

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2017년 8월 3일 (03.08.2017)

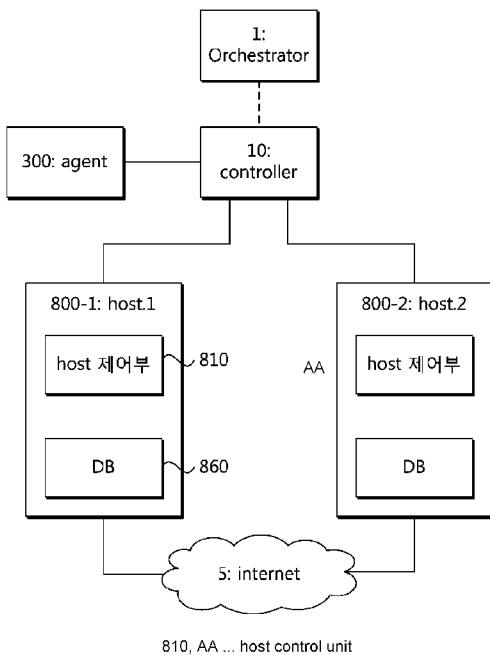


(10) 국제공개번호
WO 2017/131285 A1

- (51) 국제특허분류: H04L 12/24 (2006.01) H04L 12/749 (2013.01)
H04L 12/50 (2006.01)
 - (21) 국제출원번호: PCT/KR2016/002924
 - (22) 국제출원일: 2016년 3월 23일 (23.03.2016)
 - (25) 출원언어: 한국어
 - (26) 공개언어: 한국어
 - (30) 우선권정보: 10-2016-0008995 2016년 1월 25일 (25.01.2016) KR
10-2016-0008996 2016년 1월 25일 (25.01.2016) KR
 - (71) 출원인: 쿨클라우드(주) (KULCLOUD) [KR/KR]; 13486 경기도 성남시 분당구 판교로 253, A-501, Gyeonggi-do (KR).
 - (72) 발명자: 박성용 (PARK, Sueng Young); 16902 경기도 용인시 기흥구 죽현로 8-13, 303 동 905 호, Gyeonggi-do (KR). 공석환 (KONG, Seok Hwan); 17003 경기도 용인시 기흥구 동백 7로 80, 코아루아파트 2201 동 603 호, Gyeonggi-do (KR). 딥조이티사이키아 (SAIKIA, Dipjyoti); 13595 경기도 성남시 분당구 백현로 105, 로얄팰리스하우스빌 A 1215 호, Gyeonggi-do (KR). 정백균 (JUNG, Baek Gyun); 14049 경기도 안양시 동안구 달안로 125, Gyeonggi-do (KR).
 - (74) 대리인: 최규성 (CHOI, Kuesung); 34014 대전시 유성구 테크노중앙로 55 에이스타워 603 호, Daejeon (KR).
 - (81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
 - (84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).
- 공개:
— 국제조사보고서와 함께 (조약 제 21 조(3))

(54) Title: CONTAINER NETWORK MANAGEMENT SYSTEM AND CONTAINER NETWORKING METHOD

(54) 발명의 명칭 : 컨테이너 네트워크 관리 시스템 및 컨테이너 네트워킹 방법



(57) Abstract: The present invention relates to a software defined network (SDN)-based container network management system and a container networking method of a container network, the container network management system and the container networking method enabling an L2/L3 network between containers, enabling unnecessary multicast and broadcast traffics to be reduced, and enabling a flexible network operation. The management system can comprise: a real network interface connected to a legacy network; an SDN-based virtual switch for transmitting/receiving a packet to/from the legacy network through the real network interface; a host control unit for generating the virtual switch; a container bridge generated by the host control unit, virtually network-coupled to the virtual switch through a bridge-switch network interface (NI), and having a bridge identifier for identifying itself; and a first host generated by the host control unit, allowing a unique IP address to be allocated on the basis of the bridge net information, and comprising a plurality of containers virtually network-coupled to the container bridge.

(57) 요약서: 본 발명은 SDN(Software Defined Network) 기반의 컨테이너 네트워크 관리 시스템 및 컨테이너 네트워킹의 컨테이너 네트워킹 방법에 관한 것으로, 컨테이너 사이의 L2/L3 네트워크가 가능하도록 하며, 불필요한 멀티캐스트 및 브로드캐스트 트래픽을 줄일 수 있고, 탄력적인 네트워크 운용이 가능하도록 하며, 본 관리 시스템은 레거시 네트워크에 연결되는 실제 네트워크 인터페이스, 상기 실제 네트워크 인터페이스를 통해 레거시 네트워크와 패킷을 주고 받는, SDN(Software Defined Network) 기반의 가상 스위치, 상기 가상 스위치를 생성하는 호스트 제어부, 상기 호스트 제어부에 의해 생성되며, 브리지-스위치 NI(Network Interface)를 통해 상기 가상 스위치와 가상으로 네트워크 커플링되며, 자신을 식별하는 브리지 식별자를 구비하는 컨테이너

브리지, 및 상기 호스트 제어부에 의해 생성되고, 상기 브리지 넷 정보를 기초로 고유 IP 주소를 할당받으며, 상기 컨테이너 브리지에 가상으로 네트워크 커플링되는 복수의 컨테이너를 구비하는 제 1 호스트를 포함할 수 있다.

WO 2017/131285 A1

명세서

발명의 명칭: 컨테이너 네트워크 관리 시스템 및 컨테이너 네트워킹 방법

기술분야

- [1] 본 발명은 SDN(Software Defined Network) 기반의 컨테이너 네트워크 관리 시스템 및 컨테이너 네트워크의 컨테이너 네트워킹 방법에 관한 것으로, 컨테이너 사이의 L2/L3 네트워크가 가능하도록 하며, 불필요한 멀티캐스트 및 브로드캐스트 트래픽을 줄일 수 있고, 탄력적인 네트워크 운용이 가능하도록 하며, 레거시 네트워크와 SDN 네트워크 사이의 패킷 흐름을 가능하도록 하는 관리 시스템 및 네트워킹 방법에 관한 것이다.

배경기술

- [2] 휴대 장치 및 서버 가상화의 폭발적인 증가와 클라우드 서비스의 출현으로, 네트워크 수요가 늘어났다. SDN은 어플리케이션에서 추상화된 기본적인 네트워크 인프라 구조이며, 논리적으로 중앙 집중적인 네트워크 인텔리전스(network intelligence)이며, 제어 플레인과 데이터 플레인이 분리되어 있는 것을 특징으로 한다.
- [3] 오픈 플로우는 고속 패킷 전달과 높은 레벨의 라우팅 결정 기능들을 분리한다. 패킷 포워딩 플레인은 여전히 스위치 단에 관여되며, 반면 고수준 라우팅 결정은 분리된 컨트롤러에서 관여되며, 이들은 오픈 플로우 프로토콜을 통해 통신한다.
- [4] 그러나 기존 네트워크에서 SDN으로의 전환 과도기로서, 기존 프로토콜과 장치와 상호 작용하는 소프트웨어 정의 네트워크의 필요성이 있다. 이러한 하이브리드 SDN 네트워크를 구성하는 장비는 컴퓨팅 자원이나 네트워킹 자원 소모가 적으며, 단순한 구조를 가질 필요가 있다.
- [5] 기존의 가상 머신과는 상이한 경량화된 컨테이너가 가상 머신 대신 사용되고 있다. 컨테이너는 네트워크 관리가 존재하지 않으며, 모든 컨테이너들이 동일 L2 도메인에 존재하도록 되어 있었다. 이는 네트워크의 정책 관리가 어렵게 하며, 서비스별 네트워크 기능을 관리하기 힘들게 하는 요소가 되었다. 또한 컨테이너와 외부 네트워크 간의 연동을 제공하는 서비스가 존재하지 않았다. 기존 클라우드 기반의 서버의 경우, 각 서비스별 프론트엔드/백엔드(FrontEnd/BackEnd) 네트워크의 관리가 요구된다. 프론트엔드만 공개(public)된 네트워크에서의 접근이 가능하도록 하고, 나머지 컴퓨팅 작업은 사설(privatge) 영역인 백엔드 네트워크에서만 동작되도록 하기 위해서이다. 컨테이너는 이러한 네트워크 관리 메커니즘이 존재하지 않아, 실제적인 서비스를 하기에 네트워크 관리 측면에 어려움이 있다.
- [6] <선행기술문헌>
- [7] 비특허문헌 1. OpenFlow Switch Specification version 1.4.0(Wire Protocol 0x05),

October 14, 2013

[<https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-spec-v1.4.0.pdf>]

- [8] 비특허문헌 2. Software-Defined Networking: The New Norm for Networks, ONF White Paper, April 13, 2012
[<https://www.opennetworking.org/images/stories/downloads/sdn-resources/white-papers/wp-sdn-newnorm.pdf>]

- [9] 비특허문헌 3. ETSI GS NFV 002 v1.1.1 (2013-10)

- [10] [http://www.etsi.org/deliver/etsi_gs/NFV/001_099/002/01.01.01_60/gs_NFV002v010101p.pdf]

발명의 상세한 설명

기술적 과제

- [11] 본 발명의 목적은 컨테이너의 네트워크 관리가 가능하도록 하며, L2/L3 네트워크가 가능하도록 하는 네트워크 환경을 제공하고, 컨테이너 운용 아래에서 외부 네트워크와 분리된 사설 네트워크가 가능하도록 하는 네트워크 관리 시스템 및 그 방법을 제공하는 데 있다.

- [12] 또한, SDN 기반의 컨테이너 네트워크에서 레거시 네트워크를 지원할 수 있도록 하는 시스템 및 그 방법을 제공하는 데 또 다른 목적이 있다.

과제 해결 수단

- [13] 본 발명에 따른 컨테이너 네트워크 관리 시스템은, 레거시 네트워크에 연결되는 실제 네트워크 인터페이스; 상기 실제 네트워크 인터페이스를 통해 레거시 네트워크와 패킷을 주고 받는, SDN(Software Defined Network) 기반의 가상 스위치; 상기 가상 스위치를 생성하는 호스트 제어부; 상기 호스트 제어부에 의해 생성되며, 브리지-스위치 NI(Network Interface)를 통해 상기 가상 스위치와 가상으로 네트워크 커플링되며, 자신을 식별하는 브리지 식별자를 구비하는 컨테이너 브리지; 상기 브리지 식별자를 기초로 네트워크 서브넷 정보 및 상기 실제 네트워크 인터페이스를 게이트웨이로 하는 게이트웨이 정보를 브리지 넷 정보로 저장하는 데이터베이스; 및 상기 호스트 제어부에 의해 생성되고, 상기 브리지 넷 정보를 기초로 고유 IP 주소를 할당받으며, 상기 컨테이너 브리지에 가상으로 네트워크 커플링되는 복수의 컨테이너를 구비하는 제1 호스트를 포함할 수 있다.

- [14] 본 발명에 따른 호스트는, 레거시 네트워크에 연결되는 실제 네트워크 인터페이스; 상기 실제 네트워크 인터페이스를 통해 레거시 네트워크와 패킷을 주고 받고, 외부의 제어기에 의해 제어되는 SDN(Software Defined Network) 기반의 가상 스위치; 상기 가상 스위치를 생성하는 호스트 제어부; 상기 호스트 제어부에 의해 생성되며, 브리지-스위치 NI(Network Interface)를 통해 상기 가상 스위치와 가상으로 네트워크 커플링되며, 자신을 식별하는 브리지 식별자를

구비하는 컨테이너 브리지; 상기 브리지 식별자를 기초로 네트워크 서브넷 정보 및 상기 실제 네트워크 인터페이스를 게이트웨이로 하는 게이트웨이 정보를 브리지 넷 정보로 저장하는 데이터베이스; 및 상기 호스트 제어부에 의해 생성되고, 상기 브리지 넷 정보를 기초로 고유 IP 주소를 할당받으며, 상기 컨테이너 브리지에 가상으로 네트워크 커플링되는 복수의 컨테이너를 구비할 수 있다.

- [15] 본 발명에 따른 컨테이너 네트워크의 컨테이너 네트워킹 방법은, 컨테이너를 생성하며 실제 네트워크 인터페이스를 통해 레거시 네트워크와 연결되는 호스트에서, SDN(Software Defined Network) 기반의 가상 스위치를 생성하는 단계; 상기 가상 스위치를 상기 실제 네트워크 인터페이스와 네트워크 연결하는 단계; 상기 호스트에서, 네트워크 환경을 구별하는 브리지 식별자, 상기 가상 스위치를 게이트웨이로 하는 게이트웨이 정보, 및 네트워크 서브넷 정보를 구비하는 컨테이너 컨테이너 브리지 생성 요청을 받으면, 컨테이너 브리지를 생성하는 단계; 상기 컨테이너 브리지와 상기 가상 스위치 사이에 모든 동일 도메인 식별자를 가지는 패킷이 통과할 수 있도록 상기 컨테이너 브리지와 상기 가상 스위치를 네트워크 커플링하는 단계; 상기 호스트에서, 상기 브리지 식별자를 키로 하는 제1 컨테이너 식별자 및 제1 동일 도메인 식별자를 구비하는 컨테이너 생성 요청을 받으면, 상기 제1 컨테이너 식별자를 구비하는 제1 컨테이너를 생성하는 단계; 상기 브리지 식별자에 연관된 네트워크 서브넷 정보를 기초로 상기 제1 컨테이너에 IP 주소를 할당하는 단계; 및 상기 컨테이너 브리지와 상기 제1 컨테이너를 네트워크 커플링하고, 상기 제1 동일 도메인 식별자에 연관된 제1 도메인 태그를 가진 패킷만 상기 제1 컨테이너로 전달되도록 상기 컨테이너와 커플링되는 상기 컨테이너 브리지의 브리지-컨테이너 NI(Network Interface)에 상기 제1 도메인 태그를 지정하는 단계를 포함할 수 있다.

발명의 효과

- [16] 본 발명에 따르면, SDN 기반의 컨테이너 네트워크에서 컨테이너의 네트워크 관리가 가능하며, 컨테이너 간의 L2/L3 네트워킹을 제공하며, 공용 외부 네트워크와 서비스가 운용되는 사설 네트워크로 분리할 수 있으며, 레거시 네트워크와 통신이 가능하여 기존의 레거시 네트워크 장비를 그대로 이용할 수 있다.

도면의 간단한 설명

- [17] 도 1은 SDN 네트워크 시스템의 구조도,
 [18] 도 2는 도 1의 네트워크 시스템의 제어기의 블록 구성도(block diagram),
 [19] 도 3은 도 1의 네트워크 시스템의 스위치의 블록 구성도,
 [20] 도 4는 플로우 엔트리의 필드 테이블 및 플로우 엔트리에 따른 동작 종류를 나타내는 동작 테이블,

- [21] 도 5는 그룹 및 미터 테이블의 필드 테이블,
- [22] 도 6은 본 발명의 일 실시예에 따른 통합 라우팅 시스템을 포함하는 네트워크 시스템의 블록 구성도,
- [23] 도 7은 도 6의 네트워크 시스템의 가상화한 블록 구성도,
- [24] 도 8은 본 발명의 다른 실시예에 따른 SDN 제어기의 블록 구성도,
- [25] 도 9는 본 발명의 일 실시예에 따른 레거시 라우팅 컨테이너의 블록 구성도,
- [26] 도 10은 도 6의 제어기의 플로우에 대한 레거시 라우팅 여부 판단 방법에 대한 순서도,
- [27] 도 11은 본 발명의 일 실시예에 따른 통합 라우팅 방법에 따른 신호 흐름도,
- [28] 도 12는 본 발명의 다른 실시예에 따른 통합 라우팅 방법에 따른 신호 흐름도,
- [29] 도 13은 본 발명의 일 실시예에 따른 플로우 테이블,
- [30] 도 14는 본 발명의 일 실시예에 따른 컨테이너 네트워크 관리 시스템을 도시하는 구조도,
- [31] 도 15는 도 14의 호스트의 내부 구조를 중점적으로 나타내는 호스트의 블록 구성도,
- [32] 도 16은 본 발명의 일 실시예에 따른 컨테이너 생성 방법의 순서도,
- [33] 도 17은 도 14의 다른 호스트 내부 구조를 도시하는 구조도,
- [34] 도 18은 도 14를 간략히 도시한 구조도,
- [35] 도 19는 도 18을 레거시 가상 라우터로 변환한 네트워크 구조도, 및
- [36] 도 20 내지 도 23은 한 컨테이너에서 다른 컨테이너로의 패킷 흐름에 관한 신호 흐름도이다.

발명의 실시를 위한 형태

- [37] 이하, 도면을 참조하여 본 발명을 보다 상세하게 설명한다.
- [38] 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되어서는 안 된다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제1 구성요소는 제2 구성요소로 명명될 수 있고, 유사하게 제2 구성요소도 제1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.
- [39] 어떤 구성요소가 다른 구성요소에 "연결되어" 있다거나 "접속되어" 있다고 언급된 때에는, 그 다른 구성요소에 직접적으로 연결되어 있거나 또는 접속되어 있을 수도 있지만, 중간에 다른 구성요소가 존재할 수도 있다고 이해되어야 할 것이다. 반면에, 어떤 구성요소가 다른 구성요소에 "직접 연결되어" 있다거나 "직접 접속되어" 있다고 언급된 때에는, 중간에 다른 구성요소가 존재하지 않는 것으로 이해되어야 할 것이다. 또한 네트워크 상의 제1 구성요소와 제2 구성요소가 연결되어 있거나 접속되어 있다는 것은, 유선 또는 무선으로 제1

- 구성요소와 제2 구성요소 사이에 데이터를 주고 받을 수 있음을 의미한다.
- [40] 또한, 이하의 설명에서 사용되는 구성요소에 대한 접미사 "모듈" 및 "부"는 단순히 본 명세서 작성의 용이함만이 고려되어 부여되는 것으로서, 그 자체로 특별히 중요한 의미 또는 역할을 부여하는 것은 아니다. 따라서, 상기 "모듈" 및 "부"는 서로 혼용되어 사용될 수도 있다.
- [41] 이와 같은 구성요소들은 실제 응용에서 구현될 때 필요에 따라 2 이상의 구성요소가 하나의 구성요소로 합쳐지거나, 혹은 하나의 구성요소가 2 이상의 구성요소로 세분되어 구성될 수 있다. 도면 전체를 통하여 동일하거나 유사한 구성요소에 대해서는 동일한 도면 부호를 부여하였고, 동일한 도면 부호를 가지는 구성요소에 대한 자세한 설명은 전술한 구성요소에 대한 설명으로 대체되어 생략될 수 있다.
- [42] SDN은 패킷을 전달하는 데이터 플레인과 패킷의 흐름을 제어하는 제어 플레인을 분리된 개념이다. SDN에서 패킷이 발생했을 때, 네트워크 장비는 패킷을 어디로 전달할지 SDN 제어 소프트웨어(제어기)에게 물어보고, 그 결과를 반영하여 패킷을 전송하는 경로와 방식을 결정한다. SDN은 이론적인 개념으로, 실제로 적용하기 위해 오픈플로우(Openflow)가 등장하였다. 즉 오픈플로우는 SDN을 구현하기 위해 제정된 표준 인터페이스이다. 오픈플로우는 오픈플로우 제어기와 오픈플로우 스위치로 구성되어, 플로우 정보를 제어하여 패킷의 전달 경로 및 방식을 결정한다. 본 명세서 전반에서, 오픈플로우와 SDN은 서로 동일한 의미로 사용되거나 혼용하여 사용될 수 있다.
- [43] 플로우(flow)는 하나의 스위치 관점에서 적어도 하나의 헤더 필드의 값을 공유하는 일련의 패킷들 또는 다중 스위치의 여러 플로우 엔트리(flow entry)들의 조합에 따른 특정 경로의 패킷 흐름을 의미할 수 있다. 오픈플로우 네트워크는 플로우 단위로 경로 제어, 장애 회복, 부하 분산 및 최적화를 행할 수 있다.
- [44] 본 명세서에서 특정 용어는 다음의 기술에 의해 정의되거나 본래의 의미 이외의 의미를 더 구비할 수 있다. "플로우"는 해당 스위치에서 처리할 패킷 자체를 의미할 수 있다. "플로우"는 해당 스위치에서 처리할 패킷과 메타데이터(패킷이 인입한 인입 포트, 패킷이 다른 스위치로부터 인입한 경우 상기 다른 스위치의 인입 포트 등)를 포함하는 것을 의미할 수도 있다. "플로우 처리 정보"는 스위치에서 유입된 패킷을 처리할 정보로, 패킷 또는 패킷의 메타데이터를 수정하는데 필요한 정보 및/또는 패킷이 유출될 특정 네트워크 인터페이스(포트) 등을 의미할 수 있다. 플로우 처리 정보는 플로우 테이블의 플로우 엔트리의 내용 또는 플로우 엔트리에 적용될 내용과 동일할 수 있으며, 플로우 엔트리 그 자체를 의미할 수 있다. "플로우 처리"는 위 플로우 처리 정보에 기초하여 패킷 또는 플로우를 스위치에서 처리함을 의미할 수 있다.
- [45] 도 1은 SDN 네트워크 시스템의 구조도, 도 2는 도 1의 네트워크 시스템의 제어기의 블록 구성도(block diagram), 도 3은 도 1의 네트워크 시스템의 스위치의 블록 구성도, 도 4는 플로우 엔트리의 필드 테이블 및 플로우 엔트리에 따른 동작

- 종류를 나타내는 동작 테이블, 도 5는 그룹 및 미터 테이블의 필드 테이블이다.
- [46] 도 1(a)를 참조하면, SDN 네트워크 시스템은 제어기(controller)(10), 복수의 스위치(20) 및 복수의 네트워크 디바이스(30)를 포함할 수 있다.
- [47] 네트워크 디바이스(30)는 데이터나 정보를 주고 받고자 하는 사용자 단말 장치, 또는 특정 기능을 수행하는 물리 장치 또는 가상 장치를 포함할 수 있다. 하드웨어 관점에서, 네트워크 디바이스(30)는 PC, 클라이언트 단말기, 서버, 워크스테이션, 슈퍼컴퓨터, 이동통신 단말기, 스마트폰, 스마트패드 등이 있을 수 있다. 또한 네트워크 디바이스(30)는 물리 장치 상에 생성된 가상 머신(VM)일 수 있다.
- [48] 네트워크 디바이스(30)는 네트워크 상의 여러가지 기능을 수행하는 네트워크 기능(network function)으로 지칭될 수 있다. 네트워크 기능은 안티(anti) DDoS, 침입 감지/차단(IDS/IPS), 통합 보안 서비스, 가상 사설망 서비스, 안티 바이러스, 안티 스팸, 보안 서비스, 접근관리 서비스, 방화벽, 로드 밸런싱, QoS, 비디오 최적화 등을 포함할 수 있다. 이러한 네트워크 기능은 가상화될 수 있다.
- [49] 가상화된 네트워크 기능으로 ETSI(유럽전기통신표준협회)에서 발행한 NFV 관련 백서(비특허문헌 3 참조)에서 정의된 네트워크 기능 가상화(Network Function Virtualization; NFV)가 있다. 본 명세서에서 네트워크 기능(NF)은 네트워크 기능 가상화(NFV)와 혼용하여 사용될 수 있다. NFV는 테넌트(tenant)별 필요한 L4-7 서비스 연결을 동적으로 생성하여 필요한 네트워크 기능을 제공하거나, DDoS 공격의 경우 정책 기반으로 필요한 방화벽, IPS 및 DPI 기능 등을 일련의 서비스 체이닝으로 빠르게 제공되는데 이용될 수 있다. 또한 NFV는 방화벽이나 IDS/IPS를 쉽게 온오프 할 수 있으며, 자동으로 프로비저닝(provisioning)할 수 있다. NFV는 오버 프로비저닝의 필요성도 줄일 수 있다.
- [50] 제어기(controller)(10)는 SDN 시스템을 제어하는 일종의 지휘 컴퓨터로서, 다양하고 복잡한 기능들, 예를 들어, 라우팅, 정책 선언, 및 보안 체크 등을 할 수 있다. 제어기(10)는 하위 계층의 복수의 스위치(20)에서 발생하는 패킷의 플로우를 정의할 수 있다. 제어기(10)는 네트워크 정책 상 허용되는 플로우에 대해 네트워크 토폴로지 등을 참조하여 플로우가 경유할 경로(데이터 경로)를 계산한 후, 경로 상의 스위치에 상기 플로우의 엔트리가 설정되도록 할 수 있다. 제어기(10)는 특정 프로토콜, 예를 들어, 오픈플로우 프로토콜을 이용하여 스위치(20)와 통신할 수 있다. 제어기(10)와 스위치(20)의 통신 채널은 SSL에 의해 암호화 될 수 있다.
- [51] 도 2를 참조하면, 제어기(10)는 스위치(20)와 통신하는 스위치 통신부(110), 제어부(100), 및 저장부(190)를 포함할 수 있다.
- [52] 저장부(190)는 제어부(100)의 처리 및 제어를 위한 프로그램을 저장할 수 있다. 저장부(190)는 입력되거나 출력되는 데이터들(패킷, 메시지 등)을 임시 저장을 위한 기능을 수행할 수 있다. 저장부(190)는 플로우 엔트리를 저장하는 엔트리

- 데이터베이스(DB)(191)를 포함할 수 있다.
- [53] 제어부(100)는 통상적으로 상기 각 부의 동작을 제어하여 제어기(10)의 전반적인 동작을 제어할 수 있다. 제어부(100)는 토폴로지 관리 모듈(120), 경로 계산 모듈(125), 엔트리 관리 모듈(135) 및 메시지 관리 모듈(130)을 포함할 수 있다. 각 모듈은 제어부(100) 내에 하드웨어로 구성될 수 있고, 제어부(100)와 별개의 소프트웨어로 구성될 수도 있다.
- [54] 토폴로지 관리 모듈(120)은 스위치 통신부(110)를 통하여 수집된 스위치(20)의 접속 관계를 기초로 네트워크 토폴로지 정보를 구축 및 관리 할 수 있다. 네트워크 토폴로지 정보는 스위치들 사이의 토폴로지 및 각 스위치에 연결되어 있는 네트워크 디바이스들의 토폴로지를 포함할 수 있다. 토폴로지 정보는 저장부(190)에 저장될 수 있다.
- [55] 경로 계산 모듈(125)은 토폴로지 관리 모듈(120)에서 구축된 네트워크 토폴로지 정보를 기초로 스위치 통신부(110)를 통해 수신한 패킷의 데이터 경로 및 상기 데이터 경로 상의 스위치에서 실행될 액션 열을 구할 수 있다.
- [56] 엔트리 관리 모듈(135)은 경로 계산 모듈(125)에서 계산된 결과, QoS 등의 정책, 사용자 지시 등을 기초로 플로우 테이블, 그룹 테이블, 및 미터 테이블 등의 엔트리로서 엔트리 DB(191)에 등록할 수 있다. 엔트리 관리 모듈(135)은 스위치(20)에 미리 각 테이블의 엔트리가 등록되도록 하거나(proactive), 스위치(20)로부터의 엔트리의 추가 또는 갱신 요구에 응답(reactive)할 수 있다. 엔트리 관리 모듈(135)은 필요에 따라 또는 스위치(10)의 엔트리 소멸 메시지 등에 의해 엔트리 DB(191)의 엔트리를 변경하거나 삭제할 수 있다.
- [57] 메시지 관리 모듈(130)은 스위치 통신부(110)를 통해 수신한 메시지를 해석하거나, 스위치 통신부(110)를 통해 스위치로 전송되는 후술할 제어기-스위치 메시지를 생성할 수 있다. 제어기-스위치 메시지 중 하나인 상태 변경 메시지는 엔트리 관리 모듈(135)에 의해 생성된 엔트리 또는 엔트리 DB(191)에 저장된 엔트리에 기초하여 생성될 수 있다.
- [58] 스위치(20)는 오픈플로우 프로토콜을 지원하는 물리적인 스위치 또는 가상 스위치일 수 있다. 스위치(20)는 수신한 패킷을 처리하여, 네트워크 디바이스(30) 사이의 플로우를 중계할 수 있다. 이를 위해 스위치(20)는 하나의 플로우 테이블 또는 비특허문헌 1에 상술되어 있는 파이프라인(pipeline) 처리를 위해 다중 플로우 테이블을 구비할 수 있다.
- [59] 플로우 테이블은 네트워크 디바이스(30)의 플로우를 어떻게 처리할 지의 규칙을 정의한 플로우 엔트리를 포함할 수 있다.
- [60] 스위치(20)는 다중 스위치의 조합에 따른 플로우의 입구 및 출구 측 에지 스위치(edge switch)(ingress switch and egress switch)와 에지 스위치 사이의 코어 스위치(core switch)로 구분될 수 있다.
- [61] 도 3을 참조하면, 스위치(20)는 다른 스위치 및/또는 네트워크 디바이스와 통신하는 포트부(205), 제어기(10)와 통신하는 제어기 통신부(210), 스위치

- 제어부(200), 및 저장부(290)를 포함할 수 있다.
- [62] 포트부(205)는 스위치 또는 네트워크 디바이스와 연결된 한 쌍의 포트를 다수 구비할 수 있다. 한 쌍의 포트는 하나의 포트구로 구현될 수 있다.
- [63] 저장부(290)는 스위치 제어부(200)의 처리 및 제어를 위한 프로그램을 저장할 수 있다. 저장부(290)는 입력되거나 출력되는 데이터들(패킷, 메시지 등)을 임시 저장을 위한 기능을 수행할 수 있다. 저장부(290)는 플로우 테이블, 그룹 테이블, 및 미터 테이블 등의 테이블(291)을 구비할 수 있다. 테이블(230) 또는 테이블의 엔트리는 제어기(10)의 메시지에 기초하여 추가, 수정, 삭제될 수 있다. 테이블 엔트리는 스위치(20)에 의해 자체적으로 파괴될 수 있다.
- [64] 플로우 테이블은 오픈플로우의 파이프라인(pipeline)을 처리하기 위해 다중 플로우 테이블로 구성될 수 있다. 도 4를 참조하면, 플로우 테이블의 플로우 엔트리는 패킷과 매치하는 조건(대조 규칙)을 기술한 매치 필드(match fields), 우선 순위(priority), 매치되는 패킷이 있는 경우 업데이트되는 카운터(counters), 플로우 엔트리에 매치되는 패킷이 있으면 발생하는 다양한 액션들의 집합인 인스트럭션(instruction), 스위치에서 파괴될 시간을 기술하는 타임아웃(timeouts), 제어기에 의해 선택되어지는 오파큐(opaque) 타입으로, 제어기에 의해 플로우 통계, 플로우 변경, 및 플로우 삭제를 필터하기 위해 사용될 수 있으며, 패킷 처리시 사용되지 않는 쿠키(cookie) 등의 튜플(tuple)을 포함할 수 있다.
- [65] 인스트럭션(instruction)은 다른 플로우 테이블로 패킷을 전달하는 것과 같은 파이프라인 프로세싱을 변경할 수 있다. 또한 인스트럭션은 액션 셋(action set)에 액션을 더하는 액션(action)들의 집합, 또는 패킷에 바로 적용하기 위한 액션들의 리스트를 포함할 수 있다. 액션(action)은 특정 포트로 패킷을 전송하거나, TTL 필드를 감소시키는 것과 같이 패킷을 수정하는 작업을 의미할 수 있다. 액션은 플로우 엔트리와 연관된 인스트럭션 집합의 일부 또는 그룹 엔트리와 연관된 액션 버킷에 속할 수 있다. 액션 셋(action set)은 각 테이블에서 지시된 액션이 누적된 집합을 의미한다. 액션 셋은 매치되는 테이블이 없을 때 수행될 수 있다. 도 5는 플로우 엔트리에 의한 여러 패킷 처리를 예시한다.
- [66] 파이프라인(pipeline)은 패킷과 플로우 테이블 사이의 일련의 패킷 처리 과정을 의미한다. 스위치(20)에 패킷이 유입되면, 스위치(20)는 첫번째 플로우 테이블의 우선 순위가 높은 순서대로 패킷과 매칭되는 플로우 엔트리를 탐색한다. 매칭이 되면 해당 엔트리의 인스트럭션을 수행한다. 인스트럭션은 매칭되면 바로 수행하는 명령(apply-action), 액션 셋의 내용을 지우거나 추가/수정하는 명령(clear-action; write-action), 메타데이터(metadata) 수정 명령(write-metadata), 지정된 테이블로 메타데이터와 함께 패킷을 이동시키는 고우투 명령(goto-table) 등이 있다. 패킷과 매칭되는 플로우 엔트리가 없는 경우, 테이블 설정에 따라 패킷을 폐기(drop)하거나 제어기(10)로 패킷을 패킷-인 메시지(packet-in message)에 실어서 보낼 수 있다.
- [67] 그룹 테이블은 그룹 엔트리들을 포함할 수 있다. 그룹 테이블은 플로우

엔트리에 의해 지시되어 추가적인 포워딩 방법들을 제시할 수 있다. 도 5(a)를 참조하면, 그룹 테이블의 그룹 엔트리는 다음과 같은 필드를 구비할 수 있다. 그룹 엔트리를 구분할 수 있는 그룹 식별자(group identifier), 그룹 엔트리에 정의된 액션 버킷들을 일부(select) 또는 전부(all) 수행할 것이 여부에 대한 규칙을 명시한 그룹 타입(group type), 플로우 엔트리의 카운터와 같이 통계를 위한 카운터(counters), 및 그룹을 위해 정의된 파라미터들과 연관된 액션들의 집합인 액션 버킷(action buckets)을 포함할 수 있다.

- [68] 미터 테이블(meter table)은 미터 엔트리들(meter entries)로 구성되며, 플로우 미터-당(per-flow meters)을 정의한다. 플로우 미터-당은 오픈플로우가 다양한 QoS 작동을 적용될 수 있도록 할 수 있다. 미터(meter)는 패킷의 레이트(rate of packets)를 측정 및 제어할 수 있는 일종의 스위치 요소이다. 도 5(b)를 참조하면, 미터 테이블(meter table)은 미터를 식별하는 미터 식별자(meter identifier), 밴드(band)에 지정된 속도와 패킷 동작 방법을 나타내는 미터 밴드(meter bands), 및 패킷이 미터에서 동작될 때 업데이트되는 카운터(counters) 필드들로 구성된다. 미터 밴드(meter bands)는 패킷이 어떻게 처리되는 지를 나타내는 밴드 타입(band type), 미터에 의해 미터 밴드를 선택하는데 사용되는 레이트(rate), 미터 밴드에 의해 패킷들이 처리될 때 업데이트되는 카운터(counters), 및 선택적인 아규먼트(argument)를 가지는 밴드 타입들인 특정 아규먼트 타입(type specific argument)과 같은 필드들로 구성될 수 있다.
- [69] 스위치 제어부(200)는 통상적으로 상기 각 부의 동작을 제어하여 스위치(20)의 전반적인 동작을 제어할 수 있다. 스위치 제어부(200)는 테이블(291)을 관리하는 테이블 관리 모듈(240), 플로우 검색 모듈(220), 플로우 처리 모듈(230), 및 패킷 처리 모듈(235)를 포함할 수 있다. 각 모듈은 제어부(200) 내에 하드웨어로 구성될 수 있고, 제어부(200)와 별개의 소프트웨어로 구성될 수도 있다.
- [70] 테이블 관리 모듈(240)은 제어기 통신부(210)를 통해 제어기(10)로부터 수신한 엔트리를 적절한 테이블에 추가하거나, 타임 아웃(time out)된 엔트리를 주기적으로 제거할 수 있다.
- [71] 플로우 검색 모듈(220)은 유저 트래픽으로서 수신한 패킷으로부터 플로우 정보를 추출할 수 있다. 플로우 정보는 에지 스위치의 패킷 유입 포트인 입구 포트(ingress port)의 식별 정보, 해당 스위치의 패킷 유입 포트(incoming port)의 식별 정보, 패킷 헤더 정보(송신원 및 목적지의 IP 주소, MAC 주소, 포트, 및 VLAN 정보 등), 및 메타데이터 등을 포함할 수 있다. 메타데이터는 이전 테이블에서 선택적으로 추가되거나, 다른 스위치에서 추가된 데이터일 수 있다. 플로우 검색 모듈(220)은 추출한 플로우 정보를 참조하여 테이블(291)에 수신 패킷에 대한 플로우 엔트리가 있는지 검색할 수 있다. 플로우 검색 모듈(220)은 플로우 엔트리가 검색되면, 플로우 처리 모듈(260)에 검색된 플로우 엔트리에 따라 수신 패킷을 처리하도록 요청할 수 있다. 만일 플로우 엔트리 검색이 실패하면, 플로우 검색 모듈(220)은 수신 패킷 또는 수신 패킷의 최소한의

- 데이터를 제어기 통신부(210)를 통해 제어기(10)로 전송할 수 있다.
- [72] 플로우 처리 모듈(230)은 플로우 검색 모듈(220)에서 검색된 엔트리에 기술된 절차에 따라 패킷을 특정 포트 또는 다중 포트로 출력하거나, 드롭시키거나 또는 특정 헤더 필드를 수정하는 등의 액션을 처리할 수 있다.
- [73] 플로우 처리 모듈(230)은 플로우 엔트리의 파이프라인 프로세스를 처리하거나 액션을 변경하기 위한 인스트럭션을 실행하거나 다중 플로우 테이블에서 더 이상 다음 테이블로 갈 수 없을 때 액션 세트를 실행할 수 있다.
- [74] 패킷 처리 모듈(235)은 플로우 처리 모듈(230)에 의해 처리된 패킷을 플로우 처리 모듈(230)에서 지정한 포트부(205)의 하나 또는 2 이상의 포트에 실제로 출력할 수 있다.
- [75] 도 1(b)를 참조하면, SDN 네트워크 시스템은 오케스트레이터(1)를 더 포함할 수 있다. 오케스트레이터(1)는 가상 네트워크 디바이스, 가상 스위치 등을 생성, 변경 및 삭제할 수 있다. 오케스트레이터(1)에서 가상 네트워크 디바이스를 생성하는 경우, 오케스트레이터(1)는 가상 네트워크가 접속할 스위치의 식별 정보, 해당 스위치에 연결되는 포트 식별 정보, MAC 주소, IP 주소, 터넌트(tenant) 식별 정보 및 네트워크 식별 정보 등의 네트워크 디바이스의 정보를 제어기(10)로 제공할 수 있다.
- [76] 제어기(10) 및 스위치(20)는 오케스트레이터(1)와 별도의 인터페이스로 통신하거나, 제어기(10)의 스위치 통신부(110) 및 스위치(20)의 제어기 통신부(210)를 통해 오케스트레이터(1)와 통신할 수 있다. 스위치(20)는 제어기(10)를 통해 오케스트레이터(1)와 메시지를 주고 받을 수 있다.
- [77] 제어기(10)와 스위치(20)는 다양한 정보를 주고 받는데, 이를 오픈플로우 프로토콜 메시지(openflow protocol message)라 칭한다. 이러한 오픈플로우 메시지는 제어기-스위치 메시지(controller-to-switch message), 비동기 메시지(asynchronous message), 및 대칭 메시지(symmetrical message) 등의 타입이 있다. 각 메시지는 엔트리를 식별하는 트랜잭션 식별자(transaction id; xid)를 헤더에 구비할 수 있다.
- [78] 제어기-스위치 메시지는 제어기(10)가 생성하여 스위치(20)에 전달하는 메시지로써, 주로 스위치(20)의 상태를 관리하거나 점검하기 위해 사용된다. 제어기-스위치 메시지는 제어기(10)의 제어부(100), 특히 메시지 관리 모듈(130)에 의해 생성될 수 있다.
- [79] 제어기-스위치 메시지는 스위치의 능력(capabilities)을 문의하는 기능(features), 스위치(20)의 구성 매개 변수 등의 설정을 문의하고 설정하기 위한 설정(configuration), 오픈플로우 테이블의 플로우/그룹/미터 엔트리들을 추가/삭제/수정하기 위한 상태 변경 메시지(modify state message), 패킷-인 메시지를 통해 스위치로부터 수신한 패킷을 해당 스위치 상의 특정한 포트에 전송하도록 하는 패킷-아웃 메시지(packet-out message) 등이 있다. 상태 변경 메시지는 플로우 테이블 변경 메시지(modify flow table message), 플로우 엔트리

변경 메시지(modify flow entry message), 그룹 엔트리 변경 메시지(modify group entry message), 포트 변경 메시지(port modification message), 및 미터 엔트리 변경 메시지(meter modification message) 등이 있다.

- [80] 비동기 메시지는 스위치(20)가 생성하는 메시지로서, 스위치의 상태 변경 및 네트워크 이벤트 등을 제어기(10)에서 업데이트하기 위해 사용된다. 비동기 메시지는 스위치(20)의 제어부(200), 특히 플로우 검색 모듈(220)에 의해 생성될 수 있다.
- [81] 비동기 메시지로 패킷-인 메시지(packet-in message), 플로우 삭제 메시지(flow-removed), 에러 메시지 등이 있다. 패킷-인 메시지는 스위치(20)가 제어기(10)에게 패킷을 전송하여 패킷에 대한 제어를 받기 위해 사용된다. 패킷-인 메시지는 스위치(20)가 미지의 패킷을 수신한 경우, 데이터 경로를 요구하기 위해, 오픈플로우 스위치(20)에서 제어기(10)로 전송되는 수신 패킷 또는 그 사본의 전부 또는 일부를 포함하는 메시지이다. 유입 패킷에 연관된 엔트리의 액션이 제어기로 보내라고 정해져 있을 때에도 패킷-인 메시지가 사용된다. 삭제된 플로우(flow-removed) 메시지는 플로우 테이블에서 삭제할 플로우 엔트리 정보를 제어기(10)로 전달하기 위해 사용된다. 이 메시지는 제어기(10)가 스위치(20)에 해당 플로우 엔트리 삭제를 요청하였거나 플로우 타임아웃(timeout)에 의한 플로우 만기 처리(flow expiry process)에서 발생한다.
- [82] 대칭 메시지는 제어기(10) 및 스위치(20) 모두에서 생성되며, 상대방의 요청이 없어도 전송되는 특징이 있다. 제어기와 스위치 간에 연결을 개시할 때 사용되는 헬로(hello), 제어기 및 스위치 간 연결에 이상이 없음을 확인하기 위한 에코(echo), 및 제어기나 스위치에 의해 사용되며 문제를 반대측에 알리기 위한 에러 메시지(error message) 등을 포함할 수 있다. 에러 메시지는 대부분 제어기에 의해 개시된 요청에 따른 실패를 나타내기 위해 스위치에서 사용된다.
- [83]
- [84] 도 6은 본 발명의 일 실시예에 따른 통합 라우팅 시스템을 포함하는 네트워크 시스템의 블록 구성도, 도 7은 도 6의 네트워크 시스템의 가상화한 블록 구성도, 도 8은 본 발명의 다른 실시예에 따른 SDN 제어기의 블록 구성도, 도 9는 본 발명의 일 실시예에 따른 레거시 라우팅 에이전트의 블록 구성도이다.
- [85] 도 6에 도시된 네트워크는 복수의 스위치(SW1-SW5)로 구성된 스위치 그룹 중 오픈플로우 스위치의 플로우를 제어하는 제어기(10)를 포함하는 SDN 기반의 네트워크와 제1 내지 제3 레거시 라우터(R1-R3)의 레거시 네트워크가 혼용되어 있다. 본 명세서에서 SDN 기반의 네트워크는 오픈플로우 스위치로만 구성되거나, 오픈플로우 스위치와 기존의 스위치로 구성된 독립 네트워크를 의미한다. SDN 기반의 네트워크가 오픈플로우 스위치와 기존의 스위치로 구성되어 있는 경우, 스위치 그룹 중 네트워크 도메인의 에지에 배치되는 오픈플로우 스위치로 구성되는 것이 바람직하다.
- [86] 도 6을 참조하면, 본 발명에 따른 SDN 기반의 통합 라우팅 시스템은 제1 내지

제5 스위치(SW1-SW5)를 구비하는 스위치 그룹, 제어기(10), 및 레거시 라우팅 에이전트(300)를 포함할 수 있다. 동일하거나 유사한 구성요소에 대한 자세한 설명은 도 1 내지 도 5를 참조한다.

- [87] 제1 내지 제5 스위치(SW1-SW5) 중 외부 네트워크와 연결된 에지 스위치인 제1 및 제3 스위치(SW1, SW5)는 오픈플로우 프로토콜을 지원하는 오픈플로우 스위치이다. 오픈플로우 스위치는 물리적인 하드웨어, 가상화된 소프트웨어, 또는 하드웨어와 소프트웨어가 혼합된 형태일 수 있다.
- [88] 본 실시예에서, 제1 스위치(SW1)는 제11 포트(port 11)을 통해 제1 레거시 라우터(R1)에 연결된 에지 스위치이며, 제3 스위치(SW3)는 제32 및 제33 포트(port 32, port 33)를 통해 제2 및 제3 레거시 라우터(R2, R3)에 연결된 에지 스위치이다. 스위치 그룹은 제1 내지 제5 스위치에 연결된 복수의 네트워크 디바이스(미도시)를 더 포함할 수 있다.
- [89] 도 8을 참조하면, 제어기(10)는 스위치(20)와 통신하는 스위치 통신부(110), 제어부(100), 및 저장부(190)를 포함할 수 있다.
- [90] 제어기의 제어부(100)는 토폴로지 관리 모듈(120), 경로 계산 모듈(125), 엔트리 관리 모듈(135), 메시지 관리 모듈(130), 메시지 판단 모듈(140), 레거시 인터페이스 모듈(145)을 포함할 수 있다. 각 모듈은 제어부(100) 내에 하드웨어로 구성될 수 있고, 제어부(100)와 별개의 소프트웨어로 구성될 수도 있다. 동일한 도면 부호의 구성요소에 대한 설명은 도 2를 참조한다.
- [91] 스위치 그룹이 오픈플로우 스위치로만 구성된 경우, 토폴로지 관리 모듈(120) 및 경로 계산 모듈(125)의 기능은 도 1 내지 도 5에서 설명한 것과 동일하다. 스위치 그룹이 오픈플로우 스위치와 기존의 레거시 스위치로 구성된 경우, 토폴로지 관리 모듈(120)은 오픈플로우 스위치를 통해 레거시 스위치와의 접속 정보를 얻을 수 있다.
- [92] 레거시 인터페이스 모듈(145)은 레거시 라우팅 에이전트(300)와 통신할 수 있다. 레거시 인터페이스 모듈(145)은 토폴로지 관리 모듈(120)에서 구축한 스위치 그룹의 토폴로지 정보를 레거시 라우팅 에이전트(300)로 전송할 수 있다. 토폴로지 정보는 제1 내지 제5 스위치(SW1-SW5)의 접속 관계 정보 및 제1 내지 제5 스위치(SW1-SW5)에 연결되어 있는 복수의 네트워크 디바이스의 연결 또는 접속 정보를 포함할 수 있다.
- [93] 메시지 관리 모듈(130)은 오픈플로우 스위치로부터 수신한 플로우 문의 메시지에 구비된 플로우의 처리 규칙을 생성할 수 없는 경우, 해당 플로우를 레거시 인터페이스 모듈(145)을 통해 레거시 라우팅 에이전트(300)로 전송할 수 있다. 해당 플로우는 오픈플로우 스위치에서 수신한 패킷 및 패킷을 수신한 스위치의 포트 정보를 포함할 수 있다. 플로우의 처리 규칙을 생성할 수 없는 경우는 수신 패킷이 레거시 프로토콜로 구성되어 해석할 수 없는 경우, 및 경로 계산 모듈(125)이 레거시 패킷에 대한 경로를 계산할 수 없는 경우 등이 있을 수 있다.

- [94] 도 9를 참조하면, 레거시 라우팅 에이전트(300)은 SDN 인터페이스 모듈(345), 가상 라우터 생성부(320), 가상 라우터(340), 라우팅 처리부(330), 및 라우팅 테이블(335)을 포함할 수 있다.
- [95] SDN 인터페이스 모듈(345)은 제어기(10)와 통신할 수 있다. 레거시 인터페이스 모듈(145) 및 SDN 인터페이스 모듈(345) 각각은 제어기(10)와 레거시 라우팅 에이전트(300)의 인터페이스 역할을 할 수 있다. 레거시 인터페이스 모듈(145) 및 SDN 인터페이스 모듈(345)은 특정 프로토콜이나 특정 언어로 통신할 수 있다. 레거시 인터페이스 모듈(145) 및 SDN 인터페이스 모듈(345)은 제어기(10)와 레거시 라우팅 에이전트(300)이 주고 받는 메시지를 번역하거나 해석할 수 있다.
- [96] 가상 라우터 생성부(320)는 SDN 인터페이스 모듈(345)를 통해 수신한 스위치 그룹의 토폴로지 정보를 이용하여 가상 라우터(340)를 생성 및 관리할 수 있다. 가상 라우터(340)를 통해, 외부 레거시 네트워크 즉 제1 내지 제3 라우터(R1-R3)에서 스위치 그룹이 레거시 라우터로 취급될 수 있다.
- [97] 가상 라우터 생성부(320)는 가상 라우터(340)를 복수 개 생성할 수 있다. 도 7(a)는 가상 라우터(340)가 하나인 가상 레거시 라우터(v-R0)인 경우를, 도 7(b)는 가상 라우터(340)가 복수인 가상 레거시 라우터(v-R1, v-R2)인 경우를 도시한다.
- [98] 가상 라우터 생성부(320)는 가상 라우터(340)가 라우터 식별자 예를 들어, 룩백(lookback) IP 주소를 구비하도록 할 수 있다.
- [99] 가상 라우터 생성부(320)는 가상 라우터(340)가 스위치 그룹의 에지 스위치 즉 제1 및 제3 에지 스위치(SW1, SW3)의 에지 포트들과 대응하는 가상 라우터용 포트를 구비하도록 수 있다. 예를 들어 도 7(a)의 경우와 같이, v-R0 가상 레거시 라우터의 포트는 제1 스위치(SW1)의 제11 포트(port 11), 및 제3 스위치(SW3)의 제32 및 33 포트(port 32, port 33)의 정보를 그대로 이용할 수 있다.
- [100] 가상 라우터(340)의 포트는 패킷의 식별 정보에 연관될 수 있다. 패킷의 식별 정보는 패킷의 vLAN 정보, 이동통신망을 통해 접속되는 경우 패킷에 부가되는 터널(tunnel) 아이디 등의 태그 정보일 수 있다. 이 경우 오픈플로우 에지 스위치의 실질적인 포트 하나로 다수의 가상 라우터 포트를 생성할 수 있다. 패킷의 식별 정보에 연관되는 가상 라우터 포트는 가상 라우터(340)가 복수의 가상 레거시 라우터로 작동하도록 하는데 기여할 수 있다. 에지 스위치의 물리적 포트(실제 포트)만으로 가상 라우터를 생성하는 경우, 물리적 포트의 수에 제한을 받게 된다. 그러나 패킷 식별 정보에 연관시키는 경우, 이러한 제약 사항이 없어진다. 또한 기존의 패킷의 레거시 네트워크에서의 흐름과 유사하게 작동되도록 할 수 있다. 또한 사용자 또는 사용자 그룹 별로 가상의 레거시 라우터를 구동할 수 있다. 사용자 또는 사용자 그룹은 vLAN 또는 터널 아이디와 같은 패킷 식별 정보로 구분될 수 있다. 도 7(b)를 참조하면, 스위치 그룹은 복수의 가상 레거시 라우터(v-R1, v-R2)로 가상화되며, 복수의 가상 레거시 라우터(v-R1, v-R2)의 각 포트(vp 11~13, vp 21~23)는 패킷의 식별 정보에 각각 연관될 수 있다.

- [101] 도 7(b)를 참조하면, 복수의 가상 레거시 라우터(v-R1, v-R2)와 레거시 라우터의 접속은 제1 레거시 라우터(R1)의 하나의 실제 인터페이스가 분리된 여러개의 서브 인터페이스로 접속되거나, 제2 및 제3 레거시 라우터(R2, R3) 처럼 복수의 실제 인터페이스로 접속될 수 있다.
- [102] 가상 라우터 생성부(320)는, 제1 내지 제3 라우터(R1-R3)가 제1 내지 제5 스위치(SW1-SW5)에 연결된 복수의 네트워크 디바이스를 가상 라우터(340)에 연결된 외부 네트워크(vN)로 취급되도록 할 수 있다. 이를 통해 레거시 네트워크는 오픈플로우 스위치 그룹의 네트워크 디바이스들에 접근할 수 있다. 도 7(a)의 경우, 가상 라우터 생성부(320)는 제0 가상 레거시 라우터(v-R0)에 제0 포트(port 0)를 생성하였다. 도 7(b)의 경우, 가상 라우터 생성부(320)는 제1 및 제2 가상 레거시 라우터(v-R1, v-R2)에 제10 및 제20 포트(vp 10, vp 20)를 생성하였다. 생성된 각 포트(port 0, vp 10, vp 20)는 스위치 그룹에 복수의 네트워크 디바이스가 연결된 것과 같은 정보를 구비할 수 있다. 외부 네트워크(vN)은 복수의 네트워크 디바이스 전부 또는 그 일부로 구성될 수 있다.
- [103] 가상 라우터용 포트(port 0, port 11v, port 32v, port 33v, vp 10~13, vp 20~23)의 정보는 레거시 라우터가 가지는 포트 정보를 가질 수 있다. 예를 들어, 가상 라우터용 포트 정보는 각 가상 라우터용 포트의 MAC 주소, IP 주소, 포트 이름, 연결되어 있는 네트워크 주소 범위, 레거시 라우터 정보를 포함하며, vLAN 범위, 터널 아이디 범위 등을 더 포함할 수 있다. 이러한 포트 정보는 상술한 바와 같이 제1 및 제3 에지 스위치(SW1, SW3)의 에지 포트 정보를 상속 받거나, 가상 라우터 생성부(320)에 의해 지정될 수 있다.
- [104] 가상 라우터(340)에 생성된 가상 라우터(340)에 의한 도 6의 네트워크의 데이터 평면(data plane)은 도 7(a) 또는 도 7(b)와 같이 가상화될 수 있다. 예를 들어 도 7(a)의 경우, 가상화된 네트워크는 제1 내지 제5 스위치(SW1~SW5)가 가상 레거시 라우터(v-R0)로 가상화되고, 제0 가상 레거시 라우터(v-R0)의 제11v, 제32v, 및 제33v 포트(port 11v, 32v, 33v)는 제1 내지 제3 레거시 라우터(R1~R3)와 연결되고, 제0 가상 레거시 라우터(v-R0)의 제0 포트(port 0)는 복수의 네트워크 디바이스의 적어도 일부인 외부 네트워크(vN)와 연결될 수 있다.
- [105] 라우팅 처리부(330)는 가상 라우터(340)가 생성되면 라우팅 테이블(335)을 생성할 수 있다. 라우팅 테이블(335)은 레거시 라우터에서 라우팅에 참조되기 위해 사용되는 테이블이다. 라우팅 테이블(335)은 RIB, FIB, 및 ARP 테이블 등의 일부 또는 전부로 구성될 수 있다. 라우팅 테이블(335)은 라우팅 처리부(330)에 의해 수정되거나 업데이트 될 수 있다.
- [106] 라우팅 처리부(330)는 제어기(10)에서 문의한 플로우에 대한 레거시 라우팅 경로를 생성할 수 있다. 라우팅 처리부(330)는 플로우에 구비된 오픈플로우 스위치에서 수신한 수신 패킷, 수신 패킷이 유입된 포트 정보, 가상 라우터(340) 정보, 및 라우팅 테이블(335) 등의 일부 또는 전부를 이용하여 레거시 라우팅 정보를 생성할 수 있다.

- [107] 라우팅 처리부(330)는 레거시 라우팅을 결정하기 위해 서드 파티 라우팅 프로토콜 스택을 포함할 수 있다.
- [108] 도 10은 도 6의 제어기의 플로우에 대한 레거시 라우팅 여부 판단 방법에 대한 순서도이다. 도 6 내지 도 9를 참조한다.
- [109] 플로우에 대한 레거시 라우팅 여부 판단 방법은, 제어기(10)가 오픈플로우 스위치로부터 수신한 플로우에 대해 일반적인 SDN 제어를 할 것인지 또는 레거시 라우팅 에이전트(300)에 플로우 제어를 문의해야 하는지를 의미한다.
- [110] 도 10을 참조하면, 제어기(10)는 플로우 인입 포트가 에지 포트인지 판단한다(S510). 플로우 인입 포트가 에지 포트가 아닌 경우, 제어기(10)는 일반적인 오픈플로우 패킷에 대한 경로를 계산하는 등 SDN 기반의 플로우 제어를 할 수 있다(S590).
- [111] 플로우 인입 포트가 에지 포트인 경우, 제어기(10)는 해당 플로우의 패킷이 해석 가능한지 판단한다(S520). 패킷을 해석할 수 없는 경우, 제어기(10)는 플로우를 레거시 라우팅 에이전트(300)로 전달할 수 있다(S550). 패킷이 레거시 네트워크에서만 사용하는 프로토콜 메시지의 경우, SDN 기반의 일반적인 제어기는 패킷을 해석할 수 없기 때문이다.
- [112] 수신 패킷이 제1 레거시 네트워크에서 제2 레거시 네트워크로 전송되는 것과 같은 레거시 패킷인 경우, SDN 기반의 제어기(10)는 유입된 레거시 패킷의 라우팅 경로를 계산할 수 없다. 따라서 레거시 패킷과 같이 제어기(10)에서 경로를 계산할 수 없는 경우, 제어기(10)는 레거시 패킷을 레거시 라우팅 에이전트(300)로 보내야 바람직하다. 다만 레거시 패킷의 유출될 에지 포트와 레거시 패킷의 최종 처리 방법을 알면, 플로우 수정을 통해 제어기(10)에서 레거시 패킷을 처리할 수 있다. 이에 패킷을 해석할 수 있는 경우, 제어기(10)는 해당 플로우의 경로를 계산할 수 있는지 또는 엔트리 테이블에 엔트리가 있는지 등의 플로우 경로를 검색한다(S530). 경로를 검색할 수 없으면, 제어기(10)는 해당 플로우를 레거시 라우팅 에이전트(300)로 전달할 수 있다(S550). 경로를 검색할 수 있으면, 제어기(10)는 패킷의 출력을 지정하는 패킷-아웃 메시지를 생성하여 패킷 문의한 오픈플로우 스위치로 전송할 수 있다(S540). 이에 대한 자세한 예는 도 11 및 도 12에서 후술한다.
- [113] 도 11은 본 발명의 일 실시예에 따른 통합 라우팅 방법에 따른 신호 흐름도, 도 12는 본 발명의 다른 실시예에 따른 통합 라우팅 방법에 따른 신호 흐름도, 및 도 13은 본 발명의 일 실시예에 따른 플로우 테이블이다. 도 6 내지 도 10을 참조한다.
- [114] 도 11은 레거시 프로토콜 메시지를 본 발명이 적용된 SDN 기반의 네트워크에서 처리하는 흐름을 도시한다. 도 11은 그 일례로 제1 에지 스위치(SW1)에서 OSPF(Open Shortest Path First) 프로토콜의 헬로 메시지를 받은 경우이다.
- [115] 본 일례는 제어기(10) 및 레거시 라우팅 에이전트(300)에 의해 오픈플로우

스위치 그룹은 도 7(a)와 같이 가상화되어 있다고 가정한다.

- [116] 도 11을 참조하면, 제1 레거시 라우터(R1)와 제1 에지 스위치(SW1)가 연결되면 제1 레거시 라우터(R1)은 제1 에지 스위치(SW1)에게 OSPF 프로토콜의 헬로 메시지(Hello1)를 전송할 수 있다(S410).
- [117] 제1 에지 스위치(SW1)의 테이블(291)에 수신 패킷에 대한 플로우 엔트리가 없으므로, 제1 에지 스위치(SW1)는 알지 못하는 패킷(unkown packet)을 알리는 패킷-인 메시지를 제어기(10)로 전송한다(S420). 패킷-인 메시지는 Hello1 패킷 및 인입 포트(port 11) 정보를 구비하는 플로우를 포함하는 것이 바람직하다.
- [118] 제어기(10)의 메시지 관리 모듈(130)은 해당 플로우에 대한 처리 규칙을 생성할 수 있는지 판단할 수 있다(S430). 판단 방법에 대한 자세한 사항은 도 10을 참조한다. 본 예에서, OSPF 프로토콜 메시지는 제어기(10)가 해석할 수 없는 패킷이므로, 제어기(10)는 레거시 라우팅 에이전트(300)로 해당 플로우를 전달할 수 있다(S440).
- [119] 레거시 라우팅 에이전트(300)의 SDN 인터페이스 모듈(345)는 제어기(10)로부터 전달 받은 Hello1 패킷을 플로우에 구비된 제1 에지 스위치(SW1)의 인입 포트(port 11)와 대응하는 가상 라우터(340)의 포트(port 11v)로 전송할 수 있다. 가상 라우터(340)가 Hello1 패킷을 수신하면, 라우팅 처리부(330)는 라우팅 테이블(335)에 기반하여 Hello1 패킷의 레거시 라우팅 정보를 생성할 수 있다(S450). 본 실시예에서 라우팅 처리부(330)은 Hello1 메시지에 대응하는 Hello2 메시지를 생성하고, Hello2 패킷이 제1 레거시 라우터(R1)로 전송되도록 출력 포트를 제11v 포트(port 11v)로 지정하는 라우팅 경로를 생성할 수 있다. Hello2 메시지는 제1 레거시 라우터(R1)인 목적지 및 기지정된 가상 라우터 식별자를 구비한다. 레거시 라우팅 정보는 Hello2 패킷, 및 제11v 포트인 출력 포트를 포함할 수 있다. 본 실시예에서 가상 라우터(340)에 Hello1 패킷이 인입되는 것으로 기술하였지만 이에 한정되지 않고, 라우팅 처리부(330)가 가상 라우터(340)의 정보를 이용하여 레거시 라우팅 정보를 생성할 수 있다.
- [120] SDN 인터페이스 모듈(345)는 생성된 레거시 라우팅 정보를 제어기(10)의 레거시 인터페이스 모듈(145)로 전달할 수 있다(S460). SDN 인터페이스 모듈(345) 및 레거시 인터페이스 모듈(145) 중 어느 하나는 출력 포트인 제11v 포트(port 11v)를 제1 에지 스위치(SW1)의 제11 포트(port 11)로 변환할 수 있다. 또는 제11v 포트와 제11 포트의 이름을 동일하게 하여, 포트 변환을 생략할 수 있다.
- [121] 제어기(10)의 경로 계산 모듈(125)은 레거시 인터페이스 모듈(145)를 통해 수신한 레거시 라우팅 정보를 이용하여 Hello2 패킷이 제1 레거시 라우터(R1)의 제11 포트(port 11)로 출력되도록 하는 경로를 설정할 수 있다(S470).
- [122] 메시지 관리 모듈(130)은 설정된 경로와 레거시 라우팅 정보를 이용하여, Hello2 패킷이 인입 포트인 제11 포트(port 11)로 출력되도록 하는 패킷-아웃

- 메시지를 생성하여 제1 레거시 라우터(R1)로 전송할 수 있다(S480).
- [123] 본 실시예에서, 외부 레거시 라우터의 Hello 메시지에 대응하는 것으로 서술하였지만 이에 한정되지 않는다. 예를 들어, 레거시 라우팅 에이전트(300)는 능동적으로 에지 스위치의 에지 포트에 출력되도록 하는 OSPF 헬로 메시지를 생성하여, 제어기(10)로 전송할 수 있다. 이 경우 제어기(10)는 패킷-아웃 메시지로 헬로 패킷을 오픈플로우 스위치로 전송할 수 있다. 그리고, 패킷-인 메시지에 대응하지 않는 패킷-아웃 메시지라도 오픈플로우 스위치가 패킷-아웃 메시지의 지시대로 하도록 세팅함으로써 본 실시예를 구현할 수 있다.
- [124] 도 12는 일반적인 레거시 패킷이 제1 에지 스위치(SW1)에서 제3 에지 스위치(SW3)로 전송되는 경우를 도시한다.
- [125] 제1 에지 스위치(SW1)은 제1 레거시 라우터(R1)로부터 목적지 IP 주소가 오픈플로우 스위치 그룹에 속하지 않는 레거시 패킷 P1을 수신하는 것으로 시작한다(S610).
- [126] 제1 에지 스위치(SW1)는 패킷 P1에 대한 플로우 엔트리가 없으므로, 패킷 P1을 제어기(10)로 전송하며 플로우 처리를 문의(패킷-인 메시지)할 수 있다(S620).
- [127] 제어기(10)의 메시지 관리 모듈(130)은 해당 플로우에 대한 SDN 제어가 가능한지 판단할 수 있다(S630). 본 예에서, 패킷 P1은 해석 가능하나 레거시 네트워크를 향하므로, 제어기(10)는 패킷 P1의 경로를 생성할 수 없다. 이에 제어기(10)는, 레거시 인터페이스 모듈(145)을 통해, 패킷 P1 및 인입 포트인 제11 포트를 레거시 라우팅 에이전트(300)로 전송할 수 있다(S640).
- [128] 레거시 라우팅 에이전트(300)의 라우팅 처리부(330)는, 제어기(10)로부터 전달 받은 패킷 P1에 대해, 가상 라우터(340)의 정보 및 라우팅 테이블(335)에 기초하여 패킷 P1의 레거시 라우팅 정보를 생성할 수 있다(S650). 본 예에서 패킷 P1이 가상 라우터의 제32v 포트(port 32v)로 출력되어야 한다고 가정한다. 이 경우, 레거시 라우팅 정보는 패킷 P1에 대해 제32v 포트(port 32v)인 출력 포트, 제2 레거시 라우터(R2)의 MAC 주소인 목적지 MAC 주소, 및 제32v 포트의 MAC 주소인 소스(source) MAC 주소를 포함할 수 있다. 이러한 정보는 레거시 라우터에서 출력되는 패킷의 헤더 정보이다. 예를 들어, 제1 레거시 라우터(R1)에서 가상 레거시 라우터(v-R0)를 레거시 라우터로 보고 패킷 P1을 전송하는 경우, 패킷 P1의 헤더 정보는 다음과 같다. 소스 및 목적지 IP 주소는 패킷 P1이 생성하였을 때의 헤더 정보와 동일하므로, 본 설명에서 제하기로 한다. 패킷 P1의 소스 MAC 주소는 라우터(R1)의 출력 포트의 MAC 주소이다. 패킷 P1의 목적지 MAC 주소는 가상 레거시 라우터(v-R0)의 제11v 포트(port 11v)의 MAC 주소이다. 기존의 라우터라면, 가상 레거시 라우터(v-R0)의 제32v 포트(port 32v)로 출력되는 패킷 P1'는 다음과 같은 헤더 정보를 가질 수 있다. 패킷 P1'의 소스 MAC 주소는 가상 레거시 라우터(v-R0)의 제32v 포트(port 32v)의 MAC 주소이고, 목적지 MAC 주소는 제2 레거시 라우터의 인입 포트의 MAC 주소가 된다. 즉 레거시 라우팅시 패킷 P1의 헤더 정보의 일부가 변하게 된다.

- [129] 레거시 라우팅과 대응되도록 하기 위해, 라우팅 처리부(330)는 패킷 P1의 헤더 정보를 조정한 패킷 P1'를 생성하여 레거시 라우팅 정보에 포함시킬 수 있다.
- [130] 그러나, 라우팅 처리부(330)는 패킷 P1의 헤더 정보를 변경하는 패킷 P1'을 생성하지 않는 것이 더 바람직하다. 라우팅 처리부(330)에서 패킷의 헤더 정보를 조정하는 경우, 동일한 패킷, 또는 목적지 주소 범위가 동일한 유사한 패킷에 대해 매번 제어기(10) 또는 레거시 라우팅 에이전트(300)에서 유입 패킷을 처리해야 한다. 따라서, 패킷이 기존의 라우팅 이후의 포맷으로 변화시키는 단계는 레거시 라우팅 에이전트(300) 보다 패킷을 외부 레거시 네트워크로 출력하는 에지 스위치(본 예에서, 제3 에지 스위치(SW3))에서 패킷 조작을 하는 것이 바람직하다. 이를 위해, 앞서 설명한 레거시 라우팅 정보는 소스 및 목적지 MAC 주소를 포함할 수 있다. 제어기(10)는 이러한 라우팅 정보를 이용하여, 제3 에지 스위치에 패킷 P1의 헤더 정보를 변경하도록 하는 플로우 변경(flow-Mod) 메시지를 전송할 수 있다.
- [131] SDN 인터페이스 모듈(345)는 생성된 레거시 라우팅 정보를 제어기(10)의 레거시 인터페이스 모듈(145)로 전달할 수 있다(S660). 본 단계에서 출력 포트는 맵핑되는 에지 포트로 변환될 수 있다.
- [132] 제어기(10)는 레거시 인터페이스 모듈(145)를 통해 수신한 레거시 라우팅 정보, 특히 레거시 라우팅 정보의 레거시 경로를 이용하여 오픈플로우 스위치 그룹 내부의 플로우 처리 규칙을 생성할 수 있다.
- [133] 제어기(10)의 경로 계산 모듈(125)은 레거시 경로를 이용하여 제1 에지 스위치(SW1)에서 제3 에지 스위치(SW3)의 제32 포트에 출력되도록 하는 경로를 계산할 수 있다(S670).
- [134] 메시지 관리 모듈(130)은 계산된 경로를 기초로, 제1 에지 스위치(SW1)에 패킷 P1에 대한 출력 포트를 지정하는 패킷-아웃 메시지를 전송하고(S680), 해당 경로의 오픈플로우 스위치에 플로우 변경(flow-Mod) 변경 메시지를 전송할 수 있다(S690, S700). 메시지 관리 모듈(130)은 제1 에지 스위치(SW1)로 동일한 플로우에 대한 처리를 규정하도록 플로우 변경(flow-Mod) 메시지도 전송할 수 있다.
- [135] 플로우 처리 규칙에 따른 플로우 엔트리는 패킷 P1의 패스(path)을 관리하는 플로우에 대응하는 데이터-패킷임을 식별하는 식별자에 기초하는 것이 바람직하다. 즉, 패킷 P1에 대한 플로우 처리는 레거시 플로우임을 식별할 수 있는 식별자에 기초하여 이루어 지는 것이 바람직하다. 이를 위해 제1 에지 스위치(SW1)으로 전송되는 패킷-아웃 메시지에 레거시 식별자(tunnel ID)가 부가된 패킷 P1을 포함하도록 하고, 플로우 변경 메시지는 레거시 식별자(tunnel ID)가 부가되도록 하는 플로우 엔트리를 포함하도록 할 수 있다. 각 스위치의 플로우 테이블의 일례는 도 13을 참조한다. 도 13(a)는 제1 에지 스위치(SW1)의 플로우 테이블이다. 예를 들어, 도 13(a)의 테이블 0은 제2 레거시 라우터(R2)로 향하는 플로우에 레거시 식별자로 tunnel2를 플로우에 부가하고 테이블 1로

플로우가 이동되도록 한다. 레거시 식별자는 메타필드나 다른 필드에 기입될 수 있다. 테이블 1은 tunnel2를 가지는 플로우가 제14 포트(제4 스위치(SW4)와 연결된 제1 스위치(SW1)의 포트 정보)로 출력되도록 하는 플로우 엔트리를 구비한다. 도 13(b)는 제4 스위치(SW4)의 플로우 테이블의 예시이다. 도 13(b)의 테이블은 플로우 정보 중 레거시 식별자가 tunnel2인 플로우가 제3 스위치(SW3)와 연결된 제43 포트(port 43)로 출력되도록 한다. 도 13(c)는 제3 스위치(SW3)의 플로우 테이블의 예시이다. 도 13(c)의 테이블 0은 레거시 식별자가 tunnel2인 플로우의 레거시 식별자를 제거하고 해당 플로우를 테이블 1로 이동되도록 한다. 테이블 1은 해당 플로우를 제32포트로 출력하도록 한다. 이와 같이 다중 테이블을 이용하면, 경우의 수를 줄일 수 있다. 이는 신속한 검색을 가능하게 하고, 메모리 등의 자원 소모를 줄일 수 있다.

- [136] 제1 에지 스위치(SW1)는 레거시 식별자(tunnel ID)를 패킷 P1에 부가하거나(S710), 레거시 식별자(tunnel ID)가 부가된 패킷을 코어 네트워크로 전송할 수 있다(S720). 코어 네트워크는 에지 스위치(SW1, SW3)가 아닌 오픈플로우 스위치(SW2, SW4, SW5)로 구성된 네트워크를 의미한다.
- [137] 코어 네트워크는 해당 플로우를 제3 에지 스위치(SW3)로 전송할 수 있다(S730). 제3 에지 스위치(SW3)는 레거시 식별자를 제거하고 지정된 포트에 패킷 P1을 출력할 수 있다(S740). 이 경우, 도 13의 플로우 테이블에 도시하지는 않았지만, 제3 스위치(SW3)의 플로우 테이블은 패킷 P1의 목적지 및 소스 MAC 주소를 변경하도록 하는 플로우 엔트리를 구비하는 것이 바람직하다.
- [138]
- [139] 도 14는 본 발명의 일 실시예에 따른 컨테이너 네트워크 관리 시스템을 도시하는 구조도, 도 15는 도 14의 호스트의 내부 구조를 중점적으로 나타내는 호스트의 블록 구성도, 도 16은 본 발명의 일 실시예에 따른 컨테이너 생성 방법의 순서도, 도 17은 도 14의 다른 호스트 내부 구조를 도시하는 구조도, 도 18은 도 14를 간략히 도시한 구조도, 도 19는 도 18을 레거시 가상 라우터로 변환한 네트워크 구조도이다. 도 1 내지 도 13을 참조한다.
- [140] 도 14를 참조하면, 컨테이너 네트워크 관리 시스템은, 오케스트레이터(1), 제어기(10), 레거시 라우팅 에이전트(300), 및 복수의 호스트(800-1, 800-2; 이하, '800'으로 하나 또는 전체를 지정하기로 함)를 포함할 수 있다.
- [141] 오케스트레이터(1)는 사용자 요청이나 정책에 따라 각 호스트(800-1, 800-2)에 컨테이너 생성/삭제하도록 하고, 내부 네트워크 환경을 제어하며, 각 호스트(800-1, 800-2)의 컨테이너 간의 네트워크를 관리할 수 있다. 오케스트레이터(1)는 제어기(10)를 통해 각 호스트(800-1, 800-2)를 제어할 수 있다.
- [142] 레거시 라우팅 에이전트(300)는 제어기(10)로부터 패킷의 처리 요청을 받으면, 해당 패킷의 레거시 라우팅 정보를 생성하여 제어기(10)로 전송할 수 있다. 필요에 따라 레거시 라우팅 에이전트(300)는 패킷이 레거시 프로토콜에

적합하도록 하는 레거시 프로토콜 변환 정보를 생성하거나 패킷을 레거시 프로토콜에 적합하도록 변환할 수 있다. 레거시 프로토콜은 레거시 라우팅 프로토콜을 포함한다.

- [143] 생성된 라우팅 정보나 프로토콜 변환 정보는 제어기(10) 또는 각 호스트(800-1, 800-2)에 테이블로 저장될 수 있으며, 이 경우 제어기(10)는 레거시 라우팅 에이전트(300)로 패킷의 처리를 문의할 필요가 없다.
- [144] 호스트(800)는 SDN 기반의 가상 스위치 및 컨테이너를 제공할 수 있다. 호스트(800)는 물리적 기반의 컴퓨팅 기능을 가지는 서버일 수 있으며, 이에 한정되지 않는다. 도 15를 참조하면, 호스트(800)는 호스트 제어부(810), SDN 기반의 가상 스위치(820)(vSW), 컨테이너 브리지(830), 컨테이너(840), 호스트 저장부(860)(DB), 및 실제 네트워크 인터페이스(850, 852)를 포함할 수 있다.
- [145] 호스트 저장부(860)는 호스트 제어부(810)의 처리 및 제어를 위한 프로그램을 저장할 수 있다. 호스트 저장부(860)는 후술할 브리지 넷 정보 및 컨테이너 넷 정보를 DB 형식의 리스트로 저장할 수 있다. 또한 호스트 저장부(860)는 가상 스위치(820)에 필요한 데이터를 저장하거나 여러 식별자들을 저장할 수 있다.
- [146] 호스트 제어부(810)는 호스트(800)의 각 요소들의 동작을 제어하여 호스트(800) 전반적인 동작을 제어할 수 있다. 호스트 제어부(810)는 가상 스위치(820), 컨테이너 브리지(830), 및 컨테이너(840)를 생성할 수 있다. 호스트 제어부(810)는 가상 스위치(820), 컨테이너 브리지(830), 및 컨테이너(840) 등이 서로 네트워크가 가능하도록 네트워크 커플링할 수 있다.
- [147] 호스트 제어부(810)는 제1 및 제2 실제 네트워크 인터페이스(850, 852)를 통해 제어기(10) 및/또는 외부 공용 네트워크(5)(예를 들어, '인터넷')과 데이터를 주고 받을 수 있다. 제1 및 제2 실제 네트워크 인터페이스(850, 852)는 하나의 네트워크 인터페이스로 구현될 수도 있다.
- [148] 가상 스위치(820)는 도 1의 스위치(20)에 대응될 수 있다. 가상 스위치(820)은 도 6의 스위치 그룹 중 특히 에지 스위치에 대응될 수 있다. 가상 스위치(820)는 호스트 제어부(810)에 의해 가상으로 생성될 수 있다. 가상 스위치(820)는 제1 실제 네트워크 인터페이스(850)를 통해 제어기(10)와 메시지를 주고 받을 수 있다. 가상 스위치(820)는 제2 실제 네트워크 인터페이스(852)를 통해 외부 네트워크(5)와 패킷을 주고 받을 수 있다. 호스트 제어부(810)에 의해 제2 실제 네트워크 인터페이스(852)는 가상 스위치(820)의 네트워크 인터페이스처럼 작동될 수 있다. 가상 스위치(820)는 동일 호스트 내의 컨테이너 사이 및/또는 다른 호스트의 각 컨테이너 사이의 L2/L3 네트워크를 수행할 수 있다.
- [149] 컨테이너 브리지(830)는 호스트 제어부(810)에 의해 생성되며, 동일 서버(호스트) 내의 컨테이너 간의 브릿지 역할을 할 수 있다. 컨테이너 브리지(830)는 기존 네트워크 장비 중 허브, 브리지(bridge) 및/또는 스위치의 역할을 할 수 있다. 컨테이너 브리지(830)는 컨테이너 간의 L2 네트워크 기능을 수행할 수 있다.

- [150] 컨테이너 브리지(830)는, 서로 다른 도메인(네트워크)에 속한 컨테이너 간의 라우팅, 다른 호스트에 속한 컨테이너와의 네트워크, 패킷의 목적지가 가상 스위치(820)에 연관된 경우, 및/또는 컨테이너로부터의 유입 패킷에 대한 처리 정보가 없는 경우, 컨테이너로부터의 유입 패킷을 가상 스위치(820)로 전송할 수 있다.
- [151] 컨테이너 브리지(830)는, 브리지-스위치 NI(네트워크 인터페이스; Network Interface)(832)를 통해, 가상 스위치(820)의 가상 NI(821)와 가상으로 네트워크 커플링될 수 있다. 컨테이너 브리지(830)는, 브리지-컨테이너(831)를 통해, 컨테이너(840)의 가상 NI(841)와 네트워크 커플링될 수 있다.
- [152] 컨테이너 브리지(830)는 자신을 식별하는 브리지 식별자를 구비할 수 있다. 브리지 식별자는 컨테이너 브리지(830)에서 구축하는 서버 네트워크 환경을 다른 네트워크 환경과 구별되도록 할 수 있다. 브리지 식별자는 네트워크 서버넷 정보 및 게이트웨이 정보와 연결될 수 있다. 네트워크 서버넷 정보는 컨테이너(840)에 할당될 IP 주소에 필요하며, 게이트웨이 정보는 라우팅에 필요하다. 게이트웨이 정보는 외부 네트워크(5)와 연결된 제2 실제 네트워크 인터페이스(852)에 대한 정보(IP 주소, Mac 주소 등)를 초기에 디폴트로 가질 수 있다. 브리지 식별자를 기초로 연결된 네트워크 서버넷 정보 및 게이트웨이 정보는 브리지 넷 정보로 DB화 될 수 있다. 네트워크 서버넷 정보는 2 이상의 서버 네트워크가 구축되도록 복수의 정보를 구비할 수 있다. 복수의 네트워크 서버넷 정보는 후술할 도메인 태그로 구획될 수 있다.
- [153] 컨테이너(840)는 애플리케이션들(applications)이 독립적으로 동작하는 일종의 가상 머신이지만, 기존 가상 머신과는 달리 OS를 공유하여 가상 머신에 비해 가볍게 동작할 수 있는, 일종의 경량화된 가상 머신이다. 컨테이너(840)는 하나 또는 2 이상의 서비스를 제공할 수 있다.
- [154] 컨테이너(840)는 OS 상에서 독립적인 네트워크 환경을 구축하고, 해당 네트워크 환경에서 가상 인터페이스를 통해 네트워크 토폴로지를 구성할 수 있다. OS가 리눅스인 경우, 독립 네트워크 환경은 네임 스페이스 기술로 구현될 수 있다. 본 발명은 특히, 컨테이너(840)들 사이의 네트워킹 방법에 관련된다.
- [155] 컨테이너(840)는 컨테이너 식별자를 구비한다. 컨테이너(840)는 상위 컨테이너 브리지(830)의 브리지 식별자를 상속받을 수 있다. 컨테이너(840)는 동일한 도메인을 지시하는 동일 도메인 식별자를 구비할 수 있다. 컨테이너(840)는 IP 주소를 구비하며, 해당 IP 주소는 DHCP 서버(미도시)에 의해 브리지 넷 정보를 기초로 생성될 수 있다. DHCP 서버는 호스트(800) 외부에 배치되는 것이 바람직하다. 다른 호스트에도 IP 주소를 생성해야 하기 때문이다. DHCP 서버는 가상으로 구현될 수 있으며, 이 경우, DHCP 서버는 제어기(10) 및/또는 레거시 라우팅 에이전트(300) 내부에 생성될 수 있다. 컨테이너 식별자를 키로 IP 주소 및 동일 도메인 식별자는 컨테이너 넷 정보 리스트로 저장될 수 있다.
- [156] 컨테이너 브리지(830)는 컨테이너(840)의 동일 도메인 식별자를 기초로

- 브리지-컨테이너 NI(831)에 동일 도메인 식별자와 대응하는 도메인 태그를 지정할 수 있다. 동일 도메인 식별자와 도메인 태그는 동일할 수 있다.
- [157] 컨테이너 브리지(830)는 컨테이너(840)으로부터 유입되는 패킷에 패킷이 유입되는 브리지-컨테이너 NI(831)에 지정된 태그를 태깅할 수 있다. 도메인 태그는 vLAN, vxLAN 등의 패킷 필드, 또는 메타데이터가 사용될 수 있다.
- [158] 컨테이너 브리지(830)는 패킷에 태깅된 도메인 태그가 지정된 브리지-컨테이너 NI(831)로 패킷을 유출할 수 있다. 이에 의해, 컨테이너 브리지(830)는 동일 호스트 및 동일 네트워크에서의 컨테이너 통신을 제공할 수 있다. 이에 따라, 불필요한 브로드캐스트나 멀티캐스트 트래픽을 줄일 수 있다. 컨테이너 브리지(830)의 브리지-스위치 NI(832)에서 유출 및/또는 유입하는 패킷은 유출입 패킷의 도메인 태그와 무관하게 유출입할 수 있다.
- [159] 브리지-컨테이너 NI(831) 및 브리지-스위치 NI(832)는 각각 연관된 맥 주소를 구비할 수 있다. 브리지-컨테이너 NI(831)는 ARP 프로토콜을 사용하거나, 제어기(10)로부터 수신한 정보로부터 각 컨테이너의 맥 주소를 알 수 있다. 제어기(10)로부터 수신한 맥 정보는 리스트의 일원으로 미리 저장된 컨테이너 넷 정보로부터 취득될 수 있다. 브리지-스위치 NI(832)는 게이트웨이의 맥 주소(제2 실제 네트워크 인터페이스(852) 또는 후술할 가상 맥 주소), 다른 호스트의 동일 도메인에 속한 컨테이너의 맥 주소를 구비할 수 있다. 이에 따라 컨테이너 브리지(830)는 유입 패킷의 목적지 맥 주소를 통해 유입 패킷을 브리지-컨테이너 NI(831) 및 브리지-스위치 NI(832) 중 적절한 NI로 유출할 수 있다. 브리지-컨테이너 NI(831) 및 브리지-스위치 NI(832) 중 유입 패킷의 맥 주소에 연관된 NI가 없는 경우, 컨테이너 브리지(830)는 유입 패킷을 브리지-스위치 NI(832)로 유출할 수 있다.
- [160] 도 16을 참조하면, 호스트 제어부(810)는 가상 스위치(820)를 생성할 수 있다(S900). 가상 스위치(820)의 생성은 호스트(800)가 부팅되면서 생성되거나, 오케스트레이터(1) 또는 제어기(10)로부터 컨테이너 생성 메시지나 컨테이너 브리지 생성 메시지를 수신하면 생성될 수 있다.
- [161] 호스트 제어부(810)는, 가상 스위치(820)가 제2 실제 네트워크 인터페이스(852)를 통해 외부 네트워크(5)와 패킷을 주고 받을 수 있도록, 가상 스위치(820)와 제2 실제 네트워크 인터페이스(852)를 연결할 수 있다(S905).
- [162] 호스트 제어부(810)는, 오케스트레이터(1) 또는 제어기(10)로부터 컨테이너 브리지 생성을 지시하는 메시지를 수신하면, 컨테이너 브리지(830)를 생성할 수 있다(S910). 컨테이너 브리지 생성 메시지는 브리지 식별자, 게이트웨이 정보, 및 네트워크 서브넷 정보를 구비할 수 있다. 호스트 제어부(810)는 동일한 브리지 식별자가 있는 경우, 실패 메시지를 제어기(10)로 전송할 수 있다.
- [163] 앞서 설명한 바와 같이, 네트워크 서브넷 정보는 도메인 태그의 개수 이상의 서브 네트워크를 구축될 수 있다. 2 이상의 서브 네트워크를 구축하는 복수의 서브넷 정보는 도메인 태그 또는 동일 도메인 식별자에 연관될 수 있다. 이에

컨테이너 브리지 생성 메시지는 동일 도메인 식별자(또는 도메인 태그) 리스트를 더 구비할 수 있다. 도메인 태그 리스트의 원소들과 네트워크 서브넷 정보의 복수의 서브넷 정보 각각은 서로 연관된다.

- [164] 호스트 제어부(810)는 가상 스위치(820)과 컨테이너 브리지(830) 각각의 가상 NI를 네트워크 커플링할 수 있다(S915). 패킷은 자신의 도메인 태그와 무관하게 컨테이너 브리지(830)에서 가상 스위치(820)로 전달될 수 있다.
- [165] 호스트 제어부(810)는, 오케스트레이터(1) 또는 제어기(10)로부터 컨테이너 생성을 지시하는 메시지를 수신하면(S925), 컨테이너(840)를 생성할 수 있다(S930). 컨테이너 생성 메시지는 브리지 식별자, 컨테이너 식별자, 및 동일 도메인 식별자를 구비할 수 있다. 호스트 제어부(810)는 동일한 컨테이너 식별자가 존재하거나, 브리지 식별자가 존재하지 않는 경우, 에러 처리할 수 있다.
- [166] 호스트 제어부(810)는, DHCP 기능을 이용하여, 컨테이너(840)에 고유 IP 주소를 할당할 수 있다(S935). 또한 호스트 제어부(810)는 컨테이너 브리지(830) 및 컨테이너(840)를 네트워크 커플링할 수 있다(S840).
- [167] 호스트 제어부(810)는 컨테이너(840)의 동일 도메인 식별자에 연관된 도메인 태그를 브리지-컨테이너 NI(831)에 지정할 수 있다(S845).
- [168]
- [169] 호스트(800)는 다양한 가상 스위치와 컨테이너 브리지를 가지는 실시예로 구현될 수 있다. 도 17을 참조하면, 첫 번째 호스트(800-3)과 같이 하나의 가상 스위치에 두 개의 컨테이너 브리지를 구비하거나, 세 번째 호스트(800-5)와 같이 두 개의 가상 스위치를 구비할 수 있다. 첫 번째 및 세 번째 호스트(800-3, 800-5)는 두 번째 호스트(800-4)와 같이 취급될 수 있다. 이는 브리지-스위치 NI(832)와 가상 스위치(820)의 가상 NI(821)의 연결 구조를 트렁크 구조 또는 복수의 서브 채널로 구성함으로써 구현될 수 있다. 또한 두 개 이상의 호스트를 하나의 호스트인 것처럼 제어할 수 있다. 두 개 이상의 호스트는 첫 번째 호스트(800-3)과 두 번째 호스트(800-4)와 같이, 외부의 다른 스위치로 연결되거나, 두 번째 호스트(800-4)와 세 번째 호스트(800-5)와 같이 다른 네트워크를 가로지르는 터널링을 통해 연결될 수 있다. 다른 네트워크는 두 번째 호스트(800-4)에 연결된 외부 네트워크(5)와 동일할 수 있다. 도 17의 외부 네트워크(5)에 직접 연결되지 않은 가상 스위치(vSW)는 도 6의 코어 네트워크를 구성하는 스위치에 대응할 수 있다.
- [170] 이하, 단순한 구조 및 설명을 위해, 본 발명의 일실시예에 다른 도 14의 호스트의 내부 구조 및 연결 구조를 도 18과 같다고 가정하고 서술한다. 제1 및 제2 호스트(h1, h2)는 하나의 레거시 라우터(R0)를 통해 연결되어 있으며, 제1 호스트(h1)는 제1 가상 스위치(vSW1), 제1 컨테이너 브리지(CT.Br.1), 및 제1 내지 제3 컨테이너(ct1, ct2, ct3)를 구비하며, 제2 호스트(h2)는 제2 가상 스위치(vSW2), 제2 컨테이너 브리지(CT.Br.2), 및 제4 내지 제5 컨테이너(ct4,

ct5)를 구비한다. 도메인 태그는 vLAN을 사용하기로 하며, 제1, 제2, 및 제4 컨테이너(ct 1, 2, 4)는 vLAN 100을 가지는 브리지-컨테이너 NI에 각각 연결되고, 제3 및 제5 컨테이너(ct3, ct5)는 vLAN 200을 가지는 브리지-컨테이너 NI에 각각 연결되어 있다.

- [171] 도 17의 제1 및 제2 호스트(h1, h2)는, 레거시 라우팅 에이전트(300)에 의해, 레거시 라우터(R0)에서 도 19과 같은 토폴로지 구조로 해석될 수 있다. 제1 및 제2 호스트(h1, h2)는 도 19(a)와 같이 레거시 라우터(R0)에 연결된 실제 네트워크 인터페이스를 각각 가상 포트로서 하는 제1-0 및 제2-0 가상 라우터들(vR.I.0, vR.II.0)로 구현되거나, 도 19(b)와 같이 도메인 태그 별로 생성되는 제1-1, 제1-2, 제2-1, 및 제2-2 가상 라우터들(vR.I.1, vR.I.2, vR.II.1, vR.II.2)로 구현될 수 있다. 제1 내지 제5 컨테이너(ct1~ct5)는 도 7의 외부 네트워크(vN)에 대응될 수 있다.
- [172] 제1-0 및 제2-0 가상 라우터들(vR.I.0, vR.II.0)의 레거시 라우터(R0)와 연결된 가상 포트 정보들(P.vR.I.0, P.vR.II.0)은 제1 및 제2 호스트(h1, h2)의 실제 네트워크 인터페이스(IP 주소 및 맥 주소)를 각각 구비하는 것이 바람직하다.
- [173] 제1-1, 제1-2, 제2-1, 및 제2-2 가상 라우터들(vR.I.1, vR.I.2, vR.II.1, vR.II.2)의 레거시 라우터(R0)와 연결된 가상 포트 정보들(P.vR.I.1, P.vR.I.2, P.vR.II.1, P.vR.II.2)은 가상의 맥 주소를 구비하고, 레거시 라우터(R0)와 동일한 네트워크를 구비하는 IP 주소를 구비하는 것이 바람직하다.
- [174]
- [175] 도 20 내지 도 23은 한 컨테이너에서 다른 컨테이너로의 패킷 흐름에 관한 신호 흐름도이다. 도 1 내지 도 19, 특히, 도 14 내지 도 19를 참조한다. 이하, 설명의 단순화를 위해, 도 18의 네트워크 토폴로지 구조는 도 19(a)로 가정하고 설명한다. 또한, 각 컨테이너, 컨테이너 브리지, 및/또는 가상 스위치는 ARP 메시지나 제어기(10)(ctr)로부터 동일 도메인에 속하는 다른 컨테이너의 맥 주소를 알고 있다고 가정하며, 컨테이너는 하나의 가상 포트만을 구비한다고 가정한다.
- [176] 도 20은 동일 호스트 및 동일 도메인에 속하는 제1 컨테이너(ct1)에서 제2 컨테이너(ct2)로의 패킷 흐름을 도시한다. 제1 및 제2 컨테이너(ct1, ct2)는 동일 도메인에 속하므로, 제1 컨테이너(ct1)에 의해 생성된 제1 패킷(pk1)은 제2 컨테이너(ct2)의 IP 및 맥주소(a2, m2)를 목적지 IP 및 맥 주소로 가진다.
- [177] 제1 컨테이너(ct1)는 제1 패킷(pk1)을 제1 컨테이너 브리지(CT.Br.1)로 전달할 수 있다(S1010). 제1 컨테이너 브리지(CT.Br.1)는 맥주소 m2에 연관된 브리지-컨테이너 NI를 알고 있으므로, 제1 패킷(pk1)을 직접 제2 컨테이너(ct2)로 전달할 수 있다(S1020).
- [178] 도 21은 동일 호스트 및 이종 도메인에 속하는 제1 컨테이너(ct1)에서 제3 컨테이너(ct3)로의 패킷 흐름을 도시한다. 제1 및 제3 컨테이너(ct1, ct3)는 서로 다른 도메인에 속하므로, 제1 컨테이너(ct1)는 목적지의 맥 주소를 게이트웨이 주소, 즉 제1 호스트(h1)의 실제 네트워크 인터페이스의 맥 주소(m.h1)로 하는

- 제2 패킷(pk2)을 생성할 수 있다. 제1 컨테이너(ct1)는 생성된 제2 패킷(pk2)을 제1 컨테이너 브리지(CT.Br.1)로 전달할 수 있다(S1110).
- [179] 제1 컨테이너 브리지(CT.Br.1)는 제1 컨테이너(ct1)에 연관된 도메인 태그(100)를 vLAN 필드에 태깅할 수 있다(S1115). 제1 컨테이너 브리지(CT.Br.1)는, 게이트웨이인 맥주소 m.h1에 연관된 브리지-스위치 NI를 통해, 제1 가상 스위치(vSW1)로 vLAN이 100인 제2 패킷(pk2[100])을 전달할 수 있다(S1120).
- [180] 제1 가상 스위치(vSW1)는 제2 패킷(pk2[100])의 목적지 IP 주소의 플로우 엔트리가 있는지 판단할 수 있다. 플로우 엔트리가 없으면, 제1 가상 스위치(vSW1)는, 플로우 처리 정보를 요청하기 위해, 제어기(10)로 제2 패킷(pk2[100])을 전송할 수 있다(S1130).
- [181] 제어기(10)는 제2 컨테이너(ct2)의 네트워크 정보를 알고 있으므로, 제2 패킷(pk2)의 플로우 처리 정보를 생성할 수 있다. 제어기(10)는 제2 패킷(pk2)의 vLAN을 100에서 제2 컨테이너(ct2)가 속한 도메인 태그 200으로 변환하고, 목적지 및 소스 맥 주소를 (m.h1/m1)에서 (m2/m.h1)으로 변환할 수 있다(S1135). 단계 S1135는 제1 가상 스위치(vSW1)에서 행해질 수도 있다.
- [182] 맥 주소 및 vLAN이 변환된 제2 패킷(pk2[200])은 제어기(10)에서 제1 가상 스위치(vSW1)로(S1140), 제1 가상 스위치(vSW1)에서 제1 컨테이너 브리지(CT.Br.1)로(S1150), 및 제1 컨테이너 브리지(CT.Br.1)에서 제2 컨테이너(ct2)로(S1160) 각각 전달될 수 있다. 제1 컨테이너 브리지(CT.Br.1)는 제2 패킷(pk2)의 vLAN 정보를 제거한 후, 제2 컨테이너(ct2)로 전달할 수도 있다.
- [183] 도 22는 이중 호스트 및 동일 도메인에 속하는 제1 컨테이너(ct1)에서 제4 컨테이너(ct4)로의 패킷 흐름을 도시한다. 제1 및 제4 컨테이너(ct1, ct4)는 동일 도메인에 속하므로, 제1 컨테이너(ct1)는 목적지의 맥 주소를 제4 컨테이너(ct4)의 맥 주소(m4)로 하는 제3 패킷(pk3)을 생성할 수 있다. 제1 컨테이너(ct1)는 생성된 제3 패킷(pk3)을 제1 컨테이너 브리지(CT.Br.1)로 전달할 수 있다(S1210).
- [184] 제1 컨테이너 브리지(CT.Br.1)는 제1 컨테이너(ct1)에 연관된 도메인 태그(100)를 vLAN 필드에 태깅할 수 있다. 제1 컨테이너 브리지(CT.Br.1)에서 제4 컨테이너(ct4)의 맥 주소 학습(learning)이 되지 않은 경우, 또는 맥 주소 학습이나 제어기(10)로부터 수신한 정보를 통해 맥 주소 m4가 브리지-스위치 NI로 지정된 경우에 패킷의 유출 포트는 브리지-스위치 NI가 된다. 따라서, 제1 컨테이너 브리지(CT.Br.1)는 제3 패킷(pk3)을 브리지-스위치 NI를 통해, 제1 가상 스위치(vSW1)로 vLAN이 100인 제3 패킷(pk3[100])을 전달할 수 있다(S1215).
- [185] 제1 가상 스위치(vSW1)는 제3 패킷(pk3[100])의 목적지 IP 주소의 플로우 엔트리가 있는지 판단할 수 있다. 플로우 엔트리가 없으면, 제1 가상 스위치(vSW1)는, 플로우 처리 정보를 요청하기 위해, 제어기(10)로 제3 패킷(pk3[100])을 전송할 수 있다(S1220).

- [186] 제어기(10)는 제2 컨테이너(ct2)의 네트워크 정보를 알고 있다. 따라서 제어기(10)는 제3 패킷(pk3)을 제2 컨테이너가 속한 도메인 식별자와 연관된 도메인 태그로 변환할 수 있다(S1225). 제3 패킷(pk3)은 외부 네트워크(5)로 전달될 것이므로, 동일 도메인이더라도 다른 vLAN을 지정하는 것이 바람직하다. 다만, 제3 패킷(pk3)은 본래의 vLAN을 유지하여도 무방하다.
- [187] 제3 패킷(pk3)은 외부 네트워크(5)로 전달될 것이므로, 제어기(10)는 제3 패킷(pk3)의 레거시 프로토콜 변환 정보가 있는지 판단하여, 없으면 레거시 라우팅 에이전트(300)(agent)로 제3 패킷(pk3[10])으로 전달할 수 있다(S1230).
- [188] 레거시 라우팅 에이전트(300)는 제3 패킷(pk3[10])의 목적지 맥 주소를 제1 호스트(h1)와 연결된 레거시 라우터(R9)의 네트워크 인터페이스의 맥 주소(m.R1)로 변환하고, 소스 맥 주소를 제1 호스트의 실제 네트워크 인터페이스의 맥 주소(m.h1)로 변환할 수 있다(S1235). 본 단계는 제어기(10) 또는 제1 가상 스위치(vSW1)에서 행해질 수 있다.
- [189] 변환된 제3 패킷(pk3[10])은 제어기(10) 및 제1 가상 스위치(vSW1)로 전달되고(S1240, S1245), 제1 가상 스위치(vSW1)에서 레거시 라우터(R0)로 전달될 수 있다(S1250). 레거시 라우터(R0)는 제3 패킷(pk3)의 목적지 및 소스 맥 주소를 제2 호스트(h2)의 실제 네트워크 인터페이스의 맥 주소(m.h2) 및 레거시 라우터(R0)의 제2 호스트와 연결된 네트워크 인터페이스의 맥 주소(m.R2)로 변환할 수 있다(S1255).
- [190] 레거시 라우터(R0)는 제3 패킷(pk3[10])을 제2 가상 스위치(vSW2)로 전송할 수 있다(S1260).
- [191] 제2 가상 스위치(vSW2)는 제3 패킷(pk3)의 도메인 태그인 vLAN 10과 연관된 도메인 태그(vLAN이 100)로 변환하고, 목적지/소스 맥 주소를 (m.h2/m.R2)에서 (m2/m1)으로 변환할 수 있다(S1265).
- [192] 이후, 변환된 제3 패킷(pk3[100])은 제2 가상 스위치(vSW2)에서 제2 컨테이너 브리지(CT.Br.2)를 통해 제4 컨테이너(ct4)로 전송될 수 있다(S1270, S1275).
- [193] 도 23은 이중 호스트 및 이중 도메인에 속하는 제1 컨테이너(ct1)에서 제5 컨테이너(ct5)로의 패킷 흐름을 도시한다. 제1 및 제5 컨테이너(ct1, ct5)는 서로 다른 도메인에 속하므로, 제1 컨테이너(ct1)는 목적지의 맥 주소를 게이트웨이 주소, 즉 제1 호스트(h1)의 실제 네트워크 인터페이스의 맥 주소(m.h1)로 하는 제4 패킷(pk4)을 생성할 수 있다. 제1 컨테이너(ct1)는 생성된 제4 패킷(pk4)을 제1 컨테이너 브리지(CT.Br.1)로 전달할 수 있다(S1310).
- [194] 제1 컨테이너 브리지(CT.Br.1)는 제1 컨테이너(ct1)에 연관된 도메인 태그(100)를 vLAN 필드에 태깅할 수 있다. 제1 컨테이너 브리지(CT.Br.1)는, 게이트웨이인 맥주소 m.h1에 연관된 브리지-스위치 NI를 통해, 제1 가상 스위치(vSW1)로 vLAN이 100인 제4 패킷(pk4[100])을 전달할 수 있다(S1315).
- [195] 제1 가상 스위치(vSW1)는 제4 패킷(pk4[100])의 목적지 IP 주소의 플로우 엔트리가 있는지 판단할 수 있다. 플로우 엔트리가 없으면, 제1 가상

스위치(vSW1)는, 플로우 처리 정보를 요청하기 위해, 제어기(10)로 제4 패킷(pk4[100])을 전송할 수 있다(S1320).

- [196] 제어기(10)는 제5 컨테이너(ct5)의 네트워크 정보를 알고 있다. 따라서 제어기(10)는 제4 패킷(pk4)의 도메인 태그를 제5 컨테이너(ct5)가 속한 도메인 식별자와 연관된 도메인 태그로 변환할 수 있다(S1325). 제4 패킷(pk4)은 외부 네트워크(5)로 전달될 것이므로, 동일 도메인이더라도 다른 vLAN을 지정하는 것이 바람직하다. 또한, 동종 호스트 및 동종 도메인인 패킷과 구별되도록 하는 도메인 태그를 사용하는 것이 바람직하다. 예를 들어, 제5 컨테이너(ct5)로의 패킷의 소스 컨테이너가 제5 컨테이너(ct5)와 동일 도메인인 경우 제4 패킷(pk4)의 vLAN 값을 20으로 하고, 이종 도메인인 경우 제4 패킷(pk4)의 vLAN 값을 21로 할 수 있다. 제1 및 제5 컨테이너(ct1, ct5)는 이종 도메인이므로, 제어기(10)는 제4 패킷(pk4)의 도메인 태그를 21로 변환할 수 있다.
- [197] 제3 패킷(pk3)은 외부 네트워크(5)로 전달될 것이므로, 제어기(10)는 제3 패킷(pk3)의 레거시 프로토콜 변환 정보가 있는지 판단하여, 없으면 레거시 라우팅 에이전트(300)로 제3 패킷(pk3[10])으로 전달할 수 있다(S1330).
- [198] 레거시 라우팅 에이전트(300)는 제3 패킷(pk3[10])의 목적지 맥 주소를 제1 호스트(h1)와 연결된 레거시 라우터(R9)의 네트워크 인터페이스의 맥 주소(m.R1)로 변환하고, 소스 맥 주소를 제1 호스트의 실제 네트워크 인터페이스의 맥 주소(m.h1)로 변환할 수 있다(S1335). 본 단계는 제어기(10) 또는 제1 가상 스위치(vSW1)에서 행해질 수 있다.
- [199] 변환된 제4 패킷(pk4[21])은 제어기(10) 및 제1 가상 스위치(vSW1)로 전달되고(S1340, S1345), 제1 가상 스위치(vSW1)에서 레거시 라우터(R0)로 전달될 수 있다(S1350). 레거시 라우터(R0)는 제4 패킷(pk4)의 목적지 및 소스 맥 주소를 제2 호스트(h2)의 실제 네트워크 인터페이스의 맥 주소(m.h2) 및 레거시 라우터(R0)의 제2 호스트와 연결된 네트워크 인터페이스의 맥 주소(m.R2)로 변환할 수 있다(S1355).
- [200] 레거시 라우터(R0)는 제4 패킷(pk4[21])을 제2 가상 스위치(vSW2)로 전송할 수 있다(S1360).
- [201] 제2 가상 스위치(vSW2)는 제4 패킷(pk4)의 도메인 태그인 vLAN 21과 연관된 도메인 태그(vLAN이 200)로 변환하고, 목적지/소스 맥 주소를 (m.h2/m.R2)에서 (m2/m.h1)으로 변환할 수 있다(S1365).
- [202] 이후, 변환된 제4 패킷(pk4[200])은 제2 가상 스위치(vSW2)에서 제2 컨테이너 브리지(CT.Br.2)를 통해 제5 컨테이너(ct5)로 전송될 수 있다(S1370, S1375).
- [203]
- [204] 상기 본 발명은 하드웨어 또는 소프트웨어에서 구현될 수 있다. 구현은 상기 본 발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다.

컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피 디스크, 광 데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다. 그리고 본 발명을 구현하기 위한 기능적인(functional) 프로그램, 코드 및 코드 세그먼트들은 본 발명이 속하는 기술분야의 프로그래머들에 의해 용이하게 추론될 수 있다.

[205] 본 발명의 실시예들은 여기에 설명된 방법들 중 하나가 실행되는 프로그램가능 컴퓨터 시스템으로 운영될 수 있는, 전자적으로 판독가능한 제어 신호들을 갖는 캐리어 웨이브를 포함할 수 있다. 본 발명의 실시예들은 프로그램 코드를 갖는 컴퓨터 프로그램 제품으로서 구현될 수 있으며, 프로그램 코드는 컴퓨터 프로그램이 컴퓨터 상에서 구동될 때 방법들 중 하나를 실행하기 위하여 운영된다. 프로그램 코드는 예를 들면 기계 판독가능 캐리어 상에 저장될 수 있다. 본 발명의 일실시예는 컴퓨터 프로그램이 컴퓨터 상에 구동될 때, 여기에 설명된 방법들 중 하나를 실행하기 위한 프로그램 코드를 갖는 컴퓨터 프로그램일 수 있다. 본 발명은 위에서 설명한 방법들 중 하나를 실행하기 위한 컴퓨터, 또는 프로그램가능 논리 장치를 포함할 수 있다. 위에서 설명한 방법들의 일부 또는 모든 기능을 실행하기 위하여 프로그램가능 논리 장치(예를 들면, 필드 프로그램가능 게이트 어레이, 상보성 금속 산화물 반도체 기반 논리 회로)가 사용될 수 있다.

[206] 또한, 이상에서는 본 발명의 바람직한 실시예에 대하여 도시하고 설명하였지만, 본 발명은 상술한 특징의 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형실시들은 본 발명의 기술적 사상이나 전망으로부터 개별적으로 이해되어져서는 안 될 것이다.

[207] <부호의 설명>

[208] 10: 제어기 20: SDN 스위치

[209] 30: 네트워크 디바이스 100: 제어부

[210] 120: 토폴로지 관리 모듈 125: 경로 계산 모듈

[211] 130: 메시지 관리 모듈 135: 엔트리 관리 모듈

[212] 190: 저장부 200: 스위치 제어부

[213] 205: 포트부 210; 제어기 통신부

[214] 220: 플로우 검색 모듈 230: 플로우 처리 모듈

[215] 235: 패킷 처리 모듈 240: 테이블 관리 모듈

[216] 300: 레거시 쉐어너 에이전트

[217] 800: 호스트

청구범위

- [청구항 1] 레거시 네트워크에 연결되는 실제 네트워크 인터페이스;
 상기 실제 네트워크 인터페이스를 통해 레거시 네트워크와 패킷을 주고 받는, SDN(Software Defined Network) 기반의 가상 스위치;
 상기 가상 스위치를 생성하는 호스트 제어부;
 상기 호스트 제어부에 의해 생성되며, 브리지-스위치 NI(Network Interface)를 통해 상기 가상 스위치와 가상으로 네트워크 커플링되며, 자신을 식별하는 브리지 식별자를 구비하는 컨테이너 브리지;
 상기 브리지 식별자를 기초로 네트워크 서브넷 정보 및 상기 실제 네트워크 인터페이스를 게이트웨이로 하는 게이트웨이 정보를 브리지 넷 정보로 저장하는 데이터베이스; 및
 상기 호스트 제어부에 의해 생성되고, 상기 브리지 넷 정보를 기초로 고유 IP 주소를 할당받으며, 상기 컨테이너 브리지에 가상으로 네트워크 커플링되는 복수의 컨테이너를 구비하는 제1 호스트를 포함하는, 컨테이너 네트워크 관리 시스템.
- [청구항 2] 제 1 항에 있어서,
 상기 복수의 컨테이너는 각각 컨테이너 식별자를 구비하고,
 상기 데이터베이스는 상기 복수의 컨테이너 각각의 컨테이너 식별자, IP 주소, 및 동일 도메인 식별자를 컨테이너 넷 정보 리스트로 저장하는, 시스템.
- [청구항 3] 제 2 항에 있어서,
 상기 컨테이너 브리지는 상기 복수의 컨테이너와 커플링되는 복수의 브리지-컨테이너 NI를 구비하고,
 상기 컨테이너 브리지는, 상기 컨테이너 넷 정보 리스트의 컨테이너 식별자에 연관된 동일 도메인 식별자를 기초로, 상기 복수의 브리지-컨테이너 IN에 상기 동일 도메인 식별자와 대응하는 도메인 태그를 각각 지정하고,
 상기 컨테이너 브리지는 상기 복수의 컨테이너 중 제1 컨테이너로부터 상기 복수의 브리지-컨테이너 NI 중 제1 NI로 유입되는 제1 패킷에 상기 지정된 도메인 태그를 태깅하고,
 상기 복수의 브리지-컨테이너 NI 중 어느 한 NI는 상기 컨테이너 브리지에 임시 저장된 패킷에 태깅된 도메인 태그와 동일한 도메인 태그가 지정된 경우에만 상기 임시 저장 패킷의 유출이 가능하고,
 상기 브리지-스위치 NI는 유출입 하는 패킷의 도메인 태그와 무관하게 패킷의 유출입이 가능한, 시스템.
- [청구항 4] 제 3 항에 있어서,
 상기 복수의 브리지-컨테이너 중 제2 NI는 상기 제1 NI와 지정된 도메인

태그가 동일하고,

상기 컨테이너 브리지는, 상기 제1 패킷의 목적지가 상기 제2 NI와 연관된 경우, 상기 제1 패킷을 상기 제2 NI로 유출하는, 시스템.

[청구항 5]

제 3 항에 있어서,

상기 컨테이너 브리지는, 상기 복수의 브리지-컨테이너 NI에 연관된 맥 주소 리스트에 상기 제1 패킷의 맥 주소가 없거나 상기 브리지-스위치 NI가 상기 제1 패킷의 목적지와 연관된 경우, 상기 제1 패킷을 상기 브리지-스위치 NI로 유출하고,

상기 가상 스위치를 제어하는 제어기를 더 포함하고,

상기 가상 스위치는 상기 가상 스위치로 유입되는 패킷의 플로우 처리 정보가 없는 경우, 상기 제어기로 플로우 처리를 문의하여 상기 제어기로부터 패킷의 플로우 처리 정보를 취득하는, 시스템.

[청구항 6]

제 5 항에 있어서,

상기 복수의 브리지-컨테이너 NI 중 제3 NI는 제1 NI와 지정된 도메인 태그가 서로 상이하고,

상기 제어기는, 상기 제1 패킷의 목적지가 상기 제3 NI와 연관된 경우,

상기 제1 패킷의 도메인 태그를 상기 제3 NI에 지정된 제3 도메인 태그로 변환하거나 상기 가상 스위치가 변환하도록 지시하고,

상기 가상 스위치는 상기 제3 도메인 태그로 태깅된 패킷을 상기 컨테이너 브리지로 전달하는, 시스템.

[청구항 7]

제 5 항에 있어서,

패킷의 레거시 라우팅 정보 및 패킷이 레거시 라우팅 프로토콜에

적합하도록 하는 레거시 프로토콜 변환 정보 중 적어도 상기 레거시

라우팅 정보를 생성하고, 상기 제1 호스트에 구비된 가상 스위치가 상기 레거시 네트워크에서 레거시 라우터로 보이도록 상기 제1 호스트의 가상 스위치가 상기 레거시 네트워크와 패킷을 주고 받도록 설정하는 레거시 라우팅 에이전트를 더 포함하고,

상기 제1 호스트와 상기 레거시 네트워크로 연결되고, 컨테이너 생성이 가능한 다른 제2 호스트를 더 포함하고,

상기 제어기는, 상기 제1 패킷의 목적지가 상기 제2 호스트의 컨테이너에 연관되거나 상기 복수의 브리지-컨테이너 NI에 목적지 맥 주소가 없는

경우, 상기 제1 패킷을 상기 레거시 라우팅 에이전트로 전달하는, 시스템.

[청구항 8]

제 7 항에 있어서,

상기 제1 패킷은, 상기 제1 패킷의 목적지가 상기 제2 호스트에서 생성된

제2 컨테이너인 경우, 상기 레거시 라우팅 에이전트에 의해 소스 맥

주소가 상기 제1 호스트의 실제 네트워크 인터페이스와 연관된 맥 주소로 변환되고, 상기 제어기에 의해 상기 제2 컨테이너가 속한 도메인에

관련된 동일 도메인 식별자와 연관된 제 4 도메인 태그가 태깅되고, 상기

- 제1 호스트의 가상 스위치에 의해 상기 레거시 네트워크로 전달되는, 시스템.
- [청구항 9] 제 8 항에 있어서,
상기 제4 도메인 태그는 적어도 두 개의 값을 가지고, 상기 적어도 두 개의 값은 상기 제1 컨테이너와 상기 제2 컨테이너가 동일 도메인에 속하는 지 여부에 연관된, 시스템.
- [청구항 10] 제 8 항에 있어서,
상기 제1 호스트의 가상 스위치는 상기 레거시 네트워크로부터 제2 패킷을 수신하고,
상기 제2 패킷이 상기 제1 호스트의 가상 스위치에서 처리할 수 없는 레거시 프로토콜의 패킷인 경우, 상기 제2 패킷은 상기 레거시 라우팅 에이전트에 의해 오픈플로우 프로토콜의 패킷으로 변환되고,
상기 제2 패킷의 도메인 태그가 상기 제1 NI의 도메인 태그와 연관된 경우, 상기 제어기에 의해 상기 제2 패킷의 도메인 태그는 상기 제1 NI의 도메인 태그로 변환되는, 시스템.
- [청구항 11] 제 7 항에 있어서,
상기 레거시 네트워크와 구별되는 독립 네트워크를 구축하는 SDN 기반의 스위치 그룹을 더 포함하고,
상기 스위치 그룹은 상기 제1 호스트의 가상 스위치인 에지 스위치를 적어도 하나를 구비하고,
상기 제어기는 상기 적어도 하나의 에지 스위치의 정보를 취득하고,
상기 레거시 라우팅 에이전트는, 상기 제어기에서 취득한 적어도 하나의 에지 스위치의 정보를 기초로, 상기 레거시 네트워크에서 상기 스위치 그룹의 적어도 일부를 레거시 라우터로 취급하도록 하는 적어도 하나의 가상 라우터를 생성하는, 시스템.
- [청구항 12] 제 11 항에 있어서,
상기 적어도 하나의 가상 라우터는 가상 라우터용 포트를 구비하고,
상기 가상 라우터용 포트의 정보는 상기 실제 네트워크 인터페이스 정보와 대응하거나, 상기 가상 라우터용 포트를 유출입하는 패킷의 도메인 태그에 연관되는, 시스템.
- [청구항 13] 제 11 항에 있어서,
상기 레거시 라우팅 에이전트는, 상기 제1 호스트의 컨테이너 브리지 및 상기 복수의 컨테이너를 구비하는 상기 스위치 그룹에 연결된 네트워크 노드가 상기 레거시 네트워크에서 상기 적어도 하나의 레거시 라우터에 연결된 외부 네트워크(external network)로 취급되도록 설정하는, 시스템.
- [청구항 14] 레거시 네트워크에 연결되는 실제 네트워크 인터페이스;
상기 실제 네트워크 인터페이스를 통해 레거시 네트워크와 패킷을 주고 받고, 외부의 제어기에 의해 제어되는 SDN(Software Defined Network)

기반의 가상 스위치;
 상기 가상 스위치를 생성하는 호스트 제어부;
 상기 호스트 제어부에 의해 생성되며, 브리지-스위치 NI(Network Interface)를 통해 상기 가상 스위치와 가상으로 네트워크 커플링되며, 자신을 식별하는 브리지 식별자를 구비하는 컨테이너 브리지;
 상기 브리지 식별자를 기초로 네트워크 서브넷 정보 및 상기 실제 네트워크 인터페이스를 게이트웨이로 하는 게이트웨이 정보를 브리지 넷 정보로 저장하는 데이터베이스; 및
 상기 호스트 제어부에 의해 생성되고, 상기 브리지 넷 정보를 기초로 고유 IP 주소를 할당받으며, 상기 컨테이너 브리지에 가상으로 네트워크 커플링되는 복수의 컨테이너를 구비하는 호스트.

[청구항 15]

컨테이너를 생성하며 실제 네트워크 인터페이스를 통해 레거시 네트워크와 연결되는 호스트에서, SDN(Software Defined Network) 기반의 가상 스위치를 생성하는 단계;
 상기 가상 스위치를 상기 실제 네트워크 인터페이스와 네트워크 연결하는 단계;
 상기 호스트에서, 네트워크 환경을 구별하는 브리지 식별자, 상기 가상 스위치를 게이트웨이로 하는 게이트웨이 정보, 및 네트워크 서브넷 정보를 구비하는 컨테이너 브리지 생성 요청을 받으면, 컨테이너 브리지를 생성하는 단계;
 상기 컨테이너 브리지와 상기 가상 스위치 사이에 모든 동일 도메인 식별자를 가지는 패킷이 통과할 수 있도록 상기 컨테이너 브리지와 상기 가상 스위치를 네트워크 커플링하는 단계;
 상기 호스트에서, 상기 브리지 식별자를 키로 하는 제1 컨테이너 식별자 및 제1 동일 도메인 식별자를 구비하는 컨테이너 생성 요청을 받으면, 상기 제1 컨테이너 식별자를 구비하는 제1 컨테이너를 생성하는 단계;
 상기 브리지 식별자에 연관된 네트워크 서브넷 정보를 기초로 상기 제1 컨테이너에 IP 주소를 할당하는 단계; 및
 상기 컨테이너 브리지와 상기 제1 컨테이너를 네트워크 커플링하고, 상기 제1 동일 도메인 식별자에 연관된 제1 도메인 태그를 가진 패킷만 상기 제1 컨테이너로 전달되도록 상기 컨테이너와 커플링되는 상기 컨테이너 브리지의 브리지-컨테이너 NI(Network Interface)에 상기 제1 도메인 태그를 지정하는 단계를 포함하는, 컨테이너 네트워크의 컨테이너 네트워킹 방법.

[청구항 16]

제 15 항에 있어서,
 상기 컨테이너 브리지에서, 동일한 호스트의 동일한 도메인에 속한 제2 컨테이너가 목적지인 제1 패킷을 제1 호스트로부터 수신하는 단계; 및
 상기 제1 패킷의 맥 주소와 연관된 브리지-컨테이너 NI로 상기 제1 패킷을

- 유출하는 단계를 더 포함하는, 방법.
- [청구항 17] 제 15 항에 있어서,
 상기 컨테이너 브리지에서, 상기 제1 컨테이너에서 상기 컨테이너 브리지로 유입되는 패킷에 상기 제1 도메인 태그를 태깅하는 단계;
 상기 유입 패킷의 목적지가 상기 가상 스위치와 연관되거나 상기 제1 컨테이너에 연결된 제1 브리지-컨테이너 NI가 아닌 다른 브리지-컨테이너 NI에 상기 유입 패킷의 목적지 맥 주소가 없는 경우, 상기 유입 패킷을 상기 가상 스위치로 전달하는 단계;
 상기 가상 스위치에서 상기 전달 받은 패킷에 대한 플로우 처리 정보가 없는 경우, 상기 가상 스위치를 제어하는 제어기로 패킷의 플로우 처리를 문의하여 플로우 처리 정보를 취득하는 단계; 및
 상기 제어기에서, 패킷을 상기 레거시 네트워크로 전달해야 하는 경우, 패킷의 레거시 라우팅 정보를 생성하는 레거시 라우팅 에이전트로 상기 레거시 네트워크로 전달할 패킷에 대한 레거시 라우팅 정보를 취득하는 단계를 더 포함하는, 방법.
- [청구항 18] 제 17 항에 있어서,
 상기 컨테이너 브리지에서, 동일한 호스트의 다른 도메인에 속한 제3 컨테이너가 목적지인 제2 패킷을 상기 제1 컨테이너로부터 수신하는 단계;
 상기 제2 패킷의 게이트웨이 맥 주소와 연관된 브리지-스위치 NI로 상기 제2 패킷을 유출하는 단계;
 상기 제1 도메인 태그에서 상기 제3 컨테이너에 커플링된 브리지-컨테이너 NI에 연관된 도메인 태그로 변환된 패킷을 수신하는 단계를 더 포함하는, 방법.
- [청구항 19] 제 17 항에 있어서,
 제4 패킷은 상기 제1 컨테이너가 속한 호스트와 상이한 호스트가 목적지이고,
 상기 컨테이너 브리지에서, 상기 제4 패킷을 상기 제1 컨테이너로부터 수신하고, 상기 제4 패킷을 가상 스위치로 전달하는 단계;
 상기 제4 패킷의 소스의 맥 주소를 상기 호스트의 실제 네트워크 인터페이스의 맥 주소 또는 동일 도메인 식별자와 연관된 가상 맥 주소로 변환하고, 목적지의 맥 주소를 상기 레거시 네트워크에 속한 넥스트 홉의 맥 주소로 변환하고, 도메인 태그를 상기 제4 패킷의 목적지의 도메인 태그와 연관된 태그로 변환하는 단계; 및
 상기 가상 스위치에서, 상기 변환된 제4 패킷을 상기 레거시 네트워크로 전달하는 단계를 더 포함하는, 방법.
- [청구항 20] 제 19 항에 있어서,
 상기 제4 패킷 목적지의 도메인 태그와 연관된 태그는 적어도 두 개이고,

상기 적어도 두 개의 연관된 태그는 상기 제1 컨테이너와 상기 제4 패킷의 목적지의 도메인이 동일 여부에 따른 것인, 방법.

[청구항 21]

제 19 항에 있어서,

상기 가상 스위치에서, 다른 호스트에 속한 제4 컨테이너로부터 상기 레거시 네트워크를 통해 제5 패킷을 수신하는 단계;

상기 제5 패킷이 상기 가상 스위치 또는 상기 제어기에서 처리할 수 없는 레거시 프로토콜의 패킷인 경우, 상기 레거시 라우팅 에이전트에서 상기 제5 패킷을 오픈플로우 프로토콜로 변환하는 단계; 및

상기 제5 패킷의 제5 도메인 태그가 상기 제1 도메인 태그와 연관된 경우, 상기 제5 패킷의 도메인 태그를 상기 제1 도메인 태그로 변환하고, 목적지 맥 주소를 상기 제1 컨테이너의 맥 주소로 변환하는 단계를 더 포함하는 방법.

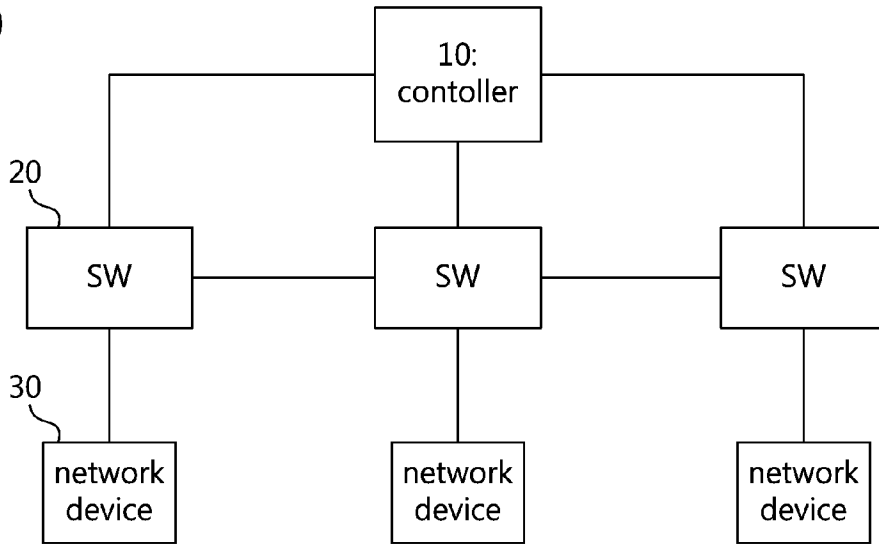
[청구항 22]

제 21 항에 있어서,

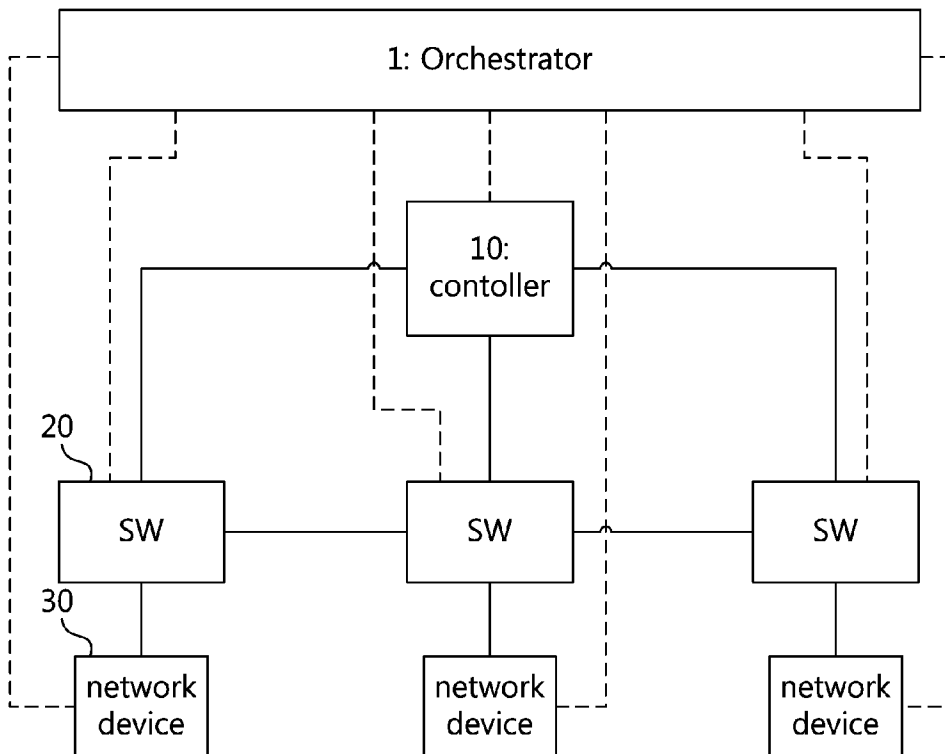
상기 가상 스위치에서, 상기 제5 도메인 태그가 상기 제1 및 제4 컨테이너가 동일한 도메인에 속한 것을 지시하는 경우, 상기 제5 패킷의 소스 맥 주소를 상기 제4 컨테이너의 맥 주소로 변환하는 단계를 더 포함하는, 방법.

[도 1]

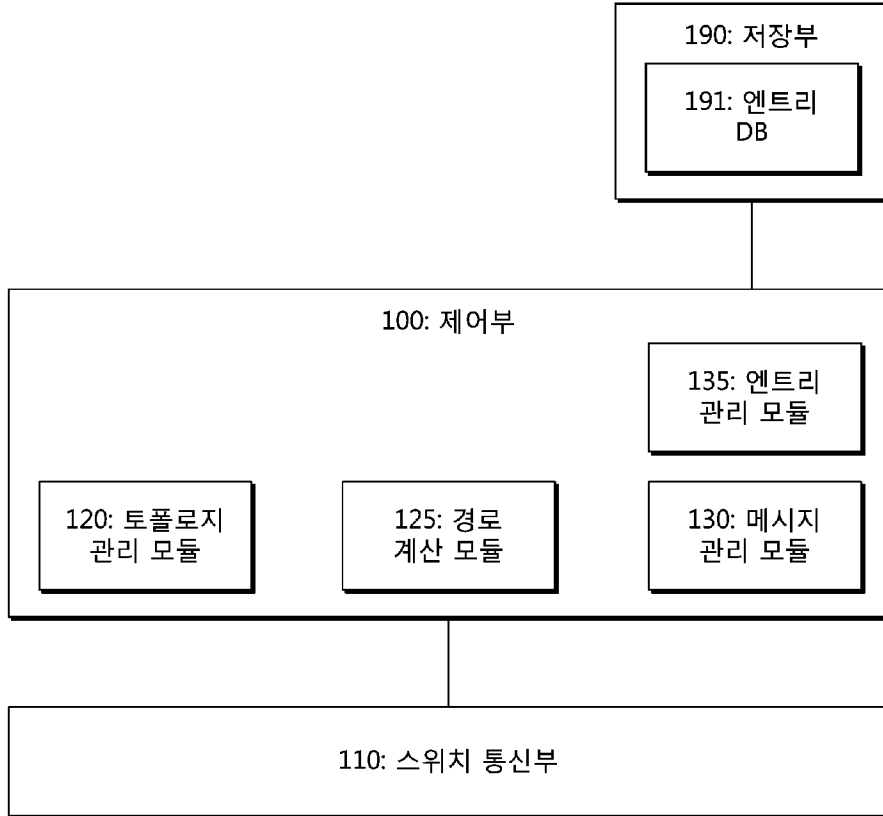
(a)



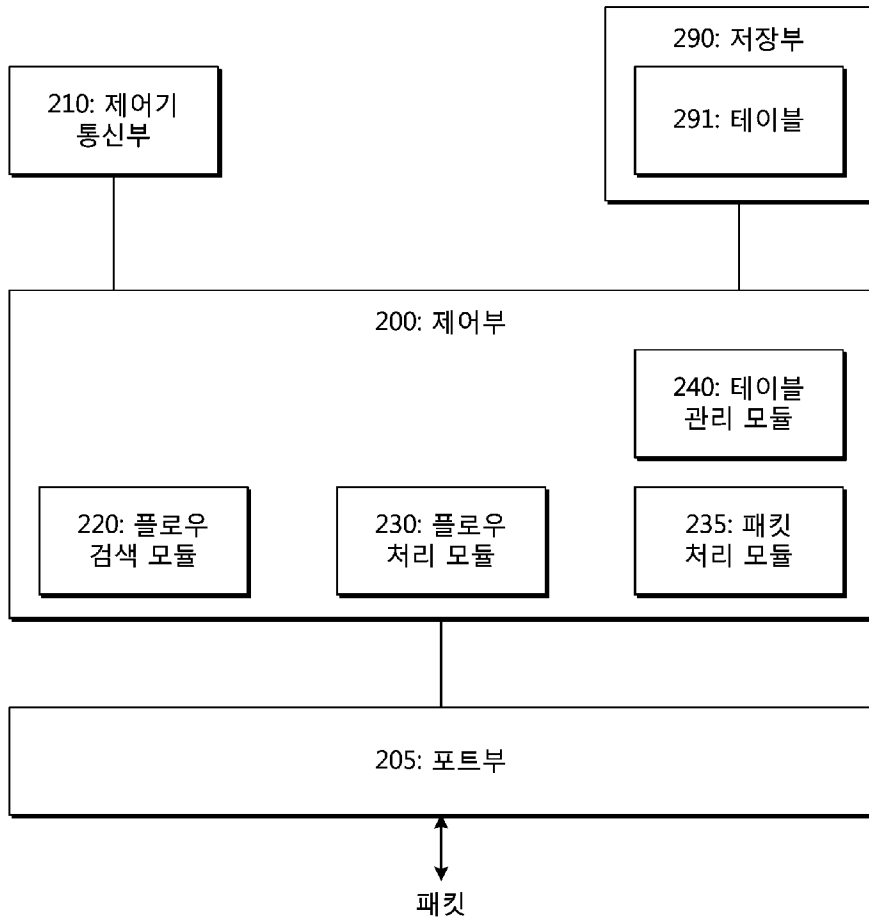
(b)



[도2]



[도3]



[도4]

(a)

Match Fields	Priority	Counters	Instructions	Timeouts	Cookie
--------------	----------	----------	--------------	----------	--------

(b)

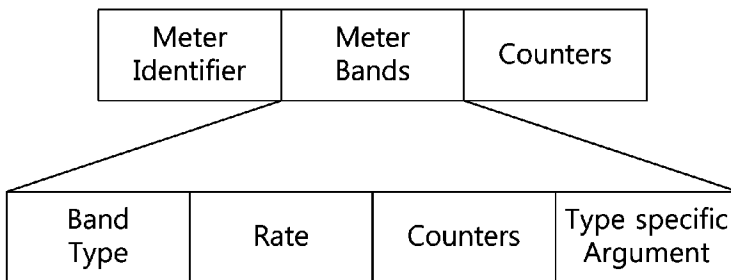
	in Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP s.port	TCP d.port	Action
Switching:	*	*	00:1f..	*	*	*	*	*	*	*	port 1
Routing:	*	*	*	*	*	*	1.2.3.4	*	*	*	port 6
VLAN sw:	*	*	00:3f..	*	vlan2	*	*	*	*	*	port 1,2,3
Firewall:	*	*	*	*	*	*	*	*	*	22 27	drop

[도5]

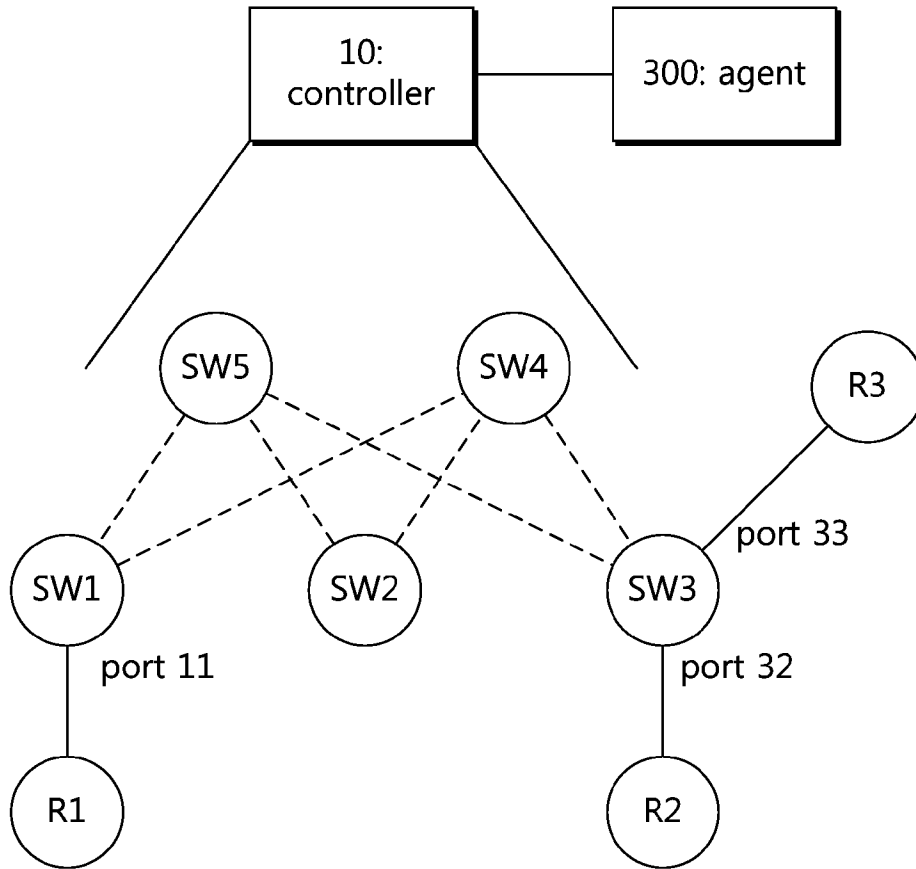
(a)

Group Identifier	Group Type	Counters	Action Buckets
------------------	------------	----------	----------------

(b)

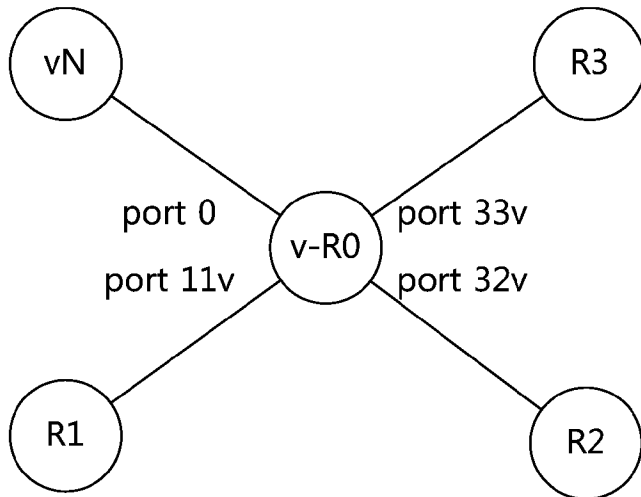


[도6]

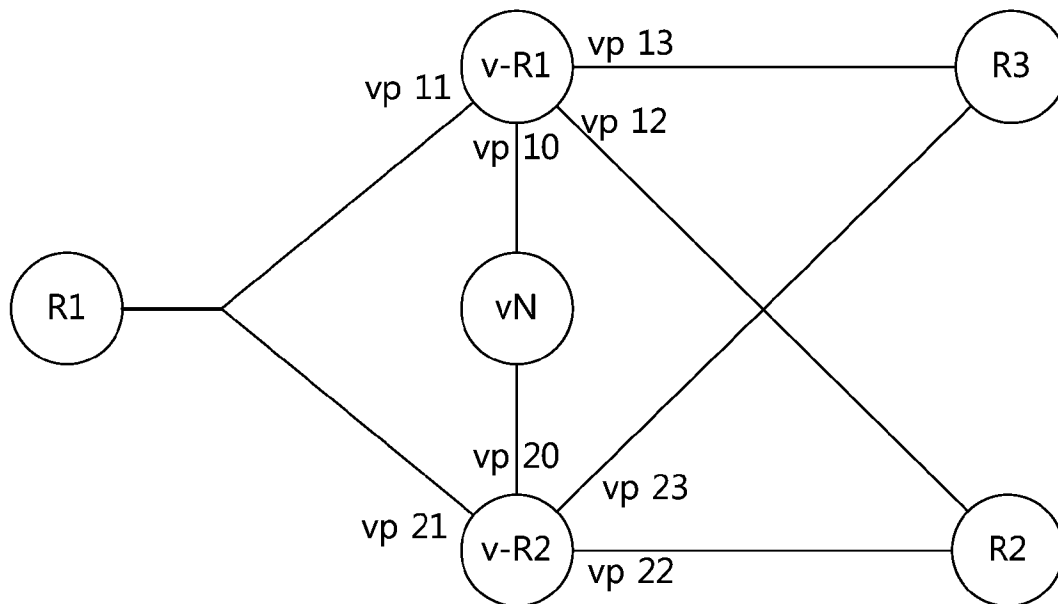


[도7]

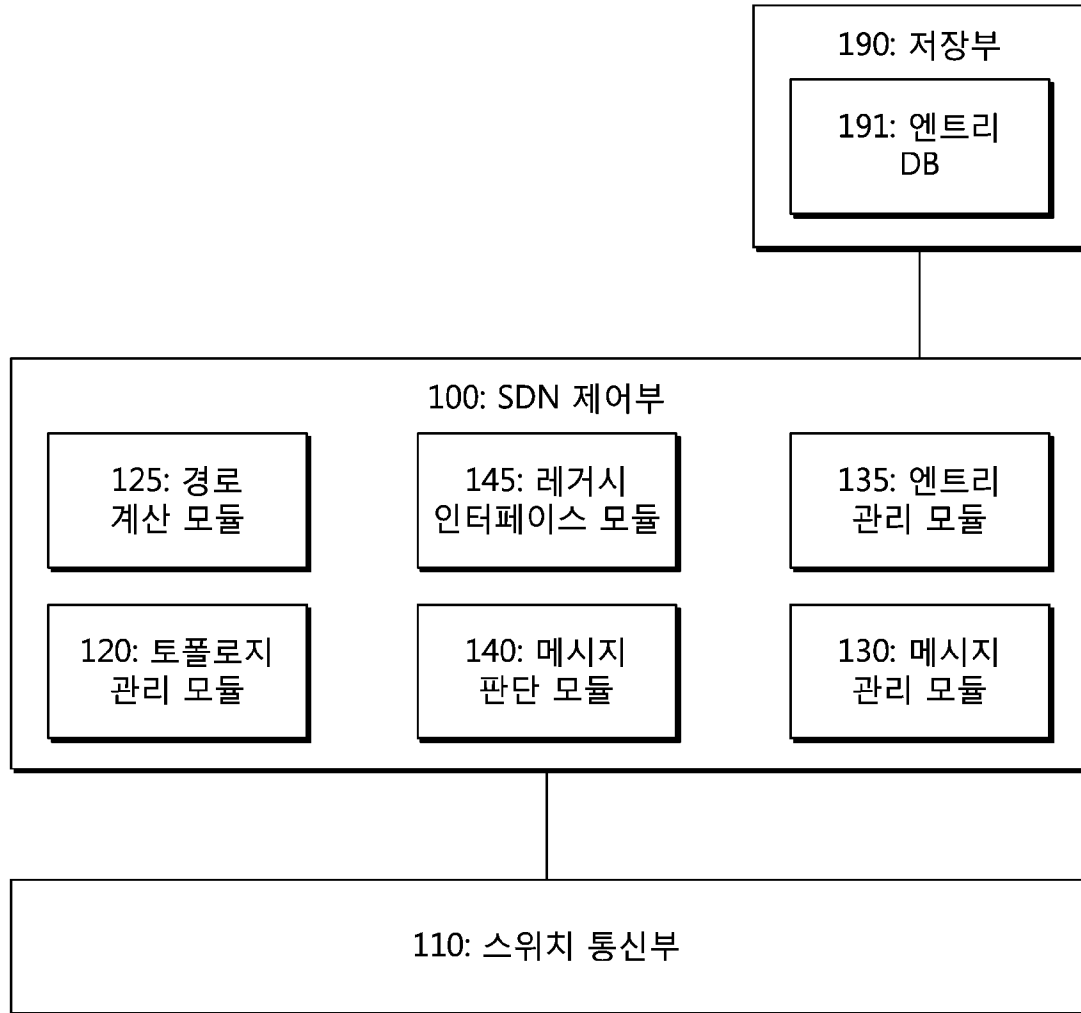
(a)



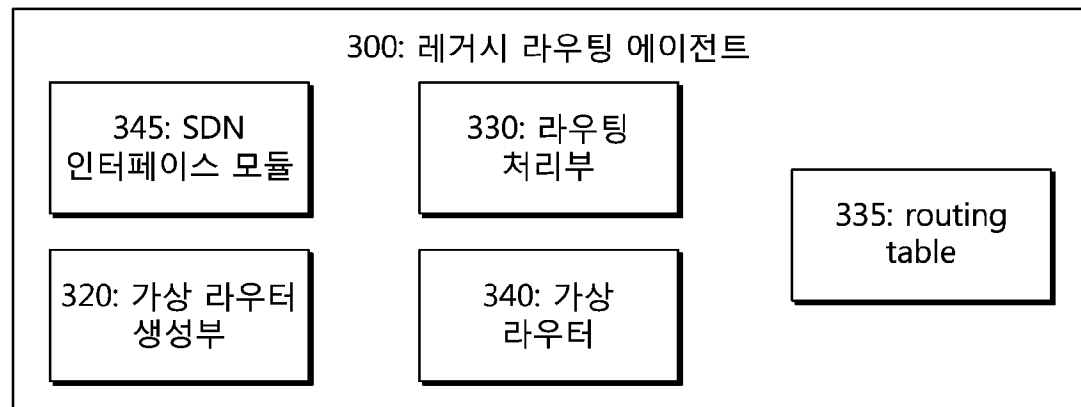
(b)



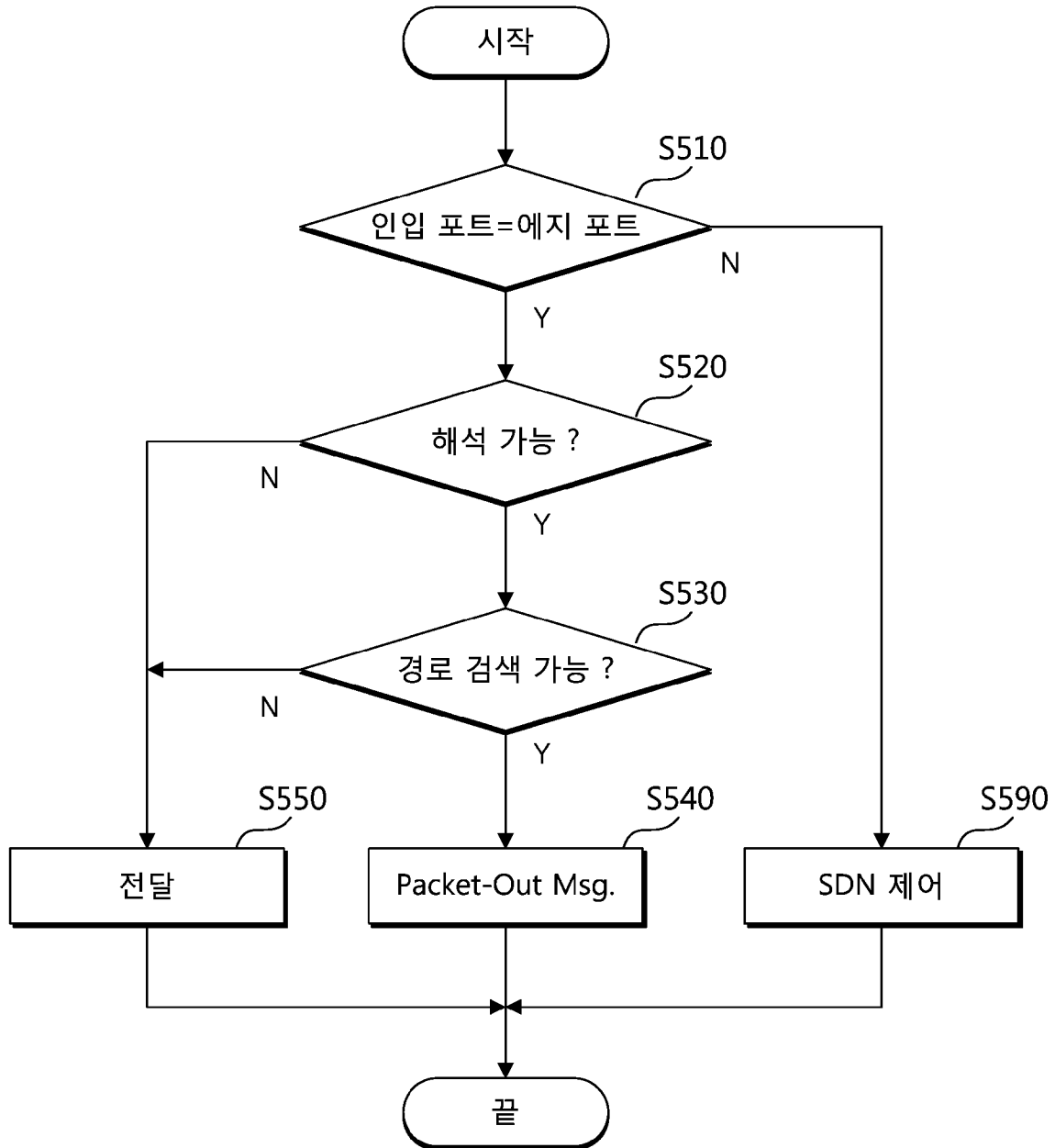
[도8]



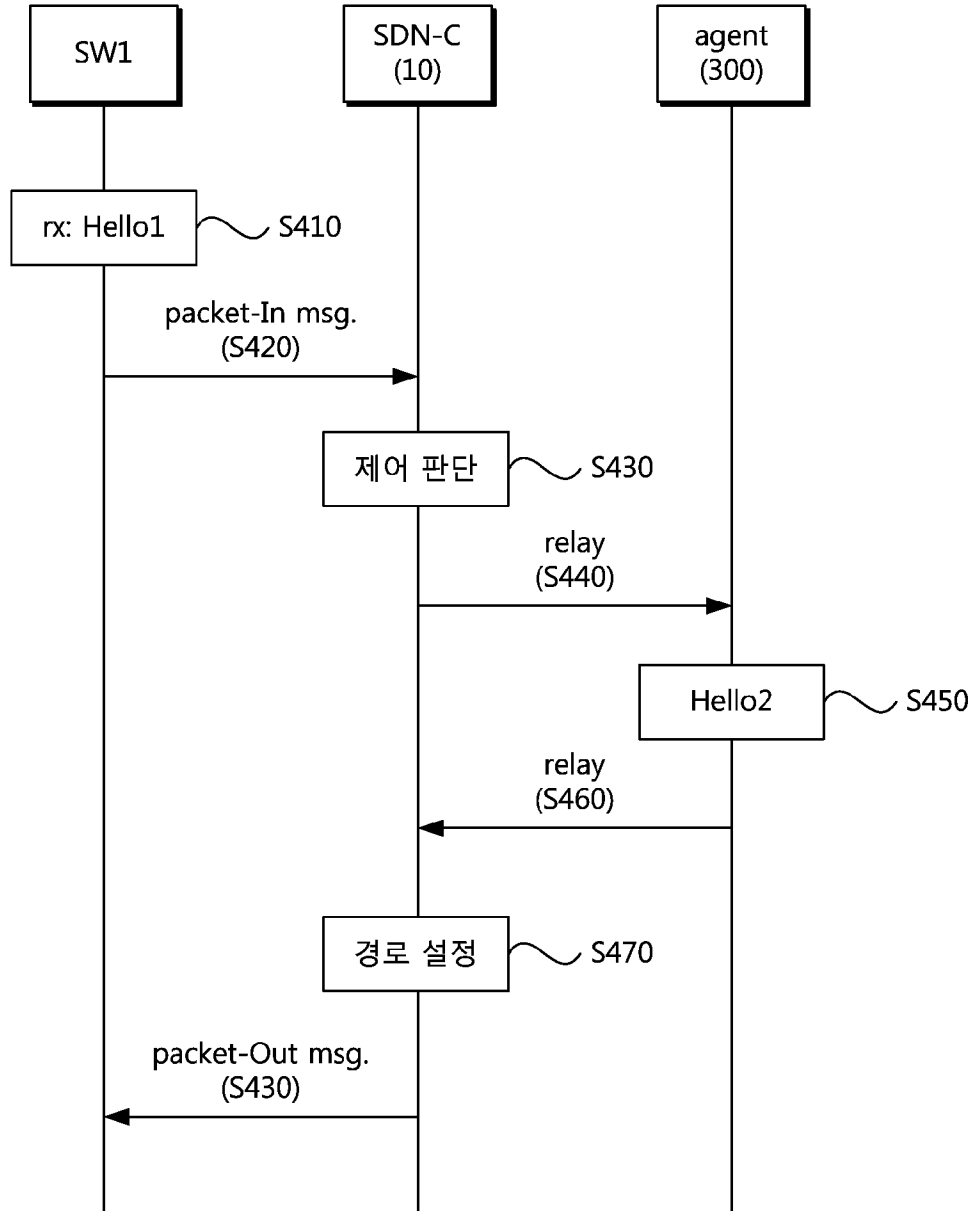
[도9]



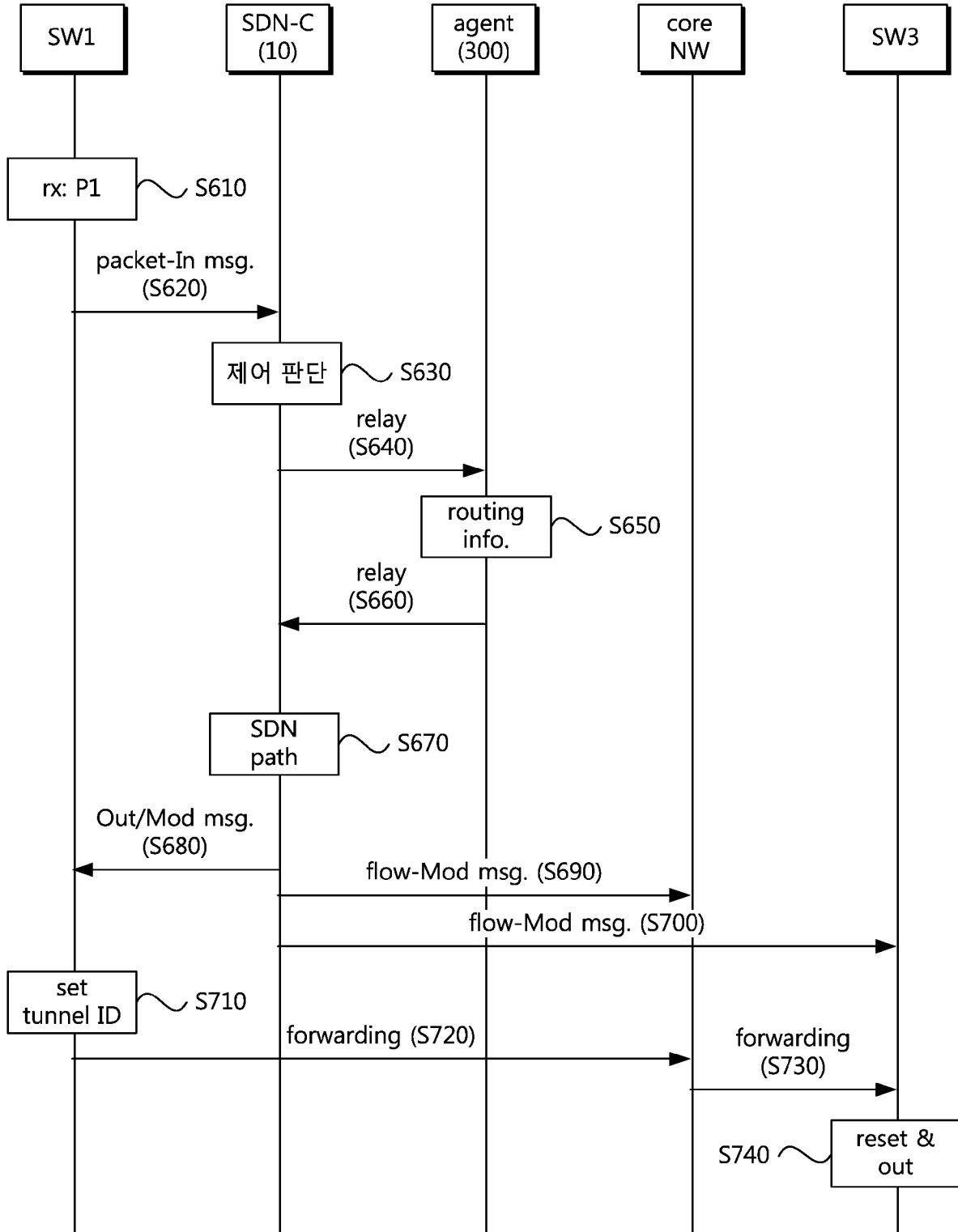
[도10]



[도 11]



[도 12]



[도 13]

(a)

table 0		
R2	set-tunnel2	goto table1
R3	set-tunnel3	goto table1

table 1	
tunnel2	out port14
tunnel3	out port15

(b)

table 1	
tunnel2	out port43

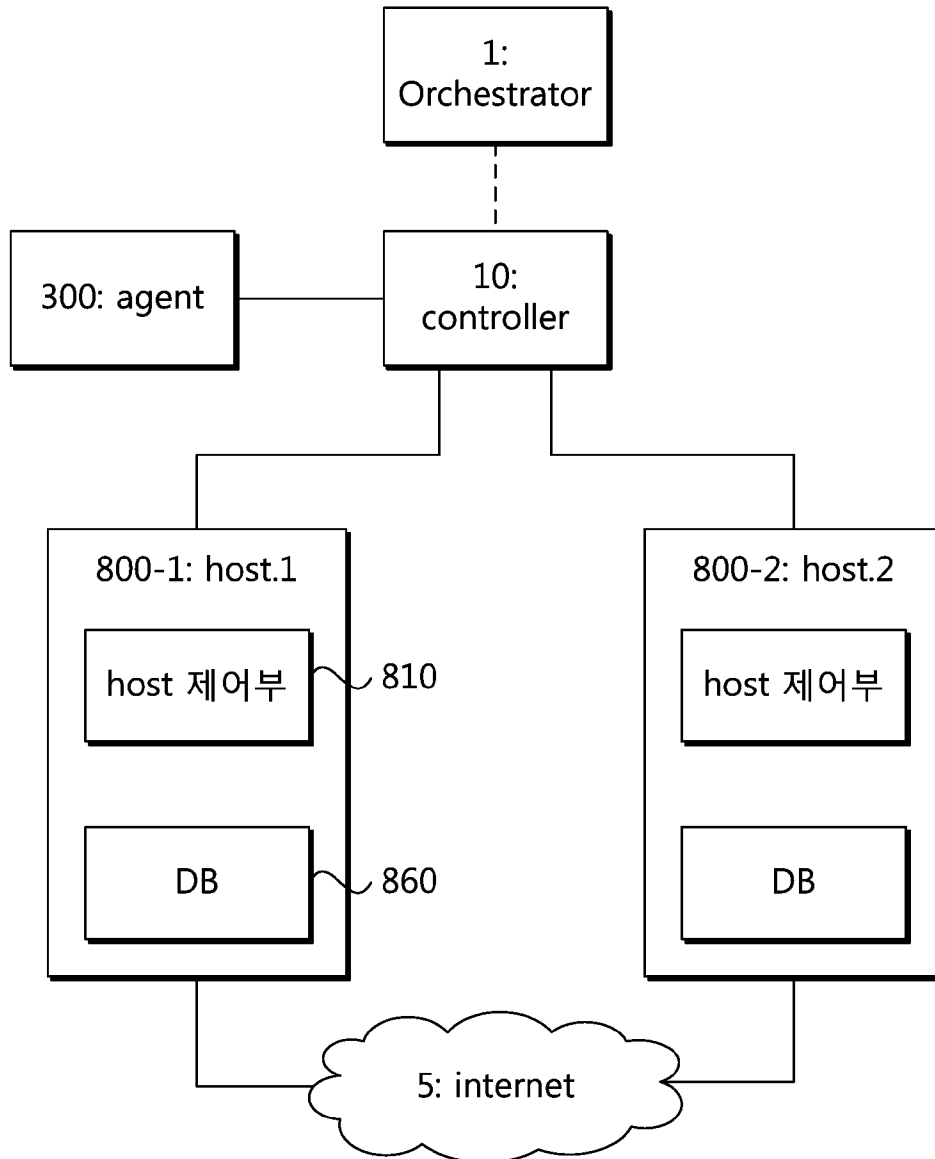
(c)

table 0		
tunnel2	off T-ID	goto table1
tunnel3	off T-ID	goto table2

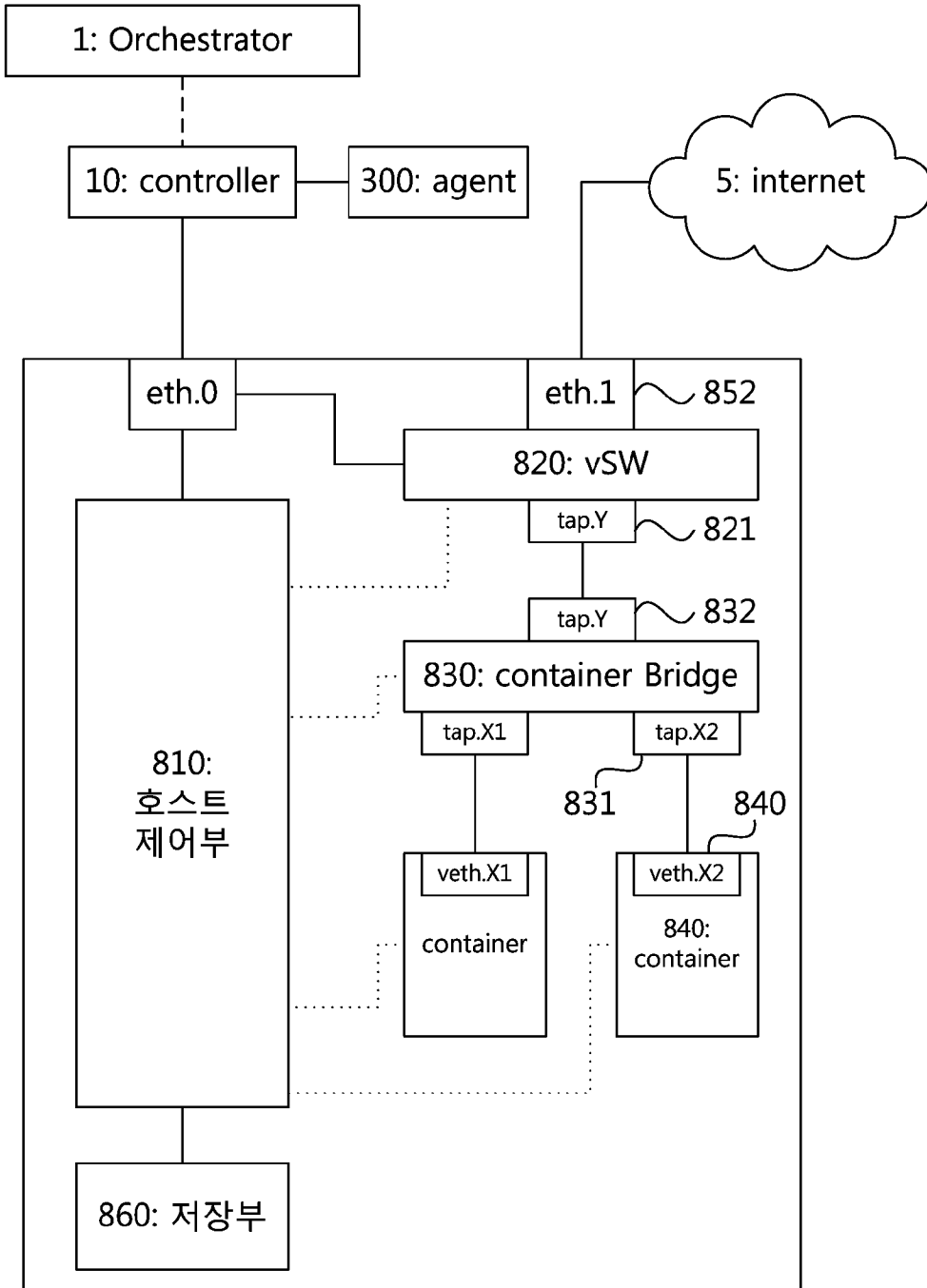
table 1	
*	out port32

table 2	
*	out port33

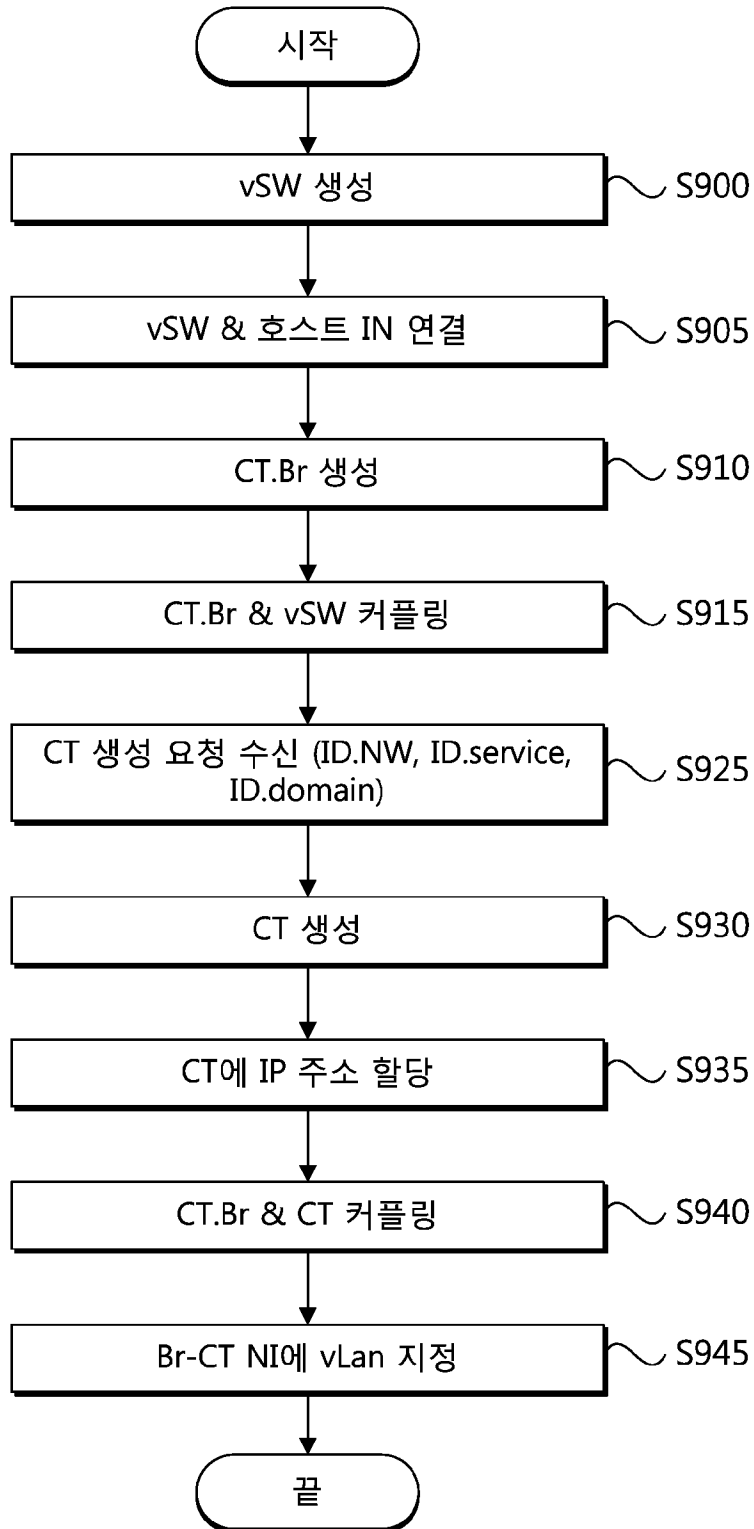
[도14]



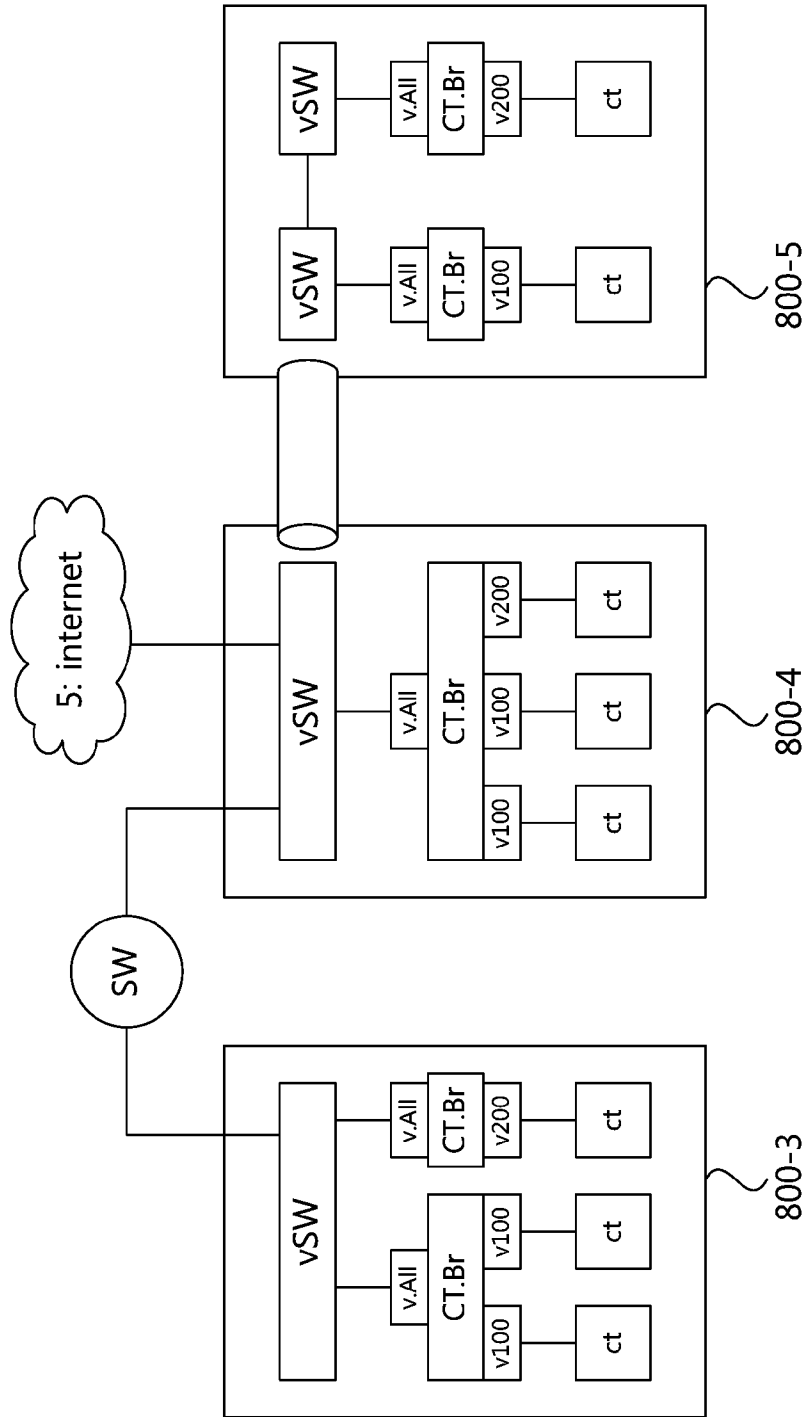
[도 15]



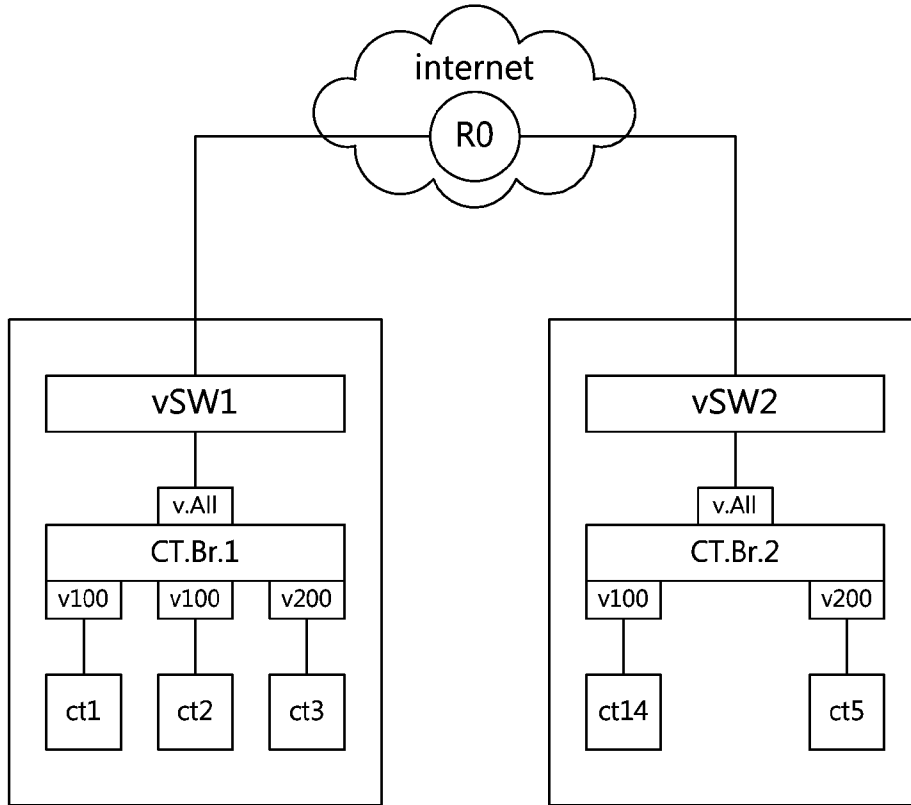
[도16]



[도17]

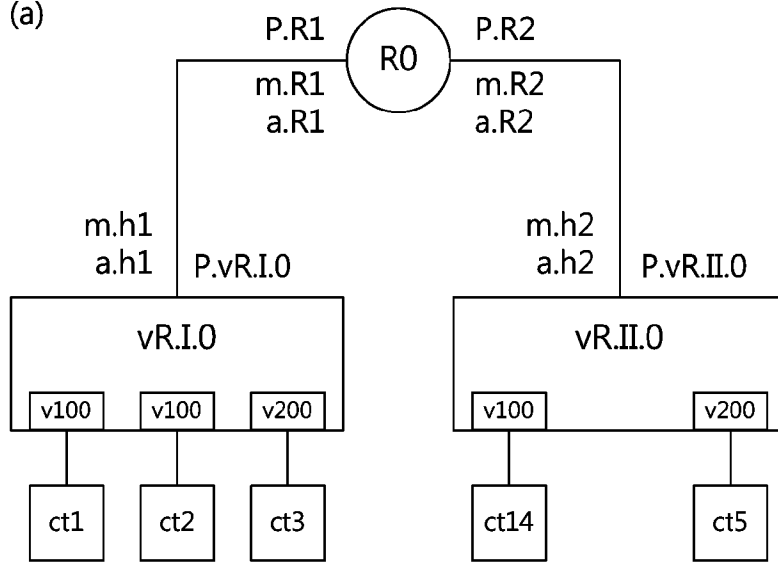


[도18]

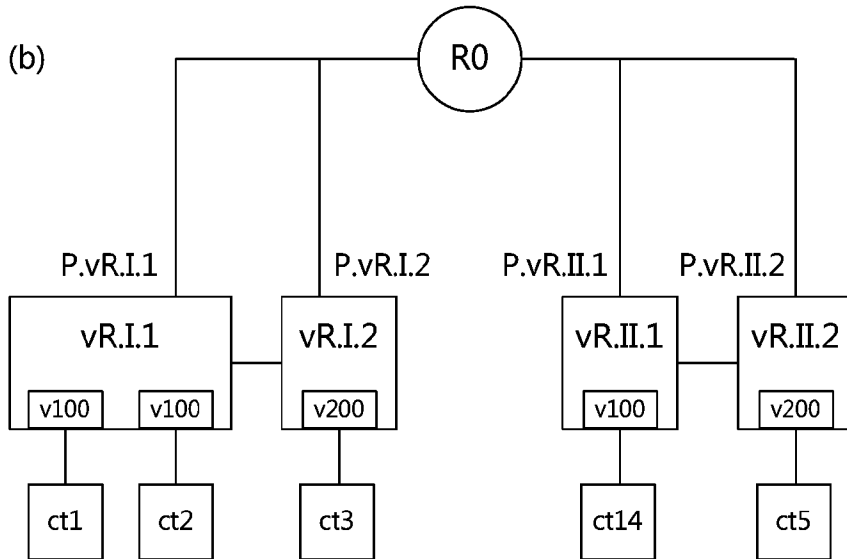


[도 19]

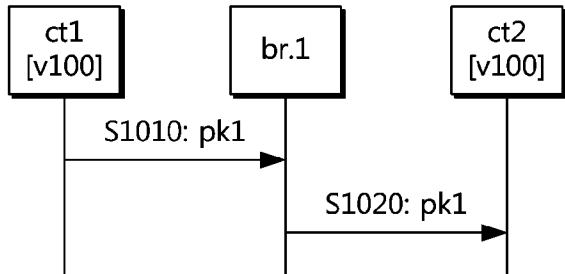
(a)



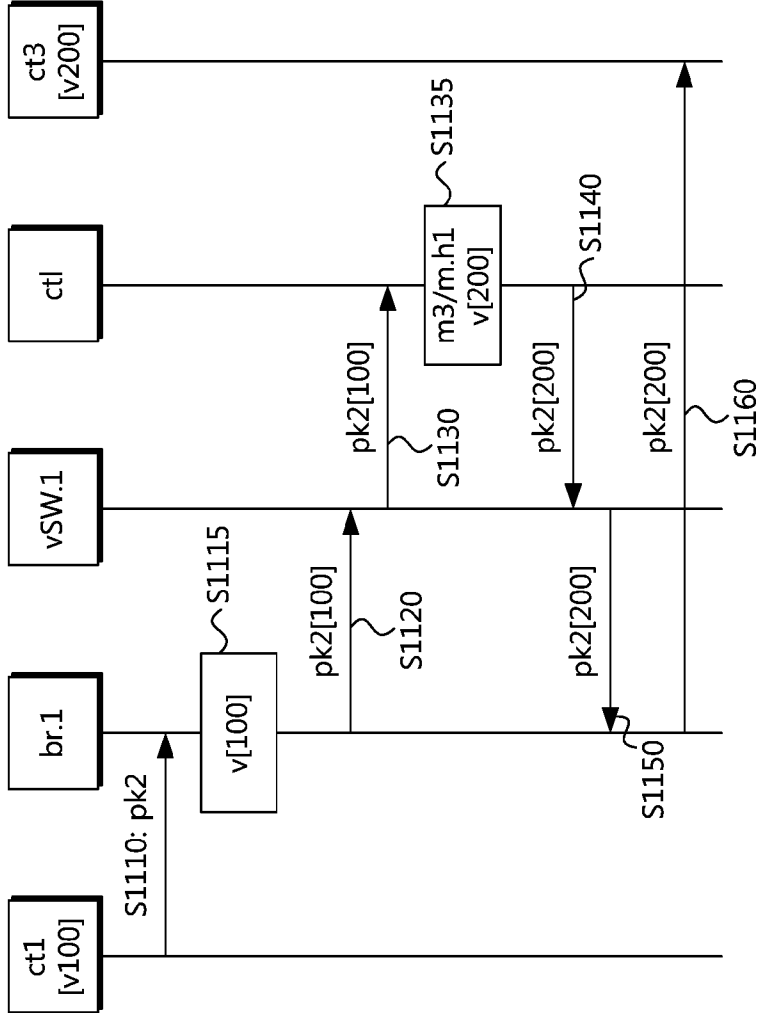
(b)

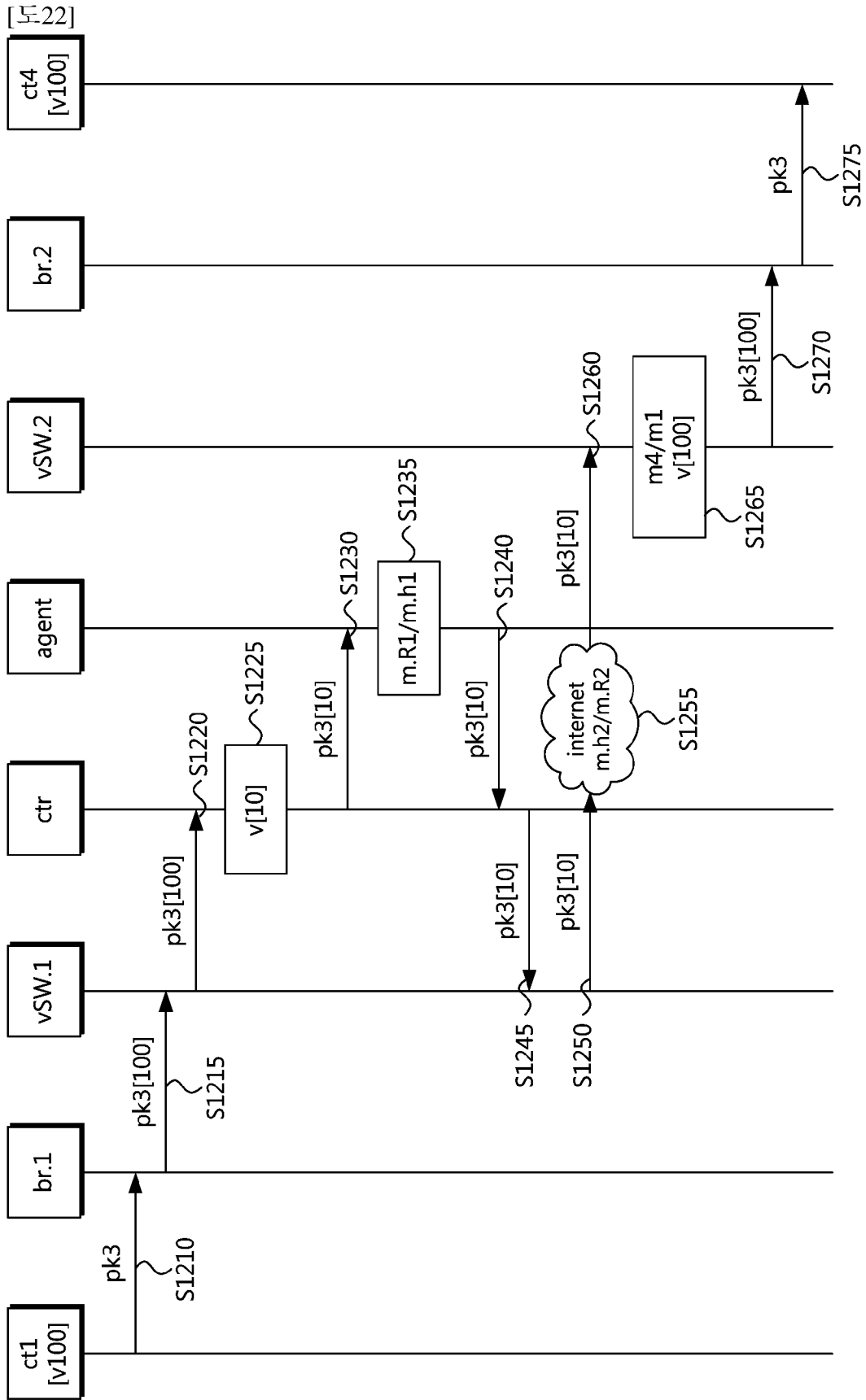


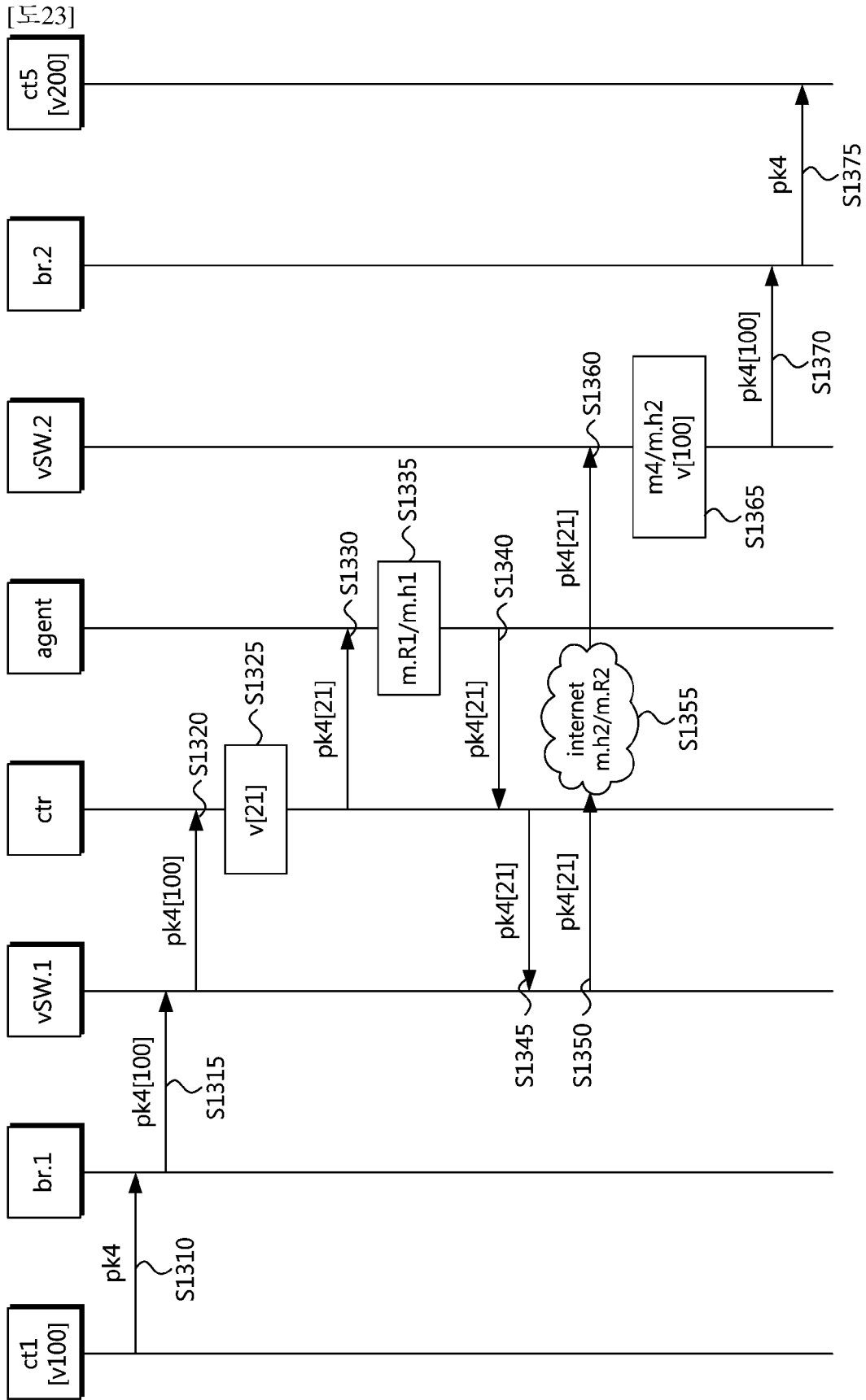
[도 20]



[圖 21]







INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2016/002924

A. CLASSIFICATION OF SUBJECT MATTER

H04L 12/24(2006.01)i, H04L 12/50(2006.01)i, H04L 12/749(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 12/24; G06F 13/40; H04L 29/06; G06F 9/455; H04L 12/28; G06F 9/50; H04L 12/707; H04L 12/50; H04L 12/749

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: network interface, virtual switch, host, coupling, bridge identifier, container bridge, database

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2015-0370586 A1 (INTEL CORPORATION) 24 December 2015 See paragraphs [0021]-[0025], [0043]-[0045], [0062]-[0063]; and figures 1, 5.	1-22
A	US 2013-0058250 A1 (CASADO, Martin et al.) 07 March 2013 See paragraphs [0175]-[0183]; and figure 12.	1-22
A	US 2014-0115706 A1 (ZANTTZ, INC.) 24 April 2014 See paragraphs [0013], [0110]-[0111]; and figure 9.	1-22
A	US 2014-0201374 A1 (FUTUREWEI TECHNOLOGIES, INC.) 17 July 2014 See paragraphs [0007]-[0009]; and figures 1, 8.	1-22
A	US 2015-0263899 A1 (NICIRA, INC.) 17 September 2015 See paragraphs [0003]-[0012]; and figure 3.	1-22

 Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

05 OCTOBER 2016 (05.10.2016)

Date of mailing of the international search report

10 OCTOBER 2016 (10.10.2016)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701,
Republic of Korea

Facsimile No. +82-42-481-8578

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2016/002924


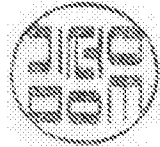
Patent document cited in search report	Publication date	Patent family member	Publication date
US 2015-0370586 A1	24/12/2015	CN 105282135 A	27/01/2016
		DE 102015108145 A1	24/12/2015
		JP 2016-009486 A	18/01/2016
		KR 10-2015-0146391 A	31/12/2015
US 2013-0058250 A1	07/03/2013	US 08717895 B2	06/05/2014
		US 2013-058208 A1	07/03/2013
		US 2013-058215 A1	07/03/2013
		US 2013-058225 A1	07/03/2013
		US 2013-058226 A1	07/03/2013
		US 2013-058228 A1	07/03/2013
		US 2013-058251 A1	07/03/2013
		US 2013-058252 A1	07/03/2013
		US 2013-058255 A1	07/03/2013
		US 2013-058331 A1	07/03/2013
		US 2013-058334 A1	07/03/2013
		US 2013-058339 A1	07/03/2013
		US 2013-058340 A1	07/03/2013
		US 2013-058341 A1	07/03/2013
		US 2013-058342 A1	07/03/2013
		US 2013-058343 A1	07/03/2013
		US 2013-058344 A1	07/03/2013
		US 2013-058348 A1	07/03/2013
		US 2013-058353 A1	07/03/2013
		US 2013-058354 A1	07/03/2013
		US 2013-058356 A1	07/03/2013
		US 2013-058357 A1	07/03/2013
		US 2013-058358 A1	07/03/2013
		US 2013-060736 A1	07/03/2013
		US 2013-060737 A1	07/03/2013
		US 2013-060738 A1	07/03/2013
		US 2013-060817 A1	07/03/2013
		US 2013-060818 A1	07/03/2013
		US 2013-060819 A1	07/03/2013
		US 2013-060922 A1	07/03/2013
		US 2013-060929 A1	07/03/2013
		US 2013-060940 A1	07/03/2013
		US 8718070 B2	06/05/2014
		US 8743888 B2	03/06/2014
		US 8743889 B2	03/06/2014
		US 8750119 B2	10/06/2014
US 8750164 B2	10/06/2014		
US 8761036 B2	24/06/2014		
US 8775594 B2	08/07/2014		
US 8817620 B2	26/08/2014		
US 8817621 B2	26/08/2014		
US 8830823 B2	09/09/2014		
US 8837493 B2	16/09/2014		
US 8842679 B2	23/09/2014		

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2016/002924

Patent document cited in search report	Publication date	Patent family member	Publication date
		US 8880468 B2	04/11/2014
		US 8913483 B2	16/12/2014
		US 8958292 B2	17/02/2015
		US 8959215 B2	17/02/2015
		US 8964598 B2	24/02/2015
		US 8966040 B2	24/02/2015
		US 9007903 B2	14/04/2015
		US 9008087 B2	14/04/2015
		US 9049153 B2	02/06/2015
		US 9077664 B2	07/07/2015
		US 9106587 B2	11/08/2015
		US 9112811 B2	18/08/2015
		US 9172663 B2	27/10/2015
		US 9231891 B2	05/01/2016
		US 9300603 B2	29/03/2016
		US 9306875 B2	05/04/2016
US 2014-0115706 A1	24/04/2014	US 2015-229663 A1	13/08/2015
		US 9021092 B2	28/04/2015
		WO 2014-063110 A1	24/04/2014
US 2014-0201374 A1	17/07/2014	CN 105247826 A	13/01/2016
		EP 2936754 A1	28/10/2015
		JP 2016-509412 A	24/03/2016
		WO 2014-110453 A1	17/07/2014
US 2015-0263899 A1	17/09/2015	US 2015-0263946 A1	17/09/2015
		US 9225597 B2	29/12/2015
		WO 2015-138043 A2	17/09/2015
		WO 2015-138043 A3	19/11/2015

A. 발명이 속하는 기술분류(국제특허분류(IPC)) H04L 12/24(2006.01)i, H04L 12/50(2006.01)i, H04L 12/749(2013.01)i		
B. 조사된 분야 조사된 최소문헌(국제특허분류를 기재) H04L 12/24; G06F 13/40; H04L 29/06; G06F 9/455; H04L 12/28; G06F 9/50; H04L 12/707; H04L 12/50; H04L 12/749 조사된 기술분야에 속하는 최소문헌 이외의 문헌 한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC 일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC 국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우)) eKOMPASS(특허청 내부 검색시스템) & 키워드: 네트워크 인터페이스, 가상 스위치, 호스트, 커플링, 브리지 식별자, 컨테이너 브리지, 데이터베이스		
C. 관련 문헌		
카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
A	US 2015-0370586 A1 (INTEL CORPORATION) 2015.12.24 단락 [0021]-[0025], [0043]-[0045], [0062]-[0063]; 및 도면 1, 5 참조.	1-22
A	US 2013-0058250 A1 (MARTIN CASADO 등) 2013.03.07 단락 [0175]-[0183]; 및 도면 12 참조.	1-22
A	US 2014-0115706 A1 (ZANTTZ, INC.) 2014.04.24 단락 [0013], [0110]-[0111]; 및 도면 9 참조.	1-22
A	US 2014-0201374 A1 (FUTUREWEI TECHNOLOGIES, INC.) 2014.07.17 단락 [0007]-[0009]; 및 도면 1, 8 참조.	1-22
A	US 2015-0263899 A1 (NICIRA, INC.) 2015.09.17 단락 [0003]-[0012]; 및 도면 3 참조.	1-22
<input type="checkbox"/> 추가 문헌이 C(계속)에 기재되어 있습니다. <input checked="" type="checkbox"/> 대응특허에 관한 별지를 참조하십시오.		
* 인용된 문헌의 특별 카테고리: “A” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌 “E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌 “L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌 “O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌 “P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌 “T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌 “X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다. “Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다. “&” 동일한 대응특허문헌에 속하는 문헌		
국제조사의 실제 완료일 2016년 10월 05일 (05.10.2016)	국제조사보고서 발송일 2016년 10월 10일 (10.10.2016)	
ISA/KR의 명칭 및 우편주소  대한민국 특허청 (35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사) 팩스 번호 +82-42-481-8578	심사관 김성우 전화번호 +82-42-481-3348	

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
		US 8880468 B2	2014/11/04
		US 8913483 B2	2014/12/16
		US 8958292 B2	2015/02/17
		US 8959215 B2	2015/02/17
		US 8964598 B2	2015/02/24
		US 8966040 B2	2015/02/24
		US 9007903 B2	2015/04/14
		US 9008087 B2	2015/04/14
		US 9049153 B2	2015/06/02
		US 9077664 B2	2015/07/07
		US 9106587 B2	2015/08/11
		US 9112811 B2	2015/08/18
		US 9172663 B2	2015/10/27
		US 9231891 B2	2016/01/05
		US 9300603 B2	2016/03/29
		US 9306875 B2	2016/04/05
US 2014-0115706 A1	2014/04/24	US 2015-229663 A1	2015/08/13
		US 9021092 B2	2015/04/28
		WO 2014-063110 A1	2014/04/24
US 2014-0201374 A1	2014/07/17	CN 105247826 A	2016/01/13
		EP 2936754 A1	2015/10/28
		JP 2016-509412 A	2016/03/24
		WO 2014-110453 A1	2014/07/17
US 2015-0263899 A1	2015/09/17	US 2015-0263946 A1	2015/09/17
		US 9225597 B2	2015/12/29
		WO 2015-138043 A2	2015/09/17
		WO 2015-138043 A3	2015/11/19