



**(19) 대한민국특허청(KR)**  
**(12) 공개특허공보(A)**

(11) 공개번호 10-2013-0101663  
 (43) 공개일자 2013년09월16일

(51) 국제특허분류(Int. Cl.)  
 H04L 12/70 (2013.01) H04L 9/32 (2006.01)  
 (21) 출원번호 10-2012-0019891  
 (22) 출원일자 2012년02월27일  
 심사청구일자 없음  
 기술이전 희망 : 기술양도, 실시권허여, 기술지도  
 (71) 출원인  
 한국전자통신연구원  
 대전광역시 유성구 가정로 218 (가정동)  
 (72) 발명자  
 윤승현  
 대전 유성구 도룡동 주공아파트 1동 103호  
 (74) 대리인  
 팬코리아특허법인

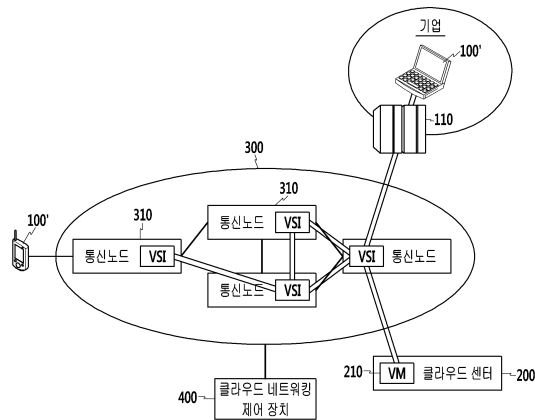
전체 청구항 수 : 총 13 항

(54) 발명의 명칭 **클라우드 네트워킹 장치 및 방법**

**(57) 요약**

통신 노드는 사용자 단말로부터 패킷을 수신하면, 동적 경로 매핑 테이블을 조회하여 상기 패킷의 정보에 대응하는 VSI가 존재하지 않는 경우 사용자 단말의 사용자 인증을 클라우드 네트워킹 제어 장치로부터 요청한다. 클라우드 네트워킹 제어 장치는 사용자가 인증된 사용자인 경우, VSI를 프로비저닝한 후 프로비저닝한 VSI의 정보를 통신 노드로 전송한다. 통신 노드는 VSI를 설정한 후 네트워크에 연결한 후 패킷을 네트워크에 연결된 VSI로 전달한다.

**대표도** - 도2



이 발명을 지원한 국가연구개발사업

과제고유번호 11913-05003

부처명 방송통신위원회

연구사업명 방송통신기술개발사업(원천기술개발사업)

연구과제명 클라우드 네트워킹 및 콘텐츠 중심 네트워킹을 위한 스마트 노드 기술개발

주관기관 한국전자통신연구원

연구기간 2011.03.01~2014.02.28

---

## 특허청구의 범위

### 청구항 1

통신 노드에서 사용자 단말을 네트워크를 통해 클라우드 센터에 연결하는 네트워킹 방법으로,  
 상기 사용자 단말로부터 패킷을 수신하는 단계,  
 동적 경로 매핑 테이블에 상기 패킷의 정보에 대응하는 VSI가 존재하지 않는 경우 상기 사용자 단말의 사용자가 인증된 사용자인지 확인하는 단계,  
 상기 사용자가 인증된 사용자인 경우, 클라우드 네트워킹 제어 장치로부터 VSI의 정보를 수신하는 단계,  
 상기 VSI를 상기 네트워크에 연결하는 단계, 그리고  
 상기 패킷을 상기 네트워크에 연결된 VSI로 전달하는 단계  
 를 포함하는 클라우드 네트워킹 방법.

### 청구항 2

제1항에서,  
 상기 전달하는 단계는  
 상기 VSI를 상기 패킷의 정보에 대응하여 매핑시켜 상기 동적 경로 매핑 테이블에 저장하는 단계를 포함하는 클라우드 네트워킹 방법.

### 청구항 3

제2항에서,  
 상기 동적 경로 매핑 테이블에 상기 패킷의 정보에 대응하는 VSI가 존재하는 경우, 해당 VSI로 상기 패킷을 전달하는 단계  
 를 더 포함하는 클라우드 네트워킹 방법.

### 청구항 4

제1항에서,  
 상기 확인하는 단계는,  
 상기 사용자의 인증을 상기 클라우드 네트워킹 제어 장치로 요청하는 단계, 그리고  
 상기 사용자의 인증 결과를 상기 클라우드 네트워킹 제어 장치로부터 수신하는 단계를 포함하는 클라우드 네트워킹 방법.

### 청구항 5

제1항에서,  
 상기 연결하는 단계는,  
 상기 VSI를 상기 네트워크의 다른 통신 노드에 설정된 VSI와 연결하는 단계를 포함하는 클라우드 네트워킹 방법.

### 청구항 6

제1항에서,  
 상기 사용자가 인증된 사용자가 아닌 경우, 상기 패킷을 폐기하는 단계  
 를 더 포함하는 클라우드 네트워킹 방법.

**청구항 7**

제1항에서,  
 상기 통신 노드는 라우터 또는 패킷 전송 스위치를 포함하는 클라우드 네트워킹 방법.

**청구항 8**

클라우드 네트워킹 제어 장치에서 사용자 단말을 네트워크를 통해 클라우드 센터에 연결하는 네트워킹 방법으로,

동적 경로 매핑 테이블에 상기 패킷의 정보에 대응하는 VSI가 존재하지 않는 경우 통신 노드로부터 상기 사용자 단말의 사용자에 대한 인증 요청을 수신하는 단계,

상기 사용자를 인증하는 단계,

상기 사용자가 인증된 사용자인 경우, 상기 통신 노드에 VSI를 프로비저닝하는 단계, 그리고

상기 통신 노드가 상기 VSI를 상기 네트워크에 연결하도록, 상기 통신 노드에 경로를 프로비저닝하는 단계 포함하는 클라우드 네트워킹 방법.

**청구항 9**

제8항에서,

상기 경로를 프로비저닝하는 단계는,

상기 네트워크에 존재하는 VSI와 네트워크 자원을 고려하여 상기 경로를 계산하는 단계를 포함하는 클라우드 네트워킹 방법.

**청구항 10**

제1항에서,

상기 VSI의 정보를 상기 통신 노드로 전송하는 단계

를 더 포함하는 클라우드 네트워킹 방법.

**청구항 11**

사용자 단말을 네트워크를 통해 클라우드 센터에 연결하는 클라우드 네트워킹 장치에서,

상기 사용자 단말로부터 패킷을 수신하면, 상기 패킷의 정보에 대응하는 VSI가 존재하는지 동적 경로 매핑 테이블을 조회하고, 상기 패킷의 정보에 대응하는 VSI로 상기 패킷을 전달하는 경로 조회부,

상기 패킷의 정보에 대응하는 VSI가 존재하지 않는 경우, 상기 사용자를 상기 클라우드 네트워킹 제어 장치로 인증 요청하는 인증부,

인증된 사용자에 대해 상기 클라우드 네트워킹 제어 장치로부터 VSI의 정보를 수신하여 상기 VSI를 설정한 후 상기 네트워크와 연결하는 VSI 설정부, 그리고

상기 설정한 VSI를 상기 패킷의 정보에 매핑시켜서 상기 동적 경로 매핑 테이블에 저장하는 경로 매핑부를 포함하는 클라우드 네트워킹 장치.

**청구항 12**

제11항에서,

상기 VSI 설정부는 상기 설정한 VSI를 상기 네트워크의 다른 통신 노드에 설정된 VSI와 터널로 연결하는 클라우드 네트워킹 장치.

**청구항 13**

제11항에서,

상기 클라우드 네트워킹 장치는 라우터 또는 패킷 전송 스위치인 클라우드 네트워킹 장치.

## 명세서

### 기술분야

- [0001] 본 발명은 클라우드 네트워킹 장치 및 방법에 관한 것으로, 특히 통신 장비를 이용하여 사용자 단말과 클라우드 센터간의 네트워크 연결을 위한 클라우드 네트워킹 장치 및 방법에 관한 것이다.

### 배경기술

- [0002] 클라우드 컴퓨팅은 정보가 인터넷 상의 클라우드 센터에 영구적으로 저장되고, 사용자 단말에는 해당 정보가 일시적으로 보관되는 컴퓨터 환경으로, 사용자의 모든 정보를 클라우드 센터에 저장하고 이 정보를 각종 사용자 단말을 이용하여 언제 어디서든 이용할 수 있도록 하는 것이다.
- [0003] 현재 클라우드 컴퓨팅 환경은 사용자 단말과 클라우드 센터간 인터넷을 통하여 연결되어 있다. 따라서 품질 문제, 보안 문제 및 신뢰성 문제가 다양하게 발생하게 된다. 보안 문제를 해결하기 위해서 IPSec(Internet Protocol Security)과 같은 IP 터널링 기술을 적용하고 있으나 품질 및 신뢰성은 인터넷과 같은 수준에 그치고 있다.
- [0004] 한편, 품질 문제, 보안 문제 및 신뢰성 문제를 우회하기 위해서 기업의 경우 기업과 데이터 센터간 별도로 전용선을 설치하거나 가상 사설망(virtual private network)을 이용하는 경우도 있으나, 이들 방법은 정적으로 제어되기 때문에 특정 위치에 한정되어 적용 가능한 것으로서 이동성을 고려한 사용자에게 적용하기가 어렵다. 특히, 스마트워크, 원격 근무가 활성화되면서 품질 문제, 보안 문제 및 신뢰성 문제가 더욱 커지게 된다. 따라서 사용자와 클라우드 센터간 연결을 위하여 가상 사설망의 네트워킹 기능을 이동 사용자에게 제공할 수 있는 기술이 필요하다.

### 발명의 내용

#### 해결하려는 과제

- [0005] 본 발명이 해결하고자 하는 기술적 과제는 이동하는 사용자와 클라우드 센터간 네트워크를 통해 직접 연결할 수 있는 클라우드 네트워킹 장치 및 방법을 제공하는 것이다.

#### 과제의 해결 수단

- [0006] 본 발명의 한 실시 예에 따르면, 통신 노드에서 사용자 단말을 네트워크를 통해 클라우드 센터에 연결하는 네트워킹 방법이 제공된다. 클라우드 네트워킹 방법은 상기 사용자 단말로부터 패킷을 수신하는 단계, 동적 경로 매핑 테이블에 상기 패킷의 정보에 대응하는 VSI가 존재하지 않는 경우 상기 사용자 단말의 사용자가 인증된 사용자인지 확인하는 단계, 상기 사용자가 인증된 사용자인 경우, 클라우드 네트워킹 제어 장치로부터 VSI의 정보를 수신하는 단계, 상기 VSI를 상기 네트워크에 연결하는 단계, 그리고 상기 패킷을 상기 네트워크에 연결된 VSI로 전달하는 단계를 포함한다.
- [0007] 상기 전달하는 단계는 상기 VSI를 상기 패킷의 정보에 대응하여 매핑시켜 상기 동적 경로 매핑 테이블에 저장하는 단계를 포함할 수 있다.
- [0008] 상기 클라우드 네트워킹 방법은 상기 동적 경로 매핑 테이블에 상기 패킷의 정보에 대응하는 VSI가 존재하는 경우, 해당 VSI로 상기 패킷을 전달하는 단계를 더 포함할 수 있다.
- [0009] 상기 확인하는 단계는 상기 사용자의 인증을 상기 클라우드 네트워킹 제어 장치로 요청하는 단계, 그리고 상기 사용자의 인증 결과를 상기 클라우드 네트워킹 제어 장치로부터 수신하는 단계를 포함할 수 있다.
- [0010] 본 발명의 다른 실시 예에 따르면, 클라우드 네트워킹 제어 장치에서 사용자 단말을 네트워크를 통해 클라우드 센터에 연결하는 네트워킹 방법이 제공된다. 클라우드 네트워킹 방법은 동적 경로 매핑 테이블에 상기 패킷의 정보에 대응하는 VSI가 존재하지 않는 경우 통신 노드로부터 상기 사용자 단말의 사용자에게 대한 인증 요청을 수신하는 단계, 상기 사용자를 인증하는 단계, 상기 사용자가 인증된 사용자인 경우, 상기 통신 노드에 VSI를 프

로비저닝하는 단계, 그리고 상기 통신 노드가 상기 VSI를 상기 네트워크에 연결하도록, 상기 통신 노드에 경로를 프로비저닝하는 단계를 포함한다.

[0011] 상기 경로를 프로비저닝하는 단계는 상기 네트워크에 존재하는 VSI와 네트워크 자원을 고려하여 상기 경로를 계산하는 단계를 포함할 수 있다.

[0012] 상기 클라우드 네트워킹 방법은 상기 VSI의 정보를 상기 통신 노드로 전송하는 단계를 더 포함할 수 있다.

[0013] 본 발명의 또 다른 실시 예에 따르면, 사용자 단말을 네트워크를 통해 클라우드 센터에 연결하는 클라우드 네트워킹 장치가 제공된다. 클라우드 네트워킹 장치는 상기 사용자 단말로부터 패킷을 수신하면, 상기 패킷의 정보에 대응하는 VSI가 존재하는지 동적 경로 매핑 테이블을 조회하고 상기 패킷의 정보에 대응하는 VSI로 상기 패킷을 전달하는 경로 조회부, 상기 패킷의 정보에 대응하는 VSI가 존재하지 않는 경우, 상기 사용자를 상기 클라우드 네트워킹 제어 장치로 인증 요청하는 인증부, 인증된 사용자에게 대해 상기 클라우드 네트워킹 제어 장치로부터 VSI의 정보를 수신하여 상기 VSI를 설정한 후 상기 네트워크와 연결하는 VSI 설정부, 그리고 상기 설정한 VSI를 상기 패킷의 정보에 매핑시켜서 상기 동적 경로 매핑 테이블에 저장하는 경로 매핑부를 포함한다.

[0014] 상기 VSI 설정부는 상기 설정한 VSI를 상기 네트워크의 다른 통신 노드에 설정된 VSI와 터널로 연결할 수 있다.

### **발명의 효과**

[0015] 본 발명의 실시 예에 의하면, 기존 인터넷망에 비해서 품질 높고 보안 및 안정성이 높은 계층 2 VPN을 이동 사용자를 대상으로 제공할 수 있다. 이에 따라 향후 고품질 클라우드 서비스 환경 및 원격 근무 환경을 개선할 수 있으며 사용자 그룹 또는 서비스 단위의 전용 네트워킹을 제공할 수 있다.

### **도면의 간단한 설명**

[0016] 도 1은 본 발명의 실시 예에 따른 클라우드 네트워킹 방법을 나타낸 도면이다.

도 2는 본 발명의 실시 예에 따른 클라우드 네트워킹 장치를 개략적으로 나타낸 도면이다.

도 3은 본 발명의 실시 예에 따른 통신 노드를 나타낸 도면이다.

도 4는 본 발명의 실시 예에 따른 클라우드 네트워킹 제어 장치를 나타낸 도면이다.

도 5는 본 발명의 실시 예에 따른 통신 노드에서의 클라우드 네트워킹 방법을 나타낸 흐름도이다.

도 6은 본 발명의 실시 예에 따른 클라우드 네트워킹 제어 장치에서의 클라우드 네트워킹 방법을 나타낸 흐름도이다.

### **발명을 실시하기 위한 구체적인 내용**

[0017] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시 예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시 예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0018] 명세서 및 청구범위 전체에서, 어떤 부분이 어떤 구성 요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성 요소를 더 포함할 수 있는 것을 의미한다.

[0019] 이제 본 발명의 실시 예에 따른 클라우드 네트워킹 장치 및 방법에 대하여 도면을 참고로 하여 상세하게 설명한다.

[0020] 도 1은 본 발명의 실시 예에 적용되는 가상 사설망의 일 예를 나타낸 도면이다.

[0021] 도 1을 참고하면, 네트워크(300) 특히, 가상 사설망(Virtual Private Network, VPN)은 기업에서 주로 사용한다. 도 1에서는 네트워크(300)로 계층(Layer) 2 기반의 VPN을 도시하였다.

[0022] 일반적으로 네트워크(300)는 각 통신 노드(310)에 설정된 가상 스위치 인스턴스(Virtual Switch Instance, VSI)를 전용 경로로 연결하여 이더넷-라인(E-Line) 서비스 또는 이더넷-랜(E-LAN) 서비스를 제공한다. 여기서 전용 경로는 다중 프로토콜 레이블 스위칭-전송 프로파일(Multi Protocol Label Switching Transport Profile,

MPLS-TP), PBB-TE(Provider Backbone Bridge Traffic Engineering) 또는 캐리어 이더넷 기반의 터널일 수 있다. 그리고 도 1에서 각 통신 노드(300)간 연결된 실선은 물리적인 연결을 의미한다.

- [0023] 기업의 사용자 단말(100)은 네트워크(300)를 통해서 클라우드 센터(200)에 연결될 수 있다.
- [0024] 클라우드 센터(200)는 사용자 단말(100)에게 제공할 데이터를 저장 및 관리한다. 클라우드 센터(200)는 가상 머신(210)을 포함하며, 가상 머신(210)은 통신 노드(310)에 설정된 VSI와 터널로 연결되며, 연결된 터널을 통해서 데이터를 사용자 단말(100)에 제공한다. 이때 원격지에 있는 기업의 사용자 단말(100)을 고려하여 모든 통신 노드(310)에 VSI를 미리 설정하고 이들 VSI를 연결해 둘 수 없으므로, 기업망 내부에 IP 오버레이 방식의 VPN 게이트웨이(110)를 설치하여 원격지에 있는 기업의 사용자 단말(100)이 VPN 게이트웨이(110)를 경유하여 클라우드 센터(200)로 연결될 수 있도록 한다. 그러나 이러한 방법은 이용자가 VPN 게이트웨이(110)까지 IP 오버레이 방식으로 접근해야 하기 때문에 품질 문제나 신뢰성 문제를 그대로 갖고 있을 수 밖에 없다.
- [0025] 아래에서는 이동 사용자에게 대한 클라우드 네트워킹 방법에 대해서 도 2 내지 도 6을 참고로 하여 자세하게 설명한다.
- [0026] 도 2는 본 발명의 실시 예에 따른 클라우드 네트워킹 장치를 개략적으로 나타낸 도면이다.
- [0027] 도 2를 참고하면, 클라우드 네트워킹 장치는 이동 사용자의 사용자 단말(100')을 네트워크(300)를 이용하여 클라우드 센터(200)에 직접 연결한다.
- [0028] 클라우드 네트워킹 장치는 네트워크(300)의 복수의 통신 노드(310) 및 클라우드 네트워킹 제어 장치(400)를 포함한다.
- [0029] 통신 노드(310)는 라우터나 패킷 전송 스위치와 같은 통신 장비로, VSI 및 터널 설정이 가능한 장비를 전제로 한다. 통신 노드(310)는 사용자 단말(100')과 클라우드 센터(200)간 데이터를 전달하는 역할을 수행한다. 이러한 통신 노드(310)로는 예를 들면 패킷 전송 계층(Packet Transport Layer, PTL) 노드 또는 IP/MPLS 노드가 사용될 수 있다. 아래에서는 설명의 편의상 통신 노드(310)가 PTL 노드인 것으로 가정하고 설명한다.
- [0030] 통신 노드(310)는 사용자 단말(100')과 클라우드 센터(200)의 연결을 위해, 사용자 단말(100')의 사용자 인증을 수행하고, 클라우드 네트워킹 제어 장치(400)의 제어에 따라서 VSI를 설정하며, 설정한 VSI를 다른 통신 노드의 VSI와 터널로 연결한다. 다음, 통신 노드(310)는 사용자 단말(100')로부터 수신한 패킷에 대해 설정한 VSI에 대한 동적 경로 매핑 테이블을 설정한다.
- [0031] 통신 노드(310)는 인증된 사용자 단말(100')로부터 패킷을 수신하면 동적 경로 매핑 테이블을 참조하여 수신한 패킷을 해당 VSI로 전달한다. 이후 통신 노드(310)는 종래의 VPN 기능과 동일하게 동작한다.
- [0032] 한편, 통신 노드(310)가 IP/MPLS 라우터인 경우에, 통신 노드(310)는 VSI 대신 가상 라우팅 포워딩 인스턴스(Virtual Routing and Forwarding Instance, VRF)를 설정하고 이를 다른 통신 노드의 VRF와 연결할 수 있으며, 이렇게 함으로써, 계층(layer) 3 VPN이나 IP VPN이 형성될 수 있다.
- [0033] 클라우드 네트워킹 제어 장치(400)는 사용자 단말(100')과 클라우드 센터(200)간 연결을 제어한다. 특히 클라우드 네트워킹 제어 장치(400)는 사용자 단말(100')의 사용자를 인증하는 역할을 하며, 사용자 단말(100')과 클라우드 센터(200)간 연결을 위하여 통신 노드(310)에 VSI를 프로비저닝하며, 네트워크(300)의 각 통신 노드(310)에 설정된 VSI와 네트워크 자원을 고려하여 프로비저닝한 VSI의 연결을 위한 경로를 계산한 후 다른 통신 노드의 VSI와 연결되도록 통신 노드(310)에 경로를 프로비저닝한다. 여기서 프로비저닝한 VSI는 설정 명령어를 통하여 통신 노드(310)에 새롭게 만든 VSI를 의미한다. 프로비저닝은 통신 노드(310)에 기능이나 동작으로 설정한다는 의미이다. 간단하게, 기능을 인에이블/디스에이블(enable/disable) 할 수 있고 경로를 어디에서부터 어디까지 연결하라는 세부적인 명령을 내릴 수 있으며, 이러한 설정을 클라우드 네트워킹 제어 장치(400)에서 통신 노드(310)에 하는 것을 프로비저닝이라 한다. 프로비저닝은 CLI(Command Line Interface)를 이용하거나 SNMP 셋(set) 명령 등으로 수행될 수 있다.
- [0034] 도 3은 본 발명의 실시 예에 따른 통신 노드를 나타낸 도면이다.
- [0035] 도 3을 참고하면, 통신 노드(310)는 인증 요청부(311), VSI 설정부(313), 경로 조회부(315), 경로 매핑부(317) 및 동적 경로 매핑 테이블(319)를 포함한다.
- [0036] 인증 요청부(311)는 경로 조회부(315)의 인증 요청을 수신하여 사용자 단말(100')의 사용자 인증을 클라우드 네트워킹 제어 장치(400)에 요청하고, 클라우드 네트워킹 제어 장치(400)로부터 인증 결과를 수신한다.

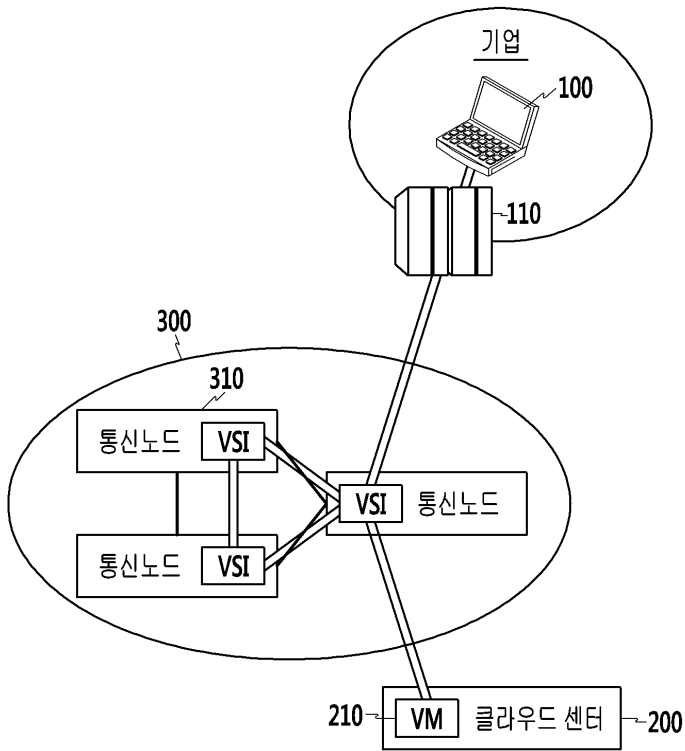
- [0037] VSI 설정부(313)는 클라우드 네트워킹 제어 장치(400)의 제어에 따라서 VSI를 설정하고 설정한 VSI를 네트워크(300)의 다른 통신 장치에 설정된 VSI와 연결한다.
- [0038] 경로 조회부(315)는 사용자 단말(100')로부터 패킷을 수신하면, 동적 경로 매핑 테이블(319)을 참조하여 수신한 패킷에 대한 경로를 조회하여 수신한 패킷을 해당 VSI로 전달한다. 한편, 경로 매핑부(315)는 수신한 패킷에 대한 경로가 동적 경로 매핑 테이블(319)에 존재하지 않는 경우, 인증 요청부(311)로 사용자 인증을 요청하여, 사용자 단말(100')을 네트워크(300)에 연결되도록 한다.
- [0039] 경로 매핑부(317)는 클라우드 네트워킹 제어 장치(400)의 제어에 따라서 인증된 사용자 단말(100')로부터 수신한 패킷의 정보에 대응하여 VSI를 매핑시켜서 저장한다. 즉, 경로 매핑부(316)는 동적 경로 매핑 테이블(3161)을 관리한다.
- [0040] 동적 경로 매핑 테이블(3161)에는 인증된 사용자 단말(100')로부터 수신한 패킷의 정보 중 적어도 하나의 정보에 대응하여 VSI가 저장되어 있다.
- [0041] 동적 경로 매핑 테이블(3161)에는 예를 들어, 인증된 사용자 단말(100')의 패킷이 수신되는 통신 노드(310)의 수신 포트 또는 VLAN 식별자(Identifier, ID)가 VSI에 매핑되어 있을 수 있으며 패킷의 헤더에 포함된 정보(IP 주소, 응용 포트 주소 등)가 VSI에 매핑되어 있을 수 있다.
- [0042] 도 4는 본 발명의 실시 예에 따른 클라우드 네트워킹 제어 장치를 나타낸 도면이다.
- [0043] 도 4를 참고하면, 클라우드 네트워킹 제어 장치(400)는 VPN 가입자 관리부(410), 인증 서버(420), VSI 제어부(430), 자원 관리부(440), 경로 계산부(450) 및 경로 제어부(460)를 포함한다.
- [0044] VPN 가입자 관리부(410)는 VPN 가입자의 정보를 관리한다. VPN 가입자 관리부(410)는 VPN 가입자와 관련된 정보를 저장하고 관리한다. 예를 들면, VPN 가입자 관리부(410)는 기초 정보에는 이름, 주민등록번호, 전화번호, 직업 및 주소 등을 저장하고 관리한다.
- [0045] 인증 서버(420)는 통신 노드(310)로부터 사용자 인증을 요청 받으면, 해당 사용자를 인증한다. 인증 서버(420)는 VPN 가입자 관리부(410)로 사용자가 VPN 가입자인지 조회 요청하여 사용자 단말(100')을 인증할 수 있다.
- [0046] VSI 제어부(430)는 인증 서버(420)에 의해 사용자가 성공적으로 인증되면 해당 통신 노드(310)에 VSI를 프로비저닝한다.
- [0047] 자원 관리부(440)는 네트워크(300)의 네트워크 자원을 관리한다. 즉, 자원 관리부(440)는 네트워크(300)의 토폴로지, 자원 할당 및 네트워크 연결 상태 등을 관리한다.
- [0048] 경로 계산부(450)는 네트워크(300)의 각 통신 노드(310)에 설정된 VSI와 이들간 경로 및 네트워크 자원을 고려하여 프로비저닝한 VSI를 다른 통신 노드의 VSI와 연결을 위한 경로를 계산한다. 경로 계산부(450)는 다양한 조건에 따라서 프로비저닝한 VSI를 다른 통신 노드의 VSI와 연결을 위한 최적의 경로를 계산할 수 있다.
- [0049] 경로 제어부(460)는 프로비저닝한 VSI를 다른 통신 노드의 VSI와 연결되도록 계산한 경로를 통신 노드(310)에 프로비저닝한다.
- [0050] 통지부(470)는 통신 노드(310)로부터 인증 요청 받은 사용자 인증 결과를 통신 노드(310)의 인증 요청부(311)로 전송한다. 통지부(470)는 사용자 인증 성공을 통신 노드(310)로 전송하면서 프로비저닝한 VSI의 정보를 통신 노드(310)에 통지한다. 프로비저닝한 VSI의 정보는 통신 노드(310)에서 이를 구분할 수 있는 VSI의 식별자(ID)나 이름(name)을 포함할 수 있다.
- [0051] 그러면, 통신 노드(310)는 클라우드 네트워킹 제어 장치(400)로부터 수신한 VSI의 정보를 토대로 해당 VSI를 동적 경로 매핑 테이블(319)에 저장한다.
- [0052] 도 5는 본 발명의 실시 예에 따른 통신 노드에서의 클라우드 네트워킹 방법을 나타낸 흐름도이다.
- [0053] 도 5를 참고하면, 통신 노드(310)는 사용자 단말(100')로부터 패킷을 수신하면(S502), 동적 경로 매핑 테이블(319)을 참조하여 수신한 패킷에 대한 경로를 조회한다(S504).
- [0054] 통신 노드(310)는 수신한 패킷에 대한 경로가 동적 경로 매핑 테이블(3161)에 존재하면(S506), 수신한 패킷을 해당하는 VSI로 전달한다(S508).
- [0055] 한편, 통신 노드(310)는 수신한 패킷에 대한 경로가 동적 경로 매핑 테이블(3161)에 존재하지 않으면, 사용자

단말(100')의 사용자에게 대한 인증을 클라우드 네트워킹 제어 장치(400)로 요청한다(S510).

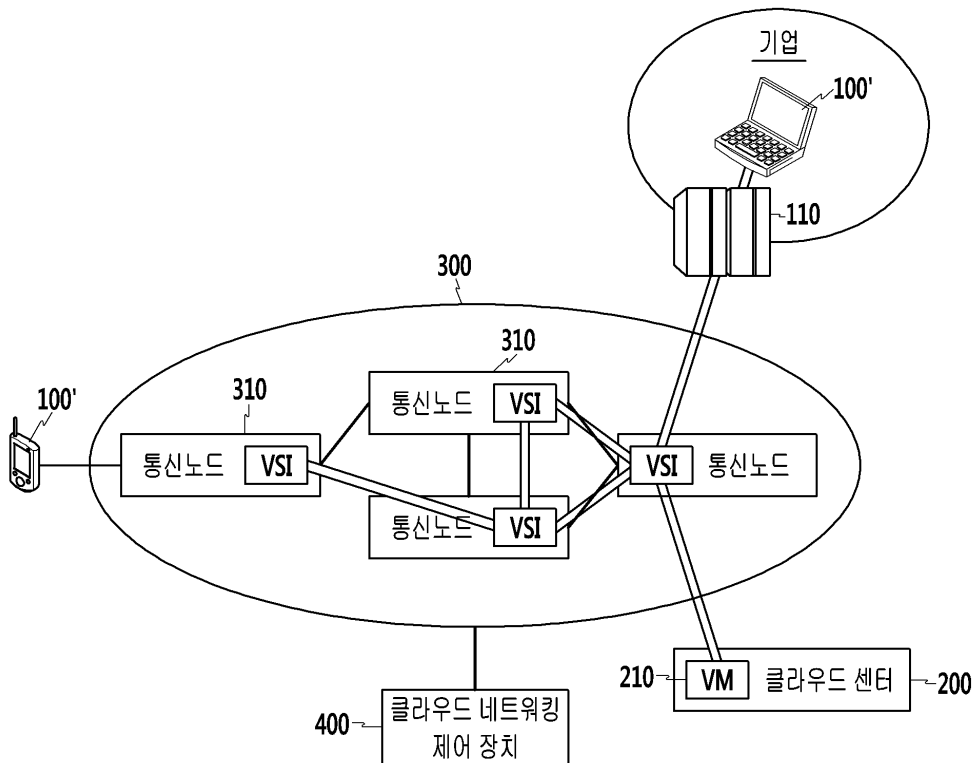
- [0056] 통신 노드(310)는 클라우드 네트워킹 제어 장치(400)로부터 인증 결과를 수신하며(S512), 인증 결과가 인증 성공인 경우(S514), 수신한 VSI의 정보를 토대로 사용자 단말(100')로부터 수신한 패킷과 해당 VSI를 매핑시켜서 동적 경로 매핑 테이블(3161)에 저장하고(S516), 사용자 단말(100')로부터 수신한 패킷을 해당 VSI에 전달한다(S508).
- [0057] 한편, 통신 노드(310)는 인증 결과가 인증 실패인 경우, 사용자 단말(100')로부터 수신한 패킷을 폐기한다(S518).
- [0058] 이와 같이, 통신 노드(310)는 인증 성공한 사용자 단말(100')의 사용자에게 대한 VSI를 설정하고, VSI를 기 설정된 다른 통신 노드의 VSI에 동적으로 연결함으로써, 사용자가 이동하여도 사용자 단말(100')을 네트워크(300)에 직접 연결시킬 수 있게 된다.
- [0059] 도 6은 본 발명의 실시 예에 따른 클라우드 네트워킹 제어 장치에서의 클라우드 네트워킹 방법을 나타낸 흐름도이다.
- [0060] 도 6을 참고하면, 클라우드 네트워킹 제어 장치(400)는 통신 노드(310)로부터 사용자 단말(100')의 사용자에게 대한 인증 요청을 수신하면(S602), 사용자 단말(100')의 사용자가 VPN 가입자인지 조회한다(S604).
- [0061] 클라우드 네트워킹 제어 장치(400)는 사용자 단말(100')의 사용자가 정상적인 VPN 가입자인 경우(S606), 통신 노드(310)에 VSI를 프로비저닝한다(S608).
- [0062] 클라우드 네트워킹 제어 장치(400)는 네트워크(300)에 설정된 VSI와 경로 및 네트워크 자원을 고려하여 프로비저닝한 VSI의 연결을 위한 최적의 경로를 계산한다(S610).
- [0063] 클라우드 네트워킹 제어 장치(400)는 계산한 최적의 경로를 통신 노드(310)에 프로비저닝하여(S612), 통신 노드(310)에서 해당 VSI를 다른 통신 노드의 VSI와 연결되도록 한다.
- [0064] 다음, 클라우드 네트워킹 제어 장치(400)는 사용자 단말(100')의 사용자에게 대한 인증 성공을 통신 노드(310)로 통지한다(S614). 이때 클라우드 네트워킹 제어 장치(400)는 프로비저닝한 VSI의 정보를 통신 노드(310)에 전송한다.
- [0065] 한편, 클라우드 네트워킹 제어 장치(400)는 사용자 단말(100')의 사용자가 정상적인 VPN 가입자가 아닌 경우(S606), 통신 노드(310)에 인증 실패를 통지한다(S616).
- [0066] 한편, 이상에서 설명한 장치 및/또는 방법은 L2 기반의 네트워크(300)를 실시 예로 가정하여 설명하였지만, 이상에서 설명한 장치 및/또는 방법은 라우터 기반의 L3 VPN, IP 기반의 VPN 및 캐리어 이더넷 기반의 VPN 또는 다중 서비스 지원 플랫폼(Multi-service Provisioning Platform, MSPP)이 결합된 SONET/SDH 망에서도 적용할 수 있다.
- [0067] 본 발명의 실시 예는 이상에서 설명한 장치 및/또는 방법을 통해서만 구현되는 것은 아니며, 본 발명의 실시 예의 구성에 대응하는 기능을 실현하는 프로그램 또는 그 프로그램이 기록된 기록 매체를 통해 구현될 수도 있으며, 이러한 구현은 앞서 설명한 실시 예의 기재로부터 본 발명이 속하는 기술 분야의 전문가라면 쉽게 구현할 수 있는 것이다.
- [0068] 이상에서 본 발명의 실시 예에 대하여 상세하게 설명하였지만 본 발명의 권리 범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리 범위에 속하는 것이다.

도면

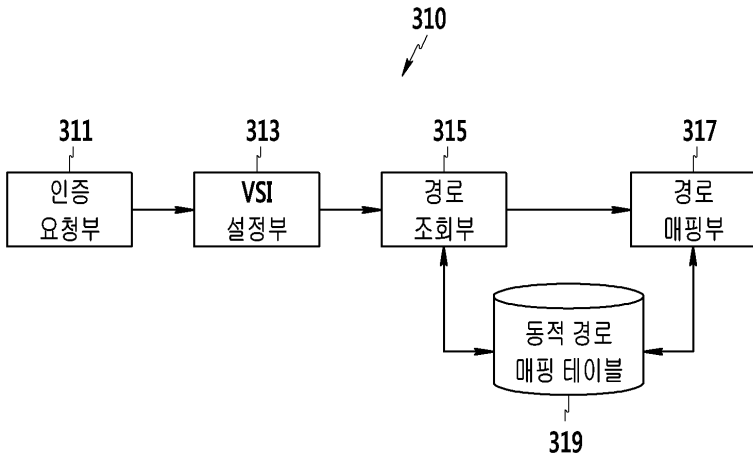
도면1



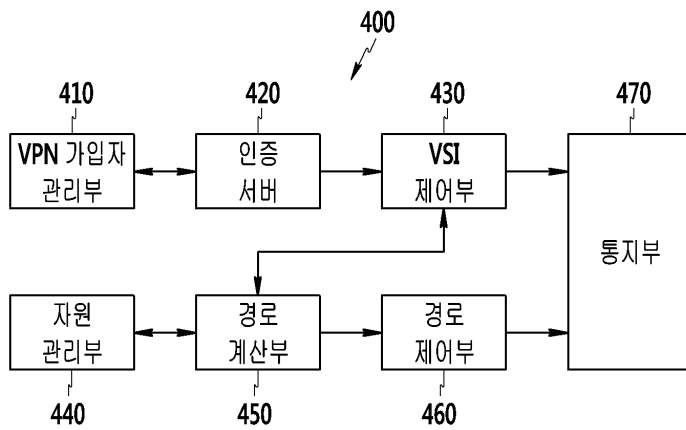
도면2



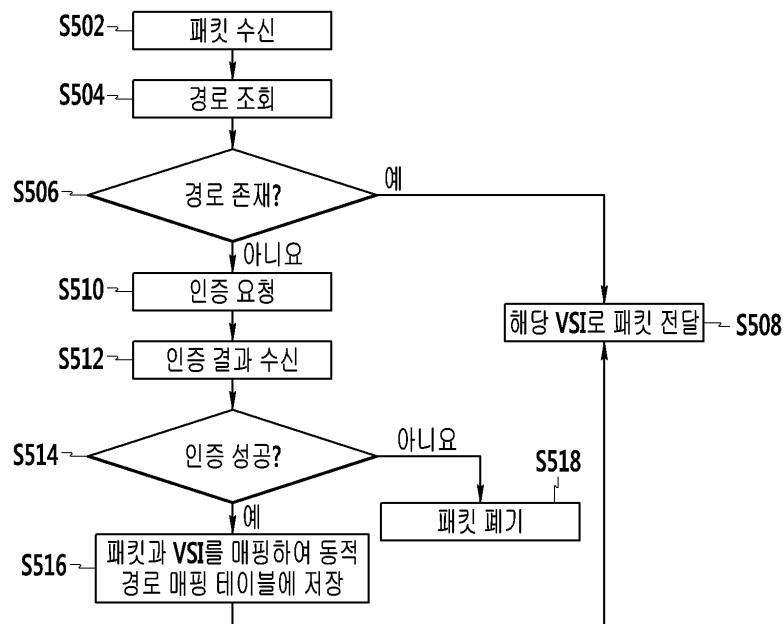
도면3



도면4



도면5



도면6

