

SD-WAN 기반의 사용자 중심 가상 전용 네트워크 시스템 설계 및 구현

김 용 환*, 김 동 균^o

Design and Implementation of User-Oriented Virtual Dedicate Network System Based on Software-Defined Wide Area Network

Yong-hwan Kim*, Dongkyun Kim^o

요 약

KREONET은 한국과학기술정보연구원(KISTI)이 관리·운영하는 국가 R&D 연구망이다. 이는 고성능 네트워크 인프라를 기반으로 산·학·연 등 약 200여 기관을 대상으로 첨단 응용 네트워크 서비스를 지원하고 있다. 하지만 KREONET은 하드웨어 기반의 폐쇄적인 환경에 의하여 제약을 받고 있어 최근 네트워크 환경의 변화에 따른 새로운 네트워크 서비스에 대한 첨단 응용 사용자들의 다양한 요구사항을 반영하는데 한계점을 지닌다. 이에 따라, KISTI는 첨단연구 및 협업의 적시성 환경 및 프로그래머블 네트워크 인프라를 구축하고 이에 기반한 새로운 첨단 응용 서비스를 지원하기 위하여 KREONET-S 프로젝트를 출범하였다. 본 논문에서는 KREONET-S 시스템 구조 및 이의 데이터/제어 평면의 네트워크 인프라 구축 현황을 제시하고, 이에 기반하여 첨단 응용 연구자들이 필요로 하는 가상 전용 네트워크를 동적 구축하는 VDN (Virtual Dedicate Network) 서비스에 관하여 설명한다. 또한 KREONET-S 환경에 VDN 애플리케이션을 구현하고 이의 성능 분석을 수행함으로써 KREONET-S 시스템이 새로운 네트워크 패러다임의 변화에 대응하는 훌륭한 방안임을 검증한다.

Key Words : SD-WAN, Virtual Dedicate Network, Network Virtualization, Dynamic Resource Allocation

ABSTRACT

KREONET is a principal national R&E network running by KISTI in Korea. It uniquely provides production research network services for around 200 non-profit research and educational organizations, based on hybrid (IP and non-IP) network infrastructure. However, KREONET is limited to meet various needs of new network services for advanced Science & Technology (S&T) users because its infrastructure is inherently derived from classical hardware-based, fixed and closed environments. So, KREONET-S is designed to provide advanced S&T services to catch up with time-to-research and time-to-collaboration. In this paper, we present a system architecture of KREONET-S based on network infrastructure that consists of data and control planes separately. Furthermore, we propose and describe VDN service which is capable of building a virtual dedicate & bandwidth-guaranteed network for S&T group dynamically. we implement VDN application on KREONET-S and then perform performance analysis for proving that KREONET-S system and VDN application can be a good solutions to cope with new network paradigms for various advanced S&T applications and users.

* First Author : Korea Institute of Science and Technology Information, yh.kim086@kisti.re.kr, 정회원

^o Corresponding Author : Korea Institute of Science and Technology Information, mirr@kisti.re.kr, 정회원

논문번호 : KICS2016-08-209, Received August 25, 2016; Revised September 9, 2016; Accepted September 9, 2016

I. 서론

최근 인터넷을 활용하는 다양한 사용자 계층 및 기기의 출현과 함께 이에 특화된 다양한 응용 서비스들이 등장하면서 특정 환경 및 새로운 요구사항에 적합한 첨단 응용 네트워크 및 서비스의 수요가 급증하고 있다¹⁻³⁾. 하지만 현재의 네트워크 구조 및 서비스들은 새로운 네트워크 환경 및 요구사항을 반영하기에 많은 제약을 가지고 있어 국내외적으로 이를 근본적으로 해결하기 위한 연구가 활발하게 진행되고 있다⁴⁻⁹⁾. 이러한 네트워크 패러다임의 변화는 네트워크에 첨단 기능을 부여하고 있으며 이의 중심에 Software-Defined Network (SDN) 기술이 서 있다. 오늘날 SDN 기술은 보다 넓은 영역에서 동적이고 유연한 지능적인 네트워크를 제공하기 위하여 근거리 통신망(Local Area Network, LAN)의 영역을 넓혀 광역망 중심의 Software-Defined Wide Area Network (SD-WAN) 기술로 진화하고 있다^{2, 10)}. 이러한 SD-WAN의 시장 점유율은 현재 1% 미만이지만, 3년 안에 전체 사용자의 최대 30%가 SD-WAN을 이용할 것이라고 예측되는 등 다양한 네트워크 단체들은 SD-WAN 기술이 새로운 네트워크 패러다임의 주축이 될 것이라 예상하고 있다¹¹⁻¹⁴⁾.

KREONET은 1988년부터 과학기술처(현 미래창조과학부)가 지원하고 한국과학기술정보연구원이 관리 운영하는 국가 R&D 연구망이다¹⁵⁾. 이는 산·학·연 등 약 200여 기관의 주요 연구 개발 기관을 대상으로 다양한 과학기술 정보자원, 슈퍼컴퓨팅, GRID, e-Science 응용분야 등의 연구자원을 제공하기 위한 고성능 네트워크 인프라를 지원하고 있다. 그림 1에서 볼 수 있듯이 KREONET은 전국적으로 17개 지역망 센터가 운영되고 있으며, 각 센터를 기점으로 전국 어디서나 다양한 연구를 수행할 수 있는 네트워크 인프라를 구축하였다. 이를 바탕으로 국내 연구자들에게 첨단 응용연구 활동을 위한 공동협업 연구 환경을 제공함으로써 국가연구망으로서 중요한 기반 인프라 역할을 수행하고 있다.

하지만 KREONET 서비스는 하드웨어 기반의 폐쇄적인 환경에 의하여 제약을 받고 있으며 새로운 네트워크 패러다임에 부합하는 첨단 응용 서비스를 지원하는데 한계점을 지닌다. 즉, 전통적인 하드웨어 인프라를 기반으로 운용되는 KREONET은 server-client 중심의 트래픽에서 east-west, server-to-server 중심의 트래픽 급증에 따른 트래픽 패턴 변화, 가상화 기술에 따른 네트워크 서버의 수 급증에 따른 부하 조정 및

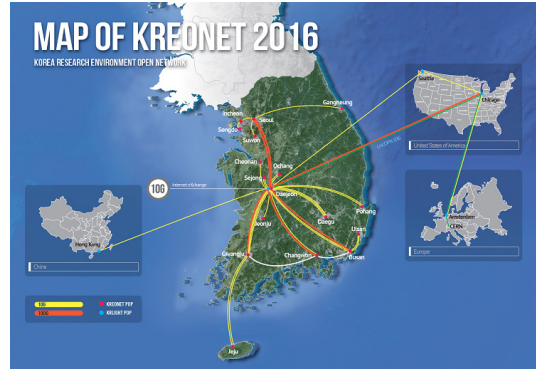


그림 1. 국내의 KREONET 네트워크 인프라 구축 현황
Fig. 1. Domestic & Global KREONET infrastructure

최적화 문제, 추상화를 고려하지 않은 고정된 토폴로지 기반의 네트워크 구조로 인한 시스템 및 구성 요소 변경의 복잡성, 총괄적인 네트워크 관리의 어려움, 벤더 의존성 등의 제약사항을 해결하기에 적합하지 않으며 이에 따라 새로운 네트워크 패러다임 및 다양한 요구사항에 대응하기 위하여 많은 시간과 비용이 요구된다¹⁶⁾.

2015년 국가과학기술연구망은 동적이고 유연한 미래인터넷으로의 효율인 전환을 위하여 KREONET의 소프트웨어화(KREONET-S^[17])를 추진 중에 있으며 소프트웨어화된 첨단연구망 인프라를 활용하여 과학기술 분야에서의 국가 초고성능 R&D 커뮤니티를 선진국 수준으로 육성 지원하고, 세계적 수준의 국내외 공동연구를 지원하고자 한다. 이러한 배경으로 출범한 KREONET-S는 크게 1) 국가별 SD-WAN 도메인 컨트롤러의 소프트웨어 기반 상호 운용을 통한 국제 프로그래머블 네트워크 인프라 구축 2) 동적인 가상/전용 네트워크 서비스의 제공을 통한 다양한 첨단연구 및 협업의 적시성 환경 구축(time-to-research and time-to-collaboration) 3) 대용량 데이터 전송과 관리를 요구하는 첨단 협업연구 환경 제공을 위한 캐리어급 SDN 제공이란 3가지 주요 사안을 목적으로 한다.

본 논문의 구성은 다음과 같다. 2장에서는 첨단 응용 서비스를 제공하기 위한 SD-WAN 기반의 KREONET-S 시스템 구조를 설명하고 이의 근간을 이루는 데이터 평면 및 제어 평면의 네트워크 인프라 구조와 구축 현황을 제시한다. 3장에서는 KREONET-S 시스템을 기반으로 첨단 응용 연구자(사용자)들이 요구하는 전용 네트워크를 짧은 시간 내 구축, 대용량 데이터 전송과 관리를 요구하는 첨단협업연구를 수행할 수 있는 가상 전용 네트워크 동적 구축(Virtual Dedicate Network, VDN) 서비스 및 사용

자중심 가상망 및 다중 계층 네트워크 가시화 (User-oriented Network Visibility, UoV) 서비스를 제공하기 위한 VDN 애플리케이션의 구조 및 기능 블록도, 동작 절차, 그리고 사용자 인터페이스에 관하여 설명한다. 4장에서는 KREONET-S 시스템 환경에서 VDN 애플리케이션의 성능에 관한 실험 환경을 구축하고 실험한 결과를 보임으로써 KREONET-S가 제공하는 VDN 서비스의 성능을 검증함과 동시에 KREONET-S 시스템이 새로운 네트워크 패러다임에 부합하는 네트워크로써 필요한 서비스 환경을 제공할 수 있음을 보인다. 마지막으로 5장에서 본 논문의 결론 및 향후 연구 방향을 제시한다.

II. SD-WAN 기반 KREONET-S 설계 및 배치

2.1 KREONET-S 시스템 구조

KREONET-S는 SD-WAN 기반의 프로그래머블/가상화 코어 및 에지/엑세스 네트워크 인프라를 구축하고 이에 기반한 첨단 응용 서비스를 지원하고 있다. 이러한 KREONET-S 시스템 및 SDN 응용 서비스들은 고에너지 물리, 천체우주, 첨단의료과학, 슈퍼컴퓨팅 등 다양한 첨단 응용 연구 및 과학 분야의 첨단협업연구를 위하여 고안되었다.

KREONET-S 시스템은 크게 하드웨어 및 소프트웨어 SDN 장비들로 구성된 네트워크 인프라, SDN

기반의 분산 제어 플랫폼, 첨단 응용 애플리케이션 및 서비스 등의 3가지 주요 부분으로 구성된다. 그림 2는 이러한 KREONET-S시스템의 구성요소 및 이의 관계를 보여준다. 첫 번째 부분은 실질적으로 사용자들에게 다양한 네트워크 서비스를 지원하기 위하여 데이터 송수신을 수행하는 데이터 평면 네트워크 인프라이다. 이는 네트워크의 CAPEX와 OPEX를 줄이기 위하여 SDN 기반의 다양한 프로그래머블 장비들로 구축되었다. 두 번째 부분은 OpenFlow, TL1, NETCONF 등의 Southbound API를 활용하여 데이터 평면 네트워크 인프라를 구성하는 다양한 하드웨어 및 소프트웨어 장비들을 총괄 제어 및 관리하는 역할을 수행하는 분산 제어 플랫폼이다. 이러한 제어 평면 인프라의 경우 KREONET-S의 고가용성, 장애복구, 확장성 등을 고려하여 다수의 SDN 제어 기기들을 분산 배치하고 가상의 중앙 집중형 방식으로 구축 및 운용 중에 있다. 그리고 이 때, 분산 제어 환경 및 East-Westbound API의 경우 Open Network Operating System (ONOS)^[18]을 채택하였다. 세 번째 부분은 위의 두 인프라(데이터 평면, 제어 평면)를 기반으로 ONOS가 제공하는 JAVA, REST API 등의 Northbound API를 활용하여 첨단 응용 사용자들을 위한 고성능의 다양한 애플리케이션 및 서비스를 제공한다. II-2절에서는 첫 번째와 두 번째 파트인 KREONET-S 시스템의 데이터 평면 및 제어 평면 네

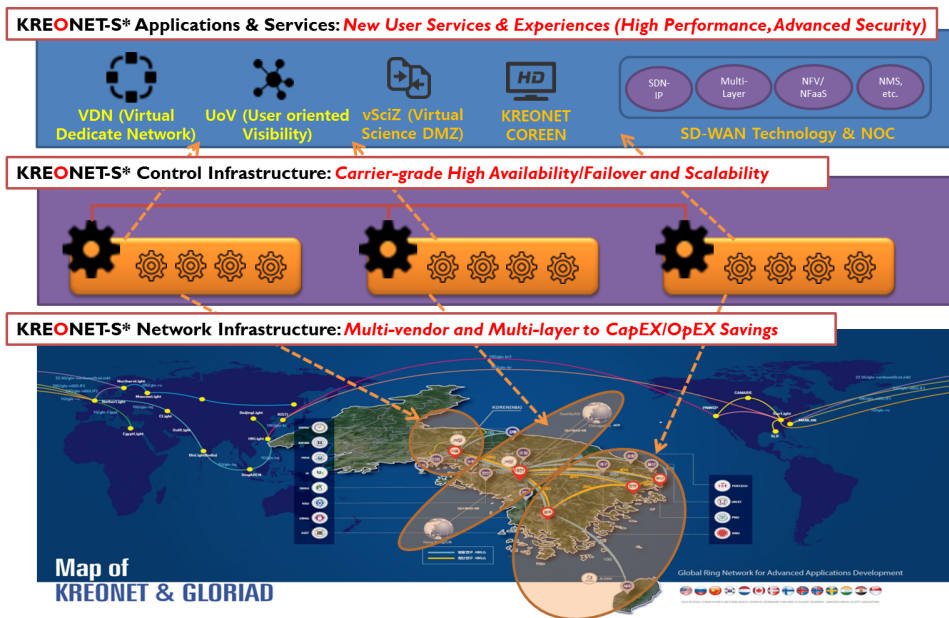


그림 2. KREONET-S 시스템의 구성 요소 및 관계
Fig. 2. System component and their relationship of KREONET-S

트위크 인프라에 대하여 기술하고, 이에 기반한 응용 애플리케이션 및 서비스 파트는 II-3절에서 상세히 다루도록 한다.

2.2 데이터 평면 설계 및 구축 현황

KREONET-S의 데이터 평면 네트워크 인프라는 크게 하드웨어 스위치와 소프트웨어 스위치로 구성되며 이들은 지리상으로 대전과 서울의 KREONET 지역망 센터에 구축되어 있다. 각 지역망 센터에는 하드웨어 스위치 장비로 코어 노드 및 에지 노드가 구축되어 있으며 이와 함께 소프트웨어 스위치로써 다수의 Open vSwitch (OVS)들이 범용 서버 상에 구축되어 있다. 한편, 하드웨어 스위치들 사이의 링크는 다중 링크로 구성되며 이는 10개의 1Gbps와 1개의 10Gbps 링크들로 이뤄진다. 또한 하드웨어 스위치와 OVS 스위치 혹은 OVS 스위치들 사이의 링크의 경우 10Gbps의 대역폭을 지닌다. 그림 3은 ONOS에서 제공하는 GUI를 통하여 이러한 하드웨어 및 소프트웨어 스위치 기반 KREONET-S의 물리적인 네트워크 토폴로지를 보여준다.

한편, 서로 다른 지역 간의 하드웨어 스위치 사이의 네트워크 구성은 패킷 광 전송(Packet Optical Transport) 기반의 다중 계층(Multi Layer) 구조로 구성되었으며 이는 효율적인 네트워크 운용 및 이에 수반하는 비용 절감의 측면에서 기존에 구축되어 운영 중인 KREONET 네트워크를 활용한다. 그림 4는 이

러한 스위치 사이의 광 전송을 위한 하드웨어 스위치와 광 전송 장비간의 연결 현황 및 대전-서울 간의 광 전송 구간을 보여준다.

2.3 데이터 평면 설계 및 구축 현황

KREONET-S는 제어 평면을 담당하는 SDN 기반의 분산 제어 플랫폼으로 ONOS를 채택하여 제어 평면 네트워크 인프라를 구축 및 운영 중에 있다. ONOS 기반의 분산 제어 플랫폼 환경을 구성한 가장 큰 이유는 여타의 단일 SDN 컨트롤러 기반의 제어 플랫폼의 경우 ONOS 비하여 보다 다양한 Southbound API를 지원할지는 모르나 잠재적인 단일 장애 지점(single point of failure, SPOF) 문제가 있어 실질적으로 첨단 응용 사용자들에게 안정적인 서비스를 제공하는데 많은 제약을 가져오기 때문이다. ONOS의 경우 다수의 분산형 컨트롤러들의 클러스터링을 통하여 가상의 중앙집중형 제어 환경을 제공하기 때문에 KREONET-S 시스템 및 서비스의 고가용성 및 확장성 측면에서 여타의 SDN 분산 제어 시스템에 비해 보다 우수하다¹⁹⁾.

KREONET-S 제어 평면의 네트워크 인프라는 7개의 SDN 컨트롤러 장비들을 추적으로 구성되어 있으며 이들은 하나의 동기화된 SDN 클러스터를 형성한다. 이러한 SDN 컨트롤러 장비들은 그림 4에서 볼 수 있듯이 3개는 대전 지역망 센터에 위치하고 4개는 서울 지역망 센터에 구축되어 운영 중에 있으며, 이들은

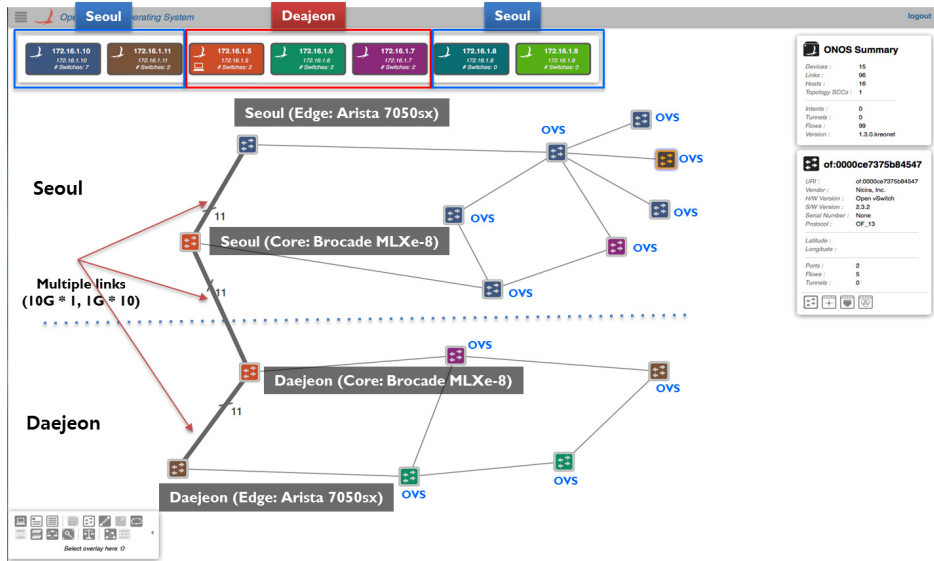


그림 3. KREONET-S의 물리적인 네트워크 토폴로지
Fig. 3. Physical network topology of KREONET-S

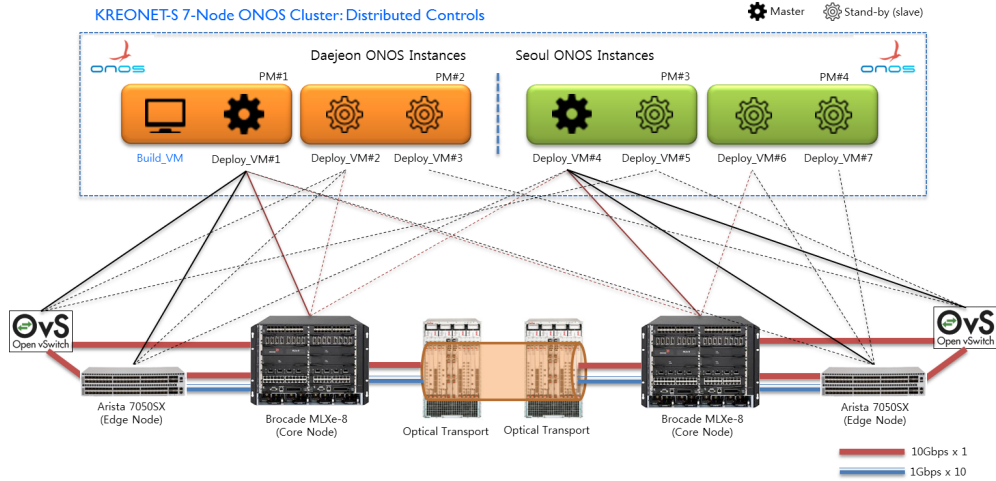


그림 4. KREONET-S 제어 평면 인프라
Fig. 4. Control plane infrastructure of KREONET-S

각각 데이터 평면의 하드웨어 및 소프트웨어 스위치와 연결되어 KREONET-S의 물리적인 네트워크 인프라를 관장한다. 그리고 이 때, 고가용성을 보장하기 위하여 각각의 스위치들은 3개 이상의 SDN 컨트롤러에 연결되어 있으며 이 중 마스터 노드가 선정되어 해당 스위치를 담당한다. 그러다 이후 임의의 스위치의 마스터 노드가 예상하지 못한 문제로 인하여 고장 나거나 동작이 멈추게 되어 본래의 기능을 담당하지 못할 경우, 나머지 노드들 중 하나의 노드가 해당 스위치의 마스터 노드의 역할을 위임받아 첨단 응용 서비스의 무결정설을 보장한다. 각 스위치와 마스터 노드 관계의 경우, 그림 3과 같이 ONOS에서 제공하는 GUI를 통하여 SDN 컨트롤러와 스위치의 색상의 구분만으로 쉽게 식별 가능하다.

그림 5는 앞서 설명한 KREONET-S의 대전 지역망 센터에 배치된 데이터 평면 및 제어 평면을 담당하는 실제 장비들의 구축 모습을 보여준다. 서버 랙의

상단에는 4개의 고성능의 범용 서버가 위치해 있으며 각 서버마다 3개의 가상 머신(Virtual Machine, VM) 들을 설치하였다. 그리고 VM 위에 3개의 ONOS 컨트롤러, 다수의 OVS 스위치, 실험 및 측정 서버들을 배치하였다. 서버 랙의 하단에는 하드웨어 스위치인 코어 및 에지 스위치를 배치하였으며 관리 및 제어 영역의 정보 교환을 위한 장비 또한 배치하였다. 이들 사이의 연결은 위의 구조에 적합하도록 양방향으로 연결되어 있으며 서울 지역망 센터로의 데이터 및 제어 평면의 정보 교환은 하단에 위치한 장비들을 통하여 이뤄진다. 한편, KREONET-S의 서울 지역망 센터의 경우 또한 ONOS 컨트롤러가 4개인 점을 제외하고는 거의 동일한 형태로 구축되어 운영 중에 있다.

III. VDN 애플리케이션 개발

3.1 VDN 애플리케이션 구조 및 기능

KREONET-S는 차세대 네트워크 기술인 SD-WAN을 활용하여 연구자가 요구하는 전용 네트워크를 짧은 시간 내 구축, 대용량 데이터 전송과 관리를 요구하는 첨단협업연구를 수행할 수 있는 VDN 애플리케이션을 제공한다. 이는 네트워크 추상화 기반 UI/UX를 고려한 사용자 기반 가상 전용 네트워크 동적 구축 서비스로 사용자 중심 가상망 및 다중 계층 네트워크 가시화 기술 및 서비스를 포함한다.

VDN 애플리케이션은 가상 전용 네트워크를 필요로 하는 임의의 사용자 그룹만을 위하여 가상 전용 네트워크에 참여하는 호스트들의 식별자, 가상 전용 네

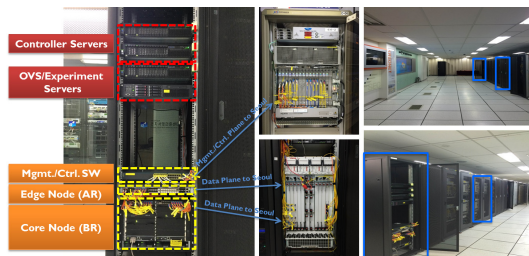


그림 5. 대전 지역망 센터의 KREONET-S 데이터 및 제어 장비 구축 모습
Fig. 5. KREONET-S network device installation in Daejeon, Korea

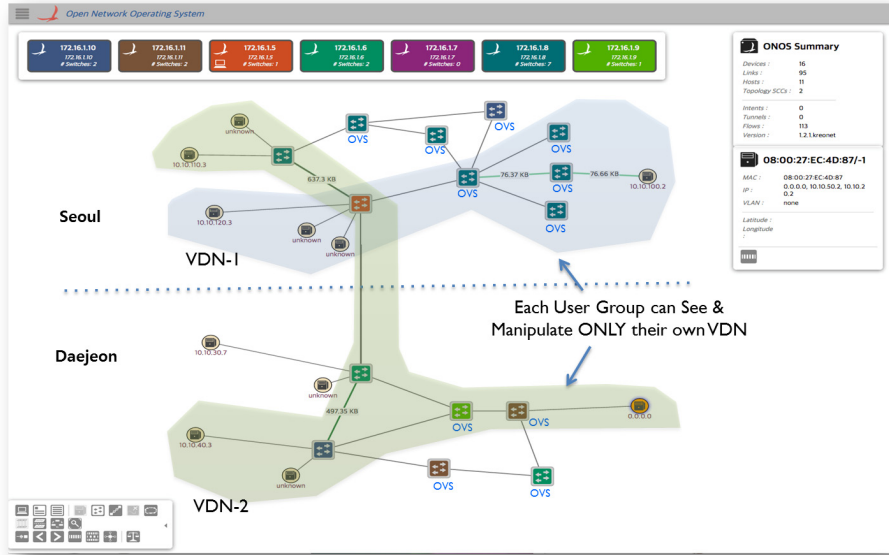


그림 6. KREONET-S 상의 독립적인 가상 전용 네트워크
 Fig. 6. Network Isolation by VDN on KREONET-S

트위크의 요구 대역폭을 입력받아 전체 네트워크 토폴로지를 토대로 참여 호스트들 사이의 전송 대역폭을 보장하는 물리적인 경로를 포함한 가상 전용 네트워크를 제공한다. 이는 참여 호스트를 중심으로 대역폭을 보장하는 네트워크 트리를 생성하고 이를 기반으로 물리적 네트워크 자원을 해당 가상 네트워크에 동적으로 할당함으로써 이뤄진다. 한편, 생성된 가상 전용 네트워크들은 ONOS 분산 제어 플랫폼에 의하여 상호 독립적으로 운영 및 관리되며 그들 사이의 데이터 통신 또한 제한된다. 이러한 가상의 독립된 네트워크를 구성 및 운용함으로써 임의의 사용자 그룹 간의 데이터 전송 보안을 강화함과 동시에 전송 효율을 향상시킬 수 있다. 그림 6은 이러한 KREONET-S 상의 독립적으로 운영 및 관리되는 가상 전용 네트워크의 예를 보여준다.

VDN 애플리케이션의 사용자는 super/admin, root, common 등의 3가지 사용자 권한을 가질 수 있으며 이에 따라 허용된 네트워크 정보 및 기능이 제한된다. super/admin 사용자(관리자)의 경우 전체 네트워크 토폴로지를 볼 수 있으며 KREONET-S 상의 모든 VDN을 관리 및 제어(생성, 갱신, 삭제)할 수 있다. root 사용자의 경우 자신의 포함한 특정 VDN들의 네트워크 토폴로지만을 볼 수 있으며 자신이 생성한 VDN에 한하여 관리 및 제어가 가능하다. common 사용자의 경우, VDN 관리 및 제어 권한이 없으며 super 및 root 사용자가 생성한 VDN에 포함된 경우 해당 VDN 네

트위크 토폴로지만을 볼 수 있다. 그리고 이 때, 사용자는 자신에게 제공되는 네트워크 토폴로지에 한하여 네트워크 자원 활용이 가능하다.

VDN 애플리케이션은 ONOS가 제공하는 Northbound API를 활용하여 개발되었으며 크게 VDN 코어 및 사용자 기반 네트워크 가상화를 담당하는 onos-gui-vdn와 생성된 VDN을 기반으로 데이터 전송을 담당하는 onos-app-fwd-vdn 부분으로 구분된다. 이의 상세한 VDN 애플리케이션 구조 및 기능 블록도는 그림 7에서 볼 수 있다.

onos-gui-vdn에서 VDN 코어는 크게 사용자 관리 (User Manager), 동기화 관리(Synchronization Manager), VDN 관리(VDN Manager), 데이터베이스 관리(Database Manager)의 4가지 구성요소로 이뤄진다. 먼저 사용자 관리는 3가지 사용자 타입에 따른 등록 및 인증 기능을 담당한다. 동기화 관리는 ONOS 분산 제어 플랫폼이 가지고 있는 네트워크 정보를 데이터베이스와 동기화하는 기능을 제공한다. VDN 관리는 가상망 생성 시 종단간 경로를 찾아 트리를 구성하고 이에 해당하는 네트워크 자원을 가상 전용 네트워크에 할당하는 역할을 수행한다. 데이터베이스 관리는 데이터베이스에 접근하여 쿼리문을 던지는 역할을 수행한다. 한편, 네트워크 가상화는 VDN 생성, 갱신, 삭제, 정보 표현을 웹 GUI를 통하여 수행하는 기능과 생성된 VDN을 네트워크 토폴로지 관점과 종단간 관점으로 웹 GUI를 통해 보여주는 기능을

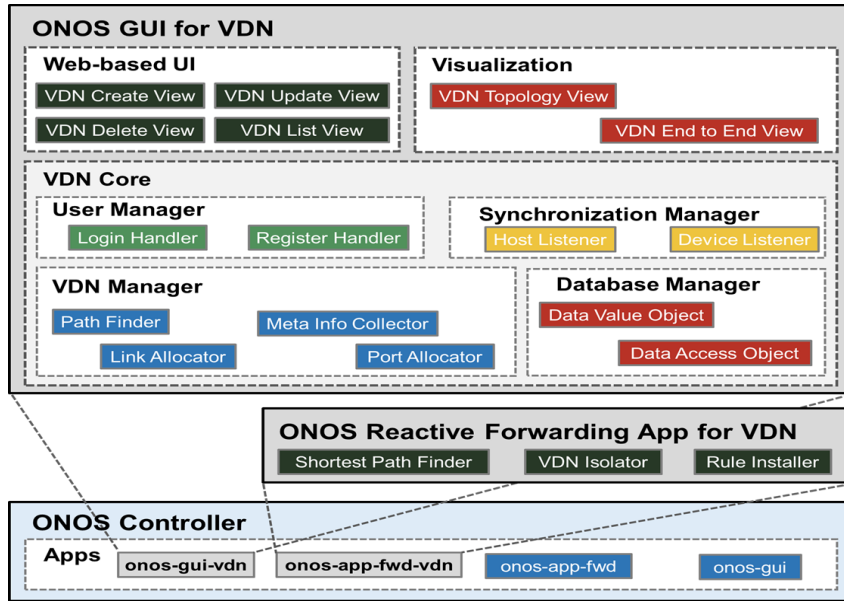


그림 7. VDN 애플리케이션 구조 및 기능 블록도
 Fig. 7. Overall VDN application architecture and function blocks

수행한다.

onos-app-fwd- vdn는 VDN 호스트들 간의 최적 경로를 찾는 Shortest Path Finder와 해당 경로상의 스위치에 플로우 규칙을 내리는 Rule Installer, 그리고 서로 다른 VDN 간에 통신 접근을 제어하는 VDN Isolator로 구성된다. 이에 관한 상세한 기능 및 절차는 III-2절에서 다루도록 한다.

3.2 VDN 환경 기반 데이터 전송 방안

SD-WAN 기반의 물리적으로 구축된 KREONET-S 네트워크상에 VDN 애플리케이션을 구동하면 ONOS 분산 제어 플랫폼은 초기에 전체 네트워크를 하나의 커다란 가상 전용 네트워크로 인식하며 이를 디폴트 가상 네트워크라 명명한다. 이 후, 임의의 호스트가 KREONET-S에 접속하고 아무런 가상 전용 네트워크에 참여되지 않은 경우 디폴트 가상 전용 네트워크에 포함된다. 즉, 가상 전용 네트워크에 참여되지 않은 호스트들 사이의 통신은 디폴트 가상 전용 네트워크를 통하여 이뤄진다.

그리고 이후, 가상 전용 네트워크가 구축되면 위의 시스템 및 방법에 의하여 독립된 네트워크(Isolated Network)가 형성되고 해당 네트워크에 속한 호스트와 디폴트 가상 전용 네트워크에 속한 호스트 사이의 통신은 제한된다. 즉, VDN 서비스 환경에서는 동일한 가상 전용 네트워크내의 호스트들 사이의 통신만이

허용된다. 이 때, ONOS 분산 제어 플랫폼은 임의의 가상 전용 네트워크 내의 호스트들 사이의 통신을 위하여 전체 네트워크가 아닌 해당하는 가상 전용 네트워크에서 데이터 전송 경로를 탐색하기 때문에 플로우 규칙 생성 시간을 현저히 줄일 수 있다.

위의 시스템 및 방법을 통하여 구축된 가상 전용 네트워크들은 ONOS 분산 제어 플랫폼에 의하여 상호 독립적으로 운영 및 관리되며, 이에 따라 배타적인 가상 전용 네트워크 간 상호 통신 또한 제한되는 독립된 네트워크이다. ONOS 분산 제어 플랫폼에 의하여 독립적으로 운영되는 가상 전용 네트워크에서의 데이터 통신은 기본적으로 배타적인 방식으로 동작한다. 즉, 배타적 데이터 통신 기법을 활용하여 가상 전용 네트워크 사이의 서로 다른 가상 전용 네트워크 내의 호스트들 사이의 통신을 제한하여 데이터 전송 보안을 강화함과 동시에 전송 효율을 향상시킨다. 이에 관한 onos-app-fwd- vdn의 데이터 전송 절차는 다음과 같다.

[onos-app-fwd- vdn 데이터 전송 절차]

- 1) SDN 스위치로부터 유입된 제 1 패킷에 관한 패킷-인 메시지(Packet-In Message) 수신하는 단계;
- 2) 메시지 내의 출발지 주소와 목적지 주소에 해당하는 호스트들의 가상 전용 네트워크 식별자를 비교하는 단계;
- 3-1) 상기 가상 전용 네트워크 식별자가 다를 경우,

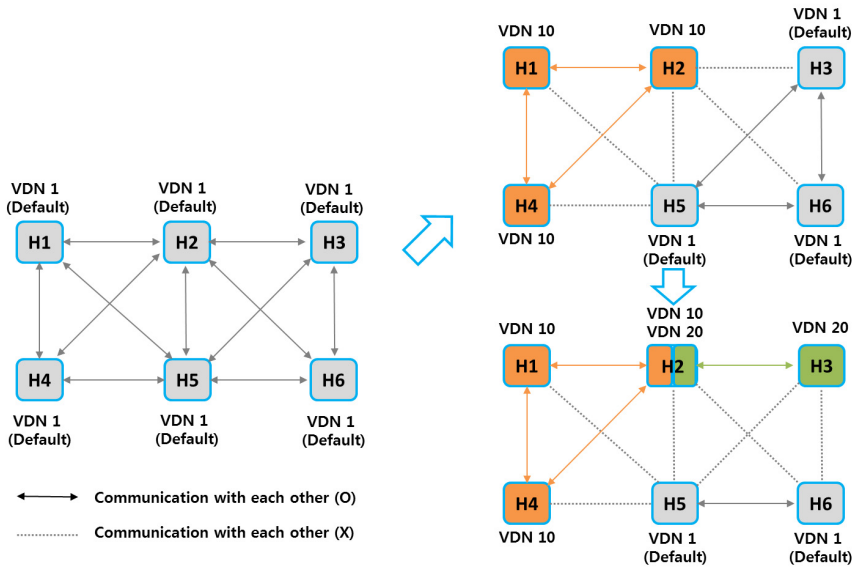


그림 8. 독립되어 운영되는 VDN 환경에서의 데이터 전송 사례
 Fig. 8. Example for data transmission on isolated VDN environments

- 해당 패킷의 전송을 제한하는 단계;
- 3-2) 동일한 경우, 상기 가상 전용 네트워크에 해당하
 는 네트워크 토폴로지(트리)를 인지하는 단계;
 - 4) 상응하는 VDN 정보에 입각하여 제 1 패킷에 관
 한 플로우 규칙을 생성하여 SDN 스위치로 전송
 하는 단계.

그림 8은 이러한 VDN 서비스의 데이터 전송 예를 보여준다. 네트워크에 아무런 가상 전용 네트워크가 생성되지 않은 경우, 모든 호스트들은 디폴트 가상 전용 네트워크를 통하여 통신이 가능하다. 이후 호스트 (H) 1, 2, 4를 위한 VDN 10이 생성되면 해당 호스트 간의 통신은 VDN 10을 통하여 이뤄지며 그 외의 호스트들과는 통신이 제한된다. 이후 H2와 H3를 위한 VDN 20이 생성될 경우, 마찬가지로 이들 간의 통신은 VDN 20을 통하여 이뤄지며 나머지 호스트들과 통신은 제한된다. 이 때, H2는 H1, H4와는 VDN 10을 통하여 통신하며 H3와는 VDN 20을 통하여 통신할 수 있으며 H5, H6와의 통신은 제한된다. H3의 경우 H2를 제외한 모든 호스트와의 통신이 제한된다. 한편 아무런 VDN에 속하지 않은 H5와 H6은 여전히 디폴트 VDN을 통하여 통신 가능하며 나머지 호스트와의 통신은 제한된다.

3.3 VDN 애플리케이션 구현 및 사용자 인터페이스

VDN 애플리케이션은 ONOS 분산 제어 플랫폼과

부합하도록 VDN 코어 및 데이터 전송 모듈(내부)은 JAVA, 네트워크 가상화 및 Web UI 모듈(외부)의 경우 AngularJS 기반으로 구현하였다.

임의의 사용자가 KREONET-S 시스템에 접속하여 인증 절차를 마치고 나면, 관리자에 의하여 부여받은 권한에 따라 VDN 관리/제어(생성, 갱신, 삭제) 및 생성된 VDN의 활용 범위가 달라진다. 기본적으로 사용자는 자신이 속한 VDN을 활용할 수 있으며 해당하는 VDN의 토폴로지 및 정보를 Web UI를 통하여 볼 수 있으며 그 외의 VDN은 활용하지도 정보를 볼 수도 없다. 하지만 VDN 관리 및 제어의 경우 관리자와 root 사용자만이 가능하며 이들의 차이는 관리자의 경우 전체 네트워크 토폴로지 정보를 모두 알 수 있으며 이에 따른 KREONET-S 상의 모든 VDN의 관리 및 제어가 가능한 반면 root 사용자는 관리자에 의하여 부여받은 부분 정보 및 자신이 생성한 VDN에 한하여 관리 및 제어가 가능하다는 점이다.

VDN 관리 및 제어는 GUI를 통하여 쉽고 빠르게 수행되며 그림 9는 VDN 생성에 관한 GUI를 보여준다. VDN 생성을 위하여 해당 VDN의 명칭을 입력하고 VDN 요구 대역폭, 호스트 리스트를 그리고 생성된 VDN을 활용한 사용자를 GUI를 통하여 선택하면 ONOS 제어 플랫폼이 가지고 있는 네트워크 토폴로지 정보를 기반으로 요구 대역폭을 보장하는 VDN 참여 호스트 간의 가상 전용 네트워크를 생성하고 선택한 사용자들이 해당 VDN을 활용할 수 있는 권한을

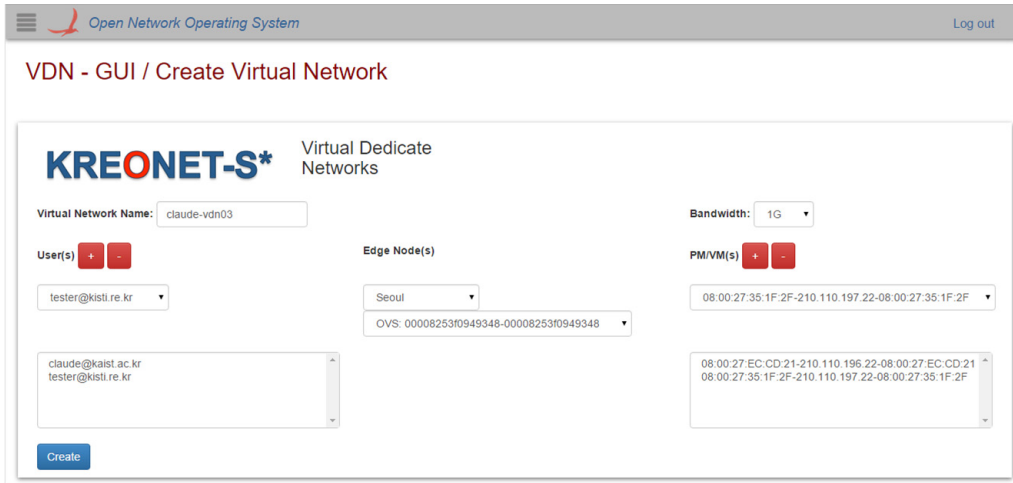
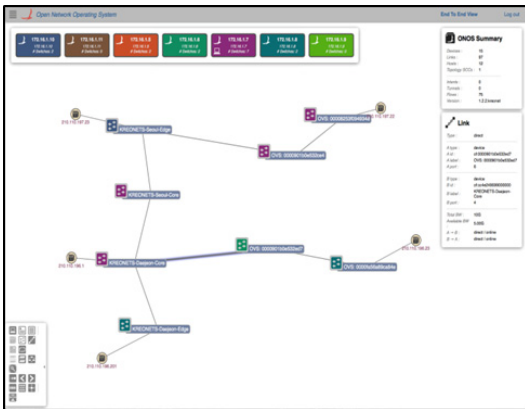


그림 9. VDN 생성을 위한 GUI
 Fig. 9. Graphical user interface (GUI) for VDN manipulation (creation case)

VDN ID	VDN Name	VDN Bandwidth (Gbps)	User Email	Device Name	Host Name
332	mirr-vdn01	1	mirr@kisti.re.kr, claude@kaist.ac.kr, ymseo@kasi.re.kr	KREONETS-Seoul-Edge, KREONETS-Daejeon-Edge, KREONETS-Daejeon-Core, KREONETS-Seoul-Core, OVS: 00008253f0949348, OVS: 0000901b0e532e4, OVS: 0000901b0e532e4, OVS: 0000f56a89ca84e	08:00:27:D9:48:C4, 08:00:27:35:1F:2F, 44:8A:5B:F3:19:8D, 08:00:27:10:55:B8, 08:00:27:EC:CD:21

(a) 텍스트 형식의 VDN 정보 확인



(b) VDN 네트워크 토폴로지 화면



(c) VDN 참여 호스트간 중단 화면

그림 10. Web UI를 통한 VDN 토폴로지 정보 및 모습 확인
 Fig. 10. VDN topologies and information on Web UI

부여한다. 한편 VDN 생성이 완료되면 사용자 편의에 따라 VDN 정보를 그림 10(a)과 같이 Web UI를 통하여 텍스트 형식으로 보거나 그림 10(b) 혹은 그림 10(c)과 같이 그래픽 형태로 볼 수도 있다. 그리고 이

때, VDN 애플리케이션은 VDN 네트워크 토폴로지 화면과 함께 VDN 참여 호스트들에 관한 중단간 화면 또한 제공하고 있어 보다 다양한 사용자 요구사항을 충족시키고자 한다.

IV. 성능분석

본 장에서는 KREONET-S 시스템 환경에서 VDN 애플리케이션의 성능에 관한 실험 환경을 구축하고 실험한 결과를 보인다. 여기서 VDN 애플리케이션의 성능은 SDN 컨트롤러의 수와 VDN 참여 호스트의 수, 그리고 네트워크 규모(에지 스위치의 수)에 따른 VDN 생성 및 갱신 속도를 비교 분석함으로써 측정토록 한다. 그리고 이 때, 네트워크 토폴로지는 기본적으로 2장에 제시된 KREONET-S 토폴로지를 기반으로 하며 네트워크 규모의 확장을 위하여 OVS 스위치를 활용하였다. 이를 통하여 구축한 시스템 및 서비스가 국가별 SDN 도메인 컨트롤러의 소프트웨어 기반 상호 운용을 통한 국제 프로그래머블 네트워크 인프라 구축, 동적인 가상/전용 네트워크 서비스의 제공을 통한 다양한 첨단연구 및 협업의 적시성 환경 구축, 그리고 대용량 데이터 전송과 관리를 요구하는 첨단 협업연구 환경 제공을 위한 캐리어급 SDN 제공이란 목적에 부합함을 보이고자 한다.

먼저, 단일 컨트롤러를 기반으로 임의의 VDN을 생성함에 있어 참여 호스트의 수에 따른 VDN 애플리케이션의 성능을 실험하기 위하여 각 지역의 에지 스위치 당 접속 호스트 수를 1에서 10까지 증가시켜가며 VDN 생성 시간을 측정하였다. 그리고 이 때, 보다 현실적인 실험 결과를 획득하기 위하여 KREONET-S 상의 4개의 하드웨어 스위치만을 활용하였다. 또한 이의 실험을 SDN 컨트롤러의 수를 2개 혹은 3개로 변경한 상태에서도 동일하게 수행하였다. 그림 11은 단일 혹은 SDN 클러스터 상에서 VDN 참여 호스트 수

의 증가에 따른 VDN 생성 시간을 보여준다. 이를 통하여 VDN 참여 호스트의 수가 증가함에 따라 VDN 생성 시간은 선형적으로 증가함을 볼 수 있다. 또한 VDN 생성 시간은 VDN 참여 호스트의 수가 2개 또는 20개일 경우, 각각 평균적으로 260ms, 550ms가 소요된 것으로 보아 VDN 참여 호스트 수에 대한 VDN 생성 시간의 증가율은 그리 크지 않음을 알 수 있다. 한편, 전반적으로 SDN 컨트롤러 수에 따라 미세하게 VDN 생성 시간이 더 소요되지만 이의 성능 차이는 미비하여 VDN 생성 과정에 중대한 영향은 미치지 않음을 확인할 수 있었다.

그림 12는 VDN 참여 호스트의 수의 증가에 따른 VDN 갱신 시간을 측정한 결과를 그래프로 나타낸 것이다. 이의 실험은 최초 각 지역의 호스트 1개씩, 총 2개의 호스트를 포함하여 서울, 대전 간 VDN을 생성한 후 기존의 호스트를 변경하거나 새로운 호스트를 추가하는 방식으로 측정하였다. 그 이외의 조건은 위의 실험과 동일하다. VDN 갱신 시간의 경우, VDN 생성 시간의 경우와 마찬가지로 VDN 참여 호스트의 수에 따라 선형적으로 증가함을 알 수 있으며 마찬가지로 이의 증가율 또한 그리 크지 않음을 확인할 수 있었다. 하지만 VDN 갱신 시간은 동일한 VDN 참여 호스트의 수에 대하여 VDN 생성 시간 보다 수십ms 정도 더 걸리는 경향을 보이고 있는데 이는 VDN 갱신 과정이 이미 만들어진 VDN 정보를 삭제하고 변경된 정보를 토대로 새로운 VDN을 생성함으로써 생기는 결과로 보인다.

2-node cluster와 3-node cluster 상의 VDN 갱신 시간은 단일 컨트롤러일 때와 비교하여 거의 비슷한

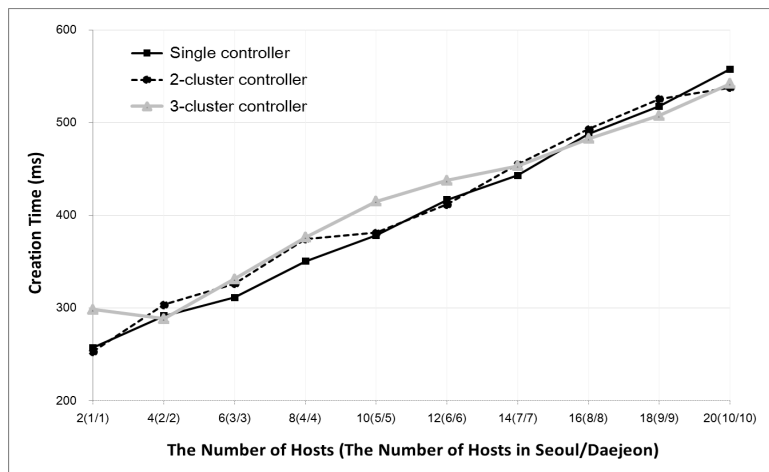


그림 11. The impact of the number of VDN hosts on VDN creation time (ms)
Fig. 11. VDN 참여 호스트 수의 증가에 따른 VDN 생성 시간

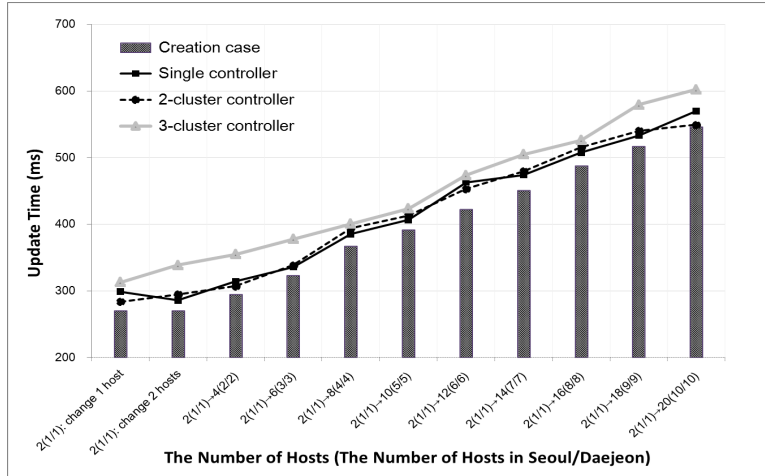


그림 12. The impact of the number of VDN hosts on VDN update time (ms)
 Fig. 12. VDN 참여 호스트 수의 증가에 따른 VDN 갱신 시간

생성시간이 걸리지만 3-node cluster 갱신 시간은 단일 컨트롤러와 2-node cluster일 때와 비교하여 20~50ms 정도 더 걸린 것으로 나타났다. 이는 VDN 갱신 과정에서 컨트롤러 간 동기화에 대한 시간 소모로 추정된다. 하지만 이 또한 VDN 생성 때와 마찬가지로 성능 차이가 미비하고 당시 네트워크 환경에 따라 많이 좌우되기 때문에 VDN 참여 호스트의 수에 따른 VDN 갱신 과정에 중대한 영향은 미치지 않는다.

다음으로 네트워크 규모가 커짐에 따라 VDN 생성 및 갱신 시간의 추이를 살펴보고자 한다. 이를 측정하기 위하여 네트워크의 규모를 결정하는 SDN 스위치와 VDN 참여 호스트 그리고 이에 따른 관련 링크를 추가한 실험을 4개의 하드웨어 스위치만을 사용했던 이전의 두 실험과 비교 분석하였다. 그리고 이 때, 네

트워크 스위치 구성 시 실질적인 하드웨어 스위치 증설 및 이에 부합하는 환경 구축의 비용과 소요 시간이 큰 관계로 각 지역망 센터의 코어 스위치를 제외하고는 OVS 스위치를 생성하고 이를 물리적 링크로 연결하여 네트워크 토폴로지를 확장 구성하였다.

그림 13은 네트워크 규모(VDN 참여 호스트의 수, 스위치의 수)의 증가에 따른 VDN 생성 시간을 나타낸다. 여기서 “Fixed Case”는 네트워크 규모가 고정된 4개의 하드웨어 스위치 기반의 환경에서 VDN 참여 호스트의 수에 따른 VDN 생성 시간을 측정한 결과이며, “Non-Fixed Case”는 2개의 코어 스위치를 제외하고 VDN 참여 호스트의 수에 맞춰 OVS 스위치를 일정하게 증가시켜 가며 VDN 생성 시간을 측정한 결과를 의미한다. 이 두 가지 경우의 차이는 OVS 스

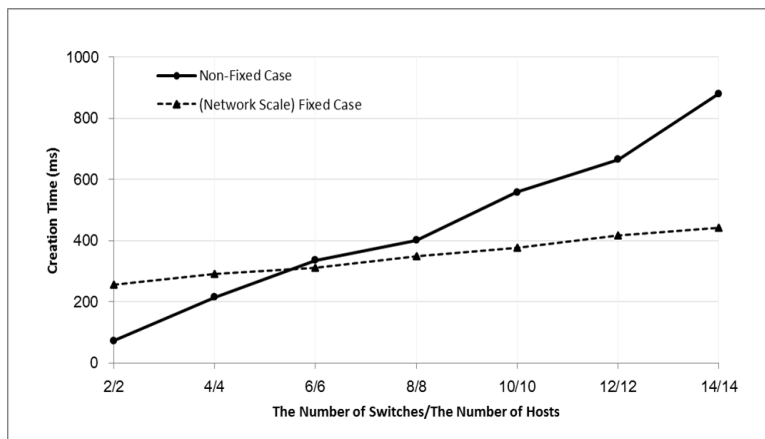


그림 13. The impact of network scale on VDN creation time (ms)
 Fig. 13. 네트워크 규모(호스트의 수, 스위치의 수)의 증가에 따른 VDN 생성 시간

위치와 VDN 참여 호스트의 수가 증가함에 따라 더욱 두드러지는데 이는 네트워크 규모가 커짐에 따라 VDN 호스트들 사이의 종단간 경로를 검색함에 있어 더 많은 시간이 소요되고, 이는 결국 전체 VDN 생성 시간의 증가를 가져오기 때문으로 보인다. 여기서 4/4의 경우 스위치의 수와 호스트의 수가 같음에도 “Non-Fixed Case”의 VDN 생성 시간이 더 빠른 이유는 에지 스위치를 하드웨어 스위치에서 소프트웨어 스위치인 OVS로 변경함으로써 물리적으로 발생하는 오버헤드가 고려되지 않기 때문으로 보인다. 이러한 측면을 감안할 때 전체 네트워크 구성이 하드웨어 스위치 기반으로 이뤄진다고 가정할 때 네트워크 규모에 따른 VDN 생성 시간의 영향은 더욱 클 것이라 예상된다.

그림 14는 네트워크 규모의 증가에 따른 VDN 갱신 시간을 측정된 결과를 그래프로 나타낸 것이다. 전반적으로 네트워크 규모에 따른 VDN 갱신 시간은 VDN 생성 시간과 유사한 결과를 보인다. 하지만 소요 시간의 차이는 기존에 생성되어 운영되던 VDN을 갱신하는 경우 조금 더 두드러짐을 보인다. 이는 VDN 갱신 과정은 기존 정보 삭제 과정과 함께 새로운 환경에 부합하도록 새로운 정보 생성이라는 측면에서 볼 때, 이의 차이는 기존 VDN 정보 삭제 시간의 증가 폭에서 찾을 수 있다. 즉, 네트워크가 규모가 커질수록 VDN 갱신에 따른 네트워크 전반에 설정된 기존 VDN의 정보를 삭제하기 위한 소요 시간 또한 선형적으로 증가함을 알 수 있다.

V. 결론

본 논문에서는 하드웨어 및 소프트웨어 SDN 장비들로 구성된 네트워크 인프라, SDN 기반의 분산 제어 플랫폼, 첨단 응용 애플리케이션 및 서비스 등 3가지 주요 파트들로 이뤄진 KREONET-S 시스템 구조를 설명하고 이의 네트워크 인프라 구축 현황에 대하여 알아보았다. 그리고 구축된 프로그래머블 네트워크 인프라를 기반으로 첨단연구 및 협업의 적시성 환경을 제공하기 위한 가상 전용 네트워크 동적 구축 서비스인 VDN 애플리케이션의 구조, 기능, 데이터 전송 절차, 사용자 인터페이스 등에 대하여 상세히 기술하였다. 또한 VDN 애플리케이션을 KREONET-S 시스템에 실제 구현하여 성능 분석을 수행하였고, 이를 통하여 KREONET-S 시스템 및 VDN 애플리케이션이 새로운 네트워크 패러다임의 변화에 따른 첨단 응용 연구 및 사용자들의 다양한 요구사항에 대응하는 훌륭한 방안이 될 수 있음을 알아보았다.

본 KREONET-S 시스템은 추후 다수의 KREONET 지역망 센터 및 국제 연구망 센터로 그 영역을 확장할 계획에 있으며 이를 통하여 국제협력 연구 수행 및 효율적인 사용자 중심 국제 네트워킹 운영 환경 제공을 제공하고자 한다. 또한 이러한 KREONET-S 시스템을 기반으로 SDN-IP망, SDN망간 연동기술, 가상 대용량 데이터 전송/협업 환경 제공을 위한 Virtual Science DMZ (vSciZ) 기술, NFV 서비스 체이닝, 네트워크 슬라이싱 기술 등을 연구하고 이를 토대로 보다 다양한 첨단 응용 서비스들을 제공할 계획이다. 이를 통하여 향후 KREONET-S가 고

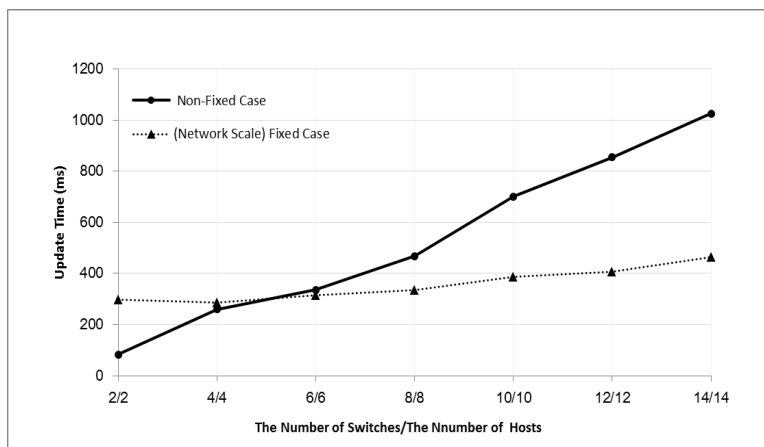


그림 14. The impact of network scale on VDN update time (ms)
 Fig. 14. 네트워크 규모(호스트의 수, 스위치의 수)의 증가에 따른 VDN 갱신 시간

에너지 물리, 친체우주, 첨단의료과학, 슈퍼컴퓨팅 등 다양한 국내외 첨단 응용 연구 및 과학 분야의 첨단협업연구 환경을 제공함으로써 국가연구망으로서 중요한 소프트웨어 기반 인프라 역할을 수행하기를 기대한다.

References

- [1] Cisco Visual Networking Index, *Forecast and Methodology*, Cisco White Paper(2014-2019), 2015.
- [2] M. K. Weldon, *The Future X Network: A Bell Labs Perspective*, Taylor & Francis Group, LLC 2016.
- [3] A. Manzalini, et al., "Software-defined networks for future networks and services," *White Paper based on the IEEE Workshop SDN4FNS*, 2014.
- [4] D. Kim, J. Kim, G. Wang, J.-H. Park, and S.-H. Kim, "K-GENI testbed deployment and federated meta operations experiment over GENI and KREONET," *Comput. Netw.*, vol. 61, pp. 39-50, Mar. 2014.
- [5] H. Lim, K. Lee, and Y. Cha, "Advance reservation framework with protection management for virtual circuit services," *J. KICS*, vol. 38, no. 11, pp. 902-910, Nov. 2013.
- [6] Van-Giang Nguyen and Y.-H. Kim, "SDN-based enterprise and campus networks: A case of VLAN management," *J. Inf. Process. Syst.*, DOI: 10.3745/JIPS.03.0039, 2015.
- [7] Y. Kyung, K. Hong, S. Park, and J. Park, "Load distribution method over multiple controllers in SDN," *J. KICS*, vol. 40, no. 6, pp. 1114-1116, Jun. 2015.
- [8] J. Jo, H. Jang, K. Lee, and J. Kong, "SDN-Based intrusion prevention system for science DMZ," *J. KICS*, vol. 40, no. 6, pp. 1070-1080, Jun. 2015.
- [9] M. Woo, "A study on node selection strategy for the virtual network embedding," *J. KICS*, vol. 39, no. 8, pp. 491-498, Aug. 2014.
- [10] Nuage Networks, *Nuage networks brings data centers and enterprise branch offices closer with SDN-Powered virtualized networks services*, Nuage Networks Press Release, Nov. 2014.
- [11] Gartber, <http://www.gartner.com/technology/home.jsp>
- [12] Broadband Forum, *Technical Working Groups Mission Statements*, Broadband Forum web site, Retrieved Aug., 25, 2016, from <http://www.broadband-forum.org/technical/technicalworkinggroups.php>.
- [13] ETSI, *Network Functions Virtualization*, Retrieved Aug., 25, 2016, from <http://www.etsi.org/technologies-clusters/technologies/nfv>
- [14] L. E. Nelson, "OpenStack Is Ready - Are You?" Forrester web site, May. 2015.
- [15] KREONET web site, Retrieved Aug., 25, 2016, from <http://www.kreonet.net/>
- [16] J. Yoo, W. Kim, and C. Yoon, "A technical trend and prospect of software defined network and openflow," *KNOM Rev.*, vol. 15, no. 2, pp. 1-24, Dec. 2012.
- [17] KREONET-S web site, Retrieved Aug., 25, 2016, from <http://www.kreonet-s.net/>
- [18] Open Network Operating System web site, Retrieved Aug., 25, 2016, from <http://onosproject.org/>
- [19] S. Shin, *Research on clustering of multiple control platform and visualization technique for software convergence network*, KISTI Report, Nov. 2015.

김 용 환 (Yong-hwan Kim)



2008년 8월 : 한국기술교육대학교 정보미디어공학과 석사
2014년 3월~2014년 8월 : 뉴욕주립대(SUNY) 컴퓨터학과 방문 연구원
2010년 8월~2015년 8월 : 한국기술교육대학교 컴퓨터공학과 박사

2016년 6월~현재 : 한국과학기술정보연구원(KISTI) 선임연구원

<관심분야> SDN, Mobility Management, Social Networks, Sensor Networks

김 동 균 (Dongkyun Kim)



1999년 2월 : 충남대학교 컴퓨터과학과 석사
2005년 2월 : 충남대학교 컴퓨터과학과 박사
2006년 4월~2007년 3월 : 미국 테네시대학(UT)/오크리지국립연구소(ORNL) Research Associate III/방문연구원

2000년 6월~현재 : 한국과학기술정보연구원(KISTI) 책임연구원

<관심분야> SDN/NFV, SD-WAN, Research Networking, Network Virtualization