Hose 기반 VPN에서의 서비스품질 제공을 위한 자원예약 프로토콜과 패킷 스케줄링 기법

(A Resource Reservation Protocol and Packet Scheduling for Qos Provisioning in Hose-based VPNs)

변 해 선 † 우 현 제 † 김 경 민 † 이 미 정 ††
(Haesun Byun) (Hyunje Woo) (Kyoungmin Kim) (Meejeong Lee)

요 약 호스(Hose) 모델 기반 VPN(Virtual Private Network) QoS(Quality of Service)를 지원하기 위한 자원준비(Provisioning) 메커니즘들 가운데, VPN 차원 상태 정보(VPN-specific state) 자원준비는 서비스 제공자에게 높은 다중화(Multiplexing) 이점을 제공한다는 장점을 가진다. 그러나, VPN 차원 상태 정보 자원준비를 위한 적합한 자원예약 프로토콜이 없기 때문에 VPN 차원 상태 정보 자원준비를 위한 동적 자동 자원예약이 어렵다. 또한, VPN 차원 상태 정보 자원준비에 의해 예약된 자원은 LAN에 접속되어 있는 호스트들이 LAN 대역폭을 공유하는 것과 유사한 방식으로 동일한 VPN에 속하는 사용자들이 공유하기 때문에 동일한 VPN에 속하는 사용자 간에 불공정한 자원 사용이 발생할 수 있다. 이에 본 논문에서는 VPN 차원 상태 정보 자원준비에 따라 동적 자동 자원 예약을 수행할 수 있도록 하는 자원예약 프로토콜을 제안하고, 혼잡 발생 시에 동일한 VPN에 속하는 사용자 간에 예약된 자원을 공정하게 사용할 수 있도록 하는 트래픽 서비스 메커니즘을 제안한다.

키워드 : 가상사설망 (VPN), 서비스 품질(QoS), 호스(Hose) 모델, 자원예약 프로토콜

Abstract Among the resource provisioning mechanisms for the hose based Virtual Private Network (VPN) Quality of Service (QoS), VPN-specific state provisioning allows the service provider to obtain highest resource multiplexing gains. However, dynamic and automatic resource reservation for the VPN-specific state provisioning is difficult due to the lack of appropriate resource reservation protocol. Furthermore, users of a VPN may experience unfair usage of resources among themselves since the reserved resources of a VPN are shared by the VPN users in a similar way that the traditional LAN bandwidth is shared by the attached hosts. In this paper, we propose a resource reservation protocol and a traffic service mechanism, which not only enable dynamic and automatic resource reservation according to the VPN-specific state provisioning algorithm, but also enforce the fair usage of reserved resources among the users of a VPN in case of congestion.

Key words : Virtual Private Network (VPN), Quality of Service (QoS), Hose model, resource reservation protocol

1. 서 론

VPN(Virtual Private Network)은 인터넷과 같은 공중망을 이용하여 둘 이상의 네트워크를 안전하게 연결한 가상사설망이다. 따라서, 사설망과 비슷한 수준의 보안과 함께 QoS(Quality of Service)를 제공해주는 것이 VPN에서 가장 중요한 이슈라 할 수 있다. 전통적으로 VPN QoS를 지원하기 위한 서비스 모델은 고객 파이프(Customer pipe) 모델이다. 이 모델은 각각의 VPN 사이트 쌍 간 QoS 요구사항을 명시하고, VPN 종단점 간 파이프에 대해 자원을 예약한다. 한편, [1]과 [2]에서는 호스(Hose) 모델이라는 또 다른 VPN QoS 서비스 모델을 제안하였다. 호스는 각각의 VPN 사이트를 서비스 제공자 네트워크에 연결하는 인터페이스를 의미한다. 호

· 본 논문은 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성·지원사업의 지원으로 수행된 연구결과입니다.
† 학생회원 : 이화여자대학교 컴퓨터학과
ladybhs@ewhain.net
hjwoo@ewhain.net
kmk@ewhain.net
†† 정 회 원 : 이화여자대학교 컴퓨터학과 교수
lmj@ewha.ac.kr
논문접수 : 2005년 9월 3일
심사완료 : 2006년 3월 27일

스 모델에서는 QoS 요구사항으로 VPN 사이트에서 서비스 제공자 네트워크로 내 보내고 받아들일 수 있는 총 트래픽의 양과 성능기대치를 명시한다. 호스 모델은 고객 파이프 모델에 비해 사용자의 QoS 요구사항 명시가 용이하고, 호스를 통해 유입되는 VPN 사용자 트래픽이 동일 VPN에 속하는 사이트 중 어느 곳이라도 전송될 수 있으므로 사용에 있어서 유연성을 제공한다. 그리고 일반적으로 고객 파이프들이 필요로 하는 대역폭의 합보다는 호스에 대해 적은 양의 대역폭을 구입해도 되므로 사용자가 엑세스 링크에서의 다중화 이점을 취할 수 있다.

그러나 네트워크 서비스 제공자의 입장에서는 간단해진 VPN 고객의 QoS 요구사항 명세를 가지고 네트워크 자원을 준비해야 하기 때문에 효율적인 자원준비 및 자원 관리 메커니즘이 요구된다. 이를 위해 통계적 다중화 메커니즘, 동적 트래픽 측정과 자원 사이즈 변화(resizing), 라우팅 알고리즘 등 네트워크상에 예약되어야 하는 자원의 요구 대역폭을 최소화하기 위해 많은 연구가 이루어졌다[1-6].

호스 모델 기반의 자원준비 메커니즘은 *제공자 파이프(Provider Pipe)*, *호스 차원 상태 정보(Hose-specific state)*, *VPN 차원 상태 정보* 등으로 분류할 수 있다[1]. 이 방법들의 주된 차이는 자원공유의 정도이다. 제공자 파이프 자원준비는 가장 간단하지만 자원 낭비가 커서 실제적인 적용에 문제가 있을 수 있고, 호스 차원 상태 정보나 VPN 차원 상태 정보는 VPN을 구성하는 호스 매개변수들을 종합적으로 고려하고, 자원공유를 활용함으로써 VPN QoS 지원을 위해 네트워크에 할당해야 하는 자원을 절감할 수 있다. 특히, VPN 차원 상태 정보 자원준비는 VPN 전체적인 차원에서 VPN의 호스 매개변수를 고려하여 자원을 할당하기 때문에 동일한 라우팅 하에서는 세 가지의 자원준비 메커니즘 가운데 필요 이상 할당되는 자원 양을 최대한 줄일 수 있는 메커니즘이다. 호스/VPN 차원 상태 정보 자원준비에서는 VPN을 위해 할당해야 하는 자원의 양을 최소화하기 위해 명시적인 라우팅(explicit routing)을 사용할 수 있는데, VPN 차원 상태 정보 자원준비를 위해서는 최소 비용 VPN 자원준비를 위해 최적화된 VPN 트리를 찾는 문제에 대한 다양한 알고리즘들이 연구·분석된 바 있다[2-6].

그런데, VPN QoS 자원준비를 위해 고려되어야 할 또 다른 매우 중요한 이슈는 이들 자원준비 메커니즘들을 네트워크에 동적이고 자동적으로 적용하는 것이다. 이를 위해서는 이들 자원준비 메커니즘에 따라 자원예약을 수행하는 프로토콜이 필요하지만, 아직 이 문제에 관해서는 연구된 바가 없다. MPLS(Multiprotocol Label Switching) 네트워크를 위한 일반적인 자원예약 프로토콜로는 RSVP-TE(Resource ReSerVation Protocol-Traffic Engineering)와 P2MP(Point-to-Multipoint) RSVP-TE가 제안된 바 있지만[7,8], 이 두 프로토콜들은 자원준비 메커니즘 중 자원의 효과적인 활용 측면에서 가장 유리한 VPN 차원 상태 정보 자원준비를 위해서는 적당하지 않은 측면이 몇 가지 있다.

또한, VPN 차원 상태 정보 자원준비는 VPN을 위해 할당해야 하는 자원을 최소화한다는 측면에서는 가장 유리하지만, 각 VPN에 대하여 예약된 자원을 그 VPN에 속하는 사용자들이 공유하기 때문에 동일한 VPN에 속하는 사용자들 간에 불공정하게 자원을 사용할 수 있다는 문제가 있다. 이것은 전통적인 LAN 대역폭을 그 LAN에 속하는 호스트들이 공유하는 경우에 발생하는 문제와 유사하다.

이에 본 논문에서는 VPN 차원 상태 정보 자원준비에 따라 동적 자동 자원 예약을 수행하기 위한 새로운 자원예약 프로토콜과 함께 동일한 VPN에 속하는 VPN 사용자들 간에 예약된 자원을 공평하게 공유하도록 하는 새로운 트래픽 서비스 메커니즘을 제안한다. 본 논문의 구성은 다음과 같다. 1장의 서론에 이어 2장에서는 관련연구로서 세 가지의 호스 모델 자원준비 메커니즘과 MPLS 네트워크를 위해 표준화 혹은 제안된 두 가지의 자원예약 프로토콜들을 설명한다. 3장에서는 제안된 메커니즘의 자세한 내용을 설명하고, 4장에서는 그 효율성을 살펴보기 위한 시뮬레이션 결과를 제시한다. 마지막으로 5장에서는 이 논문의 결론을 맺는다.

2. 관련연구

이 장에서는 호스 모델을 위한 세 가지의 자원준비 메커니즘을 설명한다. 또한, MPLS 네트워크에서의 자원예약을 위해 표준화 혹은 제안된 두 가지의 프로토콜을 살펴보고, 이들이 왜 VPN 차원 상태 정보 자원준비를 위한 자원예약 프로토콜로 사용되기에 부적합한지를 설명한다.

2.1 호스 모델을 위한 자원준비 메커니즘

1장에서 소개한 호스 모델 자원준비 메커니즘 중 가장 간단한 제공자 파이프 자원준비는 그림 1(a)와 같이 서비스 제공자의 PE(Provider Edge router) 간에 디폴트 최단 경로를 따라 제공자 파이프 를 설정하되, 각 제공자 파이프에는 그 제공자 파이프의 진입 호스로부터 유입될 수 있는 트래픽 전체가 해당 제공자 파이프의 진출 호스로 모두 나가는 최악의 경우에 해당하는 트래픽 분포를 가정하고 자원을 할당하며, 제공자 파이프간에 자원공유는 고려되지 않는다. 즉, 각 링크에서는 VPN의 제공자 파이프 별로 자원을 할당하며, 각 제공

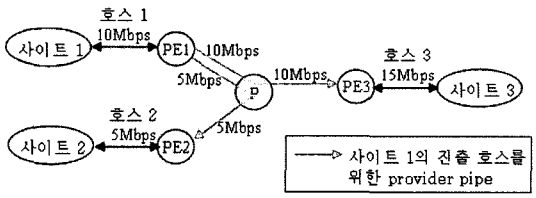

그림 1 (a) 제공자 파이프 자원준비에서 사이트 1의 진출 호스를 위한 자원할당

자 파이프를 위해 그 제공자 파이프의 진입 호스와 진출 호스 크기 중 더 작은 값만큼의 자원을 할당한다.

호스 차원 상태 정보 자원준비에서는 자원공유 가능성과 호스 차원 상태 정보를 활용하여 네트워크에서 VPN을 위해 할당해야 하는 자원 양을 줄인다. 호스 차원 상태 정보 자원준비에서는 그림 1(b)에서와 같이 VPN의 각 진입 호스가 연결되어 있는 PE를 루트로 하여 그 호스 트래픽의 목적지가 될 수 있는 모든 진출 호스들이 연결되어 있는 PE에 이르는 트리(이하에서 이를 호스 트리라 부르기로 함)를 형성한다. 그리고, 그림 1(b)에서와 같이 호스 트리의 진입, 진출 호스 매개변수들의 정보와 함께 호스 트리를 구성하는 PE 간 파이프들이 자원을 공유할 수 있음을 고려하여 호스 트리 상의 각 링크에 예약되는 자원의 양을 결정한다. 구체적으로 호스 차원 상태 정보 자원준비에서는 각 링크에 호스 트리 별로 자원을 예약하며, 특정 호스 트리를 위해 예약하는 자원의 양은 그 호스 트리의 진입 호스 크기와 진출 호스들 크기의 합 중 더 적은 값에 해당한다[1].

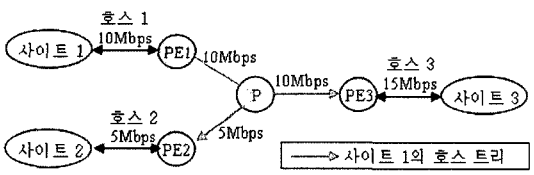

그림 1 (b) 호스 차원 상태 정보 자원준비에서 사이트 1의 호스 트리를 위한 자원할당

마지막으로, VPN 차원 상태 정보 자원준비에서는 그림 1(c)에서와 같이 VPN을 구성하는 모든 호스들의 매개변수 정보를 동시에 고려하고, 해당 VPN을 서비스하는 PE들을 모두 연결하는 그래프 혹은 트리 상에 예약되는 자원은 그 VPN에 속하는 모든 호스트들에 의해서 공유할 수 있음을 고려하여 예약될 자원의 양을 결정함으로써 한층 더 VPN을 위해 할당하는 자원의 양을 감소시킨다. 구체적으로 VPN 차원 상태 정보 자원준비에 의해 임의의 링크에 특정 VPN을 위해 예약되는 자원의 양은 그 링크를 경유하는 해당 VPN의 모든 호스 트리

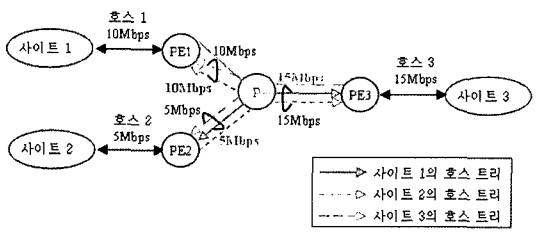

그림 1 (c) VPN 차원 상태 정보 자원준비에서의 자원할당

들의 진입 호스 크기의 합과 진출 호스 크기 합 중 더 적은 값에 해당하는 값이 된다[1].

2.2 MPLS 네트워크를 위한 자원예약 프로토콜

RSVP-TE는 MPLS 네트워크에서 P2P TE LSP (Point-to-Point Traffic Engineering Label Switched Path)를 설립하기 위한 프로토콜이다[7]. 호스 모델을 위한 자원준비 메커니즘 중 제공자 파이프 자원준비는 RSVP-TE 메커니즘을 그대로 적용함으로써 구현할 수 있다. 그러나 호스 차원 상태 정보나 VPN 차원 상태 정보 자원준비 메커니즘은 단순히 RSVP-TE 메커니즘을 적용함으로써 구현할 수 없다. RSVP-TE에서는 자원공유 옵션 중에 하나인 SE(Shared Explicit) 스타일을 이용하여 동일한 세션에 속하는 LSP들간 자원공유를 허용할 수 있다. 그런데 RSVP-TE의 세션 객체를 식별하는 요소 중 하나로 세션을 설립하고자 하는 터널의 진출 종단점 주소가 들어가기 때문에 결국 RSVP-TE을 이용한 자원공유는 터널의 진출 종단점이 동일한 LSP들간 자원 공유만이 지원 가능하다. 반면, 호스 상태 기반이나 VPN 상태 기반 자원준비 메커니즘은 터널의 진출 혹은 진입 종단점이 동일하지 않는 LSP들간의 자원 공유도 지원해야 한다.

그림 2는 RSVP-TE에서 지원하는 자원 공유와 호스 차원 상태 정보나 VPN 차원 상태 정보 자원준비 메커니즘에서 지원되어야 하는 자원 공유를 나타낸 것이다. LSR(Label Switching Router)인 PE5와 P5를 연결하는 링크를 통과하는 LSP4와 LSP5는 터널의 진출 종단

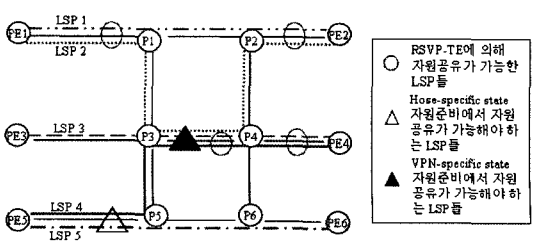

그림 2 RSVP-TE와 호스/VPN 차원 상태 정보 자원준비에서의 자원공유

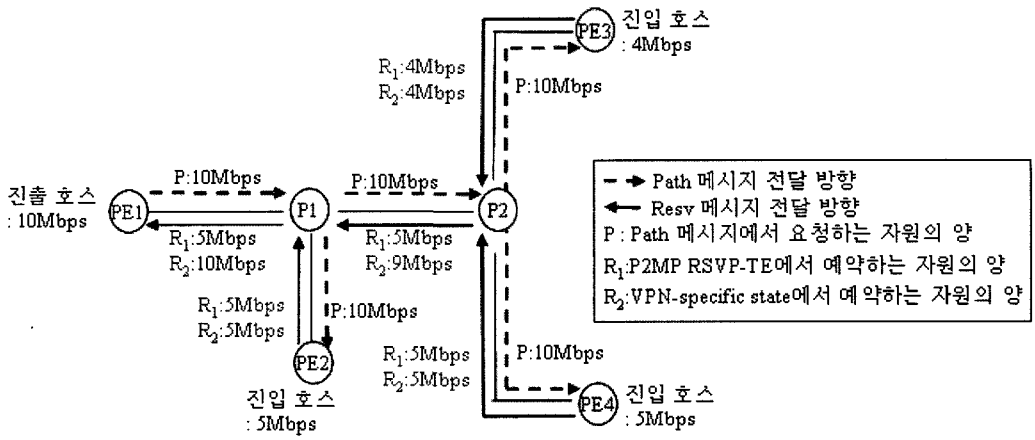

그림 3 P2MP RSVP-TE와 VPN 차원 상태 정보 자원준비에서 각 링크에 예약하는 자원의 양

점이 다르지만 VPN의 동일 호스를 서비스하는 LSP들이라면 호스 차원 상태 정보로 자원을 준비하는 경우 서로 자원을 공유할 수 있어야 한다. P3과 P4를 연결하는 링크를 통과하는 LSP2, LSP3, LSP4는 터널의 양 종단점이 모두 다른 경우이지만 VPN 차원 상태 정보로 자원을 준비하는 경우 동일 VPN을 서비스하는 LSP들이라면 서로 자원을 공유할 수 있어야 한다. 따라서 RSVP-TE는 호스 차원 상태 정보나 VPN-specific sate 자원준비를 위한 자원예약을 수행할 수 없다.

P2MP RSVP-TE는 P2MP TE LSP 설정을 위해 RSVP-TE를 확장한 프로토콜로 멀티캐스트 트래픽 전송을 위한 자원예약을 수행한다[8]. 그림 2에서와 같이 P2MP RSVP-TE는 서로 다른 진입/진출 종단점을 가진 LSP들간 자원 공유를 지원할 수 있다. 그러나 P2MP RSVP-TE는 멀티캐스트 데이타 전송을 목적으로 하므로 유니캐스트 전송을 위한 레이블 할당 및 스위칭이 이루어지지 않는다. 또한 VPN 차원 상태 정보 자원준비에서 각 링크에 예약되어야 할 자원의 양을 계산하는 방식을 적용하지 못한다. 그림 3은 P2MP RSVP-TE에서 네트워크에 예약하는 자원의 양과 VPN 차원 상태 정보 자원준비에 따라 네트워크 상에 할당해야 하는 자원의 양이 다른 예를 보인 것이다. 따라서 VPN 차원 상태 정보 자원준비를 위한 자원예약을 수행하기 위해서는 새로운 자원예약 프로토콜을 정의하거나 기존의 자원예약 프로토콜을 확장하여야 한다.

3. VPN 차원 상태 정보 자원준비를 위한 자원예약 프로토콜 및 트래픽 서비스 메커니즘

본 논문에서는 VPN QoS 자원준비를 위하여 전적으로 새로운 자원예약 프로토콜을 정의하기 보다는 IETF의 MPLS 워킹그룹에 의해 표준화가 진행되고 있는 P2MP RSVP-TE를 기반으로 확장한 자원예약 프로토콜을 제안한다. 제안하는 메커니즘은 P2MP RSVP-TE의 자원공유 지원 메커니즘을 이용하며, VPN 차원 상태 정보 자원준비에 따라 동적 자동 자원 예약을 수행하고 VPN 사용자들이 VPN에 할당된 자원을 공정하게 사용할 수 있도록 한다. 제안하는 자원예약 프로토콜에서 RSVP 메시지가 송·수신자 사이에 전달되는 방식은 기본적으로 P2MP RSVP-TE에서의 방식과 매우 유사하다. 따라서 아래의 설명에서는 P2MP RSVP TE와의 차이점에 초점을 맞춰 설명한다. 구체적으로, RSVP 메시지와 PSB(Path State Block) 및 RSB(Reservation State Block) 구조의 확장, 그리고 RSVP 메시지 프로세싱 방법의 변화 등과 함께 이에 의해 예약된 자원을 VPN 사용자들이 공평하게 공유하도록 하기 위한 트래픽 서비스 메커니즘을 설명한다.

3.1 VPN 차원 상태 정보 자원준비를 위한 자원예약 프로토콜

그림 4와 5는 제안하는 메커니즘을 위한 Path 메시지와 Resv 메시지의 형태를 보인 것이다. 이들은 그림에서 음영으로 표시한 객체(object)들을 제외하고는 P2MP RSVP-TE의 형태와 유사하다. VPN Session 객체는 P2MP RSVP-TE에서의 P2MP Session 객체를 재명명한 것이다. VPN Session 객체에는 VPN ID와 Tunnel ID가 포함되는데 이 필드들은 동일 VPN에 속하는 P2P sub-LSP들을 VPN 터널로 연관시키기 위해 사용된다. 그림 6은 동일한 VPN 터널에 속하는 호스 트리들과 P2P sub-LSP들의 관계를 보여주고 있다. VPN Session 객체의 VPN ID에는 멀티캐스트 그룹 주소가 표시되는데, VPN을 서비스하는 PE들은 자원예약을 수행하기 전에 자신이 서비스하는 VPN에 대한 멀티캐스트 그룹 주소를 알고 있어야 한다.

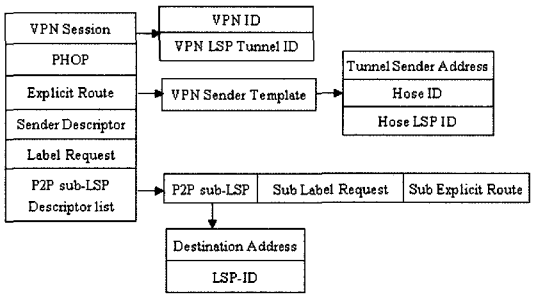

그림 4 Path 메시지 형태

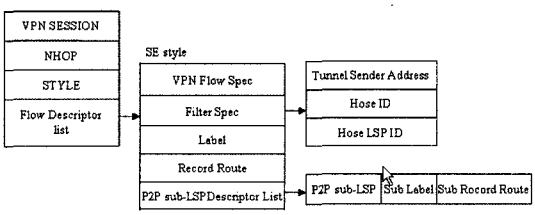

그림 5 Resv 메시지 형태

또한, Path 메시지의 *VPN Sender Template* 객체와 Resv 메시지의 *Filter Spec* 객체에는 *Hose ID*를 추가하였다. P2MP RSVP-TE의 P2MP 터널은 트래픽 소스가 항상 하나인데 반해, VPN 터널은 하나의 진입 PE에 동일 VPN에 속하는 사이트가 두 개 이상 접속되어 있는 경우 VPN 터널의 트래픽 소스가 두 개 이상이 될 수 있으므로 이를 식별하기 위하여 *Hose ID*를 사용한다.

그리고, VPN 터널을 구성하는 P2P sub-LSP들에 대해 각각 별도의 레이블을 할당하기 위해서 Path 메시지와 Resv 메시지의 *P2P sub-LSP Descriptor* 객체에 *Sub Label Request* 객체와 *Sub Label* 객체를 각각 추가하였다. P2MP 터널은 멀티캐스트 전송만을 위해 사용되므로 터널을 위한 레이블을 하나만 할당하면 되지만 VPN 터널은 유니캐스트 전송을 위해 사용될 수도 있기 때문에 각 P2P sub-LSP 별로 별도의 레이블을 할당한다.

모든 LSR는 Path 메시지에 대하여 PSB들을 유지한다. PSB는 Path 메시지가 도착한 인터페이스 상에 *<VPN session, VPN Sender Template>* 별 하나씩 생성된다. 그림 7은 PSB의 구조를 보여주고 있다. 진입 PE는 자신에게 접속되어 있는 각 진입 호스를 위하여 path 메시지를 만들고, 이를 해당 호스 트리의 목적지들을 향해 전송한다. Path 메시지는 호스 트리의 목적지를 나타내는 하나 이상의 *P2P sub-LSP Descriptor*를 포함하고 있다. 진입 PE는 Path 메시지를 받게 되면, Path 메시지를 수신한 인터페이스에 대해 Path 메시지의 *<VPN Session, VPN Sender Template>*에 대해 해당하는 PSB가 있는지 검색한다. 이 검색에서 발견된 PSB를 *Matching PSB*라 부르기로 한다. Matching PSB가 존재한다면 Matching PSB안에 수신한 Path 메시지의 *P2P sub-LSP Descriptor* 정보가 있는지 확인한다. *P2P sub-LSP Descriptor* 정보가 존재한다면 *P2P sub-LSP Descriptor*를 비롯한 Matching PSB 정보들을 리프레쉬하고 존재하지 않는다면 수신한 Path 메시지의 *P2P sub-LSP Descriptor*를 Matching PSB에 추가한다. Matching PSB가 존재하지 않는다면 새로운 PSB를 생성하며, Matching PSB를 생성 혹은 리프레쉬한 후 Path 메시지는 목적지를 향한 다음 홉으로 전달한다.

VPN Session	Sender Teamplate	Sender Tspec	PHOP	In intf	P2P sub-LSP	ERO	LABEL	Out intf	Expirstion time
					P2P sub-LSP	ERO	LABEL	Out intf	Expiration time

그림 7 PSB의 구조

VPN Session	resv Intf	Style	VPN Flow spec	Filter Spec	NHOP	P2P sub-LSP	RRO	LABEL	Expiration time
						P2P sub-LSP	RRO	LABEL	Expiration time
						P2P sub-LSP	RRO	LABEL	Expiration time
				Filter Spec	NHOP	P2P sub-LSP	RRO	LABEL	Expiration time
						P2P sub-LSP	RRO	LABEL	Expiration time
						P2P sub-LSP	RRO	LABEL	Expiration time

그림 8 RSB의 구조

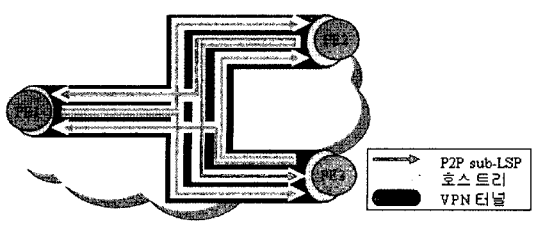

그림 6 VPN 터널과 호스 트리, P2P sub-LSPs의 관계

진출 PE는 Path 메시지를 받으면 해당 RSB를 생성 혹은 수정하고, Resv 메시지를 생성하여 Path 메시지의 소스를 향해 보낸다. 임의의 중간 LSR이 Resv 메시지를 받으면 LSR은 먼저 수신한 Resv 메시지가 적법한지 즉 이에 대응하는 Path 메시지가 있었는지를 점검하기 위해 PSB 리스트에서 수신한 Resv 메시지에 대한 *corresponding PSB*를 검색한다. Corresponding PSB는 Resv 메시지의 *<VPN session, Filter Spec, P2P sub-LSP Descriptor*, Resv 메시지 도착 인터페이스*>*와 *<VPN session, Sender Template, P2P sub-LSP Descriptor, Out intf>*가 일치하는 PSB를 의미한다. 여기에서 *Out intf*는 해당 Path 메시지를 다음 홉으로 보내기 위해 내보낸 인터페이스를 의미한다.

Resv 메시지가 유효하다면 즉 corresponding PSB를 발견하면 Active RSB를 검색하고 이를 업데이트/리프레쉬한다. RSB는 Resv 메시지가 도착하는 인터페이스상에 VPN별로 유지되며, 그림 8과 같은 구조를 가진다. Active RSB는 Resv 메시지가 도착한 인터페이스상에 있는 RSB 중 Resv 메시지의 <*VPN session*>에 해당하는 RSB를 의미한다. Active RSB는 수신한 Resv 메시지의 정보에 따라 업데이트/리프레쉬 되며, Active RSB가 없는 경우에는 새로운 RSB를 생성한다. 이때 VPN을 위해 할당하는 자원의 양을 표시해 두는 *VPN Flow Spec*에 기록할 B_{VPN} 값은 다음과 같이 계산된다.

$$\begin{cases} \text{진출 PE 라우터의 경우}, B_{VPN} = \min(\sum_{k\in K} P_k, \sum_{s\in S} H_s) \\ \text{그 외 라우터의 경우}, B_{VPN} = M_{VPN} \end{cases}$$

여기에서 K는 corresponding PSB의 <*VPN session, In intf*>와 동일한 <*VPN session, In intf*>를 가지는 PSB들의 집합을 의미하고, P_k 는 PSB k의 *Sender Tspec*의 대역폭을 나타내며, M_{VPN} 은 수신한 Resv 메시지의 *VPN Flow Spec*의 대역폭을 의미한다.

다음으로 중간 LSR은 상위 LSR로 전달할 Resv 메시지들을 생성한다. 이때 Resv 메시지의 *VPN Flow Spec*의 대역폭인 M_{VPN} 은 VPN 차원 상태 정보 자원준비 알고리즘을 적용하기 위하여 다음과 같이 계산한다.

$$M_{VPN} = \min(\sum_{k\in K} P_k, \sum_{v\in V} B^v_{VPN})$$

여기에서 V는 Active RSB의 <*VPN session, NHOP*>과 동일한 <*VPN session, NHOP*>을 가지는 RSB들의 집합을 나타내고, B^v_{VPN} 는 RSB v의 VPN Flow Spec의 대역폭이다.

3.2 예약된 VPN 자원의 공정한 사용을 위한 트래픽 서비스 메커니즘

본 논문에서 제안한 트래픽 서비스 메커니즘은 자원 활용을 최적화하기 위해 VPN 차원 상태 정보 자원준비 방식으로 자원을 할당하되, VPN을 위해 할당된 자원을 VPN의 트래픽 소스들이 공평하게 사용할 수 있도록 하는 것을 목적으로 한다. 이를 위해 제안하는 트래픽 서비스 메커니즘에서는 우선 VPN 사용자간의 공정한 사용을 "VPN 차원 상태 정보 자원준비에 의해 VPN 별로 할당된 자원을 사용하는데 있어 혼잡이 발생하였을 때 즉, VPN 사이트 (VPN 트래픽 소스)간에 경쟁이 발생하였을 때, VPN 사이트 별로 자원을 할당하는 호스 차원 상태 정보 자원준비에 의해 각 VPN 사이트에 할당되는 자원의 양에 비례하여 VPN 사이트들이 자원을 공유하도록 함"이라고 정의하였다. 즉, 임의의 링크를 지나는 서로 다른 호스 트리의 개수가 N이라고 가정하고, 그 링크에서 호스 차원 상태 정보 자원준비에 의해 호스 트리 i를 위해 할당되는 자원이 B^i_{Hose} 이고, VPN 차원 상태 정보 자원준비에 의해 VPN에 할당되는 자원이 B_{VPN} 라 하면, VPN 차원 상태 정보 자원준비가 사용되었을 때 호스 트리 i가 사용할 수 있는 공정한 몫 B^i_f 는 다음과 같이 정의된다.

$$B^i_f = \left(\frac{B^i_{Hose}}{\sum_{k=1}^{N} B^k_{Hose}}\right) \cdot B_{VPN} \quad (1)$$

이 정의에 따라 트래픽 서비스가 이루어질 수 있도록 하기 위해서는 호스 차원 상태 정보 자원준비에 의해 각 VPN 사이트 별로 할당되는 자원의 양을 LSR들이 파악하고 있어야 하므로 LSR간에 이에 관한 정보를 전달하고 유지하기 위해 RSVP 메시지와 RSB에 그림 9, 그림 10과 같이 Hose Flow Spec 필드를 추가하여야 한다. RSB의 Hose Flow Spec에 기록될 값인 B_{Hose} 는 아래와 같이 계산한다.

$$\begin{cases} \text{진출 PE LSR의 경우}, B_{Hose} = \min(P_{corr\_PSB}, \sum_{s\in S} H_s) \\ \text{그 외 LSR의 경우}, B_{Hose} = M_{Hose} \end{cases}$$

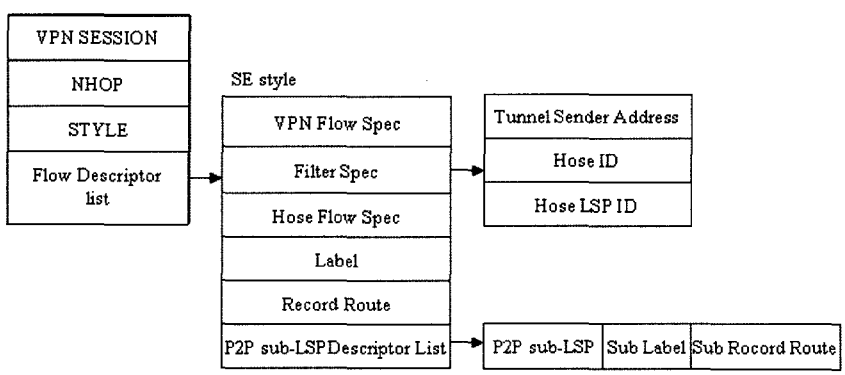

그림 9 새로운 Resv 메시지의 구조

VPN Session	resv Intf	Style	VPN Flow spec	Filter Spec	Hose Flow spec	NHOP	P2P sub-LSP	RRO	LABEL	Expiration time
							P2P sub-LSP	RRO	LABEL	Expiration time
							P2P sub-LSP	RRO	LABEL	Expiration time
				Filter Spec	Hose Flow spec	NHOP	P2P sub-LSP	RRO	LABEL	Expiration time
							P2P sub-LSP	RRO	LABEL	Expiration time
							P2P sub-LSP	RRO	LABEL	Expiration time

그림 10 새로운 RSB의 구조

여기에서 P_{corr_PSB}는 corresponding PSB의 *Sender Tspec*의 대역폭을 의미하고, S는 해당 진출 PE가 서비스하는 모든 사용자 사이트 집합을 의미하며, H_s는 진출 PE에서 사용자 사이트 s로 데이타를 내보내는 진출 호스의 크기를 나타내고, M_{Hose}는 수신한 Resv 메시지의 *Hose Flow Spec*에 표시된 대역폭을 의미한다. 이와 같이 RSB에 각 호스 별 *Hose Flow Spec*(B_{Hose})을 기록해 둠으로써 이를 이용하여 식 (1)의 B_f^i를 계산할 수 있다.

또한, 상위 LSR에게 보낼 Resv 메시지의 *Hose Flow Spec*에 기록될 값인 M_{Hose}는 아래와 같이 계산한다.

$$M_{Hose} = \min(P_{corr\_PSB}, \sum_{h \in H} B_{Hose}^h)$$

여기에서 H는 Active RSB의 <*VPN session, Filter Spec, NHOP*>과 동일한 <*VPN session, Filter Spec, NHOP*>을 가지는 RSB들의 집합을 나타내고, B_{Hose}^h는 RSB h의 *Hose Flow Spec*의 대역폭 값을 의미한다.

특정 VPN을 위해 링크 상에 예약된 자원을 그 VPN에 속하는 호스 트리들이 공정하게 사용하도록 하기 위해 먼저, 임의의 LSR의 진출(Outgoing) 인터페이스 큐에서 호스 트리 별 트래픽이 적어도 $Q_f = Q/N$의 공간을 차지할 수 있도록 보장한다. 여기서 Q는 큐의 크기이고 N은 큐를 공유하는 호스 트리의 수이다. 이를 위해 각 호스 트리 별로 진출 큐에 적재되어 있는 해당 호스 트리에 속하는 패킷 수를 카운트하는 카운터가 유지되어야 한다. 호스 트리 h에 속하는 패킷의 수를 q_h라고 하면, 호스 트리 h에 해당하는 패킷이 큐에 도착했을 때, 만약 큐의 길이 $q = \sum_{k=1}^{N} q_k$가 Q보다 작다면, 그 패킷은 큐에 저장된다. 만약, $q \geq Q$이고, $q_h < Q_f$이면, $q_{h'} > Q_f$을 가진 호스 트리 h'을 찾아서 h'의 마지막 패킷을 버리고, 방금 도착한 패킷을 큐에 저장한다. 반복적으로 동일한 호스에 대한 패킷을 삭제하지 않기 위하여 패킷을 버릴 호스 트리는 이전에 선택된 호스 트리의 다음 호스 트리로부터 시작해 라운드 로빈(Round Robin) 방식으로 찾는다. 만약 $q \geq Q$이고, $q_h \geq Q_f$이면 방금 도착한 패킷은 버린다.

또한 진출 큐에서는 그 진출 큐를 공유하는 VPN 트래픽 소스들이 식 (1)에 의해 결정되는 비중에 따라 WFQ에 의한 서비스를 받도록 한다. 진출 큐에 있는 패킷이 속한 호스를 구분할 수 있도록 하기 위해 그림 11에서와 같이 레이블 스위칭 테이블에 *Hose ID* 필드를 추가하고, 패킷의 레이블 스위칭 시에 *Hose ID*를 얻어서 패킷을 진출 큐에 삽입하기 전에 이를 그림 12에서와 같이 더미헤더로 붙여 준다.

그림 13은 LSR의 진출 인터페이스에서 2단계 WFQ를 수행하는 것을 도식화한 것이다. 외부 WFQ 서비스는 서로 다른 VPN에 해당하는 큐들 간에 VPN 차원 상태 정보 자원준비에 의해 할당된 자원 양에 따라 WFQ를 수행한다. 그리고, 내부 WFQ 서비스는 하나의 큐를 공유하는 동일한 VPN에 속하는 서로 다른 호스 트리들에게 각 호스 트리 i의 공정한 몫인 B_f^i를 비중으로 하여 서비스를 해준다. 더미헤더인 *Hose ID*는 패킷을 진출 큐에서 내보낼 때 제거한다.

In intf	In Label	Hose ID	Out intf	Out Label
IF1	L1	Hose 1	IF2	L2
IF1	L3	Hose 2	IF2	L4

그림 11 레이블 스위칭 테이블

Hose ID	Shim Header	IP	IP Payload

그림 12 호스 트리를 식별하기 위한 더미헤더

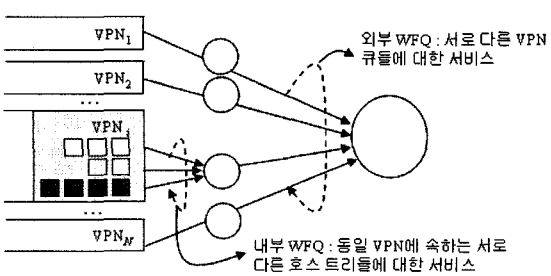

그림 13 2단계 WFQ

4. 시뮬레이션

제안된 자원예약 프로토콜 구현 및 트래픽 서비스 메커니즘의 성능을 평가하기 위해 Opnet Modeler 11.0를 이용하여 시뮬레이션을 수행하였다.

제안된 자원예약 프로토콜의 구현을 위해 Opnet Modeler의 RSVP 프로세서 모델을 수정하였는데, 여기에는 새로운 형태의 Path 메시지와 Resv 메시지 생성 및 처리, PSB 및 RSB 생성 및 처리 등 전체적인 자원예약 프로토콜 수행과정이 모두 포함된다.

제안된 트래픽 서비스 메커니즘의 성능 평가를 위해서 일반적인 VPN 차원 상태 정보 자원준비와 공정한 자원 사용 메커니즘을 적용한 제안하는 VPN 차원 상태 정보 자원준비 방법을 비교하였다. 이후부터는 이들 비교하는 방안들을 각각 plain-VPN과 fair-VPN으로 부르기로 한다.

그림 14는 시뮬레이션을 위한 네트워크 모델을 보여주고 있다. 시뮬레이션 네트워크 모델에서는 세 개의 호스가 존재하는데, 이들 중 H1과 H2는 진입 호스이고 H3은 진출 호스며 이들 호스의 크기는 모두 10Mbps라고 가정하였다. 호스 H1을 통해서는 4Mbps의 CBR 트래픽이 일정하게 네트워크로 유입되도록 하였고 호스 H2를 통해서는 4Mbps~10Mbps의 CBR 트래픽이 유입되도록 하였으며, 이들 트래픽의 목적지는 모두 사이트 3이라 가정하였다. 또한 각 LSR에서의 큐 크기는 512 바이트 패킷 1000개를 저장할 수 있다고 가정하였다.

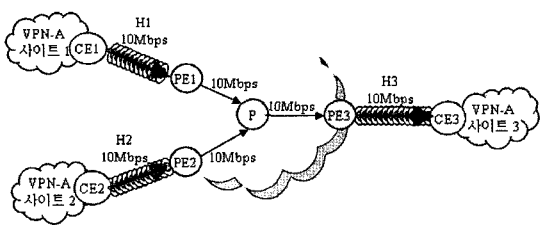

그림 14 시뮬레이션 네트워크 모델

그림 14의 각 링크에는 주어진 호스 매개변수에 따라 VPN 차원 상태 정보 자원준비에 의해서 자원을 할당할 때 그 링크에 예약되어야 하는 자원의 양을 표시하였는데, 사이트 1과 사이트 2로부터 사이트 3을 향하여 보내는 트래픽의 양이 LSR P와 PE3 사이의 링크에 예약된 자원의 양인 10Mbps를 초과하면 LSR *P*에서 혼잡이 발생하게 된다. 이 시뮬레이션 네트워크 모델은 매우 작은 규모이나 제안하는 방안의 효과를 분명하게 보여줄 수 있으며, 일반적인 네트워크에 제안하는 방안을 적용했을 때 VPN의 호스 매개변수와 네트워크 토폴로지에 의해 결과적으로 제안하는 방안의 효과가 나타나게 되는 네트워크 일부분의 성능을 보여 주는 것이라 볼 수도 있다. 여기에서 한 가지 유의할 것은 일반적인 토폴로지의 네트워크에 제안하는 방안을 적용하였을 때, VPN 호스 매개변수와 네트워크 토폴로지에 의해 제안하는 방안의 영향이 나타나지 않는 링크에서는 plain-VPN이 적용된 경우와 동일한 처리가 이루어지기 때문에 결국 제안하는 방안의 효과가 나타나는 네트워크의 국부적인 부분에서의 성능을 살펴보는 것이 의미가 있다는 점이다.

그림 15은 호스 트리 별 처리율을 보여주고 있다. 이 섹션에 제시된 모든 결과 그래프에서 x 축에 표시되어 있는 a:b는 각각 사이트 1과 사이트 2에서 네트워크로 주입하는 트래픽 발생율을 나타낸다. 그림 15에서 혼잡이 발생하지 않을 때에는 즉, a+b가 P와 PE3 사이의 링크에 예약된 대역폭보다 적을 때에는 plain-VPN과 fair-VPN의 성능은 유사하고, 두 방안에서 모두 H1과 H2의 처리율이 각 진입 호스로부터 네트워크로 주입하는 사용자 트래픽 발생율과 거의 동일함을 볼 수 있다. 그러나, 사이트 2로부터 6Mbps 이상의 트래픽이 유입되면 LSR P에서 혼잡이 발생하게 되는데, 이때 plain-VPN에서는 H1과 H2 모두 혼잡의 영향을 받고 이로 인해 사용자 트래픽 발생율보다 처리율이 낮아지게 된다. 반면에, fair-VPN에서는 트래픽 발생율이 혼잡이 발생한 링크상에서의 공정한 몫을 초과하지 않는 H1의 경우에는 그 처리율이 계속 사용자 트래픽 발생율과 거의 동일하게 유지되지만, 공정한 몫을 초과하는 트래픽을 발생시키는 H2의 경우에는 사용자 트래픽 발생율보다 낮은 처리율을 보이게 된다. VPN 차원 상태 정보 따라 VPN QoS를 위한 자원준비를 한다면 특정 목적지를 향하여 하나 이상의 사이트에서 목적지 진출 호스의 대역폭을 초과하는 트래픽을 발생했을 때에만 혼잡이 발생하게 된다. 제안하는 트래픽 서비스 메커니즘은 사이트 간 트래픽 서비스의 우선순위가 명시적으로 제시되지 않은 경우 혼잡이 발생한 링크 상에서의 공정한

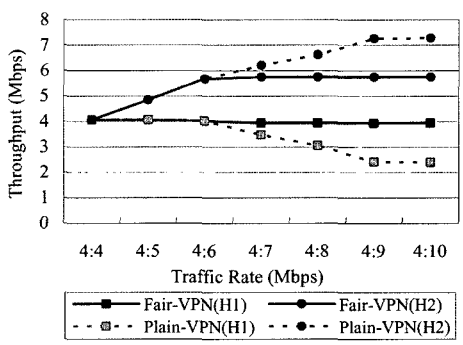

그림 15 처리율

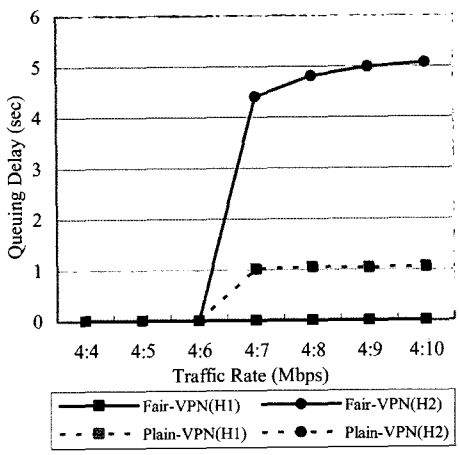

그림 16 LSR P에서의 큐잉 지연

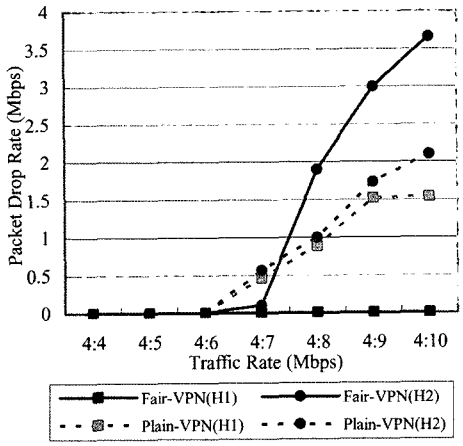

그림 17 LSR P에서의 패킷 손실률

몫보다 적은 양의 트래픽을 발생하는 사용자 사이트에 대해서는 트래픽 손실이 발생하지 않도록 하는 것이다.

그림 16과 17은 혼잡이 발생하는 LSR *P*에서의 호스별 큐잉 지연과 패킷 손실률을 보여주고 있다. H1과 H2의 사용자 트래픽 발생율의 합이 LSR P와 PE3사이의 링크에 예약된 대역폭을 초과하지 않았을 시에는 H1과 H2에 대해 모두 큐잉 지연과 패킷 손실이 거의 발생하지 않는다. 혼잡이 발생하는 경우 즉, H2의 사용자 트래픽 발생율이 6Mbps이상인 경우, Plain-VPN에서는 H1과 H2 모두 큐잉 지연과 패킷 손실이 발생하게 되고, H2의 트래픽 발생률이 증가함에 따라 큐잉 지연이나 패킷 손실은 모두 더 커지게 된다. 그러나 fair-VPN에서는 사용자 트래픽 발생율이 혼잡 링크상에서의 공정한 몫을 초과하지 않는 H1에 속하는 트래픽에 대해서는 성능저하가 나타나지 않는다. 즉, fair-VPN에서는 H1에 속하는 트래픽의 지연이나 패킷 손실이 거의 없는 상태가 계속 유지된다. 반면에 공정한 몫을 초과하여 트래픽을 발생하는 H2의 경우 P와 PE3 사이의 링크를 지나는 VPN 트래픽 양이 VPN을 위해 할당된 대역폭인 10Mbps를 넘게 되면 지연과 패킷 손실이 급격히 증가하게 된다.

끝으로 제안하는 방안의 확장성에 대해 고려해 보고자 한다. 일반적으로 RSVP는 사용자 플로우별 처리 및 상태 정보 유지를 요하기 때문에 확장성 문제를 야기한다. 그러나 제안하는 방안의 경우 개별 사용자 플로우별 자원준비가 아닌 VPN 별 자원 준비를 위해 RSVP 기반 시그널링을 사용하므로 RSVP의 일반적 확장성 문제가 발생하지는 않는다. QoS를 지원하지 않는 일반적인 사업자 기반 VPN (Provider Provisioned VPN)인 BGP/MPLS VPN[9]과 비교했을 때 BGP/MPLS VPN에서는 임의의 두 PE 사이에 최소 1개의 LSP를 설정하여 n개의 서로 다른 VPN 트래픽을 다중화한다면 제안하는 메커니즘에서는 각 VPN 별로 LSP를 두어야 하기 때문에 n개 서로 다른 VPN을 서비스하기 위해서는 n개의 LSP가 필요하게 된다. 그러나 두 PE간 설립되는 하나의 LSP에서는 동일한 VPN 사이트에 속하는 모든 사용자들의 트래픽이 다중화 되기 때문에 개별 사용자 플로우 수준의 확장성 문제는 발생하지 않는다.

5. 결 론

본 논문에서는 VPN 차원 상태 정보 자원준비에 따라 동적이고 자동적으로 VPN QoS 지원을 위한 자원 예약을 수행하는 프로토콜과 함께 VPN 사용자들이 예약된 자원을 공정하게 사용할 수 있도록 하는 트래픽 서비스 메커니즘을 제안하였다.

본 논문에서 제안한 자원 예약 프로토콜은 VPN 차원 상태 정보 자원준비 방식에 따라 자원을 예약하므로 네트워크 사업자의 다중화 이득을 향상시키고, 자원의 활용률을 높여준다. 또한 임의의 VPN을 위해 두 PE간 설립된 LSP는 해당 VPN의 사이트에 속하는 모든 사용자들이 공유하게 되므로 일반적인 RSVP의 사용자 플로우별 서비스에 의한 확장성 문제가 발생하지 않는다. 또한, 시뮬레이션을 통하여, 본 논문에서 제안한 트래픽 서비스 메커니즘은 VPN을 위해 준비된 자원보다 더 많은 VPN 트래픽 부하가 발생할 때에도 공정한 몫보다 적은 양의 트래픽을 발생하는 VPN 사용자 사이트에 대해서는 트래픽 손실이 발생하지 않도록 함을 볼 수 있었다. 즉, 제안하는 트래픽 서비스 메커니즘에 의하여 VPN 사용자 사이트 간에 공정한 자원사용이 이루어짐을 볼 수 있었다.

참 고 문 헌

[1] N.G. Duffield, P. Goyal, A. Greenberg, P. Mishra, K.K. Ramakrishnan, J. E. Van der Merwe, "Resource Management With Hoses: Point-to-Cloud Services for Virtual Private Networks," IEEE/ACM Transactions on Networking, Vol.10, No.5, October 2002.

[2] Alpar Juttner, Istvan Szabo and Aron Szentesi, "On Bandwidth Efficiency of the Hose Resource Management Model in Virtual Private Networks," IEEE INFOCOM 2003.

[3] A. Kumar, R. Rastogi, A. Silberschatz, B. Yener, "Algorithms for Provisioning Virtual Private Networks in the Hose Model," IEEE/ACM Transactions on Networking, Vol.10, No.4, August 2002.

[4] Gustavo de Veciana, Sangkyu Park, Aimin sang and Steven Weber, "Routing and Provisioning VPNs based on Hose Traffic Models and/or Constraints," Conference on Communication Control & Computing, 2002.

[5] Thomas Erlebach, Maurice Ruegg, "Optimal Bandwidth Reservation in Hose-Model VPNs with Multi-Path Routing," INFOCOM, Vol.4, March 2004.

[6] Yu-Liang Liu, Yeali S.Sun, Meng Chang Chen, "MTRA: An On-Line Hose-Model VPN Provisioning Algorithm," Technical Report, 2004.

[7] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan, G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels," RFC3209, December 2001.

[8] R. Aggarwal, D. Papadimitriou, S. Yasukawa, "Extensions to RSVP-TE for Point to Multipoint TE LSPs," draft-ietf-mpls-rsvp-te-p2mp-03.txt, October 2005.

[9] Eric C. Rosen, Yakov Rekhter, "BGP/MPLS IP VPNs," draft-ietf-l3vpn-rfc2547bis-03.txt, October 2004.

변 해 선

2001년 광주대학교 컴퓨터학과 졸업(학사). 2003년 이화여자대학교 과학기술대학원 컴퓨터학과 졸업(공학석사). 2003년~현재 이화여자대학교 컴퓨터학과 박사과정. 관심분야는 Virtual Private Network, Internet QoS, BcN and NGN, Mobile VPN

우 현 제

2004년 이화여자대학교 컴퓨터학과 졸업(학사). 2004년~현재 이화여자대학교 컴퓨터학과 석사과정. 관심분야는 MVPN, NEMO, VPN QoS

김 경 민

2005년 이화여자대학교 컴퓨터학과 졸업(학사). 2005년~현재 이화여자대학교 컴퓨터학과 석사과정. 관심분야는 VPN QoS 지원, 모바일 VPN, 무선 네트워크

이 미 정

정보과학회논문지 : 정보통신
제 33 권 제 1 호 참조