PATENT
P57716

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

KI-CHEOL LEE *et al.*

Serial No.:	*to be assigned*	Examiner:	*to be assigned*
Filed:	23 January 2006	Art Unit:	*to be assigned*

For: APPARATUS AND METHOD FOR PROVIDING MULTI PROTOCOL LABEL SWITCHING (MPLS)-BASED VIRTUAL PRIVATE NETWORK (VPN)

CLAIM OF PRIORITY UNDER 35 U.S.C. §119

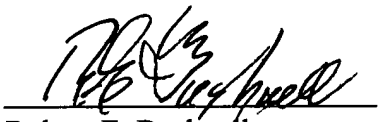
Mail Stop : Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The benefit of the filing date of the following prior foreign application, Korean Patent Application No. 10-2005-0006401 filed in Korea on 24 January 2005, filed in the U.S. Patent and Trademark Office on 23 January 2006 is hereby requested and the right of priority provided in 35 U.S.C. §119 is hereby claimed.

In support of this claim, filed herewith is certified copies of said original foreign applications.

Respectfully submitted,



Robert E. Bushnell
Reg. No.: 27,774
Attorney for the Applicant

1522 "K" Street, N.W., Suite 300
Washington, D.C. 20005
(202) 408-9040

Folio: P57716
Date: 1/23/06
I.D.: REB/fw

대한민국특허청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2005-0006401
Application Number

출 원 년 월 일 : 2005년 01월 24일
Date of Application JAN 24, 2005

출 원 인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.

2005 년 04 월 11 일

특 허 청
COMMISSIONER

CERTIFIED COPY OF
PRIORITY DOCUMENT

【서지사항】

【서류명】 특허출원서

【권리구분】 특허

【수신처】 특허청장

【제출일자】 2005.01.24

【발명의 국문명칭】 ＭＰＬＳ 기반의 ＶＰＮ 제공 장치 및 방법

【발명의 영문명칭】 APPARATUS AND METHOD FOR SERVING THE VIRTUAL PRIVATE NETWORK BASED MPLS

【출원인】

【명칭】 삼성전자 주식회사

【출원인코드】 1-1998-104271-3

【대리인】

【성명】 박상수

【대리인코드】 9-1998-000642-5

【포괄위임등록번호】 2000-054081-9

【발명자】

【성명의 국문표기】 이기철

【성명의 영문표기】 LEE,KI CHEOL

【주민등록번호】 721121-1392810

【우편번호】 463-714

【주소】 경기 성남시 분당구 구미동 무지개마을주공12단지아파트 1209동 1405 호

【국적】 KR

【발명자】

【성명의 국문표기】 남기성

【성명의 영문표기】 NAM,KEE SUNG

【주민등록번호】 620924-5100281

【우편번호】 135-272

【주소】 서울 강남구 도곡2동 467-17 타워팰리스 2차 F동 4001호

【국적】 KR

【심사청구】 청구

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인

박상수 (인)

【수수료】

【기본출원료】	0 면	38,000 원
【가산출원료】	32 면	0 원
【우선권주장료】	0 건	0 원
【심사청구료】	19 항	717,000 원
【합계】	755,000 원	

【요약서】

【요약】

본 발명은 MPLS(Multi Protocol Label Switching) 기술을 기반으로 하는 VPN(Virtual Private Network; 가상 사설 네트워크)에 관한 것으로, 중앙 집중 제어 방식을 통해 사용되는 프로토콜들을 간소화하고 발생하는 부하를 감소시키며, QoS(Quality of Service)의 보장을 용이하게 하는 MPLS 기반의 VPN 제공 장치 및 방법에 관한 것이다.

【대표도】

도 3

【색인어】

MPLS(Multi Protocol Label Switching), VPN(Virtual Private Network; 가상 사설 네트워크), 중앙 집중 제어, 라우팅 프로토콜, 시그널링 프로토콜

【명세서】

【발명의 명칭】

ＭＰＬＳ 기반의 ＶＰＮ 제공 장치 및 방법{APPARATUS AND METHOD FOR SERVING THE VIRTUAL PRIVATE NETWORK BASED MPLS}

【도면의 간단한 설명】

<1> 도 1은 BGP/MPLS(Border Gateway Protocol/Multi Protocol Label Switching) 기반 3계층 VPN 네트워크의 구성도.

<2> 도 2는 중앙 집중 제어 방식을 적용한, MPLS를 기반으로 하는 3계층 VPN 네트워크의 구성도.

<3> 도 3은 본 발명에 따른 VPN 제공 장치의 블록구성도.

<4> 도 4는 본 발명의 일실시예에 따른 도면으로, 중앙 집중 제어 방식을 적용한, MPLS를 기반으로 하는 3계층 VPN에서의 CE(Customer Edge)간 통신을 도시하는 도면.

<5> 도 5는 본 발명의 다른 실시예에 따른 도면으로, 중앙 집중 제어 방식을 적용한, MPLS를 기반으로 하는 3계층 VPN에서의 CE간 통신을 도시하는 도면.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<6> 본 발명은 MPLS(Multi Protocol Label Switching)를 기반으로 하는 가상 사설 네트워크(Virtual Private Network; VPN) 제공 장치 및 방법에 관한 것으로, 특히 네트워크 구성요소들간의 복잡한 프로토콜을 간소화할 수 있는 MPLS 기반 VPN 제공 장치 및 방법에 관한 것이다.

<7> 가상 사설 네트워크(이하 "VPN"이라 칭한다)는 저비용으로 광대역 전용 회선 서비스를 제공하기 위한 것으로, 인터넷과 같은 공중 네트워크에서 사설 링크를 만드는 것이다. 일반적으로 이것은 엔크립션(encryption)과 터널링(tunneling) 기술을 이용하여 공유 네트워크를 전용 사설 링크인 것처럼 만드는 아이디어이다. VPN은 ATM(Asynchronous Transfer Mode), 프레임 릴레이 네트워크 등에서 비교적 쉽게 구현될 수 있는데, 그것은 고객에게 전용 대역폭과 경로 제어를 제공하는 가상 회선을 구성할 수 있기 때문이다. VPN에서 트래픽은 송신자에 의해 엔크립트되고 가상 회로를 통해 보내진다.

<8> 한편, 이와 같은 VPN은 대역폭 보장, QoS(Quality of Service) 보장이 어렵다는 문제점이 있었으나 MPLS 기술을 도입함으로써 이러한 문제점을 해결하는 방법이 개발되고 있다. MPLS 기술을 사용한 VPN의 예로 2계층(Layer 2) VPN, 3계층 VPN 등이 있다. 이와 같은 MPLS 기술을 사용한 VPN을 첨부한 도면을 참조하여 설명하도록 한다.

<9> 도 1은 BGP/MPLS(Border Gateway Protocol/Multi Protocol Label Switching)

기반 3계층 VPN 네트워크의 구성도이다.

<10> BGP/MPLS 기반 3계층 VPN에서는 IP 라우팅 프로토콜을 이용하여 경로를 계산한 후, MES(MPLS Edge Switch)(또는 PE(Provider Edge) 라우터라고도 한다), MCS(MPLS Core Switch)(또는 P(Provider) 라우터라고도 한다)로 구성되는 코어 네트워크 사이에 CR-LDP(Constraint Routed Label Distribution Protocol 또는 Constraint-based Routing/Label Distribution Protocol), RSVP-TE(Resource Reservation Protocol-Traffic Engineering) 등의 MPLS 시그널링 프로토콜을 사용하여 터널 LSP(Label Switched Path)를 형성한다. 이후 각 MES는 VPN 환경설정(configuration)을 수행하는데, 도 1을 예로 들면, MES 1의 경우 if1-VPN Red, if2-VPN Blue로, MES 2의 경우 if3-VPN Red, if4-VPN Blue 형태로 VPN 환경설정을 수행할 수 있다. 그리고 각 MES는 IP 라우팅 프로토콜을 통해 하위 IP 프리픽스(prefix) 정보를 전달받고 MPLS 포워딩 테이블(forwarding table) 및 VRF(VPN Routing and Forwarding) 테이블을 생성한다. 도 1을 예로 들면, 각 MES는 VRF Red, VRF Blue를 생성한다. 이후 LSP의 이그리스(egress) MES는 MP-BGP(Multi-Protocol BGP)를 이용하여 인그리스(ingress) MES에 VPN 라우팅 정보 및 VC 레이블(label) 값을 전송한다. 이를 수신한 인그리스 MES는 수신한 VPN 라우팅 정보 및 VC 레이블 값을 이용하여 VRF 테이블을 완성한다. MES는 VRF 테이블을 완성한 후 CE(Customer Edge) 라우터들에 VPN 라우팅 정보를 전송한다. 이후 CE들은 MPLS 패킷을 생성하고 다른 CE와의 통신을 수행할 수 있다.

<11> 그런데, 도 1에 도시된 종래의 BGP/MPLS 기반 3계층 VPN은, 분산 제어 방식

을 사용하므로, VPN용 터널 LSP 생성을 위해 복잡한 IP 라우팅 프로토콜 및 MPLS 시그널링 프로토콜을 사용해야 한다. 또한 종래의 BGP/MPLS 기반 3계층 VPN은 VC(Virtual Connection; 가상 연결) 레이블 할당 및 VPN 라우팅 정보 전달을 위해 복잡한 MP-BGP 라우팅 프로토콜을 필요로 한다. 이에 따라 각 MES, MCS의 구현이 복잡해진다. 또한 MES, MCS들은 복잡한 프로토콜 스택(protocol stack)에 의해 MES, MCS가 트래픽을 전송하는 기능보다 트래픽 전송을 위한 사전 제어 기능에 더 많은 부하를 감당하게 된다. 또한 분산 제어 방식을 사용하므로, 종래의 BGP/MPLS 기반 3계층 VPN은 LSP QoS 보장이 어렵다는 문제점을 갖는다. 이러한 문제점들은 BGP/MPLS 기반 3계층 VPN만이 아닌 모든 MPLS를 기반으로 하는 VPN에서 발생할 수 있다.

<12> 그러므로, 전술한 문제점들을 해결할 수 있는 MPLS를 기반으로 하는 VPN 제공 장치 및 방법이 요구된다.

【발명이 이루고자 하는 기술적 과제】

<13> 따라서 본 발명의 목적은 MPLS(Multi Protocol Label Switching)를 사용한 VPN(Virtual Private Network)에서 터널 LSP(Label Switched Path) 생성을 위해 사용되는 복잡한 IP 라우팅 프로토콜 및 MPLS 시그널링 프로토콜을 간소화할 수 있는 MPLS를 기반으로 하는 VPN 제공 장치 및 방법을 제공함에 있다.

<14> 본 발명의 다른 목적은 MPLS를 기반으로 하는 VPN에서 VC(Virtual

Connection) 레이블 할당 및 VPN 라우팅 정보 전달을 위한 복잡한 라우팅 프로토콜을 간소화할 수 있는 MPLS를 기반으로 하는 VPN 제공 장치 및 방법을 제공함에 있다.

<15> 본 발명의 또 다른 목적은 MPLS를 기반으로 하는 VPN에서 발생하는 부하를 감소시킬 수 있는 MPLS를 기반으로 하는 VPN 제공 장치 방법을 제공함에 있다.

<16> 본 발명의 또 다른 목적은 LSP QoS 보장이 용이한 MPLS를 기반으로 하는 VPN 제공 장치 및 방법을 제공함에 있다.

<17> 이와 같은 목적들을 제공하기 위해 본 발명은; 적어도 하나의 MPLS(Multi Protocol Label Switching) 스위치를 포함하는 네트워크에서의 MPLS 기반의 VPN(Virtual Private Network) 제공 장치에 있어서, 상기 네트워크의 MPLS LSP 정보를 저장하는 LSP 관리부와, 운용자로부터 VPN 설정 요청 메시지를 수신하여 처리하는 연결 수락부와, 상기 MPLS 스위치 중의 MES(MPLS Edge Switch)로부터 상기 설정을 요청받은 VPN에 포함되는 CE(Customer Edge)의 IP 프리픽스 정보를 수집하여 VPN 토폴로지 테이블을 작성하는 토폴로지/리소스 수집부와, 상기 저장된 MPLS 네트워크의 LSP 정보 및 상기 작성된 VPN 토폴로지 테이블을 참조하여 상기 설정을 요청받은 VPN을 위한 VPN용 LSP를 생성하는 LSP 계산부를 포함함을 특징으로 하는 MPLS 기반의 VPN 제공 장치를 제공한다.

<18> 또 본 발명은; 적어도 하나의 MPLS 스위치를 포함하는 네트워크에서의 MPLS 기반의 VPN 제공 방법에 있어서, 운용자로부터 VPN 설정 요청 메시지를 수신하는

제 1 과정과, 상기 설정을 요청받은 VPN에 대한 VPN 식별자를 할당하여 상기 MPLS 스위치 중의 MES에 전송하는 제 2 과정과, 상기 MES로부터 상기 VPN에 포함되는 CE의 IP 프리픽스 정보를 수신하는 제 3 과정과, 상기 수신한 IP 프리픽스 정보를 사용하여 VPN 토폴로지 테이블을 작성하는 제 4 과정과, 상기 작성된 VPN 토폴로지 테이블 및 미리 설정된 상기 네트워크의 MPLS LSP 정보를 참조하여 상기 설정을 요청받은 VPN을 위한 VPN용 LSP를 생성하는 제 5 과정을 포함함을 특징으로 하는 MPLS 기반의 VPN 제공 방법을 제안한다.

【발명의 구성】

<19> 이하 본 발명의 바람직한 실시예들을 첨부된 도면의 참조와 함께 상세히 설명한다. 본 발명을 설명함에 있어서, 관련된 공지기능 혹은 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단된 경우 그 상세한 설명은 생략한다.

<20> 이하 기술하는 본 발명은 중앙 집중 제어 방식의 MPLS를 기반으로 하는 VPN 제공 장치 및 방법에 관한 것이다. 본 발명은 중앙 집중 제어 방식을 사용함으로써 터널 LSP(Label Switched Path) 생성을 위해 사용되는 복잡한 IP 라우팅 프로토콜 및 MPLS 시그널링 프로토콜, VC(Virtual Connection) 레이블 할당 및 VPN 라우팅 정보 전달을 위한 복잡한 라우팅 프로토콜 등을 간소화할 수 있고, 발생하는 부하를 감소시킬 수 있으며, LSP QoS 보장이 용이하게 된다.

<21> 한편, 하기에서 본 발명의 설명은 현재의 MPLS 기반 VPN에서 일반적으로 사용되고 있는 BGP/MPLS 기반 3계층 VPN을 예로 들어 이루어질 것이다.

<22> 먼저 첨부한 도면을 참조하여 본 발명이 적용된 중앙 집중 제어형의, MPLS를 기반으로 하는 VPN에 대해 설명하도록 한다.

<23> 도 2는 중앙 집중 제어 방식을 적용한, MPLS를 기반으로 하는 3계층 VPN 네트워크의 구성도이다.

<24> 도 2에 도시된 바와 같이, 본 발명에 따른 VPN 네트워크는 상기 네트워크를 중앙 집중 제어 방식으로 제어 및 관리하는 VPN 제공 장치(CCS; Centralized Control System)(200), 입력되는 IP 패킷 등의 데이터를 LSP로 매핑하거나 상위 MCS(MPLS Core Switch)로부터 전달된 MPLS 패킷을 자신에게 연결된 하위 CE(Customer Edge) 라우터에 전달하는 MES(MPLS Edge Switch), MPLS 패킷들을 스위칭하는 MCS를 포함하도록 구성될 수 있다. MES는 MPLS 네트워크의 에지에 위치하며 입력되는 데이터를 LSP로 매핑하고, MCS는 MES의 안쪽에 위치하며 전달된 MPLS 패킷들을 스위칭한다. MES 및 MCS를 "MPLS 스위치"라 통칭할 수 있다. 이하 MES 및 MCS를 특별히 구분할 필요가 없는 경우에는 MPLS 스위치라는 용어를 사용하도록 한다.

<25> 본 발명에서 MPLS 스위치들은 LSP 계산을 위한 토폴로지 정보 및 리소스 정보를 수집한다. 본 발명에서 MPLS 스위치들은 토폴로지 정보 및 리소스 정보에 대한 수집만을 수행할 뿐 LSP 계산을 수행할 필요가 없으므로, 기존의 MPLS 스위치들

에 비해 그 구조가 단순화될 수 있다. MPLS 스위치들은 인접하는 MPLS 스위치들과의 헬로 메시지 송수신을 통해 토폴로지 정보 및 리소스 정보를 수집할 수 있다. MPLS 스위치들의 토폴로지 정보 및 리소스 정보 수집에 대해서는 후에 상세히 설명하기로 한다. 본 발명과 같은 중앙 집중 제어형 MPLS 네트워크에서의 LSP 계산은, 각 MPLS 스위치들이 아닌, 중앙 집중 제어 장치(200)에서 이루어진다.

<26> 이하 중앙 집중 제어 장치(200)를 첨부한 도면을 참조하여 설명하도록 한다.

<27> 도 3은 본 발명에 따른 VPN 제공 장치의 블록구성도이다.

<28> 도 3의 VPN 제공 장치(200)는 MES, MCS와 연결되어 MPLS 기반 3계층 VPN을 생성 및 관리하는 기능을 수행한다. 이를 위해 VPN 제공 장치(200)는 MPLS 네트워크의 토폴로지 및 리소스 정보를 생성 및 관리하고 VPN 라우팅 정보를 생성 및 관리하는 토폴로지/리소스 수집부(Topology/Resource Discovery & Maintenance)(300), 운용자(operator)로부터 3계층 VPN 설정 요청을 수신하여 처리하는 연결 수락부(Connection Admission Control)(330), VPN 설정을 위한 정책을 관리하는 정책 관리부(Policy Management)(340), VPN용 LSP를 생성하는 LSP 계산부(LSP Computation)(302), 생성된 VPN용 LSP를 관리하는 LSP 관리부(LSP Management)(320), VPN 라우팅 정보 및 VPN용 LSP 정보를 각 MES, MCS로 전달하여 VPN을 활성화하는 LSP 활성화부(LSP Activation)(304), 생성된 LSP의 상태를 관리하는 LSP 감시부(Link/LSP Monitoring)(310)를 포함하도록 구성될 수 있다.

<29> 한편, VPN용 LSP의 생성 및 관리 등은 도 2에 도시된 MPLS 네트워크 상에 설

정되어 있는 MPLS LSP를 기반으로 이루어진다. 그러므로 VPN 제공을 위한 VPN용 LSP의 생성 및 관리에 대한 설명에 앞서 MPLS LSP의 생성 및 관리에 대해 설명하도록 한다.

<30> 토폴로지/리소스 수집부(300)는 본 발명에 따른 중앙 집중 제어형 MPLS 네트워크의 토폴로지(topology) 정보 및 리소스(resource) 정보를 수집한다. 토폴로지/리소스 수집부(300)는 토폴로지 정보 및 리소스 정보의 수집을 위해 각 MPLS 스위치들로부터 토폴로지 정보 및 리소스 정보들을 수신한다. 이때, MPLS 스위치들이 토폴로지/리소스 수집부(300)에 송신하는 토폴로지 정보는 인접하는 다른 MPLS 스위치들간의 연결 상태 정보이다. MPLS 스위치들은 인접하는 MPLS 스위치들과의 헬로 메시지 송수신을 통해 토폴로지 정보 및 리소스 정보를 확인할 수 있다. 헬로 메시지를 사용한 토포롤지 정보 및 리소스 정보 수집에 대해서는 그 구체적인 설명을 생략하도록 한다.

<31> 중앙 집중 제어 장치(200)는 토폴로지/리소스 테이블을 작성한 후, 토폴로지/리소스 테이블 및 네트워크 운용자(360)가 정의한 정책을 기반으로 LSP를 계산한다. LSP 계산은 중앙 집중 제어 장치(200) 내의 LSP 계산부(302)에서 수행된다. LSP 계산부(302)는 LSP 계산을 위해 CSPF(Constraint based Shortest Path First) 알고리듬을 사용할 수 있다.

<32> 한편, LSP 계산에는 정책 관리부(340)에 저장된 정책이 반영될 수도 있다. 이때, LSP 계산부(300)는 상기 정책을 만족시키도록 LSP를 계산한다.

<33> LSP 계산부(302)가 계산한 LSP는 LSP 활성화부(304)를 통해 각 MPLS 스위치에 설정된다. 모든 연결에 대한 LSP 계산을 끝낸 중앙 집중 제어 장치(200)는, 계산된 LSP 정보를 LSP 활성화부(304)에 송신한다. LSP 활성화부(304)는 각 MPLS 스위치에 설정된 LSP 정보를 송신하는 LSP 활성화 절차를 수행한다. LSP 활성화 절차에서 각 MPLS 스위치에 송신되는 정보는, FEC(Forward Equivalence Classes) 정보, 하위 인터페이스 토폴로지 정보, class to EXP 매핑 정보, LFIB(Label Forwarding Information Base) 정보 등이다.

<34> 여기서, FEC는 같은 정책에 의해 전송되는 패킷 그룹을 나타내고, 하위 인터페이스 정보는 CE 등의, MES를 통해 MPLS 네트워크에 연결되는 장치들의 정보를 나타내며, class to EXP 매핑 정보는 DiffServ DSCP(DiffServ Code Point)와 MPLS EXP 매핑 정보 또는 802.1p 클래스와 MPLS EXP 매핑 정보 등을 나타낸다. 그리고 LFIB는 각 MPLS 스위치가 처리해야 하는 MPLS 레이블 스위칭 정보로써 입력 레이블(input label), 출력 레이블(output label), 출력 인터페이스(output interface) 등의 정보를 포함할 수 있다.

<35> 한편, 중앙 집중 제어 장치(200)는 설정된 LSP들의 상태를 관리하는 LSP 관리부(320)를 더 포함할 수 있다. LSP 관리부(320)는 계산 및 설정된 LSP에 대한 정보를 저장하고 이후의 MPLS 네트워크의 운용을 관리한다. LSP 관리부(320)에 저장된 LSP 정보는 이후 설명할 MPLS 네트워크의 OAM(Operations, Administration & Maintenance)에서도 사용된다.

<36> MPLS 네트워크에서는 LSP의 성능 및 장애 정보를 검출하기 위해 MPLS OAM 기

능을 수행할 수 있다. MPLS OAM 기능에 의해 MPLS 네트워크는 LSP의 성능이 심하게 열화되거나 LSP에 장애가 발생하는 경우를 감지하고, 사용할 수 없게 된 LSP를 제거하고 새로운 LSP를 계산하거나, 사용할 수 없게 된 LSP 대신 대체 LSP로 절체하는 등의 복구 기능을 수행할 수 있다. MPLS OAM 기능 역시 중앙 집중 제어 장치(200)에 의해 수행될 수 있다.

<37> 중앙 집중 제어 장치(200)의 LSP 감시부(310)는 MPLS 네트워크의 링크 및 설정된 LSP의 성능 및 장애를 관리한다. MPLS 네트워크의 링크 및 LSP에 대한 관리 역시 헬로 메시지를 사용하여 이루어질 수 있다.

<38> 각 MPLS 스위치들은, MPLS 네트워크의 링크 및 LSP 관리를 위해, 최초 네트워크 구동 시의 토폴로지/리소스 확인 후에도, 헬로 메시지를, 통해 지속적으로 토폴로지/리소스 확인을 수행한다. 토폴로지 또는 리소스에 변화가 발생하는 경우, MPLS 스위치는 상기 변화된 사항을 중앙 집중 제어 장치(200)에게 통보함으로써 중앙 집중 제어 장치(200)가 토폴로지/리소스 테이블을 갱신할 수 있도록 한다.

<39> 헬로 메시지를 사용한 링크 감시의 예를 들면, MPLS 스위치는 Hello Dead Interval 내에 헬로 메시지가 도달하지 않으면 해당 링크에 장애가 발생했다고 판단하고 중앙 집중 제어 장치(200)에 장애 발생을 알리는 신호를 송신한다. 이 장애 발생 신호는 중앙 집중 제어 장치(200)의 LSP 감시부(310)에 송신된다. 장애 발생 신호는 장애가 발생한 링크에 대한 정보를 적어도 포함하도록 구성될 수 있다.

<40> 장애 발생 신호를 수신한 LSP 감시부(310)는, 장애가 발생한 링크에 대한 정보를 토폴로지/리소스 수집부(300)에 송신하고, 토폴로지/리소스 수집부(300)는 수신한 정보를 사용하여 토폴로지/리소스 테이블을 갱신한다. 또한 LSP 감시부(310)는 LSP 계산부(302)에 링크 장애를 통보하여 LSP 계산부(302)가 장애가 발생한 링크 내의 LSP에 대한 protection/restoration 기능을 수행하도록 한다.

<41> 또, 본 발명의 중앙 집중 제어 장치(200)는 외부로부터의 연결 요청을 수락 또는 거부하는 연결 수락부(330)를 더 포함할 수 있다. 연결 수락부(330)는 외부 운용자(360)또는 외부의 콜 서버(call server)(230)와 연결된다. 외부 서비스는 MES를 통해 MPLS 네트워크에 연결되지만, 상기 서비스에 대한 수락 여부는 중앙 집중 제어 장치(200)의 연결 수락부(330)에 의해 판단된다.

<42> 연결 수락부(330)는, 운용자(360) 또는 콜 서버(예를 들면 소프트스위치)(230) 등 외부로부터의 서비스 연결 요청을 받으면, LSP 관리부(320)를 참조하여 상기 요청된 서비스를 위해 사용 가능한 LSP와 대역폭이 존재하는지를 판단한다. 연결 수락부(330)는 설정된 LSP 중 가용한 LSP와 대역폭이 존재하면 MES로 입력되는 서비스 데이터가 해당 LSP에 매핑될 수 있도록 제어한다. 그러나 만일 가용한 LSP 또는 대역폭이 존재하지 않으면, 연결 수락부(330)는 LSP 계산부(302)에 신규 LSP의 설정을 요청하고, LSP 계산부(302)는 이에 따라 해당 서비스를 수용할 수 있는 신규 LSP를 계산한다. 한편, 요청받은 서비스를 지원할 수 있는 LSP가 존재하지 않으며 신규 LSP의 설정도 불가능하다면, LSP 계산부(302)는 해당 서비스를 요청한 상대에게 상기 서비스가 불가능함을 알린다.

<43> 또, 본 발명의 중앙 집중 제어 장치(200)는 LSP 설정 및 관리 정책을 담당하는 정책 관리부(340)를 더 포함할 수 있다. 정책 관리부(340)는 운용자(360)로부터 MPLS 네트워크에서의 LSP 설정 및 관리 정책을 수신 받고 상기 정책이 LSP 계산부(302) 또는 연결 수락부(330)의 동작에 반영될 수 있도록 한다.

<44> 이상 MPLS LSP의 생성 및 관리에 대해 설명하였다. 이와 같은 중앙 집중 제어형 MPLS 네트워크 및 중앙 집중 MPLS 네트워크에서의 MPLS LSP 설정에 대해서는 기출원된 국내출원번호 10-2004-0109024, "MPLS 네트워크의 중앙 집중 제어 장치 및 방법"에 상세히 기술되어 있다. 하기에서는 이와 같이 생성된 MPLS LSP 정보를 기반으로 하는 VPN용 LSP의 생성 및 관리를 도 2 및 도 3을 참조하여 설명하도록 한다.

<45> 3계층 VPN의 제공을 요청하는 사용자(도시하지 않음)는 VPN 설정 요청 메시지를 운용자에게 전송하고, 운용자는 이를 기반으로 VPN 설정 정보를 포함하는 설정 요청 메시지를 VPN 제공 장치(200)의 연결 수락부(330)에 전송한다. 이때 상기 VPN 설정 요청 메시지에 포함되는 VPN 설정 요청 정보는 VPN 설정 사이트(sites), VPN 설정 LSP 등급(class), LSP 대역폭, 성능 조건 등을 포함할 수 있다. VPN 설정 요청 메시지를 수신한 VPN 제공 장치(200)는 요청된 3계층 VPN에 대해 각각 VPN ID를 부여하고 부여한 VPN ID를 각 MES에 전송한다. 도 2에서는 운용자로부터 VPN 제공 장치(200)에 두개의 3계층 VPN 요청 메시지가 수신되었고 이에 따라 VPN 제공 장치(200)는 요청된 각 VPN에 대해 VPN 1(VPN ID=1000)과 VPN 2(VPN ID=2000)로 ID를 설정하여 MES에 VPN 환경설정 정보(configuration information)를 전송한다.

한편, 연결 수락부(330)는, 운용자로부터 VPN 설정 요청 메시지를 수신하면, LSP 관리부(320)를 참조하여 MPLS 네트워크에 상기 설정 요청된 VPN을 제공할 수 있을 정도의 자원이 존재하는지를 확인할 수 있을 것이다. 즉, 본 발명은 중앙 집중 제어 방식을 통해 QoS 보장 등을 용이하게 수행할 수 있게 된다.

<46> MES는 VPN 제공 장치(200)로부터 VPN 환경설정 정보를 수신하면, 다음의 표 1과 같이 해당 인터페이스별로 VPN을 설정한다. 하기의 표 1은 도 2의 MES 1 및 MES 2에 설정된 3계층 VPN 환경 정보의 일 예이다.

【표 1】

<47>

MES 1	VPN 1000	if1
	VPN 2000	if2
MES 2	VPN 1000	if3
	VPN 2000	if4

<48> 이와 같이 3계층 VPN을 설정할 경우, MES 1은 if1을 통해 입력되는 패킷들을 VPN 1000에 해당하는 패킷이라고 판단하고, if2를 통해 입력되는 패킷들을 VPN 2000에 해당하는 패킷이라고 판단한다. 또 MES 2는 if3를 통해 입력되는 패킷들을 VPN 1000에 해당하는 패킷이라고 판단하고, if4를 통해 입력되는 패킷들을 VPN 2000에 해당하는 패킷이라고 판단한다.

<49> 이후 각 MES는 IP 라우팅 프로토콜을 통해 CE들로부터 VPN에 속해있는 IP 프리픽스 정보들을 수집한다. 도 2를 예로 들면, MES 1은 CE1로부터 VPN 1000에 해당하는 175.212.0.0/16의 IP 프리픽스 정보를 수집하고, CE4로부터 VPN 2000에 속하는 131.213.0.0/16의 IP 프리픽스 정보를 수집한다. 그리고 MES 2는 CE2로부터

VPN 1000에 속하는 121.32.0.0/16의 IP 프리픽스 정보를 수집하고, CE3로부터 VPN 2000에 속하는 154.21.0.0/16의 IP 프리픽스 정보를 수집한다. 각 MES는 수집한 VPN에 해당되는 IP 프리픽스 정보를 VPN 제공 장치(200)의 토폴로지/리소스 수집부(300)에 전송한다. VPN 제공 장치(200)의 토폴로지/리소스 수집부(300)는 각 MES로부터 수신한 VPN IP 프리픽스 정보를 기반으로 하기의 표 2와 같은 VPN 토폴로지 테이블을 작성한다. 각 MES는 VPN에 속한 IP 프리픽스 정보가 변경될 때마다 변경된 정보를 VPN 제공 장치(200)에 통보하고, VPN 제공 장치(200)는 각 MES로부터 수신한 변경 정보를 기반으로 VPN 토폴로지 테이블을 수정하여 갱신한다. 하기의 표 2는 VPN 제공 장치(200)가 작성한 VPN 토폴로지 테이블의 일 예이다. 전술한 바와 같이, 본 발명에서는 MES가 CE로부터 IP 프리픽스를 수집하는 경우에만 라우팅 프로토콜이 사용되므로, 사용되는 프로토콜이 간소화된다.

【표 2】

<50>

MES ID	CE ID	VPN ID	IP Subnet
MES 1	CE 1	VPN 1000	175.212.0.0/16
	CE 4	VPN 2000	131.213.0.0/16
MES 2	CE 2	VPN 2000	121.32.0.0/16
	CE 3	VPN 2000	154.21.0.0/16

<51> 한편, 토폴로지/리소스 수집부(300)는 VPN 토폴로지 테이블을 작성한 후, 연결 요청이 이루어진 사이트(site)간에 LSP를 생성하기 위해, LSP 계산부(302)에 VPN 1000, VPN 2000을 위한 LSP 설정을 요청한다. 이때, LSP 계산부(302)는 LSP 관리부(320)에 저장된, MPLS 네트워크의 LSP 정보를 기반으로 하여 VPN용 LSP를 설정한다. LSP 계산부(302)는 연결 요청된 VPN에 대한 VC, 터널 LSP를 생성한 후

LSP 테이블을 작성한다. 이때 터널 LSP를 미리 설정해 두고 VC LSP를 나중에 생성하여 터널 LSP에 VC LSP를 매핑할 수도 있다. 한편, LSP 계산부(302)는 LSP 생성시에 정책 관리부(340)에 저장된 정책을 참조할 수 있다.

<52> 하기의 표 3 및 표 4는 각각 LSP 계산부(302)가 계산 및 작성한 VPN 1000, VPN 2000에 대한 LSP 테이블의 예들이다. 표 3은 VPN 제공 장치(200)가 VPN 1000을 위해 설정한 LSP 테이블의 예이고, 표 4는 VPN 제공 장치(200)가 VPN 2000을 위해 설정한 LSP 테이블의 예이다. 물론 LSP 테이블은 이들 예들 외에도 다양하게 작성될 수 있다. 예를 들어, 표 3 및 표 4에는 인입 인터페이스(incoming interface)가 생략되어 있으나 레이블 할당 방식에 따라 인입 인터페이스가 추가될 수도 있다. 표 3 및 표 4에서 각 VC 레이블, 터널 레이블 값들은 발명의 이해를 돕기 위해 임의로 설정한 값들이다. 레이블 값은 LSP 계산부(302)가 할당하며, 설정된 3계층 VPN용 LSP 정보는 LSP 관리부(320)에 전송되어 관리된다.

【표 3】

<53>

VPN ID	Destination CE ID	Node ID	Incoming Tunnel Label	Incoming VC Label	Outgoing Interface	Outgoing Tunnel Label	Outgoing VC Label
1000	CE 2	MES 1	-	-	a1	100	25
		MCS 1	100	25	f1	200	25
		MCS 2	200	25	h1	pop	25
		MES 2	-	25	if3	-	-
	CE 1	MES 2	-	-	i2	300	35
		MCS 4	300	35	d2	400	35
		MCS 3	400	35	b2	pop	35
		MES 1	-	35	if1	-	-

【표 4】

<54>

VPN ID	Destination CE ID	Node ID	Incoming Tunnel Label	Incoming VC Label	Outgoing Interface	Outgoing Tunnel Label	Outgoing VC Label
2000	CE 3	MES 1	-	-	a1	100	45
		MCS 1	100	45	f1	200	45
		MCS 2	200	45	h1	pop	45
		MES 2	-	45	if4	-	-
	CE 4	MES 2	-	-	i2	300	55
		MCS 4	300	55	d2	400	55
		MCS 3	400	55	b2	pop	55
		MES 1	-	55	if2	-	-

<55> LSP 계산부(302)는 설정한 LSP 정보 등을 LSP 활성화부(304)에 전송하고, LSP 활성화부(304)는 LSP 정보, VPN 토폴로지 정보, EXP 필드 매핑(field mapping) 정보 등의 LSP 활성화 정보를 각 MPLS 스위치들에 전송한다. VPN 제공 장치(200)로부터 LSP 활성화 정보를 수신한 각 MPLS 스위치는 LSP를 활성화함으로써 도 2에서와 같이 VPN 1000용 LSP와 VPN 2000용 LSP를 동작시킬 수 있다. 또한 VPN 제공 장치(200)로부터 LSP 관련 정보를 수신한 MES들은, 수신 정보를 기반으로 VRF 테이블을 작성하고, 작성한 VRF 테이블을 사용하여 입력되는 IP 패킷을 대응하는 LSP에 매핑한다. 표 5는 도 2의 경우 VPN 제공 장치(200)가 MES들에 전송하는 VPN 토폴로지 정보의 일 예이다. 이 정보를 기반으로 MES는 입력되는 IP 패킷을 LSP로 매핑할 수 있다.

<56> 표 6은 VPN 제공 장치(200)가 MES들에 전송하는 EXP 필드 매핑 정보이다. 표 6은 MES에 입력되는 IP 패킷이 DiffServ 기반일 경우를 예로 들고 있으나 802.1p 기반의 EXP 필드 매핑, 5-tuple(Source IP address, Destination IP

address, Protocol ID, Source Port, Destination Port)을 이용한 IP 플로우(flow) 기반의 EXP 필드 매핑도 가능하다. 그리고 EXP 필드 매핑과 함께 등급 매핑(class mapping)도 가능한데, 이 경우는 여러 등급의 LSP를 설정한 후 EXP 필드에 따라 해당 등급의 LSP로 매핑하는 데 사용할 수 있다. 표 6의 EXP 필드 매핑은 예를 들어 설명한 것이며 운용자에 따라 다양한 매핑 테이블을 작성하고, VPN 제공 장치(200)에서 각 노드(node)들에 전송할 수 있다.

【표 5】

<57>

VPN ID	CE ID	CE 1	CE 2
1000	IP Subnet	175.212.0.0/16	121.32.0.0/16
	연결된 MES ID	MES 1	MES 2
VPN ID	CE ID	CE 4	CE 3
2000	IP Subnet	131.213.0.0/16	153.21.0.0/16
	연결된 MES ID	MES 1	MES 2

【표 6】

<58>

DSCP	EXP	Class ID
EF	EXP0	Gold
AF11	EXP1	Silver
AF12	EXP2	Silver
AF21	EXP3	Silver
AF22	EXP4	Silver
AF31	EXP5	Silver
AF32	EXP6	Silver
BE	EXP7	Bronze

<59> 표 7, 표 8은 각각 VPN 제공 장치(200)가 MES 1과 MES에 전송하는 LFIB(Label Forwarding Information Base) 테이블의 예들이다. 표 7은 VPN 제공 장치(200)가 MES 1에 전송하는 VPN 1000, VPN 2000용 LFIB 테이블의 예이고, 표 8은 VPN 제공 장치(200)가 MES 2에 전송하는 VPN 1000, VPN 2000용 LFIB 테이블의

예이다. 각 MES는 이 테이블을 기반으로 VRF 테이블을 생성하며, MPLS 패킷을 생성하여 전송할 수 있다. LFIB 테이블 역시 예를 위해 도시한 것이며 운용자에 따라 다양하게 정의 및 형성되어 사용할 수 있다.

【표 7】

<60>

VPN ID	Destination CE ID	Incoming Interface	Incoming VC Label	Outgoing Interface	Outgoing VC Label	Outgoing Tunnel Label
1000	CE2	if1	-	a1	25	100
	CE1	b1	35	if1	-	-
2000	CE3	if2	-	a1	45	100
	CE4	b1	55	if2	-	-

【표 8】

<61>

VPN ID	Destination CE ID	Incoming Interface	Incoming VC Label	Outgoing Interface	Outgoing VC Label	Outgoing Tunnel Label
1000	CE1	if3	-	i2	35	300
	CE2	h2	25	if3	-	-
2000	CE4	if4	-	i2	55	300
	CE4	h2	45	if4	-	-

<62> 전술한 바와 같이, 각 MES, MCS들은 VPN 제공 장치(200)로부터 VPN 1000, VPN 2000에 대한 LSP 활성화 정보들을 수신하면, 설정한 L3 VPN용 LSP들을 활성화하여 VPN IP 패킷들의 송수신을 수행한다. 이를 도 4를 참조하여 설명하면 다음과 같다.

<63> 도 4는 본 발명의 일실시예에 따른 도면으로, 중앙 집중 제어 방식을 적용한, MPLS를 기반으로 하는 3계층 VPN에서의 CE간 통신을 도시하는 도면이다.

<64> MES 1은 CE1으로부터 121.32.75.37의 목적지 IP 주소를 갖는 IP 패킷을 수신하면, 상기 IP 패킷이 입력된 인터페이스를 확인하여 해당 IP 패킷이 VPN 1000에

포함되었다는 것을 확인한다. 이후 MES 1은 VPN 제공 장치(200)로부터 수신한, 표 5의 VPN 토폴로지 테이블을 참조하여 상기 IP 패킷의 목적지가 되는 호스트가 MES 2와 연결된 CE2를 통해 도달될 수 있다는 것을 확인한다. 그리고 MES 1은 표 7의 LFIB 테이블을 참조하여 MPLS 패킷을 생성한 후 MCS 1에 전송한다. 이때 도 4에 도시된 MPLS 패킷은 터널 레이블, VC 레이블, IP 목적지 주소(destination address), 페이로드(payload)만을 나타내었다. 그러나, MES1은 MPLS 패킷 생성시 LFIB 테이블 이외에 IP 패킷 내의 DSCP(DiffServ Code Point) 값을 참조하여 표 6에 나타낸 EXP 필드 매핑을 수행할 수 있다. MES1으로부터 MPLS 패킷을 수신한 MCS 1은 터널 레이블 100을 200으로 레이블 매핑한 후 MCS 2에 전송한다. MCS 2는 MCS1으로부터 MPLS 패킷을 수신하고 수신한 MPLS 패킷의 터널 레이블을 팝(pop)한 후 MES 2에 MPLS 패킷을 전송한다. MES 2는 수신한 MPLS 패킷의 VC 레이블 값을 통해 해당 MPLS 패킷이 VPN 1000에 해당한다는 것을 확인한 후 표 8의 LFIB 테이블을 참조하여 VC 레이블을 팝한 후 CE2에 IP 패킷을 전송한다. IP 패킷을 수신한 CE2는 IP 포워딩 과정을 통해 IP 패킷을 해당 호스트에 전송한다. VPN 2000의 경우에 대해서도 전술한 과정들과 동일한 과정들을 통해 IP 패킷을 송수신할 수 있다. 반대 방향에 대한 패킷 전송의 동작도 전술한 바와 동일하며 이는 도 5에 나타내었다.

<65> 도 5는 본 발명의 다른 실시예에 따른 도면으로, 중앙 집중 제어 방식을 적용한, MPLS 기반의 3계층 VPN에서의 CE간 통신을 도시하는 도면이다. 도 5는 도 4에 대한 설명을 참조하여 이해될 수 있으므로, 도 5에 대한 상세한 설명은 생략하

도록 한다.

【발명의 효과】

<66> 본 발명은 MPLS 기반의 VPN 제공에 관한 것으로, 중앙 집중 제어 방식으로 LSP를 생성 및 관리함으로써 라우팅 프로토콜 및 시그널링 프로토콜의 사용 없이 MPLS 기반 VPN 서비스를 용이하게 제공할 수 있다. 또한 복잡한 프로토콜 스택을 사용하지 않음으로써 MPLS 스위치의 구성을 간단하게 하며 구현을 용이하게 할 수 있다. 마지막으로 중앙 집중 제어 방식으로 VPN용 LSP를 생성, 관리함으로써 VPN의 QoS 보장 및 VPN 서비스의 관리를 용이하게 할 수 있다.

【특허청구범위】

【청구항 1】

적어도 하나의 MPLS(Multi Protocol Label Switching) 스위치를 포함하는 네트워크에서의 MPLS 기반의 VPN(Virtual Private Network) 제공 장치에 있어서,

상기 네트워크의 MPLS LSP 정보를 저장하는 LSP 관리부와,

운용자로부터 VPN 설정 요청 메시지를 수신하여 처리하는 연결 수락부와,

상기 MPLS 스위치 중의 MES(MPLS Edge Switch)로부터 상기 설정을 요청받은 VPN에 포함되는 CE(Customer Edge)의 IP 프리픽스 정보를 수집하여 VPN 토폴로지 테이블을 작성하는 토폴로지/리소스 수집부와,

상기 저장된 MPLS 네트워크의 LSP 정보 및 상기 작성된 VPN 토폴로지 테이블을 참조하여 상기 설정을 요청받은 VPN을 위한 VPN용 LSP를 생성하는 LSP 계산부를 포함하는 MPLS 기반의 VPN 제공 장치.

【청구항 2】

제 1항에 있어서, 상기 연결 수락부가 수신하는 VPN 설정 요청 메시지는 VPN 설정을 위한 VPN 설정 요청 정보를 포함하는 MPLS 기반의 VPN 제공 장치.

【청구항 3】

제 2항에 있어서, 상기 VPN 설정 요청 정보는 VPN 설정 사이트, VPN 설정

LSP 등급, LSP 대역폭, 성능 조건들 중 적어도 하나 이상의 항목을 포함하는 MPLS 기반의 VPN 제공 장치.

【청구항 4】

제 1항에 있어서, 상기 연결 수락부는 상기 VPN 설정 요청 메시지를 수신하면, 상기 설정을 요청받은 VPN에 대해 VPN 식별자를 할당하여 상기 MES에 전송하는 MPLS 기반의 VPN 제공 장치.

【청구항 5】

제 4항에 있어서, 상기 연결 수락부는 상기 VPN 식별자 및 상기 VPN에 대한 설정 정보를 포함하는 VPN 환경설정 정보를 상기 MES에 전송하는 MPLS 기반의 VPN 제공 장치.

【청구항 6】

제 1항에 있어서, 상기 토폴로지/리소스 수집부가 상기 MES로부터 수집하는 IP 프리픽스 정보는 상기 MES가 IP 라우팅 프로토콜을 사용하여 수집한 정보인 MPLS 기반의 VPN 제공 장치.

【청구항 7】

제 1항에 있어서, 상기 네트워크의 운용 정책을 저장하는 정책 저장부를 더 포함하는 MPLS 기반의 VPN 제공 장치.

【청구항 8】

제 7항에 있어서, 상기 LSP 계산부는 상기 LSP 관리부에 저장된 MPLS LSP 정보, 상기 작성된 VPN 토폴로지, 상기 정책 관리부에 저장된 정책, VPN 설정 요청 메시지에 포함된 정보를 참조하여 상기 VPN용 LSP를 생성하는 MPLS 기반의 VPN 제공 장치.

【청구항 9】

제 1항에 있어서, 상기 LSP 계산부가 생성한 VPN용 LSP 정보를 상기 MPLS 스위치에 전송하는 LSP 활성화부를 더 포함하는 MPLS 기반의 VPN 제공 장치.

【청구항 10】

제 9항에 있어서, 상기 LSP 활성화부는 상기 MES에 VPN 토폴로지 정보, EXP 필드 매핑 정보, LFIB(Label Forwarding Information Base) 정보를 전송하고, 상기 MPLS 스위치 중 MCS에 LFIB 정보를 전송하는 MPLS 기반의 VPN 제공 장치.

【청구항 11】

제 1항에 있어서, 상기 연결 수락부는 상기 설정을 요청받은 VPN을 제공할 수 있는 양의 자원이 상기 네트워크에 존재하는지를 판단하고 그 판단 결과에 따라 상기 VPN의에 대한 수락 여부를 결정하는 MPLS 기반의 VPN 제공 장치.

【청구항 12】

제 11항에 있어서, 상기 LSP 관리부는, 상기 연결 수락부가 상기 자원의 유무를 판단하기 위해 참조하는 상기 네트워크의 설정 정보 및 자원 정보를 저장하는 MPLS 기반의 VPN 제공 장치.

【청구항 13】

제 1항에 있어서, 상기 LSP 관리부는 상기 생성된 VPN용 LSP 정보를 저장하는 MPLS 기반의 VPN 제공 장치.

【청구항 14】

적어도 하나의 MPLS 스위치를 포함하는 네트워크에서의 MPLS 기반의 VPN 제공 방법에 있어서,

운용자로부터 VPN 설정 요청 메시지를 수신하는 제 1 과정과,

상기 설정을 요청받은 VPN에 대한 VPN 식별자를 할당하여 상기 MPLS 스위치

중의 MES에 전송하는 제 2 과정과,

상기 MES로부터 상기 VPN에 포함되는 CE의 IP 프리픽스 정보를 수신하는 제 3 과정과,

상기 수신한 IP 프리픽스 정보를 사용하여 VPN 토폴로지 테이블을 작성하는 제 4 과정과,

상기 작성된 VPN 토폴로지 테이블 및 미리 설정된 상기 네트워크의 MPLS LSP 정보를 참조하여 상기 설정을 요청받은 VPN을 위한 VPN용 LSP를 생성하는 제 5 과정을 포함하는 MPLS 기반의 VPN 제공 방법.

【청구항 15】

제 14항에 있어서, 상기 제 5과정에서 생성된 LSP 정보를 상기 MPLS 스위치에 전송하는 제 6 과정을 더 포함하는 MPLS 기반의 VPN 제공 방법.

【청구항 16】

제 14항에 있어서, 상기 연결 수락부가 수신하는 VPN 설정 요청 메시지는 VPN 설정을 위한 VPN 설정 요청 정보를 포함하는 MPLS 기반의 VPN 제공 방법.

【청구항 17】

제 16항에 있어서, 상기 VPN 설정 요청 정보는 VPN 설정 사이트, VPN 설정

LSP 등급, LSP 대역폭, 성능 조건들 중 적어도 하나 이상의 항목을 포함하는 MPLS 기반의 VPN 제공 방법.

【청구항 18】

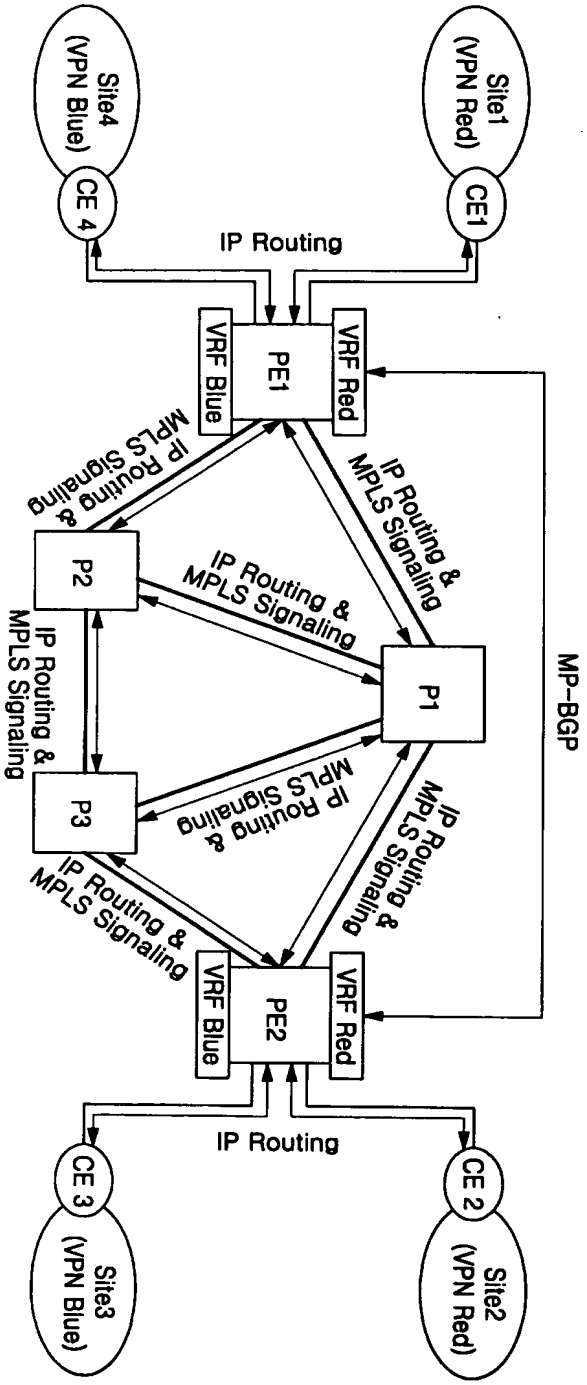
제 14항에 있어서, 상기 제 3 과정에서 상기 MES로부터 수신하는 IP 프리픽스 정보는 상기 MES가 IP 라우팅 프로토콜을 사용하여 수집한 정보인 MPLS 기반의 VPN 제공 방법.

【청구항 19】

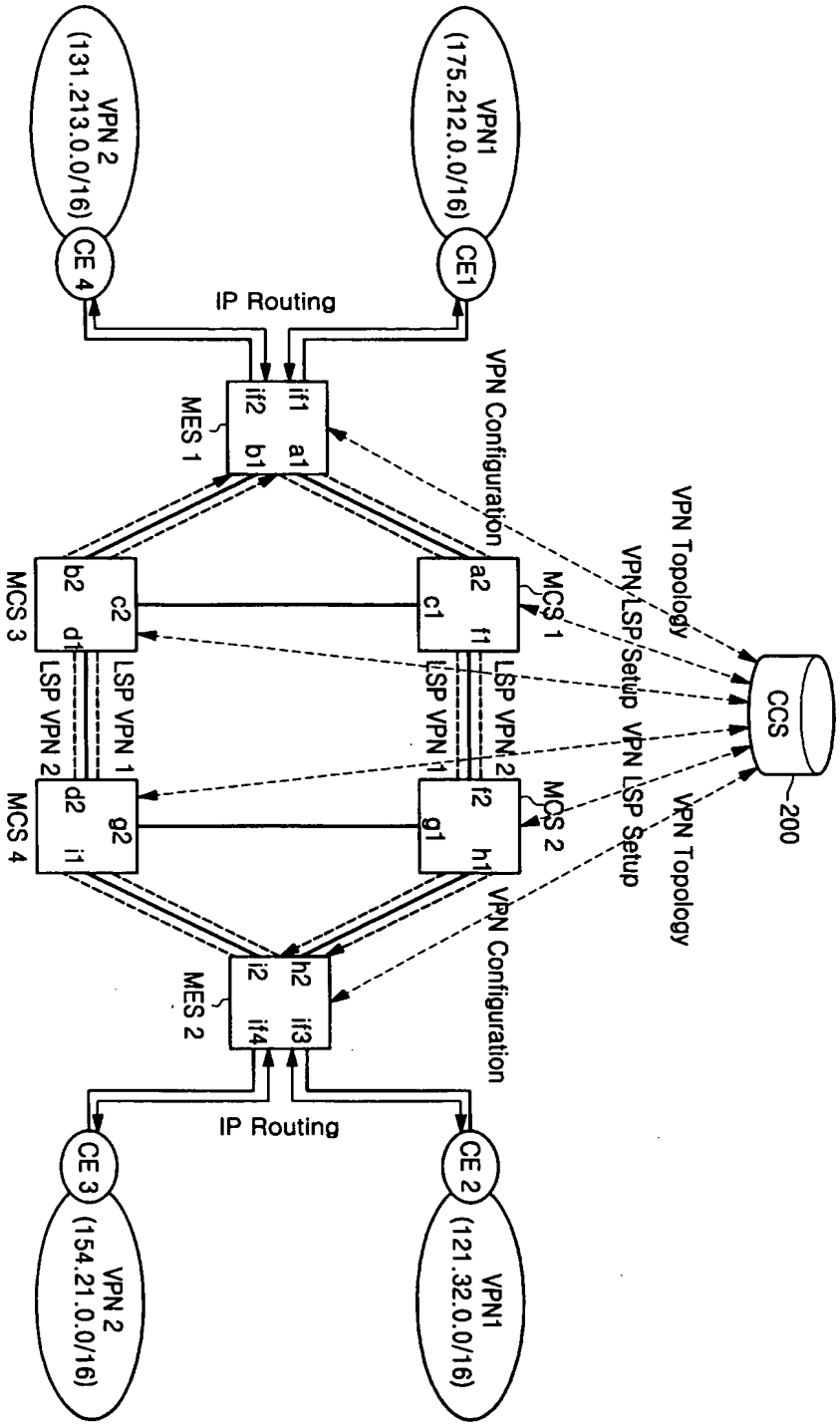
제 14항에 있어서, 상기 제 5 과정의 VPN용 LSP 생성은 상기 작성된 VPN 토폴로지, 상기 정책 관리부에 저장된 정책, VPN 설정 요청 메시지에 포함된 정보를 참조하여 수행되는 MPLS 기반의 VPN 제공 방법.

【도면】

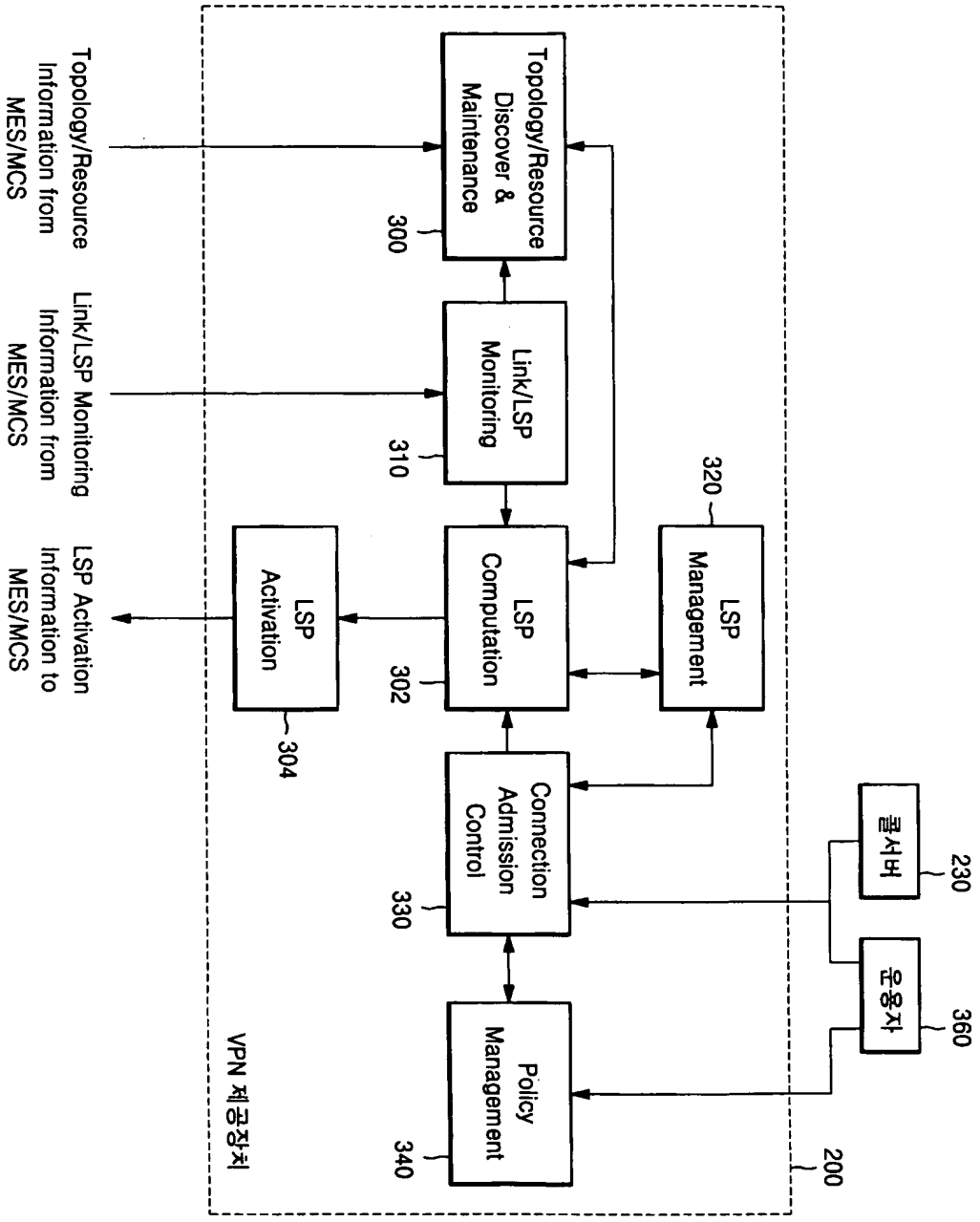
【도 1】


Site4
(VPN Blue)
CE 4
Site1
(VPN Red)
CE1
IP Routing
VRF Blue
PE1
VRF Red
IP Routing &
MPLS Signaling
IP Routing &
MPLS Signaling
P2
IP Routing &
MPLS Signaling
P1
IP Routing &
MPLS Signaling
P3
IP Routing &
MPLS Signaling
IP Routing &
MPLS Signaling
VRF Blue
PE2
VRF Red
MP-BGP
IP Routing
CE 3
Site3
(VPN Blue)
CE 2
Site2
(VPN Red)

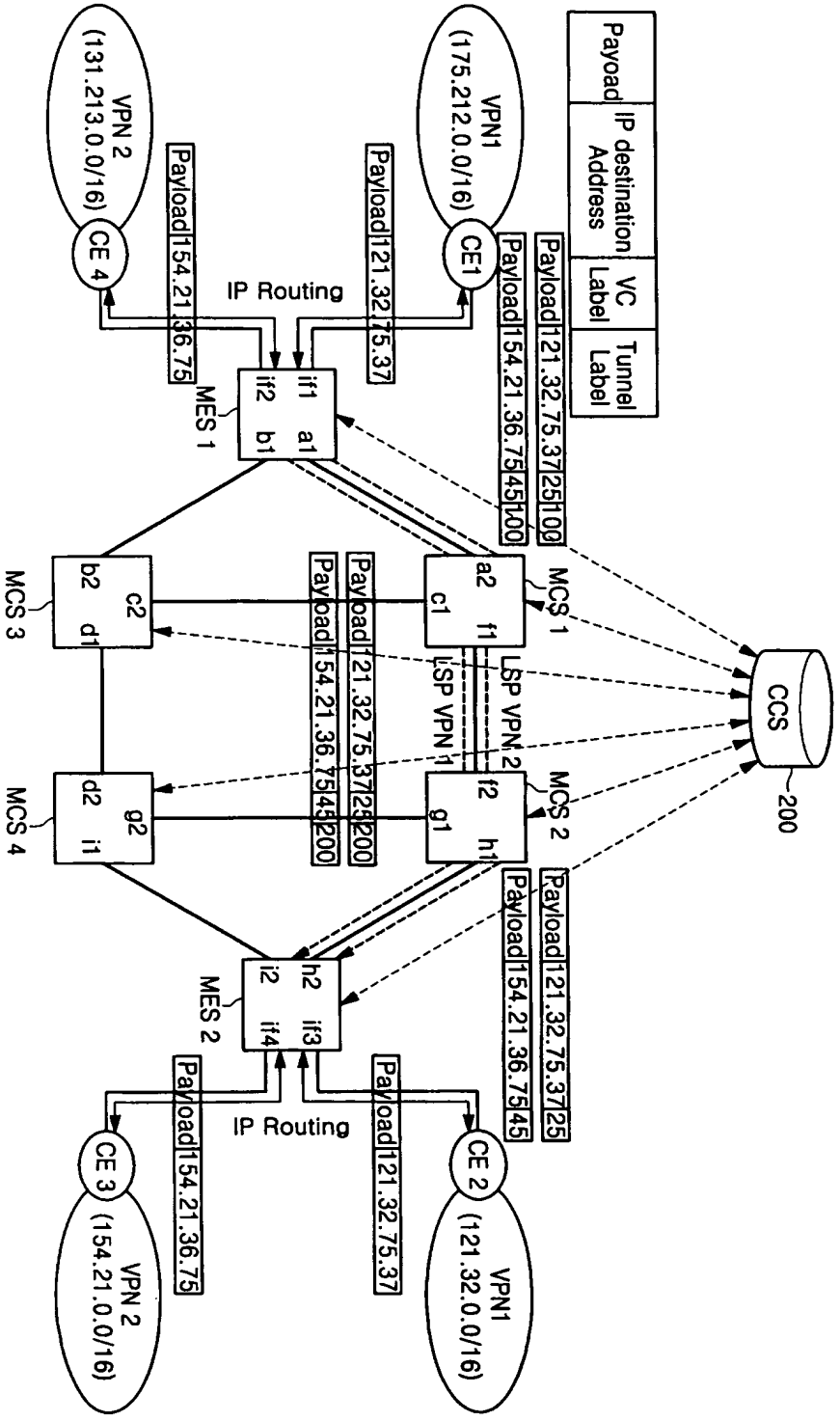
【도 2】


VPN 2
(131.213.0.0/16)
CE 4
VPN1
(175.212.0.0/16)
CE1
IP Routing
MES 1
if2
if1
b1
a1
VPN Configuration
VPN Topology
VPN LSP Setup
CCS
200
MCS 3
b2
c2
MCS 1
a2
c1
f1
d1
LSP VPN 2
LSP VPN 1
LSP VPN 2
LSP VPN 1
MCS 4
d2
g2
MCS 2
f2
g1
h1
i1
MES 2
i2
h2
if4
if3
IP Routing
CE 3
VPN 2
(154.21.0.0/16)
CE 2
VPN1
(121.32.0.0/16)

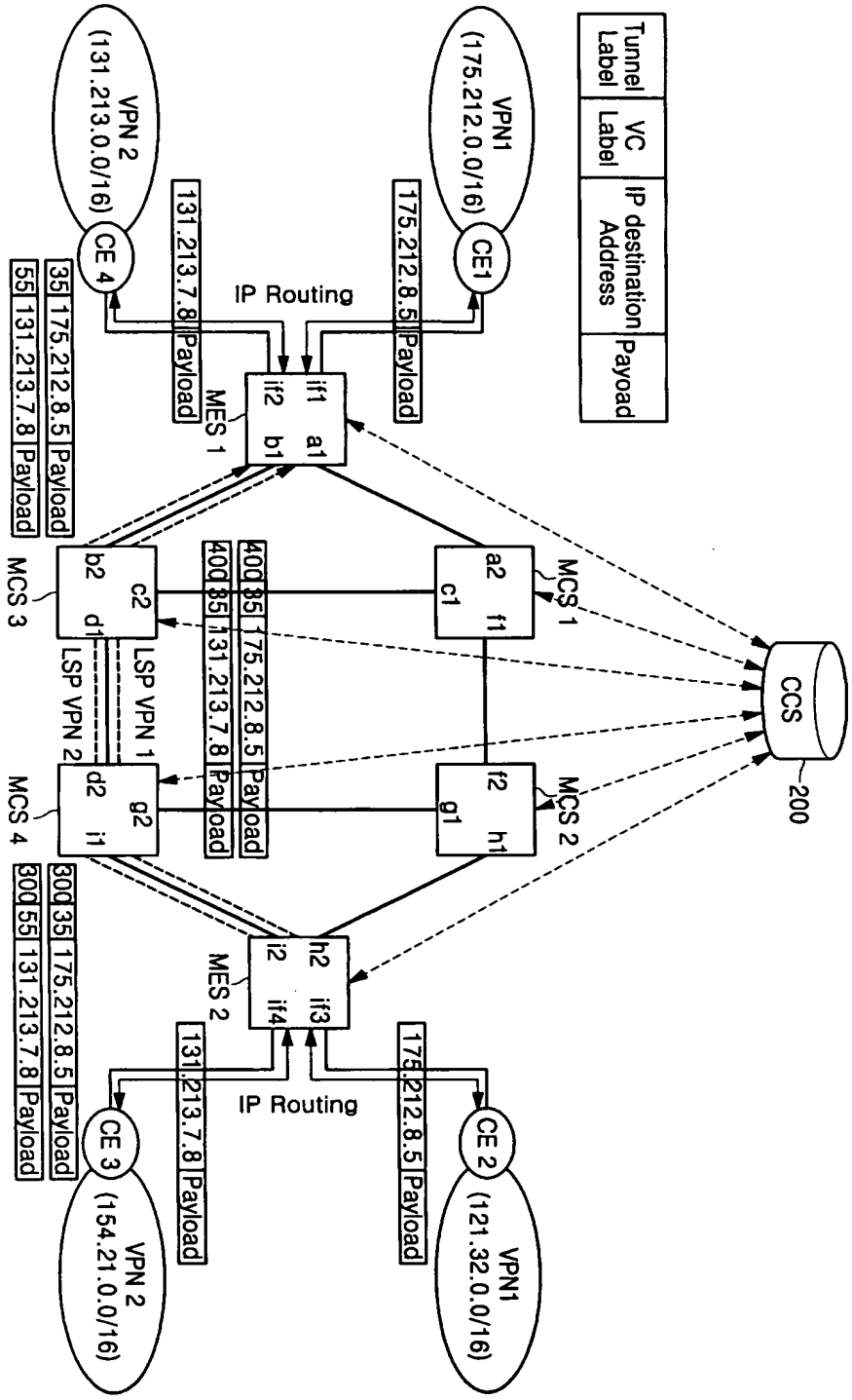
【도 3】


Topology/Resource Information from MES/MCS
Link/LSP Monitoring Information from MES/MCS
LSP Activation Information to MES/MCS
Topology/Resource Discover & Maintenance
300
Link/LSP Monitoring
310
LSP Activation
304
LSP Computation
302
LSP Management
320
Connection Admission Control
330
Policy Management
340
VPN 제공장치
200
콜서버
230
운용자
360

【도 4】


Payload
IP destination Address
VC Label
Tunnel Label
Payload121.32.75.37251 00
Payload154.21.36.7545100
VPN1 (175.212.0.0/16)
CE1
VPN 2 (131.213.0.0/16)
CE 4
Payload121.32.75.37
Payload154.21.36.75
IP Routing
MES 1
if1 a1
if2 b1
a2 c1 f1 MCS 1
b2 c2 d1 MCS 3
d2 g2 i1 MCS 4
g1 f2 h1 MCS 2
LSP VPN 1
LSP VPN 2
CCS
200
Payload121.32.75.37252 00
Payload154.21.36.7545200
Payload121.32.75.37252 5
Payload154.21.36.7545
MES 2
i2 if4
h2 if3
IP Routing
Payload154.21.36.75
Payload121.32.75.37
CE 3
CE 2
VPN 2 (154.21.0.0/16)
VPN1 (121.32.0.0/16)

【도 5】


Tunnel Label
VC Label
IP destination Address
Payoad
VPN1 (175.212.0.0/16)
CE1
175.212.8.5 Payload
VPN 2 (131.213.0.0/16)
CE 4
131.213.7.8 Payload
IP Routing
MES 1
if1 a1
if2 b1
35 175.212.8.5 Payload
55 131.213.7.8 Payload
MCS 3
b2 c2
d1
MCS 1
a2 f1
c1
400 35 175.212.8.5 Payload
400 35 131.213.7.8 Payload
LSP VPN 1
LSP VPN 2
CCS
200
MCS 4
d2 g2
i1
MCS 2
f2 h1
g1
300 35 175.212.8.5 Payload
300 55 131.213.7.8 Payload
MES 2
i2 h2
if4 if3
131.213.7.8 Payload
IP Routing
175.212.8.5 Payload
CE 3
VPN 2 (154.21.0.0/16)
CE 2
VPN1 (121.32.0.0/16)