ISBN 978-89-6211-403-4

IPv6 전환망 구축 가이드

IPv6 Deployment Guideline

2009. 9. 25

한국과학기술정보연구원

목 차

1. IPv6 망 구축 개요 ·····5

2. IPv6 전환망 구축 사례 ·····6
2.1 국내 IPv6 네트워크 구축 사례 ·····6
2.2 해외 IPv6 네트워크 구축 사례 ·····15

3. IPv6 전환망 구축 모델 ·····22
3.1 IPv6 네트워크 구성방안 1 ·····22
3.2 IPv6 네트워크 구성방안 2 ·····23
3.3 IPv6 네트워크 구성방안 3 ·····24
3.4 구성 방안 검토 ·····24

4. IPv6 네트워크 고려사항 ·····26
4.1 IPv6 네트워크 구축 고려사항 ·····26
4.2 IPv6 네트워크 구축 Troubleshooting ·····29

5. 결 론 ·····31

참고문헌 ·····32

표 목 차

[표 1] 서버 제품군의 IPv6 지원 버전별 리스트 ··27

그 림 목 차

[그림 1] 한국천문연구원 IPv4/IPv6 네트워크 ·····6
[그림 2] 한국기초과학지원연구원 IPv4/IPv6 네트워크 ·····7
[그림 3] 국가핵융합연구소 IPv4/IPv6 네트워크 ·····8
[그림 4] 한국항공우주연구원 IPv4/IPv6 네트워크 ·····8
[그림 5] 한국표준과학연구원 IPv4/IPv6 네트워크 ·····9
[그림 6] 한국지질자원연구원 IPv4/IPv6 네트워크 ·····10
[그림 7] 한국생명공학연구원 IPv4/IPv6 네트워크 ·····10
[그림 8] 충남대학교 IPv4/IPv6 네트워크 ·····11
[그림 9] 강릉시청 IPv4/IPv6 네트워크 ·····12
[그림 10] 공주시청 IPv4/IPv6 네트워크 ·····13
[그림 11] 한국인터넷진흥원 IPv4/IPv6 네트워크 ·····14
[그림 12] 한국과학기술정보연구원 IPv4/IPv6 네트워크 ·····14
[그림 13] Internet2 IPv4/IPv6 네트워크 ·····15
[그림 14] JGN2plus IPv4/IPv6 네트워크 ·····16
[그림 15] CERNET2 IPv6 네트워크 ·····16
[그림 16] TWAREN IPv6 네트워크 ·····17
[그림 17] University of Southampton IPv4/IPv6 네트워크 ·····18
[그림 18] GEANT2 백본 네트워크 ·····20
[그림 19] KanREN IPv6 네트워크 ·····21
[그림 20] IPv4 네트워크 구성도 ·····22
[그림 21] IPv6 네트워크 구성방안 1 ·····23
[그림 22] IPv4 네트워크 구성도 ·····23
[그림 23] IPv6 네트워크 구성방안 2 ·····24
[그림 24] IPv6 네트워크 구성방안 3 ·····24
[그림 25] 네트워크 장비의 IPv6 활용 여부 판단 ·····26

1. IPv6 망 구축 개요

인터넷의 폭발적인 성장으로 인하여 IPv4 주소자원이 2011년경이면 고갈될 것이라 예상하고 있으며[1] 따라서, IPv4를 대체하는 IPv6 주소로의 전환이 필요하다. 뿐만 아니라 인터넷 서비스의 중심이 음성에서 데이터로 전환됨에 따라 통신사업자들은 기존의 네트워크를 새로운 수익 창출과 비용절감을 위하여 All-IP 네트워크로 통합시켜가는 추세이기에 시장에서 필요로 하는 주소자원을 원활하게 공급하고, 방송·통신 융합형 유비쿼터스 서비스를 제공하기 위하여 IPv6 기반의 인프라 환경 제공이 필수적이다.

이에 정부에서는 "IPv6 보급 촉진 기본계획 II(2006. 12)"를 발표하여 2010년까지 정부 및 공공기관의 IPv6 도입을 완료하고 IPv6 도입 활성화를 지원하기 위한 각종 제도개선 등의 새로운 계획을 마련하였다.[2]

실제 공공분야의 IPv6의 선도적인 도입 및 전환, 확산을 위하여 한국인터넷진흥원(KISA)과 한국과학기술정보연구원(KISTI)을 중심으로 IPv6 전환확산사업을 진행하고 있다.

특히 대덕연구개발특구(이하 대덕특구)는 정부출연 연구기관 및 교육기관 등이 밀집되어 있으며, 국내의 대표적인 IT 인프라를 보유하고 있고, 발생하는 실사용자 트래픽이 대규모인 특화된 지역으로 상용서비스 수준의 IPv6 클러스터 구축, 적용 및 확산이 용이하며, 실제 IPv6 전환으로 체계적이고 검증된 성과모델을 창출할 수 있다.

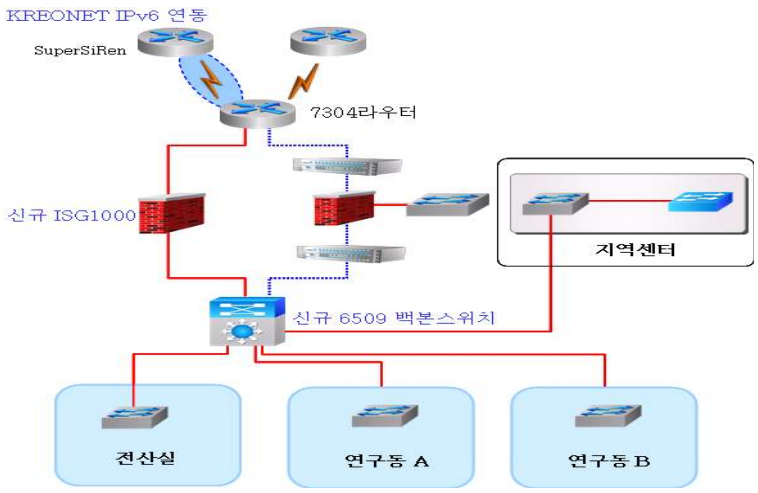
이에 본 문서에서는 대덕특구를 중심으로 한 IPv6 네트워크로의 전환 구축을 위하여 국내·외 IPv6 구축 사례에 대하여 살펴보고 IPv6 네트워크 구축 모델과 IPv6 망 구축 전환을 위해서 고려해야 할 사항들에 대하여 기술하고자 한다.

2. IPv6 전환망 구축 사례

2.1 국내 IPv6 네트워크 구축 사례

가. 한국천문연구원

한국천문연구원은 천문우주를 연구하고 관련된 연구 장비와 시설을 개발하는 전문연구기관이다. 이런 천문연의 IPv4/IPv6망으로의 전환을 위해 외부망 인입 라우터의 IPv6 설정을 통해 외부 IPv6망과의 연동 기반을 마련하였고, 연구원 내 백본 장비를 IPv6 지원가능한 장비로 교체함으로써 일부 영역이나 제한된 구역이 아닌 모든 호스트 장비에 대한 IPv6 설정 및 활용이 가능하게 구축하였다. 또한, IPv6 전용 방화벽을 구축하여 IPv6 서비스 외부 제공서비스의 보안성을 강화하였다.



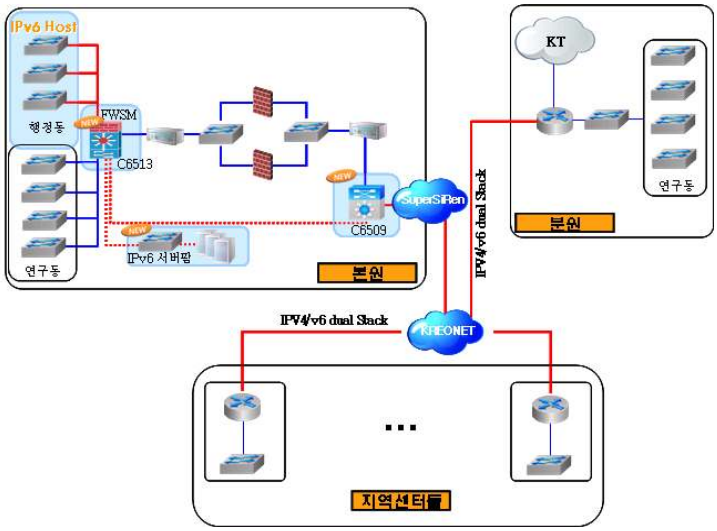
[그림 2] 한국천문연구원 IPv4/IPv6 네트워크

IPv6 외부망과의 접속을 위하여 외부망 Catalyst 7304 라우터는 OS 업그레이드를 통해 IPv6를 설정하여 외부 IPv6망과의 연동 기반 마련하였으며, 원내 기존 백본스위치를 Cisco Catalyst 6509로 교체함으로써 원내 망의 일부 영역이나 제한된 구역이 아닌 모든 호스트 장비에 대한 IPv6 설정 및 활용이 가능하게 하도록 하였다. 또한, IPv6 네트워크 보안을 위하여 Juniper ISG-1000 설치 및 운영하고 있다. 또한, Windows Server 2003으로 IPv6 전용 DNS를 구축하였다. [2][3]

나. 한국기초과학지원연구원

한국기초과학지원연구원은 IPv4/IPv6 듀얼스택 망을 지원하기 위하여 한국기초과

학지원연구원 대덕본원의 주요 네트워크 장비를 IPv6 지원가능 장비로 교체하였으며, 지역센터의 네트워크를 IPv6가 지원되도록 변경하였다. 대덕 본원 및 지역센터들을 연계하는 IPv6망을 구축하였다.

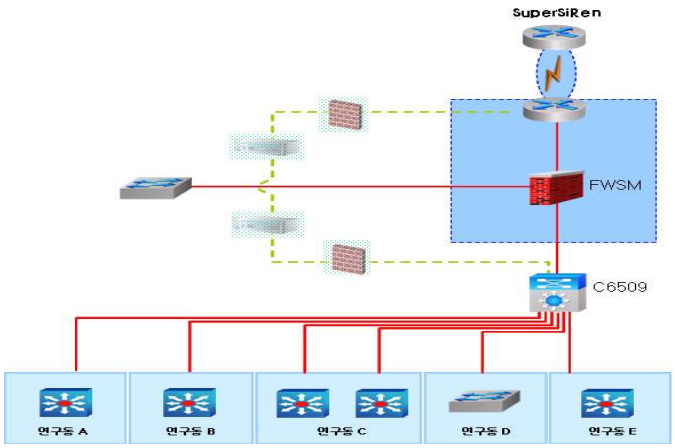


[그림 3] 한국기초과학지원연구원 IPv4/IPv6 네트워크

기존 운영중인 백본스위치(Cisco Catalyst 6509)에 IPv6 스택을 올려 IPv6를 지원하게 하였고, 기존 Cisco Catalyst 6509에 모듈형 IPv6 방화벽인 FWSM를 탑재하여 보안을 강화하였다. 또한, 대전 본원을 비롯한 지역센터간의 IPv6 지원을 가능하게 구성하여 전국적인 규모의 IPv6 네트워크 구축하였고, IPv6 주소 할당은 지역센터별로 /64단위로 분할하여 할당하였다. 아울러 본원 및 지역센터간에는 IPSec VPN를 통한 암호화 통신체계를 구축 운영하고 있다. [2][3]

다. 국가핵융합연구소

급속히 성장하고 있는 핵융합분야의 인프라의 확충에 따라 분석데이터와 각종 연구결과물의 저장 및 처리와 국내/외 원격공동연구를 위한 인프라로 활용하기 위하여 IPv6 전환망을 구축하고자 하는 국가핵융합연구소는 IPv4/IPv6 전환망을 구축하였으며, KSTAR 운전상황 모니터링 서비스를 IPv6용으로 구축하였으며, IPv6 DNS를 구축하였다.

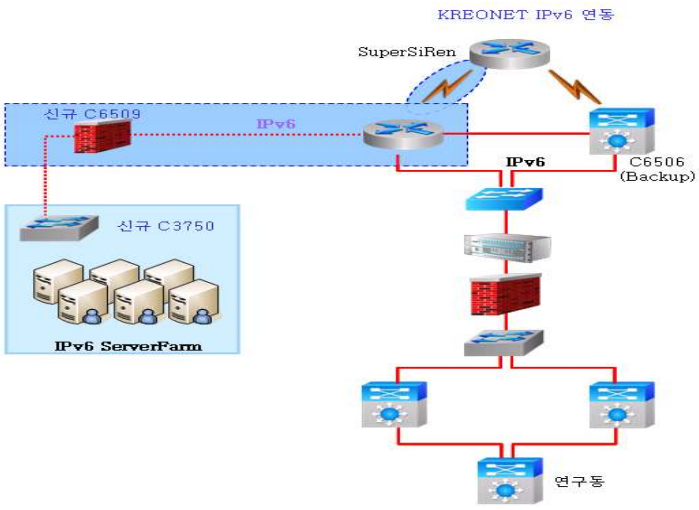


[그림 4] 국가핵융합연구소 IPv4/IPv6 네트워크

IPv6 전환 계획은 연구소내 일부구간에만 IPv6를 적용하려 하였으나 적용 범위를 확대하여 현재 연구소 전체에 IPv6망을 사용할 수 있는 환경으로 구축하였다. Cisco Catalyst 6509 라우터와 모듈형 방화벽인 FWSM를 이용하여 IPv6 전환망을 구축하였다. [2][3]

라. 한국항공우주연구원

우리나라 항공우주 분야의 연구개발을 주도하는 항공우주연구원은 신기술인 IPv6 기술의 선도적 도입으로 대덕특구내의 타 연구기관으로의 IPv6 기술확산의 기반과 향후 항공우주분야에 활용하고자 IPv6 전환망을 구축하였다. 이를 위하여 IPv4/IPv6 듀얼스택 전환망을 구축하였으며, IPv6용 항공우주연구원 홈페이지를 구축하였다.

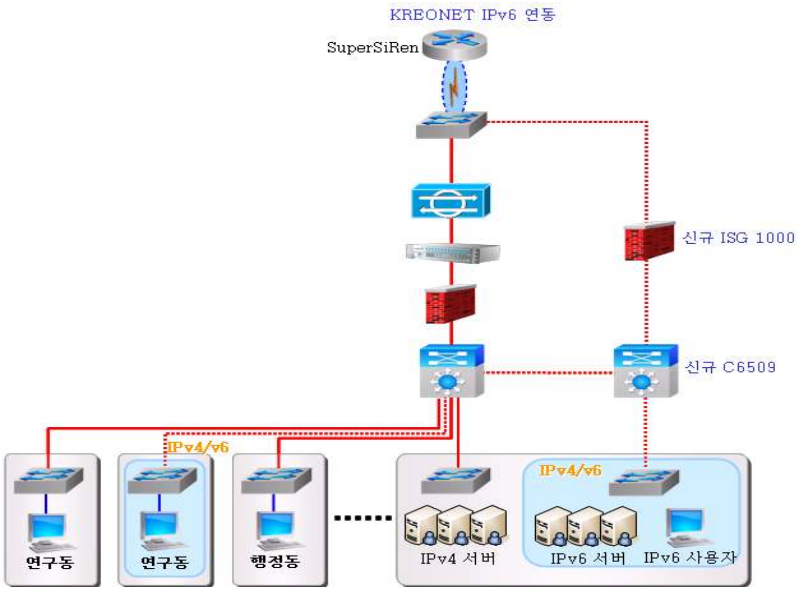


[그림 5] 한국항공우주연구원 IPv4/IPv6 네트워크

내부망은 Cisco Catalyst 6509 및 모듈형 방화벽인 FWSM를 이용하여 IPv6망을 구축하였다. 중국으로부터 해킹을 방지하고자 발신지가 중국으로 되어있는 IP를 차단하였다. [2][3]

마. 한국표준과학연구원

국가측정표준 확립 및 유지, 국가측정표준 보급, 표준과학기술 연구개발, 측정표준 국제보증 등의 국가로부터 부여받은 임무와 시대의 변천 과학기술의 발전에 따라 새롭게 요구되는 임무들을 IPv6망을 활용하여 보급하고자 선도적으로 IPv6 도입을 추진하였다. 표준과학연구원내 연구동 및 전산센터내 IPv4/IPv6 듀얼스택 망을 구축하였다.

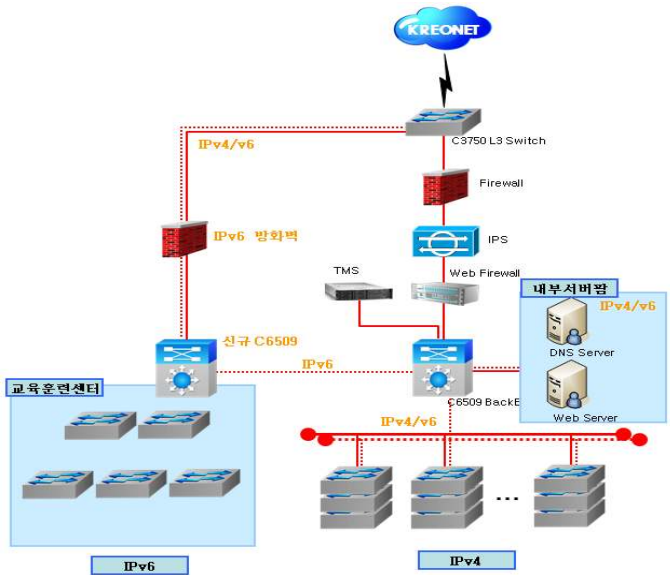


[그림 6] 한국표준과학연구원 IPv4/IPv6 네트워크

표준연구원 Cisco Catalyst 3750 L3 Switch에 IPv4/IPv6 듀얼스택을 올린 후 KREONET과 연동하고, 신규 Cisco Catalyst 6509 백본 스위치를 IPv6로 연결을 구성하였다. 신규 Cisco Catalyst 6509 백본 스위치에서 라우팅을 하고 각 서버 및 네트워크 장비를 연결할 수 있도록 구성하였다. 네트워크의 보안을 위하여 Juniper ISG-1000를 연동하였다. [2][3]

바. 한국지질자원연구원

Cisco Catalyst 3750 스위치 하단으로 IPv4 방화벽, 침입방지시스템, TMS, ESM 등의 보안시스템들이 연동되어 있고 Catalyst 6509 백본 스위치가 운영되어 각 연구동별로 Giga급으로 연동되어 있다.

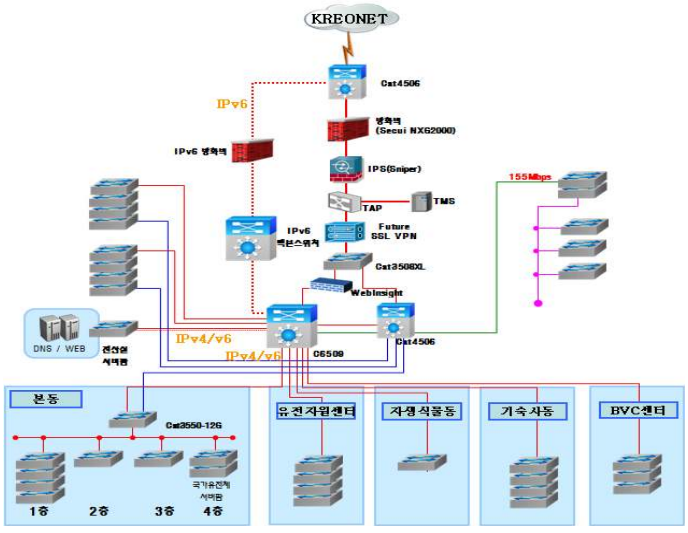


[그림 7] 한국지질자원연구원 IPv4/IPv6 네트워크

IPv6 네트워크는 Catalyst 3750 L3 스위치를 통해서 IPv6 방화벽과 IPv6 스위치를 연동하여 교육훈련센터로 연동되어 있다. 신규 구축된 IPv6 방화벽과 IPv6 Catalyst 6509 장비는 IPv4와 IPv6가 듀얼로 동작하도록 구성하였다. 따라서, 교육훈련센터의 IPv4 네트워크는 기존 백본 Catalyst 6509로 연동되지 않고, 신규 IPv4/IPv6 네트워크를 통한 후 Catalyst 3750 스위치를 통한 후 외부 네트워크로 연동되어 있다.

사. 한국생명공학연구원

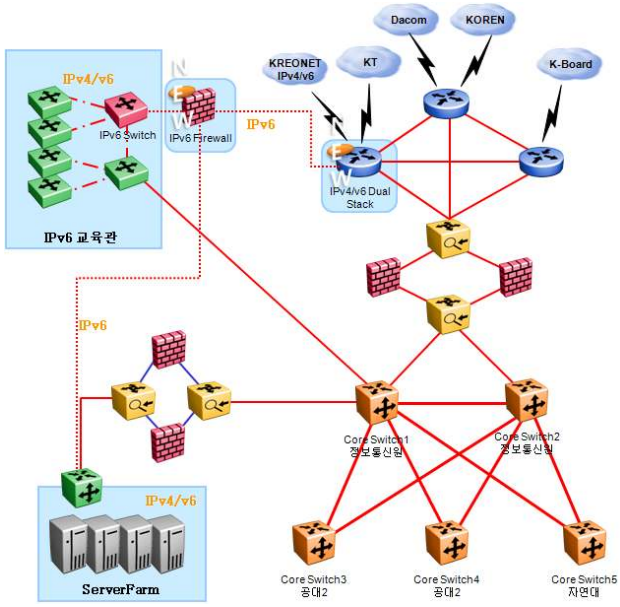
Cisco Catalyst 4506 라우터 하단에 방화벽, IPS, VPN, 웹방화벽, 바이러스 월을 연동하여 운영되고 있다.



[그림 8] 한국생명공학연구원 IPv4/IPv6 네트워크

또한 Catalyst 4506 백본 스위치 Catalyst 6509와 Catalyst 4506는 내부 스위치간과 HSRP를 사용하여 이중화 구성되어 있다. 기존 IPv4 네트워크의 변경없이 Catalyst 4506 스위치와 신규 Catalyst 6509, 방화벽을 연동하여 IPv6 네트워크를 구성하였다.

아. 충남대학교



[그림 9] 충남대학교 IPv4/IPv6 네트워크

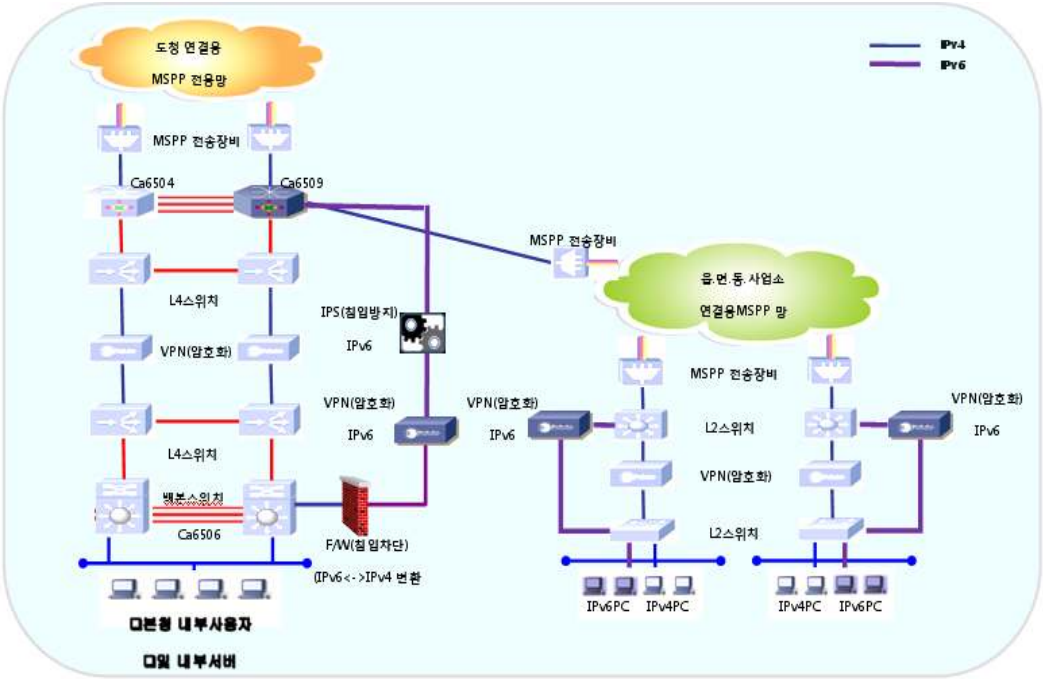
ERS8600 라우터 2대와 하나로 라우터를 통하여 외부와 연동되고 있으며, IPv6 네트워크는 교육관과 서버팜은 내부 코어스위치내에 연동되어 있다. 현재 IPv4 학내전산망과 분리하여 IPv6망을 구성하였다.

자. 강릉시청

차세대 인터넷 주소(IPv6) 확보가 유비쿼터스 전략의 새로운 화두로 떠오르면서 강릉시는 차세대인터넷 주소관리체계의 시급성을 인식하고, 새로운 IPv6 기반 u-city 특화형 도시전략구축을 위해 2005년부터 2007년까지 IPv6 시범사업에 참여하였다. 그리하여 전국 지자체 최초 3년 연속 IPv6 인프라를 구축하고 IPv6 시범 특화도시 이미지를 쌓아왔다.

2008년 강릉시청은 강릉시 내·외부망 및 행정망 내 IPv6 지원 장비 도입 및 보건소·문화교육센터·주민센터(13개동) 등 15개소에 IPv6 인프라 구축, 강릉시 홈페이

지에 IPv6 적용, IPv6 무선 Mesh망 이용 인터넷 무료서비스 존(경포해수욕장· u-문화스포츠타운) 이용 확산유도 등을 목표로 '공공기관 IPv6 장비 지원 사업'에 참여하였다.

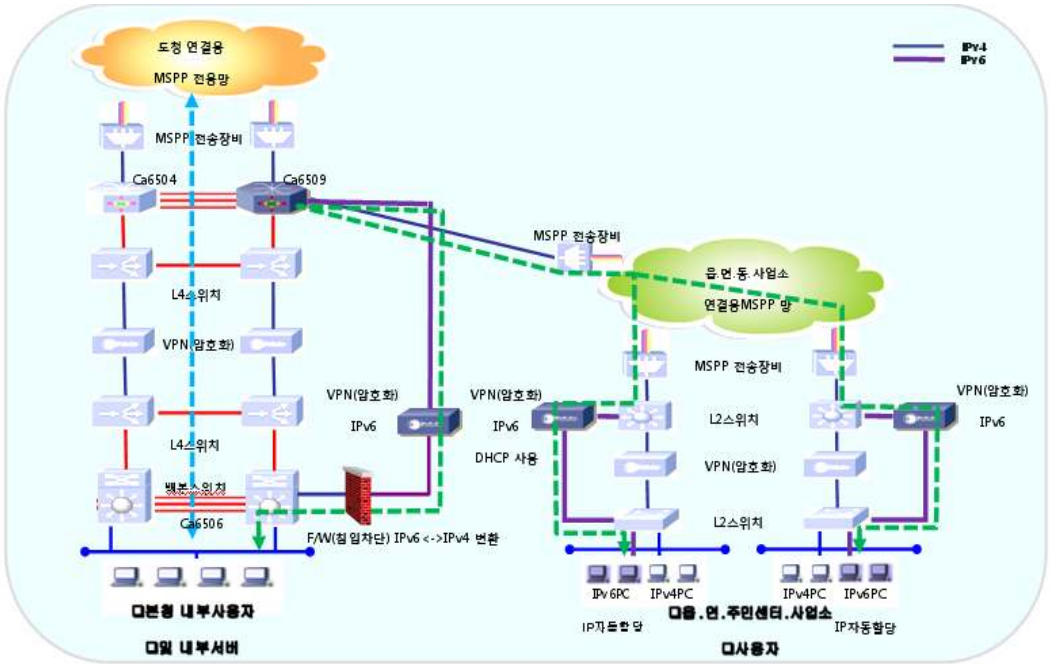


[그림 10] 강릉시청 IPv4/IPv6 네트워크

강릉시청은 내·외부망에 IPv6를 도입하기 위해 인터넷 연동 라우터를 신규 도입하고 시청과 동사무소 사이에 IPv6로 VPN 통신을 하도록 구축하였다. IPv6 IPS 장비를 구축하였고 향후의 IPv6 트래픽의 증가에 대비하여 IPS 패턴의 업데이트가 가능하도록 구성하였다. 또한 시청 내부에 IPv6↔IPv4로 변환하는 NAT-TP 기능을 Future Systems사의 WeGuardia XTM를 사용하여 구축하였으며, 무엇보다도 KT 측에 IPv6 인터넷 접속을 요구하여 상용망인 KT Pubnet에 IPv6를 적용하였다. [2]

차. 공주시청

공주시청은 내부 업무 처리를 위한 행정망과 외부 인터넷 연동망에 IPv6를 도입하였다. 공주시청은 행정망에 IPv6를 도입하기 위해 IPv6 암호화 장비 및 침입방지 시스템을 신규 도입하여 본청과 읍·면 주민센터 등 26개소에 설치하고 라우터와 스위치를 IPv4/IPv6 듀얼모드로 구성하였다.

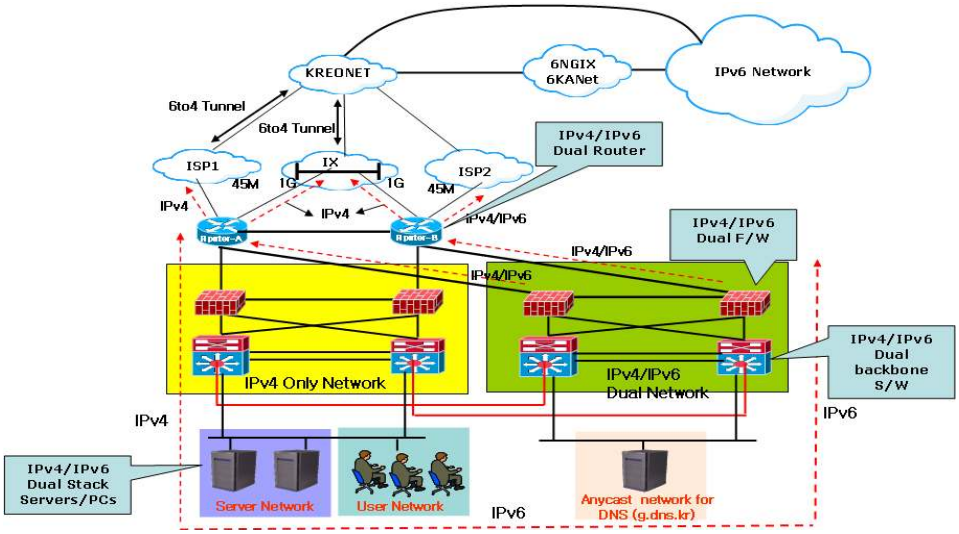


[그림 11] 공주시청 IPv4/IPv6 네트워크

공주시청은 시청과 읍·면 주민센터 등의 IPv6 단말에서 본청 서버로 접근시 해당 사업소에 있는 Future Systems사의 WeGuardia XTM 장비[10]를 사용하여 VPN으로 암호화를 수행하고 본청의 IPv6 암호화 장비에서 복호화를 수행한 후 백본스위치에서 IPv4로 변환하여 본청 서버로 전달한다. 또한, 읍·면 주민센터 등에서 타 시군구의 정보를 조회할 때는 본청 시군구서버로 요청을 하고 본청 시군구서버는 타시군구 서버의 정보를 검색하여 읍·면 주민센터 등에 정보를 전달하는 방식을 취하였다. [2]

카. 한국인터넷진흥원

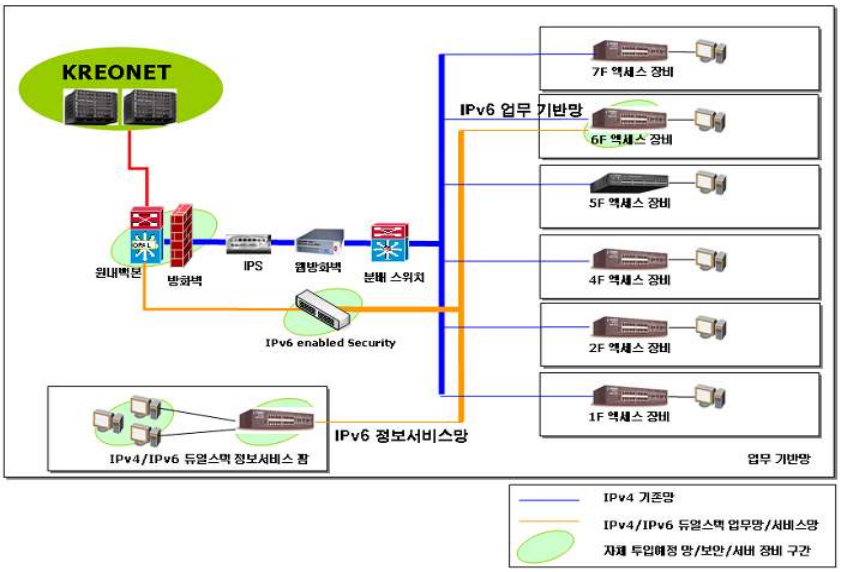
한국인터넷진흥원은 공공부문 IPv6 전환·확산 사업의 전담기관으로써 내부 네트워크 및 홈페이지에 자발적으로 IPv6를 적용함으로써 공공부문 IPv6 전환을 선도하였다. 2008년 2월에 사용자 및 서버 네트워크의 IPv6 적용을 완료하였고, 3월에 기관 대표 홈페이지 웹서버의 IPv6 전환, IPv6 DNS 구축, .KR 네임서버에 IPv6 주소 할당 및 적용을 완료하였다. 현재 IPv4/IPv6 듀얼스택으로 운영되고 있으며, 네트워크 보안을 위하여 NOKIA IP530 방화벽을 사용하고 있다. [2][16][17]



[그림 12] 한국인터넷진흥원 IPv4/IPv6 네트워크

타. 한국과학기술정보연구원

한국과학기술연구원은 과학기술정보분야의 데이터베이스 및 콘텐츠 제공은 물론, 슈퍼컴퓨팅 자원, 네트워크 자원 등의 정보자원 인프라를 보유하고, 서비스를 제공하는 기관이며, 과학기술분야의 정보제공 인프라의 선도 기관으로서, 전국 백본 및 국제 게이트웨이에 IPv6 전용 네트워크를 구축하였으며, 연구원 내의 내부망도 IPv4/IPv6 듀얼스택으로 구축하였다.



[그림 13] 한국과학기술정보연구원 IPv4/IPv6 네트워크

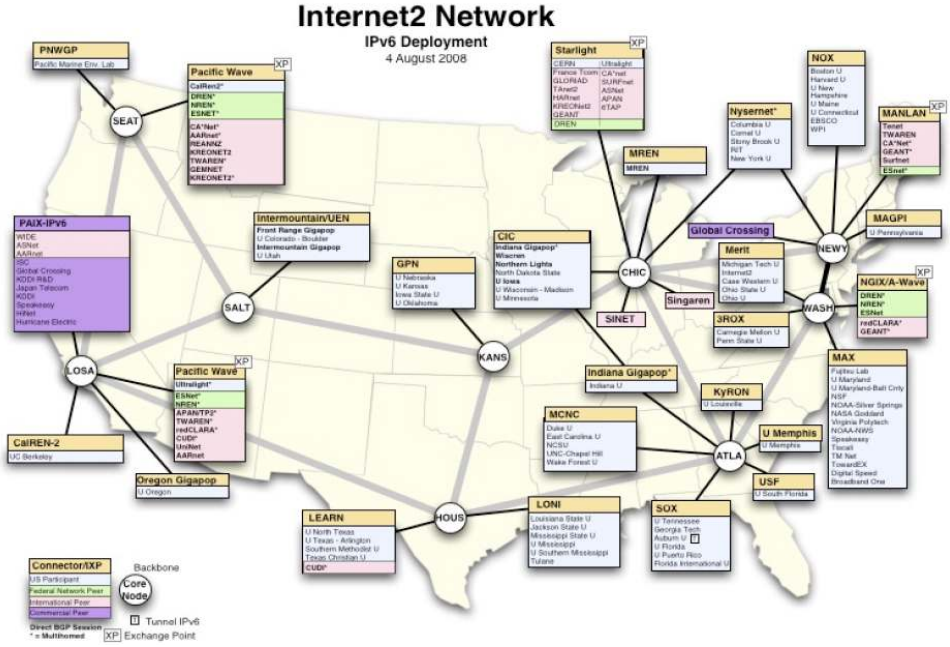
한국과학기술정보연구원은 Cisco Catalyst 6509 라우터 및 모듈형 방화벽인 FWSM

을 이용하여 원내 백본 네트워크를 IPv4/IPv6 듀얼스택으로 전환하고, IPv6 백본 스위치를 구성하여, IPv6 정보서비스망을 구축하고, 연구원 업무망의 일부를 IPv4/IPv6 듀얼스택이 가능한 구성으로 전환하였다. [1][2][18]

2.2 해외 IPv6 네트워크 구축 사례

가. Internet2 (미국)

Internet2(www.internet2.edu)는 미국 내 140 여개의 대학들이 업계 및 정부기관과의 협력 하에 진보된 연구, 교육을 지원하는 차세대 인터넷 기술과 응용을 개발하기 위한 대학연합 주도의 공동연구 사업이다.



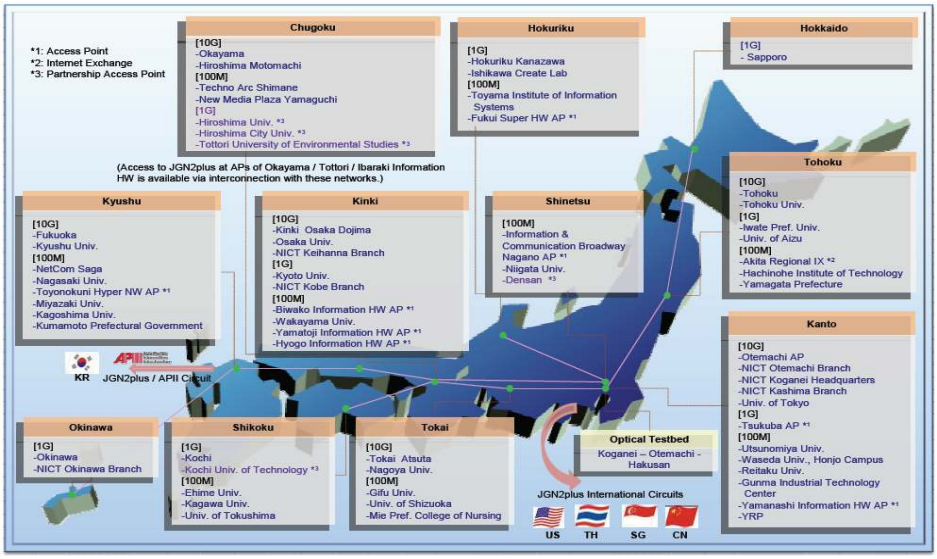
[그림 14] Internet2 IPv4/IPv6 네트워크

Internet2는 지속적으로 IPv6망을 확대 구축하고 있으며, Juniper T640 라우터를 이용하여 IPv4/IPv6 듀얼스택망을 구축하고 있다. 또한 LA의 PAIX 라우터를 통해 상용망과 상호 연동하고 있다. 향후에 상용망과의 연동은 시카고, 뉴욕, 시애틀로 확대할 예정이다. 아울러, Juniper 라우터에 설치된 방화벽 필터링을 통하여 IPv6 트래픽을 모니터링 하고 있다. [11]

- http://vixen.grnoc.iu.edu/jfirewall-viz/index-bits.html
- http://vixen.grnoc.iu.edu/jfirewall-viz/

나. JGN2plus (일본)

일본은 IPv6를 포함한 차세대 네트워크 환경을 구축하기 위하여 2000년부터 2004년까지 ATM 기반의 JGN1을 구축·운영하였으며, 이후 2004년부터 2008년까지 이더넷기반의 JGN2로 업그레이드하였다. 최근에는 2008년부터 2011년까지 운영할 JGN2plus로 업그레이드하였다. JGN2plus는 IPv4/IPv6 듀얼스택, IPv6-native 서비스를 제공할 뿐만 아니라, Layer 2 이더넷 서비스(1Gbps ~ 10Gbps)제공하며, 미국, 태국, 싱가폴, 중국, 한국과 국제적으로 연동하고 있다. [12]



[그림 15] JGN2plus IPv4/IPv6 네트워크

다. CERNET2 (중국)

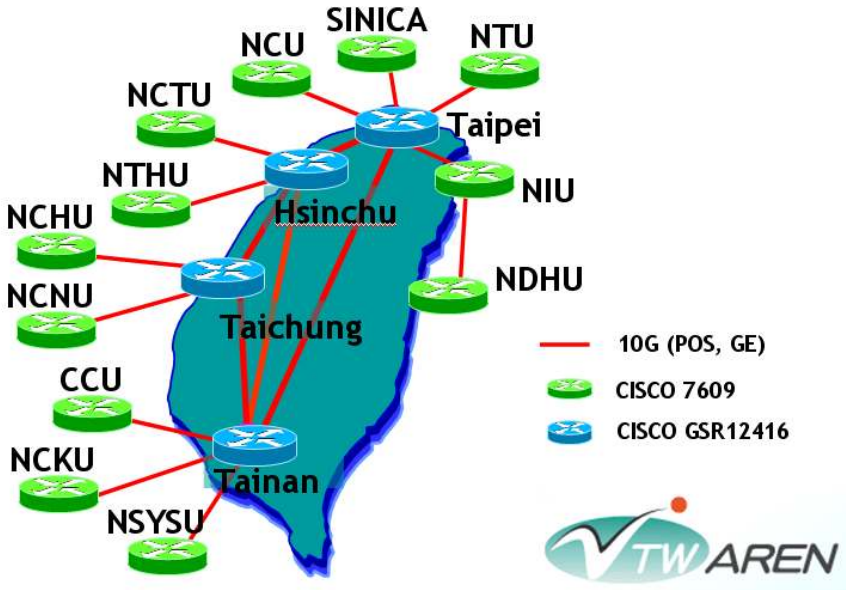
2003년에 중국 정부는 '973 프로젝트' 내에 '미래 인터넷 아키텍처 연구'의 프로젝트로 CERNET을 CERNET2로 명명하여 추진하였다. CERNET2는 순수한 native-IPv6 트래픽을 지원하도록 하고 있다.

[그림 16] CERNET2 IPv6 네트워크

CERNET2는 CNGI(China Next Generation Internet)의 백본 네트워크로서, 중국의 차세대 인터넷망이다. 중국 20개 도시에 20개의 기가팝을 운영하고 있으며 100개 이상의 대학교와 연구소들이 1Gbps ~ 10Gbps의 속도로 연동되어 있으며 국제적으로는 북미, 유럽, 아시아 지역과 2.5Gbps로 연동되어 있다. 특히 청화대학에서 자체 연구개발한 라우터 장비들을 활용하여 구축하는 등 자국 라우터설비의 사용률이 80%에 이르고 있다. [13]

라. TWAREN (대만)

대만은 e-Taiwan 프로젝트를 통해 IPv6 개발 및 전환을 도모하고 있으며 7개 주요 ISP업체들이 IPv6 주소를 할당받아 운용하고 있고 그중에 1개 업체(HiNet)은 IPv6 기반의 상용서비스를 제공하고 있다. 또한 IPv6 교육용 네트워크인 TANet(Taiwan Academic Network)를 구축하여 학교와 연구기관들에게 IPv6 서비스 제공하고 있다. 아울러 20G급의 광 네트워크를 기반으로 한 TWAREN을 구축하여 IPv6 관련 연구개발을 진행하고 있다. TWAREN을 구축하기 위해 Cisco Catalyst 7609 라우터와 GSR 12416 장비를 사용하였다. [14]

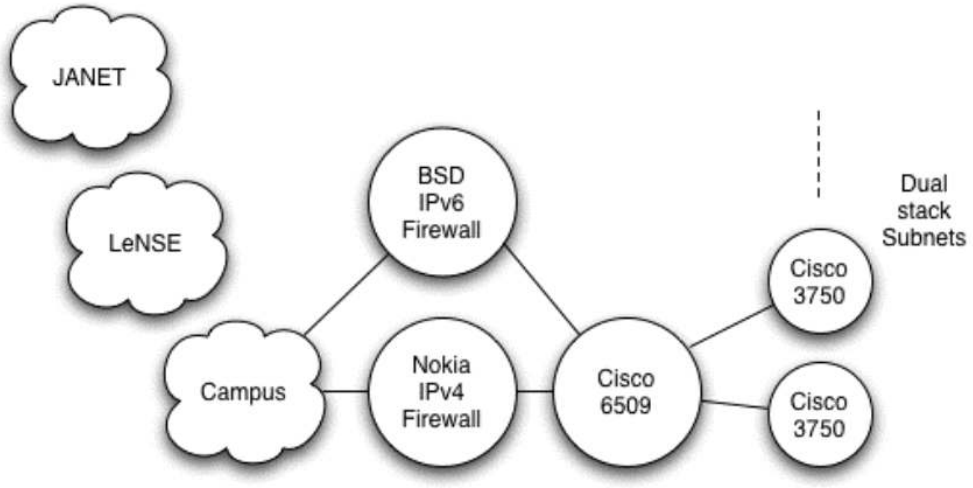


[그림 17] TWAREN IPv6 네트워크

마. University of Southampton (영국)

총 4200명의 사용자와 1900개의 IPv4 주소를 사용하고 있는 Southampton 대학교는 기존의 IPv4망에 IPv6를 올려 IPv4/IPv6 듀얼스택 네트워크를 구축하였다. 총 50대의 Cisco Catalyst 3750 스위치/라우터를 사용하였으며, 외부용 라우터 장비로

Catalyst 6509를 이용하여 구축하였다. 기존의 IPv4망에서는 Checkpoint사의 방화벽을 사용하였으나, 구축당시 본 장비는 IPv6를 지원하기 않는 관계로 IPv6용 방화벽으로 BSD IPv6 방화벽을 사용하였다. 또한, Snort v2.8.0를 이용하여 IDS를 구축하였으나, 현재 특정한 룰이 적용되어 있지는 않은 상태이다. 아울러, DNS, www, login 등과 같은 핵심 서비스들에 듀얼스택을 올려 서비스 제공하고 있다.



[그림 18] University of Southampton IPv4/IPv6 네트워크

바. GEANT (유럽)

GEANT은 유럽 30개국의 26개 주요 국가 연구교육망(NREN)을 상호 연동하여 멀티 기가비트 범유럽 데이터 통신 네트워크를 구축하는 프로젝트이다. 2004년 9월부터는 GEANT2로 발전하여 현재 34개국 국가 연구교육망들이 연동되어 있다. GEANT은 Juniper Networks사의 M160과 M40 라우터와 Cisco Systems사의 Catalyst 7500 장비로 IPv4/IPv6 듀얼스택망을 구축하고 운영하고 있다.

NREN으로서는 2003년 1월에 RedIRIS(스페인), RENATER(프랑스)가 처음으로 GEANT IPv6에 연동하였고, 2003년 9월까지 대부분의 NREN들이 GEANT IPv6에 연동하였다. 이후 2004년 8월에는 4개의 추가적인 NREN과 CANARIE 및 SINET이 연동되었다. 현재 대부분의 NREN이 IPv6-tunneling보다는 IPv6-native 방식으로 연동되어 있다. 주요 NREN의 IPv6 연동방식은 다음과 같다. [15]

○ European NRENs

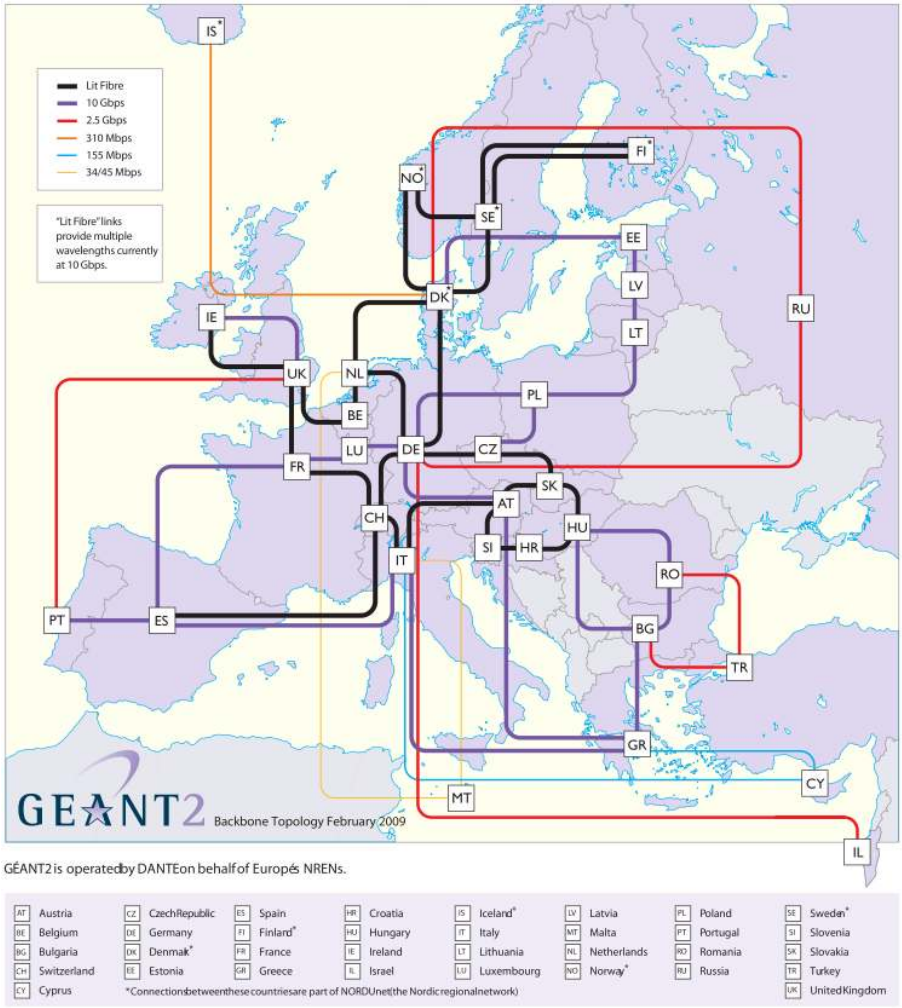
Peer	Connection Type	Connection Date
ACONET	Tunnel	13/05/2003
ARNES	Native	22/07/2003
BELNET	Native	29/07/2003
CARNET	Native	10/03/2004
CERN	Native (since 02/09/2004)	09/05/2003
CESNET	Native	30/07/2003
CYNET	Native	10/12/2004
DFN	Tunnel	16/09/2003
EEnet	Native	09/05/2003
FCCN	Native	22/04/2003
GARR	Native	29/04/2003
GRnet	Native	31/07/2003
HEAnet	Native	23/04/2003
HUNGARNET	Native (since 19/04/2004)	10/06/2003
IUCC	Native (since 05/01/2004)	29/04/2003
ISTF	Native	17/03/2005
JANET	Native	10/06/2003
SigmaNet	n/a	n/a
LITNET	Tunnel	06/05/2003
University of Malta	Native (since 26/1/2006)	29/03/2005
NORDUnet	Native	25/08/2003
PSNC	Native	06/05/2003
RBnet	Native	17/09/2003
RedIRIS	Native	10/04/2003
RENATER	Native	15/04/2003
RESTENA	Native	18/06/2003
RoEduNet	Native	09/05/2003
SANET	Native	18/10/2004
SURFnet	Native	22/04/2003
SWITCH	Native (since 09/03/2004)	09/05/2003
Ulakbim	Native	30/05/2003

○ International Peerings

Peer	Connection Type	Connection Date
Abilene	Native (DE-Washg.)	05/05/2003
	Native (NY)	10/06/2003
	Native (NL)	07/10/2003
CANARIE	Native	09/07/2003
ESnet	Native	27/05/2003
SINET	Tunnel to NY (since 20/05/04)	03/06/2003

○ Commerical Peerings

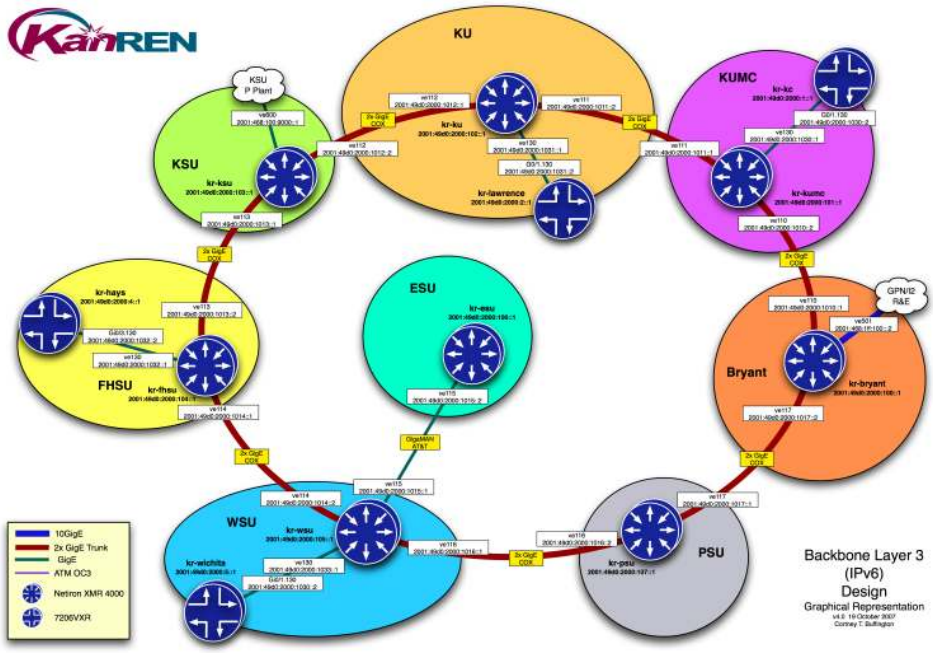
Peer	Connection Type	Connection Date
GlobalCrossing	Tunnel (Frankfurt)	25/07/2003
Telia	Tunnel	12/05/2003



[그림 19] GEANT2 백본 네트워크

사. KanREN (미국)

KanREN은 미국 캔사스주의 대학교 및 비영리 연구기관을 연결하는 연구교육망으로써 Internet2의 연구교육망의 멤버로써 활동하고 있으며, IPv6 구축에 있어서 선도적인 역할을 하고 있는 연구망이다. 특히 KanREN의 Barton County Community College는 IPv6망 전환 및 보안 정책을 구축하였고, Ft. Scott Community College는 본교 캠퍼스 및 6개 분교 캠퍼스에 IPv4/IPv6 듀얼스택을 지원하는 망을 구축하였다. Fort Hays State University는 DNS, email, Web 서비스를 학내 핵심 네트워크 및 외부 네트워크에 구축을 마쳤으며, Pittsburg State University와 Emporia State University는 두 학교간 IPv4/IPv6 듀얼스택을 지원하는 노력을 진행중에 있다. [19]



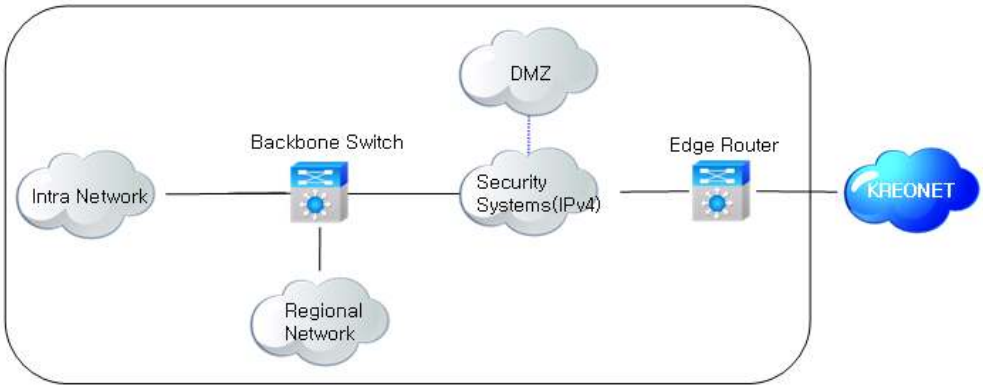
[그림 20] KanREN IPv6 네트워크

3. IPv6 전환망 구축 모델

IPv6 테스트베드의 목적이 아닌 운영 중인 기관의 네트워크에 실제 운영 가능한 IPv6 네트워크를 구성하는 것이며, 이를 위하여 현재 IPv4 네트워크 구성에 적합한 IPv6 네트워크의 전환 방안에 대하여 살펴보고자 한다.

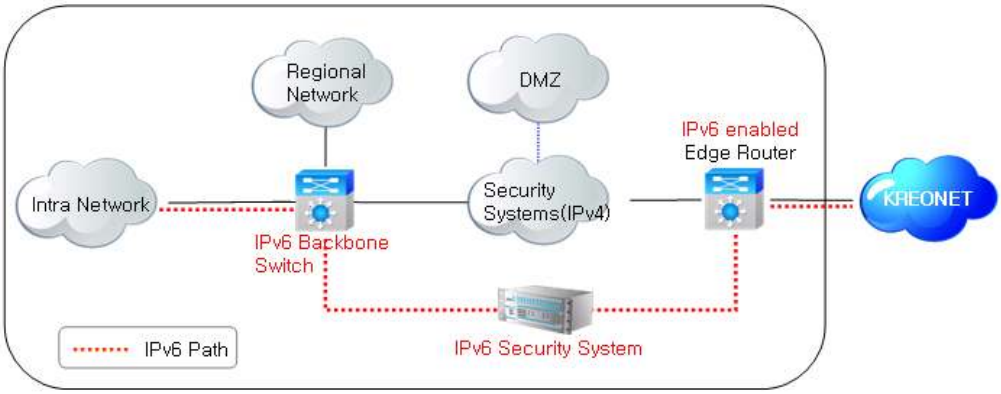
3.1 IPv6 네트워크 구성방안 1

기존의 운용중인 IPv4 네트워크 구성은 KREONET과 에지라우터가 연동되어 있으며, 백본스위치에서 내부망과 연동되어 있다. 에지라우터에서 백본스위치 사이에는 보안시스템들이 연동되어 있으며, 방화벽은 이중화되어 구성되어 있다.



[그림 21] IPv4 네트워크 구성도

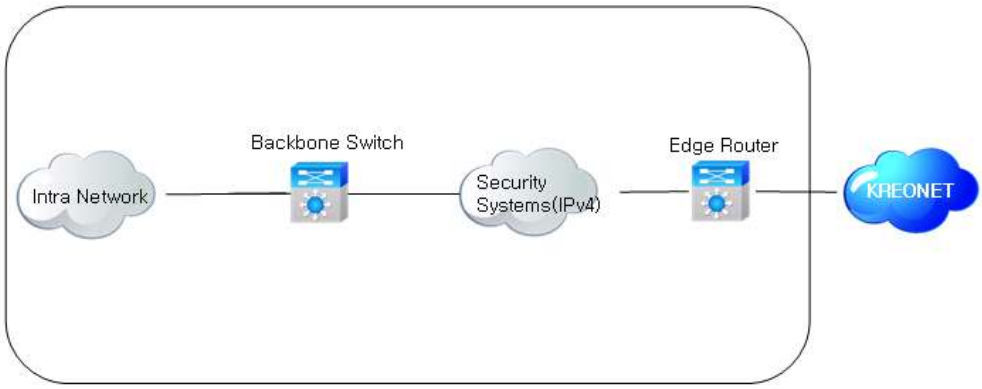
• IPv6 네트워크 구성 방안 1 : 기존의 에지라우터에 IPv6 스택을 올리고 IPv6 보안시스템을 설치한다. 기존의 노후화된 백본스위치는 IPv6가 지원되는 스위치로 교체하며, 아울러 지역 센터의 라우터가 IPv6를 지원하므로 본원과 지역 센터간에 IPv4/IPv6 듀얼모드로 연동한다. 내부망에서의 IPv4 통신은 백본스위치 ↔ 보안시스템 ↔ 에지라우터를 통해 이루어지고, IPv6 통신은 백본스위치 ↔ IPv6 보안시스템 ↔ 에지라우터를 통해 이루어지도록 구성한다.



[그림 22] IPv6 네트워크 구성방안 1

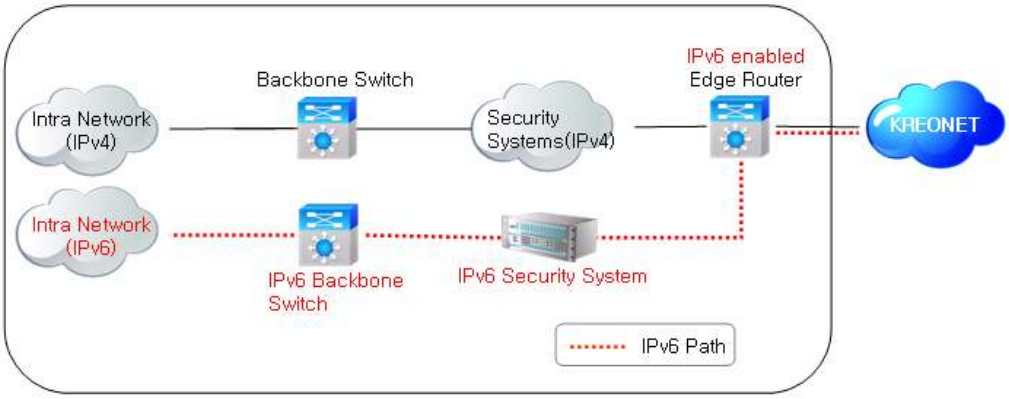
3.2 IPv6 네트워크 구성방안 2

IPv4 네트워크 구성도는 KREONET과 에지라우터가 연동되어 있으며, 에지라우터와 백본스위치 사이에는 보안시스템이, 그리고 백본스위치는 내부망과 연동되어 있다.



[그림 23] IPv4 네트워크 구성도

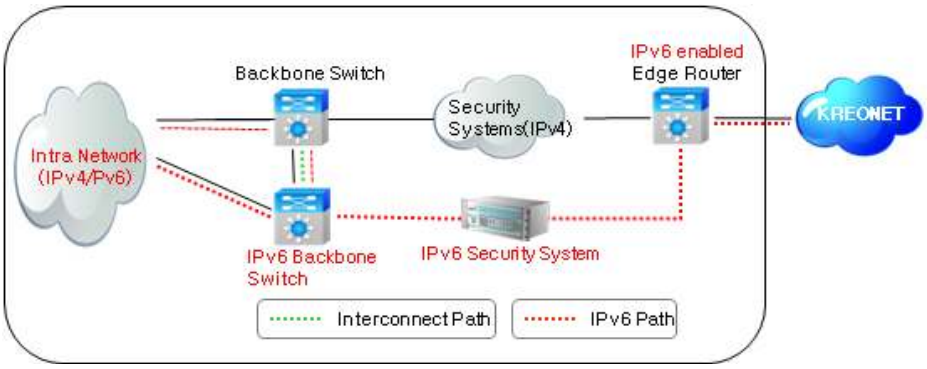
• IPv6 네트워크 구성 방안 2 : IPv6를 지원하는 에지라우터(IPv6 enabled)에 별도의 IPv6 라우터 및 보안시스템을 연동하고 내부망의 일부를 IPv6망으로 구성한다. IPv4 통신은 IPv4 백본스위치 ↔ 방화벽 및 보안시스템 ↔ 에지라우터(IPv6 스택 올림)를 통해 이루어지며, IPv6 통신은 IPv6 백본스위치 ↔ IPv6 보안시스템 ↔ 에지라우터(IPv6 enabled)를 통해 이루어진다.



[그림 24] IPv6 네트워크 구성방안 2

3.3 IPv6 네트워크 구성방안 3

네트워크 구성방안 2와 비슷하나, IPv4 백본스위치와 IPv6 백본스위치를 서로 연동하여 IPv4와 IPv6를 동시에 사용할 수 있도록 구축하였다. 내부망 사용자는 자유롭게 IPv4와 IPv6 망을 사용할 수 있으며, IPv4/IPv6 트래픽은 서로 다른 루트를 거치게 된다.



[그림 25] IPv6 네트워크 구성방안 3

3.4 구성 방안 검토

구성방안 1의 경우, 백본라우터에서 IPv4와 IPv6 트래픽을 모두 처리하는 경우이며, 구성방안 2는 IPv4와 IPv6 트래픽을 분리하여 처리한다. 방안 1의 경우, 내부 트래픽이 많지 않은 소규모 네트워크에 사용될 수 있으며, 방안 2는 내부 트래픽이 많은 경우 구성될 수 있는 방안이다. 향후 다양한 IPv6 보안시스템들이 도입되면 방안 2의 경우 백본라우터를 모두 IPv4/IPv6 듀얼스택용으로 사용할 수 있는 환경

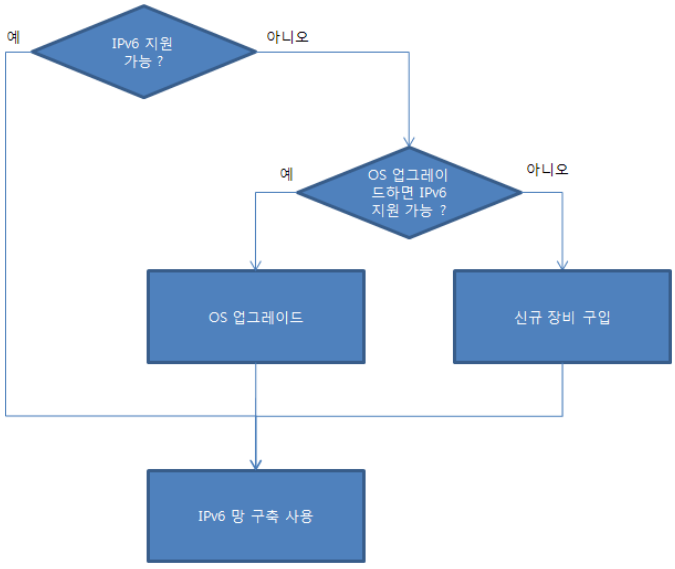
으로 전환할 수 있을 것이다.
하지만, 현재 IPv6 네트워크를 구성함에 있어 보안 문제로 인해 다양한 망 구성에 제한이 있다. 그럼에도 불구하고 가급적 사용자가 IPv4/IPv6를 모두 사용할 수 있는 환경을 만들도록 구성하였다.
위 방안 이외에도 IPv4 네트워크와 IPv6 네트워크를 분리하여 구성하는 방안이 있을 수 있다. 하지만 분리 구성 방안은 테스트베드처럼 될 확률이 높기에 가급적 지양하였다.

4. IPv6 네트워크 고려사항

4.1 IPv6 네트워크 구축 고려사항

가. IPv6 네트워크 구축 절차

기존의 운영되고 있는 IPv4 네트워크에 새롭게 IPv6 네트워크를 구축하고자 할 경우, 먼저 IPv6 네트워크 적용범위를 정한다. 내부 전체 네트워크를 IPv4/IPv6 듀얼스택을 지원하는 네트워크로 구성할 것인지 아니면 일부만에 구성할 것인지를 정한다. 만일 듀얼스택 네트워크로 구축할 경우 기존 운영중인 네트워크 장비 및 보안장비 등이 IPv6를 지원 가능한지를 판단하여야 한다. 각 장비마다 IPv6의 지원여부를 확인하고 IPv6가 지원되지 않을 경우는 OS(Operating System) 업그레이드만으로 IPv6가 지원되는지 재확인한 후 해당장비를 계속 사용할 것인지 신규로 구매할 것인지에 대한 판단을 내려야 한다. 위의 언급한 사항을 그림으로 나타내면 다음과 같다.



[그림 26] 네트워크 장비의 IPv6 활용 여부 판단

나. IPv6 장비 도입 고려사항

• 네트워크 장비

많은 네트워크 장비업체들은 문서상 IPv6 기능을 지원한다고 명시하고 있으나, 실제 IPv6를 지원하는지 지원하더라도 성능면에서 문제가 없는지에 대한 꼼꼼한 분석이 필요하다. 또한, 소프트웨어적으로 IPv6를 지원할 경우에는 하드웨어적으로 처

리하는 장비에 비해 성능이 저하될 수 있으므로 반드시 확인이 필요하다. 또한, IPv6 Ready Logo를 획득한 장비에 대해서도 실제적으로 지원이 가능한지를 확인하여야 한다. IPv6 Ready Logo를 획득한 것 자체가 IPv6를 지원하는 것으로 판단할 수 있으나 다만 실제 망에서 운영하기에 성능이나 기능면에서 부족한 장비들도 있기 때문이다.

장비의 OS를 확인하여 IPv6 지원이 가능한지도 확인하여야 한다. 예를 들어 Cisco 장비의 경우 IOS 12.2(2)T 이상 버전의 OS에서는 IPv6가 지원된다. 따라서, 현재 운영되고 있는 장비의 버전이 12.2(2)T 이하일 경우에는 업그레이드 해야만 한다. Juniper 장비의 경우 JUNOS 5.1 버전에서 IPv6를 지원한다.

• 보안장비

현재까지는 네트워크 장비에 비하여 IPv6를 지원하는 보안장비는 그 수가 적은 편이다. 대부분 Cisco, Juniper 등 외산업체가 대부분이며 퓨쳐시스템즈와 같은 국내업체 등도 IPv6를 지원하는 보안장비를 제공한다. 하지만 대부분 방화벽 정도의 수준에서만 IPv6를 지원하고 있으며 IPS 기능을 지원하는 장비는 소수이며 바이러스 월, 웹 방화벽 같은 기능을 가진 보안장비는 찾아보기 힘들다. 따라서, IPv6 확산을 위해서 개발이 더욱 필요한 분야이기도 하다. 또한 보안장비의 경우 인증 사항도 확인하여야 한다.

• 서버 운영체제

서버 OS 제품군에서 IPv6를 지원하는 버전은 다음과 같다.

[표 1] 서버 제품군의 IPv6 지원 버전별 리스트

	윈도우즈	리눅스	솔라리스	HP-UX
IPv6 지원 버젼	윈도우즈 서버 2000 이상	커널 2.2 이상	5.8 이상	11i 이상
	맥OS	FreeBSD	OpenBSD	
	10x 이상	버전 4 이상	버전 2.7 이상	

•사용자 운영체제

사용자 PC 운영체제의 대부분을 차지하는 윈도우즈의 경우는 윈도우즈 2000에서

부터 지원이 되나 별도의 프로그램을 설치해야 한다. 윈도우즈 XP의 경우는 service pack2 및 ipv6 stack를 별도로 인스톨해야 한다. 윈도우즈 비스타의 경우는 기본적으로 IPv6를 제공한다.

- 윈도우즈 XP의 IPv6 설정 방법
·IPv6 스택 설치 : 시작 → 실행 → cmd 실행 → ipv6 install
·IPv6 설치 확인 : 시작 → 실행 → cmd 실행 → ipconfig 입력후 IPv6 주소 확인

•DNS

주로 DNS 서버로 BIND와 윈도우즈 서버를 사용하고 있다. BIND 9는 BIND 버전 6.4.6 이상에서 윈도우즈 서버는 윈도우즈 2003이상에서 IPv6를 지원하고 있다.

•웹 서버

웹서버 소프트웨어로 주로 Apache, Tomcat 등이 있으며, IPv6를 지원하는 버전은 다음과 같다. Apache 버전 2.0 이상, Tomcat 버전 4.0 이상, WebtoB 4.1 이상, Jrun 4.0 이상에서 IPv6를 제공한다.

또한, 부수적으로 다음과 같은 사항들도 확인하여 미리 준비한다.

• 장비랙

표준 통신랙과 볼트 및 사이즈가 맞는 지 확인 필요하다. 대부분 장비는 표준통신랙의 크기와 규격이 맞으나 일부 맞지 않는 것이 있으므로 확인이 필요하다.

• 전원

IPv6 장비로 교체 및 신규 도입할 경우, 혹은 기존장비 섀시를 이용하고 단지 인터페이스 모듈을 교체할 경우 전원이 부족할 경우도 있으므로, 필요한 전원이 어느 정도 있지를 확인해야 한다. 부족할 경우 장비구매시 전원부에 대한 추가 구매도 필요하다.

• OS(Operating System)

네트워크 장비의 경우 고유의 OS로 운영되고 있으며, 운영되고 있는 장비의 OS가 IPv6를 지원하는지 미리 확인하고, OS 업그레이드 만으로도 IPv6 지원이 가능한 경우, OS 업그레이드를 수행한다. 예를 들어, Nortel ERS8010co 의 경우 Software

Release 4.1부터 지원 가능하나 사용되는 인터페이스 모듈 8634XGRS가 4.1에서 지원하지 않아 OS를 5.1으로 업그레이드해야 한다. 시스코 시스템즈 IOS의 경우 12.0S, 12.2T, 12.2S, 12.2SB, 12.2SR, 12.2SX, Cisco IOS XE Rlease 2.1, 12.3, 12.4 지원하며, IOS의 Release Number에 따라서 IPv6를 지원하는 특성이 틀리기 때문에 아래 참고사이트를 통해서 필요한 특성를 확인하여 맞는 버전을 선택한다. 그리고, 라이센스 레벨에 따라서 IPv6를 지원하기 않을 수 있기 때문에 IPv6를 지원하는 버전이라고 하더라도 어떤 라이센스를 사용하고 있는지를 반드시 확인해야 한다.

- 참고사이트
  http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html
- 3750E 시리즈의 경우 별도의 라이센스 구입이 필요하다.

• GBIC / 광패치코드 타입

기존 운영중인 네트워크 장비와 커넥터 타입 사전 확인 필요하다. 신규로 장비를 도입하거나 인부 인터페이스 모듈을 교체할 경우 인터페이스가 맞지 않는 경우가 종종 생기므로 사전에 확인하여 필요한 인터페이스 카드를 준비한다.

4.2 IPv6 네트워크 구축 Troubleshooting

사례 1) 기존 C6509 (SUP2, X6816)를 IPv4로 운용중이었으며, IPv6 구축을 위한 C6509 장비에 SUP2를 SUP720으로 교체후 X6816 모듈이 인식되지 않는 문제 발생

(원인) X6816은 WS-F6K-DFC인 가속모듈과 Switch Fabric 모듈이 붙여서 나오는데 WS-F6K-DFC 모듈이 SUP2에서만 인식됨

(해결) X6816과 호환가능한 X6516으로 교체하여 구축함. DFC3A부터 SUP720이 인식 가능하므로, 모듈 교체시 인터페이스 모듈 및 서브모듈도 확인이 필요

사례 2) 백본장비 교체 작업(Catalyst 6509) 후 일부 워크그룹 스위치 아래에 있는 사용자단에서 블록킹 현상 발생 => IPv4 패킷은 정상적으로 통신되나, IPv6 패킷만 정상적으로 처리 되지 못함. 에지라우터에서 IPv6 패킷을 처리하지 못함. IOS는 업그레이드 하였으나 문제 발생

(원인) 에지라우터로 사용중인 C3560 문제인줄 알았으나 방화벽의 CF(Compact Flash) 메모리 불량으로 인하여 발생한 문제

(해결) CF 메모리를 교체

사례 3) DMZ 연동된 스위치에 연결하여 IPv6 Address Auto-config 확인 후 연동하였으나 링크가 정상적으로 올라오지 않는 문제 발생

(원인) Nortel L2 스위치와 ISG1000 방화벽간 auto-nego가 지원되지 않아 링크가 올라오지 않음

(해결) 설정 변경 후 연동 확인

사례 4) IPv6 DNS 구축시 IPv6 Only Address가 아닌 IPv4/IPv6 Dual Stack Address를 사용해야 하는 이유

(원인) IPv6 Only 주소를 사용하기에는 현재 구성되어 있는 IPv4의 인터넷 환경과 OS나 애플리케이션들의 IPv6 주소에 대한 지원 문제 등 여러 가지 문제점들이 있기 때문에 IPv6 DNS 구축시 Dual-Stack으로 설치할 것을 권고. 현재 클라이언트의 OS인 Windows XP에서는 IPv6주소를 통한 DNS 쿼리 전송을 지원하지 못하고 있기 때문에 IPv4 주소를 통하여 IPv4와 IPv6의 DNS 쿼리 정보를 받아온 후 (접속 우선순위에 의하여) IPv6주소의 웹사이트로 접속을 하는 방식을 사용. 그렇기 때문에 IPv6 DNS 구성시에도 IPv4 주소는 반드시 필요

사례 5) IPv6 DNS 상위 루트 도메인 연동시 추가적으로 해야 할 작업은?

(방안) Windows 2003서버에서 DNS 설치시 root.cache 파일이 최신버전이 아니기 때문에, IPv6 상위 루트 도메인 주소가 포함된 root.cache 파일을 다운받아 업데이트를 해줘야 합니다(internic 참조). 리눅스에 BIND 설치시에도 named.ca 파일에 IPv6 상위 루트 도메인 주소가 포함되어 있는지 확인하고, IPv6 Address 정보가 없다면 파일을 업데이트

* Windows : C:₩WINDOWS₩system32₩dns₩CACHE.DNS
* Linux : /var/named/named.ca

5. 결 론

우리는 지금까지 IPv6 네트워크로의 전환구축 사례를 통해 전환구축 방안 및 서비스 그리고 문제점들을 살펴보았다. 이번 IPv6 전환 구축을 통하여 대규모 IPv6 네트워크 구축 및 운영 경험 확보가 가능하며 IPv6를 도입하려는 공공기관 및 민간부문에 검증된 IPv6 전환 확산 모델을 제시할 수 있으며, 특히 초기 IPv6 산업의 시장 형성 및 IPv6 장비 개발을 활성화 시키며 상호 운용성 시험을 통하여 국산 장비의 경쟁력 확보가 가능하여 향후 세계 IPv6 장비시장에서도 선도적인 역할의 수행이 가능하다고 본다.

하지만 네트워크 구성에 있어서 가장 큰 문제점은 IPv6의 보안적인 측면에 있다. 많은 네트워크 및 보안 담당 실무자들은 IPv6로의 전환을 인식하고 있으나 막상 IPv6 네트워크를 구축함에 있어 보안에 대해 우려하고 있다. 현재 IPv4용 방화벽, IPS, IDS, UTM, 바이러스 월, 웹 방화벽, VPN 등과 같은 다양한 보안장비가 개발되어 있으나 아직까지 다양한 IPv6용 보안시스템은 미비한 실정이다. 일부 장비들이 개발되어 있으나 성능측면에서 IPv4 장비 수준까지 올라와 있지 못한 상태이기에 IPv6를 도입하고자 하여도 기존의 IPv4 보안 시스템들이 IPv6를 지원하지 못하여 사용될 수 없게 됨에 따라 현재의 IPv4를 IPv6 네트워크로 완전히 변환하는데 한계가 존재한다. 따라서, 앞으로 IPv6로의 전환·확산 및 활성화를 위해서는 IPv6용 보안장비의 조속한 개발이 필요하며, 또한, 네트워크 운영 경험도 축적해야 한다. 물론, IPv6를 위한 킬러애플리케이션 및 IPv6 전용 콘텐츠의 개발 및 정부의 적극적인 투자 및 지원도 필요하다.

참고문헌

[1] 2008 IPv6 동향, 한국인터넷진흥원

[2] 2008 공공부문 IPv6 전환·확산 보고서, 한국인터넷진흥원

[3] 2008 대덕특구 IPv6 클러스터 구축 사업보고서 (한국과학기술정보연구원)

[4] Cisco Homepage, http://www.cisco.com

[5] Juniper Homepage, http://www.juniper.net

[6] Checkpoint Homepage, http://www.checkpoint.com

[7] F5 Networks BIG-IP Homepage, http://www.f5.com/products/hardware/big-ip.html

[8] Ahn Lab Homepage, http://home.ahnlab.com/

[9] Secui.com Product Homepage, http://www.secui.co.kr/

[10] Future Product Homepage, http://www.future.co.kr/01/0102.php

[11] http://ipv6.internet2.edu/

[12] http://www.jgn.nict.go.jp/english/index.html

[13] http://www.cernet2.edu.cn/en/6ix.htm

[14] http://www.twaren.net/english

[15] http://www.geant2.net/

[16] http://www.kisa.or.kr/

[17] http://www.vsix.net

[18] http://www.kreonet.net/english/

[19] http://www.kanren.net