

공공기관 IPv6 적용 안내서

2010.3

공공기관 IPv6 적용 안내서

2010.3



제·개정 이력

순번	제·개정일	변경내용	발간팀	연락처
1	2008.12.31	제정	기술연구팀	02)2186-4500
2	2010.2.10	개정(양식변경)	IP팀	02)405-5172
3				
4				

목 차

서문	iii
제1장 안내서 소개	1
제1절 제정배경 및 목적	1
제2절 안내서 구성	2
제2장 IPv6 소개 및 국내·외동향	3
제1절 IPv6 주소 소개	3
제2절 국내·외 IPv6 동향	7
제3장 공공기관 IPv6 적용 방법 안내	11
제1절 IPv6 적용 절차	11
제2절 IPv6 적용 대상 조사	12
제3절 IPv6 적용 시 고려사항	21
제4절 IPv6 네트워크 연동	39
제4장 공공기관 IPv6 적용사례 : 경상남도청	43
부록	56
1. 참고자료	56
2. 약어표	57
3. 네트워크/보안 장비목록	58

표 목 차

【 표 2.1 IPv4 주소고갈 예측 보고서 】	4
【 표 2.2 IPv6 주소의 장점 】	5
【 표 2.3 전환기술의 종류 】	6
【 표 2.4 IPv6 관련 정부 지침 및 계획 】	7
【 표 2.5 국내 주요 IPv6 사업 】	8
【 표 2.6 미국의 IPv6 추진 사항 】	9
【 표 3.1 주요 IT 자원항목 별 분류 예 】	12
【 표 3.2 IT 자원 현황 조사 항목 예 】	13
【 표 3.3 네트워크 및 보안 장비의 IPv6 지원여부 조사 양식 】	14
【 표 3.4 서버 및 이용단말 자원의 IPv6 지원여부 조사 양식 】	15
【 표 3.5 응용 서비스 조사 항목 】	18
【 표 3.6 응용 서비스 조사양식 예시 】	18
【 표 3.7 응용 서비스 용도별 제공경로 】	20
【 표 3.8 RA방식과 DHCP방식 주소 할당 비교 】	25
【 표 3.9 공공기관 IP 주소대역 할당 예시 】	26
【 표 3.10 네트워크 설계 시 고려사항 예시 】	27
【 표 3.11 서비스 설계 시 고려사항 예시 】	28
【 표 3.12 보안적합성 검증 의뢰 시 제출서류 】	31
【 표 3.13 주요 운영체제별 IPv6 지원현황 (2008.10. 현재) 】	33
【 표 3.14 윈도우즈 버전별 IPv6 지원현황 】	34
【 표 3.15 운영체제별 IPv6 설정 방법 】	35
【 표 3.16 DNS 애플리케이션 】	36
【 표 3.17 메일 서버(SMTP) 애플리케이션 】	37
【 표 3.18 이용자 메일(SMTP) 애플리케이션 】	37
【 표 3.19 HTTP 서버 애플리케이션 】	38
【 표 3.20 연동테스트 절차 및 명령어 】	40
【 표 4.1 IPv6 구축 소요장비 목록 】	44
【 표 4.2 장비별 주소할당 】	46
【 표 4.3 단계별 추진 목표 】	48
【 표 4.4 IPv6 장비 선정 시 고려사항 】	50

그 립 목 차

【 그림 2.1 IPv4 주소구조 】	3
【 그림 2.2 IPv6 주소의 구성 】	4
【 그림 3.1 IPv6 적용절차 】	11
【 그림 3.2 IT 자원 현황 조사 절차 】	12
【 그림 3.3 네트워크 및 보안 장비의 IPv6 지원여부 판단 절차 】	14
【 그림 3.4 서버 및 이용단말의 IPv6 지원여부 판단 절차 】	15
【 그림 3.5 자원의 활용방안 판정체계 】	16
【 그림 3.6 IPv6 지원 상태도 작성 예시 】	17
【 그림 3.7 응용서비스 및 제공경로 개념도 】	19
【 그림 3.8 IPv6 적용 대상 분류 】	21
【 그림 3.9 정책적 관점의 주소 할당 개념도 】	24
【 그림 3.10 계층적 주소 할당 개념도 】	26
【 그림 3.11 보안적합성 검증 절차 】	31
【 그림 3.12 내부 네트워크 연동 시험 구성도 】	39
【 그림 3.13 외부 네트워크와 연결 방법 】	41
【 그림 3.14 IPv6 포털 홈페이지 화면 】	42
【 그림 3.15 외부 네트워크 연동 시험 구성도 】	42
【 그림 4.1 IPv6 적용 전 네트워크 구성도 】	43
【 그림 4.2 IPv6 적용 범위 설정 】	45
【 그림 4.3 IPv6 적용 후 네트워크 구성도 】	47
【 그림 4.4 내부 네트워크 연동 경로 】	53
【 그림 4.5 외부 네트워크 연동 경로 】	54
【 그림 4.6 경상남도청 홈페이지 접속 화면 】	55

제1장

안내서 소개

제1절

제정배경 및 목적

현재 우리가 사용하고 있는 IPv4¹⁾ 주소는 WiBro²⁾, IPTV³⁾ 등 새로운 서비스의 등장과 함께 중국, 인도, 브라질 등 신흥 개발국들의 인터넷 이용이 급증하면서 2010년경에는 고갈될 것으로 예상되고 있다. 따라서 사용이 가능한 IPv4 주소의 수가 급격히 줄어들에 따라 IPv4에 비하여 주소의 수가 많은 IPv6⁴⁾를 도입할 필요성이 점차 커지고 있는 상황이다.

이에 정부는 국가적인 차원에서 IPv4 주소의 부족 문제를 해결하기 위해 세 차례에 걸쳐 IPv6와 관련된 기본 계획을 수립하였고, 총 25개의 IPv6 시범사업을 추진하였으며, 2008년에는 사업추진 주체를 한국정보사회진흥원에서 한국인터넷진흥원으로 이관하여 본격적으로 IPv6 전환 확산 사업을 추진하고 있다.

‘공공부문 IPv6 전환 확산 사업’을 수행하면서 공공기관이 IPv6를 적용할 경우, 적용하는데 필요한 추진절차, 세부 수행과제에 대한 기준이 없다는 현장의 목소리를 반영하여 IPv6 담당자를 위한 ‘공공기관 IPv6 적용 안내서’를 제정하게 되었다.

본 안내서에는 IPv6 관련 기술 및 정책 현황, IPv6 적용에 필요한 절차 및 세부 사항, 공공기관의 IPv6 적용사례 등의 내용을 담아 해당기관에 IPv6를 적용할 경우 발생할 수 있는 잠재적인 위험을 사전에 인지하여 이를 적절하게 조치함으로써 IPv6 으로 원활하게 전환시킬 수 있을 것으로 예상하고 있다.

1) IPv4 : Internet Protocol version 4

2) WiBro : Wireless Broadband, 휴대인터넷

3) IPTV(Internet Protocol TeleVision) : IP기반 네트워크 상에서 전달되는 텔레비전/비디오/오디오/텍스트/데이터 등의 멀티미디어 서비스

4) IPv6 : Internet Protocol version 6

본 안내서는 크게 네 개의 장과 부록으로 구성되어 있다.

제1장은 본 안내서를 제정하게 된 배경과 그 목적을 설명하고 안내서의 전체적인 구성을 간략히 설명하였다.

제2장은 IPv6 주소의 개념, 전환 기술을 소개하여 IPv6 주소에 대한 이해를 높였다. 또한 IPv6 주소를 적용하고자 하는 공공기관의 IPv6 환경에 대한 정보를 제공하고 국내·외 IPv6 동향을 담았다.

제3장은 3단계로 구성된 IPv6 적용절차와 각 단계별로 IPv6를 적용할 때 필요한 사항을 정리하였다.

제4장은 IPv6를 적용한 사례를 정리하여 IPv6를 적용할 때 필요한 현장의 사례를 접할 수 있도록 하였다.

마지막으로 부록에서는 본 안내서에서 사용한 참고자료, 약어표 및 IPv6 장비목록을 소개하였다.

제2장

IPv6 소개 및 국내·외 동향

제1절

IPv6 주소 소개

1. IPv4 주소 개요

1.1 IPv4 주소의 개념

IP(Internet Protocol) 주소는 인터넷에서 통신하기 위하여 각각의 컴퓨터와 통신장비에 부여되는 주소를 가리키며, 일반적으로 IP 주소라 했을 때에는 'IPv4 주소'를 의미한다. IPv4 주소는 [그림 2.1]과 같이 32비트로 구성되며, '.'으로 8비트 단위를 구분한다. 10진수로 표기할 경우, 0.0.0.0부터 255.255.255.255까지의 숫자를 조합하여 사용할 수 있다.



【 그림 2.1 IPv4 주소구조 】

이론적으로 본다면 현재 사용하고 있는 IPv4 주소는 약 43억($\approx 2^{32}$) 개의 주소를 사용할 수 있지만, 사설용으로 예약된 주소영역과 연구용으로 사용되는 특수영역을 제외한다면 실제로 사용할 수 있는 IPv4 주소의 수는 훨씬 적다. 특수용도를 목적으로 할당된 주소의 개수는 IPv4 주소의 약 7.8%인 3.37억 개로 실제로 할당 가능한 IPv4 주소의 개수는 약 40억 개보다 약간 적다.

1.2 IPv4 주소의 고갈 예상 시기

IPv4 주소의 고갈 시기에 대한 예측은 여러 기관에 의해 발표되었으며, IANA⁵⁾ 및 OECD에서 발표된 보고서에 의하면 [표 2.1]처럼 2010년경에 IPv4 주소가 고갈될 것으로 예측하고 있다.

5) IANA(Internet Assigned Names Authority, 인터넷주소자원의 총괄 관리기관) : 인터넷에 접속하기 위한 인터넷 프로토콜(IP)의 전 세계적 주소를 관리하는 중심적 기관

【 표 2.1 IPv4 주소고갈 예측 보고서 】

고갈시기(년)		보고서 제목(발행일)	발행 기관
IANA	RIR		
2010	-	Unallocated IPv4 Exhaustion (2007.8)	IANA
2010	2011	Internet address space : Economic Considerations in the management of IPv4 and in the deployment of IPv6 (2008.6)	OECD

2. IPv6 주소 개요

2.1 IPv6 주소의 개념 및 장점

IPv6 주소는 IPv4 주소가 고갈되는 문제를 해결하기 위하여 새로운 128비트 체계로 2^{128} 개의 주소를 갖는 차세대 인터넷 프로토콜 주소를 말한다.

IPv6 주소는 [그림 2.2]와 같이 16비트 단위로 구분하며 각 단위는 16진수로 변환되어 콜론(:)으로 구분하여 표기한다. 128비트의 IPv6 주소에서 앞의 64비트는 네트워크 주소를 의미하며, 뒤의 64비트는 네트워크에 연결된 통신장비 등에 할당되는 인터페이스 주소를 의미한다.



【 그림 2.2 IPv6 주소의 구성 】

주소길이와 기능에 대해 IPv6 주소가 갖는 장점은 [표 2.2]에 정리하였다.

【 표 2.2 IPv6 주소의 장점 】

구분	주요내용
확대된 주소 공간	주소길이가 128비트로 증가하여 2^{128} 개의 주소 사용 가능
단순해진 헤더 포맷	IPv4 주소 헤더의 불필요한 필드를 제거하여 보다 빠른 처리 가능
간편해진 주소 설정기능	IPv6 프로토콜에 내장된 주소 자동 설정 기능을 이용하여 플러그 앤 플레이 설치가 가능
강화된 보안성	IPv6 주소에서는 IPSec 기능을 기본 사항으로 제공
개선된 모바일 IP	IPv6 주소 헤더에서 이동성 지원

2.2 IPv6 전환기술 소개

2.2.1 듀얼스택(Dual Stack)

듀얼스택 방식은 [표 2.3]에 나타난 것처럼 시스템에 IPv4와 IPv6 프로토콜을 동시에 설정하여 통신 상대에 따라 선택적으로 사용할 수 있도록 하는 방식으로 호스트 및 라우터 등에 듀얼스택을 적용하여 IPv4와 IPv6 패킷을 모두 처리할 수 있도록 해준다. 즉, IPv4/IPv6 듀얼 네트워크 상의 노드는 IPv4 노드와 통신하기 위해서는 IPv4 패킷을 사용하고, IPv6 노드와 통신을 하기 위해서는 IPv6 패킷을 사용한다. 장기적으로 보았을 때 가장 추천되는 방식이다.

2.2.2 터널링(Tunneling)

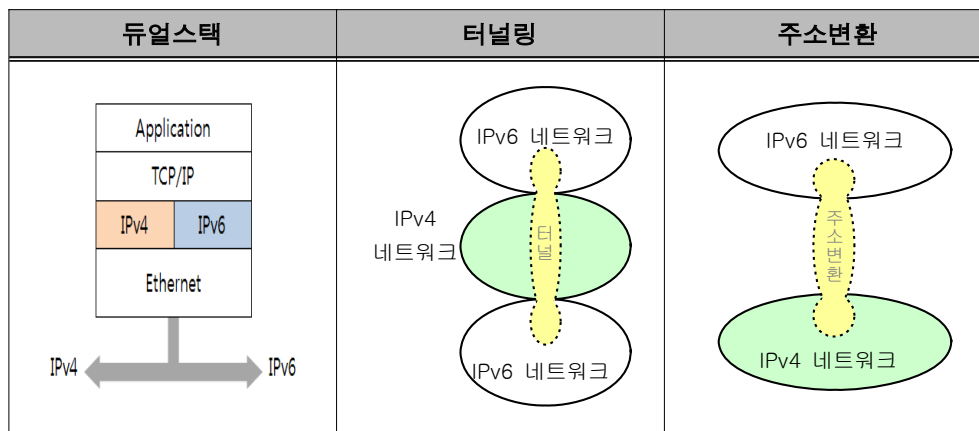
터널링 방식은 IPv4 네트워크를 경유하여 IPv6 네트워크 간 통신을 위한 방식으로, [표 2.3]에 나타난 것처럼 IPv4 네트워크를 통과하는 가상의 경로를 만들어 통신을 하는 것을 말한다. 터널링 기술은 호스트와 라우터에서 IPv6 패킷을 IPv4 패킷으로 캡슐화하여 전송함으로써 캡슐화된 IPv6 패킷이 IPv4 네트워크를 통과하게 하는 기술이다. 이런 경우, 서로 분리되어 있는 IPv6 네트워크 에지 라우터 사이의 구간엔 터널을 설정하면 된다.

2.2.3 주소 변환(Address Translation)

주소 변환 방식은 [표 2.3]에 나타난 것처럼 네트워크의 경계에서 IPv4 주소→IPv6 주소 또는 IPv6 주소→IPv4 주소로 바꾸어 통신을 가능하게 하는 방식이다. 즉, 패킷의 앞부분에 변환 헤더를 추가함으로써 주소를 변환하여 송신을 하고, 수신측에서는 변환 헤더를 제거하는 방식으로 통신을 한다. 소수의 IPv6 사이트가 대규모의 IPv4 인터넷에 연결되는 전환의 초기 단계와, 소수의 IPv4 사이트가 대규모의 IPv6 인터넷에 연결되는 전환의 마지막 단계에 사용

할 수 있다.

【 표 2.3 전환기술의 종류 】



1. 국내 IPv6 동향

국내에서는 정부가 정책적으로 IPv6 적용을 유도하기 위해 지침 및 계획을 발표하고 있으며, 이를 [표 2.4]에 정리하였다.

【 표 2.4 IPv6 관련 정부 지침 및 계획 】

부서	관련 정책	정책내용	발표일
기획재정부	2008년도 예산 및 기금운영계획 집행지침	o 정보시스템의 구축·운영에 사용되는 장비는 IPv4와 IPv6가 동시에 지원되 는 장비를 채택하여야 함	2008. 1
정부통 합전산센터	-	o 전자정부통신망의 제안요청서에 IPv6 요건화 명시 - “정보시스템 운영에 사용되는 통신장 비는 IPv4와 IPv6가 동시에 지원되 는 장비를 채택해야 함”	2007. 7
기획재정부	2008년도 예산안 작성 세부지침	o 정보시스템의 구축은 국가표준 및 정 보시스템의 구축·운영 기술 지침을 적용하고 콘텐츠 보안·시스템 보 안·네트워크 보안·정보보호서비스 등 정보보호, 감리 등 예산을 포함하 여 요구할 것을 명시	2007. 5
정보통신부	IPv6 보급 촉진 기본계획 II	o IPv6 보급 촉진을 위한 비전 및 연도 별 추진 목표 제시 - IPv6 서비스 발굴 및 보급 - IPv6 통신망 구축 - IPv6 보급 촉진을 위한 제도 개선 - IPv6 기반환경 조성 등	2006.12
행정자치부	정보시스템의 구축·운영 기술 지침	o 정보시스템 운영에 사용되는 통신장 비는 IPv4와 IPv6가 동시에 지원되 는 장비를 채택하여야 함	2006. 9
국방부	e-Defense Vision 2015	o 국방개혁기본계획에 따라 ‘미래전 대 비 선진 국방 정보환경 구축’ 추진 - 국방정보통신망에 연도별 IPv6 적용 계획 수립·추진	-

정부의 IPv6 정책에 따라 실시된 국내 주요 IPv6 사업을 [표2.5]에 요약하였다.

【 표 2.5 국내 주요 IPv6 사업 】

기관명	사업명	사업내용	기간
한국인터넷진흥원	공공기관 IPv6 장비 지원사업	<ul style="list-style-type: none"> o 15개 공공기관 및 연구기관에 IPv6 장비인 라우터 및 스위치 등의 장비 구매 지원 o 해당기관의 웹페이지, DNS 등에 IPv6를 적용 및 IPv6 이용 환경의 구축 	2008. 6~11
서울시	서울시 IPv6 시범망 ⁶⁾	<ul style="list-style-type: none"> o IPv6 접속 이용자에게 밤섬 Live CAM 및 IPv4/IPv6 속도측정 서비스 제공 o BcN⁷⁾의 기반이 되는 차세대인터넷주소 체계 정립 및 기술 노하우를 축적하고 IP주소 체계 전환에 대비하기 위한 목적으로 구축 	2006.9 ~ 2007.1
한국정보사회진흥원	KOREAv6 사업	<ul style="list-style-type: none"> o 사업 추진연도에 따라 VoIPv6, UCC 등과 접목하여 시범서비스 실시 <ul style="list-style-type: none"> - IPv6 기반의 치안 서비스 제공 - IPv6 UCC 포털 시범서비스 제공 - 지자체 VoIPv6서비스 제공 o 국내 IPv6 연동기관수 및 이용자 확대와 IPv6 상용장비의 안정성 및 상호운용성 검증 	2004 ~ 2007

2. 국외 IPv6 동향

2.1 미국

미국은 전 세계적으로 할당된 IPv4 주소 가운데 14억 개(약 32.5%)를 확보하고 있음에도 불구하고, 정부가 수요자가 되어 IPv6를 적용할 수 있도록 주도하고 있다. 신기술을 도입하는데 있어서 정부기관이 구매자로서의 역할을 하고 있으며, 공공분야에서 초기시장을 창출하는 역할을 담당하고 있다. 행정관리에산국의 요청에 따라 2008년 6월까지 연방기관의 백본에 IPv6를 적용하고 이를 응용하는 서비스 모델을 수립하였다. 아래 [표 2.6]에 미국의 IPv6 추진 내용을 정리하였다.

6) 참고 링크 : <http://www.ipv6seoul.go.kr>

7) BcN(Broadband Convergence Network, 광대역 통합망) : 음성/데이터, 유무선등 통신/방송/인터넷이 융합된 품질보장형 광대역 멀티미디어 서비스를 언제 어디서나 안전하게 이용할 수 있는 차세대 통합네트워크

【 표 2.6 미국의 IPv6 추진 사항 】

기관명	세부 추진 내용
행정관리에산국 (OMB, Office of Management & Budget)	<ul style="list-style-type: none"> o 2005년 6월에 기업의 정보관리 책임자들에게 정부시책을 배포 o 2008년 6월까지 IPv6 적용 권고, 망 적용계획 및 응용서비스 모델 수립 요청 o 각 연방 기관들이 제시하는 IPv6 적용 방안과 준수 여부를 평가하여 합격 판정을 받은 기관에 한해 IPv6 적용 요건이 충족되었음을 인정 o 2008년 4월 국세청(Internal Revenue Service), 교육부(Department of Education) 및 사회보장국(Social Security Administration)이 IPv6 적용 요건 충족 완료
사회보장국 (SSA, Social Security Administration)	<ul style="list-style-type: none"> o 2007년말에 이미 미국 행정관리에산국의 정부기관 IPv6 적용 요구사항을 충족 완료 o 2007년 12월 10일에 IPv4와 IPv6를 동시에 지원하는 듀얼스택 구조를 채택하여 IPv6 주소를 적용하여 시연 완료
국방부(DoD, Department of Defence)	<ul style="list-style-type: none"> o 'IPv6 전환 5개년 계획'을 수립 o 2003년 10월부터 신규 구입하는 통신장비에 IPv6를 필수적으로 적용하도록 요구 o 2008년까지 국방정보망을 IPv6망으로 전환할 예정 o 일반 네트워크에 IPv6를 우선 적용하고, 보안 네트워크에 적용은 추후 추진 예정

2.2 유럽

유럽연합(EU)은 2001년 유럽 내에서의 IPv6 주소를 보급하고 이를 확산시키고자 EC IPv6TF를 설립하였다. Task Force에서 내린 결정사항과 권고사항들은 2002년 European Council 회의에 제출되었고, e-Europe 2005의 일부로 차세대 인터넷 프로토콜인 IPv6 주소를 적용하는 사업이 추진되었다. Task Force의 가장 큰 실적으로는 유럽의회가 IPv6를 도입한다는 계획을 담은 성명서를 발표하게 하였다는 점이다. 또한 EC IPv6TF는 유럽 국가별로 IPv6TF를 만들어 IPv6와 관련된 정책을 조율하고 기술개발에 협력하고 있다.

2.3 일본

일본은 2001년 e-Japan 전략을 수립한 이후, 2004년 12월 u-Japan 계획을 수립하여 IPv6 기반의 네트워 인프라와 IT서비스를 발전시키고 있으며, 2010년 세계 최첨단 유비쿼터스 사회를 구현하는 목표를 정하였다. 2006년 초에는 총리 직속의 IT전략본부에서 e-Japan의 차기전략인

‘IT 신개혁 전략’을 발표하였고, 2008년까지 모든 일본정부의 전자행정 서비스에 IPv6 주소를 적용하는 사업을 추진하고 있다.

2.4 중국

중국은 2000년부터 연구 교육망인 CERNET⁸⁾을 통해 IPv6 테스트베드를 구축하여 IPv6와 관련된 연구를 시작하였으며, 2006년 9월에 세계 최초로 자국산 라우터를 이용한 IPv6 ‘CNGI-CERNET2/6IX⁹⁾’의 구축을 완료했다. CNGI-CERNET2/6IX는 중국산 IPv6 라우터를 사용한 최초의 국가 백본망으로 초당 2.5G~10GB의 데이터 전송 속도를 지원하며 CNGI 백본 네트워크에는 전국 20개 도시에 분산되어 있는 25개 주요 노드가 연결되어 있다. 중국은 2006~2010년까지 국가 경제사회개발계획에 차세대인터넷 부문을 포함시켜 IT 국가 건설의 핵심 사업으로 추진하고 있으며, IPv6의 실질적인 확산을 위해 P2P와 센서 네트워크, ITS 및 자동 차통신, 이동통신, 홈네트워크 등의 영역에서 IPv6를 적용하는 사업을 추진하고 있다.

8) CERNET : China Education and Research Network

9) CNGI-CERNET2/6IX : China's Next Generation Internet - China Education and Research Network/IPv6 Internet eXchange

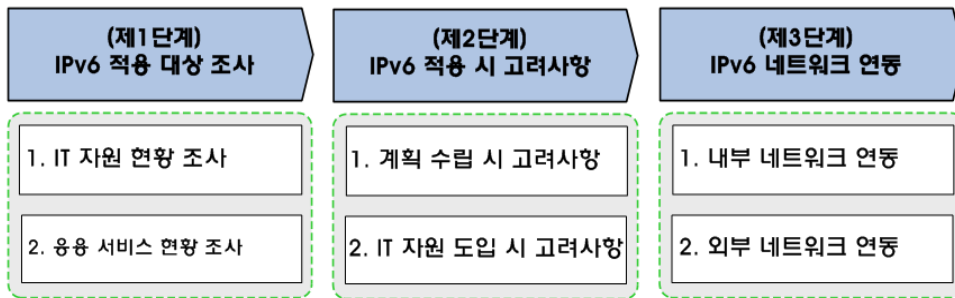
제3장

공공기관 IPv6 적용 방법 안내

제1절

IPv6 적용 절차

본 안내서는 공공기관이 IPv6를 적용하기 위한 절차로 [그림 3.1]처럼 “IPv6 적용 대상 조사”, “IPv6 적용 시 고려사항”, “IPv6 네트워크 연동” 등 총 3단계로 구분한다.



【 그림 3.1 IPv6 적용절차 】

제1단계 “IPv6 적용 대상 조사”는 IPv6를 적용하고자 하는 공공기관의 현재 내부 환경을 조사하는 단계로, 조사 대상을 IT 자원과 응용서비스로 구분하여 자원 분류에 따른 조사 방법을 제시하였다.

제2단계 “IPv6 적용 시 고려사항”은 IPv6를 적용 계획을 수립하는 단계로 계획의 수립 및 IT 자원을 도입할 때 고려하여야 할 사항을 기술하였다.

제3단계 “IPv6 네트워크 연동”은 IPv6를 구축한 이후에 내·외부의 IPv6 네트워크에 접근하기 위해 연동을 수행하는 단계로, 해당기관의 내부, 하위기관과의 연동, ISP 및 IPv6 연동망을 통한 외부 네트워크와의 연동 방법을 다루었다.

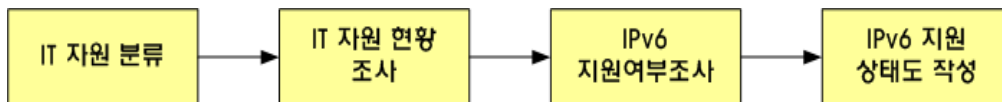
제2절

IPv6 적용 대상 조사

1. IT 자원 현황 조사

1.1 IT 자원 현황 조사 절차

IT 자원 현황 조사는 [그림 3.2]와 같이 IT 자원 분류, IT 자원 현황 조사, IPv6 지원여부 조사 및 IPv6 지원 상태도 작성 등 총 4단계로 나눌 수 있다.



【 그림 3.2 IT 자원 현황 조사 절차 】

IT 자원은 IPv6를 적용하게 되는 직접적인 대상이 되므로 현재 공공기관에서 보유하고 있는 장비를 항목에 따라 분류하고, 각 IT 자원에 대해서 IPv6를 적용했을 때 조치가 필요한지, 만약 필요하다면 어느 부분에 어떤 조치가 필요한지를 명확하게 조사하고 분석하여야 한다. IT 자원 현황을 조사한 결과는 IPv6를 적용하기 위해 기존 장비의 업그레이드, 신규 장비 도입, 장비 재배치, 폐기 판정 및 지원상태도를 작성하는데 사용되며 IPv6를 적용하는 범위 설정을 위한 자료로 활용된다.

IT 자원을 크게 네트워크, 보안, 서버 및 이용단말, 소프트웨어 등으로 분류하였다.

【 표 3.1 주요 IT 자원항목 별 분류 예 】

구 분	종 류
네트워크	o 라우터(Edge, Border 등) 및 스위치(L2, L3, L4, L7 스위치 등) o AP(Access point) 장비, NAT 장비 등
보안	o 방화벽, IPS ¹⁰⁾ , IDS ¹¹⁾ , VPN 등
서버 및 이용단말	o 서버(웹, DB, 인트라넷 등) o 클라이언트(데스크톱PC · 노트북PC 등) o 음성 · 영상기기(화상회의 기기 등) o 기타(PDA, 스마트폰, 프린터, 팩스 등) o 각 장비의 운영체제(Windows, Unix, Linux 등)
소프트웨어	o 애플리케이션 (DNS, DHCP, FTP, Sendmail, Apache, Tomcat 등) o 기타 데이터베이스(Oracle, Informix, MS-SQL, MySQL 등)

1.2 IT 자원 현황 조사 수행

IT 자원 현황 조사의 목적은 용도에 따라 IT 자원을 세분화하여 분류하고 장비의 제조사, 도입일 및 담당자 등 일반적인 사항을 조사하여 IPv6 적용시 활용하기 위해서다. 조사할 때 제조사의 기술정보 등을 이용하여 장비의 사양, OS 및 기능 등의 상세한 부분까지 조사하여야 한다. 특정 장비에 대해 IPv6 관련 자료나 특이사항을 체계적으로 정리한 후 IPv6 적용 범위를 설정할 때 활용할 수 있도록 한다.

【 표 3.2 IT 자원 현황 조사 항목 예 】

항목	주요내용
자원위치	o 자원이 설치되어 장소를 표시(본부 · 산하기관 또는 부서이름 등)
분류항목	o IT 자원 분류(네트워크, 보안, 서버 및 이용단말, 소프트웨어 등)
자원구분	o 자원의 종류 별 구분(라우터, 백본스위치, L2 · L3스위치 등)
자원이름	o 자원의 모델명 및 버전
자원일련번호	o 같은 이름의 자원이 여러 개 있을 경우 자원을 구분하는 일련번호

1.3 IT 자원의 IPv6 지원여부 조사

1.3.1 IPv6 지원여부 확인

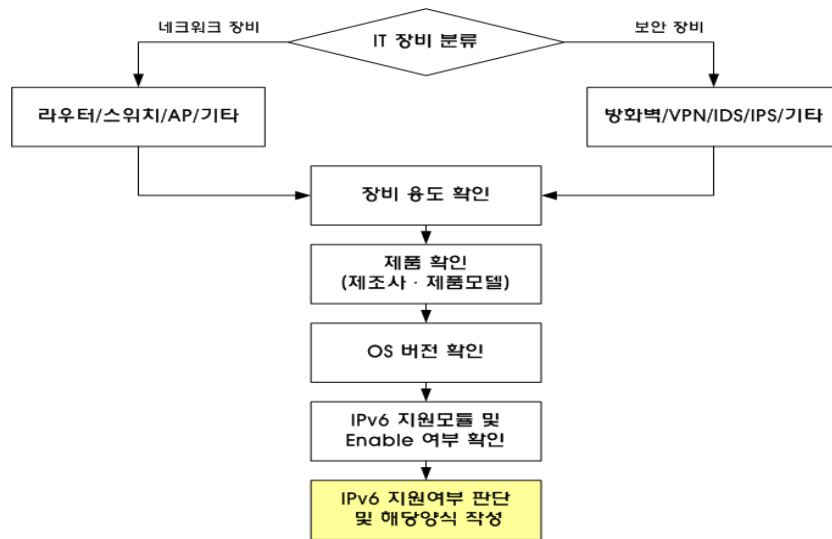
자원의 현황을 전체적으로 조사하고 그 결과를 자료화하여 유형별로 나눈 다음, 유형별 자원에 대한 IPv6 지원 여부를 조사하여 IPv6 지원을 위해 업그레이드하여야 할 사항들을 확인한다.

네트워크 및 보안 장비에 대한 IPv6 지원 여부 조사와 절차는 [그림 3.3]에 나타내었다. 먼저 IT 자원을 네트워크 또는 보안장비로 구분하여 절차에 따라 각 장비의 용도, 제조사 및 제조 모델, 및 장비의 OS 버전 등을 조사하고 IPv6를 지원하기 위한 명령어 설정 및 OS 업그레이드

10) IPS(Intrusion Protection System, 침입 방지 시스템) : 네트워크에서 공격 서명을 찾아내 자동으로 모종의 조치를 취함으로써 비정상적인 트래픽을 중단시키는 보안 솔루션

11) IDS(Intrusion Detection System, 침입 탐지 시스템) : 컴퓨터 시스템의 비정상적인 사용, 오용, 남용 등을 실시간으로 탐지하는 시스템

등의 지원 방법 등을 정리한다.



【 그림 3.3 네트워크 및 보안 장비의 IPv6 지원여부 판단 절차 】

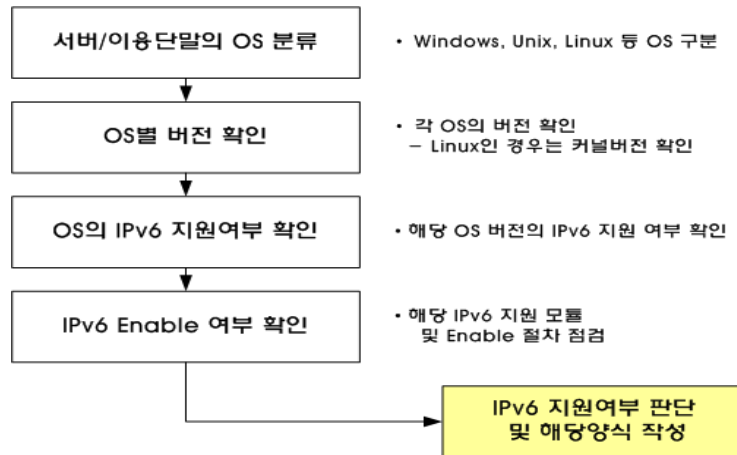
아래 [표 3.3]처럼 장비의 OS 버전, H/W 규격, IPv6 지원 여부, IPv6 지원을 위한 조치 사항 및 일반적인 관리를 위한 사항 등을 조사하여 정리하도록 한다.

【 표 3.3 네트워크 및 보안 장비의 IPv6 지원여부 조사 양식 】

자원위치			자원구분/자산번호	
모델명/ 시리얼넘버			취득일	
제조사명			담당자	
H/W 사양	프로세스 속도 및 종류		LAN Port	
	Memory		WAN Port	
	Flash		서비스 카테고리	
	I/O		치수(높이x너비x깊이)	
운영체제/버전			IPv6 지원가능 여부	
			(O, X)	
IPv6 지원을 위한 조치 사항				
특이사항				

서버 및 이용단말의 IPv6 지원여부를 조사하기 위해서는 [그림 3.4]처럼 먼저 공공기관의 서

버 및 이용단말의 OS에 따라 구분한다. Linux OS의 경우는 OS 버전과 함께 Kernel 버전도 함께 조사하여야 한다. 각 OS 버전에 따른 IPv6 지원여부와 설정 방법을 조사하고, 필요에 따라서는 모듈을 추가적으로 설치할 필요가 있는지도 확인한다.



【 그림 3.4 서버 및 이용단말의 IPv6 지원여부 판단 절차 】

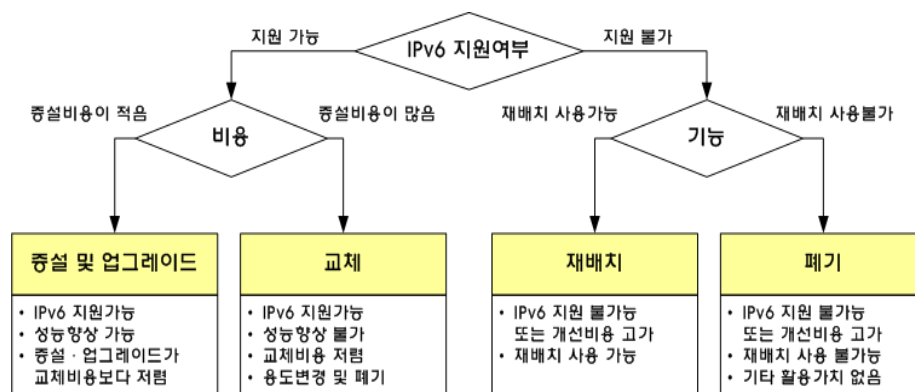
IPv6 지원 판정에 필요한 OS 종류, OS 버전, H/W 사양 및 일반적인 관리를 위한 사항 등을 [표 3.4]의 양식에 따라 작성하도록 한다.

【 표 3.4 서버 및 이용단말 자원의 IPv6 지원여부 조사 양식 】

자원위치		자원구분/자산번호	
모델명/시리얼번호		취득일	
제조사명		담당자	
H/W 사양	CPU		
	Memory		
	Disk		
	LAN Card		
운영체제/버전			IPv6 지원가능 여부
			(O, X)
IPv6 지원을 위한 조치 사항			
특이사항			

1.3.2 자원의 활용방안 판단

자원의 증설·교체 등에 대한 결정은 공공기관이 보유한 자원의 이용효율을 높여 IPv6를 적용시 발생하는 예산을 절감하고 IPv6를 적용하는 대상을 명확히 할 수 있다. 자원의 증설과 교체는 설정만으로 IPv6를 곧바로 적용할 수 있는 경우도 있고, IPv6가 지원되는 경우라고 해도 용량을 증설하거나 업그레이드가 필요한 경우도 있다. 증설 또는 업그레이드가 필요한 경우 업그레이드가 교체비용보다 비싸다고 한다면, 그 자원을 새로운 자원으로 교체하고, 교체된 자원은 재배치하여 사용하거나 폐기하는 것이 경제적이다. IPv6 지원 불가 판정을 받은 자원이라고 해도 IPv6와 IPv4가 당분간 공존하므로 IPv4 네트워크에 재배치하여 사용할 수도 있다. [그림 3.5]는 가격, 기능 및 성능 요소를 고려하여 IPv6 적용에 따른 판단 과정을 도표화한 것이다.



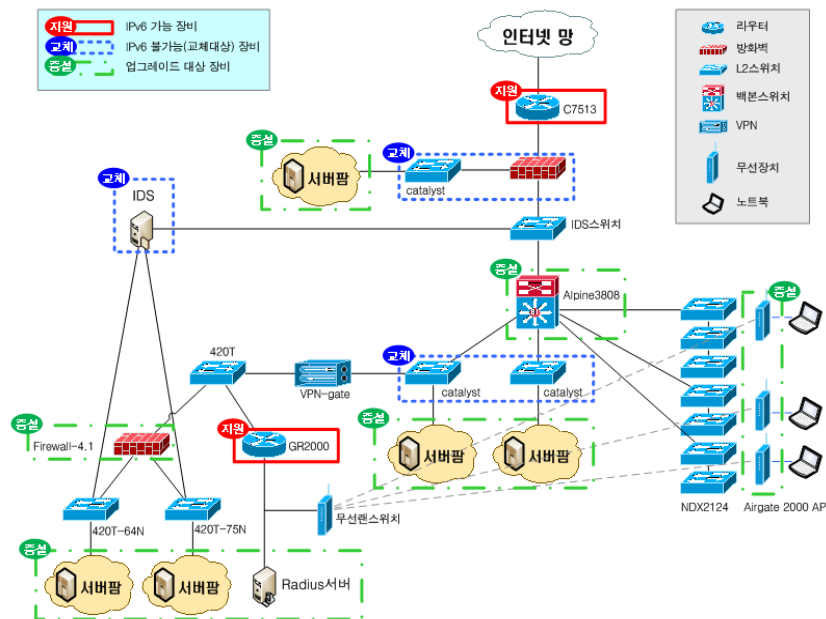
【 그림 3.5 자원의 활용방안 판정체계 】

1.4 자원의 IPv6 지원 상태도 작성

자원의 IPv6 지원 상태도는 자원의 IPv6 지원 여부를 조사한 결과와 지원방안에 대한 분석 결과를 네트워크 구성도 상에 표기하여 IPv6 적용의 가·불가 상황을 한눈에 파악할 수 있도록 하는데 목적이 있다.

또한 지원 상태도는 산하기관 및 조직별로 IPv6의 적용 여부를 쉽게 파악할 수 있어 IPv4/IPv6 전환기술을 적용하기 위한 시뮬레이션이 가능할 뿐만 아니라 적용의 범위를 설계할 때에도 유용하다. 자원의 IPv6 지원 상태도는 영역별 IPv6의 지원 상태를 도식적으로 보여주어 이해를 쉽게 하고, 각 서비스를 제공하는 서버와 이용단말 간의 트래픽흐름을 추적할 수 있게 해준다. 따라서 소요되는 예산과 확보할 수 있는 예산을 감안하여 적용 범위를 설정하는데 많은 도움을 준다.

지원 상태도를 작성하기 위해서는 먼저 구성도에서 각 서비스·네트워크 요소 별 IPv6 지원여부를 판정한다. [그림 3.6]은 지원 상태도를 작성할 때 하나의 예시를 보여준다.



【 그림 3.6 IPv6 지원 상태도 작성 예시 】

위의 예시와 같이 지원 상태도는 각 구성요소들의 IPv6에 대한 지원여부를 일목요연하게 파악할 수 있게 해준다. 지원상태가 표시되어 있지 않은 IDS스위치, 420T, VPN-gate, 420T-64N, 420T-75N, 무선랜스위치 등은 IPv6와 무관한 장비임을 나타낸다.

2. 응용 서비스 현황 조사

응용 서비스 현황 조사는 인터넷을 기반으로 하는 응용서비스에는 어떤 것이 있으며, 각 서비스 별 이용자, 제공 경로, 및 영역이 어떻게 구성되어 있는지를 파악하는 것을 말한다. 조사 항목은 [표 3.5], 조사양식의 예는 [표 3.6]과 같다.

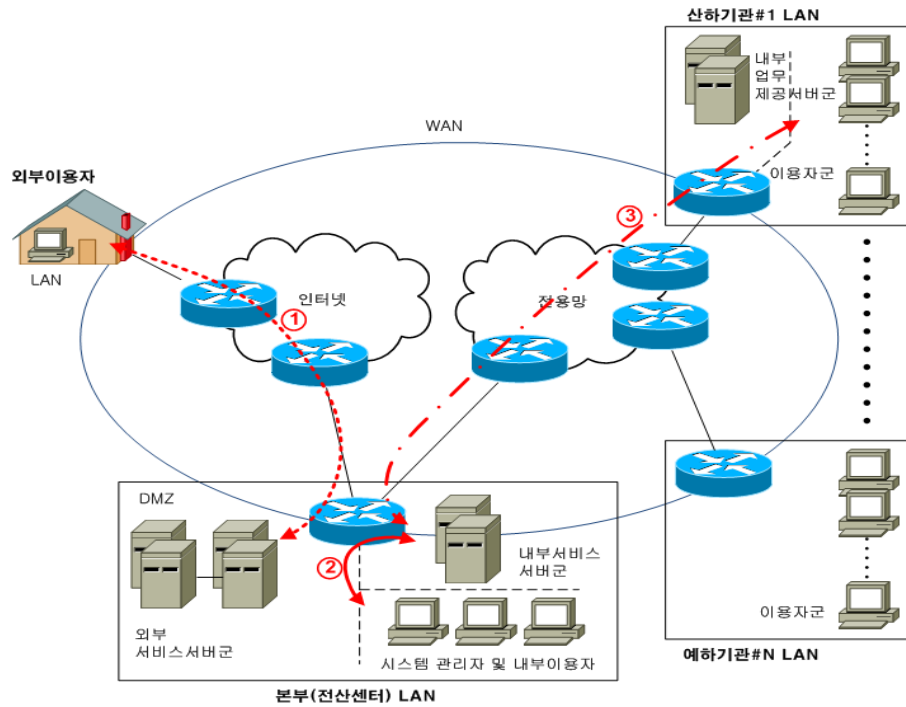
【 표 3.5 응용 서비스 조사 항목 】

항목	조사 내용 및 설명
서비스명(또는 업무명)	응용서비스의 이름
서비스 설명	응용서비스의 기능과 역할
서버 위치	보통 센터나 지역거점에 있지만 드물게 다른 곳에 있는 경우도 있음
제공 경로	네트워크상의 트래픽 제공경로로써 제공위치와 이용위치에 따라 다양함
이용단말 위치	본사(본부)나 센터에만 있을 수 있고, 전국적으로 있을 수 있음
IPv6 지원여부	무관, 지원, 미지원
IPv6 적용 시 조치사항	미지원 시 조치할 사항을 기재

【 표 3.6 응용서비스 조사양식 예시 】

서비스명 (업무명)	서비스 설명	제공경로 및 이용영역			IPv6 지원여부	IPv6 적용 시 조치사항 (소요비용 포함)
		서버 위치	제공경로	이용단말 위치		
서비스 #1						
서비스 #2						
.....						
서비스 #N						

[그림 3.7]은 서비스 제공경로 및 이용영역에 대한 이해를 돕기 위해 개념적으로 제시된 것이다.



【 그림 3.7 응용서비스 및 제공경로 개념도 】

[표 3.6]의 제공경로는 응용서비스(또는 제공업무)별 서버의 위치에서 이용단말까지의 트래픽 경로이며, 아래 [표 3.7]에 서비스 용도별 제공경로의 설명을 나타내었다. IPv6를 적용하는 계획을 수립할 때, 이 경로 상에서 해당 서비스의 트래픽이 원활하게 흐를 수 있도록 조치하면 된다. 이용영역은 이용단말군의 위치이며, 조직별로 구분할 수도 있고 서비스 이용형태별로 구분할 수도 있다. IPv6 적용 방법과 적용 범위를 검토할 때는 이용영역 및 이용형태로 구분하거나 두 가지를 종합하여 기관의 환경에 맞추어서 검토한다.

【 표 3.7 응용서비스 용도별 제공경로 】

용도	제공경로예시	경로설명
대국민용	① LAN-WAN	<ul style="list-style-type: none"> o 인터넷을 통해 대국민 서비스를 제공하는 경우의 경로 o LAN : 서비스 서버군이 위치한곳의 내부네트워크 ex) 서버군↔L4/L7스위치↔백본스위치↔라우터 o WAN : 서버군의 LAN이 서비스를 제공하기 위해 연결되는 외부네트워크 ex) LAN라우터↔인터넷↔국민
업무용	② LAN	<ul style="list-style-type: none"> o 서비스 제공서버와 이용단말이 내부네트워크에 있는 경우 o LAN : 병원, 학교와 같은 단일 기관의 내부네트워크 ex) 서버군↔L4/L7스위치↔백본스위치↔워크그룹스위치↔이용단말
	③ LAN-WAN-LAN	<ul style="list-style-type: none"> o 광역망을 갖춘 대형기관의 경우 업무서비스 제공경로 o LAN : 서비스 서버군이 위치한곳의 내부네트워크 ex) 서버군↔L4/L7스위치↔백본스위치↔라우터 o WAN : 서비스를 제공하기 위해 서버군의 LAN과 이용자들의 LAN간에 연결되는 광역네트워크 ex) LAN라우터↔광역전용망↔LAN라우터 o LAN : 서비스 이용자들이 위치한곳의 내부네트워크 ex) 이용자군↔워크그룹스위치↔백본스위치↔라우터

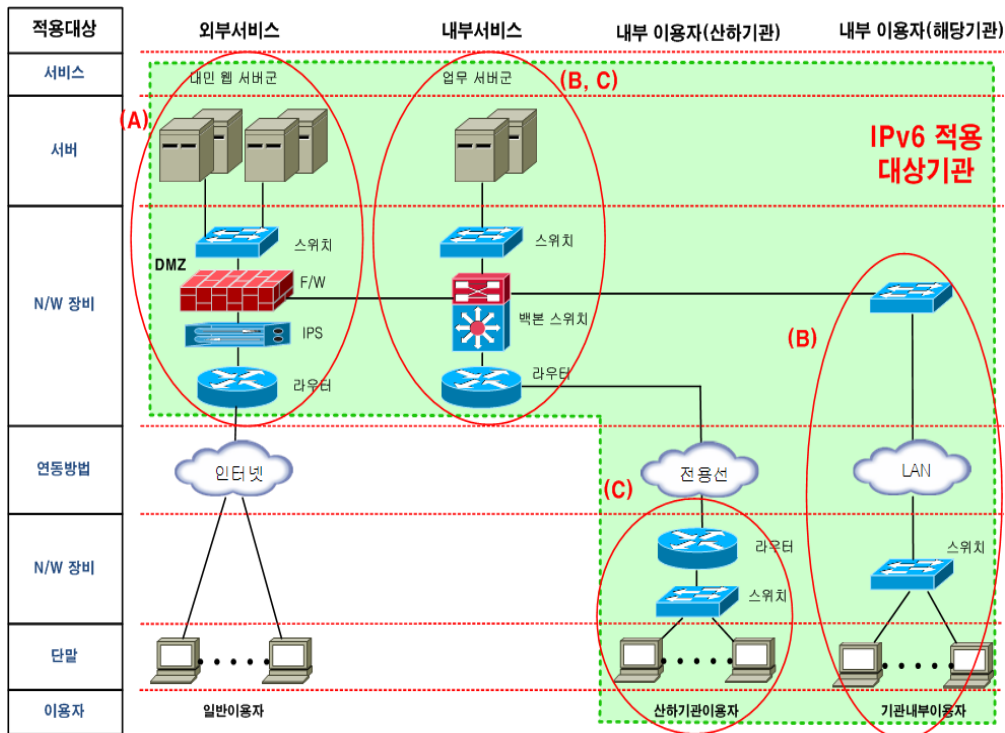
제3절

IPv6 적용 시 고려사항

1. 계획 수립 시 고려사항

1.1 적용범위 설정

공공기관에서 IPv6 적용을 추진하고 계획을 수립하기 위해서는 우선 순위를 고려하여 IPv6 적용 범위를 정하여 추진한다. 적용 범위를 결정하기 위해서는 IT 자원의 현황과 응용서비스 및 제공경로를 조사한 결과를 토대로 작성한 IPv6 지원 상태도를 활용하도록 한다. 보유 장비의 사양, 예산, 네트워크의 구성 상태, 업무용 및 대민 서비스의 종류 등에 따라 IPv6 적용 우선 순위와 적용 범위가 결정된다.



【 그림 3.8 IPv6 적용 대상 분류 】

위의 [그림 3.8]은 IPv6 적용 범위를 나타내기 위하여 적용대상을 네트워크 단위로 분류하여 나타내고 있다. 이 그림은 공공기관에서 제공하는 서비스 이용자 측면에서만 고려하여 이

용단말 위주의 그림으로 간략하게 나타내었다.

공공기관의 외부 이용자에게 제공되는 서비스를 위한 IPv6 적용, 기관 내부의 업무에 IPv6 서비스를 위한 IPv6 적용, 공공기관 내부의 이용자 적용 3가지로 구분된다. IPv6의 적용하고자 하는 공공기관은 예산, 인력, 인프라, 추진 정책 등에 따라 IPv6 적용 범위를 결정한다.

☐ 외부 서비스 적용의 범위 (A)

대민서비스와 같이 인터넷을 통해 제공되는 외부 서비스에 IPv6를 적용하여 공공기관의 외부 이용자가 IPv6 기반의 서비스를 이용하게 하는 것을 의미한다. 외부 이용자가 공공기관에 접속하여 서비스를 이용하는 경로인 라우터, IPS, 방화벽, 스위치 및 서버 구간에서 IPv6 패킷이 전송 가능하도록 IPv6를 적용하는 것이다.

☐ 내부 서비스 및 내부 이용자 적용의 범위 (B)

이는 그룹웨어 등 기관의 업무 서버군에서 제공되는 내부 서비스에 IPv6를 적용하여 해당 기관의 내부 이용자가 이를 이용하게 하는 것을 의미한다. 해당 기관의 내부 업무 서비스를 제공하는 업무 서버와 스위치에 IPv6를 적용하고, 이용자의 네트워크 구간에 해당하는 이용단말 및 스위치에 IPv6를 적용하는 것이다. 즉, 해당 기관의 내부 이용자 단말에서부터 업무용 서버까지 IPv6 패킷의 전송이 가능하도록 하는 것이다.

☐ 내부 서비스 및 내부 이용자(산하 기관) 적용의 범위 (C)

이는 해당 기관의 업무 서비스에 IPv6를 적용하고 이 서비스를 산하기관 이용자가 이용하도록 하는 것을 의미한다. 해당 기관의 업무 서비스에 IPv6를 적용하는 것은 앞의 적용 범위 (B)와 비교하면 외부 접속 라우터에 추가로 IPv6를 적용하고, 산하 기관의 내부에는 이용자의 단말 구간과 해당 단말이 연결된 네트워크의 백본스위치 및 접속라우터까지의 구간 사이에 IPv6를 적용하여 산하 기관의 내부 이용자 단말에서 상위 기관의 업무 서버까지 IPv6 패킷이 전송되도록 한다.

1.2 IPv6 주소 할당·관리

1.2.1 IPv6 주소 확보

□ IP 주소 신청 방법¹²⁾

IP주소를 할당받는 방법은 AS¹³⁾번호를 가지고 독자적인 네트워크를 구축하여 한국인터넷진흥원으로부터 직접 할당받는 방법, 인터넷 서비스를 제공하는 ISP에게 할당받는 방법이 있다. 공공기관에서 IPv6 주소를 할당받는 일반적인 방법으로는 ISP로부터 주소를 할당 받는 것이 있으며, IPv6를 적용하고자 계획을 수립할 때 IPv6 주소확보 가능여부를 ISP에 문의하여야 한다.

□ 공공기관의 IPv6 주소 확보

인터넷을 통해 타 공공기관이나 다른 IPv6 네트워크에 접속하기 위한 주소는 ISP를 통하여 IPv6 주소를 할당받는 것이 원칙이나, 상위기관으로부터 할당받을 수 있다. 한국인터넷진흥원에서 주관한 공공기관 IPv6 장비지원 사업을 수행한 공공기관들은 행정안전부에 속하는 지방자치단체이기 때문에 행정안전망과의 연동을 위해 행정안전부로부터 IPv6 주소를 확보하였다.

1.2.2 IPv6 주소 할당

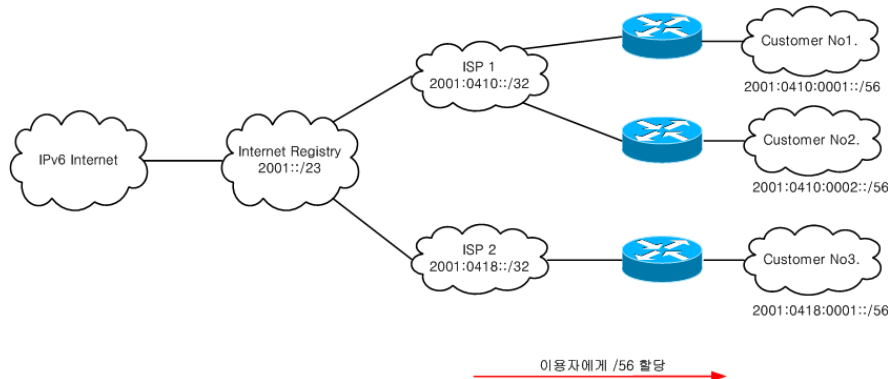
□ 주소 할당 정책

○ 네트워크 주소 부분 할당

네트워크 주소 부분은 인터넷주소의 자원관리 체계에 따라 정책적으로 할당된다. 정책적 관점에서 실제 할당되는 주소의 공간을 살펴보면 IANA는 전체 주소의 공간에서 2001::/23 이상을 레지스트리에 할당하고 각 레지스트리는 IPv6 ISP에게 /32 이상을 할당하며, ISP는 /56을 각 고객에게 할당하게 된다. [그림 3.9]는 단계적으로 /23 →/32→/56 순서로 프리픽스가 할당되는 것을 나타낸다.

12) 인터넷진흥원(<http://ip.kisa.or.kr/>)를 참조

13) AS(Autonomous System, 자율 시스템) : 1개의 관리 권한이 운용하는 라우터와 통신망의 집합체



【 그림 3.9 정책적 관점의 주소 할당 개념도 】

o 인터페이스 주소 부분 할당

인터페이스 주소 부분을 생성하는 방법은 관리자가 수동으로 할당하는 방법과 네트워크 연결과 동시에 IP 주소가 설정(Plug&Play)되는 자동 할당으로 구분할 수 있다. 또한 자동 할당은 RA¹⁴⁾방식과 DHCP 방식이 있다.

수동 할당은 네트워크 상의 호스트 및 서비스에 필요한 서버의 IP 주소를 관리자가 직접 할당하는 방식으로, 보안적인 면에서 본다면 신뢰성이 확보된 호스트만 네트워크에 접근할 수 있어 안정성을 확보할 수 있다. IPv6를 적용할 때 호스트의 수가 많지 않은 초기 시험망을 구성할 경우에 사용될 수 있다. 하지만 수동 할당의 경우, 호스트의 수가 늘어나 네트워크가 커지게 되면 관리가 어려워진다는 점도 있다.

자동할당 방식 중의 하나인 RA 방식은 장비의 고유 주소인 MAC 주소를 이용하는 것으로, 라우터가 정기적으로 배포하거나 장비가 라우터에 배포를 요청하는 경우에 주소를 할당하는 방식으로 네트워크에 배포된 RA를 통하여 주소의 프리픽스를 취득하고, 인터페이스 ID는 장비에서 생성한다. IPv6에서는 RA 방식을 사용하는 것이 일반적이다. DHCP 방식은 IP 주소 전체를 네트워크에서 취득하는 방식으로 DHCP 서버에 주소 할당을 요청하여 IP 주소를 할당 받는 방식으로 라우터 없이 서버만 사용하는 환경에서 활용이 가능하다. 클라이언트를 위한 설정 데이터를 얻는 과정은 IPv4와 유사하다.

아래 [표 3.8]는 자동할당에 해당하는 두 방식의 특징을 비교하여 보여준다.

14) RA : Router Advertisements

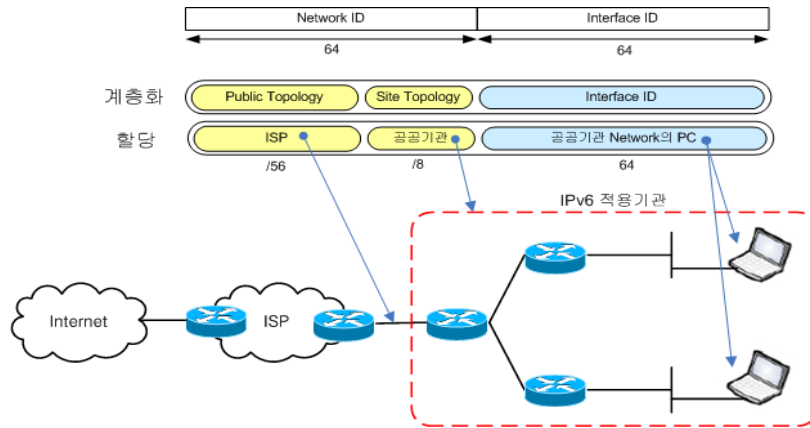
【 표 3.8 RA방식과 DHCP방식 주소 할당 비교 】

항목	RA 방식	DHCP 방식
배포 가능한 주소	IPv6 주소	IPv4 주소 및 IPv6 주소
배포 기기	라우터	DHCP 서버
배포 Timing	라우터가 정기적으로 배포 또는 장비에서 배포 요구	PC에서 배포(할당) 요구
배포 정보	IP 주소(프리픽스)	IP 주소 (전체)
	RA 배포 라우터	서버
	-	도메인 네임

□ 공공기관의 주소 할당 계획 수립

공공기관에서 주소할당 계획을 수립할 때는 공공기관의 네트워크 구조를 파악하여 실제로 IPv6 주소가 필요한 장비 및 단말에 정확하게 대응될 수 있도록 하여야 한다.

네트워크 주소를 할당할 경우, 우선적으로 고려하여야 할 사항은 네트워크 전송 효율성을 보장하기 위해 네트워크의 구조를 바탕으로 계층적으로 주소를 할당하여야 한다는 점이다. 이외에도 주소의 단편화 방지, 미래에 있을 네트워크 수요 증가에 대비한 여유 대역 보장, 네트워크를 관리하는 효율성, 주소 할당에 대한 확장성 및 유연성 등을 고려하여야 한다. [그림 3.10]은 계층적 주소 할당 개념도이다.



【 그림 3.10 계층적 주소 할당 개념도 】

예를 들면 공공기관 내부에서의 업무 성격 및 물리적인 구분(주민센터별 구분, 층 구분, 건물의 구분)에 따라 IP 주소 대역을 할당할 것인지 등에 대한 계획을 수립하여야 한다. 또한 인터페이스 및 네트워크의 유효범위에 따라 사용할 주소를 결정해야 한다. 아래 [표 3.9]는 공공기관 내·외부 네트워크 주소를 할당하는 예시이며, 네트워크의 수에 따라 프리픽스를 달리하여 주소를 할당한 것이 나타나 있다.

【 표 3.9 공공기관 IP 주소대역 할당 예시 】

구분		설명	IPv6 Address(prefix)	네트워크 수
외부 네트워크	Serial 구간	6KANet 연동	2001:xxxx:xxxx:2000/64	1
	내부 연동	장비간 인터페이스	2001:xxxx:xxxx:0000/60	16
		서버팜	2001:xxxx:xxxx:0010/60	16
		예비	2001:xxxx:xxxx:0020/64 ~ 2001:xxxx:xxxx:0FFF/64	
내부 네트워크	본청	장비간 인터페이스	2401:xxxx:xxxx:xx00/60	16
		예비	2401:xxxx:xxxx:xx10/60	16
		본청사용자용	2401:xxxx:xxxx:xx20/59	32
		예비	2401:xxxx:xxxx:xx40/58	64
	읍면동 사무소	장비간 인터페이스	2401:xxxx:xxxx:xx80/59	32
		외부사업소	2401:xxxx:xxxx:xxA0/59	32
		읍면동사무소	2401:xxxx:xxxx:xxC0/59	32
		예비	2401:xxxx:xxxx:xxE0/59	32

1.3 네트워크 및 서비스 설계

1.3.1 네트워크 설계

네트워크를 설계할 때 고려해야 할 사항은 적용 범위에 따라 내부 및 외부 네트워크로 나뉘지며, 이를 [표 3.10]에 나타내었다.

【 표 3.10 네트워크 설계 시 고려사항 예시 】

고려 사항	설 명
적용대상의 외부접속	산하기관이나 연계기관과의 연결 여부
지리적 위치	연계기관의 물리적 위치
서비스 제공 사업자	이용하고 있는 ISP 사업자에 대한 사항
멀티호밍 구성여부	이중화 및 내부 이용자를 위한 멀티호밍 필요성
라우팅 프로토콜	내·외부 라우팅 프로토콜
외부 데이터 센터	공공기관이 이용하는 외부 데이터 센터의 존재 여부
링크 구성	IPv4와 IPv6의 링크 구성(동일링크/별도링크)

내부 이용자의 네트워크만 적용대상이 될 경우, 관문라우터에서 내부 IPv6 네트워크와 외부 IPv4/IPv6 네트워크와의 연동을 위한 전환기술만 적용하고 나머지 외부접속에 관련된 사항은 무관하다.

외부 접속은 전용회선 등 산하기관 및 연계기관과 연결하기 위한 것이므로 광역망을 갖춘 기관에 적용할 때 고려해야 하는 사항이며, 필요한 IPv6 주소블록의 수량과도 관계가 있다. 외부접속의 개수는 라우팅 등 IPv6와 관련된 설정과 확보하여야 할 IP블록의 수와 직접적인 관련이 있다. 외부 접속의 수가 산하기관의 숫자라면 해당 숫자만큼 IP블록을 확보하여야 한다. 또한 산하기관이 또 다른 산하기관을 가진다면 계층 구조의 IP블록을 설계·확보한다.

멀티호밍은 백본 네트워크 안정성을 위해 2개의 ISP 사업자 회선을 사용하여 부하분산 또는 백업을 위한 것이다. 기관에서 IPv6를 적용하는 범위의 한계로 IPv4와 IPv6가 혼재할 경우, 각 구간별로 IPv4와 IPv6의 경유 링크를 동일하게 할 것인지, 다른 링크를 이용하게 할 것인지는 구성 자원의 IPv4/IPv6 변환기술에 대한 지원여부에 따라 정해지기도 하고 경유 링

크의 설계에 따라 구성 자원에 대한 교체여부가 결정되기도 한다.

전체 영역에 IPv6를 적용하기 위한 설계를 하다 보면 IPv6를 전혀 적용할 수 없는 영역이 생기기도 한다. 이 경우 내부에 IPv4 영역을 따로 둘 수 있는데, 이때 접속라우터에서 방화벽까지는 IPv4와 IPv6가 같은 링크를 사용하게 한다. 만약 네트워크 및 서비스 구성상의 문제로 IPv4와 IPv6를 각각 별도의 링크를 사용해야 한다면, only IPv4 네트워크를 따로 구축할 수 있도록 설계하여야 한다.

1.3.2 서비스 설계

네트워크 설계와 마찬가지로 현재 공공기관에서 사용 중인 서비스 현황 조사 결과를 이용하여 정의한 우선 순위에 따라 IPv6 적용을 추진한다. 서버와 이용단말의 OS, 웹서버·메일서버·DBMS¹⁵⁾ 등 상용 애플리케이션의 경우는 버전에 따라 IPv6 지원여부가 비교적 명확하여 적용 결과가 예측이 되지만, 패키지 애플리케이션이나 자체적으로 발주하여 개발된 애플리케이션의 경우는 지원 여부가 명확하지 않는 경우가 많다. 이런 경우 IPv6를 적용했을 때 생기는 위험을 회피하기 위해 사전에 테스트베드를 구성하고 이를 적용하는 시험을 하는 것이 좋다. 서비스의 설계를 위해 고려하여 할 사항의 예시를 [표 3.11]에 나타내었다.

【 표 3.11 서비스 설계 시 고려사항 예시 】

고려항목	고려사항
서비스 우선 순위	IPv6 적용을 위한 서비스의 우선 순위
업그레이드	IPv6 적용을 위한 업그레이드 가능 여부
IPv4/IPv6 지원	서비스의 IPv4/IPv6 지원 필수성 여부
IPv4/IPv6 의존도	특정 IP버전으로 서비스를 제공하여야하는지 여부
서비스 제공 범위	공공기관 내·외부에 제공되는지 여부
기존 서비스에 대한 영향	IPv6 적용으로 기존 IPv4 서비스에 주는 영향

IPv6를 적용하기 위해 제공되는 서비스 서버의 OS 및 애플리케이션의 업그레이드가 가능한지의 여부를 고려하여야 한다. 특히, 보안이나 인증과 연관되는 서비스는 공공기관의 보안정책에 맞추어 충분한 검증이 우선적으로 이루어져야 한다.

15) DBMS(DataBase Management System, 데이터베이스 관리 시스템) : 데이터베이스를 구성하고 이를 응용하기 위하여 구성된 소프트웨어 시스템.

IPv4/IPv6 지원 및 의존도는 제공하는 서비스의 특성에 따라 IPv6 적용이 필수적인지 또는 서비스가 특정 IP 버전으로만 제공되어야 하는지를 고려하는 것이다. 또한 신규 서비스는 개발 단계에서부터 IPv6의 특징을 반영할 수 있도록 추진하여 이용자의 확대 및 홍보를 위해서도 활용할 수 있도록 하여야 한다.

1.4 원상복구 계획

원상복구 계획은 IPv6를 구축하는 도중에 예상하지 못한 문제가 발생했을 때 문제점이 발생하기 이전의 상태로 되돌려 네트워크, 보안 및 서비스를 정상적으로 제공하기 위한 방안이다. 예측하지 못한 문제가 발생하게 되면 장비의 이상 동작, 타 장비와의 연동 그리고, 보안정책에서 결정된 보안 수준의 확보, 나아가 네트워크에서의 서비스 곤란 등의 상황이 일어날 수 있으므로 이에 대한 대비책이 사전에 충분히 고려되어야 하며, 네트워크·보안 장비 및 서비스 등의 모든 구성 요소를 대상으로 하는 원상 복구 계획을 수립하여야 한다.

원상 복구를 위해서는 관련 항목의 백업이 필수적이며 중요 항목으로는 장비운영 OS의 버전, 펌웨어 버전, 장비의 설정 상태, 서비스의 버전, 관련 데이터 등이 있다. 원상 복구를 위해서는 IPv6를 적용하기 이전 상태의 OS 버전이나 데이터 등에 대한 백업이 필요하므로 운영지침서의 백업 관리와 연계하여 계획을 수립하여야 한다.

원상 복구의 방법으로는 백업 자료를 통한 복구, 서버 및 이용단말의 IPv6 기능 비활성, 설정 명령어의 삭제 및 추가 모듈의 제거 등이 있으며, 시험 네트워크를 구성할 때 기존 장비로 교체할 수 있도록 구성을 하는 것도 한 방법이다.

IPv6를 초기 적용하는 단계에서는 고립존을 구축하여 사전 검증을 마친 후, 네트워크에 적용할 수 있는 방안을 고려하고, 실제 테스트는 업무 및 서비스를 제공하지 않는 야간에 실시하도록 계획을 수립한다. 테스트에 관한 사항이나 IPv6를 적용한다는 공지를 사전에 행할 수 있도록 계획을 수립하여야 한다.

원상복구 계획을 수립할 때에는 공공기관에 IPv6를 적용할 경우 발생할 수 있는 잠재적인 문제를 사전에 파악하여 IPv6를 적용했을 때 일어나는 부작용을 최소화하기 위한 위험요소에 대한 분석 결과를 반영하도록 한다. 기본적으로 분석하여야 할 위험요소로는 IPv6와 관련된 표준 성숙도, 업체의 제품 출시 일정, 상호 운용성 등이 있다.

상호 운영성에 대한 위험요소는 IPv6 Ready Logo¹⁶⁾를 획득한 제품 구매를 우선 고려하거

16) 참고 링크 (<http://www.ipv6ready.org/frames.html>)

나 테스트 베드를 구성하여 해당 기관이 도입한 IPv6 하드웨어 및 소프트웨어를 사전에 점검하여 감소시킬 수 있다.

1.5 보안적합성 검증

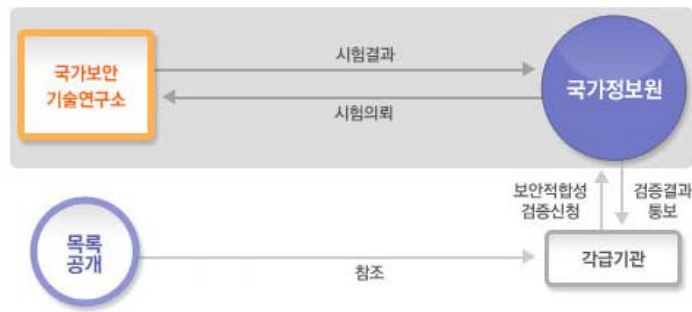
보안적합성 검증제도는 ‘전자정부구현을 위한 행정업무 등의 전자화 촉진에 관한 법률’ 등 관계법규¹⁷⁾에 의거하여 국가 및 공공기관이 도입하는 정보보호 제품의 보안적합성과 안전성을 사전에 검증함으로써 국가정보통신망의 보안 수준을 제고하기 위해 시행하는 제도이며, 2008년 4월 보안적합성검증 제도를 보완 발표한 이후 2008년 6월 1일부터 시행되고 있다. IT 보안인증사무국 홈페이지¹⁸⁾에서 제공되는 CC인증 제품 목록을 참조하여 도입하고자 하는 장비가 현재 어떤 검증을 받고 있는지에 대한 현황을 확인한다.

주의하여야 할 사항으로는 기존에 보안적합성에 대한 검증을 받은 제품을 도입하더라도 해당기관이 요구하는 보안사항과 해당기관에 구축된 네트워크 구성이 다르기 때문에 보안적합성 검증은 필수적으로 받아야 한다. 또한 IPv6 담당자는 RFP상에 보안적합성에 대한 검증필을 받은 대상만 제안에 참여할 수 있다고 명시하여 CC인증을 받은 제품이 도입 대상에서 제외되지 않도록 하여야 한다.

보안적합성 절차는 [그림 3.11]에서 나타나 있다. 보안장비를 도입하고자 하는 기관에서는 국가정보원에서 공개한 목록을 참조하여 도입장비를 선정한다. 선정한 장비에 대한 보안적합성의 검증을 국정원(문의 02-3412-3380)에 의뢰한다. 국정원에서는 국가보안기술연구소에 의뢰하여 진행된 시험결과를 받아 신청기관에 그 결과를 통보해 준다. 시험 결과에 의해 장비를 운용했을 때 잠재할 수 있는 보안 취약점이 발견되면 이를 제거한 후에 사용하여야 한다.

17) 전자정부법 2조(정보통신망 등의 보안대책 수립·시행), 국가정보보안기본지침 제91조(도입)

18) 참고 링크 (<http://www.kecs.go.kr/>)



【 그림 3.11 보안적합성 검증 절차 】

출처 : 국정원 IT보안인증사무국

보안적합성 검증을 의뢰할 때 필요한 서류는 6종으로 [표 3.12]에 나타내었다. 그 중 3종만 신청기관에서 작성하면 되고 나머지 3종은 업체에서 작성하면 된다.

【 표 3.12 보안적합성 검증 의뢰 시 제출서류 】

제출서류	서류 작성자
검증 신청서	신청기관
사용자 보안요구 사항	
정보통신망 구성도 등 운영환경	
CC인증서 사본 또는 암호검증서 사본	개발업체
보안목표명세서	
인증보고서	

2. IT 자원 도입 시 고려사항

2.1 네트워크 장비

IPv6 장비를 도입할 때 IPv6 Ready 로고를 획득하거나 TTA 인증을 받은 장비는 장비의 성능과 안정성이 검증되었으므로 우선적으로 고려할 필요가 있다. 현재 일부의 제품들만 로고를 획득한 상태이며, 앞으로 로고를 획득하게 될 장비의 수는 계속 늘어나고 있으므로 장비를 도입할 때 반드시 IPv6 Ready 로고를 획득한 장비로 한정하지는 않는 것이 좋다

일반적으로 IPv6 지원을 H/W 방식이 아닌 S/W 방식으로 처리하는 장비는 IPv4 패킷과 IPv6 패킷을 동시에 처리하게 되면 성능이 저하될 수 있다. 그러므로 IPv6를 도입할 때 처리 방식에 의한 차이를 정확하게 파악하고 이를 적절하게 조치하여야 한다.

공공기관에서 보유한 장비의 버전을 확인하고 IPv6 지원 여부를 파악하고 업그레이드를 해주어야 할 장비를 파악하도록 한다. “부록3. 네트워크/보안 장비목록”에는 업그레이드를 통해 듀얼스택 지원이 가능한 장비와 기본적으로 듀얼스택을 지원하는 장비 목록을 수록하였다. 이 목록을 참고하고 장비의 OS버전 등을 확인하여 IPv6 지원이 가능하도록 조치한다.

라우터는 장비의 OS를 조사하여 IPv6 지원 여부를 판정하며, 그에 대한 자료는 참고 문서나 웹페이지를 통해 제공된다. 시스코의 IPv6 Solution 문서¹⁹⁾에 ISO²⁰⁾ 버전이 정리되어 있는데, IOS 12.2(2)T 이상이 되어야 IPv6 지원이 가능하며 지원 프로토콜에 따라서는 IOS 12.4 이상이 요구되기도 한다. 주니퍼네트웍스의 IPv6 Information Hub 웹페이지²¹⁾에서는 IPv6와 관련된 장비를 손쉽게 검색하여 확인할 수 있다. 주니퍼네트웍스의 OS JUNOS는 9.x 버전이 출시되고 있으며, 5.1 버전 이상이면 IPv6를 지원한다. LG-Nortel은 기존 장비에 대해 IPv6를 지원할 계획이 없는 것으로 조사되었으며, 2008년 4분기에 Dual Stack 지원이 가능한 신규 장비를 출시할 예정이다.

스위치도 OS의 조사를 통해서 IPv6 지원 여부를 판정할 수 있으며, 제조사에 따라 유상 및 무상으로 IPv6를 지원하도록 업그레이드를 해줄 수 있는 제품이 있다. L4/L7 스위치는 주로 로드밸런스 용도로 사용되므로 서버나 방화벽에 대한 로드밸런스의 지원 여부도 확인하여야 한다.

IP-PBX 및 VoIP 장비는 장비, 서버 및 단말(H/W방식 또는 S/W방식)에 대해서 IPv6를 지원할 수 있도록 해주어야 한다.

2.2 보안 장비

공공기관에서 보안장비를 도입하기 위해서 CC인증제품을 대상으로 도입할 장비를 선정하고, 선정된 장비를 대상으로 보안적합성에 대한 검증 절차를 밟아야 한다. 국가정보원의 IT보

19) 참고 링크

- http://www.cisco.com/en/US/technologies/collateral/tk648/tk872/tk373/technologies_white_paper_09186a00802219bc.pdf

20) IOS (Internetwork Operating System) : 시스코사에서 생산하는 라우터의 OS

21) 참고 링크 : <http://www.juniper.net/federal/IPv6/>

안인증사무국²²⁾홈페이지에서 제공하고 있는 평가·인증 제품의 목록, 검증필 제품의 목록 및 해당 자료실에서 배포하고 있는 정보보호 인증제품의 목록을 참고하면 제품을 선정하는데 도움이 될 것이다. 정보보호 인증제품 목록에는 인증제품군별로 인증 현황과 각 제품의 규격(개요, 시스템 사항 및 주요 기능)도 간략히 제공되고 있으며 제조사의 연락처를 포함하고 있어서 제품에 대한 문의를 할 때 유용하다.

현재 대부분의 국산 제품들은 일부에 한하여 IPv6 지원이 되고 있으므로 IPv6 담당자는 “부록3. 네트워크/보안 장비목록”을 참고하여 해당 장비 업체에 IPv6 지원 여부와 인증 사항을 확인한다.

2.3 서버 및 이용단말

2.3.1 서버 운영체제

서버 OS 제품군에는 Windows, Linux, Unix(Solaris, FreeBSD, HP-UX 등) 등이 있으며, 각 운영체제별 IPv6 지원 현황은 아래 [표 3.13]에 정리되어 있다.

【 표 3.13 주요 운영체제별 IPv6 지원현황 (2008.10. 현재) 】

버전	윈도우즈	리눅스	솔라리스	HP-UX	맥OS	FreeBSD	OpenBSD
IPv6 지원버전	윈도우즈 서버 2000이상	커널 2.2 이상	5.8이상	11i 이상	10x 이상	버전 4 이상	버전 2.7 이상
최신버전	윈도우즈 서버 2008	커널 2.6.26.3	10	11i v3	10.5.3	7.0	4.4

위의 표를 이용하여 기존 서버의 운영체제에서 IPv6를 지원하는지에 대한 여부를 판단할 수 있으므로 OS의 업그레이드를 진행하여야 한다. 이때 단순히 OS 업그레이드만으로 충분한지, 아니면 하드웨어 업그레이드가 필요한지도 함께 검토되어야 한다. 하지만 최근 출시되는 거의 모든 OS에는 IPv6에 대한 지원이 기본적으로 보장되고 있기 때문에 OS의 IPv6 지원여부에 대한 고려가 점차로 줄어들고 있다.

2.3.2 이용단말 운영체제

22) 참고 링크 (<http://www.kecs.go.kr/>)

대표적인 이용단말인 PC의 경우, 거의 대부분 윈도우즈 OS를 사용하고 있다. 윈도우즈 OS 버전별로 IPv6 지원현황을 살펴보면 [표 3.14]와 같다.

【 표 3.14 윈도우즈 버전별 IPv6 지원현황 】

종류	IPv6 지원여부	비고
윈도우즈 3.1, 95, 98, ME	X	미지원
윈도우즈 2000 프로	△	별도의 애드온 프로그램 설치
윈도우즈 XP	O	service pack2 설치 필요 및 IPv6 설치 필요
윈도우즈 비스타	O	운영체제 자체에 내장

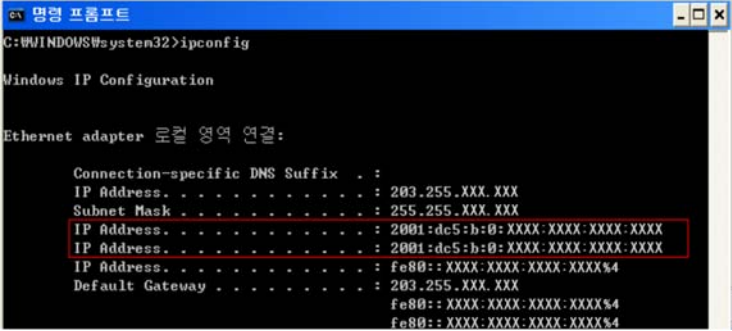
윈도우즈 2000의 경우는 별도의 프로그램을 설치하여야만 IPv6가 지원되며, 윈도우즈 XP는 서비스팩2를 설치하여 IPv6 기능을 활성화 해주어야만 한다. 윈도우즈 비스타의 경우는 별다른 설정 없이 바로 IPv6 기능이 지원된다.

윈도우즈 XP는 2008년 6월 30일부로 단종되었는데, 행정안전부에서는 행정기관의 PC 운용체계(OS)는 윈도우즈 XP를 주로 사용하되 점진적으로 윈도우즈 비스타로 전환한다고 밝혔다. 공공기관에 공급되는 컴퓨터의 운영체제는 행정기관의 내부 업무를 안정적으로 운영하기 위해 윈도우즈 비스타를 사용하는데 문제가 없다고 판단될 때까지 윈도우즈 XP가 공급될 것이며, 점진적으로 윈도우즈 비스타로 전환될 것으로 보고 있다.

2.3.3 IPv6 설정 방법

운영체제별로 IPv6를 설정하는 방법을 [표 3.15]에 나타내었으며, 설정하는 방법은 한국인터넷진흥원의 IPv6 포탈 홈페이지에서 운영체제에 맞는 서비스팩을 다운로드하여 설치한다. 윈도우즈 XP의 경우는 스타트팩 대신에 커맨드창에 'netsh interface ipv6 install'을 입력하여 설치할 수도 있다. IPv6 주소가 정상적으로 할당되었는지를 확인하기 위하여 커맨드창에 ipconfig 명령어를 입력하여 주소를 확인한다.

【 표 3.15 운영체제별 IPv6 설정 방법 】

버전	설정 방법
2000	<p>가. IPv6 Start Pack를 이용하여 설치</p> <ol style="list-style-type: none"> ① http://www.vsix.kr/startpack/setup-2000.exe 에서 IPv6 start Pack 다운로드 후 설치 ② ‘시작 → 실행 → cmd입력 → enter → ipconfig입력 → enter’를 통해 IPv6 주소 할당 여부 확인
XP / 2003	<p>가. IPv6 Start Pack를 이용하여 설치</p> <ol style="list-style-type: none"> ① http://www.vsix.kr/startpack/setup-xp.exe에서 IPv6 start Pack 다운로드 후 설치 ② ‘시작 → 실행 → cmd입력 → enter → ipconfig입력 → enter’를 통해 IPv6 주소 할당 여부 확인 <p>나. XP의 'netsh'를 이용하여 설치</p> <ol style="list-style-type: none"> ① ‘시작 → 실행 → cmd입력 → enter → netsh interface ipv6 install 입력 → enter’를 통해 IPv6 설치 ② ‘시작 → 실행 → cmd입력 → enter → ipconfig입력 → enter’를 통해 IPv6 주소 할당 여부 확인 
VISTA	<p>가. 특별한 구성 변경 없이 사용 가능(OS에 기본 탑재)</p> <p>‘시작 → 실행 → cmd입력 → enter → ipconfig입력 → enter’를 통해 IPv6 주소 할당 여부 확인</p>

2.4 소프트웨어

2.4.1 DNS

DNS 서버는 IPv4 인터넷과 IPv6 인터넷에서 모두 이용할 수 있어야 한다.

IPv6 주소의 길이가 128비트로 증가되어 이를 외우기가 더욱 어려워졌기 때문에 숫자로 구성된 IP 주소를 사용자가 쉽게 기억할 수 있는 도메인 이름으로 변환하는 서비스가 더욱 필요해졌다. 따라서 IPv4와 IPv6가 공존하는 환경에서 도메인의 이름과 매핑되는 IP 주소를 파악하기 위해서는 IPv4 주소 질의와 IPv6 주소 질의를 각기 독립적으로 수행하여 처리할 수 있는 DNS가 필요하다. 이용단말은 IPv4 주소와 IPv6 주소에 대한 DNS 응답을 이용하여 어떤 노드와 통신에 할 것인지를 선택한다.

국내에서 널리 사용되고 있는 대표적인 DNS는 BIND²³⁾와 Windows DNS가 있다. 오픈 소스인 BIND DNS는 IPv6가 윈도우즈OS에서 지원되지 않으므로, Windows OS 환경에서는 Microsoft DNS를 사용하여야 한다. IPv6 담당자가 DNS에 IPv6를 구현할 경우에는 [표 3.16]을 참조하여 적절한 버전을 설치하여야 한다.

【 표 3.16 DNS 애플리케이션 】

Application	Version	참조 웹사이트
BIND 9	BIND 8.4.6 이상 (현재 9.5.0)	http://www.bind9.net/ (리눅스, 유닉스 계열만 지원)
윈도우즈 서버	2003 이상 (현재 2008)	http://www.microsoft.com/korea/windowsserver2008/default.mspx

공공기관에서 IPv6 DNS를 신규로 구축할 경우에는 최신 버전의 BIND를 선택하는 것이 좋다. BIND 4는 현재 개발과 공식적 배포가 중단된 상태이며, BIND 8은 보안업데이트가 중단된 상태이다. BIND S/W Download 및 관련 자료는 홈페이지²⁴⁾에서 구할 수 있으며 2008년 10월 BIND 9.5.0 까지 배포되었다.

2.4.2 이메일

SMTP를 이용한 메일 서버 애플리케이션은 [표 3.17]에 정리하였다. 가장 널리 쓰이는 애플리케이션으로는 sendmail이 있으며 프로그램 다운로드 및 관련 참고 문서 등은 웹사이트를 참조하도록 한다. 이 외에도 exim, zmailer 등의 애플리케이션도 IPv6를 지원하고 있다.

23) BIND(Berkeley Internet Name Domain, 버클리 인터넷 이름 도메인) : BSD(Berkeley Software Distribution) 기반의 유닉스 시스템을 위해 설계된 도메인 네임 시스템(DNS)

24) 참고 링크 (<https://www.isc.org/software/bind>)

【 표 3.17 메일 서버(SMTP) 애플리케이션 】

Application	Version	참조 웹사이트
sendmail	8.8.0 이상 (현재 8.14.3)	http://www.sendmail.org/
exim	1.9x 이상 (현재 4.69)	http://www.exim.org/
zmailer	1.99.26 이상 (현재 2.99.57)	http://www.zmailer.org/
postfix	2.2.0 이상 (현재 2.5.5)	http://www.postfix.org/start.html

SMTP를 이용한 이메일 이용자 애플리케이션에서 IPv6를 지원할 수 있는 버전을 아래 [표 3.18]에 정리하였다. 프로그램의 다운로드 및 참고 문서 등은 웹사이트를 통해 제공되고 있다.

【 표 3.18 이용자 메일(SMTP) 애플리케이션 】

Application	Version	참조 웹사이트
mozilla-mail	1.4 이상	http://www.mozilla.org/ Mozilla 1.4는 Win32 platform을 완전히 지원하지 못함
thunderbird	1.0 이상 (현재 2.0.0.18)	http://www.mozilla.org/ 버전 1.5 이후부터 Win32 platform을 완전히 지원
ximian-evolution	1.4.5	http://www.novell.com/linux/ximian.html

2.4.3 웹

웹서비스를 위한 대표적인 애플리케이션으로 Apache, Tomcat 등이 있으며, [표 3.19]에 HTTP 서버 애플리케이션에 대한 사항을 정리하였다. 각 애플리케이션의 다운로드나 참고 문서는 해당 웹페이지에서 제공되고 있다.

【 표 3.19 HTTP 서버 애플리케이션 】

Application	Version	참조 웹사이트
Apache	2.0 이상 (현재 2.2.9)	http://httpd.apache.org/
Tomcat	4.0 이상 (현재 6.0.18)	http://tomcat.apache.org/ (Servlet/JSP ²⁵⁾ 규격에 따라 버전이 다름)
WebtoB	4.1 이상	http://www.tmax.co.kr/tmaxsoft/index.screen WebtoB 3.x 이하 2008.12.31 단종 예정 (서비스 종료 2009.12.31. 예정)
Jrun	4.0 이상	http://www.adobe.com/products/jrun/

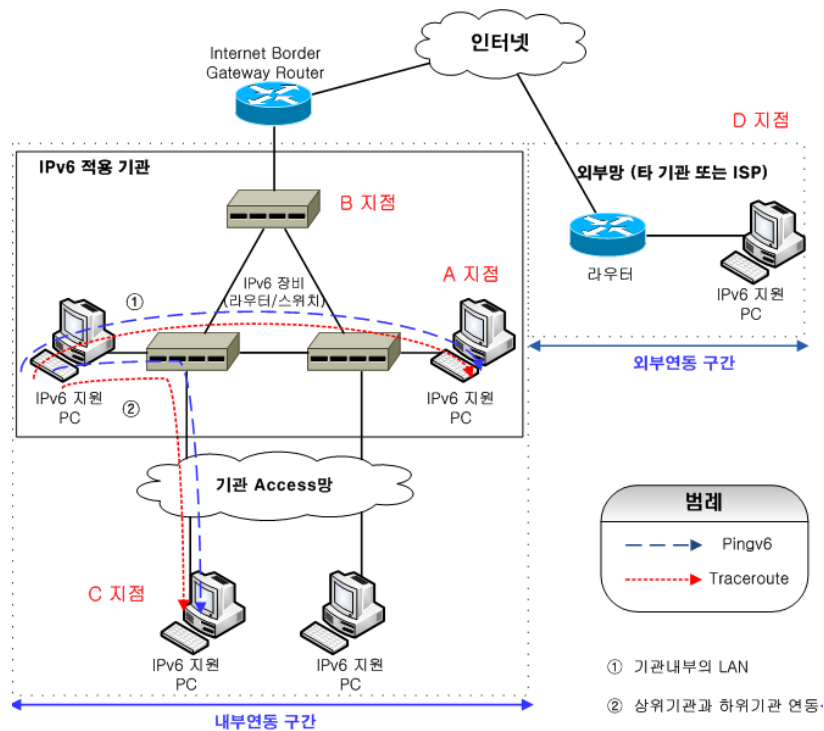
25) JSP(Java Server Page, 자바 서버 페이지) : 웹 서버에 있는 서브릿(servlet)을 사용해 웹 페이지의 내용과 모양을 제어하는 기술.

제4절

IPv6 네트워크 연동

1. 내부 네트워크 연동

내부 네트워크 연동이란 공공기관의 내부 장비간에 서로 동작되는 것을 의미한다. 공공기관의 자체적인 연동은 [그림 3.12]의 ① 경로로 표시된 내부 LAN 구간의 연동뿐만 아니라 ② 경로로 표시된 지리적으로 떨어진 상·하위기관간 WAN 구간에서의 연동까지 확인하여야 한다.



【 그림 3.12 내부 네트워크 연동 시험 구성도 】

내부 네트워크를 연동 시험하기 위해서는 2개의 연동점검용 PC가 필요하며, 이 PC에는 IPv6를 지원하는 OS가 설치되어야 하고, IPv6 Ping Test 및 Traceroute를 실행할 수 있어야 한다. 연동 테스트를 하기 위해서는 공공기관의 네트워크 구성도를 참고로 시험하게 될 접속 점을 파악한다.

IPv6를 적용하는 공공기관 내부의 라우터 및 스위치에 연결된 2대의 컴퓨터를 통해 내부 연동에 대한 점검을 실시한다. 목적지가 되는 컴퓨터는 테스트를 한 후에 다른 라우터 및 스위치에 연결([그림 3.12]상의 A지점→B지점으로 PC의 위치를 변경)하거나 산하기관의 PC(C지점과의 연동)와 연결하여 동일한 점검을 반복하면 된다. 내부의 연동을 점검할 때 2대의 PC는 동일한 라우터 및 스위치에 연결하지 않도록 한다.

윈도우즈비스타 OS가 설치된 PC를 이용하여 내부 네트워크의 경로에 IPv6 적용이 제대로 되었는지 확인하는 방법²⁶⁾을 [표 3.20]에 나타내었다.

【 표 3.20 연동테스트 절차 및 명령어 】

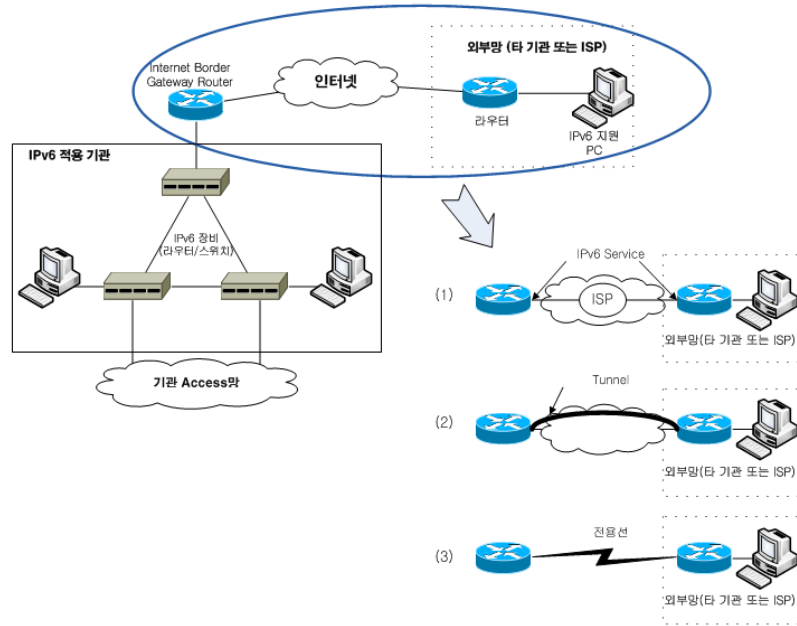
단계	테스트 절차	명령어
IPv6 구성정보 확인	1. 테스트용 PC의 IPv6 구성정보를 확인	ipconfig /all net interface ipv6 show address
IPv6 연결 테스트	2. IPv6 Ping 테스트	ping -6 <목적지 PC의 IPv6 주소> stop (10회 정도 테스트 후)
전송 확인	3. Traceroute를 실행	tracert -d -R -6 <목적지 PC의 IPv6 주소> 또는 pathping -d -6 <목적지 PC의 IPv6 주소>
테스트 종료	4. PC의 위치를 변경 (내부 : A, B, C / 외부 : D)	-
	5. 1~7번 테스트 반복(모든 코어장비에 PC를 연결하여 테스트 진행)	1~6번항 명령어 반복

2. 외부 네트워크 연동

외부 네트워크 연동은 IPv6를 적용한 타 기관과 서로 동작되는 것을 의미하며, [그림 3.13]에 표시된 경로에서의 연동을 확인한다.

공공기관과 외부 네트워크 연동은 인터넷 구간과의 연동으로 아래 [그림 3.13]처럼 세 가지의 방법이 있다. 첫 번째 방법은 상용 ISP에 의한 IPv6 서비스를 이용하는 방법인데, 현재 IPv6 서비스를 제공하는 ISP가 적으므로 구성이 어렵다. 두 번째 방법은 터널을 이용하여 한국인터넷진흥원이 제공하는 IPv6 연동망을 이용하는 방법이다.

26) “Demonstration Plan to Support Agency IPv6 Compliance, 2008.2.28 CIO”



【 그림 3.13 외부 네트워크와 연결 방법 】

현재 ISP가 IPv6 접속서비스를 제공하지 않는다면 한국인터넷진흥원에서 운영 중인 6KANet에 터널링을 이용하는 방식이 가장 좋다. 6KANet은 IPv6를 적용하고 IPv6 접속 서비스를 원하는 기관에 제공되는 무료 서비스이다.

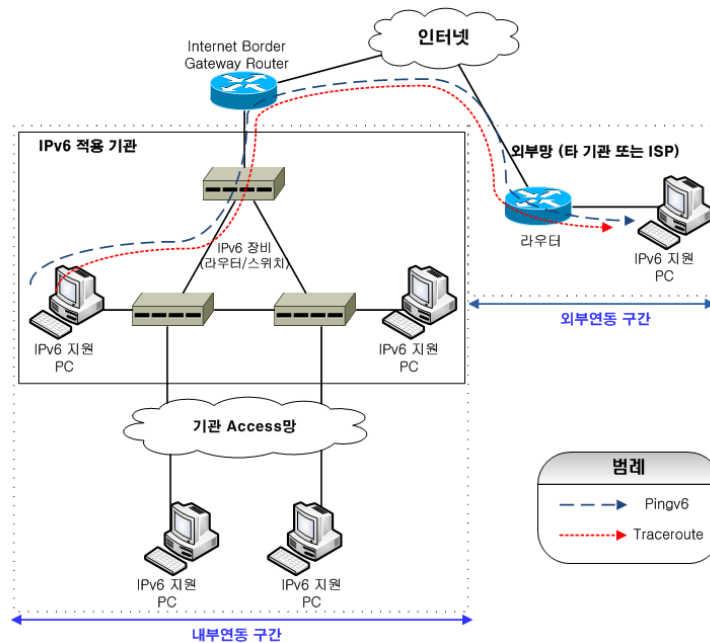
IPv6 연동망인 6KANet을 이용하기 위해서는 IPv6 연동망 가입신청서와 IPv6 연동망에 가입하고자 하는 기관이 이용 계획을 작성하여 온라인으로 한국인터넷진흥원에 신청하면 된다. [그림 3.14]는 IPv6 연동망 가입신청 양식²⁷⁾을 제공하고 있는 한국인터넷진흥원의 IPv6 포털 홈페이지 화면이다.

27) 참고 링크 (http://www.vsix.net/ipv6intro/ipv6Introduction/6ngx_01.jsp)



【 그림 3.14 IPv6 포털 홈페이지 화면 】

연동이 완료되면 정상적인 작동의 유무를 확인하기 위하여 연동을 점검하는데, 연동을 점검하는 방법은 [그림 3.15]처럼 테스트 경로가 달라진 것을 제외하고는 앞에서 설명한 점검 방법과 동일하다. 외부 네트워크 연동은 타 기관과의 협력을 얻어 점검을 진행한다.



【 그림 3.15 외부 네트워크 연동 시험 구성도 】

제4장

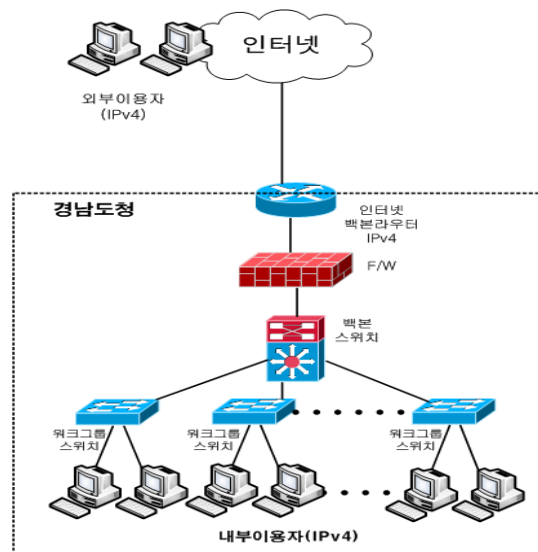
공공기관 IPv6 적용 사례 : 경상남도청

본 적용사례는 ‘2008년 공공부문 IPv6 전환 확산 사업’의 일환으로 한국인터넷진흥원이 2008년 6월~11월에 추진한 ‘공공기관 IPv6 장비 지원사업’ 대상기관 중 경상남도청의 사례를 본 안내서의 IPv6 적용절차에 따라 정리한 것이다. 이 사업에서 한국인터넷진흥원은 공공기관에 IPv6 장비인 라우터 및 스위치 등의 장비 구매를 지원하고, 해당 공공기관은 IPv6를 적용하고 IPv6 서비스를 구축하였다.

제1절

IPv6 적용 대상 조사

경상남도청에서 IPv6를 적용하기 전의 네트워크 구성도는 [그림 4.1]과 같다. IPv6를 적용함으로써 생기는 기존 네트워크의 문제점 발생 가능성을 최소화하기 위하여 IPv4 네트워크와는 별도로 IPv6 네트워크를 구축하는 방안을 선택하였다. IPv6를 적용하기 위해 기존 IPv4 네트워크의 구성요소에 변경해야 할 사항이 없으므로 기존의 IT자원과 응용서비스에 대한 현황 조사 및 네트워크 구성도에 각 장비에 대한 지원 여부를 표시하는 지원 상태도는 작성하지 않았다.



【 그림 4.1 IPv6 적용 전 네트워크 구성도 】

IPv6 네트워크를 구축하기 위한 신규 장비는 [표 4.1]에 정리하였다.

【 표 4.1 IPv6 구축 소요장비 목록 】

구분	제조사	모델명	수 량	장비 용도
IPv6 백본라우터	Alcatel	OS9800	1식	IPv6 연동망과의 연동
IPv6 백본스위치	Alcatel	OS9600	1식	IPv6 내부 백본 스위치
IPv6 방화벽	Checkpoint	UTM-1 3070	1식	IPv6 네트워크 방화벽
웹서버, DNS서버	SUN	SUN X4150	1식	IPv6 DNS 구성
웹하드 스토리지	SUN	SUN 2540	1식	IPv6 서비스 구성

제2절

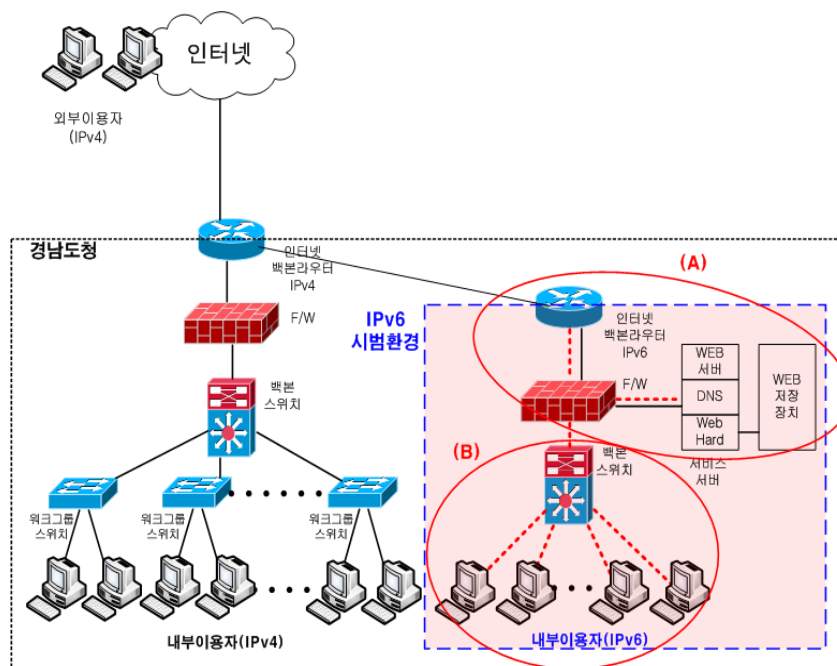
IPv6 적용 시 고려사항

1. 계획 수립 시 고려사항

1.1 적용 범위 설정

경상남도청은 경상도청의 대표 홈페이지 및 경남관광시스템, DNSv6, IPv6 소개 홈페이지, 웹하드 등과 같은 외부 서비스에 IPv6를 적용하여 외부 이용자와 내부 이용자(해당 기관)가 이용할 수 있도록 적용 범위를 설정하였다.

아래 [그림 4.2]처럼 외부 서비스의 적용 범위(A)에 해당하는 외부 서비스와 관련된 네트워크와, 일반 이용자의 구간 사이에 포함되는 제공 서비스, 방화벽 및 백본라우터에 IPv6를 적용하였다. 또한 내부 이용자의 범위(B)에 해당하는 내부 이용자와 관련된 네트워크인 이용단말과 백본 스위치에 IPv6를 적용하였다.



【 그림 4.2 IPv6 적용 범위 설정 】

1.2 IPv6 주소 할당·관리

신규로 도입하는 장비와 이용자 단말의 주소를 아래 [표 4.2]처럼 할당하여 IPv4 주소와 IPv6 주소를 이용하여 IPv6가 적용된 서비스를 이용할 수 있도록 하였다.

【 표 4.2 장비별 주소할당 】

장비별	위치	IP 주소 할당단위		혼용 여부	비 고
		IPv4	IPv6		
Pv6 백본라우터	외부	/30	-	IPv4	6to4 Tunnel
	내부	/30	/64	Dual Stack	-
IPv6 백본스위치	외부	/30	/64	Dual Stack	-
	내부	/26	/64	Dual Stack	-
IPv6 방화벽	외부	/30	/64	Dual Stack	-
	내부	/30	/64	Dual Stack	-
	DMZ	/27	/64	Dual Stack	-
웹서버, DNS서버	내부	/27	/64	Dual Stack	-
사용자 PC	내부	/26	/64	Dual Stack	자동할당

1.3 네트워크 및 서비스 설계

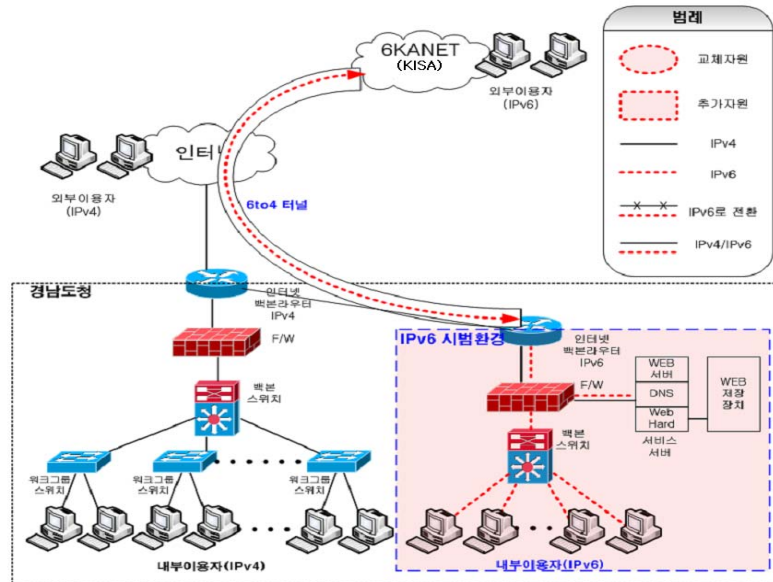
1.3.1 네트워크 설계

경남도청은 [그림 4.3]처럼 기존의 네트워크와는 별도로 내부 이용자 단말, 백본 스위치, 방화벽 및 인터넷 백본 라우터와 서비스를 구현하기 위한 웹서버, DNS서버 및 웹하드 저장장치로 IPv6 네트워크를 구성하여 기존의 인터넷 백본 라우터에 연결하여 기존의 운영 환경과 호환 및 물리·논리적으로 상호 연동될 수 있도록 구성하였다.

신규로 도입하는 장비 가운데 인터넷 백본 라우터는 IPv4/IPv6 듀얼스택을 지원하도록 설정하여 6KANet과 터널링 연동하여 내·외부 트래픽을 처리하도록 하였다. 백본 스위치는 VLAN²⁸⁾ 인터페이스의 IPv6 주소를 이용자 단말의 IPv6 Default Gateway로 설정하여 IPv4와 IPv6네트워크를 동시에 접속하는 환경을 구축하였다. 또한 네트워크 안정성을 보장하기 위해 IPv6 백본라우터 및 백본 스위치의 전원공급장치는 이중으로 구성된 장비를 선정하였다. 방화

28) VLAN(Virtual Local Area Network, 가상 LAN) : 가상적인 기능을 가진 구내 정보 통신망

벽은 IPv6 네트워크를 보호하기 위해 인가되지 않은 IP 및 Port는 차단하고 웹서버를 보호하는 웹방화벽으로 사용하였다. 기관 내부에 있는 IPv6 이용자 단말은 신규 IPv6 스위치에 직접 연결하여 서비스를 이용하도록 구성하였다.



【 그림 4.3 IPv6 적용 후 네트워크 구성도 】

1.3.2 서비스 설계

경상남도청에서는 아래 [표4.3]처럼 IPv6 환경을 제공하기 위해 5단계로 나누어 추진 목표를 설정하고 서비스 구축을 위한 설계하였다.

【 표 4.3 단계별 추진 목표 】

1단계	2단계	3단계	4단계	5단계
DNS 서버 구성	웹서버 IPv6 지원 환경 구성	이용자 단말에 대한 IPv6 지원 환경 구축	IPv6 서비스 연동 테스트	대민 IPv6 서비스 지원

우선 응용서비스에 IPv6를 적용하기 위해서 신규로 도입한 서버의 OS인 솔라리스 버전의 확인(버전 10)을 통하여 IPv6 지원이 가능하다는 것을 확인하고, IPv6 DNS를 구축하기 위해 호스트에 IPv6 주소를 등록하고, 게이트웨이의 활성화 및 BIND버전(BIND 9)을 업그레이드하

여 DNS와 관련된 파일이 IPv6를 지원할 수 있게 하였다.

웹서버는 HTTP서비스에 대한 업그레이드 및 기존의 웹서비스 데이터에 대한 링크 작업을 하여 IPv6 웹서비스를 제공할 수 있도록 구축하였다.

IPv6를 적용하여 신규로 대민 서비스를 제공하기 위해 IPv6를 홍보하는 웹서버와 웹하드 솔루션을 구축하였다. IPv6에 대한 홍보용 웹 서버는 IPv6를 기반으로 한 서비스의 활성화 및 기술을 보급하기 위하여 구축하는 것이고, IPv6를 접속하는 방법 및 IPv6가 가지고 있는 기술적 특성 등에 대한 정보를 제공한다. IPv6 기반 웹하드 솔루션은 IPv6 서비스의 활용을 유도하기 위해 구축하며, 내부의 이용자가 1차적으로 사용할 수 있도록 유도하여 자료 공유 및 협업을 수행할 수 있는 서비스로 제공하며, 2차적으로는 IPv6를 홍보하는 웹서버와 연동하여 대민 서비스의 형태로 웹하드 서비스를 일반 이용자에게 제공하도록 한다.

1.4 원상복구 계획

기존의 IPv4 네트워크와는 독립적으로 IPv6 네트워크를 구축하기 때문에 문제가 발생했을 때 이를 대처하는 것이 용이하지만, IPv6 네트워크 내부에서 사전 검증을 충분하게 행한 후에 IPv4 네트워크와 연동할 수 있도록 한다. 연동했을 때 문제가 발생하면 IPv4 네트워크와 IPv6 네트워크를 분리하여 문제점이 발생하기 이전의 네트워크 구조로 되돌릴 수 있다.

문제점이 발생할 가능성을 줄이기 위해서 서비스를 개시하기 이전에 실시한 테스트 결과와 공인기관에서 성능을 검증한 자료를 활용하도록 한다.

1.5 보안적합성 검증

방화벽을 신규로 도입하기 위해서 경상남도청에서는 해당하는 제품에 대한 CC인증의 여부를 확인하여 도입 대상의 장비로 선정하였다. 국가정보원에 문의하여 선정한 제품에 대한 보안적합성의 검증을 의뢰하였다. 보안적합성을 검증하기 위해 작성한 신청서는 아래에 예시로 나타내었다.

보안적합성 검증 신청서									
신청 기관	기 관 명	경상남도			운용부서	정보통계 담당관실			
	도입목적	경상남도 IPv6 시범망 운영							
	운용환경	사용자 수	1,000여명		망 구성	<input checked="" type="checkbox"/> 유선 <input type="checkbox"/> 무선			
		속도(대역폭)	1Gbps						
	운용형태	<input checked="" type="checkbox"/> 단독설치.운용 <input type="checkbox"/> 타 보안제품과 연동 <input type="checkbox"/> 대 국민 배포용							
	연 동 시 스템	<input type="checkbox"/> ERP <input type="checkbox"/> KMS <input type="checkbox"/> CRM <input type="checkbox"/> 전자결재 <input type="checkbox"/> 기타 그룹웨어							
신청제품	사 업 명	경상남도 IPv6 시범환경 구축사업							
	업 체 명	체크포인트			대 표 자	조현제			
	주 소	서울 영등포구 여의도동 주택건설회관 6층			전화번호	02-782-6533			
	제 품 명	UTM-1 3070			CC 인증번호	CCEVS-VR- 06-0033			
					암 호 검증번호				
					용역개발 여 부	<input type="checkbox"/> 예 <input checked="" type="checkbox"/> 아니오			
	평가기관	National Information Assurance Partnership	인증기관	NSA		등급	EAL4		
	담 당 자	전화번호							
휴대폰번호									
E-mail									
암호모듈 <input checked="" type="checkbox"/> 없음 <input type="checkbox"/> 있음(<input type="checkbox"/> 검증 <input type="checkbox"/> 미검증)									

2. IT 자원 도입 시 고려사항

라우터·스위치·방화벽 등 네트워크를 구성하는 장비는 하드웨어를 기반으로 IPv6 트래픽을 처리하는 장비를 선정하여, 서비스 트래픽을 빠르고 안정적으로 처리할 수 있도록 한다. 또한 IPv4와 IPv6 트래픽을 처리하는데 있어 동일한 성능을 보장하는 장비를 선정하여 구축한다.

도입되는 라우터·스위치·방화벽은 IPv6 네트워크를 구축하기 위한 용도의 장비이므로 국내에서 실제로 IPv6 네트워크를 구축하고 나아가 그에 대한 운영 실적을 보유한 장비를 우선

적으로 선정하여 사업을 안정적으로 수행할 수 있도록 하였으며, 기존의 IPv4네트워크에서 사용하는 Routing Protocol, Multicast 등을 지원하여 네트워크를 운영했을 때의 연속성을 보장하도록 고려하였다. 또한 도입하는 장비는 기본적으로 IPv6 Ready 장비를 도입할 수 있도록 우선적으로 고려하였으며 보안적합성에 대한 검증을 하기 위해 방화벽은 CC인증을 획득한 제품을 선정하였다.

IPv6 네트워크를 구축하기 위한 장비를 선정할 때 고려해야 할 사항을 [표 4.4]에 정리하였다.

【 표 4.4 IPv6 장비 선정 시 고려사항 】

장비 구분	선정 시 고려사항
백본라우터, 스위치	<ul style="list-style-type: none"> o 안정성 <ul style="list-style-type: none"> - IPv6 Ready Logo 획득 여부 - H/W 방식 처리 여부 - 이중화 구성 여부 - 업그레이드의 편리성(재부팅 필요 없음)
	<ul style="list-style-type: none"> o 보안성 <ul style="list-style-type: none"> - 다양한 보안 기능(사용자 인증, VLAN, 암호화, 스위치 액세스 인증, NAT, 서비스 보호 거절 기능 등)
	<ul style="list-style-type: none"> o 서비스 기능 <ul style="list-style-type: none"> - 지능성, 유선 속도 지원 보장, L2/L3/L4 스위치 용도별 기능 제공, 우선 순위 지정 등
	<ul style="list-style-type: none"> o 관리 기능 <ul style="list-style-type: none"> - QoS 우선 순위 제공, 장비 자동 구성 및 설정 등
방화벽	<ul style="list-style-type: none"> o 레퍼런스 사이트 구축, 운영 실적 및 시장 점유율 o 검증된 보안 기능 제공 (CC 인증 여부) o 관리의 편리성

2.1 도입 장비의 세부 규격

앞에서 서술한 여러 가지 고려사항들을 반영하여 경상남도청이 선정한 장비의 규격을 아래에 나타내었다.

2.1.1 백본라우터

구 분	세부 내용
규 격	<ul style="list-style-type: none"> o 16개 이상의 I/O 슬롯을 지원하는 새시형 o Hot Swap지원 o 1.5 Tbps 이상 Non-Blocking Switch Fabric제공 o 1,200 Mpps 이상 forwarding속도 제공 o 1000BaseSX/LX/LH 384 ports 이상 지원 o 10Gbps 96 ports 이상 지원 o 주요 부품 이중화 제공 <ul style="list-style-type: none"> - Main Engine, Switching Fabric, Power Supply o Hardware Based IPv4, IPv6 트래픽 처리 지원 o IPv4/IPv6 라우팅 기능 지원(RIP, OSPF, BGP 등)
OS 및 버전	6.3.1.999.R01 Service Release, August 18, 2008.,
IPv6패킷 처리방식	H/W기반 패킷 처리(6to4 Tunnel)

2.1.2 백본스위치

구 분	규격 및 내용
규 격	<ul style="list-style-type: none"> o 4개 슬롯 이상을 지원하는 새시형 o Hot Swap지원 o 400Gbps 이상 Non-Blocking Switch Fabric제공 o 286Mpps 이상 forwarding속도 제공 o 1000BaseSX/LX/LH 96 ports 이상 지원 o 10Gbps 16 ports 이상 지원 o 주요 부품 이중화 제공(Power Supply) o Hardware Based IPv4, IPv6 트래픽 처리 지원 o IPv4/IPv6 라우팅 기능 지원(RIP, OSPF, BGP 등)
OS 및 버전	6.3.1.999.R01 Service Release, August 18, 2008.
IPv6패킷 처리방식	H/W기반 패킷 처리(6to4 Tunnel)

2.1.3 방화벽

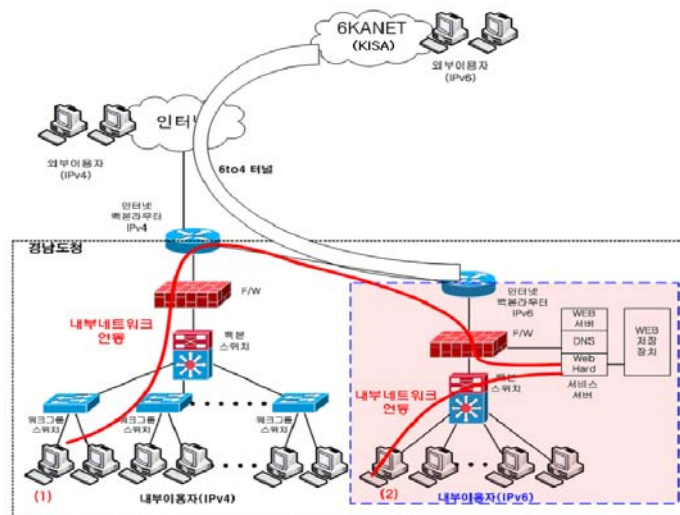
구 분	규격 및 내용
규 격	<ul style="list-style-type: none"> o Hardware 일체형 보안 전용 장비 o 최대 10포트 이상의 인터페이스 지원 o 4.5Gbps 이상의 Firewall Throughput 지원 o 1.1Gbps 이상의 VPN Throughput 지원(AES128) o 2Gbps 이상의 IPS 성능 지원 o Concurrent Session 최대 110만 이상 지원 o Stateful Inspection 방식의 IPv4 및 IPv6 지원 방화벽 o Admin 접속 채널에 암호화 및 PKI 인증 방식을 지원 o SSL VPN, Anti Virus, Anti Spyware, SPAM 필터 기능 제공 o Active/Active Load Sharing, Session Fail-Over 기능 지원 o 국제 CC(Common Criteria) EAL4 이상 등급 o FIPS 140-2인증, ICESA(Firewall, VPN)인증
OS 및 버전	CheckPoint SecurePlatform 3.0
IPv6패킷 처리방식	Dual Stack

제3절

IPv6 네트워크 연동

1. 내부 네트워크 연동

경상남도청에서 실시한 내부 네트워크의 연동 테스트는 아래 [그림 4.4]처럼 기존의 IPv4 이용자 및 신규 IPv6 이용자가 IPv6 기반의 서비스를 정상적으로 이용할 수 있는지 확인한다.



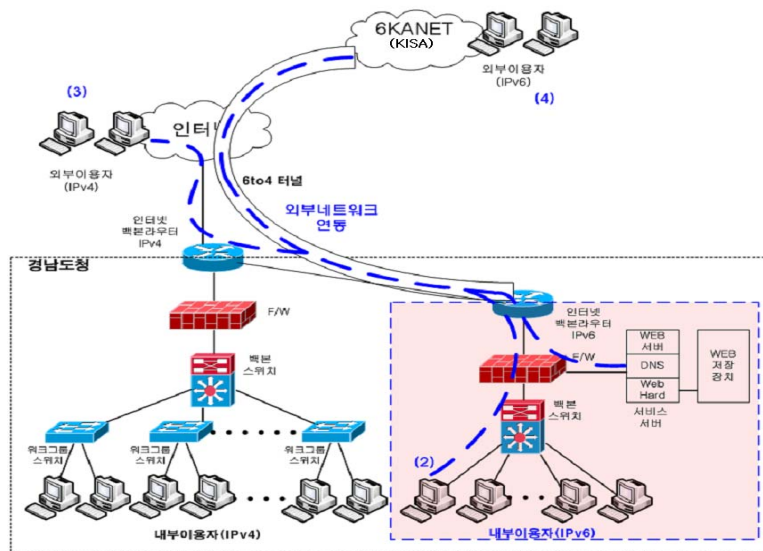
【 그림 4.4 내부 네트워크 연동 경로 】

기존 IPv4 네트워크에 포함되는 내부 이용자(1)는 기존 IPv4 네트워크에서 IPv6 백본라우터를 거쳐 신규 IPv6용 홈페이지 및 웹하드로 IPv4 접속하도록 구성되어 있다. 신규로 구축되는 IPv6 네트워크에 포함되는 내부 사용자(2)는 신규 IPv6용 백본 스위치를 통해 방화벽을 거쳐 신규 IPv6용 홈페이지 및 웹하드로 IPv6 접속하도록 구성되어 있다.

IPv6로 구축된 서비스를 이용할 수 있는지에 대한 가능 여부를 확인하고, 기관 내부에서 서비스가 정상적으로 제공되는지를 확인하였다.

2. 외부 네트워크(6KANet) 연동

이용자 단말이 외부 IPv6 서비스에 접속하거나 외부 이용자가 대민 서비스(웹 서버 등)를 IPv6로 접속할 수 있도록 외부 네트워크와의 연동은, 아래 [그림 4.5]처럼 기본적으로 6KANet과 경남도청간에 Tunnel을 이용한 IPv6연동을 수행한 후, IPv6 주소에 대한 라우팅 정보는 Static Routing Protocol을 이용하여 구성하였다.



【 그림 4.5 외부 네트워크 연동 경로】

경상남도청의 외부 IPv4 사용자(3) 및 외부 IPv6 사용자(4)는 기존 IPv4 네트워크를 통해 터널링을 구성하여 신규 IPv6용 홈페이지 및 웹하드로 접속할 수 있도록 구성되어 있다.

외부 네트워크와의 연동 상태를 확인하기 위해서 IPv6 네트워크에 포함되는 내부 이용자(2)에서 외부 이용자(3)로의 이메일을 확인하거나 또는 외부 IPv6 네트워크에서 웹사이트를 접속하여 IPv6 연동 상태를 확인하였다.

IPv6에 대한 대외홍보, 관련자료의 제공 및 대용량 파일을 저장할 수 있는 기능을 가진 웹하드 서비스를 제공하고 있는 IPv6 기반의 경상남도청의 홈페이지(<http://www.gsndv6.net/>)를 외부 이용자가 접속한 화면을 아래 [그림 4.6]에 나타내었다. 또한 홈페이지에서 제공되는 IPv6 스타트팩을 이용한 설치 방법을 예시화면과 함께 제공하여 이용자가 단말의 IPv6 활성화를 손쉽게 할 수 있도록 하고 있다.



【 그림 4.6 경상남도청 홈페이지 접속 화면 】

부록1 | 참고 자료

- 1 "Demonstration Plan to Support Agency IPv6 Compliance", M|CIO, 2008.2.28.
- 2 "IPv6 Transition Guidance", M|CIO, 2006.02.
- 3 "2007 IPv6 동향에 관한 연구", 한국정보사회진흥원, 2007.12.
- 4 "IPv6 보급 촉진 기본계획 II", 정보통신부, 2006.12
- 5 "정보시스템 운영관리 지침(TTAS.KO-10.0118/R1)", TTA, 2007.12.26.
- 6 "IPv6 환경의 보안 위협 및 공격 분석", 전자통신동향분석 22권, 2007.02
- 7 "IPv6 운영 보안가이드-IPv6 라우터편", 한국정보보호진흥원, 2006.1.
- 8 "국방분야 차세대 인터넷주소체계(IPv6) 전환 방안", 국방정책연구
2006 겨울 - 홍진기, 최인수, 임재혁
- 9 "IPv6 주소 할당 지침서(TTAS.OT-10.0029)", TTA, 2005.12.21
- 10 "IPv6보안기술해설서", 한국정보보호진흥원, 2005.10
- 11 IPv6 강좌, 온더넷, 2005
- 12 "부산시청에 IPv6 도입방안 및 비용산정", 한국전산원, 2004.12
- 13 "공공기관을 위한 IPv6 도입 전략 수립 지침서", 한국전산원, 2004.12.
- 14 "분야별 IPv6 이행 모델-KOREAv6 시범사업 수행결과", 한국전산원, 2004.12
- 15 "공공기관 IPv6 도입모델 및 전략에 관한 연구", 한국전산원, 2003.10
- 16 "IPv4IPv6 전환 실무자 지침서(프로그래밍,전환기술,방화벽)", 한국전산원
- 17 IPv6 Ready Logo 홈페이지, <http://www.ipv6ready.org/frames.html>
- 18 IT보안인증사무국 홈페이지, www.kecs.go.kr
- 19 한국인터넷진흥원 IPv6 포털홈페이지, <http://www.vsix.kr>
- 20 한국정보통신기술협회, <http://www.tta.or.kr>

부록2

약어표

AS	[Autonomous System, 자율 시스템]
AP	[Access Point]
BcN	[Broadband Convergence Network, 광대역 통합망]
BIND	[Berkeley Internet Name Domain, 버클리 인터넷 이름 도메인]
CNGI	[China Next Generation Internet]
DBMS	[Data Base Management System, 데이터베이스 관리 시스템]
DHCP	[Dynamic Host Configuration Protocol, 동적 호스트 설정 통신 규약]
DNS	[Domain Name Server, 도메인 네임 서버]
DSTM	[Dual Stack Transition Mechanism]
IANA	[Internet Assigned Number Authority, 인터넷 할당 번호 관리 기관]
IDS	[Intrusion Detection System, 침입 탐지 시스템]
IETF	[Internet Engineering Task Force, 인터넷 엔지니어링 태스크 포스]
IPS	[Intrusion Prevention System, 침입 방지 시스템]
ISP	[Internet Service Provider, 인터넷 서비스 제공자]
JSP	[Java Server Page, 자바 서버 페이지]
KOREN	[KORea advanced REsearch Network, 광대역통합연구개발망]
NAT	[Network Address Translation]
NIR	[National Internet Registry, 국가 인터넷 레지스트리]
RR	[Resource Record, 리소스 레코드]
RIR	[Regional Internet Registry, 대륙별 인터넷 레지스트리]
TTA	[Telecommunication Technology Association, 한국정보통신기술협회]
UCC	[User Created Contents, 사용자 제작 콘텐츠]
VPN	[Virtual Private Network, 가상 사설 통신망]
WAN	[Wide Area Network, 광역 통신망]
WiBro	[Wireless Broadband, 와이브로]
6KANet	[IPv6 Korea Advanced Network, 차세대인터넷 가입자망]

1. 업그레이드를 통한 Dual Stack 지원 장비

1.1 스위치

1.1.1 주니퍼 (<http://www.juniper.net>)

구분	L3 스위치	
모델명	EX3200	EX4200
Dual Stack 지원방식	S/W 업그레이드(IPv6 Licence 추가)	S/W 업그레이드(IPv6 Licence 추가)
비용	유료	유료
OS	Junos 9.3	Junos 9.3
메모리(GB)	512MB	1GB
인터페이스 (포트수 및 속도)	24포트 10/100/1000MB 48포트 10/100/1000MB	24포트 10/100/1000MB 48포트 10/100/1000MB
Switching 수용량(Gbs)	24포트 : 88Gbps 48포트 136Gbps	24포트 : 88Gbps 48포트 136Gbps
처리량(Gbs)	24포트 : 65Mpps 48포트 : 101Mpps	24포트 : 65Mpps 48포트 : 101Mpps

1.1.2 LG-Nortel (<http://www.nortel.com>)

구분	L4/L7 스위치				L3 스위치
모델명	NAS3408E (NAS3408)	NAS2424E (NAS2424)	NAS2216E (NAS2216)	NAS2208E (NAS2208)	ERS8600
Dual Stack 지원방식	SW 업그레이드	SW 업그레이드	SW 업그레이드	SW 업그레이드	모듈 추가
비용	무료	무료	무료	무료	유료
OS	AOS23.2 이상	AOS23.2 이상	AOS23.2 이상	AOS23.2 이상	v4.1 이상
메모리(GB)	1.2GB	1.2GB	1.2GB	1.2GB	768MB
인터페이스 (포트수 및 속도)	10/100/1000BASE-TX : 4	10/100BASE-TX : 24	10/100BASE-TX : 16	10/100BASE-TX : 8	Chassis type 3/6/10 Slot chassis
	1000BASE-X-SFP : 8	1000BASE-X-SFP : 4	1000BASE-X-SFP : 2	1000BASE-X-SFP : 2	
Switching 수용량(Gbs)	16Gbps	16Gbps	16Gbps	16Gbps	720Gbps
처리량(Gbs)	51K CPS	51K CPS	30K CPS	15K CPS	400Mpps
Client Session	4M session (2M Session)	4M session (2M Session)	2M session (1M Session)	1.2M session (600K Session)	L3 장비의 경우 해당 사항 없음

1.1.3 알카텔 루슨트 (<http://www.alcatel-lucent.com>)

구분	L3 스위치		
모델명	OS9800/9700/9600	OS6850-24x/48x	OS6400-24/48
Dual Stack 지원방식	자체 지원 (H/W 기반 IPv6지원)	자체 지원 (H/W 기반 IPv6지원)	자체 지원 (H/W 기반 IPv6지원)
비용	무료	무료	무료
OS	6.3.1.999.R01	6.3.1.999.R01	6.3.3.999.R01
메모리(GB)	DRAM : 256MB Flash : 128MB	DRAM : 256MB Flash : 64MB	DRAM : 256MB Flash : 128MB
인터페이스 (포트수 및 속도)	1G fiber: 384/192/95 1G UTP : 384/192/95 10G fiber 96/48/24	10G fiber: 2 and, 1G UTP : 24/48 1G fiber: 4 Combo 지원	1G fiber: 4 1G UTP : 24/48 Combo 지원
Switching 수용량(Gbs)	1.92Ybps/960Gbps /4790Gbps	128Gbps/224Gbps	192Gbps/96Gbps
처리량(Gbs)	1.92Ybps/960Gbps /4790Gbps	128Gbps/224Gbps	192Gbps/96Gbps

1.2 IP-PBX

1.2.1 어바이어 (<http://www.avaya.com>)

구분	IP-PBX & VoIP		
모델명	S8710 Server	S8720 Server	CM 1x - 5.1
Dual Stack 지원방식	H/W 업그레이드 (서버 메모리추가)	H/W 업그레이드 (서버 메모리/모듈추가)	S/W 업그레이드 (Call Manger 프로그램 업그레이드)
비용	유료	유료	유료
세부규격	IPv6 Addressing, Neighbor Discovery, Path MTU discovery, re-direct, DHCPv6, DNSv6	IPv6 Addressing, Neighbor Discovery, Path MTU discovery, re-direct, DHCPv6, DNSv6	IPv6 Addressing, Neighbor Discovery, Path MTU discovery, re-direct, DHCPv6, DNSv6
특이사항	메모리 추가시 서버 셋다운 필요	메모리 추가시 서버 셋다운 필요	-
링크주소	http://www.avaya.com/gcm/master-usa/en-us/products/offers/s8710_media_server01.htm	http://www.avaya.com/gcm/master-usa/en-us/products/offers/s8720_media_server.htm	http://www.avaya.com/gcm/master-usa/en-us/products/offers/communication_manager.htm

1.2.2 LG-Nortel (<http://www.nortel.com>)

구분	IP-PBX	
모델명	Meridian 61C, 81C	
Dual Stack 지원방식	H/W 업그레이드 (Signal Proxy server by COTS) & S/W 업그레이드 (Linux Kernel, NRS, ECM 등)	
비용	유료	
세부 규격	IPv6 Addressing, Neighbor Discovery, Path MTU discovery, re-direct, DHCPv6, DNSv6	
특이사항	Proxy Server를 통해 지원	

2. Dual Stack 지원 장비

2.1 라우터

2.1.1 시스코 (<http://www.cisco.com>)

모델명	CRS-1 series	12000 series	10000 series	7600 series	ASR 1000 series	7300 series	7200 series	3800 series	3200 series	2800 series	1800 series	870 series
IPv4/IPv6 처리방법	H/W	H/W	H/W	H/W	S/W	S/W	S/W	S/W	S/W	S/W	S/W	S/W
OS	IOS-XR	IOS-XR, IOS	IOS	IOS	IOS-XE	IOS	IOS	IOS	IOS	IOS	IOS	IOS
처리량(Mbps)	1.2Tbps	1.2Tbps	51Gbps	720Gbps	10Gbps	4Gbps	1.8Gbps	256Mbps	90Mbps	112.64Mbps	38.4Mbps	12.8Mbps
메모리(GB)	4GB	4GB	4GB	4GB	4GB	2GB	1GB	1GB	256MB	1GB	128MB	256MB
WAN 인터페이스 (포트수 및 속도)	4포트 OC-768 POS SPA	2포트 OC-192 POS LineCard	1포트 OC-48 POS LineCard	1포트 OC-192 POS SPA	1포트 OC-12 POS SPA	1포트 OC-48 POS LineCard	2포트 OC-3 POS PA	1포트 OC-3 ATM NM	4포트 Serial SMIC	1포트 T3 Serial NM	2포트 T1 Serial WIC	1포트 FE
LAN 인터페이스	1포트 10GE SPA	1포트 10GE SPA	1포트 1GE LineCard	16포트 10GE LineCard	1포트 10GE SPA	2포트 GE SPA	1포트 GE PA	1포트 GE NM	4포트 FE FESMIC	1포트 GE HWIC	1포트 FE HWIC	4포트 FE
라우팅 프로토콜	BGP, OSPF 등	BGP, OSPF 등	BGP, OSPF 등	BGP, OSPF 등	BGP, OSPF 등	BGP, OSPF 등	BGP, OSPF 등	BGP, OSPF 등	BGP, OSPF 등	BGP, OSPF 등	BGP, OSPF 등	BGP, OSPF 등
링크주소	www.cisco.com/go/crs	www.cisco.com/go/12000	www.cisco.com/go/10000	www.cisco.com/go/7600	www.cisco.com/go/asr1000	www.cisco.com/go/7300	www.cisco.com/go/7200	www.cisco.com/go/3800	www.cisco.com/go/3200	www.cisco.com/go/2800	www.cisco.com/go/1800	www.cisco.com/go/870

2.1.2 주니퍼 (<http://www.juniper.net>)

모델명	M7i	M10i	M40e	M120	M320	T320	T640	T1600	J2350	J4350	J6350	MX240	MX480	MX960
Dual Stack 지원방식	S/W	S/W	S/W	S/W	S/W	S/W	S/W	S/W	S/W	S/W	S/W	S/W	S/W	S/W
OS	Junos 5.1이상	Junos 5.1이상	Junos 5.1이상	Junos 5.1이상	Junos 5.1이상	Junos 5.1이상	Junos 5.1이상	Junos 5.1이상	Junos 8.5이상	Junos 8.5이상	Junos 8.5이상	Junos 5.1이상	Junos 5.1이상	Junos 5.1이상
처리량(Mbps)	6.4Gbps	12.8Gbps	40Gbps	120Gbps	320Gbps	320Gbps	640Gbps	1.6Tbps	750Mbps	1.6Gbps	2Gbps	240Gbps	480Gbps	960Gbps
메모리(GB)	1.5GB	1.5GB	2GB	4GB	4GB	4GB	4GB	4GB	1GB	2GB	2GB	4GB	4GB	4GB
WAN 인터페이스 (포트수및속도)	4포트 OC-12	8포트 OC-12	8포트 OC-48	2포트 OC-192	10포트 OC-192	10포트 OC-192	8포트 OC-768	16포트 OC-768	10포트E1 10포트T1	6포트E3 6포트T3	6포트E3 6포트T3	지원 않함	지원 않함	지원 않함
LAN 인터페이스	4포트 1Gbps	8포트 1Gbps	16포트 1Gbps	2포트 10Gbps	10포트 10Gbps	10포트 10Gbps	32포트 10Gbps	32포트 10Gbps	4포트 1Gbps	6포트 1Gbps	8포트 1Gbps	120포트 1Gbps 12포트 10Gbps	240포트 1Gbps 24포트 10Gbps	440포트 1Gbps 44포트 10Gbps
라우팅 프로토콜	BGP, OSPF 등	BGP, OSPF 등	BGP, OSPF 등	BGP, OSPF 등	BGP, OSPF 등	BGP, OSPF 등	BGP, OSPF 등	BGP, OSPF 등	BGP, OSPF 등	BGP, OSPF 등	BGP, OSPF 등	BGP, OSPF 등	BGP, OSPF 등	BGP, OSPF 등
링크주소	http://www.juniper.net/techpubs/hardware								http://www.juniper.net/techpubs/software/series			http://www.juniper.net/techpubs/hardware		

2.3 IP-PBX

2.3.1 LG-Nortel (<http://www.nortel.com>)

모델명	iPECS-CM	CS1000
IPv4/IPv6 처리방법	H/W & S/W	H/W & S/W
주요 기능	Max 30,000 ports, BHCC : 400,000, 지역적 이중화 지원(Local Survivability), 콜서버 및 Media Gateway의 전환은 기본적으로 AC 및 DC 선택적 이중화 기능	Call Server, Media Gateway, Signaling & Proxy Server

2.3.2 어바이어 (<http://www.avaya.com>)

모델명	S8730 Server	S8510 Server	G650 Gateway	G450 Gateway	96xx IP Phone	CM 5.x or later
지원방식	H/W	H/W	H/W	H/W	H/W	S/W
주요 기능	Max user : 36000, Max trunk : 8000, Max Gateway : 250	Max user : 2400, Max trunk : 800, Max Gateway : 250	IPv6 Addressing, Neighbor Discovery, Path MTU discovery, re-direct, DHCPv6, DNSv6	IPv6 Addressing, Neighbor Discovery, Path MTU discovery, re-direct, DHCPv6, DNSv6	IPv6 Addressing, Neighbor Discovery, Path MTU discovery, re-direct, DHCPv6, DNSv6	IPv6 Addressing, Neighbor Discovery, Path MTU discovery, re-direct, DHCPv6, DNSv6
링크주소	http://www.avaya.com/gcm/master-usa/en-us/products/offers/s8730_server.htm	http://www.avaya.com/gcm/master-usa/en-us/products/offers/s8510_server.htm	http://www.avaya.com/gcm/master-usa/en-us/products/offers/g650_media_gateway01.htm	http://www.avaya.com/gcm/master-usa/en-us/products/offers/g450_media_gateway.htm	http://www.avaya.com/gcm/master-usa/en-us/products/offers/9610_ip_telephone.htm	http://www.avaya.com/gcm/master-usa/en-us/products/offers/communication_manager.htm

2.3.3 제너시스템즈 (<http://www.xener.com>)

모델명	XIP G3
IPv4/IPv6 처리방법	HW & SW
주요 기능	<p>순수 Software 기반의 호 처리 시스템</p> <p>VoIP 프로토콜 : SIP (RFC3261)</p> <p>비디오 호 처리 지원, 화상회의 및 Video Phone 지원</p> <p>UC 메신저, XML, 화상회의 서비스 제공</p> <p>CAC (Call Admission Control)</p> <p>NAT Traversal</p> <p>Web GUI 기반으로 관리 Tool 지원</p> <p>MoH, Call Transfer, Call Forward, Call Park, Call Pick up, Conference Call 등 Web portal 모듈 탑재</p> <p>이중화 모듈 탑재</p> <p>UC 확장/통합 플랫폼 연동 지원</p> <p>본지사 구조 및 다중 사업장 지원 기능 탑재</p>

2.4 방화벽

2.4.1 시스코 (<http://www.cisco.com>)

모델명	FWSM Module	ASA 5500
IPv4/IPv6 처리방법	SW	SW
OS	자체 전용 OS	자체 전용 OS
메인메모리(Gbps)	-	12GByte
세션 처리율	1M 동시커넥션	2M 동시커넥션
방화벽 성능	5.5Gbps	10Gbps
인터페이스	16포트 10GE Module	4* 10/100/1000, 4* GE fiber, SR, LC, 2*10GE fiber, SR, LC
링크주소	www.cisco.com/go/fwsm	www.cisco.com/go/asa

2.4.2 주니퍼 (<http://www.juniper.net>)

모델명	SSG 5	SSG 20	SSG 140	SSG 320M	SSG 350M	SSG 520M	SSG 550M
OS	ScreenOS 6.1	ScreenOS 6.1	ScreenOS 6.1	ScreenOS 6.1	ScreenOS 6.1	ScreenOS 6.1	ScreenOS 6.1
메인메모리(Gbps)	128/256Mb	128/256Mb	256/512Mb	256M/1G	256M/1G	1G	1G
세션 처리율 (최대/초당)	16,000/2,800	16,000/2,800	48,000/8000	64,000/10000	96,000/12500	128,000/10000	256,000/15000
방화벽 성능	160 Mbps	160 Mbps	350 Mbps	450 Mbps	550 Mbps	650 Mbps	1 Gbps
인터페이스	7개 (10/100)	5개 (10/100) 2개 (추가slot)	8개 (10/100) 2개 (10/100/1000) 4개 (추가slot)	4개 (10/100/1000) 3개 (추가slot)	4개 (10/100/1000) 5개 (추가slot)	4개 (10/100/1000) 6개 (추가slot)	4개 (10/100/1000) 6개 (추가slot)
주요 기능	wireless(별도장비) IPSecVPN UTM(licence)	wireless(별도장비) IPSecVPN UTM(licence)	IPSecVPN UTM(licence)	IPSecVPN UTM(licence)	IPSecVPN UTM(licence)	IPSecVPN UTM(licence)	IPSecVPN UTM(licence)
링크 주소	http://www.juniper.net/products_and_services/firewall_slash_ipsec_vpn/ssg_5_slash_ssg_20/index.html		http://www.juniper.net/products_and_services/firewall_slash_ipsec_vpn/ssg_140/index.html	http://www.juniper.net/products_and_services/firewall_slash_ipsec_vpn/ssg_300_series/index.html	http://www.juniper.net/products_and_services/firewall_slash_ipsec_vpn/ssg_500_series/index.html		

모델명	ISG 1000	ISG 2000	NS 5200	NS 5400	SRX 5600	SRX 5800
OS	ScreenOS 6.1	ScreenOS 6.1	ScreenOS 6.1	ScreenOS 6.1	Junos 9.2R2	Junos 9.2R2
메인메모리(Gbps)	1/2G	1/2G	MGT1 : 1G SPM8G : 512M SPM24FE :	256M	RE: 2G	RE: 2G
세션 처리율 (최대/초당)	500,000/20,000	1,000,000/23,000	1,000,000/26,500	2,000,000/26,500	4,000,000/350,000	4,000,000/350,000
방화벽 성능	2 Gbps	4 Gbps	10 Gbps	30 Gbps	60 Gbps	120 Gbps
인터페이스	4개 (10/100/1000) 2개 (추가slot)	4개 (추가slot)	2개 (추가slot)	4개 (추가slot)	5개 (IOC:IOC당 40x1G or 4x10G)	11개 (IOC:IOC당 40x1Gor4x10G)
주요 기능	IPSecVPN IPS기능(울선) UTM(licence)	IPSecVPN IPS기능(울선) UTM(licence)	IPSecVPN UTM(licence)	IPSecVPN UTM(licence)	IDP기능 (기본사항)	IDP기능 (기본사항)
링크 주소	http://www.juniper.net/products_and_services/firewall_slash_ipsec_ipsec_vpn/isg_series_slash_gprs/index.html			http://www.juniper.net/products_and_services/firewall_slash_ipsec_vpn/netscreen_5200_slash_netscreen_5400/index.html		

2.4.3 체크포인트 (<http://www.checkpoint.com>)

모델명	Power-1	UTM-1	CheckPoint FireWall-1 / VPN-1
IPv4/IPv6 처리방법	H/W	H/W	S/W
OS	자체 전용 OS, Secure Platform	자체 전용 OS, Secure Platform	Open 플랫폼(윈도우, 솔라리스, (S/W) 리눅스, IPSO 외)
메인메모리(Gbps)	2 ~ 4 G	1 ~ 4 G	Open 플랫폼으로 H/W를 선택하여 적용함
세션 처리율	100만이상	100만이상	
방화벽 성능	9G ~ 14G	400M ~ 4G	
인터페이스	10~18개 (10/100/1000)	4~8개 (10/100/1000)	-

2.5 VPN

2.4.1 넥스지 (<http://www.nexg.net>)

모델명	VForce-860	VForce-1200	VForce-1400	VForce-1700	VForce-2200	VForce-2400	VForce-3200	VForce-3400	VForce-5200	VForce-5400
OS	VOS 3	VOS 3	VOS 4	VOS 3	VOS 3	VOS 4	VOS 3	VOS 4	VOS 3	VOS 4
CPU	RISC	RISC	Network Services Processor	VIA C3 1.2Ghz	Intel Celeron D P4 2.8Ghz	Network Services Processor (Multi-Core)	Intel Xeon 3.6Ghz	Network Services Processor (Multi-Core) OS	Intel Xeon 3.6Ghz Dual	Network Services Processor (Multi-Core)
Memory	64MB	128MB	512MB	256MB	1GB	1GB	512MB	4GB	4GB	8GB
NIC	2(Copper)	4(Copper)	3(Copper)	5(Copper)	6(Copper)	8(Copper)	8(Fiber4, Copper 4)	8(Fiber 4, Copper 4)	8(Fiber 4, Copper 4)	8(Fiber 4, Copper 4)
Switch Ports	4	4	6	-	-	4	-	-	-	-

공공기관 IPv6 적용 안내서

2010년 3월 인쇄
2010년 3월 발행

발행처: 한국인터넷진흥원

서울특별시 송파구 가락동 79-3번지
대동빌딩 한국인터넷진흥원
Tel: (02) 405-5118

인쇄처: OO
Tel: (02) 000-0000

<비매품>

- 본 안내서 내용의 무단 전재를 금하며, 가공·인용할 때에는 반드시 방송통신위원회·한국인터넷진흥원 『공공기관 IPv6 적용 안내서』라고 출처를 밝혀야 합니다.



이 책을 볼 수 있는 독자는?



업무관계자
초급

업무관계자
중급

업무관계자
고급

한국인터넷진흥원

138-950 서울시 송파구 가락동 79-3번지 대동빌딩

Tel. 405-5118 Fax. 405-5119

www.kisa.or.kr