(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0049929
(43) 공개일자 2012년05월17일

(51) 국제특허분류(Int. Cl.)
H04L 12/46 (2006.01) *H04L 12/56* (2006.01)
H04L 29/06 (2006.01)
(21) 출원번호 10-2012-7008063
(22) 출원일자(국제) 2010년09월21일
심사청구일자 2012년03월29일
(85) 번역문제출일자 2012년03월29일
(86) 국제출원번호 PCT/US2010/049570
(87) 국제공개번호 WO 2011/041162
국제공개일자 2011년04월07일
(30) 우선권주장
12/571,274 2009년09월30일 미국(US)

(71) 출원인
알까뗄 루슨트
프랑스 75007 파리 옥타브 그레드 애비뉴 3
(72) 발명자
우 토마스
미국 뉴저지주 07078 소트 힐스 엑스터 로드 2
리 리 에란
미국 뉴저지주 08820 에디슨 마사 스트리트 8
(74) 대리인
제일특허법인

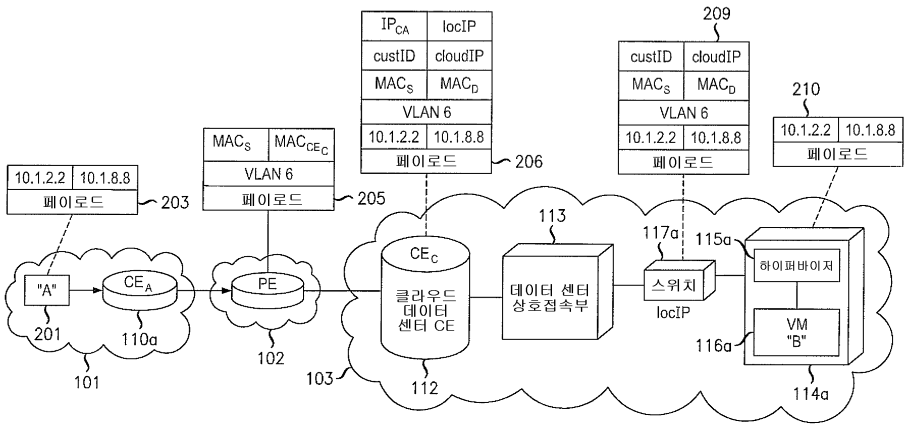
전체 청구항 수 : 총 10 항

(54) 발명의 명칭 **기업의 클라우드 컴퓨팅 내에서의 레이어 2 심리스 사이트확장**

(57) 요 약

다양한 실시예는 클라우드 데이터 센터, 클라우드 데이터 센터를 포함하는 시스템, 및 관련된 방법에 관한 것이다. 클라우드 데이터 센터는 레이어 2 프로토콜 및 MAC 어드레싱을 사용하여 사설 엔터프라이즈 네트워크 내의 어드레스와 클라우드 네트워크 내의 논리적 네트워크 내의 어드레스 사이에 패킷을 발송하기 위해 논리적 고객에지 라우터를 포함할 수 있다. 논리적 네트워크는 사설 엔터프라이즈 네트워크에 할당된 가상 머신으로 알려진 자원을 가질 수 있으며, 사설 엔터프라이즈 네트워크와 공통 IP 어드레스 공간을 공유할 수 있다. 클라우드 데이터 센터에서의 디렉토리는 가상 머신의 기업 IP 어드레스를 논리적 네트워크 내의 MAC 어드레스, 클라우드 IP 어드레스, 및 위치 IP 어드레스에 상관시킬 수 있다. 클라우드 데이터 센터는 논리적 네트워크 내의 목적지로 패킷을 발송할 때 MAC, cloudIP, 및 locIP 헤더를 이용하여 패킷을 이중 캡슐화할 수 있다.

대 표 도



특허청구의 범위

청구항 1

사설 엔터프라이즈 네트워크(private enterprise network) 내의 소스로부터 수신되는 패킷을 상기 사설 엔터프라이즈 네트워크에 할당된 클라우드 네트워크 내의 목적지로 발송하는 방법으로서, 상기 방법은

상기 클라우드 네트워크 내의 클라우드 데이터 센터(Cloud Data Center) 내의 논리적 고객 에지 라우터(logical customer edge router)에 의해, 상기 사설 엔터프라이즈 네트워크 내의 소스로부터 레이어 2 패킷을 수신하는 단계 - 상기 논리적 고객 에지 라우터는 상기 사설 엔터프라이즈 네트워크에 할당된 자원을 포함하는 상기 클라우드 네트워크 내의 논리적 네트워크 내에 위치됨 - 와,

상기 논리적 고객 에지 라우터에 의해, 디렉토리 서버에게 상기 목적지의 MAC 어드레스 및 위치 IP 어드레스에 대해 질의하는 단계와,

상기 논리적 고객 에지 라우터에 의해, 상기 목적지가 상기 논리적 네트워크 내에 존재한다고 상기 논리적 고객 에지 라우터가 판단할 때 상기 수신된 레이어 2 패킷을 캡슐화(encapsulating)하는 단계 - 상기 수신된 레이어 2 패킷은 상기 목적지의 상응하는 MAC 어드레스 헤더를 이용하여 캡슐화됨 - 와,

상기 논리적 고객 에지 라우터에 의해, 상기 목적지의 상응하는 위치 IP 헤더를 이용하여 상기 수신된 레이어 2 패킷을 추가로 캡슐화하는 단계와,

상기 논리적 고객 에지 라우터에 의해, 상기 목적지로 상기 수신된 레이어 2 패킷을 전달하는 단계 - 상기 논리적 고객 에지 라우터는 상기 목적지 위치 IP 어드레스를 통해 상기 목적지 MAC 어드레스로 상기 수신된 레이어 2 패킷을 전달함 - 를 포함하는

방법.

청구항 2

제 1 항에 있어서,

상기 목적지의 위치 IP 어드레스에서의 스위치에 의해, 상기 수신된 레이어 2 패킷의 상기 위치 IP 헤더를 캡슐화 해제(decapsulating)하는 단계와,

상기 목적지의 스위치에 의해, 상기 목적지의 MAC 어드레스로 상기 수신된 레이어 2 패킷을 전달하는 단계와,

상기 목적지의 MAC 어드레스에서의 목적지 서버에 의해, 상기 수신된 레이어 2 패킷의 상기 MAC 헤더를 캡슐화 해제하는 단계와,

상기 목적지 서버에 의해, 상기 목적지 서버 내의 상기 목적지로 상기 레이어 2 패킷을 전달하는 단계를 더 포함하는

방법.

청구항 3

제 2 항에 있어서,

상기 목적지 서버 내의 하이퍼바이저(hypervisor)에 의해, 상기 수신된 레이어 2 패킷이 동일한 기업으로부터 유래한다는 것을 확인하는 단계 - 상기 하이퍼바이저는 상기 수신된 레이어 2 패킷의 상기 헤더 내의 보안 토큰을 검사함 - 와,

상기 하이퍼바이저에 의해, 상기 레이어 2 패킷의 보안 토큰이 확인되지 않을 때 상기 레이어 2 패킷을 폐기하는 단계 - 상기 보안 토큰은 적어도 하나의 기업 고유의 키, 기업 ID, 및 목적지 IP 어드레스를 포함함 - 를 더 포함하는

방법.

청구항 4

제 2 항에 있어서,

상기 목적지 서버 내의 하이퍼바이저에 의해, 상기 수신된 레이어 2 패킷이 동일한 VLAN으로부터 유래한다는 것을 확인하는 단계 - 상기 하이퍼바이저에 의해 수행된 상기 확인은 상기 MAC 어드레스 헤더 내의 상기 레이어 2 패킷의 VLAN 태그를 분석함 - 와,

상기 하이퍼바이저에 의해, 상기 목적지가 동일한 VLAN에 속하지 않을 때 상기 레이어 2 패킷을 폐기하는 단계와,

상기 하이퍼바이저에 의해, 상기 목적지가 동일한 VLAN에 속할 때 상기 레이어 2 패킷으로부터 상기 MAC 어드레스 헤더를 스트립(stripping)하는 단계와,

상기 하이퍼바이저에 의해, 상기 목적지로 상기 레이어 2 패킷을 전달하는 단계를 더 포함하는

방법.

청구항 5

제 1 항에 있어서,

상기 논리적 고객 에지 라우터에 의해, 디렉토리 서버에게 상기 목적지의 클라우드 IP 어드레스에 대해 질의하는 단계와,

상기 논리적 고객 에지 라우터에 의해, 상기 목적지의 클라우드 IP 헤더를 이용하여 상기 수신된 레이어 2 패킷을 캡슐화하는 단계를 더 포함하며,

상기 전달 단계는

상기 논리적 고객 에지 라우터가 상기 목적지 위치 IP 어드레스를 통해 상기 목적지 클라우드 IP 어드레스로 상기 레이어 2 패킷을 전달하는 단계와,

상기 목적지의 위치 IP 어드레스에서의 스위치에 의해, 상기 수신된 레이어 2 패킷의 상기 위치 IP 헤더를 캡슐화 해제하는 단계와,

상기 목적지의 스위치에 의해, 상기 목적지의 클라우드 IP 어드레스로 상기 수신된 레이어 2 패킷을 전달하는 단계와,

상기 목적지의 클라우드 IP 어드레스에서의 목적지 서버에 의해, 상기 수신된 레이어 2 패킷의 상기 클라우드 IP 헤더를 캡슐화 해제하는 단계와,

상기 목적지 서버에 의해, 상기 목적지 서버 내의 상기 목적지로 상기 레이어 2 패킷을 전달하는 단계를 포함하는

방법.

청구항 6

사설 엔터프라이즈 네트워크에 할당된 클라우드 네트워크 내의 소스로부터 유래하는 패킷을 전달하는 방법에 있어서, 상기 방법은

상기 사설 엔터프라이즈 네트워크에 할당된 자원을 포함하는 상기 클라우드 네트워크 내의 논리적 네트워크 내에 위치되는 소스 가상 머신을 호스트하는 서버 내의 하이퍼바이저에 의해, 레이어 2 패킷을 수신하는 단계와,

상기 하이퍼바이저에 의해, 상기 레이어 2 패킷의 목적지 어드레스가 상기 서버에서의 가상 라우팅 및 전달 표

내에 존재하지 않을 때 상기 논리적 네트워크 내의 디렉토리 서버에게 목적지 어드레스에 대해 질의하는 단계와,

상기 하이퍼바이저에 의해, 상기 디렉토리 서버로부터 수신된 상기 MAC 어드레스 엔트리에 상응하는 MAC 헤더를 이용하여 상기 레이어 2 패킷을 캡슐화하는 단계와,

상기 하이퍼바이저에 의해, 상기 디렉토리 서버로부터 수신된 상기 목적지의 클라우드 IP 어드레스에 상응하는 위치 IP 헤더를 이용하여 상기 레이어 2 패킷을 추가로 캡슐화하는 단계와,

상기 하이퍼바이저에 의해, 상기 목적지 위치 IP 어드레스를 통해 상기 목적지 MAC 어드레스로 상기 레이어 2 패킷을 전달하는 단계를 포함하는

방법.

청구항 7

제 6 항에 있어서,

클라우드 데이터 센터 내의 논리적 고객 에지 라우터에 의해, 상기 패킷의 상기 위치 IP 헤더를 캡슐화 해제하는 단계와,

상기 논리적 고객 에지 라우터에 의해, 상기 디렉토리 서버 내의 상기 목적지에 대한 엔트리가 존재할 때 상기 제 1 MAC 헤더를 상기 목적지 MAC 어드레스에 상응하는 제 2 MAC 헤더로 대체하는 단계와,

상기 논리적 고객 에지 라우터에 의해, 상기 디렉토리 서버 내의 상기 목적지에 대한 엔트리가 존재할 때 상기 제 2 MAC 헤더로써 상기 레이어 2 패킷을 상기 목적지 MAC 어드레스로 터널링(tunneling)하는 단계와,

상기 논리적 고객 에지 라우터에 의해, 가상 라우팅 및 전달 표 내에 상기 목적지에 대한 엔트리가 존재하지 않을 때 상기 제 1 MAC 어드레스를 MAC 브로드캐스트 헤더로 대체하는 단계와,

상기 논리적 고객 에지 라우터에 의해, 상기 가상 라우팅 및 전달 표 내에 상기 목적지에 대한 엔트리가 존재하지 않을 때 상기 MAC 브로드캐스트 헤더로써 상기 레이어 2 패킷을 상기 사설 엔터프라이즈 네트워크 내의 각각의 고객 에지 라우터로 터널링하는 단계를 더 포함하는

방법.

청구항 8

제 6 항에 있어서,

상기 하이퍼바이저에 의해, 기업 고유의 키, 기업 ID, 및 목적지 IP 어드레스의 조합을 포함하는 보안 토큰을 계산하는 단계와,

상기 하이퍼바이저에 의해, 상기 보안 토큰을 이용하여 상기 패킷을 캡슐화하는 단계를 더 포함하는

방법.

청구항 9

제 8 항에 있어서,

상기 사설 엔터프라이즈 네트워크 내의 상기 목적지에서의 고객 에지 라우터에 의해, 상기 MAC 헤더를 캡슐화 해제하는 단계와,

상기 목적지에서의 상기 고객 에지 라우터에 의해, 상기 수신된 패킷의 상기 헤더 내의 상기 보안 토큰을 확인하는 단계와,

상기 목적지에서의 상기 고객 에지 라우터에 의해, 상기 보안 토큰이 확인되지 않을 때 상기 수신된 패킷을 폐

기하는 단계를 더 포함하는

방법.

청구항 10

제 8 항에 있어서,

상기 하이퍼바이저에 의해, 상기 디렉토리 서버로부터 수신된 상기 목적지의 클라우드 IP 어드레스에 상응하는 클라우드 IP 헤더를 이용하여 상기 레이어 2 패킷을 추가로 캡슐화하는 단계와,

클라우드 데이터 센터 내의 상기 논리적 고객 에지 라우터에 의해, 상기 패킷의 상기 클라우드 IP 헤더를 캡슐화 해제하는 단계를 더 포함하는

방법.

명 세 서

기 술 분 야

[0001] 여기에 개시된 실시예는 일반적으로 네트워크 하부 구조(network infrastructure) 및 인터넷 통신에 관한 것이다.

배 경 기 술

[0002] 클라우드 컴퓨팅 네트워크는 고도로 확장 가능한 동적 서비스(highly-scalable, dynamic service)이며, 이는 클라우드 컴퓨팅 제공자가 인터넷을 통해 고객에게 자원을 제공하게 한다. 클라우드 하부 구조(infrastructure)는 추상 계층(layer of abstraction)을 제공하며, 따라서 고객은 요청된 자원을 제공하는 클라우드 내의 특정 하부 구조에 대한 지식을 요구하지 않는다. 그러한 서비스는 고객이 피크 사용을 위한 추가적인 하드웨어에 대한 자본 지출을 피할 수 있게 해주는데, 왜냐하면 고객은 일상적인 용도에 대해 사설 엔터프라이즈 네트워크(private enterprise network) 내에 이미 적절한 하부 구조를 사용하면서 과중한 부하에 대해 클라우드 내의 추가 자원을 사용할 수 있기 때문이다.

[0003] 예를 들어, IaaS(infrastructure as a service)와 같은 시스템은 고객이 그들 자신의 컴퓨터 애플리케이션을 실행시키는 컴퓨터를 임대하게 한다. 이러한 시스템은 자원의 확장 가능성 있는(scalable) 배치를 허용하며, 고객은 그들 선택의 소프트웨어를 실행하기 위해 가상 머신, 즉, 서버 인스턴스(server instance)를 생성한다. 고객은 필요에 따라 이들 가상 머신(virtual machine)을 생성하고, 사용하며, 제거할 수 있으며, 제공자는 사용되는 활성 서버에 대해 항상 요금을 부과한다.

[0004] 그러나, 기존의 서비스는 사설 엔터프라이즈 네트워크 내측의 자원과 같은 할당된 자원을 취급하지 않는다. 이는 예를 들어 애플리케이션이 네트워크 내의 특정 위치로 데이터를 발송하거나 내부 네트워크 및 클라우드 네트워크가 상이한 어드레스 공간 또는 어드레싱 방안(addressing scheme)을 사용할 때 문제를 야기할 수 있다. 또한, 악의적인 공격으로부터 클라우드 자원을 격리시키는 것에 연관된 문제 및 클라우드 네트워크 자원으로의 접속이 내부 네트워크 하부 구조를 위태롭게 하지 않는다는 것을 보장하는 것에 연관된 문제가 존재한다. 또한, 고객은 두 개의 위치로부터의 자원을 동등한 것으로 취급하는 대신에, 별개의 세트의 내부 및 클라우드 자원을 다루는 데 있어서 추가된 복잡성에 직면할 수 있다.

[0005] 따라서, 클라우드 네트워크 내의 고객에 할당된 자원을 고객의 기존의 사설 엔터프라이즈 네트워크 내로 심리스하게(seamless) 통합시키기 위해 IaaS를 능가하는 필요성이 존재한다. 이러한 확장은 모든 할당된 클라우드 자원이 사설 엔터프라이즈 네트워크 내에 위치된 자원을 찾아보고 그에 유사하게 작용하게 할 것이다. 이러한 구현은 기업(enterprise)의 작업 부하(workload)가 전용 사설 엔터프라이즈 네트워크의 자원 및 클라우드 토폴로지(cloud topology) 내의 할당된 자원의 동적 혼합을 거쳐 심리스하게 확산하게 할 것이다.

[0006] 전술한 설명에 비추어, 클라우드 네트워크 내의 자원을 포함하도록 사설 엔터프라이즈 네트워크를 심리스하게 확장시키는 것이 바람직할 것이다. 보다 구체적으로, 사설 엔터프라이즈 네트워크 내의 자원과 클라우드 네트

워크 내의 할당된 자원 사이에 통신을 가능하게 하여 고객이 사설 네트워크 상의 자원과 동일한 방식으로 클라우드 자원을 취급할 수 있는 것이 바람직할 것이다. 다른 바람직한 양태는 본 상세한 설명을 판독하고 이해할 때 당업자에게 당연할 것이다.

발명의 내용

해결하려는 과제

[0007] 사설 엔터프라이즈 네트워크의 클라우드 네트워크 내로의 심리스(seamless) 확장을 위한 현재의 필요성에 비추어, 다양한 예시적인 실시예에 대한 발명의 내용이 제시된다. 다음의 발명의 내용 내에서 일부 간소화 및 생략이 수행될 수 있는데, 발명의 내용은 다양한 예시적인 실시예의 일부 양태를 강조하고 도입하도록 의도되지만 본 발명의 범위를 제한하도록 의도되지는 않는다. 당업자가 본 발명의 개념을 생성하고 사용하기에 충분한 바람직한 예시적인 실시예의 상세한 설명이 다음의 절들에서 뒤따를 것이다.

과제의 해결 수단

[0008] 다양한 실시예는 사설 엔터프라이즈 네트워크 내의 소스로부터 수신된 패킷을 사설 엔터프라이즈 네트워크에 할당된 클라우드 네트워크 내의 목적지로 발송하는 패킷 발송 방법에 관한 것이다. 상기 패킷 발송 방법은 상기 클라우드 네트워크 내의 클라우드 데이터 센터(Cloud Data Center) 내의 논리적 고객 에지 라우터 내에서 상기 사설 엔터프라이즈 네트워크 내의 소스로부터 레이어 2 패킷을 수신하되, 상기 클라우드 데이터 센터는 상기 사설 엔터프라이즈 네트워크에 할당된 자원을 포함하는 상기 클라우드 네트워크 내의 논리적 네트워크인 단계를 포함한다. 상기 패킷 발송 방법은 상기 클라우드 데이터 센터 내의 상기 논리적 고객 에지 라우터에 의해 디렉토리 서버에게 상기 목적지의 MAC 어드레스 및 위치 IP 어드레스에 대해 질의하는 단계, 상기 목적지가 상기 논리적 네트워크 내에 존재한다고 상기 클라우드 데이터 센터 내의 상기 논리적 고객 에지 라우터가 판단할 때 상기 목적지의 상응하는 MAC 어드레스 헤더를 이용하여 상기 수신된 레이어 2 패킷을 캡슐화하는 단계, 상기 목적지의 상응하는 위치 IP 헤더를 이용하여 상기 수신된 레이어 2 패킷을 추가로 캡슐화하는 단계, 및 상기 논리적 고객 에지 라우터에 의해 상기 수신된 레이어 2 패킷을 상기 목적지로 전달하되, 상기 논리적 고객 에지 라우터는 상기 목적지 위치 IP 어드레스를 통해 상기 목적지 MAC 어드레스로 상기 수신된 레이어 2 패킷을 전달하는 단계를 포함한다.

[0009] 다양한 실시예는 또한 사설 엔터프라이즈 네트워크에 할당된 클라우드 네트워크 내의 소스로부터 유래하는 패킷을 전달하는 방법에 관한 것일 수 있다. 상기 패킷 전달 방법은 상기 사설 엔터프라이즈 네트워크에 할당된 자원을 포함하는 상기 클라우드 네트워크 내의 논리적 네트워크 내에 위치되는 가상 머신을 호스트하는 서버 내의 하이퍼바이저가 레이어 2 패킷을 수신하는 단계, 상기 레이어 2 패킷의 목적지 어드레스가 상기 서버에서 가상 라우팅 및 전달 표 내에 존재하지 않을 때 상기 논리적 네트워크 내의 디렉토리 서버에게 목적지 어드레스에 대해 질의하는 단계, 상기 디렉토리 서버로부터 수신된 MAC 어드레스 엔트리에 상응하는 MAC 헤더를 이용하여 상기 레이어 2 패킷을 캡슐화하는 단계, 상기 디렉토리 서버로부터 수신된 상기 목적지의 클라우드 IP 어드레스에 상응하는 위치 IP 헤더를 이용하여 상기 레이어 2 패킷을 추가로 캡슐화하는 단계, 및 상기 목적지 위치 IP 어드레스를 통해 상기 목적지 MAC 어드레스로 상기 레이어 2 패킷을 전달하는 단계를 포함한다.

[0010] 다양한 실시예는 또한 사설 엔터프라이즈 네트워크 내의 적어도 하나의 고객 에지 라우터 및 상기 사설 엔터프라이즈 네트워크에 할당된 가상 머신을 호스트하고 상기 사설 엔터프라이즈 네트워크 내의 위치와 상기 클라우드 네트워크 내의 위치 사이에서 레이어 2 패킷을 발송하는 서버로 접속시키는 논리적 고객 에지 라우터에 관한 것일 수 있으며, 상기 논리적 고객 에지 라우터, 상기 가상 머신, 및 상기 사설 엔터프라이즈 네트워크 내의 상기 고객 에지 라우터는 상기 사설 엔터프라이즈 네트워크에 할당된 공통 IP 어드레스 공간 및 VLAN을 공유한다.

발명의 효과

[0011] 전술한 설명에 따라, 다양한 예시적인 실시예는 기업의 사설 어드레스 공간 내측에 클라우드 자원을 배치시켜서, 클라우드 자원을 기업의 기존의 토폴로지(topology) 내로 심리스하게 통합시킨다. 다양한 실시예

는 또한 네트워크 외측의 임의의 자원으로부터 격리된 엔터프라이즈 네트워크의 보안 경계 내측에 클라우드 자원을 배치시킴으로써 보안을 보장한다. 그에 의해, 고객은 그 고객이 엔터프라이즈 네트워크의 내부 자원을 구성하고 관리하는 것과 동일한 방식으로 클라우드 자원을 구성할 수 있다. 이들 장점에 추가하여, 다양한 실시예는 또한 클라우드 컴퓨팅 패러다임(cloud coumputing paradigm), 즉 클라우드 자원의 고도의 동적 확장 가능성(highly-dynamic scalability of cloud resources)의 장점을 유지한다.

도면의 간단한 설명

[0012] 이제 실시예에 따른 장치 및/또는 방법의 일부 실시예가 오직 예로서 도면을 참조하여 설명된다.

도 1은 사설 엔터프라이즈 네트워크를 클라우드 네트워크로 확장하기 위한 예시적인 네트워크의 개략적인 다이어그램이다.

도 2는 레이어 2(L2) 프로토콜을 사용하는 이중 캡슐화된 패킷 전송의 개략적인 다이어그램이다.

도 3은 etherIP 및 VLAN 변환을 사용하는 패킷 전송의 개략적인 다이어그램이다.

도 4는 확장된 엔터프라이즈 네트워크 내에서 발견된 네트워크 장치에 대한 예시적인 가상 라우팅 및 전달 표의 개략적인 다이어그램이다.

도 5는 클라우드 네트워크 내에서 발견된 네트워크 장치에 대한 위치 엔트리의 예시적인 디렉토리 표의 개략적인 다이어그램이다.

도 6은 확장된 엔터프라이즈 네트워크를 통해 송신된 예시적인 다이어그램의 콘텐츠를 도시하는 개략적인 다이어그램이다.

도 7은 사설 엔터프라이즈 네트워크 내의 위치로부터 클라우드 네트워크 내의 위치로 패킷을 발송하는 방법의 예시적인 실시예의 흐름도이다.

도 8은 클라우드 네트워크 내측의 위치로부터 패킷을 발송하는 방법의 예시적인 실시예의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0013] 이제 동일 부호가 동일 구성요소 또는 단계를 지칭하는 도면을 참조하여, 다양한 예시적인 실시예의 넓은 양상이 개시된다.

[0014] 도 1은 사설 엔터프라이즈 네트워크를 클라우드 토폴로지(cloud topology)로 확장하기 위한 예시적인 네트워크(100)의 개략적인 다이어그램이다. 다양한 예시적인 실시예에서, 네트워크(100)는 사설 엔터프라이즈 네트워크(101, private enterprise network), 서비스 제공자 네트워크(102, service provider network), 클라우드 네트워크(103, cloud network), 고객 에지(customer edge, CE) 장치(110a 내지 110h), 제공자 에지(provider edge, PE) 장치(111a 내지 111h), 클라우드 데이터 센터(Cloud Data Center) CE(112), 데이터 센터 상호접속부(113, Data Center Interconnect), 및 서버(114a 내지 114d)를 포함하며, 각각의 서버(114a 내지 114d)는 하이퍼바이저(115a 내지 115d) 및 가상 머신(116a 내지 116d)을 수용한다.

[0015] 사설 엔터프라이즈 네트워크(101), 서비스 제공자 네트워크(102), 및 클라우드 네트워크(103)는 각각 패킷 교환식 네트워크(packet-switched network)일 수 있다. 이러한 패킷 교환식 네트워크는 패킷 기반 프로토콜(packet-based protocol)에 따라 동작하는 임의의 네트워크일 수 있다. 따라서, 네트워크(101, 102, 103)는 각각 예를 들어 송신 제어 프로토콜/인터넷 프로토콜(Transmission Control Protocol/Internet Protocol, TCP/IP), 멀티 프로토콜 레이블 스위칭(Multi Protocol Label Switching, MPLS), 비동기 전송 모드(Asynchronous Transfer Mode, ATM), 프레임 릴레이(Frame Relay), 이더넷(Ethernet), 제공자 백본 전송(Provider Backbone Transport, PBT), 또는 당업자에게 당연한 임의의 다른 적절한 패킷 기반 프로토콜에 따라 동작할 수 있다. 보다 구체적으로, 패킷 교환식 네트워크(101, 102, 103)는 MPLS와 같은 레이어 3 프로토콜(Layer 3 protocol)을 사용하여 가상 사설 네트워크(virtual private network, VPN)으로서 통신할 수 있다.

[0016] 사설 엔터프라이즈 네트워크(101)는 고객 엔티티(customer entity) 전용인 하드웨어를 포함하는 네트워크일 수 있으며, 기업 내의 장치가 동일한 주소 공간을 차지하도록 구성될 수 있다. 사설 엔터프라이즈 네트워크(101) 내의 장치는 공통 가상 근거리 통신망(virtual local area network, VLAN)을 공유할 수 있다. 예시적인 실시

예에서, 사설 엔터프라이즈 네트워크(101)는 일련의 고객 에지(CE) 장치(110a 내지 110e)를 포함한다.

[0017] 도 1에 도시된 실시예에서, 사설 엔터프라이즈 네트워크 A(EntA)는 서비스 제공자 네트워크(102)를 통해 서로 통신하는 두 개의 상이한 사이트에 위치된 고객 에지 장치(110a 내지 110e)를 포함한다. 일부 실시예에서, 사설 엔터프라이즈 네트워크(101)는 동일한 물리적인 사이트에서 서로 직접 접속시키는 장치를 포함할 수 있다.

[0018] 사설 엔터프라이즈 네트워크(101) 내의 장치는 예를 들어 VLAN을 공유하면서 동일한 어드레스 공간을 공유할 수 있다. 사설 엔터프라이즈 네트워크(101) 내의 모든 장치는 동일한 보안 경계(security boundary) 뒤에 위치될 수 있어서, 네트워크 보안이 보안 경계 내측의 장치를 경계 외측의 장치로부터 격리시킬 수 있으며, 보안 가장자리(security border)에서의 많지 않은 허용된 통신을 제어할 수 있다. 이는 고객 에지 장치(110a 내지 110f)와 같은 장치가 보안 경계를 가로지르는 것에 연관된 예방 조치를 구현할 필요 없이 트래픽을 자유롭게 통과시키게 한다.

[0019] 서비스 제공자 네트워크(102)는 사설 엔터프라이즈 네트워크(101)에 대한 호스트로서 작용할 수 있다. 서비스 제공자 네트워크(102)는 일련의 제공자 에지(PE) 장치(111a 내지 111h)를 포함할 수 있다. 서비스 제공자 네트워크(102)는 사설 엔터프라이즈 네트워크(101)를 클라우드 네트워크(103), 다른 사설 엔터프라이즈 네트워크, 또는 무엇보다도 인터넷과 같은 다른 네트워크로 접속시킬 수 있다. 일부 실시예에서, 서비스 제공자 네트워크(102)는 사설 엔터프라이즈 네트워크(101)의 이질적인 부분을 접속시킬 수 있지만, 이들 이질적인 부분은 동일한 어드레스 공간을 공유할 수 있다.

[0020] 클라우드 네트워크(103)는 하나 이상의 서버(114a 내지 114d)를 포함할 수 있으며, 하나 이상의 서버(114a 내지 114d)는 클라우드 서비스 제공자에 의해 소유될 수 있고 인터넷을 통해 네트워크 내에 접속될 수 있다. 하부구조 서비스 모델(infrastructure service model)에서, 예를 들어 클라우드 서비스 제공자는 클라우드 네트워크(103) 내에 위치된 특정 자원을 그 클라우드 네트워크(103)의 고객에 할당할 수 있다. 이러한 특정 자원은 가상 머신(116a 내지 116d)으로서 그룹핑(grouping)될 수 있다.

[0021] 가상 머신(116a)은 사설 엔터프라이즈 네트워크(101) 내에 위치된 고객에 의해 제어되는 클라우드 네트워크(103) 내의 서버(114a) 상의 서버 인스턴스(server instance)일 수 있다. 고객은 임의의 개수의 가상 머신(116a 내지 116d)을 마음대로 생성하고, 사용하며, 제거하는 능력을 가질 수 있다. 이러한 능력은 예를 들어 대역폭, 저장 용량, 및 처리 필요성과 같은 사용자 정의 기준에 기반할 수 있다.

[0022] 고객에 할당된 가상 머신(116a 내지 116d)은 클라우드 내측에서 서로 논리적으로 접속될 수 있다. 다양한 실시예에서, 고객에 할당된 모든 가상 머신(116a 내지 116d)은 동일한 VLAN 내에 나타난다. 가상 머신(116a 내지 116d)은 동일한 서버(114a) 상에 또는 상이한 서버(114a 내지 114d) 상에 물리적으로 위치될 수 있지만, VLAN 내에서 서로 논리적 접속을 유지한다. 일부 실시예에서, 가상 머신(116a)은 클라우드 네트워크 내의 상이한 서버(114a)와 같은 상이한 물리적 위치로 이동할 수 있으며, 여전히 동일한 VLAN에 연관될 수 있다.

[0023] 가상 스터브(virtual stub, vstub)(104)는 특정 고객에 할당된 클라우드 네트워크(103) 내의 모든 자원을 포함하는 논리적 네트워크일 수 있다. 따라서, 가상 스터브(104)는 고객에 할당된 클라우드 네트워크(103) 내의 모든 활성 가상 머신(116a 내지 116d), 할당된 가상 머신(116a 내지 116d)을 호스트하고 제어할 수 있는 일련의 하이퍼바이저(115a 내지 115d), 할당된 가상 머신(116a 내지 116d)을 포함하는 각각의 서버(114a 내지 114d)에 물리적으로 접속될 수 있는 데이터 센터 상호접속부(113), 및 클라우드 네트워크(103) 내의 모든 할당된 가상 머신(116a 내지 116d)에 대한 허브로서 작용할 수 있는 클라우드 데이터 센터 CE(Cloud Data Center CE)(112)를 포함할 수 있다. 도 1에 도시된 바와 같이, 가상 스터브(104)는 사설 엔터프라이즈 네트워크(101) 내의 장치에 의해 사용된 VLAN 내에 포함될 수 있고, 물리적으로 근접하는 그의 논리적 네트워크를 필요로 하지 않으며, 데이터 센터 상호접속부(113)와 같은 상이한 물리적 서버(114a 내지 114d)를 접속시키는 네트워킹 구성요소를 포함할 수 있다. 가상 스터브는 사설 엔터프라이즈 네트워크(101)에 할당된 서버(114a 내지 114d)를 클라우드 네트워크(103) 내에 존재하지만 사설 엔터프라이즈 네트워크에 할당되지 않은 일련의 서버(119a, 119b)로부터 분리시킬 수 있다. 그러므로, 일련의 서버(119a, 119b)는 사설 엔터프라이즈 네트워크(101)로 접속하지 않을 수 있거나 동일한 어드레스 공간 또는 VLAN을 공유하지 않을 수 있다.

[0024] 고객 에지(customer edge, CE) 장치(110a)는 사설 엔터프라이즈 네트워크(101) 내의 노드일 수 있다. CE 장치(110a)는 사설 엔터프라이즈 네트워크(101) 내의 다른 고객 에지 라우터, 서비스 제공자 네트워크(102) 내의 제공자 에지 장치(111a 내지 111h), 또는 클라우드 네트워크(103) 내의 클라우드 데이터 센터 CE(112)와 같은 다른 노드로 패킷을 송신하도록 구성된, 라우터 또는 스위치와 같은 네트워크 노드일 수 있다. CE 장치(110a)는

예를 들어 MPLS를 사용하는 레이어 3 통신(L3 MPLS) 및 이더넷(Ethernet) 및 가상 사설 LAN 서비스(Virtual Private LAN Service, VPLS)를 사용하는 레이어 2 통신과 같은 복수의 레이어(layer)의 OSI 참조 모델(OSI reference model)을 사용하여 사설 엔터프라이즈 네트워크(101) 내측 및 외측에서 다른 장치와 통신할 수 있다. 일부 실시예에서, CE 장치(110a)는 물리적 장치를 거주시키는 가상 라우터일 수 있다.

[0025] 각각의 제공자 에지 장치(111a 내지 111h)는 서비스 제공자 네트워크(102) 내의 노드일 수 있으며, 라우터, 스위치 또는 유사한 하드웨어 장치일 수 있다. 제공자 에지 장치(111a 내지 111h)는 CE 장치(110a)로부터 패킷을 수신하고 서비스 제공자 네트워크(102)를 거쳐 이러한 패킷을 송신하도록 구성될 수 있다. 이들 패킷은 사설 엔터프라이즈 네트워크(101) 내의 다른 목적지로, 클라우드 네트워크(103) 내의 목적지로, 또는 도 1에 도시되지 않은 다른 네트워크 내의 목적지로 송신될 수 있다.

[0026] 클라우드 데이터 센터 CE(112)는 고객 에지 라우터일 수 있으며, 클라우드 서비스 제공자의 고객에 의해 동작되는 설비에 의해 구현될 수 있다. 비록 "고객" 에지 장치로 지칭되지만, 클라우드 데이터 센터 CE(112)는 당연히 클라우드 서비스 제공자 또는 일부 다른 엔티티에 의해 소유되고/되거나 동작될 수 있다는 것이 당연하다. 일부 실시예에서, 클라우드 데이터 센터 CE(112)는 클라우드 네트워크(103) 내측의 가상 스터브(104)에 대한 허브를 표시한다. 일부 실시예에서, 클라우드 데이터 센터 CE(112)는 복수의 엔터프라이즈 네트워크에 의해 공유될 수 있다.

[0027] 일부 실시예에서, 클라우드 네트워크(103)는 또한 클라우드 데이터 센터 CE(112)에 연관된 디렉토리 서버(directory server)를 포함할 수 있다. 디렉토리 서버는 매핑 엔트리(mapping entry)의 디렉토리를 유지할 수 있다. 보다 상세하게 후술되는 바와 같이, 이들 매핑 엔트리는 엔터프라이즈 네트워크 내의 위치 기업 IP를 기업 확장식 네트워크(100) 내의 목적지의 어드레스에 상관시킬 수 있다. 이는 위치의 MAC 어드레스, 클라우드 IP 어드레스(cloudIP), 및 위치 IP 어드레스(locIP)에 대한 엔트리를 포함할 수 있다.

[0028] MAC 어드레스는 네트워크 어댑터 또는 네트워크 인터페이스 카드(network interface card, NIC)와 같은 네트워크 내의 장치에 할당된 고유한 식별자(identifier)일 수 있다. MAC 어드레스는 장치의 제조자에 의해 제공될 수 있다. MAC 어드레스는 인터넷 프로토콜 버전 4(Internet Protocol Version 4, IPv4)에 대한 어드레스 해결 프로토콜(Address Resolution Protocol, ARP), 또는 인터넷 프로토콜 버전 6(Internet Protocol Version 6, IPv6)에 대한 이웃 탐색 프로토콜(Neighbor Discovery Protocol, NDP)을 사용하여 IP 어드레스와 함께 질의에 기반하여 결정될 수 있다. MAC 헤더는 또한 소스 및 목적지 VLAN의 VLAN 태그를 포함할 수 있다. 일부 실시예에서, VLAN 태그가 목적지의 VLAN에 상응하지 않으면, 목적지는 패킷을 드롭(drop)시킨다. 위치 IP 어드레스(locIP)는 가상 스터브(104) 내의 특정 스위치, 예를 들어 스위치(117a)의 위치를 식별할 수 있다. 가상 머신(116a)은 가상 머신(116a)가 놓여지는 IP 스위치(117a)를 지칭하는 locIP 어드레스를 가질 수 있다. 또한, 클라우드 IP 어드레스(cloudIP)는 명백하게 가상 스터브(104) 내의 각각의 가상 머신(116a 내지 116d)을 지칭할 수 있다.

[0029] 그러므로, 할당된 IP 어드레스 대신에 장치가 장치의 locIP 및 cloudIP 어드레스에 의해 가상 머신을 위치시키는 디렉토리 서버를 지칭할 수 있으므로, 가상 머신(116a)은 그 위치로부터 논리적으로 분리된 별개의 어드레스를 소유할 수 있다. 일 실시예에서, 사설 엔터프라이즈 네트워크(101) 내의 소스는 클라우드 네트워크(103) 내의 가상 머신(116a)으로 패킷 형태로 정보를 발송하기 위해 엔터프라이즈 네트워크 내의 할당된 IP 어드레스를 사용할 수 있다. 이 경우에, 클라우드 데이터 센터 CE(112)는 IP 헤더가 내장된 이더넷 프레임(Ethernet frame)을 사용하여 어드레스된 이러한 패킷을 수신할 수 있으며, 클라우드 네트워크(103) 내의 목적지 가상 머신(116a)에 상응하는 cloudIP 어드레스 헤더 및 locIP 어드레스 헤더를 이용하여 목적지 가상 머신(116a)으로 발송된 수신된 패킷을 캡슐화할 수 있다. 클라우드 데이터 센터 CE(112)는 디렉토리 서버 상에 위치된 디렉토리를 통해 기업 ID를 가상 머신(116a)의 locIP 및 cloudIP 어드레스에 상관시킬 수 있다.

[0030] 보다 상세하게 후술되는 바와 같이, 디렉토리 서버 내의 디렉토리는 사설 엔터프라이즈 네트워크(101) 및 클라우드 네트워크(103) 내의 활성 서버 및 가상 머신에 대한 어드레스 엔트리를 포함할 수 있다. 하나의 네트워크로부터 나머지 네트워크로 발송된 패킷은 클라우드 데이터 센터 CE(112)를 통과할 수 있으며, 클라우드 데이터 센터 CE(112)는 수신된 패킷의 헤더를 나머지 네트워크 내의 필수 헤더에 상관시키기 위해 디렉토리를 사용할 수 있다. 예를 들어, 클라우드 데이터 센터 CE(112)는 MAC, cloudIP, 및 locIP 어드레스 헤더를 색인하여 클라우드 네트워크 내의 패킷을 적절히 발송하기 위해 디렉토리를 사용할 수 있다. 클라우드 데이터 센터 CE(112)는 또한 클라우드 네트워크(103) 내에 유래하는 cloudIP 및 locIP 어드레스 헤더를 캡슐화 해제하고 MAC 어드레스 헤더를 제 2 MAC 어드레스 헤더로 대체하여 서비스 제공자 네트워크(102) 및 사설 엔터프라이즈 네트워크

(101) 내의 패킷을 발송하기 위해 디렉토리를 사용할 수 있다.

[0031] 오직 하나의 논리적 CE(112)가 도시되었지만, 대안적인 실시예는 클라우드 네트워크 또는 클라우드 데이터 센터 내에 복수의 논리적 CE를 포함할 수 있다. 이러한 실시예에서, 기업 어드레스 공간 내의 가상 머신(116a 내지 116d)은 각각의 논리적 CE를 이용하여 분리된 VLAN에 대한 독립적인 허브로서 작용하는 상태에서 클라우드 데이터 센터 내의 상이한 논리적 CE에 할당될 수 있다. 이러한 실시예는 또한 전술된 바와 같이 디렉토리 색인(directory lookup)이 하이퍼바이저(115a 내지 115d) 대신에 각각의 논리적 CE(112)에 의해 수행되게 할 수 있다. 대신에 데이터 패킷이 적절한 허브 논리적 CE(112)로 터널링될 수 있으므로, 복수의 논리적 CE 장치(112)는 또한 locIP 및 cloudIP 헤더가 가상 스터브(104) 내의 목적지를 클라우딩하는 필요성을 제거할 수 있다.

[0032] 데이터 센터 상호접속부(113)는 일련의 서버(114a 내지 114d)로 접속하는 스위치 또는 일련의 스위치일 수 있다. 데이터 센터 상호접속부(113)는 클라우드 데이터 센터 CE(112)를 할당된 일련의 서버(114a 내지 114d)로 직접 접속시킬 수 있다. 대안적으로, 데이터 센터 상호접속부(113)는 일련의 중간 스위치(117a 내지 117c)를 통해 일련의 서버(114a 내지 114d)로 접속시킬 수 있다. 이러한 경우에, 각각의 중간 스위치(117a 내지 117c)는 복수의 서버(114a 내지 114d)로 동시에 접속시킬 수 있다. 중간 스위치(117a)는 가상 스터브(104) 내의 고유한 위치 IP(locIP) 어드레스를 가질 수 있다. 그의 접속된 서버(114a) 중 하나의 서버 상의 가상 머신(116a)으로 어드레스된 패킷을 수신할 때, 중간 스위치(117a)는 패킷으로부터 locIP 헤더를 캡슐화 해제할 수 있으며, 그런 다음 상응하는 cloudIP 어드레스를 이용하여 서버(114a)로 패킷을 전달할 수 있다.

[0033] 서버(114a)는 클라이언트로 컴퓨팅 서비스로 제공하는 장치일 수 있다. 보다 구체적으로, 서버는 클라이언트가 예를 들어 애플리케이션을 실행하거나 파일을 메모리 내로 저장하기 위해 사용하는, 저장 및 처리 용량과 같은 컴퓨팅 자원을 호스트하는 네트워킹 장치일 수 있다. 따라서, 서버(114a 내지 114d)는 예를 들어 복수의 슬롯을 포함하는 샤시 기반 서버(chassis-based server)(즉, 블레이드 서버(blade server))일 수 있으며, 각각의 슬롯은 물리적 서버 블레이드를 유지할 수 있다. 각각의 물리적 서버(114a 내지 114d)는 하이퍼바이저(115a 내지 115d) 및 적어도 하나의 가상 머신(116a 내지 116d)을 포함할 수 있다.

[0034] 하나 이상의 하이퍼바이저(115a 내지 115d)는 각각의 물리적 서버(114a 내지 114d) 상에 위치될 수 있다. 일 실시예에서, 하이퍼바이저(115a 내지 115d)는 그들이 거주하는 물리적 서버 상에 물리적으로 위치된 각각의 할당된 가상 머신(116a 내지 116d)을 호스트한다. 그에 의해 각각의 하이퍼바이저(115a 내지 115d)는 하나 이상의 가상 머신(116a 내지 116d)을 동시에 제어할 수 있다.

[0035] 하이퍼바이저(115a 내지 115d)는 기업 정보를 인지할 수 있으며, 기업 정보는 예를 들어 그것이 호스트하는 각각의 가상 머신의 cloudIP 어드레스 및 하이퍼바이저(115a 내지 115d)를 호스트하는 중간 스위치(117a 내지 117c)의 locIP 어드레스를 포함할 수 있다. 그러므로, 하이퍼바이저(115a 내지 115d)는 그것의 호스트되는 가상 머신(116a 내지 116d)의 기업 멤버쉽(즉, 기업 ID)을 인식할 수 있다. 하이퍼바이저(115a 내지 115d)는 또한 그것의 호스트되는 가상 머신(116a 내지 116d)에 관련된 트래픽을 차단할 수 있다. 가상 머신(116a 내지 116d)이 가상 스터브(104) 외측의 목적지로 패킷을 발송할 때, 하이퍼바이저(115a 내지 115d)는 클라우드 데이터 센터 CE(112)에 연관된 MAC 어드레스 헤더, cloudIP 헤더, 및 locIP 헤더를 이용하여 그것의 호스트되는 가상 머신(116a 내지 116d) 중 하나의 가상 머신으로부터 발송된 패킷을 캡슐화할 수 있다. 하이퍼바이저(115a 내지 115d)는 또한 하이퍼바이저(115a 내지 115d)에 의해 호스트되는 가상 머신(116a 내지 116d)으로 발송된 패킷의 cloudIP 헤더를 캡슐화 해제할 수 있다.

[0036] 일부 실시예에서, 하이퍼바이저(115a 내지 115d)는 그것이 호스트하는 각각의 가상 머신(116a 내지 116d)에 대한 보안 매개변수를 인식한다. 이들 보안 매개변수는 가상 스터브(104)가 크기를 바꿀 때 임의의 의도하지 않은 정보 누설을 방지하기 위해 예를 들어 내장된 고객 ID를 포함할 수 있다. 하이퍼바이저(115a 내지 115d)는 후술되는 바와 같이 보안 토큰(또는 쌍을 이루는 보안 토큰)과 같은 다른 보안 특징을 인식할 수 있으며, 이는 악의적인 하이퍼바이저와 같은 엔티티에 의한 의도적인 공격 및 다른 텔넷 공격을 방지할 수 있다. 하이퍼바이저(115a 내지 115d)는 또한 패킷이 동일한 VLAN으로부터 유래하는 것을 보장하기 위해 MAC 어드레스 헤더 내의 VLAN 태그를 점검할 수 있다.

[0037] 도 2는 L2 프로토콜을 사용하는 이중 캡슐화된 패킷 전송의 개략적인 다이어그램이다. 도 2에 도시된 바와 같이, 각각의 종점에서 장치는 IP 어드레스를 사용하여 목적지를 어드레스할 수 있으며, 각각의 IP 어드레스는 기업의 IP 어드레스 공간 내측에 존재한다. 클라우드 네트워크(103) 내의 가상 스터브(104)는 사설 엔터프라이즈 네트워크(101)와 공통 VLAN을 공유할 수 있다. 따라서, 가상 스터브(104) 내측의 각각의 가상 머신(116a 내지 116d)은 또한 IP 서브넷 내의 상응하는 어드레스에 할당된다.

[0038] 클라우드 네트워크(103)의 특성이 가상 머신(116a 내지 116d)의 위치를 결정하기 위해 클라우드 네트워크(103) 내측의 특정 정적 IP 어드레스를 사용하지 못하게 할 수 있다는 것이 당연하다. 예를 들어, 가상 머신(116a)은 상이한 물리적 서버(114d)로 동적으로 이동할 수 있으며, 이는 임의의 주어진 시간에 특정 가상 머신(116a)을 어드레스할 때 사용하는 적절한 IP 어드레스를 결정하는 것을 어렵게 한다. 그러므로, 클라우드 네트워크(103) 내에서 가상 머신(116a)은 동일한 VLAN 내에 머무르고 그것의 기업 ID, 위치 IP 어드레스, 및 클라우드 IP 어드레스에 의해 식별된다. 이러한 어드레싱 정보는 디렉토리 서버 내의 디렉토리 내에 저장될 수 있다.

[0039] 따라서, 클라우드 네트워크(103) 내의 목적지로의 패킷의 송신은 패킷을 이중 캡슐화하는 것을 포함할 수 있으며, 그것은 또한 MAC 어드레스 헤더를 추가하는 것에 추가하여 내부 클라우드 IP 헤더 및 외부 위치 IP 헤더를 이용하여 각각의 패킷을 캡슐화하는 것을 포함할 수 있다. 예를 들어 클라우드 네트워크(103) 내의 가상 머신(116a)으로부터 사설 엔터프라이즈 네트워크(101) 내의 목적지로 패킷이 발송되고 있으면, 패킷을 캡슐화하는 제 1 MAC 어드레스 헤더, cloudIP, 및 locIP 헤더는 클라우드 데이터 센터 CE(112)에 대한 어드레스에 상응한다. 클라우드 데이터 센터 CE(112)는 가상 스터브(104)에 대한 허브로서 작용하며, 별개인 MAC 어드레스 및 클라우드 IP 어드레스를 포함한다. 클라우드 데이터 센터 CE(112)는 예를 들어 사설 엔터프라이즈 네트워크(101) 내의 목적지에 상응하는 제 2 MAC 어드레스를 사용하여 사설 엔터프라이즈 네트워크(101) 내측의 적절한 IP 어드레스로 패킷을 전달한다.

[0040] 도 2에 도시된 예에서, IP 어드레스 10.1.2.2에서의 사설 엔터프라이즈 네트워크(101) 내의 소스(201)(위치 "A")는 클라우드 네트워크(103) 내의 IP 어드레스 10.1.8.8에서의 목적지 가상 머신(116a)(위치 "B")으로 패킷(203)을 발송한다. IP 어드레스 및 페이로드(payload)의 이러한 조합은 도시된 실시예 내의 IP 패킷으로 간주될 수 있다.

[0041] 도시된 예에서, 소스 "A"(201)는 먼저 레이어 2 네트워크를 통해 목적지 "B"(116a)의 MAC 어드레스를 획득하도록 시도할 수 있다. 그러므로, 소스 "A"(201)는 ARP 요청을 생성할 수 있으며, ARP 요청은 고객 에지 라우터 CE_A(110a)에 도달할 수 있다. CE_A(110a)가 그의 VRF 표를 통해 목적지 "B"(116a)에 대한 IP 대 MAC 어드레스 매핑을 알고 있지 않으면, CE_A(110a)는 서비스 제공자 네트워크(102) 내에 위치될 수 있는 접속된 제공자 에지 라우터(PE)(111a)로 ARP 요청을 브로드캐스트할 수 있다. PE(111a)는 결국 사설 네트워크(102) 내의 모든 다른 제공자 에지 라우터(111a 내지 111f)로 ARP 요청을 브로드캐스트할 수 있다. 이는 ARP 요청을 수신하는 클라우드 네트워크(103) 내의 클라우드 데이터 센터 CE(112)로 이어질 수 있다. 클라우드 데이터 센터 CE(112)가 ARP 요청을 수신할 때, 클라우드 데이터 센터 CE(112)는 목적지 "B"(116a)의 MAC 어드레스를 획득하기 위해 디렉토리 서버에게 질의할 수 있다. 일단 획득되면, MAC 어드레스는 반대 경로를 통해 소스 "A"(201)로 반송될 수 있다.

[0042] 획득된 MAC 어드레스를 사용하여 소스 "A"(201)는 그의 레이어 2 네트워크를 통해 패킷(205)을 발송할 것이다. 패킷(205)은 수정된 MAC 어드레스와 함께 IP 패킷(203)을 포함한다. 이러한 MAC 어드레스는 또한 소스의 VLAN을 표시하는 VLAN 태그를 포함할 수 있다. 도시된 실시예에서, 목적지 "B"(116a)는 클라우드 네트워크(103) 내에 있으며, 따라서 패킷이 클라우드 데이터 센터 CE(112)로 터널링될 수 있다. 클라우드 데이터 센터 CE(112)는 디렉토리 서버에게 목적지 "B"(116a)에 대한 클라우드 IP 어드레스 및 위치 IP 어드레스에 대해 질의한다. 그 뒤에, 클라우드 데이터 센터 CE(112)는 처음에는 클라우드 IP 어드레스 헤더를 이용하여 그런 다음 locIP 어드레스 헤더를 이용하여 패킷(205)을 캡슐화한다. 그런 다음, 클라우드 데이터 센터 CE(112)는 클라우드 네트워크(103) 내의 데이터 센터 상호접속부(113) 및 다른 장치를 통해 상응하는 목적지 locIP 어드레스를 갖는 중간 스위치(117a)로 이중 캡슐화된 패킷(206)을 발송할 수 있다.

[0043] 그런 다음, 중간 스위치(117a)는 패킷(206)으로부터 locIP 헤더를 캡슐화 해제할 수 있으며, 상응하는 목적지 cloudIP 어드레스로 수정된 패킷(209)을 송신할 수 있다. 목적지 cloudIP 어드레스에 상응하는 서버(114a)에서, 서버(114a) 상의 하이퍼바이저(115a)는 수정된 패킷(209)으로부터 MAC 어드레스 헤더 및 cloudIP 헤더를 캡슐화 해제하며, 서버(114a) 상의 목적지 가상 머신 "B"(116a)로 IP 패킷(210)을 송신한다. 일부 실시예에서, 하이퍼바이저(115a)는 또한 패킷이 동일한 엔터프라이즈 네트워크로부터 유래한다는 것을 확인하기 위해 패킷(210) 내의 보안 토큰을 확인할 수 있다. 일부 실시예에서, 하이퍼바이저(115a)는 목적지 "B"(116a)가 VLAN에 속하는지 여부를 확인하기 위해 MAC 어드레스 헤더 내의 VLAN 태그를 점검할 수 있다. 목적지 "B"(116a)가 VLAN에 속하지 않을 때, 하이퍼바이저(115a)는 수정된 패킷(209)을 드롭시킬 수 있다.

[0044] 도 3은 etherIP 및 VLAN 변환을 사용하는 패킷 전송의 개략적인 다이어그램이다. 도시된 실시예는 도 2의 도시된 실시예와 동일한 시스템 구성요소를 공유할 수 있다. 도 2에서와 같이, IP 어드레스 10.1.2.2에서의 사설

엔터프라이즈 네트워크(101) 내의 소스 "A"(201)는 클라우드 네트워크(103) 내의 어드레스 10.1.8.8에서의 목적지 가상 머신 "B"(116a)로 패킷(203)을 발송한다. 소스 "A"(201)는 목적지의 적절한 MAC 어드레스에 대해 질의하며, 클라우드 데이터 센터 CE(112)로 수정된 패킷(205)을 발송한다.

[0045] 일부 실시예에서, 클라우드 데이터 센터 CE(112)는 VLAN을 국부적으로 고유한 것으로 변환할 수 있다. 도시된 실시예에서, 클라우드 데이터 센터 CE(112)는 소스 VLAN 6을 국부적으로 고유한 VLAN 10으로 변환한다. 이러한 실시예에서, 각각의 장치는 스위치에 국부적인 MAC 어드레스에 할당되며, 이는 각각의 MAC 어드레스가 일단 클라우드 네트워크(103) 내의 중간 스위치(117a)에 도달할 때 고유하게 한다. 따라서, 클라우드 데이터 센터 CE(112)는 수정된 패킷(205)을 수신할 때 오직 하나의 IP 헤더를 이용하여 패킷을 캡슐화한다. 클라우드 데이터 센터는 중간 스위치(117a)의 locIP 헤더를 이용하여 패킷(205)을 캡슐화한다. 클라우드 데이터 센터 CE(112)는 데이터 센터 상호접속부(113)를 통해 스위치(117a)로 단일 캡슐화된 패킷(306)을 전달한다. 스위치(117a)는 단일 캡슐화된 패킷(306)을 캡슐화 해제한다. 이 실시예에서 MAC 어드레스가 국부적으로 고유하므로, 스위치는 목적지 "B"(116a)로 수정된 패킷(309)을 전달할 수 있으며, 따라서 각각의 VM(116a 내지 116d)에 대한 고유한 cloudIP 어드레스는 필요하지 않다.

[0046] 도 4는 논리적 CE 라우터(112)의 예시적인 가상 라우팅 및 전달(Virtual Routing and Forwarding, VRF) 표(400)이다. 사설 엔터프라이즈 네트워크(101) 내의 고객 에지(CE) 장치(110a 내지110e) 및 서비스 제공자 네트워크(102) 내의 제공자 에지 장치(111a 내지 111h)와 같은 다른 장치는 또한 유사한 VRF 표(400)를 유지할 수 있다.

[0047] entIP 필드(401)는 하나의 위치의 기업 ID(Enterprise ID)에 상응할 수 있다. 예시적인 실시예에서, 가상 스터브(104) 내의 자원은 동일한 VLAN을 공유하며, 결과적으로 동일한 어드레스 공간을 공유할 수 있다. 도시된 실시예에서, 각각의 entIP는 국부적으로 고유한 IP 어드레스이다. MAC 필드(402)는 하나의 위치의 MAC 어드레스에 상응할 수 있다. MAC 필드는 사설 엔터프라이즈 네트워크(101) 내의 장치의 위치를 식별하기 위해 레이어 2 프로토콜에 의해 사용될 수 있으며, 클라우드 네트워크(103) 내의 장치를 식별하기 위해 locIP 필드(403) 및 cloudIP 필드(404)와 함께 사용될 수 있다.

[0048] locIP 필드(403)는 클라우드 네트워크(103) 내의 장치의 위치 IP 어드레스에 상응한다. locIP는 엔트리의 가상 머신(116a)을 호스트하는 클라우드 네트워크(103) 내의 중간 스위치(117a)의 어드레스에 상응할 수 있다. 도 4의 도시된 실시예에서, 가상 머신 엔트리(411)는 상응하는 가상 머신(116a)을 호스트하는 중간 스위치(117a)에 상응하는 20.2.2.8인 위치 IP 어드레스를 갖는다.

[0049] cloudIP 필드(404)는 클라우드 네트워크(103) 내의 가상 머신(116a)의 cloudIP 어드레스에 상응할 수 있다. locIP 필드(403)에서 중간 스위치(117a)는 중간 스위치(117a)가 호스트하는 각각의 가상 머신(116a)에 대해 별개인 중첩하지 않는 cloudIP 어드레스(404)를 갖는다. 클라우드 데이터 센터는 클라우드 네트워크(103) 내의 가상 머신(116a 내지 116d) 사이에 cloudIP를 할당할 수 있다. 도시된 실시예에서, 가상 머신 엔트리(411)는 20.2.2.1인 cloudIP 어드레스를 가지며, 따라서 중간 스위치(117a)가 가상 머신(116a)에 대한 패킷을 수신할 때 스위치는 하이퍼바이저(115a)를 통해 특정 가상 머신 20.2.2.1로 패킷을 전달할 수 있다.

[0050] nextHop 필드(405)는 장치가 패킷을 발송해야 하는 엔터프라이즈 네트워크(100) 내의 다음 위치를 지칭한다. 도시된 실시예에서, 엔트리(413)는 사설 엔터프라이즈 네트워크(101) 내의 하나의 위치에 상응하는 49-BD-D2-C7-56-2A인 MAC 어드레스와 함께 entIP 어드레스(401)를 갖는다. 따라서, 그러한 위치는 적용 가능한 locIP(403) 또는 cloudIP(404) 어드레스를 갖지 않는데, 왜냐하면 그들은 오직 클라우드 네트워크(103) 내의 어드레스에 의해 사용될 수 있기 때문이다. 그러므로, 클라우드 데이터 센터 CE(112)로부터의 상응하는 nextHop(405) 엔트리는 접속된 제공자 에지 장치(111a)를 위한 것이며, 이는 MAC 어드레스 49-BD-D2-C7-56-2A를 갖는 목적지에 대한 패킷의 수신 시에 그 자신의 VRF 표를 지칭할 것이며, 엔트리의 상응하는 nextHop(405) 어드레스로 그것을 전달할 것이다. 패킷이 결국 사설 엔터프라이즈 네트워크(101) 내의 MAC 어드레스 49-BD-D2-C7-56-2A를 갖는 목적지에 도달할 때까지 이러한 프로세스는 각각의 장치 상에서 순차적으로 계속될 것이다.

[0051] 도 5는 디렉토리 서버 내에서의 예시적인 디렉토리 표이다. 디렉토리 표(500)가 nextHop 필드(405)를 유지하지 않는다는 것을 제외하면, 디렉토리 표(500)는 entIP 필드, MAC 필드, locIP 필드, 및 cloudIP 필드를 유지하는 클라우드 데이터 센터 VRF 표(400)와 유사하다. 이는 디렉토리 표(500)가 전달 정보를 유지하지 않고 대신에 디렉토리 표(500)가 단순히 사설 엔터프라이즈 네트워크(101) 및 클라우드 네트워크(103) 내의 위치에 대한 MAC(402), locIP(403), 및 cloudIP(404) 어드레스의 포괄적인 리스트를 유지하기 때문이다.

[0052] 도시된 실시예에서, "디폴트" 엔트리(511)는 5C-66-AB-90-75-B1인 MAC 어드레스를 가지며, 그것의 locIP(403) 어드레스로서 오직 IP_{CA}를 가지고, 적용 가능한 cloudIP(404) 어드레스를 갖지 않는다. 디폴트 엔트리(511)는 명시적인 locIP(403) 또는 cloudIP(404) 어드레스를 갖지 않는 사설 엔터프라이즈 네트워크(101) 내의 장치를 지칭한다. IP_{CA} 엔트리는, 디렉토리(500) 내에 유효 locIP(403) 및 cloudIP(404) 어드레스를 갖는 엔트리(412)로서 구체적으로 리스트되지 않은 목적지를 갖는 패킷이 클라우드 데이터 센터 CE(112) 쪽으로 지향되어야 하며, 그런 다음 클라우드 데이터 센터 CE(112)는 사설 엔터프라이즈 네트워크(101) 내의 적절한 목적지로 패킷을 전달하기 위해 그것의 VRF 표(400)를 사용할 것이라는 것을 의미한다.

[0053] 예시적인 실시예에서, 가상 머신(116a)은 정지될 수 있다. 가상 머신이 정지될 때, 디렉토리에서 디렉토리(500) 내의 VM의 엔트리가 삭제될 수 있다. 또다른 예시적인 실시예에서, VM은 예를 들어 114a로부터 114c로 상이한 서버로 이동할 수 있다. VM이 또다른 서버(114c)로 이동할 때, 그것의 locIP 어드레스는 가상 머신(116a)이 현재 위치되는 새로운 서버(114c)를 반영하기 위해 디렉토리(500) 내에서 갱신될 것이다. 가상 머신(116a)은 또한 새로운 VLAN 또는 클라우드 데이터 센터 CE(112)로 이동할 수 있다. 오래된 엔트리(시기가 지난 VRF 표를 갖는 장치)의 경우에, 이전 locIP 어드레스에서의 스위치(117a)는 새로운 클라우드 데이터 센터 CE에서의 디렉토리 서버로 잘못 어드레스된 패킷을 전달할 것이다. 그런 다음, 오래된 클라우드 데이터 센터 CE(112)에서의 디렉토리 서버는 유니캐스트(unicast)를 통해 오래된 스위치의 VRF 표를 정정할 것이다.

[0054] 도 6은 시스템 내에서 사용된 이더넷 프레임의 예시적인 도면이다. 이더넷 프레임(600)은 길이가 변할 수 있는 IP 데이터그램을 갖는다. 도 6은 데이터그램(610)을 포함하는 이중 캡슐화된 패킷의 예시적인 이더넷 프레임을 도시한다. 데이터그램(610)은 다른 정보 중에서 내부 cloudIP 헤더 및 외부 locIP 헤더, 목적지 cloudIP 어드레스(603), 및 페이로드(601)를 포함한다. 소스 어드레스(605) 및 목적지 어드레스(606)는 또한 이더넷 프레임(600) 내에 포함된다.

[0055] 데이터그램(610)은 또한 보안 토큰(602)을 포함할 수 있다. 보안 토큰은 예를 들어 기업 고유의 키, 기업 ID, 및 목적지 IP 어드레스의 조합을 포함할 수 있다. 하이퍼바이저(115a)는 보안 토큰(602)을 확인하도록 시도할 수 있으며, 패킷이 잘못된 보안 토큰(602)을 포함하면 패킷을 드롭시킬 수 있다. 일 실시예에서, 패킷은 쌍을 이루는 보안 토큰(602)에 의해 부호화될 수 있다. 쌍을 이루는 보안 토큰은 쌍을 이루는 키로부터 유도될 수 있으며, 쌍을 이루는 키는 오직 하나의 사용자에 대해 사용되는 개별 키이다. 이는 악의적인 하이퍼바이저(115a)에 보안 연관성을 갖는 가상 머신(116a 내지 116d)으로 공격을 국한시킴으로써 악의적인 하이퍼바이저(115a)로부터의 공격을 방지하는 것을 도울 수 있다.

[0056] 또한, 데이터그램(610)은 보안 이유 때문에 고객 ID(604)를 포함할 수 있는데, 왜냐하면 고객 ID(604)가 가상 스터브(104) 내가 아닌 가상 머신(116a 내지 116d)으로 패킷을 발송하는 것을 방지하기 때문이다. 이러한 상황은 예를 들어 가상 머신(116a 내지 116d)이 이동하거나 정지되고 장치가 그러한 가상 머신(116)으로 트래픽을 계속하여 발송하면 발생할 수 있다. 일 실시예에서, 페이로드(601)는 공유된 그룹 키를 이용하여 암호화될 수 있다. 공유된 그룹 키는 주어진 고객 그룹의 구성원 사이에서 공유될 수 있다.

[0057] 도 7은 이중 캡슐화 및 레이어 2 프로토콜을 사용하여 사설 엔터프라이즈 네트워크(101) 내의 소스 "A"(201)로부터 클라우드 네트워크(103) 내의 목적지 "B"(116a)로 패킷(203)을 발송하는 방법(700)의 예시적인 실시예의 흐름도이다. 단계 701에서, 소스 "A"(201)는 사설 엔터프라이즈 네트워크(101) 내의 고객 에지 라우터(110a)에게 목적지 "B"(116a)의 MAC 어드레스에 대해 질의한다. 단계 702에서, 고객 에지 라우터(110a)는 그의 VRF 표에게 소스 "A"(201)의 IP 대 MAC 매핑(IP-to-MAC mapping)에 대해 질의한다. 단계 703에서, 고객 에지 라우터(110a)에 대한 매핑이 VRF 표 내에 존재하지 않으면, 고객 에지 라우터(110a)는 시스템을 통해 ARP 요청의 형태로 질의를 브로드캐스트한다. 단계 704에서, IP 대 MAC 어드레스 매핑이 장치의 VRF 표 내에 존재할 때, 고객 에지 라우터(110a)는 목적지 "B"(116a)의 MAC 어드레스를 반환한다.

[0058] 단계 702 내지 단계 704의 루프는 각각의 장치가 MAC 어드레스를 반환할 때까지 각각의 전달 장치에 대해 반복된다. 이는 각각의 장치가 클라우드 데이터 센터 CE(112)에 도달할 때까지 장치를 통해 진행할 수 있다. 단계 702에서 클라우드 데이터 센터는 대안적으로 목적지 "B"(116a)의 IP 대 MAC 어드레스 매핑을 획득하기 위해 그 디렉토리를 지칭한다. 단계 704에서, 클라우드 데이터 센터 CE(112)는 MAC 어드레스를 소스 "A"(201)로 반환한다.

[0059] 단계 705에서, 사설 엔터프라이즈 네트워크(101) 내의 소스 "A"(201)로부터의 패킷(205)이 사설 엔터프라이즈 네트워크(101) 내의 논리적 CE 장치(110a)로 송신될 수 있으며, 논리적 CE 장치(110a)는 서비스 제공자 네트워

크(102) 내의 적어도 하나의 PE 장치(111a)를 통해 클라우드 네트워크(103) 내의 클라우드 데이터 센터 CE(112)로 패킷(205)을 전달할 수 있다. 단계 706에서, 클라우드 데이터 센터 CE(112)는 디렉토리 서버에게 다시 질의할 수 있다. 제 2 질의는 위치가 클라우드 네트워크(103) 내측에 존재하면 목적지 "B"의 위치 IP(locIP) 및 클라우드 IP(cloudIP)를 위해 디렉토리(500) 색인(lookup)을 수반할 수 있다. 목적지 "B"가 클라우드 네트워크(103) 내에 존재하면, 단계 707에서, 클라우드 데이터 센터 CE(112)는 상응하는 목적지 클라우드 IP 어드레스 및 위치 IP 어드레스를 검색할 수 있다.

[0060] 단계 708에서, 클라우드 데이터 센터 CE(112)는 MAC 헤더 및 검색된 클라우드 IP 어드레스에 상응하는 헤더를 이용하여 패킷을 캡슐화할 수 있다. 단계 709에서, 클라우드 데이터 센터 CE(112)는 검색된 locIP 어드레스에 상응하는 헤더를 이용하여 수정된 패킷을 캡슐화할 수 있다. 단계 710에서, 클라우드 데이터 센터 CE(112)는 클라우드 네트워크(103)를 통해 상응하는 locIP 어드레스로 이중 캡슐화된 패킷(206)을 송신할 수 있다.

[0061] 단계 711에서, locIP 어드레스에서 중간 스위치(117a)는 이중 캡슐화된 패킷(206)으로부터의 locIP 헤더를 캡슐화 해제할 수 있고 상응하는 cloudIP 어드레스로 수정된 패킷(209)을 송신할 수 있다. 단계 712에서, 상응하는 cloudIP 어드레스에서 서버(114a)에서 하이퍼바이저(115a)는 cloudIP 헤더 및 MAC 어드레스 헤더를 제거하면서 수정된 패킷(209)을 캡슐화 해제할 수 있으며, 목적지 "B" 에서 상응하는 가상 머신(116a)으로 패킷(210)을 송신할 수 있다. 대안적인 실시예에서, 하이퍼바이저(115a)는 가상 머신(116a)으로 패킷(210)을 송신하기 전에 포함된 보안 토큰(502)을 확인함으로써 수신된 패킷(210)을 먼저 입증할 수 있다. 일부 실시예에서, 하이퍼바이저(115a)는 패킷이 동일한 VLAN으로부터 유래한다는 것을 확인함으로써 VLAN 태그를 먼저 입증할 수 있다.

[0062] 대안적인 실시예에서, 단계 710에서, 클라우드 데이터 센터 CE(112)는 가상 스터브(104)를 통해 목적지 "B"(116a)로 단일 캡슐화된 패킷(306)을 발송한다. 이러한 대안적인 실시예에서, 각각의 VLAB ID는 고유하다. 따라서, 단계 708에서, 클라우드 데이터 센터 CE(112)는 VLAN ID를 국부적으로 고유한 것으로 변환할 수 있으며, 이는 MAC 어드레스가 주어진 스위치에 대해 국부적으로 고유하게 한다. 따라서, 단계 711에서, 중간 스위치(117a)는 오직 MAC 어드레스만을 사용하여 하이퍼바이저(115a)로 수정된 패킷(309)을 발송할 수 있다. 단계 712에서, 하이퍼바이저(115a)는 목적지 "B"(116a)로 IP 패킷(210)을 발송하기 전에 MAC 어드레스 헤더를 캡슐화 해제한다.

[0063] 도 8은 클라우드 네트워크(103) 내의 소스로부터 패킷을 발송하는 예시적인 방법(800)을 도시한다. 단계 801에서, 소스 "B"의 서버(114a) 상의 하이퍼바이저(115a)는 소스 "B" 가상 머신(116a)으로부터 패킷(210)을 수신한다. 단계 802에서, 하이퍼바이저(115a)는 목적지 어드레스가 그것의 VRF 표 내에 존재하는지 여부를 점검한다. 목적지 "A"(201)에 대한 전달 엔트리가 존재하면 단계 804가 뒤따르는 반면, 목적지 어드레스 "A"(201)가 리스트되지 않으면 단계 803이 뒤따른다.

[0064] 단계 804에서, 하이퍼바이저(115a)는 상응하는 cloudIP 헤더를 이용하여 패킷(210)을 캡슐화한다. 그런 다음, 단계 805에서, 하이퍼바이저(115a)는 상응하는 locIP 및 MAC 어드레스 헤더를 이용하여 수정된 패킷(209)을 캡슐화한다. MAC 어드레스 헤더는 또한 VLAN 태그를 포함할 수 있다. 단계 806에서, 하이퍼바이저(115a)는 상응하는 locIP 어드레스로 이중 캡슐화된 패킷(206)을 발송한다.

[0065] 단계 807에서, 목적지 "A"가 클라우드 네트워크(103) 내에 존재하면, 상응하는 locIP 어드레스에서의 중간 스위치(117b)는 이중 캡슐화된 패킷(206)으로부터 locIP 헤더를 캡슐화 해제하며, 상응하는 cloudIP 어드레스로 수정된 패킷(209)을 발송한다. 단계 808에서, 상응하는 cloudIP 어드레스에서의 하이퍼바이저(115c)는 cloudIP 및 MAC 어드레스 헤더의 수정된 패킷(209)을 캡슐화 해제한다. 단계 809에서, 하이퍼바이저(115c)는 목적지 "A" VM(116c)으로 패킷(210)을 송신한다. 일부 실시예에서, 하이퍼바이저(115c)는 목적지 "A" VM으로 패킷(203)을 발송하기 전에 확인을 위해 수정된 패킷의 보안 토큰(602)을 먼저 점검한다. 일부 실시예에서, 하이퍼바이저(115a)는 패킷(209)가 동일한 VLAN으로부터 유래하는 지를 확인하기 위해 VLAN 태그를 점검할 수 있다.

[0066] 대안적으로, 단계 802에서 목적지가 사설 엔터프라이즈 네트워크(101) 내에 존재한다고 판단될 때, 방법(800)은 단계 803으로 진행한다. 단계 803에서, 하이퍼바이저(115a)는 디렉토리 서버에게 목적지 "A" MAC 어드레스, cloudIP 어드레스, 및 locIP 어드레스에 대해 질의한다. 목적지가 사설 엔터프라이즈 네트워크(101) 내에 존재할 때, 상응하는 목적지 locIP는 클라우드 데이터 센터 CE(112)로 접속된 중간 스위치 IP(117a)의 IP 어드레스이며, 상응하는 MAC 및 cloudIP 어드레스는 클라우드 데이터 센터 CE(112)에 상응한다.

[0067] 방법(800)은 단계 810으로 진행하며, 단계 810은 상세하게 전술된 단계 804에 상응한다. 그런 다음, 방법(800)은 단계 811 및 단계 812로 진행하며, 단계 811 및 단계 812는 상세하게 전술된 단계 805 및 단계 806에 상응

한다. 이는 클라우드 데이터 센터 CE(112)에 상응하는 이중 캡슐화된 패킷(209)의 cloudIP 및 MAC 어드레스를 초래한다.

[0068] 따라서, 단계 812A에서, 클라우드 데이터 센터 CE(112)는 패킷이 클라우드 데이터 센터 CE(112)와 동일한 IP 어드레스 공간 내에 존재하는지 여부를 판단한다. 패킷이 동일한 IP 어드레스 공간 내에 존재하지 않으면, 방법(800)은 단계 807로 진행한다. 패킷이 동일한 IP 어드레스 공간 내에 존재하면, 방법(800)은 단계 813으로 진행하며, 단계 813에서, 클라우드 데이터 센터 CE(112)는 그것의 locIP, MAC, 및 cloudIP 헤더의 이중 캡슐화된 패킷(206)을 캡슐화 해제한다. 단계 814에서, 클라우드 데이터 센터 CE(112)는 사설 엔터프라이즈 네트워크(101) 내의 목적지 어드레스 "A"에 대한 상응하는 엔트리를 발견하기 위해 디렉토리(400)를 사용한다.

[0069] 단계 815에서, 클라우드 데이터 센터 CE(112)는 MAC 어드레스를 사설 엔터프라이즈 네트워크(101) 내의 목적지 "A" 어드레스에 상응하는 MAC 어드레스로 대체한다. 단계 816에서, 클라우드 데이터 센터 CE(112)는 사설 엔터프라이즈 네트워크(101)를 통해 소스 "A"(201)로 패킷(206)을 송신한다. 일부 실시예에서, 디렉토리 내에 엔트리가 존재하지 않을 때, 클라우드 데이터 센터 CE(112)는 FF-FF-FF-FF-FF-FF와 같은 MAC 브로드캐스트 어드레스를 사용하여 사설 엔터프라이즈 네트워크(101) 내의 각각의 장치로 패킷(206)을 브로드캐스트할 수 있다. 단계 817에서, 사설 엔터프라이즈 네트워크(101) 내의 목적지 "A" 어드레스에서의 고객 에지 장치(110a)는 패킷(205)의 MAC 헤더를 캡슐화 해제하며, 단계 818에서, 고객 에지 장치(110a)는 상응하는 목적지 어드레스 "A"(201)로 패킷(203)을 송신한다. 대안적인 실시예에서, 고객 에지 라우터(110a)는 패킷(205)이 동일한 VLAN으로부터 유래하는 것을 확인하기 위해 VLAN 태그를 점검할 수 있다.

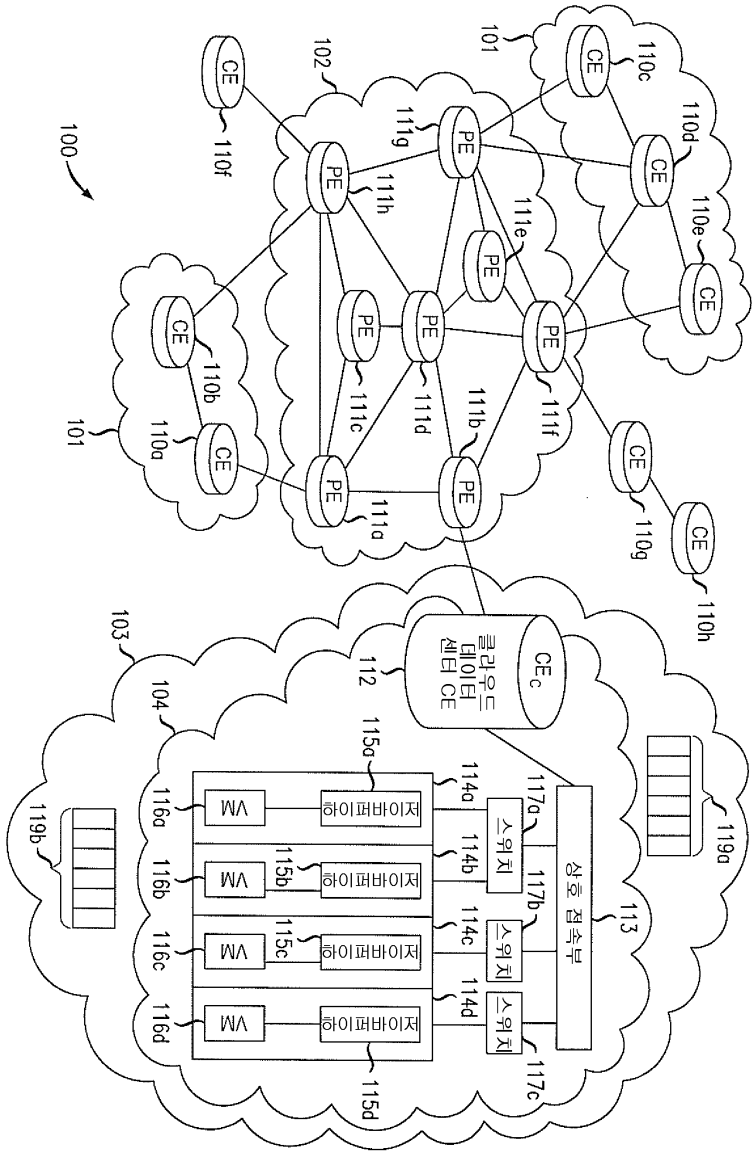
[0070] 일부 실시예에서, 각각의 VLAN은 고유한 것이며, 이는 cloudIP 어드레스를 필요하지 않게 한다. 따라서, 하이퍼바이저(115a)는 cloudIP 헤더를 이용하여 IP 패킷(210)을 캡슐화하지 않는다. 대신에, 하이퍼바이저(115a)는 목적지 "A"(201)로 단일 캡슐화된 패킷(309)을 발송한다.

[0071] 본 발명의 다양한 예시적인 실시예가 하드웨어 및/또는 펌웨어로 구현될 수 있다는 것이 전술한 설명으로부터 당연하다. 또한, 다양한 예시적인 실시예가 머신 판독 가능한 저장 매체 상에 저장된 명령으로 구현될 수 있으며, 명령은 본 명세서 내에서 상세하게 설명된 동작을 수행하도록 적어도 하나의 프로세서에 의해 판독되고 실행될 수 있다. 머신 판독 가능한 저장 매체는 네트워크 노드(예를 들어, 라우터 또는 스위치)와 같은 머신에 의해 판독 가능한 형태로 정보를 저장하기 위한 임의의 메카니즘을 포함할 수 있다. 따라서, 머신 판독 가능한 저장 매체는 ROM(read-only memory), RAM(random-access memory), 자기 디스크 저장 매체, 광 저장 매체, 플래시-메모리 장치, 및 유사한 저장 매체를 포함할 수 있다.

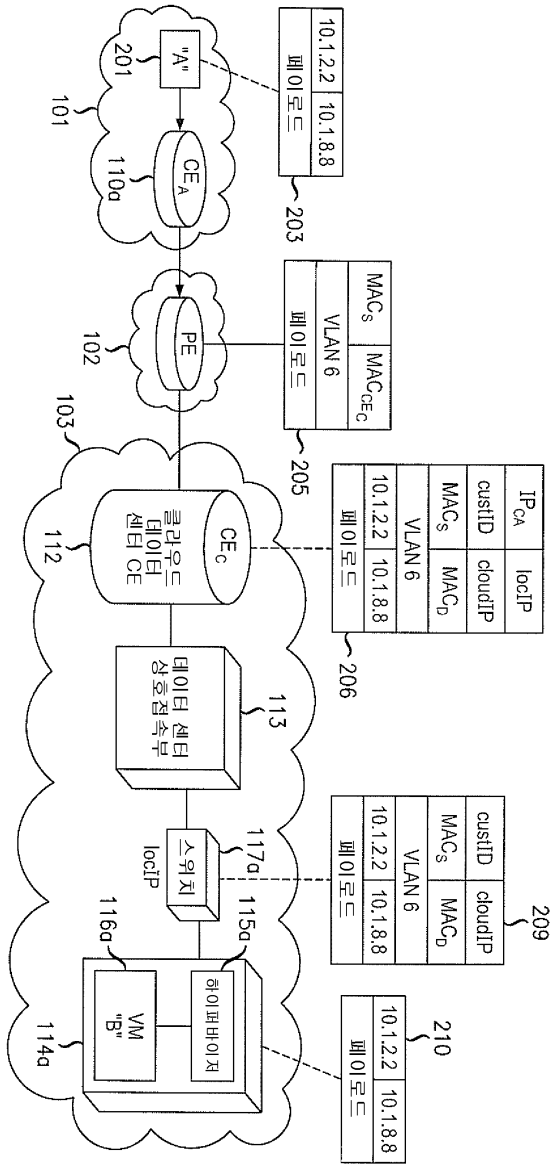
[0072] 비록 다양한 예시적인 실시예가 특히 소정의 예시적인 양태를 참조하여 상세하게 설명되었지만, 본 발명이 다른 실시예일 수 있으며, 그것의 상세는 다양한 명백한 측면에서의 수정일 수 있다는 것이 이해되어야 한다. 당업자에게 아주 당연한 바와 같이, 변경과 수정이 본 발명의 사상 및 범위 내에서 구현될 수 있다. 따라서, 전술한 개시, 설명, 및 도면은 오직 예시적인 목적을 위한 것이며, 오직 특허청구범위에 의해 정의된 본 발명을 어떠한 방식으로도 제한하지 않는다.

도면

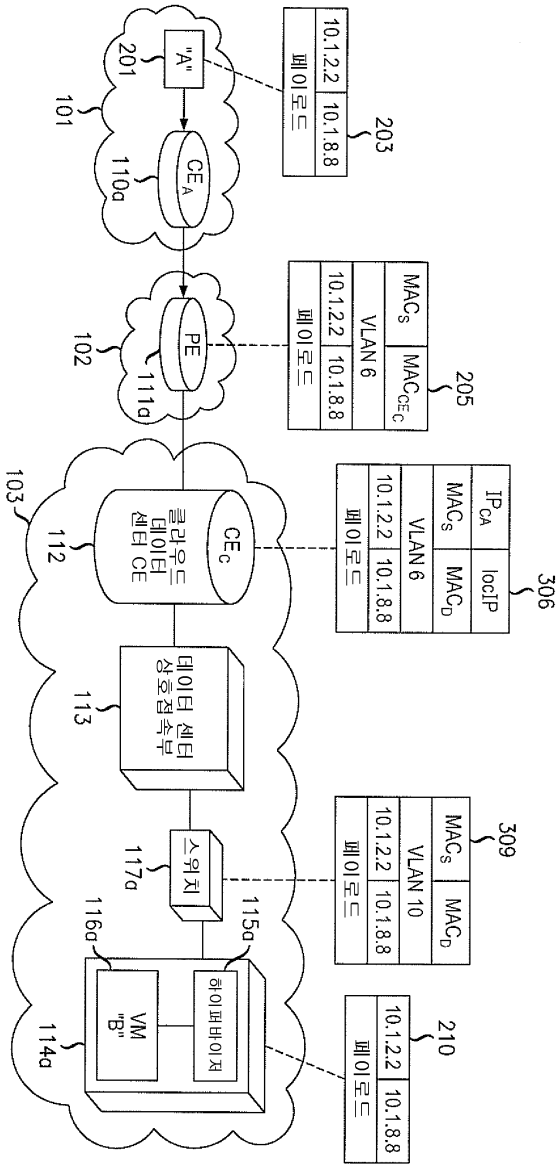
도면1


100
101
102
103
104
110a
110b
110c
110d
110e
110f
110g
110h
111a
111b
111c
111d
111e
111f
111g
111h
112
CE
PE
CEc
클라우드 데이터 센터 CE
113
상호 접속부
114a
114b
114c
114d
115a
115b
115c
115d
116a
116b
116c
116d
117a
117b
117c
119a
119b
VM
하이퍼바이저
스위치

도면2


101
201
"A"
110a
CE_A
203
10.1.2.2
10.1.8.8
페이로드
102
PE
MAC_S
VLAN 6
MAC_CEC
페이로드
205
103
112
클라우드 데이터 센터 CE
CE_C
IP_CA
custID
cloudID
locIP
MAC_S
VLAN 6
MAC_D
10.1.2.2
10.1.8.8
페이로드
206
113
데이터 센터 상호접속부
117a
스위치
locIP
209
custID
cloudID
MAC_S
VLAN 6
MAC_D
10.1.2.2
10.1.8.8
페이로드
116a
115a
VM "B"
하이퍼바이저
114a
210
10.1.2.2
10.1.8.8
페이로드

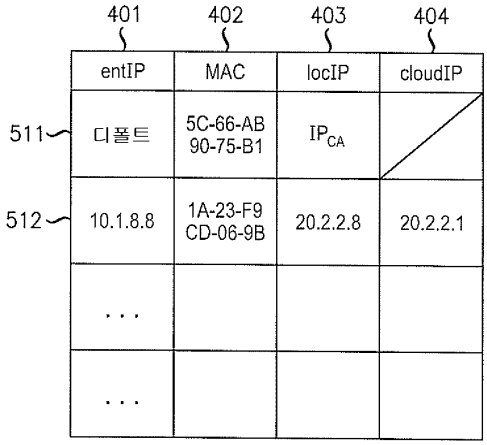
도면3



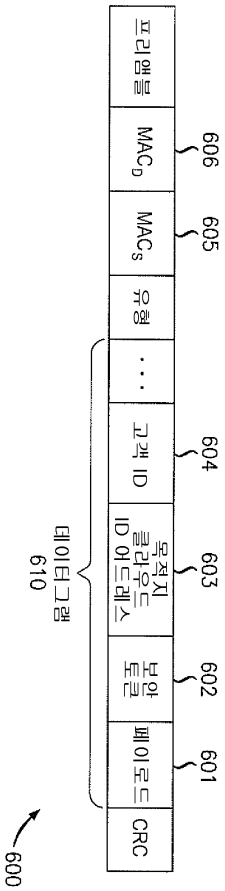
도면4

	401 entIP	402 MAC	403 locIP	404 cloudIP	405 next Hop
411	10.1.8.8	1A-23-F9-CD-06-9B	20.2.2.8	20.2.2.1	20.2.2.8
412	10.1.2.10	5C-66-AB 90-75-B1			디렉토리 서버
413	10.1.2.2	49-BD-P2-C7 56-2A			PE
	. . .				

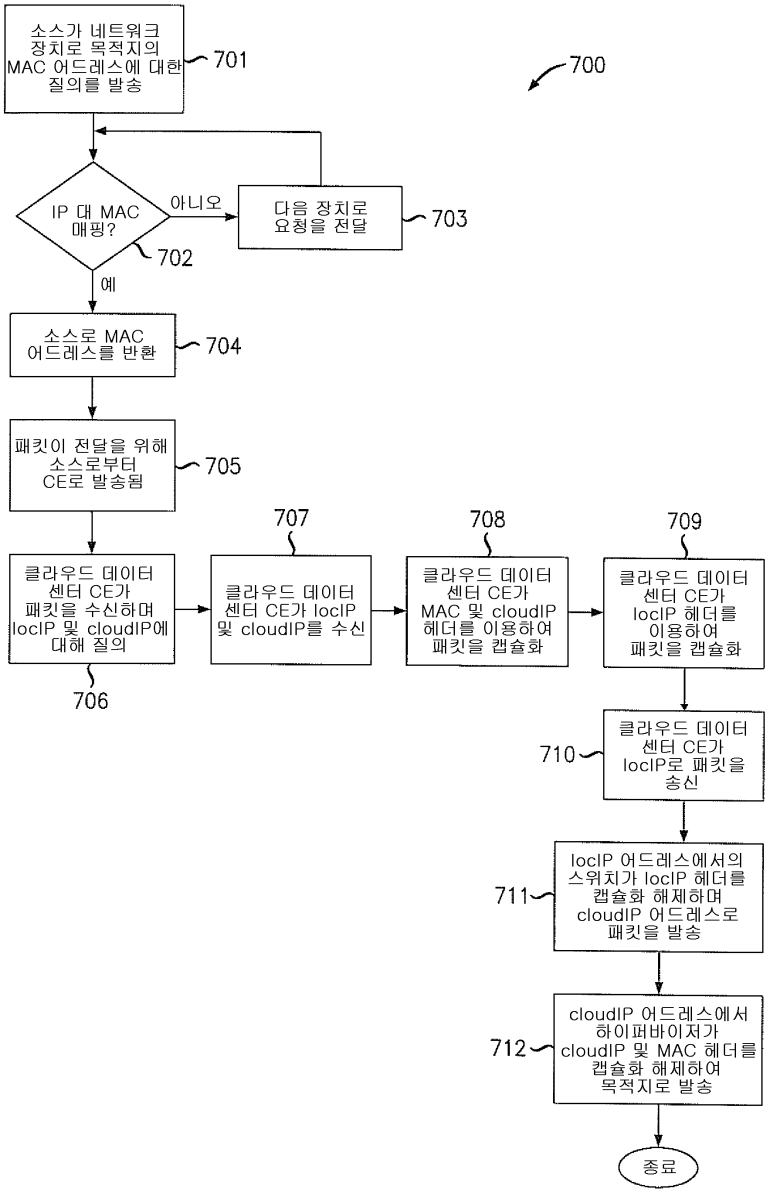
도면5


401
402
403
404
entIP
MAC
locIP
cloudIP
511
디폴트
5C-66-AB 90-75-B1
IP_{CA}
512
10.1.8.8
1A-23-F9 CD-06-9B
20.2.2.8
20.2.2.1

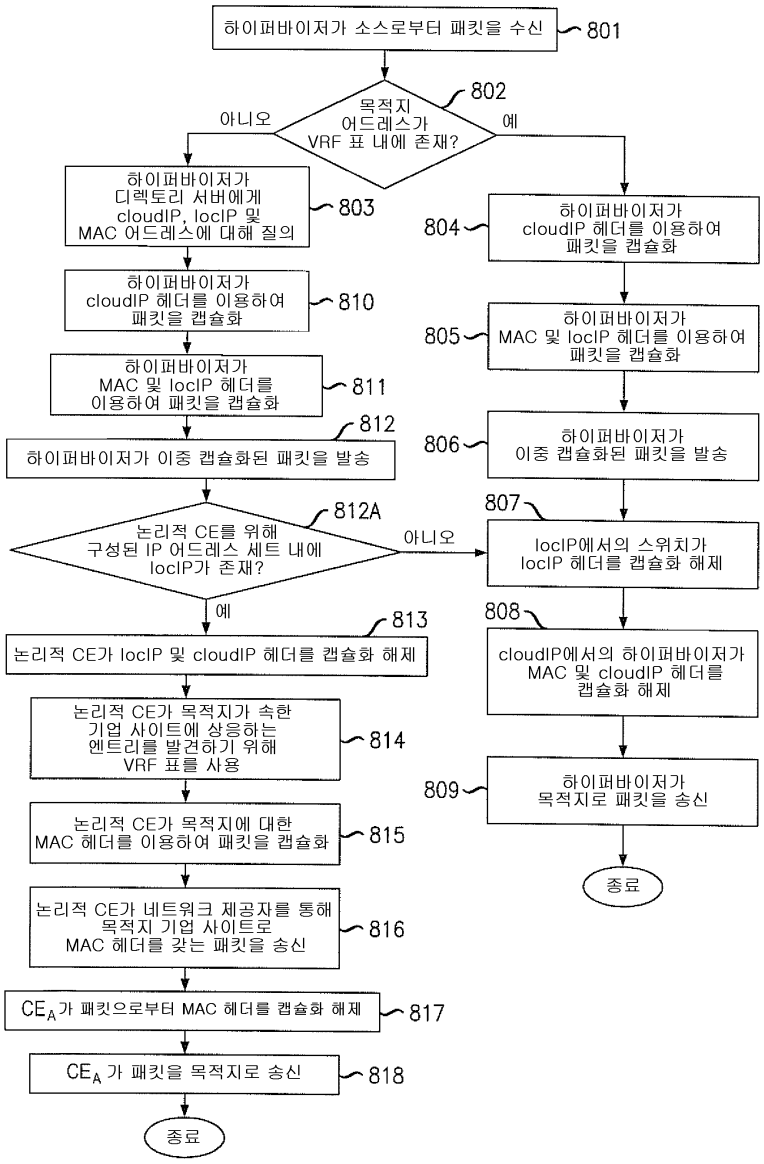
도면6


프리앰블
MAC_D
606
MAC_S
605
유형
...
고객 ID
604
목적지 클라우드 ID 어드레스
603
보안 토큰
602
페이로드
601
CRC
데이터그램 610
600

도면7


700
소스가 네트워크 장치로 목적지의 MAC 어드레스에 대한 질의를 발송
701
IP 대 MAC 매핑?
702
아니오
다음 장치로 요청을 전달
703
예
소스로 MAC 어드레스를 반환
704
패킷이 전달을 위해 소스로부터 CE로 발송됨
705
클라우드 데이터 센터 CE가 패킷을 수신하며 locIP 및 cloudIP에 대해 질의
706
707
클라우드 데이터 센터 CE가 locIP 및 cloudIP를 수신
708
클라우드 데이터 센터 CE가 MAC 및 cloudIP 헤더를 이용하여 패킷을 캡슐화
709
클라우드 데이터 센터 CE가 locIP 헤더를 이용하여 패킷을 캡슐화
710
클라우드 데이터 센터 CE가 locIP로 패킷을 송신
711
locIP 어드레스에서의 스위치가 locIP 헤더를 캡슐화 해제하며 cloudIP 어드레스로 패킷을 발송
712
cloudIP 어드레스에서 하이퍼바이저가 cloudIP 및 MAC 헤더를 캡슐화 해제하여 목적지로 발송
종료

도면8


하이퍼바이저가 소스로부터 패킷을 수신
801
목적지 어드레스가 VRF 표 내에 존재?
802
아니오
예
하이퍼바이저가 디렉토리 서버에게 cloudIP, locIP 및 MAC 어드레스에 대해 질의
803
하이퍼바이저가 cloudIP 헤더를 이용하여 패킷을 캡슐화
804
하이퍼바이저가 MAC 및 locIP 헤더를 이용하여 패킷을 캡슐화
805
하이퍼바이저가 이중 캡슐화된 패킷을 발송
806
하이퍼바이저가 cloudIP 헤더를 이용하여 패킷을 캡슐화
810
하이퍼바이저가 MAC 및 locIP 헤더를 이용하여 패킷을 캡슐화
811
하이퍼바이저가 이중 캡슐화된 패킷을 발송
812
논리적 CE를 위해 구성된 IP 어드레스 세트 내에 locIP가 존재?
812A
아니오
예
locIP에서의 스위치가 locIP 헤더를 캡슐화 해제
807
cloudIP에서의 하이퍼바이저가 MAC 및 cloudIP 헤더를 캡슐화 해제
808
하이퍼바이저가 목적지로 패킷을 송신
809
종료
논리적 CE가 locIP 및 cloudIP 헤더를 캡슐화 해제
813
논리적 CE가 목적지가 속한 기업 사이트에 상응하는 엔트리를 발견하기 위해 VRF 표를 사용
814
논리적 CE가 목적지에 대한 MAC 헤더를 이용하여 패킷을 캡슐화
815
논리적 CE가 네트워크 제공자를 통해 목적지 기업 사이트로 MAC 헤더를 갖는 패킷을 송신
816
CE_A가 패킷으로부터 MAC 헤더를 캡슐화 해제
817
CE_A가 패킷을 목적지로 송신
818
종료