BcN VPN을 위한 QoS 기술

이화여자대학교 변해선, 이미정

목 차

I. 서 론

현재 VPN은 주로 기업 고객을 대상으로 사설망을 보완하거나 대체하는 역할을 하고 있지만, BcN에서의 VPN(Virtual Private Network)은 VCN(Virtual Community Network) 그룹, 온라인 가상 게임, 소규모의 동호회 등 개인 사용자 그룹이 기업 고객과 더불어 주된 고객이 될 것으로 예상된다. 이에 따라 VPN의 수요가 증가하고 동적 VPN 형성 및 QoS(Quality of Service) 지원이 매우 중요한 이슈가 될 것이다. 동적이고 자동적인 VPN QoS 지원을 위해서는 사업자와 고객간의 SLA(Service Level Agreement), 다양한 사업자간의 SLA, 네트워크 관리, 라우팅, 트래픽 엔지니어링, 접근제어, 자원 프로비저닝, 자원예약 프로토콜 등이 제공되어야 한다.

본 고에서는 국제 표준화 기관에서의 VPN 관련 표준화 동향을 알아보고, VPN QoS 지원에 관련된 기술과 BcN에서의 VPN QoS를 지원하기 위한 서비스 구조 등을 살펴본 후 결론을 맺는다.

II. VPN을 위한 표준화 동향

IETF(Internet Engineering Task Force)에서는 L3VPN(Layer 3 Virtual Private Networks), L2VPN(Layer 2 Virtual Private Networks), L1VPN(Layer 1 Virtual Private Networks) 워킹그룹에서 VPN과 관련한 표준화 작업이 이루어지고 있다.

IETF L3VPN 워킹그룹에서는 L3VPN 서비스 요구사항(RFC 4031), L3VPN 프레임워크(RFC 4110)에서 설명한 바와 같이, 3계층에서의 CE-기반 VPN과 네트워크 기반 VPN의 표준화를 진행하고 있다. 대표적인 작업으로는 BGP/MPLS VPN(RFC 2547)을 기반으로 확장한 BGP/MPLS IP VPN (RFC 2547bis), Virtual Router IP VPN[1],

CE(Customer Edge) 기반 IPSec VPN[2] 등이 있다. 또한 VPN 사이트들이 인터-AS(Autonomous System)간 또는 인트라-AS를 통해 연결되는 다양한 VPN 구성 시나리오를 고려하고 있으며, 이러한 환경에서의 VPN을 위한 IP 멀티캐스트 및 IPv6 구축에 대한 연구를 진행하고 있다.

IETF L2VPN 워킹그룹에서는 2계층에서의 VPN 서비스를 제공하기 위한 표준화 작업을 진행 중이며, 대표적인 작업으로는 VPLS(Virtual Private LAN Service)[3], VPWS(Virtual Private Wire Service)[4], IPLS(IP-only VPNs)[5]에 관한 표준화 작업을 진행하고 있다. L2VPN 워킹 그룹에서는 인트라-AS를 통해 연결되는 VPN 구성 시나리오만을 고려하고 있다.

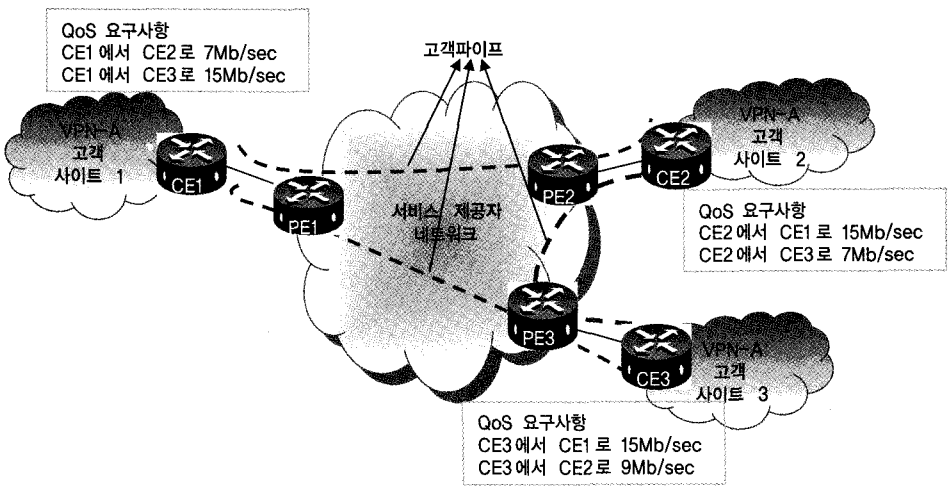
IETF L1VPN 워킹그룹에서는 GMPLS (Generalized MPLS) 네트워크상에서 CE 장비간의 1계층 VPN 서비스를 제공하기 위한 작업을 진행하고 있다. 1계층 VPN은 2계층, 3계층에서의 VPN 제어기술과 관리기술을 TDM(Time-division multiplexing)과 OTN(Optical transport network) 등의 1계층에 적용하여 VPN 서비스를 제공한다. L1VPN 워킹그룹에서는 1계층 VPN의 프레임워크[6], 네트워크 서비스 모델, 응용성[7], 시그널링 및 라우팅 스펙에 대한 작업을 진행하고 있으며, 현재는 인트라-AS을 통해 연결되는 VPN 구성 시나리오만을 고려하고 있다.

ITU-T(International Telecommunication Union - Telecommunication Standardization Sector) SG(Study Group)13에서는 1계층에서의 VPN 서비스와 구조(Y.1312, Y.1313)를 정의하였으며 IETF의 L1VPN 워킹그룹과의 공동 작업 추진을 고려하고 있다.

III. VPN을 위한 QoS 관련 기술

3.1 VPN QoS 서비스 모델

VPN QoS를 지원하기 위한 대표적인 서비스 모델로는 고객 파이프(Customer Pipe) 모델과 호스



(그림 1) 고객 파이프 모델

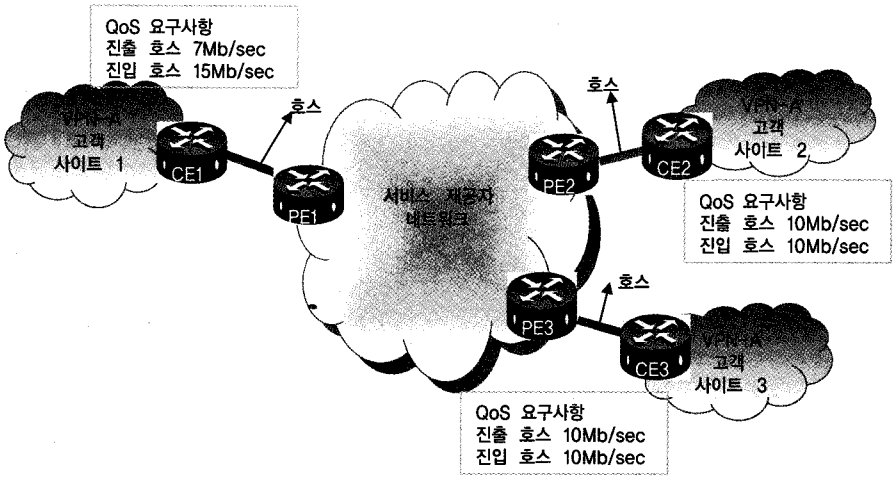
(Hose) 모델이 있다. 고객 파이프 모델에서는 (그림 1)에서 보는 바와 같이 사용자가 모든 VPN 사이트 쌍간 요구 대역폭을 QoS 요구사항으로 명시하고, 서비스 제공자는 CE(Customer Edge) 라우터 간 고객 파이프를 설립하여 자원을 예약한다. 이러한 고객 파이프 모델은 QoS 요구사항 명시가 복잡하고, 멀티플렉싱 이점을 전혀 얻을 수 없다는 문제점을 가진다.

고객 파이프 모델에서의 단점을 해결하기 위해 호스 모델이라는 새로운 VPN QoS 서비스 모델이 제안되었다. 호스는 각각의 VPN CE 라우터를 서비스 제공자 네트워크의 PE(Provider Edge) 라우터에 연결하는 인터페이스를 의미하며, 호스 모델에서는 QoS 요구사항으로 진입 호스(CE로부터 PE로 가는 방향의 호스)와 진출 호스(PE로부터 CE로 가는 방향의 호스)의 트래픽 양과 성능기대치를 명시한다. 이러한 호스 모델은 고객 파이프 모델에 비해 사용자 측에서의 QoS 요구사항 명시가 용이하고, 호스를 통해 유입되는 VPN 사용자 트래픽이 동일 VPN에 속하는 사이트 중 어느 곳이라도 전송될 수 있으므로 사용자가 VPN 자원을 보다 유연하게 활용할 수 있는 장점을 가진다. 그리고 일반적으로 고객 파이프들이 필요로 하는 대역폭의 합보다는 호스에 대해 적은 양의 대역폭을 구입해도 되므로 사용자가 엑세스 링크에서의 멀티플렉싱 이점을 취할 수 있다. 그러나 네트워크 서비스 제공자의 입장에서는 간단해진 VPN 고객의 QoS 요구사항 명세를 가지고 네트워크를 프로비저닝 해야 하기 때문에 효율적인 프로비저닝 및 자원관리 메커니즘이 요구된다.

3.2 자원 프로비저닝 메커니즘

서비스 제공자 네트워크에서의 멀티플렉싱 이점을 취하기 위해 현재 호스 모델을 위한 VPN 자원 프로비저닝 메커니즘은 사업자 파이프 기반, 호스 상태 기반, VPN 상태 기반 등으로 분류할 수 있다.

호스 모델 프로비저닝 메커니즘 중 가장 간단한 사업자 파이프 기반 프로비저닝은 (그림 3)과 같이 CE와 PE간의 호스 각각에 대하여 해당 PE 라우터 쌍간에 디폴트 최단 경로를 따라 사업자 파이프를 설정하되, 각 사업자 파이프에는 그 사업자 파이프의 진입

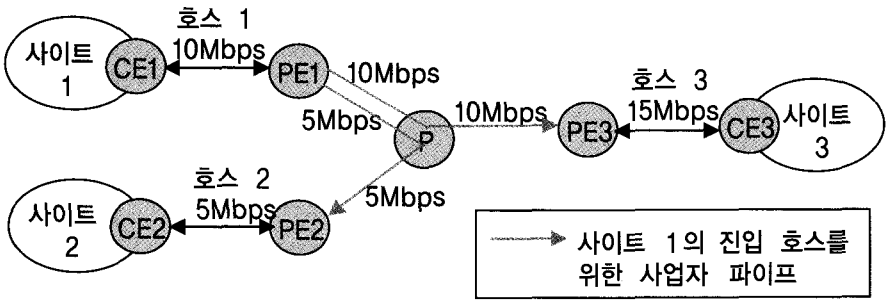


(그림 2) 호스 모델

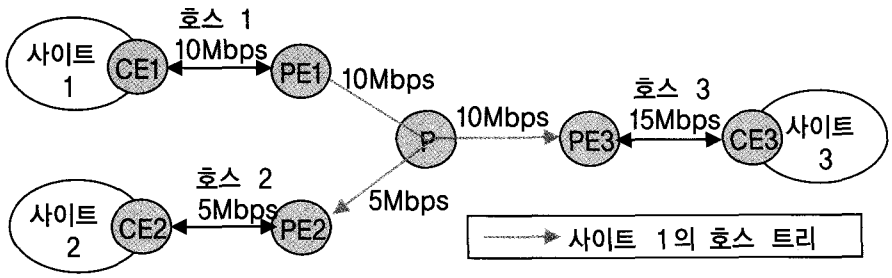
호스로부터 유입될 수 있는 트래픽 전체가 해당 사업자 파이프의 진출 호스로 모두 나가는 최악의 경우에 해당하는 트래픽 분포를 가정하고 자원을 할당한다. 또한, 사업자 파이프간의 자원공유를 고려하지 않기 때문에 각 링크에서는 VPN의 사업자 파이프별로 자원을 할당하며, 각 사업자 파이프를 위해 그 사업자 파이프의 진입 호스와 진출 호스 크기 중 더 작은 값 만큼의 자원을 할당한다.

호스 상태 기반 프로비저닝에서는 자원공유 가능성과 호스 상태 정보를 활용하여 네트워크에서 VPN을 위해 할당해야 하는 자원 양을 절감한다. 호스 상태 기반 프로비저닝에서는 (그림 4)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 호스 트리를 형성한다. 그리고 호스 트리의 진입, 진출 호스 파라미터들의 정보와 함께 호스 트리를 구성하는 PE간 사업자 파이프들이 자원을 공유할 수 있음을 고려하여 호스 트리 상의 각 링크에 예약되는 자원의 양을 결정한다. 구체적으로 호스 상태 기반 프로비저닝에서는 각 링크에 호스 트리별로 자원을 예약하며, 임의의 링크에서 특정 호스 트리를 위해 예약하는 자원의 양은 그 호스 트리의 진입 호스 크기와 임의의 링크를 경유해서 도달할 수 있는 PE의 진출 호스들 크기의 합 중 더 적은 값이 된다[8].

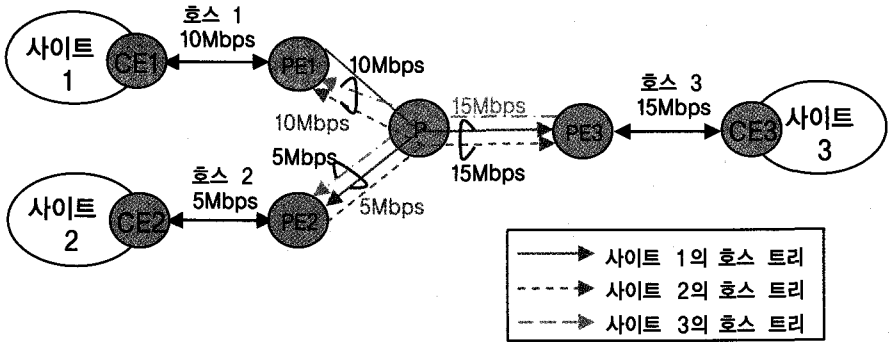
VPN 상태 기반 프로비저닝에서는 (그림 5)에서와 같이 VPN을 구성하는 모든 호스들의 파라미터 정보를 동시에 고려한다. 또한 해당 VPN을 서비스하는 PE들을 모두 연결하는 그래프 혹은 트리 상에 예약되는 자원은 그 VPN에 속하는 모든 호스트들에 의해서 공유할 수 있음을 고려하여 예약될 자원의 양을 결정함으로써 한층 더 VPN을 위해 할당하는 자원의 양



(그림 3) 사업자 파이프 기반 프로비저닝에서 사이트 1의 진입 호스를 위한 자원할당



(그림 4) 호스 상태 기반 프로비저닝에서 사이트 1의 호스 트리를 위한 자원할당



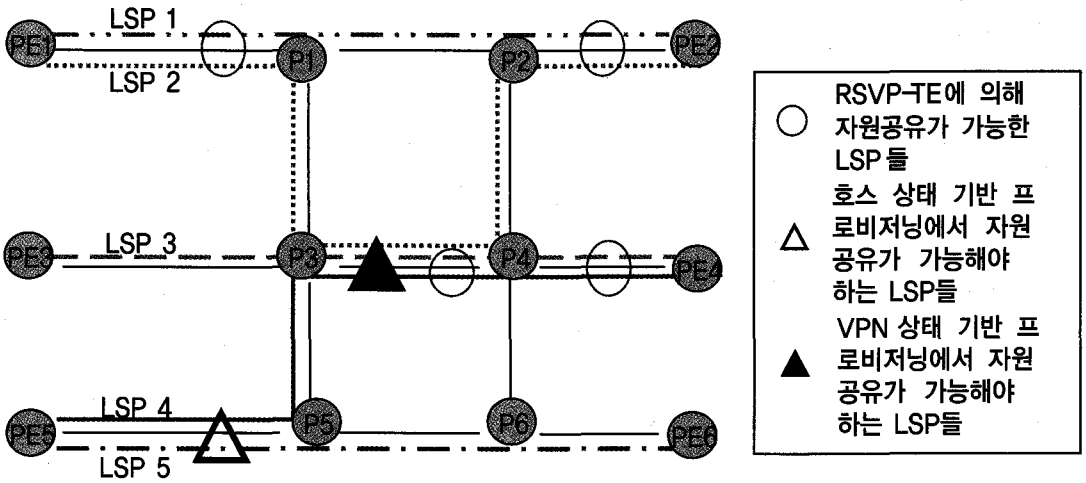
(그림 5) VPN 상태 기반 프로비저닝에서의 자원할당

을 절감한다. 구체적으로 VPN 상태 기반 프로비저닝에서는 VPN 별로 자원을 할당하되 임의의 링크에 특정 VPN을 위해 예약하는 자원의 양은 그 링크를 경유하는 해당 VPN의 모든 호스 트리들의 진입 호스 크기의 합과 진출 호스 크기 합 중 더 적은 값이 된다[8].

3.3 자원예약 프로토콜

VPN QoS 프로비저닝을 위해 고려되어야 할 또 다른 매우 중요한 이슈는 이들 프로비저닝 메커니즘들을 네트워크에 동적이고 자동적으로 적용하는 것이다. 이를 위해서는 이들 프로비저닝 메커니즘에 따라 자원예약을 수행하는 프로토콜이 필요하다.

RSVP-TE는 MPLS 네트워크에서 P2P TE LSP(Poiint-to-Point Traffic Engineering Label Switched Path)를 설립하기 위한 프로토콜이다[9]. 호스 모델을 위한 프로비저닝 메커니즘 중 사업자 파

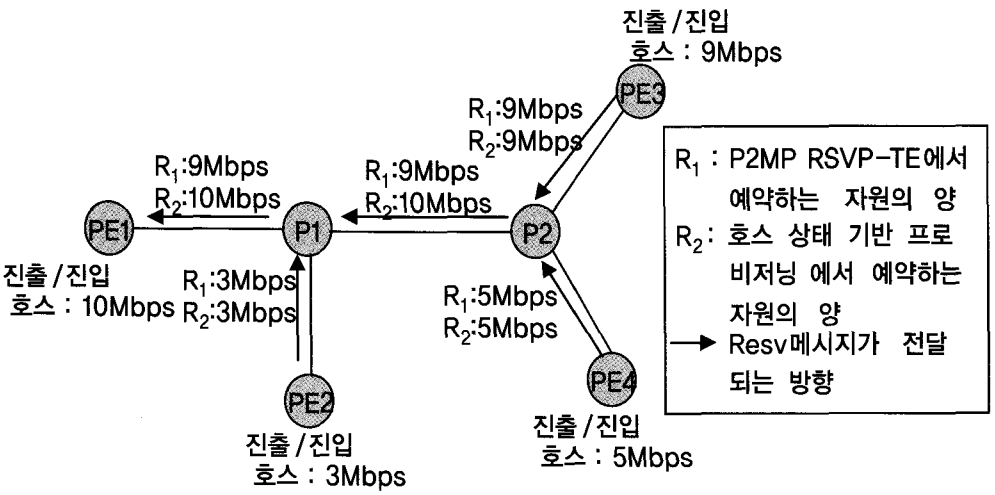


(그림 6) RSVP-TE와 호스 상태 기반/ VPN 상태 기반 프로비저닝에서의 자원공유

이프 기반 프로비저닝은 RSVP-TE 메커니즘을 그대로 적용함으로써 구현할 수 있다. 그러나 호스 상태 기반이나 VPN 상태 기반 프로비저닝 메커니즘은 단순히 RSVP-TE 메커니즘을 적용함으로써 구현할 수 없다. RSVP-TE에서는 자원공유 옵션 중에 하나인 SE(Shared Explicit) 스타일을 이용하여 동일한 세션을 가진 LSP들간 자원공유가 가능하다. RSVP-TE의 세션 객체에는 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 프로비저닝 메커니즘은 터널의 진출 혹은 진입 종단점이 동일하지 않는 LSP들간의 자원 공유도 지원해야 한다.

(그림 6)은 RSVP-TE에서 지원하는 자원 공유와 호스 상태 기반이나 VPN 상태 기반 프로비저닝 메커니즘에서 지원되어야 하는 자원 공유를 나타낸 것이다. LSR(Label Switching Router)인 PE5와 P5를 연결하는 링크를 통과하는 LSP4와 LSP5는 터널의 진출 종단점이 다르지만 VPN의 동일 호스를 서비스하는 LSP들이라면 호스 상태 기반 메커니즘으로 자원을 프로비전하는 경우 서로 자원을 공유할 수 있어야 한다. P3과 P4를 연결하는 링크를 통과하는 LSP2, LSP3, LSP4는 터널의 양 종단점이 모두 다른 경우이지만 VPN 상태 기반 프로비저닝의 경우 동일 VPN을 서비스하는 LSP들이라면 서로 자원을 공유할 수 있어야 한다. 따라서 RSVP-TE는 호스 상태 기반이나 VPN 상태 기반 프로비저닝을 위한 자원예약을 수행할 수 없다.

P2MP(Point-to-Multipoint) RSVP-TE는 P2MP TE LSP 설립하기 위해 RSVP-TE를 확장한 프로토콜로 멀티캐스트 트래픽 전송을 위한 자원예약을 수행한다[10]. P2MP RSVP-TE에 의해서 설정된 P2MP TE LSP는 특정 집합의 진입 PE를 루트로 하여 트리를 구성하는 하나 이상의 P2P sub-LSP들로 구성되며, 동일한 P2MP TE LSP에 속하는 P2P sub-LSP들 간에는 P2P sub-LSP 터널의 진출 PE가 다르더라도 서로 자원을 공유하도록 한다. 또한 P2MP TE Tunnel은 동일한 P2MP 세션에 속하는 하나 이상의 P2MP TE LSP들로 구성되는데,



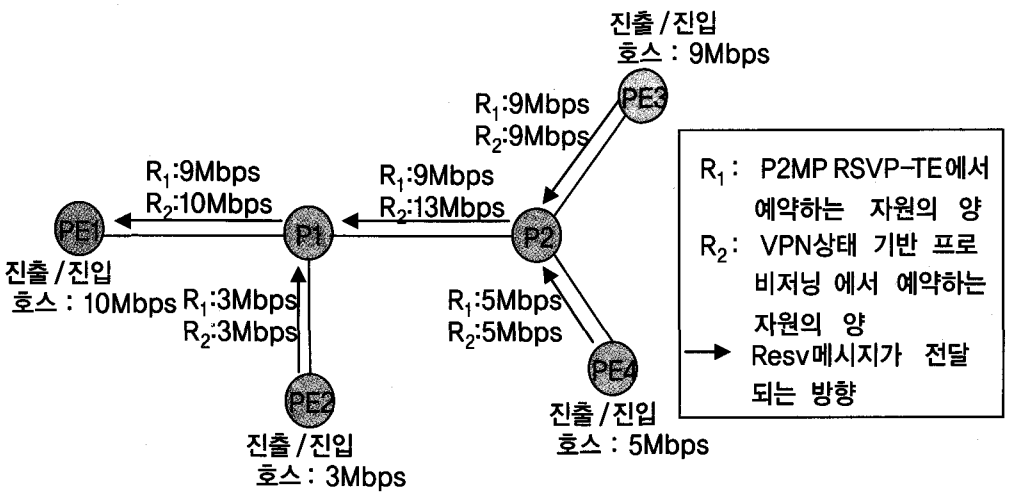
(그림 7) PE1의 진입 호스를 위해 P2MP RSVP-TE와 호스 상태 기반 프로비저닝에서 각 링크에 예약하는 자원의 양

동일한 P2MP TE Tunnel에 속하는 P2MP TE LSP들의 P2P sub-LSP들은 양 종단점이 모두 다르더라도 서로 자원을 공유할 수 있다. 이와 같은 P2MP RSVP-TE의 특성은 호스 상태 기반이나 VPN 상태 기반 프로비저닝의 자원공유 요건을 만족한다.

그러나, P2MP RSVP-TE에서는 호스 상태 기반 또는 VPN 상태 기반 프로비저닝에서 각 링크에 예약되어야 할 자원의 양을 계산하는 방식을 적용하지 못한다. P2MP RSVP-TE에서는 RSVP-TE 메커니즘을 이용하여 자원을 예약하기 때문에 임의의 링크 상에서 자원을 공유하는 P2P sub-LSP들을 위해 예약되는 자원의 양 중에서 최대값을 예약하게 된다. 따라서 호스 상태 기반 또는 VPN 상태 기반 프로비저닝에 따르는 각 링크에 예약되어야 할 자원의 양을 계산하는 방식을 적용하지 못한다.

(그림 7)은 P2MP RSVP-TE에서 각 링크에 예약하는 자원의 양이 호스 상태 기반 프로비저닝에서 예약되어야 하는 자원의 양과 어떻게 다른지에 대한 예를 보이고 있다. P2MP RSVP-TE는 자원을 공유하는 P2P sub-LSP들을 위해 예약되는 자원의 양 중에서 최대값을 예약하게 된다. 그러나 호스 상태 기반 프로비저닝에서는 각 링크에서 진입 PE의 호스의 값과 그 링크를 통과해서 P2P sub-LSP가 맺어지는 진출 PE들의 호스 파라미터의 합 중 더 적은 값에 해당하는 자원을 예약해야 한다. (그림 7)에서 보는 바와 같이, PE1이 진입 호스의 크기인 10Mbps의 자원예약을 요청하는 Path 메시지를 보내고 이를 PE2, PE3, PE4에서 각각 받았다고 가정해보자. 각 PE2, PE3, PE4는 진출 호스의 크기인 3Mbps, 9Mbps, 5Mbps의 자원을 예약하는 Resv 메시지를 보낸다. 중간의 LSR인 P2에서는 PE3과 PE4의 Resv 메시지를 받고 자원을 공유해야 하는 P2P sub-LSP임을 인식한 후, 두 P2P sub-LSP중에 더 큰 값의 자원을 예약하는 9Mbps를 선택한다. 또한 P1에서도 마찬가지로 PE2와 P2로부터 받은 Resv 메시지 중에 더 큰 값의 자원을 예약하는 9Mbps를 선택한다.

그러나 호스 상태 기반 프로비저닝에서는 각 링크에서 진입 PE의 호스의 값과 그 링크를 통과해서 P2P sub-LSP가 맺어지는 진출 PE들의 호스 파라



(그림 8) P2MP RSVP-TE와 VPN-specific state 프로비저닝에서 각 링크에 예약하는 자원의 양

미터의 합 중 더 적은 값에 해당하는 자원을 예약해야 한다. P2가 PE3과 PE4로부터 9Mbps, 5Mbps를 예약하는 Resv 메시지를 받았을 때, 진입 호스가 요구하는 자원의 양인 10Mbps와 P1 링크와 P2 링크를 통하여 받을 수 있는 진출 호스 파라미터의 합인 14Mbps 중 더 적은 값에 해당하는 10Mbps를 선택한다. P1은 진입 호스가 요구하는 자원의 양인 10Mbps와 PE1 링크와 P1 링크를 통하여 받을 수 있는 진출 호스 파라미터의 합인 17Mbps 중 더 적은 값에 해당하는 10Mbps를 선택한다.

(그림 8)은 P2MP RSVP-TE에서 각 링크에 예약하는 자원의 양이 VPN 상태 기반 프로비저닝에서 예약되어야 하는 자원의 양과 어떻게 다른지에 대한 예를 보이고 있다. P2MP RSVP-TE에서는 여러 개의 진출 호스에 대한 P2MP TE LSP가 경유하는 링크에서 이들 P2MP TE LSP중 가장 지원 요구가 큰 P2MP TE LSP가 요구하는 값을 예약하는 반면, VPN 상태 기반 프로비져닝에서는 각 링크상에서 그 링크를 경유하는 모든 진입 PE의 호스 파라미터의 합과 모든 진출 PE의 호스 파라미터의 합 중 더 적은 값에 해당하는 자원을 예약한다. (그림 8)에서 보는 바와 같이, P2에서 P1로 가는 링크에는 PE1의 진입 호스를 위한 P2MP TE LSP에 대한 Resv 메시지와 PE2의 진입 호스를 위한 P2MP TE LSP에 대한 Resv 메시지가 지나간다. 이때 P2MP RSVP-TE의 P2MP TE Tunnel 차원에서 P2가 P1에게 보내는 Resv 메시지에 들어가는 공유할 자원의 예약될 양은 PE1을 위해 예약하는 자원의 양인 9Mbps와 PE2를 위해 예약되는 자원의 양 인 3Mbps 중 더 큰 값인 9Mbps가 선택된다.

반면, VPN 상태 기반 프로비저닝에서는 PE1과 PE2의 진입 호스의 합인 13Mbps와 PE3과 PE4의 진출 호스의 합인 14Mbps 중 더 적은 값인 13Mbps를 선택된다. 또한 P1에서 PE1으로 가는 Resv 메시지에는 PE1의 진입 호스인 10Mbps와 PE2, PE3, PE4의 진출 호스인 17Mbps 중 더 작은 값인 10Mbps가 선택된다.

P2MP RSVP-TE가 호스 상태 기반과 VPN 상태 기반 프로비저닝 메커니즘에서 요구하는 자원의 양을 계산하는 방식을 지원하지 않는 것과 더불어 P2MP RSVP-TE 호스 모델에 적합하지 않는 또 하나의 이유가 있다. P2MP RSVP-TE는 멀티캐스트 데이터 전송을 목적으로 하므로 유니캐스트 전송을 위한 레이블 할당 및 스위칭이 이루어지지 않는다.

위에 본 바와 같이, 기존의 표준화 된 자원 예약 프로토콜에 의해서는 VPN 호스 모델을 지원하기 위한 호스 상태 기반이나 VPN 상태 기반 프로비저닝을 위한 자원예약을 수행하지 못한다. 따라서 새로운 자원 예약 프로토콜을 정의하거나 기존의 자원예약 프로토콜을 확장한 프로토콜이 제시되어야 할 것이다. 이를 위해 [11]에서는 호스 상태 기반과 VPN 상태 기반 프로비저닝을 위한 자원예약을 수행하기 위해 P2MP RSVP-TE를 확장한 자원예약 프로토콜을 제안하였다.

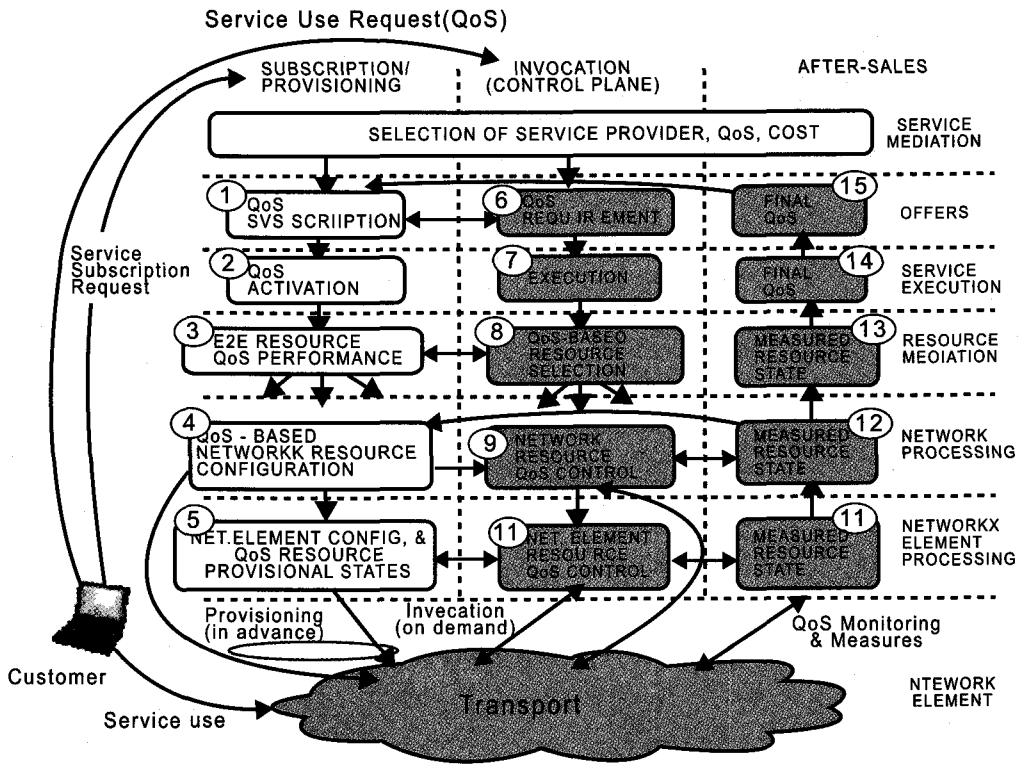
제안된 자원예약 프로토콜에서는 호스 상태 기반과 VPN 상태 기반 프로비저닝 메카니즘 각각에 대하여 RSVP 메시지 구조, PSB(Path State Block) 및 RSB(Reservation State Block) 구조, RSVP 메시지 프로세싱 방법, 각 프로비저닝 메카니즘에 따라 예약되어야 하는 자원의 양을 계산하는 방식 등을 제공한다. 또한 P2P sub-LSP상에서의 유니캐스트 전송을 위한 레이블 할당을 지원한다.

한편, VPN 상태 기반 프로비저닝은 VPN을 위해 할당해야 하는 자원을 최소화한다는 측면에서는 호스 상태 기반 프로비저닝 보다 효율적이지만, 각 VPN에 대하여 예약된 자원을 그 VPN에 속하는 사용자들이 공유하기 때문에 동일한 VPN에 속하는 사용자들 간에 불공평하게 자원을 사용할 수 있는 문제

가 있다. 이것은 전통적인 LAN 대역폭을 그 LAN에 속하는 호스트들이 공유하는 경우에 발생하는 문제와 유사하다. [12]에서는 자원 활용을 최적화하기 위해 VPN 상태 기반 프로비저닝 방식으로 자원을 할당하되, VPN을 위해 할당된 자원을 VPN의 트래픽 소스들이 공평하게 사용할 수 있도록 하는 트래픽 서비스 메커니즘을 제안하였다. 이 메커니즘에서는 호스 상태 기반에 의해 자원을 할당 할 때 각 트래픽 소스에 대해 할당되는 자원의 양에 비례하여 VPN을 위해 할당된 자원을 VPN 트래픽 소스들이 공유하는 것을 공평한 사용으로 본다. 즉, 임의의 라우터 인터페이스에서는 호스 상태 기반 프로비저닝에 의해 트래픽 소스별로 할당받게 되는 자원양의 비율에 따라 트래픽 서비스 비중(Weight)을 정하고, 이 비중에 따르는 WFQ를 적용하여 VPN 트래픽을 서비스 한다.

IV. BcN VPN을 위한 QoS 서비스 구조

ITU-T FGNGN(Focus Group on Next Generation Networks)에서는 NGN 관련 기술의 표준화 작업을 진행하고 있는데, 그 중에서 FGNGN의 워킹그룹 3에서 종단간 QoS 아키텍쳐를 위한 요



(그림 9) NGN에서의 종단간 QoS 프레임워크 모델

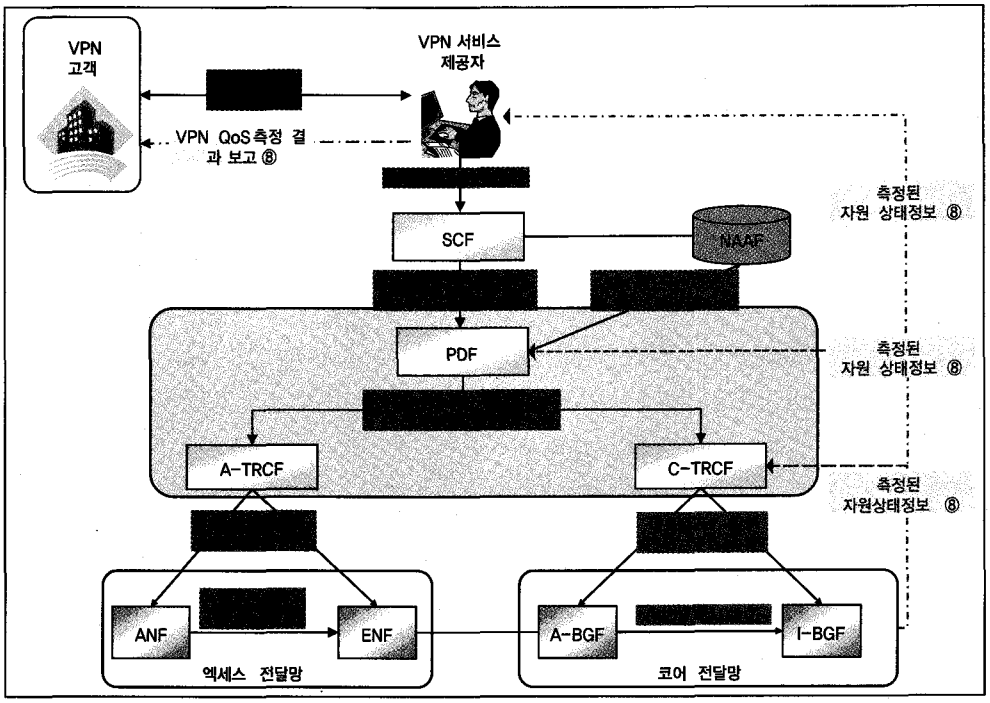
구사항과 프레임워크 등의 QoS와 관련된 표준화 작업을 진행하고 있다.

(그림 9)는 FGNGN의 워킹그룹 3에서 정의한 NGN에서의 종단간 QoS 프레임워크 모델을 나타낸 그림이다[13]. (그림 9)에서 보는 바와 같이, 사업자가 QoS 서비스를 제공하는 사이클은 크게 서비스 가입/프로비저닝 과정, 요구기반 서비스 구동 과정, 판매 후 과정으로 나눠진다. 서비스 가입/프로비저닝 과정에서는 먼저, 사업자와 고객간 서비스 및 QoS를 협상하고 SLA를 맺는다(①). SLA 협약이 이루어지고 나면 사업자는 서비스를 제어하는 개체인 SCF(Service Control Function)에게 고객이 가입한 서비스 구동을 요청한다. 서비스 구동 요청을 받은 SCF는 네트워크 및 사용자 정책을 결정하는 개체인 PDF(Policy Decision Function)에게 자원 프로비저닝 프로세스를 수행할 것을 요청한다(②). 자원 프로비저닝 프로세스 요청을 받은 PDF는 고객이 요구한 종단간 서비스 파라미터를 네트워크상의 자원 파라미터로 변환하고 그에 관련된 매핑정보 및 정책을 NAAF(Network Access Attachment Function)에 저장한다. NAAF는 사용자 등록정보, 인증, 접근권한 등의 정보를 유지하고 있는 개체이다. PDF는 또한 고객이 요구한 종단간 QoS를 지원하기 위해 전달망의 자원을 제어하는 TRCF(Transport Resource Control Function)에게 네트워크 자원 구성(configuration)을 지시한다(③). TRCF는 인터페이스, 버퍼 등에 필요한 자원을 할당 할 수 있는 경로를 검색하여 QoS 지원이 가능한 명시적 경로를 따라서 네트워크 개체(라우터 등) 인터페이스에 QoS 파라미터를 설정/관리한다(④). 명시적 경로상에 있는 네트워크 개체들은 설정된 파라미터 및 자원 사용의 프로비전 상태 정보를 유지/관리한다(⑤).

요구기반 서비스 구동 과정에서는 고객으로부터 서비스 사용에 대한 요구가 들어오면 서비스를 제어하는 개체인 SCF(Service Control Function)가 고객이 가입한 QoS와 고객이 요구한 QoS를 비교하여 이에 대한 서비스 지원여부를 결정한다(⑥). 고객이 요구한 QoS가 타당하면 고객의 요구에 적합한 서비스를 제공해주기 위해 QoS 데이터 처리 프로세스를 수행할 것을 PDF에게 요청한다(⑦). PDF는 NAAF에 저장된 사용자 접근권한 및 QoS 매핑정보를 기반으로 종단간 QoS를 지원하기 위한 자원을 선택한 후, TRCF에게 이에 대한 자원 요청을 지시한다(⑧). TRCF는 모니터링 및 측정에 의해서 획득된 네트워크 상태 정보 및 자원 사용률을 기반으로 자원 요청에 대한 승인제어(Admission Control) 여부를 결정하여 승인이 되면 네트워크 개체에 자원 파라미터 설정을 요청한다(⑨). 네트워크 개체에서는 실제 자원 상태 정보를 기반으로 자원 사용을 위한 승인제어 여부를 결정한다(⑩).

판매 후 과정에서는 각 QoS 서비스를 지원하는 개체들이 네트워크 모니터링과 측정을 통하여 남아있는 자원 및 큐 사용률 등을 체크하여 이에 대한 QoS 측정 결과를 자신의 상위 레벨의 개체에게 보고하며 최종적으로 그 결과는 고객에게 보고된다(⑪~⑮).

(그림 10)은 (그림 9)의 FGNGN에서 정의한 종단간 QoS 프레임워크 모델을 BcN VPN QoS 제공에 적용해 본 그림이다. VPN 고객은 요구하는 VPN QoS를 명시하여 VPN 서비스 제공자와 VPN SLA를 맺는다(①). 그러면 VPN 서비스 제공자는 SCF에서 VPN 서비스 구동을 요청하고(②), SCF는 PDF에게 네트워크상에 자원 프로비저닝 프로세스를 수행할 것을 요청한다(③). 이 요청을 받은 PDF는 VPN QoS 파라미터와 이를 지원하기 위한 자원 파라미터의 매핑 정보를 NAAF에 저장해놓고(④), TRCF에게 네트워크 자원 구성을 수행하도록 요청한다(⑤). 이때 PDF는 엑세스 네트워크의 자원을 관리하는 A-TRCF와 코어 네트워크의 자원을 관리하



·SCF : Service Control Fuction
·NAAF : Network Access Attachment Functions
·PDF : Policy Decision Function
·A-TRCF : Access Transport Resource Control Functional entity
·C-TRCF : Core Transport Resource Control Functional entity
·ANF : Access Node Functional entity
·ENF : Edge Node Functional entity
·A-BGF : Access Border Gateway Functional entity
·I-BGF : Interconnection Border Gateway Functional entity

(그림 10) BcN에서의 VPN QoS를 위한 프레임워크 모델

는 C-TRCF 간에 호스 모델을 적용하여 호스 인터페이스를 설립할 수도 있다. 이러한 경우, C-TRCF에서는 인터페이스, 버퍼 등에 필요한 자원을 할당할 수 있는 경로를 검색하고, QoS 보장이 가능한 명시적 경로를 따라서 라우터 인터페이스에 QoS 파라미터들을 설정하면 된다(⑥). C-TRCF는 [11]과 [12]에서 제안한 RSVP-TE 및 공평한 서비스 제공 메커니즘 등을 이용하여 자원예약을 수행할 수도 있다(⑦). 각 네트워크 개체는 자원 사용의 프로비전 상태정보를 유지하면서 네트워크 모니터링과 측정을 통하여 남아있는 자원 및 큐 사용률 등을 체크하고 이에 대한 VPN QoS 측정 결과를 상위 개체에게 보고한다(⑧).

V. 결 론

본 고에서는 VPN과 관련된 표준화 동향과 VPN QoS를 서비스하기 위한 서비스 구조 및 기술, BcN의 종단간 QoS 지원 프레임워크 내에서 VPN QoS 서비스를 제공하기 위한 모델 등에 대해서 알아보았다.

VPN에서의 호스 모델은 VPN 고객 및 서비스 제공자에게 높은 멀티플렉싱 이점을 가져다 줄 수 있는

모델이다. 이러한 호스 모델에 BcN에서의 백본 네트워크 기술인 MPLS 기술을 이용하여 호스 파라미터들을 VPN 차원으로 고려한 자원공유가 지원될 때 네트워크 사업자에게 멀티플렉싱 이점을 제공할 수 있게 된다.

이를 위해 VPN 상태 기반의 프로비저닝을 지원하는 효율적이고 동적인 자원예약 프로토콜이 제시되어야 하며, BcN 코어 네트워크의 게이트웨이 및 라우터들은 이를 구현할 수 있어야 할 것이다.

[참 고 문 헌]

[1] Paul Knight, Hamid Ould-Brahim, "Network based IP VPN Architecture using Virtual Routers", Internet Draft, April 2004

[2] Jeremy De Clercq, Olivier Paridaens, Andrew Krywaniuk, "An Architecture for Provider Provisioned CE-based Virtual Private Networks using IPsec", Internet Draft, February 2004

[3] K. Kompella, Y. Rekhter, "Virtual Private LAN Services", Internet Draft, April 2005

[4] Mustapha Aissaoui, Matthew Bocci, David Watkinson, Himanshu Shah, Paul Doolan, Peter Busschbach, Simon Delord, "OAM Procedures for VPWS Interworking", Internet Draft, October 2005

[5] Himanshu Shah, Eric Rosen, Francois Le Faucheur, Giles Heron, "IP-Only LAN Service (IPLS)", Internet Draft, October 2005

[6] Tomonori Takeda, "Framework and Requirements for Layer 1 Virtual Private Networks", Internet Draft, August 2005

[7] Tomonori Takeda, "Applicability analysis of GMPLS protocols to Layer 1 Virtual Private Networks", Internet Draft, September 2005

[8] 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

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

[10] R. Aggarwal, D. Papadimitriou, S. Yasukawa, "Extensions to RSVP-TE for Point to Multipoint TE LSPs", Internet Draft, July 2005

[11] 변해선, 이미정, "VPN Hose 모델을 지원하기 위한 자원 예약 방안", 한국컴퓨터종합학술대회, 제32권 제1호, pp. 328~339. 2005년 7월

[12] 변해선, 우현제, 김경민, 이미정, "VPN 서비스 품질 지원과 공정한 자원활용", 한국인터넷정보학회 추계 학술대회, 제6권 제2호, pp. 271~276. 2005년 11월

[13] IETF FGNGN WG3, "Requirements and framework for end to end QoS architecture in NGN", TR-e2eqos.1 FGNGN-OD-00204, August 2005

변해선

1997년 ~ 2001년 광주대학교 컴퓨터학과 학사
2001년 ~ 2003년 이화여자대학교 과학기술대학원 컴퓨터학과 석사
2003년 ~ 현재 이화여자대학교 과학기술대학원 컴퓨터학과 박사과정
관심분야 : 광대역통합망, 가상사설망, 무선 이동 네트워크, 인터넷에서의 QoS 지원

이미정

1983년 ~ 1987년 이화여자대학교 전자계산학 학사
1987년 ~ 1989년 University of North Carolina at Chapel Hill 컴퓨터학 석사
1990년 ~ 1994년 North Carolina State University 컴퓨터공학 박사
1994년 ~ 현재 이화여자대학교 공과대학 컴퓨터학과 교수
관심분야 : 고속 통신 프로토콜 설계 및 성능 분석, 멀티미디어 전송을 위한 트래픽 제어, 인터넷에서의 QoS 지원, 무선 이동 네트워크, ad-hoc 네트워크, 광대역통합망, 가상사설망