의 port 들의 최대 성능은 1Gbps지만, 전체 망의 최대 성능은 622.08Mbs 이다.

3.1 Multicast routing 과 VPLS domain 에서의 multicasting

VPLS 는 원거리 다자간 VPN 생성에 가장 적합한 기술이다. 다자간 VPN 생성 시 연구망에서 가장 많이 활용될 서비스는 원격 강의 및 HD TV 등 multicast 응용들이다. cisco 7609에서 multicast 는 multicast routing 이나 VLAN 을 이용한 multicast를 지원한다. 이러한 응용들의 VPLS 상에서 가능성을 알아보기 위해 하나의 VPLS domain 을 만들어 multicast 할 때와 multicast routing 을 통해 multicast 할 때를 비교해 본다.

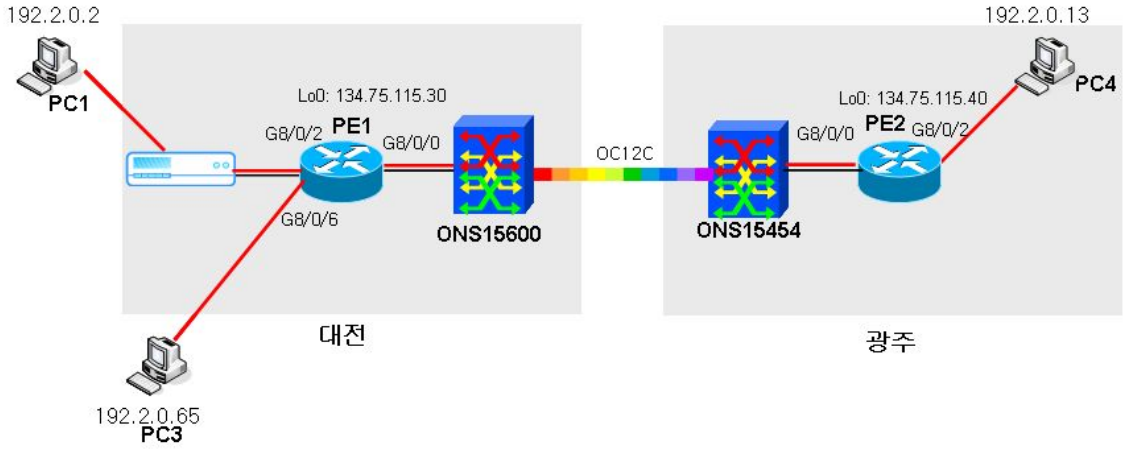

Figure 7. Multicast test network topology

Figure 7 에서와 같이, 먼저 multicast routing 을 통해 광주 PC4 가 client이고, PC1과 PC3 가 서버인 multicast packet 을 보냈다. PC1과 PC3는 서로 사양이 다른 PC로 PC3의 사양이 PC1의 사양보다 더 좋다.

Throughput	Jitter	Loss
500Mbps	0.039ms	0%
530Mbps	0.034ms	0%
560Mbps	0.029ms	0.00027%
570Mbps	0.037ms	1.8%

Table 1. PC3 Multicast Test Results with multicast routing

Throughput	Jitter	Loss
500Mbps	0.044ms	0%
530Mbps	0.039ms	0%
560Mbps	0.032ms	0.000021%
570Mbps	0.038ms	3.2%

Table 2. PC3 Multicast Test Resultswith VPLS

Throughput	Jitter	Loss
500Mbps	0.033ms	0.87%
530Mbps	0.033ms	1%
560Mbps	0.033ms	1.1%
570Mbps	0.034ms	2.7%

Table 3. PC1 Multicast Test Results with multicast routing

Throughput	Jitter	Loss
500Mbps	0.037ms	0.92%
530Mbps	0.035ms	1.1%
560Mbps	0.033ms	1.7%
570Mbps	0.029ms	4.1%

Table 4. PC1 Multicast Test Results with multicast routing

예상과 달리 multicast routing 을 통한 최대 성능치가 VPLS를 통한 multicast 보다 좋았다. Table1 과 Table 2는 PC3에서 보여 진 결과이고, Table3와 Table 4는 PC1에서의 결과이다. jitter 와 loss 율 모두 multicast routing일 경우가 약간 좋았다.
그러나, multicast routing을 통한 multicast 는 데이터의 보안에 약점이 있다. 또한, 원거리에 있는 그룹간의 VPN을 만드는데 있어, 장애가 될 만큼의 성능 저하도 없어 보인다.

3.2 QoS 설정을 통한 VPLS 상에서의 Traffic 제어

3.2.1 Output QoS 설정을 통한 Traffic 제어

연구망 사용자들은 협업을 위해 원거리에 있는 다른 연구자들과의 VPN을 원한다. 이를 위해 VPLS는 가장 적절한 기술이라 할 수 있다. 그러나, 대전의 어느 대학에 물리학과와 생물학과는 서로 다른 연구 그룹을 형성할 수 있으며, 이는 각각 광주의 어느 대학의 물리학과와 생물학과 일 수 있다. 이러할 경우 이들은 uplink를 서로 공유하게 된다. 그러나, 이들 연구 그룹이 각각의 VPN 을 위해 bandwidth를 보장받기를 원한다면, 우리는 각각의 VPLS에 대해 이를 보장해 주어야 할 것이다. Figure 8는 그러한 간단한 예를 보여준다. 대전의 PC1과 광주의 PC4, 대전의 PC2와 광주의 PC5는 각각 VPLS1과 VPLS2로 같은 VPLS domain에 있다. 최종적으로 VPLS1 은 300Mbps, VPLS2는 200Mbps의 성능을 보장 받고자 한다. 만일 PC1에서 PC4, PC3에서 PC4로 가는 트래픽에 대해 이를 보장 받고자 한다면, 시스코의 QoS policy 에 따라 input 과 output 에 대해 shaping을 할 수 있다.

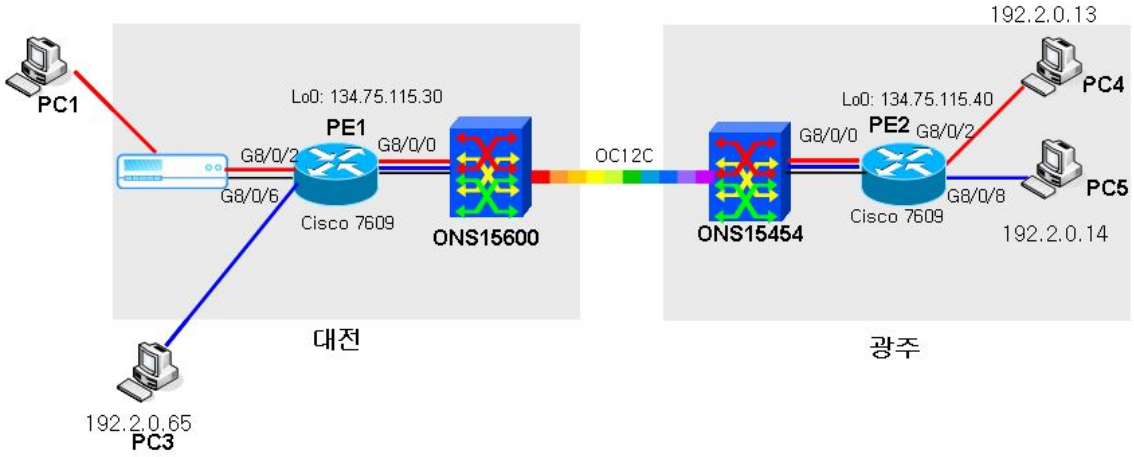

Figure 8. VPLS Output QoS Test Network Topology

그러나, cisco 7609s는 input 에 대해서는 shaping을 할 수 없으므로, 광주의 7609s 에 대해 각각 다음과 같이 shaping 을 설정한다.

```
policy-map svc600
  class class-default
    shape average 300000000
policy-map svc500
  class class-default
    shape average 200000000

interface GigabitEthernet8/0/2
 switchport
 switchport access vlan 501
 switchport mode access
 speed nonegotiate
 mls qos trust cos
```

```
 service-policy output svc600

interface GigabitEthernet8/0/8
 switchport
 switchport access vlan 502
 switchport mode access
 mls qos trust cos
 service-policy output svc500
```

Figure 9는 Output QoS 설정이 없을 때의 테스트 결과를 보여 준다. 테스트 시작할 때의 1초를 지나면, VPLS1은 220Mbps와 360Mbps 사이의 불안정한 트래픽을 보여준다. VPLS2도 마찬가지이다. 그러나, output 에 대해 shaping 을 실행한 결과 Figure 10과 같이 VPLS1은 280, VPLS 2는 190의 안정적인 성능을 보인다. 또한 정확한 300Mbps, 200Mbps 를 보장받기 위해서는 이를 고려한 shaping 이 필요할 것이다.

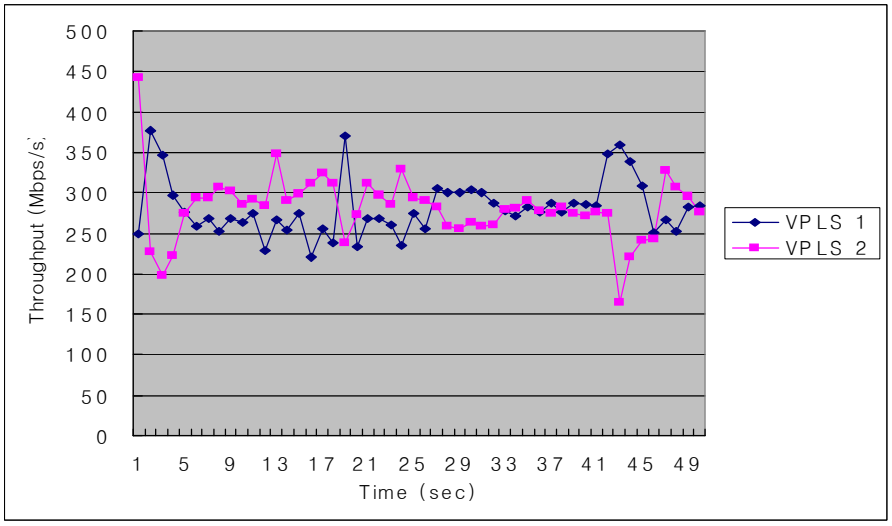

Figure 9. Traffic Flows without shaping

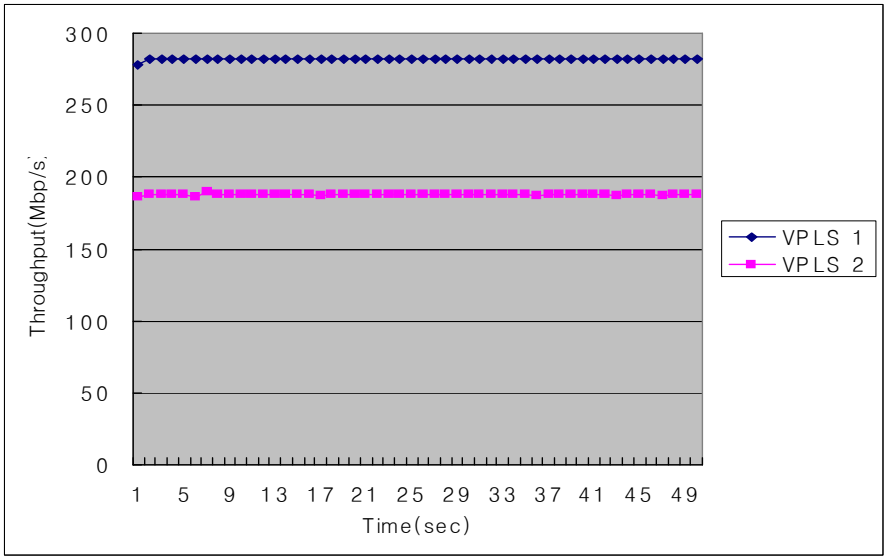

Figure 10. Traffic Flows with output shaping

3.2.2 Output QoS 와 Input QoS를 통한 Traffic 제어

연구자 그룹은 동일한 과의 동일한 층 내에서도 나누어 질 수 있다. 이를 테면, 같은 의과대학이라 하더라도, 분야에 따라 다른 연구자 그룹으로 나뉠 수 있다. 이럴 경우, VPLS 는 동일한 입력 포트에 대해 VLAN ID별로 다른 VPLS를 생성할 수 있다. Figure 11과 같이 PC1, PC3, PC4 가 동일한 그룹에 속하고, PC2, PC5가 동일한 그룹에 속하도록 VPLS를 설정할 수 있다.

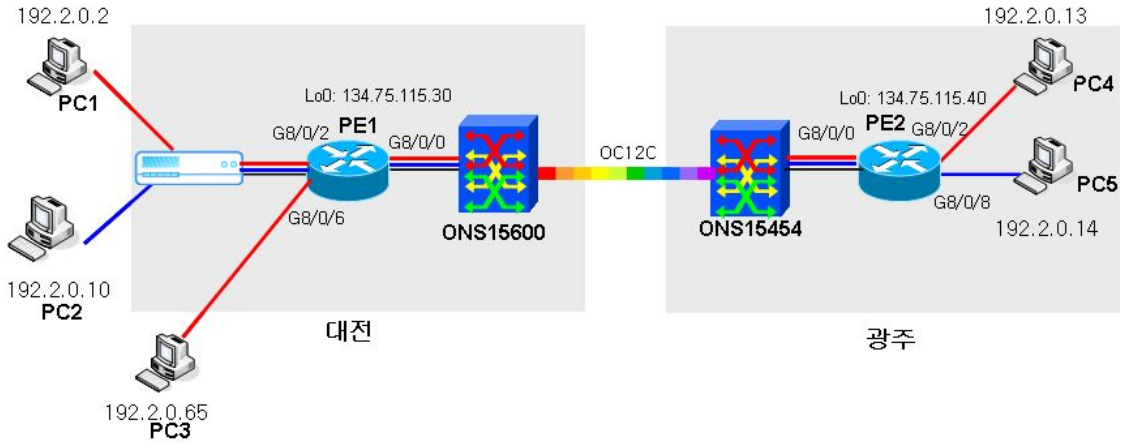

Figure 11. Network Topology for VPLS test with Input and Output QoS

이 때, PC1, PC3가 PC4로 데이터를 보내고 동시에 PC2 가 PC5로 데이터를 보내면, Figure 12와 같은 Traffic flow를 얻는다. PC1과 PC3는 G8/0/2 포트에서 서로의 트래픽에 영향을 받고, PC1과 PC3그리고 PC2의 트래픽이 함께 지나가는 G8/0/0에서는 이들 모두가 서로 영향을 끼친다. Figure 는 VPLS1과 VPLS2로 본 Traffic flow이다.

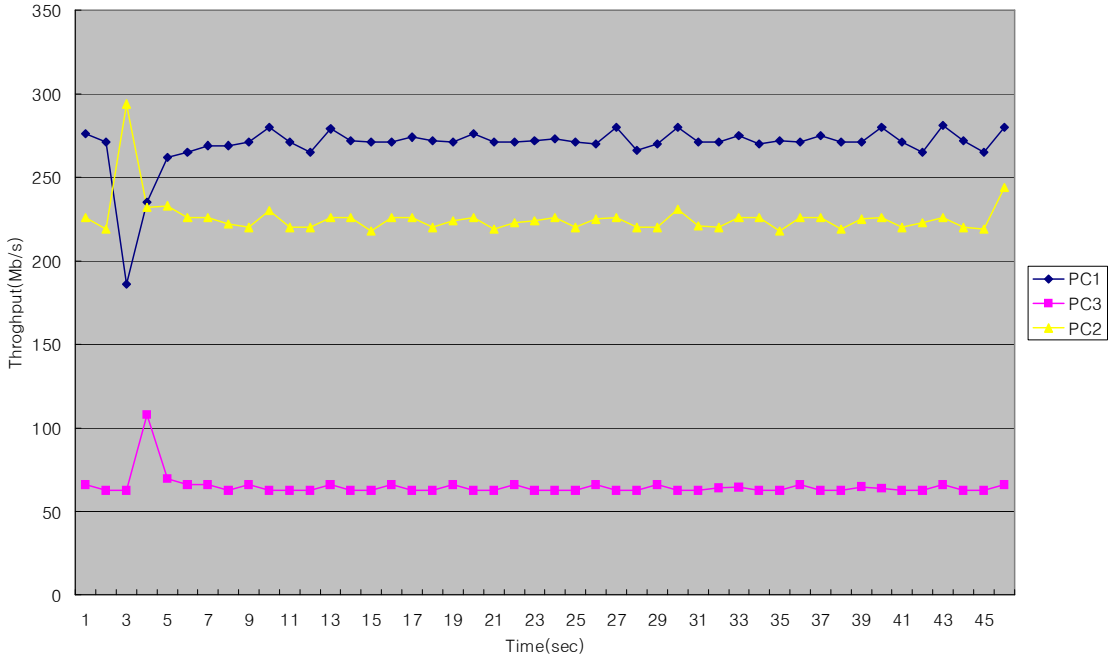

Figure 12. Traffic Flow for each client without QoS

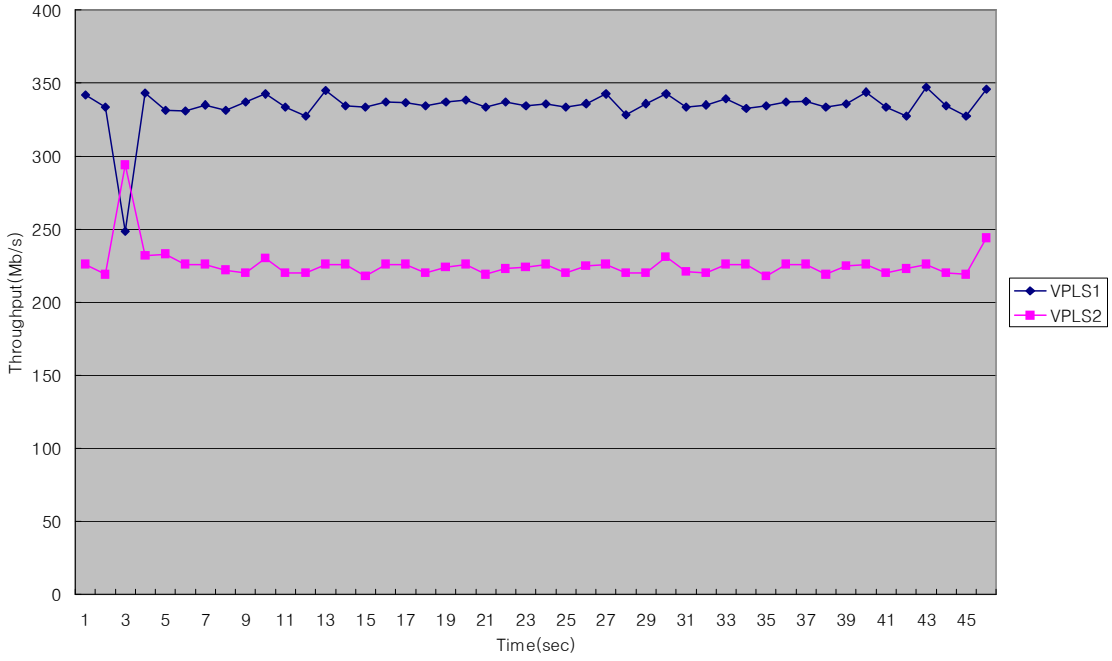

Figure 13. Traffic Flow for each VPLS without QoS

그러나, 사용자들은 PC1과 PC2, PC3 각각이 보내는 트래픽이 특의 bandwidth를 보장 받기를 원한다. Figure 14는 output shaping을 하였을 경우, VPLS1과 VPLS 2의 traffic flow를 보여준다. 각각 하나씩의 client만 있을 때 보다는 불안정 하지만, Figure 13보다는 300Mbps와 200Mbps에서 안정적인 모습을 보여준다.

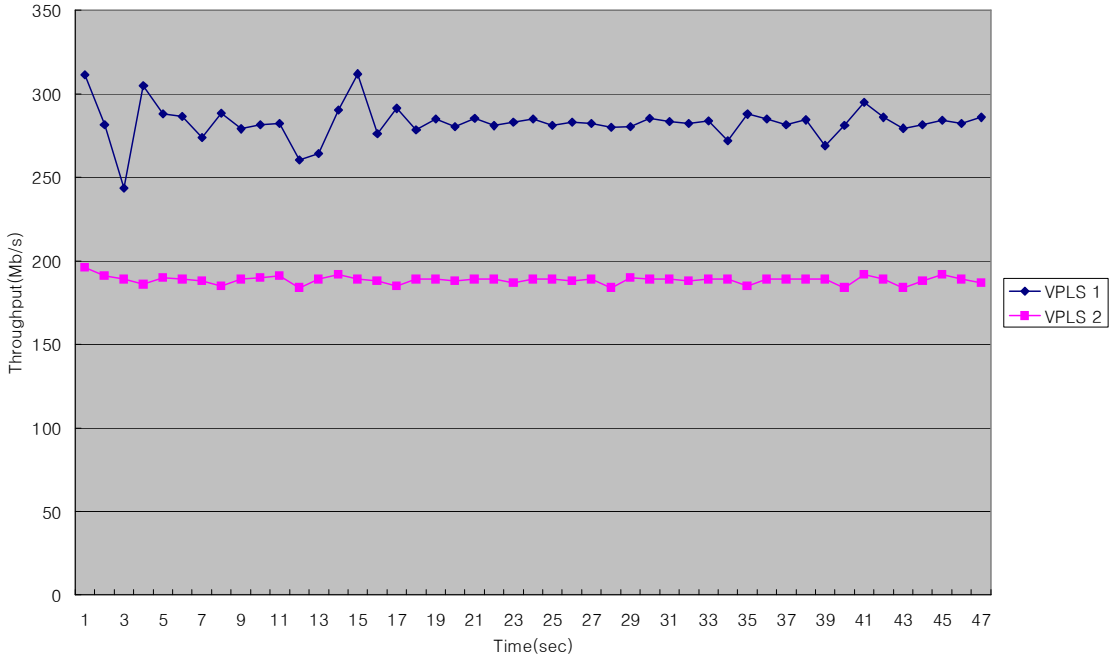

Figure 14. Traffic Flow for each VPLS without output shaping

그러나, Figure 15와 같이 각각의 client 입장에서 보면 input에서 부터 경쟁을 해야 하는 PC1과 PC2는 먼저 시작한 PC1이 트래픽을 장악하고 있으나 역시 PC1 과 PC2 는 안정적이지 못한 traffic flow를 보여준다. 즉 output shaping 만으로는 이들 PC1과 PC2의 traffic 제어까지 할 수는 없다.

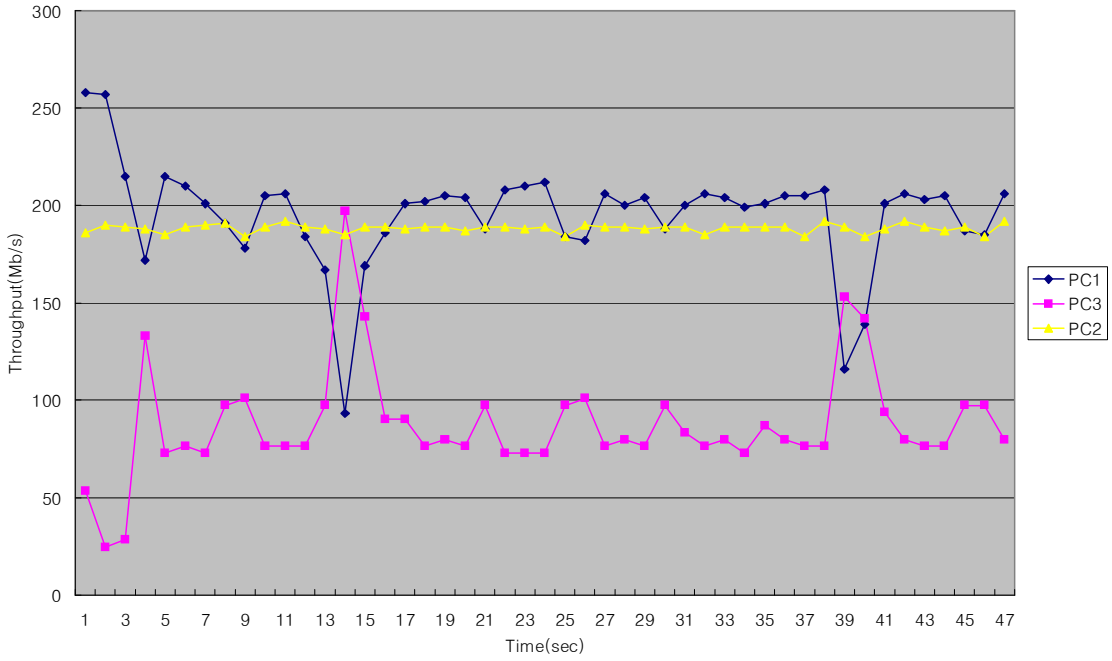

Figure 15. Traffic Flow for each client without output shaping

PC1과 PC3의 traffic 제어를 위해 본 실험에서는 다음과 같이 input 과 output을 동시에 제어해 주었다. input에서 shaping 을 쓸 수는 없었지만 policy의 cir(Committed Information Rate) 설정으로 이를 수행할 수 있었다.

```
>대전 7609
policy-map qosgroup2
  class class-default
   police cir 200000000
policy-map qosgroup1
  class class-default
   police cir 150000000
interface GigabitEthernet8/0/2
 description
 no ip address
 mls qos trust cos
 service instance 100 ethernet
  encapsulation dot1q 500
  rewrite ingress tag pop 1 symmetric
  service-policy input qosgroup1
  bridge-domain 501

 service instance 600 ethernet
  encapsulation dot1q 600
  rewrite ingress tag pop 1 symmetric
  service-policy input qosgroup2
  bridge-domain 502

>광주 7609
policy-map svc600
  class class-default
    shape average 300000000
policy-map svc500
  class class-default
    shape average 200000000

interface GigabitEthernet8/0/2
 switchport
 switchport access vlan 501
 switchport mode access
 speed nonegotiate
```

```
 mls qos trust cos
 service-policy output svc600

interface GigabitEthernet8/0/8
 switchport
 switchport access vlan 502
 switchport mode access
 mls qos trust cos
 service-policy output svc500
```

Figure 16은 input cir 과 ourput shaping 지정 후 VPLS1과 VPLS2의 Traffic 흐름을 보여준다. 그러나, 더 큰 차이는 Figure17에서 볼 수 있다. PC1과 PC3가 Figure 15보다는 대등한 traffic 흐름을 보여 주고 있다.

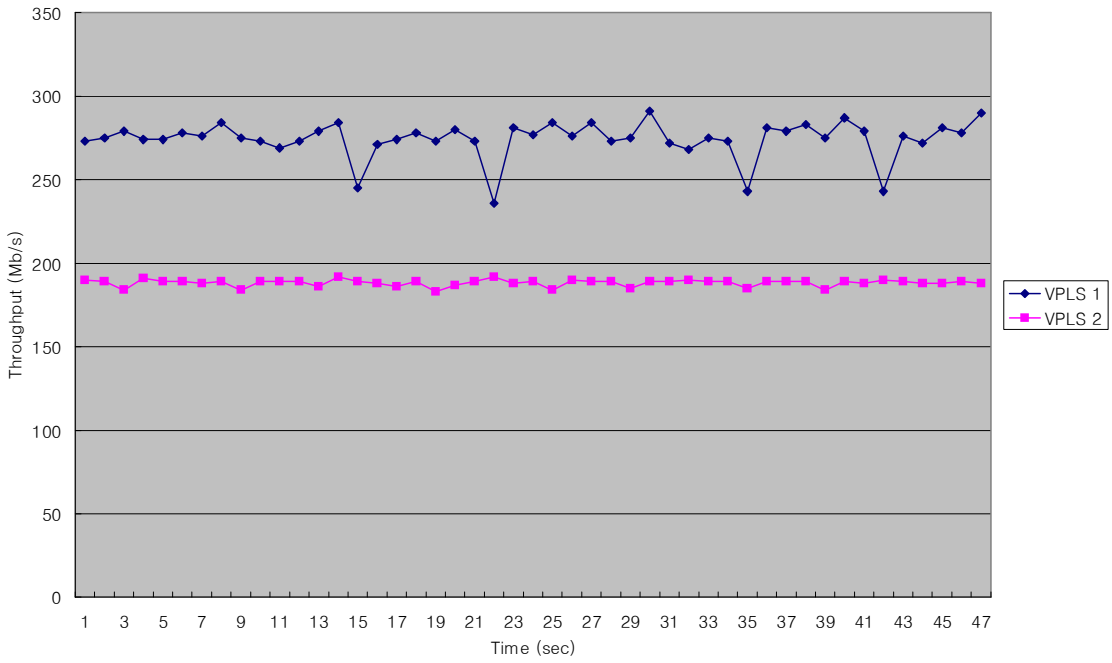

Figure 16. Traffic flow for each VPLS with input and output shaping

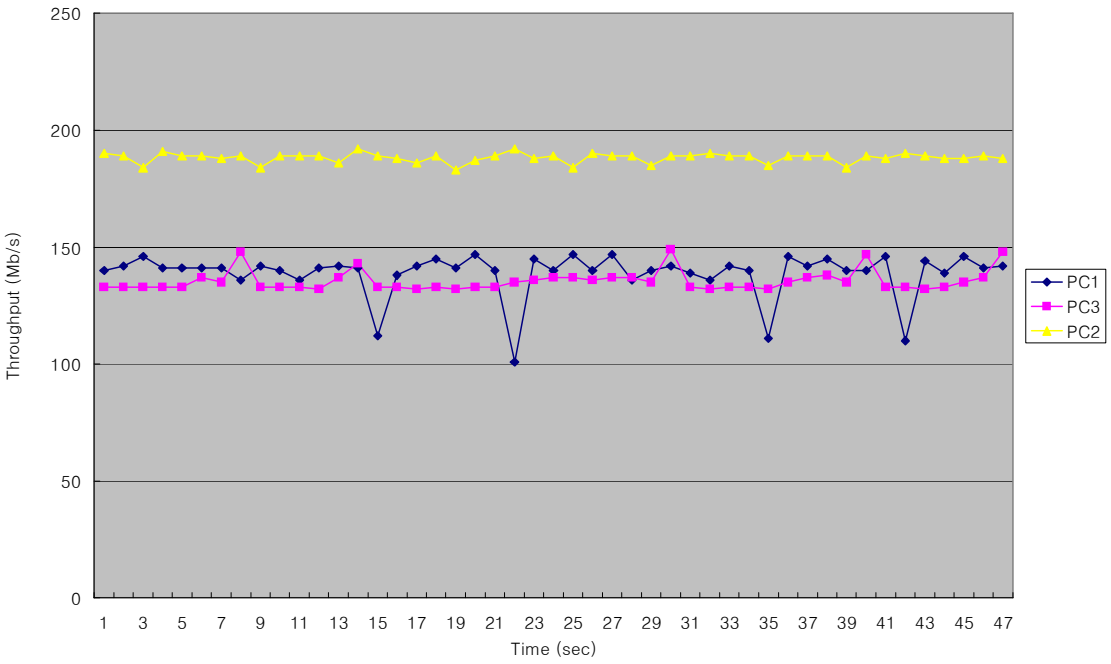

Figure 17. Traffic flow for each client with input and output shaping

5. 결론

VPLS 는 원거리에 있는 연구자 그룹을 하나의 VPN으로 연결하는 기술 중 하나이다. 확장성, 단순성, 관리성, 품질성, 안정성에서 검증 받은 기술이지만, 다양한 상황의 cisco 7609를 통한 실험에서 성능 측면에서 multicast routing의 multicast 보다 떨어졌으며, 품질 보장 측면에서도 단순한 shaping 이나 cir을 설정만으로는 원하는 bandwidth를 확실히 확보할 수 없었다. 또한 cisco 7609의 20G Line card 는 input 인터페이스에 대해 shaping을 설정할 수 없었다. 그러나, 원거리에 있는 사용자 그룹을 하나의 VPN 으로 묶으면서, multicast 와 bandwidth 보장을 한다는 측면에서 비교적 단순한 설정으로 이러한 효과를 거둘 수 있는 장점이 있다. PE 라우터가 아닌 MPLS 백본의 P 라우터들은 설정에 관여하지 않아도 되며, 오직 PE라우터와 CE의 설정으로만 가능하다는 면에서 단순성, 관리성 그리고 확장성 측면에서 다른 기술에 비해 우수하다.

결론적으로, VPLS는 연구자 응용 그룹을 위한 bandwidthrk 보장되는 VPN 서비스 제공에 적합한 기술이다. 따라서, 향후 메트로 이더넷에서 제공하는 E-LAN, EVPLAN 의 UNI가 완전히 제공된다면, 적은 비용으로 구축하고 운영할 수 있는 VPN 서비스를 제공할 수 있을 것이다.

6. 참고문헌

[1] Cisco Systems, "Cisco 7600 Series Ethernet Services 20G Linr Card Configuration Guide"

[2] Riverstone Networks, "MPLS/VPLS Evolution: A Riverstone Perspective"
[3] draft-ietf-l2vpn-vpls-ldp-applic(Internet draft)
[4] draft-serbest-l2vpn-vpls-mcast(Internet draft)