

분야별 차세대인터넷주소 IPv6 실전적용

- 요약본 -

CONTENTS

PORTAL

WEB



CHAPTER 01 소개

01 제작배경 및 목적	07
02 대상 및 범위	09

CHAPTER 02 IPv6 적용을 위한 고려사항

01 개요	10
02 서비스별 고려사항	11
2.1 망 사업자	11
2.2 서비스 제공자 및 비즈니스 이용자	12
2.3 제품 제조사	13
03 이해관계자별 고려사항	13

CHAPTER 03 관련 제품 동향

15



CHAPTER 04 시나리오에 따른 IPv6 서비스 제공방안

01 시나리오 개요 및 제약조건	16
02 IPv6 적용 시나리오	17
03 점검 리스트	22
04 테스트결과에 따른 IPv6 적용 시 점검사항	23
4.1 개인 가입자 OS 측면	23
4.2 어플리케이션 측면	24
4.3 웹사이트 이용측면	24
4.4 고객택내장비(CPE) 및 전용단말 측면	24
4.5 IP공유기 사용 측면	25
4.6 Layer2 스위치 측면	26
4.7 무선망 측면	26
4.8 서버 관리 측면	27
4.9 서버 OS 측면	27
4.10 서비스 측면	27
4.11 L4 스위치 측면	28
4.12 ActiveX 측면	28
4.13 웹인트라넷 보안 툴 IPv6 지원	28
4.14 DHCP 운영 측면	28
4.15 보안측면	29

CHAPTER 05 결론 30



〈유의사항〉

본 책자의 사용에는 제한이 없으나 다음과 같은 사항에 유의해야 한다.

○ 본 책자는 2010년 6월 시점에서 국내 시장에 출시되는 국내외 제품 및 표준기술들을 대상으로 작성되었으므로 특정 기능의 지원/미지원 여부, 시험과정에서의 이슈 사항, 혹은 표준기술들의 변동 여부 등은 독자가 본 안내서를 읽는 시점에서 기술된 내용과 다를 수 있다.

○ 책자내에 언급된 상표 제품명 등에 대한 권리는 각 상표 또는 제품을 소유한 해당기업에 있으며 설명을 위하여 특정 회사제품명 또는 화면이 표시된 경우 IPv6 적용기술에 대한 이해를 높이고자 하는 목적외에 다른 목적은 없음을 밝힌다.

○ 본 책자의 내용을 기관이나 개인이 실제 적용시에는 반드시 자체적인 시험을 통해 안정성을 검증한 뒤 시행해야 하며, 이를 지키지 않고 발생하는 문제에 대해서는 한국인터넷진흥원은 책임이 없음을 밝힌다.

※ 본 책자의 내용중 오류가 발견되었거나 내용에 대한 의견이 있을 때에는 한국인터넷진흥원(v6webmaster@kisa.or.kr)으로 해당 내용을 보내주시기 바랍니다.

제1장 소개



1. 제작배경 및 목적

현행 인터넷주소인 IPv4 주소는 2011년 2월경 전 세계적으로 할당이 중지될 것으로 예정되어 앞으로는 IPv6 주소가 전분야로 확산될 전망이다. 최근 유무선 통합서비스 제공, 스마트 폰 보급 확산 등에 따른 무선인터넷서비스 활성화로 인해 인터넷주소(IP) 수요가 급증하고 있고 중국, 인도, 브라질 등 신흥 개발국들의 인터넷 이용이 급증하면서 전 세계적으로 IP 주소 수요가 폭증한 결과다.

IPv4 주소의 할당이 중지된 이후에는 IPv6 주소만 받는 주체들이 점차 늘어갈 것이다. 정부에서 지난 10년간 다양한 IPv6 인식제고 활동을 해 온 결과 IPv6에 대한 인식은 어느 정도 형성이 되어 있으나 분야별로 기술환경이 달라 실제 적용 시 무엇을 어떻게 바꿔야 하고, 어떤 알려진 이슈가 있는지, 적용 절차 및 다른 분야 이해관계자들과의 고려사항 등 체계적으로 종합된 자료가 부족한 실정이다.

ISP, 이동통신사 등 ‘망사업자’의 경우 일반이용자 및 기업고객을 대상으로 인터넷 접속 서비스를 제공하면서 다른 망들과 연동을 통해 국내 인터넷 백본망을 형성하고 있다. 현재는 IPv6로 접속할 서비스가 없고, NAT 기술을 활용해 사설 IPv4 주소로 당분간 IPv4 주소를 나누어 쓸 수 있다는 이유로 IPv6 적용을 미루고 있으나 IPTV, VoIP 등 고품질의 서비스를 유지하고 망을 단순화, 효율화 시키며 서비스 제공자, 비즈니스 이용자 등의 요구에 선제적으로 대응하기 위해 IPv6의 도입이 필요하다.

콘텐츠 제공자(CP), 포털 등 ‘서비스 제공자’들은 네트워크 인프라위에서 다양한 콘텐츠를 생



산, 유통시키고 있는 주체들로 규모와 사업형태에 따라 망 사업자의 고객으로, 또는 독자적인 네트워크를 보유하는 형태로 사업을 운영하고 있다.

단순히 현재의 고객대응 차원에서는 서비스 제공자의 고객들은 망사업자의 최종고객들이므로 망 사업자의 IPv6 적용 추이를 지켜보면서 향후 대응하겠다는 반응이 일반적이다. 하지만 신규 서비스 대응 및 비즈니스 확장 차원에서는 이보다 좀 더 서두를 필요가 있다.

일반기업, 공공기관 등 ‘비즈니스 이용자’는 외부고객을 대상으로 웹서비스 등을 제공하면서 동시에 내부 이용자의 업무를 위한 네트워크를 운영하는 2가지 성격을 모두 가지고 있다. 일반적으로 비즈니스 영위를 위한 인터넷 이용관점에서 내부 이용자들의 업무 서비스에 좀 더 초점이 맞춰져 있다.

다른 이해관계자들이 특정 영역에 집중할 수 있는 반면, 비즈니스 이용자는 네트워크부터 어플리케이션까지 넓은 범위를 관리하고 있다. 따라서 IPv6 적용과 관련해서는 고려할 사항도 많지만, 반면 한정된 내부영역을 대상으로 단기간에 대규모의 내부 이용자들에게 IPv6를 전개할 수 있다는 장점도 있다. 비즈니스 이용자의 IPv6 적용은 초기에는 외부고객의 요구보다는 비즈니스의 확장을 염두에 둔 조직 내부 경쟁력 강화 차원에서 먼저 추진될 것으로 예상된다.

라우터, 스위치 등 네트워크 장비 제조사, 방화벽, 백신 등 보안제품 제조사, 기타 소프트웨어 개발사 등 ‘제품 제조사’는 시장의 수요에 적극 대응하면서 패키지 제품 혹은 수요기관의 개발요구에 맞춰 제품을 개발, 판매하고 있다. 이들 제품 제조사들은 IP통신 제품을 개발할 때 IPv6를 고려해야 하는데, 시장에 IPv6 제품이 다양화 되 있어야 비용 효율적인 IPv6 적용이 가능하고 관련 기술의 보편화에도 기여를 하기 때문이다.

IPv4 신규 할당중지 이후에는 누구도 더 이상 새로운 IPv4 주소를 할당 받을 수 없다. 이 시기 이후 새롭게 시장에 참여하는 포털이나 기타 기업들은 IPv6 주소만 받으므로 새로운 비즈니스 파트너들과 협력을 위해서는 IPv6를 고려해야 한다. IPv6를 적용하지 않으면 조직 내부 네트워크 확장이 어려워지고 IPv6 주소만 받은 새로운 비즈니스 파트너들과 협력에도 제한이 생긴다. 동시에 망 사업자도 서서히 IPv6 고객을 유치하고 IPv6 망과 연동을 늘려가게 되면 서비스제공자 역시 고객으로부터 IPv6 요구에 직면하게 될것이다. 시간이 갈수록 IPv6 주소만 받는 주체들이 늘어갈 것은 자명하다.

따라서 본 책자는 IPv4 신규 할당이 중지되는 2011년 이후 IPv6 Only 고객 및 서비스가 곧 출



현할 수 있다는 상황을 가정하고 작성하였다. 이런 상황에서 이해관계자별 발생 가능한 시나리오별 IPv6 도입방안을 마련하고, 실제 테스트를 통해 IPv6 도입을 위해 점검할 사항과 예상되는 이슈를 분석하였다. 본 책자는 다양한 형태로 등장할 수 있는 IPv6 도입 시나리오를 이해하고 상황에 맞게 안정적으로 IPv6를 도입할 수 있도록 관련 정보를 제공함으로써 IPv6 적용 초기에 시행착오를 최소화 할 수 있을 것을 기대한다.

2. 대상 및 범위

본 책자는 망 사업자(ISP), 서비스 제공자(포털, CP 등), 비즈니스 이용자(기업, 공공기관), 제품 제조사를 대상으로 시나리오에 따른 IPv6 도입방안을 제시하며, 관련 장비의 기술적 성숙도, 잠재적 위험, 시장의 요구 등을 종합적으로 검토해 점진적, 체계적으로 IPv6 적용을 위한 추진 방안을 제시한다.



제2장

IPv6 적용을 위한 고려사항



1. 개요

망 사업자, 서비스 제공자, 비즈니스 이용자 및 제품제조사들의 IPv6 적용 핵심 목표는 다음과 같다.

- ✓ IPv4와 동일한 수준의 보안과 운영관리(management)가 가능
- ✓ 기존 IPv4 서비스의 안정성에 영향을 주지 않는 서비스 구축
- ✓ IPv4와 IPv6 사이의 원활한 상호 연동

목표달성을 위한 첫 단계는 현재 운영중인 망의 종류, 망을 구성하는 장비현황을 면밀히 파악하는 것이며, 세부적으로 다음과 같다.

- ✓ Layer 2¹⁾ 이상의 장비에서 IP와 관련된 '기능' (보안기능, 관리용 원격접속, SNMP, 로드밸런싱 등)에서의 IPv6 지원여부
- ✓ Layer 3이상의 장비의 경우 IPv6 주소 입력가능 여부 및 라우팅 지원여부
- ✓ 방화벽, 유해트래픽 탐지/차단 등 보안장비의 경우 IPv6 주소 라우팅 이외에 보안기능 제공 여부
- ✓ 서버의 IPv6 지원 운영체제 지원여부(Windows, 리눅스, FreeBSD 등)
- ✓ 호스팅 서비스 관련 어플리케이션 IPv6 지원여부 (Windows의 DNS, IIS의 Web 또는 FTP 등)
- ✓ 일반적으로 많이 쓰이는 결제, I-PIN 인증, 광고와 같은 서비스를 제공하는 업체에서도 IPv6를 지원하는지 여부를 확인

1) 일반적으로 Layer 3 이상의 장비에만 IP이슈가 있다고 인식할 수 있으나, 실제로 IP 라우팅과 관련없는 Layer 2 스위치에서도 Multicast Snoop 등 Filter기능을 사용한다면 IP주소와 관련된 테이블을 스위치에서 처리해야 하므로 IPv6 주소 지원여부를 확인해야 한다.



2. 서비스별 고려사항

2.1 망 사업자

구분	종류	주요 점검사항	IPv6자원장비 출시여부
백본망	라우터 (L3)	- IPv6 주소 입력가능 - IPv6 라우팅 기능 - SNMP 등 관리 기능 - 보안관련 기능 - MPLS 6PE 기능 - IPv6 Multicast 기능 - IPv6 Qos 기능	출시
가입자망	라우터/스위치(L3)	- IPv6 주소 입력가능 - IPv6 라우팅 기능 - SNMP 등 관리 기능 - 보안관련 기능	출시
	스위치 (L2)	Multicast, DHCP, 인증 등 L2 이외 부가기능 사용 시 확인 필요	개발중
	VoIP교환기(SSW)	- IPv6 주소 입력가능 - SIP, H.323 Protocol 처리기능 - 보안관련 기능	개발중
	VoIP교환기 (IP-PBX)	- IPv6 주소 입력 가능 - NAT 및 DHCP 기능 - SIP, H.323 Protocol 처리기능 - 보안관련 기능	개발중
	3G망 데이터통신 (GGSN/SGSN)	- IPv6 주소 입력 가능 - SGSN과 GGSN간 IPv6 통신 - WCDMA 무선단말에 IPv6 자동 주소 할당 - GGSN과 유선망 통신시 IPv6 통신	개발중
고객	모뎀 등	- DHCP 등 L2 이외 부가기능 사용 시 확인필요 - DOCSIS3.0 이상 지원	출시
	셋톱박스	- IPv6 주소 입력 기능 - IPv6 Multicast 기능 - IPv6 Qos 기능 - 관리 기능	개발중
	PC	윈도 XP 이상	출시

※' 10.6월 현재 기준이며 최신 정보는 <http://vsix.kr>에서 확인 가능



2.2 서비스 제공자 및 비즈니스 이용자

구분	종류	주요 점검사항	IPv6 지원장비 출시 여부 ('10.6현재)
서비스망 가입자망 고객	방화벽	- IPv6 주소 입력 기능 - IPv6 라우팅 기능 - SNMP 등 관리 기능 - 보안관련 기능	출시
	L4	- IPv6 주소 입력기능 - IPv6 라우팅 기능 - SNMP 등 관리기능 - 보안관련 기능 - 로드밸런싱 기능	출시
	WEB /DNS	- IPv6 주소 입력 기능 - 미들웨어별 IPv6 기능 - IPv6의 HTTP Listen 기능 - DNS 플랫폼 기능 - DNSv6 Query 처리 - NFSv6 기능 - NTPv6 기능 - SSH 등 보안 기능 - NMS등 관리 기능 - FTP 기능 - 도메인 등록 대행자의 IPv6 도메인 등록 지원	출시
	MAIL	- IPv6 주소 입력 기능 - 플랫폼 IPv6 기능 - SMTPv6, POPv6 기능 - MAIL 도메인과 DNS 연동 기능 - EML, HTML, RFC822, S/MIME 기능 - SSH 등 보안기능 - 관리기능	출시
	DHCP	- IPv6 주소 입력 기능 - DHCPv6 Option별 처리 기능 - IPv6 Pool 할당 기능 - SSH 등 보안기능 - 관리기능	출시
	VoIP	- 음성(RTP) 데이터 처리 기능 - SSH 등 보안기능 - 관리기능 - IPv6 주소 입력 기능	출시
	VPN	- IPv6 주소 입력 기능 - IPv6 라우팅 기능 - SNMP 등 관리 기능 - 보안관련 기능 6VPN 기능	출시



구분	종류	주요 점검사항	IPv6지원장비 출시 여부 ('10.6현재)
서비스망 가입자망 고객	NMS	• IPv6 주소 입력 기능 • IPv6 모니터링 관리기능 • SNMPv6 MIB 처리기능 • WEB BASE GUI 기능 • SSH 등 보안기능	출시
	VOD	• IPv6 주소 입력 기능 • DNP For VoD 기능 • SSH 등 보안 기능 • Streaming For VoD 기능 • NMS 등 관리기능	출시

※ '10.6월 현재 기준이며 최신 정보는 <http://vsix.kr>에서 확인가능

2.3 제품 제조사

제품 제조사는 제품 구현시 RFC 문서 등 인터넷기술 표준문서에 기반하여 상기 망 사업자, 서비스 제공자 및 비즈니스 이용자의 주요 고려사항들을 개발해야 한다.

또한 장비의 신뢰성 확보를 위해 IPv6 Ready Logo, TTA verified 및 CC 인증 등 다양한 인증 체계 획득을 검토할 필요가 있다. IPv6 인증체계의 경우 IPv6기반 네트워크 · 통신장비가 표준적 합성에 맞게 정확하게 구현되었는지 검증하기 위한 프로그램으로 구성되어 있다.

3. 이해관계자별 고려사항

네트워크는 서로 다른 주체들간의 상호연동이므로 자신의 분야외에 네트워크에 연결된 다른 주체들과의 점검사항을 검토해야 한다.



망 사업자 입장에서 분야별 점검할 사항		
서비스 제공자	비즈니스 이용자	일반 이용자
- 회선고객의 요구 여부 - 가입자단 장비의 지원여부 - DNSv6 가능여부 - SNMP 관리 기능 가능여부 - IPS,IDS 보안 기능, 응용계층 서비스 지원여부	- 회선고객의 요구 여부 - 가입자단 장비의 지원여부 - DNSv6 가능여부 - SNMP 관리 기능 가능여부 - Managed 서비스의 경우 IPS,IDS 보안 기능, 응용계층 서비스 지원여부 6VPN 기능 지원여부	- 고객 OS 현황 (Windows, Mac, Linux 별 지원여부 확인) - DHCPv6 기능 가능여부 - DNSv6 가능여부 - 가입자망 지원여부

서비스 제공자 입장에서 분야별 점검할 사항		
망 사업자	비즈니스 이용자	일반 이용자
- IPv6 접속/연동 제공여부 - DNSv6 지원 여부 등	응용계층 서비스 지원여부	- 고객 OS 현황 (Windows, Mac, Linux 별 지원여부 확인) - DNSv6 가능여부 - 가입자망 지원여부 확인

비즈니스 이용자 입장에서 분야별 점검할 사항		
망 사업자	서비스 제공자	일반 이용자
- IPv6 접속/연동 제공여부 - DNSv6 가능여부 - Managed 서비스의 경우 IPS, IDS 보안 기능, 응용계층 서비스 지원여부 - IPv6 VPN 지원 여부	응용계층 서비스 지원여부	- 고객 OS 현황 (Windows, Mac, Linux 별 지원여부 확인) - DNSv6 가능여부 - 가입자망 지원여부



제3장

관련 제품 동향



현재 사업자들이 많이 사용하고 있는 시스코, 주니퍼, 3Com, 히다찌 등의 주요 장비들, MS Windows, Sun의 Solaris, FreeBSD 그리고 Linux 등의 소프트웨어에서 IPv6를 대부분 지원하고 있으며 최근 새롭게 출시되는 제품들 중심으로 대부분 IPv6를 지원하고 있다.

현재 기본적인 라우팅 기능과 기존 터널 기능 등은 큰 이슈가 없으나 최근 표준화된 6RD, DS-LITE와 같은 터널 기술들은 아직 구현되지 않은 장비들이 많다. 그밖에 L4 ~ L7 장비, VoIP(Soft Switch, IP-PBX, IP폰), 방화벽 등 보안 장비들도 조금씩 국내 제조사에서 IPv6 지원 장비를 출시하고 있다. L4/L7 장비들은 IPv6 기반 이중화 지원, 라우팅과, IPv6 환경에서의 다양한 Protocol 별 식별, SLB(Server Load Balancing), FWLB(FireWall Load Balancing) 등을 지원하고 있다.

VoIP 관련 장비 중 현재 IPv6 기반 소프트스위치는 국내 기업인 제너시스시스템즈, 아크로메이트 등이 개발 중이며, IP PBX, 게이트웨이는 애드팩테크놀러지, 모임스톤, 컨피닉스 등이 일부 제품을 출시하였거나 개발 중에 있다.

보안장비들은 2000년초부터 외산 방화벽 위주로 IPv6 지원제품이 출시되어 오다가 최근에는 제품군들이 통합보안제품(방화벽+IPS+유해트래픽 방지 등)으로 진화하면서 IPv6 기능도 탑재한 국내외 제품들이 다수 출시되고 있다. 현재 체크포인트, 퓨처 시스템, 포티넷, 안철수 연구소 등 장비 제조사들은 기존 IPv4에서 제공한 기능을 IPv6에서 대부분 지원이 되도록 개발 했다. IPv6 지원 보안장비 출시는 최근 1~2년 사이 증가하고 있으나 공공부문에서 필요한 TTA verified 인증 혹은 국정원의 CC인증 획득은 시작단계에 있다.

PC용 백신, 개인방화벽 등 인트라넷 보안솔루션들도 IPv6 지원 제품이 부족한 실정이다. 시만텍, 안철수연구소 등에서 제품이 있으나 IPv6가 부분지원되고 있다.



제4장

시나리오에 따른 IPv6 서비스 제공방안



1. 시나리오 개요 및 제약조건

IPv6 주소만 갖는 주체가 등장한다는 가정에서 가능한 모든 시나리오를 도출하기 위해 아래와 같이 세부 시나리오를 3가지로 분류하였다. IPv6 주체의 등장과 수용 관점에서 4가지 조합을 기본으로 하여 3가지 연동 시나리오와 다시 조합해 망 사업자의 대표 서비스별로 테스트베드를 구성하고 IPv6 적용 방안들과 이슈를 살펴보았다.

등장 시나리오	수용 시나리오	연동 시나리오
■ IPv4 주소 부족으로 신규 가입자에게 IPv6주소를 할당하는 경우 ■ 기존고객(IPv4 Only)이 IPv6 서비스 이용을 요청하는 경우	■ 최소비용/시간을 투입해 IPv6 Only 이용자를 수용하는 경우 ■ 대규모의 IPv6 Only 이용자를 수용 가능한 망을 구축한 경우	■ IPv4 Only와 연동 ■ IPv4 IPv6와 연동 ■ IPv6 Only와 연동

테스트 베드 구성은 서비스 제공과 이용 관점에서 단대단(end-to-end) 연결을 3개 영역으로 나누고 IPv4/IPv6 듀얼스택 상황을 최대한 배제함으로써, 망 사업자의 서비스별로 다음과 같이

	가입자망	백본망	서비스망
6-4-4	IPv6	IPv4	IPv4
6-4-6	IPv6	IPv4	IPv6
6-6-4	IPv6	IPv6	IPv4
6-6-6	IPv6	IPv6	IPv6
4-4-6	IPv4	IPv4	IPv6
4-6-6	IPv4	IPv6	IPv6
4-6-4	IPv4	IPv6	IPv4

최대 7가지 조합이 가능했다.

지금까지는 일반적으로 IPv6 전환 시나리오를 기술할 때, 가장 가능성 높은 모델로 IPv4/IPv6 듀얼스택 시나리오를 기본으로 해왔으나, 전환대상이 기존 IPv4 망에 집중되어 안정성에 대한 부담이 크고, 초기상황과 전환단계별로 무수히 많은 세부 시나리오가 도출될 수 있어 실질적인 IPv6 전환에 도움이 되기 어려웠다.

따라서 본 책자는 IPv4 신규 할당중지 이후 발생할 수 있는 IPv6 Only 이용자/서비스 제공자의 출현을 가정하고 최소비용/최단시간/최소변경으로 IPv6를 수용 할 수 있는 시나리오들을 집중적으로 검토했다. 시나리오를 최소 조건으로 단순화함으로써 이해관계자별로 이해도를 높이고 유사 시나리오에 대해서도 쉽게 접근할 수 있도록 구성하였다.

듀얼스택을 최소화했기 때문에 대부분의 시나리오에서 통신을 위해 변환장비(NAT-PT)가 사용되었으나, 현재 망 사업자 규모에서 사용 가능한 상용 장비는 없어, 장비의 처리용량과 관련된 테스트는 수행치 않고, 변환장비의 기본 기능만 활용해 시나리오 검증만 실시하였다.

※ 시나리오 기술시 불가피하게 중복되는 시나리오는 통합/제외하여 기술함

2. IPv6 적용 시나리오

2.1 시나리오1 - 최소규모 신규 IPv6 가입자 확보

IPv4 신규 할당 중지 이후 IPv4 주소 부족으로 인터넷 서비스망에 신규로 수용하는 일반이용자, 기업 또는 공공기관 등의 비즈니스 고객에게 IPv6 주소를 나누어 주는 경우로 실제 IPv6

II 상세 시나리오

	IPv4 주소 부족으로 신규 가입자에게 IPv6 주소를 할당하는 경우	기존고객(IPv4 Only)이 IPv6 서비스 이용을 요청하는 경우
최소비용/시간을 투입해 IPv6 Only 이용자를 수용하는 경우	○	
대규모의 IPv6 Only 이용자를 수용 가능한 망을 구축한 경우		



Only 이용자가 등장하는 초기상황을 가정한다.

연동방법

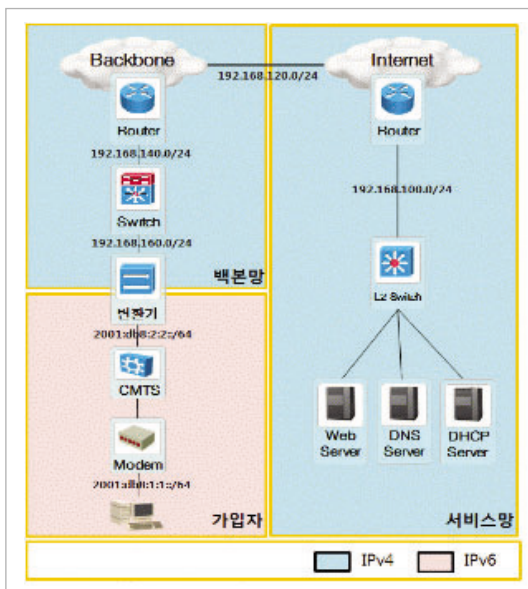
	가입자망	백본망	서비스망
6-4-4	IPv6	IPv4	IPv4
6-4-6	IPv6	IPv4	IPv6
6-6-4	IPv6	IPv6	IPv4

서비스 제공방안

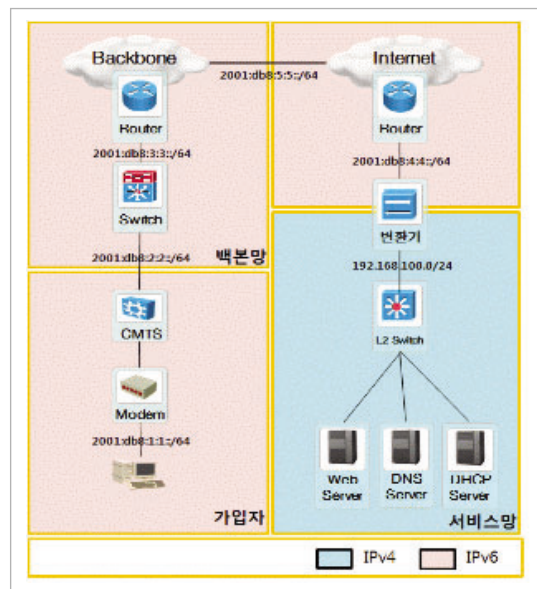
최소비용과 시간에 IPv6 이용자에게 기존 IPv4 콘텐츠를 원활히 사용하게 하기 위해서 콘텐츠 서비스 제공자나 ISP가 프로토콜 변환(IPv6↔IPv4)을 적용한다. 변환장비를 사용하게 되면 서비스 서버들의 추가적인 설정이나 OS의 변경을 하지 않아도 된다.

사내에 IPv6 Only 가입자를 수용하기 위해 상기와 같이 IPv4망과 IPv6 망 사이에 변환장비 구축하거나 처음부터 사내망을 IPv4/IPv6 듀얼스택 망으로 구축하는 방안이 있다.

[그림 4-1] HFC 6-4-4망 Test 구성도



[그림 4-2] HFC 6-6-4망 Test 구성도



2.2 시나리오2 - 최대규모 신규 IPv6 가입자 확보

본 시나리오는 신도시가 건설되는 등 일시에 동일 지역에서 많은 수의 신규 고객이 발생하거나



기존 가입자망에서 IPv6 이용자 수가 점차 증가하여 프로토콜 변환 비용이 상승할 경우 선택할 수 있는 방법이다. 망 구성장비 전체가 모두 IPv6 Only로 구성된 경우이고 서비스단도 IPv6를 지원하므로 시기적으로는 IPv6 Only 이용자가 일반화 되는 시점 이후로 볼 수 있다.

상세 시나리오

	IPv4 주소 부족으로 신규 가입자에게 IPv6 주소를 할당하는 경우	기존 고객(IPv4 Only)이 IPv6 서비스 이용을 요청하는 경우
최소비용/시간을 투입해 IPv6 Only 이용자를 수용하는 경우	○	
대규모의 IPv6 Only 이용자를 수용 가능한 망을 구축한 경우		

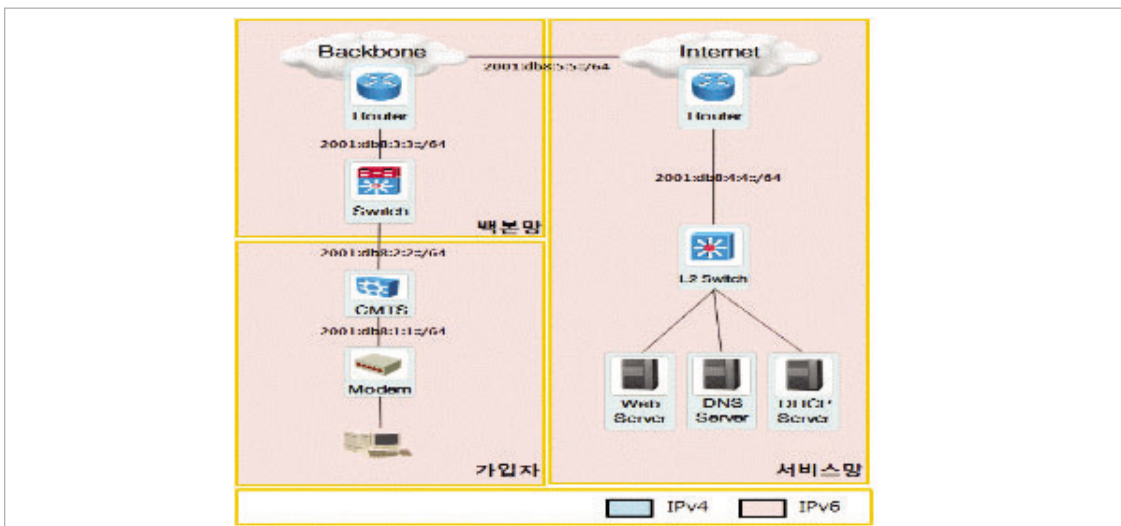
연동방법

	가입자망	백본망	서비스망
6-6-6	IPv6	IPv6	IPv6

서비스 제공방안

IPv6 Only 이용자부터 서비스망까지 종단 간 IPv6 Only 통신이 가능하다. 가입자망은 기존 IPv4 Only 이용자와 함께 겸용체제로 가져 갈수도 있지만, 신규 IPv6 이용자의 지속 증가가 예상된다면 별도 망으로 구축 하는 것도 효율적이다. 백본망은 기존 IPv4 Only 이용자를 감안하여 IPv4/IPv6 겸용 환경으로 구성하는 것이 현실적이다.

[그림 4-3] HFC 6-6-6망 Test 구성도





2.3 시나리오3 - IPv4 고객 대상 최소규모 IPv6 서비스 제공

IPv4 신규 할당 중지 이후 등장하는 포털 및 인터넷 콘텐츠를 제공하는 기업들이 IPv6 주소를 할당 받아 서비스를 제공 할 경우, 망 사업자, 서비스 제공자 등은 전환계획이 없는 ADSL 서비스 등의 기존 IPv4 Only 고객에 대해 고려해야 한다.

상세 시나리오

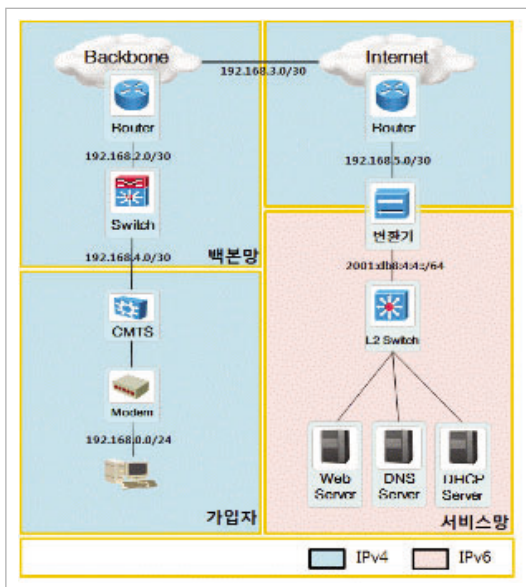
	IPv4 주소 부족으로 신규 가입자에게 IPv6 주소를 할당하는 경우	기존고객(IPv4 Only)이 IPv6 서비스 이용을 요청하는 경우
최소비용/시간을 투입해 IPv6 Only 이용자/서비스를 수용하는 경우		○
대규모의 IPv6 Only 이용자/서비스를 수용 가능한 망을 구축한 경우		

연동방법

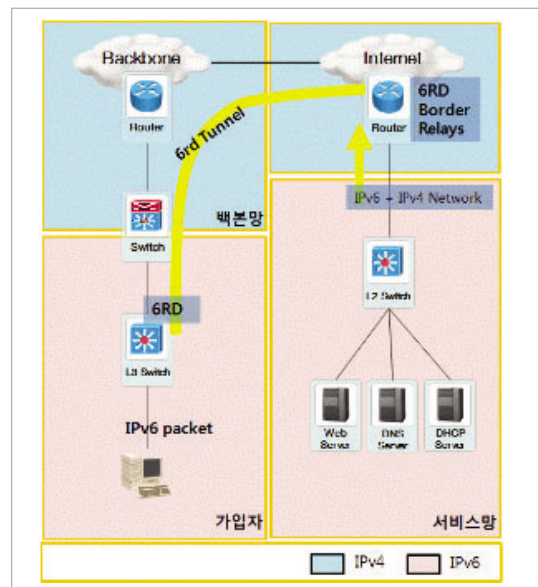
	가입자망	백본망	서비스망
4-4-6	IPv4	IPv4	IPv6
4-6-6	IPv4	IPv6	IPv6
Dualstack	IPv4/IPv6	IPv4/IPv6	IPv4/IPv6

서비스 제공방안

[그림 4-4] HFC 4-4-6망 Test 구성도



[그림 4-5] 6RD (RFC5969) 구성도





가입자망 장비의 교체를 최소화 하고 기존 IPv4 고객에게 외부의 IPv6 서비스를 제공 하기 위해서는 가입자망과 백본망 경계 단에 변환장비를 구성하거나 가입자단에 터널 기술(6RD 등)을 적용하는 방안이 있다.

2.4 시나리오4 - IPv4 고객 대상 최대규모 IPv6 서비스 제공

본 시나리오는 고객의 IPv6 요구가 일반화된 상황으로 IPv6 기반 콘텐츠 서비스가 일반화된 상황을 가정한다. 따라서 기존 가입자망에서 변환기에 의한 프로토콜 변환 비용이 상승하여 ISP들은 변환기 대신 IPv6도입을 검토하게 된다.

기본적으로 '1.2 대규모의 IPv6 Only 이용자를 수용 가능한 망을 구축한 경우'의 시나리오와 동일하나 본 시나리오에서는 기존 IPv4 고객을 고려하므로 IPv4/IPv6 듀얼스택도 고려한다.

상세 시나리오

	IPv4 주소 부족으로 신규 가입자에게 IPv6 주소를 할당하는 경우	기존고객(IPv4 Only)이 IPv6 서비스 이용을 요청하는 경우
최소비용/시간을 투입해 IPv6 Only 이용자/서비스를 수용하는 경우		
대규모의 IPv6 Only 이용자/서비스를 수용 가능한 망을 구축한 경우		○

연동방법

	가입자망	백본망	서비스망
듀얼스택	IPv4/IPv6	IPv4/IPv6	IPv4/IPv6

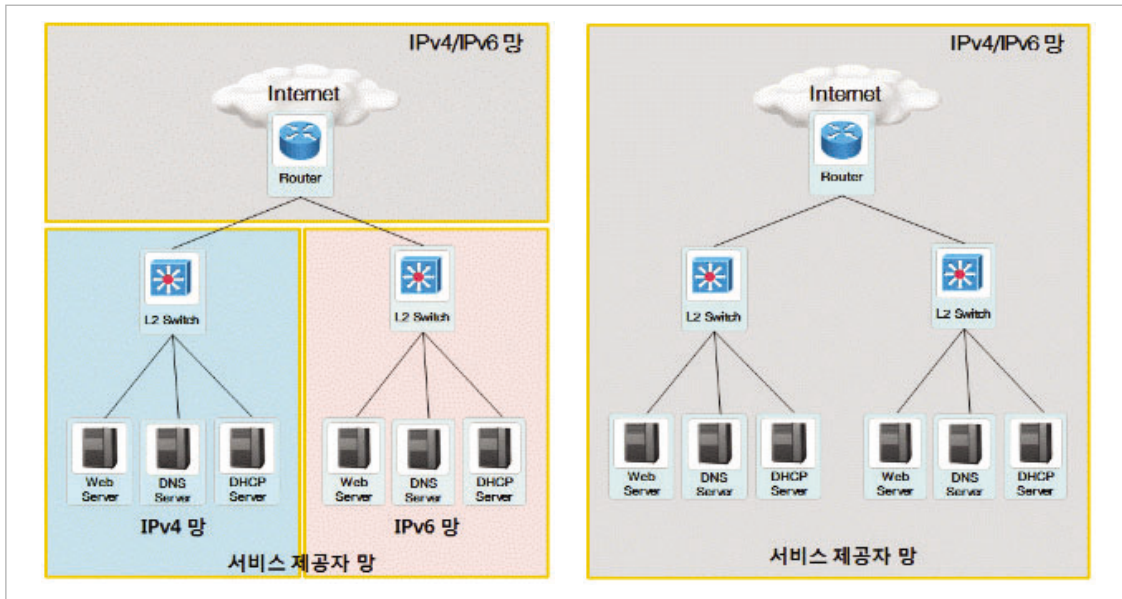
서비스 제공방안

IPv6 도입이 가능한 망은 IPv4/IPv6 듀얼스택으로 구성을 하고, 신규 투자가 어려운 VDSL, ADSL과 같은 망의 경우 기존고객을 IPv6가 지원되는 망으로 최종 이전하고 서비스 중지를 검토할 수 있다.

대규모의 IPv6 Only가입자를 수용하기 위하여 다음과 같은 방안이 있다.

- ① 기존 IPv4 서비스의 변경 없이 신규 IPv6 서비스 구축
- ② 기존 IPv4 서비스를 IPv4/IPv6 듀얼스택으로 전환

[그림 4-6] 웹서비스 Test 구성도



3. 점검 리스트

[표 4-1] 단계별 IPv6 전환 체크리스트 예시

적용단계	내 용
IPv6 전환 준비	- IPv6 도입의 기대효과를 예상하였는가? - 전환 TFT 구성은 적절하였는가? - 전환 TFT 운영에 개선할 사항은 없었는가?
IPv6 적용 계획 수립	- IT 자원 파악은 정확히 이루어졌는가? - IT 자원 파악 시 추가할 규격이나 내용은 없는가? - IPv6 도입 범위 설정에 문제는 없었는가? - IPv6 도입 우선 순위는 문제가 없었는가? - 전환비용 산출은 타당하였는가? - 사전에 고려하지 못한 사항으로 전환비용이 늘어났는가?
IPv6 구축 준비	- 위험요소분석에서 고려하지 못한 사항은 없었는가? - IPv6 주소 공간 확보를 위한 소요 주소 산출은 적절했는가? - 기관 내에 주소할당 및 관리 정책에 문제는 없는가? - 실제 네트워크 설계 시 보완할 사항은 없었는가? - 문제 발생 시 원상 복구 계획 등의 대처방안이 마련되었는가? - 대처방안은 적절히 수립되었는가? - IPv6 구축을 위한 장비 선정은 적절했는가? - 장비 발주는 원활히 이루어졌는가?



적용단계	내 용
IPv6 구축 및 점검	• 네트워크 장비 구축 시 어떤 문제점이 발생하였는가? • 보안장비 구축 시 어떤 문제점이 발생하였는가? • OS 업그레이드 시 어떤 문제점이 발생하였는가? • 애플리케이션 구축 시 어떤 문제점이 발생하였는가? • 수립된 보안정책에 따라 보안이 제공되는가? • 내·외부 네트워크 연동은 정상적으로 이루어졌는가?
IPv6 운영 및 교육·홍보	• 기존 서비스의 이용에 대한 문제는 없었는가? • 신규 서비스의 이용에 대한 문제는 없었는가? • IPv6 도입에 의해 기존 네트워크 관리에 대한 문제는 없었는가? • IPv6 망운영에 관련하여 발생한 문제는 없었는가? • 교육 계획의 수립 및 실행은 원활하게 이루어졌는가? • 교육(대상, 내용, 방법 등)에 대해 변경해야 할 사항은 없는가? • IPv6 도입에 대한 홍보는 충분히 이루어졌는가? • 홍보(대상, 내용, 방법 등)에 대해 변경해야 할 사항은 없는가?

4. 테스트결과에 따른 IPv6 전환 시 점검사항

4.1 개인 가입자 OS 측면

가입자는 IPv6를 지원하는 OS를 사용해야만 IPv6의 서비스를 제공 받을 수 있다. MS Windows 계열의 OS는 Windows XP 이상의 OS를 사용해야만 한다. 하지만 완벽한 지원은 Vista 이상 버전부터 제공중이다.

[표 4-2] 유·무선 단말기용 운영체제 IPv6 지원 여부('10.8월 현재)

종류	제조사	운영체제 명	IPv6 지원 여부	비고
PC	애플	맥OS	10.x이상	최신버전 : 10. 5. 3
	MS	Windows 3.1, 95, 98, ME	지원하지 않음	미지원
		Windows 2000 pro	조건부 지원	별도 프로그램 설치
		Windows XP	지원	서비스팩2 설치 후 IPv6 설정 필요
		Windows Vista	지원	운영체제 자체 내장, 부팅 후 자동설정
		Windows 7	지원	운영체제 자체 내장, 부팅 후 자동설정
PDA/ 스마트폰	MS	Windows CE.NET	4.1 이상 지원	3G 환경에서는 단말기의 베이스밴드 칩에서도 IPv6지원 필요
	MS	Windows Mobile	코발트 6.0 이상 지원	
	구글	안드로이드	2.1 이상 지원	
	팜	팜OS	코발트 6.0 이상	
	애플	iphone /ipod OS,	iOS 4.0 이상 지원	
	RIM	Blackberry	지원하지 않음	



4.2 어플리케이션 측면

개인 가입자가 많이 사용하는 OS별 개별 어플리케이션들은 현재까지 IPv4 전용으로 개발된 것들이 대부분 이므로 IPv6 Only 가입자를 수용하는 경우 다음과 같이 대응할 수 있다.

- ✓ 가입자에게 IPv6가 지원되는 대체 어플리케이션 목록 공지
- ✓ IPv6 지원 어플리케이션 개발
- ✓ 호스트 레벨의 변환기술(BIS, BIA) 도입 검토

단, 호스트 레벨의 변환기술은 IPv6 전환기에 단기적으로만 쓰는 전환 솔루션으로 반드시 유지해야 하는 IPv4 Only 어플리케이션이 있는 경우엔 이들 변환기술들도 검토해 볼 수 있지만 가능하면 모든 어플리케이션들이 IPv6를 지원하는 방향으로 개발하는 것을 권장한다.

4.3 웹사이트 이용측면

망 사업자가 개인고객에게 프로토콜 변환을 통한 IPv6 접속을 제공한다면 개인고객들이 자주 이용하는 웹사이트를 정상적으로 이용가능한지 확인해야 한다(activeX 등).

4.4 고객택내장비(CPE) 및 전용단말 측면

고객택내장비(CPE: Customer Premises Equipment)란 망 사업자가 고객택 내에 설치한 종단 장치로 대표적으로 케이블 모뎀, ADSL모뎀, 셋톱박스, IP공유기 등이 있다. 가입자단 IPv6 지원을 위해서는 기존 CPE들의 소프트웨어적 업그레이드나 교체가 필요하다.

케이블 인터넷망(HFC) 지원 현황

HFC 망에서 케이블 모뎀 서비스를 위한 국제기술규격인 DOCSIS 3.0부터 IPv6 및 Forwarding, Tunnel 기능이 지원되고 있다. 일부 DOCSIS 2.0 모뎀에서도 IPv6가 지원된다.²⁾

2) <http://www.arrisi.com>

IPTV 서비스 지원 현황

현 IPTV 서비스는 IPv4로 제공되고 있어 향후 IPTV 셋톱박스가 IPv6를 지원해야 하며, IPTV 구성 장비들 모두 IPv6 멀티캐스트가 지원이 되어야 한다.

ADSL/FTTH 서비스 현황

이 경우 일반적으로 CPE는 IP 장비가 아니나 칩셋 제조사에서 Modem chip과 다른 chip(간단한 switching chip)을 하나의 chip으로 만드는 경우 IP packet을 다루기 때문에 IPv6와 관련이 있으므로 장비 개발 시 여러 상황을 고려해야 한다.

무선망 단말 현황

2010년 10월 현재 3G망에서 IPv6를 지원하는 스마트폰은 Nokia의 Maemo OS를 사용하는 N900을 제외하고는 없는 상황이다. 3G망에서는 단말내 모뎀관련 기능이 IPv6 지원이 되지 않는 것으로 나타났다.

〈스마트폰 IPv6 지원 현황〉

구분	아이폰		안드로이드폰 2.1 이상	윈도우 모바일 6.1	Maemo (Nokia)
	4G	3GS			
3G 망	X	X	X	X	O
Wi-Fi	O	X	O	O	O

4.5 IP공유기 사용 측면

IPv4 기반의 가정용 공유기는 공인 IP주소 1개를 고객 댁내에서 여러 개의 사설IP 주소로 나누어 쓸 수 있는 장점이 있어 사용이 일반화 되었다. 하지만 IPv6 Only 이용자의 경우 다음과 같이 IPv6 주소 할당방식에 따라 공유기의 필요 여부가 결정된다.

① Auto-configuration을 사용했을 시 공유기 사용 여부

가입자의 MAC을 바탕으로 자동으로 IPv6 IP를 할당해주는 방법으로 이용자들은 특별한 제약 없이 자신의 모든기기에 공인 IP를 할당받게 된다. 즉 이 경우엔 공유기는 필요 없다.

② DHCPv6를 사용했을 시 공유기 사용 여부

관리자의 관리 하에 DHCPv6 서버에서 IP를 할당해주게 된다. 가입자에게 정해진 개수의 IPv6 주소만 할당해주는 방식이다. 이 경우 기존 공유기 같은 장치가 필요할 수 있으나 IPv6를 위한 새로운 NAT



기술이 필요하다.

IPv6는 모두 공인주소로써 외부로부터 내부 호스트의 주소로 바로 접속이 가능하므로 향후 홈게이트웨이 위치에서 방화벽 등 보안기능이 요구될 수 있다.

단, 가입자 PC가 IPv4/IPv6 듀얼환경인 경우, 터널 트래픽 처리 등을 위해 기존 공유기에서도 IPv6를 지원해야 한다. 일부 공유기는 펌웨어 업그레이드만으로도 가능할 수 있지만 새로운 장비로 교체가 필요한 경우도 있을 것이다.

4.6 Layer 2 스위치 측면

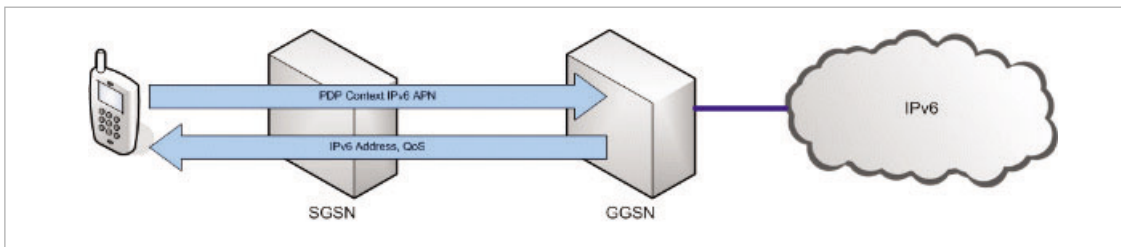
IPv6 전환 시 L2 Switch에서 발생할 수 있는 이슈들로 멀티캐스트, Netbios 및 QoS 등의 이슈들이 나올 수 있다.

- ✓ Multicast Snooping : IPTV 서비스에 활용
- ✓ NetBIOS Filter : 사용자간 원도 공유폴더 제어
- ✓ QoS : VoIP, IPTV 등 서비스의 품질보장
- ✓ DHCP Filter : 합법적인 사용자의 네트워크 접근 허용

4.7 무선망 측면

3G망을 위한 네트워크를 구성하는 주요 요소는 단말과 HLR, SGSN과 GGSN 장비로 구성된다. IPv6 접속을 위한 PDP Context 요청 및 응답은 다음과 같다.

[그림 4-7] PDP Context 절차



단말은 PDP Context 생성시에 PDP-Type을 IPv6로, APN을 IPv6를 위한 APN으로 설정하여 GGSN으로 요청을 보내고, GGSN은 해당 APN에 대한 처리를 수행한 후 결과를 단말에 전달한다.



이후 단말을 IPv6 망에 접속하게 된다. 2010년 한국인터넷진흥원과 SK텔레콤이 협력한 3G망 시범사업에서 SK텔레콤 상용망에서 사용중인 GGSN 장비에 국내최초로 IPv6를 적용하였다.

4.8 서버 관리 측면

대규모 서버팜(server farm)을 Auto-configuration 기반으로 운영할 경우 서버의 MAC주소를 기반으로 호스트 주소를 생성하는데, 테스트결과 장비가 리부팅 되더라도 주소는 거의 변경되지 않았다. 하지만 추가적으로 다음과 같은 사항을 고려할 수 있다.

- ✓ L4 스위치 사용시 동적주소 가능여부
- ✓ 서버 상위에 있는 스위치, 방화벽 등의 Auto-configuration 가능여부 등

4.9 서버 OS 측면

Windows Server 계열 OS의 경우 버전에 따라 IPv6 지원상태가 다르다. 2003 server는 부분적으로 지원되며 2008 Server 부터 IPv6를 완벽 지원한다.

4.10 서비스 측면

웹서비스 구성 시 다음의 경우 문제가 될수 있으므로 점검이 필요하다.

- ✓ 웹페이지 소스코드 상에 IPv4 주소를 하드코딩 한 경우
- ✓ 이미지를 외부의 IPv 4서버에서 sourcing하는 경우
- ✓ 타 업체와 연동된 서비스가 IPv4만 지원하는 경우(예: 카드결제, 실명 인증, 광고배너 등)

웹을 DB와 연동하는 경우 DB 버전에 따라 IPv6 기반 DB connection을 지원하였다.(MS-SQL 2005 이상 Oracle 11g 이상) IPv6를 지원하지 않더라도 웹서버와 DB서버 간의 내부연동은 IPv4로 가능하였다.



4.11 L4 스위치 측면

IPv6에서 L4장비를 구축하여 적용시키기 위해서 가장 중요한 점은 L4 장비의 IPv6 지원 여부와 load-balance 기능이다.

이러한 load-balance를 지원하기 위하여 물리적으로 서버와 L4간 IPv6 연결이 가능해야 하며 VIP(Virtual IP)를 설정하여 session별 혹은 contents 별로 load-balance가 IPv6 기반으로 이루어져야 한다.

4.12 ActiveX 측면

ActiveX는 대부분 IPv4 주소와 MAC 주소를 확인하여 중복 접속 확인 및 차단 기능으로 활용한다. 앞으로 IPv6 서비스를 수용하기 위해서 기존 ActiveX에 IPv6 주소와 DUID³⁾값도 함께 처리되도록 업데이트 되어야 한다.

4.13 인트라넷 보안 툴 IPv6 지원

개인 방화벽에서 IPv6 기반 차단을 제공하지만, 관리툴과의 통신은 IPv4만 지원하는 등 아직까지는 부분적인 지원을 제공하는 제품들이 있으므로 관련 제품 도입시엔 IPv6 지원여부를 보안 기능뿐 아니라, 일반 통신기능까지 확인이 필요하다.

4.14 DHCP 운영 측면

Windows XP의 경우 IPv6는 지원하지만 DHCPv6 Client 기능은 지원하지 않는다. DHCPv6 Client 기능은 Windows Vista 이상 버전부터 지원하므로 원활한 IPv6 서비스를 받기 위해서는 Vista 이상을 권장한다.

3) DUID(DHCPv6 Unique Identifier) : IPv4의 MAC주소 대신 사용하며, 기존 MAC주소와 시간값을 조합해 생성하거나, 벤더에서 고유값을 부여하는 방식으로 정한다.

4.15 보안측면

다음과 같은 예상되는 취약점이 있으므로 실제 IPv6 적용시 해당 대책을 검토해야 한다.

[표 4-3] IPv6 적용기술에 따른 보안 취약점 및 대책 방안

구 분	취약점	대책
Dualstack	호스트 간 예상치 못한 터널링이 발생할 수 있으며, 의도하지 않은 상호작용 때문에 새로운 취약성 발생 가능성	조직은 새로운 IPv6 기능(이동성, 비상태주소설정, ND프로토콜, IPsec 기반 종단간 암호화)를 인지하고, 침입탐지, 모니터링, 로깅 및 감사기능을 업그레이드하여 IPv4와 동일한 수준의 정보보호 대책 마련
Tunneling	비인가된 터널링 생성으로 인한 백도어 구축의 위험성 인지 필요	터널링된 트래픽을 패킷필터, 안티바이러스, 방화벽, IDS, 트래픽 필터링 정책(ingress & egress filtering)등으로 검사하여 비인가된 터널링 트래픽을 차단해야 하며, 터널링 트래픽을 IPsec(RFC 4891)으로 터널 종단 간 암호화
Address Management	시스템의 이더넷 카드 제품번호(EUI-64 인터페이스 식별자)를 사용하는 주소자동구성 방법으로 인해 공격자가 네트워크를 더 쉽게 스캐닝 가능	네트워크 경계에서 스캐닝 활동을 금지하고 암호 알고리즘사용을 통한 주소생성(CGA), DHCPv6 사용을 통한 주소할당 방법 권장



제5장 결언



국내 주요 망 사업자를 중심으로 백본망의 듀얼스택 장비 준비율은 70%를 넘어서고 있다. 대형 장비 제조사들은 이미 2000년초부터 IPv6 지원장비를 출시하고 있고, 망 사업자들도 용량증설, 노후장비 교체시기에 자연스럽게 IPv6가 지원되는 최신 장비들을 도입해온 결과다.

포털, 콘텐츠 제공자 등 서비스 제공 사업자들은 대체로 서버부분 장비 규모가 네트워크장비 규모보다 크다. 따라서 준비율 차원에서는 망 사업자 못지않지만, 실제로는 서버내에서 구동되는 OS 나 어플리케이션에 IPv6 적용을 고려해야 하기 때문에 다양한 검토가 필요하다.

기업 비즈니스를 위해 인터넷을 활용하는 비즈니스 이용자들은 망 사업자의 인터넷 서비스를 이용하면서 외부고객들을 위한 웹서비스 제공 및 내부고객을 위한 업무환경을 동시에 제공하고 있다.

현재까지 IPv6 지원 제품들은 주로 외산이 많으며, 특히 라우터, L3 스위치 등 핵심 네트워크 장비들의 외산 점유율은 높은 편이다. 이는 이미 전세계에 시스코, 줘니퍼 등의 외산 IPv4 장비가 광범위하게 보급되면서 예견된 일이었다. IPv6 지원 제품역시 기존 시장 지배적 기업들이 기능추가를 통해 그대로 주도해 나갈 확률이 높다.

준비상태는 각기 다르지만 2011년 전세계 IPv4 신규 할당 중지를 앞두고 현재 IPv6 상용망은 거의 없는 것이 현실이다. 포털중에는 글로벌 사업자중인 '구글' 정도만 IPv6 적용을 완료한 상태다. 기존 비즈니스 이용자들은 망 사업자나 서비스 제공자가 IPv6를 제공하기 전까지는 큰 움직임은 없을 것으로 예상되고 있다. 하지만 앞으로 새롭게 등장하는 비즈니스 이용자들은 IPv6 주소를 할당 받아야 한다. 기존 비즈니스 이용자들도 사업을 확장하거나 새로운 주체들과 사업을 위해서는 IPv6에 대한 준비는 필수적이다.



제품개발시 기존 제품군 위주로 IPv6 고려사항을 분석하고 추가 개발하는 방안과 함께 전환기에 필요한 새로운 제품 개발도 검토할 수 있다.

예를 들어 리저시 망의 전환을 쉽게 해주거나, IPv4/IPv6 듀얼 환경 운영에 따른 복잡성을 줄여 주는 관리툴의 개발, 새로운 보안툴의 개발 등이 있을 수 있다. 아울러 제품 개발과 함께 관련된 국내외 인증을 획득한다면 IPv6 시장 초기에 신뢰성 향상 등 다양한 이점을 얻을 수 있을 것이다.

IPv6 적용은 장비에서 단순히 IPv6를 활성화(enable) 시키는 것으로 끝나지 않는다. 적용 분야를 세세히 나누고, 단계적 적용시 우선순위와 적용방법에 대한 수많은 경우의 수를 생각해야 한다. 내부적인 적용부터 외부망과 연동, 고객민원 처리, 또한 장기적으로 듀얼환경을 운영해야 하는 고민까지 해야 하기 때문이다.

따라서 본 책자에서는 IPv6 적용의 이해를 돕기위해 분야별로 총 300여 가지 IPv6 적용 시나리오를 검토해 최종적으로 모든 시나리오의 핵심이 되는 4가지 시나리오 유형을 도출해 테스트베드를 구성하고 시험했다.

단, 실제 상용 수준의 트래픽은 고려하지 않은 테스트베드 상의 시험이므로 성능 이슈는 본 책자를 참고해 독자의 환경에서 추가 확인해야 한다.

망 사업자, 서비스 제공자 및 비즈니스 이용자 모두 테스트 결과 현재 출시된 주요 장비들로 기본적인 IPv6 망 구성에 문제는 없었다. 다만 어플리케이션에서 주소 입력시에 IPv6를 인식하지 못해 오류가 발생하는 경우가 있었으며, 이를 제외하면 현재 상황에서도 IPv6를 적용하기에 큰 문제는 없는 것으로 판단되었다.

테스트결과 분야별로 세부 이슈들을 살펴보면 다음과 같다.

망 사업자 입장에서는 L2 스위치에서의 IPv6 이슈 및 공유기, 모뎀 등 고객택내장치(CPE)의 IPv6 미지원 이슈가 있을 수 있음을 확인했다. 멀티캐스트가 필수인 IPTV 서비스의 경우 IPv6 적용시 가입자망의 L2 스위치까지 교체해야 하는 경우가 발생할 수 있다. 또한 최종 가입자까지 IPv6를 할당한다면 CPE에서 IPv6 지원여부를 확인하고 업그레이드, 교체 등의 대응방안도 마련해야 한다. 이와같은 내용은 L2 장비에서는 IPv6 이슈가 없을 것이라는 기존의 일반적 인식을 뒤집는 결과로 의미가 크다.



서비스 제공자 입장에서는 대규모 서버팜(server farm) 관리에 IPv6의 Auto-configuration 기능을 검토하였다. 테스트 결과 서버의 네트워크 인터페이스가 바뀌지 않는 한 재 부팅후에도 동일한 주소를 자동 생성하여 실제 서비스의 가능성을 보였다. 서버 OS의 경우 오래된 구버전은 IPv6를 부분적으로만 지원하고 있는 경우가 있어, 가능하면 최신버전으로 업그레이드 하거나 지원내역을 확인해야 한다. DBMS처럼 웹서버와 연동된 중요 시스템이지만 IPv4만 지원하는 경우에는 내부에서는 IPv4로 통신을 유지하고 외부로는 IPv6로 통신하는 방안을 검토할 수 있다. 마지막으로 금융권, 쇼핑몰 등에 광범위하게 사용중인 ActiveX에 대해서도 IPv6를 지원할 수 있도록 관련내용을 검토해야 한다.

비즈니스 이용자 입장에서는 업무용 PC들은 세부 버전에 따라 IPv6 동작이 상이할 수 있기 때문에 적용전에 현황파악이 중요하다. IPv6 주소 할당 시에도 Auto-configuration과 DHCP를 적절히 병행할 수 있고, PC들도 OS 버전에 따라 상이한 동작을 하므로 여러 선택사항을 고려해야 한다.

제품 제조사 입장에서는 이미 수년전부터 공공부문을 중심으로 제품 도입시 IPv6 요구사항은 지속적으로 반영되어 왔으나, IPv4 주소 할당이 중단되는 시점부터 이런 요구가 강화될 것이므로 고객의 본격적인 요구사항에 대응해야 한다.

우리는 다소 늦었지만 틈새를 공략해 국산제품을 많이 사용하는 L2 스위치, 보안장비 및 소프트웨어 위주로 IPv6를 준비하면 관련시장에 충분히 대응 가능할 것이다. 현재까지는 국내에서의 수요는 신규 서비스 위주로 발생할 것으로 예상되나, 이미 중국, 일본 등 인구수나 기술적 우위 선점에 관심이 많은 국가들에서 공격적으로 IPv6 적용에 나서고 있어 해외시장의 제품 수요도 주시할 필요가 있다.

IPv6 적용은 한번에 모든 이슈를 발견하고 해결하기 어려운 사안이다. IPv4로 시작한 첫 번째 인터넷이 있기까지 많은 시행착오가 있었듯이 IPv6로 시작하는 ‘두번째 인터넷’을 만드는 것도 이해관계자들의 지속적인 관심과 노력이 필요하다. 특히 경영진은 비즈니스의 연속성 보장 및 신규 서비스 확장의 중요성을 인식해 지속적인 투자계획을 세우고 관련 실무진들을 다각적으로 지원해야 한다. 본 실전 적용서가 IPv4 기반 인터넷이 확장을 끝내고 새로운 IPv6 인터넷의 확산이 시작되는 역사적인 원년에 국내 인터넷 이해관계자들에게 디딤돌이 되길 기대한다.

[첨부1] 망사업자 분야별 대표서비스 및 주요 점검사항

1. Metro Ethernet 서비스

구분	구성장비	종류	IPv6 지원장비 출시여부 (' 10.6현재)	주요 점검사항
백본망		L3	○	• IPv6 주소 입력가능 • IPv6 라우팅 기능 • SNMP 등 관리 기능 • 보안관련 기능
가입자망		L3	○	• IPv6 주소 입력가능 • IPv6 라우팅 기능 • SNMP 등 관리 기능 • 보안관련 기능
고객		PC	○	• 윈도우XP 이상

2. HFC 서비스

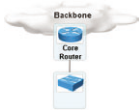
구분	구성장비	종류	IPv6 지원장비 출시여부 (' 10.6현재)	주요 점검사항
백본망		라우터 /스위치	○	• IPv6 주소 입력가능 • IPv6 라우팅 기능 • SNMP 등 관리 기능 • 보안관련 기능
가입자망 (HFC망)		L3	○	• IPv6 주소 입력가능 • IPv6 라우팅 기능 • SNMP 등 관리 기능 • 보안관련 기능
고객택내		L2	N/A	• DHCP 등 L2 이외 부가 기능 사용시 확인필요 • DOCSIS3.0 이상 지원
		L7		



3. FTTH 서비스

구분	구성장비	종류	IPv6 지원장비 출시여부 ('10.6현재)	주요 점검사항
백본망		라우터 /스위치	○	- IPv6 주소 입력가능 - IPv6 라우팅 기능 - SNMP 등 관리 기능 - 보안관련 기능 여부
가입자망 (FTTH망)		L3	X	- IPv6 주소 입력가능 - IPv6 라우팅 기능 - SNMP 등 관리 기능 - 보안관련 기능
		L1	N/A	-
		L2	N/A	Multicast, DHCP 등 L2 이외 부가기능 사용 시 확인필요
고객택내		PC	○	윈도XP 이상

4. VDSL 서비스

구분	구성장비	종류	IPv6 지원장비 출시여부 ('10.6현재)	주요 점검사항	비고
백본망		라우터 /스위치	○	- IPv6 주소 입력 기능 - IPv6 라우팅 기능 - SNMP 등 관리 기능 - 보안관련 기능	
가입자망 (FTTH망)		L3	X	- IPv6 주소 입력 가능 - IPv6 라우팅 기능 - SNMP 등 관리 기능 - 보안관련 기능	국내업체 개발중
		L1	N/A	-	
고객택내		L2	N/A	Multicast, DHCP 등 L2 이외 부가기능 사용시 확인필요	
		PC	○	윈도XP 이상	

5. WiFi 서비스

구분	구성장비	종류	IPv6 지원장비 출시여부 ('10.6현재)	주요 점검사항
백본망		L3	O	- IPv6 주소 입력 가능 - IPv6 라우팅 기능 - SNMP 등 관리 기능 - 보안관련 기능
가입자망		L2	X	- IPv6 주소 입력 가능 - IPv6인증 프로토콜 기능 - 보안관련 기능
고객		PC	O	윈도XP 이상

6. ADSL 서비스

구분	구성장비	종류	IPv6 지원장비 출시여부 ('10.6현재)	주요 점검사항
백본망		L3	O	- IPv6 주소 입력 가능 - IPv6 라우팅 기능 - SNMP 등 관리 기능 - 보안관련 기능
가입자망 (ADSL망)		L3	O	- IPv6 주소 입력 가능 - IPv6 라우팅 기능 - SNMP 등 관리 기능 - 보안관련 기능 - DHCP 기능
		다중 화기	N/A	-
고객택내		L2	N/A	Multicast, DHCP 등 L2 이외 부가기능 사용시 확인필요
		PC	O	윈도XP 이상



7. VoIP 서비스

구분	구성장비	종류	IPv6 지원장비 출시여부 ('10.6현재)	주요 점검사항
백본망		라우터/스위치	○	- IPv6 주소 입력 가능 - IPv6 라우팅 가능 - SNMP 등 관리 기능 - 보안관련 기능 - IPv6 Qos 기능
가입자망		SSW	X	- IPv6 주소 입력가능 - SIP, H.323 Protocol 처리 기능 - 보안관련 기능
		호처리장치	○	- IPv6 주소 입력 가능 - NAT 및 DHCP 기능 - SIP, H.323 Protocol 처리 기능 - 보안관련 기능
고객		IP폰	○	- IPv6주소 입력가능 - 음성통화 기능

8. 모바일 서비스

구분	구성장비	종류	IPv6 지원장비 출시여부 ('10.6현재)	주요 점검사항	비고
백본망 (유선망)		라우터 /스위치	○	- IPv6 주소 입력 가능 - IPv6 라우팅 가능 - SNMP 등 관리 기능 - 보안관련 기능 - MPLS 6PE 기능 - IPv6 Multicast 기능 - IPv6 Qos 기능	
3G망 (무선망)		L3	○	- IPv6 주소 입력 가능 - SGSN과 GGSN간 IPv6 통신 - WCDMA 무선단말에 IPv6 자동 주소 할당 - GGSN과 유선망 통신시 IPv6 통신	
		L2	○		
고객		단말	○	DHCP를 이용한 IPv6 주소 사용 가능	Nokia N900 1종

9. VPN 서비스

구분	구성장비	종류	IPv6지원장비 출시 여부 ('10.6현재)	주요 점검사항	비고
백본망		라우터 /스위치	○	- IPv6 주소 입력 기능 - IPv6 라우팅 기능 - SNMP 등 관리 기능 - 보안관련 기능 - 6VPN 기능	
가입자망		L3	○	- IPv6 주소 입력 기능 - IPv6 라우팅 기능 - SNMP 등 관리 기능 - 보안관련 기능 - 6VPN 기능	
고객		PC	○	- 윈도우XP 이상	

10. IPTV

구분	구성장비	종류	IPv6지원장비 출시 여부 ('10.6현재)	주요 점검사항	비고
백본망		라우터 /스위치	○	• IPv6 주소 입력 기능 • IPv6 라우팅 기능 • SNMP 등 관리 기능 • 보안관련 기능 • IPv6 Multicast 기능 • IPv6 Qos 기능	
가입자망		L3	○	• IPv6 주소 입력 기능 • IPv6 라우팅 기능 • SNMP 등 관리 기능 • 보안관련 기능 • IPv6 Multicast 기능 • IPv6 Qos 기능	
		L2	X	• IPv6주소 입력 기능 • IPv6 Multicast 기능 • IPv6 Qos 기능	
고객		셋탑	X	• IPv6 주소 입력 기능 • IPv6 Multicast 기능 • IPv6 Qos 기능 • 관리 기능	

분야별 차세대인터넷주소 IPv6 실전적용

【인 쇄】 2011년 1월

【발 행】 2011년 1월

【발행인】 서 종 렬

【발행처】 한국인터넷진흥원(KISA, Korea Internet & Security Agency)

서울시 송파구 가락동 79-3 대동빌딩

TEL : (02)4054-118

【인쇄처】 (주)현대아트컴 (02-2278-4482)

〈〈비매품〉〉

1. 본 연구보고서는 정보통신진흥기금으로 수행한 정보통신연구개발사업의 연구결과입니다.
2. 본 연구보고서의 내용을 발표할 때에는 반드시 한국인터넷진흥원 정보통신연구개발사업의 연구결과임을 밝혀야 합니다.
3. 본 연구보고서의 판권은 한국인터넷진흥원이 소유하고 있으며, 당 진흥원의 허가 없이 무단 전재 및 복사를 금합니다.